平成 18 年 8 月 29 日

平成 18 年度情報処理軽井沢セミナー　レポート

金沢大学 情報企画課 基盤整備第二係　松平　拓也

今年度テーマ
認証技術を知る　～PKI を中心として～

1. 課題タイトル

「PKI を用いた学内ネットワーク環境の改善」

2. 1 の概要

今回の自由課題が「今後、自分の業務の中で PKI をどのように利用していきたいかを考えてみる」というテーマであり，自分の大学において，どの部分に PKI が導入できるか，導入するメリットがあるか，導入の際にどういったことが問題（課題）として考えられるか等を 1)ユーザの視点，2)運用の視点，3)普及の視点から検討し，最終日に発表するというものであった．

今回自分は，金沢大学で PKI を導入することで，より便利でかつセキュアなネットワーク環境を構築できないか検討してみた．

本課題（発表）の内容については以下の PowerPoint を参照していただきたい．

3. 講義・演習とその成果
（何を計画し，今後どのように進めていくか。セミナーでの発表＋今後の展望について。）

講義・演習については 4 章，最終日の発表（自由研究）・今後の展望については別途以下の PowerPoint を参照していただきたい．

4. セミナーで学んだ技術及び知識

講義では以下のことについて学習した．

・PKI に関する用語の定義・意味，PKI 技術の概要について

PKI 技術を学ぶにあたっては非常に多くの用語があり，自分自身曖昧になっているところが結構多かったが，詳しく説明していただき，しっかりと用語を理解することができた．また，PKI 技術の概要についても学び，自分の中でさらに理解を深めることができた．

・PKI の技術について（基礎）

PKI の技術について，Relying Party（検証者）の立場からどのように証明書を検証し，信用するのかについて学習した．また，認証局の信頼の確保の方法について，PKI の構成について，証明書発行について，X.509 についてもしっかりと学習することができた．

・PKI の技術について（応用）

応用編では，基礎編で学んだ知識を基に，証明書検証の技術，認証局の HSM（Hardware Security Module）について，PKI によるネットワーク認証技術について等，さらに深い内容について学習した．また，PKI 技術の最近の動向についても学ぶことができた．

応用編は詳細な内容まで学ぶことができ，非常に有意義であったと思う．

実習では以下のことを行った．

－実習編その 1－

・PKI 相互運用テストスィート（PKITS）を利用し，CA（認証局）を構築し証明書を発行する．

手順としては以下の通りである．

1．自分の CA を構築する（CA の自己署名証明書を作成する．）

2．この CA の EE（End Entity）の証明書を発行する．

（今回は 1，2 で利用する鍵ペアはあらかじめ作成しておく）

3．自分の CA から階層型 CA モデル TopCA へ CA 証明書を発行する．

1～3 より，認証パスが確立されているか確認する．

4．TopCA をブリッジ CA に見立てて他の参加者の構築した CA との信頼関係を構築する．

4 を行い，自分の信頼点から他の参加者の CA 証明書ユーザの認証パスが確立しているか確認する．

この実習を通じて，鍵ペア，証明書，信頼点，認証パス等のキーワードの意味の理解を深めることができた．

－実習編その 2－

・電子署名とタイムスタンプについて

1．FileSign という電子署名ツール（http://www.epox-c.co.jp/FileSign.htm）を利用してファイルに署名を行う．（証明書はあらかじめ準備してあるものを利用．タイムスタンプなし）

2．ViewBRENT という証明書ダンプツール（http://www.imc.org/ietf-pkix/index.html）を使用し，署名フォーマットを確認する．

3．FileSign で署名の検証を行う．

次にタイムスタンプ付で署名を行い，動作の検証を行う．

この実習を通じて，電子署名とタイムスタンプについて，具体的に理解できるようになった．

5. 事前準備として知っておいたほうが良かったと思われること

講師陣がその分野でのエキスパートであるということもあり，非常に内容が濃いものであったと感じた．そのため，受講前に PKI についての一定の理解をもっている必要があるように思う．

6. セミナーの感想

本セミナーを受講することで，今まで曖昧な部分のあった用語，知識の再確認を行うことができた．また，PKI に関する最先端の研究を行っている講師の方々に懇切丁寧に指導を受けることができ，PKI を勉強するには最適な環境であったと思う．

また，少人数での講義であったため，講師の方々に多くの質問をすることができ，自分にとって有意義な時間を過ごすことができたと思う．

そして，講義時間以外でも様々な大学から来られた参加者と色々と意見を交換することもできたことは少人数の合宿形式ならではの利点であったと感じた．

一つだけ欲を言えば，もう少し実習の内容を充実させたほうがよいのではないかと感じた．

このような充実したセミナーに参加させていただき国立情報学研究所様，講師の方々に感謝の意を申し上げるとともに，本セミナーで学んだことを自分の大学ネットワークに還元できるよう努力していきたいと考えている．

課題発表で用いた資料（Microsoft PowerPoint2003 で作成）

PKIを用いた
学内ネットワーク環境の改善

金沢大学情報部情報企画課
基盤整備第二係
松平　拓也

背景&問題提起

- 平成18年度より入学生全員がノートPC必携義務化
- 無線LANアクセスポイントが全キャンパス間をほぼ網羅
- 現在，無線LAN認証にはEAP-PEAPを採用
- センターのサービス(Webベース)を利用するためには無線LAN，ファイアウォール，各アプリケーションサーバのそれぞれでユーザID，パスワードでの認証が必要

⇩ 何回も入力は大変

PKIを利用してセキュリティレベルを落とさずに認証の手間を減らすことはできないか？

目的を達成するための条件その1

- センターに認証局(RA/CA)を設置
  ⇒全学生のトラストアンカー
- 無線LAN認証にはEAP-TLSを採用
  ⇒PC(サプリカント)がEAP-TLSに対応している必要
- センター管理サーバ(Webベースでの認証)をクライアント証明書での認証に変更(サーバ証明書の発行)

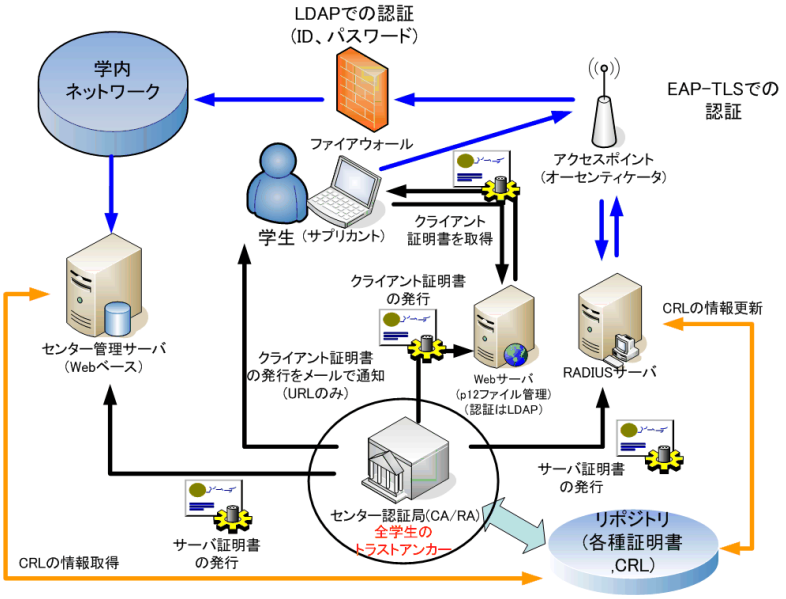
無線LAN，センター管理サーバの認証はID，パスワードを入力する必要がない

- すべてをクライアント証明書で認証すると
  盗難，紛失の際非常に危険
  ⇒ファイアウォールの通過の可否のみ
  ユーザIDとパスワードでの認証(LDAP)

目的を達成するための条件その2

- 学生全員にクライアント証明書を発行
  (全員に配布するため，暗号クレデンシャルをp12形式(PKCS#12)でRA/CA側で生成し，メールで配布先URLのみ通知)
- p12ファイルを管理しているサーバはLDAPで認証
  ⇒あらかじめLDAPサーバへの登録が必要
  (現行は学生証をカードリーダに通して登録)
  (ファイルのダウンロードはhttpsで行う)
- 単にp12ファイルをダウンロードしてインストールするだけではこのファイルの重要性が理解できない．
- 学生は「情報リテラシー」の講義が必須
  ⇒講義でEAP-TLSの設定，Webサーバへのアクセスを通じてPKIの概念を理解してもらう
  (自分の運転免許証等は他人に貸さないだろう)

システム構成図



課題と展望その1

- RA/CAの管理・運用
  RA/CAサーバは強固なセキュリティで保護されている必要
  センターの業務が増える？

- .p12ファイル(暗号クレデンシャル)の管理

[配布サーバ側]
.p12ファイルの耐タンパ性をどうやって確保？
ファイル格納サーバを別途用意
[学生側]
ダウンロードしたp12ファイルはどうやって保存？
別途USB認証トークン等，H/Wトークンに格納すべき？
PCに格納したままではセキュリティ上好ましくない

何か問題が発生した場合に「否認」されたくない

課題と展望その２

- 失効のポリシー作成
  ・盗難・紛失等，第三者に不正利用される危険性が発生したときのみ？誤って削除した場合は再度ダウンロードできる？
  ・一定期間を超えて利用されていないクライアント証明書は失効
  e.g.)履修登録サーバへ年に一度必ずログインしないと失効
- CRL情報の反映
  RADIUS，Webサーバに定期的にCRLチェックを行わせる仕組みを実装する必要がある
- 教職員への利用者層の拡大
  教職員であれば，クライアント証明書の更新頻度が高くないため，USBトークン等のH/Wトークンに格納・配布が可能
  ⇒センターWebサービスへのアクセスの利便化
  さらにはS/MIMEを利用してのメールの交換(学内)が可能に(メールの否認・改ざんを防ぐ)