福岡県立大学人間社会学部紀要
2018, Vol. 27, No. 1, 65－76

研究ノート

文系大学生のITセキュリティ実践の現状と課題

―現代的教育プログラムの構築に向けて―

中　村　晋　介*・柴　田　雅　博**・石　崎　龍　二***

Abstract：In recent years, we have seen the rapid establishment and spread of new information architectures such as smartphones, wireless LAN environments, and always-on connections. As a result, even university students studying humanities subjects, who traditionally would not be associated with this subject area, utilize these architectures in both their private and official capacities. Using quantitative surveying techniques, we measured the level of adaptability to IT environments, and, in particular, the state of web use and understanding and practical application of security issues, of university students studying humanities. The objective of this paper is to use these results to propose methods of teaching IT security programs to these students. We consider an educational program focusing on the following three points should be rapidly constructed and implemented: 1) items to take note of when students use computers (particularly, computers operating with the Windows OS), 2) knowledge regarding methods of implementing security on smartphones, and 3) the merits/demerits of using public wireless LANs.

Keywords：Informatics Education, IT Security, Smartphone

1．はじめに

さまざまな生活の場面で，インターネット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などが提唱するインターネット・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）

＊福岡県立大学人間社会学部・准教授
＊＊福岡県立大学人間社会学部・講師
＊＊＊福岡県立大学人間社会学部・教授

に対する量的調査を行い，591名から有効回答を得た[1)]．

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．　２)１日のインターネット接続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，長時間インターネットに接続している者も少なくない．３)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（８割がフィーチャーフォンを使用)．

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は，もはや日常的光景となっている．

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，こういった学生（あるいは大学教員）の多くが，インターネット上からの脅威に対し，あまりにも無知であるようだ．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慮すると，これはかなり危険な状況である．この危惧から，筆者らは大学生――特に，情報系に「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，現代的な情報セキュリティ教育プログラムを構築する必要性を痛感していた．そのためには，まず文系大学生の実情を把握する必要がある．われわれは，2016年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，構築すべき教育プログラムの方向性について論じたい．

２．分析⑴―大学生のインターネット利用実態

２．１　調査方法

調査対象校は，九州地方に位置する公立大学１校の文系学部（学生の主な専攻は，社会学，社会福祉学，心理学，幼児教育学など）である．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，２)結果は学術研究の報告書や論文としてのみ利用する，３)大学名も匿名化する，４)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，承諾した学生のみに調査票を配布，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，自宅でインターネットを利用する場合に，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回答した（表１）．

表１：自宅でwebを閲覧する場合、最も利用する端末

	度数	％
スマートフォン	225	68.6
ノート型コンピューター	86	26.2
デスクトップ型コンピューター	6	1.8
タブレット型コンピューター	3	0.9
その他（ゲーム機など）	3	0.9
DK/NA	5	1.5
全体	328	100

DK/NA：無効回答

２．３　各種webサービスの利用状況

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，インターネット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」の利用者は，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」の利用者も6.7％にとどまった．

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インターネットにつないでいない．これらコンピューターをインターネットに接続する方法は，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％）．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．

2011年度調査と比較すると，スマートフォンと無線LAN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．インターネット接続用の端末がノート型PCからスマートフォン

表２：自宅以外で無線LANを利用する場所

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

多重回答（n＝328）

表３：自宅以外で無線LANに接続する端末

	%
スマートフォン	93.6
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
携帯ゲーム機	6.8
その他の端末	2.8

多重回答（n＝328）

に変化した結果，スマートフォンでの閲覧，書き込みに適したインターネット・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．

文系の大学生たちは，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を利用して，スマートフォンでの閲覧に最適化されたインターネット・サービスを利用している．その一方，コンピューター上のブラウザを使っての閲覧／利用を前提としたインターネット・サービスからは離れがちになっている．本稿２．３で示したサービス利用状況の偏りは，ここに由来しているものだろう．

３．分析⑵―大学生のITスキル／セキュリティに関する知識・評価

３．１　大学生のスキルと知識

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（表４）．性別で比較した場合，男子学生の方が自己評価が高かったが，男子学生でも，「自分で組み立てられたり，トラブルを解決できる」者は6.1％（４名）にすぎなかった．

自分専用のコンピューターを所持する学生に限定し，「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，圧倒的多数が，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．

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3.7％（12名），「少し自信がある」は29.9％（98名），「あまり自信がない」「全く自信がない」がそれぞれ53.7％（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）（表５）．

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，文章や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
全　体　（n＝328）	1.2	29.6	59.1	10.1	100.0

χ^2＝21.476（df＝3）p＜.001

表５：コンピューター・セキュリティ対策状況への自信（%）

	かなり自信がある	少し自信がある	あまり自信がない	全く自信がない	自分専用のコンピューターがない	全体
男　性　(n＝66)	3.0	48.5	34.0	3.0	10.6	100.0
女　性　(n＝262)	3.8	25.2	58.4	9.5	3.1	100.0
全　体　(n＝328)	3.7	29.9	53.7	8.2	4.6	100.0

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，回答者ごとに合計得点を算出した．

「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」は32点で満点となる．しかし「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」の平均得点はわずか24.56点であった（クロンバックの信頼性係数αは，「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となり，これらはいずれも妥当な尺度とみなせる）．

ついで，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

表６：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	5.94	
	あまり自信がない	175	12.606	4.78	
	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	175	16.465	5.313	
	全く自信がない	26	14.960	4.695	
ITセキュリティに関するキーワード理解度得点	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	9.626	
	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	

４群にわけ，これら３種類の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６）．コンピューターのセキュリティ対策状況への自己評価と３種類の理解度／知識度得点には相関があった．

３．２　ITセキュリティ実践に関する自己評価

本調査では，「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項目の質問の中で，「なぜ，（文系の）大学生は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項目を抽出，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項目を全て投入し分析（因子抽出は最尤法，回転はクオーティマックス法）を行い，表７に示す２因子解を得た．なお，本因子分析の適合度検定の結果は$\chi^2=27.021$ $(df=8)$，$p<.001$であった．

第１因子は，「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」，「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．ITセキュリティの実践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，情報教育に携わる者にとっては周知の事項であるJVN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，理屈を知らなくても，単なる手順／スキルの位相で解決できること――を理解しているはずだ．本因子は，ITセキュリティ実践を，実際以上に難しいものと考える意識と解釈できる．以上のことから第１因子を，「ITセキュリティの実践方法の難解さ」と命名した．

第２因子は，「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」といった質問に因子負荷量が高い．この因子を「ITセキュリティ実践への過信」と命名した．

これら２つの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た．

まず，当該大学で，調査当時にITセキュリティについて言及していた講義（講義名：情報科学）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）に分け，両群で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（表８）．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ある．

ついで，１日のインターネット利用時間（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（表９，図１）．１日３時間以上インターネット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，その知識を学ぶことに躊躇している様子がうかがえる．

表７：因子分析結果

	第１因子	第２因子	共通性
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	0.826	0.166	0.710
対策方法が複雑すぎて，普通の人では対応が難しい	0.813	0.230	0.714
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	0.647	0.073	0.424
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	-0.003	0.780	0.608
アダルトサイトや，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	0.055	0.698	0.490
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	0.120	0.529	0.294
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	0.137	0.396	0.176
因子寄与	1.798	1.618	3.416
因子寄与率（%）	25.7	23.1	48.8

表８：講義の受講状況による因子得点の比較

	講義履修状況	度数	平均値	標準偏差
因子１：ITセキュリティ実践方法の難解さ	履修済み＋履修中	150	-0.115	0.856
	履修予定なし	163	0.133	0.952
因子２：ITセキュリティ実践への過大評価	履修済み＋履修中	150	-0.004	0.793
	履修予定なし	163	0.012	0.948

平均値比較（ｔ検定結果）

	ｔ値	自由度	有意確率（両側）	平均値の差
因子１：ITセキュリティ実践方法の難解さ	-2.43	310.841	0.016	-0.248
因子２：ITセキュリティ実践への過大評価	-0.16	308.251	0.871	-0.016

表９：因子得点比較（インターネット利用時間別）

	１日の利用時間	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	-0.116	0.850	

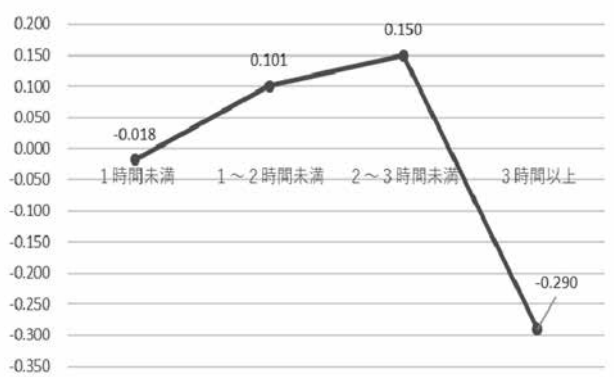

図１：因子１の因子得点比較（インターネット利用時間別）

なお，有意差は出なかったが，１日のインターネット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（デスクトップ型，ノート型，タブレット型）をインターネット閲覧用端末として利用する傾向が見られた（表10）．

本稿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．自宅でインターネット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

表10：インターネットを閲覧する端末×閲覧時間（%）

自宅でインターネットを閲覧する端末→ １日のインターネット閲覧時間↓	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

表11：理解度／知識度得点の比較

	自宅でインターネットを閲覧する端末	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	19.272	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	

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，コンピューターを利用する群の得点が高い（表11）．

４．大学生のインシデント経験

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，基本的に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，スマートフォンを用いて，無線でインターネット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サイトの偏りも，彼／彼女たちが，インターネットに接続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（本稿２．３）．

今回の調査対象者に，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，アカウントハックといった深刻な被害を受けた者の数は予想以上に少なかった（表12）．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蔓延する原因となり続けてきたことを知っている．しかし，こういったwebサイトや掲示板の大半は，コンピューターのブラウザで見ることが前提となった作りとなっている．調査対象者におけるインシデント経験の少なさは，利用端末の多くがスマートフォンであることが幸いして，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サイト閲覧を行う者を標的とする攻撃から，守られているに過ぎないのではないだろうか．

多くの大学生たちは，迷惑メールやSNS上での友人申請などといった軽微な問題にのみ遭遇している．ただし，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ことに注意されたい．学生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個人情報を抜かれていたり，ボットネットに組み込まれ，第三者による攻撃の踏み台となっているコンピューターは少なからず存在しているかも知れない．ここで留意すべきは，2009年の日本で猛威を振るい，一般企業や公的機関のwebサイトを改ざんしたdrive by download攻撃が，もっぱらインターネットにあまり詳しくないライトユーザーを標的にしていたことだ．また，2018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．

しかし，大学を出た後，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」（文系である以上，多くはWindows OSとなることが想定される）を業務で使うことになるはずだ．そうである以上，

表12：過去に遭遇したインシデント

	度数	%
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
迷惑メールが１日に10通以上来るようになった	118	37.3
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
セキュリティソフトがウィルスを自動駆除した	54	17.1
架空請求のメールや電話が届いた	54	17.1
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	25	7.6
コンピューターの調子が悪くなり，詳しい人や業者からウイルスと言われた	17	5.4
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ていた	13	4.1
ブラウザや壁紙などの設定が勝手に書き換えられていた	11	3.5
誰かが，自分になりすまして掲示板やsnsに書き込みをおこなった	11	3.5
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
ネットオークションやネット通販でのトラブル	9	2.8
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
twitterやsnsで，身に覚えがないウワサ話が広まってしまった	2	0.6
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

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だろう．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)]．

５．結論：教育プログラムの構築に向けて

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約９割が，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（表13，表14）．

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

表13：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）

そう思う	ややそう思う	あまりそう思わない	そう思わない	無回答	合計
34.8	51.8	0.9	1.5	11.0	100.0

表14：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）

そう思う	ややそう思う	あまりそう思わない	そう思わない	無回答	合計
50.0	43.3	5.5	0.0	1.2	100.0

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インターネット・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．

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（本稿3．2）

2)の理由は，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明確になったからである．今回の調査では，大学生のスマートフォン利用度の高さが浮き彫りにされたが，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）であった（「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／マルウェアの疑いすらあるアプリを自らのスマートフォンに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た．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インターネットに接続させ，各種webサービスを利用していることを指摘した．しかし，今回の調査では，多くの大学生が，無防備かつ不用意に公衆無線LANを利用していることも明らかにされている（表15）．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]．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，既に見たように，これほどスマートフォンを用いて公衆無線LANを利用しているにもかかわらず，接続端末たる自ら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の比率はわずか5.7%にとどまっていた．

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と判断できる．今回調査対象となった大学では，ITセキュリティの基礎を教授する講義の中で，この点に言及しているとの説明を受けた

表15：公衆無線LANを使用するにあたって注意していること

注意度→ 確認項目↓	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

が，教員はともかく，この点が今後重要になるとの認識を持った受講生の数は，少なくとも現状では決して多くなさそうである．

謝辞

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）の一環である．本稿は大学ICT推進協議会年次大会一般セッションでの口頭発表「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」のプロシーディングス（大会発表論文集）と当日の質疑をもとに，構成や表現を改める形で作成された．改稿に際して，統計分析は全てやりなおしている．

文献

1）中村晋介（2013），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，21巻，２号1-14.

2）Prensky C.（2001），“Digital Natives, Digital Immigrants,” *On the Horizon*, Vol. 9-5, 1-6.

3）トレンドマイクロ（2016），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.
http://blog. trendmicro. co. jp/archives/13808（2017年９月21日閲覧）

4）野澤祐一・小川貴之（2016），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.
https://www.ipa.go.jp/files/000051453.pdf（2017年９月25日閲覧）