CHAPTER 6

Certificate Authority Proxy Function の使用方法

この章は、次の内容で構成されています。

Certificate Authority Proxy Function の概要

Certificate Authority Proxy Function（CAPF）は Cisco Unified Communications Manager と共に自動的にインストールされ、設定に応じて次のタスクを実行します。

- 既存の Manufacturing Installed Certificate（MIC; 製造元でインストールされる証明書）、Locally Significant Certificate（LSC; ローカルで有効な証明書）、ランダム生成された認証文字列、または安全性の低いオプションの「null」認証によって認証する。
- ローカルで有効な証明書を、サポートされている Cisco Unified IP Phone に対して発行する。
- 電話機にある既存のローカルで有効な証明書をアップグレードする。
- 電話機の証明書を表示およびトラブルシューティングするために取得する。

Cisco Certificate Authority Proxy Function サービスをアクティブにすると、CAPF に固有な鍵ペアおよび証明書が CAPF によって自動生成されます。CAPF 証明書は Cisco CTL クライアントによってクラスタ内のすべての Cisco Unified Communications Manager サーバにコピーされ、拡張子 .0 を使用します。CAPF 証明書が存在することを確認するには、Cisco Unified Communications オペレーティング システムの GUI で、CAPF 証明書を表示します。

Cisco Unified IP Phone と CAPF の相互作用

CAPF と相互に作用するとき、電話機は認証文字列、既存の MIC または LAC 証明書、または「null」を使用して CAPF に対して自分を認証し、公開鍵と秘密鍵のペアを生成し、署名付きメッセージで公開鍵を CAPF サーバに転送します。秘密鍵はそのまま電話機に残り、外部に公開されることはありません。CAPF は、電話機証明書に署名し、その証明書を署名付きメッセージで電話機に返送します。

次の情報は、通信または電源の障害が発生した場合に適用されます。

- 電話機で証明書をインストールしているときに通信障害が発生すると、電話機は 30 秒間隔であと 3 回、証明書を取得しようとします。これらの値は設定することができません。
- 電話機で CAPF とのセッションを試行しているときに電源障害が発生すると、電話機はフラッシュに保存されている認証モードを使用します。これは、電話機がリブート後に TFTP サーバから新しい設定ファイルをロードできない場合に当たります。証明書の操作が完了すると、フラッシュ内の値はシステムによってクリアされます。

ヒント　電話機ユーザが電話機で証明書操作を中断したり、操作ステータスを確認できることに注意してください。

ヒント　鍵生成を低いプライオリティで設定すると、アクションの実行中も電話機の機能を利用できます。鍵生成の完了には 30 分以上かかります。

証明書生成中も電話機は機能しますが、TLS トラフィックが増えることにより、最小限の範囲ですがコール処理が中断される場合があります。たとえば、インストールの終了時に証明書がフラッシュに書き込まれる際に音声が乱れることがあります。

証明書用に 2048 ビットの鍵を選択すると、電話機の起動およびフェールオーバー中に電話機、Cisco Unified Communications Manager、および保護された SRST 対応ゲートウェイとの間で接続を確立するのに 60 秒以上かかる場合があります。最高のセキュリティ レベルを必要としている場合を除き、2048 ビットの鍵は設定しないでください。

次に、ユーザまたは Cisco Unified Communications Manager によって電話機がリセットされたときに CAPF が Cisco Unified IP Phone 7960 および 7940 とどのように相互に作用するかについて説明します。

（注）　次の例では、LSC が電話機内にまだ存在しない場合や、CAPF 情報 の［認証モード（Authentication Mode）］に［既存の証明書］が選択されている場合に、CAPF 証明書操作が失敗します。

例：非セキュア デバイス セキュリティ モード

この例では、［デバイスセキュリティモード（Device Security Mode）］を［非セキュア］に、CAPF 情報 の［認証モード（Authentication Mode）］を［Null ストリング］または［既存の証明書（... の優先）］に設定した後に電話機がリセットされます。電話機は、リセット後すぐにプライマリ Cisco Unified Communications Manager に登録し、設定ファイルを受け取ります。次に、電話機は自動的に CAPF とのセッションを開始し、LSC をダウンロードします。LSC のインストール後、電話機は［デバイスセキュリティモード（Device Security Mode）］を［認証のみ］または［暗号化］に設定します。

例：認証のみまたは暗号化デバイス セキュリティ モード

この例では、［デバイスセキュリティモード（Device Security Mode）］を［認証のみ］または［暗号化］に、CAPF 情報 の［認証モード（Authentication Mode）］を［Null ストリング］または［既存の証明書（... の優先）］に設定した後に電話機がリセットされます。CAPF セッションが終了して電話機が LSC をインストールするまで、電話機はプライマリ Cisco Unified Communications Manager に登録しません。セッションが終了すると、電話機は登録を行い、すぐに認証済みまたは暗号化済みモードで動作します。

この例では、電話機は CAPF サーバに自動的に接続しないので、［認証ストリング］を設定することはできません。電話機に有効な LSC がない場合、登録は失敗します。

CAPF システムの相互作用および要件

CAPF には、次の要件があります。

- CAPF を使用する前に、Cisco CTL クライアントのインストールおよび設定に必要なすべての作業を実行したことを確認します。CAPF を使用するには、最初のノードで Cisco Certificate Authority Proxy Function サービスをアクティブにする必要があります。
- 証明書のアップグレードまたはインストール操作で、電話機に対して CAPF 認証方式を［認証ストリング］にした場合、操作後に同じ認証文字列を電話機に入力する必要があります。入力しなかった場合、操作が失敗します。TFTP Encrypted Configuration エンタープライズ パラメータが有効で、認証文字列を入力しなかった場合、電話機に障害が発生し、電話機に入力された認証文字列が一致するまで復帰しないことがあります。
- スケジューリングされたメンテナンス画面で CAPF を使用することを強く推奨します。これは、同時に多数の証明書が生成されると、コール処理が中断される場合があるためです。
- Cisco Unified Communications Manager クラスタ内のすべてのサーバで、同じ管理者ユーザ名とパスワードを使用する必要があります。これで、CAPF はクラスタ内のすべてのサーバに認証を受けることができます。
- 証明書操作の間、最初のノードが実行中で正しく機能していることを確認します。
- 証明書操作の間、電話機が正しく機能していることを確認します。

ヒント　Cisco IP Telephony Backup and Restore System（BARS）を使用して、CAPF データおよびレポートをバックアップすることができます。これは Cisco Unified Communications Manager によって情報が Cisco Unified Communications Manager データベースに格納されるためです。

Cisco Unified Serviceability での CAPF の設定

次の作業を Cisco Unified Serviceability で実行します。

- Cisco Certificate Authority Proxy Function サービスをアクティブにする。
- CAPF 用のトレース設定を行う。

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

CAPF の設定用チェックリスト

表 6-1 に、ローカルで有効な証明書をインストール、アップグレード、またはトラブルシューティングする場合に実行する作業のリストを示します。

表 6-1　CAPF の設定用チェックリスト

設定手順		関連手順および関連項目
ステップ 1	ローカルで有効な証明書が電話機に存在するかどうかを判別します。 CAPF データを Cisco Unified Communications Manager パブリッシャ データベース サーバにコピーする必要があるかどうかを判別します。 **ヒント**　Cisco Unified Communications Manager 4.0 で CAPF ユーティリティを使用していて、CAPF データが Cisco Unified Communications Manager データベースに存在することを確認した場合は、Cisco Unified Communications Manager 4.0 で使用していた CAPF ユーティリティを削除できます。	• 使用している電話機モデルとこのバージョンの Cisco Unified Communications Manager をサポートする電話機のマニュアル • このバージョンの Cisco Unified Communications Manager をサポートする『*Data Migration Assistant ユーザ ガイド*』
ステップ 2	Cisco Certificate Authority Proxy Function サービスが実行されていることを確認します。 **ヒント**　このサービスは、すべての CAPF 操作時に実行されている必要があります。またこのサービスは、CTL ファイルに CAPF 証明書を組み込むために、Cisco CTL クライアントでも実行されている必要があります。	Certificate Authority Proxy Function サービスのアクティブ化（P.6-6）
ステップ 3	Cisco CTL クライアントのインストールおよび設定に必要なすべての作業を実行したことを確認します。CAPF 証明書が Cisco CTL ファイル内に存在することを確認します。	Cisco CTL クライアントの設定（P.3-11）
ステップ 4	必要に応じて、CAPF サービス パラメータを更新します。	• CAPF サービス パラメータの更新（P.6-7） • CAPF による電話機の証明書のインストール、アップグレード、トラブルシューティング、または削除（P.6-8）
ステップ 5	電話機のローカルで有効な証明書をインストール、アップグレード、またはトラブルシューティングするには、Cisco Unified Communications Manager の管理ページを使用します。	• CAPF による電話機の証明書のインストール、アップグレード、トラブルシューティング、または削除（P.6-8） • 電話の設定（Phone Configuration）ウィンドウの CAPF 設定（P.6-9） • LSC ステータスまたは認証文字列に基づく電話機の検索（P.6-10）
ステップ 6	証明書の操作が必要な場合は、認証文字列を電話機に入力します。	電話機での認証文字列の入力（P.6-12）

Certificate Authority Proxy Function サービスのアクティブ化

Cisco Unified Communications Manager では、Cisco Unified Serviceability で Certificate Authority Proxy Function サービスが自動的にアクティブになりません。

このサービスは、最初のノードでのみアクティブにします。Cisco CTL クライアントをインストールして設定する前にこのサービスをアクティブにしなかった場合は、P.3-15 の「CTL ファイルの更新」の説明に従って CTL ファイルを更新する必要があります。

サービスをアクティブにするには、次の手順を実行します。

手順

ステップ 1　Cisco Unified Serviceability で、［**Tools**］>［**Service Activation**］の順に選択します。

ステップ 2　［Server］ドロップダウン リスト ボックスから、Certificate Authority Proxy Function サービスをアクティブにするサーバを選択します。

ステップ 3　［Certificate Authority Proxy Function］チェックボックスをオンにします。

ステップ 4　［保存］をクリックします。

追加情報

詳細については、P.6-13 の「関連項目」を参照してください。

CAPF サービス パラメータの更新

CAPF サービスのパラメータを設定するウィンドウには、証明書の有効年数、システムによる鍵生成の最大再試行回数、鍵のサイズなどの情報が表示されます。

CAPF サービス パラメータが、Cisco Unified Communications Manager の管理ページで Active ステータスとして表示されるようにするには、P.6-6 の「Certificate Authority Proxy Function サービスのアクティブ化」の説明に従って Certificate Authority Proxy Function サービスをアクティブにする必要があります。

CAPF サービス パラメータを更新するには、次の手順を実行します。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで、［**システム**］>［**サービスパラメータ**］の順に選択します。

ステップ 2　［サーバ（Server）］ドロップダウン リスト ボックスから、サーバを選択します。

ヒント　クラスタの最初のノードを選択する必要があります。

ステップ 3　［サービス（Service）］ドロップダウン リスト ボックスから、Cisco Certificate Authority Proxy Function サービスを選択します。

ステップ 4　パラメータごとに表示されるヘルプの説明に従い、CAPF サービス パラメータを更新します。

（注）　CAPF サービス パラメータのヘルプを表示するには、疑問符またはパラメータ名リンクをクリックします。

ステップ 5　変更内容を有効にするには、Cisco Certificate Authority Proxy Function サービスを再起動する必要があります。

追加情報

詳細については、P.6-13 の「関連項目」を参照してください。

CAPF による電話機の証明書のインストール、アップグレード、トラブルシューティング、または削除

CAPF を使用するときに、表 6-2 を参照してください。

Certificate Authority Proxy Function を使用するには、次の手順を実行します。

手順

ステップ 1　『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の説明に従って、電話機を検索します。

ステップ 2　検索結果が表示された後、証明書をインストール、アップグレード、削除、またはトラブルシューティングする電話機を見つけて、その電話機の［**デバイス名（Device Name、回線）**］リンクをクリックします。

ステップ 3　表 6-2 の説明に従って、設定内容を入力します。

ステップ 4　［**保存**］をクリックします。

ステップ 5　［**リセット**］をクリックします。

追加情報

詳細については、P.6-13 の「関連項目」を参照してください。

電話の設定（Phone Configuration）ウィンドウの CAPF 設定

表 6-2 は、Cisco Unified Communications Manager の管理ページの［電話の設定（Phone Configuration）］ウィンドウにある CAPF 設定について説明しています。

- 設定のヒントについては、P.6-4 の「CAPF システムの相互作用および要件」を参照してください。
- 関連する情報および手順については、P.6-13 の「関連項目」を参照してください。

表 6-2　CAPF 設定

設定	説明
［証明書の操作（Certificate Operation）］	ドロップダウン リスト ボックスから、次のオプションのいずれかを選択します。 • **［保留中の操作なし］**：証明書の操作が発生しないときに表示されます（デフォルトの設定）。 • **［インストール / アップグレード］**：電話機にローカルで有効な証明書を新しくインストールするか、あるいは既存の証明書をアップグレードします。 • **［削除］**：電話機に存在するローカルで有効な証明書を削除します。 • **［トラブルシューティング］**：ローカルで有効な証明書（LSC）または製造元でインストールされる証明書（MIC）を取得します。取得することで、CAPF トレース ファイルで証明書のクレデンシャルを確認できます。電話機に両方の種類の証明書が存在する場合、Cisco Unified Communications Manager は証明書の種類ごとに 1 つずつ、2 つのトレース ファイルを作成します。 **ヒント**　［トラブルシューティング］オプションを選択すると、LSC または MIC が電話機に存在することを確認できます。電話機に証明書が存在しない場合、［削除］オプションと［トラブルシューティング］オプションは表示されません。
［認証文字列（Authentication String）］	［認証ストリング］オプションを選択した場合に、このフィールドは適用されます。文字列を手動で入力するか、あるいは［文字列を生成］ボタンをクリックして文字列を生成します。文字列は 4 ～ 10 桁にしてください。 ローカルで有効な証明書をインストール、アップグレード、またはトラブルシューティングするには、電話機ユーザまたは管理者が電話機に認証文字列を入力する必要があります。詳細については、P.6-12 の「電話機での認証文字列の入力」を参照してください。
［文字列を生成］	CAPF で自動的に認証文字列を生成する場合は、このボタンをクリックします。4 ～ 10 桁の認証文字列が［認証文字列（Authentication String）］フィールドに表示されます。
［操作の完了（Operation Completes By）］	このフィールドは、すべての証明書操作オプションをサポートし、操作を完了する必要がある期限の日付と時刻を指定します。 表示される値は、最初のノードに適用されます。
［証明書の操作ステータス（Certificate Operation Status）］	このフィールドは証明書操作の進行状況を表示します。たとえば、＜操作のタイプ＞ pending、failed、successful などで、操作のタイプには証明書操作オプションの［インストール / アップグレード］、［削除］、または［トラブルシューティング］が表示されます。このフィールドに表示される情報は変更できません。

LSC ステータスまたは認証文字列に基づく電話機の検索

証明書操作ステータスまたは認証文字列に基づいて電話機を検索するには、次の手順を実行します。

手順

ステップ 1　［デバイス］>［電話］の順に選択します。

検索と一覧表示ウィンドウが表示されます。アクティブな（前の）クエリーのレコードもウィンドウに表示される場合があります。

ステップ 2　最初のドロップダウン リスト ボックスから、次のオプションのいずれかを選択します。

- ［**LSC ステータス**］：このオプションを選択すると、ローカルで有効な証明書のインストール、アップグレード、削除、またはトラブルシューティングに CAPF を使用する電話機のリストが表示されます。
- ［**認証文字列**］：このオプションを選択すると、［認証文字列（Authentication String）］フィールドで指定された認証文字列を持つ電話機のリストが返されます。

ステップ 3　2 番目のドロップダウン リスト ボックスから、検索パターンを選択します。

ステップ 4　必要に応じて適切な検索テキストを指定します。

（注）　検索条件を追加するには、［+］ボタンをクリックします。条件を追加すると、指定したすべての条件に一致するレコードが検索されます。条件を削除するには、［–］ボタンをクリックして最後に追加した条件を削除するか、［**フィルタのクリア**］ボタンをクリックして追加したすべての検索条件を削除します。

ステップ 5　［**検索**］をクリックします。

一致するすべてのレコードが表示されます。［ページあたりの行数］ドロップダウン リスト ボックスから異なる値を選択すると各ページに表示される項目数を変更できます。

ステップ 6　表示するレコードのリストから、表示するレコードのリンクをクリックします。

（注）　リストの見出しに上向きまたは下向きの矢印がある場合は、その矢印をクリックして、ソート順序を逆にします。

ウィンドウに選択した項目が表示されます。

追加情報

詳細については、P.6-13 の「関連項目」を参照してください。

CAPF レポートの生成

必要に応じて CAPF レポートを生成し、証明書操作のステータス、認証文字列、セキュリティ プロファイル、認証モードなどを表示できます。レポートには、デバイス名、デバイスの説明、セキュリティ プロファイル、認証文字列、認証モード、LSC ステータスなどが含まれます。

CAPF レポートを生成するには、次の手順を実行します。

手順

ステップ 1　［**デバイス**］>［**電話**］の順に選択します。

［電話の検索と一覧表示（Find and List Phones）］ウィンドウが表示されます。アクティブな（前の）クエリーのレコードもウィンドウに表示される場合があります。

ステップ 2　データベースのすべてのレコードを検索するには、ダイアログボックスが空であることを確認して、ステップ 3 に進みます。

レコードの絞り込みまたは検索

- 最初のドロップダウン リスト ボックスから、検索パラメータを選択します。
- 2 番目のドロップダウン リスト ボックスから、検索パターンを選択します。
- 必要に応じて適切な検索テキストを指定します。

（注）　検索条件を追加するには、［+］ボタンをクリックします。条件を追加すると、指定したすべての条件に一致するレコードが検索されます。条件を削除するには、［–］ボタンをクリックして最後に追加した条件を削除するか、［**フィルタのクリア**］ボタンをクリックして追加したすべての検索条件を削除します。

ステップ 3　［**検索**］をクリックします。

一致するすべてのレコードが表示されます。［ページあたりの行数］ドロップダウン リスト ボックスから異なる値を選択すると各ページに表示される項目数を変更できます。

ステップ 4　［関連リンク］ドロップダウン リスト ボックスで、［**ファイルでの CAPF レポート**］を選択し、［**移動**］をクリックします。

ステップ 5　ファイルを任意の場所に保存します。

ステップ 6　Microsoft Excel を使用して .csv ファイルを開きます。

追加情報

詳細については、P.6-13 の「関連項目」を参照してください。

電話機での認証文字列の入力

認証ストリング モードを選択して認証文字列を生成した場合、ローカルで有効な証明書をインストールするには、電話機に認証文字列を入力する必要があります。

ヒント　認証文字列は 1 回の使用に限って適用されます。［電話の設定（Phone Configuration）］ウィンドウまたは CAPF レポートに表示される認証文字列を入手します。

始める前に

電話機に認証文字列を入力する前に、次の条件を満たしていることを確認します。

- CAPF 証明書が CTL ファイル内に存在する。
- P.6-6 の「Certificate Authority Proxy Function サービスのアクティブ化」の説明に従って、Cisco Certificate Authority Proxy Function サービスをアクティブにした。
- 最初のノードが実行中で、機能している。証明書のインストールごとにサーバが実行していることを確認します。
- デバイスが登録済みである。
- 署名付きイメージが電話機に存在する。使用している電話機モデルをサポートする Cisco Unified IP Phone の管理マニュアルを参照してください。

手順

ステップ 1　電話機の設定ボタンを押します。

ステップ 2　設定がロックされている場合は、**#（アスタリスク、アスタリスク、ポンド記号）を押してロックを解除します。

ステップ 3　下方にスクロールして［Settings（設定）］メニューに移動します。［Security Configuration（セキュリティ設定）］を強調表示し、［Select（選択）］ソフトキーを押します。

ステップ 4　下方にスクロールして［Security Configuration（セキュリティ設定）］メニューに移動します。［LSC］を強調表示し、［Update（更新）］ソフトキーを押します。

ステップ 5　認証文字列の入力を要求するプロンプトが表示された場合、システムから提供された文字列を入力して［Submit（送信）］ソフトキーを押します。

電話機は現在の CAPF の設定に応じて、証明書をインストール、更新、削除、または取得します。

電話機に表示されるメッセージを確認すると、証明書の操作の進捗を監視することができます。［Submit（送信）］を押すと、LSC オプションの下に「Pending（処理中）」というメッセージが表示されます。電話機は、公開鍵と秘密鍵のペアを生成し、情報を電話機に表示します。電話機が正常に手順を完了すると、成功したことを示すメッセージが電話機に表示されます。電話機に失敗のメッセージが表示されるのは、誤った認証文字列を入力したか、電話機のアップグレードを有効にしなかった場合です。

［Stop（中止）］オプションを選択すると、いつでも手順を停止できます。

電話機での認証文字列の確認

［**Settings**（設定）］>［**Model Information**（モデル情報）］の順に選択して LSC の設定が［Installed（インストール済み）］か［Not Installed（未インストール）］のどちらであるかを確認すれば、証明書がインストールされているかどうかを確認できます。

追加情報

詳細については、P.6-13 の「関連項目」を参照してください。

その他の情報

関連項目

- Certificate Authority Proxy Function の概要（P.6-2）
- Cisco Unified IP Phone と CAPF の相互作用（P.6-2）
- CAPF システムの相互作用および要件（P.6-4）
- Cisco Unified Serviceability での CAPF の設定（P.6-4）
- CAPF の設定用チェックリスト（P.6-5）
- Certificate Authority Proxy Function サービスのアクティブ化（P.6-6）
- CAPF サービス パラメータの更新（P.6-7）
- CAPF による電話機の証明書のインストール、アップグレード、トラブルシューティング、または削除（P.6-8）
- 電話の設定（Phone Configuration）ウィンドウの CAPF 設定（P.6-9）
- LSC ステータスまたは認証文字列に基づく電話機の検索（P.6-10）
- CAPF レポートの生成（P.6-11）
- 電話機での認証文字列の入力（P.6-12）
- 電話機での認証文字列の確認（P.6-13）

シスコの関連マニュアル

Cisco Unified IP Phone アドミニストレーション ガイド for Cisco Unified Communications Manager

Cisco Unified Communications Manager Serviceability アドミニストレーション ガイド