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$
==========================================================
```

2) FITELnet装置にて、RSA鍵ペアを生成し、証明書発行要求を作成してください。

2-1) FITELnet装置にてRSA鍵ペアを生成してください(以下のコマンドを実行)。

```
IPsecGW# crypto pki key generate rsa label kl1 modulus 2048
```

2-2) FITELnet装置にて証明書発行要求を作成してください(以下のコマンドを実行)。

```
IPsecGW# crypto pki enroll kl1
```

2-3) 必要な情報を入力してください。

```
fqdn         : IPsecGW.example.com
subject name : C=JP, ST=Kanagawa, O=Furukawa, CN=IPsecGW.example.com
```

※FITELnet装置に以下のIKE ID(端末側で指定するサーバ名)が設定されている前提です。

```
self-identity fqdn IPsecGW.example.com
```

(FITELnet装置におけるコマンド実行例: 手順2-2)と手順2-3)の実行例です。)

```
==================================================
IPsecGW# crypto pki enroll kl1
IPv4 address:
IPv6 address:
fqdn:IPsecGW.example.com
user-fqdn:
subject name:C=JP, ST=Kanagawa, O=Furukawa, CN=IPsecGW.example.com
Signature Algorithm [sha256|sha384|sha512|sha1]:sha256
-----BEGIN CERTIFICATE REQUEST-----
abcdefghijklmQAwUTELMAkGA1UEBhMCSlAxETAPBgNVBAgTCEthbmFnYXdhMREw
DwYDVQQKEwhGdXJ1a2F3YTEcMBoGA1UEAxMTaHJ0LXNndzEuZm5zYy5jby5qcDCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMKPsScDvPkcQfWe2qkGyDOc
FtJiyJMTz1W9e1LS/ehDmmxphReJ3bW2zuVOz6E1818SF5B4glvRD2678P+uNa1O
HMkwFqCM+a5XXb+3l54p9/6W7trh5bCKF2aMuQH1+aITvyBgisI99RVwExG5MIPi
MPdtjDQGRjDmLKZ4t3ufA9uHCkw3zFa67gYC7qrztjm3DOmGYMAuBgE4w7FbcQNX
yBmg7SRLyhlHJvFSla1fMv4T9/4W+7+ANnvE2L/V1Tr/htOUnzWxPIUqNVwRkuHR
7N7Lz4YJi5LmRoYSIFBX/wssCxczN7GwlkK47eSNKdgV4Zz+skwu5yyoVHJKly8C
AwEAAaA+MDwGCSqGSIb3MIAJDjExMCOwCwYDVR0PBAQDAgWgMB4GA1UdEQQXMBWC
E2hydC1zZ3cxLmZuc2MuY28uanAwDQYJKoZIhvcNAQEFBQADggEBAKwhFfCxHUXI
h8dm+FEVAuOAoTgKnigV3xCNrpTXqE/W2RBhn+xBn93hjpj3EzXaU8RHXgkXflMk
F3UEDNDEtRNifTaiNxeyGQC5DYaZdqOyHRaYkusX77BqFGOlkc4EWEKQqGxkAWsP
D25ZidmN2CICW2d1CAsvWR7zabBBD46xuW7j8gq2zNStB8yoi3+t5T9TUSh7uxpY
JmnOjFIhxlFFVG72qIgf/jmdWnTkjp+FFZP1OkMSLAIRmFgmVyRkP4iyG56v7gqY
mKyEUJqEBkWJScpSErpOyjP65fjRJ5KE5DsMf7dJspMjP+zo8tfuXd4KO1234567
lf9LrKgI7oc=
-----END CERTIFICATE REQUEST-----

IPsecGW#
==================================================
```

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。)

(CA局におけるコマンド実行例:
手順3-1)実行後に、証明書発行要求のtextファイル(gw.csr)の内容を表示した状態です。)

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

-----BEGIN CERTIFICATE REQUEST-----
abcdefghijklmQAwUTELMAkGA1UEBhMCSlAxETAPBgNVBAgTCEthbmFnYXdhMREw
DwYDVQQKEwhGdXJ1a2F3YTEcMBoGA1UEAxMTaHJ0LXNndzEuZm5zYy5jby5qcDCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMKPsScDvPkcQfWe2qkGyDOc
FtJiyJMTz1W9e1LS/ehDmmxphReJ3bW2zuVOz6E1818SF5B4glvRD2678P+uNa1O
HMkwFqCM+a5XXb+3l54p9/6W7trh5bCKF2aMuQH1+aITvyBgislI99RVwExG5MIPi
MPdtjDQGRjDmLKZ4t3ufA9uHCkw3zFa67gYC7qrztjm3DOmGYMAuBgE4w7FbcQNX
yBmg7SRLyhlHJvFSla1fMv4T9/4W+7+ANnvE2L/V1Tr/htOUnzWxPIUqNVwRkuHR
7N7Lz4YJi5LmRoYSIFBX/wssCxczN7GwlkK47eSNKdgV4Zz+skwu5yyoVHJKly8C
AwEAAaA+MDwGCSqGSIb3MIAJDjExMCOwCwYDVR0PBAQDAgWgMB4GA1UdEQQXMBWC
E2hydC1zZ3cxLmZuc2MuY28uanAwDQYJKoZIhvcNAQEFBQADggEBAKwhFfCxHUXI
h8dm+FEVAuOAoTgKnigV3xCNrpTXqE/W2RBhn+xBn93hjpj3EzXaU8RHXgkXflMk
F3UEDNDEtRNifTaiNxeyGQC5DYaZdqOyHRaYkusX77BqFGOlkc4EWEKQqGxkAWsP
D25ZidmN2CICW2d1CAsvWR7zabBBD46xuW7j8gq2zNStB8yoi3+t5T9TUSh7uxpY
JmnOjFIhxlFFVG72qIgf/jmdWnTkjp+FFZP10kMSLAIRmFgmVyRkP4iyG56v7gqY
mKyEUJqEBkWJScpSErpOyjP65fjRJ5KE5DsMf7dJspMjP+zo8tfuXd4KO1234567
lf9LrKgI7oc=
-----END CERTIFICATE REQUEST-----

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

3-2) 証明書発行要求に署名しFITELnet装置の証明書を発行してください。
furukawa@ubuntu:/etc/ssl$ sudo openssl ca -in gw.csr -out gw.cer
※gw.cerが証明書として出力されます(出力場所は /etc/ssl です)。

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。

(FITELnet装置におけるコマンド実行例: 手順4-1)と手順4-2)の実行例です。)

```
==================================================
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-----

IPsecGW# crypto pki add certificate cert1 kl1
Input certificate data(Finally please input <CR>)
-----BEGIN CERTIFICATE-----
 (gw.cer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