CHAPTER 10

ボイス メッセージング 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 メッセージングのセキュリティの概要

Cisco CallManager ボイス メッセージング ポートおよび Cisco Unity SCCP デバイスに対してセキュリティを設定すると、各デバイスが他のデバイスの証明書を受け入れた後に、認証済みデバイスに対して TLS 接続（ハンドシェイク）が開始されます。また、システムはデバイス間で SRTP ストリームを送信します。これは、デバイスで暗号化を設定した場合です。

デバイス セキュリティ モードが認証済みまたは暗号化済みになっている場合、Cisco Unity-CM TSP は Cisco CallManager TLS ポートを介して Cisco CallManager に接続します。デバイス セキュリティ モードがノンセキュアになっている場合、Cisco Unity TSP は Cisco CallManager SCCP ポートを介して Cisco CallManager に接続します。

セキュリティを設定する前に、次の情報を考慮してください。

- このマニュアルでは、サーバという用語は Cisco 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。
- このバージョンの Cisco 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 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 IP Telephony Platform Administration 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入れる必要があります。この作業の詳細については、『*Cisco IP Telephony Platform Administration Guide*』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、または何らかの理由で変更された場合は、Cisco IP Telephony Platform Administration 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 メッセージングは Cisco CallManager に登録できないため機能しません。
- Cisco Unity Telephony Integration Manager で指定する設定は、Cisco CallManager Administration で設定されているボイス メッセージング 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。SCCP 電話機セキュリティ プロファイルをポートに適用するときに、Cisco CallManager Administration でデバイス セキュリティ モードをボイス メッセージング ポートに適用します。

ヒント　デバイス セキュリティ モードの設定が Cisco CallManager と Cisco Unity で一致しない場合は、Cisco Unity ポートが Cisco 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 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 CallManager Administration 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。
- セキュリティ プロファイルをポートに適用するとき、Cisco CallManager は、プロファイルに対して存在する Certificate Authority Proxy Function（CAPF）設定を無視します。ボイス メッセージング ポートはこれらの設定をサポートしません。CAPF 設定ではなく、デバイス セキュリティ モードに基づいてプロファイルが選択されます。
- SCCP 電話機セキュリティ プロファイルで定義する設定の詳細については、P.5-1 の「電話機セキュリティ プロファイルの設定」を参照してください。

ボイス メッセージング ポートのセキュリティ設定用チェックリスト

ボイス メッセージング 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 メッセージング 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 Client をセキュア 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）
ステップ 3	Cisco IP Telephony Platform Administration 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 メッセージングのセキュリティの概要（P.10-2） • *Cisco IP Telephony Platform Administration Guide* • *Cisco CallManager Serviceability アドミニストレーション ガイド*
ステップ 4	Cisco CallManager Administration で、ボイス メッセージング ポートのセキュリティ プロファイルを設定し、プロファイルをポートに適用します。	• 単一ボイス メッセージング ポートへのセキュリティ プロファイルの適用（P.10-4） • Voice Messaging Port Wizard 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 メッセージング 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 CallManager 5.0 Integration Guide for Cisco Unity 4.x*
ステップ 6	Cisco CallManager Administration 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 CallManager 5.0 Integration Guide for Cisco Unity 4.x* • 単一ボイス メッセージング 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 メッセージング 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 メッセージング 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 メッセージングのセキュリティの概要（P.10-2）
- ボイス メッセージング 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 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 メッセージング 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、**SCCP Phone Security Profile** 設定を見つけます。ドロップダウン リスト ボックスから、ポートに適用するプロファイルを選択します。

ステップ 3　**Save** をクリックします。

ステップ 4　**Reset** 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。

Voice Messaging Port Wizard でのセキュリティ プロファイルの適用

Voice Messaging Port Wizard で既存のボイス メッセージング サーバの SCCP 電話機セキュリティ プロファイル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。

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 メッセージング 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 メッセージングのセキュリティの概要（P.10-2）
- ボイス メッセージング ポートのセキュリティ設定用チェックリスト（P.10-3）

Voice Messaging Port Wizard で新規ボイスメール サーバに SCCP 電話機セキュリティ プロファイル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 CallManager Administration で、**Voice Messaging > Voice Messaging Port Wizard** を選択します。

ステップ 2　新規ボイスメール　サーバにポートを追加するには、該当するオプション　ボタンをクリックして **Next** をクリックします。

ステップ 3　ボイスメール サーバの名前を入力し、**Next** をクリックします。

ステップ 4　追加するポートの数を選択して、**Next** をクリックします。

ステップ 5　Device Information ウィンドウで、SCCP Phone Security Profile ドロップダウン リスト ボックスから、適用するプロファイルを選択します。『*Cisco 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。**Next** をクリックします。

ステップ 6　『*Cisco 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。Summary ウィンドウが表示されたら、**Finish** 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）
- 対話および制限（P.1-6）
- 証明書の種類（P.1-13）
- 設定用チェックリストの概要（P.1-23）
- ボイス メッセージングのセキュリティの概要（P.10-2）
- 単一ボイス メッセージング ポートへのセキュリティ プロファイルの適用（P.10-4）
- Voice Messaging Port Wizard 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 CallManager 5.0 Integration Guide for Cisco Unity 4.x*
- *Cisco IP Telephony Platform Administration Guide*