セキュリティー

改訂日：2019 年 2 月 19 日

この章では、企業のコラボレーション向けシスコ プリファード アーキテクチャ（PA）のネットワーク アクセス セキュリティ、電話料金の詐欺行為に関するアクセス保護、証明書の管理、および暗号化について説明します。

この章の前半ではアーキテクチャの概要を示し、後半では導入手順を説明します。「アーキテクチャー」では、セキュリティのさまざまな側面について説明します。最初に、階層型セキュリティ アプローチ、不正アクセスからの保護、電話料金の詐欺行為からの保護について概説します。その後、証明書の管理と暗号化について説明します。次の項は「展開」です。この項では、証明書を生成および管理する手順と、このソリューションのすべてのコンポーネントに対して暗号化を有効化およびプロビジョニングする手順について説明します。

注　この章の情報は、製品がソフトウェアバージョン 12.5 以降を実行していることを前提としています。

この章の新規情報とは

C：表 7-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

C：表 7-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
ローカルで有効な証明書（LSC）のインスタレーション	この章の各項で説明	2019 年 1 月 23 日
ローカルで有効な証明書（LSC）をインストールするための Jabber 用の SIP OAuth モードと要件の削除	この章の各項で説明	2019 年 1 月 23 日
Cisco Meeting Management	この章の各項で説明	2019 年 1 月 23 日
CAPF オンライン CA モード	CAPF オンライン CA モード（C：7-41 ページ）	2019 年 1 月 23 日
CE エンドポイントでの MIC のサポート	この章の各項で説明	2019 年 1 月 23 日

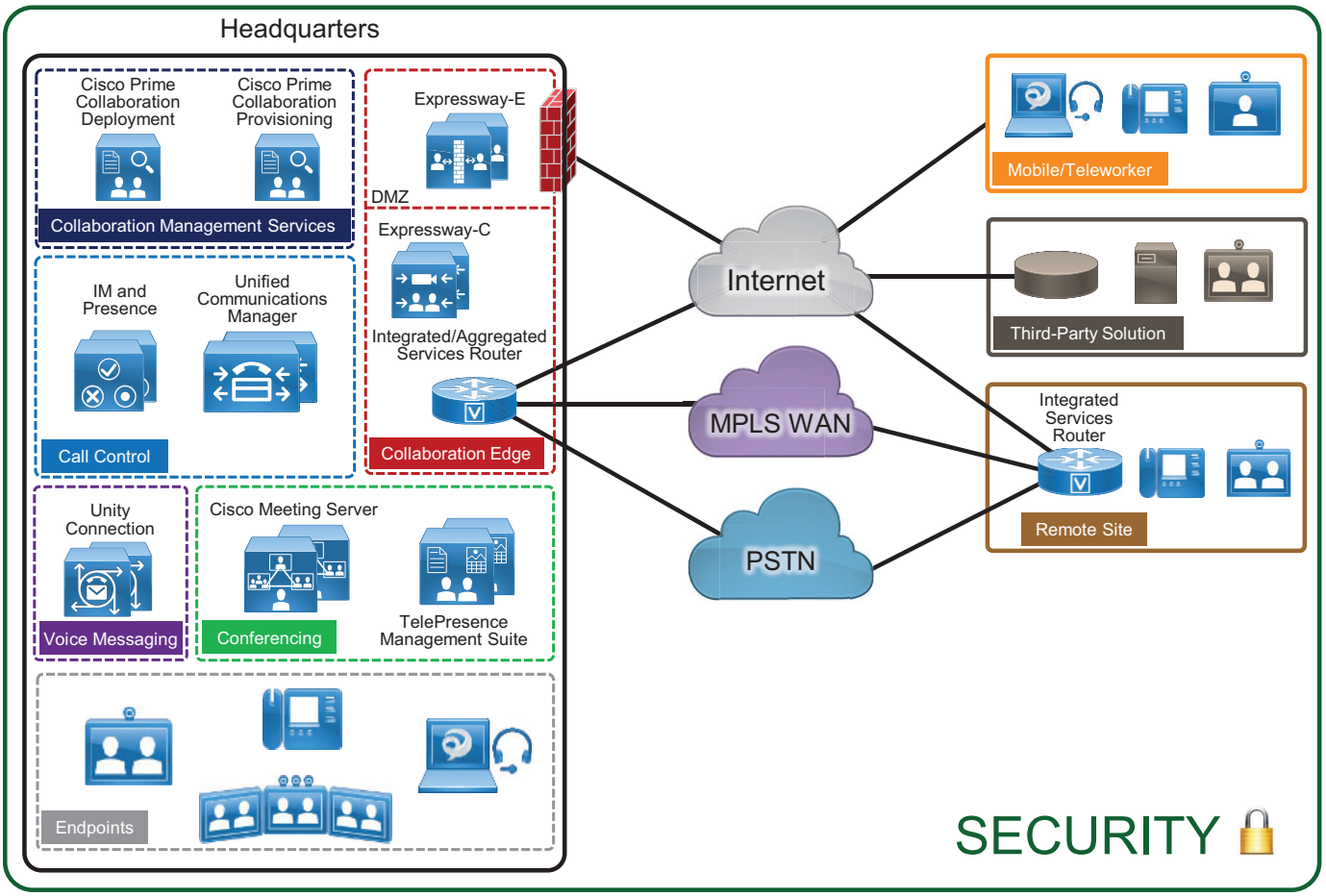
C：表 7-1 新規情報、またはこのマニュアルの以前のリリースからの変更情報（続き）

新規トピックまたは改訂されたトピック	説明箇所	改訂日
Cisco Prime License Manager はこのアーキテクチャから除外されたため、この章から削除されました。	この章のすべての項	2017 年 8 月 30 日
初期信頼リスト（ITL）とトークンレス型証明書信頼リスト（CTL）	この章の各項で説明	2017 年 8 月 30 日

コア コンポーネント

Cisco Collaboration ソリューションのすべてのコンポーネントにセキュリティが適用されます（C：図 7-1 を参照）。ソリューション全体でセキュリティを実装することが重要です。実際には、階層型アプローチでセキュリティを実装することが重要です。1 つのコンポーネントに頼ってセキュリティを提供するのではなく、多層型防御を計画します。

C：図 7-1 企業のコラボレーション向けプリファード アーキテクチャのすべてのコンポーネントのセキュリティ保護



主なメリット

この展開には次の利点があります。

- 階層型アプローチを導入することで、多層型防御が実現します。
- ネットワークとシステムへのアクセスを保護することで、サーバ、コラボレーション ソリューション、組織のその他の部分への侵害が困難になります。
- 電話料金の詐欺行為からの保護メカニズムを導入することで、不正請求の原因となるテレフォニー システム、データ ネットワーク、および PSTN 回線への不正アクセスを防止できます。
- さまざまな通信で暗号化と証明書を使用することで、盗聴、改ざん、セッション リプレイからの保護を実現できます。
- 適切な証明書管理計画を実施することで、適切なレベルの保護を実現し、かつ複雑さを軽減できます。

アーキテクチャー

はじめに、Cisco Collaboration のセキュリティ メカニズムの概要について説明します。次に、電話料金の詐欺行為の緩和と、証明書の管理および暗号化について説明します。

レイヤ化したセキュリティー

さまざまな脅威が存在し、これらの脅威に対処できるさまざまなメカニズムがあります。一般的なベスト プラクティスとして、コラボレーション導入を保護する多層セキュリティ アプローチを使用します。施設への物理アクセスと、ネットワーク、サーバ、エンドポイント、およびシステムへのアクセスを保護し、安全にする必要があります。通信を暗号化し、適切な証明書管理システムを導入する必要があります。可能な限り多くのコンポーネントおよび層を保護することでセキュリティが強化されます。特定の層またはコンポーネントが侵害を受けても、他のセキュリティ層およびセキュリティ メカニズムによりシステムは引き続き保護されます。

C：表 7-2 に、コラボレーションにおける脅威と対策の例を示します。それぞれの脅威に対して複数の対策を導入してください。

C：表 7-2　　コラボレーションの脅威とその対策の例

脅威	対策
サービス拒否（DoS）	物理的セキュリティ、ネットワーク セキュリティ、ファイアウォールおよび侵入防御システム（IPS）、QoS
スパムおよびインターネット テレフォニーでのスパム	ファイアウォールおよび高度なマルウェア防御（AMP）、Cisco Collaboration エッジ セキュリティ、Cisco Unified Communications Manager（Unified CM）ダイヤルプラン
ウイルス	ホストベースのファイアウォール、IPS、ウイルス対策ソフトウェア
電話料金の詐欺行為	Cisco Unified CM コーリング サーチ スペース（CSS）およびパーティション、電話料金の詐欺行為の防止およびアクセス保護、Cisco Collaboration エッジ セキュリティ

C：表 7-2　コラボレーションの脅威とその対策の例（続き）

脅威	対策
個人情報の入手	証明書管理を使用した暗号化、物理的セキュリティ、ネットワーク セキュリティ
中間者攻撃	証明書管理を使用した暗号化、物理的セキュリティ、ネットワーク セキュリティ
盗聴	証明書管理を使用した暗号化、物理的セキュリティ、ネットワーク セキュリティ
なりすまし	証明書管理を使用した暗号化、物理的セキュリティ、ネットワーク セキュリティ
メディア改ざん	証明書管理を使用した暗号化、物理的セキュリティ、ネットワーク セキュリティ
データ変更	証明書管理を使用した暗号化、物理的セキュリティ、ネットワーク セキュリティ
セッション リプレイ	証明書管理を使用した暗号化、物理的セキュリティ、ネットワーク セキュリティ

物理的なセキュリティー

最初の防御策は、物理的なセキュリティです。施設、ネットワーク アクセス、あるいはさらに重要なコア ネットワークインフラストラクチャおよびサーバに対する物理的セキュリティを導入することが重要です。物理的セキュリティが侵害されると、施設やサーバへの電源遮断によるサービスの中断などの単純な攻撃が可能になります。物理的にアクセスできるようになった攻撃者は、サーバ デバイスにアクセスし、パスワードをリセットしてサーバへのアクセスを可能にします。物理的にアクセスできることで、中間者攻撃などの高度な攻撃も可能になるため、2 番目のセキュリティ層であるネットワーク セキュリティが重要になります。

全般的なセキュリティ プラクティスの詳細については、次の Web サイトで入手可能なマニュアルを参照してください。

https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/index.html

https://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html

ネットワーク セキュリティー

次の防御策はネットワーク セキュリティです。次の項では、いくつかのネットワーク セキュリティ メカニズムの例を紹介します。この項では、ネットワーク セキュリティについて簡単に説明します。このガイドの展開では、ネットワーク セキュリティについては説明しません。ネットワーク セキュリティの詳細については、次のリンク先にあるネットワーク セキュリティ設計ガイドを参照してください。

https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/index.html

音声 / ビデオ VLAN

次の理由により、音声 / ビデオ VLAN とデータ VLAN を分離することを推奨します。

- 悪質なネットワーク攻撃からの保護

  VLAN アクセス コントロール、802.1Q、および 802.1p タギングを使用すると、音声デバイスを悪質な内部および外部ネットワーク攻撃から保護できます。このような攻撃には、ワーム、サービス拒絶（DoS）攻撃、データ デバイスがパケット タギングによってプライオリティ キューにアクセスする攻撃などがあります。

- 管理および設定の容易性

  アクセス レイヤで音声とデータの VLAN を分離すると、管理が容易になり、QoS 設定が簡素化されます。

音声 / ビデオ VLAN には、卓上電話（ハードウェア）とビデオ システムが含まれます。データ VLAN には、エンドユーザのデスクトップおよびラップトップ、Jabber などのソフトウェア クライアントが含まれます。アクセス リスト（ACL）、VLAN アクセス リスト（VACL）、またはファイアウォールを使用して、VLAN 間のトラフィックを制限できます。

ワイヤレス アクセスの場合は、追加の考慮事項があります。詳細については、https://www.cisco.com/go/ucsrnd から入手可能な『*Real-Time Traffic over Wireless LAN Solution Reference Network Design Guide*』および『*Cisco Collaboration System Solution Reference Network Design (SRND)*』を参照してください。

レイヤ 2 およびレイヤ 3 セキュリティ

レイヤ 2 およびレイヤ 3 で使用可能な標準セキュリティ機能を使用します。

ポート セキュリティ

スイッチ ネットワークに対する典型的な攻撃は、MAC 連想メモリ（CAM）フラッディング攻撃です。このタイプの攻撃では、スイッチに対して大量の MAC アドレスによるフラッディングが実行されることで、スイッチは、エンド ステーションまたはデバイスが接続されているポートを判別できなくなります。デバイスが接続されているポートを判別できない場合、スイッチは、そのデバイスが宛先になっているトラフィックを VLAN 全体にブロードキャストします。これにより、攻撃者は、VLAN 内のすべてのユーザに到達するすべてのトラフィックを見ることができます。MAC フラッディング攻撃を抑制するには、ポート セキュリティまたはダイナミック ポート セキュリティのいずれかを使用できます。承認メカニズムとしてポート セキュリティを使用する必要がない場合、特定のポートに接続する機器分の MAC アドレスの数を設定するダイナミック ポート セキュリティを使用できます。たとえば、1 台のワークステーションが接続されているポートの場合、取得する MAC アドレスの数を 1 に制限できます。1 台の Cisco Unified IP Phone と、その背後に 1 台のワークステーションが接続されているポートの場合、電話機の PC ポートに 1 台のワークステーションを接続するには、取得する MAC アドレスの数を 2 に設定できます（1 つは IP Phone 用、1 つは電話機の背後にあるワークステーション用）。ポート セキュリティでは、エンドポイントの MAC アドレスを確認する一種のデバイスレベル セキュリティ認証も実現します。

DHCP スヌーピング

Dynamic Host Configuration Protocol（DHCP）スヌーピングは、承認されていない DHCP または不正な DHCP サーバがネットワーク上で IP アドレスを配布するのを防止します。具体的には、信頼されていないポートからの DHCP 要求へのすべての応答をブロックします。電話機を設置する際に、そのほとんどが DHCP を使用して複数の電話機に IP アドレスを配布しており、スイッチで DHCP スヌーピング機能を使用し DHCP メッセージングを保護する必要があります。DHCP スヌーピングでは、DHCP サービス妨害（DoS）攻撃に使用される DHCP アドレス範囲枯渇攻撃からの保護も促進されます。DHCP スヌーピングを有効にすると、信頼されていない

ポートで、送信元 MAC アドレスと DHCP ペイロード情報が比較され、それらが一致しない場合は要求が失敗します。DHCP スヌーピングにより、任意の単一デバイスが特定範囲内のすべての IP アドレスをキャプチャすることを防止できますが、この機能が正しく設定されていないと、認定ユーザの IP アドレスが拒否される場合があります。

ダイナミック ARP インスペクション

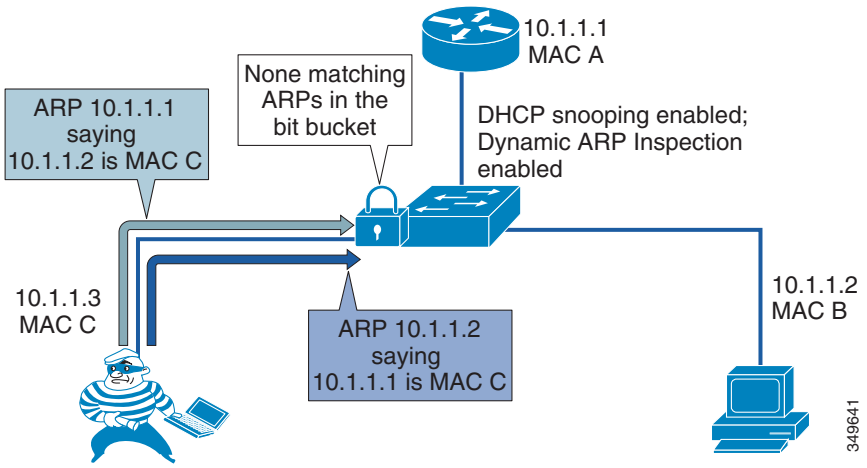
ダイナミック アドレス解決プロトコル（ARP）インスペクション（DAI）は、ルータのスイッチに接続されたデバイスに対する Gratuitous ARP 攻撃を防止するために、スイッチで使用される機能です。

Gratuitous ARP（GARP）は、要求がなくても送信される ARP 応答です。通常の使用法では、MAC ブロードキャストとして送信されます。GARP メッセージを受信する、LAN セグメント上のすべてのステーションは、この非請求 ARP 応答をキャッシュに入れます。この非請求 ARP 応答により、送信者が、GARP メッセージに含まれる IP アドレスのオーナーであることが認定されます。Gratuitous ARP には、障害時に別のステーションのアドレスを引き継ぐ必要があるステーションを正当に使用します。ただし、Gratuitous ARP は、別のステーションの身分を不正にかたること目的とした悪質なプログラムにより悪用される可能性もあります。悪質なステーションが、相互に通信しているその他の 2 つのステーションのトラフィックを自らにリダイレクトすると、GARP メッセージを送信したハッカーが中間者になります。

ダイナミック ARP インスペクション（DAI）は、信頼されていない（またはユーザ報告の）ポートからのすべての ARP 要求および応答（Gratuitous または非 Gratuitous）を検査して、それらが ARP オーナーからのものであることを確認するために使用します。ARP オーナーとは、ARP 応答に含まれている IP アドレスに一致する、DHCP バインディングが置かれているポートのことです。DAI 信頼済みポートからの ARP パケットは検査されず、それぞれの VLAN にブリッジされます。

ダイナミック ARP インスペクション（DAI）では、ARP 応答または Gratuitous ARP メッセージを正当化するために、DHCP バインディングが存在している必要があります。ホストで、アドレスを取得するための DHCP が使用されていない場合、そのホストを信頼するか、ホストの IP アドレスと MAC アドレスを対応付けるために ARP インスペクション用のアクセス コントロール リスト（ACL）を作成する必要があります（C：図 7-2 を参照）。DHCP スヌーピングと同様に、DAI は VLAN ごとに有効化されます。すべてのポートは、デフォルトで、信頼できないポートとして定義されます。DAI で DHCP スヌーピングからのバインディング情報を活用するには、DAI を有効化する前に、VLAN で DHCP スヌーピングを有効化する必要があります。

C：図 7-2　　DHCP スヌーピングおよび DAI を使用した ARP 攻撃の防止



IP ソース ガード

IP ソース ガードは、レイヤ 2 ポートで送信元 IP アドレス フィルタリングを提供して、悪意のあるホストが正規のホストの IP アドレスを装うことで正規のホストを偽装することを防ぎます。この機能では、ダイナミックな Dynamic Host Configuration Protocol（DHCP）スヌーピングおよびスタティックな IP ソース バインディングを使用して、IP アドレスと信頼できないレイヤ 2 アクセス ポート上のホストを照合します。

まず、DHCP パケットを除く、保護済みポート上の全 IP トラフィックがブロックされます。クライアントが DHCP サーバから IP アドレスを受信したあと、またスタティック IP ソース バインディングが管理者によって設定されたあと、その IP 送信元アドレスのある全トラフィックがそのクライアントから許可されます。他のホストからのトラフィックは拒否されます。このフィルタリングは、隣接ホストの IP アドレスを要求することによって、ホストのネットワーク攻撃を制限します。IP ソース ガードは、暗黙的なポート アクセス コントロール リスト（PACL）を自動的に作成するポートベースの機能です。

802.1X

802.1X は、エンドユーザまたはデバイスのアイデンティティに基づいてネットワーク接続を許可または拒否する IEEE 規格です。802.1X 認証機能は、シスコ エンドポイントのデバイス クレデンシャルの、ネットワークへのアクセス権を与える前に行う識別と検証に使用できます。802.1X は、エンド デバイスと RADIUS サーバ（Cisco Identity Service Engine（ISE）など）間で機能する MAC レイヤ プロトコルです。このプロトコルは、Extensible Authentication Protocol（EAP）over LAN（EAPOL）をカプセル化し、エンド デバイスとスイッチの間での認証メッセージの転送を行います。802.1X 認証プロセスでは、シスコのエンドポイントが 802.1X サプリカントとして動作し、ネットワーク アクセス要求を開始し、証明書（ローカルで有効な証明書を推奨）を提供します。オーセンティケータとして機能する Cisco Catalyst スイッチは、その要求を認証サーバに渡し、その電話にネットワークへのアクセスを許可するかまたはその電話からのアクセスを制限するかのいずれかを行います。

802.1X は、Cisco Unified IP Phone に接続されているデータ デバイスの認証にも使用できます。Cisco Unified IP Phone では EAPOL パススルー メカニズムが使用され、これによって、ローカルに接続された PC が 802.1X オーセンティケータに EAPOL メッセージを渡すことが可能になります。音声 VLAN 上の 1 つのデバイスとデータ VLAN 上の複数の認証されたデバイスに許可を与えるには、Cisco Catalyst Switch のポートをマルチ認証モードで設定する必要があります。

ファイアウォール、IPS、および AMP

ファイアウォールをアクセス コントロール リスト（ACL）と組み合わせて使用すると、コラボレーション サーバやゲートウェイを、これらとの通信が許可されていないデバイスから保護できます。Cisco 適応型セキュリティ アプライアンス（ASA）と FirePOWER サービスを導入できます。これにより、ASA ファイアウォール機能、次世代侵入防御システム（NGIPS）、マルウェア対策保護（AMP）の組み合わせが実現します。

Cisco Collaboration システムで使用される UDP ポートと TCP ポートの中には、ファイアウォールで開く必要があるものがあります。使用するポートを決定する際には、次のガイドを参照してください。

- Cisco Unified CM および IM と Presence については、次のリンク先にある『*System Configuration Guide for Cisco Unified Communications Manager*』の最新版を参照してください。
  https://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html
- Cisco Unity Connection については、次のリンク先にある『*Security Guide for Cisco Unity Connection*,』の最新版を参照してください。
  https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html

- Cisco Expressway については、次のリンク先にある『*Cisco Expressway IP Port Usage for Firewall Traversal Deployment Guide*』の最新版を参照してください。
  https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html
- Cisco Jabber については、次のリンク先にある『*Planning Guide for Cisco Jabber*』の最新版を参照してください。
  https://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html

QoS

ネットワークにおいてコラボレーション トラフィックが他のトラフィックよりも適切に優先され、ネットワーク フラッド攻撃（DoS 攻撃の一種）から保護されるようにするため、Quality of Service（QoS）を使用できます。QoS 自体はセキュリティ機能ではありませんが、適切に実装することで、適切な QoS レベルが設定されたパケットが優先されるようになります。これは、インターフェイス バッファに圧倒的な負担をかけるためにネットワークにパケットの大量送信を試行するパケット フラッド攻撃に対して有効です。QoS により、マークされていないパケットは削除され、適切にマークされているパケットが許可されるため、バッファが保護されます。

コラボレーション QoS ポリシーの詳細については、帯域幅管理を参照してください。

不正アクセスの防止

Cisco Collaboration ン製品のほとんどでは、プラットフォームが強化されています。たとえば、Cisco Unified CM、IM and Presence Service、および Unity Connection が使用するプラットフォームのロックダウン、root アカウントの無効化、サードパーティ製ソフトウェアのインストール禁止、ホストベースの侵入保護（SELinux）およびホストベースのファイアウォール（iptables）のインストールとデフォルトでの有効化、管理アカウントへの複雑なパスワード ポリシーの適用、セキュア管理インターフェイス（HTTPS、SSH、SFTP）の適用などです。さらに、ユーザをアクセス コントロール グループ、つまり特定のロールに割り当てることができるため、管理者、エンドユーザ、アプリケーション ユーザに対し、それぞれに必要な権限だけを付与できます。すべてのインストール パッケージは署名付きであり、OS とアプリケーションの両方が含まれています。システム監査ロギングを使用できます。このログは、問題発生時の状況を確認する上で重要です。

エッジに導入されるサーバは、インターネットへの露出が高いため、保護する必要があります。Cisco IOS Gateway または Cisco Unified Border Element では、アクセス コントロール リスト（ACL）、IP 信頼リスト、コールしきい値、コール スパイク保護、帯域幅ベースのコール アドミッション制御（CAC）、メディア ポリシング、NBAR ポリシング、音声ポリシーなど、多数のセキュリティ機能を利用できます。Cisco Expressway では、システムを保護するため、Call Processing Language（CPL）ルール、ホストベースのファイアウォール（動的システム ルール、設定不可のアプリケーション ルール、およびユーザが設定可能なルール）、自動侵入保護を設定できます。

エンドポイントの保護は、サーバの保護ほど重要ではないように思われますが、エンドポイントも保護する必要があります。エンド ユーザがエンドポイントにアクセスでき、またエンドポイントはデータ センター内ではロックダウンされていないことから、通常、エンドポイントには簡単にアクセスできます。また、エンドポイントが侵害されると被害が発生する可能性があります。エンドポイントと、エンドポイントが登録されているシステムに関する重要な情報は、電話画面と電話の Web インターフェイスで確認できます。ログをダウンロードできます。Cisco TelePresence エンドポイントなどの一部のエンドポイントには、エンドポイントのコール制御やパケット キャプチャなど、エンドポイント管理者ユーザ向けの高度な機能が多数用意されています。このようなエンドポイントでは、デフォルトのパスワード（空白）をそのままにせずに、強力なパスワードを設定してください。一般に、Web アクセス、Web 管理画面、コン

ソール アクセス、Telnet アクセス、SSH アクセスがエンドポイントで使用可能な場合は、これらを無効にすることが推奨されます。これらの機能は、必要な場合（エンドポイントのトラブルシューティング時など）に限り有効にしてください。管理ステーションや、管理者がアクセスできるステーションへのインターフェイスへのアクセスを制限するため、アクセス コントロール リストを設定してください。エンドポイントで Web アクセスを有効にする場合は、（HTTP ではなく）HTTPS のみを許可します。

Unified CM 管理電話ページの [設定へのアクセス（Settings Access）] パラメータにより、ユーザは [設定（Settings）] ボタンを押すとデバイス設定にアクセスできます。このパラメータが使用可能な場合には、無効にするかまたは [制限（Restricted）] に設定することをお勧めします（管理タスクへのアクセスが無効になります）。エンドポイントと Unified CM 間の信頼関係が失われる可能性のある操作を実行する場合（たとえば Unified CM クラスタ間でエンドポイントを移行し、すべての Unified CM クラスタに 1 つの ITLRecovery 証明書と秘密キーを配布しない場合など）は、[設定へのアクセス（Settings Access ）] を一時的に有効にできます。また、Unified CM 証明書はアップグレード中に変更してはなりませんが、Unified CM のアップグレードのために予防措置として [設定へのアクセス（Settings Access ）] を一時的に有効にすることもできます。エンドポイントと Unified CM 間の信頼関係が失われた場合は、[設定へのアクセス（Settings Access ）] を一時的に有効にすると、ユーザが各自の電話機でメニューに進み、セキュリティ設定をリセットすることで、信頼を回復できます。この操作により、初期信頼リスト（ITL）または証明書信頼リスト（CTL）が削除されます。あるいは、信頼関係が失われた場合には ITL リカバリ キーを使用して回復することもできます（詳細については「CTL および ITL」を参照）。

複雑なパスワードおよび PIN のポリシー（許容可能なログイン失敗回数、ログイン失敗によるアカウントのロックアウト期間、クレデンシャルの最小長など）がデフォルトでまだ適用されていない場合には、すべての Cisco Collaboration 製品で、管理者とユーザに対してこのポリシーが設定されていることを確認してください。

電話料金詐欺行為の削減

Cisco Unified CM

Cisco Unified CM には、電話料金の詐欺行為を防止するためのさまざまなメカニズムがあります。パーティションとコーリング サーチ スペース（CSS）により、コール可能な電話番号、ルート パターン、ディレクトリ URI、および SIP ルート パターン、またはコール発信可能なデバイスや回線へのアクセス制御とセグメンテーションが実現します。ベスト プラクティスは、パーティションとコーリング サーチ スペースに基づき、可能な限り限定的なサービス クラスを適用することです。たとえば、PSTN ゲートウェイと Expressway に接続する SIP トランクの場合は、PSTN ゲートウェイ パーティションへのアクセスを許可しないインバウンド コーリング サーチ スペースを作成します。オフネット間の転送をすべて防止するには、[コール分類（Call Classification）] エンタープライズ パラメータを使用して PSTN ゲートウェイへの SIP トランクを [オフネット（Offnet）] として分類し、[オフネット間転送のブロック（Block OffNet to OffNet Transfer）] CallManager サービス パラメータを [はい（True）] に設定します。時刻のルーティング、強制承認コード（FAC）、[アドホック会議の削除（Drop Ad hoc Conferences）] CallManager サービス パラメータの使用（[会議に OnNet 参加者がいない場合（When No OnNet Parties Remain in the Conference）] に設定）など、その他のメカニズムも使用できます。自動登録が有効な場合は、制限付きコーリング サーチ スペースを使用してデバイス プールを作成します。また、システム コール詳細レコード（CDR）をプロアクティブにモニタリングすることが推奨されます。

Cisco Unity Connection

不正ユーザが Cisco Unity Connection の転送機能を使用して不正なコールを発信する可能性があります。Unity Connection では、主に 2 通りの方法で電話料金の詐欺行為を防止します。

- Unity Connection：規制テーブルにより、着信転送、メッセージ通知、および Unity Connection のその他の機能に使用できる電話番号が制御されます。各サービス クラスにいくつかの規制テーブルが関連付けられており、必要に応じて規制テーブルを追加することもできます。詳細と例については、「ボイス メッセージング」の章を参照してください。
- Unified CM：コーリング サーチ スペースおよびコーリング サーチ スペースの再ルーティングのため、必要なパーティションのみを含めます。「ボイスメールのサービス クラス」の C：表 2-21 を参照してください。

詳細については、次のリンク先にある『*Unified Messaging Guide for Cisco Unity Connection*』の最新版を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html

次のリンク先にある『*Troubleshoot Toll Fraud via Unity Connection*』も参照してください。

https://www.cisco.com/c/en/us/support/docs/unified-communications/unity-connection/119337-technote-cuc-00.html

Cisco Expressway

Expressway の Business-to-Business 導入では、Call Processing Language（CPL）ルールを使用してデフォルト ゾーンからのコールを許可または拒否します。たとえば、（PSTN への不正コールを防止するため）プレフィックスとして 9 を使用する Business-to-Business（B2B）コールをすべて拒否する場合には、C：表 7-3 に示す設定を使用して CPL ルールを作成できます。

C：表 7-3　Business-to-Business（B2B）コールの CPL 設定

ソース タイプ	ゾーン
発信側ゾーン	DefaultZone
宛先パターン	9.*
操作	却下

Cisco IOS Gateway と Cisco Unified Border Element

テレフォニー サービス妨害（TDoS）攻撃緩和機能により、Cisco IOS Gateway と Cisco Unified Border Element が、信頼されない IP アドレスからの Session Initiation Protocol（SIP）要求に応答することが防止されます。これにより、電話料金詐欺行為を防止し、パフォーマンスが向上します。SIP スタックにより、着信 SIP 要求の送信元 IP アドレスが認証され、送信元 IP アドレスが信頼できる IP アドレス リストの IP アドレスに一致しない場合には応答がブロックされます。ダイヤルピア セッション ターゲットまたは音声クラス サーバ グループで設定されている IP アドレスは、信頼される IP アドレスのリストに自動的に追加されます。信頼される IP アドレスを追加するには、**ip address trusted list** コマンドを使用します。

この TDoS 機能を設定するには、次のコマンドを使用します。

```
voice service voip
  ip address trusted authenticate
```

Cisco Unified Border Element がレジストラ サーバとして導入されていない場合は、不要なリソースの消費を防止するためレジストラ サービスを無効にします。

証明書の管理

証明書は、Cisco Collaboration 導入において重要です。証明書により、ネットワーク上の個人ユーザ、コンピュータ、その他のサービスを認証できます。また、セキュアな接続を確立する際には証明書が必要です。適切な証明書管理を実施することで、適切なレベルの保護を実現し、かつ複雑さを軽減できます。

この項では最初に Public Key Infrastructure（PKI）を簡単に説明します。続いて一般的なガイダンスを示します。最後に、さまざまな Cisco Collaboration 製品のアーキテクチャについて詳しく説明します。

PKI の概要

Public Key Infrastructure（PKI）は、通信の安全を確保し、通信する両者の ID を確認するためのメカニズムを提供します。暗号化によって通信が保護され、公開 / 秘密キー ペアとデジタル アイデンティティ証明書を使用して ID が検証されます。

公開 / 秘密キー ペア

公開キーと秘密キーのペアは、数学的に相関付けられた、一意に関連する 2 つの暗号キーで構成されます。公開キーで暗号化されたデータは、対応する秘密キー（一般に公開しないキー）でのみ復号化できます（逆も同様です）。

証明書

デジタル証明書は、ネットワーク上の個人ユーザ、コンピュータ、その他のサービスのアイデンティティを証明する電子クレデンシャルです。これは公開キーのラッパーです。公開キーの所有者に関する情報が含まれています。たとえば、もう一方の側を認証するため TLS ハンドシェイクで使用され、またファイルのデジタル署名に使用されます。Cisco Collaboration 製品とともに導入される証明書は、X.509 標準に基づいています。証明書に含まれている情報には、次のものがあります。

- 公開キー
- 一般名（CN）
- 組織名 (O)
- 発行元名
- 有効期間（それ以前でもそれ以後でもない）
- 拡張（オプション）：サブジェクト代替名（SAN）など

証明書は、自己署名するか、認証局（CA）の署名を受けることができます。

TLS ハンドシェイクでの証明書の検証

クライアントがサーバとの TLS 接続を開始すると、TLS ハンドシェイク中にサーバからその証明書が送信されます。これにより、クライアントはサーバを認証できます。たとえば、管理者またはエンドユーザが Unified CM のページに接続する場合や、Jabber クライアントが起動し Unified CM UDS サーバ、IM and Presence サーバ、Unity Connection サーバに接続する場合などに実行されます。

場合によっては、サーバがクライアントを認証し、クライアントに対して証明書の送信を要求することもあります。これは相互認証（相互 TLS（MTLS））であり、暗号化モード（メディアおよびシグナリング暗号化で設定）での Unified CM と Cisco エンドポイント間、2 つの Unified CM クラスタを接続する SIP トランク、または Unified CM を Unity Connection、Cisco IOS Gateway、または Expressway（TLS 検証が Expressway で設定されている場合）に接続する SIP トランクで使用されます。

証明書を受信すると、検証で次の項目がチェックされます。

- ID — 証明書が発行される対象や ID は、セッションのイニシエータが意図した接続先の ID に一致しなければなりません。ホスト名（FQDN）は、コモン ネーム（CN）またはサブジェクト代替名（SAN）拡張と突き合わせてチェックされます。
- 有効期間 — 現在の時刻と日付が証明書の有効範囲内になければなりません。
- 証明書の失効状況
- 信頼性 — 証明書が信頼できるものでなければなりません。署名（発行）側を信頼できる場合、証明書は信頼できるものであると見なされます。一般的に、署名側による信頼は、署名側の証明書を信頼された証明書ストア（信頼ストア）にインポートすることにより確立されます。詳細については、自己署名証明書の代わりの CA 署名付き証明書を参照してください。

証明書に関する一般的なガイダンス

一部のサーバ（Cisco Unified CM や IM and Presence Service など）は、システム サービスに応じて異なる証明書を使用できます。Cisco Expressway などのサーバは、サーバが提供するサービスで 1 つの証明書だけを使用します。C：表 7-4 に、このプリファード アーキテクチャのサーバ証明書を示します。次の項で説明するように、ECDSA 証明書についてはこのドキュメントでは扱いません。

C：表 7-4　Cisco Collaboration 向けプリファード アーキテクチャのサーバ証明書

サービス	証明書	説明
Cisco Unified CM	tomcat	セキュアな Web 接続のために使用されます。LDAP、ILS、LBM などのサービスにも使用されます。
Cisco Unified CM	CallManager	CallManager サービスによるセキュア シグナリングと、TFTP 設定ファイルの署名に使用されます。
Cisco Unified CM	CAPF	認証局プロキシ機能（CAPF）サービスへの接続時にエンドポイントに必要です。
Cisco Unified CM	TVS	Trust Validation Service（TVS）への接続時に必要です。
Cisco Unified CM	ITLRecovery	ITL とトークンレス型 CTL ファイルの署名に使用されます。
Cisco Unified CM	ipsec	IPSec 接続に使用されます。IPSec を有効にできますが、これについてはこのドキュメントでは扱いません。IPSec 証明書は、ディザスタ リカバリ システムでも使用されます。
Cisco Unified CM	authz	OAuth に使用されます。
IM and Presence Service	tomcat	SIP クライアント（Unified CM）、Web サービス、SOAP、LDAP に使用されます。
IM and Presence Service	cup	SIP プロキシ、プレゼンス エンジン、SIP フェデレーションに使用されます。
IM and Presence Service	cup-xmpp	セキュア XMPP（IM）に使用されます。
IM and Presence Service	cup-xmpp-s2s	セキュア XMPP フェデレーションに使用されます。
IM and Presence Service	ipsec	IPSec に使用されます。
Cisco Unity Connection	tomcat	Unity Connection の Web サービス証明書。ボイス メール ポートへのメディアおよびシグナリング暗号化に使用されます。
Cisco Unity Connection	ipsec	IPSec に使用されます。

C：表 7-4　Cisco Collaboration 向けプリファード アーキテクチャのサーバ証明書（続き）

サービス	証明書	説明
Cisco Expressway-C	サーバ	Expressway-C とのすべてのセキュアな接続に使用されます。
Cisco Expressway-E	サーバ	Expressway-E とのすべてのセキュアな接続に使用されます。
Cisco Meeting Server	データベース クライアント	データベースがなく Call Bridge サービスを使用する Cisco Meeting Server が、データベースがある Cisco Meeting Server ノードと安全に接続するために使用されます。
Cisco Meeting Server	Web 管理画面、Call Bridge、XMPP、Web ブリッジ、およびデータベース サーバに使用される共有証明書	わかりやすくするため、データベース クライアントを除き、すべての Cisco Meeting Server ノードとサービスに同じ証明書を使用します。
Cisco Meeting Management	Server	Web 接続とコールブリッジ接続の場合
Survivable Remote Site Telephony（SRST）、Cisco IOS Gateway、Cisco Unified Border Element	Cisco IOS 証明書	SRST の場合、各エンドポイントの設定ファイルに SRST 証明書が含まれています。
Cisco Prime Collaboration Deployment	tomcat	Web サービスに使用されます。
Cisco Prime Collaboration Provisioning	プロビジョニング	Web アクセスのプロビジョニングに使用されます。

その他の ECDSA 証明書もありますが、この章の「RSA および ECDSA」で説明したように、この章の導入ガイダンスでは使用されないため、これらの証明書は C：表 7-4 には含まれていません。

一般に、デフォルトでは Cisco Collaboration サーバは自己署名証明書とともにインストールされます。ただし、証明書がデフォルトでインストールされない Cisco Meeting Server は例外です。

ITLRecovery 証明書以外の Cisco Unified CM の自己署名証明書の有効期間は 5 年間です。ITLRecovery 証明書の有効期間は 20 年です。証明書がシステム全体のトラスト アンカーとして使用される場合は、証明書の有効期間はさらに長くなります。

RSA および ECDSA

Cisco Collaboration 製品の証明書は通常、公開キー / 秘密キーとデジタル署名については RSA（Rivest, Shamir, and Adelman）に基づいています。一部の製品では楕円曲線デジタル署名アルゴリズム（楕円曲線 DSA）（ECDSA）証明書がサポートされていますが、簡素化するために、RSA ベースの証明書を使用することが一般に推奨されます。このドキュメントでは RSA ベースの証明書の使用について説明します。

エンドポイントについて、RSA ベースのローカルで有効な証明書 (LSC) を使用することを推奨します。Unified CM SIP TLS では、ECDSA と RSA は常に有効ですが、デフォルトでは RSA が ECDSA よりも優先されるため、RSA 証明書がネゴシエートされます。これが推奨されている設定です。HTTPS の場合、Unified CM、IM and Presence Service、Unity Connection では ECDSA はデフォルトで無効になっています。有効にするには [HTTPS 暗号方式（HTTPS Ciphers）] エンタープライズ パラメータを変更します。ただし、デフォルト設定（ECDSA 無効）を使用することが推奨されます。

注　ECDHE に基づく暗号化アルゴリズム スイートでは、ECDSA に基づく証明書は不要です。このようなスイートは RSA に基づく証明書とネゴシエートできます。

自己署名証明書の代わりの CA 署名付き証明書

デフォルトでは、ここで説明するシスコ製品のサーバのインストール時には、自己署名証明書がインストールされます（デフォルトで証明書がインストールされない Cisco Meeting Server を除く）。自己署名証明書に基づいてサービスへの信頼を確立するには、サービス（クライアント）へのセキュアな接続を必要とするすべてのエンティティの信頼された証明書ストア（または信頼ストア）に、サーバの自己署名証明書をインポートする必要があります。このようにしないと、サーバが接続を開始するときに（Unified CM SIP トランクへの接続など）、接続が失敗します。Jabber と Web ブラウザでは、ユーザに対し警告メッセージが表示されます。ユーザが証明書を受け入れると、通常その証明書は信頼された証明書ストアに追加されます。クライアントの起動中に多くの証明書を受け入れるよう何度もプロンプトが出されることは最良のユーザ エクスペリエンスとは言えないため、これは避けるべきです。より重要なこととして、ほとんどのユーザは、提示された証明書のフィンガープリントを確認してその証明書が正しいものであるかどうかを実際には検証せずに、どの証明書もそのまま受け入れてしまいます。これでは、セキュアなセッションを確立するための証明書ベースの認証のセキュリティの概念が成り立たなくなってしまいます。

自己署名証明書のインポートは、通信ピアが少ない場合は対処可能ですが、通信ピアの数が多い場合には実用的ではなくなります。これが、ほとんどのデフォルトの自己署名証明書を CA 署名付き証明書に置き換えることが推奨される主な理由です。これにより証明書の管理が簡素化されます。CA 署名付き証明書の場合、各サーバ証明書をクライアントの信頼ストアにインポートする必要はありません。ルート CA 証明書をクライアントの信頼ストアにインポートするだけで十分です。サーバ側では一般に、ルート CA 証明書をサーバの信頼ストアにインポートする必要もあります。また中間 CA を使用する場合は、証明書チェーンのすべての証明書をサーバの信頼ストアにインポートする必要もあります。CA 署名付き証明書を使用することで、署名側 CA のルート証明書がすべてのクライアントの信頼された証明書ストアにすでに追加されている限り、すべてのクライアントまたはサーバの信頼された証明書ストアを更新しなくても、新たなサービス証明書を発行できます。CA 署名付き証明書は、マルチサーバ証明書を使用する場合の要件でもあります。

CA 署名付き証明書を利用するメリットの例としては、自己署名証明書を Jabber クライアントで使用した場合は、Unified CM の tomcat 証明書 証明書（UDS および TFTP 設定ファイルのダウンロード用）、IM and Presence の tomcat および cup-xmpp 証明書（ログインおよびセキュアチャット用）、および Unity Connection の tomcat 証明書（ビジュアル ボイス メール用）は、Jabber を実行する各クライアントの信頼ストアにインポートする必要があることがあります。CA 署名付き証明書でインポートする必要があるのは、署名 CA のルート証明書のみです。

一般に、tomcat 証明書で CA 署名付き証明書を使用する場合が最も有用性が高くなります。これは、tomcat 証明書は広く使用されており、またユーザに表示される証明書であるためです。CallManager 証明書に CA 署名付き証明書を使用する場合も有用性が高くなります。これは、マルチサーバ証明書を使用でき（詳細については「マルチサーバ証明書」を参照）、SIP トランク経由で Unified CM サブスクライバに接続するすべてのエンティティの CallManager 証明書をインポートすることが回避されるためです。

ただし、1 つのエンタープライズ CA ですべての証明書を署名する必要はありません。一部の証明書は内部操作専用であり、これらの証明書を必要とするエンティティに対し、ユーザによる操作なしで提供されます。たとえば、信頼検証サービス（TVS）証明書は初期信頼リスト（ITL）ファイルに含まれており、エンドポイントの起動、再起動、またはリセット時にこの ITL ファイルがエンドポイントにより自動的にダウンロードされます。同様に、ITLRecovery 証明書は証明書信頼リスト（CTL）と初期信頼リスト（ITL）に含まれています。したがって、外部 CA でこれらの証明書に署名するメリットはありません。また、外部 CA で CAPF 証明書

に署名する実質的なメリットもありません。認証局プロキシ機能（CAPF）証明書またはエンドポイントのローカルで有効な証明書（LSC）の失効はサポートされていません。また、電話の VPN または 802.1x を設定するときには、ルート CA 証明書を ASA 信頼ストアにインポートするだけでは十分ではありません。TLS ハンドシェイク中にエンドポイントから証明書チェーンが送信されないため（したがって CAPF 証明書が送信されないため）、CAPF 証明書をインポートする必要があります。

C：表 7-5 に、CA による署名が推奨される証明書を示します。

C：表 7-5　　CA による署名が推奨される証明書

製品	証明書	注記
Cisco Unified CM、IM および Presence Service	tomcat	管理者やユーザが Web インターフェイスにアクセスする場合や、Jabber が UDS にアクセスしてログインする場合など、さまざまな用途に使用されます。
Cisco Unified CM	CallManager	SIP トランクなどさまざまな用途に使用されます。
Cisco Unified CM	ipsec	IPsec を使用する場合にのみ使用されます。
IM and Presence Service	xmpp	
IM and Presence Service	xmpp-s2s	
Cisco Unity Connection	tomcat	管理者やユーザが Web インターフェイスにアクセスする場合や、Jabber がビジュアル ボイス メールにアクセスする場合など、さまざまな用途に使用されます。
Cisco Expressway-C	サーバ	
Cisco Expressway-E	サーバ	パブリック CA を使用します。
Survivable Remote Site Telephony（SRST）と Cisco IOS Gateway	SRST と Cisco IOS ゲートウェイ	
Cisco Unified Border Element	Cisco IOS	一般にエンタープライズ CA を使用します。SIP サービス プロバイダーで暗号化がサポートされている場合は、パブリック CA を使用します。
Cisco Meeting Server	サーバ	すべての Cisco Meeting Server サービス用の共有証明書
Cisco Meeting Server	データベース クライアント	
Cisco Meeting Management	Server	
Cisco TelePresence Management Suite（TMS）	サーバ	
Cisco Prime Collaboration Deployment	tomcat	
Cisco Prime Collaboration Provisioning	プロビジョニング	

マルチサーバ証明書

証明書の管理をさらに簡素化するには、マルチサーバ証明書を使用できます。ノードごとに証明書を作成する代わりに、1 つの CA 署名付き証明書をクラスタ内のすべてのノードに使用できます。1 つの対応する秘密キーがすべてのノードで使用され、すべてのノードに自動的に反映されます。マルチサーバ証明書が使用可能な場合は常にマルチサーバ証明書を使用すること

が推奨されます。C：表 7-6 でこれを説明します。

C：表 7-6　マルチサーバ証明書のサポート

製品	証明書	注記
Unified CM and IM and Presence Service	tomcat	クラスタ内のすべての Unified CM ノードと IM and Presence ノードに対する 1 つの tomcat 証明書。証明書署名要求（CSR）を生成し、CA 発行の証明書を Unified CM パブリッシャ ノードにアップロードします。
Unified CM	CallManager	
IM and Presence Service	xmpp	
IM and Presence Service	xmpp-s2s	
Unity Connection	tomcat	

Cisco Meeting Server では、（データベース クライアント用の証明書の他に）Cisco Meeting Server クラスタ内のすべてのノードで共有される 1 つの証明書と 1 つの秘密キーを発行することもできます。ただし、秘密キーは自動的には反映されません。各 Cisco Meeting Server ノードに手動でインポートする必要があります。

注　この章で説明する Cisco Meeting Server 以外の Cisco Collaboration 製品では、ワイルドカード証明書はサポートされていません。Cisco Meeting Server では、（ワイルドカード以外の）標準証明書を発行し、その証明書をすべての Cisco Meeting Server サービスとノードに使用することが推奨されます（データベース クライアントの 2 番目の証明書を生成する必要があります）。

パブリック CA とプライベート CA

Expressway-E 証明書にはパブリック CA を使用するという要件の他に、このドキュメントで説明する Cisco Collaboration 製品のさまざまな証明書の署名に、パブリック CA またはエンタープライズ CA（プライベートまたは内部 CA）のいずれかを使用できます。パブリック CA を利用するメリットには、一部のクライアントとサーバではすでにデフォルトで主要なパブリック CA が信頼されているため、これらのデバイスとパブリック CA 間で信頼を確立する（CA 証明書をクライアントの信頼ストアにインポートする）必要がないことなどがあります。パブリック CA を使用する場合、IT 部門が内部 CA サーバをインストールして保守する必要がありません。ただし主要な短所として、証明書の発行にかかるコストと、一部のパブリック CA の制限事項があります。

CA での署名が推奨される証明書にはエンタープライズ CA を使用することが推奨され、このドキュメントでもこの点について説明しています。ただし、パブリック CA により署名する必要がある Expressway-E 証明書と、SIP サービス プロバイダーで暗号化がサポートされている場合の Cisco Unified Border Element 証明書は除きます。

Cisco Unified CM および IM と Presence

ここでは、Cisco Unified CM および IM と Presence の証明書の管理について説明します。

Unified CM 混合モード

メディアおよびシグナリング暗号化のための Unified CM 混合モード で後述するように、統一された CM 混合モードにより、電話機と TelePresence のエンドポイントでメディアおよびシグナリング暗号化が有効になります。トークンレス方式で混合モードを有効にすることが推奨されており、このドキュメントで説明しています。

CTL および ITL

証明書信頼リスト（CTL）と初期信頼リスト（ITL）は、Unified CM 証明書が含まれているファイルです。これらのファイルはシスコ エンドポイントによりダウンロードされます。これらの信頼リストにより、エンドポイントは Unified CM サービスへの信頼を確立するための最小限の Unified CM 証明書を取得します。Unified CM クラスタのモード（非セキュア モードまたは混合モード）に関係なく、ITL ファイルは常に Unified CM クラスタに存在しています。CTL ファイルは、Unified CM が混合モードの場合にのみ存在および適用されます。

CTL ファイルと ITL ファイルは、System Administrator Security Token（SAST、C：表 7-7 を参照）を使用して署名され、一連のレコードが含まれています。各レコードには、証明書、証明書のロールまたは機能、エンドポイントによる検索を容易にするために事前に抽出された証明書のフィールドが含まれています。C：表 7-7 に、証明書のロールを示します。

C：表 7-7　CTL ファイルと ITL ファイルでの証明書のロール

証明書のロール	証明書	説明
TFTP	CallManager	Unified CM TFTP サーバを認証します。たとえば、TFTP 設定ファイルの署名の検証に使用されます。この証明書ロールのレコードは、Unified CM が混合モードではない場合に ITL ファイルに含まれています。
CCM+TFTP	CallManager	暗号化シグナリングを使用して CallManager サービスを認証し、TFTP 設定ファイルの署名の検証時に Unified CM TFTP サーバを認証します。この証明書ロールのレコードは、Unified CM が混合モードである場合に ITL ファイルと CTL ファイルに含まれています。
System Administrator Security Token（SAST）	トークンレス型 CTL： パブリッシャの ITLRecovery 証明書および CallManager 証明書 ITL： TFTP サーバの ITLRecovery 証明書および CallManager 証明書	SAST（CTL、ITL、または TFTP 設定ファイルを署名するエンティティ）を認証します。 このタイプのレコードは ITL ファイルと CTL ファイルに含まれています。 ITL ファイルとトークンレス CTL ファイルは、ITL リカバリ キーを使用して署名されます。TFTP 設定ファイルは、TFTP サーバの CallManager 秘密キーを使用して署名されます。
Certificate Authority Proxy Function（CAPF）	CAPF	CAPF とのセキュア通信中に CAPF サービスを認証します。この証明書ロールのレコードは、CAPF サービスが Unified CM パブリッシャで有効化されている場合に、ITL ファイルと CTL ファイルに含まれています。
信頼検証サービス（TVS）	TVS	TVS への接続時に TVS サービスを認証します。ITL ファイルにのみ含まれています。

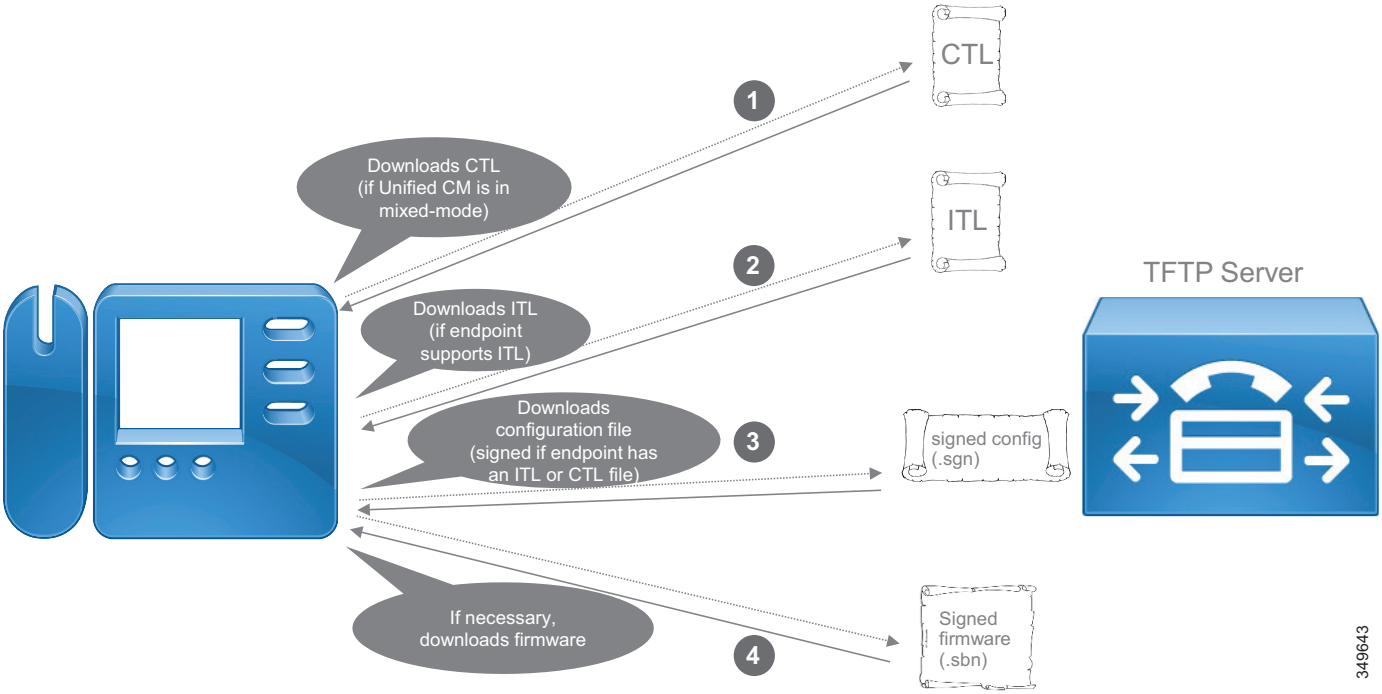
ITL は ITLRecovery 秘密キーを使用して署名されます。TFTP サービスを実行している各 Unified CM ノードには独自の ITL ファイルがあり、この ITL ファイルがエンドポイントに提供されます。

CTL ファイルは、System Administrator Security Token（SAST）の秘密キーを使用して署名されます。トークンレス CTL の場合、SAST は ITLRecovery 秘密キーです。Unified CM クラスタ全体で共有される CTL ファイルは 1 つだけです。

Unified CM が混合モードの場合、エンドポイントの起動またはリセット時に、エンドポイントの設定ファイルをダウンロードする前に証明書信頼リスト（CTL）が TFTP サーバからダウンロードされます。初期信頼リスト（ITL）がエンドポイントでサポートされている場合は、その後 TFTP サーバの ITL がダウンロードされます。ITL は Jabber ではサポートされていませんが、このプリファード アーキテクチャのその他のエンドポイントではサポートされています。エンドポイントを新規に導入し、エンドポイントが初めて Unified CM へ接続するときには、既存の CTL ファイルまたは ITL ファイルがないので、CTL または ITL 署名の検証に使用できる一連の証明書がありません。この場合、エンドポイントは 1 回限りで無条件に CTL/ITL ファイルを受け入れ、それらのファイルに含まれている証明書を保存します。エンドポイントに一連の信頼できる証明書が保存されたら、それ以降の CTL ファイルおよび ITL ファイルの署名の検証にはそれらの証明書を使用できます。

エンドポイントで ITL がサポートされている場合、または統一された CM が混合モードである（CTL ファイルがエンドポイントによりダウンロードされる）場合、エンドポイントは ITL/CTL ファイルに含まれている ITLRecovery 証明書を処理し、統一された CM TFTP サーバの CallManager 秘密キーを使用して署名されている設定ファイルを要求します。それ以外の場合（Jabber や、Unified CM が混合モードではない場合など）は、未署名の設定ファイルを要求します。エンドポイントは、設定ファイルのダウンロード後に、設定ファイルに正しいファームウェアが含まれていることを検証します。含まれていない場合は、該当するファームウェアをダウンロードし、そのファームウェアの署名を検証して、ファームウェアが改ざんされていないことを確認します。C：図 7-3 に、エンドポイントの起動中にエンドポイントによりダウンロードされるファイルの要約を示します。

C：図 7-3　　起動中にエンドポイントがダウンロードするファイル



エンドポイント証明書

エンドポイント証明書は主に、セキュア モードのエンドポイント、つまりエンドポイントでのメディアおよびシグナリング暗号化の実行時に使用されます。この証明書は、暗号化 TFTP 設定ファイル、802.1x 認証、電話の VPN、またはエンドポイントの Web サーバに HTTPS を介してアクセスする場合などにも使用できます。

シスコのエンドポイントの証明書には 2 種類あります。

- 製造元でインストールされる証明書（MIC）
- ローカルで有効な証明書（LSC）

MIC は、製造工程でエンドポイントに事前にインストールされており、Cisco Manufacturing CA により署名されています。その有効期間は 10 年であり、証明書失効はサポートされていません。MIC はメディアおよびシグナリング暗号化に使用できますが、MIC の代わりに LSC を生成することが推奨されます（これについては後述します）。Cisco IP Phone 7800 シリーズおよび 8800 シリーズ（Cisco Unified IP Conference Phone 8831 を含む）、Cisco TelePresence IX5000 シリーズのエンドポイント（Cisco MX、SX、Webex DX、および Webex Room シリーズ）、および Cisco TelePresence IX5000 シリーズエンドポイントにはすべて MIC があります。Jabber には MIC がありません。

LSC は、独自の展開にインストールする証明書です。統一された CM パブリッシャノードで実行される認証局プロキシ機能（CAPF）サービス、あるいは外部 CA によって署名されます。このプリファード アーキテクチャのすべてのシスコ エンドポイントでは LSC がサポートされます。LSC の有効期間は 5 年間であり、[Unified CM の管理（Unified CM Administration）] ページを使用するか、または有効期限に近くなると電子メールの通知が送信されるため、LSC の有効性を簡単に確認できます。このガイドに記載されているすべてのエンドポイントでは、LSC は SHA2 に基づいています。また、Jabber エンドポイントと Cisco IP Phone 7800 シリーズおよび 8800 シリーズのエンドポイントでは、2048 ビットまたは最大 4096 ビットのキー長に基づくことができます。LSC のインストールが完了すると、MIC は使用されなくなります。

MIC は、電話機がシスコの純正電話機であることを証明する目的で使用され、Cisco Manufacturing CA による署名を受けています。MIC を使用するメリットの 1 つに、Unified CM クラスタで設定されている正当な MAC アドレスが、不正なクライアントによりスプーフィングされることを防止することがあります。ただし MIC では、エンドポイントが Unified CM クラスタの一部であることは証明されません。したがって、802.1x または VPN には MIC に基づく認証を使用しないでください。このような認証を使用すると、あらゆるシスコ エンドポイント（組織外のエンドポイントを含む）が認証可能になります。通常、最初の CAPF 登録時に MIC を使用してエンドポイントの最初の LSC を生成することが推奨されます。エンドポイントで LSC が生成された後は、認証には、常に MIC ではなく LSC を使用することが推奨されます。MIC がないか、または MIC を公開するエンドポイント（たとえば、Jabber など）では、CAPF 登録認証は認証文字列またはヌル ストリングに基づいて実行できます。認証文字列に基づく認証は安全ですが、ユーザがエンドポイントで文字列を手動で入力する必要があります。この操作が現実的ではない場合は、ヌル ストリングに基づく認証を選択できますが、この認証では、最初の CAPF 登録時にすべてのエンドポイント認証が実質的に迂回されます。Jabber で LSC が生成されたら、その他のエンドポイントと同様に、LSC の更新に基づく認証が推奨されます。

電話機で LSC を発行するには、次の 3 つの方法があります。

- 最初の方法は、Cisco Unified CM の CAPF サービスに lSC に署名させる方法です。これが最も簡単な方法です。
- 2 番目の方法は、CAPF 登録を開始する際に、CAPF サービスを介して電話機に LSC を発行するオンライン外部 CA (Microsoft CA) を使用する方法です。この方法の主な利点は、LSC が独自の CA によって署名される点です。
- 3 番目の方法は、2 番目の方法に類似した方法です。LSC は外部 CA によって発行されますが、オフラインの方法では、エンドポイントの証明書署名要求 (CSR) ファイルを統一された CM から手動でエクスポートし、外部 CA によって署名してから、統一された CM にインポートし直す必要があります。この方法は手動の手順であるため、この推奨アーキテクチャでは説明されていません。

注　ワイヤレス接続を使用するエンドポイントと Jabber エンドポイントでは、CAPF が発行する LSC は Unified CM でのみ使用され、802.1X または EAP に拡張することはできません。

Jabber に関する考慮事項

暗号化されたメディアとシグナリングを実行するために、Jabber に証明書をインストールする必要はありません。Cisco Expressway のセクションで説明したように、Jabber が Mobile & Remote Access (MRA) 経由で接続している場合、他のエンドポイントと同様に、エンドポイント証明書をインストールする必要はありません。Jabber がエンタープライズ ネットワーク内にある場合、この推奨アーキテクチャでは、OAuth と SIP OAuth モードが有効であるため、LSC のインストールは必要ありません。

Survivable Remote Site Telephony（SRST）

セキュア SRST がサポートされています。Unified CM サーバが到達不能になると、エンドポイントはローカル SRST ルータに登録されます。Unified CM で暗号化モードで設定されているエンドポイントは、SRST ルータへの登録時にも、メディアとシグナリングが暗号化されたままになります。

セキュア SRST のプロビジョニング方法をまとめると、次のようになります。

1。 最初に、SRST ルータの証明書を生成します。ほとんどの証明書では、CA 署名付き証明書を使用することで証明書の管理が容易になります。

2。 [セキュア SRST（Is SRST Secure）] 設定を有効にして（チェックボックスがオン）設定されている Unified CM は、SRST ルータで実行されている証明書サーバの SRST 証明書を要求し、SRST を使用して設定されているエンドポイントの設定ファイルに SRST 証明書を挿入します。

3。 エンドポイント LSC に署名したエンティティに対応する信頼証明書を SRST ルータに手動でインポートします。CAPF を使用して LSC を発行する場合、これが CAPF 証明書となります。外部 CA を使用して lSC を発行する場合、これが CA 証明書 (または信頼チェーン証明書) となります。

4。 WAN がダウンするか、または Unified CM サーバが到達不能になると、エンドポイントは SRST と安全に通信します。エンドポイントは TFTP 設定ファイル内の SRST 証明書を使用して SRST を認証し、SRST は前の手順でインポートした LSC を発行したエンティティに対応する証明書（CAPF または外部 CA 証明書）を認証します。

Cisco Unity Connection

このドキュメントでは、次世代暗号化（NGE）を使用した Cisco Unity Connection のメディアおよびシグナリング暗号化について説明します。この構成では、Unity Connection のルート証明書および SIP 証明書の代わりに、tomcat 証明書が使用されます。Unified CM と Unity Connection の間で SIP トランクが設定されています。この SIP トランクはセキュアであり、Unified CM と Unity Connection は相互に認証します。Unified CM の認証には CallManager 証明書が使用され、Unity Connection の認証には tomcat 証明書が使用されます。前述したように、Unity CM と Unity Connection の間での証明書交換が不要になるように、エンタープライズ CA でこれらの証明書を署名することが推奨されます。ルート CA 証明書を Unified CM CallManager 信頼ストアと Unity Connection tomcat 信頼ストアにインポートする必要があります。また Unity Connection は、Unified CM TFTP サーバから tomcat 信頼ストアに Unified CM CallManager 証明書を自動的にダウンロードします。

Cisco Expressway

Cisco Expressway ソフトウェアの新規インストールには、一時的に信頼された CA と、その一時 CA が発行するサーバ証明書が付属しています。サーバ証明書を CA 署名付き証明書に置き換え、信頼する機関のルート CA 証明書または証明書チェーンをインストールすることが推奨されます。

Expressway-C 証明書は、エンタープライズ CA またはパブリック CA により署名できます。前述したように、このドキュメントではエンタープライズ CA が使用されていることを前提としています。Expressway-E では、サーバ証明書をパブリック CA で署名するという要件があります。この要件には次の 2 つの理由があります。

- モバイルおよびリモート アクセス（MRA）可能なハードウェア エンドポイントには、エンドポイントのファームウェアに含まれており信頼されるパブリック ルート CA 証明書が 100 以上含まれています。ルート CA 証明書を追加するメカニズムはないので、これらのパブリック CA のいずれかで Expressway-E 証明書を署名する必要があります。サポートされているパブリック CA の一覧は、https://www.cisco.com のエンドポイント ドキュメント（https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-technical-reference-list.html など）に記載されています。
- Cisco Expressway-E は、エンドポイント、その他の組織、さらには Cisco Collaboration Cloud とも通信するインターネットに公開されているコンポーネントです。このため、最小限の労力で最大限のセキュリティと信頼性を実現するには、パブリック CA の信頼性の基盤となる Public Key Infrastructure（PKI）が必要です。

エンドポイントがモバイルおよびリモート アクセス（MRA）経由で企業に接続している場合、CAPF 登録はサポートされません。つまり、エンドポイントが MRA 経由で接続されている場合には LSC をインストールできません。ただし、エンドポイントに MIC がない場合でも、これによってエンドポイントがエンドツーエンドの暗号化（すべてのコール レッグの暗号化）を使用できなくなることはありません。実際には、MRA 経由での接続時には MIC と LSC は不要であるかまたは使用されません。

注　（**デバイス セキュリティ モード** が **暗号化**に設定されている電話セキュリティ プロファイルを使用して）エンドポイントが暗号化モードで設定されており、MIC または LSC がエンドポイントにない場合、エンドポイントは MRA 経由で接続する際に、継続して正常に接続されます。ただし、エンドポイントが企業（オンプレミス）に直接接続する場合、エンドポイントには証明書が必要です。証明書がないとエンドポイントは登録されません。これは、OAuth トークンを使用する Jabber には適用されません。

MRA では CAPF 登録がサポートされていないため、MRA エンドポイントでの TFTP 設定ファイルの暗号化に関する考慮事項があります。詳細については、「TFTP 設定ファイルの暗号化」を参照してください。

「コラボレーション エッジ」の章でも、Cisco Expressway に関するセキュリティ上の考慮事項について説明しています。詳細についてはこの章を参照してください。

Cisco Meeting Server

デフォルトでは、Cisco Meeting Server には証明書がありません。Cisco Meeting Server では、証明書に関して複数のオプションがサポートされていますが、このドキュメントでは、データベース クライアント用に 1 つの CA 署名付き証明書を発行し、その他のサービス用にもう 1 つの CA 署名付き証明書を発行し、Cisco Meeting Server クラスタ内のすべてのノードにこれらの証明書とそれに対応する秘密キーをコピーすることを推奨しています。

Cisco Meeting Management

Cisco Meeting Management は、証明書を使用してブラウザとコールブリッジに対して自己識別します。セットアップ中に、Meeting Management が自己署名証明書を生成します。これを CA 署名付き証明書に置き換える必要があります。

Cisco Prime Collaboration Deployment

Cisco Prime Collaboration Deployment は Unified CM と同じプラットフォームを使用しますが、証明書管理用のグラフィカル ユーザ インターフェイスがありません。HTTPS の場合 ECDSA が無効になるため、tomcat 証明書だけを CA で署名する必要があります。プラットフォームの CLI（コマンド ライン インターフェイス）を使用して、証明書署名要求（CSR）を生成し、CA 署名付き tomcat 証明書をアップロードします。

Cisco Prime Collaboration Deployment は、HTTPS に基づいて SOAP サービスを使用して Cisco Collaboration 製品に接続し、Cisco Prime Collaboration Deployment タスクの実行中にデータをインポートまたはエクスポートします。

Cisco Prime Collaboration Provisioning

Cisco Prime Collaboration プロビジョニングには、デフォルトで署名付き証明書があります。この証明書を、エンタープライズ CA によって署名された証明書に置き換えることが推奨されます。Cisco Prime Collaboration プロビジョニングでは証明書チェーンはサポートされていません。プロビジョニングを実行するため、Cisco Prime Collaboration プロビジョニングは暗号化接続を介してさまざまな Cisco Collaboration サーバに接続します。

暗号化

内部ネットワークを超えて拡張するするサービスが増加し、内部ネットワークが内部攻撃の対象となる可能性があることから、暗号化と認証の重要性が増しています。

暗号化により、盗聴、改ざん、セッション リプレイなどの攻撃から保護されます。不正ユーザは、トラフィックをキャプチャできても、暗号キーなしでは通信内容を復号化または変更することはできません。暗号化では、暗号化通信の設定時にデジタル証明書による認証も実現できます。

通常、TLS の概要のセクション項で説明したように、さまざまなサーバ接続で暗号化を有効にすることをお勧めします。Jabber では、暗号化メディアとシグナリングを有効にすることを推奨します。Jabber は OAuth トークンを使用して暗号化メディアおよびシグナリングを実行することができ、LSC を必要としないため、プロビジョニングおよび管理が容易です。電話機とテレプレゼンス エンドポイントでは、可能な場合は暗号化メディアとシグナリングを有効にすることを推奨します。ただし、混合モードを有効にして、LSC をインストールする必要があるため、より多くの設定が必要になります (MIC でなく、LSC を使用することを推奨します)。

認証が一方向の認証であることがあります。たとえば、管理者またはエンド ユーザが Web ブラウザを使用して Web サービスにアクセスする場合などです。この場合、クライアント（ブラウザ）が Web サーバを認証しますが、サーバはクライアント（ブラウザ）を認証しません。認証が、相互 TLS（MTLS）を使用した双方向認証であることもあります。この場合、サーバもクライアントを認証します。たとえば、エンドポイントと、エンドポイントが登録している Unified CM サーバ間のシグナリング、または Unified CM SIP トランクに、MTLS が使用されます。

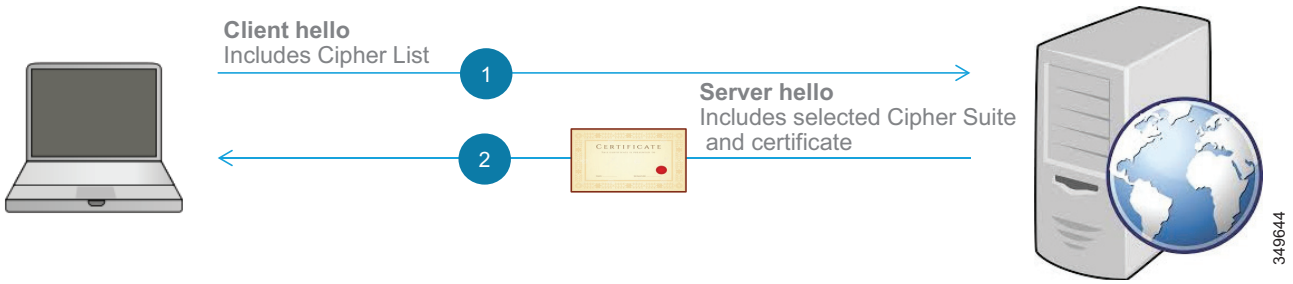
TLS の概要

Transport Layer Security（TLS）は、TCP トラフィックを暗号化する手法であり、一般に Web サービス トラフィックと SIP シグナリングに使用されます。TLS セッションの確立の全体的な流れを次に示します。

1. TLS クライアントにより TLS 接続が開始されます。このクライアントは TLS サーバに接続します。クライアントはまず、乱数とクライアントの機能を含む Client Hello を送信して、サーバとの TCP 接続を確立します。これらの機能には、クライアントでサポートされている暗号スイートのリストなどが含まれています。
2. TLS サーバは、通常はクライアントで優先される暗号スイートに基づいて暗号スイートの 1 つを選択し、Server Hello で応答します。このメッセージには、別の乱数とサーバ証明書も含まれているため、クライアントがこの証明書を認証できます。

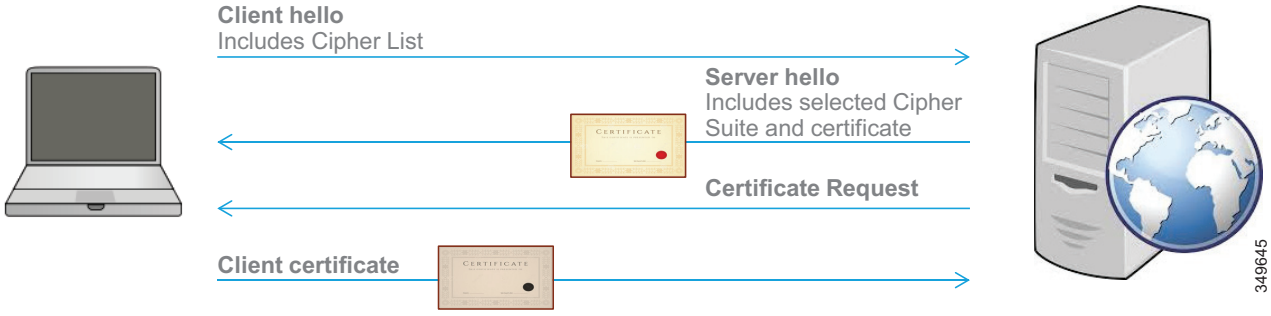
C：図 7-4 に、この 2 段階の TLS セッション確立手順を示します。便宜上、この図には TLS ハンドシェイクでのすべてのメッセージとバリエーションは含まれていません。サーバ証明書は Server Hello メッセージで送信されるか、または個別に送信されます。

C：図 7-4　TLS ハンドシェイク



認証が一方向の認証であることがあります。たとえば、管理者またはエンド ユーザが Web ブラウザを使用して Web サービスにアクセスする場合などです。この場合、クライアント（ブラウザ）が Web サーバを認証しますが、サーバはクライアント（ブラウザ）を認証しません。認証が、相互 TLS（MTLS）を使用した双方向認証であることもあります。この場合、サーバもクライアントを認証します。たとえば、エンドポイントと、エンドポイントが登録している Unified CM サーバ間のシグナリング、または Unified CM SIP トランクに、MTLS が使用されます。相互 TLS（MTLS）では、サーバもクライアントを認証します。サーバから CertificateRequest がクライアントに送信され、クライアントからそのクライアント証明書が送信されます。C：図 7-5 に全体的な流れを示します。

C：図 7-5　MTLS ハンドシェイク



RSA では、クライアントがサーバの公開キーを使用してプリマスター シークレットを暗号化し、サーバに送信します。Diffie-Hellman（DH）キー アグリーメント アルゴリズムでは、プリマスター シークレットはネットワーク経由では送信されず、クライアントとサーバが（乱数から計算され、認証のために秘密キーで署名された）データを交換します。これにより、クライアントとサーバは各自でプリマスター シークレットを導出できます。DH と変化する乱数の組み合わせ（Diffie-Hellman Ephemeral）により、Perfect Forward Secrecy（PFS）が実現します。

マスター シークレットが導出され、マスター シークレットからセッション キーが計算されます。この時点でクライアントとサーバは公開キー / 秘密キー ペア（非対称暗号化）の使用を停止し、暗号化に共有セッション キー（対称暗号化）を使用し始めます。

一般に、Cisco Collaboration 製品では TLS 1.2 がサポートされています。ただし、一部の製品ではこの TLS はまだサポートされていない可能性があり、一部の古い製品では一切サポートされていません。相互運用性を最大に引き出すため、デフォルト設定を使用し、特に無効にする必要がある場合を除き TLS 1.0 または TLS 1.1 を明示的に無効にしないでおくことをお勧めします。デフォルト設定では、クライアント インターフェイスとサーバ インターフェイスの両方で TLS 1.2 がサポートされている一般的なケースの場合、TLS 1.2 がネゴシエートされます。Cisco Collaboration 製品での TLS 1.2 のサポートと、TLS の古いバージョンを無効にする機能の詳細については、次で提供される *TLS Compatibility Matrix for Cisco Collaboration Products* の最新版を参照してください。

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/unified/communications/system/Compatibility/TLS/TLS1-2-Compatibility-Matrix.html

Cisco Unified CM および IM と Presence とエンドポイント

暗号化する主な 3 種類の接続を次に示します。

- HTTPS および管理インターフェイスまたはユーザ インターフェイス

  これらのインターフェイスのほとんどでは、デフォルトで暗号化が使用されます。たとえば、Unified CM 管理 Web インターフェイスと Unified CM エンドユーザ ポータルでは HTTPS が使用されます。パスワードまたはその他の機密情報が接続で送信される場合は、その接続を暗号化します。たとえば、LDAP と統合された Unified CM の場合は、LDAP over SSL を使用します。あるいはエンドポイントでは、エクステンション モビリティなどの Web サービスに対して HTTPS を設定します。

- シグナリング

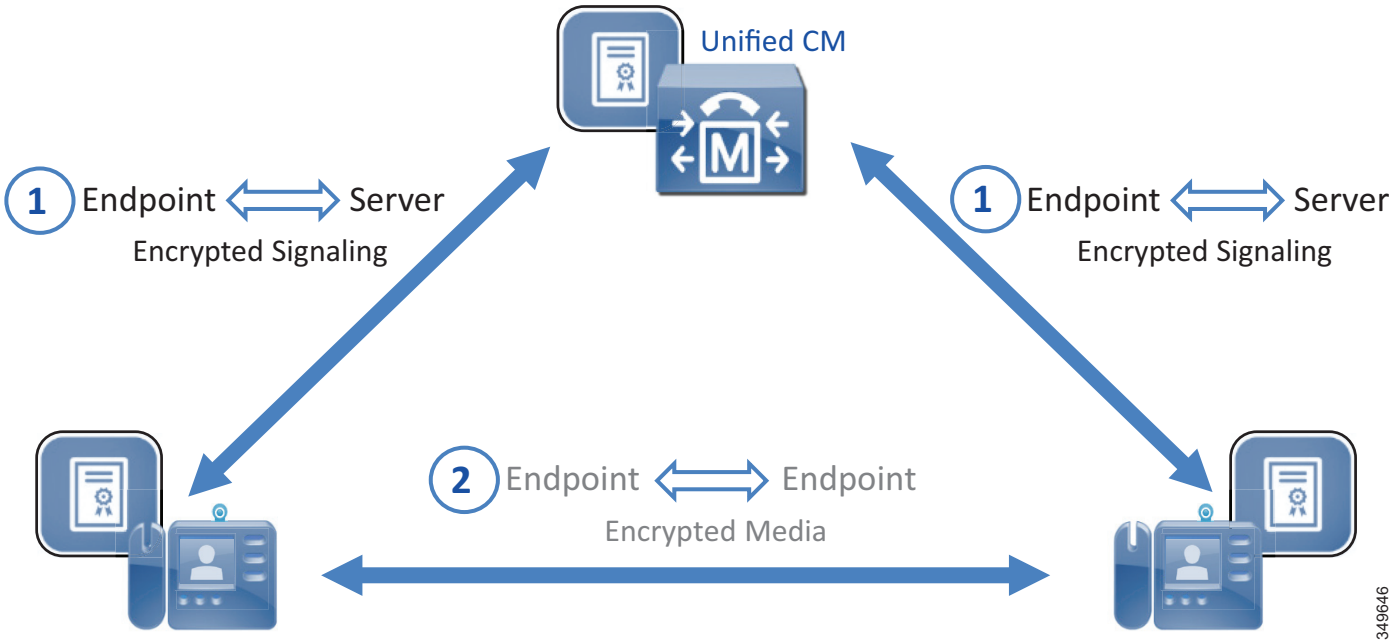
  TLS は主に、コール制御シグナリングの暗号化に使用されます。たとえば、エンドポイントと Unified CM サーバ間の SIP シグナリングまたは SIP トランクでの SIP シグナリングなどです。TLS は、XMPP など他の TCP 通信にも使用されます。

- メディア

  メディア トラフィックは、Secure RTP（SRTP）で暗号化できます。シグナリングも暗号化する必要があります。これは、（SDES を使用した）Unified CM へのシグナリングでは、メディア暗号化キーがエンドポイント間で交換されるためです。

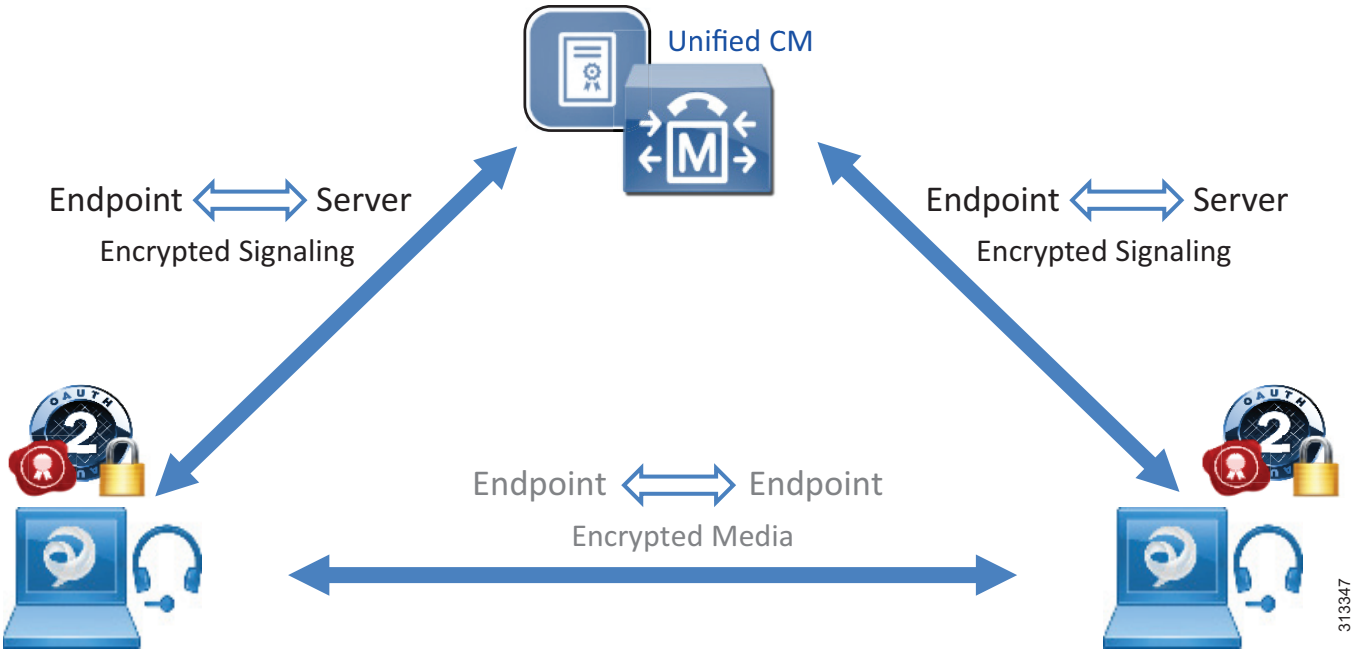
C：図 7-6 に、エンドポイントでのシグナリングとメディアの暗号化の全体像を示します。図のステップ 1 で示されるように、まず、エンドポイントと Unified CM の間の SIP シグナリングのために TLS が設定されます（エンドポイント登録）。図のステップ 2 で示されるように、エンドポイントからコールが発信されると、メディア暗号化キーが生成され、SIP TLS チャネルで送信されます。メディアは SRTP を使用して暗号化されます。C：図 7-6 で示されるように、電話機と TelePresence エンドポイントでは、シグナリング用の TLS ハンドシェイク認証は、統一された CM とエンドポイントの証明書に基づいています。

C：図 7-6　電話またはテレプレゼンスエンドポイントでのシグナリングおよびメディア暗号化



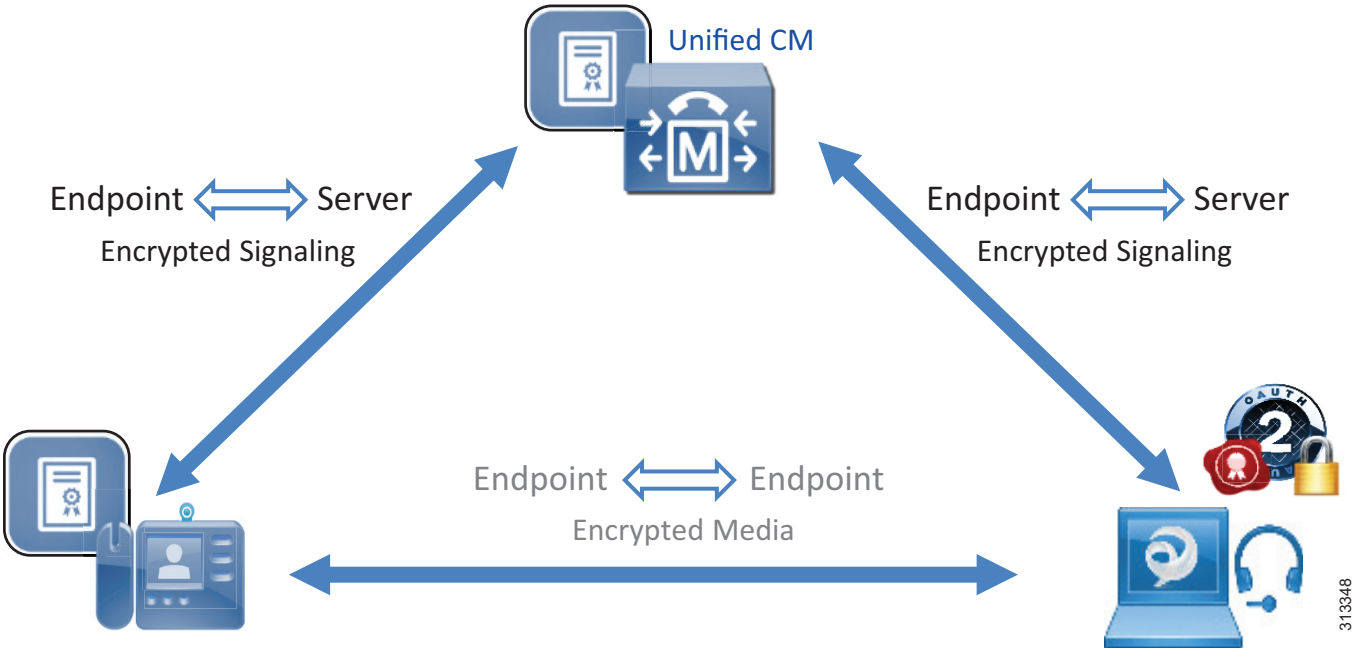
メディアとシグナリングの暗号化を実行するには、この推奨アーキテクチャの Jabber クライアントは、C：図 7-7 に示すように、TLS 認証に OAuth トークンを使用します。

C：図 7-7　Jabber を使用したシグナリングおよびメディア暗号化



LSC を使用してメディアおよびシグナリングを暗号化する電話機および TelePresence エンドポイントは、C：図 7-8 に示すように、OAuth トークンを使用する Jabber クライアントに対して暗号化されたコールを発信および受信することができます。

C：図 7-8　電話またはテレプレゼンス エンドポイントと Jabber を使用したシグナリングとメディアの暗号化



注　IM and Presence が導入されている Unified CM クラスタ内のノード間の通信（Intra-Cluster Communication Signaling（ICCS）など）を暗号化するには、IPSec を導入する必要があります。ただし、IPSec の設定と運用によって複雑さが大幅に増し、システムのスケーラビリティに影響すること、および Unified CM および IM and Presence ノードは通常、保護されており信頼できるデータ センター内に配置されていることから、IPSec の導入はほとんどの導入では通常は必要ではないため、このドキュメントでは説明しません。

暗号スイートのサポート

暗号スイートは、TLS セッションの確立に使用する暗号化アルゴリズムの組み合わせです。通信リンクの暗号化に使用できる暗号スイートは、Cisco Collaboration 製品に応じて異なります。標準的な暗号スイートは、Cisco Collaboration ソリューション全体でサポートされます。Cisco Unified CM、IM and Presence、Unity Connection などの一部の製品と、このガイドに示されているほとんどのエンドポイント（Cisco Jabber、Cisco IP Phone 7800 シリーズおよび 8800 シリーズ、Cisco Webex DX シリーズなど）では、次世代暗号化（NGE）と呼ばれる強力な新しい暗号スイートがサポートされています。これらの強力な暗号スイートは、新しいアルゴリズムをベースにしているか、またはより長い暗号キーを使用しているため、侵害が困難です。一般に、クライアントとサーバの両方でサポートされている最も強力な暗号スイートがネゴシエートされます。クライアントで弱い暗号スイートだけがサポートされている場合は、弱い暗号がネゴシエートされる可能性があります。弱すぎる暗号スイートにネゴシエートすることを回避するには、通常、ネゴシエート可能な暗号スイートを制限できます。たとえば統一された CM では、TLS 暗号スイートネゴシエーションを最も強力な暗号スイート（AES 256 と SHA 384 のみ）に制限する設定、強力な暗号スイートおよび中程度の強度の暗号スイート（AES 128 と SHA 256）を許可する設定、およびサポートされているすべての暗号スイートを許可する設定があります。より詳細な方法として、許可できる暗号スイートのリストを設定することも可能です。Cisco Collaboration ソリューション全体では、TLS 接続の設定に使用するデジタル署名アルゴリズムとして RSA がサポートされています。使用可能なもう 1 つのデジタル署名アルゴリズムとして、楕円曲線デジタル署名アルゴリズム（ECDSA）があります。ECDSA は、RSA と同レベルのセキュリティを提供しますが、キーのサイズが RSA よりも小さくなっています。ただし、すべての統一された CM サービス、すべての Cisco Collaboration 製品、またはエンドポイントでサポートされているわけではありません。また、それはサーバおよびクライアントが ECDSA ベースの証明書を持つことを必要としする場合があります。RSA と ECDSA の詳細については、「証明書の管理」を参照してください。

注　ECDHE に基づく暗号化アルゴリズム スイートでは、ECDSA に基づく証明書は不要です。このようなスイートは RSA に基づく証明書とネゴシエートできます。

次に、各種接続の暗号スイートと推奨事項を説明します。

- HTTPS 接続

  Unified CM および IM and Presence の場合、HTTPS 暗号スイートを対象としたエンタープライズ パラメータ設定が 1 つあります。このパラメータにより、RSA 専用暗号スイートが許可されるのか、またはすべての暗号スイート（RSA および ECDSA）が許可されるのかが決まります。デフォルト値（RSA 専用暗号スイートの許可）を使用することが推奨されます（詳細については「RSA および ECDSA」を参照）。

  ネゴシエートされる一般的な暗号スイートは、TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 または TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 です。これらの暗号スイートでは、ECDHE（Elliptical Curve Diffie Hellman Ephemeral）と RSA は、デジタル署名アルゴリズムとキー アグリーメントに使用される暗号を示します。AES（Advanced Encryption Standard）、GCM（Gallois Counter Mode）、および SHA（Secure Hash Algorithm）は、暗号化パケットの実際の暗号化と認証に使用されます。

- SIP TLS (シグナリング)

  Unified CM ではデフォルトで、RSA に基づく暗号スイートが ECDSA に基づく暗号スイートよりも優先されます。ECDSA はすべてのエンドポイントでサポートされているわけではなく、またすべての Cisco Collaboration サーバでサポートされているわけではないため、これは推奨される設定です。

  デフォルトでは、サポートされているすべての暗号スイートが有効になります。前述したように、より強力な暗号スイートが最初にネゴシエートされます。通常は TLS_ECDHE_RSA および AES256_GCM_SHA384 がネゴシエートされます。ただし、場合によってはこの暗号化がいずれの側でもサポートされていないため、これよりも弱い暗号をネゴシエートする必要があります。ソリューション内の各種コンポーネントでの暗号スイートの互換性を最大限に引き出すため、デフォルト設定（すべての暗号スイートを許可し、RSA を優先する）を使用することが推奨されます。

- SRTP（メディア）

  Unified CM では、デフォルトですべての暗号化が有効になっています。前述したように、強力な暗号スイートが最初に試行されます。通常、最も強力な暗号化である AEAD AES-256 GCM（Authenticated Encryption with Associated Data、Advanced Encryption Standard、256 キー サイズ、Galois Counter Mode）がネゴシエートされます。ただし Cisco IOS Gateway、一部のエンドポイント、および一部のサーバではこの暗号スイートがサポートされていないことがあります。このため、デフォルト設定を使用し、弱い暗号スイートへのフォールバックを許容することが推奨されます。シスコ エンドポイントでサポートされている暗号スイートを確認するには、Unified CM の [Cisco Unified Reporting] ページに移動します（[システム レポート（System Reports）] > [Unified CM Phone の機能リスト（Unified CM Phone Feature List）]）。

メディアおよびシグナリング暗号化のための Unified CM 混合モード

Unified CM を初めてインストールする場合、いわゆる「非セキュア モード」でインストールされますが、実際にはこのモードではほとんどのセキュリティ機能が使用可能です。たとえば、非セキュア モードの Unified CM では、署名付き TFTP 設定ファイル、暗号化 TFTP 設定ファイル、署名付き電話ファームウェア、Web サービスへの HTTPS アクセス、ローカルで有効な証明書（LSC）をインストールするための CAPF 登録、SIP トランク暗号化、電話の VPN、802.1x はすべてデフォルトで使用可能になっています。Jabber でのメディアおよびシグナリングの暗号化は、SIP OAuth モードが有効になっている場合にも可能です (詳細については、Jabber を使用した SIP OAuth の項を参照してください)。非セキュアモードで欠落しているセキュリティ機能は、電話機および TelePresence エンドポイントのメディアおよびシグナリング暗号化です。この機能を有効にするには、スマートライセンスで輸出規制機能が許可されており、統一された CM を混合モードで設定する必要があり、また統一された CM ソフトウェアの制限付きバージョンが必要です。（メディアおよびシグナリング暗号化は、無制限バージョンの Unified CM では使用できません。）

混合モードと暗号化に関する重要な考慮事項として、電話および TelePresence エンドポイントでの証明書の管理があります。エンドポイントで MIC の代わりに LSC を使用することが推奨されるため、電話機と TelePresence エンドポイントでの CAPF 登録 (LSC インストール) は、メディアとシグナリングの暗号化が有効になっている電話機と TelePresence エンドポイントで実行する必要があります。管理者は LSC の有効期間をモニタし、有効期限切れになる前に証明書を交換する必要があります。エンドポイントは、現在有効なサーバ証明書を保持する必要もあります。たとえば、現在の CallManager 証明書がなく、メディアおよびシグナリング暗号化を使用して設定されている場合は、統一された CM に登録されません。（詳細については、「CTL および ITL」を参照。）

混合モードを有効にする方法は 2 通りあります。

- ハードウェア USB eToken

  混合モードを有効にする従来の方法です。2 つ以上のハードウェア USB eToken（KEY-CCM-ADMIN-K9= または新しい KEY-CCM-ADMIN2-K9=）が必要です。証明書信頼リスト（CTL）ファイルの署名に 1 つの eToken が使用されます。もう 1 つの eToken を用意することで、1 番目の eToken が紛失した場合または使用できない状態になった場合に備えた冗長性が実現します。混合モードを有効にするには、CTL クライアント ソフトウェアを Microsoft Windows デスクトップにインストールする必要があります。この CTL クライアント ソフトウェアの実行中に、USB eToken をデスクトップに挿入する必要があります。混合モードの設定後に、Unified CM クラスタの CTL ファイルを作成し、USB eToken を取り外し、オフラインにします。

- トークンレス（ソフトウェア eToken）

  この方法では、USB トークンと Microsoft Windows デスクトップは不要です。単に CLI コマンド **utils ctl set-cluster mixed-mode** を使用して混合モードを有効にします。CTL ファイルは、ハードウェア USB eToken ではなく ITLRecovery 秘密キーによって署名されます。

トークンレス方式が推奨されます。このドキュメントではこの方式について説明します。トークンレス方式では、混合モードを有効にする方法と CTL ファイルを更新する方法がシンプルです。混合モードを有効化するときと CTL ファイルを更新するときに、USB eToken を取得し、CTL クライアントを Microsoft Windows デスクトップにインストールし、CTL クライアントを実行する必要はありません。実行する必要がある CLI コマンドは 1 つだけです。CTL の署名には、長い秘密キー（ITLRecovery 秘密キー）が使用されます。また、Cisco Unified CM 12.0 以降では、ITL ファイルとトークンレス CTL ファイルは ITLRecovery 秘密キーにより署名されるため、Trust Verification Service（TVS）に問題がある場合、CallManager 証明書の更新に関する懸念が解消され、またこの更新が原因でエンドポイントと Unified CM 間の信頼関係が失われることがなくなりました。

Jabber を使用した SIP OAuth

Jabber でメディアおよびシグナリングの暗号化を有効にするには、混合モードを有効にして、Jabber に LSC をインストールします。このアプローチの欠点は、LSC をインストールして維持するため、Jabber による追加の管理上のオーバーヘッドが必要になる場合があることです。たとえば、Jabber エンドポイントがリセットされた場合、新たな LSC をインストールする必要があります。Jabber に LSC をインストールする代わりに、SIP の OAuth トークンを有効にすることを推奨します。このモードでは、Jabber は LSC なしで、また、統一された CM で混合モードを有効にする必要なく、メディアおよびシグナリングの暗号化を実行できます。

OAuth トークンを SIP で使えるように、スマートライセンスで輸出規制機能が許可されており、統一された CM ソフトウェアの制限付きバージョンが必要です。（メディアおよびシグナリング暗号化は、無制限バージョンの Unified CM では使用できません。）

注　Jabber 以外のエンドポイントに対して暗号化メディアとシグナリングを有効にする場合も、統一された CM で混合モードを有効にする必要があります。

TFTP 設定ファイルの暗号化

TFTP 設定ファイルを暗号化しないと、すべての Unified CM TFTP サーバで TFTP 設定ファイルがプレーンテキスト形式で使用可能になります。TFTP 設定ファイルには、電話ファームウェアの情報や Unified CM クラスタの情報などが含まれています。さらに、ユーザ名とパスワードが Unified CM 管理電話ページでプロビジョニングされている場合、このユーザ名とパスワードが TFTP 設定ファイルにプレーンテキスト形式で保存されています。したがって、オンプレミスのエンドポイント（モバイルおよびリモート アクセス（MRA）経由で接続していないエンドポイント）で電話と TelePresence 用の TFTP 設定ファイルの暗号化を有効にすることが推奨されます。これは、Unified CM 管理電話ページでユーザ名、パスワード、または機密情報が設定されている場合に特に重要です。

MRA 電話および MRA TelePresence エンドポイントでは、TFTP 設定ファイル暗号化が設定されている場合、MIC が含まれていても、最初に MRA エンドポイントをオンプレミスに導入してから、統一された CM に直接登録し、その後インターネットに導入して MRA 経由で接続する必要があります。さらに、MRA 経由で接続するエンドポイントに LSC をインストールまたは更新することはできません。したがって、LSC の有効期限が切れると、エンドポイントは社内ネットワークに戻す必要があります。このような理由から、MRA 経由で接続しているエンドポイント（特に Jabber エンドポイント）では、TFTP 設定ファイルの暗号化を有効にしないでおく方が簡単です。ただし、これらのエンドポイントの機密情報（たとえばパスワード）が設定されていないことを確認してください。

Jabber クライアントは、この推奨アーキテクチャでは SIP OAuth モードに対して有効になっており、暗号化メディアおよびシグナリングには LSC は必要ありませんが、TFTP 設定ファイルの暗号化には 1 つ必要となります。Jabber クライアントで LSC を管理するには、追加の管理オーバーヘッドが必要です (たとえば、Jabber をリセットすると、LSC が削除されるので、新しい LSC をインストールする必要があります)。また、LSC は暗号化メディアおよびシグナリングには不要です。通常、Jabber クライアントに LSC をインストールしないことを推奨します。つまり、Jabber クライアントがオンプレミスであるか、MRA 経由で接続されているかにかかわらず、TFTP 設定ファイルの暗号化を採用しないことになります。ただし、Jabber クライアント用に、これらのエンドポイントの機密情報が設定されていないことを確認してください。

セキュア SRST

Cisco 4000 シリーズ サービス統合型ルータに基づく Survivable Remote Site Telephony（SRST）ルータは、セキュア SRST を使用して設定することもできます。エンドポイントは、Unified CM コール処理サーバとの通信を確立できないと SRST にフェールオーバーし、メディアおよびシグナリングは引き続きセキュア SRST で暗号化されます。エンドポイントの TFTP 設定ファイルに SRST 証明書が含まれており、SRST ルータの信頼ストアに LSC に署名した CA の証明書が含まれているため（管理者により手動でインポートされた CAPF 証明書あるいは外部 CA 証明書）、エンドポイントと SRST ルータはセキュアな認証済みセッションを確立することができます。

Cisco Meeting Server

Cisco Meeting Server ノード間の内部通信には暗号化（TLS）が使用されます。Cisco Meeting Server とその他のサーバまたはデバイス間の外部通信では、通信のタイプに応じて暗号化は強制またはオプションです。たとえば、Unified CM と Cisco Meeting Server 間の RESTful API 通信は常に暗号化されます。ただし、Cisco Meeting Server と Unified CM またはエンドポイント間の SIP シグナリングおよびメディアの設定時には、暗号化を使用してもしなくてもかまいません（暗号化が推奨されます）。会議では、すべての参加エンドポイントが暗号化されている場合（暗号化メディアおよびシグナリング）、会議ロックをサポートするすべてのエンドポイントにロック アイコンが表示されます。参加エンドポイントのいずれかがセキュアではない場合、会議ロックをサポートするすべてのエンドポイントにロック解除アイコンが表示されます。

Cisco Unity Connection

このドキュメントでは、次世代暗号化（NGE）を使用した Cisco Unity Connection のメディアおよびシグナリング暗号化について説明します。暗号化により、Unity Connection との間でのシグナリングと、エンドポイントと Unity Connection ボイスメール ポート間でのメディアが暗号化されます。デフォルトでは、Unified CM と Unity Connection 間のシグナリングでは TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 暗号スイートがネゴシエートされます。

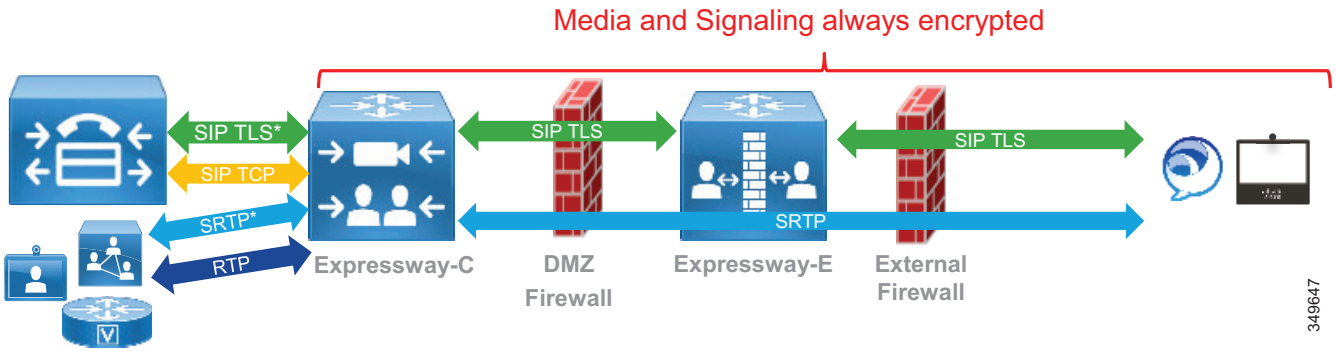
Cisco Expressway

Cisco Expressway とのモバイルおよびリモート アクセス（MRA）コミュニケーションおよび Business-to-Business（B2B）コミュニケーションについて説明します。

モバイル&リモートアクセス（MRA）

MRA エンドポイントと Expressway-C 間のメディアおよびシグナリングは常に暗号化されます。MRA エンドポイントが社内ネットワーク内部のエンドポイントをコールする場合、社内ネットワーク内のコール レッグ（Expressway-C と Unified CM 間のシグナリングおよび Expressway-C と内部エンドポイント間のメディア）は設定に基づいて暗号化できます。非暗号化モードで電話セキュリティ プロファイルを使用して MRA エンドポイントが設定されている場合、この内部コール レッグは暗号化されません。Unified CM が混合モードであり、暗号化モードで電話セキュリティ プロファイルを使用して MRA エンドポイントが設定されている場合、Expressway-C と Unified CM 間の SIP シグナリングは暗号化されます。さらに、内部エンドポイントも暗号化モードで設定されている場合、Expressway-C と内部エンドポイント間のメディアは暗号化されるため（SRTP）、メディアおよびシグナリングはエンドツーエンドで暗号化されます（厳密にはすべてのコール レッグが暗号化されます）。C：図 7-9 を参照してください。

C：図 7-9　MRA エンドポイントのメディアおよびシグナリング暗号化



MRA での SIP TLS 認証に使用される証明書は、オンプレミス コールとは異なります。エンドポイントが MRA 経由で企業に接続している場合、エンドポイントは Expressway-E サーバの証明書を検証しますが、サーバではエンドポイントの証明書は確認されません。この TLS 接続では相互認証は使用されません。MRA クライアントの MIC 証明書または LSC は、存在しているかどうかに関係なく、検証されません。MRA クライアントのユーザのユーザ名とパスワードが、Cisco Unified CM ユーザ データベースまたは統合 LDAP サーバ（Jabber がシングル サインオンを使用して導入されている場合は IdP）と照合され、ユーザが認証されます。Expressway-C と Unified CM 間のコール レッグの場合、MRA エンドポイントが暗号化モードで設定されていると、Expressway-C は Unified CM との SIP TLS 接続を確立し、MRA エンドポイ

ントの代わりにそれ自体の証明書を送信します。Unified CM はこの証明書を受信すると、その MRA エンドポイントに対して設定されている電話セキュリティ プロファイルの名前が、Expressway-C 証明書の SAN 拡張の一部であるかどうかを確認します。

Business-to-Business（B2B）コミュニケーション

Business-to-Business（B2B）コミュニケーションでは、Expressway ともう一方の側の間の接続を暗号化する必要はありません。これは、Expressway ゾーン設定の [トランスポート（Transport）] パラメータに基づきます。[トランスポート（Transport）] が [TLS] に設定されている場合、証明書の検証は不要です。管理者は証明書の検証を無効にできます。無効にするには、Expressway ゾーン設定の [TLS 検証（TLS verify）] パラメータを [オフ（Off）] に設定します。

Cisco IOS Gateway と Cisco Unified Border Element

Cisco IOS Gateways と Cisco Unified Border Element では TLS と SRTP がサポートされています。SRTP の場合、デフォルトでは暗号スイート AES_CM_128_HMAC_SHA1_32 がネゴシエートされます。暗号スイート AES_CM_128_HMAC_SHA1_80 も設定できます。NGE 暗号スイートをサポートするには、SRTP パススルーを設定する必要があります。SRTP パススルーの主なデメリットは、RTP と SRTP 間のメディア インターワーキング（RTP と SRTP をそれぞれ別のコール レッグで処理）がサポートされていない点です。

デフォルトでは、Cisco IOS Gateway または Cisco Unified Border Element からコールが発信され、SRTP が要求されるが、着信側エンドポイントでは SRTP がサポートされていない場合、コールはドロップされます。相互運用性を最大限に引き出すには、**srtp fallback** と **srtp negotiate** を設定します。これらが設定されている場合、デフォルトでは、Cisco IOS Gateway または Cisco Unified Border Element はコールをドロップしませんが、代わりに SRTP から RTP にフォールバックします。

SRTP コマンドの詳細については、次のリンク先にある『*Cisco IOS Voice Command Reference*』を参照してください。
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/vcr4/vcr4-cr-book/vcr-s11.html

マルチクラスターに関する考慮事項

マルチクラスタ導入環境では、クラスタが同じデータセンター内にある場合、クラスタ間の暗号化は重要ではありません。ただし、クラスタが異なるデータセンターに分散しており、サービス プロバイダー リンクにより接続されている場合には、次のクラスタ間リンクで暗号化を有効にすることが推奨されます。

- SIP トランク

  クラスタ間の SIP トランクを暗号化します。CA により署名された CallManager 証明書と CA 証明書（またはルート CA 証明書）がすでに CallManager 信頼ストアに格納されている場合、クラスタ間 SIP トランク暗号化のために追加の証明書関連操作を行う必要はありません。

- クラスタ間検索サービス（ILS）接続

  クラスタ間検索サービス（ILS）接続を暗号化します。ILS 暗号化を有効にするには、認証に TLS 証明書（tomcat 証明書）を使用し、承認にすべてのクラスタで共有パスワードを使用することが推奨されます。CA により署名された tomcat 証明書と CA 証明書（またはルート CA 証明書）がすでに tomcat 信頼ストアに格納されている場合、ILS 暗号化を有効にするために追加の証明書関連操作を行う必要はありません。

- Location Bandwidth Manager（LBM）リンク

  コール アドミッション制御（CAC）が設定されている場合、クラスタ間 LBM リンクも暗号化する必要があります。LBM 暗号化も tomcat 証明書に基づいており、CA により署名された tomcat 証明書と CA 証明書がすでに tomcat 信頼ストアに格納されている場合、LBM 暗号化を有効にするために追加の証明書関連操作を行う必要はありません。

コラボレーション セキュリティーのハイ アベイラビリティーに関する考慮事項

統一された CM の信頼検証サービス（TVS）には高可用性が備わっています。TVS はすべての統一された CM ノードでネットワークサービスとして動作します。エンドポイントは、Cisco Unified CM グループで設定されている Unified CM コール処理ノードと同じ TVS ノードを使用します。そのプライマリ TVS サーバはプライマリ コール処理サブスクライバであり、そのバックアップ TVS サーバはバックアップ コール処理サブスクライバです。

Unified CM パブリッシャには、セキュリティ コンポーネントに関する重要な役割があります。パブリッシャは、電話が接続する CAPF サービスを実行します。したがって、パブリッシャがダウンすると、CAPF 操作が不可能になります。たとえば、ローカルで有効な証明書（LSC）をインストールできなくなります。マルチサーバ証明書を生成し、混合モードを有効 / 無効にする操作もパブリッシャで実行され、このためにはパブリッシャが稼働している必要があります。

コラボレーション セキュリティ キャパシティ プランニング

暗号化を有効にすると、サーバの CPU およびメモリの使用率が多少増加します。ただし Cisco Unified Border Element を除き、「サイジング」で説明する簡易サイジング導入は、暗号化を有効にする操作の影響を受けません。

展開

ここでは、証明書の管理と暗号化機能の導入について説明します。まず、最初に実行する必要がある証明書の管理について説明します。すべての証明書が用意されたら、暗号化を有効化および設定できます。

ここでは、企業のコラボレーション向けプリファード アーキテクチャの次のコンポーネントの導入について説明します。

- Cisco Unified CM および IM と Presence とエンドポイント
- Cisco Unity Connection
- コラボレーション エッジ（Cisco Expressway、Cisco IOS Gateway、および Cisco Unified Border Element）
- 会議
- コラボレーション管理サービス

Cisco Unified CM および IM と Presence とエンドポイント

Cisco Unified CM および IM と Presence とエンドポイントで行う設定の概要を次に示します。

- 暗号スイートの設定
- サーバー証明書の生成と管理
- 証明書のモニタリング
- LDAP over SSL の設定
- SIP トランクの暗号化

エンドポイントでのメディアおよびシグナリング暗号化のため、次の設定を行います。

- 混合モードの設定
- エンドポイントのメディアおよびシグナリング暗号化のための CAPF 登録と設定
- セキュア SRST の設定

暗号スイートの設定

主要なセキュア接続は 3 種類あり、接続ごとに暗号エンタープライズ パラメータがあります。

- HTTPS

  「暗号スイートのサポート」で説明したように、[HTTPS 暗号（HTTPS Ciphers）] エンタープライズ パラメータではデフォルト値の [RSA 暗号のみ（RSA Ciphers only）] を使用することが推奨されます。ECDSA 暗号を有効にするには、この設定を [サポートされているすべての EC および RSA 暗号（All Supported EC and RSA Ciphers）] に変更します。

- TLS（シグナリング）

  「暗号スイートのサポート」で説明したように、[TLS 暗号（TLS Ciphers）] エンタープライズ パラメータにはデフォルト値の [すべての RSA 暗号を優先（All Ciphers RSA Preferred）] を使用することが推奨されます。ただし特定の要件がある場合、たとえば弱い暗号スイートのネゴシエーションを無効にする必要がある場合や、RSA 暗号スイートよりも ECDSA を優先してネゴシエートしたい場合などには、[TLS 暗号（TLS Ciphers）] エンタープライズ パラメータを変更できます。

- SRTP（メディア）

  「暗号スイートのサポート」で説明したように、[SRTP 暗号（SRTP Ciphers）] エンタープライズ パラメータではデフォルト値の [サポートされているすべての暗号（All Supported Ciphers）] を使用することが推奨されます。ただし特定の要件がある場合、たとえば弱い暗号スイートのネゴシエーションを無効にする必要がある場合などには [SRTP 暗号（SRTP Ciphers）] エンタープライズ パラメータを変更し、[最も強力 - AEAD AES-256 GCM 暗号のみ（Strongest - AEAD AES-256 GCM cipher only）] または [中程度 - AEAD AES-256 GCM、AEAD AES-128 GCM 暗号のみ（Medium - AEAD AES-256 GCM, AEAD AES-128 GCM ciphers only）] に設定できますが、一部のエンドポイントとサーバではこれらの暗号スイートがサポートされていないことに注意してください。詳細については、暗号スイートのサポートを参照してください。

サーバー証明書の生成と管理

「自己署名証明書の代わりの CA 署名付き証明書」で説明したように、ほとんどの証明書には CA 署名付き証明書を使用することが推奨されます。CA により署名される証明書のリストについては、C：表 7-5 を参照してください。CA の署名が不要な証明書は、変更または再生成する必要はありません。

CA 署名付き証明書を発行する全体的な手順を次に示します。

1．ルート CA 証明書をアップロードするまたは証明書チェーンを対応するサーバの信頼ストアにアップロードします。

2．証明書署名要求（CSR）を生成する希望する証明書の証明書署名要求（CSR）を生成します。

3．CSR をダウンロードする。

4．署名 CA に CSR を送信する。

5．適切なタイプを使用して新しい CA 署名付き証明書をアップロードする。

Unified CM、IM and Presence Service、および Unity Connection では、これらの操作はシステムの OS 管理 Web インターフェイスから実行します。

手順の詳細については、次のリンク先にある『*Security Guide for Cisco Unified Communications Manager*』の最新版を参照してください。
https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

1. ルート CA 証明書をアップロードする

最初に、ルート CA 証明書（パブリック CA を使用する場合は証明書チェーン）をインポートします。Unified CM と IM and Presence Service では、この操作をパブリッシャでのみ実行する必要があります。これにより、証明書はクラスタ内の他のノードの信頼ストアに自動的に配布されます。

[OS の管理（OS Administration）] ページに移動し、[セキュリティ（Security）] > [証明書の管理（Certificate Management）] > [証明書 / 証明書チェーンのアップロード（Upload Certificate/Certificate chain）] を選択して、CA 署名付き証明書を発行するサービスの信頼ストアにルート CA 証明書（または証明書チェーン）をアップロードします。RSA 証明書と ECDSA 証明書は同じ信頼ストアを共有します。C：表 7-8 に、CA 証明書をインポートする必要がある信頼ストアを示します。

C：表 7-8　Unified CM および IM and Presence Service の CA 証明書をインポートする信頼ストア

製品	CA 証明書をアップロードする必要があるノード
Unified CM	tomcat-trust
Unified CM	callManager-trust
IM and Presence Service	tomcat-trust
IM and Presence Service	cup-xmpp-trust

2. 証明書署名要求（CSR）を生成する

証明書署名要求（CSR）を生成するには、[OS の管理（OS Administration）] ページに進み、[セキュリティ（Security）] > [証明書の管理（Certificate Management）] > [CSR の生成（Generate CSR）] を選択します。

一部の証明書ではマルチサーバ機能がサポートされています。リストについては C：表 7-6 を参照してください。これらの証明書の場合、パブリッシャで CSR を生成し、[CSR] ページの [配布（Distribution）] フィールドで [マルチサーバ（SAN）（Multi-Server (SAN)）] を選択します。マルチサーバ証明書の CSR を生成する場所については、C：表 7-9 を参照してください。その他の証明書の場合、各ノードで CSR を発行し、[配布（Distribution）] フィールドではデフォルト値を使用します。

C：表 7-9　マルチサーバ証明書の CSR

製品	証明書	CSR を生成する場所
Unified CM and IM and Presence Service	tomcat	Unified CM パブリッシャ
Unified CM	CallManager	Unified CM パブリッシャ
IM and Presence Service	xmpp	IM and Presence Service パブリッシャ
IM and Presence Service	xmpp-s2s	IM and Presence Service パブリッシャ

通常は、[コモンネーム（Common Name）] フィールドのデフォルト値を変更する必要はありません。デフォルトでは、このフィールドには CSR を生成するノードの FQDN が設定されています。マルチサーバ証明書では、FQDN のホスト名部分の後に「-ms」が付加されます。

通常は、[キー長（Key Length）] に 2048 ビット以上、[ハッシュ アルゴリズム (Hash Algorithm)] に [SHA256] を使用することが推奨されます。したがってこれらのフィールドではデフォルト値を使用できます。

3. CSR をダウンロードする

4. 署名 CA に CSR を送信する

CA が対応する証明書を生成します。

キー使用法拡張機能と拡張キー使用法拡張機能により、キーの使用目的が限定されます。発行された証明書での X.509 キー使用法と X.509 拡張キー使用法が CSR の要求に一致していることを確認します。一般的な問題として、証明書を発行および署名するエンタープライズ CA が、適切な証明書テンプレートを使用して設定されておらず、適切なキー使用法拡張機能を含む証明書を発行しないことがあります。たとえば、Unified CM tomcat 証明書には「TLS Web クライアント認証」拡張キー使用法（EKU）が含まれている必要があります。TLS Web クライアント EKU が含まれているテンプレートを使用しないと、キー使用法が正しくないことが原因で、クラスタ間検索サービス（ILS）やユーザ データ ストア（UDS）などのサーバ間通信のための TLS 接続の設定が失敗します。C：表 7-10 に、キー使用法の要件を示します。原則として、CSR を生成し、CSR に指定されているキー使用法と拡張キー使用法を確認して、エンタープライズ CA に、正しいキー使用法と拡張キー使用法が含まれている証明書テンプレートがあるかどうかを確認し、ない場合には新しい証明書テンプレートを作成します。CSR を CA に送信し、証明書に戻ったら、キー使用法と拡張キー使用法が証明書に含まれていることを確認します。

C：表 7-10　キー使用法と拡張キー使用法の要件

製品	証明書	X509v3 キー使用法	X509v3 拡張キー使用法
Unified CM and IM and Presence Service	tomcat	デジタル署名、 キーの暗号化、 データの暗号化	TLS Web サーバ認証、 TLS Web クライアント認証
Unified CM	CallManager	デジタル署名、 キーの暗号化、 データの暗号化	TLS Web サーバ認証、 TLS Web クライアント認証
Unified CM	CAPF	デジタル署名、 証明書の署名、	TLS Web サーバ認証
IM and Presence Service	cup-xmpp	デジタル署名、 キーの暗号化、 データの暗号化	TLS Web サーバ認証、 TLS Web クライアント認証
IM and Presence Service	cup-xmpp-s2s	デジタル署名、 キーの暗号化、 データの暗号化	TLS Web サーバ認証、 TLS Web クライアント認証

5. 適切なタイプを使用して新しい CA 署名付き証明書をアップロードする

証明書をアップロードし、[証明書の目的（Certificate Purpose）] フィールドで対応する値を選択します。たとえば、tomcat 証明書をアップロードする場合は、[証明書の目的（Certificate Purpose）] フィールドで [tomcat] を選択します。

マルチサーバ証明書の場合、サブスクライバ ノードではなくパブリッシャ ノードでアップロード操作を実行します。

証明書のアップロードが完了したら、サービスを再起動する必要があります。GUI で、再起動するサービスが示されます。たとえば CallManager 証明書の場合、Cisco Tftp、Cisco CallManager、および Cisco CTIManager サービスを再起動する必要があります。

証明書のモニタリング

証明書の有効性のモニタリング

Unified CM で、サーバ証明書と LSC の有効性のモニタリングを有効にします。

[Cisco Unified CM OS の管理（Cisco Unified CM OS Administration）] > [セキュリティ（Security）] > [証明書モニタ（Certificate Monitor）] に移動し、通知を開始する有効期限前の日数と、通知頻度を入力します。電子メール通知を有効にします。サーバ証明書と LSC の両方がモニタされるようにするため、[LSC モニタリングの有効化（Enable LSC monitoring）] を選択します。

長期セッションの証明書有効性チェック

Unified CM は、長期接続で証明書の失効状況と有効期限状況を定期的に確認します。JTAPI/TAPI アプリケーションとの CTI 接続と LDAP 接続（および IPSec、ただし IPSec についてはこのドキュメントでは説明しません）についてこの確認を行います。

長期接続での証明書有効性チェック（有効期限および失効状況のチェック）を有効にするには、Unified CM エンタープライズ パラメータ [証明書有効性チェック（Certificate Validity Check）] をオンにします。

証明書の失効状況の検証の場合、[Cisco Unified CM OS の管理（Cisco Unified CM OS Administration）] > [セキュリティ（Security）] > [失効（Revocation）] で Online Certificate Status Protocol（OCSP）も設定します。

LDAP over SSL の設定

Microsoft Active Directory への接続に LDAP over SSL を設定します。

Unified CM で次の手順を実行します。

- LDAP 証明書が自己署名証明書の場合は、その証明書を Unified CM tomcat-trust ストアにインポートします。

  LDAP 証明書が CA 署名付き証明書の場合は、ルート CA 証明書を Unified CM tomcat-trust ストアにインポートします。LDAP 証明書の失効状況をモニタするために Online Certificate Status Protocol（OCSP）を設定している場合は、LDAP 証明書自体もインポートしてください。

- **Cisco Unified CM の管理** で、> **システム** > **LDAP** > **LDAP ディレクトリ**、また、**Cisco Unified CM の管理** > **システム** > **LDAP** > **認証**で、**LDAP ポート** を安全なポートに変更し、**TLS を使用** のオプションを有効（チェックボックスをオン）にします。通常、LDAP セキュアポートは、グローバルカタログ（GC）に対して同期する場合は「3268」、Windows Microsoft Active Directory ドメインコントローラ（DC）に対して同期する場合は「636」です。DC および GC の動作とポート番号に関する詳細については、Microsoft のドキュメンテーション https://technet.microsoft.com/en-us/library/cc978012.aspx[英語] を参照してください。

SIP トランクの暗号化

ここでは、Unified CM SIP トランクの暗号化を設定する方法を説明します。

既存のすべての SIP トランク セキュリティ プロファイルの [Unified CM の管理（Unified CM Administration）] インターフェイス（[システム（System）] > [セキュリティ（Security）] の下）で、SIP トランクのタイプ別にセキュア SIP トランク セキュリティ プロファイルを作成します。既存の SIP トランク セキュリティ プロファイルと同じパラメータ（「コール制御」の章を参照）を使用します（ただし C：表 7-11 にリストされているパラメータを除きます）。

C：表 7-11　セキュア SIP トランクの SIP トランク セキュリティ プロファイル パラメータ

パラメータ	値
[デバイスセキュリティ モード（Device Security Mode）]	暗号化
[着信転送タイプ（Incoming Transport Type）]	TLS
[発信転送タイプ（Outgoing Transport Type）]	TLS
[X.509 のサブジェクト名（X.509 Subject Name）]	リモート パーティのコモンネーム（CN）。次に例を示します。 • Unity Connection：us-cuc-ms.ent-pa.com（マルチサーバ証明書） • Cisco Meeting Server：cms.ent-pa.com（Cisco Meeting Server xmpp ドメイン名） • Expressway-C（Business-to-Business）：Expressway-C クラスタの CN • Cisco IOS Gateway および Cisco Unified Border Element：Cisco IOS Gateway と Cisco Unified Border Element により使用される CN のリスト • その他の Unified CM クラスタ：emea-cm-pub-ms.ent-pa.com（CallManager マルチサーバ証明書）
[着信ポート（Incoming Port）]	通常、5061 を入力します。Expressway への SIP トランクの場合、このプリファード アーキテクチャでは同一 Expressway クラスタでモバイルおよびリモート アクセス（MRA）と Business-to-Business（B2B）が有効であるため、Business-to-Business には異なるポートを使用します（ポート 5561 など）。

各 SIP トランクの設定では、C：表 7-12 に示す設定を使用します。

C：表 7-12　セキュア SIP トランクの SIP トランク設定

パラメータ	値
[SRTP を許可（SRTP Allowed）] このオプションが有効な場合、エンドツーエンド セキュリティを提供するため、ネットワークで暗号化 TLS を設定する必要があります。IPSec が設定されない場合、キーやその他の情報が公開されることになります。	選択（ボックスをオンにする）
[SIP 情報（SIP Information）] > [宛先（Destination）] - > [宛先ポート（Destination port）]	5061
[SIP トランク セキュリティ プロファイル（SIP Trunk security profile）]	前述の手順で作成した SIP トランク セキュリティ プロファイルを選択します。
[発信転送タイプ（Outgoing Transport Type）]	TLS

注　すべてのメッセージが暗号化されているわけではないため、Unified CM ノードと IM and Presence ノード間の Presence SIP トランクは、暗号化しないでください。

エンドポイントでのメディアおよびシグナリング暗号化

エンドポイントでメディアおよびシグナリング暗号化を設定するには、次の手順を実行します。

- SIP の OAuth トークンを有効にします (Jabber 用)。
- 混合モードを有効にします。
- メディアおよびシグナリング暗号化を有効にするため、暗号化モードで電話セキュリティ プロファイルを作成します。
- 電話セキュリティ プロファイルをエンドポイントに関連付け、MRA を介してのみ接続するエンドポイントを除き、電話機および TelePresence エンドポイントにローカルで有効な証明書 (LSC) をインストールします。

各手順の詳細については、以降の項で説明します。

SIP の OAuth トークンを有効にします

SIP に対して OAuth トークンを有効にすると、Jabber は LSC をインストールしたり、混合モードを有効にしたりせずに、メディアおよびシグナリングの暗号化を実行することができます。

SIP OAuth モードを有効にするには、次の CLI コマンドを入力します。

```
ユーティリティ sipOAuth モードの有効化
```

CallManager サービスを実行しているすべての統一された CM ノードで、このサービスを再起動します。混合モードを有効にする予定がある場合は、混合モードを有効にするまで、CallManager サービスの再起動を待っても構いません。

Jabber 使用する電話セキュリティ プロファイル

Unified CM クラスタの SIP OAuth モードを有効にした後、Jabber エンドポイントの電話セキュリティ プロファイルを作成します。

混合モードの有効化

混合モードを有効にする前に、Unified CM パブリッシャで CAPF サービスを有効にしておきます。混合モードを有効にした後で CAPF サービスを有効にする場合は、証明書信頼リスト（CTL）ファイルを更新する必要があります。

このドキュメントでは、CLI（コマンド ライン インターフェイス）（トークンレス）を使用して混合モードを有効にする方法を説明します。混合モードを有効にするには、次の手順を実行します。

- Unified CM パブリッシャに SSH で接続します。
- **utils ctl set-cluster mixed-mode** CLI コマンドを入力します。
- TFTP、CallManager、および CTIManager サービスを実行しているすべての Unified CM ノードで、これらのサービスを再起動します。

詳細については、次のリンク先にある『*Security Guide for Cisco Unified Communications Manager*』の最新版を参照してください。
https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

CAPF オンライン CA モード

LSC エンドポイント証明書が外部 CA によって署名される CAPF オンライン CA モードを選択した場合は、次の手順を実行します。

1。 CA 証明書 (またはトラストチェーン) を、統一された CM CAPF トラストにインポートします。

2。 まだ実行していない場合は、CA サーバの IIS 証明書またはその CA 証明書 (または信頼チェーン) を統一された CM tomcat-trust にインポートします。

3。 一部の電話機または TelePresence エンドポイントが暗号化モードで設定されている場合は、CA 証明書 (または信頼チェーン) を Unified CM CallManager-trust にインポートします (まだ実行していない場合)。

4。 統一された CM パブリッシャで CAPF サービスパラメータを設定します。次の設定を使用します。

フィールド	設定
エンドポイントへの証明書発行者	オンライン CA
オンライン CA ホスト名	Microsoft IIS サービスによって使用される証明書内の共通名 (CN)。通常、これは FQDN です。
オンライン CA ポート	通常は 443
オンライン CA テンプレート	Microsoft CA で定義された証明書テンプレート名
オンライン CA タイプ	**Microsoft CA**
オンライン CA ユーザ名	上記で指定した証明書テンプレートを使用して証明書を発行するための適切な権限を持つユーザのユーザ名
オンライン CA パスワード	上記で指定した証明書テンプレートを使用して証明書を発行するための適切な権限を持つユーザのパスワード

5。 統一された CM パブリッシャで Cisco Certificate Enrollment Service をアクティブにします (まだ未設定の場合)。

6。 CAPF サービスを再起動します。

電話セキュリティ プロファイルと LSC のインストール

設定プロセスのこの時点で、サーバ証明書が生成され、Unified CM が混合モードになっています。

次に、エンドポイントでのメディアおよびシグナリング暗号化を有効にするため、[デバイス セキュリティ モード（Device Security Mode）] を [暗号化（Encrypted）] に設定して電話セキュリティ プロファイルを作成します。電話セキュリティ プロファイルには次の考慮事項が適用されます。

- 電話セキュリティ プロファイルの作成時には、[電話セキュリティ プロファイルのタイプ (Phone Security Profile Type)] として [ユニバーサル デバイス テンプレート（Universal Device Template）] を使用します。このタイプの電話セキュリティ プロファイルは特定の電話モデルに固有ではなく、すべての電話モデルに適用できます。これにより、設定と証明書管理がシンプルになります。電話モデルに固有の電話セキュリティ プロファイルの場合、新しいタイプの電話の追加時に、新しい電話セキュリティ プロファイルを作成する必要があります。また、MRA エンドポイントが新しい電話セキュリティ デバイス プロファイルを使用している場合は、この新しい電話セキュリティ デバイス プロファイル名を SAN として追加して、Expressway-C 証明書を再生成する必要があります。汎用電話セキュリティ プロファイルの場合、新しいデバイス タイプが追加されるたびに新しい電話セキュリティ プロファイルを作成することや、新しい Expressway-C 証明書を再生成することは不要です。

- 電話セキュリティ プロファイルは、MRA エンドポイントと非 MRA エンドポイントの両方に関連付けることができます。ただし、電話セキュリティ プロファイルが MRA エンドポイントに関連付けられている場合は、そのプロファイル名が FQDN 形式であることを確認してください。
- メディアおよびシグナリングの暗号化の使用が推奨されるため、[デバイス セキュリティ モード（Device Security Mode）] の設定を [暗号化（Encrypted）] に設定してください。
- TFTP 設定ファイルの暗号化を有効にするには、[TFTP 暗号化設定（TFTP Encrypted Config）] オプションを選択します（ボックスをオンにします）。「アーキテクチャー」で説明したように、オンプレミス エンドポイントに対し暗号化 TFTP 設定を有効にし、MRA 経由で接続するエンドポイントに対し暗号化 TFTP 設定を無効にすること（および機密情報が電話のページに入力されていないことを確認すること）が推奨されます。また、**TFTP 暗号化設定**では、エンドポイントに証明書がインストールされている必要があります (MIC または LSC)。
- Jabber エンドポイントで使用される電話セキュリティプロファイルの **OAuth 認証の有効化（Enable OAuth Authentication**）チェックボックスをオンにします (C：表 7-14 を参照)。
- 電話セキュリティ プロファイルは、エンドポイントが CAPF に接続するときに使用される認証モードも指定します。通常、認証モードとして [既存の証明書 (LSC を優先)（By Existing Certificate (precedence to LSC)）] を使用することが推奨されます。この設定では、エンドポイントに MIC のみが含まれている場合には既存の MIC が CAPF への認証に使用されます。エンドポイントに LSC が含まれている場合は、（MIC 証明書の有無にかかわらず）LSC が使用されます。したがって、これは MIC または LSC のいずれかが含まれているエンドポイントでは適切に機能します。

  エンドポイントに MIC と LSC が含まれていない場合、LSC がインストールされるまでは認証モードを使用できません。代わりに、最初の LSC インストールでは認証文字列またはヌル ストリングに基づく認証を使用する必要があります。認証文字列に基づく認証のほうが安全ですが、管理者が認証文字列をデバイス設定ページに入力し、ユーザがエンドポイントに認証文字列を手動で入力する必要があります。この操作が現実的ではない場合は、ヌル ストリングに基づく認証を選択できますが、この認証では、最初の CAPF 登録時にすべてのエンドポイント認証が実質的に迂回されます。LSC のインストールが完了したら、認証モードが [既存の証明書 (LSC を優先)（By Existing Certificate (precedence to LSC)）] の電話セキュリティ プロファイルを割り当てる必要があります。
- 電話セキュリティ プロファイルの [キー順序（Key Order）] 設定で [RSA のみ（RSA Only）] を選択し、[RSA キー サイズ（RSA Key Size）] 設定で [2048] 以上を選択します。

上記の事項を考慮して、3 つの電話セキュリティ プロファイルを作成します。C：表 7-13 に、各プロファイルの相違点を示します。その他の設定には、前述の値を使用します。

C：表 7-13　　設定する電話セキュリティ プロファイル

電話セキュリティ プロファイル名の例	認証モード（CAPF 登録）	TFTP 暗号化設定ファイル	OAuth 認証
UDT-Encrypted-LSC-TFTPenc.ent-pa.comf	既存の証明書（LSC の優先）	イネーブル	無効
UDT-Encrypted-LSC.ent-pa.com	既存の証明書（LSC の優先）	無効	ディセーブル
UDT-Encrypted-NullString.ent-pa.com	Null 文字列または 認証ストリング	無効	ディセーブル
UDT-Jabber-SIPOAuth	Null 文字列または 認証ストリング	無効	イネーブル

3 つの電話セキュリティ プロファイルの設定が完了したら、**Cisco Unified CM の管理 > デバイス > 電話**に移動し、これらのプロファイルをエンドポイントに関連付け、エンドポイントのタイプに応じて LSC のインストールに進みます。C：表 7-14 に、エンドポイントのタイプ別の実行アクションを示します。

C：表 7-14　電話セキュリティ プロファイルの関連付けと LSC のインストール

エンドポイントのタイプ	手順（電話セキュリティ プロファイルの関連付けと LSC のインストール）
Cisco IP Phone および Cisco TelePresence エンドポイント (MIC 対応)	• **UDT-Encrypted-LSC-TFTPenc.ent-pa.com**（TFTP 設定ファイルの暗号化用）または **UDT-Encrypted-LSC.ent-pa.com**（TFTP 設定ファイルの暗号化なしの場合）をエンドポイントに関連付けます。 • LSC をインストールします。
Jabber クライアント (オンプレミスまたは MRA)	• **UDT-Jabber-SIPOAuth の関連付け**
MRA ハードウェア エンドポイント	• **UDT-Encrypted-NullString.ent-pa.com の関連付け**

電話セキュリティ プロファイルを電話に関連付けるには、電話の設定ページに移動し、[デバイス セキュリティ プロファイル（Device security profile）] 設定で必要なセキュリティ プロファイルを選択します。

LSC のインストールを設定するには、電話の設定ページの [証明書の操作（Certificate Operation）] フィールドで [インストール / アップグレード（Install/Upgrade）] を選択します。電話の設定ページの [Certification Authority Proxy Function（CAPF）の情報（Certification Authority Proxy Function (CAPF) Information）] セクションには、電話セキュリティ プロファイルの CAPF 情報が自動的に取り込まれます。[操作の完了期限 (Operation Completes By)] フィールドがまだ設定されていない場合には、このフィールドを将来の日付に更新する必要があります。

電話セキュリティ プロファイルの関連付けと LSC インストールの設定（オプション）が完了したら、設定を保存します。設定を適用するか、またはエンドポイントをリセットします。この時点で、電話セキュリティ プロファイルが適用されます。LSC インストールを設定した場合、エンドポイントが LSC を取得します。（認証文字列を使用する場合は、LSC インストールを続行するためにユーザが [更新（Update）] ボタンを押す必要があることがあります。）また、エンドポイントでメディアおよびシグナリング暗号化も設定する必要があります。

Tip　電話セキュリティ プロファイルの割り当てと CAPF 登録の実行には、Cisco Unified Communications Manager 一括管理ツール（BAT）または Cisco Prime Collaboration プロビジョニングを使用できます。

通常、Jabber エンドポイントに LSC をインストールする必要はありません。SIP OAuth モードが有効になっている場合、暗号化されたメディアとシグナリングを実行するために、Jabber は LSC を必要としません。TFTP 設定ファイルの暗号化をサポートするために、Jabber は引き続き LSC を必要とします。ただし Jabber で LSC 証明書を管理するには、追加の管理オーバーヘッドが必要になるため、通常は Jabber エンドポイントで TFTP 設定ファイルの暗号化を展開することは推奨されません。したがって、Jabber に LSC 証明書をインストールする必要はありません。

Survivable Remote Site Telephony（SRST）の有効化

Survivable Remote Site Telephony（SRST）では、次の手順を使用します。

- エンタープライズ CA を使用して、SRST ルータの証明書に署名します。Cisco IOS ルータでの証明書の管理の詳細については、「Cisco IOS Gateway と Cisco Unified Border Element」を参照してください。
- SRST が LSC を認証できるように、エンドポイント LSC に署名したエンティティに対応する信頼証明書を SRST ルータにインポートします。CAPF を使用して LSC を発行する場合、これが CAPF 証明書となります。外部 CA を使用して LSCs を発行する場合、これが CA 証明書 (または信頼チェーン証明書) となります。
- **SRST はセキュアか？**をオンにする（チェックボックスをオンにする）ことで、セキュア SRST が有効になったことを確認します。**Cisco Unified CM の管理 > システム > SRST** の SRST リファレンス設定で、

詳細については、次のリンク先にある『*Security Guide for Cisco Unified Communications Manager*』の最新版を参照してください。
https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

Cisco Unity Connection

ここでは次世代暗号化（NGE）を使用した Cisco Unity Connection のメディアおよびシグナリング暗号化について説明します。この暗号化では、Unity Connection のルート証明書および SIP 証明書の代わりに Unity Connection tomcat 証明書が使用されます。

Unity Connection でメディアおよびシグナリングのために NGE を有効にする全体的な手順は次のとおりです。

- Unity Connection で証明書を管理します。
- Unity Connection でテレフォニー統合のために暗号化を設定します。
- Unified CM で、Unity Connection への SIP トランクの暗号化を有効にします。

最初に Unity Connection で証明書を管理します。Unity Connection で次の手順を実行します。

- Unity Connection パブリッシャ ノードで、ルート CA 証明書（または証明書チェーン）を Unity Connection tomcat-trust ストアにアップロードします。同様に、ルート CA 証明書を CallManager-trust ストアにアップロードします（CA 署名付き CallManager 証明書に必要です）。これらの証明書は、Unity Connection サブスクライバ ノードの信頼ストアに自動的に反映されます。
- Unity Connection パブリッシャ ノードで、マルチサーバ tomcat 証明書を取得してエンタープライズ CA により署名するため、CSR を発行します。たとえば、コモンネームが us-cuc-ms.ent-pa.com であるとします。X509v3 キー使用法拡張機能は、デジタル署名、キーの暗号化、およびデータの暗号化です。X509v3 拡張キー使用法拡張機能は、TLS Web サーバ認証および TLS Web クライアント認証です。これはマルチサーバ証明書であるため、この証明書を Unity Connection パブリッシャにインストールすると、自動的に Unity Connection サブスクライバにもインストールされます。この新しい tomcat 証明書のインストールが完了したら、両方の Unity Connection ノードで Tomcat Service を再起動します。

CA 証明書のアップロードまたは CA 署名付き tomcat 証明書の発行の詳細については、「Cisco Unified CM および IM と Presence」を参照してください。手順は Unity Connection の場合と同じです。

Cisco Unified CM と Unity Connection で同じ CA を使用することを前提としているため、Unified CM tomcat-trust ストアに CA 証明書をインポートする必要はありません。この証明書はすでにこの信頼ストアに格納されているはずです。

次に、Unity Connection で暗号化を設定にします。

- **Cisco Unity Connection 管理 > テレフォニー統合 > セキュリティ > SIP セキュリティ プロファイル**で、次の設定を使用して新しい SIP セキュリティ プロファイルを作成します。

フィールド	設定
ポート	5061
TLS を実行（Do TLS）	チェックボックスをオンにする

  この SIP セキュリティ プロファイルには、表示名 **5061/TLS** が自動的に割り当てられます。

- **テレフォニー統合 > ポート グループ**から、ポート グループ **PhoneSystem-1** を選択し、次の設定を使用してポート グループを変更します。

フィールド	設定
SIP セキュリティ プロファイル（SIP Security Profile）	前の手順で作成した SIP セキュリティ プロファイル（**5061/TLS**）を選択する
次世代暗号化の有効化（Enable Next Generation Encryption）	チェックボックスをオンにする
セキュア RTP（Secure RTP）	チェックボックスをオンにする

- [ポート グループ（Port Group）] ページで [編集（Edit）] > [サーバ（Servers）] に移動します。SIP サーバの設定で、TLS ポートとして 5061 が設定されていることを確認します。TFTP サーバの設定で、Unified CM TFTP サーバが設定されていることを確認します。このようにして、ポート グループがリセットされると、Unity Connection の CallManager-trust ストアに CallManager 証明書が自動的にダウンロードされます。

次に、Unity Connection への Unified CM SIP トランクで暗号化を有効にします。

- 暗号化と適切な X.509 サブジェクト名が設定された SIP トランク セキュリティ プロファイルがすでに作成されている必要があります（C：表 7-11 を参照）。Unity Connection への SIP トランクに対しこの SIP トランク セキュリティ プロファイルを選択します。

この時点で、Unified CM では暗号化 SIP トランクが完全に動作するはずです。電話からボイスメール ポートへの接続時には、メディアおよびシグナリングも暗号化される必要があります。LDAP over SSL も設定する必要があります。[Cisco Unity Connection の管理（Cisco Unity Connection Administration）] > [システム設定（System Settings）] > [LDAP] に移動し、[LDAP ディレクトリの設定（LDAP Directory Configuration）] ページと [LDAP 認証（LDAP Authentication）] ページで、[TLS を使用（Use TLS）] を選択し、ポート 636 を設定します（Unified CM での LDAP over SSL の設定と同様）。

コラボレーション エッジ

ここでは、Cisco Expressway、Cisco IOS Gateway、および Cisco Unified Border Element での証明書の管理と暗号化の導入の概要を説明します。

Cisco Expressway

ここでは、0、次に暗号化に使用する設定について説明します。

Cisco Expressway 証明書の管理

「アーキテクチャー」で説明したように、Cisco Expressway ソフトウェアの新規インストールには、信頼された一時 CA と、その一時 CA が発行するサーバ証明書が付属しています。一時 CA 証明書を、信頼する CA 証明書に置き換え、Expressway の CA 署名付き証明書を生成します。「アーキテクチャー」で説明したように、Expressway-C 証明書経の署名にはエンタープライズ CA を使用し、Expressway-E 証明書への署名にはパブリック CA を使用します。Expressway-E でサポートされているパブリック CA のリストについては、cisco.com にあるエンドポイントに関するドキュメントを参照してください。たとえば、次の Web サイトから入手できる『*Certificate Authority Trust List*』を参照してください。
https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-technical-reference-list.html.

Cisco Expressway の証明書の管理を導入するには、以降の項で説明する手順を使用します。

CA ルート証明書をアップロードする。

[信頼された CA 証明書（Trusted CA certificate）] ページに移動します（[メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [信頼された CA 証明書（Trusted CA certificate）]）。このページで、既存の証明書を新しいルート CA 証明書または証明書チェーンに置き換えます。これ以降の CA 証明書は、既存の CA 証明書リストに追加されます。C：表 7-15 に示されている CA 証明書をアップロードします。この操作は、Expressway-C クラスタと Expressway-E クラスタの両方の各 Expressway ノードで行う必要があります。

C：表 7-15　Cisco Expressway 信頼ストア

Expressway-C 信頼ストア	Expressway-E 信頼ストア
• Expressway-E 証明書を署名したパブリック CA からのルート CA 証明書 • Unified CM CallManager 証明書と Expressway-C 証明書に署名するエンタープライズ CA からのルート CA 証明書（または証明書チェーン）	• Expressway-E 証明書を署名したパブリック CA からのルート CA 証明書（または証明書チェーン） • Unified CM CallManager 証明書と Expressway-C 証明書に署名するエンタープライズ CA からのルート CA 証明書 • Business-to-Business（B2B）コミュニケーションまたはクラウド コミュニケーションでは、他のビジネスのルート CA 証明書

各 Expressway ノードの証明書署名要求（CSR）を生成する。

1。 **メンテナンス > セキュリティ > サーバ証明書**に移動します。

2。 CSR を作成します。

IM and Presence のチャット ノード エリアスのサブジェクト代替名（SAN）拡張は自動的に追加されます。Expressway ノードが Expressway-C ノードまたは Expressway-E ノードのいずれであるかと、導入されている機能によっては、SAN 拡張の追加が必要となることがあります。詳細については、C：表 7-16 を参照してください。

C：表 7-16　CSR に追加するサブジェクト代替名（SAN）

サブジェクト代替名（SAN）として追加する項目	次の目的で CSR を生成する場合に追加する：		
	モバイル & リモート アクセス	**XMPP フェデレーション**	**Business-to-Business（B2B）コール**
Expressway-C クラスタ名	Expressway-C でのみ	Expressway-C でのみ	Expressway-C でのみ
Unified CM 登録ドメイン[1]	Expressway-E でのみ必要	–	–
XMPP フェデレーション ドメイン	–	Expressway-E でのみ必要	–
IM and Presence のチャット ノード エイリアス（フェデレーテッド グループ チャット）	–	Expressway-C と Expressway-E の両方で必要	–
Unified CM 電話セキュリティ プロファイル名（FQDN 形式）[2]	Expressway-C でのみ必要	–	–

1. Expressway 設定と Expressway-E 証明書で使用されている Unified CM 登録ドメインは、サービス検出中に MRA クライアントが _collab-edge DNS SRV レコードを検索するときに使用するドメインです。Unified CM 登録ドメインにより、Unified CM での MRA 登録が有効になります。この例では、これらのドメインは Unified CM で SIP URI に使用されているドメインと一致します。ただしこれらのドメインは主にサービス検出用であるため、Unified CM で使用される SIP ドメインと一致する必要はありません。
2. SIP OAuth が使用されるため、SAN の Jabber に使用される電話セキュリティプロファイル名を、Expressway-C 証明書に追加する必要はありません（C：表 7-14 を参照）。

詳細については、次のリンク先にある『*Cisco Expressway Certificate Creation and Use Deployment Guide*』の最新版を参照してください。
https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html

前述したように、操作を簡単にするため、ユニバーサル デバイス テンプレート（UDT）の使用が推奨されます。これにより、Expressway-C SAN で電話セキュリティ プロファイル名の長いリストを入力する必要がなくなります。この章の例では、CSR の [Unified CM Phone セキュリティ プロファイル名（Unified CM phone security profile names）] フィールドに、UDT-Encrypted-LSC-TFTPenc.ent-pa.com、UDT-Encrypted-RSA-LSC.ent-pa.com、および UDT-Encrypted-AuthString.ent-pa.com（または UDT-Encrypted-NullString.ent-pa.com）を入力します。

3。 CSR をダウンロードして CA に送信します。これにより、CA 署名付き証明書を発行できるようになります。Base 64 形式を使用します。C：表 7-17 に示すように、CSR の X509v3 キー使用法と X509v3 拡張キー使用法が CA から発行される証明書に含まれています。

C：表 7-17　Cisco Expressway のキー使用法と拡張キー使用法

証明書	X509v3 キー使用法	X509v3 拡張キー使用法
Expressway-C および Expressway-E	デジタル署名、キーの暗号化	TLS Web サーバー認証、TLS Web クライアント認証

4。 新規証明書のアップロード

Cisco Expressway の暗号化設定

MRA および XMPP フェデレーション

Expressway-C の Unified Communications ゾーンには TLS が使用されます。すべての Unified Communications サービス（Unified CM サーバ、IM and Presence Service ノード、Unity Connection）の [TLS 検証（TLS Verify）] が [オン（On）] に設定されていることを確認します。Unified Communications サービス ノードの検出を実行するときにこの設定を行います（[設定（Configuration）] > [Unified Communications]）。これにより、Expressway-C ノードが Unified Communications ノードの証明書を検証します。

Expressway-C と Expressway-E の間の Unified Communications トラバーサル ゾーンは、TLS 証明書検証を有効にし、メディア暗号化を設定して暗黙に設定されます。Expressway-C MRA トラバーサル ゾーンで [認証ポリシー（Authentication policy）] を [クレデンシャルを確認しない（Do not check credentials）] に設定します。Expressway-E MRA トラバーサル ゾーンで [認証ポリシー（Authentication policy）] を [クレデンシャルを確認しない（Do not check credentials）] に設定し、Expressway-C 証明書のクラスタ名（Expressway-C 証明書に SAN として追加）と一致する TLS 検証サブジェクト名を入力します。

MRA エンドポイントと Expressway-C 間のメディアおよびシグナリング トラフィックは常に暗号化されます。社内ネットワーク内部のコール レッグ（Expressway-C と Unified CM の間のシグナリングと、Expressway-C と内部エンドポイント間のメディア）を暗号化するため、暗号化モードの電話セキュリティ プロファイルを使用して MRA エンドポイントとネットワーク内部のエンドポイントを設定します。このようにすると、メディアとシグナリングがエンドツーエンドで暗号化されます（すべてのコール レッグが暗号化されます）。

XMPP フェデレーションでは、[セキュリティ モード（Security mode）] を [TLS（必須）（TLS Required）] に設定することが推奨されます。ただし、[TLS（オプション）（TLS optional）] に設定する必要があるケースがあります。たとえば [TLS（必須）（TLS Required）] は Cisco Webex Messenger でサポートされていないため、Cisco Webex Messenger を使用する企業との XMPP フェデレーションがある場合は [TLS（オプション）（TLS Optional）] を使用する必要があります。このシナリオでは、[クライアント側のセキュリティ証明書が必要（Require Client-side security certificates）] を [オフ（Off）] に設定する必要もあります。

Business-to-Business（B2B）コミュニケーション

「アーキテクチャー」で説明したように、Call Processing Language（CPL）ルールを設定します。

また、Expressway-C の Unified CM ネイバー ゾーンには C：表 7-18 に示す推奨設定を使用します。

C：表 7-18　Expressway-C Business-to-Business（B2B）Unified CM ネイバー ゾーンの設定

フィールド	設定
ポート	MRA と Business-to-Business（B2B）が同一 Expressway クラスタで有効になっている場合は、5061 以外のポート（ポート 5561 など）を使用します。
トランスポート（Transport）	TLS
TLS 検証（TLS Verify）	オン
メディア暗号化（Media Encryption）	ベストエフォート型

Expressway-C のトラバーサル ゾーンには、C：表 7-19 に示す推奨設定を使用します。

C：表 7-19　Expressway-C Business-to-Business（B2B）トラバーサル ゾーンの設定

フィールド	設定
ポート	5060、5061、およびその他のトラバーサル ゾーンで使用されているポート以外のポートを設定する必要があります。たとえば範囲 7*xxx* のポートを使用します。
トランスポート（Transport）	TLS
TLS 検証（TLS Verify）	オン
メディア暗号化（Media Encryption）	Auto

Expressway-E のトラバーサル ゾーンには、C：表 7-20 に示す推奨設定を使用します。

C：表 7-20　Expressway-E Business-to-Business（B2B）トラバーサル ゾーンの設定

フィールド	設定
ポート	Expressway-C でのトラバーサル ゾーンのポートと同じポート
トランスポート（Transport）	TLS
TLS 検証（TLS Verify）	オン
TLS 検証サブジェクト名（TLS Verify subject name）	Expressway-C クラスタ名の SAN
メディア暗号化（Media Encryption）	ベストエフォート型

Expressway-E のデフォルト ゾーン（着信コール）には、C：表 7-21 に示す推奨設定を使用します。

C：表 7-21　Expressway-E デフォルト ゾーンの設定

フィールド	設定
デフォルト ゾーンで相互 TLS を有効にする（Enable Mutual TLS on Default Zone）	オフ
認証ポリシー（Authentication policy）	クレデンシャルを確認しない
メディア暗号化（Media Encryption）	ベストエフォート型

Expressway-E の DNS ゾーン（発信コール）には、C：表 7-22 に示す推奨設定を使用します。

C：表 7-22　Expressway-E DNS ゾーンの設定

フィールド	設定
TLS 検証（TLS Verify）	オフ
メディア暗号化（Media Encryption）	ベストエフォート型

この時点で、Unified CM に SIP トランク セキュリティ プロファイルがすでに作成されている必要があります。詳細については、C：表 7-11 を参照してください。

Cisco IOS Gateway と Cisco Unified Border Element

ここでは最初に証明書の管理について説明し、続いて暗号化の設定について説明します。

証明書の管理

Cisco IOS Gateway と Cisco Unified Border Element（CUBE）でも、CA 署名付き証明書の使用が推奨されます。

証明書はさまざまな方法でアップロードできます。次の手順は、端末を使用した手動での証明書の登録に基づいています。証明書は PEM（Base 64）形式です。

1。 RSA キーペアを作成します。

例：**crypto key generate rsa general-keys label CUBE modulus 2048**

2。 Cisco Unified Border Element（CUBE）の PKI トラストポイントを作成します。

たとえば、端末を使用した手動での登録の場合は次のようにします。

```
crypto pki trustpoint CUBE-Certificate
 enrollment terminal pem
 subject-name CN=US-CUBE1.ent-pa.com
 revocation-check none
 rsakeypair CUBE
 hash sha256
```

3。 CA を使用してトラストポイントを認証し、CA 証明書を受け入れます。

基本的には、これによりそのトラストポイントの CA 証明書がアップロードされます。

例：**crypto pki authenticate CUBE-Certificate**

次に PEM 形式の CA 証明書を貼り付けます。

4。 CA サーバにトラストポイントを登録します。基本的には、これにより証明書署名要求（CSR）が作成されます。

例：**crypto pki enroll CUBE-Certificate**

この手順では、ルータのシリアル番号または IP アドレスをサブジェクト名に追加する必要はありません。

5。 この CSR に CA で署名します。

クライアントおよびサーバ Web 認証（X509v3 拡張キー使用法の TLS Web クライアント認証と TLS Web サーバ認証）のための CA テンプレートを使用します。

6。 生成された証明書を Cisco ゲートウェイにインポートします。

たとえば、端末を使用して PEM 形式の証明書を手動でインポートする場合は次のようにします。**crypto pki import CUBE-Certificate certificate**

Unified CM 証明書に CA による署名が付いていない場合、新しいトラストポイントを使用して、すべての Unified CM コール処理サブスクライバ ノードの Unified CM CallManager 証明書を、Cisco IOS Gateway および Cisco Unified Border Element（CUBE）にインポートする必要があります。

証明書の管理が完了したら、暗号化の設定に進みます。

暗号化設定

次の手順に従ってください。

1。 トラストポイントを Cisco IOS 音声プロセスに関連付けます。

次に例を示します。

```
sip-ua
 crypto signaling remote-addr [UnifiedCMIPaddress1] [mask] trustpoint
 CUBE-Certificate
 crypto signaling remote-addr [UnifiedCMIPaddress2] [mask] trustpoint
 CUBE-Certificate
```

2。 ダイヤルピアに対して TLS トランスポートを有効にします。

次に例を示します。

```
dial-peer voice 300 voip
 session protocol sipv2
 session transport tcp tls
```

3。 セキュア シグナリングを有効にします。

たとえば特定のデバイスとの間でのセキュア シグナリングを有効にするには、次のように設定します。

```
sip-ua
 crypto signaling remote-addr [UnifiedCMIPaddress1] [mask] trustpoint CUBE-Certificate
 crypto signaling remote-addr [UnifiedCMIPaddress2] [mask] trustpoint CUBE-Certificate
```

4。 SRTP を有効にします。

Cisco IOS Gateway と Cisco Unified Border Element（CUBE）では、AES_CM_128_HMAC_SHA1_80 と AES_CM_128_HMAC_SHA1_32（デフォルト）がサポートされています。AES_CM_128_HMAC_SHA1_80 を有効にするには、次のように設定します。

```
voice service voip
  sip
    srtp-auth sha1-80
```

SRTP パススルーでは、送信元デバイスと宛先デバイスの間でより強力な暗号を使用でき、Cisco Unified Border Element はパケットを転送するだけで処理は行いません。**srtp passthru** を設定するには、次のように設定します。

```
voice service voip
  srtp pass-thru
```

会議

ここでは、Cisco Meeting Server と Cisco TelePresence Management Suite（TMS）を会議サービス用に展開する方法を説明します。

Cisco Meeting Server

Cisco Meeting Server には、証明書管理用の Web インターフェイスがありません。証明書の管理には、メインボード管理プロセッサ（MMP）コマンドを使用します。

次に、Cisco Meeting Server 証明書を生成およびインストールする全体的な手順を示します。

- すべてのサービスを対象とする 1 つの CSR（および秘密キー）を生成します。この CSR で、SAN 拡張の CN フィールドに XMPP ドメインを指定します。また、SAN 拡張ですべての Cisco Meeting Server ノードの FQDN を指定します。SFTP 経由で秘密キーをダウンロードします。エンタープライズ CA で CSR を署名します。拡張キー使用法 [サーバ認証（Server Authentication）] と [クライアント認証（Client Authentication）] が存在していることを確認します。このドキュメントでは、この証明書を*共有証明書*と呼びます。
- ローカル データベースなしで Call Bridge サービスを実行する Cisco Meeting Server を導入するには、**CN=postgres** を使用してデータベース クライアントに CSR（および秘密キー）を生成します。SFTP 経由で秘密キーをダウンロードします。エンタープライズ CA で CSR を署名します。拡張キー使用法 [クライアント認証（Client Authentication）] が存在していることを確認します。
- 新しい共有 CA 署名付き証明書（および関連付けられている秘密キー）と CA 証明書を SFTP 経由ですべての Cisco Meeting Server ノードにアップロードします。また、新しいデータベース クライアント CA 署名付き証明書（および関連付けられている秘密キー）を、ローカル データベースなしで Call Bridge サービスを実行している Cisco Meeting Server ノードにアップロードします。
- 証明書をインストールします。
  - Web 管理画面：このサービスを実行する各ノードで、このサービスを無効にし、共有証明書と関連秘密キーをインストールし、サービスを有効にします。
  - Call Bridge：このサービスを実行する各ノードで、共有証明書と関連秘密キーをインストールし、サービスを再始動します。
  - XMPP：このサービスを実行する各ノードで、このサービスを無効にし、共有証明書と関連秘密キーをインストールし、サービスを有効にします。
  - Web Bridge：このサービスを実行する各ノードで、共有証明書、関連秘密キー、および CA 証明書をインストールし、サービスを再始動します。
  - データベース サーバ：ローカル データベースが存在する各ノードで、データベース クラスタリングが有効になっていないことを確認してから、共有証明書と関連秘密キーをインストールします。この操作が完了したら、ノード間のクラスタリング構成を有効にできます。
  - データベース クライアント：Call Bridge サービスを実行し、ローカル データベースがない各ノードで、データベース クラスタリングが有効になっていないことを確認してから、データベース クライアント証明書と関連秘密キーをインストールします。この操作が完了したら、ノード間のクラスタリング構成を有効にできます。

以降の項では、上記の手順の例を示します。これらの例では、エンタープライズ CA により署名された共有 Cisco Meeting Server 証明書が CAsignedCluster.cer、これに対応する秘密キーが CAsignedCluster.key、ルート CA 証明書が rootCAcert.cer です。

CSR を生成する。

データベース クライアント証明書：

```
pki csr dbclusterclient CN:postgres
```

共有証明書：

```
pki csr CAsignedCluster CN:cms.ent-pa.com OU:"TME" O:"Cisco" L:"San Jose"
ST:CaliforniaC:USsubjectAltName:us-acano1.ent-pa.com,us-acano2.ent-pa.com,us-cmsdb.ent
-pa.com,us-cmscb.ent-pa.com, cms.ent-pa.com
```

さまざまなサービスと Cisco Meeting Server ノードの証明書をインストールする。

Web 管理画面サービスを実行する各ノードで次のようにします。

```
webadmin disable
webadmin certs CAsignedCluster.key CAsignedCluster.cer
webadmin enable
```

Call Bridge サービスを実行する各ノードで次のようにします。

```
callbridge certs CAsignedCluster.key CAsignedCluster.cer
callbridge restart
```

XMPP サービスを実行する各ノードで次のようにします。

```
xmpp disable
xmpp certs none
xmpp certs CAsignedCluster.key CAsignedCluster.cer
xmpp enable
```

Web Bridge サービスを実行する各ノードで次のようにします。

```
webbridge disable
webbridge certs CAsignedCluster.key CAsignedCluster.cer
webbridge trust rootCAcert.cer
webbridge enable
```

ローカル データベースが存在している各ノードで次のようにします。

```
database cluster certs CAsignedCluster.key CAsignedCluster.cer dbclusterclient.key
dbclusterclient.cer rootCAcert.cer
```

Call Bridge サービスを実行しているがローカル データベースがない各ノードで次のようにします。

```
database cluster certs dbclusterclient.key dbclusterclient.cer rootCAcert.cer
```

詳細については、次のリンク先にある『*Cisco Meeting Server, Certificate Guidelines for Scalable and Resilient Server Deployments*』の最新版を参照してください。
https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-and-configuration-guides-list.html

Unified CM で、X.509 サブジェクト名の Cisco Meeting Server XMPP ドメイン名、TLS、および暗号化を使用して、SIP トランク セキュリティ プロファイルが設定されていることを確認します。詳細については「SIP トランクの暗号化」を参照してください。この SIP トランク セキュリティ プロファイルを、Call Bridge サービスを実行している CMS ノードへのすべての SIP トランクに関連付けます。

Cisco Meeting Management

Cisco Meeting Management は、デフォルトで自己署名証明書を使用してインストールされます。

DRreceiveraddress と、ユーザがブラウザインターフェイスに使用するアドレスを使用して、CA 署名付き証明書を生成します。

秘密キーと証明書は、次の手順を実行して、Cisco Meeting Management の外部で作成されます。

1。 次のコマンドを使用して秘密キーを生成します。

```
openssl genrsa -out privatekey.pem 2048
```

2。 step 1 の秘密キーを使用して、証明書署名要求（CSR）を生成します。

```
openssl req -new -key us-cmm-privatekey.pem -out us-cmm-certcsr.pem
```

3。 要求されたデータ（国、都道府県または地域、組織名など）を入力します。

4。 社内の認証局（CA）による署名を受けるため、Cisco Meeting Management 証明書署名要求ファイル **us-cmm-certcsr.pem** を送信します。CA から署名付き証明書 **us-cmm.cer** を受け取ります。

5。 秘密キーと証明書をアップロードします。

6。 Cisco Meeting Management を再起動します。

Cisco TelePresence Management Suite

秘密キーと証明書は、Cisco TelePresence Management Suite（TMS）外部で作成されます。この操作は、たとえば次のハイレベルな手順に従って、OpenSSL で実行することができます。

1。 次のコマンドを使用して秘密キーを生成します。

```
openssl genrsa -out us-tms1-privatekey.pem 2048
```

2。 上記の秘密キーを使用して、証明書署名要求（CSR）を生成します。

```
openssl req -new -key us-tms1-privatekey.pem -out us-tms1-certcsr.pem
```

3。 要求されたデータ（国、都道府県または地域、組織名など）を入力します。

4。 社内の認証局（CA）による署名を受けるため、TMS 証明書署名要求ファイル us-tms1-certcsr.pem を送信します。CA から署名付き証明書 us-tms1.cer を受け取ります。

5。 署名付き証明書を秘密キーと結合します。

```
openssl pkcs12 -export -inkey us-tms1-privatekey.pem -in us-tms1.cer -out
us-tms1-cert-key.p12 -name us-tms1-cert-key
```

6。 TMS でルート CA 証明書を証明機関の信頼ストアにインポートします。また、新しい TMS 証明書とその関連秘密キーをパーソナル信頼ストアにインポートします。

7。 Microsoft 管理コンソール（MMC）と証明書スナップインで、インポートした証明書を選択し、右クリックして [すべてのタスク（All Tasks）] > [秘密キーの管理（Manage Private Keys）] を選択します。TMS により使用されるユーザに、読み取り権限および完全アクセス権限を付与します（ほとんどの場合、これは SERVICE ユーザと NETWORK SERVICE ユーザです）。

8。 TMS ツールに移動し、[セキュリティ設定（Security Settings）] > [TLS 証明書（TLS Certificates）] で新しい証明書を選択します。

9。 IIS に移動し、新しい証明書へのバインドを設定します。

10。IIS サービスと TMS サービスを再起動します。

詳細については、次のリンク先にある『*Cisco TelePresence Management Suite Administrator Guide*』の最新版を参照してください。
https://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/products-maintenance-guides-list.html

また、次のリンク先にある『*TMS Certificates with TMS Tools for TLS Communication Configuration Example*』も参照してください。
https://www.cisco.com/c/en/us/support/docs/conferencing/telepresence-management-suite-tms/118723-configure-tms-00.html.

コラボレーション管理サービス

Cisco Prime Collaboration Deployment

Cisco Prime Collaboration Deployment には、プラットフォームを管理するためのグラフィカル ユーザ インターフェイス（GUI）がありません。CA 署名付き証明書を発行するには、CLI（コマンド ライン インターフェイス）に移動して CSR を発行します。CSR を生成するには CLI コマンド **set csr gen tomcat** を使用し、PEM 形式で CSR を表示するには **show csr own tomcat /tomcat.csr** を使用します。CA 証明書または下位 CA 証明書をインポートするには **set cert import trust tomcat** を使用し、tomcat 証明書をインポートするには **set cert import own tomcat tomcat-trust/**<*tomcat-certificate-name*> を使用します。

Tomcat Service を再起動するには、**utils service restart Cisco Tomcat** というコマンドを入力します。

Cisco Prime Collaboration Provisioning

証明書の操作は、[管理（Administration）] > [更新（Updates）] > [SSL 証明書（SSL Certificates）] で実行できます。[CSR の生成（Generate CSR）] をクリックして CSR を生成します。

使用するパラメータは、[キータイプ（Key Type）] が [RSA]、[キー長（Key length）] が [2048]、[ハッシュ アルゴリズム（Hash Algorithm）] が [SHA-256] です。エンタープライズ ルート CA で CSR に署名します。

[アップロード（Upload）] をクリックして CA 署名付き PCP 証明書と LDAP 証明書をアップロードします。

その後、GUI または CLI で Apache を再起動します。

詳細については、次のリンク先にある『*Cisco Prime Collaboration Provisioning Guide - Standard and Advanced*』の最新版を参照してください。
https://www.cisco.com/c/en/us/support/cloud-systems-management/prime-collaboration/products-user-guide-list.html

マルチクラスタに関する考慮事項

マルチクラスタ導入では、すべてのクラスタが同一データセンター内にない場合、クラスタ間リンクの暗号化を有効にします。

SIP トランクについては、CallManager に CA 署名付き証明書を使用することが推奨されており、また複数のクラスタに同一 CA が使用されていることを前提としていることから、クラスタ間で CallManager 証明書または CA 証明書を交換する必要はありません。

ILS 暗号化を有効にするには、認証に TLS 証明書を使用し、承認にパスワードを使用することが推奨されます。Unified CM ILS 設定ページで、[TLS 証明書の使用（Use TLS Certificates）] オプションを選択し（チェックボックスをオン）、[パスワードの使用（Use Password）] オプションを選択して（チェックボックスをオン）、Unified CM クラスタ間で共有するパスワードを入力します。エンタープライズ CA により署名された tomcat s 証明書と、すでに tomcat 信頼ストアに格納されているエンタープライズ ルート CA 証明書（または証明書チェーン）では、証明書の ILS 暗号化を有効にするために追加の操作を行う必要はありません。

LBM 暗号化を有効にするには、単に Unified CM エンタープライズ パラメータ [LBM セキュリティ モード（LBM Security Mode）] を [セキュア（Secure）] に設定します。ここでもまた、エンタープライズ CA により署名された tomcat 証明書と、すでに tomcat 信頼ストアに格納されているエンタープライズ ルート CA 証明書では、証明書の LBM 暗号化を有効にするために追加の操作を行う必要はありません。