CHAPTER 15

SIP トランク 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。

SIP トランク セキュリティ プロファイルの概要

Cisco Unified Communications Manager の管理ページでは、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 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ことで、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、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。

SIP トランク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。

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 の管理ページで SIP トランク 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。

- 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 プロファイルを適用します。
- 現在デバイスに割り当てられているセキュリティ プロファイルを削除することはできません。
- 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、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 SIP トランクの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。

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

ステップ 1　［システム］>［セキュリティプロファイル］>［SIP トランクセキュリティプロファイル］の順に選択します。

検索と一覧表示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　データベース内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 へ進みます。

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］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］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］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　表示するレコードのリストから、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、P.15-12 の「関連項目」を参照してください。

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 Communications Manager の管理ページで、[**システム**] > [**セキュリティプロファイル**] > [**SIP トランク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　次の作業のどちらかを実行します。

- 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**] をクリックします（プロファイルを表示してから、[**新規追加**] 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、各フィールドのデフォルト設定が示されます。
- 既存のセキュリティ プロファイルをコピーするには、P.15-3 の「SIP トランク 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、[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**] 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、設定内容が示されます。
- 既存のプロファイルを更新するには、P.15-3 の「SIP トランク 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 15-1 の説明に従って、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.15-10 の「SIP トランク セキュリティ プロファイルの適用」の説明に従い、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 レルムの設定（SIP Realm Configuration）] ウィンドウと、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の設定（Application 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（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のアプリケーションレベル許可を有効にした場合は、[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）。

追加情報

詳細については、P.15-12 の「関連項目」を参照してください。

SIP トランク セキュリティ プロファイルの設定内容

表 15-1 で、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。

- 設定のヒントについては、P.15-2 の「SIP トランク 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.15-12 の「関連項目」を参照してください。

表 15-1　SIP トランク セキュリティ プロファイルの設定内容

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（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。
［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］**：イメージ認証以外のセキュリティ機能を適用しない。TCP または UDP 接続で Cisco Unified Communications Manager が利用できる。 • **［認証のみ］**：Cisco Unified Communications Manager はトランク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。 • **［暗号化］**：Cisco Unified Communications Manager はトランクの整合性、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 接続を開始する。 **（注）** SIP トランクは、シグナリング暗号化をサポートします（SRTP はサポートしません）。
［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］** である場合、［TCP+UDP］が転送タイプとなります。 ［デバイスセキュリティモード（Device Security Mode）］が **［認証のみ］** または **［暗号化］** である場合、［TLS］が転送タイプとなります。 **（注）** Transport Layer Security（TLS）プロトコルによって、Cisco Unified Communications Manager とトランクとの間の接続が保護されます。

表 15-1　SIP トランク セキュリティ プロファイルの設定内容（続き）

設定	説明
［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、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］**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**［認証のみ］**または**［暗号化］**である場合、［TLS］が転送タイプとなります。 **（注）** TLS は、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暗号化を実現します。 **ヒント** TCP 接続の再利用をサポートしていない Cisco Unified Communications Manager システムと IOS ゲートウェイの間で SIP トランクを接続する場合は、発信転送タイプとして UDP を使用する必要があります。詳細については、『*Cisco Unified Communications Manager システム ガイド*』の「セッション開始プロトコル（SIP）の概要」を参照してください。
［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、Cisco Unified Communications Manager は、トランクからのすべての 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［認証のみ］または［暗号化］を選択します。 ダイジェスト認証の詳細については、P.1-21 の「ダイジェスト認証」および P.16-1 の「SIP トランクのダイジェスト認証の設定」を参照してください。 **ヒント** TCP 転送または UDP 転送を使用しているトランク上の 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、分）］	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 15-1　SIP トランク セキュリティ プロファイルの設定内容（続き）

設定	説明
［X.509 の件名（X.509 Subject Name）］	このフィールドは、［着信転送タイプ（Incoming Transport Type）］および［発信転送タイプ（Outgoing Transport Type）］に TLS を設定した場合に適用されます。 デバイス認証のために、SIP トランク デバイスの X.509 証明書の件名を入力します。Cisco Unified Communications Manager クラスタがある場合、または TLS ピアに対して SRV ルックアップを使用する場合、単一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。その結果、トランクに複数の X.509 の件名が設定されます。複数の X.509 の件名がある場合は、スペース、カンマ、セミコロン、またはコロンのいずれか 1 つを使用して、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**　件名は、送信元接続の TLS 証明書に対応します。件名が、件名とポートで一意であることを確認してください。同じ件名と着信ポートの組み合せを、異なる SIP トランクに割り当てることはできません。 例：ポート 5061 の SIP TLS trunk1 の［X.509 の件名（X.509 Subject Name）］は、my_cm1, my_cm2 です。ポート 5071 の SIP TLS trunk1 の［X.509 の件名（X.509 Subject Name）］は、my_cm2, my_cm3 です。この場合、ポート 5061 の SIP TLS trunk3 の［X.509 の件名（X.509 Subject Name）］は my_ccm4 にできますが、my_cm1 にはできません。
［着信ポート（Incoming Port）］	着信ポートを選択します。1024 ～ 65535 の一意のポート番号を入力します。着信 TCP および UDP の SIP メッセージのデフォルト ポート値は、5060 です。着信 TLS メッセージの保護されたデフォルト SIP ポートは、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 SIP トランクが、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 トランクが、同じ着信ポートを共有できます。同じポートで、TLS の SIP 転送トランクと、TLS 以外の SIP 転送トランク タイプを混合することはできません。 **ヒント**　通常のトラフィック時に SIP トランク UDP ポート上で単一の IP アドレスからの着信パケット レートが、設定済みの SIP Trunk UDP Port Throttle Threshold を超える場合は、そのしきい値を再設定してください。SIP トランクと SIP ステーションが同じ着信 UDP ポートを共有する場合、Cisco Unified Communications Manager は、2 つのサービス パラメータ値の大きい方に基づいて、パケットをスロットリング（制限）します。このパラメータに対する変更を有効にするには、Cisco CallManager サービスを再起動する必要があります。

表 15-1　SIP トランク セキュリティ プロファイルの設定内容（続き）

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許可は、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は、［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、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 レベルの許可が有効な場合は、まずトランクレベルの許可が発生してから、アプリケーション レベルの許可が発生します。つまり、Cisco 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 ユーザに許可されている方式よりも先に、（このセキュリティ プロファイルで）トランクに許可されている方式を確認します。 **ヒント**　アプリケーションの ID を信頼しない場合、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許可の使用を検討してください。アプリケーション要求は、予期しないトランクから着信することがあります。 トランクのダイジェスト認証設定の詳細については、P.16-1 の「SIP トランクのダイジェスト認証の設定」を参照してください。許可の詳細については、P.1-23 の「許可」および P.1-7 の「相互作用」を参照してください。［アプリケーションユーザの設定（Application User Configuration）］ウィンドウでアプリケーション レベルの許可を設定する方法の詳細については、『*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。
［プレゼンス登録の許可（Accept Presence Subscription）］	Cisco 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、この機能について許可するアプリケーション ユーザの［プレゼンス登録の許可（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許可が有効で、アプリケーション ユーザの［プレゼンス登録の許可（Accept Presence Subscription）］チェックボックスがオンで、トランクのチェックボックスがオフの場合、トランクに接続されている 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。

表 15-1　SIP トランク セキュリティ プロファイルの設定内容（続き）

設定	説明
［アウトオブダイアログ REFER の許可（Accept Out-of-Dialog REFER）］	Cisco Unified Communications Manager が SIP トランク経由で着信する非インバイトのアウトオブダイアログ 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、この方式について許可するアプリケーション ユーザの［アウトオブダイアログ REFER の許可（Accept Out-of-Dialog REFER）］チェックボックスをオンにします。
［未承諾 NOTIFY の許可（Accept Unsolicited Notification）］	Cisco Unified Communications Manager が SIP トランク経由で着信する非インバイトの未承諾 NOTIFY メッセージ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、この方式について許可するアプリケーション ユーザの［未承諾 NOTIFY の許可（Accept Unsolicited Notification）］チェックボックスをオンにします。
［REPLACE ヘッダの許可（Accept Replaces Header）］	Cisco 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、この方式について許可するアプリケーション ユーザの［REPLACE ヘッダの許可（Accept Replaces Header）］チェックボックスをオンにします。

SIP トランク セキュリティ プロファイルの適用

［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 プロファイルをトランクに適用します。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　『*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。

ステップ 2　［トランクの設定（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］**設定を見つけます。

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］**をクリックします。

ステップ 5　**［リセット］**をクリックして、トランクをリセットします。

追加の手順

SIP トランクにダイジェスト認証を有効にするプロファイルを適用した場合は、トランクの［SIP レルムの設定（SIP Realm 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。P.16-6 の「SIP レルムの設定」を参照してください。

アプリケーションレベルの許可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 ユーザの設定（Application User Configuration）］ウィンドウで、ダイジェスト クレデンシャルと可能な許可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）。

追加情報

詳細については、P.15-12 の「関連項目」を参照してください。

SIP トランク 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 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

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、[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、レコードの［依存関係レコード要約（Dependency Records Summary）］ウィンドウに、依存関係レコード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、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も表示されます。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　P.15-3 の「SIP トランク 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　次の作業のどちらかを実行します。

- 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、次の作業のどちらかを実行します。
  - 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。
- 単一のセキュリティ プロファイルを削除するには、検索と一覧ウィンドウで、次の作業のどちらかを実行します。
  - 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。
  - 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.15-12 の「関連項目」を参照してください。

その他の情報

関連項目

- SIP トランク セキュリティ プロファイルの概要（P.15-2）
- SIP トランク セキュリティ プロファイルの設定のヒント（P.15-2）
- SIP トランク セキュリティ プロファイルの検索（P.15-3）
- SIP トランク セキュリティ プロファイルの設定（P.15-4）
- SIP トランク セキュリティ プロファイルの設定内容（P.15-5）
- SIP トランク セキュリティ プロファイルの適用（P.15-10）
- SIP トランク セキュリティ プロファイルの削除（P.15-11）
- 許可（P.1-23）
- 相互作用（P.1-7）
- ダイジェスト認証（P.1-21）

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 Communications Manager システム ガイド