証明書の管理

証明書の概要

システムでは、自己署名証明書とサードパーティの署名付き証明書が使用されます。送信元から宛先までのデータ整合性を確保するために、デバイスのセキュア認証、データの暗号化、データのハッシュを行う際に、システム内のデバイス間で証明書を使用します。証明書を使用することにより、帯域幅、通信、操作のセキュアな転送が可能になります。

証明書を使用する際、意図した Web サイト、電話、FTP サーバなどのエンティティとの間でデータがどのように暗号化され共有されているかを理解し、それを定義することが最も重要な部分です。

システムが証明書を信頼するということは、システムにプレインストールされている証明書によって、適切な接続先と情報を共有していることが完全に確信されているということです。そうでない場合、システムはこれらのポイント間の通信を終了します。

証明書を信頼するには、サードパーティ認証局（CA）によって信頼がすでに確立されている必要があります。

まずデバイスが CA 証明書と中間証明書の両方を信頼できると認識していることが必要であり、そうであるならデバイスは Secure Socket Layer（SSL）ハンドシェイクというメッセージの交換によって提供されるサーバ証明書を信頼することができます。

（注） Tomcat 用の EC ベースの証明書がサポートされています。この新しい証明書を tomcat-ECDSA といいます。詳細については、『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』の「Enhanced TLS Encryption on IM and Presence Service」の章を参照してください。

Tomcat インターフェイスの EC 暗号はデフォルトで無効になっています。Cisco Unified Communications Manager または IM and Presence Service で [HTTPS 暗号（HTTPS Ciphers）] のエンタープライズパラメータを使用して、これらを有効にできます。このパラメータを変更すると、すべてのノードで Cisco Tomcat サービスを再起動する必要があります。

EC ベースの証明書の詳細については、Cisco Unified Communications Manager and IM and Presence Service リリース ノートの「ECDSA Support for Common Criteria for Certified Solutions」を参照してください。

サードパーティの署名付き証明書または証明書チェーン

アプリケーション証明書に署名した認証局の認証局ルート証明書をアップロードします。下位認証局がアプリケーション証明書に署名した場合は、下位認証局の認証局ルート証明書をアップロードする必要があります。すべての認証局証明書の PKCS#7 形式の証明書チェーンもアップロードできます。

認証局ルート証明書およびアプリケーション証明書は、同じ [証明書のアップロード（Upload Certificate）] ダイアログボックスを使用してアップロードできます。認証局ルート証明書または認証局証明書だけが含まれる証明書チェーンをアップロードする場合は、certificate type-trust 形式の証明書名を選択します。アプリケーション証明書またはアプリケーション証明書と認証局証明書が含まれる証明書チェーンをアップロードする場合は、証明書タイプだけが含まれている証明書名を選択します。

たとえば、Tomcat 認証局証明書または認証局証明書チェーンをアップロードする場合は [tomcat-trust] を選択します。Tomcat アプリケーション証明書またはアプリケーション証明書と認証局証明書が含まれる証明書チェーンをアップロードする場合は、[tomcat] または [tomcat-ECDSA] を選択します。

CAPF 認証局ルート証明書をアップロードすると、CallManager の信頼ストアにコピーされるため、認証局ルート証明書を個別に CallManager にアップロードする必要はありません。

（注） サードパーティの認証局署名付き証明書が正常にアップロードされると、署名付き証明書を取得するために使用された、最近生成した CSR が削除され、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。

（注） tomcat-trust、CallManager-trust、およびPhone-SAST-trust証明書がクラスタの各ノードに自動的にレプリケートされます。

（注） DirSyncサービスをセキュア モードで実行する場合に必要となるディレクトリの信頼証明書は、tomcat-trustにアップロードすることができます。

サードパーティ認証局証明書

サードパーティ認証局が発行するアプリケーション証明書を使用するには、署名付きのアプリケーション証明書と認証局ルート証明書の両方を認証局から取得するか、アプリケーション証明書と認証局証明書の両方が含まれているPKCS#7証明書チェーン（Distinguished Encoding Rules[DER]）から取得する必要があります。これらの証明書の取得に関する情報は、認証局から入手してください。証明書を取得するプロセスは、認証局によって異なります。署名アルゴリズムではRSA暗号化が使用されている必要があります。

Cisco Unified Communicationsオペレーティング システムでは、プライバシー強化メール（PEM）エンコード形式でCSRが作成されます。システムは、DERおよびPEMエンコード形式の証明書と、PEM形式のPKCS#7証明書チェーンを受け入れます。認証局プロキシ機能（CAPF）以外のすべての証明書タイプの場合、それぞれのノードについて認証局ルート証明書およびアプリケーション証明書を取得してアップロードする必要があります。

CAPFの場合、最初のノードについてのみ認証局ルート証明書およびアプリケーション証明書を取得してアップロードします。CAPFおよびUnified Communications ManagerのCSRには、認証局へのアプリケーション証明書要求に含める必要のある拡張情報が含まれています。認証局が拡張要求メカニズムをサポートしていない場合は、次の手順に従ってX.509拡張を有効にする必要があります。

- CAPF CSRでは、次の拡張情報が使用されます。

```
X509v3 拡張キーの使用： TLS Web サーバ認証、X509v3 キーの使用： デジタル署名、証明書署名
```

- TomcatおよびTomcat-ECDSAのCSRでは、次の拡張情報が使用されます。

（注） TomcatまたはTomcat-ECDSAは、キー アグリーメントやIPsecエンド システム キーを使用する必要はありません。

```
X509v3 拡張キー使用： TLS Web サーバ認証、TLS Web クライアント認証、IPSec エンド システム X509v3 キー使用： デジタル署名、キー暗号化、データ暗号化、キー同意
```

- IPsec の CSR では、次の拡張情報が使用されます。

```
X509v3 拡張キー使用： TLS Web サーバ認証、TLS Web クライアント認証、IPSec エンド システム X509v3 キー使用： デジタル署名、キー暗号化、データ暗号化、キー同意
```

- Unified Communications Manager の CSR では、次の拡張情報が使用されます。

```
X509v3 拡張キー使用： TLS Web サーバ認証、TLS Web クライアント認証 X509v3 キー使用： デジタル署名、キー暗号化、データ暗号化、キー同意
```

- IM and Presence Service cup および cup-xmpp 証明書の CSR は、次の拡張機能を使用します。

```
X509v3 拡張キー使用：TLS Web サーバ認証、TLS Web クライアント認証、IPSec エンド システム X509v3 キー使用：デジタル署名、キー暗号化、データ暗号化、キー同意
```

（注） 使用する証明書に対してCSRを生成し、SHA256署名を使用してサードパーティ認証局に署名させることもできます。この署名付き証明書を Unified Communications Manager に再度アップロードすることで、Tomcat および他の証明書が SHA256 をサポートできるようになります。

証明書署名要求のキー用途拡張

次の表に、Unified Communications Manager と IM and Presence Service の CA 証明書の両方に対する証明書署名要求（CSR）の主な使用法の拡張を示します。

表 *1 : Cisco Unified Communications Manager CSR* キー鍵用途拡張

	マルチサーバー	拡張キーの使用状況			キーの使途（Key Usage）				
		サーバ認証 (1.3.6.1.5.5.7.3.1)	クライアント認証 (1.3.6.1.5.5.7.3.2)	IP セキュリティ末端システム (1.3.6.1.5.5.7.3.5)	[デジタル署名（Digital Signature）]	鍵の暗号化	データの暗号化	鍵証明書サイン	鍵共有
CallManager CallManager-ECDSA	Y	Y	Y		Y	N	Y		
CAPF（パブリッシャーのみ）	N	Y	Y		Y	Y		Y	
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	N	Y		
TVS	Y	Y	Y		Y	Y	Y		

表 *2 : IM and Presence* サービスの *CSR* キーの用途の拡張

	マルチサーバー	拡張キーの使用状況			キーの使途（Key Usage）				
		サーバ認証 (1.3.6.1.5.5.7.3.1)	クライアント認証 (1.3.6.1.5.5.7.3.2)	IP セキュリティ末端システム (1.3.6.1.5.5.7.3.5)	[デジタル署名（Digital Signature）]	鍵の暗号化	データの暗号化	鍵証明書サイン	鍵共有
cup cup-ECDSA	N	Y	Y	Y	Y	Y	Y		Y
cup-xmpp cup-xmpp-ECDSA	Y	Y	Y	Y	Y	Y	Y		Y
cup-xmpp-s2s cup-xmpp-s2s-ECDSA	Y	Y	Y	Y	Y	Y	Y		Y
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		

証明書の表示

[証明書リスト] ページのフィルタ オプションを使用して、共通名、有効期限日付、キー タイプ、および使用方法に基づいて証明書のリストを並べ替えて表示できます。このため、フィルタ オプションを使用すると、データの並べ替え、表示、およびデータの効率的な管理を行えます。

Unified Communications Manager リリース 14 から、使用オプションを選択して、ID または信頼証明書のリストを並べ替え、表示できます。

手順

ステップ 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。
[Certificate List] ページが表示されます。

ステップ 2 **[証明書リストの検索場所]** ドロップダウン リストから、必要なフィルタ オプションを選択し、**[検索]** フィールドに検索項目を入力して **[検索]** ボタンをクリックします。

たとえば、アイデンティティ証明書だけを表示するには、[証明書の一覧の検索条件（Find Certificate List where）] ドロップダウンリストから [使用法（Usage）] を選択し、[検索（Find）] フィールドにアイデンティティを入力して、[検索（Find）] ボタンをクリックします。

証明書のダウンロード

CSR リクエストを送信する際、ダウンロード証明書タスクを使用して証明書のコピーを作成するか、証明書をアップロードします。

手順

ステップ 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。

ステップ 2 検索情報を指定し、**[検索（Find）]** をクリックします。

ステップ 3 必要なファイル名を選択し、**[ダウンロード]** をクリックします。

中間証明書のインストール

中間証明書をインストールするには、まずルート証明書をインストールしてから、署名付き証明書をアップロードする必要があります。この手順は、認証局から1つの署名付き証明書と複数の証明書が証明書チェーンで提供されている場合にのみ必要です。

手順

ステップ 1 [Cisco Unified OS の管理（Cisco Unified OS Administration）] から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** をクリックします。

ステップ 2 **[証明書/証明書チェーンのアップロード]** をクリックします。

ステップ 3 **[証明書の用途]** ドロップダウンリストで適切な信頼ストアを選択して、ルート証明書をインストールします。

ステップ 4 選択した証明書の説明を入力します。

ステップ 5 次のいずれかの手順を実行して、アップロードするファイルを選択します。

- [ファイルのアップロード（Upload File）] テキスト ボックスに、ファイルへのパスを入力します。
- [参照（Browse）] をクリックしてファイルに移動し、[開く（Open）] をクリックします。

ステップ 6 [アップロード（Upload）] をクリックします。

ステップ 7 顧客証明書をインストールしたら、FQDN を使用して Cisco Unified Intelligence Center の URL にアクセスします。IP アドレスを使用して Cisco Unified Intelligence Center にアクセスすると、カスタム証明書を正常にインストールした後でも「ここをクリックしてログインを継続します（Click here to continue）」のメッセージが表示されます。「」

（注）
- tomcat 証明書をアップロードするときは、TFTP サービスを無効にし、その後有効にします。それ以外の場合は、TFTP は古いキャッシュの自己署名された tomcat 証明書を提供し続けます。

信頼証明書の削除

削除できる証明書は、信頼できる証明書だけです。システムで生成される自己署名証明書は削除できません。

⚠

注意 証明書を削除すると、システムの動作に影響する場合があります。また、証明書が既存のチェーンの一部である場合、証明書チェーンが壊れることがあります。この関係は、**[証明書の一覧（Certificate List）]** ウィンドウ内の関連する証明書のユーザ名とサブジェクト名から確認します。この操作は取り消すことができません。

手順

ステップ 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。

ステップ 2 証明書の一覧をフィルタするには、**[検索（Find）]** コントロールを使用します。

ステップ 3 証明書のファイル名を選択します。

ステップ 4 **[削除（Delete）]** をクリックします。

ステップ 5 **[OK]** をクリックします。

（注）
- 削除する証明書が 「CAPF-trust」、「tomcat-trust」、「CallManager-trust」、または 「Phone-SAST-trust」 証明書タイプの場合、証明書はクラスタ内のすべてのサーバで削除されます。
- 証明書を CAPF-trust にインポートする場合、それはその特定のノードでのみ有効になり、クラスタ全体で複製されることはありません。

証明書の再作成

証明書が期限切れになる前に、証明書を再生成することを推奨します。RTMT（Syslog Viewer）で警告が発行され、証明書の期限が近くなると電子メールで通知が送信されます。

ただし、期限切れの証明書を再生成することもできます。電話機を再起動してサービスを再起動する必要があるため、営業時間後にこのタスクを実行します。Cisco Unified OS の管理に「cert」タイプとしてリストされている証明書のみ再作成できます。

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。証明書を再作成すると、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。

手順

ステップ 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。

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。

証明書の詳細ページで**[再生成（Regenerate）]**ボタンをクリックすると、同じキー長を持つ自己署名証明書が再生成されます。

3072 または 4096 の新しいキー長の自己署名証明書を再生成するには、**[自己署名証明書の生成（Generate Self-Signed Certificate）]** をクリックします。

ステップ 2 **[自己署名証明書の新規作成（Generate New Self-Signed Certificate）]** ウィンドウのフィールドを設定します。フィールドおよびその設定オプションの詳細については、オンラインヘルプを参照してください。

ステップ 3 **[生成（Generate）]** をクリックします。

ステップ 4 再作成された証明書の影響を受けるサービスをすべて再起動します。詳細については、証明書の名前と説明 （8 ページ）を参照してください。

ステップ 5 CAPF、ITLRecovery 証明書または CallManager 証明書の再作成後に CTL クライアントを更新します（設定している場合）。

（注） 証明書を再作成したら、システムのバックアップを実行して、最新のバックアップに再作成した証明書が含まれるようにします。バックアップに再作成した証明書が含まれていない状態でシステムの復元タスクを実行する場合は、システム内の各電話機のロックを手動で解除して、電話機を登録できるようにする必要があります。

証明書の名前と説明

次の表に、再作成可能なシステムのセキュリティ証明書と、再起動する必要がある関連サービスを示します。TFTP 証明書の再作成の詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/

products-maintenance-guides-list.html の『*Cisco Unified Communications Manager Security Guide*』を参照してください。

表 *3*:証明書の名前と説明

名前	説明	関連サービス
tomcat tomcat-ECDSA	この証明書は、SIP Oauth モードが有効になっているときに Web サービス、Cisco DRF サービス、および Cisco CallManager サービスで使用されます。	Cisco Tomcat サービス、Cisco CallManager サービス、HAProxy サービス、および Cisco ディザスタリカバリシステム（DRS）のローカルサービスとマスターサービス。
ipsec	この自己署名ルート証明書は、ユニファイド コミュニケーション マネージャ、MGCP、H.323、IM およびプレゼンス サービスとの IPsec 接続のインストール中に生成されます。	IPSec サービス
CallManager CallManager-ECDSA	これは SIP、SIP トランク、SCCP、TFTP などに使用されます。	CallManager - HAProxy サービス CallManager-ECDSA - Cisco CallManager サービス
CAPF	Unified Communications Manager Publisher で実行されている CAPF サービスによって使用されます。この証明書は、エンドポイントに LSC を発行するために使用されます(オンラインとオフラインの CAPF モードを除く)。	N/A
TVS	これは Trust 検証サービスで使用されます。これは、サーバ証明書が変更された場合に電話機のセカンダリ信頼検証メカニズムとして機能します。	N/A

（注） TVS、CAPF、またはTFTP証明書のいずれかを更新した場合に、手動または自動で電話機をリセットするには、証明書の更新に関する新しい企業パラメータの電話機の相互操作を導入します。このパラメータは、デフォルトで電話機を自動的にリセットするために設定されています。

OAuth 更新ログイン用のキーの再生成

コマンドラインインターフェイスを使用して暗号キーと署名キーの両方を再生成するには、この手順を使用します。Cisco Jabber が Unified Communications Manager との OAuth 認証に使用する暗号キーまたは署名キーが侵害された場合にのみ、この作業を実行します。署名キーは非対称で RSA ベースであるのに対し、暗号キーは対称キーです。

このタスクを完了すると、これらのキーを使用する現在のアクセストークンと更新トークンは無効になります。

エンドユーザへの影響を最小限に抑えるために、このタスクは営業時間外に完了することを推奨します。

暗号キーは、以下の CLI を使用してのみ再生成できますが、発行元の Cisco Unified OS の管理 GUI を使用して署名キーを再生成することもできます。**[セキュリティ]** > **[証明書の管理]** を選択し、**AUTHZ** 証明書を選択して、**[再作成]** をクリックします。

手順

ステップ 1 Unified Communications Manager発行元ノードで**コマンドライン**インターフェイスにログインします。

ステップ 2 暗号キーを再生成するには、次の手順を実行します。

a) `set key regen authz encryption` コマンドを実行します。

b) 「`yes`」と入力します。

ステップ 3 署名キーを再生成するには、次の手順を実行します。

a) `set key regen authz signing` コマンドを実行します。

b) 「`yes`」と入力します。

Unified Communications Manager パブリッシャ ノードがキーを再生成し、IM and Presence サービスのローカル ノードを含めたすべての Unified Communications Manager クラスタ ノードに新しいキーを複製します。

すべての UC クラスタで新しいキーを再生成して同期する必要があります。

- IM and Presence 中央クラスタ：IM and Presence 集中型展開の場合、IM and Presence ノードはテレフォニーとは別のクラスタ上で実行されています。この場合、IM and Presence Service の中央クラスタの Unified Communications Manager パブリッシャ ノードで、この手順を繰り返します。

- Cisco Expressway または Cisco Unity Connection：これらのクラスタ上でもキーを再生成します。詳細については、Cisco Expressway および Cisco Unity Connection のマニュアルを参照してください。

（注） 次のシナリオでは、Cisco XCP 認証サービスを再起動する必要があります。

- 認定証明書を再作成する場合
- IM and Presence 管理者コンソールで中央集中型導入に新しくエントリを作成する場合

証明書または証明書チェーンのアップロード

システムで信頼する新しい証明書または証明書チェーンをアップロードします。

手順

ステップ 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。

ステップ 2 **[証明書/証明書チェーンのアップロード]** をクリックします。

ステップ 3 [証明書の用途（Certificate Purpose）] ドロップダウン リストで、証明書名を選択します。

ステップ 4 次のいずれかの手順を実行して、アップロードするファイルを選択します。

- [ファイルのアップロード（Upload File）] テキスト ボックスに、ファイルへのパスを入力します。
- [参照（Browse）] をクリックしてファイルに移動してから、[開く（Open）] をクリックします。

ステップ 5 ファイルをサーバにアップロードするには、[ファイルのアップロード（Upload File）] をクリックします。

（注） 証明書をアップロードしたら、影響を受けるサービスを再起動します。サーバが再起動したら、CCMAdmin または CCMUser GUI にアクセスして、新しく追加した証明書が使用されていることを確認できます。

サードパーティ証明書の認証局の管理

このタスク フローでは、サードパーティ証明書プロセスの概要を、各ステップへの参照とともに順番に説明します。お使いのシステムは、サードパーティ認証局が PKCS # 10 証明書署名要求（CSR）を使用して発行する証明書をサポートしています。

手順

	コマンドまたはアクション	目的
ステップ 1	証明書署名要求の生成 （13 ページ）	証明書署名要求（CSR）を生成します。これは、公開キー、組織名、共通名、地域、および国などの証明書申請情報を含む暗号化されたテキストのブロックです。認証局はこの CSR を使用して、ご使用のシステムの信頼できる証明書を生成します。
ステップ 2	証明書署名要求のダウンロード （13 ページ）	CSR を作成後、ダウンロードして、認証局に証明書を送信できるようにします。
ステップ 3	認証局のドキュメントを参照してください。	認証局からアプリケーション証明書を取得します。
ステップ 4	認証局のドキュメントを参照してください。	認証局からルート証明書を取得します。
ステップ 5	信頼ストアへの認証局署名済み CAPF ルート証明書の追加 （14 ページ）	ルート証明書を信頼ストアに追加します。認証局の署名付き CAPF 証明書を使用している場合は、この手順を実行します。
ステップ 6	証明書または証明書チェーンのアップロード （11 ページ）	認証局ルート証明書をノードにアップロードします。
ステップ 7	CAPF または Cisco Unified Communications Manager の証明書を更新した場合は、新しい CTL ファイルを生成します。	『*Cisco Unified Communications Manager Security Guide*』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。 サードパーティの署名付き CAPF または CallManager 証明書をアップロードしたら、CTL クライアント（設定している場合）を再実行します。

	コマンドまたはアクション	目的
ステップ 8	サービスの再起動 （14 ページ）	新しい証明書の影響を受けるサービスを再起動します。すべての証明書タイプで、対応するサービスを再起動します（たとえば、Tomcat または Tomcat-ECDSA の証明書を更新した場合は Cisco Tomcat サービスを再起動します）。

証明書署名要求の生成

証明書署名要求（CSR）を生成します。これは、公開キー、組織名、共通名、地域、および国などの証明書申請情報を含む暗号化されたテキストのブロックです。認証局はこの CSR を使用して、ご使用のシステムの信頼できる証明書を生成します。

（注） 新しい CSR を生成すると、既存の CSR は上書きされます。

手順

ステップ 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。

ステップ 2 [CSR の作成（Generate CSR）] をクリックします。

ステップ 3 **[証明書署名要求の作成]** 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、オンライン ヘルプを参照してください。

ステップ 4 [生成（Generate）] をクリックします。

証明書署名要求のダウンロード

CSR を作成後、ダウンロードして、認証局に証明書を送信できるようにします。

手順

ステップ 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。

ステップ 2 [CSR のダウンロード（Download CSR）] をクリックします。

ステップ 3 [証明書の用途（Certificate Purpose）] ドロップダウン リストで、証明書名を選択します。

ステップ 4 [CSR のダウンロード（Download CSR）] をクリックします。

ステップ 5 （任意） プロンプトが表示されたら、[保存（Save）] をクリックします。

信頼ストアへの認証局署名済み CAPF ルート証明書の追加

認証局が署名した CAPF 証明書を使用する場合は、ルート証明書をUnified Communications Manager信頼ストアに追加します。

手順

ステップ 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。

ステップ 2 **[証明書/証明書チェーンのアップロード]** をクリックします。

ステップ 3 **[証明書/証明書チェーンのアップロード]** ポップアップ ウィンドウで、**[証明書の用途]** ドロップダウン リストから **[CallManager の信頼性]** を選択し、認証局署名済み CAPF ルート証明書を参照します。

ステップ 4 **[ファイルのアップロード]** フィールドに証明書が表示されたら、**[アップロード]** をクリックします。

サービスの再起動

クラスタ内の特定のノードで機能またはネットワーク サービスを再起動する必要がある場合は、次の手順に従います。

手順

ステップ 1 再起動するサービスのタイプに応じて、次のいずれかのタスクを実行します。

- **[ツール（Tools）] > [コントロール センター - 機能サービス（Control Center - Feature Services）]** の順に選択します。
- **[ツール（Tools）] > [コントロール センター - ネットワーク サービス（Control Center - Network Services）]** を選択します。

ステップ 2 [サーバ（Server）] ドロップダウンリストからシステム ノードを選択し、[移動（Go）] をクリックします。

ステップ 3 再起動するサービスの横にあるオプション ボタンをクリックし、[再起動（Restart）]をクリックします。

ステップ 4 再起動にはしばらく時間がかかることを示すメッセージが表示されたら、[OK] をクリックします。

オンライン証明書ステータスプロトコル（OCSP）による証明書失効（CRL）

Unified Communications Manager は、証明書失効をモニタリングするための OCSP をプロビジョニングします。スケジュールされた間隔、および証明書がアップロードされるたびにシステムが証明書のステータスをチェックし、有効性を確認します。

オンライン証明書状態プロトコル（OCSP）は、管理者がシステムの証明書要件を管理するのに役立ちます。OCSP を設定すると、証明書の有効性を確認したり期限切れの証明書をリアルタイムで無効化するための、シンプルかつ安全な自動メソッドを使用できます。

コモンクライテリア モードが有効になっている FIPS 展開の場合、OCSP はシステムのコモンクライテリア要件への準拠にも役立ちます。

有効性検査

Unified Communications Manager は、証明書のステータスを確認し、有効性を確認します。

証明書の検証は、次のように行われます。

- Unified Communications Manager は代理信頼モデル（DTM）を使用し、OCSP 署名属性のルート CA または中間 CA をチェックします。ルート CA または中間 CA は、ステータスを確認するために OCSP 証明書に署名する必要があります。委任された信頼モデルが失敗すると、Unified Communications Manager が応答側の信頼モデル（TRP）にフォールバックし、指定された OCSP 応答の署名証明書を OCSP サーバから使用して証明書を検証します。

（注） 証明書の失効ステータスを確認するために、OCSP レスポンダが実行されている必要があります。

- **[証明書失効（Certificate Revocation）]** ウィンドウで OCSP オプションを有効にすると、最も安全な方法でリアルタイムに証明書失効をチェックすることができます。オプションから、証明書の OCSP URI を使用するか、または設定済みの OCSP URI を使用するかを選択します。OCSP の手動設定の詳細については、「OCSP による証明書失効の設定」を参照してください。

（注） リーフ証明書の場合、syslog、FileBeat、SIP、ILS、LBM などの TLS クライアントは、OCSP 要求を OCSP レスポンダに送信し、OCSP レスポンダからリアルタイムで証明書失効応答を受信します。

コモンクライテリアモードを有効にした状態で検証が実行されると、証明書に対して次のいずれかのステータスが返されます。

- **[良好（Good）]**：**良好**な状態とは、ステータスの問い合わせへの肯定的な応答を示します。この肯定的な応答は、少なくとも証明書が失効していないことを示しますが、必ずしもその証明書が発行済みであること、または、その応答が生成された時刻が証明書の有効期間内にあることを意味するものではありません。レスポンダが作成したアサーションに加えて、発行や有効性の肯定的なステートメントなど、レスポンダが作成した証明書のステータスに関する追加情報を伝送するためには、応答拡張を使用できます。
- **[失効（Revoked）]**：**失効** 状態とは、証明書が失効している（恒久的または一時的に保留されている）ことを示します。
- **[不明（Unknown）]**：**不明**状態とは、OCSP レスポンダが要求された証明書を認識していないことを示します。

（注） コモンクライテリアモードでは、**失効**と**不明**の両方の場合において接続に失敗しますが、コモンクライテリアモードが有効になっていない状態では応答が**不明**ステータスである場合、接続に成功します。

証明書モニタリング タスク フロー

次のタスクを行い、証明書ステータスと有効期限を自動的にモニタするようシステムを設定します。

- 証明書の有効期限が近づいているときは、電子メールで通知する
- 有効期限が切れた証明書を失効させる

手順

	コマンドまたはアクション	目的
ステップ 1	証明書モニタ通知の設定 （17 ページ）	証明書の自動モニタリングを構成します。システムは定期的に証明書ステータ

	コマンドまたはアクション	目的
		スをチェックし、証明書の有効期限が近づいていると電子メールで通知します。
ステップ 2	OCSP による証明書失効の設定 （18 ページ）	期限切れの証明書が自動的に失効するように OCSP を設定します。

証明書モニタ通知の設定

Unified Communications Manager または IM and Presence サービスの自動証明書モニタリングを設定します。システムは定期的に証明書のステータスをチェックし、証明書の有効期限が近づいていると電子メールで通知します。

（注） [Cisco Certificate Expiry Monitor] ネットワーク サービスを実行している必要があります。デフォルトでこのサービスは有効化されていますが、**[ツール（Tools）] > [コントロール センター - ネットワーク サービス（Control Center - Network Services）]** を選択し、[Cisco Certificate Expiry Monitor サービス（Cisco Certificate Expiry Monitor Service）] の状態が [実行中（Running）] であることを検証して Cisco Unified Serviceability でサービスが実行中であることを確認できます。

手順

ステップ 1 （Unified Communications Manager の証明書モニタリングのために）Cisco Unified OS の管理にログインするか、（IM and Presence サービスの証明書モニタリングのために）Cisco Unified IM and Presence の管理にログインします。

ステップ 2 **[セキュリティ（Security）] > [証明書モニタ（Certificate Management）]** を選択します。

ステップ 3 [通知開始時期（Notification Start Time）] フィールドに、数値を入力します。この値は、近づきつつある有効期限の通知を、有効期限の何日前にシステムが開始するかを表します。

ステップ 4 [通知頻度（Notification Frequency）] フィールドには、通知を行う頻度を入力します。

ステップ 5 これはオプションです。[電子メール通知を有効にする（Enable E-mail notification）] チェックボックスをオンにして、近づきつつある証明書有効期限に関する電子メールアラートをシステムに送信させます。

ステップ 6 [LSC モニタリングを有効にする（Enable LSC Monitoring）] チェック ボックスをオンにして、LSC 証明書を証明書ステータス チェックに含めます。

ステップ 7 [電子メール ID（E-mail IDs）] フィールドに、システムが通知を送信する電子メール アドレスを入力します。複数の電子メールアドレスは、セミコロンで区切って入力できます。

ステップ 8 **[保存（Save）]** をクリックします。

（注） 証明書モニタ サービスは、デフォルトで 24 時間ごとに 1 回だけ実行します。証明書モニタ サービスを再起動すると、サービスが開始され、24 時間後に実行する次のスケジュールが計算されます。証明書の有効期限が 7 日以内に近づいても、この周期は変化しません。このサービスは、証明書の有効期限が切れる 1 日前から、有効期限が切れた後も 1 時間おきに実行します。

次のタスク

Online Certificate Status Protocol（OCSP）を設定し、期限切れの証明書をシステムが自動的に失効させるようにします。詳細については、次を参照してください。OCSP による証明書失効の設定 （18 ページ）

OCSP による証明書失効の設定

オンライン証明書ステータスプロトコル（OCSP）を有効にして、証明書の状態を定期的にチェックし、期限切れの証明書を自動的に失効させます。

始める前に

システムに OCSP チェックに必要な証明書があることを確認します。OCSP 応答属性を設定されているルート CA 証明書または中間 CA 証明書を使用することができます。または、tomcat-trust へアップロードされている指定された OCSP 署名証明書を使用することができます。

手順

ステップ 1 （Unified Communications Manager の証明書失効のために）Cisco Unified OS の管理にログインするか、（IM and Presence サービスの証明書失効のために）Cisco Unified IM and Presence の管理にログインします。

ステップ 2 **[セキュリティ（Security）] > [証明書失効（Certificate Revocation）]** を選択します。

ステップ 3 [OCSP の有効化（Enable OCSP）] チェック ボックスをオンにして、次のタスクのいずれかを実行します。

- OCSP チェックの OCSP レスポンダを指定する場合は、[設定済み OCSP URI を使用する（Use configured OCSP URI）] ボタンを選択し、[OCSP 設定済み URI（OCSP Configured URI）] フィールドにレスポンダの URI を入力します。
- OCSP レスポンダ URI で証明書を設定する場合、[証明書からの OCSP URI を使用する（Use OCSP URI from Certificate）] ボタンを選択します。

ステップ 4 [失効チェックを有効にする（Enable Revocation Check）] チェック ボックスをオンにします。

ステップ 5 [チェック間隔（Check Every）] フィールドに失効チェックの間隔を入力します。

ステップ 6 **[保存（Save）]** をクリックします。

ステップ 7 これはオプションです。CTI、IPsec または LDAP リンクがある場合は、これらの長期性接続の OCSP 失効サポートを有効にするために、上記の手順に加えて次の手順も行う必要があります。

a) Cisco Unified CM の管理から、**[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。

b) [証明書の失効や有効期限（Certificate Revocation and Expiry）] で、[証明書有効性チェック（Certificate Validity Check）] パラメーターを [True] に設定します。

c) [有効性チェック頻度（Validity Check Frequency）] パラメーターの値を設定します。

（注） **証明書失効**ウィンドウの [失効チェックを有効にする（Enable Revocation Check）] パラメーターの間隔値は、[有効チェック頻度（Validity Check Frequency）] エンタープライズ パラメーターの値よりも優先されます。

d) **[保存（Save）]** をクリックします。

証明書エラーのトラブルシュート

始める前に

IM and Presence サービス ノードから Unified Communications Manager サービスに、または、Unified Communications Manager ノードから IM and Presence サービス機能にアクセスしようとしてエラーが発生した場合は、tomcat-trust 証明書に問題があります。「サーバへの接続を確立できません（リモート ノードに接続できません）（Connection to the Server cannot be established (unable to connect to Remote Node)）」というエラー メッセージが、次の [サービスアビリティ（Serviceability ）] インターフェイス ウィンドウに表示されます。

- **サービスのアクティベーション**
- **コントロール センター - 機能サービス**
- **コントロール センター - ネットワーク サービス**

この手順を使用して、証明書のエラーを解決します。最初のステップから開始し、必要に応じて進みます。最初のステップだけでエラーが解決される場合もあれば、すべてのステップを実行することが必要になる場合もあります。

手順

ステップ 1 [Cisco Unified OS の管理（Cisco Unified OS Administration）] の **[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** で、必要な tomcat-trust 証明書が存在することを確認します。

必要な証明書がない場合は、再度確認するまで 30 分間待ちます。

ステップ 2 証明書を選択して情報を表示します。証明書の内容が、リモートノード上の対応する証明書の内容と一致することを確認します。

ステップ 3 CLI から、**utils service restart Cisco Intercluster Sync Agent** を実行して Cisco Intercluster Sync Agent サービスを再起動します。

ステップ 4 Cisco Intercluster Sync Agent サービスが再起動したら、**utils service restart Cisco Tomcat** を実行して Cisco Tomcat サービスを再起動します。

ステップ 5 30 分間待機します。前の手順で証明書のエラーが対処されず、tomcat-trust 証明書が存在する場合は、証明書を削除します。証明書を削除したら、ノードごとに Tomcat および Tomcat-ECDSA 証明書をダウンロードし、tomcat-trust 証明書としてピアにアップロードすることで、証明書を手動で交換する必要があります。

ステップ 6 証明書の交換が完了したら、**utils service restart Cisco Tomcat** を実行して、影響を受ける各サーバで Cisco Tomcat を再起動します。