



# 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 \(P.14-2\)](#)
- [SIP トランク セキュリティ プロファイルの設定のヒント \(P.14-2\)](#)
- [SIP トランク セキュリティ プロファイルの検索 \(P.14-3\)](#)
- [SIP トランク セキュリティ プロファイルの設定 \(P.14-4\)](#)
- [SIP トランク セキュリティ プロファイルの設定内容 \(P.14-5\)](#)
- [SIP トランク セキュリティ プロファイルの適用 \(P.14-10\)](#)
- [SIP トランク セキュリティ プロファイルの削除 \(P.14-11\)](#)
- [その他の情報 \(P.14-12\)](#)

## SIP トランク セキュリティ プロファイルの概要

Cisco Unified CallManager 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可能です。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 CallManager 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 CallManager 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 CallManager 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 CallManager 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** Cisco Unified CallManager 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。

[SIP トランクセキュリティプロファイルの検索と一覧表示 (Find and List SIP Trunk Security Profiles)] ウィンドウが表示されます。

- ステップ 2** 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条件を選択し、[検索] 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、検索条件を指定せずに、[検索] をクリックします。

ウィンドウが更新され、検索条件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 [名前 (Name)] リンクをクリックします。



**ヒント** 検索結果内の [名前 (Name)] または [説明] を検索するには、[絞り込み] 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条件を入力し、[検索] をクリックします。

### 追加情報

詳細については、P.14-12 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 CallManager 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、[新規追加] 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.14-3](#) 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て表示し、[コピー] ボタンをクリックして、[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.14-3](#) 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、[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** [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.14-10](#) 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alm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.14-12](#) 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 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。

- 設定のヒントについては、P.14-2 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.14-12 の「関連項目」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
[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)]	<p>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。</p> <ul style="list-style-type: none"> <li>• <b>[Non Secure]</b> : 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 CallManager が利用できる。</li> <li>• <b>[Authenticated]</b> : Cisco Unified 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。</li> <li>• <b>[Encrypted]</b> : Cisco Unified CallManager 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。</li> </ul> <p> (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)。</p>
[着信転送タイプ (Incoming Transport Type)]	<p>[デバイスセキュリティモード (Device Security Mode)] が <b>[Non Secure]</b> である場合、[TCP+UDP] が転送タイプとなります。</p> <p>[デバイスセキュリティモード (Device Security Mode)] が <b>[Authenticated]</b> または <b>[Encrypted]</b> である場合、[TLS] が転送タイプとなります。</p> <p> (注) Transport Layer Security (TLS) プロトコルによって、Cisco Unified CallManager とトランクとの間の接続が保護されます。</p>

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
[発信転送タイプ (Outgoing Transport Type)]	<p>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。</p> <p>[デバイスセキュリティモード (Device Security Mode)] が [Non Secure] である場合、[TCP] または [UDP] を選択します。</p> <p>[デバイスセキュリティモード (Device Security Mode)] が [Authenticated] または [Encrypted] である場合、[TLS] が転送タイプとなります。</p> <hr/> <p> (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。</p> <hr/> <p> ヒント TCP 接続の再利用をサポートしていない Cisco Unified CallManager 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 CallManager 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。</p>
[ダイジェスト認証を有効化 (Enable Digest Authentication)]	<p>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 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。</p> <p>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 [Authenticated] または [Encrypted] を選択します。</p> <p>ダイジェスト認証の詳細については、P.1-18 の「ダイジェスト認証」および 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。</p> <hr/> <p> 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。</p>
[ナンス確認時間 (Nonce Validity Time、分)]	<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 Unified CallManager は新しい値を生成します。</p> <hr/> <p> (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。</p>

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
[X.509 の件名 (X.509 Subject Name)]	<p data-bbox="711 315 1471 412">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。</p> <p data-bbox="711 439 1471 678">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 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。</p> <p data-bbox="711 705 1289 734">このフィールドには、4096 文字まで入力できます。</p> <p data-bbox="711 757 791 801"></p> <p data-bbox="711 808 1471 931"><b>ヒント</b> 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わせを、異なる SIP トランクに割り当てることはできません。</p> <p data-bbox="823 969 1471 1155">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。</p>
[着信ポート (Incoming Port)]	<p data-bbox="711 1184 1471 1350">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。</p> <p data-bbox="711 1377 791 1422"></p> <p data-bbox="711 1429 1471 1581"><b>ヒント</b> TLS 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。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。</p>

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
[アプリケーションレベル認証を有効化 (Enable Application Level Authorization)]	<p>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。</p> <p>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 CallManager 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。</p> <p>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 CallManager 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。</p>
	<p> <b>ヒント</b> 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。</p>
	<p>トランクのダイジェスト認証設定の詳細については、<a href="#">P.15-1</a> の「<a href="#">SIP トランクのダイジェスト認証の設定</a>」を参照してください。許可の詳細については、<a href="#">P.1-20</a> の「<a href="#">許可</a>」および <a href="#">P.1-6</a> の「<a href="#">相互作用</a>」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、『<a href="#">Cisco Unified CallManager アドミニストレーションガイド</a>』を参照してください。</p>
[プレゼンス登録の許可 (Accept Presence Subscription)]	<p>Cisco Unified 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。</p> <p>[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。</p> <p>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。</p>



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
[アウトオブダイアログ REFER の許可 (Accept Out-of-Dialog REFER)]	<p>Cisco Unified CallManager 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。</p> <p>[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。</p>
[未承諾 NOTIFY の許可 (Accept Unsolicited Notification)]	<p>Cisco Unified CallManager 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。</p> <p>[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。</p>
[REPLACE ヘッダの許可 (Accept Replaces Header)]	<p>Cisco Unified 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。</p> <p>[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。</p>

## 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 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** [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 (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** [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.15-5 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.14-12 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 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 Unified CallManager 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、[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 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.14-3 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** 複数のセキュリティ プロファイルを削除するには、[SIP トランクセキュリティプロファイルの検索と一覧表示 (Find and List SIP Trunk Security Profiles)] 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、[選択項目の削除] アイコンまたは [選択項目の削除] 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。
  - [SIP トランクセキュリティプロファイルの検索と一覧表示 (Find and List SIP Trunk Security Profiles)] 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、[選択項目の削除] アイコンまたは [選択項目の削除] ボタンをクリックします。
  - [SIP トランクセキュリティプロファイルの検索と一覧表示 (Find and List SIP Trunk Security Profiles)] ウィンドウで、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 [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たら、[削除] アイコンまたは [削除] 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、[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.14-12 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 \(P.14-2\)](#)
- [SIP トランク セキュリティ プロファイルの設定のヒント \(P.14-2\)](#)
- [SIP トランク セキュリティ プロファイルの検索 \(P.14-3\)](#)
- [SIP トランク セキュリティ プロファイルの設定 \(P.14-4\)](#)
- [SIP トランク セキュリティ プロファイルの設定内容 \(P.14-5\)](#)
- [SIP トランク セキュリティ プロファイルの適用 \(P.14-10\)](#)
- [SIP トランク セキュリティ プロファイルの削除 \(P.14-11\)](#)
- [許可 \(P.1-20\)](#)
- [相互作用 \(P.1-6\)](#)
- [ダイジェスト認証 \(P.1-18\)](#)

### シスコの関連マニュアル

*Cisco Unified CallManager* アドミニストレーションガイド

*Cisco Unified CallManager* システムガイド