CHAPTER 8

セキュア MGCP ゲートウェイの設定

この章は、次の内容で構成されています。

Cisco IOS MGCP シグナリング セキュリティの概要

Cisco 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 デバイスからノンセキュア デバイスへの転送、電話会議、トランスコーディング、保留音楽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 CallManager はセキュア コールのためのマスター暗号キーとソルトを生成し、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 CallManager はキーとソルトを送信しません。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 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 キーを暗号化せずに送信します。セッション キー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。

ゲートウェイの場所と配置および組織のセキュリティ ポリシーによっては、IPSec をオプションとすることもできます。たとえば、Cisco CallManager からゲートウェイへのパスまたはアドレス スペースを信頼している場合は、IPSec 設定をオプションとすることができます。IPSec を使用する場合は、Cisco CallManager 自体ではなくインフラストラクチャにプロビジョンすることをお勧めします。IPSec に関するその他の考慮事項および推奨事項は、P.8-4 の「IPSec に関する考慮事項と推奨事項」を参照してください。

ヒント　Cisco IOS MGCP ゲートウェイが『*Cisco CallManager セキュリティ ガイド*』で説明されている音声セキュリティ機能をサポートしているかどうかについては、『*Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*』を参照してください。

関連項目

- セキュア MGCP ゲートウェイの設定用チェックリスト（P.8-3）
- IPSec に関する考慮事項と推奨事項（P.8-4）
- Cisco IOS MGCP ゲートウェイに対するメディア認証とシグナリング認証および暗号化機能

セキュア MGCP ゲートウェイの設定用チェックリスト

表 8-1 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/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_11/gtsecure.htm

表 8-1　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 Client を混合モードでインストールし設定したことを確認します。	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設定（P.5-1）
ステップ 3	インフラストラクチャで IPSec を設定します。	IPSec に関する考慮事項と推奨事項（P.8-4）
ステップ 4	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。	Cisco IOS MGCP ゲートウェイに対するメディア認証とシグナリング認証および暗号化機能
ステップ 5	ゲートウェイにセキュリティを設定したことを確認します。	Cisco IOS MGCP ゲートウェイに対するメディア認証とシグナリング認証および暗号化機能

IPSec に関する考慮事項と推奨事項

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 を設定する前に、次の情報を考慮してください。

- シスコは、Cisco 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/go/srnd
- 『*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.8-3 の「セキュア MGCP ゲートウェイの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 ストリームのプライバシーが損なわれる可能性があります。

関連項目

- セキュア MGCP ゲートウェイの設定用チェックリスト（P.8-3）
- Cisco IOS MGCP シグナリング セキュリティの概要（P.8-2）
- Cisco IOS MGCP ゲートウェイに対するメディア認証とシグナリング認証および暗号化機能