CIS2006 2006/2/26

学生の情報セキュリティ知識欠落の問題点と教育的対応

Proposal recommending teaching Internet Security Practices as a core requirement of students' basic education curriculum

矢ヶ部一之*
Kazuyuki YAKABE

**飯箸泰宏
Yasuhiro IIHASHI

*跡見学園女子大学
Atomi University

**明治大学
Meiji University

発表の動機

- パソコンの操作方法は教えるが、安全利用の教育は皆無であることに疑問を感じた
  - 自動車の教習では、『運転操作の教習と同時に、安全運転の知識教育も 平行して行われる』のに何故か？
  - 犯罪や感染症などの多い地域へ旅する場合、ワクチンを摂取したり、安全の知識を求めるのに・・・
- ウイルスやスパイウェアの状況に個人的に危機を感じた
  - 2000年頃からスパイウェア対策ソフトの使用を始めたが、自分のPCや同僚などのPCのスキャン結果を見て、愕然とした

⇒ 学内や小規模な研究会で、2001年秋から啓蒙活動を開始

学生を取り巻くインターネット環境

- インターネットのサービス環境の発達・普及
  - 低価格な**常時**接続
  - **ブロードバンド**化
  - 新たなサービスの**種類の増加**（Blog、PodCasting、etc.）
  - **お金**が関係するサービス／利用の一般化

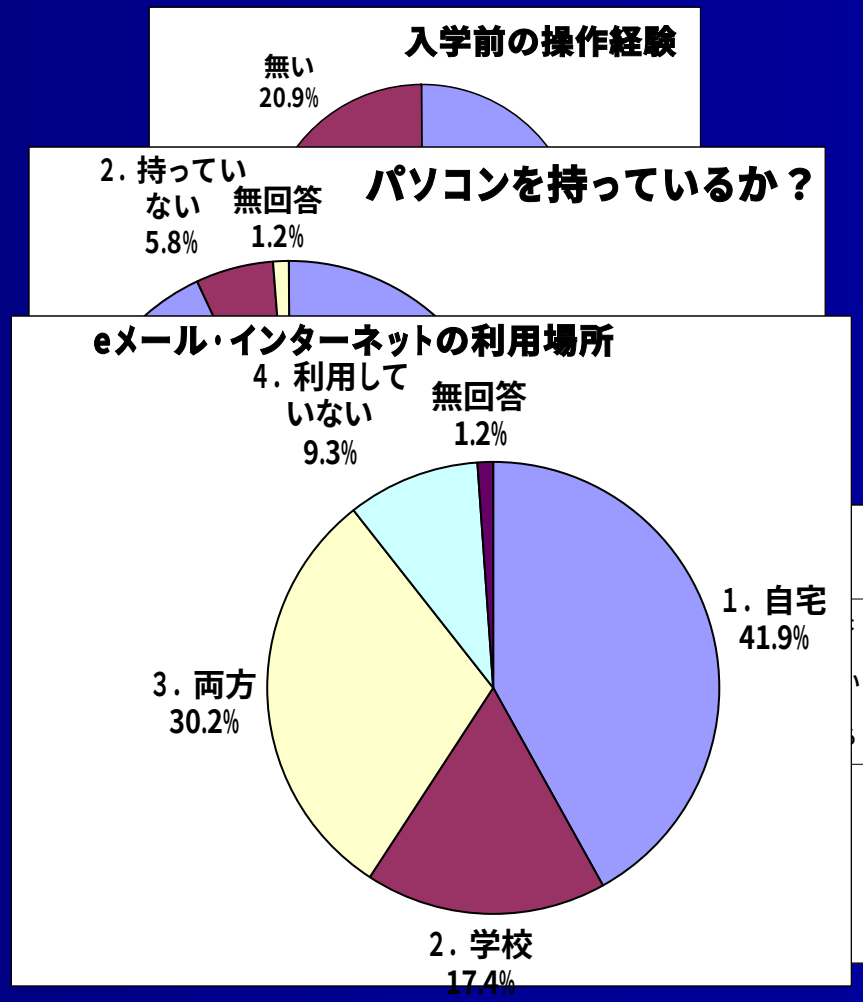
  } 犯罪・感染の増加要因

- 高等学校での教科情報の必修化（2003年度～）
- インターネット犯罪の深刻化
  - 金銭的損害や情報窃盗などが急増
  - フィッシング、スパイウェア、情報漏えい

⇒ そこそこの操作教育を受け、誰でも利用できる環境となったが、犯罪も増加

アンケート結果に見る
大学生の現状

- アンケート対象と調査日
  - 情報リテラシーの3クラス　86名
  - 文科系の学科　主に1･2年生
  - 2005年10月4日
- 結果
  - A) 初等中等教育においてパソコンの操作指導を受けた経験がある：　79%
  - B) 自宅にパソコンがある：　93%
  - C) インターネットを使用している：90%　(自宅での利用：72%)

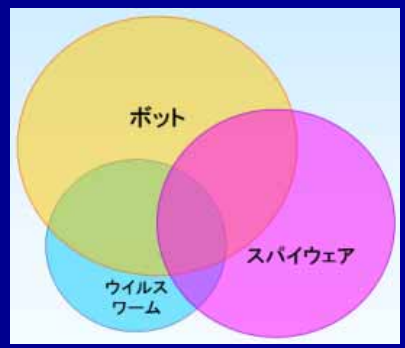


インターネット白書2005　と矛盾しない
(財団法人インターネット協会)

インターネット・リスク（犯罪）

- インターネットは、国際犯罪多発地帯
  - マルウェア（Malicious Software；悪意を持ったプログラム）
    - ウイルス、ワーム
    - スパイウェア
    - ボット（ボット・ネット）
  - 詐欺
    - フィッシング、ファーミング、他
  - 不正アクセス

  etc.



- 感染・侵入
  - ウイルス添付メール ⇒「インターネット接続＝感染」

インターネット・リスク(犯罪)の現状

- **感染・変化の速度のアップ**
  - 接続から、感染や不正アクセスされるまでの時間が毎年減少
  - **管理されていない**パソコンをネット接続した場合、2005年では数分まで短縮
- **愉快犯から金銭目的へ、破壊から情報窃盗へ**
  - 情報を盗み金銭被害を与える犯罪が急増：キーロガー、フィッシング
- **顕在から潜在へ、次はステルス化**
  - スパイウェアやボットなど、感染しても、気付かないユーザが大半
  - 大半(8～9割)の感染ユーザが自分は感染しないと思い込み、感染していること自体を知らないとの米国での調査報告が複数ある
- **無差別からターゲットを絞ったものへ**
  - 世界規模で感染を拡大する形の攻撃から、標的を絞った小規模で検出されにくい攻撃へ
- **巧妙化**
  - 対策より変化が早く、対策を逆手に取るもの、次々に変形するものもある
  - 一般メディア等が発する古い情報が誤判断を誘う　例
- **PC以外の攻撃対象の増加**
  - 携帯電話やPDAに加え、情報家電などPC以外のネット接続機器が増加
  - 既に家電が踏み台となる事件も発生
  - Network、無線(電波)での制御・破壊
- **被害者＝加害者**
  - ボット・ネット構成PCの増加

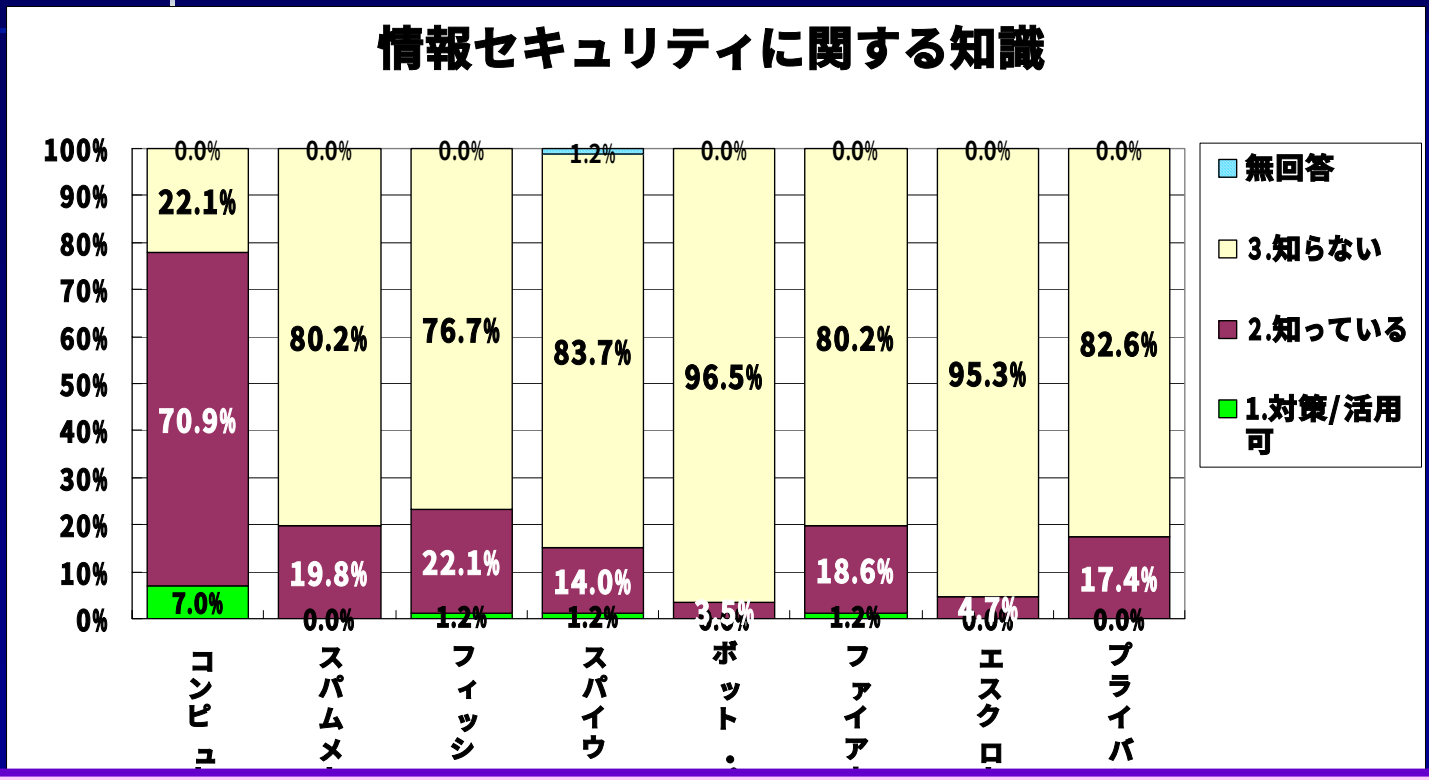
インターネット・リスクの現状　まとめ

- パソコンの適切な管理ができないと、
  - すぐに感染・侵入を許す
  - 容易に、個人情報漏えい、金銭盗難の被害者へ
  - 被害者だけに留まらず、加害者になる

⇒ 今のインターネット環境では、**現状を知り、自分のパソコンを管理し、防衛する知識が必要**

※ 各レイヤーにおいて、各種犯罪を考慮した、セキュアなインターネット・アーキテクチャ＆システム（ソフト）に置き替わるまで、この状況は続く

アンケート結果に見る
学生の情報セキュリティに関する知識



- ウイルス
  - 71%が名前だけ知っている程度
  - 対応までは7%
- フィッシング
  - 名前 23%
  - 大半は知らず
  - 対処1名
- スパイウェア
  - 名前 15%
  - 大半は知らず
  - 対処1名
- ボット
  - 名前のみ 3.5%
- エスクローサービス
  - 名前のみ 5%

大半が情報セキュリティに関しては無知であり、容易に感染し、感染しても被害が顕在化するまでは、気付かない状況にある

一般学生への情報教育の現状

- 大学では、情報リテラシー教育を行うところは多いが、**情報セキュリティ教育までは、なかなか手が回らない**
  - 情報リテラシー教育で手一杯
  - 新入生は、初心者から中級レベルのスキルまで混在
  - 情報科目が受験に関係なく、また中等教育での情報教育体制の未整備
- 情報リテラシー教育と情報セキュリティ教育は全く別であるが、情報リスクの現状と共に、それが十分認識されているとはいえない
- **学生の情報セキュリティの知識獲得は、自己責任**
  - TVをはじめとするマスメディアからの情報程度の知識
    - 内容が古くあまり役立たなかったり、実情を反映していない
    - 被害を伝えるだけで適切な対応が示されず、対処できない
    - 名前を知るのが精一杯
- **学生：現状把握や知識が不足し、正しい判断や対処の方法を知らない**

インターネット・リスクと学生の現状

- 一般学生の大半が、情報セキュリティに関しては無知に等しいが、適切な知識が得られる環境にない

⇒ 犯罪者の格好のターゲットとなり、マルウェアへの感染や情報盗難に遭う可能性が非常に高い

  - 既に、自宅PCの感染が推察できる学生が複数いることが、ウイルス感染したなりすましメールの送信などから伺える
    - メールの授業の後やレポートなどの送信先として伝えたアドレスで、ウイルス添付などが急増する

⇒ ネットの活用が進むにつれ、このリスクはさらに高まる

情報セキュリティ知識欠如の問題点

- 被害者として、時間的損害・経済的損害・精神的損害を蒙る
- 踏み台やゾンビPCの所有者となり、加害者として、他人に損害を与える
- 就職後、社会人となって、
  問題のある製品（ハード、ソフト）を開発したり、適切な対応を行う組織への変革を遅らす
  - 危機をイメージできず、問題発生の予測と対処ができない
  - 事故が拡大して、はじめて気付く

⇒ 単に、自分の被害だけの問題に留まらない

情報セキュリティ知識が必要な場面

- パソコンをインターネットに接続して利用する時
- 組織等で、セキュリティを考慮して判断すべき時
  - 安全な情報サービスの提供、安全な機器の開発を行うポリシー、手順及び組織の構築
- インターネットや無線ネットワークに接続される全ての機器を設計・製作する時
  - ネットワークや無線（電波）を介して、ディジタル情報の送受信を行う機器、ディジタル情報を受信し内部の変更を行う機器

⇒ 単に、PCでのインターネット利用の場面だけには留まらない

提 案

- これからの情報社会において、情報セキュリティの基本的な知識は必要である
  - 情報機器を快適に利用し、犯罪の被害者や加害者にならないため
  - 社会に出て、ネット社会にあるリスクを正しく理解し、その結果、正しい判断を行ったり、脆弱性の少ない機器の開発を行うため
- 大学において、
  『情報リテラシー教育と共に、情報セキュリティ教育を一般学生へも行うこと』を提案する
- 教えるべき内容
  - リスクの現状の認識と変化への対応の心構え
  - 一般ネットユーザの行うべきパソコン管理の基本

Fin