CHAPTER 9

SSL を使用した Cisco Unity Connection でのクライアント / サーバ接続の保護

この章では、証明書署名要求の作成、SSL 証明書の発行（または外部の認証局による発行）、証明書の Cisco Unity Connection サーバへのインストールによる 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 へのアクセスの保護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。

SSL 証明書をインストールして Cisco PCA、Cisco Unity Connection SRSV 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かどうかの決定

Cisco Unity Connection をインストールする場合、ローカル自己署名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 との間の通信、IMAP 電子メール クライアントと Connection との間の通信、および Connection SRSV と中央 Connection サーバとの間の通信が保護されます。これは、Cisco PCA と Connection と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、IMAP クライアントで暗号化を有効にした場合は IMAP 電子メール クライアントと Connection と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、Connection SRSV と中央 Connection サーバと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ることを意味しています。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。

（セキュリティ警告管理については、『*User Workstation Setup Guide for Cisco Unity Connection*』（*リリース 9.x*）の「Setting Up Access to the Cisco Personal Communications Assistant in Cisco Unity Connection 9.x」の章にある「Managing Security Alerts When Using Self-Signed Certificates with SSL Connections in Cisco Unity Connection」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 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/9x/user_setup/guide/9xcucuwsx.htm から入手可能です）。

自己署名証明書については、『Complete Reference Guide for Cisco Unity Connection Survivable Remote Site Voicemail (SRSV)』ガイドの「Securing Connections in Cisco Unity Connection Survivable Remote Site Voicemail 9.1(1)」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/9x/srsv/guide/9xcucsrsvx.html から入手可能です。

Connection の管理、Cisco PCA、Cisco Unity Connection SRSV、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

Cisco Unity Connection の管理、Cisco Personal Communications Assistant、Connection SRSV、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、「Microsoft 証明書サービスのインストール（Windows Server 2003 の場合のみ）」（P.9-14）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、Cisco Personal Communications Assistant、および Connection SRSV 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.9-4）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。

5. Microsoft 証明書サービスを使用してルート証明書のエクスポートおよびサーバ証明書の発行を行う場合は、「ルート証明書のエクスポートとサーバ証明書の発行（Microsoft 証明書サービスの場合のみ）」（P.9-15）の手順を実行します。

   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 にアップロードできるのは、PEM 形式（Base-64 エンコードされた DER）の証明書だけです。証明書のファイル名拡張子は .pem であることが必要です。証明書がこの形式でない場合、通常は、OpenSSL など、無償で使用できるユーティリティを使用して PEM 形式に変換できます。

   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. ルート証明書とサーバ証明書を Connection サーバにアップロードします。「ルート証明書とサーバ証明書を Cisco Unity Connection サーバにアップロードするには」（P.9-4）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.9-6）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 へのアクセスを行うすべてのコンピュータ上で、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 オペレーティング システムの管理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、[CSRCritical Services 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、[CSR のダウンロード（Download CSR）] 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（Download 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 [保存の種類（Save As Type）] リストで、[すべてのファイル（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。

ルート証明書とサーバ証明書を Cisco Unity Connection サーバにアップロードするには

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　ルート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）] を選択して、ルート CA 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、「ルート証明書をエクスポートし、サーバ証明書を発行するには」（P.9-15）の手順でエクスポートしたルート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ルート CA 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 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ルート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、「ルート証明書をエクスポートし、サーバ証明書を発行するには」（P.9-15）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 にログインします。

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。

Exchange の予定表、連絡先、および電子メールへのアクセスの保護

Exchange の予定表、連絡先、および電子メールへのアクセスの保護については、次のマニュアルを参照してください。

- *（Cisco Unity Connection 9.x）『Unified Messaging Guide for Cisco Unity Connection』（Release 9.x）*の「Configuring Cisco Unity Connection 9.x and Microsoft Exchange for Unified Messaging」の章。
http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/unified_messaging/guide/9xcucumgx.html から入手可能です。

Cisco Unified MeetingPlace へのアクセスの保護

MeetingPlace へのアクセスを保護するには、次のタスクを実行します。

1. MeetingPlace 用に SSL を設定します。詳細については、*『Administration Documentation for Cisco Unified MeetingPlace Release 8.0』*の「Configuring SSL for the Cisco Unified MeetingPlace Application Server」の章を参照してください。このガイドは、http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_maintenance_guides_list.html から入手可能です。
2. Connection と MeetingPlace を連動させます。Connection を MeetingPlace の予定表と連動するように設定するときには、セキュリティ トランスポート用に SSL を指定します。

   詳細については、次の資料を参照してください。

- *（Connection 9.x）『Unified Messaging Guide for Cisco Unity Connection』（Release 9.x）*の「Configuring Cisco Unity Connection 9.x and Cisco Unified MeetingPlace for Unified Messaging」の章。http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/unified_messaging/guide/9xcucumgx.html から入手可能です。

3. Connection サーバで、タスク 1. で MeetingPlace サーバにインストールしたサーバ証明書の入手元認証局のルート証明書をアップロードします。次の点に注意してください。
   - このルート証明書は、MeetingPlace サーバにインストールした証明書と同じものではありません。認証局のルート証明書には、MeetingPlace サーバにアップロードした証明書の信頼性を確認するのに使用できる、公開キーが含まれています。
   - Connection にアップロードできるのは、PEM 形式（Base-64 エンコードされた DER）の証明書だけです。証明書のファイル名拡張子は .pem であることが必要です。証明書がこの形式でない場合、通常は、OpenSSL など、無償で使用できるユーティリティを使用して PEM 形式に変換できます。
   - ルート証明書のファイル名には、スペースを含めることはできません。

ルート証明書を Connection サーバにアップロードするには

ステップ 1　管理者のアカウントとパスワードを使用して、Cisco Unified オペレーティング システムの管理にサインインします。

Connection のインストール時に作成した管理者アカウントは、Connection の管理へのサインインに使用するアカウントおよびパスワードとは異なります。

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　[証明書のアップロード（Upload Certificate）] を選択します。

ステップ 4　[証明書の名前（Certificate Name）] リストで、[Connection-trust] を選択します。

ステップ 5　[参照（Browse）] を選択し、MeetingPlace 用の証明書を発行した認証局のルート証明書が含まれているファイルを見つけます。

ステップ 6　[ファイルのアップロード（Upload File）] を選択します。

Cisco Unified MeetingPlace Express（Cisco Unity Connection）へのアクセスの保護

（注） Cisco Unity Connection 9.x では、Cisco Unified MeetingPlace Express との統合はサポートされていません。

MeetingPlace Express へのアクセスを保護するには、次のタスクを実行します。

1. MeetingPlace Express 用に SSL を設定します。詳細については、次を参照してください。
   a. http://docwiki.cisco.com/wiki/Cisco_Unified_MeetingPlace_Express%2C_Release_2.x にある DocWiki、『Cisco Unified MeetingPlace Express, Release 2.x』を表示します。
   b. 「Configuration and Maintenance Tasks」の「Configuring SSL and Managing Certificates for Cisco Unified MeetingPlace Express」を選択します。

2. Cisco Unity Connection と MeetingPlace Express を連動させます。Connection を MeetingPlace Express の予定表と連動するように設定するときには、セキュリティ トランスポート用に SSL を指定します。『*System Administration Guide for Cisco Unity Connection*』（*Release 9.x*）の「Creating Calendar and Contact Integrations in Cisco Unity Connection9.x」の章の「Creating a Calendar and Contact Integration with Cisco Unified MeetingPlace Express」の項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/9x/administration/guide/9xcucsagx.html から入手可能です。
3. Connection サーバで、タスク 1. で MeetingPlace Express サーバにインストールしたサーバ証明書の入手元認証局のルート証明書をアップロードします。次の点に注意してください。
   - このルート証明書は、MeetingPlace Express サーバにインストールした証明書と同じものではありません。認証局のルート証明書には、MeetingPlace Express サーバにアップロードした証明書の信頼性を確認するのに使用できる、公開キーが含まれています。
   - Connection にアップロードできるのは、PEM 形式（Base-64 エンコードされた DER）の証明書だけです。証明書のファイル名拡張子は .pem であることが必要です。証明書がこの形式でない場合、通常は、OpenSSL など、無償で使用できるユーティリティを使用して PEM 形式に変換できます。
   - ルート証明書のファイル名には、スペースを含めることはできません。

ルート証明書を Connection サーバにアップロードするには

ステップ 1　管理者のアカウントとパスワードを使用して、Cisco Unified オペレーティング システムの管理にサインインします。

Connection のインストール時に作成した管理者アカウントは、Connection の管理へのサインインに使用するアカウントおよびパスワードとは異なります。

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　[証明書のアップロード（Upload Certificate）] を選択します。

ステップ 4　[証明書の名前（Certificate Name）] リストで、[Connection-trust] を選択します。

ステップ 5　[参照（Browse）] を選択し、MeetingPlace 用の証明書を発行した認証局のルート証明書が含まれているファイルを見つけます。

ステップ 6　[ファイルのアップロード（Upload File）] を選択します。

LDAP ディレクトリへのアクセスの保護

LDAP サーバと Cisco Unity Connection の間で転送されるデータを保護する方法については、『*System Administration Guide for Cisco Unity Connection*』（Release 9.x）の「Integrating Cisco Unity Connection 9.x with an LDAP Directory」の章の「Uploading SSL Certificates on the Cisco Unity Connection Server」の項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/9x/administration/guide/9xcucsagx.html から入手可能です。

Connection ネットワーキングが設定されている場合の、Connection と Cisco Unity ゲートウェイ サーバの間の通信の保護

Connection の管理、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、「Microsoft 証明書サービスのインストール（Windows Server 2003 の場合のみ）」（P.9-14）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 Connection ゲートウェイ サーバ用に構成されている場合は、`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 Connection ゲートウェイ サーバ用に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、Cisco Unity は、Connection 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. Connection ゲートウェイ サーバで、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。「Connection ゲートウェイ サーバで証明書署名要求を作成し、ダウンロードするには」（P.9-10）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. Cisco Unity ゲートウェイ サーバで、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。「Cisco Unity ゲートウェイ サーバで証明書署名要求を作成し、ダウンロードするには」（P.9-11）の手順を行います。

   Cisco Unity フェールオーバーが設定されている場合は、このタスクをプライマリ サーバとセカンダリ サーバに対して実行します。

6. Microsoft 証明書サービスを使用してルート証明書のエクスポートおよびサーバ証明書の発行を行う場合は、「ルート証明書のエクスポートとサーバ証明書の発行（Microsoft 証明書サービスの場合のみ）」（P.9-15）の手順を実行します。

   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。

   外部の CA を使用して証明書を発行する場合は、証明書署名要求をその外部 CA に送信します。外部 CA から証明書が返されたら、タスク 7. に進みます。

   Connection にアップロードできるのは、PEM 形式（Base-64 エンコードされた DER）の証明書だけです。証明書のファイル名拡張子は .pem であることが必要です。証明書がこの形式でない場合、通常は、OpenSSL など、無償で使用できるユーティリティを使用して PEM 形式に変換できます。

   このタスクを、Connection サーバ（Connection クラスタが設定されている場合は両方のサーバ）と Cisco Unity サーバ（フェールオーバーが設定されている場合は両方のサーバ）に対して実行します。

7. ルート証明書とサーバ証明書を Connection サーバにアップロードします。「ルート証明書とサーバ証明書を Cisco Unity Connection サーバにアップロードするには」（P.9-4）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。

8. 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.9-6）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。

9. ルート証明書とサーバ証明書を Cisco Unity サーバにアップロードします。「ルート証明書とサーバ証明書を Cisco Unity サーバにアップロードするには」（P.9-13）の手順を行います。

   フェールオーバーが設定されている場合は、このタスクをプライマリ サーバとセカンダリ サーバに対して実行します。

Connection ゲートウェイ サーバで証明書署名要求を作成し、ダウンロードするには

ステップ 1　Cisco Unity Connection サーバで Cisco Unified オペレーティング システムの管理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、[CSRCritical Services 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、[CSR のダウンロード（Download CSR）] 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（Download 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 [保存の種類（Save As Type）] リストで、[すべてのファイル（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 ゲートウェイ サーバで証明書署名要求を作成し、ダウンロードするには

ステップ 1　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）] > [インターネット インフォメーション サービス（IIS）マネージャ（Internet Information Services (IIS) Manager）] を選択します。

ステップ 2　Cisco Unity サーバ名を展開します。

ステップ 3　[Web サイト（Web Sites）] を展開します。

ステップ 4　[既定の Web サイト（Default Web Site）] を右クリックし、[プロパティ（Properties）] を選択します。

ステップ 5　[既定の Web サイト プロパティ（Default Web Site Properties）] ダイアログボックスで、[ディレクトリのセキュリティ（Directory Security）] タブを選択します。

ステップ 6　[セキュアな通信（Secure Communications）] の [サーバ証明書（Server Certificate）] を選択します。

ステップ 7　Web サーバ証明書ウィザード（Web Server Certificate Wizard）で、次の手順を実行します。

a. [次へ（Next）] を選択します。

b. [新しい証明書の作成（Create a New Certificate）] を選択し、[次へ（Next）] を選択します。

c. [要求を今用意し、後で送信する（Prepare the Request Now, But Send It Later）] を選択し、[次へ（Next）] を選択します。

d. 証明書の名前と長さ（ビット）を入力します。

512 ビットの長さを選択することを強く推奨します。ビット長を大きくすると、パフォーマンスが低下する可能性があります。

e. [次へ（Next）] を選択します。

f. 組織の情報を入力し、[次へ（Next）] を選択します。

g. サイトの通常名として、Cisco Unity サーバのシステム名または完全修飾ドメイン名を入力します。

注意　この名前は、Connection サイト ゲートウェイ サーバが Cisco Unity サーバにアクセスするために URL を構築するのに使用する名前と正確に一致する必要があります。この名前は、Connection Administration の [ネットワーク（Networking）] > [リンク（Links）] > [サイト間リンク（Intersite Links）] ページの [ホスト名（Hostname）] フィールドの値です。

h. [次へ（Next）] を選択します。

i. 地理情報を入力し、[次へ（Next）] を選択します。

j. 証明書要求のファイル名と場所を指定します。このファイル名と場所の情報は次の手順で必要となるので、書き留めてください。

k. ファイルは、ディスク、または認証局（CA）のサーバがアクセスできるディレクトリに保存します。

l. [次へ（Next）] を選択します。

m. 要求ファイルの情報を確認し、[次へ（Next）] を選択します。

n. [終了（Finish）] を選択して、Web サーバ証明書ウィザード（Web Server Certificate Wizard）を終了します。

ステップ 8　[OK] をクリックして、[既定の Web サイト プロパティ（Default Web Site Properties）] ダイアログ ボックスを閉じます。

ステップ 9　[インターネット インフォメーション サービス（IIS）マネージャ（Internet Information Services Manager）] ウィンドウを閉じます。

ルート証明書とサーバ証明書を Cisco Unity Connection サーバにアップロードするには

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　ルート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）] を選択して、ルート CA 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、「ルート証明書をエクスポートし、サーバ証明書を発行するには」（P.9-15）の手順でエクスポートしたルート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ルート CA 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 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ルート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、「ルート証明書をエクスポートし、サーバ証明書を発行するには」（P.9-15）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 にログインします。

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。

ルート証明書とサーバ証明書を Cisco Unity サーバにアップロードするには

ステップ 1　Cisco Unity サーバで、コンピュータ アカウントの証明書 MMC をインストールします。

ステップ 2　証明書をアップロードします。詳細については、Microsoft 社のドキュメントを参照してください。

Microsoft 証明書サービスのインストール（Windows Server 2003 の場合のみ）

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。

ルート証明書のエクスポートとサーバ証明書の発行（Microsoft 証明書サービスの場合のみ）

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。

ルート証明書をエクスポートし、サーバ証明書を発行するには

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）] > [証明機関（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.9-14）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　ルート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. [ファイルのコピー（Copy to File）] を選択します。

e. [証明書のエクスポート ウィザードの開始（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 ファイルの形式（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.9-4）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。