CHAPTER 5

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 CallManager の管理ページでは、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 CallManager 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 CallManager 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 CallManager 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 CallManager 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 CallManager 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 CallManager 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。
- 製造元でインストールされる証明書（MIC）は、LSC のインストールのためだけに使用することをお勧めします。シスコは、Cisco Unified CallManager との TLS 接続を認証するための LSC をサポートしています。MIC ルート証明書は侵害されている可能性があるため、お客様が TLS 認証やその他の目的で MIC を使うよう電話機を設定する場合は、自らの責任で行う必要があります。MIC が侵害されている場合、シスコは一切の責任を負いません。

  Cisco Unified IP Phone 7906、7911、7941、7961、7970、および 7971 モデルをアップグレードして Cisco Unified CallManager への TLS 接続に LSC を使用できるようにし、互換性の問題が後で発生するのを避けるため MIC ルート証明書を Cisco Unified CallManager 信頼ストアから削除することをお勧めします。詳細については、P.1-14 の「電話機の証明書の種類」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 CallManager の管理ページで、［**システム**］>［**セキュリティプロファイル**］>［**電話セキュリティプロファイル**］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。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　ドロップダウン リスト ボックスから、表示するセキュリティ プロファイルの検索条件を選択し、［**検索**］をクリックします。

（注）　データベースに登録されているすべてのセキュリティ プロファイルを検索するには、検索条件を指定せずに、［**検索**］をクリックします。

ウィンドウが更新され、検索条件と一致するセキュリティ プロファイルが表示されます。

ステップ 3　表示するセキュリティ プロファイルの［**名前（Name）**］リンクをクリックします。

ヒント　検索結果内の［名前（Name）］または［説明］を検索するには、［**絞り込み**］チェックボックスをオンにして、この手順で説明したように検索条件を入力し、［**検索**］をクリックします。

選択した項目がウィンドウに表示されます。

追加情報

詳細については、P.5-15 の「関連項目」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 CallManager の管理ページで、［**システム**］>［**セキュリティプロファイル**］>［**電話セキュリティプロファイル**］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、検索ウィンドウで［**新規追加**］をクリックして、ステップ 3 へ進みます。
- 既存のセキュリティ プロファイルをコピーするには、P.5-3 の「電話機セキュリティ プロファイルの検索」の説明に従って適切なプロファイルを見つけて表示し、［**コピー（Copy）**］をクリックして、ステップ 3 へ進みます。
- 既存のプロファイルを更新するには、P.5-3 の「電話機セキュリティ プロファイルの検索」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**］をクリックすると、設定ウィンドウが表示され、各フィールドのデフォルト設定が示されます。［**コピー（Copy）**］をクリックすると、設定ウィンドウが表示され、コピーされた設定が示されます。

ステップ 3　SCCP 電話機の場合は表 5-1、SIP 電話機の場合は表 5-2 の説明に従い、適切な設定を入力します。

ステップ 4　［**保存**］をクリックします。

追加の手順

セキュリティ プロファイルを作成した後、P.5-12 の「電話機セキュリティ プロファイルの適用」の説明に従い、電話機に適用します。

SIP 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 クレデンシャル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

詳細については、P.5-15 の「関連項目」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 5-1 で、SCCP 電話機セキュリティ プロファイルの設定について説明します。

表 5-2 で、SIP 電話機セキュリティ プロファイルの設定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、P.5-2 の「電話機セキュリティ プロファイルの設定のヒント」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、P.5-15 の「関連項目」を参照してください。

表 5-1　SCCP 電話機セキュリティ 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、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］	セキュリティ プロファイルの説明を入力します。
［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。 • **［Non Secure］**：電話機にイメージ認証以外のセキュリティ機能はない。TCP 接続で Cisco Unified CallManager が利用できる。 • **［Authenticated］**：Cisco Unified CallManager は電話機の整合性と認証を提供する。NULL/SHA を使用する TLS 接続を開始する。 • **［Encrypted］**：Cisco Unified CallManager は電話機の整合性、認証、および暗号化を提供する。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 で搬送する。
［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 CallManager 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、P.1-24 の「設定ファイルの暗号化」および P.7-1 の「暗号化された電話機設定ファイルの設定」を参照してください。

表 5-1　SCCP 電話機セキュリティ 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。 • **［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。 • **［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。 • **［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。 • **［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］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、P.5-2 の「電話機セキュリティ プロファイルの設定のヒント」を参照してください）。［電話の設定（Phone Configuration）］ウィンドウでこれらを設定する方法については、『*Cisco Unified CallManager アドミニストレーション ガイド*』を参照してください。

表 5-1　SCCP 電話機セキュリティ 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］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、P.5-2 の「電話機セキュリティ プロファイルの設定のヒント」を参照してください）。［電話の設定（Phone Configuration）］ウィンドウでこれらを設定する方法については、『*Cisco Unified CallManager アドミニストレーション ガイド*』を参照してください。

表 5-2　SIP 電話機セキュリティ 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、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］	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 CallManager 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 5-2　SIP 電話機セキュリティ 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。 • **［Non Secure］**：電話機にイメージ認証以外のセキュリティ機能はない。TCP 接続で Cisco Unified CallManager が利用できる。 • **［Authenticated］**：Cisco Unified CallManager は電話機の整合性と認証を提供する。NULL/SHA を使用する TLS 接続を開始する。 • **［Encrypted］**：Cisco Unified CallManager は電話機の整合性、認証、および暗号化を提供する。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 で搬送する。
［転送タイプ（Transport Type）］	［デバイスセキュリティモード（Device Security Mode）］が **［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しません。 • **［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しません。 • **［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 **［Authenticated］** または **［Encrypted］** である場合、TLS が転送タイプとなります。TLS 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）を提供します。 プロファイルでデバイス セキュリティ モードを設定できない場合、転送タイプは UDP になります。
［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 CallManager 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。 ダイジェスト認証は、デバイス認証、整合性、および信頼性を提供しません。これらの機能を使用するには、セキュリティ モード［Authenticated］または［Encrypted］を選択します。 **（注）** ダイジェスト認証の詳細については、P.1-18 の「ダイジェスト認証」および P.8-1 の「SIP 電話機のダイジェスト認証の設定」を参照してください。

表 5-2　SIP 電話機セキュリティ プロファイル（続き）

設定	説明
［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 CallManager 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 クレデンシャル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、P.1-24 の「設定ファイルの暗号化」および P.7-1 の「暗号化された電話機設定ファイルの設定」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 CallManager 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 クレデンシャルを削除します。このオプションは、Cisco Unified IP Phone 7905、7912、7940、および 7960 モデル（SIP のみ）専用です。 詳細については、P.1-24 の「設定ファイルの暗号化」および P.7-1 の「暗号化された電話機設定ファイルの設定」を参照してください。

表 5-2　SIP 電話機セキュリティ 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。 • **［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。 • **［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。 • **［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。 • **［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］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、P.5-2 の「電話機セキュリティ プロファイルの設定のヒント」を参照してください）。［電話の設定（Phone Configuration）］ウィンドウでこれらを設定する方法については、『*Cisco Unified CallManager アドミニストレーション ガイド*』を参照してください。

表 5-2　SIP 電話機セキュリティ 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］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、この章の P.5-2 の「電話機セキュリティ プロファイルの設定のヒント」を参照してください）。［電話の設定（Phone Configuration）］ウィンドウでこれらを設定する方法については、『*Cisco Unified CallManager 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 転送を使用する SIP 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 CallManager 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、P.6-1 の「Certificate Authority Proxy Function の使用方法」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 CallManager 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］**をクリックします。

ステップ 5　**［リセット］**をクリックして、電話機をリセットします。

追加の手順

SIP 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 クレデンシャル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 クレデンシャルの設定の詳細については、P.8-1 の「SIP 電話機のダイジェスト認証の設定」を参照してください。

追加情報

詳細については、P.5-15 の「関連項目」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 CallManager 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 CallManager 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］ドロップダウン リスト ボックスから［**依存関係レコード**］を選択して、［**移動**］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**］>［**エンタープライズ パラメータ**］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 CallManager システム ガイド*』を参照してください。

手順

ステップ 1　P.5-3 の「電話機セキュリティ プロファイルの検索」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。

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**］をクリックします。この選択に対するすべての設定可能なレコードを削除するには、［**すべてを選択**］をクリックしてから［**選択項目の削除**］をクリックします。

ステップ 2　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**］をクリックします。
- 検索と一覧表示ウィンドウで、セキュリティ プロファイルの［名前（Name）］リンクをクリックします。指定したセキュリティプロファイルの設定ウィンドウが表示されたら、［**削除**］をクリックします。

ステップ 3　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**］をクリックして削除操作を取り消します。

追加情報

詳細については、P.5-15 の「関連項目」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

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 CallManager の管理ページで［**デバイス**］>［**電話**］の順に選択します。

ステップ 2　［**検索対象 : 電話 、検索条件**］ドロップダウン リスト ボックスから、［**セキュリティプロファイル**］を選択します。

ステップ 3　必要に応じて、［検索対象 : 電話 、検索条件］ドロップダウン リスト ボックスの横に表示されているドロップダウン リスト ボックスのオプションを選択してセキュリティ プロファイルの追加の検索条件を指定し、特定の検索条件を入力します。

ステップ 4　検索条件を指定した後、［**検索**］をクリックします。検索結果が表示されます。

追加情報

詳細については、P.5-15 の「関連項目」を参照してください。

その他の情報

関連項目

- ダイジェスト認証（P.1-18）
- 設定ファイルの暗号化（P.1-24）
- 電話機セキュリティ プロファイルの概要（P.5-1）
- 電話機セキュリティ プロファイルの設定のヒント（P.5-2）
- 電話機セキュリティ プロファイルの検索（P.5-3）
- 電話機セキュリティ プロファイルの設定（P.5-4）
- 電話機セキュリティ プロファイルの設定内容（P.5-5）
- 電話機セキュリティ プロファイルの適用（P.5-12）
- 電話機セキュリティ プロファイルの削除（P.5-13）
- 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.5-14）
- 暗号化された電話機設定ファイルの設定（P.7-1）
- SIP 電話機のダイジェスト認証の設定（P.8-1）
- 電話機のセキュリティ強化（P.9-1）

シスコの関連マニュアル

Cisco Unified CallManager アドミニストレーション ガイド

Cisco Unified IP Phone アドミニストレーション ガイド for Cisco Unified CallManager