ネットワークを経由した実験装置の遠隔操作のための認証基盤の構築

橋本清治

高エネルギー加速器研究機構　計算科学センター

概要

ネットワークに接続された実験装置をインターネット経由で遠隔操作する場合、ユーザ認証や操作に対するアクセス権限の管理などセキュリティ面を十分に整える必要がある。高エネルギー加速器研究機構では、情報セキュリティ技術の一つである PKI(Public Key Infrastructure)を構築して、ネットワークを経由した遠隔操作のユーザ認証に電子証明書を用いた環境の整備を行っている。現在までに KEK ネットワーク上にインターネットを経由した遠隔操作システムおよびオープンソースを利用した PKI を構築し、遠隔操作システムのユーザ認証に電子証明書を用いるためのテスト環境を構築した。

1　構築した環境

今回構築した環境は、電子証明書の申請受け付けや証明書発行を行う認証局とユーザ認証および装置の制御を行う遠隔操作アプリケーションの 2 つのシステムに分けられる。

1.1　認証局

今回構築した認証局は、

- 電子証明書の申請受け付け・登録・発行を行うアプリケーション
- 証明書を発行するまでに作成される各種中間データを格納するためのデータベース
- 発行された証明書や証明書失効リストを格納するためのディレクトリ

で構成される。これらはオープンソースを利用し構築している。利用したソフトウェアとバージョンを表 1 にまとめた。

表 1.　利用ソフトウェア一覧

認証局、登録局、申請受付サーバ	OpenCA0.9.1.2, OpenSSL0.9.7c
ディレクトリ	OpenLDAP2.1.22
データベース	Postgres7.3.2
WEB サーバ	Apache1.3.28, mod_python2.7.8, mod_ssl2.8.15-1.3.28
使用言語	Python2.2.2, perl5.8.0

1.2　遠隔操作アプリケーション

今回のアプリケーションには遠隔操作用の装置を用意した。この装置を操作するには、遠隔操作用 WEB サーバにアクセスし、操作用ページの HTML フォームから値を入力して Python で記述されたモジュールに値を渡す。この Python モジュールから装置へ値を反映させて装置の状態を変化させる。またこの装置の様子はネットワークカメラによってネットワークへ配信されており、ユーザは装置の状態を確認しながら操作ができるようになっている。

上記のサーバ、アプリケーションを KEK ネットワークに接続する。KEK ネットワークにはファイアウォールが導入されているので外部と通信を行う必要があるものについては DMZ へ接続し、外部と通信が発生しないものは KEK 内部ネットワークへ接続する。構築した環境の構成図を図 1 に示す。

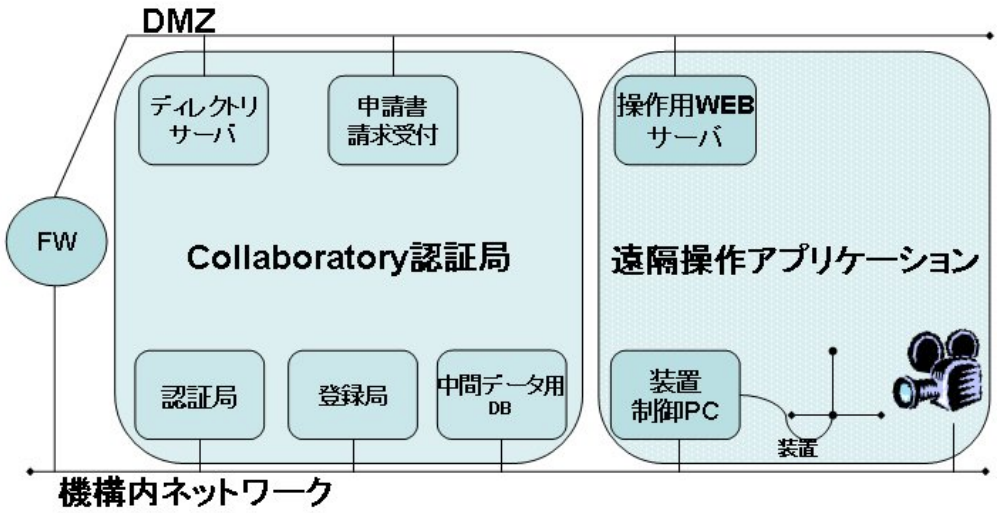

図 1.) 構成図

2　認証局の構築

今回の認証局を構築するために使用した OpenCA は、OpenSSL を CGI から利用する WEB ベースの PKI 構築パッケージである。OpenCA を使用することで、利用者からの電子証明書発行および破棄請求、管理者による証明書や証明書失効リストの発行が WEB ページを経由して可能になる。認証局の構築にあたって以下の作業が最低限必要となる。

2.1　認証局のタイプの決定

一般的に認証局には、認証局自身の電子証明書を第三者信用機関に署名してもらうタイプと自身の証明書を認証局が自分で署名する自己署名タイプの認証局がある。第三者信用機関署名タイプの認証局は、その認証局の信用を第三者機関に証明してもらえるため信頼性が高くなる。今回はテスト構築でありさほど信頼性を要求しなくとも問題ないため、自己署名タイプの認証局を構築した。

2.2　認証局の名前の決定

発行される証明書にはどこの認証局が発行したのか認証局の名前が記述される。認証局の名前は DN(Distinguished Name)形式であらわされる。また認証局名はインターネット上では一意になる必要がある。今回構築した認証局の名前は以下にした。今後この認証局を Collaboratory 認証局と記す。

DN=C=JP, O=KEK, OU=Collaboratory, CN=Collaboratory CA/emailAddress=camanager@adhoc2.kek.jp

2.3　認証局の秘密鍵・公開鍵ペアと CA 証明書の作成

Collaboratory 認証局自身の秘密鍵・公開鍵ペアおよび CA 証明書を作成する。利用者に対して電子証明書を発行するために認証局の秘密鍵が必要になる。公開鍵を含む CA 証明書は、アプリケーションや利用者がこの証明書から発行された証明書を検証するために必要になる。作成した CA 証明書はディレクトリや WEB 経由で利用者が取得できるようにしておく。図 2 に認証局の CA 証明書を示す。

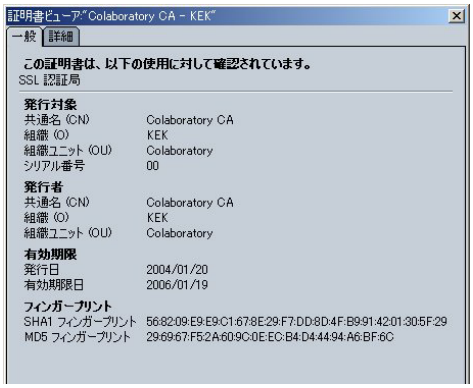

図 2.) CA 証明書

2.4　管理者の秘密鍵・公開鍵ペアと電子証明書の作成

この認証局における管理者の秘密鍵･公開鍵ペアと電子証明書を作成する。この鍵ペアと証明書は管理者の端末にインストールしてブラウザで使用可能にしておく。管理者の仕事は、利用者からの証明書発行請求の承認や証明書の失効など認証局を管理するためのマスタユーザとなる。図 3 に管理者用証明書を示す。

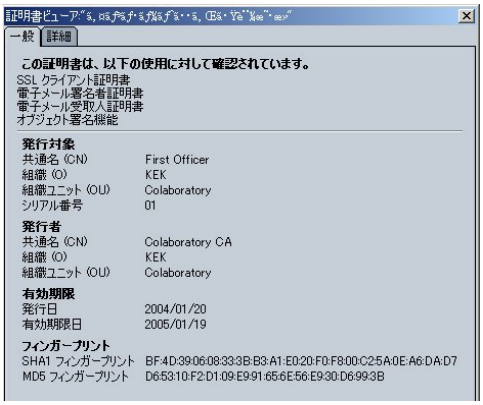

図 3.） 管理者用証明書

2.5　登録局のサーバ証明書の作成

登録局のサーバ証明書を作成する。このサーバ証明書は、管理者が登録局へ WEB アクセスする際の SSL サーバ認証に使用される。

ここまでで認証局の構築は終了となり、利用者からの証明書発行申請の受け付けや電子証明書の発行が可能になる。

3　遠隔操作用 WEB サーバの電子証明書の作成

遠隔操作用 WEB サーバにアクセスできるのは Collaboratory 認証局が発行した証明書を持つユーザだけにしたい。このため遠隔操作用 WEB サーバとユーザのブラウザ間で SSL サーバ・SSL クライアント認証を行う。SSL サーバ認証によってユーザ（ブラウザ）は WEB サーバを認証でき、SSL クライアント認証によって WEB サーバはユーザ（ブラウザ）を認証できる。この認証のためには遠隔操作用 WEB サーバの電子証明書を以下の手順で Collaboratory 認証局に発行してもらい、必要な設定を WEB サーバに実施する。

3.1　遠隔操作用 WEB サーバの名前の決定

DN 形式の名前を決定する。WEB サーバの DN の場合、CN(Common Name)にはサーバの FQDN(Fully Qualified Domain Name)を指定する。このサーバの DN は以下のとおりとした。

DN=C=JP, O=KEK, OU=Pendulum, CN=pendulum.kek.jp

```
#WEB サーバの証明書の指定
SSLCertificateFile /usr/local/apache/ssl/pendulum.cer
#WEB サーバの秘密鍵の指定
SSLCertificateKeyFile /usr/local/apache/ssl/pendulum.key
#CA 証明書のパス(1 行目）と CA 証明書を指定(2 行目)
SSLCACertificatePath /usr/local/OpenCA/var/crypto/cacerts/
SSLCACertificateFile /usr/local/OpenCA/var/crypto/cacerts/cacert.pem
#SSL クライアント認証を要求するよう設定
<Directory /usr/local/apache/htdocs/pendulum>
    SSLVerifyClient    require
    SSLVerifyDepth    10
</Directory>
```

図 5.） httpd.conf の設定例

3.2　WEB サーバの秘密鍵･公開鍵ペアと証明書署名要求の作成

WEB サーバ上で OpenSSL を使って秘密鍵･公開鍵ペアと証明書署名要求を作成する。この証明書署名要求を Collaboratory 認証局へ申請受付ページのフォーム経由でアップロードする。

3.3　WEB サーバ用証明書の発行

証明書発行申請を受けた Collaboratory 認証局では、登録局による証明書申請の承認を経て認証局において署名し証明書を発行する。

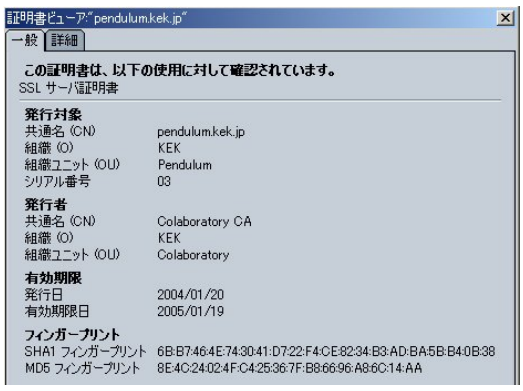

図 6.） 遠隔操作用 WEB サーバの証明書

3.4　証明書の取得

発行された証明書と Collaboratory 認証局の CA 証明書を WEB サーバに取得し、WEB サーバで必要な設定を行う。Apache において SSL クライアント認証を行うための http.conf の設定例を図 5 に示し、遠隔操作用 WEB サーバの電子証明書を図 6 に示す。

4　利用ユーザの電子証明書の作成

ユーザは、装置をコントロールするために Collaboratory 認証局から電子証明書を発行してもらう必要がある。以下にユーザの証明書を取得するまでの流れを示す。

4.1　ユーザの秘密鍵・公開鍵ペアと証明書署名要求の作成

電子証明書を取得するために受付 WEB サーバに接続し、フォームに氏名、メイルアドレス、生成する鍵の長さなど必要事項を記入しサブミットする。この時にユーザ側のブラウザによって秘密鍵と公開鍵のペアおよび証明書署名要求が作成される。作成された証明書署名要求は Collaboratory 認証局へアップロードされデータベースに格納される。ユーザの DN は、以下のように CN にユーザの氏名を入力したものになる。

DN=C=JP, O=KEK, OU=Pendulum, CN=Kiyoharu Hashimoto

4.2　ユーザ用電子証明書の発行

証明書発行申請を受けた Collaboratory 認証局では、登録局による証明書申請の承認を経て認証局において署名しユーザの電子証明書を発行する。証明書発行後、ユーザの公開鍵を含む電子証明書をディレクトリに登録し、ユーザに対して証明書の入手方法が記載されたメイルを送る。登録局からのメイルを受け取ったユーザは、メイルに書かれた方法で自分の端末に証明書を取得する。

電子証明書を取得したユーザは、操作用 WEB サーバにアクセスし SSL クライアント認証によるユーザ認証に成功した後に操作用のページを表示でき、実際に装置を操作可能となる。

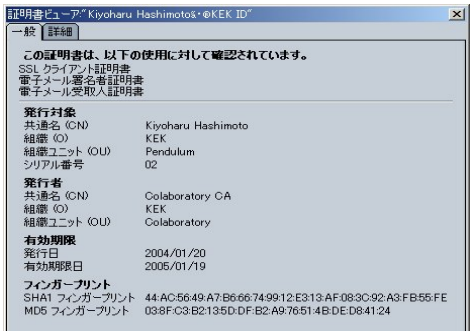

図 7.) ユーザの電子証明書

5　まとめ

認証基盤として PKI を整備し、この認証局から発行された電子証明書を持つユーザだけがネットワークに接続された装置を操作可能となる環境を構築した。電子証明書の発行請求や発行などほぼ期待したとおりに動き、遠隔操作アプリケーションのユーザ認証も問題なく動作した。PKI はオープンソースを利用して構築した。市販の PKI 製品と比べて構築までに多くの時間や労力が必要となるが、市販の PKI 製品は高額であり、安価に構築できる OpenCA は今回のような用途に有効である。今後は電子証明書ベースのアクセス権限管理の実装を進めていく。

参考文献

[1]　塚田 孝則, “企業システムのための PKI”, 日系 BP 社

[2]　OpenCA Labs, http://www.openca.org/