

平成 19 年 8 月 3 1 日

## 平成 19 年度情報処理軽井沢セミナーレポート

横浜国立大学 情報基盤センター

徐 浩源

### 1. 課題のタイトル

ユニーク ID を用いる IC カード+PKI による統一認証基盤構築の検討

### 2. 1 の概要

添付の通り

### 3. セミナーで学んだ技術及び知識

- ・ PKI 技術の概要、電子署名の仕組みと検証方法、認証局の仕組みと信頼性、PKI の構成、電子署名及び認証業務に関する法律などを学びました。
- ・ UPKI の概要、UPKI の 3 階層の考え方、UPKI の共通仕様、WebTrust 対応証明書発行(サーバ証明書)、及びキャンパス PKI の事例(東京工業大学など)を学びました。
- ・ 認証・認可方法について、オープンソースの Shibboleth の概要について講義を受けました。Shibboleth の動作などについて実習によって検証しました。また Shibboleth に関する海外の最新動向についても勉強しました。
- ・ グリッド利用のための認証について、UPKI とグリッド用認証局の仕組みと運用に関する講義を受けました。
- ・

### 4. セミナーの成果

(今後、所属機関において何を計画し、どのように進めていくかの展望について)

- ・ 今回のセミナーの参加により、UPKI など IT キャンパスを実現する認証基盤の構築に関する参考情報を得ることができました。現在議論中の本学の統一認証基盤の構築に関する問題点や認証方式などについて整理・検討を行ったうえ、具体的な実施計画を作っていく考えです。

### 5. セミナーの事前、事後において、参考になった URL とその簡単な内容紹介(1行程度で)

- ・ 参考になった PKI に関する情報 IPA のサイトは、以下です。

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

## 6. 事前準備として知っておいた方が良かったと思われること

(不足していたソフトウェアや予習事項等)

・事前に PKI の仕組みに関する知識・用語、UPKI の情報などを予習してからセミナーに参加するのが効果的だと思います。

## 7. セミナーの感想

大学の IT 環境のなかで、統一認証基盤は非常に重要な位置づけとなっています。しかし、実際統一認証基盤を構築しようとする際に難しい課題がまだまだたくさんあります。今回のセミナーは、こう言った課題を解決するために参考になる有用な情報を提供してくれました。セミナーは PKI や UPKI などに関する知識を学ぶ以外、他大学の認証基盤の整備状況などについての情報交換もできて、大変有意義な研修だと思います。

## 8. 備考、その他

今回のセミナーを企画・運営して下さった NII の講師陣と関係者に感謝の意を表したいと思います。研修で学んだことを本学の統一認証基盤の整備に活用して行きたいと考えています。

# ユニークIDを用いる ICカード+PKIによる統一認 証基盤構築の検討

横浜国立大学  
情報基盤センター  
徐 浩源

## 現状と問題点(1)

- 縦割り型の組織システムによる複雑なID管理問題
  - 学務部のシステム
  - 情報基盤センターのシステム
  - 学部独自の各種システム
  - 事務処理システム
  - 新しいシステムが増加中……

## 現状と問題点(2)

- 学務部のシステム
  - 履修登録システム
  - 証明書発行システム
  - 学生情報システム……
- 情報基盤センター
  - 電子メール
  - 教室PC利用
  - Unixサーバ利用
  - 授業支援システム(LMS)の利用
  - 無線LANの利用、認証ネットワークの利用

## 現状と問題点(3)

- 図書館
  - 図書館利用カード、利用者情報管理  
(独自のIDは学務のデータに基づいて作成。)
- 学部独自の各種システム
  - 語学事前登録システム
  - 複数メーカーの語学支援システム
- 事務
  - 物品購入管理
  - 教育・研究業績管理
  - 財務など

## 現状と問題点(4)

- 利用者にとって
  - 複数のIDとPW、覚えにくい
  - 利用時の混乱 ⇒ ときには授業の運営に影響
  - PW管理上のセキュリティ問題
- 運用管理側にとって
  - システム管理の複雑さが増し
  - セキュリティ脅威
  - 複数のシステム⇒コスト↑:重複投資、重複作業、

## 現在の身分証明書(カード)

- 学生
  - プラスチックカード(磁気テープ)+バーコード
  - 磁気テープの用途:学務、情報基盤センター利用
  - バーコードの用途:図書館利用
- 職員
  - 紙+バーコード
  - 紙:身分のID情報+写真
  - バーコード:図書館利用
- 大学入構、建物の入退出
  - 別途の磁気カード発行(車通勤用、単年度)
  - 各部局発行の各種入退出カード

## 理想と目標:統一認証基盤

### 統一認証基盤

- 全構成員に統一の身分証明書カードを新規発行
  - ・ IC+磁気テープカード (ハイブリッド)
  - ・ 接触 非接触 (カードリーダー)
  - ・ キーワード: ユニークID/PW+PKI
- 構成員の統一LDAP(データベース)
- CA局による全構成員に電子証明書発行(ICカード)
- 組織・管理体制
  - ・ システム管理:情報基盤センター
  - ・ 運用管理:教職員は人事部門、学生は学務部

## ICカード発行対象と管理体制

- 大学の構成員(1)
  - ・ 学生の範囲定義
    - ①身分証明書あり  
正規学部生、大学院生、研究生、科目聴講生  
交換留学生、短期語学留学生、
    - ②(これまで)身分証明書ない  
連合大学院生(発行の条件、要検討(\*))
    - ③ポストドクター(特別研究員)

## ICカード発行対象と管理体制

- 大学の構成員(2)
  - ・ 教員
    - ①身分証明書発行:常勤教員
    - ②身分証明書発行基準ない:非常勤教員(\*)
  - ・ 職員
    - ①身分証明書発行:常勤職員
    - ②身分証明書発行基準ない:非常勤職員(\*)
  - ・ その他
    - ①特命教員、客員教員、臨時人員

## ICカード発行対象と管理体制

- ICカードの発行対象及び管理ポリシー
  - ・ 管理・責任部署(ユニークIDの割り当て、電子証明書)
    - ①学生について ⇒ 学務部
    - ②教職員について ⇒ 人事部門
  - ・ 学部・部局は(ユニークID、電子証明書)を参照・利用
- ICカードの発行体制(カード会社利用の検討)
  - ・ アウトソーシング(外注、コストダウン)
  - ・ 学内体制(人事+学務)
  - ・ 生協との連携
- ICカード発行費用について
  - ・ 初回無料、2回以降有料

## ユニークIDについて

- ICカード発行対象者にユニークIDを付与
  - ・ ユニークID  
16桁英数字(個人基礎番号に相当)
- ユニークIDは卒業後も所有
- 最終目標:各サービスはユニークIDと連動
  - ・ 図書館(過渡期:バーコードと併用)
  - ・ 情報基盤センター(過渡期:磁気テープと併用)  
ユニークID⇔ログインID(個人定義可) と対応
  - ・ 学生・教職員への各種サービス:履修登録、...

## 統一認証基盤に展開するサービス

- 基幹サービス: Webポータルサービス
- これまでのカードとIDの統合により
  - ・ 各種サービスの展開  
学務、図書館、情報基盤センター、事務局、  
入退出、生協の現金カードのサービス
- SSO方式(認証+認可)とLDAP連携
  - ・ 認証:マスターLDAP
  - ・ 認可:ローカルLDAP+Shibboleth

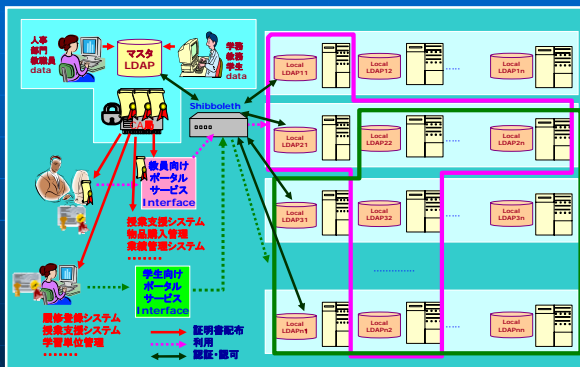
## 連携可能なサービス

- 学生の各種証明書発行管理
- 履修登録管理
- 授業支援システム
- 他大学と単位交換授業の管理
- 物品購入管理
- 人事業務管理・評価システム
- 学生情報管理システム(成績、出席管理・・・)
- 財務管理
- 特許・知的財産管理
- (車の)大学の入構管理、建物の入室管理

## システム構築例

- ポータルサービスシステム
  - 学生向け
    - 履修登録、シラバス、学習管理、授業支援、休講情報
    - 各種情報：電子ジャーナル、リモートシステム
    - キャンパスライフ情報
  - 教員向け
    - 授業支援、学務関連サービス、物品購入管理・・・
  - 職員向け：・・・
  - 広報・発信：・・・

## ポータルサービスの認証・認可方式



## 検討課題

- ICカード化とユニークID導入の利欠点の説明、経営陣のPositiveな判断を促し学内の理解を求める
- ICカードとユニークIDの運用体制(人事、学務)
- ICカード発行コスト/外注運用費予算化
- 発行対象の基準、再発行時の利用者負担
- 段階的にCA局と証明書運用発行の導入
- ICカードとクレジットカード及び生協との連携(利益)
- ユニークID/ICカード利用移行計画(部局間連携)
- 利用促進の開発と支援体制