セキュリティ

セキュリティの概要

IPv4 と IPv6 を各プロトコルの安全性という面で比較すると、IPv6 にはいくつかの利点と欠点がありますが、全体的には IPv4 と同等の安全性を備えています。IPv6 固有の利点の 1 つは、IPv6 サブネットおよびネットワークのサイズが非常に大きいことです。これにより、自動スキャンおよびワーム伝播に対する保護が改善されます。典型的なセキュリティ上の欠点は、IPv6 のアドレッシングの複雑さと、ネットワーク管理者が IPv6 プロトコルおよび IPv6 セキュリティ ツールに精通していない可能性があることです。

一般に、IPv4 のセキュリティに関する従来の問題のほとんどは IPv6 でも対処が必要です。たとえば、IPv4 の Address Resolution Protocol（ARP）のセキュリティ問題は、IPv6 のネイバー探索（ND）のセキュリティ問題に置き換えられます。

CSR 12.0 では、IPv6 セキュリティ設定にファイアウォール、sRTP、TLS など、IPv4 と同じ機能があります。

IPv6 音声シグナリングおよびメディアのプライバシーと暗号化

（注） CSR 12.0 の音声サービスを対象としたソリューション テストは実施されていません。

Internet Engineering Task Force（IETF）および RFC 4301 ～ 4303 では、IP セキュリティ（IPsec）を使用した IPv6 の認証および暗号化が要求されています。ただし、従来の IPv4 Unified Communications エンドポイントとのインターワーキング問題を避けるため、Cisco Unified Communications Manager（Unified CM）IPv4 および IPv6 導入では、引き続き Transport Layer Security（TLS）と Secure Real-Time Transport Protocol（SRTP）を使用して、IP Phone 間、IP Phone と SIP ゲートウェイおよびトランクの間で認証および暗号化を実行します。

IPsec は、IPv4 ベースの H.323 接続および Media Gateway Control Protocol（MGCP）ゲートウェイ接続にも使用できます。

Cisco Unified CM は次のセキュアなトランスポート プロトコルを提供します。

- トランスポート層セキュリティ（TLS）

  TLS はセキュア ポートと証明書交換を使用して、2 つのシステム間またはデバイス間でセキュアな信頼できるデータ転送を実現します。TLS は音声ドメインへのアクセスが行われないように、Unified CM 制御システム、デバイス、およびプロセス間の接続を保護および制御します。Unified CM は TLS を使用して、Skinny Client Control Protocol（SCCP）を実行している電話への SCCP コール、および SIP を実行している電話への SIP コールを保護します。

- IP セキュリティ（IPsec）

  IPsec は、Unified CM とゲートウェイの間の安全かつ信頼性の高いデータ転送を実現します。IPv4 ベースの IPsec は、Cisco IOS MGCP および H.323 ゲートウェイにシグナリング認証および暗号化を実装します。

Secure Real-Time Transport Protocol（SRTP）を TLS および IPsec 転送サービスに追加して、SRTP をサポートするデバイスのセキュリティ レベルを強化できます。SRTP はメディア ストリームを認証および暗号化し、Cisco Unified IP Phone の TDM またはアナログ音声ゲートウェイ ポートで発信または終端される音声会話を、音声ドメインへのアクセス権を得た盗聴者から確実に保護します。SRTP は、リプレイ攻撃に対する保護を追加します。

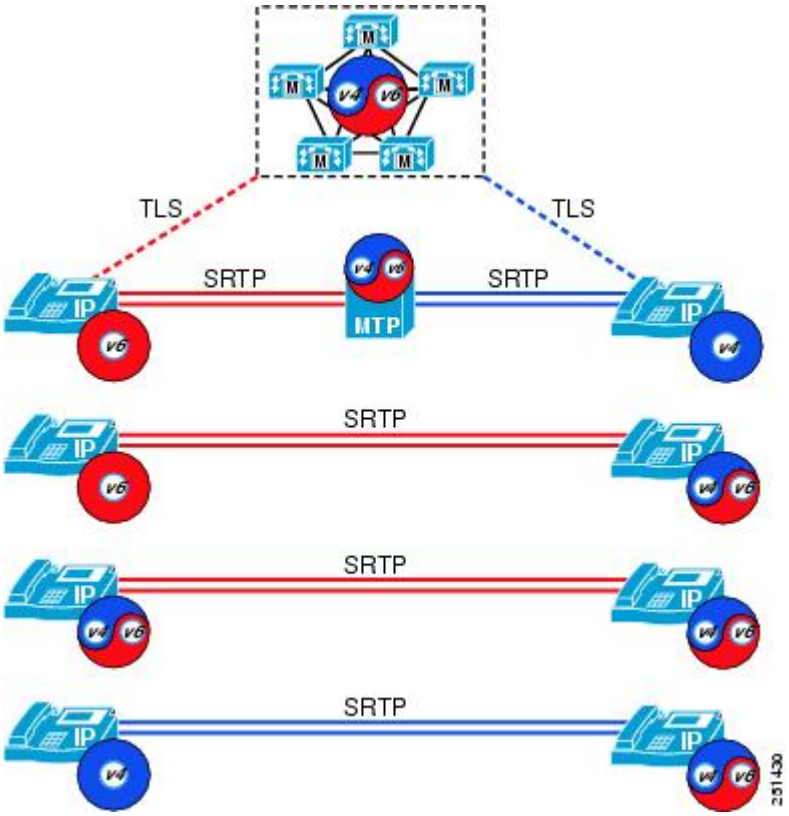
Unified CM セキュリティの詳細については、次の Web サイトで入手できる『*Cisco Unified Communications Manager Security Guide*』を参照してください。

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

IPv4 と IPv6 との間の暗号化されたメディアおよび MTP

Unified CM では、デュアルスタック（IPv4 および IPv6）とシングルスタック（IPv4 または IPv6）のデバイス間で暗号化されたコールをサポートしています。着信側デバイスと発信側デバイスの間に IP アドレッシング バージョンの不一致が存在する場合、Unified CM は動的に MTP を挿入して暗号化された音声ストリームの IP ヘッダーを変換します。動的に挿入されたこの MTP は、暗号化されたメディア ストリームに対してパススルー コーデックを使用し、IP ヘッダーのみを IPv4 から IPv6（および IPv6 から IPv4）に変更します。

図 *1 : Unified CM* によるアドレッシング モードの解決



CAPF と CTL

認証局プロキシ機能（CAPF）は、IPv4 アドレッシングと IPv6 アドレッシングの両方をサポートし、電話との通信および標準的なセキュリティ証明書機能の実行に TCP/IP を使用します。IPv6 対応の Unified CM クラスタでは、CAPF に次の機能があります。

- IPv4 専用 IP Phone に証明書を発行してアップグレードする
- IPv6 専用 IP Phone に証明書を発行してアップグレードする
- デュアルスタック（IPv4 および IPv6）IP Phone に証明書を発行してアップグレードする

証明書信頼リスト（CTL）には、新しい IPv6 機能は必要ありません。

IPv6コラボレーショントラフィックおよびファイアウォール

Cisco 適応型セキュリティ アプライアンス（ASA）は IPv6 向けに SCCP または SIP をサポートしているため、IPv6 音声トラフィック用に動的にピンホールを開く際に使用できます。この製品は、IPv6 トラフィック用の基本的なファイアウォールとトラフィック フィルタリング機能をサポートしています。

IPv6 のベーシック ファイアウォール機能を実装する場合は、次のドキュメントを参照してください。

- Cisco ASA 5500-X シリーズ ファイアウォールのコンフィギュレーション ガイド
  https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html
- Catalyst 6500 シリーズ スイッチのコンフィギュレーション ガイド
  https://www.cisco.com/c/en/us/support/switches/catalyst-6500-series-switches/products-installation-and-configuration-guides-list.html

Cisco Unified Border Element

Cisco IOS ベース ISR 4000 G3 Cisco Unified Border Element では、次のことが可能です。

- セッションの 1 つのレッグで SIP IPv6 コールを終了し、別のレッグで SIP IPv4 コールを生成する。
- セッションの 1 つのレッグで SIP IPv6 コールを終了し、別のレッグで SIP IPv6 コールを生成する。

この機能により、エンタープライズ IPv6 ネットワークとサービス プロバイダー IPv4 ネットワーク間の基本的な相互接続が可能になります。

メディアとシグナリングの両方の処理を含む基本的なコールがサポートされます。IPv6 を介した基本的な補足サービスはサポートされますが、H.323 IPv6 コールはサポートされません。

セキュリティおよび IPv6 トラフィック

この章に記載されているシスコのセキュリティ プラットフォームおよび製品の今後のリリースでは、IPv6 コラボレーション トラフィックがサポートされます。ただし、これらの製品でコラボレーション トラフィックの IPv6 がサポートされるようになるまでは、すべての IPv6 音声トラフィックをエンタープライズ ネットワーク内に保持することをお勧めします。

キャンパス ネットワーク内でファイアウォールを使用する（たとえば、Unified CM、一元化されたメディア リソース、および他の音声アプリケーションを保護する）場合は、Unified CM の [シグナリング用のIPアドレッシングモード設定（IP Addressing Mode Preference for Signaling）]

を [IPv4] に変更し、すべての SCCP および SIP シグナリング トラフィックの検査を許可します。代わりに、アクセス コントロール リスト（ACL）を使用して IPv6 トラフィックに対してファイアウォールを開くこともできます。