SIP トランクのセキュリティ プロファイルのセットアップ

この章では、SIP トランクのセキュリティ プロファイルのセットアップ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

[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] では、SIP トランクに対するセキュリティ関連の設定がグループ化され、1 つのセキュリティ 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ます。セキュリティ関連の設定には、デバイスのセキュリティ モード、ダイジェスト認証、着信転送タイプや発信転送タイプの設定などがあります。[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。

Cisco Unified Communications Manager をインストールすると、自動登録用の事前に定義された非セキュアの 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て、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ていない場合は、非セキュア プロファイルを選択します。

セキュリティ プロファイルの設定ウィンドウに表示されるのは、SIP トランクでサポートされるセキュリティ機能だけです。

SIP トランク セキュリティ プロファイルの設定のヒント

Cisco 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ときは、[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します。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。
- 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、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SIPトランクに適用されます。
- 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 SIP トランクは、新しいプロファイル名および設定を受け入れます。
- Cisco 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 モードを設定すると、Cisco Unified Communications Managerは、SIP トランクのプロファイルを作成し、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 トランクのセキュリティ 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 [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。
[検索と一覧表示（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。

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, （3 ページ） 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。

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 ボックスから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、[フィルタのクリア（Clear Filter）] ボタンをクリックします。

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 ボックス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から、表示するレコードへのリンクをクリックします。
（注） ソートの順番を逆にするには、リストのヘッダーにある上向き矢印または下向き矢印をクリックします。
ウィンドウに選択した項目が表示されます。

関連トピック

SIP トランクのセキュリティ プロファイルに関する詳細情報の入手先, （13 ページ）

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

ステップ 1 [Cisco Unified CM の管理（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）] > [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。

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、[検索対象（Find）] ウィンドウで [新規追加（Add New）] をクリックします
（プロファイルを表示してから、[新規追加（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含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、[コピー（Copy）] 列内にあるそのレコード用の [コピー（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、[コピー（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。

ステップ 3 表 1：SIP トランク セキュリティ プロファイルの構成時の設定, （4 ページ） に示すように、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、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、トランクの [SIP レルム（SIP Realm）] ウィンドウと、その SIP トランクを介して接続されるアプリケーションの [アプリケーション ユーザ（Application User）] ウィンドウで、ダイジェスト信用証明書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（認証）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、そのアプリケーションに許可される方式を設定する必要があります（まだ設定していない場合）。

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, （11 ページ）
SIP トランクのセキュリティ プロファイルに関する詳細情報の入手先, （13 ページ）

SIP トランク セキュリティ プロファイルの設定

次の表は、SIP トランクのセキュリティ プロファイルの設定を示します。

表 *1*：*SIP* トランク セキュリティ プロファイルの構成時の設定

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、[トランクの設定（Trunk Configuration）] ウィンドウで [SIP トランク セキュリティ プロファイル（SIP Trunk 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。
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。

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）]：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 接続が Cisco Unified Communications Manager に対して開きます。 • [認証済（Authenticated）]：Cisco 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）]：Cisco 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ています。AES128/SHA を使用する TLS 接続がシグナリング用に開きます。
[着信転送タイプ（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、TCP+UDP では [転送タイプ（Transport Type）] を指定します。 [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）] である場合、TLS では [転送タイプ（Transport Type）] を指定します。 （注） Transport Layer Security（TLS）プロトコルは Cisco Unified Communications Manager とトランクとの間の接続を保護します。
[発信転送タイプ（Outgoing Transport Type）]	ドロップダウンリストボックス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）] である場合、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）] である場合、TLS では [転送タイプ（Transport Type）] を指定します。 （注） TLS により、SIP トランク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の暗号化が実現します。 ヒント Cisco Unified Communications Manager システムと TCP の再使用をサポートしない IOS ゲートウェイとの間の SIP トランクを接続する場合、出力転送タイプとして UDP を使用する必要があります。

設定	説明
[ダイジェスト認証を有効化（Enable Digest Authentication）]	ダイジェスト認証を有効にする場合に、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、 Cisco Unified Communications Manager はトランクからのすべての SIP 要求をチャレンジします。 ダイジェスト認証は、デバイス認証、整合性、および機密性を提供しません。これらの機能を使用するには、[認証済（Authenticated）] または [暗号化（Encrypted）] のセキュリティ モードを選択します。 **ヒント** ダイジェスト認証を使用して、TCP または UDP 転送を使用している SIP トランク ユーザを認証します。
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。この期限が切れると、Cisco Unified Communications Manager は新しい値を生成します。 **（注）** ナンス値（ダイジェスト認証をサポートする乱数）を使用して、ダイジェスト認証パスワードの MD5 ハッシュを計算します。
X.509 のサブジェクト名（X.509 Subject Name）	このフィールドは、着信および発信転送タイプの TLS を設定する場合に適用します。 デバイス認証には、SIP トランク デバイスの X.509 証明書のサブジェクト名を入力します。 Cisco Unified Communications Manager クラスタがあるか、または TLS ピアに SRV ルックアップを使用すると、単一のトランクは複数のホストに分割され、トランクで複数の X.509 サブジェクト名が発生します。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、最大 4096 文字入力できます。 **ヒント** サブジェクト名はソース接続の TLS 証明書に対応します。サブジェクト名が、サブジェクト名とポートで一意であることを確認します。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 トランク 1 に X.509 のサブジェクト名 my_cm1、my_cm2 があります。ポート 5071 の SIP TLS トランク 2 に X.509 のサブジェクト名 my_cm2、my_cm3 と割り当てることができます。ポート 5061 の SIP TLS トランク 3 には X.509 のサブジェクト名 my_ccm4 を割り当てることはできますが、X.509 サブジェクト名 my_cm1 を割り当てることはできません。

設定	説明
[着信ポート（Incoming Port）]	着信ポートを選択します。0 ～ 65535 の範囲で一意のポート番号を入力します。着信 TCP および UDP SIP メッセージ用のデフォルト ポート値は 5060 です。着信 TLS メッセージ用の SIP のセキュア ポートのデフォルト ポート値は 5061 です。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、SIP TLS 転送トランクと SIP 非 TLS 転送トランク タイプとを混在させることはできません。
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 レベルの認証は、SIP トランクを介して接続される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。Cisco 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 レベルの許可を有効にすると、トランク レベルの認証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、 Cisco Unified Communications Manager は [アプリケーション ユーザ設定（Application User Configuration）] ウィンドウで SIP アプリケーション ユーザに認証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）トランクに対して承認されたメソッドをチェックします。 **ヒント** アプリケーションのアイデンティティを信頼しないか、またはアプリケーションが特定のトランクで信頼されていない場合は、アプリケーション レベルの認証の使用を検討してください。つまり、アプリケーション要求は想定外の別のトランクから送信される場合もあります。

設定	説明
[プレゼンスのSUBSCRIBEの許可（Accept Presence Subscription）]	Cisco Unified Communications Manager が SIP トランク経由でのプレゼンスのサブスクリプション要求を許可するようにするには、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 レベルの認証の有効化（Enable Application Level Authorization）] チェックボックスをオンにしたら、[アプリケーション ユーザ設定（Application User Configuration）] ウィンドウに移動し、この機能を認証されたアプリケーション ユーザの [プレゼンス サブスクリプションを承認（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になっている場合で、[プレゼンス サブスクリプションを承認（Accept Presence Subscription）] のチェックボックスをアプリケーション ユーザ用にはオンにしてトランク用にはオンにしない場合、403 エラー メッセージがトランクに接続された SIP ユーザ エージェントに送信されます。
[ダイアログ外参照の許可（Accept Out-of-Dialog refer）]	Cisco Unified Communications Manager が SIP トランク経由での非インバイト、ダイアログ外参照の受信要求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 レベルの許可の有効化（Enable Application Level Authorization）] チェックボックスをオンにしたら、[アプリケーション ユーザ設定（Application User Configuration）] ウィンドウに移動し、このメソッドで認証されたすべてのアプリケーション ユーザ用の [ダイアログ外参照の許可（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）]	Cisco Unified Communications Manager が SIP トランクを経由する受信非インバイト メッセージ、未承諾通知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 レベルの認証の有効化（Enable Application Level Authorization）] チェックボックスをオンにしたら、[アプリケーション ユーザ設定（Application User Configuration）] ウィンドウに移動し、このメソッドに承認されたすべてのアプリケーション ユーザの [未承認通知を承認（Accept Unsolicited Notification）] チェックボックスをオンにします。

設定	説明
[Replacesヘッダーの許可（Accept replaces header）]	Cisco Unified Communications Manager が既存の SIP ダイアログに代わる新規の SIP ダイアログを許可するようにするには、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 レベルの認証の有効化（Enable Application Level Authorization）] チェックボックスをオンにしたら、[アプリケーション ユーザ設定（Application User Configuration）] ウィンドウに移動し、このメソッドに承認されたすべてのアプリケーション ユーザの [ヘッダー置換を承認（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の送信（Transmit security status）]	Cisco Unified Communications Manager が関連付けられた SIP トランクからの発信のセキュリティ アイコン ステータスを SIP ピアに送信するようにするには、このチェックボックスをオンにします。 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 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 ボックスから、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 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 フィルタリング サービス パラメータ」に示すデフォルト フィルタを使用します。サービス パラメータを検索するには、Cisco Unified Communications Manager Administration で [システム（System）] > [サービス パラメータ（Service Parameters）] > [クラスタワイド パラメータ（デバイス-SIP）（Clusterwide Parameters (Device-SIP)）] に進みます。 • [フィルタリングなし（No Filtering）]：SIP トランクは、アウトバウンド オファーで V.150 SDP 回線のフィルタリングを行いません。 • [MER V.150 の削除（Remove MER V.150）]：SIP トランクは、アウトバウンドオファーの V.150 MER SDP 回線を削除します。トランクが MER V.150 よりも前の Cisco 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。 • [プレ MER V.150 の削除（Remove Pre-MER V.150）]：SIP トランクは、アウトバウンド オファーの非 MER 対応 V.150 回線を全て削除します。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。

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ボックスから、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 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 フィルタリング サービス パラメータ」に示すデフォルト フィルタを使用します。サービス パラメータを検索するには、Cisco Unified Communications Manager Administration で [システム（System）] > [サービス パラメータ（Service Parameters）] > [クラスタワイド パラメータ（デバイス-SIP）（Clusterwide Parameters (Device-SIP)）] に進みます。 • [フィルタリングなし（No Filtering）]：SIP トランクは、アウトバウンド オファーで V.150 SDP 回線のフィルタリングを行いません。 • [MER V.150 の削除（Remove MER V.150）]：SIP トランクは、アウトバウンドオファーの V.150 MER SDP 回線を削除します。トランクが MER V.150 よりも前の Cisco 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。 • [プレ MER V.150 の削除（Remove Pre-MER V.150）]：SIP トランクは、アウトバウンド オファーの非 MER 対応 V.150 回線を全て削除します。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。 （注） セキュアなコールの接続を確立するためには SIP の IOS を V.150 に設定する必要があります。IOS を Cisco Unified Communication 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

許可
ダイジェスト認証
SIP トランク セキュリティ プロファイルの設定のヒント, （2 ページ）
SIP トランクのセキュリティ プロファイルに関する詳細情報の入手先, （13 ページ）

SIP トランク セキュリティ プロファイルの適用

[トランク設定（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

ステップ 1 『*Administration Guide for Cisco Unified Communications Manager*』の説明に従って、トランクを検索します。

ステップ 2 [トランク設定（Trunk Configuration）] ウィンドウが表示されたら、[SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）] 設定を探します。

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 [保存（Save）] をクリックします。

ステップ 5 トランクをリセットするには、[設定を適用（Apply Config）] をクリックします。

次の作業

SIP トランクにダイジェスト認証を有効にしたプロファイルを適用した場合は、[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。

アプリケーション レベルの認証を有効にした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、適切な認証方法を設定する必要があります（まだ設定していない場合）。

関連トピック

SIP レルムの設定
SIP トランクのセキュリティ プロファイルに関する詳細情報の入手先, （13 ページ）

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が行われた SIP トランク 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。作業によるサービスの中断をできるだけ抑えて設定を適用します。（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

ステップ 1 [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）] の順に選択します。
[SIP トランク セキュリティ プロファイルの検索/一覧表示（Find and List SIP Trunk 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 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。

ステップ 4 該当する SIP トランクと同期させる 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。
[SIP トランク セキュリティ プロファイルの設定（SIP Trunk Security Profile Configuration）] ウィンドウが表示されます。

ステップ 5 追加の設定変更を加えます。

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（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。

ステップ 8 [OK] をクリックします。

関連トピック

SIP トランクのセキュリティ プロファイルに関する詳細情報の入手先, （13 ページ）

SIP トランク セキュリティ プロファイルの削除

このセクションでは、Cisco 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。

はじめる前に

Cisco Unified Communications Manager の管理（Cisco 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、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 トランクのセキュリティ プロファイル設定（SIP Trunk Security Profile Configuration）] ウィンドウの [関連リンク（Related Links）] ドロップダウン リスト ボックスで [依存の記録（Dependency Records）] を選択し、[Go] をクリックします。

依存の記録機能がシステムで有効でない場合は、依存記録の概要ウィンドウには依存の記録を有効にするために必要な手順が表示されます。また、依存の記録機能に関連して 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

ステップ 1 削除する SIP トランク セキュリティ プロファイルを探します。

ステップ 2 次のいずれかの作業を実行します。

a) 複数のセキュリティ プロファイルを削除するには、[検索と一覧表示（Find and List）] ウィンドウで次のいずれかの作業を実行します。

- 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、[選択項目の削除（Delete Selected）] をクリックします。
- [すべて選択（Select All）] に続き [選択項目の削除（Delete Selected）] をクリックすると、設定可能なすべてのレコードを削除できます。

b) 単一のセキュリティ プロファイルを削除するには、[検索と一覧表示（Find and List）] ウィンドウで次のいずれかの作業を実行します。

- 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、[選択項目の削除（Delete Selected）] をクリックします。
- 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。特定の [セキュリティ プロファイルの設定（Security Profile Configuration）] 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。

ステップ 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、[キャンセル（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, （2 ページ）
SIP トランクのセキュリティ プロファイルに関する詳細情報の入手先, （13 ページ）

SIP トランクのセキュリティ プロファイルに関する詳細情報の入手先

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, （1 ページ）
SIP トランク セキュリティ プロファイルの設定のヒント, （2 ページ）
許可
インタラクション
ダイジェスト認証