Technical Understanding of the Internet Raises Children's Security Awareness

技術的理解が高める子どもの安全意識
― 中学生を対象とした事例研究 ―

Technical Understanding of the Internet Raises Children's Security Awareness

松　村　真木子
MATSUMURA, Makiko

本研究は、インターネット教育に技術的な理解を取り入れることの重要性を提唱する。情報教育において、①「インターネットが繋がる仕組み」、②「インターネット上にアップロードした情報は消えない」、③「サイバーテロの仕組み」を技術的に学習することが、モラルを定着させる効果を検討した。

ワークショップを実施し、中学生になれば、インターネットの仕組みを技術的に理解することができること、生徒が技術的にインターネットの仕組みを理解することは、情報発信者の責任、情報を発信することの意義、情報機器の管理について、情報を扱う上でモラルの定着を促し、インターネットの安全な利用へとつながることを検証した。

さらに、中学生は、親に管理されるのではなく、自分で安全にインターネットを利用することを望んでいる。情報を発信する生徒には、実際に使う場面に応じた安全教育が望ましいことが明らかとなった。

1．はじめに

インターネットのユーザは大人から子どもまで急速に拡大している。その背景には、インターネットを利用できる情報端末がパソコンばかりではなく携帯電話に広がったこと、コンテンツが多様化し、かつ、特殊な能力を必要とせずに誰でも利用しやすいようにインターフェースが整ってきたことが挙げられる。さらに、通信料の定額化や広告を表示することで無料化しているサイトが急増していることも、利用者の拡大を促進している。

小学生になると情報教育の一環として、調べ物学習や学校間における情報発信を通した交流も実施されている。インターネットは、小学生にとっても当たり前に利用するツールとなっており、10才くらいから携帯電話を持ち始める児童が多いと報告されている[2]。

ゲームをはじめとして、ゲームの攻略方法を交換する掲示板、個人の日記を公開するブログ（プロフ）、Facebookなどの各種SNS、ツイッター、動画や音楽の投稿など、情報を発信するコンテンツが多様化し日々刷新されている。このような環境を整えるものとして、インターネットの利用を主眼とし、インターフェースの使いやすさを追求したパソコンや携帯電話が市場に出回ってきている。そのため、大人であってもパソコンの仕組みやイン

キーワード：インターネット、安全、子ども、技術的理解、モラル
Key words ：internet, security, children, technical understanding, moral

ターネットが繋がる仕組みを知らずに、インターネットを利用しているユーザは多いだろう。子どもたちも、情報を発信する画面の向こう側がどのような仕組みで繋がっているのかを学習する以前に、ゲーム機のようにパソコンや携帯電話を使っているのではないだろうか。

近年、情報を利用する際のモラル教育が重視されてきたが、モラルを下支えするために、インターネットの仕組みについての技術的な理解を図ることが必要であると考える。

子どもに携帯電話を持たせないという論調があるが、携帯電話だけを切り離して議論するのではなく、情報機器の使い方を含め、情報を安全に利用するための基礎知識を学習させることが必要である。

急速なコミュニケーションツールの発展にともない、発信した情報がどのように見られているのかを理解してこそ、子どもは安全にインターネットを利用できるようになる。

2．目的

技術的な理解の基礎があれば、インターネットを利用する際に生じる危険性について具体的に理解しやすくなり、モラルの定着も深まる。このような観点から、中学生を対象にワークショップを実施する。中学生に、インターネットの仕組みや使い方について技術的に理解させることが、モラルの認識を支え、情報セキュリティ感覚を養い、安全な利用へと導くことになるという仮説を検証する。

さらに、インターネット上での個人情報の取り扱いや個人を特定できる噂など、実際に身近に見聞きしている現状を調査する。

3．方法

ワークショップを実施し、中学生が技術的な仕組みを理解することが安全意識を定着させることについて検証する。

3.1 調査

(1) プレ・ワークショップ　2009年３月、２会場において、中学生と親30組を対象に、パソコンを安全に利用するワークショップおよびアンケート調査を実施した。

(2) ワークショップ　2009年７月および９月に、S市２中学を訪問し、中学生30名[1)]を対象に、ワークショップを実施した。

3.2 調査方法

(1) のプレ・ワークショップの結果を踏まえて、(2) のワークショップにおいては、事前アンケートを実施後に、ワークショップ（パソコン及びインターネットの技術的な仕組みを解説）、その後、事後アンケートを実施した。事前アンケートと事後アンケートを比較検討する。さらに、インターネット上で身近で起きている問題について、質問形式で調査を実施した。

3.3 調査内容

(1) のプレ・ワークショップの内容を精査し、以下３点、①「インターネット上では、ハンドルネームを使っても匿名にはならない（インターネットが繋がる仕組み）」、②「一度、インターネット上に出した情報は、完全に消すことはできない（インターネット上にアップロードした情報は消えない）」、③「ウィルスやスパイウェアに感染すると、自分も加害者になってしまう（サイバーテロの仕組み）」について、技術的な解説を中心にワークショップを実施した。

インターネット上で身近で起きている問題

およびインターネット利用上の家庭におけるルールと中学生の意識について質問形式で調査した。

4．結果

4.1　ワークショップの理解度

①「インターネットが繋がる仕組み」、②「インターネット上にアップロードした情報は消えない」、③「サイバーテロの仕組み」について、ワークショップ後にアンケート調査を実施した結果、各項目とも、90%以上が「とてもよくわかった」「よくわかった」と回答した。

理解されやすかった項目は、「一度、インターネット上に出した情報は、完全に消すことはできない（インターネット上にアップロードした情報は消えない)」である。この項目は、インターネット上に、個人情報、特に、顔のわかる画像をアップロードすると、その情報はダウンロードされて拡散するため、インターネット上から完全に削除できなくなることについて、インターネットの情報が広がる仕組みから理解させた。

次に理解されやすかった項目は、「ウィルスやスパイウェアに感染すると、自分も加害者になってしまう（サイバーテロの仕組み)」である。ウィルスやスパイウェアの働きを示し、自分で気がつかないうちに、サイバーテロの手先となることを、技術的に理解させた。

「ネット上では、ハンドルネームを使っても匿名にはならない（インターネットが繋がる仕組み)」は、ハンドルネームで意見の書き込みをしても、インターネット上ではデータの経路をたどれるため、どの機器から発信されたのかまでたどることができることを技術的に理解させた。IPアドレスとサーバとの関係については、ややイメージすることが難しかったのだろう。「とてもよくわかった」と回答した生徒が40%にとどまったが、「よくわかった」生徒が50%近くあり、合わせると90%以上の生徒が理解した。

ワークショップには、パソコンに関心がある生徒が集まったのではあるが、インターネットが繋がる技術的な仕組みについて、中学生でも理解できることが明らかとなった。

なお、情報教育のカリキュラムにおいて、インターネットの仕組みが組み込まれているが、調査した時点では、生徒たちは授業の一環としてこれを学習した経験はなかった。

4.2　技術的な理解の必要性を検証

セキュリティ意識について、ワークショップの前後、すなわち、事前アンケートおよび事後アンケートの結果を比較分析し、ワークショップの効果を検証する。各項目ごとにリスクを検討した上で、生徒のインターネット利用状況別に、ワークショップの前後でリスクの増減を検証した。

生徒のパソコンおよび携帯電話の利用状況から、利用レベルをグループ分けした。「同じ趣味の人たちが集まるサイト・会員用サイト（SNS)」「掲示板への書きこみ」「ネット上での対戦ゲーム」「日記（ブログ・プロフ）を書いている」の各スコアを合計し、平均値より低いケースを「レベル１」(17名)、平均値よりも高いケースを「レベル２」(10名）とする。すなわち、「レベル２」のグループは、インターネット上で積極的に書き込みをしているグループである。

(1)　インターネットの繋がり方---匿名のようで匿名ではない社会

インターネットは、情報機器に固有のアドレスが付けられている（Macアドレス)。イ

ンターネット上の情報のやりとりは、IPアドレス（自分の属しているネットワークのネットワークアドレスとホストサーバのアドレス）とこのMacアドレスとによって実行されている。インターネット上の技術的な側面から見れば、どの機器を利用して、どのルートを通って情報をやり取りしているのかがわかる。検索エンジンなどを使ってHPを見たり、ハンドルネームを利用して書き込みをしたりする行為を実行する場合、ユーザは、自分の存在はわからない、匿名であると思っている。しかし、技術的には、どのパソコン（携帯電話）からのアクセスなのかを明らかにすることができる。

事前アンケートにおいて、「ハンドルネームで書き込んだ内容は気にならない」「ハンドルネームを使えば安心だと思う」「顔を見て言えないことでも、ネット上なら書けてしまうことがあると思う」の平均スコア（「前・匿名を意識するスコア」とする）を算出した[2)]。

次に、事後アンケートにおいて、「ネット上に書くときに、内容に気をつけようと思いますか」「ハンドルネームでも、自分が書いたとわかることを意識しますか」「ハンドルネームでも、読む人の気持ちを考えて書こうと思いますか」の平均スコア（「後・匿名を意識するスコア」）を算出した[3)]。

「前・匿名を意識するスコア」および「後・匿名を意識するスコア」は、リスクが高いほうが、スコア（リスク・スコアとする）が高くなるように設定した。そこで、事後アンケートの「後・匿名を意識するスコア」と事前アンケートの「前・匿名を意識するスコア」の差を算出し、ワークショップの効果を測定した。

生徒の利用状況レベルごとに各リスク・スコアが減少した値の平均値を表１「匿名性」に示す。そこで、レベル別に「後・匿名を意識するスコア」マイナス「前・匿名を意識するスコア」の減少した値の平均値について、t検定を実施した。その結果、有意な差が認められた。

匿名性の理解について、リスクの減少を、74％（20名/27名）で確認することができた。「レベル1」のグループは65％（11名/17名）、「レベル2」のグループは90％（９名/10名）が、リスク・スコアが減少した。

情報発信をしている「レベル２」のグループの方が、リスク・スコアの減少ポイントが高い結果を示した。

このように、ワークショップにおいて、生徒は、匿名のようでも、技術的には匿名ではないということを理解すると、ハンドルネームであっても、インターネットの使い方に気をつけようと意識するようになったのである。

そして、書き込む時に、「常識を持って、『これは書いたらまずい』というものを書かないようにする」「あまり直接的な書き込みはしない」「きつい言葉は書かない」「言い方や相手の気持ちを考えて書き込む」「信頼できないとこには書き込まない」「あまり書き込まないようにする」[4)]と、匿名ではないことを意識するようになった。

このように、ワークショップ後に、生徒は、書き込みをする時に、匿名であっても、自分の発言に責任を持つことを意識するようになった。いわば、技術的な理解が、従来、モラルと言われている考え方をよりいっそう定着させたのである。

特に、積極的に情報を発信している生徒は、インターネットが繋がる仕組みを理解し、セキュリティ意識がより高まる結果を示した。

(2) インターネット上にアップロードした情報は消すことができない

インターネット上に情報をアップロードすると、その情報を見た多数の人がダウンロードして見るため、数秒で情報が拡散する。さらに、自分の情報が編集されて、自分の知らないところで他人に勝手にアップロードされ、利用される可能性があることを解説した。

事前アンケートにおいて、「ネット上に友達の写真を載せても気にならない」「ネット上の写真を取り替えたら、元の写真は消えたと思う」「ネット上に載せた情報は、嫌になったら削除すればよい」の平均スコア[5]（「前・情報が消せると思うスコア」とする）を算出した。

次に、事後アンケートにおいて、「ネット上に友達の写真を載せても平気だと思いますか[6]」「ネット上に載せる情報には気をつけようと思いますか[7]」の平均スコア（「後・情報が消せると思うスコア」）を算出した。「前・情報が消せると思うスコア」および「後・情報が消せると思うスコア」は、リスクが高いほうが、スコアが高くなるように設定した。「後・情報が消せると思うスコア」と「前・情報を消せると思うスコア」の差を算出し、リスク・スコアの増減を検証した。各レベルともリスク・スコアの減少が認められた。各レベルのリスク・スコアが減少した値の平均値を算出した。レベル別に「前・情報が消せると思うスコア」および「後・情報が消せると思うスコア」の平均値をt検定した結果、有意な差が認められた。結果を表１の「情報の削除」に示す。

情報の削除について、63％（17名/27名）でリスク・スコアの軽減が確認できた。「レベル１」のグループ59％（10名/17名）、「レベル２」のグループ70％（７名/10名）は、リスクのスコアが減少した。情報発信をしている「レベル２」のグループの方が、リスク・スコアの減少ポイントが高かった。

すなわち、生徒は、「初めから個人情報などを載せない」「しっかり選んでネット上に載せる」「見られて困ることを書かない」「画像をアップするときは一考してからアップ」「載せる前にもう一度見て、載せてもよいものか考えてから載せる」「迂闊に載せない」[8]と述べている。

このように、ワークショップ後に、生徒は、自分の情報や友人の情報を載せることに慎重になったのである。

インターネット上にアップロードした情報は、技術的に考えると、完全に削除されないということを理解したことで、生徒はインターネット上に個人情報を載せることの危険性に気づいたのである。

特に、積極的に情報を発信している生徒は、自分が発信する情報に責任を持つことをよりいっそう意識するようになり、安全への関心が高まった。

表１　レベル別リスク・スコア減少の平均値

	リスク・スコア減少の平均値	
	匿名性	情報の削除
レベル１	0.37 **	0.76 **
レベル２	1.07 **	1.97 **

（平均値の t 検定　** $p<0.05$ ）

(3) サイバーテロの仕組み

データやファイルをダウンロードする時に、ウィルスやスパイウェアが侵入する可能性があること、そして、ウィルスやスパイウェアが入っていることに気づかずにサイバーテロに加担する可能性があることを解説した。そ

して、基本的な対策として、セキュリティ対策ソフトの導入や知らない人からのメールや添付ファイルを開かないこと、信頼できないところからデータやファイルをダウンロードしないこと、インターネットやパソコンは使わないときには電源を切断すること等を実践的に指導した。

その結果、自由回答に、「ウィルス対策ソフトを入れる」「パソコンを使わないときは電源を消す」「使わないときはインターネットを切断する」「誰が書いたのか分からないHPには入らない」「安全なサイトからダウンロードできるものはそうして、危険なところからしかできないものはしない」「ちょっとでも怪しいサイトは開かない」などの意見が寄せられた。

このように、ワークショップ後に、生徒は、不正侵入される仕組みを理解し、セキュリティ対策を十分にとる必要があることを理解した。

4.3 インターネット利用において経験した問題

ブログなどで写真や悪口を実際に見た経験があるかなど、実際に使う場面で起こりうる危険について、口頭で質問し○×で回答を得た。信頼できるデータは30名[9]である。内訳は、情報を読むだけのグループであるレベル１が20名、情報を積極的に書き込みしているグループであるレベル２が10名である[10]。

(1) 匿名性について

最も特筆すべき項目は、「ハンドルネーム（匿名）だから、何でも書いちゃう人がいると思う」という質問に対して、生徒全員が肯定したことである。匿名であると思って、自分の発言に気をつけない人がいると思っている。インターネット上で、匿名であると考えることで、モラルが低下することがうかがわれる。

(2) 悪口や噂話について

「ブログ（プロフ）で悪口を見たことがある」については、全体の半数、レベル２のグループでは８割もが肯定した。さらに、「ネット上に、誰のことかわかる噂話を見たことがある」については、全体では４割、レベル２のグループでは半数が肯定した。学校教育の場においてネットいじめは懸念される課題である。ブログの利用者は、悪口や噂話を目にしている現状があるようだ。

(3) 記入者の特定について

全体の７割、レベル２のグループでは、９割の生徒が「ブログ（プロフ）の内容から誰が書いたかわかることがある」と回答した。ハンドルネームであっても、記載された内容から、読み手が、書き手を知っているのである。

(4) 個人情報の漏えいについて

全体の３割、レベル２のグループでは半数が「ブログ（プロフ）で友達の名前や学校名を見たことがある」と回答した。「ブログ（プロフ）で友達の写真を見たことがある」生徒は３割に留まるものの、「ブログ（プロフ）で、友達が知り合いの写真を載せているのを見たことがある」は、レベル２のグループでは、半数が肯定した。自分の写真を載せることに気をつけても、友人の写真や名前、学校名などの個人情報が載せられていることを目にしているのである。他人の個人情報も、ネット上に載せないように指導を徹底する必要がある。

(5) ネット上の友達との交流

「ネットで気が合った友達には、メールアドレスを教えたことがある」と回答したのは、

全体では13%、レベル２のグループでは３割であった。不特定多数の人が参加しているインターネット上で、見ず知らずの人と友達になることの危険性について十分に指導することが必要であろう。

4.5　パソコンや携帯電話の使い方のルール

「家族で、パソコンの使い方について話し合ったことがある」について、全体の７割の生徒が否定した。ということは、パソコンや携帯電話の使い方のルールを決めていない家庭が多いことになる。そこで、少数であるがルールがあると答えた生徒に、決めているルールを尋ねたところ、「午後11時までの利用」のように時間や「上限の金額」「有料サイトに入らない」など利用金額に関するものがほとんどであった。

また、親から、「公式サイトのみ見てよい」「インターネットは、調べ物学習だけ」と制限をつけられていても、「ゲームをしちゃう」「掲示板を読む」など、実際には親の言うことに従っていないようだ。生徒は、親に管理されることを嫌がっていた。

生徒は、「自分で安全に使いたい」との意思を示した。そのため、生徒が、自ら安全に使えるように、セキュリティ知識を学習する機会を与え、危険を回避できる判断力をつけるような指導が望ましいと考える。

一方、本調査では、７割の家庭において、パソコンを家族みんなで利用していた。情報の漏えいを防ぐには、パソコンを利用する家族全員が、それぞれパソコンを安全に管理する意識、特に、データをダウンロードすることの危険性を理解する必要がある。しかし、「ファイルをダウンロードするときに、誰かに相談する」と回答した生徒は、全体で３割、レベル2のグループでは1割であった。生徒は、多様な目的で利用するようになるにつれ、パソコンの使い方を知っていると自分の能力を過信して、誰にも相談することなく情報をダウンロードしている。インターネットで情報を発信する生徒ほど、自分の判断でダウンロードしているのである。

一般に、情報漏えい事件の原因は、データを共有化するプログラムがパソコンにダウンロードされていたり、共有に設定されていたりする場合が多い。利用する家族が勝手にデータやファイルをダウンロードすることで、情報漏えいの危険性が高まる。インターネットを利用する以上、利用者は、データやファイルをダウンロードすることの意味を理解し、危険性を判断する能力が求められる。

4.6　生徒の質問から

インターネットの安全な使い方を十分理解したと思われる生徒から、「ブログを利用している時、アバターにディズニーなどのキャラクターを利用してよいのか」という具体的な質問が上がった。知識として、著作権について注意しなければならないことを知っているが、実際に自分が情報を発信する場面になると、使い方について不安を感じるようだ。その生徒はかなり多様な使い方をしているが、安全意識も高いと思われた。しかし、このような生徒であっても、知識と実際に使う場面が結びついていないということが明らかとなった。

そのため、インターネットの安全な使い方についてモラルを教える一方、実際に使う場面で、どのような危険性が潜んでいるのかを具体的に指導することが望ましいと考える。

4.7　ワークショップのまとめ

ワークショップを実施した結果、中学生になれば、インターネットが繋がる仕組みを技

術的に理解することができること、技術的な理解はモラルを定着させ、安全意識を高めることを検証した。

さらに、インターネット上に、いじめの温床となる悪口や噂話を見聞きすることがあり、匿名であっても記入した人が誰かを特定できたり、個人情報が表示されていることがあるなど、生徒間にトラブルが起こりうる状況であることが顕在化した。ハンドルネームを用いると匿名であると思い、いじめにつながる書き込みを安易にしてしまうのだろう。だからこそ、インターネット上では技術的には匿名ではないと知ることは、いじめに繋がる発言を抑え、モラル意識を支えることになる。

さらに、中学生は、親に管理されるのではなく、自分で安全にインターネットを利用することを望んでいるため、情報発信をする生徒には、実際に使う場面に応じた安全教育が望ましいことが明らかとなった。

そのため、生徒が、自ら安全に使えるように、セキュリティ知識を学習する機会を与え、危険を回避できる判断力をつけるような指導が望ましいと考える。

5．考察

情報を発信するツールが多様化し、子どもが、対戦ゲームをやったり、ゲームの攻略方法を知る為に掲示板に投稿したり、ブログ（プロフ）や動画サイトへの投稿をする状況になってきている。唯野は、インターネット上の発言がトラブルへ発展した2004年の佐世保で起きた小学六年生の女児殺害事件を受けて、子どものインターネット利用について、情報発信者になるときに、『ネットで公開してよいもの、悪いものを判断する能力』が重要であると指摘している[1]。

小学生のうちは、情報を発信する児童はわずかである[2]が、中学生になると４人に１人が、複数のコミュニケーションツールを利用して情報を発信するようになり、いまや、情報を発信する生徒は特別な存在ではなくなっている[3]現状がある。情報教育において、情報を発信する時や情報を受け取る時のモラルに重点が置かれるようになってきている。

本研究は、モラルを定着させるために、インターネットの繋がり方を技術的に学習する効果を検証した。すなわち、情報発信者の責任として、情報を発信する時に、「してはいけないこと」をモラルとして説くだけではなく、生徒がインターネットの仕組みについて技術的に理解をすると、なぜ「してはいけないのか」理由を理解し、モラル違反を抑止することになり、ひいては、モラルを定着させ、インターネットの安全な利用につながることを検証した。

具体的には、①ハンドルネームを使って「匿名」だから何でも発言してよいのではなく、ネット上の経路をたどれば発信元を特定できるため、実際には「匿名」ではないことを生徒が理解すると、発言内容に気をつけるようになること、②インターネット上に発信した情報を完全に回収することはできないことについて技術的に理解することで、生徒が発信する情報について慎重になること、③サイバー攻撃の仕組みとともにウィルスやスパイウェアについて技術的に理解することで、生徒は自分が使う機器を安全に管理するようになることの三点について検証した。

インターネットの技術的な理解がモラルを支える事例として、2011年春に起きた大学入試問題漏えい事件を考えたい。この事件は、

高度な技術を用いた行為ではなく、携帯電話を利用した質問サイトへの投稿という単純なものであった。入試においてモラル上カンニングは「してはいけない行為」であるが、受験生がハンドルネームの匿名性を過度に信じたため実行してしまったという心理が見てとれる。もし、IPアドレスやMacアドレスにより、インターネットで発言した事項は、どこから発信したか経路がわかることをこの受験生が知っていたら、このような犯罪行為を実行しなかったであろうことは予想に難くない。また、この受験生は事件後すぐに自分のハンドルネームを削除していたが、「インターネット上に発信した情報は完全には削除できない」ことを知っていたら、この違反行為を実行することにためらいを感じたであろう。

連日テレビで報道された情報の専門家のやり取りによると、あまりにも初歩的な内容である「IPアドレスで発信元がたどれること」を知らない者の行為であるとは誰も予測していなかった。ところが、インターネットの技術的な仕組みについて基本を理解していないエンドユーザは多いのである。情報教育を高校時代から受けてきた大学生においても、セキュリティに関する技術的な知識不足が報告されている[4]。本調査に参加した中学生も、「匿名」であると思って、何でも書いている人がいると感じていた。インターネットを使い始める時に、インターネットが繋がる仕組みを学習する機会を設けることが必須である。

カリキュラム上はインターネットの繋がり方を学習させるように示唆され、情報の教科書や安全に使うためのパンフレットが配付されているが、実際に中学生に質問すると、インターネットの仕組みを学校教育の現場で学習した経験はなかった。

また、子どもがインターネットを利用する上で問題となるのが、ネットいじめである。本調査においても、生徒がネット上に本人を特定できる噂話を身近で見聞きしていた。日本ばかりでなくカナダやイギリスにおいても、かなりの中学生が、掲示板、チャットルームや画像投稿において、ネットいじめを経験していると報告されている[5][6][7][8][9]。そのため、イギリスでは、教育委員会や学校は、生徒が情報を発信することや携帯電話を学校に持ち込むことを禁止する傾向にある[10]。ところが、インターネット上の発言は発信元がたどれること、発信した情報が完全には削除されないことを理解すると、生徒は自分の発言内容に気をつけるようになるということを本研究は検証した。

すなわち、技術的な理解は、インターネット利用におけるモラルを定着させ、発信者の不正なことばのやり取りを抑止する。そのため、生徒から情報機器を取り上げるのではなく、安全意識を持ってインターネットを利用するように導くことが、将来の優れたエンドユーザを養成することになる。

唯野は、情報を発信することで、生徒がインターネット上で同じ趣味の人と交流することになり、個性を伸ばしたり、社会性を身につけたりというメリットを指摘している[1]。さらに、Sharplesらは、インターネットにおける情報発信能力は、学校においてディベイト能力へと発展すると述べている[10]。

唯野やSharplesらが議論するように、生徒のアクセスを禁止するのではなく、インターネット上にある危険性を知り、それに対処する能力を生徒が身につけられるような指導が重要である。そのためにも、生徒のインターネット教育に、技術的な理解を取り入れるこ

との重要性を提唱したい。

6．終わりに

技術的な理解を基にモラルを定着させるための情報教育をどのように実施したらよいのであろうか。児童生徒の実情を検討した報告によると、インターネット上でトラブルに遭遇した時には相談相手は親であり、教師に相談する児童生徒はいない[11]。一方、親は、情報安全教育を学校に望んでいるが、情報教育を学校現場に任せることは難しいのが現状である[1][6][10][12]。唯野が言うように、子どもを守るためには親の指導が欠かせないのである[1]。

しかし、インターネットの仕組みを技術的に理解し、子どもに伝えられる親は少ないだろう。さらに、本調査によると、中学生は、親から自立して、安全に使うために自分でルールを作ることを望んでいた。現在、親と子がともに学習できるような情報セキュリティサイト[11]は、技術的な理解を深める内容とはなっておらず、また、使いにくいとの評がある[2]。インターネットが技術的にみると発信元が特定されることを伝えているのは、総務省「国民のための情報セキュリティサイト」のみであった。しかも、サイトの最終更新が2003から2009年と古く、情報発信が多様化している現状を反映しているとは言い難いサイトもある。

そこで、金子らが実施しているように専門家による学校への出前授業[13]に加えて、地域貢献として、大学が公開講座のような形で情報教育の場を提供すること、「技術的な理解」を促すような、インターネット安全利用のための実践的な学習サイトの設立を提案する。

謝辞　本研究は、平成20年度科学費補助金（奨励研究）（課題番号20909036）の成果である。また、本研究の調査にあたって、さがみはら市都市みらい研究所より多大なるご協力を得た。ここに謝意を表したい。

注

1）そのうち、信頼できる回答者27名の分析を中心とする。ただし、4-3のみ、信頼できる回答者数は30名である。

2）「とてもそう思う」4ポイント、「そう思う」３ポイント、「あまりそう思わない」２ポイント、「全くそう思わない」１ポイント。スコアが高いほうが、リスクが高くなるように設定した。

3）逆転して、「とてもそう思う」１ポイント、「そう思う」２ポイント、「あまりそう思わない」３ポイント、「全くそう思わない」４ポイント。スコアが高いほうが、リスクが高くなるように設定した。

4）自由記述から。

5）「とてもそう思う」4ポイント、「そう思う」３ポイント、「あまりそう思わない」２ポイント、「全くそう思わない」１ポイント。スコアが高いほうが、リスクが高くなるように設定した。

6）「とてもそう思う」４ポイント、「そう思う」３ポイント、「あまりそう思わない」２ポイント、「全くそう思わない」１ポイント。スコアが高いほうが、リスクが高くなるように設定した。

7）「とてもそう思う」１ポイント、「そう思う」２ポイント、「あまりそう思わない」３ポイント、「全くそう思わない」４ポイント。スコアが高いほうが、リスクが高くなるように設定した。

8）自由記述から

9）注１参照

10）以下、ケース数が少ないため、割合で記述する。

11）　キッズgoo（http://kids.goo.ne.jp/index.html）、警察庁@police（http://www.cyberpolice.go.jp/）、総務省「国民のための情報セキュリティサイト」（http://www.soumu.go.jp/joho_tsusin/security/index.htm）、警視庁「ハイテクキッズ」http://www.keishicho.metro.tokyo.jp/haiteku/hikids/

hikids11.htm独立行政法人　情報処理推進機構（IPA）http://www.ipa.go.jp/security/index.html）

参考文献

1）唯野　司『ネット犯罪から子どもを守る』毎日コミュニケーションズ（2006）

2）松村真木子「家族で考える情報セキュリティ―小学生親子のパソコン、携帯電話とインターネットの利用実態調査と安全対策」『平成21年度　自主研究報告書』さがみはら都市みらい研究所、pp77-109（2010a）

3）松村真木子「パソコンおよび携帯電話の技術的知識を中心とした情報セキュリティ学習プログラム―中学生を核とした家族への情報セキュリティ知識の伝達―」『平成21年度　自主研究報告書』さがみはら都市みらい研究所、pp111-154（2010b）

4）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へ向けて―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』第48巻第９号（2007）

5）2005年度　情報セキュリティインシデントに関する調査報告書ver1.0、NPO日本ネットワークセキュリティ協会（2006）（http://www.jnsa.org/result/2005/20060803_pol01/index.html）

6）2005年度　情報セキュリティ推奨教育の検討に関する調査報告書、NPO日本ネットワークセキュリティ協会（2006）（http://www.jnsa.org/result/2005/20060601_edu01.pdf）

7）Li Q. :Cyberbullying in school :a research of gender differences, School Psychology International vol.57, pp157-170 (2006)

8）Smith P. et al.: An investigation into cyberbullying, its forms, awareness and impact, and the relationship between age and gender in cyberbellying. A report to the Anti-Bullying Alliance (2008)

9）Byron T.: Safer Children in a Digital world: The Report of the Byron review. Department for Culture, Media and Sport (2007)

10）Sharples, M. et al. : E-safety and Web 2.0 for children aged 11-16, Journal of computer assisted learning vol.25 pp.70-83

11）松村真木子「年齢に応じたITセキュリティ教育の構築に向けて―インターネット利用における小中学生と親と学校との関係―」『浦和大学論叢44号』（2011）

12）Green H. and Hammon C.: Their space: Education for a Digital Generation (2008)

13）金子正光・竹之内修・田島大輔「子どもたちを加害者にも被害者にもしないインターネット安全教室の現状と対策―宮崎市内の小学校における情報モラル教育の調査」宮崎公立大学人文学部紀要vol.16, No.1. pp23-44（2009）