



**Cisco Unified Communications Manager
セキュリティ ガイド
Cisco Unified Communications Manager
Business Edition 対応**

Release 6.0(1)

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 ドメインバージョンとして、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, GigaStack, 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, RateMUX, ScriptShare, SlideCast, 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.(0612R)

Cisco Unified Communications Manager セキュリティ ガイド Cisco Unified Communications Manager Business Edition 対応
Copyright © 2007 Cisco Systems, Inc.
All rights reserved.



CONTENTS

このマニュアルについて	xi
目的	xi
対象読者	xi
マニュアルの構成	xii
関連マニュアル	xiii
表記法	xiv
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

セキュリティの概要	1-1
用語	1-2
システム要件	1-5
機能一覧	1-6
セキュリティ アイコン	1-7
相互作用および制限	1-8
相互作用	1-8
制限	1-9
トランクのサポート	1-9
認証と暗号化	1-9
割り込みと暗号化	1-10
ワイドバンド コーデックと暗号化	1-10
メディア リソースと暗号化	1-10
電話機のサポートと暗号化	1-11
電話機のサポートおよび暗号化された設定ファイル	1-11
SIP トランクのサポートと暗号化	1-11
セキュリティ アイコンと暗号化	1-11
クラスタおよびデバイス セキュリティ モード	1-12
ダイジェスト認証と暗号化	1-12
パケット キャプチャと暗号化	1-12
ベスト プラクティス	1-13

デバイスのリセット、サービスの再起動またはリブート	1-13
メディア暗号化の設定と割り込み	1-14
インストール	1-14
証明書	1-15
電話機の証明書の種類	1-15
サーバの証明書の種類	1-16
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	1-18
イメージ認証	1-18
デバイス認証	1-18
ファイル認証	1-19
シグナリング認証	1-19
ダイジェスト認証	1-20
許可	1-22
暗号化の概要	1-23
シグナリング暗号化	1-23
メディア暗号化	1-23
設定ファイルの暗号化	1-25
設定用チェックリストの概要	1-26
その他の情報	1-29

CHAPTER 2

HTTP over SSL (HTTPS) の使用方法	2-1
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

Cisco CTL クライアントの設定	3-1
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	3-5
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 クライアントの設定	3-10
CTL ファイルの更新	3-13
CTL ファイル エントリの削除	3-14
Cisco Unified Communications Manager セキュリティ モードの更新	3-15
Cisco CTL クライアントの設定内容	3-16
Cisco Unified Communications Manager のセキュリティ モードの確認	3-19
Smart Card サービスの開始および自動の設定	3-20
セキュリティ トークン パスワード (etoken) の変更	3-21
Cisco Unified IP Phone 上の CTL ファイルの削除	3-22
Cisco CTL クライアントのバージョンの特定	3-23
Cisco CTL クライアントの確認とアンインストール	3-23
その他の情報	3-24

PART 2

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

CHAPTER 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	4-2
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	4-3
その他の情報	4-4

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

Certificate Authority Proxy Function の使用方法 6-1

Certificate Authority Proxy Function の概要	6-2
Cisco Unified IP Phone と CAPF の相互作用	6-3
CAPF システムの相互作用および要件	6-4
Cisco Unified 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

暗号化された電話機設定ファイルの設定	7-1
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	7-13

CHAPTER 8

SIP 電話機のダイジェスト認証の設定	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	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	8-4
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	8-5

CHAPTER 9

電話機のセキュリティ強化	9-1
Gratuitous ARP 設定の無効化	9-1
Web Access 設定の無効化	9-1
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

セキュアな会議リソースの設定	10-1
セキュアな会議の概要	10-2
会議ブリッジの要件	10-3
セキュアな会議のアイコン	10-4
セキュアな会議の保守	10-5
アドホック会議の会議リスト	10-5
最小セキュリティ レベルでのミートミー会議	10-6
Cisco Unified IP Phone サポート	10-7
CTI サポート	10-8
トランクおよびゲートウェイでのセキュアな会議	10-8
CDR データ	10-8
相互作用および制限	10-9
相互作用	10-9
制限	10-9
会議リソースのセキュリティを確保するための設定のヒント	10-11
セキュアな会議ブリッジの設定用チェックリスト	10-12
Cisco Unified Communications Manager の管理ページでのセキュアな会議ブリッジの設定	10-13
ミートミー会議の最小セキュリティ レベルの設定	10-14
セキュアな会議ブリッジの packets キャプチャの設定	10-14
その他の情報	10-15

CHAPTER 11

ボイスメール ポートのセキュリティ設定	11-1
ボイスメールのセキュリティの概要	11-1
ボイスメール セキュリティの設定のヒント	11-2
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	11-3
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	11-4
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	11-5
その他の情報	11-6

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 12

CTI、JTAPI、および TAPI の認証および暗号化の設定 12-1

- CTI、JTAPI、および TAPI アプリケーションの認証について 12-2
- CTI、JTAPI、および TAPI アプリケーションの暗号化について 12-4
- CTI、JTAPI、および TAPI アプリケーションに対する CAPF の概要 12-5
- 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 12-6
- CTI、JTAPI、および TAPI のセキュリティ設定用チェックリスト 12-7
- 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 12-9
- Certificate Authority Proxy Function サービスのアクティブ化 12-10
- CAPF サービス パラメータの更新 12-11
- 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
12-12
- 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
12-13
- アプリケーションユーザ CAPF プロファイルおよびエンドユーザ CAPF プロ
ファイルの CAPF 設定ウィンドウ 12-14
- 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 12-16
- JTAPI/TAPI セキュリティ関連サービス パラメータ 12-17
- 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 12-18
- その他の情報 12-18

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 13

Survivable Remote Site Telephony (SRST) リファレンスのセキュリティ設定
13-1

- SRST のセキュリティの概要 13-1
- SRST セキュリティの設定のヒント 13-2
- SRST のセキュリティ設定用チェックリスト 13-3
- SRST リファレンスのセキュリティ設定 13-4
- SRST リファレンスのセキュリティの設定内容 13-6
- SRST リファレンスからのセキュリティの削除 13-7
- SRST 証明書がゲートウェイから削除された場合 13-7
- その他の情報 13-7

CHAPTER 14

ゲートウェイおよびトランクの暗号化の設定 14-1

- Cisco IOS MGCP ゲートウェイの暗号化の概要 14-2

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	14-3
SIP トランクの暗号化の概要	14-4
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	14-5
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	14-6
Cisco Unified Communications Manager とゲートウェイまたはトランクとの間で IPSec を設定する場合の注意事項	14-6
SRTP を許可 (SRTP Allowed) チェックボックスの設定	14-7
その他の情報	14-8

CHAPTER 15

SIP トランク セキュリティ プロファイルの設定 15-1

SIP トランク セキュリティ プロファイルの概要	15-2
SIP トランク セキュリティ プロファイルの設定のヒント	15-2
SIP トランク セキュリティ プロファイルの検索	15-3
SIP トランク セキュリティ プロファイルの設定	15-4
SIP トランク セキュリティ プロファイルの設定内容	15-5
SIP トランク セキュリティ プロファイルの適用	15-10
SIP トランク セキュリティ プロファイルの削除	15-11
その他の情報	15-12

CHAPTER 16

SIP トランクのダイジェスト認証の設定 16-1

SIP トランク ダイジェスト認証の設定用チェックリスト	16-2
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	16-2
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	16-3
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	16-3
SIP レルムの検索	16-4
SIP レルムの設定	16-5
SIP レルムの設定内容	16-6
SIP レルムの削除	16-7
その他の情報	16-7

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 \(P.xi\)](#)
- [マニュアルの構成 \(P.xii\)](#)
- [関連マニュアル \(P.xiii\)](#)
- [表記法 \(P.xiv\)](#)
- [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 Communications Manager セキュリティ ガイド』は、システム管理者および電話機管理者が次の作業を実行する際に役立ちます。

- 認証を設定する。
- 暗号化を設定する。
- ダイジェスト認証を設定する。
- HTTPS に関連付けられているサーバ認証証明書をインストールする。
- Cisco CTL クライアントを設定します。
- 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。

対象読者

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

マニュアルの構成

表 1 は、このマニュアルの構成を示しています。

表 1 このマニュアルの構成

章番号	説明
セキュリティの基礎	
第 1 章「セキュリティの概要」	セキュリティの用語、システム要件、相互作用と制限、インストール要件、および設定用チェックリストの概要を説明します。また、さまざまなタイプの認証と暗号化についても説明します。
第 2 章「HTTP over SSL (HTTPS) の使用方法」	HTTPS の概要を説明します。また、信頼できるフォルダにサーバ認証証明書をインストールする方法も説明します。
第 3 章「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。
電話機およびボイスメール ポートのセキュリティ	
第 4 章「電話機のセキュリティの概要」	Cisco Unified Communications Manager および電話機でのセキュリティの使用法について説明し、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 Communications Manager の管理ページでセキュリティ プロファイルを設定し、電話機に適用する方法を説明します。
第 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 Communications Manager 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 Communications Manager の管理ページで SIP 電話機にダイジェスト認証を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 Communications Manager の管理ページを使用して電話機のセキュリティを強化する方法を説明します。
第 10 章「セキュアな会議リソースの設定」	セキュアな会議にメディア暗号化を設定する方法を説明します。
第 11 章「ボイスメールポートのセキュリティ設定」	Cisco Unified Communications Manager の管理ページでボイスメール ポートのセキュリティを設定する方法を説明します。
CTI、JTAPI、および TAPI のセキュリティ	
第 12 章「CTI、JTAPI、および TAPI の認証および暗号化の設定」	Cisco Unified Communications Manager の管理ページでアプリケーション ユーザ CAPF プロファイルおよびエンド ユーザ CAPF プロファイルを設定する方法を説明します。

表 1 このマニュアルの構成 (続き)

章番号	説明
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	
第 13 章「Survivable Remote Site Telephony (SRST) リファレンスのセキュリティ設定」	Cisco Unified Communications Manager 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 14 章「ゲートウェイおよびトランクの暗号化の設定」	Cisco Unified Communications Manager がセキュアなゲートウェイまたはトランクと通信する方法、および IPSec に関する推奨事項と考慮事項について説明します。
第 15 章「SIP トランク セキュリティ プロファイルの設定」	Cisco Unified Communications Manager の管理ページで SIP トランクのセキュリティ プロファイルを設定し、適用する方法を説明します。
第 16 章「SIP トランクのダイジェスト認証の設定」	Cisco Unified Communications Manager の管理ページでダイジェスト認証を SIP トランクに設定する方法を説明します。

関連マニュアル

各章に、その章のトピックについての関連マニュアルのリストを記載しています。

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

- *Cisco Unified IP Phone アドミニストレーションガイド for Cisco Unified Communications Manager*
- *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*
- *Cisco Unified Communications Manager Integration Guide for Cisco Unity*
- *Cisco Unified Communications Manager Integration Guide for Cisco Unity Connection*
- SRST 対応ゲートウェイをサポートする Cisco Unified Survivable Remote Site Telephony (SRST) の管理マニュアル
- ご使用の電話機モデルをサポートしているファームウェア リリース ノート

表記法

(注) は、次のように表しています。



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

ヒントは、次のように表しています。



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

Cisco IP テレフォニー ネットワークは、認証された通信ストリームの確立および維持、電話機にファイルを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。

- [用語 \(P.1-2\)](#)
- [システム要件 \(P.1-5\)](#)
- [機能一覧 \(P.1-6\)](#)
- [セキュリティ アイコン \(P.1-7\)](#)
- [相互作用および制限 \(P.1-8\)](#)
- [ベスト プラクティス \(P.1-13\)](#)
- [インストール \(P.1-14\)](#)
- [証明書 \(P.1-15\)](#)
- [認証、整合性、および許可の概要 \(P.1-18\)](#)
- [暗号化の概要 \(P.1-23\)](#)
- [設定用チェックリストの概要 \(P.1-26\)](#)
- [その他の情報 \(P.1-29\)](#)

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、暗号化、および他のセキュリティ機能を設定する場合に適用されます。

表 1-1 用語

用語	定義
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	通信中のエンティティの 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 Communications Manager では、許可されたユーザに一部のトランク側 SIP 要求を制限するセキュリティ プロセス。
許可ヘッダー	チャレンジに対する SIP ユーザ エージェントの応答。
証明書	証明書の保持者名、公開鍵、およびこの証明書を発行する認証局のデジタル署名が含まれているメッセージ。
Certificate Authority (CA; 認証局)	証明書を発行する信頼されたエンティティ。シスコまたはサードパーティのエンティティなど。
Certificate Authority Proxy Function (CAPF)	サポートされているデバイスが Cisco Unified Communications Manager の管理機能を使用してローカルで有効な証明書を要求できるプロセス。
Certificate Trust List (CTL; 証明書信頼リスト)	CTL クライアントで作成され、Cisco Site Administrator Security Token (セキュリティ トークン) で署名したファイル。電話機が信頼するサーバの証明書リストを含みます。
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。
デジタル署名	メッセージをハッシュ変換し、その後、署名者が自身の秘密鍵で暗号化して生成される値。メッセージの受信者は署名者の公開鍵でハッシュ変換を行ってこれを復号化します。これによって同じハッシュ関数で別のハッシュ値が生成されます。この 2 つのハッシュを比較してメッセージが一致し、内容が損なわれていないことを確認します。
DSP	Digital signaling processor (デジタル シグナル プロセッサ)。
DSP ファーム	H.323 または MGCP 対応ゲートウェイの DSP で提供される IP テレフォニー会議のネットワーク リソース。

表 1-1 用語 (続き)

用語	定義
暗号化	データを暗号文に変換するプロセスで、情報の機密性を保持し、対象とする受信者だけがデータを読み取ることができるようにします。暗号化アルゴリズムと暗号鍵が必要です。
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。
H.323	インターネット規格の一種で、一連の共通コーデック、コール設定とネゴシエーション手順、および基本的なデータ転送方式を定義します。
ハッシュ	ハッシュ関数を使用したテキスト文字列から生成される、主に 16 進数で表される数字。これによって、データに対して 1 つの小さなデジタル「フィンガープリント」を作成します。
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。
イメージ認証	電話機にバイナリ イメージをロードする前に、電話機がバイナリ イメージの整合性と発信元を検証するプロセス。
整合性	エンティティ間でデータの改ざんが行われなかったことを確認するプロセス。
IPSec	エンドツーエンドセキュリティ用に、セキュアな H.225、H.245、RAS シグナリング チャネルを提供する転送方式。
Locally Significant Certificate (LSC; ローカルで有効な証明書)	サードパーティの認証局または CAPF が発行し、電話機または JTAPI/TAPI/CTI アプリケーションにインストールされているデジタル X.509v3 証明書。
Manufacture Installed Certificate (MIC; 製造元でインストールされる証明書)	Cisco Certificate Authority によって署名され、サポートされている電話機にシスコの製造過程でインストールされた X.509v3 デジタル証明書。LSC を電話機にインストールする際の CAPF の認証メカニズムとして使用します。
Man-in-the-Middle(中間者) 攻撃	Cisco Unified Communications Manager と電話機との間で流れる情報を、攻撃者が監視して改変できるプロセス。
Multipoint Control Unit (MCU; マルチポイントコントロールユニット)	複数の H.323 エンドポイントと接続して、複数のユーザが IP ベースのビデオ会議に参加できるようになる柔軟なシステム。
MD5	暗号化で使用されるハッシュ関数。
メディア暗号化	暗号化手順によってメディアの機密を保護するプロセス。メディア暗号化では、IETF RFC 3711 で定義された Secure Real Time Protocol (SRTP) を使用します。
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可能性のある一定のカテゴリのメッセージを制限するツール。トランク側アプリケーションまたはデバイスに対して SIP 非インバイト メソッドを許可するかどうかを定義します。メソッド ACL とも呼ばれます。

表 1-1 用語 (続き)

用語	定義
混合モード	Cisco Unified Communications Manager のセキュリティ モードで、セキュア / 非セキュアのプロファイルを持つデバイスおよび RTP/SRTP メディアが Cisco Unified Communications Manager に接続できるようにする設定を行います。
ナンズ	一意のランダムな数値で、サーバが各ダイジェスト認証要求に対して生成します。MD5 ハッシュを生成するために使用されます。
非セキュア モード	Cisco Unified Communications Manager のセキュリティ モードで、非セキュア プロファイルを持つデバイスおよび RTP メディアが Cisco Unified Communications Manager に接続できるようにする設定を行います。
非セキュア コール	少なくとも 1 台のデバイスが認証も暗号化もされていないコール。
非セキュア デバイス	UDP または TCP 方式のシグナリングと非セキュア メディアを使用するデバイス。
PKI	Public Key Infrastructure (公開鍵インフラストラクチャ)。セキュリティ保護された公開鍵の配布、証明書や認証局など、公開鍵の暗号化に必要な要素のセットで構成されます。
公開鍵 / 秘密鍵	暗号化に使用される鍵。公開鍵は広く一般に流通するが秘密鍵は該当する所有者が保持します。非対称暗号化では、両方の鍵を使用します。
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。
RTP	Real-Time Transport Protocol (リアルタイム転送プロトコル)
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 証明書を発行する認証局との通信に使用されるプロトコル。
セキュア コール	すべてのデバイスが認証され、シグナリングとメディア (ボイス ストリーム) が暗号化されているコール。
シグナリング認証	転送中にシグナリング パケットが改ざんされていないことを検証する TLS プロセス。
シグナリング暗号化	デバイスと Cisco Unified Communications Manager サーバの間で送信されるすべてのシグナリング メッセージの機密保持を行うために、暗号化手法を使用するプロセス。
SIP レルム	Cisco Unified Communications Manager がチャレンジに回答するために使用する文字列 (名前)。
SRTP	ネットワークでの音声会話のセキュリティを確保し、リプレイ アタックからの保護を提供するセキュアなリアルタイム転送プロトコル。
SSL	データ通信 (インターネットでの電子メールなど) のセキュリティを確保する暗号化プロトコル。後継の TLS と同等の機能を持ちます。
Transport Layer Security (TLS)	データ通信 (インターネットでの電子メールなど) のセキュリティを確保する暗号化プロトコル。機能的には SSL と同等です。
信頼リスト	デジタル署名なしの証明書リスト。

表 1-1 用語 (続き)

用語	定義
信頼ストア	Cisco Unified Communications Manager などのアプリケーションによって明示的に信頼された X.509 証明書のリポジトリ。
X.509	PKI 認証のインポートに使用する ITU-T 暗号化規格で、証明書の形式を含んでいます。

システム要件

認証および暗号化には、次のシステム要件があります。

- Cisco Unified Communications Manager Release 6.0 は、このマニュアルで示すセキュリティ機能の最小要件として機能します。
- Cisco CTL クライアントで使用するユーザ名およびパスワード (Cisco Unified Communications Manager サーバへのログインに使用) は、Cisco Unified Communications Manager の管理ページのユーザ名およびパスワード (Cisco Unified Communications Manager の管理ページへのログインに使用するユーザ名およびパスワード) と一致する必要があります。
- LSC は、Cisco Unified Communications Manager との TLS 接続の認証用のすべての電話機にインストールされています。Certificate Authority Proxy Function (CAPF) については、[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。

機能一覧

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

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

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

表 1-2 SCCP コールのセキュリティ機能

セキュリティ機能	回線側	トランク側
転送 / 接続 / 整合性	セキュア TLS ポート	IPSec アソシエーション
デバイス認証	Cisco Unified Communications Manager および CAPF のいずれかまたは両方との TLS 証明書交換	IPSec 証明書交換、または事前共有鍵
シグナリング認証 / 暗号化	TLS モード：認証または暗号化	IPSec [認証ヘッダー、暗号化 (ESP)、または両方]
メディア暗号化	SRTP	SRTP
許可	プレゼンス要求	プレゼンス要求

注：デバイスがサポートする機能はデバイス タイプによって異なります。

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

表 1-3 SIP コールのセキュリティ機能

セキュリティ機能	回線側	トランク側
転送 / 接続 / 整合性	セキュア TLS ポート	セキュア TLS ポート
デバイス認証	Cisco Unified Communications Manager および CAPF のいずれかまたは両方との TLS 証明書交換	IPSec 証明書交換、または事前共有鍵
ダイジェスト認証	各 SIP デバイスは一意のダイジェスト ユーザ クレデンシャルを使用	SIP トランク ユーザ エージェントは一意のダイジェスト クレデンシャルを使用
シグナリング認証 / 暗号化	TLS モード：認証または暗号化 (Cisco Unified SIP Phone 7940/7960 を除く)	TLS モード：認証または暗号化モード
メディア暗号化	SRTP	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 タイプによって異なります。

セキュリティ アイコン

Cisco Unified Communications Manager は、コールに参加する Cisco Unified Communications Manager サーバとデバイスに設定されているセキュリティ レベルに応じたセキュリティのステータスをコールに提供します。セキュリティ アイコンをサポートする電話機には、コールのセキュリティ レベルが表示されます。

- シグナリング セキュリティ レベルが「認証」のコールに対しては、シールドアイコンが表示されます。シールドは、Cisco IP デバイス間のセキュアな接続を識別します。これは、デバイスのシグナリングが認証または暗号化されていることを意味します。
- 暗号化メディアのコールに対しては、電話機にロックアイコンが表示されます。これは、デバイスが暗号化シグナリングと暗号化メディアを使用していることを意味します。

コールのセキュリティ ステータスは、ポイント間、クラスタ内、クラスタ間、マルチホップ コールで変更する場合があります。SCCP 回線、SIP 回線、および H323 シグナリングでは、コールのセキュリティ ステータスが変更した場合、参加しているエンドポイントへの通知をサポートしています。コールのパスに SIP トランクが含まれる場合、コール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.1-11](#)の「[セキュリティ アイコンと暗号化](#)」を参照してください。

会議コールおよび割り込みコールでは、セキュリティ アイコンは会議のセキュリティ ステータスを表示します。詳細については、[P.10-4](#)の「[セキュアな会議のアイコン](#)」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 \(P.1-8\)](#)
- [制限 \(P.1-9\)](#)

セキュアな会議の機能に関する相互作用と制限の詳細については、[P.10-1](#) の「[セキュアな会議リソースの設定](#)」を参照してください。

相互作用

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

プレゼンス

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



(注)

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

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

SIP トランク

SIP 発信転送機能、および Web Transfer や 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 Communications Manager 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設定する必要があります。

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

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

エクステンション モビリティ

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

CTI

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

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

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

制限

次の項で、シスコのセキュリティ機能に適用される制限について説明します。

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

トランクのサポート

Cisco Unified Communications Manager Business Edition システムでは Intercluster Trunk(ICT; クラスタ間トランク)はサポートされていません。シスコは、ゲートウェイ、プロキシ、MCU、IP PSTN 接続およびデバイスで SIP トランクおよび H.323 トランクをサポートします。

認証と暗号化

認証および暗号化機能をインストールして設定する前に、次の制限を考慮してください。

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

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



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

シグナリング暗号化では NAT トラバーサルをサポートしません。NAT を使用する代わりに、LAN 拡張 VPN の使用を検討してください。

- SRTP は、音声パケットのみを暗号化します。

割り込みと暗号化

割り込みと暗号化には、次の制限が適用されます。

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



(注) リリース 8.3 以降を実行中の非セキュアまたは認証済み Cisco Unified IP Phone は、これで暗号化されたコールに割り込むことができます。セキュリティ アイコンによって会議のセキュリティ ステータスが示されます。詳細については、P.10-4 の「セキュアな会議のアイコン」を参照してください。

ワイドバンド コーデックと暗号化

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

メディア リソースと暗号化

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

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

電話機のサポートと暗号化

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

暗号化をサポートする Cisco Unified SCCP IP Phone は、7906、7911、7931 (SCCP のみ)、7940、7941、7941G-GE、7960、7961、7961G-GE、7970、7971 です。また、暗号化をサポートする Cisco Unified SIP IP Phone は、7906、7911、7941、7941G-GE、7961、7961G-GE、7970、7971 です。



警告

セキュリティ機能を最大限に活用するには、Cisco Unified IP Phone をリリース 8.3 にアップグレードすることをお勧めします。リリース 8.3 は、今回のリリースの Cisco Unified Communications Manager で暗号化機能をサポートします。これ以前のリリースの暗号化対応電話機は、これらの新しい機能を完全にはサポートしません。これらの電話機は、セキュアな会議コールおよび割り込みコールに対し、認証済みか非セキュアな参加者として参加できます。

以前のリリースの Cisco Unified Communications Manager を実行するリリース 8.3 の Cisco Unified IP Phone は、会議コールまたは割り込みコール中のセキュリティステータスを表示し、会議リストなどのセキュアな会議の機能はサポートしません。

電話機のサポートおよび暗号化された設定ファイル

暗号化された設定ファイルをサポートしない電話機もあります。また、暗号化された設定ファイルはサポートするが、署名の検証をサポートしない電話機もあります。Cisco Unified IP Phone 7905 および 7912 を除き、暗号化された設定ファイルをサポートする電話機にはすべて、完全に暗号化された設定ファイルを受信するために、Cisco Unified Communications Manager リリース 5.0 以降と互換性のあるファームウェアが必要です。Cisco Unified IP Phone 7905 および 7912 は、既存のセキュリティメカニズムを使用します。このメカニズムはこの機能のために新しいファームウェアを必要としません。暗号化された設定ファイルの電話機でのサポートについては、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 Communications Manager は主に、IOS ゲートウェイ用および、ゲートキーパー制御と非ゲートキーパー制御トランクの Cisco Unified Communications Manager H.323 トランク用に 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 Communications Manager 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 Communications Manager 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。

- コールの転送またはコールの保留などのタスクを実行するときに、暗号化ロックアイコンが電話機に表示されないことがあります。MOH など、こうしたタスクに関連付けられたメディアストリームが暗号化されていない場合、ステータスは暗号化済みから非セキュアに変化します。
- Cisco Unified Communications Manager は、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 Communications Manager 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。
- PSTN に関連するコールの場合、セキュリティアイコンで表示されるセキュリティステータスはコールの IP ドメイン部分についてのみです。

セキュアな会議でのセキュリティアイコンの表示の詳細については、P.10-4 の「セキュアな会議のアイコン」を参照してください。

クラスタおよびデバイス セキュリティ モード



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

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

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

ダイジェスト認証と暗号化

Cisco Unified Communications Manager は、複数の異なるコール レッグを持つコールとして、SIP コールを定義します。通常、2 つの SIP デバイスで 2 者が通話するとき、2 つの異なるコール レッグが存在します。1 つは、発信 SIP ユーザ エージェントと Cisco Unified Communications Manager の間 (発信コール レッグ) で、もう 1 つは Cisco Unified Communications Manager と宛先 SIP ユーザ エージェントの間 (着信コール レッグ) です。各コール レッグは、別のダイアログを表します。ダイジェスト認証は、ポイントツーポイント プロセスなので、各コール レッグの認証は別のコール レッグから独立しています。SRTP 機能は、ユーザ エージェント間でネゴシエーションされる機能に応じて、コール レッグごとに変更できます。

パケット キャプチャと暗号化

SRTP 暗号化が実装されている場合、サードパーティのスニファは動作しません。適切な認証で許可された管理者は、Cisco Unified Communications Manager の管理ページで設定を変更してパケット キャプチャを開始できます (パケット キャプチャをサポートするデバイスの場合)。Cisco Unified Communications Manager でのパケット キャプチャの設定については、今回のリリースをサポートする『Cisco Unified Communications Manager 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。
- リモートのロケーションのゲートウェイその他のアプリケーションサーバにはIPSecを使用する。



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せん。

- 通話料金の不正を防止するため、『Cisco Unified Communications Manager システムガイド』に説明されている電話会議の機能拡張を設定する。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。この作業の実行方法については、『Cisco Unified Communications Manager 機能およびサービスガイド』を参照してください。

この項では、次のトピックについて取り上げます。

- [デバイスのリセット、サービスの再起動またはリポート \(P.1-13\)](#)
- [メディア暗号化の設定と割り込み \(P.1-14\)](#)

デバイスのリセット、サービスの再起動またはリポート

ここでは、デバイスのリセット、Cisco Unified Serviceability でのサービスの再起動またはリポートが必要になる場合について説明します。

次のガイドラインを考慮します。

- Cisco Unified Communications Manager の管理ページで別のセキュリティプロファイルを適用した後、1台のデバイスをリセットする。
- 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 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 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 サービスの再起動については、『Cisco Unified Communications Manager Serviceability 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。

メディア暗号化の設定と割り込み

P.1-10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 Phone models 7960 and 7940, those encrypted devices cannot accept a barge request when they are participating in an encrypted call. When the call is encrypted, the barge attempt fails.

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

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

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



ヒント

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

インストール

認証のサポートを可能にするには、プラグインの Cisco CTL クライアントを Cisco Unified Communications Manager の管理ページからインストールします。Cisco CTL クライアントをインストールするためには、少なくとも2つのセキュリティ トークンを入手する必要があります。

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

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

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

証明書

証明書は、クライアントとサーバの ID を保護します。ルート証明書がインストールされた後、証明書はルート信頼ストアに追加され、ユーザとホスト間（デバイスおよびアプリケーション ユーザを含む）の接続のセキュリティを確保します。

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

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

Cisco Unified Communications Manager 信頼ストアの更新と証明書の管理の詳細については、今回のリリースの Cisco Unified Communications Manager をサポートする『Cisco Unified Communications Operating System 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 Communications Manager は、PEM (.pem) 形式および DER (.der) 形式の証明書のみサポートします。

この項では、次のトピックについて取り上げます。

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

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 のインストールにおける Cisco Certificate Authority Proxy Function (CAPF) に対する認証を行います。MIC は上書きすることも削除することもできません。
- **Locally Significant Certificate (LSC; ローカルで有効な証明書)**: この種類の証明書は、Cisco Certificate Authority Proxy Function (CAPF) に関連する必要な作業を実行した後で、サポートされている電話機にインストールされます。設定の作業については、[P.1-26 の「設定用チェックリストの概要」](#)を参照してください。LSC は、デバイス セキュリティ モードを認証または暗号化に設定すると、Cisco Unified Communications Manager と電話機間の接続のセキュリティを確保します。



ヒント

製造元でインストールされる証明書 (MIC) は、LSC のインストールの場合にのみ使用することをお勧めします。シスコでは、Cisco Unified Communications Manager との TLS 接続の認証用に LSC をサポートしています。MIC ルート証明書は侵害される可能性があるため、TLS 認証用またはその他の目的のために MIC を使用するように電話機を設定するお客様は、ご自身の責任で行ってください。MIC が侵害されてもシスコは責任を負いかねます。

CAPF 信頼ストアに格納されている MIC ルート証明書は、証明書のアップグレードに使用されます。Cisco Unified Communications Manager 信頼ストアの更新と証明書の管理の詳細については、今回のリリースをサポートする『Cisco Unified Communications Operating System 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 Communications Manager サーバでは、次の種類の自己署名証明書を使用します。

- HTTPS 証明書 (tomcat_cert): この自己署名ルート証明書は、Cisco Unified Communications Manager をインストールするときに、HTTPS サーバに対して生成されます。
- Cisco Unified Communications Manager ノード証明書: この自己署名ルート証明書は、Cisco Unified Communications Manager サーバに Cisco Unified Communications Manager をインストールすると自動的にインストールされます。Cisco Unified Communications Manager 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 Communications Manager 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、ユーザのサーバまたはクラスタ内のすべてのサーバにコピーされます。
- IPsec 証明書 (ipsec_cert): この自己署名ルート証明書は、Cisco Unified Communications Manager のインストール中に、MGCP および H.323 ゲートウェイとの IPsec 接続に対して生成されます。
- SRST 対応ゲートウェイ証明書: Cisco Unified Communications Manager の管理ページのセキュアな SRST リファレンスを設定するときに、Cisco Unified Communications Manager は、ゲートウェイから SRST 対応ゲートウェイ証明書を取得し、Cisco Unified Communications Manager データベースに格納します。デバイスをリセットすると、証明書は電話機設定ファイルに追加されず、証明書はデータベースに格納されるため、この証明書を証明書管理ツールで管理することはできません。

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

- Cisco Unity サーバまたは Cisco Unity Connection 証明書: Cisco Unity および Cisco Unity Connection は、この自己署名証明書を使用して、Cisco Unity SCCP および Cisco Unity Connection SCCP デバイス証明書に署名します。Cisco Unity の場合、Cisco Unity Telephony Integration Manager (UTIM) がこの証明書を管理します。Cisco Unity Connection の場合は、Cisco Unity Connection の管理機能がこの証明書を管理します。
- Cisco Unity および Cisco Unity Connection SCCP デバイス証明書: Cisco Unity および Cisco Unity Connection SCCP デバイスは、この署名証明書を使用して、Cisco Unified Communications Manager との TLS 接続を確立します。

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

- SIP Proxy サーバ証明書: Cisco Unified Communications Manager 信頼ストアに SIP ユーザ エージェント証明書が含まれ、SIP ユーザ エージェントの信頼ストアに Cisco Unified Communications Manager 証明書が含まれている場合、SIP トランク経由で接続する SIP ユーザ エージェントは、Cisco Unified Communications Manager に対して認証されます。

Cisco Unity Connection の CA 信頼証明書の詳細については、『Cisco Unity Connection システム アドミニストレーションガイド』を参照してください。これらの信頼証明書は、Exchange または Meeting Place Express との間で、電子メール、カレンダー情報、連絡先を取得するためのセキュアな接続を確立します。

外部 CA からの証明書のサポート

Cisco Unified Communications Manager は、PKCS#10 Certificate Signing Request (CSR; 証明書署名要求) メカニズムを使用して、サードパーティの認証局 (CA) との統合をサポートします。このメカニズムには、Cisco Unified Communications オペレーティングシステムの [証明書の管理] の GUI でアクセスできます。現在サードパーティの CA を使用しているお客様は、この CSR メカニズムを使用して、Cisco Unified Communications Manager と CAPF の両方の証明書を発行する必要があります。



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

シスコは、Keon および Microsoft の CA による 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 クライアントを実行した後、該当するサービスを再起動して更新します。たとえば、Cisco Unified Communications Manager 証明書を更新する場合は Cisco CallManager と Cisco Tftp を再起動し、CAPF 証明書を更新する場合は CAPF を再起動します。更新の手順については、P.3-1 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) の生成の詳細については、今回のリリースの Cisco Unified Communications Manager をサポートする『Cisco Unified Communications Operating System 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 Communications Manager との間で行われるコール処理シグナリングの変更（認証）
- [表 1-1](#) で定義した Man-in-the-Middle（中間者）攻撃（認証）
- 電話機およびサーバの ID 盗難（認証）
- リプレイ アタック（ダイジェスト認証）

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

認証、整合性、および許可の詳細については、次の項を参照してください。

- [イメージ認証 \(P.1-18\)](#)
- [デバイス認証 \(P.1-18\)](#)
- [ファイル認証 \(P.1-19\)](#)
- [シグナリング認証 \(P.1-19\)](#)
- [ダイジェスト認証 \(P.1-20\)](#)
- [許可 \(P.1-22\)](#)

イメージ認証

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

デバイス認証

このプロセスでは、通信デバイスの ID を検証し、このエンティティが主張内容と一致することを確認します。サポートされるデバイスのリストについては、[P.4-2](#) 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 Communications Manager サーバとサポートされる Cisco Unified IP Phone、SIP トランク、または JTAPI/TAPI/CTI アプリケーション（サポートされる場合）の間で発生します。認証された接続は、各エンティティが他のエンティティの証明書を受け付けたときのみ、これらのエンティティの間で発生します。この相互証明書交換プロセスが、相互認証と呼ばれるプロセスです。

デバイス認証は、[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 Communications Manager サーバ ノードおよびアプリケーションの認証の場合）および [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 Communications Manager 信頼ストアに SIP ユーザ エージェント証明書が含まれ、SIP ユーザ エージェントの信頼ストアに Cisco Unified Communications Manager 証明書が含まれている場合、SIP トランク経由で接続する SIP ユーザ エージェントは、Cisco Unified Communications Manager に対して認証されます。Cisco Unified Communications Manager 信頼ストアの更新の詳細については、今回のリリースの Cisco Unified Communications Manager をサポートする『Cisco Unified Communications Operating System 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.4-2 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、事前に、Cisco Unified Communications Manager の管理ページで、影響を受けるデバイスを再起動しておく必要があります。

電話機は、TFTP サーバからファイルを受信すると、ファイルの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 Communications Manager エントリおよび証明書が存在する必要がある。
- デバイ스에 인증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 Communications Manager は、Cisco Unified Communications Manager に接続しているデバイスの ID でチャレンジができます。チャレンジが行われるときは、デバイスは自身のダイジェスト クレデンシャル(ユーザ名やパスワードのようなもの) を Cisco Unified Communications Manager に提示して承認を受けます。提示されたクレデンシャルがそのデバイス用としてデータベースに設定済みのクレデンシャルと一致した場合、ダイジェスト認証は成功し、Cisco Unified Communications Manager は SIP 要求を処理します。



(注) クラスタのセキュリティ モードは、ダイジェスト認証に影響しません。



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

ユーザは Cisco Unified Communications Manager データベースに電話機ユーザまたはアプリケーションユーザの SIP ダイジェスト 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、[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 クレデンシャルを指定します。
- SIP 電話機の場合は、[エンドユーザの設定 (End User Configuration)] ウィンドウで、ダイジェスト認証の証明書を指定し、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。ダイジェスト クレデンシャルが TFTP ダウンロードで暗号化されずに送信されないようにする詳細については、「[暗号化された電話機設定ファイルの設定](#)」を参照してください。
- ユーザは、チャレンジを SIP トランク上で受信するための SIP レルムを設定します。SIP レルムには、レルム、ユーザ名(デバイスまたはアプリケーション ユーザ) およびダイジェスト クレデンシャルが含まれます。

SIP 電話機またはトランクのダイジェスト クレデンシャルを有効にし、ダイジェスト クレデンシャルを設定した場合、Cisco Unified Communications Manager は、ユーザ名、パスワード、およびレルムのハッシュを含むクレデンシャル チェックサムを計算します。Cisco Unified Communications Manager は値を暗号化し、ユーザ名とチェックサムをデータベースに格納します。

Cisco Unified Communications Manager は、ヘッダーにナンズとレルムを含む SIP 401 (Unauthorized) メッセージを使用してチャレンジを開始します。ナンズは、MD5 ハッシュの計算に使用するランダム数を指定します。ユーザは、SIP デバイスのセキュリティ プロファイルで電話機またはトランクのナンズ確認時間を設定します。ナンズ確認時間は、外部のデバイスに対してナンズ値が有効な時間数を分数で指定するもので、この時間を超えると Cisco Unified Communications Manager は外部デバイスを拒否して新しい番号を生成します。



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

**ヒント**

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

電話機のダイジェスト認証

電話機に対してダイジェスト認証が有効になっている場合、Cisco Unified Communications Manager は、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 Communications Manager は回線側の電話機からのチャレンジには応答しません。

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

SIP 電話機は Cisco Unified Communications Manager のレルムにのみ存在でき、これは Cisco Unified Communications Manager の管理機能のインストール時に定義されます。電話機のチャレンジ用の SIP レルムは、サービス パラメータ SIP Station Realm で設定します。各ダイジェストユーザは、レルムごとにダイジェスト クレデンシャルのセットを 1 つ持つことができます。詳細については、「[SIP 電話機のダイジェスト認証の設定](#)」を参照してください。

**ヒント**

エンド ユーザのダイジェスト認証を有効にしたが、ダイジェスト 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 Communications Manager でもチャレンジが開始されます。

トランクのダイジェスト認証

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

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

**ヒント**

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

SIP レルムの設定方法の詳細については、P.16-1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。SIP レルムとユーザ名およびパスワードは、Cisco Unified Communications Manager に対してチャレンジができる SIP トランク ユーザエージェントごとに Cisco Unified Communications Manager で設定する必要があります。各ユーザは、レルムごとにダイジェスト クレデンシャルのセットを1つ持つことができます。

許可

Cisco Unified Communications Manager は、許可プロセスを使用して、SIP 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 Communications Manager はコーリング サーチ スペースおよびパーティションを通じて許可を与えます。
- 電話機からの SIP SUBSCRIBE 要求の場合、Cisco Unified Communications Manager は、プレゼンスグループへのユーザ アクセスに許可を与えます。
- SIP トランクの場合、Cisco Unified Communications Manager はプレゼンス サブスクリプションおよび非インバイト SIP メッセージ(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、許可する SIP 要求のチェックボックスをオンにして、許可を指定します。

SIP トランクのアプリケーションの許可を有効にするには、[SIP トランクセキュリティプロファイルの設定 (SIP Trunk Security Profile Configuration)] ウィンドウで [アプリケーションレベル認証を有効化 (Enable Application Level Authorization)] チェックボックスと [ダイジェスト認証を有効化 (Enable Digest Authentication)] チェックボックスをオンにしてから、[アプリケーションユーザの設定 (Application User Configuration)] ウィンドウで許可する SIP 要求のチェックボックスをオンにします。

SIP トランクの許可とアプリケーション レベルの許可の両方を有効にすると、最初に SIP トランクの許可が発生し、次に SIP アプリケーション ユーザの許可が発生します。トランクの場合、Cisco Unified Communications Manager はトランク ACL 情報をダウンロードしてキャッシュします。ACL 情報は、着信 SIP 要求に適用されます。ACL が SIP 要求を許可しない場合、コールは 403 Forbidden メッセージで失敗します。

ACL が SIP 要求を許可する場合、Cisco Unified Communications Manager は、[SIP トランクセキュリティプロファイルの設定 (SIP Trunk Security Profile Configuration)] でダイジェスト認証が有効かどうかを確認します。ダイジェスト認証が有効でなく、アプリケーションレベルの許可が有効でない場合、Cisco Unified Communications Manager は要求を処理します。ダイジェスト認証が有効な場合、Cisco Unified Communications Manager は着信要求に認証ヘッダーが存在することを確認してから、ダイジェスト認証を使用して、発信元アプリケーションを識別します。ヘッダーが存在しない場合、Cisco Unified Communications Manager は 401 メッセージでデバイスに対するチャレンジを行います。

アプリケーションレベルの ACL を適用する前に、Cisco Unified Communications Manager は、ダイジェスト認証で SIP トランク ユーザ エージェントを認証します。そのため、アプリケーションレベルの許可を発生させるには、事前に [SIP トランクセキュリティプロファイルの設定 (SIP Trunk Security Profile Configuration)] でダイジェスト認証を有効にする必要があります。

暗号化の概要



ヒント

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

Cisco Unified Communications Manager 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.1-23)
- メディア暗号化 (P.1-23)
- 設定ファイルの暗号化 (P.1-25)

シグナリング暗号化

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

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

クラスタを混合モードに設定した場合、Cisco Unified Communications Manager による Network Address Translation (NAT; ネットワーク アドレス変換) はサポートされません。NAT はシグナリング暗号化では動作しません。

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



ヒント

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

シグナリング暗号化では NAT トラバーサルをサポートしません。NAT を使用する代わりに、LAN 拡張 VPN の使用を検討してください。

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

メディア暗号化

メディア暗号化は 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 Communications Manager は、デバイスおよびプロトコルに応じてメディア暗号鍵を異なる方法で処理します。SCCP 電話機はすべて、Cisco Unified Communications Manager からメディア暗号鍵を取得します。この場合、メディア暗号鍵は、TLS で暗号化されたシグナリングチャネルによって電話機に安全にダウンロードされます。SIP 電話機は、自身のメディア暗号鍵を生成して保存します。Cisco Unified Communications Manager システムで導出されたメディア暗号鍵は、暗号化されたシグナリングパス経由で、H323 および MGCP では IPsec で保護されたリンクを通じて、SCCP および SIP は暗号化された TLS リンクを通じてゲートウェイに安全に送出されます。

デバイスが SRTP をサポートする場合、システムは SRTP 接続を使用します。少なくとも 1 つのデバイスが SRTP をサポートしていない場合、システムは RTP 接続を使用します。SRTP から RTP へのフォールバックは、セキュアデバイスから非セキュアデバイスへの転送、トランスコーディング、保留音などで発生する場合があります。

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



警告

Cisco IOS MGCP ゲートウェイ、H.323 ゲートウェイ、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 Communications Manager 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 Communications Manager に登録されています。
2. デバイス A がデバイス B に対してコールを行うと、Cisco Unified Communications Manager はキー マネージャ機能からメディア セッション マスター値のセットを 2 つ要求します。
3. 両方のデバイスで 2 つのセットを受信します。1 つはデバイス A からデバイス B へのメディア ストリーム用、もう 1 つはデバイス B からデバイス A へのメディア ストリーム用です。
4. デバイス A は最初のマスター値セットを使用して、デバイス A からデバイス B へのメディア ストリームを暗号化して認証する鍵を取得します。
5. デバイス A は 2 番目のマスター値セットを使用して、デバイス B からデバイス A へのメディア ストリームを認証して復号化する鍵を取得します。
6. これとは反対の操作手順で、デバイス B がこれらのセットを使用します。
7. 両方のデバイスは、鍵を受信した後に必要な鍵導出を実行し、SRTP パケット処理が行われます。



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

会議コールのメディア暗号化の詳細については、P.10-1 の「セキュアな会議リソースの設定」を参照してください。

設定ファイルの暗号化

Cisco Unified Communications Manager は、TFTP サーバからの設定ファイルのダウンロードで、機密データ（ダイジェスト 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 Communications Manager は、可逆暗号化を使用して、データベース内でこれらのクレデンシャルを保護します。ダウンロード プロセス中にこのデータを保護するため、このオプションをサポートするすべての Cisco Unified IP Phone (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になっていると、デバイス設定ファイルだけがダウンロード用に暗号化されます。



(注) 状況によっては（たとえば、電話機のトラブルシューティングを行う場合や、自動登録中など）、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 Communications Manager は、暗号鍵を符号化し、データベースに格納します。TFTP サーバは、対称暗号鍵を使用して、設定ファイルを暗号化および復号化します。

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

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

詳細については、P.7-2 の「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 1-4 に、認証および暗号化を実装するために必要なすべての作業を示します。また、各章には指定されたセキュリティ機能のために実行が必要な作業のチェックリストが含まれる場合もあります。

表 1-4 認証および暗号化の設定用チェックリスト


設定手順	関連手順および関連項目
ステップ 1 Cisco Unified Serviceability で Cisco CTL Provider サービスをアクティブにします。	Cisco CTL Provider サービスのアクティブ化 (P.3-5)
ステップ 2 Cisco Unified 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。	Certificate Authority Proxy Function サービスのアクティブ化 (P.6-6)
 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。	
ステップ 3 デフォルトのポート設定を使用しない場合は、TLS 接続用のポートを設定します。	TLS 接続用ポートの設定 (P.3-6)
ステップ 4 Cisco CTL クライアント用に設定するサーバについて、少なくとも 2 つのセキュリティ トークンとパスワード、ホスト名または IP アドレス、およびポート番号を入手します。	Cisco CTL クライアントの設定 (P.3-10)
ステップ 5 Cisco CTL クライアントをインストールします。	<ul style="list-style-type: none"> • システム要件 (P.1-5) • インストール (P.1-14) • Cisco CTL クライアントのインストール (P.3-8) • Cisco CTL クライアントの設定 (P.3-10)
ステップ 6 Cisco CTL クライアントを設定します。	<ul style="list-style-type: none"> • Cisco CTL クライアントの設定 (P.3-10) • Cisco CTL クライアントの設定 (P.3-10)

表 1-4 認証および暗号化の設定用チェックリスト (続き)

設定手順	関連手順および関連項目
ステップ 7 電話機のセキュリティ プロファイルを設定します。プロファイルを設定するときは、次の作業を実行します。 <ul style="list-style-type: none"> デバイスのセキュリティ モードを設定します。 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)。追加の CAPF 設定が [電話の設定 (Phone Configuration)] ウィンドウに表示されます。 SIP 電話機でダイジェスト認証を使用する場合は、[ダイジェスト認証を有効化 (Enable Digest Authentication)] チェックボックスをオンにします。 暗号化された設定ファイルを有効にするには (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。 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。 	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のヒント (P.5-2) 暗号化された電話機設定ファイルの設定 (P.7-1) 暗号化された設定ファイルの設定のヒント (P.7-6)
ステップ 8 電話機に電話機セキュリティ プロファイルを適用します。	電話機セキュリティ プロファイルの適用 (P.5-12)
ステップ 9 電話機に証明書を発行するように CAPF を設定します。	<ul style="list-style-type: none"> システム要件 (P.1-5) CAPF の設定用チェックリスト (P.6-5)
ステップ 10 サポートされている Cisco Unified IP Phone にローカルで有効な証明書がインストールされたことを確認します。	<ul style="list-style-type: none"> システム要件 (P.1-5) 電話機での認証文字列の入力 (P.6-12)
ステップ 11 SIP 電話機のダイジェスト認証を設定します。	<ul style="list-style-type: none"> SIP 電話機のダイジェスト認証の設定 (P.8-1)
ステップ 12 電話機のセキュリティ強化作業を実行します。	<ul style="list-style-type: none"> 電話機のセキュリティ強化 (P.9-1)
ステップ 13 セキュリティ用の会議ブリッジを設定します。	<ul style="list-style-type: none"> セキュアな会議リソースの設定 (P.10-1)
ステップ 14 セキュリティ用のボイスメール ポートを設定します。	<ul style="list-style-type: none"> ボイスメール ポートのセキュリティ設定 (P.11-1) 今回のリリースの Cisco Unified Communications Manager に該当する Cisco Unity または Cisco Unity Connection のインテグレーション ガイド
ステップ 15 SRST リファレンスのセキュリティを設定します。	<ul style="list-style-type: none"> Survivable Remote Site Telephony (SRST) リファレンスのセキュリティ設定 (P.13-1)
ステップ 16 IPSec を設定します。	<ul style="list-style-type: none"> ゲートウェイおよびトランクの暗号化の設定 (P.14-1) ネットワーク インフラストラクチャで IPSec を設定する場合の注意事項 (P.14-6) Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways Cisco Unified Communications Operating System アドミニストレーション ガイド

表 1-4 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>ステップ 17 </p> <p>(注) この手順はクラスタ間環境にのみ適用されます。Cisco Unified Communications Manager Business Edition システムでは Intercluster Trunk (ICT; クラスタ間トランク) はサポートされていません。</p> <hr/> <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"> • SIP トランク セキュリティ プロファイルの設定 (P.15-1) • ダイジェスト認証のエンタープライズ パラメータの設定 (P.16-2)
<p>ステップ 18 </p> <p>(注) この手順はクラスタ間環境にのみ適用されます。Cisco Unified Communications Manager Business Edition システムでは Intercluster Trunk (ICT; クラスタ間トランク) はサポートされていません。</p> <hr/> <p>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。</p>	<ul style="list-style-type: none"> • SIP トランク セキュリティ プロファイルの適用 (P.15-10)
<p>ステップ 19 </p> <p>(注) この手順はクラスタ間環境にのみ適用されます。Cisco Unified Communications Manager Business Edition システムでは Intercluster Trunk (ICT; クラスタ間トランク) はサポートされていません。</p> <hr/> <p>トランクのダイジェスト認証を設定します。</p>	<ul style="list-style-type: none"> • SIP トランクのダイジェスト認証の設定 (P.16-1)
<p>ステップ 20 </p> <p>(注) この手順はクラスタ間環境にのみ適用されます。Cisco Unified Communications Manager Business Edition システムでは Intercluster Trunk (ICT; クラスタ間トランク) はサポートされていません。</p> <hr/> <p>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。</p>	<ul style="list-style-type: none"> • SIP トランク セキュリティ プロファイルの設定 (P.15-1) • 許可 (P.1-22)

表 1-4 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 21	すべての電話機をリセットします。	デバイスのリセット、サービスの再起動またはリブート (P.1-13)
ステップ 22	すべてのサーバをリブートします。	デバイスのリセット、サービスの再起動またはリブート (P.1-13)

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 Communications Manager*
- *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 Communications Manager Integration Guide for Cisco Unity*
- *Cisco Unified Communications Manager Integration Guide for Cisco Unity Connection*
- SRST 対応ゲートウェイをサポートする Cisco Unified Survivable Remote Site Telephony (SRST) の管理マニュアル
- *Disaster Recovery System アドミニストレーションガイド*
- *Cisco Unified Communications Manager Bulk Administration アドミニストレーションガイド*
- *Cisco Unified Communications Manager 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 Communications Manager アプリケーションには、Cisco Unified Communications Manager の管理ページ、Cisco Unified Serviceability、Cisco Unified IP Phone ユーザ オプション ページ、Cisco Unified Communications Manager Auto-Register Phone Tool、Cisco Unified Communications Manager CDR Analysis and Reporting、Dialed Number Analyzer、および Cisco Unified Real-Time Monitoring Tool があります。

Cisco Unified Communications Manager をインストールまたはアップグレードすると、HTTPS 自己署名証明書 (tomcat_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 Communications Manager 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 Communications Manager の HTTPS アプリケーション

Cisco Unified Communications Manager の HTTPS アプリケーション	Web アプリケーション
CMAAdmin	Cisco Unified Communications Manager の管理ページ
CMService	Cisco Unified Serviceability
CMUser	Cisco Personal Assistant
AST	Cisco Unified Real-Time Monitoring Tool
RTMTRReports	Cisco Unified Real-Time Monitoring Tool レポート アーカイブ
PktCap	パケット キャプチャに使用する TAC トラブルシューティング ツール
ART	Cisco Unified Communications Manager CDR Analysis and Reporting
TAPS	Cisco Unified Communications Manager Auto-Register Phone Tool
dna	Dialed Number Analyzer
drf	Disaster Recovery System
SOAP	Cisco Unified Communications Manager データベースに対して読み書きを行うための Simple Object Access Protocol API
	 <p>(注) セキュリティのために、SOAP を使用するすべての Web アプリケーションで HTTPS が必要です。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 Communications Manager をインストールまたはアップグレードした後に、初めて Cisco Unified Communications Manager の管理ページまたは他の Cisco Unified Communications Manager SSL 対応仮想ディレクトリにブラウザクライアントからアクセスすると、サーバを信頼するかどうかを確認する [セキュリティの警告] ダイアログボックスが表示されます。

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

- [はい] をクリックして、現在の Web セッションについてだけ証明書を信頼するように選択します。現在のセッションに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 Communications Manager 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 Operating System アドミニストレーションガイド』を使用して再生成できます。

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 Communications Manager 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 GUI を使用して再生成できます。

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 \(P.1-15\)](#)

シスコの関連マニュアル

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



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 \(P.3-5\)](#)
- [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 クライアントの設定 \(P.3-10\)](#)
- [CTL ファイルの更新 \(P.3-13\)](#)
- [CTL ファイル エントリの削除 \(P.3-14\)](#)
- [Cisco Unified Communications Manager セキュリティ モードの更新 \(P.3-15\)](#)
- [Cisco CTL クライアントの設定内容 \(P.3-16\)](#)
- [Cisco Unified Communications Manager のセキュリティ モードの確認 \(P.3-19\)](#)
- [Smart Card サービスの開始および自動の設定 \(P.3-20\)](#)
- [セキュリティ トークン パスワード \(etoken\) の変更 \(P.3-21\)](#)
- [Cisco Unified IP Phone 上の CTL ファイルの削除 \(P.3-22\)](#)
- [Cisco CTL クライアントのバージョンの特定 \(P.3-23\)](#)
- [Cisco CTL クライアントの確認とアンインストール \(P.3-23\)](#)
- [その他の情報 \(P.3-24\)](#)

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 CallManager および Cisco Tftp
- Certificate Authority Proxy Function (CAPF)
- PIX Firewall

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 Serviceability で Cisco CallManager および Cisco Tftp サービスを再起動する必要があります。次回、電話機を初期化するときには、CTL ファイルが TFTP サーバからダウンロードされます。CTL ファイルに自己署名証明書を持つ TFTP サーバ エントリが含まれている場合、電話機は .sgn 形式の署名付き設定ファイルを要求します。どの TFTP サーバにも証明書がない場合、電話機は署名なしファイルを要求します。

Cisco CTL クライアントが CTL ファイルにサーバ証明書を追加すると、CTL クライアントの GUI にこの証明書を表示できます。

ファイアウォールを CTL ファイルに設定すると、セキュアな Cisco Unified Communications Manager システムの一部として Cisco PIX Firewall を保護できます。Cisco CTL クライアントは、ファイアウォール証明書を「CCM」証明書として表示します。

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

- Cisco Unified Communications Manager ノードのホスト名が、Cisco CTL クライアントがインストールされているリモート PC で解決可能であることを確認します。解決可能でない場合、Cisco CTL クライアントは正しく動作しません。
- Cisco CTL Provider サービスをアクティブにする必要があります。
- CTL ファイルを作成または更新したら、Cisco Unified Serviceability で Cisco CallManager および Cisco Tftp サービスを再起動する必要があります。

次の情報は、クラスタ間環境にのみ適用されます。Cisco Unified Communications Manager Business Edition システムでは Intercluster Trunk (ICT; クラスタ間トランク) はサポートされていません。

- Cisco CTL クライアントに、代替 TFTP サーバまたは集中 TFTP サーバなどのクラスタ外サーバのエントリが含まれている場合、これらのサーバでも Cisco CTL Provider サービスを実行する必要があります。
- CTL クライアント GUI の 代替 TFTP サーバのセクションで、別のクラスタに存在する Cisco TFTP サーバを指定します。[Alternate TFTP Server] タブの設定値を使用して、代替 TFTP サーバおよび集中 TFTP サーバを CTL クライアントに設定します。



(注)


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

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

Cisco CTL クライアントの設定用チェックリスト

表 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 Communications Manager をアップグレードするときの CTL ファイル設定の詳細については、P.3-10 の「Cisco CTL クライアントの設定」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
ステップ 1 Cisco Unified Serviceability で Cisco CTL Provider サービスをアクティブにします。	Cisco CTL Provider サービスのアクティブ化 (P.3-5)
ステップ 2 Cisco Unified Serviceability で Cisco Certificate Authority Proxy サービスをアクティブにします。  ワンポイント・アドバイス Cisco CTL クライアントをインストールして設定する前にこの作業を実行すれば、CAPF を使用するために CTL ファイルを更新する必要がなくなります。	Certificate Authority Proxy Function サービスのアクティブ化 (P.6-6)
ステップ 3 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。	TLS 接続用ポートの設定 (P.3-6)
ステップ 4 Cisco CTL クライアント用に設定するサーバについて、少なくとも 2 つのセキュリティトークンとパスワード、ホスト名または IP アドレス、およびポート番号を入手します。	Cisco CTL クライアントの設定(P.3-10)
ステップ 5 Cisco CTL クライアントをインストールします。	<ul style="list-style-type: none"> システム要件 (P.1-5) インストール (P.1-14) Cisco CTL クライアントのインストール (P.3-8)
ステップ 6 Cisco CTL クライアントを設定します。	Cisco CTL クライアントの設定(P.3-10)

Cisco CTL Provider サービスのアクティブ化

Cisco CTL クライアントの設定後、Cisco CTL Provider サービスによってセキュリティ モードが非セキュア モードから混合モードに変更され、サーバ証明書が CTL ファイルに転送されます。その後、このサービスによって、CTL ファイルがすべての Cisco Unified Communications Manager および Cisco TFTP サーバに転送されます。

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

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 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 Communications Manager 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。



(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 5** サービスがサーバで実行されていることを確認します。サービスの状態を確認するには、Cisco Unified 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.3-24 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

デフォルトのポートが現在使用中の場合や、ファイアウォールを使用していてファイアウォール内のポートを使用できない場合には、異なる TLS ポート番号の設定が必要になることもあります。

- Cisco CTL Provider の TLS 接続用デフォルト ポートは 2444 です。Cisco CTL Provider ポートでは 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、セキュリティ モードの設定、CTL ファイルの TFTP サーバへの保存など、Cisco CTL クライアントの要求を処理します。
- 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 Communications Manager の TLS 接続用ポートは Cisco Unified Communications Manager ポート番号に 443 を加算 (+) した番号になるため、Cisco Unified Communications Manager のデフォルトの TLS 接続は 2443 になります。ポートが現在使用中の場合や、ファイアウォールを使用していてファイアウォール内のポートを使用できない場合にのみ、この設定を更新します。
- SIP セキュア ポートを使用すると、Cisco Unified Communications Manager は SIP 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 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 Serviceability で Cisco CTL Provider サービスを再起動する必要があります。

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

デフォルト設定を変更するには、次の手順を実行します。

手順

ステップ 1 変更するポートに応じて、次の作業を実行します。

- Cisco CTL Provider サービスの Port Number パラメータを変更するには、[ステップ 2](#) ~ [ステップ 6](#) を実行します。
- [イーサネット電話ポート (Ethernet Phone Port)] または [SIP 電話セキュアポート (SIP Phone Secure Port)] の設定を変更するには、[ステップ 7](#) ~ [ステップ 11](#) を実行します。

ステップ 2 Cisco CTL Provider ポートを変更するには、Cisco Unified Communications Manager の管理ページで [システム] > [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 Communications Manager の管理ページで [システム] > [Cisco Unified CM] の順に選択します。
- ステップ 8** 『Cisco Unified Communications Manager アドミニストレーションガイド』の説明に従い、Cisco CallManager サービスを実行しているサーバを検索します。結果が表示されたら、サーバの [名前 (Name)] リンクをクリックします。
- ステップ 9** [Cisco Unified Communications Manager の設定 (Cisco Unified 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 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.3-24 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。

- セキュリティ モードの最初の設定時
- CTL ファイルの最初の作成時
- Cisco Unified Communications Manager のインストール後
- Cisco Unified Communications Manager サーバまたは Cisco Unified Communications Manager データの復元後
- Cisco Unified Communications Manager サーバの IP アドレスまたはホスト名の変更後
- セキュリティ トークンの追加後または削除後
- PIX Firewall の追加後または削除後
- TFTP サーバの追加後または削除後
- サードパーティ CA 署名証明書のプラットフォームへのアップロード後



ヒント

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

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

手順

- ステップ 1** 『Cisco Unified Communications Manager アドミニストレーション ガイド』の説明に従い、クライアントをインストールしようとする Windows ワークステーションまたはサーバから Cisco Unified Communications Manager の管理ページに移動します。
- ステップ 2** Cisco Unified Communications Manager の管理ページで、[アプリケーション] > [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 [インストール] 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.3-24 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 CallManager サービスおよび Cisco Tftp サービスを再起動する必要があるためです。

Cisco CTL クライアントは、次のタスクを実行します。

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



(注)

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



ヒント

Cisco Unified Communications Manager の管理ページの[エンタープライズパラメータ設定 (Enterprise Parameters Configuration)] ウィンドウで Cisco Unified Communications Manager クラスタのセキュリティ パラメータを混合モードに設定することはできません。クラスタ セキュリティ モードを設定するには、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.3-16 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 Communications Manager、PIX Firewall および CAPF サーバ用の証明書エントリが含まれたファイルです。

CTL ファイルによって、電話接続用の TLS をサポートするサーバが示されます。クライアントは自動的に Cisco Unified Communications Manager、Cisco CAPF、および PIX Firewall 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。

始める前に

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



ヒント

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

- セキュリティ トークンの管理者パスワード
- PIX Firewall 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、サーバへのネットワーク接続を確認します。ネットワーク接続した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』の説明に従って ping コマンドを実行します。

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

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

- CTL ファイルをすべての Cisco Unified Communications Manager サーバに書き込む。
- CAPF capf.cer を Cisco Unified Communications Manager に書き込む。
- すべての設定済み TFTP サーバにこのファイルを書き込む。
- すべての設定済み PIX Firewall にこのファイルを書き込む。
- 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 Communications Manager サーバの設定内容を入力し、[Next] をクリックします。

ステップ 4 表 3-2 の説明に従って、[Set Cisco Unified Communications Manager Cluster to Mixed Mode] をクリックし、[Next] をクリックします。

ステップ 5 設定する内容に応じて、次の作業を実行します。

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



注意

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

- ステップ 6** アプリケーションが要求したら、現在 Cisco CTL クライアントを設定しているワークステーションまたはサーバで使用可能な USB ポートにセキュリティ トークンを 1 つ挿入して、[OK] をクリックします。
- ステップ 7** 挿入したセキュリティ トークンについての情報が表示されます。[Add] をクリックします。
- ステップ 8** 検出された証明書エントリがペインに表示されます。
- ステップ 9** 他のセキュリティ トークン (複数も可能) を証明書信頼リストに追加するには、[Add Tokens] をクリックします。
- ステップ 10** サーバまたはワークステーションに挿入したトークンを取り外していない場合は、取り外します。アプリケーションが要求したら、次のトークンを挿入して [OK] をクリックします。
- ステップ 11** 2 番目のセキュリティ トークンについての情報が表示されます。[Add] をクリックします。
- ステップ 12** すべてのセキュリティ トークンについて、[ステップ 9 ~ ステップ 11](#) を繰り返します。
- ステップ 13** 証明書エントリがペインに表示されます。
- ステップ 14** [表 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** すべてのデバイスをリセットします。詳細については、[P.1-13 の「デバイスのリセット、サービスの再起動またはリブート」](#)を参照してください。
- ステップ 21** Cisco Unified Serviceability で、Cisco CallManager サービスおよび Cisco Tftp 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.3-24 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。

- Cisco Unified Communications Manager サーバの名前または IP アドレスを変更した場合
- いずれかの設定済み TFTP サーバの IP アドレスまたはホスト名を変更した場合
- いずれかの設定済み PIX Firewall の IP アドレスまたはホスト名を変更した場合
- Cisco Unified Serviceability で Cisco Certificate Authority Function サービスを有効にした場合
- セキュリティ トークンを追加または削除する必要がある場合
- TFTP サーバを追加または削除する必要がある場合
- PIX Firewall を追加または削除する必要がある場合
- Cisco Unified Communications Manager サーバまたは Cisco Unified Communications Manager データを復元した場合
- サードパーティの CA 署名証明書をプラットフォームにアップロードした後



ヒント

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

CTL ファイルにある情報を更新するには、次の手順を実行します。

手順

- ステップ 1** 最新の CTL ファイルを設定するために挿入したセキュリティ トークンを 1 つ入手します。
- ステップ 2** インストールしたワークステーションまたはサーバのデスクトップにある [Cisco CTL Client] アイコンをダブルクリックします。
- ステップ 3** 表 3-2 の説明に従って Cisco Unified Communications Manager サーバの設定内容を入力し、[Next] をクリックします。



ヒント

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

- ステップ 4** CTL ファイルを更新するには、表 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。

■ CTL ファイル エントリの削除

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

検出された証明書エントリがペインに表示されます。



ヒント このペインでは、Cisco Unified Communications Manager、Cisco TFTP、または PIX Firewall のエントリを更新できません。Cisco Unified Communications Manager エントリを更新するには、[Cancel] をクリックし、[ステップ2](#) ~ [ステップ6](#) をもう一度実行します。

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

- サーバ設定の更新手順または新しいセキュリティ トークンの追加手順については、[P.3-10](#) 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 トークンを削除するには、[P.3-14](#) の「[CTL ファイル エントリの削除](#)」を参照してください。

ステップ8 CTL ファイルの更新が終了したら、Cisco Unified Serviceability で、Cisco CallManager および Cisco Tftp サービスを再起動します。

追加情報

詳細については、[P.3-24](#) 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てから [Delete Selected] をクリックしてエントリを削除します。

Cisco Unified Communications Manager、Cisco TFTP、PIX Firewall、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.3-24](#) の「[関連項目](#)」を参照してください。

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

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



(注)

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

Cisco CTL クライアントの初期設定後にクラスタ セキュリティ モードを変更するには、CTL ファイルを更新する必要があります。[Cluster Security Mode] ウィンドウに移動して、モードの設定を変更し、[Next]、[Finish] の順にクリックします(P.3-13 の「CTL ファイルの更新」および表 3-2 を参照)。

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

Cisco CTL クライアントの設定内容

クラスタのセキュリティ モードは、表 3-2 の説明にあるように、非セキュア モードまたは混合モードのいずれかに設定できます。混合モードだけが認証、シグナリング暗号化、およびメディア暗号化をサポートしています。



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

表 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.3-24 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
Cisco Unified Communications Manager Server	
Hostname or IP Address	サーバのホスト名または IP アドレスを入力します。
Port	この Cisco Unified Communications Manager サーバで実行されている Cisco CTL Provider サービスの CTL ポート番号を入力します。デフォルトのポート番号は 2444 です。
Username and Password	スーパーユーザの管理者権限を持つアプリケーション ユーザのユーザ名とパスワードを入力します。
Security Mode	
Set Cisco Unified Communications Manager Cluster to Mixed Mode	混合モードでは、認証済みで暗号化済み、および非セキュアの Cisco Unified IP Phone を Cisco Unified Communications Manager に登録することができます。このモードでは、認証済みまたは暗号化済みのデバイスでセキュア ポートが使用されることを Cisco Unified Communications Manager が保証します。
	<p>(注) 混合モードに設定すると、Cisco Unified Communications Manager によって自動登録は無効になります。</p>

表 3-2 CTL クライアントの設定内容 (続き)




設定	説明
Set Cisco Unified Communications Manager Cluster to Non-Secure Mode	<p>非セキュア モードに設定すると、すべてのデバイスは非認証として登録され、Cisco Unified Communications Manager はイメージ認証のみサポートします。</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 Communications Manager に登録されます。</p> <p></p> <p>ヒント 電話機をデフォルトの非セキュア モードに戻すには、電話機およびすべての Cisco Unified Communications Manager サーバから CTL ファイルを削除する必要があります。</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、Cisco Unified Communications Manager のセキュリティ モードは変更されません。
CTL Entries	
Add Tokens	<p>証明書信頼リスト (CTL) にセキュリティ トークンを追加するには、このボタンをクリックします。</p> <p>サーバまたはワークステーションに最初に挿入したトークンを取り外していない場合は、取り外します。アプリケーションが要求したら、次のトークンを挿入して [OK] をクリックします。追加したセキュリティ トークンについての情報が表示されたら、[Add] をクリックします。すべてのセキュリティ トークンについて、これらの作業を繰り返します。</p>
Add TFTP Server	<p></p> <p>(注) この設定はクラスタ間環境にのみ適用されます。Cisco Unified Communications Manager Business Edition システムでは Intercluster Trunk (ICT; クラスタ間トランク) はサポートされていません。</p> <p>CTL に代替 TFTP サーバを追加するには、このボタンをクリックします。設定の詳細については、[Alternate TFTP Server] タブの設定値が表示された後で [Help] ボタンをクリックします。設定を入力したら、[Next] をクリックします。</p>
Add Firewall	CTL に PIX Firewall を追加するには、このボタンをクリックします。設定の詳細については、[Firewall] タブの設定値が表示された後で [Help] ボタンをクリックします。設定を入力したら、[Next] をクリックします。

表 3-2 CTL クライアントの設定内容 (続き)

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

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

クラスタのセキュリティ モードを確認するには、次の手順を実行します。



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

手順

- ステップ 1** Cisco Unified Communications Manager の管理ページで [システム] > [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 Communications Manager は混合モードに正しく設定されています。(詳細については、フィールド名をクリックしてください)。



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

追加情報

詳細については、[P.3-24 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 Communications Manager のアップグレードなどを行ったら、Smart Card サービスが「開始」および「自動」になっていることを確認します。

サービスを「開始」および「自動」に設定するには、次の手順を実行します。

手順

- ステップ 1** Cisco CTL クライアントをインストールしたサーバまたはワークステーションで、[スタート]>[プログラム]>[管理ツール]>[サービス]または[スタート]>[コントロール パネル]>[管理ツール]>[サービス]の順に選択します。
- ステップ 2** [サービス] ウィンドウで、Smart Card サービスを右クリックし、[プロパティ]を選択します。
- ステップ 3** [プロパティ] ウィンドウに [全般] タブが表示されていることを確認します。
- ステップ 4** [スタートアップの種類] ドロップダウン リスト ボックスから、[自動]を選択します。
- ステップ 5** [適用] をクリックします。
- ステップ 6** [サービスの状態] 領域で、[開始] をクリックします。
- ステップ 7** [OK] をクリックします。
- ステップ 8** サーバまたはワークステーションをリポートし、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.3-24 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い場合は挿入します。
 - 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.3-24 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 Communications Manager サーバから CTL ファイルを削除する予定がない場合にお勧めします。

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

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

Cisco Unified IP Phone 上の CTL ファイルを削除するには、表 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 および同等モデル	<p>次の方法のどちらかを実行します。</p> <ul style="list-style-type: none"> • [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 Communications Manager』を参照)。CTL オプションの下にある [削除] ソフトキーを押します。 • [設定] メニューにある [削除] ソフトキーを押します。 <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 Communications Manager』を参照してください。</p>

追加情報

詳細については、P.3-24 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.3-24 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、Cisco Unified Communications Manager 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.3-24 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.1-5)
- 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.3-5)
- 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 クライアントの設定 (P.3-10)
- Cisco CTL クライアントの設定 (P.3-10)
- CTL ファイルの更新 (P.3-13)
- CTL ファイル エントリの削除 (P.3-14)
- Cisco Unified Communications Manager セキュリティ モードの更新 (P.3-15)
- Cisco CTL クライアントの設定内容 (P.3-16)
- Cisco Unified Communications Manager のセキュリティ モードの確認 (P.3-19)
- Smart Card サービスの開始および自動の設定 (P.3-20)
- Cisco Unified IP Phone 上の CTL ファイルの削除 (P.3-22)
- Cisco CTL クライアントのバージョンの特定 (P.3-23)
- Cisco CTL クライアントの確認とアンインストール (P.3-23)
- 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 Communications Manager

Cisco Unified Communications Manager トラブルシューティングガイド



PART 2

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



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 \(P.4-2\)](#)
- [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 \(P.4-3\)](#)
- [その他の情報 \(P.4-4\)](#)

電話機のセキュリティ機能について

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

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



ヒント

サポートされていないシナリオまたは安全でないシナリオについては、P.1-8 の「[相互作用および制限](#)」を参照してください。

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

ユーザが Cisco Extension Mobility を使用する場合、Cisco Unified Communications Manager はデバイスの認証および暗号化ステータスを保持します。また、共有回線が設定されている場合も、Cisco Unified Communications Manager はデバイスの認証および暗号化ステータスを保持します。



ヒント

暗号化された Cisco Unified IP Phone に対して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

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

Cisco Unified Communications Manager の管理ページでセキュリティ機能を設定できませんが、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今回のバージョンの Cisco Unified Communications Manager をサポートする Cisco Unified IP Phone の管理マニュアルおよびユーザ マニュアルを参照してください。

Cisco Unified Communications Manager がコールを認証済みまたは暗号化済みとして分類すると、コールの状態を示すアイコンが電話機に表示されます。Cisco Unified Communications Manager が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.1-7 の「セキュリティ アイコン」および P.1-8 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
ステップ 1 Cisco CTL クライアントを設定し、Cisco Unified Communications Manager セキュリティ モードを混合モードにしていない場合、設定します。	Cisco CTL クライアントの設定 (P.3-1)
ステップ 2 電話機に、ローカルで有効な証明書 (LSC) または製造元でインストールされる証明書 (MIC) が含まれていない場合、Certificate Authority Proxy Function (CAPF) を使用して LSC をインストールします。	Certificate Authority Proxy Function の使用方法 (P.6-1)
ステップ 3 電話機のセキュリティ プロファイルを設定します。	電話機セキュリティ プロファイルの設定 (P.5-1)
ステップ 4 電話機のセキュリティ プロファイルを電話機に適用します。	電話機セキュリティ プロファイルの適用 (P.5-12)
ステップ 5 SIP 電話機がダイジェスト認証をサポートする場合、[エンドユーザの設定 (End User Configuration)] ウィンドウで、ダイジェスト クレデンシャルを設定します。	<ul style="list-style-type: none"> 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.8-4)
ステップ 6 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)
ステップ 7 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。	このマニュアルでは、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は説明しません。この作業の実行方法については、ユーザの電話機モデルと今回のバージョンの Cisco Unified Communications Manager をサポートする Cisco Unified IP Phone のアドミニストレーション ガイドを参照してください。
ステップ 8 電話機設定ファイルを暗号化します(電話機がこの機能をサポートする場合)。	暗号化された電話機設定ファイルの設定 (P.7-1)
ステップ 9 電話機の設定を無効にして電話機のセキュリティを強化します。	電話機のセキュリティ強化 (P.9-1)

その他の情報

関連項目

- [相互作用および制限 \(P.1-8\)](#)
- [認証、整合性、および許可の概要 \(P.1-18\)](#)
- [暗号化の概要 \(P.1-23\)](#)
- [設定用チェックリストの概要 \(P.1-26\)](#)
- [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 \(P.4-3\)](#)
- [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 Communications Manager*
- *Cisco Unified Communications Manager 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 Communications Manager 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 Communications Manager をインストールすると、自動登録用の事前定義済み非セキュア セキュリティ プロファイルのセットが提供されます。電話機でセキュリティ機能を有効にするには、そのデバイス タイプおよびプロトコルの新しいセキュリティ プロファイルを設定し、電話機に適用する必要があります。

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

電話機セキュリティ プロファイルの設定のヒント

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

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

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

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

レコードの絞り込みまたは検索

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



(注) 検索条件を追加するには、[+] ボタンをクリックします。条件を追加すると、指定したすべての条件に一致するレコードが検索されます。条件を削除するには、[-] ボタンをクリックして最後に追加した条件を削除するか、[フィルタのクリア] ボタンをクリックして追加したすべての検索条件を削除します。

ステップ 3 [検索] をクリックします。

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

ステップ 4 表示するレコードのリストから、表示するレコードのリンクをクリックします。



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

ウィンドウに選択した項目が表示されます。

追加情報

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 [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、[新規追加] ボタンをクリックするか、検索ウィンドウの [新規追加] アイコンをクリックし、[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.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、適切なプロファイルを見つけて、コピーするセキュリティ プロファイルの横に表示されている [コピー (Copy)] ボタンをクリックし、[ステップ 3](#) に進みます。
- 既存のプロファイルを更新するには、[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、各フィールドのデフォルト設定を示した設定ウィンドウが表示されます。[コピー] をクリックすると、設定をコピーした設定ウィンドウが表示されます。

ステップ 3 SCCP 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] ボタンまたは [保存] アイコンをクリックします。

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></p> <p>ヒント セキュリティ プロファイル名にデバイス モデルとプロトコルを含めると、プロファイルを検索または更新する場合の適切なプロファイルの検出に役立ちます。</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>
[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"> • [非セキュア]: 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 Communications Manager が利用できる。 • [認証のみ]: Cisco Unified Communications Manager は電話機の整合性と認証を提供する。シグナリング用に、NULL/SHA を使用する TLS 接続を開始する。 • [暗号化]: Cisco Unified Communications Manager 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。
[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 Communications Manager は電話機が TFTP サーバからダウンロードする設定ファイルを暗号化します。詳細については、P.1-25 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。</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
[認証モード (Authentication Mode)]	<p data-bbox="659 309 1481 376">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="659 398 1481 465">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 data-bbox="659 488 1481 589">• [認証ストリング]: 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 data-bbox="659 600 1481 790">• [Null ストリング]: ユーザが介入することなく、ローカルで有効な証明書をインストール、アップグレード、削除、またはトラブルシューティングします。 このオプションではセキュリティを一切提供しません。したがって、このオプションは安全な閉じた環境の場合にだけ選択することを強く推奨します。 <li data-bbox="659 801 1481 1171">• [既存の証明書 (LSC の優先)]: 製造元でインストールされる証明書 (MIC) またはローカルで有効な証明書 (LSC) が電話機に存在する場合、LSC をインストール、アップグレード、削除、またはトラブルシューティングします。LSC が電話機に存在する場合、MIC が電話機に存在するかどうかに関係なく、認証は LSC を介して行われます。MIC と LSC が電話機に存在する場合、認証は LSC を介して行われます。電話機に LSC が存在せず、MIC が存在する場合、認証は MIC を介して行われます。 このオプションを選択する前に、証明書が電話機に存在することを確認します。このオプションを選択した場合に証明書が電話機に存在しないと、操作は失敗します。 MIC と LSC は電話機で同時に存在できるものの、電話機は常に 1 つの証明書だけを使用して CAPF を認証します。優先されるプライマリ証明書が何らかの理由で侵害された場合、あるいは他の証明書を介して認証する場合には、認証モードを更新する必要があります。 <li data-bbox="659 1182 1481 1619">• [既存の証明書 (MIC の優先)]: LSC または MIC が電話機に存在する場合、LSC をインストール、アップグレード、削除、またはトラブルシューティングします。MIC が電話機に存在する場合、LSC が電話機に存在するかどうかに関係なく、認証は MIC を介して行われます。電話機に LSC だけが存在し MIC が存在しない場合、認証は LSC を介して行われます。 このオプションを選択する前に、証明書が電話機に存在することを確認します。このオプションを選択した場合に証明書が電話機に存在しないと、操作は失敗します。 <p data-bbox="659 1641 1481 1930"> (注) [電話セキュリティプロファイルの設定 (Phone Security Profile Configuration)] ウィンドウで設定される CAPF 設定は、[電話の設定 (Phone Configuration)] ウィンドウで設定される CAPF パラメータと相互に関係があります (詳細については、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 CAPF 設定を定義する方法については、『Cisco Unified Communications Manager アドミニストレーション ガイド』を参照してください。</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> (注) [電話セキュリティプロファイルの設定 (Phone Security Profile Configuration)] ウィンドウで設定される CAPF 設定は、[電話の設定 (Phone Configuration)] ウィンドウで設定される CAPF パラメータと相互に関係があります (詳細については、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 CAPF 設定を定義する方法については、『Cisco Unified Communications Manager アドミニストレーション ガイド』を参照してください。</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> ヒント セキュリティ プロファイル名にデバイス モデルとプロトコルを含めると、プロファイルを検索または更新する場合の適切なプロファイルの検出に役立ちます。</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、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 Communications Manager 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 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"> • [非セキュア]: 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 Communications Manager が利用できる。 • [認証のみ]: Cisco Unified Communications Manager は電話機の整合性と認証を提供する。シグナリング用に、NULL/SHA を使用する TLS 接続を開始する。 • [暗号化]: Cisco Unified Communications Manager 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。
[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 [非セキュア] 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"> • [TCP]: パケットを送信された順に受信するには、Transmission Control Protocol を選択します。このプロトコルは、パケットがドロップされないことを保証しますが、セキュリティは提供しません。 • [UDP]: パケットを高速に受信するには、User Datagram Protocol を選択します。このプロトコルは、パケットをドロップすることがあり、送信された順に受信するとは限りません。セキュリティは提供しません。 • [TCP + UDP]: TCP と UDP を組み合わせて使用するには、このオプションを選択します。このオプションは、セキュリティを提供しません。 <p>[デバイスセキュリティモード (Device Security Mode)] が [認証のみ] または [暗号化] 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 Communications Manager は、電話機からのすべての SIP 要求でチャレンジを行います。</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 [認証のみ] または [暗号化] 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.1-20 の「ダイジェスト認証」および 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。</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 Communications Manager は電話機が TFTP サーバからダウンロードする設定ファイルを暗号化します。このオプションは、シスコ製電話機専用です。</p> <p> ヒント このオプションを有効にして、対称キーを設定し、ダイジェスト 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、P.1-25 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。</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 Communications Manager は電話機が TFTP サーバからダウンロードする設定ファイル内のダイジェスト クレデンシャルを削除します。このオプションは、Cisco Unified IP SIP Phone 7905、7912、7940、および 7960 モデル専用です。</p> <p>詳細については、P.1-25 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。</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 data-bbox="659 309 1481 376">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 data-bbox="659 398 1481 465">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 data-bbox="659 488 1481 589">• [認証ストリング]: 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 data-bbox="659 600 1481 790">• [Null ストリング]: ユーザが介入することなく、ローカルで有効な証明書をインストール、アップグレード、またはトラブルシューティングします。 このオプションではセキュリティ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。 <li data-bbox="659 801 1481 1137">• [既存の証明書 (LSC の優先)]: 製造元でインストールされる証明書 (MIC) またはローカルで有効な証明書 (LSC) が電話機に存在する場合、LSC をインストール、アップグレード、またはトラブルシューティングします。LSC が電話機に存在する場合、MIC が電話機に存在するかどうかに関係なく、認証は LSC を介して行われます。電話機に LSC が存在せず、MIC が存在する場合、認証は MIC を介して行われます。 このオプションを選択する前に、証明書が電話機に存在することを確認します。このオプションを選択した場合に証明書が電話機に存在しないと、操作は失敗します。 MIC と LSC は電話機で同時に存在できるものの、電話機は常に 1 つの証明書だけを使用して CAPF を認証します。優先されるプライマリ証明書が何らかの理由で侵害された場合、あるいは他の証明書を介して認証する場合には、認証モードを更新する必要があります。 <li data-bbox="659 1149 1481 1585">• [既存の証明書 (MIC の優先)]: LSC または MIC が電話機に存在する場合、LSC をインストール、アップグレード、またはトラブルシューティングします。MIC が電話機に存在する場合、LSC が電話機に存在するかどうかに関係なく、認証は MIC を介して行われます。電話機に LSC だけが存在し MIC が存在しない場合、認証は LSC を介して行われます。 このオプションを選択する前に、証明書が電話機に存在することを確認します。このオプションを選択した場合に証明書が電話機に存在しないと、操作は失敗します。 <p data-bbox="659 1608 1481 1930"> (注) [電話セキュリティプロファイルの設定 (Phone Security Profile Configuration)] ウィンドウで設定される CAPF 設定は、[電話の設定 (Phone Configuration)] ウィンドウで設定される CAPF パラメータと相互に関係があります (詳細については、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 CAPF 設定を定義する方法については、『Cisco Unified Communications Manager アドミニストレーション ガイド』を参照してください。</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の設定 (Phone Security Profile Configuration)] ウィンドウで設定される CAPF 設定は、[電話の設定 (Phone Configuration)] ウィンドウで設定される CAPF パラメータと相互に関係があります (詳細については、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 CAPF 設定を定義する方法については、『Cisco Unified Communications Manager アドミニストレーション ガイド』を参照してください。</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 SIP IP Phone が、Cisco Unified Communications Manager からの SIP メッセージの傍受に使用するポート番号を入力します。デフォルト設定は 5060 です。</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 Communications Manager アドミニストレーション ガイド』の説明に従って、電話機を検索します。
 - ステップ 2** [電話の設定 (Phone Configuration)] ウィンドウが表示されたら、[デバイスセキュリティプロファイル (Device Security Profile)] を見つけます。
 - ステップ 3** [デバイスセキュリティプロファイル (Device Security Profile)] ドロップダウン リスト ボックスから、デバイスに適用するセキュリティ プロファイルを選択します。該当する電話機タイプおよびプロトコル用に設定されている電話機セキュリティ プロファイルだけが表示されます。
 - ステップ 4** [保存] 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 Communications Manager データベースから電話機セキュリティ プロファイルを削除する方法について説明します。

始める前に

Cisco Unified Communications Manager の管理ページからセキュリティ プロファイルを削除する前に、別のプロファイルをデバイスに適用するか、該当プロファイルを使用するすべてのデバイスを削除してください。該当プロファイルを使用しているデバイスを検索するには、セキュリティプロファイルの設定ウィンドウの[関連リンク]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 Communications Manager システム ガイド』を参照してください。

手順

-
- ステップ 1** 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。
 - ステップ 2** 複数のセキュリティ プロファイルを削除するには、検索と一覧表示ウィンドウで、適切なチェックボックスの横に表示されているチェックボックスをオンにして、[選択項目の削除] 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。[すべてを選択] をクリックしてから [選択項目の削除] をクリックすると、この選択で設定可能なすべてのレコードを削除できます。
 - ステップ 3** 単一のセキュリティ プロファイルを削除するには、次の作業のどちらかを実行します。
 - 検索と一覧表示ウィンドウで、適切なセキュリティ プロファイルの横に表示されているチェックボックスをオンにして、[選択項目の削除] 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 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.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

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

ステップ 1 [デバイス]>[電話]の順に選択します。

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

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



(注) 検索条件を追加するには、[+] ボタンをクリックします。条件を追加すると、指定したすべての条件に一致するレコードが検索されます。条件を削除するには、[-] ボタンをクリックして最後に追加した条件を削除するか、[フィルタのクリア] ボタンをクリックして追加したすべての検索条件を削除します。

ステップ 3 [検索] をクリックします。

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

ステップ 4 表示するレコードのリストから、表示するレコードのリンクをクリックします。



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

ウィンドウに選択した項目が表示されます。

追加情報

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 \(P.1-20\)](#)
- [設定ファイルの暗号化 \(P.1-25\)](#)
- [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 Communications Manager 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 Communications Manager



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 \(P.6-3 \)](#)
- [CAPF システムの相互作用および要件 \(P.6-4 \)](#)
- [Cisco Unified 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 Communications Manager 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 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。

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 Cisco Unified Communications Manager サーバにコピーされ、拡張子 .0 を使用します。CAPF 証明書が存在することを確認するには、Cisco Unified Communications オペレーティング システムの GUI で、CAPF 証明書を表示します。

Cisco Unified IP Phone と CAPF の相互作用

CAPF と相互に作用するとき、電話機は認証文字列、既存の MIC または 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 Communications Manager、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 Communications Manager によって電話機がリセットされたときに CAPF が Cisco Unified IP Phone 7960 および 7940 とどのように相互に作用するかについて説明します。



(注)

次の例では、LSC が電話機内にまだ存在しない場合や、CAPF 情報の [認証モード (Authentication Mode)] に [既存の証明書] 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 [非セキュア] に、CAPF 情報の [認証モード (Authentication Mode)] を [Null スtring] または [既存の証明書 (... の優先)] 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 Cisco Unified Communications Manager に登録し、設定ファイルを受け取ります。次に、電話機は自動的に CAPF とのセッションを開始し、LSC をダウンロードします。LSC のインストール後、電話機は [デバイスセキュリティモード (Device Security Mode)] を [認証のみ] または [暗号化] に設定します。

例：認証のみまたは暗号化デバイス セキュリティ モード

この例では、[デバイスセキュリティモード (Device Security Mode)] を [認証のみ] または [暗号化] に、CAPF 情報の [認証モード (Authentication Mode)] を [Null スtring] または [既存の証明書 (... の優先)] 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 Cisco Unified Communications Manager に登録しません。セッションが終了すると、電話機は登録を行い、すぐに認証済みまたは暗号化済みモードで動作します。

この例では、電話機は CAPF サーバに自動的に接続しないので、[認証 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、Cisco Certificate Authority Proxy Function サービスをアクティブにする必要があります。
- 証明書のアップグレードまたはインストール操作で、電話機に対して CAPF 認証方式を [認証 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。
- 証明書操作の間、Cisco Unified Communications Manager 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。

**ヒント**

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

Cisco Unified Serviceability での CAPF の設定

次の作業を Cisco Unified 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 Communications Manager 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 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をインストール、アップグレード、またはトラブルシューティングする場合に実行する作業のリストを示します。

表 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
ステップ 1 ローカルで有効な証明書が電話機に存在するかどうかを判別します。	<ul style="list-style-type: none"> • 使用している電話機モデルとこのバージョンの Cisco Unified Communications Manager をサポートする電話機のマニュアル • このバージョンの Cisco Unified Communications Manager をサポートする『Data Migration Assistant ユーザガイド』
ステップ 2 Cisco Certificate Authority Proxy Function サービスが実行されていることを確認します。 ヒント このサービスは、すべての CAPF 操作時に実行されている必要があります。またこのサービスは、CTL ファイルに CAPF 証明書を組み込むために、Cisco CTL クライアントでも実行されている必要があります。	Certificate Authority Proxy Function サービスのアクティブ化 (P.6-6)
ステップ 3 Cisco CTL クライアントのインストールおよび設定に必要なすべての作業を実行したことを確認します。CAPF 証明書が Cisco CTL ファイル内に存在することを確認します。	Cisco CTL クライアントの設定 (P.3-10)
ステップ 4 必要に応じて、CAPF サービス パラメータを更新します。	<ul style="list-style-type: none"> • 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)
ステップ 5 電話機のローカルで有効な証明書をインストール、アップグレード、またはトラブルシューティングするには、Cisco Unified Communications Manager の管理ページを使用します。	<ul style="list-style-type: none"> • 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)
ステップ 6 証明書の操作が必要な場合は、認証文字列を電話機に入力します。	電話機での認証文字列の入力 (P.6-12)

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

Cisco Unified Communications Manager では、Cisco Unified 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。

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 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** [保存] 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 Communications Manager 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 Communications Manager 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、サーバを選択します。
- ステップ 3** [サービス (Service)] ドロップダウン リスト ボックスから、Cisco 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 Communications Manager アドミニストレーション ガイド』の説明に従って、電話機を検索します。
 - ステップ 2** 検索結果が表示された後、証明書をインストール、アップグレード、削除、またはトラブルシューティングする電話機を見つけて、その電話機の [デバイス名 (Device Name、回線)] リンクをクリックします。
 - ステップ 3** [表 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 Communications Manager の管理ページの [電話の設定 (Phone Configuration)] ウィンドウにある CAPF 設定について説明しています。

- 設定のヒントについては、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"> • [保留中の操作なし]: 証明書の操作が発生しないときに表示されます (デフォルトの設定)。 • [インストール/アップグレード]: 電話機にローカルで有効な証明書を新しくインストールするか、あるいは既存の証明書をアップグレードします。 • [削除]: 電話機に存在するローカルで有効な証明書を削除します。 • [トラブルシューティング]: ローカルで有効な証明書 (LSC) または製造元でインストールされる証明書 (MIC) を取得します。取得することで、CAPF トレース ファイルで証明書のクレデンシャルを確認できます。電話機に両方の種類の証明書が存在する場合、Cisco Unified Communications Manager は証明書の種類ごとに 1 つずつ、2 つのトレース ファイルを作成します。 <p> ヒント [トラブルシューティング] オプションを選択すると、LSC または MIC が電話機に存在することを確認できます。電話機に証明書が存在しない場合、[削除] オプションと [トラブルシューティング] オプションは表示されません。</p>
[認証文字列 (Authentication String)]	<p>[認証ストリング] 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せん。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。詳細については、P.6-12 の「電話機での認証文字列の入力」を参照してください。</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>
[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、< 操作のタイプ > pending、failed、successful など、操作のタイプには証明書操作オプションの [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] 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 [デバイス] > [電話] の順に選択します。

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

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

- [LSC ステータス]: 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 2 番目のドロップダウン リスト ボックスから、検索パターンを選択します。

ステップ 4 必要に応じて適切な検索テキストを指定します。



(注) 検索条件を追加するには、[+] ボタンをクリックします。条件を追加すると、指定したすべての条件に一致するレコードが検索されます。条件を削除するには、[-] ボタンをクリックして最後に追加した条件を削除するか、[フィルタのクリア] ボタンをクリックして追加したすべての検索条件を削除します。

ステップ 5 [検索] をクリックします。

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

ステップ 6 表示するレコードのリストから、表示するレコードのリンクをクリックします。



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

ウィンドウに選択した項目が表示されます。

追加情報

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 [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。アクティブな (前の) クエリーのレコードもウィンドウに表示される場合があります。

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

レコードの絞り込みまたは検索

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



(注) 検索条件を追加するには、[+] ボタンをクリックします。条件を追加すると、指定したすべての条件に一致するレコードが検索されます。条件を削除するには、[-] ボタンをクリックして最後に追加した条件を削除するか、[フィルタのクリア] ボタンをクリックして追加したすべての検索条件を削除します。

ステップ 3 [検索] をクリックします。

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

ステップ 4 [関連リンク] 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 5 ファイルを任意の場所に保存します。

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

追加情報

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。
- Cisco Unified Communications Manager サーバが実行中で機能している。
- デバイスが登録済みである。
- 署名付きイメージが電話機に存在する。使用している電話機モデルをサポートする Cisco Unified IP Phone の管理マニュアルを参照してください。

手順

- ステップ 1** 電話機の設定ボタンを押します。
- ステップ 2** 設定がロックされている場合は、**# (アスタリスク、アスタリスク、ポンド記号) を押してロックを解除します。
- ステップ 3** 下方にスクロールして [Settings (設定)] メニューに移動します。[Security Configuration (セキュリティ設定)] を強調表示し、[Select (選択)] ソフトキーを押します。
- ステップ 4** 下方にスクロールして [Security Configuration (セキュリティ設定)] メニューに移動します。[LSC] を強調表示し、[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要求するプロンプトが表示された場合、システムから提供された文字列を入力して [Submit (送信)] ソフトキーを押します。

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

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

[Stop (中止)] オプションを選択すると、いつでも手順を停止できます。

電話機での認証文字列の確認

[Settings (設定)] > [Model Information (モデル情報)] の順に選択して LSC の設定が [Installed (インストール済み)] か [Not Installed (未インストール)] のどちらであるかを確認すれば、証明書がインストールされているかどうかを確認できます。

追加情報

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 \(P.6-3 \)](#)
- [CAPF システムの相互作用および要件 \(P.6-4 \)](#)
- [Cisco Unified 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 Communications Manager

Cisco Unified Communications Manager Serviceability アドミニストレーションガイド



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 \(P.7-13\)](#)

電話機設定ファイルの暗号化について

電話機が Cisco Unified Communications Manager からダウンロードする設定ファイル内のダイジェスト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 Communications Manager 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 Communications Manager の管理ページおよび電話機で、必要なパラメータを設定し、Cisco Unified 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モデルがあります。電話機モデルとプロトコルによって、設定ファイルの暗号化に使用される方式が決まります。サポートされる方式は、Cisco Unified Communications Manager の機能と、暗号化された設定ファイルをサポートするファームウェア ロードに依存します。暗号化された設定ファイルをサポートしないバージョンに電話機ファームウェアをダウングレードした場合、TFTP サーバは、最小限の設定内容を含む暗号化されていない設定ファイルを提供します。その結果、電話機が期待されるとおりに動作しない可能性があります。

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

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

- [鍵の手動配布](#)
- [電話機の公開鍵による対称キーの暗号化](#)

「[鍵の手動配布](#)」および「[電話機の公開鍵による対称キーの暗号化](#)」の項の情報は、混合モードに設定し、Cisco Unified Communications Manager の管理ページで 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。

鍵の手動配布では、電話機がリセットされた後、Cisco Unified Communications Manager データベースに格納されている 128 ビットまたは 256 ビットの対称キーによって、電話機設定ファイルが暗号化されます。使用中の電話機モデルの鍵サイズを判別するには、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入力するか、Cisco Unified Communications Manager 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] 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 Communications Manager は、TFTP サーバが署名した暗号化された設定ファイルを電話機にダウンロードします。すべての電話機タイプが設定ファイルの署名者を検証するわけではありません。詳細については、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 Communications Manager に対する Cisco Unified IP Phone を認証し、電話機の証明書 (LSC) を発行します。

電話機に、製造元でインストールされる証明書 (MIC) またはローカルで有効な証明書 (LSC) が含まれている場合、電話機には、PKI 暗号化で使用される公開鍵と秘密鍵のペアが含まれています。

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

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

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



ヒント

この暗号化方式をサポートする電話機は、設定ファイルの暗号化設定フラグを使用して、暗号化されたファイルと暗号化されていないファイルのどちらを要求するかを決定します。[TFTP 暗号化] 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 Communications Manager 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 Communications Manager データベースと同期させることができます。エラー状態が解消された場合、電話機は次回リセット時に暗号化された設定ファイルを要求します。

サポートされる電話機のモデル

次の Cisco Unified IP Phone モデルで、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 SIP IP Phone 7905 または 7912	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 SIP IP Phone 7940 または 7960	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 SIP IP Phone 7970 または 7971、 Cisco Unified SIP IP Phone 7941 または 7961、 Cisco Unified SIP IP Phone 7911 Cisco Unified SIP IP Phone 7906	電話機の公開鍵による対称キーの暗号化 (PKI 暗号化)： 暗号化アルゴリズム：AES 128 鍵サイズ：128 ビット
Cisco Unified SCCP IP Phone 7970 または 7971、 Cisco Unified SCCP IP Phone 7941 または 7961、 Cisco Unified SIP IP Phone 7931、 Cisco Unified SCCP IP Phone 7911、 Cisco Unified SCCP IP Phone 7906	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 Communications Manager 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 Communications Manager で対称キーが欠落していたり、不一致が発生したりすると、電話機は登録できません。

Cisco Unified Communications Manager の管理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 SCCP Phone 7905、7912、7940、および 7960 は設定ファイルのダウンロードで機密データを受信しないため、これらの電話機に暗号化された設定ファイルを設定することはできません。
- [TFTP 暗号化] 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 モデルの場合、Cisco Unified Communications Manager で、暗号化された設定ファイルを有効にするために、デバイス セキュリティ モードを認証済みまたは暗号化済みに設定する必要はありません。Cisco Unified Communications Manager は、登録中の公開鍵をダウンロードするために CAPF プロセスを使用します。
- ご使用の環境がセキュアであることがわかっている場合、または PKI が有効でない電話機に対称キーを手動で設定することを避ける場合は、暗号化されていない設定ファイルを電話機にダウンロードすることもできます。ただし、この方法はお勧めできません。
- Cisco Unified IP SIP Phone 7905、7912、7940、および 7960 の場合、Cisco Unified Communications Manager 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、[設定ファイル内のダイジェスト信用証明書を除外 (Exclude Digest Credentials in Configuration File)] 設定を使用します。これは、まず対称キーを設定して電話機に入力するという作業が不要であるため、ダイジェスト クレデンシャルの初期化に便利です。

この方式では、暗号化されていない設定ファイルで電話機にダイジェスト 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 Communications Manager 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。  (注) クラスタ セキュリティ モードは、クラスタまたはスタンドアロン サーバのセキュリティ機能を設定します。	Cisco CTL クライアントの設定 (P.3-1)
ステップ 2 [電話セキュリティプロファイルの設定 (Phone Security Profile Configuration)]で[TFTP 暗号化]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"> 暗号化された設定ファイルの設定のヒント (P.7-6) 電話機設定ファイルの暗号化の有効化 (P.7-8) 電話機セキュリティ プロファイルの適用 (P.5-12)
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する場合は、鍵の手動配布の作業を実行します。	<ul style="list-style-type: none"> 暗号化された設定ファイルの設定のヒント (P.7-6) 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)
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"> 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) Certificate Authority Proxy Function の使用方法 (P.6-1)

電話機設定ファイルの暗号化の有効化

TFTP サーバは、設定ファイルを構築するときに、データベースに問い合わせます。電話機に適用されている電話機セキュリティ プロファイルで TFTP 暗号化フラグが設定されている場合、TFTP サーバは暗号化された設定ファイルを構築します。

TFTP 暗号化フラグにアクセスするには、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.7-13 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 Communications Manager データベースに存在する。
- 互換性のあるファームウェア ロードが TFTP サーバに存在する。
- Cisco Unified Communications Manager の管理ページで TFTP Encrypted Config パラメータを有効にしている。

手順

-
- ステップ 1** 『Cisco Unified Communications Manager アドミニストレーション ガイド』の説明に従って、電話機を検索します。
 - ステップ 2** [電話の設定 (Phone Configuration)] ウィンドウが表示された後、[表 7-2](#) の説明に従って、鍵の手動配布設定を定義します。これらの設定を行った後は、鍵は変更できません。
 - ステップ 3** [保存] 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.7-13 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.7-13 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 Communications Manager は入力された値を拒否します。Cisco Unified Communications Manager は、次の鍵サイズをサポートします。</p> <ul style="list-style-type: none"> • Cisco Unified IP Phone 7905、7912(SIP プロトコルのみ): 256 ビット • Cisco Unified IP Phone 7940 および 7960(SIP プロトコルのみ): 128 ビット <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 Communications Manager の管理ページで 16 進文字列を生成するには、[文字列を生成] 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 Communications Manager 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)] メニューを下方にスクロールし、電話のロック解除を強調表示して [Select (選択)] ソフトキーを押します。電話機のパスワードをキー入力し、[Accept] ソフトキーを押します。

電話機はパスワードを受け入れます。

ステップ 3 [Settings (設定)] メニューを下方にスクロールし、[Security Configuration (セキュリティ設定)] を強調表示し、[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、[Select (選択)] ソフトキーを押します。

ステップ 5 暗号鍵の入力を要求されたら、鍵 (16 進) を入力します。鍵をクリアする必要がある場合、ゼロを 32 回入力します。

ステップ 6 鍵の入力が終了したら、[Accept] ソフトキーを押します。

電話機は暗号鍵を受け入れます。

ステップ 7 電話機をリセットします。

電話機のリセット後、電話機は暗号化された設定ファイルを要求します。

LSC 証明書または MIC 証明書がインストールされていることの確認

この手順は、PKI 暗号化を使用する Cisco Unified IP Phone に適用されます。使用中の電話機が、電話機の公開鍵による対称キーの暗号化 (PKI 暗号化) 方式をサポートするかどうかを判別するには、[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 Communications Manager データベースに電話機が存在し、Cisco Unified Communications Manager 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 セクションで [トラブルシューティング] オプションを選択することにより、LSC または MIC が電話機に存在することを Cisco Unified Communications Manager の管理ページで確認できます。電話機に証明書が存在しない場合、[削除] オプションと [トラブルシューティング] オプションは表示されません。

電話機のセキュリティ設定を調べる方法でも、電話機に LSC または MIC が存在するかどうか確認できます。詳細については、このバージョンの Cisco Unified Communications Manager をサポートする Cisco Unified IP Phone モデルの Cisco Unified IP Phone のアドミニストレーション ガイドを参照してください。

- ステップ 2** 証明書が存在しない場合は、[電話の設定 (Phone Configuration)] ウィンドウの CAPF 機能を使用して、LSC をインストールします。LSC をインストールする方法については、[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.7-13 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、7931 (SCCP のみ)、7941、7961、7970、および 7971 : SEP<MAC>.cnf.xml.enc.sgn

電話機で設定ファイルにアクセスするには、暗号化をサポートする Cisco Unified IP Phone モデルと今回のリリースの Cisco Unified Communications Manager 用の 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。

電話機設定ファイルの暗号化の無効化

電話機設定ファイルの暗号化を無効にするには、Cisco Unified Communications Manager の管理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 Communications Manager データベースに残ります。

Cisco Unified IP Phone 7911、7931 (SCCP のみ)、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 SIP Phone 7940/7960/7905/7912 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 SIP Phone 7940 および 7960 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 SIP Phone 7905 および 7912 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 SIP Phone 7905、7912、7940、および 7960 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.7-13](#)の「[関連項目](#)」を参照してください。

その他の情報

関連項目

- [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 Communications Manager Bulk Administration アドミニストレーション 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

電話機のダイジェスト認証を有効にしている場合、Cisco Unified Communications Manager は、キーブ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 Communications Manager は、[エンドユーザの設定 (End User Configuration)] ウィンドウで設定されたエンドユーザのダイジェスト 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 Communications Manager は、[エンドユーザの設定 (End User Configuration)] ウィンドウで設定されたエクステンション モビリティ エンドユーザのダイジェスト 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.1-20 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 Communications Manager アドミニストレーションガイド*』の付録 C を参照してください。

この章は、次の内容で構成されています。

- [SIP 電話機ダイジェスト認証の設定用チェックリスト \(P.8-2\)](#)
- [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 \(P.8-4\)](#)
- [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 \(P.8-5\)](#)

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
ステップ 1 SIP 電話機のセキュリティ プロファイルを設定します。 [ダイジェスト認証を有効化 (Enable Digest Authentication)] チェックボックスがオンになっていることを確認しま す。	電話機セキュリティ プロファイルの設定 (P.5-1)
ステップ 2 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。	電話機セキュリティ プロファイルの設定 (P.5-1)
ステップ 3 デフォルト設定を更新する場合は、ダイジェスト認証に 関連するサービス パラメータ (SIP Station Realm サービ スパラメータなど) を設定します。	ダイジェスト認証サービス パラメータの設定 (P.8-3)
ステップ 4 [エンドユーザの設定 (End User Configuration)] ウィンド ウで、ダイジェスト クレデンシャルを設定します。	<ul style="list-style-type: none"> • 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.8-4)
ステップ 5 [電話の設定 (Phone Configuration)] ウィンドウで [ダイ ジェストユーザ (Digest User)] を選択します。 Cisco Unified SIP IP Phone 7970、7971、7961G/41G、 7961GE/41GE、および 7911 モデルでは、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。	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)
ステップ 6 Cisco Unified SIP IP Phone 7940 モデルまたは 7960 モデル では、[エンドユーザの設定 (End User Configuration)] ウィ ンドウで設定したダイジェスト クレデンシャルを入力し ます。	電話機で認証名およびパスワードを入力する方 法については、このバージョンの Cisco Unified Communications Manager をサポートする『Cisco Unified IP Phone 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 Communications Manager にはデフォルト設定の「ccmsipline」が含まれています。パラメータの詳細については、[サービスパラメータ設定 (Service Parameter Configuration)] ウィンドウに表示されている疑問符またはパラメータ名リンクをクリックします。

ダイジェスト認証サービス パラメータ (SIP Realm Station パラメータなど) を更新するには、次の手順を実行します。

手順

- ステップ 1** Cisco Unified Communications Manager の管理ページで、[システム] > [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。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.8-5 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 Communications Manager データベースにエンドユーザが存在することを前提としています。エンドユーザのダイジェスト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 Communications Manager アドミニストレーションガイド』の説明に従って、エンドユーザを検索します。
- ステップ 2** 目的の [エンドユーザの設定 (End User Configuration)] ウィンドウが表示されたら、表 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.8-5 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、[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 Communications Manager アドミニストレーション ガイド』の説明に従って、電話機を検索します。
- ステップ 2** 目的の[電話の設定 (Phone Configuration)]ウィンドウが表示されたら、[**ダイジェストユーザ (Digest User)**]設定を見つけて、電話機と関連付けるエンド ユーザを選択します。
- ステップ 3** [**保存**]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 ユーザを電話機に関連付けたら、設定を保存し、電話機をリセットします。

追加情報

詳細については、P.8-5 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 \(P.1-20\)](#)
- [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 \(P.8-4\)](#)
- [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、[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 \(P.9-1 \)](#)
- [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 Communications Manager 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 Communications Manager の管理ページで [Setting Access] 設定を無効にする必要があります。

PC Port 設定の無効化

デフォルトで Cisco Unified Communications Manager は PC ポートのあるすべての Cisco Unified IP Phone 上で PC ポートを有効にします。必要に応じて、[電話の設定 (Phone Configuration)] ウィンドウで [PC Port] 設定を無効にすることができます。PC ポートを無効にすると、ロビーや会議室の電話機で役立ちます。

電話機設定のセキュリティ強化



注意

次の手順を実行すると、電話機の機能が無効になります。

電話機の機能を無効にするには、次の手順を実行します。

手順

- ステップ 1** Cisco Unified Communications Manager の管理ページで、[**デバイス**] > [**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 \(P.9-1 \)](#)
- [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 Communications Manager



セキュアな会議リソースの設定

この章は、次の内容で構成されています。

- [セキュアな会議の概要 \(P.10-2\)](#)
- [会議ブリッジの要件 \(P.10-3\)](#)
- [セキュアな会議のアイコン \(P.10-4\)](#)
- [セキュアな会議の保守 \(P.10-5\)](#)
- [Cisco Unified IP Phone サポート \(P.10-7\)](#)
- [CTI サポート \(P.10-8\)](#)
- [トランクおよびゲートウェイでのセキュアな会議 \(P.10-8\)](#)
- [CDR データ \(P.10-8\)](#)
- [相互作用および制限 \(P.10-9\)](#)
- [会議リソースのセキュリティを確保するための設定のヒント \(P.10-11\)](#)
- [セキュアな会議ブリッジの設定用チェックリスト \(P.10-12\)](#)
- [Cisco Unified Communications Manager の管理ページでのセキュアな会議ブリッジの設定 \(P.10-13\)](#)
- [ミートミー会議の最小セキュリティ レベルの設定 \(P.10-14\)](#)
- [セキュアな会議ブリッジのパケット キャプチャの設定 \(P.10-14\)](#)
- [その他の情報 \(P.10-15\)](#)

セキュアな会議の概要

セキュアな会議機能では、会議の安全を確保するための認証と暗号化を提供します。接続されているすべてのデバイスでシグナリングおよびメディアが暗号化されている場合、会議は安全です。セキュアな会議機能は、セキュアな TLS または IPSec 接続での SRTP 暗号化をサポートしています。

システムには、会議の全体的なセキュリティ ステータスを示すセキュリティ アイコンが用意されています。セキュリティ ステータスは、接続されているデバイスのうち最も低いセキュリティ レベルで決まります。たとえば、2 つの暗号化済み接続と 1 つの認証済み接続を含むセキュアな会議の場合、会議のセキュリティ ステータスは、認証済みになります。

セキュアなアドホック会議とミートミー会議を設定するには、セキュアな会議ブリッジを設定します。

- 認証済みまたは暗号化済みの電話機からユーザが会議コールを開始すると、Cisco Unified Communications Manager はセキュアな会議ブリッジを割り当てます。
- 非セキュアの電話機からユーザがコールを開始すると、Cisco Unified Communications Manager は非セキュアの会議ブリッジを割り当てます。

会議ブリッジ リソースを非セキュアとして設定すると、電話機のセキュリティ設定にかかわらず、会議は非セキュアになります。



(注)

Cisco Unified Communications Manager は、会議を開始している電話機の Media Resource Group List (MRGL; メディア リソース グループ リスト) から会議ブリッジを割り当てます。セキュアな会議ブリッジが使用不可である場合、Cisco Unified Communications Manager は非セキュアの会議ブリッジを割り当て、会議は非セキュアになります。同様に、非セキュアの会議ブリッジが使用不可である場合、Cisco Unified Communications Manager はセキュアな会議ブリッジを割り当て、会議はセキュアになります。使用可能な会議ブリッジがない場合、コールは失敗します。

ミートミー会議コールの場合、会議を開始する電話機は、ミートミー番号用に設定された最小セキュリティ要件も満たしている必要があります。使用可能なセキュアな会議ブリッジがない場合や開催者のセキュリティ レベルが最小要件を満たしていない場合、Cisco Unified Communications Manager は会議の試行を拒否します。詳細については、P.10-6 の「[最小セキュリティ レベルでのミートミー会議](#)」を参照してください。

割り込みを使用する会議の安全を確保するには、暗号化済みモードを使用するよう電話機を設定します。デバイスが認証済みまたは暗号化済みである場合に割り込みキーを押すと、Cisco Unified Communications Manager によって割り込み側と発信先デバイスのビルトイン ブリッジとの間に安全な接続が確立されます。システムは、割り込みコールに接続されているすべての参加者に対して会議のセキュリティ ステータスを示します。



(注)

リリース 8.3 以降を実行している非セキュアまたは認証済みの Cisco Unified IP Phone は、暗号化済みコールを割り込ませることができるようになりました。

会議ブリッジの要件

会議ブリッジは、ハードウェア会議ブリッジをネットワークに追加して Cisco Unified Communications Manager の管理ページでセキュアな会議ブリッジを設定する際に、セキュアなメディア リソースとして登録できます。

H.323 または MGCP ゲートウェイで会議を提供する Digital Signal Processor (DSP; デジタル シグナル プロセッサ) ファームは、IP テレフォニー会議のネットワーク リソースとして機能します。会議ブリッジは、セキュアな SCCP クライアントとして Cisco Unified Communications Manager に登録されます。

- 会議ブリッジのルート証明書が Cisco Unified Communications Manager の信頼ストア内に存在し、Cisco Unified Communications Manager 証明書が会議ブリッジの信頼ストア内に存在している必要があります。
- セキュアな会議ブリッジのセキュリティ設定が、登録する Cisco Unified Communications Manager 内のセキュリティ設定と一致している必要があります。

会議ルータの詳細については、ご使用のルータに添付されている IOS ルータ マニュアルを参照してください。

Cisco Unified Communications Manager は、会議リソースをコールに動的に割り当てます。使用可能な会議リソースと有効なコーデックで、ルータごとに同時に使用可能なセキュアな会議の最大数が提供されます。送信ストリームと受信ストリームで、参加するエンドポイントごとにキーが個別に生成される（したがって、参加者が会議を離れるときにキーを再生成する必要がない）ので、DSP モジュールに対するセキュアな会議全体の容量は、設定可能な非セキュア容量の半分になります。

詳細については、『Cisco Unified Communications Manager システム ガイド』の「コンファレンス デバイスの概要」を参照してください。

セキュアな会議のアイコン

Cisco Unified IP Phone は、会議全体のセキュリティ レベルを示す会議セキュリティ アイコンを表示します。電話機のユーザ マニュアルで説明されているように、これらのアイコンは、安全な 2 通話者間のコールのステータス アイコンと同じです。

セキュアなアドホック会議およびミーティングの場合、会議のセキュリティ アイコンは、会議参加者の電話機のウィンドウで会議ソフトキーの横に表示されます。表示されるアイコンは、会議ブリッジおよびすべての参加者のセキュリティ レベルによって異なります。

- 会議ブリッジがセキュアですべての会議参加者が暗号化されている場合は、ロック アイコンが表示されます。
- 会議ブリッジがセキュアですべての会議参加者が認証されている場合は、シールド アイコンが表示されます。
- 会議ブリッジまたはいずれかの会議参加者が非セキュアである場合は、コール状態アイコン（アクティブ、保留中など）が表示されるか、旧式の電話機モデルではアイコンが表示されません。

暗号化された電話機がセキュアな会議ブリッジに接続する場合は、デバイスと会議ブリッジの間のメディア ストリームが暗号化されますが、会議のアイコンは、相手側のセキュリティ レベルに応じて、暗号化済み、認証済み、または非セキュアになります。非セキュア ステータスは、参加者のいずれかが非セキュアであるか、または確認できないことを意味します。

ユーザが [Barge (割込み)] を押すと、[Barge (割込み)] ソフトキーの横に表示されるアイコンが、割り込み会議のセキュリティ レベルを示します。割り込むデバイスと割り込まれるデバイスが暗号化をサポートしている場合、システムは両デバイス間のメディアを暗号化しますが、割り込み会議のステータスは、接続された参加者のセキュリティ レベルに応じて、非セキュア、認証済み、または暗号化済みになります。

セキュアな会議の保守

会議のステータスは、参加者が加わったときと退席したときに変わります。認証済みまたは非セキュアの参加者がコールに接続すると、暗号化された会議のセキュリティ レベルは認証済みまたは非セキュアに下がる場合があります。同様に、認証済みまたは非セキュアの参加者がコールを切断すると、ステータスは上がる場合があります。非セキュアの参加者が会議コールに接続すると、会議は非セキュアになります。

参加者が会議を結合した場合、結合した会議のセキュリティ ステータスが変った場合、保留された会議コールが別のデバイスで再開された場合、会議コールに割り込みが入った場合、転送された会議コールが別のデバイスで終了した場合も、会議のステータスが変わる可能性があります。



(注)

Advanced Ad Hoc Conference Enabled サービス パラメータは、会議、参加、直接転送、転送などの機能を使用してアドホック会議を互いにリンクさせることができるかどうかを決定します。

Cisco Unified Communications Manager には、セキュアな会議を保守するため、次のオプションが用意されています。

- [アドホック会議の会議リスト \(P.10-5\)](#)
- [最小セキュリティ レベルでのミーティング \(P.10-6\)](#)

アドホック会議の会議リスト

会議リストは、会議コール中に [ConfList (参加者)] ソフトキーが押された場合に、参加者の電話機に表示されます。会議リストは、会議のステータスを示し、また、暗号化されていない参加者を特定するために各参加者のセキュリティ ステータスを示します。

会議リストは、非セキュア、認証済み、暗号化済み、保留中のセキュリティ アイコンを表示します。会議の開始者は、会議リストを使用して、セキュリティ ステータスの低い参加者を退席させることができます。



(注)

Advanced Ad Hoc Conference Enabled サービス パラメータは、会議の開始者以外の会議参加者が会議参加者を退席させることができるかどうかを決定します。

参加者は、会議に参加すると、会議リストの一番上に追加されます。非セキュアの参加者を [ConfList (参加者)] ソフトキーと [RmLst (ドロップ)] ソフトキーでセキュアな会議から削除する方法は、ご使用の電話機のユーザ マニュアルを参照してください。

次の各項では、セキュアなアドホック会議とその他の機能との相互作用について説明します。

セキュアなアドホック会議と会議の結合

アドホック会議が別のアドホック会議に結合されると、結合された会議はメンバー「Conference」としてそれ自体のセキュリティ ステータスとともにリストに表示されます。Cisco Unified Communications Manager は、会議全体のセキュリティ ステータスを判別するため、結合された会議のセキュリティ レベルを組み込みます。

セキュアなアドホック会議と C 割り込み

ユーザが [cBarge (C 割込)] ソフトキーを押してアクティブな会議に参加すると、Cisco Unified Communications Manager はアドホック会議を作成し、割り込まれるデバイスのセキュリティ レベルと MRGL に従って会議ブリッジを割り当てます。C 割り込みメンバー名が会議リストに表示されます。

セキュアなアドホック会議と割り込み

セキュアなアドホック会議の参加者に割り込みがあった場合は、会議リストで割り込み元の横に割り込みコールのセキュリティ ステータスが表示されます。割り込み元と会議ブリッジの間のメディアが暗号化済みであっても、割り込み発信者の接続が認証済みであるために、割り込み元のセキュリティ アイコンが認証済みとなる場合もあります。

割り込み元がセキュアでアドホック会議が非セキュアである場合に、アドホック会議のステータスがあとからセキュアに変更されると、割り込み発信者のアイコンも更新されます。

セキュアなアドホック会議と参加

認証済みまたは暗号化済みの電話機ユーザは、Cisco Unified IP Phone (SCCP 電話機のみ) の [Join (参加)] ソフトキーを使用して、セキュアなアドホック会議を作成またはそれに参加することができます。ユーザが [Join (参加)] を押してセキュリティ ステータスの不明な参加者を既存の会議に追加すると、Cisco Unified Communications Manager は会議のステータスを不明にダウングレードします。[Join (参加)] を使用して新規メンバーを追加した参加者は、会議の開始者になり、新規メンバーやその他の参加者を会議リストから退席させることができます (Advanced Ad Hoc Conference Enabled 設定が有効になっている場合)。

セキュアなアドホック会議と保留 / 復帰

会議の開始者が参加者を追加にするため会議コールを保留にすると、追加された参加者がコールに応答するまで、会議のステータスは不明 (非セキュア) になります。新規参加者が応答すると、会議リストで会議のステータスが更新されます。

共有回線上の発信者が保留中の会議コールを別の電話機で復帰する場合は、発信者が [Resume (復帰)] を押したときに会議リストが更新されます。

最小セキュリティ レベルでのミートミー会議

管理者は、ミートミーのパターンまたは番号を非セキュア、認証済み、または暗号化済みとして設定する際に、会議の最小セキュリティ レベルを指定できます。参加者は、最小セキュリティ要件を満たしている必要があります。これを満たしていないと、システムは参加者をブロックして、コールを切断します。このアクションは、ミートミー会議コール転送、共有回線で復帰されたミートミー会議コール、結合したミートミー会議に適用されます。

ミートミー会議を開始する電話機は、最小セキュリティ レベルを満たしている必要があります。これを満たしていないと、システムは試行を拒否します。最小セキュリティ レベルが認証済みまたは暗号化済みを指定していて、セキュアな会議ブリッジが使用不可である場合、コールは失敗します。

会議ブリッジの最小レベルに非セキュアを指定すると、会議ブリッジはすべてのコールを受け入れ、会議のステータスは非セキュアになります。ミートミー会議の安全を確保する方法は、P.10-14 の「ミートミー会議の最小セキュリティ レベルの設定」を参照してください。

次の各項では、セキュアなミーティング会議とその他の機能との相互作用について説明します。

ミーティング会議とアドホック会議

ミーティング会議をアドホック会議に追加したりアドホック会議をミーティング会議に追加したりするには、アドホック会議がミーティング会議の最小セキュリティレベルを満たしている必要があります。これを満たしていないと、コールは切断されます。会議が追加されると、会議アイコンが変わります。

ミーティング会議と割り込み

ある発信者がミーティング会議の参加者に割り込んだ場合にその割り込み発信者が最小セキュリティ要件を満たしていないと、割り込まれたデバイスのセキュリティレベルがダウングレードし、割り込み発信者と割り込まれたコールの両方が切断されます。

ミーティング会議と保留 / 復帰

共有回線の電話機は、最小セキュリティレベルを満たしていないかぎり、ミーティング会議を復帰できません。電話機が最小セキュリティレベルを満たしていない場合にユーザが [Resume (復帰)] を押すと、共有回線上のすべての電話機がブロックされます。

Cisco Unified IP Phone サポート

次の Cisco Unified IP Phone モデルは、セキュアな会議とセキュアな会議アイコンをサポートしています。

- Cisco Unified IP Phone 7940 および 7960 (SCCP のみ、認証済みのセキュアな会議のみ)
- Cisco Unified IP Phone 7906、7911、および 7931 (SCCP のみ)
- Cisco Unified IP Phone 7941 および 7961
- Cisco Unified IP Phone 7970 および 7971



警告

セキュアな会議機能をフルに活用するため、暗号化機能をサポートするリリース 8.3 に Cisco Unified IP Phone をアップグレードすることをお勧めします。それより前のリリースを実行している暗号化済みの電話機では、これらの新機能が完全にはサポートされません。これらの電話機では、認証済みまたは非セキュアの参加者としてだけセキュアな会議に参加できます。

Cisco Unified Communications Manager の以前のリリースとともにリリース 8.3 を実行している Cisco Unified IP Phone では、会議コール中に会議のセキュリティステータスではなく接続のセキュリティステータスが表示されます。また、会議リストなどのセキュアな会議機能はサポートされません。

Cisco Unified IP Phone に当てはまる制限の詳細については、[P.10-9 の「制限」](#)を参照してください。

セキュアな会議コールとセキュリティアイコンの詳細については、ご使用の電話機のユーザガイドと、今回の Cisco Unified Communications Manager リリースをサポートする Cisco Unified Communications Manager 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。

CTI サポート

Cisco Unified Communications Manager は、ライセンス済み CTI デバイスでのセキュアな会議をサポートしています。詳細については、今回のリリースの『*Cisco Unified Communications Manager JTAPI Developers Guide*』および『*Cisco Unified Communications Manager TAPI Developers Guide*』を参照してください。

トランクおよびゲートウェイでのセキュアな会議

Cisco Unified Communications Manager は、クラスタ間トランク (ICT)、H.323 トランク / ゲートウェイ、および MGCP ゲートウェイを介してのセキュアな会議をサポートしています。ただし、リリース 8.2 以前を実行している暗号化済みの電話機は、ICT および H.323 コールの場合は RTP に戻り、メディアは暗号化されません。

会議に SIP トランクが含まれる場合、セキュアな会議のステータスは非セキュアになります。また、SIP トランク シグナリングは、クラスタ外の参加者へのセキュアな会議通知をサポートしていません。



(注)

Cisco Unified Communications Manager Business Edition システムでは、Intercluster Trunk (ICT; クラスタ間トランク) を介してのセキュアな会議はサポートされていません。

CDR データ

CDR データは、会議自体のセキュリティ ステータスに加えて、電話機エンドポイントから会議ブリッジへの各コール レッグのセキュリティ ステータスも示します。CDR データベース内では、2 つの値が 2 つの異なるフィールドを使用します。

最小セキュリティ レベル要件を満たしていない参加試行をミートミー会議が拒否した場合、CDR データは終了原因コード 58(ベアラ機能を現在使用できない)を示します。詳細については、『*Cisco Unified Communications Manager CDR Analysis and Reporting アドミニストレーション ガイド*』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 \(P.10-9\)](#)
- [制限 \(P.10-9\)](#)

相互作用

この項では、Cisco Unified Communications Manager とセキュアな会議機能との相互作用について説明します。

- 会議の安全を保つため、Suppress MOH to Conference Bridge サービス パラメータが False に設定されている場合でも、セキュアなアドホック会議の参加者がコールを保留にしたりコールをパークしたとき、システムは MOH を再生しません。セキュアな会議のステータスは変わりません。
- クラスタ間環境では、クラスタ外の会議参加者がセキュアなアドホック会議で保留を押すと、デバイスへのメディア ストリームが停止し、MOH が再生され、メディアのステータスが不明になります。クラスタ外の参加者が MOH 付きの保留コールを再開すると、会議のステータスは上がります。
- リモート ユーザが保留 / 復帰などの電話機能を起動すると、メディアのステータスが不明に変わり、クラスタ間トランク (ICT) でのセキュアなミートミー コールは消去されます。
- Cisco Unified Communications Manager Multilevel Precedence and Preemption 用のアナンシエータのトーンやアナウンスメントがセキュアなアドホック会議中に参加者の電話機で再生されると、会議のステータスは非セキュアに変わります。
- 発信者がセキュアな SCCP 電話機コールに割り込んだ場合、システムは発信先デバイスで内部トーン再生メカニズムを使用し、会議のステータスはセキュアに保たれます。
- 発信者がセキュアな SIP 電話機コールに割り込んだ場合、システムは保留トーンを再生し、その間、会議のステータスは非セキュアになります。
- 会議がセキュアで RSVP が有効である場合、会議はセキュアに保たれます。
- PSTN を含む会議コールでは、コールの IP ドメイン部分のセキュリティ ステータスだけがセキュリティ会議アイコンで示されます。
- Maximum Call Duration Timer サービス パラメータは、最大会議期間も制御します。
- 会議ブリッジは、パケット キャプチャをサポートします。メディア ストリームが暗号化済みであっても、パケット キャプチャ セッション中、電話機は会議について非セキュア ステータスを示します。
- ご使用のシステムに対して設定されているメディア セキュリティ ポリシーがセキュアな会議の動作を変える場合があります。たとえば、エンドポイントは、メディア セキュリティをサポートしていないエンドポイントとの会議コールに参加している場合でも、システムのメディア セキュリティ ポリシーに従ってメディア セキュリティを使用します。

制限

この項では、セキュアな会議機能での Cisco Unified Communications Manager の制限について説明します。

- リリース 8.2 以前を実行している暗号化済みの Cisco Unified IP Phone は、認証済みまたは非セキュアの参加者としてしかセキュアな会議に参加できません。
- Cisco Unified Communications Manager の以前のリリースとともにリリース 8.3 を実行している Cisco Unified IP Phone では、会議コール中に会議のセキュリティ ステータスではなく接続のセキュリティ ステータスが表示されます。また、会議リストなどのセキュアな会議機能はサポートされません。

- Cisco Unified IP Phone 7905 および 7911 は会議リストをサポートしていません。
- 帯域幅要件のため、Cisco Unified IP Phone 7940 および 7960 は、アクティブな暗号化済みコールへの暗号化済みデバイスからの割り込みをサポートしません。割り込みの試行は失敗します。
- Cisco Unified IP Phone 7931 は会議の結合をサポートしていません。
- SIP トランクを介して発信している電話機は、そのデバイスのセキュリティ ステータスに関わらず、非セキュアの電話機として扱われます。
- セキュアな電話機が SIP トランクを介してセキュアなミーティング会議に参加しようとする、コールは切断されます。SIP トランクは SIP 電話機への「認証されていないデバイス」のメッセージの提供をサポートしていないので、電話機はこのメッセージで更新されません。また、Cisco Unified 7960 SIP 電話機も「認証されていないデバイス」のメッセージをサポートしていません。
- クラスタ間では、クラスタ外の参加者に対して会議リストは表示されませんが、クラスタ間の接続でサポートされていれば、接続のセキュリティ ステータスは [Conference (会議)] ソフトキーの横に表示されます。たとえば、H.323 ICT 接続の場合、認証アイコンは表示されませんが (システムは認証済み接続を非セキュアとして扱います)、暗号化済み接続に対する暗号化アイコンは表示されます。

クラスタ外の参加者は、クラスタ境界を越えて別のクラスタへ接続する独自の会議を作成できます。システムは、接続された会議を基本的な 2 通話者間コールとして扱います。

会議リソースのセキュリティを確保するための設定のヒント



セキュアな会議ブリッジのリソースを設定する前に、次の情報を考慮に入れてください。

- セキュアな会議メッセージ用のカスタム テキストを電話機で表示する場合は、ローカリゼーションを使用します。詳細については、Cisco Unified Communications Manager Locale Installer のマニュアルを参照してください。
- 会議またはビルトイン ブリッジは、会議コールのセキュリティを確保するため、暗号化をサポートしている必要があります。
- セキュアな会議ブリッジ登録を有効にするには、クラスタのセキュリティ モードを混合モードに設定します。
- セキュアな会議ブリッジを確立するため、会議を開始する電話機が認証済みまたは暗号化済みであることを確認してください。
- 共有回線での会議の整合性を保つため、回線を共有するデバイスを別々のセキュリティ モードで設定することはしないでください。たとえば、暗号化済みの電話機が認証済みまたは非セキュアの電話機と回線を共有するように設定することはしないでください。
- クラスタ間で会議のセキュリティ ステータスを共有する場合は、SIP トランクを ICT として使用しないでください。
- クラスタのセキュリティ モードを混合モードに設定する場合は、DSP ファーム用に設定されたセキュリティ モード（非セキュアまたは暗号化済み）が Cisco Unified Communications Manager の管理ページの会議ブリッジのセキュリティ モードと一致している必要があります。一致していないと、会議ブリッジは登録されません。両方のセキュリティ モードが暗号化済みと指定されていれば、会議ブリッジは暗号化済みとして登録されます。両方のセキュリティ モードが非セキュアと指定されていれば、会議ブリッジは非セキュアとして登録されます。
- クラスタのセキュリティ モードを混合モードに設定し、会議ブリッジに適用したセキュリティ プロファイルが暗号化済みで会議ブリッジのセキュリティ レベルが非セキュアである場合、Cisco Unified Communications Manager は会議ブリッジの登録を拒否します。
- クラスタのセキュリティ モードを非セキュア モードに設定する場合は、会議ブリッジが登録されるよう、DSP ファームのセキュリティ モードを非セキュアに設定してください。Cisco Unified Communications Manager の管理ページでの設定が暗号化済みであっても、会議ブリッジは非セキュアとして登録されます。
- 登録時に、会議ブリッジは認証に合格する必要があります。認証に合格するには、DSP ファームに Cisco Unified Communications Manager 証明書が含まれ、Cisco Unified Communications Manager に DSP ファーム システムの証明書と DSP 接続の証明書が含まれている必要があります。会議ブリッジが確実に認証に合格するためには、X.509 証明書名に会議ブリッジ名が含まれている必要があります。
- 会議ブリッジの証明書が失効したか、または何らかの理由で変更された場合は、Cisco Unified Communications オペレーティング システムの管理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、会議ブリッジは Cisco Unified Communications Manager に登録できないため機能しません。
- セキュアな会議ブリッジは、ポート 2443 で TLS 接続を介して Cisco Unified Communications Manager に登録されます。非セキュアの会議ブリッジは、ポート 2000 で TCP 接続を介して Cisco Unified Communications Manager に登録されます。
- 会議ブリッジのデバイスのセキュリティ モードを変更するには、Cisco Unified Communications Manager デバイスをリセットして Cisco CallManager サービスを再起動する必要があります。

セキュアな会議ブリッジの設定用チェックリスト

ネットワークにセキュアな会議を追加するときに、表 10-1 を参照してください。

表 10-1 セキュアな会議ブリッジの設定用チェックリスト

設定手順	関連手順および関連項目
ステップ 1 Cisco CTL クライアントを混合モードでインストールし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)
ステップ 2 信頼ストアへの Cisco Unified Communications Manager 証明書の追加も含め、Cisco Unified Communications Manager 接続用の DSP ファーム セキュリティを設定したことを確認します。DSP ファームのセキュリティ レベルを暗号化済みを設定します。	ご使用の会議ブリッジのマニュアルを参照してください。
 ヒント DSP ファームは、ポート 2443 で Cisco Unified Communications Manager への TLS ポート接続を確立します。	
ステップ 3 DSP ファーム証明書が Cisco Unified Communications Manager 信頼ストア内にあることを確認してください。 証明書を追加するには、Cisco Unified Communications オペレーティングシステムの証明書管理機能を使用して DSP 証明書を Cisco Unified Communications Manager 内の信頼ストアにコピーします。 証明書のコピーが終わったら、サーバで Cisco CallManager サービスを再起動します。	<ul style="list-style-type: none"> • Cisco Unified Communications Manager アドミニストレーションガイド • Cisco Unified Communications Manager Serviceability アドミニストレーションガイド
ステップ 4 Cisco Unified Communications Manager の管理ページで、Cisco IOS Enhanced Conference Bridge を会議ブリッジ タイプとして設定し、暗号化済み会議ブリッジをデバイスのセキュリティ モードとして選択します。	<ul style="list-style-type: none"> • 会議リソースのセキュリティを確保するための設定のヒント (P.10-11) • Cisco Unified Communications Manager の管理ページでのセキュアな会議ブリッジの設定 (P.10-13)
ステップ 5 ミートミー会議の最小セキュリティ レベルを設定します。	ミートミー会議の最小セキュリティ レベルの設定 (P.10-14)
ステップ 6 (オプション) セキュアな会議ブリッジのパケット キャプチャを設定します。	セキュアな会議ブリッジのパケット キャプチャの設定 (P.10-14)
 ヒント パケット キャプチャ モードをバッチ モードに設定し、キャプチャ層を SRTP に設定します。	Cisco Unified Communications Manager トラブルシューティングガイド

Cisco Unified Communications Manager の管理ページでのセキュアな会議ブリッジの設定

Cisco Unified Communications Manager の管理ページでセキュアな会議ブリッジを設定するには、次の手順を実行します。会議ブリッジの暗号化を設定した後、Cisco Unified Communications Manager デバイスをリセットして、Cisco CallManager サービスを再起動する必要があります。

始める前に

デバイス間の接続を安全にするため、Cisco Unified Communications Manager と DSP ファームに証明書をインストールしたことを確認してください。

手順

ステップ 1 [メディアリソース]>[会議ブリッジ]を選択します。

ステップ 2 [会議ブリッジの検索と一覧表示 (Find and List Conference Bridges)]ウィンドウで、Cisco IOS Enhanced Conference Bridge がインストールされていることを確認し、[ステップ 4](#)に進みます。

データベース内にデバイスが存在しない場合は、[\[新規追加\]](#)をクリックし、[ステップ 3](#)に進みます。

ステップ 3 [会議ブリッジの設定 (Conference Bridge Configuration)]ウィンドウで、[会議ブリッジタイプ (Conference Bridge Type)]ドロップダウン リスト ボックスから **[Cisco IOS Enhanced Conference Bridge]**を選択します。『Cisco Unified Communications Manager アドミニストレーションガイド』の説明に従って、会議ブリッジ名、説明、デバイス プール、共通デバイス設定、およびロケーションを設定します。

ステップ 4 [デバイスセキュリティモード (Device Security Mode)]フィールドで、**[Encrypted Conference Bridge]**を選択します。

ステップ 5 [保存]をクリックします。

ステップ 6 [リセット]をクリックします。

追加の手順

その他の会議ブリッジ設定タスクを実行するため、[\[関連リンク\]](#)ドロップダウン リスト ボックスからオプションを選択して [\[移動\]](#)をクリックし、[\[ミーティング番号の設定 \(Meet-Me Number Configuration\)\]](#)ウィンドウまたは [\[サービスパラメータ設定 \(Service Parameter Configuration\)\]](#)ウィンドウに移動します。

追加情報

詳細については、[P.10-15](#)の「[関連項目](#)」を参照してください。

ミートミー会議の最小セキュリティ レベルの設定

ミートミー会議の最小セキュリティ レベルを設定するには、次の手順を実行します。

手順

ステップ 1 [コールルーティング] > [ミートミー番号 / パターン] を選択します。

ステップ 2 [ミートミー番号の検索と一覧表示 (Find and List Meet-Me Numbers)] ウィンドウで、ミートミー番号 / パターンが設定されていることを確認し、[ステップ 4](#) に進みます。

ミートミー番号 / パターンが設定されていない場合は、[新規追加] をクリックし、[ステップ 3](#) に進みます。

ステップ 3 [ミートミー番号の設定 (Meet-Me Number Configuration)] ウィンドウで、[電話番号またはパターン (Directory Number or Pattern)] フィールドにミートミー番号または範囲を入力します。『Cisco Unified Communications Manager アドミニストレーション ガイド』の説明に従って、説明とパーティションの値を設定します。

ステップ 4 [最小セキュリティレベル (Minimum Security Level)] フィールドで、[非セキュア] [認証のみ] または [暗号化] を選択します。

ステップ 5 [保存] をクリックします。

追加の手順

セキュアな会議ブリッジをまだインストールしていない場合は、[P.10-13](#) の「[Cisco Unified Communications Manager の管理ページでのセキュアな会議ブリッジの設定](#)」の説明にしたがって、セキュアな会議ブリッジをインストールして設定します。

追加情報

詳細については、[P.10-15](#) の「[関連項目](#)」を参照してください。

セキュアな会議ブリッジの packets キャプチャの設定

セキュアな会議ブリッジの packets キャプチャを設定するには、[サービスパラメータ設定 (Service Parameter Configuration)] ウィンドウで packets キャプチャを有効にしてから、デバイス設定ウィンドウで電話機、ゲートウェイ、またはトランクに対して packets キャプチャ モードをパッチ モードに設定し、キャプチャ層を SRTP に設定します。詳細については、『Cisco Unified Communications Manager トラブルシューティングガイド』を参照してください。

メディア ストリームが暗号化済みであっても、packets キャプチャ セッション中、電話機は会議に対して非セキュア ステータスを示します。

その他の情報

関連項目

- システム要件 (P.1-5)
- 相互作用および制限 (P.1-8)
- 証明書 (P.1-15)
- 設定用チェックリストの概要 (P.1-26)
- セキュアな会議の概要 (P.10-2)
- 会議ブリッジの要件
- セキュアな会議のアイコン (P.10-4)
- セキュアな会議の保守 (P.10-5)
- Cisco Unified IP Phone サポート (P.10-7)
- CTI サポート (P.10-8)
- トランクおよびゲートウェイでのセキュアな会議 (P.10-8)
- 相互作用および制限 (P.10-9)
- 会議リソースのセキュリティを確保するための設定のヒント (P.10-11)
- セキュアな会議ブリッジの設定用チェックリスト (P.10-12)
- Cisco Unified Communications Manager の管理ページでのセキュアな会議ブリッジの設定 (P.10-13)
- ミートミー会議の最小セキュリティ レベルの設定 (P.10-14)
- セキュアな会議ブリッジのパケット キャプチャの設定 (P.10-14)

シスコの関連マニュアル

- 『Cisco Unified Communications Manager システム ガイド』の「会議ブリッジ」
- 『Cisco Unified Communications Manager システム ガイド』の「トランスコーディング、会議、および MTP 用の Cisco DSP リソース」
- 『Cisco Unified Communications Manager アドミニストレーション ガイド』の「会議ブリッジの設定」
- 『Cisco Unified Communications Manager アドミニストレーション ガイド』の「ミートミー番号 / パターンの設定」
- Cisco Unified Communications Operating System アドミニストレーション ガイド
- Cisco Unified Communications Manager トラブルシューティング ガイド
- Cisco Unified Communications Manager CDR Analysis and Reporting 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 Communications Manager
- 今回のリリースの Cisco Unified Communications Manager およびご使用の Cisco Unified IP Phone の Cisco IP Phone ユーザ ガイドおよびリリース ノート



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 \(P.11-1\)](#)
- [ボイスメール セキュリティの設定のヒント \(P.11-2\)](#)
- [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 \(P.11-3\)](#)
- [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 \(P.11-4\)](#)
- [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 \(P.11-5\)](#)
- [その他の情報 \(P.11-6\)](#)

ボイスメールのセキュリティの概要

Cisco Unified Communications Manager ボイスメール ポートおよび Cisco Unity SCCP デバイスや Cisco Unity Connection 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。

- Cisco Unity または Cisco Unity Connection 1.2 以前で、デバイス セキュリティ モードが認証済みまたは暗号化済みになっている場合、Cisco Unity-Unified CM TSP は、TLS を介して Cisco Unified Communications Manager に接続します。デバイス セキュリティ モードが非セキュアになっている場合、Cisco Unity-Unified CM TSP は、SCCP ポートを介して Cisco Unified Communications Manager に接続します。
- Cisco Unity Connection 2.0 以降では、TLS ポートを介して Cisco Unified Communications Manager に接続します。デバイス セキュリティ モードが非セキュアになっている場合、Cisco Unity Connection は、SCCP ポートを介して Cisco Unified Communications Manager に接続します。



(注) このマニュアルでは、「サーバ」という用語は Cisco Unified Communications Manager サーバを意味します。「ボイスメール サーバ」という用語は Cisco Unity サーバまたは Cisco Unity Connection サーバを意味します。

ボイスメール セキュリティの設定のヒント

セキュリティを設定する前に、次の点を考慮してください。

- Cisco Unity の場合、Cisco Unity Telephony Integration Manager (UTIM) を使用してセキュリティ タスクを実行する必要があります。Cisco Unity Connection の場合、Cisco Unity Connection の管理を使用してセキュリティ タスクを実行する必要があります。これらのタスクの実行方法については、Cisco Unity または Cisco Unity Connection 用の、該当する Cisco Unified Communications Manager インテグレーション ガイドを参照してください。
- この章で説明する手順に加えて、Cisco Unified Communications オペレーティング システム の証明書管理機能を使用して、Cisco Unity 証明書を信頼ストアに保存する必要があります。この作業の実行の詳細については、『Cisco Unified Communications Operating System 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、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、ボイスメールは Cisco Unified Communications Manager に登録できないため機能しません。
- ボイスメール サーバのポートを設定する場合は、デバイス セキュリティ モードを選択する必要があります。
- Cisco Unity Telephony Integration Manager (UTIM) または Cisco Unity Connection の管理で指定する設定は、Cisco Unified Communications Manager の管理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 Unity Connection の管理の [ボイスメールポートの設定 (Voice Mail Port Configuration)] ウィンドウ (またはボイスメール ポート ウィザード) で、ボイスメール ポートにデバイス セキュリティ モードを適用します。



ヒント デバイス セキュリティ モードの設定が一致しない場合は、ボイスメール サーバのポートが Cisco Unified Communications Manager に登録できず、ボイスメール サーバはそれらのポートでコールを受け入れることができません。

- ポートのセキュリティ プロファイルを変更するには、Cisco Unified Communications Manager デバイスをリセットしてボイスメール サーバソフトウェアを再起動する必要があります。Cisco Unified Communications Manager の管理ページで、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、ボイスメール サーバの設定を変更する必要があります。
- ボイスメール ポート ウィザードで既存のボイスメール サーバのデバイス セキュリティ モードを変更することはできません。既存のボイスメール サーバにポートを追加すると、現在プロファイルに設定されているデバイス セキュリティ モードが自動的に新規ポートに適用されます。

ボイスメールポートのセキュリティ設定用チェックリスト

ボイスメールポートのセキュリティを設定する場合は、表 11-1 を参照してください。

表 11-1 ボイスメールポートのセキュリティ設定用チェックリスト

設定手順	関連手順および関連項目
ステップ 1 Cisco CTL クライアントを混合モードでインストールし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)
ステップ 2 電話機に認証または暗号化を設定したことを確認します。	電話機のセキュリティの概要 (P.4-1) 電話機セキュリティ プロファイルの設定 (P.5-1)
ステップ 3 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 Unified Communications Manager サーバの信頼ストアに Cisco Unity 証明書をコピーします。次に、Cisco CallManager サービスを再起動します。	<ul style="list-style-type: none"> ボイスメールセキュリティの設定のヒント (P.11-2) Cisco Unified Communications Operating System アドミニストレーションガイド Cisco Unified Communications Manager Serviceability アドミニストレーションガイド
ステップ 4 Cisco Unified Communications Manager 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"> 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.11-4) 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.11-5)
ステップ 5 Cisco Unity または Cisco Unity Connection のボイスメールポートのセキュリティ関連設定タスクを実行します。たとえば、Cisco Unity が Cisco TFTP サーバを指すように設定します。	Cisco Unity または Cisco Unity Connection 用の Cisco Unified Communications Manager インテグレーションガイド
ステップ 6 Cisco Unified Communications Manager の管理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"> Cisco Unity または Cisco Unity Connection 用の Cisco Unified Communications Manager インテグレーションガイド 単一ボイスメールポートへのセキュリティ プロファイルの適用 (P.11-4)

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 \(P.11-1\)](#)
- [ボイスメール セキュリティの設定のヒント \(P.11-2\)](#)
- [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 \(P.11-3\)](#)

手順

-
- ステップ 1** 『Cisco Unified Communications Manager アドミニストレーション ガイド』の説明に従って、ボイスメール ポートを検索します。
- ステップ 2** ポートの設定ウィンドウが表示されたら、[**デバイスセキュリティモード**] 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.11-6](#) 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.11-4 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 \(P.11-1\)](#)
- [ボイスメールセキュリティの設定のヒント \(P.11-2\)](#)
- [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 \(P.11-3\)](#)

ボイスメール ポート ウィザードで新規ボイスメール サーバにデバイス セキュリティ モードの設定を適用するには、次の手順を実行します。

手順

-
- ステップ 1** Cisco Unified Communications Manager の管理ページで、[ボイスメール] > [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 Communications Manager アドミニストレーション ガイド』の説明に従って、その他のデバイス設定を実行します。[次へ] をクリックします。
 - ステップ 6** 『Cisco Unified Communications Manager アドミニストレーション ガイド』の説明に従って、設定プロセスを続行します。要約ウィンドウが表示されたら、[終了] をクリックします。
-

追加情報

詳細については、P.11-6 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.1-5)
- 相互作用および制限 (P.1-8)
- 証明書 (P.1-15)
- 設定用チェックリストの概要 (P.1-26)
- ボイスメールのセキュリティの概要 (P.11-1)
- ボイスメール セキュリティの設定のヒント (P.11-2)
- 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.11-4)
- 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.11-5)

シスコの関連マニュアル

- 今回の Cisco Unified Communications Manager リリースに対応した Cisco Unity または Cisco Unity Connection 用の *Cisco Unified Communications Manager インテグレーション ガイド*
- *Cisco Unified Communications Operating System アドミニストレーション ガイド*



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 Communications Manager 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 Communications Manager 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については説明していません。同じく、このマニュアルでは、CTI 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 \(P.12-2\)](#)
- [CTI、JTAPI、および TAPI アプリケーションの暗号化について \(P.12-4\)](#)
- [CTI、JTAPI、および TAPI アプリケーションに対する CAPF の概要 \(P.12-5\)](#)
- [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 \(P.12-6\)](#)
- [CTI、JTAPI、および TAPI のセキュリティ設定用チェックリスト \(P.12-7\)](#)
- [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 \(P.12-9\)](#)
- [Certificate Authority Proxy Function サービスのアクティブ化 \(P.12-10\)](#)
- [CAPF サービスパラメータの更新 \(P.12-11\)](#)
- [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 \(P.12-12\)](#)
- [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 \(P.12-13\)](#)
- [アプリケーションユーザ CAPF プロファイルおよびエンドユーザ CAPF プロファイルの CAPF 設定ウィンドウ \(P.12-14\)](#)
- [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 \(P.12-16\)](#)
- [JTAPI/TAPI セキュリティ関連サービスパラメータ \(P.12-17\)](#)
- [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 \(P.12-18\)](#)
- [その他の情報 \(P.12-18\)](#)

CTI、JTAPI、および TAPI アプリケーションの認証について

Cisco Unified Communications Manager を使用して、CTIManager と CTI/JTAPI/TAPI アプリケーションとの間のシグナリング接続およびメディア ストリームを保護できます。



ヒント

次の情報では、Cisco JTAPI/TSP プラグインのインストール中にセキュリティ設定を定義したことを前提としています。また、Cisco CTL クライアントでクラスタ セキュリティ モードが混合モードに設定されていることを前提としています。この章で説明する作業を実行するときに、これらの設定が定義されていない場合、CTIManager とアプリケーションは、非セキュア ポートであるポート 2748 で接続されます。

CTIManager およびアプリケーションは、相互に認証された TLS ハンドシェイク（証明書交換）によって他方の ID を確認します。TLS 接続が確立されると、CTIManager およびアプリケーションは、TLS ポート、ポート 2749 を介して QBE メッセージを交換します。

アプリケーションとの認証を行うために、CTIManager は、Cisco Unified Communications Manager 証明書（インストール時に Cisco Unified Communications Manager サーバに自動的にインストールされる自己署名証明書、またはプラットフォームにアップロードされたサードパーティの CA 署名付き証明書）を使用します。Cisco CTL クライアントをインストールして CTL ファイルを生成した後、この証明書は CTL ファイルに自動的に追加されます。アプリケーションは、CTIManager への接続を試行する前に、TFTP サーバから CTL ファイルをダウンロードします。

JTAPI/TSP クライアントは、初めて CTL ファイルを TFTP サーバからダウンロードするときに CTL ファイルを信頼します。JTAPI/TSP クライアントは CTL ファイルを検証しないため、ダウンロードはセキュアな環境で実行することを強く推奨します。後続の CTL ファイルのダウンロードは、JTAPI/TSP クライアントで確認されます。たとえば、CTL ファイルの更新後、JTAPI/TSP クライアントは、CTL ファイルのセキュリティ トークンを使用して、ダウンロードした新しい CTL ファイルのデジタル署名を認証します。ファイルの内容には、Cisco Unified Communications Manager 証明書と CAPF サーバ証明書が含まれます。

CTL ファイルが侵害されていると判断された場合、JTAPI/TSP クライアントはダウンロードした CTL ファイルを置き換えません。クライアントはエラーをログに記録し、既存の CTL ファイルにある古い証明書を使用して、TLS 接続の確立を試行します。CTL ファイルが変更または侵害されている場合、正常に接続できない可能性があります。CTL ファイルのダウンロードに失敗し、複数の TFTP サーバが存在する場合、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、Certificate Authority Proxy Function (CAPF) が発行する証明書を使用します。アプリケーションと CTIManager とのすべての接続で TLS を使用するには、アプリケーション PC で実行されるインスタンスごとに一意の証明書が必要です。1 つの証明書ですべてのインスタンスがカバーされるわけではありません。Cisco IP Manager Assistant サービスを実行しているノードに証明書がインストールされるようにするには、表 12-2 の説明に従い、Cisco Unified Communications Manager 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のインスタンス ID を設定します。

**ヒント**

アプリケーションをある PC からアンインストールして別の PC にインストールする場合、新しい PC の各インスタンスに対して新しい証明書をインストールする必要があります。

また、アプリケーションの TLS を有効にするには、Cisco Unified Communications Manager の管理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 Communications Manager Assistant、Cisco QRT、および Cisco Web Dialer は暗号化をサポートしていません。CTIManager サービスに接続する CTI クライアントは、クライアントが音声パケットを送信する場合、暗号化をサポート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 ストリームを安全にするには、Cisco Unified Communications Manager 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 グループに追加します。これらのユーザが Standard CTI Secure Connection ユーザ グループにも存在する場合や、Cisco Unified Communications Manager セキュリティ モードが混合モードと等しい場合、CTIManager はアプリケーションとの TLS 接続を確立し、メディア イベント内でアプリケーションに鍵関連情報を提供します。

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。アプリケーションは、SRTP 鍵関連情報を記録または格納すべきではありません。

何らかの理由でアプリケーションが非セキュア ポートであるポート 2748 に接続した場合、CTIManager は鍵関連情報を送信しません。制限を設定しなかったために CTI/JTAPI/TAPI がデバイスまたはディレクトリ メンバーを監視または制御できない場合、CTIManager は鍵関連情報を送信しません。



ヒント

アプリケーションで SRTP セッション鍵を受信するには、アプリケーション ユーザまたはエンド ユーザが Standard CTI Enabled、Standard CTI Secure Connection、および Standard CTI Allow Reception of SRTP Key Material の 3 つのグループに存在する必要があります。

Cisco Unified Communications Manager は、CTI ポートおよびルート ポイントで送受信されるセキュア コールを円滑にしますが、アプリケーションがメディア パラメータを処理するため、アプリケーションがセキュア コールをサポートするように設定する必要があります。

CTI ポートやルート ポイントは、ダイナミック登録またはスタティック登録で登録されます。ポートやルート ポイントがダイナミック登録を使用する場合、メディア パラメータはコールごとに指定されます。スタティック登録の場合、メディア パラメータは登録時に指定され、コールごとに変更することはできません。CTI ポートやルート ポイントが TLS 接続を介して CTIManager に登録される場合、デバイスは安全に登録されます。このとき、アプリケーションが有効な暗号化アルゴリズムを使用し、相手がセキュアであれば、メディアは SRTP で暗号化されます。

CTI アプリケーションが、すでに確立されているコールの監視を開始するとき、アプリケーションは RTP イベントを受信しません。確立されたコールに対して、CTI アプリケーションは、コールのメディアがセキュアか非セキュアかを定義する DeviceSnapshot イベントを提供します。このイベントには、鍵関連情報は含まれません。

CTI、JTAPI、および TAPI アプリケーションに対する CAPF の概要

Certificate Authority Proxy Function (CAPF) は Cisco Unified Communications Manager と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 Communications Manager がサポートする CAPF プロファイルの違いについて説明します。

- アプリケーション ユーザ CAPF プロファイル：このプロファイルを使用すると、ローカルで有効な証明書を発行して、アプリケーション ユーザの安全を確保することができます。これにより、CTIManager サービスとアプリケーションの間で TLS 接続が開かれます。
1 つのアプリケーション ユーザ CAPF プロファイルが、サーバのサービスまたはアプリケーションの 1 つのインスタンスに対応します。同じサーバで複数の Web サービスまたはアプリケーションをアクティブにする場合は、サーバのサービスごとに 1 つずつ、合計 2 つのアプリケーション ユーザ CAPF プロファイルを設定する必要があります。
- エンドユーザ CAPF プロファイル：このプロファイルを使用すると、CTI クライアントにローカルで有効な証明書を発行することができます。これにより、CTI クライアントが TLS 接続を介して CTIManager サービスと通信できるようになります。



ヒント

JTAPI クライアントは LSC を Java Key Store 形式で、JTAPI の初期設定ウィンドウで設定したパスに格納します。TSP クライアントは LSC を暗号化形式で、デフォルト ディレクトリまたは設定したパスに格納します。

次の情報は、通信または電源の障害が発生した場合に適用されます。

- 証明書をインストールしているときに通信障害が発生すると、JTAPI クライアントは 30 秒間隔であと 3 回、証明書を取得しようとします。この値は設定することができません。
TSP クライアントの場合は、再試行回数と再試行タイマーを設定できます。これらの値は、TSP クライアントが一定の時間内に証明書の取得を試行する回数を指定することで設定します。どちらの値も、デフォルトは 0 です。最大 3 回の再試行回数を設定でき、1 (1 回だけ再試行)、2、または 3 を指定します。それぞれについて、再試行の時間を 30 秒以下で設定できます。
- JTAPI/TSP クライアントが CAPF とのセッションを試行している間に電源障害が発生した場合、クライアントは電源が復帰した後で、証明書のダウンロードを試行します。

CTI、JTAPI、および TAPI アプリケーションに対する CAPF システムの相互作用および要件





CAPF には、次の要件があります。

- アプリケーション ユーザ CAPF プロファイルおよびエンド ユーザ CAPF プロファイルを設定する前に、Cisco CTL クライアントをインストールして設定するために必要なすべての作業を実行したことを確認します。[エンタープライズパラメータ設定 (Enterprise Parameters Configuration)] ウィンドウの Cluster Security Mode が 1 (混合モード) であることを確認してください。
- 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、サーバ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 12-1 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 12-1 CTI/JTAPI/TAPI のセキュリティ設定用チェックリスト

設定手順		関連手順および関連項目
ステップ 1	<p>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> ヒント アプリケーション ユーザは、Standard CTI Enabled グループに割り当てられている必要があります。</p>	<ul style="list-style-type: none"> 『Cisco Unified Communications Manager システム ガイド』の「コンピュータ テレフォニー統合」 Cisco JTAPI インストールガイド for Cisco Unified Communications Manager Cisco TAPI インストールガイド for Cisco Unified Communications Manager Cisco Unified Communications Manager アドミニストレーションガイド
ステップ 2	<p>次の Cisco Unified Communications Manager セキュリティ機能がインストールされていることを確認します（インストールされていない場合は、これらの機能をインストールして設定します）。</p> <ul style="list-style-type: none"> CTL ファイルが作成されるように、5.0 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。 CTL プロバイダー サービスがインストールされ、サービスがアクティブであることを確認します。 CAPF 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。 <p> ヒント CAPF サービスは、CTL ファイルに CAPF 証明書を組み込むために、Cisco CTL クライアントで実行されている必要があります。電話機で CAPF を使用したときにこれらのパラメータを更新した場合は、ここでパラメータを更新する必要はありません。</p> <ul style="list-style-type: none"> Cisco Unified Communications Manager 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。 <p> ヒント 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"> Cisco CTL クライアントの設定 (P.3-1) CAPF サービス パラメータの更新 (P.12-11) Cisco Unified Communications Manager アドミニストレーションガイド
ステップ 3	<p>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> ヒント CTI アプリケーションは、アプリケーション ユーザまたはエンド ユーザに割り当てることができませんが、両方に割り当てることができません。</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.12-9)</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 12-1 CTI/JTAPI/TAPI のセキュリティ設定用チェックリスト (続き)

設定手順		関連手順および関連項目
ステップ 4	<p>SRTP を使用する場合は、Standard CTI Allow Reception of SRTP Key Material ユーザ グループにアプリケーション ユーザまたはエンド ユーザを追加します。</p> <p>ユーザはすでに Standard CTI Enabled および Standard CTI Secure Connection ユーザ グループに存在している必要があります。これらの 3 つのグループに存在しないアプリケーション ユーザまたはエンド ユーザは、SRTP セッション鍵を受信できません。</p> <p>Cisco Unified Communications Manager Assistant、Cisco QRT、および Cisco Web Dialer は暗号化をサポートしていません。CTIManager サービスに接続する CTI クライアントは、クライアントが音声パケットを送信する場合、暗号化をサポート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.12-9)</p> <p>『Cisco Unified Communications Manager アドミニストレーション ガイド』の「権限の設定」</p>
ステップ 5	<p>Cisco Unified Communications Manager の管理ページでアプリケーション ユーザ CAPF プロファイルまたはエンド ユーザ CAPF プロファイルを設定します。</p>	<ul style="list-style-type: none"> • CTI、JTAPI、および TAPI アプリケーションに対する CAPF の概要 (P.12-5) • 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.12-13) • アプリケーションユーザ CAPF プロファイルおよびエンドユーザ CAPF プロファイルの CAPF 設定ウィンドウ (P.12-14)
ステップ 6	<p>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.12-17)</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 Communications Manager 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。TLS は、SRTP 接続に必要です。ユーザがこれらのグループに存在する場合、ユーザを Standard CTI Allow Reception of SRTP Key Material ユーザグループに追加できます。アプリケーションで SRTP セッション鍵を受信するには、アプリケーション ユーザまたはエンド ユーザが Standard CTI Enabled、Standard CTI Secure Connection、および Standard CTI Allow Reception of SRTP Key Material の 3 つのグループに存在する必要があります。

Cisco Unified Communications Manager Assistant、Cisco QRT、および Cisco Web Dialer は暗号化をサポートしないため、アプリケーション ユーザである CCMQRTSecureSysUser、IPMA SecureSysUser、および WDSecureSysUser を Standard CTI Allow Reception of SRTP Key Material ユーザグループに追加する必要はありません。



ヒント

ユーザグループからのアプリケーション ユーザまたはエンド ユーザの削除については、『Cisco Unified Communications Manager アドミニストレーションガイド』を参照してください。[権限の設定 (Role Configuration)] ウィンドウでのセキュリティ関連の設定については、『Cisco Unified Communications Manager アドミニストレーションガイド』を参照してください。

手順

- ステップ 1** Cisco Unified Communications Manager の管理ページで、[ユーザ管理] > [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.12-18 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 Communications Manager は、Cisco Unified Serviceability で Certificate Authority Proxy Function サービスを自動的にアクティブ化しません。Certificate Authority Proxy Function サービスのアクティブ化については、『*Cisco Unified Communications Manager Serviceability アドミニストレーションガイド*』を参照してください。

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.3-13 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 Cisco Unified Communications Manager サーバにコピーされ、拡張子 .0 を使用します。CAPF 証明書が存在することを確認するには、Cisco Unified Communications オペレーティングシステムの GUI で、CAPF 証明書を表示します。

CAPF サービス パラメータの更新

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

Cisco Unified Communications Manager の管理ページで CAPF サービス パラメータをアクティブとして表示するには、Cisco Unified Serviceability で Certificate Authority Proxy Function サービスをアクティブ化する必要があります。



ヒント

電話機で CAPF を使用したときに CAPF サービス パラメータを更新した場合は、ここでサービス パラメータを更新する必要はありません。

CAPF サービス パラメータを更新するには、次の手順を実行します。

手順

- ステップ 1** Cisco Unified Communications Manager の管理ページで、[システム]>[サービスパラメータ]を選択します。
- ステップ 2** [サーバ (Server)] ドロップダウン リスト ボックスから、サーバを選択します。
- 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 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.12-18 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、次のオプションのいずれかを選択します。

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

レコードをフィルタリングまたは検索するには、次の手順を実行します。

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



(注) 検索条件を追加するには、[+] ボタンをクリックします。条件を追加すると、指定したすべての条件に一致するレコードが検索されます。条件を削除するには、[-] ボタンをクリックして最後に追加した条件を削除するか、[フィルタのクリア] ボタンをクリックして追加したすべての検索条件を削除します。

ステップ 3 [検索] をクリックします。

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

ステップ 4 表示するレコードのリストから、表示するレコードのリンクをクリックします。



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

ウィンドウに選択した項目が表示されます。

追加情報

詳細については、[P.12-18](#) 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 12-2 を参照してください。



ヒント

エンド ユーザ CAPF プロファイルを設定する前に、アプリケーション ユーザ CAPF プロファイルを設定することをお勧めします。

手順

ステップ 1 Cisco Unified Communications Manager の管理ページで次のいずれかのオプションを選択します。

- [ユーザ管理] > [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] ボタンまたは [新規追加] アイコンをクリックします (プロファイルを表示してから、[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をコピーするには、P.12-12 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、[コピー (Copy)] 列内にあるそのレコード用の [コピー (Copy)] ボタンをクリックします (プロファイルを表示してから、[コピー] 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、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.12-12 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 12-2 の説明に従って、適切な設定を入力します。

ステップ 4 [保存] ボタンまたは [保存] アイコンをクリックします。

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 CCMQRTSecureSysUser、IPMASecureSysUser、または WDSecureSysUser を設定する場合は、P.12-17 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.12-18 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 プロファイルおよびエンドユーザ CAPF プロファイルの CAPF 設定ウィンドウ

表 12-2 に、[アプリケーションユーザ CAPF プロファイルの設定 (Application User CAPF Profile Configuration)] ウィンドウおよび[エンドユーザ CAPF プロファイルの設定 (End User CAPF Profile Configuration)] ウィンドウでの CAPF 設定を示します。

- 設定のヒントについては、P.12-6 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.12-18 の「関連項目」を参照してください。

表 12-2 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 ID]	<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.12-17 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"> • [保留中の操作なし]: 証明書の操作が発生しないときに表示されます (デフォルトの設定)。 • [インストール/アップグレード]: アプリケーションのローカルで有効な証明書を新しくインストールするか、あるいは既存の証明書をアップグレードします。

表 12-2 アプリケーション ユーザ CAPF プロファイルおよびエンド ユーザ CAPF プロファイルの設定内容 (続き)

設定	説明
[認証モード (Authentication Mode)]	証明書のインストールまたはアップグレード操作の認証モードは [認証ストリング] 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せん。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 Communications Manager の間で接続を確立するために、60 秒以上の時間がかかることがあります。最高のセキュリティ レベルを使用する場合を除き、2048 ビットの鍵は設定しないでください。
[操作の完了 (Operation Completes By)]	このフィールドは、すべての証明書操作をサポートし、操作を完了する必要がある期限の日付と時刻を指定します。 表示される値は、最初のノードに適用されます。 この設定は、証明書操作を完了する必要があるデフォルトの日数を指定する CAPF Operation Expires in (days) エンタープライズパラメータとともに使用します。このパラメータはいつでも更新できます。
[証明書操作ステータス (Certificate Operation Status)]	このフィールドは、pending、failed、successful など、証明書操作の進行状況を表示します。 このフィールドに表示される情報は変更できません。

アプリケーション ユーザ CAPF プロファイルまたはエンド ユーザ CAPF プロファイルの削除

ここでは、アプリケーション ユーザ CAPF プロファイルまたはエンド ユーザ CAPF プロファイルを Cisco Unified Communications Manager データベースから削除する方法を説明します。

始める前に

Cisco Unified Communications Manager の管理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、レコードの[依存関係レコード要約 (Dependency Records Summary)] ウィンドウに、依存関係レコードを有効にすると実行できるアクションを示すメッセージが表示されます。また、依存関係レコード機能を使用すると、CPU 使用率が高くなるという情報も表示されます。依存関係レコードの詳細については、『Cisco Unified Communications Manager システム ガイド』を参照してください。

手順

-
- ステップ 1** P.12-12 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。
- ステップ 2** 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 3** 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] アイコンまたはボタンをクリックします。
 - 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、[削除] アイコンまたは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.12-18 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** [システム] > [サービスパラメータ] を選択します。
 - ステップ 2** [サーバ (Server)] ドロップダウン リスト ボックスから、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 \(P.12-2\)](#)
- [CTI、JTAPI、および TAPI アプリケーションの暗号化について \(P.12-4\)](#)
- [CTI、JTAPI、および TAPI アプリケーションに対する CAPF の概要 \(P.12-5\)](#)
- [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 \(P.12-6\)](#)
- [CTI、JTAPI、および TAPI のセキュリティ設定用チェックリスト \(P.12-7\)](#)
- [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 \(P.12-9\)](#)
- [Certificate Authority Proxy Function サービスのアクティブ化 \(P.12-10\)](#)
- [CAPF サービス パラメータの更新 \(P.12-11\)](#)
- [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 \(P.12-12\)](#)
- [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 \(P.12-13\)](#)
- [アプリケーションユーザ CAPF プロファイルおよびエンドユーザ CAPF プロファイルの CAPF 設定ウィンドウ \(P.12-14\)](#)
- [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 \(P.12-16\)](#)
- [JTAPI/TAPI セキュリティ関連サービス パラメータ \(P.12-17\)](#)
- [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 \(P.12-18\)](#)

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



PART 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 \(P.13-1\)](#)
- [SRST セキュリティの設定のヒント \(P.13-2\)](#)
- [SRST のセキュリティ設定用チェックリスト \(P.13-3\)](#)
- [SRST リファレンスのセキュリティ設定 \(P.13-4\)](#)
- [SRST リファレンスのセキュリティの設定内容 \(P.13-6\)](#)
- [SRST リファレンスからのセキュリティの削除 \(P.13-7\)](#)
- [SRST 証明書がゲートウェイから削除された場合 \(P.13-7\)](#)
- [その他の情報 \(P.13-7\)](#)

SRST のセキュリティの概要

SRST 対応ゲートウェイは、Cisco Unified Communications Manager がコールを完了できない場合に、制限付きのコール処理タスクを提供します。

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 Communications Manager の管理ページで SRST 設定作業を実行した後、Cisco Unified Communications Manager は TLS 接続を使用して SRST 対応ゲートウェイで証明書プロバイダ サービスを認証します。Cisco Unified Communications Manager は SRST 対応ゲートウェイから証明書を取得して、その証明書を Cisco Unified Communications Manager データベースに追加します。

Cisco Unified Communications Manager の管理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

次の基準が満たされることを確認します。この基準を満たすと、保護された電話機と SRST 対応ゲートウェイとの間で接続の安全が保障されます。

- 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混合モードを設定した。
- 電話機に認証または暗号化を設定した。
- Cisco Unified Communications Manager の管理ページで 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 Communications Manager は、SRST 対応ゲートウェイ向けに、電話機の証明書情報を含む PEM 形式のファイルを提供します。

LSC 認証では、CAPF ルート証明書 (CAPF.der) をダウンロードしてください。このルート証明書では、セキュアな 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 Communications Manager 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あります。このような場合、電話機は、クラスタ内で SRST 対応ゲートウェイおよび Cisco Unified Communications Manager サーバとの非セキュア接続を試行します。
- クラスタ セキュリティ モードが非セキュアになっている場合は、デバイス セキュリティ モードや [セキュア SRST(Is SRST Secure?)] チェックボックスなど、セキュリティ関連の設定が無視されます。設定がデータベースから削除されることはありませんが、セキュリティは提供されません。
- 電話機が SRST 対応ゲートウェイへのセキュア接続を試行するのは、クラスタ セキュリティ モードが混合モードで、電話機設定ファイル内のデバイス セキュリティ モードが認証済みまたは暗号化済みに設定されており、[SRST 参照先の設定 (SRST Reference Configuration)] ウィンドウで [セキュア SRST(Is SRST Secure?)] チェックボックスがオンになっている、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。
- 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 Communications Manager セキュリティ モードが混合モードから非セキュア モードに切り替わった場合、これらの電話機は自動的に Cisco Unified Communications Manager にフォールバックされません。SRST ルータの電源を切り、強制的にこれらの電話機を Cisco Unified Communications Manager に再登録する必要があります。電話機が Cisco Unified Communications Manager にフォールバックした後、管理者は SRST の電源を投入でき、フェールオーバーおよびフォールバックが再び自動になります。

SRST のセキュリティ設定用チェックリスト

表 13-1 を使用して、SRST のセキュリティ設定手順を進めます。

表 13-1 SRST のセキュリティ設定用チェックリスト

設定手順	関連手順および関連項目
ステップ 1 SRST 対応ゲートウェイに必要なすべての作業を実行したことを確認します。すべてを実行すると、デバイスが Cisco Unified Communications Manager およびセキュリティをサポートします。	このバージョンの Cisco Unified Communications Manager をサポートする『Cisco IOS SRST Version System Administrator Guide』これは、次の URL で入手できます。 http://www.cisco.com/univercd/cc/td/doc/product/voice/srst/srst33/srst33ad/index.htm
ステップ 2 Cisco CTL クライアントのインストールおよび設定に必要なすべての作業を実行したことを確認します。	Cisco CTL クライアントの設定 (P.3-1)
ステップ 3 電話機に証明書が存在することを確認します。	使用中の電話機モデルの Cisco Unified IP Phone マニュアルを参照してください。
ステップ 4 電話機に認証または暗号化を設定したことを確認します。	電話機セキュリティ プロファイルの適用(P.5-12)
ステップ 5 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。	SRST リファレンスのセキュリティ設定 (P.13-4)
ステップ 6 SRST 対応ゲートウェイと電話機をリセットします。	SRST リファレンスのセキュリティ設定 (P.13-4)

SRST リファレンスのセキュリティ設定

Cisco Unified Communications Manager 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 13-2 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 Communications Manager 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 Communications Manager は Cisco Unified Communications Manager サーバまたはクラスタ内の各 Cisco Unified Communications Manager サーバで、信頼できるフォルダにある SRST 対応ゲートウェイの証明書を置き換えます。
- 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 Communications Manager データベースおよび電話機の cnf.xml ファイルから SRST 対応ゲートウェイの証明書が削除されます。

SRST リファレンスの削除方法は、『Cisco Unified Communications Manager アドミニストレーションガイド』を参照してください。

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 Communications Manager の管理ページで、[システム] > [SRST] を選択します。

検索と一覧表示ウィンドウが表示されます。

ステップ 2 次の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] ボタンまたはアイコンをクリックします（プロファイルを表示してから、[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表示されます。
- 既存の SRST リファレンスをコピーするには、『Cisco Unified Communications Manager アドミニストレーションガイド』の説明に従って適切な SRST リファレンスを見つけ、[コピー (Copy)] 列内にあるそのレコード用の [コピー (Copy)] ボタンをクリックします（プロファイルを表示してから、[コピー] 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、設定内容が表示されます。
- 既存の SRST リファレンスを更新するには、『Cisco Unified Communications Manager アドミニストレーションガイド』の説明に従って適切な SRST リファレンスを見つけます。設定ウィンドウが表示され、現在の設定が表示されます。

ステップ 3 表 13-2 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 Communications Manager アドミニストレーションガイド』を参照してください。

ステップ 4 [セキュア SRST(Is SRST Secure?)] チェックボックスをオンにすると、[証明書の更新] 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**] ボタンをクリックします。



ヒント このボタンは、[**セキュア SRST(Is SRST Secure?)**] チェックボックスをオンにして [**保存**] 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.13-7](#) 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 13-2 で、保護された SRST リファレンスに対して Cisco Unified Communications Manager 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.13-2 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.13-7 の「関連項目」を参照してください。

表 13-2 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 Communications Manager データベースに格納します。</p> <p></p> <p>ヒント データベースおよび電話機から SRST 証明書を削除するには、このチェックボックスをオフにして [保存] 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 Communications Manager はこのポートを使用して SRST 対応ゲートウェイから証明書を取得します。Cisco SRST 証明書プロバイダ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></p> <p>ヒント ポートが現在使用中の場合や、ファイアウォールを使用して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></p> <p>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。</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 Communications Manager データベースに格納されている既存の SRST 対応ゲートウェイの証明書を置き換えます（証明書がデータベースに存在する場合）。従属する電話機をリセットした後、TFTP サーバは cnf.xml ファイルを（新しい SRST 対応ゲートウェイの証明書と共に）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、[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 Communications Manager データベースと IP Phone から削除する必要があります。

この作業を実行するには、[SRST 参照先の設定 (SRST Reference Configuration)] ウィンドウで、[セキュア SRST(Is SRST Secure?)] チェックボックスをオフにして [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 \(P.13-1\)](#)
- [SRST セキュリティの設定のヒント \(P.13-2\)](#)
- [SRST のセキュリティ設定用チェックリスト \(P.13-3\)](#)
- [SRST リファレンスのセキュリティ設定 \(P.13-4\)](#)
- [SRST リファレンスのセキュリティの設定内容 \(P.13-6\)](#)
- [SRST リファレンスからのセキュリティの削除 \(P.13-7\)](#)
- [SRST 証明書がゲートウェイから削除された場合 \(P.13-7\)](#)

シスコの関連マニュアル

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



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 \(P.14-2\)](#)
- [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 \(P.14-3\)](#)
- [SIP トランクの暗号化の概要 \(P.14-4\)](#)
- [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 \(P.14-5\)](#)
- [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 \(P.14-6\)](#)
- [Cisco Unified Communications Manager とゲートウェイまたはトランクとの間で IPSec を設定する場合の注意事項 \(P.14-6\)](#)
- [SRTP を許可 \(SRTP Allowed\) チェックボックスの設定 \(P.14-7\)](#)
- [その他の情報 \(P.14-8\)](#)

Cisco IOS MGCP ゲートウェイの暗号化の概要

Cisco Unified Communications Manager は、MGCP SRTP パッケージを使用するゲートウェイをサポートしています。MGCP SRTP パッケージは、ゲートウェイがセキュア RTP 接続上でパケットを暗号化および復号化するとき使用されます。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 Communications Manager はセキュア コールのためのマスター暗号鍵とソルトを生成し、SRTP ストリームの場合にのみゲートウェイに送信します。ゲートウェイでもサポートされている SRTCP ストリームの場合、Cisco Unified Communications Manager は鍵とソルトを送信しません。これらの鍵は MGCP シグナリングパスを介してゲートウェイに送信されます。これは、IPSec を使用してセキュリティを設定する必要があります。Cisco Unified Communications Manager は IPSec 接続が存在するかどうかを認識しませんが、IPSec が設定されていない場合、システムはゲートウェイにセッション鍵を暗号化せずに送信します。セッション鍵がセキュア接続を介して送信されるように、IPSec 接続が存在することを確認します。



ヒント

SRTP 用に設定された MGCP ゲートウェイが、認証されたデバイス（認証された SCCP 電話機など）とのコールに関わる場合、Cisco Unified Communications Manager はこのコールを認証済みとして分類するため、電話機にシールドアイコンが表示されます。コールに対してデバイスの SRTP 機能が正常にネゴシエートされると、Cisco Unified Communications Manager は、このコールを暗号化済みとして分類します。MGCP ゲートウェイがセキュリティアイコンを表示できる電話機に接続されている場合、コールが暗号化されていると、電話機にロックアイコンが表示されます。

H.323 ゲートウェイおよび H.323/H.225/H.245 トランクの暗号化の概要

セキュリティをサポートする H.323 ゲートウェイおよびゲートキーパーまたは非ゲートキーパー制御の H.225/H.323/H.245 トランクは、Cisco Unified Communications オペレーティング システム で IPsec アソシエーションを設定した場合、Cisco Unified Communications Manager に対して認証ができません。Cisco Unified Communications Manager とこれらのデバイスとの間で IPsec アソシエーションを作成する方法については、『Cisco Unified Communications Operating System 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 Communications Manager Business Edition システムでは Intercluster Trunk (ICT; クラスタ間トランク) はサポートされていません。H.323 トランクは、ゲートウェイ、プロキシ、MCU、IP PSTN 接続およびデバイスでサポートされています。

H.323、H.225、および H.245 デバイスは暗号鍵を生成します。これらの鍵は、IPsec で保護されたシグナリング パスを介して Cisco Unified Communications Manager に送信されます。Cisco Unified Communications Manager は IPsec 接続が存在するかどうかを認識しませんが、IPsec が設定されていない場合、セッション鍵は暗号化されずに送信されます。セッション鍵がセキュア接続を介して送信されるように、IPsec 接続が存在することを確認します。

IPsec アソシエーションの設定に加えて、Cisco Unified Communications Manager の管理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。H.323 ゲートウェイ、H.225 トランク (ゲートキーパー制御)、クラスタ間トランク (ゲートキーパー制御)、クラスタ間トランク (非ゲートキーパー制御) などのデバイス設定ウィンドウがあります。このチェックボックスをオンにしない場合、Cisco Unified Communications Manager は RTP を使用してデバイスと通信します。このチェックボックスをオンにした場合、Cisco Unified Communications Manager は、デバイスに対して SRTP が設定されているかどうかに応じて、セキュア コールまたは非セキュア コールを発生させます。



注意

Cisco Unified Communications Manager の管理ページで [SRTP を許可 (SRTP Allowed)] チェックボックスをオンにした場合は、セキュリティ関連情報が暗号化されずに送信されることを防ぐために、IPsec を設定することを強く推奨します。

Cisco Unified Communications Manager は、IPsec 接続が正しく設定されているかどうかを確認しません。接続が正しく設定されていない場合、セキュリティ関連情報が暗号化されずに送信されることがあります。

セキュア メディア パスまたはセキュア シグナリング パスを確立でき、デバイスが SRTP をサポートする場合、システムは SRTP 接続を使用します。セキュア メディア パスまたはセキュア シグナリング パスを確立できない、または 1 つ以上のデバイスが SRTP をサポートしない場合、システムは RTP 接続を使用します。SRTP から RTP への (およびその逆の) フォールバックは、セキュア デバイスから非セキュア デバイスへの転送、電話会議、トランスコーディング、保留音などで発生する場合があります。



ヒント

コールがパススルー対応 MTP を使用し、リージョン フィルタリングの後でデバイスの音声機能が一致し、どのデバイスに対しても [メディアターミネーションポイントが必須 (Media Termination Point Required)] チェックボックスがオンになっていない場合、Cisco Unified Communications Manager はこのコールをセキュアに分類します。[メディアターミネーションポイントが必須 (Media Termination Point Required)] チェックボックスがオンの場合、Cisco Unified Communications Manager は、コールの音声パススルーを無効にし、コールを非セキュアに分類します。コールに関連する MTP がない場合、デバイスの SRTP 機能によっては、Cisco Unified Communications Manager がそのコールを暗号化済みに分類することがあります。

SRTP が設定されているデバイスでは、デバイスに対する [SRTP を許可 (SRTP Allowed)] チェックボックスがオンで、デバイスの SRTP 機能がコールに対して正常にネゴシエートされた場合、Cisco Unified Communications Manager はコールを暗号化済みに分類します。この基準を満たさない場合、Cisco Unified Communications Manager は、コールを非セキュアに分類します。デバイスがセキュリティ アイコンを表示できる電話機に接続されている場合、コールが暗号化されていると、電話機にロック アイコンが表示されます。

Cisco Unified Communications Manager は、トランクまたはゲートウェイによるアウトバウンド FastStart コールを非セキュアに分類します。Cisco Unified Communications Manager の管理ページで、[SRTP を許可 (SRTP Allowed)] チェックボックスをオンにした場合、Cisco Unified Communications Manager は [アウトバウンド FastStart を有効にする (Enable Outbound FastStart)] チェックボックスを無効にします。

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。このオプションによって、シグナリング暗号化は提供されますが、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。



(注)

クラスタ間トランク (ICT) は Cisco Unified Communications Manager Business Edition システムではサポートされていません。SIP トランクは、ゲートウェイ、プロキシ、MCU、IP PSTN 接続およびデバイスでサポートされています。

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、[暗号化] 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 Communications Manager 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 14-1 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/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_11/gtsecure.htm

表 14-1 MGCP ゲートウェイのセキュリティ設定用チェックリスト

設定手順	関連手順および関連項目
ステップ 1 Cisco CTL クライアントをインストールし、設定したことを確認します。Cisco Unified Communications Manager 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)
ステップ 2 電話機に暗号化を設定したことを確認します。	電話機のセキュリティの概要 (P.4-1)
ステップ 3 IPSec を設定します。  ヒント ネットワーク インフラストラクチャで IPSec を設定することも、Cisco Unified Communications Manager とゲートウェイまたはトランクとの間で IPSec を設定することもできます。どちらかの方法で IPSec を設定した場合、もう 1 つの方法を使用する必要はありません。	<ul style="list-style-type: none"> 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.14-6) Cisco Unified Communications Manager とゲートウェイまたはトランクとの間で IPSec を設定する場合の注意事項 (P.14-6)
ステップ 4 H.323 IOS ゲートウェイおよびクラスタ間トランクの場合、Cisco Unified Communications Manager の管理ページで [SRTP を許可 (SRTP Allowed)] チェックボックスをオンにします。	[SRTP を許可 (SRTP Allowed)] チェックボックスは [トランクの設定 (Trunk Configuration)] ウィンドウまたは [ゲートウェイの設定 (Gateway Configuration)] ウィンドウに表示されます。これらのウィンドウを表示する方法については、『 <i>Cisco Unified Communications Manager 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。
ステップ 5 SIP トランクの場合、SIP トランク セキュリティ プロファイルを設定し、トランクに適用します (この処理を行っていない場合)。	<ul style="list-style-type: none"> SIP トランクの暗号化の概要 (P.14-4) SIP トランク セキュリティ プロファイルの設定 (P.15-4)
ステップ 6 ゲートウェイでセキュリティ関連の設定タスクを実行します。	<ul style="list-style-type: none"> <i>Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways</i>

ネットワーク インフラストラクチャで IPsec を設定する場合の注意事項

このマニュアルでは、IPsec の設定方法は説明しません。代わりに、ネットワーク インフラストラクチャで IPsec を設定する際の考慮事項と推奨事項を示します。IPsec をネットワーク インフラストラクチャで設定し、Cisco Unified Communications Manager とデバイスとの間では設定しない場合は、IPsec の設定前に、次のことを検討してください。

- シスコは、Cisco Unified Communications Manager 自身ではなくインフラストラクチャで IPsec をプロビジョニングすることをお勧めします。
- IPsec を設定する前に、既存の IPsec または VPN 接続、プラットフォームの CPU への影響、帯域幅への影響、ジッタまたは待ち時間、およびその他のパフォーマンス上のメトリックを考慮してください。
- 『*Voice and Video Enabled IPsec Virtual Private Networks Solution Reference Network Design Guide*』を参照してください。これは、次の URL で入手できます。
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns241/c649/ccmigration_09186a00801ea79c.pdf
- 『*Cisco IOS Security Configuration Guide, Release 12.2 (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
- 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.14-5 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 Communications Manager とゲートウェイまたはトランクとの間で IPsec を設定する場合の注意事項

この章で説明する Cisco Unified Communications Manager とゲートウェイまたはトランクとの間での IPsec の設定については、『*Cisco Unified Communications Operating System 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 Communications Manager 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 トランク (ゲートキーパー制御) のトランク設定ウィンドウ
- クラスタ間トランク (ゲートキーパー制御) のトランク設定ウィンドウ
- クラスタ間トランク (非ゲートキーパー制御) のトランク設定ウィンドウ



(注)

クラスタ間トランク (ICT) は Cisco Unified Communications Manager Business Edition システムではサポートされていません。H.323 および SIP トランクは、ゲートウェイ、プロキシ、MCU、IP PSTN 接続およびデバイスでサポートされています。

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 Communications Manager アドミニストレーション ガイド』の説明に従って、ゲートウェイまたはトランクを検索します。
- ステップ 2** ゲートウェイまたはトランクの設定ウィンドウが開いたら、[SRTP を許可 (SRTP Allowed)] チェックボックスをオンにします。
- 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.14-8 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 \(P.1-18 \)](#)
- [暗号化の概要 \(P.1-23 \)](#)
- [Cisco IOS MGCP ゲートウェイの暗号化の概要 \(P.14-2 \)](#)
- [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 \(P.14-3 \)](#)
- [SIP トランクの暗号化の概要 \(P.14-4 \)](#)
- [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 \(P.14-5 \)](#)
- [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 \(P.14-6 \)](#)
- [Cisco Unified Communications Manager とゲートウェイまたはトランクとの間で IPsec を設定する場合の注意事項 \(P.14-6 \)](#)

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 \(P.15-2\)](#)
- [SIP トランク セキュリティ プロファイルの設定のヒント \(P.15-2\)](#)
- [SIP トランク セキュリティ プロファイルの検索 \(P.15-3\)](#)
- [SIP トランク セキュリティ プロファイルの設定 \(P.15-4\)](#)
- [SIP トランク セキュリティ プロファイルの設定内容 \(P.15-5\)](#)
- [SIP トランク セキュリティ プロファイルの適用 \(P.15-10\)](#)
- [SIP トランク セキュリティ プロファイルの削除 \(P.15-11\)](#)
- [その他の情報 \(P.15-12\)](#)

SIP トランク セキュリティ プロファイルの概要

Cisco Unified Communications Manager の管理ページでは、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。



(注)

Cisco Unified Communications Manager Business Edition システムでは Intercluster Trunk (ICT; クラスター間トランク) はサポートされていません。SIP トランクは、ゲートウェイ、プロキシ、MCU、IP PSTN 接続およびデバイスでサポートされています。

Cisco Unified Communications Manager をインストールすると、自動登録用の事前定義済み非セキュア SIP トランク セキュリティ プロファイルが提供されます。SIP トランクのセキュリティ機能を有効にするには、新しいセキュリティ プロファイルを設定し、SIP トランクに適用します。トランクがセキュリティをサポートしていない場合は、非セキュア プロファイルを選択します。

SIP トランクがサポートするセキュリティ機能だけが、セキュリティ プロファイル設定ウィンドウに表示されます。

SIP トランク セキュリティ プロファイルの設定のヒント

Cisco Unified Communications Manager の管理ページで 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。

SIP トランク セキュリティ プロファイルの検索

SIP トランク セキュリティ プロファイルを検索するには、次の手順を実行します。

手順

ステップ 1 [システム] > [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。

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

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

レコードをフィルタリングまたは検索するには、次の手順を実行します。

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



(注) 検索条件を追加するには、[+] ボタンをクリックします。条件を追加すると、指定したすべての条件に一致するレコードが検索されます。条件を削除するには、[-] ボタンをクリックして最後に追加した条件を削除するか、[フィルタのクリア] ボタンをクリックして追加したすべての検索条件を削除します。

ステップ 3 [検索] をクリックします。

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

ステップ 4 表示するレコードのリストから、表示するレコードのリンクをクリックします。



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

ウィンドウに選択した項目が表示されます。

追加情報

詳細については、[P.15-12](#) 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 Communications Manager 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] ボタンまたは検索ウィンドウ内のアイコンをクリックします (プロファイルを表示してから、[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。
- 既存のセキュリティ プロファイルをコピーするには、P.15-3 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、[コピー (Copy)] 列内にあるそのレコード用の [コピー (Copy)] ボタンをクリックします (プロファイルを表示してから、[コピー] 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、設定内容が示されます。
- 既存のプロファイルを更新するには、P.15-3 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 15-1 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] ボタンまたはアイコンをクリックします。

追加の手順

セキュリティ プロファイルを作成した後、P.15-10 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.15-12 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 15-1 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.15-2 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.15-12 の「関連項目」を参照してください。

表 15-1 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"> • [非セキュア]: 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 Communications Manager が利用できる。 • [認証のみ]: Cisco Unified Communications Manager 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。 • [暗号化]: Cisco Unified Communications Manager 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。 <p> (注) 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 [非セキュア] 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 [認証のみ] または [暗号化] である場合、[TLS] が転送タイプとなります。</p> <p> (注) Transport Layer Security (TLS) プロトコルによって、Cisco Unified Communications Manager とトランクとの間の接続が保護されません。</p>

表 15-1 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 [非セキュア] 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 [認証のみ] または [暗号化] 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 Communications Manager システムと IOS ゲートウェイの間で SIP トランクを接続する場合は、発信転送タイプとして UDP を使用する必要があります。詳細については、『Cisco Unified Communications Manager システム ガイド』の「セッション開始プロトコル (SIP) の概要」を参照してください。</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 Communications Manager は、トランクからのすべての SIP 要求でチャレンジを行います。</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 [認証のみ] または [暗号化] 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.1-20 の「ダイジェスト認証」および P.16-1 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 Communications Manager 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 15-1 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 Communications Manager クラスタがある場合、または TLS ピアに対して SRV ルックアップを使用する場合、単一のトランクが複数のホストに解決されることがあります。その結果、トランクに複数の X.509 の件名が設定されます。複数の X.509 の件名がある場合は、スペース、カンマ、セミコロン、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></p> <p>ヒント 件名は、送信元接続の TLS 証明書に対応します。件名が、件名とポートで一意であることを確認してください。同じ件名と着信ポートの組み合わせを、異なる SIP トランクに割り当てることはできません。</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></p> <p>ヒント 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 15-1 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 Communications Manager は、許可されているアプリケーション方式を確認する前に、SIP アプリケーション ユーザを認証します。</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 Communications Manager は、[アプリケーションユーザの設定 (Application User Configuration)] ウィンドウで SIP アプリケーション ユーザに許可されている方式よりも先に、(このセキュリティ プロファイルで) トランクに許可されている方式を確認します。</p> <p> ヒント アプリケーションの ID を信頼しない場合、またはアプリケーションが特定のトランクで信頼されていない場合は、アプリケーションレベルの許可の使用を検討してください。アプリケーション要求は、予期しないトランクから着信することがあります。</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.16-1 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.1-22 の「許可」および P.1-8 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 Communications Manager アドミニストレーションガイド』を参照してください。</p> <p>Cisco Unified Communications Manager が SIP トランク経由で着信するプレゼンス サブスクリプション要求を受け付けるようにする場合は、このチェックボックスをオンにします。</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 15-1 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 Communications Manager 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 Communications Manager 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 Communications Manager が既存の SIP ダイアログを置き換える新しい SIP ダイアログを受け付けるようにする場合は、このチェックボックスをオンにします。</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 Communications Manager アドミニストレーション ガイド』の説明に従って、トランクを検索します。
 - ステップ 2** [トランクの設定 (Trunk Configuration)] ウィンドウが表示されたら、[SIP トランクセキュリティプロファイル] 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alm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.16-5 の「SIP レalm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.15-12 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 Communications Manager データベースから SIP トランク セキュリティ プロファイルを削除する方法について説明します。

始める前に

Cisco Unified Communications Manager の管理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、レコードの [依存関係レコード要約 (Dependency Records Summary)] ウィンドウに、依存関係レコードを有効にすると実行できるアクションを示すメッセージが表示されます。また、依存関係レコード機能を使用すると、CPU 使用率が高くなるという情報も表示されます。依存関係レコードの詳細については、『Cisco Unified Communications Manager システム ガイド』を参照してください。

手順

- ステップ 1** P.15-3 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、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 3** 単一のセキュリティ プロファイルを削除するには、次の作業のどちらかを実行します。
 - 検索と一覧表示ウィンドウで、適切なセキュリティ プロファイルの横に表示されているチェックボックスをオンにして、[選択項目の削除] アイコンまたは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] アイコンまたは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.15-12 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 \(P.15-2\)](#)
- [SIP トランク セキュリティ プロファイルの設定のヒント \(P.15-2\)](#)
- [SIP トランク セキュリティ プロファイルの検索 \(P.15-3\)](#)
- [SIP トランク セキュリティ プロファイルの設定 \(P.15-4\)](#)
- [SIP トランク セキュリティ プロファイルの設定内容 \(P.15-5\)](#)
- [SIP トランク セキュリティ プロファイルの適用 \(P.15-10\)](#)
- [SIP トランク セキュリティ プロファイルの削除 \(P.15-11\)](#)
- [許可 \(P.1-22\)](#)
- [相互作用 \(P.1-8\)](#)
- [ダイジェスト認証 \(P.1-20\)](#)

シスコの関連マニュアル

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

Cisco Unified Communications Manager システム ガイド



SIP トランクのダイジェスト認証の設定

SIP トランクにダイジェスト認証を設定すると、Cisco Unified Communications Manager は、SIP トランクで SIP 要求を受信したときに、SIP ユーザ エージェントの ID でチャレンジを行うことができます。Cisco Unified Communications Manager がトランクへ SIP 要求を送信した場合は、SIP ユーザ エージェントが Cisco Unified Communications Manager の ID でチャレンジを行うことができます。SIP トランクでのダイジェスト認証の動作の詳細については、P.1-20 の「ダイジェスト認証」を参照してください。



(注)

Cisco Unified Communications Manager Business Edition システムでは Intercluster Trunk (ICT; クラスター間トランク) はサポートされていません。SIP トランクは、ゲートウェイ、プロキシ、MCU、IP PSTN 接続およびデバイスでサポートされています。

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.16-2)
- 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.16-2)
- 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.16-3)
- 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.16-3)
- SIP レルムの検索 (P.16-4)
- SIP レルムの設定 (P.16-5)
- SIP レルムの設定内容 (P.16-6)
- SIP レルムの削除 (P.16-7)
- その他の情報 (P.16-7)

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 16-1 で説明します。

表 16-1 SIP トランクのセキュリティ設定用チェックリスト

設定手順	関連手順および関連項目
ステップ 1 SIP トランクのセキュリティ プロファイルを設定します。 [ダイジェスト認証を有効化(Enable Digest Authentication)] チェックボックスがオンになっていることを確認します。	<ul style="list-style-type: none"> • SIP トランク セキュリティ プロファイルの設定 (P.15-4) • ダイジェスト認証 (P.1-20)
ステップ 2 SIP トランク セキュリティ プロファイルをトランクに適用します。	SIP トランク セキュリティ プロファイルの適用 (P.15-10)
ステップ 3 Cluster ID エンタープライズ パラメータを設定します (設定していない場合)。 このパラメータを使用しても、Cisco Unified Communications Manager は、SIP トランクで SIP 要求を送信する SIP ユーザ エージェントの ID でチャレンジを行うことができます。	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.16-2)
ステップ 4 Cisco Unified Communications Manager は、SIP トランクで SIP 要求を送信する SIP ユーザ エージェントの ID でチャレンジを行い、 [アプリケーションユーザの設定 (Application User Configuration)] ウィンドウで、アプリケーション ユーザのダイジェスト クレデンシャルを設定します。	<ul style="list-style-type: none"> • 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.16-3) • 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.16-3)
ステップ 5 Cisco Unified Communications Manager がトランク ピアからのチャレンジに応答した場合は、SIP レルムを設定します。	<ul style="list-style-type: none"> • ダイジェスト認証 (P.1-20) • SIP レルムの設定 (P.16-5) • SIP レルムの設定内容 (P.16-6)

ダイジェスト認証のエンタープライズ パラメータの設定

Cluster ID エンタープライズ パラメータをダイジェスト認証用に設定するには、Cisco Unified Communications Manager の管理ページで、**[システム] > [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。このパラメータを使用しても、Cisco Unified Communications Manager は、SIP トランクで SIP 要求を送信する SIP ユーザ エージェントの ID でチャレンジを行うことができます。



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 Communications Manager が SIP ユーザ エージェントの ID でチャレンジを行う場合は、Cisco Unified Communications Manager の管理ページの [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 Communications Manager 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 Communications Manager アドミニストレーション ガイド』の説明に従って、アプリケーション ユーザを検索します。
- ステップ 2** アプリケーション ユーザのリンクをクリックします。
- ステップ 3** 目的の [アプリケーションユーザの設定 (Application User Configuration)] ウィンドウが表示されたら、表 16-2 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.16-7 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 16-2 で、Cisco Unified Communications Manager 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.16-7 の「関連項目」を参照してください。

表 16-2 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 Communications Manager 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 データベース内のすべてのレコードを検索するには、ダイアログボックスが空であることを確認して、[ステップ 3](#) へ進みます。

レコードをフィルタリングまたは検索するには、次の手順を実行します。

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



(注) 検索条件を追加するには、[+] ボタンをクリックします。条件を追加すると、指定したすべての条件に一致するレコードが検索されます。条件を削除するには、[-] ボタンをクリックして最後に追加した条件を削除するか、[フィルタのクリア] ボタンをクリックして追加したすべての検索条件を削除します。

ステップ 3 [検索] をクリックします。

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

ステップ 4 表示するレコードのリストから、表示するレコードのリンクをクリックします。



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

ウィンドウに選択した項目が表示されます。

追加の手順

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.16-2](#) 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.16-7](#) の「[関連項目](#)」を参照してください。

SIP レルムの設定

Cisco Unified Communications Manager が 1 つまたは複数のトランク ピアからのチャレンジに回答する場合は、Cisco Unified Communications Manager でチャレンジを実行できる SIP トランク ユーザエージェントの SIP レルムを設定する必要があります。

SIP レルムを追加または更新するには、次の手順を実行します。

手順

ステップ 1 Cisco Unified Communications Manager の管理ページで、[ユーザ管理] > [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、検索ウィンドウで [新規追加] ボタンまたは [新規追加] アイコンをクリックします (SIP レルムを表示してから、[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。
- 既存のセキュリティ プロファイルをコピーするには、P.16-4 の「SIP レルムの検索」の説明に従って適切なプロファイルを見つけ、[コピー (Copy)] 列内にあるそのレコード用の [コピー (Copy)] ボタンをクリックします (SIP レルムを表示してから、[コピー] 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、設定内容が示されます。
- 既存の SIP レルムを更新するには、P.16-4 の「SIP レルムの検索」の説明に従い、適切な SIP 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 16-3 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] ボタンまたはアイコンをクリックします。

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 Communications Manager で設定した内容と SIP ユーザエージェントで設定した内容が同じであることを確認します。

追加情報

詳細については、P.16-7 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 Communications Manager がトランク ピアによるチャレンジを受ける場合は、SIP レルムがトランク側のクレデンシャルを提供します。

表 16-3 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.16-7 の「関連項目」を参照してください。

表 16-3 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 Communications Manager サーバ名を入力します。SIP トランクはこのユーザ名を使用して、この Cisco Unified Communications Manager でチャレンジを実行します。
[ダイジェスト信用証明書 (Digest Credentials)]	このレルムとユーザに対するチャレンジに応答するために Cisco Unified Communications Manager が使用するパスワードを入力します。
[ダイジェスト信用証明書の確認 (Confirm Digest Credentials)]	確認のためパスワードを再入力します。

SIP レルムの削除

ここでは、Cisco Unified Communications Manager データベースから SIP レルムを削除する方法について説明します。

手順

-
- ステップ 1** P.16-4 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。
- ステップ 2** 複数の SIP レルムを削除するには、検索と一覧表示ウィンドウで、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 3** 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。
- 検索と一覧表示ウィンドウで、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]** アイコンまたはボタンをクリックします。
 - [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、**[削除]** アイコンまたは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.16-7 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 \(P.1-20\)](#)
- [SIP トランク ダイジェスト認証の設定用チェックリスト \(P.16-2\)](#)
- [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 \(P.16-2\)](#)
- [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 \(P.16-3\)](#)
- [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 \(P.16-3\)](#)
- [SIP レルムの検索 \(P.16-4\)](#)
- [SIP レルムの設定 \(P.16-5\)](#)
- [SIP レルムの設定内容 \(P.16-6\)](#)
- [SIP レルムの削除 \(P.16-7\)](#)



INDEX

C

Certificate Authority Proxy Function (CAPF)

- CAPF サービス 3-5
- CAPF レポートの生成 6-11
- Cisco Unified IP Phone との相互作用 6-3
- Cisco Unified Serviceability での設定 6-4
- CTI/JTAPI/TAPI アプリケーションでの
 - 概要 12-5
 - サービス パラメータの更新 12-11
 - 相互作用および要件 12-6
- 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 12-12
 - 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 12-16
 - 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 12-13
- インストール 1-14
- 概要 6-2
- サービス パラメータの更新 6-7
- サービスのアクティブ化 6-6, 12-10
- 設定内容 (表)
 - CTI/JTAPI/TAPI アプリケーションの 12-14
 - 電話機の 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
 - 認証文字列
 - 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 12-18
 - ~を使用した電話機証明書の操作 6-8
- Cisco Unified IP Phone
 - CAPF との相互作用 6-3
 - CTL ファイルの削除 3-22
 - 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 9-1
- 暗号化された設定ファイル 7-2
- セキュアな会議のサポート 10-7
- セキュリティ アイコン 1-7
- 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) 4-3
- 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 3-5
 - CTL Provider サービス 3-5
 - IP Phone 上の CTL ファイルの削除 3-22
 - Smart Card サービスの設定 3-20
 - アンインストール 3-23
 - インストール 1-14, 3-8
 - 概要 3-2
 - 確認 3-23
 - クラスタのセキュリティ モード更新 3-15
 - セキュリティ トークン
 - CTL クライアント 3-10
 - パスワードの変更 3-21
 - セキュリティ モード確認 3-19
 - 設定
 - CTL クライアント 3-10
 - TLS ポート 3-6
 - 設定内容 (表) 3-16
 - 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 3-23

CTL ファイル

- IP Phone での削除 3-22
- エントリの削除 3-14
- 更新 3-13

E

etoken

- CTL クライアント 3-10
- パスワードの変更 3-21

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

IPSec

- IPSec の設定用チェックリスト (表) 14-5
- インフラストラクチャの注意事項 14-6
- ゲートウェイまたはトランクの注意事項 14-6
- 推奨事項 14-6
- 設定 14-6

J

JTAPI

- セキュリティ サービス パラメータの設定 12-17
- セキュリティの設定用チェックリスト (表) 12-7

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) 14-5
- 設定 14-6

S

Secure Sockets Layer (SSL)

- HTTPS による 2-2
- インストール 1-14

Site Administrator Security Token (SAST) 3-2

SRST

- セキュリティの概要 13-1
- セキュリティの設定のヒント 13-2
- セキュリティの設定用チェックリスト (表) 13-3

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 13-7

SRST リファレンス

- セキュリティの設定内容 (表) 13-6
- 設定 13-4
- 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 13-7

T

TAPI

- セキュリティ サービス パラメータの設定 12-17
- セキュリティの設定用チェックリスト (表) 12-7

Tftp サービス 3-2

TLS Proxy サーバ 3-2

Transport Layer Security (TLS)

- ポート 3-6

あ

暗号化

- CTI/JTAPI/TAPI アプリケーションでの 12-4
- H.323 ゲートウェイ 14-3
- H.323/H.225/H.245 トランク 14-3
- MGCP ゲートウェイの 14-2
- SIP トランクの 14-4
- SRTP を許可 (SRTP Allowed) チェックボックスの設定 14-7
- インストール 1-14
- 概要 1-23
- ゲートウェイとトランクの設定用チェックリスト (表) 14-5
- シグナリング
 - SIP トランクの設定 15-4

- 電話機用の設定 5-4
- 制限 1-8, 1-9, 10-9
- 設定と割り込み 1-14
- 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 15-5
- 相互作用 1-8, 10-9
- 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
 - 概要 1-18
- か
- 会議ブリッジ
 - 会議リスト 10-5
 - セキュアな会議ブリッジでのパケット キャプチャの設定 10-14
 - セキュリティ 10-2
 - セキュリティ アイコン 10-4
 - セキュリティ制限 10-9
 - セキュリティの設定 10-13
 - セキュリティの設定のヒント 10-11
 - セキュリティの設定用チェックリスト (表) 10-12
 - セキュリティの相互作用 10-9
 - セキュリティ要件 10-3
- ミートミーの最小セキュリティ レベル 10-5
- ミートミーの最小セキュリティの設定 10-14
- き
- 許可
 - SIP トランクの設定 15-4
 - 概要 1-18
 - 設定内容 (表)
 - SIP トランクの 15-5
 - 相互作用 1-8
- 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 12-9
 - セキュリティの設定用チェックリスト (表) 12-7
- し
- シグナリング暗号化
 - 概要 1-23
- シグナリング認証
 - 概要 1-18
- 証明書
 - Internet Explorer の証明書 2-3
 - Netscape の証明書 2-6
 - 外部 CA 1-15
 - 種類 1-15
 - 証明書署名要求 (CSR) 1-15
- せ
- 整合性
 - 概要 1-18
- セキュアな会議
 - Cisco Unified IP Phone のサポート 10-7
 - CTI サポート 10-8
 - 会議ブリッジの要件 10-3
 - 会議リスト 10-5
 - 制限 10-9
 - セキュアな会議ブリッジの設定 10-13

- セキュリティ アイコン 10-4
- セキュリティの概要 10-2
- 設定のヒント 10-11
- 設定用チェックリスト (表) 10-12
- 相互作用 10-9
- トランクおよびゲートウェイ 10-8
- パケット キャプチャの設定 10-14
- ミートミーの最小セキュリティ レベル 10-5
- ミートミーの最小セキュリティの設定 10-14
- セキュリティ
 - Cisco Unified Communications Manager サービスの再起動 1-13
 - CTL クライアントの概要 3-2
 - HTTPS 2-2
 - SCCP コール (表) 1-6
 - SIP コール (表) 1-6
 - 暗号化に対する割り込みの使用 1-14
 - 暗号化の概要 1-23
 - インストール 1-14
 - 外部 CA 1-15
 - 機能一覧 1-6
 - 許可の概要 1-18
 - クラスタのリポート 1-13
 - サーバのリポート 1-13
 - システム要件 1-5
 - 証明書の種類 1-15
 - 制限 1-8, 1-9, 10-9
 - 相互作用 1-8, 10-9
 - その他の情報 1-29
 - デバイスのリセット 1-13
 - トークン 3-2, 3-8, 3-10, 3-13, 3-21
 - 認証および暗号化の設定用チェックリスト (表) 1-26
 - 認証の概要 1-18
 - ベスト プラクティス 1-13
 - 用語 (表) 1-2
- セキュリティ トークン
 - CTL クライアント 3-10
- セキュリティ プロファイル
 - SIP トランクの概要 15-2
 - SIP トランクの検索 15-3
 - SIP トランクの設定 15-4
 - SIP トランク用の削除 15-11
 - SIP トランク用の適用 15-10
 - 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 15-5
 - 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
 - 確認 3-19
 - 設定 3-15
 - 設定ファイル
 - 暗号化 1-23
- た
 - ダイジェスト認証
 - SIP トランクの設定 15-4
 - SIP レルムの検索 16-4
 - SIP レルムの削除 16-7
 - SIP レルムの設定 16-5
 - 概要 1-18
 - クラスタ ID 16-2
 - 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 15-5
 - SIP レルムの 16-6
 - 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 16-3
 - エンド ユーザの 8-4
 - 設定用チェックリスト (表)
 - SIP トランクの 16-2
 - 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 16-3
 - 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
 - SIP トランクの設定 15-4

- 概要 1-18
- 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 15-5
- 電話機用の設定 5-4
- 転送セキュリティ
 - SIP 電話機用の設定 5-4
 - SIP トランクの設定 15-4
 - 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 15-5
- 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 9-1
 - 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 3-22
 - ゲートウェイから削除された SRST 証明書 13-7
- に
- 認証
 - CTI/JTAPI/TAPI アプリケーションでの 12-2
 - 概要 1-18
 - 制限 1-8, 1-9
 - 相互作用 1-8
 - ダイジェスト 1-18
 - デバイス 1-18
- 認証文字列
 - CAPF による 6-2
 - CTI/JTAPI/TAPI アプリケーションでの 12-5
 - 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
 - 概要 1-18
 - 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 11-1
 - セキュリティの設定用チェックリスト (表) 11-3
 - セキュリティ要件 11-1
- 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 11-5
 - セキュリティ プロファイルの適用 11-4
 - セキュリティの概要 11-1
 - セキュリティの設定用チェックリスト (表) 11-3
- ポート
 - CTL Provider 3-6
 - Ethernet Phone 3-6
 - SIP セキュア 3-6
- め
- メディア暗号化 (「暗号化」も参照)
 - 概要 1-23
- 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 12-5
 - ~を使用した電話機の検索 6-10
- わ
- 割り込み
 - 暗号化制限と 1-14
 - セキュリティ 10-2
 - セキュリティ アイコン 10-4