



# 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ず。

- 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 アンチウィルス 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 トランスコーダ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*』に記載されたように、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](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스팅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。

### 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
<b>ステップ 1</b>	<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> <b>ヒント</b> 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>	<a href="#">Cisco CTL Provider サービスのアクティブ化 (P.3-5)</a>
<b>ステップ 2</b>	<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> <b>ワンポイントアドバイス</b> Cisco CTL クライアントをインストールして設定する前にこの作業を実行すれば、CAPFを使用するために CTL ファイルを更新する必要がなくなります。</p>	<a href="#">Certificate Authority Proxy Function サービスのアクティブ化 (P.4-12)</a>

表 1-3 認証および暗号化の設定用チェックリスト（続き）

設定手順		関連手順および関連項目
<b>ステップ 3</b>	デフォルト設定を使用しない場合は、TLS 接続用のポートを設定します。   <b>ヒント</b> 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。	<a href="#">TLS 接続用ポートの設定 (P.3-8)</a>
<b>ステップ 4</b>	Cisco CTL クライアント用に設定するサーバについて、少なくとも2つのセキュリティトークンとパスワード、ホスト名またはIPアドレス、およびポート番号を入手します。	<a href="#">CiscoCTL クライアントの設定 (P.3-14)</a>
<b>ステップ 5</b>	 <b>ヒント</b> 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。	<ul style="list-style-type: none"> <li>• <a href="#">システム要件 (P.1-5)</a></li> <li>• <a href="#">インストール (P.1-15)</a></li> <li>• <a href="#">Cisco CTL クライアントのインストール (P.3-10)</a></li> </ul>

表 1-3 認証および暗号化の設定用チェックリスト（続き）

設定手順		関連手順および関連項目
<b>ステップ 6</b>	<p>Cisco CTL クライアントを設定します。</p> <p> <b>ヒント</b> Cisco 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>
<b>ステップ 7</b>	<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 パブリッシュ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> <b>注意</b> 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 パブリッシュ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"> <li>• システム要件 (P.1-5)</li> <li>• CAPF の設定用チェックリスト (P.4-8)</li> <li>• 既存の CAPF データの移行 (P.4-6)</li> <li>• 4.0 サブスクリバサーバから 4.0 パブリッシュ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)</li> </ul>

表 1-3 認証および暗号化の設定用チェックリスト（続き）

設定手順		関連手順および関連項目
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"> <li>• システム要件 (P.1-5)</li> <li>• 電話機での認証文字列の入力 (P.4-25)</li> <li>• 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)</li> </ul>
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。   <b>ヒント</b> 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。   <b>ヒント</b> 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。   <b>ヒント</b> 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

