JPRS サーバー証明書発行サービス

サーバー証明書 インストール手順

（Apache[mod_ssl_2.0.45 以降] 新規/更新）

Version 1.0

株式会社日本レジストリサービス（JPRS）

更新履歴

日付	Version	
2016/07/29	1.0	初版リリース

中間 CA 証明書、サーバー証明書をダウンロードし、次の手順に従い証明書を設定してください。

Apache のバージョンおよび Windows 版に関する注意事項

2.0.44 以前の古い Apache 2.0 系列には、中間 CA 証明書の処理に欠陥があり、この本手順書に記載されている手順では中間 CA 証明書を**インストールできません。**新しい Apache へアップグレードしてください。

Windows 環境では実際の表記や用語が異なりますのでご注意ください。

環境	Unix	DOS（Windows）
変数置換	${変数名}	%変数名%
パス名	/ディレクトリ名/ファイル名	ドライブ名:¥ディレクトリ名¥ファイル名
プロンプト	#や$	ドライブ名>
コマンド・インタープリタ	シェル	コマンド プロンプト

またインストールの際には **TLS/SSL モジュールが同梱**されているソフトウェアパッケージをご利用ください。特に Apache Software Foundation の配布している Windows 用の Apache には、TLS/SSL モジュールが同梱されてい**ない**パッケージもありますのでご注意ください。

インストール時の注意点

本手順書で説明しているパス名は例示のため、異なる値を指定している場合は適宜読み替えてください。

/APACHE_HOME ：Apache のインストール先ディレクトリです。

bin ：コマンドがインストールされるサブディレクトリです。Apache の設定やバージョンにより「sbin」「libexec」となっている場合があります。

C: ：Windows 環境では C:ドライブに Apache がインストールされていることを前提としています。

■設定ファイルについて

TLS/SSL 通信を行うためには、Apache の起動時に読み込む設定ファイルへ証明書や鍵ペアのパス名を指定する必要があります。

デフォルトの設定ファイルは、サーバーのインストール先ディレクトリの conf サブディレクトリにあります。

サーバーの種類や版　既定の設定ファイル名	
Apache 2.2 以降	extra サブディレクトリ中の httpd-ssl.conf
2.0	ssl.conf
1.3	httpd.conf

※サーバーの種類や版にしたがって具体的なパス名は異なります。

※2 系の Apache の conf/original というサブディレクトリには、上記と同名の別ファイルのあることがあります。同名の別ファイルと間違えないようご注意ください。

※上記は、Apache-SSL や Apache の開発者がの配布しているオリジナルの値です。上記と違った値にカスタマイズし、配布されていることもあります。設定ファイルが見つからない場合、各ディストリビューションベンダーなどの配布元へお問い合わせください。

■TLS/SSL 設定ファイルの有効化

Apache 2 系列では、サーバーの設定ファイル (httpd.conf) と、TLS/SSL の設定ファイル (ssl.conf や extra/httpd-ssl.conf など) が別々になっています。

サーバーの設定ファイルにある「Include」のエントリーで、TLS/SSL の設定ファイルを取り込む指定がされています。もし TLS/SSL の設定を取り込むように設定されていない場合、「Include」の行頭にある「#」 文字を削除し、設定を取り込むよう変更をしてください。

例：Include ssl.conf

■必要モジュール群の組込み

Apache 2.3 系列以降では、 mod_ssl モジュール自身や、 mod_ssl モジュールの呼び出している下位モジュール群を、 Apache HTTP サーバーの設定ファイル (httpd.conf) より組み込む必要があります。

「LoadModule」のエントリーにモジュールとして組み込む設定がされていますが、もし設定がされていない場合はモジュールを組み込む設定をしてください。

例）

```
LoadModule socache_shmcb_module modules/mod_socache_shmcb.so
LoadModule slotmem_shm_module modules/mod_slotmem_shm.so
LoadModule ssl_module modules/mod_ssl.so
```

※すでに指定があり、行頭に「#」文字がある場合は、「#」を削除してください。

※パス名の区切り文字は、 Unix や Windows といった環境にかかわらず常に「/」文字です。

「LoadModule」：指定の名前のファイルをモジュールとして組み込む指定

「modules/mod_socache_shmcb.so」,「modules/mod_slotmem_shm.so」,
「modules/mod_ssl.so」：組み込むモジュールの入ったファイルの名前。このファイル名は、Apache-SSL や Apache の開発者が配布しているモジュールの名前です。
上記と違った値にカスタマイズし、配布されていることもありますのでご注意ください。

モジュール群を正しく組み込めない場合、各ディストリビューションベンダーなどの配布元へお問い合わせください。

モジュール群を正しく組み込めることを確認

コマンド例： `# /APACHE_HOME/bin/apachectl -t`

Windows 環境の場合

(Apache 2.2 以降) `C:¥>¥APACHE_HOME¥bin¥httpd -t`

(Apache 2.0 以前) `C:¥>¥APACHE_HOME¥bin¥Apache –t`

「Syntax OK」 と出力されることをご確認ください。

上記で「OK」が出力されない場合、設定ファイルのエントリーやファイル名などが間違っている可能性があります。

各証明書は必ずバックアップをとって、安全な場所に格納してください。

1 事前準備

1.1 中間 CA 証明書のダウンロード

以下より中間 CA 証明書をダウンロードし、保存してください。

■中間 CA 証明書について

https://jprs.jp/pubcert/info/intermediate/

1.2 サーバー証明書のダウンロード

1.2.1 JPRS から送付される場合

JPRS から送付されるメール「サーバー証明書ダウンロード手続きのご案内[FQDN]」に記載されている URL より証明書をダウンロードしてください。

1.2.2 指定事業者から提供される場合

それぞれの事業者の指定する方法にてダウンロードしてください。

※詳細はサーバー証明書を購入した指定事業者にお問合せください。

2 中間 CA 証明書のインストール

この手順では例として、設定ファイル内の SSLCertificateChainFile エントリーに、以下の指定がされているものとします (実際は 1 行の設定が、2 行以上で表示、印字されている場合があります)。

例）SSLCertificateChainFile /**APACHE_HOME**/conf/ssl.crt/ca.crt

2.1 中間 CA 証明書のディレクトリの移動

中間 CA 証明書を、SSLCertificateChainFile エントリーで指定したパス名に移動させます。

※JPRS_OVCA.cer（中間 CA 証明書）は、現在作業中のディレクトリにあるものとします。

※ドメイン認証型（DV）では、ファイル名は JPRS_DVCA.cer となります。

コマンド例： `mv JPRS_OVCA.cer /APACHE_HOME/conf/ssl.crt/ca.crt`

2.2 確認

指定したディレクトリに、「**ca.crt**」ファイルが保存されているかご確認ください。

以上で中間 CA 証明書のインストールは完了です。

3 サーバー証明書のインストール

この手順では、 例として設定ファイル内の SSLCertificateFile エントリーに、以下の指定がされているものとします。

例） SSLCertificateFile /**APACHE_HOME**/conf/ssl.crt/server.crt

3.1 サーバー証明書を、SSLCertificateFile エントリーで指定した名前のファイルとして移動

サーバー証明書を、SSLCertificateFile エントリーで指定したパス名へ移動させます。

※本書ではサーバー証明書のファイル名を「example.cer」としており、 現在作業中のディレクトリにあるものとします。

コマンド例： `mv example.cer /APACHE_HOME/conf/ssl.crt/server.crt`

3.2 確認

指定したディレクトリに「**server.crt**」ファイルが保存されているかご確認ください。

以上でサーバー証明書のインストールは完了です。

4 鍵ペアの設定

この手順では例として、設定ファイル内の SSLCertificateKeyFile エントリーに以下の指定がされているものとします。

例） SSLCertificateKeyFile **/APACHE_HOME/conf/ssl.key/server.key**

4.1 鍵ペアのファイルの移動

サーバー証明書に対応する鍵ペアのファイルを、SSLCertificateKeyFile エントリーで指定したパス名に移動させます。

※servername.key（お申込み時に生成した鍵ペアファイル）は、 現在作業中のディレクトリにあるものとします。

コマンド例： `mv servername.key /APACHE_HOME/conf/ssl.key/server.key`

4.2 確認

指定したディレクトリに 「**server.key**」 ファイルが保存されているかご確認ください。

以上で鍵ペアの設定は完了です。

5 Apache のサーバー・プロセス再起動

5.1 Apache のサーバー・プロセスの停止

Apache のサーバー・プロセスを停止してください。

コマンド例： `/APACHE_HOME/bin/apachectl stop`

5.2 Apache のサーバー・プロセスの再開

Apache のサーバープロセスを再開してください。

コマンド例： `/APACHE_HOME/bin/apachectl start`

(Apache 2.0 以前の場合　　Apache/APACHE_HOME/bin/apachectl startssl)

※「**graceful**」 や 「**restart**」 などを引数に指定して実行しても、 新しい証明書の設定になりませんので、ご注意ください。

Windows 環境の注意点

《Windows 環境の場合》

停止： (Apache 2.2 以降) `C:¥>¥APACHE_HOME¥bin¥httpd -k stop`

停止： (Apache 2.0 以前) `C:¥>¥APACHE_HOME¥bin¥Apache -k stop`

開始： (Apache 2.2 以降) `C:¥>¥APACHE_HOME¥bin¥httpd -k start`

開始： (Apache 2.0 以前) `C:¥>¥APACHE_HOME¥bin¥Apache -k start`

証明書のインストールは、以上で完了です。