CHAPTER 11

リソース ファイルの管理

ここでは、ACE Web Application Firewall Manager により使用されるポリシーのリソース ファイルでの作業方法について説明します。内容は次のとおりです。

リソース ファイルのタイプ

ACE Web Application Firewall ポリシーは、ACE Web Application Firewall によるトラフィックの処理方法を制御するオブジェクトおよび設定で構成されます。ポリシー オブジェクトの 1 つにリソース ファイルがあります。リソース ファイルは、ポリシー全体で使用できる完全独立したアーティファクトです。これには次のものが含まれます。

- 公開鍵 / 秘密鍵：公開鍵 / 秘密鍵ペアは、ACE Web Application Firewall の ID を認証するときに使用されます。
- 信頼できる認証局：ACE Web Application Firewall インスタンスが信頼できる証明書のプロバイダーを識別する X.509 証明書ファイル。
- リモート サーバ証明書：宛先サーバの識別に使用される X.509 証明書ファイル。

ここでは、リソース ファイルをアップロードおよび管理する方法について説明します。通常、ACE Web Application Firewall Manager の Web コンソールの [Resource Manager] ページから、またはリソースが適用されるページからなど、コンソールで特定のタイプのリソース ファイルをアップロードする方法は複数あります。ここでは、リソース マネージャを使用してリソースをアップロードする方法について簡単に説明します。リソースがアップロードされると、コンソールの適切な位置でメニュー選択肢として表示されます。

これは、通常、ファイルシステムの位置からではなく、URL の位置からリソースをロードするときに適しています。これを使用することで、URL ベースのリソース更新を利用できます。リソース更新は、ACE Web Application Firewall Manager がソースのアップデートがあるかどうかをチェックしてポリシーにあるリソースのアップデートをチェックするプロセスです。アップデートがある場合、リソースは更新できます。詳細については、「導入時の URL ベース リソースのリロード」（P.12-5）を参照してください。

CSR の生成

ACE Web Application Firewall に関連付けられている公開鍵 / 秘密鍵ペアを使用することで、ACE Web Application Firewall とユーザとの間、または ACE Web Application Firewall とバックエンド サービスとの間で通信チャネルを保護できます。証明書を取得する場合、まず Certificate Authority（CA; 認証局）への発行を求める、Certificate Signing Request（CSR; 証明書署名要求）を作成します。

ACE Web Application Firewall Manager の Web コンソールで証明書要求を生成するには、次の手順を実行します。

ステップ 1　操作メニューの [Resources] セクションの [Public/Private Keypairs] リンクをクリックします。

ステップ 2　ページ下部の [Generate CSR] ボタンをクリックします。

ステップ 3　[Generate Certificate Signing Request] ページで、[Resource Name] フィールドに、ポリシーでこのリソースを識別する名前を入力します。

ステップ 4　[Subject Identification Information] セクションの次のフィールドに、適切な値を入力します。

表 11-1　CSR 設定

フィールド	説明
[Common Name]	このフィールドには、ACE Web Application Firewall の外部ホスト名が含まれます。クラスタ化された Firewall 設定では、これは、ユーザがクラスタのアドレス指定に使用する共通ホスト名になります。
[E-mail Address]	CSR に対応して署名入り証明書を受け取る電子メール アドレス。
[Company (O)]	CN が関連付けられる組織または会社の名前。
[Department (OU)]	組織内の組織ユニットまたはサブグループの名前。
[City]	認証されるエンティティの地域または市。
[State]	認証されるエンティティの州または地方。
[ISO Country Code]	認証されるエンティティの国を表す 2 文字の International Standards Organization（ISO; 国際標準化機構）コード。

ステップ 5　[Key Type] メニューで、証明書のシグニチャを生成するときに使用するアルゴリズムを選択します。次のオプションから選択します。

- [RSA] : RSA 公開鍵暗号システム Secure Hash Algorithm。詳細については、W3C の Web サイトの RSA-SHA1 Signature Suite ページを参照してください。
- [DSA] : Digital Signature Algorithm Secure Hash Algorithm。詳細については、US National Institute of Standards and Technology（NIST）の Web サイトの Digital Signature Standard（DSS; デジタル シグニチャ規格）ページを参照してください。

ステップ 6　任意に、[Key Size] メニューから項目を選択して、証明書のシグニチャの生成に使用する鍵のサイズを指定します。

- [512 bits] : 512 ビット鍵を使用してシグニチャを生成します。
- [1024 bits] : 1024 ビット鍵を使用してシグニチャを生成します。これは、デフォルトの設定です。
- [2048 bits] : 2048 ビット鍵を使用してシグニチャを生成します。

ステップ 7　任意に、証明書が提供する追加の属性を定義します。

a. [Add Attribute] ボタンをクリックします。[Attribute OID] フィールドおよび [Value] フィールドは [Additional Attributes] セクションに表示されます。

b. [Attribute OID] フィールドに、追加属性の名前を OID 形式で入力します。

c. [Value] フィールドに、追加属性の値を入力します。

d. 必要に応じて前述の手順を繰り返して、必要なすべての属性を追加します。

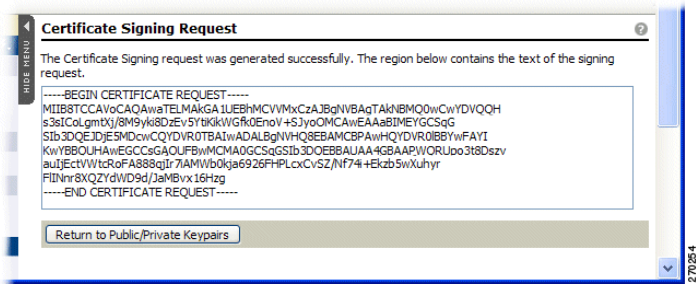
属性を削除するには、カスタム 属性のリストでその行の最後に表示されている [Remove] ボタンをクリックします。

ステップ 8　情報を入力したら、[Generate Request] ボタンをクリックします。

入力した情報を使用して ACE Web Application Firewall Manager は証明書署名要求（CSR）を生成し、これを [Certificate Signing Request] ページに表示します。

[Generated Request] ページは、次のようなページです。

図 11-1　[Generated Request] フォーム



ステップ 9　CSR データ（「-----BEGIN CERTIFICATE REQUEST-----」文字列と「-----END CERTIFICATE REQUEST-----」文字列の間の部分）をテキスト ファイルまたは電子メール メッセージにコピーします。

ステップ 10　CSR データを目的の CA に送信し、署名入りの X.509 証明書に変換します。

（注）　要求を送信する場合、CA により、必要な証明書のタイプを指定するように指示されることがあります。ACE Web Application Firewall は、通常、Apache スタイル証明書として識別される証明書を使用します。

署名入り証明書が送られたら、次のセクションに示すように、これを ACE Web Application Firewall にインストールします。

鍵ペア リソースのアップロード

鍵ペア リソースは、PKI 公開鍵/秘密鍵ペアを保存するファイルです。ACE Web Application Firewall Manager は、鍵ペア リソース ファイルを使用して、Web コンソールにアクセスしようとするブラウザとの SSL 接続を実装します。サービス トラフィックは、システム公開鍵/秘密鍵ペアによっても保護できます。

[Public/Private Keypairs] ページは、現在アクティブなサブポリシーのすべての鍵ペア リソースをリストします。このページのエントリは、システムに常駐する鍵ペア リソースを暗号化された形式で表します。

ACE Web Application Firewall Manager は、鍵ペア リソースを使用するポリシーのコンパイルおよび導入を行うときに、鍵ペア データを独自のバイナリ形式でターゲット Firewall に転送します。鍵ペアがクリア テキスト形式にはなることはありません。

鍵ペアは、それ自体、または証明書の一部として ACE Web Application Firewall Manager にアップロードできます。証明書リソースは、ACE Web Application Firewall Manager がデジタル証明書データを保存するときに使用するファイルです。証明書リソースは、任意に、証明書の関連付けられた鍵ペア データを保存できます。鍵ペア リソースのように、証明書リソースは、暗号化された形式だけで、ポリシーに存在します。

鍵ペア リソースを ACE Web Application Firewall Manager のポリシーにアップロードするには、次の手順を実行します。

ステップ 1　Manager の Web コンソールに Administrator ユーザまたは Routing ロールを持った Privileged ユーザとしてログインして、アクティブ サブポリシーを、鍵ペアを使用するサブポリシーに設定します。

ステップ 2　操作メニューで [Public/Private Keypairs] リンクをクリックします。

ステップ 3　ページ上部の [Add a New Public/Private Keypair] ボタンをクリックします （また、証明書および鍵ファイルが同じファイルにない場合 [Upload Separate Certificate and Key Files] を使用します）。

[Upload Public/Private Keypair Resource] ページが表示されます。このページには、[HTTP(S) port settings] ページからアクセスすることもできます。

ステップ 4　[Resource Name] フィールドで、鍵ペア リソースの一意な名前を入力します。この名前は、ACE Web Application Firewall Manager のユーザ インターフェイスの鍵ペアを識別します。

ステップ 5　使用する鍵ペアをファイルシステムの位置から、または URL で指定したネットワーク上の位置から識別します。

ステップ 6　鍵ペアのパスワードを [Password] フィールドに入力します。入力するパスワードはフィールドでは隠されます。

ステップ 7　[Upload] ボタンをクリックします。

ACE Web Application Firewall Manager は、鍵ペア リソースをアップロードして、これをリソースとして [Public/Private Keypairs] ページで表示します。リソースが基本的な有効性テストに合格しない場合、たとえば、リソースが有効な PEM 鍵のペアを提供しない場合、エラー メッセージが赤いテキストで [Upload Public/Private Keypair Resource] ページに表示されます。

完了したら、ポリシーの SSL 接続の設定時に鍵ペアを使用できます。

認証局リソースのアップロード

認証局（CA）の証明書をアップロードすると、その CA と ACE Web Application Firewall の信頼関係が確立されます。ACE Web Application Firewall は、証明書に署名した CA の信頼ステータスに基づいて証明書を受け入れることができます。デフォルトでは、ポリシーには CA 証明書は事前にインストールされていないので、信頼できる任意の CA の証明書をインポートする必要があります。

CA リソースはファイルとして、または URL で指定した位置から ACE Web Application Firewall Manager にアップロードできます。また、LDAP サーバから必要な情報をインポートすることもできます。[Trusted Certificate Authorities] ページは、現在アクティブなサブポリシーで使用できるすべての認証局をリストします。これらのリソースは、デジタル証明書を必要とするサービスを作成または編集する、ページのメニューの名前付き項目として表示されます。

CA リソース ファイルを ACE Web Application Firewall Manager の Web コンソールにアップロードするには、次の手順を実行します。

ステップ 1　コンソールで Administrator ユーザまたは Routing ロールを持った Privileged ユーザとして、アクティブ サブポリシーを、鍵ペアを使用するサブポリシーに設定します。

すべてのサブポリシーで鍵ペアを使用可能にするには、これを **Shared** サブポリシーに追加します。

ステップ 2　操作メニューの [Resources] セクションの [Trusted Certificate Authorities] リンクをクリックします。

ステップ 3　[Trusted Certificate Authorities] ページで、ページ上部付近の [Add a New Certificate Authority Resource] ボタンをクリックします。

[Upload Certificate Authority Resource] ページが表示されます。

ステップ 4　認証局リソースの名前を [Resource Name] フィールドに入力します。これは、ポリシー内で使用されるリソースのわかりやすい名前です。

ステップ 5　リソースのネットワーク アドレスを [URL] フィールドに入力して、[Local File] フィールドのファイル システムの位置から、またはネットワーク上の位置から証明書を指定します。

[Browse] ボタンをクリックして、証明書ファイルにナビゲートすると、[Local File] フィールドにデータが自動的に挿入されます。

ステップ 6　任意に、証明書失効リストの URL を [CRL URL] フィールドに入力します。ACE Web Application Firewall は、証明書失効リストに表示される証明書を使用する接続を拒否します。

ACE Web Application Firewall が証明書失効リストをチェックしないようにするにはこのフィールドを空白のままにします。

ステップ 7　証明書失効リストを設定した場合、ACE Web Application Firewall がリストを取得する頻度も指定します。

ステップ 8　終了したら、[Upload] をクリックして、リソースを ACE Web Application Firewall Manager にアップロードします。

CA 証明書をアップロードしたら、この信頼関係に基づいて要件を設定できます。たとえば、HTTP サーバの SSL 接続設定で、サーバ証明書が信頼できる CA により署名されるように要求できます。