ゲートウェイおよびトランクの暗号化の設定

この章では、ゲートウェイおよびトランクの暗号化の設定について説明します。

- Cisco IOS MGCP ゲートウェイの暗号化 （1 ページ）
- H.323 ゲートウェイおよび H.323/H.225/H.245 トランクの暗号化 （2 ページ）
- SIP トランクの暗号化 （4 ページ）
- セキュアなゲートウェイとトランクのセットアップ （4 ページ）
- ネットワーク インフラストラクチャ内の IPSec 設定 （5 ページ）
- Cisco Unified Communications Manager とゲートウェイまたはトランクとの間の IPSec の設定 （6 ページ）
- Cisco Unified Communications Manager Administration を使用した SRTP の許可 （6 ページ）
- ゲートウェイとトランクの暗号化に関する詳細情報の入手先 （7 ページ）

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。ゲートウェイはこれを使用してセキュアな RTP 接続を介したパケットの暗号化と復号を行います。コールセットアップの間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定されます。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。1 つ以上のデバイスが 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。

システムによって 2 つのデバイス間に SRTP コールがセットアップされると、Unified Communications Manager によってセキュアなコール用のマスター暗号化キーとソルトが生成され、SRTP ストリーム用のみゲートウェイに送信されます。ゲートウェイでは SRTCP ストリームのキーとソルトもサポートされていますが、Unified Communications Manager では送信されません。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 では IPSec 接続の有無が認識されませんが、IPSec が設定されていないとシステムではセッションキーが

クリア テキストでセッションに送信されます。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。

ヒント SRTP に設定された MGCP ゲートウェイが、SCCP の動作している認証済み電話などの認証済みデバイスとのコールに関係している場合、シールドアイコンが電話に表示されます。Unified Communications Manager ではこれらのコールが認証済みとして分類されるためです。コールについてそのデバイスの SRTP 機能のネゴシエーションが成功すると、Unified Communications Manager ではそのコールが認証済みとして分類されます。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。

H.323 ゲートウェイおよび H.323/H.225/H.245 トランクの暗号化

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。

注意 Unified Communications Manager Administration で [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。接続が正しく設定されていないと、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。

ヒント コールがパススルー対応 MTP を使用し、リージョン フィルタリング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 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。 コールを暗号化済みとして分類します。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 Allowed] チェックボックスをオンにした場合、Unified Communications Manager は **[Enable Outbound FastStart]** チェックボックスをオフにします。

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 データのパススルーを有効にするには、次のトランクおよびゲートウェイの設定で、[H.235 pass through allowed] チェックボックスをオンにします。

- H.225 トランク

- 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 トランクの暗号化

SIP トランクは、シグナリングとメディア両方のセキュア コールをサポートできます。TLS がシグナリング暗号化を提供し、SRTP が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際に次のオプションを選択します（**[System]** > **[Security Profile]** > **[SIP Trunk Security Profile] ウィンドウ**）。

- [Device Security Mode] ドロップダウン リストから 「[Encrypted]」 を選択します。
- [Incoming Transport Type] ドロップダウン リストから 「[TLS]」 を選択します。
- [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、プロファイルをトランクに適用します（**[Device]** > **[Trunk]** > **[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 Allowed] チェック ボックスをオンにします（[Device] > [Trunk] > [SIP Trunk] 設定ウィンドウも同様です）。

⚠

注意 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強く推奨します。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 と接続先のトランク間でのネットワーク セキュリティを確保する必要があります。

セキュアな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 MGCP ゲートウェイでセキュリティを設定する方法について説明しているマニュアル『*Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*』とともに使用してください。

手順

ステップ 1 Cisco CTL クライアントをインストールし、設定したことを確認します。クラスタ セキュリティ モードが混合モードであることを確認します。

ステップ 2 電話に暗号化を設定したことを確認します。

ステップ 3 IPSec を設定します。

ヒント 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。

ステップ 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 Administration] で [SRTP Allowed] チェックボックスをオンにします。

[SRTP Allowed] チェックボックスは、[Trunk Configuration] ウィンドウまたは [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、『*Administration Guide for Cisco Unified Communications Manager*』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。

ステップ 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、**[Device]** > **[Trunk]** > **[SIP Trunk]** の設定ウィンドウで 「[SRTP Allowed]」 チェックボックスを必ずオンにします。

注意 「[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強く推奨します。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 と接続先のトランク間でのネットワーク セキュリティを確保する必要があります。

ステップ 6 ゲートウェイの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。

ネットワーク インフラストラクチャ内の IPSec 設定

ここでは、IPSec の設定方法については説明しません。代わりに、ネットワーク インフラストラクチャで IPSec を設定する際の考慮事項と推奨事項について記載されています。ネットワーク インフラストラクチャ内で IPSec を設定する予定であり、Unified Communications Manager とデバイスの間では設定しない場合、IPSec の設定前に次の情報を検討してください。

- Unified Communications Manager 自体ではなく、インフラストラクチャの中で IPSec をプロビジョニングすることを推奨します。
- IPSec を設定する前に、既存の IPSec 接続または VPN 接続、プラットフォームの CPU への影響、帯域幅への影響、ジッタや遅延などのパフォーマンス メトリックについて考慮します。
- 『*Voice and Video Enabled IPSec Virtual Private Networks Solution Reference Network Design Guide*』を参照します。
- 『*Cisco IOS Security Configuration Guide, Release 12.2*』（またはそれ以降）を参照します。
- IPSec 接続のリモート エンドをセキュアな Cisco IOS MGCP ゲートウェイで終端します。
- テレフォニー サーバが存在するネットワークの信頼されている領域内のネットワーク デバイスでホストを終端します（ファイアウォールの背後、アクセス コントロール リスト（ACL）またはその他のレイヤ 3 デバイスなど）。
- ホスト側 IPSec 接続の終端に使用する機器は、ゲートウェイの数とそれらのゲートウェイに予想されるコールの量とによって決まります。たとえば、Cisco VPN 3000 シリーズ コンセントレータ、Catalyst 6500 IPSec VPN サービス モジュール、Cisco サービス統合型ルータなどがあります。
- セキュアなゲートウェイとトランクの設定の関連項目で指定されている順序で、手順を実行します。

注意 IPSec 接続を設定してその接続がアクティブであることを確認しないと、メディア ストリームのプライバシーが損なわれる可能性があります。

Cisco Unified Communications Manager とゲートウェイまたはトランクとの間の IPSec の設定

Unified Communications Manager と、この章で説明されているゲートウェイやトランクとの間の IPSec の設定に関する情報については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

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

[SRTP Allowed] チェックボックスは [Unified Communications Manager Administration] の以下の設定ウィンドウで表示されます。

- [H.323 Gateway Configuration] 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 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。

手順

ステップ 1 『*Administration Guide for Cisco 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。

ステップ 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 Allowed] チェックボックスをオンにします。

注意 SIP トランクの 「[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ることを防止するため、TLS 暗号化プロファイルの使用を強く推奨します。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 と接続先のトランク間でのネットワーク セキュリティを確保する必要があります。

ステップ 3 **[Save]** をクリックします。

ステップ 4 デバイスをリセットするには、[Reset] をクリックします。

ステップ 5 IPSec が H323 向けに正しく設定されたことを確認します。（SIP の場合は、TLS が正しく設定されたことを確認してください。）

ゲートウェイとトランクの暗号化に関する詳細情報の入手先

- 認証、整合性、および許可
- 暗号化

ゲートウェイとトランクの暗号化に関する詳細情報の入手先