

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

守山 凜[†] 川戸 聡也[†] 徳光 政弘[†]

米子工業高等専門学校[†]

1. はじめに

今日の我々の生活は、高度に複雑化した情報システムやインターネットに大きく依存し、情報セキュリティの重要性に論を俟たない。米子高専では昨今のセキュリティ事情を踏まえ、1～3年次のホームルームにおいて、SNS マナーを含む基礎的なセキュリティ教育を行っている。また2020年度から、全学科3年次の授業において技術的な内容を含むセキュリティ教育を導入した。なお、本校は2021年度より、5学科から1学科5コース制へ改組しており、これらは改組前のカリキュラムでの教育内容である。改組後は、「情報リテラシ」、「情報基礎Ⅰ」、「数理・データサイエンス基礎」、「情報基礎Ⅱ」の4科目を必修科目とし、セキュリティをはじめとする情報教育に力を入れている。

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)^[1]として、セキュリティ人材の育成に力を入れている。本校ではK-SECの助成を受け、学生が企画運営を行うセキュリティ啓発活動を実施しており、2020年度は学内の希望学生を対象に、座学と演習によるセキュリティ講習会を実施した^[2]。

本稿では2021年度に実施するセキュリティ講習会の実施計画と今後の活動の在り方について考察する。

2. 2021年度の実施計画

2.1 活動の概要

本校のセキュリティ教育の現状や2020年度の実施状況を踏まえ、授業で扱う内容以上の発展的な知識と技術を身に付けることを目的として、本校の学生を対象としたセキュリティ講習会を企画した。本講習会は、教育課程外のため希望者のみを対象として募ったところ、2名から申し込みがあり、2022年1月中旬に開催予定である。

2020年度は2日間に分けて講習会を開催したが、2021年度は1日にまとめて実施する。講習は計3時間半行い、前半1時間半は座学、後半2時間は演習を実施する。

講師は学生1名(本稿の筆頭著者で以下、講師学生)が担当し、企画および運営も講師学生が行う。演習の問題作成は有志学生7名が担当する。指導教員(本稿の共著者)は学生が作成した教材や資料の確認、機材の提供、演習環境の構築といった講習会運営の補助を行う。このような取り組みを通じて講師学生や演習問題の作成を行う学生は、積極的・能動的に調査・実験などを行ったうえで教材開発を行う。このため、文部科学省が推進する「アクティブ・ラーニング」の推進普及の一助になるものと考えられる。

2.2 座学の内容

講習の前半は、セキュリティ学習の基盤となる知識を身に付けるため、講義とハンズオン形式の演習を4部に分けて行う。

第1部では2020年度の講習会では扱わなかった、情報セキュリティの考え方や脆弱性について講義する。

第2部以降は2020年度と同一の構成である。第2部では、不正アクセスやSQLインジェクション、DoS攻撃などの攻撃手法について講義し、その対策としてパスワード管理、エスケープ処理、暗号化などの基礎技術について講義を行う。

第3部では、第2部で述べた攻撃が禁止される法的根拠として、不正アクセス禁止法などの諸法律を実際の検挙事例を交えて講義する。

第4部では、SNSの利用に関連し、何気ない風景画像からも位置情報が特定できることを体験するため、Open Source Intelligence(OSINT)の演習を行う。この中では、日本国内の風景画像を題材として、撮影された場所を特定する。

2.3 演習の内容

講習の後半は、個々のセキュリティ技術の向上を目的として、意図的に脆弱性を持たせたサーバやWebサイトへの攻撃、盗聴データの解析な

Implementation and Future Prospects of Student-Centered Cyber Security Awareness Activities

[†]Rin Moriyama, Toshiya Kawato, Masahiro Tokumitsu, National Institute of Technology, Yonago College

どの実践的な演習を行う。演習を通して技術習得だけでなく脆弱性への理解と対策方法についての理解を深める。

演習問題の作問は有志学生が行うが、作問の際には問題の概要や内容などを示す計画書を事前に提出してもらい、講師学生と指導教員らが内容を確認してフィードバックする。

クロスサイトスクリプティングに関する演習の一部を図1に示す。このような、解答にあたって実際の技術やツールの利用が必要な教材を開発し、演習で使用する。

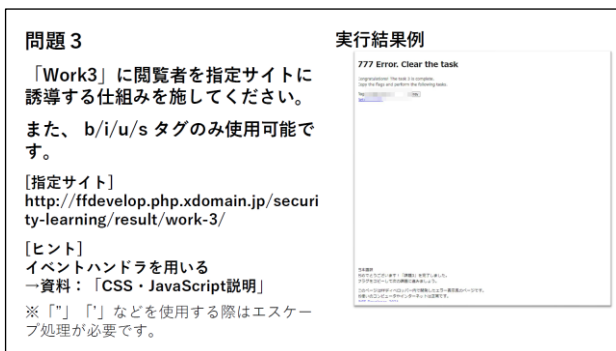


図1. 演習教材の一部

3. 今後の展望

3.1 セキュリティ教育の動向

2018年3月に高等学校情報科の学習指導要領が改訂され、2022年度から共通必修科目として「情報Ⅰ」が新設される。ここでは、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学習すると定められた^[3]。

一方で文部科学省が2015年に行った調査では、情報科担当常勤教員5732人のうち、情報科のみを担当している教員は1170人(20.4%)にすぎず、情報科を担当する教員の不足が顕著である^[4]。

3.2 今後の活動のあり方

前述のセキュリティ教育の動向などを踏まえ、今後は学内のみならず、高校生をも対象とした啓発活動を行っていく必要があると考える。

学習指導要領の改訂にはじまり、2025年度の大学入学共通テストへの教科「情報」の出題など、セキュリティをはじめとする情報教育は非常に重要なものとなっている。そこで15歳から授業や課外活動などで専門教育を受けている高専生が、その経験を活かし高校生に対して啓発活動を行うことで、情報科担当教員が不足して

いる状況でも、学習指導要領の内容に加え、技術的な内容を含む高度で発展的な情報教育を展開できるものとする。この活動は情報科の授業時間を利用し高専生が授業を行うことや、ホームルームでセキュリティに関する講演を行うことを考えている。

このような活動は単発ではなく持続的に行うことが重要である。2020年度および2021年度はともに本稿の筆頭著者が講師を務めたが、今後も活動を継続的に行うためには、特定の学生に依存しない体制を整える必要がある。また、米子高専は、鳥取県サイバーセキュリティ対策ネットワークに参加している。今後の活動にあたっては、このネットワークを活用し鳥取県警察本部や鳥取県教育委員会などの関係機関と連携していきたいと考えている。これにより、講習内容や教材の質の向上などを図る。

4. おわりに

学生主体のセキュリティ講習会を計画し、講義内容の検討、教材の開発を行った。また、今後の活動のあり方を検討した。今後は、講習会を実施およびフィードバックを得ることで内容を改善する。また、高校への展開に向けて具体的な計画を立てる。

謝辞

本研究の一部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うち「持続可能な学生サイバーセキュリティ啓発活動」の助成を受けて実施されたものである。

参考文献

- [1] 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，
<https://csinfo2018.kochi-ct.ac.jp/>，
参照日：2022-1-7。
- [2] 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，2021，2021年度工学教育研究講演会講演論文集，pp. 22-23。
- [3] 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，
https://www.mext.go.jp/content/1407073_11_1_2.pdf，参照日：2022-1-7。
- [4] 文部科学省：高等学校情報科担当教員への高等学校教諭免許状「情報」保有者の配置の促進について，
https://www.mext.go.jp/a_menu/shotou/zyouhou/1368121.htm，参照日：2022-1-7。