cybertrust

SureServer/SureServer EV

Apache + mod SSL（Windows）

CSR 作成/証明書インストール手順書

（新規・更新用）

Version 1.9

PUBLIC RELEASE

2017/04/28

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

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、Microsoft 社「Windows OS」「Apache + mod SSL」の環境下でサイバートラストのサーバ証明書をご利用いただく際の CSR 作成とサーバ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、「Apache2.2.15 win32-x86 openssl-0.9.8m-r2」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。

サーバ証明書お申込みフロー

サーバ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	お申込み前の確認
	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　P14～

↓

STEP5	証明書のインストール　P15～

↓

STEP6	SSL 通信の確認　P19～

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。

※クラウド商品（for クラウド）、マルチドメイン商品（SureServer MD など）を含みます。

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	C:¥Apache
秘密鍵ファイル・証明書ファイル保存ディレクトリ	C:¥Apache¥conf¥ssl
Apache 設定ファイル保存ディレクトリ	C:¥Apache¥conf¥httpd.conf
SSL 設定ファイルの保存ディレクトリ	C:¥Apache¥conf¥extra¥httpd-ssl.conf
サーバ証明書ファイル名	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
カレントディレクトリ	C:¥Apache¥conf¥ssl

【！】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。

・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。ご注意ください。

・本手順では以下のフォルダを作成、ファイルの保存を行い、カレントディレクトリとしてご案内いたしております。

2. 秘密鍵ファイルの作成

OpenSSL を用いて、コマンドプロンプト上で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
```

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。

■ コマンド入力

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
```

※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) 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

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) [AU]: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) [Some-State]: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) []: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) [Internet Widgits Pty Ltd]:Cybertrust Japan Co.L
td.
```

■ 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。

※指定可能な値については、「組織単位名(OU)について」をご覧ください。

例)Technical Division

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

■ Common Name* (eg, YOUR name):

入力必須項目です。

申請するサーバ証明書の 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) []:www.cybertrust.ne.jp
```

■ **以下の項目は、何も入力せずに[Enter]を押して進んでください。**

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

```
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

全ての入力が完了しますと「-out」で指定したディレクトリに CSR が作成されます。

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(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＞ ※ こちらは申請にご利用いただけません。

```
-----BEGIN CERTIFICATE REQUEST-----
・・・・・
MIIEhDCCA2wCAQAwgYkxCzAJBgNVBAYTAkpQMQ4wDAYDVQQIDAVUb2t5bzESMBAG
A1UEBwwJTWIuYXRvLWt1MSIwIAYDVQQKDBlDeWJlcnRydXNOIEphcGFuIENvLixM
dGQuMRIwEAYDVQQLDAlUZXNOIFVuaXQxHjAcBgNVBAMMFXRlc3QuY3liZXJOcnVz
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？

【！】SureServer EV[2048bit]・SureServer EV[SHA-2]、および、
SureServer[2048bit]用クロスルート方式をご利用の場合は、**中間 CA 証明書とクロスルート証明書を連結して 1 つにしたファイル**が必要になります。

6.2. SSL サーバ証明書のダウンロード

SSL サーバ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 SSL サーバ証明書・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サーバ証明書

SSLCertificateFile "SSL サーバ証明書ファイル名（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 "C:¥Apache¥conf¥ssl¥SureServer.cer"

SSLCertificateKeyFile "C:¥Apache¥conf¥ssl¥server.key"

SSLCertificateChainFile "C:¥Apache¥conf¥ssl¥PUBCAG3.cer"

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 ssl_module modules/mod_ssl.so

→LoadModule ssl_module modules/mod_ssl.so

■ 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。

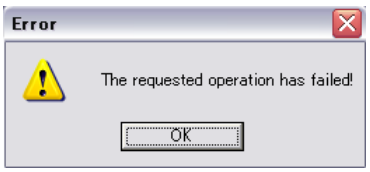
- 設定ファイル内の指定先ファイルをリネームして更新後の証明書ファイルへ差し替える。
- 設定ファイル内のフルパスの指定を更新後のファイルの保存先へ変更する。

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。

以上で証明書のインストールは完了です。

7.2. 秘密鍵ファイル暗号化によるエラーについて

Windows 環境下で暗号化した秘密鍵ファイルを使用する際、以下のエラー（The requested operation has failed!）が表示され、サーバ証明書のインストール後に Apache を起動できない場合があります。



「C:¥Apache¥logs¥error.log」に以下のエラーログが記述されます。

[error] Init: SSLPassPhraseDialog builtin is not supported on Win32 (key file 秘密鍵ファイル名)

7.3. 改善方法

本事象につきましては、秘密鍵ファイルの暗号化を解除する事で改善する場合があります。具体的な操作は以下となります。

A) 暗号化を解除した秘密鍵ファイルを新たに作成します。

■ **コマンド入力**

openssl rsa -in (暗号化された秘密鍵ファイル名) -out (新たに作成する秘密鍵ファイル名)

例)新しい秘密鍵ファイル名を「server2.key」とした場合

openssl rsa -in server.key -out server2.key

B) 「Enter PEM pass phrase」と表示されますので、秘密鍵ファイルのパスフレーズを入力します。

C) カレントディレクトリに暗号化を解除した秘密鍵ファイル「server2.key」が作成されます。

D) 作成した秘密鍵ファイルで Apache が正しく起動するか確認します。

SSL 通信の確認

8. SSL 通信の確認

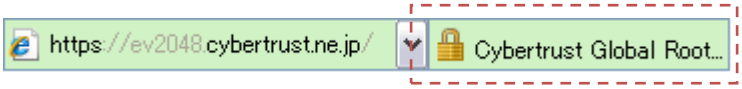
サーバ証明書が正しくインストールされ、エラーやセキュリティ警告が表示されず、正常に SSL 通信が可能であることを確認します。

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 8

＜SureServer EV[2048bit]＞



＜SureServer[2048bit]（クロスルート方式を含む）＞

- Firefox 12.0

＜SureServer EV[2048bit]＞

＜SureServer[2048bit]（クロスルート方式を含む）＞

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