大学生の IT セキュリティ実践の現状と課題
—新たな教育プログラムの構築に向けて—

中村晋介 [1)], 柴田雅博 [1)],石崎龍二 [1)] ,森脇敦史 [1)]

1) 福岡県立大学　人間社会学部

nakamura@fukuoka-pu.ac.jp　mshibata@fukuoka-pu.ac.jp

ishizaki@fukuoka-pu.ac.jp　moriwaki@fukuoka-pu.ac.jp

Current Status and Issues of University Students' IT Security Practices

Towards the Construction of Contemporary Educational Programs.

Shinsuke Nakamura[1)], Masahiro Shibata[1)], Ryuji Ishizaki[1)], Atushi Moriwaki[1)]

1) Faculty of Human and Social Sciences, Fukuoka Prefectural University.

概要

近年，スマートフォンや無線 LAN 環境，常時接続といった新たな情報アーキテクチャが急速に整備・普及した．その結果，かつてはこの方面には無縁であった文系学部に通う大学生たちも，プライベート，あるいはオフィシャルな場面で，これらを活用して IT 環境を積極的に活用する事態が生じている．本報告は，量的調査の技法をもって，4 年制大学の文系学部に通う学生の IT 環境への順応度, 特に web 利用の実態とセキュリティに対する理解度・実践度を測った上で，こういった学生への IT セキュリティ教育プログラムのあり方を提案する．現代の大学生は，いわゆる「コンピューター」よりもスマートフォンを情報端末として利用する傾向が強い．しかし，彼／彼女たちは，いずれ職場でコンピューターを操作することになるだろう．以上を踏まえ，われわれは，以下 3 点を重視した教育プログラムの構築を提案する．すなわち，1)学生が（スマートフォンではない）コンピューターを使用する場合の注意点の教授，2)多くの学生が使用しているスマートフォンのセキュリティに関する知識の教授，3)同じく使用している学生が多い無線 LAN のメリット・デメリットの教授，の 3 点である．

1　はじめに

さまざまな生活の場面で，web を頻繁に利用している現代の日本人，特に若い世代の日本人は，IPA などが提唱する web セキュリティをどの程度まで実践しているのだろうか．筆者のうち中村晋介は 2011 年秋，福岡県内の 3 大学に通う学生（文系・理系）に対する量的調査を行い，591 名から有効回答を得た．

同調査（以下，「2011 年度調査」と表記）で得られた知見のうち主なものを以下に列挙する．1)85％を超える大学生が自宅に専用のコンピュータを持っているが，コンピューター・スキルは総じて低い．コンピューター・スキルが高い大学生と，低い大学生との間では，セキュリティ実践度に明確な格差がある．3) 1 日の web 閲覧時間の長さとセキュリティ実践度の高さは連動しているが，セキュリティに関してほとんど無知なまま，長時間 web に接続している者も少なくない．4)スマートフォンを利用している者は，全体の 20％程度であった[1].

この調査の後，日本ではスマートフォン，タブレット PC，SNS，オンラインストレージサービス，公衆無線 LAN サービスなどが急速に普及した. 公衆無線 LAN に接続したスマートフォンを片手に，SNS のチェックやゲームに興ずる若者，オンライ

ンストレージに保存した文書ファイルの編集作業を宿泊先や，喫茶店，あるいは公共交通機関の中で編集を加える社会人や研究者の姿を見るのは，もはや日常的な光景になっている．

しかし，大学教員である筆者らが学生と接してきた経験を顧みると，これらデバイスや web サービスを頻繁かつ積極的に使用している学生の多くが，web 上からの脅威に対する知識を持っていないように思われた．

学生が使う情報端末が大学内のコンピューターネットワークへの侵入口とされる可能性，学生や教員の未発表研究データや個人情報が漏洩する可能性などを考えると，これはかなり危険な状況とである．こういったことから，筆者らは大学生（あるいは専門学校生）――特に，情報系には「疎い」ことに劣等感や罪悪感を抱きにくい「文系」の学生――を対象とする情報セキュリティ教育プログラムを構築する必要性を感じるようになった．

その教育プログラムは，学生たちの状況を確認した上で，彼／彼女たちの弱点に対応する形で構築される必要がある．この観点から，筆者らは，2016 年度 10 月～11 月に，九州地方の公立大学の文系学部に通う学生を対象に，1)大学生をとりまく IT 環境，2)大学生たちのセキュリティ実践状況の実態を調査した．今回はその調査結果を報告した上で，構築すべき情報セキュリティ教育プログラムの方向性や内容について論じたい．

2　分析(1)――大学生の web 利用実態

2.1 調査方法

調査対象校として，九州地方に位置する公立大学 1 校の文系学部（学生の主たる専攻は，社会学，社会福祉学，心理学，幼児教育学など）を選出，2016 年 10 月～11 月にかけて量的調査を実施した．講義時間の前後に無記名の自記式調査票を配布，1)回答は厳重な管理のもとで直ちに記号化され，統計的に処理されるため，個人が特定されることはない．誰がどのように回答したかを個別に取り上げることもない．2)学術研究の報告書や論文として公開する場合，大学名も匿名化する．3)回答者には回答を拒否・放棄する権利がある，といった説明を口頭，及び調査票表紙で告知し，承諾した学生を対象に調査を実施，328 票（男子学生 20.1%/66 票，女子学生 79.9%/262 票）の有効票を得た．学年別の分布は，1 回生 37.5%（123 票），2 回生 36.0%（118 票），3 回生 13.7%（45 票），4 回生 13.7%（39 票），大学院生 0.9%（3 票）であった．

2.2 スマートフォンの利用状況

今回の調査では，対象者 328 名のうち 97.9%（321 名）がスマートフォンを所持していた．スマートフォン所持者に，「電話，メール，カメラ以外のスマートフォンの機能を使いこなせていると思うか」との問いを投げかけると，利用者の 57.5%（184 名）が「そう思う」「ややそう思う」との肯定的な回答を返した．回答者の 4.6%（15 名）が，「自宅には自分専用のコンピューターがない」状態にあるが，この 15 名全員がスマートフォンを所持していた．

次に，自宅で web を利用すると場合に，最も利用する端末の種類を訊いたところ，7 割近い学生がスマートフォンと答えていた（表 1）．2011 年度調査と比較すると，スマートフォン浸透度の著しさがうかがえた．

表 1: 自宅で web を閲覧する場合，最も利用する端末

	度数	%
デスクトップ型コンピューター	6	1.8%
ノートブック型コンピューター	86	26.2%
タブレット型コンピューター	3	0.9%
スマートフォン	225	68.6%
その他（ゲーム機など）	3	0.9%
DK/NA	5	1.5%
全体	328	100.0%

2.3 web サービス利用状況

各種 web サービスの利用について質問（多重回答）したところ，上位を占めたのは，「LINE, Skype などの無料通話アプリ」（94.5%），「youtube などの動画共有サイト」（90.8%），「twitter や Instagram などの短文や写真を共有するサイト」（86.0%），「amazon や楽天などの通販サイト」（72.5%）であった．一方で，「Facebook，mixi などの sns」（25.0%），「『2 ちゃんねる』などの匿名掲示板」（17.3%），「『ヤフーオークション』など，国内のオークションサイト」（12.5%），「Onedrive，dropbox などのオンラインストレージ」（8.8%）などを利用する者は少ない．また，web 上からの攻撃に晒されやすい「成人向け web

サイト」「現在放映中のアニメも配信している海外の動画サイト」「コミック・同人誌などを無料閲覧できる海外のサイト」「懸賞サイト／オンラインカジノサイト」を利用している者は，いずれも全体の 10%程度であった（パーセンテージは，「よく利用する」＋「たまに利用する」の合計）．「オンラインバンキング」を利用している者も 6.7%にとどまっていた．

2.4 無線 LAN の利用状況

回答者の 95.4%（313 名）が，自分専用のコンピューターを 1 台以上所持していた．ただしその 8.6%（27 名）は，所持しているコンピューターを web につないでいない．これら 27 名は，web 閲覧を全てスマートフォンで行っているものと推察される．これらコンピューターを web に接続する方法は，有線 LAN が 16.0%（50 名），無線 LAN が 66.8%（219 名）となっていた（「不明」が 5.1%，「web につないでいない」が 8.6%）．無線 LAN の普及具合がうかがえる．

自宅以外で無線 LAN を利用していると答えた者は全体の 257 名（78.4%）．利用場所と接続端末の種別を表 2，表 3 に示す．

表 2: 自宅以外で無線 LAN を利用する場所

通っている大学構内	43.9%
友人や親戚の家	35.5%
携帯キャリアの公衆無線LAN	22.9%
カフェやコンビニの公衆無線LAN	36.1%
ポケットWi-fi	7.1%
その他	1.2%
わからない	5.2%

多重回答

表 3: 自宅以外で無線 LAN に接続する端末

ノート型コンピューター	35.2%
タブレット型コンピューター	5.2%
スマートフォン	93.6%
携帯ゲーム機	6.8%
その他の端末	2.8%

多重回答

以上，今回の調査対象となった文系の大学生たちが，可搬性が高い携帯端末であるスマートフォンを積極的に活用して，自室あるいは屋外で，無線 LAN に接続，動画共有サービスや，twitter や Instagram などの sns，そして LINE などの無料通話アプリを利用している姿が浮き彫りにされた．

2011 年度調査と比較すると，スマートフォンと無線 LAN と主軸とする新たなアーキテクチャの普及が，若者の IT 環境を大きく変化させたことがわかる．web 接続用の端末がノート型 PC からスマートフォンに変化した結果，スマートフォンでの閲覧，書き込みに適した web サービスの利用が優先されるようになった．その典型が，近年何かと話題になることが多い twitter や Instagram，LINE といったサービスである．

一方，コンピューター上のブラウザを使っての閲覧／利用を前提としたアダルトサイト，海外の違法動画／画像共有サイト，オンラインカジノ，オンラインバンキング，（従来型の）web オークションサイト，blog 型の sns（Facebook や mixi など），オンラインストレージなどのサービスを利用する大学生の数は頭打ちになっているようだ．2.3 で示した web サービス利用状況のかたよりは，ここに由来するものだろう．

3 分析(2)——大学生の IT スキル／セキュリティに関する知識・評価

3.1 大学生のコンピューター・スキル／セキュリティに関する知識

対象者に，自らのコンピューター・スキルを自己評価させた結果が表 4 である．性別で比較した場合，男子学生の方が自己評価が高くなったが（χ^2=21.476（df=3），p＜.001），その男子学生でも，「トラブルを解決できる」と称した者は 6.1%（4 名）にすぎなかった．一方，専攻，学年による有意差は出なかった．

表 4: 学生のコンピューター・スキル自己評価

	自分で組み立てたり、トラブルを解決できるレベル	ソフトをインストールしたり、コンピューターの設定を変えられるレベル	メールやインターネットを使ったり、文章をグラフを書けるレベル	簡単な操作しかわからないレベル	全体
男性（n=66）	6.1%	39.4%	48.5%	6.1%	100.0%
女性（n=262）	0.0%	27.1%	61.8%	11.1%	100.0%
合計（n=328）	1.2%	29.6%	59.1%	10.1%	100.0%

対象を自分専用のコンピューターを所持する学生に限定して，「そのコンピューターの初期設定は誰がどう行ったか」を質問したところ，「自力で行

った」は，全体の 1/4 程度（26.8%）に過ぎず，圧倒的多数は，購買店や大学生協のセットアップサービス，家族や友人に任せていた．くわえて，自分が専用で使っているコンピューターの OS の種類を答えられなかった者が 17.4%（54 名）に達していたことも懸念事項である．

自分が使用しているコンピューターのセキュリティ対策状況への自己評価を問うたところ,「かなり自信がある」が 3.8%（12 名),「少し自信がある」は 31.3%（98 名),「あまり自信がない」「全く自信がない」がそれぞれ 56.2%（176 名），8.2%（27 名）であった．性別，専攻，学年で比較したところ，性別でのみ有意差が現れた（男性の方で「かなり自信がある」「少し自信がある」者が増えていた（χ^2=18.04（df=3）p＜.001）．

本調査で使用した調査票では,「警告メッセージの意味理解度」(Java アップデートの警告,「管理者権限が必要」とのメッセージ,「無線 LAN が安全ではない」との警告，など 8 項目),「セキュリティ実践に関する知識度」(OS の修正プログラムの配布状況を確認できるか，手動でウイルススキャンをかけられるか，ファイルの暗号化方法を知っているか，など 8 項目),「IT セキュリティに関するキーワードの理解度」(ブラウザハイジャッカー，標的型攻撃，アカウントハック，ジオタグ情報，など 17 項目）を質問している．これらの質問への回答にそれぞれ得点を与えた上で，回答者ごとにそれぞれの合計得点を算出した．

3 種類の理解度／知識度得点の平均値は決して思わしくない．理論上は 32 点で満点となる「警告メッセージの意味理解度」「セキュリティ実践の知識度」の平均得点は，それぞれ 13.63 点，17.73 点に過ぎなかった．68 点満点となるはずの「IT セキュリティに関するキーワード理解度」の平均得点に至ってはわずか 24.56 点であった [1)].

ただし，自分が使用しているコンピューターのセキュリティへの自信に基づいて回答者を 4 群にわけ，これら 3 得点の平均値を分散分析で比較したところ，その全てで有意差が現れた（表 5）．一部の大学生が持つ「IT セキュリティに関する自信」は，具体的な知識に裏打ちされていることを示唆している．

表 5:各種得点の比較

	ｾｷｭﾘﾃｨへの自信度	度数	平均	標準偏差	分散分析結果
警告メッセージの意味理解度得点	かなり自信がある	12	19.333	7.303	F=12.91 p＜.001
	少し自信がある	96	15.469	5.940	
	あまり自信がない	175	12.606	4.780	
	全く自信がない	26	11.038	4.643	
セキュリティ実践の知識度得点	かなり自信がある	12	24.083	6.302	F=15.19 p＜.001
	少し自信がある	96	19.896	6.017	
	あまり自信がない	170	16.465	5.313	
	全く自信がない	25	14.960	4.695	
ITｾｷｭﾘﾃｨに関するｷｰﾜｰﾄﾞ理解度得点	かなり自信がある	11	38.182	11.496	F=9.70 p＜.001
	少し自信がある	94	32.340	9.826	
	あまり自信がない	171	28.497	8.756	
	全く自信がない	25	24.560	5.355	

3.2 IT セキュリティの実践に関する大学生の評価

今回の調査では,「IT セキュリティの実践」,「IT セキュリティ教育の現状に関する評価」について，13 項目の質問を回答者たる大学生に投げかけている．

これら 13 項目のうち,「なぜ,（特に文系の）大学生たちは IT セキュリティの知識を得ること, それを実践することに消極的なのか」に関連する 7 設問を抽出し，その内的構造を因子分析で検討した．天井効果，フロア効果は特に見られなかったので, 該当する 7 設問を全て投入し分析を行った．因子抽出法は最尤法，回転はクオーティマックス法を使用し，表 6 のパターン行列を得た．なお，Kaiser-Meyer-Olkin のサンプリング適切性基準は .711（middling），適合度検定の結果は χ 2(df=8)=27.021，p＜.001 であった．

表 6:因子分析結果

	因子1	因子2
難しい専門用語が多すぎて、何の話をしているかわからない	**.647**	.073
どこを調べれば対策が書かれているのか、普通の人には見つけ出せない	**.826**	.166
対策方法が複雑すぎて、普通の人では対応が難しい	**.813**	.230
何らかのセキュリティソフトをインストールしておけば、基本的に大丈夫だと思う	.120	**.529**
うかつな書き込みや、常識をはずれた写真を投稿しなければ大丈夫だと思う	-.003	**.780**
ｱﾀﾞﾙﾄｻｲﾄや、著作権を無視している違法動画サイトに近づかなければ大丈夫だと思う	.055	**.698**
インターネットにはまっていない人には無関係な話だと思う	.137	**.396**

「難しい専門用語が多すぎて，何の話をしているか分からない」,「対策方法が複雑すぎて，普通の人には対応が難しい」といった質問に負荷量が高い第 1 因子は,「IT セキュリティの実践方法の

難解さ」と命名することができよう．この方面に対し一定の知識を持つ者は，デスクトップ画面に表示される各種ソフトのアップデート警告や信用あるセキュリティソフトの通知，あるいは MyJVN バージョンチェッカが示す対策を取るだけで，一般ユーザーが直面するリスクのほとんどは回避できること――IT セキュリティの実践はむしろ単なるテクニックやスキルの位相にあること――を知っている．この因子は，IT セキュリティ実践を，実際以上に難しいものと考えてしまう意識と解釈できるだろう．

「何らかのセキュリティソフトをインストールしておけば大丈夫だと思う」，「アダルトサイトや違法サイトに近づかねば問題ない」，「インターネットにはまっていない人には無関係な話だと思う」といった質問に高い負荷量を示す第 2 因子は，「IT セキュリティ実践への過信」と解釈できる．

留意すべきは，2009 年の日本で猛威を振るった drive-by-download 攻撃が，一般企業や公的機関の web サイトを改ざんしたこと，むしろライトユーザーを標的にしていたことだ．また，2017 年現在，多くのブラウザハイジャッカーやマルウェア，アドウェアが，不注意なライトユーザーが「自発的に」ダウンロード／インストールすることを狙って開発・配布されている．おそらくは自分をライトユーザーと認識している文系の大学生たちにこういった意識が見られたことは，深刻な問題として受け止めるべき問題だろう．

これら 2 因子の因子得点を回答者ごとに算出し，今回の調査で用いられた調査票に配置された他の設問への回答分布との関係を探っていった．

まず，当該大学で，IT セキュリティについて言及している講義の履修状況に基づいて対象者を 2 群（履修済み+現在履修中／履修する予定はない）にわけ，因子得点の平均値を比較したところ，第 1 因子「IT セキュリティの実践に対する過大評価」で有意差が現れた（t=-2.377，p＝.018）．当該科目を「履修する予定がない」と答えた者で，IT セキュリティの実践をより難しいものと考える傾向が現れていた．

残念ながら，今回準備した調査票では，当該講義を受講する予定がないと回答した者に対して，その理由を問いかける質問を配置していない．しかし，その原因がいかなるものであろうと，IT セキュリティについて言及する講義を受講することが，セキュリティ実践を実際以上に困難なものとする意識を抑制する効果を生み出していることは間違いない．

ついで，1 日の web 利用時間（メールや LINE の利用時間は除く）によって回答者を 4 群（1 時間未満，1～2 時間未満，2～3 時間未満，3 時間以上）に分け，因子得点の平均値を比較したところ，ここでも第 1 因子のみで有意差が現れた．1 日 3 時間以上 web を利用している者は，IT セキュリティの実践を難しすぎると考えてはいない．逆に言うと，それ以外の web ライトユーザーは，IT セキュリティの実践を実際以上に困難なものと見積もり，二の足を踏んでいる様子がうかがえる．

表 7:因子得点比較

		度数	平均	標準偏差	分散分析結果
因子 1	1 時間未満	57	-0.018	0.900	F=3.997 p=.008
	1～2 時間未満	103	0.101	0.887	
	2～3 時間未満	64	0.150	0.837	
	3 時間以上	87	-0.290	0.955	
	全体	311	-0.020	0.912	
因子 2	1 時間未満	57	-0.052	0.859	F=.679 p=.566
	1～2 時間未満	103	0.016	0.822	
	2～3 時間未満	64	0.083	0.791	
	3 時間以上	87	-0.104	0.921	
	全体	311	-0.016	0.850	

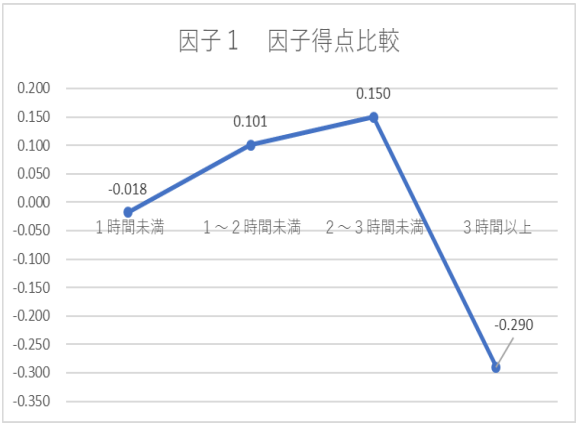

図1:因子1の因子得点比較

なお，有意差は出なかったが，1 日の web 利用時間が長い回答者は，スマートフォンよりもコンピューター（デスクトップ，ノートブック，タブレット型）を web 閲覧用端末として利用する傾向が見られた（表 8）

表 8:web を閲覧する端末×web 閲覧時間

自宅でwebを閲覧する端末→ 1日のweb閲覧時間↓	コンピューター	スマートフォン	合計
1時間未満(n=56)	26.8%	73.2%	100.0%
1～2時間未満（n=103）	25.2%	74.8%	100.0%
2～3時間未満（n=64）	31.3%	68.8%	100.0%
3時間以上（n=87）	33.3%	66.7%	100.0%
全体（n=310）	29.0%	71.0%	100.0%

3.1 で示したように，本研究では，対象者 1 人 1 人に対して「警告メッセージの意味理解度」,「セキュリティ実践の知識度」,「IT セキュリティに関するキーワード理解度」を得点化した. 自宅で web を閲覧する場合の端末として，もっぱらコンピューターを使用する群と，もっぱらスマートフォンを使用する群との間で，これら 3 つの理解度／知識度得点を比較すると，全てにおいて，もっぱらコンピューターを利用する群で得点が高くなっていた（表 9）.

表 9:理解度／知識度得点の比較

	自宅でwebを閲覧する端末	度数	平均値	標準偏差	t検定結果
警告メッセージの意味理解度得点	コンピューター	93	15.796	5.445	t=4.784 p<.001
	スマートフォン	223	12.596	5.353	
セキュリティ実践の知識度得点	コンピューター	94	19.277	6.534	t=3.292 p=.003
	スマートフォン	217	16.940	5.375	
ITセキュリティに関するキーワード得点	コンピューター	90	31.500	9.988	t=2.275 p=.031
	スマートフォン	218	28.867	8.792	

4 結論

2001 年，Mark Plenskey は，物心ついたときには既にインターネット環境が整備されており，生まれながらに IT 環境に親しんでいる世代を「Digital Natives」と呼称した．しかし，彼がこの言葉を生み出したとき，Digital Natives が使用していた主たる情報端末はあくまでパーソナル・コンピューターであり，インターネット環境への接続は基本的に有線であった[2].

しかし，今回の調査で明らかになったのは，現代の大学生が，たとえ文系であっても，スマートフォンを用いて，無線で web に常時接続し続ける存在，いわば「Smartphone Natives」となっている事実である（表 1～表 3）．学生が日常的に利用している web サイトのかたよりも，彼／彼女たちが web を閲覧する情報端末がノート型コンピューターからスマートフォンに変化したことと連動しているものだろう（本稿 2.3）.

スマートフォンの普及が, 期せずして Microsoft Windows 上で動作するマルウェアや，コンピューターを用いての web ブラウジングを行う者を標的とする攻撃から，現代の大学生を守る暫定的な防波堤になっている可能性は否定できない．情報教育に関わってきたわれわれは，いわゆる「アダルトサイト」や，著作権の面で問題がある違法動画／画像共有サイト，オンラインカジノ,「匿名」や「アンダーグラウンド」を謳う掲示板やネットワークへの不用意なアクセスが，しばしば drive-by download 攻撃やアカウントハックが万円する原因となり続けてきたことを知っているからだ.

事実，今回の調査対象者たちに，過去に遭遇したインシデント経験を問うたところ，偽セキュリティソフトやブラウザハイジャッカーに代表されるマルウェアや，アカウントハックによる深刻な被害を受けた者の数は予想以上に少なかった（表 9）．むしろ学生たちが気にかけているのは，迷惑メールや sns 上での友人申請など，無視／ブロックなどの処置で回避できる程度の軽微な問題である．いささか逆説めくが，こういった状況が，大学生たちの IT セキュリティ意識や実践へのインセンティブを阻害する要因になっている可能性も否定できない[2)].

しかし，大学を出た後の就職先で彼／彼女たちのほとんどは，スマートフォンではない「コンピューター」を業務で使うことになるはずだ．そうである以上，大学で情報教育に携わる者は，学生たちに, コンピューターを使う場合の IT セキュリティの知識と実践方法を重点的に教授する必要がある．くわえて，ここ数年，スマートフォン上で動作する OS やアプリの脆弱性を衝く攻撃や，スマートフォン利用者を狙う攻撃，特にランサムウェアの急増が報告されていることにも，われわれは注意を払う必要がある[3].

ここまでの議論を踏まえ，筆者らは，現在の学生が，コンピューターよりもスマートフォンを使ってきた／使おうとする Smartphone Natives 世代であることを念頭に置いた新たな IT セキュリティに関する教育プログラムの早急な構築を提案したい.

このような教育プログラムを提供することは,

学生たちのニーズに応えることでもある．実は，今回協力してくれた文系大学生の 9 割近くが，各種のサイバー攻撃を「いつか自分にふりかかるかも知れないと怖くなる」し，「学校教育の場で対策をきちんと教えていくべきだ」と感じていた（図 2，図 3）．

表 9：過去に遭遇したインシデント

	度数	%
ブラウザや壁紙などの設定が勝手に書き換えられた	11	3.5%
セキュリティソフトがウイルスを自動削除した	54	17.1%
コンピューターの調子が悪くなり、詳しい人や業者にウイルスと言われた	17	5.4%
アダルトサイトや知らないソフトの広告がポップアップするようになった	58	18.4%
知らないソフトがいつの間にかインストールされていた	24	7.6%
偽のセキュリティソフト/高速化ソフトをインストールしてしまった	7	2.2%
ネットオークションやネット通販でのトラブル	9	2.8%
ネットゲームやソーシャルゲームでのアカウントハック	9	2.8%
誰かが、自分になりすまして掲示板はSNSに書き込みを行った	11	3.5%
迷惑メールが１日に10通以上来るようになった	118	37.3%
twitterやSNSで、知らない人から「友だちになってください」などの連絡を受けた	129	40.8%
twitterやSNSで、自分の姿が写った写真が知らないうちにアップロードされた	13	4.1%
twitterやSNSで、身に覚えがないウワサ話が広がってしまった	2	.6%
架空請求のメールや電話が届いた	54	17.1%
その他	8	2.5%
上記のような経験は１つもない	80	25.3%

多重回答

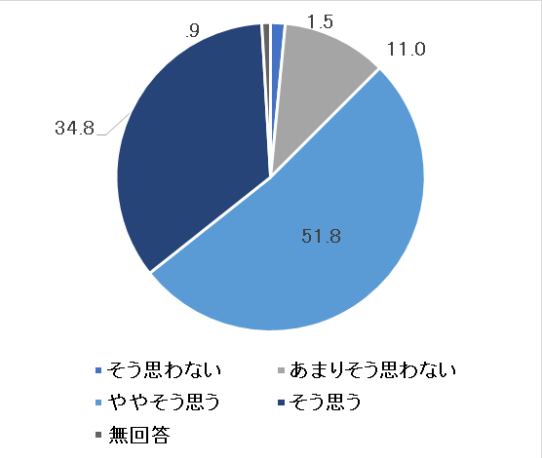

図 2：サイバー攻撃がいつか自分にふりかかるかも知れないと怖くなる（n=328）

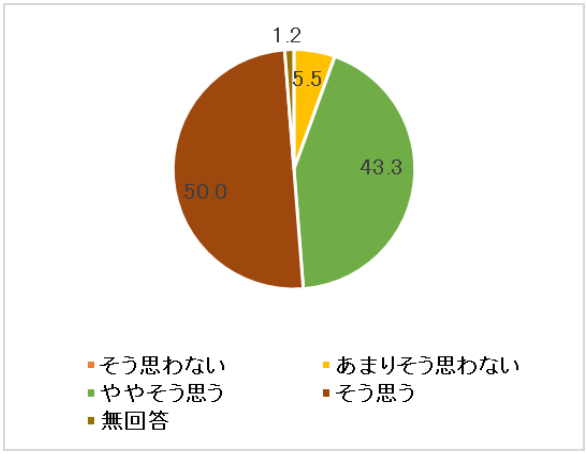

図 3：サイバー攻撃への対処法を学校教育の場できちんと教えていくべきだ（n=328）

この教育プログラムにおいて，特に重視されるべきは，1)学生がノート型／デスクトップ型コンピューターを用いる場合に取るべきセキュリティ実践の方法を，スキルやテクニックとして教えること――特にオンラインストレージやオンラインバンキングなど，スマートフォンではアクセスしづらいが故に学生たちがほとんど利用していない web サービスの安全な利用方法を教授すること，2)学生が，スマートフォンを使用する場合のセキュリティ実践について明確な知識と方法を教える，3)無線 LAN のメリット・デメリットを明白に伝える，の 3 点だと考えられる [3]．

この 3 点を挙げる理由を最後に述べたい．1)の理由としては，Smartphone Natives 世代たる現代の文系大学生には，コンピューターを使用する場合のセキュリティに関する知識があまりに希薄であること，くわえて IT セキュリティの実践方法を，実際以上に困難なものと認識していることが挙げられる（3 節）．

2)の背景には，今回の調査で，スマートフォンのセキュリティに関する文系大学生の理解や実践の不十分さが暴かれたことが指摘できる．

筆者らは，本稿 2 節で，今回の調査に協力してくれた大学生の 9 割以上がスマートフォンを日常的に使っていること，特に web に接続する端末として使用していることを示した．しかし，彼／彼女たちのうち，「自分のスマートフォンに有料のセキュリティソフトを入れている」者はわずか 5.7%（18 名）に過ぎなかった（「いいえ」が 62.5%，「わ

からない」が 29.9%）．その一方で，「無料セキュリティソフト」，「節電機能を持つアプリ」，「受信状況を改善するアプリ」など，動作に不安があるアプリ，あるいはマルウェアの疑いもあるアプリをインストールしている者は，それぞれ 34.5%（110 名），27.1%（89 名），9.1%（29 名）に達していた．

3)の理由も，今回の実態調査から導かれている．筆者らは本稿 2 節で，多くの文系大学生が，公衆無線 LAN を利用して自らのスマートフォンやノートブック型コンピューターを web に接続させ，各種 web サービスを利用していることを指摘した．しかし，「公衆無線 LAN を利用するにあたって注意していること」について学生に質問したところ，多くの学生が不注意な接続を行っている事実が判明した（表 10）．

2020 年のオリンピック開催に向けて，公衆無線 LAN がつながるエリアの拡大が推進されている現在，若い世代にとって，公衆無線 LAN を利用することは，2017 年の現在以上に，「普通の習慣」となることが十全に予想される．しかし，公衆無線 LAN が，通信内容の盗聴や，アカウント乗っ取りの舞台となりやすいサービスであることは言うまでもない[4]．

この点を知る者からすれば，今回の調査対象者たちが実践している公衆無線 LAN サービスの利用方法はあまりに無防備かつ安易だと言わざるを得ない．

表 10：公衆無線 LAN を使用するにあたって注意していること

	注意したことがない	あまり注意したことがない	ときどき注意している	いつも注意している	合計
セキュリティ保護の確認（n=256）	11.3%	36.7%	36.7%	15.2%	100.0%
公衆無線LANの設置者（n=255）	20.8%	40.4%	23.9%	14.9%	100.0%
端末に表示される警告文の内容（n=256）	11.3%	33.2%	34.8%	20.7%	100.0%

表 3 で見たように，調査対象者たちが，最も頻繁に公衆無線 LAN に接続する端末はスマートフォンであった，しかし，前頁で述べたように，そのスマートフォンに「有償のセキュリティソフト」をインストールしている者はわずか 5.7%に過ぎなかった．この状況を鑑みると，公衆無線 LAN の危険性，特にセキュリティ対策を施していないスマートフォンでそのサービスに接続することの危険性を学生に教授することは，構築すべき新たな情報教育プログラムにおいては必須事項だろう．

おわりに

今回の分析で明らかになった点をもとに，筆者らは今後，具体的な教育プログラムの内容や教材を開発していく予定である．

注

1)合計得点の信頼性分析結果を以下に示す．「警告メッセージの意味理解度」：α=.940，「セキュリティ実践の知識度」：α=.870，「IT セキュリティに関するキーワード理解度」：α=.929

2)このインシデント遭遇経験はあくまで対象者たる学生の自己申告である．所有者本人が気づかないままに，バックドアプログラムに感染していたり，ボットネットに組み込まれているコンピューターが存在している可能性は否定できない．

参考文献

[1] 中村晋介「大学生の web セキュリティ実践――量的調査の結果より」『福岡県立大学人間社会学部紀要』vol.21-2:1-14,2013.

[2] Marc Prensky, Mark,”Digital Natives, Digital Immigrants” On the Horizon Vol. 9-5, 2001.

[3] トンドマイクロ，「最新モバイル脅威事情：1 年で 4 倍！急増するモバイルへのランサムウェア攻撃」,2016. http://blog.trendmicro.co.jp/archives/13808（2017 年 9 月 21 日閲覧）

[4] 野澤祐一・小川貴之『公衆無線 LAN 利用に関わる脅威と対策――公衆無線 LAN を安全に利用するために』独立行政法人情報処理推進機構技術本部セキュリティセンター,2016. https://www.ipa.go.jp/files/000051453.pdf（2017 年 9 月 25 日閲覧）

◆本研究は，平成 28 年度文部科学省科学研究費基金基盤研究 C「大学生の IT セキュリティに関する新たな教育プログラムの構築」（課題番号 16K01122，研究代表者：中村晋介）の一環として実施されました．