nginx
CSR作成/証明書インストール手順書

サイバートラスト株式会社

2025年06月01日

【！】本手順書をご利用の前に必ずお読みください

1. 本ドキュメントは、「Linux OS」「nginx」の環境下でCSRの作成、およびサイバートラストのSSLサーバー証明書をインストールする手順について解説するドキュメントです。本手順は、「CentOS 6.3」「nginx 1.6.2」「OpenSSL 1.0.2k」の環境下で動作確認をしており、nginxおよびOpenSSLの設定がすでに完了し、単独での動作確認ができている事を前提としております。
2. 実際の手順はお客様の環境により異なる場合があり、nginxの動作を保証するものではございません。あらかじめご了承ください。
3. なお、このドキュメントは予告なく変更される場合があり、サイバートラスト株式会社はその内容に対して責任を負うものではありません。また、このドキュメント内に誤りがあった場合、サイバートラスト株式会社は一切の責任を負いません。
4. このドキュメントの一部または全部を複製することは禁じられており、提供または製造を目的として使用することはできません。ただし、サイバートラスト株式会社との契約または同意文書で定められている場合に限り、この注記の添付を条件として複製することができます。

目次

1. 秘密鍵ファイル/CSRの作成の前に

- CSRの作成にあたり、以下の弊社Webサイトもご参照ください。
  https://www.cybertrust.co.jp/ssl/support/csr.html
- 証明書の更新の際はセキュリティ上の観点により、秘密鍵ファイルとCSRを作り直すことを
  おすすめいたします。
- お客様の環境によりファイルやパスが異なりますので、環境に合わせてお読み替えください。
- カレントディレクトリは任意のディレクトリとなります。本例では各ファイルの保存用ディレクトリ
- 「ssl_certs」を作成しています。
- 既存ファイルと同名で作成した場合、既存のファイルへ新しいファイルが上書きされますので、
  別名をご指定ください。
- 本手順では、下記の設定を例としてご案内しております。

項目	ファイル名
サーバールート	/etc/nginx
秘密鍵ファイル・証明書ファイル 保存ディレクトリ	/etc/nginx/ssl_certs
SSL設定ファイル　保存ディレクトリ	/etc/nginx/conf.d/example_ssl.conf
証明書ファイル名	certs.pem
秘密鍵ファイル名	server.key
CSRファイル名	server.csr

2. 秘密鍵ファイルの作成

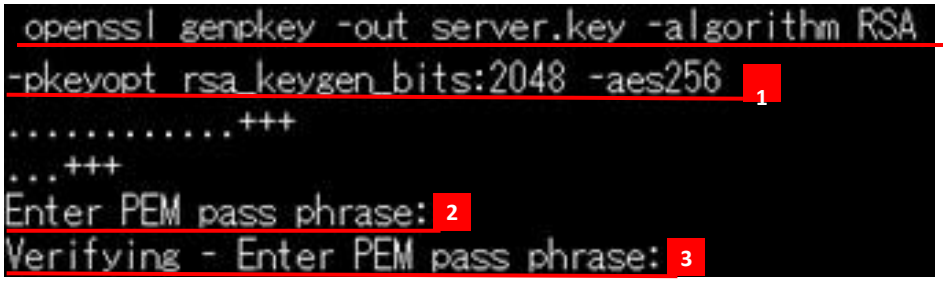
秘密鍵ファイルを作成します。

1. 以下のコマンドを実行し、秘密鍵ファイルを作成します。

   openssl genpkey -out “秘密鍵ファイル名”
   -algorithm RSA -pkeyopt rsa_keygen_bits:“公開鍵長”
   -”暗号化方式”

   ※暗号方式「AES256」、公開鍵長「2048 bit」の秘密鍵ファイル「server.key」を作成する例

   openssl genpkey -out server.key -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -aes256



2. 秘密鍵ファイルのパスフレーズとして、任意の文字列を入力します。

3. 2.で入力したパスフレーズを再入力します。

以上で、秘密鍵ファイルの作成は完了です。カレントディレクトリに秘密鍵が保存されます。

3. CSRの作成

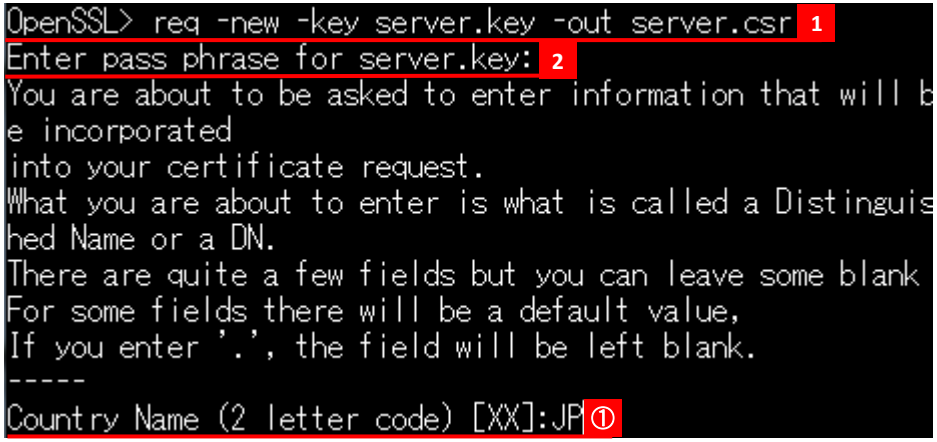
CSRを作成します。

1. 以下のコマンドを実行し、秘密鍵ファイルからCSRを作成します。

   openssl req -new -key “秘密鍵ファイル名” -out “CSR名”

   ※秘密鍵ファイル「server.key」でCSR「server.csr」を作成する例

   openssl req -new -key server.key –out server.csr



2. 秘密鍵ファイルを作成した際のパスフレーズを入力します。

3. DN情報を入力します。
   ① Country Name（2 letter code）
   「JP」と入力します。

3. CSRの作成

② State or Province Name（full name）
入力必須項目です。
申請組織の都道府県を入力します。

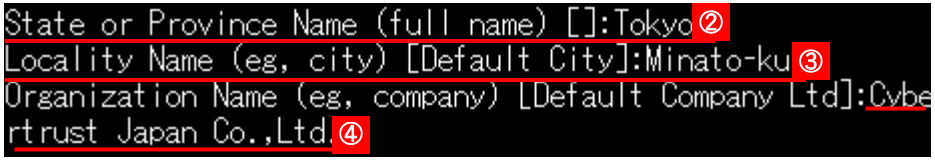
例）Tokyo

③ Locality Name（eg, city）
入力必須項目です。
申請組織の市町村を入力します。
(東京 23 区は区名)

例）Minato-ku

④ Organization Name（eg, company）
入力必須項目です。
申請組織の英訳名を入力します。

例）Cybertrust Japan Co.,Ltd.



3. CSRの作成

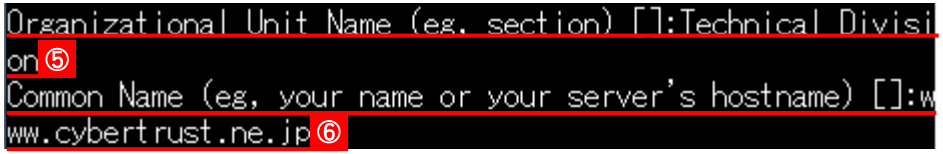
⑤ Organization Unit Name（eg, section）
任意入力項目です。
申請組織の部署名などを入力します。

例）Technical Division

※不要の場合は、何も入力せずにエンターキーを押してください。
※2022年6月23日以降に発行されるサーバー証明書には含まれません。

⑥ Common Name（eg, your name or your server’s hostname）
入力必須項目です。
申請するFQDNを入力します。

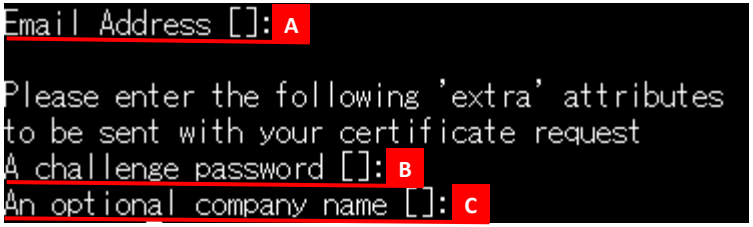
例）www.cybertrust.ne.jp



3. CSRの作成

⑦ 以下の項目は入力不要のため、何も入力せずにエンターキーを押して進んでください。

A) Email Address
B) A challenge password
C) An optional company name



以上で、CSRの作成は完了です。カレントディレクトリにCSRが保存されます。

4. 証明書のお申し込み

作成した CSR をテキストエディタで開いてコピーし、WEB の申請サイト（ SureBoard / SureHandsOn ）の申請フォームへ貼り付けて、弊社へお申し込みください。

＜CSRサンプル＞

```
-----BEGIN CERTIFICATE REQUEST-----
.....
MIIEhDCCA2wCAQAwgYkxCzAJBgNVBAYTAkpQMQ4wDAYDVQQIDAVUb2t5bzESMBAG
A1UEBwwJTWluYXRvLWt1MSIwIAYDVQQKDBlDeWJlcnRydXN0IEphcGFuIENvLixM
dGQuMRIwEAYDVQQLDAlUZXN0IFVuaXQxHjAcBgNVBAMMFXRlc3QuY3liZXJ0cnVz
2t/rD9fTPgo7u4aYzw4BpnAqLmGgy3XpsvCo6f4ROcFsgrk05FgeUCaeDFyllEST
.....
-----END CERTIFICATE REQUEST-----
```

※「-----BEGIN NEW CERTIFICATE REQUEST ---- 」から、
「-----END NEW CERTIFICATE REQUEST-----」までをハイフンを含め、すべてコピーし申請画面に貼り付けてください。

※1文字でも欠けると正しく解析できませんのでご注意ください。

5. 証明書のダウンロード

証明書が発行されましたら、サーバー証明書と中間CA証明書を事前にダウンロードします。

- 中間CA証明書のダウンロード
  - サーバー証明書をご利用の際、お使いの機器へ中間CA証明書のインストールが必要となります。
  - ご選択いただいた商品により必要な証明書が異なりますので、証明書の種類をご確認のうえ、以下弊社ホームページからダウンロードしてください。

    ▼ルート・中間CA証明書のダウンロード

    https://www.cybertrust.ne.jp/ssl/download-ca/
  - また、ご利用商品や必要な証明書の種類がご不明の場合は、以下をご覧ください。

    ▼どの中間CA証明書をダウンロードすればよいですか？

    https://www.cybertrust.co.jp/ssl/support/faq/tmxwjqz2p3bq.html

5. 証明書のダウンロード

- サーバー証明書のダウンロード
  - サーバー証明書が発行されましたら、証明書発行のお知らせのメール内リンクより事前にダウンロードし、【.cer】や【.txt】などの拡張子で保存してください。

※サーバー証明書のダウンロードについては、以下をご参考ください。

▼SSLサーバー証明書のダウンロード

https://www.cybertrust.co.jp/ssl/support/download.html

6. 証明書のインストール

SSL設定ファイルを編集し、中間CA証明書と、サーバー証明書のインストールを行います。

1. 以下のコマンドを実行し、サーバー証明書、中間CA証明書の順で連結させます。

cat “サーバー証明書ファイル名” “中間CA証明書ファイル” > “連結ファイル名”

※サーバー証明書ファイル「server.cer」と、中間CA証明書ファイル「evg3.txt」を連結し、「certs.pem」ファイルを作成する例

cat server.cer evg3.txt > certs.pem

※連結ファイルの拡張子は「.pem」を指定します。
※クロスルート証明書を設定する場合、サーバー証明書、中間CA証明書、クロスルート証明書の順に連結します。

```
cat server.cer PUBCAG3.txt > certs.pem 1
```

6. 証明書のインストール

2. 設定ファイルの以下のディレクティブに連結ファイルの保存ディレクトリのフルパスをファイル名を含めて記述します。

   ■ssl_certificate

3. 続いて、秘密鍵ファイルの保存ディレクトリのフルパスをファイル名を含めて記述します。

   ■ssl_certificate_key

更新や他社からのお乗換えの場合、いずれかのご設定を行ってください。

- 設定ファイル内の指定先ファイルをリネームし、更新後の証明書ファイルへ差し替える。
- 設定ファイル内のフルパスの指定を更新後のファイルの保存先へ変更する。

```
HTTPS server

server {
    listen       443 ssl;
    server_name  localhost;

    ssl_certificate      /etc/nginx/ssl_certs/certs.pem; 2
    ssl_certificate_key  /etc/nginx/ssl_certs/server.key 3

    ssl_session_cache shared:SSL:1m;
    ssl_session_timeout  5m;

    ssl_ciphers  HIGH:!aNULL:!MD5;
    ssl_prefer_server_ciphers   on;

    location / {
        root   /usr/share/nginx/html;
        index  index.html index.htm;
    }
}
```

※ 設定ファイルの行末に、必ずセミコロン「;」が必要です。
※ 上記は編集後の設定ファイルの例です。

6. 証明書のインストール

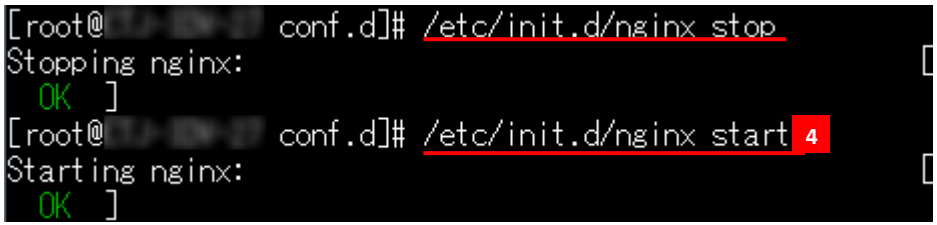
4. 設定を有効にするため、以下のコマンドでnginxの再起動を行ってください。

■サーバーの停止

nginx stop

■サーバーの起動

nginx start



※ ご利用の環境により、コマンドが異なる可能性がございます。
※ 「restart」コマンドで再起動を行った場合、設定が正しく反映されない場合があります。

以上で、設定は全て完了です。

- 作成した秘密鍵ファイルは、万が一に備えて必ず別のメディア（CDやUSBなど）にコピーして安全な場所に保管してください。
- 弊社がお客様の秘密鍵ファイルの情報が含まれた秘密鍵ファイルの情報を受け取ることはございません。あらかじめご了承ください。

7. SSL通信の確認

サーバー証明書が正しく設定され、エラーやセキュリティ警告が表示されず、正常にSSL通信が可能であることを確認します。

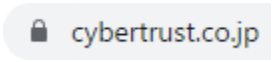
- SSL通信の確認は設定を行っているサーバー以外のWEBブラウザやスマートフォンなどの携帯端末、弊社「SSLサーバ証明書　導入サポートツール」のサーバ証明書の設定確認から行うことを推奨します。

■設定確認例

<Edge>

<Firefox>

<Chrome>



※接続時にセキュリティ警告やエラーが表示される場合は、以下よくある質問の「SSL通信時のセキュリティ警告やエラーについて」をご参照ください。

https://www.cybertrust.co.jp/ssl/support/faq/

https://www.cybertrust.co.jp

詳細は下記まで、お問い合わせください。

0120-957-975

電話受付時間 平日 9:00 ～ 18:00

servicedesk@cybertrust.ne.jp