CHAPTER 1

セキュリティの概要

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

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

用語

表 1-1 に示す定義は、Cisco IP テレフォニー ネットワークで認証、暗号化、および他のセキュリティ機能を設定する場合に適用されます。

表 1-1　用語

用語	定義
アクセス コントロール リスト（ACL）	システムの機能およびリソースにアクセスするためのアクセス権を定義するリスト。メソッド リストを参照。
認証	通信中のエンティティの ID を検証するプロセス。
許可	認証されたユーザ、サービス、またはアプリケーションに、要求されたアクションの実行に必要なアクセス権があるかどうかを指定するプロセス。Cisco Unified Communications Manager では、許可されたユーザに一部のトランク側 SIP 要求を制限するセキュリティ プロセス。
許可ヘッダー	チャレンジに対する SIP ユーザ エージェントの応答。
証明書	証明書の保持者名、公開鍵、およびこの証明書を発行する認証局のデジタル署名が含まれているメッセージ。
Certificate Authority（CA; 認証局）	証明書を発行する信頼されたエンティティ。シスコまたはサードパーティのエンティティなど。
Certificate Authority Proxy Function（CAPF）	サポートされているデバイスが Cisco Unified Communications Manager の管理機能を使用してローカルで有効な証明書を要求できるプロセス。
Certificate Trust List（CTL; 証明書信頼リスト）	CTL クライアントで作成され、Cisco Site Administrator Security Token（セキュリティ トークン）で署名したファイル。電話機が信頼するサーバの証明書リストを含みます。
チャレンジ	ダイジェスト認証において、SIP ユーザ エージェントの ID を認証するための SIP ユーザ エージェントに対する要求。
Cisco Site Administrator Security Token（セキュリティ トークン、etoken）	秘密鍵と、Cisco Certificate Authority の署名する X.509v3 証明書が含まれるポータブル ハードウェア セキュリティ モジュール。ファイルの認証に使用され、CTL ファイルに署名します。
デバイス認証	接続前に、デバイスの ID を検証し、このエンティティが主張内容と一致することを確認するプロセス。
ダイジェスト認証	デバイス認証の形式。（特に）共有パスワードの MD5 ハッシュを使用して、SIP ユーザ エージェントの ID を確認します。
ダイジェスト ユーザ	SIP 電話機または SIP トランクが送信する許可要求に含まれているユーザ名。
デジタル署名	メッセージをハッシュ変換し、その後、署名者が自身の秘密鍵で暗号化して生成される値。メッセージの受信者は署名者の公開鍵でハッシュ変換を行ってこれを復号化します。これによって同じハッシュ関数で別のハッシュ値が生成されます。この 2 つのハッシュを比較してメッセージが一致し、内容が損なわれていないことを確認します。
DSP	Digital signaling processor（デジタル シグナル プロセッサ）。
DSP ファーム	H.323 または MGCP 対応ゲートウェイの DSP で提供される IP テレフォニー会議のネットワーク リソース。

表 1-1　用語（続き）

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

表 1-1　用語（続き）

用語	定義
混合モード	Cisco Unified Communications Manager のセキュリティ モードで、セキュア / 非セキュアのプロファイルを持つデバイスおよび RTP/ SRTP メディアが Cisco Unified Communications Manager に接続できるようにする設定を行います。
ナンス	一意のランダムな数値で、サーバが各ダイジェスト認証要求に対して生成します。MD5 ハッシュを生成するために使用されます。
非セキュア モード	Cisco Unified Communications Manager のセキュリティ モードで、非セキュア プロファイルを持つデバイスおよび RTP メディアが Cisco Unified Communications Manager に接続できるようにする設定を行います。
非セキュア コール	少なくとも 1 台のデバイスが認証も暗号化もされていないコール。
非セキュア デバイス	UDP または TCP 方式のシグナリングと非セキュア メディアを使用するデバイス。
PKI	Public Key Infrastructure（公開鍵インフラストラクチャ）。セキュリティ保護された公開鍵の配布、証明書や認証局など、公開鍵の暗号化に必要な要素のセットで構成されます。
公開鍵 / 秘密鍵	暗号化に使用される鍵。公開鍵は広く一般に流通するが秘密鍵は該当する所有者が保持します。非対称暗号化では、両方の鍵を使用します。
リプレイ アタック	攻撃者が、電話機またはプロキシ サーバを識別する情報をキャプチャし、実際のデバイスを偽装しながら情報を再送するイベント。たとえば、プロキシ サーバの秘密鍵を偽装します。
RTP	Real-Time Transport Protocol（リアルタイム転送プロトコル）。
System Administrator Security Token（SAST）	CTI/JTAPI/TAPI アプリケーションでは、CTL ダウンロード用の CTL ファイルへの署名に使用するトークン。
Simple Certificate Enrollment Protocol（SCEP）	X.509 証明書を発行する認証局との通信に使用されるプロトコル。
セキュア コール	すべてのデバイスが認証され、シグナリングとメディア（ボイス ストリーム）が暗号化されているコール。
シグナリング認証	転送中にシグナリング パケットが改ざんされていないことを検証する TLS プロセス。
シグナリング暗号化	デバイスと Cisco Unified Communications Manager サーバの間で送信されるすべてのシグナリング メッセージの機密保持を行うために、暗号化手法を使用するプロセス。
SIP レルム	Cisco Unified Communications Manager がチャレンジに応答するために使用する文字列（名前）。
SRTP	ネットワークでの音声会話のセキュリティを確保し、リプレイ アタックからの保護を提供するセキュアなリアルタイム転送プロトコル。
SSL	データ通信（インターネットでの電子メールなど）のセキュリティを確保する暗号化プロトコル。後継の TLS と同等の機能を持ちます。
Transport Layer Security（TLS）	データ通信（インターネットでの電子メールなど）のセキュリティを確保する暗号化プロトコル。機能的には SSL と同等です。
信頼リスト	デジタル署名なしの証明書リスト。

表 1-1　用語（続き）

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

システム要件

認証および暗号化には、次のシステム要件があります。

- Cisco Unified Communications Manager Release 6.0 は、このマニュアルで示すセキュリティ機能の最小要件として機能します。
- Cisco CTL クライアントで使用するユーザ名およびパスワード（Cisco Unified Communications Manager サーバへのログインに使用）は、Cisco Unified Communications Manager の管理ページのユーザ名およびパスワード（Cisco Unified Communications Manager の管理ページへのログインに使用するユーザ名およびパスワード）と一致する必要があります。
- LSC は、Cisco Unified Communications Manager との TLS 接続の認証用のすべての電話機にインストールされています。Certificate Authority Proxy Function（CAPF）については、P.6-4 の「CAPF システムの相互作用および要件」を参照してください。

機能一覧

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

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

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

表 1-2　SCCP コールのセキュリティ機能

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

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

表 1-3　SIP コールのセキュリティ機能

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

セキュリティ アイコン

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

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

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

会議コールおよび割り込みコールでは、セキュリティ アイコンは会議のセキュリティ ステータスを表示します。詳細については、P.10-4 の「セキュアな会議のアイコン」を参照してください。

相互作用および制限

この項では、次のトピックについて取り上げます。

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

相互作用

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

プレゼンス

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

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

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

SIP トランク

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

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

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

エクステンション モビリティ

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

CTI

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

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

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

制限

次の項で、シスコのセキュリティ機能に適用される制限について説明します。

トランクのサポート

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

認証と暗号化

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

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

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

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

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

- SRTP は、音声パケットのみを暗号化します。

割り込みと暗号化

割り込みと暗号化には、次の制限が適用されます。

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

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

ワイドバンド コーデックと暗号化

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

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

メディア リソースと暗号化

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

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

電話機のサポートと暗号化

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

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

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

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

電話機のサポートおよび暗号化された設定ファイル

暗号化された設定ファイルをサポートしない電話機もあります。また、暗号化された設定ファイルはサポートするが、署名の検証をサポートしない電話機もあります。Cisco Unified IP Phone 7905 および 7912 を除き、暗号化された設定ファイルをサポートする電話機にはすべて、完全に暗号化された設定ファイルを受信するために、Cisco Unified Communications Manager リリース 5.0 以降と互換性のあるファームウェアが必要です。Cisco Unified IP Phone 7905 および 7912 は、既存のセキュリティ メカニズムを使用します。このメカニズムはこの機能のために新しいファームウェアを必要としません。暗号化された設定ファイルの電話機でのサポートについては、P.7-5 の「サポートされる電話機のモデル」を参照してください。

SIP トランクのサポートと暗号化

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

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

セキュリティ アイコンと暗号化

セキュリティ アイコンと暗号化には、次の制限が適用されます。

- コールの転送またはコールの保留などのタスクを実行するときに、暗号化ロック アイコンが電話機に表示されないことがあります。MOH など、こうしたタスクに関連付けられたメディア ストリームが暗号化されていない場合、ステータスは暗号化済みから非セキュアに変化します。
- Cisco Unified Communications Manager は、SIP トランク側接続で開始または終了するコールに対してはロック アイコンを表示しません。

- Cisco Unified Communications Manager は、H.323 トランクで転送されるコールに対してはシールド アイコンを表示しません。
- PSTN に関連するコールの場合、セキュリティ アイコンで表示されるセキュリティ ステータスはコールの IP ドメイン部分についてのみです。

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

クラスタおよびデバイス セキュリティ モード

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

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

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

ダイジェスト認証と暗号化

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

パケット キャプチャと暗号化

SRTP 暗号化が実装されている場合、サードパーティのスニファは動作しません。適切な認証で許可された管理者は、Cisco Unified Communications Manager の管理ページで設定を変更してパケット キャプチャを開始できます（パケット キャプチャをサポートするデバイスの場合）。Cisco Unified Communications Manager でのパケット キャプチャの設定については、今回のリリースをサポートする『*Cisco Unified Communications Manager トラブルシューティング ガイド*』を参照してください。

ベスト プラクティス

シスコでは、次のベスト プラクティスを強く推奨します。

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

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

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

この項では、次のトピックについて取り上げます。

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

デバイスのリセット、サービスの再起動またはリブート

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

次のガイドラインを考慮します。

- Cisco Unified Communications Manager の管理ページで別のセキュリティ プロファイルを適用した後、1 台のデバイスをリセットする。
- 電話機のセキュリティ強化作業を実行した場合は、デバイスをリセットする。
- クラスタ セキュリティ モードを混合モードから非セキュア モード（またはその逆）に変更した後は、デバイスをリセットする。
- Cisco CTL クライアントの設定後、または CTL ファイルの更新後は、すべてのデバイスを再起動する。
- CAPF エンタープライズ パラメータを更新した後は、デバイスをリセットする。
- TLS 接続用のポートを更新した後は、Cisco CTL Provider サービスを再起動する。
- クラスタ セキュリティ モードを混合モードから非セキュア モード（またはその逆）に変更した後は、Cisco CallManager サービスを再起動する。
- Cisco Certificate Authority Proxy Function サービスに関連する CAPF サービス パラメータを更新した後は、このサービスを再起動する。
- Cisco CTL クライアントの設定後、または CTL ファイルの更新後は、Cisco Unified Serviceability で Cisco CallManager および Cisco TFTP サービスをすべて再起動する。この作業は、これらのサービスが稼働するすべてのサーバで実行します。
- CTL Provider サービスを開始または停止した後は、すべての Cisco CallManager および Cisco TFTP サービスを再起動する。
- SRST リファレンスのセキュリティ設定後は、従属デバイスをリセットする。
- Smart Card サービスを「開始」および「自動」に設定した場合は、Cisco CTL クライアントをインストールした PC をリブートする。

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

Cisco CallManager サービスの再起動については、『*Cisco Unified Communications Manager Serviceability アドミニストレーション ガイド*』を参照してください。

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

メディア暗号化の設定と割り込み

P.1-10 の「割り込みと暗号化」に加えて、次の情報も参照してください。

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

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

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

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

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

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

インストール

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

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

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

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

証明書

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

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

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

Cisco Unified Communications Manager 信頼ストアの更新と証明書の管理の詳細については、今回のリリースの Cisco Unified Communications Manager をサポートする『*Cisco Unified Communications Operating System アドミニストレーション ガイド*』を参照してください。

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

この項では、次のトピックについて取り上げます。

電話機の証明書の種類

シスコでは次の種類の証明書を電話機で使用します。

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

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

CAPF 信頼ストアに格納されている MIC ルート証明書は、証明書のアップグレードに使用されます。Cisco Unified Communications Manager 信頼ストアの更新と証明書の管理の詳細については、今回のリリースをサポートする『*Cisco Unified Communications Operating System アドミニストレーション ガイド*』を参照してください。

サーバの証明書の種類

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

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

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

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

  証明書名は、ボイスメール サーバ名に基づく証明書の件名のハッシュを表しています。すべてのデバイス（またはポート）が、ルート証明書をルートとする証明書を発行します。
- SIP Proxy サーバ証明書 : Cisco Unified Communications Manager 信頼ストアに SIP ユーザ エージェント証明書が含まれ、SIP ユーザ エージェントの信頼ストアに Cisco Unified Communications Manager 証明書が含まれている場合、SIP トランク経由で接続する SIP ユーザ エージェントは、Cisco Unified Communications Manager に対して認証されます。

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

外部 CA からの証明書のサポート

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

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

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

サードパーティの CA 署名付き証明書をプラットフォームにアップロードした後、CTL クライアントを実行して、CTL ファイルを更新してください。CTL クライアントを実行した後、該当するサービスを再起動して更新します。たとえば、Cisco Unified Communications Manager 証明書を更新する場合は Cisco CallManager と Cisco Tftp を再起動し、CAPF 証明書を更新する場合は CAPF を再起動します。更新の手順については、P.3-1 の「Cisco CTL クライアントの設定」を参照してください。

プラットフォームでの証明書署名要求（CSR）の生成の詳細については、今回のリリースの Cisco Unified Communications Manager をサポートする『*Cisco Unified Communications Operating System アドミニストレーション ガイド*』を参照してください。

認証、整合性、および許可の概要

整合性および認証によって、次の脅威から保護します。

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

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

認証、整合性、および許可の詳細については、次の項を参照してください。

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

イメージ認証

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

デバイス認証

このプロセスでは、通信デバイスの ID を検証し、このエンティティが主張内容と一致することを確認します。サポートされるデバイスのリストについては、P.4-2 の「サポートされる電話機のモデル」を参照してください。

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

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

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

ファイル認証

このプロセスでは、電話機でダウンロードするデジタル署名されたファイルを検証します。たとえば、設定、呼出音一覧、ロケール、CTL ファイルなどがあります。電話機は署名を検証して、ファイルが作成後に改ざんされていないことを確認します。サポートされるデバイスのリストについては、P.4-2 の「サポートされる電話機のモデル」を参照してください。

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

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

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

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

（注）　クラスタのセキュリティ モードは、ダイジェスト認証に影響しません。

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

ユーザは Cisco Unified Communications Manager データベースに電話機ユーザまたはアプリケーションユーザの SIP ダイジェスト クレデンシャルを設定します。

- アプリケーションの場合は、［アプリケーションユーザの設定 (Application User Configuration)］ウィンドウでダイジェスト クレデンシャルを指定します。
- SIP 電話機の場合は、［エンドユーザの設定 (End User Configuration)］ウィンドウで、ダイジェスト認証の証明書を指定し、電話機に適用します。ユーザを設定した後でクレデンシャルを電話機に関連付けるには、［電話の設定 (Phone Configuration)］ウィンドウで［ダイジェストユーザ (Digest User)］（エンド ユーザ）を選択します。電話機をリセットした後、クレデンシャルは、TFTP サーバが電話機に提供する電話機設定ファイルに存在するようになります。ダイジェスト クレデンシャルが TFTP ダウンロードで暗号化されずに送信されることがないようにする詳細については、「暗号化された電話機設定ファイルの設定」を参照してください。
- ユーザは、チャレンジを SIP トランク上で受信するための SIP レルムを設定します。SIP レルムには、レルム、ユーザ名（デバイスまたはアプリケーション ユーザ）およびダイジェスト クレデンシャルが含まれます。

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

Cisco Unified Communications Manager は、ヘッダーにナンスとレルムを含む 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。ユーザは、SIP デバイスのセキュリティ プロファイルで電話機またはトランクのナンス確認時間を設定します。ナンス確認時間は、外部のデバイスに対してナンス値が有効な時間数を分数で指定するもので、この時間を超えると Cisco Unified Communications Manager は外部デバイスを拒否して新しい番号を生成します。

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

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

電話機のダイジェスト認証

電話機に対してダイジェスト認証が有効になっている場合、Cisco Unified Communications Manager は、キープアライブ メッセージ以外のすべての SIP 電話機要求でチャレンジを行います。Cisco Unified Communications Manager は回線側の電話機からのチャレンジには応答しません。

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

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

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

トランクのダイジェスト認証

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

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

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

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

許可

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

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

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

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

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

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

暗号化の概要

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

Cisco Unified Communications Manager は、次の種類の暗号化をサポートします。

- シグナリング暗号化（P.1-23）
- メディア暗号化（P.1-23）
- 設定ファイルの暗号化（P.1-25）

シグナリング暗号化

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

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

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

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

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

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

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

メディア暗号化

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

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

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

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

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

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

次の例で、SCCP および MGCP コールのメディア暗号化を示します。

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

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

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

設定ファイルの暗号化

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

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

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

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

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

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

詳細については、P.7-2 の「電話機設定ファイルの暗号化について」を参照してください。

設定用チェックリストの概要

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

表 1-4　認証および暗号化の設定用チェックリスト

設定手順		関連手順および関連項目
ステップ 1	Cisco Unified Serviceability で Cisco CTL Provider サービスをアクティブにします。	Cisco CTL Provider サービスのアクティブ化（P.3-5）
ステップ 2	Cisco Unified Serviceability で Cisco Certificate Authority Proxy サービスをアクティブにし、ローカルで有効な証明書のインストール、アップグレード、トラブルシューティング、または削除を行います。 **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。	TLS 接続用ポートの設定（P.3-6）
ステップ 4	Cisco CTL クライアント用に設定するサーバについて、少なくとも 2 つのセキュリティ トークンとパスワード、ホスト名または IP アドレス、およびポート番号を入手します。	Cisco CTL クライアントの設定（P.3-10）
ステップ 5	Cisco CTL クライアントをインストールします。	• システム要件（P.1-5） • インストール（P.1-14） • Cisco CTL クライアントのインストール（P.3-8） • Cisco CTL クライアントの設定（P.3-10）
ステップ 6	Cisco CTL クライアントを設定します。	• Cisco CTL クライアントの設定（P.3-10） • Cisco CTL クライアントの設定（P.3-10）

表 1-4　認証および暗号化の設定用チェックリスト（続き）

設定手順		関連手順および関連項目
ステップ 7	電話機のセキュリティ プロファイルを設定します。プロファイルを設定するときは、次の作業を実行します。 • デバイスのセキュリティ モードを設定します。 • CAPF 設定を定義します（一部の SCCP 電話機および SIP 電話機の場合）。 追加の CAPF 設定が［電話の設定 (Phone Configuration)］ウィンドウに表示されます。 • SIP 電話機でダイジェスト認証を使用する場合は、［ダイジェスト認証を有効化 (Enable Digest Authentication)］チェックボックスをオンにします。 • 暗号化された設定ファイルを有効にするには（一部の SCCP 電話機および SIP 電話機）、［TFTP 暗号化 (TFTP Encrypted Config)］チェックボックスをオンにします。 • 設定ファイルのダウンロードでダイジェスト クレデンシャルを除外するには、［設定ファイル内のダイジェスト信用証明書を除外 (Exclude Digest Credentials in Configuration File)］チェックボックスをオンにします。	電話機セキュリティ プロファイルの設定（P.5-4） 電話機セキュリティ プロファイルの設定のヒント（P.5-2） 暗号化された電話機設定ファイルの設定（P.7-1） 暗号化された設定ファイルの設定のヒント（P.7-6）
ステップ 8	電話機に電話機セキュリティ プロファイルを適用します。	電話機セキュリティ プロファイルの適用（P.5-12）
ステップ 9	電話機に証明書を発行するように CAPF を設定します。	• システム要件（P.1-5） • CAPF の設定用チェックリスト（P.6-5）
ステップ 10	サポートされている Cisco Unified IP Phone にローカルで有効な証明書がインストールされたことを確認します。	• システム要件（P.1-5） • 電話機での認証文字列の入力（P.6-12）
ステップ 11	SIP 電話機のダイジェスト認証を設定します。	• 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。	• 電話機のセキュリティ強化（P.9-1）
ステップ 13	セキュリティ用の会議ブリッジを設定します。	• セキュアな会議リソースの設定（P.10-1）
ステップ 14	セキュリティ用のボイスメール ポートを設定します。	• ボイスメール ポートのセキュリティ設定（P.11-1） • 今回のリリースの Cisco Unified Communications Manager に該当する Cisco Unity または Cisco Unity Connection のインテグレーション ガイド
ステップ 15	SRST リファレンスのセキュリティを設定します。	• Survivable Remote Site Telephony（SRST）リファレンスのセキュリティ設定（P.13-1）
ステップ 16	IPSec を設定します。	• ゲートウェイおよびトランクの暗号化の設定（P.14-1） • ネットワーク インフラストラクチャで IPSec を設定する場合の注意事項（P.14-6） • *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways* • *Cisco Unified Communications Operating System アドミニストレーション ガイド*

表 1-4　認証および暗号化の設定用チェックリスト（続き）

設定手順		関連手順および関連項目
ステップ 17	（注）　この手順はクラスタ間環境にのみ適用されます。Cisco Unified Communications Manager Business Edition システムでは Intercluster Trunk（ICT; クラスタ間トランク）はサポートされていません。 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.15-1） • ダイジェスト認証のエンタープライズ パラメータの設定（P.16-2）
ステップ 18	（注）　この手順はクラスタ間環境にのみ適用されます。Cisco Unified Communications Manager Business Edition システムでは Intercluster Trunk（ICT; クラスタ間トランク）はサポートされていません。 SIP トランク セキュリティ プロファイルをトランクに適用します。	• SIP トランク セキュリティ プロファイルの適用（P.15-10）
ステップ 19	（注）　この手順はクラスタ間環境にのみ適用されます。Cisco Unified Communications Manager Business Edition システムでは Intercluster Trunk（ICT; クラスタ間トランク）はサポートされていません。 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.16-1）
ステップ 20	（注）　この手順はクラスタ間環境にのみ適用されます。Cisco Unified Communications Manager Business Edition システムでは Intercluster Trunk（ICT; クラスタ間トランク）はサポートされていません。 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.15-1） • 許可（P.1-22）

表 1-4　認証および暗号化の設定用チェックリスト（続き）

設定手順		関連手順および関連項目
ステップ 21	すべての電話機をリセットします。	デバイスのリセット、サービスの再起動またはリブート（P.1-13）
ステップ 22	すべてのサーバをリブートします。	デバイスのリセット、サービスの再起動またはリブート（P.1-13）

その他の情報

シスコの関連マニュアル

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

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