

情報社会における危険回避に対する意識を向上させるための
授業実践とその効果

宮川 洋一 ・ 佐藤 和史

岩手大学教育学部研究年報 第74巻 別刷
平成27年3月

Reprinted from the Annual Report of
the Faculty of Education, Iwate University, Vol.74
March 2015

情報社会における危険回避に対する意識を向上させるための 授業実践とその効果

宮 川 洋 一* ・ 佐 藤 和 史**

(2014年9月30日受付, 2014年12月22日受理)

1. はじめに

本研究の目的は、技術・家庭技術分野（以下、技術科）における情報社会における危険回避に対する意識を向上させるための授業実践・評価を行うことである。

総務省の平成23年度版情報通信白書は、平成10年度以降、ICT環境の変化によるインフラ、ICT活用等の変化は大きなものがあるものの、変わらない課題として「デジタル・デバイドの解消」と「安心・安全の確保」があると示している¹⁾。特に、「スマホ革命」といわれる現在、「安心・安全の確保」の問題は急務である。

このような状況下、文部科学省は平成22年10月に、現行学習指導要領の内容を踏まえ、「教育の情報化に関する手引」刊行し、その第5章において、発達の段階に応じた情報モラル教育の必要性や具体的な指導内容等について解説している。例えば、情報モラル教育の基本的な考え方として、「社会の情報化が進展する中で、情報化の『影』の部分をも十分理解した上で、情報社会に積極的に参画する態度を育てることは、今後ますます重要になる。児童生徒の間にも携帯電話やパソコンなどを通じたインターネット利用が急速に普及し、インターネット上での誹謗中傷やいじめ、インターネット上の犯罪や違法・有害情報などの問題が発生しており、こうした問題を踏まえ、『情報モラル』について指導することが必要となっている。」²⁾としている。また、児童生徒の実態として「多くの児童生徒はインターネット上の危険に対して無防備な状態で、しかも、自分が危険な目に遭いかねない状態であることも分からずに利用している。何気なくプロフィールサイト（プロフ）に書き込んだ個人情報や悪気のない掲示板への書き込みが世界中に発信されていることや、対面のコミュニケーションとは異なり、それは記録され、削除されない限りいつまでも残る可能性があること、悪質な書き込みが犯罪となったり訴えられたりするケースもあるとの認識も低い。インターネット上のトラブルに関係する被害者、加害者も低年齢化している状況にある。中でも、携帯電話は、児童生徒にとって最も身近なインターネット端末となったが、児童生徒は携帯電話の小さな画面が世界中に繋がっていたり、主に文字だけの情報交換となったり、従来のコミュニケーションとは異なることを理解しないまま利用している。したがって、情報モラル教育には、即座に出遭うかも知れない危険をうまく

* 岩手大学教育学部

** 岩手大学教育学部 附属中学校

避ける知恵を与えるとともに、一方では、情報社会の特性の理解を進め、自分自身で的確に判断する力を育成することが求められる。」³⁾と指摘している。

これは、正しい知識を形成し、望ましい意識を醸成した上で、未知の危険に対して、思慮深く、思考・判断していく力の形成をしていく必要があることを示している。一方、いわゆる思考力・判断力を形成していく指導は、正しい知識・技能を形成し、意識の醸成をした上で成される高度な指導内容である。そのため、各教科等・領域等の特性を生かしながら、数時間扱いの題材を開発していく必要がある。

そこで、本研究では、情報モラルの指導内容が具体的に位置づいている技術科において、思考力・判断力を形成していく際に前提となる、知識の形成と意識を醸成する授業実践を行い、その効果を検証し、今後の思考力・判断力を形成しうる題材開発の足かりとする。具体的には、生徒にとって身近である個人認証（本人の知識を利用する、いわゆるパスワード）を取り上げた危険回避に対する意識の向上を高めることをねらいとした4時間扱いの題材開発と評価を試みる。

パスワードに対する教育に関する先行研究では、大学を対象とした研究がいくつか成されている。例えば、八城は、本研究においても教材として取り上げている「マイクロソフトのセキュリティとセキュリティーセンター」⁴⁾を利用した教育実践を行い、問題意識及び情報に関する知識をもっている学生には、パスワードの定期的な変更等に関する意識に一定の効果が認められる一方、意識の低い学生に対する効果は不十分であると指摘している⁵⁾。また、加藤らは、本人認証技術におけるユーザの性格とセキュリティ意識との相関に関して考察を行い、学生のセキュリティに対する意識の低さを指摘するとともに、性格とセキュリティの意識との間にある程度の関係性が存在することを指摘している⁶⁾。このように、大学生を対象とした研究では、学生の安全・安心に対する「意識」の低さが問題として取り上げられている。一方、中学校においては、パスワードを扱う授業実践が成されていることは、教科書などからも容易に想定できるが、題材を構成して実践し、その授業効果をデータに基づき検証している報告は、筆者らの知る限り見当たらない。この問題に対応していくためには、義務教育の段階から、正しい知識・技能と意識の醸成を地道に、スパイラル的に積み上げていく必要があると考えている。

なお、本研究における「情報モラル」とは、小学校、中学校、高等学校及び特別支援学校の学習指導要領解説総則編及び道徳編において示されている「情報社会で適正に活動するための基となる考え方や態度」とし、その具体的な内容としては同様に示されている「他者への影響を考え、人権、知的財産権など自他の権利を尊重し情報社会での行動に責任をもつこと」、「危険回避など情報を正しく安全に利用できること」、「コンピュータなどの情報機器の使用による健康とのかかわりを理解すること」としている⁷⁾。

2. 手続き

2.1 調査対象者

A中学校2年生 男子20名 女子18名 計38名

2.2 指導内容

(1) 主題 ネットワークの仕組みと個人認証

情報社会における危険回避に対する意識を向上させるための授業実践とその効果

段階	時間	予想される生徒の反応	教師の支援
導入	15	<p>□気にしていなかった身近なことを振り返る。</p> <ul style="list-style-type: none"> ・Windows7になった。 ・タッチパネルになった ・パスワードを要求されるようになった ・パスワードについて気にしなかった <p style="text-align: center;">ネットワークで使用するパスワードについて知ろう</p> <p>□ネットワークの利点と欠点について挙げる。</p> <p>【ネットワークの利点】</p> <ul style="list-style-type: none"> ・遠くの人とコミュニケーションがとれる。 ・様々な情報を集めることができる。 ・買い物など様々なサービスを受けられる。 <p>【ネットワークの欠点】</p> <ul style="list-style-type: none"> ・ウィルスに感染する ・個人情報が盗まれる ・プライバシーを侵害される ・不正利用される（遠隔操作） ・ハッキングされる <p>□不正に利用されないための仕組みを知る。</p> <ul style="list-style-type: none"> ・パスワードがある。 ・ウィルス対策ソフトがある。 <p>◆個人認証によって利用制限がかかっていることを実感する。</p>	<p>○パスワード入力画面が表示されることにどれくらい関心があるかを確認する。</p> <p>※OS等スペックが変更したことに興味を示すと思われる。パスワード入力画面については教師が取り上げる。</p> <p>○ネットワークの利点と欠点について知らせる。</p> <p>【ネットワークの利点】</p> <ul style="list-style-type: none"> ・情報の共有 時間削減（効率化・再利用） リスク・負担の軽減 コミュニケーション活性化 ・機器の共有 メンテナンス削減 コスト削減 <p>【ネットワークの欠点】</p> <ul style="list-style-type: none"> ・不正利用 改ざん・遠隔操作・漏えい <p>◇コンピュータやプリンタを共有している場面を紹介する。</p> <p>※機器が共有できると便利な反面、危険なことを再確認する。</p> <p>○不正に利用されないための仕組みについて知らせる。</p> <ul style="list-style-type: none"> ・個人認証（IDとPassで利用者を特定） <p>◇個人認証によって利用制限がかかっていることを体験させる。</p>
		<p style="border: 1px solid black; padding: 5px;">どのようにすれば強いパスワードになるのか</p>	
展開	15	<p>□既存の知識からパスワードを作成するとき気を付けることを挙げる。</p> <ul style="list-style-type: none"> ・生年月日・電話番号などを使用しない ・名前や単語等予想される言葉を使用しない ・単純な続き文字や繰返し文字を使用しない <p>◆パスワードを作成する。</p> <ul style="list-style-type: none"> ・パスワードチェッカーで考えたパスワードの強度を確認する ・作成とチェックを繰り返しながら規則性があるかどうかを探る ・適当に入力して変化を観察する 	<p>○パスワードを作る時に気を付けることについて考えさせる。</p> <p>※ダメなパスワードの例を提示し、生徒の既存の知識を確認する。</p> <p>◇強いパスワードを考えさせる。</p> <ul style="list-style-type: none"> ・Microsoft社のパスワードチェッカーを使用して強力なパスワードを作成する <p>※強いパスワードとは、他人に予想されにくい、もしくは解析されにくいパスワードのことをいう。</p>
	10	<p>※規則性があることに気づく。</p> <ul style="list-style-type: none"> ・12文字以上入力すると評価が変化する ・使用する種類が多いと少ない文字数で解析が難しくなる <p>2種類以上のだと11文字 3種類以上だと10文字</p> <p>□少ない文字のパスワードは簡単に解析できることを理解する。</p> <ul style="list-style-type: none"> ・4文字程度であれば10秒かからない ・解析に1秒もかからないとは意外だった ・予想通り瞬時に解析できる <p>□文字数と解析時間の関係について知る。</p> <ul style="list-style-type: none"> ・ある程度の文字数からは時間がかかる 	<p>※セキュリティが高くなる規則性があることに気付かせる。</p> <ul style="list-style-type: none"> ・文字（数字含み）・記号を組み合わせる。 ・12文字以上を使う <p>○少ない文字数だと簡単に解析されることを知らせる。</p> <ul style="list-style-type: none"> ・擬似パスワード解析ソフトを使用して4ケタのパスワード解析に時間がかからないことを知らせる。 <p>○文字数によって解析にかかる時間をまとめた資料を配布する。</p>
終結	10	<p>□今日の授業をふり振り返り、掲示板に書き込む</p> <ul style="list-style-type: none"> ・使用する文字数を12文字以上したり、記号や数字などを使用したりすると解析する時間がとても多くなるので、パスワードを作るときには文字や数字、記号を使って12文字以上にするように心がけたい。 ・不正利用などされないように、強いパスワードを使用するように心がけたい。 ・強いパスワードの作り方が分かった。 	<p>○振り返りを促す。</p> <ul style="list-style-type: none"> ・今日の授業で大事なことを掲示板に書き込ませる。 ・他の書き込みを確認させる。 <p>◆記入した内容を踏まえ学びの様子を発表させる。</p>

図1 第1時の授業内容

段階	時間	予想される生徒の反応	教師の支援
導入	10	<ul style="list-style-type: none"> <input type="checkbox"/> 前時の書き込みを再確認する。 ・書き込みを再確認する ・コメント入力をする ・理解したことを再確認する <input type="checkbox"/> 前時の学習内容を振り返る ・使用者を判断するために個人認証システムがある ・パスワードを制作するときは12文字以上で、多くの種類を使用するとよい <input type="checkbox"/> インターネット上のサービスを挙げる ・メール、掲示板、チャット ・web ページブログ、プロフ ・ネットショッピング、ネットオークション 	<ul style="list-style-type: none"> <input type="checkbox"/> 前時の書き込みを再確認させる。 ※良いと思った書き込みにコメント入力させる。 <input type="checkbox"/> 前時の学習内容を確認する。 ・個人認証 (ID パスワード) ・文字、数字、記号など多くの種類を使用する ・12文字以上で考える <input type="checkbox"/> インターネットでどんなことができるか。 ・インターネット上のサービスは基本的に情報の交換であることを知らせる
	<div style="border: 1px solid black; padding: 2px; display: inline-block;"> 情報を伝える仕組みはどうなっているのか </div>		
展開	20	<ul style="list-style-type: none"> <input type="checkbox"/> ネットワークの構成について確認する。 ・ネットワークの規模などの違いによって呼び名が違うことを知る ・構成している機器を確認する ・プロバイダを介してインターネットに接続されていることを確認する ・ネットワークをそれぞれつないだものがインターネットだということを知る <input type="checkbox"/> 「古いサイト」のサービスを利用する。 ・気にしないで情報を入力し、診断結果に一喜一憂する。 ・メールアドレスに関しては危険だと感じて、生年月日での占いをする。 ・占いをしないで他の人の様子をうかがう。 <input type="checkbox"/> ネットワーク上で行われている情報通信の仕組みを確認する。 ・コンピュータ1台1台にIPアドレスが降られていることを知る ・IPアドレスを使用して、特定のコンピュータと通信が行われていることを理解する ・情報通信には決まりがあることを知る ■ アドレスや電話番号などは個人情報なので入力しない方がよいと思ったから。 <input type="checkbox"/> 情報通信の仕組みから、 ・書き込みした個人を特定できることに驚く ・記録が残ることを知る 	<ul style="list-style-type: none"> <input type="checkbox"/> ネットワークの構成について説明する。 ・ネットワーク 2台以上のコンピュータが有線、もしくは無線で通信ができるようになっている状態 【用語】有線、無線、ハブ ・LAN (ローカルエリアネットワーク) ⇒コンピュータ室 ・WAN (ワイドエリアネットワーク) ⇒岩手大学ネットワーク (附中と大学) ・WWW (ワールドワイドウェブ) ⇒インターネット <input type="checkbox"/> インターネット上のサービスを疑似体験させる。 ・使い勝手を評価する仕事を紹介し、これから紹介するサイトの評価をしてほしいと告げる。 ・情報サイトの「古いサイト」を使用させる <input type="checkbox"/> ネットワーク上で行われている情報通信の仕組みについて説明する。 ・コンピュータにはユニークな名前が付いている (IPアドレス) ・ユニークな名前は、その都度変わる。 ・細切れにして情報を送っている (パケット) ・細かい決まりがある (プロトコル) ※「古いサイト」を使用しなかった生徒がいた場合、使用しなかった理由を話してもらおう。 <input type="checkbox"/> 情報やりとりは記録が残ることを伝える。 ・「古いサイト」で集めた情報を紹介する。 ※通信の記録が残る (ログ)
	10	<ul style="list-style-type: none"> <input type="checkbox"/> パスワードで守ろうとしていたものを再確認する。 ・名前や電話番号などの個人情報 ・大事なデータ <input type="checkbox"/> 今までのネット利用について振り返る。 ・あまり重要でない情報でも、大量で関連付けが行われると、重要なデータに変わること気づく。 ※自分から情報を漏えいする場合があることに気づく。 	<ul style="list-style-type: none"> <input type="checkbox"/> パスワードで守りたかったものは何かを再確認する。 ⇒ 個人情報 <input type="checkbox"/> 今までのネット利用について見直しをさせる。 ※同一人物が複数のサイトを運営している場合があることを告げる。 ※コンピュータは大量のデータを処理するのに適していることを再確認する。
終結	10	<ul style="list-style-type: none"> <input type="checkbox"/> 今日の授業を振り返り、掲示板に書き込む。 ・パスワードをしっかりかけていても、自分自身で情報を漏らす場合があることに気づいた。インターネットで情報を入力する際には気をつけていきたい。 ・インターネットは便利である反面、危険な面もあるので気をつけて使用したい。 	<ul style="list-style-type: none"> <input type="checkbox"/> 振り返りを促す。 ・今日の授業で大事なことを掲示板に書き込ませる。 ・他の書き込みを確認させる。 ◆ 記入した内容を踏まえ学びの様子を発表させる。

図2 第2時の授業内容

情報社会における危険回避に対する意識を向上させるための授業実践とその効果



図3 第1時で使用した「マイクロソフトのセーフティとセキュリティセンター」⁴⁾

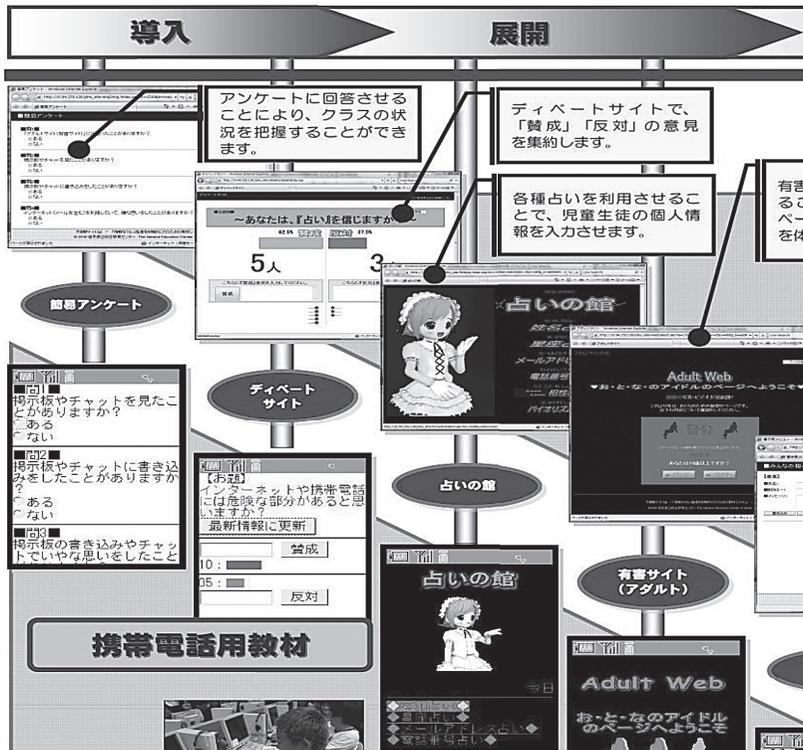


図4 第2時で使用した「占いサイト」⁸⁾

(2) 目標：評価規準「おおむね満足できる状況：B規準」

① 第1時（50分授業）

安全に情報を利用するための基本的な仕組みである個人認証について知り、その重要性に気づき、解析しにくいパスワードを作成する方法を説明できる（知識・理解）。

② 第2時（50分授業）

情報通信ネットワークの構成や使用されている機器などについて知り、その利用時に気をつけるべきことなど危険を回避する方法を知っている（知識・理解）。

③ 第3・4時（100分授業）

これまでの、自分自身の行動を振り返り、グループで発表しあったり、情報に関する技術が社会に果たしている役割と影響について考えたりして、安全に情報を利用するための方法を進んで見いだそうとしている（関心・意欲・態度、知識・理解）。

(3) 指導の実際

図1・図2に、実践的・体験的に学習した2時間の指導内容を示す。また、第1時で使用した教材「マイクロソフトのセーフティとセキュリティーセンター」⁴⁾、第2時で使用した教材「古いサイト」⁸⁾を、図3・図4にて紹介する。

第1時で使用した教材「マイクロソフトのセーフティとセキュリティーセンター」については、授業時におけるものである。なお、近年では、カスペルスキー・ラボ⁹⁾や仕様が公開されているパスワードチェッカー¹⁰⁾など、より使いやすいサイトもある。

第3・4時では、前時までの学習活動を踏まえて、より自分自身の問題として深くとらえさせるため、これまでの自分自身の行動を振り返らせたり（グループ活動）、教科書を用いて関連事項の補足説明をしったりして、第1時・第2時のまともも含めて授業を行った。

2. 3 指導効果の検証

本研究では情報モラルに対する意識について、質問紙を用いて検討を行う。そのために、宮川・森山の「情報モラルに対する意識尺度」を用意した。

本尺度は、6因子（[F1：ICT活用における危険回避に対する意識]、[F2：個人情報保護に対する意識]、[F3：情報機器使用における健康維持に対する意識]、[F4：情報社会における犯罪防止に対する意識]、[F5：ソフトウェアの不正コピーに対する意識]因子、[F6：ICT活用における著作権に対する意識]）、20項目で構成されている。また、先に述べた情報モラルの具体的な内容として示されている「他者への影響を考え、人権、知的財産権など自他の権利を尊重し情報社会での行動に責任をもつこと」を内容①、「危険回避など情報を正しく安全に利用できること」を内容②、「コンピュータなどの情報機器の使用による健康とのかかわりを理解すること」を内容③とした上で、内容①に対する因子として下位尺度をF2・F5・F6、内容②に対する因子として下位尺度をF1・F4、内容③に対する因子として下位尺度をF3とする構造になっている。質問に対する回答方法については、「とてもそう思う（5点）～まったくそう思わない（1点）」の5件法となっている¹¹⁾。

なお、質問紙の実施は、事前は、本実践の前1週間、事後は第4時の終末に実施した。

3. 結果と考察

3. 1 第1時・第2時における生徒の自己評価の様子

A校では、コンピュータ室を利用した授業の場合、自己評価をオンラインで行わせ、互いの学びの成果を可視化し、よりよい自己評価の方法を学ばせている。

ここでは、第1時・第2時の終了時に自己評価として掲示板に記述された内容について、その一部を表1・表2に示す。なお、第3時・第4時については、今回質問紙による意識調査を実施するため、コメントによる自己評価は、実施していない。

前述した評価規準(おおむね満足できる状況[B規準])に関して、オンラインの自己評価や、第3時・第4時の聞き取り調査の結果、第1時では、全38名のうち35名が、B規準をクリアしていたと判断された。また、同様に、第2時においては、37名の生徒が、教師の設定したB規準をクリアしていたと判断された。

表1 第1時における生徒の自己評価の例

	桁数の少ないパスワードや規則性のあるパスワードは簡単に見破られることがわかった。強力なパスワードをつくるには、桁数が多く数字や英字や記号など沢山の種類を盛り込んだパスワードをつくるのが大切だと感じた。
例)	強いパスワードには文字数を増やすことや、同じものを繰り返さないことが大切だということが分かりました。
	今日の授業で大切なのは、複雑なものほど、強いということが分かりました。これからつくるときに、いかしたいです。
	強いパスワードの作り方を考えてみて、なかなか思いつかず大変だった。でも、パソコンを使う上で大切になってくると思うので、忘れないようにしたい。

表2 第2時における生徒の自己評価の例

	自分の情報がLAN, WAN, WWWに分けられているのは知らなかった。また、IPアドレス, http, パケットなど、名前だけの存在だったものも今回の授業でよく理解できた。自らが発信する情報がどの程度の規模で露見されているのかを見極めて、今回の授業のようなことを本当のインターネット上でしでかさないように気を付けたい。
例)	情報をやり取りする際の規模が、LANやWAN, WWWで表されていることが分かりました。また、IPアドレスなど、個人認証などのシステムがあることがわかりました。
	今日の学習で、情報を伝えるのはパソコン同士ではなく、プロバイダなどを経由していることが分かりました。また、名前や住所などを書き込んでしまうと簡単にばれたりすることもあるので気軽に個人情報などを書き込まないように気を付けていきたいです。

3. 2 題材前後における情報モラルに対する意識の変容

本実践前後で「情報モラルに対する意識尺度」を用いた調査の結果を表3に示す。その結果、6因子のうち、F1:ICT 活用における危険回避に対する意識 ($t(37) = 2.56$ $p < .05$), F5:ソフトウェアの不正コピーに対する意識 ($t(37) = 2.06$ $p < .05$) の平均値に有意な伸びが認められた。このことから主に、パスワードを事例とした本題材における実践では、授業のねらいとしていた、危険回避に対する意識が促進されたことが示唆された。

また、特にねらいとしていなかったF5:ソフトウェアの不正コピーに対する意識の促進が見られた。これは、第2時においてIPアドレス等の情報伝達の仕組みを学び、情報漏洩の問題、特に情報の発信源が特定できることを知ったことによる抑制的な力が働き、有意差が生じたと考えられる。これは、主たる授業のねらいからすると副次的なものではあるが、指導時数がきわめて少ない技術科の授業では、仕組みを指導することにより、情報モラルに対する意識が向上するのであれば、例えば、6因子すべてについて直接扱う必要もなく、効果的に指導できる事例であると思われる。今後、このような実践事例を見いだしていくことも、技術科における情報モラル指導の役割であると考えている。

一方、第2時では、教材「占いサイト」を用いて、個人情報の漏洩を扱っているが、F2:個人情報保護に対する意識に有意差が認められなかった。これは、本実践ではあくまで、個人情報が無意図的に漏れてしまうという扱いをしているためであり、個人情報を積極的に保護していこうとする意識よりも、危険回避に対して強く意識が向いた結果であると考えられる。

表3 実践前後での情報モラルに対する意識の変容(N=38)

		事前	事後	対応のある t 検定
F1: ICT 活用における危険回避に対する意識	Mean	4.45	4.73	$t(37)=2.56$
	S.D.	0.56	0.46	*
F2: 個人情報保護に対する意識	Mean	4.44	4.49	$t(37)=0.41$
	S.D.	0.58	0.58	n.s.
F3: 情報機器使用における健康維持に対する意識	Mean	3.80	3.86	$t(37)=0.41$
	S.D.	0.71	0.92	n.s.
F4: 情報社会における犯罪防止に対する意識	Mean	3.73	3.73	$t(37)=0.07$
	S.D.	0.78	0.87	n.s.
F5: ソフトウェアの不正コピーに対する意識	Mean	3.49	3.84	$t(37)=2.06$
	S.D.	1.21	1.00	*
F6: ICT 活用における著作権に対する意識	Mean	3.64	3.91	$t(37)=1.58$
	S.D.	0.93	0.83	n.s.

* $p < .05$

4. まとめと今後の課題

本研究の目的は、技術科における情報社会における危険回避に対する意識を向上させるための授業実践と評価を行うことであった。これまでの、結果と考察に基づいて、本研究の実践条件下で得られた知見を以下に整理する。

情報社会における危険回避に対する意識を向上させるための授業実践とその効果

- (1) ネットワークの仕組みと個人認証という主題で取り組んだ4時間扱いの題材（取り上げた教材も含む）は、情報社会においてICTを活用する際の危険回避に対する意識を高める効果があることが示唆された。
- (2) IPアドレス等、情報伝達の仕組みを理解させることにより、情報モラルについて直接扱わなくても、特定の情報モラルに対する意識の向上が見られることが示された。

しかし、本研究の知見は、あくまで本調査対象校の実践条件の範囲内で、情報モラルに対する意識について、全体的な傾向として把握されたものである。今後は、多くの学校で実践を行い、本題材の有効性をさらに検討していく必要がある。その上で、情報社会に参画する上で、もっとも大切となる思考・判断力を育成する題材開発、そしてこれらの能力を評価する方法も含めて研究することが必要である。

また、パスワードは、私たちの生活において、最も身近なセキュリティ対策の一つである。近年の環境を考えると、パスワードに関する指導は繰り返し、定期的な変更に対する態度等を形成していく必要がある。なお、今後は小学校からパスワードに関する指導が増えてくる可能性もあることから、情報の科学的理解を中心としている技術科では、パスワードに対する攻撃方法の概要を理解した上で、それぞれに応じた対応方法について扱うことが必要になってくる可能性もある。

例えば、一般にパスワードに対する攻撃方法としては、大きく分けて次の三つがある。

a. 総当たり攻撃

高速なハードウェアを活用して、可能な組合せを全て試すやり方が総当たり攻撃である。対策としては、文字種と長さを増やすことになるが、パスワードのキャッシュファイルに対する攻撃の速度は、1秒間に数十億個といわれている。

b. 辞書攻撃

辞書に載っているパスワード、その末尾に数字を数文字追加しただけのパスワードは短時間に解読する攻撃方法である。辞書の大きさは数百万語に達するものもある。対策としては、辞書に載っている単語は使わない。または、載っていても良いが、2語以上（推奨3語以上）を連結文字でつないで、15文字以上の長い文字列にすることなどが有効である。

c. 類推攻撃

ターゲットの個人情報に関する知識から、攻撃者自身がパスワードを類推する攻撃方法である。通常、攻撃速度は非常に遅く、ツールを使えば辞書攻撃なみの速さとなる。

指導時数が少ない中学校技術科において、これらをどのように取り上げるかは、生徒の意識を基に教材化していく必要があるだろう。

これらについては、いずれも今後の課題としたい。

<付記>

本研究の一部は、平成24年度岩手大学教育学部プロジェクト推進事業の助成を受けたものである。

<引用文献>

- 1) 総務省 (2011) 情報通信白書平成23年版 PDF版. <http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/>

- h23/pdf/23honpen.pdf (参照日2014.9.28)
- 2) 文部科学省 (2011) 教育の情報化に関する手引. 開隆堂株式会社, 東京 p.117
 - 3) 前掲2) p.118
 - 4) マイクロソフト <https://www.microsoft.com/ja-jp/security/pc-security/password-checker.aspx> (参照日2013.2.1)
 - 5) 八城年伸 (2010) パスワードの作成に関する教育とその効果. 情報処理学会第72回全国大会講演論文集 平成22年(4):503-504
 - 6) 加藤岳久, 中澤優美子, 漁田武雄 [他] (2011) 本人認証技術におけるユーザの性格とセキュリティ意識との相関に関する考察. 情報処理学会 52(9):2537-2548
 - 7) 例えば, 文部科学省 (2008) 中学校学習指導要領解説 総則編. 株式会社ぎょうせい, 東京 pp69-70.
 - 8) 岩手県立総合教育センター http://www1.iwate-ed.jp/tantou/joho/moral/joho_site/index.html (参照日2013.2.1)
 - 9) カスペルスキー・ラボ <http://kasperskylabs.jp/ubi/wd/pwdchk/index.html> (参照日2014.11.27)
 - 10) みんなの知識ちょっと便利帳 http://www.benricho.org/password_meter/ (参照日2014.11.27)
 - 11) 宮川洋一, 森山潤 (2011) 道徳的規範意識と情報モラルに対する意識との関係. 日本教育工学会論文誌 35(1):73-82