（参考資料としての利用に限る）

Nginx+openssl サーバ証明書インストール方法

1. はじめに

Nginx+openssl 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が、必要に応じ**提供元の詳細情報**もご参照ください。
http://nginx.org/ja/docs/http/configuring_https_servers.html

(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（**bundle.crt**）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/

保存した中間 CA 証明書のファイル名を仮に YOURSERVER_ca-bundle.crt 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 Nginx 設定用証明書ファイルの生成

お客様のサーバ証明書（**YOURSERVER.crt**）と中間 **CA** 証明書（**YOURSERVER_ca-bundle.crt**）を連結した（連結順序は必ずサーバ証明書**->**中間 **CA** 証明書）ものを設定ファイルのあるディレクトリに置きます。

```
# cat YOURSERVER.crt YOURSERVER_ca-bundle.crt >
 /usr/local/nginx/conf/YOURSERVER.pem
```

3.2 nginx.conf の設定

nginx.conf の設定を書き換えるため、ディレクトリを移動します。

```
# vi /usr/local/nginx/conf/nginx.conf
```

3.2.1 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）、3.1 で連結生成したファイル（YOURSERVER.pem）のインストール先にあわせて、以下のように書き換えます。

```
http{
  (中略)
   server {
       listen       443;

       ssl                  on;
       ssl_certificate      YOURSERVER.pem;
       ssl_certificate_key  YOURSERVER.key;

       ssl_session_timeout  5m;

       ssl_protocols  SSLv3 TLSv1;
       ssl_ciphers  ALL:!EXP:!ADH:!LOW:!SSLv2:!MD5;
    }
}
```

3.3 Nginx の再起動

以下のコマンドで、Nginx 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/nginx/sbin/nginx -s stop
/usr/local/nginx/sbin/nginx
```

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。

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。