TFTP 暗号化

暗号化された TFTP 設定ファイルの概要

TFTP 設定は、電話機が登録プロセスを実行する際に TFTP サーバからダウンロードする設定ファイルを暗号化することによって、デバイスの登録プロセス中にデータを保護します。このファイルには、ユーザ名、パスワード、IP アドレス、ポートの詳細、電話機の SSH ログイン情報などの機密情報が含まれます。この機能が設定されていない場合、設定ファイルはクリアテキストで送信されます。この機能を導入すると、登録プロセス中に攻撃者がこの情報を傍受できなくなります。この情報は暗号化解除され、クリアテキストで送信されます。したがって、データを保護するために、TFTP 設定ファイルを暗号化することを推奨します。

警告 SIP 電話でダイジェスト認証オプションを有効にし、TFTP で暗号化設定オプションを無効にした場合は、ダイジェストログイン情報がクリアテキストで送信されます。

TFTP の設定後、TFTP サーバは次の手順を実行します。

- ディスク上のクリアテキストの設定ファイルをすべて削除します
- 暗号化されたバージョンのコンフィギュレーションファイルを生成します。

電話機が暗号化された電話設定ファイルをサポートし、電話設定ファイルの暗号化に必要なタスクを行った場合は、電話機は設定ファイルの暗号化バージョンを要求します。

一部の電話は、暗号化された電話設定ファイルをサポートしません。電話機のモデルとプロトコルによって、コンフィギュレーションファイルを暗号化するためにシステムが使用する方法が決定されます。サポートされる方式は、Unified Communications Manager 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。電話のファームウェアロードを、暗号化に対応していないバージョンにまでダウングレードすると、TFTP サーバは

最低限の設定を行う暗号化されていない設定ファイルを送ります。この場合、電話が期待された機能を発揮できないことがあります。

暗号化キーの配布

キー情報のプライバシーを確実に維持できるように、暗号化された電話設定ファイルに関連するタスクをセキュアな環境で実行することを推奨します。

Unified Communications Manager は、次の方式をサポートします。

- 手動キー配布
- 電話の公開キーによる対称キーの暗号化

手動キー配布と電話の公開キーによる対称キー暗号化のための設定情報は、混合モードが設定済みで、[Unified Communications Manager Administration] の [TFTP 暗号化設定（TFTP Encrypted Config）] パラメータが有効になっていることを前提としています。

暗号化された TFTP 設定ファイルのヒント

電話機のダウンロードで機密データを保護するには、TFTP 暗号化設定ファイルを有効にすることをお勧めします。電話に PKI 機能がない場合、[Unified Communications Manager Administration] と電話で対称キーも設定する必要があります。対称キーが電話機または Unified Communications Manager のいずれかに存在しない場合、または TFTP 暗号化設定ファイルの設定時に不一致が発生した場合、電話機は登録できません。

Unified Communications Manager で暗号化された設定ファイルを設定する場合は、次の点を考慮してください。

- 暗号化された設定ファイルをサポートしている電話機にのみ、[電話機のセキュリティプロファイルの設定（Phone Security Profile Configuration）] ページ)に [TFTP 暗号化設定（TFTP Encrypted Config）] チェックボックスが表示されます。暗号化された設定ファイルを Cisco Unified IP Phone の 7800、7942、および 7962（SCCP のみ）に設定することはできません。これらの電話機は設定ファイルのダウンロードで機密データを受信しないからです。
- デフォルトでは、[TFTP 暗号化設定（TFTP Encrypted Config）] チェックボックスはオフになっています。このデフォルト設定、非セキュアプロファイルを電話機に適用した場合、ダイジェストログイン情報とセキュアパスワードはクリアテキストで送信されます。
- 公開キー暗号化を使用する Cisco Unified IP Phone の場合、Unified Communications Manager では [デバイスセキュリティモード（Device Security Mod）] を [認証済み (Authenticated)] または [暗号化(Encrypted)] に設定して暗号化された設定ファイルを有効にする必要はありません。Unified Communications Manager は、登録中の公開鍵をダウンロードするために CAPF プロセスを使用します。
- 環境が安全である場合や、PKI が有効になっていない電話機に対称キーを手動で設定しないようにする場合は、暗号化されていない設定ファイルを電話機にダウンロードできます。ただし、この方法を使用することはお勧めしません。

- Cisco Unified IP Phone の 7800、7942、および 7962（SIP のみ）では、Unified Communications Manager は暗号化された設定ファイルを使用するよりも簡単で、安全性が低いダイジェストログイン情報を電話機に送信する方法を提供します。[ダイジェストログイン設定ファイルを除外（Exclude Digest Credentials in Configuration File）] 設定を使用するこの方法は、最初に対称キーを設定して電話に入力する必要がないため、ダイジェストログイン情報の初期化に役立ちます。この方法では、暗号化されていないコンフィギュレーションファイルで、電話機にダイジェストクレデンシャルを送信します。ログイン情報が電話機に入力された後は、[TFTP 暗号化設定（TFTP Encrypted Config）] オプションを無効にしてから、[電話機のセキュリティ プロファイルの設定（Phone Security Profile Configuration）] ページの [設定ファイルのダイジェストクレデンシャルを除外する（Exclude Digest Credential in Configuration File）] を有効にすることをお勧めします。これにより、今後のダウンロードからダイジェストログイン情報が除外されます。
- ダイジェストログイン情報が電話に存在するようになり、着信ファイルにダイジェストログイン情報が含まれないようになると、既存のログイン情報がそのまま使用されます。ダイジェストクレデンシャルは、電話機が工場出荷時の状態にリセットされるか、または新しいクレデンシャル(空白を含む)を受信するまで、そのまま残ります。電話機またはエンドユーザのダイジェストログイン情報を変更する場合は、対応する [電話機のセキュリティプロファイル情報（Phone Security Profile Information）] ページの [設定ファイルでのダイジェストログイン情報の除外（Exclude Digest Credential in Configuration File）] を一時的に無効にして、新しいダイジェストログイン情報を電話機にダウンロードします。

電話機の設定ファイルの暗号化のタスクフロー

TFTP 設定ファイルの暗号化を設定するには、クラスタのセキュリティが混合モードで設定されていることを確認し、手動キー暗号化と公開キー暗号化をサポートするクラスタ内の電話機を確認し、SHA-1 と SHA-512 をサポートする電話機を確認し、以下のタスクを完了します。

（注） SHA-512 クラスタ全体を有効にし、電話機がサポートしていない場合、これらの電話機は機能しません。

手順

	コマンドまたはアクション	目的
ステップ 1	TFTP 暗号化の有効化 （4 ページ）	電話機の [TFTP 設定ファイル (TFTP Configuration File)] オプションを有効にします。電話セキュリティプロファイルでこのオプションを有効にすることができます。
ステップ 2	SHA-512 署名アルゴリズムの設定 （4 ページ）	TFTP ファイル暗号化を有効化すると、デフォルトの署名アルゴリズムとして SHA-1 が設定されます。

	コマンドまたはアクション	目的
		より強力な SHA-512 アルゴリズムを使用するようにシステムを更新するには、次の手順を使用します。
ステップ 3	LSC または MIC 証明書のインストールの確認 （5 ページ）	公開キーを使用する電話機の場合は、証明書のインストールを確認します。
ステップ 4	CTL ファイルの更新 （6 ページ）	TFTP 設定ファイルの更新が完了したら、CTL ファイルを再生成します。
ステップ 5	サービスの再起動 （6 ページ）	Cisco CallManager サービスおよび Cisco TFTP サービスを再起動します。
ステップ 6	電話のリセット （6 ページ）	暗号化された TFTP 設定ファイルの更新が完了したら、電話機をリセットします。

TFTP 暗号化の有効化

この TFTP は、特定のモデルの電話の電話セキュリティプロファイル内で有効にできます。TFTP サーバからダウンロードするファイルの TFTP 暗号化を有効にするには、次の手順を実行します。

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**[システム（System）]** > **[セキュリティ（Security）]** > **[電話セキュリティプロファイル（Phone Security Profile）]**

ステップ 2 **[検索（Find）]** をクリックし、電話セキュリティ プロファイルを選択します。

ステップ 3 [**TFTP Encrypted Config**] チェックボックスをオンにします。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 クラスタで使用されている他のすべての電話セキュリティプロファイルに対して、これらの手順を繰り返します。

（注） 電話設定ファイルの暗号化を無効にするには、 Cisco Unified Communications Manager Administration の電話セキュリティプロファイルで **[TFTP 暗号化設定（TFTP Encrypted Config）]** チェックボックスをオフにして、変更内容を保存する必要があります。

SHA-512 署名アルゴリズムの設定

SHA-1 は TFTP ファイル暗号化のデフォルトのアルゴリズムです。次のオプションの手順を使用して、デジタル署名などの TFTP 設定ファイルにより強力な SHA-512 アルゴリズムを使用するようにシステムをアップグレードできます。

（注） ご使用の電話機が SHA-512 をサポートしていることを確認してください。対応していない場合は、システム更新後に電話機が動作しなくなります。

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**[システム（System）]** > **[エンタープライズパラメータ（Enterprise Parameters）]**

ステップ 2 [セキュリティパラメータ（Security Parameters）] ペインに移動します。

ステップ 3 [**TFTP File Signature Algorithm**] ドロップダウンリストから、[**SHA-512**] を選択します。

ステップ 4 [保存（Save）] をクリックします。

この手順を完了するには、ポップアップウィンドウに一覧表示されている影響を受けるサービスを再起動します。

LSC または MIC 証明書のインストールの確認

公開キーを使用する電話機の場合は、証明書のインストールを確認します。

（注） この手順は、PKI 暗号化を使用するCisco Unified IP Phoneに適用されます。電話機が PKI 暗号化をサポートしているかどうかを確認するには、「暗号化された設定ファイルをサポートする電話モデル」の項を参照して

次の手順は、電話機が Unified Communications Manager データベースに存在し、Unified Communications Manager で [TFTP 暗号化設定（TFTP Encrypted Config）] パラメータを有効にしていることを前提としています。

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）が電話に存在することを確認します。

ステップ 2 [Cisco Unified CM Administration] から、**[デバイス（Device）] > [電話機（Phone）]** の順に選択します。
電話機のリストが表示されます。

ステップ 3 [デバイス名（Device Name）] をクリックします。
[電話の設定（Phone Configuration）] ページが表示されます。

ヒント **[電話の設定（Phone Configuration）]** ページの [CAPF 設定（CAPF settings）] セクションで **[トラブルシュート（Troubleshoot）]** オプションを選択して、Unified Communications Managerの電話機にLSCまたはMICが存在するかどうかを確認します。証明書が電話機に存在しない場合、[削除（Delete）] および [トラブルシュート（Troubleshoot）] オプションは表示されません。

ヒント　電話機のセキュリティ設定を確認することによって、電話機に LSC または MIC が存在することを確認することもできます。詳細については、 Unified Communications Managerのこのバージョンをサポートする Cisco Unified 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。

ステップ 4　証明書が存在しない場合、[電話の設定（Phone Configuration）] ウィンドウで認証局プロキシ機能（CAPF）を使用して、LSC をインストールします。LSC のインストール方法については、Certificate Authority Proxy Function に関連するトピックを参照してください。

ステップ 5　CAPF を設定したら、[保存（Save）] をクリックします。

ステップ 6　[リセット（Reset）] をクリックします。
電話機はリセット後、TFTP サーバから暗号化された設定ファイルを要求します。

CTL ファイルの更新

Unified Communications Manager の変更を行った後、CTL ファイルを更新します。TFTP ファイル暗号化を有効にしているので、CTL ファイルを再生成する必要があります。

ステップ 1　コマンドライン インターフェイスにログインします。

ステップ 2　パブリッシャ ノードで **utils ctl update CTLfile** コマンドを実行します。

サービスの再起動

暗号化された TFTP 設定ファイルの更新を完了したら、Cisco TFTP サービスと Cisco CallManager サービスを再起動して変更を有効にしてください。

ステップ 1　[Cisco Unified Serviceability] から選択します。**[ツール（Tools）] > [コントロールセンター - 機能サービス（Control Center - Feature Services）]**

ステップ 2　次の 2 つのサービスを選択します。

- Cisco CallManager
- Cisco TFTP

ステップ 3　[再起動（Restart）] をクリックします。ただし、CallManager 証明書を再生成または更新した後は、TFTP サービスを手動で再起動する必要はありません。

電話のリセット

すべての暗号化された TFTP 設定ファイルの更新が完了したら、電話機をリセットしてください。

ステップ 1 [Cisco Unified CM Administration] から、**[デバイス（Device）] > [電話（Phones）]** を選択します。
ステップ 2 [検索（Find）] をクリックします。
ステップ 3 [すべて選択（Select All）] をクリックします。
ステップ 4 [選択をリセットする（Reset selected）] をクリックします。

暗号化された TFTP 設定ファイルの無効化

警告 TFTP 暗号化設定が **[False]** であるが、SIP を実行している電話でダイジェスト認証が **[True]** に設定されている場合、ダイジェストログイン情報がクリアテキストで送信される可能性があります。

設定を更新した後、電話機の暗号キーは Unified Communications Manager データベースに残ります。

Cisco Unified IP Phone7911G、7931G（SCCP のみ）、7941G、7941G-GE、7942G、7945G、7961G、7961G-GE、 7962G、7965G、7971G および 7975G は暗号化ファイル（.enc、.sgn ファイル）を要求します。暗号化設定が **False** に更新された場合は、電話は暗号化されていない、署名されたファイル（.sgn ファイル）を要求します。

Cisco Unified IP Phone は、SCCP および SIP 上で実行されている場合に、暗号化設定が **False**に更新されると、暗号化されたファイルを要求します。次回リセットされたときに電話が暗号化されていない設定ファイルを要求するように設定するには、電話の GUI から対称キーを削除します。

- Cisco Unified IP PhoneSCCP で実行される Cisco Unified IP 電話 は、6901、6911、6921、6941、6945、6961、7906G、7911G、7921G、7925G、7925G-EX、7926G、7931G、7940G、7941G、7941G-GE、7942G、7945G、7960G、7961G、7961G-GE、7962G、7965G、7970G、7971G、7971G-GE、7975G、8941、8945 です。
- Cisco Unified IP PhoneSIP で実行される Cisco Unified IP 電話 は、6901、6911、6921、6941、6945、6961、7906G、7911G、7941G、7941G-GE、7942G、7961G、7961G、7962G、7965G、7970G、7971G、7971G-GE、7975G、8941、8945、8961、9971、7811、78321、7841、7861、7832、8811、8841、8845、8851、8851NR、8861、8865、8865NE、8821、8831、8832、8832NR です。

手順

	コマンドまたはアクション	目的
ステップ 1	電話機設定ファイルの暗号化を無効にするには、電話機に関連付けられている電話機のセキュリティプ	

	コマンドまたはアクション	目的
	ロファイルの [TFTP 暗号化設定（TFTP Encrypted Config）] チェックボックスをオフにします。	
ステップ 2	Cisco Unified IP Phone 7942 および 7962（SIP のみ）の場合は、電話画面で対称キーのキー値として「32-byte 0」を入力して暗号化を無効にします。	
ステップ 3	Cisco Unified IP Phone（SIP のみ）の場合は、電話画面で対称キー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、使用している電話のモデルに対応する電話のアドミニストレーションガイドを参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。