（参考資料としての利用に限る）

OpenSSL によるサーバ証明書および秘密鍵の形式変換（PKCS#12/PEM 形式）

1. はじめに。

(ア) PKCS #12 形式は、**IIS/Windows Server において**

① 秘密鍵のバックアップを行う場合、あるいは

② サーバ証明書を秘密鍵とともにその他サーバへエクスポートする場合、あるいは

③ CSR（秘密鍵）の新規生成に拠らず、その他サーバで稼働しているサーバ証明書を秘密鍵とともに IIS にインポートする場合、

に用いられる、秘密鍵と証明書を 1 つのファイルに格納する形式です。

(イ) PEM 形式は、**apache/apache 互換サーバソフトウェアにおいて**サーバ証明書の設定時や秘密鍵のバックアップを行う場合に使用されるファイル形式で、秘密鍵、サーバ証明書、中間証明書（認証局証明書）それぞれ個別に（あるいは連結して）取り扱うことができます。

(ウ) OpenSSL を利用することで、PKCS #12 形式ファイルと PEM 形式ファイルの相互変換を行うことが可能ですので、

① **ホスティング事業者の変更時など**、異なるソフトウェア（IIS/apache）のサーバへのサーバ証明書の移設、あるいは

② **マルチドメイン証明書やワイルドカード証明書の異なるソフトウェア（IIS/apache）のサーバ間での共用**、あるいは

③ **IIS 上で稼働中のマルチドメイン証明書の付帯ドメイン追加時など**、サーバ証明書と秘密鍵の組み合わせの変更、

を行う場合に有効です。

2. **PKCS #12 形式のファイルから、PEM 形式でサーバ証明書と秘密鍵を取り出すには。**（以下、ファイル名はお客様の環境に合わせ読み換えてご参照ください。）

(ア) 下記コマンドにより、**PKCS #12 ファイル sample.p12 から秘密鍵だけを取り出し、暗号化せずに sample.key に保存します。**（IIS でエクスポート時に登録したパスワードが必要です。）

注：ここでは、秘密鍵を暗号化せずに保存します。　サーバ機再起動時などに **Apache** をスムースに起動させるためです。ファイルのパーミッションに留意してください。　セキュリティーに不安を感じられる場合には、"-nodes"を削除することで秘密鍵を暗号化して保存することもできます。　**ただし、サーバの再起動時にパスフレーズを答えられないと Apache が起動しませんのでご注意ください。**

```
$ openssl pkcs12 -in sample.p12 -nocerts -nodes -out sample.key
```

注：保存した sample.key ファイルをそのまま使用できない場合
"-----BEGIN RSA PRIVATE KEY-----"の行から"-----END RSA PRIVATE KEY-----" までの行を、ハイフンを含めて.txt にて保存し使用ください。

(イ) 下記コマンドにより、**PKCS #12 ファイル sample.p12 からサーバ証明書のみを取り出し、sample.crt に保存します。**

```
$ openssl pkcs12 -in sample.p12 -clcerts -nokeys -out sample.crt
```

注：保存した sample.crt ファイルをそのまま使用できない場合、
"-----BEGIN CERTIFICATE-----"の行から"-----END CERTIFICATE-----" までの行を、ハイフンを含めて.txt にて保存し使用ください。

(ウ) 下記コマンドにより、**PKCS #12 ファイル sample.pfx から中間 CA 証明書のみを取り出し、sample.ca-bundle に保存します。**（中間 CA 証明書が無い場合、**sample.ca-bundle** は空ファイルになります。）

```
$ openssl pkcs12 -in sample.pfx -cacerts -nokeys -out sample.ca-bundle
```

注：保存した sample.ca-bundle ファイルをそのまま使用できない場合、
"-----BEGIN CERTIFICATE-----"の行から"-----END CERTIFICATE-----" までの行を、ハイフンを含めて.txt にて保存し使用ください。

3. **PEM 形式サーバ証明書と秘密鍵から PKCS #12 形式のファイルを作り出すには。**（以下、ファイル名はお客様の環境に合わせ読み換えてご参照ください。）

(ア) 下記コマンドにより、**サーバ証明書 sample.crt と秘密鍵 sample.key から PKCS #12 ファイル sample.pfx**（拡張子は **.p12** でも可）を作成します。（保護パスワードを設定してください -このパスワードは **IIS** にインポートする際に必要です。）

```
$ openssl pkcs12 -export -in sample.crt -inkey sample.key -out sample.pfx
```

(イ) 下記コマンドにより、**サーバ証明書 sample.crt と秘密鍵 sample.key、更には CA 証明書 sample.ca-bundle （ルート証明書+中間証明書）を同梱して、一つの PKCS #12 ファイル sample.pfx（拡張子は .p12 でも可） を作成することもできます。**（保護パスワードを設定してください-このパスワードは **IIS** にインポートする際に必要です。）

```
$ openssl pkcs12 -export -in sample.crt -inkey sample.key -certfile sample.ca-bundle -out sample.pfx
```

（注）**中間+ルート証明書バンドルファイルは、以下リンク先の「証明書を設定する前に（準備作業）」をご一読頂き、”sf_bundle-g2.crt”を中間証明書一覧から取得しサーバ上で sample.ca-bundle と名称変更し保存**してください。
https://www.jcert.co.jp/support/certificate/

※ 証明書ファイル名は選択ルート（Starfield あるいは Go Daddy）およびお客様環境に即し、読み替えてください。