セキュリティの概要

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

Cisco IP テレフォニー ネットワークは、認証された通信ストリームの確立および維持、電話機にファイルを転送する前のファイルへのデジタル署名、Cisco Unified IP Phone 間でのメディア ストリームおよびコール シグナリングの暗号化を行います。

この章は、次の内容で構成されています。

認証および暗号化に関する用語

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

表 1-1　用語

用語	定義
アクセス コントロール リスト（ACL）	システムの機能およびリソースにアクセスするためのアクセス権を定義するリスト。メソッド リストを参照。
認証	エンティティの ID を検証するプロセス。
許可	認証されたユーザ、サービス、またはアプリケーションに、要求されたアクションの実行に必要なアクセス権があるかどうかを指定するプロセス。Cisco Unified CallManager では、SUBSCRIBE 要求および一部のトランク側 SIP 要求を許可されたユーザに制限するセキュリティ プロセス。
許可ヘッダー	チャレンジに対する SIP ユーザ エージェントの応答。
Certificate Authority（CA; 認証局）	証明書を発行するエンティティ。シスコまたはサードパーティのエンティティなど。
Certificate Authority Proxy Function（CAPF）	サポートされたデバイスが Cisco Unified CallManager の管理機能を使用してローカルで有効な証明書を要求できるプロセス。
Certificate Trust List（CTL; 証明書信頼リスト）	電話機が信頼する証明書のリストを含むファイル。CTL ファイルは、Cisco Site Administrator Security Token（セキュリティ トークン）によって署名されます。CTL ファイルは、Cisco CTL クライアントを使用してクラスタをセキュア / 混合モードに移行するときに自動的に作成されます。
チャレンジ	ダイジェスト認証において、SIP ユーザ エージェントの ID を認証するための SIP ユーザ エージェントに対する要求。
Cisco Site Administrator Security Token（セキュリティ トークン、etoken）	秘密鍵と、Cisco Certificate Authority の署名する X.509v3 証明書が含まれるポータブル ハードウェア セキュリティ モジュール。ファイルの認証に使用され、CTL ファイルに署名します。
デバイス認証	接続前に、デバイスの ID を検証し、このエンティティが主張内容と一致することを確認するプロセス。
ダイジェスト認証	デバイス認証の形式。（特に）共有パスワードの MD5 ハッシュを使用して、SIP ユーザ エージェントの ID を確認します。
ダイジェスト ユーザ	SIP 電話機または SIP トランクが送信する許可要求に含まれているユーザ名。
暗号化	対象とする受信者だけが確実にデータを受信し読み取るようにするプロセス。情報の機密を確保し、データをランダムで無意味な暗号文に変換するプロセスです。暗号化アルゴリズムと暗号鍵が必要です。
ファイル認証	電話機でダウンロードするデジタル署名されたファイルを検証するプロセス。電話機は署名を検証して、ファイルが作成後に改ざんされていないことを確認します。
Hypertext Transfer Protocol over Secure Sockets Layer（HTTPS; HTTP over SSL）	HTTPS サーバの ID を（少なくとも）保証する IETF が定義したプロトコル。暗号化を使用して、Tomcat サーバとブラウザ クライアントとの間で交換される情報の機密を確保します。

表 1-1　用語（続き）

用語	定義
イメージ認証	電話機でロードする前にバイナリ イメージの改ざんを防止するプロセス。このプロセスによって電話機はイメージの整合性および発信元を検証します。
整合性	エンティティ間でデータの改ざんが行われていないことを確認するプロセス。
IPSec	エンドツーエンド セキュリティ用に、セキュアな H.225、H.245、RAS シグナリング チャネルを提供する転送。
Locally Significant Certificate（LSC; ローカルで有効な証明書）	電話機または JTAPI/TAPI/CTI アプリケーションにインストールされているデジタル X.509v3 証明書。発行元は、サードパーティの認証局または CAPF です。
Manufacture Installed Certificate（MIC; 製造元でインストールされる証明書）	Cisco Certificate Authority によって署名され、サポートされている電話機にシスコの製造過程でインストールされた X.509v3 デジタル証明書。
Man-in-the-Middle（中間者）攻撃	Cisco Unified CallManager と電話機との間で流れる情報を、攻撃者が監視して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護するプロセス。メディア暗号化では、IETF RFC 3711 で定義された Secure Real Time Protocol（SRTP）を使用します。
メッセージ / データ改ざん	攻撃者が、転送中のメッセージを変更しようとするイベント。コールの途中終了も含まれます。
メソッド リスト	許可プロセス中に、SIP トランクに着信する一定のカテゴリのメッセージを制限するツール。トランク側アプリケーションまたはデバイスに対して SIP 非インバイト メソッドを許可するかどうかを定義します。メソッド ACL とも呼ばれます。
混合モード	セキュリティを設定したクラスタ内のモード。Cisco Unified CallManager に接続する認証済みデバイスおよび非認証デバイスが含まれます。
ナンス	各ダイジェスト認証要求に対してサーバが生成する一意のランダム数値。
非セキュア コール	少なくとも 1 台のデバイスが認証も暗号化もされていないコール。
PKI	Public Key Infrastructure（公開鍵インフラストラクチャ）。証明書や認証局など、公開鍵の暗号化に必要な要素のセット。
リプレイ アタック	攻撃者が、電話機またはプロキシ サーバを識別する情報をキャプチャし、実際のデバイスを偽装しながら情報を再送するイベント。たとえば、プロキシ サーバの秘密鍵を偽装します。
System Administrator Security Token（SAST）	CTI/JTAPI/TAPI アプリケーションでは、CTL ダウンロード用の CTL ファイルへの署名に使用するトークン。
Simple Certificate Enrollment Protocol（SCEP）	X.509 証明書を発行する証明書認証との通信に使用するプロトコル。
セキュア コール	すべてのデバイスが認証され、メディア ストリームが暗号化されているコール。
シグナリング認証	転送中のシグナリング パケットが改ざんされていないことを検証するプロセス。Transport Layer Security プロトコルを使用します。

表 1-1　用語（続き）

用語	定義
シグナリング暗号化	デバイスと Cisco Unified CallManager サーバの間で送信されるすべてのシグナリング メッセージの機密保持を行うために、暗号化手法を使用するプロセス。
SIP レルム	ダイジェスト認証で保護される空間を指定する文字列（名前）。SIP 要求用の回線またはトランク側のユーザ エージェントを識別します。
SSL	インターネット上の電話メールなど、データ通信の安全を確保する暗号化プロトコル。SSL は、後継規格である TLS と同等のものです。
Transport Layer Security（TLS）	インターネット上の電話メールなど、データ通信の安全を確保する暗号化プロトコル。TLS は SSL と同等の役割を果たします。
信頼リスト	デジタル署名なしの証明書リスト。
信頼ストア	Cisco Unified CallManager などのアプリケーションによって明示的に信頼された X.509 証明書のリポジトリ。
X.509	証明書の形式など、PKI 証明書をインポートするための ITU-T 暗号化規格。

システム要件

認証および暗号化には、次のシステム要件があります。

- Cisco Unified CallManager リリース 5.1(3) は、このマニュアルに記載されているセキュリティ機能の最小要件として機能します。
- クラスタのサーバごとに、異なる管理者パスワードを使用できます。
- Cisco CTL クライアントで（Cisco Unified CallManager サーバにログインするために）使用されるユーザ名とパスワードは、Cisco Unified CallManager の管理ページのユーザ名およびパスワード（Cisco Unified CallManager の管理ページにログインするために使用するユーザ名とパスワード）と同じです。
- Cisco Unified CallManager との TLS 接続を認証するため、LSC がすべての電話機に備わっている必要があります。Certificate Authority Proxy Function（CAPF）については、P.6-4 の「CAPF システムの相互作用および要件」を参照してください。
- ボイスメール ポートのセキュリティを設定する前に、Cisco Unified CallManager リリースをサポートする Cisco Unity のバージョンがインストールされていることを確認します。

機能一覧

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

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

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

表 1-2　コール処理セキュリティ機能の一覧

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

セキュリティ アイコン

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

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

ポイントツーポイント コール、クラスタ内コール、クラスタ間コール、およびマルチホップ コールの場合は、コールのセキュリティ ステータスが変わることがあります。SCCP 回線、SIP 回線、および H.323 シグナリングでは、関与するエンドポイントに、コール セキュリティ ステータスの変更が通知されます。コール パスに SIP トランクが含まれている場合、コールのステータスは非セキュアになります。セキュリティ アイコンに関連付けられている制限については、P.1-9 の「セキュリティ アイコンと暗号化」を参照してください。

相互作用および制限

この項では、次のトピックについて取り上げます。

相互作用

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

プレゼンス

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

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

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

SIP トランク

SIP 発信転送機能、および Web Transfer や Click to Dial などの高度な転送関連機能を SIP トランクで使用するには、Cisco Unified CallManager で着信アウトオブダイアログ REFER 要求を受け付けるように許可する必要があります。

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

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

エクステンション モビリティ

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

CTI

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

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

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

制限

次の項で、シスコのセキュリティ機能に適用される制限について説明します。

認証と暗号化

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

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

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

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

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

割り込みと暗号化

割り込みと暗号化には、次の制限が適用されます。

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

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

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

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

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

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

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

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

ワイドバンド コーデックと暗号化

次の情報は、暗号化が設定されていて、ワイドバンドのコーデック リージョンに関連付けられた Cisco Unified IP Phone 7960 または 7940 に適用されます。これは、TLS/SRTP 用に設定された Cisco Unified IP Phone 7960 または 7940 にのみ適用されます。

暗号化されたコールを確立するため、Cisco Unified CallManager はワイドバンド コーデックを無視して、サポートされる別のコーデックを電話機が提示するコーデック リストから選択します。コールのもう一方のデバイスで暗号化が設定されていない場合、Cisco Unified CallManager はワイドバンド コーデックを使用して認証済みおよび非セキュア コールを確立できます。

メディア リソースと暗号化

Cisco Unified CallManager は、メディア リソースを使用しないセキュア Cisco Unified IP Phone（SCCP または SIP）、セキュア CTI デバイス / ルート ポイント、セキュア Cisco MGCP IOS ゲートウェイ、セキュア SIP トランク、セキュア H.323 ゲートウェイ、およびセキュア H.323/H.245/H.225 トランク間で、認証および暗号化されたコールをサポートします。たとえば次の場合に、Cisco Unified CallManager リリース 5.1 はメディア暗号化を提供しません。

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

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

電話機のサポートと暗号化

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

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

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

電話機のサポートと暗号化設定ファイル

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

暗号化された設定ファイルの電話機でのサポートについては、P.7-5 の「サポートされる電話機のモデル」を参照してください。

SIP トランクのサポートと暗号化

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

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

セキュリティ アイコンと暗号化

セキュリティ アイコンと暗号化には、次の制限が適用されます。

- 電話会議、コールの転送、保留などのタスクを実行するときに、暗号化ロック アイコンが電話機に表示されないことがあります。MOH などのタスクに関連付けられたメディア ストリームが暗号化されていない場合、ステータスは暗号化済みから非セキュアに変化します。
- Cisco Unified CallManager は、SIP トランク側接続で開始または終了するコールに対してはロック アイコンを表示しません。
- Cisco Unified CallManager は、H.323 トランクで転送されるコールに対してはシールド アイコンを表示しません。
- コールに PSTN が関わっている場合、セキュリティ アイコンで示されるのは、そのコールの IP ドメイン部分のセキュリティ ステータスだけです。

クラスタおよびデバイス セキュリティ モード

クラスタ セキュリティ モードが非セキュアになっている場合、電話機の設定ファイルのデバイス セキュリティ モードは非セキュアになります。このような場合は、Cisco Unified CallManager の管理ページでデバイス セキュリティ モードが認証済みまたは暗号化済みと示されていても、電話機は SRST 対応ゲートウェイおよび Cisco Unified CallManager と非セキュア接続を確立します。[SRST Allowed] チェックボックスなど、デバイス セキュリティ モード以外のセキュリティ関連の設定も無視されます。Cisco Unified CallManager の管理ページ内のセキュリティ設定は削除されませんが、セキュリティは提供されません。

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

ダイジェスト認証と暗号化

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

パケット キャプチャと暗号化

SRTP 暗号化が実装されている場合、サードパーティのスニファは動作しません。適切な認証で許可された管理者は、Cisco Unified CallManager の管理ページの設定を変更して、パケットのキャプチャを開始できます（デバイスがパケット キャプチャをサポートする場合）。

Cisco Unified CallManager でのパケット キャプチャの設定については、このリリースの『*Cisco Unified CallManager トラブルシューティング ガイド*』を参照してください。

ベスト プラクティス

シスコでは、次のベスト プラクティスを強く推奨します。

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

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

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

この項では、次のトピックについて取り上げます。

デバイスのリセット、サービスの再起動、またはサーバおよびクラスタのリブート

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

次のガイドラインを考慮します。

- Cisco Unified CallManager の管理ページで、異なるセキュリティ プロファイルを適用した後は、単一デバイスをリセットする。
- 電話機のセキュリティ強化作業を実行した場合は、デバイスをリセットする。
- クラスタ全体のセキュリティ モードを混合モードから非セキュア モード（またはその逆）に変更した後は、デバイスをリセットする。
- Cisco CTL クライアントの設定後、または CTL ファイルの更新後は、すべてのデバイスを再起動する。
- CAPF エンタープライズ パラメータを更新した後は、デバイスをリセットする。
- TLS 接続用のポートを更新した後は、Cisco CTL Provider サービスを再起動する。
- クラスタ全体のセキュリティ モードを混合モードから非セキュア モード（またはその逆）に変更した後は、Cisco CallManager サービスを再起動する。
- Cisco Certificate Authority Proxy Function サービスに関連する CAPF サービス パラメータを更新した後は、このサービスを再起動する。
- Cisco CTL クライアントの設定後、または CTL ファイルの更新後は、Cisco Unified CallManager Serviceability で Cisco CallManager および Cisco TFTP サービスをすべて再起動する。この作業は、これらのサービスが稼働するすべてのサーバで実行します。
- CTL Provider サービスを開始または停止した後は、すべての Cisco CallManager および Cisco TFTP サービスを再起動する。
- SRST リファレンスのセキュリティ設定後は、従属デバイスをリセットする。
- Smart Card サービスを「開始」および「自動」に設定した場合は、Cisco CTL クライアントをインストールした PC をリブートする。

- アプリケーション ユーザ CAPF プロファイルに関連付けられているセキュリティ関連のサービス パラメータを設定した後は、Cisco CallManager IP Manager Assistant サービス、Cisco WebDialer Web サービス、および Cisco Extended Functions サービスを再起動する。

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

設定の更新後に単一のデバイスをリセットするには、P.5-12 の「電話機セキュリティ プロファイルの適用」を参照してください。

クラスタ内のデバイスをすべてリセットするには、次の手順を実行します。

手順

ステップ 1　Cisco Unified CallManager の管理ページで［**システム**］>［**Cisco Unified CallManager**］の順に選択します。

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

ステップ 2　［**検索**］をクリックします。

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

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

ステップ 4　［**リセット**］をクリックします。

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

メディア暗号化の設定と割り込み

P.1-8 の「割り込みと暗号化」に加えて、次の情報も参照してください。

暗号化が設定されている Cisco Unified IP Phone 7960 および 7940 に対して割り込みを設定しようとすると、次のメッセージが表示されます。

If you configure encryption for Cisco Unified IP Phones 7960 and 7940, those encrypted devices cannot accept a barge request when they are participating in an encrypted call.When the call is encrypted, the barge attempt fails.

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

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

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

インストール

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

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

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

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

TLS と IPSec

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

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

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

証明書

証明書は、クライアントとサーバの ID を保護します。ルート証明書がインストールされた後、証明書はルート信頼ストアに追加され、デバイスやアプリケーション ユーザなど、ユーザとホストとの間の接続を保護します。

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

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

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

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

この項では、次のトピックについて取り上げます。

- 電話機の証明書の種類（P.1-14）
- サーバの証明書の種類（P.1-15）
- 外部 CA からの証明書のサポート（P.1-16）

電話機の証明書の種類

シスコでは次の種類の証明書を電話機で使用します。

- Manufacture-Installed Certificate（MIC; 製造元でインストールされる証明書）：この証明書は、サポートされている電話機にシスコの製造過程で自動的にインストールされます。製造元でインストールされる証明書は、LSC のインストールのために、Cisco Certificate Authority Proxy Function（CAPF）を認証します。MIC は上書きすることも削除することもできません。
- Locally Significant Certificate（LSC; ローカルで有効な証明書）：この種類の証明書は、Cisco Certificate Authority Proxy Function（CAPF）に関連する必要な作業を実行した後で、サポートされている電話機にインストールされます。設定タスクについては、P.1-25 の「設定用チェックリストの概要」を参照してください。デバイス セキュリティ モードで認証または暗号化を設定すると、LSC によって Cisco Unified CallManager と電話機との間の接続が保護されます。

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

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

管理者は、MIC ルート証明書を CallManager 信頼ストアから削除する必要があります。CAP-RTP-001
CAP-RTP-002
Cisco_Manufacturing_CA
Cisco_Root_CA_2048

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

サーバの証明書の種類

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

- HTTPS 証明書（tomcat_cert）：この自己署名ルート証明書は、Cisco Unified CallManager をインストールするときに、HTTPS サーバに対して生成されます。
- Cisco Unified CallManager ノード証明書 : この自己署名ルート証明書は、Cisco Unified CallManager 5.1 をインストールすると、Cisco Unified CallManager サーバに自動的にインストールされます。Cisco Unified CallManager 証明書によって、サーバの識別情報が提供されます。この情報には、Cisco Unified CallManager サーバ名と Global Unique Identifier（GUID）が含まれます。
- CAPF 証明書 : このルート証明書は、Cisco CTL クライアントの設定が完了した後で、クラスタ内のすべてのサーバにコピーされます。
- IPSec 証明書（ipsec_cert）：この自己署名ルート証明書は、Cisco Unified CallManager のインストール中に、MGCP および H.323 ゲートウェイまたはその他の外部マシンとの IPSec 接続に対して生成されます。
- SRST 対応ゲートウェイ証明書：Cisco Unified CallManager の管理ページのセキュア SRST 参照を設定するときに、Cisco Unified CallManager は、ゲートウェイから SRST 対応ゲートウェイ証明書を取得し、Cisco Unified CallManager データベースに格納します。デバイスをリセットすると、証明書は電話機設定ファイルに追加されます。この証明書はデータベースに格納されるため、証明書管理ツールには統合されません。

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

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

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

外部 CA からの証明書のサポート

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

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

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

サードパーティの CA 署名付き証明書をプラットフォームにアップロードした後、CTL クライアントを実行して、CTL ファイルを更新してください。CTL クライアントの実行後、該当するサービスを更新のため再起動します。たとえば、Cisco Unified CallManager 証明書の更新では Cisco Unified CallManager および Cisco TFTP、CAPF 証明書の更新では CAPF を再起動します。更新の手順については、P.3-11 の「Cisco CTL クライアントの設定」を参照してください。

プラットフォームでの証明書署名要求（CSR）の生成については、『*Cisco Unified Communications Operating System アドミニストレーション ガイド*』を参照してください。

認証、整合性、および許可の概要

整合性および認証によって、次の脅威から保護します。

- TFTP ファイルの操作（整合性）
- 電話機と Cisco Unified CallManager との間で行われるコール処理シグナリングの変更（認証）
- 表 1-1 で定義した Man-in-the-Middle（中間者）攻撃（認証）
- 電話機およびサーバの ID 盗難（認証）
- リプレイ アタック（ダイジェスト認証）

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

認証、整合性、および許可の詳細については、次の項を参照してください。

- イメージ認証（P.1-17）
- デバイス認証（P.1-17）
- ファイル認証（P.1-18）
- シグナリング認証（P.1-18）
- ダイジェスト認証（P.1-18）
- 許可（P.1-20）

イメージ認証

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

デバイス認証

このプロセスでは、デバイスの ID を検証し、このエンティティが主張内容と一致することを確認します。サポートされるデバイスのリストについては、P.4-3 の「サポートされる電話機のモデル」を参照してください。

デバイス認証は、Cisco Unified CallManager サーバと、サポートされる Cisco Unified IP Phone、SIP トランク、または JTAPI/TAPI/CTI アプリケーション（サポートされる場合）の間で発生します。認証された接続は、各エンティティが他のエンティティの証明書を受け付けたときにのみ、これらのエンティティの間で発生します。この相互証明書交換プロセスは、相互認証と呼ばれます。

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

ヒント　Cisco Unified CallManager 信頼ストアに SIP ユーザ エージェント証明書が含まれ、SIP ユーザ エージェントの信頼ストアに Cisco Unified CallManager 証明書が含まれている場合、SIP トランク経由で接続する SIP ユーザ エージェントは、Cisco Unified CallManager に対して認証されます。Cisco Unified CallManager 信頼ストアの更新の詳細については、『*Cisco Unified Communications Operating System アドミニストレーション ガイド*』を参照してください。

ファイル認証

このプロセスでは、電話機でダウンロードするデジタル署名されたファイルを検証します。たとえば、設定、呼出音一覧、ロケール、CTL ファイルなどがあります。電話機は署名を検証して、ファイルが作成後に改ざんされていないことを確認します。サポートされるデバイスのリストについては、P.4-3 の「サポートされる電話機のモデル」を参照してください。

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

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

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

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

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

シグナリング認証

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

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

ダイジェスト認証

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

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

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

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

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

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

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

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

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

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

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

管理者は、電話機ユーザまたはアプリケーションユーザの SIP ダイジェスト クレデンシャルを設定します。アプリケーションの場合は、Cisco Unified CallManager の管理ページの［アプリケーション ユーザの設定（Application User Configuration）］ウィンドウで、［ダイジェスト信用証明書（Digest Credentials）］を指定します。SIP 電話機の場合は、Cisco Unified CallManager の管理ページの［エンドユーザの設定（End User Configuration）］ウィンドウで、［ダイジェスト信用証明書（Digest Credentials）］を指定し、電話機に適用します。

ユーザを設定した後でクレデンシャルを電話機に関連付けるには、［電話の設定（Phone Configuration）］ウィンドウで［ダイジェストユーザ（Digest User）］（エンド ユーザ）を選択します。電話機をリセットした後、クレデンシャルは、TFTP サーバが電話機に提供する電話機設定ファイルに存在するようになります。

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

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

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

許可

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

- SIP インバイト メッセージと in-dialog メッセージ、および SIP 電話機の場合、Cisco Unified CallManager はコーリング サーチ スペースおよびパーティションを通じて許可を与えます。
- 電話機からの SIP SUBSCRIBE 要求の場合、Cisco Unified CallManager は、プレゼンス グループへのユーザ アクセスに許可を与えます。
- SIP トランクの場合、Cisco Unified CallManager はプレゼンス サブスクリプションおよび非インバイト SIP メッセージ（アウトオブダイアログ REFER、未承諾 NOTIFY、REPLACE ヘッダー付き SIP 要求など）の許可を与えます。［SIP トランクセキュリティプロファイルの設定（SIP Trunk Security Profile Configuration）］ウィンドウで、関連するチェックボックスをオンにして、許可を指定します。

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

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

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

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

暗号化の概要

ヒント　暗号化は、Cisco Unified CallManager 5.1 をクラスタ内の各サーバにインストールすると、自動的にインストールされます。

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

- シグナリング暗号化（P.1-22）
- メディア暗号化（P.1-22）
- 設定ファイルの暗号化（P.1-24）

シグナリング暗号化

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

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

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

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

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

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

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

メディア暗号化

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

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

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

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

警告　**Cisco IOS MGCP ゲートウェイ、H.323 ゲートウェイ、H.323/H.245/H.225 トランク、および SIP トランクでセキュリティ関連情報が暗号化されずに送信されないようにするには、IPSec 設定に依存します。したがって、ゲートウェイおよびトランクに SRTP またはシグナリング暗号化を設定する前に、IPSec を設定することを強く推奨します。Cisco Unified CallManager は、IPSec が正しく設定されていることを確認しません。IPSec を正しく設定しないと、セキュリティ関連情報が公開される可能性があります。**

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

次の例で、SCCP および MGCP コールのメディア暗号化を示します。

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

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

設定ファイルの暗号化

Cisco Unified CallManager は、TFTP サーバからの設定ファイルのダウンロードで、機密データ（ダイジェスト クレデンシャルや管理者パスワードなど）を電話機に送出します。

Cisco Unified CallManager は、可逆暗号化を使用して、データベース内でこれらのクレデンシャルを保護します。ダウンロード プロセス中にこのデータを保護するため、このオプションをサポートするすべての Cisco Unified IP Phone（P.7-5 の「サポートされる電話機のモデル」を参照）で、暗号化された設定ファイルを設定することをお勧めします。このオプションが有効である場合、デバイス設定ファイルだけがダウンロード用に暗号化されます。

（注）　状況によっては（たとえば、電話機のトラブルシューティングを行う場合や、自動登録中など）、機密データを電話機にクリアでダウンロードすることを選択することもできます。

Cisco Unified CallManager は、暗号鍵を符号化し、データベースに格納します。TFTP サーバは、対称暗号鍵を使用して、設定ファイルを暗号化および復号化します。

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

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

詳細については、第 7 章「電話機設定ファイルの暗号化について」を参照してください。

設定用チェックリストの概要

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

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

表 1-3　認証および暗号化の設定用チェックリスト

設定手順		関連手順および関連項目
ステップ 1	クラスタにある各サーバの Cisco Unified CallManager Serviceability で Cisco CTL Provider サービスをアクティブにします。 **ヒント** Cisco Unified CallManager のアップグレード前にこのサービスをアクティブにした場合は、サービスを再度アクティブにする必要はありません。アップグレード後にサービスは自動的にアクティブになります。	Cisco CTL Provider サービスのアクティブ化（P.3-5）
ステップ 2	最初のノードの Cisco Unified CallManager Serviceability で Cisco Certificate Authority Proxy サービスをアクティブにし、ローカルで有効な証明書のインストール、アップグレード、トラブルシューティング、または削除を行います。 **ワンポイント アドバイス** Cisco CTL クライアントをインストールして設定する前にこの作業を実行すれば、CAPF を使用するために CTL ファイルを更新する必要がなくなります。	Certificate Authority Proxy Function サービスのアクティブ化（P.6-6）
ステップ 3	デフォルトのポート設定を使用しない場合は、TLS 接続用のポートを設定します。 **ヒント** これらの設定を Cisco Unified CallManager のアップグレード前に設定した場合、設定はアップグレード時に自動的に移行されます。	TLS 接続用ポートの設定（P.3-6）
ステップ 4	Cisco CTL クライアント用に設定するサーバについて、少なくとも 2 つのセキュリティ トークンとパスワード、ホスト名または IP アドレス、およびポート番号を入手します。	Cisco CTL クライアントの設定（P.3-11）
ステップ 5	Cisco CTL クライアントをインストールします。 **ヒント** Cisco Unified CallManager 5.1(3) にアップグレードした後で Cisco CTL ファイルを更新するには、Cisco Unified CallManager の管理機能 5.1(3) で使用可能なプラグインをインストールする必要があります。	• システム要件（P.1-4） • インストール（P.1-13） • Cisco CTL クライアントのインストール（P.3-8） • Cisco CTL クライアントのアップグレードおよび Cisco CTL ファイルの移行（P.3-10）

表 1-3　認証および暗号化の設定用チェックリスト（続き）

設定手順		関連手順および関連項目
ステップ 6	Cisco CTL クライアントを設定します。 ヒント　Cisco Unified CallManager のアップグレード前に Cisco CTL ファイルを作成した場合、Cisco CTL ファイルはアップグレード時に自動的に移行されます。Cisco Unified CallManager 5.1(3) にアップグレードした後で Cisco CTL ファイルを更新するには、Cisco CTL クライアントの 5.1(3) バージョンをインストールして設定する必要があります。	• Cisco CTL クライアントの設定（P.3-11） • Cisco CTL クライアントのアップグレードおよび Cisco CTL ファイルの移行（P.3-10）
ステップ 7	電話機のセキュリティ プロファイルを設定します。プロファイルを設定するときは、次の作業を実行します。 • デバイス セキュリティ モードを設定します（SCCP 電話機および SIP 電話機の場合）。 デバイス セキュリティ モードは、Cisco Unified CallManager のアップグレード時に自動的に移行されます。Cisco Unified CallManager 4.0 で認証だけをサポートしていたデバイスに暗号化を設定する場合は、［電話の設定（Phone Configuration）］ウィンドウで暗号化のセキュリティ プロファイルを選択する必要があります。 • CAPF 設定を定義します（一部の SCCP 電話機および SIP 電話機の場合）。 追加の CAPF 設定が［電話の設定（Phone Configuration）］ウィンドウに表示されます。 • SIP 電話機でダイジェスト認証を使用する場合は、［ダイジェスト認証を有効化（Enable Digest Authentication）］チェックボックスをオンにします。 • 暗号化された設定ファイルを有効にするには（一部の SCCP 電話機および SIP 電話機）、［TFTP 暗号化（TFTP Encrypted Config）］チェックボックスをオンにします。 • 設定ファイルのダウンロードでダイジェスト クレデンシャルを除外するには、［設定ファイル内のダイジェスト信用証明書を除外（Exclude Digest Credentials in Configuration File）］チェックボックスをオンにします。	電話機セキュリティ プロファイルの設定（P.5-1） 電話機セキュリティ プロファイルの設定のヒント（P.5-2） 暗号化された電話機設定ファイルの設定（P.7-1） 暗号化された設定ファイルの設定のヒント（P.7-6）
ステップ 8	電話機に電話機セキュリティ プロファイルを適用します。	電話機セキュリティ プロファイルの適用（P.5-12）

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 9	電話機に証明書を発行するように CAPF を設定します。 Cisco Unified CallManager 5.1 へのアップグレード前に証明書の操作を実行して CAPF をサブスクライバ サーバで実行した場合、CAPF データを 4.0 パブリッシャ データベース サーバにコピーしてから、クラスタを Cisco Unified CallManager 5.1 にアップグレードする必要があります。 **注意** Cisco Unified CallManager 4.0 サブスクライバ サーバの CAPF データは Cisco Unified CallManager 5.1 データベースに移行されません。したがって、データを 5.1 データベースにコピーしないと、データは失われます。データが失われても、CAPF ユーティリティ 1.0(1) を使用して発行したローカルで有効な証明書は電話機に残ります。しかし、この証明書はもう有効でないため、CAPF 5.1 は証明書を再発行する必要があります。	• システム要件（P.1-4） • CAPF の設定用チェックリスト（P.6-5）
ステップ 10	ローカルで有効な証明書が、サポートされている Cisco Unified IP Phone にインストールされたことを確認します。	• システム要件（P.1-4） • 電話機での認証文字列の入力（P.6-12）
ステップ 11	SIP 電話機のダイジェスト認証を設定します。	SIP 電話機のダイジェスト認証の設定（P.8-1）
ステップ 12	電話機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 Unified CallManager のアップグレード前に設定した場合、デバイス設定はアップグレード時に自動的に移行されます。	電話機のセキュリティ強化（P.9-1）
ステップ 13	セキュリティ用のボイスメール ポートを設定します。	• ボイスメール ポートのセキュリティ設定（P.10-1） • *Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity 4.x*
ステップ 14	SRST リファレンスのセキュリティを設定します。 **ヒント** 前のリリースの Cisco Unified CallManager でセキュア SRST リファレンスを設定した場合は、Cisco Unified CallManager のアップグレード時にその設定が自動的に移行されます。	Survivable Remote Site Telephony（SRST）リファレンスのセキュリティ設定（P.12-1）

表 1-3　認証および暗号化の設定用チェックリスト（続き）

設定手順		関連手順および関連項目
ステップ 15	IPSec を設定します。	• ゲートウェイおよびトランクの暗号化の設定（P.13-1） • ネットワーク インフラストラクチャで IPSec を設定する場合の注意事項（P.13-6） • *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways* • *Cisco Unified Communications Operating System アドミニストレーション ガイド*
ステップ 16	SIP トランク セキュリティ プロファイルを設定します。 ダイジェスト認証を使用する場合は、プロファイルの［ダイジェスト認証を有効化（Enable Digest Authentication）］チェックボックスをオンにします。 トランクレベルの許可の場合、許可する SIP 要求の許可チェックボックスをオンにします。 トランクレベルの許可の後、アプリケーションレベルの許可を発生させる場合は、［アプリケーションレベル認証を有効化（Enable Application Level Authorization）］チェックボックスをオンにします。 ダイジェスト認証をオンにしない場合、アプリケーションレベルの許可はオンにできません。	• SIP トランク セキュリティ プロファイルの設定（P.14-4） • ダイジェスト認証のエンタープライズ パラメータの設定（P.15-2）
ステップ 17	SIP トランク セキュリティ プロファイルをトランクに適用します。	SIP トランク セキュリティ プロファイルの適用（P.14-10）
ステップ 18	トランクのダイジェスト認証を設定します。	SIP トランクのダイジェスト認証の設定（P.15-1）
ステップ 19	SIP トランク セキュリティ プロファイルで［アプリケーションレベル認証を有効化（Enable Application Level Authorization）］チェックボックスをオンにした場合は、［アプリケーション ユーザの設定（Application User Configuration）］ウィンドウの許可チェックボックスをオンにして、許可する SIP 要求を設定します。	• SIP トランク セキュリティ プロファイルの設定（P.14-4） • 『*Cisco Unified CallManager アドミニストレーション ガイド*』のアプリケーション ユーザの許可の箇所も参照
ステップ 20	クラスタ内のすべての電話機をリセットします。	デバイスのリセット、サービスの再起動、またはサーバおよびクラスタのリブート（P.1-11）
ステップ 21	クラスタ内のすべてのサーバをリブートします。	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.1-11）

セキュア クラスタへのサブスクライバ ノードの追加

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

手順

ステップ 1　新規ノードで Cisco CTL Provider サービスをアクティブにします。

ステップ 2　既存の CTL ファイルの etoken を使用し、CTL クライアントを再実行してクラスタ内のすべてのサーバから証明書を取得し、CTL ファイルに格納します。証明書を生成して CTL ファイルを更新するには、クラスタ内のすべてのサーバで Cisco CTL Provider を実行する必要があります。

ステップ 3　すべての TFTP サーバで Tftp サービスを再起動します。

ステップ 4　すべてのノードで Cisco CallManager サービスを再起動します。

ステップ 5　すべてのデバイスをリセットして、新規 CTL ファイルをデバイスに配布します。

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

その他の情報

シスコの関連マニュアル

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

- *Cisco Unified IP Phone アドミニストレーション ガイド for Cisco Unified CallManager*
- *Cisco Unified Communications Operating System アドミニストレーション ガイド*
- *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*
- *Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity 4.x*
- SRST 対応ゲートウェイをサポートする Cisco Unified Survivable Remote Site Telephony（SRST）の管理マニュアル
- *Cisco IP Telephony Disaster Recovery Framework Administration Guide*
- *Cisco Unified CallManager アドミニストレーション ガイド*
- *Cisco Unified CallManager トラブルシューティング ガイド*
- ご使用の電話機モデルをサポートしているファームウェア リリース ノート