WebEdge バージョン3.8.x SSL接続について

WebEdgeには、Webサーバによるデータ転送を暗号化するためのSSL v3が組み込まれています。

SSLは、サーバからのネットワーク呼出しをいったん取り込み、ブラウザへ送るためにネットワーク層へ転送する前のデータを暗号化します。セッション開始時には、Webサーバとブラウザがネゴシエーションを行い、そのセッション内で使用する暗号化アルゴリズム（暗号法）を決定します。そのセッションで使われる”キー（鍵）”は、公開鍵暗号化方式を使って、安全な方法でブラウザへ送られます。
このセッションキーは、対称的に（つまり、送受信するセッションデータの暗号と復号の両方に）使用されます。

SSLセットアップの最初の手順は、証明書の作成です。

1. サーバ証明書

サーバ証明書は、サーバの身元を証明するもので、信頼のおける第三者認証機関－証明書発行局（CA：Certificate Authority）による署名が付けられます。CAは、署名することによりサーバの身元を保証します。

1.1. CSRの生成

サーバ証明書を取得するには、身元を証明するデータを添えたCSR（証明書署名要求：Certificate Signing Request）をCA（認証局）へ送らなければなりません。CSRを生成するには以下の手順に従います。

(1) 公開鍵/秘密鍵のペアの生成

keytoolコマンドを利用して公開鍵と秘密鍵を生成します。新しい公開鍵と秘密鍵のペアを作成した時点では、公開鍵は常に自己署名証明書でラップされています。

使用方法:
```
keytool -genkey -dname "CN=[Common Name], OU=[Organizational Unit],
                        O=[Organization Name], L=[Locality],
                        S=[State or Province], C=[Country Code]"
        -alias [alias]  -keyalg "[algorithm]" -keypass [key_pass]
        -keystore [key_store] -storepass [store_pass]
        -validity [Validity Period]
```

[Common Name]
　WebEdgeサーバのホスト名とドメイン名を入力します。ここに入力するホスト名とドメイン名は、IPアドレスやDNSエイリアスではなく正式なドメイン名でなければなりません。
[Organization Name]
　正式な組織名を設定します。
[Organizational Unit]
　組織内での部門名または部署名を入力します。
[Locality]
　組織の所在地の都市名を設定します。
[State or Province]
　組織の所在地の県名（または州の名前）を設定します。
[Country Code]
　組織の所在地の国別コードを入力します。国別コードは、国を表す2文字のコードです。
[alias]
　秘密鍵を参照するエイリアスを設定します。
[algorithm]
　鍵を生成するアルゴリズムを設定します。
[key_pass]
　秘密鍵に割り当てるパスワード（6文字またはそれ以上）を設定します。
[key_store]
　生成する鍵を保存するディレクトリを設定します。
[store_pass]
　[key_store] に割り当てるパスワード（6文字またはそれ以上）を設定します。
[Validity Period]
　認証の有効期限を設定します。

例:
```
cd /usr/swcm/WebEdge
jre/bin/keytool -genkey -dname "CN=www.opentech.co.jp, OU=Open Technologies, ¥
                        O=Marketing, L=Bunkyo-ku, S=Tokyo, C=JP" ¥
        -alias OpenTech -keyalg "RSA" -keypass webedge ¥
```

```
        -keystore /usr/swcm/WebEdge/config_mdn/.newkeystore ¥
        -storepass webedge -validity 180
```

(2) CSR（証明書署名要求）の生成

keytoolコマンドを利用してCAにサーバ証明書を発行してもらうためのCSRを生成します。

使用方法:
```
keytool -certreq -alias [alias] -file [alias.csr] -keystore [key_store]
```

[alias]
　　(1)で設定した [alias] を設定します。
[alias.csr]
　　CSRファイルのファイル名（拡張子 .csr）を設定します。
[key_store]
　　(1)で設定した[key_store]を設定します。

例:
```
cd /usr/swcm/WebEdge
jre/bin/keytool -certreq -alias OpenTech -file OpenTech.csr ¥
                -keystore /usr/swcm/WebEdge/config_mdn/.newkeystore
```

1.2. CSRの提出

生成したCSRはPEMでエンコードされており、CAにサーバ証明書を取得するために、電子メールあるいはCAが公開しているサーバ証明書取得のWebページで手続きを行います。
その際に、CSRファイルに記述されている次の内容が必要です。

```
-----BEGIN CERTIFICATE REQUEST----- から
...
-----END CERTIFICATE REQUEST----- までをコピー＆ペーストしCAに登録する
```

CSRをCAに提示すると、CAはサーバ証明書が発行して、電子メールにて返送してきます。
その中に記述されている、

```
-----BEGIN CERTIFICATE----- から
...
-----END CERTIFICATE----- まで
```

をコピー＆ペーストし、file.cerという名前でファイルに保存します。

ブラウザでは、CAによって発行されたサーバ証明書が設定されていなければ、例えば、
Internet Explorerでは、

「このセキュリティ証明書は、信頼できる会社から発行されていません。
　証明書を表示して、この証明機関を信頼するかどうか決定してください。」

というようにユーザに対して、サーバ証明書を信頼するかどうかの確認を求めてきます。
したがって、「1.1. CSRの生成」の「(1) 公開鍵/秘密鍵のペアの生成」で作成した自己署名証明書がラップされているだけのkeystoreファイルでは、ブラウザに対してサーバの身元を証明する正式な証明書とはなりません。

注意：登録申請方法は認証局によって違います。詳細は、各認証局にお問い合わせください。

1.3. 正規のサーバ証明書の保存

CAから正規のサーバ証明書を取得すると、SSLを使用することができます。これを行うには、keytoolコマンドを使用してCAから取得したサーバ証明書を、CSR作成時に使用したものと同じkeystoreファイルに読み込みます。
この作業によって、自己署名証明書から正規のサーバ証明書に置き換えられます。

使用方法:
```
keytool -import -alias [alias] -file [file.cer] -keystore [key_store]
```

[alias]
　　CSRを生成したときに選択したaliasと同じものを選択します。
[file.cer]
　　認証局からの正規の証明書のファイル名を設定します。
[key_store]
　　CSRを生成したときに選択したkey_storeと同じものを選択します。

例:

```
cd /usr/swcm/WebEdge
jre/bin/keytool -import -alias OpenTech -file file.cer ¥
                -keystore /usr/swcm/WebEdge/config_mdn/.newkeystore
```

2. WebEdgeのSSLを有効にする

WebEdge側の設定を変更しSSLを有効にします。mobility.cfgファイルの以下の設定キーを変更します。

sslEnable=true
→SSLを有効にする

sslcertFile=/usr/swcm/WebEdge/config_mdn/.newkeystore
→keystoreのディレクトリパスとファイル名を設定する

keystorePasswd=webedge
→keystoreのパスワードを設定する

sslserverPort=443
→一般用SSLサーバ機能を利用する場合のサーバポートを設定する（必要時以外は変更しないでください）

ssladminserverPort=8088
→管理者用SSLサーバ機能を利用する場合のサーバポートを設定する（必要時以外は変更しないでください）

これにより、SSLによるセキュアなアクセスが可能となります。SSLが利用可能なサーバへのURLは、"http"の代わりに"https"が使われます。

```
https://host.domain/          →一般ユーザSSL
https://host.domain:8088/      →管理者SSL
```

3. 試験的なSSLの利用

仮にあるいは、試しにSSLによるサーバ接続を利用されるということであれば、keytoolコマンドの-genkeyオプションにて作成したkeystoreファイルを、そのままWebEdgeのmobility.cfgに指定していただければ、httpsとして利用することはできます。
（もちろん、この時は「認証されていないサーバである」という由のダイアログがWebブラウザから警告されます。これを無視して「OK」すれば利用は可能です。）

注意：keytoolコマンドの-genkey指定する際のオプションとして、-keypassと-storepassがありますが、ここには同じ文字列を設定し、mobility.cfgの「keystorePasswd」キーにその文字列を設定しなければいけません。（これはWebEdgeの仕様です）

また、WebEdgeディレクトリ/config_mdn/下にはWebEdgeインストール時にインストーラが作成した.keystoreファイルもありますので、そのファイルを利用していただくこともできます。（もちろんこのキーはCAに認証されておりません）この時のkeystorePasswdは、"webedge"を指定して下さい。