



# 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 \(P.5-1\)](#)
- [SCCP または SIP 電話機セキュリティ プロファイルの検索 \(P.5-2\)](#)
- [SCCP または SIP 電話機セキュリティ プロファイルの設定 \(P.5-3\)](#)
- [SCCP 電話機セキュリティ プロファイル の設定内容 \(P.5-4\)](#)
- [SIP 電話機セキュリティ プロファイルの設定内容 \(P.5-6\)](#)
- [SCCP または SIP 電話機セキュリティ プロファイルの適用 \(P.5-9\)](#)
- [SCCP または SIP 電話機セキュリティ プロファイルの削除 \(P.5-10\)](#)
- [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 \(P.5-11\)](#)
- [その他の情報 \(P.5-11\)](#)

## 電話機セキュリティ プロファイルの概要

Cisco CallManager Administration では、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、セキュリティ関連の設定がグループ化されます。そのため、デバイス設定ウィンドウでプロファイルを選択することで、すべての構成済み設定を SIP または SCCP 電話機に適用できます。

電話機セキュリティ プロファイルを設定するときは、次の情報について検討してください。

- プロファイルの CAPF 設定は、Phone Configuration ウィンドウで表示される Certificate Authority Proxy Function 設定と組み合わせて設定する。
- すべての SIP および SCCP 電話機に、セキュリティ プロファイルを適用する必要がある。デバイスがセキュリティをサポートしていない場合は、ノンセキュア プロファイルを適用する。
- Cisco CallManager 5.0 アップグレードの前にデバイス セキュリティ モードを設定した場合は、Cisco CallManager がモード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する。
- デバイスが設定済みのプロファイルをサポートしない場合、Cisco CallManager は、そのプロファイルをデバイスに適用することを許可しない。

## SCCP または SIP 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 CallManager Administration で、**System > Security Profile > SIP Phone Security Profile** または **SCCP Phone Security Profile** の順に選択します。

Find and List ウィンドウが表示されます。

- 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基準を選択し、**Find** 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、検索基準を指定せずに、**Find** をクリックします。

ウィンドウが更新され、検索基準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 **Name** リンクをクリックします。



**ヒント** 検索結果内の Name または Description を検索するには、**Search Within Results** 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基準を入力し、**Find** をクリックします。

### 追加情報

詳細については、[P.5-11](#) の「[関連項目](#)」を参照してください。

## SCCP または SIP 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 CallManager Administration で、**System > Security Profile > SIP Phone Security Profile** または **SCCP 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、**Add New** ボタンをクリックし、**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、**P.5-2** の「**SCCP または SIP 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 **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、**P.5-2** の「**SCCP または SIP 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。

**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** **Save** 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.5-9** の「**SCCP または SIP 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、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。Phone Configuration ウィンドウでダイジェスト ユーザを指定します。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.5-11** の「**関連項目**」を参照してください。

## SCCP 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 5-1 SCCP 電話機セキュリティ プロファイル

設定	説明
Name	<p>セキュリティ プロファイルの名前を入力します。</p> <p>デバイスがプロファイルをサポートする場合、Phone Configuration ウィンドウの SCCP Phone Security Profile ドロップダウンリストボックスに名前が表示されます。</p>
Description	<p>セキュリティ プロファイルの説明を入力します。</p>
Device Security Mode	<p>ドロップダウン ボックスから、次のオプションのいずれか 1 つを選択します。</p> <ul style="list-style-type: none"> <li>• <b>Non Secure</b> : 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 CallManager が利用できる。</li> <li>• <b>Authenticated</b> : Cisco 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。</li> <li>• <b>Encrypted</b> : Cisco 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。</li> </ul>

表 5-1 SSCP 電話機セキュリティ プロファイル (続き)

設定	説明
Authentication Mode	<p>Certificate Authority Proxy Function で使用します。このフィールドで、Phone Configuration ウィンドウで設定した証明書の操作中に、電話機が CAPF で認証するために使用する方式を選択できます。</p> <p>ドロップダウン ボックスから、次のオプションのいずれか 1 つを選択します。</p> <ul style="list-style-type: none"> <li>• <b>By Authentication String</b> : 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。</li> <li>• <b>By Null String</b> : 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。</li> <li>• <b>By Existing Certificate (Precedence to LSC)</b> : 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。</li> <li>• <b>By Existing Certificate (Precedence to MIC)</b> : 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。</li> </ul>
Key Size	<p>CAPF で使用します。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。</p> <p>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。</p>

## SIP 電話機セキュリティ プロファイルの設定内容

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。

表 5-2 SIP 電話機セキュリティ プロファイル


設定	説明
Name	<p>セキュリティ プロファイルの名前を入力します。</p> <p></p> <p><b>ヒント</b> デバイスに正しいプロファイルを適用できるように、セキュリティ プロファイル名にはデバイス モデルを含めます。</p>
Description	セキュリティ プロファイルの説明を入力します。
Nonce Validity Time	<p>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。</p> <p>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 CallManager は新しい値を生成します。</p>
Device Security Mode	<p>ドロップダウン ボックスから、次のオプションのいずれか 1 つを選択します。</p> <ul style="list-style-type: none"> <li>• <b>Non Secure</b> : 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 CallManager が利用できる。</li> <li>• <b>Authenticated</b> : Cisco 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。</li> <li>• <b>Encrypted</b> : Cisco 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。</li> </ul>
Transport Type	<p>ドロップダウン ボックスから、次のオプションのいずれか 1 つを選択します。</p> <ul style="list-style-type: none"> <li>• <b>TCP</b> : 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。</li> <li>• <b>UDP</b> : 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。</li> <li>• <b>TLS</b> : SIP 電話機のシグナリング整合性、デバイス認証、シグナリング暗号化を保証するには、Transport Layer Security プロトコルを選択します。 認証のみをサポートするデバイスの場合、TLS_RSA_WITH_NULL_SHA アルゴリズムが使用されます。 認証と暗号化をサポートするデバイスの場合、TLS_RSA_WITH_AES128_SHA が使用されます。</li> <li>• <b>TCP + UDP</b> : TCP と UDP を組み合わせて使用するには、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。</li> </ul>

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
Enable Digest Authentication	<p data-bbox="620 309 1474 517">電話機から Cisco CallManager に要求を送信したときに、Cisco CallManager が電話機の ID でチャレンジを行うようにするには、このチェックボックスをオンにします。Cisco CallManager が ID でチャレンジを行った後、電話機は MD5 チェックサムで応答し、Cisco CallManager Administration で設定したクレデンシャルに基づいて Cisco CallManager が情報を検証します。クレデンシャルが一致した場合、電話機のダイジェスト認証は成功します。</p> <p data-bbox="620 539 1474 607">このチェックボックスをオンにすると、Cisco 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。</p> <hr/> <p data-bbox="620 629 699 674"> <b>ヒント</b></p> <p data-bbox="730 680 1474 837">ダイジェスト認証クレデンシャルは、Cisco CallManager Administration の End User ウィンドウで指定します。ユーザを設定した後でクレデンシャルを電話機に関連付けるには、Phone Configuration ウィンドウで Digest User (エンドユーザ) を選択します。</p> <p data-bbox="730 871 1474 965">ダイジェスト認証は、整合性や信頼性を提供しません。電話機の整合性と信頼性を保証するには、Transport Type を TLS に設定し、デバイスセキュリティ モードを暗号化に設定します。</p> <hr/> <p data-bbox="620 1021 667 1066"> <b>(注)</b></p> <p data-bbox="708 1072 1474 1162">ダイジェスト認証の詳細については、P.1-17 の「ダイジェスト認証」および第 8 章「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。</p>

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
Authentication Mode	<p>CAPF で使用します。このフィールドで、Phone Configuration ウィンドウで設定した証明書 of 操作中に、電話機が CAPF で認証するために使用する方式を選択できます。</p> <p>ドロップダウン ボックスから、次のオプションのいずれか 1 つを選択します。</p> <ul style="list-style-type: none"> <li>• <b>By Authentication String</b> : 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。</li> <li>• <b>By Null String</b> : 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。</li> <li>• <b>By Existing Certificate (Precedence to LSC)</b> : 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。</li> <li>• <b>By Existing Certificate (Precedence to MIC)</b> : 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。</li> </ul>
Key Size	<p>CAPF で使用します。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。</p> <p>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。</p>
SIP Phone Port	<p>Cisco SIP IP Phone が、Cisco 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。</p>



## SCCP または SIP 電話機セキュリティ プロファイルの適用

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。

認証または暗号化用に設定したセキュリティ 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. Phone Configuration ウィンドウで、ノンセキュア プロファイルを適用します。
2. 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. Phone Configuration ウィンドウで、認証または暗号化用に設定した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 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** Phone Configuration ウィンドウが表示された後、電話機のプロトコルに応じて、次の設定を見つめます。
    - **SCCP Phone Security Profile**
    - **SIP Phone Security Profile**
  - ステップ 3** セキュリティ プロファイルのドロップダウン 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。
  - ステップ 4** **Save** をクリックします。
  - ステップ 5** **Reset** 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、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、Phone Configuration ウィンドウで、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.5-11 の「[関連項目](#)」を参照してください。

## SCCP または SIP 電話機セキュリティ プロファイルの削除

ここでは、Cisco 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 CallManager Administration 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、当該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。当該プロファイルを使用しているデバイスを検索するには、Security Profile Configuration ウィンドウの Related Links ドロップダウン リスト ボックスから **Dependency Records** を選択して、**Go** をクリックします。

システムで Dependency Records 機能が有効になっていない場合は、レコードの依存性の概要ウィンドウに、Dependency Records を有効にすると実行できるアクションを示すメッセージが表示されます。また、Dependency Records 機能を使用すると、CPU 使用率が高くなるという情報も表示されます。Dependency Records の詳細については、『Cisco 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.5-2 の「SCCP または SIP 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。
- 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、Find and List 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、**Delete Selected** アイコンまたは **Delete Selected** ボタンをクリックします。
- 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。
- 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表示されているチェックボックスをオンにして、**Delete Selected** アイコンまたは **Delete Selected** ボタンをクリックします。
  - Find and List ウィンドウで、セキュリティ プロファイルの Name リンクをクリックします。指定した Security Profile Configuration ウィンドウが表示されたら、**Delete** アイコンまたは **Delete** ボタンをクリックします。
- 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、**Cancel** 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.5-11 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 CallManager Administration で **Device > Phone** の順に選択します。
  - ステップ 2** Find Phone where ドロップダウン リスト ボックスから、**Security Profile** を選択します。
  - ステップ 3** 必要に応じて、Find Phone 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基準を指定し、特定の検索基準を入力します。
  - ステップ 4** 検索基準を指定した後、**Find** 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.5-11](#) の「[関連項目](#)」を参照してください。

## その他の情報

### 関連項目

- [電話機セキュリティ プロファイルの概要 \(P.5-1\)](#)
- [SCCP または SIP 電話機セキュリティ プロファイルの検索 \(P.5-2\)](#)
- [SCCP または SIP 電話機セキュリティ プロファイルの設定 \(P.5-3\)](#)
- [SCCP 電話機セキュリティ プロファイルの設定内容 \(P.5-4\)](#)
- [SIP 電話機セキュリティ プロファイルの設定内容 \(P.5-6\)](#)
- [SCCP または SIP 電話機セキュリティ プロファイルの適用 \(P.5-9\)](#)
- [SCCP または SIP 電話機セキュリティ プロファイルの削除 \(P.5-10\)](#)
- [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 \(P.5-11\)](#)
- [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 IP Phone アドミニストレーションガイド for Cisco CallManager*

