成城大学
メディアネットワークセンター
五十嵐　一浩

大学間無線 LAN 共有に向けたPKI 導入検討

学内 PKI の必要性

- 大学間サービス連携に必須
- 最終目標は UPKI へ参加
- ID,パスワード運用の限界
  - 学生は在学中しか利用できない ID のパスワードを忘れやすい、貸し借りも頻繁
  - 教員は自動ログオン設定、学生に操作させているケースも多い

文系大学が提供できるリソースは？

- 学内全域（建物内）に WLAN を提供中
  - 非常勤教員、学会参加者、自宅が近い他大学の学生等へ WLAN 接続を提供可能
- 所属大学以外のキャンパスを利用することでシステム以外の副次的な刺激も期待
- 成城大学にとっても同じメリットが享受できる

証明書ベースの認証が必要な理由

- 他大学の学生であり、且つ利用資格を確認する一番効率的な方法
- 比較的自由に出入り可能なキャンパス内の WLAN を防御するのに有効
  - Brute force に耐えうるパスワードを全学生に設定させるのはほぼ無理
  - 定期的なパスワード変更を強制するとパスワード忘れが増加

実現方法(1)

- 実験的な位置付けで希望者のみを対象とした実績を作り、予算を確保していく必要がある。
- CA を低コストで構築する必要あり（必然的にオープンソース）
- 希望者が簡単に申請できなければならない

→　NAREGI-CA を利用

実現方法(2)

- 証明書の保存先
  - 希望者の 所有 PC へ

    2009 年に IC カードの全学導入が検討されているが、Felica に決まる可能性が高い。

    学内常設 PC は全て Laptop で、外付けリーダーの設置が困難なため、PC ログインについては証明書ベースでなく Idm と紐付けることになる。

    今回の実習で IC カード用アプリケーションの OS, Patchlevel 依存度が高いことを実感したこともあり、常設 PC 用のサービスとしては展開が難しい。

実現方法(3)

- 学内 WLAN に接続環境構築
  - 学外者専用 SSID を作成
    1. 802.1x 認証プロファイルを紐付け
    2. 専用 VLAN 作成
    3. Radius Proxy を構成
    4. Radius の UDP は L2TP 等でトンネル経由?

実現方法(4)

- 連携先組織との調整
  - 今回の研修参加大学の中から実験的に始めていきたい
- Eduroam への参加が近道？
  - 参加のためのシステム必須要件確認が先？
  - 参加に十分なクレデンシャルを満たせるか？(特にCP/CPS 監査とファシリティ・マネージメント）

本運用への課題

- 大学として CS/CPS の作成、監査タスクなど含めて、リソースをどう確保するか？
- 実験から本格的な運用へ移行する際、教授会等で承認が得られるのか？
- 学内の既存 AD と連携させていけるのか？そもそも Windows の CA で UPKI に参加できる？
- Felica ベースの IC ソリューション・インフラを変更できるか？