

openssl SSL証明書作成

○ 秘密鍵作成

【パスフレーズなし】

```
$ openssl genrsa 2048 > server.key
```

【パスフレーズあり】

```
$ openssl genrsa -des3 2048 > server.key
```

○ CSR作成

【対話型/秘密鍵作成済み】

```
$ openssl req -new -key server.key -out server.csr -sha256
```

【対話型/秘密鍵作成(パスフレーズなし) + CSR 同時作成】

```
$ openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr -sha256
```

【ワンライナー/秘密鍵作成(パスフレーズなし) + CSR 同時作成】

```
$ openssl req -new -newkey rsa:2048 -nodes -keyout private.key -out server.csr -subj  
"/C=JP/ST=Tokyo/L=Shinjuku-ku/O=ExampleCompany/CN=www.example.jp/"
```

○ CSR確認

```
$ openssl req -in server.csr -text
```

○ 証明書発行

【openssl.cnf 諸設定済】

-> 括弧[xxx]は、openssl.cnfに記述していれば不要。引数で渡した値が優先)

```
$ openssl ca -config openssl.cnf -in server.csr -out server.pem [-md sha256] [-days 365] [-extensions usr_cert]
```

○ 証明書確認

```
$ openssl x509 -in server.crt -text
```

○ 証明書失効

-> xx(シリアル値)は、index.txtを確認

```
$ openssl ca -config openssl.cnf -revoke newcerts/xx.pem
```

○ 自己署名

```
$ openssl req -new -x509 -newkey rsa:2048 -nodes -keyout server.key -out server.pem -sha256
```

添付ファイル::

Linux

一意的なソリューション ID: #1003

製作者: n/a

最終更新: 2022-01-24 15:30