平成 18 年度情報処理軽井沢セミナーレポート

平成 18 年 8 月 31 日

九州大学 情報基盤センター システム管理係
上田　将嗣

1. 課題タイトル

Web ポータルとクライアント認証

2. 概要

九州大学情報基盤センターでは、研究用計算機システムとして運用しているスーパーコンピュータ等の大型計算機について、GUI での操作を可能にする Web ポータルの導入を検討している。Web ポータルを利用する際にはこれまで以上にセキュリティに留意する必要がある。そのためクライアント証明書の利用を検討してみることとした。

3. 講義・演習とその成果

演習では、クライアント証明書の配布方法について Web を通した配布を行うこととした。安全性の面から考えると H/W トークンの採用が理想的であるが、

・利用者が全国各地にいる

・USB トークンや IC カードの採用時のコストの問題

などから難しいであろうと考えたためである。

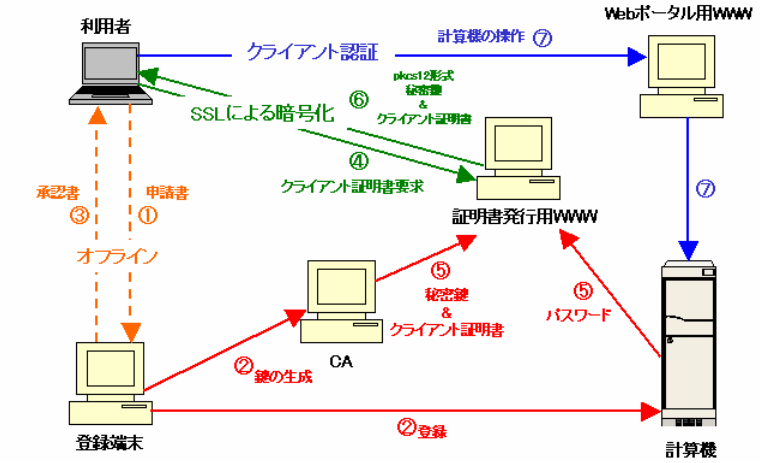

図 1 運用モデル

そこでクライアント証明書を発行するための手順として図 1 に示すような方法を考えた。

研修終了後、アカウントと鍵の登録からクライアント証明書の発行までをテスト環境で構築することにした。テスト環境では openssl-0.9.8b を用いて CA の構築・証明書の発行を行った。

・アカウントの登録＆鍵の生成

①アカウントの登録、②クライアント署名要求、③クライアント証明書の生成をひとつのスクリプトにまとめることにした。このスクリプトはアカウント名とパスワードを引数とし、データベースに格納された利用者情報から利用期限を得てクライアント証明書の有効期限を決定する。なお、今回はクライアント証明書を作成する際に C・ST・O・OU の値を固定として、CN をアカウント名とすることにした。(図 2)

```
root@vm-prime> /var/adm/lib/mkuser b79999a b79999a
spawn openssl req -new -days 123 -key /var/adm/cert/client.key -out
/var/adm/cert/b79999a/clcsr.pem
              ( 略 )
spawn openssl ca -config /usr/local/openssl/ssl/openssl-client.cnf -days 123 -in
/var/adm/cert/b79999a/clcsr.pem -out /var/adm/cert/b79999a/clcert.pem
              ( 略 )
Data Base Updated
root@vm-prime> openssl x509 –inform pem –in /var/adm/cert/b79999a/clcert.pem –text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            e3:ef:d3:c8:f1:78:b2:09
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=JP, ST=Fukuoka, O=Kyushu University, OU=Computing Communications Center,
CN=vm-prime-ca/emailAddress=ueda@cc.kyushu-u.ac.jp
        Validity
            Not Before: Aug 31 07:14:54 2006 GMT
            Not After : Jan  1 07:14:54 2007 GMT
        Subject: C=JP, ST=Fukuoka, O=Kyushu University, OU=Computing Communications Center,
CN=b79999a
              ( 略 )
```

アカウント名	b79999a
パスワード	b79999a
利用期限	2006/12/31

図 2 アカウント登録＆鍵の生成

・クライアント証明書の配布

クライアント証明書の配布に際しては、発行用の web サイトにアクセスがあった時点でのパスワードを用いて pkcs12 形式に変換する。実際のクライアント証明書の取得までの流れを以下に示す。

Web ポータル	https://192.168.130.133/login
クライアント証明書発行サイト	https://192.168.130.133/crt/index.cgi

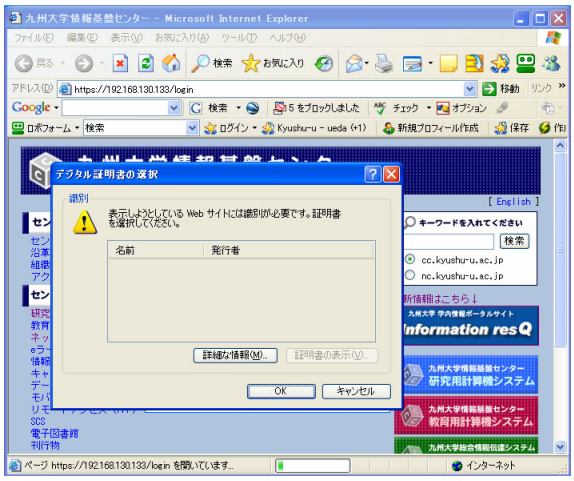

図 3 Web ポータルへのアクセス(証明書がないためアクセスできない)

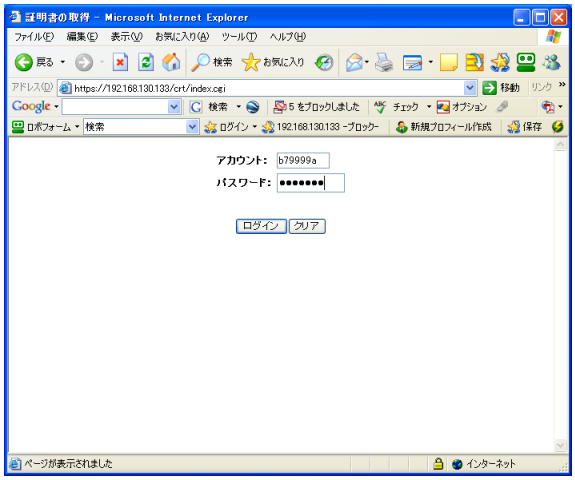

図 4 クライアント証明書取得のためのユーザー認証

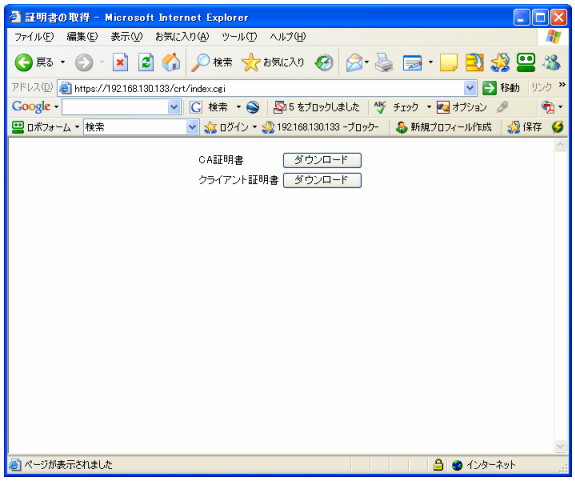

図 5 CA 証明書とクライアント証明書の取得画面

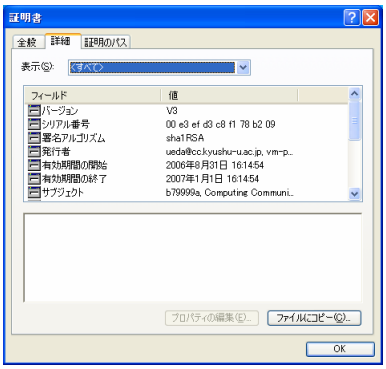

図 6 クライアント証明書

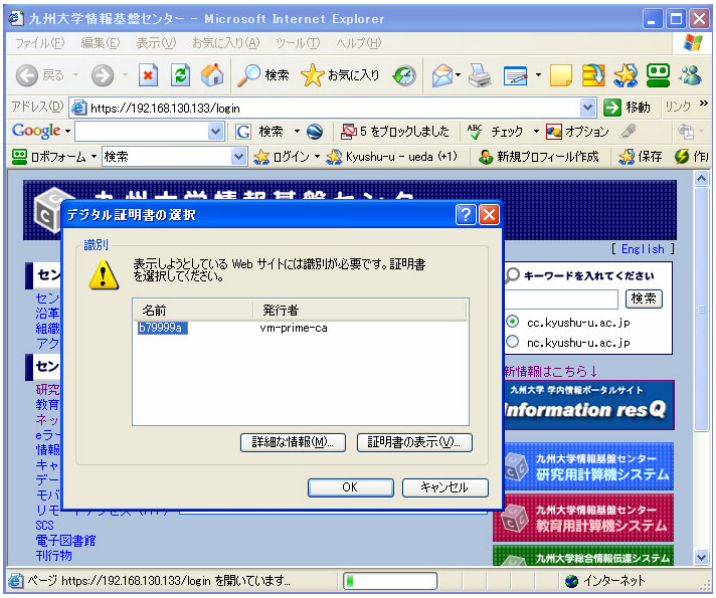

図 7 Web ポータルへのアクセス（証明書の選択）

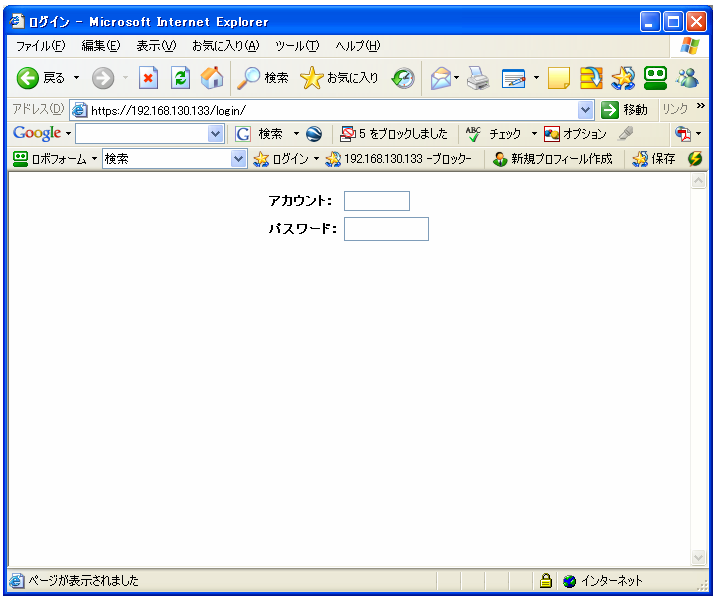

図 8 Web ポータルログイン画面

今回のテストでは CA・DB・WWW をすべて同一のマシンにインストールしたが、今後は実際の運用に即して個別にサーバを立てて LDAP などとの連携をとった環境を構築していきたい。

4. セミナーで学んだ技術および知識

PKI に関する種々の技術

参考 URL

研修時

PKI 関連技術解説

http://www.ipa.go.jp/security/pki/index.html

事前に教えていただいていたものだが『PKI 用語集』が大変役に立った。

研修終了後

SSL 用証明書の作成(Linux 編)

http://www.aconus.com/~oyaji/www/certs_linux.htm

OpenSSL を用いた証明書の作成手順が非常にわかりやすかった。

5. 事前準備として必要と思われるもの

・CA 等の構築

とりあえず一度構築して PKI に触れてみたほうがよかったと思う。

・課題の設定

課題のテーマ設定にかなりの時間を要してしまった。可能であれば事前にいくつかの候補を挙げておいたほうがよい。

6. セミナーの感想

7 月の軽井沢という快適な環境の中で、4 日間研修に集中することができました。講師や受講者やスタッフの方々から、講義中はもちろん食事中などにも貴重な意見をいただくことができ大変有意義な研修であったと思います。

この場を借りて心より厚くお礼申し上げます。