連載

情報の授業をしよう！

本コーナー「情報の授業をしよう！」は，小学校や中学校で情報活用能力を育む内容を授業で教えている先生や，高校で情報科を教えている先生が，「自分はこの内容はこういう風に教えている」というノウハウを紹介するものです．情報のさまざまな内容について，他人にどうやって分かってもらうか，という工夫やアイディアは，読者の皆様にもきっと役立つことと思います．そして「自分も教え方の工夫を紹介したい」と思われた場合は，こちらにご連絡ください．
（E-mail：editj@ipsj.or.jp）

主体的・対話的な学びを重視した情報セキュリティ授業の実践

―ハッキング体験から学ぶ情報セキュリティ―

基般

守山　凛　米子工業高等専門学校

高校生に対する情報セキュリティ教育の必要性

内閣府の調査☆1によると，2009年以降高校生のインターネット利用率は95%以上と高水準となっている．一方で，高校生が関与するサイバー犯罪が多く発生していることから情報セキュリティ教育の重要性が高まっている．

このような状況を踏まえ，2018年に改訂された高等学校学習指導要領☆2では共通教科情報科で扱われる内容が従来よりも強化された．また，専門教科情報科では情報セキュリティが独立した科目として新設されるなど，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．加えて，主体的・対話的で深い学びの視点からの授業改善も求められており，プログラミングや情報デザインなどさまざまな単元で授業改善に取り組まれている[1), 2)]．

筆者は鳥取県立高校において，情報セキュリティの単元で主体的・対話的な学びを意識した授業を実践している．授業は2022年度から米子東高校（普通科）において実施しており，2023年度からは鳥取湖陵高校（情報科）を，さらに2024年度には米子南高校（商業科）を加えた3校において各校年1回の出前授業として実施した．本稿では3年間実施してきた米子東高校での授業を中心に，3校での実践について紹介する．

☆1　内閣府：青少年のインターネット利用環境実態調査（2009～2024）．
☆2　文部科学省：高等学校学習指導要領（平成30年告示）

米子東高校における実践

授業の対象学年と内容

米子東高校は普通科を置く高校であり，1年生で情報Iを履修している．授業は同校の土曜日を活用した課外授業として企画し，1年生および2年生の希望者を対象に受講者を募ったところ3年間で延べ44名（参加当時で1年生40名，2年生4名）が参加した．授業の構成を表-1に示す．授業は1日のみの企画とし4部構成の計3時間で設定した．内容としてはSNSにおける情報セキュリティ対策などを中心に生徒に

とって身近な話題を多く扱うことで，情報セキュリティに対する興味関心を高めると同時に自身の生活を見直すきっかけとさせるなど主体的な学びを促している．また，グループでのディスカッションを取り入れることで互いの意見を比較し自身の考えを深めさせるなど，対話的な学びも促している．

第1部は座学であり，情報セキュリティの3要素[☆3]，身近に存在するサイバー攻撃手法としてマルウェアや不正アクセス，ソーシャルエンジニアリングについて講義した．

第2部および第3部では実機を用いた演習を実施した．第2部ではハッキングの体験としてOSINT[☆4]による情報推定，パスワードの強度検証を実施した．OSINTでは，SNSの投稿から投稿者の個人情報を推定する演習，風景画像から撮影場所を特定する演習の2つを実施し，容易に個人情報や位置情報を推定できることを確認した（図-1）．パスワードの強度検証では，含まれる文字の種類や桁数が異なる3つのパスワードを総当たり解析し，安易なパスワードは数秒で解析されてしまうことを確認した（図-2）．また，第2部の最後にはここまでの授業の成果をもとに，不正アクセスやソーシャルエンジニアリングなどのサイバー攻撃に対してどのような対策が有効であるかを考えるグループディスカッションを実施した．ディスカッションの後には一般的な対策の例を解説した．

第3部では情報セキュリティを確保するための技術としてファイアウォールと暗号化の演習を実施した．ファイアウォールの演習では攻撃用に用意したサーバのTCP/80番ポート（HTTP）の通信を禁止する設定をし，ポートスキャンや実際にWebサイトにアクセスするなどして設定前後の挙動を比較することで，アクセス制御の基本的な仕組みや役割を確認した（図-3）．暗号化の演習では図-4のように送信者・受信者・傍受者の3つの役割に分け，全員がすべての

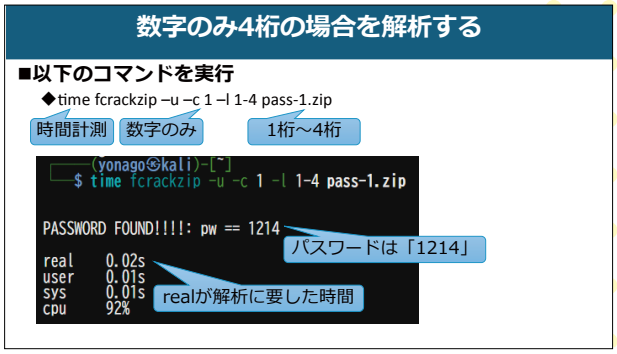
☆3 機密性（Confidentiality），完全性（Integrity），可用性（Availability）の3つを指す．

☆4 「Open Source Intelligence」の略であり，一般に公開されている情報を収集・分析して活用する手法を指す．

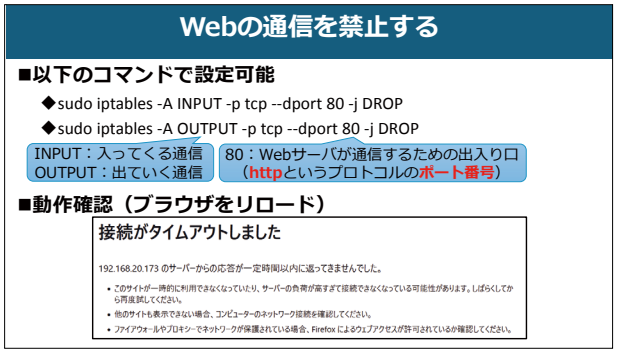
■表-1 授業の流れ

部	授業内容
第1部	・情報セキュリティの3要素 ・身近に存在する攻撃手法について
第2部	・OSINTによる情報推定 ・パスワードの強度検証
第3部	・ファイアウォールの設定 ・シーザー暗号の生成と復号
第4部	・情報セキュリティポリシー

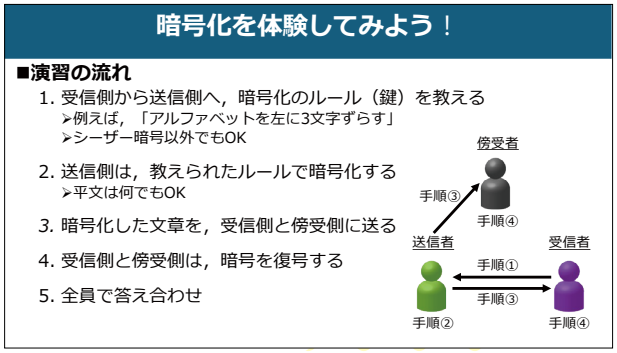
■図-1 位置情報を特定する演習



■図-2 パスワードの強度を検証する演習



■図-3 ファイアウォールの演習



■図-4 暗号化の演習

役割ができるようにローテーションしながら実施した．

第4部では情報セキュリティポリシーの役割や必要性について講義した後，関連する3つの課題についてグループディスカッションを実施した．課題1では，日常生活の中で想定される危険性や被害を考え，その被害から身を守るために必要なルールを各自で考えてもらった．課題2では，グループのメンバーで話し合い各自が考えたルールを①本当に必要か，②安全が十分に確保できるか，③利用者の利便性に配慮できているかの3つの観点から評価してもらった．課題3では，話し合いの成果をもとにグループで1つの情報セキュリティポリシーとしてまとめてもらった．

ハッキングの環境

第2部および第3部で実施した演習では，Kali Linux[☆5]とWindows 11のそれぞれがインストールされたノートパソコン計2台で構成される専用の環境を構築した．Kali Linuxには多くのペネトレーションテストツールが標準で搭載されており，今回の授業では攻撃用クライアントとして利用した．Windows 11には，攻撃対象としてペネトレーションの練習用にあえて脆弱性をもたせた仮想コンピュータであるMetasploitable2[☆6]を，VirtualBoxを用いて構築した．生徒は1人1台端末として各自が所有するChromebookからSecure Shell（SSH）にてKali Linuxに接続し，Kali Linux上でコマンドを実行することで演習に取り組んだ．なお，演習環境は外部との通信ができない専用のネットワーク内で構築することで，演習に関する通信が外部に漏洩しないようにしている（図-5）．

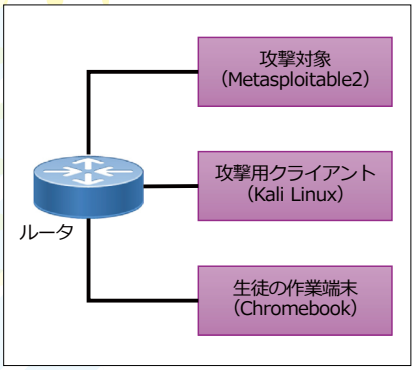
ワークシートとグループディスカッション

第4部で実施した2つのグループディスカッションではワークシートを配布し，自身の考えや他者の意見を整理できるようにした．ワークシートはGoogleドキュメントの形式とし，タブの機能を用いることで各自の作業領域を用意した．また，他者のタブを閲覧できるようにすることで自身の考えを深められるようにした．

ディスカッションの様子を図-6に，情報セキュリティポリシーに関するディスカッションで用いたワークシートの生徒記入例を図-7に示す．この生徒は，課題1においてユーザの行動などを制限させるルールを多く考えている．しかし，課題2で他者と意見を交換することで利用者の利便性への配慮が十分でないと評価している．これはほかの生徒も同様の傾向であった．これを踏まえて課題3においては，ウイルス対策ソフトウェアを導入する，USBメモリの持ち帰りは許容するがパスワードを設定する，パ

■図-6　ディスカッションの様子

☆5 https://www.kali.org/get-kali/
☆6 https://sourceforge.net/projects/metasploitable/



■図-5　ハッキングの環境

米子東高校土曜日活用事業『サイバー攻撃体験から学ぶ情報セキュリティワークショップ』ワークシート

[2-1]【個人作業】私たちが生活する中で必要な情報セキュリティポリシーを考えてみましょう．

No.	想定される危険性や被害	必要なルール	観点1	観点2	観点3
1	ランサムウェアを踏む	変なメールやサイトに関わらない	○	○	△
2	酔っ払ってusbを紛失する	管理を厳格にする　持ち帰らない	○	○	X
3	パスワードが流出する	難しいものに　人に言わない	○	○	△
4	住所を特定される	snsに写真を迂闊にあげない喋らない	○	○	X
5					

[2-2] 他者の意見も参考に，以下の3つの観点からルールを評価しましょう（表に○，△，×を記入）．
観点1：本当に必要なルールであるか
観点2：安全が十分に確保されているか
観点3：利用者の利便が考慮されているか

■図-7　ワークシートの生徒記入例（一部抜粋）

スワードには数字・小文字・大文字・記号をすべてつかって桁数を多くするなどのルールに改めていた．

鳥取湖陵高校および米子南高校における実践

授業の構成・内容

鳥取湖陵高校での授業

鳥取湖陵高校は，鳥取県で唯一の専門学科情報科である情報科学科を設置している．専門学科情報科では，現課程から専門科目として「情報セキュリティ」が独立した科目として新設され，共通的分野の科目に位置付けられている．授業は情報科学科の2年生の専門科目「情報セキュリティ」および3年生の専門科目「情報実習」において実施した．いずれの授業も2部構成とし，授業時間割に合わせて2年生は50分間，3年生は120分間の授業を実施した．

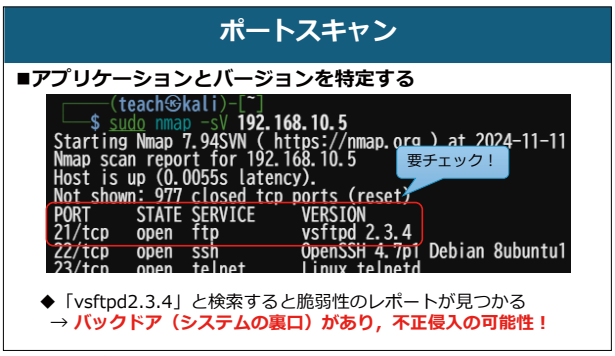
2年生の授業では専門科目「情報セキュリティ」の進度に合わせ，不正アクセスに関する内容とした．第1部は座学であり，情報のセキュリティの3要素や不正アクセスの方法について講義した．第2部で演習を取り入れ，ポートスキャン，パスワードの強度検証，ファイアウォールの設定の3つの演習を実施した．ポートスキャンでは攻撃用のサーバに対してポートスキャンをすることで，稼働しているアプリケーションやそのバージョンを解析した．また，バージョンが特定されることによりそのバージョンに存在する脆弱性を突いた攻撃を受ける可能性があることを解説した（図-8）．なお，パスワードの強度検証とファイアウォールの設定については米子東高校で実施した内容と同一である．

3年生の情報実習では，グループで協力しながら仮想のECサイトを制作している．そこで，この実習に関連してWebに関する脅威とその対策を体験的に学習する授業を実施した．第1部は座学であり，Webシステムの構成やWebに関する脅威について講義した．また，それまでの講義内容を踏まえ，Webにどのような脅威が存在するのかをグループでディスカッションする時間を設けた．第2部は演習であり，Webに関する具体的な攻撃手法として，クロスサイトスクリプティング（XSS）とSQLインジェクション（SQLi）を取り上げた．XSSでは掲示板を模したWebページに対して，偽サイトへ誘導する仕組みを実装する演習などを実施した（図-9）．SQLiではログイン画面の脆弱性を突き不正にシステムへログインする演習を実施した．それぞれの演習の後には，攻撃への対策としてエスケープ処理やハッシュ化について講義した．

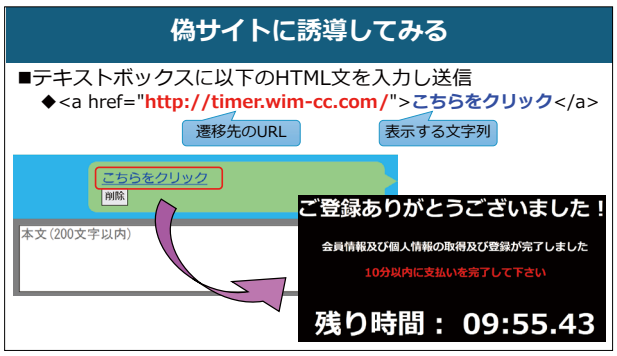
米子南高校での授業

米子南高校では商業学科ビジネス情報科（現・ITビジネス科）の2年生および3年生に対して授業を実施し，両学年で同一の構成・内容とした．

授業は学校設定科目「IT戦略」での実践である．この科目はビジネスにITを応用する方法を扱っており，情報セキュリティに関しても幅広く扱っている．そこで，幅広いサイバー攻撃手法とその対策を学ぶことを目指し，身近な攻撃手法でもある不正アクセスとWebに関するものとしてSQLiを取り上げた．いずれの内容も鳥取湖陵高校で実践した授業と同一の内容である．



■図-8　ポートスキャンの演習



■図-9　XSSの演習

演習用 Web サイト

Web に関する演習では独自開発した専用の Web アプリケーション[☆7] を用いて演習を実施した．実際のアプリケーションに対して攻撃をすることで，攻撃の仕組みや，対策方法とその効果について体験的に学ぶことができる．

SQLi の体験では，ID とパスワードによる簡単なログインシステムを用意した．このシステムには，ユーザの入力がそのまま SQL 文に代入される脆弱性を持たせている．演習では，意図的に悪意のある文を入力することで，通常は認証されない内容であってもログインが成功してしまう現象を体験する．次に，エスケープ処理を施したページに対して同様に攻撃を仕掛けることで，脆弱性が情報漏洩につながることを体験する．

XSS の体験では，HTML タグや JavaScript を埋め込むことができる脆弱性を持つ掲示板を用意した．まず，この脆弱性を利用して背景色の変更や悪意のある Web サイトへの誘導を体験する．次に，エスケープ処理や HTML タグの制限を実装したページに対して同様に攻撃を仕掛けることで，入力可能な文字や記号を制限する必要性を学ぶ．

実践のまとめと今後の展望

本実践では主体的・対話的な学びを目指して，グループディスカッションやハッキングの体験などを交えた情報セキュリティの授業を県立高校 3 校にて実施した．授業後に実施したアンケートより，生徒から次のような感想があった．

- ディスカッションでほかの人の視点を知ることができ，理解が深まった．（米子東高校）
- 実際にどのようにして不正アクセスがされているのかが分かった．（米子東高校）
- 今まで教科書で概念でしか知らなかったがハッキングなどの演習を通して詳細に理解できた．（米子東高校）
- 日ごろの授業では演習が少ないので貴重な経験となった．（鳥取湖陵高校）
- 今後 Web サイトなどを構築するときには，セキュリティ面を考慮して設計するようにしていきたい．（鳥取湖陵高校）
- 情報セキュリティ対策について学んだことを今後の生活で生かして自分の個人情報などを自分の身で守りたいと思った．（米子南高校）

これらの結果から，本授業は情報セキュリティに関する知識の定着だけでなく生徒の主体的・対話的な学びや実践的なスキルの向上，さらにはセキュリティ意識の向上に効果的であったといえる．

なお，本授業は筆者が米子高専学内で実施してきたサイバーセキュリティ啓発活動を発展させたものである[3]．活動を発展させる中で，米子高専教員の紹介で高校との連携を開始した．本取り組みでは，機材や環境の構築を高専が担い，日頃の授業に関する情報を提供するなどして相互に連携している．2024 年度からは高等学校 DX 加速化推進事業（DX ハイスクール）が開始され，高校と高等教育機関の連携が強く求められている．特に高専は高校と同年代の教育を担うため，教育課程などで共通する点も多く，高校と高専の連携が一層重要なものであると考える．

筆者は進学に伴って高専から大学に所属が変わるが，本実践で得られた知見をもとに大学院での研究を通して高校や高専と連携し，情報教育のさらなる発展に向け尽力する所存である．

参考文献

1) 稲垣俊介：「主体的・対話的で深い学び」の実現を目指すプログラミングの授業実践，高校教科「情報」シンポジウム 2022 秋論文集，pp.24-30 (2022).
2) 須藤祥代：情報の授業をしよう！：情報 I で取り組む主体的・対話的で深い学びの授業デザイン―学習サイクルを回して学びの質的改善―，情報処理，Vol.64, No.1, pp.19-25 (2022).
3) 守山　凜 他：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).

(2025 年 1 月 22 日受付)

守山　凜（学生会員）
moriyamaynct@gmail.com

米子工業高等専門学校専攻科在学中．2025 年 4 月に静岡大学大学院総合科学技術研究科情報学専攻へ進学予定．幅広く情報教育に関する研究に従事．デジタル庁デジタル推進委員．

☆7 https://sec.wim-cc.com/