CHAPTER 5

# Cisco Unified Presence と Microsoft Exchange 間でのセキュアな証明書交換の設定



## 自己署名証明書およびサードパーティ証明書の交換管理チェックリスト

自己署名証明書およびサードパーティ証明書のセキュアな交換を設定する手順の概要を表 5-1 に示します。

**表 5-1　自己署名証明書およびサードパーティ証明書チェックリスト**

| 設定手順 | | 設定方法 |
|---|---|---|
| ステップ 1 | 証明書 CA サービスをインストールする。 | **自己署名証明書**<br>「認証局（CA）サービスのインストール方法」（P.5-2） |
| ステップ 2 | Exchange サーバの IIS で CSR を作成する。 | **自己署名証明書**<br>「Exchange Server の IIS 上での CSR の作成方法」（P.5-5）<br><br>**サードパーティ証明書**<br>「Exchange Server の IIS 上での CSR の作成方法」（P.5-5） |

表 5-1　自己署名証明書およびサードパーティ証明書チェックリスト（続き）

| 設定手順 | | 設定方法 |
|---|---|---|
| ステップ 3 | CA サーバ/認証局に CSR を提出する。 | **自己署名証明書**<br>「CA サーバ/認証局への CSR の提出」（P.5-9）<br>**サードパーティ証明書**<br>認証局に CSR を要求します。 |
| ステップ 4 | 署名付き証明書をダウンロードする。 | **自己署名証明書**<br>「署名付き証明書のダウンロード」（P.5-10）<br>**サードパーティ証明書**<br>認証局から署名付き証明書が提供されます。 |
| ステップ 5 | 署名付き証明書を Exchange IIS にアップロードする。 | **自己署名証明書**<br>「署名付き証明書の Exchange IIS へのアップロード方法」（P.5-11）<br>**サードパーティ証明書**<br>「署名付き証明書の Exchange IIS へのアップロード方法」（P.5-11） |
| ステップ 6 | ルート証明書をダウンロードする。 | **自己署名証明書**<br>「ルート証明書のダウンロード」（P.5-13）<br>**サードパーティ証明書**<br>認証局にルート証明書を要求します。 |
| ステップ 7 | ルート証明書を Cisco Unified Presence サーバにアップロードします。 | **自己署名証明書**<br>「Cisco Unified Presence サーバへのルート証明書のアップロード」（P.5-13）<br>**サードパーティ証明書**<br>CA 署名付きのサードパーティ Exchange サーバ証明書がある場合は、証明書チェーン内のすべての CA 証明書を Cisco Unified Presence 信頼証明書（cup-trust）として Cisco Unified Presence にアップロードする必要があります。 |

# 認証局（CA）サービスのインストール方法

CA は Exchange サーバ上で動作しますが、サードパーティ証明書の交換におけるセキュリティを高めるために、別の Windows サーバを Certificate Authority（CA; 認証局）として使用することを推奨します。

- 「Windows Server 2003 への CA のインストール」（P.5-3）
- 「Windows Server 2008 への CA のインストール」（P.5-4）

# Windows Server 2003 への CA のインストール

### はじめる前に

- CA をインストールするためには、まず Windows Server 2003 コンピュータに Internet Information Services（IIS; インターネット インフォメーション サービス）をインストールする必要があります。IIS は、Windows 2003 コンピュータにデフォルトでインストールされません。
- Windows Server ディスク 1 および SP1 ディスクを用意してください。

### 手順

**ステップ 1**　[Start] > [Control Panel] > [Add/Remove Programs] の順に選択します。

**ステップ 2**　[Add/Remove Programs] ウィンドウの [Add/Remove Windows Components] を選択します。

**ステップ 3**　[Windows Components Wizard] が表示されます。

| ウィンドウ | 設定手順 |
|---|---|
| [Windows Components] ウィンドウ<br>ページ 1 | **a.** [Components] のリストで [Certificate Services] をオンにします。<br>**b.** ドメイン メンバーシップとコンピュータ名の変更の制約に関する警告が表示されたら、[Yes] を選択します。 |
| [CA Type] ウィンドウ<br>ページ 2 | **a.** [Stand-alone Root CA] を選択します。<br>**b.** [Next] を選択します。 |
| [CA Identifying Information] ウィンドウ<br>ページ 3 | **a.** CA サーバの [Common Name] フィールドにサーバ名を入力します。DNS がない場合は、IP アドレスを入力してください。<br>**b.** [Next] を選択します。 |
| [Certificate Database Settings] ウィンドウ<br>ページ 4 | **a.** デフォルト設定をそのまま使用します。<br>**b.** [Next] を選択します。 |

**ステップ 4**　インターネット インフォメーション サービスを停止するかどうかを確認するメッセージが表示されたら、[Yes] を選択します。

**ステップ 5**　Active Server Pages（ASP）を有効にするかどうかを確認するメッセージが表示されたら、[Yes] を選択します。

**ステップ 6**　インストール プロセスが完了したら、[Finish] を選択します。

### トラブルシューティングのヒント

CA はサードパーティの認証局であることに注意してください。CA の共通名は、CSR の作成に使用される共通名と*同じであってはなりません*。

### 次の作業

「CA サーバ / 認証局への CSR の提出」（P.5-9）

# Windows Server 2008 への CA のインストール

## 手順

**ステップ 1**　[Start] > [Administrative Tools] > [Server Manager] の順に選択します。

**ステップ 2**　コンソール ツリーで [Roles] を選択します。

**ステップ 3**　[Action] > [Add Roles] の順に選択します。

**ステップ 4**　[Add Roles] ウィザードを完了します。

| ウィンドウ | 設定手順 |
|---|---|
| [Before You Begin] ウィンドウ<br>1/13 ページ | **a.** ウィンドウに表示されている前提条件をすべて満たしていることを確認します。<br>**b.** [Next] を選択します。 |
| [Select Server Roles] ウィンドウ<br>2/13 ページ | **a.** [Active Directory Certificate Services] をオンにします。<br>**b.** [Next] を選択します。 |
| [Introduction] ウィンドウ<br>3/13 ページ | [Next] を選択します。 |
| [Select Role Services] ウィンドウ<br>4/13 ページ | **a.** 次のチェックボックスをオンにします。<br>– [Certificate Authority]<br>– [Certificate Authority Web Enrollment]<br>– [Online Responder]<br>**b.** [Next] を選択します。 |
| [Specify Setup Type] ウィンドウ<br>5/13 ページ | [Standalone] を選択します。 |
| [Specify CA Type] ウィンドウ<br>6/13 ページ | [Root CA] を選択します。 |
| [Set Up Private Key] ウィンドウ<br>7/13 ページ | [Create a new private key] を選択します。 |
| [Configure Cryptography for CA] ウィンドウ<br>8/13 ページ | デフォルトの暗号化サービス プロバイダーを選択します。 |
| [Configure CA Name] ウィンドウ<br>9/13 ページ | CA を識別する共通名を入力します。 |
| [Set Validity Period] ウィンドウ<br>10/13 ページ | この CA で作成される証明書の有効期間を設定します。<br>**（注）**　CA が発行する証明書は、ここで指定した期日まで有効です。 |

| ウィンドウ | 設定手順 |
|---|---|
| [Configure Certificate Database] ウィンドウ<br>11/13 ページ | 証明書データベースの場所をデフォルトのままにします。 |
| [Confirm Installation Selections] ウィンドウ<br>12/13 ページ | [Install] を選択します。 |
| [Installation Results] ウィンドウ<br>13/13 ページ | **a.** すべてのコンポーネントについて、[Installation Succeeded] というメッセージが表示されていることを確認します。<br>**b.** [Close] を選択します。<br>**（注）** サーバー マネージャに役割の 1 つとして [Active Directory Certificate Services] が表示されます。 |

**次の作業**

「Exchange Server の IIS 上での CSR の作成方法」（P.5-5）

# Exchange Server の IIS 上での CSR の作成方法



## CSR の作成：Windows Server 2003 の実行

Exchange の IIS で Certificate Signing Request（CSR; 証明書の署名要求）を作成する必要があります。作成した CSR は CA サーバによって署名されます。

**はじめる前に**

自己署名証明書：必要に応じて証明書 CA サービスをインストールします。

**手順**

**ステップ 1**　[Administrative Tools] から [Internet Information Services] を開きます。

**ステップ 2**　Internet Information Services（IIS; インターネット インフォメーション サービス）マネージャで次の操作を実行します。

**a.** [Default Web Site] を右クリックします。

**b.** [Properties] を選択します。

**ステップ 3**　[Directory Security] タブを選択します。

**ステップ 4**　[Server Certificate] を選択します。

**ステップ 5**　[Web Server Certificate Wizard] ウィンドウが表示されたら、[Next] を選択します。

**ステップ 6**　Web Server Certificate Wizard を完了します。

**（注）**　証明書の [Subject Alternative Name (SAN)] フィールドに値が入力されている場合、その値は証明書の Common Name（CN; 共通名）と一致している必要があります。

| ウィンドウ | 設定手順 |
|---|---|
| [Server Certificate] ウィンドウ<br>1/9 ページ | **a.** [Create a New Certificate] を選択します。<br>**b.** [Next] を選択します。 |
| [Delayed or Immediate Request] ウィンドウ<br>2/9 ページ | **a.** [Prepare the Request Now, But Send It Later] を選択します。<br>**b.** [Next] を選択します。 |
| [Name and Security Settings] ウィンドウ<br>3/9 ページ | **a.** Web サイトの証明書のデフォルト名をそのまま使用します。<br>**b.** ビット長として [1024] を選択します。<br>**c.** [Next] を選択します。 |
| [Organization Information] ウィンドウ<br>4/9 ページ | **a.** [Organization] フィールドに会社名を入力します。<br>**b.** [Organization Unit] フィールドに部署名を入力します。<br>**c.** [Next] を選択します。 |
| [Your Site's Common Name] ウィンドウ<br>5/9 ページ | **a.** [Common Name] フィールドには、Exchange サーバのホスト名または IP アドレスを入力します。<br>**（注）** ここで入力する IIS 証明書の一般名は、Cisco Unified Presence でプレゼンス ゲートウェイを設定するときに使用されるため、接続先のホスト（URI または IP アドレス）と一致している必要があります。<br>**b.** [Next] を選択します。 |
| [Geographical Information] ウィンドウ<br>6/9 ページ | **a.** 次の地理情報を入力します。<br>– [Country/Region]（国 / 地域）<br>– [State/province]（都道府県）<br>– [City/locality]（市区町村）<br>**b.** [Next] を選択します。 |
| [Certificate Request File Name] ウィンドウ<br>7/9 ページ | **a.** 証明書要求のファイル名を入力し、CSR の保存先のパスとファイル名を指定します。<br>**b.** [Next] を選択します。<br>**（注）** CSR は拡張子（.txt）なしで保存してください。この CSR ファイルを後で探す必要があるため、保存場所を覚えておいてください。このファイルを開くには、必ずメモ帳を使用します。 |

| ウィンドウ | 設定手順 |
|---|---|
| [Request File Summary] ウィンドウ<br>8/9 ページ | **a.** [Request File Summary] ウィンドウに表示されている情報に誤りがないことを確認します。<br>**b.** [Next] を選択します。 |
| [Server Certificate Completion] ウィンドウ<br>9/9 ページ | [Finish] を選択します。 |

### 次の作業

「CA サーバ / 認証局への CSR の提出」（P.5-9）

# CSR の作成：Windows Server 2008 の実行

Exchange の IIS で Certificate Signing Request（CSR; 証明書の署名要求）を作成する必要があります。作成した CSR は CA サーバによって署名されます。

### はじめる前に

### 手順

**ステップ 1**　[Administrative Tools] から [Internet Information Services (IIS) Manager] を開きます。

**ステップ 2**　IIS マネージャの左側のフレームにある [Connections] ウィンドウで [Exchange Server] を選択します。

**ステップ 3**　[Server Certificates] をダブルクリックします。

**ステップ 4**　IIS マネージャの右側のフレームにある [Actions] ウィンドウで [Create Certificate Request] を選択します。

**ステップ 5**　証明書の要求ウィザードを完了します。

| ウィンドウ | 設定手順 |
|---|---|
| [Distinguished Name Properties] ウィンドウ<br>1/5 ページ | **a.** [Common Name] フィールドには、Exchange サーバのホスト名または IP アドレスを入力します。<br>**（注）** ここで入力する IIS 証明書の一般名は、Cisco Unified Presence でプレゼンス ゲートウェイを設定するときに使用されるため、接続先のホスト（URI または IP アドレス）と一致している必要があります。<br>**b.** [Organization] フィールドに会社名を入力します。<br>**c.** [Organization Unit] フィールドに部署名を入力します。<br>**d.** 次の地理情報を入力します。<br>– [City/locality]（市区町村）<br>– [State/province]（都道府県）<br>– [Country/Region]（国 / 地域）<br>**e.** [Next] を選択します。 |
| [Cryptographic Service Provider Properties] ウィンドウ<br>2/5 ページ | **a.** デフォルトの暗号化サービス プロバイダーをそのまま使用します。<br>**b.** ビット長として [1024] を選択します。<br>**c.** [Next] を選択します。 |
| [Certificate Request File Name] ウィンドウ<br>3/5 ページ | **a.** 証明書要求のファイル名を入力します。<br>**b.** [Next] を選択します。<br>**（注）** CSR は拡張子（.txt）なしで保存してください。この CSR ファイルを後で探す必要があるため、保存場所を覚えておいてください。このファイルを開くには、必ずメモ帳を使用します。 |
| [Request File Summary] ウィンドウ<br>4/5 ページ | **a.** [Request File Summary] ウィンドウに表示されている情報に誤りがないことを確認します。<br>**b.** [Next] を選択します。 |
| [Request Certificate Completion] ウィンドウ<br>5/5 ページ | [Finish] を選択します。 |

## 次の作業

「CA サーバ / 認証局への CSR の提出」（P.5-9）

# CA サーバ/認証局への CSR の提出

IIS で Exchange 用に作成されるデフォルトの SSL 証明書には、Exchange サーバの Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）を使用し、Cisco Unified Presence が信頼している認証局の署名を付けることを推奨します。この手順により、CA が Exchange IIS からの CSR 署名できます。次の手順を CA サーバで実行し、次の場所にある Exchange サーバの FQDN を設定してください。

- Exchange 証明書
- Cisco Unified Presence の管理画面にある、Exchange プレゼンス ゲートウェイの [プレゼンス ゲートウェイ（Presence Gateway）] フィールド

### はじめる前に

Exchange サーバの IIS で CSR を作成します。

### 手順

**ステップ 1**　証明書要求ファイルを CA サーバにコピーします。

**ステップ 2**　次の URL を開きます。

http://*local-server*/certserv

または、

http://127.0.0.1/certsrv

**ステップ 3**　[Request a certificate] を選択します。

**ステップ 4**　[advanced certificate request] を選択します。

**ステップ 5**　[Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file] を選択します。

**ステップ 6**　メモ帳などのテキスト エディタを使用して、作成した CSR を開きます。

**ステップ 7**　次の行から、

**-----BEGIN CERTIFICATE REQUEST**

次の行までの情報をすべてコピーします。

**END CERTIFICATE REQUEST-----**

**ステップ 8**　CSR の内容を [Certificate Request] テキストボックスに貼り付けます。

**ステップ 9**　（任意）[Certificate Template] ドロップダウン リストのデフォルト値は [Administrator] テンプレートです。このテンプレートでは、サーバの認証に適した有効な署名付き証明書が作成されることもあれば、作成されないこともあります。エンタープライズのルート CA がある場合は、[Certificate Template] ドロップダウン リストから [Web Server] 証明書テンプレートを選択してください。[Web Server] 証明書テンプレートは表示されないことがあるため、CA 設定を既に変更している場合、この手順は不要となることがあります。

**ステップ 10**　[Submit] を選択します。

**ステップ 11**　[Start] > [Administrative Tools] > [Certification] > [Authority] > [CA name] > [Pending request] の順に選択します。[Certificate Authority] ウィンドウの [Pending Requests] の下に、送信したばかりの要求が表示されます。

**ステップ 12**　要求を右クリックし、次の操作を実行します。

- [All Tasks] を選択します。
- [Issue] を選択します。

**ステップ 13**　[Issued certificates] を選択し、証明書が発行されていることを確認します。

**次の作業**

「署名付き証明書のダウンロード」（P.5-10）

# 署名付き証明書のダウンロード

**はじめる前に**

自己署名証明書：CA サーバに CSR を提出します。

サードパーティ証明書：認証局に CSR を要求します。

**手順**

**ステップ 1**　[Administrative Tools] から [Certification Authority] を開きます。先ほど発行した証明書の要求が [Issued Requests] に表示されます。

**ステップ 2**　その要求を右クリックし、[Open] を選択します。

**ステップ 3**　[Details] タブを選択します。

**ステップ 4**　[Copy to File] を選択します。

**ステップ 5**　[Certificate Export Wizard] が表示されたら、[Next] を選択します。

**ステップ 6**　証明書のエクスポート ウィザードを完了します。

| ウィンドウ | 設定手順 |
|---|---|
| [Export File Format] ウィンドウ<br>1/3 ページ | **a.** [Base-64 encoded X.509] を選択します。<br>**b.** [Next] を選択します。 |
| [File to Export] ウィンドウ<br>2/3 ページ | **a.** 証明書の保存場所を入力します。証明書の名前には **cert.cer** を使用します（*c:¥cert.cer* など）。<br>**b.** [Next] を選択します。 |
| [Certificate Export Wizard Completion] ウィンドウ<br>3/3 ページ | **a.** 表示されている概要情報に目を通し、エクスポートが成功したことを確認します。<br>**b.** [Finish] を選択します。 |

**ステップ 7**　Cisco Unified Presence の管理に使用するコンピュータに、cert.cer をコピーするか、FTP で送信します。

**次の作業**

「署名付き証明書の Exchange IIS へのアップロード方法」（P.5-11）

# 署名付き証明書の Exchange IIS へのアップロード方法



## 署名付き証明書のアップロード：Windows 2003 の実行

ここでは、署名付き CSR を IIS にアップロードする手順を説明します。署名付き証明書をアップロードするには、Cisco Unified Presence の管理に使用するコンピュータで次の手順を実行します。

### はじめる前に

自己署名証明書：署名付き証明書をダウンロードします。

サードパーティ証明書：認証局から署名付き証明書が提供されます。

### 手順

**ステップ 1**　[Administrative Tools] から [Internet Information Services] を開きます。

**ステップ 2**　[Internet Information Services] ウィンドウで次の手順を実行します。

**a.** [Default Web Site] を右クリックします。

**b.** [Properties] を選択します。

**ステップ 3**　[Default Web Site] ウィンドウで次の手順を実行します。

**a.** [Directory Security] タブを選択します。

**b.** [Server Certificate] を選択します。

**ステップ 4**　[Web Server Certificate Wizard] ウィンドウが表示されたら、[Next] を選択します。

**ステップ 5**　Web Server Certificate Wizard を完了します。

| ウィンドウ | 設定手順 |
|---|---|
| [Pending Certificate Request] ウィンドウ<br>1/4 ページ | **a.** [Process the pending request and install the certificate] を選択します。<br>**b.** [Next] を選択します。 |
| [Process a Pending Request] ウィンドウ<br>2/4 ページ | **a.** [Browse] を選択して証明書を指定します。<br>**b.** 正しいパスおよびファイル名に移動します。<br>**c.** [Next] を選択します。 |
| [SSL Port] ウィンドウ<br>3/4 ページ | **a.** SSL ポートを「443」と入力します。<br>**b.** [Next] を選択します。 |
| [Server Certificate Completion] ウィンドウ<br>4/4 ページ | [Finish] を選択します。 |

### トラブルシューティングのヒント

証明書が信頼できる証明書ストアにない場合、署名付き CSR は信頼できません。信頼を確立するには、次の操作を実行します。

- [Directory Security] タブで [View Certificate] を選択します。
- [Details] > [Highlight root certificate] の順に選択し、[View] を選択します。
- ルート証明書の [Details] タブを選択し、証明書をインストールします。

### 次の作業

「ルート証明書のダウンロード」（P.5-13）

## 署名付き証明書のアップロード：Windows 2008 の実行

ここでは、署名付き CSR を IIS にアップロードする手順を説明します。署名付き証明書をアップロードするには、Cisco Unified Presence の管理に使用するコンピュータで次の手順を実行します。

### はじめる前に

自己署名証明書：署名付き証明書をダウンロードします。

サードパーティ証明書：認証局から署名付き証明書が提供されます。

### 手順

**ステップ 1**　[Administrative Tools] から [Internet Information Services (IIS) Manager] を開きます。

**ステップ 2**　IIS マネージャの左側のフレームにある [Connections] ウィンドウで [Exchange Server] を選択します。

**ステップ 3**　[Server Certificates] をダブルクリックします。

**ステップ 4**　IIS マネージャの右側のフレームにある [Actions] ウィンドウで [Complete Certificate Request] を選択します。

**ステップ 5**　[Specify Certificate Authority Response] ウィンドウで次の操作を実行します。

**a.** 省略記号 [...] を選択して証明書を指定します。

**b.** 正しいパスおよびファイル名に移動します。

**c.** 証明書のわかりやすい名前を入力します。

**d.** [OK] を選択します。要求が完了した証明書が証明書のリストに表示されます。

**ステップ 6**　[Internet Information Services] ウィンドウで次の手順を実行し、証明書をバインドします。

**a.** [Default Web Site] を選択します。

**b.** IIS マネージャの右側のフレームにある [Actions] ウィンドウで [Bindings] を選択します。

**ステップ 7**　[Site Bindings] ウィンドウで次の手順を実行します。

**a.** [https] を選択します。

**b.** [Edit] をクリックします。

**ステップ 8**　[Edit Site Binding] ウィンドウで次の手順を実行します。

**a.** SSL 証明書のリスト ボックスから、作成した証明書を選択します。証明書に付けた「わかりやすい名前」が表示されます。

**b.** [OK] を選択します。

### 次の作業

「ルート証明書のダウンロード」（P.5-13）

# ルート証明書のダウンロード

### はじめる前に

署名付き証明書を Exchange IIS にアップロードします。

### 手順

**ステップ 1**　CA サーバにサイン インし、Web ブラウザを開きます。

**ステップ 2**　使用している Windows プラットフォームの種類に応じ、次のいずれかの URL にアクセスします。

- Windows server 2003：http://127.0.0.1/certsrv
- Windows server 2008：https://127.0.0.1/certsrv

**ステップ 3**　[Download a CA certificate, certificate chain, or CRL] を選択します。

**ステップ 4**　[Encoding Method] で、[Base 64] を選択します。

**ステップ 5**　[Download CA Certificate] を選択します。

**ステップ 6**　証明書（**certnew.cer**）をローカル ディスクに保存します。

### トラブルシューティングのヒント

ルート証明書の件名 Common Name（CN; 共通名）がわからない場合は、外部の証明書管理ツールを使用して調べることができます。Windows オペレーティング システムで、拡張子が .CER の証明書ファイルを右クリックし、証明書のプロパティを開きます。

### 次の作業

「Cisco Unified Presence サーバへのルート証明書のアップロード」（P.5-13）

# Cisco Unified Presence サーバへのルート証明書のアップロード

### はじめる前に

- 自己署名証明書：ルート証明書をダウンロードします。
- サードパーティ証明書：認証局にルート証明書を要求します。CA 署名付きのサードパーティ Exchange サーバ証明書がある場合は、証明書チェーン内のすべての CA 証明書を Cisco Unified Presence の信頼証明書（cup-trust）として Cisco Unified Presence にアップロードする必要があります。

### 手順

**ステップ 1**　Cisco Unified Presence の管理画面にある証明書インポート ツールを使用して、証明書をアップロードします。

| 証明書のアップロード方法 | 動作 |
|---|---|
| Cisco Unified Presence の管理画面にある証明書インポート ツール<br><br>証明書インポート ツールは、信頼証明書を Cisco Unified Presence にインストールするプロセスを簡略化するもので、証明書交換の主要な方法です。このツールでは、Exchange サーバのホストとポートを指定すると、サーバから証明書チェーンがダウンロードされます。承認すると、欠落している証明書が自動的にインストールされます。<br><br>**（注）**　この手順では、Cisco Unified Presence の管理画面の証明書インポート ツールにアクセスし、インストールする方法を説明します。いずれかの形式での予定表統合のために Exchange プレゼンス ゲートウェイを設定した場合（[プレゼンス（Presence）] > [ゲートウェイ（Gateways）] の順に選択）、カスタマイズされた証明書インポート ツールを表示することもできます。 | **a.** Cisco Unified Presence の管理画面で、[システム（System）] > [セキュリティ（Security）] > [証明書インポート ツール（Certificate Import Tool）] の順に選択します。<br><br>**b.** 証明書をインストールする証明書信頼ストアとして [CUP の信頼性（CUP Trust）] を選択します。この証明書信頼ストアには、Exchange の統合に必要なプレゼンス エンジン信頼証明書が保存されます。<br><br>**c.** Exchange サーバに接続するために、次のいずれかの値を入力します。<br>– IP アドレス<br>– ホスト名<br>– FQDN<br><br>この [ピア サーバ（Peer Server）] フィールドに入力する値は、Exchange サーバの IP アドレス、ホスト名、または FQDN と完全に一致している必要があります。<br><br>**d.** Exchange サーバとの通信に使用するポートを入力します。この値は、Exchange サーバの使用可能なポートと一致している必要があります。<br><br>**e.** [送信（Submit）] を選択します。ツールが完了すると、テストごとに次の状態が報告されます。<br>– ピア サーバの到達可能性ステータス：Cisco Unified Presence が Exchange サーバに到達（ping）できるかどうかを示します。「Exchange サーバ接続ステータスのトラブルシューティング」（P.6-1）を参照してください。<br>– SSL 接続 / 証明書の確認ステータス：証明書のインポート ツールが指定されたピア サーバから証明書をダウンロードすることに成功したかどうかと、Cisco Unified Presence とリモート サーバの間にセキュアな接続が確立されたかどうかを示します。「SSL 接続 / 証明書ステータスのトラブルシューティング」（P.6-2）を参照してください。 |

**ステップ 2**　証明書のインポート ツールによって、証明書が欠落していることがわかった場合は（通常、Microsoft サーバでは CA 証明書が欠落します）、Cisco Unified OS の管理画面の [ 証明書の管理（Certificate Management）] ウィンドウを使用して、手動で CA 証明書をアップロードしてください。

| 証明書のアップロード方法 | 動作 |
|---|---|
| Cisco Unified オペレーティング システムの管理画面<br><br>Exchange サーバが SSL/TLS ハンドシェイク中に証明書を送信しない場合、それらの証明書は証明書のインポート ツールではインポートできません。その場合は、Cisco Unified オペレーティング システムの管理画面にある証明書の管理ツール（[ セキュリティ（Security）] > [ 証明書の管理（Certificate Management）] の順に選択）を使用して、欠落している証明書を手動でインポートする必要があります。 | **a.** Cisco Unified Presence サーバの管理に使用するコンピュータに、certnew.cer 証明書ファイルをコピーするか、FTP で送信します。<br>**b.** Cisco Unified Presence の管理画面のログイン ウィンドウで、[ ナビゲーション（Navigation）] メニューから [Cisco Unified OS の管理（Cisco Unified OS Administration）] を選択し、[ 移動（Go）] を選択します。<br>**c.** Cisco Unified オペレーティング システムの管理画面用のユーザ名とパスワードを入力して、[ ログイン（Login）] を選択します。<br>**d.** [ セキュリティ（Security）] > [ 証明書の管理（Certificate Management）] を選択します。<br>**e.** [ 証明書の一覧（Certificate List）] ウィンドウで [ 証明書のアップロード（Upload Certificate）] を選択します。<br>**f.** [ 証明書のアップロード（Upload Certificate）] ポップアップ ウィンドウが表示されたら、次の操作を実行します。<br>– [ 証明書の名前（Certificate Name）] リスト ボックスから [cup-trust] を選択します。<br>– 拡張子を付けずにルート証明書の名前を入力します。<br>**g.** [ 参照（Browse）] を選択し、[certnew.cer] を選択します。<br>**h.** [ ファイルのアップロード（Upload File）] を選択します。 |

**ステップ 3**　証明書のインポート ツール（ステップ 1）に戻り、すべてのステータス テストが成功したことを確認します。

**ステップ 4**　すべての Exchange 信頼証明書をアップロードしたら、Cisco UP プレゼンス エンジンと SIP プロキシ サービスを再起動します。[Cisco Unified サービスアビリティ（Cisco Unified Serviceability）] > [Tools] > [Service Activation] の順に選択します。

### トラブルシューティングのヒント

- Cisco Unified Presence では、Exchange サーバの信頼証明書を件名 Common Name（CN; 共通名）あり / なしのどちらでもアップロードできます。
- 会議通知機能および Cisco IP Phone Messenger 機能は、ネットワークを WebDAV 経由で統合した場合にのみ有効です。これらの機能は EWS 統合ではサポートされません。
- 会議通知機能を使用する場合は、すべての種類の証明書についてプレゼンス エンジンと SIP プロキシを再起動する必要があります。証明書をアップロードしたら、[Cisco Unified サービスアビリティ（Cisco Unified Serviceability）] へ移動し、まずプレゼンス エンジン、次に SIP プロキシを再起動します。これによって予定表の接続が影響を受ける可能性があることに注意してください。