



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 \(P.13-2\)](#)
- [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 \(P.13-3\)](#)
- [SIP トランクの暗号化の概要 \(P.13-4\)](#)
- [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 \(P.13-5\)](#)
- [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 \(P.13-6\)](#)
- [Cisco Unified CallManager 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 \(P.13-6\)](#)
- [SRTP を許可 \(SRTP Allowed\) チェックボックスの設定 \(P.13-7\)](#)
- [その他の情報 \(P.13-8\)](#)

Cisco IOS MGCP ゲートウェイの暗号化の概要

Cisco Unified CallManager 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判断されます。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 CallManager 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 CallManager 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 CallManager 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（認証された SCCP 電話機など）とのコールに関わる場合、Cisco Unified CallManager 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 CallManager 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 GUI で IPsec アソシエーションを設定した場合、Cisco Unified CallManager に対して認証ができます。Cisco Unified CallManager 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 アドミニストレーションガイド』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 CallManager に送信されます。Cisco Unified CallManager 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 CallManager の管理ページ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。デバイス設定ウィンドウには、[H.323 Gateway]、[H.225 Trunk (Gatekeeper Controlled)]、[Inter-Cluster Trunk (Gatekeeper Controlled)]、[Inter-Cluster Trunk (Non-Gatekeeper Controlled)] 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 CallManager 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 CallManager 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 CallManager 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 CallManager 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 CallManager 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 CallManager 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 がいない場合、デバイスの SRTP 機能によっては、Cisco Unified CallManager 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

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 CallManager 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 CallManager 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 CallManager 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 CallManager 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 CallManager 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。

SIP トランクの暗号化の概要

セキュア SIP トランクは、TLS 経由のセキュア コールをサポートできます。ただし、シグナリング暗号化はサポートされますが、メディア暗号化 (SRTP) はサポートされません。トランクがメディア暗号化をサポートしないため、コールのすべてのデバイスが認証またはシグナリング暗号化をサポートしている場合、通話中に電話機にシールドアイコンが表示されます。

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。

- [着信転送タイプ (Incoming Transport Type)] ドロップダウン リスト ボックスで、[TLS] を選択
- [発信転送タイプ (Outgoing Transport Type)] ドロップダウン リスト ボックスで、[TLS] を選択
- [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 ボックスで、[Encrypted] 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、トランクに適用します。IPSec をまだ設定していない場合は、設定します。



ヒント

SIP トランクは、IPSec 設定を使用して、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ぎます。Cisco Unified CallManager は、IPSec が正しく設定されていることを確認しません。IPSec を正しく設定しないと、セキュリティ関連情報が公開される可能性があります。

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

表 13-1 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 13-1 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.3-1)
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.4-1)
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 CallManager 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。	<ul style="list-style-type: none"> 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.13-6) Cisco Unified CallManager 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.13-6)
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 CallManager 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、Cisco Unified CallManager の管理ページの [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 CallManager 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。
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)。	<ul style="list-style-type: none"> SIP トランクの暗号化の概要 (P.13-4) SIP トランク セキュリティプロファイルの設定 (P.14-4)
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。	<ul style="list-style-type: none"> 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 CallManager 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 CallManager 自体ではなくインフラストラクチャで IPsec をプロビジョン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 (or later)』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 Series Concentrators、Catalyst 6500 IPsec VPN Services Module、または Cisco Integrated Services Routers を使用できます。
- P.13-5 の「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」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 CallManager 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

Cisco Unified CallManager と、この章で説明しているゲートウェイまたはトランクとの間で IPsec を設定する方法については、『Cisco Unified Communications Operating System アドミニストレーションガイド』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 CallManager の管理ページ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 Trunk (Gatekeeper Controlled) のトランク設定ウィンドウ
- Inter-Cluster Trunk (Gatekeeper Controlled) のトランク設定ウィンドウ
- Inter-Cluster Trunk (Non-Gatekeeper Controlled) の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または非ゲートキーパー制御の H.323/H.245/H.225 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 CallManager 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。
 - ステップ 3** [保存] をクリックします。
 - ステップ 4** [リセット] をクリックして、デバイスをリセットします。
 - ステップ 5** IPSec が正しく設定されたことを確認します。
-

追加情報

詳細については、[P.13-8](#) の「[関連項目](#)」を参照してください。

その他の情報

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 \(P.13-2\)](#)
- [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 \(P.13-3\)](#)
- [SIP トランクの暗号化の概要 \(P.13-4\)](#)
- [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 \(P.13-5\)](#)
- [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 \(P.13-6\)](#)
- [Cisco Unified CallManager 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 \(P.13-6\)](#)

シスコの関連マニュアル

- *Cisco Unified Communications Operating System アドミニストレーションガイド*
- *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*
- *Cisco IOS Security Configuration Guide, Release 12.2 (or later)*
- *Voice and Video Enabled IPSec Virtual Private Networks Solution Reference Network Design Guide*