暗号化された電話機設定ファイルの設定

セキュリティ関連の設定を構成した後、電話機設定ファイルには、ダイジェスト パスワードや電話機管理者パスワードなど、機密性が高い設定情報が含まれます。設定ファイルの機密性を守るために、設定ファイルを暗号化するように設定する必要があります。

この章は、次の内容で構成されています。

電話機設定ファイルの暗号化について

電話機設定ファイルを暗号化するには、Cisco CallManager Administration のエンタープライズ パラメータを有効にし、Cisco CallManager Administration で追加作業を実行する必要があります。パラメータを有効にして、必要なサービスを Cisco CallManager Serviceability で再起動すると、TFTP サーバは暗号化されていないテキストの設定ファイルをすべて削除してから、設定ファイルの暗号化されたバージョンを生成します。電話機が暗号化された電話機設定ファイルをサポートしている場合に、電話機設定ファイルの暗号化に必要な作業を実行すると、電話機は設定ファイルの暗号化されたバージョンを要求します。

警告　**SIP 電話機のダイジェスト認証が True で、TFTP 暗号化設定が False に設定されている場合、ダイジェスト クレデンシャルは暗号化されずに送信されます。詳細については、P.7-9 の「電話機設定ファイルの暗号化の無効化」を参照してください。**

P.7-4 の「サポートされる電話機のモデル」で説明するように、暗号化された電話機設定ファイルをサポートしない電話機モデルがあります。電話機モデルによって、設定ファイルの暗号化に使用される方式が決まります。サポートされる方式は、Cisco CallManager の機能と、暗号化された設定ファイルをサポートするファームウェア ロードに依存します。暗号化された設定ファイルをサポートしないバージョンに電話機ファームウェアをダウングレードした場合、TFTP サーバは、最小限の設定内容を含む暗号化されていない設定ファイルを提供します。その結果、電話機が期待されるとおりに動作しない可能性があります。

鍵情報の機密性を維持するために、暗号化された電話機設定ファイルに関する作業は、セキュアな環境で実行することを強く推奨します。

Cisco CallManager は、次の方式をサポートします。

- 鍵の手動配布（P.7-2）
- 電話機の公開鍵によるシンメトリック鍵の暗号化（P.7-3）

「鍵の手動配布」および「電話機の公開鍵によるシンメトリック鍵の暗号化」の項の情報は、クラスタを Secure Mode に設定し、Cisco CallManager Administration の TFTP Encrypted Configuration パラメータを有効にしたことを前提とします。

鍵の手動配布

ヒント　この方式をサポートする電話機モデルのリストについては、P.7-4 の「サポートされる電話機のモデル」を参照してください。

鍵の手動配布では、電話機がリセットされた後、Cisco CallManager データベースに入力されている 128 ビットまたは 256 ビットのシンメトリック鍵によって、電話機設定ファイルが暗号化されます。使用中の電話機モデルの鍵サイズを判別するには、P.7-4 の「サポートされる電話機のモデル」を参照してください。

設定ファイルを更新するには、管理者が手動で鍵を Cisco CallManager Administration に入力するか、Cisco CallManager Administration で鍵を生成します。データベースに鍵が存在するようになった後、管理者またはユーザは、電話機のユーザ インターフェイスにアクセスして、電話機に鍵を入力する必要があります。**Accept** ソフトキーを押すとすぐに、鍵は電話機のフラッシュに格納されます。鍵を入力した後、電話機をリセットすると、電話機は暗号化された設定ファイルを要求します。必要な作業を実行した後、シンメトリック鍵は RC4 または AES 128 暗号化アルゴリズムを使用して、設定ファイルを暗号化します。電話機が RC4 と AES 128 のどちらの暗号化アルゴリズムを使用するかを判別するには、P.7-4 の「サポートされる電話機のモデル」を参照してください。

電話機にシンメトリック鍵が含まれている場合、電話機は暗号化された設定ファイルを要求します。電話機は、TFTP サーバが署名した暗号化された設定ファイルをダウンロードします。

Cisco SIP IP Phone 7960 モデルおよび 7940 モデルは、設定ファイルの署名者を検証しません。フラッシュに格納されているシンメトリック鍵を使用して、ファイルの内容が復号化されます。復号化に失敗した場合、設定ファイルは電話機に適用されません。

ヒント　TFTP Encrypted Configuration エンタープライズ パラメータを無効にした場合、管理者は、次にリセットしたときに電話機が暗号化されていない設定ファイルを要求するように、電話機 GUI からシンメトリック鍵を削除する必要があります。

電話機の公開鍵によるシンメトリック鍵の暗号化

ヒント　この方式をサポートする電話機モデルのリストについては、P.7-4 の「サポートされる電話機のモデル」を参照してください。

電話機に、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）が含まれている場合、電話機には公開鍵と秘密鍵のペアが含まれています。この方式を初めて使うとき、設定ファイルの電話機証明書の MD5 ハッシュと、LSC または MIC の MD5 ハッシュが比較されます。電話機で問題が検出されない場合、電話機は、リセット後に TFTP サーバから暗号化された設定ファイルを要求します。電話機で問題が検出された場合（ハッシュが一致しない、電話機に証明書が含まれていない、MD5 値がブランクであるなど）、CAPF 認証モードが By Authentication String でなければ、電話機は CAPF とのセッションを開始しようとします（By Authentication String の場合は、文字列を手動で入力する必要があります）。CAPF は、電話機の公開鍵を LSC または MIC から抽出し、MD5 ハッシュを生成し、公開鍵および証明書ハッシュの値を Cisco CallManager データベースに格納します。公開鍵がデータベースに格納された後、電話機はリセットされ、新しい設定ファイルが要求されます。

公開鍵がデータベースに存在するようになり、電話機がリセットされた後、電話機用の公開鍵があることをデータベースが TFTP に通知すると、シンメトリック鍵暗号化処理が開始されます。TFTP サーバは 128 ビット シンメトリック鍵を生成します。これによって、設定ファイルは Advanced Encryption Standard（AES）128 暗号化アルゴリズムで暗号化されます。次に、電話機の公開鍵でシンメトリック鍵が暗号化され、設定ファイルの署名付きエンベロープ ヘッダーに含まれます。電話機は、ファイルの署名を検証し、署名が有効である場合は、LSC または MIC の秘密鍵を使用して、暗号化されたシンメトリック鍵を復号化します。次に、シンメトリック鍵によって、ファイルの内容が復号化されます。

設定ファイルを更新するたびに、TFTP サーバは、ファイルを暗号化する新しい鍵を自動的に生成します。

ヒント　電話機の公開鍵を使用したシンメトリック鍵の暗号化をサポートする電話機は、設定ファイルの暗号化設定フラグを使用して、暗号化されたファイルと暗号化されていないファイルのどちらを要求するかを決定します。TFTP Encrypted Configuration エンタープライズ パラメータが無効の場合、Cisco IP Phone 7911、7941、7961、7970、および 7971 モデルが暗号化されたファイル（.enc.sgn ファイル）を要求すると、Cisco CallManager は「file not found error」を電話機に送信します。次に、電話機は、暗号化されていない署名付きファイル（.sgn ファイル）を要求します。

TFTP Encrypted Configuration エンタープライズ パラメータが有効の場合、何らかの理由で電話機が暗号化されていない設定ファイルを要求すると、TFTP サーバは最小限の設定内容を含む暗号化されていないファイルを提供します。

サポートされる電話機のモデル

次の電話機モデルで、電話機設定ファイルを暗号化できます。

- Cisco SIP IP Phone 7905 または 7912：鍵の手動配布をサポート。

  シンメトリック鍵は RC4 暗号化アルゴリズムを使用し、鍵サイズは 256 ビットです。これらの SIP 電話機モデルは、ファイル署名をサポートしません。
- Cisco SIP IP Phone 7940 または 7960：鍵の手動配布をサポート。

  シンメトリック鍵は Advanced Encryption Standard（AES）128 暗号化アルゴリズムを使用し、鍵サイズは 128 ビットです。これらの SIP 電話機は、署名付きで暗号化された設定ファイルを受信しますが、署名情報を無視します。
- Cisco SIP IP Phone 7970 または 7971、Cisco SIP IP Phone 7941 または 7961、Cisco SIP IP Phone 7911、Cisco IP Phone 7970 または 7971、Cisco IP Phone 7941 または 7961、Cisco IP Phone 7911：電話機の公開鍵によるシンメトリック鍵の暗号化をサポート。

  シンメトリック鍵は AES 128 暗号化アルゴリズムを使用し、鍵サイズは 128 ビットです。これらの電話機は、ファイル署名をサポートします。

暗号化設定ファイルの設定用チェックリスト

電話機設定ファイルを暗号化するには、表 7-1 で示す作業を実行する必要があります。

表 7-1　暗号化設定ファイル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	Cluster Security Mode が Secure Mode に設定されていることを確認します。	Cisco CTL クライアントの設定（P.3-1）
ステップ 2	Cisco CallManager Administration の TFTP Encrypted Configuration エンタープライズ パラメータを有効にします。	電話機設定ファイルの暗号化エンタープライズ パラメータの有効化（P.7-6）
ステップ 3	鍵の手動配布をサポートする電話機、および電話機の公開鍵によるシンメトリック鍵の暗号化をサポートする電話機を判別します。	サポートされる電話機のモデル（P.7-4）
ステップ 4	使用中の電話機が鍵の手動配布をサポートする場合は、Cisco CallManager Administration で、鍵の手動配布の作業を実行します。	• 鍵の手動配布の設定（P.7-6） • 鍵の手動配布の設定内容（P.7-7）
ステップ 5	使用中の電話機が鍵の手動配布をサポートする場合は、電話機にシンメトリック鍵を入力し、電話機をリセットします。	電話機でのシンメトリック鍵の入力（P.7-7）
ステップ 6	使用中の電話機が、電話機の公開鍵によるシンメトリック鍵の暗号化をサポートしている場合、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ことを確認します。	• 電話機の公開鍵によるシンメトリック鍵の暗号化の使用（P.7-8） • 電話機設定ファイルの暗号化について（P.7-2） • Certificate Authority Proxy Function の使用方法（P.6-1）

電話機設定ファイルの暗号化エンタープライズ パラメータの有効化

電話機設定ファイルを暗号化する前に、Cisco CallManager Administration の TFTP Encrypted Configuration エンタープライズ パラメータを有効にする必要があります。TFTP サーバは、設定ファイルを構築するときに、データベースに問い合せます。エンタープライズ パラメータが有効の場合、TFTP サーバは暗号化された設定ファイルを構築します。

Cisco CallManager Administration のエンタープライズ 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。

デフォルト値など、エンタープライズ パラメータの詳細については、Enterprise Parameters Configuration ウィンドウに表示されている TFTP Encrypted Configuration リンクをクリックします。

鍵の手動配布の設定

使用中の電話機が鍵の手動配布をサポートしているかどうかを判別するには、P.7-4 の「サポートされる電話機のモデル」を参照してください。

鍵の手動配布を設定するには、次の手順を実行します。この手順では、電話機が Cisco CallManager データベースに存在し、互換性のあるファームウェア ロードが TFTP サーバに存在し、Cisco CallManager Administration の TFTP Encrypted Configuration エンタープライズ パラメータが有効であることを前提としています。

手順

ステップ 1　『*Cisco CallManager 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　Phone Configuration ウィンドウが表示された後、表 7-2 の説明に従って、鍵の手動配布設定を定義します。鍵を設定した後は、変更できません。

ステップ 3　**Save** をクリックします。

ステップ 4　電話機にシンメトリック鍵を入力し、電話機をリセットします。これらの作業の実行方法については、使用中の電話機モデルをサポートする電話機のアドミニストレーション ガイドを参照してください。

追加情報

詳細については、P.7-9 の「関連項目」を参照してください。

鍵の手動配布の設定内容

表 7-2 で、Phone Configuration ウィンドウに表示される手動配布の設定内容について説明します。関連する手順については、P.7-9 の「関連項目」を参照してください。

表 7-2　鍵の手動配布の設定内容

設定	説明
Symmetric Key	シンメトリック鍵として使用する 16 進文字の文字列を入力します。数字の 0 ～ 9 と、大文字または小文字の英字（A ～ F または a ～ f）を使用できます。 鍵サイズに対応した正しいビットを入力してください。そうでない場合、Cisco CallManager は入力された値を拒否します。Cisco CallManager は、次の鍵サイズをサポートします。 • Cisco IP Phone 7905 モデルおよび 7912 モデル（SIP プロトコルのみ）：256 ビット • Cisco IP Phone 7940 モデルおよび 7960 モデル（SIP プロトコルのみ）：128 ビット 鍵を設定した後は、変更できません。
Generate String	Cisco CallManager Administration で 16 進文字列を生成するには、**Generate String** ボタンをクリックします。 鍵が生成された後は、変更できません。
Revert to Database Value	データベースに存在する値に復元する場合は、このボタンをクリックします。

電話機でのシンメトリック鍵の入力

Cisco CallManager Administration で鍵の手動配布を設定した後、電話機にシンメトリック鍵を入力する方法については、使用中の電話機モデルおよびプロトコルをサポートする Cisco IP Phone のアドミニストレーション ガイドを参照してください。

電話機の公開鍵によるシンメトリック鍵の暗号化の使用

使用中の電話機が、電話機の公開鍵によるシンメトリック鍵の暗号化をサポートしているかどうかを判別するには、P.7-4 の「サポートされる電話機のモデル」を参照してください。この方式を使用するには、次の作業を実行します。この作業では、Cisco CallManager データベースに電話機が存在し、Cisco CallManager Administration の TFTP Encrypted Configuration エンタープライズ パラメータが有効であることを前提としています。

手順

ステップ 1　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ことを確認します。証明書が存在しない場合は、Phone Configuration ウィンドウの CAPF 機能を使用して、LSC をインストールします。LSC をインストールする方法については、P.6-1 の「Certificate Authority Proxy Function の使用方法」を参照してください。

ステップ 2　CAPF 設定を定義した後、**Save** をクリックします。

ステップ 3　Phone Configuration ウィンドウで、**Reset** をクリックします。

追加情報

詳細については、P.7-9 の「関連項目」を参照してください。

電話機設定ファイルが暗号化されていることの確認

電話機設定ファイルを暗号化するときは、次の形式が使用されます。

- Cisco IP Phone 7905 モデルおよび 7912 モデル（SIP プロトコルのみ）：LD <MAC>.x
- Cisco IP Phone 7940 モデルおよび 7960 モデル（SIP プロトコルのみ）：SIP<MAC>.cnf.enc.sgn
- Cisco IP Phone 7970 モデルおよび 7971 モデル（SIP プロトコルのみ）：SIP<MAC>.cnf.xml.enc.sgn
- Cisco IP Phone 7970 モデルおよび 7971 モデル（SCCP プロトコルのみ）：SEP<MAC>.cnf.xml.enc.sgn

電話機設定ファイルの暗号化の無効化

電話機設定ファイルの暗号化を無効にするには、Cisco CallManager Administration の TFTP Encrypted Configuration エンタープライズ パラメータを更新する必要があります。

警告　**SIP 電話機のダイジェスト認証が True で、TFTP 暗号化設定が False に設定されている場合、ダイジェスト クレデンシャルは暗号化されずに送信されます。**

エンタープライズ パラメータを更新した後、電話機の鍵は Cisco CallManager データベースに残ります。

Cisco IP Phone 7911、7941、7961、7970、および 7971 モデルが暗号化されたファイル（.enc.sgn ファイル）を要求している場合、暗号化設定を false に更新すると、電話機は暗号化されていない署名付きファイル（.sgn ファイル）を要求します。

Cisco IP SIP Phone 7940/7960/7905/7912 モデルが暗号化されたファイルを要求している場合、暗号化設定を false に更新したときは、次に電話機がリセットされたときに暗号化されていない設定ファイルを要求するように、管理者が電話機 GUI でシンメトリック鍵を削除する必要があります。

ヒント　Cisco IP SIP Phone 7940 モデルおよび 7960 モデルでは、電話機 GUI でシンメトリック鍵として 32 バイトの 0 を入力して、暗号化を無効にします。Cisco IP SIP Phone 7905 モデルおよび 7912 モデルでは、電話機 GUI でシンメトリック鍵を削除して、暗号化を無効にします。これらの作業の実行方法については、使用中の電話機モデルをサポートする電話機のアドミニストレーション ガイドを参照してください。

その他の情報

関連項目

- 電話機設定ファイルの暗号化について（P.7-2）
- サポートされる電話機のモデル（P.7-4）
- 暗号化設定ファイルの設定用チェックリスト（P.7-5）
- 電話機設定ファイルの暗号化エンタープライズ パラメータの有効化（P.7-6）
- 鍵の手動配布の設定（P.7-6）
- 鍵の手動配布の設定内容（P.7-7）
- 電話機でのシンメトリック鍵の入力（P.7-7）
- 電話機の公開鍵によるシンメトリック鍵の暗号化の使用（P.7-8）
- 電話機設定ファイルが暗号化されていることの確認（P.7-8）
- 電話機設定ファイルの暗号化の無効化（P.7-9）
- Certificate Authority Proxy Function の使用方法（P.6-1）

シスコの関連マニュアル

- *Cisco Bulk Administration Tool Guide*
- 電話機のモデルおよびプロトコルに対応した Cisco IP Phone アドミニストレーション ガイド