cybertrust

SSL/TLSサーバー証明書

Apache + mod SSL（Linux）

CSR 作成/証明書インストール手順書

（新規・更新用）

Version 2.2

PUBLIC RELEASE

2025/06/01

改訂履歴

日付	バージョン	内容
2012/06/22	1.0	初版リリース
2012/08/27	1.1	「OU」に関する記述内容を修正
2013/06/26	1.2	SureServer(1024bit)の受付終了に伴う修正
2013/08/02	1.3	Cybertrust Japan Public CA G3 の提供開始に伴う修正
2013/10/24	1.4	擬似乱数ファイルの作成に関する修正
2014/01/06	1.5	SureServer(1024bit)の終了に伴う修正
2015/02/09	1.6	クロスルート証明書の変更に伴う修正
2016/11/08	1.7	設定ファイルへの記述内容を修正
2016/12/15	1.8	「はじめに」の記述内容を修正
2017/04/28	1.9	「OU」に関する記述内容を修正
2022/06/24	2.0	ソフトウェアバージョンの更新に伴う修正 「OU」に関する記述内容を修正
2023/04/14	2.1	秘密鍵の作成手順を修正
2025/06/01	2.2	商品名変更に伴う修正

目次

内容

はじめに

【！】本手順書をご利用の前に必ずお読みください

本ドキュメントは、「Linux OS」「Apache」の環境下でサイバートラストのサーバー証明書をご利用いただく際の CSR 作成とサーバー証明書のインストールについて解説するドキュメントです。

本手順は、「Cent OS6.9」「Apache2.4.29」「OpenSSL 1.1.1q」の環境下で動作確認をしております。

また、OpenSSL（Path 設定を含む）、Apache がすでに設定されており、Apache 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。

実際の手順はお客様の環境により異なる場合があり、Apache 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。

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。

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。

サーバー証明書お申込みフロー

サーバー証明書のご購入については、以下のお申込みフローをご確認ください。

本手順では、赤枠 で囲まれた部分のフローをご案内しています。

STEP1	お申込み前の確認（EV認証）	お申込み前の確認（企業認証）
	CSR の作成　P6～	
STEP2	WEB からのお申し込み（SureBoard / SureHandsOn）	
STEP3	必要書類送付/申請の意思確認（電話） 証明書の発行	
STEP4	証明書のダウンロード　P13～	
STEP5	証明書のインストール　P14～	
STEP6	SSL/TLS 通信の確認　P16～	

CSR の作成

1. CSR 作成前のご確認事項

CSR 作成前に以下についてご確認ください。

1.1. 公開鍵長のご指定について

公開鍵長は「2048bit」をご指定ください。

1.2. CSR 作成時に指定する項目（DN）について

詳細は以下をご確認ください。

≫CSR 作成時に指定する項目について

1.3. 本手順の設定例について

本手順では以下の設定を例としてご案内しております。

項目	ファイル名
サーバルート	/etc/httpd
秘密鍵ファイル・証明書ファイル保存ディレクトリ	/etc/httpd/conf/ssl
設定ファイル保存ディレクトリ	/etc/httpd/conf/extra/httpd-ssl.conf
サーバー証明書ファイル名	servercert.cer
秘密鍵ファイル名	server.key
中間 CA 証明書ファイル名	evg3.txt

【！】注意事項

・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 を作り直していただく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。

・本手順では各ファイルの保存用ディレクトリ「ssl」を作成し、カレントディレクトリとして操作しています。

・出力ファイル名として既存のファイルと同名を指定した場合、確認のメッセージなどは表示されずに上書き保存されます。

2. 秘密鍵ファイルの作成

秘密鍵ファイルを作成します。

A) OpenSSL を用いて秘密鍵ファイルを作成します。

■ コマンド入力

openssl genpkey -out (秘密鍵ファイル名) -algorithm RSA
-pkeyopt rsa_keygen_bits:(公開鍵長) -(暗号方式)

例)暗号方式「AES256」で公開鍵長「2048bit」の秘密鍵ファイル「server.key」を作成

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

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

B) 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。

```
Enter PEM pass phrase:
```

C) パスフレーズを再入力します。

```
Verifying - Enter PEM pass phrase:
```

上記の操作が全て完了すると、カレントディレクトリに秘密鍵ファイルが作成されます。

3. CSR の作成

CSR を作成します。

A） 作成した秘密鍵ファイルから CSR を作成します。

■ コマンド入力

openssl req –new –key（秘密鍵ファイル名）–out（作成するCSR 名）

例）秘密鍵ファイル「server.key」から CSR「server.csr」を作成

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

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

B） 秘密鍵ファイルの作成時に入力したパスフレーズを入力します。

```
Enter pass phrase for server.key:
```

C） DN 情報の入力

CSR 作成に必要な DN 情報を入力します。

■ Country Name (2 letter code):

JPと入力します。

```
Country Name (2 letter code) [GB]:JP
```

■ State or Province Name (full name):

入力必須項目です。

申請する組織の都道府県名を入力してください。

例）Tokyo

```
State or Province Name (full name) [Berkshire]:Tokyo
```

■ Locality Name (eg, city) :

入力必須項目です。

申請する組織の市町村名を入力してください。（東京 23 区は区名）

例）Minato-ku

```
Locality Name (eg, city) [Newbury]:Minato-ku
```

■ Organization Name (eg, company):

入力必須項目です。

申請する英訳組織名を入力してください。

例）Cybertrust Japan Co.,Ltd.

```
Organization Name (eg, company) [My Company Ltd]:Cybertrust Japan Co.,Ltd
```

■ Organizational Unit Name (eg, section):

任意入力項目です。

必要に応じて申請する組織の部署名を入力してください。

※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。

例）Technical Division

```
Organizational Unit Name (eg, section) []:Technical Division
```

■ Common Name (eg, your name or your server's hostname):

入力必須項目です。

申請するサーバー証明書の FQDN（サーバ名＋ドメイン名）を入力してください。

例）www.cybertrust.ne.jp

```
Common Name (eg, your name or your server's hostname) []:www.cybertrust.ne.jp
```

■ 以下の項目は入力不要のため、何も入力せずに Enter キーを押して進んでください。

- e-Mail Address:
- A challenge password:
- An optional company name:

以上で CSR の作成は完了です。

4. 鍵ファイルのバックアップ

秘密鍵ファイルは、証明書のインストール時に必要です。

万が一に備えて、必ず別のメディア（CDやUSBメモリ等）にコピーして安全な場所に保管してください。

なお、弊社がお客様の秘密鍵ファイルの情報を受け取ることはございません。

5. 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内容をコピーし、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。

なお、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。

＜CSR サンプル＞ ※ こちらは申請にご利用いただけません。

```
-----BEGIN CERTIFICATE REQUEST-----
・・・・・
MIIEhDCCA2wCAQAwgYkxCzAJBgNVBAYTAkpQMQ4wDAYDVQQIDAVUb2t5bzESMBAG
A1UEBwwJTWluYXRvLWt1MSIwIAYDVQQKDBlDeWJlcnRydXNOIEphcGFuIENvLixM
dGQuMRIwEAYDVQQLDAlUZXNOIFVuaXQxHjAcBgNVBAMMFXRlc3QuY3liZXJOcnVz
2t/rD9fTPgo7u4aYzw4BpnAqLmGgy3XpsvCo6f4ROcFsgrk05FgeUCaeDFyllEST
・・・・・
-----END CERTIFICATE REQUEST-----
```

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

なお、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。

証明書のインストール

【！】本手順はサーバー証明書の発行後に行います。

6. 証明書のダウンロード

インストールが必要となる中間 CA 証明書・SSL サーバー証明書を事前にダウンロードします。

6.1. 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

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？

6.2. SSL サーバー証明書のダウンロード

SSL 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。

≫ SSL サーバー証明書のダウンロードについて

7. 証明書のインストール

中間 CA 証明書と SSL サーバー証明書のインストールを行います。

7.1. SSL 設定ファイルの編集

SSL 設定ファイルを編集します。

※SSL 設定ファイル名は、お客様がお使いの Apache により異なる場合があります。

例） Apache バージョンによる設定ファイル名の違い

・Apache 2.0 系 ・・・ ssl.conf

・Apache 2.2 系 ・・・ httpd-ssl.conf

・Apache 2.4 系 ・・・ httpd-ssl.conf

A） Apache の設定ファイルで SSL サーバー証明書・秘密鍵ファイル・中間 CA 証明書のフルパスとファイル名を設定します。

※以下の 3 行がコメントアウトされている場合は有効にしてください。

・SSLCertificateFile

・SSLCertificateKeyFile

・SSLCertificateChainFile

■SSLサーバー証明書

SSLCertificateFile SSL サーバー証明書ファイル名（フルパス）

■秘密鍵ファイル

SSLCertificateKeyFile 秘密鍵ファイル名（フルパス）

■中間CA証明書

SSLCertificateChainFile 中間 CA 証明書ファイル名（フルパス）

※Apache 2.4.8 以降の場合は「SSLCertificateChainFile」ディレクティブを使用せず、サーバー証明書、中間 CA 証明書の順番で連結して 1 つにしたファイルを「SSLCertificateFile」ディレクティブに設定してください。

例）設定例

SSLCertificateFile /etc/httpd/conf/ssl/servercert.cer

SSLCertificateKeyFile /etc/httpd/conf/ssl/server.key

SSLCertificateChainFile /etc/httpd/conf/ssl/evg3.txt

■ 更新や他社からの乗り換えの場合

以下のいずれかの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て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。

B） Apache の設定ファイルを確認し、以下の記述のコメントアウトを外し、SSL の設定を有効にしてください。

#LoadModule socache_shmcb_module modules/mod_socache_shmcb.so

→ LoadModule socache_shmcb_module modules/mod_socache_shmcb.so

#LoadModule ssl_module modules/mod_ssl.so

→ LoadModule ssl_module modules/mod_ssl.so

Include conf/extra/httpd-ssl.conf

→ Include conf/extra/httpd-ssl.conf

C） SSL 通信の設定を有効にするため、Apache の再起動を行ってください。

サーバー再起動：systemctl reload httpd

※ ご利用の環境によりましては、コマンドが異なる場合があります。
※ 正しく反映されない場合は停止（stop）と起動（start）をお試しください。

以上で証明書のインストールは完了です。

SSL 通信の確認

8. SSL 通信の確認

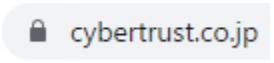
サーバー証明書が正しくインストールされ、エラーやセキュリティ警告が表示されず、正常に SSL 通信が可能であることを確認します。

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、「サーバー証明書の設定確認」から行うことを推奨します。

■ 設定確認例

- Edge

- Chrome



なお、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。

≫ SSL 通信時のセキュリティ警告やエラーについて