2006(平成 18)年 8 月 18 日

平成 18 年度情報処理軽井沢セミナーレポート

西南学院大学情報処理センター事務室
田原　裕子

1. 課題タイトル「認証技術を知る －PKI を中心として－」

2. 概要

大学という組織において、PKI によるユーザ認証技術をいかに活用できるのか、どのように導入していけばよいのかということを検討するために必要な、技術、知識を習得する。

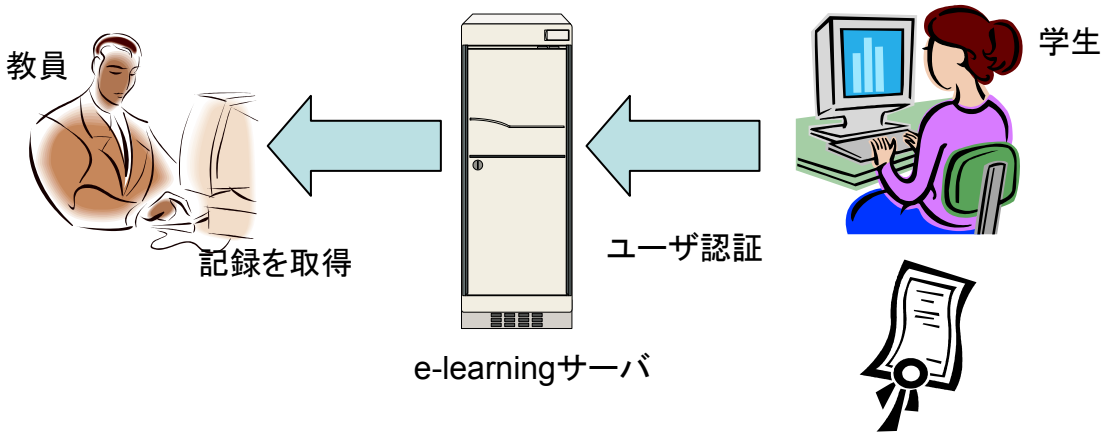
3. 講義・演習とその成果

今回の講義、演習では、PKI 構築に必要な基礎(認証局、署名、X.509 証明書、署名者の要件、検証者の要件など)、応用(証明書検証の技術、認証局の鍵管理、ネットワーク認証技術、公的個人認証サービスなど)について学んだ。

学んだ内容を基に PKI の応用を考えてみたが、いきなり複雑なことに PKI を利用することは困難なため、まず、単純なユーザ認証への利用として、「e-learning システムのユーザ認証における PKI 利用」を計画し、進める場合を考えてみた。

(1) PKI の利用目的

e-learning システムにおける「本人」認証をより確実に行うことを目的とする。現在のユーザ ID とパスワードによる認証では、「本人」がシステムを利用しているのかどうかが、不安な状況である(代理受講、代理受験、なりすましなどの問題)。そのため、PKI を構築、運営し、各ユーザに証明書を発行し、より確実な「本人」認証を行う。これにより、e-learning システムによる受講記録や成績などを正式な成績として採用できるようになると思われる。



(2) 前提

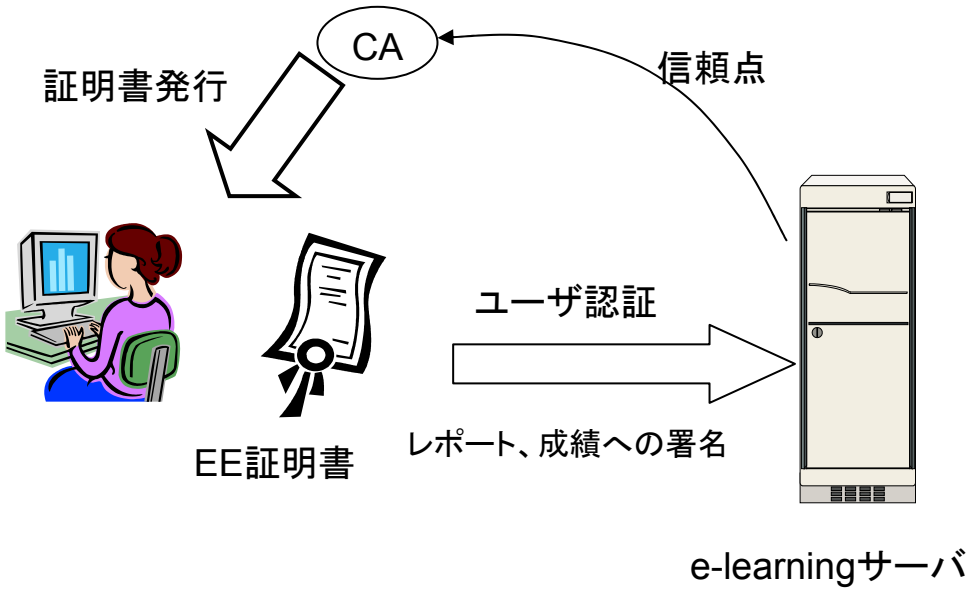
e-learning のユーザ認証において、PKI を利用するために必要な前提条件としては、次のものが挙げられる。

- 学生、教員に署名用証明書が H/W トークンで配布されていること
- 学生、教員が署名可能なアプリケーションを利用できること
- 学生、教員が署名検証アプリケーションを利用できること
- e-learning システムが証明書を使ったユーザ認証に対応していること
- 証明書の有効期限は 4 年とすること

(3) 構成

システムの構成は次のようになる。

- 学内において、CA を 1 つ構築、運営する。
- 学内 CA で、End Entity 証明書を発行し、ユーザに配布する。
- e-learning サーバはクライアント認証を行う。信頼点として、学内 CA を設定する。



(4) PKI 利用におけるメリット、デメリット

- 学生にとってのメリット
  - リモート受講可能
  - 第三者による学習記録、レポート、答案の改ざん防止(安心)
- 教員にとってのメリット
  - e-learning システムの学習記録、答案を成績として採用しやすい
  - 自分が出した成績の改ざん防止
- 学生、教員にとってのデメリット
  - H/W トークンの管理コスト(なくさないよう)

- H/W トークンを使う手間
- 署名操作、署名検証操作の手間

(5) 運用における課題

実際に運用する場合にどのようなことが課題となるか、考えてみた。

・ H/W トークンの安全な配布方法

初期 PIN コードを入れて渡し、すぐに変更するように指導する。できれば、初期 PIN コードに有効期限を設けることができるとうれしい。

・ CA の運用コスト

ユーザが H/W を紛失した場合に、CRL をメンテナンスする必要があり、その手間がかかる。

・ H/W トークン紛失時の対応の徹底

必ず速やかに届出をするように指導しておかなければ、証明書の悪用の可能性もある。

・ PIN コードがわからなくなったときの対応

現在のパスワード方式でも同様の対応が必要だが、PIN コードの場合も同様の対応が必要になると考えられる。

・ H/W トークン、PIN コードについての情報倫理教育、講習会が必要

ほとんどのユーザは H/W トークンを使ったことがなく、使い方から説明が必要。また、H/W トークン、PIN コードの管理がいかに重要なことであるのかの、情報倫理教育も必要。

・ 利用者からの質問対応、サポート

使い方についての質問などに対応する必要がある。

・ レポート、成績データの長期保存対応

証明書期限が切れたものについても確認できるようにしておく必要がある。

・ H/W トークンを忘れてきたときの対応方法の用意

H/W トークンを忘れてしまうと e-learning 授業が受けられないというのでは困るため、他の身分証等で本人確認をし、一時的な証明書の入った H/W トークンを貸し出して対応するといった方法を用意しておく必要がある。

(6) 前提を実現するための課題

・学内に対する啓蒙活動、情報倫理教育

H/W トークンの配布といった前提条件を実現するためには、かなりのコストがかかるため、学内に対する啓蒙活動、情報倫理教育を頻繁に実施し、現在のユーザ認証の脆弱性について訴えていく必要がある。

・H/W トークンを持ってもらうための使い道の用意

H/W トークンの場合、H/W トークンを友人に貸し PIN コードを教えてしまっては意味がないため、PIN コードを教えたくなくなるような H/W トークンの使い道を用意しておく必要がある。パソコンへのログオン、ポータルへの SingleSignOn、入退館システム、図書貸し出し、生協での買い物といった使い道が考えられる。

・各種 OS 対応の署名、署名検証アプリケーションの準備
・最適な H/W トークンの選出

(7) 今後の展望

e-learning システムでの PKI 利用を実現するには、多くのハードルがあるため、短期間での実現は難しい。まずは、啓蒙活動を兼ねて、S/MIME での PKI 利用を試行してみたい。

4. セミナーで学んだ技術及び知識

以下に、参考になった URL とその簡単な内容について列挙する。

http://www.sony.co.jp/Products/puppy/

ハードウェアトークンの例(指認証機能)。USB メモリに証明書を格納。

http://www.ipa.go.jp/security/rfc/RFC3280-04EN.html#42105

RFC3280 Certificate Policies の文章。

http://www.jnsa.org/mpki/index_j.html

PKI 相互運用テストスィートのサイト。実際に相互運用をする場合には動作確認に利用可能。

5. 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

実習の際にいくつかツールを使ったが、その名前と用途については、事前に把握しておいた方が良かった。例えば、ViewBER などは、簡単に利用できるものなので、事前に適当な証明書を表示させてみて、証明書の内容の確認方法などを練習しておけば良かったと思われる。

6. セミナーの感想

実際に認証局の相互運用する場合には、CP や CPS などの詳細、X.509 証明書拡張の詳細などの知識が必要になると思われるが、まだ、その計画にも着手していない段階での詳細な話は、あまり頭に残るものではないかもしれないが、そういった複雑なことまで調整をしていかなければならないという基本的な知識を得ることができ感謝している。また、他大学での証明書利用の現状についても情報を得ることができ、今後の学内での証明書利用についての啓蒙活動に役立てて生きたいと思う。

7. 備考、その他

セミナーは合宿形式で行われた。セミナーの内容自体も有益であるが、講義、演習時間以外の休憩時間や食事の際に、他大学の方との情報交換ができ、そちらも大変有益であった。

以上