

CUCM IM/Pサービス自己署名証明書の再生成

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[証明書ストアの使用率](#)

[Cisco Unified Presence\(CUP\)証明書](#)

[Cisco Unified Presence - Extensible Messaging and Presence Protocol\(CUP-XMPP\)証明書](#)

[Cisco Unified Presence - Extensible Messaging and Presence Protocol – サーバ間\(CUP-XMPP-S2S\)証明書](#)

[IPセキュリティ\(IPSec\)証明書](#)

[Tomcat証明書](#)

[証明書の再生成プロセス](#)

[CUP証明書](#)

[CUP-XMPP証明書](#)

[CUP-XMPP-S2S証明書](#)

[IPSec証明書](#)

[Tomcat証明書](#)

[期限切れの信頼証明書の削除](#)

[確認](#)

[トラブルシューティング](#)

はじめに

このドキュメントでは、CUCM IM/P 8.x以降で証明書を再生成する推奨手順を段階的に説明します。

前提条件

要件

IM & Presence(IM/P)サービス証明書に関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、IM/Pリリース8.x以降に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

証明書ストアの使用率

Cisco Unified Presence(CUP)証明書

SIPフェデレーション用のセキュアなSIP接続、Lync/OCS/LCS用のMicrosoftリモートコール制御、Cisco Unified Certificate Manager(CUCM)とIM/P間のセキュアな接続などに使用されます。

Cisco Unified Presence - Extensible Messaging and Presence Protocol(CUP-XMPP)証明書

XMPPセッションの作成時に、XMPPクライアントのセキュア接続を検証するために使用されます。

Cisco Unified Presence - Extensible Messaging and Presence Protocol – サーバ間(CUP-XMPP-S2S)証明書

外部フェデレーテッドXMPPシステムとのXMPPドメイン間フェデレーションのセキュア接続を検証するために使用されます。

IPセキュリティ(IPSec)証明書

使用目的：

- ・ デイザスタリカバリシステム(DRS)/デイザスタリカバリフレームワーク(DRF)のセキュアな接続の検証
- ・ クラスタ内のCisco Unified Communications Manager(CUCM)およびIM/PノードへのIPSecトンネルのセキュア接続を検証する

Tomcat証明書

使用目的：

- ・ クラスタ内の他のノードからのサービスページへのアクセスやJabber Accessなど、さまざまなWebアクセスを検証します。
- ・ SAMLシングルサインオン(SSO)のセキュアな接続を検証します。
- ・ クラスタ間ピアのセキュア接続を検証します。

 **注意：**ユニファイドコミュニケーションサーバでSSO機能を使用し、Cisco Tomcat証明書が再生成された場合、SSOは新しい証明書で再設定する必要があります。CUCMおよびADFS 2.0でSSOを設定するリンクは、
<https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/211302-Configure-Single-Sign-On-using-CUCM-and.html>です。

 **注：**CUCM証明書の再生成/更新プロセスへのリンクは、<https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/200199-CUCM-Certificate-Regeneration-Renewal-Pr.html>です。

証明書の再生成プロセス

CUP証明書

ステップ 1: クラスタ内の各サーバのグラフィカルユーザインターフェイス(GUI)を開きます。IM/Pパブリッシャから開始し、各IM/PサブスクリバサーバのGUIを順に開き、 Cisco Unified OS Administration > Security > Certificate Management.

ステップ 2: パブリッシャGUIから開始し、 Findを選択してすべての証明書を表示します。cup.pemの証明書を選択します。開いたら、 Regenerateを選択し、成功が表示されるまで待つからポップアップを閉じます。

ステップ 3: 後続のサブスクリバで続行し、ステップ2と同じ手順を参照して、クラスタ内のすべてのサブスクリバを完了します。

ステップ4: すべてのノードでCUP証明書が再生成された後、サービスを再起動する必要があります。

 注: プレゼンス冗長グループの設定でEnable High Availabilityにチェックマークが入っている場合は、サービスを再起動する前にUncheckにチェックマークを入れます。プレゼンス冗長グループの設定には、 CUCM Pub Administration > System > Presence Redundancy Groupからアクセスできます。サービスを再起動すると、IM/Pが一時的に停止するため、実稼働時間外に実行する必要があります。

サービスを次の順序で再起動します。

・ パブリッシャのCisco Unified Serviceabilityにログインします。

a. Cisco Unified Serviceability > Tools > Control Center - Feature Services.

b. Restart Cisco SIP Proxyサービス。

c. サービスの再起動が完了したら、サブスクリバとRestartCisco SIP Proxyサービスを続行します。

d.パブリッシャから開始し、サブスクリバから続行します。 Restart Cisco SIP Proxyサービス(Cisco Unified Serviceability > Tools > Control Center - Feature Servicesからも)

・ パブリッシャのCisco Unified Serviceabilityにログインします。

a. Cisco Unified Serviceability > Tools > Control Center - Feature Services.

b. Restart Cisco Presence Engineサービス。

c. サービスの再起動が完了したら、サブスクリバでCisco Presence EngineServiceRestart の実行を続行します。

 注: SIPフェデレーションが設定されている場合は、 RestartCisco Unified Serviceability > Tools > Control Center - Feature Services (URL)のCisco XCP SIP Federation Connection Managerサービス。パブリッシャから開始し、サブスクリバから続行します。

CUP-XMPP証明書

 注: JabberはCUCMおよびIM/P TomcatとCUP-XMPPサーバ証明書を使用してTomcatおよびCUP-XMPPサービスの接続を検証するため、これらのCUCMおよびIM/P証明書はほとんどの場合CA署名付きです。Jabberデバイスの証明書信頼ストアに、ルート証明書とCUP-XMPP証明書の一部である中間証明書がインストールされていないとします。この場合、Jabberクライアントでは、信頼できない証明書に対するセキュリティ警告ポップアップが表示されます。Jabberデバイス信頼ストアの

 証明書にまだインストールされていない場合は、ルート証明書とすべての中間証明書を、グループポリシー、MDM、電子メールなどでJabberデバイスにプッシュする必要があります。プッシュ先のJabberデバイスはJabberクライアントによって異なります。

 注：CUP-XMPP証明書が自己署名の場合、CUP-XMPP証明書がJabberデバイス証明書の信頼ストアにインストールされていないと、Jabberクライアントは信頼できない証明書に対してセキュリティ警告ポップアップを表示します。まだインストールされていない場合は、自己署名CUP-XMPP証明書をグループポリシー、MDM、電子メールなどでJabberデバイスにプッシュする必要があります。これはJabberクライアントによって異なります。

ステップ 1：クラスタ内の各サーバのGUIを開きます。IM/Pパブリッシャから開始し、各IM/PサブスクリバサーバのGUIを順に開いて、**Cisco Unified OS Administration > Security > Certificate Management**に移動します。

ステップ 2：パブリッシャGUIから開始し、Findを選択してすべての証明書を表示します。証 cup-xmpp.pem 明書のタイプ列から、自己署名かCA署名付きかを判断します。証 cup-xmpp.pem 明書がサードパーティ署名付き（タイプCA署名付き）配布マルチSANである場合、マルチSAN CUP-XMPP CSRを生成するときはこのリンクを確認し、CA署名付きCUP-XMPP証明書「[CA署名付きマルチサーバサブジェクト代替名を使用したユニファイドコミュニケーションクラスタのセットアップの設定例](#)」をCAに提出します。

証 cup-xmpp.pem 明書がサードパーティ署名付き（タイプCA署名付き）配布シングルノード（配布名は証明書の共通名と同じ）の場合、シングルノードCUP-XMPP CSRを生成し、CAに送信してCA署名付きCUP-XMPP証明書を入手する際に、このリンクを確認します。[証明書検証のためのJabberの完全な手引き](#)。証cup-xmpp.pem 明書が自己署名の場合は、ステップ3に進みます。

ステップ 3：すべての証明書を表示するためにFindを選択し、cup-xmpp.pem証明書を選択します。開いたら、Regenerateを選択し、成功が表示されるまで待つからポップアップを閉じます。

ステップ 4：後続のサブスクリバに対して処理を続行します。手順2と同じ手順を参照し、クラスタ内のすべてのサブスクリバに対して実行します。

ステップ 5：すべてのノードでCUP-XMPP証明書が再生成されたら、IM/PノードでCisco XCP Routerサービスを再起動する必要があります。

 注：プレゼンス冗長グループの設定でハイアベイラビリティの有効化がオンになっている場合は、サービスを再起動する前にUncheck、オンにします。プレゼンス冗長グループの設定には、CUCM Pub Administration > System > Presence Redundancy Groupからアクセスできます。サービスを再起動すると、IM/Pが一時的に停止するため、実稼働時間外に行う必要があります。

・パブリッシャのCisco Unified Serviceabilityにログインします。

a. Cisco Unified Serviceability > Tools > Control Center - Network Services.

b. Restart Cisco XCPルータサービス。

c. サービスの再起動が完了したら、サブスクリバのCisco XCP Restart Routerサービスを続行します。

CUP-XMPP-S2S証明書

ステップ 1: クラスタ内の各サーバのGUIを開きます。IM/Pパブリッシャから開始し、各IM/Pサブスクリバサーバへの順にGUIを開いて、Cisco Unified OS Administration > Security > Certificate Managementに移動します。

ステップ 2: パブリッシャGUIから開始し、Findを選択してすべての証明書を表示し、cup-xmpp-s2s.pem証明書を選択します。開いたら、Regenerateを選択し、成功が表示されるまで待つてからポップアップを閉じます。

ステップ 3: 後続のサブスクリバについて手順2と同じ手順を参照し、クラスタ内のすべてのサブスクリバに対して完了します。

ステップ 4: すべてのノードでCUP-XMPP-S2S証明書が再生成された後、サービスを上記の順序で再起動する必要があります。



注: プレゼンス冗長グループの設定でハイアベイラビリティを有効にするチェックボックスがオンになっている場合はUncheck、これらのサービスを再起動する前にオンにします。プレゼンス冗長グループの設定には、CUCM Pub Administration > System > Presence Redundancy Groupからアクセスできます。サービスを再起動すると、IM/Pが一時的に停止するため、実稼働時間外に実行する必要があります。

・ パブリッシャのCisco Unified Serviceabilityにログインします。

a. Cisco Unified Serviceability > Tools > Control Center - Network Services.

b. Restart Cisco XCPルータサービス。

c. サービスの再起動が完了したら、サブスクリバのCisco XCP RouterサービスRestart の開始を続行します。

・ パブリッシャのCisco Unified Serviceabilityにログインします。

a. Cisco Unified Serviceability > Tools > Control Center - Feature Services.

b. Restart Cisco XCP XMPP Federation Connection Managerサービス。

c. サービスの再起動が完了したら、サブスクリバRestart でCisco XCP XMPP Federation Connection Managerサービスの開始を続行します。

IPSec証明書



注: CUCMパブリッシャの証 ipsec.pem 明書は、有効であり、IPSec信頼ストア内のすべてのサブスクリバ (CUCMおよびIM/Pノード) に存在する必要があります。サブスクリバの証 ipsec.pem 明書が、標準導入環境のIPSec信頼ストアとしてパブリッシャに存在しない。有効性を確認するために、CUCM-PUBからの証 ipsec.pem 明書のシリアル番号とサブスクリバのIPSec-trustを比較します。これらは一致する必要があります。



注: DRSは、CUCMクラスタノード (CUCMおよびIM/Pノード) 間のデータの認証と暗号化に、送信元エージェントとローカルエージェント間のセキュアソケットレイヤ(SSL)ベースの通信を使用します。DRSは、公開/秘密キーの暗号化にIPSec証明書を使用します。Certificate ManagementページからIPSEC信頼ストア(hostname.pem)ファイルを削除すると、DRSが期待どおりに動作しなくなることに注意してください。IPSEC信頼ファイルを手動で削除する場合は、IPSEC証明書をIPSEC信頼ストアにアップロードする必要があります。詳細については、『CUCM Security Guides』の証明書管理のヘルプページを参照してください。

ステップ 1 : クラスタ内の各サーバのGUIを開きます。IM/Pパブリッシャから開始し、各IM/Pサブスクリバサーバへの順にGUIを開いて、Cisco Unified OS Administration > Security > Certificate Managementに移動します。

ステップ 2 : パブリッシャのGUIから開始し、すべての証明書を表示するように選択しますFind。Chooseipsec.pem証明書です。開いたら、Regenerateを選択し、成功が表示されるまで待つてからポップアップを閉じます。

ステップ 3 : 後続のサブスクリバについて手順2と同じ手順を参照し、クラスタ内のすべてのサブスクリバに対して完了します。

ステップ 4 : すべてのノードがIPSEC証明書を再生成した後、Restartのサービスを実行します。パブリッシャのCisco Unified Serviceabilityに移動します。Cisco Unified Serviceability > Tools > Control Center - Network Services。

a. Cisco DRFプライマリサービスでRestartを選択します。

b. サービスの再起動が完了したら、パブリッシャでCisco DRF LocalサービスのRestartを選択し、各サブスクリバのCisco DRF LocalサービスのRestartを続行します。

Tomcat証明書

 注 : JabberはCUCM TomcatおよびIM/P Tomcatサーバ証明書とCUP-XMPPサーバ証明書を使用してTomcatおよびCUP-XMPPサービスの接続を検証するため、これらのCUCM証明書とIM/P証明書はほとんどの場合CA署名付きです。Jabberデバイスに、証明書信頼ストアにインストールされているTomcat証明書の一部であるルート証明書と中間証明書がないと仮定します。この場合、Jabberクライアントは信頼できない証明書に対してセキュリティ警告ポップアップを表示します。まだJabberデバイスの証明書信頼ストアにインストールされていない場合、ルートとすべての中間証明書は、グループポリシー、MDM、電子メールなどでJabberデバイスにプッシュする必要があります。プッシュ先のJabberデバイスはJabberクライアントによって異なります。

 注 : Tomcat証明書が自己署名の場合、Tomcat証明書がJabberデバイスの証明書信頼ストアにインストールされていないと、Jabberクライアントでは信頼できない証明書に対してセキュリティ警告ポップアップが表示されます。まだJabberデバイスの証明書信頼ストアにインストールされていない場合、自己署名CUP-XMPP証明書は、Jabberクライアントに応じて、グループポリシー、MDM、電子メールなどでJabberデバイスにプッシュする必要があります。

ステップ 1 : クラスタ内の各サーバのGUIを開きます。IM/Pパブリッシャから開始し、各IM/PサブスクリバサーバのGUIを順に開いて、Cisco Unified OS Administration > Security > Certificate Managementに移動します。

ステップ 2 : パブリッシャGUIから開始し、すべての証明書Find を表示するように選択します。

・ tomcat.pemの証明書の[タイプ]列から、自己署名がCA署名付きかを確認します。

・ tomcat.pemの証明書がサードパーティの署名付き (タイプCA署名付き) 配布マルチSANである場合は、マルチSAN Tomcat CSRを生成し、CAに送信してCA署名付きTomcat証明書、[CA署名付きマルチサーバサブジェクト代替名を設定する方法の設定例に関する](#)次のリンクを参照してください

注：マルチSAN Tomcat CSRはCUCMパブリッシャで生成され、クラスタ内のすべてのCUCMおよびIM/Pノードに配布されます。

-
- ・ 証 tomcat.pem 明書がサードパーティ署名付き（タイプCA署名付き）配布シングルノード（配布名は証明書の共通名と同じ）である場合、このリンクを確認してシングルノードCUP-XMPP CSRを生成し、CAに提出してCA署名付きCUP-XMPP証明書、[Jabberの証明書検証の完全な手引き](#)
 - ・ 証 tomcat.pem 明書が自己署名の場合、ステップ3に進みます

ステップ 3：すべての証明書を表示するには、Findを選択します。

- ・ tomcat.pemの証明書を選択します。
- ・ 開いたら、Regenerateを選択し、成功のポップアップが表示されるまで待つからポップアップを閉じます。

ステップ 4 : 後続の各サブスクリバで続行し、手順2の手順を参照して、クラスタ内のすべてのサブスクリバを完了します。

ステップ 5 : すべてのノードでTomcat証明書が再生成された後、すべてのノードのTomcatサービスがRestart再生成されます。パブリッシャから開始し、その後にサブスクリバを追加します。

・ Restart Tomcatサービスを使用するには、各ノードのCLIセッションを開き、図に示すように、サービスがCisco Tomcatを再起動するまでコマンドを実行する必要があります。

```
admin:
admin:utils service restart Cisco Tomcat
Don't press Ctrl-c while the service is getting RESTARTED.If Service has not Restarted Properly, execute the same Command Again
Service Manager is running
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTED]
admin:
```

期限切れの信頼証明書の削除

 注 : 必要に応じて、(-trustで終わる) 信頼証明書を削除できます。削除できる信頼証明書は、不要な証明書、期限切れの証明書、廃止された証明書です。5つのID証明書(cup.pem 、 cup-xmpp.pem 、 cup-xmpp-s2s.pem 、 ipsec.pem 、 および tomcat.pem 証明書)は削除しないでください。次に示すように、サービスの再起動は、これらのサービス内のこれらのレガシー証明書のメモリ内の情報をクリアするように設計されています。

 注 : プレゼンス冗長グループの設定でハイアベイラビリティの有効化にチェックマークが付いている場合はUncheck、サービスがStopped/Started またはRestartedになる前に行ってください。プレゼンス冗長グループの設定には、CUCM Pub Administration > System > Presence Redundancy Groupからアクセスできます。示されているように、一部のサービスを再起動すると、IM/Pが一時的に停止するため、実稼働時間外に実行する必要があります。

ステップ 1 : 次のとおりに移動します。Cisco Unified Serviceability > Tools > Control Center - Network Services

・ ドロップダウンメニューからIM/Pパブリッシャを選択し、Cisco Certificate Expiry MonitorからStop、Cisco Intercluster Sync Agent内のStopを選択します。

・ クラスタ内の各IM/Pノードでこれらのサービスに対してStopを繰り返します。

注：Tomcat-trust証明書を削除する必要がある場合は、CUCMパブリッシャのCisco Unified Serviceability > Tools > Control Center - Network Servicesに移動します。

-
- ・ ドロップダウンから、CUCMパブリッシャを選択します。
 - ・ Cisco Certificate Expiry MonitorでStopを選択し、続いてCisco Certificate Change NotificationでStopを選択します。
 - ・ クラスタ内のすべてのCUCMノードに対して、この手順を繰り返します。

ステップ 2：Cisco Unified OS Administration > Security > Certificate Management > Findに移動します。

- ・ 有効期限が切れた信頼証明書を検索します(バージョン10.x以降では、有効期限でフィルタできます。10.0より前のバージョンからは、特定の証明書を手動で識別するか、受信した場合はRTMTアラートを使用して識別する必要があります)。

- ・ 同じ信頼証明書を複数のノードで使用できます。各ノードから個別に削除する必要があります。
- ・ 削除する信頼証明書を選択します (バージョンに応じて、ポップアップが表示されるか、同じページの証明書に移動します)。
- ・ Delete(「you are about permanently delete this certificate...」で始まるポップアップが表示されます)。
- ・ クリック OK.

ステップ 3 : 削除するすべての信頼証明書について、この手順を繰り返します。

ステップ 4 : 完了したら、削除した証明書に直接関連するサービスを再起動する必要があります。

- ・ CUP-trust: Cisco SIPプロキシ、Cisco Presence Engine。SIPフェデレーションが設定されている場合は、Cisco XCP SIP Federation Connection Manager (CUP証明書のセクションを参照)
- ・ CUP-XMPP-trust: Cisco XCPルータ (「CUP-XMPP証明書」セクションを参照)
- ・ CUP-XMPP-S2S-trust: Cisco XCPルータおよびCisco XCP XMPP Federation Connection Manager
- ・ IPSec-trust: DRF Source/DRF Local (IPSec証明書セクションを参照)
- ・ Tomcat-trust : コマンドラインからTomcatサービスを再起動します (「Tomcat証明書」の項を参照) 。

ステップ 5 : ステップ1でサービスを再起動します。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報はありません。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。