福岡県立大学人間社会学部紀要
2012, Vol. 21, No. 2, 1－14

大学生のwebセキュリティ実践

―量的調査の結果より―

中　村　晋　介

要旨　研究活動や趣味の活動において，webを頻繁に利用している現代の大学生は，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．これを明らかにするために，著者は2011年秋，福岡県内の３大学に通う学生に対する量的調査を行い，591名から有効回答を得た．主な分析結果は以下の通り．1）８割以上の大学生が自宅に専用のコンピュータを持っているが，コンピュータスキルは総じて低い．2）webセキュリティの実践度は著しく低い．コンピュータスキルが低いグループでは特に顕著である．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．各大学は，所属する学生に対して，コンピュータセキュリティに対する知識を高め，その実践を促す教育プログラムを早急に構築・実践すべきである．
キーワード　Drive-by download 攻撃，USBワーム，webセキュリティ

１．問題設定

１．１　ゼロ年代におけるコンピュータへの攻撃

2000年代前半，web経由での攻撃と言えば，そのほとんどがWindowsOSの脆弱性を狙うタイプ（e.g. Code Red，Blaster，Slammer，Sasser）か，悪意ある実行ファイルを電子メールに添付するタイプ（e.g. Klez，Nimda，Melissa）であった．

これらの攻撃に対して，当時のOS製造元やユーザはそれなりの対処を迫られた．Microsoft社は，2004年９月２日に公開されたWindows XPのアップデート「Service Pack2」で，1）ファイアウオール機能の追加，2）ワームによる感染被害を緩和する機能の実装，3）Windows Updateの更新通知の自動化を行った．企業ユーザや一般ユーザも慎重になり，添付ファイルを遮断する，見慣れない実行形式ファイルをクリックしない，などの防衛策をとるようになった．

この防衛策によって，コンピュータに対する攻撃は一時収束する方向に向かったが，2000年代後半に見いだされた２つの新戦術によって，再び多くのコンピュータが攻撃の脅威にさ

らされるようになった．１つめの戦術は，サードパーティ製アプリケーションの脆弱性を狙ったDrive-by download攻撃である．もう１つは，WindowsOSのAutorun機能を悪用し，USB接続した記憶媒体（フラッシュメモリ，ハードディスクなど）を利用し，物理的な接続によりマルウェアを感染させようとする戦術，いわゆるUSBワームである．

2009年３月ごろから問題になりはじめたGumblar攻撃は，Drive-by download攻撃の典型例である．この攻撃は，分類的に言えば，Adobe Flash Player，Adobe Acrobat，Adobe Reader，Java（JRE），Microsoft Windows，Microsoft Officeなどに含まれていた脆弱性を狙ったゼロデイ攻撃である．攻撃者は，特定のWebページを改ざん（あるいはそれらしい偽Webサイトを作成）し，そこにiframe領域を作成するJavaScript（Troj/JSRedir-R，JS_GUMBLARなどと呼称されるもの）を設置する．このWebサイトを，脆弱性を抱えたソフトウェアをインストールしているコンピュータで閲覧すると，閲覧側のコンピュータは，密かに攻撃サイトにリダイレクトされ，閲覧者が気づかないうちに，不正なマルウェアをダウンロードさせられる．

2009年３月時点では，ほとんどのセキュリティソフトはGumblar攻撃に対して無警戒であり（現在は対応済み），世界中に大きな混乱をもたらした．日本国内では，まず同人サイトや企業サイトなどに改ざん被害が広がり，いくつかの大手通販サイトや官公庁のサイトが一時閉鎖したり，警視庁ハイテク犯罪対策総合センターが捜査に乗り出すほどの騒動を引き起こした．ただし，ここで問題になったGumblar攻撃は，各方面の速やかな連携により，攻撃者が誘導をもくろんだマルウエア配信サイトのドメイン（gumblar.cn，martuz.cn）への接続が直ちにブロックされた上に，セキュリティソフトの対応が早かったため，一般ユーザーへの実害は比較的少なかったとされる．ただし，この攻撃によってWebサイトを改ざんされた事業所や官公庁，この攻撃を許してしまったセキュリティソフトベンダー，一時閉鎖した通販サイトには，相当の経済的・印象的ダメージを与えるに至った（河原 2010）．

2007年春頃に出現したとされるUSBワームは，USBフラッシュメモリの急速な普及によって蔓延した．このワームのストラテジーは，USB接続された記憶媒体内のファイルを自動実行する，WindowsOSの設定ファイルAutorun.infの悪用である．感染した記憶媒体をコンピュータにUSB接続すると，自動実行機能に基づいて，記憶媒体内の悪意ある実行ファイル（kava.exe，revo.exeなど）を接続先のコンピュータの内蔵ハードディスクにコピーする．別のクリーンな記憶媒体をこのコンピュータにUSB接続すると，今度は，これら悪意あるファイルが内蔵ハードディスクから接続された記憶媒体に自動複製されていく．

このワームのストラテジーが優れていた点は，「無知なユーザーの無警戒な行為に便乗して手動で感染を広げていく」という，ある意味ではアウト・オブ・デイトで，非効率なやり方を取った点だと言えよう．アナクロに見えたこのストラテジーであったが，インターネットカフェや大学の情報処理室など，不特定多数が使用できるコンピュータが各所に設置され，USBフラッシュメモリの爆発的な普及が始まったゼロ年代末に，この手法は思わぬ効果を発揮した．しかも，発生当初は，ほとんどの

セキュリティソフトが未対応だったために，このワームは，さまざまな変種を生み出しつつ，猛烈なスピードで拡散していった．しかし，少なくともこの当時広まったUSBワームのほとんどは，特定のオンラインゲームのアカウントハックを目的とするものであり，標的とされたゲームをプレイしていないPCユーザーの被害は比較的軽微であった．ただし，これらの不正プログラムは常駐型であり，その亜種の中には，コンピュータの処理速度を低下させたり，ユーザがwebに接続できなくなるなどの被害をもたらすものが存在することも報告されている．これら亜種の被害が随時報告されるとともに，セキュリティ対策ソフト・ベンダーによる発見・駆除プログラムの配布，ワーム感染防止機能を備えたUSBフラッシュメモリの発売，Microsoftが対策アップデートを配布したこと（2011年２月）などの対処によって，USBワームはかなりの程度まで封じこまれた[1)]．

かくして，本稿を執筆している2012年夏においては，Gumblar攻撃や，revo.exe，kano.exeなど，従来型のDrive-by download攻撃／Autorun機能を悪用したUSBワームという２つの攻撃は一時終息している．しかしながら，現状は小康状態に過ぎず，この手口を応用した新しい攻撃やワームの拡散が蔓延する可能性は捨てきれない．事実，JPCERTコーディネーションセンター（JPCERT/CC）は，2012年６月29日，Java SE JDKおよびJREの既知の脆弱性を狙ったDrive-by download攻撃を確認したと発表して注意を促すとともに，全国民に対してJava SE JDKおよびJavaのアップデートを促している．2012年６月27日，大手セキュリティソフトベンダーSymantecは，攻撃用webサイトのドメイン名を自動生成する手法を組み込んだ新世代型Drive-by download攻撃の存在を指摘するとともに，将来的にこの新世代型Drive-by download攻撃が蔓延する可能性を指摘した[2)]．USBワームに関しても，2010年６月に発見されたW32/Stuxnetのように，Autrun.inf以外の脆弱性を衝いて感染し，現実的な被害を与えかねないワームが，既に出現している．Stuxnetは，核燃料施設や原子力発電所など，スタンドアローンの産業用制御システムへのサイバー攻撃を狙ったものとされるが，その技術を応用したUSBワーム，個人ユーザや中小の事業所，大学等を標的としたワームが作成される可能性は十分に考えられる（小熊 2011）．Drive-by download攻撃やUSBワームといった手口は――さらにはKlezやNimdaのような，悪意あるプログラムをメールの添付ファイルとして送信する古典的な手口ですらも――決して過去の話ではない．これらに攻撃の亜種については，今後も留意を払っていく必要がある．

１．２　本稿の問題意識と調査概要

著者自身，2009年秋，指導する学生が持ち込んだUSBフラッシュメモリによって，２度，USBワームへの感染を受けた（外部への拡散はなし）．感染それ自体にはすぐに気づいたものの，当時はセキュリティ対策ソフト等が未対応であった時期であったため，手動駆除に多大な手間と時間を費やした．また，2009年度より，著者が福岡県立大学附属研究所／人間社会学部公共社会学科にて担当している「PCスキル養成講座」を受講した学生へのインタビューからも，ほとんどの学生にとって，自分が使用しているコンピュータやwebがブラックボックスとなっていること，webからの脅威に関する知識や実感が著しく欠落していることを感

じていた.

しかし，単位外の講義（正確には学生支援プログラムの一環）である「PCスキル養成講座」の受講者は，例年10名未満にとどまっている．同講座の受講生に対するインタビュー調査で得られたデータは，あくまでも個別の事例研究として扱われるべきものだろう[3)]．web経由での攻撃に対して，現代の大学生はどの程度までセキュリティを実践しているのだろうか．個人情報保護の機運が高まる一方で，公的機関へのハッキングやwebサイトの改ざん事件が相次ぐ今日，大学全体の情報セキュリティを守り，学生のコンピュータリテラシーを向上させる教育プログラムを考えるためにも，大学生がどの程度コンピュータ・セキュリティ（特にwebからの脅威）に対する知識を持ち，それへの対策を実践しているか，その全体的な傾向を量的調査によって把握する必要が認められた[4)]．

コンピュータ・セキュリティの知識／実践に関する大規模な調査としては，（竹村 et.al.2009），（NIRセキュアテクノロジーズ 2008），（情報処理推進機構 2011）などがある．しかし，竹村らの研究は民間企業に勤務している労働者600名を対象に，労働形態（正規雇用／非正規雇用）や，所属している組織属性（上場企業／非上場企業）といった属性変数と，労働者自身の知識や実践との連関を見ていくものであり，母集団にいささかのかたよりがある．

NIRセキュアテクノロジーズや情報処理推進機構が実施した調査は，一定年齢以上の日本国民全体を対象に2000～5000名といった膨大な回答を集めたものだが，調査手法として「webアンケート」を用いていることに問題がある．これらの調査で示された回答分布が，現実の日本国民の意識や実践の傾向をダイレクトに反映しているとは言い難い．特にwebやコンピュータに関わるテーマを対象とする場合，webアンケートで得られたデータをもとに統計的な推論をおこない，議論を展開することは論理的に妥当ではない（吉村・大隅 2004）．いささかの強引さが含まれることを留意しつつ，思いっきり敷衍するならば，コンピュータ・セキュリティに関するwebアンケートが掲載されているwebサイトに行き当たり，さらにそれに回答しようという者は，普段からセキュリティに関心を寄せている者に限られてしまう．この分野における大学生の平均的な知識や実践度を知るためには，いくつかの大学を抽出して，悉皆調査に近い形で調査を実施する方が，より実態を反映したデータを得られるはずである．

幸い，2011年度，著者は大学生を対象とする大規模な調査を実施する機会に恵まれたため，その調査に１日のweb利用時間やコンピュータ・セキュリティの実践度を問う設問を組み込んだ．本稿は同調査の結果をもとに，大学生がどの程度コンピュータ・セキュリティを実践しているか，大学は学生のコンピュータ・セキュリティ教育をどう実施すべきかを論じたものである．

調査対象は，福岡県内の公立大学１校，国立大学２校に通う学部学生である（留学生，聴講生，研究生は除外）．2011年10月，講義時間，昼食時間などを使って，学生に自記式の調査票を配布・回収した．調査票の配布前には，調査の趣旨と回答者のプライバシーについて包括的に説明するとともに，１）回答はあくまで対象者の自由意志によるものであり，答えたくない質問は無視してかまわないこと，２）データベース化に際しては匿名化を心がけ，研究終了後は

調査票を速やかに破棄すること，3)大学や学部の名前は一切出さないこと，4)集計・分析の結果は，学術的な目的でのみ利用すること，5)その他，社会調査倫理規程を遵守して調査・分析を進めること，など，自発的な協力と個人情報の保護について具体的な説明を加えた．同意を得られた者に調査票を配布し，有効票591票を確保した．その後，福岡県立大学附属研究所生涯福祉研究センター棟（当時）内のコンピュータを用いて，これらの票を電子データ化し，IBM社の統計ソフトSPSSで分析を実施した．なお，回収された調査票は2012年3月に全て断裁処分した．

性別・専攻による回答者の分布は以下の通り．性別で比較すると，男性164（27.7%），女性420（71.1%），回答拒否7（1.2%），専攻で比較すると，文系453（76.6%），理系135（22.8%），回答拒否3（0.5%）であった．学年は特に質問していない．

2．分析

2．1　大学生のweb利用・コンピュータ習熟度

「自宅に自分専用のパソコンを持っている」かという質問に対して，「持っている」と回答した者は500名（85.9%），「持っていない」が82名（13.9%），回答拒否／無回答は9名（1.5%）であった．回答拒否／無回答者を除き，性別，通っている大学の種別，専攻（理系／文系）とパソコン所持率との連関を調べたが，いずれも有意な差は見いだされなかった．現代の大学生にとって，自宅に自分専用のパソコンを持っていることは，既に日常的な光景となっているようだ．

1日当たりのweb利用時間について質問した結果を表1に示す．全体の約半分は2時間未満の利用にとどまっているが，4時間以上との回答が全体の1割を超えていることにも留意されたい．性別，通っている大学の種別，専攻（理系／文系）とパソコン所持率との連関を調べた

表1：1日のインターネット利用時間（単純集計）

	1時間未満	1時間～2時間未満	2時間～3時間未満	3時間～4時間未満	4時間以上	無回答	合　計
度数	141	174	145	64	66	1	591
%	23.9%	29.4%	24.5%	10.8%	11.2%	0.2%	100.0%

表2：性別×1日のインターネット利用時間

	1時間未満	1時間～2時間未満	2時間～3時間未満	3時間～4時間未満	4時間以上	合　計
男性（n＝164）	22.0%	24.4%	23.8%	13.4%	16.5%	100.0%
女性（n＝419）	24.8%	32.0%	24.1%	10.0%	9.1%	100.0%
全体（n＝583）	24.0%	29.8%	24.0%	11.0%	11.1%	100.0%

χ^2＝9.70（df＝4），p＝.046

ところ，性別でのみ有意差が現れた．１日に４時間以上webを閲覧している者は男子学生で多かった（表２）．なお，以下に掲載する表のうち，単純集計以外の分析では，利用した設問のうち１つ以上に「無回答／回答拒否」だった者は集計から外している．また表中の小数点は第２位～第４位で四捨五入したため，掲載された表の合計値が100.0％にならない場合が複数存在することを申し添えておく．

ついで，大学生たちが自分のコンピュータスキルをどのように見積もっているかを自己評価させた．選択肢として用意したのは，１.「自分で組み立てたり，トラブルを解決できるレベル」，２.「ソフトをインストールしたり，PCの設定を変えられるレベル」，３.「メールやネットを使ったり，文書やグラフを書けるレベル」，４.「簡単な操作しかわからないレベル」の４つである．１は，いわゆる「マニア」「コンピュータにかなり詳しい人」などと呼称されるレベルであり，以下２～４の順で「やや上級者」「中級者」「初級者」と考えて良いだろう．もう少し具体的な質問――キーボードのショートカットキーの知識，各種ソフトのインストール／アンインストール経験，OSの発売時期に関する知識，メモリやハードディスクを増設した経験，動画ファイルのダウンロード／エンコード形式の変換についての知識――などを投げかければ，より客観的なインデクスを作成することができたと思われるが，調査票に割り当てられたスペースの関係，専門用語を使うことで回答者の混乱を招くおそれなどを勘案した結果，今回は自己の主観的認識をもとにしたインデクスを使用することにした．

表３はインデクスの単純集計結果である．今回の調査には理系の学生135名（工学系：44名・医療系：91名）も含まれていたが，全体の８割近い学生が，３.「メールやネットを使ったり，文書やグラフを書けるレベル」，４.「簡単な操作しかわからないレベル」にとどまっていた．このような回答分布となった背景には，Windows95を搭載したPC-AT互換機の発売以来，ハードウェアの部分，ソフトウェアの部分の両方でコンピュータが急速にブラックボックス化していったことがあるだろう．１）大量生産・規格の同一化によるハードウェアやソフトウェアの価格下落（＝ユーザーの側からすると，プリインストールソフトの充実），２）BTOパソコンメーカーやホワイトボックス・パソコンメーカーの台頭によるコンピュータの価格破壊と，PC自作ブームの衰退，３）OSインターフェースのGUI化と，Plug and Play機能の充実，４）OSやアプリケーションソフトの高機能化／ソースコードの複雑化などが進む中で，今日，家電量販店等で市販されているコンピュータの場合，不用意なカスタマイズは――それが，プリインストールソフトの削除や，ソフトウェアやデバイスドライバの新ヴァージョンを上書きインストールするといった類のことであっても――不具合をもたらしかねない状態になっている．しかも，多くの学生は，ユーザーが筐体を開けることを想定していないノートブック型コンピュータや一体型コンピュータを，自宅のメインコンピュータとして利用している．

ほとんどの大学生は，文系であろうと理系であろうと，ハードウェアの構成やソフトウェアの動作原理，あるいはその脆弱性について無知である．「使い方を知っているだけ」のブラックボックスを用いて，レポートを書いたり，webを閲覧して趣味の情報を集めたり，オン

表３：コンピュータ習熟度（単純集計）

	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，PCの設定を変えられるレベル	メールやネットを使ったり，文書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	無回答	合　計
度数	12	132	333	109	5	591
%	2.0%	22.3%	56.3%	18.4%	0.8%	100.0%

表４：専攻・性別×コンピュータ習熟度

	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，PCの設定を変えられるレベル	メールやネットを使ったり，文書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	合　計
文系（n＝450）	1.6%	24.4%	57.8%	16.2%	100.0%
理系（n＝134）	3.7%	15.7%	53.7%	26.9%	100.0%
全体（n＝584）	2.1%	22.4%	56.8%	18.7%	100.0%

χ^2＝12.49（df＝３），p＝.006

	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，PCの設定を変えられるレベル	メールやネットを使ったり，文書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	合　計
男性（n＝162）	3.7%	27.8%	48.8%	19.8%	100.0%
女性（n＝417）	1.4%	20.6%	60.0%	18.0%	100.0%
全体（n＝579）	2.1%	22.6%	56.8%	18.5%	100.0%

χ^2＝8.29（df＝３），p＝.040

ラインゲームを行ったり，音楽を聴いたりしている．専攻，性別でこの傾向を比較した結果が表４である．

専攻別の比較結果では，文系の方がコンピュータ習熟度が高くなるという意外な結果が出たが，前節の末尾で示したように，今回の調査回答者では男女のかたよりが大きかったことに由来するものだろう．

コンピュータ習熟度とweb利用時間との間には有意な連関が見られた（表５）．web閲覧時間の長い学生の方で，コンピュータ習熟度が高い．ただし，１日に３～４時間webを閲覧している学生の65.6%，４時間以上webを閲覧している学生の56.1%以上が，トラブルの解決のみならず，ソフトのインストールやPCの設定変更に関してすら自信を持っていないという結果は，webからの脅威の面からみて，いささか憂慮すべき状況だと思われる．ソフトウェアのインストールに不安を持つ学生は，Drive-by download攻撃の標的となる各種ソフトのアップデートを実行しているのだろうか．iframe領域の作成を不可能にする有効な手段であるJavaScriptの停止，リムーバルメディアからのウイルス感染を防ぐAutorun機能の

表５：１日のweb利用時間×コンピュータ習熟度

	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，PCの設定を変えられるレベル	メールやネットを使ったり，文書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	合　計
１時間未満　（ｎ＝138）	1.4%	10.1%	54.3%	34.1%	100.0%
１時間～２時間未満（ｎ＝173）	2.3%	17.3%	60.1%	20.2%	100.0%
２時間～３時間未満（ｎ＝144）	2.8%	27.1%	58.3%	11.8%	100.0%
３時間～４時間未満　（ｎ＝64）	0.0%	34.4%	59.4%	6.3%	100.0%
４時間以上　（ｎ＝66）	3.0%	40.9%	48.5%	7.6%	100.0%
合　計　（ｎ＝585）	2.1%	22.6%	56.9%	18.5%	100.0%

$\chi^2=61.67$（df＝12），p＜.001

無効化は，いずれもブラウザやOSの「設定変更」に関する要件である．この結果に多少の不安を感じつつ，次節では，大学生たちが実際に行っているセキュリティ対策の実践状況を見ていきたい．

２．２　大学生のセキュリティ対策

今回の調査では，対象者がコンピュータのセキュリティ対策をどの程度まで実践しているかについて，ａ．セキュリティソフトの導入，ｂ．セキュリティソフトの定期的なアップデート，ｃ．OSの定期的なアップデート，ｄ．Adobe Readerの定期的なアップデート，ｅ．Flash Playerのアップデート，ｆ．定期的なウイルススキャン，ｇ．ブロードバンドルータの導入，ｈ．迷惑メールフィルタリングソフトの導入という８項目で測定した．

調査項目に「Adobe Readerの定期的なアップデート」，「Flash Playerの定期的なアップデート」を項目に入れたのは，１）Gumblar攻撃がそうであったように，この２つのソフトが抱える脆弱性がDrive-by download攻撃の標的となりやすいこと，２）調査対象者が大学生である以上，web上にPDFファイルの形式でアップロードされているファイル（論文や白書類）を閲覧する機会が高い，３）今回，調査対象となった大学生の多くは，webの動画サイトをかなりの頻度で閲覧している，の３点に基づいている[5)]．その他５項目は，従来型の攻撃への対処の程度を図るために設定した．ここも，本来ならば，ブラウザのセキュリティ設定や自動実行の阻止，Javaのアップデート，データ実行防止機能（DEP）の設定などについての質問も付け加えるべきであったが，調査前におこなったインフォーマルな聞き取り調査で，これらの項目に関する学生の理解度それ自身が著しく低いことが判明したために，今回の調査項目からは除外した．

自宅に自分専用のPCを持っていない者（82名），および各設問に対する回答拒否者（設問によって多少異なるが，10名未満）を除いた上で，学生の回答を「やっている」（実践群）と，「やっていない」「わからない」（非実践／不明群）の２群に分割して集計し表６を得た．この結果もまた憂慮すべきものである．セキュリティソフトを導入していると明示的に回答できた

表６：コンピュータセキュリティ実践度

	実践群	非実践／不明群		合計
	やっている	やっていない	わからない	
a：セキュリティソフトのインストール　（n＝502）	72.9%	10.2%	16.9%	100.0%
b：セキュリティソフトの定期的アップデート（n＝501）	54.7%	20.8%	24.6%	100.0%
c：OSの定期的なアップデート　（n＝502）	48.8%	18.7%	32.5%	100.0%
d：Adobe Readerのアップデート　（n＝499）	39.3%	15.4%	45.3%	100.0%
e：Flash Playerのアップデート　（n＝498）	38.2%	15.1%	46.8%	100.0%
f：定期的なウイルススキャン　（n＝498）	45.2%	18.9%	35.9%	100.0%
g：ブロードバンドルータの導入　（n＝496）	20.2%	20.0%	59.9%	100.0%
h：迷惑メールへの対策　（n＝498）	34.1%	25.7%	40.2%	100.0%

学生は全体の72.9％であった[6)]．セキュリティソフトの定期的なアップデートをしている学生は54.7％にとどまっている[7)]．OSのアップデートを実践している学生，Adobe Reader，Flash Playerのアップデートを実践している学生，定期的なウイルススキャンを実施している学生は全て半数を割り込んでいる．また，迷惑メールのフィルタリングソフト導入率は34.1％に過ぎなかった．ここが不徹底な者は，KlezやNimdaの亜流，さらには，偽のwebサイトに誘導し，IDやパスワード，クレジットカード番号を盗み出そうとする詐欺メールに対して，あまりに無防備だと言わざるを得ない．なお，専攻や性別といった属性変数と個別のセキュリティ項目の実践度との通連関を順次調べていったが，特に有意な傾向は見いだされなかった．

回答者ひとりひとりのセキュリティ実践度を調べるため，表６に示した８項目のそれぞれに，「やっている」と答えた場合は１点，「やっていない」「わからない」と答えた場合は０点を与えた上で，回答者ごとに８項目の合計得点を算出し，セキュリティ対策実践度得点とした．最高点は８点，最低点は０点となる．有効回答は490票，有効回答全体の平均点は3.516，標準偏差は2.659であった．８点満点であるセキュリティ実践度得点の平均点が４点を下回っている現状，標準偏差が2.5を超えている現状は，それだけで問題である．

表３で示したコンピュータ習熟度と，セキュリティ対策実践度得点との連関を，一元配置分散分析で調べ次の表７を得た．コンピュータ習熟度が高い学生と，習熟度が低い学生でセキュリティ実践度に著しい格差が生じ，きれいに２分されていた（分散分析結果 $F(3,483)=49.41$，$p<.001$，下位検定はTurkeyを使用）．

ついで，１日のweb利用時間とセキュリティ対策の実践度との連関を調べ，表８が得られた．１日のweb利用時間が長い学生は，そうでない学生よりもセキュリティ対策に留意を払っていた（分散分析結果 $F(4,485)=5.072$，$p<.001$）．しかしながら，これは全体的な傾向であり，対象者をweb利用時間でグルーピングした上で，セキュリティ対策実践度得点の分布を調べていったところ，１日のweb閲覧時間が「３時間～４時間未満」の者（有効回答55名）の29.1%，「４時間以上」の者（有効回答58名）の24.1%が，この得点が２点以下であった．

この中には，積極的なセキュリティ対策を何ひとつしないまま（＝セキュリティ対策実践度得点が０点であるにもかかわらず），１日３時間以上webサイトを閲覧している12名の学生が含まれる．セキュリティに関する知識や積極的な対策実践を行わないまま，長時間webに接続すると，侵入を狙う第三者からのポートスキャンを受ける確率や，ネットサーフィンの途中でDrive-by download攻撃を仕掛けてくる，悪意あるwebサイトの被害者となる可能性を

表７：コンピュータ習熟度とセキュリティの実践

平均値比較	度数	平均値	標準偏差
自分で組み立てたり，トラブルを解決できるレベル	10	5.600	3.204
ソフトをインストールしたり，PCの設定を変えられるレベル	113	5.566	2.091
メールやネットを使ったり，文書やグラフを書けるレベル	280	3.093	2.442
簡単な操作しかわからないレベル	84	1.857	2.083
全体	487	3.505	2.647

等質サブグループの分類	度数	α＝0.05のサブグループ	
		1	2
自分で組み立てたり，トラブルを解決できるレベル	84	1.857	
ソフトをインストールしたり，PCの設定を変えられるレベル	280	3.093	
メールやネットを使ったり，文書やグラフを書けるレベル	113		5.566
簡単な操作しかわからないレベル	10		5.600
有意確率		0.144	1.000

表８：web閲覧時間とセキュリティの実践

平均値比較	度数	平均値	標準偏差
１時間未満	106	2.925	2.738
１時間～２時間未満	144	3.132	2.634
２時間～３時間未満	127	3.787	2.581
３時間～４時間未満	55	3.964	2.252
４時間以上	58	4.534	2.735
合計	490	3.516	2.659

等質サブグループの分類	度数	α＝0.05のサブグループ	
		1	2
１時間未満	106	2.9245	
１時間～２時間未満	144	3.1319	
２時間～３時間未満	127	3.7874	3.787
３時間～４時間未満	55	3.9636	3.964
４時間以上	58		4.534
有意確率		0.077	0.347

高める行為であることは言うまでもない[8)].

3．小括と今後の課題

3．1　小括

webセキュリティに関する大学生の知識や実践は，明らかに不十分である．Drive-by download攻撃の被害を受けたり，USBワームの侵入を受けたとしても，セキュリティソフトを導入した上で，それを定期的にアップデートし，ウイルススキャンを行う習慣を付けている場合は，その被害を最小限に抑えられる，大学としては，その所属する学生に，最低限でもこれだけは実践する習慣を付けさせるべきだろう．ただし，少なくとも表6を見る限り，2011年の段階で，このような実践を行っている学生は，全体の半数にも満たなかった．また，OS（ほとんどの大学生がイメージするのは，Microsoft Windowsであろう）やAdobe製品の脆弱性や，そこを狙ったゼロデイ攻撃への認識度は，著者の予想を遥かに超えて低かった．

コンピュータに関する知識を持っている学生，webへの接続時間が長い学生――おそらく，閲覧したwebサイトから，セキュリティや攻撃についての知識を得ているのだろう――では，多少はセキュリティの実践度が上がっていた．しかし，そのような学生は，全体の一部にとどまっている．また，そのような学生のセキュリティ実践度も，全体的に見るといまだ不十分である．特に，webからの脅威に無関心なまま長時間webを閲覧している学生が一定数存在することは，極めて危険な状況だと言わざるを得ない（表7，表8）．

なぜなら，2012年現在，多くの大学には，学生が持ち込んだノート型コンピュータを学内のLANネットワークに接続できる環境が整えられているし，学生が，個人で所持するUSBフラッシュメモリや外付けHDDを接続できるコンピュータが多数配置されているからだ．ワームに感染したコンピュータやUSBフラッシュメモリが，これらのコンピュータネットワーク――大学の教職員が研究や業務で使用しているコンピュータもそこに接続されている――に接続される可能性は日々高まっている．そして，大学教職員が研究室や事務室で使用しているコンピュータに保存されている各種の研究データ，個人情報の中には，標的型攻撃の目標となる価値を持ったものも少なくない．

この状況は早急に改善される必要がある．具体的には，学生・さらには教職員に対して，webからの脅威や，それへの対策方法に関する知識の教授を必修化する必要があるだろう．情報セキュリティ政策や情報通信技術に関する教育の必要性は，政府（内閣）もしばしば言及している．2006年1月の「IT新改革戦略」，2006年2月の「第1次情報セキュリティ基本計画」，2009年2月の「第2次情報セキュリティ基本計画」などがその典型例である．特に「第2次情報セキュリティ基本計画」においては，「リスクの認識や情報セキュリティ対策の重要性の認識が必ずしも十分でない児童・生徒や保護者」の存在を踏まえた上での「学校や地域における情報モラル等の教育を推進する」ことが謳われている．ここでは「モラル」という単語が使われているが，この単語には「情報社会で適正な活動を行うための基になる考え方と態度」という註記が付され，この文章自体も「情報セキュリティの強化・推進」という項目に含まれていることに注意されたい．「webの匿名性を楯にした誹謗中傷や流言の拡散を自戒する／させる

姿勢」に加えて，「情報漏洩を防止する目的で行われるセキュリティ対策を実践するインセンティブ」という意味を，政府はこの単語に含意させていると考えるべきだろう（内閣府 2009：57)[9)]．

21世紀のわが国に生きる以上，好むと好まざるとに関わらず，われわれは公的領域，私的領域ともにwebに接続し，情報のやりとりに参加していかなければならない状況に陥っている．濱野智史が指摘したように，ゼロ年代において，各種のwebサービスは，閉ざされた一部集団が担保する下位文化の枠を超え，あらゆる人びとの行動を制御しるアーキテクチャ，複数の人びとの相互行為のあり方を規定する「場」として稼働しはじめている（濱野 2008：14)．そうである以上，サイバースペースにおけるマナーの１つとしてwebセキュリティに関する知識や実践を学生に修得させることは，教育機関としての大学にとって必要なことだろう．既に述べたように，このような修得カリキュラムを設置することは，大学それ自体が抱える研究データや個人情報の流出を防ぎ，大学の信用度やコンプライアンスを守る機能も持っている．

３．２　今後の課題

第１節で述べたように，本稿のもとになった調査は，脱稿のほぼ１年前である2011年秋に実施された．その後，今日に至るまでの１年で，スマートフォンやタブレットPCといった新しいweb端末が，著者の予想を超えるスピードで大学生に普及したこと，およびFacebookの利用者が急速に増えたことについて，最後に注意を喚起したい．現在，著者は同じテーマでの研究の継続を見越して，非公式な形で学生に聞き取りを行っている．その中で，１）スマートフォンやタブレットPCを用いてのweb閲覧や情報通信を行う場合のセキュリティ意識，２）AndroidOS，iOS，BlackberryOSなど，スマートフォンやタブレットPCに搭載されているOSのアップデートの必要性に関する認識や実践度，３）スマートフォンを標的とするマルウェアに関する認識，４）スマートフォンのジオタグ機能に関する認識，５）Facebook，twitter，LINE，Skypeといったwebサービスを利用することのデメリット，といった事案に関する大学生の認識やセキュリティ実践度の低さを，著者は痛感している．

情報処理推進機構が告知しているように，スマートフォンやタブレットPCは，小型のコンピュータであり，デスクトップ型コンピュータやノートブック型コンピュータと同様，あるいは――盗難被害を受けやすいため――それ以上のセキュリティ対策を実践する必要があるデバイスである（情報処理推進機構 2012b)．実名主義を掲げるFacebookはユーザーの名前，生年月日，住所，電話番号，メールアドレス，投稿内容，webサイトの閲覧履歴，タイムライン機能を使っての位置情報取得などによって，ユーザーのプロファイリングを着々と行っているともいわれている（守屋 2012)．個人情報保護が叫ばれる今日，大学生たちはどこまでこれらの実態を知り，どの程度まで，自己を防衛できているのだろうか．今後，スマートフォンやタブレットPCを通して，大学や事業所のコンピュータネットへの侵入を試みるインシデント，Facebookなどへの不用意な投稿がもたらすコンプライアンス問題がくり返される可能性は否定できない．今回の問題と合わせて（あるいはそれ以上に)，これらに対する学生教育の

あり方を検討していく必要がある．

［註］

1）USBワームの動作原理や被害状況については，（ITpro 2008; Yoshikawa 2008）を参照のこと．2011年6月29日，Microsoftは，「悪意のあるソフトウェアの削除ツール」で2011年5月に削除された「Autorunを悪用するマルウェアの数」が，XP Service Pack（SP）3で62%，Vista SP1で64%，Vista SP2で82%減少したと発表した（國谷 2011）．

2）従来のDrive-by download攻撃の実効性は短期間にとどまっていた．セキュリティ研究者，ホスティング・プロバイダー，ドメイン・レジストラなどが協力し，攻撃用Webサイトの閉鎖や，攻撃に用いられている危険なドメイン名の停止といった対抗措置を行うと，攻撃サイトへの接続が不可能になるからである．新世代型Drive-by download攻撃は，毎回ドメイン名を自動生成することで，この対抗措置を回避をもくろんでいる（佐藤 2012）．

3）著者が2009年度～2011年度の「PCスキル養成講座」受講生にインタビューしたところ，この講義を受ける学生は，むしろコンピュータの操作やweb閲覧について，ある程度の知識を持っており，そうであるが故に，webセキュリティやコンピュータの選び方に不安を感じている者が多いように感じた．

4）石崎龍二は，（学部1年生）福岡県立大学の学生を対象に，主要アプリケーション・ソフトの操作能力やwebを利用した情報収集能力についてのデータを収集している（石崎 2011）．しかし，石崎はセキュリティ実践の変化については調べていない．

5）本稿では積極的に言及しなかったが，今回の調査では，webの利用方法についても質問している．その中で，1日のweb利用時間と有意な連関があったものは「見のがしたアニメやPVを視聴する」「ネットゲームをする」「楽天やamazonで買い物をする」の3項目であった．これらに肯定的な回答を示す大学生は，1日のweb利用時間が長くなる．特にネットゲームをやる者では，web利用時間が顕著に長くなる．Kurbeyらが指摘した学生――依存的なまでにwebにのめり込むことで，本来の学業生活に支障をきたしている学生――が，今回調査対象となった大学にも一定数存在することを示唆する結果だと言えよう（Kurbey et.al.,2001）．

6）今日，家電量販店などで売られているメーカー製コンピュータのほとんどには，30日間無料などを謳うセキュリティソフトの体験版がプリインストールされている．今回「セキュリティソフトのインストール」を「やっていない」「わからない」と答えた大学生が使用しているコンピュータのほとんどは，この手の体験版ソフトウェアによって，限定的には保護されているはずである．ただし，ここで「やっていない」「わからない」と回答した学生が使用しているコンピュータのセキュリティソフトは，既に試用期間が切れており，ウイルス定義ファイルやファイアウオールが更新されないままに放置されている可能性が高い．

7）多くのセキュリティソフト，さらにはAdobe Reader，Flash Playerは，自らを自動的にアップデートする機能（自動更新機能）を備えている．また，セキュリティソフトはバックグラウンドで定期的なウイルススキャンを行っている．ここで問題とすべきは，40～60%の学生が，おそらくこのことそれ自体を認識していない点である．

8）2012年現在，頻出しているDrive-by download攻撃は，「ウイルスに感染している」，「ハードディスク内にエラーが発見された」といった警告画面を表示し，セキュリティ対策ソフトに見せかけたバックドア・プログラムをダウンロードさせようとするものである（情報処理推進機構 2012a）．

9）web上で無責任な中傷合戦や流言の拡散が行われるプロセスについては（荻上 2007）を参照．

［文献］

情報処理推進機構，2011，「2011年度　情報セキュリティの脅威に対する意識調査」独立行政法人情報処理推進機構.
http://www.ipa.go.jp/security/fy23/reports/ishiki/（2012年９月６日閲覧）.

――――，2012a，「コンピュータウイルス・不正アクセスの届け出状況［２月分］について」独立行政法人情報処理推進機構.
http://www.ipa.go.jp/security/txt/2012/03outline.html（2012年９月６日閲覧）.

――――，2012b，「スマートフォンのセキュリティ＜緊急回避＞対策のしおり」独立行政法人情報処理推進機構.
http://www.ipa.go.jp/security/antivirus/documents/08_smartphone.pdf（2012年９月６日閲覧）.

濱野智史，2008，『アーキテクチャの生態系――情報環境はいかに設計されてきたか』NTT出版.

石崎龍二，2011，「福岡県立大学人間社会学部新入生に対するコンピュータリテラシー教育の教育効果」『福岡県立大学人間社会学部紀要』21(1): 42-63.

ITPro，2008，「検証ラボ：ウイルスを観察してみるUSBワーム『WORM_AUTORUN_CC』」
http://itpro.nikkeibp.co.jp/article/COLUMN/20080507/300878/（2012年９月６日閲覧）.

河原潤，2010，「年をまたいで猛威をふるったガンブラー・ウイルス（第２回）」
http://it.impressbm.co.jp/e/2010/01/13/1856（2012年９月６日閲覧）.

Kurbey, Robert. W., Lavin, Michael J. and Barrows, John R., 2001, "Internet Use and Collegiate Academic Performance Decrements: Early Findings," *Jounal of Communication*, 51(2): 366-382

國谷武史，2011，「Autorun型マルウェアの感染が減少，「対策の効果あり」とMicrosoft」
http://www.itmedia.co.jp/enterprise/articles/1106/29/news106.html（2012年９月６日閲覧）.

守屋英一，2012，『フェイスブックが危ない』文藝春秋.

内閣府，2009，『第２次情報セキュリティ基本計画――IT時代の力強い「個」と「社会」の確立に向けて』内閣府情報セキュリティ会議.
http://www.nisc.go.jp/active/kihon/pdf/bpc02_ts.pdf（2012年９月６日閲覧）.

NIRセキュアテクノロジーズ，2008，『情報セキュリティに関するインターネット利用者意識調査2008報告書』NIRセキュアテクノロジーズ株式会社.
http://www.nri-secure.co.jp/news/2008/pdf/20080522_net.pdf（2012年９月６日閲覧）.

荻上チキ，2007，『ウェブ炎上――ネット群衆の暴走と可能性』筑摩書房.

小熊信孝，2011，「Stuxnet――制御システムを狙った初のマルウェア」
http://www.jpcert.or.jp/ics/2011/20110210-oguma.pdf（2012年９月６日閲覧）.

佐藤信正，2012，「無駄に印刷させるウイルス／ドライブバイ・ダウンロード攻撃に新手の手法」
http://pc.nikkeibp.co.jp/article/trend/20120709/1055083/（2012年９月６日閲覧）.

竹村敏彦・嶋滝和典・今川拓郎，2009，「労働者の情報セキュリティ意識に関する研究」『RCCCディスカッションペーパーシリーズ』No.85: 1-19.

Yoshikawa Takashi, 2008,「USBワームが作成する『Autorun.inf』の分析とその傾向」『TrendLabs Security Blog』
http://blog.trendmicro.co.jp/archives/2668（2012年９月６日閲覧）.

吉村宰・大隅昇，2004，『インターネット調査の信頼性と質の確保に向けての体系的研究』文部科学省統計数理研究所.