CHAPTER 24

ゲートウェイおよびトランクの暗号化の設定

この章は、次の内容で構成されています。

Cisco IOS MGCP ゲートウェイの暗号化の概要

Cisco 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。コール設定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判別されます。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。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（およびその逆の）フォールバックは、セキュア デバイスから非セキュア デバイスへの転送、電話会議、トランスコーディング、保留音などで発生する場合があります。

システムが 2 つのデバイス間で暗号化済み SRTP コールを設定すると、Cisco Unified Communications Manager はセキュア コールのためのマスター暗号鍵とソルトを生成し、SRTP ストリームの場合にのみゲートウェイに送信します。ゲートウェイでもサポートされている SRTCP ストリームの場合、Cisco Unified Communications Manager は鍵とソルトを送信しません。これらの鍵は 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。これは、IPSec を使用してセキュリティを設定する必要があります。Cisco 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鍵を暗号化せずに送信します。セッション鍵がセキュア接続を介して送信されるように、IPSec 接続が存在することを確認します。

ヒント　SRTP 用に設定された MGCP ゲートウェイが、認証されたデバイス（SCCP を実行する認証された電話機など）とのコールに関わる場合、Cisco Unified Communications Manager はこのコールを認証済みとして分類するため、電話機にシールド アイコンが表示されます。コールに対してデバイスの SRTP 機能が正常にネゴシエートされると、Cisco Unified Communications Manager は、このコールを暗号化済みとして分類します。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機に接続されている場合、コールが暗号化されていると、電話機にロック 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 トランクの暗号化の概要

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 オペレーティング システムで IPSec アソシエーションを設定した場合、Cisco Unified Communications Manager に対して認証ができます。Cisco Unified Communications Manager とこれらのデバイスとの間で IPSec アソシエーションを作成する方法については、『*Cisco Unified Communications Operating System Administration Guide*』を参照してください。

H.323、H.225、および H.245 デバイスは暗号鍵を生成します。これらの鍵は、IPSec で保護されたシグナリング パスを介して Cisco Unified Communications Manager に送信されます。Cisco 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、セッション鍵は暗号化されずに送信されます。セッション鍵がセキュア接続を介して送信されるように、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、Cisco Unified Communications Manager の管理のデバイス設定ウィンドウで [SRTP を許可(SRTP Allowed)] チェックボックスをオンにする必要があります。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）、クラスタ間トランク（非ゲートキーパー制御）などのデバイス設定ウィンドウがあります。このチェックボックスをオンにしない場合、Cisco 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した場合、Cisco Unified Communications Manager は、デバイスに対して SRTP が設定されているかどうかに応じて、セキュア コールまたは非セキュア コールを発生させます。

注意　Cisco Unified Communications Manager の管理ページで [SRTP を許可(SRTP Allowed)] チェックボックスをオンにした場合は、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。

Cisco Unified Communications Manager は、IPSec 接続が正しく設定されている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場合、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、または 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（およびその逆の）フォールバックは、セキュア デバイスから非セキュア デバイスへの転送、電話会議、トランスコーディング、保留音などで発生する場合があります。

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、どのデバイスに対しても [メディアターミネーションポイントが必須 (Media Termination Point Required)] チェックボックスがオンになっていない場合、Cisco Unified Communications Manager はこのコールをセキュアに分類します。[メディアターミネーションポイントが必須 (Media Termination Point Required)] チェックボックスがオンの場合、Cisco 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に分類します。コールに関連する MTP がない場合、デバイスの SRTP 機能によっては、Cisco Unified Communications Manager がそのコールを暗号化済みに分類することがあります。

SRTP が設定されているデバイスでは、デバイスに対する [SRTP を許可 (SRTP Allowed)] チェックボックスがオンで、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た場合、Cisco Unified Communications Manager はコールを暗号化済みに分類します。この基準を満たさない場合、Cisco Unified Communications Manager は、コールを非セキュアに分類します。デバイスがセキュリティ アイコンを表示できる電話機に接続されている場合、コールが暗号化されていると、電話機にロック アイコンが表示されます。

Cisco Unified Communications Manager は、トランクまたはゲートウェイによるアウトバウンド FastStart コールを非セキュアに分類します。Cisco Unified Communications Manager の管理ページで、[SRTP を許可 (SRTP Allowed)] チェックボックスをオンにした場合、Cisco Unified Communications Manager は [アウトバウンド FastStart を有効にする (Enable Outbound FastStart)] チェックボックスを無効にします。

Cisco 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、共有秘密鍵（Diffie-Hellman 鍵）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通過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 データを通過できるようにするには、次のトランクおよびゲートウェイの設定で [H.235 パススルー使用可能 (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

トランクおよびゲートウェイの設定については、『*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。

SIP トランクの暗号化の概要

SIP トランクは、シグナリングとメディア両方についてセキュア コールをサポートできます。シグナリング暗号化は TLS によって、メディア暗号化は SRTP によって提供されます。

トランクに対してシグナリングの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 (Encrypted)] を選択
- [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
- [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

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（[デバイス (Device)] > [トランク (Trunk)] > SIP トランクの設定ウィンドウ）。

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（同様に [デバイス (Device)] > [トランク (Trunk)] > SIP トランクの設定ウィンドウ）。

注意 この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鍵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場合でも SRTP は機能しますが、シグナリングおよびトレースで鍵が公開されます。この場合、Cisco Unified Communications Manager とトランクの接続先の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。

SIP トランク セキュリティ プロファイルの設定の詳細については、「SIP トランク セキュリティ プロファイルの設定」の章を参照してください。

ゲートウェイおよびトランクのセキュリティ設定用チェックリスト

表 24-1 を、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。このマニュアルは、次の URL で入手できます。

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a0080357589.html

表 24-1　MGCP ゲートウェイのセキュリティ設定用チェックリスト

設定手順		関連手順および関連項目
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。	「Cisco CTL クライアントの設定」（P.4-1）
ステップ 2	電話機に暗号化を設定したことを確認します。	「電話機のセキュリティの概要」（P.6-1）
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、Cisco 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。どちらかの方法で IPSec を設定した場合、もう 1 つの方法を使用する必要はありません。	• 「ネットワーク インフラストラクチャで IPSec を設定する場合の注意事項」（P.24-5） • 「Cisco Unified Communications Manager とゲートウェイまたはトランクとの間で IPSec を設定する場合の注意事項」（P.24-6）
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、Cisco Unified Communications Manager の管理ページで [SRTP を許可 (SRTP Allowed)] チェックボックスをオンにします。	[SRTP を許可 (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。

表 24-1　MGCP ゲートウェイのセキュリティ設定用チェックリスト（続き）

設定手順		関連手順および関連項目
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、[デバイス(Device)] > [トランク(Trunk)] > SIP トランクの設定ウィンドウで、[SRTP を許可(SRTP Allowed)] チェックボックスを必ずオンにします。 **注意**　[SRTP を許可(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鍵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場合でも SRTP は機能しますが、シグナリングおよびトレースで鍵が公開されます。この場合、Cisco Unified Communications Manager とトランクの接続先の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。	• 「SIP トランクの暗号化の概要」（P.24-3） • 「SIP トランク セキュリティ プロファイルの設定」（P.25-3）
ステップ 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。	• 『*Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*』

ネットワーク インフラストラクチャで IPSec を設定する場合の注意事項

このマニュアルでは、IPSec の設定方法は説明しません。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を示します。IPSec をネットワーク インフラストラクチャで設定し、Cisco Unified Communications Manager とデバイスとの間では設定しない場合は、IPSec の設定前に、次のことを検討してください。

- シスコは、Cisco Unified Communications Manager 自体ではなくインフラストラクチャで IPSec をプロビジョニングすることをお勧めします。
- IPSec を設定する前に、既存の IPSec 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、ジッタまたは待ち時間、およびその他のパフォーマンス上のメトリックを考慮してください。
- 『*Voice and Video Enabled IPSec Virtual Private Networks Solution Reference Network Design Guide*』を参照してください。これは、次の URL で入手できます。

  http://www.cisco.com/application/pdf/en/us/guest/netsol/ns241/c649/ccmigration_09186a00801ea79c.pdf
- 『*Cisco IOS Security Configuration Guide, Release 12.2*』（またはそれ以降）を参照してください。これは、次の URL で入手できます。

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_book09186a0080087df1.html
- セキュア Cisco IOS MGCP ゲートウェイで接続のリモート エンドを終了します。

- テレフォニー サーバがあるネットワークの信頼されている領域内で、ネットワーク デバイスのホスト エンドを終了します。たとえば、ファイアウォール内のアクセス コントロール リスト（ACL）またはその他のレイヤ 3 デバイスです。
- ホスト エンド IPSec 接続を終了するために使用する装置は、ゲートウェイの数やゲートウェイへの予期されるコール ボリュームによって異なります。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、または Cisco サービス統合型ルータを使用できます。
- 「ゲートウェイおよびトランクのセキュリティ設定用チェックリスト」（P.24-4）に示されている順序どおりに手順を実行してください。

注意　IPSEC 接続を設定して接続がアクティブであることを確認しないと、メディア ストリームの機密性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で IPSec を設定する場合の注意事項

この章で説明する Cisco Unified Communications Manager とゲートウェイまたはトランクとの間での IPSec の設定については、『*Cisco Unified Communications Operating System Administration Guide*』を参照してください。

[SRTP を許可 (SRTP Allowed)] チェックボックスの設定

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

- H.323 のゲートウェイ設定ウィンドウ
- H.225 トランク（ゲートキーパー制御）のトランク設定ウィンドウ
- クラスタ間トランク（ゲートキーパー制御）のトランク設定ウィンドウ
- クラスタ間トランク（非ゲートキーパー制御）のトランク設定ウィンドウ
- SIP トランク設定ウィンドウ

H.323 ゲートウェイ、および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 トランクまたは SIP トランクに対して [SRTP を許可 (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　『*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、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が開いたら、[SRTP を許可 (SRTP Allowed)] チェックボックスをオンにします。

注意　SIP トランクに対して [SRTP を許可 (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鍵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場合でも SRTP は機能しますが、シグナリングおよびトレースで鍵が公開されます。この場合、Cisco Unified Communications Manager とトランクの接続先の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。

ステップ 3　[保存 (Save)] をクリックします。

ステップ 4　[リセット (Reset)] をクリックして、デバイスをリセットします。

ステップ 5　H323 について IPSec が正しく設定されたことを確認します（SIP については、TLS が正しく設定されたことを確認します）。

追加情報

「関連項目」（P.24-7）を参照してください。

参考情報

関連項目

- 「認証、整合性、および許可の概要」（P.1-17）
- 「暗号化の概要」（P.1-22）
- 「Cisco IOS MGCP ゲートウェイの暗号化の概要」（P.24-1）
- 「H.323 ゲートウェイおよび H.323/H.225/H.245 トランクの暗号化の概要」（P.24-2）
- 「SIP トランクの暗号化の概要」（P.24-3）
- 「ゲートウェイおよびトランクのセキュリティ設定用チェックリスト」（P.24-4）
- 「ネットワーク インフラストラクチャで IPSec を設定する場合の注意事項」（P.24-5）
- 「Cisco Unified Communications Manager とゲートウェイまたはトランクとの間で IPSec を設定する場合の注意事項」（P.24-6）

シスコの関連マニュアル

- 『*Cisco Unified Communications Operating System Administration Guide*』
- 『*Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*』
- 『*Cisco IOS Security Configuration Guide, Release 12.2*』（またはそれ以降）
- 『*Voice and Video Enabled IPSec Virtual Private Networks Solution Reference Network Design Guide*』