証明書

証明書の管理

証明書管理機能は、さまざまな証明書タイプ、証明書の管理に関連するタスク、および証明書をモニタおよび失効させる方法の概要を提供します。

証明書概要

証明書は、導入でセキュアな接続を確立するために不可欠です。ネットワーク上で個人、コンピュータ、および他のサービスを認証します。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。

証明書は、証明書所有者のアイデンティティを証明するファイルであり、次の情報が含まれます。

- 証明書所有者の名前
- 公開キー
- 証明書を発行する認証局のデジタル署名

Unified Communications Manager は、暗号化を有効にし、サーバとクライアントのアイデンティティを検証するために、Public Key Infrastructure（PKI）を使用する証明書を使用します。適切な信頼ストアに一致する証明書がある場合を除き、他のシステムは信頼されず、アクセスが拒否されます。

ルート証明書は、デバイスやアプリケーションユーザなど、ユーザとホスト間のセキュアな接続を確保します。証明書は、クライアントとサーバのアイデンティティの安全性を確保し、これらをルート信頼ストアに追加します。

管理者は、サーバ証明書のフィンガープリントを表示し、自己署名証明書を再生成して、Unified Communications Manager インターフェイスから信頼証明書を削除できます。また、CLI を使用して自己署名証明書を再生成して表示することもできます。

Unified Communications Manager 信頼ストアを更新して証明書を管理する方法 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。

（注） Unified Communications Manager は、PEM（.pem）形式および DER（.der）形式の証明書のみサポートします。DER あるいは PEM の証明書のサポートされる最大サイズは 4096 ビットです。

（注） Unified Communications Manager は、ワイルドカードエントリを含む証明書をサポートしていません。例：*.cisco.com

（注） いずれかの Unified Communications Manager 信頼ストアに期限切れの証明書がある場合、これらの証明書は、リリース 12.5(1)SU6 および 14SU2 以降へのアップグレード中にインポートされません。

2 つの証明書をアップロードする場合は、これらの名前と有効期間は同じであるが、シリアル番号と署名アルゴリズムが異なっていることを確認してください。

例：

`27:20:41:0c:5b:08:69:80:42:62:4f:13:bd:16:06:6a` シリアル番号と SHA-1 アルゴリズムを持つルート CA が Unified Communications Manager tomcat-trust に存在します。

`7b:35:33:71:0b:7c:08:b2:47:b3:aa:f9:5c:0d:ca:e4` シリアル番号と SHA-256 アルゴリズムの証明書をアップロードしようとすると、証明書管理は次の処理を実行します。

- 着信証明書の有効性を確認します。
- tomcatTomcat 信頼フォルダ内にある同じ名前の証明書を検索します
- Tomcat 信頼フォルダにある既存の証明書のシリアル番号と、アップロードされている着信証明書のシリアル番号を比較します。

それらのシリアル番号が異なる場合は、両方の証明書の有効期限開始日を確認します。新しい着信証明書の開始タイムスタンプが最新の場合は、既存の証明書は置き換えられ、そうでない場合はアップロードされません。

SHA-1 と SHA-256 のアルゴリズムでは、件名または共通名が同じであれば、同じエンティティに属していることを意味しています。この Unified Communications Manager フレームワークは、Unified Communications Manager サーバ上でこれら両方のアルゴリズムを同時にサポートしませ

ん。特定の信頼フォルダ内では、署名アルゴリズムが何であれ、いずれかのエンティティに属する 1 つの証明書のみがサポートされます。

証明書タイプ

このセクションでは、さまざまな種類の証明書と証明書署名要求、キーの用途拡張の概要を説明します。

電話機の証明書タイプ

電話機証明書は、電話機を認証するための一意の識別子です。これは、IP攻撃に対するセキュリティにとって重要です。

電話機の証明書は次のとおりです。

表 *1:*

電話機の証明書	説明
製造元でインストールされる証明書（MIC）	MIC は Cisco Manufacturing CA によって署名され、署名された証明書はサポートされている Cisco Unified IP Phone に自動的にインストールされます。 MICは、ローカルで有効な証明書（LSC）のインストールまたは暗号化された設定ファイルのダウンロードに対して、シスコ認証局プロキシ機能（CAPF）で認証します。管理者は証明書を変更、削除、または無効にできないため、有効期限が切れた後は使用できません。
ローカルで有効な証明書（LSC）	Cisco Unified IP Phone は、セキュアモードで動作するために LSC を必要とし、認証と暗号化に使用されます。これらは CAPF、オンラインまたはオフライン CA により署名され、MIC よりも優先されます。 CAPF に関連付けられている必要なタスクを実行すると、サポートされている電話機にこの証明書がインストールされます。認証または暗号化を使用するようにデバイスセキュリティモードを設定した後に、LSC により、Unified Communications Manager と電話機間の接続のセキュリティが確保されます。

ヒント MIC は LSC のインストール時にのみ使用することを推奨します。シスコでは、Unified Communications Manager との TLS 接続の認証用に LSC をサポートしています。電話の設定で TLS 認証などの目的で MIC を使用した場合、MIC ルート証明書は容易に侵害されるため、当社は何ら責任を負いません

Unified Communications Manager への TLS 接続に LSC を使用するには、Cisco Unified IP Phone 6900、7900、8900、および 9900 シリーズをアップグレードします。今後の互換性の問題を回

避するために、Unified Communications Manager 信頼ストアから MIC ルート証明書を削除します。

（注） Unified Communications Manager への TLS 接続に MIC を使用する一部の電話機モデルは、登録できない場合があります。

管理者は Unified Communications Manager 信頼ストアから次の MIC ルート証明書を削除する必要があります。

- CAP-RTP-001
- CAP-RTP-002
- Cisco_Manufacturing_CA
- Cisco_Root_CA_2048
- Cisco_Manufacturing_CA_SHA2
- Cisco_Root_CA_M2
- ACT2_SUDI_CA

CAPF 信頼ストアに残された MIC ルート証明書は、証明書のアップグレードに使用されます。Unified Communications Manager 信頼ストアの更新と証明書の管理については、『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。

（注） CAP-RTP-001 および CAP-RTP-002 証明書は、Unified Communications Manager から削除されます。

（注） Unified Communications Manager リリース 12.5.1SU2 以前では、Cisco Manufacturing 証明書を CallManger 信頼ストアから削除すると、電話機の製造元でインストールされた証明書（MIC）を検証できないため、セキュアオンボーディング機能は動作しません。ただし、Unified Communications Manager リリース 12.5.1SU3 以降では、CAPF 信頼ストアを使用して電話機の MIC を検証するため、この機能は動作します。

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 *2*: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。
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。

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。

外部 CA からの証明書のサポート

Unified Communications Manager は、PKCS#10 Certificate Signing Request（CSR; 証明書署名要求）メカニズムを使用して、サードパーティの認証局（CA）との統合をサポートします。このメカニズムには、Unified Communications Manager の GUI でアクセスできます。

現在、サードパーティ CA を使用しているお客様は、CSR メカニズムを使用して次の証明書を発行する必要があります。

- Unified Communications Manager
- CAPF
- IPSec

- Tomcat
- 信頼検証サービス（TVS）

（注） マルチサーバ（SAN）の CA 署名付き証明書は、証明書が発行元にアップロードされた場合にのみクラスタ内のノードに適用されます。新しいマルチサーバ証明書を生成します。新しいノードを追加したり、再作成するたびにクラスタにアップロードします。

システムを混合モードで実行すると、一部のエンドポイントでは、キーサイズが4096以上の CA 証明書を受け入れることができない場合があります。混合モードで CA 証明書を使用するには、次のいずれかのオプションを選択します。

- 証明書のキーサイズが 4096 未満の証明書を使用します。
- 自己署名証明書を使用します。

（注） Cisco の CTL クライアントは、リリース 14 からサポートされなくなりました。Cisco CTL プラグインではなく、CLI コマンドを使用して、Unified Communications Manager サーバーを混合モードに切り替えることをお勧めします。

CTL クライアントを実行した後、該当するサービスを再起動して更新します。

例：

- Unified Communications Manager 証明書を更新する際 に、TFTP サービスと Unified Communications Manager サービスを再起動します。
- CAPF 証明書を更新するときに CAPF を再起動します。

Unified Communications Manager または CAPF 証明書をアップロードした後に、ITL ファイルを更新するために自動的に電話がリセットされる場合があります。

プラットフォームでの証明書署名要求（CSR）の生成方法については、『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。

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 *3 : 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	N	Y		
CAPF（パブリッシャのみ）	N	Y	N		Y	N		Y	
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	N	Y		
信頼検証サービス（TVS）	N	Y	Y		Y	Y	Y		

表 *4 : 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		
cup-xmpp cup-xmpp-ECDSA	Y	Y	Y	Y	Y	Y	Y		
cup-xmpp-s2s cup-xmpp-s2s-ECDSA	Y	Y	Y	Y	Y	Y	Y		
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		

（注） CA 署名証明書のプロセスの一部として、「データ暗号化」ビットが変更または削除されていないことを確認します。

証明書タスク

このセクションでは、証明書を管理するすべての手順を示します。

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。

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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

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。

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。

BCFIPS プロバイダーの証明書表示データは、リリース 14SU2 以降で変更されました。

14SU1 までのタグ名	**14SU2 からのタグ名**
発行者名	発行者 DN
有効期限	開始日
送信先	最終日
サブジェクト名	サブジェクト DN
キー	公開キー（3Public Key）
キー値	モジュラス

（注） x509 拡張機能は、実際のキー使用法名ではなく OID 名で表示されます。

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。

ステップ 1 [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。

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（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している場合にのみ必要です。

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

ステップ 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。

ステップ 4 選択した証明書の目的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 サービスを再起動します。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。
- 電話機のエッジ信頼から証明書をアップロードするには、パブリッシャから行う必要があります。

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。

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。
- 電話エッジトラストからの証明書の削除は、パブリッシャから行う必要があります。
- 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。

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（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。

ステップ 4 [生成（Generate）] をクリックします。

証明書署名要求のフィールド

表 *5:* 証明書署名要求のフィールド

フィールド	説明
Certificate Purpose	ドロップダウンリストから、値を選択します。 • **CallManager** • **CallManager-ECDSA**

Distribution	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>`

Common Name / Common Name_SerialNumber	**重要** リリース 14SU1 以降でサポートされます。 共通名、または共通名に証明書のシリアル番号を付加したものが表示されます。共通名または Common Name_SerialNumber は、証明書のファイル名です。 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。
Include OU in CSR	**重要** リリース 14SU1 以降でサポートされます。 デフォルトでは、組織単位フィールドは証明書署名要求から削除されています。証明書署名要求に組織単位フィールドを含めるには、このオプションを選択します。 （**注**） 証明書署名要求に組織単位があり、署名付き CA 証明書にない場合は、署名付き CA 証明書を Unified Communications Manager にアップロードできます。
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。

フィールド	説明
Key Type	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。
Key Length	**[キー長（Key Length）]**ドロップダウンリストから、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）]**ドロップダウンリストから値を選択して、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）]**ドロップダウンリストから、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。

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。

ステップ 1 [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。

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。

自己署名証明書の生成

ステップ 1 [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。
[証明書の一覧（Certificate List）] ウィンドウが表示されます。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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 （16 ページ）

自己署名証明書のフィールド

表 *6:* 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
Distribution	ドロップダウンリストから Unified Communications Manager サーバを選択します。
Common Name / Common Name_SerialNumber	共通名、または共通名に証明書のシリアル番号を付加したものが表示されます。共通名または Common Name_SerialNumber は、証明書のファイル名です。
CSR に OU を含める	デフォルトでは、組織単位フィールドは証明書署名要求から削除されています。証明書署名要求に組織単位フィールドを含めるには、このオプションを選択します。 （注） 証明書署名要求に組織単位があり、署名付き CA 証明書にない場合は、署名付き CA 証明書を Unified Communications Manager にアップロードできます。

フィールド	説明
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。
Key Type	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。

フィールド	説明
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。
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。

フィールド	説明
Validity Period (in years)	自己署名証明書の有効期間を設定するには、ドロップダウンリストから [5]、[10]、または [20] などのオプションを選択します。 （注） すべての自己署名証明書のデフォルトの有効期間は 5 年です。

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。

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。

（注） 証明書を再生成する場合、**[再生成（Regeneration）]** ウィンドウを閉じて、新しく生成された証明書を開くまで、**[証明書の説明（Certificate Description）]** フィールドは更新されません。

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 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 （20 ページ）」を参照してください。

ステップ 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 にある『*Cisco Unified Communications Manager* セキュリティガイド』を参照してください。

表 7: 証明書の名前と説明

名前	説明	再起動サービス
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。	（注） 以下のサービスの再起動は、リリース 14 以降に適用されます。 Cisco Tomcat サービス、Cisco Disaster Recovery System（DRS）ローカルおよびマスターサービス、Cisco UDS Tomcat および Cisco AXL Tomcat ウェブサービス。 SAML SSO が Tomcat 証明書で有効になっている場合は、IDP で SP メタデータを再プロビジョニングする必要があります。
ipsec	この自己署名ルート証明書は、Unified Communications Manager、MGCP、H.323、および IM and Presence 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。

名前	説明	再起動サービス
CallManager CallManager-ECDSA	SIP、SIP トランク、SCCP、TFTP などに使用されます。	（注） リリース 14 の場合、次のサービスを再起動します。 Cisco Call Manager サービスおよびその他の関連サービス（Cisco CTI Manager、HAProxy サービスなど）：サーバーがセキュアモードの場合に CTL ファイルを更新します。 （注） 以下のサービスの再起動は、リリース 14 SU1 以降に適用されます。 CallManager - HAProxy サービスで、サーバーがセキュアモードの場合は CTL ファイルを更新します。 CallManager-ECDSA - Cisco CallManager サービス、HAProxy サービス、TFTP、CTL。
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。
- 証明書の再生成、削除、および更新後、「再起動サービス」の列に記載されている適切なサービスを再起動してください。

重要 これは、リリース 14SU2 以降に適用されます。

CLI を使用したマルチ SAN 証明書のアップロードはサポートされていません。これらの証明書は、常に OS 管理 GUI を使用してアップロードする必要があります。

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。

ステップ 1 CAPF 証明書を再生成します。

ステップ 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 セキュリティガイド』の「証明書の再生成」セクションを参照してください。

ステップ 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* セキュリティガイド』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。

ステップ 1 TVS 証明書の再生成

ステップ 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 セキュリティガイド』 の「証明書の再生成」セクションを参照してください。

ステップ 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。

ステップ 1 TFTP 証明書を再生成します。

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。

ステップ 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。

ステップ 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。

ステップ 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、『*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。

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、『*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。

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、『セキュリティガイド』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

（注） リリース 14 以降では、SIP OAuth が有効になっている場合、Tomcat の再起動後に SIP OAuth を使用するように設定された電話機を手動でリセットする必要があります。

Tomcat 証明書を再生成するには、次の手順を実行します。

ステップ 1 Tomcat 証明書を再生成します。

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。

ステップ 2 Tomcat サービスの再起動

詳細については、『*Cisco Unified Communications* アドミニストレーション ガイド』を参照してください。

ステップ 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、『*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。

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。

ステップ 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。

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。

- 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

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。

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（Upload Certificate/Certificate chain）] 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（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。

ステップ 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。

ステップ 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。

ステップ 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。

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。
- Unified Communications Manager は、同じ SubjectDN を持つ複数の証明書を同じ信頼ストアにアップロードすることをサポートしていません。サーバーが新しい証明書と既存の証明書を区別するために、ユーザーは新しい CN を別の名前で使用するか、SubjectDN-issue-CA-G2 または SubjectDN-issue-CA-2023 のように文字をサフィックスとして使用することをお勧めします。ハッシュリンクも同じように作成されます。

証明書のモニタリングと失効タスクのフロー

このセクションでは、更新が必要な証明書をモニタし、有効期限が切れた証明書を無効にできます。

証明書モニタリングの概要

管理者は、自動化されたシステムが Unified Communications Manager および IM and Presence Service サービスに含まれている場合、証明書を 追跡および更新できる必要があります。証明書モニタリングは、管理者が証明書のステータスを継続的に知り、証明書の有効期限が近づいたときに電子メールで通知を受信するのに役立ちます。

証明書モニタリングの設定

Cisco Certificate Expiry Monitor ネットワークサービスが実行されている必要があります。このサービスはデフォルトで有効になりますが、Cisco Unified Serviceability でサービスが実行されていることを確かめるには、**[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）]** のステータスが **[実行中（Running）]** であることを確認します。

ステップ 1 Cisco Unified OS Administration で、**[セキュリティ（Security）]** > **[証明書モニタ（Certificate Monitor）]** を選択します。

ステップ 2 設定の詳細を入力または選択します。

ステップ 3 [保存（Save）] をクリックして、設定を保存します。

（注） デフォルトで、証明書モニタサービスは 24 時間ごとに 1 回実行されます。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、この頻度は変わりません。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。

証明書失効の概要

このセクションでは、証明書失効について説明します。Cisco UCM は、証明書失効をモニタするためにオンライン証明書ステータスプロトコル（OCSP）をプロビジョニングします。証明書がアップロードされるたびに、スケジュールされたタイムラインで、システムはそのステータスをチェックして有効性を確認します。

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。

証明書失効の設定

[有効性検証（Validation Checks）] では、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。

証明書の検証手順は次のとおりです。

- 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、OCSP 証明書に署名してステータスを確認する必要があります。
- 代理信頼モデルが失敗した場合は、レスポンダの信頼モデル（TRP）に戻ります。次に、Unified Communications Manager は OCSP サーバからの指定された OCSP 応答署名証明書を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には、OCSP 応答側が実行されている必要があります。

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。

（注） syslog、FileBeat、SIP、ILS、LBM など、TLS クライアントは OCSP からリアルタイムで失効応答を受信します。

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 応答属性で設定されたルート CA 証明書または中間 CA 証明書、または tomcat-trust にアップロードされた、指定 OCSP 署名証明書を使用できます。

重要 このセクションは、リリース 14SU3 以降に適用されます。

証明書失効は、無効で信頼できない証明書を、信頼できる有効な証明書と区別するプロセスです。CA が 1 つ以上のデジタル証明書が信頼できなくなったことを通知し、期限日の前に証明書を本質的に無効にする場合。

証明書失効リスト（CRL）は、実際の期限日または割り当てられた期限日の前に認証局によって失効されたデジタル証明書のリストです。証明書失効リストは、Public Key Infrastructure（PKI）と Web セキュリティに不可欠です。すべての CA には、独自の CRL リストがあります。

この機能は主に CA 発行の CAPF 署名付き電話 LSC 向けに設計されています。CA からダウンロードした最新の CRL ファイルと以前にダウンロードした CRL ファイルに相違がある場合は常に、*CRLChanged* アラームが生成され、syslog のメッセージとともに RTMT に表示されます。*CRLChanged* アラームの詳細については、Cisco Unified Real-Time Monitoring Tool を確認してください。

管理者は、有効な証明書チェーンを更新して置き換えることでアラームに対処し、CallManager で影響を受けるサービスを再起動して、取り消された証明書を使用していた既存の TLS 接続を終了する必要があります。その後、有効な新しい証明書を使用して新しい接続が確立されます。

ステップ 1 Cisco Unified OS Administration で、**[セキュリティ（Security）] > [証明書失効（Certificate Revocation）]** を選択します。

ステップ 2 **[ANATの有効化（Enable OCSP）]** チェックボックスを選択します。

ステップ 3 証明書に OCSP レスポンダ URI が設定されている場合は、[証明書からの OCSP URI を使用する（Use OCSP URI from Certificate）] オプションをクリックします。

または

ステップ 4 OCSP チェックに OCSP レスポンダを指定する場合は、[設定された OCSP URI を使用（Use Configured OCSP URI Option）] をクリックします。

ステップ 5 レスポンダの [OCSP の設定済み URI] を入力します。

ステップ 6 失効チェックを有効にするには、[失効チェックの有効化（Enable Revocation Check）] チェックボックスをオンにします。

ステップ 7 失効ステータスを確認する**頻度**を入力し、[時間（Hours）] または [Days（日）] から**時間間隔**をクリックします。

ステップ 8 **[CRL有効化（Enable CRL）]** チェックボックスをオンにします。

ステップ 9 CRL ファイルのダウンロード元の **CRL 配布ポイント URI** を入力します。

ステップ 10 [保存（Save）] をクリックします。

（注） シスコサービスのリストを再起動して、リアルタイム OCSP を有効にするように求める、アラートがポップアップ表示されます。このポップアップは、**[OCSPの有効化（Enable OCSP）]** チェックボックスをオンにした場合、または以降の変更を保存した場合にのみ表示されます。

OCSP レスポンダは、検証とコモンクライテリアモードがオンの場合に、次のいずれかのステータスを返します。

- [良好（Good）]：OCSP レスポンダがステータスの照会に対して肯定的な応答を送信していることを示します。証明書は失効しませんが、証明書が発行されたという意味でも、応答時間が証明書の有効期間内にあるという意味でもありません。Response 拡張機能は、発行、有効性など、証明書のステータスに関してレスポンダが行ったより多くの要求を伝えます。
- [失効（Revoked）]：証明書が永久的または一時的に失効（保留）ステータスにあることを示します。
- [不明（Unknown）]：OCSP レスポンダが要求された証明書について認識していないことを示しています。

警告 コモンクライテリアモードを有効にした場合、接続は **[失効済み（Revoked）]** および **[不明（Unknown）]** のケースで失敗します。コモンクライテリアモードを無効にすると、接続は **[不明（Unknown）]** のケースで成功します。

ステップ 11 （任意） CTI、IPsec または LDAP リンクがある場合は、これらの長期的に中断しない接続の 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 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。
b) [証明書失効と有効期限（Certificate Revocation and Expiry）] ペインに移動します。

c) [証明書有効性チェック（Certificate Validity Check）] パラメータを [有効（Enabled）] に設定します。
d) [有効性チェック頻度（Validity Check Frequency）] パラメータの値を入力します。

（注） **[証明書失効（Certificate Revocation）]** ページの **[失効チェックの有効化（Enable Revocation Check）]** パラメータの間隔値は、**[有効性チェックの頻度（Validity Check Frequency）]** エンタープライズパラメータの値よりも優先されます。

e) [保存（Save）] をクリックします。

簡素化された証明書管理

更新プログラムのコレクションにより、管理する必要がある証明書の数が大幅に削減されるため、証明書の要件を満たすことが容易になります。Unified Communications Managerには8つのアイデンティティ証明書があります。各ノードのCallManager、CallManager-ECDSA、Tomcat、Tomcat-ECDSA、IPsec、CAPF、TVS、ITL Recoveryです。これらの証明書は、有効期間に基づいて定期的に更新する必要があります。したがって、マルチクラスタ展開シナリオでは、これらの証明書を管理することは困難です。

簡略化された証明書管理の概要

証明書を効率的に管理するには、証明書の数を減らして再利用するオプションがあります。

- **TVS によるマルチサーバ SAN 証明書のサポート**：TVS は、自己署名オプションと CA 署名オプションの両方でマルチサーバ SAN 証明書をサポートするようになり、クラスタに単一の証明書を導入できるようになりました。これらの証明書はクラスタベースです。各クラスタには、ITL ファイルサイズと管理オーバーヘッドを削減する TVS 証明書を 1 つだけ持つオプションがあります。たとえば、21 のノードがある場合、各クラスタに必要な証明書は 1 つだけです。
- **パブリッシャノードから生成された CAPF 証明書**：CAPF 証明書がパブリッシャノードからのみ生成されるようになり、クラスタに単一の証明書を展開できるようになりました。ただし、CAPF 証明書は、エンドポイント登録用のパブリッシャノードとサブスクライバノードの両方で信頼証明書（Callmanager-trust）として使用できます。
- **マルチサーバ SAN 自己署名証明書のサポート**：Tomcat、Tomcat-ECDSA、CallManager、CallManager-ECDSA 証明書は、マルチサーバ SAN 自己署名証明書をサポートするようになりました。以前は、マルチサーバ SAN 証明書は CA 署名付き証明書でのみサポートされていました。マルチサーバ SAN 自己署名証明書を使用することで、サードパーティ認証局から CA を管理するコストを回避できるようになりました。
- **CallManager にマルチサーバ Tomcat 証明書を再利用する**：CallManager 証明書にマルチサーバ Tomcat 証明書を再利用できるようになりました。これは、それぞれに個別の証明書を生成する必要がないためです。CallManager 証明書にマルチサーバ Tomcat 証明書を再

利用する方法の詳細については、「CallManager 用のマルチサーバ Tomcat 証明書の再利用（34 ページ）」を参照してください。

- **自己署名証明書の有効期間**：自己署名証明書のデフォルトの有効期間が短縮されます。有効期間を短縮することで、キーは短い期間で定期的に更新され、古い証明書が削除されます。証明書の有効期間が長いほど、秘密キーが侵害される可能性が高くなります。すべての自己署名証明書のデフォルトの有効期間は 5 年です。

  [有効期間（Validity Period）]フィールドを使用して、自己署名証明書の有効期間を設定するオプションもあります。詳細については、自己署名証明書の生成セクションを参照してください。

表 *8 : Cisco Unified Communications Manager CSR* キーの用途拡張

	Unified CM リリース 14 以前				Unified CMリリース14 以降			
証明書	マルチサーバ SAN 自己署名をサポート	マルチサーバ SAN CA 署名をサポート	10ノードクラスタで管理する証明書の数	ノード/クラスタベース	マルチサーバ SAN 自己署名をサポート	マルチサーバ CA 署名をサポート	10ノードクラスタで管理する証明書の数	ノード/クラスタベース
Tomcat	N	Y	1	自己署名時のノードベース	Y	Y	1	Cluster-based
Tomcat-ECDSA	N	Y	1	自己署名時のノードベース	Y	Y	1	Cluster-based
CallManager	N	Y	1	自己署名時のノードベース	Y	Y	0	Cluster-based
CallManager-ECDSA	N	Y	1	自己署名時のノードベース	Y	Y	0	Cluster-based
信頼検証サービス（TVS）	N	N	10	ノードベース	Y	Y	1	Cluster-based
CAPF	N	N	10	ノードベース	Y	N	1	パブリッシャでのみ
IPsec	N	N	10	ノードベース	N	N	0	ノードベース
ITLRecovery	N	N	1	ノードベース	N	N	1	Cluster-based

簡素化された証明書管理ユーザインターフェイスの更新

次のユーザインターフェイスの更新が導入されました。

- **[証明書の再利用（Reuse Certificate）]**：[証明書管理（Certificate Management）] ウィンドウには、Tomcat マルチサーバ証明書を CallManager アプリケーションと共有できるこの新しいオプションがあります。これにより、ITL ファイルのサイズが削減され、オーバーヘッドが削減されます。
- **[証明書の表示（Show Certificates）]**：Cisco Unified OS の管理インターフェイスの [証明書の管理（Certificate Management）] ウィンドウには、アイデンティティと信頼の証明書のリストを表示できる新しいフィルタリングオプションがあります。

CallManager 用のマルチサーバ Tomcat 証明書の再利用

CallManager アプリケーションで Tomcat マルチサーバ証明書を再利用できるようになりました。CA から 1 つの証明書を取得し、アプリケーション間で再利用できます。これにより、管理オーバーヘッドとコストの最適化が削減されます。

（注） Tomcat 証明書を再利用する前に、マルチサーバ SAN サポート証明書であることを確認してください。

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。
[証明書の一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2 **[証明書の再利用（Reuse Certificate）]** をクリックします。
[他のサービスに Tomcat 証明書を使用する]ページが表示されます。

ステップ 3 **[Tomcat タイプの選択]**ドロップダウンリストから、**[tomcat]** または **[tomcat-ECDSA]** を選択します。

ステップ 4 **[次の証明書を置き換える]** ペインで、**[CallManager]** または **[CallManager-ECDSA]** チェックボックスをオンにします。

ステップ 5 CallManager 証明書を tomcat マルチサーバ SAN 証明書に置き換えるには、**[終了（Finish）]**をクリックします。

（注）
- 証明書タイプとして tomcat を選択すると、CallManager が置換として有効になります。
- 証明書タイプとして tomcat-ECDSA を選択すると、置換として CallManager-ECDSA が有効になります。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。