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（P.14-1）
- SIP トランク セキュリティ プロファイルの検索（P.14-2）
- SIP トランク セキュリティ プロファイルの設定（P.14-3）
- SIP トランク セキュリティ プロファイルの設定内容（P.14-4）
- SIP トランク セキュリティ プロファイルの適用（P.14-7）
- SIP トランク セキュリティ プロファイルの削除（P.14-8）
- その他の情報（P.14-9）

SIP トランク 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、着信転送タイプまたは発信転送タイプの設定など、SIP トランク セキュリティ関連の設定がグループ化されます。SIP Trunk Configuration 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 トランクに適用できます。すべての SIP トランクに、セキュリティ プロファイルを適用する必要があります。SIP トランクがセキュリティをサポートしない場合は、ノンセキュア 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　Cisco CallManager Administration で、**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。

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 SIP トランク 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.14-9 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 CallManager Administration で、**System > Security Profile > SIP Trunk Security Profile** 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、**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.14-2 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.14-2 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、ステップ 3 に進みます。

ステップ 3　表 14-1 の説明に従って、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.14-7 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 Realm 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 Application User 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）。

アプリケーションレベル許可 SIP トランクを有効にした場合は、Application User ウィンドウで、そのトランクに許可される方式を設定する必要があります。

追加情報

詳細については、P.14-9 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 14-1 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。Cisco CallManager の方式許可の詳細については、P.1-6 の「対話」を参照してください。

表 14-1　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
Name	セキュリティ プロファイルの名前を入力します。名前は、Trunk Configuration ウィンドウの SIP Trunk Security Profile ドロップダウン リスト ボックスに表示されます。
Description	セキュリティ プロファイルの説明を入力します。
Incoming Transport Type	ドロップダウン リスト ボックスから、着信転送モードを選択します。 **ヒント**　Transport Layer Security（TLS）プロトコルによって、Cisco CallManager とトランクとの間の接続が保護されます。TLS オプションを選択する場合は、Outgoing Transport Type ドロップダウン リスト ボックスでも TLS オプションを選択してください。
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。Incoming Transport Type に TLS を選択した場合は、Outgoing Transport Type にも TLS を選択する必要があります。 **ヒント**　SIP トランク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。
Device Security Mode	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。 • **Non Secure**：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 CallManager が利用できる。 • **Authenticated**：Cisco CallManager 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。 • **Encrypted**：Cisco CallManager 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。 **ヒント**　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）。

表 14-1　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
Enable Digest Authentication	Cisco CallManager が、トランクに接続する SIP ユーザ エージェントの ID でチャレンジを行う場合は、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、トランクは MD5 チェックサム、ユーザ名、パスワード、ナンス値、要求された URI 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、ダイジェスト認証は成功します。 このチェックボックスをオンにすると、Cisco CallManager 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、整合性や信頼性を提供しません。トランクの整合性および信頼性を保証するには、TLS プロトコルを設定します。
Nonce Validity Time	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。 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。
X.509 Subject Name	このフィールドは、Incoming Transport Type および Outgoing Transport Type に TLS を設定した場合に適用されます。 SIP トランクに接続されている認証済みデバイスに対する X.509 証明書の件名を入力します。Cisco CallManager 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 Subject Name は、my_cm1, my_cm2 です。ポート 5071 の SIP TLS trunk1 の 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 Subject Name は my_ccm4 にできますが、my_cm1 にはできません。
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。 入力した値は、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。必要に応じて、同じ着信ポート番号をすべての SIP トランクに設定できます。

表 14-1　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
Enable Application Level Authorization	このチェックボックスをオンにする場合は、Enable Digest Authentication チェックボックスをオンにし、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。トランクのダイジェスト認証設定の詳細については、P.15-1 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。 このチェックボックスをオンにすると、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。アプリケーションレベルの許可は、アプリケーションから SIP ユーザ エージェントで送信された SIP メッセージに対して発生します。アプリケーションレベルの許可は、Application User Configuration ウィンドウ（User Management > Application User）でオンにした許可チェックボックスに基づきます。 **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。
Accept Presence Subscription	Cisco CallManager 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。 Enable Application Level Authorization チェックボックスをオンにした場合は、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 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 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。
Accept Out-of-Dialog Refer	Cisco CallManager が SIP トランク経由で着信する non-INVITE、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。 Enable Application Level Authorization チェックボックスをオンにした場合は、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 Accept Out-of-Dialog Refer チェックボックスをオンにします。
Accept Unsolicited Notification	Cisco CallManager が SIP トランク経由で着信する non-INVITE、Unsolicited Notification 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。 Enable Application Level Authorization チェックボックスをオンにした場合は、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 Accept Unsolicited Notification チェックボックスをオンにします。

表 14-1　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
Accept Header Replacement	Cisco CallManager 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。 Enable Application Level Authorization チェックボックスをオンにした場合は、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 Accept Header Replacement 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

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 CallManager 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　Trunk Configuration ウィンドウが表示されたら、**SIP Trunk Security Profile** 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　**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 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 Realm 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 Application User 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）。P.15-5 の「SIP レルムの設定」を参照してください。

追加情報

詳細については、P.14-9 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 CallManager 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 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、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.14-2 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　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 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 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.14-9 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.14-1）
- SIP トランク セキュリティ プロファイルの検索（P.14-2）
- SIP トランク セキュリティ プロファイルの設定（P.14-3）
- SIP トランク セキュリティ プロファイルの設定内容（P.14-4）
- SIP トランク セキュリティ プロファイルの適用（P.14-7）
- SIP トランク セキュリティ プロファイルの削除（P.14-8）

シスコの関連マニュアル

Cisco CallManager アドミニストレーション ガイド