Cisco Adaptive Security Appliance による SIP フェデレーション セキュリティ証明書の設定

（注） IM and Presence サービス リリース 9.0(1) 以降では、Microsoft Lync とのドメイン間フェデレーションがサポートされています。OCS とのドメイン間フェデレーションへの参照には、別途明示的な指定がない限り、Microsoft Lync が指定されます。

IM and Presence サービスと Cisco Adaptive Security Appliance の間でのセキュリティ証明書交換

Cisco Adaptive Security Appliance でのキーペアとトラスト ポイントの生成

この証明書に対してキー ペア（例、**cmp_proxy_key**）を作成し、Cisco Adaptive Security Appliance から IM and Presence サービスへの自己署名証明書を識別するトラストポイント（例、**imp_proxy**）を設定する必要があります。CiscoAdaptive Security Appliance で自己署名証明書を作成しているこ

とを示すために登録タイプを“self”と指定するとともに、証明書のサブジェクト名にインターフェイス内の IP アドレスを指定する必要があります。

はじめる前に

次の章に記載されている設定タスクを実行したことを確認します。

- SIP フェデレーション用の IM and Presence サービスの設定
- SIP フェデレーションに関する Cisco Adaptive Security Appliance（ASA）の設定

手順

ステップ 1 Cisco Adaptive Security Appliance で、設定モードに入ります。

```
> Enable
> <password>
> configure terminal
```

ステップ 2 次のコマンドを入力して、この証明書のキー ペアを生成します。

```
crypto key generate rsa label imp_proxy_key modulus 1024
```

ステップ 3 次の一連のコマンドを入力して、IM and Presence サービスのトラストポイントを作成します。

```
crypto ca trustpoint trustpoint_name (for example, imp_proxy)
(config-ca-trustpoint)# enrollment self
(config-ca-trustpoint)# fqdn none
(config-ca-trustpoint)# subject-name cn=ASA_inside_interface_ip_address
(config-ca-trustpoint)# keypair imp_proxy_key
```

トラブルシューティングのヒント

show crypto key mypubkey rsa コマンドを入力して、キー ペアが生成されていることを確認します。

次の作業

Cisco Adaptive Security Appliance での自己署名証明書の作成, （2 ページ）

Cisco Adaptive Security Appliance での自己署名証明書の作成

はじめる前に

- Cisco Adaptive Security Appliance でのキーペアとトラスト ポイントの生成, （1 ページ）の手順を実行します。

- この手順を実行するには、UNIX 対応のテキスト エディタが必要です。Microsoft ワードパッド、バージョン 5.1 または Microsoft メモ帳、バージョン 5.1 Service Pack 2 を推奨します。

手順

ステップ 1 次のコマンドを入力して、自己署名証明書を作成します。
`(config-ca-trustpoint)# crypto ca enroll trustpoint_name (for example, imp_proxy)`

ステップ 2 サブジェクト名にデバイスのシリアル番号を含めることを確認するメッセージが表示されたら、**no** と入力します。

ステップ 3 自己署名証明書を作成するよう求めるプロンプトに対して、**yes** で応答します。

ステップ 4 次のコマンドを入力して、IM and Presence サービスにエクスポートする証明書を作成します。
crypto ca export *imp_proxy* **identity-certificate**

これによって、たとえば、PEM でエンコードされたアイデンティティ証明書が画面に表示されます。

```
-----BEGIN
CERTIFICATE-----MIIBnDCCAQWgAwIBAgIBMTANBgkqhkiG9w0BAQQFADAUMRIwEAYDVQQDEwlDVVAt……..-----END
CERTIFICATE-----
```

ステップ 5 Cisco Adaptive Security Appliance 証明書の内容全体をコピーし、ワードパッドかメモ帳のファイル（.pem の拡張子を付ける）に貼り付けます。

ステップ 6 .pem ファイルをローカル マシンに保存します。

次の作業

IM and Presence サービスへの自己署名証明書のインポート, （3 ページ）

IM and Presence サービスへの自己署名証明書のインポート

はじめる前に

の手順を実行します。 Cisco Adaptive Security Appliance での自己署名証明書の作成, （2 ページ）

手順

ステップ 1 [Cisco Unified IM and Presence Operating System Administration] ユーザ インターフェイスにログインします。[セキュリティ（Security）] > [証明書管理（Certificate Management）] を選択します。

ステップ 2 [証明書のアップロード（Upload Certificate）] をクリックします。

ステップ 3 [Certificate Purpose（証明書目的）] で、[cup-trust] を選択します。

（注） ルート名のフィールドは空白のままにしておきます。

ステップ 4 [参照（Browse）] をクリックし、ローカル コンピュータで（前の手順で作成した）Cisco Adaptive Security Appliance の .pem 証明書ファイルを特定します。

ステップ 5 [ファイルのアップロード（Upload File）] をクリックし、証明書を IM and Presence サービス ノードにアップロードします。
トラブルシューティングのヒント

証明書の一覧で、`<asa ip address>.pem` と `<asa ip address>.der` を検索すると、見つかります。

次の作業

IM and Presence サービスでの新しい証明書の生成, （4 ページ）

IM and Presence サービスでの新しい証明書の生成

（注） Cisco ASA ファイアウォールの証明書は、内外でサーバ認証属性とクライアント認証属性が設定されている必要があります。これは、証明書の強化キー使用（EKU）パラメータ、または次のオブジェクト ID（OID）の値を調べることで確認できます。

1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2

はじめる前に

の手順を実行します。 IM and Presence サービスへの自己署名証明書のインポート, （3 ページ）

手順

ステップ 1 **[Cisco Unified IM and Presence Operating System Administration]** ユーザ インターフェイスにログインします。[セキュリティ（Security）]>[証明書管理（Certificate Management）] を選択します。

ステップ 2 [新規作成（Generate New）] をクリックします。

ステップ 3 [証明書目的（Certificate Purpose）] ドロップダウン リストで、cup を選択します。

ステップ 4 [生成（Generate）] をクリックします。

次の作業

Cisco Adaptive Security Appliance への IM and Presence サービス証明書のインポート, （5 ページ）

Cisco Adaptive Security Appliance への IM and Presence サービス証明書のインポート

IM and Presence サービス証明書を Cisco Cisco Adaptive Security Appliance にインポートするには、IM and Presence サービスからインポートした証明書を識別するためのトラストポイント（たとえば **cert_from_imp**）を作成し、“terminal” として登録タイプを指定し、IM and Presence サービスから取得した証明書が端末に張り付けられることを表示する必要があります。

（注） IM and Presence サービスと Cisco Unified Communications Manager のノード、ならびに Cisco Adaptive Security Appliance は、同じ NTP ソースから同期する必要があります。

はじめる前に

- IM and Presence サービスでの新しい証明書の生成, （4 ページ）の手順を実行します。
- この手順を実行するには、UNIX 対応のテキスト エディタが必要です。Microsoft ワードパッド、バージョン 5.1 または Microsoft メモ帳、バージョン 5.1 Service Pack 2 を推奨します。

手順

ステップ 1 コンフィギュレーション モードを開始します。

```
> Enable
> <password>
> configure terminal
```

ステップ 2 次のコマンド シーケンスを入力して、インポートした IM and Presence サービス証明書のトラストポイントを作成します。

```
crypto ca trustpoint cert_from_imp enrollment terminal
```

ステップ 3 次のコマンドを入力して、IM and Presence サービスから証明書をインポートします。

```
crypto ca authenticate cert_from_imp
```

ステップ 4 [Cisco Unified IM and Presence Operating System Administration] ユーザ インターフェイスにログインします。IM and Presence サービスで [セキュリティ（Security）] > [証明書管理（Certificate Management）]を選択します。

ステップ 5 [検索（Find）] をクリックします。

ステップ 6 前の手順で作成した IM and Presence サービス証明書を特定します。

ステップ 7 [ダウンロード（Download）] をクリックします。

ステップ 8 推奨されているテキスト エディタの 1 つを使用して、imp.pem ファイルを開きます。

ステップ 9 imp.pem の内容を切り取って、Cisco Adaptive Security Appliance 端末に貼り付けます。

ステップ 10 **quit** を入力します。

ステップ 11 証明書の承認を確認するメッセージが表示されたら、**yes** と入力します。

ステップ 12 証明書を表示するには、**show crypto ca certificate** コマンドを実行します。

次の作業

Microsoft CA を使用した Cisco Adaptive Security Appliance と Microsoft Access Edge（外部インターフェイス）の間でのセキュリティ証明書交換, （6 ページ）

Microsoft CA を使用した Cisco Adaptive Security Appliance と Microsoft Access Edge（外部インターフェイス）の間でのセキュリティ証明書交換

次の手順は、Microsoft CA を使用して証明書を設定する方法を示した例です。

（注） VeriSign CA を使用した手順の例は、このマニュアルの付録に記載されています。

CA トラストポイント

トラストポイントを作成する場合、トラストポイントに対して使用する登録方法を指定する必要があります。登録方法としては、Simple Certificate Enrollment Process（SCEP）を使用できます（Microsoft CA を使用する場合）。SCEP では、**enrollment url** コマンドを使用して、宣言したトラストポイントの SCEP による登録に使用する URL を定義します。定義した URL は、使用する CA の URL にする必要があります。

このほかに使用できる登録方法には、手動登録があります。手動登録では、**enrollment terminal** コマンドを使用して、CA から受信した証明書をターミナルに貼り付けます。いずれの登録方法の手順についても、この項で説明します。登録方法の詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

SCEP を使用するには、次の URL から Microsoft SCEP アドオンをダウンロードする必要があります。

http://www.microsoft.com/Downloads/details.aspx?familyid=9F306763-D036-41D8-8860-1636411B2D01&displaylang=en

SCEP アドオンは、証明書を設定する Microsoft CA にインストールする必要があります。

次のように SCEP アドオンをダウンロードします。

- **scepsetup.exe** をダウンロードし、実行します。
- [ローカル システム アカウント（local system account）] を選択します。
- [登録する SCEP チャレンジ フレーズ（SCEP challenge phrase to enroll）] を選択解除します。
- CA の詳細を入力します。

[終了（Finish）] をクリックして、SCEP の URL を取得します。この URL は、Cisco Adaptive Security Appliance（ASA）でのトラストポイントの登録時に使用します。

SCEP を使用した Cisco Adaptive Security Appliance での証明書の設定

手順

ステップ 1 次のコマンドを入力して、CA のキー ペアを生成します。
crypto key generate rsa label *public_key_for_ca* **modulus 1024**

ステップ 2 次のコマンドを入力して、CA を識別するトラストポイントを作成します。
crypto ca trustpoint *trustpoint_name*

ステップ 3 **client-types** コマンドを使用して、トラストポイントのクライアント接続タイプを指定します。このクライアント接続タイプは、ユーザ接続に関連付けられた証明書を検証するために使用できます。**client-types ssl** 設定を指定する次のコマンドを入力することで、このトラストポイントを使用して SSL クライアント接続が確認できることを指定します。
`(config-ca-trustpoint)#` **client-types ssl**

ステップ 4 次のコマンドを入力して、パブリック IM and Presence サービス アドレスの FQDN を設定します。
fqdn *fqdn_public_imp_address*

（注） ここで、VPN 認証に関する警告が発行される場合があります。

ステップ 5 次のコマンドを入力して、トラストポイントのキー ペアを設定します。
keypair *public_key_for_ca*

ステップ 6 次のコマンドを入力して、トラストポイントの登録方法を設定します。
enrollment url http://*ca_ip_address***/certsrv/mscep/mscep.dll**

ステップ 7 次のコマンドを入力して、設定したトラストポイントの CA 証明書を取得します。
crypto ca authenticate *trustpoint_name*

```
INFO: Certificate has the following attributes: Fingerprint: cc966ba6 90dfe235 6fe632fc
2e521e48
```

ステップ 8 CA からの証明書の承認を確認するメッセージが表示されたら、**yes** と入力します。

```
Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.
```

ステップ 9 **crypto ca enroll** コマンドを実行します。

crypto ca enroll *trustpoint_name*

次の警告の出力が表示されます。

```
%WARNING: The certificate enrollment is configured with an fqdn that differs from the system
fqdn.If this certificate will be used for VPN authentication this may cause connection
problems.
```

ステップ 10 登録の続行を確認するメッセージが表示されたら、**yes** と入力します。

```
Would you like to continue with this enrollment? [yes/no]: yes

% Start certificate enrollment..
```

ステップ 11 チャレンジ パスワードを作成するよう求めるプロンプトに対して、パスワードを入力します。

```
% Create a challenge password.You will need to verbally provide this password to the CA
Administrator in order to revoke your certificate.For security reasons your password will
not be saved in the configuration.Please make a note of it.

Password: <password>

********** Re-enter password: **********
```

ステップ 12 サブジェクト名にデバイスのシリアル番号を含めることを確認するメッセージが表示されたら、**no** と入力します。

ステップ 13 CA に証明書を要求するよう求めるメッセージが表示されたら、**yes** と入力します。

```
Request certificate from CA? [yes/no]: yes

% Certificate request sent to Certificate Authority
```

ステップ 14 CA に移動し、保留されていた証明書を発行します（証明書が自動的に発行されていなかった場合）。

次の作業

外部 Access Edge インターフェイスの証明書の設定, （10 ページ）

手動による登録を使用した Cisco Adaptive Security Appliance での証明書の設定

CA 証明書のアップロードによるトラストポイントの登録：

手順

ステップ 1 次のコマンドを入力して、CA のキー ペアを生成します。
crypto key generate rsa label *public_key_for_ca* **modulus 1024**

ステップ 2 次のコマンド シーケンスを入力して、CA を識別するトラストポイントを生成します。
crypto ca trustpoint *trustpoint_name* **fqdn** *fqdn_public_imp_address* **client-types ssl keypair** *public_key_for_ca*

（注）
- FQDN 値は、パブリック IM and Presence サービス アドレスの FQDN である必要があります。
- キー ペア値は、CA 用に作成されたキー ペアである必要があります。

ステップ 3 次のコマンドを入力して、トラストポイントの登録方法を設定します。
enrollment terminal

ステップ 4 次のコマンドを入力して、証明書を認証します。
crypto ca authenticate *trustpoint_name*

ステップ 5 CA のルート証明書を取得します。
a) CA の Web ページに移動します（例：`http(s)://ca_ip_address/certsrv`）。
b) [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）] をクリックします。
c) Base 64 を選択します。
d) CA 証明書のダウンロード
e) 証明書を .cer ファイルとして保存します（例：`CARoot.cer`）。

ステップ 6 ルート証明書（.cer ファイル）をテキスト エディタで開きます。

ステップ 7 Cisco Adaptive Security Appliance 端末に証明書の内容をコピー アンド ペーストします。

ステップ 8 証明書の承認を確認するメッセージが表示されたら、**yes** と入力します。
Cisco Adaptive Security Appliance のパブリック証明書に CSR を生成します。

ステップ 9 次のコマンドを入力して、CA に対する登録要求を送信します。
crypto ca enroll *trustpoint_name*

ステップ 10 サブジェクト名にデバイスのシリアル番号を含めるかどうかを尋ねるプロンプトに対して、**no** で応答します。

ステップ 11 証明書要求を表示するよう求めるプロンプトに対して、**yes** で応答します。

ステップ 12 この Base-64 証明書をコピーして、テキスト エディタに貼り付けます（後の手順で使用するため）。

ステップ 13 登録要求を再表示するよう求めるプロンプトに対して、**no** で応答します。

ステップ 14 （手順 4 でコピーした）base-64 証明書を CA の証明書要求ページに貼り付けます。
a) CA の Web ページに移動します（例：`http(s)://ca_ip_address/certsrv`）。
b) [証明書を要求する（Request a certificate）] をクリックします。
c) [証明書の要求の詳細設定（Advanced certificate request）] をクリックします。

d) [Base 64 エンコード CMC または PKCS #10 ファイルを使用して証明書の要求を送信する...（Submit a certificate request by using a base-64-encoded CMC orPKCS#10 file...）] を選択します。
e) （手順 4 でコピーした）base-64 証明書を貼り付けます。
f) 要求を送信し、CA から証明書を発行します。
g) 証明書をダウンロードし、.cer ファイルとして保存します。
h) 証明書をテキスト エディタで開き、内容をコピーして端末に貼り付けます。別の行に **quit** という単語を入力して終了します。

ステップ 15 次のコマンドを入力して、CA から受信した証明書をインポートします。

```
crypto ca import trustpoint_name certificate
```

ステップ 16 登録を続行するかどうかを尋ねるプロンプトに対して、**yes** で応答します。

次の作業

外部 Access Edge インターフェイスの証明書の設定, （10 ページ）

外部 Access Edge インターフェイスの証明書の設定

この手順では、スタンドアロン CA を使用して Access Edge サーバで証明書を設定する方法について説明します。

CA 証明書チェーンのダウンロード

手順

ステップ 1 Access Edge サーバで、[スタート（Start）] > [実行（Run）] を選択します。
ステップ 2 http://<name of your Issuing CA Server>/certsrv を入力し、[OK] をクリックします。
ステップ 3 [タスクの選択（Select a task）] メニューから [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）] をクリックします。
ステップ 4 [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）] メニューから [CA 証明書チェーンのダウンロード（Download CA certificate chain）] をクリックします。
ステップ 5 [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）] をクリックします。
ステップ 6 サーバのハードディスク ドライブにファイルを保存します。このファイルの拡張子は .p7b です。この .p7b ファイルを開くと、チェーンに次の 2 つの証明書が表示されます。
a) スタンドアロンのルート CA 証明書の名前
b) スタンドアロンの下位 CA 証明書の名前（ある場合）

次の作業

CA 証明書チェーンのインストール, （11 ページ）

CA 証明書チェーンのインストール

はじめる前に

の手順を実行します。CA 証明書チェーンのダウンロード, （10 ページ）

手順

ステップ 1 [スタート（Start）] > [実行（Run）] を選択します。

ステップ 2 `mmc` を入力し、[OK] をクリックします。

ステップ 3 [ファイル（File）] メニューで、[スナップインの追加と削除（Add/Remove Snap-in）] を選択します。

ステップ 4 [スナップインの追加と削除（Add/Remove Snap-in）] ダイアログボックスで [追加（Add）] をクリックします。

ステップ 5 [利用可能なスタンドアロン スナップイン（Available Standalone Snap-ins）] のリストで [Certificates（証明書）] を選択します。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [コンピュータ アカウント（Computer account）] を選択します。

ステップ 8 [Next] をクリックします。

ステップ 9 [コンピュータの選択（Select Computer）] ダイアログボックスで、次のタスクを実行します。

a) [<ローカル コンピュータ>（このコンソールを実行しているコンピュータ）] が選択されていることを確認します。

b) [終了（Finish）] をクリックします。

ステップ 10 [閉じる（Close）] をクリックします。

ステップ 11 [OK] をクリックします。

ステップ 12 [証明書（Certificates）] コンソールの左側のペインで、[証明書：ローカルコンピュータ（Certificates: Local Computer）] を展開します。

ステップ 13 [信頼されたルート証明機関（Trusted Root Certification Authorities）] を展開します。

ステップ 14 [証明書（Certificates）] を右クリックし、[すべてのタスク（All Tasks）] をポイントします。

ステップ 15 [インポート（Import）] をクリックします。

ステップ 16 [インポート（Import）] ウィザードで、[次へ（Next）] をクリックします。

ステップ 17 [参照（Browse）] をクリックして、証明書チェーンを保存した場所に移動します。

ステップ 18 ファイルを選択し、[開く（Open）] をクリックします。

ステップ 19 [Next] をクリックします。

ステップ 20 [証明書をすべてストアに配置する（Place all certificates in the store）] というデフォルト値のままにして、[証明書ストア（Certificate store）] の下に [信頼されるルート証明機関（Trusted Root Certification Authorities）] が表示されていることを確認します。

ステップ 21 [Next] をクリックします。

ステップ 22 [終了（Finish）] をクリックします。

次の作業

CA サーバからの証明書の要求, （12 ページ）

CA サーバからの証明書の要求

はじめる前に

の手順を実行します。 CA 証明書チェーンのインストール, （11 ページ）

手順

ステップ 1 Access Edge サーバにログインし、Web ブラウザを開きます。

ステップ 2 URL **http://***certificate_authority_server_IP_address***/certsrv** を開きます。

ステップ 3 [証明書を要求する（Request a Certificate）] をクリックします。

ステップ 4 [証明書の要求の詳細設定（Advanced certificate request）] をクリックします。

ステップ 5 [この CA への要求を作成して送信する（Create and submit a request to this CA）] をクリックします。

ステップ 6 [必要な証明書の種類（Type of Certificate Needed）] リストから **[その他（Other）]** をクリックします。

ステップ 7 件名共通名に Access Edge 外部インターフェイスの FQDN を入力します。

ステップ 8 [オブジェクト識別子（OID）（Object Identifier (OID)）] フィールドに、次の値を入力します。
1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2

（注） OID の中央にある 2 つの 1 をカンマで区切ります。

ステップ 9 次のいずれかの手順を実行します。

a) Windows Certificate Authority 2003 を使用する場合は、[主要オプション（Key Options）] で [ローカルコンピュータ証明書ストアに証明書を格納（Store certificate in the local computer certificate store）] チェックボックスをオンにします。

b) Windows Certificate Authority 2008 を使用している場合は、この項の「トラブルシューティングのヒント」で説明している回避策を参照してください。

ステップ 10 わかりやすい名前を入力します。

ステップ 11 [送信（Submit）] をクリックします。

次の作業

CA サーバからの証明書のダウンロード, （13 ページ）

CA サーバからの証明書のダウンロード

はじめる前に

の手順を実行します。 CA サーバからの証明書の要求, （12 ページ）

手順

ステップ 1 [スタート（Start）] > [管理ツール（Administrative Tools）] > [認証局（Certificate Authority）] を選択して、CA コンソールを起動します。

ステップ 2 左側のペインで、[保留中の要求（Pending Requests）] をクリックします。

ステップ 3 右側のペインで、ユーザが送信した証明書要求を右クリックします。

ステップ 4 [すべてのタスク（All Tasks）] > [発行（Issue）] を選択します。

ステップ 5 CA を実行している Access Edge サーバで `http://local_server/certsrv` を開きます。

ステップ 6 [保留中の証明書要求の状態の表示（View the Status of a Pending Certificate Request）] をクリックし、証明書要求をクリックします。

ステップ 7 [この証明書のインストール（Install this certificate）] をクリックします。

次の作業

Access Edge への証明書のアップロード, （14 ページ）

Access Edge への証明書のアップロード

この手順では、証明書ウィザードを使用して Access Edge サーバに証明書をアップロードする方法について説明します。また、Access Edge サーバには手動で証明書をインポートすることもできます。それには、[Microsoft Office Communications Server 2007] > [プロパティ（Properties）] > [エッジ インターフェイス（Edge Interfaces）] を選択します。

はじめる前に

の手順を実行します。 CA サーバからの証明書のダウンロード, （13 ページ）

手順

ステップ 1 Access Edge サーバで、[スタート（Start）] > [管理ツール（Administrative Tools）] > [コンピュータの管理（Computer Management）] を選択します。

ステップ 2 左側のペインで、[Microsoft Office Communications Server 2007] を右クリックします。

ステップ 3 [証明書（Certificates）] をクリックします。

ステップ 4 [Next] をクリックします。

ステップ 5 [既存の証明書を割り当てる（Assign an existing certificate）] タスク オプションをクリックします。

ステップ 6 [Next] をクリックします。

ステップ 7 外部 Access Edge インターフェイスに使用する証明書を選択し、[次へ（Next）] をクリックします。

ステップ 8 [Next] をクリックします。

ステップ 9 [エッジ サーバのパブリック インターフェイス（Edge Server Public Interface）] チェックボックスをオンにし、[次へ（Next）] をクリックします。

ステップ 10 [Next] をクリックします。

ステップ 11 [終了（Finish）] をクリックします。

次の作業

Cisco Adaptive Securiy Appliance での TLS プロキシ設定

エンタープライズ認証局を使用した Access Edge のカスタム証明書の作成

次の手順を参照する必要があるのは、Microsoft エンタープライズ Certificate Authority を使用して Access Edge の外部インターフェイスまたは Cisco Adaptive Security Appliance にクライアント/サーバ ロール証明書を発行する場合です。

はじめる前に

次の手順を実行するには、認証局がエンタープライズ CA で、Windows Server 2003 または 2008 の Enterprise Edition にインストールされている必要があります。

この手順の詳細については、http://technet.microsoft.com/en-us/library/bb694035.aspx に記載されている Microsoft の指示を参照してください。

カスタム証明書テンプレートの作成および発行

手順

ステップ 1 次の URL にある Microsoft サイト「Creating and Issuing the Site Server Signing Certificate Template on the Certification Authority」の手順 1 ～ 6 を実行します。
http://technet.microsoft.com/en-us/library/bb694035.aspx#BKMK_siteserver1

ヒント 手順 5 では、この特別なテンプレートに相互認証証明書などの適切な名前を使用します。

ステップ 2 Microsoft サイトの手順 7 ～ 12 の代わりに次の手順を実行します。

a) [拡張（Extensions）] タブを選択します。[アプリケーションのポリシー（Application Policies）] の下に [クライアント認証（Client Authentication）] および [サーバ認証（Server Authentication）] があり、他のポリシーがないことを確認します。これらのポリシーがない場合は、続行する前に追加する必要があります。

- [アプリケーション ポリシーの拡張の編集（Edit Application Policies Extension）] ダイアログボックスで、[追加（Add）] を選択します。
- [アプリケーションのポリシーの追加（Add Application Policy）] ダイアログボックスで、[クライアント認証（Client Authentication）] を選択し、Shift を押してから [サーバ認証（Server Authentication）] を選択して、[追加（Add）] をクリックします。
- [アプリケーション ポリシーの拡張の編集（Edit Application Policies Extension）] ダイアログボックスで、他にポリシーがあれば、それを選択して [削除（Remove）] を選択します。

[新しいテンプレートのプロパティ（Properties of New Template）] ダイアログボックスに、[アプリケーションのポリシー（Application Policies）] の説明として、クライアント認証（Client Authentication）とサーバ認証（Server Authentication）のリストが表示されます。

b) [発行要件（Issuance Requirement）] タブを選択します。証明書が自動的に発行されないようにしたい場合は、[CA 証明書マネージャの許可（CA certificate manager approval）] を選択します。これ以外の場合は、このオプションは空白のままにしておきます。

c) [セキュリティ（Security）] タブを選択し、必要なすべてのユーザとグループに読み取り権限と登録権限を必ず付与します。

d) [要求の処理（Request Handling）] タブを選択し、[CSP] ボタンをクリックします。

e) [CSP の選択（CSP Selection）] ダイアログボックスで、[要求で次の CSP のいずれかを使用（Requests must use one of the following CSP's）] をオンにします。

f) CSP のリストから、[Microsoft Basic Cryptographic Provider v1.0 および Microsoft Enhanced Cryptographic Provider v1.0（Microsoft Basic Cryptographic Provider v1.0 and Microsoft Enhanced Cryptographic Provider v1.0）] を選択し、[OK] を選択します。

ステップ 3 次の URL にある Microsoft サイト「Creating and Issuing the Site Server Signing Certificate Template on the Certification Authority」の手順 13 ～ 15 に進みます。
http://technet.microsoft.com/en-us/library/bb694035.aspx#BKMK_siteserver1

次の作業

サイト サーバ署名証明書の要求, （17 ページ）

サイト サーバ署名証明書の要求

手順

ステップ 1 次の URL にある Microsoft サイト「Site Server Signing Certificate for the Server That Will Run the Configuration Manager 2007 Site Server」の手順 1 ～ 6 を実行します。
http://technet.microsoft.com/en-us/library/bb694035.aspx#BKMK_siteserver2

ヒント 手順 5 では、相互認証証明書など、以前に作成した証明書テンプレートの名前を選択し、[名前（Name）] フィールドに Access Edge の外部 FQDN を入力します。

ステップ 2 Microsoft サイトの手順 7 ～ 8 の代わりに次の手順を実行します。

a) 証明書要求が自動的に発行される場合は、署名証明書をインストールするオプションが提示されます。[この証明書のインストール（Install this Certificate）] を選択します。

b) 証明書要求が自動的に出されなければ証明書を導入するために管理者を待ちます。発行されたら、次を実行します。

- メンバ サーバで、Internet Explorer をロードし、`http://<server>/certsrv` のアドレスを使用して Web 登録サービスに接続します。ここで、`<server>` はエンタープライズ CA の名前または IP アドレスです。
- [ようこそ（Welcome）] ページで、[保留中の証明書の要求の状態（View the status of a pending certificate request）] を選択します。

c) 発行された証明書を選択し、[この証明書のインストール（Install this Certificate）] を選択します。

TLS フェデレーション用の Lync エッジ サーバでのセキュリティ証明書の設定

Microsoft Lync との TLS フェデレーション用に Access Edge 上で証明書を設定する方法については、URL http://technet.microsoft.com/en-us/library/gg398409.aspx にある Microsoft TechNet ライブラリの文書を参照してください。IM and Presence サービスでフェデレーテッド接続を行うには相互 TLS 認証が必要なため、サーバ認証とクライアント認証を両方サポートするよう Microsoft Lync 証明書を設定する必要があります。上記のガイドに従う場合は、2 番目の項をスキップして 3 番目の項に移動します。この項には、AOL とのパブリック IM 接続をサポートするエッジ サーバの外部

インターフェイスに対して証明書要求を作成する方法が記載されています。AOL にも、IM and Presence サービスと同じ相互 TLS 認証要件があります。このガイドは、TLS 上で IM and Presence サービスとのフェデレーションを直接行うよう Lync Server を設定するのにも使用できます。

ダイレクト フェデレーションを行えるよう Lync Server でスタティック ルートを設定する方法については、IM and Presence から Lync へのスタティック ルートの設定を参照してください。