

# [研究論文] スマートフォンのセキュリティ意識・知識・行動 ——大学生へのアンケート調査を通じて——

渡邊信吾<sup>1</sup>・三浦直子<sup>2</sup>

1 工学部機械工学科平成 26 年度卒業生

2 基礎・教養教育センター

## Study of Security Consciousness, Knowledge, and Behavior on a Smart Phone: Questionnaire survey for students

Shingo WATANABE<sup>1</sup>, Naoko MIURA<sup>2</sup>

### Abstract

We conducted a questionnaire survey to students about the security consciousness, knowledge, and behavior on a smart phone. Though we considered that there might be relations among them, there are no relations as a result of survey. On the other hand, it becomes clear that a student's gender influences the security knowledge and the behavior on SNS, and that the faculty to which a student belongs influences the security consciousness and the attacker or victim experiences. Moreover, a student's "behavioral patterns", such as a practical use of functions on a smart phone and a participating situation to SNS, affects to the behaviors on SNS and to the attacker or victim experiences. The Social attribution such as gender and a faculty and the usual "behavioral pattern" on a smart phone influence whether a student behavior is safe or risky, rather than the security consciousness and knowledge. Therefore, we propose that a suitable "training (experience study)" for each social attribution is more effective in the security countermeasures on a smart phone than a lecture.

Keywords: Security, Consciousness, Knowledge, Behavior, Smart phone, SNS, Countermeasures.

### 1. 研究目的

2008 年に Softbank が国内初 iPhone を販売して以来、日本におけるスマートフォンの普及率は急増している。ビデオリサーチインタラクティブ社が 2014 年 2 月に実施した調査によれば、生徒や学生のじつに 8 割が、スマートフォンを所有している<sup>1)</sup>。旧来の携帯電話（ガラパゴス・ケータイ）<sup>2)</sup>とは異なり、機能やデザインの面で飛躍的な進歩を遂げたスマートフォンは、パソコンに近い機能を持っている。タッチパネルによって直感的に操作できるだけでなく、インターネットとの連携を強めて多種多様なアプリをダウンロードし最新の機能へと拡張できるようになったスマートフォンは、SNS 上で人々と幅広い交流をしたり、気軽にソーシャル・ゲームやネットショッピングを楽しんだり、音楽や動画を鑑賞したりすることを可能にし、人々に支持されて急速に普及してきた。

他方で、パソコンに匹敵する構造と機能をもつスマート

フォンが身近となり、誰でも簡単かつ気軽に使用できるようになったことから、パソコンだけではなくスマートフォンにおいても、ウィルス感染や不正アクセス、個人情報の流出といった被害件数が増加してきている。パソコンは人々の生活に普及して久しく、学校でも情報セキュリティ教育に力が入れられてきた。それゆえ、セキュリティ対策ソフトを利用する人も多く、セキュリティに関する利用者の知識や意識も比較的高いといえる。他方で、パソコンと同様の機能を持ち合わせているスマートフォンは、従来の携帯電話（ガラパゴス・ケータイ）に代わって人々の間に急速に普及したものの、ガラパゴス・ケータイよりも遥かにウィルス感染や不正アクセスなどの被害にあう確率が高まっている。なかでも、twitter や facebook、LINE など、SNS 上の被害が注目されている。スマートフォンから SNS を閲覧・投稿することが手軽になったこともあり、社会的な影響を考慮せずに悪ふざけ画像や反社会的な文章を投稿し、個人情報の流出やネット炎上に発展するなど、注目

を集めている。2013 年の春から夏にかけて、twitter 上で「バカッター」「バイトテロ」と呼ばれた事例が、ネットのニュース記事だけでなく、テレビや新聞でも大きく報道されたことは記憶に新しい。独立行政法人情報処理推進機構によれば、2014 年 3 月の時点で、スマートフォンに関する被害届件数は、じつに 1,414 万件にも上っているという<sup>3)</sup>。また、2014 年の秋から冬にかけては、LINE や twitter のアカウントが乗っ取られたりするなどの事件も増加して、話題となった。

国内での販売開始後、わずか数年の間に急速に普及したスマートフォンは、新たに、上記のようなセキュリティの危機をもたらしている。そこで、こうした危機的状況のなかで、スマートフォンを保有する大学生は、どのようなセキュリティ意識や知識を持ち、安全または危険な使用をしているのか調査し分析をすることが、本研究の目的である。

## 2. 調査の概要

### 2.1 調査内容

本研究では、最初に文献調査を行い、スマートフォンの歴史と現状、及び今日のサイバー犯罪と既存のセキュリティ意識の研究動向を把握した<sup>4)</sup>。

そこから、スマートフォンのセキュリティに関する意識・知識・行動には相互に関連性があるのではないかという仮説を立てた。すなわち、セキュリティ意識の高い利用者は、セキュリティに関する知識が豊富であり、それゆえ安全な使い方をして、被害から守られているのに対して、セキュリティ意識が低い利用者は、セキュリティに関する知識も乏しく、それゆえ危険な使い方をしてしまい、被害を受けてしまうのではないか、という仮説である。

次に、大学生を対象としてスマートフォンのセキュリティに関する意識・知識・行動相互の関連性や、それらに影響を及ぼす他の要因を調べるために、アンケート調査を実施した。本論文では、このアンケート調査の分析結果と考察を論じる。

### 2.2 調査対象の限定について

なお、調査対象を大学生に限定したのは、セキュリティに関する意識・知識・行動を比較し、仮説を検証するためである。社会人の場合は、既婚か未婚か、有職か無職か、子供の有無や子供の年齢など、各自の属性によってスマートフォンの使用に大きな偏りが生じると予想されるため、仮説検証の対象とすることが難しいのではないかと考えた。また、小中高の生徒では、所有率が大学生ほど高くはなく、学校や家庭の指導下にあるため、スマートフォンの使用やセキュリティ知識に関する回答の多様性が相対的に低いことが予想され、同様に仮説検証の対象とすることが難しいと懸念されたためである。

本研究では、このような世代による影響を制御すべく、年齢や生活環境が比較的近似した、首都圏の大学生を調査対象として設定することとした。

## 2.3 調査方法

2014 年 12 月下旬に、神奈川県厚木市と東京都豊島区に所在する私立大学 2 校において、クラス（授業教室）単位の集団自記法を採用した。（県内の理系大学では情報系・工学系の学生が履修する 3 クラスに、都内の総合大学では社会系の学生が履修する 2 クラスに調査協力を依頼した。また、学科系列の偏りを修正するために、都内・県内の総合大学・文系大学に通う友人の協力を得て、人文系の学生へも調査を依頼した。）大学生 250 名に調査票を配布し、238 名から有効回答を得た（回収率 95.2%）。このうち、「スマートフォンを所有している」と回答した 223 名の調査票の集計結果について、本論文で分析し考察する<sup>5)</sup>。

意識や行動を尋ねるという質問内容の性質上、回答の大半は（数量データではなく）カテゴリカル・データとなった。そこで、要因間の関連性を分析するために、クロス集計してカイ二乗検定を行った。

## 3. アンケート調査の結果と考察

### 3.1 単純集計の結果と考察

最初に、質問票（アンケート用紙）に記載された質問項目の順番に従って、回答の単純集計の結果について考察したい。なお、グラフは次頁に掲載する。

#### (1) スマートフォンの機能の利用状況

図 1 は、スマートフォンでどのような機能を利用しているかについて（複数回答）、多い順に並べ替えた横棒グラフである。また、これらのなかで一番よく利用する機能を尋ねた質問では、SNS が 45%、次いでインターネット接続が 24%、ゲームやビジネスツール等のアプリケーションが 23%、通話・メールが 5%、動画鑑賞が 4%、その他が 1%となった。また、利用する機能の数では、3 つが 35%、4 つが 24%、2 つが 15%、5 つが 12%、6 つが 11%、1 つが 5%となっており、全体を平均すると 3.61 の機能を利用しているという結果となった。（以下、クロス集計の際には、スマートフォンで利用する機能の数を、使いこなしの指標「利用度」として、3 つに再コード化し分析する。）

#### (2) スマートフォンのセキュリティ意識

図 2 は、スマートフォンに関するセキュリティ意識を尋ねた質問（複数回答）を、回答者が多い順に並べ替えた横棒グラフである。それぞれ「Web 登録した住所やクレジットカードなどの情報が流出してしまわないか心配だ」「友人が自分の情報（名前、大学名、写真など）を SNS へ投稿すると不快に感じる」「自分で SNS に投稿・公開した情報を見られても、やましいことはないので平気だ」「万が一スマートフォンの中身を見られても、やましいことはないので平気だ」「スマートフォンのセキュリティに気をつけないとトラブルになることがあると言われても、あまり実感がわからない（自分には関係がないように感じる）」「スマートフォンを落としても、ちゃんとロックをかけて

いるので安心だ」という質問文のキーワードを掲載している。スマートフォンのセキュリティ意識の鋭敏さを基軸に、質問項目のプラス・マイナスを調整した意識スコアを6点満点とすると、平均は4.02点となった。

### (3) スマートフォンのセキュリティに関する知識

図3は、スマートフォンのセキュリティに関する知識を尋ねた質問（複数回答）を、回答者が多い順に並べ替えた横棒グラフである。それぞれ「Web 登録したパスワードが単純だと個人情報盗まれることがあると知っている」「LINE のアカウントが乗っ取られる事件があったことを知っている」「なくしたスマートフォンが使われないように、遠隔操作でロックできることを知っている」「アプリをダウンロードするときに、電話帳や画像などへのアクセスを許可すると、自分の電話帳や画像などの個人データがアプリ企業に収集されることを知っている」「スマホ専用のウィルス対策ソフトがあることを知っている」「韓国政府が LINE を傍受し、通話やメールのデータを収集して保管し分析していることを知っている」という質問文のキーワードを掲載している。スマートフォンのセキュリティに関する知識スコアを6点満点とすると、平均は3.97点となった。

### (4) スマートフォンにおける加害経験・被害経験

図4は、スマートフォンにおける実際の加害経験や被害経験を尋ねた質問（複数回答）を、回答者が多い順に並べ替えた横棒グラフである。「誹謗中傷」の加害経験が15%であるのに対して、被害経験は20%と増加しているのは、加害者が多数の被害者を誹謗中傷する場合と、加害者が無自覚のまま誹謗中傷している場合（被害者にとっては誹謗中傷と受け止められるが、加害者本人は誹謗中傷したつもりはないというケース）が考えられる。逆に、「アカウント乗っ取り」では、加害経験が5%なのに対して、被害経験が4%と減少している。これは、加害経験を問うのに「乗っ取ろうと試みたことがある」と尋ねているのに対して、被害経験では「乗っ取られたことがある」と質問しており、そのため加害行動を試してみたが成功しなかった（ログインできなかった）ケースが含まれるためと推測される。なお、加害経験の質問項目のなかに「無断投稿」を加えなかったのは、悪意をもって罵倒するような「誹謗中傷」とは異なり、（意図的に晒し上げているというよりも）無自覚に友人の情報を漏えいさせている場合には、自らの加害性を意識しづらいと想定されたためである。参考までに、旅行時の SNS への画像投稿を尋ねた別の質問（複数回答ではなく、一番近い選択肢を1つだけ回答するという様式）では、SNS 上へ旅行時の投稿をする際に、一緒に旅行へ出掛けた友人の氏名を人物画像とともに投稿する（いわば、悪意のない・無自覚な「無断投稿」が常習化している）という回答が、全体の1割弱（9%）に上っていたことを指摘しておきたい。「誹謗中傷」の自覚的な加害経験が15%だったのに対して、その被害経験は20%であることを鑑

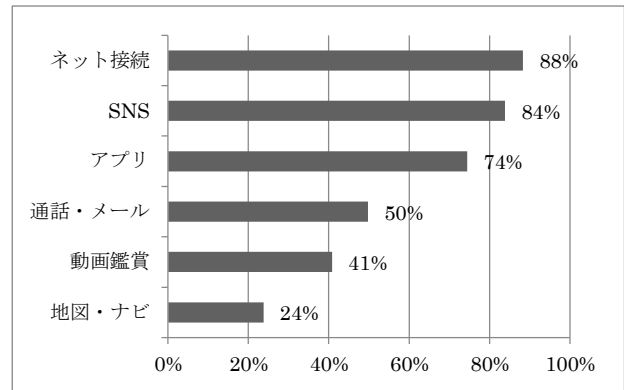


図1 スマートフォンの機能の利用状況（複数回答）

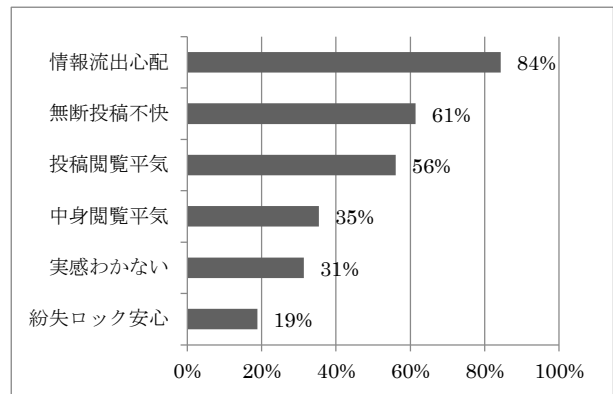


図2 スマートフォンのセキュリティ意識（複数回答）

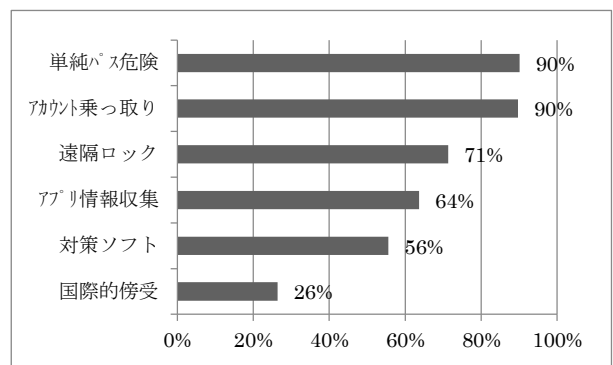


図3 スマートフォンのセキュリティ知識（複数回答）

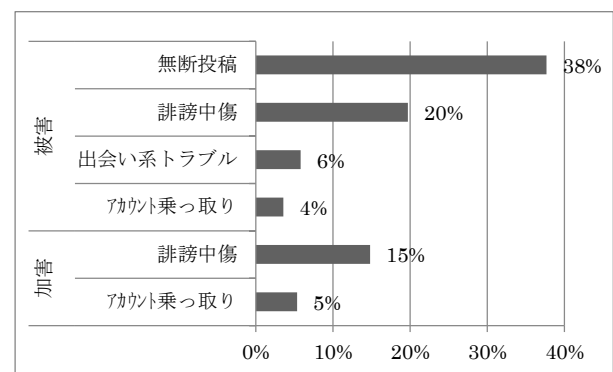


図4 スマートフォンの加害経験・被害経験（複数回答）

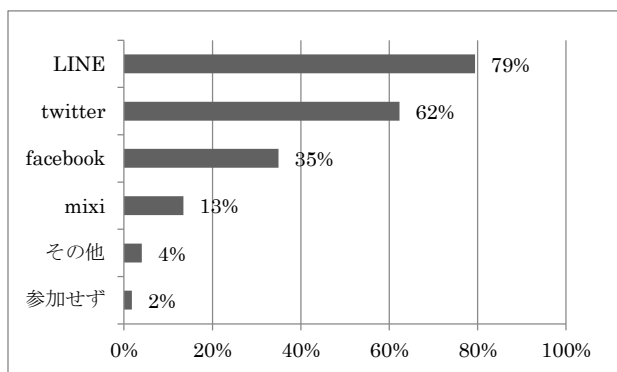


図5 スマートフォンからのSNS参加状況（複数回答）

みると、「無断投稿」の被害経験が38%にも上っていることから、実際には30%前後の人々に加害経験があるだろうと想定される。

#### (5) スマートフォンからのSNSへの参加状況

図5は、スマートフォンから参加しているSNSについて尋ねた質問（複数回答）を、回答者が多い順に並べ替えた横棒グラフである。また、これらのなかで一番よく参加しているメインのSNSを尋ねた質問では、LINEが71%、twitterが28%、facebookやmixiを含むその他が1%という回答を得た。さらに、参加しているSNSの数に注目すると、2つが40%、3つが28%、1つが15%、4つが14%、SNSに参加していないが2%、5つ以上が1%で、全体で平均すると2.39（参加していない人も含む平均）、SNSへの参加者のみに限定した平均では2.45という結果となった。加えて、これらのSNSのうち、1つでも本名で参加しているものがあるかどうか（本名参加SNSの有無）について尋ねたところ、「ある」が71%、「ない」が29%と、約3割が匿名に徹してSNSに参加していることが明らかとなった。（以下、クロス集計の際には、参加しているSNSの数を、web上での社交の指数「SNS参加数」として、4つに再コード化し分析する。）

### 3.2 クロス集計の結果と考察・その1：

#### 仮説の検証と影響する要因の探索

前述のとおり、スマートフォンのセキュリティに関する意識・知識・行動には相互に関連性があるのではないかという仮説を検証するために、クロス集計を行い、その割合を比較する。しかし、横棒グラフで関連性が表れたように見えても、偶然に本調査の回答者においてそのような結果が生じたという可能性が残る。例えば、セキュリティ意識の高いグループの7割は知識も多く、意識の低いグループで知識が多いのは1割だけの場合、意識と知識の間には関連性があるということができたとして、では、セキュリティ意識の高いグループの7割は知識も多いが、意識の低いグループでも5割が知識も多い場合はどうだろうか。わずかな差であれば、そこには統計的な有意差があるというよりも、今回の調査でたまたま偶然に差が出ただけかもしれ

れない。回答者を変えれば、今回とは全く異なる結果が得られるかもしれない。

そこで、母集団においても有意な差があるかどうかを調べるために、「AとBとは統計的に独立である（AとBの間には関連性がない）」という帰無仮説を立て、これを棄却することで対立仮説（AとBの間に関連性がある）の正しさを支持するという検定の手順を取る。クロス集計から算出したカイ二乗の統計量が十分に大きな値でなければ、帰無仮説を棄却することができず、AとBとの間に有意差がある（関連性がある）とはいえない。逆に、カイ二乗の統計量が十分に大きければ、帰無仮説を棄却し、対立仮説を採択することができる<sup>6)</sup>。本論文では、カイ二乗検定の有意水準を5%未満（ $\alpha < 0.05$ ）に設定し、カイ二乗値は四捨五入して小数点第3位まで求めることとする。（なお、クロス集計の際、 $2 \times 2$ 表すなわち自由度  $df=1$  の実際のカイ二乗の値は、カイ二乗分布よりも大きな平均と分散をもつため、イエーツの連続性の修正を施し、カイ二乗分布に近い分布をとる統計量を計算することとする<sup>7)</sup>。）

#### (1) セキュリティ意識・知識・行動の関連性の検証

仮説を検証すべく、クロス集計に基づき検定を行った。意識の指標には、スマートフォンのセキュリティ意識の鋭敏さを基軸に、質問項目のプラス・マイナスを調整した意識スコア（6点満点）を求めて、3段階（高中低）に再コード化した「意識度」を、知識の指標には、スマートフォンに関わるセキュリティの知識を尋ねた知識スコア（6点満点）から3段階（高中低）に再コード化した「知識度」を用いている。また、セキュリティに関する行動の指標として、「加害経験」（2つの加害行動を尋ねた質問項目のうち、いずれか1つまたは両方に該当したもの）、「被害経験」（4つの被害体験を尋ねた質問項目のうち、1つ以上に該当したもの）、そして旅行をした際に想定されるSNSへの「画像投稿」（位置情報を付して画像を投稿、人物画像と氏名を投稿、食べ物の画像のみ、風景の画像のみ、画像は投稿しない）と、その「公開範囲」（全員に公開、フォロワーに公開、一部のフォロワーを選んで公開、公開せず）という4つを設定した。

まず、意識度×知識度を集計し検定してみると、自由度  $df=4$ 、棄却値=9.488 に対して、算出されたカイ二乗値  $\chi^2=8.237$  と、設定した有意水準に満たなかった。

次に、意識度×加害経験、意識度×被害経験について見てみると、ともに自由度  $df=2$ 、棄却値=5.991 に対して、算出されたカイ二乗値は、加害経験の  $\chi^2=0.159$ 、被害経験の  $\chi^2=1.709$  と、いずれも有意水準に遠く及ばなかった。さらに、意識度×画像投稿では、自由度  $df=8$ 、棄却値=15.507 に対し、算出されたカイ二乗値は  $\chi^2=5.527$  となり、また意識度×公開範囲でも、自由度  $df=6$ 、棄却値=12.592 に対して、算出されたカイ二乗値は  $\chi^2=10.573$  と、いずれも有意水準に満たなかった。

同様に、知識度×加害経験、知識度×被害経験についても、ともに自由度  $df=2$ 、棄却値=5.991 に対して、算出



されたカイ二乗値は、加害経験の  $\chi^2=0.394$ 、被害経験の  $\chi^2=4.466$  と、いずれも有意水準に満たなかった。さらに、知識度×画像投稿では、自由度  $df=8$ 、棄却値=15.507 に対して、算出されたカイ二乗値  $\chi^2=13.098$  と有意水準に及ばず、知識度×公開範囲では、自由度  $df=6$ 、棄却値=12.592 に対して、算出されたカイ二乗値  $\chi^2=9.246$  と、いずれも有意水準に満たなかった。

以上の検定結果から明らかとなったのは、当初に設定した仮説に反して、セキュリティに関する意識・知識・行動の間には、相互に関連性があるとはいえない(いずれも有意水準に満たないため、帰無仮説が棄却できない)ということである。一般的に考えられているように、また学校や企業といった組織内におけるセキュリティ対策の暗黙の前提となっているように、セキュリティに関する知識が増えればセキュリティ意識が高まり、セキュリティ意識が高まれば安全な行動を取る——というような、直接的な関係を調査結果に見出すことはできなかった。言い換えれば、セキュリティ意識・知識・行動には、それぞれ別の異なる要因が影響していると考えられる。

それでは、具体的にどのような要因が関係しているのだろうか。仮説モデルを修正すべく、その他の要因についてクロス集計し検定をした結果のうち、有意水準を満たした(関連性に有意差が算出された)ものに限定して、以下に掲載する。

## (2) 性別が及ぼす影響

社会学のジェンダー研究において、一般的に人々の意識・知識・行動には男女差が見られることが広く知られている。そこで、最初に性別とのクロス集計を試みた。図は次頁にまとめて掲載する。

性別×知識度を集計し検定してみると、自由度  $df=2$ 、棄却値=5.991 に対して、算出されたカイ二乗値  $\chi^2=8.334$  と、有意差が認められた。知識スコアの平均は、男性が 4.02 点、女性が 3.74 点であったが、図 7 から分かるとおり、男性は知識度の低いグループで女性の約 2 倍の人数がいるが、知識度の高いグループでも 1.5 倍近くいることから、知識は高低に偏る傾向が見られる。対して、女性では、中間的な知識度をもつグループが全体の 6 割以上を占めるという同質性が見て取れる。(他方で、既存のジェンダー研究における知見とは対照的に、図 6 の性別×意識度のグラフで有意差が認められなかったことは、大変興味深い。セキュリティ意識には、性別以外の要因が影響すると想定される。)

また、性別と SNS 上での行動との間にも、関連性を見出すことができた。性別×画像投稿は、自由度  $df=4$ 、有意水準を 5%未満よりも厳しい 1%未満 ( $\alpha < 0.01$ ) に設定しても、その棄却値=13.277 に対して、算出されたカイ二乗値  $\chi^2=14.192$  と、有意差が認められた(図 8)。性別×公開範囲では、自由度  $df=3$ 、有意水準をさらに厳しく 0.01%未満 ( $\alpha < 0.0001$ ) と設定しても、その棄却値

=21.108 に対して、算出されたカイ二乗値  $\chi^2=25.088$  と、有意差が認められた(図 9)。これら 2 つの図からわかることは、男性は SNS を全員に公開する、すなわち不特定多数に向けて投稿する割合が高いため、投稿する画像も「景色のみ」や「投稿せず」といった個人情報に配慮したものが多くなったと考えられる。対して、女性では位置情報を開示したり、名前と人物画像を載せたりといった、比較的個人情報に関わる内容を投稿する回答が相対的に多いのは、女性は 6 割前後がフォロワーに向けてのみ公開している(投稿を読まれたくない相手はフォロワーから外すといった対策も講じられる)といった安心感からではないかと想定される。

## (3) 学科系列が及ぼす影響

性別という回答者の属性によって知識や行動に関連性が見出されたため、次に、所属する学科系列(情報系、工学系、社会系、人文系)によってセキュリティ意識・知識・行動に関連性が見られるか、クロス集計し検定を行った。図は、次頁にまとめて掲載する。

学科系列×意識度では有意差が算出された。図 10 は学科系列×意識度のグラフであり、自由度  $df=6$ 、棄却値=12.592 に対して、算出されたカイ二乗値  $\chi^2=12.993$  であった。回答者が所属する学科系列は、悲観(心配・不安)や楽観(平気・安心)といったセキュリティ意識(意識度)に影響を及ぼしている。技術の発展に信頼をおく工学系が比較的楽観的で(意識スコアの平均が 3.74 点と一番低く)、情報技術に関する専門知識をもつ情報系と、逆に情報技術から学科の専門分野が一番かけ離れた人文系が、それゆえかえて警戒心が強くなるのか、比較的悲観的(意識スコアの平均がそれぞれ 4.27 点、4.10 点と高め)であり、社会系がそれに続く(平均が 3.83 点)という結果になった。

対して、性別とは対称的に、学科系列×知識度では、5%の有意水準にわずかに満たなかった(図 10)。ここでもまた、理系はセキュリティの知識が多く、文系は少ないという一般的な想定とは反対の結果となった。知識の多いグループだけを見れば、想定通り理系と文系とで差が認められたものの、セキュリティに関する知識の少ないグループが工学系のなかでかなりの割合を占めていることが、その原因ではないかと考えられる。

次に、学科系列と SNS 上での行動について調べた。学科系列×画像投稿は、自由度  $df=12$ 、棄却値=21.026 に対して、算出されたカイ二乗値  $\chi^2=21.676$  と、有意差が認められた(図 12)。また、学科系列×公開範囲でも、自由度  $df=9$ 、棄却値=16.919 に対して、算出されたカイ二乗値  $\chi^2=20.306$  と、有意差が認められた(図 13)。しかし、これらに関しては解釈に注意が必要である。図 12 と図 8(性別×画像投稿)、また図 13 と図 9(性別×公開範囲)とを比較すると、理系(情報系・工学系)と男性、文系(社会系・人文系)と女性の回答傾向が非常に似通っていることが見て取れる<sup>8)</sup>。理系には男性が多く、文系には女性が多く進学していることから、また(帰無仮説を棄却

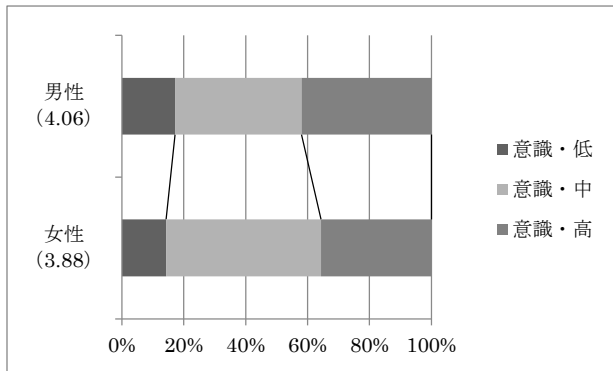


図 6 性別 × 意識度 (α &gt; 0.55 : 有意差なし)

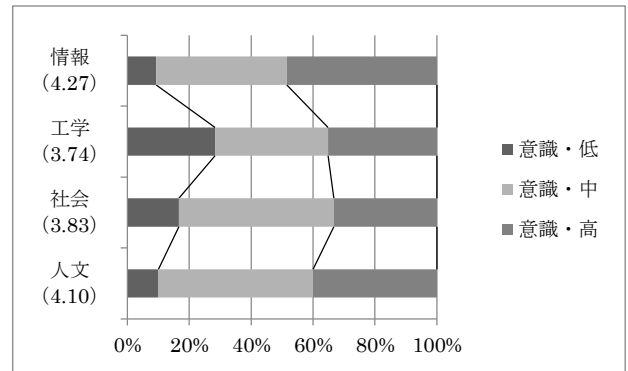


図 10 学科系列 × 意識度 (0.01 &lt; α &lt; 0.05)

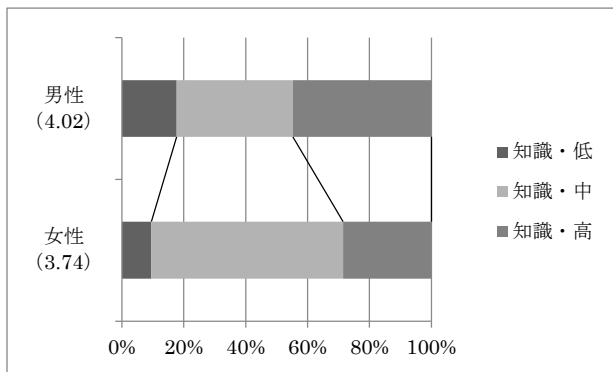


図 7 性別 × 知識度 (0.01 &lt; α &lt; 0.05)

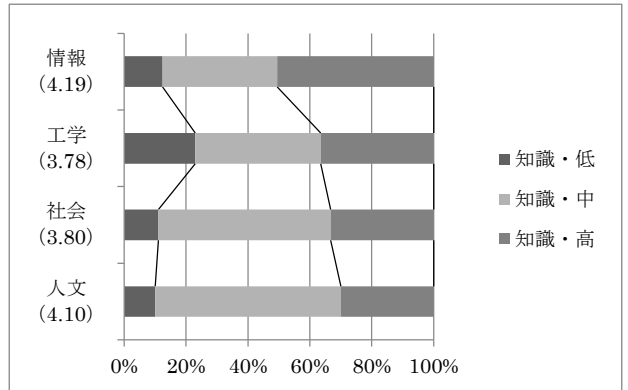


図 11 学科系列 × 知識度 (α &gt; 0.1 : 有意差なし)

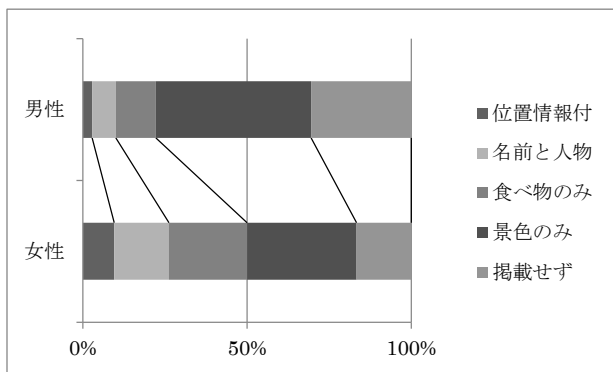


図 8 性別 × 画像投稿 (α &lt; 0.01)

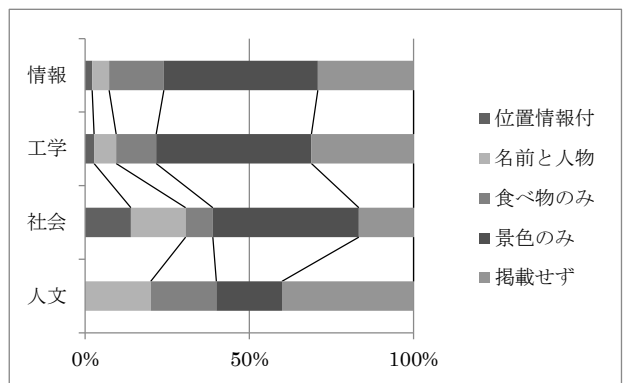


図 12 学科系列 × 画像投稿 (0.01 &lt; α &lt; 0.05)

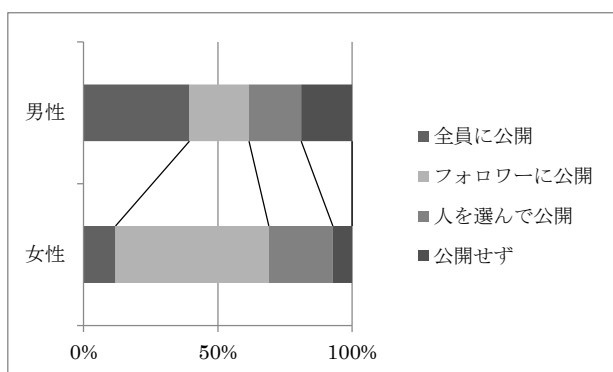


図 9 性別 × 公開範囲 (α &lt; 0.0001)

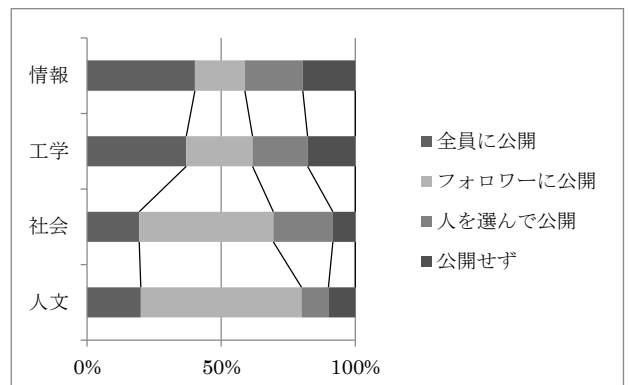
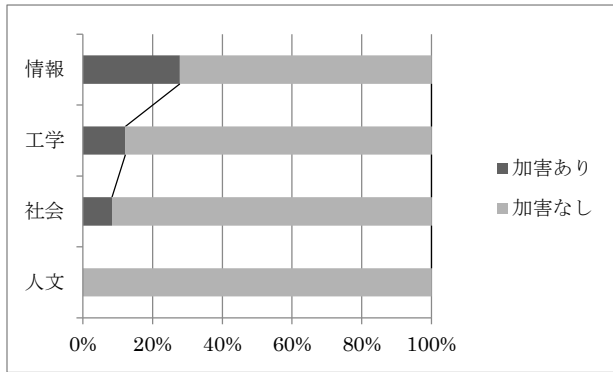
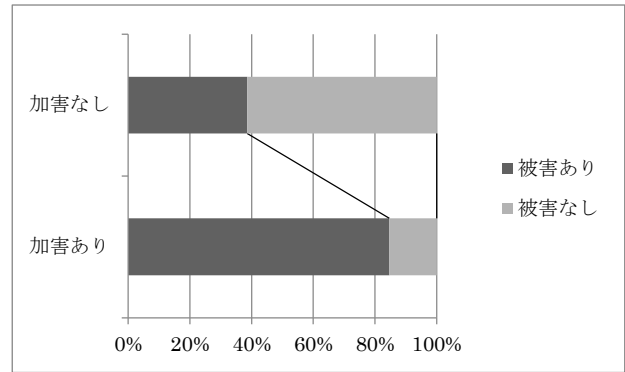
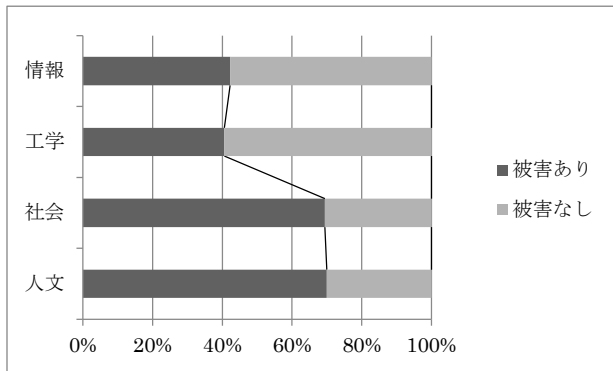
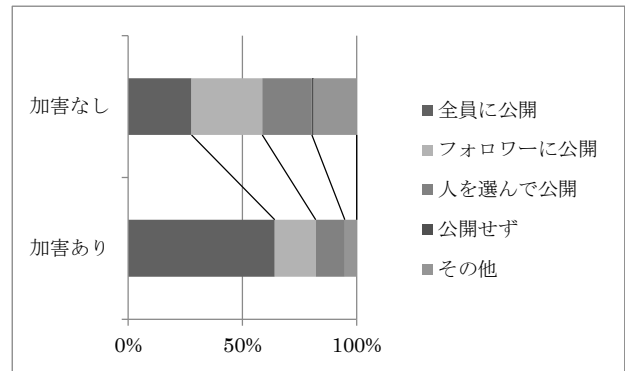


図 13 学科系列 × 公開範囲 (公開範囲 (0.01 &lt; α &lt; 0.05))

図 14 学科系列×加害経験の有無 ( $\alpha < 0.01$ )図 16 加害経験の有無×被害経験の有無 ( $\alpha < 0.000005$ )図 15 学科系列×被害経験の有無 ( $\alpha < 0.01$ )図 17 加害経験の有無×公開範囲 ( $\alpha < 0.001$ )

する有意水準を満たしているとはいえず、性別と比べて学科系列の危険率  $\alpha$  のほうが相対的に大きいことから、擬似的な関連性が算出された可能性にも配慮する必要がある。つまり、性別が SNS 上の行動に強い影響を及ぼし、また性別によって進学する学科系列が影響される場合、本来は両者に及ぼされる「性別の影響」の反映に過ぎないにもかかわらず、学科系列と SNS 上の行動との間に擬似的な関連性を見て取ってしまうという可能性を排除しきれないことを念頭において、結果の考察を慎重に行う必要がある。(擬似的な関連性なのか、独立した影響なのかを検定するためには、多重クロス集計等による詳細な検定が必要であるが、ここではその可能性を指摘するにとどめたい。)

また、学科系列×加害経験 (図 14)、学科系列×被害経験 (図 15) では、いずれも自由度  $df=3$  で、有意水準を 1% 未満 ( $\alpha < 0.01$ ) に設定しても、その棄却値=11.345 に対して、算出されたカイ二乗値は、それぞれ  $\chi^2=12.555$ 、 $\chi^2=11.485$  と、有意差が認められた。この結果は、大変興味深い。というのも、前述したとおり、知識度×加害経験、知識度×被害経験では有意差が算出されなかったにもかかわらず、上記で知識度と関連性が見出された学科系列と加害経験・被害経験について検定したところ、関係性が見出されたからである。このことから、単にセキュリティに関する知識の多少ではなく、どのような学科系列に所属しているのかが、加害行動・被害体験に影響を与えるということが明らかとなった。言い換えれば、(加害に関する知識を含む) 多くの知識を持つ個人がいたとしても、所属

する学科系列が実際の加害行動の有無(実行へ移すか/移さないか)に影響を及ぼすということである。それはまた、セキュリティに関する知識の多少とはあまり関係なく(知識があっても/なくても)、所属する学科系列によって、被害を受けやすい/受けにくいといった傾向が見出されるということもできる。ここから、所属する学科系列に応じた行動傾向や行動規範(例えば、加害するという好奇心を抑えるべきか/好奇心から実行してみるべきか等)の存在を、いわば集団的な行動様式の存在を想定することができるかもしれない。(この点に関しては、次節「3.3 クロス集計の結果と考察・その2」でさらに考察を深めたい。)

#### (4) 加害経験と被害経験の影響

加害経験×被害経験をクロス集計し、2×2 表のためイエーツの連続性の修正を施して検定したところ、自由度  $df=1$  で、求められるカイ二乗値  $\chi^2=25.576$  と算出されたが、これは有意水準を 0.00005% と極めて低く設定した際の棄却値=25.264 をも満たしている。上記の図 16 に表れているように、加害経験と被害経験には強い関連性があり、加害経験のある人の 8 割以上が、被害経験もあるという結果となった。これらのグループでは、被害を受けることで、加害の手口や経路などを知ってしまい加害行動に興味を持ったり、やられたからやり返したりしたのかもしれない。いずれにせよ、加害者は同時に被害者でもあり、先にどちらの立場にあったにせよ、リスクの高い行動と馴れ親しんでいるグループだと考えられる。

また、前出の学科系列が、加害経験と被害経験の両方に関連していたのに対して、SNS 上の行動との関係に注目すると、加害経験×公開範囲のみ有意差が算出された(図 17)。自由度  $df=4$  で、0.01%の有意水準の棄却値=18.467 に対して、カイ二乗値  $\chi^2=19.628$  と、関連性が認められた。先ほど、加害グループはリスクの高い行動と馴れ親しんでいるという考察を述べたが、公開範囲においても、加害経験のないグループと比較して、SNS を不特定多数へ公開しネット上の多様な人々と交流するという行動様式を身につけている割合が非常に高い(およそ 2.5 倍)ということが見て取れる。

#### (5) 利用度と SNS 参加数の影響

前節「単純集計の結果と考察」で言及した、調査票で尋ねた質問項目のうち、スマートフォンの多彩な機能の利用状況を再コード化した「利用度」と、スマートフォンからの SNS 参加状況を再コード化した「SNS 参加数」を、セキュリティ意識・知識・行動とクロス集計し検定を行ったところ、複数の項目で有意差が算出された。

利用度に関しては、知識度および公開範囲で関連性が認められた。利用度×知識度では、自由度  $df=4$ 、0.05%の有意水準の棄却値=14.860 に対して、カイ二乗値  $\chi^2=17.118$  と有意水準を満たした。図 18 から分かることは、利用状況にかかわらず、知識度の高い人々の比率は 4 割前後と変わらないが、利用する機能が多いグループでは、知識度の低い人々が、他の利用度のグループと比べて 3 倍に急増している点である。同様に、利用度×公開範囲でも、自由度  $df=6$ 、1%の有意水準の棄却値=16.812 に対して、カイ二乗値  $\chi^2=19.042$  と有意水準を満たした。図 19 を見ると、利用する機能が多くスマートフォンを使いこなすグループほど公開対象が広い様子が、よく分かる。

次に、SNS 参加数について見てみると、画像投稿、公開範囲、被害経験という行動に関する質問項目と関連性が認められた(加害経験、および意識度や知識度とは、有意水準に満たなかった)。SNS 参加数×画像投稿では、自由度  $df=12$ 、0.01%という厳しい有意水準の棄却値=32.909 に対して、カイ二乗値  $\chi^2=34.327$  と有意水準を満たした。図 20 では、参加している SNS の数が増加するほど、個人情報を開示する傾向がよく見て取れる。また、SNS 参加数×公開範囲について算出したところ、カイ二乗値  $\chi^2=40.079$  となり、自由度  $df=9$  の有意水準 0.0005%の棄却値=35.431 をも満たしている。図 21 を見ると、SNS 参加数が増加するに従って、「人を選んで公開」「公開せず」が減少し、「全体に公開」「フォロワーに公開」の比率が増加している。最後に、SNS 参加数×被害経験では、カイ二乗値  $\chi^2=19.008$  と算出され、自由度  $df=3$  の有意水準 0.005%の棄却値=17.730 をも満たしている。図 22 では、SNS 参加数が複数になった途端に、被害経験者の割合が 2 倍以上に跳ね上がっている。参加する SNS 数を 1 つと回答した人の多くが LINE を挙げていることから、このグループは SNS で未知の不特定多数と交流する

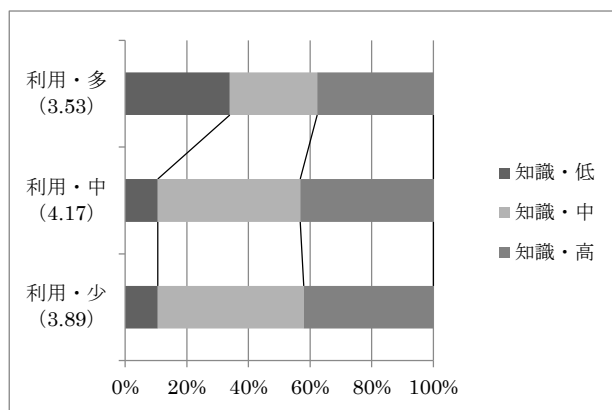


図 18 利用度×知識度 ( $\alpha < 0.005$ )

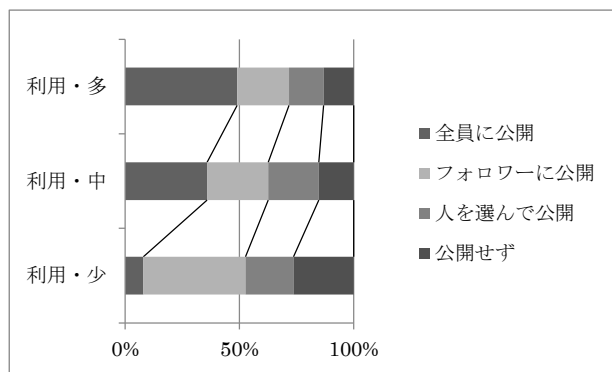


図 19 利用度×公開範囲 ( $\alpha < 0.01$ )

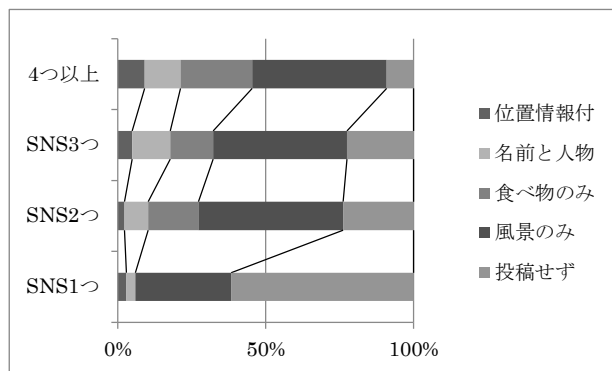


図 20 SNS 参加数×画像投稿 ( $\alpha < 0.001$ )

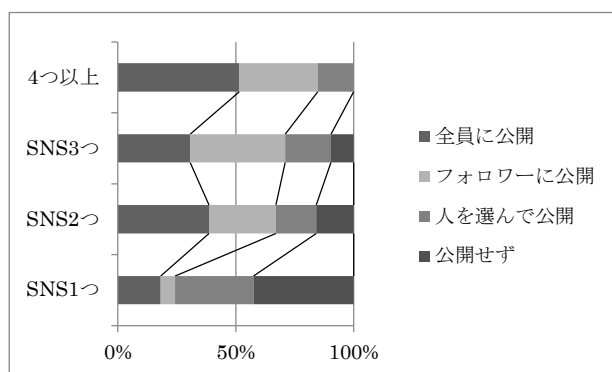


図 21 SNS 参加数×公開範囲 ( $\alpha < 0.00005$ )



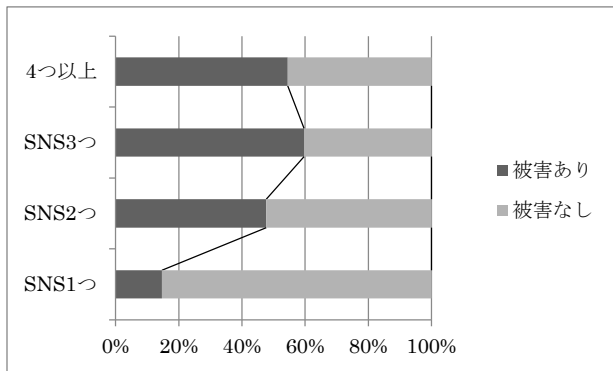


図22 SNS参加数×被害経験 (α&lt;0.0005)

よりも、既知の友人との連絡手段として使用することが想定される。それゆえ、見知らぬ第三者と出会う確率も低く、リスクな行動に巻き込まれにくいために、被害経験者が1割強と、他のグループと比べて非常に少ないのではないだろうか。（対して、SNS参加数×加害経験は、5%の有意水準を満たさない。どのグループにも1割弱～2割程度、加害経験のある人が存在する。SNS参加数は、被害経験とは高い関連性を見出せても、加害行動に対しては必ずしも影響があるとはいえないという結果となった。）

なお、このSNS参加数は、アカウント数ではなくSNSの種類であることに注意したい。言い換えれば複数のSNSに参加することは、SNSの性質に応じて交流の場を使い分けるといった姿勢や行動様式の違いを意味するものと考えられる。SNS参加数に関わる図20～図22のグラフでは、いずれも「SNS1つ」とそれ以外（複数のSNSに参加）のグループとの間に大きな差異が見られる。上述のとおり、LINEは既知の友人との連絡手段として活用されることから、友人関係の延長線上で、日常生活との使い分けをせずに用いることができるSNSである。このことから、SNS参加数が場の使い分けという姿勢（行動様式）を表していることが見てとれる。

### 3.3 クロス集計の結果と考察・その2：

#### 詳細な（全項目の）クロス集計からの探索

以上に見てきたように、セキュリティ意識・知識・行動の間には、意外なことに、相互に関係性があるとは言えなかった（有意水準を満たさず、帰無仮説を棄却できなかった）。代わって、回答者の性別、学科（学科系列）などの自らが属する「社会的集団」、そしてスマートフォン機能の利用状況（利用度）・SNSへの参加状況（SNS参加数）といった「行動様式」が、セキュリティに関する行動に大きな影響を与えていることが判明した。そこで、探索的なデータ分析のために、調査票の質問項目すべてを、性別、学科系列、年齢、購入年、所有時期（年齢と購入年から推定）、利用時間、利用度、意識度、知識度、SNS参加数、そして行動の指標として、加害経験、被害経験に加え、投稿注意（無断投稿した友人に注意したことがあるか）に対して一つ一つクロス集計し、それぞれカイ二乗検定を行っ

た。検定の結果、満たした有意水準の危険率 $\alpha$ が0.05以上の場合には空欄のままとし、 $0.01 < \alpha < 0.05$ は「\*」、 $\alpha < 0.01$ は「\*\*」、 $\alpha < 0.005$ は「\*\*\*」を記載したものが、次頁の「表1 クロス集計によるカイ二乗検定結果」である。質問項目の順番は、実際の調査票の順番に対応している。また、質問項目欄にカギカッコを付して掲載したものは、再コード化して作成した項目（直接、調査票で尋ねていないもの）である。以下、本節では、この詳細な（全項目の）クロス集計の検定結果一覧について検討する。

#### (1) 意識度と知識度への関連項目の詳細

まず、意識度および知識度に関連する項目として新たに有意差が見出されたものについて、詳細を考察する。

意識度に関連するのは、全項目の詳細なクロス集計でもわずかで、前節で言及した学科系列（\*）に加えて、地図やナビ機能の利用（\*）、無断投稿の被害経験（\*）、一番よく参加するSNS、OSの更新頻度という合計5つの項目があると分かった。

地図やナビ機能を利用するグループのほうが、意識度も高い傾向にある。この機能は、他にも性別、購入年、所有時期、知識度と関連が見られる興味深い質問項目で、外出を前提に用いる機能であることから、活発さや外向性の指標とも考えられる。ここから、セキュリティ意識を醸成する一因は、日常の活動や行動様式にもあると考えられよう。

また、一番よく参加するSNSは、LINE・twitter・その他の3つに分かれたが、twitterを利用するグループが、意識度も高い傾向が見られた。日頃、仲間内でクローズドな連絡手段としてLINEを用いるグループに比べ、twitterをメインに使うグループのほうが第三者と広く交流できるという点で、やはり外向性を反映していると思なすことができよう。なお、無断投稿の被害（\*）と、更新頻度（\*）に関しては、学科系列からの間接的な影響とも考えられることに注意したい<sup>9)</sup>。

他方で、意識度×OSの更新頻度は、危機意識を反映しているのか、比較的大きな関連性が見られた。意識の高いグループは、通知があればそのつど更新するか、自分でカスタマイズする傾向が大きい。（対して、意識の中～低いグループは、溜めてから一気に更新する傾向がある。学科系列×更新頻度（\*\*）の有意差にも、同様の専門知識に由来するセキュリティへの注意や工夫が見て取れよう。）

以上、見てきたように、意識を高めても、SNS上への画像投稿や公開範囲、無断投稿注意などの行動には、明確な影響は確認できなかった（帰無仮説が棄却できなかった）。言い換えれば、セキュリティに対する悲観（心配・不安）や楽観（平気・安心）という意識の違いは、自らの「能動的」な行動には影響が薄いものの、OSの更新頻度といった「受動的」な行動とは関連性が見て取れた。それゆえ、OS更新の自動通知のように、スマートフォンのアーキテクチャを変えることは、受動的なセキュリティ行動に効果があると考えられる。

表1 クロス集計によるカイ二乗検定結果 (\*...0.01 <  $\alpha$  < 0.05、\*... $\alpha$  < 0.01、\*... $\alpha$  < 0.005)

項目	性別	学科系列	年齢	購入年	所有時期	利用時間	利用度	意識度	知識度	SNS参加数	投稿注意	加害経験	被害経験
利用 通話・メール										*			
利用 インターネット		**											
利用 動画鑑賞	*								**				
利用 アプリ	*	**	*	*	*	**			*				
利用 地図	*			*	*		*		*				
利用 SNS	*												*
利用 「利用度」	*			*					**	*			
利用 一番利用機能	**	*			*				**	**			**
意識 実感なし									*				
意識 ロック安心						*							
意識 中身平気													
意識 投稿平気													
意識 流出心配													
意識 投稿不快				*									
意識 「意識度」		*											
知識 対策ソフト	*	*											
知識 遠隔ロック													
知識 バス複雑				*		**							
知識 アプリ収集													
知識 アカ乗っ取り						*							
知識 国際傍受	**		*										
知識 「知識度」	*					**	*				**	*	*
行動 加害:誹謗中傷		*		*							*	*	*
行動 加害:乗っ取り									*	*	*	*	*
行動 「加害経験」		*									*	*	*
行動 被害:誹謗中傷		*				*					*	*	*
行動 被害:乗っ取り				*							*	*	*
行動 被害:無断投稿	*	**	*				*		*	*	*	*	*
行動 被害:出会い系									*	*	*	*	*
行動 「被害経験」		*								*	*	*	*
行動 投稿注意		*					*		*	*	*	*	*
参加 LINE						**	*						*
参加 twitter		*				*	*					*	*
参加 facebook	**	*	*	*							*	*	*
参加 mixi	**	*	*	*	*				*	*	*	*	*
参加 参加せず						*	*						
参加 「SNS参加数」	*		*	*	*	*	*						*
参加 一番参加SNS							*					*	*
参加 本名SNS有無	**	*		*					*	*	*	*	*
行動 OS更新頻度		*					*		*	*	*	*	*
行動 OS通知設定	*								*	*	*	*	*
行動 投稿内容	*	*								*	*	*	*
行動 公開範囲	**	*				*	*			*	*	*	*

次に、知識度は、利用機能の複数の項目と関連があり、前節で言及した利用度(\*\*\* )に加えて、動画鑑賞(\*\*)、ゲームなどのアプリ(\*)、地図やナビ(\*)との関連が見出せた。いずれも、当該機能をよく利用するグループのほうが、知識度の低い人々の割合が2倍以上となっている。セキュリティに関する最新の知識を得るルートの多くがネット上の文字情報(IT 関連のニュースや専門サイトの記事等)であることを考慮すると、多彩な機能の利用は、相対的に文章を読ませなくするのかもしれない。

また、知識×乗っ取りの加害経験(\*)も、ネット上で知識を得て関心を持ち、つい試してみたためと考えられる。加えて、知識×無断投稿への注意(\*\*\* )との関連は興味深い。知識があるからこそ、自分の被害や友人の炎上のリスクなど、その先に波及しうる展開を予見して「友人」を注意するという行動につながったと考えられる。他方で、意識度と「自分」の行動(画像投稿や公開範囲等)との間には、関連性が見出されなかったことは注目に値する。

## (2) 性別による影響の詳細

知識と同様、利用機能の大半に、男女間で有意差が認められた。SNS のみ女性の、他の機能は男性の利用割合が高かった。一番よく利用する機能では、女性の8割弱がSNSを挙げたのに対して、男性ではネット、アプリ、SNSがそれぞれ3割前後だった。この結果は、性別によって生活様式(ライフスタイル)が異なるという社会的知見にも合致する。なお、一番よく利用する機能の偏りは男女の生活様式の差であって、決して学科系列(人文系、社会系、工学系、情報系)、すなわち文理などの大学内での場の違いによるものではない。というのも、学科系列×一番利用する機能をクロス集計したところ、危険率が75%を越えてしまい( $\alpha > 0.75$ )、帰無仮説(学科系列と一番利用する機能の間には何の関連性もない)が支持される割合が高く、それゆえ関連性が見出せなかったためである。

他方で性別は、セキュリティ意識にほとんど影響を及ぼしていない(関連性があるとはいえない)。セキュリティ意識に関与・影響する要素は、今回の調査で明らかになったもの以外で別にあるのかもしれない(例えば、学歴=偏差値や、家庭環境=出身階層など)。

セキュリティに関する知識については、国際傍受(\*\*)など日常の生活圏から遠い、政治経済的な知識は、既存の社会的知見と同様、男女差が顕著(男性のほうがよく知る)であった。なお、対策ソフトの知識(\*)については、学科系列×対策ソフト(\*)からの間接的な影響が想定されるので、注意したい。同様に、OS更新の通知設定(\*)に見られた男女差も、学科系列×通知設定(\*\*)の影響による疑似的な関連性である可能性を否定できない<sup>10)</sup>。

また、加害経験・被害経験にも、性別はあまり影響していない。無断投稿の被害に女性が多い(\*)のも、女性のほうがSNSをよく利用することに由来すると解釈できる。同様に、例えば、SNSアカウント乗っ取りの加害経験や、出会い系トラブルの被害経験は男女ともに1割ほど存在

するが、いずれも(統計的有意差は算出されなかったものの)女性のほうが、経験比率が若干高かった。

SNSの利用状況については、「facebook」に男女差が顕著(\*\*\* )で、女性の参加比率が高い。SNS参加数や本名で参加しているSNSの有無でも、男女差が大きい(いずれも\*\*で、女性の参加数が多く本名参加率も高い)。

加えて、SNS上での行動に注目すれば、前節のとおり、画像投稿(\*)、公開範囲(\*\*\* )の両方で、性別からの影響が見られた。これらを、SNSというネット上での「社交」の仕方と見れば、人間関係のつながり方において男女差があるという既存のジェンダー研究と合致する。そのため、SNS上の振る舞い(行動)という、加害や被害などに顕在する以前のセキュリティに関わる潜在的な傾向に、性別による生活様式(ライフスタイル)の違いが影響していると考えられる。

## (3) 学科系列による影響の詳細

学科系列も、性別と同様、複数の項目に比較的大きな影響を与える要因であることが判明した。

利用機能では、インターネット(\*\*)とアプリ(\*\*\*)の利用で、理系学科が多いという統計的有意差が算出された。情報系・工学系の学生は、スマートフォンを、ガラパゴス・ケータイの延長線上というより、ハンディなパソコンとして使用する(ネットに接続したり、アプリでカスタマイズしたりする)傾向があるのかもしれない。

また学科系列は、前述したように意識度(\*)に影響を及ぼす数少ない要因である。他方で、知識については、学科による授業内容の違い(情報系はセキュリティに関する知識も豊富ではないかという事前の予想)にもかかわらず、対策ソフト(\*)以外は有意な関連性が見出せなかった。対して、OSの更新頻度(\*\*)に見られる学科系列の関連性は、情報系・工学系では通知があるたびに更新したり、新しいバージョンの評判などを検索して自分なりに対応する「その他」を選んだりする割合が比較的高く、理系の専門知識を反映した有意差が見受けられる。社会系・人文系では、何度か通知されてから、つまり通知を溜めてから更新する傾向が見られた。

さらに、実際の行動に注目すれば、学科系列は多角的かつ大きな影響を及ぼしていることが明らかとなった。所属する学科系列によって、加害経験(\*\*)と被害経験(\*\*)だけでなく、個別の加害・被害項目でも関連性が算出された。好奇心からか、情報系では加害経験・被害経験ともに多いという結果となった。また、twitter(\*)やfacebook(\*\*\* )への参加、本名で参加するSNSの有無(\*\*)、SNSの画像投稿(\*)や公開範囲(\*)でも、学科系列との関連が見られた。総じてSNS上では、文系はオープンで、理系は慎重な行動をとる傾向が見られた。

換言すれば、学科系列によって意識は醸成されても、知識は別の要因の影響を受けることが明らかとなった。また、意識や知識よりも、行動において、学科系列の強い影響が見られることが分かった。

#### (4) 利用度と SNS 参加数による影響の詳細

利用度と SNS 参加状況の一部の項目に、また行動では SNS の公開範囲にのみ、顕著な有意差が見られた (\*\* ないし \*\*\* )。しかし、利用度は意識に関する項目および公開範囲以外の行動については (加害経験・被害経験にも OS 更新にも一切)、関連性を見出すことができなかった。利用度 (利用する機能数の多寡) を、個人のスマートフォンの使いこなしと見るならば、それは知識や SNS の参加状況 (および公開範囲) とは関連性があるものの、セキュリティ意識や行動に関しては関連があるとは言えないことが判明した。

また、SNS 参加数は、利用する機能の一部と、加害経験・被害経験の一部、および SNS 上の行動 (画像投稿・公開範囲) に強い関連性が見出されるが、セキュリティ意識や知識に関するすべての項目で、統計的有意差は算出されなかった。前節で指摘したとおり、SNS 参加数をネット上での社交の指標と見るならば、複数の SNS の場を「使い分ける」姿勢が、スマートフォンの使い方 (機能の利用) や加害経験・被害経験、SNS 上の行動などに共通するスマートフォンの「行動様式」の存在を想定することができる。行動様式は、行動に影響を及ぼし、意識や知識とは無関係の原理である。それゆえ、「意識・知識・行動は相互に関連性がある」という仮説が当てはまらなかったのではない。仮説モデルを修正するとすれば、意識・知識・行動の生成には、それぞれ別の要因が作用しているというものになる。

#### (5) 加害経験・被害経験に関する影響の詳細

上述のとおり、意識や知識とは別に、SNS への姿勢、スマートフォンの使い方と、セキュリティに関する行動に共通する「行動様式」を想定すると、加害行動と被害体験の強い関連性についても、よりよく説明することができる。すなわち、被害経験のある者は加害者になりやすく、加害経験のある者はまた被害者になりやすい (ハイリスクな行動様式を身につけているグループ)。対して、被害経験のない者は加害者にもなりにくく、加害経験のない者は被害者にもなりにくい (安全な行動様式を身につけているグループ)。また、加害経験と被害経験は、参加する SNS の種類や数 (SNS ごとの作法や使い分け)、そして画像投稿や公開範囲 (SNS 上での行動) と関連性が、特に被害有無との強い関連性が見出せるのである。

また、SNS 参加数と同様に、加害経験・被害経験でもまた、セキュリティ意識やセキュリティに関する知識を尋ねるすべての項目で統計的有意差が算出できなかった。ここでもまた、意識・知識と、行動とは、異なる生成原理によって影響を受けていることが指摘できる。

#### (6) その他

最後に、その他の項目に関する興味深い検定結果について、前出の表を考察したい。

最初に、年齢・購入年・所有時期の関係である。回答者

の意識や知識よりも、属性が行動に影響を与える可能性を検証すべく、それぞれの質問項目について年齢と購入年でもクロス集計を作成した。加えて、年齢と購入年の質問から、スマホを所有したおおよその時期 (中学・高校・大学時代いずれかのライフステージ) を算出し、所有時期によるクロス集計も参考として作成した<sup>11)</sup>。例えば、一番よく利用する機能について、購入年では帰無仮説が破棄できなかったが、購入時期で集計すると有意差 (\*) が確認された。すなわち、中学以前に所有したグループの約 50% がネット接続を、高校時代のグループでは SNS を、大学時代から所有したグループではゲームなどのアプリを、それぞれ一番利用するという特徴が見られた。また、パスワードを複雑にしないと不正アクセスされる危険性があるという知識についても、現在の年齢や購入年ではなく、所有時期 (ライフステージ) によって、有意差が見られた。具体的には、中学以前に所有したグループの 7 割強しか知っていないが、高校時代・大学時代と所有時期が上がると、9 割〜9 割強が知っているという回答している。中学時代、周囲の大半がガラパゴス・ケータイを持っているなかで早々にスマートフォンを所有するようになったグループは、ケータイをもつ友人たちと同様に、パスワードの重要性をあまり認識していなかったためと思われる。このように、所有時期 (ライフステージ) も、性別や学科と同様、そこから影響を受ける「社会的集団」と見なすことができよう。

次に、利用時間については、他の質問項目との間に、ほとんど関連性が見出せなかった (意識・被害・SNS 参加で 1 つずつのみ)。例えば、SNS での交流から抜け出せずに「長時間」参加し続けるグループがあるのではないかと予測していたが、SNS に参加しないグループとするグループの間で、1 日のうちで 3 時間〜5 時間、5 時間以上と、比較的長時間利用する比率は変わらなかった。違いは、SNS に参加するグループは、1 時間〜3 時間が 2 割ほどいたのに対して、参加しないグループではゼロだった (1 時間未満が取って代わった)。他方で、唯一高い関連性が見出せたのが、アプリの利用であった。これは、ソーシャル・ゲーム等のアプリの登場により、リアルタイムでゲームの設計を変化させてユーザーを夢中にさせる技術が導入され、青少年のネット依存が深刻化してきているという昨今の社会問題を反映しており、非常に興味深い結果である。

## 4. 結語

本研究では、スマートフォンに関するセキュリティ意識・知識・行動について、大学生にアンケート調査を実施した。その際、「知識の多い人は、意識も高く、慎重で安全な使い方をする」という仮説を事前に想定していた。この仮説は広く一般に支持されているものであり、それゆえ学校や企業などの組織におけるセキュリティ対策でも、セキュリティに関する講演会を開催して正しい知識を増やし、意識を高めることで、安心・安全な行動を促すことを目的としているといえよう。



しかし、アンケート調査の結果、セキュリティ意識・知識・行動それぞれの間に明確な関連性は見出せなかった。他方で、知識と SNS 上の行動には性別が影響を与え、意識と加害・被害経験には所属する学科系列が影響を与えることが明らかとなった。また、加害経験と被害経験の間に強い関連があり、他人を攻撃したことがある人は自らも攻撃されたことがある人だと分かった。加えて、スマートフォンの機能の活用状況や SNS への参加状況などの「行動様式」が、SNS 上の行動や加害・被害経験に影響を与えることが分かった。言い換えれば、セキュリティに関する知識や意識よりも、性別や学科という「社会的集団」およびスマートフォンの「行動様式」が、セキュリティに関わる行動に影響するのである。社会生活において占める位置(社会的集団)と、行動様式によって、安心・安全な行動か、ハイリスクな行動かという実際の行動の違いが生じる。既存の社会学用語で言い換えるならば、セキュリティに関する知識や意識ではなく、無自覚なハビトゥスによって、スマートフォンのセキュリティに関する慣習行動が方向づけられているということである。「ハビトゥス」とは、自分が所属・配置された社会的な位置・カテゴリーに由来する「性向(ディスポジション)」すなわち行動の生成原理として定義される。(そして、今回の調査で尋ねることができなかった、家庭環境や社会階級などからも影響を受ける。) 今後は、セキュリティをめぐる意識・知識・行動の社会学的研究として、ハビトゥス論からのアプローチへと進展させていきたい。

最後に、本研究の調査結果を踏まえ、今後のスマートフォンに関するセキュリティ対策は、講演等によって知識を増やすだけでなく、例えば「訓練(体験学習)」を行うことで実際の行動を安全に保つことができると提案したい。

## 注

- 1) 15 歳～19 歳のうち、男性の 77.8%、女性の 84.8%が、スマートフォンを所有している。詳細は、株式会社ビデオリサーチインタラクティブ(2014)を参照されたい。
- 2) ガラパゴス・ケータイ(通称ガラケー)とは、フューチャーフォンとも呼ばれる、日本固有の発展を遂げた携帯電話のことを指す。本論文では、「スマートフォン」との対比で「ガラパゴス・ケータイ」という名称を用いる。
- 3) スマートフォン被害の特徴として、ユーザーの心理を巧みに騙し、攻撃を仕掛けてくる被害が多く見られるという。詳細は、独立行政法人情報処理推進機構(2014)を参照されたい。
- 4) 紙面の都合上、文献調査の詳細は省略する。詳細は、渡邊(2014)を参照されたい。
- 5) 残りの 15 名のうち、13 名がガラパゴス・ケータイのみを所有し、2 名は携帯電話を(スマートフォンも、ガラパゴス・ケータイも)所有していないという回答だったため、本論文での分析対象からは除外している。
- 6) 太郎丸博(2005)、第 2 章「クロス表と独立性の検定」

pp. 8-21 より。

- 7) 太郎丸博(2005)、第 4 章「続・クロス表の分析」pp. 45-47 より。イエーツの連続性の修正とは、セル度数から期待度数を引いたあと、その差分の絶対値からさらに 0.5 を引いて二乗するものである。
- 8) 左右の横帯グラフを比較してみると、男性と情報系・工学系、女性と社会系の選択肢の比率が極めて近似している。なお、今回の調査で、人文系の回答者が相対的に少なく、それゆえに(とくに画像投稿において)人文系と女性の回答比率とは少しずれているように見えると思われる。
- 9) 性別×学科系列×投稿内容または公開範囲と同様に、ここでもまた、学科系列×無断投稿の被害(\*\*\* )が、学科系列×意識度(\*)によって、意識度と無断投稿の被害の間に疑似的な関連性が算出できてしまった可能性も捨てきれない。検定結果から安易に直接的な影響を想定するのではなく、結果を慎重に考察する必要がある。
- 10) 前述したとおり、学科系列の構成比に男女差が大きく、疑似的な関連性が表れやすい。
- 11) 所有時期を直接尋ねる質問項目は設定していない。そのため、実際には、早生まれかどうかによって学年にズレが生じるため、年齢と購入年から算出した所有時期は、あくまでも探索的分析のための参考要因・ひとつの目安であることに注意されたい。

## 参考文献

- [1] 株式会社ビデオリサーチインタラクティブ: プレスリリース, 性別・世代別のスマートフォン利用状況, <http://www.videoi.co.jp/release/20140225.html>, (2014)
- [2] 独立行政法人情報処理推進機構: コンピューターウイルス・不正アクセスの届出状況および被害相談(2014 年第一四半期), <https://www.ipa.go.jp/files/000038479.pdf>, (2014)
- [3] 渡邊省吾: スマートフォンに対するセキュリティ意識: 大学生へのアンケート調査を通じて, 平成 26 年度神奈川工科大学工学部機械工学科卒業論文(指導教員 三浦直子), (2014)
- [4] 太郎丸博: 人文・社会科学のためのカテゴリーカル・データ解析入門, ナカニシヤ出版, pp. 8-21, 45-47, (2005)
- [5] 白谷秀一・朴相権・内田龍史(編著): 実践はじめての社会調査(新版), 自治体研究社, pp. 116-119, (2012)
- [7] 菅 民郎: すべてがわかるアンケートデータの分析, 現代数学社, pp. 44-51, (2000)
- [8] 菅 民郎: らくらく図解アンケートデータ分析教室, オーム社, pp. 280-283, (2007)
- [9] 松村真木子: 人文系大学生の情報セキュリティ意識とスキル, 情報処理学会研究報告コンピュータセキュリティ(CSEC) 43, (2006).
- [10] 八城年伸: パスワード管理意識に対する性別による違いについて, 情報処理学会第 75 回全国大会講演論文集, (2013)