SSL によるトラフィックの保護

ACE XML Gateway は SSL/TLS を使用してユーザにセキュリティを保証するとともに、Gateway とバックエンド サービスの間のトラフィックを保護します。ここでは、ACE XML Gateway とユーザの間で SSL/TLS をセットアップする方法を説明します。

注： このマニュアルでは、以下 SSL/TLS を SSL と省略表記します。厳密にはバージョン 3.0 以下が SSL、バージョン 3.1 が TLS になります。

SSL の仕様では、SSL ハンドシェイクの一部として X.509 証明書の呈示がサーバに要求されます。多くの場合、呈示された証明書が一定の条件に合致しないと、クライアントは SSL ハンドシェイクを中断して通信を中止します。

接続を中断する条件はクライアントにより異なりますが、一般的には SSL 接続を確立するために ACE XML Gateway が呈示する証明書には、次の属性が必要です。

- 証明書が有効なこと（現在の日付が有効な「開始日」と「終了日」の間でなければならない）
- 「サーバ認証」用の拡張鍵があること
- ゲートウェイの DN には、サーバの IP アドレスに名前解決するホスト名と等しい CN があること
- クライアントはサーバ証明書の発行元 CA（認証局）を信頼するように設定されていること。また、サーバ証明書は CA の CRL（失効証明書リスト）に記載されていないこと

このシステムの実装では、ほとんどの場合、これらの要求に合致する CA 署名付きサーバ証明書の要求を組み込み、導入の際にはそれぞれの XML Gateway に証明書をインストールすることになります。

XML Manager コンソールには、証明書への署名要求を生成し、署名された証明書をアップロードするツールが備わっています。ただし、以降の説明では、ACE XML Gateway のサンプル リソース Web サイトから入手できるサンプルの証明書を使うことにします。

SSL 証明書による認証について

ACE XML Gateway はクライアントの証明書を確認しなくてもクライアントとの間で SSL セッションを確立できますが、たいていの場合、SSL ではクライアントの証明書の確認を行います。

ACE XML Gateway は、クライアント認証のために呈示された証明書を複数の方法で確認できます。最も単純な方法はサムプリントの合致によるものです。この方法では、ユーザから呈示された証明書と、ID 認証要件として設定されているものを ACE XML Gateway が比較します。サムプリントが合致すると、そのユーザが適格であると見なされます。

ACE XML Gateway は、クライアントの証明書を発行した認証局に基づいてユーザを認証することもできます。

ここでは、サムプリント照合による認証方法を説明します。この方法では、最初にその証明書の証明情報を定義する新しいオーセンティケータを作成します。次に、保護されたポートを待ち受けるハンドラをセットアップします。

必要な準備

評価用として利用できる証明書を持っていない場合は、次のリソース サンプル ページから証明書を入手できます。

http://example.reactivity.com/security.html

始める前に、Oak サーバ（このページの最下部）の 1 つで用いるサーバ用証明書を PKCS #12 形式でダウンロードします（次に行う手順では、Oak Server 証明書のうちの最初の P12 形式証明書、`maple.p12` を使用します）。PKCS #12 形式ファイルはパスワードで保護されていることがよくあります。このサンプルの証明書はパスワード `swordfish` で保護されています。

また、Oak セキュリティ チームの架空ビジネス パートナー（Beagle Partners, Inc. など）から PEM 形式のクライアント証明書と P12 形式の公開鍵 / 秘密鍵ペアも入手する必要があります。これにはサンプルの Web ページを使います。

XML Gateway の HTTPS ポートを開く

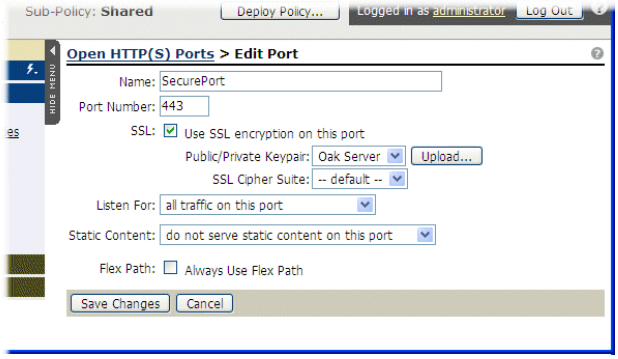
最初に ACE XML Gateway にリスニング ポートを開きます。このポートに SSL の使用を設定します。

1. 操作メニューで **[Open HTTP(S) Ports]** リンクをクリックします。
2. **Open HTTP(S) Ports** ページで **[Add a New Port]** ボタンをクリックします。
3. ポートの名前を入力します（`SecurePort` など）。この名前はリスニング ポートを識別するためのもので、この XML Manager でのみ使用されます。
4. **[Port Number]** として 443 と入力します。これは SSL 用として慣例となっている番号です。
5. **[SSL]** チェック ボックスを選択します。
6. **Public/Private Keypairs** ラベルの横に「public/private keypairs have been uploaded」というメッセージが表示されるはずです。このメッセージの横の **[Upload]** ボタンをクリックします。
7. [Upload Resorce] ウィンドウにリソースの名前を入力します（`Oak Server` など）。

8. **[Browse]** ボタンをクリックし、サンプルページ `maple.p12` からダウンロードした Oak サーバの P12 ファイルをファイル選択ダイアログで探します。
9. **[Password]** 欄に `swordfish` と入力します。
10. **[Public/Private Keypairs]** 欄の中の P12 ファイルに対して **[Upload]** をクリックします。

    次のような **Edit Port** ページが表示されます。

図 14-1　Edit Port ページ



11. **[Save Changes]** をクリックします。

このポート リストの中に新しいポートが現れます。

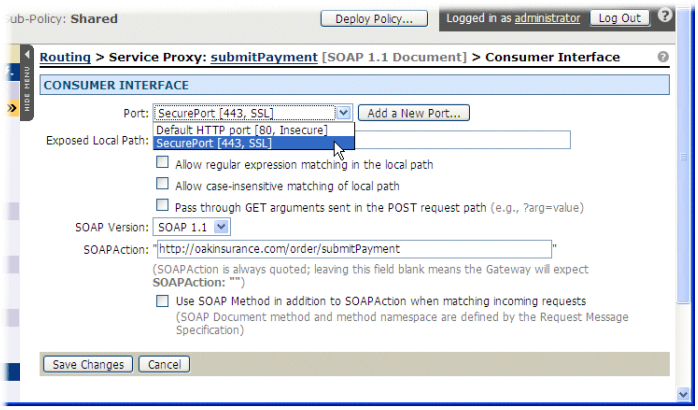
利用ポートの保護をサービス プロキシに設定

保護されたポートを利用するために、サービス プロキシを次のように設定します。

1. 操作メニューで **[Routing Browser]** リンクをクリックします。
2. `submitPayment` というサービス プロキシの名前をクリックします。

   `submitPayment` に対応した情報ページが表示されます。
3. **Consumer Interface** という見出しの横の **[Edit]** リンクをクリックします。
4. 作成した新しいポート SecurePort を **[Port]** ドロップダウン メニューから選択します。

図 14-2　ユーザ向けポートを変更する



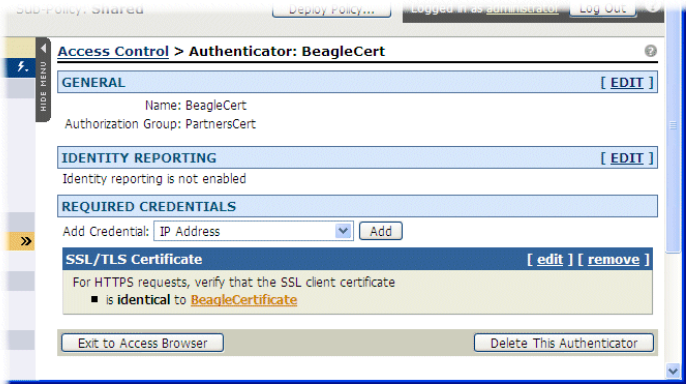
5. **[Save Changes]** をクリックします。

証明書のアクセス要件の作成

次の手順で新しいオーセンティケータを作成します。

1. 操作メニューで **[Access Control Browser]** をクリックします。
2. アクセス コントロール ブラウザで **[Add an Authenticator]** をクリックします。
3. オーセンティケータに名前をつけ（BeagleCert など）、新しい認証グループ PartnersCert に加えます。
4. **[Create]** をクリックします。
5. **Add Credential** メニューから **[SSL/TLS Certificate]** という項目を選択し、**[Add]** をクリックします。
6. **SSL/TLS Certificate** ページで、デフォルトの認証方法 **[SSL Certificate Fingerprint]** が選択された状態のまま、**[Upload]** をクリックして ACE XML Gateway に証明書ファイルをアップロードします。
7. **Upload Consumer Certificate Resource** ウィンドウで **[Resource Name]** 欄に名前を入力します（BeagleCert など）。ポリシー内の証明書をこの名前で識別します。
8. **[Local File]** 欄の横の **[Browse]** ボタンをクリックし、サンプルのセキュリティ リソース ページ `beagle.pem` からダウンロードした証明書ファイルを探します。
9. **[Local File]** 欄に証明書ファイルへのパスが入力された状態で **[Upload]** をクリックします。
10. **[Save Changes]** をクリックします。新しい証明書要件が証明情報リストに現れます。

図 14-3　証明情報リスト



11. **[Exit to Access Browser]** ボタンをクリックします。
12. アクセス コントロール ブラウザで Public 一覧表の右側の SubmitPayment サービス プロキシをクリックします。
13. Access Control for the Service Proxy ページで **[Access is restricted to the following authorization groups]** を選択し、さきほど作成したグループのチェックボックスを選択します。
14. **[Save Changes]** をクリックしてからこのポリシーを導入します。

それでは、このサービス プロキシへの要求を発行してみます。次に、要求とともに Beagle クライアントの証明書を渡す方法を説明します。

証明書アクセス要件のテスト

WFetch で要求の中の証明書を渡すには、最初に証明書を Internet Explorer にアップロードする必要があります（WFetch は要求だけでなく、IE の中にある証明書を渡すことができます）。証明書を Internet Explorer 6.0 にインポートする方法を次に説明します。別の方法として、Curl という HTTP クライアントのコマンド ライン ツールを使用して証明書の受け取りをテストできます。

必要であれば、次の URL から Beagle パートナーの P12 証明書 / 鍵ペアをサンプル ページからダウンロードしてください（まだ行っていない場合）。

http://example.reactivity.com/security.html

証明書をダウンロードしたら、次の手順に従ってください。

1. Internet Explorer で **[Tools > Internet Options]** をクリックします。
2. **[Content]** タブを選択してから **[Certificates]** ボタンをクリックします。
3. **[Import]** ボタンをクリックし、Certificate Import ウィザードを使用して `beagle.p12` ファイルを Internet Explorer にインポートします。
4. 要求された場合はそのファイルのパスワード swordfish を入力します。

要求を発行する前に、WFetch で次の変更を行います。

- **[Port]** として 443 を選択します。
- **[Connect]** 欄では `[https]` を選択します。
- **[cipher]** オプションは `[default]` のまま残します。
- Client cert には `[** cert from IE **]` を選択します。Internet Explorer に複数の証明書が存在する場合は、さきほどアップロードした証明書を選択してください。
- **[Headers and Body]** 欄に次のテキストをペーストしてください。

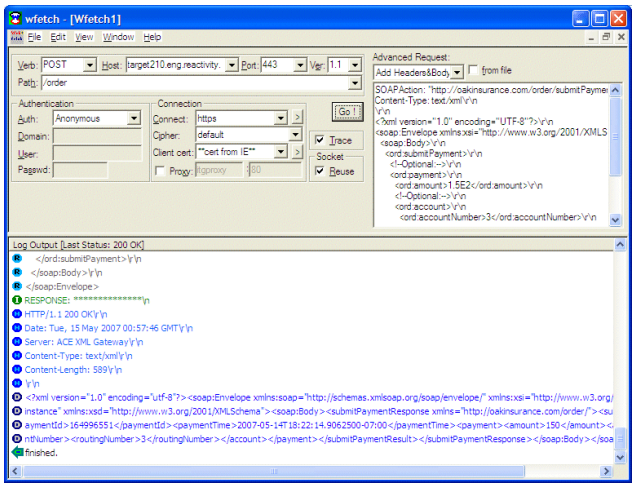
出力例 14-1　SubmitPayment 要求

```
SOAPAction: "http://oakinsurance.com/order/submitPayment"

<?xml version="1.0" encoding="utf-8"?>
 <soap:Envelope
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
   <submitPayment xmlns="http://oakinsurance.com/order/">
   <payment>
    <amount>246.46</amount>
    <account>
      <accountNumber>123456</accountNumber>
      <routingNumber>789123</routingNumber>
    </account>
   </payment>
  </submitPayment>
 </soap:Body>
</soap:Envelope>
```

[Go!] をクリックすると、次のような応答が返ってきます。

図 14-4　証明書の設定を行った WFetch



Curl から送る要求に証明書を組み入れる

Curl を利用すると、次のコマンドでテスト メッセージを発行できます（コマンドライン上で一度にコマンド全体を入力する必要があります)。

```
curl -E beagle.pem:swordfish -k -v
  -H 'Content-Type: text/xml' -H
'SOAPAction: "http://oakinsurance.com/order/submitPayment"'
    --data-binary @- https://10.0.101.73/order
    < payment.xml
```

コマンドの中には Beagle の証明書である beagle.pem（この例では）とともにパスワードも含めることに注意してください。また、payment.xml には、サービスに渡す本文のコンテンツを含めなければなりません。コンテンツは次のようになります。

出力例 14-2　payment.xml のコンテンツ

```
<?xml version="1.0" encoding="utf-8"?>
 <soap:Envelope
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
   <submitPayment xmlns="http://oakinsurance.com/order/">
   <payment>
    <amount>246.46</amount>
    <account>
      <accountNumber>123456</accountNumber>
      <routingNumber>789123</routingNumber>
    </account>
   </payment>
  </submitPayment>
 </soap:Body>
</soap:Envelope>
```