IM and Presence と Microsoft Exchange 間のセキュアな証明書交換

自己署名証明書およびサードパーティ証明書の交換の管理

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次の表に示します。

表 *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：	[Cisco Unity Connection の管理（Cisco Unity Connection Administration）] から [システム設定（System Settings）]>[エンタープライズ パラメータ（Enterprise Parameters）] を選択し、トレース可能な最大デバイス数を設定する。[デバイス レベル トレースの最大数（Max Number of Device Level Trace）] フィールドに値を入力します。デフォルトは 12 です。	『Cisco Unity Connection System Administration Guide』
ステップ 2：	証明書 CA サービスをインストールする。	**自己署名証明書** 認証局（CA）サービスのインストール, （3 ページ）
ステップ 3：	Exchange サーバの IIS で CSR を作成する。	**自己署名証明書** Exchange サーバの IIS での CSR の生成, （7 ページ） **サードパーティ証明書** Exchange サーバの IIS での CSR の生成, （7 ページ）
ステップ 4：	CA サーバ/認証局に CSR を提出する。	**自己署名証明書** CA サーバ/認証局への CSR の提出, （9 ページ） **サードパーティ証明書** 認証局に CSR を要求します。
ステップ 5：	署名済みの証明書をダウンロードする。	**自己署名証明書** 署名付き証明書のダウンロード, （11 ページ） **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。

設定手順		設定方法
ステップ 6：	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** 署名付き証明書の Exchange IIS へのアップロード，（12 ページ） **サードパーティ証明書** 署名付き証明書の Exchange IIS へのアップロード，（12 ページ）
ステップ 7	ルート証明書をダウンロードする。	**自己署名証明書** ルート証明書のダウンロード，（14ページ） **サードパーティ証明書** 認証局にルート証明書を要求する。
ステップ 8：	ルート証明書を IM and Presence サーバにアップロードする。	**自己署名証明書** ルート証明書の IM and Presence サーバへのアップロード，（15 ページ） **サードパーティ証明書** サードパーティの CA 署名付きの 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 IM and Presence の信頼証明書（cup-trust）として IM and 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

CA は Exchange サーバ上で実行することもできますが、サードパーティの証明書交換のセキュリティを強化するために、別の Windows サーバを認証局（別名 CA）として使用することをお勧めします。

- Windows Server 2003 への CA のインストール，（4 ページ）
- Windows Server 2008 への CA のインストール，（5 ページ）

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には、まず Windows Server 2003 コンピュータにインターネット インフォメーション サービス（IIS）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 ディスクがあることを確認します。

手順

ステップ 1 [スタート（Start）] > [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）] の順に選択します。

ステップ 2 [プログラムの追加と削除（Add or Remove Programs）] ウィンドウで [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 3 [Windows コンポーネント（Windows Components）] ウィザードの 1 ページ目の [Components（コンポーネント）] で [証明書サービス（Certificate Services）] を選択し、ドメインのメンバーシップとコンピュータの名前変更の制約に関する警告が表示されたら [はい（Yes）] を選択します。

ステップ 4 [Windows コンポーネント（Windows Components）] ウィザードの 2 ページ目で [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。

ステップ 5 [Windows コンポーネント（Windows Components）] ウィザードの 3 ページ目で、CA サーバの [共通名（Common Name）] フィールドにサーバの名前を入力します。 DNS がない場合は、IP アドレスを入力してください。 [次へ（Next）] を選択します。

ステップ 6 [Windows コンポーネント（Windows Components）] ウィザードの 4 ページ目でデフォルトの設定を受け入れ、[次へ（Next）] を選択します。

ステップ 7 Internet Information Services を停止するよう指示されたら [はい（Yes）] を選択します。

ステップ 8 Active Server Pages（ASP）を有効にするよう指示されたら [はい（Yes）] を選択します。

ステップ 9 インストール手順が完了したら [終了（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権限であることを覚えておいてください。 CA の共通名と、CSR の生成に使用された共通名を同じにすることはできません。

次の作業

CSR の生成（Windows Server 2008）, （8 ページ）

Windows Server 2008 への CA のインストール

手順

ステップ 1 [スタート（Start）]>[管理ツール（Administrative Tools）]>[サーバマネージャー（Server Manager）] を選択します。

ステップ 2 コンソール ツリーで [役割（Roles）] を選択します。

ステップ 3 [操作（Action）] > [役割の追加（Add Roles）] を選択します。

ステップ 4 [役割の追加（Add Roles）] ウィザードを完了します。

ウィンドウ	設定手順
[開始する前に（Before You Begin）] ウィンドウ 1/13 ページ	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、[次へ（Next）] を選択します。
[サーバの役割の選択（Select Server Roles）] ウィンドウ 2/13 ページ	[Active Directory 証明書サービス（Active Directory Certificate Services）] にチェックを入れ、[次へ（Next）] を選択します。
[開始（Introduction）] ウィンドウ 3/13 ページ	[次へ（Next）] を選択します。
[役割サービスの選択（Select Role Services）] ウィンドウ 4/13 ページ	次のボックスを選択し、[次へ（Next）] を選択します。 • Certificate Authority • Certificate Authority Web Enrollment • Online Responder
[セットアップ タイプの指定（Specify Setup Type）] ウィンドウ 5/13 ページ	[スタンドアロン（Standalone）] を選択します。
[CA タイプの指定（Specify CA Type）] ウィンドウ 6/13 ページ	[ルート CA（Root CA）] を選択します。

ウィンドウ	設定手順
[秘密キーの設定（Set Up Private Key）] ウィンドウ 7/13 ページ	[新しい秘密キーを作成する（Create a new private key）] を選択します。
[CA の暗号化を設定（Configure Cryptography for CA）] ウィンドウ 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。
[CA 名の設定（Configure CA Name）] ウィンドウ 9/13 ページ	CA を識別する共通名を入力します。
[有効期限の設定（Set Validity Period）] ウィンドウ 10/13 ページ	CA に対して生成された証明書の有効期間を設定します。 （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。
[証明書データベースを構成（Configure Certificate Database）] ウィンドウ 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。
[インストール内容の確認（Confirm Installation Selections）] ウィンドウ 12/13 ページ	[インストール（Install）] を選択します。
[インストールの結果（Installation Results）] ウィンドウ 13/13 ページ	すべてのコンポーネントについて、[インストールが正常に完了しました（Installation Succeeded）] というメッセージが表示されていることを確認し、[閉じる（Close）] を選択します。 （注） サーバ マネージャに役割の 1 つとして [Active Directory 証明書サービス（Active Directory Certificate Services）] が表示されます。

次の作業

Exchange サーバの IIS での CSR の生成, （7 ページ）

Exchange サーバの IIS での CSR の生成

CSR の生成（Windows Server 2003）

Exchange の IIS で証明書の署名要求（CSR）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。 証明書の [サブジェクトの別名（Subject Alternative Name (SAN)）] フィールドに値が入力されている場合、その値は証明書の共通名（CN）と一致している必要があります。

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 [管理ツール（Administrative Tools）] から [インターネット インフォメーション サービス（Internet Information Services）] を開きます。

ステップ 2 [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 3 [ディレクトリ セキュリティ（Directory Security）] タブを選択します。

ステップ 4 [サーバ証明書（Server Certificate）] を選択し、[次へ（Next）] を選択します。

ステップ 5 [新しい証明書の作成（Create a new certificate）] を [サーバ証明書（Server Certificate）] ウィンドウから選択し、[次へ（Next）] を選択します。

ステップ 6 [証明書の要求の送信方法（Delayed or Immediate Request）] ウィンドウで [証明書の要求を作成して後で送信する（Prepare the request now, but send it later）] を選択し、[次へ（Next）] を選択します。

ステップ 7 デフォルトの Web サイト証明書名を受け入れ、[名前およびセキュリティの設定（Name and Security Settings）] でビット長として [2048] を選択し、[次へ（Next）] を選択します。

ステップ 8 [組織情報（Organization Information）] ウィンドウの [組織（Organization）] フィールドに会社名、[組織単位（Organizational Unit）] フィールドに部署名をそれぞれ入力し、[次へ（Next）] を選択します。

ステップ 9 Exchange サーバのホスト名と IP アドレスを [サイトの一般名（Your Site's Common Name）] ウィンドウの [共通名（Common Name）] フィールドに入力し、[次へ（Next）] を選択します。

（注） ここで入力する IIS 証明書の一般名は、IM and 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。

ステップ 10 [地理情報（Geographical Information）] ウィンドウに地理情報を入力し、[次へ（Next）] を選択します。

ステップ 11 [証明書要求ファイル名（Certificate Request File Name）] ウィンドウに、証明書要求の適切なファイル名を入力し、CSR を保存するパスとファイル名を指定して [次へ（Next）] を選択します。

（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。

ステップ 12 [要求ファイルの概要（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、[次へ（Next）] を選択します。

ステップ 13 [完了（Finish）] を選択します。

次の作業

CA サーバ/認証局への CSR の提出, （9 ページ）

CSR の生成（Windows Server 2008）

Exchange の IIS で証明書の署名要求（CSR）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。

手順

ステップ 1 [管理ツール（Administrative Tools）] から [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 [接続（Connections）] ウィンドウで [Exchange Server] を選択します。

ステップ 3 [サーバ証明書（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 [操作（Actions）] ウィンドウで [証明書の要求の作成（Create Certificate Request）] を選択します。

ステップ 5 [識別名プロパティ（Distinguished Name Properties）] ウィンドウに関連情報を入力し、[次へ（Next）] を選択します。

a) [共通名（Common Name）] フィールドに Exchange Server ホスト名または IP アドレスを入力します。

（注） ここで入力する IIS 証明書の一般名は、IM and 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。

b) [組織（Organization）] フィールドに会社名を入力します。

c) [組織単位（Organizational Unit）] フィールドに部署名を入力します。

d) 地理情報を入力します。

ステップ 6 デフォルトの暗号化サービスプロバイダーを受け入れ、[暗号化サービスプロバイダのプロパティ（Cryptographic Service Provider Properties）] ウィンドウでビット長を [2048] に設定し、[次へ（Next）] を選択します。

ステップ 7 [証明書要求ファイル名（Certificate Request File Name）] ウィンドウで証明書要求の適切なファイル名を入力し、[次へ（Next）] を選択します。

（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。

ステップ 8 [要求ファイルの概要（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、[次へ（Next）] を選択します。

ステップ 9 [完了（Finish）] を選択します。

次の作業

CA サーバ/認証局への CSR の提出, （9 ページ）

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 サーバの完全修飾ドメイン名（FQDN）を使用し、IM and 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 に署名できます。 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 CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] の 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 次のいずれかの URL にアクセスします。

- Windows 2003 または Windows 2008：http://local-server/certserv

または

- Windows 2003：http://127.0.0.1/certserv

- Windows 2008：http://127.0.0.1/certsrv

ステップ 3 [証明書の要求（Request a certificate）] を選択します。

ステップ 4 [詳細証明書要求（advanced certificate request）] を選択します。

ステップ 5 [ベース 64 エンコード CMC または PKCS #10 ファイルを使用して証明書要求を送信するか、ベース 64 エンコード PKCS #7 ファイルを使用して更新要求を送信する（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 [証明書要求（Certificate Request）] テキストボックスに貼り付けます。

ステップ 9 （任意）[証明書テンプレート（Certificate Template）] ドロップダウン リストのデフォルト値は [管理者（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、[証明書テンプレート（Certificate Template）] ドロップダウン リストから [Web サーバ（Web Server）] 証明書テンプレートを選択してください。 [Web サーバ（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 設定をすで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 [送信（Submit）] を選択します。

ステップ 11 [管理ツール（Administrative Tools）] で [スタート（Start）] > [管理ツール（Administrative Tools）] > [証明（Certification）] > [機関（Authority）] > [CA 名（CA name）] > [保留中の要求（Pending Request）] を選択し、認証局を開きます。 [認証局（Certificate Authority）] ウィンドウの [保留中の要求（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。

- [すべてのタスク（All Tasks）] を選択します。
- [発行（Issue）] を選択します。

ステップ 13 [発行済み証明書（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, （11 ページ）

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 [管理ツール（Administrative Tools）] から [認証局（Certification Authority）] を開きます。 先ほど発行した証明書の要求が [発行済み要求（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、[開く（Open）] を選択します。

ステップ 3 [詳細（Details）] タブを選択します。

ステップ 4 [ファイルのコピー（Copy to File）] を選択します。

ステップ 5 [証明書のエクスポート ウィザード（Certificate Export Wizard）] が表示されたら、[次へ（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
[エクスポート ファイル形式（Export File Format）] ウィンドウ 1/3 ページ	[Base-64 encoded X.509] を選択し、[次へ（Next）] を選択します。
[エクスポートするファイル（File to Export）] ウィンドウ 2/3 ページ	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）。 [次へ（Next）] を選択します。
[証明書エクスポート ウィザードの完了（Certificate Export Wizard Completion）] ウィンドウ 3/3 ページ	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て [完了（Finish）] を選択します。

ステップ 7 IM and 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, （12 ページ）

署名付き証明書の Exchange IIS へのアップロード

署名付き証明書のアップロード（Windows 2003）

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、IM and 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 [管理ツール（Administrative Tools）] から [インターネット インフォメーション サービス（Internet Information Services）] を開きます。

ステップ 2 [インターネット インフォメーション サービス（Internet Information Services）] ウィンドウで次の手順を実行します。

a) [既定の Web サイト（Default Web Site）] を右クリックします。

b) [プロパティ（Properties）] を選択します。

ステップ 3 [既定の Web サイト（Default Web Site）] ウィンドウで次の手順を実行します。

a) [ディレクトリ セキュリティ（Directory Security）] タブを選択します。

b) [サーバ証明書（Server Certificate）] を選択します。

ステップ 4 [Web サーバ証明書ウィザード（Web Server Certificate Wizard）] ウィンドウが表示されたら、[次へ（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
[保留中の証明書要求（Pending Certificate Request）] ウィンドウ 1/4 ページ	[保留中の要求を処理し、証明書をインストールする（Process the Pending Request and Install the Certificate）] を選択し、[次へ（Next）] を選択します。

ウィンドウ	設定手順
[保留中の要求の処理（Process a Pending Request）] ウィンドウ 2/4 ページ	[参照（Browse）] を選択して証明書を探し、正しいパスとファイル名を選択して [次へ（Next）] を選択します。
[SSL ポート（SSL Port）] ウィンドウ 3/4 ページ	SSL ポートには **443** と入力し、[次へ（Next）] を選択します。
[サーバ証明書の完了（Server Certificate Completion）] ウィンドウ 4/4 ページ	[完了（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。

- [ディレクトリ セキュリティ（Directory Security）] タブで [証明書の表示（View Certificate）] を選択します。
- [詳細（Details）] > [ルート証明書の強調表示（Highlight root certificate）] を選択し、[表示（View）] を選択します。
- ルート証明書の [詳細（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, （14 ページ）

署名付き証明書のアップロード（Windows 2008）

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、IM and 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 [管理ツール（Administrative Tools）] から [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 [接続（Connections）] ウィンドウで [Exchange Server] を選択します。

ステップ 3 [サーバ証明書（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 [操作（Actions）] ウィンドウで [証明書要求の完了（Complete Certificate Request）] を選択します。

ステップ 5 [認証局の応答の指定（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 [インターネット インフォメーション サービス（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) [既定の Web サイト（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 [操作（Actions）] ウィンドウで [バインディング（Bindings）] を選択します。

ステップ 7 [サイト バインディング（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) [編集（Edit）] をクリックします。

ステップ 8 [サイト バインディングの編集（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, （14 ページ）

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。

a) Windows server 2003：http://127.0.0.1/certserv

b) Windows server 2008：https://127.0.0.1/certsrv

ステップ 3 [CA 証明書、証明書チェーン、または CRL のダウンロード（Download a CA certificate, certificate chain, or CRL）] を選択します。

ステップ 4 [エンコード方法（Encoding Method）] で、[Base 64] を選択します。

ステップ 5 [CA 証明書のダウンロード（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

ルート証明書のサブジェクトの共通名（CN）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

ルート証明書の IM and Presence サーバへのアップロード, （15 ページ）

ルート証明書の IM and Presence サーバへのアップロード

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 IM and 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 CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] の [証明書インポート ツール（Certificate Import Tool）] を使用して、次の操作を行います。

証明書のアップロード方法	アクション
[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] の [証明書インポート ツール（Certificate Import Tool）] [証明書インポート ツール（Certificate Import Tool）] は、信頼証明書を IM and 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。 （注） この手順では、[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] の [証明書インポート ツール（Certificate Import Tool）] にアクセスし、設定する方法を 1 つ紹介します。 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。	1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] の [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）] を選択します。 2 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。 3 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。 • IP アドレス • ホスト名 • FQDN 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。 4 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。 5 [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。 • ピア サーバの到達可能性ステータス：IM and Presence が Exchange サーバに到達（ping）できるかどうかを示します。 Exchange サーバの接続ステータスに関するトラブルシューティングを参照してください。 • 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、IM and 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 接続と証明書のステータスのトラブルシューティング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	アクション
Cisco Unified Operating System Administration 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。	1 IM and 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。 2 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] のログイン ウィンドウの [ナビゲーション（Navigation）] メニューから [Cisco Unified IM and Presence OS の管理（Cisco Unified IM and Presence OS Administration）] を選択し、[移動（Go）] を選択します。 3 Cisco Unified IM and Presence 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。 4 [セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。 5 [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。 6 [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。 • [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。 • 拡張子を付けずにルート証明書の名前を入力します。 7 [参照（Browse）] を選択し、[certnew.cer] を選択します。 8 [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, （15 ページ））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 Presence Engine と SIP プロキシ サービスを再起動します。 [Cisco Unified IM and Presence のサービスアビリティ（Cisco Unified IM and Presence Serviceability）] > [ツール（Tools）] > [サービスの開始（Service Activation）] を選択します。

トラブルシューティングのヒント

- IM and Presence では、Exchange サーバの信頼証明書をサブジェクトの共通名（CN）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 IM and Presence のサービスアビリティ（Cisco Unified IM and Presence 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。