Web公開版

卒業論文

座学と実技による
中高生向け情報セキュリティ教育の検討

指導教員　川戸 聡也　講師

提出年月日　令和5年1月27日

米子工業高等専門学校　電子制御工学科
18333　守山 凛

目 次

図 目 次

表 目 次

第1章　序論

1.1　研究背景

総務省が発表した「令和4年度版 情報通信白書」によれば，我が国における2021年の個人のインターネット利用率は82.9%に上り，2013年にはじめて80%を記録して以降，高水準を記録し続けている．年齢階層別では，13歳〜19歳が98.7%と最も高く，中高生を中心として広く利用されていることが分かる．近年では，テレビやエアコン，冷蔵庫などの家電をはじめ，あらゆる「モノ」をネットワークに接続しようとする「IoT（Internet of Things)」が広く普及しており，インターネットをはじめとするICTは，重要な社会インフラとなっている．

その一方で，インターネットを利用している12歳以上の者の約75%がインターネットの利用時に何らかの不安を感じている．具体的な不安の内容としては,「個人情報やインターネット利用履歴の漏えい」の割合が90.1%と最も高く，次いで「コンピューターウイルスへの感染」が62.7%,「架空請求やインターネットを利用した詐欺」が54.1%となっている [1,2]．実際に，警察庁やJPCERTコーディネーションセンターなどの調べでは，不正アクセスや改ざん，フィッシング，マルウェア感染などの情報セキュリティインシデントは増加傾向にある．特に，新型コロナウイルスが流行し始めて以降，フィッシングおよび改ざんの被害報告件数は過去最多を更新するなど，ICTの安心安全な利用に対する課題が浮き彫りとなっている [3–5].

また我が国では，従来より，情報セキュリティ人材の不足が指摘されている．経済産業省は，2016年時点で13.2万人の人材が不足しており，2020年には19.3万人に増加すると推計している [6]．日本政府は，人材育成の基本方針の一部として，初等教育段階での情報活用能力の育成や，産学官連携による高等教育段階での情報技術人材の育成，サイバーセキュリティ関連ツールや機器を用いた学習環境の整備，実践的な演習によるスキル開発を定めており，情報セキュリティ教育の必要性を示している [7].

1.2 研究目的

情報セキュリティ教育の重要性が唱えられる昨今，国立高等専門学校機構では，サイバーセキュリティ人材育成事業（K-SEC）として，合宿講座の開催や，教材の開発，高専セキュリティコンテストの開催などを通して，高度な情報セキュリティ人材の育成に取り組んでいる [8,9]．筆者は2020年度から，K-SECの助成を受け，米子高専の学生を対象とした情報セキュリティ啓発活動として，実機演習を交えた教育活動に取り組んできた [10,11]．

しかし，ICTが浸透し，生活に必要不可欠となっている現代では，ICTを利用する全ての者が情報セキュリティを学ぶ必要がある．近年では，中学生が校内のサーバーに記録された成績表を改ざんした事例や，17歳の高校生がコンピュータウイルスを作成し掲示板に投稿した事例など，中学生や高校生が加害者となる事例が多く発生している [12]．また，オンラインゲームの乗っ取りや，架空請求などの被害に遭う中高生が増加している [13] ことから，中高生に対する情報セキュリティ教育の重要性が高まっている．

そこで，情報セキュリティ人材育成の推進普及や，サイバー犯罪被害および非行の抑止，中学校および高等学校における情報教育の授業改善に寄与することを目的に，中高生を対象とした教育手法の検討と実践を行う．

本研究では，情報セキュリティ学習の基盤となる知識を身に着けるための「座学」と，危険性や対策を体験的に学習するための「実技」を組み合わせた教育手法を提案する．これにより，生徒の情報セキュリティ学習への興味関心を高めると同時に，日常生活における情報セキュリティ対策の実践や情報セキュリティ学習を継続するきっかけづくりとして期待できる．教育手法および内容については，教育対象となる年代の情報セキュリティに対する意識や考え方を調査・分析すると同時に，情報セキュリティ教育が拡充された高等学校の共通必履修科目「情報I」の教科書を分析することで，より効果的な教育手法および内容を検討する．また，提案した教育手法と内容を基に，米子高専が主催する「公開講座」と，米子東高校で行われる「土曜日活用授業」の2通りにて授業を実践し，参加者へのアンケートによるフィードバックを行い，有効性を検証する．

1.3　本論文の構成

本論文は7章構成になっており，以下の順で研究成果を述べる．

第1章では，本研究の背景と目的を述べる．

第2章では，従来の情報セキュリティ教育として，国内外の事例について簡単に紹介する．併せて，従来の手法に対する本研究の位置づけを述べる．

第3章では，授業設計のための共通事項として，米子高専学内において実施したアンケートの分析結果，高等学校「情報I」の教科用図書の分析結果について述べる．

第4章では，中学生に対する授業の実践として，米子高専の公開講座における授業の内容と，事後アンケートの分析結果について述べる．

第5章では，高校生に対する授業の実践として，米子東高校において実施した授業の内容と，事後アンケートの分析結果について述べる．

第6章では，本研究の関連として，鳥取県警と連携して実施した「鳥取県警察サイバー防犯ボランティア」における筆者の活動について述べる．

第7章では，研究のまとめとして，得られた知見と今後の展望について述べる．

第2章　先行研究

2.1　国内の先行研究

2.1.1　中学校における事例

塩田らは,「自分ももしかしたらトラブルにあうかもしれない」という当事者意識を促すことを目的に，架空請求やなりすまし，不正アクセスなどのトラブル事例について学習できるカード教材を開発し，埼玉県内の中学校で授業実践を行っている [14].

多田らは，パスワード構成や二段階認証の仕組みについて授業前に各自で調べ，授業では事前に調べた内容を全体で共有し，パスワードの強度について考える授業を行っている．この授業では，学習カードを用いて学んだ内容の活用の仕方を確認するものとなっている [15,16].

2.1.2　高等学校における事例

今川らは，SSL 通信とファイアウォールのシミュレーションシステムを用いた教育手法を提案している．このシステムは，パソコン 4 台を 1 組としてネットワークを構成し，ネットワークの設定や通信のやり取りなど，実際のネットワークと同じ動作で通信できるアプリケーションとなっている [17].

増山は，シナリオに基づいて標的型メールの判別と対応を学習させる教材を開発し，事前学習により標的型メールの例と見分け方について学習したのち，標的型メールについてグループでの議論などを通じて，標的型メールへの対策能力を得ることを目指すという授業実践を行っている [18].

西郡らは，スマートフォンゲームの盗聴・改ざんやパソコンの遠隔操作をテーマに，サイバー攻撃の手法や脅威を知り，被害の疑似体験によりサイバー攻撃の脅威を実感すること，サイバー犯罪に関する法律を学び正しい倫理観を持つことを狙いとした授業実践を行っている [19].

2.1.3　高等専門学校における事例

栗原らは，K-SEC において開発されたセキュリティに関する人狼ゲームを低学年の HR に取り入れている．また，ゲームルールの変更や，全学生がプレーヤーとしてゲームに参加できるようにするなど，既存の教材を改造し，独自の教材を開発している [20].

土居は，北海道警察サイバーセキュリティ対策本部との人材育成に関する連携協定を通じたセキュリティ教育を実施している．この中で，2019 年には一般の人を対象とした，スマートフォンアプリのインストールやアプリが要求する権限に関して啓蒙するシステムが開発された [21].

都立産業技術高専では,「情報セキュリティ技術者育成プログラム」として，専攻科までを含めた技術者育成プログラムが実施されている．このプログラムでは，企業や大学，警察庁などと連携し，アクセス制御や脆弱性の検出，マルウェアの解析といった演習を交えた授業が行われている [22–24].

干川らは，CTF 演習のような攻防型演習の特徴を利用した教育システムを提案している．このシステムでは，DoS 攻撃，IoT の乗っ取り，ポータルサイトへの攻撃，動画配信サーバの攻撃といった演習を実施できる [25].

2.1.4　大学・大学院における事例

山之上らは，大学生向けのビデオ教材を作成している．この教材は，パスワードや通信の暗号化，電子署名などの技術的な内容に加え，パスワード管理や情報セキュリティポリシーなど技術的でない内容も含まれている．開発したビデオ教材は，鹿児島大学や東京農工大学，東京学芸大学での導入事例がある [26].

広島大学では，2011 年度より全学生を対象とする情報セキュリティ・コンプライアンス教育が実施されている．この中では，ビデオ教材を用いたネット上のトラブルの紹介や，学内で実際に発生したインシデント事例の紹介，トラブルへの対処方法を解説している [27].

佐々木らは，産学協同による情報セキュリティ教育として，SEA/J と協力し，東京電機大学大学院の学生を対象とした授業を実践している．この授業では，暗号についての座学や，不正侵入やアクセス制御について実機による演習が組み込まれている [28].

大久保らは，指紋認証実験を取り入れた情報セキュリティ教育を提案している．この授業では，グミに自分の指紋をコピーして作成した「グミ指」を利用した認証突破実験を取り入れている [29].

2.2 国外の先行研究

2.2.1 アメリカにおける事例

国家安全保障局と国立科学財団は，幼稚園から高校までの園児・児童・生徒および教師を対象とした「Gen Cyber」を実施している．このイベントでは，ロールプレイングやディスカッションなどを通じてサイバーセキュリティへの関心を高める活動が行われている [30]．また，ソーシャルエンジニアリングの概念や，フィッシングメールへの対応を学習するための VR アプリケーションが開発され,「Gen Cyber」において実践されている [31].

ラドフォード大学では，高校生を対象に「RUSecure CTF Contest」と呼ばれるイベントを実施している．このイベントは，暗号やハッシュ，フォレンジック，Web セキュリティ，Windows セキュリティなどに加え，IoT デバイスのハッキングや，システムやデバイスを攻撃から保護するための課題など，さまざまな課題に挑戦するコンテストである [32].

テキサス大学では，大学生を対象に，情報セキュリティに関するコンペティションを授業内で実施している．このコンペティションは，ネットワークの設定や情報セキュリティの管理，情報セキュリティマネジメントなどに関する内容であり，インシデントに対応する能力を身に付けることを目的としている [33].

2.2.2 イギリスにおける事例

Jaffray Alice は，探偵をテーマとしたシリアスゲームの教材を開発し，大学生を対象に実践している．シリアスゲームとは，教育や体験などエンターテインメント以外の目的で作られたゲームのことであり，このゲームは，情報セキュリティの 3 要素や，セキュリティの脅威と攻撃，リスク管理についての知識を定着させることが目的となっている [34, 35].

2.2.3 ドイツにおける事例

トリアー大学では，学生がいつでもどこでも情報セキュリティを実践できるようにするため,「Tele-Lab IT Security」と呼ばれる学習システムを開発している．このシステムは，暗号化，ディジタル署名，認証，セキュリティスキャンなどの基本概念を学習する，Web ベースのオンラインシステムである．実戦経験を積むことができるといった特徴を持っており，シミュレーションではなく，実際の Linux システムで動作するものである [36].

2.3 本研究の位置づけ

先行研究においては，高専や大学・大学院における専門教育では，実機を用いた実践的な演習を組み込んだ教育手法が多く提案されている．一方で，小中学生や高校生など，情報セキュリティに関して学び始めとなる者に対する教育では，講義形式やゲーム形式の教育手法が多く提案されており，実践的な演習を組み込んだ教育はほぼ行われていない．サイバー攻撃や防御に関する実践的な演習を行うことで，攻撃の手法やその対策方法について体験的に学習することができ，生徒の理解を促進させることができると考えられる．

そこで本研究では，情報セキュリティに関して学び始めとなる者に対して，実機を用いた実践的な演習を組み込んだ教育手法を提案し，教育実践を行う．情報セキュリティの重要性を体験的に学習することで，生徒の興味関心を高め，日常生活における情報セキュリティ対策の実践や情報セキュリティ学習へのきっかけをつくる．

第3章　授業設計のための共通事項

3.1　学内でのアンケート調査の実施

3.1.1　調査の概要

本研究を取り組むにあたり，教育手法の検討や実践には，教育対象となる年代の情報セキュリティに対する知識や技能を把握する必要がある．そこで教育対象となる年代の情報セキュリティに対する考え方などを把握するためのアンケート調査を実施した．高校生と同じ年代であり，回答の依頼から収集まで容易にできる点から，調査対象を本校の本科1年生から3年生までの全学生603名とし，倫理審査委員会からの承認を得た上で7月から8月の間に実施した．

アンケートへの回答は任意であり，あらかじめ対象学生に調査の趣旨を説明し，同意の得られた学生のみ回答してもらう形とした．学生への説明は，原則として，担任の先生の協力の元，HRの時間を利用して口頭にて行った．担任の先生の協力が得られなかったクラスの学生に対しては，当該クラスの学生を通じて，書面にて説明を行った．アンケートの有効回答数は，62.19%にあたる375名であった．

また，4章以降で述べる公開講座や米子東高校での授業においては，本調査で得られた情報セキュリティに関する知識や技能，考え方を教育手法や教育内容に反映させ，生徒が興味を持てる授業設計を心がけた．

3.1.2　調査の結果と分析

(1) 情報授業に対する意見

情報の授業に対する意見や要望を尋ねたところ，以下の回答があった．

- 直近の事例を踏まえて最新技術などの講義をしてほしい．
- 実際に攻撃を受けている様子を見たことが無く，イメージしにくい．
- 実機を使った演習などを交えた講義をしてほしい．

学生からは教育手法に関して多くの指摘があった．本校の情報に関する授業は，コンピュータの操作方法を学ぶ「情報リテラシ」，データの解析やグラフ作成を学ぶ「数理・データサイエンス基礎」，Python プログラミングやコンピュータの基礎を学ぶ「情報基礎 I」，ネットワークや情報システムの基礎を学ぶ「情報基礎 II」の 4 科目となっており，情報セキュリティについては「情報基礎 II」で学ぶ [37]．しかし，いずれの科目も 5 クラスの一斉授業で行われているため，演習の実施が困難なものだと考えられる．

(2) 「情報モラル」の認知度について

「情報モラル」について，どのようなものか知っているかを尋ねた．この結果を図 3.1 に示す．また「知っている」と回答した学生に対し，「情報モラル」と聞いてイメージすることを尋ねたところ，SNS の使い方，個人情報，マナー，権利の保護などの回答があった．

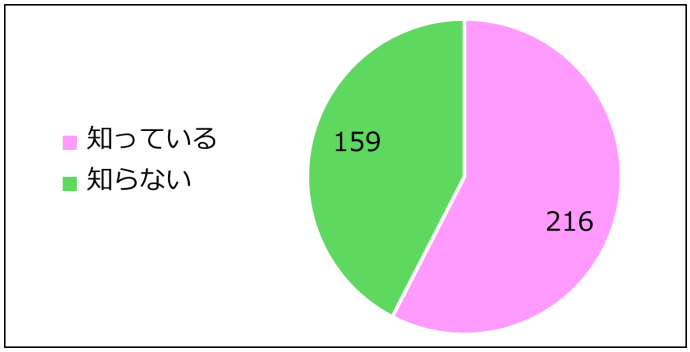


図 3.1 学内における情報モラルの認知状況

(3) 「情報セキュリティ」の認知度について

「情報セキュリティ」について，どのようなものか知っているかを尋ねた．この結果を図 3.2 に示す．また「知っている」と回答した学生に対し,「情報セキュリティ」と聞いてイメージすることを尋ねたところ，情報の保護，暗号やウイルス感染，パスワードなどの回答があったが，SNS の使い方や権利の保護など，情報モラルに関する内容を挙げている学生はいなかった．このため，情報モラルと情報セキュリティの違いについて，一定の理解があると考えられる．

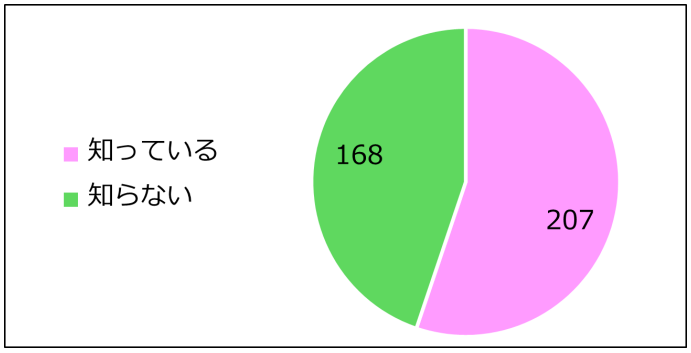


図 3.2 学内における情報セキュリティの認知状況

(4) 情報モラル・情報セキュリティ教育の受講経験

情報モラルや情報セキュリティに関する教育を受けたことがあるかを尋ねた．この結果を図 3.3 に示す．6 割の学生が「受けたことがある」と回答しており，「受けたことがある」と回答した学生に，その内容を尋ねたところ，誹謗中傷やネットいじめ，SNS の使い方，多要素認証などが挙げられた．回答の約 7 割が情報モラルに関するものであり，教育内容が偏っていると考えられる．

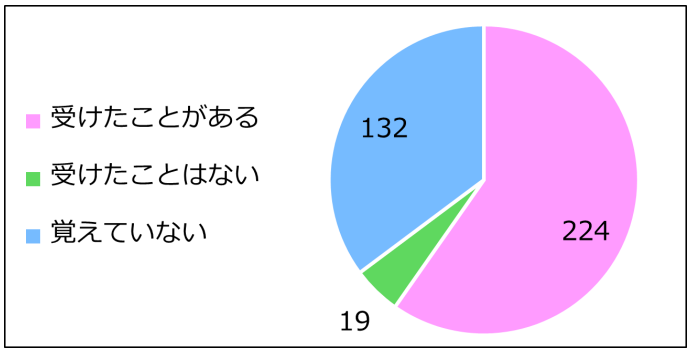


図 3.3 学内における情報セキュリティ教育の受講経験

(5) 情報セキュリティに関する興味関心

情報セキュリティに関して興味や関心があるかを尋ねた．この結果を図 3.4 に示す．肯定的な回答は約 4 割であり，ICT が急速に普及し情報セキュリティの重要性が指摘される中では，肯定的な回答数が少ないものと考えられる．

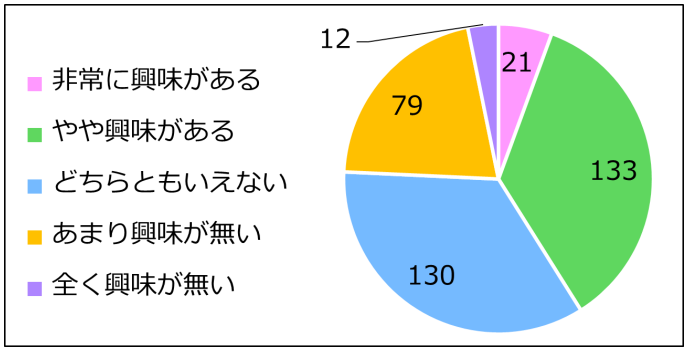


図 3.4 学内における情報セキュリティへの興味の状況

(6) インターネット利用における不安

日頃のインターネット利用で不安に感じることがあるかを尋ねた．この結果を図 3.5 に示す．約 3 分の 1 の学生が「ある」と回答している一方，多くの学生が「ない」と回答している．ICT の普及により，我々の身近なところでもサイバー犯罪被害に遭う可能性が高いため，学生が危機感を感じられるように教育手法や内容を工夫する必要がある．また「不安がある」と回答した学生に対し，不安の内容を尋ねたところ，個人情報の流出や，ウイルスへの感染，パスワードの漏えいなどが挙げられ，これらに対する対策方法などを教育する必要があると考えられる．

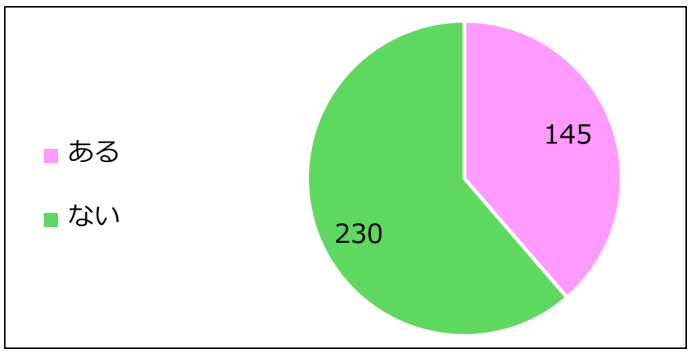


図 3.5 学内におけるインターネット利用における不安の有無

(7) 情報セキュリティの生活への意識状況

情報モラルや情報セキュリティを日常生活で意識しているかを尋ねた．この結果を図 3.6 に示す．5 割弱の学生が肯定的に回答しているが，ICT が急速に普及し情報セキュリティの重要性が指摘される中では，肯定的な回答数が少ないものと考えられる．

また，肯定的な回答をした学生に対して，どのようなことを意識しているかを尋ねた．結果，パスワードを強度なものにする，通信の暗号化の確認，多要素認証の導入，SNS の公開範囲の設定，正しい情報発信が挙げられた．本校の「情報基礎Ⅱ」の授業では，情報セキュリティ対策として，ユーザ ID とパスワードの管理，認証，通信の暗号化，個人情報の保護などが扱われるが，このような対策は実践できていることが分かる．

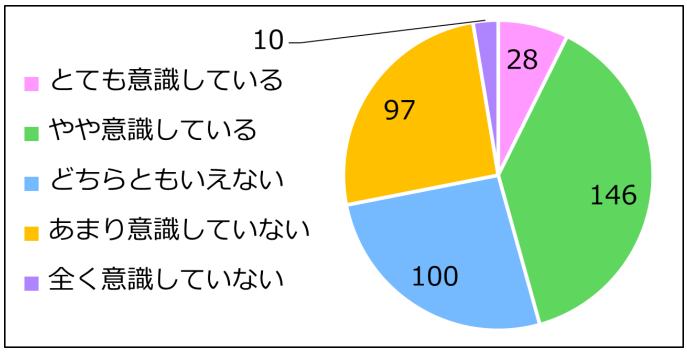


図 3.6 学内における情報セキュリティの生活への意識状況

(8) 各種サイバー攻撃に関する知識および技能

表 3.1 に示す各サイバー攻撃について，表 3.2 の尺度で，学生の持つ知識および技能の状況を調査した．この結果を図 3.7 に示す．なお評価の尺度は，株式会社ラック『情報リテラシー啓発のための羅針盤』[12]，文部科学省『平成 30 年告示高等学校学習指導要領』[38]，国立高等専門学校機構『モデルコアカリキュラム』[39] を参考とした．また国立高等専門学校機構『モデルコアカリキュラム』より，高専生が満たすべきスキルを Lv.4 と定義する．

表 3.1 調査したサイバー攻撃の一覧

質問番号	攻撃名
質問 1	不正アクセス
質問 2	マルウェア
質問 3	DoS 攻撃
質問 4	フィッシング
質問 5	パスワードリスト攻撃
質問 6	標的型攻撃
質問 7	偽セキュリティソフト
質問 8	偽警告
質問 9	ランサムウェア
質問 10	不正ログイン
質問 11	ソーシャルエンジニアリング
質問 12	架空請求
質問 13	クロスサイトスクリプティング
質問 14	SQL インジェクション
質問 15	クロスサイトリクエストフォージェリ
質問 16	OS コマンドインジェクション

表 3.2 スキルの評価尺度

レベル	スキル
Lv.0	全く知らない
Lv.1	名前は聞いたことがある
Lv.2	概要をある程度知っている
Lv.3	対処法を知っている
Lv.4	対策が実践できる
Lv.5	第三者に説明できる

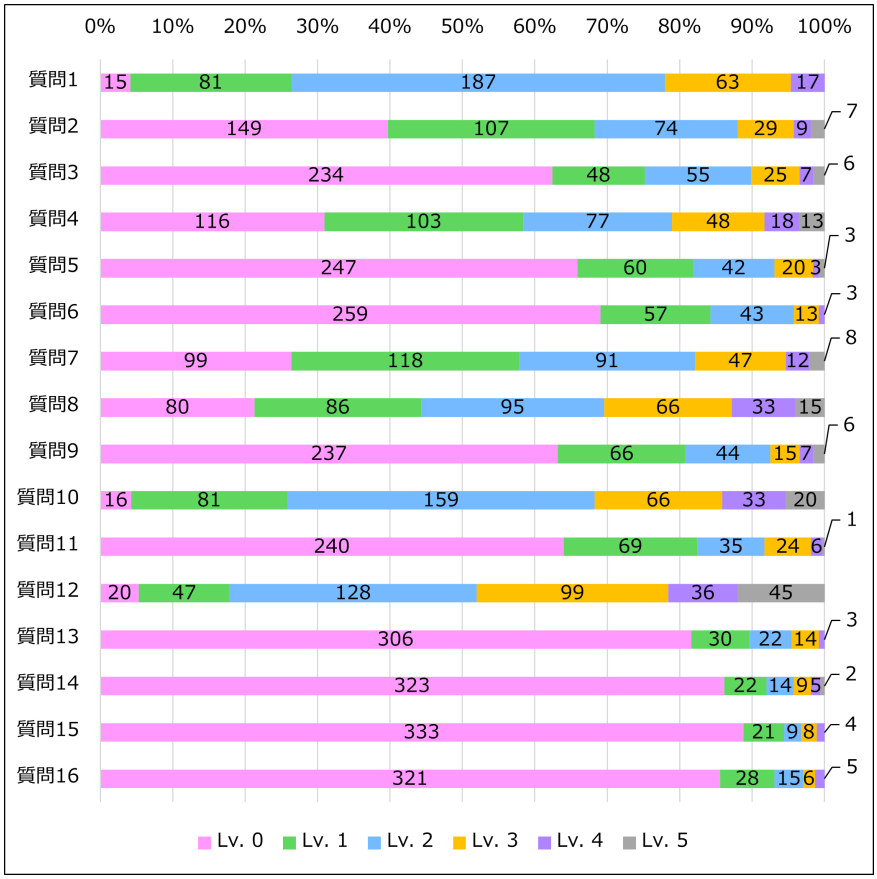


図 3.7 学内におけるサイバー攻撃に関する知識及び技能の状況

結果より，不正アクセスや，フィッシング，不正ログイン，架空請求など，ニュースなどでも見聞きすることが多い攻撃についてはLv.2以上の学生が多いことが分かる．その一方で，マルウェアやソーシャルエンジニアリングなどの身近に存在する攻撃手法については，名前を知っている程度であり，教育の必要があると考えられる．

(9) サイバー犯罪被害の経験について

次のようなサイバー犯罪被害に遭ったことがあるかを尋ねた．この結果を図 3.8 に示す．いずれかの経験をした学生のうちの過半数が,「偽の警告画面が表示されたことがある」と回答している．しかし，(8) の通り，対処法などを知っている学生が少なく，教育の必要があると考えられる．

1. 何者かによる不正アクセスが試みられたというメールを受信した．
2. メールの添付ファイルを開いた結果，ファイルが暗号化された．
3. URL のアクセスと，ID・パスワードなどの入力を求めるメールや SNS メッセージを受信した．
4. 突然，ブラウザに「ウイルスに感染した」と警告画面が現れた．
5. 宅配便の不在通知が SMS（ショートメッセージサービス）でスマホに届いた．
6. 「あなたのスマホはウイルスに感染しています」という警告画面が表示された．
7. 上記のような経験はない．
8. 上記のようなトラブルや被害があったかどうかわからない．

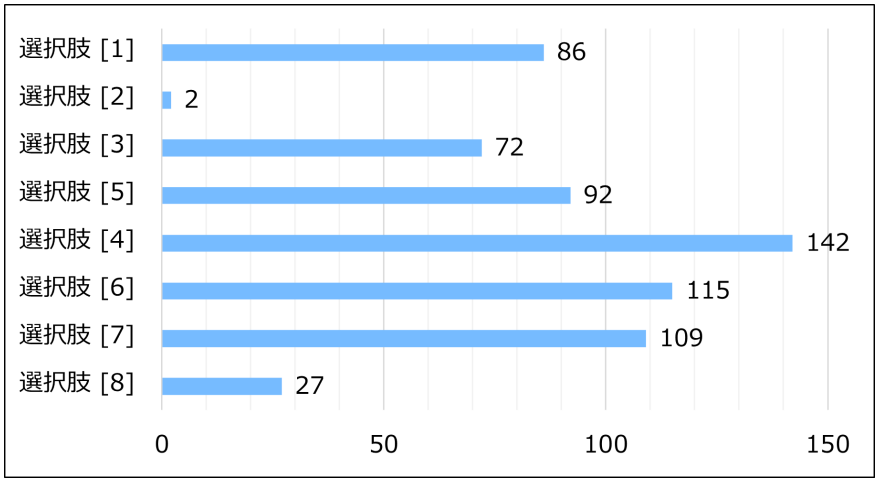


図 3.8 学内におけるサイバー犯罪被害の経験状況

(10) 情報セキュリティ対策の実施状況

以下のような情報セキュリティ対策を実施しているかを尋ねた．この結果を図 3.9 に示す．結果より，いずれの対策も実施していない学生は 3.5%程度であり，多くの学生が適切な対策を取っていることが分かる．パスワードの使いまわし，初期パスワードの変更，バックアップや売却時のデータ消去などデータの取扱いについては実施率が低く，教育の必要性があると考えられる．

1. パスワードは他人が推測しにくい（氏名や誕生日などの情報を用いない）内容を設定している．
2. パスワードはできるだけ長い文字数（8〜10 文字以上）を設定している．
3. サービス毎に異なるパスワードを設定している（使いまわしていない）．
4. 初期パスワードが設定されている場合は，そのまま使わず必ず変更している．
5. セキュリティ対策ソフトやサービスを利用している．
6. パソコンやスマートフォンのデータをバックアップしている．
7. OS などのソフトウェアやアプリケーションはサポートが切れていないものを使用し，かつ最新の状態にアップデートしている．
8. スマートフォンやパソコンを廃棄または売却する際は，データが復元できないような消去または物理的な破壊を行っている．
9. 自宅のパソコンを家族で使う場合，利用者毎にアカウント（ID，パスワード）を分けている．
10. メールや SNS メッセージにある添付ファイルは不用意に開かない，また本文中の URL も不用意にクリックしないようにしている．
11. 怪しいと思ったホームページに行き着いたら先に進まない，情報を入力しないようにしている．
12. パソコンやスマートフォンには，ログインパスワードを設定している．

13. パスワード，指紋，ワンタイムパスワードなどから 2 種類以上の要素を組み合わせた多要素認証を積極的に利用している．

14. アプリをインストールする前または実行時に要求される権限を確認している．

15. 1 つも実施していない．

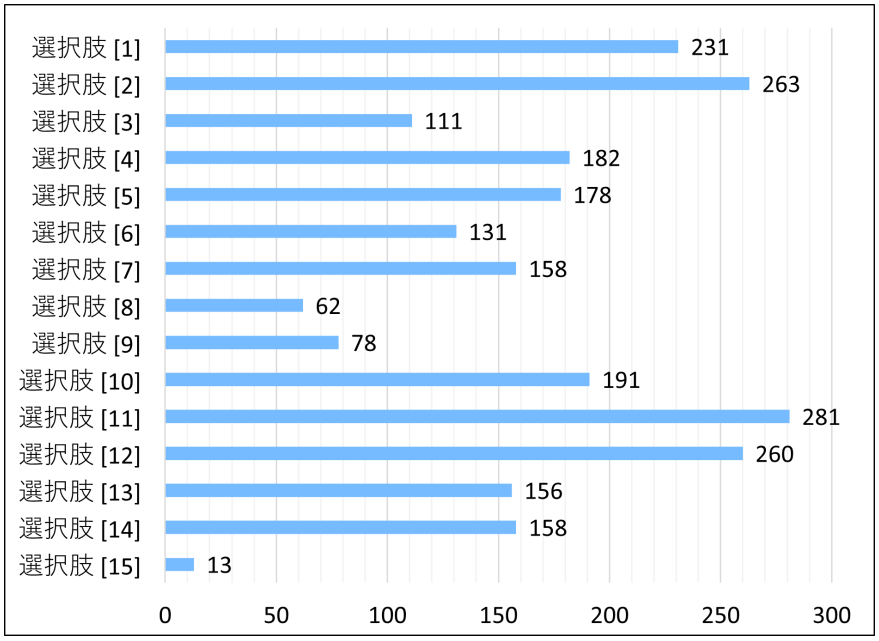


図 3.9 学内における情報セキュリティ対策の実施状況

3.2 高等学校「情報 I」の教科書分析

3.2.1 調査の背景

高等学校共通教科情報科は従来,「社会と情報」および「情報の科学」の 2 科目から 1 科目を選択する選択必履修科目となっていた．しかし，平成 30 年 3 月に学習指導要領が改訂され，情報技術を適切かつ効果的に活用する力を全ての生徒に育む共通必履修科目として「情報 I」，情報システムやデータを適切かつ効果的に活用する力やコンテンツを創造する力を育む選択科目として「情報 II」の 2 科目に再編された [40]．令和 7 年度からは大学入学共通テストに教科「情報」が追加され，情報 I が出題されることが決定 [41] しており，情報教育が重要なものとなっている．

また 1 章でも述べたように，情報セキュリティインシデントは近年増加傾向にある．学習指導要領では情報 I において，情報セキュリティの重要性や，情報セキュリティを確保するための方法や技術を学ぶとされており，高等学校での情報セキュリティ教育が重要視されていることが分かる [38].

しかし，実際の教科指導では，各校が採用する教科用図書（以下,「教科書」という）によって取り扱われる内容に差が生じることが予想される．そのため，各教科書で取り扱われる内容を正確に把握することで，全生徒に共通して求められている知識及び技能を体系化し，今後の教科指導に反映させる必要があると考えられる．

これまでに教科書の内容に関する分析や比較を目的とした報告がいくつかなされている．御家らは，ピクトグラムの説明に関する掲載状況や，取り扱っているピクトグラムの比較を行っている [42]．井出は，各教科書の使用プログラミング言語や，扱っているプログラミングの諸概念の比較を行っている [43]．赤澤らは，高等学校共通教科情報科の知識体系の明確化を目的として，全教科書の索引に着目して情報 ABC から情報 I・Ⅱ までの高等学校情報科で扱う用語の変遷についての考察 [44] や，情報 I の教科書の索引に掲載されている用語から知識体系に関する考察 [45] を行なっている．また成瀬らは，情報 I の教科書および傍用問題集でのデータサイエンス分野の取扱いや授業プランの検討を行っている [46]．このように情報 I の特定の分野や観点に着目した教科書の分析が行われてきたが，情報セキュリティに関する教科書の分析については報告されていない．

そこで，高校生に求められている情報セキュリティに関する知識および技能を把握し，4 章以降で述べる公開講座や米子東高校での授業の内容を検討するための指標とするため，学習指導要領に基づいてどのような用語が用いられているのかを情報 I の検定済教科書全体から調査し，傾向や特徴について分析する．

3.2.2 学習指導要領における取扱い

情報 I は，(1) 情報社会の問題解決，(2) コミュニケーションと情報デザイン，(3) コンピュータとプログラミング，(4) 情報通信ネットワークとデータの活用，の 4 単元から構成され，情報セキュリティに関する内容は，単元 (1) と単元 (4)

で登場する．また各単元の学習内容は,「ア 次のような知識および技能を身に付けること」「イ 次のような思考力，判断力，表現力等を身に付けること」の順に記載されている．

(1) 知識・技能

「ア 次のような知識および技能を身に付けること」では，以下の 2 点が学習内容として挙げられている．

単元 (1) 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及び情報モラルについて理解すること

単元 (4) 情報通信ネットワークの仕組みや構成要素，プロトコルの役割及び情報セキュリティを確保するための方法や技術について理解すること

また，これらの具体的な学習事項として，学習指導要領解説 [38] では，表 3.3 に示す用語が用いられている．

表 3.3 知識・技能に関する学習項目

単元 (1) に関する用語	単元 (4) に関する用語
個人情報保護法	個人認証
不正アクセス禁止法	暗号化
情報セキュリティの 3 要素	デジタル署名
パスワード	デジタル証明書
ソーシャルエンジニアリング	暗号化プロトコル

(2) 思考力・判断力・表現力

「イ 次のような思考力，判断力，表現力等を身に付けること」では，以下の2点が学習内容として挙げられている．

単元 (1) 情報に関する法規や制度及びマナーの意義，情報社会において個人の果たす役割や責任，情報モラルなどについて，それらの背景を科学的に捉え，考察すること

単元 (4) 目的や状況に応じて，情報通信ネットワークにおける必要な構成要素を選択するとともに，情報セキュリティを確保する方法について考えること

また，これらの具体的な学習事項として，単元 (1) では表 3.4 に示す用語が用いられている．単元 (4) では，情報セキュリティに関する用語は用いられていないが，関連事項として以下の事項を扱うとされている．

- 目的や方法に応じて情報通信ネットワークを構築するために必要な構成要素やプロトコル
- 安全で効率的な情報通信ネットワークの設計に必要なこと
- 無線 LAN において情報セキュリティを確保する方法
- 公衆無線 LAN を安全・安心に利用するための注意点
- あらかじめ用意したトラブルを抱えている情報通信ネットワークの不具合を解決したりすること

表 3.4 思考力・判断力・表現力に関する学習項目

単元 (1) に関する用語
サイバー犯罪
パスワード
生体認証
個人認証
セキュリティ更新プログラム

3.2.3　各教科書の内容

情報セキュリティの取扱いに関して，各教科書の内容の特徴を述べる．各項のタイトルは，教科書番号，教科書名，括弧内に教科書会社を表す．以下，教科書番号順に述べる．なお，ここで取り上げる用語は，情報処理推進機構の『情報セキュリティ読本』[47] や，情報処理安全確保支援士試験の試験要綱 Ver.5.0 [48] を参考にしている．

(1) 701 新編情報 I（東京書籍）

701 は，理論編と実習編，資料編の 3 編で構成されており，情報セキュリティに関する内容は理論編にのみ掲載がある．701 の理論編では，図や画像を多く用いられており，生徒が視覚的に理解しやすい構成となっている．

701 で取り扱われる情報セキュリティに関する用語は 26 語と最も少ない．その学習内容は，学習指導要領に基づき情報セキュリティの基礎に重点が置かれている．701 の特徴として，ハッカーとクラッカーの違いが説明されていることや，情報セキュリティの 3 要素である機密性，完全性，可用性について，それぞれに対応する技術が述べられていることが挙げられる．

(2) 702 情報 I Step Forward!（東京書籍）

702 も 701 と同様に，理論編と実習編，資料編の 3 編で構成されている．情報セキュリティに関する内容は理論編にのみに掲載がある．702 は 701 とは異なり，図や画像は少なく，文章での説明を中心として構成されている．

702 で取り扱われる用語は 32 語であり，基礎的なものを中心に掲載されている．702 の特徴として，情報セキュリティの 3 要素である機密性，完全性，可用性について，それぞれに対応する技術が述べられていることや，不正アクセスの具体的手法として「ブルートフォース攻撃」の掲載があることが挙げられる．

(3) 703 高校情報 I Python（実教出版）

703 では，学習項目を 35 のテーマに分けて構成しており，そのうち 3 つのテーマについて，情報セキュリティに関する記述がある．703 では，文章による説明を中心とし，適宜，図を用いることで視覚的に理解しやすい構成となっている．

703 に掲載されている用語は 34 語であり，学習指導要領に基づくものに加え，発展的な内容についても記述がある．情報セキュリティを確保するための技術については，電子透かしや SSL/TLS，アクセスログなど，情報システムの管理者の視点に立った内容が記述されている．また，コンピュータウイルスに感染した際の対処方法の記述があることも特徴の 1 つである．

なお，704 高校情報 I JavaScript（実教出版）は，703 と情報セキュリティに関する内容が同一であるため省略する．

(4) 705 最新情報 I（実教出版）

705 は 703 と同様に，文章による説明が中心に構成されている．情報セキュリティに関する内容は，4 章 2 節に「情報セキュリティ」として独立した節となっている．

705 に掲載のある用語は 48 語であり，学習指導要領にも記述のある基礎的な内容に加え，RSA 暗号や SSL/TLS，アクセス制御などの発展的な内容，IDS や IPS，DMZ などの情報システムの管理者の視点に立った内容も掲載されている．また，703 および 704 と同様に，コンピュータウイルスに感染した際の対処方法についても掲載されている．

(5) 706 図説情報 I（実教出版）

706 は，文章による説明を最小限に留め，図を中心に構成されており，視覚的に分かりやすい構成となっている．各章の最後には実習が用意されており，学んだ知識や技術の定着を図ることができるようになっている．

706 に掲載のある用語は 41 語であり，各教科書と共通し情報セキュリティに関する基本的事項が抑えられているほか，認証 3 要素や，コンピュータウイルスの 3 つの機能，機密性・完全性・可用性のそれぞれに対する脅威と対策について扱われている．また，パスワードの作成に関する実習が組み込まれており，生活の中で実践可能な知識・技術を身に付けることができるようになっている．

(6) 707 実践情報Ⅰ（開隆堂）

707は706と同様に，図や画像を中心とした構成となっており，生徒が視覚的に理解できるように工夫されている．それぞれの学習項目の末尾には実習のパートが用意されているため，学習内容の更なる定着を図ることができるようになっている．

707に掲載のある用語は26語と701と並んで最も少ない．学習内容としては，学習指導要領に基づく基本的事項がその大部分を占めている．実習パートでは，暗号化の体験としてバーナム暗号の暗号化と復号に関する実習が用意されている．

(7) 708 高等学校 情報Ⅰ（数研出版）

708は705などと同様に，文章による説明を中心として構成されている．各学習項目には，僅かながら実習のパートも用意されている．

708で取り扱われる用語は50語であり，13冊ある教科書の中で最も多い．学習内容としては，情報セキュリティの3要素である機密性・完全性・可用性のみならず，真正性，責任追跡性，信頼性，否認防止を加えた7要素や，コンピュータウイルスの3つの機能，RSA暗号，アクセス制御など発展的な内容についても多く取り扱われている．

(8) 709 情報Ⅰ Next（数研出版）

709は，図を多用し説明が簡潔にまとめられた構成となっている．また，各章の最後には演習が多く組み込まれているため，学習内容の更なる定着を図ることができるようになっている．

709で扱われる用語は35語であり，DoS攻撃や辞書攻撃，ソーシャルエンジニアリング，キーロガーなど多くの攻撃方法が紹介されており，それぞれについて事例を交えて説明されている．また，パスワードや暗号の生成に関する実習も含まれており，体験的に学ぶことができるように構成されている．

(9) 710 情報 I（日本文教）

710 は，709 などと同様に図を多く用いており説明が簡潔にまとめられた構成となっている．また，グループでのディスカッションを多く取り扱っており，生徒自らが問題意識をもつことができるように構成されている．

710 で扱われている用語は 39 語であり，RSA 暗号や量子暗号，ハッシュ関数，WEP や TKIP といった無線 LAN の暗号化プロトコルなど，発展的な内容を多く取り扱っている．また，乗っ取りや，不正送金などサイバー犯罪の原因や対策についてのディスカッションも扱われている．

(10) 711/712 情報 I 図解と実習（日本文教）

711 は，図解というタイトルの通り，図を中心に構成されており，文章による説明は必要最小限に留めている．

711 にて扱われる用語は 27 語であり，学習指導要領に基づく基礎的な内容がその大部分を占めている．

712 は 711 の実習関連の内容のみを集約した書き込み式の別冊の教科書であるが，情報セキュリティに関する記述はない．

(11) 713 高等学校 情報 I（第一学習社）

713 は文章による説明を中心とし，適宜，図を用いることで視覚的に理解しやすい構成となっている．

713 で扱われる用語は 39 語となっており，基礎的な内容に加えて，認証 3 要素や，DoS 攻撃，PKI，SSL/TLS，無線 LAN の暗号化プロトコルなど発展的な内容を幅広く扱っている．また，シーザー暗号の生成に関する実習や，パスワードの強度に関する具体的な説明もなされており，学習内容の更なる定着を図ることができるようになっている．

3.2.4 用語の比較と考察

情報セキュリティの記述がない 712 を除外し，また 703 と 704 を 1 冊とした全 11 冊の教科書に用いられる情報セキュリティ関連用語は,「生体認証」と「バイ

オメトリクス」のような同義語を1語としてまとめると87語ある．ここで，用語ごとの掲載教科書数を表3.5に示す．

表 3.5 掲載教科書数の割合

掲載教科書数	用語数	割合 (%)
1	28	32.2
2	14	16.1
3	7	8.0
4	3	3.4
5	4	4.6
6	4	4.6
7	5	5.7
8	0	0.0
9	3	3.4
10	5	5.7
11	14	16.1
合計	87	100

(1) 全教科書に掲載のある用語

全11冊全ての教科書で扱われている用語は表3.6の通りであり，全体の僅か16.1%にあたる14語のみであった．情報セキュリティの3要素や，暗号化やデジタル署名といった情報セキュリティを確保するための基礎技術について扱われており，これらの内容は情報セキュリティ学習の基盤となる重要語句であると考えられる．

令和2年9月に日本学術会議は「情報教育課程の設計指針」を公表しており，カテゴリA4のレベル3として「情報セキュリティの考え方・原理と暗号などのセキュリティ技術の理解」が挙げられている．これは高等学校の情報科の必履修科目を通して全員が学ぶことが望まれる内容とされているものであり，表3.6に挙げられる用語は，これに合致している [49]．

表 3.6 全ての教科書に記述のある用語

用語	
パスワード	共通鍵暗号方式
機密性	公開鍵暗号方式
可用性	ファイアウォール
完全性	コンピュータウイルス
情報セキュリティ	不正アクセス
ユーザ ID	デジタル署名
暗号化	個人情報

(2) 過半数の教科書で掲載されている用語

過半数となる 6 冊以上の教科書に掲載されている用語は表 3.7 の通りであり，全教科書に掲載のある 14 語を含め全体の 35.6%にあたる 31 語である．

ランサムウェアや改ざんなどの近年増加している攻撃手法や，ソーシャルエンジニアリングやフィッシングなどの非常に身近な攻撃手法については掲載数が多いことが分かる．特に，ソーシャルエンジニアリングやフィッシングは高校生でも被害に遭う可能性が非常に高い攻撃手法であるので，全生徒が学ぶことが望ましいと考えられる．

また，2 章で述べたように，学習指導要領および解説には，暗号化プロトコルや，デジタル証明書，生体認証の掲載がある．しかし，表 3.7 から分かるように，これらの用語は一部の教科書で掲載されていない．これらの用語や具体的事項は，情報セキュリティを確保するための基本的な技術であるので，全生徒が学習するべきと考えられる．

表 3.7 過半数の教科書で掲載のある用語

掲載教科書数	用語
6	ワーム
	スパイウェア
	マルウェア
	ランサムウェア
7	サイバー犯罪
	セキュリティホール
	TLS
	定義ファイル
	デジタル証明書
9	情報セキュリティポリシ
	改ざん
	SSL
10	ソーシャルエンジニアリング
	認証
	生体認証
	ウイルス対策ソフトウェア
	フィッシング

(3) 掲載数の少ない用語

掲載されている教科書が 6 冊未満の用語は全体の 64.4%にあたる 56 語である．掲載数が 2 冊〜5 冊である用語を表 3.8，1 冊にのみ掲載のある用語を表 3.9 にそれぞれ示す．掲載数の少ない用語は，暗号化の具体的手法や暗号化プロトコルに関するものや，通信の監視に関するものなど情報セキュリティ技術についての用語が多くを占めている．これらの内容については，専門教科情報の「情報セキュリティ」において取り扱われるなど専門性が高い内容であり，全生徒が共通して学習することが望まれる内容とは考えにくい．そのため，生徒の興味関心に応じ学習内容の柔軟な対応が求められる．

しかし，認証の方法として 10 冊の教科書で生体認証の掲載がある（表 3.7）一方で，知識認証や所有物認証，またそれらを組み合わせる多要素認証についての掲載が少ない．しかし近年では，増加傾向にある各種サイバー犯罪への対策として多要素認証の設定が推奨されている [50] ため，知識認証や所有物認証など様々な認証方法についても全生徒が学ぶ必要があるものと考えられる．

表 3.8 掲載数の少ない用語

掲載冊数	用語	
5	フィルタリング	トロイの木馬
	二段階認証	DoS 攻撃
4	電子透かし	シーザ暗号
	キーロガー	
3	電子認証	アクセス制御
	RSA 暗号	多要素認証
	認証局	WEP
	WPA2	
2	ホワイトハッカー	ボット
	ブロックチェーン	セキュリティパッチ
	ハイブリッド暗号	知識認証
	所有物認証	自己伝染機能
	潜伏機能	発病機能
	クラッキング	サイバー攻撃
	DDoS 攻撃	アクセスログ

表 3.9 1 冊でのみ掲載のある用語

用語	
盗聴	ブルートフォース攻撃
標的型攻撃メール	FIDO 認証
パッチファイル	SMS 認証
アドウェア	IDS
IPS	DMZ
脅威	プライバシーマーク
バーナム暗号	真正性
責任追跡性	信頼性
否認防止	クラッカー
ハッカー	クッキー
スキミング	辞書攻撃
量子暗号	ハッシュ関数
TKIP	CCMP
ハッシュ値	PKI

3.2.5　調査のまとめ

情報Iの検定済教科書における情報セキュリティの取扱い状況について正確に把握して今後の教科指導に役立てるため，各検定済教科書において記載されている用語を調査・分析した．同じ科目でありながら，教科書会社や各教科書によって，取り扱われる内容には大きな差が生じており，利用する教科書によって学校間や生徒間で知識や技能に偏りが生じる可能性があることが分かった．

ICTが急速に普及し，情報セキュリティ対策の重要性が指摘される中で，全ての高校生が情報セキュリティに関する知識および技術を適切かつ効果的に活用する力を身に付ける必要がある．そのため，情報科担当教員は自校が採択している教科書以外で取り扱われる内容も考慮した教科指導が求められていくと考えられる．

第4章　公開講座の実施と評価

4.1　講座の概要

2022年10月に「君もハッカーに!?ハッキング体験で情報セキュリティについて学ぼう!」と題した公開講座を実施した．公開講座は学校が主催するものであり，内容や受講者の募集を学校として広報する．そのため，筆者が直接周知するよりも高い宣伝効果が期待でき，受講者を広く募ることができると考え，公開講座の枠組みを利用し，講座を実施した．

公開講座では，コロナ禍ということもあり，実施時間や定員に制約があった．そのため，今回は実施時間を2時間，定員を10名，募集の対象を中高生とした．中学生を中心として25名の申し込みがあったが，抽選を行い定員通りの10名にて講座を実施した．また，公開講座の会場として，本校の情報システム端末室1を利用した．

4.2　教育の手法

主な対象者は中高生であるため，情報セキュリティに関しては学び始めとなる者が多く参加すると考えられた．継続して学んでもらうためにも，情報セキュリティに触れる際に嫌悪感や困難さを抱かせてしまうことは避けたい．その一方で，公開講座は希望者のみの参加であるため，受講者は情報セキュリティに対してある程度の興味を持っているとも考えられた．

そこで，日本政府の人材育成の基本方針や筆者のこれまでの経験や取り組みを踏まえ，実際のペネトレーションツールを利用したハッキングの体験など，実機による実践的な演習を交えた教育手法を検討した．授業の題材としては，情報セキュリティに関する身近な内容とし，情報セキュリティを身近に感じてもらう内容である．これら2つの観点を踏まえ，講座の目的を,『身近に存在する危険性を体験的に学び，情報セキュリティの重要性を理解すること』とした．

4.3 講座の内容

検討の結果，表 4.1 に示す 10 項目について，実機を用いた演習を交えて，情報セキュリティに関する基礎的な知識や，ハッキング手法とその対策方法を体験的に学ぶ内容とした．

第 1 部は座学であり，情報セキュリティの定義や，サイバー攻撃手法，情報セキュリティに関連した法規など，情報セキュリティ学習の基盤となる知識を学ぶ．

第 2 部以降は演習である．まず第 2 部では，コンピュータに対するハッキングとして，ポートスキャンや辞書攻撃といった攻撃手法を体験する．

第 3 部では，Web ページに対する攻撃として，Web ページの背景を変更する，利用者を偽サイトに誘導する仕組みをつくるといった演習を実施する．

情報セキュリティ学習の基盤となる知識および技能を全受講者が理解することを目指し，第 3 部までの内容は，全受講者が進度を揃えて取り組む．また，講座の最後には第 4 部として，自由に演習する時間を設けることで，それぞれの受講者が，自分の興味のある攻撃やその対策方法を体験できるようにした．

講座はハッキングなどの演習を中心とした内容で構成されているが，システムに存在する脆弱性やそれに伴う被害，攻撃への有効な対策方法を学ぶことが講座の本来の目的である．そこで，ユーザ権限の設定や，接続元 IP アドレスの制限，強固なパスワード設定と解析といった演習を取り入れ，攻撃への対策方法についても体験的に学習できる内容とした．また，受講者が実際に攻撃者となることを抑止するため，サイバー犯罪となる行為やその事例についても講義した．

4.4 教材の開発

講座では，投影するスライド資料と，第 4 部の演習で使用する演習手順書の 2 種類の教材を作成した．受講者には，演習手順書と，スライド資料の一部を穴抜きにしたノートを印刷して配布した．

クロスサイトスクリプティングの説明に用いたスライドの一部を図 4.1 に，辞書攻撃の演習に用いたスライドの一部を図 4.2 および図 4.3 に，クロスサイトスクリプティングの演習で用いたスライドの一部を図 4.4 に示す．

表 4.1 公開講座の内容

部	内容
第 1 部	[1] 情報セキュリティの定義 [2] 不正アクセスについての説明 [3] クロスサイトスクリプティングについての説明 [4] SQL インジェクションについての説明 [5] 情報セキュリティ関連法規についての説明
第 2 部	[6] ポートスキャンの演習 [7] パスワード解析（辞書攻撃）の演習 [8] データベースへの不正侵入の演習
第 3 部	[9] クロスサイトスクリプティングの演習
第 4 部	[10] 自由に演習に取り組む

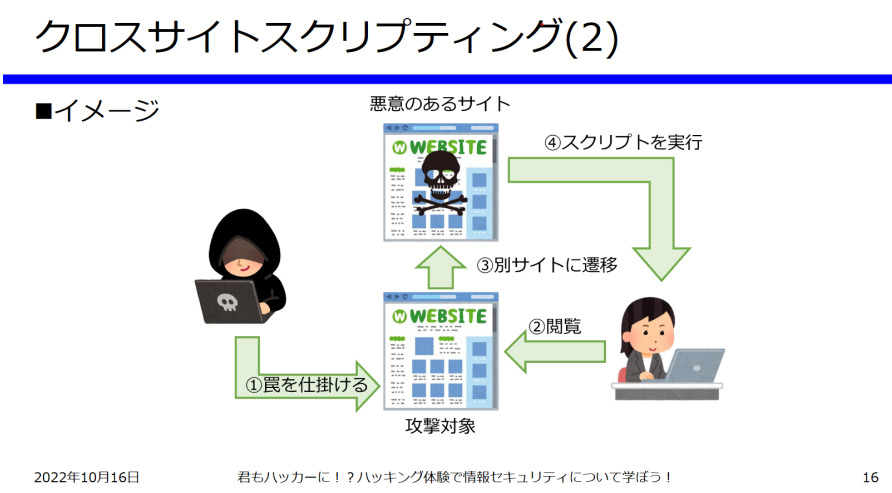


図 4.1 クロスサイトスクリプティングの説明のスライドの一部

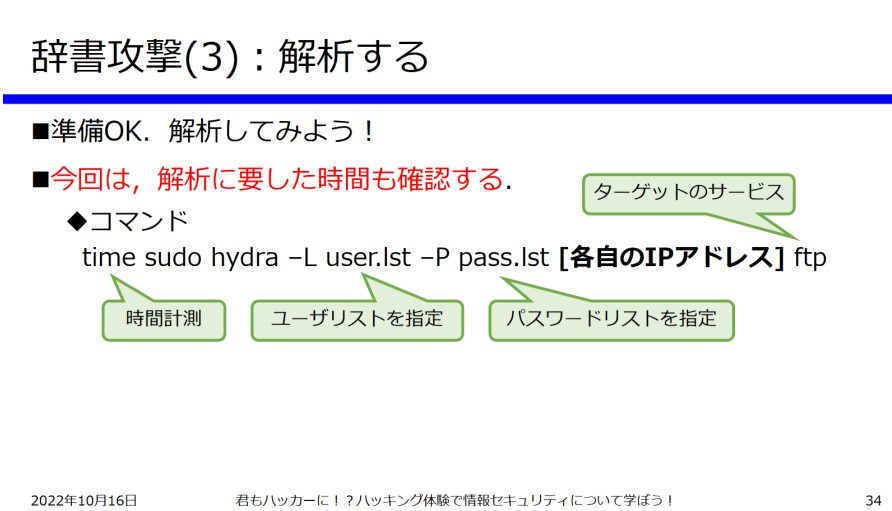
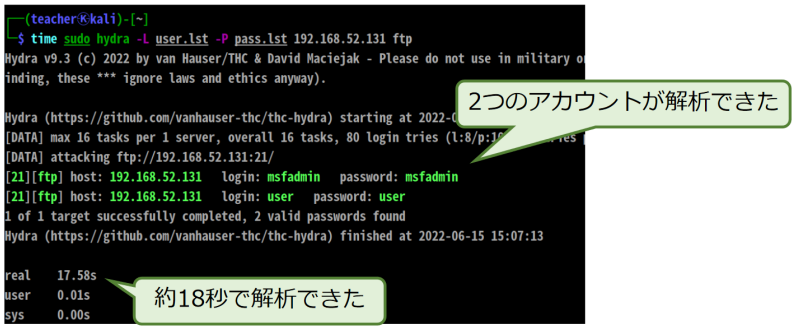


図 4.2 辞書攻撃のスライドの一部（コマンドの使用方法）

辞書攻撃(4)：実行結果

■実行結果



2022年10月16日　君もハッカーに！？ハッキング体験で情報セキュリティについて学ぼう！　35

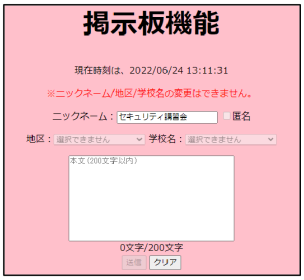
図 4.3 辞書攻撃のスライドの一部（コマンドの実行結果）

背景色の変更(3)：実装

■入力エリア（テキストボックス）に以下のHTML文を入力し送信.

◆<style>body{background:**pink**;}</style>

本文　　背景色の指定



◆実装は，「問題１」のページを使う

各自の端末のデスクトップに「html.txt」があるのでコピー＆ペースで利用可能

2022年10月16日　君もハッカーに！？ハッキング体験で情報セキュリティについて学ぼう！　59

図 4.4 クロスサイトスクリプティングの演習のスライドの一部

第 1 部の座学において使用するスライドでは，図 4.1 のように，図を用いて受講者が視覚的に理解できるようにするといった工夫を加えた．

第 2 部や第 3 部の演習で利用するスライドでは，図 4.2 から図 4.4 のように，実行結果の画像を添付する，実行結果の見方を細かく紹介するなどの工夫を加えた．

教材の作成では，K-SEC が公開する教材の一部を活用したほか，情報処理推進機構『情報セキュリティ読本』[47] や，瀬戸美月・齋藤健一『徹底攻略 情報処理安全確保支援士教科書 令和 4 年度』[51] を参考にした．

4.5 演習環境の構築

第 2 部では実機を用いた演習を実施するため，専用の演習環境を構築した．受講者が演習に取り組むための端末には，Raspberry Pi 4B [52] の 8GB モデルを利用し，OS として Raspberry Pi OS を利用した．攻撃用のクライアントには「Kali Linux」[53]，非被攻撃用サーバに「Metasploitable2」[54] を利用した．Kali Linux は，数多くのペネトレーションツールを標準で搭載しており，実際のセキュリティ検査の現場においても幅広く利用されている Debian 系 OS である．Metasploitable2 は，ペネトレーションの練習やテストのためにあえて脆弱性を持たせた仮想コンピュータであり，OS として Ubuntu が利用されている．

講座の受講者は，図 4.5 のように，各自の Raspberry Pi から Kali Linux へ SSH（Secure Shell）でリモート接続することで演習を実施した．

公開講座で利用するネットワークの構成を図 4.6 に示す．各端末は学校のネットワークの直下に設置されるが，Kali Linux および Metasploitable2 は仮想マシンとして「VMware Workstation Player」[55] を利用して構築した．構築には，IPUSIRON『ハッキング・ラボのつくりかた』[56] を参考とした．

また，第 3 部では Web ページに対する攻撃を体験するが，ここで利用する Web サイトは，筆者が所属する研究室の学生が作成したオリジナルサイトを利用した．

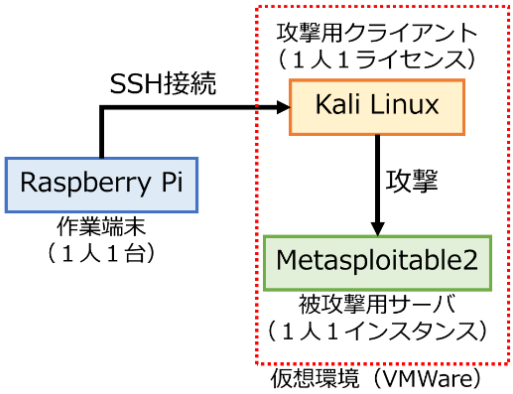


図 4.5 演習環境への接続方法

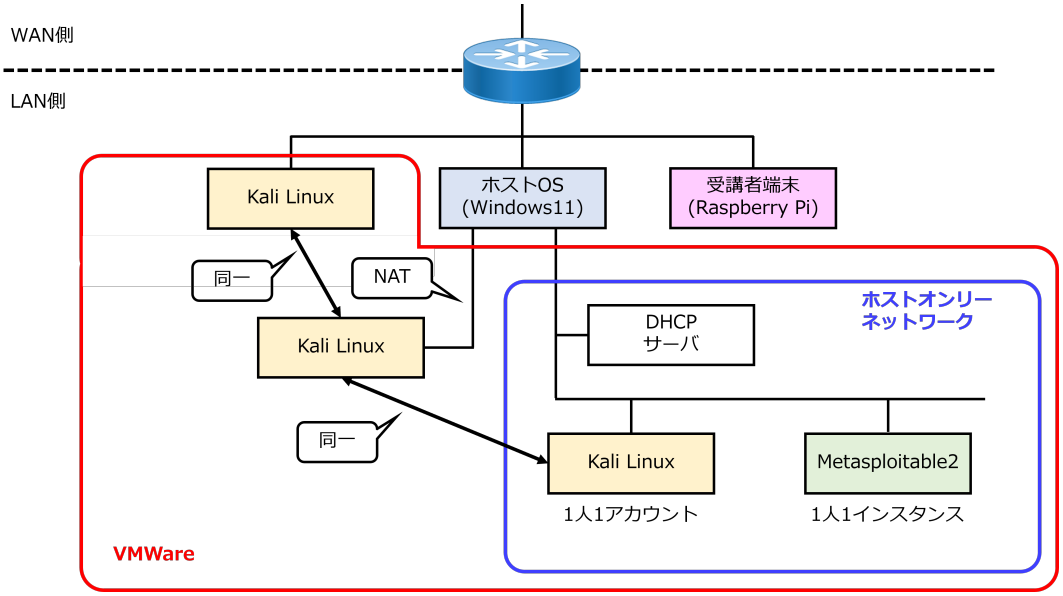


図 4.6 演習環境のネットワーク構成

4.6　授業の実践

講座は 10 月 16 日に実施し，講座当日のスタッフとして，筆者が講師を務めた．また本卒業研究の指導教員も対応し，開発した教材の確認や講師の補佐といった講座運営の補助を担った．講座当日の様子を図 4.7 および図 4.8 に示す．

図 4.7 公開講座での座学の様子

図 4.8 公開講座での演習の様子

講座の終了後にアンケートを実施し，10 名の受講者のうち，5 名から回答を得ることができた．

(1) 講座の進行速度についての評価

講座の進行速度について尋ねた結果を図 4.9 に示す．過半数の受講者が「適切」と回答している一方で，2 名の受講者が「やや速い」と回答している．受講者に配布したスライドの穴抜き資料には，文章を埋める箇所があった．この穴埋めのための時間が足りていないために，受講者は「やや速い」と感じたものと考えられる．

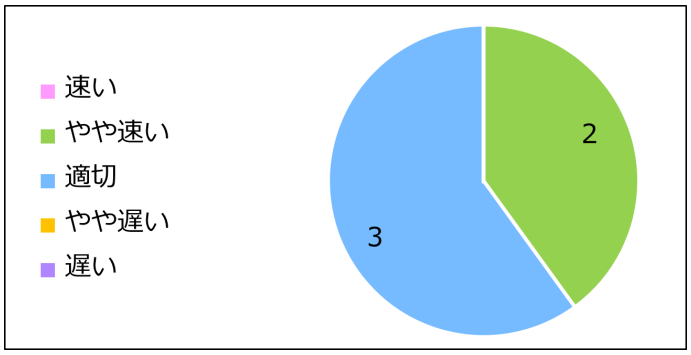


図 4.9 公開講座の進行速度に関する質問の回答結果

(2) 講座の実施時間についての評価

講座は 2 時間で実施したが，この実施時間が適切であったかを尋ねた．この結果を図 4.10 に示す．また，第 4 部として自由に演習に取り組む時間を 20 分設けたが，この時間が適切であったかを尋ねた．この結果を図 4.11 に示す．講座の実施時間については，多くの受講者が「適切」と回答している一方で,「やや長い」と「やや短い」との回答が 1 名ずつあった．また第 4 部の割当時間については「やや短い」との回答が過半数を占めた．このため，第 4 部の割当時間を増やし，演習に取り組みたい受講者のみが演習を継続できる時間を設けるなど，講座時間の調整が行える講座内容を組む必要があると考えられる．

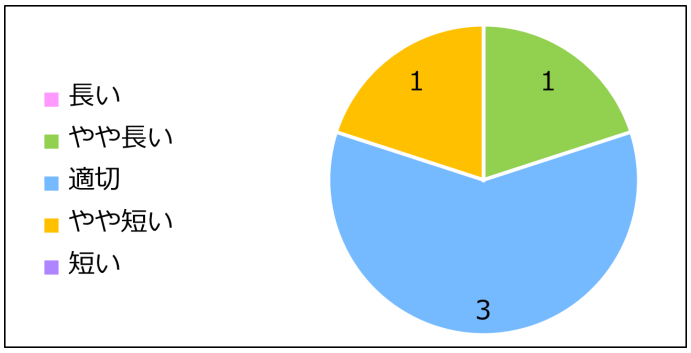


図 4.10 公開講座の実施時間に関する質問の回答結果

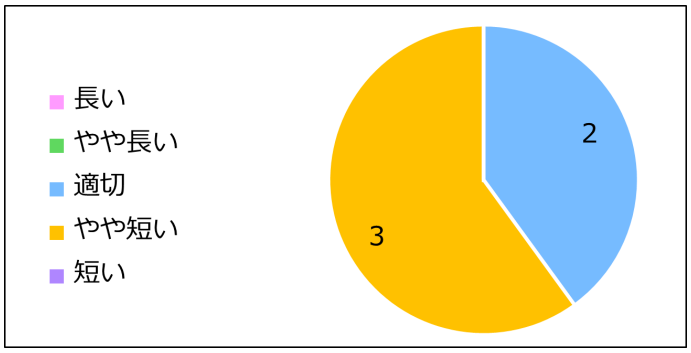


図 4.11 第 4 部の割当時間に関する質問の回答結果

(3) 説明についての評価

講座中の説明が分かりやすいものであったかを尋ねた．この結果を図 4.12 に示す．多くの受講者が「分かりやすい」と回答し，高い評価を得ることができた．講座中では，身近における例を示した説明を行うなどの工夫を行ったため，高い評価を得ることができたと考えられる．

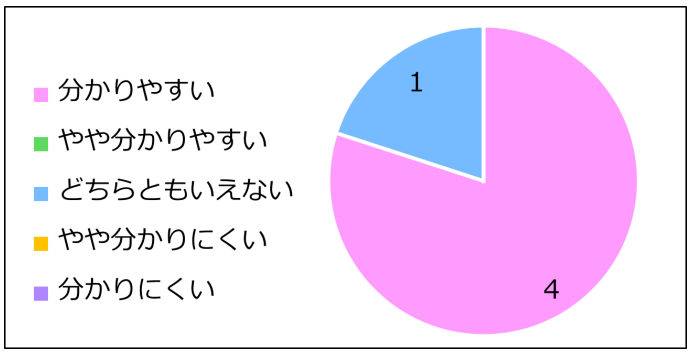


図 4.12 公開講座の説明に関する質問の回答結果

(4) 教材についての評価

講座で利用した教材についての評価を尋ねた．スライドが分かりやすいものであったかを尋ねた結果を図 4.13，演習手順書が分かりやすいものであったかを尋ねた結果を図 4.14 に示す．いずれの教材についても多くの受講者が肯定的な回答をしている．これは，教材開発においてイラストを多用するなどの工夫を行っており，この点が評価されたと考えられる．

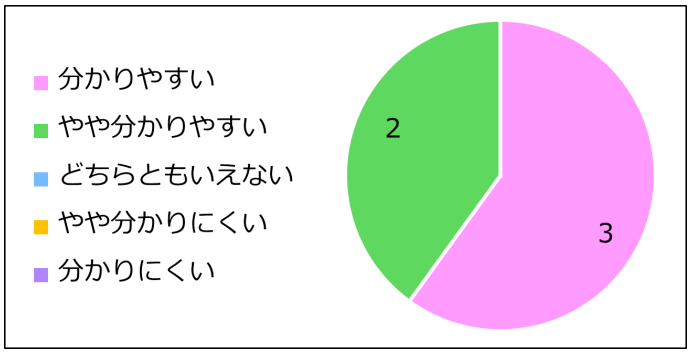


図 4.13 公開講座のスライドに関する質問の回答結果

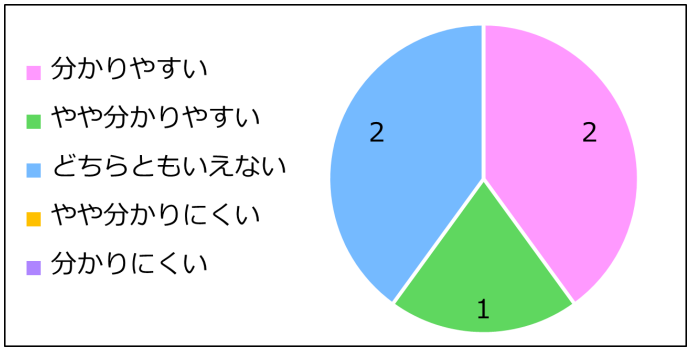


図 4.14 公開講座の演習手順書に関する質問の回答結果

(5) 講座内容についての評価

講座内容についての評価を尋ねた．興味を持てた内容の結果を図 4.15 に，興味が持てなかった内容の結果を図 4.16 に示す．なお，各図中の選択肢は，表 4.1 の学習項目に対応している．SQL インジェクションの説明に対して改善が必要との声が多い結果となった．これは日常生活との関わりが薄く，受講者がイメージしにくいためだと考えられる．一方で，演習に関しては好評価を受けており，セキュリティ学習の動機付けとして効果があると考えられる．

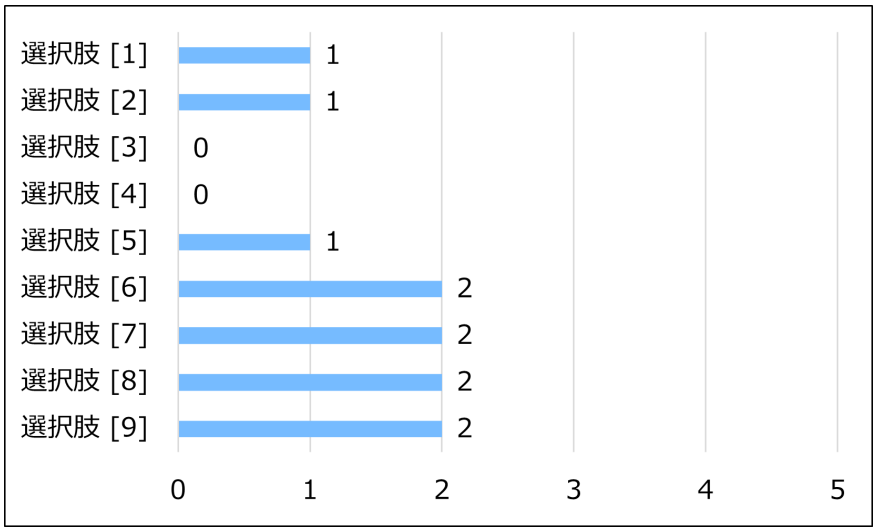


図 4.15 公開講座で興味が持てた内容の回答結果

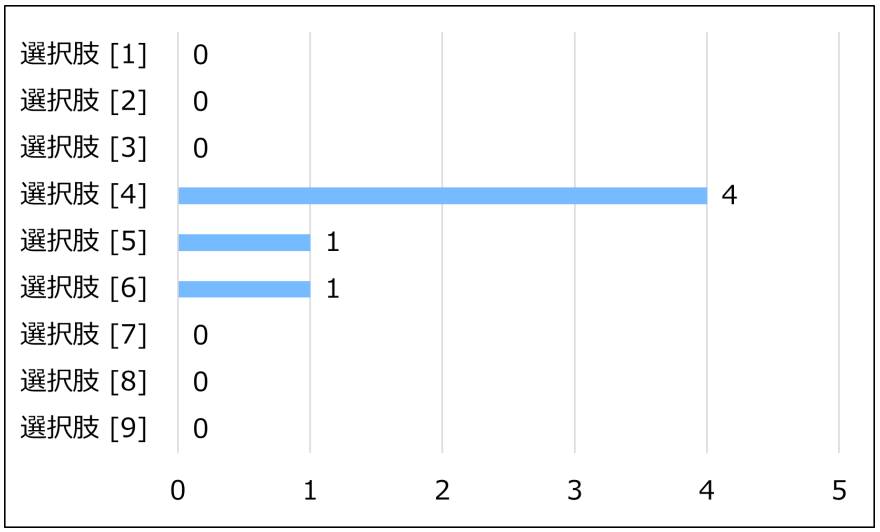


図 4.16 公開講座で興味が持てなかった内容の回答結果

(6) 今後の講座参加への意欲について

今後も同様の講座がある場合に，参加したいかを尋ねた．この結果を図 4.17 に示す．5 名全員から肯定的な回答を得ることができた．そのため,『情報セキュリティ学習を継続してもらうため，情報セキュリティに触れる際に嫌悪感や困難さを抱かせてしまうことは避ける』という講座の目標を達成できていると考えられる．

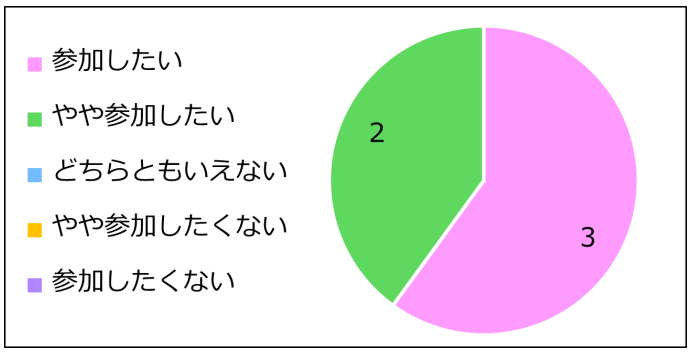


図 4.17 今後の講座参加に関する質問の回答結果

(7) 講座の満足度

講座の満足度を，1 から 5 までの 5 段階で尋ねた．この結果を図 4.18 に示す．結果，全ての受講者から肯定的な回答があり，(6) の結果と併せ，今後の講座開催に一定の需要があると考えられる．

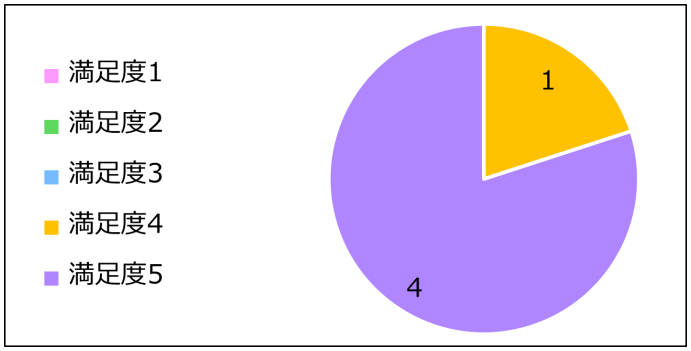


図 4.18 公開講座の満足度に関する質問の回答結果

(8) 感想など

感想などの自由記述では，今後学んでみたい内容として「DoS 攻撃」が挙げられた．近年では，DoS 攻撃がニュースなどで話題になることが多いため，受講者にとって馴染みのある攻撃手法であると言える．今後は，話題性のある内容を交えた教育内容を検討していく必要があると考えられる．

第5章　米子東高校での授業実施と評価

5.1　授業の概要

8月に，本校教員の紹介により，米子東高校の情報科担当教員（以下，情報科教員という）の方と知り合う機会があり，米子東高校の希望する生徒に対して授業を行うこととなった．授業は，米子東高校の土曜日活用授業として企画した．教育課程外での実施となるため，希望者のみを対象として参加者を募集したところ，1年生および2年生から30名の申し込みがあり，当日は27名が参加した．

5.2　授業の設計

5.2.1　設計の方法

授業を設計するにあたり，参加申し込みのあった生徒に対して事前にアンケートを実施した．アンケートは，情報授業に対する意見や要望，情報セキュリティに関する知識および技能の現状を調査するものであり，3.1節で述べた，学内で実施したアンケートと同様の質問である．

参加申し込み数が30名であるのに対し，アンケートの回答は32件であり，数名の生徒が複数回答していた．しかし，回答を匿名にするために，個人を識別できる設問は用意しておらず，複数回答している生徒の回答は特定できなかった．そのため，ここでは32名として集計・分析した．

5.2.2　事前アンケートの結果と分析

(1) 情報授業に対する意見

情報の授業に対する意見や要望を尋ねたところ，以下の回答があった．

- 具体的な例を挙げて説明してほしい．
- ペアワークなどを増やして，興味をもって授業を受けれるようにしてほしい．
- 語句だけでは理解しづらく，実際に生徒が触って実行したりする機会を増やしてほしい．

生徒からは教育手法に関して多くの指摘があり，授業実施の際にはこれらを解決できる授業方法を検討する必要が考えられる．

(2) 「情報モラル」の認知度について

「情報モラル」について，どのようなものか知っているかを尋ねた．この結果を図 5.1 に示す．またまた「知っている」と回答した生徒に対し，情報モラルと聞いたときにイメージすることを尋ねたところ，誹謗中傷や個人情報，著作権などの回答があった．

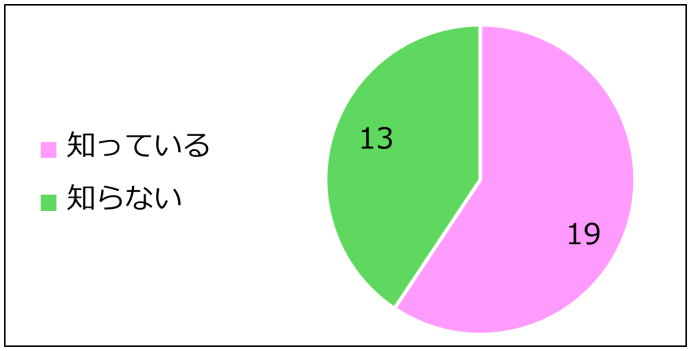


図 5.1 米子東高校における情報モラルの認知状況

(3) 「情報セキュリティ」の認知度について

「情報セキュリティ」について，どのようなものか知っているかを尋ねた．この結果を図 5.2 に示す．また「知っている」と回答した生徒に対し，情報セキュリティと聞いたときにイメージすることを尋ねたところ，情報の保護や，不正アクセス，パスワード，暗号化などの回答があったが，SNS の使い方や権利の保護など，情報モラルに関する内容を挙げている生徒はいなかったため，情報モラルと情報セキュリティの違いについて，一定の理解があると考えられる．

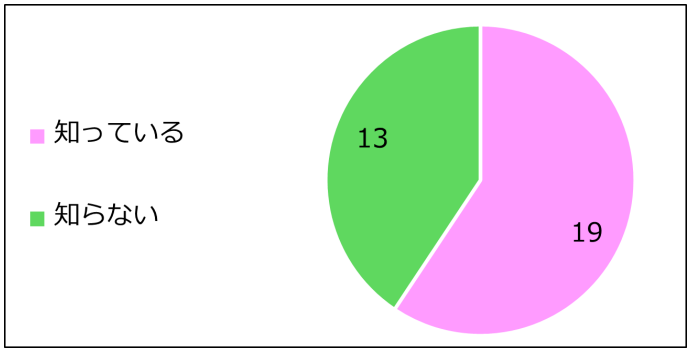


図 5.2 米子東高校における情報セキュリティの認知状況

(4) 情報モラル・情報セキュリティ教育の受講経験

情報モラルや情報セキュリティに関する教育を受けたことがあるかを尋ねた．この結果を図 5.3 に示す．4 割の生徒が「受けたことがある」と回答している一方，3 割の生徒が「受けたことはない」と回答した．また「受けたことがある」と回答した生徒に対して，その内容を尋ねたところ，個人情報の保護や，SNS による誹謗中傷などが挙げられ，情報モラルに関するものが回答の多くを占めていた．また，語句の意味を学習した程度との回答もあり，情報モラル教育，情報セキュリティ教育ともに学習内容が満足とは言えない．

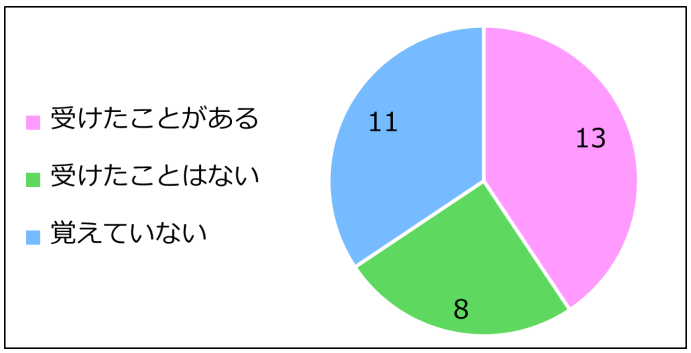


図 5.3 米子東高校における情報セキュリティ教育の受講経験

(5) 情報セキュリティに関する興味関心

情報セキュリティに関して興味や関心があるかを尋ねた．この結果を図 5.4 に示す．非常に多くの生徒から肯定的な回答を得ることができた．本調査の対象は授業に参加を希望した生徒であるため，妥当な結果であると考えられる．

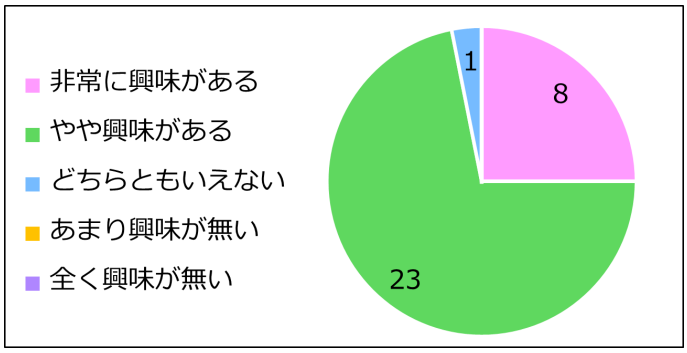


図 5.4 米子東高校における情報セキュリティへの興味の状況

(6) インターネット利用における不安

日頃のインターネット利用で不安に感じることがあるか尋ねた．この結果を図 5.5 に示す．3 分の 1 の生徒が「不安がある」と回答している一方，多くの生徒が「不安がない」と回答している．ICT の普及により，我々の身近なところでもサイバー犯罪被害に遭う可能性が高いため，生徒が危機感を感じられるように教育の必要がある．また「不安がある」と回答した生徒に対し，不安の内容を尋ねたところ，なりすましや乗っ取りなど，SNS 利用に関する面で不安を感じている生徒が多い結果となり，これらに対する教育が必要であると考えられる．

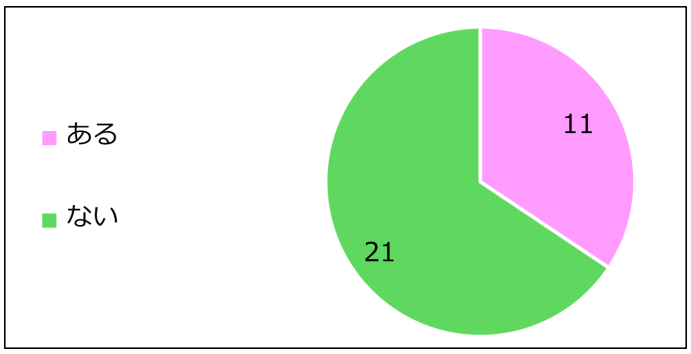


図 5.5 米子東高校におけるインターネット利用における不安の有無

(7) 情報セキュリティの生活への意識状況

情報モラルや情報セキュリティを日常生活で意識しているかを尋ねた．この結果を図 5.6 に示す．半数の生徒が意識していると回答している一方で，1 年生では意識していない生徒が一定数見受けられ，教育内容の改善が求められていると考えられる．また「意識している」または「やや意識している」と回答した生徒に対して，どのようなことを意識しているか尋ねたところ，個人を特定可能な情報は発信しない，パスワードは他人に分かりにくいようにするなどの回答があった．このため，一部の生徒は，共通教科「情報 I」の教科書に記述があり，授業で扱われる範囲内の対策は実践できていると考えられる．

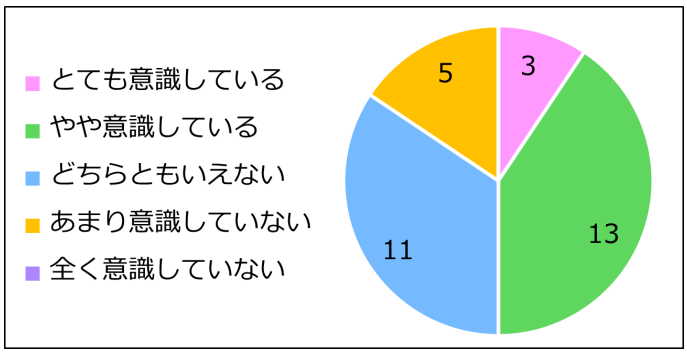


図 5.6 米子東高校における情報セキュリティの生活への意識状況

(8) 各種サイバー攻撃に関する知識および技能

表 5.1 に示す各サイバー攻撃について，表 5.2 の尺度で，生徒の持つ知識および技能の状況を調査した．この結果を図 5.7 に示す．なお評価の尺度は，株式会社ラック『情報リテラシー啓発のための羅針盤』[12]，文部科学省『平成 30 年告示高等学校学習指導要領』[38]，国立高等専門学校機構『モデルコアカリキュラム』[39] を参考とした．また株式会社ラック『情報リテラシー啓発のための羅針盤』より，高校生が満たすべきスキルを Lv.3 と定義する．

表 5.1 調査したサイバー攻撃の一覧

質問番号	攻撃名
質問 1	不正アクセス
質問 2	マルウェア
質問 3	DoS 攻撃
質問 4	フィッシング
質問 5	パスワードリスト攻撃
質問 6	標的型攻撃
質問 7	偽セキュリティソフト
質問 8	偽警告
質問 9	ランサムウェア
質問 10	不正ログイン
質問 11	ソーシャルエンジニアリング
質問 12	架空請求
質問 13	クロスサイトスクリプティング
質問 14	SQL インジェクション
質問 15	クロスサイトリクエストフォージェリ
質問 16	OS コマンドインジェクション

表 5.2 スキルの評価尺度

レベル	スキル
Lv.0	全く知らない
Lv.1	名前は聞いたことがある
Lv.2	概要をある程度知っている
Lv.3	対処法を知っている
Lv.4	対策が実践できる
Lv.5	第三者に説明できる

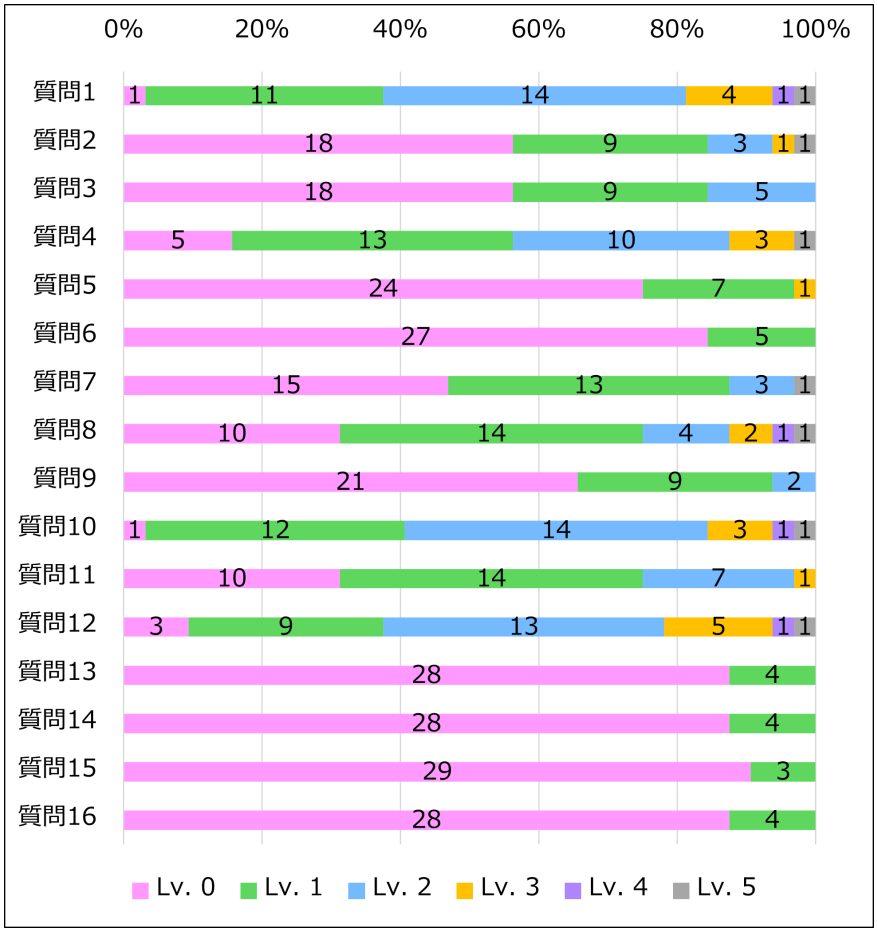


図 5.7 米子東高校におけるサイバー攻撃に関する知識及び技能の状況

結果，多くの攻撃手法について，Lv.3 を満たしている生徒は 1 割未満であり，知識および技能が不足していることが分かる．特に，マルウェアやソーシャルエンジニアリング，不正ログインなど，身近な攻撃についても知識や技能が不足しており，身近な攻撃手法から教育する必要があると考えられる．

(9) サイバー犯罪被害の経験について

次のようなサイバー犯罪被害に遭ったことがあるかを尋ねた．この結果を図5.8に示す．いずれかの経験をした生徒のうちの過半数が，偽の警告画面が表示されたことがあると回答している．しかし，(8)の結果の通り，対処法などを知っている生徒が少なく，教育の必要があると考えられる．

1. 何者かによる不正アクセスが試みられたというメールを受信した．
2. メールの添付ファイルを開いた結果，ファイルが暗号化された．
3. URLのアクセスと，ID・パスワードなどの入力を求めるメールやSNSメッセージを受信した．
4. 突然，ブラウザに「ウイルスに感染した」と警告画面が現れた．
5. 宅配便の不在通知がSMS（ショートメッセージサービス）でスマホに届いた．
6. 「あなたのスマホはウイルスに感染しています」という警告画面が表示された．
7. 上記のような経験はない．
8. 上記のようなトラブルや被害があったかどうかわからない．

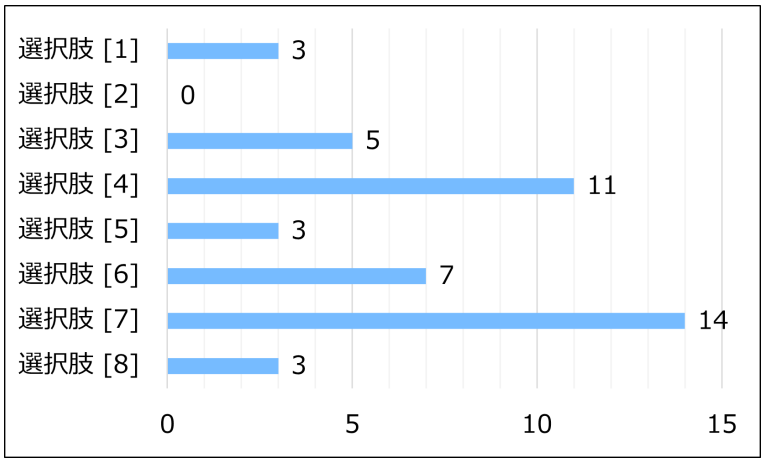


図 5.8 米子東高校におけるサイバー犯罪被害の経験状況

(10) 情報セキュリティ対策の実施状況

以下のような情報セキュリティ対策を実施しているかを尋ねた．この結果を図 5.9 に示す．結果より，いずれの対策も実施していない生徒は 1 人もおらず，多くの生徒が適切な対策を取っていることが分かる．パスワードの設定ルールに関しては，授業での取り扱いもあり，高い実施率である一方で，同じく授業での取り扱いがある，パスワードの使いまわしや初期パスワードの変更などについては，実施率が低く，教育が不十分であると考えられる．また，データのバックアップや，売却時のデータ消去といった，データの取扱いは，授業内での取り扱いがないため実施率が低く，教育の必要があると考えられる．

1. パスワードは他人が推測しにくい（氏名や誕生日などの情報を用いない）内容を設定している．
2. パスワードはできるだけ長い文字数（8〜10 文字以上）を設定している．
3. サービス毎に異なるパスワードを設定している（使いまわしていない）．
4. 初期パスワードが設定されている場合は，そのまま使わず必ず変更している．
5. セキュリティ対策ソフトやサービスを利用している．
6. パソコンやスマートフォンのデータをバックアップしている．
7. OS などのソフトウェアやアプリケーションはサポートが切れていないものを使用し，かつ最新の状態にアップデートしている．
8. スマートフォンやパソコンを廃棄または売却する際は，データが復元できないような消去または物理的な破壊を行っている．
9. 自宅のパソコンを家族で使う場合，利用者毎にアカウント（ID，パスワード）をわけている．
10. メールや SNS メッセージにある添付ファイルは不用意に開かない，また本文中の URL も不用意にクリックしないようにしている．

11. 怪しいと思ったホームページに行き着いたら先に進まない，情報を入力しないようにしている．

12. パソコンやスマートフォンには，ログインパスワードを設定している．

13. パスワード，指紋，ワンタイムパスワードなどから 2 種類以上の要素を組み合わせた多要素認証を積極的に利用している．

14. アプリをインストールする前または実行時に要求される権限を確認している．

15. 1 つも実施していない．

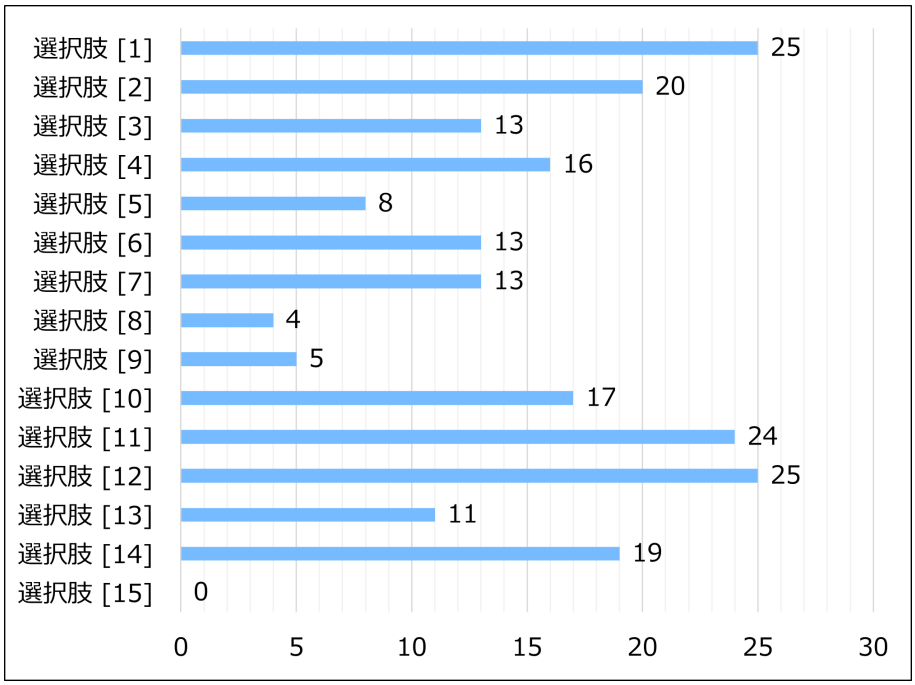


図 5.9 米子東高校における情報セキュリティ対策の実施状況

5.2.3 教育の手法と内容

事前のアンケート結果を踏まえ，以下の2点を重視した授業を行うこととし，表5.3に示す構成とした．

1. 身近な内容を取り扱う

2. 実機による演習のみならず，グループワークを取り入れる

表 5.3 授業の構成

部	授業項目
第1部	[1] 情報セキュリティについての説明 [2] 不正アクセスについての説明 [3] 標的型攻撃についての説明 [4] ソーシャルエンジニアリングについての説明 [5] マルウェアについての説明 [6] マルウェアについてのグループワーク
第2部	[7] ポートスキャンの演習 [8] パスワード解析（辞書攻撃）の演習 [9] パスワード解析（総当たり攻撃）の演習 [10] データベースへの不正侵入の演習
第3部	[11] シーザ暗号（暗号化／復号）の演習 [12] アクセス制御の演習 [13] ログ分析の演習 [14] サイバー犯罪の紹介

授業は3部構成で行い，第1部は座学であり，身近に存在する攻撃手法と対策方法を説明した．マルウェアについては，冒頭にマルウェアの定義や分類について説明した後，感染経路と対策方法について考えるグループワークを実施した．

グループワークは3人または4人のグループで，感染経路と対策について15分で話し合いをしてもらった．話し合いの後には，各グループで出た意見を全員で共有し，他者の意見や考えに触れる機会を設けた．最後には，まとめとして，感染しないための対策と感染後の対応について講義した．

第2部はハッキング体験であり，実際のペネトレーションツールを利用した演習を実施した．

第3部では，第2部で述べた攻撃に対する対策についての演習を実施した．また，サイバー犯罪には証拠が残ることをアクセスログの解析を通して説明した．

5.3　教材の開発

授業では，投影するスライド資料と，グループワークで利用するワークシートの 2 種類の教材を作成した．生徒には，ワークシートと，スライド資料の一部を穴抜きにした授業ノートを印刷して配布した．

ソーシャルエンジニアリングの説明に用いたスライドの一部を図 5.10 に，総当たり攻撃の演習に用いたスライドの一部を図 5.11 に，ログ解析の演習で用いたスライドの一部を図 5.12 にそれぞれ示す．

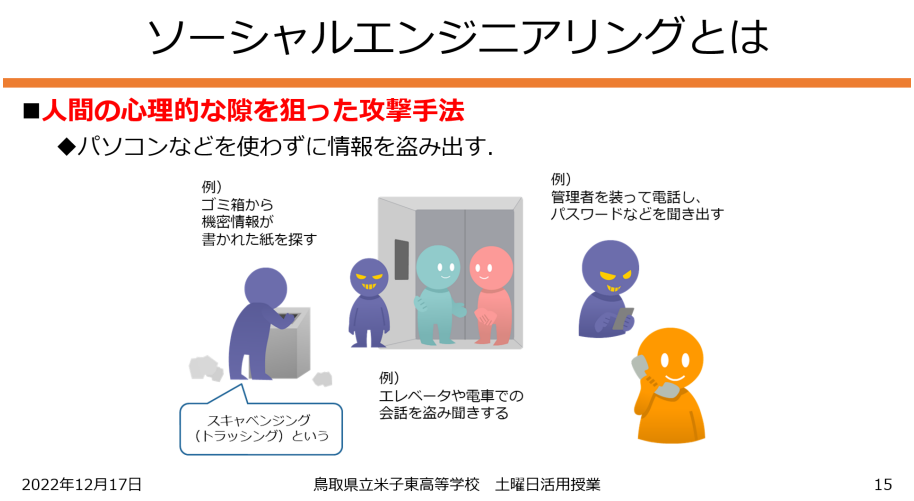


図 5.10 ソーシャルエンジニアリングのスライドの一部

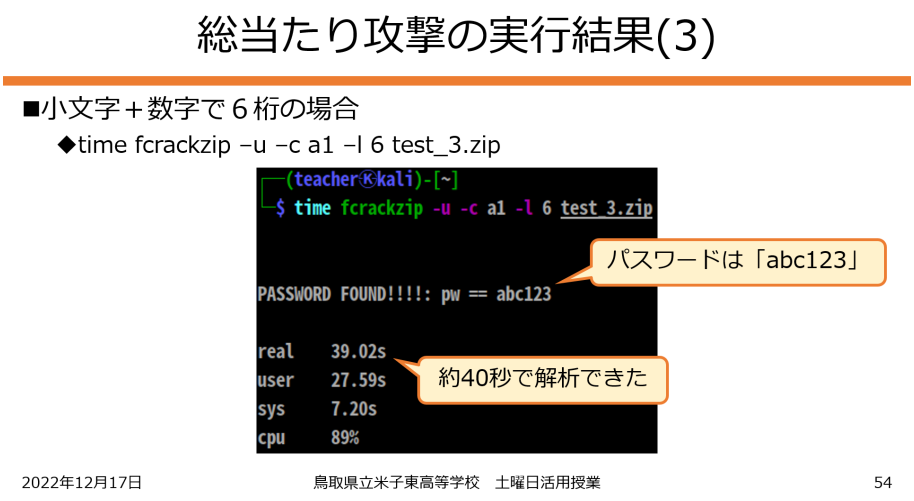


図 5.11 総当たり攻撃のスライドの一部

図 5.12 ログ解析演習のスライドの一部

第 1 部の座学において使用するスライドでは，図 5.10 のように，図を用いて生徒が視覚的に理解できるようにする，重要な箇所は赤字にするといった工夫を加えた．

第 2 部や第 3 部の演習で利用するスライドでは，図 5.11 や図 5.12 のように，実行結果の画像を添付する，実行結果の見方を細かく紹介するなどの工夫を加えた．

教材の作成では，K-SEC が公開する教材の一部を活用したほか，高等学校「情報 I」検定済み教科書全 13 冊，JPCERT コーディネーションセンターの講演資料 [57]，情報処理推進機構『情報セキュリティ読本』[47]，齋藤孝道『マスタリング TCP/IP 情報セキュリティ編』[58] を参考にした．

5.4　演習環境の構築

第 2 部および第 3 部では，実機を用いた演習を実施するため，第 4 章ど同様に，専用の演習環境を構築した．第 4 章と同様に，攻撃用のクライアントには「Kali Linux」[53]，非被攻撃用サーバに「Metasploitable2」[54] を利用した．

授業の参加者は，図 5.13 のように，各自の作業用端末から Kali Linux へ SSH でリモート接続することで演習を実施した．米子東高校では，生徒の学習用端末として 1 人 1 台，Chromebook 導入している．そこで生徒の作業用端末は各自が所有する Chromebook を利用した．

授業当日に利用するネットワークの構成を図 5.14 に示す．当日は，外部への通信ができない専用の回線を用意し，演習を実施した．

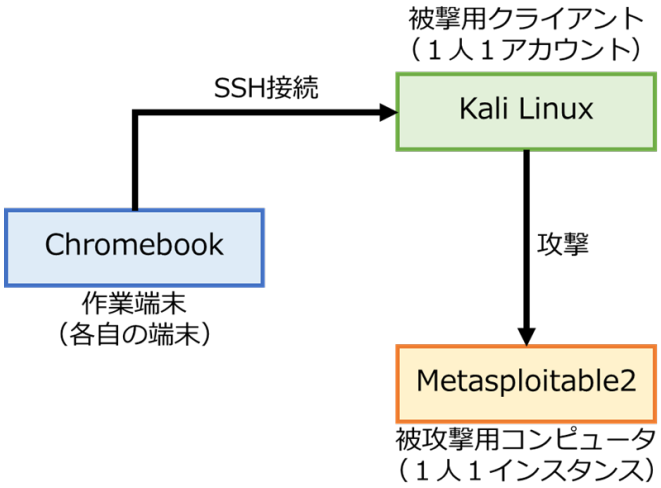


図 5.13 演習環境への接続方法

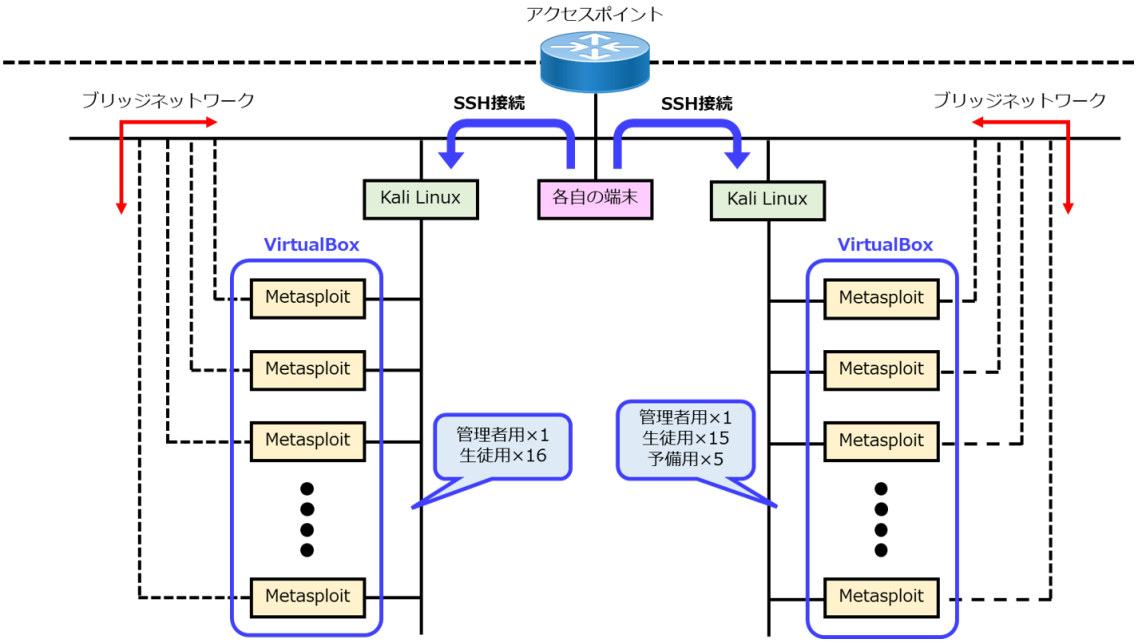


図 5.14 演習環境のネットワーク構成

5.5　授業の実践

授業は 12 月 17 日土曜日の 9 時から 12 時までの 3 時間で実施し，滞りなく終えることができた．当日は，筆者が講師を務め，本校学生 2 名，本校指導教員，情報科教員が補助についた．授業当日の様子を，図 5.15 および図 5.16 に示す．

図 5.15 授業中の講義の様子

図 5.16 授業中の演習の様子

授業後には，アンケートを実施し，生徒 25 名と情報科教員から回答を得ることができた．以下，アンケート結果とその分析について述べる．

5.5.1　参加生徒に対するアンケートの結果と分析

(1) 授業の進行速度についての評価

授業の進行速度について尋ねた結果を図 5.17 に示す．多くの生徒から「適切」との回答を得ることができた．一方で,「やや遅い」と回答した生徒が 5 分の 1 を占めており，授業運営に課題があることが分かる．

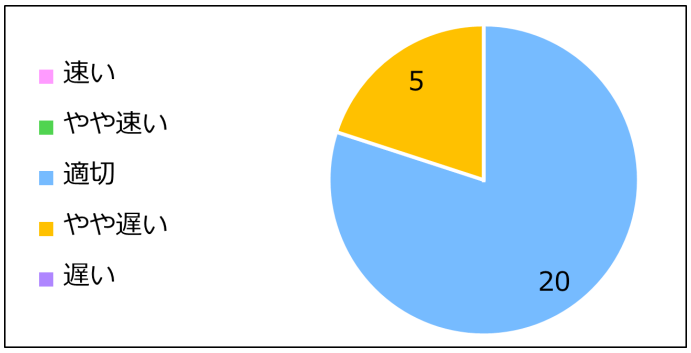


図 5.17 授業の進行速度に関する質問の回答結果

(2) 授業の実施時間についての評価

授業は 3 時間で実施したが，この実施時間が適切であったかを尋ねた．この結果を図 5.18 に示す．多くの生徒が「適切」と回答している一方で,「やや長い」や「やや短い」との回答もあった．このため，公開講座のように，自由参加で演習に取り組む時間を設けるなどし，対応していく必要があるものと考えられる．

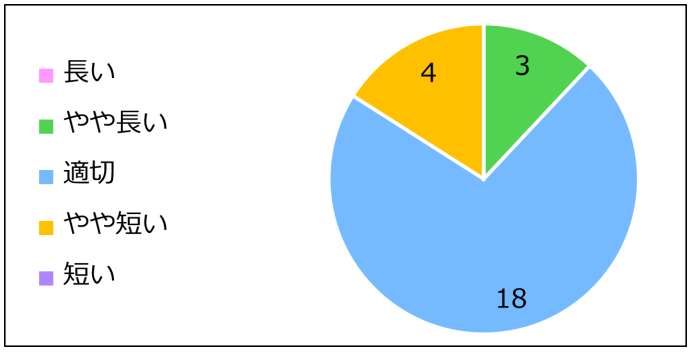


図 5.18 授業の実施時間に関する質問の回答結果

(3) 説明についての評価

授業中の説明が分かりやすいものであったかを尋ねた．この結果を図 5.19 に示す．多くの生徒が肯定的な回答であり，高い評価を得ることができた．授業中では，身近における例を示した説明を行うなどの工夫を行ったため，高い評価を得ることができたと考えられる．

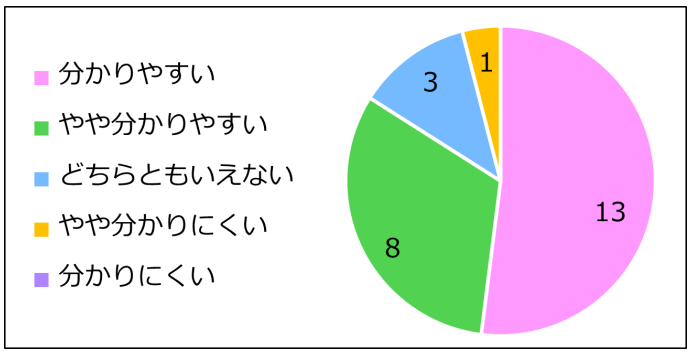


図 5.19 授業の説明に関する質問の回答結果

(4) 教材についての評価

授業中に利用した教材についての評価を尋ねた．スライドが分かりやすいものであったかを尋ねた結果を図5.20に，ワークシートが利用しやすいものであったかを尋ねた結果を図5.21に示す．いずれの教材についても多くの生徒から肯定的な回答を得ることができた．これは，教材開発においてイラストを多用する，コマンドの実行結果の画像を多く配置するなどの工夫を行っており，この点が評価されたと考えられる．

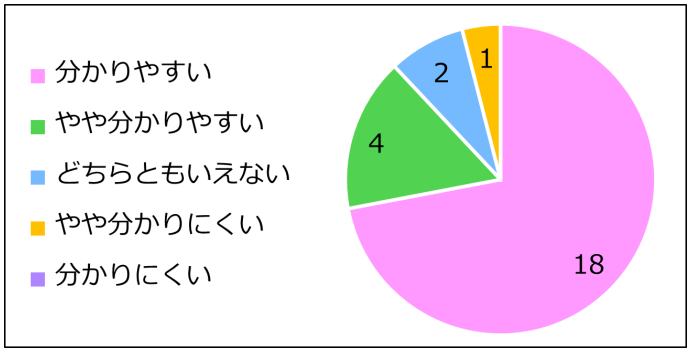


図 5.20 授業で利用したスライドに関する質問の回答結果

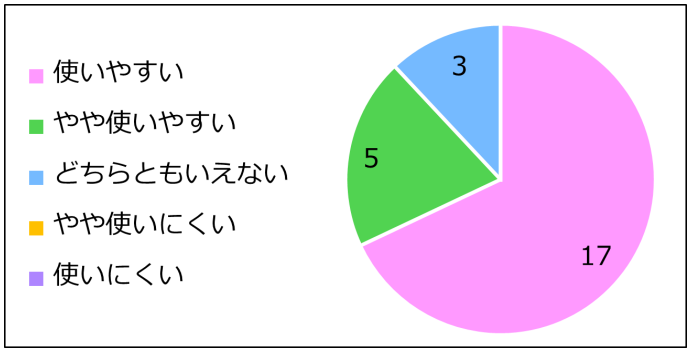


図 5.21 授業で利用したワークシートに関する質問の回答結果

(5) 授業内容についての評価

授業内容についての評価を尋ねた．興味を持てた内容の結果を図 5.22 に，興味が持てなかった内容の結果を図 5.23 に示す．なお，各図中の選択肢は，表 5.3 の学習項目に対応している．

興味を持てた内容についての回答の理由としては,『グループワークではほかの人の視点を知ることができ，理解が深まった』,『実施にどのようにして不正侵入が行われているのかわかった』,『今まで教科書で概念でしか知らなかったものを実際にハッキングすることで詳細に理解できた』などあり，グループワークや演習について高い評価を得ることができた．

一方で，興味が持てなかった内容，理解が難しかった内容についての回答の理由の多くは,『専門用語の理解が難しかった』であった．授業で習っていない用語をはじめ，専門用語について，その都度用語を説明するなどの工夫が必要であると考えられる．

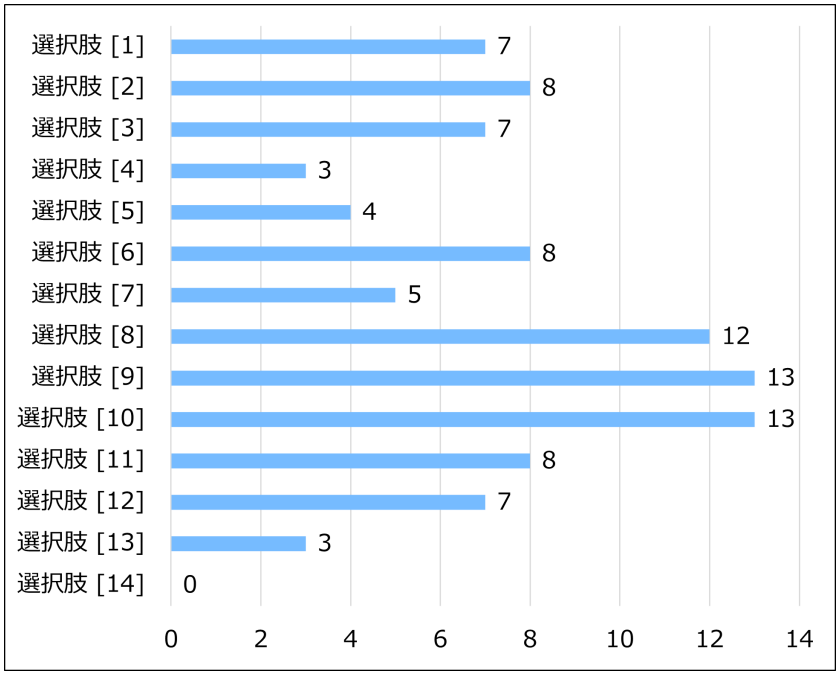


図 5.22 授業で興味が持てた内容の回答結果

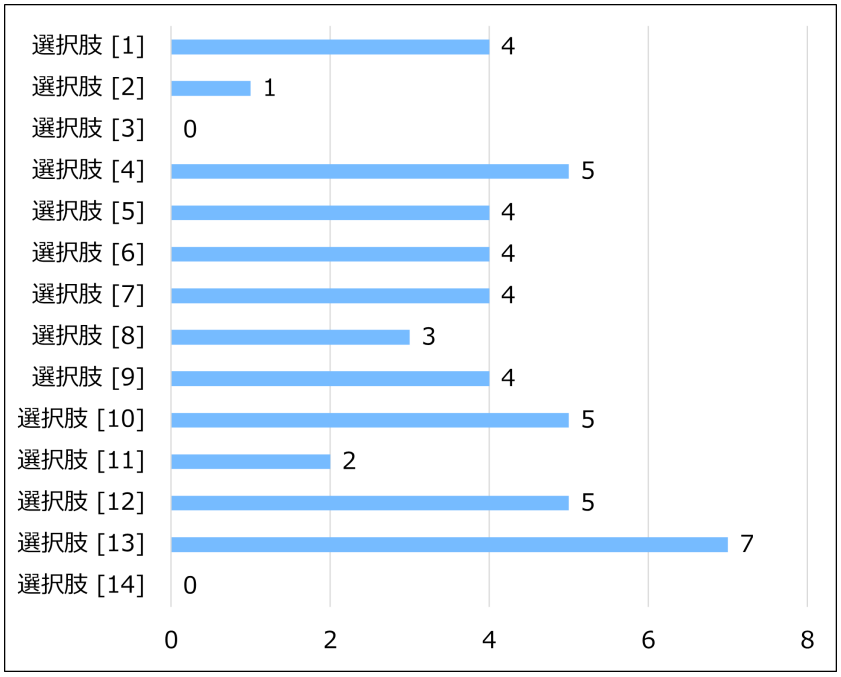


図 5.23 授業で興味が持てなかった内容の回答結果

(6) 学生が講師を務めることについての評価

学生が講師を務めることに対して，教員などの大人が講師を務める場合との比較を尋ねた．結果を図 5.24 に示す．7 割を超える生徒から肯定的な回答があり，その理由として,『生徒と講師の年齢が近いため親近感があり，質問がしやすかった』との声が多かった．

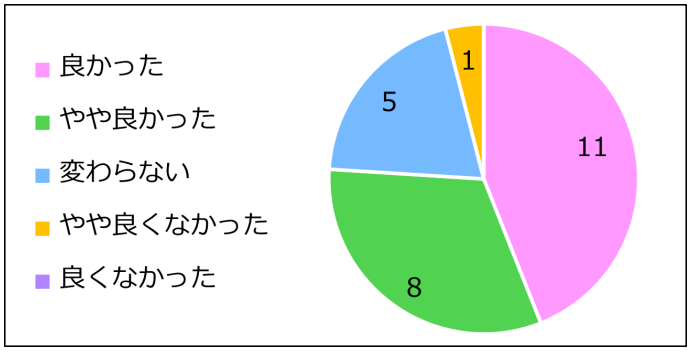


図 5.24 授業で学生が講師を務めることに関する質問の回答結果

(7) 今後の学生による教育活動についての意見

今後も学生が講師を務める教育活動を実施することについて意見を尋ねた．活動の実施に関する賛否の結果を図 5.25 に示す．多くの生徒から肯定的な回答を得ることができ，その理由として『学生の方々に教わる方が私たちと年齢も近く，気軽に学べて理解もしやすい』,『同じ年代の人の高度な専門的な知識に触れることで，学習意識が高まる』などの声があった．(6) の結果と併せて，共に高い評価を得ることができ，学生による教育活動は，講義を受ける生徒にとっても意義があるものと考えられる．

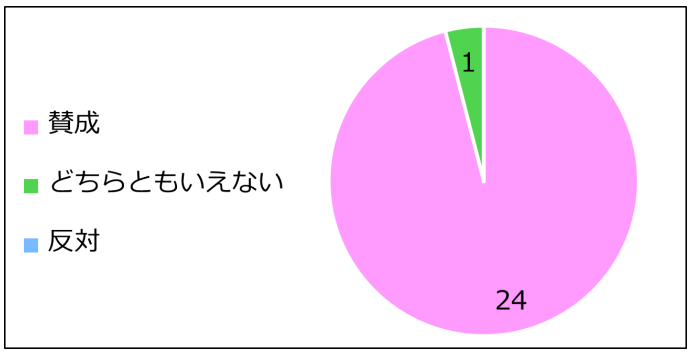


図 5.25 今後の学生による教育活動に関する質問の回答結果

(8) 授業の満足度

授業の満足度を，1 から 5 までの 5 段階で尋ねた．この結果を図 5.26 に示す．結果，多くの生徒から肯定的な回答があり，(7) の結果と併せて，今後の講座開催に一定の需要があるものと考えられる．

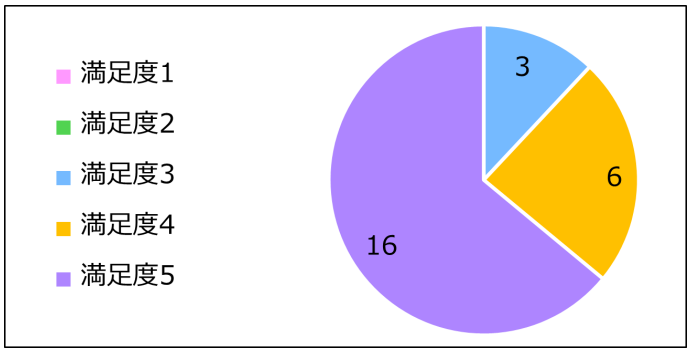


図 5.26 授業の満足度に関する質問の回答結果

(9) 感想など

感想などの自由記述では,『学校でやらないことを知ることができたのは良い経験になった』,『実際にハッキング体験をすることで，パスワードを解析される時間やどういう風に攻撃されるのかなど，目に見えてわかった』『学んだセキュリティ対策を日常生活でも実践していきたい』との高い評価を得ることができた．また,『次は，データベースの侵入以外の不正侵入を学びたい』との声もあり，参加する生徒のニーズに応えた授業設計についても検討する必要がある．

一方で,『演習のとき進度が遅い生徒に合わせていたので，することがない時間がかなり長かった』との声もあり，授業運営に対して課題があることが分かった．今後，習熟度別での授業実施を検討していく必要があると考えられる．

5.5.2　情報科教員に対するアンケートの結果

(1) 授業の進行速度についての評価

授業の進行速度について，図 5.17 と同様の尺度で尋ねた．結果,「適切」との評価を受けた.

(2) 授業の実施時間についての評価

授業の実施時間について，図 5.18 と同様の尺度で尋ねた．結果,「やや短い」との評価を受けた.

(3) 説明についての評価

授業の説明について，図 5.19 と同様の尺度で尋ねた．結果,「分かりやすい」との評価を受けた.

(4) 教材についての評価

授業で利用したスライド資料について，図 5.20 と同様の尺度で尋ねた．結果,「やや分かりやすい」との評価を受けた．併せて，この理由を尋ねたところ，以下の回答があった.

- 説明を聞きながら目で追う事のできる分量にまとめられていたこと
- 説明のスピードが適切で資料とあっている
- コマンドの入力において，コロンを入力する生徒が多いので改善が必要

(5) 授業内容についての評価

授業内容について，生徒が理解しやすかったと思われる項目として，以下の項目が挙げられた．この理由として『情報 I の授業では実習が時間的にも，準備においても難しく今回のように授業時間外で行うことができたのは生徒にとっても貴重な体験となった』との意見であった.

[3] 標的型攻撃についての説明

[7] ポートスキャンの演習

[8] パスワード解析（辞書攻撃）の演習

[9] パスワード解析（総当たり攻撃）の演習

[10] データベースへの不正侵入の演習

[11] シーザ暗号（暗号化／復号）の演習

その一方で，説明や内容に改善が必要な項目として，以下の項目が挙げられた．この理由として『データベースの概念がよくわかっていないため，生徒は何をやっているのかがよくわかっていなかったのではないか』,『サーバの名称をわかりやすいものに変えることでも，生徒の理解の助けることに繋がる』との指摘があった．

[10] データベースへの不正侵入の演習

[12] アクセス制御の演習

(6) 今後の学生による教育活動についての意見

今後も学生が講師を務める教育活動を実施することについて，図 5.25 と同様の尺度で尋ねた．結果,「賛成」との意見であった．この理由として,『授業の領域（学習指導要領）を超える内容を授業で扱うには時間的に難しい．また，内容も高度であり生徒にとっても刺激がある．今後，情報セキュリティに関する分野への進学を考える生徒が増えるようにするために，連携をしたい.』との声があった．また,『生徒の興味関心や視野を広げるためにも今後とも様々な連携ができると嬉しいと考えている』との意見も頂いた．

5.5.3　アンケート結果の分析

生徒に対する事後アンケートの (1)〜(5)，(7) の回答結果と同様，教育手法および内容について高い評価を得ることができた．一方で，教材については改善すべき点も挙げられた．改善点として挙げられたコマンド入力については，生徒が UNIX のコマンド操作に不慣れであることが原因だと考えられる．そのため，UNIX コマンドに関するルールなどをまとめた「チートシート」を作成するなど，UNIX コマンドに不慣れであることを考慮した教材作成で対応が可能であると考えられる．

第6章　鳥取県警との連携

6.1　連携の概要

鳥取県警察では，サイバー空間における県民生活の安全と平穏の確保に資することを目的として「鳥取県警察サイバー防犯ボランティア」（以下，ボランティアという）が運用されている．ボランティアの活動内容として，サイバー犯罪被害防止のための教育やサイバーセキュリティに関する広報啓発などが挙げられる [59].

本研究の実施にあたり，筆者が所属する研究室の学生 4 名および指導教員は団体として，このボランティアに登録し，鳥取県警察本部生活安全部サイバー犯罪対策課の方々と連携を行った．

6.2　連携の成果

連携の成果として，サイバー犯罪対策課からの打診により，8 月 21 日に倉吉市で開催された「GIGA スクールフェア 2022 in TOTTORI」[60] において講演を実施した．講演は，サイバー犯罪対策課の方々と連携して実施し，小学生とその保護者 8 組に対して「クイズで学ぼう インターネットで犯罪に巻き込まれないために」と題して講演を行った．

講演では，初めにサイバー犯罪対策課の方が，SNS やオンラインゲームを題材に，インターネット上の危険性についてクイズを交えて説明した．その後筆者が，インターネット上の危険性から身を守る対策を，SNS への投稿（図 6.1）やパスワードの管理（図 6.2）を題材に説明した．講演の様子を図 6.3 に示す．

なお，本講演のほか，4 章で述べた公開講座や，5 章で述べた米子東高校での授業についても，ボランティアの活動に繋がるものである．また，ボランティアの活動を開始した当初は，小中高校での警察と連携した出前授業の実施を検討していたが，警察からの授業の依頼が無かったため，実施できなかった．

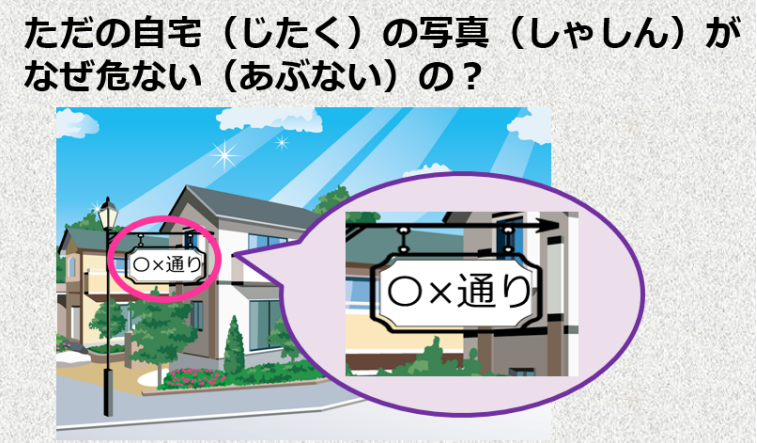


図 6.1 SNS の投稿に関するスライド

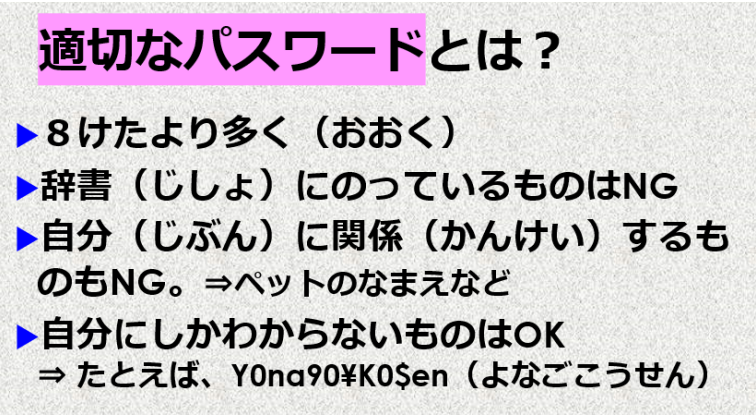


図 6.2 パスワードの設定に関するスライド

図 6.3 講演の様子

第7章　結論

7.1　本研究の成果

本研究では中高生を対象とした情報セキュリティ教育として，座学と実機による演習を組み合わせた教育手法を提案し，公開講座と米子東高校の土曜日活用授業として実践した．授業後のアンケートにより，演習を取り入れることで，生徒の興味関心が高まること，生徒の理解促進，情報セキュリティ対策の生活への実践のきっかけづくりといった教育効果があることが分かった．

また，3章で述べた教科書分析により，同じ科目でありながら，教科書会社や各教科書によって，取り扱われる内容には大きな差が生じており，利用する教科書によって学校間や生徒間で知識や技能に偏りが生じる可能性があることが分かった．全ての高校生が情報セキュリティに関する知識および技術を適切かつ効果的に活用する力を身に付けるため，情報科担当教員は自校が採択している教科書以外で取り扱われる内容も考慮した教科指導が求められていくと考えられる．

なお，本研究の成果は，2022年度工学教育研究講演会 [61] にて対外的に発表しており，情報処理学会コンピュータと教育研究会168回研究発表会 [62]，情報処理学会 第85回全国大会 [63]，日本産業技術教育学会情報分科会第38回研究発表会においても発表予定である．また，山陰中央新報社から取材を受け，1月5日付で掲載された [64]．この記事を図7.1に示す．

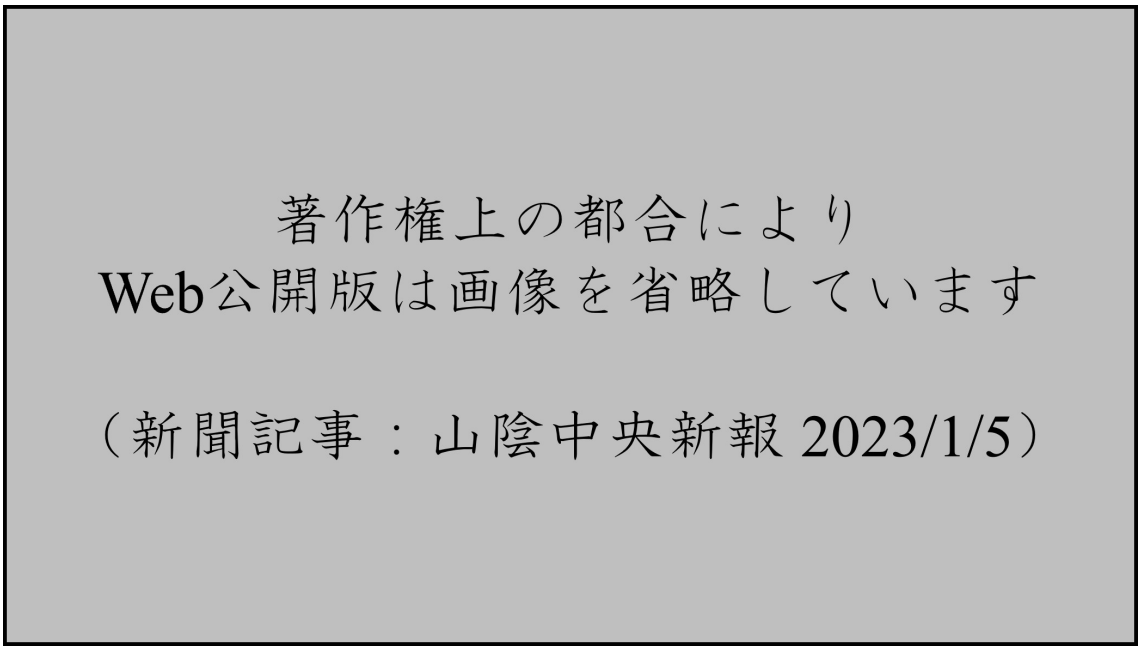


図 7.1 山陰中央新報の掲載紙面

7.2 今後の展望

今後の展望として，以下の点が挙げられる．

1. 既習の内容を考慮した授業の設計
2. 習熟度別での授業実施の検討
3. 共通教科「情報Ⅱ」および専門教科「情報」の教科書分析
4. 米子東高校以外の高校，中学校の教員との連携

まず，授業の内容については，アンケートにおいて『既に学習した内容だった』との指摘があった．今後の授業実施の際には，情報科の授業と連携し，授業で学習する内容を考慮した授業を行う必要がある．アンケートにおいては,『進度が遅い生徒に合わせると，速い人は手の空く時間が多い』との指摘も受けた．キーボード操作や情報セキュリティに関する事前知識などをもとに習熟度別での授業実施を検討し，授業中に手の空く生徒が可能な限り少なくなるように工夫する．

また，3章で述べた教科書分析に関しては，共通教科「情報Ⅱ」および専門教科「情報」の教科書についても分析することや，教科書の採択学校数についても調査することで，生徒に求められている知識および技能の都道府県別または全国的な傾向を把握する予定である．

最後に，今回の授業は本校の公開講座と，米子東高校の土曜日活用授業と限られた範囲での実施であった．今後はより広い範囲での実施を検討し，そのために，米子東高校以外の高校や中学校の教員と連携を進めていきたい．そして，本研究で得られた知見をもとに，情報セキュリティ教育に限らず，幅広い意味での情報教育の発展にも寄与していきたい．

謝辞

研究の実施や，本論文の執筆にあたりご指導いただきました川戸聡也 講師，米子東高校での授業実施に多大なご協力いただいた鳥取県立米子東高等学校 佐々木章人 教諭，佐々木先生をご紹介いただいた内田雅人 助教に心からお礼申し上げます．また，サイバー防犯ボランティアとして活動するにあたりご協力いただきました鳥取県警察本部生活安全部サイバー犯罪対策課 西根嘉宣 様，杉谷淳行 様，薄田康拡 様に感謝いたします．研究を進める中で，授業の準備や授業当日にサポートしてくれた研究室のメンバーや，電子制御工学科3年 佐野颯音くんに対しても，この場を借りて感謝申し上げます．

筆者が本研究を始めたきっかけは，3年生からはじめたセキュリティ啓発活動でした．このきっかけをくださり，今年度は演習環境として利用した機材を提供していただきました徳光政弘 准教授に感謝申し上げます．

学内でのアンケート実施にご協力いただいた大庭経示 教授，川邊博 教授，竹内彰継 教授，中島美智子 教授，渡邊健 教授，井上学 准教授，小林玉青 准教授，堀畑佳宏 准教授，本村信一 准教授，原田桃子 講師，藤本晃嗣 講師，電子制御工学科3年 片尾祐行くん，物質工学科3年 砂山遥香さんに対しても感謝いたします．

また，本研究の取り組みを取材していただきました，山陰中央新報社米子総局報道部 柴田広大 様に対しても感謝いたします．

さて，ここからは5年間の高専生活を振り返りたいと思います．

当初は，第一希望の電気情報工学科から流れる形で電子制御工学科に入学しましたが，5年間の高専生活で様々なことを経験でき，電子制御工学科で良かったと思っています．

1年生から4年生までは「何か高専らしいことをしたい」との思いでロボコンに参加し，4年生ではBチームのリーダー兼ロボコン同好会の副会長という大役を担いました．今ではロボットと無縁のテーマで研究に取り組んでいますが，

4年間のロボコン活動で得た経験は一生の宝物だと感じています．特に，学年や学科が異なる学生が一緒になって共通の目標に向かって進んでいくというのは高専ロボコンならではの貴重な経験だと感じています．

2年生のときには，徳光先生からのお誘いでK-SECの合宿講座に参加し，情報セキュリティに興味を持ち始めました．3年生では，同じく徳光先生からのお誘いで情報セキュリティ啓発活動を始めるなど，ロボコン以外でも様々な経験ができました．これらの活動は，卒業研究のテーマを「情報セキュリティ教育」にするきっかけでもあります．こうして考えてみると，今の自分があるのは徳光先生のおかけではないかと思います．

振り返ると良いことばかりの5年間に見えますが，進路活動では苦労しました．4年生の11月までは大学編入をするつもりでした．編入を考え始めた当初は，情報セキュリティ関係の研究室があるY大学やO大学を考えていましたが，試験科目に絶望し，K大学やH大学に変更．しかし，4年生の10月に受験したTOEIC-IPのスコアで絶望し，大学編入を諦めて専攻科へ志願変更しました．笑い話のような専攻科志願理由ですが，当時はかなり凹みました．今では,『専攻科修了まで今の研究は続けられるし』と開き直っています．

今年は，研究活動に没頭する1年間でしたが，反省も多いです．自分で言うのも何ですが，研究の進捗が早すぎるために，毎月何かしらの研究内容を追加したので，無計画な1年でした．実は米子東高校での授業，学内でのアンケート，教科書の分析などの大半は，年度当初の予定には無かったものでした．後輩の皆さんは，計画性をもって研究を進めましょうね．これからは，5年間で学んだことを意識して，何事にも全力で取り組んでいけたらと思います．川戸先生には，専攻科修了までご迷惑をおかけするかもしれませんが，これからもよろしくお願いいたします．

最後に，本研究に携わられた全ての皆様に今一度感謝申し上げ，謝辞とさせていただきます．ありがとうございました．

参考文献

[1] 総 務省：令和 4 年度版 情報通信白書. 入手先 <https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r04/pdf/01honpen.pdf>（参照 2023-01-27）.

[2] 株式会社エヌ・ティ・ティピー・シーコミュニケーションズ：【事例あり】IoT とは？仕組み・機能を分かりやすく解説. 入手先 <https://www.nttpc.co.jp/column/iot_mobile/iot.html>（参照 2023-01-27）.

[3] 警 察庁:サイバー空間をめぐる脅威の情勢等. 入手先 <https://www.npa.go.jp/publications/statistics/cybersecurity/index.html>（参照 2023-01-27）.

[4] JPCERT コーディネーションセンター：インシデント報告対応レポート. 入手先 <https://www.jpcert.or.jp/ir/report.html>（参照 2023-01-27）.

[5] フィッシング対策協議会:月次報告書. 入手先 <https://www.antiphishing.jp/report/monthly/>（参照 2023-01-27）.

[6] 経済産業省：IT 人材の最新動向と将来推計に関する調査結果. 入手先 <https://www.meti.go.jp/shingikai/economy/daiyoji_sangyo_skill/pdf/001_s02_00.pdf>（参照 2023-01-27）.

[7] 内閣サイバーセキュリティセンター：サイバーセキュリティ戦略. 入手先 <https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2018.pdf>（参照 2023-01-27）.

[8] 国立高等専門学校機構:サイバーセキュリティ人材育成事業. 入手先 <https://csinfo2018.kochi-ct.ac.jp/index.html>（参照 2023-01-27）.

[9] 内閣サイバーセキュリティセンター：高専における人材の育成. 入手先 <https://security-portal.nisc.go.jp/curriculum/torikumi/k-sec_ikusei.html>（参照 2023-01-27）.

[10] 守山 凜ほか：高専生が運営する学内向けセキュリティ講習会の試行，工学教育，Vol. 70, No. 4, pp. 171–176 (2022).

[11] 守山 凜ほか：学生主体のサイバーセキュリティ啓発活動の実施と今後の展望，第 84 回全国大会講演論文集，Vol. 2022, No. 1, pp. 661–662 (2022).

[12] 株式会社ラック：情報リテラシー啓発のための羅針盤. 入手先 <https://www.lac.co.jp/corporate/pdf/compass.pdf>（参照 2023-01-27）.

[13] 消費者庁：若者・高校生に多いトラブル事例と解説. 入手先 <https://www.caa.go.jp/policies/policy/consumer_education/public_awareness/teaching_material/material_007/pdf/03_moshitora-k.pdf>（参照 2023-01-27）.

[14] 塩田真吾ほか：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，コンピュータ＆エデュケーション，Vol. 44, pp. 85–90 (2018).

[15] 多田義男ほか：技術・家庭科（技術分野）における情報セキュリティ授業の実践，情報処理学会研究報告，Vol. 2022-CE-164, No. 29, pp. 1–6 (2022).

[16] 多田義男：技術・家庭科（技術分野）における情報セキュリティ授業の実践―パスワードの大切さを理解しよう―，情報処理， Vol. 63, No. 11, pp. 621–625 (2022).

[17] 今川俊明ほか：高校における情報セキュリティ教育の提案，情報処理学会第 68 回全国大会講演論文集，Vol. 2006, No. 1 (2006).

[18] 増山一光：シナリオによる標的型メール対策教材を用いた情報セキュリティ教育の実践，教育情報研究，Vol. 33, No. 1, pp. 25–32 (2017).

[19] 西郡裕子ほか：県立高校における「サイバーセキュリティ技術実践授業」の実施について，情報処理学会第 79 回全国大会講演論文集，Vol. 2017, No. 1, pp. 727–728 (2017).

[20] 栗原義武ほか：サイバーセキュリティ人材育成事業における初学者向け教材の実践報告と新教材への試み，新居浜工業高等専門学校紀要，Vol. 56, pp. 11–17 (2020).

[21] 土居茂雄：苫小牧高専と北海道警察が連携したサイバーセキュリティ教育，工学教育，Vol. 69, No. 1, pp. 92–97 (2021).

[22] 柴崎年彦ほか：都立産技高専の情報セキュリティ技術者育成プログラム，工学教育研究講演会講演論文集，Vol. 2019, pp. 134–135 (2019).

[23] 柴崎年彦ほか：都立産技高専の情報セキュリティ技術者育成プログラムⅡ，工学教育研究講演会講演論文集，Vol. 2020, pp. 122–123 (2020).

[24] 東京都立産業技術高等専門学校：情報セキュリティ技術者育成プログラム．入手先 <https://www.metro-cit.ac.jp/major/infosecurity.html>（参照 2023-01-27）．

[25] 干川尚人ほか：サービス拒否攻撃演習システムの実装とそのアクティブラーニングシナリオによるセキュリティ技術教育，電子情報通信学会論文誌 B, Vol. 103, No. 4, pp. 180–183 (2020).

[26] 山之上卓ほか：情報倫理ビデオの製作と大学の情報セキュリティへの応用，情報処理学会研究報告，Vol. 2008-IOT-001, No. 13, pp. 71–76 (2008).

[27] 西村浩二ほか：広島大学における情報セキュリティ・コンプライアンス教育の取組み，情報処理学会研究報告，Vol. 2012-IOT-018, No. 2, pp. 1–6 (2012).

[28] 佐々木良一ほか：産学協同によるセキュリティ教育の実践と課題，情報処理学会研究報告，Vol. 2006-DPS-126, No. 26, pp. 117–122 (2006).

[29] 大久保誠也ほか：指紋認証実験を取り入れた情報セキュリティ教育の試行，情報処理学会研究報告，Vol. 2010-CE-103, No. 13, pp. 1–7 (2010).

[30] Ladabouche, T. et al.: GenCyber: Inspiring the Next Generation of Cyber Stars, IEEE Security & Privacy, Vol. 14, No. 5, pp. 84–86 (2016).

[31] Jin, G. et al.: Game Based Cybersecurity Training for High School Students, Proceedings of the 49th ACM Technical Symposium on Computer Science Education, pp. 68–73 (2018).

[32] Chase, J. et al.: High School Cybersecurity? Challenge Accepted–Radford University's RUSecure CTF Contest for High School Students, Journal of The Colloquium for Information Systems Security Education, Vol. 9, No. 1, pp. 1–6 (2022).

[33] Conklin, A.: Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course, Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06), Vol. 9, pp. 1–6 (2006).

[34] Jaffray, A. et al.: SherLOCKED: A Detective-Themed Serious Game for Cyber Security Education, Human Aspects of Information Security and Assurance, pp. 35–45.

[35] 遠藤　学:ボクらは「桃鉄」で日本地理を、「信長の野望」や「三国志」で歴史を学んだ. 入手先 <https://nlab.itmedia.co.jp/games/articles/0505/31/news003.html>（参照 2023-01-27）.

[36] Hu, J. et al.: Tele-Lab IT Security: An Architecture for Interactive Lessons for Security Education, SIGCSE Bull., Vol. 36, No. 1, pp. 412–416 (2004).

[37] 米子工業高等専門学校：令和 4 年度　Web シラバス. 入手先 <https://syllabus.kosen-k.go.jp/Pages/PublicSubjects?school_id=30&department_id=33&year=2022&lang=ja>（参照 2023-01-27）.

[38] 文部科学省：【情報編】高等学校学習指導要領（平成 30 年告示）解説. 入手先 <https://www.mext.go.jp/content/1407073_11_1_2.pdf>（参照 2023-01-27）.

[39] 国立高等専門学校機構：モデルコアカリキュラム．入手先 <https://www.kosen-k.go.jp/about/profile/main_super_kosen.html>（参照 2023-01-27）．

[40] 鹿野利春ほか：情報科教育法 ―これからの情報科教育―，実教出版 (2022).

[41] 大学入試センター：令和 7 年度以降の試験に向けた検討について． 入手先 <https://www.dnc.ac.jp/kyotsu/shiken_jouhou/r7ikou/r7ikou.html>（参照 2023-01-27）．

[42] 御家雄一ほか：情報 I の教科書におけるピクトグラムの扱いについての比較，情報処理学会研究報告，Vol. 2021-CLE-35, No. 22, pp. 1–7 (2021).

[43] 井手広康：大学入学共通テスト「情報」サンプル問題を踏まえた情報 I の教科書におけるプログラミング分野の比較，情報教育シンポジウム論文集，Vol. 2021, pp. 246–253 (2021).

[44] 赤澤紀子ほか：情報科教科書に現れる用語の変遷―情報 ABC から情報 I・Ⅱまで―，情報処理学会研究報告，Vol. 2022-CE-166, No. 5, pp. 1–9 (2022).

[45] 赤澤紀子ほか：高等学校共通教科情報科の知識体系に関する一考察，情報処理学会論文誌教育とコンピュータ（TCE），Vol. 8, No. 3, pp. 19–34 (2022).

[46] 成瀬浩健ほか：高等学校「情報 I」教科書および傍用問題集でのデータサイエンスの扱いについて，情報処理学会研究報告，Vol. 2022-CE-163, No. 11, pp. 1–4 (2022).

[47] 情報処理推進機構：情報セキュリティ読本 五訂版―IT 時代の危機管理入門―，実教出版 (2020).

[48] 情報処理推進機構：情報処理技術者試験 試験要綱 Ver.5.0. 入手先 <https://www.jitec.ipa.go.jp/1_13download/youkou_ver5_0.pdf>（参照 2023-01-27）．

[49] 日本学術会議情報学委員会情報学教育分科会：報告「情報教育課程の設計指針―初等教育から高等教育まで」. 入手先 <https://www.scj.go.jp/ja/info/kohyo/pdf/kohyo-24-h200925.pdf>（参照 2023-01-27）．

[50] 情報処理推進機構：情報セキュリティ白書 2022. 入手先 <https://www.ipa.go.jp/files/000100472.pdf>（参照 2023-01-27）.

[51] 瀬戸美月ほか：徹底攻略 情報処理安全確保支援士教科書 令和 4 年度，インプレス (2021).

[52] Raspberry Pi 財団：Raspberry Pi 4. 入手先 <https://www.raspberrypi.com/products/raspberry-pi-4-model-b/>（参照 2023-01-27）.

[53] Security, O.: Kali Linux. 入手先 <https://www.kali.org/get-kali/>（参照 2023-01-27）.

[54] Rapid7: Metasploitable 2 Exploitability Guide. 入手先 <https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/>（参照 2023-01-27）.

[55] VMware, I.: VMware Workstation Player. 入手先 <https://www.vmware.com/jp/products/workstation-player.html>（参照 2023-01-27）.

[56] IPUSIRON: ハッキング・ラボのつくりかた 仮想環境におけるハッカー体験学習，翔泳社 (2018).

[57] 小熊信孝：Stuxnet －制御システムを狙った初のマルウエアー. 入手先 <https://www.jpcert.or.jp/ics/2011/20110210-oguma.pdf>（参照 2023-01-27）.

[58] 齋藤孝道：マスタリング TCP/IP 情報セキュリティ編，オーム社 (2019).

[59] 鳥取県警察本部:鳥取県警察サイバー防犯ボランティア運用要綱の制定について（例規通達）. 入手先 <https://www.pref.tottori.lg.jp/274341.htm>（参照 2023-01-27）.

[60] 鳥取県教育委員会:GIGA スクールフェア 2022 in TOTTORI. 入手先 <https://www.pref.tottori.lg.jp/298270.htm>（参照 2023-01-27）.

[61] 守山　凜ほか：小中高生を対象とした高専生による情報セキュリティ教育の検討，工学教育研究講演会講演論文集，Vol. 2022 (2022).

[62] 守山　凜ほか：高等学校情報科「情報I」の検定済教科書における情報セキュリティの取扱いに関する分析，情報処理学会研究報告，Vol. 2023-CE-168, No. 3 (2023).

[63] 守山　凜ほか：ハッキング演習を交えた中高生向け情報セキュリティ講座の実施，情報処理学会第 85 回全国大会講演論文集 (未公刊).

[64] 山陰中央新報社：米子高専生・守山さんが講座　中高生 ネットトラブルから守れ. 山陰中央新報 1 月 5 日付.

業績リスト

誌上発表

和文誌 査読有り

1. 守山　凜，川戸聡也，徳光政弘：高専生が運営する学内向けセキュリティ講習会の試行，工学教育，Vol.70，No.4，pp.171–176 (2022).

口頭発表・ポスター発表

国内学会 査読有り

1. 守山　凜，川戸聡也，徳光政弘：学生によるサイバーセキュリティ教育の実践，工学教育研究講演会講演論文集，Vol.2021，pp.22–23 (2021).

2. 守山　凜，岩尾朋哉，若林遥大，川戸聡也：小中高生を対象とした高専生による情報セキュリティ教育の検討，工学教育研究講演会講演論文集，Vol.2022，pp.266–267 (2022).

3. 若林遥大，岩尾朋哉，守山　凜，川戸聡也：統合開発環境にチャット機能を統合したプログラミング教育支援システムの開発，工学教育研究講演会講演論文集，Vol.2022，pp.268–269 (2022).

国内学会 査読無し

1. 守山　凜，川戸聡也，徳光政弘：座学と演習を含む学生主体の情報セキュリティ講習会の実施，第 26 回高専シンポジウム (2021).

2. 守山　凜，川戸聡也，徳光政弘：座学と演習を含む学生主体の情報セキュリティ講習会の試行とアンケート結果の分析，電気学会中国支部第 13 回高専研究発表会講演予稿集，pp.11–12 (2021).

3. 守山　凜，川戸聡也，徳光政弘：学生主体のサイバーセキュリティ啓発活動の実施と今後の展望，情報処理学会第 84 回全国大会講演論文集，Vol.2022，No.1，pp.661–662 (2022).

4. 守山　凜，川戸聡也：高等学校情報科「情報 I」の検定済教科書における情報セキュリティの取扱いに関する分析，Vol.2023-CE-168，No.3，pp.1–6 (2023).

5. 守山　凜，川戸聡也：ハッキング演習を交えた中高生向け情報セキュリティ講座の実施，情報処理学会第 85 回全国大会講演論文集 (未公刊).

受賞

1. 学生奨励賞，情報処理学会コンピュータと教育研究会 168 回研究発表会 (2023).

以上