デフォルトのセキュリティ設定

ここでは、デフォルトのセキュリティ設定について説明します。

デフォルトのセキュリティ機能

デフォルトでは、セキュリティはCisco Unified IP 電話 s に対して次の自動セキュリティ機能を提供します。

- 電話機の設定ファイルの署名
- 電話機の設定ファイルの暗号化のサポート

- Tomcat および他の Web サービスでの https の利用（MIDlet）

Unified Communications Manager リリース 8.0 以降では、CTL クライアントが実行されているかどうかにかかわらず、これらのセキュリティ機能がデフォルトで提供されています。

信頼検証サービス

ネットワーク内に多数の電話機があり、Cisco Unified IP 電話 のメモリも限られています。したがって、Unified Communications Manager は TVS を介してリモート信頼ストアとして動作するため、各電話機に証明書信頼ストアを配置する必要はありません。Cisco Unified IP 電話 は CTL ファイルまたは ITL ファイルを使用して署名または証明書を検証できないため、検証のために TVS サーバに問い合わせることもできます。したがって、中央信頼ストアを持つことは、信頼ストアをすべての Cisco Unified IP 電話 に持つよりも管理が簡単です。

TVS を使用すると、HTTPS を確立しているときに、Cisco Unified IP 電話 で EM サービス、ディレクトリ、および MIDlet などのアプリケーションサーバを認証できます。

TV には、次の機能があります。

- 拡張性：Cisco Unified IP 電話 のリソースは、信頼する証明書の数に影響されません。
- 柔軟性: 信頼証明書の追加または削除は、システムに自動的に反映されます。
- デフォルトのセキュリティ：非メディアおよびシグナリングセキュリティ機能はデフォルトのインストールに含まれており、ユーザの介入は必要ではありません。

（注） セキュアなシグナリングおよびメディアを有効にする場合は、CTL ファイルを作成してから、クラスタを混合モードに設定する必要がありますCTL ファイルを作成し、クラスタを混合モードに設定するには、CLI コマンド **utils ctl set-cluster mixed-mode** を使用します。

TVS を説明する基本的な概念を次に示します。

- TVS は、Unified Communications Manager サーバ 上で実行され、Cisco IP 電話に代わって証明書を認証します。
- Cisco Unified IP 電話 は、信頼できる証明書をすべてダウンロードするのではなく、TVS を信頼する必要があるだけです。
- ITL ファイルはユーザの介入なしで自動的に生成されます。ITL ファイルは、Cisco Unified IP 電話 によりダウンロードされ、信頼はそこからフローします。

TV の説明

TVS を説明する基本的な概念を次に示します。

- TVS は Unified Communications Manager サーバ上で動作し、Cisco IP 電話 の代わりに証明書を認証します。
- 信頼できる証明書をすべてダウンロードするのではなく、Cisco IP 電話では TVS を信頼するだけで済みます。
- ITL ファイルはユーザの介入なしで自動的に生成されます。ITL ファイルは Cisco IP 電話によってダウンロードされ、そこから信頼情報がフローします。

初期信頼リスト

初期信頼リスト（ITL）ファイルは、エンドポイントが Unified Communications Manager を信頼できるよう、最初のセキュリティに使用されます。ITL は明示的に有効にするセキュリティ機能を必要としません。ITL ファイルは、TFTP サービスがアクティブになり、クラスタがインストールされると自動的に作成されます。Unified Communications Manager の TFTP サーバの秘密キーは、ITL ファイルの署名に使用されます。

Unified Communications Manager クラスタまたはサーバが非セキュアモードの場合、ITL ファイルはサポートされている Cisco Unified IP 電話 ごとにダウンロードされます。CLI コマンド **admin:show itl** を使用して、ITL ファイルの内容を表示できます。

Cisco Unified IP 電話 は、次のタスクを実行するために ITL ファイルが必要です。

- CAPF とセキュアに通信する。設定ファイル暗号化をサポートするための前提条件です。
- 設定ファイルの署名を認証する。
- TVS を使用する EM サービス、ディレクトリ、MIDlet などのアプリケーション サーバを認証します。

Cisco IP 電話 に CTL ファイルがまだ存在していない場合、最初の ITL ファイルが自動的に信頼されます。テレビは、署名者に対応する証明書を返すことができる必要があります。

Cisco IP 電話 に既存の CTL ファイルがある場合、ITL ファイルの署名の認証にその CTL ファイルが使用されます。

（注） SHA-1 または MD5 アルゴリズム値は、初期信頼リスト（ITL）ファイルの値に変更があった場合にのみ変更されます。ITL ファイルのチェックサム値を使用すると、Cisco IP 電話 と Unified Communications Manager クラスタの間にある ITL ファイルの差異を特定できます。ITL ファイルのチェックサム値は、ITL ファイルを変更した場合にのみ変更されます。

最初の信頼リスト (ITL) ファイルは、CTL ファイルと同じ形式になっています。ただし、これはより小さく、スリムのバージョンです。

ITL ファイルには次の属性が適用されます。

- TFTP サービスがアクティブ化され、クラスタをインストールすると、システムによって ITL ファイルが自動的に作成されます。内容が変更された場合、ITL ファイルは自動的に更新されます。
- ITL ファイルは eToken を必要としません。このファイルはソフト eToken（TFTP サーバの CallManager 証明書に関連付けられている秘密キー）を使用します。
- リセット中、再起動中、または CTL ファイルのダウンロード後に、Cisco Unified IP 電話 は ITL ファイルをダウンロードします。

ITL ファイルには次の証明書が含まれています。

- ITLRecovery 証明書：この証明書は ITL ファイルに署名します。
- TFTP サーバの CallManager 証明書：この証明書を使用すると、ITL ファイル署名と電話機設定ファイル署名を認証できます。
- クラスタ上で使用可能なすべての TVS 証明書：これらの証明書を使用すると、電話機は TVS と安全に通信し、証明書認証を要求できます。
- CAPF 証明書: これらの証明書は、コンフィギュレーションファイルの暗号化をサポートします。CAPF 証明書は必ずしも ITL ファイル内に存在する必要はありません（TVS で認証可能）が、CAPF 証明書によって CAPF への接続が簡易化されます。

ITL ファイルには証明書ごとに 1 つのレコードが含まれます。各レコードの内容は次のとおりです。

- 証明書
- Cisco IP 電話 によるルックアップを容易にするための、事前に抽出された証明書フィールド。
- 証明書の権限（TFTP、CUCM、TFTP+CCM、CAPF、TV、SAST）

TFTP サーバの CallManager 証明書は、2 つの異なる権限を持つ次の 2 つの ITL レコード内に存在します。

- TFTP 権限 または TFTP および CCM 権限：設定ファイルの署名を認証する。
- SAST 権限：ITL ファイルの署名を認証する。

初期信頼リストファイル

最初の信頼リスト (ITL) ファイルは、CTL ファイルと同じ形式になっています。ただし、これはより小さく、スリムのバージョンです。

ITL ファイルには次の属性が適用されます。

- システムは、クラスタのインストール時に自動的に ITL ファイルを作成します。内容が変更された場合、ITL ファイルは自動的に更新されます。
- ITL ファイルは eToken を必要としません。このファイルはソフト eToken（TFTP サーバの CallManager 証明書に関連付けられている秘密キー）を使用します。

- リセット中、再起動中、または CTL ファイルのダウンロード後に、Cisco Unified IP 電話 は ITL ファイルをダウンロードします。

ITL ファイルの内容

ITL ファイルには次の証明書が含まれています。

- TFTP サーバの CallManager 証明書：この証明書を使用すると、ITL ファイル署名と電話機設定ファイル署名を認証できます。
- クラスタ上で使用可能なすべての TVS 証明書：これらの証明書を使用すると、電話機は TVS と安全に通信し、証明書認証を要求できます。
- CAPF 証明書: これらの証明書は、コンフィギュレーションファイルの暗号化をサポートします。CAPF 証明書は必ずしも ITL ファイル内に存在する必要はありません（TVS で認証可能）が、CAPF 証明書によって CAPF への接続が簡易化されます。

ITL ファイルには証明書ごとに 1 つのレコードが含まれます。各レコードの内容は次のとおりです。

- 証明書
- Cisco IP 電話 によるルックアップを容易にするための、事前に抽出された証明書フィールド。
- 証明書の権限（TFTP、CUCM、TFTP+CCM、CAPF、TV、SAST）

TFTP サーバの CallManager 証明書は、2 つの異なる権限を持つ次の 2 つの ITL レコード内に存在します。

- TFTP 権限 または TFTP および CCM 権限：設定ファイルの署名を認証する。
- SAST 権限：ITL ファイルの署名を認証する。

ITL と CTL ファイルの相互作用

Cisco IP 電話 は、クラスタ セキュリティ モード（非セキュアまたは混合モード）を確認する際に CTL ファイルを使用します。CTL ファイルは、Unified Communications Manager レコードに Unified Communications Manager 証明書を含めることで、クラスタ セキュリティ モードを追跡します。

ITL ファイルには、クラスタセキュリティモードの指示も含まれています。

ITLRecovery 証明書の証明書管理の変更

- ITLRecovery の有効期間が 5 年間から 20 年間に延長され、より長い期間にわたって同じ ITLRecovery 証明書が使用されるようになりました。

（注） Unified Communications Manager をアップグレードした場合、ITLRecovery 証明書の有効期間は引き続き 5 年のままです。Unified Communications Manager をアップグレードすると、新しいリリースに証明書がコピーされます。ただし、ITLRecovery 証明書を再生成するか、Unified Communications Manager の新規インストールを実行すると、ITLRecovery の有効期間が 20 年に延長されます。

- ITLRecovery 証明書を再生成する前に、CLI と GUI の両方に警告メッセージが表示されます。この警告メッセージは、トークンレス CTL を使用しており、CallManager 証明書を再生成する場合に、CTL ファイルに更新された CallManager 証明書があり、その証明書がエンドポイントに更新されていることを確認するために表示されます。

ITLRecovery 証明書

ITLRecovery Certificate 機能では、新しい **ITL ファイルステータス**ドロップダウンリストが導入され、管理者は古い ITL を持つ電話機を識別して、それらの電話機に必要なアクションを実行できるようになりました。

一部の電話機は、ITL ファイルが更新されたときに最新の ITL ファイルを取得せず、古いものを保持します（CM 証明書の更新など）。システムは、不一致の ITL ファイルがある電話機の集中型レポートをユーザインターフェイスに表示します。

次に、さまざまな ITLRecovery シナリオを示します。

TFTP Service Activaton:

- TFTP サービスがアクティブになると、生成された ITL ファイルのハッシュがサーバのホスト名とともに DB に保存されます。ITL が TFTP コードで更新されるたびに更新されます。
- TFTP ホスト名がすでにテーブルに存在する場合は、生成された ITL ハッシュが保存されている値と比較されます。
  - ITL ハッシュが同じでない場合、新しい ITL ハッシュが DB で更新されます。
  - ITL ハッシュが同じ場合、TFTP ログに「Tftp Itl hash not changed」と表示されます。

デバイス登録と ITLFile のダウンロード

- 電話機がUnified Communications Managerに登録されると、サーバに存在する ITLFile の詳細（サーバのホスト名、ハッシュ、タイムスタンプ）が DB に存在しません。
- 電話機がUnified Communications Managerに登録されると、電話機に適用された ITL ファイルの詳細を含む SIP アラームが送信されます。これは、DB に保存されている ITL ファイルのハッシュと比較されます。
  - ITL ハッシュが同じ場合、デバイスハッシュ情報は新しいタイムスタンプで更新されます。

- ITL ハッシュが同じでない場合、報告された ITL ハッシュとタイムスタンプがデバイスに対して更新されます。

- 電話機の登録が解除されると、そのデバイスの信頼ハッシュ情報が削除されます。

連携動作と制限事項

Unified Communications Manager クラスタに 39 を超える証明書がある場合、Cisco IP 電話 上の ITL ファイル サイズが 64 キロバイトを超えます。ITL ファイル サイズが増加すると、電話での ITL の正常なロードに影響し、Unified Communications Manager での電話登録が失敗することになります。

Cisco Unified IP 電話 の ITL ファイルの更新

電話機にインストールされている ITL ファイルでデフォルトのセキュリティを使用している Unified Communication Manager との集中型 TFTP では、TFTP 設定ファイルは検証されません。

リモートクラスタからの電話機が集中型 TFTP 展開に追加される前に、次の手順を実行します。

手順

Step 1 中央 TFTP サーバで、Enterprise パラメータ **Prepare cluster for PRE CM-8.0 rollback** を有効にします。

Step 2 TVS および TFTP を再起動します。

Step 3 すべての電話機をリセットして、ITL 署名検証を無効にする新しい ITL ファイルがダウンロードされていることを確認します。

Step 4 HTTPS ではなく HTTP を使用するように、エンタープライズパラメータセキュア https Url を設定します。

（注） Unified Communications Manager のリリース 10.5 以降では、[**クラスタの 8.0 以前へのロールバック準備（Prepare Cluster for Rollback to pre-8.0）**] エンタープライズ パラメータを有効にした後、電話が自動的にリセットされます。中央 TFTP サーバの Unified Communications Manager バージョンとこのパラメータを有効にする方法については、Cisco Unified Communications Manager セキュリティ ガイドの「8.0 より前のリリースへのクラスタのロールバック」セクションを参照してください。

自動登録

システムは混合モードと非セキュアモードの両方で自動登録をサポートします。また、デフォルトの設定ファイルに対する署名も行われます。「デフォルトのセキュリティ」がサポートされていない Cisco IP 電話 には、署名されていないデフォルトの設定ファイルが提供されます。

ITL ファイルステータスの取得

電話機の ITL ファイルステータスを取得するには、次の手順を使用します。

Procedure

Step 1 Cisco Unified Communications Manager Administrationから、**[デバイス（Device）] > [電話（Phone）]** を選択します。

Step 2 **[電話機を探す（Find Phone where）]** ドロップダウンリストで **[ITL ファイルステータス（ITL File Status）]** を選択し、条件を選択します。

フィールド	説明
一致	サーバと電話機の ITL ハッシュが同じ
MisMatch	サーバの ITL ハッシュが電話機の ITL ハッシュと異なる
未インストール	電話機が新しい CUCM サーバへの登録に失敗し、以前のサーバにバウンスする
不明	電話機またはサーバの ITL ハッシュが不明

Step 3 [検索（Find）] をクリックします。

Cisco Unified IP 電話 サポートリストの取得

Cisco Unified Reporting ツールを使用して、デフォルトでセキュリティをサポートするシスコエンドポイントのリストを生成します。

手順

Step 1 [Cisco Unified Reporting] から [システムレポート（System Reports）] をクリックします。

Step 2 [システムレポート（System Reports）] リストで、[Unified CM 電話機能一覧（Unified CM Phone Feature List）] をクリックします。

Step 3 **[製品（Product）]** ドロップダウンリストから、**[デフォルトのセキュリティ（Security By Default）]** を選択します。

Step 4 [送信（Submit）] をクリックします。
特定の電話でサポートされている機能のリストを含むレポートが生成されます。

認定されたソリューション向けコモン クライテリアの ECDSA サポート

Unified Communications Manager は、楕円曲線デジタル署名アルゴリズム（ECDSA）証明書をサポートします。これらの証明書は、RSA ベースの証明書よりも堅牢であり、コモン クライテリア（CC）認定のある製品に必要となります。米国政府の Commercial Solutions for Classified Systems（CSfC）プログラムは、CC 認定が必要なので、Unified Communications Manager にはこれが含まれています。

ECDSA 証明書は、証明書マネージャ、SIP、Certificate Authority Proxy Function（CAPF）、Transport Layer Security（TLS）、トレース、エントロピー、HTTP、CTI Manager で既存の RSA 証明書とともに使用できます。

（注） ECDSA は、Unified Communications Manager と Tomcat についてのみサポートされています。

証明書マネージャでの ECDSA サポート

Unified Communications Manager リリース 11.0 の証明書マネージャでは、自己署名 ECDSA 証明書と ECDSA 証明書署名要求（CSR）の両方の生成がサポートされています。これより前の Unified Communications Manager では、**RSA** 証明書のみがサポートされていました。しかし、Unified Communications Manager リリース 11.0 以降では、既存の **RSA** 証明書に加えて **CallManager-ECDSA** 証明書がサポートされます。

CallManager 証明書と **CallManager-ECDSA** 証明書の両方が、共通の信頼ストアである CallManager-Trust を共有します。Unified Communications Manager によって、これらの証明書がこの信頼ストアにアップロードされます。

証明書マネージャでは、キー長の値が異なる ECDSA 証明書の生成がサポートされています。

Unified Communications Manager をインストールすると、自己署名証明書が生成されます。Unified Communications Manager リリース 11.0 には常時 ECDSA 証明書が存在し、この証明書が SIP インターフェイスで使用されます。Secure Computer Telephony Integration (CTI) Manager インターフェイスは、ECDSA 証明書もサポートしています。CTI Manager と SIP サーバの両方が同じサーバ証明書を使用しているため、両方のインターフェイスが同期して動作します。

SIP での ECDSA サポート

Unified Communications Manager リリース 11.0 には SIP 回線と SIP トランク インターフェイス向けの ECDSA サポートが含まれています。Unified Communications Manager とエンドポイント電話またはビデオ デバイスとの間の接続は SIP 回線接続であるのに対し、2 つの Unified Communications Manager 間の接続は SIP トランク接続です。すべての SIP 接続は、ECDSA 暗号方式をサポートし、ECDSA 証明書を使用します。

SIP が (Transport Layer Security) TLS 接続を行うシナリオを次に示します。

- SIP が TLS サーバとして機能する場合：Unified Communications Manager が着信するセキュア SIP 接続の TLS サーバとして機能する場合、SIP トランク インターフェイスは CallManager-ECDSA の証明書がディスクにあるかどうかを判断します。証明書がディスクに存在する場合、選択した暗号スイートが**TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256**または**TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384**場合、SIP トランクインターフェイスは CallManager ECDSA 証明書を使用します。SIP トランクインターフェイスは、ECDSA 暗号スイートをサポートしていないクライアントからの接続に対して RSA TLS 暗号スイートを引き続きサポートします。**[TLS Ciphers]** ドロップダウンリストには、Unified Communications Manager が TLS サーバとして機能するときにサポートされている暗号スイートの設定を許可するオプションがあります。
- Sip が TLS クライアントとして機能する場合: sip トランクインターフェイスが TLS クライアントとして機能する場合、SIP トランクインターフェイスは、Cisco Unified Communications Manager の [**エンタープライズパラメータ (Enterprise Parameters)**] ウィンドウの [**Tls 暗号 (tls cipher)**] フィールド (**ECDSA 暗号**オプションも含む) に基づいて、要求された暗号スイートのリストをサーバに送信します。[TLS Ciphers]。この設定により、TLS クライアント暗号スイートリストおよびサポートされている暗号スイートが優先順に決定されます。

（注） ECDSA クライアント証明書をサポートしていない以前のリリースの Unified Communications Manager と TLS 接続を確立する場合、この接続では RSA 暗号スイートが使用されます。TLS 接続で送信されるクライアント証明書は、選択した TLS 暗号に関連付けられている必要はありません。以前のリリースの Unified Communications Manager でも、TLS サーバが ECDSA クライアント証明書を受信して処理することがサポートされています。

Unified Communications Manager への接続に ECDSA 暗号を使用するデバイスでは、アイデンティティ信頼リスト（ITL ファイル）に CallManager-ECDSA 証明書が必要です。次に、CallManager ECDSA 証明書によって保護されている接続を信頼するために、デバイスは CallManager ECDSA 証明書をローカル証明書ストアに組み込む必要があります。

CAPF での ECDSA サポート

Certificate Authority Proxy Function（CAPF）は、シスコのエンドポイントと Unified Communications Manager との間で証明書を交換する、シスコ独自のメソッドです。Cisco エンドポイントのみが CAPF を使用します。一般的な基準要件を達成するために、CAPF は CAPF バージョン3に更新されます。これにより、クライアントは ECDSA ローカルで有効な証明書 (LSC) で提供されるようになります。カスタマーがローカルで LSC を作成します。LSC は製造元が作成した製造元でインストールされた証明書 (MIC) に代わるものです。

CAPF バージョン 3 を使うことで、Unified Communications Manager サーバから電話、CTI アプリケーション、Jabber クライアントに対し、LSC で使用される EC キーの生成を指示できます。EC キーが生成されると、Unified Communications Manager は ECDSA LSC を生成して Cisco エンドポイントに送信するか、または ECDSA CSR を生成します。

エンドポイントに CAPF バージョン3のサポートがない場合は、必要な EC キーサイズと RSA キーサイズを設定し、Cisco ユニファイド CM Administration からバックアップとして [**電話の設定 (Phone Configuration)**] ウィンドウで [**ec キー優先 (rsa Backup)**] オプションを選択できます。このバックアップオプションは、CAPF サーバが ec キーペアに要求を送信しようとし、電話機が EC キーをサポートしていないサーバと通信する場合に便利です。サーバは EC キーペアの代わりに RSA キーペアを生成する要求を送信します。

（注） Cisco エンドポイントが CAPF バージョン3をサポートしていて、**エンドポイントの Advanced Encryption Algorithm Support**パラメータを有効にせずに、**電話の設定**で**EC 優先、rsa バックアップ**オプションを選択した場合、ECDSA または RSA ベースの lscs は発行されません。Cisco エンドポイントが CAPF バージョン3をサポートしていない場合、**エンドポイントの Advanced Encryption Algorithm support**パラメータを有効または無効にすると、RSA ベースの lscs が発行されます。

（注） Endpoint **Advanced Encryption アルゴリズムのサポート**パラメータは、電話機が高度な TLS 暗号を使用して TFTP 設定ファイルをダウンロードすることを示します。デフォルトでは、EC の暗号が最も優先順位が高く設定されています。このソリューションは、MRA を使用しないオンプレミスの展開でのみサポートされています。

エントロピー

強力な暗号化を行うには、エントロピーの堅牢なソースが必要です。エントロピーはデータのランダム性の尺度であり、一般的な基準要件の最小しきい値を決定するのに役に立ちます。暗号化や暗号化などのデータ変換技術は、その有効性を高めるためにエントロピーの適切なソースに依存しています。ECDSA などの強力な暗号化アルゴリズムでエントロピーの弱いソースが使用されている場合は、暗号化が簡単に切断される可能性があります。

Unified Communications Manager リリース 11.0 では、Unified Communications Manager のエントロピー ソースが向上しました。エントロピー モニタリング デーモンは設定が不要な組み込み機能です。ただし、Unified Communications Manager CLI によってオフにすることができます。

エントロピーモニタリングデーモンサービスを制御するには、次の CLI コマンドを使用します。

CLI コマンド	説明
ユーティリティサービス開始エントロピーモニタリングデーモン	エントロピー モニタリング デーモン サービスを開始します。
ユーティリティサービス停止エントロピーモニタリングデーモン	エントロピー モニタリング デーモン サービスを停止します。
ユーティリティサービスアクティブエントロピーモニタリングデーモン	エントロピー モニタリング デーモン サービスをアクティブにします。さらにカーネル モジュールがロードされます。
ユーティリティサービス deactive エントロピーモニタリングデーモン	エントロピー モニタリング デーモン サービスを非アクティブ化します。さらにカーネル モジュールがアンロードされます。

コンフィギュレーション ダウンロードの HTTPS サポート

セキュアなコンフィギュレーション ダウンロードのため Unified Communications Manager リリース 11.0 では、以前のリリースでの HTTP および TFTP インターフェイスに加えて、HTTPS をサポートするように機能強化されました。必要に応じて、クライアントとサーバの両方が相互認証を使用します。ECDSA lscs および暗号化された TFTP 設定を使用して登録されたクライアントは、lscs を提示する必要があります。

HTTPS インターフェイスは、CallManager と CallManager ECDSA 証明書の両方をサーバ証明書として使用します。

（注） CallManager、CallManager ECDSA、または tomcat 証明書を更新する場合は、TFTP サービスを非アクティブ化してから再アクティブ化する必要があります。ポート6971は CallManager および CallManager ECDSA 証明書の認証に使用されますが、ポート6972は tomcat 証明書の認証に使用されます。

CTI Manager のサポート

コンピュータテレフォニーインテグレーション (CTI) インターフェイスは、4つの新しい暗号方式をサポートするように強化されています。暗号スイートは、
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256、
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384、

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 、および **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384**です。これらの暗号スイートのサポートによって、CTI Manager インターフェイスでは、Unified Communications Manager 内に存在する場合に、**CallManager-ECDSA** 証明書の保有が必要となりました。SIP インターフェイスと同様、CTI Manager セキュア インターフェイスでサポートされる TLS 暗号方式の設定には、Unified Communications Manager 内のエンタープライズ パラメータ [TLS Ciphers] オプションが使用されます。

証明書の再生成

Unified Communications Manager 証明書の 1 つを再生成した場合、この項で説明する手順を実行する必要があります。

注意 証明書を再作成すると、システムの動作に影響する場合があります。証明書を再生成すると、サードパーティの署名付き証明書（アップロードされている場合）を含む既存の証明書が上書きされます。詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

CAPF 証明書の再生成

CAPF 証明書を再生成するには、次の手順を実行します。

（注） CAPF 証明書がパブリッシャにある場合は、電話機が自動的に再起動して ITL ファイルを更新することがあります。これは、[証明書の更新時の電話の連携（Phone Interaction on Certificate Update）] パラメータが自動的にリセットされる場合に適用されます。

手順

Step 1 CAPF 証明書を再生成します。

Step 2 CTL ファイルがある場合は、CTL ファイルを更新する必要があります。

詳細については、『Cisco Unified Communications Manager Security Guide』の「証明書の再生成」セクションを参照してください。

Step 3 CAPF 証明書が再生成されると、CAPF サービスが自動的に再起動されます。

詳細については、『*Cisco Unified Communications Manager Security Guide*』の「「Activating the Certificate Authority Proxy Function Service」」の項を参照してください。

TVS 証明書の再生成

（注） TV と TFTP の両方の証明書を再生成する場合は、TV 証明書を再生成し、可能な電話機の再起動が完了するまで待ってから、TFTP 証明書を再生成します。これは、[証明書の更新時の電話の連携（Phone Interaction on Certificate Update）] パラメータが自動的にリセットされる場合に適用されます。

手順

Step 1 TVS 証明書の再生成

Step 2 CTL ファイルがある場合は、CTL ファイルを更新する必要があります。

詳細については、『Cisco Unified Communications Manager Security Guide』 の「証明書の再生成」セクションを参照してください。

Step 3 TVS 証明書が再生成されると、TVS サービスが自動的に再起動されます。

TFTP 証明書の再生成

TFTP 証明書を再生成するには、次の手順を実行します。

（注） 複数の証明書を再生成する予定の場合は、最後にTFTP証明書を再生成する必要があります。TFTP証明書を再生成する前に、可能な電話機の再起動が完了するまで待ちます。この手順に従わないと、すべての Cisco IP 電話 から ITL ファイルを手動で削除する必要が生じることがあります。これは、[証明書の更新時の電話の連携（Phone Interaction on Certificate Update）] パラメータが自動的にリセットされる場合に適用されます。

手順

Step 1 TFTP 証明書を再生成します。

詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

Step 2 TFTPサービスが有効化されている場合は、すべての電話機が自動的に再起動するまで待ちます。

Step 3 クラスタが混合モードの場合は、CTL ファイルを更新します。

Step 4 クラスタが EMCC 導入に含まれる場合、証明書の一括プロビジョニングの手順を繰り返します。

詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

ITLRecovery 証明書の再生成

警告 この証明書の有効期限が電話機で長いため、ITLRecovery 証明書は頻繁に再生成しないでください。また、この証明書には CallManager 証明書も含まれています。

非セキュアクラスタの ITLRecovery 証明書の再生成

1. ITL ファイルが有効であること、およびクラスタ内のすべての電話機が現在の ITL ファイルを信頼しているかどうかを確認します。
2. ITLRecovery 証明書を再生成します。

   各クラスタ内のパブリッシャに移動し、ITLRecovery 証明書を再生成します。

   1. [Unified OS の管理（Unified OS Administration）] から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。
   2. [検索（Find）] をクリックします。

      [証明書リスト（Certificate List）] ウィンドウが表示されます。
   3. 表示された証明書のリストから、ITLRecovery pem 証明書のリンクをクリックします。
   4. ITLRecovery 証明書を再生成するには、**[再生成 (再生成)]** をクリックします。
   5. 確認メッセージポップアップで、**[OK]**をクリックします。
3. CallManager 証明書のユーティリティ `itl reset localkey\`を使用して itl ファイルに署名し、新しい itl ファイルを受け入れます。
4. クラスタ内のすべての電話機を一括してリセットします。

（注） クラスタ内のすべての電話機が登録されていることを確認してください。

5. TFTP サービスを再起動して、新しい ITLRecovery 証明書によって ITL ファイルが再署名されるようにします。

   新しい ITLRecovery 証明書は、リセット中に電話機にアップロードされます。
6. クラスタ内のすべての電話機を一括してリセットし、新しい ITL ファイルを取得します。
7. リセット後に、新しい ITLRecovery 証明書を使用して電話機がアップロードされます。

セキュアクラスタの ITLRecovery 証明書の再生成

トークンベースの ITL ファイルからトークンレス ITL ファイルに移行する場合は、『security guide』の「migration」の項を参照してください。

1. ITL ファイルが有効であることと、クラスタ内のすべての電話機が現在の ITL ファイルを信頼していることを確認します。
2. `Show ctl`コマンドを使用して ctl ファイルを確認します。
3. ITLRecovery 証明書を再生成します。

   各クラスタ内のパブリッシャに移動し、ITLRecovery 証明書を再生成します。

   1. [Unified OS の管理（Unified OS Administration）] から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）] > [検索（Find）]** を選択します。
   2. [**検索（Find**）] をクリックして、証明書の一覧を表示します。

      [証明書リスト（Certificate List）] ウィンドウが表示されます。
   3. 表示された証明書のリストから、ITLRecovery pem 証明書のリンクをクリックします。
   4. ITLRecovery 証明書を再生成するには、[**再生成 (再生成)**] をクリックします。
   5. 確認メッセージポップアップで、[**OK]**をクリックします。
4. CallManager 証明書で、CTLFile にユーティリティ `ctl reset localkey\`を使用して署名します。これにより、新しい ITLRecovery 証明書を使用して CTLFile も更新されます。
5. クラスタ内のすべての電話機を一括してリセットし、新しいITLRecovery証明書を使用して新しい CTLFile をピックアップします。

（注）
- クラスタ内のすべての電話機が登録済みであることを確認してください。
- ITLRecoveryを再生成すると、システム全体の証明書が有効化に使用される場合、クラスタの SAML SSO ログインに影響します。

6. 新しい ITLRecovery Certificate CTLFile `ctl Update CTLFile`によって再署名されるように、を更新します。
7. クラスタ内のすべての電話機を一括してリセットし、新しいITLRecovery証明書によって署名された新しい CTLFile をピックアップします。
8. リセット後、新しい ITLRecovery 証明書が電話機にアップロードされます。

tomcat 証明書の再生成

Tomcat 証明書を再生成するには、次の手順を実行します。

手順

Step 1 Tomcat 証明書を再生成します。

詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

Step 2 Tomcat サービスの再起動

詳細については、『*Administration Guide for Cisco Unified Communications*』を参照してください。

Step 3 クラスタが EMCC 導入に含まれる場合、証明書の一括プロビジョニングの手順を繰り返します。

詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

TFTP 証明書の再生成後のシステムバックアップ手順

ITL ファイルのトラストアンカーは、ソフトウェアエンティティである TFTP 秘密キーです。サーバがクラッシュすると、キーが失われ、電話機は新しい ITL ファイルを検証できなくなります。

Unified Communications Manager リリース 10.0 では、TFTP 証明書と秘密キーの両方がディザスタリカバリ システムによってバックアップされます。システムは、秘密キーの秘密を保持するためにバックアップパッケージを暗号化します。サーバがクラッシュすると、以前の証明書とキーが復元されます。

TFTP 証明書が再生成されるたびに、新しいシステムのバックアップを作成する必要があります。バックアップ手順については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

Cisco Unified Communications Manager リリース7.x からリリース8.6 以降へのアップグレードの更新

クラスタをリリース7.xからリリース8.6以降にアップグレードするには、次の手順を実行します。

手順

Step 1 クラスタをアップグレードするための通常の手順に従ってください。詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

ヒント　クラスタのすべてのノードを Unified Communications Manager リリース 8.6 以降にアップグレードした後、さらにこの手順に従ってご使用の Cisco Unified IP 電話 をシステムに登録する必要があります。

Step 2　次のリリースのいずれかを混合モードで実行している場合、CTL クライアントの実行が必要です。

- Unified Communications Manager リリース 7.1(2)
  - 7.1 (2) のすべての通常リリース
  - 007.001 (002.32016.001) より前の712のすべての ES リリース
- Unified Communications Manager リリース 7.1(3)
  - 007.001 (003.21900.003) より前の713のすべての通常リリース = 7.1 (3a) su1a
  - 007.001 (003.21005.001) より前の713のすべての ES リリース

（注）　CTL クライアントの実行の詳細については、第 4 章「「CTL クライアントの設定」」を参照してください。

Step 3　Cisco IP 電話 が自動的に再起動され、Unified Communications Manager に登録されるまで、10 分間待ちます。

注意　クラスタを回復できるようにするには、ディザスタリカバリシステム(DRS) を使用してクラスタをバックアップする必要があります。

Step 4　ご使用のクラスタをバックアップします。

DRS を使用してクラスタをバックアップするには、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

次のタスク

アップグレード後にパブリッシャが起動したら、CAR の移行が完了するまで再起動しないでください。このフェーズでは、古いバージョンに切り替えたり、DRS バックアップを実行したりすることはできません。CAR 移行ステータスをモニタするには、**Cisco ユニファイドサービスの** > > **CDR Analysis and Reporting**に移動します。

8.0 より前のリリースへのクラスタのロールバック

クラスタを Unified Communications Manager の旧リリース（リリース 8.0 よりも前）にロールバックする場合は、その前に [Prepare Cluster for Rollback to pre-8.0] エンタープライズパラメータを使用したロールバックの準備が必要です。

クラスタをロールバックするための準備を行うには、クラスタの各サーバで次の手順に従います。

手順

Step 1 Unified Communications Manager で、**[システム（System）] > [エンタープライズパラメータ設定（Enterprise Parameters Configuration）]** を選択します。

[Enterprise Parameters Configuration] ウィンドウが表示されます。

[Prepare Cluster for Rollback to pre-8.0] エンタープライズ パラメータを [True] に設定します。

（注） クラスタを Unified Communications Manager のバージョン 8.0 以前へロールバックする準備を行う場合のみ、このパラメータを有効にします。このパラメータが有効になっている間、HTTPS を使う電話サービス（たとえば、エクステンションモビリティなど）は機能しません。ただし、このパラメータが有効になっていても、基本的な電話の発信および受信は引き続き可能です。

Step 2 Cisco IP 電話が自動的に再起動され、Unified Communications Manager に登録されるまで、10 分間待ちます。

Step 3 クラスタの各サーバを以前のリリースに戻します。

クラスタを以前のバージョンに戻す方法の詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

Step 4 クラスタが以前のバージョンへの切り替えを完了するまで待ちます。

Step 5 次のリリースのいずれかを混合モードで実行している場合、CTL クライアントの実行が必要です。

- Unified Communications Manager リリース 7.1(2)
  - 7.1 (2) のすべての通常リリース
  - 007.001 (002.32016.001) より前の712のすべての ES リリース
- Unified Communications Manager リリース 7.1（3）
  - 007.001 (003.21900.003) より前の713のすべての通常リリース = 7.1 (3a) su1a
  - 007.001 (003.21005.001) より前の713のすべての ES リリース

（注） CTL クライアントの実行方法の詳細については、「「CTL クライアントの設定」」の章を参照してください。

Step 6 「[Prepare Cluster for Rollback to pre-8.0]」 エンタープライズ パラメータが [True] に設定されている場合、社内ディレクトリが機能するために以下の変更が必要です。

[Device] > [Device Settings] > [Phone Services] > [Corporate Directory] で、サービス URL を「Application:Cisco/CorporateDirectory」から「http://<ipaddr>:8080/ccmcip/xmldirectoryinput.jsp」へと変更します。

Step 7 「[Prepare Cluster for Rollback to pre-8.0]」 エンタープライズ パラメータが [True] に設定されている場合、パーソナル ディレクトリが機能するために以下の変更が必要です。

[Device] > [Device Settings] > [Phone Services] > [Personal Directory] で、サービス URL を「Application:Cisco/PersonalDirectory」から「http://<ipaddr>>:8080/ccmpd/pdCheckLogin.do?name=undefined」へと変更します。

復帰後のリリース8.6 以降へのスイッチバック

クラスタをリリース7.x に戻した後にリリース8.6 またはそれ以降のパーティションに切り替える場合は、次の手順に従います。

手順

Step 1 クラスタを非アクティブのパーティションに再度切り替えるための手順に従います。詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

Step 2 次のいずれかのリリースを混合モードで使用していた場合は、CTL クライアントを実行する必要があります。

Unified Communications Manager リリース 7.1(2)

- 7.1 (2) のすべての通常リリース
- 007.001 (002.32016.001) より前の712のすべての ES リリース
- Unified Communications Manager リリース 7.1(3)
  - 007.001 (003.21900.003) より前の713のすべての通常リリース = 7.1 (3a) su1a
  - 007.001 (003.21005.001) より前の713のすべての ES リリース

（注） CTL クライアントの実行方法の詳細については、「「CTL クライアントの設定」」の章を参照してください。

Step 3 [Unified Communications Manager Administration]で、**[System]** > **[Enterprise Parameters Configuration]** を選択します。

[Enterprise Parameters Configuration] ウィンドウが表示されます。

[Prepare Cluster for Rollback to pre-8.6] エンタープライズ パラメータを [False] に設定します。

Step 4 Cisco Unified IP 電話 が自動的に再起動され、Unified Communications Manager に登録されるまで、10 分間待ちます。

Cisco Unified Communications Manager と ITL ファイルを使用したクラスタ間での IP フォンの移行

Unified Communications Manager 8.0(1) 以降では、新しいデフォルトのセキュリティ機能と初期信頼リスト（ITL）ファイルが導入されました。この新機能を使用する場合は、異なるユニファイドCMクラスタ間で電話を移動する際には注意が必要です。また、移行のための適切な手順に従っていることを確認してください。

⚠

注意 正しい手順に従わないと、数千台の電話の ITL ファイルを手動で削除しなければならない状況が発生する可能性があります。

新しい ITL ファイルをサポートする Cisco IP 電話 では、Unified CM TFTP サーバからこの特別なファイルをダウンロードする必要があります。ITL ファイルが電話にインストールされると、設定ファイルおよびITL ファイルの以降の更新では、以下のいずれかによる署名が必要となります。

- 電話機に現在インストールされている TFTP サーバ証明書
- クラスタのいずれかで TV サービスを検証できる TFTP 証明書。ITL ファイルにリストされているクラスタ内の TV サービスの証明書を確認できます。

この新しいセキュリティ機能により、電話を別のクラスタに移動する場合に、次の 3 つの問題が発生する可能性があります。

1. 新しいクラスタの ITL ファイルが現在の ITL ファイルの署名者によって署名されていないため、電話が新しい ITL ファイルや設定ファイルを受け入れることができない問題。
2. 電話の既存の ITL にリストされている TVS サーバは、電話が新しいクラスタに移動すると接続できなくなる可能性があるという問題。
3. TVS サーバが証明書の検証のためにアクセス可能でも、古いクラスタ サーバには新しいサーバ証明書がない可能性があるという問題。

この 3 つの問題のうち 1 つ以上が発生した場合、考えられる解決策の 1 つは、クラスタ間を移動中のすべての電話から ITL ファイルを手作業で削除することです。ただし、この解決方法は電話の数が増えるにつれて大変な労力を必要とするため、望ましい解決策ではありません。

最も推奨されるオプションは、Cisco Unified CM エンタープライズ パラメータ [Prepare Cluster for Rollback to pre-8.0] を使用することです。このパラメータを [True] に設定すると、電話は空の TVS および TFTP 証明書セクションを含む特殊な ITL ファイルをダウンロードします。

電話に空の ITL ファイルがあると、（8.x 以前の Unified CM クラスタへの移行の場合）電話は署名のない設定ファイルをすべて受け入れます。また、（異なる Unified CM 8.x クラスタへの移行の場合）新しい ITL ファイルをすべて受け入れます。

空の ITL ファイルは、電話の **[Settings]** > **[Security]** > **[Trust List]** > **[ITL]** をチェックすることで確認できます。古い TVS や TFTP サーバが指定されていた場所には、空のエントリが表示されます。

新しい空の ITL ファイルをダウンロードできるまで、電話には古い Unified CM サーバにアクセスできる必要があります。

古いクラスタをオンラインのままにする予定の場合は、[Prepare cluster For Rollback to pre-8.0] エンタープライズパラメータを無効にして、デフォルトでセキュリティを復元します。

関連トピック

8.0 より前のリリースへのクラスタのロールバック, on page 18

証明書の一括エクスポート

新旧のクラスタが同時にオンラインになっている場合には証明書の一括移行による方法を使用できます。

Cisco Unified IP 電話 は、ダウンロードしたすべてのファイルを、ITL ファイルまたは ITL ファイルに指定されている TVS サーバと照合することに注意してください。電話を新しいクラスタに移動する必要がある場合、新しいクラスタが提示する ITL ファイルは、古いクラスタの TVS 証明書ストアの信頼を得る必要があります。

（注） 証明書の一括エクスポートは、電話の移行中、両方のクラスタがネットワークに接続され、オンラインである場合のみ機能します。

（注） 証明書一括インポート中、Cisco Extension Mobility Cross Cluster（EMCC）が動作を継続するには、訪問クラスタとホーム クラスタの両方において付加的な ITLRecovery 証明書をインポートすることが必要です。[証明書の一括管理（Bulk Certificate Management）] の [証明書タイプ（Certificate Type）] ドロップダウン リストに、ITL_Recovery 証明書をインポートするための新しいオプションが追加されています。

証明書の一括エクスポートを使用するには、以下の手順を実行します。

手順

Step 1 [Cisco Unified Operating System Administration] から、**[Security]** > **[Bulk Certificate Management]** を選択します。

Step 2 新しい宛先のクラスタ（TFTP のみ）から中央 SFTP サーバに証明書をエクスポートします。

Step 3 証明書の一括処理用のインターフェイスを使用して SFTP サーバで証明書（TFTP のみ）を統合します。

Step 4 元のクラスタで証明書の一括機能を使用し、中央SFTPサーバからTFTP証明書をインポートします。

Step 5 DHCPオプション150、またはその他の方法を使用して、電話機に新しい宛先クラスタを指定します。

電話は新しい宛先クラスタのITLファイルをダウンロードし、既存のITLファイルと照合することを試みます。証明書は既存のITLファイル内に存在しないため、電話は古いTVSサーバに新しいITLファイルの署名の確認を要求します。電話機はTCPポート2445の古いクラスタにTVSクエリを送信してこの要求を行います。

証明書のエクスポート、統合、インポートが正常に行われると、TVSは成功を返し、電話のメモリにあるITLファイルは新しくダウンロードされたITLファイルに置き換わります。

これで電話機は新しいクラスタから署名付きのコンフィギュレーション ファイルをダウンロードし、検証できるようになります。

自己署名証明書の生成

手順

Step 1 [Cisco Unified OS Administration] から **[Security]** > **[Certificate Management]** を選択します。
[証明書の一覧（Certificate List）] ウィンドウが表示されます。

Step 2 検索パラメータを入力して、証明書を検索して設定の詳細を表示します。
すべての条件に一致したレコードが **[Certificate List]** ウィンドウに表示されます。

Step 3 新しい自己署名証明書を生成するには、[Generate Self-Signed Certificate] をクリックします。
[Generate New Self-Signed Certificate] ウィンドウが表示されます。

Step 4 [Certificate Purpose] ドロップダウン ボックスから、[CallManager-ECDSA] などのシステム セキュリティ証明書を選択します。

Step 5 [Generate New Self-Signed Certificate] ウィンドウのフィールドを設定します。フィールドとその設定オプションの詳細については、「関連項目」の項を参照してください。

Step 6 [生成（Generate）] をクリックします。

関連トピック

自己署名証明書のフィールド, on page 24

自己署名証明書のフィールド

表 *1:* 自己署名証明書のフィールド

フィールド	説明
[Certificate Purpose]	ドロップダウンリストから必要なオプションを選択します。 次のいずれかのオプションを選択すると、[**Key Type**] フィールドは自動的に**RSA**に設定されます。 • Tomcat • IPSec • ITLRecovery • CallManager • CAPF • TVS 次のいずれかのオプションを選択すると、[**Key Type**] フィールドは自動的に**EC** (楕円曲線) に設定されます。 • tomcat-ECDSA • CallManager-ECDSA
ディストリビューション	ドロップダウンリストから Unified Communications Manager サーバを選択します。
[Auto-populated Domains]	[証明書の目的 (**Certificate** by)] ドロップダウンリストを使用して、次のいずれかのオプションを選択した場合にのみ表示されます。 • tomcat • tomcat-ECDSA • CallManager • CallManager-ECDSA • TVS このフィールドには、1つの証明書によって保護されているホスト名が一覧表示されます。証明書の共通名は、ホスト名と同じです。両方、**CALLMANAGER ecdsa**と**tomcat の**両方の証明書には、ホスト名とは異なる共通の名前があります。 このフィールドには、**CALLMANAGER ECDSA**証明書の完全修飾ドメイン名が表示されます。

フィールド	説明
キー タイプ	このフィールドには、公開キーと秘密キーのペアの暗号化および復号化に使用されるキーのタイプがリストされます。 Unified Communications Manager は **EC** および **RSA** キー タイプをサポートしています。
キーの長さ（Key Length）	ドロップダウンリストから、次のいずれかの値を選択します。 • 1024 • 2048 • 3072 • 4096 キーの長さによっては、自己署名証明書要求によってハッシュアルゴリズムの選択肢が制限されます。ハッシュアルゴリズムを限定して選択した場合は、キー長の強度以上のハッシュアルゴリズム強度を使用できます。 • キー長の値が256の場合、サポートされているハッシュアルゴリズムは SHA256、SHA384、または SHA512 です。 • キー長の値が384の場合、サポートされているハッシュアルゴリズムは SHA384 または SHA512 です。 （注） **キー長**の値が3072または4096の証明書は、RSA 証明書に対してのみ選択されます。これらのオプションは、ECDSA 証明書では使用できません。 （注） CallManager の **[Certificate Purpose]** で選択された RSA **キー長**の値が 2048 を超えると、電話機のモデルによっては登録に失敗する場合があります。 詳細については、Cisco Unified Reporting Tool（CURT）の [**Unified CM Phone Feature List Report**] で、**3072/4096 RSA キー サイズ サポート**に対応した電話機モデルの一覧を確認できます。

フィールド	説明
Hash Algorithm	ドロップダウンリストからキーの長さ以上の値を選択します。 （注） • [**ハッシュアルゴリズム (Hash Algorithm)**] ドロップダウンリストの値は、[**キー長 (Key Length)**] フィールドで選択した値に基づいて変わります。 • システムが FIPS モードで実行されている場合は、必ずハッシュアルゴリズムとして SHA256 を選択する必要があります。

証明書署名要求の生成

特定の証明書タイプに対して新しい証明書署名要求を生成すると、アプリケーションはその証明書タイプの既存の証明書署名要求を上書きします。

CA 署名付き証明書をアップロードするには、Cisco ユニファイドオペレーティングシステムの管理から CSR を生成し、CA に提示します。CSR を生成するたびに、CSR とともに新しい秘密キーが生成されます。

秘密キーは、CSR の生成時に選択したサーバとサービスに固有のファイルです。セキュリティコンプライアンスのために、この秘密キーを誰とも共有しないでください。秘密キーを誰かに渡すと、証明書のセキュリティが損なわれます。また、古い CSR を使用して証明書を作成する場合は、同じサービス用の新しい CSR を再生成しないでください。Unified Communications Manager は古い CSR と秘密キーを削除し、それらの両方を新しいものに置き換えて、古い CSR を使用不能にします。

（注） Unified Communications Manager リリース 11.0 以降では、TFTP またはすべての一括操作ユニットを選択した場合は、ECDSA 証明書は RSA 証明書に含まれるようになります。

手順

Step 1 [Cisco Unified OS Administration] から **[Security]** > **[Certificate Management]** を選択します。
[証明書の一覧（Certificate List）] ウィンドウが表示されます。

Step 2 [CSR の作成（Generate CSR）] をクリックします。
[Generate Certificate Signing Request] ウィンドウが表示されます。

Step 3 検索パラメータを入力して、証明書を検索して設定の詳細を表示します。
すべての条件に一致したレコードが **[Certificate List]** ウィンドウに表示されます。

Step 4 [証明書の目的 (**Certificate** by)] ドロップダウンボックスから、 **CallManager-ECDSA**などのシステムセキュリティ証明書を選択します。

Step 5 [Generate Certificate Signing Request] ウィンドウのフィールドを設定します。フィールドとその設定オプションの詳細については、「関連項目」の項を参照してください。

Step 6 [生成（Generate）] をクリックします。

関連トピック

証明書署名要求のフィールド, on page 27

証明書署名要求のフィールド

表 *2:* 証明書署名要求のフィールド

フィールド	説明
[Certificate Purpose]	ドロップダウン ボックスから値を選択します。 • **CallManager** • **CallManager-ECDSA**

ディストリビューション	Unified Communications Manager サーバを選択します。
	ECDSA の MultiServer にこのフィールドを選択すると、構文は次のとおりです。
	`Callmanager-ecdsa common name: <host-name>-EC-ms.<domain>`
	RSA の MultiServer にこのフィールドを選択すると、構文は次のとおりです。
	`Callmanager common name: <host-name>-ms.<domain>`

	デフォルトでは、**[Distribution]** フィールドで選択した Unified Communications Manager アプリケーションの名前が表示されます。
[Auto-populated Domains]	このフィールドは、サブジェクト代替名 (SANs) セクションに表示されます。単一の証明書によって保護されるホスト名が一覧表示されます。
[Parent Domain]	このフィールドは [Subject Alternate Names（SANs）] セクションに表示されます。デフォルトドメイン名を表示します。必要に応じて、ドメイン名を変更できます。
キー タイプ	このフィールドは、公開キーと秘密キーのペアの暗号化と復号化に使用されるキーのタイプを示します。 Unified Communications Manager は **EC** および **RSA** キー タイプをサポートしています。

フィールド	説明
キーの長さ（Key Length）	[**Key Length**] ドロップダウンボックスから、値の1つを選択します。 キーの長さによっては、CSR要求によってハッシュアルゴリズムの選択肢が制限されます。ハッシュアルゴリズムを限定して選択することで、キー長の強度以上のハッシュアルゴリズム強度を使用できます。たとえば、キーの長さが256の場合、サポートされているハッシュアルゴリズムはSHA256、SHA384、またはSHA512です。同様に、384のキー長の場合、サポートされているハッシュアルゴリズムはSHA384またはSHA512です。 （注） **キー長**の値が3072または4096の証明書は、RSA証明書に対してのみ選択できます。これらのオプションは、ECDSA証明書については使用できません。 （注） 一部の電話機モデルでは、CallManagerの[証明書の目的（Certificate Purpose）]に対して選択されたRSAの[キーの長さ（key length）]が2048を超える場合、登録に失敗します。Cisco Unified Reporting Tool（CURT）の[Unified CM Phone Feature List Report]で、3072/4096 RSAキー サイズ サポート機能をサポートする電話モデルの一覧を確認できます。
Hash Algorithm	[**ハッシュアルゴリズム (Hash algorithm)**] ドロップダウンボックスから値を選択して、楕円曲線のキー長としてより強力なハッシュアルゴリズムを設定します。[**ハッシュアルゴリズム (Hash Algorithm)**] ドロップダウンボックスから、値の1つを選択します。 （注） • [**ハッシュアルゴリズム (Hash Algorithm)**] フィールドの値は、[**キー長 (Key Length)**] フィールドで選択した値に基づいて変わります。 • システムがFIPSモードで実行されている場合は、必ずハッシュアルゴリズムとしてSHA256を選択する必要があります。

連携動作と制限事項

• **TLS_ECDHE_ECDSA_WITH_AES256_SHA384**および TLS_ECDHE_ECDSA_WITH_AES128_SHA256 をサポートしない SIP デバイスは、引き続き TLS_ECDHE_RSA_WITH_AES_256_SHA384 、**TLS_ECDHE_ に接続できます RSA_WITH_AES_128_SHA256**、またはAES128_SHA。これらのオプションは、選択したTLS

暗号オプションによって異なります。[**Ecdsa only**] オプションを選択した場合、ecdsa 暗号をサポートしていないデバイスは、SIP インターフェイスへの TLS 接続を確立できません。[**ECDSA only**] オプションを選択した場合、このパラメータの値は **TLS_ECDHE_ECDSA_WITH_AES128_SHA256** と **TLS_ECDHE_ECDSA_WITH_AES256_SHA384** になります。

- CTI Manager セキュアクライアントは、 **TLS_ECDHE_RSA_WITH_AES_128_SHA256** 、 **TLS_ECDHE_RSA_WITH_AES_256_SHA384**、 **TLS_ECDHE_ECDSA_WITH_AES_128_SHA256**、および **TLS_ECDHE_ECDSA_WITH_AES_256_SHA384** をサポートしていません。ただし、 **AES128_SHA** を使用して接続できます。

ITL ファイルの一括リセットの実行

この手順を実行できるのは、Unified Communications Manager パブリッシャのみからであることを確認してください。

電話機が ITL ファイル 署名者を信頼できなくなり、かつ TFTP サービスによってローカルに提供された ITL ファイルを認証できないか、TVS を使用して認証できない場合は、ITL ファイルの一括リセットが実行されます。

一括リセットを実行するには、CLI コマンド **utils itl reset** を使用します。このコマンドは新しい ITL リカバリファイルを生成し、電話機と CUCM の TFTP サービス間の信頼を再確立します。

ヒント Unified Communications Manager をインストールする場合は、CLI コマンド **file get tftp** *ITLRecovery.p12* を使用して ITL リカバリペアをエクスポートしてから、DR を介してバックアップを実行します。（キーのエクスポート先となる）SFTP サーバとパスワードの入力を求めるプロンプトも表示されます。

手順

Step 1 次のいずれかの手順を実行します。

- **utils itl reset localkey** を実行します。
- **utils itl reset remotekey** を実行します。

（注） **utils itl reset localkey** の場合、ローカルキーはパブリッシャにあります。このコマンドを発行しているとき、ITL 回復キーをリセットしている間、ITL ファイルは CallManager キーによって一時的に署名されます。

Step 2 **show itl** を実行してリセットが正常に行われたことを確認します。

Step 3 Cisco Unified CM Administration から、**[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）]** を選択します。

Step 4 [Reset] をクリックします。

デバイスが再起動されます。これで、CallManager キーで署名された ITL ファイルをダウンロードし、設定ファイルを受け入れる準備が整いました。

Step 5 TFTP サービスを再起動し、すべてのデバイスを再起動します。

（注） TFTP サービスを再起動すると、ITL ファイルが ITLRecovery キーによって署名され、ステップ 1 の変更がロールバックされます。

デバイスは、ITLRecovery キーで署名された ITL ファイルをダウンロードし、Unified Communications Manager に正しく再登録します。

CTL ローカルキーのリセット

Unified Communications Manager クラスタ上のデバイスがロックされ、信頼されたステータスが失われる場合は、CLI コマンド **ctl reset localkey** を使用して Cisco Trust List（CTL）ファイルのリセットを実行します。このコマンドにより、新しい CTL ファイルが生成されます。

手順

Step 1 **utils ctl reset localkey** の実行

（注） **utils ctl reset localkey** では、ローカルキーはパブリッシャ側にあります。このコマンドを発行すると、CTL ファイルは ITLRecovery キーによって一時的に署名されます。

Step 2 リセットが正常に行われたことを確認するには **show ctl** を実行します。

Step 3 Cisco Unified CM Administration から、**[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）]** を選択します。
[エンタープライズパラメータの設定（Enterprise Parameters Configuration）] ページが表示されます。

Step 4 [Reset] をクリックします。

デバイスが再起動されます。これで、CallManager キーで署名された CTL ファイルをダウンロードし、設定ファイルを受け入れる準備が整いました。

Step 5 **utils ctl update CTLFile** を実行して、ステップ 1 の変更をロールバックする必要なサービスを再起動します。

デバイスが再起動されます。これで、ITLRecovery キーで署名された CTL ファイルをダウンロードし、設定ファイルを受け入れる準備が整いました。

デバイスは、必要なキーを使用して署名された CTL ファイルをダウンロードし、Unified Communications Manager に再度正しく登録します。

ITLRecovery 証明書の有効期間の表示

ITLRecovery 証明書は電話機での有効期間が長いです。[証明書ファイルデータ（Certificate File Data）] ペインに移動し、有効期間または他の ITLRecovery 証明書の詳細を表示できます。

手順

Step 1 Cisco Unified OS の管理から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

Step 2 証明書を検索し、設定の詳細を表示するには、必要な検索パラメータを入力します。
条件に一致する証明書のリストが [証明書リスト（Certificate List）] ページに表示されます。

Step 3 [ITLRecovery] リンクをクリックして、有効期間を確認します。

ITLRecovery 証明書の詳細が [証明書ファイルデータ（Certificate File Data）] ペインに表示 されます。

有効期間は現在の年から 20 年です。

連絡先検索認証タスクフロー

Unified Communications Manager で連絡先検索の認証をセットアップするには、次のタスクを実行します。この機能が設定されている場合、ユーザはディレクトリで他のユーザを検索する前にユーザ自身を認証する必要があります。

手順

	コマンドまたはアクション	目的
Step 1	連絡先検索の認証の電話サポートの確認（32 ページ）	電話でこの機能がサポートされていることを確認します。Cisco Unified Reporting で [Unified CM Phone Feature List] レポートを実行し、この機能をサポートしている電話モデルのリストを確認します。
Step 2	連絡先検索の認証の有効化 （32 ページ）	Unified Communications Manager で連絡先検索の認証を設定します。

	コマンドまたはアクション	目的
Step 3	連絡先検索用のセキュアなディレクトリサーバの設定 （33 ページ）	電話のユーザがディレクトリで他のユーザを検索したときに示される URL を Unified Communications Manager で設定するには、次の手順を実行します。

連絡先検索の認証の電話サポートの確認

導入環境内の電話が連絡先検索の認証をサポートしていることを確認します。[Phone Feature List] レポートを実行して、この機能をサポートしているすべての電話モデルのリストを取得します。

手順

Step 1 Cisco Unified Reporting から [システム レポート(System Reports)] をクリックします。

Step 2 **[ユニファイド CM 電話機能 (Unified CM Phone Feature)]** を選択します。

Step 3 [ユニファイド CM 電話機能 (Unified CM Phone Feature)] レポートをクリックします。

Step 4 [製品 (Product)] フィールドはデフォルト値のままにします。

Step 5 **[機能 (Feature)]** ドロップダウンから **[Authenticated Contact Search]** を選択します。

Step 6 [送信（Submit）] をクリックします。

連絡先検索の認証の有効化

電話ユーザの連絡先検索認証を設定するには、Unified Communications Manager で次の手順を使用します。

手順

Step 1 コマンドライン インターフェイスにログインします。

Step 2 **utils contactsearchauthentication status** コマンドを実行し、このノードの連絡先検索の認証の設定を確認します。

Step 3 連絡先検索の認証の設定が必要な場合、

- 認証を有効にするには、**utils contactsearchauthentication enable** コマンドを実行します。
- 認証を無効にするには、**utils contactsearchauthentication disable** コマンドを実行します。

Step 4 すべての Unified Communications Manager のクラスタノードに対してこの手順を繰り返します。

（注） 変更を有効にするには、電話をリセットする必要があります。

連絡先検索用のセキュアなディレクトリ サーバの設定

UDS がユーザ検索リクエストを送信するディレクトリサーバ URL を Unified Communications Manager に設定するには、次の手順を使用します。デフォルトの値は `https://<cucm-fqdn-or-ip>:port/cucm-uds/users` です。

（注） デフォルトの UDS ポートは 8443 です。連絡先検索の認証が有効になると、デフォルトの UDS ポートは 9443 に切り替わります。その後、連絡先検索の認証を無効にした場合は、UDS ポートを手動で 8443 に戻す必要があります。

手順

Step 1 Cisco Unified Communications Manager Administrationから、**[システム（System）] > [エンタープライズパラメータ（Enterprise Parameter）]** を選択します。

Step 2 [Secure Contact Search URL] テキスト ボックスに、セキュアな UDS ディレクトリ要求の URL を入力します。

（注） URL には、Cisco TFTP サービスを実行していないノードを選択することを推奨します。Cisco TFTP と UDS サービスのいずれかのサービスが再起動すると、互いに悪影響が及ぶ可能性があります。

Step 3 [保存（Save）] をクリックします。