平成 20 年度 情報処理軽井沢セミナーレポート

成城大学 メディアネットワークセンター
五十嵐 一浩

■参加動機とセミナーでの課題

成城大学では 2009 年 4 月に学内教室用 PC 500 台のリプレイスを控えており、同時に学生証の IC カード化検討も進められている。キャンパス PKI を構築するには絶好の機会であるため、学内認証局運用に必要な実務知識を習得し、学術教育研究機関相互連携に向けての第一歩を踏み出すことを目標としたい。

■発表内容

テーマ:「大学間無線 LAN 共有に向けた PKI 導入検討」

我々が所属する学術教育機関の使命の一つとして、広範囲な学習・研究環境を学生に提供し、世界に誇れる人材を育成することが挙げられるが、大学間連携はその役割の主要部分を担うと感じている。CSI 構想や UPKI はまさにその理想を現実化してくれると信じているが、文系私立大学のシステム部署主導という制約の中で、参加に向けてどのように最初の一歩を踏み出していけるのか、実装可能なアプローチを検討してみた。

現在、成城大学ではユーザーID とパスワードによる認証を Active Directory で管理している。学生にとっては、在学期間中しか有効でないアカウントの魅力は薄いようで、学生間での ID・パスワード貸借が頻繁に発生している。また、教員の中にも PC を自動ログインで利用していたり、学生に PC 管理を任せるなど、学内で本人確認を軽視する風潮があるため、認証強化の必要性という観点からもキャンパス PKI 実装への期待を感じていた。

2007 年 10 月に整備したキャンパス内建物全域をカバーする無線 LAN 環境は、システム部門主導の大学間連携を進める上で、本学からの唯一提供可能なリソースであると思われる。近隣居住の学生、非常勤教員、学会参加者らに対して申請を要せず無線 LAN インフラを提供できれば、役割の一旦を果たすと共に、今後の連携展開のトリガーとなり得る。特に学生にとっては、自分の所属大学以外のキャンパスに触れることで、システム連携以外にも副次的な刺激効果が期待できるのではないかと考える。現状では認証に 802.1x (PEAP) を採用しているため、ID の貸借を根絶できない限り、利用者の本人特定が困難であり、連携先からの監査要求を満たせない可能性がある。また、比較的出入りの自由な大学キャンパス内では常にクラッカーからの攻撃も意識する必要がある。全学生に Brute Force Attack に耐えうる強度の高いパスワードを設定

させるのは不可能であるし、定期的なパスワード変更ポリシーを設定してしまうとパスワード忘れが増加してしまう。EAP-TLS の採用は、ID 貸借の規制、攻撃からの回避と共に、他大学の学生且つ利用資格を有するというクレデンシャルを確認するための一番効率的な方法となり得る。

実装手順については、あくまで実験的位置付けから開始せざるを得ない関係上、CA を低コストで構築する必要がある。また申請処理の効率化が必須となるため、Web の操作インターフェイスを持つことも大切な要件に挙げられる。今回の実習課題で利用したオープンソースの NAREGI-CA は選択肢の一つである。他の候補としては、運用中の Windows Server で証明書サービスを稼働させ、UPKI での連携方法を評価するという方法も考えた。

発行した証明書は、研修参加前はスマートカードへの格納を想定していたが、学内の学生証 IC カード化方針が非接触式の Felica を軸に展開することになり、また、ハイブリッド IC についてはコストの問題で導入への理解が得られなかった為、利用者の持ち込み PC に保存させる方向でスタートしたい。IC カードリーダーが OS バージョンやパッチレベルに非常に依存度が高いことも今回の NAREGI-CA 構築実習にて体感し、学内常設 PC のパッチ管理への影響も考慮事項として認識した。今回、無線 LAN 認証用途だけに限定すれば、PC への証明書配布が妥当だと判断し、IC カードや USB トークンの活用は次フェーズでの課題とした。

学外者へ提供する学内無線 LAN 環境は、専用 ESSID を設け、802.1x 認証プロファイルを紐づけて、専用 VLAN 経由で接続サービスを提供する。認証用の Radius Proxy については、WAN を通過する UDP パケットを L2TP でトンネリングすべきだと感じるが、接続先が多地点となると実装が困難かとも思われる。

学内での環境整備以上に大切なことは、関東近郊で連携先組織を探し、運用方針や監査手順等を取り決めることである。最初は、軽井沢セミナーの演習を自発的に延長するという形で、研修参加大学の中から始めさせてもらえるのが理想である。CP/CPS の相互評価、実運用や監査にかかるコスト算出の機会としても有効ではないかと思う。個別に連携組織を求めずに、Eduroam へ参加することが CSI 参加への一番の近道なのではないかとも思うが、PEAP でも参加可能であるならば、学内認証局の構築という主題から逸れてしまう可能性もあるので、慎重に検討したい。

実験的な実装であれば、システムとしてなんとか試験運用までは辿り着けそうにも思えるが、システム以外からの視点も含め、今回の講義で学んだ内容を基に、新たに認識した課題にも触れておきたい。

まず、CP/CPS の作成について、ガイドラインとテンプレートを提供していただけたことは、多大

な労力の節減となるが、これまで考慮すらしていなかったファシリティ要件のための工事費用や、監査タスク、運用体制とコスト等、インソースモデルで実装するには大学全体を巻き込んだプロジェクトとして立ち上げる必要性を感じた。インソースモデルでの予算やリソースが確保できない場合、アウトソースを検討することになると思うが、現状では PKI のためだけに大規模な予算編成は難しく、大学連携により享受できるサービスの内容に大きく依存することになるであろう。

他大学との連携では、教育コンテンツの共有、単位互換制度等が想定されるが、それらは教授会、理事会等の承認事項となってしまい、システム部門主導で活性化させるには限界がある。

また、既存学内システムとの整合性という観点から、 Active Directory を廃止することが事実上不可能であるため、CA 用アプリケーションは Windows の証明書サービスを使った組織間連携を検討すべきだとも感じている。Microsoft 社の Whitepaper には Windows Server 間相互認証の解説があり、オープンソース CA との相互認証についても不可能ではないと思われる。

2009 年度から学内で Felica ベースの IC 学生証を配布、段階的な非接触 IC カードサービスの開始が計画されている。将来、証明書の IC カード格納を実現するには、非接触 IC カードインフラの再整備というかなり困難なタスクが追加される。

キャンパス PKI を構築・運用するには、想定以上の体力と負荷がかかることは明白であるが、今後世界をリードしていく優秀な人材を育成するためにも、その困難を乗り越えて実装する価値のあるものと認識している。今後も学内コンセンサスを得られるよう、システム部門として可能な限りのアプローチを続けていきたい。

■セミナー全体の感想

NAREGI-CA 実習はトラブルシュート含みであったために大変実用的な研修になったと思います。集中力の高まる研修環境は、時間が経過するのを忘れる程快適でした。

毎晩遅くまでお付き合いいただいた講師・スタッフの皆様、本当にありがとうございました。

(参考)

Windows Server 2003 の相互認証と認定従属の計画と実装

http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03qswp.mspx

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？