（参考資料としての利用に限る）

Apache 1.3+Apache-SSL CSR ファイル作成方法

1. はじめに

Apache-1.3 と Apache-SSL 環境下での、CSR 作成手順を以下に説明します。
大まかな手順は、以下のとおりです。

(1) 必要なソフトウエアの確認
(2) サーバの秘密鍵と CSR の作成
(3) CSR をジェイサートへお送りいただく
(4) 秘密鍵のバックアップを取る

2. 必要なソフトウエアと入手先

以下のソフトウエアが必要となります。
インストールされていないパッケージがある場合は、OS・ディストリビューションの用意しているパッケージ、もしくは以下を参照し、入手してインストールしてください。

名称	機能	入手先
OpenSSL	SSL ツールキット	http://www.openssl.org/ ソースをダウンロードし、コンパイルとインストールを行います。　手順も上記サイトに記載されています。
Apache-SSL	SSL 対応 patch	http://www.apache-ssl.org/ パッチをダウンロードし、下記の Apache ソースにあててコンパイルとインストールを行います。 手順も Apache のサイトとソースに含まれる Readme に記載されています。
Apache 1.3	Web サーバソフト	http://www.apache.jp/ ソースをダウンロードし、上記 patch をあて、コンパイルとインストールを行います。 手順も上記サイトと Apache-SSL ソース内 Readme に記載されています。

RedHat 系 Linux ディストリビューションの場合は、次のようにしてインストール状況を確認できます。

```
$ rpm -qa openssl apache-ssl
```

3. サーバの秘密鍵と CSR の生成

CSR(証明書署名要求）と秘密鍵を生成します。

CSR はサーバの公開鍵に署名してもらうための申請書です。

CSR を生成するために、サーバの秘密鍵を生成します。

注：秘密鍵の鍵長は 2048bit をご利用ください。

3.1 ディレクトリの設定

httpd の設定ファイルのあるディレクトリに移動し、ディレクトリを新たに作成します。以下に例を示しますが、実際の環境に読み替えてください。

```
# cd /usr/local/apache/conf
# mkdir ssl.crt ssl.csr ssl.key
```

注： 同一名のディレクトリがある場合、内容が上書きされてしまいますので、別の名前で新たにディレクトリを作成します。

3.2 CSR と秘密鍵の生成

次のコマンド・ラインで、秘密鍵（YOURSERVER.key）と CSR（YOURSERVER.csr）を同時に生成します。

秘密鍵長は 2048bit を指定してください。

YOURSERVER は例で、ファイル名は任意に付けることができます。拡張子は記載例に従ってください。

```
# openssl req -new –newkey rsa:2048 -nodes -keyout ssl.key/YOURSERVER.key -out
ssl.csr/YOURSERVER.csr
```

注： ここでは、秘密鍵を保護するパスフレーズをつけておりません。パスフレーズ付きの場合、Apache-SSL では httpdsd がうまく起動しないためです。ファイルのパーミッションに留意してください。パスフレーズで暗号化するには、

```
# openssl rsa -aes256 -in ssl.key/YOURSERVER.key -out ssl.key/YOURSERVER.key.enc
```

とするとパスフレーズが聞かれ、入力したパスフレーズで暗号化された YOURSERVER.key.enc が生成されます。

YOURSERVER.key の代わりに YOURSERVER.key.enc を利用することもできますが、サーバの再起動時にパスフレーズを答えられないと Apache が再起動しません。

3.3　CSR 生成情報の入力

ここで、CSR 生成に必要な情報を入力します。

CSR に入力された情報と「ジェイストア」にてエントリいただいた申請情報に不一致があったり、入力された情報が不正確な場合、サーバ証明書が発行できませんので、十分ご注意ください。

注：CSR 内の情報に綴り（スペル）等の誤りがあった場合には、正しい綴り（スペル）に修正して、再度 CSR を提出していただく必要がありますので、ご注意ください。

3.3.1 CSR 生成情報入力例

以下に、CSR 生成情報の入力例を示します。

Country Name (2 letter code) [GB] : JP ←文字国名（2 文字の ISO CODE）
State or Province Name (full name) [Bershire] : Tokyo←都道府県
Locality Name (eg, city) [Newbury] : Chiyoda-ku←市区町村
Organization Name (eg, company) [My Company Ltd] : J Cert, Inc.←組織名
Organizational Unit Name (eg, section) [ ] : System Administration←部署名
Common Name (eg, your name or your server's hostname) [ ] : sample.jcert.co.jp←サーバ名
Email Address[ ]:
Please enter the following 'extra' attributes to be sent with your certificate request A challenge password [ ]:
An optional company name [ ]:

3.3.2 CSR 生成情報に入力する項目

CSR 生成情報の入力には、入力項目が規定されています。以下を参照してください。

項目名	意味と入力できる値	入力例
Country Name	国名を示す英字２文字を入力します。 国名に対応した入力文字は、ISO CODE で決まっております。 日本の場合 JP になります。	JP
State or Province Name	申請組織の本店所在地の都道府県を入力します。	Tokyo
Locality Name	申請組織の本店所在地の市区町村を入力します。	Chiyoda-ku
Organization Name	申請組織の名称を入力します。	J Cert, Inc.
Organizational Unit Name	申請組織の部署名等を入力します。	System Administration
Common Name	申請するサーバ証明書のコモンネーム（一般名）を入力します。	sample.jcert.co.jp

注：次の項目は空欄で構いません。項目を空欄にするには「.」(ピリオド)を入力してください。

Email Address

A challenge password

An optional company name

3.3.3 CSR 生成情報入力に使用できる文字

CSR 生成情報入力に使用できる文字には、以下の制限があります。これを守らないと、CSR が生成できません。 入力は、全て半角で行います。**なお、コモンネームには以下の「英字」「数字」および「 - （ハイフン）」のみが利用できます。**

字種	使用できる範囲
英字、数字	大文字 A～Z　小文字 a～z　0～9
記号 スペース	'(アポストロフィ）　-（ハイフン）　,(カンマ）　=(イコール）　/（スラッシュ） ()（括弧）　.(ピリオド）　：（コロン）

4. CSR を送付

完成した CSR ファイルをテキストエディタで開き、「ジェイストア」申請画面にコピー&ペーストしてください。

以下に、CSR ファイルを開いた例を示します。

```
-----BEGIN CERTIFICATE REQUEST-----
MIIByTCCATICAQAwgYgxCzAJBgNVBAYTAkpQMQ4wDAYDVQQIEwVUb2t5bzETMBEG
A1UEBxMKQ2hpeW9kYS1rdTEaMBgGA1UEChMRQ29tb2RvIEphcGFuIEluYy4xFzAV
:
:
RFi8OQRtKDSGL9mqC4FLk/cAxcNs4X+yzUNp9jn9IldCGEtTg4aRIBFKpWTobwh6
m0jpoMYpQ8DNwO0vpjAGruzQ/ARdw/xaLmQyqaU=
-----END CERTIFICATE REQUEST-----
```

注： -----BEGIN CERTIFICATE REQUEST----- から -----END CERTIFICATE REQUEST----- までをハイフンを含めて、「ジェイストア」申請画面に貼り付けてください。 1 文字でも欠けますと、CSR ファイルフォーマットエラーとなり、サーバ証明書のお申込を受付できません。

5. 秘密鍵のバックアップ

サーバ証明書が発行されるまでに、サーバトラブルなどで、秘密鍵が失われてしまう可能性があります。秘密鍵とサーバ証明書はペアですので、秘密鍵が失われるとサーバ証明書も使用できなくなってしまいます。　これを防止するためにも、秘密鍵ファイルを別の媒体にバックアップしておきます。

バックアップの際には秘密鍵ファイルにパスフレーズを付けておくことをお勧めします。