N-010

情報セキュリティインシデントの擬似体験を通じた情報セキュリティ教育の多元的展開
Multifaceted Development of Information Security Education through Simulated Experiences of Information Security Incidents

花田　経子‡
Kyoko Hanada

1. はじめに

学校教育において情報教育を進めていくための施策が実施されるようになって 20 年以上が経過している。高等学校の情報教科の誕生や、中学校における技術・家庭科の技術分野での情報領域の取り扱いなど、教科として情報を教えることが進められるようになっている。また、情報モラル教育についても小学校中学校高等学校の正課における展開がなされるようになった。学習指導要領に記載されている教育課程については、学校側は適切に実施することが可能な仕組みが形作られているため、本来であれば情報教育のうち、情報モラル教育についても適切に実施されることが可能な環境にあるといえる。そして、年数を鑑みてもすでにある程度の教育実績と成果があらわれていて然るべき状況下に置かれていると判断できよう。

しかしながら、制度としては年数が経ち、適切に実施できている学校等もある一方で、残念ながら大多数の教育現場では十分な指導ができていると言い難い現状にある。情報モラル教育に関しては、子どもたちに対して安全かどうかが不明なサービス（例えば、プロフィール公開サービスやブログへのアクセス、学校裏サイトなどの学校外での情報共有サービスなど）に対してアクセスを控えさせるような教育が主流であった。またそのような環境下で、教師や保護者がそれらのサイトを監視し、問題のある投稿がないかをチェックするなどの活動も実施されていた。このような教師や保護者による無償の努力と、サービスそのものを利用させないという方向性にもとづく指導によって、かろうじて子どもたちの安全性が確保されている状況にあった。

2015 年以降、スマートフォンの普及によって子どもたちが利用する端末の性能が向上し、あらゆるサービスがスマートフォンから実施可能となった。また、SNS のような他者に対して閉じた環境でのコミュニケーションが可能なツールが浸透し、保護者や教師による監視ができにくい環境が醸成された。加えて、SNS や動画視聴サービスが展開するサービス形態は、個人の興味嗜好に対して的確に反映する情報を提供することが可能な形式を持っているため、マスコミュニケーションで展開されてきた情報の意図的かつ強制的な提供ができにくい環境が生まれた。インターネットサービスの普及とともに個人のスマートフォンを所有する年齢は年々下がり続け、子どもたちは SNS を利用し、情報の投稿や収集、コミュニケーションをほぼ一つの端末において実施している状況にある。さらに GIGA スクール端末の導入と現行学習指導要領による ICT 利活用教育の実施で、これまでサービスそのものを利用させないことで培ってきた情報モラル教育のあり方そのものを見直す必要性がでてきている。

子どもたちは学校現場における情報モラル教育を通じて確かに情報端末の安全な利用やそのために必要な対応方法を学ぶ機会を持っている。しかし、学校現場において生徒たちの SNS トラブルや SNS を使ったいじめ行為は低年齢化して、小学校においても指導の課題となっているのが現状である。また、子どもたちによる情報の不適切な取り扱いや行動が、児童ポルノなどの性犯罪被害・加害や、不正アクセスなどのサイバー犯罪に至ってしまう事案も増加している。

本稿では、情報モラル教育という形式の中で、本質的に必要とされる“情報セキュリティリスクリテラシ”をどのように実施していくことが可能かを検討している。学校現場での情報モラル教育は多くの時間を割くことが難しい現状にあるため、なるべく短期間で効率的に効果をもたらすことができるようにするための工夫を展開している。その手段として、本稿では情報セキュリティリスクに対する実効性ある教育活動を、短時間かつ簡易に実施していくための手段として、情報セキュリティインシデントを擬似体験しリスクに対する対応能力を向上させるためのボードゲーム型教材を提案している。さらに本教材を多元的に展開させていくことで問題解決を図ろうとしている。情報セキュリティインシデントの擬似体験をすることができる教材を用い、児童生徒のコミュニケーションを通じてその内容を定着させ、その上で効率よく学習することのできる多元的な教材展開を示すことが本稿の目的である。

2. 学習指導要領における情報セキュリティリスクリテラシの取り扱い

本来、社会全体における情報セキュリティ対策は、情報資産に関係しリスク要因となるすべての関係者に対して、同一のレベルの中で設定された対策が実施されることで有効性を発揮する。そして、すべての関与者自身が、情報資産やそれを扱う行為において、情報セキュリティリスクがどのように存在するかを認識した上で、リスクへの適切な対応をする能力――本稿では、この能力のことを“情報セキュリティリスクリテラシ”とする――を保有することが必要となる。本稿で取り扱う子どもたちにとっても、この情報セキュリティリスクリテラシは学習を適切に実施していく上で必ず身につけていかなければならない能力である。

子どもたちが学ぶ場として提供されている学校では、教育内容をカリキュラムとして定めている。このカリキュラムは、学校ごとや地域ごとに特色を持って作成されるものの、全国のどの地域で教育を受けても、ある一定の水準の教育を受けられるようにするため、学校教育法等に基づき、各学校でカリキュラムを編成する際の基準を定めている。これが、学習指導要領である。学習指導要領は、学校ごとのカリキュラムを編成する際の基準であるため、学習指導要領に定められている内容は何らかの形で必ずその学校のカリキュラムに組み入れられることが前提となっている。

したがって、現行学習指導要領で情報セキュリティリスクリテラシに該当する項目がどのように扱われているかを見ていくことが重要となる。

現行学習指導要領では、教育活動の目的として子どもたちの“情報活用能力”を育成していくことを求めている。この情報活用能力とは「世の中の様々な事象を情報とその結び付きとして捉え，情報及び情報技術を適切かつ効果的に活用して，問題を発見・解決したり自分の考えを形成したりしていくために必要な資質・能力」（文科省[1]）であり、図 1 のようにまとめられている。図 1 で示した情報教育の３観点８要素（以後、３観点８要素）において、「情報社会に参画する態度」は「情報モラル」とまとめられている。

【情報教育の３観点８要素】

情報活用の実践力
- 課題や目的に応じた情報手段の適切な活用
- 必要な情報の主体的な収集・判断・表現・処理・創造
- 受け手の状況などを踏まえた発信・伝達

情報の科学的な理解
- 情報活用の基礎となる情報手段の特性の理解
- 情報を適切に扱ったり，自らの情報活用を評価・改善するための基礎的な理論や方法の理解

情報社会に参画する態度
- 社会生活の中で情報や情報技術が果たしている役割や及ぼしている影響の理解
- 情報のモラルの必要性や情報に対する責任
- 望ましい情報社会の創造に参画しようとする態度

図１　情報教育の３観点８要素

さらに文部科学省は、図 2 のような『情報モラル教育モデル指導カリキュラム一覧表』を 2007 年に提供している(文科省[2])。この内容では、情報モラルに求められている要素を「情報社会の倫理」、「法の理解と遵守」、「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」の 5 項目に分類している。

図２　情報モラルモデルカリキュラム

本稿で扱う情報セキュリティリスクリテラシは、総務省[3]においてまとめられた“これからのデジタル社会において身につける能力”（以後、ICT リテラシ）のうち、情報セキュリティ上のリスクに特化したものである（表 1）。

情報セキュリティリスクリテラシ
1.プライバシーリスクへの対応能力
2.情報資産の安全管理能力
3.違法・有害情報リスクへの対応能力
4.法令遵守・炎上リスクへの対応能力
5.セキュリティインシデントへの対応能力
6.信頼できる情報を的確に入手できる能力

表１　情報セキュリティリスクリテラシ

表 1 で示した項目が図 2 において展開されているかを確認してみると、ほぼすべての領域で取り扱いがあることがわかる。したがって、学習指導要領上の情報モラル教育では、本稿でのべる情報セキュリティリスクリテラシが展開されることを想定した教育であると位置付けられる。したがって、情報セキュリティリスクリテラシを学校現場にお置いて実施する際には、十分な情報モラル教育が展開されていれば大きな問題はないといえる。

3. 学校現場における情報モラル教育の抱える課題

上記のように、学校教育現場で情報モラル教育は長年実施されている。しかしながら、総務省が毎年実施している ILAS の結果などからもわかるように、情報モラル教育が十分に効果をあげているとは言い難い現状がある（総務省[4]、表 2）。

総　合		71.4%	(前年度 71.1%)
1.違法有害情報リスク	1a. 違法情報リスク 著作権、肖像権、出会い系サイト等	75.0%	(前年度 75.1%)
	1b. 有害情報リスク 不適切投稿、炎上、閲覧制限等	69.5%	(前年度 68.4%)
2.不適正利用リスク	2a. 不適切接触リスク 匿名SNS、迷惑メール、SNSいじめ等	77.7%	(前年度 77.6%)
	2b. 不適正取引リスク フィッシング、ネット上の売買等	59.6%	(前年度 60.3%)
	2c. 不適切利用リスク 過大消費、依存、歩きスマホ、マナー等	80.7%	(前年度 79.7%)
3.プライバシー・セキュリティリスク	3a. プライバシーリスク プライバシー、個人情報の流出等	67.0%	(前年度 66.2%)
	3b. セキュリティリスク ID・パスワード、ウイルス等	70.6%	(前年度 70.2%)

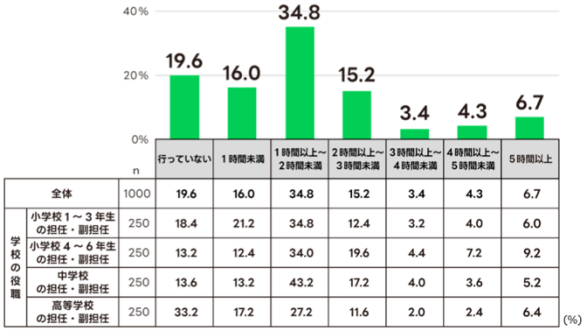
表２　リスクごとの正答率（総務省 ILAS）

その主な原因として、次の３項目があげられる。
(ア)　実施時間数の不足
(イ)　実施教科・実施形態の不明確さ
(ウ)　実施内容のミスマッチ

時間数については、LINE みらい財団[5]の調査結果から、1 時間～2 時間程度の時間を割り当てていることがわかる（図 3）。花田・砂原[6]において詳細に示したように、情報モラル教育が学校におけるカリキュラムの中であまり重要な教育項目として割り当てられていない現状がわかる。

次に、実施教科・実施形態の不明確さについては、LINE みらい財団[5]の調査結果から同様に総合的な学習の時間での教科配分であることがわかる（図 4）。さらに、教科担

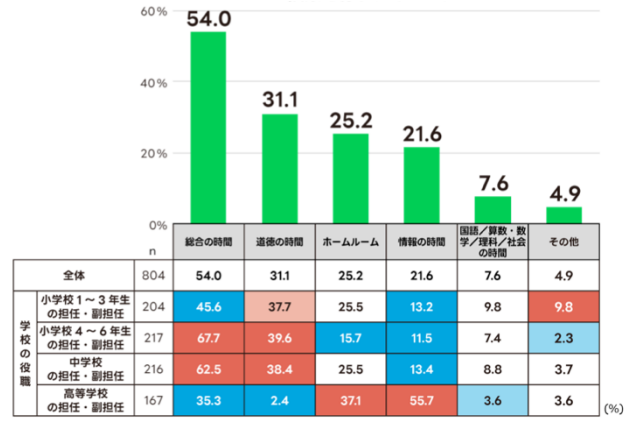
当が直接実施するのではなく、外部講師を招いて実施し、その後ホームルームや道徳教科で振り返りを実施して終了するという形での内容が主である。このような状況下で、有効性の高い情報モラル教育を実施することはかなり難しい現状にある。



		n	行っていない	1時間未満	1時間以上～2時間未満	2時間以上～3時間未満	3時間以上～4時間未満	4時間以上～5時間未満	5時間以上
全体		1000	19.6	16.0	34.8	15.2	3.4	4.3	6.7
学校の役職	小学校1～3年生の担任・副担任	250	18.4	21.2	34.8	12.4	3.2	4.0	6.0
	小学校4～6年生の担任・副担任	250	13.2	12.4	34.0	19.6	4.4	7.2	9.2
	中学校の担任・副担任	250	13.6	13.2	43.2	17.2	4.0	3.6	5.2
	高等学校の担任・副担任	250	33.2	17.2	27.2	11.6	2.0	2.4	6.4

(%)

図 3　情報モラル教育の実施時間



		n	総合の時間	道徳の時間	ホームルーム	情報の時間	国語／算数・数学／理科／社会の時間	その他
全体		804	54.0	31.1	25.2	21.6	7.6	4.9
学校の役職	小学校1～3年生の担任・副担任	204	45.6	37.7	25.5	13.2	9.8	9.8
	小学校4～6年生の担任・副担任	217	67.7	39.6	15.7	11.5	7.4	2.3
	中学校の担任・副担任	216	62.5	38.4	25.5	13.4	8.8	3.7
	高等学校の担任・副担任	167	35.3	2.4	37.1	55.7	3.6	3.6

(%)

図 4　情報モラルの実施教科

実施内容のミスマッチについては、総務省 ILAS（総務省[4]）に実際に情報モラル教育として教わった内容が示されている（図 5）。

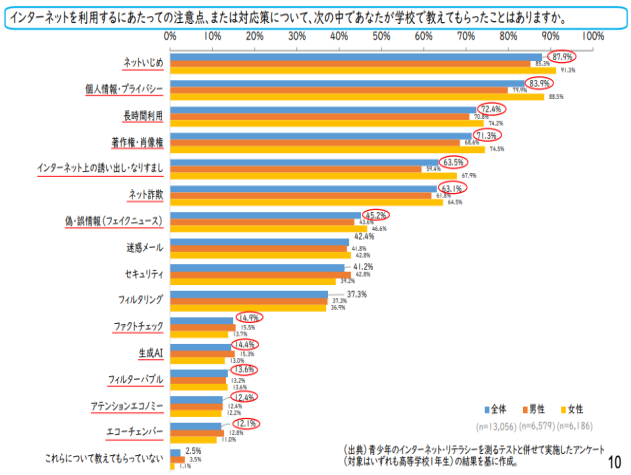


図 5　実際に教わった内容（総務省 ILAS2024）

図 5 と表 2 を見比べると、教わった比率が高くても正答率が低い項目がいくつかある。例えば、個人情報やプライバシーについてはかなりの生徒が教わっていると回答しているのにも関わらず、正答率があまり高くない。これは教えた内容が定着していない上に、実際のトラブルに遭遇した際に活かすことができるような教育方法ではなかったことが背景にある。また、表 2 の結果で特にポイントが低い不適正取引リスクについては、教わっていない可能性の方が高い。この場合、子どもたちは自分が既に持っている何らかの知識で回答を行うため、知識を持っている子どもと知識を持っていない子どもの差が広がる可能性がある。特に、不適正取引リスクのような要素の場合、実際に何らかの形でインターネット上における金銭的な取引を行った経験のある子どもとない子どもでは経験値が異なるため、知識に差が出る可能性がある。また、この場合子どもたち自身がトラブルに対応する場合において最適な対応をしているとは限らないため、金銭や身体等に対する直接・間接的被害を受けているリスクが発生していることを否定できない。

以上より、学校現場における情報モラル教育が、情報セキュリティリスクリテラシを獲得するための十分な場となっていない。この現状を改善するための教育活動の取り組みについて次に述べる。

4. インシデントの擬似体験とコミュニケーションを通じた学習

花田・砂原[6]では、情報セキュリティリスクリテラシを教育していくために教材の検討を行なった。その教材が満たすべき要件を次の 4 要件としてまとめている。

- 要件 1：児童・生徒の苦手とするリスクを重点的に教育することができる教材
- 要件 2：教員研修の中であらかじめ学んでおくことで、複雑化する指導に柔軟に対応できる教材
- 要件 3：教員研修においても短時間で有効性の高い教材
- 要件 4：児童・生徒のセキュリティインシデントにどのように対応すればいいのか（特に指導のタイミング）がすぐに判断できる教材

この要件は、教育を実施する側である教員と子どもを見守る立場である保護者の立場でまとめられたものである。

教育を受ける子どもに対して適用するべき要件としては、次の 3 要件が整理できる。

- 要件 1 ：情報セキュリティリスクをすぐに把握することのできる教材
- 要件 2 ：外部講師が 1 時間程度で実施した場合でも的確に理解させることのできる教材
- 要件 3 ：子どもたち自身が課題に直接向き合うことが可能な教材

以上の要件を満たす教材として開発したのが、愛知県警察サイバー犯罪対策課と共同で作成・監修を行い公開している『サイバーポリスゲーム』（小学生版）である。

サイバーポリスゲームでは、［問題発生カード］と［クイズカード］が用意されている。このうち、問題発生カードが目指しているのは図 6 のとおりである。

(a)インシデントの疑似体験から学ぶ	実際のインシデントに類似した内容の理解 インシデントが実際に発生するとどのような結果をもたらすのかを理解させる
(b)守るために必要な知識の習得	実際の犯罪手法や情報セキュリティ対策に求められる知識を習得する

図 6　問題発生カードとクイズカードの役割

問題発生カードは、インシデントの擬似体験を中心とした内容である。過去に愛知県警が取り扱った相談事例を子供達にわかりやすく単純な文章に置き換え、その上で、なぜこのインシデントが発生したのかを理解させる仕組みをとっている（図 7）。

１問目では、「このインシデントが具体的に発動したらどのようなトラブルになるのか」を考えさせる。このとき、「自分の意見を発表しよう」と仕向けて、他者の意見を聞く話し合い学習を遂行させる。このことで、いろんな人の考え方に触れて、自分以外の他者の経験や知識、考え方を取り入れるように努めさせる。用意されたワークシートを用いて、そこで記録をとることで、これらの項目をフィードバックできるようにも対応している。

２問目では、行動規範として示している［インターネット５つの約束］のどれを守っていたらこのインシデントは発動しなくて済んだのかを考えさせている。インシデント後の対応方法を含めて、子どもたちにわかりやすく提示することで、理解を促進させる効果を持っている。

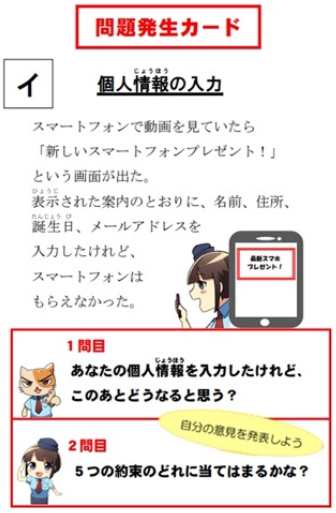


図 7　問題発生カードの内容

これらを活用した結果は次の通りである。明確な効果を期待することができる上に、総務省 ILAS では難しかったリスクに対して直接的な教育を展開することが可能である。

この教育効果をもとに、小学生版を高校生が自分達向けに改変する活動や、教師保護者専用のバージョンさくせいなど、多元的な展開を実施している。これらについても、効果が現れており、有益な教育体制であると言える。

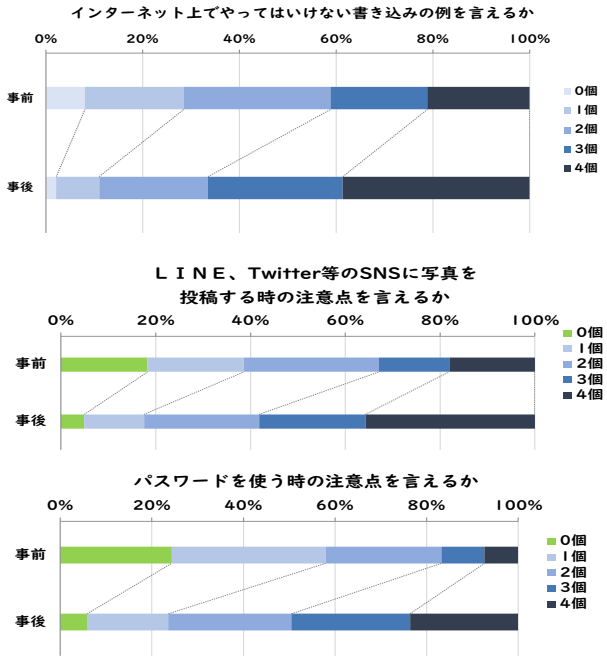


図 8　サイバーポリスゲームの効果

謝辞

サイバーポリスゲームの提供者である愛知県警察サイバー犯罪対策課より、授業利用・多元的な展開に関して多大なる協力を得られたことに対し謝意を表する。

参考文献

[1] 文部科学省，『教育の情報化の手引き追補版（令和 2 年 6 月）』，https://www.mext.go.jp/content/20200608-mxt_jogai01-000003284_003.pdf
[2] 文部科学省，『情報モラル指導モデルカリキュラム』，https://www.mext.go.jp/component/a_menu/education/detail/__icsFiles/afieldfile/2010/09/07/1296869.pdf
[3] 総務省，「ICT 活用のためのリテラシー向上に関する検討会（第 10 回）会議資料」，https://www.soumu.go.jp/main_sosiki/kenkyu/ict_literacy/02ryutsu05_04000222.html
[4] 総務省，ILAS https://www.soumu.go.jp/main_sosiki/joho_tsusin/kyouiku_joho-ka/ilas.html
[5] LINE みらい財団，「GIGA スクール構想における情報モラル教育の実状等に関する調査報告書」，2023 年 11 月，https://s.yimg.jp/dl/miraifoundation/LINEMiraiFoundation_ICT_report_20231127.pdf
[6] 花田経子・砂原秀樹，「教師や保護者から子どもへの継続的な情報セキュリティ教育を可能にする情報セキュリティ教材の開発」，情報処理学会 dicomo2025，2025 年 6 月。
[7] 愛知県警察，『サイバーポリスゲーム（小学生版）』https://www.pref.aichi.jp/police/anzen/cyber/game/cyberpolicegame.html

[8] 愛知県警察，『サイバーポリスゲーム【デジタル版】（小学生版）
https://www.pref.aichi.jp/police/anzen/cyber/game/digitalgame.html

[9] 花田経子，「組織における一般ユーザが潜在的に抱える情報セキュリティリスクに対する教育教材の開発」，情報処理学会電子化知的財産・社会基盤研究会，第 107 回発表予稿，2025 年 2 月。
[10] 花田経子，「ICT 機器の安全利用を促すための小学校高学年向けアナログゲーム教材の開発」，日本デジタル教科書学会，第 8 回年次大会発表予稿，2019 年 8 月。
[11] 花田経子，「すごろくおよびスタンプラリー形式の小学校高学年向け情報モラル教材の開発とデジタル化への対応」，日本デジタル教科書学会，第 10 回年次大会発表予稿，2021 年 8 月。
[12] 野部緑・花田経子，「ボードゲーム制作を利用した情報モラル教育」，情報処理学会コンピュータと教育研究会，第 174 回発表予稿，2024 年 3 月。
[13] 花田経子，「大学生ボランティアによる情報セキュリティ啓発活動の現状と高齢者向け教材の開発過程」，情報処理学会電子化知的財産・社会基盤研究会，第 104 回発表予稿，2024 年 6 月。
[14] 花田経子，「ボードゲーム型教材を活用した多元的な情報セキュリティ教材の開発」，デジタル教科書学会，第 13 回年次大会発表予稿，2024 年 8 月。
[15] 花田経子，「大学生および高校生に対する情報セキュリティリスクの効果的な学習を促すための教材開発」，情報ネットワーク法学会，2024 年研究大会発表予稿，2024 年 12 月。