



トランクとゲートウェイのSIPセキュリティ

- トランクとゲートウェイの SIP セキュリティの概要, on page 1
- トランクとゲートウェイの SIP セキュリティ設定タスクフロー, on page 5

トランクとゲートウェイの SIP セキュリティの概要

このセクションでは、SIP トランクの暗号化、ゲートウェイの暗号化の概要、およびセキュリティプロファイル設定のヒントについて説明します。

SIP トランクの暗号化

SIP トランクは、シグナリングとメディアの両方でセキュアなコールをサポートできます。TLS はシグナリング暗号化を提供し、SRTP はメディア暗号化を提供します。

トランクのシグナリング暗号化を設定するには、SIP トランク セキュリティ プロファイルを設定するときに次のオプションを選択します（[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）] ウィンドウ）。

- [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、“[暗号化済（Encrypted）]” を選択します。
- [着信転送タイプ（Incoming Transport Type）] ドロップダウンリストから “[TLS]” を選択します。
- [発信転送タイプ（Outgoing Transport Type）] ドロップダウンリストから “[TLS]” を選択します。

SIP トランク セキュリティ プロファイルを設定した後、トランクに適用します（[デバイス（Device）] > [トランク（Trunk）] > [SIP トランク（SIP Trunk）] 設定ウィンドウ）。

トランクに対してメディア暗号化を設定するには、[SRTPを許可（SRTP Allowed）] チェックボックスをオンにします（[デバイス（Device）] [トランク] [SIP トランク（SIP Trunk）] 設定ウィンドウでも同様です）。

**Caution**

このチェックボックスをオンにする場合は、キーやその他のセキュリティ関連情報がコールネゴシエーション中に公開されないように、暗号化された TLS プロファイルを使用することを推奨します。非セキュアプロファイルを使用する場合でも SRTP は機能しますが、キーはシグナリングおよびトレースで公開されます。この場合、Unified Communications Manager とトランクの接続先間でネットワークのセキュリティを確保する必要があります。

Cisco IOS MGCP ゲートウェイの暗号化

Unified Communications Manager は、MGCP SRTP パッケージを使用するゲートウェイをサポートしています。MGCP SRTP パッケージは、ゲートウェイがセキュア RTP 接続上でパケットを暗号化および復号化するときに使用されます。コールセットアップ中に交換される情報によって、ゲートウェイがコールに SRTP を使用するかどうかが決まります。デバイスが SRTP をサポートしている場合、システムは SRTP 接続を使用します。少なくとも1つのデバイスが SRTP をサポートしていない場合、システムは RTP 接続を使用します。SRTP から RTP へのフォールバック（またはその逆）は、安全なデバイスから安全ではないデバイスへの転送、会議、トランスコーディング、保留音などの場合に発生する可能性があります。

システムが2台のデバイス間で暗号化 SRTP コールを設定する場合、Unified Communications Manager はセキュアコール用のマスター暗号化キーと salt を生成し、SRTP ストリーム専用のゲートウェイに送信します。Unified Communications Manager は SRTCP ストリーム用のキーと salt を送信しませんが、ゲートウェイはこれらもサポートします。これらのキーは、MGCP シグナリングパスを介してゲートウェイに送信されます。このパスは IPSec を使用して保護する必要があります。Unified Communications Manager は IPSec 接続が存在するかどうかを認識しませんが、IPSec が設定されていない場合、システムはゲートウェイにセッションキーをクリアテキストで送信します。セッションキーがセキュアな接続を介して送信されるよう、IPSec 接続が存在することを確認します。

**Tip**

SRTP 用に設定されている MGCP ゲートウェイが、認証済みデバイス（たとえば、SCCP を実行している認証済み電話機）とのコールに関与している場合、Unified Communications Manager がコールを認証済みとして分類するため、電話機に保護アイコンが表示されます。Unified Communications Manager は、デバイスの SRTP 機能がコールのネゴシエートに成功した場合、コールを暗号化として分類します。MGCP ゲートウェイが、セキュリティアイコンを表示できる電話に接続されている場合、コールが暗号化されているときは電話に鍵アイコンが表示されます。

次に、MGCP E1 PRI ゲートウェイについての説明を示します。

- SRTP 暗号化の MGCP ゲートウェイを設定する必要があります。コマンド **mgcppackage-capabilitysrtp-package** を使用してゲートウェイを設定します。
- MGCP ゲートウェイでは、[高度な IP サービス (Advanced IP Services)] または [高度な企業サービス (Advanced Enterprise Services)] イメージを指定する必要があります。
たとえば、**c3745-adventerprisek9-mz.124-6.T.bin** など。

- 保護ステータスは、COCP PRI Setup、Alert、および Connect の各メッセージで独自の FacilityIE を使用して、交換用の CP E1 PRI ゲートウェイと交換されます。
- Unified Communications Manager は、Cisco Unified IP Phone でのみセキュア通知トーンを再生します。ネットワーク内の PBX は、コールのゲートウェイ側にトーンを再生します。
- Cisco Unified IP Phone と MGCP E1 PRI ゲートウェイの間のメディアが暗号化されていないと、コールはドロップされます。



Note MGCP ゲートウェイの暗号化の詳細については、使用している Cisco IOS ソフトウェアのバージョンの『*Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*』を参照してください。

H.323 ゲートウェイおよび h.323/h.323/h トランク暗号化 (h.323)

セキュリティをサポートする H.323 ゲートウェイおよびゲートキーパー、または非ゲートキーパー制御の H.225/H.323/H.245 トランクは、Cisco Unified Communications Operating System で IPsec アソシエーションを設定した場合、Unified Communications Manager に対して認証できます。Unified Communications Manager とこれらのデバイスの間での IPsec アソシエーション作成については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

H.323、H.225、および H.245 デバイスでは暗号キーが生成されます。これらのキーは、IPsec で保護されたシグナリングパスを介して Unified Communications Manager に送信されます。Unified Communications Manager は IPsec 接続が存在するかどうかを認識しませんが、IPsec が設定されていない場合、セッションキーは暗号化されずに送信されます。セッションキーがセキュアな接続を介して送信されるよう、IPsec 接続が存在することを確認します。

IPsec アソシエーションの設定に加えて、Unified Communications Manager Administration のデバイス設定ウィンドウにある [SRTP 許可 (SRTP Allowed)] チェックボックスにマークを付ける必要があります。これは H.323 ゲートウェイ、H.225 トランク (ゲートキーパー制御)、クラスタ間トランク (ゲートキーパー制御)、およびクラスタ間トランク (非ゲートキーパー制御) の設定ウィンドウなどに存在します。このチェックボックスをオンにしない場合、Unified Communications Manager は RTP を使用してデバイスと通信します。このチェックボックスをオンにする場合、Unified Communications Manager は SRTP がデバイスに対して設定されているかどうかに応じて、セキュア コールと非セキュア コールを許可します。



Caution

Unified Communications Manager Administration で [SRTP を許可 (SRTP Allowed)] チェックボックスをオンにする場合は、セキュリティ関連情報が暗号化されずに送信されることを防ぐために、IPsec を設定することを強く推奨します。

Unified Communications Manager は、IPsec 接続が正しく設定されたかどうかを確認しません。接続を正しく設定しないと、セキュリティ関連の情報がクリアテキストで送信されることがあります。

セキュアメディアパスまたはセキュアシグナリングパスを確立でき、デバイスが SRTP をサポートする場合、システムは SRTP 接続を使用します。セキュアメディアパスまたはセキュアシグナリングパスを確立できないか、1 つ以上のデバイスが SRTP をサポートしない場合、システムは RTP 接続を使用します。SRTP から RTP へのフォールバック（またはその逆）は、安全なデバイスから安全ではないデバイスへの転送、会議、トランスコーディング、保留音などの場合に発生する可能性があります。

**Tip**

コールがパススルー対応 MTP を使用し、リージョンフィルタ処理の後でデバイスの音声機能が一致し、どのデバイスについても [MTP が必要かどうか (MTP Required)] チェックボックスがオンになっていない場合、Unified Communications Manager はそのコールをセキュアとして分類します。[MTP Required] チェックボックスがオンの場合、Unified Communications Manager はコールの音声パススルーを無効にし、コールを非セキュアとして分類します。MTP がコールに関係しない場合、Unified Communications Manager はデバイスの SRTP 機能に応じてそのコールを暗号化済みに分類することがあります。

Unified Communications Manager は、そのデバイスの [SRTP Allowed] チェックボックスがオンで、そのデバイスの SRTP 機能がコールに対して正常にネゴシエートされれば、コールを暗号化済みに分類します。前述の条件を満たさない場合、Unified Communications Manager はコールを非セキュアとして分類します。デバイスが、セキュリティアイコンを表示できる電話に接続されている場合、コールが暗号化されているときは電話機に鍵アイコンが表示されます。

Unified Communications Manager は、トランクまたはゲートウェイ経由の発信 FastStart コールを非セキュアとして分類します。Unified Communications Manager Administration で [SRTP を許可する (SRTP Allowed)] チェックボックスをオンにした場合、Unified Communications Manager により [アウトバウンド FastStart を有効にする (Enable Outbound FastStart)] チェックボックスがオフになります。

Unified Communications Manager の一部の種類のゲートウェイおよびトランクでは、共有秘密キー (Diffie-Hellman キー) やその他の H.235 データを 2 つの H.235 エンドポイント間で透過的にパススルーさせることができます。このため、これら 2 つのエンドポイントではセキュアメディアチャネルを確立できます。

[H.235 data] の通過を有効にするには、次のトランクおよびゲートウェイの構成時の設定で [h.235 パススルーを許可する] チェックボックスをオンにします。

- 「-225 Trunk」
- ICT ゲートキーパー制御
- ICT 非ゲートキーパー制御
- H.323 ゲートウェイ

トランクとゲートウェイの設定の詳細については、『Administration Guide for Cisco Unified Communications Manager』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。

トランクとゲートウェイの SIP セキュリティ設定タスクフロー

このセクションでは、すべてのトランクとゲートウェイの SIP セキュリティの設定について説明します。

セキュアゲートウェイとトランクのセットアップ

この手順は、Cisco IOS のメディアおよびシグナリングの認証および暗号化機能と組み合わせて使用します。これにより、セキュリティのために Cisco IOS の管理用 cp ゲートウェイを設定する方法に関する情報が提供されます。

Procedure

Step 1 `ctls ctl` コマンドを実行してクラスタを混合モードに設定したことを確認します。

Step 2 電話機が暗号化用に設定されていることを確認します。

Step 3 IPSec を設定します。

Tip ネットワーク インフラストラクチャで IPSec を設定することも、Unified Communications Manager とゲートウェイまたはトランクとの間で IPSec を設定することもできます。IPSec を設定するために 1 つの方式を実装する場合、他の方式を実装する必要はありません。

Step 4 H.323 IOS ゲートウェイおよびクラスタ間トランクの場合、Unified Communications Manager で [SRTPを許可する (SRTP Allowed)] チェックボックスをオンにします。

[SRTPを許可する (SRTP Allowed)] チェックボックスは、[トランクの設定 (Trunk Configuration)] ウィンドウまたは [ゲートウェイの設定 (Gateway Configuration)] ウィンドウに表示されます。これらのウィンドウを表示する方法については、[Cisco Unified Communications Manager アドミニストレーションガイド](#)のトランクおよびゲートウェイに関する章を参照してください。

Step 5 SIP トランクの場合、SIP トランク セキュリティプロファイルを設定し、トランクに適用します（この処理を行っていない場合）。また、でも [SRTPを許可する (SRTP Allowed)] チェックボックスをオンにします。[デバイス (Device)] > [トランク (Trunk)] > [SIP トランク設定 (SIP Trunk Configuration)] 閉じます。

Caution [SRTPを許可する (SRTP Allowed)] チェックボックスをオンにする場合、コール ネゴシエーション中にキーやその他のセキュリティ関連情報が公開されないようにするために、暗号化された TLS プロファイルを使用することを推奨します。非セキュアプロファイルを使用すると、SRTP は機能しますが、キーはシグナリングおよびトレースで公開されます。この場合、Unified Communications Manager とトランクの接続先間でネットワークのセキュリティを確保する必要があります。

Step 6 ゲートウェイでセキュリティ関連の設定タスクを実行します。

詳細については、『*Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*』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。

Procedure

-
- Step 1** Cisco Unified Communications Manager Administration から次を選択します。[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)]。
- Step 2** 次のいずれかの操作を行います。
- 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。
 - 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。
 - 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](#)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alm (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)。
-

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。

Table 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。
デバイスセキュリティモード SIP	<p>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。</p> <ul style="list-style-type: none"> • [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。 <p>Note [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。</p> <p>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。</p> <p>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。</p>

設定	説明
着信転送タイプ	<p>[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。</p> <p>[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。</p> <p>Note 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。</p>
発信転送タイプ	<p>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。</p> <p>[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。</p> <p>[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。</p> <p>Note 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。</p> <p>Tip 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。</p>
ダイジェスト認証の有効化	<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、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。</p> <p>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。</p> <p>Tip 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。</p>
ナンス確認時間	<p>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。</p> <p>Note 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。</p>

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	<p>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。</p> <p>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。</p> <p>このフィールドには、4096 文字まで入力できます。</p> <p>Tip 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。</p>
着信ポート	<p>着信ポートを選択します。0 ~ 65535 の範囲の一意的なポート番号値を 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。</p> <p>Tip 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。</p>

設定	説明
アプリケーションレベル認証を有効化	<p>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。</p> <p>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。</p> <p>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。</p> <p>Tip 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。</p>
プレゼンスサブスクリプションの許可	<p>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。</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。</p> <p>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。</p>

設定	説明
Out-of-Dialog REFER の許可	<p>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。</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。</p>
Unsolicited NOTIFY の許可	<p>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。</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。</p>
ヘッダー置き換えの許可	<p>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。</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。</p>
セキュリティステータスを送信	<p>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。</p> <p>デフォルトでは、このボックスはオフになっています。</p>

設定	説明
SIP V.150アウトバウンドSDPオファァのフィルタリング	<p>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。</p> <ul style="list-style-type: none"> • [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 オファァのフィルタリング (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。サービスパラメータを見つけるには、次のように進みます。[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))] (Cisco Unified Communications Manager Administration) 。 • [フィルタなし (No Filtering)]: SIP トランクは、アウトバウンドオファァ内の 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ァ内の 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ァで非 MER 対応 V.150 回線をすべて削除します。クラスタがプレ MER 回線でオファァを処理できない 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	<p>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。</p> <ul style="list-style-type: none"> • [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。サービスパラメータを見つけるには、次のように進みます。 [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))] (Cisco Unified Communications Manager Administration) 。 • [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。 <p>Note 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。</p>

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。

Procedure

- 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alm (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)。

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。)

Procedure

- Step 1** 選択 [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)]。
- 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。

IPsec の設定

IPsec は、暗号セキュリティ サービスを使用した IP ネットワーク経由の非公開でセキュアな通信を保証するフレームワークです。IPsec ポリシーが IPsec セキュリティ サービスの設定に使用され

ます。このポリシーは、ネットワーク上のほとんどのトラフィックタイプにさまざまなレベルの保護を提供します。コンピュータ、部門（OU）、ドメイン、サイト、またはグローバル企業のセキュリティ要件を満たすように IPsec ポリシーを設定できます。

Cisco Unified Communications Manager Administration を使用した SRTP の許可

[SRTP を許可する（SRTP Allowed）] チェックボックスは、Unified Communications Manager の次の設定ウィンドウに表示されます。

- H.323 ゲートウェイの設定ウィンドウ
- [H.225 Trunk (Gatekeeper Controlled) Configuration] ウィンドウ
- [Inter-Cluster Trunk (Gatekeeper Controlled) Configuration] ウィンドウ
- [Inter-Cluster Trunk (Non-Gatekeeper Controlled) Configuration] ウィンドウ
- [SIP トランクの設定 (SIP Trunk Configuration)] ウィンドウ

H.323 ゲートウェイ、ゲートキーパー制御または非ゲートキーパー制御の H.323/H.245/H.225 トランク、SIP トランクの [SRTP Allowed] チェックボックスを設定するには、次の手順を実行します。

Procedure

-
- Step 1** Unified Communications Manager の説明に従って、ゲートウェイまたはトランクを検索します。
- Step 2** ゲートウェイまたはトランクの設定ウィンドウを開いた後、[SRTP を許可する（SRTP Allowed）] チェックボックスをオンにします。
- Caution** SIP トランクの [SRTP を許可する（SRTP Allowed）] チェックボックスをオンにする場合は、キーや他のセキュリティ関連の情報がネゴシエーション中に公開されないように TLS 暗号化プロファイルの使用を推奨します。非セキュアプロファイルを使用すると、SRTP は機能しますが、キーはシグナリングおよびトレースで公開されます。この場合、Unified Communications Manager とトランクの接続先間でネットワークのセキュリティを確保する必要があります。
- Step 3** [保存（Save）] をクリックします。
- Step 4** デバイスをリセットするには、[Reset] をクリックします。
- Step 5** IPsec が H323 に対して正しく設定されていることを確認します。（SIP の場合は、TLS が正しく設定されていることを確認してください）。
-