授業実践

ハッキング体験を通した主体的・対話的な情報セキュリティの授業

静岡大学大学院（前 米子工業高等専門学校） 守山 凜

1．はじめに

情報セキュリティ教育の重要性が高まる中，2018年に改訂された高等学校学習指導要領では共通教科情報科や専門教科の代替科目で扱われる情報セキュリティに関す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，高等学校における情報セキュリティ教育が重要視されていることがわかる。加えて，「主体的・対話的で深い学び」の実現に向けアクティブラーニングの視点に立った授業改善が求められている[1]。

しかし，情報セキュリティ分野は専門的な知識や技術が必要であること，学校や教育委員会のセキュリティポリシーによる制約を受けることなどの理由から実習を取り入れることが難しく，単調な授業になりやすい傾向にある。そこで，筆者は情報セキュリティ分野における主体的・対話的で深い学びの実現に向け，ハッキングの体験などを取り入れた授業を鳥取県立高校で実践した。授業は2022年度から米子東高校で実施しており，2023年度からは鳥取湖陵高校，2024年度には米子南高校を加えた計３校において実施した。本授業を通して生徒が情報セキュリティに関する正しい知識を身に付けるだけでなく，セキュリティ技術を適切に活用する力を養い，セキュリティへの意識を高めることを期待している。本報告では，各学校における授業の内容，生徒へのアンケート結果を報告する。

2．授業の内容

2.1　米子東高校

米子東高校は普通科を置く高校であり，１年次で情報Ⅰを履修している。また，同校はスーパーサイエンスハイスクールに指定されており，土曜日を活用した課外授業などを定期的に実施している。そこで，本実践を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におけるセキュリティ対策など身近な内容を多く取り扱い，実機による演習やグループディスカッションを取り入れることで主体的・対話的な学びを促す授業とした。

第１部は座学であり，情報セキュリティの定義，脅威と脆弱性，サイバー攻撃の事例と対策，情報セキュリティポリシーについて講義した。また，情報セキュリティポリシーに関連して，情報セキュリティ対策のためのルールについて考えるグループワークを実施した。このグループワークは，日常生活において必要なルールを考えるものである。各自でルールを考えた後，３～４名のグループでディスカッションをしながら，以下の３つの基準からルールを見直す内容とした。

(1) 本当に必要なルールであるか
(2) 安全が十分に確保されているか
(3) 利用者の利便が考慮されているか

第２部以降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，パスワードの

解析，Open-Source Intelligence（OSINT）による情報推定を実施した。パスワード解析では辞書攻撃と総当たり攻撃の２つについて，攻撃方法を概説した後，桁数や文字の種類が異なる３種類のパスワードを解析した。解析の際には，解析に要した時間を測定し，安全なパスワードについて考察した。OSINTは，一般に公開された情報をもとに多様な情報を組み合わせて分析する活動である。今回の授業では，SNSのプロフィールや投稿から個人情報を推定する演習，風景画像から撮影された市区町村を特定する演習の２つを実施し，容易に情報を推定･特定できることを確認した(図１)。

第３部では情報セキュリティ技術を扱い，ファイアウォールの設定と暗号化の演習を実施した。ファイアウォールの設定では特定のポートの通信可否を設定する演習，通信できる利用者を制限する演習を実施し，アクセス制御の基本的な仕組みと役割について確認した。また，ホワイトリストとブラックリストの２つの制御方式について説明し，それぞれの利点と欠点を各自が考える時間を設けた。暗号化の演習は図３のように，送信者・受信者・傍受者の３人１組のグループを組み，グループ内でそれぞれの役をローテーションして実施した。また，共通鍵暗号方式と公開鍵暗号方式について，それぞれの利点と欠点をグループで話し合う時間を設けた。

撮影場所を特定してストリートビューで再現しよう

図１　OSINTの演習

数字のみ4桁の場合を解析する

■以下のコマンドを実行

◆time fcrackzip -u -c 1 -l 1-4 pass-1.zip

時間計測　数字のみ　1桁～4桁

```
┌──(yonago㉿kali)-[~]
└─$ time fcrackzip -u -c 1 -l 1-4 pass-1.zip

PASSWORD FOUND!!!!: pw == 1214
real    0.02s
user    0.01s
sys     0.01s
cpu     92%
```

パスワードは「1214」

realが解析に要した時間

図２　パスワードの解析演習

暗号化を体験してみよう！

■演習の流れ

1. 受信側から送信側へ，暗号化のルール（鍵）を教える
   ➢例えば，「アルファベットを左に3文字ずらす」
   ➢シーザー暗号以外でもOK
2. 送信側は，教えられたルールで暗号化する
   ➢平文は何でもOK
3. 暗号化した文章を，受信側と傍受側に送る
4. 受信側と傍受側は，暗号を復号する
5. 全員で答え合わせ

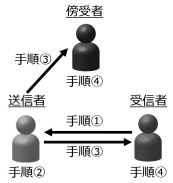

図３　暗号化の演習手順

2.2　鳥取湖陵高校・米子南高校

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４)。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

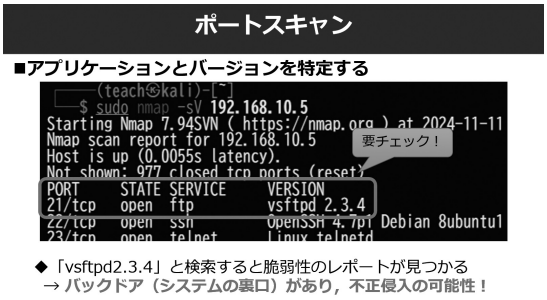

図４　ポートスキャンの演習

仮想のECサイトを制作し，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などの演習を実施した（図５）。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。

３．演習環境

ポートスキャンパスワード，ファイアウォールに関する演習では，実機を用いて演習を実施するため，専用の環境を構築した。攻撃用クライアントには，実際の情報セキュリティに係る検査の現場でも幅広く利用されている「Kali Linux」を用い，被攻撃用のサーバには，仮想マシンである「Metasploitable2」を利用した。生徒は，各自が所有するChromebookからSecure Shell（SSH）にてKali Linuxに接続し，演習を実施した。なお，当日は外部への通信ができない専用のネットワーク内で演習を行うことで，攻撃に関するパケットが外部に流出しないようにした（図６）。

Webに関する演習では，独自開発した専用のWebアプリケーションを用いて実施した[2]。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を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もログインが成功してしまう現象を体験する。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

図５　XSSの演習

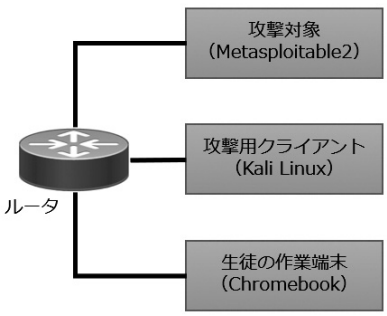

図６　演習環境

を持つ掲示板を用意した。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。また，SQLiやXSSへの対策としてエスケープ処理やHTMLタグの制限を実装したページに対しても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。

4．授業の評価

4.1　理解度

理解度のテストとして授業で取り扱った項目について論述形式で知識を問うテストを授業前後にそれぞれ実施した。

米子東高校の生徒に対して実施した暗号化に関する事前テストでは，「データの形式を変える」，「第三者にわからないようにする」といった漠然とした表現が中心となっており，暗号化の仕組みや用途に関する具体的な知識が不足していた。一方，事後テストでは共通鍵暗号方式や公開鍵暗号方式などの暗号化手法について言及する回答が増加し，それぞれの特徴や利点・欠点について具体的に説明されていた。なお，この傾向は他の授業項目や他校の実践においても同様であった。

4.2　情報セキュリティに対する意識

日常生活で情報セキュリティを意識しているかを授業前に調査した結果を図７に示す。専門学科情報科を置く鳥取湖陵高校では，日常的に情報セキュリティに関連する内容を授業で扱っていることもあり，意識している学生が７割を超えていた。一方で，普通科の米子東高校や商業科の米子南高校では４分の１程度であった。また，意識していると答えた学生に，意識していることや実施している情報セキュリティ対策を尋ねたところ，「SNSで悪口や過激な発言をしない」や「むやみに個人情報を公開しない」などの情報モラルに関するものが多く，情報セキュリティと情報モラルの違いが曖昧となっている生徒が多かった。情報セキュリティに関する記述では，データをバックアップしていると回答した生徒が多かった。

意識が変化したかを尋ねたところ，約75％の生徒が意識するよう変化したと回答した。また，意識するよう変化したと答えた学生に対して，授業以降に実施するようになった情報セキュリティ対策を尋ねたところ，「パスワードを使い回さないようにしている」，「アルファベットや記号を含めた複雑なパスワードを設定するようにしている」，といったパスワードの設定に関する記述が多く見られた。また，鳥取湖陵高校３年生からは「実習で制作しているECサイトでもセキュリティを意識している」といった記述もあった。

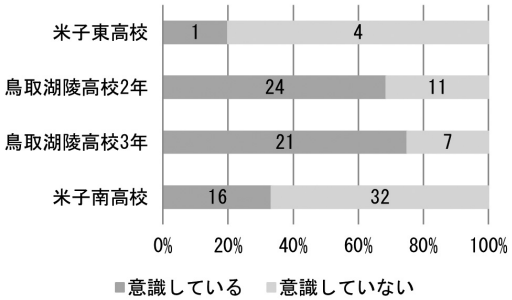

図７　授業前の情報セキュリティに対する意識

5．まとめ

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校において実施した。授業の前後に実施した各種調査の結果により，理解の深化や情報セキュリティ対策の実践力の向上といった学習効果があることがわかった。

また，本実践は高校と高専が相互に連携して取り組んだものであるが，授業後のアンケートより生徒および高校教員の双方から有意義な取り組みであったと評価された。筆者は３月に高専を修了し大学院に進学したが，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を深めることで，双方の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］文部科学省：【情報編】高等学校学習指導要領解説（平成30年告示）
［2］Webセキュリティ演習ツール，https://sec.wim-cc.com/