平成１８年度軽井沢セミナーレポート

帯広畜産大学　教育研究協力部学術情報課
情報処理センター　遠藤睦美

１．課題タイトル

「Ｗｅｂ上からの端末接続申請見直しについて」

２．１の概要

【端末接続申請の現行の運用について】

- 畜大では、学内に接続する端末の接続申請をＷｅｂ上から行わせている。
- 学生の場合は、指導教員に端末管理責任者になってもらう必要がある。
- 申請後、情報処理センターに申請内容のメールが届く。端末管理責任者にも控えのメールを送信している。
- 接続承認書は端末管理責任者宛てに送付する。

【問題点】

学生が申請するとき、指導教員と相談せずに、勝手に申請をあげてしまうことがある。指導教員の中には控えメールを確認しない人や接続承認書が届いたことすらもわからない人もあり、学生から接続承認されたかどうかの問い合わせが来ることがある。

また、情報処理センター側でも、指導教員の同意が得られているかどうかの確認ができない。

【解決策として電子署名を利用】

指導教員に控えメールを電子署名つきで情報処理センターに返送してもらうことにより、情報処理センター側で指導教員本人の同意が得られていることを確認できる。また、控えメールを返送することにより、指導教員側も申請内容を確認できる。

アカウントサーバにＣＡを作成して、電子署名に必要な証明書を教職員に発行する。

【上記解決策の問題点】

- 証明書をどのような形で渡すか？

  ファイルベースだと、学生に証明書ファイルを渡し、自分のパソコンを使わせて学生に署名させる教員もでてくるのでは？（なりすましの問題）

  セキュリティポリシーで証明書の貸し借りを禁止し、教職員に徹底するしかなさそう。
- 研究生等、身分のはっきりしない人の場合はどうするか？

  端末管理責任者の署名を検証するのが目的なので、端末管理責任者になる必要のな

い人への配布は考えない。

・ 電子署名の添付手順は？

教員によって、使うメーラーがまちまちである。署名ツールで署名を作成し、メールに添付する手順も案内する必要がある。

・ その他

証明書も個人情報であることを教育する必要がある。

３．講義・演習とその成果

【１日目】

ＰＫＩ技術の基礎を学習。実習１では、テストスィートを使って公開鍵・私有鍵・証明書を実際に作成した。作成した証明書は

・ 自分のＣＡ（MyCA）の自己署名証明書
・ 自分のＣＡ（MyCA）から TopCA へのＣＡ証明書
・ 自分の EE 証明書

作成した証明書をインストールし、ＥＥ証明書からの認証パスを確認した。

【２日目】

・実習１続き

TopCA から MyCA への証明書を発行し、TopCA を介して他の CA の証明書ユーザの認証パスが確立されているのを確認した。

・ 基礎編続き

電子署名の仕組みとタイムスタンプについて学習した。

・ 応用編

ネットワーク認証への応用、電子署名の展開と電子署名法、公的個人認証サービス（住基カード）について学習

・ 実習２

電子署名の作成・検証

署名ツール（FileSign）をインストールし、ツールを使用してテキストファイルに対し、署名を行った。また、作成した署名をツールを使用して検証した。また、ツール上でタイムスタンプの設定をし、タイムスタンプつき署名の作成・検証を行った。ViewBERNT での署名フォーマット確認では、フォーマットの表示がうまくいかず、確認はできなかったが、署名の作成・検証およびタイムスタンプについては理解できた。

【３日目】

ＰＫＩの技術（補足編）として、ＰＫＩに関連した標準とその動向、ＩＤカード・

バイオメトリックス認証・ＩＣ旅券への応用例、ＰＫＩ相互運用、認証局の認定と監査等について説明があった。

その後、課題作成に入った。

【４日目】

課題発表（プレゼンテーション）

４．セミナーで学んだ技術及び知識

ＰＫＩの技術の基礎、ＰＫＩを利用した認証、電子署名の仕組み、ＰＫＩ技術の応用等

５．事前準備として必要と思われるもの

予備知識として、認証や暗号化などのセキュリティ技術とその動向。

６．セミナーの感想

講義については、多少予備知識がないとつらいかもしれない。しかし、ＰＫＩ技術の応用（電子署名、ＩＣカード、住基ネットなど）については、興味深く聞くことができた。

ＰＫＩの全体像について、ある程度は理解できたと思う。

７．備考、その他

７／１２～１４に、情報セキュリティ担当者研修を受講した。その中で、暗号化・電子署名・ＰＫＩ技術についても触れていたが、ＰＫＩ技術の基礎編のダイジェスト版的な内容で、軽井沢セミナーの復習にもなった。