CHAPTER 7

電話機セキュリティ プロファイルの設定

この章は、次の内容で構成されています。

電話機セキュリティ プロファイルの概要

Cisco Unified Communications Manager の管理では、電話機タイプおよびプロトコルに対するセキュリティ関連の設定がセキュリティ プロファイルとしてまとめられ、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、一部の CAPF 設定などがあります。[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、構成済み設定を電話機に適用します。

Cisco 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。電話機でセキュリティ機能を有効にするには、そのデバイス タイプおよびプロトコルの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。

選択したデバイスおよびプロトコルがサポートするセキュリティ機能だけが、セキュリティ プロファイル設定ウィンドウに表示されます。

電話機セキュリティ プロファイルの設定のヒント

Cisco Unified Communications Manager の管理ページで電話機セキュリティ プロファイルを設定する場合は、次の点を考慮してください。

- 電話機を設定する場合は、[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する必要があります。デバイスがセキュリティ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。
- 事前定義済みの非セキュア プロファイルは、削除することも変更することもできません。
- 現在デバイスに割り当てられているセキュリティ プロファイルを削除することはできません。
- 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、再構成した設定が、そのプロファイルを割り当てられているすべての電話機に適用されます。
- 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。古いプロファイル名および設定を割り当てられている電話機は、新しいプロファイル名および設定を受け入れます。
- 電話機セキュリティ プロファイルの CAPF 設定（認証モードおよび鍵サイズ）は、[電話の設定(Phone Configuration)] ウィンドウにも表示されます。Manufacture-Installed Certificate（MIC; 製造元でインストールされる証明書）または Locally Significant Certificate（LSC; ローカルで有効な証明書）に関連する証明書操作の CAPF 設定を定義する必要があります。[電話の設定(Phone Configuration)] ウィンドウで、これらのフィールドを直接更新できます。
  - セキュリティ プロファイルで CAPF 設定を更新すると、[電話の設定(Phone Configuration)] ウィンドウで設定が更新されます。
  - [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、Cisco 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、Cisco Unified Communications Manager は新しいプロファイルを作成して電話機に適用します。
- Cisco Unified Communications Manager 5.0 以降へのアップグレード前にデバイス セキュリティ モードを設定した場合は、Cisco Unified Communications Manager がモデルとプロトコルに基づいてプロファイルを作成し、デバイスにプロファイルを適用します。
- Manufacturer-Installed Certificate（MIC; 製造元でインストールされる証明書）は、LSC のインストールでのみ使用することをお勧めします。シスコでは、Cisco 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 認証用またはその他の目的のために MIC を使用するように電話機を設定するお客様は、ご自身の責任で行ってください。MIC が侵害されてもシスコは責任を負いかねます。

  Cisco Unified Communications Manager との TLS 接続で LCS を使用するには Cisco Unified IP Phone モデル 7906G、7911G、7931G（SCCP のみ）、7941G、7941G-GE、7942G、7945G、7961G、7961G-GE、7962G、7965G、797G、7971G、7971G-GE、および 7975G をアップグレードし、CallManager 信頼ストアから MIC ルート証明書を削除して今後の互換性の問題を回避することをお勧めします。詳細については、「証明書」（P.1-15）を参照してください。

電話機セキュリティ プロファイルの検索

電話機セキュリティ プロファイルを検索するには、次の手順を実行します。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで、[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)] の順に選択します。

[電話セキュリティプロファイルの検索と一覧表示 (Find and List Phone Security Profile)] ウィンドウが表示されます。アクティブな（前の）クエリーのレコードもウィンドウに表示される場合があります。

ステップ 2　データベースのすべてのレコードを検索するには、ダイアログボックスが空であることを確認して、ステップ 3 に進みます。

レコードをフィルタリングまたは検索するには、次の手順を実行します。

- 最初のドロップダウン リスト ボックスから、検索パラメータを選択します。
- 2 番目のドロップダウン リスト ボックスから、検索パターンを選択します。
- 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、指定したすべての条件に一致す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した条件を削除するか、[フィルタのクリア (Clear Filter)] ボタンをクリックして追加し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。

一致するすべてのレコードが表示されます。[ページあたりの行数 (Rows per Page)] ドロップダウン リスト ボックスから異なる値を選択すると各ページに表示される項目数を変更できます。

ステップ 4　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）　リストの見出しに上向きまたは下向きの矢印がある場合は、その矢印をクリックして、ソート順序を逆にします。

ウィンドウに選択した項目が表示されます。

追加情報

「関連項目」（P.7-14）を参照してください。

電話機セキュリティ プロファイルの設定

セキュリティ プロファイルを追加、更新、またはコピーするには、次の手順を実行します。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで、[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)] の順に選択します。

ステップ 2　次の作業のいずれかを実行します。

- 新しいプロファイルを追加するには、検索ウィンドウの [新規追加 (Add New)] をクリックし、ステップ 3 に進みます。
- 既存のセキュリティ プロファイルをコピーするには、「電話機セキュリティ プロファイルの検索」（P.7-3）の説明に従い、適切なプロファイルを見つけて、コピーするセキュリティ プロファイルの横に表示されている [コピー (Copy)] ボタンをクリックし、ステップ 3 に進みます。
- 既存のプロファイルを更新するには、「電話機セキュリティ プロファイルの検索」（P.7-3）の説明に従い、適切なセキュリティ プロファイルを見つけて、ステップ 3 に進みます。

[新規追加 (Add New)] をクリックすると、各フィールドのデフォルト設定を示し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、設定をコピーした設定ウィンドウが表示されます。

ステップ 3　SCCP を実行する電話機の場合は表 7-1、SIP を実行する電話機の場合は表 7-2 の説明に従い、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。

次の作業

セキュリティ プロファイルを作成した後、「電話機セキュリティ プロファイルの適用」（P.7-11）の説明に従い、電話機に適用します。

SIP を実行する電話機の電話機セキュリティ プロファイルでダイジェスト認証を設定した場合は、[エンドユーザの設定 (End User Configuration)] ウィンドウでダイジェスト信用証明書を設定する必要があります。その後、[電話の設定 (Phone Configuration)] ウィンドウの [ダイジェストユーザ (Digest User)] 設定を使用して、ユーザを電話機に関連付ける必要があります。

追加情報

「関連項目」（P.7-14）を参照してください。

電話機セキュリティ プロファイルの設定内容

表 7-1 では、SCCP を実行する電話機のセキュリティ プロファイルの設定内容について説明します。

表 7-2 では、SIP を実行する電話機のセキュリティ プロファイルの設定内容について説明します。

選択した電話機タイプおよびプロトコルがサポートしている設定だけが表示されます。

- 設定のヒントについては、「電話機セキュリティ プロファイルの設定のヒント」（P.7-2）を参照してください。
- 関連する情報および手順については、「関連項目」（P.7-14）を参照してください。

表 7-1　SCCP を実行する電話機のセキュリティ プロファイル

設定	説明
[名前(Name)]	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、該当する電話機タイプおよびプロトコルの [電話の設定(Phone Configuration)] ウィンドウにある [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 ボックス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、プロファイルを検索または更新する場合の適切なプロファイルの検出に役立ちます。
[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。
[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 ボックスから、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)]：電話機にイメージ認証以外のセキュリティ機能はありません。TCP 接続で Cisco Unified Communications Manager が利用できます。 • [認証のみ(Authenticated)]：Cisco Unified Communications Manager は電話機の整合性と認証を提供します。シグナリング用に、NULL/SHA を使用する TLS 接続を開始します。 • [暗号化(Encrypted)]：Cisco 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。シグナリング用に AES128/SHA を使用する TLS 接続を開始し、すべての電話機コールのメディアを SRTP で搬送します。
[TFTP暗号化(TFTP Encrypted Config)]	このチェックボックスがオンの場合、Cisco Unified Communications Manager は電話機が TFTP サーバからダウンロードする設定ファイルを暗号化します。詳細については、「設定ファイルの暗号化」（P.1-25）および「暗号化された電話機設定ファイルの設定」の手順（P.10-1）を参照してください。

表 7-1　SCCP を実行する電話機のセキュリティ プロファイル （続き）

設定	説明
[認証モード (Authentication Mode)]	このフィールドでは、電話機が CAPF 証明書操作中に使用する認証方式を選択できます。 ドロップダウン リスト ボックスから、次のオプションのいずれかを選択します。 • [認証ストリング (By Authentication String)]: ユーザが電話機に CAPF 認証文字列を入力した場合だけ、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。 • [Null ストリング (By Null String)]: ユーザが介入することなく、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を一切提供しません。したがって、このオプションは安全な閉じた環境の場合にだけ選択することを強く推奨します。 • [既存の証明書 (LSC の優先) (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) が電話機に存在する場合、LSC 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。LSC が電話機に存在する場合、MIC が電話機に存在するかどうかに関係なく、認証は LSC を介して行われます。MIC と LSC が電話機に存在する場合、認証は LSC を介して行われます。電話機に LSC が存在せず、MIC が存在する場合、認証は MIC を介して行われます。 このオプションを選択する前に、証明書が電話機に存在することを確認します。このオプションを選択した場合に証明書が電話機に存在しないと、操作は失敗します。 MIC と LSC は電話機で同時に存在できるものの、電話機は常に 1 つの証明書だけを使用して CAPF を認証します。優先されるプライマリ証明書が何らかの理由で侵害された場合、あるいは他の証明書を介して認証する場合には、認証モードを更新する必要があります。 • [既存の証明書 (MIC の優先) (By Existing Certificate (Precedence to MIC))] : LSC または MIC が電話機に存在する場合、LSC 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。MIC が電話機に存在する場合、LSC が電話機に存在するかどうかに関係なく、認証は MIC を介して行われます。電話機に LSC だけが存在し MIC が存在しない場合、認証は LSC を介して行われます。 このオプションを選択する前に、証明書が電話機に存在することを確認します。このオプションを選択した場合に証明書が電話機に存在しないと、操作は失敗します。 **（注）** [電話セキュリティプロファイルの設定 (Phone Security Profile Configuration)] 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 パラメータと相互に関係があります（詳細については、「電話機セキュリティ プロファイルの設定のヒント」（P.7-2）を参照してください）。[電話の設定 (Phone Configuration)] ウィンドウで CAPF 設定を定義する方法については、『*Cisco Unified Communications Manager アドミニストレーション ガイド*』を参照してください。

表 7-1　SCCP を実行する電話機のセキュリティ プロファイル （続き）

設定	説明
[キーサイズ (Key Size、ビット)]	CAPF で使用されるこの設定では、ドロップダウン リスト ボックスから証明書の鍵サイズを選択します。デフォルト設定値は 1024 です。これ以外のオプションには、512 と 2048 があります。 デフォルト設定値よりも大きな鍵サイズを選択すると、電話機で鍵生成に必要なエントロピーを生成するためにさらに時間がかかります。鍵生成を低いプライオリティで設定すると、アクションの実行中も電話機の機能を利用できます。電話機モデルによっては、鍵生成の完了に 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の設定 (Phone Security Profile Configuration)] 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 パラメータと相互に関係があります（詳細については、「電話機セキュリティ プロファイルの設定のヒント」（P.7-2）を参照してください）。[電話の設定 (Phone Configuration)] ウィンドウで CAPF 設定を定義する方法については、『*Cisco Unified Communications Manager アドミニストレーション ガイド*』を参照してください。

表 7-2　SIP を実行する電話機のセキュリティ プロファイル

設定	説明
[名前 (Name)]	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、該当する電話機タイプおよびプロトコルの [電話の設定 (Phone Configuration)] ウィンドウにある [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 ボックス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、プロファイルを検索または更新する場合の適切なプロファイルの検出に役立ちます。
[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)]	ナンス値が有効な時間を秒単位で入力します。デフォルト値は 600（10 分）です。この時間が経過すると、Cisco 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ランダム値で、ダイジェスト認証パスワードの MD5 ハッシュの計算に使用されます。

表 7-2　SIP を実行する電話機のセキュリティ プロファイル （続き）

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 ボックスから、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)]：電話機にイメージ認証以外のセキュリティ機能はありません。TCP 接続で Cisco Unified Communications Manager が利用できます。 • [認証のみ(Authenticated)]：Cisco Unified Communications Manager は電話機の整合性と認証を提供します。シグナリング用に、NULL/SHA を使用する TLS 接続を開始します。 • [暗号化(Encrypted)]：Cisco 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。シグナリング用に AES128/SHA を使用する TLS 接続を開始し、すべての SRTP 対応ホップ上のすべての電話機コールのメディアを SRTP で搬送します。
[転送タイプ(Transport Type)]	[デバイスセキュリティモード(Device Security Mode)] が [非セキュア(Non Secure)] である場合は、ドロップダウン リスト ボックスから次のオプションのいずれかを選択します(表示されないオプションもあります)。 • [TCP]：パケットを送信された順に受信するには、Transmission Control Protocol を選択します。このプロトコルは、パケットがドロップされないことを保証しますが、セキュリティは提供されません。 • [UDP]：パケットを高速に受信するには、User Datagram Protocol を選択します。このプロトコルは、パケットをドロップすることがあり、送信された順に受信するとは限りません。セキュリティは提供されません。 • [TCP + UDP]：TCP と UDP を組み合せて使用するには、このオプションを選択します。このオプションでは、セキュリティは提供されません。 [デバイスセキュリティモード(Device Security Mode)] が [認証のみ(Authenticated)] または [暗号化(Encrypted)] である場合、TLS が転送タイプとなります。TLS では、SIP 電話機のシグナリング整合性、デバイス認証、およびシグナリング暗号化（暗号化モードのみ）が提供されます。 プロファイルでデバイス セキュリティ モードを設定できない場合、転送タイプは UDP になります。

表 7-2　SIP を実行する電話機のセキュリティ プロファイル （続き）

設定	説明
[ダイジェスト認証を有効化(Enable Digest Authentication)]	このチェックボックスをオンにすると、Cisco 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、および信頼性は提供されません。これらの機能を使用するには、セキュリティ モード [認証のみ(Authenticated)] または [暗号化(Encrypted)] を選択します。 **（注）** ダイジェスト認証の詳細については、「ダイジェスト認証」(P.1-20)および「SIP 電話機のダイジェスト認証の設定」(P.11-1)を参照してください。
[TFTP暗号化(TFTP Encrypted Config)]	このチェックボックスがオンの場合、Cisco Unified Communications Manager は電話機が TFTP サーバからダウンロードする設定ファイルを暗号化します。このオプションは、シスコ製電話機専用です。 **ヒント** このオプションを有効にして、対称キーを設定し、ダイジェスト信用証明書と管理者パスワードを保護することをお勧めします。 詳細については、「設定ファイルの暗号化」(P.1-25)および「暗号化された電話機設定ファイルの設定」(P.10-1)を参照してください。
[設定ファイル内のダイジェスト信用証明書を除外(Exclude Digest Credentials in Configuration File)]	このチェックボックスがオンの場合、Cisco Unified Communications Manager は電話機が TFTP サーバからダウンロードする設定ファイル内のダイジェスト信用証明書を削除します。このオプションは、Cisco Unified IP Phone 7905G、7912G、7940G、および 7960G（SIP のみ）用です。 詳細については、「設定ファイルの暗号化」(P.1-25)および「暗号化された電話機設定ファイルの設定」(P.10-1)を参照してください。

表 7-2　SIP を実行する電話機のセキュリティ プロファイル （続き）

設定	説明
[認証モード (Authentication Mode)]	このフィールドでは、電話機が CAPF 証明書操作中に使用する認証方式を選択できます。このオプションは、シスコ製電話機専用です。 ドロップダウン リスト ボックスから、次のオプションのいずれかを選択します。 • [認証ストリング (By Authentication String)] : ユーザが電話機に CAPF 認証文字列を入力した場合だけ、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。 • [Null ストリング (By Null String)]:ユーザが介入することなく、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は一切提供されません。したがって、このオプションは安全な閉じた環境の場合にだけ選択することを強く推奨します。 • [既存の証明書 (LSC の優先) (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) が電話機に存在する場合、LSC 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。LSC が電話機に存在する場合、MIC が電話機に存在するかどうかに関係なく、認証は LSC を介して行われます。電話機に LSC が存在せず、MIC が存在する場合、認証は MIC を介して行われます。 このオプションを選択する前に、証明書が電話機に存在することを確認します。このオプションを選択した場合に証明書が電話機に存在しないと、操作は失敗します。 MIC と LSC は電話機で同時に存在できるものの、電話機は常に 1 つの証明書だけを使用して CAPF を認証します。優先されるプライマリ証明書が何らかの理由で侵害された場合、あるいは他の証明書を介して認証する場合には、認証モードを更新する必要があります。 • [既存の証明書 (MIC の優先) (By Existing Certificate (Precedence to MIC))] : LSC または MIC が電話機に存在する場合、LSC 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。MIC が電話機に存在する場合、LSC が電話機に存在するかどうかに関係なく、認証は MIC を介して行われます。電話機に LSC だけが存在し MIC が存在しない場合、認証は LSC を介して行われます。 このオプションを選択する前に、証明書が電話機に存在することを確認します。このオプションを選択した場合に証明書が電話機に存在しないと、操作は失敗します。 **（注）** [電話セキュリティプロファイルの設定 (Phone Security Profile Configuration)] 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 パラメータと相互に関係があります（詳細については、「電話機セキュリティ プロファイルの設定のヒント」（P.7-2）を参照してください）。[電話の設定 (Phone Configuration)] ウィンドウで CAPF 設定を定義する方法については、『*Cisco Unified Communications Manager アドミニストレーション ガイド*』を参照してください。

表 7-2　SIP を実行する電話機のセキュリティ プロファイル （続き）

設定	説明
[キーサイズ(Key Size、ビット)]	CAPF で使用されるこの設定では、ドロップダウン リスト ボックスから証明書の鍵サイズを選択します。デフォルト設定値は 1024 です。これ以外のオプションには、512 と 2048 があります。 デフォルト設定値よりも大きな鍵サイズを選択すると、電話機で鍵生成に必要なエントロピーを生成するためにさらに時間がかかります。鍵生成を低いプライオリティで設定すると、アクションの実行中も電話機の機能を利用できます。電話機モデルによっては、鍵生成の完了に 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の設定(Phone Security Profile Configuration)] 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 パラメータと相互に関係があります（詳細については、「電話機セキュリティ プロファイルの設定のヒント」（P.7-2）を参照してください）。[電話の設定(Phone Configuration)] ウィンドウで CAPF 設定を定義する方法については、『*Cisco Unified Communications Manager アドミニストレーション ガイド*』を参照してください。
[SIP 電話ポート(SIP Phone Port)]	この設定は、UDP 転送を使用し SIP を実行する電話機に適用されます。 UDP を使用する Cisco Unified IP Phone（SIP のみ）が、Cisco Unified Communications Manager からの SIP メッセージの傍受に使用する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 を使用する電話機は、この設定を無視します。

電話機セキュリティ プロファイルの適用

[電話の設定(Phone Configuration)] ウィンドウで、電話機セキュリティ プロファイルを電話機に適用します。

始める前に

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、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る証明書（MIC）が含まれていることを確認します。

電話機に証明書が含まれていない場合は、次の手順を実行します。

1. [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。
2. [電話の設定(Phone Configuration)] ウィンドウで、CAPF 設定で設定された証明書をインストールします。この作業の実行の詳細については、「Certificate Authority Proxy Function の使用方法」（P.9-1）を参照してください。
3. [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したデバイス セキュリティ プロファイルを適用します。

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

手順

ステップ 1　『*Cisco Unified Communications Manager 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　[電話の設定(Phone Configuration)] ウィンドウが表示されたら、[デバイスセキュリティプロファイル(Device Security Profile)] を見つけます。

ステップ 3　[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 ボックスから、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。該当する電話機タイプおよびプロトコル用に設定されている電話機セキュリティ プロファイルだけが表示されます。

ステップ 4　[保存(Save)] をクリックします。

ステップ 5　該当する電話機に変更を適用するには、[設定の適用] をクリックします。

次の作業

SIP を実行する電話機にダイジェスト認証を設定した場合は、[エンドユーザの設定(End User Configuration)] ウィンドウで、ダイジェスト信用証明書を設定する必要があります。次に、[電話の設定(Phone Configuration)] ウィンドウで、[ダイジェストユーザ(Digest User)] 設定を定義する必要があります。ダイジェスト ユーザおよびダイジェスト信用証明書の設定の詳細については、「SIP 電話機のダイジェスト認証の設定」（P.11-1）を参照してください。

追加情報

「関連項目」（P.7-14）を参照してください。

電話機セキュリティ プロファイルと影響を受ける電話機の同期

電話機を、設定変更が行われた電話機セキュリティ プロファイルと同期させるには、次の手順を実行します。この手順では、できる限り簡潔な方法で主な設定内容を適用します（たとえば、影響を受ける電話機の一部では、リセットまたは再起動する必要がない場合があります）。

手順

ステップ 1　[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)] の順に選択します。

[電話セキュリティプロファイルの検索と一覧表示(Find and List Phone Security Profiles)] ウィンドウが表示されます。

ステップ 2　使用する検索条件を選択します。

ステップ 3　[検索(Find)] をクリックします。

ウィンドウに検索条件と一致する電話機セキュリティ プロファイルのリストが表示されます。

ステップ 4　該当する電話機と同期させる電話機セキュリティ プロファイルをクリックします。[電話セキュリティプロファイルの設定(Phone Security Profile Configuration)] ウィンドウが表示されます。

ステップ 5　設定の変更を行います。

ステップ 6　[保存(Save)] をクリックします。

ステップ 7　[設定の適用] をクリックします。

[設定情報の適用] ダイアログボックスが表示されます。

ステップ 8　[OK] をクリックします。

追加情報

「関連項目」（P.7-14）を参照してください。

電話機セキュリティ プロファイルの削除

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

始める前に

Cisco Unified Communications Manager の管理ページからセキュリティ 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。該当プロファイルを使用しているデバイスを検索するには、セキュリティプロファイルの設定ウィンドウの [関連リンク (Related Links)] ドロップダウン リスト ボックスから [依存関係レコード (Dependency Records)] を選択して、[移動 (Go)] をクリックします。

システムで依存関係レコード機能が有効になっていない場合は、[システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)] の順に選択し、[Enable Dependency Records] 設定を [True] に変更します。依存関係レコード機能を使用すると、CPU 使用率が高くなるという情報を示すメッセージが表示されます。変更内容を保存して、依存関係レコードをアクティブにします。依存関係レコードの詳細については、『*Cisco Unified Communications Manager システム ガイド*』を参照してください。

手順

ステップ 1　「電話機セキュリティ プロファイルの検索」（P.7-3）の手順に従って、セキュリティ プロファイルを検索します。

ステップ 2　複数のセキュリティ プロファイルを削除するには、検索と一覧表示ウィンドウで、適切なチェックボックスの横に表示されているチェックボックスをオンにして、[選択項目の削除 (Delete Selected)] をクリックします。[すべてを選択 (Select All)] をクリックしてから [選択項目の削除 (Delete Selected)] をクリックすると、この選択で設定可能なすべてのレコードを削除できます。

ステップ 3　単一のセキュリティ プロファイルを削除するには、次の作業のどちらかを実行します。

- 検索と一覧表示ウィンドウで、適切なセキュリティ　プロファイルの横に表示されているチェックボックスをオンにして、[選択項目の削除 (Delete Selected)] をクリックします。

ステップ 4　削除操作の確認を要求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、[キャンセル (Cancel)] をクリックして削除操作を取り消します。

追加情報

「関連項目」（P.7-14）を参照してください。

電話機セキュリティ プロファイルを使用している電話機の検索

特定の電話機セキュリティ プロファイルを使用してい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 の管理ページで、[デバイス (Device)] > [電話 (Phone)] の順に選択します。

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

- 2 番目のドロップダウン リスト ボックスから検索パターンを選択します。
- 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、指定したすべての条件に一致す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した条件を削除するか、[フィルタのクリア (Clear Filter)] ボタンをクリックして追加し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。

一致するすべてのレコードが表示されます。[ページあたりの行数 (Rows per Page)] ドロップダウン リスト ボックスから異なる値を選択すると各ページに表示される項目数を変更できます。

ステップ 4　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）　リストの見出しに上向きまたは下向きの矢印がある場合は、その矢印をクリックして、ソート順序を逆にします。

ウィンドウに選択した項目が表示されます。

追加情報

詳細については、「関連項目」（P.7-14）を参照してください。

参考情報

関連項目

- 「ダイジェスト認証」（P.1-20）
- 「設定ファイルの暗号化」（P.1-25）
- 「電話機セキュリティ プロファイルの概要」（P.7-1）
- 「電話機セキュリティ プロファイルの設定のヒント」（P.7-2）
- 「電話機セキュリティ プロファイルの検索」（P.7-3）
- 「電話機セキュリティ プロファイルの設定」（P.7-4）
- 「電話機セキュリティ プロファイルの設定内容」（P.7-4）
- 「電話機セキュリティ プロファイルの適用」（P.7-11）

- 「電話機セキュリティ プロファイルと影響を受ける電話機の同期」（P.7-12）
- 「電話機セキュリティ プロファイルの削除」（P.7-13）
- 「電話機セキュリティ プロファイルを使用している電話機の検索」（P.7-14）
- 「暗号化された電話機設定ファイルの設定」（P.10-1）
- 「SIP 電話機のダイジェスト認証の設定」（P.11-1）
- 「電話機のセキュリティ強化」（P.12-1）

シスコの関連マニュアル

『*Cisco Unified Communications Manager アドミニストレーション ガイド*』

『*Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager*』