Cisco CallManager セキュリティ ガイド

Release 5.0(1)

Text Part Number: OL-8356-01-J

CONTENTS

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

『*Cisco CallManager セキュリティ ガイド*』は、システム管理者および電話機管理者が次の作業を実行する際に役立ちます。

- 認証を設定する。
- 暗号化を設定する。
- ダイジェスト認証を設定する。
- HTTPS に関連付けられているサーバ認証証明書をインストールする。
- セキュリティ プロファイルを設定する。
- サポートされている Cisco IP Phone モデルのローカルで有効な証明書をインストール、アップグレード、または削除できるように Certificate Authority Proxy Function（CAPF）を設定する。
- 電話機のセキュリティを強化する。
- Survivable Remote Site Telephony（SRST）リファレンスについてセキュリティを設定する。
- ゲートウェイおよびトランクについてセキュリティを設定する。
- 問題をトラブルシュートする。

対象読者

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

マニュアルの構成

表 1 は、このマニュアルの構成を示しています。

表 1　　このマニュアルの構成

章番号	説明
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、相互対話と制限、インストール要件、および設定用チェックリストの概要を説明します。また、さまざまなタイプの認証と暗号化についても説明します。
第 2 章「HTTP over SSL（HTTPS）の使用方法」	HTTPS の概要を説明します。また、信頼できるフォルダにサーバ認証証明書をインストールする方法も説明します。
第 3 章「Cisco CTL クライアントの設定」	Cisco CTL クライアントをインストールおよび設定することにより認証を設定する方法を説明します。
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 CallManager および電話機でのセキュリティの使用方法について説明し、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 CallManager Administration 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ト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 CallManager Administration 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 CallManager Administration を使用してダイジェスト認証を SIP 電話機に設定する方法を説明します。
第 9 章「電話機のセキュリティ強化」	Cisco CallManager Administration を使用して電話機のセキュリティを強化する方法を説明します。
第 10 章「ボイス メッセージング ポートのセキュリティ設定」	Cisco CallManager Administration でボイスメール ポートのセキュリティを設定する方法を説明します。
CTI、JTAPI、および TAPI のセキュリティ	
第 11 章「CTI、JTAPI、および TAPI の認証および暗号化の設定」	Cisco CallManager Administration 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。
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 12 章「Survivable Remote Site Telephony（SRST）リファレンスのセキュリティ設定」	Cisco CallManager Administration で SRST リファレンスについてセキュリティを設定する方法を説明します。
第 13 章「ゲートウェイおよびトランクの暗号化の設定」	Cisco CallManager がセキュアなゲートウェイまたはトランクと通信する方法、および IPSec に関する推奨事項と考慮事項について説明します。

表 1　このマニュアルの構成（続き）

章番号	説明
第 14 章「SIP トランク セキュリティ プロファイルの設定」	Cisco CallManager Administration で SIP トランクのセキュリティ プロファイルを設定し、適用する方法を説明します。
第 15 章「SIP トランクのダイジェスト認証の設定」	Cisco CallManager Administration 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。
セキュリティのトラブルシューティング	
第 16 章「トラブルシューティング」	セキュリティ関連の操作および問題について、一般的なガイドラインを示します。

関連マニュアル

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

- *Cisco IP Phone アドミニストレーション ガイド for Cisco CallManager*
- *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*
- *Cisco CallManager 5.0 Integration Guide for Cisco Unity 4.x*
- SRST 対応ゲートウェイをサポートしている Cisco 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

シスコの製品マニュアルやその他の資料は、Cisco.com でご利用いただけます。また、テクニカルサポートおよびその他のリソースを、さまざまな方法で入手することができます。ここでは、シスコ製品に関する技術情報を入手する方法について説明します。

Cisco.com

次の URL から、シスコ製品の最新資料を入手することができます。

http://www.cisco.com/techsupport

シスコの Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com

シスコの Web サイトの各国語版には、次の URL からアクセスできます。

http://www.cisco.com/public/countries_languages.shtml

シスコ製品の最新資料の日本語版は、次の URL からアクセスしてください。

http://www.cisco.com/jp

Product Documentation DVD（英語版）

シスコ製品のマニュアルおよびその他の資料は、製品に付属の Product Documentation DVD パッケージでご利用いただけます。Product Documentation DVD は定期的に更新されるので、印刷資料よりも新しい情報が得られます。

Product Documentation DVD は、技術情報を包含する製品マニュアルをポータブルなメディアに格納した、包括的なライブラリです。この DVD を使用することにより、シスコ製の各ハードウェアやソフトウェアのインストール、コンフィギュレーション、およびコマンドに関する複数のバージョンのマニュアルにアクセスし、技術情報を HTML で参照できます。また、この DVD を使用すると、シスコの Web サイトで参照できるのと同じマニュアルに、インターネットに接続せずにアクセスできます。一部の製品については、PDF 版のマニュアルもご利用いただけます。

Product Documentation DVD は、1 回単位で入手することも、または定期購読することもできます。Cisco.com 登録ユーザ（Cisco Direct Customers）の場合、Cisco Marketplace から Cisco Documentation DVD（Product Number DOC-DOCDVD=）を発注できます。

http://www.cisco.com/go/marketplace/

マニュアルの発注方法（英語版）

2005 年 6 月 30 日以降、Cisco.com 登録ユーザの場合、Cisco Marketplace の Product Documentation Store からシスコ製品の英文マニュアルを発注できるようになっています。次の URL にアクセスしてください。

http://www.cisco.com/go/marketplace/

Cisco.com に登録されていない場合、製品を購入された代理店へお問い合せください。

シスコシステムズマニュアルセンター

シスコシステムズマニュアルセンターでは、シスコ製品の日本語マニュアルの最新版を PDF 形式で公開しています。また、日本語マニュアル、および日本語マニュアル CD-ROM もオンラインで発注可能です。ご希望の方は、次の URL にアクセスしてください。

http://www2.hipri.com/cisco/

また、シスコシステムズマニュアルセンターでは、日本語マニュアル中の誤記、誤植に関するコメントをお受けしています。次の URL の「製品マニュアル内容不良報告」をクリックすると、コメント入力画面が表示されます。

http://www2.hipri.com/cisco/

なお、技術内容に関するお問い合せは、この Web サイトではお受けできませんので、製品を購入された各代理店へお問い合せください。

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、http://www.cisco.com/wwl/export/crypto/tool/stqrg.html で参照できます。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。

シスコでは、オンラインの Security Vulnerability Policy ポータル（英文のみ）を無料で提供しています。URL は次のとおりです。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このサイトは、次の目的に利用できます。

- シスコ製品のセキュリティ脆弱性を報告する。
- シスコ製品に伴うセキュリティ事象についてサポートを受ける。
- シスコからセキュリティ情報を受け取るための登録をする。

シスコ製品に関するセキュリティ勧告および注意事項の最新のリストには、次の URL からアクセスできます。

http://www.cisco.com/go/psirt

勧告および注意事項がアップデートされた時点でリアルタイムに確認する場合は、次の URL から Product Security Incident Response Team Really Simple Syndication（PSIRT RSS）フィードにアクセスしてください。

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

シスコ製品のセキュリティ問題の報告

シスコでは、セキュアな製品を提供すべく全力を尽くしています。製品のリリース前には内部でテストを行い、すべての脆弱性を早急に修正するよう努力しています。万一、シスコ製品に脆弱性が見つかった場合は、PSIRT にご連絡ください。

- 緊急の場合：security-alert@cisco.com（英語のみ）

  緊急とは、システムがアクティブな攻撃を受けている場合、または至急の対応を要する重大なセキュリティ上の脆弱性が報告されている場合を指します。これに該当しない場合はすべて、緊急でないと見なされます。
- 緊急でない場合：psirt@cisco.com（英語のみ）

緊急の場合は、電話で PSIRT に連絡することもできます。

- 1 877 228-7302（英語のみ）
- 1 408 525-6532（英語のみ）

ヒント シスコに機密情報をお送りいただく際には、PGP（Pretty Good Privacy）または互換製品を使用して、暗号化することをお勧めします。PSIRT は、PGP バージョン 2.*x* から 8.*x* と互換性のある暗号化情報に対応しています。

無効になった、または有効期限が切れた暗号鍵は、絶対に使用しないでください。PSIRT に連絡する際に使用する正しい公開鍵には、Security Vulnerability Policy ページの Contact Summary セクションからリンクできます。次の URL にアクセスしてください。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このページ上のリンクからは、現在使用されている最新の PGP 鍵の ID にアクセスできます。

テクニカル サポート

Cisco Technical Support では、24 時間テクニカル サポートを提供しています。Cisco.com の Cisco Technical Support & Documentation Web サイトでは、多数のサポート リソースをオンラインで提供しています。また、シスコと正式なサービス契約を交わしているお客様には、Cisco Technical Assistance Center（TAC）のエンジニアが電話でのサポートにも対応します。シスコと正式なサービス契約を交わしていない場合は、代理店にお問い合せください。

Cisco Technical Support & Documentation Web サイト

Cisco Technical Support & Documentation Web サイトでは、シスコ製品やシスコの技術に関するトラブルシューティングにお役立ていただけるように、オンラインでマニュアルやツールを提供しています。この Web サイトは、24 時間、いつでも利用可能です。URL は次のとおりです。

http://www.cisco.com/techsupport

Cisco Technical Support & Documentation Web サイトのツールにアクセスするには、Cisco.com のユーザ ID とパスワードが必要です。サービス契約が有効で、ユーザ ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://tools.cisco.com/RPF/register/register.do

（注） Web または電話でサービス リクエストを発行する前に、Cisco Product Identification（CPI）ツールを使用して製品のシリアル番号を確認してください。CPI ツールには、Cisco Technical Support & Documentation Web サイトから、Documentation & Tools の下の **Tools & Resources** リンクをクリックするとアクセスできます。アルファベット順の索引ドロップダウン リストから **Cisco Product Identification Tool** を選択するか、Alerts & RMAs の下の **Cisco Product Identification Tool** リンクをクリックします。CPI ツールには、3 つの検索オプションがあります。製品 ID またはモデル名による検索、ツリー表示による検索、**show** コマンド出力のコピー アンド ペーストによる特定製品の検索です。検索結果では、製品が図示され、シリアル番号ラベルの位置が強調表示されます。ご使用の製品でシリアル番号ラベルを確認し、その情報を記録してからサービス コールをかけてください。

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト（http://www.cisco.com/tac）のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://www.cisco.com/jp/register

サービス リクエストの発行

オンラインの TAC Service Request Tool を使用すると、S3 と S4 のサービス リクエストを短時間でオープンできます（S3：ネットワークに軽微な障害が発生した、S4：製品情報が必要である）。状況を入力すると、その状況を解決するための推奨手段が検索されます。これらの推奨手段で問題を解決できない場合は、シスコのエンジニアが対応します。TAC Service Request Tool には、次の URL からアクセスできます。

http://www.cisco.com/techsupport/servicerequest

S1 または S2 のサービス リクエストの場合、またはインターネットにアクセスできない場合は、Cisco TAC に電話でお問い合せください（S1：ネットワークがダウンした、S2：ネットワークの機能が著しく低下した）。S1 および S2 のサービス リクエストには、シスコのエンジニアがすぐに割り当てられ、業務を円滑に継続できるようサポートします。

Cisco TAC の連絡先については、次の URL を参照してください。

http://www.cisco.com/techsupport/contacts

サービス リクエストのシビラティの定義

シスコでは、報告されるサービス リクエストを標準化するために、シビラティを定義しています。

シビラティ 1（S1）：ネットワークが「ダウン」した状態か、業務に致命的な損害が発生した場合。お客様およびシスコが、24 時間体制でこの問題を解決する必要があると判断した場合。

シビラティ 2（S2）：既存のネットワーク動作が著しく低下したか、シスコ製品が十分に機能しないため、業務に重大な影響を及ぼした場合。お客様およびシスコが、通常の業務中の全時間を費やして、この問題を解決する必要があると判断した場合。

シビラティ 3（S3）：ネットワークの動作パフォーマンスが低下しているが、ほとんどの業務運用は継続できる場合。お客様およびシスコが、業務時間中にサービスを十分なレベルにまで復旧させる必要があると判断した場合。

シビラティ 4（S4）：シスコ製品の機能、インストレーション、コンフィギュレーションについて、情報または支援が必要な場合。業務の運用には、ほとんど影響がありません。

その他の資料および情報の入手方法

シスコの製品、テクノロジー、およびネットワーク ソリューションに関する情報について、さまざまな資料をオンラインおよび印刷物で入手できます。

- Cisco Marketplace では、シスコの書籍やリファレンス ガイド、マニュアル、ロゴ製品を数多く提供しています。購入を希望される場合は、次の URL にアクセスしてください。

  http://www.cisco.com/go/marketplace/

- Cisco Press では、ネットワーキング全般、トレーニング、および認定資格に関する書籍を広範囲にわたって出版しています。これらの出版物は、初級者にも上級者にも役立ちます。Cisco Press の最新の出版情報やその他の情報を調べるには、次の URL からアクセスしてください。

  http://www.ciscopress.com

- 『*Packet*』はシスコシステムズが発行する技術者向けの雑誌で、インターネットやネットワークへの投資を最大限に活用するために役立ちます。本誌は季刊誌として発行され、業界の最先端トレンド、最新テクノロジー、シスコ製品やソリューション情報が記載されています。また、ネットワーク構成およびトラブルシューティングに関するヒント、コンフィギュレーション例、カスタマー ケース スタディ、認定情報とトレーニング情報、および充実したオンラインサービスへのリンクの内容が含まれます。『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/packet

  日本語版『*Packet*』は、米国版『*Packet*』と日本版のオリジナル記事で構成されています。日本語版『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/japanese/warp/public/3/jp/news/packet/

- 『*iQ Magazine*』はシスコシステムズの季刊誌で、成長企業が収益を上げ、業務を効率化し、サービスを拡大するためには技術をどのように利用したらよいかを学べるように構成されています。本誌では、実例とビジネス戦略を挙げて、成長企業が直面する問題とそれを解決するための技術を紹介し、読者が技術への投資に関して適切な決定を下せるよう配慮しています。『*iQ Magazine*』には、次の URL からアクセスしてください。

  http://www.cisco.com/go/iqmagazine

  デジタル版には、次の URL からアクセスできます。

  http://ciscoiq.texterity.com/ciscoiq/sample/

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『*Internet Protocol Journal*』には、次の URL からアクセスしてください。

  http://www.cisco.com/ipj

- シスコシステムズが提供するネットワーキング製品、および各種のカスタマー サポート サービスは、次の URL から入手できます。

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection は対話形式の Web サイトです。このサイトでは、ネットワーキング製品やテクノロジーに関する質問、提案、および情報をネットワーキング担当者がシスコの専門家や他のネットワーキング担当者と共有できます。次の URL にアクセスしてディスカッションに参加してください。

  http://www.cisco.com/discuss/networking

- シスコは、国際的なレベルのネットワーク関連トレーニングを実施しています。最新情報については、次の URL からアクセスしてください。

  http://www.cisco.com/en/US/learning/index.html

PART 1

セキュリティの基礎

セキュリティの概要

Cisco CallManager システムにセキュリティ機構を実装すると、電話機や Cisco CallManager サーバの ID 盗難、データ改ざん、コール シグナリングやメディア ストリームの改ざんを防止することができます。Cisco IP テレフォニー ネットワークは、以下の処理を行います。

- 認証された通信ストリームの確立と維持
- 電話機にファイルを転送する前の、ファイルへのデジタル署名
- Cisco 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

この章は、次の内容で構成されています。

認証および暗号化に関する用語

表 1-1 に示す定義は、Cisco IP テレフォニー ネットワークで認証および暗号化を設定する場合に適用されます。

表 1-1　用語

用語	定義
アクセス コントロール リスト（ACL）	システムの機能およびリソースにアクセスするためのアクセス権を定義するリスト。メソッド リストを参照。
認証	エンティティの ID を検証するプロセス。
許可	認証されたユーザ、サービス、またはアプリケーションに、要求されたアクションの実行に必要なアクセス権があるかどうかを指定すること。Cisco CallManager では、SUBSCRIBE 要求および一部のトランク側 SIP 要求を許可されたユーザに制限するセキュリティ プロセス。
許可ヘッダー	チャレンジに対する SIP ユーザ エージェントの応答。
Certificate Authority （CA; 認証局）	証明書を発行するエンティティ。シスコまたはサードパーティのエンティティなど。
Certificate Authority Proxy Function（CAPF）	サポートされたデバイスが Cisco CallManager Administration 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）	Cisco CTL クライアントをインストールし、設定した後で自動的に作成され、電話機で使用されるファイル。Cisco Site Administrator Security Token（セキュリティ トークン）が署名した信頼される項目の事前定義済みのリストが含まれ、サーバおよびセキュリティ トークンの証明書を検証するための認証情報を提供します。CTL 署名済み証明書のリスト。
チャレンジ	認証のダイジェストで、有効な秘密鍵とその他のセキュア データを SIP ユーザ エージェントに提供することで、ID を認証するように要求します。
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 ファイルへの署名および証明書の秘密鍵取得を行います。
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	SIP 電話機およびトランクが使用。Cisco CallManager が 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るプロセス。
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。SIP ソースまたはアプリケーション ユーザを識別するプロセス。
暗号化	対象とする受信者だけが確実にデータを受信し読み取るようにするプロセス。情報の機密を確保し、データをランダムで無意味な暗号文に変換するプロセスです。暗号化アルゴリズムと暗号鍵が必要です。
ファイル認証	電話機でダウンロードするデジタル署名されたファイルを検証するプロセス。電話機は署名を検証して、ファイルが作成後に改ざんされていないことを確認します。
Hypertext Transfer Protocol over Secure Sockets Layer（HTTPS; HTTP over SSL）	HTTPS サーバの ID を（少なくとも）保証する IETF が定義したプロトコル。暗号化を使用して、tomcat サーバとブラウザ クライアントとの間で交換される情報の機密を確保します。

表 1-1　用語（続き）

用語	定義
イメージ認証	電話機でロードする前にバイナリ イメージの改ざんを防止するプロセス。このプロセスによって電話機はイメージの整合性および発信元を検証します。
整合性	エンティティ間でデータの改ざんが行われていないことを確認するプロセス。
IPSec	エンドツーエンド セキュリティ用に、セキュアな H.225、H.245、RAS シグナリング チャネルを提供します。
Locally Significant Certificate （LSC; ローカルで有効な証明書）	電話機または JTAPI/TAPI/CTI アプリケーションにインストールされているデジタル X.509v3 証明書。発行元は、サードパーティの認証局または CAPF です。
Manufacture Installed Certificate （MIC; 製造元でインストールされる証明書）	Cisco Certificate Authority によって署名され、サポートされている電話機にシスコの製造過程でインストールされた X.509v3 デジタル証明書。
Man-in-the-Middle （中間者）攻撃	Cisco CallManager 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。
メディア暗号化	暗号化手順を使用してメディアの機密を保持するプロセス。メディア暗号化では、IETF RFC 3711 で定義された Secure Real Time Protocol（SRTP）を使用します。
メッセージ / データ改ざん	攻撃者が、転送中のメッセージを変更しようとするイベント。コールの途中終了も含まれます。
メソッド リスト	許可プロセス中に、SIP トランクに着信する一定のカテゴリのメッセージを制限するツール。トランク側アプリケーションまたはデバイスに対して SIP nonINVITE 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。
セキュア モード	セキュリティを設定したクラスタ内のモード。Cisco CallManager に接続する認証済みデバイスおよび非認証デバイスが含まれます。
ナンス	各ダイジェスト認証要求に対してサーバが生成する一意のランダム数値。
ノンセキュア 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。
応答攻撃	攻撃者が、電話機または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する情報で応答するイベント。たとえば、プロキシ サーバの秘密鍵を偽装します。
System Administrator Security Token（SAST）	CTI/JTAPI/TAPI アプリケーションでは、CTL ダウンロード用の CTL ファイルへの署名に使用するトークン。
Simple Certificate Enrollment Protocol（SCEP）	CAPF 機能を使用して証明書を生成するために、Microsoft Certificate Services Manager が使用するアドオン。
セキュア コール	すべてのデバイスが認証され、メディア ストリームが暗号化されているコール。
シグナリング認証	転送中のシグナリング パケットが改ざんされていないことを検証するプロセス。Transport Layer Security プロトコルを使用します。
シグナリング暗号化	デバイスと Cisco CallManager サーバの間で送信されるすべてのシグナリング メッセージの機密保持を行うために、暗号化手法を使用するプロセス。

表 1-1　用語（続き）

用語	定義
SIP レルム	ダイジェスト認証で保護される空間を指定する文字列（名前）。SIP 要求用の回線またはトランク側のユーザ エージェントを識別します。
SSL	転送セキュリティ用の TLS インフラストラクチャの一部。
Transport Layer Security（TLS）	IETF を定義するセキュリティ プロトコル。整合性、認証、および暗号化を提供し、IP 通信スタック内の TCP 層に存在します。
信頼リスト	デジタル署名なしの証明書リスト。
信頼ストア	信頼された証明書のリストが含まれています。また、Cisco CallManager、CA、CAPF、ルート、およびピア証明書の公開鍵が信頼ストアに保管されます。
X.509	デジタル ユーザおよび CA 証明書をインポートするためのバイナリ形式。

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 CallManager 5.0(1) は、最小要件として機能します。
- クラスタのサーバごとに、異なる Administrator パスワードを使用できます。
- Cisco CTLclient で（Cisco CallManager サーバにログインするために）使用されるユーザ名とパスワードは、Cisco CallManager Administration ユーザ名およびパスワード（Cisco CallManager Administration にログインするために使用するユーザ名とパスワード）と同じです。
- Certificate Authority Proxy Function（CAPF）については、P.6-4 の「CAPF システムの対話および要件」を参照してください。
- ボイスメール ポートのセキュリティを設定する前に、Cisco CallManager 5.0 をサポートする Cisco Unity のバージョンがインストールされていることを確認します。

機能一覧

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

トランスポート層セキュリティには、音声ドメインへのアクセスを制御および防止するためにシグナリングの認証と暗号化を行う TLS および IPSec が含まれます。SRTP は、メディア認証および暗号化をセキュア プライバシーに追加し、音声会話およびその他のメディアに機密性を追加します。Cisco CallManager システムで導出されたメディア暗号鍵は、暗号化されたシグナリング パス経由で、TLS（または、一部の電話機モデルでは TCP）を通じて Cisco IP Phone に、または IPSec で保護されたリンクを通じてゲートウェイに、安全に送出されます。

表 1-2 に、サポートおよび設定されている機能に応じて SIP または SCCP コール中に Cisco CallManager が実装できるセキュリティ機能の概要を示します。

表 1-2　コール処理セキュリティ機能の一覧

セキュリティ機能	回線側	トランク側
転送 / 接続 / 整合性	セキュア TLS ポート	IPSec アソシエーション セキュア TLS ポート（SIP トランクのみ）
デバイス認証	CAPF との TLS 証明書交換	IPSec 証明書交換、または事前共有鍵
ダイジェスト認証	SIP 電話機ユーザのみ	SIP トランク ユーザまたは SIP トランク アプリケーション ユーザのみ
シグナリング認証 / 暗号化	TLS モード：認証または暗号化	IPSec［認証ヘッダー、暗号化（ESP）、または両方］ TLS モード：認証または暗号化モード（SIP トランクのみ）
メディア暗号化	SRTP	SRTP
許可	プレゼンス SUBSCRIBE 要求	プレゼンス SUBSCRIBE 要求 メソッド リスト
注：デバイスがサポートする機能は、デバイス タイプおよびプロトコルによって異なります。		

セキュリティ アイコン

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

- シグナリング セキュリティ レベルが「認証」のコールに対しては、シールド アイコンが表示されます。シールドは、Cisco IP デバイス間のセキュアな接続を示します。
- 暗号化されたメディアのコールに対しては、ロック アイコンが表示されます。これは、Cisco IP デバイス間のメディア ストリームが暗号化されていることを意味します。

セキュリティ アイコンに関連付けられている制限については、P.1-9 の「電話機アイコンと暗号化」を参照してください。

対話および制限

この項では、次のトピックについて取り上げます。

対話

ここでは、シスコのセキュリティ機能が Cisco CallManager アプリケーションと対話する方法について説明します。

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 CallManager 機能およびサービス ガイド*』を参照してください。

SIP トランクでプレゼンス要求を許可するには、Cisco CallManager で SIP トランクのプレゼンス要求を受け付けるように許可する必要があります。また、必要な場合、Cisco CallManager がリモート デバイスおよびアプリケーションからの着信プレゼンス要求を受け付けて認証するように、Cisco CallManager Administration でエンド ユーザ クライアントを設定します。

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 CallManager で着信 Out of Dialog REFER 要求を受け付けるように許可する必要があります。

イベント レポートをサポートし（MWI サポートなど）、1 コールあたりの MTP 割り当て（ボイス メッセージング サーバからなど）を削減するには、Cisco CallManager で Unsolicited Notification SIP 要求を受け付けるように許可する必要があります。

Cisco CallManager が、SIP トランクの外部コールを外部デバイスまたはパーティに転送できるようにするには（有人転送など）、Cisco CallManager で REFER および INVITE の置換ヘッダー付き SIP 要求を受け付けるように許可する必要があります。

エクステンション モビリティでは、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。

Cisco IPMA は、CTI（トランスポート層セキュリティ接続）へのセキュア接続をサポートします。管理者は、CAPF プロファイルを設定する必要があります（IPMA ノードごとに 1 つ）。

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

デバイス セキュリティ モードが認証済みまたは暗号化済みになっている場合、Cisco Unity-CM TSP は Cisco CallManager TLS ポートを介して Cisco CallManager に接続します。セキュリティ モードがノンセキュアになっている場合、Cisco Unity TSP は Cisco CallManager ポートを介して Cisco CallManager に接続します。

制限

次の項で、シスコのセキュリティ機能に適用される制限について説明します。

認証と暗号化

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

- クラスタをデバイス認証に必要なセキュア モードに設定すると、自動登録機能は動作しません。
- デバイス認証がクラスタに存在しない場合、つまり CTL Provider サービスを有効にしていないか Cisco CTL クライアントをインストールして設定していない場合、シグナリング暗号化およびメディア暗号化を実装できません。
- クラスタをセキュア モードに設定した場合、Cisco CallManager による Network Address Translation（NAT; ネットワーク アドレス変換）はサポートされません。

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

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

  シグナリング暗号化では NAT トラバーサルをサポートしません。NAT を使用する代わりに、LAN 拡張 VPN の使用を検討してください。
- SRTP は、音声パケットのみを暗号化します。

割り込みと暗号化

割り込みと暗号化には、次の制限が適用されます。

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

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

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

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

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

- Cisco IP Phone モデル 7960 および モデルで暗号化機能を設定すると、設定された IP Phone が暗号化されたコールに参加する際に、割り込み要求を受け入れません。コールが暗号化されると、割り込みが失敗します。割り込みが失敗したことを示すトーンが電話機で再生されます。

  次の設定を試みると、Cisco CallManager Administration にメッセージが表示されます。

  - Phone Configuration ウィンドウで、暗号化をサポートするセキュリティ プロファイルを適用し、Built In Bridge 設定に **On** を選択し（デフォルト設定は On）、さらにこの特定の設定の作成後に **Save** をクリックする。
  - Service Parameter ウィンドウで、Builtin Bridge Enable パラメータを更新する。

ワイドバンド コーデックと暗号化

次の情報は、暗号化が設定されていて、ワイドバンドのコーデック リージョンに関連付けられた Cisco IP Phone 7960 モデルまたは 7940 モデルに適用されます。これは、TLS/SRTP 用に設定された Cisco IP Phone 7960 モデルまたは 7940 モデル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 CallManager はワイドバンド コーデックを無視して、サポートされる別のコーデックを電話機が提示するコーデック リストから選択します。コールのもう一方のデバイスで暗号化が設定されていない場合、Cisco CallManager はワイドバンド コーデックを使用して認証済みおよびノンセキュア コールを確立できます。

メディア リソースと暗号化

Cisco CallManager は、メディア リソースを使用しないセキュア Cisco IP Phone（SCCP または SIP）、セキュア CTI デバイス / ルート ポイント、セキュア Cisco MGCP IOS ゲートウェイ、セキュア SIP トランク、セキュア H.323 ゲートウェイ、およびセキュア H.323/H.245/H.225 トランク間で、認証および暗号化されたコールをサポートします。たとえば次の場合に、Cisco CallManager 5.0 はメディア暗号化を提供しません。

- トランスコーダまたはメディア終端点に関連するコール
- Ad hoc 会議または Meet Me 会議
- 保留音に関連するコール

デバイス サポートと暗号化

Cisco IP Phone 7912 モデルなど一部の電話機は、暗号化されたコールをサポートしません。別の電話機は、暗号化はサポートしますが、証明書の署名の検証はサポートしません。詳細については、使用している電話機モデルおよびこのバージョンの Cisco CallManager をサポートする Cisco IP Phone 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。

SIP トランクは SRTP 暗号化をサポートしません。Cisco CallManager は、SIP トランクおよび TLS とのセキュア コールで RTP 暗号化をサポートします。

（注）

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

暗号化された設定ファイルをサポートしない電話機もあります。また、暗号化された設定ファイルはサポートするが、署名の検証をサポートしない電話機もあります。暗号化された設定ファイルをサポートするすべての電話機は、完全に暗号化された設定ファイルを受信するために、このリリースと互換性のある新しいファームウェアを必要とします（Cisco IP Phone 7905 モデルおよび 7912 モデル以外）。Cisco IP Phone 7905 モデルおよび 7912 モデルは、既存のセキュリティ機構を使用し、この機能のために新しいファームウェアを必要としません。

暗号化された設定ファイルの電話機でのサポートについては、P.7-4 の「サポートされる電話機のモデル」を参照してください。

電話機アイコンと暗号化

暗号化のロック アイコンは、Cisco IP デバイス間のメディア ストリームが暗号化されていることを示します。

電話会議、コールの転送、保留などのタスクを実行するときに、暗号化ロック アイコンが電話機に表示されないことがあります。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ノンセキュアに変化します。

Cisco CallManager は、SIP トランク側接続で開始または終了するコールに対してはロック アイコンを表示しません。Cisco CallManager は、H.323 トランクで転送されるコールに対してはシールドアイコンを表示しません。

クラスタおよびデバイス セキュリティ モード

クラスタ セキュリティ モードがノンセキュアになっている場合は、Cisco CallManager Administration 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 モードはノンセキュアです。このような場合、電話機は、クラスタ内で SRST 対応ゲートウェイおよび Cisco CallManager サーバとのノンセキュア接続を試行します。

クラスタ セキュリティ モードがノン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 SRST Allowed チェックボックスなど、Cisco CallManager Administration 内のセキュリティ関連の設定が無視されます。Cisco CallManager Administration 内の設定は削除されませんが、セキュリティは提供されません。

電話機が SRST 対応ゲートウェイへのセキュア接続を試行するのは、クラスタ セキュリティ モードがセキュアで、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、Trunk Configuration ウィンドウで SRST 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。

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 CallManager Administration の設定を変更して、Cisco CallManager Administration でのパケットのキャプチャを開始できます（デバイスがパケット キャプチャをサポートする場合）。

ベスト プラクティス

シスコでは、次のベスト プラクティスを強く推奨します。

- 必ず安全なテスト環境でインストールおよび設定タスクを実行してから、広範囲のネットワークに展開する。
- ゲートウェイ、および Cisco Unity、Cisco IP Contact Center（IPCC）、またはその他の Cisco CallManager サーバなど、リモート ロケーションのその他のアプリケーション サーバには、IPSec を使用する。

注意　これらのインスタンスで IPSec を使用しない場合、セッション暗号鍵が暗号化されずに転送されます。

- 通話料金の不正を防止するため、『*Cisco CallManager システム ガイド*』に説明されている電話会議の機能拡張を設定する。同様に、コールの外部転送を制限する設定作業を実行することができます。この作業を実行する方法については、『*Cisco CallManager 機能およびサービス ガイド*』を参照してください。

デバイスのリセット、サービスの再起動、またはサーバおよびクラスタのリブート

ここでは、デバイスのリセットが必要な場合、Cisco CallManager Serviceability でサービスの再起動が必要な場合、またはサーバおよびクラスタをリブートする場合について説明します。

次のガイドラインを考慮します。

- Cisco CallManager Administration で、異なるセキュリティ プロファイルを適用した後は、単一デバイスをリセットする。
- 電話機のセキュリティ強化作業を実行した場合は、デバイスをリセットする。
- クラスタ全体のセキュリティ モードをセキュア モードからノンセキュア モード（またはその逆）に変更した後は、デバイスをリセットする。
- Cisco CTL クライアントの設定後、または CTL ファイルの更新後は、すべてのデバイスを再起動する。
- CAPF エンタープライズ パラメータを更新した後は、デバイスをリセットする。
- TLS 接続用のポートを更新した後は、Cisco CTL Provider サービスを再起動する。
- クラスタ全体のセキュリティ モードをセキュア モードからノンセキュア 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 CallManager Serviceability で Cisco CallManager および Cisco TFTP サービスをすべて再起動する。この作業は、これらのサービスが稼働するすべてのサーバで実行します。
- CTL Provider サービスを開始または停止した後は、すべての Cisco CallManager および Cisco TFTP サービスを再起動する。
- SRST リファレンスのセキュリティ設定後は、従属デバイスをリセットする。
- Smart Card サービスを Started および Automatic 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サーバをリブートする。
- 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（IPMA）サービス、Cisco WebDialer Web サービス、および Cisco Extended Functions サービスを再起動する。

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

設定の更新後に単一のデバイスをリセットするには、P.5-9 の「SCCP または SIP 電話機セキュリティ プロファイルの適用」を参照してください。

クラスタ内のデバイスをすべてリセットするには、次の手順を実行します。

手順

ステップ 1　Cisco CallManager Administration で **System > Cisco CallManager** の順に選択します。

Find/List ウィンドウが表示されます。

ステップ 2　**Find** をクリックします。

設定済みの Cisco CallManager サーバのリストが表示されます。

ステップ 3　デバイスをリセットする Cisco CallManager を選択します。

ステップ 4　**Reset** をクリックします。

ステップ 5　クラスタ内のサーバごとに、ステップ 2 とステップ 4 を実行します。

メディア暗号化の設定と割り込み

P.1-7 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 IP Phone 7960 モデルおよび 7940 モデル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 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 CallManager Administration で次の作業を実行したときです。

- Phone Configuration ウィンドウで、Device Security Mode に **Encrypted** を選択し（システム デフォルトは Encrypted）、Built In Bridge 設定に **On** を選択し（デフォルト設定は On）、さらにこの特定の設定の作成後に **Insert** または **Update** をクリックする。
- Enterprise Parameter ウィンドウで、Device Security Mode パラメータを更新する。
- Service Parameter ウィンドウで、Built In Bridge Enable パラメータを更新する。

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

インストール

認証のサポートを可能にするには、プラグインの Cisco CTL クライアントを Cisco CallManager Administration 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 CallManager のインストール時に、メディアおよびシグナリング暗号化機能が自動的にインストールされます。

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

Cisco Certificate Authority Proxy Function（CAPF）は、Cisco CallManager Administration の一部として自動的にインストールされます。

TLS と IPSec

転送セキュリティは、データの符号化、パッキング、送信を扱います。Cisco CallManager は、次のセキュア転送プロトコルを提供します。

- Transport Layer Security（TLS）は、セキュア ポートと証明書交換を使用して、2 つのシステムまたはデバイスの間で、セキュアで信頼性の高いデータ転送を提供します。TLS は、Cisco CallManager で制御されたシステム、デバイス、およびプロセス間の接続を保護および制御し、音声ドメインへのアクセスを防止します。Cisco CallManager は TLS を使用して、SCCP 電話機への SCCP コール、および SIP 電話機またはトランクへの SIP コールを保護します。
- IP Security（IPSec）は、Cisco CallManager とゲートウェイの間で、セキュアで信頼性の高いデータ転送を提供します。IPSec は、Cisco IOS MGCP および H.323 ゲートウェイへのシグナリング認証および暗号化を実装します。IPSec は、リアルタイム プロトコル（RTP）を使用してメッセージを認証し、実際のデータ ストリームを接続で転送します。

セキュア RTP（SRTP）をサポートするデバイスの次のレベルのセキュリティとして、TLS および IPSec 転送サービスに SRTP を追加できます。SRTP は、メディア ストリーム（音声パケット）を認証および暗号化して、Cisco IP Phone で発信または着信する音声会話および TDM またはアナログ音声ゲートウェイ ポートを音声ドメインにアクセスする盗聴者から保護します。SRTP は、応答攻撃からの保護を追加します。

証明書の種類

証明書は、クライアントとサーバの ID を保護します。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。特定の電話機モデルでは、MIC と Locally Significant Certificate （LSC; ローカルで有効な証明書）を 1 つずつ同じ電話機にインストールできます。その場合、デバイス セキュリティ モードで認証または暗号化を設定すると、Cisco CallManager に認証を受けるときに LSC が MIC より優先されます。

  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。特定の電話機モデルでは、LSC と MIC を 1 つずつ同じ電話機にインストールできます。その場合、デバイス セキュリティ モードで認証または暗号化を設定すると、Cisco CallManager に認証を受けるときに LSC が MIC より優先されます。

Certificate Management Tool は、電話機に格納されているこれらの証明書を管理しません。

Cisco CallManager サーバでは、次の種類の自己署名証明書を使用します。

- HTTPS 証明書（tomcat_cert）：この自己署名ルート証明書は、Cisco CallManager をインストールするときに、HTTPS サーバに対して生成されます。
- Cisco CallManager ノード証明書（ccmnode_cert）：この自己署名ルート証明書は、Cisco CallManager 5.0(1) をインストールすると、Cisco CallManager サーバに自動的にインストールされます。Cisco CallManager 証明書によって、サーバの識別情報が提供されます。この情報には、Cisco CallManager サーバ名と Global Unique Identifier（GUID）が含まれます。
- CAPF 証明書（CAPF_cert）：このルート証明書は、Cisco CTL クライアントの設定が完了した後で、クラスタ内のすべてのサーバにコピーされます。
- IPSec 証明書（ipsec_cert）：この自己署名ルート証明書は、Cisco CallManager 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 CallManager Administration のセキュア SRST 参照を設定するときに、Cisco CallManager は、ゲートウェイから SRST 対応ゲートウェイ証明書を取得し、Cisco CallManager データベースに格納します。デバイスをリセットすると、証明書は電話機設定ファイルに追加されます。この証明書はデータベースに格納されるため、証明書管理ツールには統合されません。

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、ユーザとホストとの間の接続を保護し、アプリケーション デバイスを統合します。セキュリティ上の理由により、信頼される証明書ファイルは通常、証明書名の c_rehash を表す 8 桁の数値として格納されます（f7a74b2c.0 など）。

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

- Cisco Unity サーバ証明書：Cisco Unity は、この自己署名証明書を使用して、Cisco Unity SCCP デバイス証明書に署名します。Cisco Unity Telephony Integration Manager がこの証明書を管理します。
- Cisco Unity SCCP デバイス証明書：Cisco Unity SCCP デバイスは、この署名証明書を使用して、Cisco CallManager との TLS 接続を確立します。すべての Unity デバイス（またはポート）が、Unity ルート証明書をルートとする証明書を発行します。Unity 証明書名は、Unity マシン名に基づく証明書の件名のハッシュです。
- SIP Proxy サーバ証明書：Cisco CallManager 信頼ストアに SIP ユーザ エージェント証明書が含まれ、SIP ユーザ エージェントの信頼ストアに Cisco CallManager 証明書が含まれている場合、SIP トランク経由で接続する SIP ユーザ エージェントは、Cisco CallManager に対して認証されます。

管理者には、証明書に対して読み取り専用のアクセス権があります。管理者は Cisco IPT Platform 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。

(注)　Cisco CallManager は、PEM（.pem）形式および DER（.der）形式の証明書のみサポートします。

Cisco CallManager 信頼ストアの更新、Certificate Signing Request（CSR）の生成、および証明書の管理の詳細については、『*Cisco IP Telephony Platform Administration Guide*』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 CallManager との間で行われるコール処理シグナリングの変更（認証）
- 表 1-1 で定義した Man-in-the-Middle（中間者）攻撃（認証）
- 電話機およびサーバの ID 盗難（認証）
- 応答攻撃（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.1-15）
- デバイス認証（P.1-15）
- ファイル認証（P.1-16）
- シグナリング認証（P.1-16）
- ダイジェスト認証（P.1-17）
- 許可（P.1-18）

イメージ認証

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

デバイス認証

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

デバイス認証は、P.3-1 の「Cisco CTL クライアントの設定」で説明する Cisco CTL ファイルの作成（Cisco CallManager サーバ ノードおよびアプリケーションの認証の場合）、およびP.6-1 の「Certificate Authority Proxy Function の使用方法」で説明する Certificate Authority Proxy Function（電話機および JTAPI/TAPI/CTI アプリケーションの認証の場合）に依存します。

ヒント　Cisco CallManager 信頼ストアに SIP ユーザ エージェント証明書が含まれ、SIP ユーザ エージェントの信頼ストアに Cisco CallManager 証明書が含まれている場合、SIP トランク経由で接続する SIP ユーザ エージェントは、Cisco CallManager に対して認証されます。Cisco CallManager 信頼ストアの更新の詳細については、『*Cisco IP Telephony Platform Administration Guide*』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。

クラスタをノンセキュア 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。クラスタをセキュア モードに設定した場合、TFTP サーバは呼出音一覧、ローカライズ、デフォルトの .cnf.xml、呼出音一覧 wav ファイルなど、.sgn 形式のスタティック ファイルに署名します。TFTP サーバは、ファイルのデータが変更されたことを確認するたびに、<device name>.cnf.xml 形式のファイルに署名します。

キャッシングが無効になっている場合、TFTP サーバは署名付きファイルをディスクに書き込みます。TFTP サーバは、保存されたファイルが変更されたことを確認すると、再度そのファイルに署名します。ディスク上に新しいファイルを置くと、保存されていたファイルは上書きされて削除されます。電話機で新しいファイルをダウンロードするには、管理者が Cisco CallManager Administration で影響を受けたデバイスを再起動しておく必要があります。

電話機は、TFTP サーバからファイルを受信すると、ファイルのシグニチャを確認して、ファイルの整合性を検証します。電話機で認証された接続を確立するには、次の基準が満たされることを確認します。

- 証明書が電話機に存在する必要がある。
- CTL ファイルが電話機にあり、そのファイルに Cisco CallManager エントリおよび証明書が存在する必要がある。
- デバイスに認証または暗号化を設定した。

（注） ファイル認証は Certificate Trust List（CTL; 証明書信頼リスト）ファイルの作成に依存します。これについては、P.3-1 の「Cisco CTL クライアントの設定」で説明します。

シグナリング認証

このプロセスはシグナリング整合性とも呼ばれ、TLS プロトコルを使用して、転送中のシグナリング パケットが改ざんされていないことを検証します。

シグナリング認証は Certificate Trust List（CTL; 証明書信頼リスト）ファイルの作成に依存します。これについては、P.3-1 の「Cisco CTL クライアントの設定」で説明します。

ダイジェスト認証

この SIP トランクおよび電話機用のプロセスによって、Cisco CallManager は、SIP ユーザ エージェント（UA）が Cisco CallManager に要求を送信したときに、UA の ID でチャレンジができます（SIP ユーザ エージェントは、SIP メッセージを発信したデバイスまたはアプリケーションを表します）。

Cisco CallManager は、回線側電話機またはデバイスから発信され、SIP トランク経由で到達した SIP コールのユーザ エージェント サーバ（UAS）、SIP トランクに向けて発信された SIP コールのユーザ エージェント クライアント（UAC）、または、回線対回線接続またはトランク対トランク接続のバックツーバック ユーザ エージェント（B2BUA）として機能します。ほとんどの環境では、Cisco CallManager 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。

Cisco CallManager は、SIP トランク経由で接続する SIP 電話機または SIP デバイスで（UAS として）チャレンジを行うことができます。また、SIP トランク インターフェイスで受信したチャレンジに（UAC として）応答できます。電話機に対してダイジェスト認証が有効になっている場合、Cisco CallManager は、キープアライブ メッセージ以外のすべての SIP 電話機要求でチャレンジを行います。

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

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

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

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

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

ヒント SIP 電話機は、Cisco CallManager レルムの中にのみ存在できます。SIP トランクの場合、レルムは SIP トランク経由で接続するドメイン（xyz.com など）を表し、要求の発信元の識別に役立ちます。

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

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

管理者は、電話機ユーザまたはアプリケーションユーザの SIP ダイジェスト クレデンシャルを設定します。アプリケーションの場合は、Cisco CallManager Administration の Applications 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、Cisco CallManager Administration の End User ウィンドウで、ダイジェスト認証クレデンシャルを指定し、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、Phone Configuration ウィンドウで Digest User（エンド ユーザ）を選択します。電話機をリセットした後、クレデンシャルは、TFTP サーバが電話機に提供する電話機設定ファイルに存在するようになります。

エンド ユーザのダイジェスト認証を有効にしたが、ダイジェスト クレデンシャルは設定しなかった場合、電話機は登録できません。クラスタ モードがノンセキュアで、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 CallManager でもチャレンジが開始されます。

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

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

許可

Cisco CallManager は、許可プロセスを使用して、SIP 電話機、SIP トランク、および SIP トランクの SIP アプリケーション要求からのメッセージについて、一定のカテゴリを制限します。

SIP INVITE メッセージと in-dialog メッセージ、および SIP 電話機の場合、Cisco CallManager は通話検索空間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 CallManager は、プレゼンス グループへのユーザ アクセスに許可を与えます。

SIP トランクの場合、Cisco CallManager はプレゼンス サブスクリプションおよび non-INVITE SIP メッセージ（out-of-dial REFER、Unsolicited Notification、置換ヘッダー付き SIP 要求など）の許可を与えます。SIP Trunk Security Profile ウィンドウで、関連するチェックボックスをオンにして、許可を指定します。

アプリケーションレベルの許可が設定されている場合、許可は、まず SIP トランクに対して発生し（SIP Trunk Security Profile での設定に従います）、次に SIP トランクの SIP アプリケーション ユーザ エージェントに対して発生します（Application User Configuration での設定に従います）。トランクの場合、Cisco CallManager はトランク ACL 情報をダウンロードしてキャッシュします。ACL 情報は、着信 SIP 要求に適用されます。ACL が SIP 要求を許可しない場合、コールは 403 Forbidden メッセージで失敗します。

ACL が SIP 要求を許可する場合、Cisco CallManager は、SIP Trunk Security Profile 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 CallManager は要求を処理します。ダイジェスト認証が有効な場合、Cisco CallManager は着信要求に認証ヘッダーが存在することを確認してから、ダイジェスト認証を使用して、発信元アプリケーションを識別します。ヘッダーが存在しない場合、Cisco CallManager は 401 メッセージでデバイスに対するチャレンジを行います。

SIP アプリケーション許可を SIP トランクで有効にするには、SIP Trunk Security Profile ウィンドウで Enable Application Level Authorization チェックボックスをオンにする必要があります。アプリケーションレベルの ACL を適用する前に、Cisco CallManager は、ダイジェスト認証で SIP トランク ユーザ エージェントを認証します。そのため、アプリケーションレベルの許可を発生させるには、SIP Trunk Security Profile でダイジェスト認証を有効にする必要があります。

暗号化の概要

ヒント　暗号化は、Cisco CallManager 5.0(1) をクラスタ内の各サーバにインストールすると、自動的にインストールされます。

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

- シグナリング暗号化（P.1-20）
- メディア暗号化（P.1-20）
- 設定ファイルの暗号化（P.1-22）

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 CallManager サーバとの間で送信されるすべての SIP および SCCP シグナリング メッセージが確実に暗号化されます。

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

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

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

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

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

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

メディア暗号化

メディア暗号化は SRTP を使用し、対象とする受信者だけが、サポートされるデバイス間のメディア ストリームを解釈できるようになります。サポートには、オーディオ ストリームだけが含まれます。メディア暗号化には、デバイス用のメディア マスター鍵ペアの作成、デバイスへの鍵配送、鍵転送中の配送の保護が含まれます。

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 デバイスからノンセキュア デバイスへの転送、電話会議、トランスコーディング、保留音などで発生する場合があります。

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

ヒント 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 CallManager は、IPSec が正しく設定されていることを確認しません。IPSec を正しく設定しないと、セキュリティ関連情報が公開される可能性があります。

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

次の例で、SCCP および MGCP コールのメディア暗号化を示します。

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

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

設定ファイルの暗号化

Cisco CallManager は、暗号化された設定ファイルをサポートする電話機用の設定ファイル ダウンロードの一部として、ダイジェスト クレデンシャルおよびその他の保護されたデータを電話機に送出します（P.7-4 の「サポートされる電話機のモデル」を参照）。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。Cisco CallManager は、暗号鍵を符号化し、データベースに格納します。

暗号化された設定ファイルを有効にするには、TFTP Encrypted Configuration エンタープライズ パラメータを True に設定します。TFTP サーバは、シンメトリック鍵と公開鍵の暗号化を使用して、設定ファイルを暗号化および復号化します。詳細については、第 7 章「電話機設定ファイルの暗号化について」を参照してください。

TFTP Encrypted Configuration エンタープライズ パラメータを False に設定すると、Cisco CallManager は、SIP 電話機またはトランク セキュリティ プロファイルでダイジェスト認証が有効になっている場合にダイジェスト クレデンシャルが暗号化されずに送信されるという警告メッセージを表示します。

設定用チェックリストの概要

表 1-3 に、認証および暗号化を実装するために必要な作業を示します。また、各章には指定されたセキュリティ機能のために実行が必要な作業のチェックリストが含まれる場合もあります。

表 1-3　認証および暗号化の設定用チェックリスト

設定手順		関連手順および関連項目
ステップ 1	クラスタにある各サーバの Cisco CallManager Serviceability で Cisco CTL Provider サービスをアクティブにします。 **ヒント** Cisco CallManager のアップグレード前にこのサービスをアクティブにした場合は、サービスを再度アクティブにする必要はありません。アップグレード後にサービスは自動的にアクティブになります。	Cisco CTL Provider サービスのアクティブ化（P.3-4）
ステップ 2	最初のノードの Cisco CallManager Serviceability で Cisco Certificate Authority Proxy サービスをアクティブにし、ローカルで有効な証明書のインストール、アップグレード、トラブルシューティング、または削除を行います。 **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。 **ヒント** これらの設定を Cisco CallManager のアップグレード前に設定した場合、設定はアップグレード時に自動的に移行されます。	TLS 接続用ポートの設定（P.3-5）
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.3-9）
ステップ 5	Cisco CTL クライアントをインストールします。 **ヒント** Cisco CallManager 4.0 で使用できた Cisco CTL クライアントは使用できません。Cisco CallManager 5.0(1) にアップグレードした後で Cisco CTL ファイルを更新するには、Cisco CallManager Administration 5.0(1) で使用可能なプラグインをインストールする必要があります。	• システム要件（P.1-4） • インストール（P.1-12） • Cisco CTL クライアントのインストール（P.3-7）

表 1-3　認証および暗号化の設定用チェックリスト（続き）

設定手順		関連手順および関連項目
ステップ 6	Cisco CTL クライアントを設定します。 **ヒント** Cisco CallManager のアップグレード前に Cisco CTL ファイルを作成した場合、Cisco CTL ファイルはアップグレード時に自動的に移行されます。Cisco CallManager 5.0(1) にアップグレードした後で Cisco CTL ファイルを更新するには、Cisco CTL クライアントの 5.0(1) バージョンをインストールして設定する必要があります。	Cisco CTL クライアントの設定（P.3-9）
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。 • デバイス セキュリティ モードを設定します（SCCP 電話機および SIP 電話機の場合）。 デバイス セキュリティ モードは、Cisco CallManager のアップグレード時に自動的に移行されます。Cisco CallManager 4.0 で認証だけをサポートしていたデバイスに暗号化を設定する場合は、Phone Configuration ウィンドウで暗号化のセキュリティ プロファイルを選択する必要があります。 • 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 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、Enable Digest Authentication 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.5-1）
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。	SCCP または SIP 電話機セキュリティ プロファイルの適用（P.5-9）
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。 Cisco CallManager 5.0(1) へのアップグレード前に証明書の操作を実行して CAPF をサブスクライバ サーバで実行した場合、CAPF データを 4.0 パブリッシャ データベース サーバにコピーしてから、クラスタを Cisco CallManager 5.0 にアップグレードする必要があります。 **注意** Cisco CallManager 4.0 サブスクライバ サーバの CAPF データは Cisco CallManager 5.0(1) データベースに移行されません。したがって、データを 5.0(1) データベースにコピーしないと、データは失われます。データが失われても、CAPF ユーティリティ 1.0(1) を使用して発行したローカルで有効な証明書は電話機に残ります。しかし、この証明書はもう有効でないため、CAPF 5.0(1) は証明書を再発行する必要があります。	• システム要件（P.1-4） • CAPF の設定用チェックリスト（P.6-5）

表 1-3　認証および暗号化の設定用チェックリスト（続き）

設定手順		関連手順および関連項目
ステップ 10	ローカルで有効な証明書が、サポートされている Cisco IP Phone にインストールされたことを確認します。	• システム要件（P.1-4） • 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。	SIP 電話機のダイジェスト認証の設定（P.8-1）
ステップ 12	電話機設定ファイルの暗号化を設定します。	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 13	電話機のセキュリティ強化作業を実行します。 **ヒント**　電話機のセキュリティ強化設定を Cisco CallManager のアップグレード前に設定した場合、デバイス設定はアップグレード時に自動的に移行されます。	電話機のセキュリティ強化（P.9-1）
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。	• ボイス メッセージング ポートのセキュリティ設定（P.10-1） • *Cisco CallManager 5.0 Integration Guide for Cisco Unity 4.x*
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。 **ヒント**　前のリリースの Cisco CallManager でセキュア SRST リファレンスを設定した場合は、Cisco CallManager のアップグレード時にその設定が自動的に移行されます。	Survivable Remote Site Telephony（SRST）リファレンスのセキュリティ設定（P.12-1）
ステップ 16	IPSec を設定します。	• ゲートウェイおよびトランクの暗号化の設定（P.13-1） • 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.13-6） • *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways* • *Cisco IP Telephony Platform Administration Guide*
ステップ 17	SIP トランク 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使用する場合は、プロファイルの Enable Digest Authentication チェックボックスをオンにします。 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。 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、Enable Application Level Authorization チェックボックスをオンにします。 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。	• 許可（P.1-18） • SIP トランク セキュリティ プロファイルの設定（P.14-3） • ダイジェスト認証のエンタープライズ パラメータの設定（P.15-2）

表 1-3　認証および暗号化の設定用チェックリスト（続き）

設定手順		関連手順および関連項目
ステップ 18	SIP トランク セキュリティ プロファイルをトランクに適用します。	SIP トランク セキュリティ プロファイルの適用（P.14-7）
ステップ 19	トランクのダイジェスト認証を設定します。	SIP トランクのダイジェスト認証の設定（P.15-1）
ステップ 20	SIP トランク セキュリティ プロファイルで Enable Application Level Authorization チェックボックスをオンにした場合は、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。	*Cisco CallManager アドミニストレーション ガイド*
ステップ 21	クラスタ内のすべての電話機をリセットします。	デバイスのリセット、サービスの再起動、またはサーバおよびクラスタのリブート（P.1-10）
ステップ 22	クラスタ内の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、またはサーバおよびクラスタのリブート（P.1-10）

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 IP Phone アドミニストレーション ガイド for Cisco CallManager*
- *Cisco IP Telephony Platform Administration Guide*
- *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*
- *Cisco CallManager 5.0 Integration Guide for Cisco Unity 4.x*
- SRST 対応ゲートウェイをサポートする Cisco Survivable Remote Site Telephony（SRST）の管理マニュアル
- *Cisco IP Telephony Disaster Recovery Framework Administration Guide*
- *Cisco CallManager Bulk Administration Guide*
- 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

CHAPTER 2

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

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 CallManager アプリケーションには、Cisco CallManager Administration、Cisco CallManager Serviceability、Cisco IP Phone User Option Pages、TAPS、Cisco CDR Analysis and Reporting（CAR）、Cisco Dialed Number Analyzer、Real Time Monitoring Tool があります。

Cisco CallManager をインストールまたはアップグレードすると、HTTPS 自己署名証明書（tomcat_cert）がプラットフォームで生成されます。自己署名証明書は、アップグレード中に移行されます。.DER 形式および .PEM 形式で、証明書のコピーが作成されます。表 2-1 に、仮想ディレクトリを示します。

表 2-1　Cisco CallManager 仮想ディレクトリ

Cisco CallManager 仮想ディレクトリ	対応するアプリケーション
CCMAdmin	Cisco CallManager Administration
CCMService	Cisco CallManager Serviceability
CCMUser	Cisco Personal Communications Assistant
AST	Real-Time Monitoring Tool （RTMT）
RTMTReports	RTMT レポート アーカイブ
CCMTraceAnalysis	Trace Analysis Tool
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 CDR Analysis and Reporting （CAR）
TAPS	Tool for Auto-Registration Phone Support（TAPS）
dna	Cisco Dialed Number Analyzer
drf	Cisco IP Telephony Disaster Recovery System

（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 Security Alert 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、Security Alert 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。

Cisco CallManager 5.0(1) をインストールまたはアップグレードした後に、初めて Cisco CallManager Administration または他の Cisco CallManager SSL 対応仮想ディレクトリにブラウザ クライアントからアクセスすると、サーバを信頼するかどうかを確認する Security Alert 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。

- Yes 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、Security Alert 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。
- **View Certificate** > **Install Certificate** 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 Security Alert ダイアログボックスが表示されることはありません。
- No 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、Yes をクリックするか、または **View Certificate** > **Install Certificate** 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 Security Alert 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 CallManager Administration など）を参照します。

ステップ 2　Security Alert ダイアログボックスが表示されたら、**View Certificate** をクリックします。

ステップ 3　Certificate ペインの **Install Certificate** をクリックします。

ステップ 4　Certificate Import Wizard が表示されたら、**Next** をクリックします。

ステップ 5　**Place all certificates in the following store** オプション ボタンをクリックし、**Browse** をクリックします。

ステップ 6　**Trusted Root Certification Authorities** を参照し、選択して、**OK** をクリックします。

ステップ 7　**Next** をクリックします。

ステップ 8　**Finish** をクリックします。

ステップ 9　Security Warning Box に証明書のサムプリントが表示されます。

Yes 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、**Yes** 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、Security Alert 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　Certificate ペインの Certification Path 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

Security Alert ダイアログボックスが表示されたら、**View Certificate** ボタンをクリックし、**Details** 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。

- Version
- Serial Number
- Signature Algorithm
- Issuer
- Valid From
- Valid To
- Subject
- Public key
- Subject Key Installer
- Key Usage
- Enhanced Key Usage
- Thumbprint Algorithm

- Thumbprint

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。

- All：すべてのオプションが Details ペインに表示されます。
- Version 1 Fields Only：Version、Serial Number、Signature Algorithm、Issuer、Valid From、Valid To、Subject、および Public Key オプションが表示されます。
- Extensions Only：Subject Key Identifier、Key Usage、および Enhanced Key Usage オプションが表示されます。
- Critical Extensions Only：存在する場合は Critical Extensions が表示されます。
- Properties Only：Thumbprint Algorithm と Thumbprint オプションが表示されます。

（注） 自己署名証明書は、Cisco IPT Platform Administration GUI で再生成できます。

証明書のファイルへのコピー

証明書をファイルにコピーし、ローカルに保管することによって、必要なときにいつでも証明書を復元することができます。

次の手順を実行すると、標準の証明書保管形式で証明書がコピーされます。証明書の内容をファイルにコピーするには、次の手順を実行します。

手順

ステップ 1　Security Alert ダイアログボックスで、**View Certificate** をクリックします。

ステップ 2　**Details** タブをクリックします。

ステップ 3　**Copy to File** ボタンをクリックします。

ステップ 4　Certificate Export Wizard が表示されます。**Next** 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、**Next** 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。**Save**　をクリックします。

ステップ 7　ファイル名とパスが Certificate Export Wizard ペインに表示されます。**Next** 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。**Finish** 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 CallManager Administration 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。

- Accept this certificate for this session
- Do not accept this certificate and do not connect
- Accept this certificate forever (until it expires)

（注）　Do not accept 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、**Examine Certificate** をクリックします。クレデンシャルを確認し、**Close** をクリックします。

ステップ 3　**OK** をクリックします。

Security Warning 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 IPT Platform Administration GUI で再生成できます。

追加情報

詳細については、P.2-8 の「関連項目」を参照してください。

その他の情報

関連項目

証明書の種類（P.1-13）

シスコの関連マニュアル

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

CHAPTER 3

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

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） 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。

ヒント 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）

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

（注） Cisco CallManager ノードのホスト名は、CTL クライアントがインストールされているリモート PC で解決可能である必要があります。そうでない場合、CTL クライアントは正しく動作しません。

Cisco CallManager Administration 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。

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	クラスタにある各 Cisco CallManager の Cisco CallManager Serviceability で Cisco CTL Provider サービスをアクティブにします。 **ヒント**　Cisco CallManager のアップグレード前にこのサービスをアクティブにした場合は、サービスを再度アクティブにする必要はありません。アップグレード後にサービスは自動的にアクティブになります。	Cisco CTL Provider サービスのアクティブ化（P.3-4）
ステップ 2	最初のノードの Cisco CallManager 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。 **ヒント**　これらの設定を Cisco CallManager のアップグレード前に設定した場合、設定は自動的に移行されます。	TLS 接続用ポートの設定（P.3-5）
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.3-9）
ステップ 5	Cisco CTL クライアントをインストールします。	• システム要件（P.1-4） • インストール（P.1-12） • Cisco CTL クライアントのインストール（P.3-7）
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.3-9）

Cisco CTL Provider サービスのアクティブ化

Cisco CTL クライアントの設定後、このサービスによってクラスタのセキュリティ モードがノンセキュア モードからセキュア 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 CallManager および Cisco TFTP サーバに転送されます。

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

ヒント　クラスタ内のすべてのサーバで Cisco CTL Provider サービスをアクティブにする必要があります。

サービスをアクティブにするには、次の手順を実行します。

手順

ステップ 1　Cisco CallManager Serviceability で **Tools > Service Activation** の順に選択します。

ステップ 2　Servers ドロップダウン リスト ボックスで、Cisco CallManager サービスまたは Cisco TFTP サービスをアクティブにしたサーバを選択します。

ステップ 3　**Cisco CTL Provider** サービス オプション ボタンをクリックします。

ステップ 4　**Save** をクリックします。

ステップ 5　クラスタ内のすべてのサーバで、この手順を実行します。

（注）　Cisco CTL Provider サービスをアクティブにする前に、CTL ポートを入力できます。デフォルトのポート番号を変更する場合は、P.3-5 の「TLS 接続用ポートの設定」を参照してください。

ステップ 6　サービスがクラスタ内のすべてのサーバで実行されていることを確認します。サービスの状態を確認するには、Cisco CallManager Serviceability で **Tools > Control Center - Feature Services** の順に選択します。

追加情報

詳細については、P.3-20 の「関連項目」を参照してください。

Cisco CAPF サービスのアクティブ化

このサービスのアクティブ化については、P.6-6 の「Certificate Authority Proxy Function サービスのアクティブ化」を参照してください。

ワンポイント・アドバイス

Cisco CTL クライアントをインストールして設定する前にこの作業を実行すれば、CAPF を使用するために CTL ファイルを更新する必要がなくなります。

TLS 接続用ポートの設定

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

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

Ethernet Phone ポートは、SCCP 電話機からの登録要求を監視します。ノンセキュア モードの場合、電話機はポート 2000 を介して接続されます。セキュア モードの場合、Cisco CallManager の TLS 接続用ポートは Cisco CallManager ポート番号に 443 を加算(+)した番号になるため、Cisco CallManager のデフォルトの TLS 接続は 2443 になります。ポートが現在使用中の場合や、ファイアウォールを使用していてファイアウォール内のポートを使用できない場合にのみ、この設定を更新します。

SIP Secure ポートを使用すると、Cisco CallManager は SIP 電話機からの SIP メッセージを傍受できます。デフォルト値は 5061 です。このポートを変更した場合は、Cisco CallManager Serviceability で Cisco CallManager サービスを再起動し、SIP 電話機をリセットする必要があります。

ヒント

ポートを更新した後は、Cisco CallManager Administration 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。CTL クライアントが使用するポートは、Cisco CallManager にシグナルを戻すために、TLS を実行している電話機も使用します。これらのポートは、電話機が認証済みステータスまたは暗号化済みステータスに設定されているすべての VLAN に対して開いている必要があります。

デフォルト設定を変更するには、次の手順を実行します。

手順

ステップ 1　変更するポートに応じて、次の作業を実行します。

- Cisco CTL Provider サービスの Port Number パラメータを変更するには、ステップ 2 ～ステップ 6 を実行します。
- Ethernet Phone Port または 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 CallManager Administration で **System > Service Parameters** の順に選択します。

ステップ 3　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　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、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　**Save** をクリックします。

ステップ 7　Ethernet Phone Port または SIP Phone Secure Port の設定を変更するには、Cisco CallManager Administration で **System > Cisco CallManager** の順に選択します。

ステップ 8　『*Cisco CallManager アドミニストレーション ガイド*』の説明に従い、Cisco CallManager サービスを実行しているサーバを検索します。結果が表示されたら、サーバの **Name** リンクをクリックします。

ステップ 9　Cisco CallManager Configuration ウィンドウが表示されたら、Ethernet Phone Port フィールドまたは 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 CallManager Serviceability で Cisco CallManager サービスを再起動します。

ステップ 11　**Save** をクリックします。

追加情報

詳細については、P.3-20 の「関連項目」を参照してください。

Cisco CTL クライアントのインストール

次のイベントが発生するときには、クライアントを使用して CTL ファイルを更新する必要があります。

- クラスタのセキュリティ モードの最初の設定時
- CTL ファイルの最初の作成時
- Cisco CallManager のインストール後
- Cisco CallManager サーバまたは Cisco CallManager データの復元後
- Cisco CallManager サーバの IP アドレスまたはホスト名の変更後
- セキュリティ トークン、TFTP サーバ、または Cisco CallManager サーバの追加後または削除後

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 started および automatic 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 CallManager アドミニストレーション ガイド*』の説明に従い、クライアントをインストールしようとする Windows ワークステーションまたはサーバから、Cisco CallManager Administration に移動します。

ステップ 2　Cisco CallManager Administration で、**Application > Plugins** の順に選択します。

Find and List Plugins ウィンドウが表示されます。

ステップ 3　Plugin Type equals ドロップダウン リスト ボックスから **Installation** を選択し、**Find** 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 Client プラグイン名のちょうど反対側にある **Download** をクリックします。

ステップ 6　**Save** 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）　Download Complete ボックスで **Open** 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、**Continue** 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.3-20 の「関連項目」を参照してください。

Cisco CTL クライアントのアップグレードおよび Cisco CTL ファイルの移行

Cisco CallManager 5.0(1) をアップグレードした後で CTL ファイルを変更するには、アップグレード前にインストールしていた Cisco CTL クライアントを削除し、最新の Cisco CTL クライアントをインストールし（P.3-7 の「Cisco CTL クライアントのインストール」を参照）、CTL ファイルを再生成する必要があります。

Cisco CallManager をアップグレードする前にサーバの削除や追加を実行しなかった場合は、アップグレード後に Cisco CTL クライアントを再設定する必要はありません。Cisco CallManager のアップグレードにより、CTL ファイル内のデータは自動的に移行されます。

Cisco CTL クライアントの設定

ヒント　Cisco CTL クライアントは、スケジューリングされたメンテナンス画面で設定します。これは、Cisco CallManager および Cisco TFTP サービスを実行するクラスタにあるすべてのサーバの Cisco CallManager Serviceability で、これらのサービスを再起動する必要があるためです。

Cisco CTL クライアントは、次のタスクを実行します。

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

ヒント　Cisco CallManager Administration の Enterprise Parameters ウィンドウで、Cisco CallManager クラスタ全体のパラメータをセキュア モードに設定することはできません。クラスタ全体のモードを設定するには、CTL クライアントを設定する必要があります。詳細については、P.3-14 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 CallManager、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 CallManager および Cisco CAPF サーバを検出して、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 CallManager Serviceability でアクティブにしたことを確認します。少なくとも 2 つのセキュリティ トークンを入手します。これらのセキュリティ トークンは、Cisco certificate authority が発行します。シスコから取得したセキュリティ トークンを使用する必要があります。トークンを一度に 1 つずつサーバまたはワークステーションの USB ポートに挿入します。サーバに USB ポートがない場合、USB PCI カードを使用することができます。

次のパスワード、ホスト名または IP アドレス、ポート番号を取得します。

- Cisco CallManager の管理ユーザ名とパスワード
- セキュリティ トークンの管理者パスワード

これらの説明については、表 3-2 を参照してください。

ヒント　Cisco CTL クライアントをインストールする前に、クラスタの各サーバへのネットワーク接続を確認します。クラスタのすべてのサーバにネットワーク接続できることを確認するには、『*Cisco IP Telephony Platform Administration Guide*』の説明に従い、ping コマンドを発行します。

複数の Cisco CTL クライアントをインストールした場合、Cisco CallManager では一度に 1 台のクライアントの CTL 設定情報しか受け入れません。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 CallManager によって自動的に保存されます。

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

- CTL ファイルをクラスタ内のすべての Cisco CallManager サーバに書き込む。
- CAPF capf.cer をクラスタ内のすべての Cisco CallManager 後続ノード（最初のノード以外）に書き込む。
- PEM 形式の CAPF 証明書ファイルをクラスタ内のすべての Cisco CallManager 後続ノード（最初のノード以外）に書き込む。
- 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。
- **Start > Programs > 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 CallManager サーバの設定内容を入力し、**Next** をクリックします。

ステップ 4　表 3-2 の説明に従って、**Set CallManager Cluster to Secure Mode** をクリックし、**Next** をクリックします。

ステップ 5　設定する内容に応じて、次の作業を実行します。

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

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

ステップ 6　アプリケーションが要求したら、現在 Cisco CTL クライアントを設定しているワークステーションまたはサーバで使用可能な USB ポートにセキュリティ トークンを 1 つ挿入して、**OK** をクリックします。

ステップ 7　挿入したセキュリティ トークンについての情報が表示されます。**Add** をクリックします。

ステップ 8　検出された証明書エントリがペインに表示されます。

ステップ 9　他のセキュリティ トークン（複数も可能）を証明書信頼リストに追加するには、**Add Tokens** をクリックします。

ステップ 10　サーバまたはワークステーションに挿入したトークンを取り外していない場合は、取り外します。アプリケーションが要求したら、次のトークンを挿入して **OK** をクリックします。

ステップ 11　2 番目のセキュリティ トークンについての情報が表示されます。**Add** をクリックします。

ステップ 12　すべてのセキュリティ トークンについて、ステップ 9 ～ステップ 11 を繰り返します。

ステップ 13　証明書エントリがペインに表示されます。

ステップ 14　表 3-2 の説明に従って、設定内容を入力します。

ステップ 15　**Next** をクリックします。

ステップ 16　表 3-2 の説明に従って設定内容を入力し、**Next** をクリックします。

ステップ 17　すべてのセキュリティ トークンおよびサーバを追加したら、**Finish** をクリックします。

ステップ 18　表 3-2 の説明に従ってセキュリティ トークンのユーザ パスワードを入力し、**OK** をクリックします。

ステップ 19　クライアントによって CTL ファイルが作成されると、各サーバのウィンドウに、サーバ、ファイル ロケーション、および CTL ファイルのステータスが表示されます。**Finish** をクリックします。

ステップ 20　クラスタ内のすべてのデバイスをリセットします。詳細については、P.1-10 の「デバイスのリセット、サービスの再起動、またはサーバおよびクラスタのリブート」を参照してください。

ステップ 21　Cisco CallManager Serviceability で、クラスタ内の各サーバで実行されている Cisco CallManager 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.3-20 の「関連項目」を参照してください。

CTL ファイルの更新

次のシナリオが発生した場合、CTL ファイルを更新する必要があります。

- 新しい Cisco CallManager サーバをクラスタに追加した場合
- クラスタ内の Cisco CallManager サーバの名前または IP アドレスを変更した場合
- Cisco CallManager Serviceability で Cisco Certificate Authority Function サービスを有効にした場合
- セキュリティ トークンを新たに追加または削除する必要がある場合
- Cisco CallManager サーバまたは Cisco CallManager データを復元した場合

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 CallManager サーバの設定内容を入力し、**Next** をクリックします。

ヒント　このウィンドウでは、Cisco CallManager サーバについて更新します。

ステップ 4　CTL ファイルを更新するには、表 3-2 の説明にあるように **Update CTL File** をクリックし、**Next** をクリックします。

注意　すべての CTL ファイルを更新するには、すでに CTL ファイルに存在するセキュリティ トークンを（1 つ）USB ポートに挿入する必要があります。クライアントでは、このトークンを使用して CTL ファイルのシグニチャを検証します。CTL クライアントによってシグニチャが検証されるまで、新しいトークンは追加できません。ワークステーションまたはサーバに USB ポートが 2 つある場合は、両方のセキュリティ トークンを同時に挿入しないでください。

ステップ 5　現在 CTL ファイルを更新しているワークステーションまたはサーバで使用可能な USB ポートにまだセキュリティ トークンを挿入していない場合は、いずれかのセキュリティ トークンを挿入してから **OK** をクリックします。

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

検出された証明書エントリがペインに表示されます。

ヒント　このペインでは、Cisco CallManager および Cisco TFTP エントリを更新できません。Cisco CallManager エントリを更新するには **Cancel** をクリックし、ステップ 2 ～ステップ 6 をもう一度実行します。

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

- 新しいセキュリティ トークンを追加するには、P.3-9 の「Cisco CTL クライアントの設定」を参照する。
- セキュリティ トークンを削除するには、P.3-13 の「CTL ファイル エントリの削除」を参照する。

追加情報

詳細については、P.3-20 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、**Delete Selected** をクリックしてエントリを削除します。

Cisco CallManager、Cisco TFTP、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.3-20 の「関連項目」を参照してください。

クラスタ全体のセキュリティ モードの更新

クラスタ全体のセキュリティ モードを設定するには、Cisco CTL クライアントを使用する必要があります。クラスタ全体のセキュリティ モードは、Cisco CallManager Administration の Enterprise Parameters ウィンドウで変更することはできません。

Cisco CTL クライアントの初期設定後にクラスタ全体のセキュリティ モードを変更するには、P.3-12 の「CTL ファイルの更新」および表 3-2 の説明に従って CTL ファイルを更新する必要があります。クラスタ全体のセキュリティ モードをセキュア モードからノンセキュア モードに変更した場合、CTL ファイルはクラスタ内のサーバに存在したままですが、CTL ファイルに証明書は含まれません。CTL ファイルに証明書が存在しないため、電話機は署名なし設定ファイルを要求し、ノンセキュアとして Cisco CallManager に登録されます。

Cisco CTL クライアントの設定内容

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

表 3-2 を使用して、初めての Cisco CTL クライアント設定、CTL ファイルの更新、または混合モードからノンセキュア モードへの変更を行うことができます。

表 3-2　CTL クライアントの設定内容

設定	説明
CallManager サーバ	
Hostname or IP Address	最初のノードのホスト名または IP アドレスを入力します。
Port	ポート番号を入力します。これは、指定した Cisco CallManager サーバで実行されている Cisco CTL Provider サービスの CTL ポートです。デフォルトのポート番号は 2444 です。
Username and Password	最初のノードで管理者特権を持つユーザ名とパスワードと同じものを入力します。
オプション ボタン	
Set CallManager Cluster to Secure Mode	セキュア モードでは、認証済みまたは暗号化済みの Cisco IP Phone と、認証されていない Cisco IP Phone を Cisco CallManager に登録することができます。このモードでは、認証済みまたは暗号化済みのデバイスでセキュア ポートが使用されることを Cisco CallManager が保証します。 **（注）** クラスタをセキュア モードに設定すると、Cisco CallManager によって自動登録は無効になります。
Set CallManager Cluster to Nonsecure Mode	すべてのデバイスが非認証として Cisco CallManager に登録されます。Cisco CallManager ではイメージ認証だけをサポートします。 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、ノンセキュアとして CiscoCallManager に登録されます。 **ヒント** 電話機をデフォルトのノンセキュア モードに戻すには、電話機およびすべての Cisco CallManager サーバから CTL ファイルを削除する必要があります。 このモードでは自動登録を使用できます。
Update CTL File	CTL ファイルの作成後にこのファイルを変更するには、このオプションを選択する必要があります。このオプションを選択すると、クラスタのセキュリティ モードは変更されません。
セキュリティ トークン	
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 CallManager クラスタのセキュリティ モードの確認

Cisco CallManager クラスタのセキュリティ モードを確認するには、次の手順を実行します。

手順

ステップ 1　Cisco CallManager Administration で **System > Enterprise Parameters** 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 CallManager クラスタはセキュア 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 CallManager Administration では変更できません。この値が表示されるのは、Cisco CTL クライアントの設定後です。

追加情報

詳細については、P.3-20 の「関連項目」を参照してください。

Smart Card サービスの Started および Automatic への設定

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 automatic および started に設定する必要があります。

ヒント　サービスが started および automatic 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 CallManager のアップグレードなどを行ったら、Smart Card サービスが started および automatic になっていることを確認します。

サービスを started および automatic 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、**Start > Programs > Administrative Tools > Services** または **Start > Control Panel > Administrative Tools > Services** の順に選択します。

ステップ 2　Services ウィンドウで、**Smart Card** サービスを右クリックし、**Properties** を選択します。

ステップ 3　Properties ウィンドウに General タブが表示されていることを確認します。

ステップ 4　Startup type ドロップダウン リスト ボックスから、**Automatic** を選択します。

ステップ 5　**Apply** をクリックします。

ステップ 6　Service Status 領域で、**Start** をクリックします。

ステップ 7　**OK** をクリックします。

ステップ 8　サーバまたはワークステーションをリブートし、サービスが動作していることを確認します。

追加情報

詳細については、P.3-20 の「関連項目」を参照してください。

セキュリティ トークン パスワード（etoken）の変更

この管理パスワードは、証明書の秘密鍵を取得し、CTL ファイルが署名されることを保証します。各セキュリティ トークンには、デフォルト パスワードが付属されています。セキュリティ トークン パスワードはいつでも変更できます。Cisco CTL クライアントによりパスワードの変更を求めるプロンプトが表示されたら、設定を続行する前にパスワードを変更する必要があります。

パスワード設定の関連情報を検討するには、**Show Tips** ボタンをクリックします。何らかの理由でパスワードを設定できない場合は、表示されるヒントを検討してください。

セキュリティ トークン パスワードを変更するには、次の手順を実行します。

手順

ステップ 1　Cisco CTL クライアントを Windows サーバまたはワークステーションにインストールしたことを確認します。

ステップ 2　Cisco CTL クライアントをインストールした Windows サーバまたはワークステーションの USB ポートにセキュリティ トークンが挿入されていなければ挿入します。

ステップ 3　**Start** > **Programs** > **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

P.16-5 の「CTL セキュリティ トークンのトラブルシューティング」を参照してください。

詳細については、P.3-20 の「関連項目」を参照してください。

Cisco 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 CallManager サーバから CTL ファイルを削除する予定がない場合にお勧めします。

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

- CTL ファイルに署名したセキュリティ トークンをすべて紛失した。
- CTL ファイルに署名したセキュリティ トークンが漏洩した。
- IP Phone をセキュア クラスタから、ストレージ領域、ノンセキュア クラスタ、または異なるドメインの別のセキュア クラスタへと移動する。
- IP Phone を、未知のセキュリティ ポリシーを持つ領域からセキュア クラスタへと移動する。
- 代替 TFTP サーバ アドレスを、CTL ファイル内に存在しないサーバへと変更する。

Cisco 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 IP Phone 上の CTL ファイルの削除

Cisco IP Phone モデル	作業
Cisco IP Phone 7960 および 7940	IP Phone 上の Security Configuration メニューにある、**CTL file**、**unlock** または ****#**、および **erase** を押します。
Cisco IP Phone 7970	次の方法のどちらかを実行します。 • Security Configuration メニューのロックを解除します（『*Cisco IP Phone アドミニストレーション ガイド for Cisco CallManager*』を参照）。CTL オプションの下にある **Erase** ソフトキーを押します。 • Settings メニューにある **Erase** ソフトキーを押します。 **（注）** Settings メニューにある Erase 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 IP Phone アドミニストレーション ガイド for Cisco CallManager*』を参照してください。

追加情報

詳細については、P.3-20 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。
- **Start > Programs > 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.3-20 の「関連項目」を参照してください。

Cisco CTL クライアントの確認とアンインストール

Cisco CTL クライアントをアンインストールしても、CTL ファイルは削除されません。同様に、クライアントをアンインストールしても、クラスタ全体のセキュリティ モードと CTL ファイルは変更されません。必要であれば、CTL クライアントをアンインストールし、クライアントを別の Windows ワークステーションまたはサーバにインストールして、同じ CTL ファイルを引き続き使用することができます。

Cisco CTL クライアントがインストールされていることを確認するには、次の手順を実行します。

手順

ステップ 1　**Start > Control Panel > Add Remove Programs** の順に選択します。

ステップ 2　**Add Remove Programs** 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　クライアントを削除するには、**Remove** をクリックします。

追加情報

詳細については、P.3-20 の「関連項目」を参照してください。

その他の情報

関連項目

- システム要件（P.1-4）
- Cisco CTL クライアントの概要（P.3-2）
- Cisco CTL クライアントの設定用チェックリスト（P.3-3）
- Cisco CTL Provider サービスのアクティブ化（P.3-4）
- 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.3-5）
- Cisco CTL クライアントのインストール（P.3-7）
- Cisco CTL クライアントのアップグレードおよび Cisco CTL ファイルの移行（P.3-8）
- Cisco CTL クライアントの設定（P.3-9）
- CTL ファイルの更新（P.3-12）
- CTL ファイル エントリの削除（P.3-13）
- クラスタ全体のセキュリティ モードの更新（P.3-13）
- Cisco CTL クライアントの設定内容（P.3-14）
- Cisco CallManager クラスタのセキュリティ モードの確認（P.3-15）
- Smart Card サービスの Started および Automatic への設定（P.3-16）
- Cisco IP Phone 上の CTL ファイルの削除（P.3-18）
- Cisco CTL クライアントのバージョンの特定（P.3-19）
- Cisco CTL クライアントの確認とアンインストール（P.3-19）
- Certificate Authority Proxy Function の使用方法（P.6-1）
- CTL セキュリティ トークンのトラブルシューティング（P.16-5）

シスコの関連マニュアル

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

PART 2

Cisco IP Phone および Cisco Unity ボイス メッセージング 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

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

Cisco CallManager の新規インストールを実行している場合、Cisco CallManager クラスタはノンセキュア モードで起動します。Cisco CallManager のインストール後に電話機が起動すると、デバイスはすべてノンセキュアとして Cisco CallManager に登録されます。

Cisco CallManager 4.0(1) またはそれ以降のリリースからアップグレードした後は、アップグレード前に有効にしたデバイス セキュリティ モードで電話機が起動します。デバイスはすべて選択されたセキュリティ モードを使用して登録されます。

Cisco CallManager 5.0(1) のインストールを行うと、Cisco CallManager および TFTP サーバに自己署名証明書が作成されます。クラスタに認証を設定した後、Cisco CallManager はこの自己署名証明書を使用してサポートされた Cisco IP Phone を認証します。自己署名証明書が Cisco CallManager および TFTP サーバに存在していれば、Cisco CallManager はそれぞれの Cisco CallManager アップグレード時に証明書を再発行しません。新しい証明書エントリで新しい CTL ファイルを作成する必要があります。

ヒント　サポートされていないシナリオまたは安全でないシナリオについては、P.1-6 の「対話および制限」を参照してください。

Cisco CallManager は認証および暗号化のステータスをデバイス レベルで維持します。コールに関係するすべてのデバイスがセキュアとして登録されると、コール ステータスはセキュアとして登録されます。いずれか 1 つのデバイスがノン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、そのコールはノンセキュアとして登録されます。

ユーザが Cisco CallManager エクステンション モビリティを使用する場合、Cisco CallManager はデバイスの認証および暗号化ステータスを保持します。また、共有回線が設定されている場合も、Cisco CallManager はデバイスの認証および暗号化ステータスを保持します。

ヒント　暗号化された Cisco IP Phone に対して共有回線を設定する場合は、回線を共有するすべてのデバイスを暗号化用に設定します。つまり、暗号化をサポートするセキュリティ プロファイルを適用して、すべてのデバイスのデバイス セキュリティ モードを暗号化済みに設定します。

サポートされる電話機のモデル

このセキュリティ ガイドでは、各 Cisco IP Phone でサポートされるセキュリティ機能を示しません。使用している電話機でサポートされるセキュリティ機能の一覧については、Cisco CallManager 5.0(1) 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 CallManager Administration でセキュリティ機能を設定できますが、Cisco TFTP サーバで互換ファームウェア ロードをインストールするまで、その機能は動作しません。

電話機のセキュリティ設定の確認

セキュリティをサポートする電話機に、特定のセキュリティ関連設定を構成して表示することができます。たとえば、電話機にインストールされている証明書がローカルで有効な証明書（LSC）か製造元でインストールされる証明書（MIC）かを確認できます。セキュリティ メニューおよびアイコンの詳細については、使用している電話機モデルおよびこのバージョンの Cisco CallManager をサポートする Cisco IP Phone の管理およびユーザ マニュアルを参照してください。

Cisco CallManager がコールを認証済みまたは暗号化済みとして分類すると、コールの状態を示すアイコンが電話機に表示されます。Cisco CallManager がコールを認証済みまたは暗号化済みとして分類する場合を判別するには、P.1-6 の「対話および制限」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、クラスタ セキュリティ モードを Secure Mode 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。	SCCP または SIP 電話機セキュリティ プロファイルの適用（P.5-9）
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、Cisco CallManager Administration の End User 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。	• 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、Cisco CallManager Administration の Phone Configuration ウィンドウで、Digest User を選択します。	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 SIP IP Phone 7960 または 7940 で、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。	『*Cisco CallManager セキュリティ ガイド*』では、電話機でダイジェスト認証クレデンシャルを入力する手順について説明しません。この作業の実行方法については、使用している電話機モデルとこのバージョンの Cisco CallManager をサポートする Cisco 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	Cisco CallManager Administration で電話機の設定を無効にして電話機のセキュリティを強化します。	電話機のセキュリティ強化（P.9-1）

その他の情報

関連項目

- 対話および制限（P.1-6）
- 認証、整合性、および許可の概要（P.1-15）
- 暗号化の概要（P.1-20）
- 設定用チェックリストの概要（P.1-23）
- 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 IP Phone アドミニストレーション ガイド for Cisco CallManager*
- *Cisco CallManager トラブルシューティング ガイド*

CHAPTER 5

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

Cisco CallManager Administration では、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、セキュリティ関連の設定がグループ化されます。そのため、デバイス設定ウィンドウでプロファイルを選択することで、すべての構成済み設定を SIP または SCCP 電話機に適用できます。

電話機セキュリティ プロファイルを設定するときは、次の情報について検討してください。

- プロファイルの CAPF 設定は、Phone Configuration ウィンドウで表示される Certificate Authority Proxy Function 設定と組み合せて設定する。
- すべての SIP および SCCP 電話機に、セキュリティ プロファイルを適用する必要がある。デバイスがセキュリティをサポートしていない場合は、ノンセキュア プロファイルを適用する。
- Cisco CallManager 5.0 アップグレードの前にデバイス セキュリティ モードを設定した場合は、Cisco CallManager がモードに基づいてプロファイルを作成し、デバイスにプロファイルを適用する。
- デバイスが設定済みのプロファイルをサポートしない場合、Cisco CallManager は、そのプロファイルをデバイスに適用することを許可しない。

SCCP または SIP 電話機セキュリティ プロファイルの検索

電話機セキュリティ プロファイルを検索するには、次の手順を実行します。

手順

ステップ 1　Cisco CallManager Administration で、**System** > **Security Profile** > **SIP Phone Security Profile** または **SCCP Phone Security Profile** の順に選択します。

Find and List ウィンドウが表示されます。

ステップ 2　ドロップダウン リスト ボックスから、表示するセキュリティ プロファイルの検索基準を選択し、**Find** をクリックします。

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

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

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

ヒント　検索結果内の Name または Description を検索するには、**Search Within Results** チェックボックスをオンにして、この手順で説明したように検索基準を入力し、**Find** をクリックします。

追加情報

詳細については、P.5-11 の「関連項目」を参照してください。

SCCP または SIP 電話機セキュリティ プロファイルの設定

セキュリティ プロファイルを追加、更新、またはコピーするには、次の手順を実行します。

手順

ステップ 1　Cisco CallManager Administration で、**System** > **Security Profile** > **SIP Phone Security Profile** または **SCCP Phone Security Profile** 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、**Add New** ボタンをクリックし、ステップ 3 に進みます。
- 既存のセキュリティ プロファイルをコピーするには、P.5-2 の「SCCP または SIP 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 **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.5-2 の「SCCP または SIP 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。

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　**Save** 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.5-9 の「SCCP または SIP 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、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。Phone Configuration ウィンドウでダイジェスト ユーザを指定します。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.5-11 の「関連項目」を参照してください。

SCCP 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 5-1　SCCP 電話機セキュリティ プロファイル

設定	説明
Name	セキュリティ プロファイルの名前を入力します。 デバイスがプロファイルをサポートする場合、Phone Configuration ウィンドウの SCCP Phone 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。
Description	セキュリティ プロファイルの説明を入力します。
Device Security Mode	ドロップダウン ボックスから、次のオプションのいずれか 1 つを選択します。 • **Non Secure**：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 CallManager が利用できる。 • **Authenticated**：Cisco CallManager は電話機の整合性と認証を提供する。NULL/SHA を使用する TLS 接続を開始する。 • **Encrypted**：Cisco CallManager は電話機の整合性、認証、および暗号化を提供する。シグナリング用に AES128/SHA を使用する TLS 接続を開始し、すべての電話機コールのメディアを SRTP で搬送する。

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
Authentication Mode	Certificate Authority Proxy Function で使用します。このフィールドで、Phone Configuration ウィンドウで設定した証明書の操作中に、電話機が CAPF で認証するために使用する方式を選択できます。 ドロップダウン ボックスから、次のオプションのいずれか 1 つを選択します。 • **By Authentication String**：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。 • **By Null String**：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。 • **By Existing Certificate (Precedence to LSC)**：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。 • **By Existing Certificate (Precedence to MIC)**：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。
Key Size	CAPF で使用します。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。 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。

SIP 電話機セキュリティ プロファイルの設定内容

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。

表 5-2　SIP 電話機セキュリティ プロファイル

設定	説明
Name	セキュリティ プロファイルの名前を入力します。 **ヒント**　デバイスに正しいプロファイルを適用できるように、セキュリティ プロファイル名にはデバイス モデルを含めます。
Description	セキュリティ プロファイルの説明を入力します。
Nonce Validity Time	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。 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 CallManager は新しい値を生成します。
Device Security Mode	ドロップダウン ボックスから、次のオプションのいずれか 1 つを選択します。 • **Non Secure**：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 CallManager が利用できる。 • **Authenticated**：Cisco CallManager は電話機の整合性と認証を提供する。NULL/SHA を使用する TLS 接続を開始する。 • **Encrypted**：Cisco CallManager は電話機の整合性、認証、および暗号化を提供する。シグナリング用に AES128/SHA を使用する TLS 接続を開始し、すべての電話機コールのメディアを SRTP で搬送する。
Transport Type	ドロップダウン ボックスから、次のオプションのいずれか 1 つを選択します。 • **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。 • **TLS**：SIP 電話機のシグナリング整合性、デバイス認証、シグナリング暗号化を保証するには、Transport Layer Security プロトコルを選択します。 認証のみをサポートするデバイスの場合、TLS_RSA_WITH_NULL_SHA アルゴリズムが使用されます。 認証と暗号化をサポートするデバイスの場合、TLS_RSA_WITH_AES128_SHA が使用されます。 • **TCP + UDP**：TCP と UDP を組み合せて使用するには、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。

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
Enable Digest Authentication	電話機から Cisco CallManager に要求を送信したときに、Cisco CallManager が電話機の ID でチャレンジを行うようにするには、このチェックボックスをオンにします。Cisco CallManager が ID でチャレンジを行った後、電話機は MD5 チェックサムで応答し、Cisco CallManager Administration で設定したクレデンシャルに基づいて Cisco CallManager が情報を検証します。クレデンシャルが一致した場合、電話機のダイジェスト認証は成功します。 このチェックボックスをオンにすると、Cisco CallManager は、電話機からのすべての SIP 要求でチャレンジを行います。 **ヒント**　ダイジェスト認証クレデンシャルは、Cisco CallManager Administration の End User ウィンドウで指定します。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、Phone Configuration ウィンドウで Digest User（エンド ユーザ）を選択します。 ダイジェスト認証は、整合性や信頼性を提供しません。電話機の整合性と信頼性を保証するには、Transport Type を TLS に設定し、デバイス セキュリティ モードを暗号化に設定します。 **（注）**　ダイジェスト認証の詳細については、P.1-17 の「ダイジェスト認証」および第 8 章「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。

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
Authentication Mode	CAPF で使用します。このフィールドで、Phone Configuration ウィンドウで設定した証明書の操作中に、電話機が CAPF で認証するために使用する方式を選択できます。 ドロップダウン ボックスから、次のオプションのいずれか 1 つを選択します。 • **By Authentication String**：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。 • **By Null String**：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。 • **By Existing Certificate (Precedence to LSC)**：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。 • **By Existing Certificate (Precedence to MIC)**：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。
Key Size	CAPF で使用します。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。 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。
SIP Phone Port	Cisco SIP IP Phone が、Cisco CallManager からの SIP メッセージの傍受に使用するポート番号を入力します。デフォルト設定は 5060 です。

SCCP または SIP 電話機セキュリティ プロファイルの適用

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。

認証または暗号化用に設定したセキュリティ 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. Phone Configuration ウィンドウで、ノンセキュア プロファイルを適用します。
2. 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. Phone Configuration ウィンドウで、認証または暗号化用に設定した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 CallManager アドミニストレーション ガイド*』の説明に従って、電話機を検索します。

ステップ 2　Phone Configuration ウィンドウが表示された後、電話機のプロトコルに応じて、次の設定を見つけます。

- **SCCP Phone Security Profile**
- **SIP Phone Security Profile**

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　**Save** をクリックします。

ステップ 5　**Reset** 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、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、Phone Configuration ウィンドウで、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.5-11 の「関連項目」を参照してください。

SCCP または SIP 電話機セキュリティ プロファイルの削除

ここでは、Cisco CallManager データベースから電話機セキュリティ プロファイルを削除する方法について説明します。

始める前に

Cisco CallManager Administration 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、当該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。当該プロファイルを使用しているデバイスを検索するには、Security Profile Configuration ウィンドウの Related Links ドロップダウン リスト ボックスから **Dependency Records** を選択して、**Go** をクリックします。

システムで Dependency Records 機能が有効になっていない場合は、レコードの依存性の概要ウィンドウに、Dependency Records 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、Dependency Records 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。Dependency Records の詳細については、『*Cisco CallManager システム ガイド*』を参照してください。

手順

ステップ 1　P.5-2 の「SCCP または SIP 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、Find and List 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、**Delete Selected** アイコンまたは **Delete Selected** ボタンをクリックします。

ステップ 3　単一のセキュリティ プロファイルを削除するには、次の作業のどちらかを実行します。

- Find and List 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、**Delete Selected** アイコンまたは **Delete Selected** ボタンをクリックします。
- Find and List ウィンドウで、セキュリティ プロファイルの Name リンクをクリックします。指定した Security Profile Configuration ウィンドウが表示されたら、**Delete** アイコンまたは **Delete** 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、**Cancel** 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.5-11 の「関連項目」を参照してください。

電話機セキュリティ プロファイルを使用している電話機の検索

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

ステップ 1　Cisco CallManager Administration で **Device** > **Phone** の順に選択します。

ステップ 2　Find Phone where ドロップダウン リスト ボックスから、**Security Profile** を選択します。

ステップ 3　必要に応じて、Find Phone ドロップダウン リスト ボックスの横に表示されているドロップダウン リスト ボックスのオプションを選択してセキュリティ プロファイルの追加の検索基準を指定し、特定の検索基準を入力します。

ステップ 4　検索基準を指定した後、**Find** をクリックします。検索結果が表示されます。

追加情報

詳細については、P.5-11 の「関連項目」を参照してください。

その他の情報

関連項目

- 電話機セキュリティ プロファイルの概要（P.5-1）
- SCCP または SIP 電話機セキュリティ プロファイルの検索（P.5-2）
- SCCP または SIP 電話機セキュリティ プロファイルの設定（P.5-3）
- SCCP 電話機セキュリティ プロファイル の設定内容（P.5-4）
- SIP 電話機セキュリティ プロファイルの設定内容（P.5-6）
- SCCP または SIP 電話機セキュリティ プロファイルの適用（P.5-9）
- SCCP または SIP 電話機セキュリティ プロファイルの削除（P.5-10）
- 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.5-11）
- 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 IP Phone アドミニストレーション ガイド for Cisco CallManager

その他の情報

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

Certificate Authority Proxy Function（CAPF）は Cisco CallManager と共に自動的にインストールされ、設定に応じて次のタスクを実行します。

- 既存の Manufacturing Installed Certificate（MIC; 製造元でインストールされる証明書）、Locally Significant Certificate（LSC; ローカルで有効な証明書）、ランダム生成された認証文字列、または安全性の低いオプションの「null」認証によって認証する。
- ローカルで有効な証明書を、サポートされている Cisco IP Phone モデルに対して発行する。
- 電話機にある既存のローカルで有効な証明書をアップグレードする。
- 電話機の証明書を表示およびトラブルシューティングするために取得する。
- 製造元でインストールされる証明書によって認証する。

Cisco Certificate Authority Proxy Function サービスをアクティブにすると、CAPF に固有な鍵のペアおよび証明書が CAPF によって自動生成されます。CAPF 証明書は Cisco CTL クライアントによってクラスタ内のすべてのサーバにコピーされ、拡張子 .0 を使用します。CAPF 証明書が存在することを確認するには、Cisco IPT Platform GUI で、CAPF 証明書を表示します。

Cisco IP Phone と CAPF の対話

CAPF と対話するとき、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る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乱れることがあります。

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 CallManager、および保護された SRST 対応ゲートウェイとの間で接続を確立するのに 60 秒以上かかる場合があります。最高のセキュリティ レベルを必要としている場合を除き、2048 ビットの鍵は設定しないでください。

次に、ユーザまたは Cisco CallManager によって電話機がリセットされたときに CAPF が Cisco IP Phone 7960 および 7940 とどのように相互対話するかについて説明します。

（注）　次の例では、LSC が電話機内にまだ存在しない場合や、CAPF Authentication Mode に By Existing Certificate が選択されている場合に、CAPF 証明書操作が失敗します。

例：ノンセキュアの Device Security Mode

この例では、Device Security Mode を Nonsecure に、CAPF Authentication Mode を By Null String または By Existing Certificate (Precedence...) に設定した後に電話機がリセットされます。電話機は、リセット後すぐにプライマリ Cisco CallManager に登録し、設定ファイルを受け取ります。次に、電話機は自動的に CAPF とのセッションを開始し、LSC をダウンロードします。LSC のインストール後、電話機は Device Support Mode を Authenticated または Encrypted に設定します。

例：認証済みまたは暗号化済みの Device Security Mode

この例では、Device Security Mode を Authenticated または Encrypted に、CAPF Authentication Mode を By Null String または By Existing Certificate (Precedence...) に設定した後に電話機がリセットされます。CAPF セッションが終了して電話機が LSC をインストールするまで、電話機はプライマリ Cisco CallManager に登録しません。セッションが終了すると、電話機は登録を行い、すぐに認証済みまたは暗号化済みモードで動作します。

この例では、電話機は CAPF サーバに自動的に接続しないので、By Authentication String を設定することはできません。電話機に有効な LSC がない場合、登録は失敗します。

CAPF システムの対話および要件

CAPF には、次の要件があります。

- CAPF を使用する前に、Cisco CTL クライアントのインストールおよび設定に必要なすべての作業を実行したことを確認します。CAPF を使用するには、最初のノードで Cisco Certificate Authority Proxy Function サービスをアクティブにする必要があります。
- このリリースの Cisco CallManager は、SCEP または Microsoft CA や Keon CA などサードパーティの CA 署名付き LSC 証明書をサポートしません。サードパーティ証明書のサポートは、将来のリリースで予定されています。現在、サードパーティ CA を使用している場合は、5.0 に移行する前に、有効期間が長い（6 か月以上の）証明書を再発行し、サードパーティ証明書がサポートされる前に失効しないようにしてください。
- 証明書のアップグレードまたはインストール操作で、電話機に対して CAPF 認証方式を By Authentication String にした場合、操作後に同じ認証文字列を電話機に入力する必要があります。入力しなかった場合、操作が失敗します。TFTP Encrypted Configuration エンタープライズ パラメータが有効で、認証文字列を入力しなかった場合、電話機に障害が発生し、電話機に入力された認証文字列が一致するまで復帰しないことがあります。
- スケジューリングされたメンテナンス画面で CAPF を使用することを強く推奨します。これは、同時に多数の証明書が生成されると、コール処理が中断される場合があるためです。
- Cisco CallManager 5.0(1) クラスタ内のすべてのサーバで、同じ管理者ユーザ名とパスワードを使用する必要があります。これで、CAPF はクラスタ内のすべてのサーバに認証を受けることができます。
- 証明書操作の間、最初のノードが実行中で正しく機能していることを確認します。
- 証明書操作の間、電話機が正しく機能していることを確認します。

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

Cisco CallManager Serviceability での CAPF の設定

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

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

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

CAPF の設定用チェックリスト

表 6-1 に、ローカルで有効な証明書をインストール、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。 CAP 1.0(1) データを Cisco CallManager 4.0 パブリッシャ データベース サーバにコピーする必要があるかどうかを判別します。 **ヒント**　Cisco CallManager 4.0 で CAPF ユーティリティを使用していて、CAPF データが Cisco CallManager 5.0(1) データベースに存在することを確認した場合は、Cisco CallManager 4.0 で使用していた CAPF ユーティリティを削除できます。	• 使用している電話機モデルと、このバージョンの Cisco CallManager をサポートする電話機のマニュアル • *Cisco IP Telephony Data Migration Assistant 2.0 User Guide*
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.3-9）
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。	• 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 CallManager Administration を使用します。	• 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） • 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 CallManager 5.0(1) では、Cisco CallManager Serviceability で Certificate Authority Proxy Function サービスが自動的にアクティブになりません。

このサービスは、最初のノードでのみアクティブにします。Cisco CTL クライアントをインストールして設定する前にこのサービスをアクティブにしなかった場合は、P.3-12 の「CTL ファイルの更新」の説明に従って CTL ファイルを更新する必要があります。

サービスをアクティブにするには、次の手順を実行します。

手順

ステップ 1　Cisco CallManager Serviceability で **Tools > Service Activation** の順に選択します。

ステップ 2　Servers ドロップダウン リスト ボックスから、Certificate Authority Proxy Function サービスをアクティブにするサーバを選択します。

ステップ 3　**Certificate Authority Proxy Function** チェックボックスをオンにします。

ステップ 4　**Save** をクリックします。

追加情報

詳細については、P.6-12 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 Service Parameter 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 CallManager Administration 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 CallManager Administration で、**System > Service Parameters** 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、最初のノードを選択します。

ステップ 3　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.6-12 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 を使用するときに、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 CallManager アドミニストレーション ガイド*』の説明に従って、電話機を検索します。

ステップ 2　検索結果が表示された後、証明書をインストール、アップグレード、削除、またはトラブルシューティングする電話機を見つけて、その電話機の **Device Name (Line)** 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　**Save** をクリックします。

ステップ 5　**Reset** をクリックします。

追加情報

詳細については、P.6-12 の「関連項目」を参照してください。

Phone Configuration ウィンドウの CAPF 設定

表 6-2 は、Cisco CallManager Administration の Phone Configuration ウィンドウにある CAPF 設定について説明しています。関連する手順については、P.6-12 の「関連項目」を参照してください。

表 6-2　CAPF 設定

設定	説明
Certificate Operation	ドロップダウン ボックスから、次のオプションのいずれか 1 つを選択します。 • **No Pending Operation**：証明書の操作が発生しないときに表示されます（デフォルトの設定）。 • **Install/Upgrade**：電話機にローカルで有効な証明書を新しくインストールするか、あるいは既存の証明書をアップグレードします。 • **Delete**：電話機に存在するローカルで有効な証明書を削除します。 • **Troubleshoot**：ローカルで有効な証明書（LSC）または製造元でインストールされる証明書（MIC）を取得します。取得することで、CAPF トレース ファイルで証明書のクレデンシャルを確認できます。電話機に両方の種類の証明書が存在する場合、Cisco CallManager は証明書の種類ごとに 1 つずつ、2 つのトレース ファイルを作成します。 Troubleshoot オプションを選択すると、LSC または MIC が電話機に存在することを確認できます。 **ヒント**　電話機に証明書が存在しない場合、Delete オプションと Troubleshoot オプションは表示されません。
Authentication String	By Authentication String オプションを選択した場合に、このフィールドは適用されます。文字列を手動で入力するか、あるいは Generate String 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、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。
Generate String	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 Authentication String フィールドに表示されます。
Operation Completes by	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。 表示される値は、最初のノードに適用されます。
Operation Status	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、<operation type> pending、failed、successful などで、operating type には証明書操作オプションの Install/Upgrade、Delete、または Troubleshoot が表示されます。このフィールドに表示される情報は変更できません。

LSC ステータスまたは認証文字列に基づく電話機の検索

証明書操作ステータスまたは認証文字列に基づいて電話機を検索するには、次の手順を実行します。

手順

ステップ 1　Cisco CallManager Administration で **Device** > **Phone** の順に選択します。

ステップ 2　Find Phone where ドロップダウン リスト ボックスから、次のオプションのいずれか 1 つを選択します。

- **LSC Status**：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。
- **Authentication String**：このオプションを選択すると、Authentication String フィールドで指定された認証文字列を持つ電話機のリストが返されます。

ステップ 3　必要に応じて、Find Phone Where ドロップダウン リスト ボックスの横に表示されているドロップダウン リスト ボックスのオプションを選択して LSC ステータスまたは認証文字列の追加の検索基準を指定し、特定の検索基準を入力します。

ステップ 4　検索基準を指定した後、**Find** をクリックします。

ヒント　検索結果内の追加情報を検索するには、**Search Within Results** チェックボックスをオンにして、検索基準を入力し、**Find** をクリックします。

追加情報

詳細については、P.6-12 の「関連項目」を参照してください。

CAPF レポートの生成

必要に応じて CAPF レポートを生成し、証明書操作のステータス、認証文字列、セキュリティ プロファイル、認証モードなどを表示できます。レポートには、デバイス名、デバイスの説明、セキュリティ プロファイル、認証文字列、認証モード、LSC ステータスなどが含まれます。

CAPF レポートを生成するには、次の手順を実行します。

手順

ステップ 1　Cisco CallManager Administration で **Device > Phone** の順に選択します。

Find/List ウィンドウが表示されます。

ステップ 2　Find Phone Where ドロップダウン リスト ボックスで、次のオプションのいずれか 1 つを選択します。

- Device Name
- Device Description
- LSC Status
- Authentication String
- Security Profile

ヒント　必要に応じて、Find Phone Where ドロップダウン リスト ボックスの横に表示されているドロップダウン リスト ボックスのオプションを選択して追加の検索基準を指定し、特定の検索基準を入力します。

検索結果が表示されます。

ヒント　検索結果内の追加情報を検索するには、**Search Within Results** チェックボックスをオンにして、検索基準を入力し、**Find** をクリックします。

ステップ 3　Related Links ドロップダウン リスト ボックスで、**CAPF Report in File** を選択し、**Go** をクリックします。

ステップ 4　ファイルを任意の場所に保存します。

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

追加情報

詳細については、P.6-12 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

By Authentication String モードを選択して Cisco CallManager で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前に、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。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。電話機に認証文字列を入力する方法の詳細については、使用している電話機モデルおよびこのバージョンの Cisco CallManager をサポートする電話機のマニュアルを参照してください。

電話機に認証文字列を入力する前に、次の条件を満たしていることを確認します。

- CAPF 証明書が CTL ファイル内に存在する。
- P.6-6 の「Certificate Authority Proxy Function サービスのアクティブ化」の説明に従って、Cisco Certificate Authority Proxy Function サービスをアクティブにした。
- 最初のノードが実行中で、機能している。証明書のインストールごとにサーバが実行していることを確認します。
- 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 IP Phone の管理マニュアルを参照してください。

追加情報

詳細については、P.6-12 の「関連項目」を参照してください。

その他の情報

関連項目

- Certificate Authority Proxy Function の概要（P.6-2）
- Cisco IP Phone と CAPF の対話（P.6-3）
- CAPF システムの対話および要件（P.6-4）
- Cisco CallManager Serviceability での CAPF の設定（P.6-4）
- CAPF の設定用チェックリスト（P.6-5）
- Certificate Authority Proxy Function サービスのアクティブ化（P.6-6）
- CAPF サービス パラメータの更新（P.6-7）
- CAPF による電話機の証明書のインストール、アップグレード、トラブルシューティング、または削除（P.6-8）
- 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）

シスコの関連マニュアル

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

Cisco CallManager Serviceability のマニュアル

CHAPTER 7

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、機密性が高い設定情報が含まれます。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

電話機設定ファイルを暗号化するには、Cisco CallManager Administration のエンタープライズ パラメータを有効にし、Cisco CallManager Administration で追加作業を実行する必要があります。パラメータを有効にして、必要なサービスを Cisco CallManager Serviceability で再起動すると、TFTP サーバは暗号化されていないテキストの設定ファイルをすべて削除してから、設定ファイルの暗号化されたバージョンを生成します。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 True で、TFTP 暗号化設定が False に設定されている場合、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.7-9 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.7-4 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 CallManager の機能と、暗号化された設定ファイルをサポートするファームウェア ロードに依存します。暗号化された設定ファイルをサポートしないバージョンに電話機ファームウェアをダウングレードした場合、TFTP サーバは、最小限の設定内容を含む暗号化されていない設定ファイルを提供します。その結果、電話機が期待されるとおりに動作しない可能性があります。

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

Cisco CallManager は、次の方式をサポートします。

- 鍵の手動配布（P.7-2）
- 電話機の公開鍵によるシンメトリック鍵の暗号化（P.7-3）

「鍵の手動配布」および「電話機の公開鍵によるシンメトリック鍵の暗号化」の項の情報は、クラスタを Secure Mode に設定し、Cisco CallManager Administration の TFTP Encrypted Configuration 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.7-4 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 CallManager データベースに入力されている 128 ビットまたは 256 ビットのシンメトリック鍵によって、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.7-4 の「サポートされる電話機のモデル」を参照してください。

設定ファイルを更新するには、管理者が手動で鍵を Cisco CallManager Administration に入力するか、Cisco CallManager Administration 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、シンメトリック鍵は 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.7-4 の「サポートされる電話機のモデル」を参照してください。

電話機にシンメトリック鍵が含まれている場合、電話機は暗号化された設定ファイルを要求します。電話機は、TFTP サーバが署名した暗号化された設定ファイルをダウンロードします。

Cisco SIP IP Phone 7960 モデルおよび 7940 モデルは、設定ファイルの署名者を検証しません。フラッシュに格納されているシンメトリック鍵を使用して、ファイルの内容が復号化されます。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 Encrypted Configuration エンタープライズ パラメータを無効にした場合、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 からシンメトリック鍵を削除する必要があります。

電話機の公開鍵によるシンメトリック鍵の暗号化

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.7-4 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、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 By Authentication String でなければ、電話機は CAPF とのセッションを開始しようとします（By Authentication String の場合は、文字列を手動で入力する必要があります）。CAPF は、電話機の公開鍵を LSC または MIC から抽出し、MD5 ハッシュを生成し、公開鍵および証明書ハッシュの値を Cisco CallManager データベースに格納します。公開鍵がデータベースに格納された後、電話機はリセットされ、新しい設定ファイルが要求されます。

公開鍵がデータベースに存在するようになり、電話機がリセットされた後、電話機用の公開鍵があることをデータベースが TFTP に通知すると、シンメトリック鍵暗号化処理が開始されます。TFTP サーバは 128 ビット シンメトリック鍵を生成します。これによって、設定ファイルは Advanced Encryption Standard（AES）128 暗号化アルゴリズムで暗号化されます。次に、電話機の公開鍵でシンメトリック鍵が暗号化され、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、暗号化されたシンメトリック鍵を復号化します。次に、シンメトリック鍵によって、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　電話機の公開鍵を使用したシンメトリック鍵の暗号化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 Encrypted Configuration エンタープライズ パラメータが無効の場合、Cisco IP Phone 7911、7941、7961、7970、および 7971 モデルが暗号化されたファイル（.enc.sgn ファイル）を要求すると、Cisco CallManager は「file not found error」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 Encrypted Configuration エンタープライズ パラメータが有効の場合、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。

サポートされる電話機のモデル

次の電話機モデルで、電話機設定ファイルを暗号化できます。

- Cisco SIP IP Phone 7905 または 7912：鍵の手動配布をサポート。

  シンメトリック鍵は RC4 暗号化アルゴリズムを使用し、鍵サイズは 256 ビットです。これらの SIP 電話機モデルは、ファイル署名をサポートしません。

- Cisco SIP IP Phone 7940 または 7960：鍵の手動配布をサポート。

  シンメトリック鍵は Advanced Encryption Standard（AES）128 暗号化アルゴリズムを使用し、鍵サイズは 128 ビットです。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しますが、署名情報を無視します。

- Cisco SIP IP Phone 7970 または 7971、Cisco SIP IP Phone 7941 または 7961、Cisco SIP IP Phone 7911、Cisco IP Phone 7970 または 7971、Cisco IP Phone 7941 または 7961、Cisco IP Phone 7911：電話機の公開鍵によるシンメトリック鍵の暗号化をサポート。

  シンメトリック鍵は AES 128 暗号化アルゴリズムを使用し、鍵サイズは 128 ビットです。これらの電話機は、ファイル署名をサポートします。

暗号化設定ファイルの設定用チェックリスト

電話機設定ファイルを暗号化するには、表 7-1 で示す作業を実行する必要があります。

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	Cluster Security Mode が Secure Mode に設定されていることを確認します。	Cisco CTL クライアントの設定（P.3-1）
ステップ 2	Cisco CallManager Administration の TFTP Encrypted Configuration エンタープライズ パラメータを有効にします。	電話機設定ファイルの暗号化エンタープライズ パラメータの有効化（P.7-6）
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シンメトリック鍵の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.7-4）
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、Cisco CallManager Administration で、鍵の手動配布の作業を実行します。	• 鍵の手動配布の設定（P.7-6） • 鍵の手動配布の設定内容（P.7-7）
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、電話機にシンメトリック鍵を入力し、電話機をリセットします。	電話機でのシンメトリック鍵の入力（P.7-7）
ステップ 6	使用中の電話機が、電話機の公開鍵によるシンメトリック鍵の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。	• 電話機の公開鍵によるシンメトリック鍵の暗号化の使用（P.7-8） • 電話機設定ファイルの暗号化について（P.7-2） • 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エンタープライズ パラメータの有効化

電話機設定ファイルを暗号化する前に、Cisco CallManager Administration の TFTP Encrypted Configuration エンタープライズ パラメータを有効にする必要があります。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せます。エンタープライズ パラメータが有効の場合、TFTP サーバは暗号化された設定ファイルを構築します。

Cisco CallManager Administration のエンタープライズ パラメータにアクセスするには、**System** > **Enterprise Parameters** の順に選択します。

デフォルト値など、エンタープライズ パラメータの詳細については、Enterprise Parameters Configuration ウィンドウに表示されている TFTP Encrypted Configuration リンクをクリックします。

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.7-4 の「サポートされる電話機のモデル」を参照してください。

鍵の手動配布を設定するには、次の手順を実行します。この手順では、電話機が Cisco CallManager データベースに存在し、互換性のあるファームウェア ロードが TFTP サーバに存在し、Cisco CallManager Administration の TFTP Encrypted Configuration エンタープライズ パラメータが有効であることを前提としています。

手順

ステップ 1　『*Cisco CallManager アドミニストレーション ガイド*』の説明に従って、電話機を検索します。

ステップ 2　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。鍵を設定した後は、変更できません。

ステップ 3　**Save** をクリックします。

ステップ 4　電話機にシンメトリック鍵を入力し、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.7-9 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、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。関連する手順については、P.7-9 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
Symmetric Key	シンメトリック鍵として使用する 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。 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 CallManager は入力された値を拒否します。Cisco CallManager は、次の鍵サイズをサポートします。 • Cisco IP Phone 7905 モデルおよび 7912 モデル（SIP プロトコルのみ）：256 ビット • Cisco IP Phone 7940 モデルおよび 7960 モデル（SIP プロトコルのみ）：128 ビット 鍵を設定した後は、変更できません。
Generate String	Cisco CallManager Administration で 16 進文字列を生成するには、**Generate String** ボタンをクリックします。 鍵が生成された後は、変更できません。
Revert to Database Value	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。

電話機でのシンメトリック鍵の入力

Cisco CallManager Administration で鍵の手動配布を設定した後、電話機にシンメトリック鍵を入力する方法については、使用中の電話機モデルおよびプロトコルをサポートする Cisco 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。

電話機の公開鍵によるシンメトリック鍵の暗号化の使用

使用中の電話機が、電話機の公開鍵によるシンメトリック鍵の暗号化をサポートしているかどうかを判別するには、P.7-4 の「サポートされる電話機のモデル」を参照してください。この方式を使用するには、次の作業を実行します。この作業では、Cisco CallManager データベースに電話機が存在し、Cisco CallManager Administration の TFTP Encrypted Configuration エンタープライズ パラメータが有効である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。証明書が存在しない場合は、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 2　CAPF 設定を定義した後、**Save** をクリックします。

ステップ 3　Phone Configuration ウィンドウで、**Reset** をクリックします。

追加情報

詳細については、P.7-9 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 IP Phone 7905 モデルおよび 7912 モデル（SIP プロトコルのみ）：LD <MAC>.x
- Cisco IP Phone 7940 モデルおよび 7960 モデル（SIP プロトコルのみ）：SIP<MAC>.cnf.enc.sgn
- Cisco IP Phone 7970 モデルおよび 7971 モデル（SIP プロトコルのみ）：SIP<MAC>.cnf.xml.enc.sgn
- Cisco IP Phone 7970 モデルおよび 7971 モデル（SCCP プロトコルのみ）：SEP<MAC>.cnf.xml.enc.sgn

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 CallManager Administration の TFTP Encrypted Configuration エンタープライズ パラメータを更新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 True で、TFTP 暗号化設定が False に設定されている場合、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。**

エンタープライズ パラメータを更新した後、電話機の鍵は Cisco CallManager データベースに残ります。

Cisco IP Phone 7911、7941、7961、7970、および 7971 モデル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 false に更新すると、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 IP SIP Phone 7940/7960/7905/7912 モデル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 false に更新したときは、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 でシンメトリック鍵を削除する必要があります。

ヒント　Cisco IP SIP Phone 7940 モデルおよび 7960 モデルでは、電話機 GUI でシンメトリック鍵として 32 バイトの 0 を入力して、暗号化を無効にします。Cisco IP SIP Phone 7905 モデルおよび 7912 モデルでは、電話機 GUI でシンメトリック鍵を削除して、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。

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.7-4）
- 暗号化設定ファイルの設定用チェックリスト（P.7-5）
- 電話機設定ファイルの暗号化エンタープライズ パラメータの有効化（P.7-6）
- 鍵の手動配布の設定（P.7-6）
- 鍵の手動配布の設定内容（P.7-7）
- 電話機でのシンメトリック鍵の入力（P.7-7）
- 電話機の公開鍵によるシンメトリック鍵の暗号化の使用（P.7-8）
- 電話機設定ファイルが暗号化されていることの確認（P.7-8）
- 電話機設定ファイルの暗号化の無効化（P.7-9）
- Certificate Authority Proxy Function の使用方法（P.6-1）

シスコの関連マニュアル

- *Cisco Bulk Administration Tool Guide*
- 電話機のモデルおよびプロトコルに対応した Cisco IP Phone アドミニストレーション ガイド

■　その他の情報

SIP 電話機のダイジェスト認証の設定

SIP 電話機にダイジェスト認証を設定すると、電話機が SIP 要求を Cisco CallManager に送信するたびに、Cisco CallManager は電話機の ID でチャレンジを行います。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.1-17 の「ダイジェスト認証」を参照してください。

この章は、次の内容で構成されています。

SIP 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。**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	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。	• 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	Phone Configuration ウィンドウで Digest User を選択します。 Cisco 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。	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 SIP IP Phone 7940 モデルまたは 7960 モデルでは、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。	『*Cisco CallManager セキュリティ ガイド*』では、電話機でダイジェスト認証クレデンシャルを入力する手順について説明しません。この作業の実行方法については、使用している電話機のモデルとこのバージョンの Cisco CallManager をサポートする Cisco 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。

ダイジェスト認証サービス パラメータの設定

Cisco CallManager サービスをサポートする SIP Realm Station サービス パラメータは、Cisco CallManager が 401 Unauthorized メッセージに対応して SIP 電話機でチャレンジを行うときに、realm フィールドで使用する文字列を指定します。パラメータの詳細については、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 CallManager Administration で、**System > Service Parameters** 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、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　Service ドロップダウン リスト ボックスから、**Cisco CallManager** サービスを選択します。サービス名の横に Active と表示されていることを確認します。

ステップ 4　ヘルプの説明に従って、**SIP Realm Station** パラメータを更新します。CAPF サービス パラメータのヘルプを表示するには、疑問符またはパラメータ名リンクをクリックします。

ステップ 5　**Save** 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。

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 CallManager データベースにエンド ユーザが存在することを前提としています。エンド ユーザのダイジェスト クレデンシャルを設定するには、次の手順を実行します。

手順

ステップ 1　『*Cisco CallManager アドミニストレーション ガイド*』の説明に従って、エンド ユーザを検索します。

ステップ 2　目的の 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　**Save** 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

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、Cisco CallManager Administration の 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 SIP IP Phone 7960 または 7940 の 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、Cisco CallManager Administration の 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。

表 8-2　ダイジェスト クレデンシャル

設定	説明
Digest Credentials	英数字文字列を入力します。
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。

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 CallManager アドミニストレーション ガイド*』の説明に従って、電話機を検索します。

ステップ 2　目的の Phone Configuration ウィンドウが表示されたら、**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　**Save** をクリックします。

ステップ 4　**Reset** をクリックします。

エンド ユーザを電話機に関連付け、設定を保存し、電話機をリセットした後、Cisco CallManager は、その電話機からのすべての SIP 要求でチャレンジを行います。Cisco CallManager は、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 CallManager は、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。

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.1-17）
- 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）
- 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）
- 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

使用中の電話機モデルおよびこのバージョンの Cisco CallManager をサポートする Cisco IP Phone アドミニストレーション ガイド

その他の情報

電話機のセキュリティ強化

電話機のセキュリティを強化するには、Cisco CallManager Administration の 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

デフォルトで Cisco 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、Cisco CallManager Administration の 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サビリティ 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 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。Cisco CallManager Administration の 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 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 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 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 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 IP Phone の Settings 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。Cisco CallManager Administration の Phone Configuration ウィンドウで Setting Access 設定を無効にすると、電話機で Settings 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、Ring Type、Network Configuration、Model Information、および Status 設定があります。

これらの設定は、Cisco CallManager Administration の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 Volume 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、Ring Type、Network Configuration、Model Information、Status、および Volume 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 CallManager Administration で Setting Access 設定を有効にする必要があります。

PC Port 設定の無効化

デフォルトで Cisco CallManager は、PC ポートのあるすべての Cisco IP Phone 上で PC ポートを有効にします。必要に応じて、Cisco CallManager Administration の 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 CallManager Administration で **Device > Phone** 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 **Find** 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 **Find** 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 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 Setting

ヒント　これらの設定に関する情報を確認するには、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　**Save** をクリックします。

ステップ 7　**Reset** をクリックします。

追加情報

詳細については、P.9-4 の「関連項目」を参照してください。

その他の情報

関連項目

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

シスコの関連マニュアル

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

CHAPTER 10

ボイス メッセージング 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 メッセージングのセキュリティの概要

Cisco CallManager ボイス メッセージング ポートおよび Cisco Unity SCCP デバイスに対してセキュリティを設定すると、各デバイスが他のデバイスの証明書を受け入れた後に、認証済みデバイスに対して TLS 接続（ハンドシェイク）が開始されます。また、システムはデバイス間で SRTP ストリームを送信します。これは、デバイスで暗号化を設定した場合です。

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 CallManager TLS ポートを介して Cisco CallManager に接続します。デバイス セキュリティ モードがノンセキュアになっている場合、Cisco Unity TSP は Cisco CallManager SCCP ポートを介して Cisco CallManager に接続します。

セキュリティを設定する前に、次の情報を考慮してください。

- このマニュアルでは、サーバという用語は Cisco CallManager クラスタ内のサーバを意味します。ボイスメール サーバという用語は Cisco Unity サーバを意味します。
- このバージョンの Cisco CallManager では Cisco Unity 4.0(5) 以降を実行する必要があります。
- Cisco Unity Telephony Integration Manager を使用して Cisco Unity のセキュリティ タスクを実行する必要があります。これらのタスクの実行方法は、『*Cisco CallManager 5.0 Integration Guide for Cisco Unity 4.x*』を参照してください。
- この章で説明する手順に加えて、Cisco IP Telephony Platform Administration 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入れる必要があります。この作業の詳細については、『*Cisco IP Telephony Platform Administration Guide*』を参照してください。

  証明書をコピーした後、クラスタ内の各サーバで Cisco CallManager サービスを再起動する必要があります。
- Cisco Unity 証明書が失効した、または何らかの理由で変更された場合は、Cisco IP Telephony Platform Administration 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 メッセージングは Cisco CallManager に登録できないため機能しません。
- Cisco Unity Telephony Integration Manager で指定する設定は、Cisco CallManager Administration で設定されているボイス メッセージング 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。SCCP 電話機セキュリティ プロファイルをポートに適用するときに、Cisco CallManager Administration でデバイス セキュリティ モードをボイス メッセージング ポートに適用します。

ヒント　デバイス セキュリティ モードの設定が Cisco CallManager と Cisco Unity で一致しない場合は、Cisco Unity ポートが Cisco CallManager に登録できず、Cisco Unity はそれらのポートでコールを受け入れることができません。

- ポートのセキュリティ プロファイルを変更するには、Cisco CallManager デバイスをリセットして Cisco Unity ソフトウェアを再起動する必要があります。Cisco CallManager Administration で、以前のプロファイルと異なるデバイス セキュリティ モードを使用するセキュリティ プロファイルを適用する場合は、Cisco Unity の設定を変更する必要があります。
- セキュリティ プロファイルをポートに適用するとき、Cisco CallManager は、プロファイルに対して存在する Certificate Authority Proxy Function（CAPF）設定を無視します。ボイス メッセージング ポートはこれらの設定をサポートしません。CAPF 設定ではなく、デバイス セキュリティ モードに基づいてプロファイルが選択されます。
- SCCP 電話機セキュリティ プロファイルで定義する設定の詳細については、P.5-1 の「電話機セキュリティ プロファイルの設定」を参照してください。

ボイス メッセージング ポートのセキュリティ設定用チェックリスト

ボイス メッセージング ポートのセキュリティを設定する場合は、表 10-1 を参照してください。

表 10-1　ボイス メッセージング 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 Client をセキュア 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）
ステップ 3	Cisco IP Telephony Platform Administration の証明書管理機能を使用して、クラスタ内の各サーバの信頼ストアに Cisco Unity 証明書をコピーします。次に、各サーバで Cisco CallManager サービスを再起動します。	• ボイス メッセージングのセキュリティの概要（P.10-2） • *Cisco IP Telephony Platform Administration Guide* • *Cisco CallManager Serviceability アドミニストレーション ガイド*
ステップ 4	Cisco CallManager Administration で、ボイス メッセージング ポートのセキュリティ プロファイルを設定し、プロファイルをポートに適用します。	• 単一ボイス メッセージング ポートへのセキュリティ プロファイルの適用（P.10-4） • Voice Messaging Port Wizard でのセキュリティ プロファイルの適用（P.10-5）
ステップ 5	Cisco Unity ボイス メッセージング 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 CallManager 5.0 Integration Guide for Cisco Unity 4.x*
ステップ 6	Cisco CallManager Administration 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。	• *Cisco CallManager 5.0 Integration Guide for Cisco Unity 4.x* • 単一ボイス メッセージング ポートへのセキュリティ プロファイルの適用（P.10-4）

単一ボイス メッセージング 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 メッセージング 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 メッセージングのセキュリティの概要（P.10-2）
- ボイス メッセージング ポートのセキュリティ設定用チェックリスト（P.10-3）

手順

ステップ 1　『*Cisco CallManager アドミニストレーション ガイド*』の説明に従って、ボイス メッセージング 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、**SCCP Phone Security Profile** 設定を見つけます。ドロップダウン リスト ボックスから、ポートに適用するプロファイルを選択します。

ステップ 3　**Save** をクリックします。

ステップ 4　**Reset** をクリックします。

追加情報

詳細については、P.10-6 の「関連項目」を参照してください。

Voice Messaging Port Wizard でのセキュリティ プロファイルの適用

Voice Messaging Port Wizard で既存のボイス メッセージング サーバの SCCP 電話機セキュリティ プロファイル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。

既存のボイスメール サーバのセキュリティ設定を変更する方法は、P.10-4 の「単一ボイス メッセージング 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 メッセージングのセキュリティの概要（P.10-2）
- ボイス メッセージング ポートのセキュリティ設定用チェックリスト（P.10-3）

Voice Messaging Port Wizard で新規ボイスメール サーバに SCCP 電話機セキュリティ プロファイル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 CallManager Administration で、**Voice Messaging > Voice Messaging Port Wizard** を選択します。

ステップ 2　新規ボイスメール　サーバにポートを追加するには、該当するオプション　ボタンをクリックして **Next** をクリックします。

ステップ 3　ボイスメール サーバの名前を入力し、**Next** をクリックします。

ステップ 4　追加するポートの数を選択して、**Next** をクリックします。

ステップ 5　Device Information ウィンドウで、SCCP Phone Security Profile ドロップダウン リスト ボックスから、適用するプロファイルを選択します。『*Cisco CallManager アドミニストレーション ガイド*』の説明に従って、その他のデバイス設定を実行します。**Next** をクリックします。

ステップ 6　『*Cisco CallManager アドミニストレーション ガイド*』の説明に従って、設定プロセスを続行します。Summary ウィンドウが表示されたら、**Finish** をクリックします。

追加情報

詳細については、P.10-6 の「関連項目」を参照してください。

その他の情報

関連項目

- システム要件（P.1-4）
- 対話および制限（P.1-6）
- 証明書の種類（P.1-13）
- 設定用チェックリストの概要（P.1-23）
- ボイス メッセージングのセキュリティの概要（P.10-2）
- 単一ボイス メッセージング ポートへのセキュリティ プロファイルの適用（P.10-4）
- Voice Messaging Port Wizard でのセキュリティ プロファイルの適用（P.10-5）

シスコの関連マニュアル

- *Cisco CallManager 5.0 Integration Guide for Cisco Unity 4.x*
- *Cisco IP Telephony Platform Administration Guide*

PART 3

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

CHAPTER 11

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 CallManager Administration 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 CallManager Administration で使用できる Cisco JTAPI または TSP プラグインのインストール方法や、インストール中にセキュリティ パラメータを設定する方法は説明しません。同じく、このマニュアルでは、CTI 制御デバイスまたは回線に制限を設定する方法も説明しません。

この章は、次の内容で構成されています。

CTI、JTAPI、および TAPI アプリケーションの認証について

Cisco CallManager 5.0 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 Cluster Security Mode が Secure Mode 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、ノンセキュア ポートであるポート 2748 で接続されます。

CTIManager とアプリケーションは、相互認証 TLS ハンドシェーク（証明書交換）で相手の ID を確認します。TLS 接続が発生すると、CTIManager とアプリケーションは、TLS ポート（ポート 2749）で QBE メッセージを交換します。

アプリケーションとの認証を行うために、CTIManager は、Cisco CallManager 5.0 のインストール時に Cisco CallManager サーバに自動的にインストールされる Cisco CallManager 自己署名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、CTL ファイルを生成した後、この証明書が自動的に CTL ファイルに追加されます。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 ファイルを更新し、JTAPI/TSP クライアントがこのファイルを TFTP サーバからダウンロードした後、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、新しい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 CallManager 自己署名証明書と CAPF サーバ証明書が含まれます。

CTL ファイルが侵害されていると判断された場合、JTAPI/TSP クライアントはダウンロードした CTL ファイルを置き換えません。クライアントはエラーをログに記録し、既存の CTL ファイルにある古い証明書を使用して、TLS 接続の確立を試行します。CTL ファイルが変更または侵害されている場合、正常に接続できない可能性があります。CTL ファイルのダウンロードに失敗し、複数の TFTP サーバが存在する場合、P.3-1 の「Cisco CTL クライアントの設定」で説明するように、別の TFTP サーバでファイルをダウンロードするように設定できます。JTAPI/TAPI クライアントは、次の条件下では、どのポートにも接続しません。

- 何らかの理由でクライアントが CTL ファイルをダウンロードできない（CTL ファイルが存在しないなど）
- クライアントに既存の CTL ファイルがない
- アプリケーション ユーザをセキュア CTI ユーザとして設定した

CTIManager との認証を行うために、アプリケーションは、Cisco CallManager の Certificate Authority Proxy Function（CAPF）が発行する証明書を使用します。アプリケーションと CTIManager とのすべての接続で TLS を使用するには、アプリケーション PC で実行されるインスタンスごとに一意の証明書が必要です。たとえば、Cisco IPMA が、クラスタ内の 2 つの異なるノードで 2 つのサービス インスタンスを実行している場合、各インスタンスに独自の証明書が必要です。1 つの証明書ですべてのインスタンスがカバーされるわけではありません。IPMA サービスを実行しているノードに証明書がインストールされるようにするには、表 11-2 の説明に従い、Cisco CallManager Administration 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。

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

アプリケーションと CTIManager の間のメディア ストリームを保護するには、Cisco CallManager Administration で、アプリケーション ユーザまたはエンド ユーザを Standard CTI Allow Reception of SRTP Key Material ユーザ グループに追加する必要があります。クラスタ セキュリティ モードが Secure Mode の場合、アプリケーション ユーザおよびエンド ユーザをこのグループと Standard CTI Secure Connection ユーザ グループに追加すると、CTIManager はアプリケーションとの TLS 接続を確立し、メディア イベントでアプリケーションに鍵関連情報を提供します。アプリケーションは SRTP 鍵関連情報を記録または格納しませんが、鍵関連情報を使用して RTP ストリームを暗号化し、CTIManager からの SRTP ストリームを復号化します。アプリケーションが SRTP 鍵関連情報を記録または格納しないことに注意してください。

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

ヒント アプリケーション 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 グループに存在することを確認します。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 CallManager は、CTI ポートおよびルート ポイントで送受信されるセキュア コールを円滑にしますが、アプリケーションがメディア パラメータを処理するため、アプリケーションがセキュア コールをサポートするように設定する必要があります。CTI ポートやルート ポイントは、ダイナミック登録またはスタティック登録で登録されます。ポートやルート ポイントがダイナミック登録を使用する場合、メディア パラメータはコールごとに指定されます。スタティック登録の場合、メディア パラメータは登録時に指定され、コールごとに変更することはできません。CTI ポートやルート ポイントが TLS 接続を介して CTIManager に登録される場合、デバイスは安全に登録されます。このとき、アプリケーションが有効な暗号化アルゴリズムを使用し、相手がセキュアであれば、メディアは SRTP で暗号化されます。

CTI アプリケーションが、すでに確立されているコールの監視を開始するとき、アプリケーションは RTP イベントを受信しません。確立されたコールに対して、CTI アプリケーションは、コールのメディアがセキュアかノン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 CallManager と共に自動的にインストールされ、設定に応じて次の CTI/TAPI/TAPI アプリケーション用のタスクを実行します。

- 認証文字列によって JTAPI/TSP クライアントを認証する。
- CTI/JTAPI/TAPI アプリケーション ユーザまたはエンド ユーザに、ローカルで有効な証明書（LSC）を発行する。
- 既存のローカルで有効な証明書をアップグレードする。
- 証明書を表示およびトラブルシューティングするために取得する。

JTAPI/TSP クライアントが CAPF と対話するとき、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。

Application User CAPF Profile Configuration ウィンドウまたは 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 CallManager がサポートする CAPF プロファイルの違いについて説明します。

- アプリケーション ユーザ CAPF プロファイル：このプロファイルを使用すると、セキュア アプリケーション ユーザにローカルで有効な証明書を発行できます。証明書を発行し、その他のセキュリティ関連作業を実行すると、CTIManager サービスとアプリケーションの間で、TLS 接続が開始されます。

  1 つのアプリケーション ユーザ CAPF プロファイルが、サーバのサービスまたはアプリケーションの 1 つのインスタンスに対応します。たとえば、クラスタ内の 2 つのサーバでサービスまたはアプリケーションをアクティブにする場合は、サーバごとに 1 つずつ、合計 2 つのアプリケーション ユーザ CAPF プロファイルを設定する必要があります。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、たとえば、合計 2 つのアプリケーション ユーザ CAPF プロファイルを設定する必要があります。
- エンド ユーザ CAPF プロファイル：このプロファイルを使用すると、CTI クライアントにローカルで有効な証明書を発行できます。証明書を発行し、その他のセキュリティ関連作業を実行すると、CTI クライアントは TLS 接続で CTIManager サービスと通信します。

ヒント　JTAPI クライアントは LSC を Java Key Store 形式で、JTAPI Preferences 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 システムの対話および要件

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。Cisco CTL クライアントで Cluster Security Mode が Secure Mode に設定されていることを確認します。
- CAPF を使用するには、最初のノードで Cisco Certificate Authority Proxy Function サービスをアクティブにする必要があります。
- 同時に多数の証明書が生成されると、コール処理が中断される場合があるため、スケジューリングされたメンテナンス画面で CAPF を使用することを強く推奨します。
- 証明書操作の間、最初のノードが実行中で正しく機能していることを確認します。
- 証明書操作の間、CTI/ JTAPI/TAPI アプリケーションが正しく機能していることを確認します。

CTI、JTAPI、および TAPI のセキュリティ設定用チェックリスト

表 11-1 に、CTI/JTAPI/TAPI アプリケーションを保護するために実行する作業のリストを示します。

表 11-1　CTI/JTAPI/TAPI のセキュリティ設定用チェックリスト

設定手順		関連手順および関連項目
ステップ 1	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。 **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。	• 『*Cisco CallManager システム ガイド Release 5.0*』の「コンピュータ テレフォニー統合」 • *Cisco JTAPI インストレーション ガイド for Cisco CallManager 5.0* • *Cisco TAPI インストレーション ガイド for Cisco CallManager 5.0* • *Cisco CallManager アドミニストレーション ガイド Release 5.0*
ステップ 2	次の CallManager セキュリティ機能がインストールされていることを確認します（インストールされていない場合は、これらの機能をインストールして設定します）。 • 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。 **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。 • クラスタ セキュリティ モードが Secure Mode に設定されていることを確認します。 **ヒント** クラスタ セキュリティ モードが Secure Mode 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。	• 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.11-11） • *Cisco CallManager アドミニストレーション ガイド*
ステップ 3	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。 **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すが、両方に割り当てることはできません。	セキュリティ関連ユーザ グループへのアプリケーション ユーザおよびエンド ユーザの追加（P.11-9）

表 11-1　CTI/JTAPI/TAPI のセキュリティ設定用チェックリスト（続き）

設定手順		関連手順および関連項目
ステップ 4	SRTP を使用して CTIManager とアプリケーションの間のメディア ストリームを保護する場合は、アプリケーション ユーザまたはエンド ユーザを Standard CTI Allow Reception of SRTP Key Material ユーザ グループに追加します。 アプリケーション ユーザまたはエンド 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 グループに存在することを確認します。これが、TLS および SRTP 接続の基本設定になります。これらのグループにユーザを追加した後、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。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。 Cisco IPMA、Cisco QRT、および Cisco WebDialer は暗号化をサポートしません。CTIManager サービスに接続する CTI クライアントは、クライアントが音声パケットを送信する場合、暗号化をサポートしないことがあります。	セキュリティ関連ユーザ グループへのアプリケーション ユーザおよびエンド ユーザの追加（P.11-9） 『*Cisco CallManager アドミニストレーション ガイド*』の「ロールの設定」
ステップ 5	Cisco CallManager Administration 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。	• CTI、JTAPI、および TAPI アプリケーションに対する CAPF の概要（P.11-5） • アプリケーション　ユーザまたはエンド ユーザの CAPF プロファイルの設定（P.11-13） • Application User CAPF Profile ウィンドウおよび End User CAPF Profile ウィンドウの CAPF 設定（P.11-14）
ステップ 6	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。	JTAPI/TAPI セキュリティ関連サービス パラメータ（P.11-17）

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 CallManager Administration に表示されます。これらのグループは削除できません。

アプリケーション ユーザまたはエンド ユーザが CTIManager と通信するときに TLS 接続を使用するようにするには、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、両方に割り当てることはできません。

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

ヒント　アプリケーション　ユーザまたはエンド　ユーザをユーザ　グループから削除する方法については、『*Cisco CallManager アドミニストレーション ガイド*』を参照してください。Role Configuration ウィンドウのセキュリティ関連設定の詳細については、『*Cisco CallManager アドミニストレーション ガイド*』を参照してください。

手順

ステップ 1　Cisco CallManager Administration で **User Management > User Groups** 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、**Find** 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　**Add Application Users to Group** 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、検索基準を指定し、**Find** をクリックします。

検索基準を指定せずに Find 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、**Add Selected** をクリックします。

User Group 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　**Add Users to Group** 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、検索基準を指定し、**Find** をクリックします。

検索基準を指定せずに Find 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、**Add Selected** をクリックします。

User Group ウィンドウにユーザが表示されます。

追加情報

詳細については、P.11-18 の「関連項目」を参照してください。

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

Cisco CallManager 5.0(1) では、Cisco CallManager Serviceability で Certificate Authority Proxy Function サービスが自動的にアクティブになりません。Certificate Authority Proxy Function サービスのアクティブ化の詳細については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』を参照してください。

CAPF 機能を使用するには、最初のノードでこのサービスをアクティブにする必要があります。Cisco CTL クライアントをインストールして設定する前にこのサービスをアクティブにしなかった場合は、P.3-12 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 に固有な鍵のペアおよび証明書が CAPF によって自動生成されます。CAPF 証明書は Cisco CTL クライアントによってクラスタ内のすべてのサーバにコピーされ、拡張子 .0 を使用します。CAPF 証明書が存在することを確認するには、Cisco IPT Platform 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 Service Parameter 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。

ヒント このリリースの Cisco CallManager は、SCEP または Microsoft CA や Keon CA などサードパーティの CA 署名付き LSC 証明書をサポートしません。サードパーティ証明書のサポートは、将来のリリースで予定されています。現在、サードパーティ CA を使用している場合は、5.0 に移行する前に、有効期間が長い（6 か月以上の）証明書を再発行し、サードパーティ証明書がサポートされる前に失効しないようにしてください。

CAPF サービス パラメータが、Cisco CallManager Administration で Active として表示されるようにするには、Cisco CallManager Serviceability で、Certificate Authority Proxy Function サービスをアクティブにする必要があります。

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

CAPF サービス パラメータを更新するには、次の手順を実行します。

手順

ステップ 1　Cisco CallManager Administration で、**System > Service Parameters** 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、最初のノードを選択します。

ステップ 3　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 CallManager Serviceability で Cisco Certificate Authority Proxy Function サービスを再起動する必要があります。

追加情報

詳細については、P.11-18 の「関連項目」を参照してください。

アプリケーション ユーザまたはエンド ユーザの CAPF プロファイルの検索

アプリケーション ユーザまたはエンド ユーザの CAPF プロファイルを検索するには、次の手順に従います。

手順

ステップ 1　アクセスするプロファイルに応じて、Cisco CallManager Administration で次のオプションのどちらかを選択します。

- **User Management > Application User CAPF Profile**
- **User Management > End User CAPF Profile**

Find and List ウィンドウが表示されます。

ステップ 2　ドロップダウン リスト ボックスから、表示するプロファイルの検索基準を選択し、**Find** をクリックします。

（注）　データベースに登録されているすべてのアプリケーション ユーザ CAPF プロファイルまたはエンド ユーザ CAPF プロファイルを検索するには、検索基準を指定せずに、**Find** をクリックします。

ウィンドウが更新され、検索基準と一致するプロファイルが表示されます。

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

ヒント　検索結果の中で Instance ID、Application User（アプリケーション ユーザ CAPF プロファイルのみ）、または End User ID（エンド ユーザ CAPF プロファイルのみ）を検索するには、**Search Within Results** チェックボックスをオンにし、この手順の説明に従って検索基準を入力し、**Find** をクリックします。

追加情報

詳細については、P.11-18 の「関連項目」を参照してください。

アプリケーション ユーザまたはエンド ユーザの CAPF プロファイルの設定

JTAPI/TAPI/CTI アプリケーションのローカルで有効な証明書をインストール、アップグレード、またはトラブルシューティングする場合は、表 11-2 を参照してください。

ヒント　次の手順は、アプリケーション ユーザ CAPF プロファイルとエンド ユーザ CAPF プロファイルの両方をサポートしますが、両方を同時に設定することはできません。エンド ユーザ CAPF プロファイルを設定する前に、アプリケーション ユーザ CAPF プロファイルを設定することが推奨されます。

手順

ステップ 1　Cisco CallManager Administration で、次のオプションのどちらかを選択します。

- **User Management > Application User CAPF Profile**
- **User Management > End User CAPF Profile**

ステップ 2　Find/List Application User CAPF Profile Configuration ウィンドウまたは Find/List End User CAPF Profile Configuration ウィンドウが表示されたら、次の作業のどちらかを実行します。

- 既存のアプリケーション ユーザ CAPF プロファイルまたはエンド ユーザ CAPF プロファイルを検索するには、検索基準を指定し、**Find** をクリックします。
  検索基準を指定せずに Find をクリックすると、システムにあるすべてのアプリケーション ユーザ CAPF プロファイルまたはエンド ユーザ CAPF プロファイルが表示されます。
- 新し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 プロファイルを追加するには、**Add New** をクリックします。

ステップ 3　CAPF Profile プロファイル設定ウィンドウが表示されたら、表 11-2 の説明に従って、設定内容を入力します。

ステップ 4　**Save** 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

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.11-17 の「JTAPI/TAPI セキュリティ関連サービス パラメータ」の説明に従って、サービス パラメータを設定する必要があります。

追加情報

詳細については、P.11-18 の「関連項目」を参照してください。

Application User CAPF Profile ウィンドウおよび End User CAPF Profile ウィンドウの CAPF 設定

表 11-2 で、Cisco CallManager Administration の Application User CAPF Profile ウィンドウおよび End User CAPF Profile ウィンドウの CAPF 設定について説明します。関連する手順については、P.11-18 の「関連項目」を参照してください。

表 11-2　アプリケーション ユーザ CAPF プロファイルおよびエンド ユーザ CAPF プロファイルの設定内容

設定	説明
Application User	この設定には、Application User ウィンドウに存在するユーザが表示されます。ドロップダウン リスト ボックスから、CAPF 操作を実行する対象のアプリケーション ユーザを選択します。 この設定は、End User CAPF Profile ウィンドウには表示されません。
End User	この設定には、End User ウィンドウに存在するユーザが表示されます。ドロップダウン リスト ボックスから、CAPF 操作を実行する対象のエンド ユーザを選択します。 この設定は、Application User CAPF Profile ウィンドウには表示されません。
Instance ID	クラスタでは、アプリケーションの複数の接続（インスタンス）を実行できます。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（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。たとえば、クラスタの 2 つのサーバでサービスまたはアプリケーションのインスタンスが 2 つ実行されている場合、各インスタンスに独自の証明書が必要です。 CAPF は、Application User または End User と Instance ID の設定を使用して、証明書操作を実行する場所を判別します。設定しているアプリケーション ユーザまたはエンド ユーザに対して、a ～ z、A ～ Z、ダッシュ（-）、アンダースコア（_）、またはピリオド（.）を使用して、一意の文字列を入力します。 このフィールドは、Web サービスおよびアプリケーションをサポートする CAPF Profile Instance ID for Secure Connection to CTIManager サービス パラメータに関係があります。このパラメータにアクセスする方法については、P.11-17 の「JTAPI/TAPI セキュリティ関連サービス パラメータ」を参照してください。
Certificate Operation	ドロップダウン ボックスから、次のオプションのいずれか 1 つを選択します。 • **No Pending Operation**：証明書の操作が発生しないときに表示されます（デフォルトの設定）。 • **Install/Upgrade**：アプリケーションのローカルで有効な証明書を新しくインストールするか、あるいは既存の証明書をアップグレードします。

表 11-2　アプリケーション ユーザ CAPF プロファイルおよびエンド ユーザ CAPF プロファイルの設定内容（続き）

設定	説明
Authentication Mode	認証モードは、指定された証明書操作のときに、アプリケーションが CAPF で認証する方法として機能します。デフォルトでは、Cisco CallManager Administration は By Authentication String を表示して、ユーザまたは管理者が JTAPI/TSP Preferences 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。
Authentication String	一意の文字列を手動で入力するか、あるいは Generate String 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 Preferences GUI 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。
Generate String	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 Authentication String フィールドに表示されます。
Key Size (bits)	ドロップダウン リスト ボックスから、証明書の鍵のサイズを選択します。デフォルト設定値は 1024 です。これ以外のオプションには、512 と 2048 があります。 鍵生成を低いプライオリティで設定すると、アクションの実行中もアプリケーションの機能を利用できます。鍵生成が完了するまで、30 秒以上の時間がかかることがあります。 証明書に 2048 ビットの鍵を選択した場合、アプリケーションと Cisco CallManager の間で接続を確立するために、60 秒以上の時間がかかることがあります。最高のセキュリティ レベルを使用する場合を除き、2048 ビットの鍵は設定しないでください。
Operation Completes by	このフィールドは、すべての証明書操作をサポートし、操作を完了する必要がある期限の日付と時刻を指定します。 表示される値は、最初のノードに適用されます。 この設定は、証明書操作を完了する必要があるデフォルトの日数を指定する CAPF Operation Expires in (days) エンタープライズ パラメータと組み合せて使用します。このパラメータは、必要に応じて更新できます。
Operation Status	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、<operation type> pending、failed、successful などで、operating type には、指定した Certificate Operation 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。

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 CallManager データベースから削除する方法を説明します。

始める前に

Cisco CallManager Administration 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、当該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。当該プロファイルを使用しているデバイスを検索するには、Security Profile Configuration ウィンドウの Related Links ドロップダウン リスト ボックスから **Dependency Records** を選択して、**Go** をクリックします。

システムで Dependency Records 機能が有効になっていない場合は、レコードの依存性の概要ウィンドウに、Dependency Records 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、Dependency Records 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。Dependency Records の詳細については、『*Cisco CallManager システム ガイド*』を参照してください。

手順

ステップ 1　P.11-12 の「アプリケーション ユーザまたはエンド ユーザの CAPF プロファイルの検索」の説明に従い、アプリケーション ユーザ CAPF プロファイルまたはエンド ユーザ CAPF プロファイルを検索します。

ステップ 2　複数のプロファイルを削除するには、Find and List 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、**Delete Selected** アイコンまたは **Delete Selected** ボタンをクリックします。

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。

- Find and List 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、**Delete Selected** アイコンまたは **Delete Selected** ボタンをクリックします。
- Find and List ウィンドウで、プロファイルの Name リンクをクリックします。指定した Application User CAPF Profile Configuration ウィンドウまたは End User CAPF Profile Configuration ウィンドウが表示されたら、**Delete Selected** アイコンまたは **Delete Selected** 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、**Cancel** をクリックして削除操作を取り消します。

追加情報

詳細については、P.11-18 の「関連項目」を参照してください。

JTAPI/TAPI セキュリティ関連サービス パラメータ

アプリケーション ユーザ CAPF プロファイルまたはエンド ユーザ CAPF プロファイルを設定した後、Web サービスまたはアプリケーションに対して、次のサービス パラメータを設定する必要があります。

- CTIManager Connection Security Flag
- CAPF Profile Instance ID for Secure Connection to CTIManager

サービス パラメータにアクセスするには、次の手順を実行します。

手順

ステップ 1　Cisco CallManager Administration で、**System > Service Parameters** 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、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　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　**Save** 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（Find/List ウィンドウではありません）、または JTAPI/TSP Preferences GUI ウィンドウで、証明書操作のステータスを表示できます。

その他の情報

関連項目

- Cisco CTL クライアントの設定（P.3-1）
- CTI、JTAPI、および TAPI アプリケーションの認証について（P.11-2）
- CTI、JTAPI、および TAPI アプリケーションの暗号化について（P.11-4）
- CTI、JTAPI、および TAPI アプリケーションに対する CAPF の概要（P.11-5）
- CTI、JTAPI、および TAPI アプリケーションに対する CAPF システムの対話および要件（P.11-6）
- CTI、JTAPI、および TAPI のセキュリティ設定用チェックリスト（P.11-7）
- セキュリティ関連ユーザ グループへのアプリケーション ユーザおよびエンド ユーザの追加（P.11-9）
- Certificate Authority Proxy Function サービスのアクティブ化（P.11-10）
- CAPF サービス パラメータの更新（P.11-11）
- アプリケーション ユーザまたはエンド ユーザの CAPF プロファイルの検索（P.11-12）
- アプリケーション ユーザまたはエンド ユーザの CAPF プロファイルの設定（P.11-13）
- Application User CAPF Profile ウィンドウおよび End User CAPF Profile ウィンドウの CAPF 設定（P.11-14）
- アプリケーション ユーザ CAPF プロファイルまたはエンド ユーザ CAPF プロファイルの削除（P.11-16）
- JTAPI/TAPI セキュリティ関連サービス パラメータ（P.11-17）
- アプリケーション ユーザまたはエンド ユーザに対する証明書操作のステータスの表示（P.11-17）

シスコの関連マニュアル

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

PART 4

SRST リファレンス、トランク、および ゲートウェイのセキュリティ

CHAPTER 12

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

SRST 対応ゲートウェイは、Cisco CallManager がコールを完了できない場合に、制限付きのコール処理タスクを提供します。保護された SRST 対応ゲートウェイには、自己署名証明書が含まれています。Cisco CallManager Administration で SRST 設定作業を実行した後、Cisco CallManager は TLS 接続を使用して SRST 対応ゲートウェイで Certificate Provider サービスを認証します。
次に、Cisco CallManager は SRST 対応ゲートウェイから証明書を取得して、その証明書を Cisco CallManager データベースに追加します。

Cisco CallManager Administration 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。

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 TLS ハンドシェイクが行われます。

- 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クラスタをセキュア モードに設定した。
- 電話機に認証または暗号化を設定した。
- Cisco CallManager Administration 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。

クラスタ セキュリティ モードがノンセキュアになっている場合は、Cisco CallManager Administration 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 モードはノンセキュアのままです。このような場合、電話機は、クラスタ内で SRST 対応ゲートウェイおよび Cisco CallManager サーバとのノンセキュア接続を試行します。

クラスタ セキュリティ モードがノン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 IS SRST Secure? チェックボックスなど、Cisco CallManager Administration 内のセキュリティ関連の設定が無視されます。Cisco CallManager Administration 内の設定は削除されませんが、セキュリティは提供されません。

電話機が SRST 対応ゲートウェイへのセキュア接続を試行するのは、クラスタ セキュリティ モードが Secure Mode 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 Configuration ウィンドウで Is SRST Secure? 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。

ヒント　前のリリースの Cisco CallManager でセキュア SRST リファレンスを設定した場合は、Cisco CallManager のアップグレード時にその設定が自動的に移行されます。

（注）　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 CallManager クラスタがセキュア モードからノンセキュア モードに切り替わった場合、これらの電話機は自動的には Cisco CallManager にフォールバックされません。管理者が SRST ルータの電源を切り、強制的にこれらの電話機を Cisco CallManager に再登録する必要があります。電話機が Cisco CallManager にフォールバックした後、管理者は SRST の電源を投入でき、フェールオーバーおよびフォールバックが再び自動になります。

SRST のセキュリティ設定用チェックリスト

表 12-1 を使用して、SRST のセキュリティ設定手順を進めます。

表 12-1　SRST のセキュリティ設定用チェックリスト

設定手順		関連手順および関連項目
ステップ 1	SRST 対応ゲートウェイで必要なすべての作業を実行したことを確認します。すべてを実行すると、デバイスが Cisco CallManager およびセキュリティをサポートします。	このバージョンの Cisco CallManager をサポートする『*Cisco IOS SRST Version 3.3 System Administrator Guide*』。これは、次の URL で入手できます。 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 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。	SCCP または SIP 電話機セキュリティ プロファイルの適用（P.5-9）
ステップ 5	Cisco CallManager Administration で SRST リファレンスにセキュリティを設定します。これには、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.12-4）
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.12-4）

SRST リファレンスのセキュリティ設定

Cisco CallManager Administration で SRST リファレンスを追加、更新、または削除する前に、次の点を考慮してください。

- 保護された SRST リファレンスの追加：初めて SRST リファレンスにセキュリティを設定する場合、表 12-2 で説明するすべての項目を設定する必要があります。
- 保護された SRST リファレンスの更新：Cisco CallManager Administration 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、Update Certificate 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 CallManager はクラスタ内の各サーバで、信頼できるフォルダにある SRST 対応ゲートウェイの証明書を置き換えます。
- 保護された SRST リファレンスの削除：保護された SRST リファレンスを削除すると、Cisco CallManager データベースおよび電話機の cnf.xml ファイルから SRST 対応ゲートウェイの証明書が削除されます。

  SRST リファレンスを削除する方法については、『*Cisco CallManager アドミニストレーション ガイド*』を参照してください。

SRST リファレンスのセキュリティを設定するには、次の手順を実行します。

手順

ステップ 1　Cisco CallManager Administration で **System > SRST** 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 SRST リファレンスを追加するには、**Add New** ボタンをクリックし、ステップ 3 に進みます。
- 既存の SRST リファレンスをコピーするには、『*Cisco CallManager アドミニストレーション ガイド*』の説明に従って適切な SRST リファレンスを見つけ、コピーするリファレンスの横に表示されている **Copy** ボタンをクリックして、ステップ 3 に進みます。
- 既存の SRST リファレンスを更新するには、『*Cisco CallManager アドミニストレーション ガイド*』の説明に従って適切な SRST リファレンスを見つけ、ステップ 3 に進みます。

ステップ 3　表 12-2 の説明に従い、セキュリティ関連の設定を入力します。

その他の SRST リファレンス設定内容の説明については、『*Cisco CallManager アドミニストレーション ガイド*』を参照してください。

ステップ 4　Is SRST Secure? チェックボックスをオンにすると、Update Certificate 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　**Save** 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、**Update Certificate** ボタンをクリックします。

ヒント　このボタンは、Is SRST Secure? チェックボックスをオンにして Save 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、**Save** をクリックします。

ステップ 8　**Close** をクリックします。

ステップ 9　SRST Reference Configuration ウィンドウで、**Reset** をクリックします。

追加の手順

Device Pool Configuration ウィンドウで SRST リファレンスが有効になったことを確認します。

追加情報

詳細については、P.12-7 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 12-2 で、保護された SRST リファレンスに対して Cisco CallManager Administration で使用できる設定について説明します。

表 12-2　SRST リファレンスのセキュリティの設定内容

設定	説明
Is SRST Secure?	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。 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 Certificate Provider 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 CallManager データベースに格納します。 **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 **Save** をクリックし、従属する電話機をリセットします。
SRST Certificate Provider Port	このポートは、SRST 対応ゲートウェイ上で Certificate Provider サービスに対する要求を監視します。Cisco CallManager はこのポートを使用して SRST 対応ゲートウェイから証明書を取得します。Cisco SRST Certificate Provider のデフォルト ポートは 2445 です。 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。 **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いてファイアウォール内のポートを使用できない場合には、異なるポート番号の設定が必要になることもあります。
Update Certificate	**ヒント**　このボタンは、Is SRST Secure? チェックボックスをオンにして Save をクリックした後にだけ表示されます。 このボタンをクリックすると、Cisco CTL クライアントは Cisco CallManager データベースに格納されている既存の SRST 対応ゲートウェイの証明書を置き換えます（証明書がデータベースに存在する場合）。従属する電話機をリセットした後、TFTP サーバは cnf.xml ファイルを（新しい SRST 対応ゲートウェイの証明書と共に）電話機に送信します。

セキュア SRST リファレンスのトラブルシューティング

この項では、次のトピックについて取り上げます。

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 リファレンスをノンセキュアにするには、Cisco CallManager Administration の SRST Configuration ウィンドウで、**Is the SRTS 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 リファレンスの設定時に表示されるセキュリティ メッセージ

Cisco CallManager Administration でセキュア SRST リファレンスを設定するときに、メッセージ「Port Numbers can only contain digits.」が表示される場合があります。

このメッセージは、SRST Certificate Provider Port を設定するときに、不正なポート番号を入力した場合に表示されます。ポート番号は、1024 ～ 49151 の範囲に存在する必要があります。

SRST 証明書がゲートウェイから削除された場合のトラブルシューティング

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 CallManager データベースと IP Phone から削除する必要があります。

この作業を実行するには、SRST Configuration ウィンドウで、**Is the SRST Secure?** チェックボックスをオフにして **Update** をクリックし、**Reset Devices** をクリックします。

その他の情報

関連項目

シスコの関連マニュアル

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

その他の情報

CHAPTER 13

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

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

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

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

セキュリティをサポートする H.323 ゲートウェイおよびゲートキーパーまたは非ゲートキーパー制御の H.225/H.323/H.245 トランクは、Cisco IPT Platform Administration で IPSec アソシエーションを設定した場合、Cisco CallManager に対して認証ができます。Cisco CallManager とこれらのデバイスとの間で IPSec アソシエーションを作成する方法については、『*Cisco IP Telephony Platform Administration Guide*』を参照してください。

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

IPSec アソシエーションの設定に加えて、Cisco CallManager Administration のデバイス設定ウィンドウで SRTP Allowed チェックボックスをオンにする必要があります。デバイス設定ウィンドウには、H.323 Gateway、H.225 Trunk (Gatekeeper Controlled)、Inter-Cluster Trunk (Gatekeeper Controlled)、Inter-Cluster Trunk (Non-Gatekeeper Controlled) があります。このチェックボックスをオンにしない場合、Cisco CallManager は RTP を使用してデバイスと通信します。このチェックボックスをオンにした場合、Cisco CallManager は、デバイスに対して SRTP が設定されているかどうかに応じて、セキュア コールまたはノンセキュア コールを発生させます。

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

セキュア メディア パスまたはセキュア シグナリング パスを確立でき、デバイスが SRTP をサポートする場合、システムは SRTP 接続を使用します。セキュア メディア パスまたはセキュア シグナリング パスを確立できない、または 1 つ以上のデバイスが SRTP をサポートしない場合、システムは RTP 接続を使用します。SRTP から RTP への（およびその逆の）フォールバックは、セキュア デバイスからノンセキュア 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 MTP Required チェックボックスがオンになっていない場合、Cisco CallManager はこのコールをセキュアに分類します。MTP Required チェックボックスがオンの場合、Cisco CallManager は、コールの音声パススルーを無効にし、コールをノン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 CallManager がそのコールを暗号化済みに分類することがあります。

SRTP が設定されているデバイスでは、デバイスに対する SRTP 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 CallManager はコールを暗号化済みに分類します。この基準を満たさない場合、Cisco CallManager は、コールをノン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 CallManager は、トランクまたはゲートウェイによる発信ファストスタート コールをノンセキュアに分類します。Cisco CallManager Administration で、SRTP Allowed チェックボックスをオンにした場合、Cisco CallManager は Enable Outbound FastStart チェックボックスを無効にします。

SIP トランクの暗号化の概要

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

トランクに対してシグナリングの暗号化を設定するには、SIP トランク セキュリティ プロファイルを設定するときに、次のオプションを選択します。

- Incoming Transport Type ドロップダウン リスト ボックスで、TLS を選択
- Outgoing Transport Type ドロップダウン リスト ボックスで、TLS を選択
- Device Security Mode ドロップダウン リスト ボックスで、Encrypted を選択

SIP トランク セキュリティ プロファイルを設定した後、トランクに適用します。IPSec をまだ設定していない場合は、設定します。

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

ゲートウェイおよびトランクのセキュリティ設定用チェックリスト

表 13-1 を、Cisco IOS MGCP ゲートウェイでセキュリティを設定する方法について説明しているマニュアル『*Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*』とともに使用してください。このマニュアルは、次の URL で入手できます。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_11/gtsecure.htm

表 13-1　MGCP ゲートウェイのセキュリティ設定用チェックリスト

設定手順		関連手順および関連項目
ステップ 1	Cisco CTL Client をインストールし、設定したことを確認します。クラスタ セキュリティ モードがセキュア 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 CallManager とゲートウェイまたはトランクとの間で IPSec を設定することもできます。どちらかの方法で IPSec を設定した場合、もう 1 つの方法を使用する必要はありません。	• ネットワーク インフラストラクチャで IPSec を設定する場合の注意事項（P.13-6） • Cisco CallManager とゲートウェイまたはトランクとの間で IPSec を設定する場合の注意事項（P.13-7）
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 CallManager Administration で SRTP Allowed チェックボックスをオンにします。	SRTP Allowed チェックボックスは、Cisco CallManager Administration の Trunk Configuration ウィンドウまたは 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、『*Cisco CallManager アドミニストレーション ガイド*』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）。	• SIP トランクの暗号化の概要（P.13-4） • SIP トランク セキュリティ プロファイルの設定（P.14-3）
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。	• *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*

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 CallManager とデバイスとの間では設定しない場合は、IPSec の設定前に、次のことを検討してください。

- シスコは、Cisco CallManager 自体ではなくインフラストラクチャで IPSec をプロビジョンすることをお勧めします。
- IPSec を設定する前に、既存の IPSec または VPN 接続、プラットフォームの CPU への影響、帯域幅への影響、ジッタまたは待ち時間、およびその他のパフォーマンス上のメトリックを考慮してください。
- 『*Voice and Video Enabled IPSec Virtual Private Networks Solution Reference Network Design Guide*』を参照してください。これは、次の URL で入手できます。

  http://www.cisco.com/application/pdf/en/us/guest/netsol/ns241/c649/ccmigration_09186a00801ea79c.pdf
- 『*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.13-5 の「ゲートウェイおよびトランクのセキュリティ設定用チェックリスト」に示されている順序どおりに手順を実行してください。

注意　IPSEC 接続を設定して接続がアクティブであることを確認しないと、メディア ストリームの機密性が損なわれる可能性があります。

Cisco CallManager とゲートウェイまたはトランクとの間で IPSec を設定する場合の注意事項

Cisco CallManager と、この章で説明しているゲートウェイまたはトランクとの間で IPSec を設定する方法については、『*Cisco IP Telephony Platform Administration Guide*』を参照してください。

SRTP Allowed チェックボックスの設定

SRTP Allowed チェックボックスは、Cisco CallManager Administration の次の設定ウィンドウに表示されます。

- H.323 Gateway Configuration ウィンドウ
- H.225 Trunk (Gatekeeper Controlled) Configuration ウィンドウ
- Inter-Cluster Trunk (Gatekeeper Controlled) Configuration ウィンドウ
- Inter-Cluster Trunk (Non-Gatekeeper Controlled) Configuration ウィンドウ

H.323 ゲートウェイ、およびゲートキーパーまたは非ゲートキーパー制御の H.323/H.245/H.225 トランクに対して SRTP 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 CallManager アドミニストレーション ガイド*』の説明に従って、ゲートウェイまたはトランクを検索します。

ステップ 2　ゲートウェイまたはトランクの設定ウィンドウが開いたら、SRTP Allowed チェックボックスをオンにします。

ステップ 3　**Save** をクリックします。

ステップ 4　**Reset** をクリックして、デバイスをリセットします。

ステップ 5　IPSec が正しく設定されたことを確認します。

追加情報

詳細については、P.13-8 の「関連項目」を参照してください。

その他の情報

関連項目

- 認証、整合性、および許可の概要（P.1-15）
- 暗号化の概要（P.1-20）
- Cisco IOS MGCP ゲートウェイの暗号化の概要（P.13-2）
- H.323 ゲートウェイおよび H.323/H.225/H.245 トランクの暗号化の概要（P.13-3）
- SIP トランクの暗号化の概要（P.13-4）
- ゲートウェイおよびトランクのセキュリティ設定用チェックリスト（P.13-5）
- ネットワーク インフラストラクチャで IPSec を設定する場合の注意事項（P.13-6）
- Cisco CallManager とゲートウェイまたはトランクとの間で IPSec を設定する場合の注意事項（P.13-7）

シスコの関連マニュアル

- *Cisco IP Telephony Platform Administration Guide*
- *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*

CHAPTER 14

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

Cisco CallManager Administration では、デバイス セキュリティ モード、ダイジェスト認証、着信転送タイプまたは発信転送タイプの設定など、SIP トランク セキュリティ関連の設定がグループ化されます。SIP Trunk Configuration ウィンドウでプロファイルを選択することで、すべての構成済み設定を SIP トランクに適用できます。すべての SIP トランクに、セキュリティ プロファイルを適用する必要があります。SIP トランクがセキュリティをサポートしない場合は、ノンセキュア プロファイルを適用します。

SIP トランク セキュリティ プロファイルの検索

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

手順

ステップ 1　Cisco CallManager Administration で、**System** > **Security Profile** > **SIP Trunk Security Profile** の順に選択します。

Find and List ウィンドウが表示されます。

ステップ 2　ドロップダウン リスト ボックスから、表示するセキュリティ プロファイルの検索基準を選択し、**Find** をクリックします。

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

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

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

ヒント　検索結果内の Name または Description を検索するには、**Search Within Results** チェックボックスをオンにして、この手順で説明したように検索基準を入力し、**Find** をクリックします。

追加情報

詳細については、P.14-9 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 CallManager Administration で、**System > Security Profile > SIP Trunk Security Profile** 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、**Add New** ボタンをクリックし、ステップ 3 に進みます。
- 既存のセキュリティ プロファイルをコピーするには、P.14-2 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 **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.14-2 の「SIP トランク セキュリティ プロファイルの検索」の説明に従い、適切なセキュリティ プロファイルを見つけて、ステップ 3 に進みます。

ステップ 3　表 14-1 の説明に従って、適切な設定を入力します。

ステップ 4　**Save** をクリックします。

追加の手順

セキュリティ プロファイルを作成した後、P.14-7 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 Realm 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 Application User 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）。

アプリケーションレベル許可 SIP トランクを有効にした場合は、Application User ウィンドウで、そのトランクに許可される方式を設定する必要があります。

追加情報

詳細については、P.14-9 の「関連項目」を参照してください。

SIP トランク セキュリティ プロファイルの設定内容

表 14-1 で、SIP トランク セキュリティ プロファイルの設定について説明します。Cisco CallManager の方式許可の詳細については、P.1-6 の「対話」を参照してください。

表 14-1　SIP トランク セキュリティ プロファイルの設定内容

設定	説明
Name	セキュリティ プロファイルの名前を入力します。名前は、Trunk Configuration ウィンドウの SIP Trunk Security Profile ドロップダウン リスト ボックスに表示されます。
Description	セキュリティ プロファイルの説明を入力します。
Incoming Transport Type	ドロップダウン リスト ボックスから、着信転送モードを選択します。 **ヒント**　Transport Layer Security（TLS）プロトコルによって、Cisco CallManager とトランクとの間の接続が保護されます。TLS オプションを選択する場合は、Outgoing Transport Type ドロップダウン リスト ボックスでも TLS オプションを選択してください。
Outgoing Transport Type	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。Incoming Transport Type に TLS を選択した場合は、Outgoing Transport Type にも TLS を選択する必要があります。 **ヒント**　SIP トランクのシグナリング整合性、デバイス認証、シグナリング暗号化を保証するには、Transport Layer Security プロトコルを選択します。
Device Security Mode	ドロップダウン ボックスから、次のオプションのいずれか 1 つを選択します。 • **Non Secure**：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 CallManager が利用できる。 • **Authenticated**：Cisco CallManager はトランクの整合性と認証を提供する。NULL/SHA を使用する TLS 接続を開始する。 • **Encrypted**：Cisco CallManager はトランクの整合性、認証、およびシグナリング暗号化を提供する。シグナリング用に、AES128/SHA を使用する TLS 接続を開始する。 **ヒント**　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）。

表 14-1　SIP トランク セキュリティ プロファイルの設定内容（続き）

設定	説明
Enable Digest Authentication	Cisco CallManager が、トランクに接続する SIP ユーザ エージェントの ID でチャレンジを行う場合は、このチェックボックスをオンにします。Cisco CallManager が ID でチャレンジを行った後、トランクは MD5 チェックサム、ユーザ名、パスワード、ナンス値、要求された URI で応答し、Cisco CallManager Administration で設定したクレデンシャルに基づいて Cisco CallManager が情報を検証します。クレデンシャルが一致した場合、ダイジェスト認証は成功します。 このチェックボックスをオンにすると、Cisco CallManager は、トランクからのすべての SIP 要求でチャレンジを行います。 ダイジェスト認証は、整合性や信頼性を提供しません。トランクの整合性および信頼性を保証するには、TLS プロトコルを設定します。
Nonce Validity Time	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。 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 CallManager は新しい値を生成します。
X.509 Subject Name	このフィールドは、Incoming Transport Type および Outgoing Transport Type に TLS を設定した場合に適用されます。 SIP トランクに接続されている認証済みデバイスに対する X.509 証明書の件名を入力します。Cisco CallManager クラスタがある場合、または TLS ピアに対して SRV ルックアップを使用する場合、単一のトランクが複数のホストに解決されることがあります。その結果、トランクに複数の X.509 の件名が設定されます。複数の X.509 の件名がある場合は、スペース、カンマ、セミコロン、またはコロンのいずれか 1 つを使用して、名前を区切ります。 このフィールドには、4096 文字まで入力できます。 **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せを、異なる SIP トランクに割り当てることはできません。 例：ポート 5061 の SIP TLS trunk1 の X.509 Subject Name は、my_cm1, my_cm2 です。ポート 5071 の SIP TLS trunk1 の 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 Subject Name は my_ccm4 にできますが、my_cm1 にはできません。
Incoming Port	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。 入力した値は、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。必要に応じて、同じ着信ポート番号をすべての SIP トランクに設定できます。

表 14-1　SIP トランク セキュリティ プロファイルの設定内容（続き）

設定	説明
Enable Application Level Authorization	このチェックボックスをオンにする場合は、Enable Digest Authentication チェックボックスをオンにし、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。トランクのダイジェスト認証設定の詳細については、P.15-1 の「SIP トランクのダイジェスト認証の設定」を参照してください。 このチェックボックスをオンにすると、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。アプリケーションレベルの許可は、アプリケーションから SIP ユーザ エージェントで送信された SIP メッセージに対して発生します。アプリケーションレベルの許可は、Application User Configuration ウィンドウ（User Management > Application User）でオンにした許可チェックボックスに基づきます。 **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。
Accept Presence Subscription	Cisco CallManager が SIP トランク経由で着信するプレゼンス サブスクリプション要求を受け付けるようにする場合は、このチェックボックスをオンにします。 Enable Application Level Authorization チェックボックスをオンにした場合は、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 Accept Presence Subscription チェックボックスをオンにします。 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 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。
Accept Out-of-Dialog Refer	Cisco CallManager が SIP トランク経由で着信する non-INVITE、Out-of-Dialog 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。 Enable Application Level Authorization チェックボックスをオンにした場合は、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 Accept Out-of-Dialog Refer チェックボックスをオンにします。
Accept Unsolicited Notification	Cisco CallManager が SIP トランク経由で着信する non-INVITE、Unsolicited Notification 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。 Enable Application Level Authorization チェックボックスをオンにした場合は、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 Accept Unsolicited Notification チェックボックスをオンにします。

表 14-1　SIP トランク セキュリティ プロファイルの設定内容（続き）

設定	説明
Accept Header Replacement	Cisco CallManager が既存の SIP ダイアログを置き換える新しい SIP ダイアログを受け付けるようにする場合は、このチェックボックスをオンにします。 Enable Application Level Authorization チェックボックスをオンにした場合は、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 Accept Header Replacement チェックボックスをオンにします。

SIP トランク セキュリティ プロファイルの適用

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 CallManager アドミニストレーション ガイド*』の説明に従って、トランクを検索します。

ステップ 2　Trunk Configuration ウィンドウが表示されたら、**SIP Trunk Security Profile** 設定を見つけます。

ステップ 3　セキュリティ プロファイルのドロップダウン リスト ボックスから、デバイスに適用するセキュリティ プロファイルを選択します。

ステップ 4　**Save** をクリックします。

ステップ 5　**Reset** をクリックして、電話機をリセットします。

追加の手順

SIP トランクにダイジェスト認証を設定した場合は、トランクの SIP Realm 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 Application User 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）。P.15-5 の「SIP レルムの設定」を参照してください。

追加情報

詳細については、P.14-9 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 CallManager データベースから SIP トランク セキュリティ プロファイルを削除する方法について説明します。

始める前に

Cisco CallManager Administration 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、当該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。当該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 Trunk Security Profile Configuration ウィンドウの Related Links ドロップダウン リスト ボックスから **Dependency Records** を選択して、**Go** をクリックします。

システムで Dependency Records 機能が有効になっていない場合は、レコードの依存性の概要ウィンドウに、Dependency Records 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、Dependency Records 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。Dependency Records の詳細については、『*Cisco CallManager システム ガイド*』を参照してください。

手順

ステップ 1　P.14-2 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、Find and List 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、**Delete Selected** アイコンまたは **Delete Selected** ボタンをクリックします。

ステップ 3　単一のセキュリティ プロファイルを削除するには、次の作業のどちらかを実行します。

- Find and List 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、**Delete Selected** アイコンまたは **Delete Selected** ボタンをクリックします。
- Find and List ウィンドウで、セキュリティ プロファイルの **Name** リンクをクリックします。指定した Security Profile Configuration ウィンドウが表示されたら、**Delete Selected** アイコンまたは **Delete Selected** 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、**Cancel** をクリックして削除操作を取り消します。

追加情報

詳細については、P.14-9 の「関連項目」を参照してください。

その他の情報

関連項目

- SIP トランク セキュリティ プロファイルの概要（P.14-1）
- SIP トランク セキュリティ プロファイルの検索（P.14-2）
- SIP トランク セキュリティ プロファイルの設定（P.14-3）
- SIP トランク セキュリティ プロファイルの設定内容（P.14-4）
- SIP トランク セキュリティ プロファイルの適用（P.14-7）
- SIP トランク セキュリティ プロファイルの削除（P.14-8）

シスコの関連マニュアル

Cisco CallManager アドミニストレーション ガイド

その他の情報

CHAPTER 15

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、トランクが SIP 要求を Cisco CallManager に送信するたびに、Cisco CallManager はトランクに接続している SIP ユーザ エージェントの ID でチャレンジを行います。次に、SIP ユーザ エージェントが Cisco CallManager の ID でチャレンジを行うことができます。SIP トランクでのダイジェスト認証の動作の詳細については、P.1-17 の「ダイジェスト認証」を参照してください。

この章は、次の内容で構成されています。

SIP トランク ダイジェスト認証の設定用チェックリスト

SIP トランクにダイジェスト認証を設定する作業を表 15-1 で説明します。

表 15-1　SIP トランクのセキュリティ設定用チェックリスト

設定手順		関連手順および関連項目
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。**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。	• SIP トランク セキュリティ プロファイルの設定（P.14-3） • ダイジェスト認証（P.1-17）
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.14-7）
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）。 このパラメータは、Cisco CallManager を UAS としてサポートします。つまり、Cisco CallManager は SIP ユーザ エージェントの ID でチャレンジを行います。	ダイジェスト認証のエンタープライズ パラメータの設定（P.15-2）
ステップ 4	Cisco CallManager がトランクのユーザ エージェント サーバ（UAS）として動作する場合は、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。	• Application User Configuration ウィンドウでのダイジェスト クレデンシャルの設定（P.15-3） • アプリケーション ユーザ ダイジェスト クレデンシャルの設定内容（P.15-3）
ステップ 5	Cisco CallManager がユーザ エージェント クライアント（UAC）として動作する場合は、SIP レルムを設定します。 トランクが Cisco CallManager の ID でチャレンジを行う場合、Cisco CallManager はユーザ エージェント クライアントとして動作します。	• ダイジェスト認証（P.1-17） • SIP レルムの設定（P.15-5） • SIP レルムの設定内容（P.15-6）

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 CallManager Administration で、**System > Enterprise Parameters** の順に選択します。**Cluster ID** パラメータを見つけ、パラメータをサポートするヘルプの説明に従って値を更新します。このパラメータは、Cisco CallManager を UAS としてサポートします。つまり、Cisco CallManager は SIP ユーザ エージェントの ID でチャレンジを行います。

ヒント　パラメータのヘルプにアクセスするには、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。

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 CallManager がユーザ エージェント サーバとして動作する場合（Cisco CallManager が SIP ユーザ エージェントの ID でチャレンジを行う場合）、Cisco CallManager Administration の 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 CallManager は、これらのクレデンシャルを使用して、SIP UAC 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 CallManager アドミニストレーション ガイド*』の説明に従って、アプリケーション ユーザを検索します。

ステップ 2　アプリケーション ユーザのリンクをクリックします。

ステップ 3　目的の Application User Configuration ウィンドウが表示されたら、表 15-3 の説明に従って、適切な文字列を入力します。

ステップ 4　**Save** をクリックします。

追加情報

詳細については、P.15-7 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 15-3 で、Cisco CallManager Administration の 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。

表 15-2　ダイジェスト認証クレデンシャル

設定	説明
Digest Credentials	英数字文字列を入力します。
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 CallManager Administration で **User Management > SIP Realm** の順に選択します。

Find and List ウィンドウが表示されます。

ステップ 2　ドロップダウン リスト ボックスから、表示する SIP レルムの検索基準を選択し、**Find** をクリックします。

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

ウィンドウが更新され、検索基準と一致する SIP レルムが表示されます。

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

ヒント　検索結果内の Realm または User を検索するには、**Search Within Results** チェックボックスをオンにして、この手順で説明したように検索基準を入力し、**Find** をクリックします。

追加の手順

Cluster ID エンタープライズ パラメータをまだ設定していない場合は、P.15-2 の「ダイジェスト認証のエンタープライズ パラメータの設定」の説明に従って設定します。

追加情報

詳細については、P.15-7 の「関連項目」を参照してください。

SIP レルムの設定

Cisco CallManager がユーザ エージェント クライアント（UAC）として動作する場合、SIP トランク ユーザ エージェントごとに SIP レルムを設定する必要があります。トランク ピアが Cisco CallManager の ID でチャレンジを行う場合、Cisco CallManager はユーザ エージェント クライアントとして動作します。

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 CallManager Administration で **User Management > SIP Realm** 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、**Add New** ボタンをクリックし、ステップ 3 に進みます。
- 既存の SIP レルムを更新するには、P.15-4 の「SIP レルムの検索」の説明に従い、適切なセキュリティ プロファイルを見つけて、ステップ 3 に進みます。

ステップ 3　表 15-3 の説明に従って、適切な設定を入力します。

ステップ 4　**Save** 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 CallManager で設定した内容と SIP ユーザ エージェントで設定した内容が同じであることを確認します。

追加情報

詳細については、P.15-7 の「関連項目」を参照してください。

SIP レルムの設定内容

Cisco CallManager がユーザ エージェント クライアント（UAC）として動作する場合は、SIP レルムを設定する必要があります。トランク ピアが Cisco CallManager の ID でチャレンジを行う場合、Cisco CallManager はユーザ エージェント クライアントとして動作します。レルムは、トランク側のクレデンシャルを提供します。

表 15-3 で、SIP レルムの設定内容を説明します。

表 15-3　SIP レルム セキュリティ プロファイル

設定	説明
Realm	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。
User	Cisco CallManager と関連付けるユーザ名を入力します（サーバ名など）。SIP トランクは、Cisco CallManager の ID でチャレンジを行うときに、このユーザ名を使用します。
Password	Cisco CallManager と関連付けるパスワードを入力します。SIP トランクは、Cisco CallManager の ID でチャレンジを行うときに、このパスワードを使用します。
Password Confirmation	パスワードを正しく入力したことを確認するために、このフィールドにパスワードを入力します。

SIP レルムの削除

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

手順

ステップ 1　P.15-4 の「SIP レルムの検索」の手順に従って、SIP レルムを検索します。

ステップ 2　複数の SIP レルムを削除するには、Find and List 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、**Delete Selected** アイコンまたは **Delete Selected** ボタンをクリックします。

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。

- Find and List 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、**Delete Selected** アイコンまたは **Delete Selected** ボタンをクリックします。
- Find and List ウィンドウで、**Realm** リンクをクリックします。指定した SIP Realm Configuration ウィンドウが表示されたら、**Delete Selected** アイコンまたは **Delete Selected** 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、**Cancel** 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.15-7 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.1-17）
- SIP トランク ダイジェスト認証の設定用チェックリスト（P.15-2）
- ダイジェスト認証のエンタープライズ パラメータの設定（P.15-2）
- Application User Configuration ウィンドウでのダイジェスト クレデンシャルの設定（P.15-3）
- アプリケーション ユーザ ダイジェスト クレデンシャルの設定内容（P.15-3）
- SIP レルムの検索（P.15-4）
- SIP レルムの設定（P.15-5）
- SIP レルムの設定内容（P.15-6）
- SIP レルムの削除（P.15-7）

その他の情報

PART 5

セキュリティのトラブルシューティング

CHAPTER 16

トラブルシューティング

この章では、セキュリティ関連の測定、およびセキュリティ関連の問題をトラブルシューティングするときの一般的なガイドラインについて説明します。この章は、次の内容で構成されています。

Cisco CallManager のアラーム、パフォーマンス モニタ、ログ、およびトレースまたはエラー メッセージと修正処置の詳細については、次のマニュアル（またはオンライン ヘルプ）を参照してください。

- Real-Time Monitoring Tool（RTMT）の GUI およびパフォーマンス モニタのアラームの詳細については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』および『*Cisco CallManager Serviceability システム ガイド*』を参照してください。
- エラー メッセージの詳細については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』を参照してください。
- RTMT でのログおよびトレースの表示の詳細については、『*Cisco CallManager Serviceability システム ガイド*』を参照してください。
- パケット キャプチャの使用または設定、およびキャプチャしたパケットの分析の詳細については、『*Cisco CallManager トラブルシューティング ガイド Release 5.0(1)*』を参照してください。
- トラブルシューティングの手順および修正処置の詳細については、『*Cisco CallManager トラブルシューティング ガイド Release5.0(1)*』を参照してください。

(注) この章では、Cisco IP Phone がロード エラーやセキュリティのバグなどによって障害を起こした場合に IP Phone をリセットする方法は説明していません。IP Phone のリセットについては、IP Phone のモデルに対応した『*Cisco IP Phone アドミニストレーション ガイド for Cisco CallManager*』を参照してください。

Cisco IP Phone 7970 モデル、7960 モデル、および 7940 モデルだけから CTL ファイルを削除する方法については、表 3-3、または IP Phone のモデルに対応した『*Cisco IP Phone アドミニストレーション ガイド for Cisco CallManager*』を参照してください。

CLI の使用方法

Cisco IPT Platform Administration GUI の使用中に問題が発生した場合、管理者はコマンドライン インターフェイス（CLI）を使用して、トラブルシューティングの目的でシステム機能にアクセスできます。

CLI インターフェイスを使用するには、SSH アクセスができる環境とログイン ID およびパスワードが必要です。CLI を使用してログ、トレース、およびパフォーマンス モニタを表示する方法については、『*Cisco IP Telephony Platform Administration Guide*』を参照してください。

アラームの使用方法

Cisco CallManager Serviceability は、X.509 名不一致、認証エラー、暗号化エラーに対して、セキュリティ関連アラームを生成します。Serviceability GUI を使用して、アラームを定義できます。

アラームは、TFTP サーバおよび CTL ファイルのエラーが発生したときに、IP Phone で生成されます。IP Phone で生成されるアラームについては、IP Phone のモデルとタイプ（SCCP または SIP）に対応した『*Cisco IP Phone アドミニストレーション ガイド for Cisco CallManager*』と、P.3-18 の「Cisco IP Phone 上の CTL ファイルの削除」を参照してください。

パフォーマンス モニタ カウンタの使用方法

パフォーマンス モニタ カウンタは、Cisco CallManager に登録する認証済み IP Phone の数、完了した認証済みコールの数、および任意の時点でアクティブになっている認証済みコールの数を監視します。表 16-1 に、セキュリティ機能に適用されるパフォーマンス カウンタを示します。

表 16-1　セキュリティ パフォーマンス カウンタ

オブジェクト	カウンタ
Cisco CallManager	AuthenticatedCallsActive
	AuthenticatedCallsCompleted
	AuthenticatedPartiallyRegisteredPhone
	AuthenticatedRegisteredPhones
	EncryptedCallsActive
	EncryptedCallsCompleted
	EncryptedPartiallyRegisteredPhone
	EncryptedRegisteredPhones
	CCMSIPLineServerAuthChallenges
	CCMSIPLineServerAuthFailures
	CCMSIPTrunkServerAuthChallenges
	CCMSIPTrunkServerAuthFailures
	CCMSIPTrunkClientAuthResponses
	CCMSIPTrunkClientAuthRejects
	CCMSIPPresenceAuthorizations
	CCMSIPPresenceAuthorizationsFailure
	CCMSIPTrunkMethodAuthorization
	CCMSIPTrunkMethodAuthorizationFailure
	TLSConnectedSIPTrunk
SIP スタック	StatusCodes4xxIns（405 Method Not Allowed など）
	StatusCodes4xxOuts（405 Method Not Allowed など）
TFTP サーバ	BuildSigCount
	EncryptCount

RTMT でパフォーマンス カウンタにアクセスする方法、perfmon ログの設定、およびカウンタの詳細については、『*CallManager Serviceability システム ガイド*』、を参照してください。

CLI コマンドの **show perf** は、パフォーマンス モニタ情報を表示します。CLI インターフェイスの使用方法については、『*Cisco IP Telephony Platform Administration Guide*』を参照してください。

ログおよびトレース ファイルの確認

Cisco Partner や Cisco Technical Assistance Center（TAC）など、この製品のテクニカル サポートに連絡する場合は、事前に、RTMT でノードのログ ファイルおよびトレース ファイルを確認してください。

管理者は、Serviceability Real-Time Monitoring Tool（RTMT）の Trace Collection Tool を使用して、ログ ファイルおよびトレース ファイルをサーバからダウンロードできます。ファイルを収集した後、RTMT の適切なビューアで表示できます。

（注） 暗号化をサポートするデバイスの場合、SRTP 鍵関連情報はトレース ファイルに表示されません。

トレース収集ツールの使用方法およびフィルタリングを使用してログ ファイル レコードを確認する方法については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』および『*Cisco CallManager Serviceability システム ガイド*』を参照してください。

Cisco CallManager は、ログ ファイルおよびトレース ファイルを複数のディレクトリに格納します（cm/log、cm/trace、tomcat/logs、tomcat/logs/security など）。CLI コマンドの **activelog** および **inactivelog** を使用して、ログ ファイルおよびトレース ファイルの検索、表示、および操作ができます。

CLI インターフェイスの使用方法の詳細については、『*Cisco IP Telephony Platform Administration Guide*』を参照してください。

ヒント ログ ファイルまたはトレース ファイルのディレクトリおよびファイル名がわからない場合は、TAC に問い合せてください。

セキュリティ ファイルのバックアップと復元

CAPF データなど、セキュリティ ファイルのバックアップおよび復元の手順については、『*Cisco IP Telephone Disaster Recovery Framework Administration Guide*』を参照してください。

証明書のトラブルシューティング

Cisco IPT Platform Administration の証明書管理ツールを使用すると、証明書の表示、削除と再生成、証明書の有効期限の監視、証明書および CTL ファイルのダウンロードとアップロード（更新した CTL ファイルを Unity にアップロードするなど）ができます。CLI を使用すると、自己署名証明書および信頼された証明書の一覧および表示、自己署名証明書の再生成ができます。

CLI コマンドの **show cert**、**show web-security**、**set cert regen**、および **set web-security** を使用して、CLI インターフェイスで証明書を管理できます（たとえば、**set cert regen tomcat** と使用します）。GUI または CLI を使用して証明書を管理する方法については、『*Cisco IP Telephony Platform Administration Guide*』を参照してください。

CTL セキュリティ トークンのトラブルシューティング

この項は、次の内容で構成されています。

すべてのセキュリティ トークン（etoken）を紛失した場合は、Cisco TAC に問い合せてください。

不適切なセキュリティ トークン パスワードを続けて入力した場合のロックされたセキュリティ トークンのトラブルシューティング

各セキュリティ トークンには、リトライ カウンタが含まれています。リトライ カウンタは、etoken Password ウィンドウへのログインの連続試行回数を指定します。セキュリティ トークンのリトライ カウンタ値は 15 です。連続試行回数がカウンタ値を超えた場合、つまり、16 回連続で試行が失敗した場合は、セキュリティ トークンがロックされ、使用不能になったことを示すメッセージが表示されます。ロックされたセキュリティ トークンを再び有効にすることはできません。

追加のセキュリティ トークン（複数可）を取得し、CTL ファイルを設定します（P.3-9 の「Cisco CTL クライアントの設定」を参照）。必要であれば、新しいセキュリティ トークン（複数可）を購入し、ファイルを設定します。

ヒント　パスワードを正しく入力すると、カウンタがゼロにリセットされます。

セキュリティ トークン（etoken）を 1 つ紛失した場合のトラブルシューティング

セキュリティ トークンを 1 つ紛失した場合は、次の手順を実行します。

手順

ステップ 1　新しいセキュリティ トークンを購入します。

ステップ 2　CTL ファイルに署名したトークンを使用し、次の作業を実行して CTL ファイルを更新します。

a. 新しいトークンを CTL ファイルに追加します。

b. 紛失したトークンを CTL ファイルから削除します。

各作業の実行方法の詳細については、P.3-12 の「CTL ファイルの更新」を参照してください。

ステップ 3　IP Phone をすべてリセットします（P.1-10 の「デバイスのリセット、サービスの再起動、またはサーバおよびクラスタのリブート」を参照）。

CAPF のトラブルシューティング

この項では、次のトピックについて取り上げます。

IP Phone での認証文字列のトラブルシューティング

IP Phone で不適切な認証文字列を入力すると、IP Phone 上にメッセージが表示されます。IP Phone に正しい認証文字列を入力します。

ヒント

IP Phone が Cisco CallManager に登録されていることを確認してください。IP Phone が Cisco CallManager に登録されていない場合、IP Phone で認証文字列を入力することはできません。

IP Phone のデバイス セキュリティ モードがノンセキュアになっていることを確認してください。

電話機に適用されるセキュリティ プロファイルの認証モードが By Authentication String に設定されていることを確認します。

CAPF では、IP Phone で認証文字列を入力できる連続試行回数が制限されています。10 回連続で正しい認証文字列が入力されなかった場合は、正しい文字列の入力を再試行できる状態になるまでに、10 分以上かかります。

ローカルで有効な証明書の検証が失敗する場合のトラブルシューティング

IP Phone では、次のような場合に、ローカルで有効な証明書の検証が失敗することがあります。たとえば、証明書が CAPF によって発行されたバージョンでない場合、CAPF 証明書がクラスタ内の一部のサーバ上に存在しない場合、CAPF 証明書が CAPF ディレクトリ内に存在しない場合、IP Phone が Cisco CallManager に登録されていない場合などです。ローカルで有効な証明書の検証が失敗する場合は、SDL トレース ファイルと CAPF トレース ファイルでエラーを検討します。

CAPF 証明書がクラスタ内のサーバすべてにインストールされていることの確認

Cisco Certificate Authority Proxy Function サービスをアクティブにすると、CAPF に固有な鍵ペアおよび証明書が CAPF によって自動生成されます。CAPF 証明書は Cisco CTL クライアントによってクラスタ内のすべてのサーバにコピーされ、拡張子 .0 を使用します。CAPF 証明書が存在することを確認するには、Cisco IPT Platform GUI または CLI で、CAPF 証明書を表示します。

- DER 符号化形式の場合：CAPF.cer
- PEM 符号化形式の場合：CAPF.cer と同じ通常名文字列が含まれる .0 拡張子ファイル

ローカルで有効な証明書が IP Phone 上に存在することの確認

ローカルで有効な証明書が電話機にインストールされていることを確認するには、Model Information または Security Configuration 電話機メニューを使用して、LSC 設定を表示します。詳細については、IP Phone のモデルとタイプ（SCCP または SIP）に対応した『*Cisco 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。

製造元でインストールされる証明書（MIC）が IP Phone 内に存在することの確認

MIC が電話機に存在することを確認するには、Model Information または Security Configuration 電話機メニューを使用して、MIC 設定を表示します。詳細については、IP Phone のモデルとタイプ（SCCP または SIP）に対応した『*Cisco IP Phone アドミニストレーション ガイド*』を参照してください。

電話機および Cisco IOS MGCP ゲートウェイの暗号化のトラブルシューティング

この項では、次のトピックについて取り上げます。

パケット キャプチャの使用方法

SRTP 暗号化を有効にした後は、メディア パケットと TCP パケットのスニファを実行するサードパーティ製のトラブルシューティング ツールが連動しないため、問題が発生する場合は、Cisco CallManager Administration を使用して次の作業を実行する必要があります。

- Cisco CallManager とデバイス（Cisco IP Phone、Cisco SIP IP Phone、Cisco IOS MGCP ゲートウェイ、H.323 ゲートウェイ、または H.323/H.245/H.225 トランク）との間で交換されるメッセージのパケットを分析する。

（注） SIP トランクは SRTP をサポートしません。

- デバイス間の SRTP パケットをキャプチャする。
- メッセージからメディアの暗号鍵関連情報を抽出し、デバイス間のメディアを復号化する。

パケット キャプチャの使用または設定、およびキャプチャした SRTP 暗号化コール（および、その他のすべてのコール タイプ）のパケットの分析の詳細については、『*Cisco CallManager トラブルシューティング ガイド Release 5.0(1)*』を参照してください。

ヒント この作業を同時に複数のデバイスで実行すると、CPU 消費量が高くなり、コール処理が中断される場合があります。この作業は、コール処理の中断を最小限に抑えられるときに実行することを強くお勧めします。

BAT に対する IP Phone のパケット キャプチャの設定

この Cisco CallManager リリースと互換性のある Bulk Administration Tool を使用すると、電話機でパケット キャプチャ モードを設定できます。この作業を実行する方法については、『*Cisco CallManager Bulk Administration Guide*』を参照してください。

ヒント BAT でこの作業を実行すると、CPU 消費量が高くなり、コール処理が中断される場合があります。この作業は、コール処理の中断を最小限に抑えられるときに実行することを強くお勧めします。

その他の情報

関連項目

- 対話および制限（P.1-6）
- 証明書の種類（P.1-13）
- メディア暗号化の設定と割り込み（P.1-11）
- CLI の使用方法（P.16-2）
- アラームの使用方法（P.16-2）
- パフォーマンス モニタ カウンタの使用方法（P.16-3）
- ログおよびトレース ファイルの確認（P.16-4）
- セキュリティ ファイルのバックアップと復元（P.16-4）
- 証明書のトラブルシューティング（P.16-4）
- CTL セキュリティ トークンのトラブルシューティング（P.16-5）
- CAPF のトラブルシューティング（P.16-6）
- 電話機および Cisco IOS MGCP ゲートウェイの暗号化のトラブルシューティング（P.16-8）

シスコの関連マニュアル

- *Cisco IP Telephone Disaster Recovery Framework Administration Guide*
- *Cisco CallManager Bulk Administration Guide*
- *Cisco CallManager Serviceability アドミニストレーション ガイド*
- *Cisco CallManager Serviceability システム ガイド*
- *Cisco CallManager トラブルシューティング ガイド Release5.0(1)*
- *Cisco IP Telephony Platform Administration Guide*
- 電話機のモデルおよびプロトコルに対応した Cisco IP Phone アドミニストレーション ガイド

B

C

E

H

I

J

M

S

T

あ

い

き

く

こ

し

せ

た

て

と

に

ふ

ほ

ま

め

も

ろ

わ