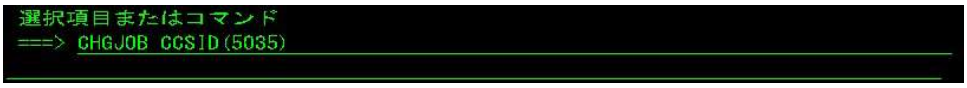
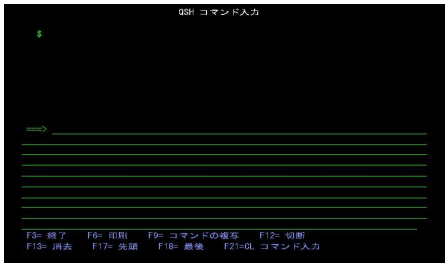
2. 鍵ストア及び鍵ペアの生成

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	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。 
2	IBMi にサインオンし、ジョブの CCSID を 5035 に変更します。 
3	QSH の開始コマンドを実行します。 
4	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、コマンド入力欄がブランクの状態で F14 を打鍵すると最初の状態に戻ります。  

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

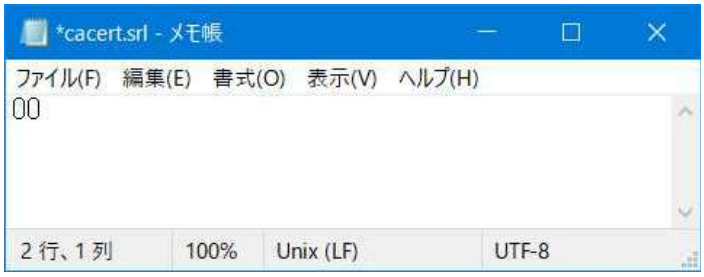
前章でローカル CA を作成していないときはこの章は読み飛ばしてください。

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。

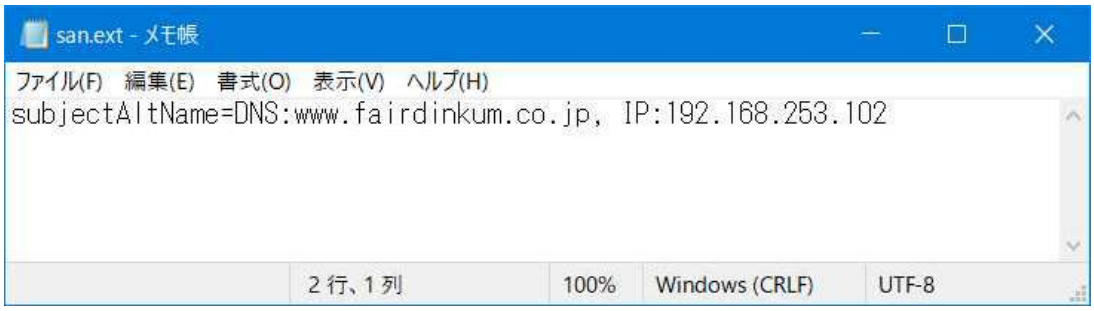
demoCA フォルダに移動します。

```
cd /QOpenSys/QIBM/ProdData/SC1/OpenSSL/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も確認できます(下図参照)。