電話機のセキュリティ

電話のセキュリティの概要

インストール時は、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、電話機を起動すると、デバイスはすべて非セキュアとして Unified Communications Manager に登録されます。

Unified Communications Manager 4.0(1) 以降のリリースからアップグレードした後は、アップグレード前に有効にしたデバイスセキュリティモードで電話機が起動します。デバイスはすべて、選択されたセキュリティモードを使用して登録されます。

Unified Communications Manager をインストールすると、Unified Communications Manager および TFTP サーバに自己署名証明書が作成されます。自己署名証明書ではなく、Unified Communications Manager のサードパーティの CA 署名付き証明書を使用することもできます。認証を設定した後、Unified Communications Manager は、証明書を使用して、サポートされている Cisco Unified IP Phone で認証します。Unified Communications Manager および TFTP サーバに証明書が存在した後、Unified Communications Manager は各 Unified Communications Manager アップグレード中に証明書を再発行しません。CLI コマンド **ctl update CTLFile** を使用して、ctl ファイルを新しい証明書エントリで更新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 は認証および暗号化のステータスをデバイスレベルで維持します。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。

Unified Communications Manager では、ユーザが Cisco Extension Mobility を使用している場合、デバイスの認証と暗号化のステータスは保持されます。また、Unified Communications Manager では、共有回線が設定されている場合、デバイスの認証と暗号化のステータスも保持されます。

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。

電話機のセキュリティ強化の概要

このセクションでは、Gratuitous ARP 無効化、Web アクセス無効化、PC 音声 VLAN アクセス無効化、アクセス無効化設定、PC ポート無効化など、電話機のセキュリティ強化動作の概要を説明します。

Cisco IP 電話への接続のセキュリティを強化するために、次のオプション設定を使用します。これらの設定は、[電話機の設定（Phone Configuration）] ウィンドウの [プロダクト固有の設定（Product Specific Configuration Layout）] に表示 されます。

これらを企業全体の一連の電話機またはすべての電話機に適用するには、[共通電話プロファイルの設定（Common Phone Profile Configuration）] ウィンドウおよび [エンタープライズ電話の設定（Enterprise Phone Configuration）] にもこれらの設定が表示されます。

表 *1:* 電話機のセキュリティ強化の動作

電話機のセキュリティ強化の動作	説明	
Gratuitous ARP の無効化	デフォルトでは、Cisco Unified IP 電話 s は ARP パケットを受け入れます。デバイスが使用する Gratuitous ARP パケットは、ネットワークにデバイスの存在を公表するために使用されます。ただし、攻撃者はこれらのパケットを使用して、有効なネットワークデバイスをスプーフィングすることができます。たとえば、攻撃者は、デフォルトルータであると主張するパケットを送信する可能性があります。これを選択した場合は、[**電話の設定 (Phone Configuration**)] ウィンドウで、無償 ARP を無効にすることができます。 （**注**） この機能を無効にしても、電話機がデフォルトルータを特定することはできません。	

電話機のセキュリティ強化の動作	説明	
Web アクセスの無効化	電話の Web サーバ機能を無効にすると、統計および設定情報を提供する電話内部の Web ページへのアクセスがブロックされます。Cisco Quality Report Tool などの機能は、電話の Web ページにアクセスしないと正しく動作しません。また、Web サーバを無効にすると、CiscoWorks など、Web アクセスに依存するサービスアビリティ アプリケーションにも影響します。 Web サービスが無効になっているかどうかを確認するために、電話機は設定ファイルのパラメータを解析して、サービスが無効になっているか、有効になっているかを示します。Web サービスが無効になっている場合、電話機はモニタリング目的で HTTP ポート80を開かず、電話機の内部 web ページへのアクセスをブロックします。	

電話機のセキュリティ強化の動作	説明	
PC 音声 VLAN へのアクセスの無効化	デフォルトでは、Cisco IP 電話はスイッチ ポート（上流に位置するスイッチに面したポート）で受信したすべてのパケットを PC ポートに転送します。[Phone Configuration] ウィンドウの [PC Voice VLAN Access] 設定を無効にすると、PC ポートから受信した音声 VLAN 機能を使用するパケットはドロップされます。さまざまな Cisco IP 電話 がそれぞれ異なる方法でこの機能を使用しています。 • Cisco Unified IP 電話 7942 と 7962 は、PC ポートで送受信される、音声 VLAN のタグが付いたパケットをドロップします。 • Cisco Unified IP 電話 7970G は、PC ポートで送受信される、VLAN で 802.1Q のタグが含まれるすべてのパケットをドロップします。	

電話機のセキュリティ強化の動作	説明	
アクセスの無効化の設定	デフォルトでは、Cisco IP 電話の [Applications] ボタンを押すと、電話の設定情報を含むさまざまな情報にアクセスできます。[Phone Configuration] ウィンドウで [Setting Access] パラメータ設定を無効にすると、通常は電話の [Applications] ボタンを押すと表示されるすべてのオプション（[Contrast]、[Ring Type]、[Network Configuration]、[Model Information]、[Status] などの設定）へのアクセスが拒否されます。 Unified Communications Manager Administration 内の設定を無効にすると、以前の設定は電話に表示されません。この設定を無効にすると、電話ユーザは [音量 (Volume)] ボタンに関連付けられている設定を保存できません。たとえば、ユーザはボリュームを保存できません。 この設定を無効にすると、現在のコントラスト、呼出音タイプ、ネットワーク設定、モデル情報、ステータス、および電話機に存在するボリューム設定が自動的に保存されます。これらの電話機設定を変更するには、Unified Communications Manager Administration で [設定へのアクセス（Setting Access）] 設定を有効にします。	

電話機のセキュリティ強化の動作	説明	
PC ポートのディセーブル化	デフォルトでは、Unified Communications Manager は PC ポートを備えているすべての Cisco IP 電話 で PC ポートを有効にします。これを選択した場合は、[電話の設定 (Phone Configuration)] ウィンドウで [PC ポート (PC Port)] 設定を無効にすることができます。PC ポートを無効にすると、ロビーまたは会議室の電話機で役立ちます。 （注） PC ポートは一部の電話機で使用でき、ユーザは電話機にコンピュータを接続できます。この接続方法は、ユーザが 1 つの LAN ポートだけを必要とすることを意味します。	

電話のセキュリティ強化の設定

電話のセキュリティ強化は、接続のセキュリティを強化するために電話機に適用できるオプションの設定で構成されています。次の3つの設定ウィンドウのいずれかを使用して設定を適用できます。

- 電話の設定 - [電話の設定（Phone Configuration）] ウィンドウを使用して、個々の電話に設定を適用します。
- 共通の電話プロファイル - [共通の電話プロファイル（Common Phone Profile）] ウィンドウを使用して、このプロファイルを使用するすべての電話機に設定を適用します。
- 企業電話 - [企業電話（Enterprise Phone）] ウィンドウを使用して、企業全体のすべての電話機に設定を適用します。

（注） これらの各ウィンドウに競合する設定が表示される場合、電話が正しい設定を判断するために使用する優先順位は次のとおりです。1) 電話の設定、2) 共通の電話プロファイル、3) 企業電話。

電話のセキュリティ強化を設定するには、次の手順を実行します。

ステップ 1 Cisco Unified Communications Manager Administrationから、**[デバイス（Device）]** > **[電話（Phone）]** を選択します。

ステップ 2 電話機の検索条件を指定して [**検索（Find**）] をクリックし、すべての電話機を表示します。

ステップ 3 デバイス名をクリックします。

ステップ 4 次の製品固有のパラメータを見つけます。

a) [PC ポート（PC Port）]
b) [設定アクセス（Settings Access）]
c) [無償 ARP（Gratuitous ARP）]
d) [PC の音声 VLAN へのアクセス（PC Voice VLAN Access）]
e) [Web アクセス（Web Access）]

ヒント これらの設定の情報を確認するには、[**電話の設定 (Phone Configuration**)] ウィンドウのパラメータの横に表示される [ヘルプ (help)] アイコンをクリックします。

ステップ 5 無効にする各パラメータのドロップダウンリストから、[**無効 (Disabled**)] を選択します。スピーカフォンまたはスピーカフォンとヘッドセットを無効にするには、対応するチェックボックスをオンにします。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 [リセット（Reset）] をクリックします。

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。

[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。

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 Phone 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。

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。

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。

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、**utils ctl** CLI コマンドを実行し、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。

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、[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。

ステップ 6 Cisco Unified IP Phone 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。

サードパーティの CA 署名付き証明書をプラットフォームにアップロードした後、**utils ctl** CLI コマンドセットを実行して CTL ファイルを更新する必要があります。

ステップ 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。

ステップ 8 電話機を強化するには、電話機の設定を無効にします。

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。

ステップ 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。

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。

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、**[デバイス (Device)]** > **[電話 (Phone)]** > **[追加 (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 **[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。

ステップ 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。

ステップ 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。

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 **[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。

ステップ 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。

ステップ 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。

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、**[デバイス (Device)]** > **[電話 (Phone)]** > **[追加 (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 **[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。

クラスタ間での電話の移行

クラスタ間で電話を移動するには、次の手順に従ってください。たとえば、クラスタ 1 からクラスタ 2 に移動するとします。

ステップ 1 クラスタ 2 で、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。

ステップ 2 [検索（Find）] をクリックします。

ステップ 3 証明書の一覧で、ITLRecovery 証明書をクリックし、[.PEM ファイルのダウンロード（Download .PEM File）] または [.DER ファイルのダウンロード（Download .DER File）] のいずれかをクリックすることにより、いずれかのファイル形式の証明書をコンピュータにダウンロードします。
証明書の詳細が表示されます。

ステップ 4 証明書の一覧で、CallManager 証明書をクリックし、[.PEM ファイルのダウンロード（Download .PEM File）] または [.DER ファイルのダウンロード（Download .DER File）] のいずれかをクリックすることにより、いずれかのファイル形式の証明書をコンピュータにダウンロードします。
証明書の詳細が表示されます。

ステップ 5 クラスタ 1 で、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。
[証明書の一覧（Certificate List）] ウィンドウが表示されます。

ステップ 6 [証明書チェーンのアップロード（Upload Certificate Chain）] をクリックすることにより、ダウンロードした証明書をアップロードします。

ステップ 7 [証明書の目的（Certificate Purpose）] ドロップダウン リストで、[電話と SAST 間の信頼（Phone-SAST-trust）] を選択します。

ステップ 8 [ファイルのアップロード（Upload File）] フィールドで、[ファイルの選択（Choose File）] をクリックし、手順 3 でダウンロードした ITLRecovery ファイルを参照し、[ファイルのアップロード（Upload File）] をクリックします。

アップロードされた ITLRecovery ファイルが、クラスタ 1 の [証明書リスト（Certificate List）] ウィンドウで [電話と SAST 間の信頼（Phone-SAST-Trust）] 証明書に対して表示されます。新しい ITL ファイルにクラスタ 2 の ITLRecovery 証明書がある場合は、コマンド `show itl` を実行します。

ステップ 9 クラスターの電話にローカルで有効な証明書（LSC）がある場合、クラスタ 1 からの CAPF 証明書をクラスタ 2 の CAPF 信頼ストアにアップロードしなければなりません。

ステップ 10 （任意） この手順は、クラスタが混合モードの場合にのみ適用可能です。CLI で **utils ctl update CTLFile** コマンドを実行することにより、CTL ファイルをクラスタ 1 で再生成します。

（注）
- `show ctl` CLI コマンドを実行することにより、クラスタ 2 の ITLRecovery 証明書と CallManager 証明書が、SAST としての役割で CTL ファイルに含められるようにします。
- 電話が新しい CTL ファイルおよび ITL ファイルを受け取っていることを確認します。更新された CTL ファイルには、クラスタ 2 の ITLRecovery 証明書が含まれています。

クラスタ 1 からクラスタ 2 に移行する電話が、クラスタ 2 の ITLRecovery 証明書を受け付けるようになります。

ステップ 11 クラスタ間で電話を移行します。

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 *2:* 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 Phone 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。

電話セキュリティプロファイル

Unified Communications Managerで、電話機のタイプとプロトコルのセキュリティ関連の設定をセキュリティプロファイルにグループ分けします。したがって、この 1 つのセキュリティプロファイルを複数の電話機に割り当てることができます。セキュリティ関連の設定には、デバイスセキュリティモード、ダイジェスト認証、いくつかの CAPF 設定などがあります。Unified Communications Manager をインストールすると、自動登録用の事前定義済み非セキュア セキュリティ プロファイルのセットが提供されます。

[電話の設定（Phone Configuration）] ウィンドウでセキュリティ プロファイルを選択することで、構成済みの設定を電話に適用します。電話機のセキュリティ機能を有効にするには、デバイスタイプとプロトコルに応じた新しいセキュリティプロファイルを設定してから、そのプロファイルを電話機に適用する必要があります。選択されたデバイスとプロトコルがサポートするセキュリティ機能のみが、[セキュリティプロファイルの設定（security profile settings）] ウィンドウに表示されます。

前提条件

電話セキュリティプロファイルを設定する前に、次の情報を考慮してください。

- 電話を設定するときは、[**電話の設定（Phone Configuration**）] ウィンドウでセキュリティプロファイルを選択します。デバイスがセキュリティまたはセキュアプロファイルをサポートしていない場合は、非セキュアプロファイルを適用します。

- 事前定義された非セキュアプロファイルを削除または変更することはできません。
- デバイスに現在割り当てられているセキュリティプロファイルは削除できません。
- すでに電話機に割り当てられているセキュリティプロファイルの設定を変更すると、その特定のプロファイルが割り当てられているすべての電話に、再設定された設定が適用されます。
- デバイスに割り当てられているセキュリティファイルの名前を変更できます。以前のプロファイル名と設定で割り当てられた電話機は、新しいプロファイル名と設定を前提としています。
- CAPF 設定、認証モード、およびキーサイズは、[電話の設定 (**Phone Configuration**)] ウィンドウに表示されます。Mic または LSCs に関連する証明書操作の CAPF 設定を構成する必要があります。これらのフィールドは、[電話の**設定 (Phone Configuration**)] ウィンドウで直接更新できます。
- セキュリティプロファイルの CAPF 設定を更新すると、[電話の設定（Phone Configuration）] ウィンドウ上の設定も同様に更新されます。
- [電話の設定（Phone Configuration）] ウィンドウで CAPF 設定を更新し、一致するプロファイルが見つかった場合、Unified Communications Manager は一致するプロファイルを電話機に適用します。
- [電話の設定（Phone Configuration）] ウィンドウで CAPF 設定を更新し、一致するプロファイルが見つからなかった場合、Unified Communications Manager は新しいプロファイルを作成してそのプロファイルを電話機に適用します。
- アップグレード前にデバイス セキュリティ モードを設定済みの場合は、Unified Communications Manager が設定済みのモデルとプロトコルに基づいてプロファイルを作成し、デバイスにそのプロファイルを適用します。
- MIC は LSC のインストール時にのみ使用することを推奨します。シスコでは、Unified Communications Manager との TLS 接続の認証用に LSC をサポートしています。MIC ルート証明書は侵害される可能性があるため、TLS 認証またはその他の目的に MIC を使用するように電話を設定するユーザは、ご自身の責任で行ってください。MIC が侵害された場合シスコはその責任を負いません。
- TLS 接続に LSC を使用するには、Cisco IP 電話 をアップグレードし、互換性の問題を回避するために MIC ルート証明書を CallManager 信頼ストアから削除することを推奨します。

電話セキュリティ プロファイルの設定

次の表では、SCCP を実行している電話のセキュリティ プロファイルに関する設定について説明します。

選択した電話のタイプおよびプロトコルがサポートする設定のみ表示します。

表 *3: SCCP* を実行している電話のセキュリティ プロファイル

設定	説明
名前	セキュリティ プロファイルの名前を入力します。 新しいプロファイルを保存すると、電話タイプとプロトコルの [電話の設定（Phone Configuration）] ウィンドウの [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にその名前が表示されます。 **ヒント** セキュリティ プロファイル名にデバイス モデルとプロトコルを含めると、プロファイルの検索または更新時に正しいプロファイルを検索できます。
[説明（Description）]	セキュリティ プロファイルの説明を入力します。説明には、任意の言語で最大 50 文字を指定できますが、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、バックスラッシュ（\）、山カッコ（<>）は使用できません。

設定	説明
[デバイス セキュリティ モード（Device Security Mode）]	

設定	説明
	ドロップダウンリストから、次のオプションのいずれかを選択します。 • [非セキュア（Non Secure）]：イメージ、ファイル、デバイス認証を除くセキュリティ機能は電話機に存在しません。TCP接続でUnified Communications Manager が利用できます。 • [認証済（Authenticated）]： Unified Communications Managerは電話機の整合性と認証を提供します。NULL/SHA を使用する TLS 接続がシグナリングに対して開きます。 • [暗号化（Encrypted）]：Unified Communications Manager はトランクの整合性、認証、およびシグナリング暗号化を提供します。 説明したように、次の暗号方式がサポートされています。 **TLS暗号方式** このパラメータは、Unified Communications Manager で SIP TLS 接続およびインバウンドの CTI Manager TLS CTI 接続を確立するためにサポートされる暗号を定義します。 最も強力：AES-256 SHA-384 のみ：RSA 優先 • `TLS_ECDHE_RSA with AES256_GCM_SHA384` • `TLS_ECDHE_RSA with AES256_GCM_SHA384` （注） パラメータ [SRTP暗号方式（SRTP Ciphers）] の値を [最も強力 - AEAD AES-256 GCM 暗号のみ（Strongest - AEAD AES-256 GCM cipher only）] に設定することを強くお勧めします。このオプションを選択すると、電話機は認証モードで登録されません。 最も強力：AES-256 SHA-384 のみ：ECDSA 優先 • `TLS_ECDHE_ECDSA with AES256_GCM_SHA384` • `TLS_ECDHE_RSA with AES256_GCM_SHA384` 中 - AES-256 AES-128のみ: RSA優先 （注） パラメータ [SRTP暗号方式（SRTP Ciphers）] の値を [最も強力 - AEAD AES-256 GCM 暗号のみ（Strongest - AEAD AES-256 GCM cipher only）] に設定することを強くお勧めします。このオプションを選択すると、電話機は認証モードで登録されません。 • `TLS_ECDHE_RSA with AES256_GCM_SHA384` • `TLS_ECDHE_ECDSA with AES256_GCM_SHA384` • `TLS_ECDHE_RSA with AES128_GCM_SHA256`

設定	説明
	• TLS_ECDHE_ECDSA with AES128_GCM_SHA256 （注） このオプションを選択した場合、パラメータ [SRTP 暗号方式（SRTP Ciphers）] の値を [最も強力 - AEAD AES-256 GCM 暗号のみ（Strongest - AEAD AES-256 GCM cipher only）] に設定することを強くお勧めします。このオプションを選択すると、電話機は認証モードで登録されません。 中程度：AES-256 AES-128 のみ：ECDSA 優先 • TLS_ECDHE_ECDSA with AES256_GCM_SHA384 • TLS_ECDHE_RSA with AES256_GCM_SHA384 • TLS_ECDHE_ECDSA with AES128_GCM_SHA256 • TLS_ECDHE_RSA with AES128_GCM_SHA256 （注） このオプションを選択した場合、パラメータ [SRTP 暗号方式（SRTP Ciphers）] の値を [最も強力 - AEAD AES-256 GCM 暗号のみ（Strongest - AEAD AES-256 GCM cipher only）] に設定することを強くお勧めします。このオプションを選択すると、電話機は認証モードで登録されません。 すべての暗号方式: RSA優先 • TLS_ECDHE_RSA with AES256_GCM_SHA384 • TLS_ECDHE_ECDSA with AES256_GCM_SHA384 • TLS_ECDHE_RSA with AES128_GCM_SHA256 • TLS_ECDHE_ECDSA with AES128_GCM_SHA256 • TLS_RSA with AES_128_CBC_SHA1 すべての暗号 ECDSA 優先 • TLS_ECDHE_ECDSA with AES256_GCM_SHA384 • TLS_ECDHE_RSA with AES256_GCM_SHA384 • TLS_ECDHE_ECDSA with AES128_GCM_SHA256 • TLS_ECDHE_RSA with AES128_GCM_SHA256

設定	説明
	• TLS_RSA with AES_128_CBC_SHA1 （注） [認証済み（Authenticated）] として選択されている [デバイスセキュリティプロファイル（Device Security Profile）] を使用してトランクを設定した場合、Unified Communications Manager は、NULL_SHA 暗号を使用した TLS 接続（データ暗号化なし）を開始します。これらのトランクは、通知先デバイスが NULL_SHA 暗号をサポートしていない場合は、そのデバイスを登録したり、コールを発信したりしません。 NULL_SHA 暗号をサポートしていない通知先デバイスでは、[暗号化 (Encrypted)] として選択した [デバイスのセキュリティプロファイル (トランク)] で設定する必要があります。このデバイスセキュリティプロファイルを使用すると、トランクは、データの暗号化を可能にする追加の TLS 暗号を提供します。
[TFTP Encrypted Config]	このチェックボックスがオンの場合、Unified Communications Manager は電話機が TFTP サーバからダウンロードするファイルを暗号化します。

設定	説明
[認証モード（Authentication Mode）]	

設定	説明
	このフィールドでは、電話機がCAPF証明書の操作時に使用する認証方法を選択できます。 ドロップダウン リスト ボックスから、次のいずれかのオプションを選択します。 • **[By Authentication String]**：ユーザが電話に CAPF 認証文字列を入力した場合にのみ、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。 • **[By Null String]**：ユーザの介入なしで、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、セキュリティは提供されません。このオプションは、閉鎖された安全な環境だけで選択することをお勧めします。 • **[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）が電話に存在する場合に、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。電話機に LSC が存在する場合、電話機に MIC が存在するかどうかに関係なく、LSC によって認証が行われます。電話機に MIC と LSC が存在する場合、LSC によって認証が行われます。電話機にLSCが存在しないが、MICが存在する場合、MICによって認証が行われます。 このオプションを選択する前に、電話機に証明書が存在することを確認してください。このオプションを選択して、電話機に証明書が存在しない場合、操作は失敗します。 MIC と LSC が同時に電話機に存在できる場合でも、電話機が CAPF への認証に使用する証明書は常に 1 つだけです。優先されるプライマリ証明書が何らかの理由で破損した場合、または別の証明書を使用して認証を受ける場合は、認証モードを更新する必要があります。 • **[By Existing Certificate (Precedence to MIC)]**：電話に LSC または MICが存在する場合に、製造元でインストールされる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。電話機に LSC が存在する場合、電話機に MIC が存在するかどうかに関係なく、LSCによって認証が行われます。電話機に LSC が存在するが、MIC が存在しない場合、LSC によって認証が行われます。 このオプションを選択する前に、電話機に証明書が存在することを確認してください。このオプションを選択して、電話機に証明

設定	説明
	書が存在しない場合、操作は失敗します。 （注） [電話セキュリティ プロファイル（Phone Security Profile）] ウィンドウで設定される CAPF 設定は、[電話の設定（Phone Configuration）] ウィンドウで設定される CAPF パラメータと連携します。
[キーの順序（Key Order）]	このフィールドは、CAPF のキーの順序を指定します。ドロップダウン リストから、次のいずれかの値を選択します。 • **[RSA のみ（RSA Only）]** • **[ECのみ（EC Only）]** • **[EC 優先、RSA バックアップ（EC Preferred, RSA Backup）]** （注） **[Key Order]**、**[RSA Key Size]**、および**[EC Key Size]** フィールドの値に基づいて電話を追加すると、デバイス セキュリティ プロファイルがその電話に関連付けられます。**[EC Only]**値 を選択し、**[EC Key Size]** の値を [256] ビットにすると、デバイス セキュリティ プロファイルには値**EC-256** が付加されます。
[RSA Key Size (Bits)]	ドロップダウン リスト ボックスから、**[512]**、**[1024]**、**[2048]**、**[3072]**、または**4096** のいずれかの値を選択します。 （注） CallManager が **[Certificate Purpose]** で選択した RSA の **[key length]** が 2048 より大きいと、一部の電話モデルが登録に失敗する場合があります。*Cisco Unified Reporting Tool*（*CURT*）の [Unified CM Phone Feature List Report] で、3072/4096 RSA キーサイズサポート機能をサポートする電話モデルの一覧を確認できます。
[ECキーサイズ（ビット）（EC Key Size (Bits)）]	ドロップダウンリストから、**256**、**384**、または**521**のいずれかの値を選択します。

次の表では、SIP を実行している電話のセキュリティ プロファイルに対する設定について説明します。

表 *4: SIP* を実行している電話のセキュリティ プロファイル

設定	説明
名前	セキュリティ プロファイルの名前を入力します。 新しいプロファイルを保存すると、電話タイプとプロトコルの [電話の設定（Phone Configuration）] ウィンドウの [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にその名前が表示されます。 **ヒント** セキュリティ プロファイル名にデバイス モデルとプロトコルを含めると、プロファイルの検索または更新時に正しいプロファイルを検索できます。
[説明（Description）]	セキュリティ プロファイルの説明を入力します。
[ナンス確認時間（Nonce Validity Time）]	ナンス値が有効な分数（秒単位）を入力します。デフォルト値は 600（10 分）です。この時間が経過すると、Unified Communications Manager は新しい値を生成します。 **（注）** ナンス値は、ダイジェスト認証をサポートする乱数であり、ダイジェスト認証パスワードの MD5 ハッシュを計算するときに使用されます。

設定	説明
[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、次のオプションのいずれかを選択します。 • [非セキュア（Non Secure）]：イメージ、ファイル、デバイス認証を除くセキュリティ機能は電話機に存在しません。TCP 接続で Unified Communications Manager が利用できます。 • [認証済（Authenticated）]： Unified Communications Managerは電話機の整合性と認証を提供します。NULL/SHA を使用する TLS 接続がシグナリングに対して開きます。 • [暗号化（Encrypted）]： Unified Communications Managerは電話機の整合性、認証、および暗号化を提供します。シグナリングに AES128/SHA を使用する TLS 接続が開き、SRTP はすべての SRTP 対応ホップでのすべてのコールに対してメディアを伝送します。 （注） [認証済み（Authenticated）] として選択されている [デバイスセキュリティプロファイル（Device Security Profile）] を使用してトランクを設定した場合、Unified Communications Manager は、NULL_SHA 暗号を使用した TLS 接続（データ暗号化なし）を開始します。これらのトランクは、通知先デバイスが NULL_SHA 暗号をサポートしていない場合は、そのデバイスを登録したり、コールを発信したりしません。NULL_SHA 暗号をサポートしていない通知先デバイスでは、[暗号化 (Encrypted)] として選択した [デバイスのセキュリティプロファイル (トランク)] で設定する必要があります。このデバイスセキュリティプロファイルを使用すると、トランクは、データの暗号化を可能にする追加の TLS 暗号を提供します。

設定	説明
転送タイプ	[デバイスセキュリティモード（Device Security Mode）] が **[非セキュア（Non Secure）]** の場合は、ドロップダウンリストから次のオプションのいずれかを選択します（一部のオプションは表示されないことがあります）。 • [TCP]：Transmission Control Protocol を選択し、パケットが送信したときと同じ順序で受信されるようにします。このプロトコルを使用すると、パケットはドロップされませんが、プロトコルはセキュリティを提供しません。 • [UDP]：User Datagram Protocol を選択し、パケットがすばやく受信されるようにします。このプロトコルはパケットをドロップする可能性があり、パケットは送信された順序で受信されない場合があります。このプロトコルはセキュリティを提供しません。 • **[TCP + UDP]**：TCP と UDP を組み合わせて使用する場合は、このオプションを選択します。このオプションはセキュリティを提供しません。 [デバイスセキュリティモード（Device Security Mode）] が [認証（Authenticated）] または [暗号化（Encrypted）] の場合、TLS では [転送タイプ（Transport Type）] を指定します。TLS は、SIP 電話に対してシグナリングの整合性、デバイス認証、およびシグナリング暗号化（暗号化モードに限る）を提供します。 プロファイルで [デバイス セキュリティ モード（Device Security Mode）] を設定できない場合は、転送タイプとして UDP を指定します。
[ダイジェスト認証の有効化（Enable Digest Authentication）]	このチェックボックスをオンにすると、Unified Communications Manager は、電話機からのすべての SIP 要求でチャレンジを行います。 ダイジェスト認証ではデバイス認証、整合性、機密性は提供されません。これらの機能を使用するには、認証または暗号化のセキュリティモードを選択します。
TFTP 暗号化（TFTP Encrypted Config）	このチェックボックスがオンの場合、Unified Communications Manager は電話機が TFTP サーバからダウンロードするファイルを暗号化します。このオプションはシスコ製電話機に限り使用できます。 **ヒント** このオプションを有効にして、対称キーを設定し、ダイジェストログイン情報と管理者パスワードを保護することをお勧めします。

設定	説明
[OAuth 認証の有効化（Enable OAuth Authentication）]	[**デバイスセキュリティプロファイル**] ドロップダウンリストから **[暗号化 (Encrypted)] を選択**すると、このチェックボックスが使用可能になります。 このチェックボックスをオンにすると、Unified Communications Manager では、電話セキュリティプロファイルに関連付けられているデバイスをSIP OAuthポートに登録することができるようになります。デフォルトでは、このチェックボックスはオフになっています。 SIP OAuth を有効にするには、次のようにします。 • [Transport Type] が [TLS] の場合： • [デバイスセキュリティモード（Device Security Mode）]は [暗号化（Encrypted）]です。 • ダイジェスト認証の無効化 • 暗号化設定は無効です。 （注） Unified Communications Manager リリース12.5以降、Jabber デバイスは SIP OAuth 認証に対応しています。
[Exclude Digest Credentials in Configuration File]	このチェックボックスをオンにすると、Unified Communications Manager は電話機が TFTP サーバからの電話ダウンロードのダイジェストログイン情報を削除します。このオプションは、Cisco IP 電話、7942、および 7962 (SIP のみ) に対応しています。

設定	説明
[認証モード（Authentication Mode）]	

設定	説明
	このフィールドでは、電話機がCAPF証明書の操作時に使用する認証方法を選択できます。このオプションはシスコ製電話機に限り使用できます。 ドロップダウンリストから、次のオプションのいずれかを選択します。 • **[By Authentication String]**：ユーザが電話にCAPF認証文字列を入力した場合にのみ、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、またはトラブルシューティングします。 • **[By Null String]**：ユーザの介入なしで、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、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が確保されません。したがって、セキュアな閉じた環境の場合にだけこのオプションを選択することをお勧めします。 • **[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）が電話に存在する場合に、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、またはトラブルシューティングします。電話機にLSCが存在する場合、電話機にMICが存在するかどうかに関係なく、LSCによって認証が行われます。電話機にLSCが存在しないが、MICが存在する場合、MICによって認証が行われます。 このオプションを選択する前に、電話機に証明書が存在することを確認してください。このオプションを選択して、電話機に証明書が存在しない場合、操作は失敗します。 MICとLSCが同時に電話機に存在できる場合でも、電話機がCAPFへの認証に使用する証明書は常に1つだけです。優先されるプライマリ証明書が何らかの理由で破損した場合、または別の証明書を使用して認証を受ける場合は、認証モードを更新する必要があります。 • **[By Existing Certificate (Precedence to MIC)]**：電話にLSCまたはMICが存在する場合に、製造元でインストールされる証明書をインストール/アップグレード、またはトラブルシューティングします。電話機にLSCが存在する場合、電話機にMICが存在するかどうかに関係なく、LSCによって認証が行われます。電話機にLSCが存在するが、MICが存在しない場合、LSCによって認証が行われます。 このオプションを選択する前に、電話機に証明書が存在することを確認してください。このオプションを選択して、電話機に証明

設定	説明
	書が存在しない場合、操作は失敗します。 （注） [電話セキュリティ プロファイル（Phone Security Profile）] ウィンドウで設定される CAPF 設定は、[電話の設定（Phone Configuration）] ウィンドウで設定される CAPF パラメータと連携します。
[キー サイズ（Key Size）]	CAPF で使用されるこの設定では、ドロップダウンリストから証明書のキー サイズを選択します。デフォルト設定は 1024 です。キー サイズのもう 1 つのオプションは、512 です。 デフォルトの設定より大きいキーサイズを選択すると、電話機でキーの生成に必要なエントロピーを生成するのに時間がかかります。キーの生成を低い優先順位で設定すると、操作の実行中に、電話機が機能します。電話機のモデルによっては、キーの生成が完了するまでに、30 分以上かかることがあります。 （注） [電話セキュリティ プロファイル（Phone Security Profile）] ウィンドウで設定される CAPF 設定は、[電話の設定（Phone Configuration）] ウィンドウで設定される CAPF パラメータと連携します。
SIP 電話ポート（SIP Phone Port）	この設定は、UDP 転送を使用し SIP を実行する電話に適用されます。 UDP を使用して Unified Communications Manager からの SIP メッセージをリッスンする Cisco Unified IP Phone（SIP のみ）のポート番号を入力します。デフォルト設定は 5060 です。 TCP または TLS を使用している電話機はこの設定を無視します。

電話のセキュリティの設定タスクフロー

電話機のセキュリティを設定するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	（任意）電話セキュリティプロファイルの検索 （31 ページ）	電話機を保護するために、電話機のセキュリティプロファイルを検索します。
ステップ 2	電話セキュリティプロファイルのセットアップ	電話機を保護するために、電話機のセキュリティプロファイルを設定します。
ステップ 3	電話機へのセキュリティ プロファイルの適用	電話セキュリティプロファイルを適用して電話を保護します。

	コマンドまたはアクション	目的
ステップ 4	電話機のセキュリティプロファイルと電話機の同期	選択した電話機とすべての電話セキュリティプロファイルを同期します。
ステップ 5	（任意） 電話セキュリティ プロファイルの削除	電話に関連付けられているすべての電話セキュリティプロファイルを削除します。
ステップ 6	電話機のセキュリティプロファイルを使用した電話機の検索	電話のセキュリティプロファイルに関連付けられているすべての電話を検索します。
ステップ 7	SIP トランク セキュリティ プロファイルのインタラクションと制限事項	SIP トランク セキュリティ プロファイルのインタラクションと制限事項

電話セキュリティプロファイルの検索

電話セキュリティプロファイルを検索するには、次の手順を実行します。

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

このウィンドウには、アクティブな（以前の）クエリーのレコードも表示されることがあります。

ステップ 2 データベース内のレコードをすべて表示するには、ダイアログボックスを空欄のままにして、ステップ 3（31 ページ） に進みます。

レコードをフィルタまたは検索するには、次の手順を実行します。

a) 最初のドロップダウンリストで、検索パラメータを選択します。
b) 2 番目のドロップダウンリストで、検索パターンを選択します。
c) 必要に応じて、適切な検索テキストを指定します。

（注） 検索条件をさらに追加するには、[+] ボタンをクリックします。 条件を追加すると、指定した条件をすべて満たしているレコードが検索されます。条件を削除するには、**[-]** ボタンをクリックして最後に追加された条件を削除するか、または**[フィルタのクリア（Clear Filter）]** をクリックして、追加されたすべての検索条件を削除します。

ステップ 3 [検索（Find）] をクリックします。

条件を満たしているレコードがすべて表示されます。1 ページあたりの項目の表示件数を変更するには、[ページあたりの行数（Rows per Page）] ドロップダウンリストで別の値を選択します。

ステップ 4 表示されるレコードのリストで、表示するレコードのリンクをクリックします。

（注） ソート順を反転させるには、リスト見出しの上矢印または下矢印が使用可能であればそれをクリックします。

ウィンドウに、選択したレコードが表示されます。

電話セキュリティプロファイルのセットアップ

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。

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

ステップ 2 次のいずれかの作業を実行します。

a) 新しいプロファイルを追加するには、[新規追加（Add New）] をクリックします。

b) 既存のセキュリティプロファイルをコピーするには、適切なプロファイルを検索し、コピーするセキュリティプロファイルの横にある [コピー（Copy）] ボタンをクリックして続行します。

c) 既存のプロファイルを更新するには、適切なセキュリティプロファイルを見つけて続行します。

[Add New] をクリックすると、各フィールドにデフォルト設定が入力された設定ウィンドウが表示されます。[コピー（Copy）] をクリックすると、コピーした設定が入力された設定ウィンドウが表示されます。

ステップ 3 SCCP または SIP を実行している電話機の適切な設定を入力します。

ステップ 4 [保存（Save）] をクリックします。

電話機へのセキュリティ プロファイルの適用

電話機の認証に証明書を使用するセキュリティプロファイルを適用する前に、特定の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) が含まれていることを確認してください。

電話機のセキュリティ機能を有効にするには、デバイスタイプとプロトコルに応じた新しいセキュリティプロファイルを設定し、電話機に適用する必要があります。ただし、電話機に証明書が含まれていない場合は、次のタスクを実行します。

- [**電話の設定 (Phone Configuration**)] ウィンドウで、非セキュアプロファイルを適用します。
- [**電話の設定 (Phone Configuration**)] ウィンドウで、capf設定を構成することによって証明書をインストールします。
- [**電話の設定 (Phone Configuration**)] ウィンドウで、認証または暗号化用に設定されたデバイスセキュリティプロファイルを適用します。

デバイスに電話セキュリティ プロファイルを適用するには、次の手順を実行します。

ステップ 1 [**電話の設定（Phone Configuration**）] ウィンドウの [**プロトコル固有情報（Protocol Specific Information**）] セクションに移動します。

ステップ 2 **[Device Security Profile]** ドロップダウンリストから、デバイスに適用するセキュリティ プロファイルを選択します。
電話機タイプとプロトコルに対してのみ設定されている電話セキュリティプロファイルが表示されます。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 該当する電話に変更を適用するには、[**設定の適用 (Apply Config)**] をクリックします。

（注） セキュリティプロファイルを削除するには、[**Find And List**] ウィンドウで該当するセキュリティプロファイルの横にあるチェックボックスをオンにし、[**delete Selected**] をクリックします。

電話機のセキュリティプロファイルと電話機の同期

電話セキュリティプロファイルに複数の電話を同期させるには、次の手順を実行します。

ステップ 1 [Unified Communications Manager Administration] で、**[システム（System）] > [セキュリティ プロファイル（Security Profile）] > [電話セキュリティ プロファイル（Phone Security Profile）]** を選択します。

ステップ 2 使用する検索条件を選択し、[検索（Find）] をクリックします。
検索条件に一致する電話セキュリティ プロファイルの一覧がウィンドウに表示されます。

ステップ 3 該当する電話機を同期する電話セキュリティプロファイルをクリックします。

ステップ 4 追加の設定変更を加えます。

ステップ 5 **[保存（Save）]** をクリックします。

ステップ 6 **[設定の適用（Apply Config）]** をクリックします。
[**設定情報の適用（Apply Configuration Information**）] ダイアログボックスが表示されます。

ステップ 7 **[OK]** をクリックします。

電話セキュリティ プロファイルの削除

Unified Communications Managerでセキュリティプロファイルを削除する前に、別のプロファイルをデバイスに適用するか、該当プロファイルを使用するすべてのデバイスを削除してください。

プロファイルを使用するデバイスを確認するには、ステップ 1 を実行します。

ステップ 1 [セキュリティプロファイルの設定（Security Profile Configuration）] ウィンドウで、[関連リンク（Related Links）] ドロップダウンリストから [依存関係レコード（Dependency Records）] を選択し、[移動（Go）] をクリックします。

依存関係レコード機能がシステムで有効になっていない場合は、**[システム]** > **[エンタープライズパラメータ設定 (system Enterprise Parameters Configuration)]** に移動し、[依存関係レコードの有効化 (Enable dependency Records)] 設定を **[True]** に変更依存関係レコード機能に関連する高 CPU 使用率に関する情報がメッセージに表示されます。依存関係レコードを有効にするには、変更を保存します。依存関係レコードの詳細については、『Cisco Unified Communications Manager システム設定ガイド』を参照してください。

ここでは、Unified Communications Manager データベースから電話セキュリティ プロファイルを削除する方法について説明します。

ステップ 2 削除するセキュリティプロファイルを検索します。

ステップ 3 複数のセキュリティプロファイルを削除するには、[**Find And List**] ウィンドウで該当するチェックボックスの横にあるチェックボックスをオンにします。次に、[**Delete Selected**] をクリックします。この選択で設定可能なすべてのレコードを削除するには、[すべて選択（Select All）] をクリックして、[選択項目の削除（Delete Selected）] をクリックします。

ステップ 4 単一のセキュリティプロファイルを削除するには、次のいずれかの作業を行います。

a) [**Find And List**] ウィンドウで、適切なセキュリティプロファイルの横にあるチェックボックスをオンにします。次に、[**Delete Selected**] をクリックします。

ステップ 5 削除操作を確認するプロンプトが表示されたら、[OK] をクリックして削除するか、[Cancel] をクリックして削除の操作をキャンセルします。

電話機のセキュリティプロファイルを使用した電話機の検索

特定のセキュリティプロファイルを使用する電話機を検索するには、次の手順を実行します。

ステップ 1 Cisco Unified Communications Manager Administrationから、**[デバイス（Device）]** > **[電話（Phone）]** を選択します。

ステップ 2 最初のドロップダウンリストから、検索パラメータ **[セキュリティプロファイル（Security Profile）]** を選択します。

a) ドロップダウンリストで、検索パターンを選択します。

b) 必要に応じて、適切な検索テキストを指定します。

（注） 追加の検索条件を追加するには、**[+]** をクリックします。条件を追加した場合、指定した条件をすべて満たしているレコードが検索されます。条件を削除する場合、最後に追加した条件を削除するには、[-] をクリックします。追加した検索条件をすべて削除するには、[Clear Filter] をクリックします。

ステップ 3 [検索（Find）] をクリックします。

条件を満たしているレコードがすべて表示されます。1 ページあたりの項目の表示件数を変更するには、[ページあたりの行数（Rows per Page）] ドロップダウンリストで別の値を選択します。

ステップ 4 表示されるレコードのリストで、表示するレコードのリンクをクリックします。

（注） ソート順を反転させるには、リスト見出しの上矢印または下矢印が使用可能であればそれをクリックします。

ウィンドウに、選択したレコードが表示されます。

SIP トランク セキュリティ プロファイルのインタラクションと制限事項

次の表に、SIP トランクセキュリティプロファイルの機能の連携動作と制限事項を示します。

表 *5 : SIP* トランク セキュリティ プロファイルのインタラクションと制限事項

機能	連携動作と制限事項
90 日間の評価ライセンス	90 日の評価期間を使用して実行している間、セキュア SIP トランクを導入することはできません。セキュア SIP トランクを導入するには、製品登録トークンで [エクスポート管理された機能を許可（Allow export-controlled functionality）] を選択した Smart Software Manager アカウントにシステムを登録してある必要があり ます。

SIP 電話機のダイジェスト認証の概要

ダイジェスト認証を使用すると、Unified Communications Manager は SIP を実行している電話機の要求メッセージをチャレンジできます。これには、キープアライブを除くすべての要求メッセージが含まれます。電話が提供するログイン情報の有効性を確認するために、Unified Communications Manager は [エンドユーザの設定（End User Configuration）] ウィンドウでの設定に基づいて、エンドユーザのダイジェストログイン情報を使用します。

電話が Extension Mobility をサポートする場合、Extension Mobility ユーザがログインすると、Unified Communications Manager は、[エンドユーザの設定（End User Configuration）] ウィンドウでの設定に基づいて、Extension Mobility エンドユーザのダイジェストログイン情報を使用します。

SIP 電話機のダイジェスト認証の前提条件

デバイスのダイジェスト認証を有効にすると、デバイスには一意のダイジェストユーザ ID とパスワードを登録する必要があります。電話ユーザやアプリケーションユーザには、Unified Communications Manager データベースで SIP ダイジェストログイン情報を設定する必要があります。

次の手順を実行してください。

- アプリケーションには、[アプリケーションユーザの設定（Application User Configuration）] ウィンドウでダイジェストログイン情報を指定します。
- SIP を実行している電話には、[エンドユーザの設定（End User Configuration）] ウィンドウでダイジェスト認証用のログイン情報を指定します。

ユーザを設定した後にログイン情報を電話と関連付けるには、[電話の設定（Phone Configuration）] ウィンドウで [ダイジェストユーザ（Digest User）] を選択します。電話をリセットした後、ログイン情報は TFTP サーバから電話機に提供される電話設定ファイル内に存在します。

- SIP トランクで受信したチャレンジの場合、レルムユーザ名（デバイスまたはアプリケーション ユーザ）およびダイジェストログイン情報を指定する SIP レルムを設定します。

（注） クラスタセキュリティモードはダイジェスト認証には影響しないことに注意してください。

SIP 電話のダイジェスト認証の設定タスクフロー

SIP 電話のダイジェスト認証を設定するには、次のタスクを完了します。

手順

	コマンドまたはアクション	目的
ステップ 1	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	ダイジェストログイン情報を、電話機を所有するエンドユーザに割り当てます。
ステップ 2	電話セキュリティプロファイルでのダイジェスト認証の有効化	電話機に関連付ける電話機のセキュリティプロファイルでダイジェスト認証を有効にします。
ステップ 3	電話機へのダイジェスト認証の割り当て	[電話の設定（Phone Configuration）] で、ユーザをダイジェストユーザとして割り当てます。ダイジェスト認証が有効なセキュリティプロファイルが割り当てられていることを確認します。
ステップ 4	エンドユーザのダイジェストクレデンシャルの設定	エンドユーザ ダイジェストのログイン情報を設定します。
ステップ 5	SIP ステーションレルムの設定 （38 ページ）	Unified CM が Unauthorized メッセージが原因で SIP 要求をチャレンジするのに使用する [レルム（Realm）] フィールドに文字列を割り当てます。

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

この手順を使用して、電話を所有しているエンドユーザにダイジェストログイン情報を割り当てます。電話機は、ログイン情報を使用して認証します。

ステップ 1 Cisco Unified Communications Manager Administration で、**[ユーザ管理（User Management）] > [エンドユーザ（End User）]** を選択します。

ステップ 2 **[検索 (Find)]** をクリックして、電話を所有しているエンドユーザを選択します。

ステップ 3 次のフィールドにクレデンシャルを入力します。

- ダイジェスト クレデンシャル（Digest Credentials）
- [ダイジェストクレデンシャルの確認（Confirm Digest Credentials）]

ステップ 4 [保存（Save）] をクリックします。

電話セキュリティプロファイルでのダイジェスト認証の有効化

電話セキュリティプロファイルを使用して電話のダイジェスト認証を有効にするには、次の手順を実行します。

ステップ 1 [Cisco Unified CM 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。

ステップ 2 **[検索（Find）]** をクリックして、対象の電話機に関連付けられている電話セキュリティ プロファイルを選択します。

ステップ 3 **[ダイジェスト認証を有効化（Enable Digest Authentication）]** 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。

電話機へのダイジェスト認証の割り当て

この手順を使用して、ダイジェストユーザとダイジェスト認証に対応したセキュリティプロファイルを電話機に関連付けます。

ステップ 1 Cisco Unified Communications Manager Administration から、**[デバイス（Device）]** > [電話（Phone）] を選択します。

ステップ 2 **[検索 (Find)]** をクリックして、ダイジェスト認証を割り当てる電話を選択します。

ステップ 3 **[ダイジェストユーザ (Digest User)]** ドロップダウンリストから、ダイジェストクレデンシャルを割り当てたエンドユーザを割り当てます。

ステップ 4 ダイジェスト認証を有効にした電話セキュリティプロファイルが、**[デバイス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から割り当てられていることを確認します。

ステップ 5 [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。

エンドユーザを電話機に関連付けた後、設定を保存し、電話機をリセットします。

SIP ステーションレルムの設定

401の不正なメッセージへの応答で SIP 電話がチャレンジされた場合に、Cisco Unified Communications Manager が使用する文字列を [レルム (Realm)] フィールドに割り当てます。これは、電話機がダイジェスト認証用に設定されている場合に適用されます。

（注） このサービス パラメータのデフォルトの文字列は「ccmsipline」です。

ステップ 1 Unified Communications Managerから、**[System（システム）] > [Service Parameters（サービスパラメータ）]** を選択します。

ステップ 2 **[サーバ（Server）]** ドロップダウンリストから、CiscoCallManager サービスをアクティブ化したノードを選択します。

ステップ 3 **[サービス（Service）]** ドロップダウンリストから、CiscoCallManager サービスを選択します。サービス名の横に「Active」と表示されることを確認します。

ステップ 4 ヘルプの説明に従って、**SIP Realm Station** パラメータを更新します。パラメータのヘルプを表示するには、疑問符またはパラメータ名のリンクをクリックします。

ステップ 5 [保存（Save）] をクリックします。

エンドユーザのダイジェストクレデンシャルの設定

ダイジェストログイン情報の詳細を表示するには、次の手順を実行します。

Cisco Unified Communications Manager の管理ページから、[ユーザ管理（User Management）] > [エンドユーザ（End User）] を選択し、[ユーザ ID（User ID）]をクリックすると、[エンドユーザの設定（End User Configuration）] ウィンドウが表示されます。ダイジェストクレデンシャルは、[**エンドユーザの設定 (End User Configuration)**] ウィンドウの [**ユーザ情報 (user Information)**] ペインで使用できます。

表 *6 :* ダイジェスト クレデンシャル（*Digest Credentials*）

設定	説明
ダイジェストクレデンシャル（Digest Credentials）	英数字の文字列を入力します。
[ダイジェストクレデンシャルの確認（Confirm Digest Credentials）]	[ダイジェストクレデンシャル（Digest Credentials）] の入力が正しいことを確認するために、このフィールドに再度クレデンシャルを入力します。

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。