**・コマンド履歴を削除する(sudo　history 　–c　)**

●**実習１－１　Webサーバー（Apache）確認と準備**

**Sudo systemctl status apache2**

①Webサーバーが起動し動作しているか確認する

　　起動していない場合、Webサーバーを起動させる

**Sudo systemctl start apache2**

②ブラウザを開き、Webサーバーのホームページを確認する

③opensslパッケージがインストールされているかバージョンを確認する。

**openssl version**

　 インストールされていない場合は、インストールする

**sudo apt install -y openssl**

　④鍵や証明書を作成するディレクトリを作成する

|  |
| --- |
| sudo mkdir /ca ・・・証明書を保管するディレクトリ  sudo mkdir /ca/private　　　　　 ・・・秘密鍵を保管するディレクトリ |

●**実習１－２**

**今回の実習では、秘密鍵、証明書を作成して、HTTPS通信ができるようにする**

**＊自己認証局と公開鍵の作成しない。**

**(１)　プライベートキーの作成（秘密鍵名：server.key）**

　 保存ディレクトリ ：　/ca/private/

　　ファイル名：　server.key

パスフレーズ (PEM pass phrase) : 123qwe

①　SSLプライベートキー保存ディレクトリへ移動

**Cd** /ca/private/

②　プライベートキーの作成

**Sudo openssl genrsa -aes256 -out server.key 2048**

③　サーバプライベートキーの確認　**ls**

　　表示例

**server.key**

**(２)** **証明書発行要求（CSR）の作成 (有効期限３６５日　server.csr)**

　　保存ディレクトリ ：　/ca

　 ファイル名 ：　server.csr

有効期限　　　　 ： 365日

----------------------------------------

＜登録内容　→の右の値を順に入力する　＞

国コード　　　　　　：Country Name　 →　JP

都道府県名　　　　　：State or Province Name→ OSAKA

市区町村名　　　　　：Locality　Name → OSAKA

会社名 ：Organization Name → ECCComp

部門名 　　　　　 :Organization Unit Name→ IT

サーバ名（FQDN） 　　：Common Name → クラス名出席番号.ecccomp.ac.jp

管理者メールアドレス：Email Address → クラス名出席番号@ecccomp.ac.jp

以降（チャレンジ、追加会社名）なしとして「Enter」キー

**Cd /ca**

1. /caディレクトリに移動する

②　証明書発行要求（CSR）の作成 (有効期限３６５日　server.csr)

**Sudo openssl req -new -key /ca/private/server.key -out server.csr -days 365**

③　サイト証明書発行要求（CSR）の確認　**ls**

　　表示例

**server.csr**

**(３)** **証明書（PEM）の作成（server.pem、自己認証局なし）**

　　保存ディレクトリ：　/ca

　　ファイル名 ：　server.pem

1. 証明書（PEM）の作成（server.csrからserver.pem）

**sudo openssl x509 -days 365 -in server.csr -out server.pem -req -signkey server.key**

②　証明書（PEM）の確認　**ls**

　　表示例

**server.csr server.pem**

**(４)** **証明書関連ファイルのセキュリティ設定**

　パーミッション ：　600（所有者のみ　読み取り書き込み権限あり）

①　対象ファイル（３つ）のパーミッションを600に設定する

**sudo chmod 600 /ca**

1. 設定出来たかどうか、ファイルの詳細情報を表示して確認する

**Sudo ls -l**

**(５)** **SSLの設定を設定ファイルに登録**

**（/etc/apache2/sites-available/default-ssl.conf）**

①　編集前にオリジナル状態のバックアップの為、default-ssl.confと同じディレクトリに  
「default-ss.conf.org」の名前でコピーしておく

**Cd /etc/apache2/sites-available**

**Sudo Cp default-ssl.conf default-ss.conf.org**

1. viエディタで開いてdefault-ssl.confを編集する

**Sudo Vi default-ssl.conf**

<設定内容>

・SSLCertificateKeyFile サーバ秘密鍵絶対パスに変更　　　　　　（変更）

・SSLCertificateFile 　　サーバ証明書絶対パスに変更　　　　　　（変更）

**(６)** **Apacheの設定の有効化と再起動、動作確認**

①　設定したSSLを有効化する

**Sudo a2enmod ssl**

**sudo a2ensite default-ssl**

②　Apacheを再起動する

**Sudo systemctl restart apache2**

③　Windowsのブラウザから下記アドレスにアクセスし、証明書が表示されることを確認する

https://自マシンのＩＰアドレス/



**●実習１－３　HTTPSへリダイレクト**

このままでは、URLにhttpsと入力しない場合、HTTPS通信ができません。ここでは通常のURLを

入力した場合でもHTTP通信できるようにリダイレクトさせます。

**（１）HTTPリダイレクトの設定**

①　Apacheの設定ファイルを変更

vi /etc/apache2/sites-avialable/000-default.conf

②　<VirtualHost \*:80>～</VirtualHost>に次の項目を追加する

|  |
| --- |
| **RewriteEngine On**  **RewriteCond %{HTTPS} off**  **RewriteRule ^(.\*)$ https://%{HTTP\_HOST}%{REQUEST\_URI} [R=301,L]** |
|  |

　 ③　設定を有効化する

Sudo a2enmod rewrite

④　Apacheを再起動する

Sudo systemctl restart apache2

**（２）【チェック項目】HTTPからHTTPSへリダイレクトを確認**

ブラウザを開き、http://IPアドレスでサイトへアクセスし、HTTPSに変更された確認

1. 授業中に実施できた場合  
   教員にIPアドレスを連絡してチェックしてもらうこと。
2. 後日実施等で教員チェックが難しい場合  
   ブラウザのアドレスバーと証明書ビューアを含むスクリーンショット画像を保存

**●実習１－４　提出用ファイルの作成と提出**

①　証明書、秘密鍵をcatコマンドで表示してコピーする、ファイル名は以下の通り

　　　　　　server.key →　クラス名番号server.key

　　　　　　server.pem →　クラス名番号server.pem

　　　　②　Apacheの設定ファイル（/etc/apache2/sites-avialable/000-default.conf）を表示してコピー

する、ファイル名は以下の通り

000-default.conf →　クラス名番号000-default.conf

**●課題提出**

**【全員】**

**「実習01クラス名番号」のフォルダを作成し、３つのファイル（クラス名番号server.key、クラス名番号server.pem、クラス名番号000-default.conf）とログファイルを入れて、sv23の指定された場所へ提出しなさい。**

**【教員未チェックの人】**

**上記のファイルに加えて、ブラウザのアドレスバーと証明書ビューアを含むスクリーンショット画像を提出する。ファイル名の最初を「実習01クラス名番号」（例：実習01IE2A99.png）にすること。（実習1-3(2)）**