



# Cisco Unified CallManager セキュリティ ガイド

Release 5.1(3)

Text Part Number: OL-14151-01-J



**【注意】この文書はお客様の便宜のために作成された参考和訳であり、お客様とシスコシステムズとの間の契約を構成するものではありません。正式な契約条件は、弊社担当者、または弊社販売パートナーにご確認ください。**

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。見当たらない場合には、代理店にご連絡ください。

シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB ( University of California, Berkeley ) パブリック ドメイン パーミッションとして、UCB が開発したプログラムを最適化したものです。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、すべてのマニュアルおよび上記各社のソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記各社は、商品性や特定の目的への適合性、権利を侵害しないことに関する、または取り扱い、使用、または取り引きによって発生する、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、シスコおよびその代理店は、このマニュアルの使用またはこのマニュアルを使用できないことによって起こる制約、利益の損失、データの損傷など間接的で偶発的に起こる特殊な損害のあらゆる可能性がシスコまたは代理店に知らされていても、それらに対する責任を一切負いかねます。

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

*Cisco Unified CallManager セキュリティ ガイド*

Copyright © 2007 Cisco Systems, Inc.

All rights reserved.



<b>このマニュアルについて</b>	<b>xi</b>
目的	xi
対象読者	xii
マニュアルの構成	xii
関連マニュアル	xiii
表記法	xiii
技術情報の入手方法、サポートの利用方法、およびセキュリティ ガイドライン	xiv
シスコ製品のセキュリティの概要	xiv

---

**PART 1**

---

**セキュリティの基礎**

---

**CHAPTER 1**

<b>セキュリティの概要</b>	<b>1-1</b>
認証および暗号化に関する用語	1-2
システム要件	1-4
機能一覧	1-5
セキュリティ アイコン	1-5
相互作用および制限	1-6
相互作用	1-6
制限	1-7
認証と暗号化	1-7
割り込みと暗号化	1-8
ワイドバンド コーデックと暗号化	1-8
メディア リソースと暗号化	1-8
電話機のサポートと暗号化	1-9
電話機のサポートと暗号化設定ファイル	1-9
SIP トランクのサポートと暗号化	1-9
セキュリティ アイコンと暗号化	1-9
クラスタおよびデバイス セキュリティ モード	1-10
ダイジェスト認証と暗号化	1-10
パケット キャプチャと暗号化	1-10
ベスト プラクティス	1-11

デバイスのリセット、サービスの再起動、またはサーバおよびクラスタのリ ブート	1-11
メディア暗号化の設定と割り込み	1-12
インストール	1-13
TLS と IPSec	1-13
証明書	1-14
電話機の証明書の種類	1-14
サーバの証明書の種類	1-15
外部 CA からの証明書のサポート	1-16
認証、整合性、および許可の概要	1-17
イメージ認証	1-17
デバイス認証	1-17
ファイル認証	1-18
シグナリング認証	1-18
ダイジェスト認証	1-18
許可	1-20
暗号化の概要	1-22
シグナリング暗号化	1-22
メディア暗号化	1-22
設定ファイルの暗号化	1-24
設定用チェックリストの概要	1-25
セキュア クラスタへのサブスクリバ ノードの追加	1-29
その他の情報	1-30

CHAPTER 2

<b>HTTP over SSL (HTTPS) の使用方法</b>	<b>2-1</b>
HTTPS の概要	2-2
Internet Explorer による HTTPS の使用方法	2-3
Internet Explorer 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	2-3
証明書の詳細表示	2-4
証明書のファイルへのコピー	2-5
Netscape による HTTPS の使用方法	2-6
Netscape 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	2-7
その他の情報	2-8

CHAPTER 3

<b>Cisco CTL クライアントの設定</b>	<b>3-1</b>
Cisco CTL クライアントの概要	3-2
Cisco CTL クライアントの設定のヒント	3-3
Cisco CTL クライアントの設定用チェックリスト	3-4

Cisco CTL Provider サービスのアクティブ化	3-5
Cisco CAPF サービスのアクティブ化	3-6
TLS 接続用ポートの設定	3-6
Cisco CTL クライアントのインストール	3-8
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	3-10
Cisco CTL クライアントの設定	3-11
CTL ファイルの更新	3-15
CTL ファイル エントリの削除	3-17
クラスタ全体のセキュリティ モードの更新	3-17
Cisco CTL クライアントの設定内容	3-18
Cisco Unified CallManager クラスタのセキュリティ モードの確認	3-20
Smart Card サービスの開始および自動の設定	3-21
セキュリティ トークン パスワード ( etoken ) の変更	3-22
Cisco Unified IP Phone 上の CTL ファイルの削除	3-23
Cisco CTL クライアントのバージョンの特定	3-24
Cisco CTL クライアントの確認とアンインストール	3-24
その他の情報	3-25

## PART 2

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

## CHAPTER 4

**電話機のセキュリティの概要** 4-1

電話機のセキュリティ機能について	4-2
サポートされる電話機のモデル	4-3
電話機のセキュリティ設定の確認	4-3
電話機のセキュリティ設定用チェックリスト	4-4
その他の情報	4-5

## CHAPTER 5

**電話機セキュリティ プロファイルの設定** 5-1

電話機セキュリティ プロファイルの概要	5-1
電話機セキュリティ プロファイルの設定のヒント	5-2
電話機セキュリティ プロファイルの検索	5-3
電話機セキュリティ プロファイルの設定	5-4
電話機セキュリティ プロファイルの設定内容	5-5
電話機セキュリティ プロファイルの適用	5-12
電話機セキュリティ プロファイルの削除	5-13
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	5-14
その他の情報	5-15

CHAPTER 6

<b>Certificate Authority Proxy Function の使用方法</b>	<b>6-1</b>
Certificate Authority Proxy Function の概要	6-2
Cisco Unified IP Phone と CAPF の相互作用	6-2
CAPF システムの相互作用および要件	6-4
Cisco Unified CallManager Serviceability での CAPF の設定	6-4
CAPF の設定用チェックリスト	6-5
Certificate Authority Proxy Function サービスのアクティブ化	6-6
CAPF サービス パラメータの更新	6-7
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	6-8
電話の設定 ( Phone Configuration ) ウィンドウの CAPF 設定	6-9
LSC ステータスまたは認証文字列に基づく電話機の検索	6-10
CAPF レポートの生成	6-11
電話機での認証文字列の入力	6-12
電話機での認証文字列の確認	6-13
その他の情報	6-13

CHAPTER 7

<b>暗号化された電話機設定ファイルの設定</b>	<b>7-1</b>
電話機設定ファイルの暗号化について	7-2
鍵の手動配布	7-2
電話機の公開鍵による対称キーの暗号化	7-3
サポートされる電話機のモデル	7-5
暗号化された設定ファイルの設定のヒント	7-6
暗号化設定ファイルの設定用チェックリスト	7-7
電話機設定ファイルの暗号化の有効化	7-8
鍵の手動配布の設定	7-8
鍵の手動配布の設定内容	7-9
電話機での対称キーの入力	7-10
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	7-11
電話機設定ファイルが暗号化されていることの確認	7-12
電話機設定ファイルの暗号化の無効化	7-12
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クレデンシャルの除外	7-13
その他の情報	7-14

CHAPTER 8

<b>SIP 電話機のダイジェスト認証の設定</b>	<b>8-1</b>
SIP 電話機ダイジェスト認証の設定用チェックリスト	8-2
ダイジェスト認証サービス パラメータの設定	8-3

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 クレデンシャルの設定	8-4
エンドユーザダイジェストクレデンシャルの設定内容	8-5
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	8-5
その他の情報	8-6

## CHAPTER 9

<b>電話機のセキュリティ強化</b>	9-1
Gratuitous ARP 設定の無効化	9-1
Web Access 設定の無効化	9-2
PC Voice VLAN Access 設定の無効化	9-2
Setting Access 設定の無効化	9-2
PC Port 設定の無効化	9-2
電話機設定のセキュリティ強化	9-3
その他の情報	9-4

## CHAPTER 10

<b>ボイスメールポートのセキュリティ設定</b>	10-1
ボイスメールのセキュリティの概要	10-1
ボイスメールセキュリティの設定のヒント	10-2
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	10-3
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	10-4
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	10-5
その他の情報	10-6

## PART 3

**Cisco CTI、JTAPI、および TAPI アプリケーションのセキュリティ**

## CHAPTER 11

<b>CTI、JTAPI、および TAPI の認証および暗号化の設定</b>	11-1
CTI、JTAPI、および TAPI アプリケーションの認証について	11-2
CTI、JTAPI、および TAPI アプリケーションの暗号化について	11-4
CTI、JTAPI、および TAPI アプリケーションに対する CAPF の概要	11-5
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	11-6
CTI、JTAPI、および TAPI のセキュリティ設定用チェックリスト	11-7
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およびエンドユーザの追加	11-9
Certificate Authority Proxy Function サービスのアクティブ化	11-11
CAPF サービスパラメータの更新	11-11
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	11-12
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	11-13

アプリケーションユーザ CAPF プロファイル ウィンドウおよび エンドユーザ CAPF プロファイル ウィンドウの CAPF 設定	11-14
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	11-16
JTAPI/TAPI セキュリティ関連サービス パラメータ	11-17
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	11-17
その他の情報	11-18

PART 4

**SRST リファレンス、トランク、およびゲートウェイのセキュリティ**

CHAPTER 12

**Survivable Remote Site Telephony (SRST) リファレンスのセキュリティ設定**  
12-1

SRST のセキュリティの概要	12-1
SRST セキュリティの設定のヒント	12-2
SRST のセキュリティ設定用チェックリスト	12-3
SRST リファレンスのセキュリティ設定	12-4
SRST リファレンスのセキュリティの設定内容	12-6
SRST リファレンスからのセキュリティの削除	12-7
SRST 証明書がゲートウェイから削除された場合	12-7
その他の情報	12-8

CHAPTER 13

**ゲートウェイおよびトランクの暗号化の設定** 13-1

Cisco IOS MGCP ゲートウェイの暗号化の概要	13-2
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	13-3
SIP トランクの暗号化の概要	13-4
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	13-5
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	13-6
Cisco Unified CallManager 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	13-6
SRTP を許可 (SRTP Allowed) チェックボックスの設定	13-7
その他の情報	13-8

CHAPTER 14

**SIP トランク セキュリティ プロファイルの設定** 14-1

SIP トランク セキュリティ プロファイルの概要	14-2
SIP トランク セキュリティ プロファイルの設定のヒント	14-2
SIP トランク セキュリティ プロファイルの検索	14-3
SIP トランク セキュリティ プロファイルの設定	14-4
SIP トランク セキュリティ プロファイルの設定内容	14-5
SIP トランク セキュリティ プロファイルの適用	14-10

SIP トランク セキュリティ プロファイルの削除	14-11
その他の情報	14-12

---

**CHAPTER 15**

<b>SIP トランクのダイジェスト認証の設定</b>	<b>15-1</b>
SIP トランク ダイジェスト認証の設定用チェックリスト	15-2
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	15-2
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 クレデンシャルの設定	15-3
アプリケーション ユーザ ダイジェスト クレデンシャルの設定内容	15-3
SIP レルムの検索	15-4
SIP レルムの設定	15-5
SIP レルムの設定内容	15-6
SIP レルムの削除	15-7
その他の情報	15-8

---

**INDEX****索引**





# このマニュアルについて

---

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 \(P.xi\)](#)
- [対象読者 \(P.xii\)](#)
- [マニュアルの構成 \(P.xii\)](#)
- [関連マニュアル \(P.xiii\)](#)
- [表記法 \(P.xiii\)](#)
- [技術情報の入手方法、サポートの利用方法、およびセキュリティ ガイドライン \(P.xiv\)](#)

## 目的

『Cisco Unified CallManager 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。
- 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) リファレンス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。
- 問題をトラブルシューティングする。

## 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、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

章番号	説明
<b>セキュリティの基礎</b>	
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、相互対話と制限、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「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。
<b>電話機およびボイスメール ポートのセキュリティ</b>	
第 4 章「電話機のセキュリティの概要」	Cisco Unified CallManager および電話機でのセキュリティの使用法について説明し、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 5 章「電話機セキュリティ プロファイルの設定」	Cisco Unified CallManager 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 6 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ティングする方法も説明します。
第 7 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 CallManager の管理ページで設定する方法を説明します。
第 8 章「SIP 電話機のダイジェスト認証の設定」	Cisco Unified CallManager の管理ページを使用してダイジェスト認証を SIP 電話機に設定する方法を説明します。
第 9 章「電話機のセキュリティ強化」	Cisco Unified CallManager 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 10 章「ボイスメール ポートのセキュリティ設定」	Cisco Unified CallManager 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。
<b>CTI、JTAPI、および TAPI のセキュリティ</b>	
第 11 章「CTI、JTAPI、および TAPI の認証および暗号化の設定」	Cisco Unified CallManager 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。

表 1 このマニュアルの構成 (続き)

章番号	説明
<b>SRST リファレンス、ゲートウェイ、およびトランクのセキュリティ</b>	
第 12 章「Survivable Remote Site Telephony (SRST) リファレンスのセキュリティ設定」	Cisco Unified CallManager の管理ページで SRST リファレンスについてセキュリティを設定する方法を説明します。
第 13 章「ゲートウェイおよびトランクの暗号化の設定」	Cisco Unified CallManager 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 14 章「SIP トランク セキュリティ プロファイルの設定」	Cisco Unified CallManager 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。
第 15 章「SIP トランクのダイジェスト認証の設定」	Cisco Unified CallManager 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。

## 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 アドミニストレーション ガイド for Cisco Unified CallManager*
- *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*
- *Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity 4.x*
- 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**

便利なヒントです。

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。

## 技術情報の入手方法、サポートの利用方法、およびセキュリティ ガイドライン

技術情報の入手、サポートの利用、技術情報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、推奨するエイリアスおよび一般的なシスコのマニュアルに関する情報は、月刊の『*What's New in Cisco Product Documentation*』を参照してください。ここでは、新規および改訂版のシスコの技術マニュアルもすべて記載されています。次の URL からアクセスできます。

<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する必要があります。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。

シスコの暗号化製品に適用される米国の法律の概要については、次の URL で参照できます。

<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

何かご不明な点があれば、[export@cisco.com](mailto:export@cisco.com) まで電子メールを送信してください。



**PART 1**

**セキュリティの基礎**







# セキュリティの概要

Cisco Unified CallManager 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 CallManager 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送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。

- [認証および暗号化に関する用語 \(P.1-2\)](#)
- [システム要件 \(P.1-4\)](#)
- [機能一覧 \(P.1-5\)](#)
- [セキュリティ アイコン \(P.1-5\)](#)
- [相互作用および制限 \(P.1-6\)](#)
- [ベスト プラクティス \(P.1-11\)](#)
- [インストール \(P.1-13\)](#)
- [TLS と IPSec \(P.1-13\)](#)
- [証明書 \(P.1-14\)](#)
- [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 \(P.1-25\)](#)
- [セキュア クラスタへのサブスライバ ノードの追加 \(P.1-29\)](#)
- [その他の情報 \(P.1-30\)](#)

## 認証および暗号化に関する用語

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および暗号化を設定する場合に適用されます。

表 1-1 用語

用語	定義
アクセス コントロール リスト (ACL)	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。
認証	エンティティの ID 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 CallManager では、SUBSCRIBE 要求および一部のトランク側 SIP 要求を許可されたユーザに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。
Certificate Authority (CA; 認証局)	証明書を発行するエンティティ。シスコまたはサードパーティのエンティティなど。
Certificate Authority Proxy Function (CAPF)	サポートされたデバイスが Cisco Unified CallManager 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)	電話機が信頼する証明書のリストを含むファイル。CTL ファイルは、Cisco Site Administrator Security Token (セキュリティ トークン) によって署名されます。CTL ファイルは、Cisco CTL クライアントを使用してクラスタをセキュア / 混合モードに移行するときに自動的に作成されます。
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。
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。
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。
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 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。
暗号化	対象とする受信者だけが確実にデータを受信し読み取るようにするプロセス。情報の機密を確保し、データをランダムで無意味な暗号文に変換するプロセスです。暗号化アルゴリズムと暗号鍵が必要です。
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。
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。

表 1-1 用語（続き）

用語	定義
イメージ認証	電話機でロードする前にバイナリ イメージの改ざんを防止するプロセス。このプロセスによって電話機はイメージの整合性および発信元を検証します。
整合性	エンティティ間でデータの改ざんが行われていないことを確認するプロセス。
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。
Locally Significant Certificate (LSC; ローカルで有効な証明書)	電話機または JTAPI/TAPI/CTI アプリケーションにインストールされているデジタル X.509v3 証明書。発行元は、サードパーティの認証局または CAPF です。
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。
Man-in-the-Middle (中間者) 攻撃	Cisco Unified CallManager と電話機との間で流れる情報を、攻撃者が監視して変更できるプロセス。
メディア暗号化	暗号化手順を使用し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。
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。
メソッドリスト	許可プロセス中に、SIP トランクに着信す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 と呼ばれます。
混合モード	セキュリティを設定したクラスタ内のモード。Cisco Unified CallManager に接続する認証済みデバイスおよび非認証デバイスが含まれます。
ナンス	各ダイジェスト認証要求に対してサーバが生成する一意のランダム数値。
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。
PKI	Public Key Infrastructure (公開鍵インフラストラクチャ)。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。
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。
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。
Simple Certificate Enrollment Protocol (SCEP)	X.509 証明書を発行する証明書認証との通信に使用するプロトコル。
セキュア コール	すべてのデバイスが認証され、メディア ストリームが暗号化されているコール。
シグナリング認証	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するプロセス。Transport Layer Security プロトコルを使用します。

表 1-1 用語（続き）

用語	定義
シグナリング暗号化	デバイスと Cisco Unified CallManager 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。
SIP レルム	ダイジェスト認証で保護される空間を指定する文字列(名前)、SIP 要求用の回線またはトランク側のユーザエージェントを識別します。
SSL	インターネット上の電話メールなど、データ通信の安全を確保する暗号化プロトコル。SSL は、後継規格である TLS と同等のものです。
Transport Layer Security ( TLS )	インターネット上の電話メールなど、データ通信の安全を確保する暗号化プロトコル。TLS は SSL と同等の役割を果たします。
信頼リスト	デジタル署名なしの証明書リスト。
信頼ストア	Cisco Unified CallManager 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。
X.509	証明書の形式など、PKI 証明書をインポートするための ITU-T 暗号化規格。

## 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 CallManager リリース 5.1(3) は、このマニュアルに記載されている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（Cisco Unified CallManager サーバにログインするために）使用されるユーザ名とパスワードは、Cisco Unified CallManager の管理ページのユーザ名およびパスワード（Cisco Unified CallManager の管理ページにログインするために使用するユーザ名とパスワード）と同じです。
- Cisco Unified CallManager との TLS 接続を認証するため、LSC がすべての電話機に備わっている必要があります。Certificate Authority Proxy Function ( CAPF ) については、[P.6-4 の「CAPF システムの相互作用および要件」](#)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、Cisco Unified CallManager リリースをサポートする Cisco Unity 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 CallManager 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、サポートおよび設定されている機能に応じて SIP または SCCP コール中に Cisco Unified CallManager が実装できるセキュリティ機能の概要を示します。

表 1-2 コール処理セキュリティ機能の一覧

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  セキュア TLS ポート (SIP トランクのみ)
デバイス認証	Cisco Unified CallManager または CAPF あるいはその両方との 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	SIP 電話機ユーザのみ	SIP トランク ユーザおよび SIP トランク アプリケーション ユーザ
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 ]  TLS モード：認証または暗号化モード (SIP トランクのみ)
メディア暗号化	SRTP	SRTP (SIP トランク用の RTP)
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 タイプおよびプロトコルによって異なります。

## セキュリティ アイコン

セキュリティ アイコンをサポートする電話機は、コールに関連付けられている Cisco Unified CallManager セキュリティ レベルを表示します。

- 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 のデバイス間のセキュアな接続を示します。つまり、そのデバイスのシグナリングは認証または暗号化されています。
- 暗号化されたメディアによるコールの場合、つまり、暗号化されたシグナリングと暗号化されたメディアをデバイスで使用している場合は、電話機にロック アイコンが表示されます。

ポイントツーポイント コール、クラスタ内コール、クラスタ間コール、およびマルチホップ コールの場合は、コールのセキュリティ ステータスが変更ことがあります。SCCP 回線、SIP 回線、および H.323 シグナリングでは、関与するエンドポイントに、コール セキュリティ ステータスの変更が通知されます。コール パスに SIP トランクが含まれている場合、コール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、P.1-9 の「[セキュリティ アイコンと暗号化](#)」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.1-6)
- 制限 (P.1-7)
- ベスト プラクティス (P.1-11)
- デバイスのリセット、サービスの再起動、またはサーバおよびクラスタのリブート (P.1-11)
- メディア暗号化の設定と割り込み (P.1-12)

## 相互作用

ここでは、シスコのセキュリティ機能が Cisco Unified CallManager 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 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 CallManager 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 CallManager で SIP トランクのプレゼンス要求を受け付けるように許可する必要があります。また、必要な場合、Cisco Unified CallManager がリモート 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付けて認証するように、Cisco Unified CallManager の管理ページでエンド ユーザクライアントを設定します。

### SIP トランク

SIP 発信転送機能、および Web Transfer や Click to Dial 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 CallManager で着信アウトオブダイアログ REFER 要求を受け付けるように許可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 CallManager で未承諾 NOTIFY SIP 要求を受け付けるように許可する必要があります。

Cisco Unified CallManager 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 CallManager 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許可する必要があります。

### 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 クレデンシャルが変更されます。

### CTI

Cisco Unified CallManager Assistant は、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。管理者は、CAPF プロファイルを設定する必要があります (Cisco Unified CallManager Assistant ノードごとに 1 つ)。

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 CallManager TLS ポートを介して Cisco Unified CallManager 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、Cisco Unity TSP は Cisco Unified CallManager ポートを介して Cisco Unified CallManager 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 \(P.1-7\)](#)
- [割り込みと暗号化 \(P.1-8\)](#)
- [ワイドバンド コーデックと暗号化 \(P.1-8\)](#)
- [メディア リソースと暗号化 \(P.1-8\)](#)
- [電話機のサポートと暗号化 \(P.1-9\)](#)
- [電話機のサポートと暗号化設定ファイル \(P.1-9\)](#)
- [SIP トランクのサポートと暗号化 \(P.1-9\)](#)
- [セキュリティ アイコンと暗号化 \(P.1-9\)](#)
- [クラスタおよびデバイス セキュリティ モード \(P.1-10\)](#)
- [ダイジェスト認証と暗号化 \(P.1-10\)](#)
- [パケット キャプチャと暗号化 \(P.1-10\)](#)

## 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。

- クラスタを混合モードに設定すると、自動登録機能は動作しません。
- デバイス認証がクラスタに存在しない場合、つまり CTL Provider サービスを有効にしていないか Cisco CTL クライアントをインストールして設定していない場合、シグナリング暗号化およびメディア暗号化を実装できません。
- クラスタを混合モードに設定した場合、Cisco Unified CallManager 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。

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。

- 割り込みに使用する Cisco Unified IP Phone 7970 モデルに暗号化が設定されていない場合、Cisco Unified IP Phone 7960 モデル (SCCP) および 7970 モデルのユーザは暗号化されたコールに割り込むことができません。この場合、割り込みが失敗すると、割り込みを開始した電話機でビジー トーンが再生されます。

発信側の電話機に暗号化が設定されている場合、割り込みの発信側は暗号化された電話機からの認証済みコールまたは非セキュア コールに割り込むことができます。割り込みが発生した後、Cisco Unified CallManager はこのコールを非セキュアとして分類します。

発信側の電話機に暗号化が設定されている場合、割り込みの発信側は暗号化されたコールに割り込むことができ、コールの状態は暗号化済みであることが電話機に示されます。

割り込みに使用する電話機が非セキュアの場合でも、ユーザは認証済みコールに割り込むことができます。発信側の電話機でセキュリティがサポートされていない場合でも、そのコールで認証アイコンは引き続き認証済みデバイスに表示されます。



**ヒント** 割り込み機能が必要な場合には C 割り込みを設定できますが、コールは自動的に Cisco Unified CallManager によって非セキュアとして分類されます。

- Cisco Unified IP Phone 7960 および 7940 に暗号化機能を設定した場合、それらの暗号化済みのデバイスでは、暗号化されたコールに参加するときに割り込み要求を受け入れることができません。コールが暗号化されると、割り込みが失敗します。割り込みが失敗したことを示すトーンが電話機で再生されます。

次の設定を試みると、Cisco Unified CallManager の管理ページにメッセージが表示されます。

- [ 電話の設定 ( Phone Configuration ) ] ウィンドウで、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、[ ビルトインブリッジ ( Built In Bridge ) ] 設定に [ On ] を選択し ( デフォルト設定は [ On ] )、さらにこの特定の設定の作成後に [ 保存 ] をクリックする。
- [ サービスパラメータ設定 ( Service Parameter Configuration ) ] ウィンドウで、Built In Bridge Enable パラメータを更新する。

## 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 7960 または 7940 に適用されます。これは、TLS/SRTP 用に設定された Cisco Unified IP Phone 7960 または 7940 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 CallManager 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 CallManager 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 CallManager 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、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。たとえば次の場合に、Cisco Unified CallManager リリース 5.1 はメディア暗号化を提供しません。

- トランスコーダまたはメディア ターミネーション ポイントに関連するコール

- Ad hoc 会議または Meet Me 会議
- 保留音に関連するコール

## 電話機のサポートと暗号化

Cisco Unified IP Phone 7912 など、一部の Cisco Unified IP Phone は、暗号化された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。詳細については、暗号化をサポートする Cisco Unified IP Phone とこのバージョンの Cisco Unified CallManager 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。



(注)

このリリースでは、暗号化をサポートする Cisco Unified IP Phone (SCCP のみ) は、7906、7911、7940、7941、7941G-GE、7960、7961、7961G-GE、7970、7971 です。暗号化をサポートする Cisco Unified IP Phone (SIP のみ) は、7906、7911、7941、7941G-GE、7961、7961G-GE、7970、7971 です。

Cisco Unified IP Phone 7940/7960 (SIP のみ) モデルは、TLS でのシグナリング暗号化をサポートしません。

## 電話機のサポートと暗号化設定ファイル

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。暗号化された設定ファイルをサポートするすべての電話機は、完全に暗号化された設定ファイルを受信するために、このリリースと互換性のある新しいファームウェアを必要とします (Cisco Unified IP Phone 7905 および 7912 以外)。Cisco Unified IP Phone 7905 および 7912 は、既存のセキュリティ機構を使用し、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、[P.7-5](#) の「サポートされる電話機のモデル」を参照してください。

## SIP トランクのサポートと暗号化

Cisco Unified CallManager は主に、IOS ゲートウェイおよびゲートキーパー制御および非ゲートキーパー制御トランクの Cisco Unified CallManager H.323 トランク用に、SRTP をサポートします。SRTP がコールを保証できない場合は、Cisco Unified CallManager が RTP を保証します。

SIP トランクは SRTP 暗号化をサポートしません。Cisco Unified CallManager は、TLS で SIP トランク上のコールを保護します。

## 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。

- 電話会議、コールの転送、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 などの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 CallManager は、SIP トランク側接続で開始または終了するコールに対してはロック アイコンを表示しません。
- Cisco Unified CallManager は、H.323 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。
- コールに PSTN が関わっている場合、セキュリティ アイコンで示されるのは、そのコールの IP ドメイン部分のセキュリティ ステータスだけです。

## クラスタおよびデバイス セキュリティ モード

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、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になります。このような場合は、Cisco Unified CallManager の管理ページでデバイス 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、電話機は SRST 対応ゲートウェイおよび Cisco Unified CallManager と非セキュア接続を確立します。[ SRST Allowed ] チェックボックスなど、デバイス セキュリティ モード以外のセキュリティ関連の設定も無視されます。Cisco Unified CallManager の管理ページ内のセキュリティ設定は削除されませんが、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 [ SRTP を許可( SRTP Allowed ) ] チェックボックスがオンになっている、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 CallManager 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 CallManager の間 ( 発信コール レッグ ) で、もう 1 つは Cisco Unified CallManager 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 CallManager の管理ページの設定を変更して、パケットのキャプチャを開始できます ( デバイスがパケット キャプチャをサポートする場合 )。

Cisco Unified CallManager でのパケット キャプチャの設定については、このリリースの『Cisco Unified CallManager トラブルシューティングガイド』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する。
- ゲートウェイ、および Cisco Unity、Cisco Unified Contact Center、またはその他の Cisco Unified CallManager サーバなど、リモートロケーションのその他のアプリケーションサーバには、IPSec を使用する。



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 CallManager 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する。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。この作業を実行する方法については、『Cisco Unified CallManager 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、またはサーバおよびクラスタのリポート \(P.1-11\)](#)
- [メディア暗号化の設定と割り込み \(P.1-12\)](#)

## デバイスのリセット、サービスの再起動、またはサーバおよびクラスタのリポート

ここでは、デバイスのリセットが必要な場合、Cisco Unified CallManager Serviceability でサービスの再起動が必要な場合、またはサーバおよびクラスタをリポートす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 CallManager の管理ページで、異なるセキュリティプロファイルを適用した後は、単一デバイスをリセットする。
- 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する。
- クラスタ全体の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する。
- 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する。
- 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する。
- TLS 接続用のポートを更新した後は、Cisco CTL Provider サービスを再起動する。
- クラスタ全体の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 サービスを再起動する。
- 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する。
- 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 CallManager Serviceability で Cisco CallManager および Cisco TFTP サービスをすべて再起動する。この作業は、これらのサービスが稼働する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、すべての Cisco CallManager および Cisco TFTP サービスを再起動する。
- SRST リファレンスのセキュリティ設定後は、従属デバイスをリセットする。
- 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 をリポートする。

- 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 CallManager IP Manager Assistant サービス、Cisco WebDialer Web サービス、および Cisco Extended Functions サービスを再起動する。

Cisco CallManager サービスを再起動するには、『Cisco Unified CallManager Serviceability アドミニストレーションガイド』を参照してください。

設定の更新後に単一のデバイスをリセットするには、P.5-12の「電話機セキュリティ プロファイルの適用」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 CallManager の管理ページで [システム] > [Cisco Unified CallManager] の順に選択します。

[Cisco Unified CallManager の検索と一覧表示 (Find and List Cisco Unified CallManagers)] ウィンドウが表示されます。

**ステップ 2** [検索] をクリックします。

設定済みの Cisco Unified CallManager 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 CallManager を選択します。

**ステップ 4** [リセット] 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

P.1-8の「割り込みと暗号化」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 7960 および 7940 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 Phones 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 CallManager の管理ページで次の作業を実行したときです。

- [電話の設定 (Phone Configuration)] ウィンドウで、[デバイスセキュリティモード (Device Security Mode)] に [Encrypted] を選択し (システム デフォルトは [Encrypted])、[ビルトインブリッジ (Built In Bridge)] 設定に [On] を選択し (デフォルト設定は [On])、さらにこの特定の設定の作成後に [保存] をクリックする。
- [エンタープライズパラメータ設定 (Enterprise Parameters Configuration)] ウィンドウで、Device 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、Built In Bridge Enable パラメータを更新する。



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 CallManager 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 CallManager 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 CallManager は Cisco Unified CallManager 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 CallManager 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、送信を扱います。Cisco Unified CallManager は、次のセキュア転送プロトコルを提供します。

- Transport Layer Security ( TLS ) は、セキュア ポートと証明書交換を使用して、2 つのシステムまたはデバイス間で、セキュアで信頼性の高いデータ転送を提供します。TLS は、Cisco Unified CallManager 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 CallManager は TLS を使用して、SCCP 電話機への SCCP コール、および SIP 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 ) は、Cisco Unified CallManager とゲートウェイの間で、セキュアで信頼性の高いデータ転送を提供します。IPSec は、Cisco IOS MGCP および H.323 ゲートウェイへのシグナリング認証および暗号化を実装します。

セキュア RTP ( SRTP ) 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て、Cisco Unified IP Phone で発信または着信する音声会話および TDM またはアナログ音声ゲートウェイ ポートを音声ドメインにアクセスする盗聴者から保護します。SRTP は、リプレイ アタックからの保護を追加します。

## 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、デバイスやアプリケーション ユーザなど、ユーザとホストとの間の接続を保護します。

管理者は Cisco Unified Communications オペレーティング システム 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。

Cisco Unified CallManager の信頼ストアの更新および証明書の管理の詳細については、『Cisco Unified Communications Operating System アドミニストレーション ガイド』を参照してください。



(注)

Cisco Unified CallManager 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 \(P.1-14\)](#)
- [サーバの証明書の種類 \(P.1-15\)](#)
- [外部 CA からの証明書のサポート \(P.1-16\)](#)

## 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 のインストールのために、Cisco Certificate Authority Proxy Function ( CAPF ) を認証します。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。設定タスクについては、[P.1-25 の「設定用チェックリストの概要」](#)を参照してください。デバイス セキュリティ モードで認証または暗号化を設定すると、LSC によって Cisco Unified CallManager と電話機との間の接続が保護されます。



ヒント

製造元でインストールされる証明書 ( MIC ) は、LSC のインストールのためだけに使用することをお勧めします。シスコは、Cisco Unified CallManager との TLS 接続を認証するための LSC をサポートしています。MIC ルート証明書は侵害されている可能性があるため、お客様が TLS 認証やその他の目的で MIC を使用するように電話機を設定する場合は、自らの責任で行う必要があります。MIC が侵害されている場合、シスコは一切の責任を負いません。

Cisco Unified IP Phone 7906、7911、7941、7961、7970、および 7971 をアップグレードして Cisco Unified CallManager への TLS 接続に LSC を使用できるようにし、互換性の問題が後で発生するのを避けるため MIC ルート証明書を CallManager 信頼ストアから削除することをお勧めします。Cisco Unified CallManager への TLS 接続に MIC を使用する電話機の中には、登録できないものもあります。

管理者は、MIC ルート証明書を CallManager 信頼ストアから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 信頼ストア内にある MIC ルート証明書は、証明書の更新に使用されます。Cisco Unified CallManager 信頼ストアの更新の詳細については、『Cisco Unified Communications Operating System アドミニストレーションガイド』を参照してください。

## サーバの証明書の種類

Cisco Unified CallManager 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\_cert) : この自己署名ルート証明書は、Cisco Unified CallManager 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 Unified CallManager ノード証明書 : この自己署名ルート証明書は、Cisco Unified CallManager 5.1 をインストールすると、Cisco Unified CallManager サーバに自動的にインストールされます。Cisco Unified CallManager 証明書によって、サーバの識別情報が提供されます。この情報には、Cisco Unified CallManager サーバ名と Global Unique Identifier (GUID) が含まれます。
- CAPF 証明書 : このルート証明書は、Cisco CTL クライアントの設定が完了した後で、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 CallManager のインストール中に、MGCP および H.323 ゲートウェイまたはその他の外部マシンとの 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 CallManager の管理ページのセキュア SRST 参照を設定するときに、Cisco Unified CallManager 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 CallManager 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。この証明書はデータベースに格納されるため、証明書管理ツールには統合されません。

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

- Cisco Unity サーバ証明書 : Cisco Unity は、この自己署名証明書を使用して、Cisco Unity SCCP デバイス証明書に署名します。Cisco Unity Telephony Integration Manager がこの証明書を管理します。
- Cisco Unity SCCP デバイス証明書 : Cisco Unity SCCP デバイスは、この署名証明書を使用して、Cisco Unified CallManager との TLS 接続を確立します。すべての Unity デバイス (またはポート) が、Unity ルート証明書をルートとする証明書を発行します。Unity 証明書名は、Unity マシン名に基づく証明書の件名のハッシュです。すべてのデバイス (またはポート) が、Unity ルート証明書をルートとする証明書を発行します。
- LDAP 社内ディレクトリ証明書 (directory-trust) : Cisco Unified CallManager は、この署名付き証明書を使用して、ディレクトリ同期および LDAP 認証のため LDAP over SSL をサポートします。directory-trust 証明書は、社内ディレクトリ (Active Directory または Netscape Directory) から Cisco Unified CallManager 信頼ストアに追加されます。信頼された証明書をアップロードした後、Cisco Tomcat サービスと Cisco DirSync サービスを再起動する必要があります。
- SIP Proxy サーバ証明書 : Cisco Unified 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 CallManager 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 CallManager に対して認証されます。

証明書管理ツールの GUI を使用して CallManager に証明書をアップロードする方法は、『Cisco Unified Communications Operating System アドミニストレーションガイド』を参照してください。

## 外部 CA からの証明書のサポート

Cisco Unified CallManager 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 Certificate Manager 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、CallManager と CAPF の両方の証明書を発行する必要があります。



(注) このリリースの Cisco Unified CallManager は、SCEP インターフェイスをサポートしていません。

シスコは、Keon および Microsoft の CA で PKCS#10 CSR サポート メカニズムを検証済みです。ただし、PKCS#10 CSR をサポートする他の外部 CA による証明書の発行は検証していません。

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 クライアントの実行後、該当するサービスを更新のため再起動します。たとえば、Cisco Unified CallManager 証明書の更新では Cisco Unified CallManager および Cisco TFTP、CAPF 証明書の更新では CAPF を再起動します。更新の手順については、P.3-11 の「Cisco CTL クライアントの設定」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) の生成については、『Cisco Unified Communications Operating System アドミニストレーションガイド』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 CallManager 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.1-17）](#)
- [デバイス認証（P.1-17）](#)
- [ファイル認証（P.1-18）](#)
- [シグナリング認証（P.1-18）](#)
- [ダイジェスト認証（P.1-18）](#)
- [許可（P.1-20）](#)

### イメージ認証

このプロセスは、バイナリ イメージ（つまり、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 CallManager 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、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、[P.4-3 の「サポートされる電話機のモデル」](#)を参照してください。

デバイス認証は、Cisco Unified CallManager 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は、相互認証と呼ばれます。

デバイス認証は、[P.3-1 の「Cisco CTL クライアントの設定」](#)で説明する Cisco CTL ファイルの作成（Cisco Unified CallManager 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 [P.6-1 の「Certificate Authority Proxy Function の使用方法」](#)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

Cisco Unified 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 CallManager 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 CallManager に対して認証されます。Cisco Unified CallManager 信頼ストアの更新の詳細については、『[Cisco Unified Communications Operating System アドミニストレーション ガイド](#)』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、P.4-3 の「サポートされる電話機のモデル」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、管理者が Cisco Unified CallManager の管理ページで、影響を受けた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、ファイルのシグニチャを確認して、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、次の基準が満たされることを確認します。

- 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 CallManager 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、P.3-1 の「Cisco CTL クライアントの設定」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、P.3-1 の「Cisco CTL クライアントの設定」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 CallManager は、SIP ユーザ エージェント (UA) が Cisco Unified CallManager に要求を送信したときに、UA の ID でチャレンジができます (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)。

Cisco Unified CallManager 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 CallManager は主に、SCCP および SIP エンドポイントを接続するバックツーバック ユーザ エージェントとして機能します。

Cisco Unified CallManager は、SIP トランク経由で接続する SIP 電話機または SIP デバイスで (UAS として) チャレンジを行うことができます。また、SIP トランク インターフェイスで受信したチャレンジに (UAC として) 応答できます。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 CallManager は、キープアライブ メッセージ以外のすべての SIP 電話機要求でチャレンジを行います。

**(注)**

Cisco Unified CallManager は、回線側の電話機からのチャレンジには応答しません。

Cisco Unified CallManager 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 UA と Cisco Unified CallManager の間 (発信コール レッグ) で、もう 1 つは Cisco Unified CallManager と宛先 SIP UA 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。

**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。

Cisco Unified CallManager サーバは、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てチャレンジを開始します (ナンスは、MD5 ハッシュの計算に使用するランダム数を指定します)。SIP ユーザ エージェントが Cisco Unified CallManager の ID でチャレンジを行うとき、Cisco Unified CallManager は SIP 401 および SIP 407 (Proxy Authentication Required) メッセージに応答します。

SIP 電話機またはトランクのダイジェスト認証を有効にして、ダイジェスト クレデンシャルを設定した後、Cisco Unified CallManager は、ユーザ名、パスワード、およびレルムのハッシュを含むクレデンシャル チェックサムを計算します。Cisco Unified CallManager 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。各ダイジェスト ユーザは、レルムごとにダイジェスト クレデンシャルのセットを 1 つ持つことができます。

**ヒント**

SIP 電話機は、Cisco Unified CallManager レルムの中のみ存在できます。SIP トランクの場合、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。

Cisco Unified CallManager がユーザ エージェントでチャレンジを行うとき、Cisco Unified CallManager は、ユーザ エージェントがクレデンシャルを表す必要のあるレルムとナンスの値を示します。応答を受信した後、Cisco Unified CallManager 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、UA からの応答ヘッダーで受信したクレデンシャルを比較して検証します。クレデンシャルが一致した場合、ダイジェスト認証は成功し、Cisco Unified CallManager は SIP 要求を処理します。

SIP トランク経由で接続しているユーザ エージェントからのチャレンジに回答するとき、Cisco Unified CallManager は、チャレンジ メッセージ ヘッダーで指定されているレルムに設定されている Cisco Unified CallManager ユーザ名およびパスワードで回答します。Cisco Unified CallManager がチャレンジを受ける場合、Cisco Unified CallManager は、チャレンジ メッセージで指定されているレルムに基づいてユーザ名をロックアップし、パスワードを暗号化します。Cisco Unified CallManager は、パスワードを復号化し、ダイジェストを計算し、応答メッセージで表します。

管理者は、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 クレデンシャルを設定します。アプリケーションの場合は、Cisco Unified CallManager の管理ページの [ 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 (Digest Credentials) ] を指定します。SIP 電話機の場合は、Cisco Unified CallManager の管理ページの [ 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 (Digest Credentials) ] を指定し、電話機に適用します。

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。

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 クレデンシャル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 クレデンシャルを設定した場合、ダイジェスト クレデンシャルは電話機に送信されますが、Cisco Unified CallManager でもチャレンジが開始されます。

管理者は、電話機に対するチャレンジ用、および SIP トランク経由で受信するチャレンジ用の SIP レルムを設定します。SIP レルム GUI は、UAC モードのトランク側クレデンシャルを提供します。電話機の SIP レルムは、サービス パラメータ SIP Station Realm で設定します。SIP レルムとユーザ名およびパスワードは、Cisco Unified CallManager 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 CallManager の管理ページで設定する必要があります。

管理者は、外部デバイスに対してナンス値が有効な時間を分単位で設定します。この時間を超えると、Cisco Unified CallManager はナンス値を拒否し、新しい番号を生成します。

## 許可

Cisco Unified CallManager は、許可プロセスを使用して、SIP 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 電話機の場合、Cisco Unified CallManager 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 CallManager 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 CallManager 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 (アウトオブダイアログ REFER、未承諾 NOTIFY、REPLACE 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、関連する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 アプリケーションへ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、まず SIP トランクの許可が行われ、それから SIP アプリケーション ユーザの許可が行われます。トランクの場合、Cisco Unified CallManager はトランク 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 CallManager 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 CallManager 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 CallManager 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 CallManager 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 CallManager 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、[ 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

暗号化は、Cisco Unified CallManager 5.1 をクラスタ内の各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。

Cisco Unified CallManager では、次の種類の暗号化をサポートします。

- シグナリング暗号化 (P.1-22)
- メディア暗号化 (P.1-22)
- 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 CallManager 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 CallManager 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 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。



(注)

Cisco Unified CallManager 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 電話機はすべて、Cisco Unified CallManager 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 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 CallManager 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、IPSec で保護された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、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。

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、H.323/H.245/H.225 トランク、および SIP トランクでセキュリティ関連情報が暗号化されずに送信されないようにするには、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 CallManager は、IPSec が正しく設定されていることを確認しません。IPSec を正しく設定しないと、セキュリティ関連情報が公開される可能性があります。

セキュア SIP トランクは、TLS 経由のセキュア コールをサポートできます。ただし、シグナリング暗号化はサポートされますが、メディア暗号化 (SRTP) はサポートされません。トランクがメディア暗号化をサポートしないため、コールのすべてのデバイスが認証またはシグナリング暗号化をサポートしている場合、通話中に電話機にシールド アイコンが表示されます。

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 CallManager 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 CallManager 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 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 CallManager に送信します。

## 設定ファイルの暗号化

Cisco Unified CallManager 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 クレデンシャルや管理者パスワードなど）を電話機に送出します。

Cisco Unified CallManager 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（P.7-5 の「サポートされる電話機のモデル」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である場合、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）、機密データを電話機にクリアでダウンロードすることを選択することもできます。

Cisco Unified CallManager 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 CallManager 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 CallManager および電話機で一意的対称キーを設定する必要があります。

Cisco Unified CallManager の管理ページの [ 電話セキュリティプロファイル ] 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、[第7章「電話機設定ファイルの暗号化について」](#)を参照してください。

## 設定用チェックリストの概要

表 1-3 に、認証および暗号化を実装するために必要な作業を示します。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があります。

- 新規インストールに対して認証および暗号化を実装するには、表 1-3 を参照してください。
- セキュア クラスタにサブスライバ ノードを追加するには、P.1-29 の「セキュア クラスタへのサブスライバ ノードの追加」を参照してください。

表 1-3 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
<p><b>ステップ 1</b> クラスタにある各サーバの Cisco Unified CallManager Serviceability で Cisco CTL Provider サービスをアクティブにします。</p> <p> <b>ヒント</b> Cisco Unified CallManager 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。</p>	Cisco CTL Provider サービスのアクティブ化 (P.3-5)
<p><b>ステップ 2</b> 最初のノードの Cisco Unified CallManager Serviceability 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。</p> <p> <b>ワンポイントアドバイス</b> 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。</p>	Certificate Authority Proxy Function サービスのアクティブ化 (P.6-6)
<p><b>ステップ 3</b> 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。</p> <p> <b>ヒント</b> これらの設定を Cisco Unified CallManager 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。</p>	TLS 接続用ポートの設定 (P.3-6)
<p><b>ステップ 4</b> 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。</p>	Cisco CTL クライアントの設定 (P.3-11)
<p><b>ステップ 5</b> Cisco CTL クライアントをインストールします。</p> <p> <b>ヒント</b> Cisco Unified CallManager 5.1(3) 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 Unified CallManager の管理機能 5.1(3) で使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。</p>	<ul style="list-style-type: none"> <li>• システム要件 (P.1-4)</li> <li>• インストール (P.1-13)</li> <li>• Cisco CTL クライアントのインストール (P.3-8)</li> <li>• 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.3-10)</li> </ul>

表 1-3 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
<b>ステップ 6</b>	<p>Cisco CTL クライアントを設定します。</p> <p> <b>ヒント</b> Cisco Unified CallManager 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。Cisco Unified CallManager 5.1(3) 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 5.1(3) 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。</p>	<ul style="list-style-type: none"> <li>• <a href="#">Cisco CTL クライアントの設定 ( P.3-11 )</a></li> <li>• <a href="#">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.3-10 )</a></li> </ul>
<b>ステップ 7</b>	<p>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。</p> <ul style="list-style-type: none"> <li>• デバイス セキュリティ モードを設定します( SCCP 電話機および SIP 電話機の場合 )。</li> </ul> <p>デバイス セキュリティ モードは、Cisco Unified CallManager のアップグレード時に自動的に移行されます。Cisco Unified CallManager 4.0 で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。</p> <ul style="list-style-type: none"> <li>• CAPF 設定を定義します ( 一部の SCCP 電話機および SIP 電話機の場合 )。</li> </ul> <p>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。</p> <ul style="list-style-type: none"> <li>• SIP 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。</li> <li>• 暗号化された設定ファイルを有効にするには ( 一部の SCCP 電話機および SIP 電話機 )、[ TFTP 暗号化 ( TFTP Encrypted Config ) ] チェックボックスをオンにします。</li> <li>• 設定ファイルのダウンロードでダイジェストクレデンシャルを除外するには、[ 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。</li> </ul>	<p><a href="#">電話機セキュリティ プロファイルの設定 ( P.5-1 )</a></p> <p><a href="#">電話機セキュリティ プロファイルの設定のヒント ( P.5-2 )</a></p> <p><a href="#">暗号化された電話機設定ファイルの設定 ( P.7-1 )</a></p> <p><a href="#">暗号化された設定ファイルの設定のヒント ( P.7-6 )</a></p>
<b>ステップ 8</b>	<p>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。</p>	<p><a href="#">電話機セキュリティ プロファイルの適用 ( P.5-12 )</a></p>

表 1-3 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
<p><b>ステップ 9</b> 電話機に証明書を発行するように CAPF を設定します。</p> <p>Cisco Unified CallManager 5.1 へのアップグレード前に証明書の操作を実行して CAPF をサブスクリバ サーバで実行した場合、CAPF データを 4.0 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 Cisco Unified CallManager 5.1 にアップグレードする必要があります。</p> <p> <b>注意</b> Cisco Unified CallManager 4.0 サブスクリバ サーバの CAPF データは Cisco Unified CallManager 5.1 データベースに移行されません。したがって、データを 5.1 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 1.0(1) 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、CAPF 5.1 は証明書を再発行する必要があります。</p>	<ul style="list-style-type: none"> <li>システム要件 ( P.1-4 )</li> <li>CAPF の設定用チェックリスト ( P.6-5 )</li> </ul>
<p><b>ステップ 10</b> ローカルで有効な証明書が、サポートされている Cisco Unified IP Phone にインストールされたことを確認します。</p>	<ul style="list-style-type: none"> <li>システム要件 ( P.1-4 )</li> <li>電話機での認証文字列の入力 ( P.6-12 )</li> </ul>
<p><b>ステップ 11</b> SIP 電話機のダイジェスト認証を設定します。</p>	SIP 電話機のダイジェスト認証の設定 ( P.8-1 )
<p><b>ステップ 12</b> 電話機のセキュリティ強化作業を実行します。</p> <p> <b>ヒント</b> 電話機のセキュリティ強化設定を Cisco Unified CallManager 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。</p>	電話機のセキュリティ強化 ( P.9-1 )
<p><b>ステップ 13</b> セキュリティ用のボイスメール ポートを設定します。</p>	<ul style="list-style-type: none"> <li>ボイスメール ポートのセキュリティ設定 ( P.10-1 )</li> <li>Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity 4.x</li> </ul>
<p><b>ステップ 14</b> SRST リファレンスのセキュリティを設定します。</p> <p> <b>ヒント</b> 前のリリースの Cisco Unified CallManager でセキュア SRST リファレンスを設定した場合は、Cisco Unified CallManager 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。</p>	Survivable Remote Site Telephony( SRST )リファレンスのセキュリティ設定 ( P.12-1 )

表 1-3 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 15	IPSec を設定します。	<ul style="list-style-type: none"> <li>ゲートウェイおよびトランクの暗号化の設定 (P.13-1)</li> <li>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.13-6)</li> <li><i>Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways</i></li> <li><i>Cisco Unified Communications Operating System アドミニストレーション ガイド</i></li> </ul>
ステップ 16	<p>SIP トランク セキュリティ プロファイルを設定します。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>	<ul style="list-style-type: none"> <li>SIP トランク セキュリティ プロファイルの設定 (P.14-4)</li> <li>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.15-2)</li> </ul>
ステップ 17	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.14-10)
ステップ 18	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.15-1)
ステップ 19	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。	<ul style="list-style-type: none"> <li>SIP トランク セキュリティ プロファイルの設定 (P.14-4)</li> <li>『<i>Cisco Unified CallManager アドミニストレーション ガイド</i>』のアプリケーションユーザの許可の箇所も参照</li> </ul>
ステップ 20	クラスタ内の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、またはサーバおよびクラスタのリポート (P.1-11)
ステップ 21	クラスタ内のすべてのサーバをリポートします。	デバイスのリセット、サービスの再起動、またはサーバおよびクラスタのリポート (P.1-11)

## セキュア クラスタへのサブスクリバ ノードの追加

クラスタがすでにセキュアになっている場合は、次の手順を実行して、新規サブスクリバ ノードをセキュア クラスタに追加します(この手順は、ノードが正常に追加されていることを想定しています)。

### 手順

- 
- ステップ 1** 新規ノードで Cisco CTL Provider サービスをアクティブにします。
  - ステップ 2** 既存の CTL ファイルの etoken を使用し、CTL クライアントを再実行してクラスタ内のすべてのサーバから証明書を取得し、CTL ファイルに格納します。証明書を生成して CTL ファイルを更新するには、クラスタ内のすべてのサーバで Cisco CTL Provider を実行する必要があります。
  - ステップ 3** すべての TFTP サーバで Tftp サービスを再起動します。
  - ステップ 4** すべてのノードで Cisco CallManager サービスを再起動します。
  - ステップ 5** すべてのデバイスをリセットして、新規 CTL ファイルをデバイスに配布します。
- 

クラスタへのノードの追加の詳細は、『Cisco Unified CallManager アドミニストレーション ガイド』の「サーバの設定」を参照してください。

## その他の情報

### 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 アドミニストレーション ガイド for Cisco Unified CallManager*
- *Cisco Unified Communications Operating System アドミニストレーション ガイド*
- *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*
- *Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity 4.x*
- 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
- *Cisco IP Telephony Disaster Recovery Framework Administration Guide*
- *Cisco Unified CallManager アドミニストレーション ガイド*
- *Cisco Unified CallManager トラブルシューティング ガイド*
- 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



## 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 \( P.2-2 \)](#)
- [Internet Explorer による HTTPS の使用方法 \( P.2-3 \)](#)
- [Internet Explorer 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 \( P.2-3 \)](#)
- [証明書の詳細表示 \( P.2-4 \)](#)
- [証明書のファイルへのコピー \( P.2-5 \)](#)
- [Netscape 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 \( P.2-7 \)](#)
- [その他の情報 \( P.2-8 \)](#)

## HTTPS の概要

Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS; HTTP over SSL) は、ブラウザクライアントと tomcat サーバとの間の通信を保護し、証明書および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を暗号化します。また、HTTPS によってユーザのログインパスワードも Web で安全に転送されるようになります。サーバの識別情報を保護する HTTPS をサポートする Cisco Unified CallManager アプリケーションには、Cisco Unified CallManager の管理機能、Cisco Unified CallManager Serviceability、Cisco Unified IP Phone ユーザ オプション ページ、TAPS、Cisco Unified CallManager CDR Analysis and Reporting (CAR)、Cisco Unified Dialed Number Analyzer、Cisco Unified CallManager Real Time Monitoring Tool があります。

Cisco Unified CallManager 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\_cert) がプラットフォームで生成されます。自己署名証明書は、アップグレード中に移行されます。.DER 形式および .PEM 形式で、証明書のコピーが作成されます。表 2-1 に、Cisco Unified CallManager 内の、HTTPS を使用するアプリケーションを示します。

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

Cisco Unified CallManager の HTTPS アプリケーション	Web アプリケーション
CMAdmin	Cisco Unified CallManager の管理機能
CMService	Cisco Unified CallManager Serviceability
CMUser	Cisco Personal Communications Assistant
AST	Cisco Unified CallManager Real-Time Monitoring Tool
RTMTReports	Cisco Unified CallManager 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 CallManager CDR Analysis and Reporting
TAPS	Tool for Auto-Registration Phone Support (TAPS)
dna	Dialed Number Analyzer
drf	障害復旧システム
SOAP	Cisco Unified CallManager 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
	 <p><b>(注)</b> 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。SOAP アプリケーションでは、HTTP はサポートされていません。HTTP を使用する既存のアプリケーションは失敗します。ディレクトリを変更することによって、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。</p>



(注)

ホスト名を使用して Web アプリケーションにアクセスし、信頼できるフォルダに証明書をインストールした後、ローカルホストか IP アドレスを使用してそのアプリケーションへのアクセスを試みた場合、セキュリティ証明書の名前が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] ダイアログボックスが表示されます。

URL にローカルホスト、IP アドレス、またはホスト名を使用して HTTPS をサポートするアプリケーションにアクセスする場合、URL の種類別 (ローカルホスト、IP アドレスなど) の信頼できるフォルダに証明書を保存する必要があります。保存しないと、[セキュリティの警告] ダイアログボックスはそれぞれの種類について表示されます。

## Internet Explorer による HTTPS の使用方法

この項では、Internet Explorer での HTTPS の使用に関連した次のトピックについて取り上げます。

- [Internet Explorer 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 \(P.2-3\)](#)
- [証明書の詳細表示 \(P.2-4\)](#)
- [証明書のファイルへのコピー \(P.2-5\)](#)

Cisco Unified CallManager 5.1 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 CallManager の管理ページまたは他の Cisco Unified CallManager 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ついてだけ証明書を信頼する場合、[セキュリティの警告] ダイアログボックスはアプリケーションにアクセスするたびに表示されます。つまり、証明書を信頼できるフォルダにインストールしない限り、ダイアログボックスは表示されます。
- [証明書の表示] > [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 [証明書の表示] > [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。

## Internet Explorer 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信頼できるフォルダに HTTPS 証明書を保存して、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ないようにするには、次の手順を実行します。

### 手順

**ステップ 1** tomcat サーバのアプリケーション (Cisco Unified CallManager の管理ページなど) を参照します。

**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、[証明書の表示] をクリックします。

- 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。
- ステップ9** [セキュリティ警告] ボックスに証明書のサムプリントが表示されます。
- [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] をクリックして続行します。



**(注)** URL にローカルホスト、IP アドレス、またはホスト名を使用して HTTPS をサポートするアプリケーションにアクセスする場合、URL の種類別 (ローカルホスト、IP アドレスなど) の信頼できるフォルダに証明書を保存する必要があります。保存しないと、[セキュリティの警告] ダイアログボックスはそれぞれの種類について表示されます。



**ヒント** [証明書] ペインの [証明書のパス] 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。

#### 追加情報

詳細については、[P.2-8](#) の「[関連項目](#)」を参照してください。

## 証明書の詳細表示

[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、[証明書の表示] ボタンをクリックし、[詳細設定] タブをクリックして、証明書の詳細を表示します。



**ヒント** このペインの設定に表示されているデータは一切変更できません。

次の証明書設定が表示されます。

- 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
- 公開キー
- サブジェクト キー識別子
- キー使用法
- 拡張キー使用法
- 拇印アルゴリズム
- 拇印

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 [詳細設定] 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。



(注)

自己署名証明書は、Cisco Unified Communications オペレーティング システムの管理ページの GUI で再生成できます。

## 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、[証明書の表示] をクリックします。

**ステップ 2** [詳細設定] 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 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 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。[ 完了 ] 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

詳細については、P.2-8 の「[関連項目](#)」を参照してください。

## Netscape による HTTPS の使用方法

この項では、Netscape での HTTPS の使用について取り上げます。

Netscape で HTTPS を使用する場合、証明書のクレデンシャルを表示する、あるセッションで証明書を信頼する、証明書を期限切れまで信頼する、あるいは証明書をまったく信頼しない、という作業が行えます。

Netscape には、証明書をファイルにコピーするための証明書エクスポートユーティリティがありません。



#### ヒント

あるセッションだけで証明書を信頼する場合、HTTPS をサポートするアプリケーションにアクセスするたびに「[Netscape 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](#)」の手順を繰り返す必要があります。証明書を信頼しない場合は、アプリケーションにアクセスできません。

## Netscape 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

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** Cisco Unified CallManager の管理ページなどのアプリケーションに Netscape でアクセスします。

証明書認証のダイアログボックスが表示されます。

**ステップ 2** 次のオプション ボタンのいずれか 1 つをクリックします。

- [ この証明書のこのセッションのために一時的に受け入れる ]
- [ この証明書を受け入れない / この Web サイトに接続しない ]
- [ この証明書を永続的に受け入れる ]



**(注)** [ この証明書を受け入れない / この Web サイトに接続しない ] を選択すると、アプリケーションは表示されません。



**(注)** 続行する前に証明書のクレデンシャルを表示するには、[ 証明書を調査 ] をクリックします。クレデンシャルを確認し、[ 閉じる ] をクリックします。

**ステップ 3** [ OK ] をクリックします。

[ セキュリティに関する報告 ] ダイアログボックスが表示されます。

**ステップ 4** [ OK ] をクリックします。



**(注)** 自己署名証明書は、Cisco Unified Communications オペレーティング システムの管理ページの GUI で再生成できます。

### 追加情報

詳細については、[P.2-8 の「関連項目」](#)を参照してください。

## その他の情報

### 関連項目

[証明書 \(P.1-14\)](#)

### シスコの関連マニュアル

- *Cisco Unified CallManager Serviceability* アドミニストレーション ガイド
- *Cisco Unified Communications Operating System* アドミニストレーション ガイド
- *Cisco Unified CallManager* 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



## 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 \(P.3-2\)](#)
- [Cisco CTL クライアントの設定のヒント \(P.3-3\)](#)
- [Cisco CTL クライアントの設定用チェックリスト \(P.3-4\)](#)
- [Cisco CTL Provider サービスのアクティブ化 \(P.3-5\)](#)
- [Cisco CAPF サービスのアクティブ化 \(P.3-6\)](#)
- [TLS 接続用ポートの設定 \(P.3-6\)](#)
- [Cisco CTL クライアントのインストール \(P.3-8\)](#)
- [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 \(P.3-10\)](#)
- [Cisco CTL クライアントの設定 \(P.3-11\)](#)
- [CTL ファイルの更新 \(P.3-15\)](#)
- [CTL ファイル エントリの削除 \(P.3-17\)](#)
- [クラスタ全体のセキュリティ モードの更新 \(P.3-17\)](#)
- [Cisco CTL クライアントの設定内容 \(P.3-18\)](#)
- [Cisco Unified CallManager クラスタのセキュリティ モードの確認 \(P.3-20\)](#)
- [Smart Card サービスの開始および自動の設定 \(P.3-21\)](#)
- [セキュリティ トークン パスワード \(etoken\) の変更 \(P.3-22\)](#)
- [Cisco Unified IP Phone 上の CTL ファイルの削除 \(P.3-23\)](#)
- [Cisco CTL クライアントのバージョンの特定 \(P.3-24\)](#)
- [Cisco CTL クライアントの確認とアンインストール \(P.3-24\)](#)
- [その他の情報 \(P.3-25\)](#)

## 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る Windows のバージョンは、Windows 2000 と Windows XP 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。

- Site Administrator Security Token (SAST)
- 同一のサーバで実行される Cisco Unified CallManager および Cisco TFTP
- Certificate Authority Proxy Function (CAPF)
- ファイアウォールなどの TLS プロキシ サーバ

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、シグニチャ、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 Unified CallManager Serviceability で Cisco CallManager および Cisco Tftp サービスを、これらのサービスを実行するすべての Cisco Unified CallManager サーバで、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 クライアントによって CTL ファイルにサーバ証明書が追加されると、CTL クライアント GUI で証明書を表示できるようになります。

CTL ファイルで TLS プロキシ サーバを設定する場合は、セキュア Cisco Unified CallManager システムの一部として Cisco ASA ファイアウォールをセキュアにすることができます。Cisco CTL クライアントは、「CCM」証明書としてファイアウォール証明書を表示します。

Cisco Unified CallManager の管理ページは、etoken を使用して、Cisco CTL クライアントとプロバイダーとの間の TLS 接続を認証します。

## Cisco CTL クライアントの設定のヒント

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。

- Cisco Unified CallManager 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。
- 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。
- 代替または集中 TFTP サーバなどのクラスタ外のサーバのエントリが Cisco CTL クライアントに含まれている場合は、それらのサーバで CTL Provider サービスも実行する必要があります。
- CTL クライアント GUI の [ Alternate TFTP Server ] タブ設定値のセクションの代替 TFTP サーバは、別のクラスタ内にある Cisco TFTP サーバを意味します。これらの設定を使用して、CTL クライアント内の代替 TFTP サーバと集中 TFTP サーバを設定します。



(注)

クラスタ外の（代替および集中）TFTP サーバで Tftp サービス パラメータを設定するについては、『Cisco Unified CallManager システム ガイド』の「Cisco TFTP」を参照してください。

- 集中 TFTP コンフィギュレーションの場合は、混合モードで稼働しているすべてのクラスタ外の TFTP サーバが、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の CTL ファイルに追加する必要があります。マスター TFTP サーバは、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 サーバからコンフィギュレーション ファイルを提供します。集中 TFTP コンフィギュレーション内のすべてのクラスタが同じセキュリティ モードを使用する必要はありません。クラスタはそれぞれ独自のモードを選択できます。
- CTL ファイルを作成または更新したら、Cisco Unified CallManager Serviceability で Cisco CallManager および Cisco Tftp サービスを、これらのサービスを実行するすべての Cisco Unified CallManager サーバで再起動する必要があります。

## Cisco CTL クライアントの設定用チェックリスト

表 3-1 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 CallManager をアップグレードする際の CTL ファイルの設定の詳細については、P.3-10 の「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」を参照してください。

表 3-1 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
<p><b>ステップ 1</b> クラスタにある各 Cisco Unified CallManager に対して、Cisco Unified CallManager Serviceability で Cisco CTL Provider サービスをアクティブにします。</p> <p> <b>ヒント</b> Cisco Unified CallManager 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。</p>	Cisco CTL Provider サービスのアクティブ化 (P.3-5)
<p><b>ステップ 2</b> 最初のノードの Cisco Unified CallManager Serviceability で Cisco Certificate Authority Proxy サービスをアクティブにします。</p> <p> <b>ワンポイントアドバイス</b> 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。</p>	Certificate Authority Proxy Function サービスのアクティブ化 (P.6-6)
<p><b>ステップ 3</b> 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。</p> <p> <b>ヒント</b> これらの設定を Cisco Unified CallManager 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。</p>	TLS 接続用ポートの設定 (P.3-6)
<p><b>ステップ 4</b> 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。</p>	Cisco CTL クライアントの設定 (P.3-11)
<p><b>ステップ 5</b> Cisco CTL クライアントをインストールします。</p>	<ul style="list-style-type: none"> <li>システム要件 (P.1-4)</li> <li>インストール (P.1-13)</li> <li>Cisco CTL クライアントのインストール (P.3-8)</li> </ul>
<p><b>ステップ 6</b> Cisco CTL クライアントを設定します。</p>	<p>Cisco CTL クライアントの設定 (P.3-11)</p> <p>Cisco CTL クライアント オンライン ヘルプ</p>

## 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、このサービスによってクラスタ セキュリティ モードがノンセキュア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。次に、サービスによって CTL ファイルがすべての Cisco Unified CallManager 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 CallManager をアップグレードした場合、Cisco Unified CallManager 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 CallManager Serviceability 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 Unified 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。
- ステップ 5** 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、P.3-6 の「[TLS 接続用ポートの設定](#)」を参照してください。

- ステップ 6** サービスがクラスタ内のすべての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 CallManager Serviceability で [ Tools ] > [ Control Center - Feature Services ] の順に選択します。

### 追加情報

詳細については、P.3-25 の「[関連項目](#)」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、P.6-6の「Certificate Authority Proxy Function サービスのアクティブ化」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

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。

Cisco CTL Provider の TLS 接続用デフォルトポートは 2444 です。Cisco CTL Provider ポートでは 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、クラスタ全体のセキュリティモード設定、CTL ファイルの TFTP サーバへの保存、クラスタ内の Cisco Unified CallManager および TFTP サーバリストの取得などの、Cisco CTL クライアントの要求を処理します。

Ethernet Phone ポートは、SCCP 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 CallManager の TLS 接続用ポートは Cisco Unified CallManager ポート番号に 443 を加算 (+) した番号になるため、Cisco Unified CallManager のデフォルトの TLS 接続は 2443 になります。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のみ、この設定を更新します。

SIP Secure ポートを使用すると、Cisco Unified CallManager は SIP 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 CallManager Serviceability で Cisco CallManager サービスを再起動し、SIP 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 CallManager の管理ページで Cisco CTL Provider サービスを再起動する必要があります。

CTL クライアントが動作している場所からデータ VLAN への CTL ポートを開く必要があります。CTL クライアントは、Cisco Unified CallManager にシグナルを戻すために、TLS を実行している電話機と同じ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 に対して開いている必要があります。

デフォルト設定を変更するには、次の手順を実行します。

### 手順

**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 CallManager の管理ページで [ システム ] > [ サービスパラメータ ] 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 ] 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 CallManager の管理ページで [ システム ] > [ Cisco Unified CallManager ] の順に選択します。

**ステップ8** 『Cisco Unified CallManager 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 CallManager の設定 ( Cisco Unified CallManager 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 CallManager Serviceability で Cisco CallManager サービスを再起動します。

**ステップ11** [ 保存 ] をクリックします。

---

#### 追加情報

詳細については、[P.3-25 の「関連項目」](#)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。

- クラスタのセキュリティ モードの最初の設定時
- CTL ファイルの最初の作成時
- Cisco Unified CallManager のインストール後
- Cisco Unified CallManager サーバまたは Cisco Unified CallManager データの復元後
- Cisco Unified CallManager 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、TFTP サーバ、ASA ファイアウォール、または Cisco Unified CallManager サーバの追加後または削除後
- 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



### 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 CallManager 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 CallManager の管理ページに移動します。
- ステップ 2** Cisco Unified CallManager の管理ページで、[アプリケーション]>[プラグイン]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] ドロップダウン リスト ボックスから [Installation] を選択し、[検索] 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、ウィンドウの右側の、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] 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

詳細については、P.3-25 の「[関連項目](#)」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 CallManager リリース 5.0 を 5.1 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てから、最新の Cisco CTL クライアントをインストールし (P.3-8 の「Cisco CTL クライアントのインストール」を参照) CTL ファイルを再生成する必要があります。Cisco Unified CallManager をアップグレードする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 CallManager 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。

4.x リリースから 5.x リリースへアップグレードし、クラスタでセキュリティを有効にする場合は、アップグレードより以前にインストールした 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。アップグレードしたクラスタでセキュリティを有効にするには、次の手順を実行します。

### 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** P.3-8 の「Cisco CTL クライアントのインストール」の説明に従って、新しい Cisco CTL クライアントをインストールします。
  - ステップ 3** P.3-11 の「Cisco CTL クライアントの設定」の説明に従い、以前使用した USB キーの少なくとも 1 つを使って、Cisco CTL クライアントを実行します。
  - ステップ 4** Cisco CallManager および Cisco Tftp サービスを実行しているすべての Cisco Unified CallManager サーバおよびクラスタ内のすべての TFTP サーバの Cisco Unified CallManager Serviceability で、これらのサービスを再起動します。
- 

### 追加情報

詳細については、P.3-25 の「関連項目」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、スケジュールされたメンテナンス画面で設定します。これは、Cisco Unified CallManager および Cisco TFTP サービスを実行するすべての Cisco Unified CallManager サーバおよびクラスタ内のすべての TFTP サーバの Cisco Unified CallManager Serviceability 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 CallManager クラスタのセキュリティ モードを設定する。



### ヒント

Cisco Unified CallManager 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 CallManager クラスタ全体のパラメータを混合モードに設定することはできません。クラスタ全体のモードを設定するには、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、[P.3-18](#) の「[Cisco CTL クライアントの設定内容](#)」を参照してください。

- Certificate Trust List (CTL; 証明書信頼リスト) を作成する。これは、セキュリティ トークン、Cisco Unified CallManager、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 CallManager、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)

CTL クライアントは、Cisco Unified CallManager スーパークラスタ サポートも提供します。これには、最大 16 のコール処理サーバ、1 つのパブリッシャ、2 つの TFTP サーバ、最大 9 つのメディアリソース サーバが含まれています。

### 始める前に



### ヒント

Cisco Unified CallManager をアップグレードする際の CTL ファイルの設定の詳細については、[P.3-10](#) の「[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](#)」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 CallManager Serviceability 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、Cisco certificate authority 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 CallManager の管理ユーザ名とパスワード
- 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 3-2 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、クラスタの各サーバへのネットワーク接続を確認します。クラスタ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するには、『Cisco Unified Communications Operating System アドミニストレーション ガイド』の説明に従い、ping コマンドを発行します。

複数の Cisco CTL クライアントをインストールした場合、Cisco Unified CallManager 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られません。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 CallManager 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 ファイルをクラスタ内のすべての Cisco Unified CallManager サーバに書き込む。
- CAPF capf.cer をクラスタ内のすべての Cisco Unified CallManager 後続ノード（最初のノード以外）に書き込む。
- 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 CallManager 後続ノード（最初のノード以外）に書き込む。
- 設定されたすべての TFTP サーバにファイルを書き込みます。
- 設定されたすべての ASA ファイアウォールにファイルを書き込みます。
- CTL ファイルを作成した時点で 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 ファイルに署名する。

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** 次の作業のどちらかを実行します。

- 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 3-2 の説明に従って、Cisco Unified CallManager 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 3-2 の説明に従って、[ Set Cisco Unified CallManager 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 3-2](#) 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 3-2](#) 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 3-2](#) 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** クラスタ内のすべてのデバイスをリセットします。詳細については、[P.1-11](#) の「[デバイスのリセット、サービスの再起動、またはサーバおよびクラスタのリブート](#)」を参照してください。

- ステップ 21** Cisco Unified CallManager Serviceability で、Cisco Unified CallManager および Cisco Tftp サービスを実行しているすべての Cisco Unified CallManager サーバおよび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 トークンを安全な任意の場所に格納します。
- 

#### 追加情報

詳細については、[P.3-25 の「関連項目」](#)を参照してください。

## CTL ファイルの更新

次のシナリオが発生した場合、CTL ファイルを更新する必要があります。

- 新しい Cisco Unified CallManager サーバをクラスタに追加した場合
- クラスタ内の Cisco Unified CallManager サーバの名前または IP アドレスを変更した場合
- 設定された TFTP サーバまたは 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 CallManager Serviceability 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、TFTP サーバ、ASA ファイアウォール、または Cisco Unified CallManager サーバの追加後または削除する必要がある場合
- Cisco Unified CallManager サーバまたは Cisco Unified CallManager データの復元後
- 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



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 3-2 の説明に従って、Cisco Unified CallManager 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 CallManager 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 3-2 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 ファイルのシグニチャを検証します。CTL クライアントによってシグニチャが検証されるまで、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 CallManager および Cisco TFTP エントリを更新できません。Cisco Unified CallManager 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。

- サーバ設定の更新または新規セキュリティ トークンの追加については、[P.3-11](#) の「[Cisco CTL クライアントの設定](#)」を参照してください。
- セキュリティ トークンの削除については、[P.3-17](#) の「[CTL ファイル エントリの削除](#)」を参照してください。

#### 追加情報

詳細については、[P.3-25](#) の「[関連項目](#)」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、[ Delete Selected ] をクリックしてエントリを削除します。

Cisco Unified CallManager、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

詳細については、[P.3-25 の「関連項目」](#)を参照してください。

## クラスタ全体のセキュリティ モードの更新

クラスタ全体のセキュリティ 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。クラスタ全体のセキュリティ モードは、Cisco Unified CallManager 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。

Cisco CTL クライアントの初期設定後にクラスタ全体のセキュリティ 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。[P.3-15 の「CTL ファイルの更新」](#)および[表 3-2](#)の説明に従って、[ Cluster Security Mode ] ウィンドウに移動し、モード設定を変更して、[ Next ] をクリックしてから [ Finish ] をクリックします。

クラスタ全体のセキュリティ 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 ファイルはクラスタ内の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 CallManager に登録されます。

## Cisco CTL クライアントの設定内容

クラスタは、表 3-2 の説明にあるように 2 つのモードのどちらかに設定できます。混合モードだけが認証をサポートしています。Cisco CTL クライアントに認証を設定する場合は、[ Set Cisco Unified CallManager Cluster to Mixed Mode ] を選択する必要があります。

表 3-2 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、P.3-3 の「Cisco CTL クライアントの設定のヒント」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、P.3-25 の「関連項目」を参照してください。

表 3-2 CTL クライアントの設定内容

設定	説明
<b>Cisco Unified CallManager Server</b>	
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	ポート番号を入力します。これは、指定した Cisco Unified CallManager サーバで実行されている Cisco CTL Provider サービスの CTL ポートです。デフォルトのポート番号は 2444 です。
Username and Password	最初のノードで管理者特権を持つユーザ名とパスワードと同じものを入力します。
<b>Security Mode オプション ボタン</b>	
Set Cisco Unified CallManager Cluster to Mixed Mode	<p>混合モードでは、認証済みまたは暗号化済みの Cisco Unified IP Phone と、認証されていない Cisco Unified IP Phone を Cisco Unified CallManager 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 CallManager が保証します。</p> <p> <b>(注)</b> クラスタを混合モードに設定すると、Cisco Unified CallManager によって自動登録は無効になります。</p>
Set Cisco Unified CallManager Cluster to Non-Secure Mode	<p>すべてのデバイスが非認証として Cisco Unified CallManager に登録されます。Cisco Unified CallManager ではイメージ認証だけをサポートします。</p> <p>このモードを選択すると、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 CallManager に登録されます。</p> <p> <b>ヒント</b> 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 CallManager サーバから CTL ファイルを削除する必要があります。</p> <p>このモードでは自動登録を使用できます。</p>
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、クラスタのセキュリティモードは変更されません。

表 3-2 CTL クライアントの設定内容 (続き)

設定	説明
<b>CTL Entries オプション ボタン</b>	
Add Tokens	このボタンをクリックすると、証明書信頼リストにセキュリティトークンが追加されます。  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。追加のトークンについてセキュリティ トークン情報が表示されたら、[Add] をクリックし、このタスクを繰り返します。
Add TFTP Server	このボタンをクリックすると、証明書信頼リストに代替 TFTP サーバが追加されます。設定に関する情報を参照するには、[Alternate TFTP Server] タブ設定値の表示後に [Help] ボタンをクリックします。設定を入力したら、[Next] をクリックします。
Add Firewall	このボタンをクリックすると、証明書信頼リストにファイアウォール (TLS プロキシ サーバ) が追加されます。設定に関する情報を参照するには、[Firewall] タブ設定の表示後に [Help] ボタンをクリックします。設定を入力したら、[Next] をクリックします。
<b>Alternate TFTP Server</b>	
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 サーバは、別のクラスタ内にある Cisco TFTP サーバを意味します。代替 TFTP サーバの設定に 2 つの異なるクラスタを使用している場合は、どちらのクラスタもクラスタ全体で同じセキュリティ モードを使用している必要があります。つまり、両方のクラスタで Cisco CTL クライアントをインストールして設定する必要があります。同様に、どちらのクラスタも同じバージョンの Cisco Unified CallManager を実行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に対して同じであることを確認してください。
Port	このリリースの Cisco Unified CallManager では必要ありません。
Username and Password	このリリースの Cisco Unified CallManager では必要ありません。
<b>TLS Proxy Server</b>	
Hostname or IP Address	TLS プロキシのホスト名または IP アドレスを入力します。
Port	ポート番号を入力します。これは、ファイアウォールで実行されている Cisco CTL Provider サービスの CTL ポートです。デフォルトのポート番号は 2444 です。
Username and Password	最初のノードで管理者特権を持つユーザ名とパスワードと同じものを入力します。
<b>Security Token</b>	
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 CallManager クラスタのセキュリティ モードの確認

Cisco Unified CallManager 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。

### 手順

- 
- ステップ 1** Cisco Unified CallManager の管理ページで [システム] > [エンタープライズパラメータ] 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 CallManager クラスタ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 CallManager の管理ページでは変更できません。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

詳細については、[P.3-25 の「関連項目」](#)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 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 CallManager 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

詳細については、[P.3-25](#) の「[関連項目](#)」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 パスワードが付属されています。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

詳細については、[P.3-25](#) の「[関連項目](#)」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

セキュアな実験室環境でこの作業を実行することをお勧めします。特に、クラスタ内の Cisco Unified CallManager 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。
- IP Phone をセキュア クラスタから、ストレージ領域、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。
- IP Phone 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 クラスタへと移動する。
- 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 3-3 の作業を実行します。

表 3-3 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 7960 および 7940	IP Phone 上の [セキュリティ設定] メニューにある、[CTL ファイル] [解除] または **#, および [削除] を押します。
Cisco Unified IP Phone 7970	<p>次の方法のどちらかを実行します。</p> <ul style="list-style-type: none"> <li>• [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 アドミニストレーション ガイド for Cisco Unified CallManager』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。</li> <li>• [設定] メニューにある [削除] ソフトキーを押します。</li> </ul> <p> (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 アドミニストレーション ガイド for Cisco Unified CallManager』を参照してください。</p>

### 追加情報

詳細については、P.3-25 の「関連項目」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** 次の作業のどちらかを実行します。

- 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

詳細については、[P.3-25](#) の「[関連項目](#)」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、クラスタ全体のセキュリティ モードと CTL ファイルは変更されません。必要であれば、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 ] > [ アプリケーションの追加と削除 ] の順に選択します。

**ステップ 2** [ アプリケーションの追加と削除 ] をダブルクリックします。

**ステップ 3** 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 4** 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

詳細については、[P.3-25](#) の「[関連項目](#)」を参照してください。

## その他の情報

### 関連項目

- システム要件 (P.1-4)
- Cisco CTL クライアントの概要 (P.3-2)
- Cisco CTL クライアントの設定用チェックリスト (P.3-4)
- Cisco CTL Provider サービスのアクティブ化 (P.3-5)
- Cisco CAPF サービスのアクティブ化 (P.3-6)
- TLS 接続用ポートの設定 (P.3-6)
- Cisco CTL クライアントのインストール (P.3-8)
- 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.3-10)
- Cisco CTL クライアントの設定 (P.3-11)
- CTL ファイルの更新 (P.3-15)
- CTL ファイル エントリの削除 (P.3-17)
- クラスタ全体のセキュリティ モードの更新 (P.3-17)
- Cisco CTL クライアントの設定内容 (P.3-18)
- Cisco Unified CallManager クラスタのセキュリティ モードの確認 (P.3-20)
- Smart Card サービスの開始および自動の設定 (P.3-21)
- Cisco Unified IP Phone 上の CTL ファイルの削除 (P.3-23)
- Cisco CTL クライアントのバージョンの特定 (P.3-24)
- Cisco CTL クライアントの確認とアンインストール (P.3-24)
- Certificate Authority Proxy Function の使用方法 (P.6-1)

### シスコの関連マニュアル

*Cisco Unified IP Phone アドミニストレーション ガイド for Cisco Unified CallManager*

*Cisco Unified CallManager トラブルシューティング ガイド*





## PART 2

### Cisco Unified IP Phone および Cisco Unity 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 \(P.4-2\)](#)
- [サポートされる電話機のモデル \(P.4-3\)](#)
- [電話機のセキュリティ設定の確認 \(P.4-3\)](#)
- [電話機のセキュリティ設定用チェックリスト \(P.4-4\)](#)
- [その他の情報 \(P.4-5\)](#)

## 電話機のセキュリティ機能について

Cisco Unified CallManager のインストール時に、Cisco Unified CallManager クラスタは非セキュアモードで起動します。Cisco Unified CallManager のインストール後に電話機が起動すると、デバイスはすべて非セキュアとして Cisco Unified CallManager に登録されます。

Cisco Unified CallManager 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 CallManager 5.1 のインストールを行うと、Cisco Unified CallManager 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 CallManager 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 CallManager 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 CallManager および TFTP サーバに存在していれば、Cisco Unified CallManager はそれぞれの Cisco Unified CallManager 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、P.1-6 の「相互作用および制限」を参照してください。

Cisco Unified CallManager 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 CallManager 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、共有回線が設定されている場合も、Cisco Unified CallManager 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 に対して共有回線を設定する場合は、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。

## サポートされる電話機のモデル

このセキュリティガイドでは、各 Cisco Unified IP Phone でサポートされるセキュリティ機能を示しません。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、Cisco Unified CallManager リリース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 CallManager の管理ページでセキュリティ機能を設定できますが、Cisco TFTP サーバで互換ファームウェア ロードをインストールするまで、その機能は動作しません。

## 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このバージョンの Cisco Unified CallManager 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 CallManager 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 CallManager がコールを認証済みまたは暗号化済みとして分類する場合を判別するには、[P.1-5 の「セキュリティアイコン」](#)および [P.1-6 の「相互作用および制限」](#)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 4-1 で説明します。

表 4-1 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
<b>ステップ 1</b> Cisco CTL クライアントを設定し、クラスタ 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.3-1)
<b>ステップ 2</b> 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.6-1)
<b>ステップ 3</b> 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.5-1)
<b>ステップ 4</b> 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.5-12)
<b>ステップ 5</b> SIP 電話機がダイジェスト認証をサポートする場合、Cisco Unified CallManager の管理ページの [ エンドユーザの設定 (End User Configuration) ] ウィンドウで、ダイジェスト クレデンシャルを設定します。	<ul style="list-style-type: none"> <li>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 クレデンシャルの設定 (P.8-4)</li> <li>エンドユーザダイジェスト クレデンシャルの設定内容 (P.8-5)</li> </ul>
<b>ステップ 6</b> ダイジェスト クレデンシャルを設定した後、Cisco Unified CallManager の管理ページの [ 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.8-5)
<b>ステップ 7</b> Cisco Unified IP Phone 7960 または 7940 (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 クレデンシャル) を入力します。	<sup>¶</sup> Cisco Unified CallManager セキュリティ ガイド <sup>¶</sup> では、電話機でダイジェスト認証 クレデンシャルを入力する手順について説明しません。この作業の実行方法については、使用している電話機のモデルとこのバージョンの Cisco Unified CallManager 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。
<b>ステップ 8</b> 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.7-1)
<b>ステップ 9</b> Cisco Unified CallManager の管理ページで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.9-1)

## その他の情報

### 関連項目

- [相互作用および制限 \(P.1-6\)](#)
- [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 \(P.6-1\)](#)
- [電話機のセキュリティ設定用チェックリスト \(P.4-4\)](#)
- [電話機セキュリティ プロファイルの設定 \(P.5-1\)](#)
- [暗号化された電話機設定ファイルの設定 \(P.7-1\)](#)
- [電話機のセキュリティ強化 \(P.9-1\)](#)

### シスコの関連マニュアル

- [Cisco Unified IP Phone アドミニストレーション ガイド for Cisco Unified CallManager](#)
- [Cisco Unified CallManager トラブルシューティング ガイド](#)





# 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 \(P.5-1\)](#)
- [電話機セキュリティ プロファイルの設定のヒント \(P.5-2\)](#)
- [電話機セキュリティ プロファイルの検索 \(P.5-3\)](#)
- [電話機セキュリティ プロファイルの設定 \(P.5-4\)](#)
- [電話機セキュリティ プロファイルの設定内容 \(P.5-5\)](#)
- [電話機セキュリティ プロファイルの適用 \(P.5-12\)](#)
- [電話機セキュリティ プロファイルの削除 \(P.5-13\)](#)
- [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 \(P.5-14\)](#)
- [その他の情報 \(P.5-15\)](#)

## 電話機セキュリティ プロファイルの概要

Cisco Unified CallManager の管理ページでは、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 CallManager 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 CallManager 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 CallManager 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 CallManager 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 CallManager 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 CallManager 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。
- 製造元でインストールされる証明書 ( MIC ) は、LSC のインストールのためだけに使用することをお勧めします。シスコは、Cisco Unified CallManager との TLS 接続を認証するための LSC をサポートしています。MIC ルート証明書は侵害されている可能性があるため、お客様が TLS 認証やその他の目的で MIC を使うよう電話機を設定する場合は、自らの責任で行う必要があります。MIC が侵害されている場合、シスコは一切の責任を負いません。

Cisco Unified IP Phone 7906、7911、7941、7961、7970、および 7971 モデルをアップグレードして Cisco Unified CallManager への TLS 接続に LSC を使用できるようにし、互換性の問題が後で発生するのを避けるため MIC ルート証明書を Cisco Unified CallManager 信頼ストアから削除することをお勧めします。詳細については、[P.1-14 の「電話機の証明書の種類」](#)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 CallManager の管理ページで、[システム]>[セキュリティプロファイル]>[電話セキュリティプロファイル]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。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** ドロップダウン リスト ボックスから、表示するセキュリティ プロファイルの検索条件を選択し、[検索]をクリックします。



**(注)** データベースに登録されているすべてのセキュリティ プロファイルを検索するには、検索条件を指定せずに、[検索]をクリックします。

ウィンドウが更新され、検索条件と一致するセキュリティ プロファイルが表示されます。

- ステップ 3** 表示するセキュリティ プロファイルの [名前 (Name)] リンクをクリックします。



**ヒント** 検索結果内の [名前 (Name)] または [説明] を検索するには、[絞り込み] チェックボックスをオンにして、この手順で説明したように検索条件を入力し、[検索]をクリックします。

選択した項目がウィンドウに表示されます。

### 追加情報

詳細については、P.5-15 の「関連項目」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 CallManager の管理ページで、[ システム ] > [ セキュリティプロファイル ] > [ 電話セキュリティプロファイル ] 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 ] をクリックして、[ステップ 3](#) へ進みます。
- 既存のセキュリティ プロファイルをコピーするには、[P.5-3](#) の「[電話機セキュリティ プロファイルの検索](#)」の説明に従って適切なプロファイルを見つけて表示し、[ コピー (Copy) ] をクリックして、[ステップ 3](#) へ進みます。
- 既存のプロファイルを更新するには、[P.5-3](#) の「[電話機セキュリティ プロファイルの検索](#)」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 ] をクリックすると、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。[ コピー (Copy) ] をクリックすると、設定ウィンドウが表示され、コピーされた設定が示されます。

**ステップ 3** SCCP 電話機の場合は[表 5-1](#)、SIP 電話機の場合は[表 5-2](#) の説明に従い、適切な設定を入力します。

**ステップ 4** [ 保存 ] をクリックします。

### 追加の手順

セキュリティ プロファイルを作成した後、[P.5-12](#) の「[電話機セキュリティ プロファイルの適用](#)」の説明に従い、電話機に適用します。

SIP 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クレデンシャル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

詳細については、[P.5-15](#) の「[関連項目](#)」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 5-1 で、SCCP 電話機セキュリティ プロファイルの設定について説明します。

表 5-2 で、SIP 電話機セキュリティ プロファイルの設定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、P.5-2 の「電話機セキュリティ プロファイルの設定のヒント」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、P.5-15 の「関連項目」を参照してください。

表 5-1 SCCP 電話機セキュリティ プロファイル

設定	説明
[名前]	<p>セキュリティ プロファイルの名前を入力します。</p> <p>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。</p> <p> <b>ヒント</b> 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。</p>
[説明]	セキュリティ プロファイルの説明を入力します。
[デバイスセキュリティモード (Device Security Mode)]	<p>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。</p> <ul style="list-style-type: none"> <li>• <b>[ Non Secure ]</b>: 電話機にイメージ認証以外のセキュリティ機能はない。TCP 接続で Cisco Unified CallManager が利用できる。</li> <li>• <b>[ Authenticated ]</b>: Cisco Unified CallManager は電話機の整合性と認証を提供する。NULL/SHA を使用する TLS 接続を開始する。</li> <li>• <b>[ Encrypted ]</b>: Cisco Unified CallManager は電話機の整合性、認証、および暗号化を提供する。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 で搬送する。</li> </ul>
[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 CallManager 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、P.1-24 の「設定ファイルの暗号化」および P.7-1 の「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。

表 5-1 SCCP 電話機セキュリティ プロファイル (続き)

設定	説明
[ 認証モード ( Authentication Mode ) ]	<p data-bbox="707 309 1479 371">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。</p> <p data-bbox="707 394 1479 456">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。</p> <ul data-bbox="722 479 1479 712" style="list-style-type: none"> <li data-bbox="722 479 1479 609">• [ <b>By Authentication String</b> ]: 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。</li> <li data-bbox="722 620 1479 712">• [ <b>By Null String</b> ]: 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。</li> </ul> <p data-bbox="754 723 1479 817">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。</p> <ul data-bbox="722 840 1479 1120" style="list-style-type: none"> <li data-bbox="722 840 1479 1120">• [ <b>By Existing Certificate ( Precedence to LSC )</b> ]: 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。</li> </ul> <p data-bbox="754 1131 1479 1225">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。</p> <p data-bbox="754 1236 1479 1397">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。</p> <ul data-bbox="722 1408 1479 1599" style="list-style-type: none"> <li data-bbox="722 1408 1479 1599">• [ <b>By Existing Certificate( Precedence to MIC )</b> ]: 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。</li> </ul> <p data-bbox="754 1610 1479 1704">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。</p> <p data-bbox="707 1727 754 1765"></p> <p data-bbox="707 1765 1479 2009"><b>(注)</b> [ 電話セキュリティプロファイル ] 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、P.5-2 の「電話機セキュリティ プロファイルの設定のヒント」を参照してください )。[ 電話の設定 ( Phone Configuration ) ] ウィンドウでこれらを設定する方法については、『Cisco Unified CallManager アドミニストレーションガイド』を参照してください。</p>

表 5-1 SCCP 電話機セキュリティ プロファイル (続き)

設定	説明
[ キーサイズ ( Key Size、ビット ) ]	<p>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。</p> <p>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。</p> <p> <b>(注)</b> [電話セキュリティプロファイル] 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、P.5-2 の「電話機セキュリティ プロファイルの設定のヒント」を参照してください)。[電話の設定 ( Phone Configuration )] ウィンドウでこれらを設定する方法については、『Cisco Unified CallManager アドミニストレーションガイド』を参照してください。</p>

表 5-2 SIP 電話機セキュリティ プロファイル

設定	説明
[ 名前 ]	<p>セキュリティ プロファイルの名前を入力します。</p> <p>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。</p> <p> <b>ヒント</b> 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。</p>
[ 説明 ]	<p>セキュリティ プロファイルの説明を入力します。</p>
[ ナンス確認時間 ( Nonce Validity Time ) ]	<p>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 CallManager は新しい値を生成します。</p> <p> <b>(注)</b> 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。</p>

表 5-2 SIP 電話機セキュリティ プロファイル (続き)

設定	説明
[ デバイスセキュリティモード ( Device Security Mode ) ]	<p>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。</p> <ul style="list-style-type: none"> <li>• [ <b>Non Secure</b> ]: 電話機にイメージ認証以外のセキュリティ機能はない。TCP 接続で Cisco Unified CallManager が利用できる。</li> <li>• [ <b>Authenticated</b> ]: Cisco Unified CallManager は電話機の整合性と認証を提供する。NULL/SHA を使用する TLS 接続を開始する。</li> <li>• [ <b>Encrypted</b> ]: Cisco Unified CallManager は電話機の整合性、認証、および暗号化を提供する。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 で搬送する。</li> </ul>
[ 転送タイプ ( Transport Type ) ]	<p>[ デバイスセキュリティモード ( Device Security Mode ) ] が [ <b>Non Secure</b> ] 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 )。</p> <ul style="list-style-type: none"> <li>• [ <b>TCP</b> ]: 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。</li> <li>• [ <b>UDP</b> ]: 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しません。</li> <li>• [ <b>TCP + UDP</b> ]: 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。このオプションは、セキュリティを提供しません。</li> </ul> <p>[ デバイスセキュリティモード ( Device Security Mode ) ] が [ <b>Authenticated</b> ] または [ <b>Encrypted</b> ] である場合、TLS が転送タイプとなります。TLS 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 ) を提供します。</p> <p>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。</p>
[ ダイジェスト認証を有効化 ( Enable Digest Authentication ) ]	<p>このチェックボックスをオンにすると、Cisco Unified CallManager 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。</p> <p>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 [ <b>Authenticated</b> ] または [ <b>Encrypted</b> ] を選択します。</p> <p> (注) ダイジェスト認証の詳細については、P.1-18 の「<a href="#">ダイジェスト認証</a>」および P.8-1 の「<a href="#">SIP 電話機のダイジェスト認証の設定</a>」を参照してください。</p>

表 5-2 SIP 電話機セキュリティ プロファイル (続き)

設定	説明
[ TFTP 暗号化 ( TFTP Encrypted Config )]	<p>このチェックボックスがオンの場合、Cisco Unified CallManager 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。</p> <p> <b>ヒント</b> このオプションを有効にして、対称キーを設定し、ダイジェストクレデンシャルと管理者パスワードを保護することをお勧めします。</p> <p>詳細については、<a href="#">P.1-24 の「設定ファイルの暗号化」</a>および <a href="#">P.7-1 の「暗号化された電話機設定ファイルの設定」</a>を参照してください。</p>
[ 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 )]	<p>このチェックボックスがオンの場合、Cisco Unified CallManager 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クレデンシャルを削除します。このオプションは、Cisco Unified IP Phone 7905、7912、7940、および 7960 モデル ( SIP のみ) 専用です。</p> <p>詳細については、<a href="#">P.1-24 の「設定ファイルの暗号化」</a>および <a href="#">P.7-1 の「暗号化された電話機設定ファイルの設定」</a>を参照してください。</p>

表 5-2 SIP 電話機セキュリティ プロファイル (続き)

設定	説明
[ 認証モード ( Authentication Mode ) ]	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• [ <b>By Authentication String</b> ]: 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。</li> <li>• [ <b>By Null String</b> ]: 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。</li> </ul> <p>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。</p> <ul style="list-style-type: none"> <li>• [ <b>By Existing Certificate ( Precedence to LSC )</b> ]: 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。</li> </ul> <p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• [ <b>By Existing Certificate( Precedence to MIC )</b> ]: 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。</li> </ul> <p>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。</p> <p> (注) [ 電話セキュリティプロファイル ] 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、P.5-2 の「電話機セキュリティ プロファイルの設定のヒント」を参照してください )。[ 電話の設定 ( Phone Configuration ) ] ウィンドウでこれらを設定する方法については、『Cisco Unified CallManager アドミニストレーションガイド』を参照してください。</p>

表 5-2 SIP 電話機セキュリティ プロファイル (続き)

設定	説明
[ キーサイズ (Key Size、ビット)]	<p>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。</p> <p>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。</p> <p> (注) [電話セキュリティプロファイル] 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、この章の P.5-2 の「電話機セキュリティ プロファイルの設定のヒント」を参照してください)。[電話の設定 (Phone Configuration)] ウィンドウでこれらを設定する方法については、『Cisco Unified CallManager アドミニストレーション ガイド』を参照してください。</p>
[ SIP 電話ポート (SIP Phone Port)]	<p>この設定は、UDP 転送を使用する SIP 電話機に適用されます。</p> <p>UDP を使用する Cisco Unified IP Phone (SIP のみ) が、Cisco Unified CallManager 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。</p> <p>TCP または TLS を使用する電話機は、この設定を無視します。</p>

## 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、[P.6-1 の「Certificate Authority Proxy Function の使用方法」](#)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 CallManager 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 ] をクリックします。
  - ステップ 5** [ リセット ] をクリックして、電話機をリセットします。
- 

### 追加の手順

SIP 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 クレデンシャル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 クレデンシャルの設定の詳細については、[P.8-1 の「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。

### 追加情報

詳細については、[P.5-15 の「関連項目」](#)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 CallManager 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 CallManager 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 ] ドロップダウン リスト ボックスから [ 依存関係レコード ] を選択して、[ 移動 ] 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 ] > [ エンタープライズパラメータ ] 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 CallManager システム ガイド』を参照してください。

### 手順

**ステップ 1** P.5-3 の「電話機セキュリティ プロファイルの検索」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。

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 ] 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 ] をクリックしてから [ 選択項目の削除 ] をクリックします。

**ステップ 2** 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 ] をクリックします。
- 検索と一覧表示ウィンドウで、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 ] 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 ] をクリックして削除操作を取り消します。

### 追加情報

詳細については、P.5-15 の「関連項目」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

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 CallManager の管理ページで [ デバイス ] > [ 電話 ] の順に選択します。
  - ステップ 2** [ 検索対象 : 電話、検索条件 ] ドロップダウン リスト ボックスから、[ セキュリティプロファイル ] を選択します。
  - ステップ 3** 必要に応じて、[ 検索対象 : 電話、検索条件 ] ドロップダウン リスト ボックスの横に表示されているドロップダウン リスト ボックスのオプションを選択してセキュリティ プロファイルの追加の検索条件を指定し、特定の検索条件を入力します。
  - ステップ 4** 検索条件を指定した後、[ 検索 ] をクリックします。検索結果が表示されます。
- 

### 追加情報

詳細については、[P.5-15 の「関連項目」](#)を参照してください。

## その他の情報

### 関連項目

- [ダイジェスト認証 \(P.1-18\)](#)
- [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 \(P.5-1\)](#)
- [電話機セキュリティ プロファイルの設定のヒント \(P.5-2\)](#)
- [電話機セキュリティ プロファイルの検索 \(P.5-3\)](#)
- [電話機セキュリティ プロファイルの設定 \(P.5-4\)](#)
- [電話機セキュリティ プロファイルの設定内容 \(P.5-5\)](#)
- [電話機セキュリティ プロファイルの適用 \(P.5-12\)](#)
- [電話機セキュリティ プロファイルの削除 \(P.5-13\)](#)
- [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 \(P.5-14\)](#)
- [暗号化された電話機設定ファイルの設定 \(P.7-1\)](#)
- [SIP 電話機のダイジェスト認証の設定 \(P.8-1\)](#)
- [電話機のセキュリティ強化 \(P.9-1\)](#)

### シスコの関連マニュアル

*Cisco Unified CallManager アドミニストレーション ガイド*

*Cisco Unified IP Phone アドミニストレーション ガイド for Cisco Unified CallManager*





# 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 \( P.6-2 \)](#)
- [Cisco Unified IP Phone と CAPF の相互作用 \( P.6-2 \)](#)
- [CAPF システムの相互作用および要件 \( P.6-4 \)](#)
- [Cisco Unified CallManager Serviceability での CAPF の設定 \( P.6-4 \)](#)
- [CAPF の設定用チェックリスト \( P.6-5 \)](#)
- [Certificate Authority Proxy Function サービスのアクティブ化 \( P.6-6 \)](#)
- [CAPF サービス パラメータの更新 \( P.6-7 \)](#)
- [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 \( P.6-8 \)](#)
- [電話の設定 \( Phone Configuration \) ウィンドウの CAPF 設定 \( P.6-9 \)](#)
- [LSC ステータスまたは認証文字列に基づく電話機の検索 \( P.6-10 \)](#)
- [CAPF レポートの生成 \( P.6-11 \)](#)
- [電話機での認証文字列の入力 \( P.6-12 \)](#)
- [電話機での認証文字列の確認 \( P.6-13 \)](#)
- [その他の情報 \( P.6-13 \)](#)

## Certificate Authority Proxy Function の概要

Certificate Authority Proxy Function (CAPF) は Cisco Unified CallManager と共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」認証によって認証する。
- 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 モデルに対して発行する。
- 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する。
- 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する。
- 製造元でインストールされる証明書によって認証する。

Cisco Certificate Authority Proxy Function サービスをアクティブにすると、CAPF に固有な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 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 LAC 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当たります。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ない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かかることがあります。

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 CallManager、および保護された 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 CallManager によって電話機がリセットされたときに CAPF が Cisco Unified IP Phone 7960 および 7940 とどのように相互対話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 [ 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 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 [ Non Secure ] に、CAPF 情報の [ 認証モード ( Authentication Mode ) ] を [ By Null String ] または [ 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 CallManager 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 [ Authenticated ] または [ 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 [ Authenticated ] または [ Encrypted ] に、CAPF 情報の [ 認証モード ( Authentication Mode ) ] を [ By Null String ] または [ 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 CallManager 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、[ 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。

## 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。



### 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 CallManager によって情報が Cisco Unified CallManager データベースに格納されるためです。

- 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 [ 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 CallManager 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、その電話機が送信する LSC 証明書は別の CAPF によって発行されたものとなり、CTL ファイル内にあるものとは異なるため、Cisco Unified Call Manager はその証明書を信頼しません。保護された電話機を登録できるようにするには、P.3-23 の「Cisco Unified IP Phone 上の CTL ファイルの削除」に従って既存の CTL ファイルを削除します。次に、[ Install/Upgrade ] オプションを使用して新規 CAPF で新規 LSC 証明書をインストールし、新規 CTL ファイル用に電話機をリセットします（あるいは MIC を使用します）。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 [ Delete ] オプションを使用します。

## Cisco Unified CallManager Serviceability での CAPF の設定

次の作業を Cisco Unified CallManager Serviceability で実行します。

- Cisco Certificate Authority Proxy Function サービスをアクティブにする。
- CAPF 用のトレース設定を行う。

詳細については、Cisco Unified CallManager Serviceability のマニュアルを参照してください。

## CAPF の設定用チェックリスト

表 6-1 に、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判別し、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 6-1 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
<p><b>ステップ 1</b> 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判別します。</p> <p>CAP 1.0(1) データを Cisco Unified CallManager 4.0 パブリッシュ 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判別します。</p> <p> <b>ヒント</b> Cisco Unified CallManager 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 CallManager 5.x データベースに存在することを確認した場合は、Cisco Unified CallManager 4.0 で使用していた CAPF ユーティリティを削除できます。</p>	<ul style="list-style-type: none"> <li>• 使用している電話機モデルと、このバージョンの Cisco Unified CallManager をサポートする電話機のマニュアル</li> <li>• <i>Data Migration Assistant 2.0 User Guide</i></li> </ul>
<p><b>ステップ 2</b> 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。</p> <p> <b>ヒント</b> 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。</p>	<p><a href="#">Certificate Authority Proxy Function サービスのアクティブ化 (P.6-6)</a></p>
<p><b>ステップ 3</b> 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。</p>	<p><a href="#">Cisco CTL クライアントの設定 (P.3-11)</a></p>
<p><b>ステップ 4</b> 必要に応じて、CAPF サービス パラメータを更新します。</p>	<ul style="list-style-type: none"> <li>• <a href="#">CAPF サービス パラメータの更新(P.6-7)</a></li> <li>• <a href="#">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.6-8)</a></li> </ul>
<p><b>ステップ 5</b> 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 CallManager の管理ページを使用します。</p>	<ul style="list-style-type: none"> <li>• <a href="#">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.6-8)</a></li> <li>• <a href="#">電話の設定 ( Phone Configuration ) ウィンドウの CAPF 設定 (P.6-9)</a></li> <li>• <a href="#">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.6-10)</a></li> </ul>
<p><b>ステップ 6</b> 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。</p>	<p><a href="#">電話機での認証文字列の入力 (P.6-12)</a></p>

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

Cisco Unified CallManager では、Cisco Unified CallManager Serviceability で Certificate Authority Proxy Function サービスが自動的にアクティブになりません。

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。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、[P.3-15 の「CTL ファイルの更新」](#)の説明に従って CTL ファイルを更新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 CallManager Serviceability 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

詳細については、[P.6-13 の「関連項目」](#)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 CallManager の管理ページで Active ステータスとして表示されるようにするには、[P.6-6 の「Certificate Authority Proxy Function サービスのアクティブ化」](#)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 CallManager の管理ページで [システム]>[サービスパラメータ] の順に選択します。
- 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、最初の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 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

詳細については、[P.6-13 の「関連項目」](#)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、[表 6-2](#) 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 CallManager 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 6-2](#) の説明に従って、設定内容を入力します。
  - ステップ 4** [保存] をクリックします。
  - ステップ 5** [リセット] をクリックします。
- 

### 追加情報

詳細については、[P.6-13](#) の「[関連項目](#)」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 6-2 は、Cisco Unified CallManager 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、P.6-4 の「CAPF システムの相互作用および要件」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、P.6-13 の「関連項目」を参照してください。

表 6-2 CAPF 設定

設定	説明
[ 証明書の操作 (Certificate Operation) ]	<p>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。</p> <ul style="list-style-type: none"> <li>• [ 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)。</li> <li>• [ 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。</li> <li>• [ 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。</li> <li>• [ 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 CallManager 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。</li> </ul> <p>[ 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。</p> <p> <b>ヒント</b> 電話機に証明書が存在しない場合、[ Delete ] オプションと [ Troubleshoot ] オプションは表示されません。</p>
[ 認証文字列 (Authentication String) ]	<p>[ 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 ] 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。</p> <p>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。</p>
[ 文字列を生成 ]	<p>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。</p>
[ 操作の完了 (Operation Completes By) ]	<p>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。</p> <p>表示される値は、最初のノードに適用されます。</p>
[ 証明書の操作ステータス (Certificate Operation Status) ]	<p>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、&lt;操作のタイプ&gt; pending、failed、successful など、操作のタイプには証明書操作オプションの [ Install/Upgrade ]、[ Delete ]、または [ Troubleshoot ] 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。</p>

## 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 CallManager の管理ページで [ デバイス ] > [ 電話 ] の順に選択します。
- ステップ 2** [ 検索対象 : 電話、検索条件 ] 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 1 つを選択します。
  - [ LSC ステータス ]: 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 ]: 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** 必要に応じて、[ 検索対象 : 電話、検索条件 ] ドロップダウン リスト ボックスの横に表示されているドロップダウン リスト ボックスのオプションを選択して LSC ステータスまたは認証文字列の追加の検索条件を指定し、特定の検索条件を入力します。
- ステップ 4** 検索条件を指定した後、[ 検索 ] をクリックします。



**ヒント** 検索結果内の追加情報を検索するには、[ 絞り込み ] チェックボックスをオンにして、検索条件を入力し、[ 検索 ] をクリックします。

### 追加情報

詳細については、[P.6-13 の「関連項目」](#)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 CallManager の管理ページで [ **デバイス** ] > [ **電話** ] の順に選択します。

[ 電話の検索と一覧表示 ( Find and List Phones ) ] ウィンドウが表示されます。

**ステップ 2** [ 検索対象 : 電話、検索条件 ] ドロップダウン リスト ボックスで、次のオプションのいずれか 1 つを選択します。

- [ デバイス名 ]
- [ 説明 ]
- [ LSC ステータス ]
- [ 認証文字列 ]
- [ セキュリティプロファイル ]



**ヒント** 必要に応じて、[ 検索対象 : 電話、検索条件 ] ドロップダウン リスト ボックスの横に表示されているドロップダウン リスト ボックスのオプションを選択して追加の検索条件を指定し、特定の検索条件を入力します。

検索結果が表示されます。



**ヒント** 検索結果内の追加情報を検索するには、[ **絞り込み** ] チェックボックスをオンにして、検索条件を入力し、[ **検索** ] をクリックします。

**ステップ 3** [ 関連リンク ] 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** ] を選択し、[ **移動** ] をクリックします。

**ステップ 4** ファイルを任意の場所に保存します。

**ステップ 5** Microsoft Excel を使用して .csv ファイルを開きます。

### 追加情報

詳細については、[P.6-13 の「関連項目」](#)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。
- P.6-6 の「Certificate Authority Proxy Function サービスのアクティブ化」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。
- 最初のノードが実行中で、機能している。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します。
- ドライブが登録されている。
- 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 ) を押してアンロックします。
- ステップ 3** [ Settings ( 設定 ) ] メニューへスクロール ダウンします。「Security Configuration ( セキュリティ設定 )」を強調表示して [ Select ( 選択 ) ] ソフトキーを押します。
- ステップ 4** [ Security Configuration ( セキュリティ設定 ) ] メニューへスクロール ダウンします。「LSC」を強調表示して [ Update ( 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求めるプロンプトが表示されたら、システムが提供した文字列を入力し、[ Submit ( 送信 ) ] ソフトキーを押します。

電話機は現在の CAPF 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。

電話機に表示されたメッセージを確認することで、証明書操作の進行状況を監視できます。[ Submit ( 送信 ) ] を押すと、「Pending ( 処理中 )」というメッセージが LSC オプションの下に表示されます。電話機は公開鍵と秘密鍵のペアを生成し、電話機に関する情報を表示します。電話機が処理を正常に完了すると、成功を示すメッセージが表示されます。失敗を示すメッセージが電話機に表示された場合は、入力した認証文字列が間違っているか、電話機でアップグレードが有効になっていません。

[ Stop ( 中止 ) ] オプションを選択すれば、いつでもプロセスを停止できます。

---

### 追加情報

詳細については、P.6-13 の「関連項目」を参照してください。

## 電話機での認証文字列の確認

電話機に証明書がインストールされたことを確認するには、[ Settings( 設定 ) ] > [ Model Information ( モデル情報 ) ] を選択し、LSC 設定を表示します。この設定に、「Installed ( インストール済み )」または「Not Installed ( 未インストール )」と示されます。

### 追加情報

詳細については、P.6-13 の「関連項目」を参照してください。

## その他の情報

### 関連項目

- [Certificate Authority Proxy Function の概要 \( P.6-2 \)](#)
- [Cisco Unified IP Phone と CAPF の相互作用 \( P.6-2 \)](#)
- [CAPF システムの相互作用および要件 \( P.6-4 \)](#)
- [Cisco Unified CallManager Serviceability での CAPF の設定 \( P.6-4 \)](#)
- [CAPF の設定用チェックリスト \( P.6-5 \)](#)
- [Certificate Authority Proxy Function サービスのアクティブ化 \( P.6-6 \)](#)
- [CAPF サービス パラメータの更新 \( P.6-7 \)](#)
- [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 \( P.6-8 \)](#)
- [電話の設定 \( Phone Configuration \) ウィンドウの CAPF 設定 \( P.6-9 \)](#)
- [LSC ステータスまたは認証文字列に基づく電話機の検索 \( P.6-10 \)](#)
- [CAPF レポートの生成 \( P.6-11 \)](#)
- [電話機での認証文字列の入力 \( P.6-12 \)](#)
- [電話機での認証文字列の確認 \( P.6-13 \)](#)

### シスコの関連マニュアル

*Cisco Unified IP Phone アドミニストレーション ガイド for Cisco Unified CallManager*

Cisco Unified CallManager Serviceability のマニュアル





## 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 \(P.7-2\)](#)
- [サポートされる電話機のモデル \(P.7-5\)](#)
- [暗号化された設定ファイルの設定のヒント \(P.7-6\)](#)
- [暗号化設定ファイルの設定用チェックリスト \(P.7-7\)](#)
- [電話機設定ファイルの暗号化の有効化 \(P.7-8\)](#)
- [鍵の手動配布の設定 \(P.7-8\)](#)
- [鍵の手動配布の設定内容 \(P.7-9\)](#)
- [電話機での対称キーの入力 \(P.7-10\)](#)
- [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 \(P.7-11\)](#)
- [電話機設定ファイルが暗号化されていることの確認 \(P.7-12\)](#)
- [電話機設定ファイルの暗号化の無効化 \(P.7-12\)](#)
- [その他の情報 \(P.7-14\)](#)

## 電話機設定ファイルの暗号化について

電話機が Cisco Unified CallManager からダウンロードする設定ファイル内のダイジェスト クレデンシャルおよびセキュア 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 ] オプションを有効にして、Cisco Unified CallManager の管理ページで追加作業を実行する必要があります。

[ TFTP 暗号化 ] オプションを有効にして、Cisco Unified CallManager 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 CallManager Serviceability 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する。
2. 暗号化されたバージョンの設定ファイルを生成する。

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 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 クレデンシャルは暗号化されずに送信されます。詳細については、[P.7-12 の「電話機設定ファイルの暗号化の無効化」](#)を参照してください。

[P.7-5 の「サポートされる電話機のモデル」](#)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 CallManager 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 CallManager 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、クラスタを混合モードに設定し、Cisco Unified CallManager の管理ページで 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、[P.7-5 の「サポートされる電話機のモデル」](#)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 CallManager 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判別するには、P.7-5 の「サポートされる電話機のモデル」を参照してください。

設定ファイルを暗号化するには、管理者が手動で鍵を Cisco Unified CallManager の管理ページに入力するか、Cisco Unified CallManager の管理ページの [ 電話の設定 ( Phone Configuration ) ] ウィンドウで鍵を生成します。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 ( 受け入れ ) ] 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判別するには、P.7-5 の「サポートされる電話機のモデル」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 CallManager 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、P.7-5 の「サポートされる電話機のモデル」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 ] 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電話機が暗号化されていない設定ファイルを要求するように、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モデルのリストについては、P.7-5 の「サポートされる電話機のモデル」を参照してください。

Certificate Authority Proxy Function ( CAPF ) の詳細については、P.6-2 の「Certificate Authority Proxy Function の概要」を参照してください。Certificate Authority Proxy Function ( CAPF ) は、Cisco Unified CallManager に対する Cisco Unified IP Phone の認証、および電話機の証明書 ( LSC ) の発行を行います。

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 TFTP サーバから暗号化された設定ファイルを要求します。電話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 値が空白であるなど )、CAPF 認証モードが [ 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 ( [ 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 CallManager 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 ] 設定が無効の場合、Cisco Unified IP Phone 7911、7941、7961、7970、および 7971 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 CallManager はファイルが見つからない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 ] 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 CallManager 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 7905 または 7912 (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 7940 または 7960 (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：これらの SIP 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 7970 または 7971 (SIP のみ)、 Cisco Unified IP Phone 7941 または 7961 (SIP のみ)、 Cisco Unified IP Phone 7911 (SIP のみ)、 Cisco Unified IP Phone 7906 (SIP のみ)	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 暗号化アルゴリズム：AES 128 鍵サイズ：128 ビット
Cisco Unified IP Phone 7970 または 7971 (SCCP のみ)、 Cisco Unified IP Phone 7941 または 7961 (SCCP のみ)、 Cisco Unified IP Phone 7911 (SCCP のみ)、 Cisco Unified IP Phone 7906 (SCCP のみ)	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 ] 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 CallManager の管理ページ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 ] フラグが設定されている場合、電話機または Cisco Unified CallManager 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 CallManager の管理ページで、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 ] フラグが表示されます。Cisco Unified IP Phone 7905、7912、7940、および 7960 (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、これらのモデル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 ] 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 クレデンシャルおよびセキュア パスワードはクリアで送信されます。
- 公開鍵暗号化を使用する Cisco Unified Phone の場合、Cisco Unified CallManager は、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して、暗号化された設定ファイルを有効にするように要求しません。Cisco Unified CallManager は、登録中の公開鍵のダウンロードに 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 7905、7912、7940、および 7960 (SIP のみ) の場合、Cisco Unified CallManager の管理ページに、ダイジェスト クレデンシャル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、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 クレデンシャルの初期化に便利です。この方式では、[ 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 クレデンシャルを送信します。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 クレデンシャルが除外されます。

これらの電話機にすでにダイジェスト クレデンシャルが存在しており、着信ファイルにダイジェスト クレデンシャル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 クレデンシャル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 クレデンシャルを変更した場合は、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 クレデンシャル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 7-1 を使用して、Cisco Unified CallManager の管理ページで暗号化された設定ファイルの設定手順を進めます。

表 7-1 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。	Cisco CTL クライアントの設定 (P.3-1)
ステップ 2 [電話セキュリティプロファイル]で,[TFTP 暗号化]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。	<ul style="list-style-type: none"> <li>暗号化された設定ファイルの設定のヒント (P.7-6)</li> <li>電話機設定ファイルの暗号化の有効化 (P.7-8)</li> <li>電話機セキュリティ プロファイルの適用 (P.5-12)</li> </ul>
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判別します。	サポートされる電話機のモデル (P.7-5)
ステップ 4 使用中の電話機が鍵の手動配布をサポートしている場合は、鍵の手動配布の作業を実行します。	<ul style="list-style-type: none"> <li>暗号化された設定ファイルの設定のヒント (P.7-6)</li> <li>鍵の手動配布の設定 (P.7-8)</li> <li>鍵の手動配布の設定内容 (P.7-9)</li> </ul>
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.7-10)
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。	<ul style="list-style-type: none"> <li>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.7-11)</li> <li>Certificate Authority Proxy Function の使用方法 (P.6-1)</li> </ul>

## 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、P.5-3 の「電話機セキュリティ プロファイルの検索」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 ] チェックボックスをオンにします。

### 追加情報

詳細については、P.7-14 の「関連項目」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判別するには、P.7-5 の「サポートされる電話機のモデル」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 CallManager 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 CallManager の管理ページで TFTP Encrypted Config パラメータを有効にした。

### 手順

- 
- ステップ 1** 『Cisco Unified CallManager 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 7-2 の説明に従って、鍵の手動配布設定を定義します。設定の完了後は、鍵は変更しないでください。
  - ステップ 3** [ 保存 ] 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

詳細については、P.7-14 の「関連項目」を参照してください。

## 鍵の手動配布の設定内容

表 7-2 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、P.7-6 の「暗号化された設定ファイルの設定のヒント」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、P.7-14 の「関連項目」を参照してください。

表 7-2 鍵の手動配布の設定内容

設定	説明
[ 対称キー ( Symmetric Key ) ]	<p>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。</p> <p>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 CallManager は入力された値を拒否します。Cisco Unified CallManager は、次の鍵サイズをサポートします。</p> <ul style="list-style-type: none"> <li>• Cisco Unified IP Phone 7905 および 7912 ( SIP プロトコルのみ ): 256 ビット</li> <li>• Cisco Unified IP Phone 7940 および 7960 ( SIP プロトコルのみ ): 128 ビット</li> </ul> <p>鍵を設定した後は、変更できません。</p>
[ 文字列を生成 ]	<p>Cisco Unified CallManager 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 ] ボタンをクリックします。</p> <p>鍵を設定した後は、変更できません。</p>
[ データベース値を復元 ]	<p>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。</p>

## 電話機での対称キーの入力

Cisco Unified CallManager の管理ページ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、[ Settings (設定) ] メニューへスクロールダウンし、**電話のロック解除**を強調表示して、[ Select (選択) ] ソフトキーを押します。電話パスワードを入力し、[ Accept (受け入れ) ] ソフトキーを押します。
- 電話機がパスワードを受け入れます。
- ステップ 3** [ Settings (設定) ] メニューへスクロールダウンし、[ Security Configuration (セキュリティ設定) ] を強調表示して、[ Select (選択) ] ソフトキーを押します。
- ステップ 4** [ Security Configuration (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て、[ Select (選択) ] ソフトキーを押します。
- ステップ 5** 暗号鍵の入力を求めるプロンプトが表示されたら、鍵を入力します (16 進数で)。鍵をクリアする必要がある場合は、ゼロを 32 個入力します。
- ステップ 6** 鍵の入力が終わったら、[ Accept (受け入れ) ] ソフトキーを押します。
- 電話機が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。
- ステップ 8** 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。
-

## 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判別するには、[P.7-5 の「サポートされる電話機のモデル」](#)を参照してください。

次の手順では、Cisco Unified CallManager データベースに電話機が存在し、Cisco Unified CallManager の管理ページで 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 設定セクションで [Troubleshoot] オプションを選択することにより、Cisco Unified CallManager の管理ページで 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、[Delete] オプションと [Troubleshoot] オプションは表示されません。

LSC または MIC が電話機に存在するかどうかは、電話機のセキュリティ設定を確認することによっても判別できます。詳細については、このバージョンの Cisco Unified CallManager をサポートする Cisco Unified IP Phone 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。

- 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、[P.6-1 の「Certificate Authority Proxy Function の使用方法」](#)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] 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] 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

詳細については、[P.7-14 の「関連項目」](#)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 7905 および 7912 ( SIP プロトコルのみ ): LD <MAC>.x
- Cisco Unified IP Phone 7940 および 7960 ( SIP プロトコルのみ ): SIP<MAC>.cnf.enc.sgn
- Cisco Unified IP Phone 7911、7941、7961、7970、および 7971 : SEP<MAC>.cnf.xml.enc.sgn

詳細については、暗号化とこのバージョンの Cisco Unified CallManager をサポートする Cisco Unified IP Phone 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 CallManager の管理ページの電話機セキュリティ プロファイルで [ TFTP 暗号化 ] 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 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、ダイジェストクレデンシャル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 CallManager データベースに残ります。

Cisco Unified IP Phone 7911、7941、7961、7970、および 7971 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 7940/7960/7905/7912 ( 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 7940 および 7960 ( 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 7905 および 7912 ( 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 クレデンシャルの除外

初期設定後に電話機に送信される設定ファイルからダイジェスト クレデンシャルを除外するには、電話機に適用されるセキュリティ プロファイルの[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 7905、7912、7940、および 7960 (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 クレデンシャルを変更した場合は、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、[P.7-6](#)の「[暗号化された設定ファイルの設定のヒント](#)」を参照してください。

### 追加情報

詳細については、[P.7-14](#)の「[関連項目](#)」を参照してください。

## その他の情報

### 関連項目

- [電話機設定ファイルの暗号化について \(P.7-2\)](#)
- [サポートされる電話機のモデル \(P.7-5\)](#)
- [暗号化された設定ファイルの設定のヒント \(P.7-6\)](#)
- [暗号化設定ファイルの設定用チェックリスト \(P.7-7\)](#)
- [電話機設定ファイルの暗号化の有効化 \(P.7-8\)](#)
- [鍵の手動配布の設定 \(P.7-8\)](#)
- [鍵の手動配布の設定内容 \(P.7-9\)](#)
- [電話機での対称キーの入力 \(P.7-10\)](#)
- [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 \(P.7-11\)](#)
- [電話機設定ファイルが暗号化されていることの確認 \(P.7-12\)](#)
- [電話機設定ファイルの暗号化の無効化 \(P.7-12\)](#)
- [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 クレデンシャルの除外 \(P.7-13\)](#)
- [Certificate Authority Proxy Function の使用方法 \(P.6-1\)](#)
- [電話機セキュリティ プロファイルの設定のヒント \(P.5-2\)](#)

### シスコの関連マニュアル

- [Cisco Unified CallManager 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](#)



## SIP 電話機のダイジェスト認証の設定

電話機に対してダイジェスト認証を設定すると、Cisco Unified CallManager は、キープアライブメッセージ以外のすべての SIP 電話機要求でチャレンジを行います。Cisco Unified CallManager 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クレデンシャルを使用して、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 CallManager 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クレデンシャルを使用します。

SIP 電話機でのダイジェスト認証の動作の詳細については、[P.1-18 の「ダイジェスト認証」](#)を参照してください。

シスコ以外の SIP 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 CallManager 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 \(P.8-2\)](#)
- [ダイジェスト認証サービス パラメータの設定 \(P.8-3\)](#)
- [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 クレデンシャルの設定 \(P.8-4\)](#)
- [エンドユーザダイジェストクレデンシャルの設定内容 \(P.8-5\)](#)
- [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 \(P.8-5\)](#)
- [その他の情報 \(P.8-6\)](#)

## SIP 電話機ダイジェスト認証の設定用チェックリスト

SIP 電話機にダイジェスト認証を設定する作業を表 8-1 で説明します。

表 8-1 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
<b>ステップ 1</b> SIP 電話機のセキュリティ プロファイルを設定します。[ <b>ダイジェスト認証を有効化 (Enable Digest Authentication)</b> ] 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。	<b>電話機セキュリティ プロファイルの設定 (P.5-1)</b>
<b>ステップ 2</b> SIP 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。	<b>電話機セキュリティ プロファイルの設定 (P.5-1)</b>
<b>ステップ 3</b> 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。	<b>ダイジェスト認証サービス パラメータの設定 (P.8-3)</b>
<b>ステップ 4</b> [ <b>エンドユーザの設定 (End User Configuration)</b> ] ウィンドウで、ダイジェスト クレデンシャルを設定します。	<ul style="list-style-type: none"> <li>• <b>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 クレデンシャルの設定 (P.8-4)</b></li> <li>• <b>エンドユーザダイジェストクレデンシャルの設定内容 (P.8-5)</b></li> </ul>
<b>ステップ 5</b> [ <b>電話の設定 (Phone Configuration)</b> ] ウィンドウで [ <b>ダイジェストユーザ (Digest User)</b> ] を選択します。  7970、7971、7961G/41G、7961GE/41GE、および 7911 などの Cisco Unified IP Phone (SIP のみ) 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クレデンシャルが含まれます。	<b>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.8-5)</b>
<b>ステップ 6</b> Cisco Unified IP Phone 7940 または 7960 (SIP のみ) では、[ <b>エンドユーザの設定 (End User Configuration)</b> ] ウィンドウで設定したダイジェスト クレデンシャルを入力します。	電話機で認証名と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 CallManager をサポートする『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。

## ダイジェスト認証サービスパラメータの設定

電話機でのチャレンジ用の SIP レalm 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 CallManager はデフォルト設定として ccmsipline を指定します。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 CallManager の管理ページで [ システム ] > [ サービスパラメータ ] の順に選択します。
- 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。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** [ 保存 ] をクリックします。

### 追加情報

詳細については、P.8-6 の「[関連項目](#)」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 クレデンシャルの設定

次の手順では、Cisco Unified CallManager 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 クレデンシャルを設定するには、次の手順を実行します。

### 手順

- 
- ステップ 1** 『Cisco Unified CallManager 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 8-2](#) 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 ] をクリックします。
  - ステップ 4** その他のエンド ユーザについて、この手順を繰り返し、ダイジェスト クレデンシャルを設定します。
- 

### 追加の手順

[ エンドユーザの設定 (End User Configuration) ] ウィンドウでダイジェスト クレデンシャルを設定した後、[ 電話の設定 (Phone Configuration) ] ウィンドウにアクセスして、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 SIP IP Phone 7960 または 7940 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クレデンシャルを入力します。

### 追加情報

詳細については、[P.8-6](#) の「[関連項目](#)」を参照してください。

## エンドユーザダイジェストクレデンシャルの設定内容

表 8-2 で、Cisco Unified CallManager 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クレデンシャルの設定について説明します。関連する手順については、P.8-5 の「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」を参照してください。

表 8-2 ダイジェストクレデンシャル

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 ) ]	ダイジェストクレデンシャル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 CallManager 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 ] をクリックします。
- ステップ 4 [ リセット ] をクリックします。

エンドユーザを電話機と関連付けたら、設定を保存して電話機をリセットします。

### 追加情報

詳細については、P.8-6 の「関連項目」を参照してください。

## その他の情報

### 関連項目

- [ダイジェスト認証 \(P.1-18\)](#)
- [電話機セキュリティ プロファイルの設定 \(P.5-1\)](#)
- [SIP 電話機ダイジェスト認証の設定用チェックリスト \(P.8-2\)](#)
- [ダイジェスト認証サービス パラメータの設定 \(P.8-3\)](#)
- [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 クレデンシャルの設定 \(P.8-4\)](#)
- [エンドユーザダイジェストクレデンシャルの設定内容 \(P.8-5\)](#)
- [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 \(P.8-5\)](#)

### シスコの関連マニュアル

*Cisco SIP IP Phone アドミニストレータガイド*



## 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 CallManager 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 設定の無効化 \( P.9-1 \)](#)
- [Web Access 設定の無効化 \( P.9-2 \)](#)
- [PC Voice VLAN Access 設定の無効化 \( P.9-2 \)](#)
- [Setting Access 設定の無効化 \( P.9-2 \)](#)
- [PC Port 設定の無効化 \( P.9-2 \)](#)
- [電話機設定のセキュリティ強化 \( P.9-3 \)](#)
- [その他の情報 \( P.9-4 \)](#)

### Gratuitous ARP 設定の無効化

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 Access 設定の無効化

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 Quality Report Tool 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。さまざまな Cisco Unified IP Phone モデルがそれぞれの方法でこの機能を使用しています。

- Cisco Unified IP Phone 7940/7960 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する。
- Cisco Unified IP Phone 7970 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する。
- Cisco Unified IP Phone 7912 は、この機能を実行できない。

## 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、[ Contrast (コントラスト) ] [ Ring Type (呼出音タイプ) ] [ Network Configuration (ネットワークの設定) ] [ Model Information (モデル情報) ] および [ Status (ステータス) ] 設定があります。

これらの設定は、Cisco Unified CallManager の管理ページ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 [ Contrast (コントラスト) ]、[ Ring Type (呼出音タイプ) ] [ Network Configuration (ネットワークの設定) ] [ Model Information (モデル情報) ] [ Status (ステータス) ] および [ Volume (音量) ] 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 CallManager の管理ページで [ 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 CallManager 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 ポート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 CallManager の管理ページで [ デバイス ] > [ 電話 ] 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 ] 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 ] 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 ] をクリックします。
- ステップ 7** [ リセット ] をクリックします。

### 追加情報

詳細については、P.9-4 の「関連項目」を参照してください。

## その他の情報

### 関連項目

- [Gratuitous ARP 設定の無効化 \( P.9-1 \)](#)
- [Web Access 設定の無効化 \( P.9-2 \)](#)
- [PC Voice VLAN Access 設定の無効化 \( P.9-2 \)](#)
- [Setting Access 設定の無効化 \( P.9-2 \)](#)
- [PC Port 設定の無効化 \( P.9-2 \)](#)
- [電話機設定のセキュリティ強化 \( P.9-3 \)](#)

### シスコの関連マニュアル

*Cisco Unified IP Phone アドミニストレーションガイド for Cisco Unified CallManager*



# 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 \(P.10-1\)](#)
- [ボイスメール セキュリティの設定のヒント \(P.10-2\)](#)
- [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 \(P.10-3\)](#)
- [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 \(P.10-4\)](#)
- [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 \(P.10-5\)](#)
- [その他の情報 \(P.10-6\)](#)

## ボイスメールのセキュリティの概要

Cisco Unified CallManager ボイスメール ポートおよび Cisco Unity SCCP 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。

デバイス セキュリティ モードが認証のみまたは暗号化になっている場合、Cisco Unity-CM TSP は Cisco Unified CallManager TLS ポートを介して Cisco Unified CallManager 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 TSP は Cisco Unified CallManager SCCP ポートを介して Cisco Unified CallManager に接続します。



(注)

このマニュアルでは、サーバという用語は Cisco Unified CallManager クラスタ内の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。

- このバージョンの Cisco Unified CallManager では Cisco Unity 4.0(5) 以降を実行する必要があります。
- Cisco Unity Telephony Integration Manager を使用して Cisco Unity のセキュリティ 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は、『Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity 4.x』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管理ページ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。この作業の詳細については、『Cisco Unified Communications Operating System アドミニストレーションガイド』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ページ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、ボイスメール機能は Cisco Unified CallManager 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 で指定する設定は、Cisco Unified CallManager の管理ページ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 Unified CallManager の管理ページの[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 Cisco Unified CallManager と Cisco Unity で一致しない場合は、Cisco Unity ポートが Cisco Unified CallManager に登録できず、Cisco Unity 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 CallManager デバイスをリセットして Cisco Unity ソフトウェアを再起動する必要があります。Cisco Unified CallManager の管理ページで、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、Cisco Unity 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場合は、表 10-1 を参照してください。

表 10-1 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
<b>ステップ 1</b> Cisco CTL クライアントを混合モードでインストールし設定したことを確認します。	Cisco CTL クライアントの設定 (P.3-1)
<b>ステップ 2</b> 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.4-1) 電話機セキュリティ プロファイルの設定 (P.5-1)
<b>ステップ 3</b> Cisco Unified Communications オペレーティングシステムの管理ページの証明書管理機能を使用して、クラスタ内の各サーバの信頼ストアに Cisco Unity 証明書をコピーします。次に、各サーバで Cisco CallManager サービスを再起動します。	<ul style="list-style-type: none"> <li>ボイスメール セキュリティの設定のヒント (P.10-2)</li> <li>Cisco Unified Communications Operating System アドミニストレーションガイド</li> <li>Cisco Unified CallManager Serviceability アドミニストレーションガイド</li> </ul>
<b>ステップ 4</b> Cisco Unified CallManager の管理ページで、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。	<ul style="list-style-type: none"> <li>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.10-4)</li> <li>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.10-5)</li> </ul>
<b>ステップ 5</b> Cisco Unity 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 Unified CallManager 5.0 Integration Guide for Cisco Unity 4.x
<b>ステップ 6</b> Cisco Unified CallManager の管理ページでデバイスをリセットし、Cisco Unity ソフトウェアを再起動します。	<ul style="list-style-type: none"> <li>Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity 4.x</li> <li>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.10-4)</li> </ul>

## 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 \(P.10-1\)](#)
- [ボイスメールセキュリティの設定のヒント \(P.10-2\)](#)
- [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 \(P.10-3\)](#)

### 手順

- 
- ステップ 1** 『Cisco Unified CallManager 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** ] 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。デフォルト値は未選択です。
- ステップ 3** [ **保存** ] をクリックします。
- ステップ 4** [ **リセット** ] をクリックします。
- 

### 追加情報

詳細については、[P.10-6](#) の「[関連項目](#)」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、P.10-4の「[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](#)」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 \(P.10-1\)](#)
- [ボイスメールセキュリティの設定のヒント \(P.10-2\)](#)
- [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 \(P.10-3\)](#)

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 CallManager の管理ページで、[ボイスメール] > [Cisco ボイスメールポートウィザード] 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] 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] 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] 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。デフォルト値は未選択です。
  - ステップ 5** 『Cisco Unified CallManager 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] をクリックします。
  - ステップ 6** 『Cisco Unified CallManager 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] をクリックします。
- 

### 追加情報

詳細については、P.10-6の「[関連項目](#)」を参照してください。

## その他の情報

### 関連項目

- システム要件 (P.1-4)
- 相互作用および制限 (P.1-6)
- 証明書 (P.1-14)
- 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.10-1)
- ボイスメール セキュリティの設定のヒント (P.10-2)
- 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.10-4)
- 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.10-5)

### シスコの関連マニュアル

- *Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity 4.x*
- *Cisco Unified Communications Operating System アドミニストレーション ガイド*



**PART 3**

**Cisco CTI、JTAPI、および  
TAPI アプリケーションのセキュリティ**







# CTI、JTAPI、および TAPI の認証 および暗号化の設定

この章では、CTI、JTAPI、および TAPI アプリケーションを保護する方法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および暗号化を設定するために、Cisco Unified CallManager の管理ページ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 CallManager の管理ページで使用できる 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は説明しません。同じく、このマニュアルでは、CTI 制御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 \(P.11-2\)](#)
- [CTI、JTAPI、および TAPI アプリケーションの暗号化について \(P.11-4\)](#)
- [CTI、JTAPI、および TAPI アプリケーションに対する CAPF の概要 \(P.11-5\)](#)
- [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 \(P.11-6\)](#)
- [CTI、JTAPI、および TAPI のセキュリティ設定用チェックリスト \(P.11-7\)](#)
- [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 ユーザおよびエンド ユーザの追加 \(P.11-9\)](#)
- [Certificate Authority Proxy Function サービスのアクティブ化 \(P.11-11\)](#)
- [CAPF サービス パラメータの更新 \(P.11-11\)](#)
- [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 \(P.11-12\)](#)
- [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 \(P.11-13\)](#)
- [アプリケーションユーザ CAPF プロファイル ウィンドウおよび エンドユーザ CAPF プロファイル ウィンドウの CAPF 設定 \(P.11-14\)](#)
- [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 \(P.11-16\)](#)
- [JTAPI/TAPI セキュリティ関連サービス パラメータ \(P.11-17\)](#)
- [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 \(P.11-17\)](#)
- [その他の情報 \(P.11-18\)](#)

## CTI、JTAPI、および TAPI アプリケーションの認証について

Cisco Unified CallManager 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 とアプリケーションは、相互認証 TLS ハンドシェイク (証明書交換) で相手の ID を確認します。TLS 接続が発生すると、CTIManager とアプリケーションは、TLS ポート (ポート 2749) で 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 CallManager 証明書 (Cisco Unified CallManager のインストール時に Cisco Unified CallManager 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 CallManager 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、P.3-1 の「Cisco CTL クライアントの設定」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、Cisco Unified CallManager の 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。たとえば、Cisco Unified CallManager Assistant が、クラスタ内の 2 つの異なるノードで 2 つのサービス インスタンスを実行している場合、各インスタンスに独自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 CallManager 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 11-2 の説明に従い、Cisco Unified CallManager の管理ページ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的インスタンス 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。

アプリケーションに対して TLS を有効にするには、前述の作業に加えて、Cisco Unified CallManager の管理ページで、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 CallManager Assistant、Cisco QRT、および Cisco WebDialer は暗号化をサポートしません。CTIManager サービスに接続する CTI クライアントは、クライアントが音声パケットを送信する場合、暗号化をサポートしないことがあります。

アプリケーションと CTIManager の間のメディア ストリームを保護するには、Cisco Unified CallManager の管理ページで、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 グループに追加する必要があります。クラスタ セキュリティ モードが混合モードの場合、アプリケーション ユーザおよびエンド ユーザをこのグループと Standard CTI Secure Connection ユーザ グループに追加すると、CTIManager はアプリケーションとの TLS 接続を確立し、メディア イベントでアプリケーションに鍵関連情報を提供します。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。アプリケーションが SRTP 鍵関連情報を記録または格納しないことに注意してください。

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 CallManager 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 CallManager と共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する。
- 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) を発行する。
- 既存のローカルで有効な証明書をアップグレードする。
- 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する。

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 CallManager 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、セキュア アプリケーション ユーザにローカルで有効な証明書を発行できます。証明書を発行し、その他のセキュリティ関連作業を実行すると、CTIManager サービスとアプリケーションの間で、TLS 接続が開始されます。  
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できます。それによって、CTI クライアントは TLS 接続で CTIManager サービスと通信します。



### 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)] ウィンドウのクラスタセキュリティ モードが 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 11-1 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 11-1 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
<p><b>ステップ 1</b> 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。</p> <p> <b>ヒント</b> アプリケーション ユーザは、Standard CTI Enabled グループに割り当てられている必要があります。</p>	<ul style="list-style-type: none"> <li>『Cisco Unified CallManager システムガイド Release 5.1』の「コンピュータ テレフォニー統合」</li> <li>Cisco JTAPI インストレーション ガイド for Cisco Unified CallManager 5.1</li> <li>Cisco TAPI インストレーション ガイド for Cisco Unified CallManager 5.1</li> <li>Cisco Unified CallManager アドミニストレーション ガイド</li> </ul>
<p><b>ステップ 2</b> 次の CallManager 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)。</p> <ul style="list-style-type: none"> <li>CTL ファイルが作成されるように、5.1(3) 用の 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。</li> <li>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。</li> <li>CAPF 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。必要に応じて、CAPF サービス パラメータを更新します。</li> </ul> <p> <b>ヒント</b> 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。</p> <ul style="list-style-type: none"> <li>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。</li> </ul> <p> <b>ヒント</b> 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。</p>	<ul style="list-style-type: none"> <li><a href="#">Cisco CTL クライアントの設定(P.3-1)</a></li> <li><a href="#">CAPF サービス パラメータの更新(P.11-11)</a></li> <li>Cisco Unified CallManager アドミニストレーション ガイド</li> </ul>
<p><b>ステップ 3</b> 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。</p> <p> <b>ヒント</b> 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ができません。</p>	<p><a href="#">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 ユーザおよびエンド ユーザの追加 (P.11-9)</a></p>

## ■ CTI、JTAPI、および TAPI のセキュリティ設定用チェックリスト

表 11-1 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
<p><b>ステップ 4</b> SRTP を使用して CTIManager とアプリケーションの間のメディア ストリームを保護する場合は、アプリケーション ユーザまたはエンド ユーザを Standard CTI Allow Reception of SRTP Key Material ユーザ グループに追加します。</p> <p>ユーザはすでに Standard CTI Enabled and 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。</p> <p>Cisco Unified CallManager Assistant、Cisco QRT、および Cisco WebDialer は暗号化をサポートしません。CTIManager サービスに接続する CTI クライアントは、クライアントが音声パケットを送信する場合、暗号化をサポートしないことがあります。</p>	<p>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 ユーザおよびエンド ユーザの追加 (P.11-9)</p> <p>『Cisco Unified CallManager アドミニストレーションガイド』の「権限の設定」</p>
<p><b>ステップ 5</b> Cisco Unified CallManager の管理ページで、アプリケーション ユーザ CAPF プロファイルまたはエンド ユーザ CAPF プロファイルを設定します。</p>	<ul style="list-style-type: none"> <li>• CTI、JTAPI、および TAPI アプリケーションに対する CAPF の概要 (P.11-5)</li> <li>• 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.11-13)</li> <li>• アプリケーションユーザ CAPF プロファイル ウィンドウおよび エンド ユーザCAPFプロファイルウィンドウの CAPF 設定 (P.11-14)</li> </ul>
<p><b>ステップ 6</b> 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。</p>	<p>JTAPI/TAPI セキュリティ関連サービス パラメータ (P.11-17)</p>

## 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 ユーザおよびエンド 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 CallManager の管理ページに表示されます。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、両方に割り当ててはできません。

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 CallManager 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 Unified CMQRTSecureSysUser、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

アプリケーション ユーザまたはエンド ユーザをユーザグループから削除する方法については、『Cisco Unified CallManager 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) ] ウィンドウのセキュリティ関連設定の詳細については、『Cisco Unified CallManager 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 CallManager の管理ページで [ ユーザ管理 ] > [ ユーザグループ ] 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 ] をクリックします。
- ステップ 3** 目的に応じて、次の作業のいずれか 1 つを実行します。

- 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する。
- [ 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する。
- [ 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する。

**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](#)] 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、[\[ 検索 \]](#) をクリックします。

検索条件を指定せずに [\[ 検索 \]](#) 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、[\[ 選択項目の追加 \]](#) 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](#)] 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、[\[ 検索 \]](#) をクリックします。

検索条件を指定せずに [\[ 検索 \]](#) 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、[\[ 選択項目の追加 \]](#) 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

詳細については、[P.11-18](#) の「[関連項目](#)」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 CallManager では、Cisco Unified CallManager Serviceability で Certificate Authority Proxy Function サービスが自動的にアクティブになりません。Certificate Authority Proxy Function サービスのアクティブ化の詳細については、『Cisco Unified CallManager Serviceability アドミニストレーションガイド』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、P.3-15 の「CTL ファイルの更新」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 に固有な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 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。

CAPF サービス パラメータが、Cisco Unified CallManager の管理ページで Active として表示されるようにするには、Cisco Unified CallManager Serviceability で、Certificate Authority Proxy Function サービスをアクティブに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 CallManager の管理ページで [システム] > [サービスパラメータ] の順に選択します。
- 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、最初の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 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 CallManager Serviceability 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

詳細については、P.11-18 の「関連項目」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** アクセスするプロファイルに応じて、Cisco Unified CallManager の管理ページで次のオプションのどちらかを選択します。

- [ ユーザ管理 ] > [ アプリケーションユーザ CAPF プロファイル ]
- [ ユーザ管理 ] > [ エンドユーザ CAPF プロファイル ]

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** ドロップダウン リスト ボックスから、表示するプロファイルの検索条件を選択し、[ 検索 ] をクリックします。



**(注)** データベースに登録されているすべて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 プロファイルを検索するには、検索条件を指定せずに、[ 検索 ] をクリックします。

ウィンドウが更新され、検索条件と一致するプロファイルが表示されます。

**ステップ 3** 表示するプロファイルの [ インスタンス ID ( Instance Id ) ] リンク、[ アプリケーションユーザ ( Application User ) ] リンク ( アプリケーション ユーザ CAPF プロファイルのみ ) または [ エンドユーザ ID ( End User Id ) ] リンク ( エンド ユーザ CAPF プロファイルのみ ) をクリックします。



**ヒント** 検索結果の中で [ インスタンス ID ( Instance Id ) ] [ アプリケーションユーザ ( Application User ) ] ( アプリケーション ユーザ CAPF プロファイルのみ ) または [ エンドユーザ ID ( End User Id ) ] ( エンド ユーザ CAPF プロファイルのみ ) を検索するには、[ 絞り込み ] チェックボックスをオンにし、この手順の説明に従って検索条件を入力し、[ 検索 ] をクリックします。

選択した項目が表示されます。

### 追加情報

詳細については、[P.11-18 の「関連項目」](#)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 11-2 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が推奨されます。

## 手順

**ステップ 1** Cisco Unified CallManager の管理ページで、次のオプションのどちらかを選択します。

- [ ユーザ管理 ] > [ アプリケーションユーザ CAPF プロファイル ]
- [ ユーザ管理 ] > [ エンドユーザ CAPF プロファイル ]

検索と一覧表示ウィンドウが表示されます。

**ステップ 2** 次の作業のどちらかを実行します。

- 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 ] 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 ] ボタンまたはアイコン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のコピーするには、P.11-12 の「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」の説明に従って適切なプロファイルを見つけて表示し、[ コピー ( Copy ) ] ボタンをクリックします。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、P.11-12 の「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」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 11-2 の説明に従って、設定内容を入力します。

**ステップ 4** [ 保存 ] 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。

## 追加の手順

[ 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 Unified CMQRTSecureSysUser、IPMASecureSysUser、または WDSecureSysUser を設定する場合は、P.11-17 の「JTAPI/TAPI セキュリティ関連サービス パラメータ」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

詳細については、P.11-18 の「関連項目」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 ウィンドウおよび エンドユーザ CAPF プロファイル ウィンドウの CAPF 設定

表 11-2 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 プロファイルの画面の CAPF 設定について説明します。

- 設定のヒントについては、P.11-6 の「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」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、P.11-18 の「関連項目」を参照してください。

表 11-2 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 ]	<p>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。これにより、設定されたアプリケーション ユーザが表示されます。</p> <p>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。</p>
[ エンドユーザ ]	<p>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。これにより、設定されたエンド ユーザが表示されます。</p> <p>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。</p>
[ インスタンス ID ]	<p>1 ~ 128 字の英数字および特殊文字を入力します。特殊文字は、ドット (.)、ダッシュ (-)、アンダースコア (_) を使用できます。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。</p> <p>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必要です。</p> <p>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、P.11-17 の「JTAPI/TAPI セキュリティ関連 サービス パラメータ」を参照してください。</p>
[ 証明書の操作 (Certificate Operation) ]	<p>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。</p> <ul style="list-style-type: none"> <li>• [ 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)。</li> <li>• [ 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。</li> </ul>

表 11-2 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 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 ] 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 ]	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 秒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 CallManager 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 ( 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 パラメータと組み合わせて使用します。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 CallManager 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 CallManager の管理ページからアプリケーション 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 ] ドロップダウン リストボックスから [ 依存関係レコード ] を選択して、[ 移動 ] 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、[ 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 CallManager システム ガイド』を参照してください。

### 手順

**ステップ 1** P.11-12 の「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」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。

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 ] アイコンまたは [ 選択項目の削除 ] ボタンをクリックします。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 ] をクリックしてから [ 選択項目の削除 ] をクリックします。

**ステップ 2** 単一の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 ] をクリックします。
- 検索と一覧表示ウィンドウで、プロファイルの [ インスタンス ID (Instance Id) ] リンクをクリックします。指定した [ 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) ] ウィンドウが表示されたら、[ 選択項目の削除 ] 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 ] をクリックして削除操作を取り消します。

### 追加情報

詳細については、P.11-18 の「関連項目」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、Web サービスまたはアプリケーションに対して、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 CallManager の管理ページで [システム] > [サービスパラメータ] の順に選択します。
- 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、Web サービスまたはアプリケーション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、Web サービスまたはアプリケーションを選択します。
- 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] 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。

## その他の情報

### 関連項目

- [Cisco CTL クライアントの設定 \(P.3-1\)](#)
- [CTI、JTAPI、および TAPI アプリケーションの認証について \(P.11-2\)](#)
- [CTI、JTAPI、および TAPI アプリケーションの暗号化について \(P.11-4\)](#)
- [CTI、JTAPI、および TAPI アプリケーションに対する CAPF の概要 \(P.11-5\)](#)
- [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 \(P.11-6\)](#)
- [CTI、JTAPI、および TAPI のセキュリティ設定用チェックリスト \(P.11-7\)](#)
- [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およびエンドユーザの追加 \(P.11-9\)](#)
- [Certificate Authority Proxy Function サービスのアクティブ化 \(P.11-11\)](#)
- [CAPF サービスパラメータの更新 \(P.11-11\)](#)
- [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 \(P.11-12\)](#)
- [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 \(P.11-13\)](#)
- [アプリケーションユーザ CAPF プロファイルウィンドウおよびエンドユーザ CAPF プロファイルウィンドウの CAPF 設定 \(P.11-14\)](#)
- [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 \(P.11-16\)](#)
- [JTAPI/TAPI セキュリティ関連サービスパラメータ \(P.11-17\)](#)
- [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 \(P.11-17\)](#)

### シスコの関連マニュアル

- [Cisco JTAPI インストレーションガイド for Cisco Unified CallManager](#)
- [Cisco TAPI インストレーションガイド for Cisco Unified CallManager](#)
- 『Cisco Unified CallManager システムガイド』の「コンピュータテレフォニー統合」
- [Cisco Unified CallManager アドミニストレーションガイド](#)



## PART 4

### SRST リファレンス、トランク、および ゲートウェイのセキュリティ







# Survivable Remote Site Telephony (SRST) リファレンス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。

- [SRST のセキュリティの概要 \(P.12-1\)](#)
- [SRST セキュリティの設定のヒント \(P.12-2\)](#)
- [SRST のセキュリティ設定用チェックリスト \(P.12-3\)](#)
- [SRST リファレンスのセキュリティ設定 \(P.12-4\)](#)
- [SRST リファレンスのセキュリティの設定内容 \(P.12-6\)](#)
- [SRST リファレンスからのセキュリティの削除 \(P.12-7\)](#)
- [SRST 証明書がゲートウェイから削除された場合 \(P.12-7\)](#)
- [その他の情報 \(P.12-8\)](#)

## SRST のセキュリティの概要

SRST 対応ゲートウェイは、Cisco Unified CallManager 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。

保護された 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 CallManager の管理ページで SRST 設定作業を実行した後、Cisco Unified CallManager 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 サービスを認証します。次に、Cisco Unified CallManager 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 CallManager データベースに追加します。

Cisco Unified CallManager の管理ページ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 セキュリティの設定のヒント

保護された電話機と SRST 対応ゲートウェイとの接続の安全を確保するため、次の基準が満たされることを確認します。

- SRST リファレンス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クラスタを混合モードに設定した。
- 電話機に認証または暗号化を設定した。
- Cisco Unified CallManager の管理ページで SRST リファレンスを設定した。
- 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 CallManager 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、セキュアな 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 CallManager の管理ページでデバイス 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 CallManager サーバとの非セキュア接続を試行します。
- 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、Cisco Unified CallManager の管理ページ内のセキュリティ関連の設定が無視されます。Cisco Unified CallManager の管理ページ内の設定は削除されませんが、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る、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 CallManager でセキュア SRST リファレンスを設定した場合は、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 Cisco Unified CallManager クラスタ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 Cisco Unified CallManager にフォールバックされません。管理者が SRST ルータの電源を切り、強制的にこれらの電話機を Cisco Unified CallManager に再登録する必要があります。電話機が Cisco Unified CallManager 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 12-1 を使用して、SRST のセキュリティ設定手順を進めます。

表 12-1 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
<b>ステップ 1</b> 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 CallManager 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 CallManager をサポートする『Cisco IOS SRST Version 3.3 System Administrator Guide』これは、次の URL で入手できます。  <a href="http://www.cisco.com/univercd/cc/td/doc/product/voice/srst/srst33/srst33ad/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/voice/srst/srst33/srst33ad/index.htm</a>
<b>ステップ 2</b> 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。	<a href="#">Cisco CTL クライアントの設定 (P.3-1)</a>
<b>ステップ 3</b> 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。
<b>ステップ 4</b> 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。	<a href="#">電話機セキュリティ プロファイルの適用 (P.5-12)</a>
<b>ステップ 5</b> Cisco Unified CallManager の管理ページで SRST リファレンスにセキュリティを設定します。これには、[デバイスプール設定 (Device Pool Configuration)] ウィンドウで SRST リファレンスを有効にする作業も含まれます。	<a href="#">SRST リファレンスのセキュリティ設定 (P.12-4)</a>
<b>ステップ 6</b> SRST 対応ゲートウェイと電話機をリセットします。	<a href="#">SRST リファレンスのセキュリティ設定 (P.12-4)</a>

## SRST リファレンスのセキュリティ設定

Cisco Unified CallManager の管理ページで SRST リファレンスを追加、更新、または削除する前に、次の点を考慮してください。

- 保護された SRST リファレンスの追加：初めて SRST リファレンスにセキュリティを設定する場合、表 12-2 で説明するすべての項目を設定する必要があります。
- 保護された SRST リファレンスの更新：Cisco Unified CallManager の管理ページで 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 ] 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 CallManager はクラスタ内の各サーバで、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。
- 保護された SRST リファレンスの削除：保護された SRST リファレンスを削除すると、Cisco Unified CallManager 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 リファレンスを削除する方法については、『Cisco Unified CallManager アドミニストレーションガイド』を参照してください。

SRST リファレンスのセキュリティを設定するには、次の手順を実行します。

### 手順

**ステップ 1** Cisco Unified CallManager の管理ページで [ システム ] > [ SRST ] 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** 次の作業のどちらかを実行します。

- 新しい SRST リファレンスを追加するには、検索ウィンドウで [ 新規追加 ] 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 ] ボタンまたはアイコン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 リファレンスをコピーするには、『Cisco Unified CallManager 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 リファレンスを見つけ、[ コピー (Copy) ] をクリックします。設定ウィンドウが表示され、設定が示されます。
- 既存の SRST リファレンスを更新するには、『Cisco Unified CallManager 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 リファレンスを見つけます。設定ウィンドウが表示され、現在の設定が示されます。

**ステップ 3** 表 12-2 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 リファレンス設定内容の説明については、『Cisco Unified CallManager 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 ] 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 ] 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 ] 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] 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] をクリックします。

**ステップ 8** [閉じる] 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] をクリックします。

---

#### 追加の手順

[デバイスプール設定 (Device Pool Configuration)] ウィンドウで SRST リファレンスが有効になったことを確認します。

#### 追加情報

詳細については、[P.12-8 の「関連項目」](#)を参照してください。

## SRST リファレンスのセキュリティの設定内容

表 12-2 で、保護された SRST リファレンスに対して Cisco Unified CallManager の管理ページ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、P.12-2 の「SRST セキュリティの設定のヒント」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、P.12-8 の「関連項目」を参照してください。

表 12-2 SRST リファレンスのセキュリティの設定内容

設定	説明
[セキュア SRST (Is SRST Secure?)]	<p>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。</p> <p>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 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 CallManager データベースに格納します。</p> <p> <b>ヒント</b> 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] をクリックし、従属する電話機をリセットします。</p>
[SRST 証明書プロバイダポート (SRST Certificate Provider Port)]	<p>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 サービスに対する要求を監視します。Cisco Unified CallManager 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 証明書プロバイダのデフォルトポートは 2445 です。</p> <p>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。</p> <p> <b>ヒント</b> 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。</p>
[証明書の更新]	<p> <b>ヒント</b> 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] をクリックした後にだけ表示されます。</p> <p>このボタンをクリックすると、Cisco CTL クライアントは Cisco Unified CallManager 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共に) 電話機に送信します。</p>

## SRST リファレンスからのセキュリティの削除

セキュリティの設定後に SRST リファレンスを非セキュアにするには、Cisco Unified CallManager の管理ページの [ 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ている場合は、その SRST 証明書を Cisco Unified CallManager 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 [ **保存** ] をクリックし、[ **リセット** ] をクリックします。

## その他の情報

### 関連項目

- [SRST のセキュリティの概要 \(P.12-1\)](#)
- [SRST セキュリティの設定のヒント \(P.12-2\)](#)
- [SRST のセキュリティ設定用チェックリスト \(P.12-3\)](#)
- [SRST リファレンスのセキュリティ設定 \(P.12-4\)](#)
- [SRST リファレンスのセキュリティの設定内容 \(P.12-6\)](#)
- [SRST リファレンスからのセキュリティの削除 \(P.12-7\)](#)
- [SRST 証明書がゲートウェイから削除された場合 \(P.12-7\)](#)

### シスコの関連マニュアル

- *Cisco IOS SRST Version 3.3 System Administrator Guide*
- *Cisco Unified CallManager アドミニストレーション ガイド*



# 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 \(P.13-2\)](#)
- [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 \(P.13-3\)](#)
- [SIP トランクの暗号化の概要 \(P.13-4\)](#)
- [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 \(P.13-5\)](#)
- [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 \(P.13-6\)](#)
- [Cisco Unified CallManager 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 \(P.13-6\)](#)
- [SRTP を許可 \(SRTP Allowed\) チェックボックスの設定 \(P.13-7\)](#)
- [その他の情報 \(P.13-8\)](#)

## Cisco IOS MGCP ゲートウェイの暗号化の概要

Cisco Unified CallManager 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せん。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 CallManager 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 CallManager 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 CallManager 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（認証された SCCP 電話機など）とのコールに関わる場合、Cisco Unified CallManager 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 CallManager 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 GUI で IPsec アソシエーションを設定した場合、Cisco Unified CallManager に対して認証ができます。Cisco Unified CallManager 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 アドミニストレーションガイド』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 CallManager に送信されます。Cisco Unified CallManager 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 CallManager の管理ページ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。デバイス設定ウィンドウには、[H.323 Gateway] [H.225 Trunk (Gatekeeper Controlled)] [Inter-Cluster Trunk (Gatekeeper Controlled)] [Inter-Cluster Trunk (Non-Gatekeeper Controlled)] 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 CallManager 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 CallManager 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 CallManager 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 CallManager 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 CallManager 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 CallManager 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 CallManager 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 CallManager 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 CallManager 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 CallManager 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 CallManager 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 CallManager 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。

## SIP トランクの暗号化の概要

セキュア SIP トランクは、TLS 経由のセキュア コールをサポートできます。ただし、シグナリング暗号化はサポートされますが、メディア暗号化 ( SRTP ) はサポートされません。トランクがメディア暗号化をサポートしないため、コールのすべてのデバイスが認証またはシグナリング暗号化をサポートしている場合、通話中に電話機にシールド アイコンが表示されます。

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。

- [ 着信転送タイプ ( Incoming Transport Type ) ] ドロップダウン リスト ボックスで、[ TLS ] を選択
- [ 発信転送タイプ ( Outgoing Transport Type ) ] ドロップダウン リスト ボックスで、[ TLS ] を選択
- [ デバイスセキュリティモード ( Device Security Mode ) ] ドロップダウン リスト ボックスで、[ Encrypted ] 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、トランクに適用します。IPSec をまだ設定していない場合は、設定します。



### ヒント

SIP トランクは、IPSec 設定を使用して、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。Cisco Unified CallManager は、IPSec が正しく設定されていることを確認しません。IPSec を正しく設定しないと、セキュリティ関連情報が公開される可能性があります。

## 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

表 13-1 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](http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a0080357589.html)

表 13-1 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
<b>ステップ 1</b> 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.3-1)
<b>ステップ 2</b> 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.4-1)
<b>ステップ 3</b> IPSec を設定します。   <b>ヒント</b> 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 CallManager 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。	<ul style="list-style-type: none"> <li>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.13-6)</li> <li>Cisco Unified CallManager 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.13-6)</li> </ul>
<b>ステップ 4</b> 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 CallManager 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、Cisco Unified CallManager の管理ページの [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、『 <i>Cisco Unified CallManager アドミニストレーションガイド</i> 』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。
<b>ステップ 5</b> 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)。	<ul style="list-style-type: none"> <li>SIP トランクの暗号化の概要 (P.13-4)</li> <li>SIP トランクセキュリティプロファイルの設定 (P.14-4)</li> </ul>
<b>ステップ 6</b> 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。	<ul style="list-style-type: none"> <li><i>Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways</i></li> </ul>

## 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 CallManager 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 CallManager 自体ではなくインフラストラクチャで IPsec をプロビジョン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](http://www.cisco.com/application/pdf/en/us/guest/netsol/ns241/c649/ccmigration_09186a00801ea79c.pdf)
- 『Cisco IOS Security Configuration Guide, Release 12.2 (or later)』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](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 Series Concentrators、Catalyst 6500 IPsec VPN Services Module、または Cisco Integrated Services Routers を使用できます。
- P.13-5 の「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」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 CallManager 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

Cisco Unified CallManager と、この章で説明しているゲートウェイまたはトランクとの間で IPsec を設定する方法については、『Cisco Unified Communications Operating System アドミニストレーションガイド』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 CallManager の管理ページ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 Trunk ( Gatekeeper Controlled ) のトランク設定ウィンドウ
- Inter-Cluster Trunk ( Gatekeeper Controlled ) のトランク設定ウィンドウ
- Inter-Cluster Trunk ( Non-Gatekeeper Controlled ) の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または非ゲートキーパー制御の H.323/H.245/H.225 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 CallManager 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。
  - ステップ 3** [ 保存 ] をクリックします。
  - ステップ 4** [ リセット ] をクリックして、デバイスをリセットします。
  - ステップ 5** IPSec が正しく設定されたことを確認します。
- 

### 追加情報

詳細については、P.13-8 の「[関連項目](#)」を参照してください。

## その他の情報

### 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 \(P.13-2\)](#)
- [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 \(P.13-3\)](#)
- [SIP トランクの暗号化の概要 \(P.13-4\)](#)
- [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 \(P.13-5\)](#)
- [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 \(P.13-6\)](#)
- [Cisco Unified CallManager 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 \(P.13-6\)](#)

### シスコの関連マニュアル

- *Cisco Unified Communications Operating System アドミニストレーション ガイド*
- *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*
- *Cisco IOS Security Configuration Guide, Release 12.2 (or later)*
- *Voice and Video Enabled IPSec Virtual Private Networks Solution Reference Network Design Guide*



# 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 \(P.14-2\)](#)
- [SIP トランク セキュリティ プロファイルの設定のヒント \(P.14-2\)](#)
- [SIP トランク セキュリティ プロファイルの検索 \(P.14-3\)](#)
- [SIP トランク セキュリティ プロファイルの設定 \(P.14-4\)](#)
- [SIP トランク セキュリティ プロファイルの設定内容 \(P.14-5\)](#)
- [SIP トランク セキュリティ プロファイルの適用 \(P.14-10\)](#)
- [SIP トランク セキュリティ プロファイルの削除 \(P.14-11\)](#)
- [その他の情報 \(P.14-12\)](#)

## SIP トランク セキュリティ プロファイルの概要

Cisco Unified CallManager の管理ページでは、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 CallManager 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 CallManager の管理ページで 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 CallManager 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 CallManager 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** Cisco Unified CallManager の管理ページで、[システム]>[セキュリティプロファイル]>[SIP トランクセキュリティプロファイル]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** ドロップダウン リスト ボックスから、表示するセキュリティ プロファイルの検索条件を選択し、[検索]をクリックします。



**(注)** データベースに登録されているすべての SIP トランク セキュリティ プロファイルを検索するには、検索条件を指定せずに、[検索]をクリックします。

ウィンドウが更新され、検索条件と一致するセキュリティ プロファイルが表示されます。

- ステップ 3** 表示するセキュリティ プロファイルの [名前 (Name)] リンクをクリックします。



**ヒント** 検索結果内の [名前 (Name)] または [説明] を検索するには、[絞り込み] チェックボックスをオンにして、この手順で説明したように検索条件を入力し、[検索]をクリックします。

### 追加情報

詳細については、P.14-12 の「関連項目」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 CallManager の管理ページで、[ システム ] > [ セキュリティプロファイル ] > [ SIP トランクセキュリティプロファイル ] の順に選択します。

**ステップ 2** 次の作業のどちらかを実行します。

- 新しいプロファイルを追加するには、[ 新規追加 ] ボタンをクリックし、[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、[P.14-3](#) の「[SIP トランク セキュリティ プロファイルの検索](#)」の説明に従って適切なプロファイルを見つけて表示し、[ コピー ] ボタンをクリックして、[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、[P.14-3](#) の「[SIP トランク セキュリティ プロファイルの検索](#)」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。

**ステップ 3** [表 14-1](#) 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 ] をクリックします。

### 追加の手順

セキュリティ プロファイルを作成した後、[P.14-10](#) の「[SIP トランク セキュリティ プロファイルの適用](#)」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alm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 クレデンシャルを設定する必要があります (まだ設定していない場合)。

SIP トランクを介して接続され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

詳細については、[P.14-12](#) の「[関連項目](#)」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 14-1 で、SIP トランク セキュリティ プロファイルの設定について説明します。

- 設定のヒントについては、P.14-2 の「SIP トランク セキュリティ プロファイルの設定のヒント」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、P.14-12 の「関連項目」を参照してください。

表 14-1 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]	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]	セキュリティ プロファイルの説明を入力します。
[デバイスセキュリティモード (Device Security Mode)]	<p>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。</p> <ul style="list-style-type: none"> <li>• <b>[ Non Secure ]</b>: イメージ認証以外のセキュリティ機能を適用しない。TCP または UDP 接続で Cisco Unified CallManager が利用できる。</li> <li>• <b>[ Authenticated ]</b>: Cisco Unified CallManager はトランクの整合性と認証を提供する。NULL/SHA を使用する TLS 接続を開始する。</li> <li>• <b>[ Encrypted ]</b>: Cisco Unified CallManager はトランクの整合性、認証、および暗号化を提供する。シグナリング用に、AES128/SHA を使用する TLS 接続を開始する。</li> </ul> <p> <b>(注)</b> SIP トランクは、シグナリング暗号化をサポートします (SRTP はサポートしません)。</p>
[着信転送タイプ (Incoming Transport Type)]	<p>[デバイスセキュリティモード (Device Security Mode)] が <b>[ Non Secure ]</b> である場合、[TCP+UDP] が転送タイプとなります。</p> <p>[デバイスセキュリティモード (Device Security Mode)] が <b>[ Authenticated ]</b> または <b>[ Encrypted ]</b> である場合、[TLS] が転送タイプとなります。</p> <p> <b>(注)</b> Transport Layer Security (TLS) プロトコルによって、Cisco Unified CallManager とトランクとの間の接続が保護されます。</p>

表 14-1 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 ) ]	<p>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。</p> <p>[ デバイスセキュリティモード ( Device Security Mode ) ] が [ Non Secure ] である場合、[ TCP ] または [ UDP ] を選択します。</p> <p>[ デバイスセキュリティモード ( Device Security Mode ) ] が [ Authenticated ] または [ Encrypted ] である場合、[ TLS ] が転送タイプとなります。</p> <p> (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。</p> <p> ヒント TCP 接続の再利用をサポートしていない Cisco Unified CallManager 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 CallManager 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。</p>
[ ダイジェスト認証を有効化 ( Enable Digest Authentication ) ]	<p>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 CallManager 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。</p> <p>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 [ Authenticated ] または [ Encrypted ] を選択します。</p> <p>ダイジェスト認証の詳細については、P.1-18 の「ダイジェスト認証」および P.15-1 の「SIP トランクのダイジェスト認証の設定」を参照してください。</p> <p> 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。</p>
[ ナンス確認時間 ( Nonce Validity Time、分 ) ]	<p>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 CallManager は新しい値を生成します。</p> <p> (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。</p>

表 14-1 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 ) ]	<p>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。</p> <p>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 CallManager 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、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。</p> <p>このフィールドには、4096 文字まで入力できます。</p> <p> <b>ヒント</b> 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。</p> <p>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。</p>
[ 着信ポート ( Incoming Port ) ]	<p>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。</p> <p> <b>ヒント</b> TLS を使用するすべて 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。</p>

表 14-1 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 ) ]	<p>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。</p> <p>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 CallManager 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。</p> <p>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 CallManager 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。</p> <p> <b>ヒント</b> 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。</p>
[ プレゼンス登録の許可 ( Accept Presence Subscription ) ]	<p>トランクのダイジェスト認証設定の詳細については、P.15-1 の「SIP トランクのダイジェスト認証の設定」を参照してください。許可の詳細については、P.1-20 の「許可」および P.1-6 の「相互作用」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 CallManager アドミニストレーションガイド』を参照してください。</p> <p>Cisco Unified CallManager 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。</p> <p>[ 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 [ プレゼンス登録の許可 ( Accept Presence Subscription ) ] チェックボックスをオンにします。</p> <p>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 [ プレゼンス登録の許可 ( 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。</p>

表 14-1 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
[ アウトオブダイアログ REFER の許可 ( Accept Out-of-Dialog REFER )]	<p>Cisco Unified CallManager が SIP トランク経由で着信する非インバイトのアウトオブダイアログ 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。</p> <p>[ 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 [ アウトオブダイアログ REFER の許可 ( Accept Out-of-Dialog REFER )] チェックボックスをオンにします。</p>
[ 未承諾 NOTIFY の許可 ( Accept Unsolicited Notification )]	<p>Cisco Unified CallManager が SIP トランク経由で着信する非インバイトの未承諾 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。</p> <p>[ 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 [ 未承諾 NOTIFY の許可 ( Accept Unsolicited Notification )] チェックボックスをオンにします。</p>
[ REPLACE ヘッダの許可 ( Accept Replaces Header )]	<p>Cisco Unified CallManager 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。</p> <p>[ 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。</p>

## 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 CallManager 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 ] をクリックします。
- ステップ 5** [ リセット ] をクリックして、トランクをリセットします。

### 追加の手順

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 クレデンシャルを設定する必要 があります。P.15-5 の「SIP レルムの設定」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 ャ ユーザの設定 ( Application User Configuration ) ] ウィンドウで、ダイジェスト クレデンシャルと可 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

詳細については、P.14-12 の「関連項目」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 CallManager 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 CallManager 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、[ 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 ] ドロップダウンリストボックスから [ 依存関係レコード ] を選択して、[ 移動 ] 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、[ 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 CallManager システム ガイド』を参照してください。

### 手順

- ステップ 1** P.14-3 の「SIP トランク セキュリティ プロファイルの検索」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、[ 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 ] アイコンまたは [ 選択項目の削除 ] ボタンをクリックします。
- 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。
  - [ 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 ] アイコンまたは [ 選択項目の削除 ] ボタンをクリックします。
  - [ SIP トランクセキュリティプロファイルの検索と一覧表示 ( Find and List SIP Trunk Security Profiles ) ] ウィンドウで、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 [ 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たら、[ 削除 ] アイコンまたは [ 削除 ] ボタンをクリックします。
- 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 ] をクリックして削除操作を取り消します。

### 追加情報

詳細については、P.14-12 の「関連項目」を参照してください。

## その他の情報

### 関連項目

- [SIP トランク セキュリティ プロファイルの概要 \(P.14-2\)](#)
- [SIP トランク セキュリティ プロファイルの設定のヒント \(P.14-2\)](#)
- [SIP トランク セキュリティ プロファイルの検索 \(P.14-3\)](#)
- [SIP トランク セキュリティ プロファイルの設定 \(P.14-4\)](#)
- [SIP トランク セキュリティ プロファイルの設定内容 \(P.14-5\)](#)
- [SIP トランク セキュリティ プロファイルの適用 \(P.14-10\)](#)
- [SIP トランク セキュリティ プロファイルの削除 \(P.14-11\)](#)
- [許可 \(P.1-20\)](#)
- [相互作用 \(P.1-6\)](#)
- [ダイジェスト認証 \(P.1-18\)](#)

### シスコの関連マニュアル

*Cisco Unified CallManager アドミニストレーション ガイド*

*Cisco Unified CallManager システム ガイド*



# 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 CallManager 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 でチャレンジを行います。すると、Cisco Unified CallManager が SIP 要求をトランクに送信したときに、SIP ユーザ エージェントは Cisco Unified CallManager 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、[P.1-18 の「ダイジェスト認証」](#)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 ダイジェスト認証の設定用チェックリスト \(P.15-2\)](#)
- [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 \(P.15-2\)](#)
- [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クレデンシャルの設定 \(P.15-3\)](#)
- [アプリケーション ユーザダイジェストクレデンシャルの設定内容 \(P.15-3\)](#)
- [SIP レルムの検索 \(P.15-4\)](#)
- [SIP レルムの設定 \(P.15-5\)](#)
- [SIP レルムの設定内容 \(P.15-6\)](#)
- [SIP レルムの削除 \(P.15-7\)](#)
- [その他の情報 \(P.15-8\)](#)

## SIP トランク 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 15-1 で説明します。

表 15-1 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
<b>ステップ 1</b> 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。	<ul style="list-style-type: none"> <li>SIP トランク セキュリティ プロファイルの設定 (P.14-4)</li> <li>ダイジェスト認証 (P.1-18)</li> </ul>
<b>ステップ 2</b> 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.14-10)
<b>ステップ 3</b> 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)。  このパラメータを設定すると、Cisco Unified CallManager 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.15-2)
<b>ステップ 4</b> Cisco Unified CallManager が SIP トランクで SIP 要求を送信する SIP ユーザ エージェントの ID でチャレンジを行う場合は、[アプリケーションユーザの設定 (Application User Configuration)] ウィンドウで、アプリケーション ユーザのダイジェスト クレデンシャルを設定します。	<ul style="list-style-type: none"> <li>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 クレデンシャルの設定 (P.15-3)</li> <li>アプリケーション ユーザ ダイジェスト クレデンシャルの設定内容 (P.15-3)</li> </ul>
<b>ステップ 5</b> Cisco Unified CallManager がトランク ピアからのチャレンジに応答する場合は、SIP レルムを設定します。	<ul style="list-style-type: none"> <li>ダイジェスト認証 (P.1-18)</li> <li>SIP レルムの設定 (P.15-5)</li> <li>SIP レルムの設定内容 (P.15-6)</li> </ul>

## 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 CallManager の管理ページで、[システム] > [エンタープライズパラメータ] 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。このパラメータを設定すると、Cisco Unified CallManager 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 クレデンシャルの設定

Cisco Unified CallManager 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 CallManager の管理ページの [ 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 クレデンシャルを設定する必要があります。Cisco Unified CallManager は、これらのクレデンシャルを使用して、SIP トランクで要求を送信する SIP ユーザエージェントの 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 クレデンシャルを設定するには、次の手順を実行します。

### 手順

- ステップ 1** 『Cisco Unified CallManager 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 15-2 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 ] をクリックします。

### 追加情報

詳細については、P.15-8 の「関連項目」を参照してください。

## アプリケーション ユーザ ダイジェスト クレデンシャルの設定内容

表 15-2 で、Cisco Unified CallManager の管理ページの [ 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 クレデンシャル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、P.15-8 の「関連項目」を参照してください。

表 15-2 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 クレデンシャル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 CallManager の管理ページで **[ ユーザ管理 ] > [ SIP レルム ]** の順に選択します。

[ SIP レルムの検索と一覧表示 ( Find and List SIP Realms ) ] 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** ドロップダウン リスト ボックスから、表示する SIP レルムの検索条件を選択し、**[ 検索 ]** をクリックします。



**(注)** データベースに登録されているすべての SIP レルムを検索するには、検索条件を指定せずに、**[ 検索 ]** をクリックします。

ウィンドウが更新され、検索条件と一致する SIP レルムが表示されます。

**ステップ 3** 表示する SIP レルムの **[ レルム ( Realm ) ]** リンクをクリックします。



**ヒント** 検索結果内の **[ レルム ( Realm ) ]** または **[ ユーザ ( User ) ]** を検索するには、**[ 絞り込み ]** チェックボックスをオンにして、この手順で説明したように検索条件を入力し、**[ 検索 ]** をクリックします。

選択した項目が表示されます。

### 追加の手順

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、[P.15-2 の「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」](#)の説明に従って設定します。

### 追加情報

詳細については、[P.15-8 の「関連項目」](#)を参照してください。

## SIP レルムの設定

Cisco Unified CallManager が 1 つ以上のトランク ピアからのチャレンジに応答する場合は、Cisco Unified CallManager 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、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 CallManager の管理ページで [ ユーザ管理 ] > [ SIP レルム ] の順に選択します。

**ステップ 2** 次の作業のどちらかを実行します。

- 新しい SIP レルムを追加するには、[ 新規追加 ] ボタンをクリックし、[ステップ 3](#) に進みます。
- 既存の SIP レルムを更新するには、[P.15-4](#) の「[SIP レルムの検索](#)」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。

**ステップ 3** [表 15-3](#) 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 ] 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。

---

### 追加の手順

ダイジェスト認証を成功させるために、Cisco Unified CallManager 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

詳細については、[P.15-8](#) の「[関連項目](#)」を参照してください。

## SIP レルムの設定内容

Cisco Unified CallManager がトランク ピアからチャレンジを受けるとき、SIP レルムはトランク側のクレデンシャルを提供します。

表 15-3 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、P.15-8 の「関連項目」を参照してください。

表 15-3 SIP レルム セキュリティ プロファイル

設定	説明
[ レルム ]	SIP トランクに接続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 ]	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 CallManager 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 CallManager でチャレンジを行います。
[ ダイジェスト信用証明書 ( Digest Credentials ) ]	このレルムおよびユーザに対するチャレンジに応答するために Cisco Unified CallManager 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 CallManager 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** P.15-4 の「[SIP レルムの検索](#)」の手順に従って、SIP レルムを検索します。

複数の SIP レルムを削除するには、[ SIP レルムの検索と一覧表示 ( Find and List SIP Realms ) ] 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** ] アイコンまたは [ **選択項目の削除** ] ボタンをクリックします。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** ] をクリックしてから [ **選択項目の削除** ] をクリックします。

**ステップ 2** 単一の SIP レルムを削除するには、次の作業のどちらかを実行します。

- [ SIP レルムの検索と一覧表示 ( Find and List SIP Realms ) ] ウィンドウで、適切な SIP 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** ] をクリックします。
- [ SIP レルムの検索と一覧表示 ( Find and List SIP Realms ) ] ウィンドウで、[ **レルム ( Realm )** ] 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** ] 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** ] をクリックして削除操作を取り消します。

---

### 追加情報

詳細については、[P.15-8 の「関連項目」](#)を参照してください。

## その他の情報

### 関連項目

- [ダイジェスト認証 \( P.1-18 \)](#)
- [SIP トランク ダイジェスト認証の設定用チェックリスト \( P.15-2 \)](#)
- [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 \( P.15-2 \)](#)
- [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 クレデンシャルの設定 \( P.15-3 \)](#)
- [アプリケーション ユーザ ダイジェスト クレデンシャルの設定内容 \( P.15-3 \)](#)
- [SIP レルムの検索 \( P.15-4 \)](#)
- [SIP レルムの設定 \( P.15-5 \)](#)
- [SIP レルムの設定内容 \( P.15-6 \)](#)
- [SIP レルムの削除 \( P.15-7 \)](#)



## C

### Certificate Authority Proxy Function (CAPF)

- CAPF サービス 3-6
- CAPF レポートの生成 6-11
- Cisco Unified CallManager Serviceability での設定 6-4
- Cisco Unified IP Phone との相互作用 6-2
- LSC または認証文字列を使用した電話機の検索 6-10
- アプリケーション ユーザまたはエンド ユーザの CAPF プロファイルの検索 11-12
- アプリケーション ユーザまたはエンド ユーザの CAPF プロファイルの削除 11-16
- 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 11-13
- インストール 1-13
- 概要 6-2
  - CTI/JTAPI/TAPI アプリケーションの サービス パラメータの更新 11-5 6-7
  - CTI/JTAPI/TAPI 用の サービスのアクティブ化 11-11 6-6, 11-11
  - 設定内容 (表)
    - CTI/JTAPI/TAPI アプリケーションの 電話機の 11-14 6-9
    - 設定用チェックリスト (表) 6-5
    - 相互作用および要件 6-4
      - CTI/JTAPI/TAPI アプリケーションでの 11-6
  - 認証文字列 6-2
    - 電話機での入力 6-12
  - 表示、アプリケーション ユーザやエンド ユーザへの証明書操作のステータスの ~を使用した電話機証明書の操作 11-17 6-8
- Cisco Unified IP Phone
  - CAPF との相互作用 6-2
  - CTL ファイルの削除 3-23
  - GARP 設定の無効化 9-1
  - PC Port 設定の無効化 9-2

- PC Voice VLAN Access 設定の無効化 9-2
- Setting Access 設定の無効化 9-2
- Web Access 設定の無効化 9-2
- 「暗号化された設定ファイル」も参照
- セキュリティ アイコン 1-5
- セキュリティ 機能について 4-2
- セキュリティ 設定の確認 4-3
- セキュリティの設定用チェックリスト (表) 4-4
- 設定内容 (表)
  - CAPF の 6-9
- 電話機セキュリティ プロファイルの設定のヒント 5-2
- 認証文字列
  - 電話機での入力 6-12
- CTL Provider
  - サービスのアクティブ化 3-5
- CTL クライアント
  - CAPF サービス 3-6
  - CTL Provider サービス 3-5
  - IP Phone 上の CTL ファイルの削除 3-23
  - Smart Card サービスの設定 3-21
  - アップグレード 3-10
  - アンインストール 3-24
  - 移行 3-10
  - インストール 1-13, 3-8
  - 概要 3-2
  - 確認 3-24
  - クラスタ全体のセキュリティ モード 更新 3-17
  - セキュリティ トークン パスワード 変更 3-22
  - セキュリティ モード 確認 3-20
  - 設定 3-11
    - TLS ポート 3-6
  - 設定内容 (表) 3-18
  - 設定のヒント 3-3

- 設定用チェックリスト (表) 3-4
- バージョン
  - 特定 3-24
- CTL ファイル
  - IP Phone での削除 3-23
  - エントリの削除 3-17
  - 更新 3-15
- E
- etoken
  - パスワードの変更 3-22
- H
- HTTPS
  - Internet Explorer による 2-3
  - Netscape による 2-6
  - 概要 2-2
  - 仮想ディレクトリ (表) 2-2
- I
- IP Phone
  - 「Cisco Unified IP Phone」を参照
- IPSec 1-13
  - IPSec の設定用チェックリスト (表) 13-5
  - インフラストラクチャの注意事項 13-6
  - ゲートウェイまたはトランクの注意事項 13-6
  - 推奨事項 13-6
  - 設定 13-6
- J
- JTAPI
  - セキュリティ サービス パラメータの設定 11-17
  - セキュリティの設定用チェックリスト (表) 11-7
- M
- MGCP ゲートウェイ
  - セキュリティの設定用チェックリスト (表) 13-5
  - 設定 13-6
- S
- Secure Sockets Layer (SSL)
  - HTTPS による 2-2
  - インストール 1-13
- Site Administrator Security Token (SAST) 3-2
- SRST
  - セキュリティの概要 12-1
  - セキュリティの設定のヒント 12-2
  - セキュリティの設定用チェックリスト (表) 12-3
  - トラブルシューティング
    - ゲートウェイから削除された証明書 12-7
- SRST リファレンス
  - セキュリティの設定内容 (表) 12-6
  - 設定 12-4
  - トラブルシューティング
    - セキュアなリファレンスの削除 12-7
- T
- TAPI
  - セキュリティ サービス パラメータの設定 11-17
  - セキュリティの設定用チェックリスト (表) 11-7
- Tftp サービス 3-2
- TLS プロキシ サーバ 3-2
- Transport Layer Security (TLS) 1-13
  - ポート 3-6
- あ
- 暗号化
  - CTI/JTAPI/TAPI アプリケーションでの 11-4
  - H.323 ゲートウェイの概要 13-3
  - H.323/H.225/H.245 トランクの概要 13-3
  - MGCP ゲートウェイの概要 13-2
  - SIP トランクの概要 13-4
  - SRTP を許可 (SRTP Allowed) チェックボックスの設定 13-7
  - インストール 1-13
  - 概要 1-22
  - ゲートウェイとトランクの設定用チェックリスト (表) 13-5
  - シグナリング
    - SIP トランクの設定 14-4
    - 電話機用の設定 5-4

- 制限 1-6, 1-7
- 設定と割り込み 1-12
- 設定内容 (表)
  - SCCP 電話機の 5-5
  - SIP 電話機セキュリティ プロファイルの 5-7
  - SIP トランクの 14-5
- 相互作用 1-6
- 電話機用の設定 5-4
- 暗号化された設定ファイル
  - 鍵の手動設定用チェックリスト (表) 7-9
  - 鍵の手動配布 7-2
  - 鍵の手動配布の設定 7-8
  - 確認 7-12
  - 公開鍵による対称キーの暗号化 7-3
  - 公開鍵による対称キーの暗号化の使用 7-11
  - 設定内容 (表)
    - 鍵の手動配布の 7-9
  - 設定のヒント 7-6
  - 設定用チェックリスト (表) 7-7
  - 対称キーの入力 7-10
  - 電話機のサポート 7-5
    - ~について 7-2
  - 無効化 7-12
  - 有効化 7-8
- い
- イメージ認証 1-17
- き
- 許可 1-17
  - SIP トランクの設定 14-4
    - 概要 1-17
    - 設定内容 (表)
      - SIP トランクの 14-5
    - 相互作用 1-6
- こ
- コンピュータテレフォニー インテグレーション (CTI)
  - セキュア ユーザ グループ
    - アプリケーション ユーザおよびエンド ユーザの追加 11-9
- セキュリティの設定用チェックリスト (表) 11-7
- し
- シグナリング暗号化
  - 概要 1-22
- シグナリング認証
  - 概要 1-17
- 証明書
  - Internet Explorer の証明書 2-3
  - Netscape の証明書 2-6
  - 外部 CA 1-14
    - 種類 1-14
- 証明書署名要求 (CSR) 1-14
- せ
- 整合性
  - 概要 1-17
- セキュリティ
  - Cisco Unified CallManager サービスの再起動 1-11
  - CTL クライアントの概要 3-2
  - HTTPS 2-2
  - 暗号化に対する割り込みの使用 1-12
  - 暗号化の概要
    - インストール 1-13
    - 外部 CA 1-14
    - 機能一覧 1-5
    - 機能一覧 (表) 1-5
    - 許可の概要 1-17
    - クラスタのリポート 1-11
    - サーバのリポート 1-11
    - システム要件 1-4
    - 証明書の種類 1-14
    - 制限 1-6, 1-7
    - セキュア クラスタへのサブスクリバ ノードの追加 1-29
    - 相互作用 1-6
    - その他の情報 1-30
    - デバイスのリセット 1-11
    - トークン 3-2, 3-8, 3-11, 3-15, 3-22
    - 認証および暗号化の設定用チェックリスト (表) 1-25
    - 認証の概要 1-17

- ベスト プラクティス 1-11
  - 用語 (表) 1-2
  - セキュリティ プロファイル
    - SIP トランクの概要 14-2
    - SIP トランクの検索 14-3
    - SIP トランクの設定 14-4
    - SIP トランク用の削除 14-11
    - SIP トランク用の適用 14-10
    - 設定内容 (表)
      - SCCP 電話機の 5-5
      - SIP 電話機の 5-7
      - SIP トランクの 14-5
    - 電話機への適用 5-12
    - 電話機用の概要 5-1
    - 電話機用の検索 5-3
    - 電話機用の削除 5-13
    - 電話機用の設定 5-4
    - 電話機用の設定のヒント 5-2
    - ~を使用している電話機の検索 5-14
  - セキュリティ モード
    - クラスタ全体
      - 確認 3-20
      - 設定 3-17
  - 設定ファイルの暗号化
    - 「暗号化された設定ファイル」を参照
- た
- ダイジェスト認証 1-17
    - SIP トランクの設定 14-4
    - SIP レルムの検索 15-4
    - SIP レルムの削除 15-7
    - SIP レルムの設定 15-5
    - クラスタ ID 15-2
    - サービス パラメータの設定 8-3
    - 設定内容 (表)
      - SIP 電話機の 5-7
      - SIP トランクの 14-5
      - SIP レルムの 15-6
      - アプリケーション ユーザ ダイジェスト クレデンシャルの 15-3
      - エンド ユーザの 8-5
    - 設定用チェックリスト (表)
      - SIP トランクの 15-2
      - 電話機の 8-2
    - ダイジェスト クレデンシャルの設定
      - アプリケーション ユーザの 15-3
      - エンド ユーザの 8-4
    - ダイジェスト ユーザと電話機との関連付け 8-5
    - 電話機用の設定 5-4
- て
- デバイス認証 1-17
    - SIP トランクの設定 14-4
    - 設定内容 (表)
      - SCCP 電話機の 5-5
      - SIP 電話機の 5-7
      - SIP トランクの 14-5
    - 電話機用の設定 5-4
  - 転送セキュリティ
    - IPSec 1-13
    - SIP 電話機用の設定 5-4
    - SIP トランクの設定 14-4
    - TLS 1-13
    - 設定内容 (表)
      - SCCP 電話機の 5-5
      - SIP 電話機の 5-7
      - SIP トランクの 14-5
    - ~とセキュア リアルタイム プロトコル (SRTP) 1-13
    - ~とリアルタイム プロトコル (RTP) 1-13
  - 電話機のセキュリティ強化
    - GARP 設定の無効化 9-1
    - PC Port 設定の無効化 9-2
    - PC Voice VLAN Access 設定の無効化 9-2
    - Setting Access 設定の無効化 9-2
    - Web Access 設定の無効化 9-2
    - 設定 9-3
- と
- トラブルシューティング
    - IP Phone 上の CTL ファイルの削除 3-23
    - ゲートウェイから削除された SRST 証明書 12-7
- に
- 認証
    - CTI/JTAPI/TAPI アプリケーションでの 11-2
    - 概要 1-17

- 制限 1-6, 1-7
- 相互作用 1-6
- 「ダイジェスト認証」も参照
- 「デバイス認証」も参照
- 認証文字列 6-2, 11-5
  - 電話機での入力 6-12
  - ~を使用した電話機の検索 6-10
  
- ふ
  
- ファイル認証 1-17
  - 電話機用の設定 5-4
  
- ほ
  
- ボイスメール
  - セキュリティの概要 10-1
  - セキュリティの設定用チェックリスト(表) 10-3
  - セキュリティ要件 10-1
- ボイスメール ポート
  - ウィザードを使用したセキュリティ プロファイルの適用 10-5
  - セキュリティ プロファイルの適用 10-4
  - セキュリティの概要 10-1
  - セキュリティの設定用チェックリスト(表) 10-3
- ポート
  - CTL Provider 3-6
  - Ethernet Phone 3-6
  - SIP Secure 3-6
  
- ま
  
- マニュアル
  - 関連マニュアル xiii
  - 対象読者 xii
  - 表記法 xiii
  - マニュアルの構成 xii
  - 目的 xi
  
- め
  
- メディア暗号化(「暗号化」も参照)
  - 概要 1-22
  
- ろ
  
- ローカルで有効な証明書(LSC)
  - CTI/JTAPI/TAPI アプリケーションでの ~を使用した電話機の検索 11-5 6-10
  
- わ
  
- 割り込み
  - 暗号化制限と 1-12