児童・生徒を対象とした情報セキュリティ教育で取り扱うべきインシデントに対する検討

増山　一光*1
Email: kazu-masuyama@pen-kanagawa.ed.jp

*1：神奈川県立商工高等学校

◎Key Words　　情報セキュリティ教育，インシデント，情報教育

1.　はじめに

情報セキュリティ教育には安全教育の側面があり，児童・生徒が直面するであろうインシデントを取り上げ，そのリスクを低減させるようなふるまいを身につけるとともに，事前の対策を日常的に行わせることで被害を最小限にすることが目的の一つとなっている。しかしながら，こうしたインシデントは，日々，高度化・巧妙化しており，その対策が難しくなってきているのが現実である。さらに，児童・生徒の ICT を取り巻く環境も大きく変化してきており，学校教育の中で把握することも難しくなってきている。その結果として，深刻な被害をもたらす様々なインシデントに直面することも少なくない。

そこで，本稿では，児童・生徒が個人として受ける可能性のある経済的被害やプライバシーに関する被害に着目して，どのようなインシデントを教材として取り上げるべきかを検討して，児童・生徒の心身の発達を考慮しながらインシデントを多角的にとらえられるような効果的な学習手法について考察することを目的とする。

2.　児童・生徒の ICT 環境

全般的な ICT 環境の大きな変化は，2017 年の世帯における情報通信機器の保有状況をみると，スマートフォンの保有率（75.1%）が固定電話（70.6%）とパソコン（72.5%）の保有率を超えたことである [(1)]。さらにモバイル端末全体の保有率では実に 94.8%になっており，スマートフォンが情報通信において大きな役割を果たしていることがわかる。

インターネットの利用に着目すると，小学生（男子：87.8%，女子：83.4%），中学生（男子：95.0%，女子：95.3%），高校生（男子：99.3%，女子：98.7%）となっており，特にスマートフォンでのインターネット利用をみると，小学生では 40.7%，中学生では 65.8%，高校生では 94.3%となっている[(2)]。このことから，児童・生徒のほとんどがインターネットの利用をしており，接続機器として高校生のほとんどがスマートフォンを使用しているとともに，小中学生でもかなり利用しているがスマートフォン以外の接続機器も多く使用されていることがわかる。

スマートフォンのインターネット利用者の利用内容の上位を校種別にまとめたものが表 1 である。この表から校種別ごとで順位は違うが，利用内容は 5 種類が共通していることがわかる。特に中高生に関しては，スマートフォンでのインターネット利用はコミュニケーションが中心であり，サービスという視点からは小学生から高校生まで動画視聴が盛んに行われていることがわかる。

表１　校種別のインターネット利用内容[(2)]

内容	小学生	中学生	高校生
ゲーム	76.2	66.7	71.5
動画視聴	62.0	74.9	85.2
コミュニケーション	35.4	76.2	89.9
音楽視聴	35.1	63.2	78.8
情報検索	33.0	53.5	66.7

単位：%

このようなことから，児童・生徒のほとんどがインターネットへのアクセスをしており，その中心となる接続端末はスマートフォンになっている。インターンネットにおいて最も利用されている内容は，小学生がゲーム，中高生がコミュニケーションである。この状況を踏まえて，情報セキュリティ教育においてどのようなインシデントを扱うことで，安全・安心なインターネット利活用が可能となるのかを検討するものとする。

3.　学校教育における情報セキュリティ教育

3.1　情報モラル指導モデルカリキュラム表

情報セキュリティ教育の指導内容は，2007 年に文部科学省委託事業として小学校（低学年，中学年，高学年），中学校，高等学校を対象とした情報モラル指導モデルカリキュラム表[(3)]に示された。

このカリキュラム表での分類には，情報社会の倫理，法の理解と順守，安全への知恵，情報セキュリティ，公共的なネットワーク社会の構築という 5 つがあり，それぞれに大目標と中目標が設定されている。各対象に対して，5 つの分類と大目標・中目標がリンクしており，多角的に指導内容を確認することができる特徴がある。

情報セキュリティの分類には，小学生では 2 つの大目標が設定されている。1 つ目は中学年から高学年を対象にして「生活の中で必要となる情報セキュリティの基本を知る」という大目標が設定され，中学年の中目標として「認証の重要性を理解し，正しく利用できる」と，高学年の中目標として「不正使用や不正アクセスされないように利用できる」が定められている。2 つ目は高学年を対象として「情報セキュリティの確保のために，対策・対応がとれる」という大目標が設定され，高学年の中目標として「情報の破壊や流出を守る方法を知る」が定められてい

る。

同様に，中学生と高校生を対象にした大目標が設定されている。1つ目は「情報セキュリティに関する基礎的・基本的な知識を身につける」という大目標が設定され，中学校の中目標として「情報セキュリティの基礎的な知識を身につける」と，高等学校の中目標として「情報セキュリティに関する基礎的な知識を身につけ，適切な行動ができる」が定められている。2つ目は「情報セキュリティの確保のために，対策・対応がとれる」という大目標が設定され，中学校の中目標として「基礎的なセキュリティ対策が立てられている」と，高等学校の中目標として「情報セキュリティに関し，事前対策・緊急対応・事後対策ができる」が定められている。

大目標に着目すると，校種間における差異は大きくないことから，発達段階に応じて情報セキュリティに関する知識を身につけることと，情報セキュリティに関する対策・対応ができることを求めていることがわかる。

中目標に着目すると，校種間における達成すべき内容の難易度が高くなっているように思われるとともに，具体性が欠ける面が見られる。このことは，どの校種で情報セキュリティのどのような内容を取り上げるべきかということが捉えにくいことを示している。

さらに，近年，高度化の一途を辿っている情報セキュリティに関するインシデントに対して，発達段階に応じてどのように対応すべきかという視点を見出すことができなくなってきている。

3.2 学習指導要領

小学校学習指導要領[4]では、情報活用能力の育成に情報モラルの育成を含めて教育課程の編成を図ることが明記されており、指導にあたっても情報モラルの指導を充実させることとされている。同様に，特別の教科としての道徳においても情報モラルの指導が掲げられている。しかしながら，情報セキュリティの記述はなく，あくまでも情報活用能力に伴う情報モラルの育成に焦点が当てられている。このことは，発達段階を考慮すれば重要なことであるが，児童のインターネットの利用内容の多様化と利用時間の増大を考慮すれば情報セキュリティをどのように扱うかが課題となるであろう。

中学校学習指導要領[5]では，小学校学習指導要領と同様に情報モラルの育成が示されているが，情報セキュリティに関しては技術・家庭で扱われている。技術・家庭の「D情報の技術」の分野において，情報のデジタル化や処理の自動化，システム化，情報セキュリティ等に関わる基礎的な技術の仕組み及び情報モラルの必要性について理解することが示されている。この内容の取扱いには，著作権を含めた知的財産権，発信した情報に関する責任，及び社会におけるサイバーセキュリティが重要であることについて扱うとされている。

中学校学習指導要領では，小学校の段階よりも内容的に発展しており，発達段階やICTの利用状況に応じたものになっていることがわかる。しかしながら，技術・家庭と特別の教科である道徳を中心として扱うことから，時間的かつ内容的に制約されてしまうことや，教員によって授業展開に差が生じてしまうことから，効果的な授業を目指して組織的な改善の取り組みが望まれる。

高等学校学習指導要領[6]では，教科情報において情報セキュリティが扱われるとともに，専門教科情報では「情報セキュリティ」という科目が設置され，情報セキュリティ教育の充実がみられる。あわせて，その他の専門教科でも情報に関する科目の中で必ず情報セキュリティの内容が取り扱われるようになっている。

高等学校では2021年度より順次，学習指導要領の移行が行われ情報セキュリティ教育の充実が図られるが，形式的な学習に終わることなく日常生活と将来において活かすことができる情報セキュリティ教育を目指さなければならない。

一方では，高校生において小学校や中学校で身につけておくべき情報モラルの欠如もみられるので，情報モラルに関する指導も欠かせないのが現状である。

3.3 インターネット安全教室

2020年に(独)情報処理推進機構からインターネット安全教室[7]という情報モラル・情報セキュリティに関する教材が公表されている。これは，前述の情報モラル指導モデルカリキュラム表や学習指導要領に準拠したものになっている。

2009年に施行された青少年インターネット環境整備法では，フィルタリングの普及促進だけでなく、子どもたちに「インターネットを適切に活用する力を習得させる」ことが示されていることから，学校や家庭で、子どもたちを指導していくことが求められている。そのため，この教材の特徴は，学校だけでなく家庭や社会など幅広く利用できる点である。具体的な対象は，「小学校1年生～3年生」「小学校 4 年生～6 年生」「中学生・高校生以上」「保護者・一般」であり，幅広い年齢層が対象になっている。このことは，一貫した学習を年齢や理解度に合わせて，教材の活用ができることになる。

この教材の構成は，次の通りである。

・オープニングスライド　1本
・5つのテーマ（対象にあわせた教材20本）
・番外編　2本

この構成の中に5つのテーマを設定しているが，これらのテーマとねらいを示したものが表2である。

これまで示した通り，この教材は数多く多角的に用意されており，スライドだけでなく動画を視聴できるテーマもあるので，効果的な学習が期待できる。しかしながら，いくつかの課題や改善点が散見される。具体的には，第1に，対象の目安となっている小学1～3年の学習内容が小学1・2年生にはやや難解な点があり，一方で中学生・高校生の学習内容は高校生には容易すぎる面があり，学習のレベルを講師または教員が選別するのが難しくなっている。

第2に，フィルタリングを一つのテーマとしているが，中学生・高校生の多くがフィルタリングを使用していない現実があり，テーマとして採択するのではなく特に保護者の学習内容を充実すべきである。

第3に，教材の種類も多く充実しており，テーマごとの学習目標を実現しているが，情報モラルや情報セキュリティの全体像の把握が難しい側面がある。これは，個別のインシデントへの対策については学習できるが，そのインシデントが情報モラルや情報セキュリティの視点か

らみたときの位置づけがわかりにくい点が挙げられる。

表2　教材のテーマとねらい

テーマ	ねらい
SNS とのつきあい方	SNS とは？SNS の可能性，利点も確認した上で，個人情報拡散や危険な「出会い」などの負の面があることを理解し，対応する力をつける。
フィルタリング ペアレンタルコントロール	保護者の機能，使用制限の重要性，インターネット利用が当たり前の時代になぜ必要か？の理解から安心・安全，また健全に利用するためのツールとして活用することを促す。
知っておきたい情報セキュリティ	コンピューターウイルス，脅迫，詐欺等を含む脅威から，若年層，一般ユーザーが注意すべきこと，その対応策を伝える。
インターネットの基礎知識	インターネット，SNS などの利用者の心構えとして，その仕組みを知り，個人個人の判断の基準となるよう啓発をする。インターネットは道具であり，活用にはメリット・デメリットがあることも伝えたい。
みんなで考える，情報モラル，情報セキュリティ	情報モラル，情報セキュリティを学び，考えた上で自分の為に，また人に伝える為に標語を作成するワーク。標語を作る上でのポイントや注意点を学ぶ。

4.　インシデントの動向

情報セキュリティに関するインシデントは，毎年，様々なものが発生している。これをまとめて発表しているものは，(独)情報処理推進機構が公表をしている情報セキュリティ 10 大脅威 2020[8]である。表3は，「個人」向け脅威の上位10のインシデントを示している。なお，ランク外の脅威だから対策を行わなくて良いということではなく，継続しての対策が必要になると指摘している。

表3　「個人」向け脅威

順位	内容
1	スマホ決済の不正利用
2	フィッシングによる個人情報の詐取
3	クレジットカード情報の不正利用
4	インターネットバンキングの不正利用
5	メールや SMS 等を使った脅迫・詐欺の手口による金銭要求
6	不正アプリによるスマートフォン利用者への被害
7	ネット上の誹謗・中傷・デマ
8	インターネット上のサービスへの不正ログイン
9	偽警告によるインターネット詐欺
10	インターネット上のサービスからの個人情報の窃取

表3のインシデントから結果的に個人情報に関わるものが多いことがわかる。このことは，情報セキュリティにおいて個人を対象としたインシデントでは，個人情報を流出させたり，不正に得ることを目的にしているものが多いのである。

実際に，個人情報が漏えいした場合の被害者への影響を「経済的損失」と「精神的苦痛」という2種類の尺度で分類したものが図1である[9]。

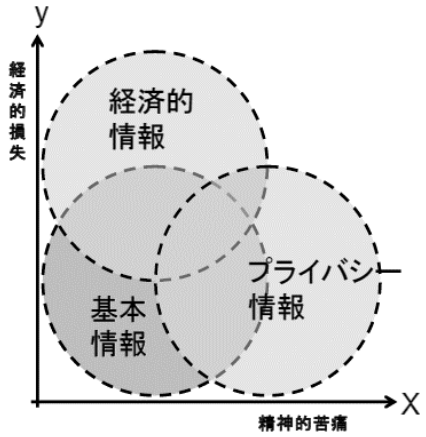

図 1　個人の情報資産

図中では，個人情報を基本情報，経済的情報，プライバシー情報に分けている。基本情報には，氏名，住所，生年月日，性別，メールアドレス，健康保険番号などがある。経済的情報は，口座番号と暗証番号，クレジットカード番号とカードの有効期限など流出すると経済的損失をもたらす情報である。プライバシー情報には病状，信条，思想，宗教などがある。これらの組み合わせによって X 軸に精神的苦痛の度合いを，Y 軸に経済的損失の度合いを表している。

図1を用いて表3の「個人」向け脅威をみると，経済的損失につながるインシデントがほとんどであり，インシデントの多くは攻撃者が経済目的で行っていることがわかる。一方で，直接的に精神的苦痛につながるインシデントは第6位や第10位が該当すると思われる。しかしながら，インシデントによる被害を受けるということは，そのすべてにおいて精神的被害を受けることから，複合的被害を引き起こす可能性が高いのである。

また，注目すべきインシデントは第 7 位にある「ネット上の誹謗・中傷・デマ」である。このインシデントは，あくまでも個人が被害者として位置づけられているが，これは普通のインターネット利用者によって引き起こされているものも少なくない。このことは，表 3 は個人に対する脅威ではあるが，一転して攻撃者になりえることを示しており，加害者と被害者が表裏一体であるという現実を示している。

このように，個人を対象としたインシデントは手法が巧妙化しており，その標的としては個人情報が狙われ，経済的損失と精神的苦痛がもたらされてしまっている。一方では，一般のインターネット利用者が誹謗・中傷・デマを発信してしまうことで加害者になってしまうというインシデントの二面性も発生している。

5. 情報セキュリティ教育で扱うべきインシデント

情報セキュリティ教育において，インシデントを扱う際の前提としては，第 1 に児童・生徒の ICT 環境の状況を把握する必要がある。これは児童・生徒の日常生活の中で，関連性の低いインシデントを取り上げても教育効果が低くなってしまうためである。

第 2 に，児童・生徒の情報に関する知識技能のレベルの把握が重要である。インシデントに対する解説をする際の理解度に影響することになる。しかしながら，インシデントに対する授業の過程の中で知識技能を補うことは可能であろう。

これまで述べてきたことを踏まえて，個人に対するインシデントを図式化したものが図 2 である。

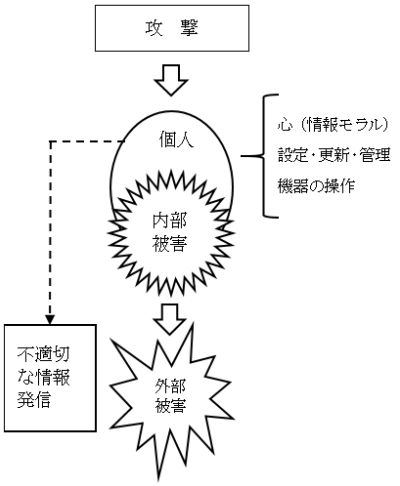

図 2　個人に対するインシデント

情報セキュリティ教育においてインシデントを取り扱う際に，話題性を考えて最新のものを取り扱い，内容も明確に分かっていない状況の中で，単に危険性のみを指摘するものが少なくない。このような教育活動では，児童・生徒の情報セキュリティ意識の向上にはつながらないのが現実である。

実際に情報セキュリティ教育でインシデントを扱う場合には，まず，図 2 のようにインシデントがどのような攻撃で，何を目的にしているのかを明確にしなければならない。このプロセスで攻撃の仕組みを理解させることで，個人が行う対策を学ぶことができる。こうした攻撃の内容と対策を対にしてインシデントを学ばなければならないのである。

次に，その攻撃によってどのような被害がもたらされるのかを明確にする。図 2 にある内部被害の大半は精神的苦痛を伴うものであり，その内容を事前に理解していれば適切な対応も可能になるであろう。外部被害は，経済的損失や情報流出が想定されるが，これについても攻撃の仕組みを知ることで適切な管理や運用を促すことができる。

しかしながら，インシデントを学んでいるにもかかわらず，不適切な情報発信を行って自らが攻撃者になってしまうこともある。単にインシデントの技術的内容だけを取り扱うのではなく，心の面である情報モラルを意識してインシデントを取り扱わなければならない。

以上のことから，情報セキュリティ教育で扱うべきインシデントは，児童・生徒の ICT 環境を把握した上で，インシデントの内容が研究者や公的機関などによって仕組みや被害の範囲が把握されているものとし，児童・生徒が自律的に対策を立案できるようにしなければならないのである。そして，こうした教育活動を通じてインシデントを引き起こすような加害者にしないための情報モラル教育も併せて行わなければならない。

6. おわりに

本稿では，児童・生徒の ICT 環境，学校教育における情報セキュリティ教育，インシデントの動向を踏まえて情報セキュリティ教育で扱うべきインシデントについて述べてきた。

今後は，情報セキュリティ教育で扱うべきインシデントを踏まえて児童・生徒が使用できる教材を開発する予定である。具体的には，話し合いによる深い学びを目指したカードゲーム教材を検討しており，教育実践を通じて開発していきたいと考えている。

謝辞

本研究は，JSPS 科研費 JP20H00756 の助成を受けたものです。

参考文献

(1) 総務省：“平成 30 年版情報通信白書”，https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/pdf/index.html（参照日 2020.5.20）
(2) 内閣府：“平成 30 年度 青少年のインターネット利用環境実態調査”，https://www8.cao.go.jp/youth/youth-harm/chousa/h30/net-jittai/pdf-index.html（参照日 2020.5.20）
(3) 社団法人　日本教育工学振興会（JAPET）：“すべての先生のための「情報モラル」指導実践キックオフガイド”，http://jnk4.info/www/moral-guidebook-2007/kickoff/pdf/moralguide_all.pdf（参照日 2020.5.20）
(4) 文部科学省：“小学校学習指導要領（平成 29 年告示）”，https://www.mext.go.jp/content/1413522_001.pdf（参照日 2020.5.20）
(5) 文部科学省：“中学校学習指導要領（平成 29 年告示）”，https://www.mext.go.jp/content/1413522_002.pdf（参照日 2020.5.20）
(6) 文部科学省：“高等学校学習指導要領（平成 30 年告示）”，https://www.mext.go.jp/content/1384661_6_1_3.pdf（参照日 2020.5.20）
(7) （独）情報処理推進機構：“インターネット安全教室”，https://www.ipa.go.jp/security/keihatsu/material.html（参照日 2020.5.20）
(8) （独）情報処理推進機構：“情報セキュリティ 10 大脅威 2020”，https://www.ipa.go.jp/security/vuln/10threats2020.html（参照日 2020.5.20）
(9) NPO 日本ネットワークセキュリティ協会：“情報セキュリティインシデントに関する調査報告書別紙”，https://www.jnsa.org/result/incident/data/2017incident_survey_sokuhou_attachment_ver1.0.pdf（参照日 2020.5.20）