

## Equalizer サーバ証明書インストール手順について

本資料では Equalizer SIシリーズで、HTTPSクラスタへサーバ証明書をインストールする手順について説明しています。

CSR作成の手順	P2 ~ 3
Compositeファイル作成手順	P4
Compositeファイルアップロード手順	P5 ~ 6
サーバ証明書の注意事項	P7

本資料は Equalizer E350si/450si/E550si v7.2.4e 上での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。



## CSR作成手順

\*1  
サーバ証明書を発行するには CSR を作成しCA(認証局)へ提出する必要がある、  
CSR作成はEqualizer上で行うことができます。  
CAが提示している作成手順が以下と違う場合は、そちらの手順にて  
作成を行ってください。

---

Equalizerコンソール画面へシリアルケーブル または SSH  
にてログインします。 ログインは root にて行って下さい。  
(SSH の場合はログイン後に su root を入力し root権限に切り替えます)

ディレクトリを移動します

```
# cd /tmp
```

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)

“snmpctl: Operation not supported” というエラーが出て、rand.dat が作成されていれば  
作業に問題はございません。

1024bit 3DES により秘密鍵を生成します

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

パスワード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が鍵長となります。

key.pem = パスワードの必要な秘密鍵。任意のファイル名)

パスワードを無効にする場合は下記を実行します。

(パスワードを無効にしない場合は へお進み下さい)

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

パスワード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。

生成した秘密鍵によってCSR を作成します。

でパスフレーズを無効にした場合：

```
# openssl req -new -key keyout.pem -out csr.pem
csr.pem = 出力するCSR。任意のファイル名
```

でパスフレーズを無効にしない場合：

```
# openssl req new key key.pem out csr.pem
csr.pem = 出力するCSR。任意のファイル名
# Enter pass phrase for key.pem:
(4 で入力したパスフレーズを入力します)
```

証明書情報(ディスティングイッシュネーム)を入力します。  
CA に申請する情報を入力して下さい。

(例)

Country Name <国>	: JP
State or Province Name <都道府県名>	: Tokyo
Locality Name <市区町村名>	: Chiyoda-ku
Organization Name (eg, company) <正式英語組織名>	: Example Inc.,
Organizational Unit Name (eg, section) <部門名>	: System 1
Common Name (eg, YOUR name) <URL<FQDN>>	: www.example.com
Email Address <管理者のメール<省略可>>	

A challenge password <省略>

An optional company name <省略>

A challenge password、An optional company name の入力は省略して下さい。  
何も入力せずEnterキーを押し決定します。

Equalizer上から FTPコマンドを使用し、作成したCSR および 秘密鍵 を外部へ転送します。

上記CSR を元に、CAへサーバ証明書の発行を申請します。

必要な証明書の枚数などは CAにより異なりますので、申請先CAへ直接お問い合わせ下さい。

## Compositeファイル 作成手順

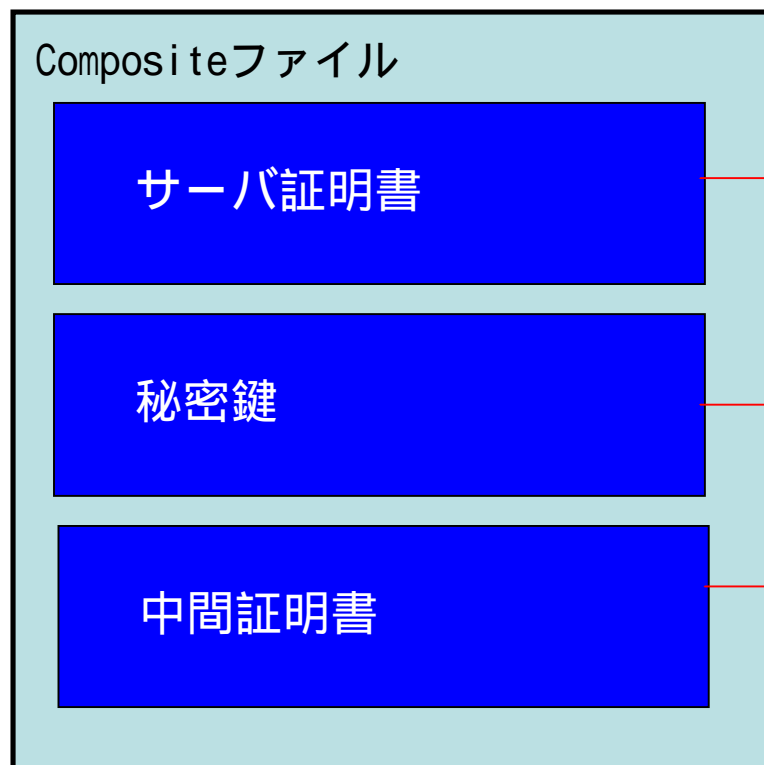
Equalizerへアップロードするファイルは Compositeファイル と呼ばれます。

これは

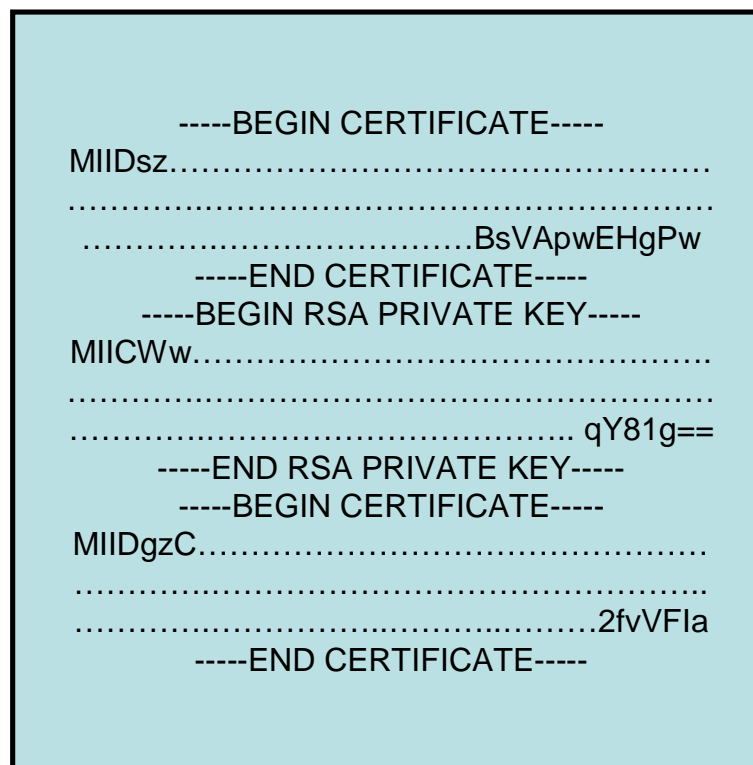
- ・ CA より発行されたサーバ証明書
- ・ 秘密鍵
- ・ 中間証明書

の3点を順にあわせたテキスト形式ファイルです。  
拡張子 “.pem” にて保存します。

### イメージ図

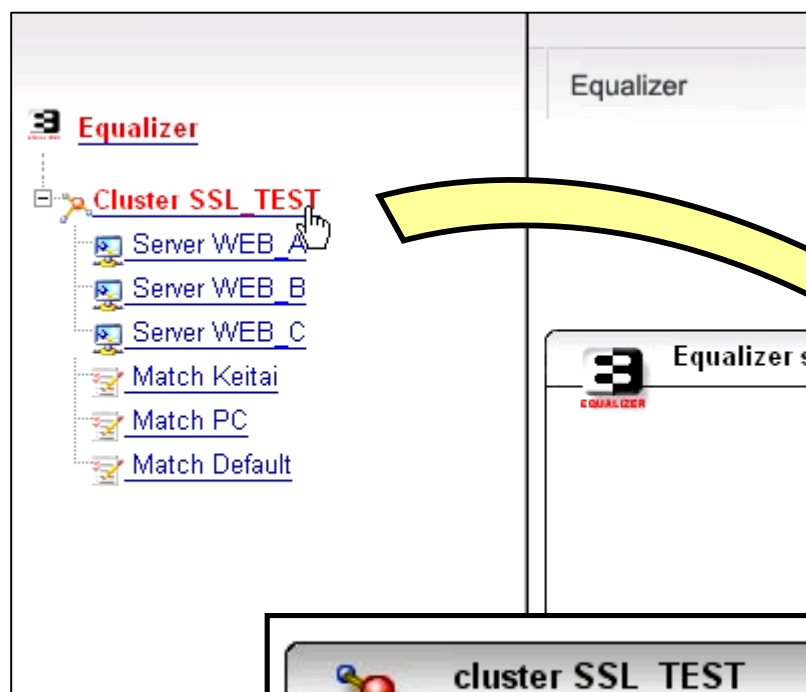


### 実際のファイル



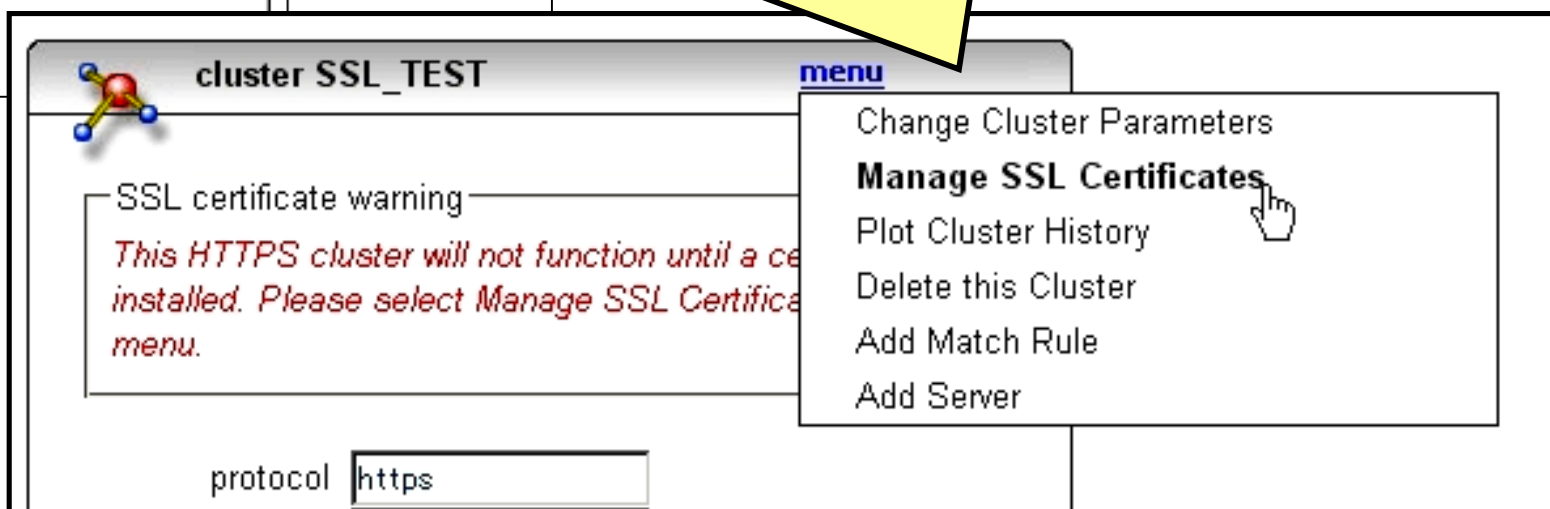
## Compositeファイル アップロード手順

Compositeファイル は EqualizerのWeb管理画面からアップロードします。  
ブラウザから ユーザ touch にて Equalizerへログインして下さい。



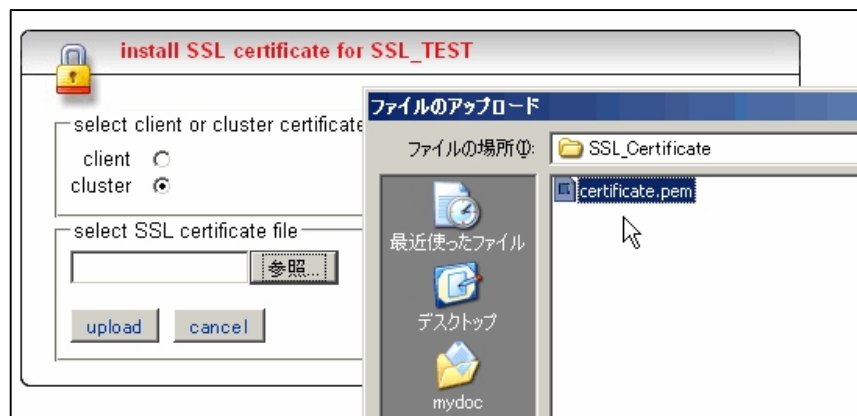
画面左のリストから、HTTPSクラスタを選択します。  
サーバ証明書が無い状態では、赤色で表示されます。

表示された画面の menu から “Manage SSL Certificates”  
を選択します。



下記のように“参照”ボタンが表示されますので、ローカルPC上から Compositeファイルを選択し、“upload” ボタンを押します。画面が切り替わり、反映されます。画面左リストのクラスタ名が緑色で表示されていることをご確認下さい。

CSR作成時にパスフレーズを有効にした場合は、このアップロード時にパスフレーズ入力画面が表示されます。



cluster SSL certificate chain details for SSL_TEST - 2 certificates found	
certificate 1	
serial number	0
keylength	1024
issuer	/C=JP/ST=Tokyo/L=Kanda/O=yellow
subject	/C=JP/ST=Tokyo/L=Kanda/O=yellow
valid from	Feb 14 14:18:57 2008 GMT
valid till	Feb 13 14:18:57 2009 GMT
certificate 2	
serial number	254B8A853842CCE358F8C5DDAE22f
keylength	1024
issuer	/C=US/O=VeriSign, Inc./OU=Class 3
subject	/O=VeriSign Trust Network/OU=Veri
valid from	Apr 17 00:00:00 1997 GMT
valid till	Oct 24 23:59:59 2011 GMT

クラスタ内のサーバ証明書情報を確認すると、左のように Certificate が反映されています。

Certificate 1 がサーバ証明書  
Certificate 2 が中間証明書 となります。

証明書の内容や、有効期限なども確認可能です。

## ！ サーバ証明書に関する注意事項 ！

HA構成の場合、サーバ証明書情報は両機器間にて共有されない為、**Primary/Backup 両方にアップロードする必要があります。**

機器のコンフィグ情報である「バックアップファイル」には**アップロードしたサーバ証明書の情報はセキュリティの観点から含まれません。**

Xcelカードを使用している場合は、秘密鍵は同様の理由でXcelカード内に格納されているため、**Web管理画面・コンソール画面から秘密鍵情報を参照することは出来ません。**

ハードウェア故障などで、機器交換を行った場合は「バックアップファイル」にて設定をリストアした後、**サーバ証明書を再度アップロードする必要があります。**