

(参考資料としての利用に限る)

Apache 2.x+mod_ssl サーバ証明書インストール方法

1. はじめに

Apache-2.x と Mod-SSL 環境下での、サーバ証明書インストール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) 証明書の受理とインストール準備
- (2) 環境設定と動作確認
- (3) 秘密鍵と証明書のバックアップ

ディレクトリ等は、セットアップされる環境に合わせて読み替えてください。

2. 証明書の受理とインストール準備

証明書が発行されますと、お客様のサーバ証明書 (エンド証明書) が添付ファイルとしてメールにて送信されますので、名前をつけて保存します。

2.1 お客様のサーバ証明書の受理と保存

お客様のサーバ証明書は、発行時のメールに添付されていますので、名前をつけて保存します。
仮にファイル名は YOURSERVER.crt とします。

2.2 中間 CA 証明書の受理と保存

サーバ証明書を使用するには、中間 CA 証明書が必要になります。

中間 CA 証明書は、「証明書を設定する前に (準備作業)」をご一読頂き、中間証明書一覧から取得してください。 <https://www.jcert.co.jp/support/certificate.html>

保存した中間 CA 証明書のファイル名を仮に YOURSERVER.ca-bundle (拡張子は、.cert のままでも構いませんが、その場合後述 3.1.1 でのパスの設定も同様に設定してください) へと変更します。

3. 環境設定と動作確認

環境設定ファイルを書き換え、必要なファイルをコピーし、動作確認を行います。

注：ファイルの内容を書き換える前に、バックアップを取っておくことをお勧めします。

3.1 httpd-ssl.conf の設定

httpd-ssl.conf の設定を書き換えるため、ディレクトリを移動し、バックアップを取得します。
その後 httpd-ssl.conf の設定ファイルの書き換えを行います。

(移動処理)

```
cd /usr/local/apache2/conf/extra
```

(バックアップ取得)

```
# cp -p httpd-ssl.conf httpd-ssl.conf.back
```

(設定ファイルの書き換え)

```
# vi httpd-ssl.conf
```

3.1.1 証明書ファイルの指定

上記で開いたファイルの以下の行を、秘密鍵 (YOURSERVER.key)、お客様のサーバ証明書 (YOURSERVER.crt)、中間 CA 証明書 (YOURSERVER.ca-bundle) のインストール先にあわせて、以下のよう書き換えます。

```
SSLCertificateFile /usr/local/apache2/conf/ssl.crt/YOURSERVER.crt
```

```
SSLCertificateKeyFile /usr/local/apache2/conf/ssl.key/YOURSERVER.key
```

```
SSLCertificateChainFile /usr/local/apache2/conf/ssl.crt/YOURSERVER.ca-bundle
```

注： **apache2.4.8** 以降では、中間証明書ファイルを指定する **SSLCertificateChainFile** ディレクティブが無くなっており、お客様のサーバ証明書と中間証明書をテキスト形式で同梱して **YOURSERVER.crt** を新たに生成し (生成方法は欄外ご参照) **SSLCertificateFile** ディレクティブに設定してください。

この際、中間証明書は 以下から **SHA-2** 用 **bundle_apache248b.txt** を取得して下さい。

<https://www.jcert.co.jp/support/certificate.html>

3.1.2 SSL Virtual Host の設定

SSL Virtual Host 設定の次の行を、コモンネーム (FQDN) に合わせて書き換えます。 **443** はポート番号を示します。

以下の例ではコモンネーム (FQDN) は **sample.jcert.co.jp** となっております。実際の環境に読み替えて設定してください。

```
ServerName sample.jcert.co.jp:443
```

3.2 ファイルのコピー

2 で保存したお客様のサーバ証明書 (YOURSERVER.crt) と、中間 CA 証明書 (YOURSERVER.ca-bundle)、また CSR 作成時に使用した秘密鍵 (YOURSERVER.key) を、上記環境設定に示したディレクトリにコピーします。

3.3 Apache の再起動

以下のコマンドで、Apache を再起動させます。

注：お客様の環境によってはコマンドが異なる場合があります。

```
/usr/local/apache2/bin/apachectl stop
```

```
/usr/local/apache2/bin/apachectl startssl
```

以上で、サーバ証明書のインストールは完了です。

3.4 動作確認

Web ブラウザから、証明書を設定した URL へアクセスし、SSL が正しく動作していることを確認します。

4. 証明書と秘密鍵のバックアップ

万一のサーバトラブルによる再設定や、ハード更新時の再インストールに備えて、サーバ証明書と秘密鍵をバックアップしておきます。

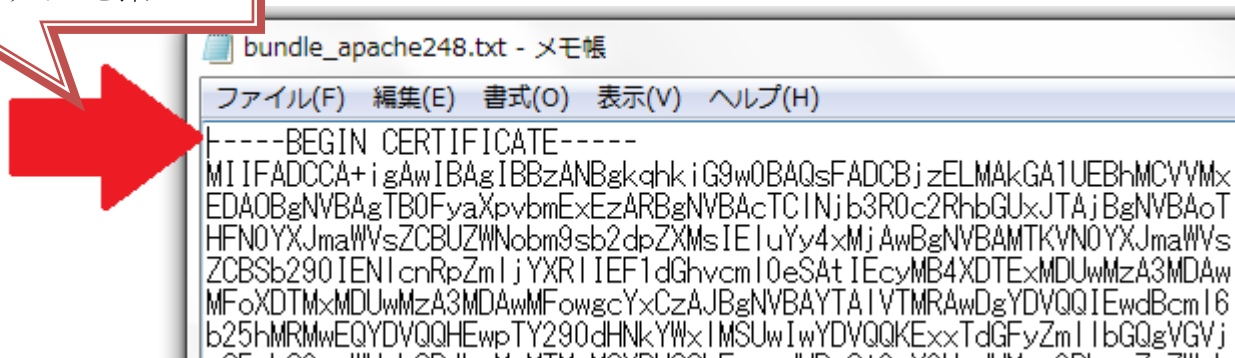
https://www.jcert.co.jp/support/pdf/faq3/OpenSSL_PKCS.pdf

バックアップするファイルは、お客様のサーバ証明書 (YOURSERVER.crt) と、秘密鍵 (YOURSERVER.key) です。 バックアップファイルは、書き換え不可能なメディアに書き込み、厳重に管理してください。

【ご参考】

お客様のサーバ証明書と中間証明書をテキスト形式で同梱して **YOURSERVER.crt** を新たに生成するには、それぞれの証明書ファイルの拡張子を **.txt** に変換し、お客様証明書ファイル (最上階層) + 中間証明書ファイル (それより下階層に - **SHA-2** 限定中間証明書+**SHA-2** ルート証明書の **2** 階層の同梱ファイルとなっております) としてテキストファイル上で **3** 階層に連結のうえ、**YOURSERVER.crt** 名にて保存してください。

ここで改行してお客様証明書ファイルを挿入！



```
bundle_apache248.txt - メモ帳
ファイル(F) 編集(E) 書式(O) 表示(V) ヘルプ(H)
-----BEGIN CERTIFICATE-----
MIIFADCCA+i_gAwIBAgIBBzANBgkqhkiG9w0BAQsFADCBjzELMAkGA1UEBhMCVVMx
EDAQBgNVBAgTB0FyaXpvbmlExZARBgNVBAcTCiNjb3R0c2RhbGUxJTAjBgNVBAoT
HFNOYXJmaWVsZCB1ZWNobm9sb2dpZXMsIEIuYy4xMjAwBgNVBAMTKVNOYXJmaWVs
ZCB1ZWNobm9sb2dpZXMsIEIuYy4xMjAwBgNVBAYTAiVTRMRwYwDgYDZQQIEwdBcmI6
b25hMRMwEQYDZQQHEwpTY290dHNkYWxIMSUwIwYDZQQKExxTdGFyZmIibGQgVGZj
b25hMRMwEQYDZQQHEwpTY290dHNkYWxIMSUwIwYDZQQKExxTdGFyZmIibGQgVGZj
```

【注意】 連結した3階層の証明書ファイルの頭部と末尾のハイフン (5個ずつ) の前後には 一切スペースや改行が入らないように、保存してください！

(補足資料)

Apache 1 枚の証明書の複数サイトでの利用方法

1. はじめに

Apache 環境下において、同一サーバ上で、かつ 1 個の IP アドレス配下で、ワイルドカード証明書やマルチドメイン証明書など 1 枚の証明書を複数のサイトで利用する場合の設定方法について、以下に説明します。

2. 設定方法

以下の例では、既に <https://sample.jcert.co.jp/> というサイトの設定が有効であり、同じワイルドカード証明書やマルチドメイン証明書を用いて、同一サーバ上に <https://www.jcert.co.jp/> というサイトを追加運用する方法を説明します。

当該ワイルドカード証明書やマルチドメイン証明書のインストールに関しましては、別途 <https://www.jcert.co.jp/support/certificate.html> に記載のマニュアルを参照下さい。

また、設定値は適宜環境に合わせて読み替えてください。

2.1 NameVirtualHost の設定

<https://sample.jcert.co.jp/> の VirtualHost の設定より前に NameVirtualHost の設定を追加します。

```
NameVirtualHost *:443
```

: 1 台のサーバに複数の IP アドレスが割り当てられている場合には、* の代わりに複数サイトの https 通信で共有する特定の IP アドレスを指定してください。

2.2 <https://sample.jcert.co.jp/> の設定

<https://sample.jcert.co.jp/> の VirtualHost の設定を確認し、

```
<VirtualHost _default_:443>
```

となっている場合は

```
<VirtualHost *:443>
```

と `_default_` を `*` へ変更します。

: 1 台のサーバに複数の IP アドレスが割り当てられている場合には、* の代わりに複数サイトの https 通信で共有する特定の IP アドレスを指定してください。

2.3 <https://www.jcert.co.jp/> の設定

<https://sample.jcert.co.jp/> の VirtualHost の設定よりも後に (</VirtualHost> で閉じた後に)
<https://www.jcert.co.jp/> 用の VirtualHost の設定をします。

```
<VirtualHost *:443>  
DocumentRoot "/a/path/to/wwwdocs"  
ServerName www.jcert.co.jp:443  
(以下略)  
</VirtualHost>
```

2.4 更にサイトを追加する場合

同じ証明書で運用するサイトを更に追加したい場合には、**2.3** と同様の手順で必要な数だけ
VirtualHost の設定を追記下さい。

2.5 再起動

インストール時と同様の方法で再起動してください。

この文書に記載されている情報は予告なしに変更されることがあります。この文書に記載されている情報に従ってユーザーが操作を行った結果、ユーザーが被る損害については、ジェイサートでは一切責任を負いません。ユーザーは自己責任においてのみ、この文書を使用するものとします。
