CHAPTER 10

ボイスメール ポートのセキュリティ設定

この章は、次の内容で構成されています。

ボイスメールのセキュリティの概要

Cisco Unified CallManager ボイスメール ポートおよび Cisco Unity SCCP デバイスにセキュリティを設定するには、ポートに対してセキュアなデバイス セキュリティ モードを選択します。認証済みのボイスメール ポートを選択すると、TLS 接続が開始されます。この接続では、相互証明書交換（各デバイスが相手のデバイスの証明書を受け入れる）を使用して、デバイスが認証されます。暗号化済みのボイスメール ポートを選択すると、システムはまずデバイスを認証してから、デバイス間で暗号化されたボイス ストリームを送信します。

デバイス セキュリティ モードが認証のみまたは暗号化になっている場合、Cisco Unity-CM TSP は Cisco Unified CallManager TLS ポートを介して Cisco Unified CallManager に接続します。デバイス セキュリティ モードが非セキュアになっている場合、Cisco Unity TSP は Cisco Unified CallManager SCCP ポートを介して Cisco Unified CallManager に接続します。

（注） このマニュアルでは、サーバという用語は Cisco Unified CallManager クラスタ内のサーバを意味します。ボイスメール サーバという用語は Cisco Unity サーバを意味します。

ボイスメール セキュリティの設定のヒント

セキュリティを設定する前に、次の点を考慮してください。

- このバージョンの Cisco Unified CallManager では Cisco Unity 4.0(5) 以降を実行する必要があります。
- Cisco Unity Telephony Integration Manager を使用して Cisco Unity のセキュリティ タスクを実行する必要があります。これらのタスクの実行方法は、『*Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity 4.x*』を参照してください。
- この章で説明する手順に加えて、Cisco Unified Communications オペレーティング システムの管理ページの証明書管理機能を使用して、Cisco Unity 証明書を信頼ストアに保存する必要があります。この作業の詳細については、『*Cisco Unified Communications Operating System アドミニストレーション ガイド*』を参照してください。

  証明書をコピーした後、クラスタ内の各サーバで Cisco CallManager サービスを再起動する必要があります。
- Cisco Unity　証明書が失効したか、または何らかの理由で変更された場合は、Cisco　Unified Communications オペレーティング システムの管理ページの証明書管理機能を使用して、信頼ストアの証明書を更新します。証明書が一致しないと TLS 認証は失敗し、ボイスメール機能は Cisco Unified CallManager に登録できないため機能しません。
- ボイスメール サーバのポートを設定する場合は、デバイス セキュリティ モードを選択する必要があります。
- Cisco Unity Telephony Integration Manager で指定する設定は、Cisco Unified CallManager の管理ページで設定されているボイスメール ポートのデバイス セキュリティ モードと一致している必要があります。Cisco Unified CallManager の管理ページの［ボイスメールポートの設定（Voice Mail Port Configuration）］ウィンドウ（またはボイスメール ポート ウィザード）で、ボイスメール ポートにデバイス セキュリティ モードを適用します。

ヒント　デバイス セキュリティ モードの設定が Cisco Unified CallManager と Cisco Unity で一致しない場合は、Cisco Unity ポートが Cisco Unified CallManager に登録できず、Cisco Unity はそれらのポートでコールを受け入れることができません。

- ポートのセキュリティ プロファイルを変更するには、Cisco Unified CallManager デバイスをリセットして Cisco Unity ソフトウェアを再起動する必要があります。Cisco Unified CallManager の管理ページで、以前のプロファイルと異なるデバイス セキュリティ モードを使用するセキュリティ プロファイルを適用する場合は、Cisco Unity の設定を変更する必要があります。
- ボイスメール ポート ウィザードで既存のボイスメール サーバのデバイス セキュリティ モードを変更することはできません。既存のボイスメール サーバにポートを追加すると、現在プロファイルに設定されているデバイス セキュリティ モードが自動的に新規ポートに適用されます。

ボイスメール ポートのセキュリティ設定用チェックリスト

ボイスメール ポートのセキュリティを設定する場合は、表 10-1 を参照してください。

表 10-1　ボイスメール ポート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 クライアント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	電話機に認証または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の概要（P.4-1） 電話機セキュリティ プロファイルの設定（P.5-1）
ステップ 3	Cisco Unified Communications オペレーティング システムの管理ページの証明書管理機能を使用して、クラスタ内の各サーバの信頼ストアに Cisco Unity 証明書をコピーします。次に、各サーバで Cisco CallManager サービスを再起動します。	• ボイスメール セキュリティの設定のヒント（P.10-2） • *Cisco Unified Communications Operating System アドミニストレーション ガイド* • *Cisco Unified CallManager Serviceability アドミニストレーション ガイド*
ステップ 4	Cisco Unified CallManager の管理ページで、ボイスメール ポートのデバイス セキュリティ モードを設定します。	• 単一ボイスメール ポートへのセキュリティ プロファイルの適用（P.10-4） • ボイスメール ポート ウィザードでのセキュリティ プロファイルの適用（P.10-5）
ステップ 5	Cisco Unity ボイスメール ポートのセキュリティ関連設定タスクを実行します。たとえば、Cisco Unity が Cisco TFTP サーバを指すように設定します。	*Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity 4.x*
ステップ 6	Cisco Unified CallManager の管理ページでデバイスをリセットし、Cisco Unity ソフトウェアを再起動します。	• *Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity 4.x* • 単一ボイスメール ポートへのセキュリティ プロファイルの適用（P.10-4）

単一ボイスメール ポートへのセキュリティ プロファイルの適用

単一のボイスメール ポートにセキュリティ プロファイルを適用するには、次の手順を実行します。

この手順では、デバイスはデータベースに追加済みで、証明書が存在しない場合は証明書が電話機にインストール済みであることを前提としています。セキュリティ プロファイルを初めて適用した後、またはセキュリティ プロファイルを変更した場合、デバイスをリセットする必要があります。

セキュリティ プロファイルを適用する前に、次の項を検討してください。

- ボイスメールのセキュリティの概要（P.10-1）
- ボイスメール セキュリティの設定のヒント（P.10-2）
- ボイスメール ポートのセキュリティ設定用チェックリスト（P.10-3）

手順

ステップ 1　『*Cisco Unified CallManager アドミニストレーション ガイド*』の説明に従って、ボイスメール ポートを検索します。

ステップ 2　ポートの設定ウィンドウが表示されたら、**［デバイスセキュリティモード］**設定を見つけます。ドロップダウン リスト ボックスから、ポートに適用するセキュリティ モードを選択します。このオプションは、データベースで事前定義されています。デフォルト値は未選択です。

ステップ 3　**［保存］**をクリックします。

ステップ 4　**［リセット］**をクリックします。

追加情報

詳細については、P.10-6 の「関連項目」を参照してください。

ボイスメール ポート ウィザードでのセキュリティ プロファイルの適用

既存のボイスメール サーバのセキュリティ設定を変更する方法は、P.10-4 の「単一ボイスメール ポートへのセキュリティ プロファイルの適用」を参照してください。

セキュリティ プロファイルを適用する前に、次の項を検討してください。

- ボイスメールのセキュリティの概要（P.10-1）
- ボイスメール セキュリティの設定のヒント（P.10-2）
- ボイスメール ポートのセキュリティ設定用チェックリスト（P.10-3）

ボイスメール ポート ウィザードで新規ボイスメール サーバにデバイス セキュリティ モードの設定を適用するには、次の手順を実行します。

手順

ステップ 1　Cisco Unified CallManager の管理ページで、［**ボイスメール**］>［**Cisco ボイスメールポートウィザード**］を選択します。

ステップ 2　ボイスメール サーバの名前を入力し、［**次へ**］をクリックします。

ステップ 3　追加するポートの数を選択して、［**次へ**］をクリックします。

ステップ 4　［Cisco ボイスメールデバイス情報］ウィンドウで、ドロップダウン リスト ボックスからデバイス セキュリティ モードを選択します。このオプションは、データベースで事前定義されています。デフォルト値は未選択です。

ステップ 5　『*Cisco Unified CallManager アドミニストレーション ガイド*』の説明に従って、その他のデバイス設定を実行します。［**次へ**］をクリックします。

ステップ 6　『*Cisco Unified CallManager アドミニストレーション ガイド*』の説明に従って、設定プロセスを続行します。要約ウィンドウが表示されたら、［**終了**］をクリックします。

追加情報

詳細については、P.10-6 の「関連項目」を参照してください。

その他の情報

関連項目

- システム要件（P.1-4）
- 相互作用および制限（P.1-6）
- 証明書（P.1-14）
- 設定用チェックリストの概要（P.1-25）
- ボイスメールのセキュリティの概要（P.10-1）
- ボイスメール セキュリティの設定のヒント（P.10-2）
- 単一ボイスメール ポートへのセキュリティ プロファイルの適用（P.10-4）
- ボイスメール ポート ウィザードでのセキュリティ プロファイルの適用（P.10-5）

シスコの関連マニュアル

- *Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity 4.x*
- *Cisco Unified Communications Operating System アドミニストレーション ガイド*