# セキュアな個人認証環境構築への取り組み

橋本清治

高エネルギー加速器研究機構　共通基盤研究施設

## 1　はじめに

高エネルギー加速器研究機構(KEK)では大型加速器や測定装置などの物理実験装置を用いて様々な研究プロジェクトが進められており、国内外の研究機関や大学の研究者が参加して共同で実験が行われている。機構の計算機資源やネットワーク環境は様々な立場の研究者によって利用される。計算機資源やネットワーク環境を利用するために利用者を正しく本人であることを確認するための個人認証が必要となるが、このような状況に合わせて安全を確保しつつユーザの利便性が失われないような個人認証環境が必要となる。

安全な個人認証を実現するための技術として電子証明書を用いる認証技術がある。電子証明書を用いた個人認証を実現するためには認証局の構築が必要となる。認証局の構築には主にアウトソース型とインハウス型とあり両者でかかる経済的コストや人的コストにおいて違いがある。また、電子証明書を IC カードに格納することで安全性を高め、同時に常に持ち歩くものという携帯性を持たせることで複数の場所や移動先で利用できるようになり利便性が向上すると考えられる。

## 2　アウトソース型／インハウス型認証局の構築

自組織内で電子証明書を利用する個人認証を実現するには、まず電子証明書を発行するための認証局が必要になる。認証局の構築には、認証局の構築及び運用を外部に委託するアウトソース型と認証局を自組織内設備で構築し運用するインハウス型とあり、それぞれにメリットとデメリットがある。

アウトソース型の認証局は、導入から運用までを迅速に行うことができ、サーバ機器の準備、認証局の管理や運用を行うための担当者への教育や実運用にかかる負担を軽減できる。しかし、認証局の導入及び維持するための費用が発生するため、証明書 1 枚あたりの単価は高くなる。実験参加のために訪れる多数の共同利用ユーザに対してこの認証局から証明書を発行することは、金額面では相当の負担になる。

これに対してインハウス型の認証局は、導入から運用までかかる時間や機材の調達、導入作業、担当者の教育や運用管理にかかる負担は大きい。しかし、一度認証局が稼動すれば維持費用についてアウトソース型のように大きくは発生せず証明書一枚あたりの単価はずっと安くなる。

表 1.　認証局タイプのコストと主となる証明書発行対象者

| 認証局タイプ | 導入コスト | | 運用コスト | | 主となる証明書発行対象 |
|---|---|---|---|---|---|
| | 人的 | 経済的 | 人的 | 経済的 | |
| アウトソース型 | 低 | 高 | 低 | 高 | 共同利用ユーザ |
| インハウス型 | 高 | 高 | 高 | 低 | 組織スタッフ |

発行された電子証明書は IC カードに格納する。IC カードのインターフェイスには接触型及び非接触型がある。接触型のインターフェイスの標準規格として ISO7816 があり、非接触型のインターフェイスの標準規格として ISO1444 TypeA,TypeB や FeliCa がある。ユーザの端末で IC カードを利用するために IC カードリーダが必要となる。IC カードリーダと端末は USB、RS-232C、PCMCIA などのインターフェイスで接続される。

表 2.　IC カードと IC カードリーダ

| IC カード | | IC カードリーダ | | プラットホーム |
|---|---|---|---|---|
| インターフェース | 規格 | 製品名 | インターフェース | |
| ハイブリッド<br>(接触/非接触) | ISO7816/<br>FeliCa | OmniKey<br>CardMan3021/<br>4040 | USB/PCMCIA | Windows/MacOSX<br>Linux |
| FeliCa デュアル<br>(非接触) | FeliCa | Sony<br>PaSoRi | USB | Windows のみ |

## 2.1　アウトソース型認証局

アウトソース型の認証局を構築するにあたっては、証明書発行業務(IA)、登録業務(RA)における証明書発行申請の受け付け業務、IC カード発行業務を外部に委託した。IC カードは 1 枚のカードに ISO7816 方式の接触型インターフェイス及び FeliCa 方式の非接触型インターフェイスを搭載して別々の用途で使用できるようにしたハイブリッドカードタイプを用いた。IC カードリーダには USB で端末と接続ができる OmniKey 社製の CardMan3021 と PCMCIA で端末と接続ができる CardMan4040 を用いた。利用プラットホームは Windows、MacOSX、Linux とした。

実際に認証局が稼動するまでに委託先の技術担当者と複数回の打ち合わせを持ち

- 認証局の名前
- 証明書に記載するフィールド名の取り決め
- IC カードの券面に印刷する項目
- FeliCa 部に書き込む値

などについて検討し、これらについて全て決定して最終的に認証局が立ち上がった。またプライベート証明書に加えてベリサイン社のパブリック S/MIME 証明書も IC カードに格納することとした。アウトソース認証局での担当者の主な業務は、対面による利用者の確認及び証明書発行申請の承認となる。


図 1.　ハイブリッドタイプの IC カード

## 2.2　インハウス型認証局

インハウス型の認証局の構築はオープンソースソフトウェアを組み合わせた。発行業務、登録業務を行う認証局ソフトウェアには、国立情報学研究所が開発した NAREGI-CA ソフトウェア[1]を用い、ディレクトリサーバには OpenLDAP を用いた。NAREGI-CA ソフトウェアについて構築前に機能検証を実施し、検証作業において確認された挙動などについて NAREGI-CA 開発者に対してヒアリングを行った。また、証明書発行業務の効率化のために、iscert を開発した。iscert は NAREGI-CA 環境において電子証明書の

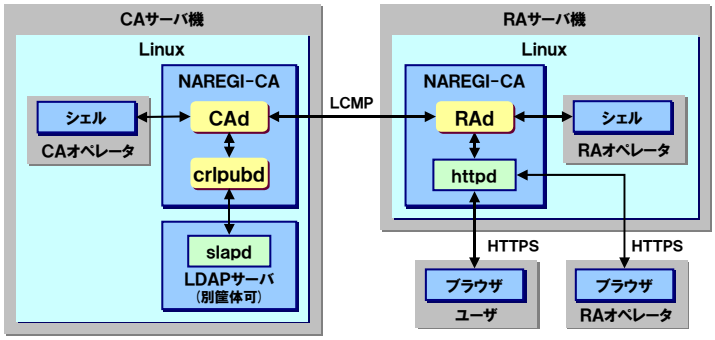


図 2.　インハウス型認証局構成図

発行、失効や発行済電子証明書の一覧表示を行うことができる。さらに複数のユーザに対する証明書の発行及び失効の操作を一度に実行することができる。これにより有効期限切れ証明書の一括失効などが簡単に行える。IC カードには一つのチップで接触型と非接触型の両方に対応している FeliCa デュアルインターフェイスタイプを用いた。カードリーダには USB で端末と接続ができる Sony 社製の PaSoRi を用い利用プラットホームは Windows のみとした。インハウス型認証局での担当者の主な業務は、対面による利用者の確認、証明書発行申請受付け、発行申請の承認、証明書の発行となる。

## 3　本認証局発行の電子証明書による個人認証の検証

今回構築した２つの認証局から発行された電子証明書を IC カードに格納してそれを用いて正しく個人認証が働くかどうか検証を行った。検証項目は実運用を想定したものを選定している。これまでに SSL-VPN 方式によるリモートアクセスのための個人認証、EAP-TLS 方式による無線 LAN 接続のための 802.1X 認証[2]、機構内製のウェブアプリケーションを利用するための個人認証について検証を行った。

その結果、IC カードを利用するためのソフトウェアのセットアップに不明確な点があり、導入容易性に問題点が見受けられるといった問題点があるが、これはドキュメントを整備するなど運用である程度回避できる問題であり、主となる各検証項目の個人認証に関わる部分に問題は見受けられなかった。

## 4　まとめ

KEK のような計算機資源やネットワーク環境を関係する様々な立場の研究者が利用するような環境において、電子証明書による認証技術を用いて利用者にとって安全で利便性の高い個人認証環境を提供することを目指して、アウトソース型の認証局とインハウス型の認証局を構築した。また、電子証明書を IC カードに格納して安全性や利便性を高めるために接触、非接触、FeliCa デュアルインターフェイスなど複数方式の IC カードを導入した。

アウトソース型の認証局は導入や運用が容易ではあるが維持費用が大きくかかるという特徴があり、インハウス型の認証局は導入や運用のコストは大きいが維持費用は少ないという特徴がある。運用に際してはそれぞれの特質を見極める必要がある。

今回構築した個人認証環境のセキュリティ強度について問題はなく、検証の結果からも実運用下での個人認証に供することに問題はないと考えられる。

今後は

- 認証局の CP/CPS の作成
- 機構職員が持つ磁気カードや J-PARC で使われている FeliCa カードなどで行っている建屋、実験施設等への入退室管理システムとの連携

などが大きな課題である。

## 参考文献等

[1]　NAREGI-CA, http://www.naregi.org/index.html

[2]　手島　直哉、青柳　哲雄、橋本　清治、真鍋　篤、湯浅　富久子、中島　憲宏、“J-PARC 情報システムグループ認証システムグループによる IC カード PKI 認証方式のフィージビリティ・スタディ実施報告”