情報コミュニケーション学会第9回研究会
CIS2012(2012.6.9)

大学入学時における学生の情報セキュリティに関する理解状況について

Students' Understanding of Information Security in Entering University

上繁　義史† Yoshifumi UESHIGE
柳生　大輔† Daisuke YAGYU
鈴木　斉‡ Hitoshi SUZUKI
古賀　掲維† Aoi KOGA
丹羽　量久† Kazuhisa NIWA
藤井　美知子† Michiko FUJII
野﨑　剛一† Koichi NOZAKI

†長崎大学情報メディア基盤センター
Information Media Center, Nagasaki University

‡長崎大学経済学部
Faculty of Economics, Nagasaki University

概要

情報セキュリティ教育を効果的に行うための基礎資料として，平成 24 年度入学者を対象として，入学時点での情報セキュリティに関する理解や知識に関するアンケートを実施した。アンケート回答の回収には e ラーニングシステムを利用し，全体で 1588 名（全対象者の 94.4%）の回答を得た。その集計の結果，パソコンへのウイルス対策ソフト利用やアカウントの管理について，一定の理解がされている傾向が明らかになった。その一方スマートフォンやタブレット端末についてウイルス対策の必要性が必ずしも認識されていない傾向が見られた。情報セキュリティに関する語句・用語をどの程度知っているかについては，ウイルス，個人情報，ワンクリック詐欺といったものはよく認知されている一方，専門性の高いものについては必ずしも十分には認知されていない傾向が見られた。

■キーワード■

アンケート，情報セキュリティ，教養教育，情報リテラシー

はじめに

情報セキュリティを組織運営の中で実践していくためには，技術の活用・日々の管理運用・効果的なルール整備の 3 つをバランスよく実施することが重要である。近年大学においても部分的ではあるが，情報セキュリティマネジメントシステム（Information Security Management System; ISMS）を構築し，ISO27001 認証を取得するに至っている。その中では，構成員（教職員や学生など）へのセキュリティ教育を実施して，その効果測定が行われる[1]。

高等学校において 2003 年度から情報科目が必修化され，2009 年の改訂において，情報セキュリティに関する内容が拡充される[2]など，初等中等教育においても，その重要性が認識されるに至っている。2010 年の改訂において高校学習指導要領[3]でも，情報セキュリティに関する記述が増えている。

長崎大学では，教職員・学生の情報セキュリティ向上を目標に掲げている[4]。そのための行動計画として情報セキュリティに関する教育を挙げている。長崎大学では，平成 24 年度より，教養必修科目として情報系科目「情報基礎」を全学部共通の講義内容にて開講しており，著者らが全クラスの講義を担当している。情報セキュリティについて今年度の授業を効果的に実施し，今後の教育内容を検討していくための基礎資料を得ることを目的として，学部 1 年次の全入学者を対象に入学時点での情報セキュリティに関する理解や知識に関するアンケートを実施したので報告する。

アンケートの実施方法

本アンケートは，主に情報基礎の授業時間の中で実施された。平成 24 年 4 月 5 日より 1 年次生への授業が開始され，多くのクラスについては，第 1 回目の講義の終わりに時間（10 分程度）をとって実施した。内容の性質上，情報セキュリティに関する講義よりも前に実施した。

表 1　アンケート回収率

対象学部	全学部（教育学部，経済学部，医学部，歯学部，薬学部，水産学部，工学部，環境科学部）
クラス数	30 クラス
対象者数	1,683 名
回答者数	1,588 名
アンケート回収率	94.4%

アンケート設問の提示及び回答は本学の e ラーニングシステム「WebClass」[5]を用いて行った。設問数は 7 問であった。個々の設問については，後述する。

アンケート結果と考察

以下でそれぞれの設問とその集計結果について述べ，考察を加えていく。

パソコン等の機器の管理について

設問 1　以下の機器について，自分以外の人が扱えないようにしていますか？
※　家族で共有している場合には「はい」か「いいえ」のいずれかで答えて下さい
(1)　パソコン（例：スクリーンセイバーにパスワード保護の設定をしている）
(2)　スマートフォンあるいは携帯電話（例：端末に暗証番号やパスワードを設定している）
(3)　タブレット端末（例：端末に暗証番号やパスワードを設定している）
選択肢：①はい，②いいえ，③持っていない

この設問では，所有する機器の管理状況をたずねている。集計結果は図 1 のような結果となった。図に示すように，パソコンについては 34.7%，スマートフォンや携帯電話については，48.2%の学生がパスワード・暗証番号を設定するなど，何らかの処置を行っていることが分かった。タブレット端末については，「持っていない」との回答が全体の 77.6%を占めたものの，6.5%（保有者の約 1/3）が自分だけが扱えるようにしていることが分かった。

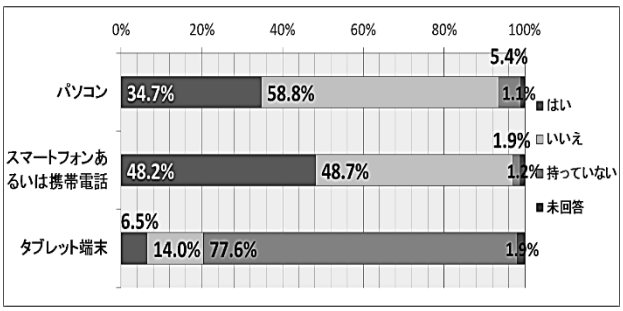


図 1　設問 1 の集計結果

学生が所有する機器が私物である点を考慮すると，①パソコンは学生自身が所有しており，本人以外が触れることがない，②学生は家族共有パソコンの 1 ユーザとして ID・パスワードを与えられている，といった状況が考えられる。

スマートフォンや携帯電話については，機器の紛失・盗難や情報漏洩のリスクを考慮し，記憶された情報の保護を目的に暗証番号等を設定している学生が増えているものと思われる。

タブレット端末については必ずしも利用者が多いわけではなかったが，スマートフォン・携帯電話と同様のリスクを考慮したためと考えられる。

設問 2　以下の機器について，「無くしそうになった」あるいは「無くした」ことがありますか？
(1)　パソコン
(2)　スマートフォンあるいは携帯電話
(3)　タブレット端末
(4)　USB メモリ
選択肢：①はい，②いいえ，③持っていない

この設問は自宅外などに持ち出した機器の取り扱い状況に関する質問である。集計結果は図 2 のようになった。パソコン，タブレット端末については「はい」の回答がそれぞれ 0.7%，1.3%となっている。これは保有するパソコンの大半がデスクトップか，

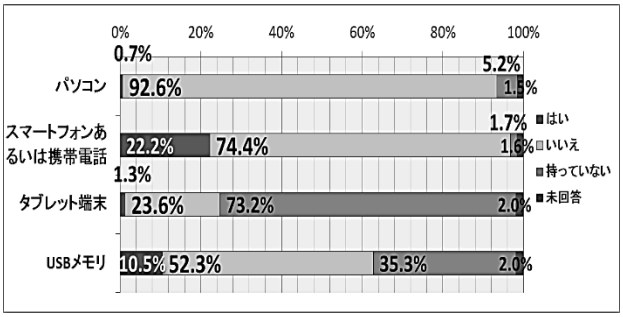


図 2　設問 2 の集計結果

（筐体が大きいなどの理由で）自宅から持ち出さないノートパソコンであるためと思われる。また，タ

ブレット端末は筐体の大きさがノートパソコンよりは小さく可搬性が高いが，携帯電話やスマートフォンより大きく，外出先でバッグ等から出してそのまま放置するといった状況が少ないことが考えられる。

一方，「スマートフォンあるいは携帯電話」，「USB メモリ」について，「はい」との回答がそれぞれ 22.2%，10.5%を占めた。これらの機器は小さく，携行が極めて容易であるため，外出時にポケットやバッグに入れて持ち歩くなどして「無くしそうになった」あるいは「無くした」という経験につながったと思われる。本アンケートの回答時点では， USB メモリを「持っていない」との回答が 35.3%あったが，その利便性や入手の容易さから，この割合は時間をおうごとに減少するものと思われ，その利活用に関するセキュリティについて教育が必要と考えられる。

ウイルス対策の状況

設問 3　以下の機器に，ウイルス対策ソフトをインストールしていますか？
※　家族で共有している場合には「はい」か「いいえ」のいずれかで答えて下さい。
※　買ったときに既に入っていた人は「はい」と答えて下さい。
(1)　パソコン
(2)　スマートフォン
(3)　タブレット端末
選択肢：①はい，②いいえ，③持っていない

この設問はウイルス対策の最初のステップが講じられているかをたずねたものである。集計した結果，図 3 のようになった。パソコンについては 80.7%がインストールしているとの回答であり，パソコンにおける情報セキュリティ維持の基本として定着しつつあるとみられる。理由としては，購入時にプレインストールされた試用版を継続して使っているケースが多くなったためと考えられる。ただし試用期間が終了して放置されているケースを含むものと思われる。

一方，スマートフォンでは「はい」との回答が 28.4%にとどまっており，パソコンと比較してウイルス対策ソフトの普及が進んでいないことがわかった。「はい」の回答の中には，一部のキャリアで行われている，情報セキュリティに関するサービス（ウイルス対策ソフトのインストール・パターン定義ファイルの提

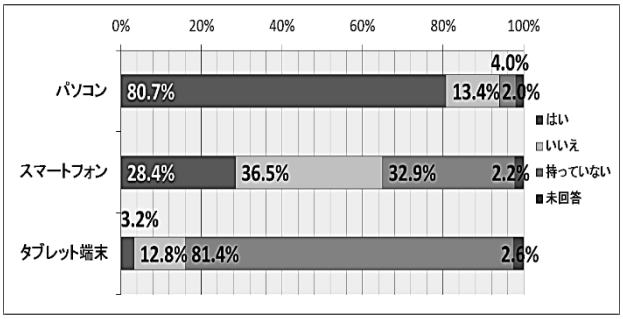


図 3　設問 3 の集計結果

供など）の利用者を含むものと思われる。一方，「いいえ」との回答については，（Android ユーザであっても）スマートフォンにウイルス対策が必要との認識が徹底されていないことが理由として考えられる。

タブレット端末については，「いいえ」の回答が「はい」のそれを上回っているが，その理由はスマートフォンの場合と同様であると考えられる。

設問 4　以下の機器で，ウイルスやワームなどが検出されたことがありますか？
※　家族で共有している場合には「はい」「いいえ」「ウイルス対策ソフトを入れていない」のいずれかで答えて下さい。
※　買ったときにウイルス対策ソフトが既に入っていた人は「はい」か「いいえ」のいずれかで答えて下さい。
（1）パソコン
（2）スマートフォン
（3）タブレット端末
選択肢：①はい，②いいえ，③ウイルス対策ソフトを入れていない，④機器を持っていない

設問 3 と関連して，ウイルス検出の経験をたずねている。その結果，図 4 に示すように，パソコンについては 28.7%が経験ありと回答している。スマートフォン，タブレット端末ではそれぞれ 2.0%，0.5%が経験したと回答している。

パソコンでの検出事例の多くは，Web サービスに関連して保存された Tracking Cookie に起因するものと思われる。また，マルウェアを埋め込まれた Web サイトを閲覧したり，様々なソフトウェアやコンテンツをダウンロードしたりする中でマルウェアに感染したケースが考えられる。

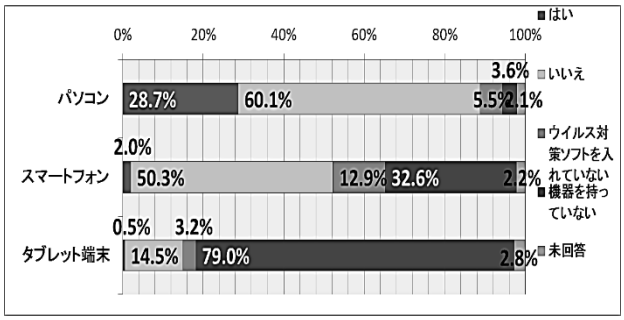


図 4　設問 4 の集計結果

スマートフォン，タブレット端末での検出については，(独) 情報処理推進機構の注意喚起[6]にもあるように，不正なアプリをインストールしたことが原因と考えられる。

アカウント管理に関する理解

設問 5　長大 ID や様々な Web のサービスの ID をもっていると思いますが，ID とパスワードをどのように管理していますか？

選択肢：

① **すぐ見られるところにメモを置いている**
② **手帳に書いている**
③ **パソコンや携帯電話，スマートフォンにメモしている**
④ **ブラウザなどに記憶させている（「パスワードを記憶させますか？」のメッセージに「はい」と押した経験がある人はあてはまります）**
⑤ **頭に記憶している**
⑥ **よくわからない**
⑦ **その他（自由記述）**

この設問では，アカウントの管理状況をたずねている。設問文中の長大 ID は長崎大学入学（教職員の場合には新採用）の時点で発行される ID のことで，本学の統合認証サービスと連携したシステムへのログインに使われている。

本設問の回答状況は図 5 のようになった。60.7%が「頭に記憶している」，17.7%が「手帳に書いている」，11.3%が「パソコンや携帯電話，スマートフォンにメモしている」と回答している。これらの回答については，他者から見られるリスク回避の努力が伺える。

その一方で 4.2%が「すぐ見られるところにメモを置いている」，2.0%が「ブラウザなどに記憶させている」など，他人にアカウントを悪用されるリスクを抱えた回答者が存在することが分かる。1 人しか使わないような，個人所有のパソコンであれば，このリスクは小さいと見ることが出来るが，そうでないパソコン（大学の研究室設置のパソコンなど）においては，格段に高いリスクとなる。そのため，アカウントの管理について，入学時点での十分に理解させる必要があると思われる。

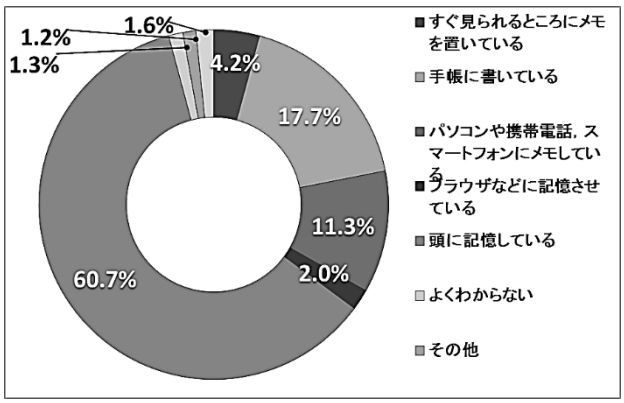


図 5　設問 5 の集計結果

「その他」の回答については，自由記述式で具体的な管理方法をたずねている。多かった回答としては「メモを財布等に入れて持ち歩いている」が挙げられる。「手帳に書いている」と同様に，他者に見えないように管理していることがわかる。また「隠しフォルダに保管する」，「パスワードを書いたファイルを暗号化している」といった回答が見られた。「隠しフォルダに保管する」はセキュリティとしては十分とは言えないまでも，容易に他人の目に触れないための工夫をしている様子が分かる。

設問 6　長大 ID や様々な Web のサービスの ID をもっていると思いますが，自分の ID とパスワードを他人に教えたことがありますか？

選択肢：**①はい，②いいえ，③覚えていない**

これは設問 5 と同様に，アカウントの取り扱いについてたずねたものである。この設問の集計結果は図 6 のようになった。93.5%の学生が「いいえ」と回答しており，「パスワードを他人に教えない」という

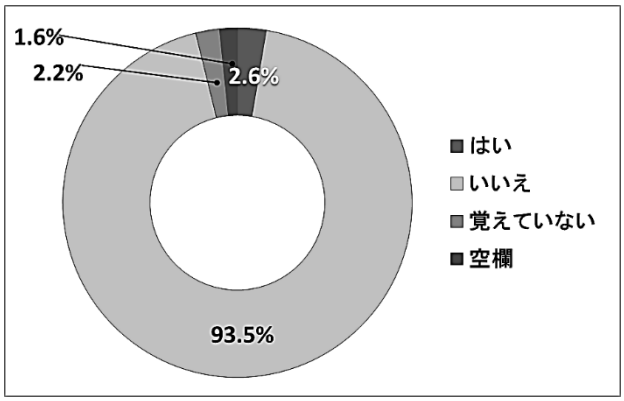


図 6　設問 6 の集計結果

考え方が理解されているものと思われるが，一方で「パスワードを他人に教える必要がなかった」といった消極的な理由も含むと考えられる。

「はい」との回答が 2.6%見られたが，これはネットのサービスやゲームでのIDの貸し借りといった原因が考えられる。大学の ID の貸し借りを行うようになれば，他者によるなりすましや不正行為といった，大変大きなリスク要因となるため，アカウント管理について理解を促進させる必要がある。

情報セキュリティの専門用語に関する知識

設問 7　コンピュータに関連して「小中高校で習ったことがある」あるいは「知っている」語句を下の選択肢から選んで下さい。(複数選ぶことができます)

選択肢：**①機密性・完全性・可用性**，**②暗号化**，**③ファイル共有**，**④コンピュータウイルス**，**⑤ワーム**，**⑥個人情報**，**⑦電子署名**，**⑧認証**，**⑨スパイウェア**，**⑩スパムメール**，**⑪ワンクリック詐欺**，**⑫フィッシング詐欺**，**⑬セキュリティホール**，**⑭ボット**，**⑮その他（自由記述）**

本設問は，複数選択式で情報セキュリティに関連する語彙がどの程度あるかを調べる目的でたずねている。この設問の集計結果は図 7 のようになった。

「個人情報」,「コンピュータウイルス」,「ワンクリック詐欺」がそれぞれ回答者数の 75.9%，75.8%，67.3%を占めており，個人情報の取り扱いの重要性，ウイルス感染防止，ワンクリック詐欺などの犯罪の被害防止といった話題が，初等中等教育の段階で採り上げられているものと思われる。

これに続いて「ファイル共有」,「フィッシング詐欺」,「認証」,「暗号化」,「スパムメール」の回答がそれぞれ 43.4%，39.0%，38.7%，38.5%，36.5%となっており，ネットワーク技術，セキュリティ技術に関連する用語などがある程度認知されている様子が分かる。

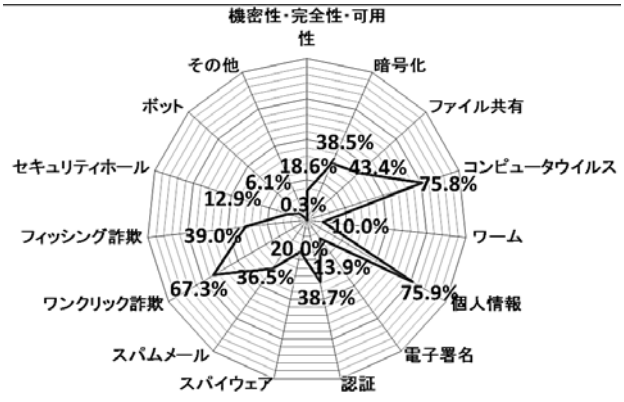


図 7　設問 7 の集計結果

その一方，「スパイウェア」,「機密性・完全性・可用性」,「セキュリティホール」,「ワーム」,「ボット」については，それぞれ 20.0%, 18.6%, 13.9%, 12.9%, 6.1%となっており，他の選択肢に比べて，認知度が低いことが明らかとなった。藤井らの調査によると，高校における情報科目の履修時期は 1 年次が多く，また情報 A のみの履修が多いという傾向があり[7]，より専門性の高い用語や最近のセキュリティ維持の阻害に関わる用語については，この影響により採り上げるのが難しいものと思われる。

次に，図 8 に本設問で選択した選択肢の個数の分布を示す。それぞれの選択肢について，当該の選択肢を選んだ回答者が選んだ選択肢の個数の分布も同図に示す。図 8(a)より，全体では 3 個のところにピークが見られることが分かる。

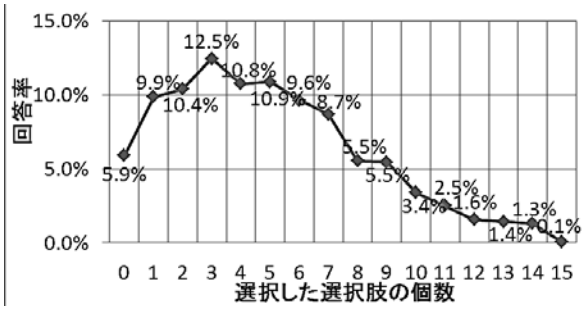
「個人情報」,「コンピュータウイルス」,「ワンクリック詐欺」のような，回答者数が多い選択肢については，図 8(b)のように，比較的少ない選択肢数の箇所（グラフ全体の左側）に集中する傾向が見られ，情報セキュリティの語彙が少ないと見られる学生にも広く浸透している様子が分かる。

「ファイル共有」,「フィッシング詐欺」,「認証」,「暗号化」,「スパムメール」のように，全体の 4 割前後が選択した選択肢については，選択肢数 7 をピークにややグラフの右側に重心を持つ分布となっており（図 8(c)），複数選択した学生が（つまりある程度の情報セキュリティの語彙がある学生が）回答しているものと思われる。

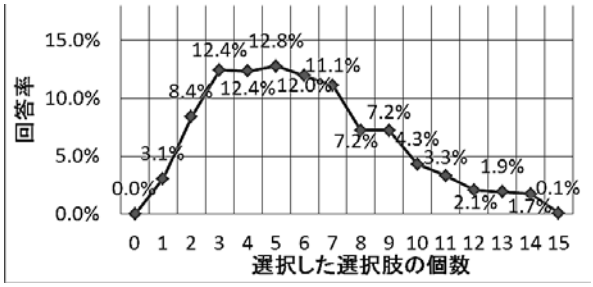
「スパイウェア」,「機密性・完全性・可用性」,「セキュリティホール」,「ワーム」,「ボット」といった，選択した回答者数が少ない選択肢については，図 8(d)のように，選択肢数が多い方にピークをもつ傾向が見られ，一部の学生は情報セキュリティについて相当の語彙をもっていると思われる。特に図 8(e)に示すように，ボットを知っていると回答した人は全員 5 個以上の用語を知っており，ピークが 14 個のところに現れるなど，その傾向が際立っている。

まとめ

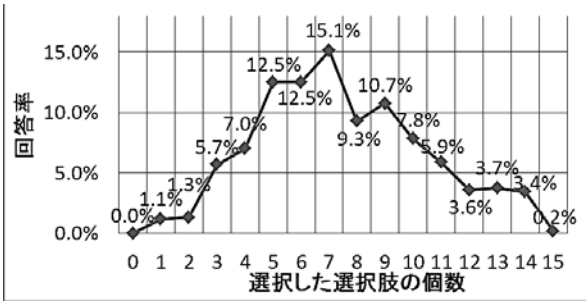
本研究では，長崎大学学部 1 年生に対して，情報セ



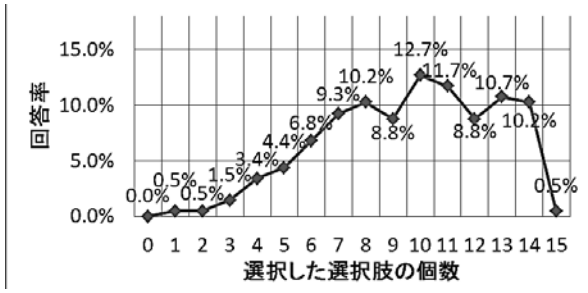
(a) 全体（回答数 1,588）



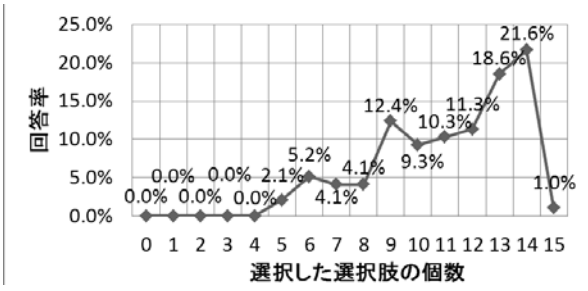
(b) 個人情報を選択（回答数 1,205）



(c) 認証を選択（回答数 614）



(d) セキュリティホールを選択（回答数 205）



(e) ボットを選択（回答数 97）

図 8　設問 7 における選択肢と回答した選択肢の個数の関係

キュリティの理解度・知識に関するアンケートを実施し，回答率は 94.4%であった。今回のアンケートから，パソコン端末に関連するセキュリティについてはある程度理解が進んでいるが，スマートフォンやタブレット端末へのセキュリティについては理解が十分とは言えないことが分かった。また，情報セキュリティに関する用語については，個人情報，ウイルス，ワンクリック詐欺といったものは知られているものの，それ以外の用語については十分には知られていない傾向が分かった。

今後，科目「情報基礎」の履修期間の後半に再度アンケートを行い，理解状況の変化について検討する予定である。

参考文献

[1] 島田裕次，榎木千昭，澤田智輝，内山公雄，五井孝，ISO27001 規格要求事項の解説とその実務，日科技連，2006，259p.

[2] 普及啓発･人材育成専門員会，“第 5 回会合資料 情報セキュリティ人材育成プログラムを踏まえた2012 年度以降の当面の課題等について(案)”，内閣官房情報セキュリティセンター，2012-03-26，http://www.nisc.go.jp/conference/seisaku/jinzai/dai5/pdf/shiryou01.pdf，（参照 2012-05-11).

[3] 文部科学省，“高等学校学習指導要領（ポイント，本文，解説等）”，文部科学省，2010-12-21，http://www.mext.go.jp/a_menu/shotou/new-cs/youryou/1304427.htm，（参照 2012-05-11）

[4] 長崎大学，“中期目標・中期計画・年度計画”，長崎大学，2012-03-30，http://www.nagasaki-u.ac.jp/ja/about/philosophy/plan/index.html，(参照 2012-05-11).

[5] WebClass 社 Web サイト, http://www.webclass.jp/index.html，(参照 2012-05-11).

[6] 情報処理推進機構セキュリティセンター，“Android OS を標的としたウイルスに関する注意喚起”，情報処理推進機構，2011-01-21，http://www.ipa.go.jp/security/topics/alert20110121.html，（参照 2012-05-11）

[7] 藤井ら，“2012 年度長崎大学入学生を対象とした情報科目の学習経験の実態調査”，情報コミュニケーション学会第 9 回研究会予稿集，2012