CHAPTER 4

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 CallManager 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。

- ローカルで有効な証明書を、サポートされている Cisco IP Phone モデルに対して発行する。
- SCEP を使用して、サポートされる Cisco IP Phone モデルに代わって、サードパーティの認証局による証明書を要求する。
- 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。
- 電話機にあるローカルで有効な証明書を削除する。
- 製造元でインストールされる証明書によって認証する。

Cisco Certificate Authority Proxy Function サービスをアクティブにすると、CAPF に固有なキー 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、各サーバの C:\Program Files\Cisco\Certificates を参照して次のファイルを検索します。

- DER 符号化形式の場合：CAPF.cer
- PEM 符号化形式の場合：CAPF.cer と同じ通常名文字列が含まれる .0 拡張子ファイル

関連項目

- CAPF システムの対話および要件（P.4-5）
- CAPF の設定用チェックリスト（P.4-10）

Cisco IP Phone と CAPF の対話

電話機が CAPF と対話するときに、電話機はその公開キーと秘密キーのペアを生成し、署名付きの暗号化メッセージで公開キーを CAPF サーバへ転送します。秘密キー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。Cisco CallManager Administration での設定に応じて、CAPF は電話機の証明書に署名するか、またはサードパーティのシスコ認定 CA サーバに対する SCEP プロトコル プロキシとして動作し、電話機の証明書に署名する場合があります。その後で CAPF は署名付きの暗号化メッセージで証明書を電話機に戻します。

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　キー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。キー生成の完了には 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 ビットのキーを選択すると、電話機の起動およびフェールオーバー中に電話機、Cisco CallManager、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 ビットのキーは設定しないでください。

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

次の例では、LSC が電話機内にまだ存在しない場合や、CAPF Authentication Mode に By Existing Certificate が選択されている場合に、CAPF 証明書操作が失敗します。

例：ノンセキュアの Device Security Mode

この例では、Device Security Mode をノンセキュアに、CAPF Authentication Mode を By Null String または By Existing Certificate (Precedence...) 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 CallManager 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 Device Support Mode を Authenticated または Encrypted に設定します。

例：認証済みまたは暗号化済みの Device Security Mode

この例では、Device Security Mode を認証済みまたは暗号化済みに、CAPF Authentication Mode を By Null String または By Existing Certificate (Precedence...) 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 CallManager 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、By Authentication String 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。

関連項目

- CAPF システムの対話および要件（P.4-5）
- CAPF の設定用チェックリスト（P.4-10）
- *Cisco IP Phone アドミニストレーション ガイド for Cisco CallManager*

CAPF システムの対話および要件

CAPF には、次の要件があります。

- Cisco CallManager 4.1 にアップグレードする前に、次の項を確認します。
  - 既存の CAPF データの移行（P.4-8）
  - 4.0 サブスクライバ サーバから 4.0 パブリッシャ データベース サーバへの CAPF 1.0(1) データのコピー（P.4-12）
- 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、パブリッシャ データベース サーバで 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。
- 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 CallManager 4.1 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、パブリッシャ データベース サーバ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。
- Microsoft Certificate Services ソフトウェアが Windows 2003 サーバで実行されている場合は、Microsoft Certificate Services を CAPF で使用することもできます。このソフトウェアの使用方法、またはトラブルシューティングのサポートについては、認証局のベンダーに直接連絡してください。

  CAPF が Microsoft Certificate Services による証明書を要求する場合は、IP アドレスまたはホスト名など、この認証局の必要な設定情報を該当する CAPF サービス パラメータに入力する必要があります。

  Microsoft Certificate Services を使用する場合は、Microsoft Certificate Services をインストールしたサーバに SCEP アドオンをインストールする必要があります。SCEP アドオンを入手するには、認証局のベンダーに直接連絡してください。

ヒント　サードパーティの認証局は、ユーザが Cisco CallManager Administration で設定した CAPF 設定を上書きする証明書発行ポリシーを強制する場合があります。サードパーティの Certificate Authority（CA; 認証局）を CAPF で使用する前に、認証局のベンダーによる資料を参照して、証明書の発行に影響を及ぼす可能性のある制限事項がないことを確認してください。

- Keon Utility を使用して CAPF の証明書を生成することもできます。IP アドレスまたはホスト名など、この認証局の必要な設定情報を該当する CAPF サービス パラメータに入力する必要があります。また、該当するサービス パラメータ フィールドに Keon Jurisdiction ID を入力する必要もあります。

  Keon ソフトウェアの使用方法、またはトラブルシューティングのサポートについては、認証局のベンダーに直接連絡してください。
- Keon Utility または Microsoft Certificate Services を CAPF で使用するには、次の Object ID を定義する必要があります。次の設定の使用方法については、認証局のベンダーによる資料を参照してください。
  - (1.3.6.1.5.5.7.3.1) Server SSL/TLS authentication
  - (1.3.5.1.5.5.7.3.2) Client SSL/TLS authentication
  - (1.3.6.1.5.5.7.3.5) IPSec end system authentication

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 CallManager によって情報が Cisco CallManager データベースに格納されるためです。

関連項目

- Certificate Authority Proxy Function の概要（P.4-2）
- CAPF システムの対話および要件（P.4-5）
- 既存の CAPF データの移行（P.4-8）
- CAPF の設定用チェックリスト（P.4-10）

Cisco CallManager Serviceability での CAPF の設定

次の作業を Cisco CallManager 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。

関連項目

- *Cisco CallManager Serviceability アドミニストレーション ガイド*
- *Cisco CallManager Serviceability システム ガイド*

既存の CAPF データの移行

注意　ここで説明する作業の実行に失敗すると、CAPF データが失われる可能性があります。P.4-10 の「CAPF の設定用チェックリスト」および P.4-12 の「4.0 サブスクライバ サーバから 4.0 パブリッシャ データベース サーバへの CAPF 1.0(1) データのコピー」に加えて、次の情報も参照してください。

ローカルで有効な証明書をインストールまたは上書きする前に、次の詳細を確認してください。

- Cisco CallManager 4.0 パブリッシャ データベース サーバに CAPF がインストールされていた Cisco CallManager 4.0 からのアップグレード：Cisco CallManager 4.0 で証明書の操作を実行し、CAPF 1.0(1) をパブリッシャ データベース サーバ上で実行していた場合は、最新の操作ステータスが Cisco CallManager 4.1 データベースに移行されます。
- Cisco CallManager 4.0 サブスクライバ サーバに CAPF がインストールされていた Cisco CallManager からのアップグレード：Cisco CallManager 4.0 で証明書の操作を実行し、CAPF 1.0(1) をサブスクライバ サーバ上で実行していた場合は、CAPF データを 4.0 パブリッシャ データベース サーバにコピーしてから、クラスタを Cisco CallManager 4.1 にアップグレードする必要があります。

注意　Cisco CallManager 4.0 または 4.1 へアップグレードする前にデータをコピーできなかった場合、Cisco CallManager 4.0 サブスクライバ サーバ上の CAPF データは Cisco CallManager 4.1 データベースに移行されず、データは失われる可能性があります。データが失われた場合、CAPF utility 1.0(1) を使用して発行したローカルで有効な証明書は電話機に残ります。CAPF 4.1(3) は証明書を再発行しますが、証明書は有効ではありません。

- Cisco CallManager 4.1(x) のいずれかのリリースから、以降のリリースの Cisco CallManager 4.1(x) へのアップグレード：アップグレードによって CAPF データは自動的に移行されます。

関連項目

- Certificate Authority Proxy Function の概要（P.4-2）
- CAPF システムの対話および要件（P.4-5）
- CAPF の設定用チェックリスト（P.4-10）
- 4.0 サブスクライバ サーバから 4.0 パブリッシャ データベース サーバへの CAPF 1.0(1) データのコピー（P.4-12）

CAPF の設定用チェックリスト

表 4-1 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、削除、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 4-1　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。 CAP 1.0(1) データを Cisco CallManager 4.1(3) 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。	• Manufacture-Installed Certificate（MIC）が IP Phone 内に存在することの確認（P.9-43） • ローカルで有効な証明書が IP Phone 上に存在することの確認（P.9-42） • 既存の CAPF データの移行（P.4-8） • 4.0 サブスクライバ サーバから 4.0 パブリッシャ データベース サーバへの CAPF 1.0(1) データのコピー（P.4-12）
ステップ 2	Cisco CallManager 4.0 で CAPF utility を使用していて、CAPF データが Cisco CallManager 4.1 データベースに存在することを確認した場合は、Cisco CallManager 4.0 で使用していた CAPF utility を削除します。	**Settings > Control Panel** を選択します。**Add/Remove Programs** をダブルクリックして、ユーティリティを探します。ユーティリティを削除します。
ステップ 3	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.4-14）

表 4-1　CAPF の設定用チェックリスト（続き）

設定手順		関連手順および関連項目
ステップ 4	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.3-15）
ステップ 5	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.4-15）
ステップ 6	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、削除、またはトラブルシューティングするには、Cisco CallManager Administration または BAT を使用します。	• ローカルで有効な証明書のインストールおよびアップグレード（P.4-18） • Phone Configuration ウィンドウの CAPF 設定（P.4-21） • Bulk Administration Tool による CAPF の使用方法（P.4-25）
ステップ 7	CAPF を使用するデバイスのリストを表示するには、Cisco CallManager Administration で CAPF レポートを生成します。	CAPF レポートの生成（P.4-26）
ステップ 8	Authentication Mode 用の認証文字列オプションを選択した場合は、電話機で認証文字列を入力します。	電話機での認証文字列の入力（P.4-27）
ステップ 9	証明書の操作が予定したとおりに正常終了したことを確認します。	• ローカルで有効な証明書が IP Phone 上に存在することの確認（P.9-42） • Manufacture-Installed Certificate（MIC）が IP Phone 内に存在することの確認（P.9-43）

4.0 サブスクライバ サーバから 4.0 パブリッシャ データベース サーバへの CAPF 1.0(1) データのコピー

注意　CAPF utility 1.0(1) を Cisco CallManager 4.0 サブスクライバ サーバにインストールした場合、CAPF データを 4.0 パブリッシャ データベース サーバにコピーしてから、Cisco CallManager 4.1 にアップグレードする必要があります。この作業を実行しないと、CAPF データが失われることがあります。たとえば、C:\Program Files\Cisco\CAPF\CAPF.phone にある電話機レコード ファイルが失われる可能性があります。データが失われると、CAPF utility 1.0(1) を使用して発行したローカルで有効な証明書は電話機に残ります。CAPF 4.1(3) は証明書を再発行しますが、証明書は有効ではありません。

次に示す手順は、P.4-8 の「既存の CAPF データの移行」と併せて使用してください。ファイルをコピーするには、次の手順を実行します。

手順

ステップ 1　CAPF 1.0 がインストールされているマシンから Cisco CallManager 4.0 がインストールされているパブリッシャ データベース サーバに、表 4-2 のファイルをコピーします。

表 4-2　サーバからサーバへのコピー

コピー対象ファイル	CAPF 1.0 がインストールされているコピー元マシン内の場所	Cisco CallManager 4.0 がインストールされているコピー先パブリッシャ データベース サーバ内の場所
***.0**	C:\Program Files\Cisco\CAPF	C:\Program Files\Cisco\Certificates
CAPF.phone	C:\Program Files\Cisco\CAPF	C:\Program Files\Cisco\CAPF
CAPF.config ファイル	C:\Program Files\Cisco\CAPF	C:\Program Files\Cisco\CAPF

ステップ 2　クラスタ内のすべてのサーバを Cisco CallManager 4.1 にアップグレードします。

ステップ 3　クラスタを Cisco CallManager 4.1 にアップグレードしたら、Cisco CTL クライアントをアップグレードし、電話機を使用する前にクライアントを実行します。Cisco CTL クライアントによって、CAPF 証明書がクラスタ内のすべてのサーバにコピーされます。

ステップ 4　Cisco CallManager 4.0 で使用していた CAPF utility をアンインストールします。表 4-1 を参照してください。

ステップ 5　詳細については、P.9-43 の「新規 CAPF 証明書の生成」を参照してください。

関連項目

- Certificate Authority Proxy Function の概要（P.4-2）
- CAPF システムの対話および要件（P.4-5）
- 既存の CAPF データの移行（P.4-8）
- CAPF の設定用チェックリスト（P.4-10）

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

Cisco CallManager 4.1 では、Cisco CallManager 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、パブリッシャ データベース サーバ上だけで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.3-21 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 CallManager Serviceability で **Tools > Service Activation** の順に選択します。

ステップ 2　ウィンドウの左側のペインで、パブリッシャ データベース サーバを選択します。

ステップ 3　**Certificate Authority Proxy Function** サービスのチェックボックスをオンにします。

ステップ 4　**Update** をクリックします。

関連項目

- CAPF の設定用チェックリスト（P.4-10）
- *Cisco CallManager Serviceability アドミニストレーション ガイド*
- *Cisco CallManager Serviceability システム ガイド*

CAPF サービス パラメータの更新

証明書の生成に Microsoft Certificate Services または Keon Utility を使用している場合、Cisco CallManager Administration で一部の CAPF サービス パラメータを更新する必要があります。

CAPF Service Parameter ウィンドウには、証明書の有効年数、システムによるキー生成の最大再試行回数、キー サイズなどの情報も表示されます。

Cisco CallManager Administration で CAPF サービス パラメータを表示する前に、P.4-14 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 CallManager Administration で **Service > Service Parameter** 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、パブリッシャ データベース サーバを選択します。

ステップ 3　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　CAPF サービス パラメータを更新します。Service Parameter ウィンドウで i ボタンをクリックし、次のサービス パラメータに関する説明を表示します。

- Certificate Issuer
- Duration of Certificate Validity (years)
- Key Size (bits)
- Maximum Allowable Time for Key Generation (minutes)
- Maximum Allowable Attempts for Key Generation
- Keon Jurisdiction ID

- SCEP Port Number
- Certificate Authority Address

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。

関連項目

- Certificate Authority Proxy Function の概要（P.4-2）
- CAPF システムの対話および要件（P.4-5）
- CAPF の設定用チェックリスト（P.4-10）
- Certificate Authority Proxy Function サービスのアクティブ化（P.4-14）

CAPF エンタープライズ パラメータの更新

次のエンタープライズ パラメータは CAPF をサポートしています。

- CAPF Phone Port
- CAPF Operation Expires in (days)

ヒント　Cisco CallManager Administration のパラメータにアクセスするには、**System > Enterprise Parameters** の順に選択します。パラメータの説明を表示するには、Enterprise Parameters ウィンドウに表示される i ボタンをクリックします。変更内容を有効にするには、パラメータの更新後に電話機をリセットする必要があります。

関連項目

- Certificate Authority Proxy Function の概要（P.4-2）
- CAPF システムの対話および要件（P.4-5）
- CAPF の設定用チェックリスト（P.4-10）
- Certificate Authority Proxy Function サービスのアクティブ化（P.4-14）
- CAPF サービス パラメータの更新（P.4-15）

ローカルで有効な証明書のインストールおよびアップグレード

CAPF を使用するときに、表 4-3 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 CallManager Administration で **Device > Phone** の順に選択します。

ステップ 2　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検索します。電話機の検索については、『*Cisco CallManager 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　表 4-3 の説明に従って、設定内容を入力します。

ステップ 4　**Update** をクリックします。

ステップ 5　**Reset Phone** をクリックします。

ステップ 6　Install/Upgrade Certificate Operation オプションと By Authentication String モード オプションを選択した場合は、電話機に認証文字列を入力する必要があります。この作業を実行する方法については、P.4-27 の「電話機での認証文字列の入力」を参照してください。

関連項目

- Certificate Authority Proxy Function の概要（P.4-2）
- CAPF システムの対話および要件（P.4-5）
- CAPF の設定用チェックリスト（P.4-10）
- Phone Configuration ウィンドウの CAPF 設定（P.4-21）
- Bulk Administration Tool による CAPF の使用方法（P.4-25）
- 電話機での認証文字列の入力（P.4-27）

ローカルで有効な証明書の削除

CAPF では、シスコの製造過程で電話機にインストールされた証明書は削除しません。CAPF で削除するのは、CAPF またはシスコ認定のサードパーティ認証局が発行した証明書だけです。

注意　電話機に Manufacture Installed Certificate （MIC; 製造元でインストールされる証明書）が含まれない場合は、Locally Significant Certificate （LSC; ローカルで有効な証明書）を削除する前に、電話機のデバイス セキュリティ モードをノンセキュアに変更する必要があります。デバイス セキュリティ モードを変更する前に証明書を削除すると、電話機を Cisco CallManager に登録できません。デバイス セキュリティ モードの変更については、P.5-1 の「電話機のセキュリティ設定」を参照してください。

電話機ではなく Cisco CallManager Administration から証明書を削除するには、次の手順を実行します。

手順

ステップ 1　Cisco CallManager Administration で **Device > Phone** の順に選択します。

ステップ 2　ローカルで有効な証明書を削除する電話機を検索します。CAPF を使用する電話機の検索方法については、『*Cisco CallManager 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　Certificate Operation ドロップダウン リスト ボックスから、**Delete** オプションを選択します。

ステップ 4　**Update** をクリックします。

ステップ 5　**Reset Phone** をクリックします。

ステップ 6　By Authentication String モードを選択した場合は、証明書を取り消す文字列を入力する必要があります。

ステップ 7　証明書の発行にシスコ認定のサードパーティ認証局を使用していた場合、その認証局が証明書を取り消したことを確認します。この作業を実行する方法については、サードパーティの認証局ベンダーにお問い合せください。

証明書が認証局によって電話機から削除されると、Phone Configuration ウィンドウの Operation Status フィールドに Delete Success と表示されます。

関連項目

- Certificate Authority Proxy Function の概要（P.4-2）
- CAPF システムの対話および要件（P.4-5）
- 既存の CAPF データの移行（P.4-8）
- Certificate Authority Proxy Function サービスのアクティブ化（P.4-14）
- CAPF サービス パラメータの更新（P.4-15）
- ローカルで有効な証明書のインストールおよびアップグレード（P.4-18）
- Phone Configuration ウィンドウの CAPF 設定（P.4-21）
- Bulk Administration Tool による CAPF の使用方法（P.4-25）
- 電話機での認証文字列の入力（P.4-27）
- ローカルで有効な証明書の削除（P.4-19）

Phone Configuration ウィンドウの CAPF 設定

表 4-3 は、Cisco CallManager Administration の Phone Configuration ウィンドウにある CAPF 設定について説明しています。

表 4-3　CAPF 設定

設定	説明
Certificate Operation	ドロップダウン ボックスから、次のオプションのいずれか 1 つを選択します。 • **No Pending Operation**：証明書の操作が予定されていないときに表示されます（デフォルトの設定）。 • **Install/Upgrade**：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。 • **Delete**：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。 • **Troubleshoot**：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 CallManager 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。 Troubleshoot 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。 **ヒント**　電話機に証明書が存在しない場合、Delete オプションと Troubleshoot オプションは表示されません。
Authentication Mode	このフィールドによって、電話機で CAPF を認証する方法を選択することができます。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、削除、またはトラブルシューティングする場合、あるいは製造元でインストールされる証明書によって認証する場合に、このフィールドを使用します。ドロップダウン ボックスから、次のオプションのいずれか 1 つを選択します。 • **By Authentication String**：ユーザが電話機に CAPF 認証文字列を入力した場合だけ、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、削除、またはトラブルシューティングします。

表 4-3　CAPF 設定（続き）

設定	説明
	• **By Null String** : ユーザが介入することなく、自動的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、削除、またはトラブルシューティングします。 このオプションではセキュリティを一切提供しません。したがって、このオプションは安全な閉じた環境の場合にだけ選択することを強く推奨します。 • **By Existing Certificate (Precedence to LSC)** : 製造元でインストールされる証明書（MIC）またはローカルで有効な証明書（LSC）が電話機に存在する場合、自動的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、削除、またはトラブルシューティングします。LSC が電話機に存在する場合、MIC が電話機に存在するかどうかに関係なく、認証は LSC を介して行われます。MIC と LSC が電話機に存在する場合、認証は LSC を介して行われます。電話機に LSC が存在せず、MIC が存在する場合、認証は MIC を介して行われます。 このオプションを選択する前に、証明書が電話機に存在することを確認します。このオプションを選択した場合に証明書が電話機に存在しないと、操作は失敗します。 MIC と LSC は電話機で同時に存在できるものの、電話機は常に 1 つの証明書だけを使用して CAPF を認証します。優先されるプライマリ証明書が何らかの理由で侵害された場合、あるいは他の証明書を介して認証する場合には、認証モードを更新する必要があります。 • **By Existing Certificate (Precedence to MIC)** : LSC または MIC が電話機に存在する場合、自動的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、削除、またはトラブルシューティングします。MIC が電話機に存在する場合、LSC が電話機に存在するかどうかに関係なく、認証は MIC を介して行われます。電話機に LSC だけが存在し MIC が存在しない場合、認証は LSC を介して行われます。 このオプションを選択する前に、証明書が電話機に存在することを確認します。このオプションを選択した場合に証明書が電話機に存在しないと、操作は失敗します。

表 4-3　CAPF 設定（続き）

設定	説明
Authentication String	By Authentication String 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 Generate String 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、削除、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。
Generate String	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 Authentication String フィールドに表示されます。
Key Size (bits)	ドロップダウン リスト ボックスから、証明書のキー サイズを選択します。デフォルト設定値は 1024 です。これ以外のオプションには、512 と 2048 があります。 デフォルト設定値よりも大きなキー サイズを選択すると、電話機でキー生成に必要なエントロピーを生成するためにさらに時間がかかります。キー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。電話機モデルによっては、キー生成の完了に 30 分以上かかることがあります。
Operation Completes by	このフィールドは Certificate Operation の Install/Upgrade、Delete、および Troubleshoot オプションをサポートしており、操作の完了が必要な期限として日付と時刻を指定します。 表示される値は、パブリッシャ データベース サーバに適用されます。
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、<operation type> pending、failed、successful などで、operating type には Certificate Operation オプションの Install/Upgrade、Delete、または Troubleshoot 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。

関連項目

- Certificate Authority Proxy Function の概要（P.4-2）
- CAPF システムの対話および要件（P.4-5）
- CAPF の設定用チェックリスト（P.4-10）
- ローカルで有効な証明書のインストールおよびアップグレード（P.4-18）
- Bulk Administration Tool による CAPF の使用方法（P.4-25）
- 電話機での認証文字列の入力（P.4-27）
- ローカルで有効な証明書の削除（P.4-19）

Bulk Administration Tool による CAPF の使用方法

多数のローカルで有効な証明書を同時にインストール、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場合には、クラスタで実行されているバージョンの Cisco CallManager と互換性のある Cisco Bulk Administration Tool を使用する必要があります。

BAT を使用して証明書をインストールまたは削除する前に、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。

証明書のインストールは、スケジューリングされたメンテナンス画面で行うことを強く推奨します。これは、証明書の生成によってコール処理が中断される可能性があるためです。

関連項目

- CAPF の設定用チェックリスト（P.4-10）
- Certificate Authority Proxy Function サービスのアクティブ化（P.4-14）
- *Bulk Administration Tool ユーザ ガイド*

CAPF レポートの生成

Cisco CallManager Administration では、CAPF レポートを生成して証明書の操作ステータス、認証文字列、またはリストされたデバイスの認証モードを確認することができます。CAPF レポートを生成したら、レポートを CSV ファイルで表示することができます。

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　Cisco CallManager Administration で **Device > Device Settings > CAPF Report** の順に選択します。

ステップ 2　レポートに表示するデバイスを検索するには、Find/List ドロップダウン リスト ボックスから検索対象を選択します。

ステップ 3　**Find** をクリックします。

デバイス リストが表示されます。

ステップ 4　CAPF レポートを CSV ファイルで表示するには、ウィンドウの右上隅にある **View the Report in File** リンクをクリックします。

ステップ 5　必要に応じて、CSV ファイルを安全な場所に保存して修正することもできます。

関連項目

- Certificate Authority Proxy Function の概要（P.4-2）
- CAPF システムの対話および要件（P.4-5）
- CAPF の設定用チェックリスト（P.4-10）
- Phone Configuration ウィンドウの CAPF 設定（P.4-21）
- 電話機での認証文字列の入力（P.4-27）

LSC Status の選択による電話機の検索

LSC Status を選択して電話機を検索およびリストする方法については、P.5-14 の「認証、暗号化、LSC ステータスによる電話機の検索」を参照してください。

関連項目

- CAPF の設定用チェックリスト（P.4-10）
- トラブルシューティング（P.9-1）

電話機での認証文字列の入力

By Authentication String モードを選択して Cisco CallManager で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前に、電話機に認証文字列を入力する必要があります。

ヒント　電話機ユーザは次の手順を実行して、証明書をインストールすることができます。認証文字列は 1 回の使用に限って適用されます。

始める前に

- CAPF 証明書が CiscoCTL ファイル内に存在することを確認します。
- CAPF 証明書が Cisco CallManager サーバの証明書フォルダに存在することを確認します。それには、サーバで C:\Program Files\Cisco\Certificates を参照します。
- P.4-14 の「Certificate Authority Proxy Function サービスのアクティブ化」で説明されているように、Cisco Certificate Authority Proxy Function サービスをアクティブにしたことを確認します。
- パブリッシャ データベース サーバ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。
- 署名付きイメージが電話機に存在することを確認します。使用している電話機モデルをサポートする Cisco IP Phone の管理マニュアルを参照してください。

- Phone Configuration ウィンドウまたは CAPF Report ウィンドウに表示される認証文字列を入手します。

手順

ステップ 1　Phone Configuration ウィンドウまたは CAPF Report ウィンドウから、デバイスの CAPF 認証文字列を入手します。

ステップ 2　デバイスが Cisco CallManager に登録されていることを確認します。

ステップ 3　デバイス セキュリティ モードが Nonsecure であることを確認します。

ステップ 4　ノンセキュアの Cisco IP Phone model 7970、7960、または 7940 で **Settings** ボタンを押します。

ステップ 5　Settings メニューで **Security Configuration** オプションまでスクロールし、**Select** ソフトキーを押します。

ヒント　電話メニューがロックされている場合は、電話機のマニュアルの説明に従ってメニューをロック解除します。

ステップ 6　**LSC** オプションまでスクロールして、**Update** ソフトキーを押します。

ステップ 7　電話機の 4 ～ 10 桁の認証文字列を入力して、**Submit** を押します。

ヒント　Submit を押す前に認証文字列を変更する必要がある場合は、**<<** を押します。

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

電話機に表示されるメッセージを確認することで、証明書操作の進行状況を監視します。Submit を押すと、Pending というメッセージが LSC オプションの下に表示されます。電話機は公開キーと秘密キーのペアを生成し、電話機に関する情報を表示します。電話機がプロセスを正常に完了すると、成功を示すメッセージが表示されます。失敗を示すメッセージが電話機に表示された場合は、間違った認証文字列を入力したか、電話機でアップグレードを有効にしていませんでした。P.9-1 の「トラブルシューティング」を参照してください。

Stop オプションを選択すれば、いつでもプロセスを停止することができます。

電話機に証明書がインストールされたことを確認するには、**Settings > Model Information** を選択し、LSC 設定を表示します。この設定に、Installed または Not Installed と示されます。

関連項目

- CAPF の設定用チェックリスト（P.4-10）
- Phone Configuration ウィンドウの CAPF 設定（P.4-21）
- Bulk Administration Tool による CAPF の使用方法（P.4-25）
- 電話機での認証文字列の入力（P.4-27）
- ローカルで有効な証明書の削除（P.4-19）
- *Cisco IP Phone 7960G/7940G アドミニストレーション ガイド for Cisco CallManager*