高エネルギー加速器研究機構　計算科学センター

自前 CA 及び SSL サーバ構築作業ログ

高瀬　亘

2011/12/07

目次

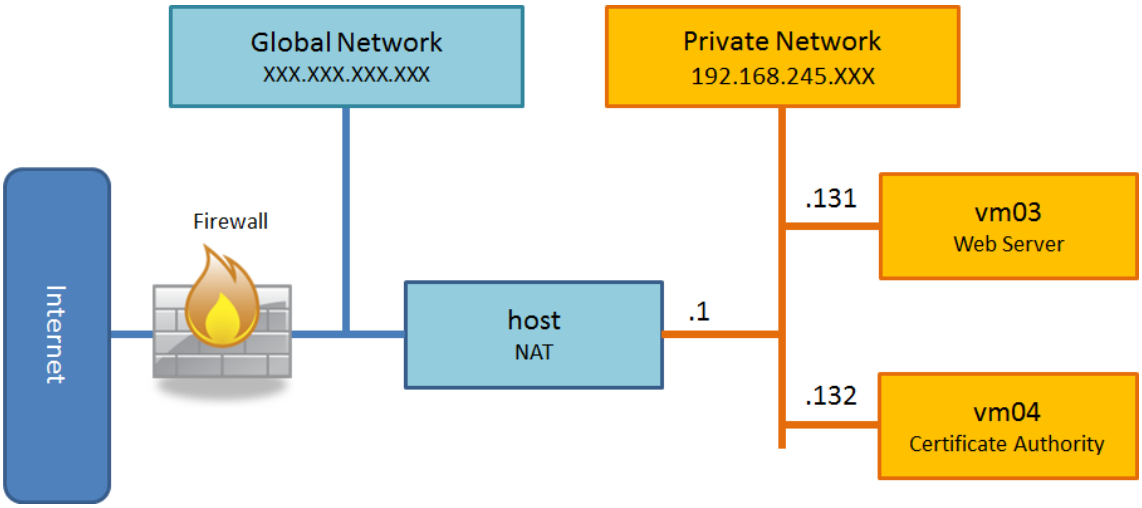
1. はじめに

本書は、過去に筆者が自前CA局とSSLを利用したWebサーバを構築した時の作業ログに修正をほどこし、公開可能にしたものです。

インターネット上には、CA及びSSLサーバの構築に関する記事がいくつか存在しますが、筆者が探した限りでは、CAとSSLサーバが同一マシン上にある例がほとんでした。CA側の作業とSSLサーバ側の作業を切り分けて考えやすいように、本書ではCA局とSSLサーバを別マシンに構築します。

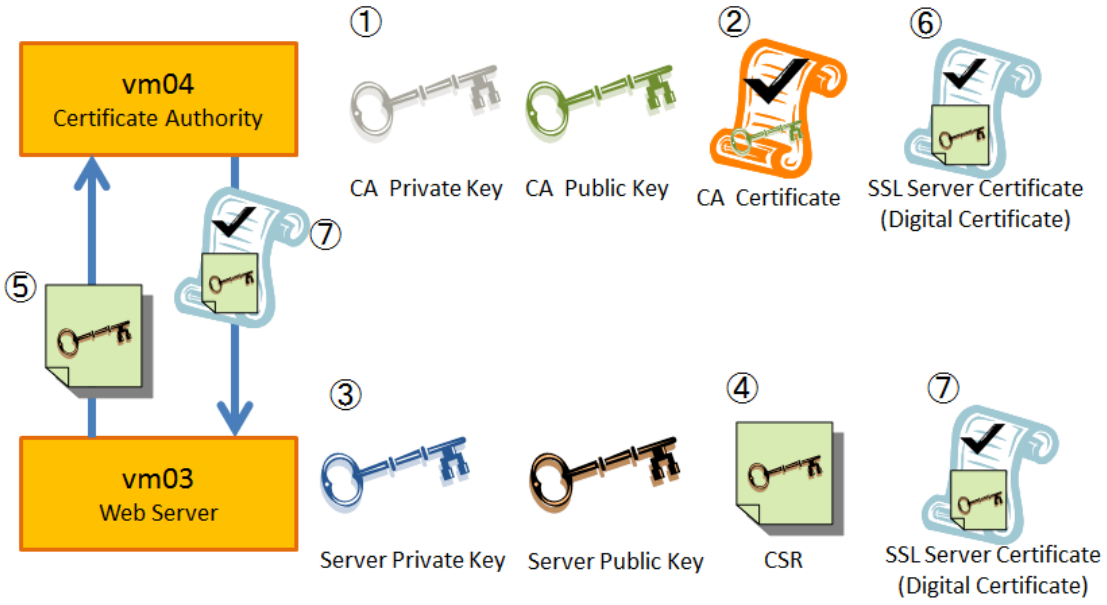
2. ネットワーク構成

- 本書では、1 台のホストマシン(host)上に VM(Virtual Machine)を 2 台(vm03, vm04)立ち上げ、vm03 上に SSL を利用した Web サーバを、vm04 上に自前 CA 局を構築する
- OS は、vm03, vm04 ともに CentOS 5.5(64bit)を使用している
- host⇔vm0X 間、vm03⇔vm04 間は、ホスト名のみでアクセスできるものとする



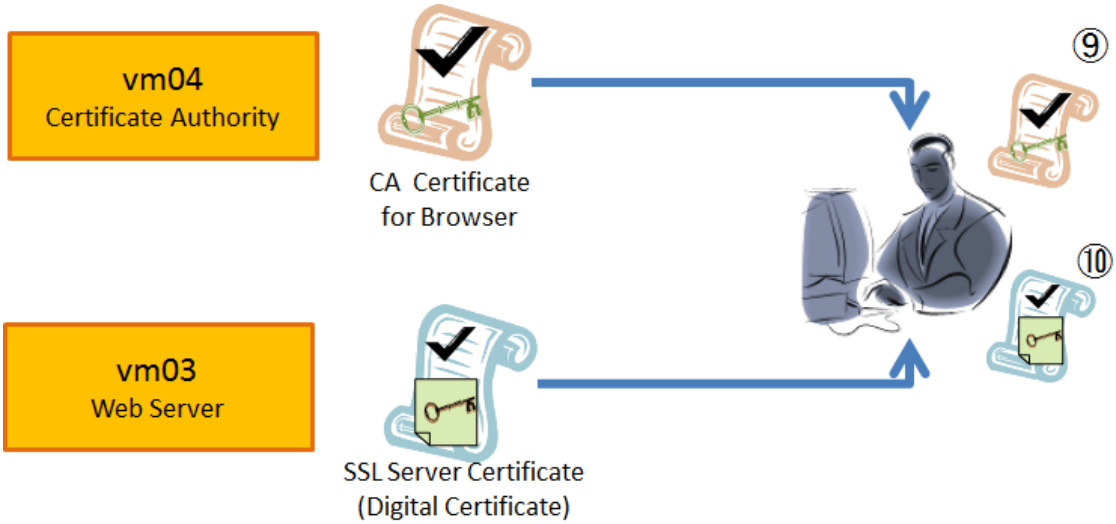
3. CA と SSL サーバの関係及び SSL サイト実現までの概略

① CA は CA 証明書(CA 秘密鍵による署名と CA 公開鍵を含む)を作成
② SSL を利用したい Web サーバ(以下、サーバ)はサーバ秘密鍵/公開鍵を用意
③ サーバは CSR(Certificate Signing Request ； サーバ公開鍵を含む)を作成
④ サーバは CA に CSR を渡す
⑤ CA は SSL サーバ証明書(デジタル証明書 ； CA 秘密鍵による署名と CSR を含む)を作成
⑥ 本人証明データの確認、ドメイン認証、組織認証を行い、CSR の正当性を確認
⑦ CA はサーバに SSL サーバ証明書を送る

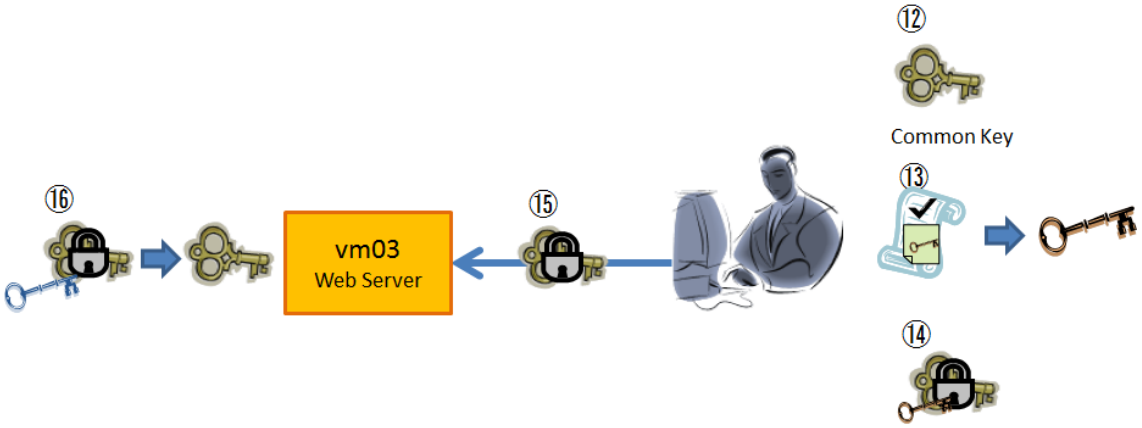


次ページに続く

⑧ CA はブラウザ用の CA 証明書(PEM から DER に変換したもの)を作成してユーザへ配布できる状態にする
⑨ ブラウザは CA 証明書をインポートする
⑩ サーバはブラウザからアクセスがあった時、ブラウザへ SSL サーバ証明書(デジタル証明書)を送る
⑪ ブラウザは、受け取った SSL サーバ証明書が信頼された CA 発行のものかを検証する
- ブラウザにインストールされている CA 証明書内の公開鍵を使用し、SSL サーバ証明書についている CA の署名を検証
- CA 証明書がインポートされていない場合は警告が出る



⑫ ブラウザは共通鍵を作成
⑬ ブラウザは SSL サーバ証明書からサーバ公開鍵を取り出す
⑭ ブラウザはサーバ公開鍵を使用して共通鍵を暗号化する
⑮ ブラウザは暗号化した共通鍵をサーバに送る
⑯ サーバは受けとった共通鍵をサーバ秘密鍵で復号する
⑰ サーバ・ブラウザ間で共通鍵を使用して暗号化された通信が実現する



4. 事前準備(vm03, vm04)

4.1. OSの確認

```
[root@vm04 ~]# cat /etc/redhat-release
  CentOS release 5.5 (Final)
```

4.2. iptablesの設定

```
[root@vm04 ~]# vi iptables.sh
  #!/bin/sh

  /etc/init.d/iptables stop

  iptables -F
  iptables -X

  iptables -P INPUT ACCEPT
  iptables -P OUTPUT ACCEPT
  iptables -P FORWARD DROP

  iptables -A INPUT -s 192.168.245.0/24 -j ACCEPT
  iptables -A OUTPUT -s 192.168.245.0/24 -j ACCEPT
  iptables -A INPUT -s 127.0.0.1 -j ACCEPT
  iptables -A OUTPUT -s 127.0.0.1 -j ACCEPT
  iptables -A INPUT -i lo -j ACCEPT
  iptables -A OUTPUT -o lo -j ACCEPT

  /etc/init.d/iptables save
  /etc/init.d/iptables start
[root@vm04 ~]# sh iptables.sh
```

4.3. opensslコマンドのPATHの確認

```
[root@vm04 ~]# which openssl
  /usr/bin/openssl
```

5. CA の構築(vm04)

5.1. openssl.cnf の設定

```
[root@vm04 ~]# cd /etc/pki/tls/
[root@vm04 tls]# vi openssl.cnf
  -- snipped --
  [ CA_default ]
  ...
  x509_extensions        = usr_cert
  ↓変更
  x509_extensions        = v3_ca
  -- snipped --
  [ usr_cert ]
  ...
  #nsCertType                    = server
  ↓変更
  nsCertType                     = server
  -- snipped --
  [ v3_ca ]
  ...
  #nsCertType = sslCA, emailCA
  ↓変更
  nsCertType = sslCA
  -- snipped --
```

5.2. CA の構築

```
[root@vm04 tls]# cd misc/
[root@vm04 misc]# ./CA -newca
  -- snipped --
  Country Name (2 letter code) [GB]:JP
  State or Province Name (full name) [Berkshire]:Ibaraki
  Locality Name (eg, city) [Newbury]:Tsukuba
  Organization Name (eg, company) [My Company Ltd]:KEK
  Organizational Unit Name (eg, section) []:CRC
  Common Name (eg, your name or your server's hostname) []:vm04
  Email Address []:

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

```
  -- snipped --
  Certificate Details:
          Serial Number: 0 (0x0)
          Validity
              Not Before: Nov 29 08:13:55 2011 GMT
              Not After : Nov 28 08:13:55 2014 GMT
          Subject:
              countryName               = JP
              stateOrProvinceName       = Ibaraki
              organizationName          = KEK
              organizationalUnitName    = CRC
              commonName                = vm04
          X509v3 extensions:
              X509v3 Subject Key Identifier:
                  48:86:FA:C3:24:2E:09:EA:6C:59:FD:09:2D:8C:EE:A7:12:2A:DA:12
              X509v3 Authority Key Identifier:
                  keyid:48:86:FA:C3:24:2E:09:EA:6C:59:FD:09:2D:8C:EE:A7:12:2A:DA:12
                  DirName:/C=JP/ST=Ibaraki/O=KEK/OU=CRC/CN=vm04
                  serial:00

              X509v3 Basic Constraints:
                  CA:TRUE
              Netscape Cert Type:
                  SSL CA
```

5.3. CA 証明書(cacert.pem)、CA 秘密鍵(cakey.pem)の確認

```
[root@vm04 misc]# ls /etc/pki/CA/cacert.pem
  /etc/pki/CA/cacert.pem
[root@vm04 misc]# ls /etc/pki/CA/private/cakey.pem
  /etc/pki/CA/private/cakey.pem
```

5.4. CA 秘密鍵を他ユーザから見られなくする

```
[root@vm04 misc]# chmod 600 /etc/pki/CA/private/cakey.pem
[root@vm04 misc]# chmod 700 /etc/pki/CA/private/
```

5.5. CA 秘密鍵の中身を見てみる

```
[root@vm04 misc]# openssl rsa -in /etc/pki/CA/private/cakey.pem -text
```

6. SSL サーバ鍵の作成と CSR の発行・送信(vm03)

6.1. サーバ秘密鍵の生成

```
[root@vm03 ~]# openssl md5 * > rand.dat
[root@vm03 ~]# openssl genrsa -rand rand.dat -des3 2048 > serverkey.pem
```

6.2. サーバ秘密鍵を他ユーザから見られなくする

```
[root@vm03 ~]# chmod 600 serverkey.pem
```

6.3. サーバ秘密鍵の中身を見てみる

```
[root@vm03 ~]# openssl rsa -in serverkey.pem -text
```

6.4. CSR の生成

```
[root@vm03 ~]# openssl req -new -key serverkey.pem -out csr.pem
  -- snipped --
  Country Name (2 letter code) [GB]:JP
  State or Province Name (full name) [Berkshire]:Ibaraki
  Locality Name (eg, city) [Newbury]:Tsukuba
  Organization Name (eg, company) [My Company Ltd]:KEK
  Organizational Unit Name (eg, section) []:CRC
  Common Name (eg, your name or your server's hostname) []:vm03
  Email Address []:
  Please enter the following 'extra' attributes
  to be sent with your certificate request
  A challenge password []:
  An optional company name []:
```

6.5. CSR の中身を見てみる

```
[root@vm03 ~]# openssl req -in csr.pem -text
```

6.6. CSR を CA に送る

```
[root@vm03 ~]# scp csr.pem vm04:/tmp/csr_vm03.pem
```

6.7. サーバ秘密鍵の配置

```
[root@vm03 ~]# chmod 700 /etc/pki/tls/private/
[root@vm03 ~]# mv serverkey.pem /etc/pki/tls/private/
```

7. SSL サーバ証明書の発行・送信と配布用 CA 証明書の送信(vm04)

7.1. CSR ファイルの確認

```
[root@vm04 ~]# ls /tmp/csr_vm03.pem
  /tmp/csr_vm03.pem
```

7.2. SSL サーバ証明書の作成

```
[root@vm04 ~]# cd /etc/pki/tls/misc/
[root@vm04 misc]# openssl ca -extensions usr_cert -in /tmp/csr_vm03.pem -out ¥
/tmp/servercert.pem
  -- snipped --
  Certificate Details:
          Serial Number: 1 (0x1)
          Validity
              Not Before: Nov 29 08:16:23 2011 GMT
              Not After : Nov 28 08:16:23 2012 GMT
          Subject:
              countryName               = JP
              stateOrProvinceName       = Ibaraki
              organizationName          = KEK
              organizationalUnitName    = CRC
              commonName                = vm03
          X509v3 extensions:
              X509v3 Basic Constraints:
                  CA:FALSE
              Netscape Cert Type:
                  SSL Server
              Netscape Comment:
                  OpenSSL Generated Certificate
              X509v3 Subject Key Identifier:
                  1D:A7:6F:80:69:C8:D8:1A:B3:38:8F:AB:CF:8A:32:E7:F9:78:E1:1C
              X509v3 Authority Key Identifier:
                  keyid:48:86:FA:C3:24:2E:09:EA:6C:59:FD:09:2D:8C:EE:A7:12:2A:DA:12

  Certificate is to be certified until Nov 28 08:16:23 2012 GMT (365 days)
  Sign the certificate? [y/n]:y


  1 out of 1 certificate requests certified, commit? [y/n]y
  -- snipped --
```

7.3. SSL サーバ証明書の中身を見てみる

```
[root@vm04 misc]# openssl x509 -in /tmp/servercert.pem -text
```

7.4. CA が発行した証明書の概要を確認

```
[root@vm04 misc]# cat /etc/pki/CA/index.txt
V    141128081355Z        00      unknown /C=JP/ST=Ibaraki/O=KEK/OU=CRC/CN=vm04
V    121128081623Z        01      unknown /C=JP/ST=Ibaraki/O=KEK/OU=CRC/CN=vm03
```

7.5. SSL サーバ証明書をサーバに送る

```
[root@vm04 misc]# scp /tmp/servercert.pem vm03:/tmp/
```

7.6. ブラウザ用の CA 証明書(バイナリ)をサーバに送る

```
[root@vm04 misc]# openssl x509 -inform PEM -outform DER -in /etc/pki/CA/cacert.pem ¥
-out /tmp/cacert.der
[root@vm04 misc]# scp /tmp/cacert.der vm03:/tmp/
```

8. SSL 対応 Web サーバ設定(vm03)

8.1. SSL サーバ証明書、CA 証明書の確認

```
[root@vm03 ~]# ls /tmp/
  cacert.der  servercert.pem
```

8.2. SSL サーバ証明書の配置

```
[root@vm03 ~]# mv /tmp/servercert.pem /etc/pki/tls/certs/
```

8.3. サーバ秘密鍵、SSL サーバ証明書の配置の確認

```
[root@vm03 ~]# ls /etc/pki/tls/private/serverkey.pem
  /etc/pki/tls/private/serverkey.pem
[root@vm03 ~]# ls /etc/pki/tls/certs/servercert.pem
  /etc/pki/tls/certs/servercert.pem
```

8.4. mod_ssl のインストール

```
[root@vm03 ~]# yum install mod_ssl -y
```

8.5. SSL 用ページの作成

```
[root@vm03 ~]# mkdir /var/www/html/ssl/
[root@vm03 ~]# chmod 755 /var/www/html/ssl/
[root@vm03 ~]# vi /var/www/html/ssl/index.html
  <html>
  <head>
   <title>SSL Page</title>
  </head>
  <body>
   This is SSL Page.
  </body>
  </html>
```

8.6. httpd.conf の設定

```
[root@vm03 ~]# vi /etc/httpd/conf/httpd.conf
  -- snipped --
  ServerName vm03:80  ←追加
  -- snipped --
  <Directory "/var/www/html">
```

```
    ...
    AddType application/x-x509-ca-cert .der  ←追加
</Directory>
-- snipped --
```

8.7. ssl.conf の設定

```
[root@vm03 ~]# vi /etc/httpd/conf.d/ssl.conf
 --snipped --
 AddType application/x-x509-ca-cert .crt .pem  ←変更
 -- snipped --
 SSLCertificateFile /etc/pki/tls/certs/servercert.pem  ←変更
 -- snipped --
 SSLCertificateKeyFile /etc/pki/tls/private/serverkey.pem  ←変更
 -- snipped --
 DocumentRoot "/var/www/html/ssl"  ←変更
 ServerName vm03:443  ←変更
 -- snipped --
```

8.8. Apache の起動

```
[root@vm03 ~]# /etc/init.d/httpd start
 Stopping httpd:                                            [FAILED]
 Starting httpd: Syntax error on line 115 of /etc/httpd/conf.d/ssl.conf:
 SSLCertificateFile: file '/etc/pki/tls/certs/servercert.pem' does not exist or is
empty
                                                            [FAILED]
```

※上記のエラーが出た場合は、SELinux が有効になっている可能性があるので 8.8.1 項以降の作業を行う

※エラーが出なかった場合は、8.9 節の作業へ進む

8.8.1. SELinux の確認と対応

```
[root@vm03 ~]# getenforce
 Enforcing
[root@vm03 ~]# chcon user_u:object_r:httpd_config_t /etc/pki/tls/certs/servercert.pem
[root@vm03 ~]# chcon ¥
user_u:object_r:httpd_config_t /etc/pki/tls/certs/private/serverkey.pem  ←不要かもしれない
```

8.8.2. SELinux の無効化(希望者のみ)

```
[root@vm03 ~]# vi /etc/selinux/config
  SELINUX=disabled  ←変更
[root@vm03 ~]# reboot
```

8.8.3. Apache の起動

```
[root@vm03 ~]# /etc/init.d/httpd restart
  Stopping httpd:                                            [  OK  ]
  Starting httpd: Apache/2.2.3 mod_ssl/2.2.3 (Pass Phrase Dialog)
  Some of your private key files are encrypted for security reasons.
  In order to read them you have to provide the pass phrases.

  Server vm03:443 (RSA)
  Enter pass phrase:

  OK: Pass Phrase Dialog successful.
                                                             [  OK  ]
```

※下記のエラーが出た場合は、ルートディレクトリやホームディレクトリに移動して再度 httpd サービスを起動してみる

```
   shell-init: error retrieving current directory: getcwd: cannot access parent
   directories: No such file or directory
```

8.9. サーバ秘密鍵のパスフレーズを削除

※Apache の再起動の度にパスフレーズを入力するのが嫌な人のみ対象

```
[root@vm03 ~]# openssl rsa -in /etc/pki/tls/private/serverkey.pem ¥
-out /etc/pki/tls/private/serverkey.pem
```

8.10. ブラウザインポート用 CA 証明書の公開

```
[root@vm03 ~]# mv /tmp/cacert.der /var/www/html/
[root@vm03 ~]# rm /tmp/cacert.der
```

9. ブラウザの設定(host)

9.1. http://vm03/cacert.der へアクセスし cacert.der をダウンロード

9.1.1. FireFox3.6 の場合

ツール→オプション→詳細→暗号化→証明書を表示→認証局証明書→インポート→cacert.der を選択→この認証局による Web サイトの識別を信頼する→OK

9.1.2. IE8 の場合

ツール→インターネットオプション→コンテンツ→証明書→信頼されたルート証明書→インポート→cacert.der を選択→証明書をすべて次のストアに配置する→OK

9.2. https://vm03/へアクセス

9.2.1. CA 証明書がブラウザにインポートされている場合

ページが表示される

9.2.2. CA 証明書がブラウザにインポートされていない場合

FireFox3.6

接続の安全性を確認できません→危険性を理解した上で接続するには→例外を追加→セキュリティ例外を承認→ページが表示される

IE8

Internet Explorer ではこのページは表示できません