

IKEv2証明書発行手順書

2020年6月 初版

OpenSSLのCA局による、CA証明書およびFITELnet装置証明書の発行手順をご説明します。

【前提】

- ・本手順書では、CA局としてLinux(Ubuntu 14.04.5 LTS)を使用します。
- ・OpenSSLのコンフィグ(openssl.cnf)は、以下が設定されている状態とします。

[openssl.cnf](#)

デフォルトの openssl.cnf からの変更箇所は以下をご参照ください。

[デフォルトのopenssl.cnfからの変更箇所](#)

1) 次の手順で、CA局を立ててください。

1-1) 下記コマンドを実行してください。

```
furukawa@ubuntu:/etc/ssl$ sudo /usr/lib/ssl/misc/CA.sh -newca
```

※CA証明書の有効期限を変更する場合は、CA.sh のCADAYSを編集してから実行してください。

(例: CADAYS="-days 7300")

1-2) 必要な情報を入力してください。

```
C : JP
ST : Kanagawa
O : Furukawa
CN : CA1
```

1-3) CA証明書が生成されていることを確認してください(以下★)。

```
furukawa@ubuntu:/etc/ssl$ ls -l /etc/ssl/demoCA/
total 28
-rw-r--r-- 1 root root 4248 May 25 18:16 cacert.pem★
-rw-r--r-- 1 root root 952 May 25 18:16 careq.pem
drwxr-xr-x 2 root root 4096 May 25 18:14 certs
drwxr-xr-x 2 root root 4096 May 25 18:14 crl
-rw-r--r-- 1 root root 0 May 25 18:14 index.txt
drwxr-xr-x 2 root root 4096 May 25 18:14 newcerts
drwxr-xr-x 2 root root 4096 May 25 18:14 private
```

(CA.shの実行例: 手順1-1)と手順1-2)の実行例です。)

```
=====
furukawa@ubuntu:/etc/ssl$ sudo /usr/lib/ssl/misc/CA.sh -newca
CA certificate filename (or enter to create)
```

Making CA certificate ...

Generating a 2048 bit RSA private key

.....+++

.....+++

writing new private key to './demoCA/private/./cakey.pem'

Enter PEM pass phrase:

Verifying - Enter PEM pass phrase:

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:JP

State or Province Name (full name) [Some-State]:Kanagawa

Locality Name (eg, city) []:

Organization Name (eg, company) [Internet Widgits Pty Ltd]:Furukawa

Organizational Unit Name (eg, section) []:

Common Name (e.g. server FQDN or YOUR name) []:CA1

Email Address []:

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:

An optional company name []:

Using configuration from /usr/lib/ssl/openssl.cnf

Enter pass phrase for ./demoCA/private/./cakey.pem:

Check that the request matches the signature

Signature ok

Certificate Details:

Serial Number: 10171089557646302467 (0x8d26f8105e315d03)

Validity

Not Before: May 29 02:07:37 2020 GMT

Not After : May 24 02:07:37 2040 GMT

Subject:

countryName = JP

stateOrProvinceName = Kanagawa

organizationName = Furukawa

commonName = CA1

X509v3 extensions:

X509v3 Subject Key Identifier:

9B:67:7A:E6:B2:66:62:AE:B9:CD:B7:F7:D8:15:D5:7C:77:4C:69:06

X509v3 Authority Key Identifier:

keyid:9B:67:7A:E6:B2:66:62:AE:B9:CD:B7:F7:D8:15:D5:7C:77:4C:69:06

X509v3 Basic Constraints:

CA:TRUE

Certificate is to be certified until May 24 02:07:37 2040 GMT (7300 days)

Write out database with 1 new entries

Data Base Updated

furukawa@ubuntu:/etc/ssl\$

=====

- 3) FITElnet装置の証明書を発行してください。
3-1) 2)で出力された証明書発行要求をtextファイルに張り付けてCA局に置いてください。
(textファイルの置き場所は /etc/ssl です。)

```
furukawa@ubuntu:/etc/ssl$ cat gw.csr
```

```
furukawa@ubuntu:/etc/ssl$
```

- 4) FITELnet装置にCA局とFITELnet装置の証明書を登録してください。
- 4-1) FITELnet装置にCA局の証明書を登録してください(以下のコマンドを実行)。
- ```
IPsecGW# crypto pki add ca certificate CA1 1
```
- ※1)で生成された cacert.pem に含まれるPEMフォーマット部分を貼り付けます。
- 4-2) FITELnet装置にFITELnet装置の証明書を登録してください(以下のコマンドを実行)。
- ```
IPsecGW# crypto pki add certificate cert1 kl1
```
- ※2)で生成されたRSA鍵ペア kl1 と証明書 cert1 を紐付けます。
- ※3)で生成された gw.cer に含まれるPEMフォーマット部分を貼り付けます。

```
IPsecGW# crypto pki add ca certificate CA1 1
Input certificate data(Finally please input <CR>)
-----BEGIN CERTIFICATE-----
(cacert.pemに含まれるPEMフォーマット部分)
-----END CERTIFICATE-----
```

5) VPNクライアント装置にて以下の手順を行って、CA証明書を登録してください。

[Windows10にCA証明書をインストールする方法](#)