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 C:¥Program Files¥WebEdge
jre¥bin¥keytool.exe -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 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 C:¥Program Files¥WebEdge
jre¥bin¥keytool.exe -certreq -alias OpenTech -file OpenTech.csr
                    -keystore 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-----
...
-----END CERTIFICATE REQUEST-----
```

から

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 -trustcacerts -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 C:¥Program Files¥WebEdge
jre¥bin¥keytool.exe -import -trustcacerts -alias OpenTech -file file.cer
                    -keystore 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=/Program Files/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。