授業実践

共通教科「情報」における情報セキュリティ授業の実践について

岩手県立盛岡南高等学校教諭　竹山　仁

1．はじめに

高等学校学習指導要領情報編の解説においては，「情報セキュリティを確保するための方法については，情報通信ネットワークや通信サービスを安全に利用するためには，暗号化やファイアウォール（Firewall）などの情報セキュリティを高めるための工夫が必要であることを理解させる。ここでは，利用者としての視点から，個人識別やパスワードの個人認証など，情報セキュリティを確保するために必要な基礎的な知識と技能を習得させる。」と示されており，生徒にスマートフォンを含め，情報モラルや情報セキュリティに関して正しい知識を持たせ，大人になったときに正しくインターネットを活用させるようにすることが急務である。

SNSによる書き込みで被害にあう生徒も少なからずいること，さらに2014年９月には高校１年生の生徒がゲーム会社のサーバー機に対してDDoS攻撃を行い，電子計算機損壊等業務妨害罪が初適用される事件が発生したことなどを受けて，これまでの情報モラル・情報セキュリティの指導では不十分な点が見られるようになった。さらに，2014年11月には「サイバーセキュリティ基本法」が国会で可決・成立し，今後情報セキュリティの指導についても見直しが必要と考えられる。そこで，私が行った情報モラルと情報セキュリティの指導実践を中心に報告していく。

2．IPA制作の情報セキュリティビデオの上映

2014年９月に，独立行政法人情報処理推進機構（IPA）が制作・公開している無料動画「スマートフォンのセキュリティ」と「SNSの心得」を生徒に視聴させ，その有効性についてアンケートを行った。これらの動画はIPA制作の「映像で知る情報セキュリティ～映像コンテンツ一覧～」（http://www.ipa.go.jp/security/keihatsu/videos/）の中に収録されている。視聴させた動画は，IPAが配布しているDVDやIPAが発信しているYouTube映像の中から，情報モラル指導に適切な内容のもの，これから生徒が生きていくうちに必要になるものを選んで上映した。上映時間は各動画とも10分程度である。

「あなたの書き込みは世界中から見られてる」
（IPA Channelより）

SNSの書き込みについての動画と，スマートフォンセキュリティについての動画を視聴させた後，「動画を見ての情報モラルの必要性について」のアンケートを実施した。結果は，図１のとおりである。

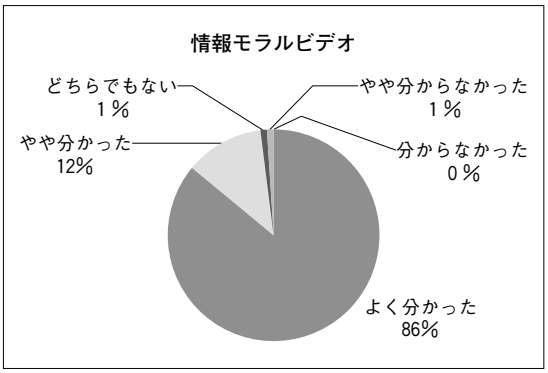

図1　ビデオ視聴後のアンケート結果

IPAにより一般向けに作られた動画であったこと，時間も1本10分程度で分かりやすく作られていたこともあり，一部を除き「よく分かった」，「やや分かった」との意見であった。

生徒の感想としては，「遊び半分でネットに載せてしまうと，自分が思っている以上に広まり，大変なことになってしまうと思った。」「アプリをダウンロードしただけで，ウイルスに感染したりSNSなどでも自分の思っている以上にいろんな人に見られていることがびっくりしました。」「スマートフォンにもコンピュータウイルスがあることを知り，気をつけたい。」などの記述が多かった。中には「家族がゲーム機でインターネットをしているので注意していきたい。」と記述している生徒もいたので，家族でインターネットの使い方について話題にする良い機会になったと思われる。

また，スマートフォンが小型のコンピュータであることを認識させる機会にもなった。「スマートフォンにもコンピュータウイルスがあることを知った。」「アプリのインストールに留意する。」など肯定的な意見が多かった。パソコン以上にコンピュータウイルスの存在やその脅威について学習させる良い機会になったと思われる。

3．情報セキュリティの授業実践（1）
～ポッドキャストと新聞記事の活用～

前述したとおり，2014年9月に企業のサーバー機に対してDDoS攻撃を行ったとして，高校生に電子計算機損壊等業務妨害罪が初適用される事件があった。その後も，国内だけではなく，世界的にサイバー攻撃の事件が報道されるようになり，今後生徒が大人になったとき，スマートフォンを含めた情報セキュリティの必要性，自分の身は自分で防衛するための知識を学ぶ必要性を痛感した。

そこで，情報セキュリティの講義の導入として，ラジオのポッドキャストを活用し，スマートフォンのセキュリティについての番組を視聴させた。番組はTOKYO　FM「Weeklyニッポン」の第29回「自分で守ろう！スマホのセキュリティ」（2014年10月19日付）である。ポッドキャストをダウンロードし，生徒に視聴させた。内容は，内閣官房情報セキュリティセンターの専門家がスマートフォンに潜む問題点や，公衆Wi-Fiを使うときの注意点について解説したものである。視聴と同時に，高校生によるDDoS攻撃の事例をあげ，2014年10月23日付の岩手日報と日本経済新聞の新聞記事を配布して生徒に読ませ，感想を記録させた。この授業での理解度は，図2のようになった。

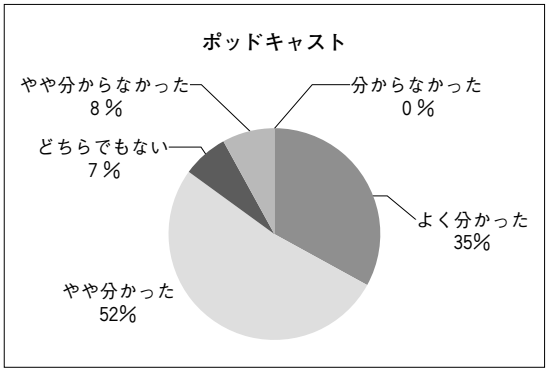

図2　ポッドキャストによるセキュリティ授業の理解度

この図より，動画よりは「よく分かった」という率は低いものの，「よく分かった」「やや分かった」で約8割の生徒が占めていることから，時期を考慮すればポッドキャストの使用は有効であると考えられる。授業の感想として次のようなものがあった。

「スマートフォンは意外と危険なものである。こまめにアップデートする，スマホにロックをかけるなどしたい。」

「ネット上の犯罪はかなり増えている。どれだけ減らせるかは自分たち次第なので，スマホのセキュリティを心がけたい。」

「問題に巻き込まれる可能性があるので，しっかりとした知識を身につけたい。」

「ウイルスやハッキングは身近なところに隠れているので，セキュリティの安全性をもう一度見つめ直すべきだ。」

「DDoS攻撃の怖さと，同い年の人がネット犯罪をしてしまったことがわかった。」

「ネット犯罪がなくなるようになるためには，自分自身の意識が大切。」

「今日の授業で，今のうちから情報セキュリティについて学んでおくべきだと感じた。」

「今までスマホを使ってきて，とても危険な使い方をしていたと感じた。」

4．情報セキュリティの授業実践（2）
～授業プリントの見直し～

前項で述べたとおり，高校生によるDDoS攻撃の事件が発生した。ほかにも，官公庁や企業のコンピュータへのサイバー攻撃，家庭用Wi-Fiルーターの脆弱性による個人情報の流出なども報道されている。また，年末年始のSNS大量送信によりネットワークが機能不全に陥る，ある意味DDoS攻撃のような事態も起こっている。

このように，インターネットが発達し，高校生だけではなく小・中学生でもスマートフォン等の携帯端末を持つ現在において，情報モラルとともに，「情報セキュリティ」の指導をきちんとしていかなければ，知らないうちにサイバー犯罪行為を犯す危険性が高い。そうさせないために，これまでの「情報モラル」だけではなく，「情報セキュリティ」についてどこまで指導するか検討をしてきた。

最初のうちは共通教科「情報」の教科書レベルのものを中心に指導してきたが，2014年度は「情報モラル」だけではなく，「情報セキュリティ」についても踏み込んで指導することにした。

内容については，IPAが実施している国家試験「ITパスポート試験」の問題や，P検（ICTプロフィシエンシー検定試験：P検協会主催）準2級レベルの問題を参考にして授業プリントを作成した。指導内容として，「フィッシング詐欺」「DoS攻撃」「DDoS攻撃」「クロスサイトスクリプティング」「SQLインジェクション」「ゼロディ攻撃」などを取り上げた。

11月の授業の後，生徒に情報セキュリティ授業についてアンケートを取った。その結果は，次の図3のとおりである。

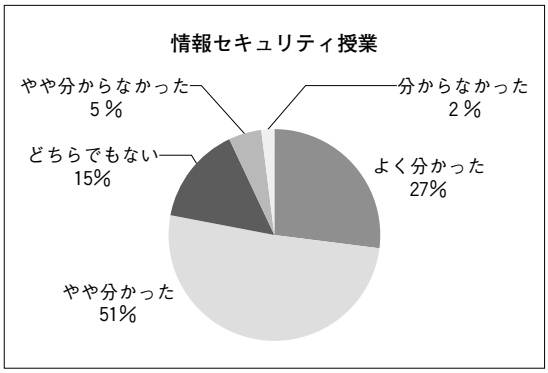

図3　情報セキュリティ授業のアンケート

以下は生徒の感想を抜粋したものである。

「簡単にコンピュータウイルスに感染しないように自分の情報を外部に流さないように気をつけて管理していきたい。」

「こんなにもたくさんの，セキュリティや違法行為があることが分かった。考えて使っていこうと思った。」

「悪意を持って他人のコンピュータのデータやプログラムを盗み見られたり，改ざん，破壊されたりする行為が，自分にも起こりうることなのかもしれないと思ったら，怖かった。だからそうならないように，こまめにバックアップをするなど自己的に出来る対策をしたいと思った。」

「自分も一人暮らししたときに，対処できるように学ぶことはすごく大切なことだと思った。対策を一人でもできるように慣れていきたいと思った。」

「すごく身近にあるものが一歩間違えば大変なことになることが分かった。」

これらの感想からも分かるように，当初はコンピュータウイルスの存在を知らなかった生徒も，今後自分のスマートフォンが遠隔操作されるなどして，ほかのコンピュータの攻撃の踏み台になる可能性があること，辞書攻撃等によりパスワード等が簡単に解読されうる事実があることを学び，自分のスマートフォン等を自己防衛することの大切さを学んだ。そして将来，卒業後の生活における情報セキュリティの必要性，自己防衛の重要性，スマートフォンをはじめとする情報機器を様々な情報セキュリティ上の攻撃から防衛するための知識を得て，今後の自分たちの生活の意識が変化したと思われる。さらには，家庭内でのLAN環境を検証し，情報セキュリティについて見直しをしようとする生徒もいた。

内容については「フィッシング詐欺」「DoS攻撃」「DDoS攻撃」「クロスサイトスクリプティング」「SQLインジェクション」「ゼロディ攻撃」「辞書攻撃」「電子計算機使用詐欺罪」「電子計算機損壊等妨害罪」などを取り上げたが，生徒によるSNSの書き込みや「ネットいじめ」の予防だけではなく，もっと踏み込んで「ネット犯罪に巻き込まれない」，さらには生徒が「ネット犯罪を起こさない」よう指導をしていかなければならないと強く感じた。そのためには，今後高校段階では「情報モラル」だけではなく，「情報セキュリティ対策」についても指導を行うことで，今現在の生徒のスマートフォンの使い方だけではなく，将来生徒が社会人になり，家庭を持って次世代の子どもができたときに，その子どもたちが安全にインターネットを使える環境を整備することの重要性を指導する観点が必要であると強く感じた。

5．まとめ

高校生の場合，今後は中学校段階以前でインターネットに触れ，スマートフォンを所持してくることが考えられる。もっと早い段階では小学校段階でゲーム機でインターネットを活用してSNS等を行っていることも考えられる。さらに，乳幼児期にタブレットやスマートフォンに親しんできていることもあり得る時代である。そういったことから，社会への入り口である高校段階では，従前の「（携帯電話・スマートフォンにおける）情報モラル」だけではなく，スマートフォンやコンピュータにおけるコンピュータウイルスの被害やDDoS攻撃等のサイバー攻撃，サイバー犯罪から身を守る上で，「情報セキュリティ」教育が今後必要であると考えられる。

2020年に東京オリンピックを控え，サイバー空間でのセキュリティ向上も叫ばれている。技術者レベルだけではなく，これからは一般市民レベルでのセキュリティ対策，あるいは家庭で子どもたちを指導する立場になる「親」としてのセキュリティ対策が必要である。とくに，高校生に対しては，次世代の未来の「子どもたち」が安全・安心にインターネットを使い，協同型学習を円滑に進めるために，そのベースとなる「情報セキュリティ教育」の指導が不可欠である。実際に，小学校の教員が困っているのは，小学校の児童に対するセキュリティ教育ではなく，児童の親に対する情報モラル・セキュリティの指導であるといった声も上がっている。

今後は，パスワードクラッキングの事例や標的型攻撃を含め，高校生が社会の一員になったときに困らないようなセキュリティ事例に踏み込んだ授業の展開を進めていきたい。

参考文献

・独立行政法人情報処理推進機構
http://www.ipa.go.jp/
・TOKYO FM「Weeklyニッポン」ポッドキャスト
http://www.tfm.co.jp/podcasts/japan/
・日経コンピュータ「すべてわかるセキュリティ大全」日経BP社
・日経NETWORK「絶対わかる！セキュリティ超入門」日経BP社
・高橋麻奈「やさしい情報セキュリティスペシャリスト講座2013・2014年版」ソフトバンククリエイティブ
・一田一樹「ネットの危険を正しく知るファミリーセキュリティ読本」原書房