

# 学校設定科目を用いた 情報セキュリティ教育の実践

増山一光<sup>†, ††</sup> 佐藤直<sup>†</sup>

神奈川県立神奈川総合産業高等学校では、高等学校における情報セキュリティ教育の必要性から学校設定科目として「情報セキュリティ」を設置している。そこで、授業実践としてコンピュータウイルスとファイル共有ソフトについて取り上げる。これらの実践から、情報セキュリティインシデントへの対策能力の向上と適切な情報モラルの形成について考察する。そして、高等学校での情報セキュリティ教育の課題を明らかにする。

## A practice of information security education using school setting subjects

Kazumitsu Masuyama<sup>†, ††</sup> and Naoshi Sato<sup>†</sup>

Kanagawa prefectural Kanagawa sogo sangyo high school is executing “information security” as a school setting subject. Based on the experience of teaching, we discuss improvement of ability to deal with information security incidents, and establishment on information ethics. Further we clarify issues of information security education in high school.

### 1. はじめに

#### 1.1 背景

今日、情報セキュリティは国民的課題となっており、わが国の情報セキュリティの取り組みを推進する計画としては、第2次情報セキュリティ基本計画[1]がある。このなかの重点政策における4つの領域の1つとして、個人に対する取り組みが次のよう

に示されている。

- ・情報セキュリティ教育の強化・推進
- ・個人の底上げに向けたより効果的な普及・啓発活動の実現
- ・対策が困難な個人も含めた情報セキュリティ水準向上に向けた取り組み

このことから、情報セキュリティに対して教育が果たすべき役割が大きくなってきている。特に高校生は次世代の情報セキュリティを担う人材であり、情報セキュリティに対して適切な対応と行動をとることができる能力と態度を育成していかなければならない。そのため、高等学校において情報セキュリティ教育の実現が必要不可欠になってきている。

一方で、高校生に対する情報セキュリティインシデントによる被害が急増している。具体的な被害状況に関する調査である「高校生のCGM（消費者生成メディア）利用実態」[2]によると、高校生の約3割は過去にコンピュータウイルスの被害に遭遇し、半数以上は有害情報に接している。実際に本稿で扱う神奈川総合産業高等学校における学校設定科目「情報セキュリティ」における受講生徒の事前調査でも、33%の生徒がコンピュータウイルスの被害に遭っている。さらに、ウイルス対策ソフトをインストールしていない生徒も18%に上っている。このようなことから、高校生に対する情報セキュリティ教育の実施が急務となっている現状がある。

#### 1.2 先行研究

これまで情報セキュリティ教育は、大学もしくは大学院を中心にして行われてきた。たとえば、工学系大学や産学共同での情報セキュリティ教育の実践が報告[3][4]されている。同様に人文系大学生を対象にした実践[5]もみられる。こうしたから、情報セキュリティ教育は、理系や文系を問わず広く実践されている教育活動であるといえる。

高等学校では2003年度より教科「情報」が設置され、情報教育が展開されている。この中で、情報セキュリティに関する項目は各科目の学習分野として扱われている。しかし、情報セキュリティの内容が広範囲かつ高度であるため、体系的な学習が行われているわけではなく、断片的な知識と技能にとどまっているのが現状である。

他方、情報モラル教育は初等中等教育において積極的に行われている。これには、情報モラルに起因する事件・事故が発生したことが影響しているとともに、情報機器の保有の低年齢化が進行しているからである。具体的な取り組みとしては、情報モラルに関する教材開発[6]、チャットを用いた授業実践[7]、学校と家庭との連携[8]などがあげられる。

こうした状況から、高等学校において求められる情報セキュリティ教育は、発達段階に応じた情報モラルを基盤とし、情報セキュリティに関する導入的な内容で行われるべきである。

<sup>†</sup> 情報セキュリティ大学院大学  
Institute of Information Security

<sup>††</sup> 神奈川総合産業高等学校  
Kanagawa Sogo Sangyo High School

### 1.3 本研究の目的

本研究の目的は、神奈川県立神奈川総合産業高等学校における学校設定科目「情報セキュリティ」での授業実践によって、情報セキュリティインシデントへの対策能力が向上し、情報セキュリティに関する事象に対して適切な情報モラルが育成されているかについて考察を行うことである。

情報セキュリティインシデントへの対策能力については、情報セキュリティインシデントに対する知識を含めた対策能力の変化に着目する。生徒の中には、情報セキュリティインシデントへの対応があまりできていないものも少なくない。そこで、ここではコンピュータウイルスを取り上げ、対策能力の向上がみられるかを検証する。

情報モラルの形成については、形成されている情報モラルの特質や構造などに着目する。そこで、ここではファイル共有ソフトを取り上げ、授業を受けている生徒集団を対象とした情報モラルの分析を行うことで、適切な情報モラルが形成されているかを検証する。

## 2. 学校設定科目「情報セキュリティ」

### 2.1 学校設定科目の設定の背景

神奈川総合産業高等学校は 2005 年に単位制専門高校として開校した。本校の教育課程では、情報系において様々な科目を展開している。そのなかで、情報セキュリティに対する適切な能力と態度を育成する必要から、情報系の科目の 1 つとして学校設定科目「情報セキュリティ」を設置している。

なお、学校設定科目とは、学習指導要領[9]において、地域、学校及び生徒の実態、学科の特色等に応じ、特色ある教育課程の編成に資するために設定された科目となっている。

### 2.2 学習目標

学校設定科目「情報セキュリティ」の科目の目標としては、「情報セキュリティに関する基本的な知識を学び、情報システムのセキュリティポリシーの策定および実施、分析、見直しができるようにする」となっている。このような目標の実現に向けて、高校生としての情報セキュリティに対する意識と能力を向上させるとともに、将来的には、実社会の所属組織において情報セキュリティ対策を担える人材の育成を目指している。

この科目において、生徒に育成すべき能力としては、第 1 に情報セキュリティインシデントに対応する能力がある。これは日常生活において発生するインシデントに対して、被害を最小限にすることができる能力のことである。第 2 に情報セキュリティに対するリスクを想定する能力であり、情報システムの利用や情報の取り扱いにおい

て、常時、新たなリスクを想定しつつ行動する能力のことである。第 3 に情報セキュリティに関する情報収集能力であり、日々発信される情報セキュリティに関する情報の収集・分析・活用を行える能力のことである。

さらに、情報モラルについては授業全体を通じて必ず育成しなければならないものである。これは、情報セキュリティを支える基盤となる態度であるとともに、情報セキュリティの実現に向けたモチベーションになるからである。

### 2.3 科目内容

学校設定科目「情報セキュリティ」の 2010 年度後期の科目内容は表 1 の通りである。情報セキュリティに関する内容は広範囲に及び、その内容が高度なものも少なくない。高等学校における時間の限られた授業において、そのすべてを扱うことは不可能である。こうしたことから、授業の対象となる生徒のコンピュータや情報に関する知識の程度やその利用状況を把握して、科目内容を絞り込んだ。

表 1 学校設定科目「情報セキュリティ」における科目内容  
Table1 "information security" curriculum.

内容のまとめ	単元
総論	・情報セキュリティの定義
マルウェア対策	・コンピュータウイルス ・ファイル共有ソフト ・BOT
ユーザインシデント対策	・スパムメール ・フィッシング詐欺
暗号、認証	・暗号と認証
マネジメント	・個人情報漏えい ・不正アクセス ・セキュリティポリシー
まとめ	・情報セキュリティの動向

本校では、この科目を半期 1 単位科目として、1 コマの授業を 90 分で実施している。コンピュータウイルス及び暗号と認証は 2 コマで行っているが、他の内容は 1 コマで行っている。科目内容だけを見ると、あまり関連性のない項目の羅列になっているが、それぞれの科目内容で関連性を持たして授業展開を行っている。これにより、様々なリスクの実態を把握するとともに、複合的な情報セキュリティインシデントにも対応できる能力の育成を目指している。

### 3. 授業実践と研究方法

ここでは、学校設定科目「情報セキュリティ」におけるコンピュータウイルス、ファイル共有ソフトに関する授業実践を示すことにする。そのなかで、それぞれの内容における情報セキュリティに関する能力を育成するための学習活動を中心に上げる。なお、授業実施の概要は次の通りである。

- ①対象：高校2年生及び3年生
- ②人数およびクラス：20人と36人の2クラス展開（2010年度後期）  
高校3年生（男子：23人，女子：10人）  
高校2年生（男子：18人，女子：5人）
- ③実施場所：本校教室
- ④実施時期：コンピュータウイルス（2010年10月14，15日）  
ファイル共有ソフト（2010年11月4，12日）

#### 3.1 コンピュータウイルス

##### 3.1.1 授業実践

高校生にとって最も身近な情報セキュリティインシデントの1つとして、コンピュータウイルスがある。これに関する授業内容は表2の通りである。

授業の1時間目はコンピュータウイルスの定義、種類、歴史など基本的な内容を取り上げたうえで、コンピュータウイルスの現状について示した。2時間目はコンピュータウイルス対策を中心に授業を行い、感染前と感染後の具体的な対処法について、擬似的な実践を踏まえて授業展開をした。

特に、2時間目に行ったコンピュータウイルス対策の授業では、まず事前策としてウイルス対策ソフトのインストールの徹底とパターンファイルの更新が有効であることを説明した。実際には、高校生はこの最も基本的な対策を行っていないものが少なくないので、コンピュータウイルスによる感染自体を把握できていないのが現状であり、加害者になってしまうことも多くなっている。

次に、コンピュータウイルスに感染した際の対策方法の具体的な手順を示しながら、擬似的な実演を交えて授業展開を行った。このなかで、ウイルスの駆除に関してはウイルス対策ソフト以外での手法をほとんど知らない状況であったので、専用ツールの活用や手動での駆除方法を示した。

##### 3.1.2 研究方法

この授業実践において、情報セキュリティインシデントへの対応能力の向上をみるための研究方法として、コンピュータウイルスへの対策能力に関して2回のアンケート調査を行った。1回目の調査はコンピュータウイルスの1時間目の授業において学習した後に実施した。調査形式としては、「コンピュータウイルスに感染した場合に、どのような対応をとるか」という問いに対して、箇条書きで回答するものである。な

お、この段階ではコンピュータウイルスへの感染対策の授業は行っておらず、生徒が事前に対策法をどのくらい理解しているかを知るための調査である。2回目の調査は、コンピュータウイルスへの対策を学習し、さらに他の情報セキュリティインシデント対策を学習した上で、1回目の調査の約2か月後に実施した。

表2 コンピュータウイルスの授業内容

Table2 Content of the subject on computer virus.

<1時間目>
・コンピュータウイルスの定義
・コンピュータウイルスの種類
・コンピュータウイルスの歴史
・コンピュータウイルスへの感染状況
-----
<2時間目>
・コンピュータウイルスに感染する前の対策
-ウイルス対策ソフトの有効利用について
・コンピュータウイルスに感染後の対策
-具体的なウイルス駆除方法について

#### 3.2 ファイル共有ソフト

##### 3.2.1 授業実践

ファイル共有ソフトに関しては、多くの生徒がWinny利用の危険性を理解している。これは暴露ウイルスによって個人情報漏えいがもたらされることに起因している。一方では、ファイル共有ソフトの技術的側面やWinny裁判など、多面的に考察すべき点がある。このようなことを踏まえ、授業内容は表3の通りとした。

まず、ファイル共有ソフトの概要とその仕組みについての授業を展開した。その過程において、Winnyの製作者の著書[10]を参考にすることでその動作を示し、さらにはファイル共有ソフトの利用による著作権の侵害や個人情報漏えいなどの問題点を明確にした。

次に、Winny裁判の1審と2審の新聞記事を配布して、技術的側面とこれまでに指摘した利用によって生じる問題点の両面からファイル共有ソフトに関して考えさせた。学習活動としては、発問をしてそれに答えさせる形で考え方を整理させていった。

さらに、ケーススタディを行った。ここで、「Winny利用の果て」[11]というファイル共有ソフトの利用によって発生した事件を例として取り上げ、どのような対応をすればよかったのかを考えさせた。具体的には、プリントに対応を記述する方式で行った。

### 3.2.2 研究方法

この授業実践において、適切な情報モラルの形成に関する研究方法として、まず、ファイル共有ソフトが抱える様々な問題点を各生徒に指摘させた。次に、これらの指摘されたものを集団の意見として再構成させ、授業を受講している集団においてどのようなものが形成されているかについて分析を試みることにした。

具体的には、授業で行ったケーススタディを踏まえて、「ファイル共有ソフトにおいて、何が問題であるか」という問いに対して自由記述で回答させた。ここで得られたものを分解して、カテゴリー化による再構成を行うことで、集団内にどのような構造の情報モラルが形成されているかを示すことにした。

表3 ファイル共有ソフトの授業内容  
 Table3 Content of the subject on file-sharing software.

- ・ファイル共有ソフトとは
- ・ファイル共有ソフトの仕組みと問題点
- ・Winny 裁判
- ・ファイル共有ソフトの世界的利用状況
- ・ケーススタディ

## 4. 結果と考察

### 4.1 情報セキュリティインシデントへの対策能力の向上

ここでの調査は、箇条書きでコンピュータウイルスへの対策を記述するものであることから、これらに対する評価が必要になる。この評価については、記述内容からコンピュータウイルスに感染した時の対策となるものを抽出して、点数化する方法をとった。具体的には、それぞれの個別対策を1つ1点として評価し、記述された文章における全得点を算出するものである。なお、個々の対策に重み付けをしないで、すべて同一の点数で評価したのは、多くの対策手法を理解しているかという点に着目したためである。

表4は、第1回調査におけるコンピュータウイルスへの対策内容との回答数に関するものである。第1回の調査段階ではコンピュータウイルスへの対策についての授業は行っていないが、状況としては、ほとんどの生徒がコンピュータウイルスへの対策ができていないことがわかる。

まず、表4から最も基本的な対策であるウイルス対策ソフトの利用に関して、8件しか回答されていないことがわかる。これは、ウイルス対策ソフトの処理が自動化したことにより、インストールしていることを意識していない生徒が増えてきているこ

とを示している。また、インストールしているウイルス対策ソフトを活用する方法を知らない生徒も少なくないのである。

次に、表4において、第3者への相談、パソコンを使用しない、業者等への修理依頼といった回答が多いことから、自らが能動的にコンピュータウイルスに対応する生徒が少ないといえる。この理由として、近年、OSのセキュリティが向上し、様々な対策がとられることにより、コンピュータウイルスに感染することが少なくなっているため、自ら対応する機会が減少してきていることが考えられる。

表4 第1回調査の回答結果  
 Table4 Results of the first survey.

対策内容	件数
第3者への相談	22
対策方法等の調査	15
ネットワークの切断	14
パソコンを使用しない	12
ウイルス対策ソフトの使用	8
OSなどの再インストール	5
データのバックアップ	5
業者等への修理依頼	5
その他	4
合計	90

また、図1は生徒個人の得点の分布を示したヒストグラムである。図1から、多くの生徒が1ないしは2程度の得点しか挙げていないことがわかる。このことからコンピュータウイルスへの対策をほとんど知らない状況にあるといえる。

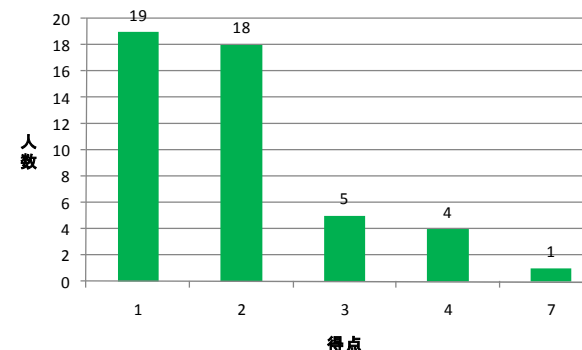


図1 第1回調査での得点別ヒストグラム  
 Figure1 Histogram of the first survey.

第2回調査は、コンピュータウイルスや様々な情報セキュリティインシデント対策に関する授業を行い、第1回調査の約2か月後に実施したものである。その結果が表5と図2である。

表5 第2回調査の回答結果  
Table5 Results of the second survey.

対策内容	件数	対策内容	件数
ウイルス対策ソフトの使用	41	復元ポイントの利用	7
ネットワークの切断	33	専用ツールでの駆除	7
システムの更新	23	データのバックアップ	5
ウイルスチェック	20	ルータの導入	4
対策方法等の調査	16	業者等への修理依頼	4
第三者への相談	13	オンラインスキキャン	4
パソコンを使用しない	12	被害調査	3
OSなどの再インストール	9	手動駆除	3
ファイアウォール	8	その他	9
		合計	221

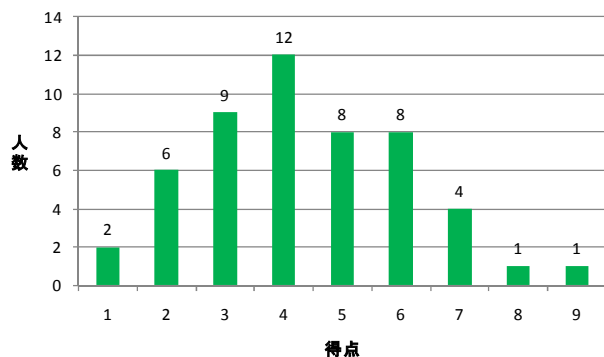


図2 第2回調査での得点別ヒストグラム  
Figure2 Histogram of the second survey.

表5から、第2回調査では第1回調査よりも多様な対策内容が回答されていることがわかる。これは、学校設定科目「情報セキュリティ」の授業を通じて多くの対策を学習した成果であるといえる。特に、第2回調査ではコンピュータウイルスへの最も

基本的な対策であるウイルス対策ソフトの利用、ネットワークの切断、システムの更新、ウイルスチェックなどが上位を占めるようになっている。

図2は第2回調査における生徒個人の得点の分布を示したヒストグラムである。各個人の得点については図1と比較しても得点分布に変化がみられ、高得点となっていることがわかる。さらに、図3に第1回調査と第2回調査の平均点の推移を示す。図3より、全体では、第1回調査の平均点は1.91(標準偏差=1.64)であったのに対し、第2回調査の平均点は4.33(標準偏差=3.38)になっている。また、図3では全体だけでなく、各集団(高校2,3年生男女)の平均点の推移も示した。全ての集団において第1回調査よりも第2回調査の平均点が向上していることがわかる。

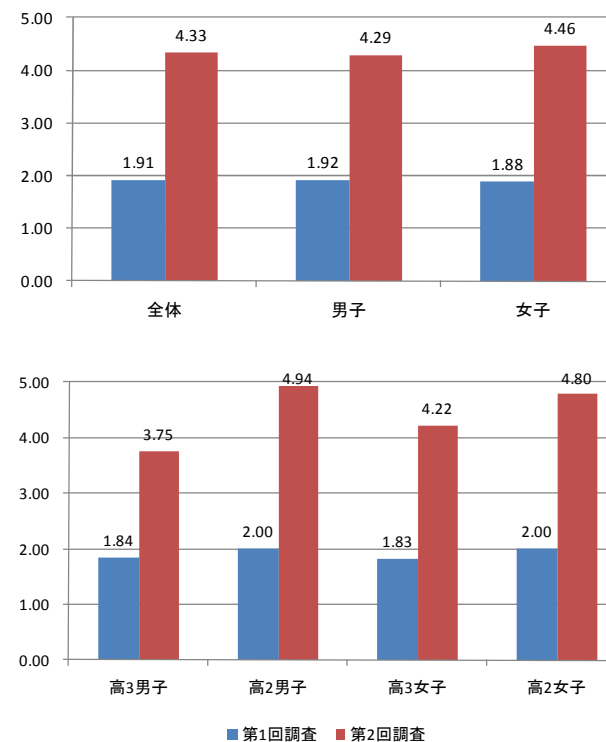


図3 調査における平均点の推移  
Figure3 Change in average scores on survey.

ここで、第1回調査と第2回調査の平均点の推移に対してt検定(片側検定)を行うことにする。まず、全体としては有意差( $t=7.59$   $df=90$   $P<.01$ )が認められた。男子間( $t=6.34$   $df=66$   $P<.01$ )と女子間( $t=4.00$   $df=19$   $P<.01$ )でも同様に有意差が認められる。次に、各学年男女別でみると、高3男子( $t=4.35$   $df=34$   $P<.01$ )、高2男子( $t=4.90$   $df=30$   $P<.01$ )、高3女子( $t=2.60$   $df=13$  n.s.)、高2女子( $t=5.71$   $df=4$   $P<.01$ )となり、高3女子については有意差が認められなかったが、他の集団では有意差が認められた。以上から、おおむね授業実践によりコンピュータウイルスを中心とした情報セキュリティインシデントへの対策能力が向上したといえる。

## 4.2 適切な情報モラルの形成

### 4.2.1 情報モラルのカテゴリー化に対する評価

前述の通り、生徒が「ファイル共有ソフトにおいて、何が問題であるか」という問いに対して、自由に記述する形式で回答させた。自由記述であることから、生徒によって文章の量の違いがみられるとともに、内容についても1つの事項について深化させるような記述や自らの考えを列挙する記述など多様な結果が得られた。

このような生徒の記述を分析することで、授業における集団の情報モラルの形成を確認する。各個人の記述内容に対する分析であることから、その手法としては、グラウンデッドセオリアプローチ[12]による質的な分析を用いる。

分析の手順として、はじめに、データの切片化、すなわち、有意な回答内容に分解し短い記述で表現する作業を行う。さらに、この分解した内容が同一の内容のものである場合、1つのカテゴリーにまとめる。こうした作業を行うことで、集団における情報モラルに関する意見をカテゴリー化する。

さらに、このカテゴリー化した項目に対して、情報モラルの視点から評価を行うために、玉田ら[13]が提案している情報モラル教育に求められる「3種の知識」のいずれであるかを当てはめる。「3種の知識」とは、道徳的規範知識、情報技術の知識、合理的判断の知識から構成されている。道徳的規範知識とは、小中学校の道徳の学習目標の中で特に情報モラル判断に直接的に関係するものであり、節度、正義、思いやりなどが含まれる。情報技術の知識とは、情報技術の特性、仕組みや関連する法律の知識が含まれる。合理的判断の知識とは、道徳規範知識と情報技術の知識を組み合わせた枠組みになっている。

実際に今回の調査をカテゴリー化したものが図4である。図中ではカテゴリー化した結果を、1つ1つを四角形にまとめ、四角形内の太字が意見を集約した表題(カテゴリー名)で、これに属する代表的な意見を列挙したものである。なお、括弧内は意見の数を表している。

図4において、白い四角形のカテゴリーはファイル共有ソフトの利用に関するもので、網掛けのある四角形のカテゴリーはファイル共有ソフトによる影響として分類ができ、加えて、「3種の知識」をあてはめてファイル共有ソフトの情報モラルの評価を

行っている。

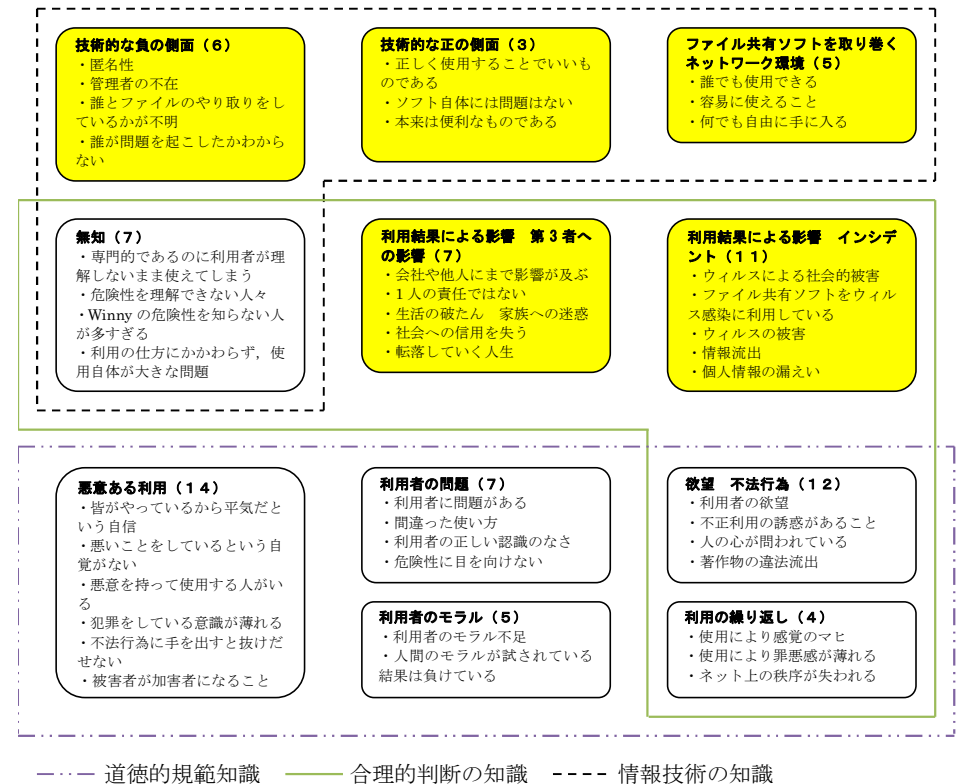


図4 情報モラルのカテゴリー化  
Figure4 Categorization of information ethics.

「3種の知識」に沿って、カテゴリー化の内容をみると次のようになる。道徳的規範知識では、多くの場合、ファイル共有ソフトの利用に関する正義についての指摘を行っている。これについては、通常ではコンピュータソフトウェアの開発段階で正義は確保されていることから、その利用に関して正義が問われることは多くない。しかし、ファイル共有ソフトでは利用者自身の正義が試されている傾向がある。そのため、ファイル共有ソフトの利用者が、皆が使用しているから平気であると考え

ることは、一層、責任の所在を不明確にしているという回答があった。さらに、こうした利用を支えているのが自らの欲望であり、著作権の侵害などの不法行為を行い、結果として利用を繰り返すことになるという回答もみられる。

情報技術の知識では、まず、ファイル共有ソフトの技術面からみた正と負の両面の評価がみられる。具体的には、授業で学習した意図的な匿名性の実現やソフト自体の管理が行われていないという負の面に対するものだけではなく、ファイル共有の技術自体を評価している回答もあった。次に、技術利用環境としての現在のインターネットにおいて、ファイル共有ソフトが誰でも入手・使用できることを問題視している回答もみられた。これらのことから、ファイル共有ソフトは技術的なレベルが高く理解できないことが多いにもかかわらず、安易な入手が可能であるため、その危険性がわからないで利用してしまうことを示している。

合理的判断の知識では、ファイル共有ソフトの利用による影響に関する指摘がみられる。それは、暴露ウィルスへの感染、情報漏えい、著作権侵害を通じて、非常に広範囲にわたる影響が発生することであり、自分が被害者であり加害者となり、家族・友人や第三者を巻き込む情報セキュリティインシデントになることを把握している。このことから、多くの生徒が合理的判断による問題の所在を理解しているといえる。

以上の分析から、今回の調査に対する全体的な情報モラルの捉え方は、「3種の知識」についてバランスよくみていることがわかる。具体的には、ファイル共有ソフトに関する情報モラルの問題を、道徳的規範知識と情報技術の知識から捉え、複合的に発生する情報モラル上の課題に対しても合理的判断の知識としてみている。ただし、図4中の「無知」、「欲望 不法行為」、「利用の繰り返し」は合理的判断の知識として評価したが、それぞれ情報技術の知識と道徳的規範知識の内容との関連が高いので重複させている。

生徒の回答をカテゴリー化しただけの内容では、ファイル共有ソフトの利用とその影響を述べているにすぎないが、「3種の知識」を用いてカテゴリー化した内容に新たな評価を加えることで、受講している生徒の多くがファイル共有ソフトの情報モラル上の問題を事前に把握していたことと、学校設定科目「情報セキュリティ」の授業による多角的な学習による情報モラルの形成がされていたことが確認できた。

#### 4.2.2 利用プロセスによる情報モラルの再構成

ここでは、生徒が指摘したファイル共有ソフトの利用に関して、利用プロセスと情報モラルの関係を分析する。そこで、図4でカテゴリー化したものをストーリーラインとして表し、ファイル共有ソフトの利用プロセスとして再構成し図5に示す。図5の利用プロセスは、技術を基盤としたファイル共有ソフトの存在、これを利用するユーザの目的・心理や行動、利用による結果という3段階になっている。

ファイル共有ソフトに関する情報モラルを再構築して考察する理由としては、情報モラルから考慮すべき多くの問題を包含するファイル共有ソフトであっても、ユーザ

が利用するという行為に関しては他のソフトウェアとの違いはほとんどないからである。加えて、利用プロセスが同じならば、その根底に存在する情報モラル上の問題を明確化しやすいと考えたからである。

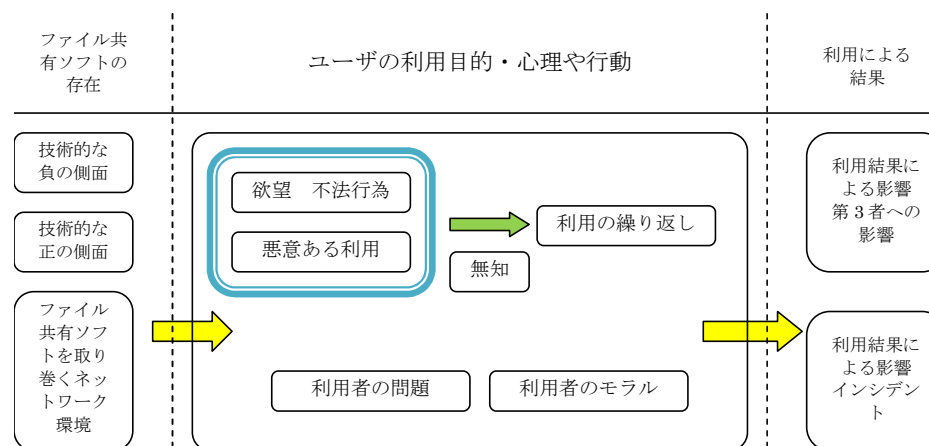


図5 利用プロセスからみた情報モラル  
 Figure5 Usage process on information ethics.

図5のように、利用プロセスを用いてファイル共有ソフトの情報モラル上の課題を整理してみると、多くの生徒が問題として「なぜ利用するのか」ということを指摘している。この指摘は、ファイル共有ソフトに関連する問題が利用の必要性という根本的な原因に着目していることを表している。端的に解釈すれば、何人かの生徒が指摘しているように、利用しなければ問題は生じないことから、問題が発生するリスクを冒しても利用する要因があるはずなのであると考えていることを意味している。

従って、ここで注目すべき事項は、ファイル共有ソフトを利用するユーザのニーズがどのようなものであるかということになる。多くの生徒が指摘しているように、ファイル共有ソフトを利用する最大の理由としては、音楽、映画などの著作物の不正入手であるといえる。これ自体が不法行為であるが、ファイル共有ソフトの利用による入手は物理的なものを入手するわけではないので、犯罪意識が薄いと考えられる。さらに、自らの欲望を優先させるために、発生する影響を考慮することができずに利用を繰り返し、重大な結果を招いてしまうのである。

このようにファイル共有ソフトの利用者のニーズが不適切なものであり、その利用によって結果がほとんど予測できない状況に陥ることを示している。これまでの検討

により、個人のニーズと技術的な理解から情報モラル上の課題をまとめると次の2点を導くことができる。

- ・利用者の適切なモチベーションの欠如
- ・起こりうる事態の予測ができない

つまり、今回の調査から、図5の二重枠のところは「3種の知識」の道徳的規範知識に属したコアカテゴリーになっており、生徒の集団で形成された根本的な情報モラル上の課題は利用者の欲望、不法行為、悪意ある利用にみられ、その影響は計り知れないことを示している。

以上のように、グラウンデッドセオリーアプローチをベースとして、「3種の知識」を考慮して分析した結果、授業を受けた生徒の集団においてバランスのとれた適切な情報モラルの形成がされているのである。

## 5. 課題

### 5.1 実効力ある情報セキュリティ教育の構築

前章において、授業実践により情報セキュリティインシデントへの対策能力の向上や適切な情報モラルの形成がされていることがわかった。しかしながら、実際に情報セキュリティインシデントに直面した時に、今回の授業実践が必ずしも実効性あるものであるとは限らない。

これは、情報セキュリティ教育において、情報セキュリティインシデントの発生時の環境を再現した授業展開が難しいという特質を有しているからである。そこで、今後は実験的な環境での情報セキュリティに関する実習を踏まえた授業展開を検討する必要がある。

### 5.2 生徒の不適切な行動の防止

情報セキュリティ教育を展開することで、生徒の不適切な行動を助長し、スク립トキディを育成してしまうのではないかという危惧がある。確かに、多くの情報セキュリティインシデントの解説をする過程で、興味本位からツール等を使用したいと考える生徒はいると思われる。今回の授業実践においても、コンピュータウイルスやマルウェアの不正入手やWinnyの利用が考えられなくはない。

しかしながら、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、自らが行った行動の結果を想定させることで、適切な行動を引き出すことが可能になる。加えて、日常の学校生活における情報セキュリティに関する指導も効果的となる。

## 6. まとめ

本稿においては、高等学校における情報セキュリティ教育についての実践を行い、次のような実践や考察を行った。

- ・学校設定科目「情報セキュリティ」のカリキュラム構築と授業実践を行った。
- ・情報セキュリティインシデントへの対策能力の向上に関する考察をした。
- ・適切な情報モラルの形成に関する考察をした。
- ・今後の情報セキュリティ教育の展開における課題を示した。

## 参考文献

- 1) 情報セキュリティ政策会議：2次情報セキュリティ基本計画，[http://www.nisc.go.jp/active/kihon/pdf/bpc02\\_ts.pdf](http://www.nisc.go.jp/active/kihon/pdf/bpc02_ts.pdf)(accessed 2010.10.31)
- 2) マカフィー：「高校生のCGM 利用実態」調査結果，[http://www.mcafee.com/japan/about/preview/pr\\_10b.asp?pr=10/09/22-1](http://www.mcafee.com/japan/about/preview/pr_10b.asp?pr=10/09/22-1)(accessed 2010.10.31)
- 3) 佐々木良一：東京電機大学における情報セキュリティ教育，電子情報通信学会技術研究報告 SITE, pp.7-12(2004).
- 4) 佐々木良一，松田剛，伊藤栄二：産学協同によるセキュリティ教育の実践と課題，情報処理学会研究報告 CSEC, pp.117-112(2006).
- 5) 松村真木子：情報セキュリティに敏感な一般エンドユーザ養成に向けて - 情報セキュリティ意識調査を事例として，情報処理学会論文誌, Vol.48, No.9, pp.3183-3192(2007)
- 6) 梅田恭子，江島徹郎，江崎浩成：情報モラルの4つの判断観点とゴールベースシナリオ理論に基づく体験学習教材の開発と実践，愛知教育大学研究報告, 58, pp.195-201(2009)
- 7) 戸田和幸，野崎浩成：「他者意識・自己防衛」を意識した情報モラル教育 - 情報化社会を生きる力との関連 -，愛知教育大学教育実践総合センター紀要, 第13号, pp.45-49(2010)
- 8) 山本朋弘，清水康敬：情報モラル指導における家庭と小学校の連携促進に関する検討，日本教育工学会論文誌, 32(2), pp.181-188(2008)
- 9) 文部科学省:高等学校学習指導要領, 東山書房 (2009)
- 10) 金子勇：Winnyの技術，アスキー (2005)
- 11) 萩原栄幸：Winny利用の果て，<http://www.itmedia.co.jp/enterprise/articles/0901/13/news010.html>(accessed 2010.10.31).
- 12) 戈木クレイグヒル滋子：質的研究方法ゼミナール，医学書院 (2009)
- 13) 玉田和恵，松田稔樹：「3種の知識」による情報モラル指導法の開発，日本教育工学会論文誌, 28(2), pp.79-88(2004)