電話機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。

電話機のセキュリティ設定の概要

Cisco CallManager の新規インストールを実行している場合、Cisco CallManager クラスタはノンセキュア モードで起動します。Cisco CallManager のインストール後に電話機が起動すると、デバイスはすべてノンセキュアとして Cisco CallManager に登録されます。

Cisco CallManager 4.0(1) またはそれ以降のリリースからアップグレードした後は、アップグレード前に有効にしたセキュア モードで電話機が起動します。デバイスはすべて選択されたセキュリティ モードを使用して登録されます。

Cisco CallManager のインストールを行うと、対応する Cisco CallManager および TFTP サーバに自己署名証明書が作成されます。クラスタに認証を設定した後、Cisco CallManager はこの自己署名証明書を使用してサポートされた Cisco IP Phone を認証します。自己署名証明書が Cisco CallManager および TFTP サーバに存在していれば、Cisco CallManager はそれぞれの Cisco CallManager アップグレード時に証明書を再発行しません。

ヒント　サポートされていないシナリオまたは安全でないシナリオについては、P.1-6 の「制限」を参照してください。

Cisco CallManager は認証および暗号化のステータスをデバイス レベルで維持します。コールに関係するすべてのデバイスがセキュアとして登録されると、コール ステータスはセキュアとして登録されます。デバイスのいずれか 1 つがノンセキュアとして登録されると、発信者または受信者の電話機がセキュアとして登録されても、そのコールはノンセキュアとして登録されます。

ユーザが Cisco CallManager エクステンション モビリティを使用する場合、Cisco CallManager はデバイスの認証および暗号化ステータスを保持します。また、共有回線が設定されている場合も、Cisco CallManager はデバイスの認証および暗号化ステータスを保持します。

表 5-1 に、さまざまな Cisco IP Phone でサポートされる機能のリストを示します。

ヒント Cisco CallManager Administration で機能を設定することができますが、それらは互換性のあるファームウェア ロードをインストールするまで電話機で機能しない場合があります。

サポートされる電話機および機能の最新のリストは、Cisco CallManager 4.1(3) をサポートする電話機管理およびユーザ マニュアル、Cisco CallManager リリース ノート、Cisco CallManager サービス リリース readme ドキュメント、ご使用のファームウェア ロードをサポートするファームウェア マニュアルを参照してください。

表 5-1　Cisco IP Phone の機能

Cisco IP Phone モデル	サポートされている機能
Cisco IP Phone 7970 および 7971	イメージ認証、ファイル認証、デバイス認証、シグナリング暗号化、メディア暗号化、製造元でインストールされる証明書、ファクトリ リセット、および Web サーバ無効化などの電話機のセキュリティ強化 **ヒント** Cisco CallManager 4.1(3) の Cisco IP Phone 7970 および 7971 のデフォルト ファームウェア ロードは、セキュア SRST またはローカルで有効な証明書をサポートしていません。Cisco CallManager Administration でこれらの電話機モデルに対してローカルで有効な証明書とセキュア SRST を設定することはできますが、それらの設定を有効にするには、互換性のあるファームウェア ロードにアップグレードする必要があります。システムは、互換性のあるファームウェア ロードをインストールするまで、LSC およびセキュア SRST の設定を無視します。
Cisco IP Phone 7960 および 7940	イメージ認証、ファイル認証、デバイス認証、シグナリング暗号化、メディア暗号化、ローカルで有効な証明書、ファクトリ リセット、および Web サーバ無効化などの電話機のセキュリティ強化

表 5-1　Cisco IP Phone の機能（続き）

Cisco IP Phone モデル	サポートされている機能
Cisco IP Phone 7912、7905G、および 7902	イメージ認証、ファクトリ リセット、および Web サーバ無効化、Gratuitous ARP 設定無効化、Setting Access 設定無効化などの電話機のセキュリティ強化
Cisco IP Phone 7910	イメージ認証

ヒント　暗号化された Cisco IP Phone に対して共有回線を設定する場合は、暗号化に対して回線を共有するデバイスをすべて設定します。つまり、すべてのデバイスのデバイス セキュリティ モードを暗号化済みに設定します。

セキュリティをサポートする電話機に、特定のセキュリティ関連設定を構成して表示することができます。たとえば、サポートされている電話機で、電話機にインストールされている証明書がローカルで有効な証明書（LSC）か製造元でインストールされる証明書（MIC）かを確認できます。セキュリティ メニューおよびアイコンの詳細については、使用している電話機モデルおよびこのバージョンの Cisco CallManager をサポートする Cisco IP Phone 管理およびユーザ マニュアルを参照してください。

同様に、Cisco CallManager がコールを認証済みまたは暗号化済みとして分類すると、コールの状態を示すアイコンが電話機に表示されます。Cisco CallManager がコールを認証済みまたは暗号化済みとして分類する場合を判別するには、P.1-6 の「制限」を参照してください。

次のタスクを実行して、サポートされる電話機のセキュリティを設定します。

- サポートされる電話機で Locally Significant Certificate（LSC; ローカルで有効な証明書）をインストールまたはアップグレードし、証明書を削除またはトラブルシューティングする。
- サポートされる電話機に、Device Security Mode を使用して認証または暗号化を設定する。
- Cisco CallManager Administration で電話機の設定を無効にして電話機のセキュリティを強化する。

関連項目

- 電話機におけるローカルで有効な証明書のインストール、アップグレード、削除、またはトラブルシューティング（P.5-6）
- デバイス セキュリティ モードの設定（P.5-7）
- Device Security Mode 設定（P.5-13）
- 認証、暗号化、LSC ステータスによる電話機の検索（P.5-14）
- 電話機のセキュリティ強化（P.5-15）
- 電話機のセキュリティ強化作業の実行（P.5-18）

電話機におけるローカルで有効な証明書のインストール、アップグレード、削除、またはトラブルシューティング

ローカルで有効な証明書を電話機でインストール、アップグレード、削除、またはトラブルシューティングするには、Cisco CallManager Administration の Phone Configuration ウィンドウで CAPF 設定値を構成する必要があります。CAPF 設定値を構成する方法については、P.4-1 の「Certificate Authority Proxy Function の使用方法」を参照してください。

関連項目

- CAPF の設定用チェックリスト（P.4-10）
- CAPF システムの対話および要件（P.4-5）
- デバイス セキュリティ モードの設定（P.5-7）
- 認証、暗号化、LSC ステータスによる電話機の検索（P.5-14）
- 電話機のセキュリティ強化（P.5-15）
- 電話機のセキュリティ強化作業の実行（P.5-18）
- トラブルシューティング（P.9-1）

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。

- 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 Phone 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、サポートされる電話機モデルにデバイス セキュリティ モードを設定する。

ヒント　デバイス セキュリティ モードを設定するには、ローカルで有効な証明書または製造元でインストールされる証明書が電話機に必要です。

クラスタ セキュリティ モードがノンセキュアになっている場合は、Cisco CallManager Administration でデバイス セキュリティ モードが認証済みまたは暗号化済みと示されていても、電話機の設定ファイルのデバイス セキュリティ モードはノンセキュアです。このような場合、電話機は、クラスタ内で SRST 対応ゲートウェイおよび Cisco CallManager サーバとのノンセキュア接続を試行します。

クラスタ セキュリティ モードがノンセキュアになっている場合は、デバイス セキュリティ モードなど、Cisco CallManager Administration 内のセキュリティ関連の設定が無視されます。Cisco CallManager Administration 内の設定は削除されませんが、セキュリティは提供されません。

デバイス セキュリティ モードの設定内容については、P.5-13 の「Device Security Mode 設定」を参照してください。

関連項目

- 電話機のセキュリティ設定の概要（P.5-2）
- 対話および制限（P.1-6）
- Cisco CTL Provider サービスのアクティブ化（P.3-6）

- Cisco CTL クライアントの設定（P.3-15）
- CTL ファイルの更新（P.3-21）
- Device Security Mode 設定（P.5-13）
- Certificate Authority Proxy Function の使用方法（P.4-1）
- トラブルシューティング（P.9-1）

サポートされる電話機モデルに対するセキュリティ 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。

Cisco CallManager Administration で、すべての電話機タイプのセキュリティ デバイス システム デフォルトは Non-Secure と表示されます。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。詳細については、表 5-2 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

- システム要件（P.1-5）
- 対話および制限（P.1-6）
- デバイス セキュリティ モードの設定（P.5-7）
- Certificate Authority Proxy Function の使用方法（P.4-1）

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。

Cisco CallManager Administration の Phone Configuration ウィンドウで Device Security Mode を設定すると、デバイス設定 .xml ファイルが再構成されます。デバイス セキュリティ モードを初めて設定した後、あるいはデバイス 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。リセットすると、電話機は新しい設定ファイルを要求します。

手順

ステップ 1　Cisco CallManager Administration で **Device > Phone** の順に選択します。

ステップ 2　電話機の検索対象を指定して **Find** をクリックするか、電話機すべてのリストを表示するために **Find** をクリックします。

データベースに電話機を追加していない場合、電話機はリストに表示されません。IP Phone 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　デバイス名をクリックして、デバイスの Phone Configuration ウィンドウを開きます。

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。

電話機タイプがセキュリティをサポートしていない場合、このオプションは表示されません。その電話機タイプには認証も暗号化も設定することができません。

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 5-2 を参照してください。

Device Security Mode ドロップダウン リスト ボックスは、電話機が認証または暗号化をサポートしている場合にだけ表示されます。たとえば、電話機が暗号化をサポートしていない場合、暗号化オプションはドロップダウン リスト ボックスに表示されません。

ステップ 6　**Update** をクリックします。

ステップ 7　**Reset Phone** をクリックします。

注意　電話機をリセットすると、システムはゲートウェイを介して行われているすべてのコールを終了します。

関連項目

- 電話機のセキュリティ設定の概要（P.5-2）
- 対話および制限（P.1-6）
- Device Security Mode 設定（P.5-13）
- Certificate Authority Proxy Function の使用方法（P.4-1）

Cisco Bulk Administration Tool を使用したデバイス セキュリティ モードの設定

Cisco CallManager 4.1(3) をサポートする Cisco Bulk Administration Tool を使用して、暗号化または認証をサポートする特定の電話機モデルにデバイス セキュリティ モードを設定することができます。この作業の実行方法の詳細については、このバージョンの Cisco CallManager をサポートする『*Bulk Administration Tool ユーザ ガイド*』を参照してください。

関連項目

- 電話機のセキュリティ設定の概要（P.5-2）
- 対話および制限（P.1-6）
- Device Security Mode 設定（P.5-13）
- Certificate Authority Proxy Function の使用方法（P.4-1）
- *Bulk Administration Tool ユーザ ガイド*

Device Security Mode 設定

Device Security Mode には、表 5-2 に示すオプションがあります。

表 5-2　Device Security Mode

オプション	説明
Use System Default	電話機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	電話機にイメージ認証以外のセキュリティ機能はない。TCP 接続で Cisco CallManager が利用できる。
Authenticated	Cisco CallManager は電話機の整合性と認証を提供する。NULL/SHA を使用する TLS 接続を開始する。
Encrypted	Cisco CallManager は電話機の整合性、認証、および暗号化を提供する。AES128/SHA を使用する TLS 接続を開始する。

関連項目

- 電話機のセキュリティ設定の概要（P.5-2）
- 対話および制限（P.1-6）
- デバイス セキュリティ モードの設定（P.5-7）
- Certificate Authority Proxy Function の使用方法（P.4-1）
- *Bulk Administration Tool ユーザ ガイド*

認証、暗号化、LSC ステータスによる電話機の検索

セキュリティ機能に関連付けられている電話機を検索するため、Cisco CallManager Administration の Phone Find/List ウィンドウで次の基準のどちらかを選択できます。

- **Device Security Mode**：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電話機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。Find ボタンをクリックすると、電話機モデル、Device Security Mode、Device Name、Description、Directory Number、Owner User ID などが表示されます（設定されている場合）。
- **LSC Status**：このオプションを選択すると、ローカルで有効な証明書のインストール、アップグレード、削除、またはトラブルシューティングに CAPF を使用する電話機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、CAPF によって現在実行されている Certification Operation を指定することもできます。たとえば、Operation Pending、Success、Upgrade Failed、Delete Failed、Troubleshoot Failed などがあります。Find ボタンをクリックすると、電話機モデル、LSC Status、Device Name、Description、Directory Number、および Owner User ID が表示されます（設定されている場合）。

電話機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。

ヒント　Cisco CallManager Administration の Phone Find/List ウィンドウでは、デバイスの削除およびリセットも実行できます。

関連項目

- *Cisco CallManager アドミニストレーション ガイド*
- Certificate Authority Proxy Function の使用方法（P.4-1）

電話機のセキュリティ強化

電話機のセキュリティを強化するには、Cisco CallManager Administration の Phone Configuration ウィンドウで作業を実行する必要があります。この項では、次のトピックについて取り上げます。

Gratuitous ARP 設定の無効化

デフォルトで Cisco IP Phone は Gratuitous ARP パケットを受け入れます。デバイスによって使用されるパケットは、ネットワーク上にデバイスがあることを宣言します。しかし、攻撃者はこうしたパケットを使用して有効なネットワーク デバイスのスプーフィングを行うことができます。たとえば、攻撃者はデフォルト ルータを宣言するパケットを送信できます。必要に応じて、Cisco CallManager Administration の Phone Configuration ウィンドウで Gratuitous APP 設定を無効にすることができます。

（注）　この設定を無効化しても、電話機はデフォルト　ルータを識別することができます。

Web Access 設定の無効化

電話機の Web サーバ機能を無効にすると、統計および設定情報を提供する電話機の内部 Web ページにアクセスできなくなります。電話機の Web ページにアクセスできないと、Cisco Quality Report Tool などの機能が正しく動作しません。また Web サーバを無効にすると、CiscoWorks など、Web アクセスに依存するサービサビリティ アプリケーションにも影響があります。

Web サービスが無効かどうかを判別するため、電話機はサービスの無効 / 有効を示す設定ファイル内のパラメータを解析します。Web サービスが無効であれば、電話機はモニタリング用に HTTP ポート 80 を開かず、電話機の内部 Web ページに対するアクセスをブロックします。

PC Voice VLAN Access 設定の無効化

デフォルトで Cisco IP Phone はスイッチ ポート（上流のスイッチを向くポート）で受信したすべてのパケットを PC ポートに転送します。Cisco CallManager Administration の Phone Configuration ウィンドウで PC Voice VLAN Access 設定を無効にすると、ボイス VLAN 機能を使用する PC ポートから受信したパケットは廃棄されます。さまざまな Cisco IP Phone モデルがそれぞれの方法でこの機能を使用しています。

- Cisco IP Phone 7940/7960 モデルは、PC ポートで送受信される、ボイス VLAN のタグが付いたパケットをすべて廃棄する。
- Cisco IP Phone 7970 モデルは、PC ポートで送受信され、802.1Q タグが含まれる ボイス VLAN 上のパケットをすべて廃棄する。
- Cisco IP Phone 7912 モデルはこの機能を実行できない。

Setting Access 設定の無効化

デフォルトでは、Cisco IP Phone の Settings ボタンを押すと、電話機の設定情報を含むさまざまな情報にアクセスできます。Cisco CallManager Administration の Phone Configuration ウィンドウで Setting Access 設定を無効にすると、電話機で Settings ボタンを押したときに通常は表示されるすべてのオプションにアクセスできなくなります。オプションには、Contrast、Ring Type、Network Configuration、Model Information、および Status 設定があります。

これらの設定は、Cisco CallManager Administration の設定を無効にすると、電話機に表示されません。設定を無効にした場合、電話機ユーザは Volume ボタンに関連付けられた設定を保存できません。たとえば、ユーザは音量を保存できなくなります。

この設定を無効にすると、電話機の現在の Contrast、Ring Type、Network Configuration、Model Information、Status、および Volume 設定が自動的に保存されます。これらの電話機設定を変更するには、Cisco CallManager Administration で Setting Access 設定を有効にする必要があります。

PC Port 設定の無効化

デフォルトで Cisco CallManager は、PC ポートのあるすべての Cisco IP Phone 上で PC ポートを有効にします。必要に応じて、Cisco CallManager Administration の Phone Configuration ウィンドウで PC Port 設定を無効にすることができます。PC ポートを無効にすると、ロビーや会議室の電話機で役立ちます。

関連項目

- 電話機のセキュリティ設定の概要（P.5-2）
- 電話機のセキュリティ強化作業の実行（P.5-18）
- *Cisco IP Phone アドミニストレーション ガイド for Cisco CallManager*

電話機のセキュリティ強化作業の実行

注意　次の手順を実行すると、電話機の機能が無効になります。

次の手順を実行してください。

手順

ステップ 1　Cisco CallManager Administration で **Device > Phone** の順に選択します。

ステップ 2　電話機の検索対象を指定して **Find** をクリックするか、電話機すべてのリストを表示するために **Find** をクリックします。

ステップ 3　デバイス名をクリックして、デバイスの Phone Configuration ウィンドウを開きます。

ステップ 4　次の製品固有のパラメータを探します。

- PC Port
- Settings Access
- Gratuitous ARP
- PC Voice VLAN Access
- Web Access

ヒント　これらの設定に関する情報を確認するには、Phone Configuration ウィンドウでパラメータの横に表示されている i ボタンをクリックします。

ステップ 5　無効にする各パラメータのドロップダウン リスト ボックスから、**Disabled** を選択します。

ステップ 6　**Update** をクリックします。

関連項目

- 電話機のセキュリティ設定の概要（P.5-2）
- Gratuitous ARP 設定の無効化（P.5-15）
- Web Access 設定の無効化（P.5-15）
- PC Voice VLAN Access 設定の無効化（P.5-16）
- Setting Access 設定の無効化（P.5-16）
- PC Port 設定の無効化（P.5-17）