CHAPTER 25

Cisco PCA および IMAP 電子メール クライアントから Cisco Unity Connection へのアクセスの保護

この章では、Cisco Personal Communications Assistant（Cisco PCA）および IMAP 電子メール クライアントから Cisco Unity Connection へのアクセスを保護するために、証明書署名要求を作成し、SSL 証明書を発行し（または外部認証局に発行してもらい）、Cisco Unity Connection サーバに証明書をインストールする方法について説明します。

次の各項を参照してください。

SSL 証明書を作成してインストールするかどうかの決定

Cisco Unity Connection をインストールすると、ローカル証明書が自動的に作成されてインストールされ、Cisco PCA と Connection の間、および IMAP 電子メール クライアントと Connection の間の通信を保護します。つまり、Cisco PCA と Connection の間のすべてのネットワーク トラフィック（ユーザ名、パスワード、その他のテキスト データ、およびボイス メッセージを含む）が自動的に暗号化されます。また、IMAP クライアントで暗号化を有効にしている場合は、IMAP 電子メール クライアントと Connection の間のネットワーク トラフィックが自動的に暗号化されます。ただし、man-in-the-middle 攻撃の危険性を低減したい場合は、この章の手順を実行してください。

Cisco PCA の Web サイトでは、ユーザが Connection でメッセージおよび個人設定を管理するために使用する Web ツールにアクセスできます。IMAP クライアントから Connection ボイス メッセージへのアクセスは、ライセンスが必要な機能であることに注意してください。

SSL 証明書をインストールすると決めた場合は、ユーザのワークステーション上の信頼されたルート ストアに認証局の信頼証明書を追加することも検討することをお勧めします。追加しないと、Cisco PCA にアクセスするユーザ、および一部の IMAP 電子メール クライアントで Connection ボイス メッセージにアクセスするユーザに対して、Web ブラウザでセキュリティ警告が表示されます。

（セキュリティ警告の管理については、『*Cisco Unity Connection ユーザワークステーション セットアップ ガイド*』の「Cisco Personal Communications Assistant へのアクセスの設定」の章の「SSL 接続で自己署名証明書を使用する場合のセキュリティ警告の管理」の項を参照してください。サポートされている IMAP 電子メール クライアントの設定については、『*Cisco Unity Connection ユーザワークステーション セットアップ ガイド*』の「Cisco Unity Connection ボイス メッセージにアクセスするための電子メール アカウントの設定」の章を参照してください）

SSL サーバ証明書の作成とインストール

SSL サーバ証明書を作成してインストールし、Cisco Personal Communications Assistant および IMAP 電子メール クライアントから Cisco Unity Connection へのアクセスを保護するには、次の作業を行います。

1. Microsoft 証明書サービスを使用して証明書を発行する場合は、Microsoft 証明書サービスをインストールします。P.25-3 の手順「Microsoft 証明書サービス コンポーネントをインストールする」を実行します。

   別のアプリケーションを使用して証明書を発行する場合は、そのアプリケーションをインストールします。インストール手順については、製造元のマニュアルを参照してください。次に、ステップ 2. に進みます。

   外部認証局を使用して証明書を発行する場合は、ステップ 2. に進みます。

（注） Microsoft 証明書サービス、または証明書署名要求を作成できる別のアプリケーションをすでにインストールしている場合は、この手順をスキップしてください。

2. 証明書署名要求を作成します。次に、Microsoft 証明書サービス、または証明書を発行する別のアプリケーションをインストールしたサーバに、証明書署名要求をダウンロードします。あるいは、証明書署名要求を外部 Certification Authority（CA; 認証局）に送信するために使用できるサーバに、証明書署名要求をダウンロードします。P.25-4 の手順「証明書署名要求を作成してダウンロードする」を実行します。
3. Microsoft 証明書サービスを使用してサーバ証明書を発行する場合は、P.25-5 の手順「サーバ証明書を発行する（Microsoft 証明書サービスを使用して証明書を発行する場合のみ）」を実行します。

   別のアプリケーションを使用して証明書を発行する場合は、そのアプリケーションのドキュメントで、証明書を発行する手順を参照してください。

   外部 CA を使用して証明書を発行する場合は、外部 CA に証明書署名要求を送信します。外部 CA から証明書が返送された後、ステップ 4. に進みます。
4. Cisco Unity Connection サーバにサーバ証明書をインストールします。P.25-6 の手順「証明書をインストールする」を実行します。

Microsoft 証明書サービス コンポーネントをインストールする

ステップ 1　Cisco PCA を使用するすべてのクライアント コンピュータ、または IMAP クライアントを使用して Cisco Unity Connection ボイス メッセージにアクセスするすべてのクライアント コンピュータによって解決できる DNS 名（FQDN）または IP アドレスを持つ任意のサーバで、ローカル Administrators グループのメンバーであるアカウントを使用して Windows にログオンします。

ステップ 2　Windows の［スタート］メニューから［**設定**］>［**コントロール パネル**］>［**プログラムの追加と削除**］をクリックします。

ステップ 3　［プログラムの追加と削除］コントロール パネルの左ペインで、［**Windows コンポーネントの追加と削除**］をクリックします。

ステップ 4　［Windows コンポーネント］ダイアログボックスで、［**証明書サービス**］チェックボックスをオンにします。この他の項目は変更しないでください。

ステップ 5　コンピュータ名およびドメイン　メンバシップの変更ができなくなるという警告が表示された場合は、［**はい**］をクリックします。

ステップ 6　［次へ］をクリックします。

ステップ 7　［証明機関の種類］ページで、**［スタンドアロンのルート CA］**をクリックし、**［次へ］**をクリックします（スタンドアロンの認証局（CA）は、Active Directory を必要としない CA です）。

ステップ 8　［CA 識別情報］ページの［この CA の共通名］フィールドに、認証局の名前を入力します。

ステップ 9　［識別名のサフィックス］フィールドで、デフォルト値をそのまま使用します。

ステップ 10［有効期間］で、デフォルト値の**［5 年］**をそのまま使用します。

ステップ 11［次へ］をクリックします。

ステップ 12［証明書データベースの設定］ページで、**［次へ］**をクリックしてデフォルト値をそのまま使用します。

コンピュータ上でインターネット インフォメーション サービスが動作しているため、停止してから処理を続行する必要があるというメッセージが表示された場合は、**［はい］**をクリックしてサービスを停止します。

ステップ 13 Windows Server 2003 ディスクをドライブに挿入するように要求された場合は、Cisco Unity Connection ディスク（同じ必須ソフトウェアが収録されています）または Windows Server 2003 ディスクを挿入します。

ステップ 14［Windows コンポーネント ウィザードの完了］ダイアログボックスで、**［完了］**をクリックします。

ステップ 15［プログラムの追加と削除］ダイアログボックスを閉じます。

証明書署名要求を作成してダウンロードする

ステップ 1　Cisco Unified オペレーティングシステムの管理にログインします。

ステップ 2　［セキュリティ（Security）］メニューで、**［証明書の管理（Certificate Management）］**をクリックします。

ステップ 3　［証明書の一覧（Certificate List）］ページで、**［CSR の作成（Generate CSR）］**をクリックします。

ステップ 4　［証明書署名要求の作成（Generate Certificate Signing Request）］ページの**［証明書の名前（Certificate Name）］**リストで、**［Tomcat］**をクリックします。

ステップ 5　**［CSR の作成（Generate CSR）］**をクリックします。

ステップ 6　［ステータス（Status）］領域に、CSR が正常に生成されたというメッセージが表示された後、**［閉じる（Close）］**をクリックします。

ステップ 7　［証明書の一覧（Certificate List）］ページで、**［CSR のダウンロード（Download CSR）］**をクリックします。

ステップ 8　［証明書署名要求のダウンロード（Download Certificate Signing Request）］ページの**［証明書の名前（Certificate Name）］**リストで、**［Tomcat］**をクリックします。

ステップ 9　**［CSR のダウンロード（Download CSR）］**をクリックします。

ステップ 10　［ファイルのダウンロード］ダイアログボックスで、**［保存］**をクリックします。

ステップ 11　［名前を付けて保存］ダイアログボックスの**［ファイルの種類］**リストで、**［すべてのファイル］**をクリックします。

ステップ 12　Microsoft 証明書サービスをインストールしたサーバ上、または CSR を外部認証局に送信するために使用できるサーバ上の場所に、ファイル **tomcat.csr** を保存します。

ステップ 13　［証明書署名要求のダウンロード（Download Certificate Signing Request）］ページで、**［閉じる（Close）］**をクリックします。

サーバ証明書を発行する（Microsoft 証明書サービスを使用して証明書を発行する場合のみ）

ステップ 1　Microsoft 証明書サービスをインストールしたサーバ上で、Domain Admins グループに所属するアカウントを使用して Windows にログインします。

ステップ 2　Windows の［スタート］メニューで、**［プログラム］>［管理ツール］>［証明機関］**をクリックします。

ステップ 3　左ペインで、**［証明機関（ローカル）］>［< 認証局名 >］**を展開します。< 認証局名 > は、P.25-3 の手順「Microsoft 証明書サービス コンポーネントをインストールする」で Microsoft 証明書サービスをインストールしたときに認証局に付けた名前です。

ステップ 4　認証局の名前を右クリックし、**［すべてのタスク］>［新しい要求の送信］**をクリックします。

ステップ 5　P.25-4 の手順「証明書署名要求を作成してダウンロードする」で作成した最初の証明書署名要求ファイルの場所を参照し、ファイルをダブルクリックします。

ステップ 6　［証明機関］の左ペインで、**［保留中の要求］**をクリックします。

ステップ 7　ステップ 5 で送信した保留中の要求を右クリックし、**［すべてのタスク］>［発行］**をクリックします。

ステップ 8　［証明機関］の左ペインで、**［発行した証明書］**をクリックします。

ステップ 9　新しい証明書を右クリックし、**［すべてのタスク］>［バイナリ データのエクスポート］**をクリックします。

ステップ 10　［バイナリ データのエクスポート］ダイアログボックスで、［バイナリ データを含む列］リストの**［バイナリ証明書］**をクリックします。

ステップ 11　**［バイナリ データをファイルに保存する］**をクリックします。

ステップ 12　**［OK］**をクリックします。

ステップ 13　［バイナリ データの保存］ダイアログボックスで、パスとファイル名を入力し、この情報を書き留めます。この情報は以降の手順で必要になります。

Cisco Unity Connection サーバからアクセスできるネットワーク ロケーションを選択します。

ステップ 14［**OK**］をクリックします。

ステップ 15［証明機関］を閉じます。

証明書をインストールする

ステップ 1　Cisco Unified オペレーティングシステムの管理にログオンします。

ステップ 2　［セキュリティ（Security）］メニューで、**［証明書の管理（Certificate Management）］**をクリックします。

ステップ 3　［証明書の一覧（Certificate List）］ページで、**［証明書のアップロード（Upload Certificate）］**をクリックします。

ステップ 4　［証明書のアップロード（Upload Certificate）］ページの**［証明書の名前（Certificate Name）］**リストで、**［tomcat-trust］**をクリックします。

ステップ 5　［ルート証明書（Root Certificate）］フィールドに、Microsoft 証明書サービスまたは別のアプリケーションで発行した証明書ファイルの名前、または外部 CA から取得した証明書ファイルの名前を入力します。

ステップ 6　**［参照（Browse）］**をクリックします。

ステップ 7　［ファイルの選択］ダイアログボックスで、証明書ファイルの場所を参照し、ファイル名をクリックして、**［開く］**をクリックします。

ステップ 8　［証明書のアップロード（Upload Certificate）］ページで、**［ファイルのアップロード（Upload File）］**をクリックします。

ステップ 9　［ステータス（Status）］領域で、アップロードが成功したと報告された後、**［閉じる（Close）］**をクリックします。