証明書概要

証明書の概要

証明書とは、証明書保持者名、公開キー、および証明書を発行する認証局のデジタル署名を含むファイルです。証明書は、証明書の所有者の身元を証明します。

ユニファイドコミュニケーションマネージャーは、公開キー基盤 (PKI) を使用する証明書を使用して、サーバとクライアントのアイデンティティを検証し、暗号化を有効化します。別のシステム (たとえば、電話機や media server) がユニファイドコミュニケーションマネージャーに接続しようとすると、そのシステム自身の身元を確認するために、その証明書がユニファイドコミュニケーションマネージャーに提示されます。適切なトラストストアに一致する証明書がある場合を除き、ユニファイドコミュニケーションマネージャーは他のシステムを信頼せず、アクセスが拒否されます。

ユニファイドコミュニケーションマネージャーは、次の 2 つの広範なクラスの証明書を使用します。

- 自己署名付き証明書:デフォルトでは、ユニファイドコミュニケーションマネージャーは自己署名付き証明書を使用します。これらは、サーバまたはクライアントの身元を確認するために、ユニファイドコミュニケーションマネージャーが証明書に署名する証明書です。ユニファイドコミュニケーションマネージャーは、自身の自己署名証明書を発行することも、または認証局のプロキシ機能を使用して、電話機の代理証明書を発行することもできます。
- CA 署名付き証明書: サードパーティ認証局 (CA) によって署名された証明書を使用するようにユニファイドコミュニケーションマネージャーを設定することもできます。認証署名要求 (CSR) は、ユニファイドコミュニケーションに代わって CA が証明書に署名するようにする必要があります。CA は要求を受信し、CA 署名された証明書を発行します。CA 署名付きの証明書を使用するには、最初に、ユニファイドコミュニケーションマネージャーに CA ルート証明書チェーンをインストールする必要があります。

（注） 通常、自己署名付き証明書は、社内のファイアウォールを通過しない内部接続に対して受け入れられます。ただし、WAN 接続の場合、またはパブリックインターネットを使用する接続の場合は、CA 署名付き証明書を使用する必要があります。

（注） X.509 の一般的な時間値。PKI 証明書は、グリニッジ標準時 (GMT) で表記されている**必要**があり、秒 (YYYYMMDDHHMMSSZ) を含める必要があります。秒の端数は許可されていません。このルールに違反する証明書は、ピアエンティティから提供されているか、またはトラストストアに読み込まれているかに関係なく、証明書の検証プロセスを失敗させる可能性があります。

CTL ファイル

Cisco Certificate Trust List は、Cisco CTL クライアントで混合モードを有効にするか、またはユーティリティ ctl CLI コマンドの 1 つを実行することによって作成されるファイルです (たとえば、ユーティリティ ctl update CTLFile)。混在モードが有効になっている場合、CTL ファイルは、TFTP サーバを経由して Cisco IP 電話 にインストールされます。CTL ファイルには、認証局プロキシ機能のシステム証明書やその他の証明書など、信頼できる電話機の証明書のリストが含まれています。

CTL ファイルの設定方法の詳細については、「CTL Client セットアップ」の章を参照してください。

TLS

トランスポート回線シグナリング (TLS) は CA 署名された証明書を使用します。TLS が設定されている場合、もう一方のシステムは、最初の connection セットアップの一部として、その証明書をユニファイドコミュニケーションマネージャーに提示します。他のシステムの証明書がインストールされている場合は、他のシステムを信頼し、通信が行われます。他のシステムの証明書が存在しない場合、もう一方のシステムは信頼されず、通信は失敗します。

サードパーティー CA 署名付き証明書

CA で署名された証明書は、デジタル証明書に署名および発行する信頼できるサードパーティ証明書です。

デフォルトでは、Unified Communications Manager はすべての接続に自己署名証明書を使用します。ただし、証明書に署名するようにサードパーティ CA を設定することによって、セキュリティを追加できます。サードパーティ CA を使用するには、CA ルート証明書チェーンを Cisco Unified Communications Manager Administration にインストールします。

CA で署名された証明書を発行するには、CA が証明書を発行して署名できるように証明書署名要求（CSR）を提出する必要があります。証明書をアップロード、ダウンロード、および表示する方法の詳細については、「**自己署名証明書**」セクションを参照してください。

構成

Unified Communications Manager に接続している別のシステムからの CA で署名された証明書を使用する場合は、 Cisco Unified Communications Manager Administration で次の手順を実行します。

- 証明書を署名した CA のルート証明書をアップロードします。
- 他のシステムから CA 署名付き証明書をアップロードします。

CA で署名された証明書を Unified Communications Manager で使用する場合は、次の手順に従います。

- Cisco Unified Communications Manager Administration で CA で署名された証明書を要求するには、CSR を完了します。
- CA ルート証明書チェーンと CA で署名された証明書の両方を次のページでダウンロードします。 Cisco Unified Communications Manager Administration
- CA ルート証明書チェーンと CA で署名された証明書の両方をアップロードします。

CA のルート証明書の取得と設定の方法の詳細については、証明機関のマニュアルを参照してください。

証明書署名要求のキー用途拡張

次の表には、Unified Communications Manager と IM and Presence Service の CA 証明書の証明書署名要求（CSR）のキーの用途拡張が表示されています。

表 *1 : Cisco Unified Communications Manager CSR* キーの用途拡張

	マルチサーバ	キーの拡張用途			キーの用途				
		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	鍵の暗号化	データの暗号化	キー証明書署名	鍵共有
CallManager CallManager-ECDSA	Y	Y	Y		Y	Y	Y		
CAPF（パブリッシャのみ）	N	Y	Y		Y	Y		Y	
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		
信頼検証サービス（TVS）	Y	Y	Y		Y	Y	Y		

表 *2 : IM and Presence Service CSR* キーの用途拡張

	マルチサーバ	キーの拡張用途			キーの用途				
		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	鍵の暗号化	データの暗号化	キー証明書署名	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		

サーバ証明書のタイプ

サーバ証明書は、基本的にサーバを識別するための証明書です。サーバ証明書は、コンテンツを暗号化および復号化する論拠の役目を果たします。

Unified Communications Manager サーバ内の自己署名証明書（所有）証明書タイプは次のとおりです。

Unified Communications Manager は次の証明書タイプを Unified Communications Manager 信頼ストアにインポートします。

表 *3 :* 証明書タイプと説明

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

証明書タイプ	説明
SIP プロキシサーバ証明書	CallManager 信頼ストアに SIP ユーザエージェント証明書が含まれ、SIP ユーザエージェントの信頼ストアに Unified Communications Manager 証明書が含まれている場合、SIP トランク経由で接続する SIP ユーザエージェントは、Unified Communications Manager に対して認証されます。

（注） 証明書名は、ボイスメールサーバ名に基づく証明書のサブジェクト名のハッシュを表します。すべてのデバイス (またはポート) は、ルート証明書をルートとする証明書を発行します。

次の追加の信頼ストアが存在します。

- tomcat および web アプリケーションの共通信頼ストア
- IPSec-trust
- CAPF-trust
- Userlicensing: 信頼
- TVS-trust
- Phone-SAST-trust
- Phone-CTL-trust

Cisco Unity Connection の CA 信頼証明書の詳細については、Cisco Unified Communications Manager アドミニストレーション ガイドを参照してください。これらの信頼証明書は、電子メール、予定表情報、連絡先を取得するための Exchange または Meeting Place Express へのセキュアな接続を確保します。

証明書の管理タスク

証明書の表示

証明書の一覧を共通名、有効期限、キータイプ、使用法に基づいて並べ替えて表示するには、[証明書の一覧（Certificate List）] ページでフィルタオプションを使用します。フィルタオプションにより、データの並べ替え、表示、管理を効率的に行うことができます。

Unified Communications Manager リリース 14 以降では、アイデンティティ証明書または信頼証明書の一覧を並べ替えて表示するときの基準として、使用法オプションを選択できます。

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。
[Certificate List] ページが表示されます。

Step 2 [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目的のフィルタオプションを選択し、[検索（Find）] フィールドに検索項目を入力して、[検索（Find）] 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要求を送信する場合は、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

Step 1 [Cisco Unified OS Administration] から **[Security]** > **[Certificate Management]** を選択します。

Step 2 検索情報を指定し、[検索（Find）] をクリックします。

Step 3 必要なファイル名を選択し、[ダウンロード（Download）] 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、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している場合にのみ必要です。

手順

Step 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。

Step 2 [証明書/証明書チェーンのアップロード（Upload Certificate/Certificate chain）] をクリックします。

Step 3 ルート証明書をインストールするには、**[証明書の目的（Certificate Purpose）]** ドロップダウンリストから適切な信頼ストアを選択します。

Step 4 選択した証明書の目的の説明を入力します。

Step 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。

Step 6 [アップロード（Upload）] をクリックします。

Step 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

Step 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）]** を選択します。

Step 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。

Step 3 証明書のファイル名を選択します。

Step 4 [削除（Delete）] をクリックします。

Step 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

Step 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。

Step 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。

Step 3 [生成（Generate）] をクリックします。

Step 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。

Step 5 CAPF 証明書、ITLRecovery 証明書、または CallManager 証明書の再生成後に CTL ファイルを更新します（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 *4*: 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 モードが有効な場合に 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 Disaster Recovery System（DRS）ローカルおよびマスターサービス。
CallManager CallManager-ECDSA	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 パブリッシャで実行されている CAPF サービスで使用されます。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（オンラインおよびオフライン CAPF モードを除く）。	該当なし
信頼検証サービス（TVS）	これは信頼検証サービスで使用され、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。	該当なし

（注） [セキュリティパラメータ（Security Parameter）] セクションには、新しいエンタープライズパラメータとして [証明書更新時の電話機の動作（Phone Interaction on Certificate Update）] が導入され、TVS、CAPF、TFTP のいずれかの証明書が更新されたときに、電話機のリセットを手動で行うか自動で行うかを設定できます。デフォルトでは、このパラメータは電話機を自動的にリセットするよう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、パブリッシャノードの 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（Security）] > [証明書の管理（Certificate Management）]** を選択し、**AUTHZ** 証明書を選択して、**[再作成（Regenerate）]** をクリックします。

手順

Step 1 Unified Communications Manager パブリッシャノードで、**コマンドラインインターフェイス**にログインします。

Step 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。

Step 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。

- Authz 証明書を再生成する場合
- IM and Presenc e管理コンソールで集中型展開に新しいエントリを作成する場合

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

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 [CSR の作成（Generate CSR）] をクリックします。

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

Step 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 を生成した後にダウンロードし、認証局に提出する準備をします。

手順

Step 1 [Cisco Unified OS Administration] から **[Security] > [Certificate Management]** を選択します。

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

Step 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。

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

Step 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

認証局署名済み CAPF ルート証明書を使用 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

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 [Upload Certificate/Certificate chain] をクリックします。

Step 3 [証明書/証明書チェーンのアップロード（Upload Certificate/Certificate chain）] ポップアップウィンドウで、[証明書の目的（Certificate Purpose）] ドロップダウンリストから [CallManager-trust] を選択し、認証局署名済み CAPF ルート証明書を参照します。

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

CTL ファイルの更新

この手順を使用して、CLI コマンドを使用して CTL ファイルを更新します。混合モードが有効になっている場合は、新しい証明書をアップロードするたびに CTL ファイルを更新する必要があります。

手順

Step 1 Unified Communications Manager のパブリッシャノードから、**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 ctl update CTLfile` コマンドを実行します。CTL ファイルを再生成すると、ファイルが TFTP サーバにアップロードされて、電話機に自動的に送信されます。

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ブ化（Service Activation）]**
- **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

Step 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。

Step 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。

Step 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。

Step 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。

Step 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。

Step 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。