論　文

# 情報セキュリティ教育の効果と課題

## ―― A 高等学校「情報科」を事例に ――

尾　上　妥　理

〔抄　録〕

本稿は，A 高等学校「情報科」を事例に，情報セキュリティ教育の実践が，高校生の情報セキュリティに関する状況に，どのような効果をもたらしているのかを分析することを通して，今後の情報セキュリティ教育の一助とすることを目的とする。研究方法は，A 高等学校の 1 年情報科 39 名，3 年情報科 30 名，3 年商業科 24 名の生徒を対象に，情報セキュリティに関する状況について，質問紙調査を実施し分析を行った。結果，情報機器の習熟度や，インターネット上の攻撃・脅威に対する知識の習得状況は，いずれも 1 年情報科，3 年商業科よりも 3 年情報科が高かった。しかし，トラブルや被害につながる経験，また実際にトラブルや被害にあった経験については，当初，インターネット上の攻撃・脅威について「知らない生徒」の方が，多いと筆者は考えていたが，「知っている生徒」の方が，実際には多かった。本稿では，これらの検証を踏まえた今後の情報セキュリティ教育の在り方について論じる。

**キーワード**：情報セキュリティ教育，専門教科「情報」，情報教育，倫理観，情報モラル

## 1．はじめに

### 1.1　情報セキュリティ教育の必要性

今日，情報セキュリティに関する多くの事件が毎日のように起こっており，これに関連する報道は後を絶たない。学校教育において情報リテラシーの育成が推進され，情報セキュリティ教育の一層の充実が求められている背景には，こうした現状があることが指摘できる。また，独立行政法人情報処理推進機構セキュリティセンター（IPA）（2018）の「情報セキュリティ 10 大脅威」においては[1]，「組織」向け脅威として，「脅威に対応するためのセキュリティ人材の不足」，そして，「個人」向け脅威として「情報モラル欠如に伴う犯罪の低年齢化」があげられている。このような状況からも，専門教科「情報」において，情報技術者としての倫理観の涵養，

情報モラル教育を基盤とした情報セキュリティ教育を実践し，情報セキュリティ人材の育成を視野に入れた取組を推進することは，ますます重要になるといえる。

### 1.2　情報セキュリティ教育の取組

こうした動きの中，現在，各高等学校においては，情報セキュリティに関するさまざまな取組がなされている。例えば，増山一光（2012）によると[2]，学校設定科目として「情報セキュリティ」を設置し，教育実践が行われた。実践内容として，コンピュータウイルスに関する内容が取り扱われているが，そのことにより，コンピュータウイルスへの対策に関する行動変容がみられ，コンピュータウイルスによる情報セキュリティインシデントに対する総合的な能力を得ている。一方で，情報セキュリティ教育の展開は，さまざまな情報セキュリティインシデントへの対策を学習できる反面，悪意を持った攻撃者の手口についても知ることになる。このような教育上のジレンマに対して，授業展開の過程で常に情報モラルに根ざした生徒へのアプローチを行い，自らが行った行動を想定させることで，適切な行動を引き出すことが必要になるということが示されている。この点は，増山，佐藤（2010）も[3]，授業展開の場合の注意事項として,「無線 LAN の危険性だけを単に指摘しても有効なセキュリティ教育にはならない。」や,「何が危険で，どのような対策が必要であるか明確に把握させることが大切である。一方で，このようなセキュリティ教育の必要性に関しては誰もが認めるところであるが，技術的なセキュリティ教育に特化すると，結果的にクラッカーを育成することにはならないかという危惧が生じる。」と述べている。その対策として,「セキュリティ教育の根幹は「倫理観の育成」にあることから，偏りのない総合的なアプローチによる授業展開が必要となるのである。」また,「高等学校段階における技術面だけでなく心理面からの情報セキュリティを重んじる態度の育成が必要となるのである。」とまとめている。

また，佐藤，西郡ら（2017）の研究では，共通教科「情報」の科目「社会と情報」において,「スマートフォンとオンラインゲーム情報の盗聴・改ざん」,「パソコンの遠隔操作」をテーマにした「サイバーセキュリティ技術実践授業」における効果や課題について考察されている。この授業においては，仮想環境によるパソコンの乗っ取り遠隔操作や，スマートフォンのオンラインゲームの盗聴・改ざんといった内容が扱われている。アンケート結果より，生徒の理解度は，9 割以上が「理解できた」であり,「言葉だけでは分からないが，体験することで危険性がよく分かる」というような感想が示されている。そして，サイバー犯罪に興味を持ってしまう等の悪影響については，自由記述のアンケートから 6 名程度確認されたということであるが，そのような生徒にも，法や倫理について説明することで対応したという実践事例が示されている[4]。

このように情報教育に関する授業を展開する際には，情報が持つ有効性と危険性の両面を伝える必要があり，増山（2013）[5]も，安全教育の視点からみた情報セキュリティ教育の目的として次の 2 点を挙げている。「第 1 に，生徒を被害者にしないために，情報社会での護身術として

情報セキュリティを学ぶということである。これは，高校生にとってリスクの存在を把握して情報社会で安全を確保することは，適切な社会生活を営むうえでも重要になると考えられるからである。第 2 に，生徒を加害者にしないために，適切な情報セキュリティに関する知識・技能を身に付けた上での行動できるようにすることである。これは，情報機器やインターネットの利用環境を適切に整え，自らの振る舞いが第三者にどのような影響を与えるのかを考慮させつつ行動することによって，適切な行為を身に付けさせることができると考えられるからである。」としている。田中，池田ら（2016）も，情報モラル研究の観点から知識と行動の不一致を認識させ適切な行動意図の形成を促す情報モラル教育の重要性を論じている [6]。

他方で，宮崎（2020）は，「高校教科「情報」が設置されたにも関わらず，各学校では ICT の整備が行き届いていないのが現状である。」[7] と学校内の環境整備が追い付いていないこと指摘する。また，小熊，山本ら（2020）は，教員への意識調査を実施し，「情報セキュリティ」「情報セキュリティポリシー」「ソフトウェアインストール」「メール誤送信」についての意識は高い一方で，「不正侵入」「データ破損対策」「情報セキュリティの法律」の意識は低いことを明らかにし，教員用の研修や研修向け教材の開発を行い，教員の人的な情報セキュリティ問題を解決する必要性を指摘するなど [8]，生徒のみならず学校における環境整備や教員側の意識についての課題もみえてくる。

### 1.3　情報セキュリティに対する意識調査

本稿では，質問紙調査において独立行政法人情報処理推進機構セキュリティセンターセキュリティ対策推進部実施の「2019 年度情報セキュリティに対する意識調査 [9]」を援用している。この調査は，全国 13 歳以上のインターネット利用者 5000 人に対して実施されたものである。パソコン調査とスマートデバイス調査が行われたが，本稿においては，パソコン調査を援用した。年代別には，10 代 6.0%，20 代 14.5%，30 代 16.7%，40 代 21.7%，50 代 18.1%，60 代 14.0%，70 代以上 9.1% の割合になっている。この調査結果の内，本稿で援用した設問の結果を示しておく。パソコンの習熟度（本稿設問 2）について最も高かったのは，「パソコンに関する基本的な知識を有しており，具体的な操作方法やトラブル発生時の対応等は自分で調べて対処することができるレベル」（39.8%），次いで「パソコンの基本的な操作や簡単な設定変更はでき，予期せぬ挙動やエラーが発生した場合も他者からの説明があれば理解，対処できるレベル」（31.7%），「パソコンの基本的な操作はできるが，設定変更等は自分ではできず他者にお願いをするレベル」（17.2%），「パソコンに関する十分な知識を有しており，具体的な操作方法やトラブル発生時の対応などについて他者に説明することができるレベル」（11.2%）と続く。情報セキュリティに関する攻撃・脅威等の理解（本稿設問 3）について最も高かったのは，「フィッシング詐欺」（88.8%）であった。次いで「ワンクリック請求」（85.0%），「セキュリティホール（脆弱性）」（71.4%），「マルウェア」（60.6%）と続く。また過去 1 年間のインターネット利用中の経験（本

稿設問 4）について最も高かったのは，「本文中の URL にアクセスするように促す不審なメールを受信した」（34.1%）であった。次いで「ブラウザに突然「ウイルスに感染した」などの警告画面が表示された」（26.7%），「添付ファイルを開くように促す不審なメールを受信した」（25.8%），「身に覚えのない支払いを求める（架空請求）メールを受信した」（19.7%）と続く。過去 1 年間のインターネット利用中の被害（本稿設問 5）について最も高かったのは，「過去 1 年間で上記のような被害はない」（52.5%）であった。次いで，「上記のようなトラブルや被害にあったかどうかわからない」（23.8%），「ウイルスに感染した（セキュリティソフトによる検出で実害にはいたらなかったケースを含む）」（9.2%），「パソコンが突然動作しなくなってしまった（原因はウイルスや不正アクセスに限らず，故障や劣化なども含む）」（8.0%）と続く。

### 1.4　問題の所在

情報の専門的教育の取組を通して，一定の成果が得られている一方で課題も多いが，こうした課題を克服し，生徒が日常の中で情報セキュリティに配慮して情報機器を扱うスキルを習得することは教育推進のためにも極めて重要となる。この点について小熊，山本（2020）は「情報セキュリティは，これまで情報モラル教育の 1 つとしてとらえられることが多かったが，今後は情報教育の一つとして位置づけることで，特定の教科だけなく，学校教育全体で指導することが可能になる。」と論じている [10]。

こうした状況を背景におくことで，次の点を指摘することができる。すなわち，環境において差異はある中でも，まず，実践的な情報セキュリティ教育を浸透させるためには，授業展開の過程で常に情報モラルに根ざした生徒へのアプローチを行い，自らが行った行動を想定させることで，適切な行動を引き出すことが必要になること。次に，このような内容を実践的に取り組む情報科における情報セキュリティ教育を通じて，情報セキュリティインシデントに対する行動変容がみられ対応能力が高まるということや，一方で情報科における情報セキュリティ教育の取組によって，情報セキュリティに関するトラブルに遭遇する可能性があると考えられることである。つまり，情報セキュリティ教育を功罪両面から捉えることで，安全かつ実践的な教育活動のための手掛かりを見出すことができるといえよう。

そこで本稿では，A 高等学校「情報科」における情報セキュリティ教育を事例に，高等学校の情報セキュリティ教育が，どのような効果をもたらしているのかを分析することを通して課題を明らかにしたい。そして，今後の情報セキュリティ教育の一助とすることを目的とする。

## 2. 方法

### 2.1　調査対象：

**プロフィール**：A 高等学校は，情報に関する学科 2 クラスと商業に関する学科 6 クラスからな

る専門高校である。特徴としては，専門的な学びを柱とし，産官学連携をはじめとした地域とのつながりをもった特色ある教育活動を実践している。

①**１年情報科**：入学してから３ヵ月少ししか経過しておらず，また，新型コロナウイルス感染症による特別休暇があったために，情報セキュリティに関する学習がまだ進んでいない状況である。

②**３年情報科**：入学時より，情報の専門分野において，情報セキュリティに関する学習を行ってきた。情報セキュリティの学習においては，情報セキュリティの概念，脅威や攻撃手法，対策が理解でき，初歩の実装技術を実践できることや，法規に関する基礎的な知識を習得し，サイバー空間で適切に判断・行動する態度を身につけることを目標としている。

③**３年商業科**：情報に関する学習は行っており，その中には，情報セキュリティについての要素が含まれているものの，特化した取組は実践されていない。

調査対象の設定理由は，情報セキュリティ教育を実践している情報科と情報教育は実践しているものの情報セキュリティ教育には，深く取り組んでいない商業科との比較，また情報科においても１年と３年との学年による比較を行うためである。

**方法**：質問紙調査　Google フォームを使用

**時期**：2020 年 7 月

**調査項目**：独立行政法人情報処理推進機構セキュリティセンターセキュリティ対策推進部実施の「2019 年度情報セキュリティに対する意識調査」を援用。

**回収率**：質問紙の全体の回収率は，92 名（100%）であり，区分別にみると，1 年情報科が 39 名（100%），3 年情報科が 29 名（100%），3 年商業科が 24 名（100%）の回数率であった。

### 2.2　設問の構成

質問紙調査は，独立行政法人情報処理推進機構セキュリティセンターセキュリティ対策推進部実施の「2019 年度情報セキュリティに対する意識調査」を援用し，次の５つの領域で設計している。1）利用機器，2）習熟度，3）攻撃・脅威の理解，4）経験，5）被害，である。（付表参照）

### 2.3　分析手順

1）利用機器

生徒たちが，普段プライベートでインターネットサービス利用時に使用している情報機器についての回答を学年・学科別に単純集計した。

2）習熟度

パソコンの習熟度，およびスマートデバイス（スマートフォン・タブレット端末）の習熟度についての回答を学年・学科別に集計した。各属性の度数について，偏りがあるかどうかを調

べるためカイ二乗検定を行った。

3）攻撃・脅威の理解

インターネット上の攻撃・脅威について知っているかという問いについての回答を学年・学科別に単純集計した。

4）経験

過去 1 年間，インターネット利用時に被害につながる経験をしたかどうかの回答を学年・学科別に単純集計した。

5）被害

過去 1 年間，インターネット利用時に被害にあったかどうかの回答を学年・学科別に単純集計した。

※トラブルや被害につながる経験について

ここでは，それぞれの攻撃･脅威について「1 詳しい内容を知っている」と「2 概要をある程度知っている」を選択した生徒の合計を「知っている生徒」，また，「3 名前を聞いたことがある」と「4 名前も概要も知らない」を選択した生徒の合計を「知らない生徒」と定義して分析した。表 10 は，設問 3，設問 4 の結果から，それぞれの攻撃･脅威について「知っている生徒」と「知らない生徒」で，設問 4 の「9 過去 1 年間で上記のような経験はない（トラブルや被害につながる経験がない）」と回答した生徒の割合を単純集計したものである。

※トラブルや被害の経験について

表 11 は，設問 3，設問 5 の結果から，それぞれの攻撃・脅威について「知っている生徒」と「知らない生徒」で，設問 5 の「14 過去 1 年間で上記のような被害はない（トラブルや被害にあった経験がない）」と回答した生徒の割合を単純集計したものである。

## 3. 結果

本節では調査の結果をみていくこととする。

まず，表 1 は，（設問 1）生徒たちが普段プライベートでインターネットサービス利用時に使用している情報機器について学年・学科別に単純集計したものである。スマートフォンの利用が 1 年情報科 36 名（92.3%），3 年商業科 23 名（95.8%），3 年情報科（28 名）96.6% であった。3 年情報科は，普段プライベートでインターネットサービスを利用する際には，16 名（55.2%）の利用率であった。また，情報科の生徒はゲーム機器の利用が 1 年 32 名（82.1%），3 年 15 名（51.7%）であった。

表 2 は，（設問 2-1）パソコンの習熟度について学年･学科別に集計したものである。結果，パソコンの習熟度について学年･学科によって有意な差が認められた（$x^2$=61.656, df=6, p<.01）。1

表 1：利用している情報機器

| # | 項目（全体の上位順） | 全体N=92 該当数 | % | 1 年情報科n=39 該当数 | % | 3 年商業科n=24 該当数 | % | 3 年情報科n=29 該当数 | % |
|---|---|---|---|---|---|---|---|---|---|
| 2 | スマートフォン | 87 | 94.6 | 36 | 92.3 | 23 | 95.8 | 28 | 96.6 |
| 5 | ゲーム機器 | 55 | 59.8 | 32 | 82.1 | 8 | 33.3 | 15 | 51.7 |
| 1 | パソコン | 48 | 52.2 | 22 | 56.4 | 10 | 41.7 | 16 | 55.2 |
| 3 | タブレット端末 | 29 | 31.5 | 16 | 41.0 | 9 | 37.5 | 4 | 13.8 |
| 4 | 携帯電話 | 3 | 3.3 | 1 | 2.6 | 1 | 4.2 | 1 | 3.4 |
| 6 | その他 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 |
| 7 | 無 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 |

表 2：パソコンの習熟度

| # | 項目（全体の上位順） | 全体N=92 該当数 | % | 1 年情報科n=39 該当数 | % | 3 年商業科n=24 該当数 | % | 3 年情報科n=29 該当数 | % |
|---|---|---|---|---|---|---|---|---|---|
| 3 | 基本的な操作や簡単な設定変更はできる | 36 | 39.1 | 15 | 38.5 | 10 | 41.7 | 11 | 37.9 |
| 2 | 基本的な知識はある | 25 | 27.2 | 6 | 15.4 | 6 | 25.0 | 13 | 44.8 |
| 4 | 基本的な操作はできる | 25 | 27.2 | 16 | 41.0 | 8 | 33.3 | 1 | 3.4 |
| 1 | 十分な知識がある | 6 | 6.5 | 2 | 5.1 | 0 | 0.0 | 4 | 13.8 |
| | 合計 | 92 | 100.0 | 39 | 100.0 | 24 | 100.0 | 29 | 100.0 |

($x^2$=61.656, df=6, p<.01)

表 3：スマートデバイス（スマートフォン・タブレット端末）の習熟度

| # | 項目（全体の上位順） | 全体N=92 該当数 | % | 1 年情報科n=39 該当数 | % | 3 年商業科n=24 該当数 | % | 3 年情報科n=29 該当数 | % |
|---|---|---|---|---|---|---|---|---|---|
| 2 | 基本的な知識はある | 55 | 59.8 | 21 | 53.8 | 15 | 62.5 | 19 | 65.5 |
| 3 | 基本的な操作や簡単な設定変更はできる | 18 | 19.6 | 13 | 33.3 | 2 | 8.3 | 3 | 10.3 |
| 4 | 基本的な操作はできる | 10 | 10.9 | 3 | 7.7 | 6 | 25.0 | 1 | 3.4 |
| 1 | 十分な知識がある | 9 | 9.8 | 2 | 5.1 | 1 | 4.2 | 6 | 20.7 |
| | 合計 | 92 | 100.0 | 39 | 100.0 | 24 | 100.0 | 29 | 100.0 |

($x^2$=64.144, df=6, p<.01)

年情報科は，「4 パソコンの基本的な操作はできる」が 16 名（41.0%），「2 パソコンの基本的な知識はある」が 6 名（15.4%）。3 年生商業科は，「4 パソコンの基本的な操作はできる」が 8 名（33.3%），「1 パソコンに関する十分な知識がある」が 0 名（0.0%）。3 年情報科は，「1 パソコンに関する十分な知識がある」が 4 名（13.8%），「2 パソコンの基本的な知識はある」が 13 名（44.8%），「4 パソコンの基本的な操作はできる」が 1 名（3.4%）であった。

表 3 は，（設問 2-2）スマートデバイス（スマートフォン・タブレット端末）の習熟度について学年・学科別に集計したものである。結果，スマートデバイスの習熟度について学年・学科によって有意な差が認められた（$x^2$=64.144, df=6, p<.01）。1 年情報科は，「3 スマートデバイスの基本的な操作や簡単な設定変更はできる」が 13 名（33.3%）。3 年生商業科は，「4 スマートデ

バイスの基本的な操作はできるが，設定変更等は自分ではできない」が 6 名（25.0%），「1 スマートデバイスに関する十分な知識を有している」が 1 名（4.2%），「3 スマートデバイスの基本的な操作や簡単な設定変更はできる」が 2 名（8.3%）。3 年情報科は，「1 スマートデバイスに関する十分な知識を有している」が 6 名（20.7%），「3 スマートデバイスの基本的な操作や簡単な設定変更はできる」が 3 名（10.3%），「4 スマートデバイスの基本的な操作はできるが，設定変更等は自分ではできない」が 1 名（3.4%）であった。

表 4 ～ 7 は，（設問 3）インターネット上の攻撃・脅威について知っているかという問いについての回答を学年・学科別に単純集計したものである。

「1 詳しい内容を知っている」と「2 概要をある程度知っている」と合わせた割合をみていくと，全体では，「1 ワンクリック請求」を知っている割合が 80 名（87.0%），「3 フィッシング詐欺」が 54 名（58.7%）であった。それ以外のものについての割合は，50%以下であった。

表 8 は，（設問 4）過去 1 年間，インターネット利用時に被害につながる経験をしたかどうかの回答を学年・学科別に単純集計したものである。「9 過去 1 年間で上記のような経験はない」

表 4：攻撃・脅威の理解（全体）（N=92）

| | 1 詳しい内容を知っている | | 2 概要をある程度知っている | | 3 名前を聞いたことがある | | 4 名前も概要も知らない | | 合計 | |
|---|---|---|---|---|---|---|---|---|---|---|
| # 項目 | 該当数 | % | 該当数 | % | 該当数 | % | 該当数 | % | 該当数 | % |
| 1 ワンクリック請求 | 26 | 28.3 | 54 | 58.7 | 10 | 10.9 | 2 | 2.2 | 92 | 100.0 |
| 2 パスワードリスト攻撃 | 8 | 8.7 | 25 | 27.2 | 25 | 27.2 | 34 | 37.0 | 92 | 100.0 |
| 3 フィッシング詐欺 | 18 | 19.6 | 36 | 39.1 | 30 | 32.6 | 8 | 8.7 | 92 | 100.0 |
| 4 セキュリティホール | 8 | 8.7 | 29 | 31.5 | 35 | 38.0 | 20 | 21.7 | 92 | 100.0 |
| 5 標的型攻撃 | 5 | 5.4 | 16 | 17.4 | 27 | 29.3 | 44 | 47.8 | 92 | 100.0 |
| 6 マルウェア | 9 | 9.8 | 16 | 17.4 | 27 | 29.3 | 40 | 43.5 | 92 | 100.0 |
| 7 偽セキュリティソフト | 9 | 9.8 | 22 | 23.9 | 31 | 33.7 | 30 | 32.6 | 92 | 100.0 |
| 8 DoS攻撃 | 15 | 16.3 | 19 | 20.7 | 21 | 22.8 | 37 | 40.2 | 92 | 100.0 |
| 9 ビジネスメール詐欺 | 5 | 5.4 | 25 | 27.2 | 41 | 44.6 | 21 | 22.8 | 92 | 100.0 |
| 10 偽警告 | 11 | 12.0 | 33 | 35.9 | 25 | 27.2 | 23 | 25.0 | 92 | 100.0 |
| 11 ランサムウェア | 11 | 12.0 | 10 | 10.9 | 31 | 33.7 | 40 | 43.5 | 92 | 100.0 |
| 12 セクストーション | 3 | 3.3 | 14 | 15.2 | 26 | 28.3 | 49 | 53.3 | 92 | 100.0 |

表 5：攻撃・脅威の理解（1 年情報科）（n=39）

| | 1 詳しい内容を知っている | | 2 概要をある程度知っている | | 3 名前を聞いたことがある | | 4 名前も概要も知らない | | 合計 | |
|---|---|---|---|---|---|---|---|---|---|---|
| # 項目 | 該当数 | % | 該当数 | % | 該当数 | % | 該当数 | % | 該当数 | % |
| 1 ワンクリック請求 | 8 | 20.5 | 25 | 64.1 | 6 | 15.4 | 0 | 0.0 | 39 | 100.0 |
| 2 パスワードリスト攻撃 | 0 | 0.0 | 10 | 25.6 | 9 | 23.1 | 20 | 51.3 | 39 | 100.0 |
| 3 フィッシング詐欺 | 4 | 10.3 | 14 | 35.9 | 20 | 51.3 | 1 | 2.6 | 39 | 100.0 |
| 4 セキュリティホール | 1 | 2.6 | 7 | 17.9 | 13 | 33.3 | 18 | 46.2 | 39 | 100.0 |
| 5 標的型攻撃 | 2 | 5.1 | 2 | 5.1 | 11 | 28.2 | 24 | 61.5 | 39 | 100.0 |
| 6 マルウェア | 1 | 2.6 | 5 | 12.8 | 12 | 30.8 | 21 | 53.8 | 39 | 100.0 |
| 7 偽セキュリティソフト | 3 | 7.7 | 9 | 23.1 | 13 | 33.3 | 14 | 35.9 | 39 | 100.0 |
| 8 DoS攻撃 | 4 | 10.3 | 4 | 10.3 | 9 | 23.1 | 22 | 56.4 | 39 | 100.0 |
| 9 ビジネスメール詐欺 | 3 | 7.7 | 9 | 23.1 | 16 | 41.0 | 11 | 28.2 | 39 | 100.0 |
| 10 偽警告 | 3 | 7.7 | 10 | 25.6 | 12 | 30.8 | 14 | 35.9 | 39 | 100.0 |
| 11 ランサムウェア | 1 | 2.6 | 1 | 2.6 | 14 | 35.9 | 23 | 59.0 | 39 | 100.0 |
| 12 セクストーション | 1 | 2.6 | 4 | 10.3 | 11 | 28.2 | 23 | 59.0 | 39 | 100.0 |

表 6：攻撃・脅威の理解（3 年商業科）（n=24）

| | 1 詳しい内容を知っている | | 2 概要をある程度知っている | | 3 名前を聞いたことがある | | 4 名前も概要も知らない | | 合計 | |
|---|---|---|---|---|---|---|---|---|---|---|
| # 項目 | 該当数 | % | 該当数 | % | 該当数 | % | 該当数 | % | 該当数 | % |
| 1 ワンクリック請求 | 5 | 20.8 | 14 | 58.3 | 3 | 12.5 | 2 | 8.3 | 24 | 100.0 |
| 2 パスワードリスト攻撃 | 1 | 4.2 | 3 | 12.5 | 7 | 29.2 | 13 | 54.2 | 24 | 100.0 |
| 3 フィッシング詐欺 | 3 | 12.5 | 6 | 25.0 | 8 | 33.3 | 7 | 29.2 | 24 | 100.0 |
| 4 セキュリティホール | 2 | 8.3 | 4 | 16.7 | 16 | 66.7 | 2 | 8.3 | 24 | 100.0 |
| 5 標的型攻撃 | 0 | 0.0 | 0 | 0.0 | 4 | 16.7 | 20 | 83.3 | 24 | 100.0 |
| 6 マルウェア | 1 | 4.2 | 1 | 4.2 | 3 | 12.5 | 19 | 79.2 | 24 | 100.0 |
| 7 偽セキュリティソフト | 0 | 0.0 | 4 | 16.7 | 8 | 33.3 | 12 | 50.0 | 24 | 100.0 |
| 8 DoS攻撃 | 1 | 4.2 | 1 | 4.2 | 7 | 29.2 | 15 | 62.5 | 24 | 100.0 |
| 9 ビジネスメール詐欺 | 0 | 0.0 | 8 | 33.3 | 11 | 45.8 | 5 | 20.8 | 24 | 100.0 |
| 10 偽警告 | 2 | 8.3 | 8 | 33.3 | 7 | 29.2 | 7 | 29.2 | 24 | 100.0 |
| 11 ランサムウェア | 1 | 4.2 | 0 | 0.0 | 6 | 25.0 | 17 | 70.8 | 24 | 100.0 |
| 12 セクストーション | 0 | 0.0 | 1 | 4.2 | 4 | 16.7 | 19 | 79.2 | 24 | 100.0 |

表 7：攻撃・脅威の理解（3 年情報科）（n=29）

| | 1 詳しい内容を知っている | | 2 概要をある程度知っている | | 3 名前を聞いたことがある | | 4 名前も概要も知らない | | 合計 | |
|---|---|---|---|---|---|---|---|---|---|---|
| # 項目 | 該当数 | % | 該当数 | % | 該当数 | % | 該当数 | % | 該当数 | % |
| 1 ワンクリック請求 | 13 | 44.8 | 15 | 51.7 | 1 | 3.4 | 0 | 0.0 | 29 | 100.0 |
| 2 パスワードリスト攻撃 | 7 | 24.1 | 12 | 41.4 | 9 | 31.0 | 1 | 3.4 | 29 | 100.0 |
| 3 フィッシング詐欺 | 11 | 37.9 | 16 | 55.2 | 2 | 6.9 | 0 | 0.0 | 29 | 100.0 |
| 4 セキュリティホール | 5 | 17.2 | 18 | 62.1 | 6 | 20.7 | 0 | 0.0 | 29 | 100.0 |
| 5 標的型攻撃 | 3 | 10.3 | 14 | 48.3 | 12 | 41.4 | 0 | 0.0 | 29 | 100.0 |
| 6 マルウェア | 7 | 24.1 | 10 | 34.5 | 12 | 41.4 | 0 | 0.0 | 29 | 100.0 |
| 7 偽セキュリティソフト | 6 | 20.7 | 9 | 31.0 | 10 | 34.5 | 4 | 13.8 | 29 | 100.0 |
| 8 DoS攻撃 | 10 | 34.5 | 14 | 48.3 | 5 | 17.2 | 0 | 0.0 | 29 | 100.0 |
| 9 ビジネスメール詐欺 | 2 | 6.9 | 8 | 27.6 | 14 | 48.3 | 5 | 17.2 | 29 | 100.0 |
| 10 偽警告 | 6 | 20.7 | 15 | 51.7 | 6 | 20.7 | 2 | 6.9 | 29 | 100.0 |
| 11 ランサムウェア | 9 | 31.0 | 9 | 31.0 | 11 | 37.9 | 0 | 0.0 | 29 | 100.0 |
| 12 セクストーション | 2 | 6.9 | 9 | 31.0 | 11 | 37.9 | 7 | 24.1 | 29 | 100.0 |

表 8：過去 1 年間のインターネット利用時の経験

| | | 全体N=92 | | 1 年情報科n=39 | | 3 年商業科n=24 | | 3 年情報科n=29 | |
|---|---|---|---|---|---|---|---|---|---|
| # | 項目<br>（全体の上位順） | 該当数 | % | 該当数 | % | 該当数 | % | 該当数 | % |
| 9 | 過去1年間で上記のような経験はない | 37 | 40.2 | 19 | 48.7 | 5 | 20.8 | 13 | 44.8 |
| 5 | ブラウザに突然「ウイルスに感染した」<br>などの警告画面が表示された | 22 | 23.9 | 9 | 23.1 | 6 | 25.0 | 7 | 24.1 |
| 2 | 本文中のURLにアクセスするようにうながす<br>不審なメールを受信した | 17 | 18.5 | 6 | 15.4 | 7 | 29.2 | 4 | 13.8 |
| 1 | 添付ファイルを開くようにうながす不審な<br>メールを受信した | 16 | 17.4 | 7 | 17.9 | 6 | 25.0 | 3 | 10.3 |
| 10 | 上記のようなトラブルや被害が<br>あったかどうかわからない | 12 | 13.0 | 6 | 15.4 | 4 | 16.7 | 2 | 6.9 |
| 3 | 第三者による不正アクセスを<br>試みられたというメールを受信した | 10 | 10.9 | 3 | 7.7 | 2 | 8.3 | 5 | 17.2 |
| 4 | 身に覚えのない支払いを求める（架空請求）<br>メールを受信した | 9 | 9.8 | 4 | 10.3 | 3 | 12.5 | 2 | 6.9 |
| 8 | アダルトサイトの登録完了画面が<br>突然表示された | 9 | 9.8 | 4 | 10.3 | 3 | 12.5 | 2 | 6.9 |
| 7 | インターネットバンキング利用中に<br>いつもと異なる不審な認証画面が表示された | 3 | 3.3 | 1 | 2.6 | 1 | 4.2 | 1 | 3.4 |
| 6 | カード会社からクレジットカードの不正利用の<br>可能性があるという連絡を受けた | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 |

と回答している生徒の割合が 1 年情報科は 19 名（48.7%），3 年情報科は 13 名（44.8%）であった。3 年商業科では，「2 本文中の URL にアクセスするようにうながす不審なメールを受信した」が 7 名（29.2%）であった。また，「10 上記のようなトラブルや被害があったかどうかわからない」と回答している生徒が，1 年情報科 6 名（15.4%），3 年商業科 4 名（16.7%），3 年情報科 2 名（6.9%）であった。

表 9 は，（設問 5）過去 1 年間，インターネット利用時に被害にあったかどうかの回答を学年・学科別に単純集計したものである。「14 過去 1 年間で上記のような被害はない」は，1 年情報科 31 名（79.5%），3 年商業科 13 名（54.2%），3 年情報科 22 名（75.9%）であった。3 年商業科は，「1 ウイルスに感染した（セキュリティソフトによる検出で実害にはいたらなかったケースを含む）」が 3 名（12.5%）であった。また，「15 上記のようなトラブルや被害があったかどうかわからない」と回答した生徒の割合が，1 年情報科 4 名（10.3%），3 年商業科 5 名（20.8%），3 年情報科 2 名（6.9%）であった。

次に実際のトラブルや被害につながる経験について分析した。表 10 は，設問 3，設問 4 の結果から，それぞれの攻撃・脅威について「知っている生徒」と「知らない生徒」で，設問 4 の

表 9：過去 1 年間のインターネット利用時の被害

| | | 全体N=92 | | 1 年情報科n=39 | | 3 年商業科n=24 | | 3 年情報科n=29 | |
|---|---|---|---|---|---|---|---|---|---|
| # | 項目<br>（全体の上位順） | 該当数 | % | 該当数 | % | 該当数 | % | 該当数 | % |
| 14 | 過去1年間で上記のような被害はない | 66 | 71.7 | 31 | 79.5 | 13 | 54.2 | 22 | 75.9 |
| 15 | 上記のようなトラブルや被害があったかどうか<br>わからない | 11 | 12.0 | 4 | 10.3 | 5 | 20.8 | 2 | 6.9 |
| 1 | ウイルスに感染した（セキュリティソフトによる<br>検出で実害にはいたらなかったケースを含む） | 4 | 4.3 | 0 | 0.0 | 3 | 12.5 | 1 | 3.4 |
| 13 | パソコンが突然作動しなくなってしまった | 4 | 4.3 | 2 | 5.1 | 1 | 4.2 | 1 | 3.4 |
| 4 | サービスに登録していた個人情報やパソコン<br>またはクラウドに保存していたデータが流出した | 3 | 3.3 | 1 | 2.6 | 0 | 0.0 | 2 | 6.9 |
| 2 | 利用しているサービスのアカウントが第三者に<br>不正にアクセスされた | 2 | 2.2 | 1 | 2.6 | 1 | 4.2 | 0 | 0.0 |
| 3 | 不審なメール送信の踏み台とされた<br>（身に覚えのないメールを送信されていた） | 1 | 1.1 | 0 | 0.0 | 1 | 4.2 | 0 | 0.0 |
| 5 | パソコンに保存していたファイルが暗号化されて<br>しまい利用できなくなった | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 |
| 6 | 不審なメール（および，その後の電話対応など）<br>の誘導に従って金銭を支払ってしまった | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 |
| 7 | ブラウザの警告画面の誘導に従って金銭を<br>支払ってしまった | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 |
| 8 | アダルトサイトの登録完了画面の誘導に<br>したがって金銭を支払ってしまった | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 |
| 9 | 暗号化されたファイルを復号するための手続き<br>という誘導に従って金銭を支払ってしまった | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 |
| 10 | クレジットカードが不正利用された<br>（実際に金銭被害にあった） | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 |
| 11 | インターネットバンキングの口座で<br>不正送金の被害にあった | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 |
| 12 | 偽ECサイトやオークションなど，支払いをしても<br>商品が届かないなどの詐欺の被害にあった | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 | 0 | 0.0 |

表 10：設問 4 の 9 トラブルや被害につながる経験がない生徒の割合（n=37）

| | | 知っている生徒 | | 知らない生徒 | | 合計 | |
|---|---|---|---|---|---|---|---|
| # | 項目 | 該当数 | % | 該当数 | % | 該当数 | % |
| 1 | ワンクリック請求 | 31 | 83.8 | 6 | 16.2 | 37 | 100.0 |
| 2 | パスワードリスト攻撃 | 16 | 43.2 | 21 | 56.8 | 37 | 100.0 |
| 3 | フィッシング詐欺 | 21 | 56.8 | 16 | 43.2 | 37 | 100.0 |
| 4 | セキュリティホール | 15 | 40.5 | 22 | 59.5 | 37 | 100.0 |
| 5 | 標的型攻撃 | 9 | 24.3 | 28 | 75.7 | 37 | 100.0 |
| 6 | マルウェア | 11 | 29.7 | 26 | 70.3 | 37 | 100.0 |
| 7 | 偽セキュリティソフト | 14 | 37.8 | 23 | 62.2 | 37 | 100.0 |
| 8 | DoS攻撃 | 17 | 45.9 | 20 | 54.1 | 37 | 100.0 |
| 9 | ビジネスメール詐欺 | 12 | 32.4 | 25 | 67.6 | 37 | 100.0 |
| 10 | 偽警告 | 19 | 51.4 | 18 | 48.6 | 37 | 100.0 |
| 11 | ランサムウェア | 8 | 21.6 | 29 | 78.4 | 37 | 100.0 |
| 12 | セクストーション | 11 | 29.7 | 26 | 70.3 | 37 | 100.0 |

表 11：設問 5 の 14 トラブルや被害にあった経験がない生徒の割合（n=66）

| | | 知っている生徒 | | 知らない生徒 | | 合計 | |
|---|---|---|---|---|---|---|---|
| # | 項目 | 該当数 | % | 該当数 | % | 該当数 | % |
| 1 | ワンクリック請求 | 58 | 87.9 | 8 | 12.1 | 66 | 100.0 |
| 2 | パスワードリスト攻撃 | 26 | 39.4 | 40 | 60.6 | 66 | 100.0 |
| 3 | フィッシング詐欺 | 39 | 59.1 | 27 | 40.9 | 66 | 100.0 |
| 4 | セキュリティホール | 27 | 40.9 | 39 | 59.1 | 66 | 100.0 |
| 5 | 標的型攻撃 | 14 | 21.2 | 52 | 78.8 | 66 | 100.0 |
| 6 | マルウェア | 17 | 25.8 | 49 | 74.2 | 66 | 100.0 |
| 7 | 偽セキュリティソフト | 24 | 36.4 | 42 | 63.6 | 66 | 100.0 |
| 8 | DoS攻撃 | 25 | 37.9 | 41 | 62.1 | 66 | 100.0 |
| 9 | ビジネスメール詐欺 | 20 | 30.3 | 46 | 69.7 | 66 | 100.0 |
| 10 | 偽警告 | 29 | 43.9 | 37 | 56.1 | 66 | 100.0 |
| 11 | ランサムウェア | 14 | 21.2 | 52 | 78.8 | 66 | 100.0 |
| 12 | セクストーション | 14 | 21.2 | 52 | 78.8 | 66 | 100.0 |

「9 過去 1 年間で上記のような経験はない（トラブルや被害につながる経験がない）」と回答した生徒の割合を単純集計したものである。

結果は，「1 ワンクリック詐欺」と「3 フィッシング詐欺」を除いて，「トラブルや被害につながる経験がない」生徒の内，「知らない生徒」の割合が 50%以上であった。

また，実際のトラブルや被害の経験についての結果（表 11）は，「1 ワンクリック請求」と「3 フィッシング詐欺」を除いて，「トラブルや被害にあった経験がない」生徒の内，「知らない生徒」の割合が 50%以上であった。

ここでも，先の「トラブルや被害につながる経験がない」生徒の場合と同様の結果となった。

以上が調査結果である。次節では，これらを踏まえて考察を進めたい。

# 4. 考察

## 4.1 全体の結果を通して

調査を通してみえてくるのは，情報機器の習熟度（設問 2）や，インターネット上の攻撃･脅威に対する知識に関して（設問 3），いずれも 1 年生情報科，3 年生商業科よりも 3 年生情報科が高いことや，トラブルや被害につながる経験（設問 4），また，実際にトラブルや被害にあった経験（設問 5）については，インターネット上の攻撃･脅威について「知っている生徒」の方が多いことである。

### 4.1.1 利用機器

設問 1 より普段プライベートでインターネットを利用する際には，どの学年・学科においても 90％を超える生徒がスマートフォンを活用している。情報科の生徒は，1 年次において，全員ノートパソコンの購入をしており，さまざまな授業の中で活用している。また，自宅に持ち帰って家庭学習に使用することも可としている。今回の調査時点においては，1 年情報科は，まだノートパソコンの購入をしていない。3 年情報科は，全員がノートパソコンを所持しているが，利用は 16 名（55.2%）にとどまっている。この結果より，インターネット接続する情報機器として，パソコンよりもスマートフォンを利用することが高校生にとって一般的であることがわかる。これは今後の情報教育を推進する際に使用する端末の選択について，前提として踏まえておくべき事項である。また，今後，社会に出て働く状況を考えた際にも，使用する情報端末を状況に応じて選択する能力の育成という視点が必要となってくる。

### 4.1.2 パソコン，スマートデバイスの習熟度

パソコンの習熟度に関しては，3 年情報科が高く，1 年情報科，3 年商業科については低い（設問 2-1)。また，スマートデバイス（スマートフォン・タブレット端末）の習熟度についても，3 年情報科が高く，1 年情報科，3 年商業科については低い（設問 2-2)。ここでは情報教育によって，パソコンやスマートデバイスの習熟度が高まるということということが明らかとなった。

### 4.1.3 インターネット上の攻撃・脅威に対する理解

インターネット上の攻撃･脅威については，3 年情報科の生徒がよく知っているという結果が得られた（設問 3)。ここでは，情報セキュリティ教育によって，インターネット上の攻撃や脅威についての知識が，向上したことがわかった。しかしその状況は予想したよりも低い水準であった。設問 3 におけるさまざまなインターネット上での攻撃・脅威についての学習は，授業等において多角的に取り入れられ実践されている。しかしそれぞれの攻撃や脅威に対する理解度は予想していたよりも低かった。授業等での取組があまり反映されていない結果となってい

る。今回の結果から，それぞれの攻撃・脅威についての理解度が明らかとなったのである。その結果をもとに，今後の授業展開にいかし，理解度の向上を図っていく必要がある。

#### 4.1.4　過去 1 年間のインターネット利用時における被害につながる経験や実際の被害

過去 1 年間のインターネット利用時における被害につながる経験（設問 4）や実際の被害（設問 5）について，被害にあっていない生徒の割合は情報科の生徒の方が多かった。ここでは，情報セキュリティ教育が，インターネット利用時における被害につながる経験や実際の被害の防止に一定役立っていると考えられる。これは，情報セキュリティ教育の重要性を示す大きな要素であると考える。しかし，「知っている生徒」の方が，トラブルや被害につながる経験が少ないと予想していたが，「知らない生徒」の方が少ないという逆の結果が得られた。また，実際にトラブルや被害にあった経験についても同様の結果となった。この結果は，情報セキュリティ教育を推進していくにあたっての課題といえる。

これらのことから，情報セキュリティ教育の実践が，情報セキュリティに関する攻撃や脅威についての知識を高め，情報セキュリティインシデント遭遇の減少に関連していることがいえる。この点は，情報セキュリティ教育の成果の一つといえる。

しかし実際の被害を食い止めることにつながっていない状況があるということがわかった。3 年情報科の生徒は，情報セキュリティ教育によって知識・技術を得たことによる慢心があったということが考えられる。この点は，情報セキュリティ教育がもたらす負の一面と捉える必要があり，教育の在り方を問う大きな課題である。

### 4.2　課題解決に向けて

これらのことから，本研究の目的である A 高等学校の情報セキュリティ教育の実践が，高校生の情報セキュリティに関する状況にどのような効果をもたらしているのかを分析することを通して課題を明らかにすることができた。

こうした一面の要因には，授業で行っている内容は，最新の動向に留意して扱っているものの，攻撃手法が日々進化していることがあげられる。この点について，情報セキュリティにおいては，未知の攻撃手法に対応できる能力が重要であり，高等学校学習指導要領（平成 30 年告示）解説「情報編」[11]においても，「情報セキュリティに関する諸問題に対し，具体的な事例を通して主体的に考えるようにする。また，このような学習活動を通して，情報技術者の社会における責任と果たすべき役割を理解し，新たな問題に対して継続的に取り組む重要性を理解できるようにする。」と示されている。

心理面での問題点克服への一つの示唆として，内田が提唱する情報セキュリティ分野への心理学の適用について考えたい。内田（2012）は，「人間の弱さを攻撃側が利用しているのであれば，その調査分析により対応を考えるだけでなく，攻撃側や防御側の分析やセキュリティ対策

等に心理学や行動科学，社会学等の知見を利用することは，「敵を知り，己を知らば，百戦危うからず」であろう。」と述べている[12]。情報セキュリティといえば，一般的には，サイバーセキュリティを想起する人が多い。しかし，情報セキュリティには，サイバー空間だけではなく，私たちの普段の社会生活においても対策を必要とする場面が多々ある。具体的には，「ソーシャル・エンジニアリング」という攻撃手法がある。この攻撃は，話術や盗み聞き・盗み見等を利用し，人間の心理・行動の隙を突くことで情報を不正に取得する手段の総称である。日々報道でとりあげられている「振り込め詐欺」に類するものもソーシャル・エンジニアリングの一種であるといえる。この振り込め詐欺について，内田（2012）は，「電話によるソーシャルエンジニアの凄さは実際に経験しないと分かり難いかも知れない。国内では「自分は被害者にならない」，「被害者は高齢者だけでは？」との話が「振り込め詐欺」であるが，被害者年齢をみると，60 歳未満が約 22 % あり，被害者は高齢者だけではない。」と指摘する[13]。この例をみても，自分は高齢者ではないから大丈夫だという慢心が被害につながっていることが伺える。そしてまた，サイバー空間における攻撃も，この人間の心理や行動を巧みに突いたものが多いといえる。これらのことから，情報セキュリティ対策においては，専門的な知識・技術だけではなく，人間そのものの脆弱性についての理解が重要であるといえる。内田ら（2007）[14] は，Kevin Mitnick 等が示している「6 つの人間の脆弱性」をあげている。これは，何かを与えてくれた人に対してお返しをせずにはいられない気持ちになることを利用した「返報性」，自由意思によりとった行動がその後の行動にある拘束をもたらす「コミットメントと一貫性」，他人が何を正しいと考えているかによって，自分が正しいかどうかを判断する特性を利用した「社会的証明」，好意を持っている人から頼まれると，承諾してしまうことを利用した「好意」，権限を持つ者の命令に従ってしまうことを利用した「権威」，手に入りにくい物であるほど，貴重なものに思え，手に入れたくなってしまう特性を利用した「希少性」の 6 つの要素からなっている。

情報セキュリティ教育においては，このような人間の心理や行動の特性についても踏まえた授業計画の必要性がある。これらの点については，さらに検証を行い，これまでの授業実践の改善を図ることが重要となる。

また，高等学校学習指導要領（平成 30 年告示）解説「情報編」では[15]，「情報セキュリティ技術について，その仕組みを理解し活用できることが必要である。そのために生徒や地域の実態及び学科の特色等に応じた情報セキュリティ技術を選択し，実習を効果的に取り入れて扱うことが大切である。」と示されている。A 高等学校においては，この点に留意し，情報セキュリティ教育の実践が行われてきている。情報セキュリティ教育は，その学習を深めていく過程において，攻撃手法を知る機会となる場合も多い。この点については，どの学習段階において，どの内容を扱うのかということについて，慎重に選択しなければならない。情報セキュリティ教育は，「諸刃の剣」である点に留意する必要がある。

情報セキュリティ教育は，情報モラルや道徳的な人間形成のもとに成り立つ。特に専門教科

「情報」においては，情報技術者をめざす生徒の育成を通して，技術者倫理にまで高めた倫理観の涵養が求められるといえよう。

## 5. おわりに

本研究により，情報セキュリティ教育の実践が，情報セキュリティに関する攻撃や脅威についての知識を高め，情報セキュリティインシデント遭遇の減少に関連していることがわかった。この点は，情報セキュリティ教育の成果の一つといえる。しかし一方で実際の被害を食い止めることにつながっていない状況がある。この点が，本研究により明らかとなった問題点であり，この問題の克服が課題である。考察によって導き出した取組を教育活動の中で実践し，その結果をあらためて調査することによってさらなる検証を進める必要がある。

情報セキュリティを取り巻く状況は，日々刻々と変化している。サイバー攻撃をはじめとした攻撃手法は，日々進化している。その攻撃を防御するためには，防御方法も進化させ対応しなければならない。情報セキュリティ教育においては，情報セキュリティの基本的な知識・技術を習得するとともに，変化する状況に対応していく必要がある。そのためには，常に新しい教育内容の検討と教員の不断の研鑽が必要となる。また，最新の状況を教育内容に反映させるためには，産官学をはじめとした学校外部との連携が重要となってくる。

今後，専門教科「情報」だけでなく，初等中等教育の各段階における情報セキュリティ教育の在り方を検討し，構築していく必要がある。専門教科「情報」における情報セキュリティ教育の実践事例が一つのモデルとなり，共通教科「情報」や，さらには中学校，小学校での教育実践へと広げていくことができればと考える。

〔注〕

1　独立行政法人情報処理推進機構セキュリティセンター .「情報セキュリティ 10 大脅威」. 2018.

2　増山一光 .「学校設定科目によるコンピュータウイルス対策教育の実践」.『教育情報研究 27 巻 3 号』. 2012, pp.15-25.

3　増山一光，佐藤直 .「SSH 校における情報セキュリティを重視した無線 LAN 教育の実践」.『情報教育シンポジウム 2010 論文集（6）』. 2010, pp.34-41.

4　佐藤直 , 西郡裕子 , 中島尚樹 , 西山賢志郎 , 武藤幸一 , 山田恭弘 .「県立高校における「サイバーセキュリティ技術実践授業」の実施について」.『情報処理学会第 79 回全国大会　講演論文集』. 2017, pp.727-728.

5　増山一光 .「高校生に対する情報セキュリティ教育の教授法に関する研究－インストラクショナルデザインによる実践－」. 情報セキュリティ大学院大学 , 2013, 博士論文 .

6　田中浩治 , 池田満 , 園田未来 , 堀雅洋 .「情報モラル行動における知識と行動の不一致に関する心理実験的検討」.『日本教育工学会論文誌 40 巻 3 号』. 2016, pp.153-164.

7　宮崎智絵 .「ICT 活用教育と高校教科「情報」における情報倫理教育」.『立正大学教職教育センター年報第 2 号』. 2020, pp.61-73.

8　小熊良一 , 山本利一 , 在間拓幹 .「小・中学校教員の情報セキュリティに関する「意識」「行動」「知識」に関する調査」.『教育情報研究 36 巻 1 号』. 2020, pp.13-24.
9　独立行政法人情報処理推進機構セキュリティセンターセキュリティ対策推進部 .「2019 年度情報セキュリティに対する意識調査」. 2019.
10　小熊良一 , 山本利一 .「義務教育における情報セキュリティ教育の現状と課題」.『群馬大学教育学部紀要．芸術・技術・体育・生活科学編 2020, 55』. 2020, pp.79-90.
11　文部科学省 .「高等学校学習指導要領解説「情報編」」. 2018.
12　内田勝也 .「情報セキュリティ心理学：人的側面からの情報セキュリティ」.『情報の科学と技術 62 巻 8 号』. 2012, pp.336-341.
13　内田勝也 . 2012. 前掲書 .
14　内田勝也 , 矢竹清一郎 , 森貴男 , 山口健太郎 , 東華枝 .「情報セキュリティ心理学の提案」.『情報処理学会研究報告 . DPS, マルチメディア通信と分散処理研究会報告 130』. 2007, pp.327-331.
15　文部科学省 . 2018. 前掲書 .

**〔付表〕質問紙**

設問 1　あなたが普段プライベートでインターネットサービスを利用している機器を，すべて答えてください。
1 パソコン
2 スマートフォン
3 タブレット端末（iPad, MediaPad, ZenPad, Kindle Fire 等）
4 携帯電話（フィーチャーフォン）
5 ゲーム機器（ニンテンドー 3DS，PS4 等）
6 その他
7 プライベートでインターネットサービスの利用は無い

設問 2-1　あなたのパソコンの習熟度として，最もあてはまるレベルを回答してください。（答えは 1 つ）
1 パソコンに関する十分な知識を有しており，具体的な操作方補うやトラブル発生時の対応について他者に説明することができるレベル
2 パソコンに関する基本的な知識を有しており，具体的な操作方法やトラブル発生時の対応等は自分で調べて対処することができるレベル
3 パソコンの基本的な操作や簡単な操作や簡単な設定変更はでき，予期せぬ挙動やエラーが発生した場合も他者からの説明があれば理解，対応できるレベル
4 パソコンの基本的な操作はできるが，設定変更等は自分ではできず他者にお願いをする必要があるレベル

設問 2-2　あなたのスマートデバイス（スマートフォン・タブレット端末）の習熟度として，最もあてはまるレベルを回答してください。（答えは 1 つ）
1 スマートデバイスに関する十分な知識を有しており，具体的な操作方法やトラブル発生時

の対応等について他者に説明することができるレベル
2 スマートデバイスに関する基本的な知識を有しており，具体的な操作方法やトラブル発生時の対応等は自分で調べて対処することができるレベル
3 スマートデバイスの基本的な操作や簡単な設定変更はでき，予期せぬ挙動やエラーが発生した場合も他者からの説明があれば理解，対処できるレベル
4 スマートデバイスの基本的な操作はできるが，設定変更等は自分ではできず他者にお願いする必要があるレベル

設問 3　あなたは，次のようなインターネット上での攻撃・脅威などについて知っていますか。あてはまるものをそれぞれ 1 つずつ選択してください。（答えはそれぞれ 1 つ）
（以下の攻撃・脅威に対する選択肢）
1 詳しい内容を知っている
2 概要をある程度知っている
3 名前を聞いたことがある
4 名前も概要も知らない
（攻撃・脅威）
1 ワンクリック請求
2 パスワードリスト攻撃（リスト型アカウントハッキング）
3 フィッシング詐欺
4 セキュリティホール（脆弱性）
5 標的型攻撃
6 マルウェア
7 偽セキュリティソフト
8 DoS（サービス妨害）攻撃
9 ビジネスメール詐欺（BEC）
10 偽警告（サポート詐欺）
11 ランサムウェア
12 セクストーション（性的脅迫）

設問 4　あなたは過去 1 年間，インターネット利用中に次にあげるような経験をしたことがありますか。あてはまるものをすべて選択してください。（答えはいくつでも）
1 添付ファイルを開くようにうながす不審なメールを受信した
2 本文中の URL にアクセスするようにうながす不審なメールを受信した
3 第三者による不正アクセスを試みられたというメールを受信した（実際に不正アクセスの被害にはいたらない）
4 身に覚えのない支払いを求める（架空請求）メールを受信した
5 ブラウザに突然「ウイルスに感染した」などの警告画面が表示された
6 カード会社からクレジットカードの不正利用の可能性があるという連絡を受けた（実際の金銭被害までにはいたらない）

7 インターネットバンキング利用中にいつもと異なる不審な認証画面が表示された
8 アダルトサイトの登録完了画面が突然表示された
9 過去 1 年間で上記のような経験はない
10 上記のようなトラブルや被害があったかどうかわからない

設問 5　あなたは過去 1 年間，インターネット利用中に次にあげるような被害にあったことがありますか。あてはまるものをすべて選択しなさい。（答えはいくつでも）
1 ウイルスに感染した（セキュリティソフトによる検出で実害にはいたらなかったケースを含む）
2 利用しているサービスのアカウントが第三者に不正にアクセスされた
3 不審なメール送信の踏み台とされた（身に覚えのないメールを送信されていた）
4 サービスに登録していた個人情報やパソコンまたはクラウドに保存していたデータが流出した
5 パソコンに保存していたファイルが暗号化されてしまい利用できなくなった
6 不審なメール（および，その後の電話対応など）の誘導に従って金銭を支払ってしまった
7 ブラウザの警告画面（および，その後のソフト購入や電話対応など）の誘導に従って金銭を支払ってしまった
8 アダルトサイトの警告画面（および，その後の電話対応など）の誘導に従って金銭を支払ってしまった
9 暗号化されたファイルを復号するための手続きという誘導に従って金銭を支払ってしまった
10 クレジットカードが不正利用された（実際に金銭被害にあった）
11 インターネットバンキングの口座で不正送金の被害にあった
12 偽 EC サイトでのショッピングやオークションなど，支払いをしても商品が届かないまたは別商品であったといった詐欺の被害にあった
13 パソコンが突然作動しなくなってしまった（原因はウイルスや不正アクセスに限らず，故障や劣化なども含む）
14 過去 1 年間で上記のような被害はない
15 上記のようなトラブルや被害があったかどうかわからない

（おのえ　だり　教育学研究科生涯教育専攻修士課程修了）
（指導教員：原　清治 教授）
2021 年 9 月 29 日受理