

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

あらまし：インターネット利用及びそれに伴うリスクの拡大や変化に対し、そこに置かれた学生の環境とリスクに関する知識を考慮した場合、個々人が判断するには適切な情報(教育)が与えられていない。学生の置かれた現状、学生の入学時の情報教育の状況及びインターネット・リスクに対する知識のアンケート結果を示し、現在及び将来の社会活動を考慮した場合、現在行われている情報リテラシー教育に加え、情報セキュリティ教育を行うことの必要性を示す。

キーワード：情報リテラシー教育 情報セキュリティ教育 インターネット・リスク パソコンの管理

1. はじめに

低価格な常時接続の提供、ブロードバンド化[1]によるアクセス速度のアップ、ブログやポッドキャストをはじめとする新たなサービスの種類の増加など、インターネットのサービス環境が発達し、お金が関係するサービス及びその利用も一般化している。日本の初等・中等教育においては、情報教育が必修化[2]されている。一方、ネット犯罪は巧妙化すると共に性格も変化し、愉快犯から経済犯へと主体が移り、金銭的損害や情報窃盗などが急増し、深刻さを増している。

2. 学生とネット犯罪の現状

2.1 学生環境の現状 (2005/10月のアンケート結果)

学生(文系86名)へのアンケートの結果、79%が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り、93%が自宅にパソコンを有し、90%がインターネットを使用している。大半の学生が自宅にパソコンを所有し、インターネットを利用しているといえる。

これは、2005年の日本のインターネット人口が7千万人台となり、インターネット世帯浸透率が80%超となっていることと矛盾しない[1]。

2.2 インターネット・リスク(犯罪)の現状

インターネット・リスクには、マルウェア(Malicious Software; 悪意を持ったプログラム)、不正アクセス、詐欺などがあるが、その現状は以下の通りである([3]ほか)：

- 感染・変化の速度のアップ：最低限の管理がなされていないパソコンをネット接続した場合、感染や不正アクセスされるまでの時間が毎年減少し、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
 - 顕在から潜伏化へ：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。米国での昨年の調査で、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主体が変化
 - 巧妙化：対策より変化が早く、対策を逆手に取るものもあり、一般メディア等が発する古い情報が誤判断を誘う
 - パソコン以外のネット接続機器(携帯電話やPDAに加え、情報家電など)の増加による攻撃対象の増加：既に家電が踏み台となる事件も発生
- このように、リスクの主体がウイルス添付メールの時代とは大きく異なり、基本的なパソコンの管理を怠った場合、「インターネット接続=感染」とも言える状況にある。さらに、そっと隠れて侵入し、知らない間

に情報を盗んだり、パソコンを乗っ取り悪事に利用し、気付いたときは、銀行口座が空になったり、プライベートな情報が世界中にばら撒かれる事態となる。

2.3 学生の知識の現状(アンケート)と大学の対応

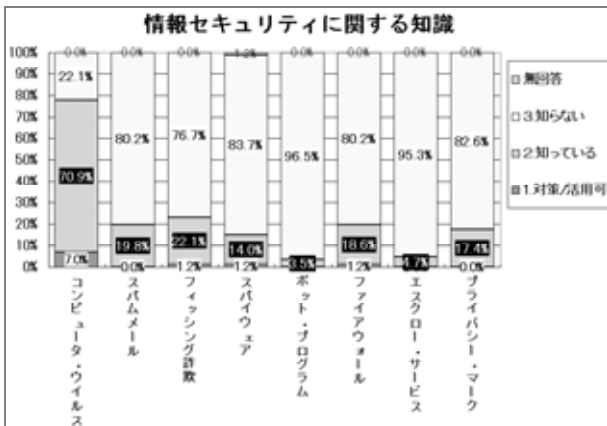


図 1 情報セキュリティに関する学生の知識

比較的有名なコンピュータウイルスでも、71%が名前を知っている程度で、対応方法まで知っているのはわずか7%に過ぎない。昨年、TVなどで多く報道されたフィッシング詐欺やスパイウェアでさえ、名前を知っているのが15~23%で、大半は存在自体を知らず、対応まで知っているのは各1名にすぎない。最も悪質で危険なボットや、ネットオークション等での高額な金額の商品売買で詐欺回避に有効なエスクローサービスに関しては、4~5%が名前を知っているにすぎない。

この結果から、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と言える。

学業や企業のニーズを反映し、大学でも情報リテラシー教育を行うところは多い。しかし、受験に関係しないことや中等教育での教育体制の未整備などもあり、基本操作でさえ、初心者から中級レベルのスキルまで混在し、情報リテラシー教育で手一杯となっており、情報セキュリティ教育まで手が回らないのが実情である。また、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。

結果、大半の学生が、TVをはじめとするマスメディアからの情報程度の知識、すなわち、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かったり、被害を伝えるだけで適切な対応が示されない情報を得ている状況であり、名前を知るのが精一杯となっている。いかなる人でも、現状を把握せず、その知識もな

ければ、正しい判断も対処の方法も分からない。

以上のように、情報セキュリティに関しては無知に等しく、現状のままでは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く、今後、ネットの活用がさらに進むにつれ、このリスクはさらに高まる状況にある。

3. 問題点と情報セキュリティの知識が必要な場面

情報セキュリティの無知により生じる問題点：

- 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
- 企業に就職後において、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

情報セキュリティの知識が必要な場面：

- 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
- 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

4. まとめ(提案)

今後の情報社会において、

- 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

に情報セキュリティの基本的な知識は必要であり、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。

教えるべき内容としては以下のものがある：

- リスクの現状の認識、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

参考文献(既発表資料)

- [1] インターネット白書 2005、財団法人インターネット協会 <http://www.iajapan.org/iwp/>
- [2] 文部科学省 情報化への対応 http://www.mext.go.jp/a_menu/shotou/zyouhou/main18_a2.htm
- [3] IBM Report: Surge in CRIMINAL-DRIVEN CYBER ATTACKS Anticipated in 2006