CHAPTER 3

Cisco Unity Connection、Cisco Unified Communications Manager、および IP 電話の間の接続の保護

この章では、Cisco Unity Connection、Cisco Unified Communications Manager、および IP 電話の間の接続に関連して発生する可能性がある、セキュリティ上の問題について説明します。また、とるべき対策に関する情報、意思決定に役立つ推奨事項、下した決定の効果に関する情報、およびベスト プラクティスも紹介します。

次の項を参照してください。

Cisco Unity Connection、Cisco Unified Communications Manager、および IP 電話の間の接続に関連するセキュリティ上の問題

Cisco Unity Connection システムは、Connection のボイス メッセージ ポート（SCCP 連動用）またはポート グループ（SIP 連動用）、Cisco Unified Communications Manager、および IP 電話の間の接続に関して、潜在的な脆弱性を持ちます。

次のような脅威が発生する可能性があります。

- 中間者攻撃（Cisco Unified CM と Connection の間の情報フローが監視され、改変される）
- ネットワーク トラフィック スニフィング（ソフトウェアを通じて、Cisco Unified CM、Connection、および Cisco Unified CM で管理される IP 電話の間を流れる通話内容やシグナリング情報がキャプチャされる）
- Connection と Cisco Unified CM の間のコール シグナリングの改変
- Connection とエンドポイント（IP フォンやゲートウェイなど）の間のメディア ストリームの改変

- Connection の ID 盗用（Connection 以外のデバイスが、Connection サーバとして Cisco Unified CM にアクセスする）
- Cisco Unified CM サーバの ID 盗用（Cisco Unified CM 以外のサーバが、Cisco Unified CM サーバとして Connection にアクセスする）

Cisco Unity Connection ボイス メッセージ ポート用の Cisco Unified Communications Manager セキュリティ機能

Cisco Unified CM では、Connection との接続を、「Cisco Unity Connection、Cisco Unified Communications Manager、および IP 電話の間の接続に関連するセキュリティ上の問題」（P.3-1）に挙げた脅威から保護できます。Connection で使用可能な Cisco Unified CM のセキュリティ機能について、表 3-1 で説明します。

表 3-1　Cisco Unity Connection で使用される Cisco Unified CM のセキュリティ機能

セキュリティ機能	説明
シグナリング認証	トランスポート層セキュリティ（TLS）プロトコルを使用して、シグナリング パケットが転送中に改ざんされていないことを検証するプロセスです。シグナリング認証は Cisco 証明書信頼リスト（CTL）ファイルの作成に依存します。 この機能によって、次の脅威から保護されます。 • Cisco Unified CM と Connection の間の情報フローを改変する中間者攻撃。 • コールシグナリングの改変。 • Connection サーバの ID 盗用。 • Cisco Unified CM サーバの ID 盗用。
デバイス認証	デバイスの ID を検証してエンティティが正当なものであることを確認するプロセスです。このプロセスは、Cisco Unified CM と、Connection ボイス メッセージ ポート（SCCP 連動用）または Connection ポート グループ（SIP 連動用）との間で、各デバイスがもう一方のデバイスの証明書を受け入れるときに発生します。証明書が受け入れられると、デバイス間に安全な接続が確立されます。デバイス認証は Cisco 証明書信頼リスト（CTL）ファイルの作成に依存します。 この機能によって、次の脅威から保護されます。 • Cisco Unified CM と Connection の間の情報フローを改変する中間者攻撃。 • メディア ストリームの改変。 • Connection サーバの ID 盗用。 • Cisco Unified CM サーバの ID 盗用。

表 3-1　Cisco Unity Connection で使用される Cisco Unified CM のセキュリティ機能 （続き）

セキュリティ機能	説明
シグナリング暗号化	暗号化の手法を使用して、Connection と Cisco Unified CM の間で送信されるすべての SCCP または SIP シグナリング メッセージの機密を保護するプロセスです。シグナリング暗号化によって、相手に関連する情報、相手が入力した DTMF 番号、通話の状態、メディア暗号キーなどの情報が意図しないアクセスや不正なアクセスから保護されることが保証されます。 この機能によって、次の脅威から保護されます。 • Cisco Unified CM と Connection の間の情報フローを監視する中間者攻撃。 • Cisco Unified CM と Connection の間のシグナリング情報フローを監視するネットワーク トラフィック スニフィング。
メディアの暗号化	暗号化の手順を使用して、メディアの機密を保持するプロセスです。このプロセスでは、IETF RFC 3711 で定義されている Secure Real Time Protocol（SRTP）を使用して、目的の受信者だけが Connection とエンドポイント（電話機やゲートウェイなど）の間のメディア ストリームを解釈できるようにします。サポートされているのは、音声ストリームだけです。メディア暗号化には、デバイス用のメディア マスター キー ペアの作成、Connection とエンドポイントへのキーの配布、さらにはキーの転送中の安全確保が含まれます。Connection とエンドポイントは、そのキーを使用してメディア ストリームの暗号化と復号化を行います。 この機能によって、次の脅威から保護されます。 • Cisco Unified CM と Connection の間のメディア ストリームを傍受する中間者攻撃。 • Cisco Unified CM が管理する Cisco Unified CM、Connection、および IP 電話の間を流れる電話通話を盗聴するネットワーク トラフィックのスニフィング。

認証とシグナリング暗号化は、メディアを暗号化するための最小要件です。つまり、デバイスがシグナリング暗号化と認証をサポートしていない場合、メディア暗号化は行われません。

Cisco Unified CM のセキュリティ（認証および暗号化）では、Connection への通話だけを保護します。メッセージ ストアで録音されたメッセージは、Cisco Unified CM の認証および暗号化機能では保護されませんが、Connection の個人情報の安全が図られるメッセージ機能で保護できます。Connection の安全なメッセージ機能の詳細については、「プライベートまたはセキュアとマークされたメッセージの Cisco Unity Connection での処理方法」（P.10-1）を参照してください。

Cisco Unified Communications Manager および Cisco Unity Connection のセキュリティ モードの設定

Cisco Unified Communications Manager および Cisco Unity Connection には、ボイス メッセージ ポート（SCCP 連動用）またはポート グループ（SIP 連動用）について、表 3-2 に示すセキュリティ モード オプションがあります。

注意　Connection ボイス メッセージ ポート（SCCP 連動用）またはポート グループ（SIP 連動用）のクラスタ セキュリティ モード設定は、Cisco Unified CM ポートのセキュリティ モード設定と一致する必要があります。一致しないと、Cisco Unified CM での認証および暗号化が失敗します。

表 3-2　セキュリティ モード オプション

設定	効果
非セキュア	コールシグナリング メッセージがクリア（暗号化されていない）テキストとして送信され、認証された TLS ポートではなく非認証ポートを使用して Cisco Unified CM に接続されるため、コールシグナリング メッセージの完全性とプライバシーは保証されません。 また、メディア ストリームも暗号化できません。
認証	コールシグナリング メッセージは認証された TLS ポートを使用して Cisco Unified CM に接続されるため、完全性が保証されます。ただし、クリア（暗号化されていない）テキストで送信されるため、コールシグナリング メッセージのプライバシーは保証されません。 また、メディア ストリームも暗号化されません。
暗号化	コールシグナリング メッセージは認証された TLS ポートを使用して Cisco Unified CM に接続され、暗号化されるため、完全性とプライバシーが保証されます。 また、メディア ストリームも暗号化できます。 **注意**　メディア ストリームが暗号化されるようにするには、両方のエンドポイントが暗号化モードで登録されている必要があります。ただし、一方のエンドポイントが非セキュア モードまたは認証モードに設定され、もう一方のエンドポイントが暗号化モードに設定されている場合、メディア ストリームは暗号化されません。また、仲介デバイス（トランスコーダやゲートウェイなど）で暗号化が有効になっていない場合も、メディア ストリームは暗号化されません。

Cisco Unity Connection、Cisco Unified Communications Manager、および IP 電話の間の接続を保護するためのベスト プラクティス

Cisco Unity Connection と Cisco Unified Communications Manager の両方でボイス メッセージ ポートの認証および暗号化を有効にする場合は、『*Cisco Unified Communications Manager SCCP Integration Guide for ConnectionRelease 9.x*』を参照してください。このガイドは、http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/integration/guide/cucm_sccp/cucintcucmskinny.html から入手可能です。