Cisco Unity Connection、Cisco Unified Communications Manager、および IP フォン間の接続の保護

Cisco Unity Connection、Cisco Unified Communications Manager、および IP フォン間の接続の保護

はじめに

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、講じ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。

Unity Connection、Cisco Unified Communications Manager、および IP フォン間の接続に関するセキュリティの問題

Cisco Unity Connection システムは、 Unity Connection のボイス メッセージ ポート（SCCP 統合用）またはポート グループ（SIP 統合用）、Cisco Unified Communications Manager、および IP フォンの間の接続に関して、潜在的な脆弱性ポイントを持ちます。

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 Unity Connection 間の情報フローの監視と改変）

- ネットワークトラフィック スニフィング（Cisco Unified CM、Unity Connection、および Cisco Unified CM で管理される IP フォン間の通話内容やシグナリング情報のソフトウェアによるキャプチャ）
- Unity Connection と Cisco Unified CM 間のコール シグナリングの改変
- Unity 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
- Unity Connection の ID 盗用（Unity Connection 以外のデバイスが Cisco Unified CM に対し、そのデバイス自体が Unity Connection サーバであると示す場合）
- Cisco Unified CM サーバの ID 盗用（Cisco Unified CM 以外のサーバが Unity Connection に対し、そのサーバ自体が Cisco Unified CM サーバであると示す場合）

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

Cisco Unified CM は、「Unity Connection、Cisco Unified Communications Manager、および IP フォン間の接続に関するセキュリティの問題」に記載されている脅威から Unity Connection への接続を保護できます。Unity Connection が利用できる Cisco Unified CM のセキュリティ機能を表 1 : Cisco Unity Connection が使用する Cisco Unified CM セキュリティ機能 に示します。

表 *1 : Cisco Unity Connection* が使用する *Cisco Unified CM* 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。 • 中間者攻撃（Cisco Unified CM と Unity Connection 間の情報フローの改変）。 • コールシグナリングの改変。 • Unity Connection サーバの ID 盗用。 • Cisco Unified CM サーバの ID 盗用。

セキュリティ機能	説明
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、Unity Connection ボイス メッセージング ポート（SCCP 統合用）または Unity Connection ポート グループ（SIP 統合用）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。 • 中間者攻撃（Cisco Unified CM と Unity Connection 間の情報フローの改変）。 • メディア ストリームの改変。 • Unity Connection サーバの ID 盗用。 • Cisco Unified CM サーバの ID 盗用。
シグナリング暗号化	暗号化の手法を使用して、Unity 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。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。 • 中間者攻撃（Cisco Unified CM と Unity Connection 間の情報フローの監視）。 • ネットワーク トラフィック スニフィング（Cisco Unified CM と Unity Connection 間のシグナリング情報フローの監視）。

セキュリティ機能	説明
メディア暗号化	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 Unity 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 プレーヤー キー ペアの作成、Unity 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。Unity 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。 • 中間者攻撃（Cisco Unified CM と Unity Connection 間のメディア ストリームのリッスン）。 • ネットワーク トラフィック スニフィング（Cisco Unified CM、Unity Connection、および Cisco Unified CM で管理される IP フォン間の電話による通話内容の盗聴）。

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 セキュリティ（認証と暗号化）では、Unity Connection へのコールだけが保護されます。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、Unity Connection のプライベート セキュア メッセージング機能で保護できます。Unity Connection のセキュア メッセージング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処理」を参照してください。

自己暗号化ドライブ

Cisco Unity Connection は、自己暗号化ドライブ（SED）もサポートしています。これは、フルディスク暗号化（FDE）とも呼ばれます。FDE は、ハードドライブで使用可能なすべてのデータを暗号化するために使用される暗号化方式です。このデータには、ファイル、オペレーティングシステム、およびソフトウェアプログラムが含まれます。ディスク上の使用可能なハードウェアは、すべての受信データを暗号化し、すべての送信データの暗号化を解除します。ドライブがロックされると、暗号化キーが内部で作成され保存されます。このドライブに保存され

ているすべてのデータは、そのキーを使用して暗号化され、暗号化された形式で保存されます。FDE は、キー ID とセキュリティ キーで構成されます。

詳細については、「https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/gui/config/guide/2-0/b_Cisco_UCS_C-series_GUI_Configuration_Guide_201/b_Cisco_UCS_C-series_GUI_Configuration_Guide_201_chapter_010011.html#concept_E8C37FA4A71F4C8F8E1B9B94305AD844」を参照してください。

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

Cisco Unified Communications Manager と Cisco Unity Connection のボイス メッセージング ポート（SCCP 統合用）またはポート グループ（SIP 統合用）のセキュリティ モード オプションを 表 2 : セキュリティ モード オプション に示します。

注意 Unity Connection ボイス メッセージ ポート（SCCP 統合用）またはポート グループ（SIP 統合用）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。一致していない場合、Cisco Unified CM の認証と暗号化は失敗します。

表 *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、認証済み 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。

設定	効果
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。 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 フォン間の接続の保護に関する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ングポートに対し認証と暗号化を有効にするには、『*Cisco Unified Communications Manager SCCP Integration Guide for Unity Connection Release 14*』を参照してください。このファイルは次の URL から入手可能です。https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/integration/cucm_sccp/b_14cucintcucmskinny.html