セキュリティ用のボイスメール ポートの設定

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 CallManager ボイスメール 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 TSP は Cisco CallManager TLS ポートを介して Cisco CallManager に接続します。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 Integration Guide for Cisco Unity 4.0*』を参照してください。
- この章で説明する手順に加えて、クラスタ内の各サーバで C:\Program Files\Cisco\Certificates に Cisco Unity 証明書をコピーする必要があります。このタスクの詳細については、『*Cisco CallManager Integration Guide for Cisco Unity 4.0*』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。
- 何らかの理由で Cisco Unity 証明書の有効期限が切れた場合や証明書が変更された場合は、新規証明書がクラスタ内の各サーバに存在することを確認してください。証明書が一致しないと TLS 認証は失敗し、ボイスメールは 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ール 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。

ヒント　デバイス セキュリティ設定が 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。

- デバイス セキュリティ モードを変更するには、Cisco CallManager デバイスをリセットして Cisco Unity Integration Manager を再起動する必要があります。Cisco CallManager Administration で設定を変更した場合は、Cisco Unity でも設定を変更する必要があります。

デバイス セキュリティ モードの設定

デバイスに認証または暗号化を設定するには、次の作業のいずれか 1 つを実行します。

- ボイスメール　ポートおよびサポートされる電話機モデルに、システム　デフォルトのデバイス セキュリティ モードを設定する。
- Cisco CallManager Administration の Voice Mail Port Configuration ウィンドウで、単一デバイスにデバイス セキュリティ モードを設定する。
- Cisco Bulk Administration Tool を使用して、サポートされるボイスメール ポートにデバイス セキュリティ モードを設定する。

関連項目

- ボイスメールのセキュリティの概要（P.6-2）
- 対話および制限（P.1-6）
- セキュリティ デバイス システム デフォルトの設定（P.6-5）
- 単一デバイスに対するデバイス セキュリティ モードの設定（P.6-7）
- Voice Mail Port Wizard での Device Security Mode の設定（P.6-9）
- Device Security Mode 設定（P.6-11）
- セキュア ボイスメール ポート設定用チェックリスト（P.6-12）

セキュリティ デバイス システム デフォルトの設定

（注） この手順では、変更内容を有効にするためにデバイスをリセットして Cisco CallManager サービスを再起動する必要があります。

Device Security Mode エンタープライズ パラメータは、電話機とボイスメール ポートの両方に適用されます。このエンタープライズ パラメータを設定すると、すべてのボイスメール ポート、およびクラスタ内の Cisco IP Phone モデル 7940、7960、7970 に適用されます。

4.1(3) アップグレード前にこの設定が Authenticated または Encrypted として表示される場合は、Voice Mail Port ウィンドウで Device Security Mode を更新するまでボイスメール ポートがノンセキュアとして設定されていることに注意してください。

セキュリティ デバイス システム デフォルトを Authenticated または Encrypted に設定するには、次の手順を実行します。

手順

ステップ 1　Cisco CallManager Administration で **System > Enterprise Parameters** の順に選択します。

ステップ 2　Security Parameters セクションで **Device Security Mode** を探します。

ステップ 3　ドロップダウン リスト ボックスから、**Authenticated** または **Encrypted** を選択します。これらのオプションの詳細については、表 6-1 を参照してください。

ステップ 4　Enterprise Parameters ウィンドウ最上部の **Update** をクリックします。

ステップ 5　クラスタ内のすべてのデバイスをリセットします。P.1-11 の「デバイスのリセット、サービスの再起動、またはサーバおよびクラスタのリブート」を参照してください。

ステップ 6　変更内容を有効にするため、Cisco CallManager サービスを再起動します。

関連項目

- ボイスメールのセキュリティの概要（P.6-2）
- 対話および制限（P.1-6）
- Device Security Mode 設定（P.6-11）
- セキュア ボイスメール ポート設定用チェックリスト（P.6-12）

単一デバイスに対するデバイス セキュリティ モードの設定

単一デバイスにデバイス セキュリティ モードを設定するには、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。

デバイス セキュリティ モードを初めて設定した後やデバイス セキュリティ モードを変更した場合は、デバイスをリセットする必要があります。

Device Security Mode のデフォルト設定はノンセキュアです。

手順

ステップ 1　Cisco CallManager Administration で、**Feature > Voice Mail > Voice Mail Port** を選択します。

ステップ 2　デバイスの検索対象を指定してから **Find** をクリックするか、**Find** をクリックしてボイスメール ポートすべてのリストを表示します。

ボイスメール ポートをデータベースに追加していない場合、そのポートはリストに表示されません。ボイスメール ポートの追加については、『*Cisco CallManager アドミニストレーション ガイド*』を参照してください。

ステップ 3　ポートの設定ウィンドウを開くには、デバイス名をクリックします。

ステップ 4　**Device Security Mode** ドロップダウン リスト ボックスを見つけます。

ステップ 5　Device Security Mode ドロップダウン リスト ボックスから、設定するオプションを選択します。オプションの説明については、表 6-1 を参照してください。

ステップ 6　**Update** をクリックします。

ステップ 7　**Reset Port** をクリックします。

関連項目

- ボイスメールのセキュリティの概要（P.6-2）
- 対話および制限（P.1-6）
- Device Security Mode 設定（P.6-11）
- セキュア ボイスメール ポート設定用チェックリスト（P.6-12）

Voice Mail Port Wizard での Device Security Mode の設定

Voice Mail Port Wizard で既存のボイスメール サーバの Device Security Mode 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.6-7 の「単一デバイスに対するデバイス セキュリティ モードの設定」を参照してください。

Voice Mail Port Wizard で新規ボイスメール サーバの Device Security Mode を設定するには、次の手順を実行します。

手順

ステップ 1　Cisco CallManager Administration で、**Feature > Voice Mail > Voice Mail 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ます。

ステップ 5　Device Information ウィンドウで、Device Security Mode ドロップダウン リスト ボックスから **Authenticated** または **Encrypted** 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。

認証または暗号化のためのボイスメール ポートの検索

セキュリティ機能に関連付けられているボイスメール ポートを検索するには、Cisco CallManager Administration の Voice-Mail Port Find/List ウィンドウで Device Security Mode を選択します。

このオプションを選択すると、認証または暗号化をサポートするボイスメール ポートのリストが表示されます。このオプションを選択する場合、デバイスが Authenticated か Encrypted かを指定することもできます。

ボイスメール ポートを検索してリスト表示する方法については、『*Cisco CallManager アドミニストレーション ガイド*』を参照してください。

関連項目

Cisco CallManager アドミニストレーション ガイド

Device Security Mode 設定

Device Security Mode には、表 6-1 に示すオプションがあります。

表 6-1　Device Security Mode

オプション	説明
Use System Default	ボイスメール ポートはエンタープライズ パラメータ、Device Security Mode で指定した値を使用する。
Non-secure	ボイスメール ポートは、セキュリティ機能を使用しない。TCP 接続で Cisco CallManager が利用できる。
Authenticated	Cisco CallManager はボイスメール ポートの整合性と認証を提供する。ボイスメール ポートと Cisco CallManager の間で、NULL/SHA を使用する TLS 接続が確立される。
Encrypted	Cisco CallManager はボイスメール ポートの整合性、認証、および暗号化を提供する。ボイスメール ポートと Cisco CallManager の間で、AES128/SHA を使用する TLS 接続が確立される。

関連項目

- ボイスメールのセキュリティの概要（P.6-2）
- 対話および制限（P.1-6）
- セキュア ボイスメール ポート設定用チェックリスト（P.6-12）

セキュア ボイスメール ポート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 6-2 を参照してください。

表 6-2　ボイスメール ポートを保護するための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設定（P.5-1）
ステップ 3	Cisco Unity 証明書をクラスタ内の各サーバにコピーし、各サーバで Cisco CallManager サービスを再起動します。	• ボイスメールのセキュリティの概要（P.6-2） • *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。 **ヒント**　4.1(3) へのアップグレード前に Device Security Mode エンタープライズ パラメータを設定した場合、このステップは省いてください。ボイスメール ポートは、自動的にエンタープライズ パラメータ設定を使用します。	• セキュリティ デバイス システム デフォルトの設定（P.6-5） • 単一デバイスに対するデバイス　セキュリティ モードの設定（P.6-7） • Voice Mail Port Wizard での Device Security Mode の設定（P.6-9） • Device Security Mode 設定（P.6-11）
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 CallManager 4.1 Integration Guide for Cisco Unity 4.0*
ステップ 6	Cisco CallManager Administration でデバイスをリセットし、Cisco Unity Integration Manager を再起動します。	• *Cisco CallManager 4.1 Integration Guide for Cisco Unity 4.0* • デバイスのリセット、サービスの再起動、またはサーバおよびクラスタのリブート（P.1-11）