電話機のセキュリティ

この章では、電話機のセキュリティについて説明します。

電話のセキュリティの概要

インストール時に、Unified Communications Manager は非セキュア モードで起動します。Unified Communications Manager のインストール後に電話が起動すると、すべてのデバイスは Unified Communications Manager に非セキュアとして登録されます。

Unified Communications Manager 4.0(1) 以降のリリースからアップグレードすると、電話はアップグレード前に有効にしたデバイスのセキュリティ モードで起動します。すべてのデバイスは選択したセキュリティ モードを使用して登録されます。

Unified Communications Manager のインストール時に、自己署名証明書が Unified Communications Manager および TFTP サーバで作成されます。また、自己署名証明書ではなくサードパーティの CA 署名付き証明書を Unified Communications Manager に使用するように選択できます。認証後、Unified Communications Manager は証明書を使ってサポートしているCisco Unified IP 電話 を認証します。証明書が Unified Communications Manager および TFTP サーバに存在する場合は、Unified Communications Managerはそれぞれの Unified Communications Managerアップグレードで証明書を再発行しません。新しい証明書エントリを含む新しいCTL ファイルを作成する必要があります。

ヒント　サポートされていない、または非セキュアなシナリオについては、連携動作と制限事項に関連するトピックを参照してください。

Unified Communications Manager はデバイス レベルで認証と暗号化のステータスを維持しています。コールに関係するすべてのデバイスがセキュアとして登録されている場合、コールステータスはセキュアとして登録されます。一方のデバイスが非セキュアとして登録されている場合、発信者または受信者の電話機がセキュアとして登録されていても、コールは非セキュアとして登録されます。

ユーザが Cisco Extension Mobility（EM; エクステンション モビリティ）を使用する場合、Unified Communications Manager はデバイスの認証ステータスと暗号化ステータスを保持します。Unified Communications Manager は、共有回線が設定される場合にもデバイスの認証ステータスおよび暗号化ステータスを保持します。

ヒント　暗号化された Cisco IP 電話 に対して共有回線を設定するときには、回線を共有するすべてのデバイスで暗号化を設定します。つまり、暗号化をサポートするセキュリティ プロファイルを適用することで、すべてのデバイスのデバイス セキュリティ モードを暗号化に設定します。

関連トピック

連携動作と制限事項

信頼できるデバイス

Unified Communications Manager では Cisco IP 電話 の電話モデルによってセキュリティ アイコンを有効にできます。セキュリティ アイコンは、コールがセキュアであるかどうか、接続されたデバイスが信頼できるかどうかを示します。

信頼できるデバイスとは、シスコ製デバイスか、シスコの信頼される接続のセキュリティ基準に合格したサードパーティ製デバイスを表します。これには、シグナリングおよびメディア暗号化、プラットフォーム ハードニング、保証などがあります。デバイスが信頼できる場合、セキュリティ アイコンが表示され、サポートされるデバイスでセキュア トーンが再生されます。さらに、デバイスはセキュア コールに関係する他の機能やインジケータも備えていることがあります。

デバイスをシステムに追加すると、Unified Communications Manager はデバイスが信頼できるかどうかを判断します。セキュリティ アイコンは情報目的でだけ表示され、管理者は直接設定できません。

Unified Communications Manager はアイコンおよびメッセージを Unified Communications Manager Administration に表示することでゲートウェイが信頼できるかを示します。

このセクションでは、Cisco IP 電話 および Unified Communications Manager Administration の両方での信頼できるデバイスのセキュリティ アイコンの動作について説明します。

Cisco Unified Communications Manager の管理

[Unified Communications Manager Administration] の次のウィンドウには、デバイスが信頼されているかどうかが表示されます。

[Gateway Configuration]

ゲートウェイ タイプごとに、[Gateway Configuration] ウィンドウ（**[Device]** > **[Gateway]**）には、[Device Is Trusted] または [Device Is Not Trusted] と対応するアイコンが表示されます。

システムはデバイス タイプに基づいて、デバイスが信頼できるかどうかを判断します。ユーザはデバイスが信頼できるかどうかを設定できません。

電話の設定

電話デバイス タイプごとに、[Phone Configuration] ウィンドウ（**[Device]** > **[Phone]**）に [Device Is Trusted] または [Device Is Not Trusted] と対応するアイコンが表示されます。

システムはデバイス タイプに基づいて、デバイスが信頼できるかどうかを判断します。ユーザはデバイスが信頼できるかどうかを設定できません。

デバイスが信頼決定基準と呼ばれる

ユーザがコールするデバイスのタイプは、電話に表示されるセキュリティ アイコンに影響します。システムは次の 3 つの基準に基づいて、コールがセキュアであるかどうかを判定します。

- コールのすべてのデバイスが信頼できるか。
- シグナリングはセキュア（認証されていて暗号化されている）か。
- メディアはセキュアか。

サポート対象の Cisco Unified IP 電話 にロック セキュリティ アイコンが表示される前に、これら 3 つの基準がすべて満たされている必要があることに注意してください。信頼できないデバイスを含むコールでは、シグナリングおよびメディアのセキュリティに関係なく、コール全体のステータスはセキュアでないままで、電話機にロック アイコンが表示されません。たとえば、会議で信頼できないデバイスを含めた場合、システムは、そのコール レッグと会議自体をセキュアでないものと見なします。

電話機モデルのサポート

Unified Communications Manager でセキュリティをサポートする電話モデルは、セキュアなシスコの電話とセキュアな推奨ベンダーの電話という 2 つのカテゴリに分類されます。セキュアなシスコの電話機には、製造元でインストールされる証明書 (MIC) が事前にインストールされており、認証局プロキシ機能 (CAPF) を使用してローカルで有効な証明書 (LSC) の自動生成と交換をサポートしています。セキュアなシスコの電話機は、追加の証明書の管理なしで MIC を使用して Cisco ユニファイド CM に登録できます。セキュリティを強化するために、CAPF を使用して電話機に

LSC を作成してインストールすることができます。詳細については、電話セキュリティのセットアップと設定に関連するトピックを参照してください。

セキュアな推奨ベンダーの電話機には、MIC が事前にインストールされておらず、LSCs を生成するための CAPF がサポートされていません。セキュアな推奨ベンダーの電話機が Cisco ユニファイド CM に接続するためには、デバイスに証明書を提供するか、デバイスによって生成される必要があります。電話機のサプライヤは、電話機の証明書を取得または生成する方法の詳細を提供する必要があります。証明書を取得したら、OS 管理証明書管理インターフェイスを使用して Cisco ユニファイド CM に証明書をアップロードする必要があります。詳細については、推奨ベンダーの SIP 電話のセキュリティ設定に関連するトピックを参照してください。

お使いの電話でサポートされるセキュリティ機能のリストについては、この Unified Communications Manager リリースに対応した電話管理およびユーザ マニュアル、またはファームウェア ロードに対応したファームウェアのマニュアルを参照してください。

また、シスコのユニファイドレポートを使用して、特定の機能をサポートしている電話機を一覧表示することもできます。Cisco Unified Reporting の詳細については、『Cisco Unified Reporting Administration Guide』を参照してください。

関連トピック

電話機のセキュリティの設定, on page 6
推奨ベンダーの SIP 電話セキュリティのセットアップ, on page 4
電話機のセキュリティ設定の表示, on page 6

推奨ベンダーの SIP 電話セキュリティのセットアップ

推奨ベンダーのセキュアな電話とは、サードパーティ ベンダーによって製造されているが、COP ファイルを使用して Cisco Unified データベースにインストールされている電話です。推奨ベンダーの SIP 電話のセキュリティは、Unified Communications Manager が提供しています。セキュリティをサポートするためには、COP ファイル内の推奨ベンダーの SIP 電話のセキュリティ暗号化またはセキュリティ認証を有効にする必要があります。これらの電話タイプは、[新しい電話の追加(Add a New Phone)] ウィンドウのドロップダウンリストに表示されます。すべての推奨ベンダーの電話はダイジェスト認証をサポートしていますが、すべての推奨ベンダーの電話が TLS セキュリティをサポートするわけではありません。セキュリティ機能は、電話機のモデルに基づいています。電話セキュリティプロファイルに 「[Device Security Mode]」 フィールドが含まれる場合、電話は TLS をサポートしています。

推奨ベンダーの電話機が TLS セキュリティをサポートしている場合は、デバイスごとの証明書と共有証明書の2つのモードが考えられます。電話機のサプライヤは、電話機に適用されるモード、および電話機の証明書の生成または取得の手順を指定する必要があります。

推奨ベンダーの SIP 電話セキュリティプロファイルのデバイスごとの証明書の設定

デバイスごとの証明書を使用して推奨ベンダーの SIP 電話セキュリティプロファイルを設定するには、次の手順を実行します。

手順

Step 1 OS 管理証明書管理インターフェイスを使用して、各電話機の証明書をアップロードします。

Step 2 [Cisco Unified Administration] で、**[System]** > **[Security]** > **[Phone Security Profile]** の順に選択します。

Step 3 この電話のデバイスタイプに対して新しい電話セキュリティプロファイルを設定し、**[デバイスセキュリティモード（Device Security Mode）]** ドロップダウンリストで **[暗号化（Encrypted）]** または **[認証済み（Authenticated）]** を選択します。

Step 4 CCMAdmin インターフェイスで新しい SIP 電話を設定するには、**[デバイス (Device)]** > **[電話 (Phone)]** > **[追加 (Add new]** の順に選択します。

Step 5 [Phone Type] を選択します。

Step 6 必須フィールドに入力します。

Step 7 **[デバイスのセキュリティプロファイル（Device Security Profile）]** ドロップダウンリストで、作成したプロファイルを選択します。

推奨ベンダーのSIP電話セキュリティプロファイルの共有証明書のセットアップ

共有証明書を使用して推奨ベンダーの SIP 電話セキュリティプロファイルを設定するには、次の手順を実行します。

手順

Step 1 電話機のベンダーの指示を使用して、サブジェクト代替名 (SAN) 文字列を使用して証明書を生成します。SAN のタイプは DNS である必要があります。この手順で指定した SAN をメモしておきます。たとえば、X509v3 extensions の場合は次のようになります。

- サブジェクト代替名
- DNS:AscomGroup01.acme.com

（注） SAN は DNS タイプである必要があります。または、セキュリティが有効になっていません。

Step 2 OS 管理証明書管理インターフェイスを使用して、共有証明書をアップロードします。

Step 3 [Cisco Unified Administration] で、**[System]** > **[Security]** > **[Phone Security Profile]** の順に選択します。

Step 4 **[名前 (name)]** フィールドにサブジェクト代替名 (san) の名前を入力します。これは、優先ベンダーから提供された証明書の名前です。または、san がない場合は、証明書名を入力します。

（注） セキュリティプロファイルの名前は、証明書のSANと完全に一致する必要があります。そうしないと、セキュリティが有効になりません。

Step 5 **[デバイスセキュリティモード（Device Security Mode）]** ドロップダウンリストで、**[暗号化（Encrypted）]** または **[認証済み（Authenticated）]** を選択します。

Step 6 [転送タイプ（Transport type）] ドロップダウンリストで、**[TLS]** を選択します。

Step 7 CCMAdmin インターフェイスで新しい SIP 電話を設定するには、**[デバイス (Device)]** > **[電話 (Phone)]** > **[追加 (Add new]** の順に選択します。

Step 8 [Phone Type] を選択します。

Step 9 各必須フィールドに入力します

Step 10 **[デバイスのセキュリティプロファイル（Device Security Profile）]** ドロップダウンリストで、作成したプロファイルを選択します。

関連トピック

電話セキュリティ プロファイルの設定

電話機のセキュリティ設定の表示

セキュリティをサポートする電話機の特定のセキュリティ関連の設定を構成して表示することができます。たとえば、電話機にローカルで有効な証明書または製造元でインストールされた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。セキュアメニューと アイコンの詳細については、ご使用の電話モデルに対応する*Cisco IP* 電話 の管理ガイド および *Cisco IP* 電話 ユーザ ガイドを参照してください。

Unified Communications Manager がコールを認証済みまたは暗号化済みと分類すると、コール状態を示すアイコンが電話に表示されます。Unified Communications Manager がどの時点でコールを認証済みまたは暗号化済みとして分類するかも決定します。

関連トピック

連携動作と制限事項
セキュリティ アイコン

電話機のセキュリティの設定

次の手順では、サポートされている電話のセキュリティを設定するタスクについて説明します。

手順

Step 1 まだ設定していない場合は、Cisco CTL クライアントを設定し、Unified Communications Manager セキュリティモードが混合モードであることを確認します。

Step 2 電話機に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た証明書 (MIC) が含まれていない場合は、Certificate Authority Proxy Function (CAPF) を使用して LSC をインストールします。

Step 3 電話セキュリティ プロファイルを設定します。

Step 4 電話に電話セキュリティ プロファイルを適用します。

Step 5 ダイジェストクレデンシャルを設定した後、[電話の設定 (Phone Configuration)] ウィンドウからダイジェストユーザを選択します。

Step 6 Cisco Unified IP 電話 7962 または 7942（SIP のみ）で、[エンドユーザ設定（End User Configuration）] ウィンドウで設定したダイジェスト認証のユーザ名とパスワード（ダイジェストログイン情報）を入力します。

（注） このドキュメントでは、電話へのダイジェスト認証クレデンシャルの入力方法は説明していません。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『*Cisco IP* 電話アドミニストレーション ガイド』を参照してください。

このドキュメントでは、電話へのダイジェスト認証クレデンシャルの入力方法は説明していません。このタスクの実行方法については、お使いの電話機モデルをサポートする Cisco Unified Communications Manager アドミニストレーション ガイド およびこのバージョンの Unified Communications Manager を参照してください。

Step 7 電話機がこの機能をサポートしている場合は、電話機の設定ファイルを暗号化します。

Step 8 電話機を強化するには、電話機の設定を無効にします。

関連トピック

- 電話機へのセキュリティ プロファイルの適用
- Certificate Authority Proxy Function
- Cisco CTL クライアントの設定
- 暗号化された電話設定ファイルの設定
- エンドユーザのダイジェストクレデンシャルの設定
- 電話のセキュリティ強化
- 電話セキュリティ プロファイルの設定
- 電話ユーザへのダイジェストクレデンシャルの割り当て
- 電話機へのダイジェスト認証の割り当て

電話セキュリティの連携動作と制限事項

ここでは、電話機のセキュリティに関する対話と制限について説明します。

表 *1:* 電話セキュリティの連携動作と制限事項

機能	連携動作および制限事項
証明書の暗号化	Unified Communications Manager リリース 11.5(1) SU1 から、CAPF サービスで発行されるすべての LSC 証明書は SHA-256 アルゴリズムで署名されます。したがって、Cisco Unified IP 電話 7900 シリーズ、8900 シリーズ、および 9900 シリーズは、SHA-256 で署名された LSC 証明書および外部 SHA2 アイデンティティ証明書（Tomcat、CallManager、CAPF、TVS など）をサポートします。署名の検証が必要な、その他の暗号化の操作では、SHA-1 のみがサポートされます。 （注） ソフトウェアメンテナンスが終了した電話モデルまたはサポート終了電話モデルを使用する場合は、Unified Communications Manager11.5(1)SU1 リリースより前のバージョンを使用することを推奨します。

電話機のセキュリティに関する詳細情報の入手先

関連するシスコのドキュメント

- 『*Administration Guide for Cisco Unified Communications Manager*』
- 『*Cisco Unified Communications Manager*のトラブルシューティングガイド』

関連トピック

連携動作と制限事項
認証、整合性、および許可
暗号化
認証と暗号化のセットアップ
Certificate Authority Proxy Function
電話機のセキュリティの設定, on page 6
電話セキュリティ プロファイルの設定
暗号化された電話設定ファイルの設定
電話のセキュリティ強化

TFTP OAuth の概要

この機能により、Unified Communications Manager のセキュリティが強化されます。セキュリティを向上させるために、Unified Communications Manager は SIP OAuth 対応の電話機をチェックし、TFTP OAuth を使用して設定ファイル要求を認証および承認します。Unified Communications Manager

は、エンドポイントによって提示されたトークンを確認し、有効なものだけにコンフィギュレーションファイルを提供します。

TFTP OAuth は次をサポートします。

- TFTP ファイルのダウンロードは、認証された電話に対してのみ、セキュリティで保護されたポートを介して行われていることを確認します。
- CAPF 操作は、セキュアなファイル転送には必須ではありません。

次の電話機モデルは、TFTP OAuth をサポートしています。

- 7811
- 7821
- 7832
- 7841
- 7861
- 8811
- 8832
- 8841
- 8845
- 8851
- 8851NR
- 8861
- 8865
- 8865NR

TFTP OAuth タスクフロー

始める前に

- Cisco CallManager エンタープライズパラメータの **[クラスタ SIPOAuth モード（Cluster SIPOAuth Mode）]** フィールドが **[有効（Enabled）]** に設定されていることを確認します。CLI から SIP OAuth を有効にする方法の詳細については、「SIP OAuth Configuration through CLI」を参照してください。

手順

	コマンドまたはアクション	目的
Step 1	電話セキュリティプロファイルでデバイスセキュリティモードを設定する	電話セキュリティプロファイルでデバイスセキュリティモードを設定します。
Step 2	Phone Edge TrustへのCA証明書のアップロード	CA 証明書は、Cisco Tomcat 証明書を Phone Edge Trust に発行するために使用されます。

電話セキュリティプロファイルでデバイスセキュリティモードを設定する

この手順を使用して、電話機のセキュリティプロファイルで**デバイスセキュリティモード（Device Security Mode）**を設定します。これは、その電話機の**[電話機のセキュリティプロファイル（Phone Security Profile）]**内でデバイスセキュリティモードを**[暗号化（Encrypted）]**に設定している場合にのみ必要です。

手順

Step 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、**[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）]** の順に選択します。

Step 2 次のいずれかを実行します。

- 既存の電話セキュリティプロファイルを検索する
- [新規追加（Add New）] をクリックします。

Step 3 [電話セキュリティプロファイル情報（Phone Security Profile Information）] セクションの **[デバイスセキュリティモード（Device Security Mode）]** ドロップダウンリストから、**[暗号化（Encrypted）]** を選択します。

Step 4 **[転送タイプ（Transport type）]** ドロップダウンリストで、**[TLS]** を選択します。

Step 5 [OAuth 認証の有効化（Enable OAuth Authentication）] チェックボックスをオンにします。

Step 6 **[保存（Save）]** をクリックします。

Step 7 電話セキュリティプロファイルを電話に関連付けます。電話セキュリティ電話を適用する方法の詳細については、Cisco Unified Communications Manager セキュリティ ガイドの「セキュリティプロファイルを電話に適用する」セクションを参照してください。

（注） 変更を有効にするには、スマートフォンをリセットしてください。

（注） [SIP OAuth モード（SIP OAuth Mode）] が有効な場合、**[ダイジェスト認証を有効化（Enable Digest Authentication）]** および **[TFTP 暗号化設定（TFTP Encrypted Config）]** オプションはサポートされません。電話機は、**https(6971)**を介して TFTP 設定ファイルを安全にダウンロードし、認証にトークンを使用します。

Phone Edge TrustへのCA証明書のアップロード

この手順を使用して、Tomcat 署名付き証明書のルート証明書を Phone EdgeTrust にアップロードします。

（注） この手順は Cisco Phone に対してのみ実行され、Cisco Jabber には適用されません。

手順

Step 1 Cisco Unified OS の管理から、**[セキュリティ（Security）]** > **[証明書の管理（Certificate Management）]** を選択します。

Step 2 [Upload Certificate/Certificate chain] をクリックします。

Step 3 **[証明書/証明書チェーンのアップロード]** ウィンドウで、**[証明書の目的]** ドロップダウンリストから **[電話-エッジ-信頼]** を選択します。

Step 4 **[ファイルのアップロード]** フィールドで、**[参照]** をクリックして証明書をアップロードします。

Step 5 [アップロード（Upload）] をクリックします。