SIP トランク セキュリティ プロファイルの設定

この章では、SIP トランクセキュリティプロファイルの設定について説明します。

SIP トランク セキュリティ プロファイルの設定について

Unified Communications Manager Administration では、単一のセキュリティ プロファイルを複数の SIP トランクに割り当てることができるよう、SIP トランクのセキュリティ関連の設定項目をグループ化しています。セキュリティ関連の設定項目には、デバイス セキュリティ モード、ダイジェスト認証、着信/発信転送タイプの設定があります。[トランクの設定（Trunk Configuration）] ウィンドウでセキュリティプロファイルを選択する際に、構成済みの設定を SIP トランクに適用します。

Unified Communications Manager をインストールすると、自動登録用の定義済み非セキュア SIP トランク セキュリティ プロファイルが提供されます。SIP トランクのセキュリティ機能を有効にするには、新しいセキュリティ プロファイルを設定し、それを SIP トランクに適用します。トランクがセキュリティをサポートしない場合は、非セキュア プロファイルを選択してください。

セキュリティ プロファイルの設定ウィンドウには、SIP トランクがサポートするセキュリティ機能だけが表示されます。

SIP トランク セキュリティ プロファイルの設定のヒント

[Unified Communications Manager Administration] で SIP トランク セキュリティ プロファイルを設定する際には以下の情報を考慮してください。

- SIP トランクを設定する場合は、[トランクの設定 (Trunk 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 プロファイルを選択します。
- 現在デバイスに割り当てられているセキュリティ プロファイルは削除できません。
- すでに SIP トランク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、そのプロファイルが割り当てられているすべての SIP トランク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。古いプロファイル名と設定が割り当てられている SIP トランクは、新しいプロファイル名と設定を前提としています。
- Unified Communications Manager 5.0 以降のアップグレード前にデバイス セキュリティ モードを設定していた場合、Unified Communications Manager は SIP トランクのプロファイルを作成し、そのプロファイルをデバイスに適用します。

SIP トランクセキュリティプロファイルの検索

SIP トランク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

Step 1 **[System]** > **[Security Profile]** > **[SIP Trunk 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。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。

Step 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、Step 3 （3 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) ドロップダウン リスト ボックスで検索パラメータを選択します。
b) 次に、ドロップダウン リスト ボックス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。

SIP トランク セキュリティ プロファイルの設定

（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。条件を削除する場合、最後に追加した条件を削除するには、[-] ボタンをクリックします。追加した検索条件をすべて削除するには、[Clear Filter] ボタンをクリックします。

Step 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 ボックスで別の値を選択します。

Step 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。

選択した項目がウィンドウに表示されます。

関連トピック

SIP トランクセキュリティプロファイルに関する詳細情報の入手先, on page 14

SIP トランク セキュリティ プロファイルの設定

SIP トランク 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

Step 1 Cisco Unified Communications Manager Administrationから、**[システム（System）] > [セキュリティ プロファイル（Security Profile）] > [SIP トランクセキュリティプロファイル（SIP Trunk Security Profile）]** を選択します。

Step 2 次のいずれかの操作を行います。

a) 新しいプロファイルを追加するには、[Find] ウィンドウで [Add New] をクリックします

（プロファイルを表示してから、[Add New] をクリックすることもできます）。

各フィールドにデフォルト設定が取り込まれた設定ウィンドウが表示されます。

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見つけ、[Copy] 列内にあるそのレコード用の [Copy] アイコンをクリックします

（プロファイルを表示してから、[Copy] をクリックすることもできます）。

設定ウィンドウが表示され、設定された項目が示されます。

c) 既存のプロファイルを更新するには、SIP トランクセキュリティプロファイルの検索（2 ページ）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表示します。

設定ウィンドウが表示され、現在の設定が示されます。

Step 3 「SIP トランク セキュリティ プロファイルの設定」の説明に従って、適切な設定を入力します。

Step 4 [保存（Save）] をクリックします。

セキュリティプロファイルを作成したら、それをトランクに適用します。SIP トランクにダイジェスト認証を設定した場合は、SIP トランクを介して接続されているアプリケーションの [**Sip レルム (Sip Realm)] 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 (まだ設定していない場合)。SIP トランクを介して接続されているアプリケーションに対してアプリケーションレベルの許可を有効にした場合は、[**アプリケーションユーザ (Application User)**] ウィンドウでアプリケーションに許可されているメソッドを設定する必要があります (まだ実行していない場合)。

関連トピック

SIP トランクセキュリティプロファイルの適用, on page 12
SIP トランクセキュリティプロファイルに関する詳細情報の入手先, on page 14

SIP トランク セキュリティ プロファイルの設定

次の表では、[SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）] の設定項目について説明します。

表 *1 : SIP* トランク セキュリティ プロファイルの設定項目

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、[トランクの設定（Trunk Configuration）] ウィンドウの [SIP トランク セキュリティ プロファイルの設定（SIP Trunk Security Profile）] ドロップダウンリストにその名前が表示されます。
説明	セキュリティプロファイルの説明を入力します。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。

SIP トランク セキュリティ プロファイルの設定

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）]：イメージ認証以外のセキュリティ機能は適用されません。TCP または UDP 接続で Unified Communications Manager が利用できます。 • [認証済み（Authenticated）]：Unified Communications Manager はトランクの整合性と認証を提供します。NULL/SHA を使用する TLS 接続が開きます。 • [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。AES128/SHA を使用する TLS 接続がシグナリング用に開きます。 （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接続先デバイスでは、トランクを **[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（Device Security Profile）] オプション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。
[Incoming 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）] の場合、転送タイプは TCP+UDP になります。 [デバイスセキュリティモード（Device Security Mode）] が [認証済（Authenticated）] または [暗号化（Encrypted）] の場合、TLS で転送タイプが指定されます。 （注） Transport Layer Security（TLS）プロトコルによって、 Unified Communications Managerとトランク間の接続が保護されます。

SIP トランク セキュリティ プロファイルの設定

設定	説明
[発信転送タイプ（Outgoing Transport Type）]	ドロップダウン リストから適切な発信転送モードを選択します。 [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、[TCP] または [UDP] を選択します。 [デバイスセキュリティモード（Device Security Mode）] が [認証済（Authenticated）] または [暗号化（Encrypted）] の場合、TLS で転送タイプが指定されます。 （注） TLS により、SIP トランクのシグナリング完全性、デバイス認証、およびシグナリング暗号化が保証されます。 ヒント TCP 接続の再利用をサポートしていない Unified Communications Manager システムと IOS ゲートウェイ間で SIP トランクを接続する場合は、発信トランスポートタイプとして UDP を使用する必要があります。
[ダイジェスト認証の有効化（Enable Digest Authentication）]	ダイジェスト認証を有効にするには、このチェックボックスをオンにします。このチェックボックスをオンにすると、Unified Communications Manager は、トランクからのすべての SIP 要求に対して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、完全性、および機密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 [認証済（Authenticated）] または [暗号化（Encrypted）] を選択してください。 ヒント TCP または UDP 転送を使用しているトランクでの SIP トランク ユーザを認証するには、ダイジェスト認証を使用してください。
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。

SIP トランク セキュリティ プロファイルの設定

設定	説明
安全な証明書の件名またはサブジェクトの別名	このフィールドは、着信転送タイプおよび発信転送タイプにTLSを設定した場合に適用されます。 デバイス認証では、SIP トランク デバイスのセキュアな証明書のサブジェクトまたはサブジェクト代替名を入力します。Unified Communications Manager クラスタを使用している場合、または TLS ピアに SRV ルックアップを使用している場合は、1 つのトランクが複数のホストに解決されることがあります。このように解決された場合、トランクに複数のセキュアな証明書のサブジェクトまたはサブジェクト代替名が設定されます。X.509 のサブジェクト名が複数存在する場合、スペース、カンマ、セミコロン、コロンのいずれかを入力して名前を区切ります。 このフィールドには、4096 文字まで入力できます。 **ヒント** サブジェクト名は、送信元接続 TLS 証明書に対応します。サブジェクト名とポートごとにサブジェクト名が一意になるようにしてください。異なるSIPトランクに同じサブジェクト名と着信ポートの組み合わせを割り当てることはできません。例: ポート 5061 の SIP TLS trunk1 は、セキュリティ保護された証明書の件名またはサブジェクト代替名 my_cm1, my_cm2 を持っています。ポート 5071 の SIP TLS trunk2 には、セキュリティで保護された証明書のサブジェクトまたはサブジェクト代替名 my_cm2, my_cm3 があります。ポート 5061 の SIP TLS trunk3は、セキュリティで保護された証明書の件名またはサブジェクト代替名my_ccm4を含むことができますが、安全な証明書のサブジェクトまたはサブジェクト代替名 my_cm1 を含めることはできません。
[着信ポート（Incoming Port）]	着信ポートを選択します。0 ～ 65535 の範囲の一意のポート番号値を 1 つ入力します。着信 TCP および UDP SIP メッセージのデフォルト ポート値として 5060 が指定されます。着信 TLS メッセージのデフォルトの保護されたSIPポートには5061が指定されます。ここで入力した値は、このプロファイルを使用するすべての SIP トランクに適用されます。 **ヒント** TLSを使用するすべてのSIPトランクは同じ着信ポートを共有できます。TCP + UDP を使用するすべての SIP トランクは同じ着信ポートを共有できます。同じポートで、TLS SIP転送トランクと TLS 以外の SIP 転送トランク タイプを混在させることはできません。

SIP トランク セキュリティ プロファイルの設定

設定	説明
[アプリケーション レベル認証を有効化（Enable Application Level Authorization）]	アプリケーション レベルの認証が、SIP トランクを介して接続されたアプリケーションに適用されます。 このチェックボックスをオンにする場合、[ダイジェスト認証を有効化（Enable Digest Authentication）] チェックボックスもオンにして、トランクのダイジェスト認証を設定する必要があります。Unified Communications Manager は、許可されているアプリケーション方式を確認する前に、SIP アプリケーションユーザを認証します。 アプリケーションレベルの許可が有効な場合、トランクレベルの許可が最初に発生してからアプリケーションレベルの許可が発生するため、Unified Communications Manager は [アプリケーションユーザの設定（Application User Configuration）] ウィンドウで SIP アプリケーションユーザに対して許可されたメソッドより先に、（このセキュリティプロファイル内の）トランクに対して許可されたメソッドをチェックします。 **ヒント** アプリケーションを信頼性を識別できない場合、または特定のトランクでアプリケーションが信頼されない場合（つまり、予期したものとは異なるトランクからアプリケーション要求が着信する場合）には、アプリケーション レベル認証の使用を考慮してください。
[プレゼンスの SUBSCRIBE の許可（Accept Presence Subscription）]	Unified Communications Manager が SIP トランク経由で着信するプレゼンスサブスクリプション要求を受け付けるようにする場合は、このチェックボックスをオンにします。 [アプリケーション レベル認証を有効化（Enable Application level authorization）] チェックボックスをオンにした場合は、[アプリケーション ユーザの設定（Application User Configuration）] ウィンドウに移動し、この機能に関して許可されるアプリケーション ユーザの [プレゼンスの SUBSCRIBE の許可（Accept Presence Subscription）] チェックボックスをオンにします。 アプリケーション レベルの認証が有効な場合、[プレゼンスの SUBSCRIBE の許可（Accept Presence Subscription）] チェックボックスがアプリケーション ユーザに関してオンに設定され、トランクに関してはオンに設定されない場合、トランクに接続される SIP ユーザ エージェントに 403 エラー メッセージが送信されます。

SIP トランク セキュリティ プロファイルの設定

設定	説明
Out-of-Dialog REFER の許可（Accept Out-of-dialog REFER）	Unified Communications Manager が SIP トランク経由で着信する非インバイトの Out-of-Dialog REFER 要求を受け付けるようにする場合は、このチェックボックスをオンにします。 [アプリケーション レベル認証を有効化（Enable Application level authorization）] チェックボックスをオンにした場合は、[アプリケーション ユーザの設定（Application User Configuration）] ウィンドウに移動し、この方式に関して許可されるアプリケーション ユーザの [Out-of-Dialog REFER の許可（Accept Out-of-dialog REFER）] チェックボックスをオンにします。
[Unsolicited NOTIFY の許可（Accept Unsolicited Notification）]	Unified Communications Manager が SIP トランク経由で着信する非 INVITE、Unsolicited NOTIFY メッセージを受け入れるようにするには、このチェックボックスをオンにします。 [アプリケーション レベル認証を有効化（Enable Application level authorization）] チェックボックスをオンにした場合は、[アプリケーション ユーザの設定（Application User Configuration）] ウィンドウに移動し、この方式に関して許可されるアプリケーション ユーザの [Unsolicited NOTIFY の許可（Accept Unsolicited Notification）] チェックボックスをオンにします。
[ヘッダー置き換えの許可（Accept Replaces Header）]	Unified Communications Manager が既存の SIP ダイアログを置き換える新しい SIP ダイアログを受け付けるようにする場合は、このチェックボックスをオンにします。 [アプリケーション レベル認証を有効化（Enable Application level authorization）] チェックボックスをオンにした場合は、[アプリケーション ユーザの設定（Application User Configuration）] ウィンドウに移動し、この方式に関して許可される [ヘッダー置き換えの許可（Accept Header Replacement）] チェックボックスをオンにします。
[セキュリティ ステータスを送信（Transmit Security Status）]	Unified Communications Manager が、関連付けられた SIP トランクから SIP ピアにコールのセキュリティ アイコン ステータスを送信するようにする場合は、このチェックボックスをオンにします。 デフォルトでは、このボックスはオフになっています。

SIP トランク セキュリティ プロファイルの設定

設定	説明
[SIP V.150アウトバウンドSDPオファーのフィルタリング（SIP V.150 Outbound SDP Offer Filtering）]	ドロップダウンリストから、次のフィルタ処理オプションのいずれかを選択します。 • [デフォルトのフィルタを使用（Use Default Filter）]：SIP トランクは、[SIP V.150 アウトバウンド SDP オファーのフィルタリング（SIP V.150 Outbound SDP Offer Filtering）] サービス パラメータで指定されたデフォルト フィルタを使用します。このサービスパラメータを見つけるには、 Cisco Unified Communications Manager Administration で、**[システム（System）] > [サービスパラメータ（Service Parameters）] > [クラスタ全体のパラメータ（デバイス-SIP）（Clusterwide Parameters (Device-SIP)）]** の順に移動します。 • [フィルタなし（No Filtering）]：SIP トランクは、アウトバウンド オファー内の V.150 SDP 行のフィルタリングを実行しません。 • [MER V.150 を削除（Remove MER V.150）]：SIP トランクは、アウトバウンド オファー内の V.150 MER SDP 行を削除します。 トランクが MER V.150 よりも前の Unified Communications Manager に接続する際のあいまいさを低減するには、このオプションを選択します。 • [Remove Pre-MER V.150]：SIP トランクは、アウトバウンド オファーで非 MER 対応 V.150 回線をすべて削除します。クラスタがプレ MER 回線でオファーを処理できない MER 準拠デバイスのネットワークに含まれる際のあいまいさを低減するには、このオプションを選択します。

SIP トランク セキュリティ プロファイルの設定

設定	説明
[SIP V.150アウトバウンドSDPオファーのフィルタリング（SIP V.150 Outbound SDP Offer Filtering）]	ドロップダウンリストから、次のフィルタ処理オプションのいずれかを選択します。 • [デフォルトのフィルタを使用（Use Default Filter）]：SIP トランクは、[SIP V.150 アウトバウンド SDP オファーのフィルタリング（SIP V.150 Outbound SDP Offer Filtering）] サービス パラメータで指定されたデフォルト フィルタを使用します。このサービスパラメータを見つけるには、 Cisco Unified Communications Manager Administration で、**[システム（System）] > [サービスパラメータ（Service Parameters）] > [クラスタ全体のパラメータ（デバイス-SIP）（Clusterwide Parameters (Device-SIP)）]** の順に移動します。 • [フィルタなし（No Filtering）]：SIP トランクは、アウトバウンド オファー内の V.150 SDP 行のフィルタリングを実行しません。 • [MER V.150 を削除（Remove MER V.150）]：SIP トランクは、アウトバウンド オファー内の V.150 MER SDP 行を削除します。 トランクが MER V.150 よりも前の Unified Communications Manager に接続する際のあいまいさを低減するには、このオプションを選択します。 • [Remove Pre-MER V.150]：SIP トランクは、アウトバウンド オファーで非 MER 対応 V.150 回線をすべて削除します。MER より前の行を使用するオファーを処理できない MER 準拠デバイスからなるネットワークにクラスタが含まれている場合、あいまいさを減らすには、このオプションを選択します。 （注） セキュアなコール接続を確立するには、V.150 用に SIP で IOS を設定する必要があります。IOS をUnified Communications Managerで設定する際の詳細については、http://www.cisco.com/c/en/us/td/docs/ios/12_4t/12_4t4/mer_cg_15_1_4M.htmlをご覧ください。

関連トピック

認証
ダイジェスト認証
SIP トランクのダイジェスト認証の設定
SIP トランク セキュリティ プロファイルの設定のヒント, on page 2
SIP トランクセキュリティプロファイルに関する詳細情報の入手先, on page 14

SIP トランクセキュリティプロファイルの適用

[Trunk Configuration] ウィンドウでトランクに SIP トランク セキュリティ プロファイルを適用します。デバイスにセキュリティ 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

Step 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、トランクを検索します。

Step 2 [**Trunk Configuration**] ウィンドウが表示されたら、[**SIP trunk Security Profile**] の設定を見つけます。

Step 3 **セキュリティプロファイル**の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。

Step 4 [保存（Save）] をクリックします。

Step 5 トランクをリセットするには、[**Apply Config**] をクリックします。
ダイジェスト認証を有効にしたプロファイルを SIP トランクに適用した場合は、トランクの [SIP レルム（SIP Realm）] ウィンドウでダイジェストログイン情報を設定する必要があります。アプリケーションレベルの認証を有効にするプロファイルを適用した場合は、[**アプリケーションユーザ (Application User)**] ウィンドウでダイジェストクレデンシャルと許可された認可方式を設定する必要があります (まだ実行していない場合)。

関連トピック

SIP レルムの設定
SIP トランクセキュリティプロファイルに関する詳細情報の入手先, on page 14

Sip トランクセキュリティプロファイルと SIP トランクの同期

SIP トランクを設定変更を行った SIP トランクセキュリティプロファイルと同期するには、次の手順を実行します。これにより、最も影響の少ない方法で未処理の設定が適用されます。（たとえば、影響を受けるデバイスの一部では、リセットまたは再起動が不要な場合があります。）

手順

Step 1 **[System] > [Security Profile] > [SIP Trunk Security Profile]** の順に選択します。

Step 2 使用する検索条件を選択します。

Step 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 SIP トランク セキュリティ プロファイルのリストが表示されます。

Step 4 該当する SIP トランクを同期する SIP トランクセキュリティプロファイルをクリックします。

Step 5 追加の設定変更を加えます。

Step 6 [保存（Save）] をクリックします。

Step 7 [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）] ダイアログが表示されます。

Step 8 [OK] をクリックします。

関連トピック

SIP トランクセキュリティプロファイルに関する詳細情報の入手先, on page 14

SIP トランク セキュリティ プロファイルの削除

この項では、Unified Communications Manager データベースから SIP トランク 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

[Unified Communications Manager Administration] からセキュリティ プロファイルを削除する前に、デバイスに別のプロファイルを適用するか、そのプロファイルを使用するすべてのデバイスを削除する必要があります。プロファイルを使用しているデバイスを検索するには、[SIP Trunk Security Profile Configuration] ウィンドウの [Related Links] ドロップダウン リスト ボックスで [Dependency Records] を選択し、[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でない場合は、依存関係レコード概要ウィンドウに、依存関係レコードを有効にするために実行できる操作が表示されます。また、依存関係レコード機能に関連して CPU 負荷が高くなることについての情報も表示されます。依存関係レコードの詳細は、『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

手順

Step 1 削除する SIP トランクセキュリティプロファイルを検索します。

Step 2 次のいずれかの操作を行います。

a) 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**] ウィンドウで次のいずれかのタスクを実行します。

- 削除するセキュリティ プロファイルの隣にあるチェック ボックスをオンにして、[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。

b) 単一のセキュリティプロファイルを削除するには、[**Find And List**] ウィンドウで次のいずれかのタスクを実行します。

- 削除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ます。次に、[**Delete Selected**] をクリックします。
- 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。特定の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、[**選択項目の削除 (Delete Selected)**] をクリックします。

Step 3 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。

関連トピック

SIP トランクセキュリティプロファイルの検索, on page 2
SIP トランクセキュリティプロファイルに関する詳細情報の入手先, on page 14

SIP トランクセキュリティプロファイルに関する詳細情報の入手先

- 認証
- 連携動作
- ダイジェスト認証

関連トピック

SIP トランク セキュリティ プロファイルの設定について, on page 1
SIP トランク セキュリティ プロファイルの設定のヒント, on page 2
認証
連携動作
ダイジェスト認証