必要なもの

・Apache(apache_1.3.29)
・OpenSSL(openssl-0.9.7c)
・mod_ssl(mod_ssl-2.8.16-1.3.29)

インストール

■ openssl のコンパイル

```
tar xvfz openssl-0.9.7c.tar.gz
cd openssl-0.9.7c
./config --prefix=/usr/local --openssldir=/usr/local/openssl -fPIC
make
```

■ mod_ssl 付きの apache のコンパイル

```
tar zxvf apache_1.3.29
tar xvfz mod_ssl-2.8.3-1.3.29.tar.gz
cd mod_ssl-2.8.3-1.3.29
./configure --with-apache=../apache_1.3.29 --with-ssl=../openssl-0.9.7c?
 --prefix=/usr/local/apache --enable-shared=ssl --enable-module=so?
 --enable-rule=SHARED_CORE --enable-module=rewrite --enable-shared=rewrite
make
make certificate
make install
```

設定

httpd.conf

・Port は通常の HTTP を 8080 から 80 に、また HTTPS を 8443 から 443 に変更
・<VertualHost> のところのサーバ名に注意

起動

start のかわりに startssl

設定方法 (自分が CA になる)

■ CA 自身の秘密鍵 ca.key の作成。

```
$ openssl genrsa -des3 -out ca.key 1024
```

■ CA 自身の証明書 ca.crt を作成。

```
$ openssl req -new -x509 -key ca.key -out ca.crt
```

```
Using configuration from /usr/local/ssl/openssl.cnf
Enter PEM pass phrase:       <--- パスフレーズ入力
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
```

```
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:JP
State or Province Name (full name) [Some-State]:Kanagawa
Locality Name (eg, city) []:Yokohama
Organization Name (eg, company) [Internet Widgits Pty Ltd]:T.I.Tech
Organizational Unit Name (eg, section) []:Sugino Laboratory
Common Name (eg, YOUR name) []:foo baar
Email Address []:foo@bar
```

■サーバ用秘密鍵 server.key の作成。

```
$ openssl genrsa -des3 -out server.key 1024
```

■サーバ証明書発行のための CSR (Certificate Signing Request) の作成。

```
$ openssl req -new -key server.key -out server.csr
```

```
Using configuration from /usr/local/ssl/openssl.cnf
Enter PEM pass phrase:       <--- パスフレーズ入力
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:JP
State or Province Name (full name) [Some-State]:Kanagawa
Locality Name (eg, city) []:Yokohama
Organization Name (eg, company) [Internet Widgits Pty Ltd]:T.I.Tech
Organizational Unit Name (eg, section) []:Sugino Laboratory
Common Name (eg, YOUR name) []:www.sgn.ip.titech.ac.jp
Email Address []:foo@bar

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:         <--- Enter
An optional company name []:     <--- Enter
```

■サーバ用証明書の発行。

この時、ca.key は ca.crt 等はこのファイル名通りでないとダメ

```
$ $SRC/mod_ssl-2.8.16-1.3.29/pkg.contrib/sign.sh server.csr
```

```
...
Certificate is to be certified until Sep 13 04:30:55 2001 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y

...
```

■コピー

SSLCertificateFile /usr/local/apache/conf/ssl.crt/server.crt

SSLCertificateKeyFile /usr/local/apache/conf/ssl.key/server.key