CHAPTER 25

Cisco Unity Connection 8.x の SSL 設定

この章では、Cisco Unity Connection Administration、Cisco Personal Communications Assistant（Cisco PCA）、および IMAP 電子メール クライアントが Cisco Unity Connection へ安全にアクセスするための、証明書の署名要求の作成、SSL 証明書の発行（または外部の認証局による証明書の発行）、および Cisco Unity Connection サーバにおける証明書のインストールについて説明します。

Cisco PCA の Web サイトでは、ユーザが Connection でのメッセージと個人設定の管理に使用できる、各種 Web ツールにアクセスできます。IMAP クライアントから Connection のボイス メッセージへのアクセスは、ライセンスが必要な機能です。

次の項を参照してください。

- 「Cisco Unity Connection 8.x で SSL 証明書を作成およびインストールするかどうかの決定」（P.25-1）
- 「Cisco Unity Connection Administration、Cisco PCA、および IMAP 電子メール クライアントからの Cisco Unity Connection 8.x へのアクセスの保護」（P.25-2）
- 「Cisco Unity Connection 8.x への Microsoft 証明書サービスのインストール（Windows Server 2003 のみ）」（P.25-5）

Cisco Unity Connection 8.x で SSL 証明書を作成および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、インストールされて、Cisco PCA と Connection の間、および IMAP 電子メール クライアントと Connection の間の通信が保護されます。これは、Cisco PCA と Connection 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ることを意味します。また、IMAP クライアントで暗号化を有効にしている場合には、IMAP 電子メール クライアントと Connection 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、中間者攻撃のリスクを軽減する必要がある場合は、この章で説明する手順を実行してください。

SSL 証明書のインストールを決定した場合は、認証局の信頼証明書をユーザのワークステーションの信頼されたルート ストアに追加することも検討してください。この追加を行わないと、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 のボイス 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 アラートの管理については、『*User Workstation Setup Guide for Cisco Unity Connection*』（*Release 8.x*）「Setting Up Access to the Cisco Personal Communications Assistant in Cisco Unity Connection 8.x」の章にある「Managing Security Alerts When Using Self-Signed Certificates with SSL Connections in Cisco Unity Connection 8.x」の項を参照してください。サポートされる IMAP 電子メール クライアントの設定については、同じガイドの「Configuring an Email

Account to Access Cisco Unity Connection 8.x Voice Messages」の章を参照してください。このガイドは、http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/user_setup/guide/8xcucuwsx.htm から入手可能です)。

Cisco Unity Connection Administration、Cisco PCA、および IMAP 電子メール クライアントからの Cisco Unity Connection 8.x へのアクセスの保護

Cisco Unity Connection Administration、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、次のタスクを実行して、SSL サーバ証明書を作成し、インストールします。

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。Windows Server 2003 を実行しているサーバに Microsoft 証明書サービスをインストールする方法については、「Cisco Unity Connection 8.x への Microsoft 証明書サービスのインストール（Windows Server 2003 のみ）」（P.25-5）を参照してください。それ以降のバージョンの Windows Server を実行しているサーバに Microsoft 証明書サービスをインストールする方法については、Microsoft 社のドキュメントを参照してください。

   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。インストールの方法については、製造元が提供しているドキュメントを参照してください。その後で、タスク 2. に進みます。

   外部の認証局を使用して証明書を発行する場合は、タスク 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ある場合は、タスク 2. に進みます。

2. Connection クラスタが設定されている場合は、`set web-security` CLI コマンドをクラスタ内の両方の Connection サーバで実行し、両方のサーバに同じユーザの別名を割り当てます。ユーザの別名は、証明書署名要求と証明書に、自動的に含められます。`set web-security` CLI コマンドについては、該当する『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』を参照してください。このガイドは、http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html から入手可能です。

3. Connection クラスタが設定されている場合は、タスク 2. で割り当てたユーザの別名を含んでいる DNS A レコードを設定します。まず、パブリッシャ サーバをリストしてください。それによって、すべての IMAP 電子メール アプリケーションおよび Cisco Personal Communications Assistant が、Connection のボイス メッセージに同じ Connection サーバ名を使用してアクセスできるようになります。

4. 証明書署名要求を作成します。その後で、Microsoft 証明書サービスまたは証明書を発行するその他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するか、証明書署名要求を外部の CA に送る際に使用するサーバに要求をダウンロードします。「証明書署名要求を作成およびダウンロードするには」（P.25-3）の手順を行います。

   Connection クラスタが設定されている場合は、Connection クラスタ内の両方のサーバに対してこのタスクを実行します。

5. Microsoft 証明書サービスを使用して、発行元の証明書をエクスポートする場合、およびサーバの証明書を発行する場合は、「Cisco Unity Connection 8.x での発行元証明書のエクスポートとサーバ証明書の発行（Microsoft 証明書サービスのみ）」（P.25-6）の手順に従います。

   証明書の発行に別のアプリケーションを使用する場合は、証明書の発行についてアプリケーションの資料を参照してください。

   証明書の発行に外部の CA を使用する場合は、外部の CA に証明書署名要求を送信します。外部 CA から証明書が返されたら、タスク 6. に進みます。

   Connection クラスタが設定されている場合は、Connection クラスタ内の両方のサーバに対してこのタスクを実行します。

6. 発行元の証明書、およびサーバの証明書を Connection サーバへアップロードします。「Cisco Unity Connection サーバに発行元およびサーバの証明書をアップロードする方法」（P.25-4）の手順を行います。

   Connection クラスタが設定されている場合は、Connection クラスタ内の両方のサーバに対してこのタスクを実行します。

7. Connection IMAP サーバ サービスを再起動して、Connection および IMAP 電子メール クライアントが新しい SSL 証明書を使用するようにします。「Connection IMAP サーバ サービスを再起動するには」（P.25-5）の手順を行います。

   Connection クラスタが設定されている場合は、Connection クラスタ内の両方のサーバに対してこのタスクを実行します。

8. ユーザが Connection の管理、Cisco PCA、または IMAP 電子メール クライアントを使用して Connection にアクセスするたびに、セキュリティ警告が表示されないようにするには、ユーザが Connection にアクセスするすべてのコンピュータで次のタスクを実行します。

   - タスク 6. で Connection サーバにアップロードしたサーバ証明書を証明書ストアにインポートします。手順は、使用するブラウザまたは IMAP 電子メール クライアントによって異なります。詳細については、ブラウザまたは IMAP 電子メール クライアントのドキュメントを参照してください。
   - タスク 6. で Connection サーバにアップロードしたサーバ証明書を Java ストアにインポートします。手順は、クライアント コンピュータ上で実行されているオペレーティング システムによって異なります。詳細については、オペレーティング システムのドキュメントおよび Java ランタイム環境のドキュメントを参照してください。

証明書署名要求を作成およびダウンロードするには

ステップ 1　Cisco Unity Connection サーバで Cisco Unified Operating System Administration にサインインします。

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）] を選択します。

ステップ 3　[証明書の一覧（Certificate List）] ページで、[CSR の作成（Generate CSR）] を選択します。

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] を選択します。

ステップ 5　[CSR の作成（Generate CSR）] を選択します。

ステップ 6　CSR が正常に生成されたことを示すメッセージがステータス エリアに表示されたら、[閉じる（Close）] を選択します。

ステップ 7　[証明書の一覧（Certificate List）] ページで、[Download CSR（CSR のダウンロード）] を選択します。

ステップ 8　[証明書署名要求のダウンロード（Generate Certificate Signing Request）] ページの [証明書の名前（Certificate Name）] リストで、[tomcat] を選択します。

ステップ 9　[CSR のダウンロード（Download CSR）] を選択します。

ステップ 10　[ファイルのダウンロード（File Download）] ダイアログボックスで、[保存（Save）] を選択します。

ステップ 11　[名前を付けて保存（Save As）] ダイアログボックスの [ファイルの種類（Save As Type）] リストで、[すべての種類（All Files）] を選択します。

ステップ 12　**tomcat.csr** ファイルを、Microsoft 証明書サービスをインストールしたサーバ、または外部の認証局に CSR を送信するのに使用できるサーバ上の場所に保存します。

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）] を選択します。

Cisco Unity Connection サーバに発行元およびサーバの証明書をアップロードする方法

ステップ 1　証明書署名要求を作成した Cisco Unity Connection サーバで、Cisco Unified Operating System Administration にサインインします。

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）] を選択します。

（注）　[検索（Find）] を選択し、現在そのサーバにインストールされている証明書のリストを表示すると、既存の、自動的に生成された、Tomcat の自己署名証明書が表示されます。この証明書は、この手順でアップロードする Tomcat 証明書とは関係のないものです。

ステップ 3　発行元の証明書をアップロードします。

a.　[証明書の一覧（Certificate List）] ページで、[証明書のアップロード（Upload Certificate）] を選択します。

b.　[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] を選択します。

c.　[ルート証明書（Root Certificate）] フィールドは空白のままにします。

d.　[参照（Browse）] を選択し、発行元の CA 証明書のロケーションを参照します。

Microsoft 証明書サービスを使用して証明書を発行した場合、これは、「発行元の証明書をエクスポートしてサーバ証明書を発行する方法」（P.25-7）の手順 でエクスポートした発行元証明書のロケーションになります。

外部の認証局を使用して証明書を発行した場合、これは、外部認証局から受け取った発行元の CA 証明書のロケーションになります。

e.　ファイルの名前を選択します。

f.　[開く（Open）] を選択します。

g.　[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）] を選択します。

h.　アップロードに成功したことを示すメッセージがステータス エリアに表示されたら、[閉じる（Close）] を選択します。

ステップ 4　サーバ証明書をアップロードします。

a.　[証明書の一覧（Certificate List）] ページで、[証明書のアップロード（Upload Certificate）] を選択します。

b.　[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] を選択します。

c. [ルート証明書（Root Certificate）] フィールドに、ステップ 3 でアップロードした発行元証明書のファイル名を入力します。

d. [参照（Browse）] を選択して、サーバ証明書の場所を参照します。

証明書の発行に Microsoft 証明書サービスを使用した場合は、「発行元の証明書をエクスポートしてサーバ証明書を発行する方法」（P.25-7）の手順で発行したサーバ証明書がこの場所に保存されます。

証明書の発行に外部の認証局を使用した場合は、外部の認証局から受け取ったサーバ証明書がこの場所に保存されます。

e. ファイルの名前を選択します。

f. [開く（Open）] を選択します。

g. [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）] を選択します。

h. アップロードに成功したことを示すメッセージがステータス エリアに表示されたら、[閉じる（Close）] を選択します。

ステップ 5　Tomcat サービスを再起動します（このサービスは Cisco Unified Serviceability からは再起動できません）。

a. SSH アプリケーションを使用して Connection サーバにサインインします。

b. 次の CLI コマンドを使用して Tomcat サービスを再起動します。

```
utils service restart Cisco Tomcat
```

Connection IMAP サーバ サービスを再起動するには

ステップ 1　Cisco Unity Connection Serviceability にサインインします。

ステップ 2　[ツール（Tools）] メニューで [サービス管理（Service Management）] を選択します。

ステップ 3　[オプション サービス（Optional Services）] セクションで、Connection IMAP サーバ サービスに [停止（Stop）] を選択します。

ステップ 4　Connection IMAP サーバ サービスが正常に停止したことを示すメッセージがステータス エリアに表示されたら、このサービスに [開始（Start）] を選択します。

Cisco Unity Connection 8.x への Microsoft 証明書サービスのインストール（Windows Server 2003 のみ）

サードパーティの認証局を使用して SSL 証明書を発行する場合や、Microsoft 証明書サービスがすでにインストールされている場合は、この項の手順を省略してください。

Microsoft 証明書サービスを使用して独自の証明書を発行する場合で、Windows Server 2003 を実行しているサーバにこのアプリケーションをインストールする場合に、この項の手順を実行します。

ルート認証局（Microsoft 証明書サービスの一般的な名称）を Windows Server 2008 サーバにインストールする場合は、Windows Server 2008 のオンライン ヘルプを参照してください。

Microsoft 証明書サービス コンポーネントをインストールするには

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 のボイス メッセージにアクセスするすべてのクライアント コンピュータで解決できる DNS 名（FQDN）または IP アドレスを持つサーバ上で、ローカル Administrators グループのメンバであるアカウントを使用して Windows にサインインします。

ステップ 2　Windows の [スタート（Start）] メニューで、[設定（Settings）] > [コントロール パネル（Control Panel）] > [プログラムの追加と削除（Add or Remove Programs）] を選択します。

ステップ 3　[プログラムの追加と削除（Add or Remove Programs）] の左側のパネルで、[Windows コンポーネントの追加と削除（Add/Remove Windows Components）] を選択します。

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

ステップ 5　コンピュータ名の変更やドメイン メンバーシップの変更ができないことを通知する警告が表示されたら、[はい（Yes）] を選択します。

ステップ 6　[次へ（Next）] を選択します。

ステップ 7　[CA の種類（CA Type）] ページで、[スタンドアロンのルート CA（Stand-alone Root CA）] を選択し、[次へ（Next）] を選択します（スタンドアロンの認証局（CA）とは、Active Directory を必要としない CA です）。

ステップ 8　[CA の ID 情報（CA Identifying Information）] ページの [この CA の通常名（Common Name for This CA）] フィールドに、認証局の名前を入力します。

ステップ 9　[識別名サフィックス（Distinguished Name Suffix）] フィールドで、デフォルトの値を受け入れます。

ステップ 10　有効期間として、デフォルト値の [5 年（5 Years）] を受け入れます。

ステップ 11　[次へ（Next）] を選択します。

ステップ 12　[証明書データベース設定（Certificate Database Settings）] ページで、[次へ（Next）] を選択してデフォルト値を受け入れます。

インターネット インフォメーション サービスがコンピュータ上で実行されており、先に進むにはこのサービスを停止する必要があることを通知するメッセージが表示されたら、[はい（Yes）] を選択してこのサービスを停止します。

ステップ 13　Windows Server 2003 のディスクをドライブに挿入するように求められたら、そのように実行します。

ステップ 14　[Windows コンポーネントの完了ウィザード（Completing the Windows Components Wizard）] ダイアログボックスで、[終了（Finish）] を選択します。

ステップ 15　[プログラムの追加と削除（Add or Remove Programs）] ダイアログボックスを閉じます。

Cisco Unity Connection 8.x での発行元証明書のエクスポートとサーバ証明書の発行（Microsoft 証明書サービスのみ）

Microsoft 証明書サービスを使用して証明書を発行する場合だけ、次の手順を実行します。

発行元の証明書をエクスポートしてサーバ証明書を発行する方法

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で、Domain Admins グループのメンバであるアカウントを使用して Windows にサインインします。

ステップ 2　Windows の [スタート（Start）] メニューで、[プログラム（Programs）] > [管理ツール（Administrative Tools）] > [認証局（Certification Authority）] を選択します。

ステップ 3　左側のパネルで、[認証局（ローカル）（Certification Authority (Local)）] > [<認証局の名前>] を展開します。<認証局の名前> は、「Microsoft 証明書サービス コンポーネントをインストールするには」（P.25-6）の手順で 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になります。

ステップ 4　発行元の証明書をエクスポートします。

a. 認証局の名前を右クリックし、[プロパティ（Properties）] を選択します。

b. [全般（General）] タブで、[証明書の表示（View Certificate）] を選択します。

c. [詳細（Details）] タブを選択します。

d. [ファイルにコピー（Copy to File）] を選択します。

e. [証明書エクスポートウィザードへようこそ（Welcome to the Certificate Export Wizard）] ページで、[次へ（Next）] を選択します。

f. [エクスポート ファイル形式（Export File Format）] ページで [次へ（Next）] をクリックして、デフォルト値 [DER Encoded Binary X.509 (.CER)] を受け入れます。

g. [エクスポートするファイル（File to Export）] ページで、.cer ファイルのパスとファイル名を入力します。Connection サーバからアクセス可能なネットワーク上の場所を選択します。

パスとファイル名を書き留めます。この情報は後の手順で必要になります。

h. ウィザードでエクスポートが完了するまで、画面に表示される指示に従って操作します。

i. [OK] を選択して [証明書（Certificate）] ダイアログボックスを閉じ、もう一度 [OK] を選択して [プロパティ（Properties）] ダイアログボックスを閉じます。

ステップ 5　サーバ証明書を発行します。

a. 認証局の名前を右クリックし、[すべてのタスク（All Tasks）] > [新しい要求の送信（Submit New Request）] を選択します。

b. 「証明書署名要求を作成およびダウンロードするには」（P.25-3）の手順 で作成した証明書署名要求ファイルの場所に移動し、このファイルをダブルクリックします。

c. [認証局（Certification Authority）] の左側のパネルで [保留中の要求（Pending Requests）] を選択します。

d. b. 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（All Tasks）] > [発行（Issue）] を選択します。

e. [認証局（Certification Authority）] の左側のパネルで [発行済み証明書（Issued Certificates）] を選択します。

f. 新しい証明書を右クリックし、[すべてのタスク（All Tasks）] > [バイナリ データのエクスポート（Export Binary Data）] を選択します。

g. [バイナリ データのエクスポート（Export Binary Data）] ダイアログボックスの [バイナリ データが含まれている列（Columns that Contain Binary Data）] リストで、[バイナリ証明書（Binary Certificate）] を選択します。

h. [バイナリ データをファイルに保存（Save Binary Data to a File）] を選択します。

i. [OK] を選択します。

j. [バイナリ データの保存（Save Binary Data）] ダイアログボックスで、パスとファイル名を入力します。Cisco Unity Connection サーバからアクセス可能なネットワーク上の場所を選択します。

パスとファイル名を書き留めます。この情報は後の手順で必要になります。

k. [OK] を選択します。

ステップ 6　[認証局（Certification Authority）] を閉じます。