



Cisco CallManager セキュリティ ガイド

Release 4.1(2)



このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。見当たらない場合には、代理店にご連絡ください。

シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティングシステムの UCB (University of California, Berkeley) パブリックドメインバージョンとして、UCB が開発したプログラムを最適化したものです。All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、すべてのマニュアルおよび上記各社のソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記各社は、商品性や特定の目的への適合性、権利を侵害しないことに関する、または取り扱い、使用、または取り引きによって発生する、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその代理店は、このマニュアルの使用またはこのマニュアルを使用できないことによって起こる制約、利益の損失、データの損傷など間接的で偶発的に起こる特殊な損害のあらゆる可能性がシスコまたは代理店に知らされていても、それらに対する責任を一切負いかねます。

CCSP、Cisco Square Bridge のロゴ、Cisco Unity、Follow Me Browsing、FormShare、および StackWise は、Cisco Systems, Inc. の商標です。Changing the Way We Work, Live, Play, and Learn、および iQuick Study は、Cisco Systems, Inc. のサービスマークです。Aironet、ASIST、BPX、Catalyst、CCDA、CCDP、CCIE、CCIP、CCNA、CCNP、Cisco、Cisco Certified Internetwork Expert のロゴ、Cisco IOS、Cisco Press、Cisco Systems、Cisco Systems Capital、Cisco Systems のロゴ、Empowering the Internet Generation、Enterprise/Solver、EtherChannel、EtherFast、EtherSwitch、Fast Step、GigaDrive、GigaStack、HomeLink、Internet Quotient、IOS、IP/TV、iQ Expertise、iQ のロゴ、iQ Net Readiness Scorecard、LightStream、Linksys、MeetingPlace、MGX、Networkers のロゴ、Networking Academy、Network Registrar、Packet、PIX、Post-Routing、Pre-Routing、ProConnect、RateMUX、Registrar、ScriptShare、SlideCast、SMARTnet、StrataView Plus、SwitchProbe、TeleRouter、The Fastest Way to Increase Your Internet Quotient、TransPath、および VCO は、米国および一部の国における Cisco Systems, Inc. とその関連会社の登録商標です。

このマニュアルまたは Web サイトで言及されているその他の商標はすべて、それぞれの所有者のもです。「パートナー」という語の使用は、シスコと他社の提携関係を意味するものではありません。(0406R)

Cisco CallManager セキュリティ ガイド

Copyright © 2004 Cisco Systems, Inc.

All rights reserved.



このマニュアルについて	xi
目的	xii
対象読者	xii
マニュアルの構成	xiii
関連マニュアル	xiv
表記法	xv
技術情報の入手方法	xvi
Cisco.com	xvi
マニュアルの発注方法（英語版）	xvi
シスコシステムズマニュアルセンター	xvii
テクニカル サポート	xviii
Cisco Technical Support Web サイト	xviii
Japan TAC Web サイト	xviii
サービス リクエストの発行	xix
サービス リクエストのシビラティの定義	xix
その他の資料および情報の入手方法	xx

CHAPTER 1

セキュリティの概要	1-1
認証および暗号化に関する用語	1-2
システム要件	1-5
対話および制限	1-6
インストール	1-15

証明書の種類	1-16
認証および整合性の概要	1-18
暗号化の概要	1-21
設定用チェックリストの概要	1-24
その他の情報	1-29

CHAPTER 2

HTTP over SSL (HTTPS) の使用方法 2-1

HTTPS の概要	2-2
Internet Explorer による HTTPS の使用方法	2-5
Internet Explorer を使用して証明書を信頼できるフォルダに保存する方法	2-6
証明書の詳細表示	2-7
証明書のファイルへのコピー	2-8
Netscape による HTTPS の使用方法	2-10
Netscape を使用して証明書を信頼できるフォルダに保存する方法	2-11
サードパーティの認証局によるサーバ認証証明書の使用方法	2-13

CHAPTER 3

Cisco CTL クライアントの設定 3-1

Cisco CTL クライアントの概要	3-2
Cisco CTL クライアントの設定用チェックリスト	3-3
Cisco CTL Provider サービスのアクティブ化	3-5
Cisco CAPF サービスのアクティブ化	3-7
TLS 接続用ポートの設定	3-8
Cisco CTL クライアントのインストール	3-10
Cisco CTL クライアントのアップグレードおよび Cisco CTL ファイルの移行	3-13

CiscoCTL クライアントの設定	3-14
CTL ファイルの更新	3-20
クラスタ全体のセキュリティ モードの更新	3-23
Cisco CTL クライアント設定	3-24
CTL ファイル エントリの削除	3-27

CHAPTER 4

Certificate Authority Proxy Function の使用方法	4-1
Certificate Authority Proxy Function の概要	4-2
Cisco IP Phone と CAPF の対話	4-3
CAPF システムの対話および要件	4-4
Cisco CallManager Serviceability での CAPF の設定	4-6
既存の CAPF データの移行	4-6
CAPF の設定用チェックリスト	4-8
4.0 サブスクライバ サーバから 4.0 パブリッシャ データベース サーバへの CAPF 1.0(1) データのコピー	4-10
Certificate Authority Proxy Function サービスのアクティブ化	4-12
CAPF サービス パラメータの更新	4-13
CAPF サービス パラメータ	4-14
CAPF エンタープライズ パラメータの更新	4-16
ローカルで有効な証明書のインストールおよびアップグレード	4-17
ローカルで有効な証明書の削除	4-18
Phone Configuration ウィンドウの CAPF 設定	4-20
Bulk Administration Tool による CAPF の使用方法	4-23
CAPF レポートの生成	4-24
LSC Status の選択による電話機の検索	4-25
電話機での認証文字列の入力	4-25

CHAPTER 5

電話機のセキュリティ設定 5-1

電話機のセキュリティ設定の概要 5-2

電話機における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 5-3

デバイス セキュリティ モードの設定 5-4

サポートされる電話機モデルに対するセキュリティ デバイス システム デフォルトの設定 5-5

単一デバイスに対するデバイス セキュリティ モードの設定 5-6

Cisco Bulk Administration Tool を使用したデバイス セキュリティ モードの設定 5-8

Device Security Mode 設定 5-9

認証、暗号化、LSC ステータスによる電話機の検索 5-10

電話機のセキュリティ強化 5-11

電話機のセキュリティ強化作業の実行 5-14

CHAPTER 6

Survivable Remote Site Telephony (SRST) リファレンスのセキュリティ設定 6-1

SRST のセキュリティの概要 6-2

SRST のセキュリティ設定用チェックリスト 6-3

SRST リファレンスのセキュリティ設定 6-4

SRST リファレンスのセキュリティ設定 6-6

CHAPTER 7

トラブルシューティング 7-1

アラームの使用法 7-2

Microsoft パフォーマンス モニタ カウンタの使用法 7-3

ログ ファイルの検討 7-4

HTTPS のトラブルシューティング 7-5

HTTPS の設定時に表示されるメッセージ	7-5
HTTPS の有効化	7-7
仮想ディレクトリの HTTPS の無効化	7-8
HTTPS 証明書の削除	7-9
Cisco CTL クライアントのトラブルシューティング	7-10
セキュリティ トークン パスワード (Etoken) の変更	7-10
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	7-12
Smart Card サービスの Started および Automatic への設定	7-13
Cisco CTL クライアントに関するメッセージ	7-14
CTL ファイルに問題がある場合の IP Phone のトラブルシューティング	7-27
Cisco IP Phone およびサーバ上の CTL ファイルの比較	7-29
Cisco IP Phone 上の CTL ファイルの削除	7-30
サーバ上の CTL ファイルの削除	7-32
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	7-33
セキュリティ トークン (Etoken) をすべて紛失した場合のトラブルシューティング	7-34
Cisco CallManager クラスタのセキュリティ モードの確認	7-36
Cisco CTL クライアントの確認とアンインストール	7-37
Cisco CTL クライアントのバージョンの特定	7-38
CAPF のトラブルシューティング	7-39
CAPF に関するメッセージ	7-39
IP Phone での認証文字列のトラブルシューティング	7-40

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	7-41
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	7-41
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	7-42
Manufactured-Installed Certificate (MIC) が IP Phone 内に存在することの確認	7-42
暗号化のトラブルシューティング	7-43
SRTP/SCCP のトラブルシューティングの概要	7-43
パケット キャプチャの設定チェックリスト	7-44
パケット キャプチャ サービス パラメータの設定	7-45
パケット キャプチャ サービス パラメータ	7-46
BAT に対するパケット キャプチャの設定	7-47
Phone Configuration ウィンドウでのパケット キャプチャの設定	7-47
IP Phone のパケット キャプチャ設定の設定値	7-48
キャプチャされたパケットの解析	7-50
Cisco CallManager Administration でのパケット キャプチャに関するメッセージ	7-51
暗号化および割り込みの設定に関するメッセージ	7-51
セキュア SRST リファレンスのトラブルシューティング	7-53
SRST リファレンスからのセキュリティの削除	7-53
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	7-53
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	7-54



T A B L E S

表 1	このマニュアルの構成	xiii
表 1-1	用語	1-2
表 1-2	Cisco IP Phone の機能	1-7
表 1-3	認証および暗号化の設定用チェックリスト	1-24
表 2-1	Cisco CallManager 仮想ディレクトリ	2-2
表 3-1	Cisco CTL クライアントの設定用チェックリスト	3-3
表 3-2	CTL クライアントの設定	3-24
表 4-1	CAPF の設定用チェックリスト	4-8
表 4-2	サーバからサーバへのコピー	4-10
表 4-3	CAPF サービス パラメータ	4-14
表 4-4	CAPF エンタープライズ パラメータ	4-16
表 4-5	CAPF 設定	4-20
表 5-1	Device Security Mode	5-9
表 6-1	SRST のセキュリティ設定用チェックリスト	6-3
表 6-2	SRST リファレンスのセキュリティ設定	6-6
表 7-1	HTTPS 設定時に表示されるメッセージ	7-5
表 7-2	Cisco CTL クライアントに関するメッセージ	7-14
表 7-3	IP Phone に関連する CTL ファイルの問題	7-27
表 7-4	Cisco IP Phone 上の CTL ファイルの削除	7-31
表 7-5	CAPF に関するメッセージ	7-39
表 7-6	パケット キャプチャの設定チェックリスト	7-44
表 7-7	パケット キャプチャ設定の設定値	7-46
表 7-8	IP Phone のパケット キャプチャ設定の設定値	7-49
表 7-9	パケット キャプチャに関するメッセージ	7-51



このマニュアルについて

ここでは、このマニュアルの目的、対象読者、構成、および表記法、そして関連資料の入手方法について説明します。

次のトピックについて取り上げます。

- [目的 \(P. xii\)](#)
- [対象読者 \(P. xii\)](#)
- [マニュアルの構成 \(P. xiii\)](#)
- [関連マニュアル \(P. xiv\)](#)
- [表記法 \(P. xv\)](#)
- [技術情報の入手方法 \(P. xvi\)](#)

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。
- 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。
- 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。
- セキュリティに Survivable Remote Site Telephony (SRST) リファレンスを設定する。
- 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
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。
第 4 章「Certificate Authority Proxy Function の使用方法」	Certificate Authority Proxy Function の概要を説明します。また、サポートされている電話機のローカルで有効な証明書をインストール、アップグレード、削除、またはトラブルシューティングする方法も説明します。
第 5 章「電話機のセキュリティ設定」	サポートされている電話機に Device Security Mode を設定する方法を説明します。また、Cisco CallManager Administration で電話機の設定値の一部を無効にしてセキュリティを強化する方法も説明します。
第 6 章「Survivable Remote Site Telephony (SRST) リファレンスのセキュリティ設定」	Cisco CallManager Administration でセキュリティに SRST リファレンスを設定する方法を説明します。
第 7 章「トラブルシューティング」	セキュリティに関連するいくつかの問題を解決する方法を説明します。

関連マニュアル

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

- *Cisco IP Phone 7960G/7940G アドミニストレーション ガイド for Cisco CallManager*
- *Cisco IP Phone Administration Guide for Cisco CallManager, Cisco IP Phone Model 7970G*
- *Cisco IP Phone 7902G/7905G/7912G アドミニストレーション ガイド Cisco CallManager Release 4.0*
- 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
- *Cisco IP Telephony Solution Reference Network Design Guide*
- 通話料金の不正、オペレーティング システムの強化、TCP/UDP ポートなどのトピックに関するセキュリティ アプリケーション ノート
- クラスタにインストールされている Cisco CallManager 4.1 バージョンと互換性のある Cisco Security Agent のマニュアル
- cisco.com でシスコが提供するオペレーティング システムのアップグレードおよびサービス リリースに関する Readme ドキュメント
- ディレクトリ アプリケーション対応の Cisco MultiLevel Administration、通話料金の不正防止、および SSL の使用方法について説明している Cisco CallManager Administration ドキュメント
- Cisco IOS MGCP ゲートウェイに対するメディア認証とシグナリング認証および暗号化機能
- *Configuring IPSEC from Cisco CallManager to MGCP Gateways*
- SRST 対応の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

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。

ヒントでは、次の表記法を使用しています。



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/univercd/home/home.htm>

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>

マニュアルの発注方法（英語版）

英文マニュアルの発注方法については、次の URL にアクセスしてください。

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

シスコ製品の英文マニュアルは、次の方法で発注できます。

- Cisco.com（Cisco Direct Customers）に登録されている場合、Ordering Tool からシスコ製品の英文マニュアルを発注できます。次の URL にアクセスしてください。

<http://www.cisco.com/en/US/partner/ordering/index.shtml>

- 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わせください。

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わせは、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わせください。

テクニカル サポート

シスコと正式なサービス契約を交わしているすべてのお客様、パートナー、および代理店は、Cisco Technical Support で 24 時間テクニカル サポートを利用することができます。Cisco.com の Cisco Technical Support 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、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、代理店にお問い合わせください。

Cisco Technical Support Web サイト

Cisco Technical Support 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 365 日、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 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>

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自動的に検索されます。これらの推奨手段で問題を解決できない場合は、Cisco TAC 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 に電話でお問い合わせください (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、Cisco TAC 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。

シビルティ 4 (S4): シスコ製品の機能、インストール、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、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 Product Catalog』には、シスコシステムズが提供するネットワーキング製品のほか、発注方法やカスタマー サポート サービスについての情報が記載されています。『Cisco Product Catalog』には、次の URL からアクセスしてください。

<http://cisco.com/univercd/cc/td/doc/pcat/>

- 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>

- 『*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>



セキュリティの概要

Cisco CallManager システムに認証および暗号化を実装すると、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。こうした脅威を防ぐために、Cisco IP テレフォニー ネットワークでは認証された通信ストリームを確立して維持し、ファイルを電話機に転送する前にデジタル署名を行い、Cisco IP Phone 間のメディア ストリームおよびコール シグナリングを暗号化します。

この章は、次の内容で構成されています。

- [認証および暗号化に関する用語 \(P.1-2\)](#)
- [システム要件 \(P.1-5\)](#)
- [対話および制限 \(P.1-6\)](#)
- [ベスト プラクティス \(P.1-11\)](#)
- [デバイスのリセット、サービスの再起動、またはサーバおよびクラスタのリブート \(P.1-13\)](#)
- [インストール \(P.1-15\)](#)
- [証明書の種類 \(P.1-16\)](#)
- [認証および整合性の概要 \(P.1-18\)](#)
- [暗号化の概要 \(P.1-21\)](#)
- [設定用チェックリストの概要 \(P.1-24\)](#)
- [その他の情報 \(P.1-29\)](#)

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
認証	エンティティの ID を検証するプロセス。
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 IP Phone が使用するリスト。このファイルは、Cisco CallManager クラスタに Cisco CTL クライアントをインストールおよび設定した後で作成します。ファイルには、Cisco Site Administrator Security Token (セキュリティ トークン) が署名する信頼された項目の事前定義済みリストが含まれており、サーバの証明書および Cisco IP Phone のセキュリティ トークンを検証するための認証情報を提供します。
Cisco Site Administrator Security Token (セキュリティ トークン、etoken)	秘密キーと、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キー取得を行います。
デバイス認証	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。
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。
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。

表 1-1 用語（続き）

用語	定義
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（米国技術特別調査委員会）が定義したプロトコル。暗号化を使用して、IIS サーバとブラウザ クライアントとの間で交換される情報の機密を確保します。
イメージ認証	電話機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。
Locally Significant Certificate (LSC; ローカルで有効な証明書)	電話機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 (仲介者) 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。
混合モード	セキュリティを設定したクラスタ内のモード。Cisco 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。
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。
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 SCCP 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
保護された Survivable Remote Site Telephony (SRST) リファレンス	保護対象の電話機に認証を受けたゲートウェイ。Cisco CallManager がタスクを実行できない場合に、制限付きのコール処理タスクを実行します。
Transport Layer Security (TLS)	IETF によって定義されたセキュリティ 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。

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 4.1(2) はクラスタ内の各サーバに対する最小要件です。
- シスコが提供するオペレーティング システム バージョン 2000.2.6（またはそれ以降）は、クラスタ内の各サーバに対する最小要件です。オペレーティング システム 2000.2.6（またはそれ以降）に対応する最新のオペレーティング システム サービス リリースがインストールされていることを確認します。
- Cisco CTL クライアントをインストールする前に、ワークステーションまたはサーバで Windows 2000 sp3a（またはそれ以降）が動作していることを確認します。
- クラスタ内の各サーバでは、Windows 管理者と同じユーザ名およびパスワードが必要です。
- Certificate Authority Proxy Function (CAPF) については、[P.4-4 の「CAPF システムの対話および要件」](#)を参照してください。

関連項目

- [対話および制限 \(P.1-6\)](#)
- [インストール \(P.1-15\)](#)
- [設定用チェックリストの概要 \(P.1-24\)](#)
- [トラブルシューティング \(P.7-1\)](#)
- [CAPF システムの対話および要件 \(P.4-4\)](#)

対話および制限

この項は、次の内容で構成されています。

- [Cisco CallManager と Cisco IP Phone との対話 \(P.1-6 \)](#)
- [サポートされる電話機でのセキュリティ メニューおよびアイコン \(P.1-8 \)](#)
- [制限 \(P.1-8 \)](#)
- [ベスト プラクティス \(P.1-11 \)](#)
- [デバイスのリセット、サービスの再起動、またはサーバおよびクラスタのリブート \(P.1-13 \)](#)

Cisco CallManager と Cisco IP Phone との対話

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セキュア 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 のインストールを行うと、対応する 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。



ヒント

サポートされていないシナリオまたは安全でないシナリオについては、[P.1-8 の「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。デバイスのいずれか 1 つ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。



(注)

このマニュアルに記載された機能は、限定された Cisco IP Phone モデルでサポートされています。サポートしている電話機の最新リストについては、Cisco CallManager 4.1(2) をサポートする電話機の管理マニュアルを参照してください。

表 1-2 に、さまざまな Cisco IP Phone でサポートされる機能のリストを示します。

表 1-2 Cisco IP Phone の機能

Cisco IP Phone モデル	サポートされている機能
Cisco IP Phone 7970	イメージ認証、ファイル認証、デバイス認証、シグナリング暗号化、メディア暗号化、製造元でインストールされる証明書、ファクトリリセット、および Web サーバ無効化などの電話機のセキュリティ強化
Cisco IP Phone 7960 および 7940	イメージ認証、ファイル認証、デバイス認証、シグナリング暗号化、メディア暗号化、ローカルで有効な証明書、ファクトリリセット、および Web サーバ無効化などの電話機のセキュリティ強化
Cisco IP Phone 7912、 7910、7905G、および 7902	イメージ認証

サポートされる電話機でのセキュリティ メニューおよびアイコン

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、サポートされている電話機で、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 管理およびユーザ マニュアルを参照してください。

同様に、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.1-8 の「制限」](#)を参照してください。

制限

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混合モードに設定すると、自動登録機能は動作しません。
- デバイス認証がクラスタに存在しない場合、つまり 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。
- マルチクラスタ TFTP 構成を使用する場合、Cisco CTL クライアントを介して、すべての Cisco CallManager クラスタに同じセキュリティ モードを設定する必要があります。各クラスタに Cisco CTL クライアントをインストールし、設定時にクラスタ全体で同じセキュリティ モードを選択する必要があります。



注意

設定ファイルを作成するための TFTP パスおよび代替 TFTP パスは必ず固有のパスにしてください。パスが固有でない場合、ほかのクラスタが作成した CTL ファイルが TFTP サーバによって上書きされる可能性があります。

- クラスタを混合モードに設定した場合、シスコでは Cisco CallManager による Network Address Translation (NAT; ネットワーク アドレス変換) をサポートしません。VOIP のファイアウォールおよび NAT トラバーサルを許可する Application Layer Gateways (ALG) 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 を有効化すると、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 を有効化すると、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。

- 割り込みに使用する電話機に暗号化が設定されていない場合、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。

ここで説明した情報は、[P.7-51](#) の「[暗号化および割り込みの設定に関するメッセージ](#)」と併せて使用してください。



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せん。

- 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。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。
- Cisco CallManager はメディア リソースが使用されていない単一クラスタ内のセキュア Cisco IP Phone とセキュア IOS ゲートウェイとの間で、認証済み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 4.1(2) は認証、整合性、暗号化をどれも提供しません。
 - Computer Telephony Integration (CTI; コンピュータテレフォニー インテグレーション) デバイス、一部のゲートウェイ、クラスタ間トランク、トランスコーダ、メディア終端点
 - 2 つの異なるクラスタを介して行われるコール
 - Ad hoc 会議または Meet Me 会議
 - Music on Hold (MOH; 保留音楽)
 - Session Initiation Protocol (SIP; セッション開始プロトコル) および H.323 デバイス
 - 一部の Cisco IP Phone モデル



ヒント

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。

**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。

CAPF を使用すると CPU 使用率が上昇するため、CAPF を使用して証明書を生成するときは VNC を使用しないでください。

ベスト プラクティス

シスコでは、次のベスト プラクティスを強く推奨します。

- 必ず安全なテスト環境でインストールおよび設定タスクを実行してから、広範囲のネットワークに展開する。
- Cisco CallManager 4.1 は DC Directory に対して LDAPS (LDAP over SSL) を自動的にインストールする。Microsoft Active Directory や Netscape Server Directory など、会社のディレクトリを Cisco CallManager と統合する場合には、SSL をサポートするオプションを設定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、『*Installing Cisco Customer Directory Configuration Plugin for Cisco CallManager 4.0(1)*』を参照してください。

LDAPS を使用するシスコ提供アプリケーションのリストについては、『*Cisco CallManager システム ガイド*』を参照してください。

- このマニュアルに記載されている機能は、Cisco.com で入手可能なシスコが提供する最新のオペレーティング システムのサービス リリースおよびアップグレードと共に使用する。
- このマニュアルに記載されている機能は、このリリースの Cisco CallManager をサポートする Cisco Security Agent と共に使用する。
- このマニュアルに記載されている機能は、シスコ認定のサードパーティ製セキュリティ アプリケーション (MacAfee アンチウイルス ソフトウェアなど) と共に使用する。
- リモート ロケーションにあるゲートウェイおよびその他のアプリケーション サーバに対しては Windows ネイティブ モード IPSEC を使用する。たとえば、Cisco Unity、Cisco IP Contact Center (IPCC)、その他の Cisco CallManager サーバなどです。

- Cisco CallManager およびセキュアな Cisco IOS MGCP ゲートウェイ間の IPSEC を設定する。Cisco IOS MGCP ゲートウェイには、2600 XM、2691、2811、2821、2851、3640A、3660、3725、3745、38XX シリーズ、および VG224 があります。

Cisco CallManager サーバおよびゲートウェイを設定した後、Windows 2000 IPSEC を使用すると、セキュアな MGCP ゲートウェイが Cisco CallManager と連携します。これで、MGCP ゲートウェイと Cisco CallManager の間でシグナリング情報（たとえば、DTMF 番号、パスワード、PIN、暗号キーなど）が送信されるたびに、確実に暗号化されます。MGCP ゲートウェイと Cisco CallManager の間のコール制御とシグナリング パケットはすべて、このセキュア IPSEC トンネルを経由します。

Cisco CallManager は、セキュア コールのためのマスター暗号キーとソルトを生成し、SRTP ストリームの場合にのみゲートウェイに送信します。Cisco IOS MGCP ゲートウェイでサポートされている SRTCP ストリームの場合、Cisco CallManager はキーとソルトを送信しません。

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必要です。Cisco CallManager は、デバイスに対する SRTP 接続を確立しますが、デバイスが SRTP をサポートしていなければ、ゲートウェイと交信して、コールが RTP 接続を使用することを確認します。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、保留音楽、非 SRTP トランスコードを使用するコールなどで発生する場合があります。

Cisco IOS MGCP ゲートウェイおよび Cisco CallManager 間のセキュリティを設定するには、Cisco CTL クライアントを混合モードでインストールおよび設定したことを確認してください。Cisco CallManager Administration で、電話機に暗号化を設定したことを確認します。次に、Cisco CallManager およびゲートウェイ間で、IPSEC を設定します。IPSEC の設定方法に関する情報については、Microsoft および / またはシスコが提供している IPSEC 関連資料を参照してください。最後に、『*Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*』で記載されたように、ゲートウェイ上でセキュリティ関連の設定タスクを実行します。このドキュメントは、次の URL から入手できます。

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

- 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。
- SRST リファレンスおよび SRST 対応ゲートウェイでセキュリティを設定する。
- Cisco CallManager から MGCP ゲートウェイまで IPSEC を設定する。

デバイスのリセット、サービスの再起動、またはサーバおよびクラスタのリポート

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

次のガイドラインを考慮します。

- 単一デバイスのセキュリティ モードを Cisco CallManager Administration で変更した後は、デバイスをリセットする。
- 電話機のセキュリティ強化作業を実行した場合は、デバイスをリセットする。
- クラスタ全体のセキュリティ モードを混合モードからノンセキュア 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。
- 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。
- CAPF エンタープライズパラメータの更新後は、デバイスをリセットする。
- TLS 接続用のポートを更新した後は、Cisco CTL Provider サービスを再起動する。
- クラスタ全体のセキュリティ モードを混合モードからノンセキュア 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動するすべてのサーバで実行します。
- 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。

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.5-6 の「単一デバイスに対するデバイス セキュリティ モードの設定」](#)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。
 - ステップ 2 ウィンドウの左側のペインで、サーバを選択します。
 - ステップ 3 **Reset Devices** をクリックします。
 - ステップ 4 クラスタ内のサーバごとに、[ステップ 2](#) と [ステップ 3](#) を実行します。
-

関連項目

- [システム要件 \(P.1-5\)](#)
- [Cisco CTL クライアントの設定 \(P.3-1\)](#)
- [Certificate Authority Proxy Function の使用方法 \(P.4-1\)](#)
- [設定用チェックリストの概要 \(P.1-24\)](#)
- [トラブルシューティング \(P.7-1\)](#)

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 クライアントは、USB ポートのある単一の Windows 2000 サーバまたはワークステーションにインストールする必要があります。USB ポートのある Cisco CallManager サーバにクライアントをインストールするよう選択することもできます。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。

関連項目

- [Cisco CTL クライアントの設定 \(P.3-1 \)](#)
- [HTTP over SSL \(HTTPS \) の使用方法 \(P.2-1 \)](#)

証明書の種類

シスコでは次の種類の証明書を電話機およびサーバで使用します。

- **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。
- **CAPF 証明書:** この証明書は、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。この証明書は、クラスタ内の各サーバで C:\Program Files\Cisco\Certificates にインストールされます。
- **HTTPS 証明書:** SSL 対応の Cisco CallManager 仮想ディレクトリをホスティングする IIS Web サイトにインストールされると、このサーバ認証証明書 `httpscert.cer` は IIS サーバとブラウザ クライアントとの間の認証を提供します。この証明書は C:\Program Files\Cisco\Certificates にインストールされます。
- **自己署名 Cisco CallManager 証明書:** この証明書 `ccmserver.cer` は、Cisco CallManager 4.1 のインストール時に自動的にインストールされます。
Cisco CallManager 自己署名証明書によって、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。Cisco CallManager は、DER 形式の証明書をクラスタ内の各サーバの C:\Program Files\Cisco\Certificates に格納します。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。
- **SRST 対応ゲートウェイの SRST 証明書:** SRST リファレンスでセキュリティを設定し、電話機をリセットした後で、この証明書は Cisco CallManager データベースに追加されます。電話機はこの証明書を設定ファイルから取得しま

す。この証明書は、Cisco CTL ファイルにはありません。ゲートウェイの SRST 証明書の詳細については、ゲートウェイをサポートする Cisco SRST のマニュアルを参照してください。

関連項目

- [対話および制限 \(P.1-6\)](#)
- [インストール \(P.1-15\)](#)
- [認証および整合性の概要 \(P.1-18\)](#)
- [HTTP over SSL \(HTTPS\) の使用方法 \(P.2-1\)](#)
- [Cisco CTL クライアントの設定 \(P.3-1\)](#)
- [Certificate Authority Proxy Function の使用方法 \(P.4-1\)](#)
- [Survivable Remote Site Telephony \(SRST\) リファレンスのセキュリティ設定 \(P.6-1\)](#)

認証および整合性の概要

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（仲介者）攻撃（認証）
- 電話機およびサーバの ID 盗難（認証）

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。

サポートされるデバイスのリストについては、[P.1-6 の「対話および制限」](#)を参照してください。

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要求する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.1-6 の「対話および制限」](#)を参照してください。

デバイス認証は、各エンティティが他方のエンティティの持つ証明書を受け入れるときに、Cisco CallManager サーバとサポートされる Cisco IP Phone との間で行われます。そのときだけ、エンティティ間の接続が保護されます。デバイス認証は、[P.3-1 の「Cisco CTL クライアントの設定」](#)で説明するように、Cisco CTL ファイルの作成に依存します。

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。電話機はシグニチャを検証して、ファイルの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.1-6の「対話および制限」](#)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。クラスタを混合モードに設定した場合、TFTP サーバは呼出音一覧、ローカライズ、デフォルトの .cnf.xml、呼出音一覧 wav 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 TLS 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。

関連項目

- システム要件 (P.1-5)
- 対話および制限 (P.1-6)
- Cisco CTL クライアントの設定 (P.3-1)
- Certificate Authority Proxy Function の使用方法 (P.4-1)
- デバイス セキュリティ モードの設定 (P.5-4)
- トラブルシューティング (P.7-1)

暗号化の概要



ヒント

暗号化は、Cisco CallManager 4.1 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。暗号化をサポートするデバイスのリストについては、[P.1-5](#) の「**システム要件**」を参照してください。

セキュリティ パッケージのファイルは、C:\Program Files\Cisco\bin 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 \(P.1-21\)](#)
- [メディア暗号化 \(P.1-22\)](#)

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 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、メディア暗号キーなどについて、予期しないアクセスや不正アクセスから保護します。

クラスタを混合モードに設定した場合、シスコでは Cisco CallManager による Network Address Translation (NAT; ネットワーク アドレス変換) をサポートしません。VOIP のファイアウォールおよび NAT トラバースを許可する Application Layer Gateways (ALG) 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 を有効化すると、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 を有効化すると、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。

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 キー ペアの作成、デバイスへのキー配送、キー転送中の配送の保護が含まれます。

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。

次の例で、具体的にメディア暗号化を説明します。

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キーを取得します。
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キーを取得します。
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、キーを受信した後に必要なキー導出を実行し、SRTP パケット処理が行われます。

**ヒント**

サポートされる項目のリストについては、P.1-6 の「[対話および制限](#)」を参照してください。

関連項目

- [システム要件](#) (P.1-5)
- [対話および制限](#) (P.1-6)
- [デバイス セキュリティ モードの設定](#) (P.5-4)
- [トラブルシューティング](#) (P.7-1)

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	<p>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。</p> <p></p> <p>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。</p>	Cisco CTL Provider サービスのアクティブ化 (P.3-5)
ステップ 2	<p>パブリッシャ データベース サーバの 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。</p> <p></p> <p>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。</p>	Certificate Authority Proxy Function サービスのアクティブ化 (P.4-12)

表 1-3 認証および暗号化の設定用チェックリスト（続き）



設定手順	関連手順および関連項目
<p>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。</p> <p> 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。</p>	<p>TLS 接続用ポートの設定 (P.3-8)</p>
<p>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。</p>	<p>CiscoCTL クライアントの設定 (P.3-14)</p>
<p>ステップ 5 Cisco CTL クライアントをインストールします。</p> <p> 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 4.1 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 4.1 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。ファイルを変更する必要がない場合、クライアントの 4.1 バージョンをインストールする必要はありません。</p>	<ul style="list-style-type: none"> • システム要件 (P.1-5) • インストール (P.1-15) • Cisco CTL クライアントのインストール (P.3-10)

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	<p>Cisco CTL クライアントを設定します。</p> <p> 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 4.1 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 4.1 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。</p>	<p>CiscoCTL クライアントの設定 (P.3-14)</p>
ステップ 7	<p>証明書を発行するように CAPF を設定します。</p> <p>Cisco CallManager 4.1 へのアップグレード前に証明書の操作を実行して CAPF をサブスクリバサーバで実行した場合、CAPF データを 4.0 パブリッシャデータベースサーバにコピーしてから、クラスタを Cisco CallManager 4.1 にアップグレードする必要があります。</p> <p> 注意 Cisco CallManager 4.0 サブスクリバサーバの CAPF データは Cisco CallManager 4.1 データベースに移行されません。したがって、データを 4.1 パブリッシャデータベースにコピーしないと、データは失われます。データが失われた場合、CAPF utility 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が、CAPF 4.1(2) は証明書を再発行します。しかし、この証明書は有効ではありません。</p>	<ul style="list-style-type: none"> • システム要件 (P.1-5) • CAPF の設定用チェックリスト (P.4-8) • 既存の CAPF データの移行 (P.4-6) • 4.0 サブスクリバサーバから 4.0 パブリッシャデータベースサーバへの CAPF 1.0(1) データのコピー (P.4-10)

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 8 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。	<ul style="list-style-type: none"> システム要件 (P.1-5) 電話機での認証文字列の入力 (P.4-25) 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 (P.7-42)
ステップ 9 サポートされているデバイスに認証または暗号化を設定します。  ヒント デバイス設定は、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、Cisco CallManager Administration の Phone Configuration ウィンドウで Device Security Mode を更新する必要があります。	デバイス セキュリティ モードの設定 (P.5-4)
ステップ 10 SRST リファレンスのセキュリティを設定します。  ヒント この機能は、Cisco CallManager 4.1(1) 以降でサポートされています。	Survivable Remote Site Telephony (SRST) リファレンスのセキュリティ設定 (P.6-1)
ステップ 11 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作業の実行 (P.5-14)
ステップ 12 Cisco CallManager およびセキュアな Cisco IOS MGCP ゲートウェイ間で、IPSEC を設定します。	ベスト プラクティス (P.1-11)

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 13	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.1-13)
ステップ 14	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.1-13)

その他の情報

シスコの関連マニュアル

- *Cisco IP Phone 7960G/7940G アドミニストレーション ガイド for Cisco CallManager*
- *Cisco IP Phone Administration Guide for Cisco CallManager, Cisco IP Phone Model 7970G*
- *Cisco IP Phone 7902G/7905G/7912G アドミニストレーション ガイド Cisco CallManager Release 4.0*
- 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
- *Cisco IP Telephony Solution Reference Network Design Guide*
- 通話料金の不正、オペレーティング システムの強化、TCP/UDP ポートなどのトピックに関するセキュリティ アプリケーション ノート
- クラスタにインストールされている Cisco CallManager 4.1 バージョンと互換性のある Cisco Security Agent のマニュアル
- cisco.com でシスコが提供するオペレーティング システムのアップグレードおよびサービス リリースに関する Readme ドキュメント
- ディレクトリ アプリケーション対応の Cisco MultiLevel Administration、通話料金の不正防止、および SSL の使用方法について説明している Cisco CallManager Administration ドキュメント
- Cisco IOS MGCP ゲートウェイに対するメディア認証とシグナリング認証および暗号化機能
- *Configuring IPSEC from Cisco CallManager to MGCP Gateways*
- SRST 対応の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



HTTP over SSL (HTTPS) の使用方法

この章は、次の内容で構成されています。

- [HTTPS の概要 \(P.2-2 \)](#)
- [Internet Explorer を使用して証明書を信頼できるフォルダに保存する方法 \(P.2-6 \)](#)
- [証明書の詳細表示 \(P.2-7 \)](#)
- [証明書のファイルへのコピー \(P.2-8 \)](#)
- [Netscape を使用して証明書を信頼できるフォルダに保存する方法 \(P.2-11 \)](#)
- [サードパーティの認証局によるサーバ認証証明書の使用方法 \(P.2-13 \)](#)

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 IIS サーバとの間の通信を保護し、証明書および公開キー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、Bulk Administration Tool (BAT)、TAPS、Cisco CDR Analysis and Reporting (CAR)、Trace Collection Tool、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場合、HTTPS 自己署名証明書である httpscert.cer は、表 2-1 の Cisco CallManager 仮想ディレクトリをホスティングする IIS のデフォルト Web サイトに自動的にインストールされます。

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 IP Phone User Option Pages
AST	Real-Time Monitoring Tool (RTMT)
RTMTReports	RTMT レポート アーカイブ
CCMTraceAnalysis	Trace Analysis Tool
PktCap	IREC などのツール
	 (注) こうしたトラブルシューティング ツールでは、仮想ディレクトリを使用して SCCP シグナリング パケット トレースの含まれるトレース ファイルを取得します。
ART	Cisco CDR Analysis and Reporting (CAR)

表 2-1 Cisco CallManager 仮想ディレクトリ (続き)

Cisco CallManager 仮想ディレクトリ	対応するアプリケーション
CCMSERVICETraceCollection Tool	Trace Collection Tool
BAT	Bulk Administration Tool (BAT)
TAPS	Tool for Auto-Registered Phones Support (TAPS)

HTTPS 証明書は、C:\Program Files\Cisco\Certificates ディレクトリに格納されま
す。必要に応じて、認証局からサーバ認証証明書をインストールし、HTTPS 自
己署名証明書の代わりに使用することができます。Cisco CallManager のインス
トールまたはアップグレード後に認証局の証明書を使用するには、P.7-1 の「[ト
ラブルシューティング](#)」で説明するように、自己署名証明書を削除する必要があ
ります。次に、認証局の資料で説明されているように、認証局から提供された
サーバ認証証明書をインストールします。



(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。

関連項目

- *Cisco CallManager アドミニストレーション ガイド*
- *Cisco CallManager システム ガイド*
- *Bulk Administration Tool ユーザ ガイド*

- *Cisco CallManager Serviceability アドミニストレーション ガイド*
- *Cisco CallManager Serviceability System Guide*
- *Web での Cisco IP Phone のカスタマイズ*
- [Internet Explorer を使用して証明書を信頼できるフォルダに保存する方法 \(P.2-6\)](#)
- [証明書の詳細表示 \(P.2-7\)](#)
- [証明書のファイルへのコピー \(P.2-8\)](#)

Internet Explorer による HTTPS の使用方法

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

- [Internet Explorer を使用して証明書を信頼できるフォルダに保存する方法 \(P.2-6\)](#)
- [証明書の詳細表示 \(P.2-7\)](#)
- [証明書のファイルへのコピー \(P.2-8\)](#)

Cisco CallManager 4.1 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 またはほかの 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。

関連項目

- [HTTPS の概要 \(P.2-2\)](#)
- [Internet Explorer を使用して証明書を信頼できるフォルダに保存する方法 \(P.2-6\)](#)
- [証明書の詳細表示 \(P.2-7\)](#)
- [証明書のファイルへのコピー \(P.2-8\)](#)
- [HTTPS のトラブルシューティング \(P.7-5\)](#)

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 IIS サーバでアプリケーションを参照します。
 - 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 **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** に移動します。
 - 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 **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。

関連項目

- [HTTPS の概要 \(P.2-2\)](#)
- [証明書の詳細表示 \(P.2-7\)](#)
- [証明書のファイルへのコピー \(P.2-8\)](#)

証明書の詳細表示

証明書の詳細を表示するには、次の作業のどちらかを実行します。

- **View Certificate** ボタンをクリックしてから、**Details** タブをクリックします。
- 証明書が存在するサーバの `C:\Program Files\Cisco\Certificates\httpscert.cert` で証明書を右クリックし、**Open** をクリックします。



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。次の設定の説明については、Microsoft の資料を参照してください。

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 : ある場合は 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せん。

関連項目

- [HTTPS の概要 \(P.2-2\)](#)
- [Internet Explorer を使用して証明書を信頼できるフォルダに保存する方法 \(P.2-6\)](#)
- [証明書のファイルへのコピー \(P.2-8\)](#)

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。また、次の手順を実行して、別のユーザから受信した証明書ファイルをインストール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 Welcome 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。ファイルのエクスポート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の情報で転送します。
 - **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 エクスポートするファイルに移動します。
- ステップ 7 **Finish** をクリックします。
- ステップ 8 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。
-

関連項目

- [HTTPS の概要 \(P.2-2\)](#)
- [Internet Explorer を使用して証明書を信頼できるフォルダに保存する方法 \(P.2-6\)](#)
- [証明書の詳細表示 \(P.2-7\)](#)

Netscape による HTTPS の使用方法

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。



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。

関連項目

- [HTTPS の概要 \(P.2-2\)](#)
- [Netscape を使用して証明書を信頼できるフォルダに保存する方法 \(P.2-11\)](#)
- [HTTPS のトラブルシューティング \(P.7-5\)](#)

Netscape を使用して証明書を信頼できるフォルダに保存する方法

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 からアクセスします。

ステップ 2 New Site Certificate ウィンドウが表示されたら、**Next** をクリックします。

ステップ 3 次の New Site Certificate ウィンドウが表示されたら、**Next** をクリックします。



ヒント

Next をクリックする前に証明書のクレデンシャルを表示するには、**More Info** をクリックします。クレデンシャルを確認して **OK** をクリックした後、New Site Certificate ウィンドウで **Next** をクリックします。

ステップ 4 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)

ステップ 5 **Next** をクリックします。

ステップ 6 Do not accept this certificate... オプション ボタンをクリックした場合は、[ステップ 8](#)に進みます。

ステップ 7 情報がほかのサイトへ送信される前に Netscape で警告を表示する場合は、**Warn me before I send information to this site** チェックボックスをオンにし、**Next** をクリックします。

ステップ 8 **Finish** をクリックします。

関連項目

- [HTTPS の概要 \(P.2-2\)](#)
- [Netscape による HTTPS の使用方法 \(P.2-10\)](#)
- [HTTPS のトラブルシューティング \(P.7-5\)](#)

サードパーティの認証局によるサーバ認証証明書 の使用法

Cisco CallManager 提供の証明書ではなく、サードパーティの認証局によるサーバ認証証明書を使用するには、次の手順を実行します。

手順

ステップ 1 P.7-7 の「HTTPS の有効化」の説明に従って、HTTPS 証明書を削除します。

ステップ 2 使用する証明書をインストールします。

ステップ 3 証明書ファイルを右クリックします。

ステップ 4 **Install Certificate** オプションを選択します。



ヒント インストールは、デフォルト設定を使用して実行できます。

ステップ 5 次の手順を実行して、IIS のデフォルト Web サイトに証明書をインストールします。

- a. **Start > Programs > Administrative Tools > Internet Service Manager** の順に選択します。
- b. 証明書をインストールするサーバの名前をクリックします。
- c. **Directory Security** タブをクリックします。
- d. **Secure Communications** で **Server Certificate** ボタンをクリックします。
- e. **Next** をクリックします。
- f. **Assign an Existing Certificate** オプションを選択します。
- g. ステップ 2 の証明書を選択します。
- h. **Next** をクリックします。
- i. **Finish** をクリックします。

関連項目

- [トラブルシューティング \(P.7-1\)](#)
- [HTTPS の概要 \(P.2-2\)](#)



Cisco CTL クライアントの設定

この章は、次の内容で構成されています。

- [Cisco CTL クライアントの概要 \(P.3-2\)](#)
- [Cisco CTL クライアントの設定用チェックリスト \(P.3-3\)](#)
- [Cisco CTL Provider サービスのアクティブ化 \(P.3-5\)](#)
- [TLS 接続用ポートの設定 \(P.3-8\)](#)
- [Cisco CTL クライアントのインストール \(P.3-10\)](#)
- [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 \(P.3-13\)](#)
- [CiscoCTL クライアントの設定 \(P.3-14\)](#)
- [CTL ファイルの更新 \(P.3-20\)](#)
- [クラスタ全体のセキュリティ モードの更新 \(P.3-23\)](#)
- [Cisco CTL クライアント設定 \(P.3-24\)](#)
- [CTL ファイル エントリの削除 \(P.3-27\)](#)

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、Cisco Certificate Trust List (CTL) クライアントを USB ポートのある単一の Windows 2000 ワークステーションまたはサーバ (Cisco CallManager サーバなど) にインストールおよび設定したときに作成されます。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)
- 代替の Cisco TFTP

CTL ファイルには、サーバのサーバ証明書、公開キー、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 は .tlv 形式の CTL ファイルを TFTP File Location および TFTP Alternate File Locations で指定されたディレクトリに格納します。

Cisco CTL クライアントをインストールおよび設定し、証明書が電話機に存在することを確認して、デバイスに認証または暗号化を設定したら、電話機は TLS SCCP ポートを介して TLS 接続を確立します。このポートは、443 を加算 (+) したポート番号に設定されています。デフォルトでは、電話機は TLS を使用してポート 2443 に接続します。ハンドシェイクによって証明書が認証され、保護された接続が確立されます。



関連項目

- [Cisco CTL クライアントの設定用チェックリスト \(P.3-3\)](#)
- [認証および整合性の概要 \(P.1-18\)](#)

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
<p>ステップ 1 クラスタにある各 Cisco CallManager および Cisco TFTP 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。</p> <p> 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。</p>	<p>Cisco CTL Provider サービスのアクティブ化 (P.3-5)</p>
<p>ステップ 2 パブリッシャ データベース サーバの Cisco CallManager Serviceability で Cisco Certificate Authority Proxy サービスをアクティブにします。</p> <p> 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。</p>	<p>Certificate Authority Proxy Function サービスのアクティブ化 (P.4-12)</p>

Cisco CTL クライアントの設定用チェックリスト

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 3	<p>デフォルト設定を使用しない場合は、TLS 接続用のポートを設定します。</p> <p> 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。</p>	TLS 接続用ポートの設定 (P.3-8)
ステップ 4	<p>Cisco CTL クライアント用に設定するサーバについて、少なくとも2つのセキュリティトークンとパスワード、ホスト名または IP アドレス、およびポート番号を入手します。</p>	CiscoCTL クライアントの設定 (P.3-14)
ステップ 5	<p>Cisco CTL クライアントをインストールします。</p> <p> 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 4.1 にアップグレードした後で CTL ファイルを更新するには、Cisco CallManager Administration 4.1 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。</p>	<ul style="list-style-type: none"> • システム要件 (P.1-5) • インストール (P.1-15) • Cisco CTL クライアントのインストール (P.3-10)
ステップ 6	<p>Cisco CTL クライアントを設定します。</p> <p> ヒント Cisco CallManager のアップグレード前に CTL ファイルを作成した場合、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 Release 4.1 にアップグレードした後で CTL ファイルを更新するには、Cisco CallManager Administration 4.1 で使用可能な Cisco CTL クライアントをインストールおよび設定する必要があります。</p>	CiscoCTL クライアントの設定 (P.3-14)

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混合モード、およびその逆に変更され、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。

ローカルの Administrator パスワードまたは Power Users アカウントのユーザ名とパスワードが、すべての Cisco CallManager および Cisco TFTP サーバ上で同期されていることを確認します。

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 ウィンドウの左側のペインで、Cisco CallManager 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 **CTL Provider** サービス チェックボックスをオンにします。
- ステップ 4 **Update** 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) サービスをアクティブにすると、Cisco CTL Provider サービスはデフォルトの CTL ポート (2444) に復元されます。このポートを変更する場合は、[P.3-8 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** の順に選択します。

関連項目

- *Cisco CallManager Serviceability アドミニストレーション ガイド*
- *Cisco CallManager Serviceability System Guide*
- [Cisco CTL Provider サービスのアクティブ化 \(P.3-5\)](#)
- [Cisco CTL クライアントのインストール \(P.3-10\)](#)

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.4-12](#)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。

関連項目

- [Cisco CTL クライアントの設定用チェックリスト \(P.3-3\)](#)
- [CAPF の設定用チェックリスト \(P.4-8\)](#)
- [Certificate Authority Proxy Function サービスのアクティブ化 \(P.4-12\)](#)
- [設定用チェックリストの概要 \(P.1-24\)](#)

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。

Cisco CallManager ポートでは、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。混合モードの場合、Cisco CallManager の TLS 接続用ポートは Cisco CallManager のポート番号に 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。



ヒント

ポートを更新した後は、Cisco CallManager Administration で Cisco Provider サービスを再起動する必要があります。

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 ポートを変更するには、**ステップ 2 ~ ステップ 6** を実行します。
- Cisco CallManager ポートを変更するには、**ステップ 7 ~ ステップ 10** 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 **Service > Service Parameters** の順に選択します。

ステップ 3 Cisco CTL Provider サービスが実行されているサーバを選択します。

ステップ 4 Cisco CTL Provider サービスを選択します。



ヒント ウィンドウの右上隅にある **i** ボタンをクリックすると、サービスパラメータに関する情報を確認できます。

ステップ 5 Cisco CTL Provider ポートを変更するには、Port Number 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 **Update** をクリックします。

ステップ 7 Cisco CallManager ポートを変更するには、Cisco CallManager Administration で **System > Cisco CallManager** の順に選択します。

ステップ 8 Cisco CallManager サービスが実行されているサーバを選択します。

ステップ 9 Ethernet Phone 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 **Update** をクリックします。

関連項目

- [Cisco CTL Provider サービスのアクティブ化 \(P.3-5\)](#)
- [Cisco CTL クライアントのインストール \(P.3-10\)](#)
- [CiscoCTL クライアントの設定 \(P.3-14\)](#)
- [Cisco CTL クライアント設定 \(P.3-24\)](#)
- [トラブルシューティング \(P.7-1\)](#)

Cisco CTL クライアントのインストール

Cisco CTL クライアントは、USB ポートのある単一の Windows 2000 ワークステーションまたはサーバにインストールします。サーバまたはワークステーションはリモート サイトに置くことができます。Cisco CallManager がインストールされているサーバに USB ポートさえあれば、このサーバにクライアントをインストールすることもできます。

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。

- 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



注意

Terminal Services は、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。

プラグインを実行する前に、Cisco Security Agent (CSA)、またはシスコが認定したその他の侵入検知あるいはアンチウイルス アプリケーションを無効にしておく必要があります。アプリケーションを無効にしないと、インストールすることができず、回復不可能なエラーが発生する場合があります。



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。この作業を実行する方法については、[P.7-1 の「トラブルシューティング」](#)を参照してください。

プラグインのインストール中に表示される可能性があるメッセージのリストを確認するには、[P.7-1 の「トラブルシューティング」](#)を参照してください。

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 Smart Card サービスが started および automatic に設定されていることを確認します。詳細については、P.7-13 の「[Smart Card サービスの Started および Automatic への設定](#)」を参照してください。
- ステップ 2 USB ポートのある Windows 2000 ワークステーションまたはサーバから Cisco CallManager Administration を参照します。この場所は、クライアントをインストールしようとしている場所です。
- ステップ 3 Cisco CallManager Administration で、**Application > Install Plugins** の順に選択します。
- ステップ 4 ファイルをダウンロードするには、**Cisco CTL Client** をクリックします。
- ステップ 5 ファイルを任意の場所にダウンロードします。
- ステップ 6 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。
- ステップ 7 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 8 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 9 使用許諾契約に同意して **Next** をクリックします。
- ステップ 10 クライアントが存在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 11 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 12 インストールが完了したら、**Finish** をクリックして終了します。



ヒント

クライアントがインストールされたことを確認するには、P.7-1 の「[トラブルシューティング](#)」を参照してください。

関連項目

- [システム要件 \(P.1-5\)](#)
- [対話および制限 \(P.1-6\)](#)
- [Cisco CTL Provider サービスのアクティブ化 \(P.3-5\)](#)
- [Smart Card サービスの Started および Automatic への設定 \(P.7-13\)](#)
- [Cisco CTL Provider サービスのアクティブ化 \(P.3-5\)](#)
- [CiscoCTL クライアントの設定 \(P.3-14\)](#)
- [CTL ファイルの更新 \(P.3-20\)](#)
- [CTL ファイル エントリの削除 \(P.3-27\)](#)
- [デバイス セキュリティ モードの設定 \(P.5-4\)](#)
- [トラブルシューティング \(P.7-1\)](#)

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 4.1 にアップグレードした後で CTL ファイルを変更するには、Cisco CallManager Administration 4.1 で使用可能な Cisco CTL クライアントをインストールおよび設定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。

関連項目

- [Cisco CTL クライアントの設定用チェックリスト \(P.3-3\)](#)
- [Cisco CTL クライアントのインストール \(P.3-10\)](#)
- [CiscoCTL クライアントの設定 \(P.3-14\)](#)
- [トラブルシューティング \(P.7-1\)](#)

CiscoCTL 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 クラスタ全体に混合モードを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.3-24 の「Cisco CTL クライアント設定」](#)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、代替 TFTP、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、Cisco TFTP サーバ、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。

代替 TFTP サーバおよび Site Administrator Security Token (SAST) は手動で CTL ファイルに追加する必要があります。

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。



ヒント

代替 TFTP サーバは、異なるクラスタにある場合でも設定することができます。手動で設定することにより、代替 TFTP サーバからの証明書が CTL ファイルに追加されます。これは、TFTP サービスパラメータで指定された FileLocation パスに書き込まれます。マルチクラスタ構成では、代替 TFTP サーバ上のドライブをマッピングし、FileLocation パラメータをマッピングされたドライブに設定する必要があります。たとえば、代替 TFTP サーバとして TFTP1 を使用し、ドライブ L: を TFTP1 上のパスにマッピングした場合、FileLocation は L:\TFTPPath となります。TFTP サーバを追加する必要があります。たとえば、TFTP1 の場合、TFTP1 の有効な管理者ユーザ名とパスワードを指定して追加します。Cisco CTL クライアントによって、CTL ファイルが L:\TFTPPath に書き込まれます。

この TFTP 設定を実装する前に、マルチクラスタ環境にあるすべてのサーバで、同じバージョンの Cisco CallManager が実行され、同じクラスタ全体のセキュリティモードが設定されている必要があります。マルチクラスタ環境にあるすべてのサーバで、Cisco CTL Provider サービスを実行する必要があることに注意してください。

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。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 用のローカル管理者パスワード、ホスト名または IP アドレス、CTL Provider サービス用のポート番号
- 代替 TFTP 用のローカル管理者パスワードと、ホスト名または IP アドレス
- 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、クラスタ内の各サーバに対してネットワーク接続があることを確認してください。同様に、サーバが DNS を使用していること、および各サーバが実行中であることを確認してください。クラスタ内のすべてのサーバに対してネットワーク接続があることを確認するには、各サーバに ping コマンドを発行します。**Start > Run** の順に選択してから、**cmd** と入力し、**OK** をクリックします。コマンドプロンプトで **ping <server>** と入力します。ここで **server** には Cisco CallManager Administration の Server Configuration ウィンドウに表示されるサーバの名前を指定します。クラスタ内のサーバごとに、ping コマンドを繰り返します。

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られません。ただし、設定作業は同時に 5 台までの Cisco CTL クライアントで実行できます。あるクライアントで設定作業を実行している間、その他のクライアントで入力した情報は Cisco 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完了後に

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。
- CTL ファイルを設定された代替 TFTP サーバに書き込む。
- CAPF capf.cer をクラスタ内のすべての Cisco CallManager サブスクライバに書き込む。
- 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 サブスクライバに書き込む。

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 の説明にあるように、**Set CallManager Cluster to Mixed Mode** をクリックし、Next をクリックします。

ステップ 5 設定する内容に応じて、次の作業を実行します。

- セキュリティ トークンを追加するには、[ステップ 6](#) ~ [ステップ 12](#) を参照します。
- 代替 TFTP サーバを追加するには、[ステップ 13](#) ~ [ステップ 15](#) 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 ほかのセキュリティ 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。代替 TFTP サーバを追加する必要がある場合は、**Add TFTP Server** をクリックします。
- 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.1-13 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。



ヒント

Cisco CallManager クラスタが混合モードに設定されたことを確認するには、P.7-1 の「[トラブルシューティング](#)」を参照してください。

セキュリティ トークンのパスワード変更を求めるプロンプトが表示される場合は、P.7-1 の「[トラブルシューティング](#)」を参照してください。

関連項目

- [Cisco CTL クライアント設定 \(P.3-24 \)](#)
- [システム要件 \(P.1-5 \)](#)
- [対話および制限 \(P.1-6 \)](#)
- [Cisco CTL Provider サービスのアクティブ化 \(P.3-5 \)](#)
- [Smart Card サービスの Started および Automatic への設定 \(P.7-13 \)](#)
- [Cisco CTL Provider サービスのアクティブ化 \(P.3-5 \)](#)
- [Cisco CTL クライアント設定 \(P.3-24 \)](#)
- [CiscoCTL クライアントの設定 \(P.3-14 \)](#)
- [CTL ファイルの更新 \(P.3-20 \)](#)
- [デバイス セキュリティ モードの設定 \(P.5-4 \)](#)
- [トラブルシューティング \(P.7-1 \)](#)

CTL ファイルの更新

次のシナリオが発生した場合に 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
- 追加のセキュリティ トークンを追加または削除する必要がある場合
- 代替 TFTP サーバを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

変更内容を有効にするには、Cisco CallManager および Cisco TFTP サービスを実行す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ります。また、サービスの再起動後にクラスタ内のすべてのデバイスをリセットする必要もあります。この作業を実行する方法の詳細については、[P.1-13](#) の「[デバイスのリセット、サービスの再起動、またはサーバおよびクラスタのリポート](#)」を参照してください。



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 (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。

- 代替 TFTP エントリを更新するには、[P.3-27](#) の「[CTL ファイル エントリの削除](#)」の説明に従ってエントリを削除してから、[P.3-14](#) の「[CiscoCTL クライアントの設定](#)」の説明に従ってエントリを追加する。
- 新しいセキュリティ トークンを追加するには、[P.3-14](#) の「[CiscoCTL 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.3-27](#) の「[CTL ファイル エントリの削除](#)」を参照する。



ヒント

セキュリティ トークンのパスワード変更を求めるプロンプトが表示される場合は、[P.7-1](#) の「[トラブルシューティング](#)」を参照してください。

関連項目

- [Cisco CTL クライアント設定 \(P.3-24\)](#)
- [システム要件 \(P.1-5\)](#)
- [対話および制限 \(P.1-6\)](#)
- [Cisco CTL Provider サービスのアクティブ化 \(P.3-5\)](#)
- [Smart Card サービスの Started および Automatic への設定 \(P.7-13\)](#)
- [Cisco CTL Provider サービスのアクティブ化 \(P.3-5\)](#)
- [CiscoCTL クライアントの設定 \(P.3-14\)](#)
- [CTL ファイルの更新 \(P.3-20\)](#)
- [デバイスセキュリティ モードの設定 \(P.5-4\)](#)
- [トラブルシューティング \(P.7-1\)](#)

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.3-20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 モードを混合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。

関連項目

- [CTL ファイルの更新 \(P.3-20\)](#)
- [Cisco CTL クライアント設定 \(P.3-24\)](#)
- [トラブルシューティング \(P.7-1\)](#)

Cisco CTL クライアント設定

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

表 3-2 を使用して、初めての Cisco CTL クライアント設定、CTL ファイルの更新、または混合モードから 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



設定	説明
CallManager サーバ	
Hostname or IP Address	Cisco CallManager または Cisco TFTP サービスを実行しているクラスタ内のサーバについて、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	Cisco CallManager サーバで管理者特権を持つユーザ名およびパスワードを入力します。
	 ヒント Cisco CallManager の Administrator または Power User アカウントのユーザ名とパスワードを入力したことを確認します。クラスタ内のすべてのサーバで、同一のユーザ名とパスワードが必要です。
オプション ボタン	
Set CallManager Cluster to Mixed Mode	混合モードでは、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な SCCP ポートが使用されることを Cisco CallManager が保証します。
	 (注) クラスタを混合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。

表 3-2 CTL クライアントの設定 (続き)






設定	説明
Set CallManager Cluster to Non-Secure Mode	<p>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。</p> <p>このモードを選択すると、CTL クライアントは CTL ファイルにあるすべてのエントリの証明書を削除しますが、CTL ファイルは引き続き指定したディレクトリに存在します。電話機は署名なし設定ファイルを要求し、ノンセキュアとして CiscoCallManager に登録されます。</p> <p> 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。電話機および Cisco CallManager サーバからの CTL ファイル削除については、P.7-1 の「トラブルシューティング」を参照してください。</p> <p> ヒント このモードでは自動登録を使用できます。</p>
Update CTL File	<p>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。</p>
代替 TFTP サーバ	<p>Hostname or IP Address</p> <p> (注) 代替 TFTP サーバでは、別のクラスタにある Cisco TFTP サーバを指定します。代替 TFTP サーバ設定で 2 つの異なるクラスタを使用する場合は、両方のクラスタで同じクラスタ全体のセキュリティ モードを使用する必要があります。つまり、両方のクラスタに Cisco CTL クライアントをインストールして設定する必要があります。同様に、どちらのクラスタでも同じバージョンの Cisco CallManager を実行する必要があります。</p> <p> 注意 TFTP サービス パラメータ FileLocation 内のパスが、クラスタ内のすべてのサーバで同一であることを確認してください。</p> <p>TFTP サーバのホスト名または IP アドレスを入力します。</p>

表 3-2 CTL クライアントの設定 (続き)

設定	説明
Port	ポート番号を入力します。これは、指定した TFTP 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	サーバでローカルの管理者特権を持つユーザ名およびパスワードを入力します。
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、証明書の秘密キーを取得して CTL ファイルが署名済みであることを確認します。
	
ヒント	このパスワードを変更するには、 P.7-10 の「 セキュリティ トークンパスワード (Etoken) の変更 」を参照してください。

関連項目

- [システム要件 \(P.1-5\)](#)
- [対話および制限 \(P.1-6\)](#)
- [Cisco CTL Provider サービスのアクティブ化 \(P.3-5\)](#)
- [Cisco CTL Provider サービスのアクティブ化 \(P.3-5\)](#)
- [Cisco CTL クライアントのインストール \(P.3-10\)](#)
- [CiscoCTL クライアントの設定 \(P.3-14\)](#)
- [CTL ファイルの更新 \(P.3-20\)](#)
- [デバイス セキュリティ モードの設定 \(P.5-4\)](#)
- [トラブルシューティング \(P.7-1\)](#)

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 を実行するサーバは、CTL ファイルから削除することができません。CTL ファイルに手動で追加した代替 TFTP サーバおよびセキュリティ トークンは削除できますが、クライアントによって自動検出された TFTP サーバは削除できません。

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。



ヒント

Cisco CTL クライアントのアンインストール、電話機からの CTL ファイル削除、またはサーバからの CTL ファイル削除については、[P.7-10](#) の「[Cisco CTL クライアントのトラブルシューティング](#)」を参照してください。

関連項目

- [システム要件 \(P.1-5\)](#)
- [対話および制限 \(P.1-6\)](#)
- [Cisco CTL Provider サービスのアクティブ化 \(P.3-5\)](#)
- [Cisco CTL クライアントのインストール \(P.3-10\)](#)
- [CiscoCTL クライアントの設定 \(P.3-14\)](#)
- [CTL ファイルの更新 \(P.3-20\)](#)
- [デバイス セキュリティ モードの設定 \(P.5-4\)](#)
- [トラブルシューティング \(P.7-1\)](#)

■ CTL ファイル エントリの削除



Certificate Authority Proxy Function の使用方法

この章は、次の内容で構成されています。

- [Certificate Authority Proxy Function の概要 \(P.4-2\)](#)
- [Cisco IP Phone と CAPF の対話 \(P.4-3\)](#)
- [CAPF システムの対話および要件 \(P.4-4\)](#)
- [既存の CAPF データの移行 \(P.4-6\)](#)
- [Cisco CallManager Serviceability での CAPF の設定 \(P.4-6\)](#)
- [CAPF の設定用チェックリスト \(P.4-8\)](#)
- [4.0 サブスクリバ サーバから 4.0 パブリッシャ データベース サーバへの CAPF 1.0\(1\) データのコピー \(P.4-10\)](#)
- [Certificate Authority Proxy Function サービスのアクティブ化 \(P.4-12\)](#)
- [CAPF サービス パラメータの更新 \(P.4-13\)](#)
- [CAPF エンタープライズパラメータの更新 \(P.4-16\)](#)
- [CAPF サービス パラメータ \(P.4-14\)](#)
- [ローカルで有効な証明書のインストールおよびアップグレード \(P.4-17\)](#)
- [ローカルで有効な証明書の削除 \(P.4-18\)](#)
- [Phone Configuration ウィンドウの CAPF 設定 \(P.4-20\)](#)
- [Bulk Administration Tool による CAPF の使用方法 \(P.4-23\)](#)
- [CAPF レポートの生成 \(P.4-24\)](#)
- [LSC Status の選択による電話機の検索 \(P.4-25\)](#)

- [電話機での認証文字列の入力 \(P.4-25\)](#)

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。

- 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。
- SCEP を使用して、サポートされる Cisco IP Phone モデルに代わって、サードパーティの認証局による証明書を要求する。
- 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。
- 電話機にあるローカルで有効な証明書を削除する。
- 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 に固有なキー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、各サーバの C:\Program Files\Cisco\Certificates を参照して次のファイルを検索します。

- 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

関連項目

- [CAPF システムの対話および要件 \(P.4-4\)](#)
- [CAPF の設定用チェックリスト \(P.4-8\)](#)

Cisco IP Phone と CAPF の対話

電話機が CAPF と対話するときに、電話機はその公開キーと秘密キーのペアを生成し、署名付きメッセージで公開キーを CAPF サーバへ転送します。秘密キー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。Cisco CallManager Administration での設定に応じて、CAPF は電話機の証明書に署名するか、またはサードパーティのシスコ認定 CA サーバに対する SCEP プロトコル プロキシとして動作し、電話機の証明書に署名する場合があります。その後で CAPF は署名付きメッセージで証明書を電話機に戻します。

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、電話機がリポート後に TFTP サーバから新しい設定ファイルをロードできない場合に当たります。証明書の操作が完了すると、フラッシュ内の値はシステムによってクリアされます。



ヒント

電話機ユーザが電話機で証明書操作を中断したり、操作ステータスを確認できないことに注意してください。

関連項目

- [CAPF システムの対話および要件 \(P.4-4\)](#)
- [CAPF の設定用チェックリスト \(P.4-8\)](#)
- *Cisco IP Phone Administration Guide for Cisco CallManager*

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。

- Cisco CallManager 4.1 にアップグレードする前に、次の項を確認します。
 - 既存の CAPF データの移行 (P.4-6)
 - 4.0 サブスクリバサーバから 4.0 パブリッシャ データベース サーバへの CAPF 1.0(1) データのコピー (P.4-10)
- 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、パブリッシャ データベース サーバで 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。
- 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 4.1 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、パブリッシャ データベース サーバが実行中で正しく機能していることを確認します。
- 証明書操作の間、電話機が正しく機能していることを確認します。
- Microsoft Certificate Services ソフトウェアが Windows 2003 サーバで実行されている場合は、Microsoft Certificate Services を CAPF で使用することもできます。このソフトウェアの使用法、またはトラブルシューティングのサポートについては、認証局のベンダーに直接連絡してください。

CAPF が Microsoft Certificate Services による証明書を要求する場合は、IP アドレスまたはホスト名など、この認証局の必要な設定情報を該当する CAPF サービス パラメータに入力する必要があります。

Microsoft Certificate Services を使用する場合は、Microsoft Certificate Services をインストールしたサーバに SCEP アドオンをインストールする必要があります。SCEP アドオンを入手するには、認証局のベンダーに直接連絡してください。



ヒント

サードパーティの Certificate Authority (CA; 認証局) を CAPF で使用する前に、認証局のベンダーによる資料を参照して、証明書の発行に影響を及ぼす可能性のある制限事項がないことを確認してください。

- Keon Utility を使用して CAPF の証明書を生成することもできます。IP アドレスまたはホスト名など、この認証局の必要な設定情報を該当する CAPF サービス パラメータに入力する必要があります。また、該当するサービス パラメータ フィールドに Keon Jurisdiction ID を入力する必要があります。
Keon ソフトウェアの使用方法、またはトラブルシューティングのサポートについては、認証局のベンダーに直接連絡してください。
- Keon Utility または Microsoft Certificate Services を CAPF で使用するには、次の Object ID を定義する必要があります。次の設定の使用方法については、認証局のベンダーによる資料を参照してください。
 - (1.3.6.1.5.5.7.3.1) Server SSL/TLS authentication
 - (1.3.5.1.5.5.7.3.2) Client SSL/TLS authentication
 - (1.3.6.1.5.5.7.3.5) IPSec end system authentication



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。

関連項目

- [Certificate Authority Proxy Function の概要 \(P.4-2 \)](#)
- [CAPF システムの対話および要件 \(P.4-4 \)](#)
- [既存の CAPF データの移行 \(P.4-6 \)](#)
- [CAPF の設定用チェックリスト \(P.4-8 \)](#)

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。

関連項目

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

既存の CAPF データの移行



注意

ここで説明する作業の実行に失敗すると、CAPF データが失われる可能性があります。

ローカルで有効な証明書をインストールまたは上書きする前に、次の詳細を確認してください。

- Cisco CallManager 4.0 パブリッシャ データベース サーバに CAPF がインストールされていた Cisco CallManager 4.0 からのアップグレード：Cisco CallManager 4.0 で証明書の操作を実行し、CAPF 1.0(1) をパブリッシャ データベース サーバ上で実行していた場合は、最新の操作ステータスが Cisco CallManager 4.1 データベースに移行されます。
- Cisco CallManager 4.0 サブスクリバ サーバに CAPF がインストールされていた Cisco CallManager からのアップグレード：Cisco CallManager 4.0 で証明書の操作を実行し、CAPF 1.0(1) をサブスクリバ サーバ上で実行していた場合は、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 4.1 にアップグレードする必要があります。

**注意**

Cisco CallManager 4.1 へアップグレードする前にデータをコピーできなかった場合、Cisco CallManager 4.0 サブスクリバ サーバ上の CAPF データは Cisco CallManager 4.1 データベースに移行されず、データは失われる可能性があります。データが失われた場合、CAPF utility 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。CAPF 4.1(2) は証明書を再発行しますが、証明書は有効ではありません。

- Cisco CallManager 4.1(x) のいずれかのリリースから、以降のリリースの Cisco CallManager 4.1(x) へのアップグレード: アップグレードによって CAPF データは自動的に移行されます。

関連項目

- [Certificate Authority Proxy Function の概要 \(P.4-2 \)](#)
- [CAPF システムの対話および要件 \(P.4-4 \)](#)
- [CAPF の設定用チェックリスト \(P.4-8 \)](#)
- [4.0 サブスクリバ サーバから 4.0 パブリッシャ データベース サーバへの CAPF 1.0\(1\) データのコピー \(P.4-10 \)](#)

CAPF の設定用チェックリスト

表 4-1 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、削除、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 4-1 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	<p>ローカルで有効な証明書が電話機に存在するかどうかを判別します。</p> <p>CAP 1.0(1) データを Cisco CallManager 4.1(2) 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。</p>	<ul style="list-style-type: none"> • Manufactured-Installed Certificate (MIC) が IP Phone 内に存在することの確認 (P.7-42) • 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 (P.7-42) • 既存の CAPF データの移行 (P.4-6) • 4.0 サブスクライバ サーバから 4.0 パブリッシャ データベース サーバへの CAPF 1.0(1) データのコピー (P.4-10)
ステップ 2	<p>Cisco CallManager 4.0 で CAPF utility を使用して、CAPF データが Cisco CallManager 4.1 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 utility を削除します。</p>	<p>Settings > Control Panel を選択します。Add/Remove Programs をダブルクリックして、ユーティリティを探します。ユーティリティを削除します。</p>
ステップ 3	<p>Cisco Certificate Authority Proxy Function サービスが実行されていることを確認します。</p> <p> 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。</p>	<p>Certificate Authority Proxy Function サービスのアクティブ化 (P.4-12)</p>

表 4-1 CAPF 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 4	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。	CiscoCTL クライアントの設定 (P.3-14)
ステップ 5	必要に応じて、CAPF サービスパラメータを更新します。	<ul style="list-style-type: none"> • CAPF サービスパラメータの更新 (P.4-13) • CAPF サービスパラメータ (P.4-14)
ステップ 6	電話機のローカルで有効な証明書をインストール、アップグレード、削除、またはトラブルシューティングするには、Cisco CallManager Administration または BAT を使用します。	<ul style="list-style-type: none"> • ローカルで有効な証明書のインストールおよびアップグレード (P.4-17) • Phone Configuration ウィンドウの CAPF 設定 (P.4-20) • Bulk Administration Tool による CAPF の使用方法 (P.4-23)
ステップ 7	CAPF を使用するデバイスのリストを表示するには、Cisco CallManager Administration で CAPF レポートを生成します。	CAPF レポートの生成 (P.4-24)
ステップ 8	証明書の操作に必要な場合は、電話機に認証文字列を入力します。	電話機での認証文字列の入力 (P.4-25)
ステップ 9	証明書の操作が予定したとおりに正常終了したことを確認します。	<ul style="list-style-type: none"> • 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 (P.7-42) • Manufactured-Installed Certificate (MIC) が IP Phone 内に存在することの確認 (P.7-42)

4.0 サブスクリイバサーバから 4.0 パブリッシャ データベース サーバへの CAPF 1.0(1) データのコピー



注意

CAPF utility 1.0(1) を Cisco CallManager 4.0 サブスクリイバサーバにインストールした場合、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、Cisco CallManager 4.1 にアップグレードする必要があります。この作業を実行しないと、CAPF データが失われることがあります。たとえば、C:\Program Files\Cisco\CAPF\CAPF.phone にある電話機レコード ファイルが失われる可能性があります。データが失われると、CAPF utility 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。CAPF 4.1(2) は証明書を再発行しますが、証明書は有効ではありません。

次に示す手順は、[P.4-6 の「既存の CAPF データの移行」](#)と併せて使用してください。ファイルをコピーするには、次の手順を実行します。

手順

- ステップ 1** CAPF 1.0 がインストールされているマシンから Cisco CallManager 4.0 がインストールされているパブリッシャ データベース サーバに、[表 4-2](#) のファイルをコピーします。

表 4-2 サーバからサーバへのコピー

コピー対象ファイル	CAPF 1.0 がインストールされている コピー元マシン内の場所	Cisco CallManager 4.0 がインストールされている コピー先パブリッシャ データベース サーバ内の場所
*.0	C:\Program Files\Cisco\CAPF	C:\Program Files\Cisco\Certificates
CAPF.phone	C:\Program Files\Cisco\CAPF	C:\Program Files\Cisco\CAPF
CAPE.cfg ファイル	C:\Program Files\Cisco\CAPF	C:\Program Files\Cisco\CAPF

- ステップ 2** クラスタ内のすべてのサーバを Cisco CallManager 4.1 にアップグレードします。

- ステップ 3 クラスタを Cisco CallManager 4.1 にアップグレードしたら、Cisco CTL クライアントをアップグレードし、電話機を使用する前にクライアントを実行します。Cisco CTL クライアントによって、CAPF 証明書がクラスタ内のすべてのサーバにコピーされます。
- ステップ 4 Cisco CallManager 4.0 で使用していた CAPF utility を削除します。表 4-1 を参照してください。
-

関連項目

- [Certificate Authority Proxy Function の概要 \(P.4-2\)](#)
- [CAPF システムの対話および要件 \(P.4-4\)](#)
- [既存の CAPF データの移行 \(P.4-6\)](#)
- [CAPF の設定用チェックリスト \(P.4-8\)](#)

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

Cisco CallManager 4.1 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、パブリッシャ データベース サーバ上だけで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.3-20 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 ウィンドウの左側のペインで、パブリッシャ データベース サーバを選択します。
 - ステップ 3 **Certificate Authority Proxy Function** サービスのチェックボックスをオンにします。
 - ステップ 4 **Update** をクリックします。
-

関連項目

- [CAPF の設定用チェックリスト \(P.4-8\)](#)
- *Cisco CallManager Serviceability アドミニストレーション ガイド*
- *Cisco CallManager Serviceability Service Guide*

CAPF サービス パラメータの更新

証明書の生成に Microsoft Certificate Services または Keon Utility を使用している場合、Cisco CallManager Administration で一部の CAPF サービス パラメータを更新する必要があります。

CAPF Service Parameter ウィンドウには、証明書の有効年数、システムによるキー生成の最大再試行回数、キー サイズなどの情報も表示されます。

Cisco CallManager Administration で CAPF サービス パラメータを表示する前に、[P.4-12 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 **Service > Service Parameter** 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、パブリッシャ データベース 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、Cisco Certificate Authority Proxy Function サービスを選択します。
- ステップ 4 [表 4-3](#) の説明に従って、CAPF サービス パラメータを更新します。
- 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。

関連項目

- [Certificate Authority Proxy Function の概要 \(P.4-2\)](#)
- [CAPF システムの対話および要件 \(P.4-4\)](#)

- CAPF の設定用チェックリスト (P.4-8)
- Certificate Authority Proxy Function サービスのアクティブ化 (P.4-12)
- CAPF サービス パラメータ (P.4-14)

CAPF サービス パラメータ

表 4-3 は、P.4-13 の「CAPF サービス パラメータの更新」と併せて使用してください。

表 4-3 CAPF サービス パラメータ


パラメータ	説明
Certificate Issuer	<p>ドロップダウン リスト ボックスから、ローカルで有効な証明書を発行するエントリを選択します。</p> <p></p> <p>ヒント このフィールドを更新した場合は、Cisco CTL 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。</p>
Duration of Certificate Validity (years)	<p>このフィールドには、ローカルで有効な証明書の有効年数を指定します。</p> <p>Keon や Microsoft Certificate Services など、サードパーティの証明書発行者の場合、このフィールドには別の値が作成されている場合もあります。こうした発行者が作成する値は、このフィールドに表示されません。証明書の有効年数の詳細については、証明書の発行者にお問い合わせください。</p>
Key Size (bits)	<p>このフィールドには、CAPF 公開キーおよび秘密キーの生成に CAPF が使用するキー サイズを指定します。</p>

表 4-3 CAPF サービス パラメータ (続き)

パラメータ	説明
Maximum Allowable Time for Key Generation (minutes)	このフィールドには、CAPF が CAPF キーの生成を試みる時間を秒数で指定します。また、このパラメータでは電話機でキー生成プロセスが完了するのを CAPF が待つ最大分数も指定します。
Maximum Allowable Attempts for Key Generation	このフィールドには、CAPF が CAPF キーを生成しようとする最大試行回数を指定します。また、このパラメータでは電話機で対応するキーを生成できる最大試行回数も指定します。
Keon Jurisdiction ID	このフィールドには、Keon Utility で使用する Jurisdiction ID を指定します。
SCEP Port Number	このフィールドには、CAPF サーバの SCEP ポート番号を指定します。
Certificate Authority Address	Microsoft Certificate Services または Keon Utility をインストールしたサーバの IP アドレスを入力します。 Certificate Generation Method ドロップダウン リストボックスから Cisco Certificate Authority Proxy Server を選択した場合、CAPF サーバの IP アドレスを入力する必要はありません。

関連項目

- [Certificate Authority Proxy Function の概要 \(P.4-2\)](#)
- [CAPF システムの対話および要件 \(P.4-4\)](#)
- [CAPF の設定用チェックリスト \(P.4-8\)](#)
- [Certificate Authority Proxy Function サービスのアクティブ化 \(P.4-12\)](#)
- [CAPF サービス パラメータの更新 \(P.4-13\)](#)

CAPF エンタープライズ パラメータの更新

表 4-4 に示すエンタープライズ パラメータは CAPF をサポートしています。Cisco CallManager Administration の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。



ヒント

変更内容を有効にするには、パラメータの更新後に電話機をリセットする必要があります。

表 4-4 CAPF エンタープライズ パラメータ

パラメータ	説明
CAPF Phone Port	このパラメータには、電話機から証明書を要求するために Cisco Authority Proxy Function サービスが使用するポートを指定します。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。
CAPF Operation Expires in (days)	このパラメータは、CAPF を使用するすべての電話機に影響します。ここには、証明書のトラブルシューティング、インストール、アップグレード、削除など、任意の CAPF 操作を完了する必要がある日数を指定します。

関連項目

- [Certificate Authority Proxy Function の概要 \(P.4-2\)](#)
- [CAPF システムの対話および要件 \(P.4-4\)](#)
- [CAPF の設定用チェックリスト \(P.4-8\)](#)
- [Certificate Authority Proxy Function サービスのアクティブ化 \(P.4-12\)](#)
- [CAPF サービス パラメータの更新 \(P.4-13\)](#)

ローカルで有効な証明書のインストールおよびアップグレード

CAPF を使用するとき、[表 4-5](#) 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 Administration で **Device > Phone** の順に選択します。
 - ステップ 2 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検索します。電話機の検索については、『*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 3 [表 4-5](#) の説明に従って、設定内容を入力します。
 - ステップ 4 **Update** をクリックします。
 - ステップ 5 **Reset Phone** をクリックします。
 - ステップ 6 Install/Upgrade Certificate Operation オプションと By Authentication String モード オプションを選択した場合は、電話機に認証文字列を入力する必要があります。この作業を実行する方法については、[P.4-25](#) の「**電話機での認証文字列の入力**」を参照してください。
-

関連項目

- [Certificate Authority Proxy Function の概要 \(P.4-2\)](#)
- [CAPF システムの対話および要件 \(P.4-4\)](#)
- [CAPF の設定用チェックリスト \(P.4-8\)](#)
- [Phone Configuration ウィンドウの CAPF 設定 \(P.4-20\)](#)
- [Bulk Administration Tool による CAPF の使用方法 \(P.4-23\)](#)
- [電話機での認証文字列の入力 \(P.4-25\)](#)

ローカルで有効な証明書の削除

CAPF では、シスコの製造過程で電話機にインストールされた証明書は削除しません。CAPF で削除するのは、CAPF またはシスコ認定のサードパーティ認証局が発行した証明書だけです。



注意

電話機に Manufacture Installed Certificate (MIC; 製造元でインストールされる証明書) が含まれない場合は、Locally Significant Certificate (LSC; ローカルで有効な証明書) を削除する前に、電話機のデバイス セキュリティ モードをノンセキュアに変更する必要があります。デバイス セキュリティ モードを変更する前に証明書を削除すると、電話機を Cisco CallManager に登録できません。デバイス セキュリティ モードの変更については、P.5-1 の「電話機のセキュリティ設定」を参照してください。

電話機ではなく Cisco CallManager Administration から証明書を削除するには、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 ローカルで有効な証明書を削除する電話機を検索します。CAPF を使用する電話機の検索方法については、『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。
- ステップ 3 Certificate Operation ドロップダウン リスト ボックスから、**Delete** オプションを選択します。
- ステップ 4 **Update** をクリックします。
- ステップ 5 **Reset Phone** をクリックします。

ステップ 6 By Authentication String モードを選択した場合は、証明書を取り消す文字列を入力する必要があります。

ステップ 7 証明書の発行にシスコ認定のサードパーティ認証局を使用していた場合、その認証局が証明書を取り消したことを確認します。この作業を実行する方法については、サードパーティの認証局ベンダーにお問い合わせください。

証明書が認証局によって電話機から削除されると、Phone Configuration ウィンドウの Operation Status フィールドに Delete Success と表示されます。

関連項目

- [Certificate Authority Proxy Function の概要 \(P.4-2\)](#)
- [CAPF システムの対話および要件 \(P.4-4\)](#)
- [既存の CAPF データの移行 \(P.4-6\)](#)
- [Certificate Authority Proxy Function サービスのアクティブ化 \(P.4-12\)](#)
- [CAPF サービス パラメータの更新 \(P.4-13\)](#)
- [CAPF サービス パラメータ \(P.4-14\)](#)
- [ローカルで有効な証明書のインストールおよびアップグレード \(P.4-17\)](#)
- [Phone Configuration ウィンドウの CAPF 設定 \(P.4-20\)](#)
- [Bulk Administration Tool による CAPF の使用方法 \(P.4-23\)](#)
- [電話機での認証文字列の入力 \(P.4-25\)](#)
- [ローカルで有効な証明書の削除 \(P.4-18\)](#)

Phone Configuration ウィンドウの CAPF 設定

表 4-5 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。

表 4-5 CAPF 設定

設定	説明
Certificate Operation	<p>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。</p> <ul style="list-style-type: none"> • No Pending Operation : 証明書の操作が行われてい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。 <p>Troubleshoot オプションを選択すると、LSC または MIC が電話機に存在することを確認できます。</p>
Authentication Mode	<p>このフィールドによって、電話機で CAPF を認証する方法を選択することができます。ローカルで有効な証明書をインストール、アップグレード、削除、またはトラブルシューティングする場合、あるいは製造元でインストールされる証明書によって認証する場合に、このフィールドを使用します。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。</p> <ul style="list-style-type: none"> • 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、自動的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、削除、またはトラブルシューティングします。 <p>このオプションではセキュリティを一切提供しません。したがって、このオプションは安全な閉じた環境の場合にだけ選択することを強く推奨します。</p>

表 4-5 CAPF 設定 (続き)

設定	説明
	<ul style="list-style-type: none"> 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、自動的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、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、あるいはほか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、自動的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、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。
Authentication String	<p>By Authentication String オプションを選択した場合に、このフィールドは適用されます。文字列を手動で入力するか、あるいは 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。</p> <p>ローカルで有効な証明書をインストール、アップグレード、削除、またはトラブルシューティングするには、電話機ユーザまたは管理者が電話機に認証文字列を入力する必要があります。</p>
Generate String	<p>CAPF で自動的に認証文字列を生成する場合は、このボタンをクリックします。4 ~ 10 桁の認証文字列が Authentication String フィールドに表示されます。</p>

表 4-5 CAPF 設定 (続き)

設定	説明
Key Size (bits)	<p>ドロップダウン リスト ボックスから、証明書のキー サイズを選択します。デフォルト設定値は 1024 です。これ以外のオプションには、512 と 2048 があります。</p> <p>デフォルト設定値よりも大きなキー サイズを選択すると、電話機でキー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。</p>
Operation Completes by	<p>このフィールドは Certificate Operation の Install/Upgrade、Delete、および Troubleshoot オプションをサポートしており、操作の完了が必要な期限として日付と時刻を指定します。</p> <p>表示される値は、パブリッシュ データベース サーバに適用されます。</p>
Operation Status	<p>このフィールドは証明書操作の進行状況を表示します。たとえば、<operation type> pending、failed、successful など、operating type には Certificate Operation オプションの Install/Upgrade、Delete、または Troubleshoot が表示されます。このフィールドに表示される情報は変更できません。</p>

関連項目

- [Certificate Authority Proxy Function の概要 \(P.4-2 \)](#)
- [CAPF システムの対話および要件 \(P.4-4 \)](#)
- [CAPF の設定用チェックリスト \(P.4-8 \)](#)
- [ローカルで有効な証明書のインストールおよびアップグレード \(P.4-17 \)](#)
- [Bulk Administration Tool による CAPF の使用方法 \(P.4-23 \)](#)
- [電話機での認証文字列の入力 \(P.4-25 \)](#)
- [ローカルで有効な証明書の削除 \(P.4-18 \)](#)

Bulk Administration Tool による CAPF の使用方法

多数のローカルで有効な証明書を同時にインストール、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場合には、クラスタで実行されているバージョンの Cisco CallManager と互換性のある Cisco Bulk Administration Tool を使用する必要があります。

BAT を使用して証明書をインストールまたは削除する前に、Cisco Certificate Authority Proxy Function サービスをアクティブにする必要があります。

証明書のインストールは、スケジューリングされたメンテナンス画面で行うことを強く推奨します。これは、証明書の生成によってコール処理が中断される可能性があるためです。

関連項目

- [CAPF の設定用チェックリスト \(P.4-8\)](#)
- [Certificate Authority Proxy Function サービスのアクティブ化 \(P.4-12\)](#)
- *Bulk Administration Tool ユーザガイド*

CAPF レポートの生成

Cisco CallManager Administration では、CAPF レポートを生成して証明書の操作ステータス、認証文字列、またはリストされたデバイスの認証モードを確認することができます。CAPF レポートを生成したら、レポートを CSV ファイルで表示することができます。

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 > Device Settings > CAPF Report** の順に選択します。
 - ステップ 2 レポートに表示するデバイスを検索するには、Find/List ドロップダウン リストボックスから検索対象を選択します。
 - ステップ 3 **Find** をクリックします。

デバイス リストが表示されます。
 - ステップ 4 CAPF レポートを CSV ファイルで表示するには、ウィンドウの右上隅にある **View the Report in File** リンクをクリックします。
 - ステップ 5 必要に応じて、CSV ファイルを安全な場所に保存して修正することもできます。
-

関連項目

- [Certificate Authority Proxy Function の概要 \(P.4-2\)](#)
- [CAPF システムの対話および要件 \(P.4-4\)](#)
- [CAPF の設定用チェックリスト \(P.4-8\)](#)
- [Phone Configuration ウィンドウの CAPF 設定 \(P.4-20\)](#)
- [電話機での認証文字列の入力 \(P.4-25\)](#)

LSC Status の選択による電話機の検索

LSC Status を選択して電話機を検索およびリストする方法については、[P.5-10](#) の「[認証、暗号化、LSC ステータスによる電話機の検索](#)」を参照してください。

関連項目

- [CAPF の設定用チェックリスト \(P.4-8\)](#)
- [トラブルシューティング \(P.7-1\)](#)

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

電話機ユーザは次の手順を実行して、証明書をインストールすることができます。認証文字列は 1 回の使用に限り適用されます。

始める前に

- CAPF 証明書が CiscoCTL ファイル内に存在することを確認します。
- CAPF 証明書が Cisco CallManager サーバの証明書フォルダに存在することを確認します。それには、サーバで C:\Program Files\Cisco\Certificates を参照します。
- [P.4-12](#) の「[Certificate Authority Proxy Function サービスのアクティブ化](#)」で説明されているように、Cisco Certificate Authority Proxy Function サービスをアクティブにしたことを確認します。
- パブリッシャ データベース サーバが実行中で正しく機能していることを確認します。証明書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ことを確認します。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。

- Phone Configuration ウィンドウまたは CAPF Report ウィンドウに表示される認証文字列を入手します。

手順

- ステップ 1 Phone Configuration ウィンドウまたは CAPF Report ウィンドウから、デバイスの CAPF 認証文字列を入手します。
- ステップ 2 デバイスが Cisco CallManager に登録されていることを確認します。
- ステップ 3 デバイス セキュリティ モードが Nonsecure であることを確認します。
- ステップ 4 ノンセキュアの Cisco IP Phone model 7970、7960、または 7940 で **Settings** ボタンを押します。
- ステップ 5 Settings メニューで **Security Configuration** オプションまでスクロールし、**Select** ソフトキーを押します。



ヒント

電話メニューがロックされている場合は、**# を押すとメニューをロック解除できます。

- ステップ 6 LSC オプションまでスクロールして、**Update** ソフトキーを押します。
- ステップ 7 電話機の 4 ~ 10 桁の認証文字列を入力して、**Submit** を押します。



ヒント

Submit を押す前に認証文字列を変更する必要がある場合は、<< を押します。

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

電話機に表示されるメッセージを確認することで、証明書操作の進行状況を監視します。Submit を押すと、Pending というメッセージが LSC オプションの下に表示されます。電話機は公開キーと秘密キーのペアを生成し、電話機に関する情報を表示します。電話機がプロセスを正常に完了すると、成功を示すメッセージが表示されます。失敗を示すメッセージが電話機に表示された場合は、間違った認証文字列を入力したか、電話機でアップグレードを有効にしていませんでした。P.7-1 の「[トラブルシューティング](#)」を参照してください。

Stop オプションを選択すれば、いつでもプロセスを停止することができます。

電話機に証明書がインストールされたことを確認するには、**Settings > Model Information** を選択し、LSC 設定を表示します。この設定に、Installed または Not Installed と示されます。

関連項目

- [CAPF の設定用チェックリスト \(P.4-8\)](#)
- [Phone Configuration ウィンドウの CAPF 設定 \(P.4-20\)](#)
- [Bulk Administration Tool による CAPF の使用方法 \(P.4-23\)](#)
- [電話機での認証文字列の入力 \(P.4-25\)](#)
- [ローカルで有効な証明書の削除 \(P.4-18\)](#)
- *Cisco IP Phone 7960G/7940G アドミニストレーション ガイド for Cisco CallManager*



電話機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。

- [電話機のセキュリティ設定の概要 \(P.5-2\)](#)
- [電話機における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 \(P.5-3\)](#)
- [デバイス セキュリティ モードの設定 \(P.5-4\)](#)
- [サポートされる電話機モデルに対するセキュリティ デバイス システム デフォルトの設定 \(P.5-5\)](#)
- [単一デバイスに対するデバイス セキュリティ モードの設定 \(P.5-6\)](#)
- [Cisco Bulk Administration Tool を使用したデバイス セキュリティ モードの設定 \(P.5-8\)](#)
- [Device Security Mode 設定 \(P.5-9\)](#)
- [認証、暗号化、LSC ステータスによる電話機の検索 \(P.5-10\)](#)
- [電話機のセキュリティ強化 \(P.5-11\)](#)
- [Gratuitous ARP 設定の無効化 \(P.5-11\)](#)
- [Web Access 設定の無効化 \(P.5-11\)](#)
- [PC Voice VLAN Access 設定の無効化 \(P.5-12\)](#)
- [Setting Access 設定の無効化 \(P.5-12\)](#)
- [PC Port 設定の無効化 \(P.5-13\)](#)
- [電話機のセキュリティ強化作業の実行 \(P.5-14\)](#)

電話機のセキュリティ設定の概要

ここでは、サポートされる電話機にセキュリティを設定するために実行する次の作業概要について説明します。

- サポートされる電話機で Locally Significant Certificate (LSC; 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し、証明書を削除またはトラブルシューティングする。
- サポートされる電話機に、Device Security Mode を使用して認証または暗号化を設定する。
- 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する。

関連項目

- [電話機における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 \(P.5-3\)](#)
- [デバイスセキュリティモードの設定 \(P.5-4\)](#)
- [Device Security Mode 設定 \(P.5-9\)](#)
- [認証、暗号化、LSC ステータスによる電話機の検索 \(P.5-10\)](#)
- [電話機のセキュリティ強化 \(P.5-11\)](#)
- [電話機のセキュリティ強化作業の実行 \(P.5-14\)](#)

電話機における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

ローカルで有効な証明書を電話機でインストール、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には、Cisco CallManager Administration の Phone Configuration ウィンドウで CAPF 設定値を構成する必要があります。CAPF 設定値を構成する方法については、P.4-1 の「Certificate Authority Proxy Function の使用方法」を参照してください。

関連項目

- [CAPF の設定用チェックリスト \(P.4-8\)](#)
- [CAPF システムの対話および要件 \(P.4-4\)](#)
- [デバイス セキュリティ モードの設定 \(P.5-4\)](#)
- [認証、暗号化、LSC ステータスによる電話機の検索 \(P.5-10\)](#)
- [電話機のセキュリティ強化 \(P.5-11\)](#)
- [電話機のセキュリティ強化作業の実行 \(P.5-14\)](#)
- [トラブルシューティング \(P.7-1\)](#)

デバイス セキュリティ モードの設定

デバイスに認証または暗号化を設定するには、次の作業のいずれか 1 つを実行します。

- サポートされる電話機モデルに、デフォルトのデバイス セキュリティ モードを設定する。
- Cisco CallManager Administration の Phone Configuration ウィンドウで、単一デバイスにデバイス セキュリティ モードを設定する。
- Cisco Bulk Administration Tool を使用して、サポートされる電話機モデルにデバイス セキュリティ モードを設定する。



ヒント

デバイス セキュリティ モードを設定するには、ローカルで有効な証明書または製造元でインストールされる証明書が電話機に必要です。

デバイス セキュリティ モードの設定内容については、[P.5-9 の「Device Security Mode 設定」](#)を参照してください。

関連項目

- [システム要件 \(P.1-5\)](#)
- [対話および制限 \(P.1-6\)](#)
- [Cisco CTL Provider サービスのアクティブ化 \(P.3-5\)](#)
- [CiscoCTL クライアントの設定 \(P.3-14\)](#)
- [CTL ファイルの更新 \(P.3-20\)](#)
- [デバイス セキュリティ モードの設定 \(P.5-4\)](#)
- [Certificate Authority Proxy Function の使用方法 \(P.4-1\)](#)
- [トラブルシューティング \(P.7-1\)](#)

サポートされる電話機モデルに対するセキュリティ デバイス システム デフォルトの設定



(注) この手順では、変更内容を有効にするためにデバイスをリセットして Cisco CallManager サービスを再起動する必要があります。

Cisco CallManager Administration で、すべての電話機タイプのセキュリティ デバイス システム デフォルトは Non-Secure と表示されます。セキュリティ デバイス システム デフォルトを Authenticated または Encrypted 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 CallManager Administration で **System > Enterprise Parameters** の順に選択します。
- ステップ 2 Security Parameters セクションで **Device Security Mode** を探します。
- ステップ 3 ドロップダウン リスト ボックスから、**Authenticated** または **Encrypted** を選択します。詳細については、表 5-1 を参照してください。
- ステップ 4 Enterprise Parameters ウィンドウ最上部の **Update** をクリックします。
- ステップ 5 クラスタ内のすべてのデバイスをリセットします。P.1-13 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ポート**」を参照してください。
- ステップ 6 変更内容を有効にするため、Cisco CallManager サービスを再起動します。

関連項目

- システム要件 (P.1-5)
- 対話および制限 (P.1-6)
- デバイス セキュリティ モードの設定 (P.5-4)
- Certificate Authority Proxy Function の使用方法 (P.4-1)

単一デバイスに対するデバイス セキュリティ モードの設定

単一デバイスにデバイス セキュリティ モードを設定するには、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。

Cisco CallManager Administration の Phone Configuration ウィンドウで Device Security Mode を設定すると、デバイス設定 .xml ファイルが再構成されます。デバイス セキュリティ モードを初めて設定した後、あるいはデバイス セキュリティ モードを変更した場合は、デバイスをリセットする必要があります。リセットすると、電話機は新しい設定ファイルを要求します。

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。

データベースに電話機を追加していない場合、電話機はリストに表示されません。電話機の追加については、『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 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 **Device Security Mode** ドロップダウン リスト ボックスを見つけます。

電話機タイプがセキュリティをサポートしていない場合、このオプションは表示されません。その電話機タイプには認証も暗号化も設定することができません。

ステップ 5 **Device Security Mode** ドロップダウン リスト ボックスから、設定するオプションを選択します。オプションの説明については、表 5-1 を参照してください。

Device Security Mode ドロップダウン リスト ボックスは、電話機が認証または暗号化をサポートしている場合にだけ表示されます。たとえば、電話機が暗号化をサポートしていない場合、暗号化オプションはドロップダウン リスト ボックスに表示されません。

ステップ 6 **Update** をクリックします。

ステップ 7 **Reset Phone** をクリックします。



注意

電話機をリセットすると、システムはゲートウェイを介して行われているすべてのコールを終了します。

関連項目

- [システム要件 \(P.1-5\)](#)
- [対話および制限 \(P.1-6\)](#)
- [デバイス セキュリティ モードの設定 \(P.5-4\)](#)
- [Certificate Authority Proxy Function の使用方法 \(P.4-1\)](#)

Cisco Bulk Administration Tool を使用したデバイス セキュリティ モードの設定

Cisco CallManager 4.1(2) をサポートする Cisco Bulk Administration Tool を使用して、暗号化または認証をサポートする特定の電話機モデルにデバイス セキュリティ モードを設定することができます。この作業の実行方法の詳細については、このバージョンの Cisco CallManager をサポートする『*Bulk Administration Tool ユーザガイド*』を参照してください。

関連項目

- [システム要件 \(P.1-5\)](#)
- [対話および制限 \(P.1-6\)](#)
- [デバイス セキュリティ モードの設定 \(P.5-4\)](#)
- [Certificate Authority Proxy Function の使用方法 \(P.4-1\)](#)
- [Bulk Administration Tool ユーザガイド](#)

Device Security Mode 設定

Device Security Mode には、[表 5-1](#) に示すオプションがあります。

表 5-1 Device Security Mode

オプション	説明
Use System Default	電話機はエンタープライズ パラメータ、Device Security Mode で指定した値を使用する。
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。AES128/SHA を使用する TLS 接続を開始する。

関連項目

- [システム要件 \(P.1-5\)](#)
- [対話および制限 \(P.1-6\)](#)
- [デバイス セキュリティ モードの設定 \(P.5-4\)](#)
- [Certificate Authority Proxy Function の使用方法 \(P.4-1\)](#)
- *Bulk Administration Tool ユーザガイド*

認証、暗号化、LSC ステータスによる電話機の検索

セキュリティ機能に関連付けられている電話機を検索するため、Cisco CallManager Administration の Phone Find/List ウィンドウで次の基準のどちらかを選択できます。

- **Device Security Mode** : このオプションを選択すると、認証または暗号化をサポートする電話機のリストが表示されます。このオプションを選択する場合、デバイスが **Authenticated** か **Encrypted** かを指定することもできます。Find ボタンをクリックすると、電話機モデル、Device Security Mode、Device Name、Description、Directory Number、Owner User ID などが表示されます（設定されている場合）。
- **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。このオプションを選択する場合、CAPF によって現在実行されている Certification Operation を指定することもできます。たとえば、Operation Pending、Success、Upgrade Failed、Delete Failed、Troubleshoot Failed などがあります。Find ボタンをクリックすると、電話機モデル、LSC Status、Device Name、Description、Directory Number、および Owner User ID が表示されます（設定されている場合）。

電話機を検索してリスト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』を参照してください。



ヒント

Cisco CallManager Administration の Phone Find/List ウィンドウでは、デバイスの削除およびリセットも実行できます。

関連項目

- *Cisco CallManager アドミニストレーションガイド*
- [Certificate Authority Proxy Function の使用方法 \(P.4-1\)](#)

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。この項では、次のトピックについて取り上げます。

- [Gratuitous ARP 設定の無効化 \(P.5-11 \)](#)
- [Web Access 設定の無効化 \(P.5-11 \)](#)
- [PC Voice VLAN Access 設定の無効化 \(P.5-12 \)](#)
- [Setting Access 設定の無効化 \(P.5-12 \)](#)
- [PC Port 設定の無効化 \(P.5-13 \)](#)

Gratuitous ARP 設定の無効化

デフォルトで Cisco IP Phone は Gratuitous ARP (GARP) パケットを受け入れます。デバイスによって使用される GARP 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 GARP 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) GARP 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バサビリティ 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 モデルは、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 モデルは、PC ポートで送受信され、802.1Q タグが含まれるボイス VLAN 上のパケットをすべて廃棄する。
- Cisco IP Phone 7912 モデル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。

関連項目

- [対話および制限 \(P.1-6\)](#)
- [電話機のセキュリティ強化作業の実行 \(P.5-14\)](#)
- *Cisco IP Phone Administration Guide for Cisco CallManager*

電話機のセキュリティ強化作業の実行



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。

次の手順を実行してください。

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



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 **i** ボタンをクリックします。

- 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。

ステップ 6 Update をクリックします。

関連項目

- [対話および制限 \(P.1-6 \)](#)
- [Gratuitous ARP 設定の無効化 \(P.5-11 \)](#)
- [Web Access 設定の無効化 \(P.5-11 \)](#)
- [PC Voice VLAN Access 設定の無効化 \(P.5-12 \)](#)
- [Setting Access 設定の無効化 \(P.5-12 \)](#)
- [PC Port 設定の無効化 \(P.5-13 \)](#)



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

この章は、次の内容で構成されています。

- [SRST のセキュリティの概要 \(P.6-2\)](#)
- [SRST のセキュリティ設定用チェックリスト \(P.6-3\)](#)
- [SRST リファレンスのセキュリティ設定 \(P.6-4\)](#)
- [SRST リファレンスのセキュリティ設定 \(P.6-6\)](#)

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、自己署名証明書または認証局が発行した証明書が含まれます。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 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

Cisco CallManager では、SRST 証明書に対して深度 1 のチェーニングだけをサポートします。つまり、電話機の設定ファイルには単一の発行者による証明書しか含まれません。HSRP はサポートされていません。

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、自己署名証明書または認証局が発行した証明書が含まれる。
- Cisco CTL クライアントを介してクラスタを混合モードに設定した。
- 電話機に認証または暗号化を設定した。
- Cisco 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。

関連項目

- [SRST のセキュリティ設定用チェックリスト \(P.6-3\)](#)
- [SRST リファレンスのセキュリティ設定 \(P.6-4\)](#)
- [SRST リファレンスのセキュリティ設定 \(P.6-6\)](#)
- [トラブルシューティング \(P.7-1\)](#)

SRST のセキュリティ設定用チェックリスト

表 6-1 を使用して、SRST のセキュリティ設定手順を進めます。

表 6-1 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 SRST 対応ゲートウェイのシステム アドミニストレーション ガイド
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。	<ul style="list-style-type: none"> 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 (P.7-42) Manufactured-Installed Certificate (MIC) が IP Phone 内に存在することの確認 (P.7-42)
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。	デバイス セキュリティ モードの設定 (P.5-4)
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.6-4)
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.6-4)

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 6-2 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 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 SRST 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 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 証明書が削除されます。

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。

- 初めて SRST リファレンスを追加する。この作業を実行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。
- セキュリティを設定する SRST リファレンスを検索する。SRST リファレンスの検索については、『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。既存の SRST リファレンスにセキュリティを設定して更新するには、表 6-2 を使用してください。

ステップ 3 SRST リファレンスを追加したか、更新したかに応じて、**Insert** または **Update** をクリックします。

ステップ 4 データベース内の SRST 証明書を更新するには、**Update SRST Certificate** ボタンをクリックします。



ヒント

このボタンは、既存の SRST リファレンスを更新する場合にだけ表示されます。

ステップ 5 **Reset Devices** をクリックします。

ステップ 6 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。

関連項目

- [SRST のセキュリティの概要 \(P.6-2\)](#)
- [SRST のセキュリティ設定用チェックリスト \(P.6-3\)](#)
- [SRST リファレンスのセキュリティ設定 \(P.6-6\)](#)
- [トラブルシューティング \(P.7-1\)](#)

SRST リファレンスのセキュリティ設定

表 6-2 を使用して、SRST リファレンスのセキュリティを設定します。

表 6-2 SRST リファレンスのセキュリティ設定




設定	説明
Is SRST Secure?	<p>SRST 対応ゲートウェイに、自己署名証明書または認証局が発行した証明書が含まれることを確認した後、このチェックボックスをオンにします。</p> <p>SRST を設定してゲートウェイおよび従属する電話機をリセットすると、Cisco CTL Provider サービスは SRST 対応ゲートウェイで 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。</p> <p></p> <p>ヒント データベースおよび電話機から SRST 証明書を削除するには、このチェックボックスをオフにして Update をクリックし、従属する電話機をリセットします。</p>
SRST Certificate Provider Port	<p>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。</p> <p>SRST 対応ゲートウェイ上でこのポートを設定した後、このフィールドにポート番号を入力します。</p> <p></p> <p>ヒント ポートが現在使用中の場合や、ファイアウォールを使用してファイアウォール内のポートを使用できない場合には、異なるポート番号の設定が必要になることもあります。</p>

表 6-2 SRST リファレンスのセキュリティ設定 (続き)

設定	説明
Update SRST Certificate	 ヒント このボタンが表示されるのは、既存の SRST リファレンスのセキュリティ設定だけです。 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 証明書を置き換えます。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 証明書と共に) 電話機に送信します。

関連項目

- [SRST のセキュリティの概要 \(P.6-2\)](#)
- [SRST のセキュリティ設定用チェックリスト \(P.6-3\)](#)
- [トラブルシューティング \(P.7-1\)](#)



トラブルシューティング

この章は、次の内容で構成されています。

- [アラームの使用方法 \(P.7-2\)](#)
- [Microsoft パフォーマンス モニタ カウンタの使用方法 \(P.7-3\)](#)
- [ログ ファイルの検討 \(P.7-4\)](#)
- [HTTPS のトラブルシューティング \(P.7-5\)](#)
- [Cisco CTL クライアントのトラブルシューティング \(P.7-10\)](#)
- [CAPF のトラブルシューティング \(P.7-39\)](#)
- [暗号化のトラブルシューティング \(P.7-43\)](#)
- [セキュア SRST リファレンスのトラブルシューティング \(P.7-53\)](#)



ヒント

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 Administration Guide for Cisco CallManager*』を参照してください。

ここでは、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説明します。この作業の実行方法については、[表 7-4](#)、または IP Phone のモデルに対応した『*Cisco IP Phone Administration Guide for Cisco CallManager*』を参照してください。

アラームの使用法

Cisco CallManager Serviceability は、次の場合にアラームを生成します。

- 認証済みデバイスが非 TLS SCCP 接続を使用して登録する場合や、認証されていない IP Phone が TLS SCCP 接続を使用して登録する場合。
- ピア証明書のタイトルに含まれているデバイス名が、デバイス登録に使用されるデバイス名と一致しない場合。
- デバイスが Cisco CallManager 設定と互換性のない TLS 接続を使用して、Cisco CallManager に登録する場合。

次の状況では、IP Phone でアラームが生成される場合があります。

- TFTP Not Authorized: <IP address>

IP Phone がこのアラームを生成するのは、TFTP サーバ情報（代替またはそれ以外）が CTL ファイル内に存在しない場合です。DHCP がプライマリとバックアップのサーバアドレスを提供した状況で、どちらのアドレスも CTL ファイルに存在しない場合は、IP Phone がアラームを 2 回発行することがあります。CTL ファイル情報を正しく入力したこと、および DHCP サーバに正しいアドレスを設定したことを確認してください。

- File Auth Failed

IP Phone がこのアラームを生成する理由には、CTL ファイルの破損など、さまざまなものがあります。CTL ファイルが破損した場合は、sniffer トレースを使用して、ネットワークのトラブルシューティングを行う必要があります。問題を特定できない場合は、コンソール ケーブルを使用してデバッグする必要があります。詳細については、『*Cisco IP Phone Administration Guide for Cisco CallManager*』を参照してください（ただし、Cisco IP Phone 7970 モデル、7960 モデル、および 7940 モデルの場合で、IP Phone モデルに対応した管理マニュアルに詳細が記載されていないとき）。



ヒント

IP Phone で生成されるその他のアラームについては、IP Phone のモデルに対応した『*Cisco IP Phone Administration Guide for Cisco CallManager*』と、[P.7-27 の「CTL ファイルに問題がある場合の IP Phone のトラブルシューティング」](#)を参照してください。

関連項目

- *Cisco CallManager Serviceability アドミニストレーション ガイド*
- *Cisco CallManager Serviceability System Guide*
- *Cisco IP Phone Administration Guide for Cisco CallManager*

Microsoft パフォーマンス モニタ カウンタの使用法

Microsoft 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するために用意されています。

関連項目

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

ログ ファイルの検討

Cisco AVVID 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、事前に次のログ ファイルを取得して検討します。

- Cisco CallManager : C:\Program Files\Cisco\Trace\CCM
- TFTP : C:\Program Files\Cisco\Trace\TFTP
- DBL : C:\Program Files\Cisco\Trace\DBL
 - C:\Program Files\Cisco\Trace\DBL\DBLR*
 - C:\Program Files\Cisco\Trace\DBL\DBLR*
 - C:\Program Files\Cisco\Trace\DBL\DBL_CCM*
 - C:\Program Files\Cisco\Trace\DBL\DBL_TFTP*
 - C:\Program Files\Cisco\Trace\DBL\DBL_CTLPROVIDER*
- Cisco CallManager SDL Traces : C:\Program Files\Cisco\Trace\SDL\CCM



ヒント 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 ファイルを検討します。

- HTTPS : C:\program files\common files\cisco\logs\HTTPSCertInstall.log
- CTL Provider Service : C:\Program Files\Cisco\Trace\CTLProvider
- Cisco CTL クライアント : C:\Program Files\Cisco\CTL Client\Trace
デフォルトでは、Cisco CTL クライアントのインストール先は、CTL クライアントが存在するサーバまたはワークステーション上の C:\Program Files\Cisco\CTL File になります (C:\actinstall.log を参照)。
- Cisco Certificate Authority Proxy Function (CAPF) サービス : C:\Program Files\Cisco\Trace\CAPF
- SRST リファレンス : winnt\system32\Trace

関連項目

- [Cisco CTL クライアントの設定 \(P.3-1 \)](#)
- [Certificate Authority Proxy Function の使用方法 \(P.4-1 \)](#)

- [HTTP over SSL \(HTTPS\) の使用方法 \(P.2-1\)](#)
- [Survivable Remote Site Telephony \(SRST\) リファレンスのセキュリティ設定 \(P.6-1\)](#)

HTTPS 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。

- [HTTPS の設定時に表示されるメッセージ \(P.7-5\)](#)
- [HTTPS の有効化 \(P.7-7\)](#)
- [仮想ディレクトリの HTTPS の無効化 \(P.7-8\)](#)

HTTPS の設定時に表示されるメッセージ

表 7-1 は、HTTPS の設定時に問題が発生した場合に表示されるメッセージ、その問題への修正処置、および理由を説明しています。

表 7-1 HTTPS 設定時に表示されるメッセージ

メッセージ	修正処置または理由
The security library has encountered an improperly formatted DER-encoded message.	<p>このエラーが発生するのは、HTTPS サービスを有効にする証明書が、証明書のサブジェクト名としてホスト名を使用するためです。Netscape 4.79 はサブジェクト名に含まれているアンダースコアを無効な文字と見なすため、HTTPS は動作しません。</p> <p>メッセージが表示された場合は、OK をクリックします。</p> <p>HTTPS をサポートするには、Internet Explorer を使用します。Netscape 4.79 とホスト名を使用してアプリケーションにアクセスするには、HTTPS を無効にします (P.7-8 の「仮想ディレクトリの HTTPS の無効化」を参照)。</p>

表 7-1 HTTPS 設定時に表示されるメッセージ (続き)

メッセージ	修正処置または理由
<p>A network error occurred while Netscape was receiving data.</p> <p>(Network Error: Connection refused)</p> <p>Try connecting again.</p>	<p>HTTPS 用の Cisco CallManager 証明書が、ローカルの Netscape 4.79 ブラウザに存在しますが、Cisco CallManager HTTPS 証明書が表示されました。ユーザは、Netscape 4.79 ブラウザを使用して接続することはできません。</p> <p>次の方法のどちらかを実行します。</p> <ul style="list-style-type: none"> • Internet Explorer を使用して、アプリケーションにアクセスします。 • Netscape 4.79 を使用して、Communicator -> Tools -> Security Info -> Certificates -> Web sites の順に選択し、Cisco CallManager サーバ用の HTTPS 証明書を強調表示させます。Web Sites Certificates ウィンドウで Delete をクリックします。確認プロンプトで OK をクリックして確定します。次に OK をクリックします。

関連項目

- [HTTPS の有効化 \(P.7-7\)](#)
- [HTTPS 証明書の削除 \(P.7-9\)](#)
- [HTTP over SSL \(HTTPS\) の使用方法 \(P.2-1\)](#)

HTTPS の有効化

仮想ディレクトリの HTTPS を有効にするには、次の手順を実行します。

手順

-
- ステップ 1 **Start > Programs > Administrative Tools > Internet Services Manager** の順に選択します。
 - ステップ 2 HTTPS 証明書が存在するサーバの名前をクリックします。
 - ステップ 3 **Default Web Site** をクリックします。
 - ステップ 4 仮想ディレクトリをクリックします。
 - ステップ 5 **Properties** を右クリックします。
 - ステップ 6 **Directory Security** タブをクリックします。
 - ステップ 7 **Secure Communications** の下にある **Edit** ボタンをクリックします。
 - ステップ 8 **SSL Required** チェックボックスをオンにします。
 - ステップ 9 HTTPS を有効にするすべての仮想ディレクトリについて、この手順を実行します。
-

関連項目

- [HTTPS の有効化 \(P.7-7\)](#)
- [HTTPS の設定時に表示されるメッセージ \(P.7-5\)](#)
- [HTTP over SSL \(HTTPS\) の使用方法 \(P.2-1\)](#)

仮想ディレクトリの HTTPS の無効化

仮想ディレクトリの HTTPS 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 **Start > Programs > Administrative Tools > Internet Services Manager** の順に選択します。
- ステップ 2 HTTPS 証明書が存在するサーバの名前をクリックします。
- ステップ 3 **Default Web Site** をクリックします。
- ステップ 4 仮想ディレクトリ（たとえば、CCMAdmin）をクリックします。
- ステップ 5 **Properties** を右クリックします。
- ステップ 6 **Directory Security** タブをクリックします。
- ステップ 7 **Secure Communications** の下にある **Edit** をクリックします。
- ステップ 8 **SSL Required** チェックボックスをオフにします。
- ステップ 9 この作業を、CCMAdmin、CCMSservice、CCMUser、AST、BAT、RTMTReports、CCMTraceAnalysis、CCMSserviceTraceCollectionTool、PktCap、および ART の各仮想ディレクトリについて実行します。

関連項目

- [HTTP over SSL \(HTTPS\) の使用方法 \(P.2-1\)](#)
- [HTTPS 証明書の削除 \(P.7-9\)](#)
- [HTTPS の有効化 \(P.7-7\)](#)

HTTPS 証明書の削除

HTTPS 証明書を削除するには、次の手順を実行します。

手順

-
- ステップ 1 **Start > Programs > Administrative Tools > Internet Services Manager** の順に選択します。
 - ステップ 2 HTTPS 証明書が存在するサーバの名前をクリックします。
 - ステップ 3 **Directory Security** タブをクリックします。
 - ステップ 4 **Secure Communications** で **Server Certificate** ボタンをクリックします。
 - ステップ 5 **Next** をクリックします。
 - ステップ 6 **Remove the Current Certificate** を選択します。
 - 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。
-

関連項目

- [HTTPS の有効化 \(P.7-7\)](#)
- [HTTPS の設定時に表示されるメッセージ \(P.7-5\)](#)
- [HTTP over SSL \(HTTPS\) の使用方法 \(P.2-1\)](#)

Cisco CTL クライアント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。

- [セキュリティ トークン パスワード \(Etoken\) の変更 \(P.7-10\)](#)
- [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 \(P.7-12\)](#)
- [Smart Card サービスの Started および Automatic への設定 \(P.7-13\)](#)
- [Cisco CTL クライアントに関するメッセージ \(P.7-14\)](#)
- [CTL ファイルに問題がある場合の IP Phone のトラブルシューティング \(P.7-27\)](#)
- [Cisco IP Phone およびサーバ上の CTL ファイルの比較 \(P.7-29\)](#)
- [Cisco IP Phone 上の CTL ファイルの削除 \(P.7-30\)](#)
- [サーバ上の CTL ファイルの削除 \(P.7-32\)](#)
- [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 \(P.7-33\)](#)
- [セキュリティ トークン \(Etoken\) をすべて紛失した場合のトラブルシューティング \(P.7-34\)](#)
- [Cisco CTL クライアントの確認とアンインストール \(P.7-37\)](#)
- [Cisco CallManager クラスタのセキュリティ モードの確認 \(P.7-36\)](#)

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、証明書の秘密キーを取得し、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 2000 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 2000 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。
-

関連項目

- [Cisco CTL クライアントのインストール \(P.3-10\)](#)
- [CiscoCTL クライアントの設定 \(P.3-14\)](#)
- [CTL ファイルの更新 \(P.3-20\)](#)
- [Cisco CTL クライアント設定 \(P.3-24\)](#)

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.3-14 の「CiscoCTL 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。

関連項目

- [Cisco CTL クライアントのインストール \(P.3-10\)](#)
- [CiscoCTL クライアントの設定 \(P.3-14\)](#)
- [CTL ファイルの更新 \(P.3-20\)](#)
- [Cisco CTL クライアント設定 \(P.3-24\)](#)

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** 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。

関連項目

- システム要件 (P.1-5)
- 対話および制限 (P.1-6)
- Cisco CTL Provider サービスのアクティブ化 (P.3-5)
- Cisco CTL Provider サービスのアクティブ化 (P.3-5)
- CiscoCTL クライアントの設定 (P.3-14)
- CTL ファイルの更新 (P.3-20)
- デバイス セキュリティ モードの設定 (P.5-4)

Cisco CTL クライアントに関するメッセージ

表 7-2 は、Cisco CTL クライアントに関して表示される可能性のあるメッセージと、対応する修正処置または理由を示しています。

表 7-2 Cisco CTL クライアントに関するメッセージ

メッセージ	修正処置または理由
Unknown CTL Error	内部 CTL エラーが発生しました。CTL ログでエラーを検討してください。
Invalid Port number	有効なポート番号（数字のみ）を入力します。
Invalid Range for port numbers	正しい範囲を指定します。有効なポート番号範囲は、1026 ~ 32767 です。
Could not write information to the local Windows Registry	CTL クライアントにレジストリへのアクセス権がありません。ローカル管理者アカウントまたはローカル パワー ユーザ アカウントを使用してログインしたことを確認してください。Cisco CTL クライアントでは、サーバ名、ポート、および管理者名は以後のログイン用に保存されません。

表 7-2 Cisco CTL クライアントに関するメッセージ (続き)

メッセージ	修正処置または理由
Invalid Group Name	CTL Provider サービスで、ユーザの属する Windows 2000 ユーザ グループを取得できません。ローカル管理者アカウントまたはローカル パワー ユーザ アカウントを使用してログインしたことを確認してください。
Invalid User Name	有効なユーザ名を入力しませんでした。user name フィールドがブランクであるか、名前が最大文字数を超過しています。有効なユーザ名を入力します。
Invalid IP Address	有効な IP アドレスを入力しませんでした。アドレスが X.X.X.X 形式になっており、有効な IP 範囲を含んでいることを確認してください。有効な IP アドレスを入力します。
Invalid Hostname	有効なホスト名を入力しませんでした。server name フィールドがブランクであるか、フィールド内の文字数が最大許容文字数を超過しています。有効なホスト名を入力します。
User could not be authenticated	指定されたユーザ名に対して、誤ったパスワードを入力しました。正しいパスワードを入力します。
Invalid Password	無効なパスワードを入力しました。パスワードがブランクであるか、パスワードが最大許容文字数を超過しています。正しいパスワードを入力します。
Cannot run CTL Client from Terminal Services	CTL クライアントが Terminal Services と連動しません。アプリケーションをインストールしたマシン上でクライアントを設定する必要があります。
Failed to create CTL File	エラー発生後、CTL client ウィンドウ内に、サーバと障害理由のリストを示すダイアログボックスが表示されます。
Please insert a Security Token.Click Ok when done	セキュリティ トークンを挿入し、OK をクリックします。メッセージが引き続き表示される場合は、クライアントマシン上の Etoken Notification サービスを再起動します。
Cannot create CTL Entries.Total number of CTL Records has exceeded the Maximum	CTL ファイルに含まれている証明書またはエントリの数が、ファイルで許容された最大数を超過しています。不要なサーバまたは etoken を削除します。最大限度は 100 です。

表 7-2 Cisco CTL クライアントに関するメッセージ (続き)


メッセージ	修正処置または理由
Unable to create CTL Entry	CTL ファイルが、最大ファイル サイズの限度を越えています。最大ファイル サイズは 75K です。不要なセキュリティ トークンまたは代替 TFTP サーバ エントリの削除を検討します。
Unable to parse CTL File	システムで CTL ファイルを分析できませんでした。CTL ファイルが破損しています。クラスタ内のすべてのサーバ上で、CTL ファイルが他のユーザによって改ざんまたは置換されていないかどうかを調べます。  ヒント CTL クライアントからサブスクリバ サーバに接続し、サブスクリバ サーバから CTL ファイルを取得することができます。サブスクリバ サーバ上のファイルが破損している場合は、既存の CTL ファイルを削除し、新しいファイルを作成します。サブスクリバ サーバ上の CTL ファイルが破損していなければ、ファイルをパブリッシャに手動でコピーします。ただし、ファイルをコピーする前に、CTL ファイルが最新のものであることを確認してください。
CTL Client version is not compatible with the CTL Provider	CTL クライアントのバージョンと Cisco CallManager のバージョンを比較します。Cisco CallManager Administration 4.1 に表示される Cisco CTL クライアントを実行します。
Please select an item to delete	CTL Entries ウィンドウで、エントリを選択してから Delete をクリックします。
Error occurred when creating Dialog	システム メモリが不足しています。メモリ リソースを開放してから、CTL クライアントを再実行します。
--- No Issuer Name---	ノンセキュア モードでは、CTL Entries ウィンドウで発行者が No Issuer Name と表示されます。このメッセージは、ノンセキュア モードになっているためにアプリケーションが CTL ファイルにヌルの発行者名を書き込むことを示しています。

表 7-2 Cisco CTL クライアントに関するメッセージ (続き)

メッセージ	修正処置または理由
--- No Subject Name---	ノンセキュア モードでは、CTL Entries ウィンドウでサブジェクト名が No Subject Name と表示されます。このメッセージは、ノンセキュア モードになっているためにアプリケーションが CTL ファイルにヌルの発行者名を書き込むことを示しています。
You cannot delete this item.You can only delete Security Tokens and multi-cluster TFTP	CTL Entries ウィンドウで削除できるのは、セキュリティ トークンと代替 TFTP サーバだけです。
Are you sure you want to delete this item?	このメッセージは、CTL Entries ウィンドウからエントリを削除する前に表示されます。
You have selected to exit the CTL Client application.Are you sure you want to exit?	このメッセージは、Cisco CTL クライアント ウィンドウで Cancel をクリックしたとき、またはウィンドウを終了するときに表示されます。
You must have at least 2 security tokens in the CTL File	Finish をクリックして CTL ファイルに署名する前に、CTL Entries ペインに 2 つ以上のセキュリティ トークンが存在することを確認してください。
You must have at least one CallManager server in the cluster	Finish をクリックして CTL ファイルに署名する前に、CTL Entries ペインに 1 つの Cisco CallManager サーバ (CCM+TFTP 機能を含む) が存在することを確認してください。
Could not get CallManager Certificate from server <server name>	次の作業を実行してください。 <ol style="list-style-type: none"> 1. Cisco CallManager サーバにネットワーク接続できることを確認します。 2. Cisco CTL Provider サービスが設定されているポートに、Cisco CTL クライアントが接続されていることを確認します。 3. Cisco CallManager の自己署名証明書が c:\program files\cisco\certificates\ccmsserver.cer に存在することを確認します。 4. Cisco CallManager Serviceability で、Cisco CTL Provider サービスの詳細なトレースを有効にし、そのサービスのトレースを検討します。

表 7-2 Cisco CTL クライアントに関するメッセージ (続き)

メッセージ	修正処置または理由
Entry for Server already exists.	サーバのエントリがすでに CTL ファイル内に存在します。
No Help available.	このウィンドウのオンライン ヘルプは存在しません。
No CTL File exists on the server but the CallManager Cluster Security Mode is in Mixed Mode. You must create the CTL File and set Call Manager Cluster to Mixed Mode.	このメッセージが表示されるのは、CTL ファイルが他のユーザによって手動で削除または改ざんされている場合です。CTL ファイルから、証明書やセキュリティ トークンの情報を含むデータが一部削除されています。CTL ファイルを再作成します。
The CTL File signature is invalid or the CTL File is corrupt.	CTL ファイルが破損しています。CTL ファイルから、証明書やセキュリティ トークンの情報を含むデータが一部削除されています。CTL ファイルを再作成します。
You must recreate the CTL File.All existing certificate information in the CTL file will be lost.	Cisco CTL を実行して、CTL ファイルを再作成します。
There are no Security Tokens in CTL File.You must have at least 2 security tokens.Select Update CTL File to add security Tokens.	このメッセージが表示されるのは、CTL ファイルが破損している場合、無効の場合、または CTL クライアントでセキュリティ トークン情報を読み取ることができない場合です。CTL ファイルには、2 つ以上のセキュリティ トークンのエントリが含まれている必要があります。Update CTL File オプションを選択し、CTL ファイルを再作成します。
Please insert a Security Token.Click Ok when done.	USB ポートに Cisco セキュリティ トークンを挿入します。OK をクリックします。このメッセージが引き続き表示される場合は、セキュリティ トークンがシスコから発行されていること、および Etoken Notification サービスと Smart Card サービスが動作していることを確認してください。
Please insert another Security Token.Click Ok when done.	CTL ファイルに新しいトークンを追加するには、USB ポートに Cisco セキュリティ トークンを挿入します。OK をクリックします。このメッセージが引き続き表示される場合は、セキュリティ トークンがシスコから発行されていること、および Etoken Notification サービスと Smart Card サービスが動作していることを確認してください。

表 7-2 Cisco CTL クライアントに関するメッセージ (続き)

メッセージ	修正処置または理由
The Security Token you have inserted already exists in the CTL File.	セキュリティ トークン情報がすでに CTL ファイル内に存在します。ファイル内に存在しないトークンを挿入します。
The Security Token cannot be used to sign the CTL File.The token must already exist in the CTL file.	ファイル内に存在するトークンを挿入して、CTL ファイルに署名する必要があります。
No CTL File.	CTLFile.tlv が存在しません。
Error opening CTL File.	アプリケーションで CTLFile.tlv を開くことができません。Cisco CTL Provider サービスのトレースを検討してください。
Error reading CTL File.	システムで CTLFile.tlv を読み取ることができませんでした。Cisco CTL Provider サービスのトレースを検討してください。
CTL Filename or contents are invalid.	CTL ファイル名が無効であるか、CTL ファイルの内容が無効です。CTLFile.tlv が TFTP サービス パラメータの FileLocation パスに存在することを確認し、Cisco CTL Provider サービスのトレースを検討してください。
CTL File is not valid.	CTL ファイルが破損しているか、無効です。Cisco CTL Provider サービスのトレースを検討してください。
CTL File created successfully.	CTL ファイルは TFTPPath ロケーションに存在します。
CTL File operation was not successful on one or all the servers.Please correct the error and run the CTL Client again.	このエラーが表示された CTL クライアント ウィンドウで、サーバ名、パス、およびエラーの理由を確認してください。
You must restart all the CallManager and TFTP nodes in the Cluster.	CTL ファイルを作成したら、サービスを実行するクラスタ内のすべてのサーバ上で Cisco CallManager と TFTP サービスを再起動します。同様に、デバイスもリセットします。
No Valid Server Certificate found.	アプリケーションでセキュリティ トークン証明書を読み取ることができません。セキュリティ トークンがシスコから発行されていること、およびトークンが有効であることを確認してください。
No Server Certificate File found.	アプリケーションで Cisco CallManager サーバから証明書ファイルを読み取ることができません。 c:\program files\cisco\certificates\ccmserver.cer が存在することを確認してください。

表 7-2 Cisco CTL クライアントに関するメッセージ (続き)

メッセージ	修正処置または理由
Server Certificate is Invalid.	アプリケーションが無効な Cisco CallManager 証明書を検出しました。c:\program files\cisco\certificates\ccmserver.cer が存在することを確認してください。Cisco CTL Provider サービスのトレースを検討してください。
Certificate Date Invalid.	アプリケーションが、証明書に無効なデータが含まれていることを検出しました。Cisco CTL Provider サービスのトレースを検討してください。 Cisco CTL クライアントの Security Token Information ウィンドウで、セキュリティ トークン証明書の発行日と有効期限を確認してください。
Certificate expired.	証明書の期限が切れました。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
Certificate is not of type RSA.	Cisco CallManager 証明書が RSA タイプを使用していません。ccmserver.cer をダブルクリックします。Certificate Details ウィンドウで、公開キーに RSA が指定されていることを確認してください。指定されていない場合、Cisco CallManager サーバ証明書は無効です。
No Issuer Name in Certificate.	証明書に発行者名が含まれていません。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
Issuer name is not valid.	証明書の発行者名が無効です。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
Invalid Issuer Name length.	証明書の発行者名の長さが、256 文字を超えています。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
No Subject Name in Certificate.	証明書にサブジェクト名が含まれていません。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。

表 7-2 Cisco CTL クライアントに関するメッセージ (続き)

メッセージ	修正処置または理由
Subject name is not valid.	証明書のサブジェクト名が無効です。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
Invalid Subject Name length.	証明書のサブジェクト名が、256 文字を超えています。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
No Public Key in Certificate.	証明書に公開キーが含まれていません。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
Public Key is not valid.	証明書の公開キーが無効です。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
Invalid Public Key length.	証明書の公開キーの長さが、512 文字を超えています。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
No Private Key File.	証明書に秘密キーが含まれていません。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
Private Key File is not valid.	証明書の秘密キーが無効です。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
Invalid Cipher for Private key.	証明書の秘密キー暗号が無効です。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
Invalid Signature length.	証明書のシグニチャの長さが、1024 文字を超えています。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
Invalid Signature Algorithm.	証明書のシグニチャ アルゴリズムが無効です。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。

表 7-2 Cisco CTL クライアントに関するメッセージ (続き)

メッセージ	修正処置または理由
No Signature.	証明書にシグニチャが含まれていません。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
Invalid Thumbprint.	証明書の指紋が無効です。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
Invalid Serial Number.	証明書のシリアル番号が無効です。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
Invalid Serial Number length.	証明書のシリアル番号が、256 文字を超えています。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
Error Opening Security Token Store.	アプリケーションでセキュリティ トークン証明書を読み取ることができません。Etoken Notification サービスと Smart Card サービスが動作していることを確認してください。
No Certificate in Security Token.	セキュリティ トークンに証明書が含まれていません。セキュリティ トークンがシスコから発行されていることを確認してください。
Could not Sign Message.	Cisco CTL クライアントで CTL ファイルの内容に署名できません。Cisco CTL クライアントのトレースを検討してから、Cisco CTL クライアントを再度実行します。
Could not verify Message.	Cisco CTL クライアントで、CTL ファイルの内容への署名後にシグニチャを確認できません。Cisco CTL クライアントのトレースを検討してから、Cisco CTL クライアントを再度実行します。
Could not sign CTL File.	Cisco CTL クライアントのトレースを検討してから、Cisco CTL クライアントを再度実行します。

表 7-2 Cisco CTL クライアントに関するメッセージ (続き)

メッセージ	修正処置または理由
For the security of the phones, tokens inserted during update cannot be used to sign the CTL File.You must use one of the tokens that already existed in the CTL file to sign.Once this token has been inserted and the phones have been restarted, you may use the new tokens to sign the CTL File.	このメッセージは、修正処置を示しています。
Error Initializing SDI Control.	CTL Provider のトレースの初期化時に重大エラーが発生しました。Cisco CallManager Serviceability でトレースを設定します。
DBL Exception occurred.	CTL Provider の Database 層の初期化時に重大エラーが発生しました。DBL ログで例外を検討してください。
CM Name is too long.	入力した Cisco CallManager ホスト名が、256 文字を超えています。ホスト名を再度入力します。
Init TLS Failed.	アプリケーションで、Cisco CTL クライアントと Cisco CTL Provider サービスの間の SSL を初期化できません。Cisco CTL クライアントのトレースを検討してから、Cisco CTL クライアントを再度実行します。
TLS Connect Error when Opening Sockets.	Cisco CTL クライアントのトレースを検討してから、Cisco CTL クライアントを再度実行します。
Error occurred during SSL Handshake.	Cisco CTL クライアントのトレースを検討してから、Cisco CTL クライアントを再度実行します。
Could not connect to CTL provider Service.	クライアントの接続する Cisco CTL Provider ホスト名が、有効およびアクセス可能であることを確認してください。CTL Provider が、クライアントの接続するポートを傍受していることを確認してください。
Parsing data from CTLProvider failed.	内部エラーが発生しました。Cisco CTL クライアントが、Cisco CTL Provider サービスから無効なデータを受信しました。

表 7-2 Cisco CTL クライアントに関するメッセージ (続き)

メッセージ	修正処置または理由
Error occurred during Post CTL File operation.	Cisco CTL クライアントがクラスタ内のサーバに CTL ファイルをコピーしようとしたときに、内部エラーが発生しました。
Error occurred during Get CAPF File operation.	Cisco CTL クライアントが certificate trust list フォルダからファイルを取得しようとしたときに、内部エラーが発生しました。
Error occurred during Get CCM Certificate operation.	Cisco CTL クライアントが Cisco CallManager 証明書を取得しようとしたときに、内部エラーが発生しました。
Error occurred during Get CAPF Certificate operation.	Cisco CTL クライアントが CAPF 証明書を取得しようとしたときに、内部エラーが発生しました。
Error occurred during Authenticate User operation.	Cisco CTL クライアントがユーザを認証しようとしたときに、内部エラーが発生しました。
Invalid Response for Authenticate User operation.	Cisco CTL クライアントのバージョンが、Cisco CTL Provider サービスと互換性がありません。Cisco CallManager Administration 4.1 に表示される Cisco CTL クライアント プラグインをインストールおよび設定します。
Invalid Response for Get CCM List operation.	Cisco CTL クライアントのバージョンが、Cisco CTL Provider サービスと互換性がありません。Cisco CallManager Administration 4.1 に表示される Cisco CTL クライアント プラグインをインストールおよび設定します。
Invalid Response for Get CCM Certificate operation.	Cisco CTL クライアントのバージョンが、Cisco CTL Provider サービスと互換性がありません。Cisco CallManager Administration 4.1 に表示される Cisco CTL クライアント プラグインをインストールおよび設定します。
Invalid Response for Get CAPF Certificate operation.	Cisco CTL クライアントのバージョンが、Cisco CTL Provider サービスと互換性がありません。Cisco CallManager Administration 4.1 に表示される Cisco CTL クライアント プラグインをインストールおよび設定します。

表 7-2 Cisco CTL クライアントに関するメッセージ (続き)

メッセージ	修正処置または理由
Invalid Response for get CTL File operation.	Cisco CTL クライアントのバージョンが、Cisco CTL Provider サービスと互換性がありません。Cisco CallManager Administration 4.1 に表示される Cisco CTL クライアント プラグインをインストールおよび設定します。
Invalid Response for Get CAPF File operation.	Cisco CTL クライアントのバージョンが、Cisco CTL Provider サービスと互換性がありません。Cisco CallManager Administration 4.1 に表示される Cisco CTL クライアント プラグインをインストールおよび設定します。
Invalid Response for Get Cluster Security Mode operation.	Cisco CTL クライアントのバージョンが、Cisco CTL Provider サービスと互換性がありません。Cisco CallManager Administration 4.1 に表示される Cisco CTL クライアント プラグインをインストールおよび設定します。
Invalid Response for Get CTL Version operation.	Cisco CTL クライアントのバージョンが、Cisco CTL Provider サービスと互換性がありません。Cisco CallManager Administration 4.1 に表示される Cisco CTL クライアント プラグインをインストールおよび設定します。
Invalid Response for Get Alternate Paths operation.	Cisco CTL クライアントのバージョンが、Cisco CTL Provider サービスと互換性がありません。Cisco CallManager Administration 4.1 に表示される Cisco CTL クライアント プラグインをインストールおよび設定します。
Invalid Response for Authenticate User operation.	Cisco CTL クライアントのバージョンが、Cisco CTL Provider サービスと互換性がありません。Cisco CallManager Administration 4.1 に表示される Cisco CTL クライアント プラグインをインストールおよび設定します。
Not enough Memory to run Application.	システム メモリが不足しているため、Cisco CTL クライアントを実行できません。メモリ リソースを開放してから、Cisco CTL クライアントを再実行します。

表 7-2 Cisco CTL クライアントに関するメッセージ (続き)

メッセージ	修正処置または理由
Could not get CAPF Certificate(s).CAPF Service seems to be running on the CCM Publisher but the certificate file(s) do not exist in the Certificates trust path.Please check if the following certificates exist.	パブリッシャ データベース サーバ上で CAPF Service をアクティブにした場合は、capf.cer ファイルおよび対応する capf (.0) ファイルが certificates trust フォルダに存在することを確認してください。
Entry for this certificate already exists.	代替 TFTP サーバが CTL ファイル内に存在しないことを確認してください。
Failed to set Cluster Security Mode on the CallManager publisher.You must run the CTL Client again to set the correct value for the Cluster Security Mode.	CTL クライアントで Cluster Security Mode を正しい値に設定できません。このメッセージは、修正処置を示しています。
The Alternate TFTP Server entry is invalid.You must delete the entry for the Alternate TFTP Server and add it again	Cisco CTL Entries ペインから代替 TFTP サーバのエントリを削除し、エントリを再度追加します。このタスクを実行しないと、IP Phone が登録に失敗する場合があります。

関連項目

- [システム要件 \(P.1-5\)](#)
- [対話および制限 \(P.1-6\)](#)
- [Cisco CTL クライアントのインストール \(P.3-10\)](#)
- [CiscoCTL クライアントの設定 \(P.3-14\)](#)
- [CTL ファイルの更新 \(P.3-20\)](#)
- [ログ ファイルの検討 \(P.7-4\)](#)

CTL ファイルに問題がある場合の IP Phone のトラブルシューティング

表 7-3 は、IP Phone 上の CTL ファイルに関して発生する可能性のある問題を説明しています。

表 7-3 の修正処置を実行するには、CTL ファイル内に存在するセキュリティ トークンを 1 つ取得します。CTL ファイルを更新するには、P.3-20 の「CTL ファイルの更新」を参照してください。

表 7-3 IP Phone に関連する CTL ファイルの問題

問題	考えられる原因	修正処置
IP Phone が CTL ファイルを認証できない。	<p>次の原因を検討してください。</p> <ul style="list-style-type: none"> 最新の CTL ファイルに署名したセキュリティ トークンが、IP Phone 上の CTL ファイル内に存在しない。 既存の CTL ファイルに新しいセキュリティ トークンを追加しようとした。ファイルに追加された最後のトークンを使用して CTL ファイルに署名しようとした。IP Phone 上の既存の CTL ファイルに、新しいセキュリティ トークンのレコードが含まれていない可能性がある。 	<p>CTL ファイルを更新し、ファイル内に存在するセキュリティ トークンを使用して CTL ファイルに署名します。</p> <p>問題が引き続き発生する場合は、IP Phone から CTL ファイルを削除し、Cisco CTL クライアントを再度実行します。</p>
IP Phone が、CTL ファイル以外の設定ファイルを認証できない。	CTL ファイル内に不適切な TFTP エントリが存在する。	CTL ファイルを更新します。

表 7-3 IP Phone に関連する CTL ファイルの問題 (続き)

問題	考えられる原因	修正処置
IP Phone が TFTP 認証エラーを報告する。	次の原因を検討してください。 <ul style="list-style-type: none"> IP Phone の代替 TFTP アドレスが CTL ファイル内に存在しない。 新しい TFTP レコードを含む新しい CTL ファイルを作成した場合、IP Phone 上の既存の CTL ファイルに新しい TFTP サーバのレコードが含まれていない可能性がある。 	CTL ファイルを更新します。 新しい CTL ファイルに含まれている TFTP 情報が、IP Phone 上の既存の CTL ファイル内の情報と異なる場合は、IP Phone から既存の CTL ファイルを削除します。P.7-30 の「Cisco IP Phone 上の CTL ファイルの削除」を参照してください。
IP Phone が Cisco CallManager に登録されない。	CTL ファイルに、Cisco CallManager サーバに関する正しい情報が含まれていない。 自動登録が有効になっている可能性がある。	自動登録が無効になっていることを確認してください。 CTL ファイルを更新します。
IP Phone が、ローカルで有効な証明書を取得するための正しい CAPF サーバと相互対話しない。 TLS ハンドシェイク エラーが発生する。	CTL ファイルが最後に更新された後で、CAPF 証明書が変更されている。	CTL ファイルを更新します。
IP Phone が署名付きの設定ファイルを要求しない。	CTL ファイルに含まれている TFTP エントリに、証明書が関連付けられていない。	CTL ファイルを更新します。 CTL ファイルを更新したら、Cisco CallManager クラスタ全体のセキュリティ モードを混合モードに設定したことを確認してください。

関連項目

- システム要件 (P.1-5)
- Cisco CTL Provider サービスのアクティブ化 (P.3-5)

- Cisco CTL クライアントのインストール (P.3-10)
- CiscoCTL クライアントの設定 (P.3-14)
- CTL ファイルの更新 (P.3-20)
- ログ ファイルの検討 (P.7-4)

Cisco IP Phone およびサーバ上の CTL ファイルの比較

IP Phone 上の CTL ファイルのバージョンを特定するには、MD5 ハッシュを計算します。MD5 ハッシュとは、ファイルの内容に基づいて計算される暗号ハッシュです。

IP Phone には、MD5 ハッシュ値を計算するための、CTL ファイル用のオプションがあります。MD5 アプリケーションを使用すると、ディスク上のファイルの MD5 ハッシュを計算できます。ディスク上に保存されている CTL ファイルのハッシュ値と、IP Phone 上に表示される値を比較すると、IP Phone にインストールされているバージョンを特定できます。

IP Phone 上の CTL ファイルのバージョンを特定したら、サーバの CTL ファイルに対して MD5 チェックを実行すると、IP Phone が正しい CTL ファイルを使用していることを確認できます。

MD5 値を計算するには、次の手順を実行します。

手順

- ステップ 1 CTL ファイルが存在するサーバ上で、コマンド ウィンドウを開き、`cd c:\program files\cisco\bin\` と入力します。
- ステップ 2 ファイルの MD5 値を計算するには、`MD5UTIL.EXE <drive:><path><filename>` と入力します。



ヒント `<drive:><path> <filename>` という変数は、MD5 値の計算対象となるドライブ、ディレクトリ、またはその両方を指定します。この説明を CLI に表示するには、`md5util -?` と入力します。

たとえば、CTL ファイルの MD5 値を計算するには、MD5UTIL.exe c:\program files\cisco\ftfppath\ctlfile.tlv と入力します。

関連項目

- [Cisco CTL Provider サービスのアクティブ化 \(P.3-5\)](#)
- [CiscoCTL クライアントの設定 \(P.3-14\)](#)
- [CTL ファイルの更新 \(P.3-20\)](#)
- [Cisco CTL クライアント設定 \(P.3-24\)](#)

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 7-4](#) の作業を実行します。

表 7-4 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	<p data-bbox="649 418 1245 451">次の方法のどちらかを実行します。</p> <ul data-bbox="662 472 1245 667" style="list-style-type: none"> <li data-bbox="662 472 1245 594">• Security Configuration メニューのロックを解除します (『Cisco IP Phone Administration Guide 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。 <li data-bbox="662 610 1245 667">• Settings メニューにある Erase ソフトキーを押します。 <p data-bbox="649 688 1245 889"> (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 Administration Guide for Cisco CallManager』を参照してください。</p>

関連項目

- システム要件 (P.1-5)
- Cisco CTL Provider サービスのアクティブ化 (P.3-5)
- Cisco CTL クライアントのインストール (P.3-10)
- CiscoCTL クライアントの設定 (P.3-14)
- CTL ファイルの更新 (P.3-20)
- ログ ファイルの検討 (P.7-4)

サーバ上の CTL ファイルの削除

次の状況が発生した場合は、サーバ上の 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。



ヒント

Cisco CallManager または Cisco TFTP サービスが動作するクラスタ内のサーバすべてからファイルを必ず削除してください。

CTL ファイルを削除するには、次の手順を実行します。

手順

-
- ステップ 1 C:\Program Files\Cisco\ftppath (デフォルトの場所) または CTLFile.tlv が保存されている場所を参照します。
 - ステップ 2 CTLFile.tlv を右クリックし、**Delete** を選択します。
 - ステップ 3 Cisco CallManager または Cisco TFTP サービスが動作するクラスタ内のサーバすべてについて、この手順を実行します。
-

関連項目

- [システム要件 \(P.1-5\)](#)
- [Cisco CTL Provider サービスのアクティブ化 \(P.3-5\)](#)
- [Cisco CTL クライアントのインストール \(P.3-10\)](#)
- [CiscoCTL クライアントの設定 \(P.3-14\)](#)
- [CTL ファイルの更新 \(P.3-20\)](#)
- [ログ ファイルの検討 \(P.7-4\)](#)

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。
- 新しいトークンを CTL ファイルに追加します。
 - 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.3-20 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.1-13 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ポート」](#)を参照)。
-

関連項目

- [システム要件 \(P.1-5 \)](#)
- [Cisco CTL Provider サービスのアクティブ化 \(P.3-5 \)](#)
- [Cisco CTL クライアントのインストール \(P.3-10 \)](#)
- [CiscoCTL クライアントの設定 \(P.3-14 \)](#)
- [CTL ファイルの更新 \(P.3-20 \)](#)
- [ログ ファイルの検討 \(P.7-4 \)](#)

セキュリティ トークン (Etoken) をすべて紛失した場合のトラブルシューティング



ヒント

次の手順は、定期のメンテナンス期間に実行してください。これは、変更内容を有効にするために、クラスタ内のサーバすべてをリブートする必要があるためです。

セキュリティ トークンを紛失した場合、CTL ファイルを更新する必要がある場合は、次の手順を実行します。

手順

- ステップ 1 各 Cisco CallManager、Cisco TFTP、または代替 TFTP サーバ上で、CTLFile.tlv ファイルが存在するディレクトリを参照します。

デフォルト ディレクトリは、C:\program files\cisco\fttppath です。CTL ファイルが保存されている場所を特定するには、Cisco CallManager Administration の Service Parameters ウィンドウで、TFTP サービスの File Location サービス パラメータを見つけます。
- ステップ 2 CTLFile.tlv を削除します。
- ステップ 3 [ステップ 1](#) と [ステップ 2](#) を、すべての Cisco CallManager、Cisco TFTP、および代替 TFTP サーバについて繰り返します。
- ステップ 4 新しいセキュリティ トークンを 2 つ以上取得します。
- ステップ 5 Cisco CTL クライアントを使用して、CTL ファイルを作成します([P.3-10](#) の「Cisco CTL クライアントのインストール」と [P.3-14](#) の「Cisco CTL クライアントの設定」を参照)。

**ヒント**

クラスタ全体のセキュリティ モードが混合モードの場合は、Cisco CTL クライアントにより、「No CTL File exists on the server but the CallManager Cluster Security Mode is in Mixed Mode.For the system to function, you must create the CTL File and set CallManager Cluster to Mixed Mode. 」というメッセージが表示されます。**OK** をクリックします。次に、**Set Call Manager Cluster to Mixed Mode** を選択して、CTL ファイルの設定を完了します。

ステップ 6 すべてのサーバ上に CTL ファイルを作成したら、IP Phone から CTL ファイルを削除します（P.7-30 の「Cisco IP Phone 上の CTL ファイルの削除」を参照）。

ステップ 7 クラスタ内のサーバをすべてリポートします。

関連項目

- システム要件（P.1-5）
- Cisco CTL Provider サービスのアクティブ化（P.3-5）
- Cisco CTL クライアントのインストール（P.3-10）
- CiscoCTL クライアントの設定（P.3-14）
- CTL ファイルの更新（P.3-20）
- ログ ファイルの検討（P.7-4）

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 クラスタは混合モードに正しく設定されています。



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。

関連項目

- [システム要件 \(P.1-5\)](#)
- [Cisco CTL Provider サービスのアクティブ化 \(P.3-5\)](#)
- [Cisco CTL クライアントのインストール \(P.3-10\)](#)
- [CiscoCTL クライアントの設定 \(P.3-14\)](#)
- [CTL ファイルの更新 \(P.3-20\)](#)
- [ログ ファイルの検討 \(P.7-4\)](#)

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 2000 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。
-

関連項目

- [システム要件 \(P.1-5\)](#)
- [Cisco CTL Provider サービスのアクティブ化 \(P.3-5\)](#)
- [Cisco CTL クライアントのインストール \(P.3-10\)](#)
- [CiscoCTL クライアントの設定 \(P.3-14\)](#)
- [CTL ファイルの更新 \(P.3-20\)](#)
- [ログ ファイルの検討 \(P.7-4\)](#)

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

関連項目

- [Cisco CTL Provider サービスのアクティブ化 \(P.3-5\)](#)
- [Cisco CTL クライアントのインストール \(P.3-10\)](#)
- [CiscoCTL クライアントの設定 \(P.3-14\)](#)

CAPF 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。

- CAPF に関するメッセージ (P.7-39)
- IP Phone での認証文字列のトラブルシューティング (P.7-40)
- 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 (P.7-41)
- 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 (P.7-41)
- 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 (P.7-42)
- Manufactured-Installed Certificate (MIC) が IP Phone 内に存在することの確認 (P.7-42)

CAPF に関するメッセージ

表 7-5 は、CAPF に関するメッセージと修正処置を示しています。

表 7-5 CAPF に関するメッセージ

メッセージ	修正処置
Authentication String contains one or more invalid characters.Valid characters for Authentication String are numbers.	メッセージで指摘されたように、適切な情報を入力します。
CAPF Authentication String length should be between 4 and 10.	認証文字列の範囲は、4 ~ 10 桁です。適切な情報を入力します。
Operation Completes By contains one or more invalid characters.Valid characters for Operation Completes By are numbers.	メッセージで指摘されたように、適切な情報を入力します。
Invalid Year.Please enter a value equal to or greater than the current year.	このメッセージは、修正処置を示しています。
Invalid Month.Please adjust your entry to continue.	このメッセージは、修正処置を示しています。
Invalid Date.Please enter a value equal to or greater than the current date.	過去の日付を入力しました。適切な日付を入力します。

表 7-5 CAPF に関するメッセージ (続き)

メッセージ	修正処置
Invalid Date.Please adjust your entry to continue.	その月に対して無効な日付を入力しました。適切な日付を入力します。
Invalid Time.Please enter a value equal to or greater than current time (hours).	過去の時間を入力しました。適切な時間を入力します。
Invalid Time.Please adjust your entry to continue.	このメッセージは、修正処置を示しています。

関連項目

- システム要件 (P.1-5)
- 対話および制限 (P.1-6)
- Certificate Authority Proxy Function の概要 (P.4-2)
- CAPF の設定用チェックリスト (P.4-8)
- Phone Configuration ウィンドウの CAPF 設定 (P.4-20)
- 電話機での認証文字列の入力 (P.4-25)

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。

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。

関連項目

- [電話機での認証文字列の入力 \(P.4-25\)](#)
- [CAPF の設定用チェックリスト \(P.4-8\)](#)
- [Phone Configuration ウィンドウの CAPF 設定 \(P.4-20\)](#)

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。

関連項目

- [電話機での認証文字列の入力 \(P.4-25\)](#)
- [CAPF の設定用チェックリスト \(P.4-8\)](#)
- [Phone Configuration ウィンドウの CAPF 設定 \(P.4-20\)](#)
- [ログ ファイルの検討 \(P.7-4\)](#)
- [Certificate Authority Proxy Function の概要 \(P.4-2\)](#)

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 によって、キーペアと CAPF 固有の証明書が自動的に生成されます。CAPF 証明書は、Cisco CTL クライアントによってクラスタ内のサーバすべてにコピーされるもので、拡張子には .0 が使用されます。CAPF 証明書が存在することを確認するには、クラスタ内の各サーバで C:\Program Files\Cisco\Certificates を参照し、次のファイルを見つけます。

- DER 符号化形式：CAPF.cer
- PEM 符号化形式：CAPF.cer と同じ通常名の文字列を含む .0 拡張子のファイル

関連項目

- [電話機での認証文字列の入力 \(P.4-25\)](#)
- [CAPF の設定用チェックリスト \(P.4-8\)](#)
- [Phone Configuration ウィンドウの CAPF 設定 \(P.4-20\)](#)

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 IP Phone にインストールされていることを確認するには、**Settings > Model Information** の順に選択し、LSC 設定を表示します。LSC 設定では、環境に応じて、**Installed** または **Not Installed** と表示されます。

関連項目

- [電話機での認証文字列の入力 \(P.4-25\)](#)
- [CAPF の設定用チェックリスト \(P.4-8\)](#)
- [Phone Configuration ウィンドウの CAPF 設定 \(P.4-20\)](#)

Manufactured-Installed Certificate (MIC) が IP Phone 内に存在することの確認

MIC が IP Phone 内に存在することを確認するには、IP Phone の Security Configuration メニューで MIC option を選択します。この設定では、環境に応じて、**Installed** または **Not Installed** と表示されます。

関連項目

- [CAPF の設定用チェックリスト \(P.4-8\)](#)
- [Phone Configuration ウィンドウの CAPF 設定 \(P.4-20\)](#)
- [ログ ファイルの検討 \(P.7-4\)](#)
- [Certificate Authority Proxy Function の概要 \(P.4-2\)](#)

暗号化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。

- [SRTP/SCCP のトラブルシューティングの概要 \(P.7-43\)](#)
- [パケットキャプチャの設定チェックリスト \(P.7-44\)](#)
- [パケットキャプチャ サービス パラメータの設定 \(P.7-45\)](#)
- [パケットキャプチャ サービス パラメータ \(P.7-46\)](#)
- [BAT に対するパケットキャプチャの設定 \(P.7-47\)](#)
- [Phone Configuration ウィンドウでのパケットキャプチャの設定 \(P.7-47\)](#)
- [IP Phone のパケットキャプチャ設定の設定値 \(P.7-48\)](#)
- [キャプチャされたパケットの解析 \(P.7-50\)](#)
- [Cisco CallManager Administration でのパケットキャプチャに関するメッセージ \(P.7-51\)](#)
- [暗号化および割り込みの設定に関するメッセージ \(P.7-51\)](#)

SRTP/SCCP のトラブルシューティングの概要

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 ツールが運動しないため、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 とデバイス間で交換される SCCP メッセージの TCP パケットを解析する。
- デバイス間の SRTP パケットをキャプチャする。
- SCCP メッセージからメディアの暗号化キー関連情報を抽出し、デバイス間のメディアを復号化する。

関連項目

- [パケットキャプチャの設定チェックリスト \(P.7-44\)](#)
- [パケットキャプチャ サービス パラメータ \(P.7-46\)](#)
- [IP Phone のパケットキャプチャ設定の設定値 \(P.7-48\)](#)
- [キャプチャされたパケットの解析 \(P.7-50\)](#)
- [Cisco CallManager Administration でのパケットキャプチャに関するメッセージ \(P.7-51\)](#)

パケット キャプチャの設定チェックリスト

該当するデータを抽出および解析するには、次に示す表 7-6 の作業を実行します。

表 7-6 パケット キャプチャの設定チェックリスト

設定手順	関連手順および関連項目
ステップ 1 Cisco CallManager Administration の Service Parameter ウィンドウでパケット キャプチャを有効にします。	<ul style="list-style-type: none"> パケット キャプチャ サービスパラメータの設定 (P.7-45) パケット キャプチャ サービスパラメータ (P.7-46)
ステップ 2 サービスパラメータのデフォルト設定を使用しない場合は、Service Parameter ウィンドウで別の適用可能なサービスパラメータに更新します。	<ul style="list-style-type: none"> パケット キャプチャ サービスパラメータの設定 (P.7-45) パケット キャプチャ サービスパラメータ (P.7-46)
ステップ 3 Phone Configuration ウィンドウで、デバイスごとにパケット キャプチャを設定します。  (注) パケット キャプチャを一度に多くのデバイスに対して有効にしないことを強くお勧めします。これは、そのように設定すると、ネットワークにおける CPU 消費量が高くなる場合があるためです。	<ul style="list-style-type: none"> Phone Configuration ウィンドウでのパケット キャプチャの設定 (P.7-47) IP Phone のパケット キャプチャ設定の設定値 (P.7-48)
ステップ 4 パケットをキャプチャしたら、Signal Packet Capture Mode を None に設定し、Packet Capture Enable サービスパラメータを False に設定します。	<ul style="list-style-type: none"> パケット キャプチャ サービスパラメータの設定 (P.7-45) パケット キャプチャ サービスパラメータ (P.7-46)
ステップ 5 パケットの解析に必要なファイルを収集します。	キャプチャされたパケットの解析 (P.7-50)
ステップ 6 Cisco Technical Assistance Center (TAC) がパケットを解析します。この作業を実行するには、TAC に直接連絡してください。	キャプチャされたパケットの解析 (P.7-50)

パケット キャプチャ サービス パラメータの設定

パケット キャプチャのパラメータを設定するには、次の手順を実行します。

手順

- ステップ 1 Cisco CallManager Administration で、**Service > 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、**Cisco CallManager** サービスを選択します。
- ステップ 4 Packet Capture パラメータまでスクロールし、設定値を設定します（表 7-8 を参照）。
- ステップ 5 変更内容を有効にするには、**Update** をクリックします。
- ステップ 6 パケット キャプチャの設定を続行するには、[P.7-47 の「Phone Configuration ウィンドウでのパケット キャプチャの設定」](#)を参照してください。

関連項目

- [パケット キャプチャの設定チェックリスト \(P.7-44\)](#)
- [パケット キャプチャ サービス パラメータ \(P.7-46\)](#)

パケット キャプチャ サービス パラメータ

P.7-45 の「パケット キャプチャ サービス パラメータの設定」および表 7-7 を参照してください。

表 7-7 パケット キャプチャ設定の設定値

パラメータ	説明
Packet Capture Enable	このパラメータは、TLS 接続でのパケット キャプチャを有効にします。デフォルト値については、Service Parameter ウィンドウに表示される <i>i</i> ボタンをクリックしてください。
Packet Capture Service Listen TLS Port	このポートは、TLS 接続でのパケットをキャプチャするためのリアルタイム デバッグ ツールからの要求を受け付けます。デフォルト値については、Service Parameter ウィンドウに表示される <i>i</i> ボタンをクリックしてください。
Packet capture Max real time Client Connections	このパラメータは、パケット キャプチャに使用可能なリアルタイム デバッグ ツールからの接続の最大数を指定します。デフォルト値については、Service Parameter ウィンドウに表示される <i>i</i> ボタンをクリックしてください。
Packet Capture Max File	このパラメータは、バッチ モードのデバッグ時に Cisco CallManager で作成されるパケット キャプチャ ファイルの最大サイズを指定します。最大値に達すると、Cisco CallManager はファイルへの書き込みを停止します。デフォルト値と最大値については、Service Parameter ウィンドウに表示される <i>i</i> ボタンをクリックしてください。

関連項目

- [パケット キャプチャの設定チェックリスト \(P.7-44\)](#)
- [パケット キャプチャ サービス パラメータの設定 \(P.7-45\)](#)
- [IP Phone のパケット キャプチャ設定の設定値 \(P.7-48\)](#)

BAT に対するパケット 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、Packet Capture モードを設定できます。この作業の実行方法については、『*Bulk Administration Tool ユーザガイド*』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。

関連項目

- *Bulk Administration Tool ユーザガイド*
- [SRTP/SCCP のトラブルシューティングの概要 \(P.7-43\)](#)
- [パケット キャプチャの設定チェックリスト \(P.7-44\)](#)

Phone Configuration ウィンドウでのパケット キャプチャの設定

Service Parameter ウィンドウでパケット キャプチャを有効にしたら、Cisco CallManager Administration の Phone Configuration ウィンドウで、デバイスごとにパケット キャプチャを設定する必要があります。

パケット キャプチャをデバイスごとに有効または無効にします。パケット キャプチャのデフォルト設定は、None です。



ヒント

パケット キャプチャを一度に多くのデバイスに対して有効にしないことを強くお勧めします。これは、そのように設定すると、ネットワークにおける CPU 消費量が高くなる場合があるためです。

パケットをキャプチャしない場合や、作業が完了した場合は、Signal Packet Capture Mode を None に設定し、Packet Capture Enable サービスパラメータを False に設定します。

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 IP Phone の検索対象を指定してから **Find** をクリックするか、**Find** をクリックして IP Phone すべてのリストを表示します。

IP Phone をデータベースに追加していない場合、リストに IP Phone は表示されません。IP Phone の追加については、『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 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 トラブルシューティングの設定値を設定します（表 7-8 を参照）。

ステップ 5 **Update** をクリックします。

ステップ 6 **Reset Phone** をクリックします。

IP Phone をリセットすると、デバイス上のアクティブ コールは終了します。

関連項目

- [IP Phone のパケット キャプチャ設定の設定値 \(P.7-48\)](#)
- [パケット キャプチャの設定チェックリスト \(P.7-44\)](#)

IP Phone のパケット キャプチャ設定の設定値

[P.7-47 の「Phone Configuration ウィンドウでのパケット キャプチャの設定」](#)および [表 7-8](#) を参照してください。

表 7-8 IP Phone のパケット キャプチャ設定の設定値

設定	説明
Signal Packet Capture Mode	<p>ドロップダウン リスト ボックスから、次のオプションのどちらかを選択します。</p> <ul style="list-style-type: none"> Real-Time Mode : Cisco CallManager が、復号化されたメッセージまたは暗号化されていないメッセージを、セキュアなチャネルを通じて解析デバイスに送信します。Cisco CallManager とデバッグ ツール (IREC) の間に、TLS 接続が確立されます。認証後、Cisco CallManager は SCCP メッセージを、接続されているリアルタイム デバッグ ツールすべてに送信します。このアクションの対象は、パケット キャプチャを設定した選択済みのデバイスだけです。このモードの場合、ネットワーク上でスニファは使用できません。デバッグ ツール (IREC) は、SRTP パケットをキャプチャし、暗号化された SCCP メッセージから抽出されたキー関連情報を使用して、パケットを復号化します。デバッグ サイトにあるデバッグ ツールを実行する必要があります。 Batch Processing Mode : Cisco CallManager が、復号化されたメッセージまたは暗号化されていないメッセージをファイルに書き込み、システムが各ファイルを暗号化します。システムは、毎日、新しい暗号化キーを使用して新しいファイルを作成します。また、Cisco CallManager は 7 日ごとにファイルを格納する際に、ファイルを暗号化するキーをセキュアな場所に格納します。Cisco CallManager はファイルを C:\Program Files\Cisco\PktCap に格納します。単一のファイルに含まれるのは、タイム スタンプ、送信元 IP アドレス、宛先 IP アドレス、SCCP メッセージ長、および SCCP メッセージです。デバッグ ツールは、HTTPS、管理者のユーザ名とパスワード、および指定された日付を使用して、キャプチャされたパケットを含む単一の暗号化ファイルを要求します。同様に、ツールは暗号化された圧縮ファイルを復号化するキー情報を要求します。 <p>TAC に連絡する前に、関係するデバイス間でスニファトレースを使用して、SRTP パケットをキャプチャする必要があります。</p>
Packet Capture Duration	<p>このフィールドは、1 つのパケット キャプチャ セッションに割り当てる時間の最大値 (分単位) を指定します。デフォルトは 60 です。</p>

関連項目

- [パケットキャプチャの設定チェックリスト \(P.7-44\)](#)
- [キャプチャされたパケットの解析 \(P.7-50\)](#)
- [Phone Configuration ウィンドウでのパケットキャプチャの設定 \(P.7-47\)](#)
- [Cisco CallManager Administration でのパケットキャプチャに関するメッセージ \(P.7-51\)](#)

キャプチャされたパケットの解析

Cisco Technical Assistance Center (TAC) は、デバッグ ツールを使用してパケットを解析します。TAC に連絡する前に、関係するデバイス間でスニファトレースを使用して、SRTP パケットをキャプチャします。次の情報を収集したら、TAC に直接連絡してください。

- パケットキャプチャ ファイル：
<https://<server name or IP address>/pktcap/pktcap.asp?file=mm-dd-yyyy.pkt>。
ここで、サーバを参照し、月、日、年 (mm-dd-yyyy) に基づいてパケットキャプチャ ファイルを見つけます。
- ファイルのキー：
<https://<server name or IP address>/pktcap/pktcap.asp?key=mm-dd-yyyy.pkt>。
ここで、サーバを参照し、月、日、年 (mm-dd-yyyy) に基づいてキーを見つけます。
- Cisco CallManager サーバの管理ユーザ名とパスワード。

関連項目

- [パケットキャプチャの設定チェックリスト \(P.7-44\)](#)
- [IP Phone のパケットキャプチャ設定の設定値 \(P.7-48\)](#)
- [Cisco CallManager Administration でのパケットキャプチャに関するメッセージ \(P.7-51\)](#)

Cisco CallManager Administration でのパケット キャプチャに関するメッセージ

表 7-9 は、Cisco CallManager Administration でパケット キャプチャを設定するときに表示される可能性のあるメッセージのリストを示しています。

表 7-9 パケット キャプチャに関するメッセージ

メッセージ	修正処置
Packet Capture Duration contains one or more invalid characters.Valid characters for Packet Capture Duration are numbers.	このメッセージは、修正処置を示しています。
Invalid Packet Capture Duration.Packet Capture Duration should be between 0 and 300.	メッセージで指摘されたように、適切な情報を入力します。

関連項目

- [IP Phone のパケット キャプチャ設定の設定値 \(P.7-48 \)](#)
- [パケット キャプチャの設定チェックリスト \(P.7-44 \)](#)

暗号化および割り込みの設定に関するメッセージ

P.1-6 の「対話および制限」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、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。

関連項目

- [対話および制限 \(P.1-6\)](#)
- [暗号化の概要 \(P.1-21\)](#)
- [その他の情報 \(P.1-29\)](#)

セキュア SRST リファレンスのトラブルシューティング

この項は、次の内容で構成されています。

- [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 \(P.7-53\)](#)
- [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 \(P.7-54\)](#)

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。

関連項目

- [Survivable Remote Site Telephony \(SRST\) リファレンスのセキュリティ設定 \(P.6-1\)](#)
- *Cisco CallManager アドミニストレーション ガイド*
- SRST 対応のゲートウェイおよびこのバージョンの Cisco CallManager に対応したシステム管理マニュアル

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、次のメッセージが表示される場合があります。

「Port Numbers can only contain digits.」というメッセージです。このメッセージが表示されるのは、SRST Certificate Provider Port の設定時に無効なポート番号を入力した場合です。ポート番号は、1024 ~ 49151 の範囲に存在する必要があります。

関連項目

- [Survivable Remote Site Telephony \(SRST\) リファレンスのセキュリティ設定 \(P.6-1\)](#)
- *Cisco CallManager アドミニストレーション ガイド*
- SRST 対応のゲートウェイおよびこのバージョンの Cisco CallManager に対応したシステム管理マニュアル

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** をクリックします。次に、**Reset Devices** をクリックします。

関連項目

- [Survivable Remote Site Telephony \(SRST\) リファレンスのセキュリティ設定 \(P.6-1\)](#)
- *Cisco CallManager アドミニストレーション ガイド*
- SRST 対応のゲートウェイおよびこのバージョンの Cisco CallManager に対応したシステム管理マニュアル



C	
Certificate Authority Proxy Function (CAPF)	
CAPF 証明書のインストールの確認	7-41
CAPF を使用する電話機の検索	4-25
Cisco CallManager Serviceability の設定	4-6
Cisco CAPF サービス	3-7
IP Phone で入力された不適切な認証文字列	7-40
Manufacture-Installed Certificate が存在することの確認	7-42
エンタープライズパラメータ設定 (表)	4-16
概要	4-2
既存データの移行	4-10
サービスパラメータ設定 (表)	4-14
サービスパラメータの手順	4-13
設定 (表)	4-20
設定用チェックリスト (表)	4-8
対話および要件	4-4
電話機での認証文字列の入力	4-25
認証文字列	4-2
メッセージ	7-39
レポートの生成	4-24
ローカルで有効な証明書のインストールおよびアップグレード	4-17
ローカルで有効な証明書のインストールの確認	7-42
ローカルで有効な証明書の削除	4-18
Cisco CTL クライアント	
1 つのセキュリティトークンの紛失	7-33
Cisco CAPF サービス	3-7
Cisco CTL Provider サービス	3-5
CTL ファイルの移行	3-13
CTL ファイルの比較	7-29
IP Phone 上の CTL ファイルの削除	7-30
IP Phone のトラブルシューティング	7-27
Smart Card サービスの設定	7-13
TLS ポートの設定	3-8
アンインストール	7-37
インストール	3-10
概要	3-2
確認	7-37
クラスタ全体のセキュリティモードの更新	3-23
サーバ上の CTL ファイルの削除	7-32
すべてのセキュリティトークンの紛失	7-34
セキュリティトークンパスワードの変更	7-10
セキュリティモードの確認	7-36
設定	3-14
設定 (表)	3-24
設定用チェックリスト (表)	3-3
トラブルシューティング	7-10

- バージョンの特定 7-38
- プラグインのアップグレード 3-13
- メッセージ 7-5, 7-14
- ロックされたセキュリティ トークン 7-12
- Cisco IP Phone
 - CTL エラーのトラブルシューティング 7-27
 - CTL ファイルの削除 7-30
 - GARP 設定の無効化 5-11
 - IP Phone で入力された不適切な認証文字列 7-40
 - MD5 アプリケーションの使用 7-29
 - MD5 ハッシュの計算 7-29
 - PC Port 設定の無効化 5-13
 - PC Voice VLAN Access 設定の無効化 5-12
 - Setting Access 設定の無効化 5-12
 - Web Access 設定の無効化 5-11
 - セキュリティ機能 (表) 1-7
 - セキュリティ強化の設定 5-14
 - ローカルで有効な証明書のインストールの確認 7-42
- CTL クライアント
 - 1 つのセキュリティ トークンの紛失 7-33
 - Cisco CAPF サービス 3-7
 - Cisco CTL Provider サービス 3-5
 - CTL ファイルの移行 3-13
 - CTL ファイルの比較 7-29
 - IP Phone 上の CTL ファイルの削除 7-30
 - IP Phone のトラブルシューティング 7-27
 - Smart Card サービスの設定 7-13
 - TLS ポートの設定 3-8
 - アンインストール 7-37
 - インストール 3-10
 - 概要 3-2
- 確認 7-37
- クラスタ全体のセキュリティ モードの更新 3-23
- サーバ上の CTL ファイルの削除 7-32
- すべてのセキュリティ トークンの紛失 7-34
- セキュリティ トークン パスワードの変更 7-10
- セキュリティ モードの確認 7-36
- 設定 3-14
- 設定 (表) 3-24
- 設定用チェックリスト (表) 3-3
- トラブルシューティング 7-10
- バージョンの特定 7-38
- プラグインのアップグレード 3-13
- メッセージ 7-5, 7-14
- ロックされたセキュリティ トークン 7-12
- CTL ファイル
 - 1 つのセキュリティ トークンの紛失 7-33
 - IP Phone での削除 7-30
 - エントリの削除 3-27
 - 更新 3-20
 - サーバでの削除 7-32
 - すべてのセキュリティ トークンの紛失 7-34
 - 比較 7-29
- H
- HTTPS
 - Internet Explorer のサポート 2-5
 - Netscape のサポート 2-10
 - 概要 2-2

仮想ディレクトリ (表) 2-2
 サードパーティ証明書の使用方法 2-13
 証明書の削除 7-9
 証明書の詳細表示 (Internet Explorer) 2-7
 証明書を信頼できるフォルダに保存 (Internet Explorer) 2-6
 証明書を信頼できるフォルダに保存 (Netscape) 2-11
 証明書をファイルにコピー (Internet Explorer) 2-8
 トラブルシューティング 7-5
 無効化 7-8
 有効化 7-7

I

IP Phone

CTL エラーのトラブルシューティング 7-27
 CTL ファイルの削除 7-30
 GARP 設定の無効化 5-11
 IP Phone で入力された不適切な認証文字列 7-40
 MD5 アプリケーションの使用 7-29
 MD5 ハッシュの計算 7-29
 PC Port 設定の無効化 5-13
 PC Voice VLAN Access 設定の無効化 5-12
 Setting Access 設定の無効化 5-12
 Web Access 設定の無効化 5-11
 セキュリティ機能 (表) 1-7
 セキュリティ強化の設定 5-14
 ローカルで有効な証明書のインストールの確認 7-42

M

MGCP ゲートウェイ
 セキュリティの概要 1-11

S

SRST
 ゲートウェイから削除された証明書 7-54
 セキュリティ関連のメッセージ 7-53
 セキュリティ設定 (表) 6-6
 セキュリティ設定用チェックリスト (表) 6-3
 セキュリティの概要 6-2
 トラブルシューティング 7-53
 リファレンスのセキュリティ設定 6-4
 リファレンスのセキュリティの削除 7-53

SRST リファレンス

ゲートウェイから削除された証明書 7-54
 セキュリティ関連のメッセージ 7-53
 セキュリティ設定 (表) 6-6
 セキュリティの削除 7-53
 セキュリティの設定 6-4

あ

暗号化

Device Security Mode 設定 (表) 5-9
 SRTP/SCCP のトラブルシューティング 7-43
 インストール 1-15
 概要 1-21
 制限 1-6

- 対話 1-6
- デバイスの設定 5-4
- 割り込み制限 7-51

- い
- イメージ認証
 - 概要 1-18

- し
- シグナリング暗号化
 - インストール 1-15
 - 概要 1-21
 - デバイスの設定 5-4
- シグナリング整合性
 - 概要 1-18
- シグナリング認証
 - インストール 1-15
 - 概要 1-18
 - デバイスの設定 5-4
- 証明書
 - 種類 1-16
- 資料
 - 関連 xiv

- せ
- 整合性
 - 概要 1-18
- セキュリティ
 - Certificate Authority Proxy Function (CAPF)の概要 4-2
 - Cisco CallManager サービスの再起動 1-13
 - Cisco CAPF サービス 3-7
 - Cisco CTL Provider サービス 3-5
 - Cisco CTL クライアントの概要 3-2
 - Cisco CTL クライアントの設定用チェックリスト (表) 3-3
 - Etoken 3-10
 - HTTPS 2-2
 - IP Phone のパケット キャプチャ 7-43
 - MGCP ゲートウェイ 1-11
 - SRST の概要 6-2
 - TLS ポート 3-8
 - アラーム 7-2
 - 暗号化 1-21
 - 暗号化に対する割り込みの使用 7-51
 - インストール 1-15
 - クラスタのリポート 1-13
 - サーバのリポート 1-13
 - システム要件 1-5
 - 証明書の種類 1-16
 - 制限 1-6
 - 設定の概要 (表) 1-24
 - その他の情報 1-29
 - 対話 1-6
 - デバイスのリセット 1-13
 - トークン 3-10
 - 認証 1-18
 - パフォーマンス モニタ カウンタ 7-3
 - ベスト プラクティス 1-11
 - 用語 (表) 1-2
 - ログ ファイル 7-4

- て
- デバイス認証
- インストール 1-15
 - 概要 1-18
 - デバイスの設定 5-4
- 電話機
- GARP 設定の無効化 5-11
 - PC Port 設定の無効化 5-13
 - PC Voice VLAN Access 設定の無効化 5-12
 - Setting Access 設定の無効化 5-12
 - Web Access 設定の無効化 5-11
 - セキュリティ強化の設定 5-14
- 電話機のセキュリティ強化
- GARP 設定の無効化 5-11
 - PC Port 設定の無効化 5-13
 - PC Voice VLAN Access 設定の無効化 5-12
 - Setting Access 設定の無効化 5-12
 - Web Access 設定の無効化 5-11
 - 設定 5-14
- と
- トラブルシューティング
- 1つのセキュリティ トークンの紛失 7-33
 - CAPF 証明書のインストールの確認 7-41
 - CAPF メッセージ 7-39
 - Cisco CTL クライアント 7-10
 - Cisco CTL クライアント メッセージ 7-5, 7-14
 - HTTPS 7-5
 - IP Phone 上の CTL ファイルの削除 7-30
 - IP Phone で入力された不適切な認証文字列 7-40
 - Manufacture-Installed Certificate が存在することの確認 7-42
 - MD5 アプリケーションの使用 7-29
 - SRST セキュリティ関連のメッセージ 7-53
 - SRST リファレンス 7-53
 - SRST リファレンスからのセキュリティの削除 7-53
 - SRTP/SCCP の概要 7-43
 - キャプチャされたパケットの解析 7-50
 - ゲートウェイから削除された SRST 証明書 7-54
 - サーバ上の CTL ファイルの削除 7-32
 - すべてのセキュリティ トークンの紛失 7-34
 - セキュリティ アラーム 7-2
 - セキュリティ パフォーマンス モニタ カウンタ 7-3
 - セキュリティ ログ ファイル 7-4
 - パケット キャプチャ サービス パラメータ 7-45
 - パケット キャプチャ設定の設定値 (表) 7-48
 - パケット キャプチャの設定チェックリスト (表) 7-44
 - パケット キャプチャのメッセージ 7-51
 - ローカルで有効な証明書のインストールの確認 7-42
 - ローカルで有効な証明書の検証が失敗する 7-41
 - ロックされたセキュリティ トークン 7-12

- に
- 認証
- Device Security Mode 設定 (表) 5-9
 - インストール 1-15
 - 概要 1-18
 - 制限 1-6
 - 対話 1-6
 - デバイスの設定 5-4
- 認証文字列 4-2
- ふ
- ファイル認証
- 概要 1-18
 - デバイスの設定 5-4
- ま
- マニュアル
- 関連マニュアル xiv
 - 対象読者 xii
 - 表記法 xv
 - マニュアルの構成 xiii
 - 目的 xii
- め
- メディア暗号化
- インストール 1-15
 - 概要 1-21
 - デバイスの設定 5-4
- ろ
- ローカルで有効な証明書
- IP Phone で入力された不適切な認証文字列 7-40
 - インストールの確認 7-42