博士論文

小・中学校における児童・生徒の
情報セキュリティ教育に関する実践研究

2021年

東京学芸大学大学院連合学校教育学研究科

学校教育学専攻 生活・技術系教育講座

(埼玉大学)

小熊 良一

学 位 論 文 要 旨

氏 名　小 熊 良 一

題　目　小・中学校における児童・生徒の情報セキュリティ教育に関する実践研究

本研究の目的は，小・中学校における情報セキュリティ教育に焦点をあて，指導者である教員の実態を踏まえ，小・中学校修了段階の意識と知識を調査し，小・中学校における情報セキュリティ教育の課題と現状を明らかにするとともに，児童・生徒の情報セキュリティの意識と知識を高めるための教材を開発し，効果的な指導の在り方を提案することである。

本論文は，緒言と結言を含め 5 つの章で構成されている。第 1 章では，本研究の目的を踏まえ，研究の背景，初等中等教育における文部科学省が示す情報セキュリティ教育について整理するとともに，先行研究を洗い出し，研究計画を策定した。次の 2 章から 4 章は，①情報セキュリティに関する小・中学校の実態調査（2 章），②児童・生徒の情報セキュリティ教材の開発（3 章），③小・中学校における授業実践（4 章）に大きく分類できる。

①情報セキュリティに関する小・中学校の実態調査（2 章）では，小・中学校に勤務する教員の実態調査をおこなった。また，その調査項目や調査結果の知見を基に小・中学校修了段階の児童・生徒の実態調査をおこなった。小・中学校に勤務する教員の実態として，学校において情報セキュリティを確保することが大切であると認識しているが，実際の行動にむすびついていない傾向があることが示された。小学校修了段階の児童の調査では，「小学生のインターネットの利用は日常的なものとなっており，ゲーム機や個人用のスマートフォンを利用していること」，「すべての児童が情報セキュリティの学習をしていると認識していないこと」，「技術的対策の意識に低い傾向があること」，「物理的対策と人的対策の知識は，ある程度身に付いているが，技術的対策についての知識は不足していること」が示された。また，中学校修了段階の調査では，「携帯型情報端末の利用や利用サービスを踏まえた情報セキュリティ教育が必要であること」，「情報セキュリティを含む情報モラルの学習機会は，学校の集会と技術分野の授業が中心であること」，「人的対策の知識はある程度もちあわせているが，技術的対策に課題があること」が示された。小学校において情報セキュリティ教育を充実させるためには，情報セキュリティの指導内容を明確にし，すべての教員が指導できる教材や指導方法を示すことが必要であることを見出した。また，中学校において情報セキュリティ教育を充実させるためには，技術・家庭科（技術分野）の授業で，情報セキュリティを効果的に指導する教材や指導方法を示すことが必要であることを見出した。

②児童・生徒の情報セキュリティ教材の開発（3 章）では，文部科学省が示す情報セキ

ュリティ教育の目標と前述の実態調査を踏まえて，小学校高学年および中学校技術・家庭科(技術分野)で活用できる情報セキュリティ教材の開発をおこなった。小学校高学年用の指導内容は，「情報セキュリティの原則」，「身近にある情報」，「インターネットにおける情報」，「情報端末・外部媒体の管理」，「個人情報管理」，「ID・パスワード管理」，「ダウンロード」，「フィルタリング」，「ウィルス対策ソフトウェア」，「ソフトウェア更新」の 10 個の指導内容を摘出し，児童の実態をふまえて 4 つの開発要件に従い教材を作成した。中学校用の指導内容は，「リンクの対応」，「ファイアウォール」，「アカウント管理」，「ソフトウェア更新」，「ウィルス対策ソフトウェア」，「バックアップ」，「フィルタリング」，「暗号化」，「ID・パスワード」，「生体認証」，「多要素認証」，「パスワード作成・管理技術」「サイバー空間における情報セキュリティの被害とその対応」，「生活の中で想定されるトラブルへの対応」，「コンピュータウィルスの感染，ハッキング等による被害事例とその対応」の 15 個を摘出し，生徒の実態をふまえた 6 つの開発要件に従い教材を作成した。

③小・中学校における授業実践（4 章）では，開発した教材を用いて授業実践をおこない教材と指導の効果を検証した。小学校高学年における授業実践では，開発した小学生高学年用教材で学習することで，「情報セキュリティの認識の有無に関わらず意識の向上に効果があること」，「人的対策の知識の向上に効果があること」，「1 単位時間（45 分）の授業で，小学校高学年に必要な情報セキュリティの技術的対策の理解につながること」が確認された。中学校における授業実践では，開発した中学生用教材で学習をすることで，「情報セキュリティ対策の必要性の意識が，知識に裏付けられた意識に変容していくこと」，「中学校修了時の課題である『情報セキュリティを確保する仕組み』や『コンピュータウィルスに対する技術』の知識の習得に有効であること」，「1 単位時間（50 分）で，技術・家庭科(技術分野)で学ぶべき情報セキュリティの知識を高めること」が確認された。

以上の結果から第 5 章では，本研究で得られた主要な知見を整理し，小・中学校における情報セキュリティ教育について提案すると共に今後の課題を展望した。

目　次

第1章 緒言

１．研究の目的

本研究の目的は，小・中学校における情報セキュリティ教育に焦点をあて，指導者である教員の実態を踏まえ，小・中学校修了段階の意識と知識を調査し，小・中学校における情報セキュリティ教育の課題と現状を明らかにするとともに，児童・生徒の情報セキュリティの意識と知識を高めるための教材を開発し，効果的な指導の在り方を提案することである。

この研究の目的を達成するために第1章では，①情報セキュリティの現状の把握，②情報セキュリティの概念，③初等中等教育における情報セキュリティ，④小・中学校を対象とした情報セキュリティの研究を整理・分類し，課題の所在を明らかにしていく。

2. 研究の背景

2.1 「情報セキュリティ」の現状とこれまでの歴史

情報セキュリティを確保することは，インターネットの発展に伴いますます重要となっている。日本では，1984年のJUNET[1)]や，1988年WIDEプロジェクト[2)]などがスタートし，大学や企業の研究者など限られた人によるインターネットの利用が始まった。1991年にWorld Wide Webの技術[3)]，1993年にWebブラウザが開発されるなど技術の発展に伴い，1990年代に入りインターネットが一般にも利用されるようになった。そして，インターネットの普及に伴い，コンピュータウィルスへの対応が必要となった。1990年の通産省によるウィルスに対する予防，発見，駆除，復旧等の対策のために策定されたガイドラインである「コンピュータウィルス対策基準」[4)]の策定，1991年のIPA内にコンピュータウィルス対策室の設置を皮切りに，国による情報セキュリティ対策が始まった。

通産省は，インターネットの普及が本格化してくると1995年に「コンピュータウィルス対策基準」を改定，1996年には，情報システムへの不正なアクセスを予防，発見，防止，復旧，再発予防などをすることを目的に策定されたガイドラインである「コンピュータ不正アクセス対策基準」[5)]を策定している。1997年に情報セキュリティに対する組織として，セキュリティセンター(IPA/ISEC)を設立し，ウィルス対策室，不正アクセス対策室，暗号技術調査室及び企画室を設置した。

また，法的整備も進み，1999年には 「不正アクセス行為の禁止等に関する法律(不正アクセス禁止法)」[6)]が成立した。2000年には，省庁ホームページの改ざん事件などが起き，サイバー空間における情報セキュリティを確保する必要性が高まってきた。日本政府は，内閣安全保障・危機管理室に情報セキュリティ対策室の専門家チームを設置した。さらに日本政府としてはじめて，サイバーテロ対策のための行動計画である「重要インフラのサイバーテロ対策に係る特別行動計画」[7)]を策定した。

さらに，2001年には，コンピュータシステム全般への不正アクセスを禁止し，国を跨いだ組織犯罪の捜査のために，国内法に基づく刑事手続きを整備する国際条約である「サイバー犯罪条約」[8]が，採択された。

情報セキュリティ対策は，政府の対策だけにとどまらず，2003年には，経済産業省により，民間企業や政府，地方自治体等の情報セキュリティ対策を目的とした監査制度「情報セキュリティ監査制度」[9]を開始した。個人情報の保護に関する法律である「個人情報保護法」[10]が成立し，2005年に全面施行された。

現在も，情報セキュリティ対策の重要度は，ますます高まっている。最近では，2014年に「サイバーセキュリティ基本法」[11]の成立，2015年の内閣サイバーセキュリティセンター（NISC)の設置など新たな脅威への対応がおこなわれている。

これらの背景から，インターネットを介した脅威は，ますます増加傾向[12]にあり，情報セキュリティへの意識や情報セキュリティ対策の知識は，我々の生活に必要不可欠なものであると考えられる。

2.2 情報セキュリティの概念

情報セキュリティの3要素であるCIA(機密性，完全性，可用性)は，国際標準化機構(以下ISO)[13]や国際電気標準会議(以下IEC)[14]といった団体が情報セキュリティの国際標準として定めている。代表的な国際標準には「ISO/IEC 27001」などがあり，情報セキュリティに関する基準は国際的に統一されている。基準を定めているのはISOとIECである。情報セキュリティの対応が進んでいるアメリカでは，2002年に制定された「連邦情報セキュリティマネジメント法(Federal Information Security Management Act of 2002)」[15]により情報セキュリティの定義が，ISO/IEC 27001のものに定められている。

日本で広く使われている情報セキュリティの概念には，JISQ27001[16]及びJISQ27002[17]がある。この概念は，英国規格として登場したBS7799を基盤として国際規格化したもので，具体的な情報セキュリティの実施基準を示すBS7799-1と情報セキュリティのためのマネジメントシステムの仕様を定めたBS7799-2からなっている。それぞれが，ISO/IEC27001(情報セキュリティマネジメントシステムー要求事項)とISO/IEC27002(情報セキュリティマネジメントの実践のための規範)となった。ISO/IEC27001，ISO/IEC27002は，それぞれ日本語化され，日本工業規格JISQ27001，JISQ27002として発行された。

これらのことから考えると日本で採用されているJISQ27001およびJISQ27002の概念は，日本だけでなく国際的に通用する情報セキュリティの概念であると考えられる。以下にJISQ27001，JISQ27002の用語の定義を示す。

(1) JISQ27001（ISO/IEC 27001）の定義

JISQ27001は，情報セキュリティマネジメントシステム(以下ISMS)に関する国際規格である。情報の機密性・完全性・可用性の3つをバランスよくマネジメントし，情報を有効

活用するための組織の枠組みを示している。JISQ27001では，情報セキュリティの用語として，機密性，完全性，可用性，真正性，責任追跡性，否認防止，信頼性，リスク，脆弱性，脅威，情報セキュリティインシデント，情報セキュリティ事象，リスク対応の14個の用語を定義している。表1.1に JISQ27001の用語の定義を示す。

表1.1　JISQ27001（ISO/IEC 27001）における情報セキュリティの定義

用語	定義
情報セキュリティ	情報の機密性，完全性及び可用性を維持すること。さらに，真正性，責任追跡性，否認防止及び信頼性のような特性を維持することを含めてもよい
機密性	許可されていない個人，エンティティ又はプロセスに対して，情報を使用不可又は非公開にする特性
完全性	資産の正確さ及び完全さを保護する特性
可用性	許可されたエンティティが要求したときに，アクセス及び使用が可能である特性
真正性	ある主体又は資源が，主張どおりであることを確実にする特性。真正性は，利用者，プロセス，システム，情報などのエンティティに対して適用する
責任追跡性	あるエンティティの動作が，その動作から動作主のエンティティまで一意に追跡できる事を確実にする特性
否認防止	ある活動又は事象が起きたことを，後になって否認されないように証明する能力
信頼性	意図した動作及び結果に一致する特性
リスク	事象の発生確率と事象の結果との組合せ
脆弱性	1 つ以上の脅威がつけこむことができる，資産又は資産グループがもつ弱点
脅威	システム又は組織に損害を与える可能性があるインシデントの潜在的な原因
情報セキュリティインシデント	望まない単独もしくは一連の情報セキュリティ事象，又は予期しない単独もしくは一連の情報セキュリティ事象であって，事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの
情報セキュリティ事象	システム，サービス又はネットワークにおける特定の状態の発生。特定の状態とは，情報セキュリティ基本方針への違反もしくは管理策の不具合の可能性，又はセキュリティに関連するかもしれない未知の状況を示していることをいう
リスク対応	リスクを変更させるための方策を，選択及び実施するプロセス

※「JISQ27001」から筆者作成

(2) JISQ27002(ISO/IEC 27002)の定義

表1.2に JISQ27002の用語の定義を示す。JIS Q 27002は，情報セキュリティ管理策を実施するための規範のことである。管理策を組織の中でどのように実施するのか具体的な方法が示されている。

表1.2　JISQ27002（ISO/IEC 27002）における情報セキュリティの定義

用語	定義
情報セキュリティ	情報の機密性，完全性，可用性を維持すること
機密性	情報へのアクセスを認められた者だけが，その情報にアクセスできる状態を確保すること
完全性	情報が破壊，改ざん又は消去されていない状態を確保すること
可用性	情報へのアクセスを認められた者が，必要時に中断することなく，情報及び関連資産にアクセスできる状態を確保すること

※「JISQ27002」から筆者作成

JISQ27002では，情報セキュリティと情報セキュリティの用語として，機密性，完全性，可用性の3つの用語を定義している。総務省では，この定義を情報セキュリティの定義としている。

3. 初等中等教育における情報セキュリティ教育

3.1 学校における情報セキュリティおよび情報セキュリティ教育の現状とこれまでの歴史

2016年2月に佐賀県の学校教育ネットワークへの不正アクセスにより，生徒や保護者等の個人情報が窃取された事件が起きた。文部科学省は，各学校の情報セキュリティ確保のため，2016年7月に「教育情報セキュリティのための緊急提言」[18]を発表した。また，2016年9月に教育情報セキュリティ対策推進チームをつくり，学校における情報セキュリティ対策の考え方を整理することを目的として，2018年11月に「教育情報セキュリティポリシーに関するガイドライン」[19]を発表している。2017年3月に学校における情報セキュリティおよびICT環境整備等に関する研修教材として，「小中高等学校等教職員・教育委員会指導主事向け教材」[20]，「教育委員会システム担当者・構築保守事業者向け教材」[21]を発表している。このように学校における情報セキュリティは，ますます重要になっており，学校の組織つくりや教員用の教材の作成などがすすめられている。

児童・生徒への情報セキュリティ教育は，2006年に「情報モラル指導実践キックオフガイド」[22]において情報モラル指導モデルカリキュラムを作成し，初等中等教育の体系的な情報モラル教育の１つとして情報セキュリティを位置付け，各発達段階の目標を示した。「中学校学習指導要領(平成20年告示)」[23]，「高等学校学習指導要領(平成21年告示)」[24]には，情報の活用，情報モラルなどの情報教育の充実を図ることとし，中学校では，技術・家庭科(技術分野)，高等学校においては，情報において情報セキュリティの指導内容を加えた。2011年には，具体的な指導事例を入れた「情報モラル教育実践ガイダンス」[25]を発表している。また，2013年には，生徒用教材として，「情報化社会の新たな問題を考えるための児童生徒向けの教材」[26]，「教員向けの手引書」[27]を発表し，2015年，2018年と3度の改定をしている。「中学校学習指導要領(平成29年告示)」[28]，「高等学校学習指導要領(平成30年告示)」[29]では，中学校技術・家庭科(技術分野)，高

等学校情報の中に，サイバーセキュリティなど新たな内容が加えられている。さらに，2020年には，「学校教育の情報化の推進に関する法律」[30]が施行され，学校における児童・生徒等の個人情報の適正な取扱い及びサイバーセキュリティの確保が明記された。

このように，学校における情報セキュリティや児童・生徒への情報セキュリティ教育は，時代とともに変化しており，ますます重要となっている。

3.2 初等中等教育における情報教育と情報セキュリティ教育の関係

文部科学省は，情報教育を「児童・生徒の情報活用能力の育成を図るもの」としている。情報教育の目標は，「情報活用の実践力」，「情報の科学的な理解」，「情報社会に参画する態度」の 3 つの観点に整理されている。「情報活用の実践力」とは，課題や目的に応じて情報手段を適切に活用することを含めて，必要な情報を主体的に収集・判断・表現・処理・創造し，受け手の状況などをふまえて発信・伝達できる能力のことである。「情報の科学的な理解」とは，情報活用の基礎となる情報手段の特性の理解と情報を適切に扱ったり，自らの情報活用を評価・改善したりするための基礎的な理論や方法の理解のことである。「情報社会に参画する態度」とは，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を理解し，情報モラルの必要性や情報に対する責任について考え，望ましい情報社会の創造に参画しようとする態度のことである。情報教育の 3 つの観点に沿って，情報セキュリティを整理した内容を表 1.3 に示す。

これらを整理すると，情報セキュリティ教育は，「情報活用の実践力」，「情報の科学的な理解」，「情報社会に参画する態度」の 3 つをバランスよく学習して成りたつことになる。

表1.3　情報教育と情報セキュリティ教育

観点	内容
情報活用の実践力	情報セキュリティを確保しながら，必要な情報を主体的に収集・判断・表現・処理・創造し，発信・伝達できる能力
情報の科学的な理解	情報セキュリティを確保する方法や仕組みの理解
情報社会に参画する態度	情報セキュリティを確保する必要性について考え，望ましい情報社会の創造に参画しようとする態度

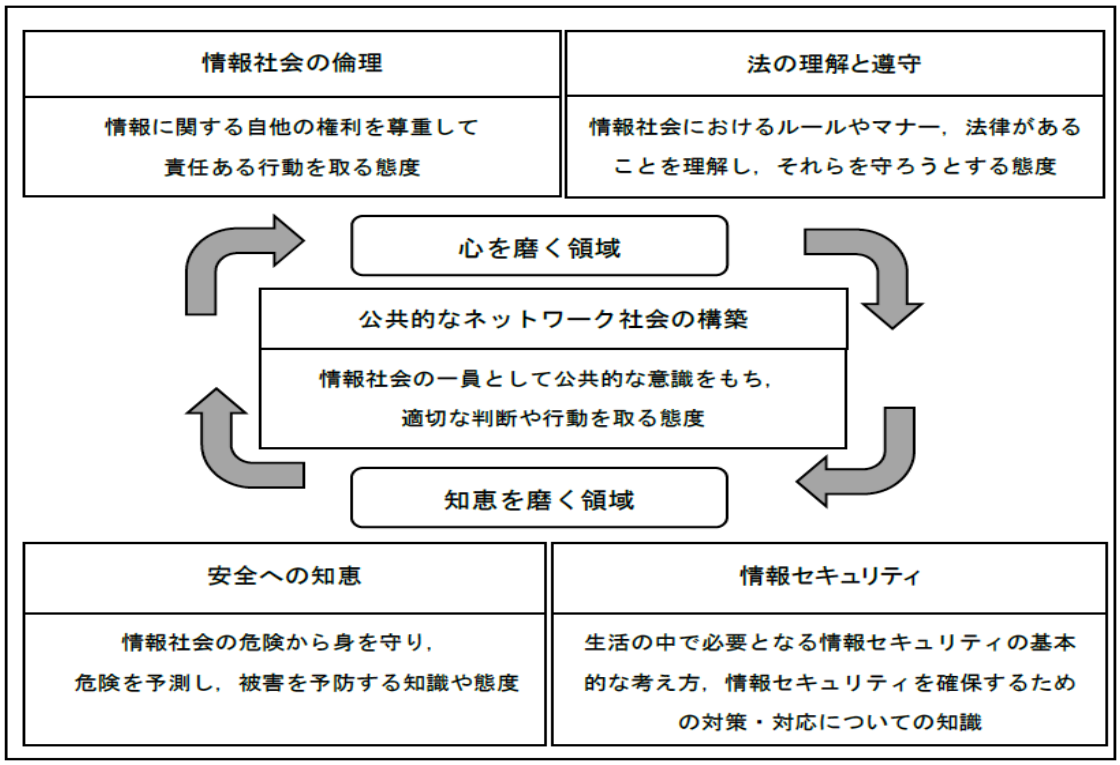
※文部科学省：「教育の情報化の手引き」から筆者作成

3.3 初等中等教育における情報モラル教育と情報セキュリティ教育の関係

文部科学省は，情報モラルを「情報社会で適正な活動をおこなうための基になる考え方と態度」と定義している。また，「心を磨く領域」，「知恵を磨く領域」の2つの領域，「情報の倫理」，「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の構築」の5つの分野を教育することとしている。「情報

セキュリティ」は，5つの分野の1つとして位置付けられており，“生活の中で必要となる情報セキュリティの基本的な考え方，情報セキュリティを確保するための対策・対応についての知識”を学ぶこととしている。

これらを整理すると初等中等教育では，「情報セキュリティの基本的な考え方」と「情報セキュリティを確保するための対応策」を学び，この知識を活用して適切な行動や判断ができることが求められるようになる。文部科学省が示す情報モラル教育の内容を図1.1に示す。



※文部科学省：「情報モラル教育実践ガイダンス」から引用

図1.1　情報モラル教育の内容

3.4　学習指導要領が示す情報セキュリティ教育

(1) 学習指導要領が示す情報セキュリティ教育

文部科学省より示された「幼稚園教育要領，小・中学校学習指導要領等の改訂のポイント」[31]には，「その他の重要事項」の1つとして「情報活用能力(プログラミング教育を含む)」が示されている。具体的には，「コンピュータ等を活用した学習活動の充実(各教科等)」，「コンピュータでの文字入力等の習得，プログラミング的思考の育成(小：総則，各教科等(算数，理科，総合的な学習の時間など)」の2つが示されている。情報セキュリティは，「コンピュータ等を活用した学習活動の充実」にかかわるもので

あり，小・中学校では，各教科において実践することになる。また，「高等学校学習指導要領等の改訂のポイント」[32]には，「その他の重要事項」の1つとして「情報活用能力(プログラミング教育を含む)」が示されている。具体的には，「情報科の科目を再編し，全ての生徒が履修する「情報Ⅰ」を新設することにより，プログラミング，ネットワーク(情報セキュリティを含む。)やデータベース(データ活用)の基礎等の内容を必修化(情報)」，「データサイエンス等に関する内容を大幅に充実(情報)」，「コンピュータ等を活用した学習活動の充実(各教科等)」の3つが示されており，新設された「情報Ⅰ」の学習内容として，すべての生徒が情報セキュリティについて学ぶこととなる。

このように，2020年より小学校から順次スタートしている現在の学習指導要領では，小学校，中学校，高等学校の各段階ですべての児童・生徒が，発達段階にあった情報セキュリティを学ぶことになった。

(2) 小学校学習指導要領が示す情報セキュリティ教育

「小学校学習指導要領(平成29年告示)」[33]には，「情報セキュリティ」という単語の記述は見られない。各教科等の解説編を見ると「小学校学習指導要領(平成29年告示)解説 社会編」[34]において小学校5年「情報化と産業の関わり」で，大量の情報や情報通信技術の活用について扱っている。また，「小学校学習指導要領(平成29年告示)解説 特別の教科道徳編」[35]において，情報モラルを扱っている。しかし，情報セキュリティの内容は，2つの教科とも学習の対象となっていない。

表1.4に「小学校学習指導要領(平成29年告示)解説 総則編」[36]の「第2節教育課程の編成」および「第3節教育課程の実施と学習評価」の記述内容を示す。

表1.4　「小学校学習指導要領(平成29年告示)解説 総則編」の記述内容

第 2 節　教育課程の編成 (1) 学習の基盤となる資質・能力(第 1 章第 2 の 2 の (1)) イ　情報活用能力 情報活用能力をより具体的に捉えれば，学習活動において必要に応じてコンピュータ等の情報手段を適切に用いて情報を得たり，情報を整理・比較したり，得られた情報を分かりやすく発信・伝達したり，必要に応じて保存・ 共有したりといったことができる力であり，さらに，このような学習活動を 遂行する上で必要となる情報手段の基本的な操作の習得や，プログラミング的思考，情報モラル，情報セキュリティ，統計等に関する資質・能力等も含むものである。こうした情報活用能力は，各教科等の学びを支える基盤であり，これを確実に育んでいくためには，各教科等の特質に応じて適切な学習場面で育成を図ることが重要であるとともに，そうして育まれた情報活用能力を発揮させることにより，各教科等における主体的・対話的で深い学びへとつながっていくことが一層期待されるものである。
第 3 節　教育課程の実施と学習評価 1　主体的・対話的で深い学びの実現に向けた授業改善 (3) コンピュータ等や教材・教具の活用，コンピュータの基本的な操作やプログラミングの体験 (第 1 章第 3 の 1 の (3)) さらに，児童が安心して情報手段を活用できるよう，情報機器にフィルタリング機能の措置を講じたり，個人情報の漏えい等の情報セキュリティ事故が生じることのないよう，学校において取り得る対策を十全に講じたりすることなどが必要である。

※文部科学省：「小学校学習指導要領(平成29年告示)解説 総則編」から引用

「小学校学習指導要領（平成29年告示)解説 総則編」には，情報セキュリティは各教科の学びを支える情報活用能力の1つであり，学校は情報機器に個人情報の漏えい等の事故がないように情報セキュリティ対策をしてコンピュータ等を扱うように注意喚起がおこなわれている。

(3) 中学校学習指導要領が示す情報セキュリティ教育

「中学校学習指導要領(平成29年告示)」には，「第8節 技術・家庭」，「D 情報の技術」の指導内容として情報セキュリティの内容が記述されている。また，「中学校学習指導要領(平成29年告示) 解説 技術・家庭科編」[37]の具体的な改善事項の中に“急速な発達を遂げている情報の技術に関しては，小学校におけるプログラミング教育の成果を生かし，発展させるという視点から，従前からの計測・制御に加えて，双方向性のあるコンテンツに関するプログラミングや，ネットワークやデータを活用して処理するプログラミングも題材として扱うことが考えられる。その際，情報セキュリティ等についても充実する。”と記述されている。情報セキュリティについては，双方向性のあるコンテンツに関するプログラミングの中で扱うとともにサイバーセキュリティについても扱い指導内容が充実することとなった。

「中学校学習指導要領(平成29年告示)解説 特別の教科道徳編」[38]には，“情報機器の使い方やインターネットの操作，危機回避の方法やその際の行動の具体的な練習をおこなうことにその主眼をおくのではないことに留意する必要がある。”と記述されている。つまり，情報セキュリティを指導内容として扱うことは示されていない。

また，「中学校学習指導要領(平成29年告示)解説 総則編」[39]には，小学校と同様に情報活用能力と学校における情報セキュリティ対策の重要性が示されている。

これらを整理すると中学校における情報セキュリティ教育は，「技術・家庭科(技術分野)」が，教科の指導内容として，小学校での学習を発展させて，指導することになる。

(4) 高等学校の学習指導要領が示す情報セキュリティ教育

2020年度の高等学校への進学率は95.8%である[40]。この進学率から，日本における高等学校の教育は，国民の教育レベルを高めるうえで義務教育と同等の意義があると考えられる[41]。文部科学省が示す情報セキュリティ教育の内容は，高等学校における教育が指導の最終的なものであるため，高等学校の指導内容を把握する必要がある。

高等学校では，2022年度から実施される教科「情報」の内容が再編成されている。「情報」は，「社会と情報」，「情報の科学」が必履修科目で4単位とされていた[42]。「高等学校学習指導要領(平成30年告示)」[43] においては，「情報Ⅰ」，「情報Ⅱ」と再編され，すべての生徒が履修する必履修科目は「情報Ⅰ」の2単位と少なくなった。「情報Ⅰ」では，プログラミング，ネットワーク，情報セキュリティの基礎について学ぶ。

「情報Ⅱ」は，選択必須科目となる。なお，「情報Ⅱ」および，主として専門学科に

おいて開設される「工業」，「商業」，「水産」，「情報」の4つの教科は，「情報Ⅰ」の履修後，各専門学科の特性に基づいて実施される。

このように高等学校では，小学校および中学校における情報教育を発展させて，すべての生徒が「情報Ⅰ」を履修する。また，各学校の判断により選択必須科目として「情報Ⅱ」を履修する。専門学科においては，専門に合わせた情報セキュリティ教育をおこなうことになる。以下に高等学校における具体的な指導内容を示す。

① 情報「情報Ⅰ」

すべての生徒が履修する「情報Ⅰ」の内容は，これからの国民の素養であると考えられる。小学校および中学校における情報セキュリティの内容の出口と考えるうえで，最も関連の深い内容である。

「情報Ⅰ」では，「(1) 情報社会の問題解決」および「(3) 情報通信ネットワークとデータの活用」の2つの項目で情報セキュリティについて学習する。各項目における指導事項を表1.5に示す。

表1.5　情報「情報Ⅰ」における指導事項

項目	指導事項
(1)情報社会の問題解決	○情報に関する法規や制度 ○情報セキュリティの重要性 ○情報社会における個人の責任 ○情報モラル
(3)情報通信ネットワークとデータの活用	○情報通信ネットワークの仕組みや構成要素 ○プロトコルの役割 ○情報セキュリティを確保するための方法や技術

※文部科学省：「高等学校学習指導要領(平成30年告示)解説 情報編」から筆者作成

② 情報「情報Ⅱ」

「情報Ⅱ」では，「情報Ⅰ」での学習を踏まえて，「(1) 情報社会の進展と情報技術」および「(4) 情報システムとプログラミング」の2つの項目で情報セキュリティについて学習する。各項目における指導事項を表1.6に示す。

表1.6　情報「情報Ⅱ」における指導事項

項目	指導事項
(1)情報社会の進展と情報技術	○情報技術の発展 ・情報セキュリティ及び情報に関する法規・制度の変化 ○情報社会の進展 ○将来の情報技術と情報社会の在り方
(4)情報システムとプログラミング	・情報システムにおける情報の流れや処理の仕組み ・情報セキュリティを確保する方法や技術

※文部科学省：「高等学校学習指導要領(平成30年告示)解説 情報編」から筆者作成

③ 専門学科

専門学科において開設される各教科では，「工業」[44]，「商業」[45]，「水産」[46]，「情報」において，情報セキュリティについて学習する。各教科における指導内容を表1.7に示す。

表1.7　専門学科の教科における指導

教科	項目	指導事項
工業	(2) セキュリティ技術	ア．情報セキュリティ技術
		イ．情報セキュリティ管理
		ウ．情報セキュリティに関する法規
商業	〈情報処理〉	
	(2) コンピュータシステムと情報ネットワーク	ア．コンピュータシステムの概要
		イ．情報通信ネットワークの仕組みと構成
		ウ．情報通信ネットワークの活用
		エ．情報セキュリティの確保と法規
	ネットワーク活用	ア．インターネットの仕組み
	(2) インターネットと情報セキュリティ	イ．ハードウェアとソフトウェアの導入
		ウ．情報セキュリティの確保
	ネットワーク管理	ア．情報セキュリティ管理の目的と重要性
	(2) 情報セキュリティ管理	イ．人的対策
		ウ．技術的対策
		エ．物理的対策
水産	水産や海洋における情報技術	イ．情報セキュリティと情報モラル
	有線通信機器	エ．情報セキュリティの技術
情報	＜情報セキュリティ＞	
	(1) 情報社会と情報セキュリティ	ア．情報セキュリティの現状
		イ．情報セキュリティの必要性
	(2) 情報セキュリティと法規	ア．情報セキュリティ関連法規
		イ．情報セキュリティ関連ガイドライン
	(3) 情報セキュリティ対策	ア．人的セキュリティ対策
		イ．技術的セキュリティ対策
		ウ．物理的セキュリティ対策
	(4) 情報セキュリティマネジメント	ア．情報セキュリティポリシー
		イ．リスク管理

※文部科学省：「高等学校学習指導要領(平成30年告示)」から筆者作成

3.5 初等中等教育における体系的な情報セキュリティ教育

国立教育政策研究所は，情報モラル教育の指導内容を示す資料として2007年に「情報モラル指導実践キックオフガイド」[47]の中で「情報モラル指導モデルカリキュラム表」を発表している。

「情報モラル指導モデルカリキュラム表」には，情報モラルの5つの分野である「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の構築」について，大目標，中目標，小目標を小学校1～2年，小学校3～4年，小学校5～6年，中学校，高等学校の5つの発達段階に分けて体系的に示している。

小学校における情報セキュリティ教育は，中学年と高学年を通した知識・概念の大目標“生活の中で必要となる情報セキュリティの基本を知る”と記述しており，中学年と高学年に発達段階に合わせた中目標を示している。技能・方法論については，高学年の大目標として，“情報セキュリティの確保のための対応・対策がとれる”とし，中目標を“情報の破壊や流出を防ぐ方法を知る”と示している。大目標，中目標を具体化する内容として，各中目標に対して2〜3個の小目標が示されている。

また，文部科学省は，2019年に「教育の情報化の手引き-追補版-」[48]を発表し，「情報活用能力の体系表例」を示している。「情報活用能力の体系表例」は，「A 知識および技能」，「B 思考力，判断力，表現力等」，「C 学びに向かう力，表現力等」の資質・能力の3つの柱で，小学校低学年，小学校中学年，小学校高学年，中学校，高等学校の5つの発達段階に分けて体系的に示されている。小学校における情報セキュリティについては，「A 知識および技能」，「C 学びに向かう力，表現力等」で示されている。「A 知識および技能」では，「自分の情報や他人の情報の大切さ(中学年)」，「生活の中で必要となる基本的な情報セキュリティ(中学年)」「情報を守るための方法(高学年)」「情報技術の悪用に関する危険性(高学年)」の4つが示されている。「C 学びに向かう力，表現力等」では，「生活の中で必要となる情報セキュリティについてふまえ，行動しようとする」と示されている。

これらを整理すると，文部科学省が示す初等中等教育における体系的な情報セキュリティ教育は以下のようになる。

小学校では，低学年で「情報の大切さ」，中学年で「情報を守ることの大切さ」を学び，高学年で，「情報セキュリティの基本」と「生活の中で必要な基本的な情報セキュリティ対策」を学ぶことが示されている。また，中学校「技術・家庭科（技術分野）」および高等学校「情報Ⅰ」では，サイバーセキュリティを含んだ情報セキュリティ対策の仕組や具体的な対策・対応を学ぶことが示されている。

初等中等教育における体系的な情報セキュリティ教育を表1.8に示す。

表1.8　初等中等教育における体系的な情報セキュリティ教育

情報モラル指導モデルカリキュラム表 ◎大目標　○中目標　・小目標	情報活用能力の体系表例
＜小学校低学年＞ 記述なし	A 知識及び技能 ・人の作った物を大切にすることや他者に伝えてはいけない情報があること ・コンピュータなどを利用するときの基本的なルール
＜小学校中学年＞ ◎生活の中で必要となる情報セキュリティの基本を知る ○認証の重要性を理解し，正しく利用できる ・パスワードは誰にも教えない ・自分の使った端末をそのまま放置しない	A 知識及び技能 ・自分の情報や他人の情報の大切さ ・生活の中で必要となる基本的な情報セキュリティ
＜小学校高学年＞ ◎生活の中で必要となる情報セキュリティの基本を知る ○不正使用や不正アクセスされないように利用できる ・パスワードは自分で管理しなければならないことを理解する ・どのようにして個人情報が漏れていくかを知る ◎情報セキュリティの確保のために，対策・対応がとれる ○情報の破壊や流出を防ぐ方法を知る ・ウィルスに対する簡単な知識を知る ・自分の端末は人に貸さない ・ダウンロードには危険が伴うものがあることを知る	A 知識及び技能 ・情報に関する自分や他者の権利 ・情報を守るための方法 ・情報技術の悪用に関する危険 C 学びに向かう力，表現力等 ・生活の中で必要となる情報セキュリティについて踏まえ，行動しようとする
＜中学校＞ ◎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 ○情報セキュリティの基礎的な知識を身につける ・もれた個人情報がどう悪用されるかを知る ◎情報セキュリティの確保のために，対策・対応がとれる ○基礎的なセキュリティ対策が立てられる ・不正アクセスによる(個人)情報の漏洩を防ぐことができる	A 知識及び技能 ・情報に関する個人の権利とその重要性 ・情報セキュリティの確保のための対策・対応 ・仮想的な空間の保護・治安維持のための，サイバーセキュリティの重要性 C 学びに向かう力，表現力等 ・情報セキュリティの確保のための対策・対応の必要性を踏まえ，行動しようとする
＜高等学校＞ ◎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 ○情報セキュリティに関する基本的な知識を身につけ，適切な行動ができる ・暗号化によって情報を守ることを知り，活用する ◎情報セキュリティの確保のために，対策・対応がとれる ○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 ・ウィルスに対し，事前対策・緊急対応・事後対策が取れる ・パソコンやパソコンの情報を，的確に守る技法を知り，実行できる ・ネットワークを介した攻撃に対し，対策・対応がとれる(ファイアウォールなど)	A 知識及び技能 ・情報に関する個人の権利とその重要性 ・情報セキュリティの確保のための対策・対応の科学的な理解 ・仮想的な空間の保護・治安維持のための，サイバーセキュリティの科学的な理解 C 学びに向かう力，表現力等 ・情報セキュリティを確保する意義を踏まえ，適切に行動しようとする ・仮想的な空間の保護・治安維持のためのサイバーセキュリティの意義を踏まえ，適切に行動しようとする

※文部科学省：「情報モラル指導モデルカリキュラム表」，「情報活用能力の体系表例」から筆者作成

4. 本研究における文言の整理

前述の社会における情報セキュリティの概念および初等中等教育における情報セキュリティの歴史と現状を踏まえて，本研究の中核をなす文言である「情報モラル」，「情報セキュリティ」，「情報モラル教育」，「情報セキュリティ教育」の4つの文言を以下に定義する。

(1) 情報モラル

文部科学省の「教育の情報化の手引き」で示されている「情報社会で適正な活動をおこなうための基になる考え方と態度」が，「情報モラル」の定義として，一般的に使われている。また，石原(2011)[49]によると「情報モラル」を育成する教育を「情報モラル教育」とし，その内容を“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や，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”と示している。

本研究は，小・中学校を対象とした研究であるため，文部科学省の「情報モラル」の定義を「情報社会で適正な活動をおこなうための基になる考え方と態度」とする。

(2) 情報セキュリティ

「情報セキュリティ」の定義として，総務省の「国民のための情報セキュリティサイト」[50]では，JIS Q 27001およびJIS Q 27002の“情報の機密性，完全性および可用性を維持すること”を採用している。この定義が社会で一般的に利用されている。

学校における情報セキュリティの定義は，「教育の情報化に関する手引(令和元年12月)」[51]第7章 学校におけるICT環境整備 第5節 教育情報セキュリティに“「情報セキュリティ」とは，情報の「機密性(情報に関して，アクセスを認可されたものだけがこれにアクセスできる状態を確保すること)」，「完全性(情報が，破壊，改ざん又は消去されていない状態を確保すること)」「可用性(情報へのアクセスを認可されたものが，必要時に中断されることなく，情報および関連資産にアクセスできる状態を確保すること)」を維持することである。”と示されている。なお，「小学校学習指導要領(平成29年告示)」[52]「中学校学習指導要領(平成29年告示)」[53]および各解説には具体的に定義は示されているものはない。

「技術・家庭科（技術分野）」の教科書では，「情報を安全に保つための技術や対策(A社)」[54]，「情報通信ネットワークを安全に保つための操作や対策(B社)」[55]と定義されている。また，情報セキュリティの技術として，「様々な攻撃や誤った操作から情報通信ネットワークを守り，安心に使えるようにする技術(C社)」[56]と示されている。いずれも前述のJISQ27001およびJISQ27002の定義を生徒向けの言葉に要約したものである。

これらのことをふまえて，本研究における「情報セキュリティ」の定義は，“情報の

機密性，完全性および可用性を維持すること”とする。

(3) 情報モラル教育

文部科学省は，「情報モラル」を「情報の倫理」，「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の構築」の 5 つの分野に分け教育し，心と知恵を磨くこととしている。前述のとおり「情報モラル」の定義は，「情報社会で適正な活動をおこなうための基になる考え方と態度」が，学校で浸透している。

このことをふまえて「情報モラル教育」の定義を「情報社会で適正な活動をおこなうための基になる考え方と態度を育成する教育」とする。

(4) 情報セキュリティ教育

文部科学省は，「情報セキュリティ」を「情報モラル」の「知恵を磨く領域」の1つの分野として位置付けており，“生活の中で必要となる情報セキュリティの基本的な考え方，情報セキュリティを確保するための対策・対応についての知識”としている。

このことをふまえて，本研究における「情報セキュリティ教育」の定義は，“生活の中で必要となる情報セキュリティの基本的な考え方，情報セキュリティを確保するための対策・対応についての知識を育成する教育”とする。

「情報モラル教育」と「情報セキュリティ教育」は，同じ用語が使用されている場合があるが，上記の通り，「情報モラル教育」は考え方や態度を育成するもの，「情報セキュリティ教育」は考え方や知識を育成するものであると相違を説明することができる。

5. 情報セキュリティに関する研究の整理

情報セキュリティに関する研究を整理するために国立情報学研究所が運営する学術論文や図書・雑誌などの学術情報データベースCiNiiより検出し，調査した。研究論文は，情報セキュリティに関する論文は1,313件検出された。なお，本論文数には，筆者の執筆した論文も含まれる(2021年7月8日現在)。

5.1　調査の方法

調査の方法は，「情報セキュリティ」というキーワードで検出された1,313件の論文の中から学校にかかわる論文を年代別に摘出した。さらに摘出した論文を研究対象および研究内容を6つに分類整理し，考察をおこなった。

5.2 情報セキュリティに関する研究の推移

情報セキュリティに関する研究論文数を 5 年ごとに整理したものを表 1.9 に示す。

表1.9　情報セキュリティに関する研究論文数

研究年代	情報セキュリティの論文数	学校に関わる情報セキュリティの論文数
～1985	15	0
1986～1990	8	0
1990～1995	15	0
1996～2000	46	0
2001～2005	173	4
2005～2010	340	10
2011～2015	385	30
2016～	331	41

※2021 年 8 月 8 日現在

最も古い情報セキュリティの研究論文は，「ARPANET」が「大学間を結ぶ，学術・一般向けのネットワーク」と定義され「Internet」という言葉が誕生した 1983 年のものである [57]。日本におけるデータベースサービスの現状と課題の中で情報セキュリティの必要性を取り上げている [58]。時代背景として，Windows95 が発売されインターネットが身近になったころから情報セキュリティに関する研究論文が大幅に増加している。

学校に関わる情報セキュリティの研究論文は，「情報セキュリティ」，「学校」の 2 つのキーワードを含む論文を検索した。研究論文数は，85 件であり，情報セキュリティ全体の研究と比較するとわずか 6.4%しか発表されていない。

学校に関わる情報セキュリティの最も古い研究論文は，2004 年に発表された高校生向

けの教育用コンテンツの研究である [59]。2004 年は，情報教育の展開期にあたり，インターネットや暴力シーンのあるメディア映像の自粛，教育界では義務教育段階での情報モラル教育の本格的な導入の検討を迫られることとなった時期である。以後，学校に関わる情報セキュリティに関する研究がおこなわれるようになった。

2017 年の学習指導要領改訂での情報セキュリティ教育の充実を受けて，学校を対象とした情報セキュリティの研究も増加傾向にある。

5.3 学校に関わる情報セキュリティ研究の対象と内容

学校に関わる情報セキュリティに関する研究対象の割合を表1.10に示す。

高等学校を対象とした研究が24件(28.2%)と最も多い。次いで教員20件(23.5%)となっている。義務教育段階の児童・生徒対象の研究については，小学生8件(9.4%)，中学生14件(16.5%)と他の対象と比べて低い傾向にあることが示された。なお，研究には小・中学生両方を対象とした研究も2件見受けられた。

表1.10　情報セキュリティに関する研究対象の割合

研究対象	論文数	割合(%)
小学生	8	9.4
中学生	14	16.5
高校生	24	28.2
教員	20	23.5
その他	19	22.4

※2021年8月8日現在

研究内容は，「教材開発」，「システム開発」，「実態調査」，「指導方法」，「教員研修プログラム」，「その他」の5つのカテゴリに分類した。なお，「その他」は，運用や地域サポートの取り組みなどの研究である。

研究内容は，教材開発が18件(21.1%)で他のカテゴリと比較して最も多い。次いでシステムの開発16件(18.8%)，実態調査，教員研修プログラムが9件(10.5%)，指導方法が8件(9.4%)であった。教材開発，指導方法に関わる研究は，高等学校情報を対象とした研究論文が半数以上を占めており，小学校を対象とした研究は3件，中学校を対象とした研究は4件であった。学校に関わる情報セキュリティに関する研究内容の割合を表1.11に示す。

表1.11　情報セキュリティに関する研究内容の割合

研究内容	論文数	割合(%)
教材開発	18	21.1
システム開発	16	18.8
実態調査	9	10.5
教員研修プログラム	9	10.5
指導方法	8	9.4
その他	15	17.6

※2021年8月8日現在

(1) 情報セキュリティのシステム開発に関する研究

情報セキュリティのシステム開発に関する研究は，学校の情報セキュリティを守るための技術的対策に関する研究である。

佐村ら(2006～2008)[60)~62)]は，情報端末の情報セキュリティ対策として，パスワード等，特殊な設定をするものではなく，行動的生体認証の一種であるキーストローク認証を活用した技術的対策を提案している。田村ら(2015)[63)]は，社会で多く利用されているボットについて，人間特有の画像認識能力を利用することで，利便性を保ち十分な堅牢性をもつ新たなCAPTCHA方式を開発し，そのシステム実装に必要な妨害図形の量に関する閾値を明らかにし，提案手法が攻撃に対して十分な耐性をもち，ユーザビリティが優れていることを示した研究をおこなっている。野間口ら(2015)[64)]は，重要な情報セキュリティ技術の1つである高速かつ大容量な暗号処理が可能な共通鍵ストリーム暗号の開発をおこなっている。動的に変化する非線形処理構造をもつストリーム暗号の試作に関する設計方針とその基本処理について示し，それが鍵長よりも十分大きい複雑度をもち，その出力乱数系列が統計的に優れた特性をもつことを示すことを報告している。

学校は，多くの情報を管理するが，教員が校務分掌のひとつとして担当することが多く，専門的な知識をもつケースは少ない。OECD国際教員指導環境調査(TALIS2013)[65)]で，１週間当たりの勤務時間が参加国最長といわれている日本の教員に，新たな負担をかけるのは現実的ではない。これらの現状を踏まえて，授業や生徒指導などの本務をおこないながら情報セキュリティを確保するために，複雑なパスワードや，特別なシステムの管理や専門的な知識をもたなくても，安全・確実に情報セキュリティを確保できるシステムの研究がおこなわれている。

情報セキュリティを確保するためには，技術的対策に加えて，人的対策が必要である。今後も，新しい技術に対応した安全な情報セキュリティのシステムと優れたユーザビリティを兼ね備えた研究が求められている。

(2) 情報セキュリティ教材開発に関する研究

情報セキュリティ教材開発に関する研究については，小中高生を対象にした研究と教員を対象にした研究がある。

花田(2019)[66]は，小学校高学年向けの情報モラル用のすごろく型ゲームを共同開発し，ゲーミフィケーションの要素を活かして情報セキュリティの学習へのハードルを下げるとともに，子どもたちの話し合いを促す指導法を提案している。岡田ら(2021)[67]は，小学校高学年用の謎解きスタンプラリー型の教材を開発し，謎解き問題で知識を習得，伝達，振り返りという学習課程でスタンプを押し進めていくことで，SNS リテラシーを向上させる実践をおこなっている。

前原ら(2008)[68] は，中学生を対象にして，日々の校内情報ネットワークの利用に関連づけて，IDとパスワードの入力を入口とした情報セキュリティの意識を高める教材を開発している。塩田ら(2018)[69] は，中学生を対象にして当事者意識を促すことを目的としたスマホ画面を模したカード型教材を開発している。開発した教材で学習することにより，当事者意識とセキュリティ対策への意欲の向上が見られたと報告している。

渥美(2009)[70]は，高校生を対象にした「情報処理Ⅰ」の学習において，「電子メール」を題材とした公開鍵基盤や公開鍵暗号方式を利用した情報セキュリティの技術に着目した教材を開発している。

また，小林ら(2008)[71]は，小・中学校の教員を対象にコンピュータのロックの方法やファイルへのパスワードの設定方法などを各場面において指示する教材を開発し，情報セキュリティに関する技能面と行動面を改善させる研究に取り組んでいる。

小・中学生を対象にした教材開発に関する研究は，情報教育や情報モラル教育の一部として情報セキュリティを扱ったものが中心であり，情報セキュリティ教育に特化した研究が必要である。また，小・中学校における教育の情報セキュリティ教育の繋がりを見通した研究が不足している。

2020年に一人一台端末が，全国の学校で，小・中学校に整備された[72]。これらのことから，教材開発に関する研究は，現在の学校での情報端末の環境を踏まえ，小・中学校の情報セキュリティ教育の繋がりを見通した研究が必要であると考える。

(3) 情報セキュリティの実態調査に関する研究

水沼ら(2009)[73]は，中学生を対象に携帯電話について2,000人規模の調査をおこない，掲示板などからの個人情報の流出の危険性を警告し，中学生への情報セキュリティ教育の必要性を提言している。森ら(2010～2012)[74)～76]は，平成18年から継続的に大学に入学した1年生の調査をおこない，高等学校での情報セキュリティ教育が改善されつつあることを示している。また，小熊ら(2017)[77]は，総務省，文部科学省，警察庁などの省庁がおこなっている実態調査の傾向について報告し，小・中学校における情報セキュリティ教育の指導力の不足を指摘している。

これらの先行研究より，実態調査については，携帯型端末の所持率，生活への影響，指導実態などについて様々な形でおこなわれている。また，調査対象については，小学校，中学校，高等学校の幅広い層におこなわれていることが分かった。

しかし，教員の調査は，意識が中心で知識を明確にするための調査が不足している。また，児童・生徒の調査は，小・中学校の修了段階に合わせた情報セキュリティの意識と知識を関連させた調査が不足しているため，小・中学校の学習を修了した段階での情報セキュリティへの意識や知識の実態を把握することが必要であると考える。

(4) 情報セキュリティの教員研修プログラムに関する研究

山本(2016)[78]は，複数校における研究授業や大学と連携した体系的な教員プログラムについて，日々の授業と関連させた教員の経験年数を踏まえた東京都の取組みを報告している。高瀬ら(2018)[79]は，ヒューマンエラー対策の m-SHEL モデルを援用し，「学校の情報セキュリティリスクへの自覚」をテーマとした研修が，教員の情報セキュリティリスクへの自覚が促されることを報告している。

これらの先行研究より，情報セキュリティに関する研修は，各教育委員会で初任者研修，法定研修の機会に実施していることが分かった。しかし，情報セキュリティ対策の変化は著しいため，毎年，最新の内容を取り入れた知識を学ぶことが必要不可欠である。定期的に最新の情報セキュリティが学べる研修プログラムや個別学習を想定した研修用教材の研究が必要であると考えられる。

(5) 指導方法に関する研究

指導方法に関する研究については，片岡(2013)[80]により，情報セキュリティをテーマとし，①情報収集・整理，②レポートやマインドマップによる課題解決法の理解と判断，③学習成果の発表という3段階の課題解決型の指導過程が研究されている。また，堤ら(2016)[81]は，中学校の「技術・家庭科(技術分野)」の授業における6時間の情報セキュリティの学習過程を提案し，5・6時間目の題材のまとめの段階で知識構成型ジグソー法を用いた学習の効果を報告している。

これらの先行研究より，情報セキュリティの授業については，知識伝達型の授業に偏る傾向があるが，課題解決やジグソー学習を取り入れるなどして児童・生徒の活動を中心にした指導方法が研究されていることが分かった。指導方法に関する研究は，教材開発の研究と一緒におこなわれるべきものである。しかし，現在の研究は，教材開発と指導方法の両方を考慮した研究が不足している。今までにおこなわれた研究は，小学校や中学校など各発達段階の指導法で完結しているため義務教育段階を見通した指導方法の開発が必要であると考えられる。

5.4　学校を対象とした情報セキュリティに関する研究の課題

前述のとおり，学校を対象とした情報セキュリティの研究は，学校において教員が，情報セキュリティを守るための知識やシステムの研究が中心であり，児童・生徒の情報セキュリティを確保する能力を高める研究が不足していることが分かる。

また，先行研究では，教員の実態，児童・生徒の小・中学校の修了段階の意識・知識の実態が充分に把握できていないという課題がある。また，教材や指導方法に関しては，各学校段階での指導で完結しているため小・中学校全体を見渡した研究が必要であると考える。

したがって，今後の小・中学校を対象とした情報セキュリティに関する研究としては，「小学校学習指導要領(平成29年告示)」[82]，「中学校学習指導要領(平成29年告示)」[83]で目指す指導内容を踏まえ，指導する教員の実態，現在の義務教育修了段階での実態を調査し，調査に即した教材開発と授業実践をおこない，その効果を研究する必要がある。

6. 研究の方法

本研究では，前述の先行研究の調査から明らかになった「教員の実態，児童・生徒の小・中学校の修了段階の意識・知識の実態の把握」，「小・中学校全体を見渡した教材や指導方法の不足」という課題を解決するために，以下の研究をおこなう。①小・中学校の教員と小・中学校修了段階の児童・生徒の情報セキュリティに関する意識や知識の実態を把握する。②調査結果を基に，児童・生徒向けに必要な情報セキュリティの指導内容を検討し，教材開発をおこなう。③開発した教材を用いた授業実践を行うとともに教育効果について検証をおこなう。④検証した内容から教材と指導方法を提案するとともに今後の課題を明らかにする。

7. 本論文の構成

本論文は以下のように構成されている。

第1章では，情報セキュリティ教育の歴史や現状を把握する。そして，小・中学校を対象とした情報セキュリティの研究を整理・分類し，課題の所在を明らかにする。

第2章では，教員の情報セキュリティの実態調査を踏まえて，小・中学校修了段階の情報セキュリティの調査項目を摘出する。そして，小・中学校修了段階での児童・生徒の情報セキュリティに関する実態を調査し，小・中学校修了段階で不足している情報セキュリティの意識と知識を明らかにする。

第3章では，第2章で得られた知見から，小学校高学年および技術・家庭科(技術分野)で利用できる情報セキュリティ教材を開発する。

第4章では3章で開発した情報セキュリティ教材を用いた小・中学校での授業の方法を提案し，教材および指導の効果について検証をおこなう。

第5章では，これらの課題を総括し，学校現場での示唆および今後の課題について述べる。本論文の構成図を図1.2に示す。

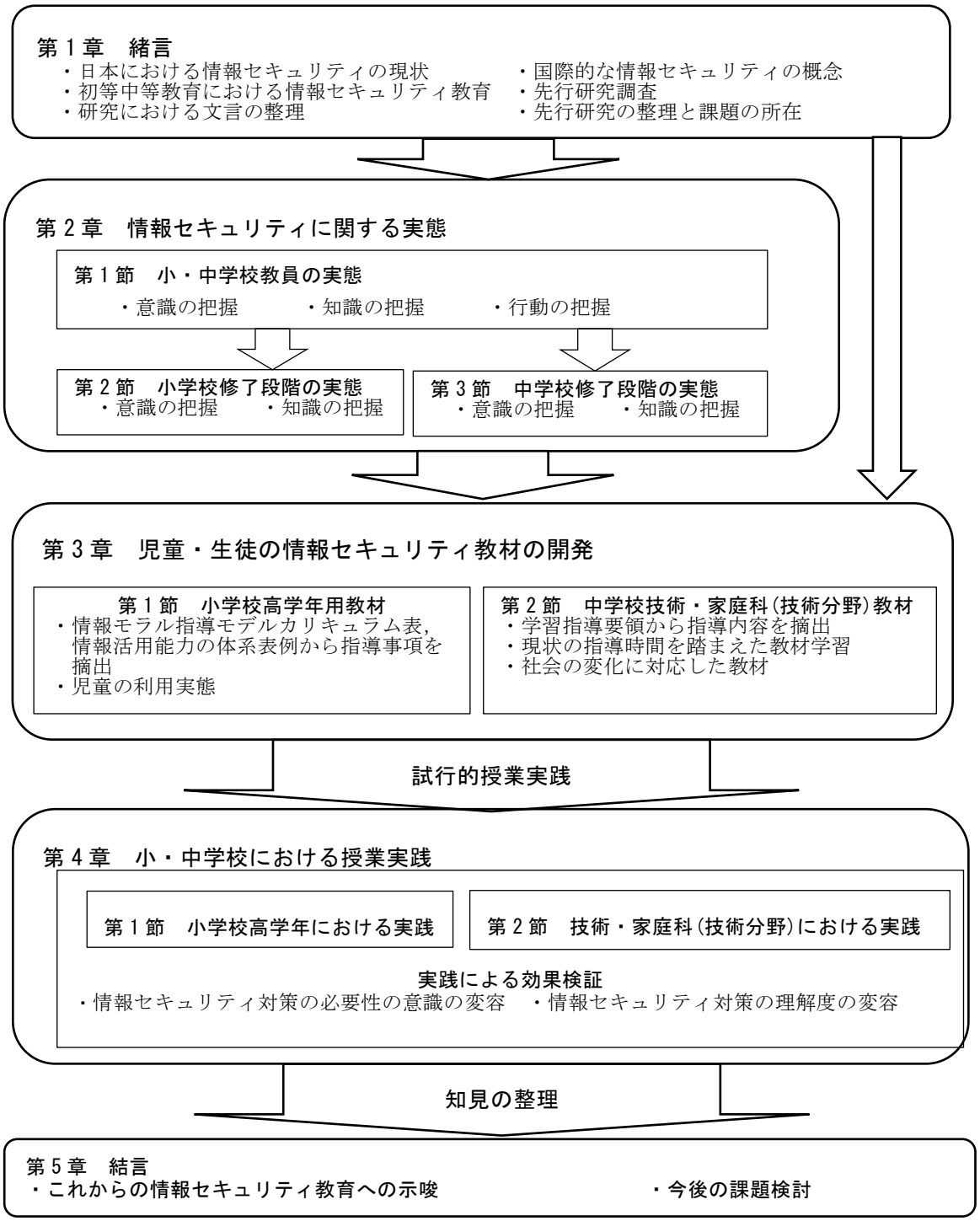


図1.2　論文構成図

8.　結言

第 1 章では，情報セキュリティの現状の把握，初等中等教育における情報セキュリティを調査・整理し，本研究で中核となる文言の整理をおこなった。また，小・中学校を対象とした情報セキュリティの研究を整理・分類した結果，教員の実態と児童・生徒の小・中学校の修了段階の意識・知識の実態が充分に把握できていないという課題が明らかになった。

第2章では，教員の情報セキュリティの実態調査をおこなう。そして，その調査の知見を踏まえて，小・中学生に対しての情報セキュリティの調査項目を摘出し，児童・生徒の情報セキュリティに関する実態を調査し，小・中学校修了段階で不足している情報セキュリティの意識と知識を明らかにする。

参考文献

1) 吉村伸：JUNET協会の設立と解散，https://portal.graphy.co.jp/?p=351，(2021.8.8最終確認)
2)日本ネットワークインフォメーションセンター，https://www.nic.ad.jp/ja/basics/terms/wide- project.html，(2021.8.8最終確認)
3) 村井純，「インターネット」，岩波書店，pp.70-71(1995)
4) 経済産業省：コンピュータウィルス対策基準，https://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm，(2021.8.8最終確認)
5) 経済産業省：コンピュータ不正アクセス対策基準，https://www.meti.go.jp/policy/netsecurity/UAaccessCMG.htm，(2021.8.8最終確認)
6) 総務省：不正アクセス行為の禁止等に関する法律，https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=411AC0000000128，(2021.8.8最終確認)
7) 内閣サイバーセキュリティセンター，重要インフラのサイバーテロ対策に係る特別行動計画，http://www.kantei.go.jp/jp/it/security/taisaku/2000_1215/pdfs/txt3.pdf，(2021.8.8最終確認)
8) 外務省：サイバー犯罪条約，https://www.mofa.go.jp/mofaj/gaiko/treaty/pdfs/treaty159_4a.pdf，(2021.8.8最終確認)
9) 経済産業省：情報セキュリティ監査制度，https://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex04.pdf，(2021.8.8最終確認)
10)個人情報保護委員会：個人情報保護法，https://www.ppc.go.jp/files/pdf/290530_personal_law.pdf，(2021.8.8最終確認)
11)総務省：サイバーセキュリティ基本法，https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=426AC1000000104(2019.9.8最終確認)
12)独立行政機構情報情報処理推進機構サイバーセキュリティセンター：情報セキュリティ10大脅威2021，pp.5-32(2021)
13)国際標準化機構(International Organization for Standardization)，https://www.iso.org/home.html，(2021.8.8最終確認)
14)国際電気標準会議(International Electro technical Commission)，https://www.iec.ch/homepage，(2021.8.8最終確認)
15)U.S. Federal Government: Federal Information Security Management Act of 2002，https://www.ipa.go.jp/files/000015362.pdf，(2021.8.8最終確認)
16)日本工業標準調査会 JISC：JIS Q 27001 情報セキュリティマネジメントシステム-要求事項，https://www.jisc.go.jp/pdfa5/PDFView/ShowPDF/kAEAAKYCL9qqUSg88tCC，(2021.8.8最終確認)
17)日本工業標準調査会 JISC：JISQ27002 情報セキュリティ管理策の実践のための規

範，https://www.jisc.go.jp/pdfa4/PDFView/ShowPDF/SwAAAIYSD50e9NeHcapN，(2021.8.8最終確認)
18)文部科学省：教育情報セキュリティのための緊急提言，https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/__icsFiles/afieldfile/2017/03/08/1377772_2.pdf (2021.8.8最終確認)
19)文部科学省：教育情報セキュリティポリシーに関するガイドライン，http://www.mext.go.jp/a_menu/shotou/zyouhou/detail/__icsFiles/afieldfile/2017/10/18/1397369.pdf，(2021.8.8最終確認)
20)文部科学省：学校における情報セキュリティおよびICT環境整備等に関する研修教材 小中高等学校等教職員・教育委員会指導主事向け教材(2017)
21)文部科学省：学校における情報セキュリティおよびICT環境整備等に関する研修教材 教育委員システム担当者・構築保守事業者向け教材(2017)
22)日本教育工学振興会：情報モラル指導実践キックオフガイド(2007)
23)文部科学省：中学校学習指導要領(平成20年告示)，東山書房，(2008)
24)文部科学省：高等学校学習指導要領(平成21年告示)，東山書房，(2009)
25)国立教育政策研究所：情報モラル教育実践ガイダンス(2013)
26)文部科学省：情報化社会の新たな問題を考えるための児童生徒向けの教材，http://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1416322.htm，(2019.9.10最終確認)
27)文部科学省：情報化社会の新たな問題を考えるための児童生徒向けの教材教員向けの手引書(2018)
28)文部科学省：中学校学習指導要領(平成29年告示)，株式会社東山書房，p.21 (2017)
29)文部科学省：高等学校学習指導要領(平成30年告示)，株式会社東山書房，p.20 (2018)
30)学校教育の情報化の推進に関する法律，https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/__icsFiles/afieldfile/2019/07/01/1418577_002_1.pdf，(2021.8.30最終確認)
31)文部科学省(2017)：幼稚園教育要領，小・中学校学習指導要領等の改訂のポイント，https://www.mext.go.jp/content/1421692_1.pdf，(2021.8.8最終確認)
32)文部科学省(2017)：高等学校学習指導要領等の改訂のポイント，https://www.mext.go.jp/component/a_menu/education/micro_detail/__icsFiles/afieldfile/2019/09/30/1421692_2.pdf，(2019.9.10最終確認)
33)文部科学省：小学校学習指導要領(平成29年告示)，株式会社東洋館出版社(2017)
34)文部科学省：小学校学習指導要領(平成29年告示)解説 社会編，日本文教出版株式会社，pp.171-174(2017)
35)文部科学省：小学校学習指導要領(平成29年告示)解説 特別の教科 道徳編，廣済堂あ

かつき株式会社，pp.97-99（2017）
36)文部科学省：小学校学習指導要領(平成29年告示)解説 総則編，東洋館出版社，pp.51-52，p.187(2017)
37)文部科学省：中学校学習指導要領(平成29年告示)解説 技術・家庭科編，開隆堂出版株式会社，p.11(2017)
38)文部科学省：中学校学習指導要領(平成29年告示)解説 特別の教科道徳編，教育出版株式会社，p.100(2017)
39)文部科学省：中学校学習指導要領(平成29年告示)解説 総則編，株式会社東山書房，p.86（2017）
40)文部科学省:令和３年度学校基本調査調査（速報値）結果のポイント，p.2(2020)
41)文部科学省: 高等学校教育の現状について，https://www.mext.go.jp/a_menu/shotou/kaikaku/20201027-mxt_kouhou02-1.pdf(2021.8.8最終確認)
42)文部科学省：高等学校学習指導要領(平成21年告示)解説 情報編，開隆堂出版株式会社，(2010)
43)文部科学省：高等校学習指導要領(平成30年告示)解説 情報編，開隆堂出版株式会社，(2018)
44)文部科学省：高学校学習指導要領(平成30年告示)解説 工業編，実教出版株式会社，pp.173-175（2018）
45)文部科学省：高学校学習指導要領(平成30年告示)解説 商業編，実教出版株式会社，pp.125-128（2018）
46)文部科学省：高学校学習指導要領(平成30年告示)解説 水産編，海文堂出版株式会社，pp.39-43（2018）
47)前掲22)，pp.6-7(2007)
48)文部科学省：情報活用能力の体系表例，教育の情報化の手引き-追補版-，pp.41-42（2020）
49)石原一彦：情報モラル教育の変遷と情報モラル教材，岐阜聖徳学園大学紀要教育学部編50巻，pp.101-116(2011)
50)総務省：国民のための情報セキュリティサイト，https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/index.html(2021.8.8最終確認)
51)文部科学省：情報活用能力の体系表例，教育の情報化の手引き(令和元年12月)，pp.232-239(2019)
52)前掲33)，(2017)
53)前掲28)，(2017)
54)竹野英敏 他：技術・家庭科　技術分野テクノロジーに希望を載せて，開隆堂，p.228(2020)
55)中村祐治 他：New技術・家庭 技術分野明日を創造する，教育図書，p.212(2020)

56)田口浩継 他：新しい技術・家庭科 技術分野 未来を創るTechnology，東京書籍，p.198(2020)
57)PC・IT・WEBの基礎知識はじめの一歩，https://www.ippo.ne.jp/howto/about/05history/2-1(2021.8.8最終確認)
58)篠崎和紀：「データベース台帳総覧」からみた我が国データベースサービスの現状と課題，月刊JICST1983年26巻6号，pp.437-440(1983)
59)本村猛能：我が国の情報教育の成立・展開期における学習者の意識から見たカリキュラム評価，兵庫教育大学大学院 連合学校教育学研究科学位論文，pp.9-10(2016)
60)佐村敏治・西村治彦：キーストロークダイナミックスにおける日本語文の特徴分析，自動制御連合講演会講演論文集49，p.621(2006)
61)佐村敏治・西村治彦：キーストロークダイナミックスによる日本語文での個人識別，システム制御，情報学会研究発表講演会講演論文集 SCI07，p.314(2007)
62)佐村敏治・西村治彦：キーストロークダイナミックスによる不正アクセス検知へのサポート，システム制御情報学会研究発表講演会講演論文集 SCI08，p.367(2008)
63)田村拓己・久保田真一郎・油田健太郎・片山徹郎・朴美娘・岡崎直宣：文字認識攻撃に耐性を持つランダム妨害図形を用いた画像ベースCAPTCHA方式の提案， 情報処理学会論文誌 56(3)，pp.808-818(2015)
64)野間口広・岩切宗利：非線形処理構造を持つストリーム暗号に関する一検討，研究報告マルチメディア通信と分散処理 2015-DPS-162(25)，pp.1-8(2015)
65)文部科学省：ＯＥＣＤ 国際教員指導環境調査(TALIS2013)のポイント，http://www.mext.go.jp/component/b_menu/other/__icsFiles/afieldfile/2014/06/30/1349189_2.pdf，(2021.8.8最終確認)
66)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，pp.111-112(2019)
67)岡田光代・花田・経子・山内正人・野尻梢・砂原 秀樹：謎解きスタンプラリー型小学生向けセキュリティ教材の開発，情報処理学会マルチメディア分散協調とモバイルシンポジウム2021論文集，pp.1599-1603 (2021)
68)前原俊信・相原玲二・平賀博之・山下雅文・岡本英治・入川義克・下前弘司・村山太郎・山岡大基・合田大輔・川中裕美子：確かな学力を育むためのマルチメディア活用--科学的思考力やリテラシーを育むことを目指して，広島大学学部・附属学校共同研究機構部・附属学校共同研究紀要 (37)，pp.189-193(2008)
69)塩田真吾・髙瀬和也・酒井郷平・小林渓太・籔内祥司：当事者意識を促す中学生向け情報セキュリティ教材の開発と評価 －「あやしさ」を判断させるカード教材の開発－，一般社団法人 CIECコンピュータ＆エデュケーション 44，pp.85-90(2018)
70)渥美清隆：高専入学直後の学生に対する情報化社会に関する講義とその試作方法について，情報処理学会研究報告インターネットと運用技術(IOT)2009巻21号，pp.295-

298(2009)
71)小林勝・川島芳昭・石川賢：情報セキュリティに関する研修教材の開発－教員の意識面の向上と行動面の改善を目的として－，宇都宮大学教育学部教育実践総合センター紀要no.31，pp.17-24(2008)
72)文部科学省：ＧＩＧＡスクール構想の下で整備された１人１台端末の積極的な利活用等について（通知），https://www.mext.go.jp/content/20210414-mxt_jogai01-000014225_001.pdf(2021.8.8最終確認)
73)水沼彩子・内田勝也：子どもと携帯サイトに関する課題について，電子情報通信学会技術研究報告109(115)，pp.65-70(2009)
74)森幹彦・平岡斉士・上田浩・喜多一・竹尾賢一・植木徹・石井良和・外村孝一郎・徳平省一：情報教育に関する大学新入生の状況変化―京都大学新入生アンケートの結果から，情報処理学会論文誌 51(10)，pp.196-197(2010)
75)森幹彦・上田浩・喜多一：教科「情報」の履修状況と情報リテラシーに関する平成22年度新入生アンケートの結果について，情報処理学会研究報告インターネットと運用技術(IOT) 2011-IOT-12(22)，pp.1-7(2011)
76)森幹彦・平岡斉士・上田浩・喜多一・竹尾賢一・植木徹・石井良和・外村孝一郎・徳平省一：教科「情報」の履修状況と情報リテラシーに関する大学新入生の状況-平成24年度京都大学新入生アンケートの結果から -，情報処理学会「インターネットと運用技術シンポジウム2012」論文集 ，pp.23-30(2012)
77)小熊良一・本村猛能：日本の小学校・中学校の情報モラル教育に関する教科書，学習指導要領，実態調査報告書の分析，群馬大学教科教育学研究16号，pp.45-54(2017)
78)山本博之：情報科における研究会活動の意義と高校現場の研修体制，情報処理57(7)，pp.666-669(2016)
79)髙瀬和也・酒井郷平・塩田真吾：ヒューマンエラー対策手法を用いた個人情報漏洩を防ぐ教員研修教材の開発と評価，コンピュータ＆エデュケーション45，pp.115-120(2018)
80)片岡久明：情報セキュリティをテーマとした課題解決型授業の実践，北海道教育大学学校教育学会誌，第18号，pp.15-24(2013)
81)堤健人・川田和男：協働的問題解決を取り入れた技術科の授業実践，広島大学附属東雲中学校研究紀要，第47号，pp.55-60(2016)
82)前掲32)，(2017)
83)前掲27)，(2017)

関連論文

1)小熊良一・山本利一：日本の学校教育における教員の情報セキュリティ研究の課題と展望，群馬大学教育学部紀要芸術・技術・体育・生活科学編，第54巻，pp.61-67 (2019)

2)小熊良一・山本利一：義務教育における情報セキュリティ教育の現状と課題，群馬大学教育学部紀要芸術・技術・体育・生活科学編，第55巻，pp.79-90(2020)

第2章　情報セキュリティ教育に関する実態

1. 緒言

第1章では，情報セキュリティの概念や日本の初等中等教育における情報セキュリティ教育の歴史の整理，先行研究の調査をおこない，文部科学省が示す情報セキュリティ教育を整理し，研究の方向性を定めてきた。先行研究の調査から，教員の実態，児童・生徒の小・中学校の修了段階の意識・知識の実態の把握が不足していることが明らかになった。

第2章では，児童・生徒の実態を把握する。児童・生徒の実態を把握するためには，指導する教員の情報セキュリティへの意識，行動，知識の現状を確認し，その知見を基に児童・生徒のより具体的な調査方法や項目を検討する必要がある。そこで，第１段として，小・中学校に勤務する教員の実態を調査する。次に，小学校修了段階の児童の情報セキュリティの意識と知識を調査し，実態を把握する。小学校と同様に，中学校修了段階の生徒の情報セキュリティの意識と知識を調査し，実態を把握する。これらから，小・中学校における情報セキュリティ教育の現状と課題を明らかにする。

小・中学校の教員の情報セキュリティの意識と知識は，児童・生徒の指導に影響を及ぼす。教員の実態調査は，文部科学省が実施した「学校における教育の情報化の実態等に関する調査」[84]で，情報セキュリティの基本的な知識や児童・生徒への指導力についての意識調査がおこなわれている。また，坂東ら(2020)[85]により，小学校教員を対象にした情報セキュリティの指導意識に関する研究がおこなわれている。いずれの調査も教員の意識調査が中心であり，教員の情報セキュリティの意識，知識，行動を踏まえた実態についての視点が不足している。

児童・生徒の実態調査は，内閣府で実施した「青少年のインターネット利用環境実態調査」[86]，文部科学省で実施した「全国学力・学習状況調査」の質問紙調査[87]，など全国規模で調査がおこなわれている。しかし，現在おこなわれている調査は，実施時期と調査対象を小・中学校の修了段階に限定しておらず，小・中学校修了段階での情報セキュリティ教育の成果を把握することを目的とした調査という視点が不足している。

第2章は，3つの節で構成している。第1節では小・中学校教員の実態を調査し，小・中学校に勤務する教員の情報セキュリティへの意識，行動，知識を確認し，その知見を基に児童・生徒の調査項目を検討する。第2節では，第1節で得た知見を基に小学校修了段階の実態を調査し，その結果から現在の小学校における情報セキュリティ教育の現状と課題を明らかにする。第3節では，第1節で得た知見を基に中学校修了段階の実態を調査し，その結果から現在の中学校における情報セキュリティ教育の現状と課題を明らかにする。この3つの調査で得た知見を活かして第3章で情報セキュリティ教材を作成し，第4

章で開発した情報セキュリティ教材を活用した授業実践をおこない，教材および指導の効果について検証をおこなっていく。

第1節　小・中学校教員の実態

1.1 はじめに

学校は，学籍関係，進路関係，健康関係など個人情報を含んだ資料[88]を管理している。その中には，指導要録のように保護者についての個人情報が含まれている資料もある。小・中学校の教員は，これらの資料をなんらかの形で日々の業務で扱っており，情報セキュリティ対策に対しての意識と知識に裏付けされた適切な行動が求められる。そして，これらの意識，行動，知識が，児童・生徒への指導の礎となると考えられる。

文部科学省が発表した「令和元年度学校における教育の情報化の実態等に関する調査結果」[89]によると，教員のＩＣＴ活用指導力の状況の調査で，「D. 情報活用の基盤となる知識や態度について指導する能力」に関する4つの中で「D3. 情報セキュリティ指導に関する項目」が，76.8%と最も低い結果となっている。これは，情報セキュリティに関する知識や行動に不安があるためと考えられる。また，坂東ら(2020)[90]がおこなった情報セキュリティ教育に関する小学校教員の意識調査の結果では，情報セキュリティ教育を実施する必要性は感じているものの，自分で情報セキュリティを指導する自信がないという実態が報告されており，教職の経験年数にかかわらず情報セキュリティの知識水準が情報セキュリティ教育の指導に対しての自信に影響することが報告されている。

これらを整理すると情報セキュリティに関しての指導力は，自分自身の情報セキュリティの知識を高めなければ，教職の経験年数を重ねても向上しないことになる。

そこで，第１節では，小・中学校に勤務する教員の情報セキュリティに関する意識，行動，知識の現状を調査することとした。

1.2 調査の対象と方法

(1) 調査の目的

小・中学校に勤務する教員の情報セキュリティに関する意識，行動，知識について実態調査をおこない，現状と課題を明らかにする。

(2) 調査期日

2018年6月に実施した。

(3) 調査対象

A県の小学校，中学校，中等教育学校前期課程に勤務する教員178名(小学校88名，中学校・中等教育学校90名)に実施した。本実践対象者のうち，回答に不備のあった 19名を分析から除外した。その結果，有効回答数は159名(小学校81名，中学校・中等教育学校78名)，有効回答率は 89.3%であった。調査対象の各学校種別の人数および割合を表2.1に示す。

表2.1　調査対象の各学校種別の人数および割合

校種(A県内の学校数)	人数	割合(%)
小学校(312)	81	50.9
中学校・中等教育学校(170)	78	49.1

※割合は調査対象者の人数の比較

1.3　調査方法

調査は，A県教育センターで実施された5年目の教員を対象とした研修の後に実施した。並行して，小・中学校で情報システム運営担当経験のある教員に郵送により実施した。マークシートと記述式による調査を併用して実施した。

1.4 調査項目および分析方法

調査項目は，中学校で利用されている技術・家庭科(技術分野)[91)~93)]の3社の教科書で共通して取り上げている内容および「公益財団法人全国商業高等学校協会情報処理検定」[94)]で実施している「ビジネス情報部門2級」の第45回～第56回までの12回の情報セキュリティに関する検定問題の中で，2回以上出題されている内容とした。「ビジネス情報部門2級」検定は，情報処理技術者などの資格への入口としてつくられた高校生向けの検定試験で，一般的な情報セキュリティに関して出題がされているものである。また，岡山県総合教育センターが作成した「教職員の情報セキュリティ意識を高める校内研修パッケージ」[95)]を参考にした。

設問は，「情報セキュリティの必要性の意識」，「情報セキュリティを確保するための意識と行動」，「情報セキュリティの知識」の3つの調査項目で作成した。

「情報セキュリティの必要性の意識」は，学校における情報セキュリティの必要性の考えについて1問の設問を作成した。

「情報セキュリティを確保するための意識と行動」は，不正侵入対策，情報漏えい対策の2つの内容で，物理的対策(端末管理，外部媒体管理，情報破棄，出力用紙管理，情報整理)，人的対策(Webページ閲覧，ソフトウェアインストール，機密文書管理，誤送信，データ消去)，技術的対策(ウィルス対策ソフトウェア，OS・ソフトウェア更新，ウィルス対策ソフトウェア更新，ID・パスワード管理，暗号化)について15問作成した。

「情報セキュリティの知識」は，技術的対策(個人認証，ID，パスワード，ファイアウォール，フィルタリング，ウィルス対策ソフトウェア，ウィルス対策ソフトウェア更新，セキュリティホール，暗号化，バックアップ)の回答について9問作成した。

「意識」，「行動」については，5件法で回答を求めた。5件法で回答を求めたものは，「意識」については，「重要である」を5点，「どちらかといえば重要である」を4点，「どちらともいえない」を3点，「どちらかといえば重要でない」を2点，「重要でない」を1点と見なし得点化し，平均と標準偏差を求めた。「行動」については，「して

いる」を5点，「どちらかといえばしている」を4点，「どちらともいえない」を3点，「どちらかといえばしていない」を2点，「していない」を1点と見なして数量化して，「意識」と同様な処理をおこなった。また，「意識」と「行動」の同じ設問については，t検定(対応あり)をほどこし，差異を確認した。「知識」については，各設問の空欄(A～L)に，適切な言葉を記述式で回答し，文章を完成させる問題とした。分析は，正答・誤答で分類整理をおこなった。さらに，情報セキュリティの知識と行動の関係を把握するために，前述した「情報セキュリティを確保するための行動」と「情報セキュリティの知識」の関連する調査について，行動に関する調査項目を上位群と下位群に分類し，知識の正答率について，比較をおこなった。

本調査は，事前に教員研修の主催者及び回答者に，実態調査の了解を得たうえでおこなった。また，研修受講者およびアンケート回答者には，倫理的配慮として，アンケートの使用目的，および研究用途以外には用いないこと，個人が特定されないように配慮することを説明した。活用した設問と設問項目を表2.2に示す。

表2.2　小・中学校教員の設問と設問項目

1. 情報セキュリティの重要性の意識	
①学校において情報セキュリティを確保することは大切だと思いますか。	(情報セキュリティの重要性)
2.情報セキュリティを確保するための意識と行動	
＜物理的対策(情報漏えい)＞	
②離席時や帰宅時にコンピュータを不正操作されないための対策をしている。	(端末管理)
③USBメモリなどを持ち出す時には，常に携行している。	(外部媒体管理)
④機密情報を含む紙や記録媒体は，適切な方法で廃棄や削除をしている。	(情報破棄)
⑤コピーやプリンタの出力用紙は，直ちに回収している。	(出力用紙管理)
⑥帰宅時には机上を片付けている。	(情報の整理)
＜人的対策(不正侵入)＞	
⑦仕事に関係のないWebページは職場では見ないようにしている。	(Web ページ閲覧)
⑧学校のコンピュータに無断でソフトウェアをインストールしないようにしている。	(ソフトウェアインストール)
＜人的対策(情報漏えい対策)＞	
⑨機密情報は電子メールで送らないようにしている。	(機密文書管理)
⑩電子メールを誤送信しないように注意している。	(誤送信)
⑪仕事のため自宅で使用したデータは，自宅のコンピュータから必ず消去している。	(データ消去)
＜技術的対策(不正侵入)＞	
⑫ウィルス対策ソフトウェアを自宅のコンピュータにもインストールしている。	(ウィルス対策ソフトウェア)
⑬OS(Windows等)やソフトウェアは定期的に更新し，最新の状態にしている。	(OS・ソフトウェア更新)
⑭ウィルス対策ソフトウェアは，定期的に更新し，最新の状態にしている。	(ウィルス対策ソフトウェア更新)
＜技術的対策(情報漏えい対策)＞	
⑮コンピュータのユーザーIDやパスワードは，他人に知られないよう管理している。	(ID・パスワード管理)
⑯持ち出したデータは，パスワードが設定されているか暗号化されている。	(暗号化)
3.情報セキュリティの知識	
⑰不正侵入を防ぐ技術として(A.個人認証)や(B.ファイアウォール)などがあります。(A)の仕組みとして(C.ID)と(D パスワード)を組み合わせて入力する方法が使われます。(B)は防火壁の意味で，一定の基準を設けて，通過させる情報と通過させない情報を選別しネットワーク外部からの不正進入を防ぐ仕組みです。	
⑱インターネット上の有害な情報を制限・遮断するシステムとして(E.フィルタリング)があります。	
⑲コンピュータウィルスに感染しないように(F.ウィルス対策ソフトウェア)をインストールすることが有効です。なお，(F)で対応できるのはすでに知られているコンピュータウィルスのみなのでウィルス定義ファイルを常に最新のものに(G.アップデイト)しておくことが大切です。	
⑳(H.セキュリティホール)は，プログラムの設計ミスなどにより発生するセキュリティ上の欠陥のことです。	
㉑ネットワークを利用して情報を送受信するとき他人に見られたり書き換えられたりする危険があります。これを防ぐために情報を(I.暗号化)して送受信をすることができます。(I.暗号化)された情報は他の人が見ても暗号文になっているため内容を知ることができません。	

1.5 結果と考察

(1) 情報セキュリティの重要性の意識

質問項目1「情報セキュリティの重要性」は，意識の平均4.90と高い値を示した。回答の割合は，「思う」90.6%，「どちらかといえば思う」8.8%，「どちらともいえない」0.6%,「どちらかといえば思わない」0%，「思わない」0%であった。この結果から，小・中学校に勤務する教員は，学校において情報セキュリティを確保することが大切であると認識していることが示された。この理由として，USBメモリや書類の紛失による個人情報の漏えいやインターネットを介したコンピュータウィルスの感染などの問題が学校で起きており，教員の情報セキュリティを確保することの重要性への認識が高まっているためと考える。「情報セキュリティの重要性」の結果を表2.3に示す。

表2.3 情報セキュリティの重要性

No.	質問項目	平均	S.D.
1.	情報セキュリティの必要性	4.90	0.32

(N=159)

(2) 情報セキュリティを確保するための意識と行動

「情報セキュリティを確保するための意識と行動」の結果を表2.4に示す。

物理的対策は，端末管理，外部媒体管理，情報破棄，出力用紙管理，情報の整理について調査をおこなった。

質問項目2「端末管理」は，意識の平均4.62，行動の平均3.34であった。意識と行動に関して t 検定(対応あり)をおこなった結果，有意差が確認された($t(158)=13.07$, $p<.01$)。

質問項目3「外部媒体管理」は，意識の平均4.90，行動の平均4.53であった。意識と行動に関して t 検定(対応あり)をおこなった結果，有意差が確認された($t(158)=5.97$, $p<.01$)。

質問項目4「情報破棄」は，意識の平均4.94，行動の平均4.65であった。意識と行動に関して t 検定(対応あり)をおこなった結果，有意差が確認された($t(158)=6.20$, $p<.05$)。

質問項目5「出力用紙管理」は，意識の平均4.40，行動の平均4.09であった。意識と行動に関して t 検定(対応あり)をおこなった結果，有意差が確認された($t(158)=4.27$, $p<.01$)。

質問項目6「情報の整理」は，意識の平均4.49，行動の平均4.07であった。意識と行動に関して t 検定(対応あり)をおこなった結果，有意差が確認された($t(158)=5.30$, $p<.01$)。

これらの結果から，情報セキュリティを確保するために物理的対策をおこなうことの

重要性は認識しているものの，実際の行動にむすびついていないということが示された。その理由として，多忙な業務のために紙媒体の処理や，USBメモリなどの外部媒体管理などができていないことが推測できる。物理的対策を確実なものにしていくためには，廃棄や整理，外部媒体や端末の管理を学校としてルール化して徹底するなどの対策が必要と考える。

人的対策は， 不正侵入(Webページ閲覧，ソフトウェアインストール）及び，不正侵入情報漏えい（機密文書管理，誤送信，データ消去）について調査をおこなった。

不正侵入の人的対策についての結果を以下に示す。質問項目7「Webページ閲覧」は，意識の平均4.43，行動の平均4.26であった。意識と行動に関して t 検定(対応あり)をおこなった結果，有意差が確認された($t(158)=2.26$, $p<.05$)。

質問項目8「ソフトウェアインストール」は，意識の平均4.76，行動の平均4.59であった。意識と行動に関して t 検定(対応あり)をおこなった結果，有意差が確認された($t(158)=2.36$, $p<.05$)。

これらの結果から，不正侵入に対して人的対策をおこなうことの重要性は認識しているものの，実際の行動にむすびついていないということが示された。この理由として，利用する端末を自分にとって，使いやすくしようとする意識が働いていると推測できる。ソフトウェアのインストールやWebページの閲覧については，技術的な利用制限が可能なため，情報セキュリティの視点からのリスクを考慮し，業務に支障のきたさない範囲で利用制限をかけることが必要と考える。

つぎに，情報漏えいの人的対策についての結果を以下に示す。質問項目9「機密文書管理」は，意識の平均4.84，行動の平均4.79であった。意識と行動に関して t 検定(対応あり)をおこなった結果，有意差は確認されなかった($t(158)=1.05$, $n.s.$)。

質問項目10「誤送信」は，意識の平均4.93，行動の平均4.76であった。意識と行動に関して t 検定(対応あり)をおこなった結果，有意差が確認された($t(158)=2.23$, $p<.01$)。

質問項目11「データ消去」は，意識の平均4.64，行動の平均3.48であった。意識と行動に関して t 検定(対応あり)をおこなった結果，有意差が確認された($t(158)=11.06$, $p<.01$)。

これらの結果から，情報漏えいに対して人的対策をおこなうことの重要性は認識しているものの，実際の行動にむすびついていないものもあることが示された。その理由として，授業や生徒指導などの多忙な業務の間に文書処理などをおこなうため，最終的な安全確認がおろそかになっていると推測できる。各学校には，情報を扱うための情報セキュリティポリシーが定められており，個人情報を扱うルールが決まっている。情報の大切さとルールを厳守する行動を促す対策が必要と考える。

技術的対策は，不正侵入(ウィルス対策ソフトウェア，OS・ソフトウェア更新，ウィルス対策ソフトウェア更新）及び不正侵入情報漏えい（ID・パスワード管理，暗号化）に

ついて調査をおこなった。

不正侵入の技術的対策についての結果を以下に示す。質問項目12「ウィルス対策ソフトウェア」は，意識の平均4.87，行動の平均4.58であった。意識と行動に関して t 検定(対応あり)をおこなった結果，有意差が確認された(t (158)=4.10， p<.01)。

質問項目13「OS・ソフトウェア更新」は，意識の平均4.63，行動の平均は3.93であった。意識と行動に関して t 検定(対応あり)をおこなった結果，有意差が確認された(t (158)=7.79， p<.01)。

質問項目14「ウィルス対策ソフトウェア更新」は，意識の平均4.86，行動の平均4.23であった。意識と行動に関して t 検定(対応あり)をおこなった結果，有意差が確認された(t (158)=7.67， p<.01)。

表2.4　情報セキュリティを確保するための意識と行動

№		意識		行動		
	質問項目	平均	S.D.	平均	S.D.	検定
	＜物理的対策＞					
2.	端末管理	4.62	0.60	3.34	1.39	**
3.	外部媒体管理	4.90	0.32	4.53	0.79	**
4.	情報破棄	4.94	0.26	4.65	0.60	*
5.	出力用紙管理	4.40	0.71	4.09	0.86	**
6.	情報の整理	4.49	0.67	4.07	1.04	**
	＜人的対策＞					
7.	Webページ閲覧	4.43	0.67	4.26	0.94	*
8.	ソフトウェアインストール	4.76	0.52	4.59	0.94	*
9.	機密文書管理	4.84	0.48	4.79	0.59	*n. s.*
10.	誤送信	4.93	0.26	4.76	0.48	**
11.	データ消去	4.64	0.57	3.48	1.35	**
	＜技術的対策＞					
12.	ウィルス対策ソフトウェア	4.87	0.38	4.58	1.00	**
13.	OS・ソフトウェア更新	4.63	0.55	3.93	1.14	**
14.	ウィルス対策ソフトウェア更新	4.86	0.39	4.23	1.12	**
15.	ID・パスワード管理	4.84	0.41	4.39	0.91	**
16.	暗号化	4.84	0.40	3.30	1.42	**

*：p<.05 **：p<.01 (N=159)

これらの結果から，不正侵入に対して技術的対策をおこなうことの重要性は認識しているものの，実際の行動にむすびついていないことが示された。この理由として，一部

の教員が，ウィルス対策ソフトウェアやソフトウェア更新などの技術的対策の効果を理解していないことが推測できる。不正侵入に対して技術的対策をおこなう意義や方法を周知する学習の機会が必要であると考えられる。

つぎに，情報漏えいの技術的対策についての結果を以下に示す。質問項目15「ID・パスワード管理」は，意識の平均4.84，行動の平均4.39であった。意識と行動に関して t 検定(対応あり)をおこなった結果，有意差が確認された($t(158)=6.74$, $p<.01$)。

質問項目16「暗号化」は，意識の平均4.84，行動の平均3.30であった。意識と行動に関して t 検定(対応あり)をおこなった結果，有意差が確認された($t(158)=14.22$, $p<.01$)。

これらの結果から，情報漏えいに対して技術的対策をおこなうことの重要性は認識しているものの，実際の行動にむすびついていないことが示された。この理由として，一部の教員にID・パスワード管理を忘れてしまう心配があるという心理的な不安があることが想定される。ID・パスワードは，生体認証，多要素認証など最新の技術で人間の記憶を補うことができる。これらの技術を導入することで教員の不安を回避できるものと考えられる。

(3) 情報セキュリティの知識

情報セキュリティの知識の正答率を表2.5に示す。

情報セキュリティの知識の設問は，「不正侵入」と「情報漏えい」の 2 つの内容に分類することができる。「不正侵入」に関わる 4 項目の知識は，質問項目 B「ファイアウォール」52.8%，質問項目 E「フィルタリング」44.7%，質問項目 F「ウィルス対策ソフトウェア」69.2%，質問項目 G「アップデイト」77.4%という結果であった。

表2.5　情報セキュリティの知識の正答率(N=159)

No.	質問項目	正答数	割合(%)
A.	個人認証	27	17.0
B.	ファイアウォール	84	52.8
C.	ID	64	40.3
D.	パスワード	65	40.9
E.	フィルタリング	71	44.7
F.	ウィルス対策ソフトウェア	110	69.2
G.	アップデイト	123	77.4
H.	セキュリティホール	18	11.3
I.	暗号化	116	73.0

(N=159)

質問項目B「ファイアウォール」，質問項目E「フィルタリング」の2つは，質問項目F「ウィルス対策ソフトウェア」，質問項目G「アップデイト」の2つと比較すると正答率が低かった。このことは，情報セキュリティを確保するための対応策と比較して，情報セキュリティを確保するための仕組みの知識が不足していることを示していると考える。

「情報漏えい」に関する正答率は，質問項目A「個人認証」17.0%，質問項目C「ID」40.3%，質問項目D「パスワード」40.9%，質問項目H「セキュリティホール」11.3%，質問項目I「暗号化」73.0%という結果であった。質問項目A「個人認証」，質問項目C「ID」，質問項目D「パスワード」について正答率が50%以下であった。また，質問項目I「暗号化」は，他の4つの質問項目と比較して正答率が高かった。

これらの結果から，不正侵入に関わる知識と同様に情報セキュリティを確保するための対応策と比較して，情報セキュリティを確保するための仕組みの知識が不足していることを示していると考えられる。なお，本調査をおこなうことで情報セキュリティの知識が身に付き，今回の知識の結果に影響があった可能性があったことを追記しておく。

(3) 情報セキュリティの行動と知識の関連

情報セキュリティの知識と行動の関連を把握するために，前述した「情報セキュリティを確保するための行動」と「情報セキュリティの知識」の関連する項目を比較した。「情報セキュリティの行動」について「している」，「どちらかといえばしている」と答えた教員を上位群，「どちらかといえばしていない」，「していない」と答えた教員を下位群として，関連する「情報セキュリティの知識」の正答率を比較した。比較した項目は，「ID・パスワード」，「ウィルス対策ソフトウェア」，「アップデイト」，「暗号化」の4つである。以下に調査結果を示す。

調査項目1「ID・パスワード」は，「情報セキュリティの知識」の質問項目C「ID」と質問項目D「パスワード」の両方の正答について，「情報セキュリティを確保するための行動」の質問項目15「ID・パスワード管理」の上位群（142名）と下位群（10名）を比較した。調査の結果，上位群の正答率46.5%，下位群の正答率30.0%であった。

調査項目2「ウィルス対策ソフトウェア」は，「情報セキュリティの知識」の質問項目F「ウィルス対策ソフトウェア」の正答について，「情報セキュリティを確保するための行動」の質問項目12「ウィルス対策ソフトウェア」の上位群（141名）と下位群（9名）を比較した。調査の結果，上位群の正答率69.5%，下位群の正答率66.7%であった。

調査項目 3「アップデイト」は，「情報セキュリティの知識」の質問項目 G「アップデイト」の正答について，「情報セキュリティを確保するための行動」の質問項目 13「OS・ソフトウェア更新」の上位群（114 名）と下位群（21 名）を比較した。調査の結果，上位群の正答率 78.9%，下位群の正答率 68.9%であった。

調査項目 4「暗号化」は，「情報セキュリティの知識」の質問項目 I「暗号化」の正答

について，「情報セキュリティを確保するための行動」の質問項目 16「暗号化」の上位群（91 名）と下位群（50 名）を比較した。調査の結果，上位群の正答率 78.0%，下位群の正答率 72.0%であった。

これらの結果から，4 つの調査項目とも，「情報セキュリティを確保するための行動」の上位群が，下位群と比較すると正答率が高い結果となった。この結果から情報セキュリティの知識と行動には，相関関係があると推測される。情報セキュリティの知識を高めることで，情報セキュリティを確保する行動につながる可能性があることが示唆されたと考える。

情報セキュリティの行動と知識の関連を表2.6に示す。

表2.6 情報セキュリティの「行動」と「知識」の関連

No.	調査項目	上位群の正答率(%)	下位群の正答率(%)
1.	ID・パスワード	46.5	30.0
2.	ウィルス対策ソフトウェア	69.5	66.7
3.	OS・ソフトウェア更新	78.9	68.9
4.	暗号化	78.0	72.0

この調査結果から，情報セキュリティの「知識」のある教員は，適切な「行動」につながっていると考えられる。教員の情報セキュリティの「知識の習得」，「行動の変容」の関係を図 2.1 に示す。

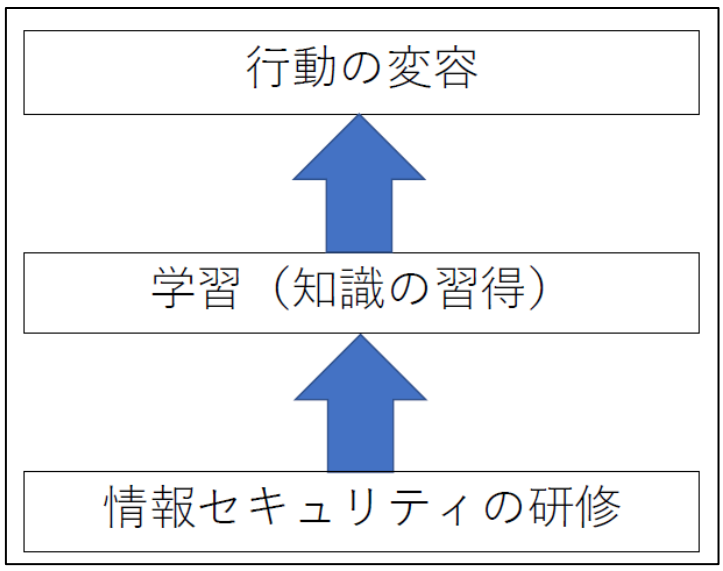


図2.1 教員の情報セキュリティの「知識の習得」，「行動の変容」の関係

小・中学校に勤務する教員は，前述のとおり「情報セキュリティへの重要性の意識」は高い。しかし，情報セキュリティの「知識」が不足しているため，物理的対策，人的対策，技術的対策の行動にむすびついていない。

学校の情報セキュリティを確保するには，3つの方法が必要であると考えられる。1つ目は，廃棄や整理，外部媒体や端末の管理の知識を高め，情報セキュリティポリシーの周知を徹底し行動に結びつけること。2つ目は，ウィルス対策ソフトウェアやソフトウェア更新などの情報セキュリティ対策の具体的な方法やその効果などの知識を習得する研修を充実させること。3つ目は，生体認証，多要素認証など人間の記憶を補う技術的対策の方策を理解し，日々の業務に取り入れていくことである。

情報セキュリティの重要性の「意識」の基に，「知識」を増やすことにより，「行動」の変容につながり，情報セキュリティを確保することにつながっていくと考えられる。

1.6 おわりに

以上，第１節で，小・中学校に勤務する教員の情報セキュリティに関する実態調査の結果を整理する。

1. 小・中学校に勤務する教員は，学校において情報セキュリティを確保することが大切であると認識している。
2. 情報セキュリティを確保するために物理的対策をおこなうことの重要性は認識しているものの，実際の行動にむすびついていないということが示された。物理的対策を確実なものにしていくために，廃棄や整理，外部媒体や端末の管理を学校としてルール化して徹底するなどの対策が必要である。
3. 不正侵入に対して人的対策をおこなうことの重要性は認識しているものの，実際の行動にむすびついていないということが示された。情報セキュリティの視点からのリスクを考慮し業務に支障のきたさない範囲で利用制限をかけることが必要である。
4. 情報漏えいに対して人的対策をおこなうことの重要性は認識しているものの，実際の行動にむすびついていないものもあることが示された。情報セキュリティの知識を高め，各学校の情報セキュリティポリシーの厳守につながる研修が必要である。
5. 不正侵入に対して技術的対策をおこなうことの重要性は認識しているものの，実際の行動にむすびついていないことが示された。不正侵入に対して技術的対策をおこなう意義や方法を周知する学習の機会が必要である。
6. 情報漏えいに対して技術的対策をおこなうことの重要性は認識しているものの，実際の行動にむすびついていないことが示された。生体認証，多要素認証など人間の記憶を補う技術的対策の方策を理解し，日々の業務に取り入れていくことが必要である。

教員の情報セキュリティへの「意識」と「知識」，情報セキュリティに配慮した「行動」の蓄積は，児童・生徒に情報セキュリティを指導する基礎となる。

第1節の教員の調査の知見を踏まえて，小・中学生の情報セキュリティの意識と知識の調査内容を検討し，第2節では，小学校の修了段階の情報セキュリティ教育の実態を調査していく。また，第3節では，中学校の修了段階の情報セキュリティ教育の実態を調査していく。

第2節　小学校修了段階の実態

2.1 はじめに

第 1 章で，小学校では，中学校の技術・家庭科(技術分野)や高等学校の情報のように情報セキュリティを指導する教科が定められていないことを述べた。そのため，情報セキュリティの指導は各学校の取組に任されている[96)]。

内閣府が，令和2年11月～12月に実施した「青少年のインターネット利用環境実態調査」[97)]によると小学生5・6年生のインターネットの利用率(91.7%)，利用端末については，スマートフォン(44.4%)，携帯ゲーム機(44.1%)が中心であり，35.0%の利用端末にフィルタリング等の対策がおこなわれていることが報告されている。また，文部科学省が小学校6年生を対象にした毎年5月に実施している「全国学力・学習状況調査の質問紙調査」[98)]によると，平成24年～平成30年の7年間の報告で“インターネットを長時間利用すると学力に影響がある”と報告されている。

2018年に安心ネットづくり促進協議会が発表した小学生1年生から6年生を対象にした情報モラルに関する調査[99)]では，情報セキュリティに関する2項目で，「セキュリティソフトウェアの知識」の正答率が67.4%，「ウィルス対策の理解」の正答率が52.1%であった。

いずれの先行調査も調査時期が小学校の修了段階に特定されていないため，小学校の情報セキュリティ教育で身に付けた最終的な実態を把握することが難しい。また，調査内容が，情報モラルの調査の一部としておこなわれているため物理的対策，人的対策，技術的対策の3つの対策から情報セキュリティの意識や知識をとらえるものになっていない。

そこで第2節では，　第1節で得た小・中学校に勤務する教員の実態調査の知見を踏まえて情報セキュリティの調査項目を作成し，4月の小学校卒業直後にインターネットの利用実態，情報セキュリティの意識・知識を調査し，小学校修了段階で身に付けている情報セキュリティの意識と知識の現状を把握することとした。

2.2 調査の対象と方法

(1) 調査の目的

小学校卒業直後にインターネットの利用実態，情報セキュリティの意識と知識の実態調査をおこない，小学校修了段階で身に付けている情報セキュリティの意識と知識を把握することにより，小学校での情報セキュリティ教育の現状を明らかにする。

(2) 調査期日

2021年4月に実施した。

(3) 調査対象

2021年3月に小学校を卒業したA県内の公立中学校2校の中学校1年生158名を調査対象と

した。

(4)調査方法

調査は，技術・家庭科(技術分野)の中学1年の4月の最初の授業の中で30分配当し，インターネットによるアンケートフォーム(Google Form)を使って実施した。

2.3 調査項目および分析方法

調査項目は，前節の小・中学校に勤務する教員の実態調査で明らかにした情報セキュリティの意識，行動，知識の調査項目と知見を踏まえ，インターネットの利用実態，情報セキュリティの意識，情報セキュリティの知識の3つの内容について作成した。また，文部科学省が作成した「情報モラル指導モデルカリキュラム表」[100]および「情報活用能力の体系表例」[101]の小学校の指導内容，「技術・家庭科(技術分野)」の3社の教科書で共通して取り上げている内容をふまえて作成した。

利用実態の調査項目と選択項目を表2.10に示す。

表2.10　利用実態の調査項目と選択項目

1.あなたが小学校の時，学校の授業で勉強したものをすべて選んでください。	(学習経験)
a.インターネットで被害者にならない使い方　b.インターネットの法律　c.情報セキュリティ d.インターネットで加害者にならない使い方　e.インターネットを適切に使う方法 f.学校では勉強したことがない	
2.あなたが，家でインターネットを利用している機器をすべて選んでください	(利用端末)
a.家族共用のスマートフォン　b.自分専用のスマートフォン　c.ゲーム機 d.学校のタブレットPC　e.個人のタブレットPC　f.家族共用のPC g.自分専用のPC　h.個人のPC	
3.あなたがインターネットに利用しているサービスをすべて選んでください	(利用サービス)
a.学校の勉強　b.通信講座やインターネットの勉強　c.インターネット検索　d.読書 e.懸賞応募　f.音楽　g.動画視聴　h.ゲーム i.買い物　j.フリマ　k.電子メール　l.LINE m.FaceBook　n.Twitter　o.その他	
4.あなたは，平日，インターネットを家でどれくらい使っていますか。	(平日の利用時間)
a.使っていない　b.1時間未満　c.1～2時間　d.2～3時間 e.3～4時間　f.4～5時間　g.5時間以上	
5.あなたは，休日，インターネットを家でどれくらい使っていますか。	(休日の利用時間)
a.使っていない　b.1時間未満　c.1～2時間　d.2～3時間 e.3～4時間　f.4～5時間　g.5時間以上	

※()は調査項目

情報セキュリティの意識は，物理的対策(外部媒体管理，端末管理)，人的対策(ID・パスワード管理，個人情報管理，ダウンロード)，技術的対策(フィルタリング，ウィルス対策ソフトウェア，ソフトウェア更新)の3つの対策について8個の調査項目および設問を作成した。意識の調査は，情報セキュリティを確保することの重要性の考えに対して，4件法で調査をおこない「あてはまる」を4点，「どちらかというとあてはまる」を3点，「どちらかというとあてはまらない」を2点，「あてはまらない」を1点とみなし得点化し，平均と標準偏差を求めた。情報セキュリティの意識の調査項目を表2.11に示す。

表2.11　情報セキュリティの意識の調査項目

＜物理的対策＞
6.SDカードやUSBメモリをなくしたり，壊したりすることのないよう扱うことは大切だと思いますか。(外部媒体管理)
7.タブレットPC，スマートフォン，ゲーム機をなくしたり，壊したりすることのないように扱うことは大切だと思いますか。(端末管理)
＜人的対策＞
8.自分のIDやパスワードを管理することは大切だと思いますか。(ID・パスワード管理)
9.インターネットで個人情報(自分の名前や電話番号など)を書き込むときは，安全を確認することが大切だと思いますか。(個人情報管理)
10.インターネットにある音声や動画などのデータをダウンロードするときは，安全を確認することが大切だと思いますか。(ダウンロード)
＜技術的対策＞
11.スマートフォンやゲーム機にフィルタリングをすることは大切だと思いますか。(フィルタリング)
12.スマートフォンやゲーム機にウィルス対策ソフトウェアを入れることは大切だと思いますか。(ウィルス対策ソフトウェア)
13.スマートフォンやゲーム機のソフトウェアやアプリを最新版にしておくことは，大切だと思いますか。(ソフトウェア更新)

※()は調査項目

情報セキュリティの知識は，物理的対策(外部媒体管理，端末管理)，人的対策(ID・パスワード管理，個人情報管理，ダウンロード)，技術的対策(フィルタリング，ファイアウォール，SSL/TSL，ウィルス対策PC，ウィルス対策携帯型情報端末，アップデイト)の3つの対策について12個の調査項目および設問を作成した。調査は，各設問に対して，「正しい，違っている，意味がわからない」の中から，適切な回答を選ぶ設問とし，正答率の調査をおこなった。さらに，情報モラル学習の経験を認識している群と認識していない群に分け，これらの差について t検定(対応のない)をほどこし，差異を確認した。知識については，情報セキュリティ教育群と未学習群の正答・誤答にクロス集計をほど

こした。情報セキュリティの知識の調査項目を表2.12に示す。

表2.12 情報セキュリティの知識の調査項目

＜物理的対策＞	
14.データを保存するSDカードは，自分のものなので管理する時に特に注意する必要はない。	（外部媒体管理）
15.自分のスマートフォンやゲーム機は，自分のものなので安全な場所で管理する必要はない。	（端末管理）
＜人的対策＞	
16.パスワードが必要なサイトでは，自分のパスワードを仲のよい友達に教えておくほうがよい。	（ID・パスワード管理）
17.懸賞サイトに住所や名前を記入しても問題はない。	（個人情報管理）
18.インターネットで公開されている無料マンガはダウンロードしても安全である。	（ダウンロード）
＜技術的対策＞	
19.ホームページを見るだけで，パソコンがウィルスでおかしくなることがある。	（フィルタリング）
20.ファイアウォールはインターネットからの不正侵入を守ってくれる。	（ファイアウォール）
21.URLの先頭に「https:」のついているWebページは危険である。	（SSL・TSL）
22.スマートフォンにはウィルスがないのでウィルス対策アプリはなくてよい。	（携帯型情報端末対策）
23.ウィルス対策ソフトウェアをいれればＰＣがコンピュータウィルスに感染しない。	（PC対策）
24.技術的対策パソコンのソフトウェア，スマートフォンのアプリは購入した時のままが安全なので，最新版にする必要はない。	（ソフトウェア更新）
25.ＰＣで書いた作文をＵＳＢメモリに保存するだけでは安全とは言えない。	（データ保護対策）

※()は調査項目

2.4 小学生の学習経験と利用実態の調査結果

(1) 小学校における情報モラルの学習の認識

前述のとおり小学校における情報セキュリティは教科や指導内容が学習指導要領で示されていないため，情報セキュリティの指導は各学校や教師の取組に任されている。

情報セキュリティは，情報モラル教育の内容の1つとして扱われている。情報モラル教育は，2分野5領域の内容をバランスよく指導することが必要である。しかし，「情報セキュリティ」，「法の理解や遵守」の2つの分野にかかわる項目については，学習したと認識している児童が4割程度と他の3つの項目と比較して低い傾向が示された。

この結果は，小学校における情報モラルの教育が「安全への知恵」の分野に関係する指導に偏っていることを示しており，「情報セキュリティ」や「法の理解や遵守」の2つの分野にかかわる学習の指導を充実させていく必要があることが示された。

小学校における情報モラル学習の認識の調査結果を表2.13に示す。

表2.13　情報モラル学習の認識

No.	選択項目	回答数	割合(%)
1.	インターネットで被害者にならない使い方	110	69.6
2.	インターネットの法律	62	39.2
3.	情報セキュリティ	64	40.5
4.	インターネットで加害者にならない使い方	86	54.4
5.	インターネットを適切に使う方法	142	89.9
6.	学校では勉強したことがない	5	3.2

(N=158)

(2) 利用端末

小学生の利用端末の調査結果を表2.14に示す。ゲーム機の利用が84.2%ともっとも多く，次いで自分専用のスマートフォンとなっている。2020年度より小・中学校においては一人一台端末の整備が進み，調査対象の学校でも一人一台端末が児童・生徒に用意されている。しかし，学校用のタブレットの利用は37.3%であった。この結果から小学生のインターネット接続のための端末は，ゲーム機やスマートフォン等の自分専用の携帯型情報端末が中心であることが示された。ゲーム機やスマートフォンは，各端末にペアレントコントロール等のフィルタリング設定がかけられるため，コンピュータと技術的対策に違いがある。小学生を対象とした情報セキュリティ教育は，携帯型情報端末の利用を想定する必要があることが示された。

表2.14　小学生の利用端末

No.	選択項目	回答数	割合(%)
1.	家族共用のスマートフォン	49	31.0
2.	自分専用のスマートフォン	87	55.1
3.	ゲーム機	133	84.2
4.	学校のタブレット PC	59	37.3
5.	個人のタブレット PC	42	26.6
6.	家族共用の PC	56	35.4
7.	自分専用の PC	13	8.2
8.	個人の PC	7	4.4

(N=158)

(3) 利用サービス

小学生の利用サービスの調査結果を表2.15に示す。

50%以上の利用サービスは，動画視聴が89.2%，インターネット検索が72.8%，オンラインゲームが72.2%，音楽が65.2%，学校の勉強が53.8%，LINEが53.2%という結果となった。他の利用サービスは30%以下という結果であった。特に動画視聴，インターネット検索，オンラインゲームに関しては，70%を超えているため，この3つのサービスに関する情報セキュリティ教育が必要であることが示された。

表2.15　利用サービス

No.	選択項目	回答数	割合(%)
1.	学校の勉強	85	53.8
2.	通信講座やインターネットの勉強	24	15.2
3.	インターネット検索	115	72.8
4.	読書	35	22.2
5.	懸賞応募	6	3.8
6.	音楽	103	65.2
7.	動画	141	89.2
8.	ゲーム	114	72.2
9.	買い物	21	13.3
10.	フリマ	11	7.0
11.	電子メール	34	21.5
12.	Line	84	53.2
13.	Face Book	14	8.9
14.	Twitter	30	19.0
15.	その他	5	3.2

(N=158)

(4) インターネットの利用時間

小学生のインターネット利用時間の調査結果を表2.16に示す。

表2.16　小学生のインターネット利用時間

		平日		休日	
No.	時間	回答数	割合(%)	回答数	割合(%)
1.	使っていない	5	3.2	4	2.5
2.	1 時間未満	38	24.0	15	9.5
3.	1～2 時間	44	27.8	24	15.2
4.	2～3 時間	36	22.8	35	22.2
5.	3～4 時間	18	11.4	23	14.6
6.	4～5 時間	9	5.7	18	11.4
7.	5 時間以上	8	5.1	39	24.7

(N=158)

小学生の平日のインターネットの利用時間は，50.6%の児童が1時間～3時間利用している結果であった。休日については，利用時間が平日より増加しており，5時間以上利用している児童が24.7%という結果となった。インターネットの利用時間が長くなると個人情報などのデータが外部へ漏洩するなどの危険性も高まってくる。現在の小学生の利用時間を踏まえると小学校における情報セキュリティ教育の必要性が示されたと考えられる。

(5) 小学生の情報セキュリティ教育経験とインターネットの利用実態に関する整理

利用実態の調査結果を以下に示す。

1. 小学校における情報モラル教育は，5つの分野の中の１つである「安全への知恵」の分野が中心であり，「情報セキュリティ」や「法の理解と遵守」の2つの分野についての学習を認識している児童が少ない。
2. 小学生のインターネット接続のための端末は，ゲーム機やスマートフォン等の自分専用のモバイル端末である。
3. 小学生の利用サービスは，動画視聴，インターネット検索，オンラインゲームが多く，70%を超えている。
4. 小学生の平日のインターネットの利用時間は，50.6%の児童が1時間～3時間利用しており，休日については，5時間以上利用している児童が24.7%いる。

小学生は，動画視聴，インターネット検索，オンラインゲームなどインターネットを介したサービスを自分専用のモバイル端末を使って利用しており，生活にかかせないものとなっている。しかし，情報セキュリティ教育を受けたと認識している児童は少ない。この利用実態をふまえて小学校における情報セキュリティ教育の内容を検討していく必要があると考える。なお，実態調査の結果は，内閣府の「青少年のインターネット利用環境実態調査」と重なるものであったことを追記する。

2.5 小学校修了段階における情報セキュリティへの意識

情報セキュリティの意識の調査結果を表2.17に示す。

物理的対策については，調査項目6「外部媒体管理」は，平均3.91，調査項目7「端末管理」は，平均3.97であった。

人的対策については，調査項目8「ID・パスワード管理」は，平均3.97，調査項目9「個人情報管理」は，平均3.89， 調査項目10「ダウンロード」は，平均3.82であった。

技術的対策については，調査項目11「フィルタリング」は，平均3.65，調査項目12「ウィルス対策」は，平均3.65，調査項目13「ソフトウェア更新」は平均3.82であった。

この結果から，特別な教科「道徳」で学習する基本的な生活習慣とかかわりの深い物

理的対策と文部科学省が示す「情報モラル指導モデルカリキュラム表」，「情報活用能力体系表列」で小学校の中学年と高学年の指導目標に対して，インターネット特有の対策である技術的対策の意識に課題があることが確認された。

表2.17 情報セキュリティの意識

No.	調査項目	平均	S.D.
＜物理的対策＞			
6.	外部媒体管理	3.91	0.40
7.	端末管理	3.97	0.18
＜人的対策＞			
8.	ID・パスワード	3.97	0.18
9.	個人情報	3.89	0.49
10.	ダウンロード	3.82	0.50
＜技術的対策＞			
11.	安全の仕組	3.65	0.64
12.	ウィルス対策	3.61	0.74
13.	ソフトウェア更新	3.49	0.79

(*N*=158)

2.6 小学校修了段階における情報セキュリティの知識

情報セキュリティの知識の調査結果を表2.18に示す。

物理的対策の正答率は，調査項目14「外部媒体管理」が87.3%，調査項目15「端末管理が88.6%であり，2つの項目ともに80%を上回る結果となった。

表2.18 情報セキュリティの知識

No.	調査項目	正答(%)	誤答(%)	意味がわからない(%)
＜物理的対策＞				
14.	外部媒体管理	87.3	7.6	5.1
15.	端末管理	88.6	8.2	3.2
＜人的対策＞				
16.	ID とパスワード	90.5	3.8	5.7
17.	個人情報	87.3	5.1	7.6
18.	ダウンロード	65.8	8.9	25.3
＜技術的対策＞				
19.	フィルタリング	39.2	18.4	42.4
20.	ファイアウォール	16.5	12.0	71.5
21.	SSL/TSL	20.9	9.5	69.6
22.	携帯型情報端末対策	85.4	3.2	11.4
23.	PC 対策	51.3	11.4	37.3
24.	ソフトウェア更新	61.4	7.0	31.6
25.	データ保護対策	27.8	17.7	54.4

(*N*=158)

人的対策の正答率は，調査項目16「ID・パスワード」が90.5%，調査項目17「個人情報管理」が87.3%であり，2つの項目が80%を上回る結果となった。しかし，調査項目18「ダウンロード」は65.8%で，80%を下回っており，人的対策の内容によって知識の正答率に差があることが示された。

技術的対策については，調査項目22「携帯型情報端末対策」が，80%を上回ったのみであった。

情報セキュリティ対策の技術的な仕組みに関する3つの項目については,調査項目20「ファイアウォール」が16.5%，調査項目21「SSL/TSL」が20.9%， 調査項目22「データ保護対策」が27.8%であった。この原因として，主に中学校で学習する内容のため，既存の知識が不足しており，正答率が低い結果となったと推測される。

しかし，第一章で前述した小学校で学ぶことが推奨されている内容に関連する3つの項目についても，調査項目19「フィルタリング」が39.2%，調査項目23「PC対策」が51.3%，調査項目24「ソフトウェア更新」が61.4%であることから，現在の小学校における情報セキュリティ教育に課題があることが推測される。

これらの結果を整理すると情報セキュリティの知識については，物理的対策と人的対策の知識はある程度身に付いているが，技術的対策についての知識には課題があることが示された。

2.7 技術的対策の意識と知識による差異

「2.5 小学校修了段階における情報セキュリティへの意識」において前述したとおり，情報セキュリティの意識は，物理的対策，人的対策と比較して，技術的対策の意識に課題があることが確認された。

そこで，技術的対策の意識に関する調査項目3問の平均3.55と比較し，意識の高い児童(104名)と意識の低い児童(54名)に分類し，知識の調査項目について，正答を1点，誤答を0点として12個の合計点を算出し，比較をおこなった。意識の高い児童の平均は7.49，意識の低い児童の平均は6.70であった。技術的意識と知識に関して t 検定(対応あり)をおこなった結果，有意差が確認された($t(157)=2.17$, $p<.05$)。この結果から，技術的対策の意識の高い児童は，情報セキュリティの知識が高いことが確認された。「技術的対策の意識と知識の関係」について調査結果を表2.19に示す。

表2.19 技術的対策の意識と知識の関係

	意識の高い児童 (N=104)		意識の低い児童 (N=54)		
項目	平均	S.D.	平均	S.D.	検定
情報セキュリティの知識	7.49	2.19	6.70	2.12	*

*：$p<.05$

図 2.2 に「意識の高い対策についての情報セキュリティ学習の効果」を示す。意識の高い「物理的対策」，「人的対策」については，情報セキュリティの学習をすることで，知識を習得し，情報セキュリティを確保する行動の変容につながっていくと考えられる。

また，情報セキュリティの意識の低い「技術的対策」については，情報セキュリティの学習をすることにより知識を習得し，意識が高まり，情報セキュリティを確保する行動の変容につながっていくと考えられる。図 2.3 に「意識の低い対策についての情報セキュリティ学習の効果」を示す。

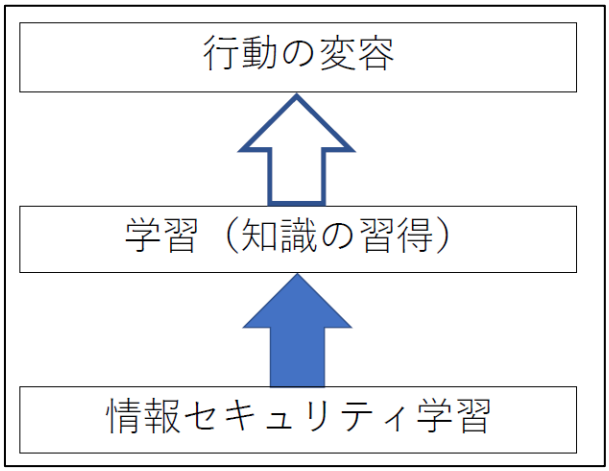


図 2.2 「意識の高い対策についての情報セキュリティ学習の効果」

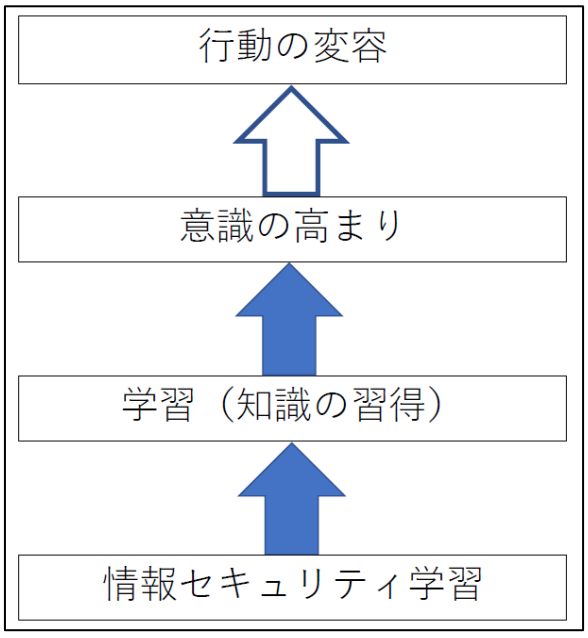


図 2.3 「意識の低い対策についての情報セキュリティ学習の効果」

2.8 おわりに

本調査において以下の5つのことが示された。

1. 小学生のインターネットの利用は平日・休日に関わらず生活にかかせないものとなっており，インターネットを安全に使う意識や知識が必要になっている。
2. 小学校での情報セキュリティ教育を経験したと認識している児童は40%程度である。
3. 情報セキュリティの意識については，物理的対策，人的対策と比較して，インターネット特有の対策である技術的対策の意識に課題がある。
4. 情報セキュリティの知識については，物理的対策と人的対策の知識はある程度身に付いているが，技術的対策についての知識には課題がある。
5. 情報セキュリティの意識と知識は密接に関係しており，意識の高い対策については，情報セキュリティの学習をすることで知識を習得し，情報セキュリティの意識の低い対策については，情報セキュリティの学習により知識を習得することで，意識が高まり，行動の変容につながっていくと考えられる。

情報セキュリティ教育は，インターネットを日々の生活で活用している小学生に欠かせないものである。令和2年度より小学校から始まっている学習指導要領では，情報セキュリティを確保する能力を国民の素養ととらえ，小中高等学校において体系的な学習目標を示している。しかし，小学校においては，指導すべき教科が定められていないことに加え，具体的な指導内容が示されていないため，小学校修了段階において，情報セキュリティの意識と知識に課題があることがわかった。

第3章1節では，本調査で得られた小学校修了段階の情報セキュリティに関する知見を踏まえ，文部科学省が示す小学校における情報セキュリティの体系的な位置づけを踏まえた具体的な学習内容を明確にし，具体的な教材や指導過程を示していく。

第3節　中学校修了段階の実態

3.1 はじめに

2021年度より全面実施される「中学校学習指導要領(平成29年告示)」[102]では，教育内容改訂の重要事項の1つとして，「情報の活用，情報モラルなどの情報教育の充実」が示された。文部科学省は，情報セキュリティに関する指導を情報モラルの5領域の1つとして位置づけ，初等・中等教育を5つの発達段階に分け指導目標を定めている。情報セキュリティ教育は，技術・家庭科(技術分野)で情報モラル教育の中で指導されている。しかし，技術・家庭科(技術分野)での情報セキュリティ教育に関わる配当時間数や教材を調べたところ，3年間で1時間程度の指導時間であるという結果[103]であり，中学校修了段階で必要な情報セキュリティの知識や対応力が身に付いているかを把握する必要がある。

文部科学省が中学校3年生を対象にした毎年5月に実施している「全国学力・学習状況調査の質問紙調査」[104]によると，平成24年～平成30年の7年間の報告でインターネットを長時間利用すると学力に影響があることが報告されている。また，15歳児を対象にした「Key Features of OECD Program for International Student Assessment 2018 (PISA2018)」[105]によると，“学校外でのインターネットの利用時間が4時間以上になると，読解力，数学的リテラシー，科学的リテラシーの3分野ともに平均得点が低下する。”と報告されている。これらのことを踏まえるとインターネットの長時間の利用は学力に影響を及ぼすことが分かる。2018年に安心ネットづくり促進協議会が発表した中学生を対象にした情報モラルに関する調査では，情報セキュリティに関する2項目で，「セキュリティソフトウェアの知識」の正答率が，78.4%，「ウィルス対策の理解」の正答率が，84.3%であった。いずれの先行調査や先行研究も調査時期が中学校の修了段階に限定されていないため，中学校の学習で身に付けた最終的な情報セキュリティの意識と知識を把握することができない。また，調査内容が，情報モラルの調査の一部としておこなわれているため，物理的対策，人的対策，技術的対策の3つの対策の側面から情報セキュリティの意識や知識をとらえるものになっていない。

そこで，中学校3年生3月にインターネットの利用実態，情報セキュリティの意識，知識を調査し，中学校での情報セキュリティ教育の現状を把握することとした。

第3節では，中学3年の卒業直前に情報セキュリティに関する実態調査により，インターネットの利用実態，情報セキュリティの意識，知識を把握し，中学校修了段階での情報セキュリティ教育の現状と課題を明らかにすることとした。

3.2 調査の対象と方法

(1) 調査の目的

中学3年の卒業直前にインターネットの利用実態，情報セキュリティの意識と知識の実態調査をおこない，中学校修了段階で身に付けている情報セキュリティの意識と知識を把握することにより，中学校での情報セキュリティ教育の現状と課題を明らかにする。

(2) 期日

2018年3月に実施した。

(3) 対象

2018年3月に卒業直前のA県内の公立中学校7校，中学3年生795名を調査対象とした。

(4) 調査方法

調査は，技術・家庭科(技術分野)の中学3年の授業の中でマークシートにより30分配当し，実施した。

(5) 調査項目および分析方法

調査項目は，第1節の小・中学校に勤務する教員の実態調査で明らかにした情報セキュリティの意識，知識，行動の調査項目を基に作成した。また，中学校の技術・家庭科(技術分野)で学習する情報セキュリティ教育内容から知識と対応策に関する内容を抽出した。調査は，各設問に対して，適切な選択項目を選ぶようにした。「利用実態と意識」の調査項目と選択項目を表2.20に示す。

表2.20 「利用実態と意識」の調査項目と選択項目

1. あなたのスマートフォンやゲーム機などのモバイル端末を使ったインターネットの1日の利用時間についてお答えください。 (携帯型情報端末の利用時間) a.使っていない　b.1時間未満　c.1～2時間　d.2～3時間 e.3～4時間　f.4～5時間　g.5時間以上
2. あなたのパソコンを使ったインターネットの1日の利用時間についてお答えください。 (パソコンの利用時間) a.使っていない　b.1時間未満　c.1～2時間　d.2～3時間 e.3～4時間　f.4～5時間　g.5時間以上
3. あなたが，インターネットで利用しているものをお答えください。(複数回答可) (利用しているサービス) a.電子メール　b.SNS(Facebook・Twitter など)　c.コミュニケーションアプリ d.検索　e.ゲーム　e.音楽鑑賞　f.動画視聴　g.ショッピング　h.その他
4. あなたが，インターネットの安全な使い方を学んだ機会についてお答えください。(複数回答可) (学習の機会) a. 技術・家庭科(技術分野)の授業　b. 技術・家庭科(技術分野)以外の授業　c.学校の集会 d.学校以外の研修会等　e.保護者　f.販売店　g.知人　h.自分で調べた i.学んだことはない　j.その他
5. あなたは，利用時間や使い方など，適切にインターネットを利用できていますか。 (インターネットの適切な利用の意識) a.できていると思う　b.どちらかと言うとできていると思う c.どちらかというとできていない　d.できていない

※()は調査項目

「情報セキュリティの知識」の調査項目と選択項目を表2.21に示す。

表2.21 「情報セキュリティの知識」の調査項目と選択肢

＜1. 不正侵入を防ぐ技術＞

a01. コンピュータウィルスのネット上の感染経路の説明として，最も適切なものはどれか。（リンクの対応）

ア．ネットを通じていても友人から受け取っているのなら感染しない
イ．ホームページを見ただけでウィルス感染することもある(※正答)
ウ．PCではウィルスが多く出回っているが，スマートフォンのウィルスはない
エ．言葉や内容の意味がわからない

a02. ファイアウォールの役割として最も適切なものはどれか。（ファイアウォール）

ア．外部のネットワークからの不正な侵入を防ぐ(※正答)
イ．データの破損を防ぐ
ウ．個人情報を守る
エ．言葉や内容の意味がわからない

a03. スマートフォンで使用するアプリの説明の中には，個人情報を登録するアプリもある。この説明として，最も適切なものはどれか。（アカウント管理）

ア．ダウンロードする前にアクセス許可設定などを確認したほうが良い(※正答)
イ．無料でも役に立つアプリが多いので，すべて利用して問題ない
ウ．アプリマーケット上のアプリは信頼性･安全性は高いので安心して良い
エ．言葉や内容の意味がわからない

＜2. コンピュータウィルスに対する技術＞

a04. コンピュータウィルスからＰＣを守る対策として最も適切なものはどれか。（ソフトウェア更新）

ア．ウィルス対策ソフトウェアを入れる
イ．特に対策をする必要はない，
ウ．ウィルス対策ソフトウェアを入れ，ソフトウェアやＯＳを最新の状態に更新する(※正答)
エ．言葉や内容の意味がわからない

a05. スマートフォンのセキュリティ対策ソフトウェアを利用することで，対応できることはどれか。（セキュリティ対策ソフトウェア）

ア．不正なアプリの監視(正答)
イ．アプリの新規インストールの禁止
ウ．Wi-Fiを利用したインターネット接続の禁止
エ．言葉や内容の意味がわからない

＜3. データの故障や安全に関する技術＞

a06. 自分で作成したデータをＵＳＢメモリに保存する時，安全対策としてやるべきものとして最も適切なものはどれか。（バックアップ）

ア．暗号化する
イ．暗号化し，バックアップをとる(※正答)
ウ．特に対策する必要はない
エ．言葉や内容の意味がわからない

＜4.違法・有害情報に関する技術＞

a07. 携帯ゲーム機を利用する際に気を付けることとして，最も適切なものはどれか。（フィルタリング）

ア．携帯ゲーム機であれば個人情報がネットに流れる心配はない
イ．携帯ゲーム機でネット接続する時はフィルタリングを設定するべきである(※正答)
ウ．携帯ゲーム機のネットワークは子供用に設計されているので安全である
エ．言葉や内容の意味がわからない

＜5. ID・パスワード管理＞

a08. インターネット上で自分の IDとパスワードを他人に教えるだけで簡単にお金がもらえる方法があると友人から聞いた。次の中で適切なものはどれか。（ID・パスワード）

ア．もらえる金額が高額であれば，やってみてもいい
イ．もらえる金額が少額であれば，問題はない
ウ．いくらお金がもらえるとはいえ，他人に IDやパスワードを教えてはいけない(※正答)
エ．言葉や内容の意味がわからない

※()は調査項目

調査内容を作成するにあたり2012年に総務省総合通信基盤局総務省情報通信政策研究所が作成した「青少年のインターネット・リテラシー指標(ILAS)」[106]を参考にした。調査内容は，「利用実態と意識」，「情報セキュリティの知識」の2つの内容についておこなった。

第2節と同様に「利用実態」は，「モバイル端末の利用時間」，「パソコンの利用時間」，「学習の機会」，「利用しているサービス」，について4つの項目について調査をおこなった。調査項目は第１節の小・中学校教員の調査項目で明らかにした課題を基に作成した。「携帯型情報端末の利用時間」，「パソコンの利用時間」，「学習の機会」，「利用しているサービス」，「インターネットの適切な利用の意識」については，各項目を集計し，その割合を比較した。

「適切な利用の意識」については，情報セキュリティの視点から自分の行動を振り返るものとし，「とてもそうおもう」を4点，「どちらかというとそうおもう」を3点，「どちらかというとできていないとおもう」を2点，「できていないとおもう」を１点と見なし得点化し，平均と標準偏差を求めた。

情報セキュリティの知識の設問は，情報セキュリティの教員の知識の調査の問題を基に「1.不正侵入を防ぐ技術(1)～(3)」，「2.コンピュータウィルスに対する技術(1)(2)」，「3.データの故障や障害に関する技術」，「4.違法・有害情報に関する技術」，「5. ID・パスワード管理」の5つの調査項目，計8問を作成した。

設問は，中学校で利用されている中学校の技術・家庭科（技術分野）の3社の教科書で共通して取り上げている内容とした。

3.3 中学生の利用実態

(1) 利用時間

携帯型情報端末とパソコンとインターネットの1日の利用時間を表2.23に示す。

表2.23　インターネットの利用時間

		携帯型情報端末		パソコン	
No.	時間	回答数	割合(%)	回答数	割合(%)
1.	使っていない	54	6.8	573	72.1
2.	1時間未満	235	29.5	150	18.8
3.	1～2時間	224	28.2	30	3.8
4.	2～3時間	129	16.2	15	1.9
5.	3～4時間	79	9.9	11	1.4
6.	4～5時間	32	4.0	4	0.5
7.	5時間以上	38	4.8	7	0.9

(N=795)

パソコンでインターネットを利用している生徒は，30%以下，携帯型情報端末では90%以上である。前節で調査した小学校修了段階と比較すると中学校修了段階の利用時間は増えている。この結果から中学生の大半は，何らかの形でインターネットを利用していることが示された。また，90%以上がスマートフォンなどの携帯型情報端末を利用してインターネットを利用しているため，携帯型情報端末の利用を踏まえた情報セキュリティ教育が必要であることが示された。本調査の結果は，内閣府の「青少年のインターネット利用環境実態調査」と同様であることを追記しておく。

(2) 利用しているサービス

インターネットで利用しているサービスを表2.24に示す。

表2.24　インターネットで利用している利用サービス

No.	調査項目	回答数	割合(%)
1.	電子メール	181	22.8
2.	SNS	204	25.7
3.	メッセンジャーアプリ	535	67.3
4.	インターネット検索	495	62.3
5.	ゲーム	477	60.0
6.	音楽鑑賞	495	62.3
7.	動画視聴	419	52.7
8.	ショッピング	172	21.6
9.	その他	23	2.9

(N=795)

調査項目 3「メッセンジャーアプリ」，調査項目 4「インターネット検索」，調査項目 5「ゲーム」，調査項目 6「音楽鑑賞」については，60%以上，動画視聴は 50%以上の生徒が，利用していることが示された。また，コミュニケーションのひとつの手段である調査項目 1「電子メール」については，22.8%であった。この結果から，メッセンジャーアプリ，インターネット検索，音楽鑑賞，ゲーム，動画視聴など中学生の実態を踏まえた情報セキュリティ教育が必要であることが示された。総務省は，SNS を「限られたユーザーだけが参加できる Web サイトの会員制サービス」と定義している。本調査における SNS とは，登録したユーザーが，インターネット上で誰でも閲覧可能なものに限ったものである。

(3) 情報セキュリティを含む情報モラルの学習機会の認識

情報セキュリティを含む情報モラルの学習機会の認識の調査結果を表2.25に示す。

選択項目3「学校の集会」が64.0%で，続いて，選択項目1「技術・家庭科(技術分野)の

授業」となっている。選択項目2「技術・家庭科(技術分野)以外の授業」で学習したと認識している生徒はわずか12.5%であった。

学校の集会(特別活動)でおこなわれる内容は，各学校の課題を踏まえた「安全への知恵」が中心となることが多い。また，情報セキュリティ教育は，技術・家庭科(技術分野)で教科の指導内容となっているためこのような結果が示されたと推測される。

表2.25　情報セキュリティを含む情報モラルの学習機会の認識

No.	選択項目	回答数	割合(%)
1.	技術・家庭科(技術分野)の授業	413	51.9
2.	技術・家庭科(技術分野)以外の授業	99	12.5
3.	学校の集会	509	64.0
4.	学校以外の研修会	6	0.8
5.	保護者	114	14.3
6.	販売店	49	6.2
7.	友人	34	4.3
8.	自分で調べた	48	6.0
9.	学んだことはない	26	3.3
10.	その他	18	2.3

(N=795)

3.4 適切な利用の意識

適切な利用の意識の調査結果を表2.26に示す。「できている」30.8%，「どちらかというとできている」44.7%と適切な利用に関して肯定的な回答は，75.5%であった。

2021年に発表された「青少年のネット利用実態把握を目的とした調査令和元年度最終報告書」[107] によると「インターネットの安全な利用」に関して肯定的な回答をした中学生は90%と報告されている。その結果と比較すると本調査の対象生徒は，適切な利用意識が低い傾向があることが示された。この報告は実施期間が9〜10月であり，学年が定められていない調査のため，本調査との差がでたものと考えられる。

表2.26　適切な利用の意識の割合

No.	選択項目	回答数	割合(%)
1 .	できている	245	30.8
2 .	どちらかというとできている	355	44.7
3 .	どちらかとういとできていない	159	20.0
4 .	できていない	28	3.5

(N=795)

3.5　情報セキュリティの知識

情報セキュリティの知識に関する調査の結果を表2.27に示す。7つの調査の中で正答率

が，80%を超えた調査項目は，選択項目a03「アカウント管理」，選択項目a05「セキュリティ対策ソフトウェア」，選択項目a08「ID・パスワード」の3つであった。

また，正答率が，80%を下回った調査項目は，調査項目a01「リンクの対応」，調査項目a02「ファイアウォール」，調査項目a04「ソフトウェア更新」，調査項目a06「バックアップ」，調査項目a07「フィルタリング」であった。特に，調査項目a02「ファイアウォール」は，正答率が36.4%と他の調査項目と比較して低く「技術・家庭科（技術分野）」の学習で課題があることが示された。

表2.27　項目別の知識の正答率

No.	調査項目	正答率(%)	誤答率(%)
＜1.不正侵入を防ぐ技術＞			
a01.	リンクの対応	68.2	31.8
a02.	ファイアウォール	36.4	63.6
a03.	アカウント管理	84.2	15.8
＜2.コンピュータウィルスに対する技術＞			
a04.	ソフトウェア更新	68.2	31.8
a05.	セキュリティ対策ソフトウェア	81.4	18.6
＜3.データの故障や障害に関する技術＞			
a06.	バックアップ	60.3	38.7
＜4.違法・有害情報に関する技術＞			
a07.	フィルタリング	79.6	23.1
＜5.ID・パスワード管理＞			
a08.	ID・パスワード	87.7	12.3

（N=795）

3.6 技術・家庭科(技術分野)での情報セキュリティ教育効果

前述のとおり中学校における情報セキュリティ教育は，技術・家庭科（技術分野）での学習が中核となっている。そこで，技術の授業で学習した認識のない生徒（382名）と学習した認識がある生徒（413名）を分類し，知識の調査項目について，正答を1点，誤答を0点とし8問の合計点を算出し比較をおこなった。

学習した認識のない生徒の平均は5.48，学習した認識のある生徒の平均は6.18であった。技術の授業で学習経験の有無と知識得点に関して t 検定（対応なし）をおこなった結果，有意差が確認された（$t(793)=5.08$，$p<.01$）。

この結果から，情報セキュリティの知識が高い生徒は，技術の授業で学習した認識のある生徒であることが，確認された。

このことから，中学校において，情報セキュリティの知識を高めていくには技術・家庭科（技術分野）における情報セキュリティの授業を充実させることが必要であると考えられる。

技術・家庭科（技術分野）での情報セキュリティ教育の効果の結果を表2.28に示す。

表2.28　技術・家庭科(技術分野)での情報セキュリティ教育の効果

	認識なし(N=382)		認識あり(N=413)		
調査項目	平均	S.D.	平均	S.D.	検定
技術・家庭科(技術分野)の学習経験	5.48	2.11	6.18	1.80	**

**：$p<.01$（$N=795$）

3.7 おわりに

中学校修了段階の実態を調査して，以下のことが示された。

1. 中学生に対しては，携帯型情報端末の利用を踏まえた情報セキュリティ教育が必要である。
2. メッセンジャーアプリ，インターネット検索，音楽鑑賞，ゲーム，動画視聴など中学生の実態を踏まえた情報セキュリティ教育が必要である。
3. 情報セキュリティを含む情報モラルの学習機会は，「学校の集会」と「技術・家庭科(技術分野)の授業」が中心であり，「技術・家庭科(技術分野)以外の授業」の学習経験はわずか12.5%である。
4. 調査対象者の75.5%が，インターネットの適切な利用に対して肯定的に回答している。
5. 「アカウント管理」，「セキュリティ対策ソフトウェア」，「ID・パスワード」など人的対策の知識はある程度もちあわせているが，技術的対策の知識である「ファイアウォール」に課題がある。このことは，「技術・家庭科（技術分野）」の指導に改善の余地があることを示している。
6. 「技術・家庭科（技術分野）」の情報セキュリティの授業を充実させることが，中学校において情報セキュリティ教育を充実させていくうえで重要である。

中学校修了段階では，小学校修了段階と比較すると先行研究の結果と同様にインターネットの利用率も高まる。また，小学校には，情報セキュリティを学習内容とする教科はないが，中学校は，「技術・家庭科（技術分野）」の授業で，情報セキュリティについて教科の学習として学ぶことになる。

教員の調査結果から，情報セキュリティの知識を高めることで，情報セキュリティを確保する行動につながる可能性が示されている。中学校では，情報セキュリティの知識を学ぶのは「技術・家庭科（技術分野）」の授業である。

つまり，中学校の情報セキュリティ教育を充実させるためには，「技術・家庭科（技術分野）」の授業において，本調査における知見をふまえた具体的な教材や指導展開を示していくことが必要であると考える。

第3章2節では，本調査で得られた中学校修了段階の情報セキュリティに関する知見を踏まえ，文部科学省が示す中学校における情報セキュリティの体系的な位置づけを踏まえた具体的な学習内容を明確にし，具体的な教材や指導過程を示していく。

２．結言

本章では，小・中学校に勤務する教員の実態調査をおこない，その知見を基に小・中学校修了段階の児童・生徒およびに情報セキュリティに関する実態調査をおこなった。以下に本章で得られた小・中学校修了段階における情報セキュリティ教育についての知見をまとめる。

(1) 小・中学校教員の実態

① 小・中学校に勤務する教員は，学校において情報セキュリティを確保することが大切であると認識している。
② 情報セキュリティを確保するために物理的対策，人的対策，技術的対策をおこなうことの重要性は認識しているものの，実際の行動にむすびついていない傾向がある。
③ 情報セキュリティの知識と行動には，相関関係があると推測され，情報セキュリティの知識を高めることで，情報セキュリティを確保する行動につながる可能性がある。

(2) 小学校修了段階の実態

① 小学生のインターネットの利用は日常的なものとなっており，ゲーム機や個人用のスマートフォンを利用している。
② 小学校で情報セキュリティの学習をしたと認識している児童は，40%程度である。
③ 小学生の情報セキュリティの意識として技術的対策の意識に低い傾向がある。
④ 小学生の情報セキュリティの知識については，物理的対策と人的対策の知識は，ある程度身に付いているが，技術的対策についての知識は不足している。
⑤ 情報セキュリティの意識と知識は密接に関係しており，意識の高い対策については，情報セキュリティの学習をすることで知識を習得し，情報セキュリティの意識の低い対策については，情報セキュリティの学習により知識を習得することで，意識が高まり，行動の変容につながっていくと考えられる。

(3) 中学校修了段階の実態

① 中学生に対しては，携帯型情報端末の利用を踏まえた情報セキュリティ教育が必要である。
② メッセンジャーアプリ，インターネット検索，音楽鑑賞，ゲーム，動画視聴など中学生の実態を踏まえた情報セキュリティ教育が必要である。
③ 情報セキュリティを含む情報モラルを学習したと認識している生徒は，「学校の集会」と「技術・家庭科(技術分野)の授業」が中心であり，「技術・家庭科(技術分野)以外の授業」での機会で学習したと意識している生徒はわずか12.5%である。
④ 調査対象者の75.5%が，インターネットの適切な利用に対して肯定的に回答してい

る。

⑤「アカウント管理」，「セキュリティ対策ソフトウェア」，「ID・パスワード」など人的対策の知識はある程度もちあわせているが，技術的対策の知識である「ファイアウォール」に課題がある。このことは，「技術・家庭科（技術分野）」の指導に改善の余地があることを示している。

⑥「技術・家庭科（技術分野）」の情報セキュリティの授業を充実させることが，中学校において情報セキュリティ教育を充実させていくうえで重要である。

なお，北海道，関東，関西の 7 都道府県の管理職，情報教育担当の指導主事，教諭に本調査結果と勤務する地域との相違について聞き取り調査をおこなった結果，本調査結果と同じ傾向であることが確認された。

これらの実態から見えた課題を解決し，情報セキュリティ教育を充実させるためには，小学校および中学校において，それぞれ違う対策が必要である。

小学校では，特定の免許をもつ教員だけでなく，すべての教員が情報セキュリティ教育を指導することが想定される。そのため，情報セキュリティ教育の内容を明確に示し，すべての教員が，情報セキュリティの指導ができる学習教材や指導過程が必要である。

中学校では，情報セキュリティ教育は，主に技術・家庭科（技術分野）の中で実施されている。技術・家庭科（技術分野）は，学習指導要領において，情報セキュリティの指導内容が示されている。しかし，情報セキュリティについて学習できる時間は限られており，本調査から見えた課題をふまえて効果的で効率的な学習をすることが重要である。情報セキュリティを確保する仕組などの調査からわかった知識や対応策を補填する教材を開発し，その教材の活用方法を示していく必要がある。

第3章では，本章での知見を生かし，小学校および中学校の授業で活用する教材を開発していく。

参考文献

84)文部科学省：学校における教育の情報化の実態等に関する調査結果〔確定値〕（令和元年度），pp.13-15(2019)
85)阪東哲也・掛川淳一・世良啓太・森山 潤:小学生を対象とした情報セキュリティ教育の指導に対する小学校教員の意識調査，日本産業技術教育学会技術教育分科会2020年度研究発表会講演要旨集，pp.13-14(2020)
86)内閣府：令和2年度青少年のインターネット利用環境実態調査報告書(2021)
87)文部科学省：平成31年度(令和元年度) 全国学力・学習状況調査報告書【質問紙調査】，pp.10-49(2020)
88)文部科学省: 第１章 学校における情報セキュリティについて，学びのイノベーション事業実証研究報告書 別冊資料編，pp.1-66(2019)
89)前掲84)，pp.13-15(2019)
90)前掲85)，pp.13-14(2020)
91)安東茂樹 他:情報通信ネットワークと情報セキュリティ，技術・家庭(技術分野)，開隆堂，pp.190-201(2016)
92)田口浩継 他:コンピュータと情報通信ネットワーク，新編新しい技術・家庭(技術分野)，東京書籍，pp196-211(2016)
93)佐竹隆顕 他:ネットワークを支える技術，新技術・家庭技術分野，教育図書，pp.202-217(2016)
94)財団法人全国商業高等学校協会，情報処理検定ビジネス情報部門２級問題，http://www.zensho.or.jp/puf/examination/pastexams/information.html，（2021.8.8最終確認）
95)岡山県総合教育センター，教職員の情報セキュリティ意識を高める校内研修パッケージ，http://www.edu-ctr.pref.okayama.jp/chosa/kiyou/h22/10-06pack/index.html，（2021.8.8最終確認）
96)前掲88)，pp.1-66(2019)
97)前掲86)，(2021)
98)国立教育政策研究所：教育課程研究センター「全国学力・学習状況調査」，https://www.nier.go.jp/kaihatsu/zenkokugakuryoku.html ，（2021.8.8最終確認）
99)安心ネットづくり促進協議会:「青少年と保護者におけるインターネット・リテラシー調査安心協ＩＬＡＳ最終報告書」，pp.6-18(2018)
100)前掲22),pp.6-7(2007)
101)文部科学省：情報活用能力の体系表例，教育の情報化の手引き(令和元年12月)，pp.232-239(2019)
102)前掲28)，p.21(2017)
103)前掲48)，pp.21-22(2019)

104)前掲28), pp.10-49(2020)
105)PISA: Key Features of OECD Program for International Student Assessment 2018 (PISA2018),p.3(2019)
106)総務省:青少年のインターネット・リテラシー指標(ILAS), https://www.soumu.go.jp/use_the_internet_wisely/special/ilas/, (2021.8.8最終確認)
107)LINE株式会社:「青少年のネット利用実態把握を目的とした調査令和元年度最終報告書」, https://line-mirai.org/ja/report/detail/3, (2021.8.8最終確認)

関連論文

1) 小熊良一・山本利一：小・中学校教員の情報セキュリティに関する「意識」「行動」「知識」に関する調査, 教育情報研究 36(1), pp.13-24(2020)

2) Ryoichi Oguma, Toshikazu Yamamoto：Survey on information morals and information security knowledge and responsiveness at the stage of completing compulsory education in Japan, The Proceedings of International Conference on Technology Education in Asia-Pacific Region 2021, pp.146-pp155(2021)

第 3 章　　児童・生徒の情報セキュリティ教材の開発

1. 緒言

小・中学校における情報セキュリティ教育は，第1章で前述したとおり，情報モラル教育の１つの分野として位置付けられている。小学校における情報セキュリティは，指導内容とする教科が決められていないため，各学校や教師の取組にまかされている。中学校における情報セキュリティ教育は，中学校技術・家庭科(技術分野)において，教科の指導内容として示されている。

情報セキュリティ教材については，様々な研究がおこなわれている。藤川ら(2019)[108]は，情報セキュリティ教育における「主体的・対話的で深い学び」の実現を目指してSNSノベルゲームを開発している。また，花田(2019)[109]は，ICT 機器の安全利用を促すための小学校高学年向けのすごろく型のアナログ教材を開発している。いずれの研究も児童の情報セキュリティへの意識を高めるものであるが，第1章で前述したとおり初等中等教育を見通した指導の視点が不足しており，体系的な情報セキュリティ教育の視点から小学校での指導内容を明確にした教材が必要であると考える。石原(2011)[110]は，学校でよく使われる11個の情報モラル教材をプロット型，暗転型，暗転問いかけ型，活用提案型の4つに分類し，情報セキュリティ教材は，暗転型と活用提案型に属するとしている。また，新しい情報社会に対応するためには，子どもたちの情報活用に前向きな姿に導く情報セキュリティの教材が必要であると提案している。豊田(2018)[111]は，インターネットで公開されている情報セキュリティを含む情報モラル教材全体を分析し，授業の位置付けの困難さ，対象年齢の設定の不整合，指導者側の教材内容理解の困難さ，編集・加工・改変性の乏しさ，教室設備への対応の困難さ，注意喚起の内容が主流であること，視聴時間が長い，という7つの課題を挙げている。

これらの先行研究から，情報セキュリティ教育を実施していくためには，指導すべき内容を明確にして効果的な学習ができること，教師の情報セキュリティの知識を補うことをふまえた教材が必要であると考えられる。

第3章では，第1章で前述した小・中学校で学ぶべき情報セキュリティ教育内容，第2章で示した小・中学校の教員および児童・生徒の実態をふまえて，児童・生徒の情報セキュリティを確保しようとする意識，情報セキュリティを確保するために必要な知識を高めるための教材を提案する。

第3章は，「第1節小学校における情報セキュリティ教材」，「第2節中学校における情報セキュリティ教材」の2つの節で構成している。

第1節　小学校における情報セキュリティ教材

1.1 はじめに

文部科学省は，小学校より発達段階に合わせた体系的な情報モラル教育がすすめられるように2007年に「情報モラル指導実践キックオフガイド」[112]の中で，「情報モラル指導モデルカリキュラム表」を発表した。また，2020年に新しい学習指導要領に対応した「教育の情報化の手引き-追補版-」[113]の中で「情報活用能力の体系表例」を発表した。

第１節では，第2章で前述した小学校修了段階の実態と「情報モラル指導実践キックオフガイド」，「教育の情報化の手引き-追補版-」，「小学校学習指導要領(平成29年告示)」[114]をふまえて，小学校における情報セキュリティ教育の具体的な内容を摘出し，小学校における情報セキュリティ教材を開発することとした。

1.2　文部科学省が示す小学校における情報セキュリティの指導内容

2020年より実施されている小学校の教育課程では，教育内容改訂の重要事項の1つとして，情報活用能力の充実が示されている。文部科学省より示された「幼稚園教育要領，小・中学校学習指導要領等の改訂のポイント」には，「その他の重要事項」の1つとして，情報活用能力(プログラミング教育を含む)が示されている。具体的には，「コンピュータ等を活用した学習活動の充実(各教科等)」，「コンピュータでの文字入力等の習得，プログラミング的思考の育成(小：総則，各教科等(算数，理科，総合的な学習の時間など)」の2つが示されている。情報セキュリティ教育は，「コンピュータ等を活用した学習活動の充実」に含まれる。

1.3 小学校における情報セキュリティの指導事項

小学校における情報セキュリティの指導事項を具体的に示すものとして，第1章で前述した「情報モラル指導モデルカリキュラム表」および「情報活用能力の体系表例」がある。

「情報モラル指導モデルカリキュラム表」，「情報活用能力の体系表例」を整理すると，小学校低学年では「情報の大切さ」，小学校中学年では，「情報を守ることの大切さ」を学ぶ。小学校高学年では，情報セキュリティの基本と生活の中で必要な基本的な情報セキュリティ対策を学ぶことになる。

「小学校学習指導要領(平成29年告示)」には，情報セキュリティに関する記載はない。しかし，「小学校学習指導要領(平成29年告示)解説 総則編」[115]には，情報セキュリティについて，各教科の学びを支える情報活用能力の１つとして記載されている。各教科等の解説では，「小学校学習指導要領(平成29年告示)解説 社会編」[116]において小学校5年「情報化と産業のかかわり」で，大量の情報や情報通信技術の活用を扱っている。また，「小学校学習指導要領(平成29年告示)解説 特別の教科 道徳編」[117]においても，情

報モラルを扱っている。しかし，2つの教科ともに情報セキュリティについての内容は扱っていない。

「情報モラル指導モデルカリキュラム表」，「情報活用能力の体系表例」の情報セキュリティに関する小学校に関連する記載事項を表3.1に示す。

表3.1　小学校における情報セキュリティの指導事項

情報モラル指導モデルカリキュラム表 ◎大目標　○中目標　・小目標	情報活用能力の体系表例
＜低学年＞	
記載なし	A 知識および技能 ・人の作った物を大切にすることや他者に伝えてはいけない情報があること ・コンピュータなどを利用するときの基本的なルール
＜中学年＞	
◎生活の中で必要となる情報セキュリティの基本を知る ○認証の重要性を理解し，正しく利用できる ・パスワードは誰にも教えない ・自分の使った端末をそのまま放置しない	A 知識および技能 ・自分の情報や他人の情報の大切さ ・生活の中で必要となる基本的な情報セキュリティ
＜高学年＞	
◎生活の中で必要となる情報セキュリティの基本を知る ○不正使用や不正アクセスされないように利用できる ・パスワードは自分で管理しなければならないことを理解する ・どのようにして個人情報が漏れていくかを知る ◎情報セキュリティの確保のために，対策・対応がとれる ○情報の破壊や流出を防ぐ方法を知る ・ウィルスに対する簡単な知識を知る ・自分の端末は人に貸さない ・ダウンロードには危険が伴うものがあることを知る	A 知識および技能 ・情報に関する自分や他者の権利 ・情報を守るための方法 ・情報技術の悪用に関する危険 C 学びに向かう力，表現力等 ・生活の中で必要となる情報セキュリティについてふまえ，行動しようとする

1.4 小学校における指導内容

小学校における情報セキュリティ教育の指導内容は，「情報モラル指導モデルカリキュラム表」，「情報活用能力の体系表例」と第2章第2節の調査結果をもとに摘出した。

「A.情報セキュリティの概要」，「B.情報セキュリティを確保する基本的な方法」の2つの項目と具体的な指導内容を10個摘出した。

「A.情報セキュリティの概要」は，身近にある情報の価値と情報セキュリティの三大要素である機密性・完全性・可用性をふまえた情報セキュリティの原則である。指導内容は，「A1.情報セキュリティの原則」「A2.身近にある情報」「A3.インターネットにおける情報」の3個である。

「B.情報セキュリティを確保する基本的な方法」は，情報セキュリティを確保する対策を物理的対策，人的対策，技術的対策の3つの側面から整理したものである。指導内容は，物理的対策として「B1.情報端末・外部媒体の管理」，人的対策として「B2.個人情報管理」「B3.ID・パスワード管理」「B4.ダウンロード」の3個，技術的対策として「B

5.フィルタリング」「B6.ウィルス対策ソフトウェア」「B7.ソフトウェア更新」の3個である。表3.2に小学校における指導内容を示す。

表3.2　小学校における指導内容

情報モラル指導モデルカリキュラム表 ◎大目標○中目標・小目標	情報活用能力の体系表例	摘出した小学校における指導内容
＜低学年＞ 記載なし	＜知識および技能＞ ・人の作った物を大切にすることや他者に伝えてはいけない情報があること ・コンピュータなどを利用するときの基本的なルール	A. 情報セキュリティの概要 A1.情報セキュリティの原則 A2.身近にある情報 A3.インターネットにおける情報 B.情報セキュリティを確保する基本的な方法 ○物理的対策 B1.情報端末・外部媒体の管理
＜中学年＞ ◎生活の中で必要となる情報セキュリティの基本を知る ○認証の重要性を理解し，正しく利用できる ・パスワードは誰にも教えない ・自分の使った端末をそのまま放置しない	＜知識および技能＞ ・自分の情報や他人の情報の大切さ ・生活の中で必要となる基本的な情報セキュリティ	A.情報セキュリティの概要 A1.情報セキュリティの原則 A2.身近にある情報 A3.インターネットにおける情報 B.情報セキュリティを確保する基本的な方法 ○物理的対策 B1.情報端末・外部媒体の管理 ○人的対策 B2.個人情報管理 B3.ID・パスワード管理
＜高学年＞ ◎生活の中で必要となる情報セキュリティの基本を知る ○不正使用や不正アクセスされないように利用できる ・パスワードは自分で管理しなければならないことを理解する ・どのようにして個人情報が漏れていくかを知る ◎情報セキュリティの確保のために，対策・対応がとれる ○情報の破壊や流出を防ぐ方法を知る ・ウィルスに対する簡単な知識を知る ・自分の端末は人に貸さない ・ダウンロードには危険が伴うものがあることを知る	＜知識および技能＞ ・情報に関する自分や他者の権利 ・情報を守るための方法 ・情報技術の悪用に関する危険 ＜学びに向かう力，表現力等＞ ・生活の中で必要となる情報セキュリティについてふまえ，行動しようとする	A.情報セキュリティの概要 A1.情報セキュリティの原則 A2.身近にある情報 A3.インターネットにおける情報 B.情報セキュリティを確保する基本的な方法 ○物理的対策 B1.情報端末・外部媒体の管理 ○人的対策 B2.個人情報管理 B3.ID・パスワード管理 B4.ダウンロード ○技術的対策 B5.フィルタリング B6.ウィルス対策ソフトウェア B7.ソフトウェア更新

低学年では，情報セキュリティの概念として，情報セキュリティの原則，身近にある情報を学ぶ。情報セキュリティを確保する基本的な方法として，情報端末・外部媒体の管理を学ぶ。中学年では，情報セキュリティを確保する基本的な方法として，個人情報管理，ID・パスワード管理といった人的対策が加わる。高学年では，情報セキュリティ

の概要として，インターネットにおける情報が加わる。また，情報セキュリティを確保する基本的な方法として，ダウンロード，フィルタリング，ウィルス対策ソフトウェア，ソフトウェア更新などインターネットに関わる内容が加わる。

1.5 既存の情報セキュリティ教材

摘出した小学校における情報セキュリティの指導内容と既存の情報セキュリティ教材の内容を表3.3に示す。各省庁が提供している情報セキュリティの小学生向け教材は，文部科学省[118]，独立行政法人情報処理推進機構(以下IPA)[119]がある。市販の教材としては，H社が提供している教材[120]がある。3つの教材とも情報モラル教材の内容の1つとして情報セキュリティを扱っている。

表3.3　既存の情報セキュリティ教材の内容

指導内容	文部科学省	IPA	H 社
A1.情報セキュリティの原則			○
A2.身近にある情報	○	○	○
A3.インターネットにおける情報	○	○	○
B1.情報端末・外部媒体の管理	○	○	○
B2.個人情報管理	○	○	○
B3.ID・パスワード管理	○	○	○
B4.ダウンロード		○	○
B5.フィルタリング			○
B6.ウィルス対策ソフトウェア	○	○	○
B7.ソフトウェア更新		○	○

文部科学省は，動画教材を提供している。この教材は，10分程度で作成されており，実写によるドラマとその解説で構成されている。小学生向けに2つの教材がある。この教材は，主に情報セキュリティの被害と対応に主眼が置かれているため，摘出した小学校で学ぶべき情報セキュリティの指導内容について不足している部分がある。

IPAは，小学生向け動画を3つ，学習漫画を1つ，小中高生を対象にした動画を4つ，学習漫画を2つ提供している。各教材は，1つ1つの教材が個別に完結しており教材間のつながりが見られないため，内容の重なりや不足部分がある。いずれの教材もID・パスワード，個人情報の管理など情報セキュリティの人的対策の学習内容に特化しており，情報端末の管理などの物理的対策やフィルタリングなどの技術的対策の学習内容が不足している。

H社が提供している小学生用教材は，5分程度のアニメ動画を中心とし，各事例について1単位時間で指導する教材である。情報モラル教育全体を網羅し，「情報活用能力の体系表例」に対応した62個の教材を準備している。情報セキュリティについては，小学生

に対応した教材が4つ用意されており，すべての指導内容を学習するためには4時間必要である。4つの教材のうち2つは中学校・高等学校と共通の教材である。

調査した3つの教材で共通する課題は，小学校で必要な情報セキュリティの学習をすべて網羅するために複数時間の学習が必要なことである。また，学習対象年齢が小中高生という幅広い年齢層を対象としているものも多く，小学生にとって必ずしも理解しやすいものであるとはいえない。

前述のとおり小学校は，情報セキュリティを指導する教科が定められていないため，学習計画と教材研究を各学校や教員がおこなう必要がある。さらに，教員の情報セキュリティの知識も不足している現状がある。既存の教材での学習では，多忙な教員の仕事にさらなる負担をあたえることにつながると想定される。

この問題を解決するためには，児童の実態をふまえて，なるべく短い時間で効果的に小学校において学ぶべき情報セキュリティの指導内容を網羅できるパッケージ化された教材が必要であると考える。

1.6 開発要件

先行研究，教師および児童の実態をふまえて以下に示す5つの小学校用情報セキュリティ教材の開発要件を設定した。また，開発要件は，児童が一人一台端末を使った新たな学習環境での授業をふまえたものとした。

① 小学校から高等学校までの体系的な情報セキュリティ教育をふまえ，「情報モラル指導モデルカリキュラム表」，「情報活用能力の体系表例」の小学校高学年の内容を網羅したものとする。
② 小学生のインターネットの利用実態をふまえ，オンラインゲーム，動画視聴，SNSを中心とした内容とする。
③ 児童が，一人一台端末を使い，OSの環境に左右されずに学習できるように，Webブラウザで提供できる教材とする。
④ 教材は，小学生の発達段階や生活経験を考慮し，イラストとわかりやすい文章で構成する。
⑤ １単位時間(45分)で学習できる教材とする。

1.7 教材の構成と内容

教材は，「情報セキュリティの基本」，「情報を守るための方法」，「生活の中の情報セキュリティ」の3つで構成した。教材の構成を，図3.1に示す。

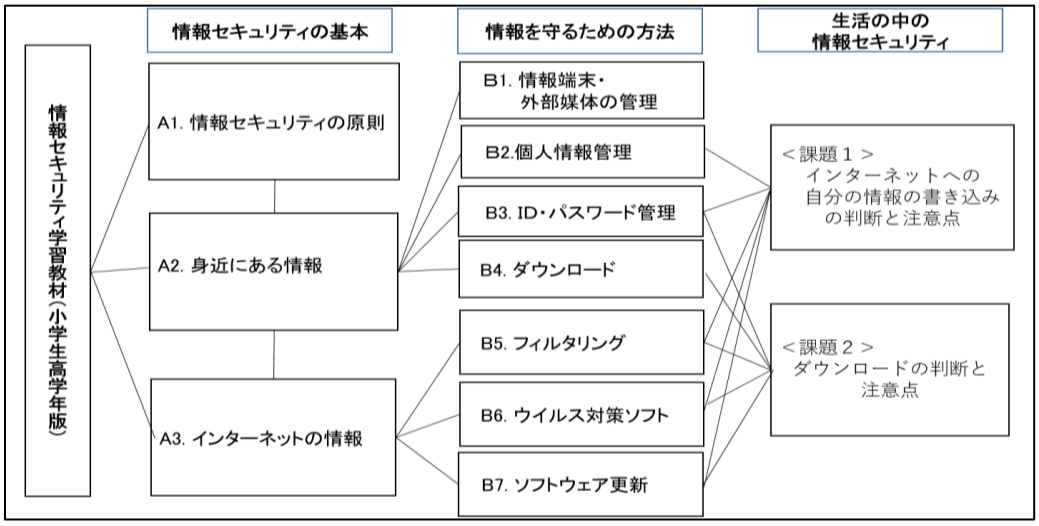


図3.1　教材の構成

「情報セキュリティの基本」は，身近にある情報の価値と情報セキュリティの三大要素である機密性，完全性，可用性を学ぶことをねらいとしている。「情報を守るための方法」は，情報セキュリティを確保するための物理的対策，人的対策，技術的対策について具体的な方法を学ぶことをねらいとしている。

「生活の中の情報セキュリティ」は，「情報セキュリティの基本」「情報を守るための方法」で学んだ知識を活用して，生活の中でのインターネットの使い方について情報セキュリティの視点をふまえ，考えるものである。

(1) 情報セキュリティの基本

「情報セキュリティの基本」は，「情報セキュリティの原則」，「身近にある情報」，「インターネットの情報」の3つの学習をおこなうものである。

教員が，授業のはじめに大型画面に教材を提示し，一斉指導で利用することを想定しているが，一人一台端末を使った個別学習や高学年においては，探究活動でも活用できるよう設計している。

「情報セキュリティの基本」では，情報セキュリティの概要や必要性を学ぶとともに，身近にある情報の大切さと情報セキュリティ対策の必要性に気付かせることをねらいとしている。「情報セキュリティの基本」の学習内容を以下に示す。

「情報セキュリティの原則」は，情報管理の三原則である機密性，完全性，可用性を学習する。小学生に理解しやすいように，機密性，完全性，可用性を「大切なものを自分だけ見られるようにすること」，「勝手に変更されないようにすること」，「自分だけが必要な時に操作できること」とやさしい言葉で示している。

「身近にある情報」は，小学生が何気なく使っている名前，電話番号，ID，パスワードなどは，個人情報で，大切なものであり，自分で意識して管理する必要があることを

学習する。

「インターネットの情報」では，インターネットには，公開性という特性があるために，インターネットでの情報を守るためには，特別な対策が必要であることを学習する。図3.2に「インターネットの情報」の教材を示す。

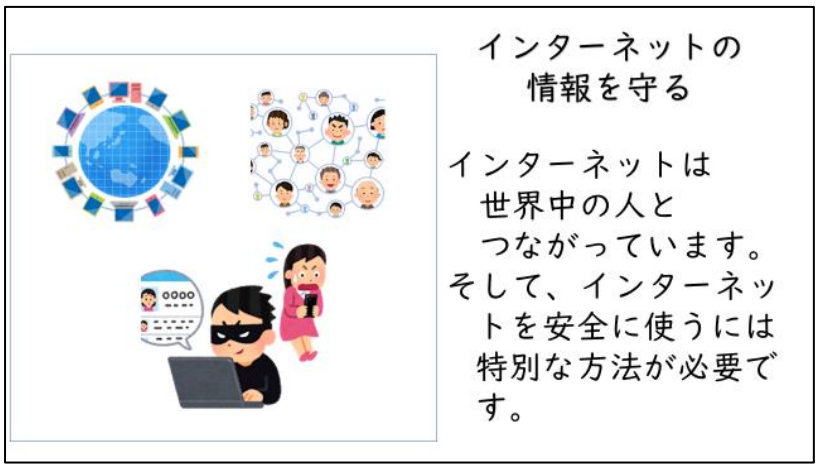


図3.2　インターネットの情報

(2) 情報を守るための方法

「情報を守るための方法」は，「情報端末・外部媒体の管理」，「名前や住所などの個人を識別できる情報の管理」，「ID・パスワードの管理」，「ダウンロード」，「フィルタリング」，「ウィルス対策ソフト」，「ソフトウェア更新」の7つの情報セキュリティ対策の学習をおこなうものである。

「情報を守るための方法」は，物理的対策，人的対策，技術的対策の3つの具体的な情報セキュリティ対策とセキュリティ対策をしなかった場合のリスクについて理解することをねらいとしている。

「情報を守るための方法」の学習内容を以下に示す。

「物理的対策」は，スマートフォン・ゲーム機などの情報端末やUSBメモリ，フラシュカードなど外部媒体の管理の大切さと具体的な管理の方法を学習する。具体的な管理の方法として，管理場所を決めて管理することで情報端末や外部媒体の紛失や破損のリスクを少なくすることができることを学習する。

「人的対策」は，ID・パスワードの漏えい，ダウンロードなど一人一人の適切な情報管理の大切さと人的対策をおこなわなかった場合のリスクを学習する。ID・パスワードが漏えいした場合，他人がなりすますことができるなどの危険性を示し，具体的な方法として「安全が確認できない安易なダウンロードをしないこと」，「ID・パスワードを教えないこと」を学習する。

「技術的対策」は，インターネットを使う時の特別な対策と必要性について学習す

る。具体的な対策としてフィルタリング，ウィルス対策ソフト，アップデイトの3つの対策をすることでリスクを軽減し，安心してインターネットを使うことができることを学習する。

図 3.3 に「技術的対策」の教材を示す。

図3.3　技術的対策

(3) 生活の中の情報セキュリティ

「生活の中の情報セキュリティ」は，「情報セキュリティの基本」，「情報を守るための方法」で学習した知識を活用して，課題解決学習をおこなうものである。

グループ学習およびクラスでの一斉学習での利用を想定している。教師が，大型画面に課題を提示し，その課題をグループで考え，グループの意見をクラス全体で発表し，知の共有をおこなうことができる。

「生活の中の情報セキュリティ」は，情報セキュリティの確保のための対策・対応の知識を基にして，適切な行動しようとする態度を身に付けることをねらいとしている。

教材は，課題1「インターネットへの情報の書き込みの判断と注意点」，課題2「ダウンロードの判断と注意点」の2つの内容で構成されている。

利用方法は，小学生の身近で起きそうな「問題」を示し，どのような行動をとるか意思決定をする。さらに，意思決定をするうえで「心配なことを考える」ようにし，グループやクラスで意思決定をうえでの情報セキュリティの視点から考えたことについて協議できるようにした。

図3.4に「インターネットへの情報の書き込みの判断と注意点」の教材を示す。

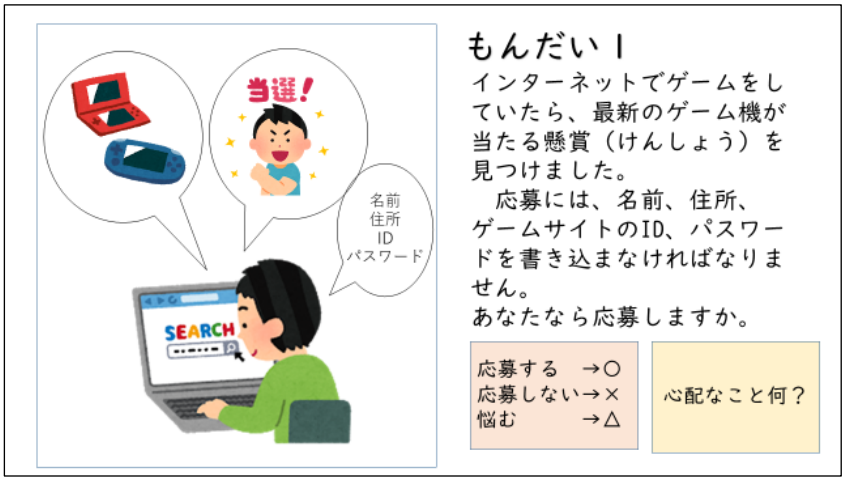


図3.4　インターネットへの情報の書き込みの判断と注意点

1.8 おわりに

第 1 節では，「情報モラル指導モデルカリキュラム表」，「情報活用能力の体系表例」で示された小学校高学年の目標を指導するために「A1.情報セキュリティの原則」，「A2.身近にある情報」，「A3.インターネットにおける情報」，「B1.情報端末・外部媒体の管理」，「B2.個人情報管理」，「B3.ID・パスワード管理」，「B4.ダウンロード」，「B5.フィルタリング」，「B6.ウィルス対策ソフトウェア」，「B7.ソフトウェア更新」の 10 個の指導内容を定めた。

また，摘出した指導内容と第2章2節で調査した小学生の実態をふまえ，1単位時間(45分)で学習できる教材を開発した。開発した教材は，「情報セキュリティの基本」，「情報を守るための方法」，「生活の中の情報セキュリティ」の3つの内容で構成した。

この教材を活用して授業をおこなうことで，児童一人一台端末の新たな学習環境において，限られた学習時間の中で小学校高学年における情報セキュリティ学習が効果的にすすめられるものと考えられる。

第2節　中学校における情報セキュリティ教材

2.1 はじめに

第2節では，第2章で前述した中学校修了段階の実態と「情報モラル指導実践キックオフガイド」，「教育の情報化の手引き-追補版-」，「中学校学習指導要領(平成29年告示)」をふまえて，中学校における情報セキュリティ教育の具体的な内容を摘出していく。

中学校における情報セキュリティ教育は，技術・家庭科(技術分野)の授業においておこなわれている。しかし，技術・家庭科(技術分野)の授業の中で情報セキュリティ教育にあてることができる時間は，限られており，効率的で効果的な学習をおこなうことが必要である。

第2節では，技術・家庭科(技術分野)において，限られた時間の中で効果的な学習につながる情報セキュリティ教材を開発することとした。

2.2 中学校における情報セキュリティの指導事項

「中学校学習指導要領(平成29年告示)」[121]には，「第8節　技術・家庭」「D　情報の技術」の指導内容として情報セキュリティ教育の内容が記載されている。また，技術・家庭科(技術分野)の具体的な改善事項の中に“急速な発達を遂げている情報の技術に関しては，小学校におけるプログラミング教育の成果を生かし，発展させるという視点から，従前からの計測・制御に加えて，双方向性のあるコンテンツに関するプログラミングやネットワークやデータを活用して処理するプログラミングも題材として扱うことが考えられる。その際，情報セキュリティ等についても充実する。”と記載されている。表3.4に技術・家庭科(技術分野)における指導事項を示す。

表3.4　技術・家庭科(技術分野)における指導事項

観点	指導事項	指導内容
情報活用の実践力	情報セキュリティ等に関わる問題の解決	・情報セキュリティ等に関わる問題からの課題を設定
情報の科学的な理解	情報セキュリティ等の基礎的な技術の仕組	・個人認証 ・コンピュータへの不正な侵入を防ぐ技術(ファイアウォール，セキュリティ対策ソフトウェア)
	サイバーセキュリティ	・仮想的な空間(サイバー空間など)の保護・治安維持
情報社会に参画する態度	情報セキュリティと社会のかかわり 情報の技術の悪用が社会与える多大な経済的・精神的な損害	・情報セキュリティ等に技術と社会からの要求，安全性，システム，経済性の関係 ・コンピュータウィルス，ハッキング等

また，「中学校学習指導要領(平成29年告示)解説 特別の教科 道徳編」[122]には，“情

報機器の使い方やインターネットの操作，危機回避の方法やその際の行動の具体的な練習を行うことにその主眼をおくのではないことに留意する必要がある。”と記載されており，情報セキュリティに関する具体的な内容は示されていない。なお，「中学校学習指導要領（平成29年告示)解説 総則編」[123]には，小学校と同様に各教科の学びを支える力と指導者側の安全管理体制として情報セキュリティを確保することの重要性が記載されている。

2.3 検定教科書

中学校において，情報セキュリティを教科の指導内容として定めている教科は，技術・家庭科(技術分野)の1つである。技術・家庭科の教科書は，3社[124)~126)] から出版されている。「情報セキュリティ等の基礎的な技術の仕組」は，個人認証として3社ともID・パスワード，生体認証が記載されている。A社については，多要素認証も記載されている。「不正な侵入を防ぐ技術」では，3社ともファイアウォール，セキュリティ対策ソフトウェア(不正プログラム対策ソフトウェア)，暗号化(SSL)，フィルタリング，バックアップを取り上げている。A社については，暗号化(TLS)も記載されている。サイバーセキュリティについては，サイバーセキュリティの内容と意義が記載されている。表3.5に令和3年度に利用されている技術・家庭科(技術分野)の教科書の記載内容を示す。

表3.5 技術・家庭科(技術分野)の教科書の記載内容

指導事項	A 社	B 社	C 社
情報セキュリティ等の基礎的な技術の仕組	○個人認証 ・ID・パスワード ・生体認証 ・多要素認証 ○不正な侵入を防ぐ技術 ・ファイアウォール ・不正プログラム対策ソフトウェア ・暗号化(SSL/TLS) ・フィルタリング ・バックアップ	○個人認証 ・ID・パスワード ・生体認証 ○不正な侵入を防ぐ技術 ・ファイアウォール ・セキュリティ対策ソフトウェア ・暗号化(SSL) ・フィルタリング ・バックアップ	○個人認証 ・ID・パスワード ・生体認証 ○不正な侵入を防ぐ技術 ・ファイアウォール ・セキュリティ対策ソフトウェア ・暗号化(SSL) ・フィルタリング ・バックアップ
サイバーセキュリティ	・サイバーセキュリティ	・サイバーセキュリティ	・サイバーセキュリティ

2.4 中学校における指導内容

前述したように中学校における情報セキュリティの指導内容については，「教育の情報化に関する手引-追補版-」に示された情報活用能力の体系表例に4つ，技術・家庭科(技術分野)における情報セキュリティの指導については，「中学校学習指導要領(平成29年告示)解説 技術・家庭編」[127)]に6つが示されている。これらの指導内容と第2章第3節で前述した調査結果を基に，技術・家庭科(技術分野)における具体的な指導内容を表3.6

に示す15項目(a.1～12，b，c，d)を摘出した。表3.6に中学校における指導内容を示す。

表3.6 中学校における指導内容

教育の情報化に関する手引	中学校学習指導要領(平成29年告示)解説 技術・家庭編		中学校における指導内容
情報セキュリティの確保のための対策・対応	個人認証	ＩＤ・パスワード管理	a1.リンクの対応 a2.ファイアウォール a3.アカウント管理
	コンピュータへの不正な侵入を防ぐ技術	・ファイアウォール ・セキュリティ対策ソフトウェア ・暗号化技術 ・パスワード作成・管理技術 ・フィルタリング	a4.ソフトウェア更新 a5.セキュリティ対策ソフトウェア a6.バックアップ a7.フィルタリング a8.暗号化 a9.ID・パスワード a10.生体認証 a11.多要素認証 a12.パスワード作成・管理技術
仮想的な空間の保護・治安維持のための，サイバーセキュリティの重要性	サイバーセキュリティ	・仮想的な空間(サイバー空間など)の保護・治安維持	b.サイバー空間における情報セキュリティの被害とその対応
情報セキュリティの確保のための対策・対応をふまえた行動	情報セキュリティ等に関わる問題の解決 情報セキュリティと社会のかかわり	・情報セキュリティ等に関わる問題からの課題を設定 ・情報セキュリティ等に技術と社会からの要求，安全性 ・システム，経済性の関係	c.生活の中で想定されるトラブルへの対応
仮想的な空間の保護・治安維持のためのサイバーセキュリティの重要性をふまえた行動	情報の技術の悪用が社会与える多大な経済的精神的な損害	・コンピュータウィルス対策 ・ハッキング対策	d.コンピュータウィルスの感染，ハッキング等による被害事例とその対応

2.5 既存の情報セキュリティ教材

各省庁が提供している情報セキュリティの中学生向け教材は，前節で示した小学生向け情報セキュリティ教材と同様に文部科学省[128)]，IPA[129)]が無償で提供している。市販の教材としては，H社[130)]が提供している教材がある。3つの教材とも情報モラル教材の内容の1つとして情報セキュリティを扱っている。

文部科学省は，動画教材を提供している。この教材は，10分程度で作成されており，実写によるドラマとその解説で構成されている。中学生向けに1つの教材がある。この教材は，主に情報セキュリティの被害と対応に主眼が置かれているため，技術・家庭科(技術分野)で示されている指導内容が網羅されていないため，教科指導の教材としては不充分であると考えられる。

IPAは，中高生向け動画を1つ，学習漫画を3つ，小中高生向け学習漫画を2つ，中高

生・一般を対象とした動画を6つ，学習漫画を2つ提供している。中学生のみを対象とした教材はなく，第3章1節と重複する教材もある。

各教材は，1つ1つの教材が個別に完結しており教材間のつながりが見られないため，内容の重なりや不足部分がある。いずれの教材もID・パスワード，個人情報の管理など情報セキュリティの人的対策の学習内容に特化しており，情報端末の管理などの物理的対策やフィルタリングなどの技術的対策の学習内容が不足している。

H社が提供している教材は，5分程度のアニメ動画を中心とし，各事例について1単位時間で指導する教材である。情報モラル教育全体を網羅し，「情報活用能力の体系表例」に対応した50個の教材を準備している。情報セキュリティについては，中学生に対応した事例が7つ用意されており，すべての指導内容を学習するためには複数時間必要であると考えられる。7つの教材の4つは，小学校と共通の教材である。技術・家庭科（技術分野）における教科の指導という視点で考えると「ファイアウォール」の内容が欠如しているため，本教材だけでは，情報セキュリティの仕組についての指導が充分にできないと考えられる。表3.7に，摘出した中学校における既存の教材の内容を示す。

表3.7　既存の情報セキュリティ教材の内容

指導内容	文部科学省	IPA	H 社
a 1. リンクの対応			○
a 2. ファイアウォール			
a 3. アカウント管理		○	○
a 4. ソフトウェア更新	○	○	○
a 5. ウィルス対策ソフトウェア	○	○	○
a 6. バックアップ		○	○
a 7. フィルタリング		○	○
a 8. 暗号化		○	○
a 9. ID・パスワード	○	○	○
a10. 生体認証			○
a11. 多要素認証			○
a12. パスワード作成・管理技術			○
b ．サイバー空間における情報セキュリティの被害とその対応	○	○	○
c ．生活の中で想定されるトラブルへの対応	○	○	○
d ．コンピュータウィルスの感染，ハッキング等による被害事例とその対応	○	○	○

調査した3つの教材で共通することとして，内容別のコンテンツが個別で存在するため，すべての内容を学習するためには，複数時間の学習時間を確保することが必要である。技術・家庭科(技術分野)での情報セキュリティ指導の指導時間数を調べたところ，3年間で1時間程度の指導時間であるという限られた時間であった[131)]。

これらのことから，既存の教材を使った学習では，限られた指導時間の中で，中学校の指導内容をすべて網羅するのは，難しいと考える。この問題を解決するためには，生徒の実態をふまえて，技術・家庭科(技術分野)で学ぶべき情報セキュリティの指導内容を網羅できるパッケージ化された教材が必要であると考える。

2.6 開発要件

先行研究をふまえて，以下に示す7つの開発要件を設定した。また，開発要件は小学校と同様に，生徒一人一台端末を使った新たな学習環境での授業をふまえたものとした。

① 学習指導要領に示されている指導内容を網羅する。
② 生徒の実態を踏まえた個別学習に対応できる。
③ 限られた時間(50分)の授業で効果的に学習が完結する。
④ 社会の変化に対応し，情報セキュリティに関する不変の内容と最新のテクノロジーの内容を入れる。
⑤ 学習した知識を活用した課題解決学習ができる。
⑥ 中学生の生活経験や発達段階を考慮し，イラストと簡潔な文章で構成する。
⑦ OSの環境に左右されずに学習できるように，Webブラウザで提供できる教材とする。

2.7 教材の構成と内容

教材の構成を図3.5に示す。本教材は，「身近にひそむ危険」，「情報セキュリティ対策」，「情報セキュリティの課題解決」の3つの内容で構成した。

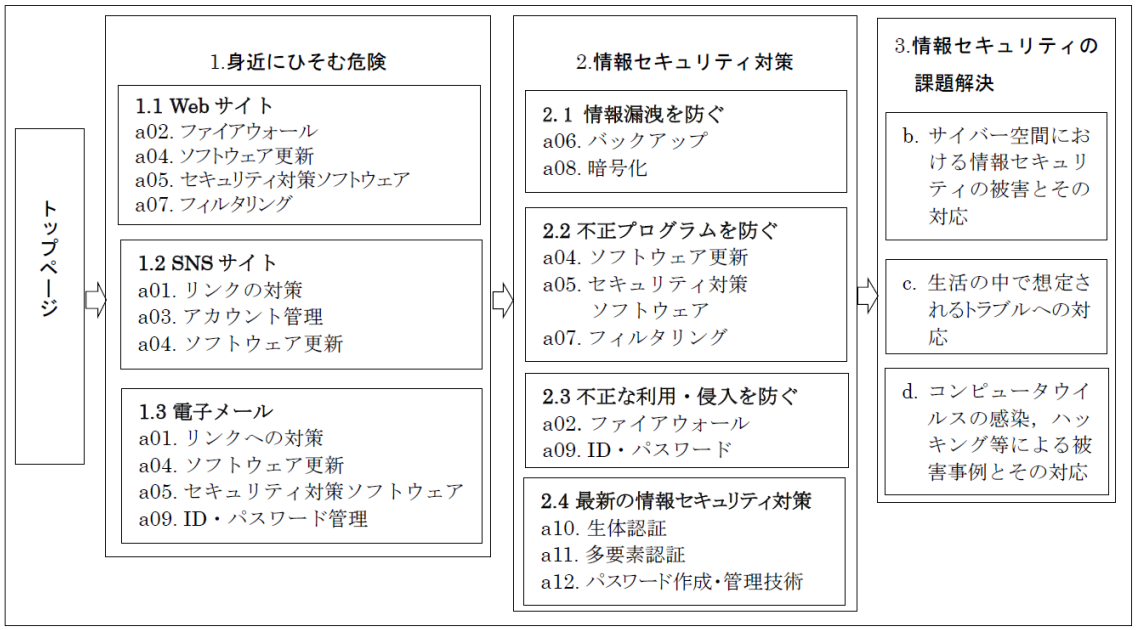


図3.5 教材の構成

「身近にひそむ危険」は，中学生が日常的に使っているインターネットサービスの情報セキュリティの危険性とその対策を学ぶためのものである。「情報セキュリティ対策」は，情報セキュリティの基本的な対策と最新のテクノロジーについて学ぶものである。また，「情報セキュリティの課題解決」は，情報セキュリティの課題を見出し，その課題を学習した知識を活用して，解決方法を考えるものである。「身近にひそむ危険」，「情報セキュリティ対策」は，生徒による個別学習用の教材として作成した。「情報セキュリティの課題解決」は，授業の中で教師が提示しながら，グループ学習や一斉学習で活用できるように作成した。教材をすべて学習することで，前述した技術・家庭科(技術分野)の指導内容15個(a.1～12，b，c，d)の内容をすべて学習できるようにした。

本教材は，技術・家庭科(技術分野)の授業で，１単位時間（50分）での利用を想定している。活用例として一人一台端末を使い「身近にひそむ危険」，「情報セキュリティ対策」で個別学習をおこない，その後に「情報セキュリティの課題解決」をグループ学習や一斉学習などでおこなうことが考えられる。

(1) 身近にひそむ危険

「身近にひそむ危険」は，　中学生がよく利用する「Webサイト」，「SNS」，「電子メール」の利用時の3つの危険性と情報セキュリティ対策の知識や具体的な行動についての学習をおこなうものである。なお，「電子メール」は，現段階での利用実態は少ないが，現代の生活に欠かせないツールであり，教科書で共通に扱っている内容であるため教材の内容とした。

教員が，大型画面に教材を提示して指導をする一斉学習と一人一台端末を使った個別学習の2つの利用方法を想定している。

「身近にひそむ危険」では，「Webサイト」，「SNS」，「電子メール」の3つのサービスを利用する時の危険性，情報セキュリティ対策をおこなわない場合のリスク，具体的な対策を学習することをねらいとしている。具体的な対策として，「リンクの対応」，「ファイアウォール」，「アカウント管理」，「ソフトウェア更新」，「セキュリティ対策ソフトウェア」，「フィルタリング」を学習する。

「SNSサイトの情報セキュリティ」の教材を図3.6に示す。

この教材では，情報セキュリティ対策をおこなわずに SNS を利用した時の危険性について学ぶことができる。総務省は，SNS を「限られたユーザーだけが参加できる Web サイトの会員制サービス」と定義している。本教材における SNS は，登録したユーザーが，インターネット上で誰でも閲覧可能なものに加え，特定な相手と情報交換が可能なメッセンジャーアプリを含む広義のものである。

被害事例として，「アカウントののっとり」，「アカウントからの不正な投稿」，「フィッシング詐欺」の具体的な3つの被害事例を取り上げている。

具体的な情報セキュリティ対策では，SNSサイトの利用に必要な情報セキュリティ対策として，「ソフトウェア更新」，「プライバシー設定」，「リンクへの対策」，「アカウント管理」の4つの対策を示している。

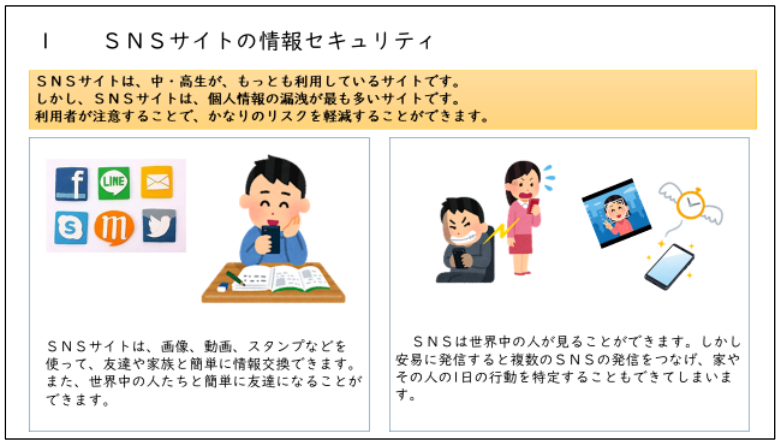


図3.6 SNSサイト

(2) 情報セキュリティ対策

「情報セキュリティ対策」は，「不正な利用・侵入を防ぐ」，「不正プログラムを防ぐ」，「情報漏えいを防ぐ」，「最新の情報セキュリティ対策」で構成されており，情報セキュリティ対策を包括的に学習するものである。「情報セキュリティ対策」は，一人一台端末を使った個別学習で利用することを想定している。

「情報セキュリティ対策」は，基本的な対策と最新の対策を学ぶことをねらいとしており，情報セキュリティ対策をしなかった場合のリスクと具体的におこなうべき対策を示している。

具体的な学習内容を以下に示す。「情報漏えいを防ぐ」では，「バックアップ」，「暗号化」の2つの具体的な対策を学習する。「不正プログラムを防ぐ」は，「ソフトウェア更新」，「セキュリティ対策ソフトウェア」，「フィルタリング」の3つの具体的な対策を学習する。「不正な利用・侵入を防ぐ」では，「ファイアウォール」，「ID・パスワード」の2つの具体的な対策を学習する。また，「最新の情報セキュリティ対策」では，「パスワード管理アプリ」，「パスワード作成アプリ」，「多要素認証」，「生体認証」の4つの最新の情報セキュリティの技術を学習する。開発教材では，情報セキュリティの技術的な仕組みや具体的な方法を学べるようにした。

「最新の情報セキュリティ対策」を例に教材を説明する。この教材では，ID・パスワードの管理のリスクである「パスワード忘れ」，「パスワードの盗難」を示している。このリスクを回避するための最新の技術として，指紋や顔を使った生体認証とワンタイ

ムパスワード，複数端末による認証といった多要素認証を取り上げている。「情報セキュリティの対策」の教材を図3.7に示す。

図3.7　情報セキュリティの対策

(3) 情報セキュリティの課題解決

「情報セキュリティの課題解決」は，「身近にひそむ危険」および「情報セキュリティ対策」で学んだ知識を活用して，課題解決学習をおこなうものである。

グループ学習およびクラスでの一斉学習での利用を想定している。「情報セキュリティの課題解決」は，情報セキュリティの確保のための対策・対応をふまえ，行動しようとする能力を身に付けることをねらいとしている。内容は，「課題の発見」，「対応策の検討」の2つで構成されている。「課題の発見」では，個人情報の流出，ID・パスワード管理，リンクの対応の課題に気づき，「対応策の検討」では，リンクへの対策，ID・パスワード管理，ウィルス対策ソフトウェア更新の3つの対応策を考える。「情報セキュリティの課題解決」の教材を図3.8に示す。

図3.8　情報セキュリティの課題解決

「情報セキュリティの課題解決」の教材を以下に説明する。この教材では，インターネットからの懸賞応募を題材にして，ID・パスワードの漏えいとダウンロードによるウィルス感染の事例を取り上げている。そして，この主人公が，どのように行動すべきであったかをグループ学習や一斉学習で協議をおこなうように設計している。

2.8 おわりに

第３節では，中学校における情報セキュリティの指導内容を「情報モラル指導モデルカリキュラム表」，「情報活用能力の体系表例」，「中学校学習指導要領(平成29年告示)解説 技術・家庭編」から，「a1. リンクの対応」，「a2. ファイアウォール」，「a3. アカウント管理」，「a4. ソフトウェア更新」，「a5. ウィルス対策ソフトウェア」，「a6. バックアップ」，「a7. フィルタリング」，「a8. 暗号化」，「a9. ID・パスワード」，「a10. 生体認証」，「a11. 多要素認証」，「a12. パスワード作成・管理技術」，「b. サイバー空間における情報セキュリティの被害とその対応」，「c. 生活の中で想定されるトラブルへの対応」，「d. コンピュータウィルスの感染，ハッキング等による被害事例とその対応」の15個の指導内容を摘出した。

つぎに，第2章第3節で調査した生徒の実態と15個の指導内容を踏まえて「技術・家庭科（技術分野）」の1単位時間(50分)で学習できる教材を開発した。開発した教材は，「身近にひそむ危険」，「情報セキュリティ対策」，「情報セキュリティの課題解決」の3つの内容で構成した。

この教材を活用して授業をおこなうことで，限られた学習時間の中で，技術・家庭科(技術分野)における情報セキュリティ教育が効果的にすすめられるものと考えられる。

２．結言

本章では，小学校高学年および中学校技術・家庭科(技術分野)で情報セキュリティ教育をおこなうための教材の開発をおこなった。以下に本章での成果をまとめる。

1. 小学校の情報セキュリティ教育の内容を「情報モラル指導モデルカリキュラム表」，「情報活用能力の体系表例」から「A1.情報セキュリティの原則」，「A2.身近にある情報」，「A3.インターネットにおける情報」，「B1.情報端末・外部媒体の管理」，「B2.個人情報管理」，「B3.ID・パスワード管理」，「B4.ダウンロード」，「B5.フィルタリング」，「B6.ウィルス対策ソフトウェア」，「B7.ソフトウェア更新」の10個の指導内容を摘出した。
2. 中学校における情報セキュリティの指導内容を「情報モラル指導モデルカリキュラム表」，「情報活用能力の体系表例」，「中学校学習指導要領(平成29年告示)解説技術・家庭編」から「a1.リンクの対応」，「a2.ファイアウォール」，「a3.アカウント管理」，「a4.ソフトウェア更新」，「a5.ウィルス対策ソフトウェア」，「a6.バックアップ」，「a7.フィルタリング」，「a8.暗号化」，「a9.ID・パスワード」，「a10.生体認証」，「a11.多要素認証」，「a12.パスワード作成・管理技術」，「b.サイバー空間における情報セキュリティの被害とその対応」，「c.生活の中で想定されるトラブルへの対応」，「d.コンピュータウィルスの感染，ハッキング等による被害事例とその対応」の15個を摘出した。
3. 「情報モラル指導モデルカリキュラム表」，「情報活用能力の体系表例」の小学校高学年の目標，児童の実態をふまえた5つの開発要件に従い小学校高学年用情報セキュリティ教材を作成した。
4. 「情報モラル指導モデルカリキュラム表」，「情報活用能力の体系表例」の中学校の内容，技術・家庭科(技術分野)の指導内容，生徒の実態をふまえた7つの開発要件に従い中学生用情報セキュリティ教材を作成した。

次章では，本章で開発した教材を用いた授業実践をおこない，教材の効果の検証と教材を用いた指導について提案する。

参考文献

108)藤川真樹・叶稜也・伊藤愛里・安部芳絵:小学校高学年を対象としたSNS教育ゲームの開発，情報処理学会　マルチメディア分散協調とモバイルシンポジウム2019論文集，pp.695-702(2019)
109)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発表予稿集8，pp.111-112(2019)
110)前掲47)，pp.101-116(2011)
111)豊田充崇：対話的な学びを重視した情報モラル指導用教材の開発とその有効性，和歌山大学教職大学院紀要学校教育実践研究No.3，pp.21-28(2018)
112)前掲22)，pp.6-7(2007)
113)前掲48)，pp.232-239(2019)
114)前掲33)，pp.91-92(2017)
115)前掲36)，pp.51-52(2017)
116)前掲34)，pp.171-174(2017)
117)前掲35)，pp.97-99(2017)
118)文部科学省:パスワードについて考えよう情報化社会の問題を考えるための新たな教材，pp.118-124(2016)
119)独立行政法人情報処理推進機構:情報セキュリティ 普及啓発 映像コンテンツ「君はどっちＰＣ・携帯・スマートフォン」，https://www.youtube.com/watch?v=k2VT6x4wBSk，(2021.8.8最終確認)
120)広島県教科用図書販売株式会社:情報モラル教育支援ソフト「事例で学ぶNetモラル」(2021)
121)前掲23)，pp.132-136(2017)
122)前掲38)，p.100(2017)
123)前掲39)，p.86(2017)
124)前掲54)，p.228(2020)
125)前掲55)，p.212(2020)
126)前掲56)，p.198(2020)
127)前掲37)，p.11(2017)
128)前掲113)，pp.118-124(2016)
129)前掲114)，https://www.youtube.com/watch?v=k2VT6x4wBSk，(2021.8.8最終確認)
130)前掲115)，(2021)
131)小熊良一・山本利一・濵 嘉孝，生徒の情報セキュリティへの意識を高める教材と指導法の研究，日本産業技術教育学会　第29回関東支部大会（群馬）講演要旨集，pp.67-68(2017)

関係論文

１)小熊良一・山本利一：小学校高学年における情報セキュリティWeb教材開発と授業実践，教育方法研究，第37巻，第1号，pp.53-62(2021)

２)小熊良一・山本利一：中学校技術・家庭科(技術分野)における「情報セキュリティ」のオンライン教材の開発と授業実践，日本産業技術教育学会誌，第 63 巻，第 4 号，pp.39-48(2021)

第4章 小・中学校における授業実践

１．緒言

第3章では，小学校高学年および中学校技術・家庭科(技術分野)において情報セキュリティ教育をおこなうための教材開発をおこなった。第4章では開発した教材を活用して授業実践をおこない，その効果を検証する。

情報セキュリティ教育を扱った授業実践は，小学校高学年および中学校の技術・家庭科(技術分野)の授業で報告されている。小学生を対象とした授業実践として，藤川ら(2019)[132]は，SNSノベルゲームを開発し，情報セキュリティ教育における主体的・対話的で深い学びの実現を報告している。花田(2019)[133]は，すごろく型のアナログ教材を開発し，小学校高学年において，ICT 機器の安全利用を促すための実践をおこなっている。また，技術・家庭科(技術分野)における授業実践として，堤ら(2016)[134]はジグソー法を用いた情報セキュリティの授業が協働的問題解決を促すと報告している。いずれの研究も児童・生徒の情報セキュリティへの意識が高まることが実証されているが，知識の高まりについての実証は不充分である。

第4章では，第3章で開発した情報セキュリティ教材を活用して，小学5・6年生と中学2・3年生に対して，授業実践を行い，開発した2つの教材の意識と知識の効果について検証を試みた。

第4章は，「第1節小学校における授業実践」，「第2節中学校における授業実践」で構成している。

第1節　小学校における授業実践

1.1 はじめに

第3章1節で開発した小学生用情報セキュリティ教材の効果を図るため，小学5・6年生を対象に授業実践をおこなった。

小学校における授業実践は，2020年9月，2021年7月にA県内の2校の小学校5年生1クラス(29名)，6年生4クラス(113名)の計142名を対象に「総合的な学習の時間」において，1単位時間(45分)で実施した[注1)]。なお，教材は，小学校高学年での学習を想定した教材であるため，5年生と6年生で実施した。また，2021年9月の実践では，2021年の小学校卒業段階の実態調査の結果を踏まえて，技術的対策に関わる内容について一部修正を施した。授業形態は，一斉学習，グループ学習，個別学習の3つの形態を取り入れた。一斉学習は，授業の導入時に授業のねらいと教材の利用法を全員で確認し，授業の終末で，学習の成果を伝え合い，クラス全体の多様な意見を知るのに有効である。グループ学習は，少人数での話合いで課題を解決することにより，情報セキュリティに関して主体的に考え，他の意見を取り入れながら方向性を導きだすことができる。個別学習は，一人一台端末で教材を活用することで，一人一人の児童の実態にあった学習が可能になる。

1.2 目指す資質・能力および授業の概要

(1) 目指す資質・能力

本実践で目指す資質・能力は，「情報セキュリティを確保する必要性を知る(知識および技能)」，「既存の知識を活用し，情報セキュリティ上の課題を発見し，対応策を考える(思考力，判断力，表現力等)」，「情報セキュリティに配慮し，生活を送っていこうとする態度をはぐくむ(学びに向かう力人間性等)」とした。

授業は，開発した教材を利用しておこなった。授業の様子を図4.1に示す。

図4.1 授業の様子

(2) 授業の概要および児童の反応

授業の具体的な指導内容と活用した開発教材，児童の反応を以下に示す。

① 情報セキュリティの基本

「1.情報セキュリティの基本」を活用して，小学生用情報セキュリティ教材の利用方法と情報セキュリティの必要性を考える学習を一斉学習でおこなった。

身のまわりには，名前や住所などたくさんの個人情報があること，情報セキュリティの原則，情報を守ることの大切さを学ばせた。次に，インターネット利用時の人的対策と物理的対策の大切さについて考えさせた。児童からは，ゲーム機を紛失してしまったり，兄弟に自分の ID でゲームを使われてしまったりしたなどの過去の自分の経験を想起した発言が見られた。また，インターネットを利用する時には，特別な情報セキュリティ対策を講じる必要があることを知らせた。

② 情報を守るための方法

「2.情報を守るための方法」を活用して，情報セキュリティの人的対策と技術的対策について，一人一台端末による個別学習をおこなった。

学習内容は，人的対策として，ID・パスワード管理，ダウンロード，個人情報の書き込み，技術的対策として，ウィルス対策ソフト，OS・ソフトウェアのアップデイトであった。

机間支援の中では，自分の所有するスマートフォンやオンラインゲームを安全に使うための情報セキュリティ対策など自分の生活を想起した個別の質問が見られた。

③ 生活の中の情報セキュリティ

学習のまとめとして，「3.生活の中の情報セキュリティ」を活用して，グループ学習をおこなった。なお，グループ学習は，全員が，主体的に話合いに参加できるよう3～4名でグループを編成した。

「課題1：インターネットを見ていたら，最新のゲーム機が当たる懸賞を見つけました。懸賞の応募には，名前，住所，SNSサイトのID，パスワードを書き込まなければなりません。あなたならどうしますか。」，「課題2：SNSサイトに，今苦戦しているゲームのクリア方法の動画をダウンロードできるサイトを見つけました。あなたならどうしますか。」に対して情報セキュリティの視点から考えた適切な行動を決定させ，その理由を考えさせた。

グループ学習で話合った結果をクラス全体で発表させた。また，グループ学習では，適切な行動の決定に対して，意見が分かれるなどしている中でお互いの意見を聞き，情報セキュリティについて意欲的に考えている様子が見られた。また，授業後の児童の感想には，「インターネットの安全を守りながら，ゲーム機を使っていきたい」などの情

報セキュリティへの行動の変容につながる意見も複数見られた。

1.3 調査項目および分析方法

実態調査は，授業実践の事前と事後に20分間実施した。本実践対象者のうち，欠席および回答に不備のあった3名を分析から除外した。その結果，有効回答数は139名，有効回答率は98.6%であった。

調査項目は，第3章で前述した小学校修了段階の調査をふまえて，情報セキュリティ対策の意識と知識の2種類を作成した。情報セキュリティ対策の意識の調査項目を表4.1に示す。

表4.1　「情報セキュリティ対策の意識」の調査項目

＜1.情報セキュリティの認識＞
情報セキュリティという言葉を知っていますか
＜2.物理的対策の意識＞
スマートフォンやゲーム機は，なくさないように管理しようと思いますか
＜3.人的対策の意識＞
インターネットで情報検索やゲームをする時は，安全を考えて利用しようと思いますか
＜4.技術的対策の意識＞
スマートフォンやゲーム機には，フィルタリングやウィルス対策などの安全対策をしようと思いますか

情報セキュリティ対策の意識については，「1.情報セキュリティの認識」，「2.物理的対策」，「3.人的対策」，「4.技術的対策」の4項目で作成し，4件法で回答を求めた。4件法で回答を求めたものは，「あてはまる」を4点，「少しあてはまる」を3点，「あまりあてはまらない」を2点，「あてはまらない」を1点とし得点化し，平均と標準偏差を求めた。また，「2.物理的対策」，「3.人的対策」，「4.技術的対策」の3項目については，事前・事後の結果に統計処理をほどこした。

情報セキュリティの知識については，前章で前述した「情報モラル指導モデルカリキュラム表」，「情報活用能力の体系表例」から摘出した指導内容から7問作成した。また，安心ネットづくり促進協会が作成した「安心協ILASテスト小学生版」を参考にした。回答は，「1.正しい」，「2.ちがっている」，「3.意味が分からない」の中から適切な回答を選ぶ選択式とした。分析は，事前・事後に正答・誤答に対して，マクネマー検定を実施した[注2)]。また，「正答」を1点，「誤答」を0点として得点化し，知識全体の得点を集計し，事前と事後の平均と標準偏差を求め，t検定をほどこした。

本調査は，事前に学校長および授業者に，実態調査の了解を得たうえでおこなった。また，児童には，倫理的配慮として，使用目的，および研究用途以外には用いないこ

と，個人が特定されないように配慮することを説明した。情報セキュリティの知識の調査項目を表4.2に示す。

表4.2　「情報セキュリティの知識」の調査項目

＜人的対策＞
B2. ID・パスワード管理
パスワードが必要なサイトでは，自分のパスワードを仲のよい友達に教えておくほうがよい
B3. 個人情報管理
懸賞サイトに住所や名前を記入しても問題はない
B4. ダウンロード
インターネットで公開されている無料マンガはダウンロードしても安全である
＜技術的対策＞
B5. フィルタリング
ホームページを見みるだけで，パソコンがウィルスでおかしくなることがある
B6. ウィルス対策ソフトウェア(携帯型情報端末対策)
スマートフォンにはウィルスがないのでウィルス対策ソフトはなくてよい
B6. ウィルス対策ソフトウェア(PC対策)
ウィルス対策ソフトウェアをいれればＰＣがコンピュータウィルスに感染しない
B7. ソフトウェア更新
パソコンのソフトウェア，スマートフォンのアプリは購入した時のままが安全なので，アップデイトする必要はない

1.4 調査結果

(1) 意識の調査結果

調査項目１「情報セキュリティの認識」の平均は2.53，標準偏差は1.14であった。回答は，「あてはまる(26.4%)」，「少しあてはまる(25.9%)」，「あまりあてはまらない(21.6%)」「あてはまらない(25.9%)」という結果であり，「あまりあてはまらない」，「あてはまらない」という否定的な回答を選択した児童が47.5%と半数に近い割合であった。また，標準偏差は1.14とばらつきがある状態であった。以上のことから学習前の児童は，情報セキュリティの認識について，それらを認識している児童と，そうでない児童のばらつきがあることが示された。

事前の調査結果では，調査項目2「物理的対策」は，平均3.88，調査項目3「人的対策」は平均3.79という結果であった。この要因として，2つの調査項目は，特別の教科道徳で取り上げる「A.主として自分自身に関すること」にかかわっており，日々の生活のモラルとの延長上にあるためと考えられる。一方，調査項目4「技術的対策」の平均は，3.55であり，他の2つの調査項目と比較してやや低い値を示した。これは，技術的対策がインターネット利用時の特有のものであり，日々の生活との関わりが弱いためと考えられる。

事後の調査結果を以下に示す。

調査項目2「物理的対策」は，平均3.99であり，事前調査の値と t 検定(対応あり)をほどこした結果，有意差が見られた($t(138)=2.59$，$p<.05$)。調査項目3「人的対策」の平均

は，3.94であり，事前調査の値と t 検定(対応あり)をほどこした結果，有意差が確認された($t(138)=3.98$, $p<.01$)。また，調査項目4「技術的対策」の調査結果は，3.85であり，事前調査の値と t 検定(対応あり)をほどこした結果，有意差が確認された($t(138)=4.60$, $p<.01$)。

この結果から，3つの項目に有意差がみとめられたため，開発した小学生用情報セキュリティ教材で学習することは，情報セキュリティの認識の有無に関わらず情報セキュリティの意識の向上に効果があることが確認された。物理的対策，人的対策，技術的対策の意識の結果を表4.3に示す。

表4.3　意識の調査結果

		事前		事後	
No.	調査項目	平均	S.D.	平均	S.D.	検定
2.	物的対策	3.88	0.47	3.99	0.12	*
3.	人的対策	3.79	0.48	3.94	0.30	**
4.	技術的対策	3.55	0.77	3.85	0.38	**

*：$p<.05$　**：$p<.01$（$N=139$）

(2) 知識の調査結果

① 人的対策の知識

人的対策の知識に関する事前の正答率は，調査項目B2「ID・パスワード管理」は，90.7%，調査項目B3「個人情報管理」は，87.8%，調査項目B4「ダウンロード」は，75.5%という結果であった。事後の正答率を下記に示す。調査項目B2「ID・パスワード管理」の正答率は，96.4%であった。事前の調査とマクネマー検定をほどこした結果，有意差が確認された($\chi 2(1)=6.13$, $p<.05$)。調査項目B3「個人情報管理」の正答率は，95.7%であった。事前の調査とマクネマー検定をほどこした結果，有意差が確認された($\chi 2(1)=9.09$, $p<.01$)。調査項目B4「ダウンロード」事後の正答率は，83.5%であった。事前の調査とマクネマー検定をほどこした結果，有意差は確認されなかった($\chi 2(1)=3.23$, *n. s.*)。

この結果から，2つの項目に有意差がみとめられたため，開発した小学生用情報セキュリティ教材で学習することは，人的対策の知識の向上に効果があることが確認された。調査項目B4「ダウンロード」については，事前調査で正答であった児童10名が事後調査で誤答になり，データにちらばりがあったため有意差が確認されなかった。この項目については，Web教材の内容や指導の方法をさらに充実させていく必要があると考えられる。人的対策の知識に関する事前・事後の正答率を表4.4に示す。

表4.4　人的対策の知識に関する事前・事後の正答率

No.　調査項目	事前(%)	事後(%)	検定
B2. ID・パスワード管理	90.7	96.4	*
B3. 個人情報管理	87.8	95.7	**
B4. ダンロード	75.5	83.5	*n. s.*

*：p<.05 **：p<.01（N=139）

② 技術的対策の知識

技術的対策の知識に関する事前の調査は，調査項目B5「フィルタリング」は，47.5%，調査項目B6「ウィルス対策ソフトウェア(携帯型情報端末の対応)」は，74.8%，調査項目B6「ウィルス対策ソフトウェア(PCの対応)」は，34.5%，調査項目B7「ソフトウェア更新」は，67.6%という結果であった。

技術的対策の知識に関する事前・事後の結果を表4.5に示す。

表4.5　技術的対策の知識に関する事前・事後の正答率

No.　調査項目	事前(%)	事後(%)	検定
B5. フィルタリング	47.5	52.5	**
B6. ウィルス対策ソフト(携帯型端末対策)	74.8	88.5	**
B6. ウィルス対策ソフト(PC 対策)	34.5	46.0	*
B7. ソフトウェア更新	67.6	77.0	*

*：p<.05 **：p<.01（N=139）

調査項目B5「フィルタリング」の事後の正答率は，52.5%であった。事前の調査とマクネマー検定をほどこした結果，有意差が確認された(χ2(1)=19.45，p<.01)。調査項目B6「ウィルス対策ソフトウェア(携帯型情報端末の対応)」の事後の正答率は，88.5%であった．事前の調査とマクネマー検定をほどこした結果，有意差が確認された(χ2(1)=10.45，p<.01)。調査項目B6「ウィルス対策ソフトウェア(PCの対応)」の事後の正答率は，46.0%であった。事前の調査とマクネマー検定をほどこした結果，有意差が確認された(χ2(1)=4.89，p<.05)。調査項目B7「ソフトウェア更新」の事後の正答率は，77.0%であった。事前の調査とマクネマー検定をほどこした結果，有意差が確認された(χ2(1)=5.33，p<.05)。

この結果から，4つの調査項目に有意差がみとめられたため，開発した小学生用情報セキュリティ教材で学習することは，技術対策の知識の向上に効果があることが確認された。しかし，調査項目B5「フィルタリング」の事後の正答率は52.5%，調査項目B6「ウィルス対策ソフト(PC対策)」の事後の正答率は46.0%であり，教材の内容や指導の方法をさらに充実させていく余地があると考えられる。

③　知識全体の調査結果

事前・事後の情報セキュリティの知識得点の結果を表4.6に示す。情報セキュリティの知識の設問7問に対して正答を1点として集計したところ，事前の得点は平均4.78であった。また，事後の得点の平均は，5.59であった。事前調査の値と t 検定(対応あり)をほどこした結果，有意差が確認された($t(138)=6.26$, $p<.01$)。

授業後の感想には，教材の理解しやすさに関する意見，自分の生活との関わりに関する意見が多くみられた。このことから，小学生用情報セキュリティ教材が小学校高学年の児童の実態に適しており，情報セキュリティの学習の大切さを一斉学習で確認し，個別学習で知識を習得し，その知識を活かした話合い活動によるグループ学習，話合い活動の成果について一斉学習という授業展開が効果的であったためと考えられる。

この結果から，開発した小学生用情報セキュリティ教材を使った1単位時間(45分)の授業をおこなうことにより，小学校高学年で学ぶべき情報セキュリティ全体の知識を高めることに効果が示されたと考えられる。

表4.6　知識全体の事前・事後の得点

	事前		事後		
	平均	S.D.	平均	S.D.	検定
知識得点	4.78	1.61	5.59	1.14	**

**：$p<.01$ (N=139)

1.5　おわりに

小学生用情報セキュリティ教材を活用した授業の効果の検証をおこなった結果を以下にまとめる。

1. 開発した小学生用情報セキュリティ教材で学習することは，情報セキュリティの認識の有無に関わらず情報セキュリティの意識の向上に効果があることが確認された。
2. 開発した情報セキュリティ教材で学習することは，人的対策の知識の向上に効果があることが確認された。
3. 調査項目B4「ダウンロード」については，事前調査で正答であったが，事後調査で誤答になった児童がいた。Web教材の内容や指導の方法をさらに充実させていく必要がある。
4. 開発した小学生用情報セキュリティ教材を利用した学習は，1単位時間(45分)という短時間の授業で，小学校高学年に必要な情報セキュリティの技術的対策の理解につながることが確認された。
5. 「B5.フィルタリング」の事後の正答率は52.5%，「B6.ウィルス対策ソフト(PC対策)」の事後の正答率は46.0%であり，教材の内容や指導の方法をさらに充実させていく余地があると考えられる。

以上の結果より，開発した小学生用情報セキュリティの教材を活用した授業を１単位時間（45分）おこなうことにより，小中高等学校における体系的な情報セキュリティ教育の視点からとらえた小学校高学年に必要な情報セキュリティの技術的対策への意識の高まりと理解に一定の効果が示された。

第2節　中学校における授業実践

2.1 はじめに

第3章2節で開発した中学生用情報セキュリティ教材の効果を図るため，中学校において授業実践をおこなった。

中学校の技術・家庭科(技術分野)における授業実践は，2020年9月，2021年7月にA県内2校の2年生3クラス(95名)，3年生2クラス(40名)の計135名を対象に実施した[注3)]。なお，技術・家庭科の授業は，題材を指導する学年を各学校で決めるため，実践校の年間指導計画に合わせて2年生と3年生で実施した。

授業形態は，一斉学習，グループ学習，個別学習の3つの形態を取り入れた。一斉学習は，授業の導入時に授業のねらいと教材の利用法を全員で確認し，授業の終末で，学習の成果を伝え合い，クラス全体の多様な意見を知るのに有効である。グループ学習は，少人数での話合いで課題を解決することにより，情報セキュリティに関して主体的に考え，他の意見を取り入れながら方向性を導きだすことができる。個別学習は，一人一台端末で教材を活用することで，一人一人の生徒の実態にあった学習が可能になる。

2.2 指導目標および授業の展開

授業実践は，担当教諭との話合いのもと，1単位時間（50分）で実施した。

指導目標は，「生活に必要な情報セキュリティ対策を考えよう」とした。授業の様子を図4.2に示す。

図4.2 授業の様子

授業は，開発したオンライン教材を利用しておこなった。授業の展開として，「1.身近にひそむ危険」，「2.情報セキュリティ対策」，「3.情報セキュリティの課題解決」の３つの内容で実施した。授業の具体的な指導内容と活用した開発教材，生徒の反応を以下に示す。

(1) 身近にひそむ危険

「1.身近にひそむ危険」では，情報セキュリティの必要性について，情報セキュリティ対策を講じなかった時のWebサイト，SNS，電子メールを利用のトラブル事例を基に情報セキュリティの必要性について学習した。はじめに教師からオンライン教材の概要と利用方法を説明した。利用方法を説明するにあたり，開発した教材の「1.1 Webサイト」を教師用端末から大型画面に提示し，一斉学習をおこなった。次に，一人一台端末を利用し，「1.2 SNS」，「1.3 電子メール」について個別学習をおこなった。

(2) 情報セキュリティ対策

「2.情報セキュリティ対策」は，一人一台端末を利用し，個別学習で学習をおこなった。

評価基準は，「情報セキュリティを確保するために必要な技術と対応方法を知る。」とした。

学習内容は，「情報漏えいを防ぐ」，「不正プログラムを防ぐ」，「不正な侵入を防ぐ」，「最新の情報セキュリティ対策」の 4 つである。

机間支援の中で，最新の情報セキュリティの技術や普段利用しているスマートフォンの情報セキュリティの問題点についての個別の質問があった。

(3) 情報セキュリティの課題解決

「3.情報セキュリティの課題解決」では，教師から与らえた課題についてグループで話合いをおこなった。次にグループの話合いの結果をクラス全体で発表させ，意見交換をおこなった。なお，グループ学習は，各授業で3～4名のグループを編成した。

評価基準は，「既存の知識を活用し，情報セキュリティ上の課題を発見し，対応策を考える」とした。

クラス全体の発表では，自分のトラブルの経験をふまえながら，IDやパスワードの知識の重要性に関する意見やこれから情報端末をどのように使っていくべきかなど意識の変化や行動の変容につながる意見が見られた。

また，授業後の感想では，日常使っているインターネットの危険性，情報セキュリティ対策の重要性，オンライン教材を使った学習の効果に関する意見が見られた。

2.3 調査項目および分析方法

本実践対象者のうち，欠席および回答に不備のあった 8名を分析から除外した 。その結果，有効回答数は127名，有効回答率は 94.1%であった。情報セキュリティの知識の調査項目を表4.9に示す。調査項目は，第2章で前述した中学校修了段階の調査結果をふまえて，情報セキュリティ対策の必要性の意識と情報セキュリティの知識の2種類を作成した。

表4.9　情報セキュリティの知識の調査項目と選択肢

1.不正侵入を防ぐ技術

a01.コンピュータウィルスのネット上の感染経路の説明として，最も適切なものはどれか。
（リンクの対応）

ア.ネットを通じていても友人から受け取っているのなら感染しない
イ.ホームページを見ただけでウィルス感染することもある(※正答)
ウ.PCではウィルスが多く出回っているが，スマホのウィルスはない
エ.言葉や内容の意味がわからない

a02.ファイアウォールの役割として最も適切なものはどれか。（ファイアウォール）

ア.外部のネットワークからの不正な侵入を防ぐ(※正答)
イ.データの破損を防ぐ
ウ.個人情報を守る
エ.言葉や内容の意味がわからない

a03.スマホで使用するアプリの説明の中には，個人情報を登録するアプリもある。
この説明として，最も適切なものはどれか。（アカウント管理）

ア.ダウンロードする前にアクセス許可設定などを確認したほうが良い(※正答)
イ.無料でも役にたつアプリが多いので，すべて利用して問題ない
ウ.アプリマーケット上のアプリは信頼性･安全性は高いので安心して良い
エ.言葉や内容の意味がわからない

2.コンピュータウィルスに対する技術

a04.コンピュータウィルスからＰＣを守る対策として最も適切なものはどれか。（ソフトウェア更新）

ア.ウィルス対策ソフトウェアを入れる
イ.特に対策をする必要はない，
ウ.ウィルス対策ソフトウェアを入れ，ソフトウェアやOSを最新の状態に更新する(※正答)
エ.言葉や内容の意味がわからない

a05.スマホのセキュリティ対策ソフトを利用することで，対応できることはどれか。
（セキュリティ対策ソフトウェア）

ア.不正なアプリの監視(正答)
イ.アプリの新規インストールの禁止
ウ.Wi-Fiを利用したインターネット接続の禁止
エ.言葉や内容の意味がわからない

3.データの故障や安全に関する技術

a06.自分で作成したデータをUSBメモリに保存する時，安全対策としてやるべきものとして最も適切なものはどれか。（バックアップ）

ア.暗号化する
イ.暗号化し，バックアップをとる(※正答)
ウ.特に対策する必要はない
エ.言葉や内容の意味がわからない

4.違法・有害情報に関する技術

a07.携帯ゲーム機を利用する際に気を付けることとして，最も適切なものはどれか。(フィルタリング)

ア.携帯ゲーム機であれば個人情報がネットに流れる心配はない
イ.携帯ゲーム機でネット接続する時はフィルタリングを設定するべきである(※正答)
ウ.携帯ゲーム機のネットワークは子供用に設計されているので安全である
エ.言葉や内容の意味がわからない

5. 情報を安全に送受信する技術

a08.URL の先頭に「https:」のついているWebページの意味として適切なものはどれか。（暗号化）

ア.鍵がかかっており安全なWebページである(※正答)
イ.安全とも危険ともいえないWebページである
ウ.情報を盗まれる可能性の高いWebページである
エ.言葉や内容の意味がわからない

6. ID・パスワード管理

a09.インターネット上で自分の IDとパスワードを他人に教えるだけで簡単にお金がもらえる方法があると友人から聞いた。次の中で適切なものはどれか。（ID・パスワード）

ア.もらえる金額が高額であれば，やってみてもいい
イ.もらえる金額が少額であれば，問題はない
ウ.いくらお金がもらえるとはいえ，他人に IDやパスワードを教えてはいけない(※正答)
エ.言葉や内容の意味がわからない

情報セキュリティ対策の必要性の意識の設問は，第2章で前述した中学校修了段階の意識の調査結果をもとに物理的対策，人的対策，技術的対策の3項目で作成し，4件法で回答を求めた。4件法で回答を求めたものは，「思う」を4点，「少し思う」を3点，「あまり思わない」を2点，「思わない」を1点とし，得点化し平均と標準偏差を求め，統計処理をほどこした。情報セキュリティの必要性の調査項目は，物理的対策が，「スマホやパソコンなどは，なくさないように管理しようと思いますか」，人的対策が，「インターネットを使う時は，安全を考えて利用しようと思いますか」，技術的対策が，「スマホやパソコンには，フィルタリングやウィルス対策などの安全対策をしようと思いますか」とした。

情報セキュリティの知識の設問は，第2章で前述した中学校修了段階の知識の調査結果をもとに「1.不正侵入を防ぐ技術(1)～(3)」，「2.コンピュータウィルスに対する技術(1)(2)」，「3.データの故障や障害に関する技術」，「4.違法・有害情報に関する技術」，「5.情報を安全に送受信する技術」，「6.ID・パスワード管理」の6つの調査項目，計9問を作成した。

設問は，中学校で利用されている中学校の技術・家庭科(技術分野)の3社の教科書で共通して取り上げている内容とした。設問は，4つの選択肢の中から正しい回答を選ぶ選択式の設問とした。分析は，各設問の事前・事後に正答・誤答に対して，マクネマー検定を実施した[注4)]。

本調査は，事前に学校長および授業者に，実態調査の了解をえたうえでおこなった。また，生徒には，倫理的配慮として，使用目的，および研究用途以外には用いないこと，個人が特定されないように配慮することを説明した。

2.4 調査結果

(1) 情報セキュリティ対策の意識

事前・事後の物理的対策，人的対策，技術的対策の「情報セキュリティ対策の意識」の調査結果を表4.10に示す。

表4.10　情報セキュリティ対策の必要性の意識の調査結果

		事前		事後		
No.	調査項目	平均	S.D.	平均	S.D.	検定
1.	物的対策	3.89	0.40	3.98	0.15	**
2.	人的対策	3.86	0.39	3.98	0.15	**
3.	技術的対策	3.63	0.60	3.93	0.26	**

**：$p<.01$（$N=127$）

「情報セキュリティ対策の意識」の事前調査結果の平均は，調査項目1「物的対策」は，3.89，調査項目2「人的対策」は，3.86，調査項目3「技術的対策」は，3.63であった。すべての調査項目で高い値を示したが，技術的対策については，他の2つの調査項目と比較するとやや低い値を示した。

事後調査の結果を下記に示す。調査項目1「物理的対策」の事後調査の結果は，3.98であり，事前調査の値とt検定(対応あり)をほどこした結果，有意差が確認された($t(126)=2.23$，$p<.01$)。調査項目2「人的対策」の事後調査の結果は，3.98であり，事前調査の値とt検定をほどこした結果，有意差が確認された($t(126)=3.25$，$p<.01$)。また，調査項目3「技術的対策」の事後調査の結果は，3.93であり，事前調査の値とt検定をほどこした結果，有意差が確認された($t(126)=5.54$，$p<.01$)。

授業後の生徒の感想には，「いろいろなケースに対応した行動手段が知れ，安全意識が高まった」と類似した意見が複数確認された。このことは，開発した情報セキュリティ教材を利用して学習することで，知識に裏打ちされた意識に変容していくことを示しているものと考えられる。

(2) 情報セキュリティの知識

情報セキュリティの知識の事前・事後の正答率を表4.11に示す。

表4.11　項目別の知識の事前・事後の正答率

No.　調査項目	事前(%)	事後(%)	検定
＜1.不正侵入を防ぐ技術＞			
a01.リンクの対応	92.1	95.3	*n. s.*
a02.ファイアウォール	66.9	81.9	**
a03.アカウント管理	93.7	99.2	*
＜2.コンピュータウィルスに対する技術＞			
a04.ソフトウェア更新	57.5	70.1	*
a05.セキュリティ対策ソフトウェア	75.6	81.1	*n. s.*
＜3.データの故障や障害に関する技術＞			
a06.バックアップ	70.1	80.3	**
＜4.違法・有害情報に関する技術＞			
a07.フィルタリング	88.2	96.1	**
＜5.情報を安全に送受信する技術＞			
a08.暗号化	55.1	71.7	**
＜6.ID・パスワード管理＞			
a09.ID・パスワード	96.9	98.4	*n. s.*

*：$p<.05$ **：$p<.01$ (N=127)

情報セキュリティの知識の事前調査の正答率は，調査項目a01「リンクの対応」が，92.1%，調査項目a03「アカウント管理」が，93.7%，調査項目a07「フィルタリング」

は，88.2%，調査項目a09「ID・パスワード」は，96.9%と4つの調査項目については，80%以上の正答率であった。一方，調査項目a02「ファイアウォール」は，66.9%，調査項目a04「ソフトウェア更新」は，57.5%，調査項目a05「セキュリティ対策ソフトウェア」は，75.6%，調査項目a06「バックアップ」は，70.1%，調査項目a08「暗号化」は，55.1%と，5つの調査項目の正答率は，80%以下であった。この5つの調査項目の知識は，前述の4つの調査項目と比較すると充分な知識が身についていない実態が確認され，適切な指導が必要なことが示された。

事後調査の結果を下記に示す。「1.不正侵入を防ぐ技術」は，調査項目a01「リンクの対応」，調査項目a02「ファイアウォール」，調査項目a03「アカウント管理」の3つの調査項目について調査をおこなった。調査項目a01「リンクの対応」の事後調査の正答率は95.3%であり，事前調査の値とマクネマー検定をほどこした結果，有意差が確認されなかった($\chi 2(1)=2.25$，$n.s.$)。調査項目a02「ファイアウォール」の事後調査の正答率は，81.9%であり，事前調査の値とマクネマー検定をほどこした結果，有意差が確認された($\chi 2(1)=17.05$，$p<.01$)。調査項目a03「アカウント管理」の事後の正答率は，99.2%であり，事前調査の値とマクネマー検定をほどこした結果，有意差が確認された($\chi 2(1)=5.14$，$p<.05$)。

この結果から，「1.不正侵入を防ぐ技術」に関する知識の習得には，学習効果があると示された。また，第2章で前述した中学校修了時の課題である「情報セキュリティを確保する仕組み」の知識の習得に有効であることが示された。その理由として，開発した教材では，単なる単語だけでなく情報セキュリティの技術的な仕組みや具体的な方法を学んだためと考えられる。

「2.コンピュータウィルスに対する技術」は，調査項目a04「ソフトウェア更新」，調査項目a05「セキュリティ対策ソフトウェア」の2つの調査項目について調査をおこなった。調査項目a04「ソフトウェア更新」の事後の正答率は70.1%であり，事前調査の値とマクネマー検定をほどこした結果，有意差が確認された($\chi 2(1)=6.62$，$p<.05$)。調査項目a05「セキュリティ対策ソフトウェア」の事後調査の正答率は，81.1%であった。事前調査の値とマクネマー検定をほどこした結果，事前調査で正答であった生徒3名が事後調査で誤答になりデータにちらばりがあったため有意差が確認されなかった($\chi 2(1)=2.77$，$n.s.$)。

この結果から，「2.コンピュータウィルスに対する技術」に関する知識の習得には，学習効果があると示された。第2章で前述した中学校修了時の課題として，コンピュータウィルスへの対応力を高めるためにソフトウェア更新を理解する必要性が示されたが，本教材を使った学習はこの課題の解決につながるものと考えられる。

「3.データの故障や障害に関する技術」は，調査項目a06「バックアップ」についての調査をおこなった。事後調査の正答率は80.3%であり，事前調査の値とマクネマー検定をほどこした結果，有意差が確認された($\chi 2(1)=9.60$，$p<.01$)。第2章で前述した中学校修

了時の課題として，コンピュータウィルスへの対応力を高めるためにデータ保護について理解する必要性が示されたが，本教材を使った学習はデータのバックアップの必要性の理解につながるものと考えられる。

「4.違法・有害情報に関する技術」は，調査項目a07「フィルタリング」について調査をおこなった。事後調査の正答率は96.1%であり，事前調査の値とマクネマー検定をほどこした結果，有意差が確認された($\chi 2(1)=8.10$, $p<.01$)。第2章で前述した中学校修了時の課題である「情報セキュリティを確保する仕組み」の理解の促進につながっていくことが示された。

「5.情報を安全に送受信する技術」は，「a08.暗号化」について調査をおこなった。事後調査の正答率は71.7%であり，事前調査の値とマクネマー検定をほどこした結果，有意差が確認された($\chi 2(1)=13.79$, $p<.01$)。「a08.暗号化」は，今回調査した9つの調査項目の中で事前の調査結果の正答率が最も低い項目であったが，事後調査で，正答率が，16.6%高く有意差が確認された。このことは，開発したオンライン教材を活用した学習が効果的であったためと考えられる。

「6.ID・パスワード管理の技術」は，「a09.ID・パスワード」についての調査をおこなった。事後調査の正答率は98.4%であり，事前調査の値とマクネマー検定をほどこした結果，有意差が確認されなかった($\chi 2(1)=0.5$, $n.s$)。これは，事前の正答率が96.89%と高かったためと考えられる。しかし,正答率は，1.5%高まっており，教材の効果があったと推測できる。第2章で前述した中学校修了時の課題であったID・パスワードの知識については，80%を超える正答率であったため，本教材を使った学習により，技術・家庭科（技術分野）の指導上の課題に対して克服につながると考えられる。

これらの結果は，１時間という限られた時間の中で，本教材を活用して技術・家庭科(技術分野)の学習をおこなうことで，技術・家庭科(技術分野)で学ぶべき，情報セキュリティの理解の促進につながっていくことが示されたものと考える。

2.5 おわりに

技術・家庭科(技術分野)の授業で活用できる情報セキュリティ教材の効果の検証結果をまとめる。

1. 授業の事前事後の意識調査の結果や生徒の感想から，開発した教材で授業をおこなうことにより，情報セキュリティ対策の必要性の意識が，知識に裏付けられた意識に変容していくことが確認された。
2. 「1.不正侵入を防ぐ技術」に関する知識の習得には，学習効果があると示された。第2章で前述した中学校修了時の課題である「情報セキュリティを確保する仕組み」の知識の習得に有効であることが示された。
3. 「2.コンピュータウィルスに対する技術」に関する知識の習得には，学習効果があると示された。第2章で前述した中学校修了時の課題として，コンピュータウィルスへの

対応力を高めるためにソフトウェア更新を理解する必要性が示された。

4. 開発した教材での学習は，1単位時間（50分）という限られた授業で，学習指導要領で示された技術・家庭科(技術分野)で学ぶべき情報セキュリティ知識を高めることにつながることが確認された。また，生徒の実態調査で明らかになった「ファイアウォール」についても知識の正答率が，66.9%から81.9%に高まった。

以上の結果より，前述の 5 つの開発要件をふまえて作成した情報セキュリティ教材は，技術・家庭科(技術分野)の学習で活用することにより 1 単位時間（50 分）という限られた時間の中で，小・中学校における体系的な情報セキュリティ教育の視点からとらえた中学校の情報セキュリティの理解の促進と，それらに関する意識の向上が確認された。しかし，生徒の事後の感想に，「自分でどのくらいできるようになったかを確認したい」といった個別の変容を確認する機能への要望があった。本教材は，技術・家庭科（技術分野）の教科学習で利用する教材であることから，今後は，教材に「振り返りテスト」などの自己評価機能を取り入れていく必要があると考える。また，授業実践は，「一斉学習→個別学習→グループ学習→一斉学習」という学習形態を組み合わせた学習過程でおこなったが，他の学習過程のパターンを試すなどして，開発教材を使ったさらなる効果的な指導方法の検討の必要がある。

２．結言

本章では，第3章において開発した教材を用いた授業を検討し，授業実践を通して児童・生徒に育まれる能力に関する調査と分析をおこなった。以下に結果をまとめる。

(1) 小学校

① 開発した小学生用情報セキュリティ教材で学習することは，情報セキュリティの認識の有無に関わらず情報セキュリティの意識の向上に効果があることが確認された。

② 開発した情報セキュリティ教材で学習することは，人的対策の知識の向上に効果があることが確認された。

③ 調査項目B4「ダウンロード」については，他の2つの調査項目と比較して事前・事後ともに正答率が低いため，Web教材の内容や指導の方法をさらに充実させていく必要がある。

④ 開発した情報セキュリティの教材を利用した学習は，1単位時間という短時間の授業で，小学校高学年に必要な情報セキュリティの技術的対策の理解につながることが確認された。

⑤ 「B5.フィルタリング」の事後の正答率は52.5%，「B6.ウィルス対策ソフト(PC対策)」の事後の正答率は46.0%であり，教材の内容や指導の方法をさらに充実させていく余地があると考えられる。

(2) 中学校

① 授業の事前事後の意識調査の結果や生徒の感想から，開発した教材で授業をおこなうことにより，情報セキュリティ対策の必要性の意識が，知識に裏付けられた意識に変容していくことが確認された。

② 「1.不正侵入を防ぐ技術」に関する知識の習得には，学習効果があると示された。第2章で前述した中学校修了時の課題である「情報セキュリティを確保する仕組み」の知識の習得に有効であることが示された。

③ 「2.コンピュータウィルスに対する技術」に関する知識の習得には，学習効果があると示された。第2章で前述した中学校修了時の課題として，コンピュータウィルスへの対応力を高めるためにソフトウェア更新を理解する必要性が示された。

④ 開発した教材での学習は，1単位時間（50分）という限られた授業時間の中で，学習指導要領で示された技術・家庭科(技術分野)で学ぶべき情報セキュリティの知識を高めることにつながることが確認された。また，生徒の実態調査で明らかになった「ファイアウォール」についても知識の正答率が，66.9%から81.9%に高まった。

小学校の高学年の授業実践では，開発した教材を活用し学習することで，1単位時間（45分）の授業で，技術的セキュリティへの意識の高まりと小学校高学年に必要な情報セキュリティの技術的対策の理解につながることが確認された。

中学校の技術・家庭科(技術分野)の授業実践では，1単位時間（50分）の授業で，情報セキュリティ対策の必要性の意識が，知識に裏打ちされたものに変容していき，技術・家庭科(技術分野)で学ぶべき情報セキュリティの理解につながることが確認された。

以上のことから，開発した教材を活用した学習をおこなうことで，1単位時間という限られた時間の授業で，小学校および中学校の各発達段階にあった情報セキュリティの意識と情報セキュリティの理解を促す可能性が示唆された。

本章で活用した教材は，小・中学校における体系的な情報セキュリティ教育を想定し開発しているため，本教材を各学校段階で活用し学習をおこなうことで，小・中学校で必要な情報セキュリティの能力を着実に身に付けていくことができるものと考えられる。

授業実践は，一斉学習→個別学習→グループ学習→一斉学習という学習形態を組み合わせた学習過程でおこなったが，他の学習過程のパターンを試すなどして，開発教材を使ったさらなる効果的な指導方法の検討の必要がある。

本実践で活用した指導案，ワークシートなどの教材などを加えたパッケージ化した授業資料を提供し，多くの学校での本教材が活用できる環境を整えていきたい。また，情報セキュリティを確保するための行動の変容に関する追跡調査が必要である。

次章では，本実践で得た知見をまとめるとともに，今後の情報セキュリティ教育を実践するための提案をおこなう。

参考文献

132)前掲103)，pp.695-702(2019)

133)前掲104)，pp.111-112(2019)

134)堤健人・川田和男：協働的問題解決を取り入れた技術科の授業実践，広島大学附属東雲中学校 中学教育 研究紀要47巻，pp.55-60(2016)

関係論文

１)小熊良一・山本利一：小学校高学年における情報セキュリティWeb教材開発と授業実践，教育方法研究，第37巻，第1号，pp.53-62(2021)

２)小熊良一・山本利一：中学校技術・家庭科(技術分野)における「情報セキュリティ」のオンライン教材の開発と授業実践，日本産業技術教育学会誌，第 63 巻,第 4 号，pp.39-48(2021)

第5章 結言

5.1 本研究で得られた知見の整理

本研究の目的は，小・中学校における情報セキュリティ教育に焦点をあて，指導者である教員の実態を踏まえ，小・中学校修了段階の意識と知識を調査し，小・中学校における情報セキュリティ教育の課題と現状を明らかにするとともに，児童・生徒の情報セキュリティの意識と知識を高めるための教材を開発し，効果的な指導の在り方を提案することである。

第1章では，情報セキュリティの概念や日本の初等中等教育における情報セキュリティの歴史の整理，先行研究の調査をおこない，小・中学校で現在おこなわれている情報セキュリティ教育の現状を整理し，課題の所在を明らかにした。

第2章では，教員の情報セキュリティの実態を調査し，調査で得た知見を基に，小・中学校修了段階での情報セキュリティに関する実態を調査した。

第3章では，小学校高学年および中学校技術・家庭科(技術分野)で活用できる情報セキュリティの教材開発をおこなった。

第4章では，開発した教材を用いた授業実践を通して，教材及び指導の効果を検証した。各章で得られた知見を以下に整理する。

5.2 第1章のまとめ

第1章では，情報セキュリティの概念や日本の初等中等教育における情報セキュリティの歴史の整理，先行研究の調査をおこない，小・中学校で現在おこなわれている情報セキュリティ教育を整理し，課題の所在を明らかにした。

文部科学省は，小学校低学年で「情報の大切さ」，小学校中学年で「情報を守ることの大切さ」，小学校高学年で「情報セキュリティの基本と生活の中で必要な基本的な情報セキュリティ対策」のように発達段階にあわせた情報セキュリティ教育の概要を示している。しかし，情報セキュリティを指導する教科や具体的な指導内容が示されていないため，具体的な情報セキュリティ教育は各学校に任されている。

中学校では，サイバーセキュリティを含んだ情報セキュリティ対策の仕組や具体的な対策・対応を技術・家庭科(技術分野)で学ぶことになる。なお，初等中等教育における情報セキュリティの指導は高等学校での指導が出口とされており，高等学校では，「情報Ⅰ」ですべての生徒が学ぶことになる。

次に，学校に関する情報セキュリティの研究を調査した。調査の結果，教員が，業務の中で，情報セキュリティを守るための方策やシステムの研究が多く，児童・生徒の情報セキュリティを確保する能力を高めるための研究が不足していることがわかった。

今後の情報セキュリティに関する研究としては，「小学校学習指導要領(平成29年告

示)」，「中学校学習指導要領(平成29年告示)」で目指す指導内容をふまえ，指導する教員の実態，小・中学校修了段階での実態を調査し，調査に即した教材開発と授業実践を行い，その効果を示す必要があることを明らかにした。

5.3 第2章のまとめ

第2章では，小・中学校に勤務する教員の実態調査をおこない，その知見を基に小・中学校修了段階の児童・生徒に情報セキュリティに関する実態調査をおこなった。以下に本章で得られた小・中学校修了段階における情報セキュリティ教育についての知見をまとめる。

(1) 小・中学校教員の実態

① 小・中学校に勤務する教員は，学校において情報セキュリティを確保することが大切であると認識している。

② 情報セキュリティを確保するために物理的対策，人的対策，技術的対策をおこなうことの重要性は認識しているものの，実際の行動にむすびついていない傾向がある。

③ 情報セキュリティの知識と行動には，相関関係があると推測され，情報セキュリティの知識を高めることで，情報セキュリティを確保する行動につながる可能性がある。

(2) 小学校修了段階の実態

① 小学生のインターネットの利用は日常的なものとなっており，ゲーム機や個人用のスマートフォンを利用している。

② 小学校での情報セキュリティ教育の経験は40%程度で，すべての児童が学習していると認識していない。

③ 小学生の情報セキュリティの意識として技術的対策の意識に低い傾向がある。

④ 小学生の情報セキュリティの知識については，物理的対策と人的対策の知識は，ある程度身に付いているが，技術的対策についての知識は不足している。

⑤ 情報セキュリティの意識と知識は密接に関係しており，意識の高い対策については，情報セキュリティの学習をすることで知識を習得し，意識の低い対策については，情報セキュリティの学習により知識を習得することで，意識が高まり，行動の変容につながっていくと考えられる。

(3) 中学校修了段階の実態

① 中学生に対しては，携帯型情報端末の利用をふまえた情報セキュリティ教育が必要である。

② メッセンジャーアプリ，インターネット検索，音楽鑑賞，ゲーム，動画視聴など中学生の実態をふまえた情報セキュリティ教育が必要である。

③ 情報セキュリティを含む情報モラルの学習機会は，「学校の集会」と「技術・家庭科（技術分野）の授業」が中心であり，「技術・家庭科（技術分野）以外の授業」の学習経験はわずか12.5%である。

④ 調査対象者の75.5%が，インターネットの適切な利用に対して肯定的に回答している。
⑤「アカウント管理」，「セキュリティ対策ソフトウェア」，「ID・パスワード」など人的対策の知識はある程度もちあわせているが，技術的対策の知識である「ファイアウォール」に課題がある。このことは，「技術・家庭科（技術分野）」の指導に改善の余地があることを示している。

これらの実態から見えた課題を解決し情報セキュリティ教育を充実させるためには，小学校および中学校において，それぞれ異なる対策が必要である。

小学校では，特定の免許をもつ教員だけでなくすべての教員が情報セキュリティ教育をおこなうことが想定される。そのため，情報セキュリティの教育内容を具体的に示し，すべての教員が情報指導できる教材や指導方法が必要である。

中学校では，技術・家庭科「技術分野」の情報セキュリティ教育を限られた時間の中で効果的に指導する教材や指導方法が必要である。

5.4 第 3 章のまとめ

第3章では，小学校高学年および中学校技術・家庭科(技術分野)で活用できる情報セキュリティの教材の開発をおこなった。教材を開発するにあたり，文部科学省が示す目標をふまえて，小学校高学年および中学校技術・家庭科(技術分野)で学ぶべき情報セキュリティの指導内容を明確にし，教材を開発した。以下に第3章での成果を整理する。

① 小学校の情報セキュリティ教育の内容を「情報モラル指導モデルカリキュラム表」，「情報活用能力の体系表例」から「A1.情報セキュリティの原則」，「A2.身近にある情報」，「A3.インターネットにおける情報」，「B1.情報端末・外部媒体の管理」，「B2.個人情報管理」，「B3.ID・パスワード管理」，「B4.ダウンロード」，「B5.フィルタリング」，「B6.ウィルス対策ソフトウェア」，「B7.ソフトウェア更新」の10個の指導内容を摘出した。
② 中学校における情報セキュリティの指導内容を「情報モラル指導モデルカリキュラム表」，「情報活用能力の体系表例」，「中学校学習指導要領(平成29年告示)解説 技術・家庭編」から「a1.リンクの対応」，「a2.ファイアウォール」，「a3.アカウント管理」，「a4.ソフトウェア更新」，「a5.ウィルス対策ソフトウェア」，「a6.バックアップ」，「a7.フィルタリング」，「a8.暗号化」，「a9.ID・パスワード」，「a10.生体認証」，「a11.多要素認証」，「a12.パスワード作成・管理技術」，「b.サイバー空間における情報セキュリティの被害とその対応」，「c.生活の中で想定されるトラブルへの対応」，「d.コンピュータウィルスの感染，ハッキング等による被害事例とその対応」の15個を摘出した。
③ 「情報モラル指導モデルカリキュラム表」，「情報活用能力の体系表例」の小学校高

学年の内容を網羅し，児童の実態をふまえた5つの開発要件に従い小学校高学年用情報セキュリティ教材を作成した。

④ 「情報モラル指導モデルカリキュラム表」，「情報活用能力の体系表例」の中学校の内容，技術・家庭科(技術分野)の指導内容，生徒の実態をふまえた7つの開発要件に従い中学生用情報セキュリティ教材を作成した。

5.5 第 4 章のまとめ

第4章では，開発した教材を用いた授業実践を通して，教材の効果を検証した。以下に得られた知見を整理する。

(1) 小学校

① 開発した小学生用情報セキュリティ教材で学習することは，情報セキュリティの認識の有無に関わらず情報セキュリティの意識の向上に効果があることが確認された。

② 開発した情報セキュリティ教材で学習することは，人的対策の知識の向上に効果があることが確認された。

③ 調査項目「B4.ダウンロード」については，他の2つの調査項目と比較して事前・事後ともに正答率が低いため，Web教材の内容や指導の方法をさらに充実させていく必要がある。

④ 開発した情報セキュリティ教材を利用した学習は，1単位時間(45分)という限られた授業で，小学校高学年に必要な情報セキュリティの技術的対策の理解につながることが確認された。

⑤「B5.フィルタリング」の事後の正答率は52.5%，「B6.ウィルス対策ソフト(PC対策)」の事後の正答率は46.0%であり，教材の内容や指導の方法をさらに充実させていく余地があると考えられる。

(2)中学校

① 授業の事前事後の意識調査の結果や生徒の感想から，開発した教材で授業をおこなうことにより，情報セキュリティ対策の必要性の意識が，知識に裏付けられた意識に変容していくことが確認された。

② 「1.不正侵入を防ぐ技術」に関する知識の習得には，学習効果があることが示された。第2章で前述した中学校修了時の課題である「情報セキュリティを確保する仕組み」の知識の習得に有効であることが示された。

③ 「2.コンピュータウィルスに対する技術」に関する知識の習得には，学習効果があることが示された。第2章で前述した中学校修了時の課題として，コンピュータウィルスへの対応力を高めるためにソフトウェア更新を理解する必要性が示された。

④ 開発した情報セキュリティ教材を利用した学習は，1単位時間（50分）という限られた授業で，学習指導要領で示された技術・家庭科(技術分野)で学ぶべき情報セキュリティの知識を高めることにつながることが確認された。また，生徒の実態調査で明ら

かになった「ファイアウォール」についても知識の正答率が，66.9%から81.9%に高まった。

以上の知見から，指導事項や指導する教科等が各学校の裁量にまかされている小学校，限られた学習時間の中で実施される中学校技術・家庭科(技術分野)の学習において，開発した教材を利用して授業を展開することで，情報セキュリティに対する意識の向上と情報セキュリティを確保するための理解につながる効果をみとめることができた。これらのことから本研究により開発した情報セキュリティ教材は，小・中学校における情報セキュリティ教育に有用な教材であることを検証できた。図5.1に本研究によって得られた知見を示す。

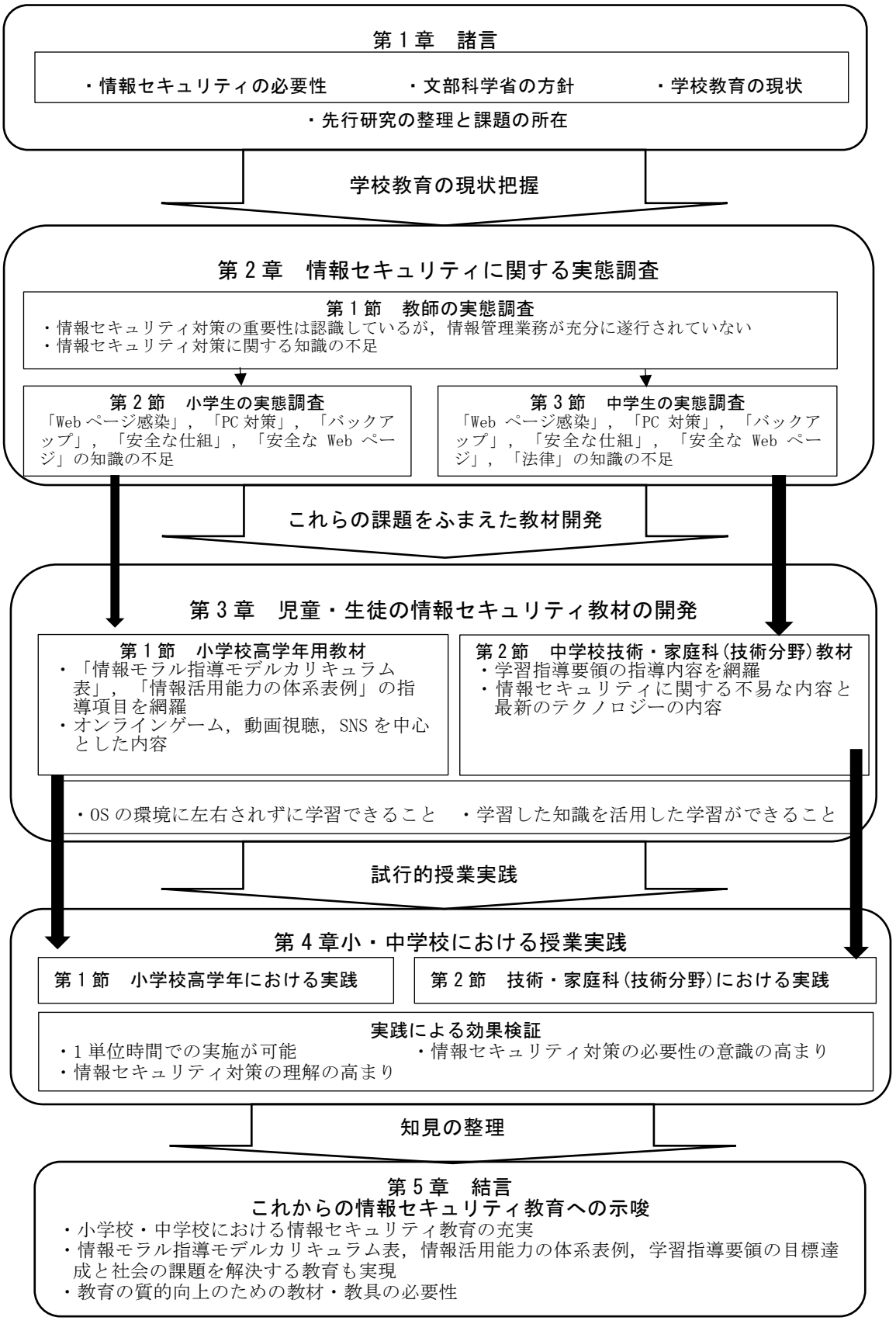


図5.1 本研究によって得られた知見

5.6 本研究で得られた成果に基づく教育実践への示唆

本研究から得られた成果および結論から，小・中学校における情報セキュリティを充実させるための教育実践への示唆を以下にまとめる。

文部科学省は，小学校低学年・小学校中学年・小学校高学年・中学校・高等学校の5つの発達段階にあわせた情報セキュリティ教育の目標を示している。しかし，小学校における情報セキュリティ教育は，具体的な指導内容や指導教科が定められていないため学校や教師の努力に依存している。また，中学校においては，情報セキュリティを指導する中心の教科である技術・家庭科（技術分野）の指導時間が不足していることが示された。小学校における情報セキュリティの指導内容と指導教科を明確にし，中学校の技術・家庭科（技術分野），高等学校の教科「情報」での学びを体系的にとらえた学校現場における指導の充実が求められる。

本研究では，小・中学校に勤務する教員及び小学校修了段階の児童の実態，中学校修了段階の生徒の実態を調査した。小・中学校に勤務する教員の実態として，情報セキュリティを確保することが大切であると認識しているものの，知識が不足しており，実際の行動にむすびついていない傾向があることが示された。小・中学校の教員は，本研究によって明らかになった教員の実態を踏まえて，教員の知識を高め，物理的対策，人的対策，技術的対策の行動につなげていくとともに情報セキュリティの知識と行動を背景とした指導力を身に付ける必要がある。また，小学校修了段階の児童の実態として，物理的対策と人的対策の知識はある程度身に付いているが，技術的対策についての知識は不足していることが示された。中学校においては，技術・家庭科（技術分野）で指導している技術的対策の知識である「ファイアウォール」に課題があり，指導に改善の余地があることが示された。本研究では，この調査結果と文部科学省が示す体系的な情報セキュリティの目標を踏まえ，小学校の指導内容を「A1.情報セキュリティの原則」，「A2.身近にある情報」，「A3.インターネットにおける情報」，「B1.情報端末・外部媒体の管理」，「B2.個人情報管理」，「B3.ID・パスワード管理」，「B4.ダウンロード」，「B5.フィルタリング」，「B6.ウィルス対策ソフトウェア」，「B7.ソフトウェア更新」の10個の指導内容を摘出した。また，中学校の指導内容を「a1.リンクの対応」，「a2.ファイアウォール」，「a3.アカウント管理」，「a4.ソフトウェア更新」，「a5.ウィルス対策ソフトウェア」，「a6.バックアップ」，「a7.フィルタリング」，「a8.暗号化」，「a9.ID・パスワード」，「a10.生体認証」，「a11.多要素認証」，「a12.パスワード作成・管理技術」，「b.サイバー空間における情報セキュリティの被害とその対応」，「c.生活の中で想定されるトラブルへの対応」，「d.コンピュータウィルスの感染，ハッキング等による被害事例とその対応」の15個の指導内容を摘出した。さらに摘出した内容を基に，1単位時間で学習できる情報セキュリティ教材を作成し，授業実践をおこなった。

小学校においては，開発した情報セキュリティの教材を利用した 1 単位時間（45分）

の学習により，情報セキュリティの意識，人的対策の知識，情報セキュリティの技術的対策の知識の向上につながることが確認された。中学校の学習においては，開発した情報セキュリティの教材を利用した１単位時間（50分）の学習により，学習指導要領で示された技術・家庭科(技術分野)で学ぶべき情報セキュリティの知識を高めることにつながることが確認された。また，本教材を使った学習では，学習のまとめに，学習した情報セキュリティの「知識及び技能」を活用した課題解決学習を取り入れているため，「思考力・判断力・表現力」及び「主体的に学ぶ態度」の育成にもつながっていくものである。さらに，本教材は，各発達段階で身に付けるべき内容を踏まえた教材であるため，小・中学校の系統的な情報セキュリティ教育に効果があるものと考えられる。

情報セキュリティを確保する能力は，これからの情報化社会を生きる小・中学生にはなくてはならないものである。情報セキュリティを確保する能力を身に付けるためには，いつの時代も変わらない不変のものと，時代により常に変化する内容を学ぶ必要がある。情報セキュリティ教育は，情報技術の発展に柔軟に対応した学習を小・中学校の各段階で体系的に進めていく必要がある。今後の展望として，サイバー空間や生体認証など新たな科学技術を取り入れた情報セキュリティ対策の指導を充実させていく必要があると考える。

今後は，この研究を足掛かりに全国の小・中学校において，すべての児童・生徒に効果的な情報セキュリティ学習がおこなわれることを期待する。

5.7 今後の課題

本研究では，以下のような課題が残されている。

第一に第2章で述べた教育現場の実態調査において，教員，小学校修了段階，中学校修了段階での調査はおこなったが，高等学校修了段階での調査はおこなっていない。文部科学省が示す初等中等教育における情報セキュリティ教育の出口は高等学校に設定されているため，高等学校修了段階の情報セキュリティの実態も把握する必要があるであろう。また，本研究における調査は，一部の地域に限定された調査であるため，対象地域を広げた調査が必要である。

第二に第3章で述べた教材は，学校の授業の中で利用することを想定している。オンライン教材であるが個別に理解度を調査するテスト機能は含まれていない。一人一台端末が整備され，学校において，個別学習も充実してくる。今後は，個別学習に対応した機能も加えていく必要がある。また，開発教材を継続的に更新し，学校における情報セキュリティ教育を充実させるため，教育委員会や学校が主催する教員研修等と連携した仕組みを模索していく必要がある。

第三に第4章で述べた授業実践では，児童・生徒の意識と知識を中心とした調査分析に留まっており，授業実践で得られた見方・考え方といった多様な観点からの調査分析や行動の変容の調査が必要である。方法として，ワークシートや生徒の発話を質的分析し，知識ネットワークの広がりや知識の活用のされ方を明らかにしたり，行動の変容に関する事後の追跡調査をしたりするなどが考えられる。また，小・中学校における情報セキュリティ教育を充実させるため，本実践で活用した指導案，ワークシートなどの教材などの授業資料を提供していく必要がある。

今後は，これらの諸課題を明らかにするための実践的研究に取組むとともに情報セキュリティ教育のさらなる発展を願ってやまない。

謝辞

本論文の執筆および研究をすすめるにあたり，多くの方々にご指導とご支援を賜りました。特に，主指導教員の埼玉大学 教授 山本 利一 先生には，研究の基礎からご指導を頂きました。山本先生の研究に対する熱い想いと広い見識を身近で感じながら，研究に対する姿勢に感銘を受けました。山本先生のご指導無しには，本研究の遂行はあり得ませんでした。心より感謝申し上げます。

また，副査としてご指導頂きました，埼玉大学 教授 葉石 光一 先生，東京学芸大学 教授 櫨山 淳雄 先生には，それぞれの専門分野から丁寧なご指導とご助言を頂きました。深く感謝申し上げます。

さらに，本研究に貴重なご助言を頂きました，横浜国立大学 教授 鬼藤 明仁 先生，埼玉大学 准教授 荻窪 光慈 先生，日本工業大学教授 本村 猛能 先生，北海道教育大学 准教授 佐藤 正直 先生には，多大なご支援を賜り深く感謝申し上げます。

本研究は，私が前職の指導主事の時からすすめており，勤務先であった群馬県総合教育センター元所長　岡島 美智子 先生，野村 晃男 先生をはじめ，元同僚の皆様方にも多大なるご理解とご支援を頂戴いたしました。心より感謝申し上げます。

本論文の研究が，教育の情報化の発展に少しでもお役に立てれば幸いです。

最後に，本研究に協力頂きました，群馬県の先生方，生徒，児童，保護者の皆様方，友人，家族，すべての皆様方に感謝の意を表し，謝辞と致します。

2021 年 12月 8 日

小熊　良一

本研究に関する学術論文及び本論文と既刊論文に関わる注

1. 本研究に関する学術論文

第1章

1.義務教育における情報セキュリティ教育の現状と課題，小熊良一・山本利一，群馬大学教育学部紀要，芸術・技術・体育・生活科学編，第55巻，pp.79-90，2020年3月

2.日本の学校教育における教員の情報セキュリティ研究の課題と展望，小熊良一・山本利一，群馬大学教育学部紀要，芸術・技術・体育・生活科学編，第54巻，pp.61-67，2019年3月

第2章

1.小・中学校教員の情報セキュリティに関する「意識」「行動」「知識」に関する調査（R），小熊良一・山本利一・在間拓幹，教育情報研究，第36巻，第1号，pp.13-24，2020年7月

2.Survey on information morals and information security knowledge and responsiveness at the stage of completing compulsory education in Japan（R），Ryoichi Oguma・Toshikazu Yamamoto，The Proceedings of International Conference on Technology Education in Asia-Pacific Region 2021，pp.146-155，2021年2月

第3章

1.小学校高学年における情報セキュリティWeb教材開発と授業実践（R），小熊良一・山本利一，教育情報研究，第37巻，第1号，pp.53-62，2021年10月

2.中学校技術・家庭科(技術分野)における「情報セキュリティ」のオンライン教材の開発と授業実践（R），小熊良一・山本利一，日本産業技術教育学会誌，第 63 巻，第 4 号，pp.39-48，2021 年 12 月

第4章

1.小学校高学年における情報セキュリティWeb教材開発と授業実践（R），小熊良一・山本利一，教育情報研究，第37巻，第1号，pp.53-62，2021年10月

2.中学校技術・家庭科(技術分野)における「情報セキュリティ」のオンライン教材の開発と授業実践（R），小熊良一・山本利一，日本産業技術教育学会誌，第 63 巻，第 4 号，pp.39-48，2021 年 12 月

2. 本論文と既刊論文に関わる注

本研究に関わる上記の既刊論文では，小学校における授業実践について，29名で実施した結果を報告しているが，本論文では，検定力を高めるため，113名の追加実践をおこない，142名の実践として報告している（注1）。同様に，中学校における授業実践についても95名の追加実践をおこない，135名の実践として報告している（注3）。

また，授業実践の事前・事後の知識の効果分析について，既刊論文では，χ2検定をおこなっているが，本論文では，マクネマー検定に変更し，事前・事後の正答・誤答の対応がわかるようにした（注2，注4）。