東北大生協情報倫理講座における応用セキュリティ教育

The Advanced Security Education Course in the Tohoku-U-Coop Information Ethics Education Curriculum

金谷吉成*，飯塚聖司†，中村智将‡，高橋望**，浜田良樹††
*東北大学大学院法学研究科　†東北大学農学部３年　‡東北大学工学部３年
**東北大学生活協同組合　††東北大学大学院情報科学研究科
kanaya@law.tohoku.ac.jp

抄録　東北大学生活協同組合が実施する 2005 年度のパソコン講座事業では、前期に著作権や電子商取引，個人情報保護などの基礎的な知識を身につけるための情報倫理講座を開講した。さらに，後期には情報倫理講座発展編という位置付けで応用セキュリティ教育の講座を設け，情報倫理教育の内容をより具体的に体験させることに加え，通常の講座では学ぶことのない特殊なスキルについて扱うことで，情報倫理の実践的な学習を目指した。この講座は自由なキャリアデザインという観点から５つのテーマからの選択性とし、受講生は各々の興味関心に従って受講した。本稿ではそのうち特に「総合セキュリティ講座」「ブログを開設しよう」「フリーソフトで遊ぼう」について概観し、応用セキュリティ教育の意義と展望について論じる。

キーワード　セキュリティ教育，情報倫理，キャリアデザイン，フィッシング詐欺，架空請求，ブログ，フリーソフト

1. はじめに

近年，IT やインターネットの普及発展に伴い，情報倫理，情報モラルに関する教育をどのように取り扱っていくのかが課題となっている。東北大学生活協同組合（以下「東北大生協」という。）のパソコン講座事業は，全国的に見ても情報倫理教育に対して先進的な取り組みをしてきており，本年度は前期にディベートを用いた参加型の情報倫理教育，後期に応用セキュリティ教育の二段構成とした。以下，そのうち応用セキュリティ教育の具体的内容について概観する。

2. 東北大生協パソコン講座

2.1 情報倫理講座の導入

東北大生協では，新入生に対するパソコン共同購入事業の一環として，1999 年よりパソコン講座を実施している。これは当初，学生が購入したパソコンを使いこなせるようにパソコンの基本的な使用方法をレクチャーするものに過ぎなかった。しかし，大学に入学するまでの課程で情報教育に触れたことのある学生が増え，また携帯電話やブロードバンド接続の普及など学生を取り巻く環境が変化することにより，パソコン講座に求められるニーズも変化してきた。そこで，このようなニーズに呼応して，2004 年度からパソコン講座の科目のひとつとして情報倫理講座を導入し，著作権や電子商取引，個人情報保護などの問題を学生に身近な問題として考えさせることにした[1]。

2.2 情報倫理講座の課題

情報倫理講座が扱う著作権，電子商取引，個人情報保護などの問題について，受講生が自らの問題として認識し具体的に考えるためには，法的な思考の前提となるまとまった知識の詰め込みはどうしても避けられない。また，情報倫理講座では，学生が将来危機に直面したときに，ふり返って参考にできるようになるべく網羅的な内容を目指した。そのため，内容がどうしても抽象的，広範的になりがちで，受講生からは「具体性に欠ける」「内容が浅い」などの意見が出された。

2.3 課題への対応

上述の課題を受けて，2005 年度は情報倫理講座の中にディベートを導入して，受講生の主体的な参加を促すことにした[2]。また，後期には情報倫理講座発展編という位置付けで応用セキュリティ教育の講座を設け，情報倫理教育の内容をより具体的に体験させるとともに，通常の講座では学ぶことのない特

殊なスキルについて扱うことで，情報倫理の実践的な学習を目指した。

3. 応用セキュリティ教育

3.1 実施体制

応用セキュリティ教育は，情報倫理講座と同様に，東北大学の教員，グループ・アドバイザ（以下「GA」という。），生協職員が共同してカリキュラムを作成し実施する。中でも受講生の先輩でもある GA の果たす役割は大きく，GA 自身が興味を持ちまたは情報倫理の実際の問題に直面したようなテーマを選んで，ティーチングプランおよび講義資料を作成し，模擬授業を経て受講生に直接教える。その過程において，GA 自身が自己の知識を整理し受講生に伝えることで大きく成長するとともに，知の世代間継承（互学互修）が行われる[3]。この点は，類似のセミナー事業者には真似のできない，本パソコン講座の優れた特徴といってよい。

3.2 ５つのテーマ

今年度，応用セキュリティ教育において取り上げたテーマは次の５つである。

(1) 総合セキュリティ講座…フィッシング詐欺，架空請求メールを受講生に実際に体験させる。さらに，ウイルスに感染するとどうなるかを受講生の目の前で見せつつ，具体的なセキュリティ対策の方法を理解してもらう。

(2) ブログを開設しよう…ブログとは何か，ブログの開設方法，デザインの変更，書き込みのコツなどを受講生が実際に体験しながら進め，ネチケットやマナーを身近なこととして考えさせる。

(3) フリーソフトで遊ぼう…フリーソフトのゲームや便利なツールを紹介しつつ，楽しみながらソフトウェアの安全な導入方法，脆弱性や不具合に対するソフトウェア更新の重要性を学ぶ。

(4) オープンソースを使ってみよう…Knoppix や OpenOffice.org 等のオープンソースの世界を体験させ，その理論と新たな可能性に触れてみる。さらに，受講生のキャリアデザインの一例として，コンピュータ・プログラミングへの動機付けやオープンソース・コミュニティの紹介を行う。

(5) パソコンを分解してみよう…パソコンの分解・組み立てを通して，普段何気なく使っているパソコンの仕組みや内部構造を肌で感じてもらう。これも(4)同様，キャリアデザインの一例という位置付けである。

受講生は，これら５つのテーマから各々の興味関心に従って講座をいくつでも選択して受講する。以下，このうち「総合セキュリティ講座」「ブログを開設しよう」「フリーソフトで遊ぼう」について述べる。

なお，「オープンソース」「パソコン分解」については，セキュリティ教育という観点からはやや異質であると思われるかもしれない。だが，情報倫理をことさらに強調すると，極端な萎縮を招き健全なキャリア育成を阻害してしまうため，そういった問題に対するフォローアップとして今回講座に取り入れることにした。

3.3 総合セキュリティ講座

3.3.1 目的と進め方

本講座は，受講生が実際にフィッシング詐欺の勧誘メールや架空請求メールを受け取り，そういった脅威への対応を自己の経験として身に付けさせることを目的とする。講座は，スクリーンに表示される説明スライド（図１）と受講生に直接送られる電子メール，そしてあらかじめ用意したウェブサイトを使用して進められる。

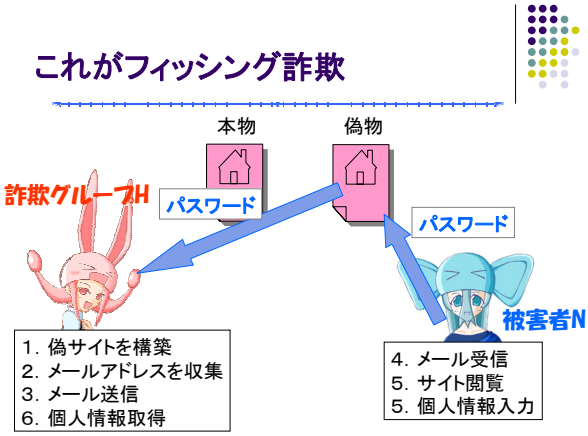

図１　説明スライド

フィッシング詐欺で使用する偽物サイトや架空請求メールは GA が自作した。テストウイルスは講師

の側で危険のないものを用意するが，受講生に対しては，さらなる安全の確保と不安の解消のため，講座専用のメールアドレスを配布し，それを使用してもらうことにした。

3.3.2 フィッシング詐欺

まず，講師が受講生に対してメールを送信する。メールには，本講座のウェブサイト・アドレスなるものが記載されており，受講生はメールに従ってウェブサイトにアクセスすることになる。普段見慣れたはずの「パソコン講座サポートページ」の画面が表示されるが，ここで講師は，実はこれが本物そっくりの偽物ページであることを告げる。受講生は簡単に騙されてしまったというわけだ。

現実には，大手企業や有名ウェブサイトの名前を巧妙に騙ったメールが送られてくる場合があり，またアドレス偽装の方法も，単純にアドレスの混同を引き起こすような表記からアドレス表示部分をまるごと画像で加工するような手の込んだものまであるのだということ，そして自らの身を守るために気を付けなければならないことをスライドで説明する。実際のメールとスライドを組み合わせた説明により，受講生は，フィッシング詐欺の脅威を身近な問題として認識できるようになる。

3.3.3 ワンクリック詐欺，メールによる架空請求

上述のフィッシング詐欺の場合と同様，講師が受講生に対してウェブサイト・アドレスを記載したメールを送信する。受講生がウェブサイトを開くと，「有料の会員制サイトへの入会手続きが完了しました」といったメッセージが表示され，さらに続けて利用料金を請求するメールが送られてくる。

こうした一連の流れを体験させた上で，架空請求への対処方法をあらためて説明することで，受講生の理解がさらに深まることが期待できる。

3.3.4 スパイウェア，コンピュータ・ウイルス

講師による説明の後で，受講生は，実際にスパイウェア対策ソフトを導入してパソコンのチェックを行う。また，講師からテストウイルスが添付されたメールが送信され，受講生は，ウイルス対策ソフトの挙動を実際に体験する。パソコンにそれほど慣れていない者は，ウイルスに対して過剰な恐怖心を持っており，ウイルス対策ソフトがウイルスを検知した段階でパニックに陥ってしまい適切な対応ができなくなることも多いが，実際の挙動を経験することは，そういった点でも効果が高いと思われる。

3.3.5 その他のセキュリティ対策

一般的なセキュリティ対策として，ウイルス定義ファイルの更新やシステムのソフトウェア更新，いざというときに備えてのバックアップの方法などについて説明を行い，受講生は自分のパソコンで実際に手を動かしてその方法を身に付ける。

3.4 ブログを開設しよう

3.4.1 目的と進め方

本講座は，最近急速に普及してきたブログと呼ばれる日記風ウェブサイトを題材として取り上げ，ブログの開設から書き込みまでを受講生に体験させることを通じて，インターネット上のネチケットやマナーについて考え意識させることを目的とする。講座は，テーマにふさわしくブログ上に説明を用意して，受講生がそこにアクセスして学べるようにした（図２）。

図２　講座ブログ

3.4.2 ブログの開設から書き込みまで

まずは，ブログを使ってブログとは何かを説明する。説明の対象が受講生の目の前に提示されているのであるから，受講生の飲み込みも早い。

その後，受講者に実際にブログの開設手続きをさせるのだが，その中で，インターネット上で個人情

報を入力することの怖さや注意点について解説を行う。具体的な手続きと直接関連する事項であり，教育効果は高いと思われる。

そうして，さらにブログへの投稿と編集，デザインの変更や各種機能の紹介，コメントとトラックバックについて，実例を示しながら解説する。特にブログの重要要素であるコメントとトラックバックについては，複数の受講者が相互にトラックバックを送りあうなど，受講者間の交流を図った。また，受講生のコミュニケーション能力を育成するという観点から，ブログを書き続けていくコツなどにも触れることにした。

3.4.3 ネチケットやマナー

インターネットには，ブログのような新しくて便利なコミュニケーション手段が存在するが，非対面コミュニケーションであるが故のさまざまな問題もある。また，ブログを表現の場としてみると，著作権侵害や名誉毀損的表現，個人情報漏洩やプライバシー権侵害の問題などがあり，そうした問題について自ら考えられるよう促すことが重要であると考える。

3.5 フリーソフトで遊ぼう

3.5.1 目的

本講座は，フリーソフトのゲームや便利なツールを実際に使ってみて，楽しみながらソフトウェアの安全な導入方法，脆弱性や不具合に対するソフトウェア更新の重要性を学ぶことを目的とする。

3.5.2 遊びからセキュリティを学ぶ

講座の重要な目的のひとつに，受講生が楽しみながら能動的に学ぶということを掲げたため，受講生のモチベーションは高かったように思われる。講座では，インターネットからソフトをダウンロードする際，ソフトの安全性や信頼性をきちんと確認すること，ウイルスチェックを行うこと，説明書を読み何か問題が起こったときは自分自身で調べ対処しなければならないことなどを説明した。

4. 展望と課題

情報倫理講座の射程範囲は，著作権，電子商取引，個人情報保護，不正アクセスなど多岐にわたる。それゆえ，情報倫理に関する教育は総論的になりがちで，受講生に具体的に問題の所在を認識させるためには，今回のようなテーマ密着型の応用講座が果たす役割は大きいといえる。

しかし一方で，パソコン講座が始まる 4 月から応用セキュリティ講座が行われる 11～12 月にかけて，受講者数が大幅に減少しているという問題がある。受講生の長期間にわたるモチベーションの維持をどのように図っていくかが，今後の課題である[4]。

5. おわりに

今日の高度情報化社会においては，人はさまざまな新しい問題に直面することになる。情報倫理は，そのような状況において，行動の指針を示すものであるが，日々生じる新しい問題に対しては，自らが問題の所在を認識し，適切に考え判断する能力が求められる。そのためにも，学生が主体的に取り組んでいけるような実践的な情報倫理教育カリキュラムの開発が，今後ますます重要な意味を持つものといえる。

参考文献

[1] 浜田良樹，谷内毅，杉八合勲，金谷吉成「パソコン講座における情報倫理教育のカリキュラム開発について～実践情報モラル教育論」，コンピュータ＆エデュケーション Vol.17，pp.154-158，2004.

[2] 浜田良樹，金谷吉成，飯塚聖司，高橋望「ディベートを用いた参加型情報倫理教育～実践情報モラル教育論 II」，コンピュータ＆エデュケーション Vol.20，pp.80-85，2006.

[3] 妹尾堅一郎「『互学互修』モデルの可能性―先端的専門職教育における『学び合い・助け合い』」，コンピュータ＆エデュケーション Vol.15，pp.24-30，2003.

[4] 浜田良樹，金谷吉成，高橋望「東北大生協における情報倫理講座の発足とその影響」，2006 PC カンファレンス論文集，2006.