
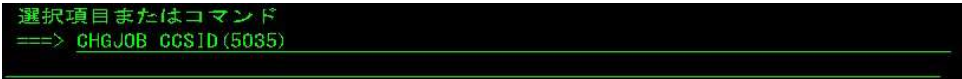


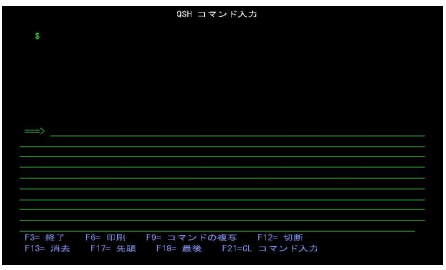


2. 鍵ストア及び鍵ペアの生成

QSH コマンドを実行する準備が出来ていないときは、まず、表 2-1(p.3)の手順を実施します。

表 2-1 QSH コマンドを実行するための準備

手順	内容
1	<p>エミュレータのホストコードページを 939「日本(拡張ローマ字)」に変更します。</p> 
2	<p>IBMi にサインオンし、ジョブの CCSID を 5035 に変更します。</p> 
3	<p>QSH の開始コマンドを実行します。</p> 
4	<p>コマンド入力欄に「10」と入力して F14 を打鍵し、コマンド行を 10 行に拡張します(下図参照)。この操作は、以降の操作をしやすくするための設定です(必須ではありません)。なお、コマンド入力欄が空白の状態でも F14 を打鍵すると最初の状態に戻ります。</p> <div style="display: flex; justify-content: space-around;">   </div>

4. ローカル認証局(CA)の作成

テスト用のローカル CA 作成が不要のときはこの章は読み飛ばしてください。

ローカル CA は、自己証明書の CSR に対して署名付き証明書を発行/インポートまでをテストするために作成します。実際の運用においては、外部の CA(または別途、貴社にて運用されているローカル CA)を使用されることになります。

QSH コマンドを実行する準備が出来ていないときは、まず、表 2-1(p.3)の手順を実施します。次に openssl コマンドを使ってローカル CA を作成します。

OpenSSL フォルダに移動します。

```
cd /QOpenSys/QIBM/ProdData/SC1/OpenSSL
```

次に./misc フォルダにある CA.sh(シェルスクリプト)を newca オプション(新しい CA 作成オプション)で実行します。

```
./misc/CA.sh -newca
```

このスクリプトは対話的に処理されますので、適切な値で応答します。以下は例です。

1. password
2. JP
3. Tokyo
4. Asakusabashi
5. Fairdinkum
6. WilComm/aXes Team
7. Fairdinkum.co.jp
8. axes@fairdinkum.co.jp
9. password

demoCA というローカル CA が作成されます。

5. 署名付き証明書を発行

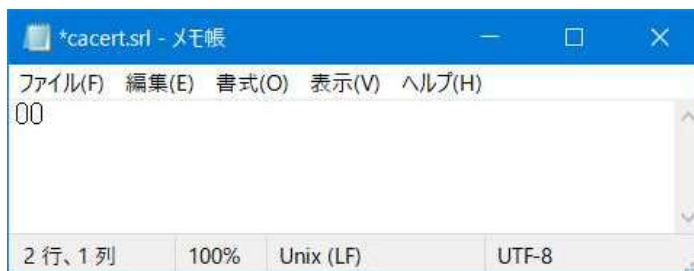
前章でローカル CA を作成していないときはこの章は読み飛ばしてください。

QSH コマンドを実行する準備が出来ていないときは、まず、表 2-1(p.3)の手順を実施します。次に openssl コマンドを使って、前章で作成したローカル CA にて署名付き証明書を発行します。

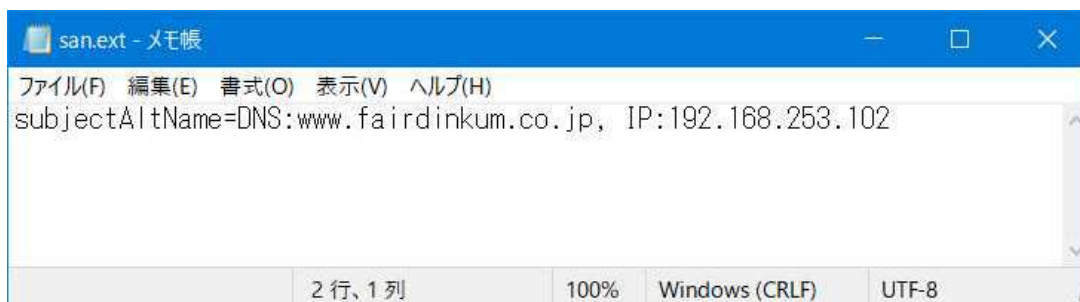
demoCA フォルダに移動します。

```
cd /Q0penSys/Q1BM/ProdData/SC1/0penSSL/demoCA
```

demoCA フォルダ内に cacert.srl(中身は"00")が無ければ、Windows のメモ帳などで作成します。cacert.srl には、このローカル CA で証明書が発行されるたびにシリアル値(カウント値)が書き出されます。



demoCA フォルダ内に san.ext というテキストファイルを用意します。このファイルの情報は署名付き証明書を発行する際に SAN(Subject Alternative Name)を指定するために使用します。フォーマットは下図の通りです。



openssl コマンドで CSR に対する署名付き証明書を発行します。

```
openssl  
x509  
-req  
-CA cacert.pem  
-CAkey ./private/cakey.pem  
-in /axesjsm/jsm/instance/pki/server.csr  
-out /axesjsm/jsm/instance/pki/server.crt  
-days 365  
-extfile san.ext
```

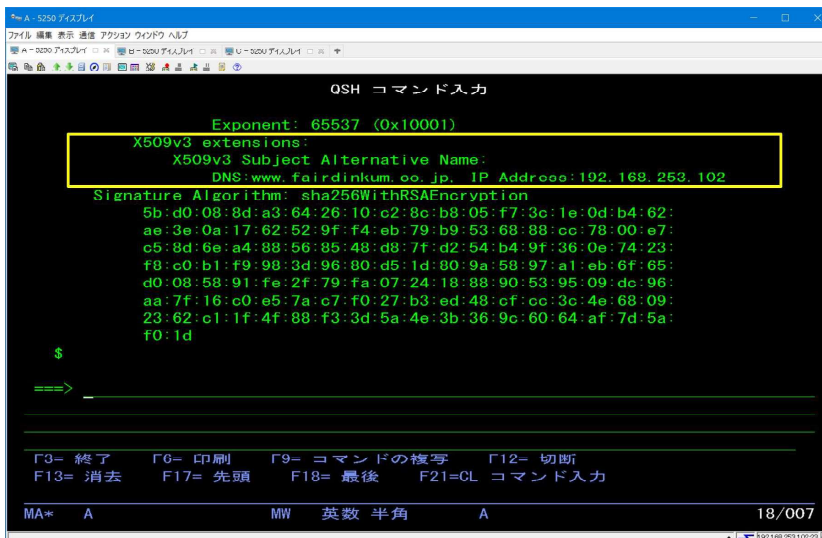
- ✓ 水色のラベルの箇所は aXes の導入バージョン/方法によって異なります。ご不明な場合は弊社 aXes サポートデスクまでお問い合わせくださいませ。
- ✓ 黄色のラベル箇所は適宜、任意の値に書き換えてご使用ください。

以下の openssl コマンドで、発行された署名付き証明書の内容を確認できます。

```
openssl
x509
-text
-noout
-in /axesjsm/jsm/instance/pki/server.crt
```

- ✓ 水色のラベルの箇所は aXes の導入バージョン/方法によって異なります。ご不明な場合は弊社 aXes サポートデスクまでお問い合わせくださいませ。

SAN の情報が含まれているかどうか確認できます(下図参照)。



```
OSH コマンド入力
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Alternative Name:
DNS:www.fairdinkum.co.jp, IP Address:192.168.253.102
Signature Algorithm: sha256WithRSAEncryption
5b:d0:08:8d:a3:64:26:10:c2:8c:b8:05:f7:3c:1e:0d:b4:62:
ae:3e:0a:17:62:52:9f:f4:eb:79:b9:53:68:88:cc:78:00:e7:
c5:8d:6e:a4:88:56:85:48:d8:7f:d2:54:b4:9f:36:0e:74:23:
f8:c0:b1:f9:98:3d:96:80:d5:1d:80:9a:58:97:a1:eb:6f:65:
d0:08:58:91:fe:2f:79:fa:07:24:18:88:90:53:95:09:dc:96:
aa:7f:16:c0:e5:7a:c7:f0:27:b3:ed:48:cf:cc:3c:4e:68:09:
23:62:c1:1f:4f:88:f3:3d:5a:4e:3b:36:9c:60:64:af:7d:5a:
f0:1d
$
==>
Γ9= 終了      Γ6= 印刷      Γ9= コマンドの複写  Γ12= 切断
F13= 消去     F17= 先頭     F18= 最後         F21=CL コマンド入力
MA*  A                MW  英数 半角      A                18/007
```