電話のセキュリティ

この章では、電話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 Phone 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で新しい 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シナリオまたは安全でないシナリオについては、連携動作と制限事項に関連する項目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ると、コール ステータスはセキュアとして登録されます。1 つのデバイスが非セキュアとして登録されると、発信者または受信者の電話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 Phone 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。

信頼できるデバイス

Unified Communications Manager では Cisco IP Phone 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 Phone 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 Administration

[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。

[Phone Configuration]

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。

コールしたデバイスの信頼判定基準

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断します。

- 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。

サポートされる Cisco IP Phone にロック セキュリティ アイコンが表示される前に、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が関与するコールでは、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非セキュアなままで、電話機にロック アイコンが表示されません。たとえば、会議に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非セキュアと見なします。

電話モデルのサポート

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には、製造元でインストールされる証明書（MIC ）がプリインストールされ、Certificate Authority Proxy Function（CAPF）を使用した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ます。セキュアなシスコの電話は、追加の証明書の管理なしで MIC を使用して Cisco Unified CM に登録できます。セキュリティ強化のために、CAPF を使用して

LSC を作成し、電話にインストールできます。詳細については、電話のセキュリティ設定とセットアップの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には MIC がプリインストールされていないので、LSC の作成で CAPF をサポートしません。セキュアな推奨ベンダーの電話が Cisco Unified CM に接続するには、証明書がデバイスにあるか、デバイスによって生成される必要があります。電話のサプライヤが、電話の証明書を取得または生成する方法についての詳細を提供する必要があります。証明書を入手したら、OS 管理者証明書の管理インターフェイスを使用して、Cisco Unified 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 セットアップに関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。

Cisco Unified Reporting を使用して特定の機能をサポートする電話をリスト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。

推奨ベンダーの SIP 電話のセキュリティ設定

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には、COP ファイルで、推奨ベンダーの SIP 電話のセキュリティ暗号化および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 [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。ダイジェスト認証はすべての推奨ベンダーの電話でサポートされていますが、TLS セキュリティはすべての推奨ベンダーの電話でサポートされているわけではありません。セキュリティ機能は電話のモデルにより異なります。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が TLS セキュリティをサポートしている場合は、デバイス別の証明書と共有証明書の 2 つのモードが可能です。電話のサプライヤは電話で使用できるモードを指定し、証明書の生成または取得の手順を提供する必要があります。

デバイス別の証明書による推奨ベンダーの SIP 電話セキュリティ プロファイルのセットアップ

デバイス別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

ステップ 1 OS管理の証明書管理インターフェイスを使用して、電話ごとに証明書をアップロードします。

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

ステップ 3 この電話のデバイス タイプの新しい電話セキュリティ プロファイルを設定し、[Device Security Mode] ドロップダウン リスト ボックスで [Encrypted] または [Authenticated] を選択します。

ステップ 4 CCMAdmin インターフェイスで新しい SIP 電話を設定するには、**[Device]** > **[Phone]** > **[Add New]** の順に選択します。

ステップ 5 [Phone Type] を選択します。

ステップ 6 必須フィールドに入力します。

ステップ 7 [Device Security Profile] ドロップダウン リスト ボックスで、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設定

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

ステップ 1 電話のベンダーの手順を使用して、サブジェクト代替名（SAN）の文字列を指定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 拡張の場合、次のようになります。

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

（注） SAN のタイプは DNS である必要があります。そうでない場合、セキュリティは有効になりません。

ステップ 2 OS 管理の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。

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

ステップ 4 [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、推奨ベンダーによって提供される証明書上の名前です。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 と正確に一致している必要があります。一致しない場合、セキュリティは有効になりません。

ステップ 5 [Device Security Mode] ドロップダウン リスト ボックスで、[Encrypted] または [Authenticated] を選択します。

ステップ 6 [Transport type] ドロップダウン リスト ボックスで、[TLS] を選択します。

ステップ 7 CCMAdmin インターフェイスで新しい SIP 電話を設定するには、**[Device]** > **[Phone]** > **[Add New]** の順に選択します。

ステップ 8 [Phone Type] を選択します。

ステップ 9 各必須フィールドに入力します

ステップ 10 [Device Security Profile] ドロップダウン リスト ボックスで、作成したプロファイルを選択します。

電話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の特定のセキュリティ関連項目の設定とその確認を行うことができます。たとえば、電話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る証明書（MIC）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 Phone Administration Guide*』および『*Cisco IP Phone User Guide*』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。

電話のセキュリティの設定

ここでは、サポートされている電話のセキュリティを設定する作業を説明します。

手順

ステップ 1 Cisco CTL クライアントが設定されていない場合はこれを設定し、Unified Communications Manager のセキュリティ モードが混合モードであることを確認します。

ステップ 2 電話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る証明書（MIC）がない場合は、Certificate Authority Proxy Function（CAPF）を使用して LSC をインストールします。

ステップ 3 電話セキュリティ プロファイルを設定します。

ステップ 4 電話に電話セキュリティ プロファイルを適用します。

ステップ 5 ダイジェスト クレデンシャルを設定した後、[Phone Configuration] ウィンドウでダイジェスト ユーザを選択してください。

ステップ 6 Cisco Unified IP Phone 7962 および 7942（SIP のみ）では、[End User Configuration] ウィンドウで設定したダイジェスト認証ユーザ名とパスワード（ダイジェストクレデンシャル）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 Phone Administration Guide*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。電話に認証名とパスワードを入力する方法については、ご使用の電話とバージョンの Unified Communications Manager に対応した『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

ステップ 7 電話設定ファイルを暗号化します（暗号化機能をもつ電話のみ）。

ステップ 8 電話のセキュリティをより強化するには、電話設定を無効にします。

電話セキュリティの連携動作と制限事項

このセクションでは、電話セキュリティの連携動作と制限を示します。

機能	連携動作および制限事項
証明書の暗号化	Cisco Unified Communications Manager リリース 11.5(1)SU1 以降、CAPF サービスによって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ています。したがって、Cisco Unified IP 電話 7900 シリーズ、8900 シリーズ、および 9900 シリーズのモデルは、SHA-256 署名済み 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またはサポートが終了した電話モデルを使用する場合は、Unified Communications Manager の 11.5(1)SU1 より前のリリースの使用を強くお勧めします。

電話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』