情報セキュリティに敏感な一般エンドユーザ養成へ向けて —情報セキュリティ意識調査を事例として

松村 真木子†

個人が情報を発信する機会が拡大し，急速に変容している高度情報化社会において，一般エンドユーザは，セキュリティ対策を講じる知識が必要となっている．本稿は，一般エンドユーザである A 女子大学生を対象にセキュリティ知識を調査した事例研究である．本調査対象者は，理念的に理解できる基本的なセキュリティ知識を持つ人が多いが，PC を制御する具体的な仕組みや無線 LAN に関する知識が不足している．そのため，変化の激しい情報社会の実情を正しく把握し，様々な脅威に対峙し適切な対処法を柔軟に選択できるような，セキュリティに敏感なエンドユーザを養成するモデルを提示する．

The Information Security Developing Model for End Users —A Case Study of End User Security Behaviors

Makiko Matsumura†

The explosive growth of the internet and new technologies leave users responsible for their own security. Our survey suggests that the students who are not IT experts understand the network security ethical issues but lack sufficient technical skills to keep their computers safe. The Information Security Developing Model for End Users provides the processes for the students to be more security sensitive and conscious end users with determining their level of security posture, applying active learning on mechanism hardware and on wireless networks.

1. はじめに

急速に変容する情報社会の環境において，一般エンドユーザ☆は情報セキュリティに敏感であることが求められるようになった．本稿では，一般エンドユーザである人文系大学生のパソコン（以下 PC とする）とインターネットの利用方法，セキュリティ知識の現状についての調査結果を分析し，セキュリティ意識が高い集団とセキュリティ意識が低い集団ではどのような違いがあるのかを検証する．その結果から，情報セキュリティに敏感なエンドユーザを養成するモデルを提案する．情報セキュリティに敏感なエンドユーザとは，① PC やインターネットを利用するうえで，その危険性を理解し，状況に応じて対策をとる知識がある，② 自分のセキュリティレベルを知り，必要に応じて学習し能力を向上させる意識があるユーザと定義する．

2. 情報社会のいま

2.1 PC の普及

個人の生活が情報ネットワーク社会に密接につながるようになったのは，10 年あまりのことである．PC 普及率は，1996 年に全国平均 16%，首都圏 21%であったが，2001 年には首都圏で，2002 年には全国平均で過半数となり，2006 年現在，首都圏では 9 割にも達する[1)]．PC は一般家庭に家電なみに普及している．また，光通信網も発達し，家庭からも高速でインターネットが利用できるようになった．

PC の能力が飛躍的に高性能となり，さらに，汎用機の価格が下がり所有しやすくなった．そのため，現在大学に通う学生は，理工系の学生でなくても PC を大学に携帯する光景が珍しくなくなった．

2.2 教育現場における情報化

IT 革命のかけ声とともに教育現場に PC が導入され，2003 年度には高等学校で情報が必修科目となっ

† 国立保健医療科学院（協力研究員）
National Institute of Public Health

☆ 本稿では，情報技術を専門として学習していないユーザを意味する．

た．2006 年，日本全国の高等学校で情報を必修科目として履修した学生が初めて大学に入学した．

学生たちは，インターネットを利用して授業やレポートに関する記事を検索し，図書館の本を検索し，貸出しの予約などの手続きを行い，また，授業の教材や連絡事項をネット上で閲覧し情報を得るなど，教育現場での情報化は確実に進んでおり，学生生活に浸透している．

就職活動の現場でもエントリシートによる応募をインターネットで受け付ける企業が多い．さらに，応募の要件となる TOEFL などの資格試験がコンピュータでの手続きに始まり，試験までもコンピュータ化している．

このように，大学生にとって PC を利用することは学生生活の一部となっている．

2.3 個人的利用の拡大にともなう危機管理意識の重要性

気軽にインターネットを利用する場所として漫画喫茶やネットカフェがある．さらに，無線 LAN が普及したため，駅やカフェなどでも公衆スポットからインターネットを利用することができるようになった．公衆無線 LAN にはセキュリティ対策が施されていないため，利用に際してセキュリティに関する責任は，利用するユーザに任されている[2]．

このようなインフラの普及に加えて，利用目的はネットショッピングやネットバンキングなどへと多様化している．情報ネットワークの専門技術者ではない一般エンドユーザであっても，インターネットに潜在する危険性を理解したうえで PC を利用する時期に来ている．一般エンドユーザが，情報セキュリティに敏感な意識を求められる時代となったのである．

2.4 社会の安定に寄与する一般エンドユーザの責任

2000 年に世界を震撼させた love letter ウイルスによって，PC の危険性が世間に広く認識され始めた．その後，ウイルスは発信者が無自覚なうちにネットワークへ拡散させる仕掛けが施されるようになり，また，知らぬ間にスパイウェアに侵入され情報漏えいに至るなど，一般エンドユーザも多様な危険に遭遇し加害者にもなりうる状況である．

White は，このような情報社会において，コミュニティのセキュリティを向上させるためには，構成員である管理者，指導者，市民が脅威の実態を知り，各自が自分のセキュリティレベルを知り，訓練を受けて能力を向上させることが必要であると述べている[3]．社会の安全は，ユーザそれぞれのセキュリティ意識に支えられている．すなわち，自分の利用する PC を安全な状態に保つことで，ネットワークにおいて加害者とならないために，ユーザは，PC の脆弱性を理解し，インターネット利用における危機回避策をとる知識が必要となっている．つまり，ユーザには，社会の一員としてインターネット上の危険性を理解し対策をとる術を身につける自己責任がある．

ところで，新しいインターネット利用術として一般ユーザが気楽に日記を公開するブログが増加している．このようにブログが広がった背景には，バーチャルな匿名の世界への不安感がひろがり，限られた人の集うコミュニティ「ソーシャルネットワーキングサービス」（以下 SNS とする）が登場したことがあげられる．たとえば，日本では，2004 年に mixi が誕生した．ここでは，友人の招待が参加条件となっている．友人を介した参加者のみのコミュニティは安全性を全面に出し，実名での交流を推奨し輪を広げてきた．そして，2006 年度秋には参加者が 500 万人にのぼり，その後も増加しつづけている．参加者の増加にともない，掲示板に悪意の情報が流されたり，実名であるがゆえにトラブルに巻き込まれたりする事件が発生した．そこで，実名への注意が喚起されるようになった．

SNS では，コミュニケーションの基本は，個人がブログで情報を発信することである．特殊な技術や費用が必要なくだれでもブログに参加できるため，参加する学生も多い．ブログランキングにより広告収入につながる場合もあり，ブログは単なる表現の手段から富を得る道具にも進化しつつある．新しい表現方法がつねに多方面へ変容し，拡散している．

SNS には，プロフィールという項目があり，個人情報を載せるようになっている．公開範囲は各自が定めることになっているが，個人情報の開示につながる．また，インターネット上で企業がサービスとして情報を提供する際，個人情報の記入を求めるログインサービスがある．これらは，利用者の自己責任で個人情報を提供することになるので，ユーザ各自がセキュリティを自覚的に判断できることが望ましい．

ユーザが社会の一員として，セキュリティ対策を施すことは，コミュニティの安全に貢献することになる[4]．

2.5 大学における情報教育

大学教育における情報教育について，学生の PC 利用状況の調査研究があり[5)~8)]，いずれも PC 利用への関心の高さを論じている．時間の経過とともに，技術や利用方法が急速に変化した．情報ネットワーク技術が飛躍的に発展し，それにつれて悪意のしかけが多様化している．その技術刷新の期間が短いため，そのときどきの脅威に応じることができる情報セキュリティ

の専門家を養成することが，大学および大学院教育において重要な課題となっている[9]．情報技術が有益にも悪意にも急速に展開し，瞬時に全世界に拡散していく社会において，その技術を支えるセキュリティ部門の専門家の養成は急務であろう．高等教育を終えた専門家が，社会で即戦力となれるように，実践的カリキュラムが提案されている[10)~12)]．最新の技術に対応できるように，技術者の再教育やサイバー犯罪に対応できる専門家の養成も提案されている[9),13)]．また，学生が専門知識を悪意に利用しないように，情報セキュリティ倫理教育プログラムも提案されている[14)]．

近年猛威を振るっている深刻な脅威は個人情報の漏えいである．その原因は，PC や外部記憶装置の紛失や盗難など人為的な理由，外部からの不正侵入，共有ファイルを介するウイルスなどである[15)]．政府，警察，企業が情報漏えい事件の当事者となったが，従業員のセキュリティ意識が高ければ防ぐことができた事件も多い．たとえば，従業員が，ウイルスに感染しているのを知らずに PC を利用したため，インターネット上に情報漏えいが起きた事件である．エンドユーザが，自分が利用する PC のセキュリティ状況を知っていたならば，または，共有ファイルを利用する危険性を理解していたならば，多くの事件は未然に防ぐことができたであろう．

情報漏えいを起こすと事業所は多大な信用を失墜することになる．しかし，企業においてはセキュリティ対策専門の人材不足が深刻であり，かつ，一般従業員に対するセキュリティ教育，訓練の遅れが危惧されている[4),16)~18)]．一般エンドユーザである従業員が，各自，基本的なセキュリティ対策を施すことができれば，企業全体のセキュリティレベルは高まる．しかし，企業は，従業員のセキュリティ能力を訓練する必要性を知りながら，他業務で時間がとれない，または，訓練のノウハウがないといった理由から先送りにしているのが現状である[15),16),18)]．

このような状況において，大学が，情報技術専門家の養成と同様に，情報セキュリティに敏感な一般ユーザを養成して社会へ送り出すことができれば，社会の安全に貢献することになるだろう．

2.6 一般エンドユーザに求められる基本的なセキュリティ知識

上述したように，情報技術のエンドユーザは，利用する際にネット社会に潜む危険性に意識的であり，常時危機回避策を講じる能力が求められる．情報技術専門家養成課程ではない学生を対象にした，情報セキュリティ教育カリキュラムを築らや星野が提言している[6),19)]が，いずれもセキュリティ教育を課題とし，学内ネットワーク利用における情報技術専門教育課程に準じたカリキュラムを提案している．情報技術専門家養成課程ではない学生を対象とした情報セキュリティ意識についての研究はいまだ薄い状況である．

Stanton らは，パスワードの管理を例にあげ，初歩的な知識不足や単純なミス（naïve mistake）をなくすことにより，コミュニティのセキュリティレベルをあげるモデルを提案した．この単純なミスは，情報セキュリティの問題において，ユーザ側の意図的な悪意と積極的な貢献との間にあるグレーゾーンに位置する．そして，情報の専門家においてさえも，うっかりパスワードをキーボードの下に貼るようなミスをすることがあるため，ユーザが，セキュリティ項目ごとに単純なミスをしていないかを点検する重要性を指摘している[4)]．

White は，構成員のセキュリティ意識とスキルレベルによりコミュニティの安全を判定するモデルを提案した．それによると，第 1 ステップは，管理者，指導者，ユーザが，様々な脅威の存在を知ること，第 2 ステップは，ファイアウォールなどの基本的対策をとることである[3)]．そこで，筆者は，この第 2 ステップまでを一般エンドユーザが求められる基本的セキュリティ対策であると考える．

一般エンドユーザは，大学卒業までに，ネットワークを利用するうえでの脅威を知り，情報モラルの学習に加えて，PC およびネットワークを安全に保つために基本的な技術，設定方法を学習する機会があるならば，社会に出てからも，基本的なセキュリティ知識を基に，状況に応じて脅威への対策をとることができるようになり，つねにセキュリティ能力を向上させるよう意識し，セキュリティに敏感なエンドユーザになる．

3. 本稿の目的

本稿では，一般エンドユーザである人文系学生を対象に，インターネットの利用方法，セキュリティ知識の現状について調査分析する．次に，セキュリティ意識が低い集団，セキュリティ意識が高い集団について，PC の設定方法の理解と PC の利用方法について検証し，情報セキュリティに敏感なエンドユーザを養成するモデルを提案する．

4. 研 究 方 法

事例研究として，A 女子大学（首都圏・人文系）において，情報セキュリティについての意識調査を実施した．第 1 回調査を 2006 年 1 月（175 名），2006 年

春入学した学生を対象に，第2回調査を2006年11月（163名）に実施した．総合学習大教室でB専攻をしている学生に調査票を配布し，その場で回収した．第1回調査は，2学年以上の学生の約1/4にあたる175名，第2回調査は，1学年の学生約2/3にあたる163名の学生を対象として行った（全員への配布回収ではないので，回収率は算出できない）☆．

2006年入学の第2回調査対象者には，社会人学生や浪人経験者，短大からの編入生を含む．そのため，高校で情報必修経験者を必修群，それ以外を第1回調査対象者に加えて非必修群とする．両群とも1年次前期に大学の情報科目を履修している．

調査内容：メール・ネットショッピング・ブログを書くなどPCの利用状況，パスワードの管理・個人情報の保護など大学入学以前の情報セキュリティ学習歴，ウイルス・迷惑メールなどの体験と身近な人がそれらの脅威を体験したことを見聞きした経験，ウイルスソフトの導入・インターネット上でむやみに個人情報を書き込まない・cookieの受け入れを制限している・無線LANへのパスワード設定など利用するPCに実施しているセキュリティ対策．

5. 調査結果—基本的なセキュリティ知識

5.1 PCのセキュリティ設定

情報ネットワークを利用する際に知っておきたい基本的なセキュリティ知識と不正侵入防止策について尋ねた．どの項目も必修群と非必修群に有意な差は認められなかった．

8割以上と実行率が高かった項目は，「知らない人からのメールは開かない」「インターネット上にむやみに個人情報を書き込まない」である．両群とも，差出人が不明のメールは開かない，個人情報を簡単に開示しないなど基本的なネットワーク利用上の理念的な知識を持つ人が多かったが，「セキュリティソフトを導入している（ウイルス対策・ファイアウォールの設定）」について「この項目を知らない」と回答した人が3割にのぼった．

さらに，「Java スクリプト ActiveX コントロールを『無効』にしている」「cookie の受け入れを制限している」については9割近くが「この項目を知らない」と回答した．

5.2 無線LANの知識

「無線LANを無効にしている」について「この項目を知らない」と回答した人は，両群とも9割以上，「無線LANにパスワードを設定している」について「この項目を知らない」を回答した人は9割近くである．両群ともに無線LANの知識が不足している．

表1 エンドユーザに必要なセキュリティ知識
Table 1 Security capability needed for End Users.

危険性	項目	対策		知識
個人情報	個人情報の漏えい	個人情報を記入しない		有
ウイルス	添付ファイル	すぐに開かない	セキュリティソフト	
	Web閲覧	フィルタリング		
不正侵入	ID・パスワード	ID・パスワードの管理		
	スパイウェア	ファイルを安易にダウンローしない	ファイアーウォール	無
	共有ファイルの危険性	設定方法		
	cookie			
	ActivX・Java スクリプト			
	無線LAN			

第2回調査には所有PCがノート型か，ノート型PCの場合にデフォルトのまま使用しているのかどうかという設問を追加した．その理由は，ノート型PCの場合には，デフォルトで無線LANが自動接続に設定されており，安全上問題があるので，実際の使用状況を確認するためである．購入時に添付されるパンフレットには，無線LANにパスワードの設定を促すような注意書きが説明書に付記されている場合もあるが，一般ユーザには分かりにくい．

第2回調査対象者の中でノート型PCを所有しているのは77人であり，そのうち81%がデフォルトのまま使用していると回答した．

5.3 外部の共有PC利用

個人情報を守るために気をつけなければならないことがもう1つある．ネットカフェ，漫画喫茶，公共図書館などの自宅以外の共有PCを利用する場合，個人を特定できる情報を，利用したPCに残さないことである．そのためには，個人を特定できるユーザ番号やパスワードの入力をしないこと，または，入力した場合に履歴を消去する必要がある．

両群とも7割が個人情報を入力しない，2割が履歴の消去をしており，大学入学以前の学習経験による有意な差は両群に認められない．

5.4 PCのセキュリティ対策まとめ

ネットワークを利用するために理念的に理解できる項目については，セキュリティ意識が高かったのであるが，PCを制御する具体的な項目についての知識が不足している．

無線LANを使っていない場合においても，デフォルトのままにしておくのは危険である．しかし，この危険性にも無自覚である．無線LANの利用には無防備であるが，外部PCの利用は学校の図書館を利用し

☆ 本調査は，小規模調査であるため，そこから得られる結果はすぐには一般化できないが，本調査対象者の情報セキュリティ意識の傾向は1つの事実として検証し今後の研究につなげたい．

ている場合が多いためもあり，個人情報の管理については慎重である（**表 1** 参照）．

6. 分析―情報セキュリティ知識・PC の使用方法・セキュリティ学習経験の関係について

PC のセキュリティ対策が実行されるにはどのような条件が必要であろうか．PC の利用実態を中心に，大学入学以前のセキュリティ学習経験をあわせて検証する．

セキュリティ対策の基本である「インターネット上でむやみに，個人情報を書き込まない」項目について，ロジスティック回帰分析☆を実施した．必修群，非必修群それぞれについて有意な差が認められた項目を比較して検討する．ロジスティック分析から，個人情報保護意識を構成している要因を確認する．すなわち，最も基本的なセキュリティ項目の 1 つである個人情報保護意識の構造が明らかになる．

次に，情報セキュリティ意識が低いこと，情報セキュリティ意識が高いことについて判別分析☆☆を用いて検討する．ここでは，PC の使い方，脅威の体験とセキュリティ知識について，情報セキュリティ意識が低い集団に属する人，情報セキュリティ意識が高い集団に属する人の行動を構造化するねらいがある．

6.1 個人情報の保護

6.1.1 ロジスティック回帰分析結果（表 2）

必修群では，個人情報保護の重要性を大学入学までに学んだ経験があると回答した人では，「インターネット上でむやみに，個人情報を書き込まない」を選択することが，回答しなかった人に比べて 15 倍となる．「知らない人からのメールを開かない」を回答した人では，「インターネット上でむやみに，個人情報を書き込まない」を選択するのが 7.9 倍となる．「セキュリティソフトを導入している」と回答した人では，「インターネット上でむやみに，個人情報を書き込まない」を選択するのが 3.1 倍に，ネットショッピングをよく使う人では，「インターネット上でむやみに，個人情報を書き込まない」を選択するのが 2.9 倍となる．ブログを書く人では，「インターネット上でむやみに，個人情報を書き込まない」を選択するのが 0.7 倍減少する．

非必修群では，「セキュリティソフトを導入している」を回答した人では，「インターネット上でむやみに，個人情報を書き込まない」を選択するのが 5.6 倍となり，「知らない人からのメールを開かない」を回答した人では，「インターネット上でむやみに，個人情報を書き込まない」を選択するのが 5.1 倍となる．ウイルスの危険性を学習した経験がある人では，「インターネット上でむやみに，個人情報を書き込まない」を選択するのが 3.4 倍となる．

表 2 インターネット上でむやみに個人情報を書き込まない
Table 2 Identity security.

必修群	B	有意確率	Exp (B)
ネットショッピング	1.098	**	2.999
ブログを書く	−0.424	*	0.654
ネットの脅威を体験			
ネットの脅威を身近で見聞きする			
知らない人からのメールは開かない	2.068	**	7.911
セキュリティソフトを導入（ウィルス対策・ファイアーウフォールの設定））	1.119	*	3.061
無線LANにパスワードを設定している			
個人情報保護の重要性を既習	2.738	*	15.456
ウィルスの危険性を既習			
ID・パスワードの管理を既習			
定数	−2.696	**	0.067

*:p<0.1,**:p<0.05 (−2LL 72.523) (N142)

非必修群	B	有意確率	Exp (B)
ネットショッピング			
ブログを書く			
ネットの脅威を体験			
ネットの脅威を身近で見聞きする			
知らない人からのメールは開かない	1.636	**	5.136
セキュリティソフトを導入（ウィルス対策・ファイアーウフォールの設定））	1.716	**	5.560
無線LANにパスワードを設定している			
個人情報保護の重要性を既習			
ウィルスの危険性を既習	1.217	*	3.377
ID・パスワードの管理を既習			
定数			

*:p<0.1,**:p<0.05 (−2LL 103.555) (N196)

6.1.2 個人情報保護の構造

両群とも，多くの人が「知らない人からのメールは開かない」「ウイルスソフトを導入している」という最も基本的なセキュリティ知識があり，このことが個人情報保護の意識を高めている．しかし，必修群と非必修群は，個人情報保護に影響している要因が異なっている．すなわち，必修群では，大学入学前に個人情報保護の重要性について学習した経験の効果が強く現れている．非必修群では，ウイルスの危険性を学習した効果が現れている．さらに，PC の使用方法について，必修群では，ネットショッピングの利用者が，個人情報保護に慎重になっている．また，ブログを書くということは，個人情報をある程度公開することになる．そのため，「インターネット上でむやみに，個人情報を書き込まない」が減少するものとみられる．

6.2 情報セキュリティ意識が低い集団

上述したように，両群とも個人情報保護への意識を

☆ ロジスティック回帰分析は，独立な因子の影響を定量的（オッズ比（B））に評価する分析方法である．

☆☆ 判別分析とは，1 つの従属変数を，複数の独立変数を用いて群わけすることで，あるデータがどの群に属するのかを予測する方法．

高めた項目は，「ウイルスソフトを導入している」ことである．インターネットを利用する際には，最も基本的かつ分かりやすい対策の 1 つであるが，「この項目を知らない」と回答した人が 3 割もいたことに危機感をいだく．ウイルスに罹患すると，メールをやりとりしている相手にも迷惑をかけることになり，ネット上にウイルスを増殖させる原因ともなりかねない．このような人は，無自覚であっても社会を危険にさらしている．そこで，「ウイルスソフトを導入している」について，「この項目を知らない」と回答した人々を，本稿ではセキュリティ意識が低い集団とする．セキュリティ意識が低い集団に属する人について，PC の使用方法とセキュリティの実施状況とについて判別分析を実施した．

6.2.1 PC の使用方法判別分析結果 1（表 3）

両群とも PC でメールをし，ネットショッピングをし，PC をよく使っている．必修群は，ブログを書き，非必修群は，掲示板へ書き込みをしている．ウイルスの危険性に無自覚のまま，PC を多様な目的に利用している．情報セキュリティ意識が低い集団に属する人たちは，非常に危険な使い方をしている状況にある．

6.2.2 脅威の体験☆とセキュリティ知識

情報セキュリティ意識が低い集団においては両群とも，セキュリティの基本的対策すべての項目を知らなかった．特に，必修群でも，「知らない人からのメールは開かない」，「無線 LAN にパスワードを設定している」について知らないと回答している．非必修群は，「無線 LAN にパスワードを設定している」，「インターネット上でむやみに，個人情報を書き込まない」，「Java スクリプトや ActiveX コントロールを『無効』にしている」を知らないと回答している．

しかし，「インターネット上でむやみに，個人情報を書き込まないを知らない」項目については必修群では低い値を示しているが，非必修群では高い値を示している．さらに，ネット上での脅威の体験については，必修群は体験していないが，非必修群はかなり体験している．ネット上の脅威を身近で見聞きしたことも，必修群ではわずかであるが，非必修群は身近で見聞きした経験がかなりある．必修群では，大学入学前の学習効果が若干現れているため，さらに，まだ 1 年であり PC の使用頻度が少ないこともあって脅威に出会う機会が少ないのであろう．一方，大学入学前にセキュリティの教育を受けていない非必修群はセキュリティ知識がなく，無自覚であるがゆえに PC をいろいろな目的で使っている．その結果，何らかの脅威を体験し，身近でも見聞きしているなど非常に危険な状況にある．

情報セキュリティ意識が低い集団に属する人は，基本的なセキュリティの知識がなく，無防備なままネットショッピングなど多目的に PC を利用しており危険な状態にある．

表 3 情報セキュリティ意識が低い集団
Table 3 The group with low knowledge about Information security.

PCの使い方	判別に寄与する関数	
	必修群	非必修群
PC使用頻度	0.279	0.642
PCでe-mail	0.459	0.349
掲示板への書き込み	−0.230	0.449
ネットショッピング	0.466	0.306
音楽・映像のダウンロード	0.260	−0.300
HPを作成している	0.006	−0.139
ブログを書く	0.327	−0.018
有意確率	*	**
交差確認済みのｸﾞﾙｰﾌﾟ化されたｹｰｽのうち正しく分類	60.00%	61.40%
*:p<0.1,**:p<0.05	(N130)	(N176)

脅威の体験とセキュリティ知識	判別に寄与する関数	
	必修群	非必修群
ネットの脅威を体験	−0.382	0.363
ネットの脅威を身近で見聞きする	0.076	0.282
「知らない人からのメールは開かない」を知らない	0.611	0.207
「JavaスクリプトやActiveXコントロールを「無効」にしている」を知らない	0.327	0.469
「cookieの受け入れを制限している」を知らない	0.163	0.279
「インターネットでむやみに、個人情報を書き込まない」を知らない	0.137	0.407
「無線LANにパスワードを設定している」を知らない	0.237	0.568
有意確率	**	***
交差確認済みのｸﾞﾙｰﾌﾟ化されたｹｰｽのうち正しく分類	66.70%	59.00%
:p<0.05,*:p<0.001	(N114)	(N166)

6.3 情報セキュリティ意識が高い集団

上述したように，無線 LAN の設定は，最も実行されていない項目の 1 つである．ノート型 PC の普及とともに，無線 LAN が気軽に利用できる環境が整ってきているが，セキュリティの設定は浸透していないのが現状である．その中で，パスワードを設定していると回答した人は，セキュリティの意識が高いと考え

☆ 本稿において「ネットの脅威の体験」とは，「ウィルスに感染した」「迷惑メール・チェーンメールを受け取った」「不正アクセスされた」「掲示板で中傷された」「不当に個人情報をとられた」のいずれかの体験があること．「ネットの脅威を身近で見聞きする」は，身近な人から「ネットの脅威の体験」をしたと聞いたことがあること．

る．そこで，そのような人をセキュリティ意識が高い集団に属する人として，判別分析を実施する．該当するデータが少ないため（N43)☆，必修群，非必修群を分けずに分析する．

6.3.1 PC の使い方判別分析結果 2（表 4）

情報セキュリティ意識が高い人たちは，PC でメールをし，ブログを書き，HP を作成するなど PC の使用頻度が高い．しかし，掲示板への書き込みやネットショッピングはしていない．HP を作成しているため PC のスキルが高いと考えられる．

6.3.2 脅威の体験とセキュリティ知識

「セキュリティソフトを導入（ウィルス対策・ファイアウォールの設定)」し，ネットの脅威を身近で見聞きしているが，脅威を体験してはいない．

「Java スクリプトや ActiveX コントロールを『無効』にしている」，「cookie の受け入れを制限している」，「自宅以外の PC を利用するときに，個人情報を入力しない・個人情報を入力した場合削除している」など，全体的に学生の認知度が低かった項目も，情報セキュリティの意識が高い人は実行している．

「インターネット上でむやみに，個人情報を書き込まない」が負の値を示しているのは，ブログを書く際に，個人情報を記入しているからと考えられる．

情報セキュリティ意識が高い集団に属している人は，危険性を理解して，対策を講じつつ，ブログを書き，メールをしている．情報セキュリティの意識が高い集団に属する人々は，セキュリティの脅威を知り，セキュリティ対策の知識を持ち，慎重に PC を利用している．

表 4 情報セキュリティ意識が高い集団
Table 4 The group with high knowledge about Information security.

PCの使用方法	判別に寄与する関数
PC使用頻度	0.267
PCでe−mail	0.630
掲示板への書き込み	−0.978
ネットショッピング	−0.352
音楽・映像のダウンロード	−0.013
HPを作成している	0.293
ブログを書く	0.352
有意確率	*
交差確認済みのｸﾞﾙｰﾌﾟ化されたケースのうち正しく分類	54.90%

*:p<0.1 （N319）

脅威の体験とセキュリティの実行	判別に寄与する関数
ネットの脅威を体験	−0.363
ネットの脅威を身近で見聞きする	0.453
知らない人からのメールは開かない	0.022
セキュリティソフトを導入（ウィルス対策・ファイアーウフォールの設定））	0.603
JavaスクリプトやActiveXコントロールを「無効」にしている	0.276
cookieの受け入れを制限している	0.284
インターネットでむやみに、個人情報を書き込まない	−0.176
自宅以外のPCを利用するときに、個人情報を入力しない・個人情報を入力した場合削除している	0.192
有意確率	**
交差確認済みのｸﾞﾙｰﾌﾟ化されたケースのうち正しく分類	74.00%

**:p<0.05 （N331）

☆ N はデータ件数を示す．表によって N の値が異なるのは，欠損値を含むデータを分析から除外したためである．

6.4 ま と め

「知らない人からのメールは開かない」「ウイルスソフトを導入している」という最も基本的なセキュリティ知識と基本的な項目の学習経験として，必修群では「個人情報の重要性」・非必修群では「ウイルスの危険性」の学習経験が，個人情報保護の意識を高めている．

情報セキュリティ意識が低い集団に属する人たちは，基本的なセキュリティの知識がないまま，多様な目的で PC を使い，非常に危険な状況にある．

情報セキュリティ意識が高い集団に属する人たちは，情報社会の危険性を理解して，対策を講じつつ，ブログを書き HP を作成しメールをしている．情報セキュリティの意識が高い人々は，セキュリティの脅威を知り，セキュリティ対策の知識を持ち，慎重に PC を利用している．彼らが，情報社会において，自己責任において行動しているセキュリティに敏感なエンドユーザである．

7. 考 察

本稿は，A 女子大生を事例として，情報技術専門家養成課程ではない学生が PC の使い方，自分が利用する PC の管理をするためのセキュリティ知識，および，「インターネット上でむやみに個人情報を書き込まない」ことの構造について，高等学校で「情報」が必修だった群とそれ以前の非必修群とに分けて比較検討した．さらに，情報セキュリティ意識が低い集団，情報セキュリティ意識が高い集団について検討した．

両群とも，基本的なネットワーク利用上の知識を持つ人が多かったが，セキュリティソフトの導入について「この項目を知らない」と回答した人が 3 割にものぼった．この割合はかなり問題であろう．Goo research が実施したユーザアンケートでも，10%のユーザがセキュリティソフトを導入していなかったが，この事態を問題としている[20]．ウイルスを撒き散らす媒介とならないために，セキュリティソフトの導入は，

社会の一員としての義務であろう．Whiteは，コミュニティにおいて，成員各自にそのセキュリティを構成する責任があると指摘している[3]が，セキュリティソフトの導入はその責任の基本的な項目である．一個人の初歩的な知識不足や単純なミスが社会へ脅威となる[4),21)]ことを，エンドユーザは自己責任として自覚する必要がある．

不正侵入や個人情報の不当な取得手段となりうるJavaスクリプト，ActiveXコントロール，cookieの受け入れ，無線LANの制御方法など，より具体的な仕組みについては認知度が低い．築らが報告しているが，「学内LAN利用のための知識とセキュリティ一般，情報倫理一般の知識が渾然一体となっている[6)]」ものとみられる．これらの傾向は，必修群と非必修群との間に相違は見られない．しかし，PCの仕組みを理解したうえで技術的な操作が必要となる項目については，佐々木らが指摘するように，一般ユーザにウイルス対策や不正侵入対策など具体的に教える[5)]機会が必要である．すなわち，学内LANの利用における情報倫理教育に加えて，ある程度の時間をかけて情報社会の脅威と具体的な対処法[19)]を実習する機会が必要である．本稿では，本調査対象者は，情報倫理面は理解しているが，自分のPCの仕組みについての知識と無線LANに関するセキュリティ知識が不足していることを検証した．

無線LANの利用は，今後ますます拡大するだろう．Chenowethらは，大学内で実験を実施し，無線LANを使用している学生ユーザの中に10%ほどが，セキュリティ対策をしていないことを検証した．セキュリティの情報を随時受けられる学内においても，これほどまでにセキュリティに無関心であるということが明らかになった事実は，公衆スポットの利用者が拡大しつつあり，悪意の侵入の機会が増加している現在，無線LANの利用に対する警鐘である．公衆スポットを利用する無線LANは，セキュリティがユーザの自己責任となっているため，ユーザにどのように脆弱性を理解させ，セキュリティ対策がいかに重要であるかを認識させるかが今後の課題であると指摘している[2)]．

個人情報保護の意識を例にとると，基本的なセキュリティ知識とその学習経験の効果が確認された．しかし，ブログの書き込みをする人では，「インターネット上でむやみに，個人情報を書き込まない」が減少する．これは，SNSのプロフィール欄やブログでは，実名での情報発信を薦めていることが一因であろう．本調査においても自由記述欄に，特定のSNSへの参加を表明している回答が散見された．友人のブログへの意見を実名で記入するということもあるだろう．Web上での個人情報の公開を懸念する調査結果がある[22)]．個人情報の保護は，理解されやすい項目であるが，SNSやブログを利用する人の広がりを視野に入れると，ユーザ各自が，情報の公開やその影響について改めて自覚する必要がある．

情報セキュリティ意識が低い集団に属する人々は，セキュリティについて無知であり，PCを多目的に使用し，危険な状況にいる．そのため，なんらかの脅威に出会う可能性が高い．一方，情報セキュリティ意識が高い集団に属する人々は，インターネットの危険性を十分理解し，セキュリティの設定を講じたうえで，メール，ブログやHP作成にPCを利用している．情報セキュリティを自覚しつつPCを利用しているため，セキュリティに敏感なエンドユーザといえる．

8. セキュリティに敏感なエンドユーザ養成モデル

情報技術専門家養成課程ではない学生にとって，大学での情報教育は，一般エンドユーザとなって情報社会を生きていくうえで必要な意識やスキルを身につける最後の機会である．社会人になれば，PCの利用目的はより多様化するであろう．

個人が情報を世界に向けて手軽に発信し，閉じられているはずのSNSが膨張しつつあり，情報社会は急速に変容している．このような変化の激しい情報社会の実情を正しく把握し，様々な脅威に対峙し適切な対処法を柔軟に選択できるようなセキュリティに敏感なエンドユーザを養成するモデルを提示する（**図1**参照）．

一般エンドユーザの現状は，多くがセキュリティ対策の基本的な知識・技術が不足している．これを補う具体的な教育の機会が必要である．大学におけるセキュリティ教育では，情報倫理教育を行うばかりでなく，まず，学生が自分のセキュリティ意識のレベルを確認するプログラムを導入して現状把握をさせたうえで，PCの仕組みやインターネットの具体的なセキュリティ対策技術，特に無線LANの設定や汎用OSの基本的な制御方法の習得を目標とした実習を導入することを提言する．理念の理解だけでなく，実際に手元のPCのセキュリティ対策を講じる技術を身につけることによって，学生時代にセキュリティに敏感なユーザになっていれば，社会人になってからも，日々進化するネットワークの状況に敏感になり，状況に応じて表出する様々な脅威に対して，新たに必要な知識を学習し，柔軟に対処する能力を高めるようになるものと期待できる．社会の安全のためには，このような情報

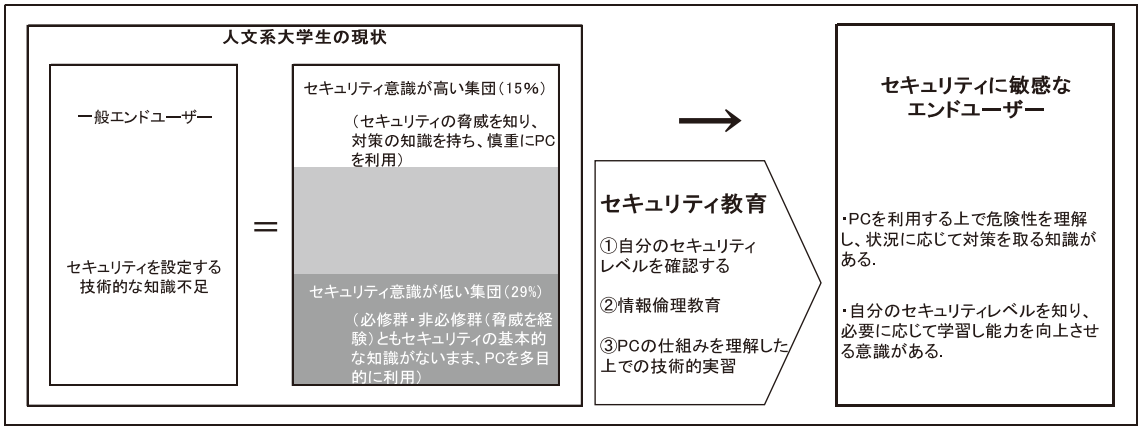

図 1 セキュリティに敏感なユーザ養成モデル
Fig. 1 The information security developing model for End Users.

セキュリティに敏感であるエンドユーザが増加することが望ましい.

9. おわりに

本調査研究は，エンドユーザの情報セキュリティ知識について検証し，情報セキュリティ意識の低い集団，情報セキュリティ意識の高い集団の PC の使い方と情報セキュリティ知識について構造的に検討した.

本調査は小規模の事例研究であるが，今後調査を拡大し精査を重ねたい．また，セキュリティに敏感なエンドユーザ養成へ向けた教育プログラムの学習成果について，PC を制御する具体的な項目についての知識がある者，情報社会の脅威と具体的な対処法の実習を経験した者などについて比較評価を行うことを今後の課題としたい.

謝辞 本稿は，第 33 回セキュリティ研究会において報告した内容を再考，加筆修正したものである．研究会に出席された先生方からいただきました温かいご助言に感謝しております．また，文章に丁寧に目を通し．校正に多大なご支援をいただきましたピアグループの香西真弓さん（オフィスワーク研究家）に感謝いたします.

参考文献

1) 民力，朝日出版社 (1996–2006).
2) Chenoweth, T., Minch, R. and Tabor, S.: User Security Behavior on Wireless Networks: An Empirical Study, *The 40th Annual Hawaii International Conference on System Sciences* (*HICSS'07*), pp.1–8 (2007). http://csdl2.computer.org/comp/proceedings/hicss/2007/2755/00/27550145b.pdf
3) White, G.B.: The Community Cyber Security Maturity Model, *The 40th Annual Hawaii International Conference on System Sciences* (*HICSS'07*), pp.1–8 (2007). http://csdl2.computer.org/comp/proceedings/hicss/2007/2755/00/27550099b.pdf
4) Stanton, J.M., Stam, K.R., Mastrangelo, P. and Jolton, J.: Analysis of end user security behaviors, *Computer & Security*, pp.1–10 (2004).
5) 佐々木良一，杉立 敦：情報セキュリティ教育の現状と今後，信学技報，No.33, pp.1–6 (2002).
6) 築 雅之，竹本宣弘：情報セキュリティ教育のための小規模ベース構築ツールの開発，情報文化学会全国大会講演予稿集，pp.33–36 (2002).
7) 永井昌寛，奥田隆史，高橋一幸，野口 覚：高校時・大学入学時におけるコンピュータ利用状況と意識実態分析，日本教育工学会論文誌，Vol.27, pp.65–68 (2003).
8) 高橋正行，長友幸子，岩泉庄一，深瀬啓司，下山淳，森下博正，神長京子，磯崎善則：高等学校における情報教育に関する実証的研究，日本教育情報学会第 20 回年会，pp.206–207 (2004).
9) McGinnis, D.R. and Comstock, K.: The Implication of Information Assurance and Security Crisis on Computing Model Curricula, Information Systems Education Journal, Vol.1, No.9, pp.3–12 (2003). http://isedj.org/1/9
10) Conklin, A.: Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course, *The 39th Annual Hawaii International Conference on System Sciences* (*HICSS'06*), pp.1–6 (2006). http://csdl2.computer.org/comp/proceedings/hicss/2006/2507/09/250790220b.pdf
11) Dark, M.J., Ekstrom, J.J. and Lunt, B.M.: Integrating Information Assurance and Security into IT Education: A Look at the Model

Curriculum and Emerging Practice, *Journal of information Technology Education*, Vol.5, pp.398–403 (2006).
12) Rommey, G.W., Jones, J.K., Rogers, B.L. and MacCabe, P.: IT Security Education is Enhanced by Analyzing Honeynet Data, *ITHET 6th Annual International Conference*, pp.F3D-10–14 (2005).
13) Vaughn, R.B. and Damper, D.A.: The Development of a University-based Forensics Training Center as a Regional Outreach and Service Activity, *The 40th Annual Hawaii International Conference on System Sciences* (*HICSS'07*), pp.1–8 (2007). http://csdl2.computer.org/comp/proceedings/hicss/2007/2755/00/27550265c.pdf
14) Dark, M.: A Framework for Information Security Ethics Education, *The 10th Colloquium for information Systems Security Education*, pp.109–115, CISSE (2006).
15) NPO 日本ネットワークセキュリティ協会：2005 年度情報セキュリティインシデントに関する調査報告書, Ver1.0 (July 2006). http://www.jnsa.org/result/2005/20060803_pol01/index.html
16) NRI セキュアテクノロジーズ：企業における情報セキュリティ実態調査 2005 報告書（単純集計）(July 2005). http://www.nri-secure.co.jp/news/2005/0720-report.html
17) NPO 情報セキュリティフォーラム：情報セキュリティに関するアンケート調査　調査報告書 (Mar. 2006).
18) NPO 日本ネットワークセキュリティ協会：2005 年度情報セキュリティ推奨教育の検討に関する調査報告書 (Apr. 2006). http://www.jnsa.org/result/2005/20060601_edu01.pdf
19) 星野　隆：大学の情報教育における情報セキュリティ教育の研究，中央学院大学商経論叢，Vol.18, pp.113–127 (2004).
20) Impress Watch Opinion/先進ユーザーアンケートセキュリティについて，*Goo research*, Vol.7 (Dec. 2006). http://research.goo.ne.jp/service/download.html
21) Nash, V. and Peltu, M.: Rethinking safety and security in a networked world: reducing harm by increasing cooperation, Oxford Internet Institute, Forum Discussion Paper, No.6 pp.1–30 (2005).
22) Web 上で個人情報を公開しすぎていませんか？, *Goo research*, Vol.6 (Oct. 2006). http://research.goo.ne.jp/service/download.html

(平成 18 年 11 月 27 日受付)
(平成 19 年 6 月 5 日採録)

松村真木子（正会員）

お茶の水女子大学人間文化研究科人間発達学専攻博士課程単位満期取得退学. 情報セキュリティに関心があり，一般エンドユーザの視点から，社会学的アプローチによる情報セキュリティ研究に取り組んでいる．また，1980 年代以降のイギリス社会の変容を統計データおよび面接調査から研究している．日本社会学会会員.