



SureServer for SAKURA/SureServer for SAKURA(EV)

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 1.1

PUBLIC RELEASE

2015/04/21

改訂履歴

日付	バージョン	内容
2014/12/10	1.0	初版リリース
2015/04/21	1.1	サイバートラストの WEB ディレクトリ変更に伴うリンク先 URL の修正

目次

はじめに.....	4
CSR の作成.....	5
1. CSR 作成前のご確認事項.....	6
1.1. 公開鍵長のご指定について.....	6
1.2. CSR 作成時に指定する項目 (DN) について.....	6
1.3. 本手順の設定例について.....	7
2. 秘密鍵ファイルの作成.....	8
3. CSR の作成.....	10
4. 鍵ファイルのバックアップ.....	12
5. 証明書のお申し込み.....	12
証明書のインストール.....	13
6. 証明書のダウンロード.....	14
6.1. 中間 CA 証明書のダウンロード.....	14
6.2. SSL サーバー証明書のダウンロード.....	14
7. 証明書のインストール.....	16
7.1. SSL 設定ファイルの編集.....	16
SSL 通信の確認.....	18
8. SSL 通信の確認.....	19

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 OS5.6」「Apache2.2.3」「OpenSSL 0.9.8e」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た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ます、Apache の動作を保証するものではありません。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ます、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。

このドキュメントで説明するソフトウェアはライセンスに基づいて配布されるものであり、ライセンスの条項に従った使用のみ許可されます。このドキュメントは、本来の使用目的のために発行され、公に発行されるものではありません。

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。

サイバートラスト株式会社から事前に書面による合意を得ない限り、このドキュメントまたはその一部から直接的または間接的に知り得た内容または主題に関して、個々の企業やその従業員などの第三者に対し、口頭、文書、またはその他のいかなる手段によっても伝達することはできません。

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。

※2048bit 未満の鍵長をご指定の場合、証明書の申請時にエラーとなりますのでご注意ください。

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。
- CSR に使用出来る文字は半角英数字(a~z, A~Z, 0~9)と記号(「”」「#」「;」「+」を除く)です。
- 日本語は使用しないでください。
- 個人事業主の方は入力項目が異なります。詳細につきましては、[個人事業主のお申し込み方法](#)をご参照ください。

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	https:// www.cybertrust.ne.jp /index.html ⇒ www.cybertrust.ne.jp
	グローバル IP アドレス(※1)	https:// 212.xxx.xxx.xxx /index.html ⇒ 212.xxx.xxx.xxx
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 SureServer for SAKURA(EV) は、コモンネームをグローバル IP アドレスとしてご指定いただけません。

※2 申請法人以外の名称、屋号、商標、住所、場所、その他特定の自然人や法人を参照する値を指定することはできません。

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	SureServer.cer
秘密鍵ファイル名	server.key
中間 CA 証明書ファイル名	PUBCAG3.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てください。
- ・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:ls a directory:bss_file.c:198:
19246:error:20082002:BIIO 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。

※申請法人以外の名称、屋号、商標、住所、場所、その他特定の自然人や法人を参照する値を指定することはできません。

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、オンラインサインアップの入力フォームに貼り付けて、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-----
.
.
.
MIIEhDCCA2wCAQAwYkxCzAJBgNVBAYTAKpQM4wDAYDQQIDAVU2t5bzESMBAG
A1UEBwwJTWluYXRvLWt1MSIwIAYDVQQKDBIDeWJlcnRydXNOIEphcGFuIENvLixM
dGQuMRIwEAYDVQQLDAIUZXNOIFVuaXQxHjAcBgNVBAMMFXRlc3QuY3liZXJ0cnVz
2t/rD9fTPgo7u4aYzw4BpnAqLmGgy3XpsvCo6f4R0cFsgrk05FgeUCaeDFyIIEST
.
.
.
-----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 URL からダウンロードしてください。

商品名	中間 CA 証明書
SureServer for SAKURA	https://www.cybertrust.ne.jp/sureserver/download/root_ca/PUBCAG3_sha2.txt
SureServer for SAKURA(EV)	https://www.cybertrust.ne.jp/sureserver/download/root_ca/evcag2_sha2_1_2.txt

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、事前にダウンロードし、【.txt】や【.pem】などの拡張子で保存してください。

- A) SSL サーバー証明書の発行後にお送りするメール(件名:[さくらインターネット]《重要》SureServer サーバー証明書発行のお知らせ)に記載されている URL にアクセスします。
- B) SSL サーバー証明書のダウンロード画面が表示されますので、お申し込み完了後にお送りしたメール(件名:【重要】お申込受付完了のお知らせ(ダウンロードパスワードご案内))に記載のパスワードを入力し、ダウンロードボタンをクリックしてください。

- C) SSL サーバー証明書のダウンロード画面表示にならない、SSL サーバー証明書を任意のフォルダに保存してください。**

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 1.3 系 ... httpd.conf
- Apache 2.0 系 ... ssl.conf
- Apache 2.2 系 ... httpd-ssl.conf

A) Apache の設定ファイルに以下の 3 行を追加し、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。

■ 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)

例) 設定例

```
SSLCertificateFile /usr/local/apache2/conf/ssl/SureServer.cer
SSLCertificateKeyFile /usr/local/apache2/conf/ssl/server.key
SSLCertificateChainFile usr/local/apache2/conf/ssl/PUBCAG3.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

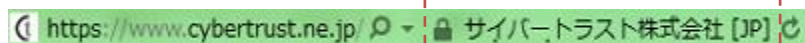
サーバー証明書が正しくインストールされ、エラーやセキュリティ警告が表示されず、正常に SSL 通信が可能であることを確認します。

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、「[サーバー証明書の設定確認](#)」から行うことを推奨します。

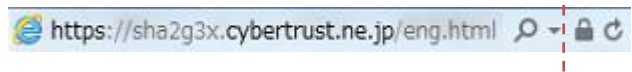
■ 設定確認例

- Internet Explorer 10

<SureServer for SAKURA(EV)>

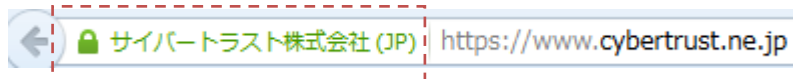


<SureServer for SAKURA>

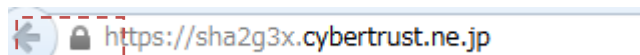


- Firefox 34

<SureServer for SAKURA(EV)>



<SureServe for SAKURA>



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](#)