



JPRS サーバー証明書発行サービス

サーバー証明書 インストール手順 (nginx 新規/更新)

Version 1.1

株式会社日本レジストリサービス (JPRS)

更新履歴

日付	Version	
2016/07/29	1.0	初版リリース
2026/04/28	1.1	クロスルート証明書の手順追記

以下の

- ssl_certificate
- ssl_certificate_key

等の指定は nginx の設定ファイルの中にあります。**既定の設定ファイルの名前は、**

「nginx.conf」であり、nginx のインストール先直下の「conf/」ディレクトリにあります。

設定ファイルでは、「#」文字で行内コメントが始まります。以下で使用する各種の指定の左に「#」文字のないことを確認してください。

1 事前準備

1.1 中間 CA 証明書とクロスルート証明書のダウンロード

以下より中間 CA 証明書とクロスルート証明書をダウンロードし、保存してください。

■ 中間 CA 証明書について

<https://jprs.jp/pubcert/info/intermediate/>

1.2 サーバー証明書のダウンロード

1.2.1 JPRS から送付される場合

JPRS から送付されるメール「サーバー証明書ダウンロード手続きのご案内[FQDN]」に記載されている URL より証明書をダウンロードしてください。

1.2.2 指定事業者から提供される場合

それぞれの事業者の指定する方法にてダウンロードしてください。

※詳細はサーバー証明書を購入した指定事業者にお問合せください。

2 証明書インストール

設定ファイルの「ssl_certificate」に指定するパス名のファイルに、2枚の証明書をつないで保存します。

この手順では、例として設定ファイルの「ssl_certificate」に以下と設定することを前提としています。「/pathname/of」は実際のパス名に読み替えてください。

例) 「ssl_certificate」に「**/pathname/of/combined.crt**」と設定

2.1 サーバー証明書と中間 CA 証明書の二つを一つのファイルにつなぐ

次のコマンドを入力し、ダウンロードしたサーバー証明書(例: exsample.cer)と中間 CA 証明書(例: JPRS_OVCA.cer)の二つのファイルを一つにつないでください。

※ダウンロードしたファイルは、現在作業中のディレクトリにあるものとします。

コマンド例:

```
# cat exsample.cer JPRS.cer tlsruarootca2024cross-pem.cer > /pathname/of/combined.crt
```

「exsample.cer」: サーバー証明書のパス名

「JPRS.cer」: 中間 CA 証明書のパス名

「/pathname/of/combined.crt」: 設定ファイルの「ssl_certificate」に指定したパス名

※相対パス名を指定すると、nginx のインストール先ディレクトリ直下の「conf/」ディレクトリからの相対パス名とみなされます

以上で証明書のインストールは完了です。

3 鍵ペアのインストール

設定ファイルの「ssl_certificate_key」で指定するパス名のファイルに、鍵ペアのファイルを移動していただきます。

この手順では、例として設定ファイルの「ssl_certificate_key」に以下と設定することを前提としています。

例) 「ssl_certificate_key」に「**/pathname/of/server.key**」と設定

3.1 鍵ペアファイルの移動

サーバー証明書に対応する鍵ペアのファイルを、指定したパス名に移動させます。

※servername.key (お申込み時に生成した鍵ペアファイル) は、現在作業中のディレクトリにあるものとします。

コマンド例 : `# mv -i servername.key /pathname/of/server.key`

※注意 : シェルのプロンプトの前に別なプロンプトが出た場合は、既存ファイルに対する上書きの可能性がありますので、パス名を確認してください。

以上で鍵ペアのインストールは完了です。

4 SSL/TLS の有効化

ウェブ・サーバーに SSL/TLS を有効にするための作業をします。SSL/TLS を設定済みであれば、以降で説明するように設定されているかどうかをご確認ください。

4.1 SSL/TLS の有効化

SSL/TLS を有効にするため、設定ファイルに次のように指定してください。

指定例 :

```
listen 443 ssl;
server_name www.example.jp;
#ssl on;
ssl_certificate /pathname/of/combined.crt;
ssl_certificate_key /pathname/of/server.key;
ssl_session_timeout 5m;
#ssl_protocols TLSv1;
```

「443」 : (https で) サーバーの待ち受けるポート番号

「ssl」 : https の指定です。1.0.4 版以前では省いてください

「ssl on;」 : https の古い指定です。1.0.4 版以前ではコメント文字(#)を外してください

「www.example.jp」 : 証明書のコモン・ネーム (CN) の値。

「/pathname/of/combined.crt」 : 「証明書のインストール」 でインストールした証明書のパス名

「/pathname/of/server.key」 : 「鍵ペアのインストール」 でインストールした鍵ペアのパス名

「ssl_protocols TLSv1;」 : プロトコルの古い指定で、1.5.4 版以降では、指定は不要です。1.5.3 版以前ではコメント文字(#)を外してください。

以上で SSL/TLS の有効化は完了です。

nginx における注意点

1.7.3 より古い nginx では、鍵ペアをパス・フレーズで保護できません。鍵ペアのファイルは、持ち主以外には読み書きもアクセスもできないディレクトリーに置くことを推奨します。

セキュリティホールとなるため「ssl_protocols」に「SSLv2」を指定しないでください。

1.1.13 以降の 1.1 系や、1.0.12 以降の 1.0 系では、「ssl_protocols」に「TLSv1.1 TLSv1.2」を追加で指定し、TLS1.1/TLS1.2 を有効にできます

1.13.0 以降では、OpenSSL のバージョンなどにより、「ssl_protocols」に「 TLSv1.3」を追加で指定できることがあります。

5 サーバードプロセスの再起動

サーバードプロセスをいったん停止した後、再起動してください。

もし起動していなければ、5-2.のようにサーバードプロセスを起動してください。

5.1 サーバードプロセスの停止

停止コマンド `# /NGINX_HOME/sbin/nginx -s stop`

「/NGINX_HOME」 : nginx のインストール先ディレクトリ

5.2 サーバードプロセスの再開

再開コマンド `# /NGINX_HOME/sbin/nginx`

「/NGINX_HOME」 : nginx のインストール先ディレクトリ

注意:待ち受けるポート番号によっては、スーパーユーザー特権が**不要**な場合もあります。

以上でサーバード・プロセスの再起動の完了です。

証明書のインストールは、以上で完了です。