CUCM 証明書の再生成/更新プロセス

目次

はじめに

このドキュメントでは、Cisco Unified Communications Manager(CUCM)リリース8.x以降で使用される証明書を再生成する方法について説明します。望ましくないシステムの停止を回避するため、デフォルトのセキュリティ機能（ITL）および混合モード（CTL）についても説明します。たとえば、電話登録の問題や、設定変更やファームウェアを受け入れない電話機を回避する方法を説明します。

> **注意**：証明書の再生成は、常にメンテナンス ウィンドウで実行することを推奨します。

前提条件

要件

次の項目に関する知識が推奨されます。

- CallManager
- CAPF（Certificate Authority Proxy Function）

- IPSec
- Tomcat
- TVS（信頼検証サービス）
- ITLRecovery（CUCM 10.X 以降のみ）
- phone-vpn-trust
- phone-sast-trust
- phone-trust
- phone-ctl-trust
- LSC（ローカルで有効な証明書）
- MIC（製造元でインストールされた証明書）

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づくものです。

- CUCMリリース9.1(2)SU2a、
- CUCMリリース8.x以降

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。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。

証明書を再生成するタイミング?

新規インストール後に CUCM で使用される証明書の多くは、デフォルトで 5 年間有効な自己署名証明書です。現在、5年間の時間範囲をCUCM上の短い時間範囲に変更することはできません。ただし、認証局（CA）はほぼあらゆる時間範囲で証明書を発行することができます。

また、事前にロードされ、有効期間がより長い、信頼できる証明書もあります（CAPF-trust や CallManager-trust など）。たとえば、Cisco Manufacturing CA証明書はCUCM信頼ストアで特定の機能に提供され、2029年まで期限切れになることはありません。

証明書は、満了する前に再生成する必要があります。証明書の期限が近づくと、RTMT(Syslog Viewer)で警告が表示され、設定されている場合は通知を含む電子メールが送信されます。

CUCM01.der証明書の有効期限が**5月19日14時46分**に**信頼ストア**のサーバCUCM02で**14時46**分に詳細な証明書の有効期限通知の例を次に示示します。

```
At Fri Sep 05 02:00:56 CEST 2014 on node 192.168.1.2, the following
SyslogSeverityMatchFound events generated:

SeverityMatch : Critical

MatchedEvent : Sep 5 02:00:06 CUCM02 local7 2 : 864: CUCM02.localdomain:
Sep 05 2014 00:00:06.433 UTC : %UC_CERT-2-CertValidfor7days:
%[Message=Certificate expiration Notification. Certificate name:CUCM01.der
Unit:tomcat-trust Type:own-cert Expiration:Mon May 19 14:46:]
[AppID=Cisco Certificate Monitor][ClusterID=][NodeID=CUCM02]:
Alarm to indicate that Certificate has Expired or Expires in less than seven days

AppID : Cisco Syslog Agent
```

```
ClusterID :

NodeID : CUCM02

TimeStamp : Fri Sep 05 02:00:16 CEST 2014
```

サービス証明書(-trustのラベルが付いていない証明書ストア)が既に期限切れになっている場合は、それらを再生成することは可能です。クラスタの設定によっては、期限切れの証明書が CUCM 機能に影響する可能性があることを考慮してください。考慮事項については、次のセクションで説明します。

証明書ストアによるサービスへの影響

CUCMクラスタ全体ですべての証明書を更新するには、システムの適切な機能が不可欠です。証明書が期限切れまたは無効になると、システムの正常な機能に大きな影響を与える可能性があります。特定の証明書のいずれかが無効または期限切れになった場合に発生する可能性のある問題のリストを次に示します。影響の違いは、システム設定によって異なる場合があります。

CallManager.pem

- TFTP が信頼されません（電話機は署名付きのコンフィギュレーション ファイルや ITL ファイルを受け付けません）。
- 電話サービスが影響を受ける可能性があります。
- Secure Session Initiation Protocol(SIP)トランクまたはメディアリソース(会議ブリッジ、メディアターミネーションポイント(MTP)、Xcodersなど)は登録または動作しません。
- AXL 要求が失敗します。

Tomcat.pem

- 電話機が社内ディレクトリなどの CUCM ノードでホストされる HTTPS サービスにアクセスできません。
- クラスタ内の他のノードからサービス ページにアクセスできないなど、CUCM の Web GUI 問題が発生します。
- エクステンション モビリティおよびクラスタ間のエクステンション モビリティの問題が発生します。

CAPF.pem

- 電話機が、電話 VPN 802.1x または電話プロキシを認証しません。
- 電話機の LSC 証明書を発行できません。
- 暗号化されたコンフィギュレーション ファイルが機能しません。

IPSec.pem

- ディザスタ リカバリ システム（DRS）/ディザスタ リカバリ フレームワーク（DRF）が正しく動作しない可能性があります。
- 他の CUCM クラスタにつながるゲートウェイ（GW）への IPSec トンネルが動作しません。

信頼検証サービス(TVS)

電話機が HTTPS サービスを認証できません。電話機がコンフィギュレーション ファイルを認証できません（これは CUCM のほぼすべてに影響を与える可能性があります）。

phone-vpn-trust

VPNのHTTPS URLを認証できないため、電話機のVPNは機能しません。

> **注**：これが存在しなくても問題ありません。これは、特定のコンフィギュレーションに限ります。

phone-sast-trust

以前のCTL/eTokenはCTLを更新または変更できません。

> **注**：これが存在しなくても問題ありません。これは、特定のコンフィギュレーションに限ります。

phone-trust および phone-ctl-trust

UnityまたはUnity Connectionのビジュアルボイスメールが機能しない。

> **注**：これが存在しなくても問題ありません。これは、特定のコンフィギュレーションに限ります。

LSCおよび MIC

電話機が登録されず、電話機が電話機VPN、電話プロキシ、または802.1xに認証されない。

> **注**：MIC はほとんどの電話機モデルにデフォルトで付属しています。LSC は CAPF によって署名され、デフォルトで 5 年間有効です。CIPC（Cisco IP Communicator）および Jabber などのソフトウェア クライアントは、MIC がインストールされていません。

DRS バックアップの作成

このような大きな変更を行う前に、DRS のバックアップを作成することを推奨します。CUCM DRF バックアップは、クラスタ内のすべての証明書をバックアップします。すべてのDRSバックアップ/復元の手順については、『Cisco *Disaster Recovery System Administration Guide for Cisco Unified Communications Manager*』を参照してください。

> **注意**:Cisco Bug ID CSCtn50405**に注意してください。**CUCM DRFバックアップでは証明書がバックアップされません。

混合モードの判別

クラスタが CTL/Secure/混合モードのどのモードで実行されているかを調べるには、[Cisco Unified CM Administration] > [System] > [Enterprise Parameters] > [Cluster Security Mode] を選択します（0 == Non-Secure、1 == 混合モード）。

クラスタが混合モードの場合

CUCM クラスタを混合モードで実行している場合、すべての証明書を変更した後で、CTL ファイルを更新する変更があることを意味します。この方法の手順は、『シスコ セキュリティ ガイド』に記載しています。ただし、混合モード機能の最初の開始から少なくとも1つのeTokenがあり、

eTokenパスワードが既知であることを確認してください。

注：CTLの更新は自動的には行われません（ITLファイルの場合と同様）。 これは、CTL クライアントまたは CLI コマンドを使用して、管理者が手動で実行する必要があります。

CUCM 10.X 以降では、次の 2 つの方法でクラスタを混合モードにすることができます。

- CLI コマンド：この方法を使用すると、CTL ファイルがパブリッシャ サーバの CallManager.pem 証明書によって署名されます。

```
admin:show ctl
The checksum value of the CTL file:
0c05655de63fe2a042cf252d96c6d609(MD5)
8c92d1a569f7263cf4485812366e66e3b503a2f5(SHA1)

Length of CTL file: 4947
The CTL File was last modified on Fri Mar 06 19:45:13 CET 2015

[...]

CTL Record #:1
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1156
2 DNSNAME 16 cucm-1051-a-pub
3 SUBJECTNAME 62 CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
ST=Malopolska;C=PL
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 62 CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
ST=Malopolska;C=PL
6 SERIALNUMBER 16 70:CA:F6:4E:09:07:51:B9:DF:22:F4:9F:75:4F:C5:BB
7 PUBLICKEY 140
8 SIGNATURE 128
9 CERTIFICATE 694 E9 D4 33 64 5B C8 8C ED 51 4D 8F E5 EA 5B 6D 21
A5 A3 8C 9C (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

- CTL クライアント：この方法を使用すると、CTL ファイルがハードウェア eToken のいずれかによって署名されます。

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
```

```
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

注:CUCM Mixed ModeとTokenless CTLを使用して使用する方法の間を移動できます。

クラスタのセキュリティを保護する方法に応じて、適切な CTL 更新手順を実行する必要があります。CTL クライアントを再実行するか、または CLI から **utils ctl update CTLfile コマンドを入力します。**

クラスタのデフォルト セキュリティを確認する

ITLの問題を回避することは、多くの機能が失敗したり、電話機が設定の変更に従うことを拒否したりする可能性があるため重要です。ITLの問題は、次の2つの方法で回避できます。

クラスタの準備を使用した8.0より前へのロールバック機能

この機能により、すべてのサーバのITLが空白になるため、電話機はどのTFTPサーバも信頼されます。このパラメータが[True]に設定されている場合、電話サービス（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、基本的な通話の発信と受信は継続できます。

注：このパラメータを変更すると、すべての電話機がリセットされます。

この機能を設定したら、すべてのTFTPサーバを再起動する必要があります（新しいITLを提供するため）。すべての電話機をリセットして、新しい**空の**ITLを要求する必要があります。証明書の変更が完了し、必要なすべてのサービスが再起動したら、この機能を[**False**]に戻し、TFTPサービスを再起動し、電話機をリセットできます（これにより、電話機は有効なITLファイルを取得できます）。 その後、すべての機能は以前と同じように動作し続けます。

特定の順序で証明書を再生成する

この手順は、使用可能な信頼できる TFTP サーバから得た有効な/更新された ITL ファイルを、TFTP サーバに提供します。

1. プライマリ TFTP サーバの TFTP サービスを停止します。
2. 必要に応じて、プライマリTFTPサーバの証明書を変更します。
3. 電話機をリセットします（新しい ITL ファイルをセカンダリ TFTP サーバから取得するため）。再生成した証明書に応じて、この手順は自動的に行われます。
4. 電話機が復帰したら、プライマリ TFTP サーバの TFTP サービスを開始します。
5. セカンダリ TFTP サーバの証明書を変更します。
6. 電話機をリセットします（新しい ITL ファイルをプライマリ TFTP サーバから取得するため）。

注意：両方の TFTP サーバの証明書を同時に編集しないでください。これを行うと、電話機

で信頼できる TFTP サーバがなくなり、ローカル管理者は手動ですべての電話機から ITL を削除する必要があります。

CUCM での証明書の削除と再生成

サービス証明書（「-trust」とラベリングされない証明書ストア）のみを再生成できます。信頼ストア（「-trust」とラベリングされる証明書ストア）の証明書は再生成できないため、削除する必要があります。

> **注意**：Cisco Bug ID CSCut58407（CAPF/CallManager/TVS-trust を削除した場合、デバイスが再起動してはならない）を確認してください。

すべての証明書を変更したら、変更を反映するため、それぞれのサービスを再起動する必要があります。これについては「証明書の再生成と削除の後」セクションで説明します。

> **注意**： Cisco Bug ID CSCto86463（削除した証明書が再び表示され、CUCM から証明書を削除できない）を確認してください。これは、削除された証明書が削除後も引き続き表示され続けるという問題です。問題の回避策を実行します。

CLI での証明書の再生成

> **注意**：証明書の再生成により、クラスタ内のITLファイルの自動更新がトリガーされます。これにより、クラスタ全体のソフトフォンのリセットがトリガーされ、電話機がローカルITLの更新をトリガーできるようになります。これはCAPFおよびCallManager証明書の再生成に重点を置いていますが、TomcatなどのCUCM内の他の証明書ストアで発生する可能性があります。

CAPFの再生成：CAPF 証明書が再生成されると、自動的に CAPF-trust と CallManager-trust にアップロードされます。また、CAPF には常に固有のサブジェクト名ヘッダーがありますので、以前に使用した CAPF 証明書がそのまま認証に使用されます。

```
set cert regen CAPF
```

> **注**:CAPF証明書が期限切れになると、CUCMは証明書を拒否するため、LSCを使用する電話機はCUCMに登録できません。ただし、新しい CAPF 証明書のある電話機に新しい LSC を生成することはできます。電話機を再起動すると、電話機は設定をダウンロードし、LSC を更新するため CAPF に接続します。LSC が更新されると、電話機は登録されます。これは、新しい CAPF 証明書が ITL ファイルにあり、電話機が自分の署名した証明書（callmanager.pem）をダウンロードして信頼している場合に限り、機能します。

CallManagerの再生成：CallManager が再生成されると、自動的に CallManager-trust にアップロードされます。

```
set cert regen CallManager
```
IPsecの再生成：IPsec 証明書が再生成されると、自動的に ipsec-trust にアップロードされます。

```
set cert regen ipsec
```
Tomcatの再生成：Tomcat 証明書が再生成されると、自動的に tomcat-trust にアップロードされます。

```
set cert regen tomcat
```
TVSの再生成：

```
set cert regen TVS
```
何を期待するか

CLI で証明書を再生成すると、この変更の確認が求められます。**yes**と入力し、**Enter**をクリックします。

```
admin:set cert regen CAPF

WARNING: This operation will overwrite any CA signed certificate previously imported
for CAPF

Proceed with regeneration (yes|no)? yes

Successfully Regenerated Certificate for CAPF.

You must restart services related to CAPF for the regenerated certificates to become active.
```
CLI での証明書の削除

CAPF-trust 証明書の削除

```
set cert delete CAPF <name of certificate>.pem
```
CallManager-trust 証明書の削除

```
set cert delete CallManager <name of certificate>.pem
```
ipsec-trust 証明書の削除

```
set cert delete ipsec <name of certificate>.pem
```
Tomcat-trust 証明書の削除

```
set cert delete tomcat <name of certificate>.pem
```
TVS-trust 証明書の削除

```
set cert delete TVS <name of certificate>.pem
```
Web GUI での証明書の再生成

CAPFの再生成：

CAPF 証明書が再生成されると、自動的に CAPF-trust と CallManager-trust にアップロードされます。また、CAPF 証明書には常に固有のサブジェクト名ヘッダーがありますので、以前に使用した CAPF 証明書がそのまま認証に使用されます。

```
OS Admin > Security > Certificate Management > Find > Click CAPF certificate > Regenerate
```

CallManagerの再生成：

再生成が行われると、CallManager証明書は自動的にCallManager-trustにアップロードされます。

```
OS Admin > Security > Certificate Management > Find > Click CallManager certificate > Regenerate
```

IPsecの再生成：

IPsec 証明書が再生成されると、自動的に ipsec-trust にアップロードされます。

```
OS Admin > Security > Certificate Management > Find > Click ipsec certificate > Regenerate
```

Tomcatの再生成：

Tomcat 証明書が再生成されると、自動的に tomcat-trust にアップロードされます。

```
OS Admin > Security > Certificate Management > Find > Click tomcat certificate > Regenerate
```

TVSの再生成：

```
OS Admin > Security > Certificate Management > Find > Click TVS certificate > Regenerate
```

Web GUI での証明書の削除

```
OS Admin > Security > Certificate Management > Find > Click X certificate within the
'-trust' store > Remove/Delete
```

証明書の再生成と削除の後

証明書ストアから証明書を削除または再生成したら、変更を反映するため、それぞれのサービスを再起動する必要があります。

ストア	サービスの再起動	「Catalyst
Tomcat	Tomcat	CLI：utils service restart Cisco Tomcat Web Gui:[**Cisco Unified Serviceability] > [Tools] > [Control Center - Feature Services] > （サーバの選択）に移動**します。 **Cisco CallManager**の下で**Restart**をクリックします。
CallManager	CallManager;TFTP;CTIManager	Web Gui:[**Cisco Unified Serviceability] > [Tools] > [Control Center - Feature Services] > （サーバの選択）に移動**します。 **Cisco Tftp**の下で**Restart**をクリックしま

		す。 Web Gui:[Cisco Unified Serviceability] > [Tools] > [Control Center - Feature Services] > （サーバの選択）に移動します。 Cisco CTIManagerの下でRestartをクリックします。
CAPF	CAPF（パブリッシャでのみ）	Web Gui:[Cisco Unified Serviceability] > [Tools] > [Control Center - Feature Services] > （サーバの選択）に移動します。[Cisco Certificate Authority Proxy Function]で[Restart]をクリックします。
TVS	信頼検証サービス（各サーバ）	Web Gui:[Cisco Unified Serviceability] > [Tools] > [Control Center - Network Services] > （サーバの選択）に移動します。 Cisco Trust Verification Serviceの下でRestartをクリックします。
IPSec	Cisco DRF Local（すべてのノードで）、Cisco DRF Master（パブリッシャで）	CLI：utils service restart Cisco DRF Local CLI：utils service restart Cisco DRF Master

電話機の LSC のインストールと更新

CAPF 証明書が再生成されたら、クラスタ内のすべての電話機の LSC 証明書を、新しい CAPF 証明書によって署名された LSC で更新する必要があります。

1. [CUCM Serviceability] > [Service Activation] に移動します。パブリッシャ サーバで Cisco CTL Provider および Cisco Certificate Authority Proxy Function をアクティブにします。

2. [CUCM CCMAdmin]で、[Device] > [Phone]に移動します。LSC をプロビジョニングする IP Phone を選択します。

3. [Certificate Operation]の下の[Device configuration]ページで、[Install / Upgrade] > [By Null String]に移動します。

4. CCMAdmin の電話機設定を保存し、[Apply Config] を選択します。

LSC のインストールに問題がある場合、電話機で次の操作を実行してください。

電話機がリセットされたら、物理的な電話機の下でSettings > (6) Security Configuration > (4) LSC > **#（この操作によりGUIがロック解除され、次のステップに進むことができます）> Update（前のステップを実行するまで更新はされません）。 次に、[Submit]をクリックします。

無線電話（7921/25）でない限り、電話機に証明書を割り当てないでください。 無線電話は自身を認証するためにサード パーティ認証局（CA）を使用します。

結論

この手順で問題が発生したか、またはサポートが必要な場合、Cisco Technical Assistance Center（TAC）にお問い合わせください。この場合、DRF バックアップを準備しておいてください。TAC が他の方法でサービスを復元できない場合、サービスを復元するための最後の手段として使用します。