

(参考資料としての利用に限る)

Ngix+openssl サーバ証明書インストール方法

1. はじめに

Ngix+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 証明書は、よくある質問「証明書のインストール方法」の案内に従い、レポジトリから取得してください。<http://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** 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）を連結した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 > YOURSERVER.pem
```

（ファイルの結合後、元のファイルは削除いただいて結構です。）

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.pemt）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。

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。