APPENDIX A

Cisco Unity Connection ボイス メッセージ ポートの Cisco Unified Communications Manager 認証および暗号化

Cisco Unity Connection と Cisco Unified Communications Manager 間の接続は、Cisco Unity Connection システムが攻撃を受けやすい箇所の 1 つです。脅威としては、次のようなことが考えられます。

- 中間者攻撃（攻撃者が Cisco Unified CM と Cisco Unity Connection ボイス メッセージ ポート間の情報フローを監視および改変するプロセス）
- ネットワーク トラフィック スニフィング（攻撃者がソフトウェアを使用して、Cisco Unified CM、Cisco Unity Connection ボイス メッセージ ポート、および Cisco Unified CM の管理対象 IP Phone の間を流れる電話通話やシグナリング情報を取り込むプロセス）
- Cisco Unity Connection ボイス メッセージ ポートと Cisco Unified CM 間のコール シグナリングの改変
- Cisco Unity Connection ボイス メッセージ ポートとエンドポイント（電話機やゲートウェイなど）間のメディア ストリームの改変
- Cisco Unity Connection ボイス メッセージ ポートの ID 盗難（Cisco Unity Connection 以外のデバイスが Cisco Unity Connection ボイス メッセージ ポートとして Cisco Unified CM にアクセスするプロセス）
- Cisco Unified CM サーバの ID 盗難（Cisco Unified CM 以外のサーバが Cisco Unified CM サーバとして Cisco Unity Connection ボイス メッセージ ポートにアクセスするプロセス）

Cisco Unified CM セキュリティ機能

Cisco Unified CM 4.1(3) 以降では、Cisco Unity Connection との接続を上記のような脅威からセキュリティで保護できます。表 A-1 では、Cisco Unity Connection で利用できる Cisco Unified CM セキュリティ機能について説明します。

表 A-1　Cisco Unity Connection で使用される 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	Transport Layer Security（TLS）プロトコルを使用して、伝送中にシグナリング パケットが改ざんされていないことを検証するプロセス。シグナリング認証は、Cisco Certificate Trust List（CTL）ファイルの作成に依存します。 **脅威に対する効果：**この機能は次の脅威から保護します。 • Cisco Unified CM と Cisco Unity Connection ボイス メッセージ ポート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 • Cisco Unity Connection ボイス メッセージ ポートの ID 盗難 • Cisco Unified CM サーバの ID 盗難
デバイス認証	デバイスの ID を検証して、エンティティがその ID 情報と一致していることを確認するプロセス。このプロセスは、各デバイスが他のデバイスの証明書を受け入れるときに、Cisco Unified CM と Cisco Unity Connection ボイス メッセージ ポート間で行われます。証明書が受け入れられると、デバイス間にセキュア接続が確立されます。デバイス認証は、Cisco Certificate Trust List（CTL）ファイルの作成に依存します。 **脅威に対する効果：**この機能は次の脅威から保護します。 • Cisco Unified CM と Cisco Unity Connection ボイス メッセージ ポート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 • Cisco Unity Connection ボイス メッセージ ポートの ID 盗難 • Cisco Unified CM サーバの ID 盗難
シグナリング暗号化	暗号方式を使用して、Cisco Unity Connection ボイス メッセージ ポートと Cisco Unified CM 間で送信されるすべての SCCP シグナリング メッセージの機密を（暗号化により）保持するプロセス。シグナリング暗号化により、各側に関連する情報、各側で入力された DTMF 番号、コール ステータス、およびメディア暗号鍵などが、不意のアクセスや不正アクセスから保護されることが保証されます。 **脅威に対する効果：**この機能は次の脅威から保護します。 • Cisco Unified CM と Cisco Unity Connection ボイス メッセージ ポート間の情報フローを監視する中間者攻撃 • Cisco Unified CM と Cisco Unity Connection ボイス メッセージ ポート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

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

セキュリティ機能	説明
メディア暗号化	暗号化手順を使用してメディアの機密を保持するプロセス。このプロセスは、IETF RFC 3711 で定義された Secure Real Time Protocol（SRTP）を使用して、目的の受信者だけが Cisco Unity Connection ボイス メッセージ ポートとエンドポイント（電話機やゲートウェイなど）間のメディア ストリームを解釈できることを保証します。サポートされるのは、オーディオ ストリームだけです。メディア暗号化では、デバイス用のメディア マスター鍵ペアの作成、Cisco Unity Connection とエンドポイントへの鍵の配送、および鍵の転送時の配送の保護などが行われます。Cisco Unity Connection とエンドポイントでは、その鍵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。 **脅威に対する効果：**この機能は次の脅威から保護します。 • Cisco Unified CM と Cisco Unity Connection ボイス メッセージ ポート間のメディア ストリームを傍受する中間者攻撃 • Cisco Unified CM、Cisco Unity Connection ボイス メッセージ ポート、および Cisco Unified CM の管理対象 IP Phone 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 スニフィング

認証およびシグナリング暗号化は、メディア暗号化の最小要件です。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。

（注） Cisco Unified CM 認証および暗号化によって保護されるのは、ボイス メッセージ ポートへの通話だけです。メッセージ ストアに記録されたメッセージは、Cisco Unified CM 認証および暗号化機能によって保護されません。

機能の概要

Cisco Unity Connection と Cisco Unified CM 間のセキュリティ機能（認証および暗号化）では、次のものが必要になります。

- Cisco Unity Connection の管理でセキュア クラスタに登録されたすべての Cisco Unified CM サーバがリストされている Cisco Unified CM CTL ファイル。
- 認証および暗号化、またはそのどちらかを使用する各 Cisco Unity Connection サーバの Cisco Unity Connection サーバ ルート証明書。ルート証明書は、作成日から 20 年間有効です。
- Cisco Unity Connection サーバ ルート証明書をルートとし、ボイス メッセージ ポートが Cisco Unified CM サーバへの登録時に提示する、Cisco Unity Connection ボイス メッセージ ポート デバイス証明書。

Cisco Unity Connection ボイス メッセージ ポートの認証および暗号化プロセスは、次のとおりです。

1. 各 Cisco Unity Connection ボイス メッセージ ポートが TFTP サーバに接続し、CTL ファイルをダウンロードして、すべての Cisco Unified CM サーバの証明書を抽出します。
2. 各 Cisco Unity Connection ボイス メッセージ ポートが Cisco Unified CM TLS ポートへのネットワーク接続を確立します。デフォルトでは、TLS ポートは 2443 です。ただし、ポート番号は設定変更できます。
3. 各 Cisco Unity Connection ボイス メッセージ ポートが Cisco Unified CM サーバへの TLS 接続を確立します。その際、デバイス証明書が確認され、ボイス メッセージ ポートが認証されます。
4. 各 Cisco Unity Connection ボイス メッセージ ポートが Cisco Unified CM サーバに登録します。その際、そのポートがメディア暗号化を使用するかどうかも指定します。

通話の動作

Cisco Unity Connection と Cisco Unified CM 間で通話が発信される場合、コールシグナリング メッセージとメディア ストリームは、次の方法で処理されます。

- 両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、コールシグナリング メッセージとメディア ストリームは暗号化されます。
- 一方のエンドポイントが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、コールシグナリング メッセージは認証されます。ただし、コールシグナリング メッセージもメディア ストリームも暗号化されません。
- 一方のエンドポイントが非セキュア　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、コールシグナリング メッセージもメディア ストリームも暗号化されません。

Cisco Unity Connection のセキュリティ モード設定

Cisco Unity Connection の管理の［セキュリティ モード（Security Mode）］の設定により、ポートにおけるコールシグナリング メッセージの処理方法と、メディア ストリームの暗号化が可能かどうかが決まります。表 A-2 では、各ポートに対する［テレフォニー統合（Telephony Integrations）］>［ポート（Port）］>［ポートの基本設定（Port Basics）］ページの［セキュリティ モード（Security Mode）］設定の効果について説明します。

表 A-2　ボイス メッセージ ポートに関する［セキュリティ モード（Security Mode）］の設定

設定	動作
［非セキュア（Non-secure）］	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（Authenticated）］	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（Encrypted）］	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。

セキュリティの無効化と再有効化

Cisco Unity Connection と Cisco Unified CM 間の認証および暗号化機能の有効と無効を切り替えるには、すべての Cisco Unified CM クラスタの［セキュリティ モード（Security Mode）］を［非セキュア（Non-secure）］に変更し、さらに Cisco Unified CM の管理ページで適切な設定を変更します。

認証および暗号化を再度有効にするには、［セキュリティ モード（Security Mode）］を［認証（Authenticated）］または［暗号化（Encrypted）］に変更します。

（注）　認証および暗号化を無効にした場合や再度有効にした場合、Cisco Unity Connection サーバ ルート証明書をエクスポートしてすべての Cisco Unified CM サーバにコピーする必要はありません。

複数のクラスタに対する複数の設定

Cisco Unity Connection に複数の Cisco Unified CM 電話システム連動が含まれている場合は、Cisco Unified CM 電話システム連動ごとに異なる［セキュリティ モード（Security Mode）］設定を保持できます。たとえば、1 つ目の Cisco Unified CM 電話システム連動を［暗号化（Encrypted）］に設定し、2 つ目の Cisco Unified CM 電話システム連動を［非セキュア（Non-secure）］に設定することができます。

個別のボイス メッセージ ポートの設定

トラブルシューティングを行う場合は、Cisco Unity Connection ボイス メッセージ ポートの認証および暗号化の有効と無効を個別に切り替えることができます。それ以外の場合は、Cisco Unified CM ポート グループ内のすべてのボイス メッセージ ポートを同一の［セキュリティ モード（Security Mode）］設定にしておくことをお勧めします。