情報セキュリティ教育の効果と課題
～スマートフォン利用を中心にして～

有　田　真貴子　　大　塚　絵里子　　梶　田　鈴　子

The Effects and Problems of Information Security Education: Focusing on the Smartphone User

Makiko Arita　　Eriko Otuka　　Suzuko Kajita

（2015年11月27日受理）

1．はじめに

中村学園大学短期大学部キャリア開発学科（以下本学科という）では，平成21年度より学生に市販のｅラーニングコンテンツを利用した情報セキュリティ教育を行っている[1) 2) 3) 4) 5) 6)]。しかし，２年間という限られた学習時間の中で行う情報セキュリティ教育は，十分とは言えない現状がある。

本学科平成26年度の入学生に実施したスマートフォンに関するアンケートでは，以下の課題が示された。

・学習した内容を実践していない（ウイルス対策ソフトのダウンロードなど）。
・学生が疑問に思っている点を，学習教材の中に反映することができなかった。
・自作の教材を利用していたにもかかわらず，学習効果が向上しなかった。
・学生に知っておいてほしい内容をより詳しく教材に入れる必要がある。
・確認テストの点数が伸びていない。

さらに，スマートフォンに依存している学生が少なからずいるのではないか，ということが分かった[6)]。

総務省情報通信政策研究所の調査によると，高校生を対象に行った調査で，59.8% の生徒が中程度以上の依存傾向にあることが分かった。依存度の高い生徒は睡眠時間や，学習時間を削ってまでスマートフォンを利用しているケースが多い。さらに，男子生徒よりも，女子生徒の依存が高い傾向にある[7)]。本学科に在籍する学生のほとんどが女子学生であるため，今後はスマートフォン依存症への対応も重要性を増している。

また，最近ではスマートフォンの普及に伴い，スマートフォンのワンクリック詐欺にも新たな手口が出現するなど[8)]，スマートフォンを標的にした犯罪の手口は巧妙化している。動画やゲームなどの多様なサービスへのアクセスが容易になり，スマートフォンを利用する時間が長くなったことが要因の一つではないかと考える。

スマートフォンを含む情報端末による犯罪や被害に学生が遭わないよう，適切に機器を利用する必要がある。そのためにも，随時情報を提供していかなければならない。

このような現状を踏まえ，平成27年度は新しい教材を導入するなど，改善を行った。

これにより，学生のスマートフォンの利用状況や利用する際の意識について教育効果が見られたのか検証を行うため，スマートフォン利用に主眼を置いて，平成26年度と平成27年度のアンケート結果，テスト結果，ならびに，iOS と Android を利用している学生に分けて比較した。本稿では，その結果と，教育効果をより高めるための今後の課題について報告する。

2．対象と方法

本研究は，本学科開講科目「コンピュータ基礎演習A」（１年次前学期必修科目）に履修登録した，平成26年度入学生169名，平成27年度入学生173名が対象である。

調査は，平成26年と平成27年ともに５月から７月までの期間で実施した（表１）。なお「コンピュータ基礎演習 A」は４クラス体制で行っており，各調査はクラス単位で実施した。

別刷請求先：有田真貴子，中村学園大学短期大学部キャリア開発学科，〒814-0198　福岡市城南区別府5-7-1
E-mail：arita@nakamura-u.ac.jp

表１　平成26年度・平成27年度調査内容と実施時期

調査内容	実施時期
事前アンケート 事前確認テスト	５月下旬から ６月上旬
自主学習	５月下旬から７月下旬
事後アンケート 事後確認テスト	7月中旬から 7月下旬

2.1　アンケート調査

学習の前と後に，情報セキュリティおよびスマートフォンに関する知識度，理解度，意識度について平成26年度に行った調査[6]と同じアンケート調査を行った。

質問項目は，事前アンケートでは，情報セキュリティやスマートフォンに関する知識や利用状況についての質問を43問設けた。質問１は，インターネットを利用する際にどのように意識して利用しているのかを複数回答させた。質問２は，スマートフォンを利用する際にどのように意識して利用しているのかを複数回答させた。質問３から質問15までは，学習前の時点で，どの程度情報セキュリティについて理解しているのか，「コンピュータウイルスの感染方法について理解していますか。」といった尋ね方をして，５段階評価で回答させた。質問16から質問41までは，スマートフォンの利用状況について回答させた。回答形式は選択形式または自由記述形式とした。また，質問42および質問43は，情報セキュリティについて不安な点はないか，スマートフォンについて不安な点はないか，記述形式で回答は必須とした。

一方，事後アンケートでは，質問１で学習後インターネットについてどのように実感しているのか複数回答させた。さらに，質問２では学習後スマートフォンについてどのように実感しているのか複数回答させた。

また，質問３から質問15までは，「コンピュータウイルスの感染方法について理解できましたか。」というように事前アンケートと関係性を持たせて尋ね，５段階評価で回答させた。質問16から質問40および質問42は，事前アンケートと同じ内容のものを使用した。質問41は，情報セキュリティや，スマートフォンについてどのように学習したかを複数回答させた。質問43および質問44は記述形式で，回答は必須とした。

2.2　確認テスト

事前・事後アンケートの後にそれぞれ情報セキュリティ・スマートフォンに関する平成26年度に行った調査[6]と同じ確認テスト（事前確認テスト，事後確認テスト）を実施した。

事前確認テストに関しては成績に反映しない旨を学生たちに伝え，抜き打ちで行った。

また，問題数は32問であった。

2.3　自主学習

学生は事前アンケートと事前確認テストの実施後から，各自で学習を開始した。

1 でも述べた平成26年度の調査で見えた課題を踏まえ，本年度はｅラーニング教材をリニューアルした。本年度から利用を開始したｅラーニング教材は，『富士通ラーニングマネージメントシステム Internet Navigware「事例で学ぶ情報セキュリティ2015」）』[9]である（表２）。新たに，スマートフォンの不正アプリケーションや SNS についての内容も追加された。

また，情報処理推進機構（IPA）のホームページと動画[10]を教材として提示した。動画は「あなたのスマートフォン，のぞかれていませんか？」「＜乗っ取り＞の危険があなたのスマートフォンにも！」などである。学生により身近で具体的な事例を取り上げることで，興味を持たせることを目的とした。

さらに，平成26年度に作成した自作教材も提示した。平成26年度の調査では，自作の教材で思ったほどの学習効果を上げることができなかった。学生の学習意欲が低かったことが一因だったと考える。そのため，スライド教材を意識してみるように本年度は教材を提示するだけではなく，授業の折に触れ，ニュースや新聞で取り上げられた情報セキュリティ関連の事件について学生に説明を行った。また，情報端末を扱ううえで日ごろ気を付けるべき点など，細かく注意喚起を行った。

なお，学習をさせるにあたり，事後確認テストでは成績評価との関連を持たせて６割以上の正解を達成目標として明示し，学習意欲の向上を目指した。

表２　ｅラーニング教材「事例で学ぶ情報セキュリティ2015」

学習を始める前に
はじめに
動作環境
操作方法
学習目標
第１章　情報化社会の現状
1-1　情報化の進展
1-2　身の回りにある情報資産
1-3　情報セキュリティの必要性
第１章　チェック問題（評点：100）
第２章　情報化社会の脅威
2-1　情報化社会の脅威
2-2　ウイルスの脅威
2-3　情報漏洩と不正アクセスの脅威

３．結果と考察

事前・事後のアンケート調査と事前・事後の確認テストを欠席した学生を除いて集計と分析を行った。平成26年度は163名（受講者の96.4％），平成27年度は169名（受講者の97.7％）が考察の対象となった。

結果の詳細については，以下のとおりである。

3.1　情報セキュリティに関する分析

記述形式の回答を除くアンケートの集計結果を付録１に示す。

事前アンケートと事後アンケートでの質問３から質問15について，選択肢を表３のように数量化し，表側を事前アンケートの選択肢，表頭を事後アンケートの選択肢として，クロス集計を行った。

表３　アンケートの選択肢の数量化

数量化	事前アンケート	事後アンケート
1	理解している	理解できた
2	ある程度理解している	ある程度理解できた
3	どちらとも言えない	どちらとも言えない
4	あまり理解していない	あまり理解できなかった
5	理解していない	理解できなかった

3.2　意識調査

まず，事前アンケート質問１で，インターネットを利用する際に実感，意識しているものについて尋ねた結果を述べる。前回までの調査結果である平成22年度，平成24年度，平成25年度，平成26年度と平成27年度のデータを集計した結果が図１である。なお，調査方法はいずれの年度も同じである。

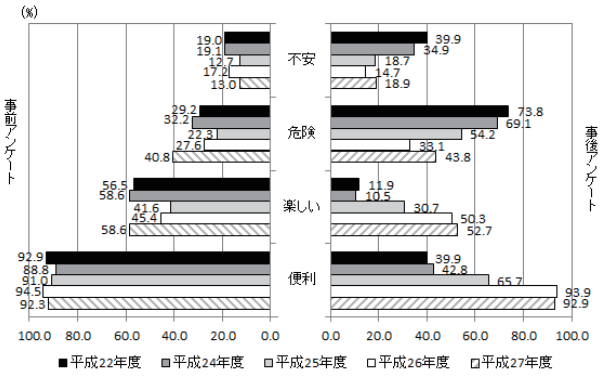

図１　質問１の事前・事後アンケートの変化（複数回答）

得られたデータを元に，平成27年度と過年度で分割表検定を用いて傾向に差があるのかを見たところ，表４に示す結果が得られた。

表４　平成27年度と過年度間の傾向について

年度	事前／事後	項目	平成27年度の傾向	有意水準
22	事後	便利 楽しい	増加	p<0.001
		不安 危険	減少	
24	事後	便利 楽しい	増加	p<0.001
		不安 危険	減少	
25	事前	楽しい	増加	p<0.01
		危険		p<0.001
	事後	便利		
		楽しい		

また，年度ごとに学習前と学習後の意識を比較してみると，平成22年度と平成24年度は４つの項目すべてで有意差が見られた（平成24年度「不安」のみ p<0.01，他は p<0.001）。一方，平成25年度は「便利」（p<0.001）・「楽しい」（p<0.05）・「危険」（p<0.001）については有意差が認められたが，「不安」については有意差が認められなかった。平成26年度並びに平成27年度は，すべての項目で有意差が認められなかった。

次にスマートフォンを利用するにあたっての意識を調査した結果を述べる（図２）。学習前後において，平成26年度はいずれの項目でも有意差は見られなかったが，平成27年度は「不安」において有意差が見られた（p<0.01）。また，平成26年度と平成27年度を比較すると，学習前の「危険」（p<0.01）と学習後の「不安」（p<0.05）で有意差が見られた。

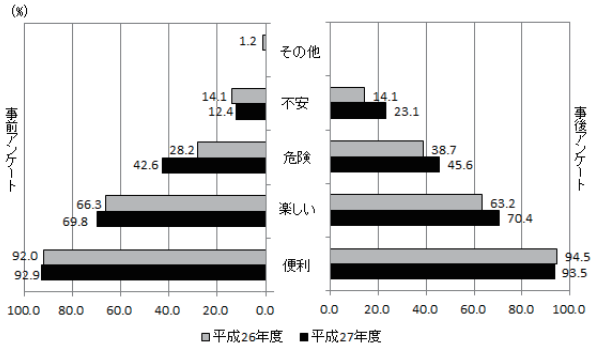

図２　スマートフォン利用における学習前後の意識の変化

質問３から質問15では，基本的な情報セキュリティの知識の有無について質問した。数量化に基づいた学生ごとの事前アンケートと事後アンケートの平均値の関連を見ると，平成27年度の相関係数は0.231で弱い相関が見られた。

3.3　スマートフォン利用状況

利用している OS について（質問16）尋ねた事後アンケートでは，iOS と回答した学生（以下 iOS ユーザーと呼ぶ）が78.7％，Android と回答した学生（以下 Android ユーザーと呼ぶ）が21.3％であった。

次に，主に利用する機能について（質問19）尋ねた。平成26年度と平成27年度の事後アンケート結果を比較した結果が図4である。なお，項目「ゲーム」については平成26年度より追加した。マイナビが2016年卒の大学生を対象に調査した「ソーシャルメディア・SNS を使う感覚」によると，利用目的は友人との連絡手段53.4％，情報を得ることのできるニュース媒体44.3％となっている[11]。本学科学生の LINE の利用率は98.8％と過去２年で一番割合が高いことが分かる。LINE や Twitter は匿名（ニックネーム）で利用でき，個人が特定されにくいことから，実名登録制である Facebook に比べ，学生は気軽に利用しているのではないかと考える。その他に記載された利用する機能については，写真・動画共有アプリケーションである Instagram（インスタグラム）があった。SNS の利用率増加がカメラの利用につながっていると推測する。

平成26年度と平成27年度の傾向を分析したところ，次の傾向が分かった。

- 平成27年度の学生は，平成26年度の学生と比べ，LINE を利用する割合が高い（p<0.05）。
- 平成27年度の学生は，平成26年度の学生と比べ，Twitter を利用する割合が高い（p<0.05）。
- 平成27年度の学生は，平成26年度の学生と比べ，カメラを利用する割合が高い（p<0.05）。

さらに，平成26年度と平成27年度の平日，休日の利用時間を比較した（図３）。

平日と休日，また，学習前後の利用時間を比較したが，有意差は見られなかった。本年度は，平成26年度の利用時間の結果を受け，本学科にもスマートフォン依存が疑われる学生がいることから，授業内で複数回，注意喚起を行った。しかし，学習後にも１日12時間以上と回答している学生がおり，特に休日の利用状況から推察してスマートフォンに依存している学生が増加傾向にあるのではないかと考えられる。

3.4　個人情報の取扱い

マイナビの調査では，2016年卒の大学生の96.6％が SNS を活用している[11]。また，最近では就職活動にも SNS を利用する学生がいる。本学科でも多くの学生が SNS を利用しているため，個人情報をどのように取り扱っているか尋ねた（質問21）。平成26年度と平成27年度の事後アンケートを比較した結果を図5に示す。

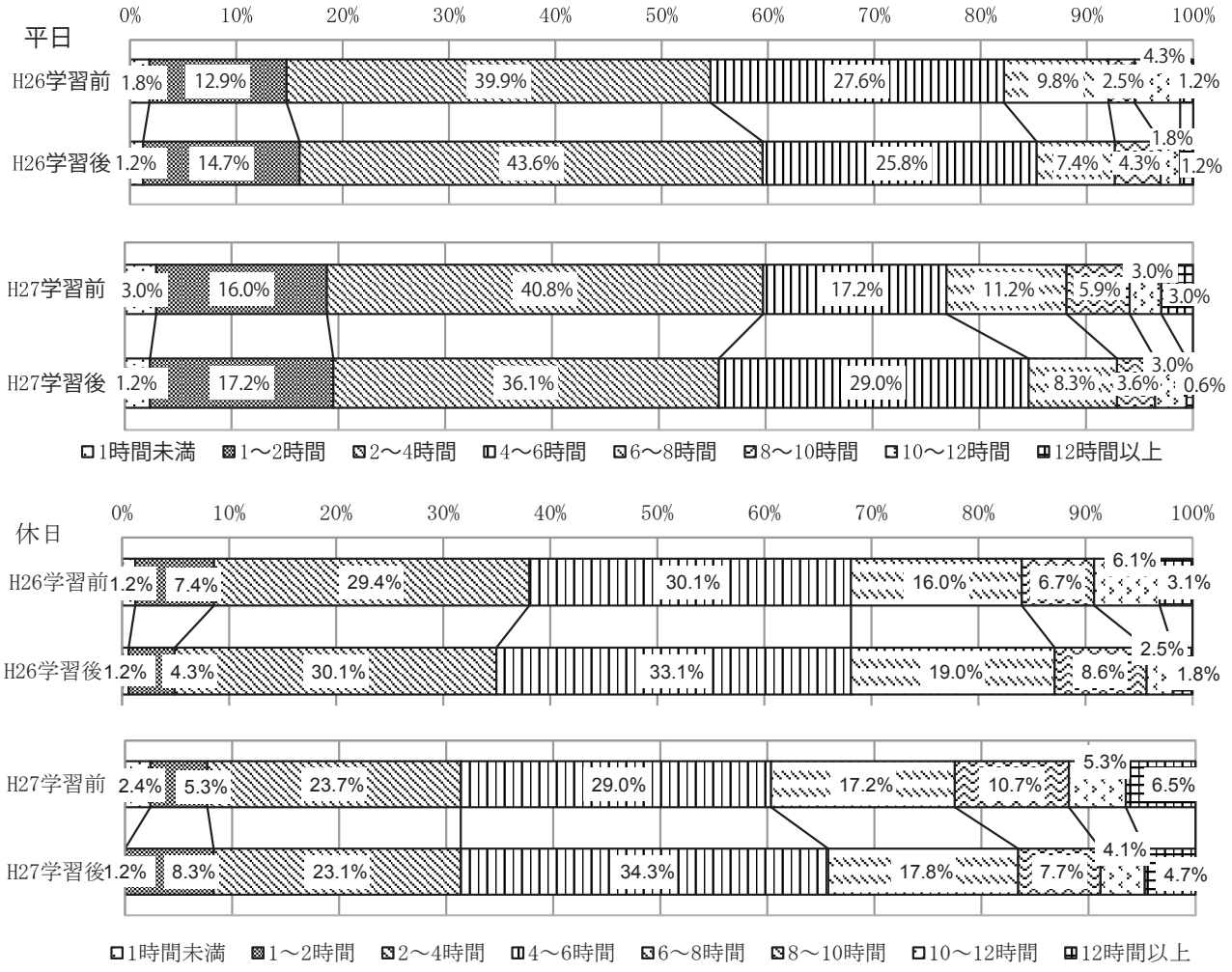

図３　平日と休日のスマートフォン利用時間

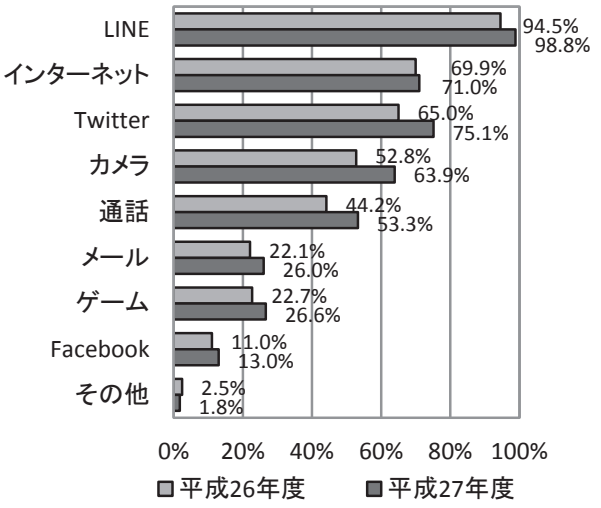

図４　事後アンケート　主に利用する機能（複数回答）

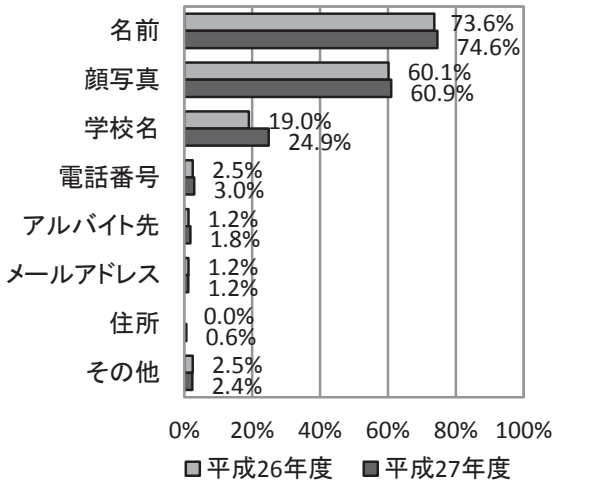

図５　事後アンケート　SNS に登録している情報（複数回答）

平成26年度と平成27年度の学習後において，有意差は見られなかったが，学習前において，平成27年度の学生は平成26年度の学生と比べると，学校名を登録している割合が高いことが分かった（$p<0.05$）。

SNS を利用するうえで，名前の登録はほぼ必須であると考える。自作の学習教材には，SNS に登録する個人情報に十分注意するよう呼びかける内容を入れたが，学習後もなお，半分以上の学生が顔写真を登録していることが分かる。

総務省によると，公開している情報が断片的なものであっても，さまざまな情報を組み合わせることにより，個人を特定できる可能性が高いとしている[12]。また，万が一，インターネット上に不適切な内容を書き込んでしまった場合，削除をしたとしても“Web 魚拓”で内容は永久に残るため[13]，SNS に登録している個人情報から，“炎上”に巻き込まれてしまう恐れもある。図５の結果より，電話番号や住所を登録している学生もいるため，学生が SNS を発端としたストーカー被害などの犯罪に遭わないためにも，今後も継続して SNS 利用についての指導が必要である。

3.5　OS ごとのセキュリティ意識の違いについて

本学科の学生の OS の利用状況は iOS ユーザーと Android ユーザーのどちらかであった。そのため，OS ごとに分析を試みた。比較の対象は平成27年度のみとした。次のような結果が得られた。

まず，アプリケーションをインストールする際に，配信元や利用条件などをよく確認しているか（質問24）を尋ねた結果が図６である。

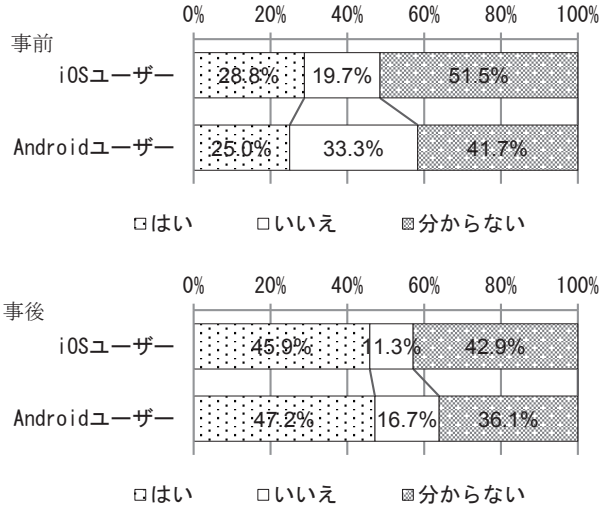

図６　配信元や利用条件などをよく確認しているか

OS 別では，学習前も学習後も，iOS ユーザーと Android ユーザーともに有意差は見られなかったが，両 OS とも「確認している」割合が多くなり，「確認していない」割合が少なくなった。しかし，「分からない」と回答した学生が両 OS とも学習後に約４割程度いることから，「確認している」という回答が増えたからといって安心はできない。

また，平成26年度と平成27年度の全体を比較してみると，平成27年度の学習前後において有意差が見られた（$p<0.001$）。さらに，学習後は，平成26年度より平成27年度の方が良い結果となった（$p<0.05$）。

また，「アプリによっては確認している」と回答した学生は，「有名なアプリ」や「みんなが使っているから」と基準が安易なものであることを危惧する。学習後もなお，安全に対する意識に関して課題が残る結果となった。補助教材には，アプリケーションの入手先に注意すること，インストールするアプリケーションが求めてくる情報は何か，利用条件を確認することなどを示した。なぜ，配信元や利用条件などを確認しないのか，事後アンケートで理由を尋ねると，インストール時の利用条件は，長い文章であることや，何を確認すれば良いか分からないため，きちんと確認をするという行動に結びついていないことが分かった。

次に，スマートフォンの OS を最新のものにしているか（質問26）尋ねた結果が図７である。

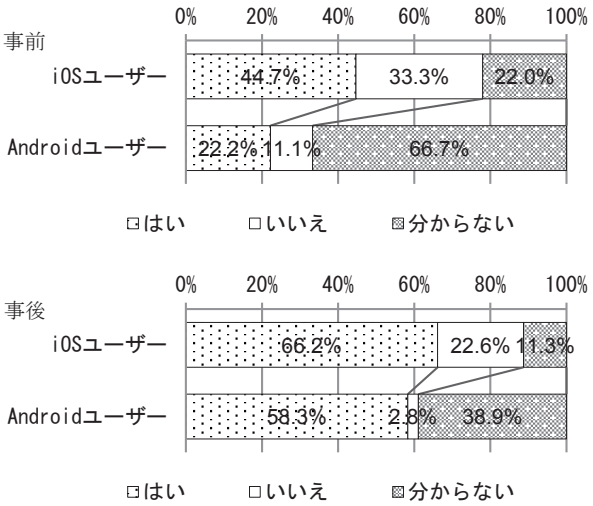

図７　OS を最新のものにしているか

OS 別では学習前と学習後ともに iOS ユーザーと Android ユーザーに差が見られた（$p<0.01$）。iOS ユーザーの方が学習前から OS の更新をしていることが分かる。学習後 Android ユーザーも OS の更新の必要性を理解し更新をしているようだが，学習後にも約４割の学生が「分からない」と回答している点は今後の課題である。

また，平成26年度と平成27年度の全体を比較したところ，どちらの年度とも学習前後で有意差が見られた（平成26年度（$p<0.05$），平成27年度（$p<0.001$））。

また，学習前は平成26年度の方が平成27年度より良い結果であった（$p<0.05$）が，学習後には有意差は見られなかった。

事後アンケートではどちらの年度も「最新のものにしている」と回答した学生が６割以上と学習の効果がみられた。

さらに，どちらの年度も「分からない」と答えた学生は更新の仕方を理解していないことが分かった。今後は

具体的な更新方法まで教材に入れる必要があると感じた。

次に，スマートフォンにパスワードによるロックをかけているか（質問28）尋ねた結果が図８である。

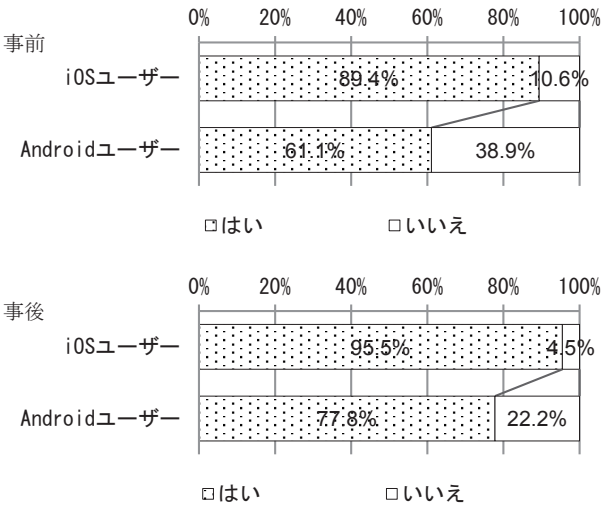

図８　パスワードによるロックをかけているか

事前アンケートおよび事後アンケート共に有意差がみられ，iOS ユーザーの方がロックをかけている割合が多いことが分かった（p<0.05）。

スマートフォンは大量の情報を保持できる機器である。情報の中には，所有者の情報だけではなく，知人の連絡先なども入っているため，紛失した場合には情報漏洩や悪用される危険性がある。パスワードによるロックをかけることで悪用されにくくなる。簡単にできる対策であるため，今後も継続的にロックをかけることを呼びかけたいと考える。

次に，スマートフォンのウイルス感染について知っているか（質問30）尋ねた結果が図９である。

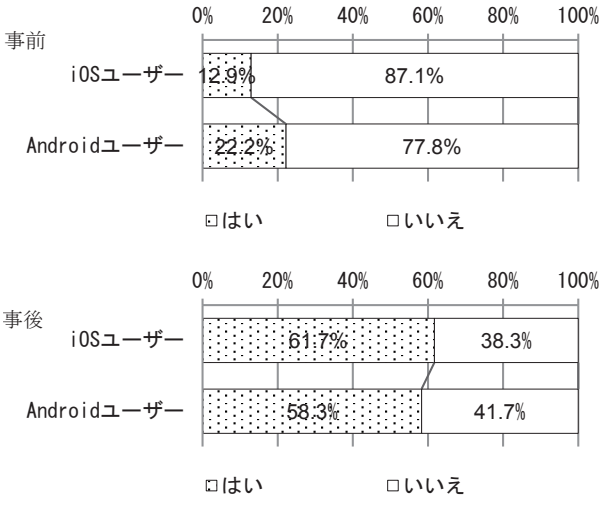

図９　ウイルス感染について知っているか

両 OS の事前アンケートと事後アンケートを比較したところ iOS ユーザーおよび Android ユーザーどちらとも有意な差が見られ，学習後の方が良い結果となった（iOS ユーザー（p<0.001），Android ユーザー（p<0.05））。

しかし，学習後にも理解していない学生が約４割近くいることから，一概にはいい結果が出たとは言い切れない。課題の残る結果となった。

なお，先般からニュースになっているが，iOS アプリケーションにマルウェアが発見された[14]。iOS ユーザーは今後，今まで以上に注意を払う必要がある[6]。

また，平成26年度，平成27年度の全体の結果を比較したところ，事前と事後に有意差が見られた（p<0.001）。そのため，意識が改善されたことが分かる。また，学習前には平成26年度と平成27年度は有意差が見られなかったが，学習後は平成27年度の方が平成26年度より良い結果となった。（p<0.001）。

学習前にどのような事を知っているのかを学生に尋ねると，どちらの年度も，「アカウントを乗っ取られる」や，「アプリケーションを通して感染する」と述べている。また，平成27年度には「パソコンと USB で繋いで扱うとそれを通してウイルスに感染する」という，iOS で最も注意が必要な感染方法についても知っている学生がいた。学習後は，「アプリケーションや迷惑メールから感染する」や，「安全なアプリと見せかけて悪性なアプリケーションをインストールさせる」など学習後はウイルス感染の経路などについてより深く理解したことが分かる。

次に，スマートフォンにウイルス対策ソフトをインストールしているか（質問32）尋ねた結果を図10に示す。

両 OS の事前アンケートと事後アンケートを比較したところ結果に差が見られた（p<0.001）。事後において，

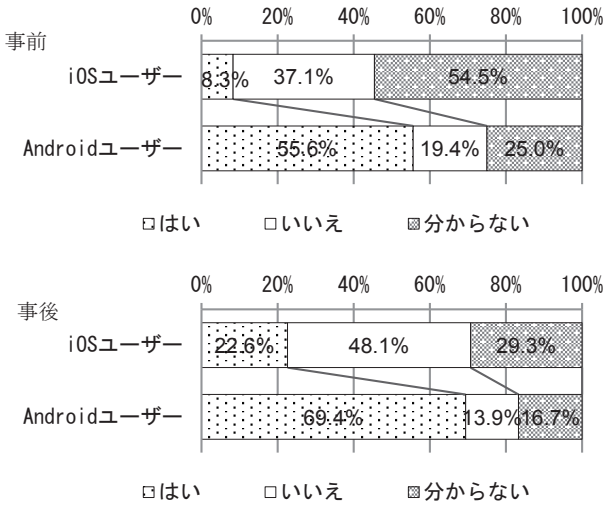

図10　ウイルス対策ソフトをインストールしているか

iOS ユーザーの「分からない」と回答した割合は減少したが，それに伴い「いいえ」と回答した割合も増加したところを見ると，Android ユーザーに比べ，iOS ユーザーのウイルス対策について認識の甘さが伺える。

また，年度ごとに全体の結果を見てみると，平成26年度は学習前後で有意差が見られなかったが，平成27年度は有意差が見られた（p<0.001）。また，学習前は平成26年度と平成27年度に有意差は見られなかったが，学習後は平成27年度の方が平成26年度より良い結果となった（p<0.001）。

次に，スマートフォンの GPS（位置情報）機能について知っているか（質問36）尋ねた結果を図11に示す。

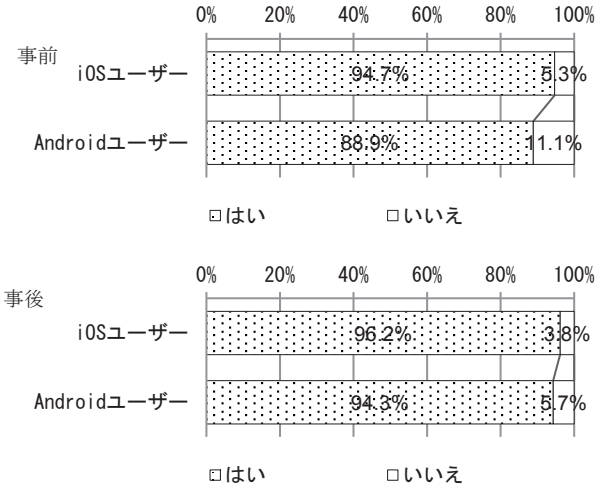

図11　GPS 機能について知っているか

両 OS の事前アンケートと事後アンケートを比較したところ，認知度で差は見られなかった。しかし，学習前は Android ユーザーの方が認知度は低い結果であったが，学習後には両 OS とも９割以上の学生が「知っている」と回答したことから，学習の効果が見られる。さらに，Android ユーザーの学習前と学習後を比較すると有意差が見られた（p<0.001）。

また，平成27年度の全体の結果を見てみると，事後アンケートでは95.9％の学生が「知っている」と回答した。

しかし，スマートフォンで写真を撮る際に GPS の設定はどうしているか（質問39）尋ねた結果，学習後には「分からない」と回答した割合は低くなったものの（p<0.01），依然自身が使う端末の設定方法までは理解していない学生がいる様子が伺える。

さらに，質問20では SNS を利用しているか尋ねた。事前アンケートでは iOS ユーザーと Android ユーザーどちらの学生もほぼ全員の学生が利用していたが，事後アンケートの結果を見ると利用している学生が若干減少した。危機意識を持たせることも重要であるが，危機意識をあおるばかりでは，教育成果が出たとは言えない。そのため「正しい使い方」を教育することが重要である。今後は SNS の利用に重点を置いた教育も進めていく必要があると考える。

3.6　事前確認テストおよび事後確認テスト

各確認テストの内容を付録2に示す。確認テストは１問１点として集計した。

平成26年度と平成27年度の問題ごとの正答率の変化を図12と表５に，平成26年度および平成27年度の確認テストの結果を表６に示す。

順位和検定を用いて分析をした結果，事前確認テストと事後確認テストでは，どちらの年度も事後確認テストの方が成績の良いことが分かった（p<0.01）。

表５　平成27年度　確認テスト正答率

時期 / 正解率	H26事前	H26事後	H27事前	H27事後
最高正答率	78.13％	96.88％	78.13％	93.75％
最低正答率	28.13％	37.50％	34.38％	37.50％
平均正答率	55.94％	75.63％	57.81％	70.94％
標準偏差	10.31％	10.47％	9.56％	10.81％

McNemar 検定を用いてそれぞれの年度で問題ごとに事前確認テスト，事後確認テストの結果を分析したところ，正答率に有意差が認められたのは全32問中平成26年度は26問，平成27年度は20問であった。有意差のない問題を見てみると，本年度問題10については，正答率が1.1％下がっていた。また，平成26年度は9.2％正答率を下げていた問題20に関して，本年度も正答率が2.3％下がっていた。**2.3**でも述べたが，学習をさせるにあたり，事後確認テストで６割以上正解することを目標として定めた。この達成目標である得点率60％以上に達成した学生は，平成26年度は156名（95.7％），平成27年度は151名（87.3％）であった。

次に，平成27年度の学生ごとの事前確認テストと事後確認テストの点数の関連を見てみると，相関係数は0.349で弱い正の相関があることが分かった（p<0.001）。

3.7　学習方法について

事後アンケート（質問41）で，学習方法について複数回答で答えさせた。

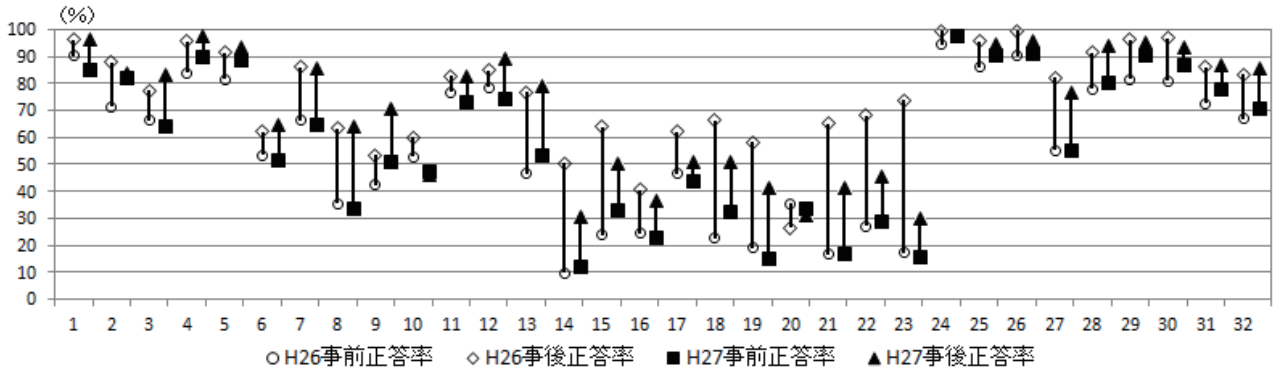

図12　確認テストの問題ごとの正答率

回答項目は「１．スライドショー（筆者らが作成）」,「２．ｅラーニング」,「３．インターネット」,「４．授業で使用しているテキスト」,「５．特に学習していない」,「６．その他」とした。平成26年度と平成27年度の結果を表５に示す。なお，複数の学習方法を利用した学生がいるため,「１．スライドショー（筆者らが作成）」と「２．ｅラーニング」を利用して学習した学生については,「１・２」と表記している。また，アンケートでは，勉強方法のみを問い，それぞれの学習時間については問わなかった。

表６　学習方法について

学習方法	平成26年度		平成27年度	
	平均点	人　数	平均点	人　数
1	24.4	111	21.5	14
2	25.8	4	22.0	25
3	24.4	5	21.2	5
4	26.3	6		
5	24.7	6	20.4	5
1・2	22.5	12	23.8	67
1・3	23.2	10	22.0	7
1・4	26.0	1	22.3	3
1・6	27.0	1		
2・3	19.0	3	19.5	8
2・4			20.0	2
3・4	20.0	1		
4・6	27.0	1		
1・2・3			22.6	16
1・2・4			24.0	5
1・3・4			22.3	4
2・3・4	25.0	1	24.0	1
1・2・3・4	30.0	1	23.9	7

3.6でも述べたが，学習前確認テストの全体の平均点は18.5点，学習後確認テストの全体の平均点は22.7点であった。表４の結果より，スライドショーとｅラーニング，授業のテキストを用いた学習方法が，特に効果を上げたことが分かる。しかし，平成26年度の事後確認テストの全体の平均点は24.2点[6]であり，平成27年度は得点を下げている。この結果から，自作の教材内容の見直しや学生が関心を持って学習できるよう，より一層学習効果を上げる方法を検討しなければならない。

４．今後の課題

今回の調査では，スマートフォンのウイルスや，OSの更新などについて，学習後もなお事後アンケートで「分からない」と回答した学生がいた。また，得点が昨年度に比べ伸び悩んだことなど，課題が残る結果となった。

しかし，学習後に改善のみられることから，学習には一定の効果があったと考えられる。今後の課題として，以下のような点があげられる。

第一の課題として，4つの点において教材の改善が必要である。

１）**3.5**でも述べたが，現在自作の教材では，OSの更新の必要性については述べているが，更新の具体的な方法までは示せていない。今後は具体的な更新方法まで，掲載する必要がある。

２）iOSアプリケーションにマルウェアが発見された事例[14]など，スマートフォンに関する新たなトラブルは頻繁に報告されている。時代に即した教材内容にする必要がある。

３）アンケートの意見から，ウイルス対策ソフトについて，自分のスマートフォンにウイルス対策ソフトが入っているか知る方法について，ウイルスに感染してしまった場合の対応について，ウイルス対策ソフトの種類や導入に必要な金額について，具体的に紹介する。また，迷惑メールについても,「困っているがどうしたら良いか分からない」という意見が多数あった。迷惑メールといった身近なトラブルへの対処方法についてもより具体的な内容を教材に入れ，学生の意見を反映させたものにする。

4）今回学生に提示したIPAの教材は，動画以外にも，セキュリティの警告に少女マンガ風のイラストを使用するなど若者が興味を持ちやすい形で事例を紹介している[9]。このような外部の情報セキュリティサイトも上手く活用し，学習に役立てたい。

さらに，本年度授業内で最新の事例などを学生に提示した。今後も情報を学生へ周知して行きたいと考える。

第二の課題として，アンケートとテストの精査が必要である。

第一の課題で述べたとおり，スマートフォンなどの情報機器に関するセキュリティの情報は日々更新されている。アンケート内容と確認テスト問題も教材の内容と併せていくことが必要である。

学生の意見がより分かりやすいアンケートや理解度がみえるテスト内容を検討したい。

第三の課題として，SNSの適切な利用方法の周知があげられる。

スマートフォンのトラブルと切っても切り離せないのがSNSである。スマートフォンの普及に伴い，SNSの利用率も上がっている。個人情報の取り扱いでSNSについても触れているが，今後ますます増えるであろうSNSに関したトラブルに学生が遭わないためにも，SNS別に具体的な注意を学生に知らせていきたい。

また，総務省情報通信政策研究所の調査[7]で女子生徒がより，スマートフォンへの依存度が高いと示されていた。そのため，学生のほとんどが女子学生である本学科は特に力を入れて指導をする必要がある。昼休みの学生の様子を見てみるとほとんどの学生がLINEやTwitterを確認しているように見える。スマートフォン依存症の対策として，就寝する1時間前から起床するまで電源を切っておくなど，少しでもスマートフォンと離れる時間が必要ではないかと考える。

図4で示したとおり，本学科におけるLINEの利用率は98.8％にも達している。便利なアプリケーションであり，本学科でもゼミナールでの連絡手段に利用しているという話をよく耳にする。しかし，昨今の報道でも多く取り上げられているが，アカウントの乗っ取り被害や，便利であるはずの「既読」機能が原因で，LINEでのやりとりにいつも気を取られてしまうなど，デメリットがあることも常に頭に入れて利用しなければならない。

最後に第四の課題として，確認テストの点数の伸び悩みである。**3.6**でも述べたとおり，事後確認テストで目標の得点を取得した学生が少なかった。

第二の課題でも述べたが，来年度はテスト内容を検討する。

さらに，eラーニングの内容から発展した問題を作成することを検討したい。

冒頭で述べたとおり，スマートフォンを含む情報端末による犯罪や被害に学生が遭わないように，適切にスマートフォンを利用する必要がある。そのためにも，随時情報を提供していかなくてはならない。

スマートフォンは，私たちの生活をより便利に手助けしてくれるツールである。正しい知識を持って，安全に利用してほしいものである。

引用及び参考文献・URL

1）花隈悦子，梶田鈴子，eラーニング教材を使った情報セキュリティ教育の試みと評価，中村学園大学・中村学園大学短期大学部研究紀要第42号，293-302，2009.

2）花隈悦子，eラーニング教材を使った情報セキュリティ教育の試みと評価（2），中村学園大学・中村学園大学短期大学部研究紀要第43号，293-302，2010.

3）有田真貴子，梶田鈴子，情報セキュリティ教育におけるeラーニング教材の学習効果の検証，中村学園大学・中村学園大学短期大学部研究紀要第45号，65-74，2013.

4）有田真貴子，梶田鈴子，情報セキュリティ学習における自学自習の効果と課題，中村学園大学・中村学園大学短期大学部研究紀要第46号，47-57，2014.

5）大塚絵里子，梶田鈴子，短期大学生におけるスマートフォン利用の現状分析，中村学園大学・中村学園大学短期大学部研究紀要第46号，71-80，2014.

6）大塚絵里子，有田真貴子，梶田鈴子，情報セキュリティ教育における新たな試み，中村学園大学・中村学園大学短期大学部研究紀要第47号，55-69，2015.

7）総務省情報通信政策研究所，高校生のスマートフォン・アプリ利用とネット依存傾向に関する調査報告書
http://www.soumu.go.jp/main_content/000302914.pdf.

8）独立行政法人　情報処理推進機構スマートフォンでのワンクリック請求の新しい手口にご用心」～　業者への電話，メールは絶対NG　～，
http://www.ipa.go.jp/security/txt/2015/04outline.html.

9）Fujitsu Internet Navigware　eラーニングソリューション
http://jp.fujitsu.com/solutions/elearning/.

10）独立行政法人　情報処理推進機構，https://www.jpa.go.jp.

11）2016年卒マイナビ大学生のライフスタイル調査
http://saponet.mynavi.jp/enq_gakusei/lifestyle/.

12）総務省，国民のための情報セキュリティサイト
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/attention/02.html.

13）日経BP社，キーワードで学ぶ最新情報トピックス2015，2015.

14）マイナビニュース，iOSデバイスに感染するWireLurker

マルウェアの仕組みと対策,
http://news.mynavi.jp/articles/2014/11/10/iphone_
security/.

付録１　事前アンケート及び事後アンケートの内容と集計結果（記述解答を除く）

事前アンケート

1. インターネットを利用する際、下記の項目について自分が実感しているもの、意識しているものを選びなさい。（複数回答可）

便利	156(92.3%)
楽しい	99(58.6%)
危険	69(40.8%)
不安	22(13.0%)
その他	0(0.0%)

2. スマートフォンを利用する際、下記の項目について自分が実感しているもの、意識しているものを選びなさい。（複数回答可）

便利	157(92.9%)
楽しい	118(69.8%)
危険	71(42.0%)
不安	21(12.4%)
その他	1(0.6%)

17. 平日ではどれくらいの時間スマートフォンを使用しますか。
18. 休日ではどれくらいの時間スマートフォンを使用しますか。
19. スマートフォンでは、主に何の機能を使用していますか。（複数回答可）
21. （20 で「はい」と答えた方）SNS（Twitter や Facebook、LINE など）にはどのような情報をのせていますか。（複数回答可）
23. （22 で「はい」と答えた方）内容・原因・対処について差し支えない範囲で教えてください。
25. （24 の質問）その理由は何ですか。
27. （26 の質問）その理由は何ですか。
29. （28 の質問）その理由は何ですか。
31. （30 で「はい」と答えた方）どんなことを知っていますか。
33. （32 の質問）その理由は何ですか。
35. （34 で「はい」と答えた方）どのような状況でいつ気付いたか・対処について差し支えない範囲で教えてください。
38. （37 で「変更している」「変更していない」「必要に応じて変更している」と答えた方）その理由は何ですか。
40. （39 で「オンにしている」「オフにしている」「必要に応じて変更している」と答えた方）その理由は何ですか。
41. スマートフォンを利用していて不安を感じること、感じたことはありますか。
42. 情報セキュリティについて気になることや心配なこと、実際に経験したトラブル、その他聞きたいことなどがあれば自由に書いてください。
43. スマートフォンについて気になることや心配なこと、実際に経験したトラブル、その他聞きたいことなどがあれば自由に書いてください。

3. コンピュータウィルスの感染方法について

	1	2	3	4	5	計
1	2	3	1	0	0	6(3.6%)
2	14	23	0	0	1	38(22.5%)
3	17	21	2	1	0	41(24.3%)
4	16	22	6	2	0	46(27.2%)
5	11	18	7	2	0	38(22.5%)
計	60 (35.5%)	87 (51.5%)	16 (9.5%)	5 (3.0%)	1 (0.6%)	169

5. コンピュータウィルスに感染した場合の対処方法について

	1	2	3	4	5	計
1	0	1	0	0	0	1(0.6%)
2	1	2	0	0	0	3(1.8%)
3	5	12	4	1	0	22(13.0%)
4	9	27	11	1	0	48(28.4%)
5	21	43	24	6	1	95(56.2%)
計	36 (21.3%)	85 (50.3%)	39 (23.1%)	8 (4.7%)	1 (0.6%)	169

7. USB メモリを介して感染するウイルスについて

	1	2	3	4	5	計
1	1	1	0	0	0	2(1.2%)
2	3	5	0	0	0	8(4.7%)
3	3	6	2	0	0	11(6.5%)
4	15	19	2	1	0	37(21.9%)
5	31	51	22	6	1	111(65.7%)
計	53 (31.4%)	82 (48.5%)	26 (15.4%)	7 (4.1%)	1 (0.6%)	169

9. 不正アクセスの被害に遭った場合どのように対処をするかについて

	1	2	3	4	5	計
1	1	2	0	0	0	3(1.8%)
2	5	11	1	0	0	17(10.1%)
3	8	12	4	0	0	24(14.2%)
4	7	24	15	4	0	50(29.6%)
5	20	28	20	6	1	75(44.4%)
計	41 (24.3%)	77 (45.6%)	40 (23.7%)	10 (5.9%)	1 (0.6%)	169

11. 個人情報の漏洩を防ぐための安全なホームページの見分け方について

	1	2	3	4	計
1	4	1	1	1	7(4.1%)
2	12	12	2	0	26(15.4%)
3	8	18	12	2	40(23.7%)
4	17	20	14	3	54(32.0%)
5	17	17	6	2	42(24.9%)
計	58 (34.3%)	68 (40.2%)	35 (20.7%)	8 (4.7%)	169

13. 著作権について

	1	2	3	4	5	計
1	36	15	1	1	0	53(31.4%)
2	32	27	9	0	1	69(40.8%)
3	14	18	3	0	0	35(20.7%)
4	5	3	0	0	0	8(4.7%)
5	2	1	1	0	0	4(2.4%)
計	89 (52.7%)	64 (37.9%)	14 (8.3%)	1 (0.6%)	1 (0.6%)	169

事後アンケート

1. インターネットを利用する際、下記の項目について自分が実感しているもの、意識しているものを選びなさい。（複数回答可）

便利	157(92.9%)
楽しい	89(52.7%)
危険	74(43.8%)
不安	32(18.9%)
その他	0(0.0%)

2. スマートフォンを利用する際、下記の項目について自分が実感しているもの、意識しているものを選びなさい。（複数回答可）

便利	158(93.5%)
楽しい	119(70.4%)
危険	77(45.6%)
不安	39(23.1%)
その他	0(0.0%)

17. 平日ではどれくらいの時間スマートフォンを使用しますか。
18. 休日ではどれくらいの時間スマートフォンを使用しますか。
19. スマートフォンでは、主に何の機能を使用していますか。（複数回答可）
21. （20 で「はい」と答えた方）SNS（Twitter や Facebook、LINE など）にはどのような情報をのせていますか。（複数回答可）
23. （22 で「はい」と答えた方）内容・原因・対処について差し支えない範囲で教えてください。
25. （24 の質問）その理由は何ですか。
27. （26 の質問）その理由は何ですか。
29. （28 の質問）その理由は何ですか。
31. （30 で「はい」と答えた方）どんなことを知っていますか。
33. （32 の質問）その理由は何ですか。
35. （34 で「はい」と答えた方）どのような状況でいつ気付いたか・対処について差し支えない範囲で教えてください。
38. （37 で「変更している」「変更していない」「必要に応じて変更している」と答えた方）その理由は何ですか。
40. （39 で「オンにしている」「オフにしている」「必要に応じて変更している」と答えた方）その理由は何ですか。
41. 情報セキュリティや、スマートフォンについてどのように学習をしましたか。（その他を選んだ人は、具体的に（書籍のタイトルなど）記入をしてください。）
42. 学習後スマートフォンを利用していて不安を感じること、感じたことはありますか。
43. 情報セキュリティについて気になることや心配なこと、実際に経験したトラブル、その他聞きたいことなどがあれば自由に書いてください。
44. スマートフォンについて気になることや心配なこと、実際に経験したトラブル、その他聞きたいことなどがあれば自由に書いてください。

4. コンピュータウィルスに感染した場合起こる現象について

	1	2	3	4	5	計
1	4	4	0	0	0	8(4.7%)
2	18	14	2	0	0	34(20.1%)
3	13	19	5	0	1	38(22.5%)
4	21	26	6	0	0	53(31.4%)
5	13	12	10	1	0	36(21.3%)
計	69 (40.8%)	75 (44.4%)	23 (13.6%)	1 (0.6%)	1 (0.6%)	169

6. ウィルス対策ソフトの機能について

	1	2	3	4	5	計
1	4	1	0	0	0	5(3.0%)
2	4	14	0	0	0	18(10.7%)
3	6	15	7	0	0	28(16.6%)
4	10	19	7	3	0	39(23.1%)
5	23	31	20	4	1	79(46.7%)
計	47 (27.8%)	80 (47.3%)	34 (20.1%)	7 (4.1%)	1 (0.6%)	169

8. 不正アクセスがどのようなものかについて

	1	2	3	4	5	計
1	10	7	0	0	0	17(10.1%)
2	14	20	2	1	0	37(21.9%)
3	21	25	8	0	0	54(32.0%)
4	13	18	2	1	0	34(20.1%)
5	8	13	5	0	1	27(16.0%)
計	66 (39.1%)	83 (49.1%)	17 (10.1%)	2 (1.2%)	1 (0.6%)	169

10. 「個人情報」の具体的な意味合いについて

	1	2	3	5	計
1	20	9	2	0	31(18.3%)
2	27	23	6	1	57(33.7%)
3	23	23	10	0	56(33.1%)
4	10	5	3	0	18(10.7%)
5	1	5	1	0	7(4.1%)
計	81 (47.9%)	65 (38.5%)	22 (13.0%)	1 (0.6%)	169

12. 迷惑メールの見分け方について

	1	2	3	4	計
1	38	14	1	0	53(31.4%)
2	29	21	4	2	56(33.1%)
3	18	9	3	0	30(17.8%)
4	5	7	7	1	20(11.8%)
5	2	6	0	2	10(5.9%)
計	92 (54.4%)	57 (33.7%)	15 (8.9%)	5 (3.0%)	169

14. エスクローサービスについて

	1	2	3	4	5	計
1	1	0	0	0	0	1(0.6%)
3	4	1	3	0	0	8(4.7%)
4	0	4	5	0	0	9(5.3%)
5	20	38	58	28	7	151(89.3%)
計	25 (14.8%)	43 (25.4%)	66 (39.1%)	28 (16.6%)	7 (4.1%)	169

15. ソーシャルエンジニアリングについて

	1	2	3	4	5	計
1	0	0	1	1	0	2(1.2%)
3	2	2	4	0	0	8(4.7%)
4	0	6	8	2	0	16(9.5%)
5	21	45	49	22	6	143(84.6%)
計	23 (13.6%)	53 (31.4%)	62 (36.7%)	25 (14.8%)	6 (3.6%)	169

20. SNS（Twitter やFacebook、LINE など）を利用していますか。

	はい	いいえ	計
はい	164	4	168(99.4%)
いいえ	0	1	1(0.6%)
計	164 (97.0%)	5 (3.0%)	169

24. アプリをインストールする際に、配信元や利用条件などをよく確認していますか。

	はい	いいえ	アプリによっては確認している	計
はい	37	2	8	47(27.8%)
いいえ	13	13	13	39(23.1%)
アプリによっては確認している	28	6	49	83(49.1%)
計	78 (46.2%)	21 (12.4%)	70 (41.4%)	169

28. スマートフォンにパスワードによるロックをかけていますか。

	はい	いいえ	計
はい	139	1	140(82.8%)
いいえ	16	13	29(17.2%)
計	155 (91.7%)	14 (8.3%)	169

32. スマートフォンにウイルス対策ソフトをインストールしていますか。

	はい	いいえ	分からない	計
はい	23	5	3	31(18.3%)
いいえ	11	35	10	56(33.1%)
分からない	21	29	32	82(48.5%)
計	55 (32.5%)	69 (40.8%)	45 (26.6%)	169

36. スマートフォンの GPS（位置情報）機能について知っていますか。

	知っている	知らない	計
知っている	154	3	157(92.9%)
知らない	8	4	12(7.1%)
計	162 (95.9%)	7 (4.1%)	169

39. スマートフォンで写真を撮る際に、GPS（位置情報）機能の設定はどうしていますか。

	オンにしている	オフにしている	必要に応じて変更している	分からない	計
オンにしている	4	3	0	2	9(5.3%)
オフにしている	1	89	4	5	99(58.6%)
必要に応じて変更している	1	5	0	1	7(4.1%)
分からない	1	34	2	17	54(32.0%)
計	7 (4.1%)	131 (77.5%)	6 (3.6%)	25 (14.8%)	169

16. 現在スマートフォンで使用している OS は何ですか。

	iOS（iPhone）	Android	計
iOS（iPhone）	130	2	132(78.1%)
Android	3	33	36(21.3%)
持っていない	0	1	1(0.6%)
計	134 (79.3%)	38 (22.5%)	169

22. （20 の質問で「はい」と答えた方）SNS を通じての嫌がらせ・迷惑行為などにあったことがありますか。

	はい	いいえ	計
はい	2	9	11(6.7%)
いいえ	3	149	152(92.1%)
未回答	0	2	2(1.2%)
計	5 (3.0%)	160 (97.0%)	169

26. スマートフォンの OS は最新のものにしていますか。

	はい	いいえ	分からない	計
はい	54	11	2	67(39.6%)
いいえ	26	18	4	48(28.4%)
分からない	29	2	23	54(32.0%)
計	109 (64.5%)	31 (18.3%)	29 (17.2%)	169

30. スマートフォンのウイルス感染について知っていますか。

	はい	いいえ	計
はい	24	1	25(14.8%)
いいえ	79	65	144(85.2%)
計	103 (60.9%)	66 (39.1%)	169

34. スマートフォンのウイルスに感染したことはありますか。

	いいえ	分からない	計
はい	1	0	1(0.6%)
いいえ	135	10	145(85.8%)
分からない	17	6	23(13.6%)
計	153 (90.5%)	16 (9.5%)	169

37. スマートフォンの GPS（位置情報）機能の設定はアプリによって変更していますか。

	変更している	変更していない	必要に応じて変更している	分からない	計
変更している	43	4	8	2	57(33.7%)
変更していない	12	6	3	4	25(14.8%)
必要に応じて変更している	18	3	12	3	36(21.3%)
分からない	15	4	8	24	51(30.2%)
計	88 (52.1%)	17 (10.1%)	31 (18.3%)	33 (19.5%)	163

付録2 確認テスト問題

1. どのような状況においても情報セキュリティ対策は大切なものです。次の中で正しいものはどれでしょうか。
   ア ウイルス対策ソフトの使用期限が切れた。ウイルス対策ソフトが動いていても、直ちに継続するためのライセンスを購入するか、新たに購入するかしなくてはならない
   イ 引っ越したばかりで、パーソナルファイヤーウォールもブロードバンドルータも持っていない。いずれかを購入するために短時間インターネットにつないだ
   ウ OSやソフトウェアへのパッチの適用は、手間がかかるので、毎年、年末にまとめて行っている
2. 適切なパスワードは情報セキュリティ対策の基本となります。パスワードについて、次の中で誤りでないものはどれでしょうか。
   ア 自分が応援しているサッカーチームの名前をパスワードにしている
   イ パスワードを紙に書いて鍵のかかる自分の引き出しにしまっている
   ウ 自分が使うパスワードは昔から統一して同じものを使い続けている
3. 受け取りたくない迷惑メールを減らすための対応として、次の中で誤っているものはどれでしょうか。
   ア 長くて分かりにくいメールアドレスを使う
   イ あらかじめ決めておいたメールアドレスやドメインからの電子メールしか受け取らないようにしておく
   ウ 電子メールを送ってきた人に返事を書いて、もう送ってこないように伝える
4. 自分が利用している銀行から「すぐに更新手続きを行ってください」というメールが届きました。その電子メールには、「リンクをクリックしてホームページを開き、お使いの銀行口座のIDとパスワードを入力してください」と書かれています。この場合に、次の中で正しいものはどれでしょうか。
   ア 自分の利用している銀行からの電子メールなので、リンクをクリックして、電子メールに書かれているとおりに銀行口座のIDとパスワードを入力する
   イ 本当に正しいメールなのかどうかがわからないので、電話帳や検索サイトなどでその銀行の連絡先を調べて連絡し、電子メールの内容が本当かどうかを確かめる
   ウ 詳細が分からないので、電子メールに書いてある連絡先に問い合わせる
5. ファイル共有ソフトを使う上での危険性の認識として、正しいものはどれでしょうか。
   ア 目的のファイルをダウンロードすると同時に自分のパソコンのファイルを公開するため、ウイルスなどに感染すると、気付かない間に公開して欲しくないファイルまで公開してしまう
   イ ウイルスが多く流通しているが、ファイル名やアイコンを確認することでウイルスかどうかは簡単に判別できる
   ウ 一旦流出してしまったファイルは取り消すことは簡単だが、流出したことに気付きにくいのが問題だ
6. 無線LANのセキュリティ技術について、次の中で正しいものはどれでしょうか。
   ア 電波は自分の家の中だけでなく、隣の家や近くの道路にまで届くこともある
   イ 無線LANを使うときはアクセスポイントを隠し、さらにMACアドレスをフィルタリングして接続できる機器を制限すれば、とりあえず不正に使われることはない
   ウ 暗号化は、多くの機器がサポートしているWEPが望ましい
7. ボットに関する説明として、次の中で正しいものはどれでしょうか。
   ア 画面の表示などですぐにわかるので、ボットに感染したとわかったときに駆除ソフトで駆除するか、OSを再インストールすれば良い
   イ 外部からの命令によって他のコンピュータへの攻撃などに利用される
   ウ ウイルス対策ソフトやウイルス対策サービスさえ利用していれば大丈夫だ
8. 知らない会社から「御見積書の送付」という件名で、添付ファイルとホームページへのリンクが付いた電子メールが送られてきました。この場合の対応方法として、次の中で誤っているものはどれでしょうか。
   ア 電子メールの添付ファイルを開いて、詳細を確認する
   イ 知らない会社から届いた電子メールなので、添付ファイルやリンク先は開かずに放っておく
   ウ どうすればよいか分からないので、情報システム担当者に来てもらい、実際に電子メールを見てもらう
9. 人間の心理的な隙などを突いて、情報を盗み出す手法を「ソーシャルエンジニアリング」と言います。ソーシャルエンジニアリングへの対策として、次の中で正しいものはどれでしょうか。
   ア 情報システム部から内線電話でパスワードの確認を受けたが、口頭ではパスワードは伝えないようにした
   イ 取引先の銀行から電子メールで「ホームページ上でIDとパスワードを入力するように」と記載されていたが、念のためその電子メールに記載されていた電話番号に確認した
   ウ パスワードなどを記載したメモを廃棄する場合には、誰にも見られないようにゴミ箱に捨てている
10. 個人情報や機密情報が保存されているコンピュータやメディアを廃棄するときの正しい方法はどれでしょうか。
   ア 自分の作成したファイルや電子メールのデータは、すべて“ごみ箱”に捨てた後で“ごみ箱”を空にした
   イ ハードディスクをフォーマットしてから廃棄した
   ウ データ消去用のソフトウェアを利用して、すべてのデータを消去した
11. 外部にノートパソコンを持ち出す場合のセキュリティ対策として、次の中で正しいものはどれでしょうか。
   ア 内部のハードディスクを正しく暗号化しておけば、ハードディスクを取り出されても、データを読み取られることはない
   イ コンピュータに正しくパスワードを設定しておけば、たとえノートパソコンの盗難にあってもハードディスクのデータを読み取られることはない
   ウ ノートパソコンの盗難にあわなければ、ハードディスクのデータを読み取られることはない
12. 持ち運び可能なUSBメモリの危険性と情報セキュリティ対策について正しいものはどれでしょうか。
   ア USBメモリを介して感染するウイルスがあるため、ウイルス感染を防ぐために携帯のデジタルオーディオプレーヤーにファイルを保存している
   イ 個人情報ファイルをUSBメモリに保存したが、不要になったので通常の消し方でファイルを削除した
   ウ 知り合いからファイルをUSBメモリで受け取ることになったが、USBメモリを接続するときにはウイルス対策しているコンピュータを使用する必要がある
13. 情報セキュリティポリシーは、企業や組織の情報資産を情報セキュリティ上のさまざまな脅威から守るために作成するものです。情報セキュリティポリシーについて、次の中で誤っているものはどれでしょうか。
   ア 企業規模によらず必要なものである
   イ 実施後は、当初の内容を変更してはならない
   ウ 情報資産を情報セキュリティ上の脅威から守るために不可欠なものである。
14. ウイルスの機能のうち、誤っているものを選びなさい。
   ア 自己伝染機能　　イ 感染機能　　ウ 潜伏機能
15. クラッカーの攻撃など、インターネットを通じて入ってくるものを防ぐしくみを何というか。
   ア セキュリティホール　　イ プロテクト　　ウ ファイアーウォール
16. 安全なホームページの見分け方として、間違っているものを選びなさい。
   ア 会社名、所在地、電話番号等が明記されている
   イ プライバシーポリシーが明記されている
   ウ URLの先頭に「https」が表示されている

17. プリンタやスキャナなどの周辺機器とパソコンをつなぐ接着剤のような役割を受け持つプログラムのことを何というか。正しいものを選びなさい。
　ア　ドライバファイル　　イ　cssファイル　　ウ　ネットワークファイル
18. ネットワークに接続されているコンピュータの場所を表わすゼッケン番号のようなものを何というか。正しいものを選びなさい。
　ア　IPアドレス　　イ　プロトコル　　ウ　URL
19. 「パブリシティーの権利」の説明として、正しいものを選びなさい。
　ア　商標を保護される権利のこと
　イ　芸能人や著名人、スポーツ選手などの氏名や肖像等を商業的に使用する場合の権利のこと
　ウ　人間の知的活動により生み出された概念や知識が財産として価値を有する場合に、その創作者だけ利用可能な権利のこと
20. ソーシャルエンジニアリングの対策として、誤っているものを選びなさい。
　ア　周囲に相談する　　イ　むやみに情報を書き込まない　　ウ　パーソナルファイアーウォールを利用する
21. 「不正アクセス」の種類として、誤っているものを選びなさい。
　ア　ウイルスメールの送信　　イ　なりすまし　　ウ　踏み台
22. ネットオークションにおけるトラブルを防ぐために、第三者的立場にある業者が、発送や代金の受け渡しなどを代行してくれるサービスのことを何というか。正しいものを選びなさい。
　ア　ホスティングサービス　　イ　サービスパック　　ウ　エスクローサービス
23. ネットワークを介してコンピュータに侵入し、ウイルス付のメールを大量にばらまく手法が典型的なウイルスを何というか。正しいものを選びなさい。
　ア　トロイの木馬　　イ　ボット　　ウ　ワーム
24. 新しく購入したスマートフォンの利用環境設定時に、情報セキュリティ対策として行うべき対応のうち、最適な選択肢はどれでしょうか。
　ア　ウイルス対策ソフトを導入する他、起動画面にもパスワード設定を行う
　イ　ウイルス対応ソフトは導入せず、起動画面にパスワードを設定する
　ウ　信頼できる製造メーカーの製品を購入しているため、特に対策は必要ない
25. スマートフォンに導入されている OS に情報セキュリティ上の欠陥が見つかりました。その情報セキュリティ対策として行うべき行動のうち、最も最適な選択肢はどれでしょうか。
　ア　ウイルス対策ソフトの更新を止める
　イ　OSの修正プログラム（セキュリティパッチ）を適用する
　ウ　情報セキュリティ上の欠陥を放置していても、インターネットの利用には問題ない
26. スマートフォンのOSやソフトウエアに発見された情報セキュリティ上の欠陥を修正せずに放置した場合に考えられる状況は、どの選択肢でしょうか。
　ア　ウイルス対策ソフトを導入していれば、情報セキュリティ上の欠陥を修正しなくてもウイルスに感染することはない
　イ　OSやソフトウエアに見られる情報セキュリティ上の欠陥は、対策を打たなくても時間の経過とともに自然と修復される
　ウ　ウイルス感染の危険性が増大する
27. スマートフォンに保存されている写真や動画がインターネット上に漏洩しないために、日ごろから注意すべき行動として、間違っている選択肢はどれでしょう。
　ア　ファイル共有ソフトを用い、不特定多数のコンピュータ間で様々なファイルを共有する
　イ　セキュリティ対策ソフトを導入する
　ウ　漏洩して困るファイルにはパスワードをかけておく
28. 家族や友人と写った写真や動画をインターネット上に公開するときの行動として、間違っている選択肢はどれでしょうか。
　ア　インターネット上に公開する写真などに写っている家族や友人から、その写真や動画を公開することの許可を得る
　イ　きれいに撮れた写真なので、インターネット上にすぐに公開する
　ウ　ブログなどの日記に掲載する写真は、公開しても困らないようなものを選択して掲載する
29. SNSやブログの利用に関して、情報セキュリティの観点から間違っている選択肢はどれでしょうか。
　ア　SNSやブログで知り合った人との交流を広げるためにも、自分のプライバシー情報は積極的に公開して、相手から信頼を受けるようにしている
　イ　友人を名乗る不審なメッセージが届いたときは、本人から直接得ている連絡先に確実に確認を行うよう配慮している
　ウ　ブログなどの日記に掲載する写真は、公開しても誰も困らない写真を選択して掲載する
30. スマートフォンを通じてSNSやブログに情報を公開することに関して間違っている選択肢はどれでしょう。
　ア　スマートフォンで撮影した写真には、位置情報が記録されている場合もあるので、居場所の情報が知られたくない場合は、位置情報の設定を加工して知られないように取り扱うことにしている
　イ　SNSやブログのプロフィールで公開する情報は、誰に見られてもいいように取捨選択している
　ウ　街中でスマートフォンで撮影した写真に他人が写っている場合、自分とは関係のない人なので、特に配慮することなく公開しても問題はない
31. 紛失したら困る重要な情報が保存されたスマートフォンを持って外出する時、情報セキュリティ対策上、注意すべきこととして間違っている選択肢はどれでしょうか。
　ア　機器の紛失や盗難を防ぐために、貴重品を扱うのと同様に、常に所在を意識した行動をする
　イ　パスワード設定をしておく
　ウ　重要な情報を持っていることを周りに気づかれないよう、持っていることを忘れて、平常通りの行動をする。
32. 外出先で無線LANに接続してインターネットを利用する場合のセキュリティに関する注意として間違っている選択肢はどれでしょう。
　ア　パソコンのファイアウォール機能を有効にしておく
　イ　電波を利用した通信形態をとる無線LANは盗聴される心配はない
　ウ　漏洩して困るような情報のやり取りや、金銭取引を行わないようにしている