1ZJ-02

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

守山　凜†　　川戸　聡也†
米子工業高等専門学校†

1. はじめに

今日の我々の生活は，インターネットをはじめとする ICT に大きく依存しており，ICT は重要な社会インフラとなっている．その一方で，個人情報などの情報漏洩や，マルウェアへの感染などに不安を感じる人が 70%を超えるなど，インターネットをはじめとする ICT の安全な利用に対する課題が浮き彫りとなっている[1].

また，我が国における情報セキュリティ人材の不足が指摘されて久しい．日本政府は，人材育成の基本方針として，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挙げている[2].

このような背景を踏まえ筆者らは，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の助成を受け，学生が企画・運営する学内向けの情報セキュリティ教育に取り組んできた[3]. しかし，ICT が浸透している現代では，ICT を利用する全ての者が情報セキュリティについて学ぶ必要がある.

そこで，情報教育が急速に普及する中高生に着目し，中高生を対象とした情報セキュリティ教育を企画および公開講座において実践した．本稿では，実施した公開講座の教育手法と内容，受講者に対して実施したアンケートの分析結果を報告する.

2. 公開講座の概要

本研究の教育実践の機会として，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．公開講座は筆者らが所属する米子高専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，筆者ら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することとした.

Information Security Lectures for Middle and High School Students with Hacking Exercises
†Rin Moriyama, Toshiya Kawato,
National Institute of Technology, Yonago College

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.

講座当日のスタッフとして，本稿の筆頭著者である学生 1 名が講師を務め，教育手法の検討や教材の開発を担当した．また，共著者である指導教員も対応し，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.

3. 教育手法と内容

3.1 概要

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．一方で，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た上で臨むとも考えられた.

そこで，日本政府の人材育成の基本方針や筆者らのこれまでの経験や取り組みを踏まえ，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とすることとした．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.

3.2 講座内容の詳細

検討の結果，表 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．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，パートⅢまでは全受講者が進度を揃えて取り組む．また，パートⅣとして，講座の最後には自由に演習する時間を設けることで，受講者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.

表１　講座内容

パート	内容
Ⅰ 講義	A. 情報セキュリティの定義 B. 不正アクセス C. クロスサイトスクリプティング D. SQL インジェクション E. 情報セキュリティに関する法規
Ⅱ 演習 1	F. ポートスキャン G. 辞書攻撃 H. データベースへの不正侵入
Ⅲ 演習 2	I. クロスサイトスクリプティング
Ⅳ 演習 3	J. 自由にハッキングを体験する

講座はハッキングなどの演習を中心とした構成ではあるが，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．

図１に利用した教材の一例を示す．視覚的に理解しやすい教材を目指し，イラストを用いるなどの工夫を加えた．

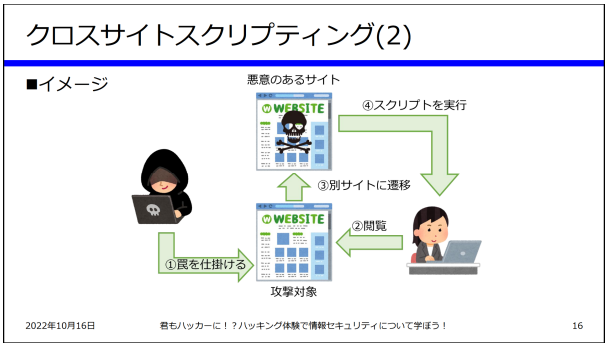

図１　利用した教材の一例

4.　アンケート結果の分析

講座の終了後にアンケートを実施し，10 名の参加者の内，5 名から回答を得ることができた．

図２は，全受講者が一斉に取り組んだ内容に対する評価の結果である．図中のアルファベットは，表 1 の講座内容に対応している．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かった．これは日常生活との関りが薄く，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．

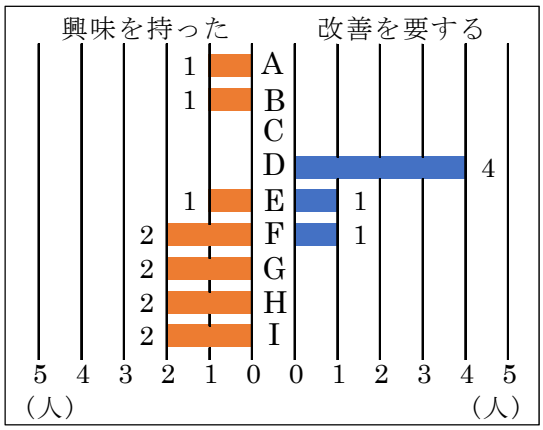

図２　講座内容に対する評価

また，今後も情報セキュリティに関する講座がある場合に参加したいかどうか尋ねたところ，5 名全員が肯定的な意見であった．そのため『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．

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 攻撃がニュース等で話題になることが多いため，生徒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きたい．

5.　おわりに

本研究では，中高生を対象とした情報セキュリティ教育について，教育手法を検討，教材を開発し，公開講座で実践した．講座内容や開発した教材については，概ね高い評価を得られた．

今後は，中学校や高等学校における授業への応用を考えており，既に近隣の公立高校にて１件の講座を実施済みである．中学校の先生や高等学校の情報科担当教員との更なる連携を進めていきたい．併せて，アンケートの結果をもとに，教育手法や教材を改良し，質の向上を図る．

参考文献

[1] 総務省：令和 4 年版情報通信白書，https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r04/pdf/01honpen.pdf，参照日：2023-01-13.

[2] 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，https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2018.pdf，参照日：2023-01-13.

[3] 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，70-4，pp.171-176，2022.