cybertrust

DigiCert SSL/TLS 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 1.5

PUBLIC RELEASE

2018/10/25

改訂履歴

日付	バージョン	内容
2017/02/13	1.0	初版リリース
2017/03/08	1.1	「はじめに」の記述内容を修正
2017/04/28	1.2	「OU」に関する記述内容を修正
2018/08/09	1.3	ドメイン名変更に伴い記述内容を修正
2018/10/01	1.4	「グローバル IP」「OU」に関する記述内容を修正
2018/10/25	1.5	ドメイン名変更に伴い記述内容を修正

目次

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 DigiCert SSL/TLS 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 OS6.3」「Apache2.2.15」「OpenSSL 1.0.1e」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。

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	CSR の作成　P6～
↓	
STEP2	WEB からのお申し込み（Cert Station）
↓	
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　P15～
↓	
STEP5	証明書のインストール　P16～
↓	
STEP6	SSL 通信の確認　P18～

cybertrust

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

CSR 作成時に以下の項目を指定いただきますので、あらかじめ必要項目をご確認ください。

【!】以下の点についてご注意ください。

・●印がついている項目は必須設定項目です。
・各項目の最大文字数は半角 64 文字(半角スペースを含む)です。日本語は 20 文字です。
・CSR に使用できる文字は半角英数字(a～z, A～Z, 0～9)と記号(「"」「#」「;」「+」を除く)です。
・組織名(O)、市町村名(L)、都道府県(S)については、CSR 作成時の値に関わらず、
申請法人で指定した値(日本語 or 英語)が証明書情報へ反映されます。

入力項目		内容	入力例
●	コモンネーム(CN)	実際に接続する URL の FQDN(※1)	https://www.cybertrust.ne.jp/index.html ⇒ www.cybertrust.ne.jp
	組織単位名(OU)	部署名(任意)(※2)	Technical Division
●	組織名(O)	申請組織の名称(英名)	Cybertrust Japan Co.,Ltd.
●	市町村名(L)	申請組織の事業所住所の「市町村名」(英名) ※東京は 23 区	Minato-ku
●	都道府県名(S/ST)	申請組織の事業所住所の「都道府県名」(英名)	Tokyo
●	国名(C)	申請組織の国名(JP 固定)	JP

※1 DigiCert SSL/TLS 証明書は、グローバル IP アドレス、プライベート IP アドレスならびにベースドメイン名、ホスト名はコモンネームとしてご指定いただけませんのでご注意ください。

※2 OU の値は空欄で申請することをお勧めします。詳細はこちらをご覧ください。

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
サーバールート	/usr/local/apache2
秘密鍵ファイル・証明書ファイル保存ディレクトリ	/usr/local/apache2/conf/ssl
設定ファイル保存ディレクトリ	/usr/local/apache2/conf/extra/httpd-ssl.conf
サーバー証明書ファイル名	Digicert.cer
秘密鍵ファイル名	server.key
中間 CA 証明書ファイル名	DC_OVCA.cer

【！】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。

・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」を作成しています。

・既存の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。

2. 秘密鍵ファイルの作成

OpenSSL を用いて秘密鍵ファイルを作成します。

A) 擬似乱数ファイルを作成します。

※本項で作成する疑似乱数は、秘密鍵の推測をより困難にするため、一時的に利用します。疑似乱数を使用しない場合は本手順をスキップして B)へお進みください。

■ コマンド入力

openssl（ハッシュ関数）＊＞（擬似乱数ファイル名）.dat

例）ハッシュ関数「sha1」を用いて、擬似乱数ファイル「sha1.dat」を作成

openssl sha1 ＊＞ sha1.dat

```
openssl sha1 * > sha1.dat
```

擬似乱数ファイルがカレントディレクトリに作成されます。

【！】注意事項

・本コマンドはディレクトリ内のファイルから擬似乱数ファイルを作成します。
・カレントディレクトリに参照元となるファイルが存在していない場合は以下が表示され、擬似乱数ファイルを正しく作成されませんので、あらかじめ任意のファイルを 1 つ以上置いてください。

```
*: No such file or directory
```

・以下のエラーが表示された場合は、カレントディレクトリ内にディレクトリが含まれています。本エラーが表示されましても、乱数ファイルは正常に作成されます。

※以下は「test」というディレクトリが含まれている場合のエラー表示例です。

```
Read Error in test
19246:error:0200B015:system library:fread:Is a directory:bss_file.c:198:
19246:error:20082002:BIO routines:FILE_READ:system lib:bss_file.c:199:
```

B） 作成した擬似乱数ファイルから秘密鍵ファイルを作成します。

openssl genrsa（暗号方式）-out（秘密鍵ファイル名）-rand（擬似乱数ファイル名）（公開鍵長）

例）暗号方式「des3」と擬似乱数ファイル「sha1.dat」を用いて公開鍵長「2048bit」の秘密鍵ファイル「server.key」を作成

openssl genrsa -des3 -out server.key -rand sha1.dat 2048

```
openssl genrsa -des3 -out server.key -rand sha1.dat 2048
```

※擬似乱数を作成していない場合

openssl genrsa（暗号方式）-out（秘密鍵ファイル名）（公開鍵長）

例）暗号方式「des3」を用いて公開鍵長「2048bit」の秘密鍵ファイル「server.key」を作成

openssl genrsa -des3 -out server.key 2048

C） 以下が表示されますので、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 pass phrase for server.key:
```

D） パスフレーズを再入力します。

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

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。（東京は 23 区）

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。

※OU の値は空欄で申請することをお勧めします。詳細はこちらをご覧ください。

```
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（サーバー名＋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となります。

万が一に備えて、必ず別のメディア（CD や USB 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。あらかじめご了承ください。

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（Cert Station）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＞ ※ こちらは申請にご利用いただけません。

```
-----BEGIN CERTIFICATE REQUEST-----
・・・・・
MIIEhDCCA2wCAQAwgYkxCzAJBgNVBAYTAkpQMQ4wDAYDVQQIDAVUb2t5bzESMBAG
A1UEBwwJTWluYXRvLWt1MSIwIAYDVQQKDBlDeWJlcnRydXN0IEphcGFuIENvLixM
dGQuMRIwEAYDVQQLDAlUZXN0IFVuaXQxHjAcBgNVBAMMFXRlc3QuY3liZXJOcnVz
2t/rD9fTPgo7u4aYzw4BpnAqLmGgy3XpsvCo6f4ROcFsgrkO5FgeUCaeDFyllEST
・・・・・
-----END CERTIFICATE REQUEST-----
```

「-----BEGIN CERTIFICATE REQUEST----- 」から、「-----END 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 文字でも欠けるとフォーマットエラーとなります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。

≫ EV SSL Plus 中間 CA 証明書ダウンロード

≫ SSL Plus 中間 CA 証明書ダウンロード

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。

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 SSL

・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 /usr/local/apache2/conf/ssl/Digicert.cer

SSLCertificateKeyFile /usr/local/apache2/conf/ssl/server.key

SSLCertificateChainFile usr/local/apache2/conf/ssl/DC_OVCA.cer

■ 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） 設定を有効にするため、Apache の再起動を行ってください。

サーバー停止：/usr/local/apache2/bin/apachectl stop

サーバー起動：/usr/local/apache2/bin/apachectl start

※ 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。
※「apachectl restart」コマンドで再起動を行った場合、正しく反映されない場合があります。

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

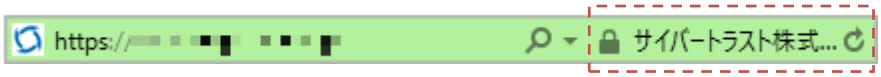
サーバー証明書が正しくインストールされ、エラーやセキュリティ警告が表示されず、正常に SSL 通信が可能であることを確認します。

SSL 通信の確認は設定を行っているサーバー以外の Web ブラウザや携帯電話、スマートフォンなどの携帯端末などから行うことを推奨します。

■ 設定確認例

- Internet Explorer 11

＜EV SSL Plus＞



＜SSL Plus＞

- Firefox 51

＜EV SSL Plus＞

＜SSL Plus＞