

Coyote Point Systems
Equalizer E350/450-1U
v7 CSR 作成手順書

株式会社ネットワーク

第 1.1 版 平成 16 年 3 月 1 日

Equalizer E350/450-1U CSR 作成手順

1. はじめに

この資料は、Equalizer E350/450-1U v7 上で CSR を作成する手順について記述しています。

作成する CSR は RSA 3DES 1024bit で暗号化することを前提としています。

CSR を提出する CA によってこの暗号化をサポートしていない場合は、暗号化の鍵長や暗号化アルゴリズムを変更する必要があります。Equalizer 上で Openssl のオンラインマニュアル等を参照し、手順内容を変更して下さい。

2. CSR 作成時の注意

- パスフレーズで保護された秘密鍵を使用することはできません。パスフレーズを使用しないように鍵を生成して下さい。発行済みサーバ証明書の CSR がパスフレーズを使用する秘密鍵とペアになっている場合には、このサーバ証明書を Equalizer にインストールすることはできません。サーバで CSR を作成する場合には、パスフレーズを無効化した秘密鍵によって CSR を生成して下さい。また、サーバで生成した秘密鍵のパスフレーズを Equalizer 上で無効化することも可能です。秘密鍵を FTP で Equalizer 上にダウンロードし、下記コマンドを実行してください。

```
#openssl rsa -in key.pem -out keyout.pem
```

コマンド実行時にはパスフレーズの入力が必要です。

key.pem=作成済みのパスフレーズの必要な秘密鍵ファイル。

keyout.pem=無効化して出力する秘密鍵ファイル。任意のファイル名。

- CSR 作成の手順は、基本的に証明書を発行する CA の指定に従ってください。本手順書の内容が CA の推奨する手順と異なる場合は、本手順を遵守する必要ありません。

3. E350/450-1U で CSR を作成する手順

1. Root でログオンします。

2. 作業ディレクトリに移動します

```
#cd /tmp
```

3. 秘密鍵作成のための擬似乱数を作成します

```
#openssl md5 * > rand.dat
```

rand.dat=出力する擬似乱数。任意のファイル名。

4. 1024bit 3DES により秘密鍵を生成します

```
#openssl genrsa -rand rand.dat -des3 1024 > key.pem
```

パスフレーズの入力を求められます。任意の文字列を入力して下さい。

1024=鍵長

key.pem=パスフレーズの必要な秘密鍵。任意のファイル名。

5. パスフレーズを無効にします。

```
#openssl rsa -in key.pem -out keyout.pem
```

パスフレーズの入力を求められます。先ほどの文字列を入力して下さい。

keyout.pem=無効化して出力する秘密鍵。任意のファイル名。

6. 生成した秘密鍵によって CSR を作成します。

```
#openssl req -new -key keyout.pem -out csr.pem
```

csr.pem=出力する CSR。任意のファイル名。

CSR 作成時に証明書情報(ディステイングイッシュネーム)の問い合わせがあります。
CA に申請する情報に従って入力して下さい。

Country Name <国>
State of Province Name <都道府県名>
Locality Name <市区町村名>
Organization Name (eg, company) <正式英語組織名>
Organizational Unit Name (eg, section) <部門名>
Common Name (eg, YOUR name) <URL<FQDN>>
Email Address <管理者のメール<省略可>>
A challenge password <省略>
An optional company name <省略>
Email Address <管理者のメール<省略可>>

A challenge password、An optional company name の入力は省略して下さい。Blank で Enter。

- 作成した CSR を FTP でローカルマシンにアップロードし、CA へサーバ証明書の申請を行ってください。

HTTPS クラスタへサーバ証明書をインストールするには、CSR 作成時に用いた秘密鍵も必要です。
CSR と一緒にこの秘密鍵もローカルマシンにアップロードして下さい。

HTTPS クラスタへインストールする証明書ファイル(composite file)は、CA から発行された証明書(テキスト)と秘密鍵(テキスト)を同一テキストファイルに張り合わせたものです。

4. 参考

SSL アクセラレータ使用時に申請する証明書数に関して

証明書を発行する CA にお問い合わせ下さい。CA によって申請の際の制約が異なります。
日本 Verisign では同一 CommonName で実際のサーバ台数分の申請が必要なようです。

<http://www.verisign.co.jp/server/help/faq/100020/index.html>

(リンク切れの場合はご容赦願います)