http://homepage2.nifty.com/shagam/columns/columns002.html
http://shooting-star.myhome.cx/cygwin/proftpd.html
http://www.atmarkit.co.jp/flinux/rensai/linuxtips/702apachessl.html

proftpd を使って FTP over SSL のサーバを立てる

Explicit

サーバの USER コマンドに対してクライアントがユーザ名の代わりに AUTH SSL/AUTH TLS を発行し、サーバからの応答受信後クライアントから SSL/TLS ハンドシェイクを開始し、SSL/TLS セッション確立後にログインを開始する方式。すなわち、非暗号化状態で接続を開始し、ユーザ名とパスワードを検証する直前にセキュアなデータ接続を行う。

Implicit

いきなりクライアントから SSL/TLS ハンドシェイクを開始し、SSL/TLS セッション確立後にログインを開始する方式。すなわち、クライアントはサーバへのすべての要求をセキュア状態で送信する。

■ダウンロード

http://www.proftpd.org/

■インストール

```
./configure --with-modules=mod_tls
make
make install
```

Cygwin の場合は

```
./configure --with-modules=mod_tls --disable-ipv6
```

のように、ipv6 を無効にする必要があるかも。

インストールが終わると
設定ファイルと実行体がインストールされる。

```
/usr/local/etc/proftpd.conf
/usr/local/sbin/proftpd
```

■設定

/usr/local/etc/proftpd.conf
CentOS の場合

```
User        nobody
Group       nobody
```

Cygwin の場合

```
User        SYSTEM
Group      Administrators
```

Cygwin の場合はログの出力先のディレクトリのパーミッションを設定しておく。

■サービス登録

CentOS の場合
ソースディレクトリに移動して

```
cp contrib/dist/rpm/proftpd.init.d /etc/init.d/proftpd
chmod +x /etc/init.d/proftpd
```

必要に応じて起動ファイルを編集

```
vi /etc/init.d/proftpd
```

Cygwin の場合

```
cygrunsrv -I proftpd -d "CYGWIN proftpd" \
-p /usr/local/sbin/proftpd -e CYGWIN="ntsec nosmbntsec" \
-a "--nodaemon" --termsig TERM --shutdown \
-1 /var/log/proftpd/cygrunsrv_out.log \
-2 /var/log/proftpd/cygrunsrv_err.log
```

まずここまで設定して、FTP での接続確認をする。
FTP で接続出来ないときは、ログを確認して対応する。

■ SSL の設定

http://www.atmarkit.co.jp/flinux/rensai/linuxtips/702apachessl.html

SSL を使用するには、まず CA の秘密鍵を作成する。root で以下のコマンドを実行する。

```
# openssl genrsa -rand /var/log/maillog -out ca.key 1024
161380 semi-random bytes loaded
Generating RSA private key, 1024 bit long modulus
......++++++
.++++++
e is 65537 (0x10001)
```

次に、ca.key から CA 証明書の署名要求（CSR）を作成する。ここで対話的に入力した国名などの情報は、発行される証明書に表示される。

```
# openssl req -new -key ca.key -out ca.csr
 （省略）
-----
Country Name (2 letter code) [GB]:JP  ←２文字国名（JP）
State or Province Name (full name) [Berkshire]:Tokyo  ←都道府県
Locality Name (eg, city) [Newbury]:Chiyoda  ←区市町村
Organization Name (eg, company) [My Company Ltd]:Example Corp.  ←組織名
Organizational Unit Name (eg, section) []:Example Dept.  ←部署名
Common Name (eg, your name or your server's hostname) []:Noriyuki
 Kitaura  ←担当者名またはサーバ名など
Email Address []:kitaura@example.co.jp  ←メールアドレス

Please enter the following 'extra' attributes
```

```
to be sent with your certificate request
A challenge password []:  ← [Enter] キー
An optional company name []:  ← [Enter] キー
```

続いて、CA 証明書に署名して発行する。ここでは指定していないが、-days オプションにより、証明書の有効期限を設定することも可能だ。例えば、「-days 365」とすると 1 年間有効の証明書が発行される。

```
# openssl x509 -req -in ca.csr -signkey ca.key -out ca.crt
Signature ok
    subject=/C=JP/ST=Tokyo/L=Chiyoda/O=Example        Corp./OU=Example              Dept./CN=Noriyuki
Kitaura/emailAddress=kitaura@example.co.jp
Getting Private key
```

以降はサーバ用の証明書を作成する作業になる。最初に、サーバ用の秘密鍵を作成する。

```
# openssl genrsa -rand /var/log/maillog -out server.key 1024
5974 semi-random bytes loaded
Generating RSA private key, 1024 bit long modulus
...........++++++
.....................................................++++++
e is 65537 (0x10001)
```

サーバ用の秘密鍵からサーバ証明書の CSR を作成する。CA 証明書の CSR と同様に、各種情報を対話的に入力する。Common Name にはサーバのホスト名を入力する。

```
# openssl req -new -key server.key -out server.csr
 (省略)
-----
Country Name (2 letter code) [GB]:JP
State or Province Name (full name) [Berkshire]:Tokyo
Locality Name (eg, city) [Newbury]:Chiyoda
Organization Name (eg, company) [My Company Ltd]:Example Corp.
Organizational Unit Name (eg, section) []:Example Dept.
Common Name (eg, your name or your server's hostname) []:www.example.jp  ←ホスト名
Email Address []:webmaster@example.jp

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

サーバ用の証明書に署名して発行する前に、認証局が使用するシリアルナンバーのファイルを作成しておく必要がある。

```
# echo 01 > ca.srl
```

準備ができたので、証明書を発行する。ここでは、「-days 365」として 1 年間有効の証明書を発行している。

```
# openssl x509 -req -days 365 -CA ca.crt -CAkey ca.key -in server.csr -out server.crt
Signature ok
            subject=/C=JP/ST=Tokyo/L=Chiyoda/O=Example                              Corp./OU=Example
Dept./CN=example.jp/emailAddress=webmaster@example.jp
Getting CA Private Key
```

server.crt と server.key を以下のようにコピーする。

```
# cp server.crt /usr/local/etc/
```

```
# cp server.key /usr/local/etc/
```

/usr/local/etc/proftpd.conf
に以下の内容を書き加える。

```
<IfModule mod_tls.c>
    TLSEngine on
    TLSLog  /var/log/proftpd/tls.log
    TLSProtocol SSLv23
    TLSCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP

    # Are clients required to use FTP over TLS when talking to this server?
    TLSRequired off

    # Server's certificate
    TLSRSACertificateFile /usr/local/etc/server.crt
    TLSRSACertificateKeyFile /usr/local/etc/server.key

    # Authenticate clients that want to use FTP over TLS?
    TLSVerifyClient off
</IfModule>
```