電話機のセキュリティの概要

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機能について

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デバイス セキュリティ 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 5.0(1) のインストールを行うと、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。新しい証明書エントリで新しい CTL ファイルを作成する必要があります。

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「対話および制限」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。いずれか 1 つのデバイス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。

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、回線を共有するすべてのデバイスを暗号化用に設定します。つまり、暗号化をサポートするセキュリティ プロファイルを適用して、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。

サポートされる電話機のモデル

このセキュリティ ガイドでは、各 Cisco IP Phone でサポートされるセキュリティ機能を示しません。使用している電話機でサポートされるセキュリティ機能の一覧については、Cisco CallManager 5.0(1) をサポートする電話機の管理マニュアルおよびユーザ マニュアル、または、使用しているファームウェア ロードをサポートするファームウェアのマニュアルを参照してください。

Cisco CallManager Administration でセキュリティ機能を設定できますが、Cisco TFTP サーバで互換ファームウェア ロードをインストールするまで、その機能は動作しません。

電話機のセキュリティ設定の確認

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、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 の管理およびユーザ マニュアルを参照してください。

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「対話および制限」を参照してください。

電話機のセキュリティ設定用チェックリスト

サポートされる電話機のセキュリティを設定する作業を表 4-1 で説明します。

表 4-1　電話機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 クライアントを設定し、クラスタ セキュリティ モードを Secure Mode にしていない場合、設定します。	Cisco CTL クライアントの設定（P.3-1）
ステップ 2	電話機に、ローカルで有効な証明書（LSC）または製造元でインストールされる証明書（MIC）が含まれていない場合、Certificate Authority Proxy Function（CAPF）を使用して LSC をインストールします。	Certificate Authority Proxy Function の使用方法（P.6-1）
ステップ 3	電話機のセキュリティ プロファイルを設定します。	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 4	電話機のセキュリティ プロファイルを電話機に適用します。	SCCP または SIP 電話機セキュリティ プロファイルの適用（P.5-9）
ステップ 5	SIP 電話機がダイジェスト認証をサポートする場合、Cisco CallManager Administration の End User ウィンドウで、ダイジェスト クレデンシャルを設定します。	• End User Configuration ウィンドウでのダイジェスト クレデンシャルの設定（P.8-4） • エンド ユーザ ダイジェスト クレデンシャルの設定内容（P.8-4）
ステップ 6	ダイジェスト クレデンシャルを設定した後、Cisco CallManager Administration の Phone Configuration ウィンドウで、Digest User を選択します。	Phone Configuration ウィンドウでのダイジェスト ユーザの設定（P.8-5）
ステップ 7	Cisco SIP IP Phone 7960 または 7940 で、End User Configuration ウィンドウで設定したダイジェスト認証ユーザ名およびパスワード（ダイジェスト クレデンシャル）を入力します。	『*Cisco CallManager セキュリティ ガイド*』では、電話機でダイジェスト認証クレデンシャルを入力する手順について説明しません。この作業の実行方法については、使用している電話機モデルとこのバージョンの Cisco CallManager をサポートする Cisco IP Phone の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 8	電話機設定ファイルを暗号化します（電話機がこの機能をサポートする場合）。	暗号化された電話機設定ファイルの設定（P.7-1）
ステップ 9	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します。	電話機のセキュリティ強化（P.9-1）

その他の情報

関連項目

- 対話および制限（P.1-6）
- 認証、整合性、および許可の概要（P.1-15）
- 暗号化の概要（P.1-20）
- 設定用チェックリストの概要（P.1-23）
- Certificate Authority Proxy Function の使用方法（P.6-1）
- 電話機のセキュリティ設定用チェックリスト（P.4-3）
- 電話機セキュリティ プロファイルの設定（P.5-1）
- 暗号化された電話機設定ファイルの設定（P.7-1）
- 電話機のセキュリティ強化（P.9-1）

シスコの関連マニュアル

- *Cisco IP Phone アドミニストレーション ガイド for Cisco CallManager*
- *Cisco CallManager トラブルシューティング ガイド*