7ZC-01

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

佐藤直[1]　西郡裕子[1]　中島尚樹[1]　西山賢志郎[1]　武藤幸一[2]　山田恭弘[3]

概要：情報セキュリティ大学院大学と神奈川県教育委員会教育局が共同にて，県立高校の正規授業科目（社会と情報）として，「スマートフォンのオンラインゲーム情報の盗聴・改ざん」「パソコンの遠隔操作」をテーマに「サイバーセキュリティ技術実践授業」を実施した．スマートフォンやパソコンなど，高校生にとって身近なツールを用いて，情報化社会に欠かせないセキュリティを学ぶことを特徴としており，より実践的で全国的にも例のない教育プログラムである．本論文では，授業の内容および実施状況について報告し，生徒からのアンケート結果を基に，本教育の効果および課題を考察する．

1. はじめに

神奈川県と学校法人岩崎学園[4]は 2016 年 1 月に「連携と協力に関する包括協定」[5]の締結を行い，具体的な連携事業の一つとして，情報セキュリティ大学院大学による「サイバーセキュリティ技術実践授業の実施」を神奈川県立住吉高校にて 2016 年 11 月に実施した．

県立住吉高校は，文部科学省が実施する情報通信技術を活用した教育振興事業「情報教育推進校（IE-School）」調査研究に係わる「情報教育推進校（IE-School）」として神奈川県教育委員会から採択されている．[6]

【実施概要】
- 授業名称：「サイバーセキュリティ技術実践授業」
- 授業内容：「パソコンへのサイバー攻撃」，「スマートフォンのオンラインゲーム情報盗聴・改ざん」
- 対象:神奈川県立住吉高等学校 1 年生(9 クラス 360 名） ※各クラス 2 時限ずつ
- 実施日程：2016 年 11 月 14 日～11 月 18 日
- 共催：神奈川県 教育委員会 教育局
  学校法人岩崎学園　情報セキュリティ大学院大学
- 指導：佐藤直教授，大学院生 3 名

2. 授業の狙い

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，セキュリティ意識の醸成を図ることを狙いとしている．

また，違法な遠隔操作やチート行為を擬似体験することによる悪影響の可能性についても，受講後アンケートから分析を行う．

3. 授業実施環境

3-1. パソコンの乗っ取り遠隔操作

対象校内の PC ルームにある生徒用端末 40 台に仮想 PC を構築した．攻撃者側の生徒が仮想 PC 上でマルウェアを作成し，被害者側の生徒の仮想 PC がそのマルウェアに感染し，攻撃者側の生徒から遠隔操作される体験授業を行った．

【環境概要】
- 生徒端末 OS：Windows 7 Professional 32bit
- 仮想 PC の OS：Windows XP
- マルウェア作成ツール：Posion Ivy v2.3.2 [7]

3-2. スマートフォンのオンラインゲームの盗聴・改ざん

スマートフォンのオンライントランプゲーム High&Low（2 枚のカードのうち，隠れているカードの数字が，見えているカードの数字の上か下かを当てるゲーム）は，授業用に作成した．生徒用端末 20 台を，それぞれに対応する 20 台のスマートフォンのプロキシに設定し，スマートフォンの通信を盗聴すると，隠れているカードの数字を確認でき，必ずゲームに勝てること，掛け金を改ざんすると大勝

[1] 情報セキュリティ大学院大学(INSTITUTE of INFORMATION SECURITY)
[2] 情報科学専門学校(INFORMATION SCIENCE COLLEGE)
[3] 神奈川県立住吉高校(Kanagawa Prefectural Sumiyoshi High School)
[4] 学校法人岩崎学園 HP，http://www.iwasaki.ac.jp/
[5] 神奈川県政策局自治振興部地域政策課平成 28 年 1 月 28 日記者発表資料，http://www.pref.kanagawa.jp/prs/p995543.html(2016-12-21 参照)
[6] 文部科学省 教育の情報化の推進 http://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1374407.htm(2016-12-21 参照)
[7]「remote administration tool (RAT)」バックドア型マルウェア，Trend Micro セキュリティ情報，http://about-threats.trendmicro.com/malware.aspx?language=jp&name=POISONIVY(2016-12-21 参照)

Copyright ©2017 Information Processing Society of Japan.
All Rights Reserved.

ちすることを擬似体験する授業を行った.

【環境概要】
- 生徒端末 OS：Windows 7 Professional 32bit
- スマートフォン OS：Android (version は不明)
- パケット盗聴･改ざんツール：burpsuite v1.6.32 [8]

3-3. アンケートの実施

授業に参加した全生徒にアンケート回答に協力してもらった.

【アンケート項目】
本人又は家族の情報セキュリティ被害経験（6 項目），情報セキュリティ対策の実施状況（6 項目），各授業の理解度（5 段階評価），必要性（3 段階評価，必要性があると回答した生徒には今後受けたい授業内容について自由記述），感想

4. 授業実施内容

正規授業科目「社会と情報」として，1 クラス 2 時限ずつ，「パソコンの乗っ取り遠隔操作」「スマートフォンのオンラインゲームの盗聴・改ざん」を体験学習する．授業は資料に基づき，主に次項に記載する内容を実施した.

4-1. パソコンの乗っ取り遠隔操作

① サイバーセキュリティの概要解説
② マルウェアの解説
③ PC・スマホ・インターネットの危険性の解説
④ 体験内容の解説
⑤ 体験（攻撃者側と被害者側で二人一組）
⑥ 関連する法律・刑罰と事件事例の解説
⑦ 被害に遭わないためのポイント解説

4-2. スマートフォンのオンラインゲームの盗聴・改ざん

① チートについての解説
② パケットの盗聴・改ざんについて解説
③ 体験内容の解説
④ 体験（二人一組）
⑤ 関連する法律・刑罰と事件事例の解説
⑥ 被害に遭わないためのポイント解説
⑦ 受講後アンケート

5. アンケート結果（有効回答件数 307 件）

「授業の必要性について」の結果について図 1 に示す.「必要だと思う」が 58%，「どちらともいえない」が 31%「必要と思わない」と回答した生徒が約 11%であった．「授業の理解度について」の結果について「乗っ取り遠隔操作」は，「大体理解できた」「すべて理解できた」が 90.9%，「オンラインゲームの盗聴・改ざん」は 91.2%であった.

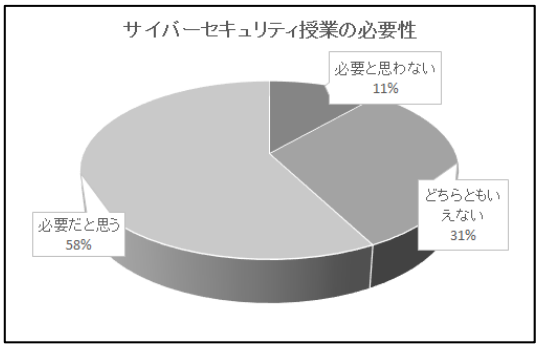

図 1　サイバーセキュリティ授業の必要性

今後受けたい授業（自由記述）については，今回のような体験型が良いという意見が多くみられた．その他，対処方法を教える授業が良いという意見もあった.「必要と思わない」と回答した生徒でも「初めてハッキングやチート行為の恐ろしさを知った」「自分がそういう行為をする側にならない様に気をつけようと強く感じた」という感想も多く見られた.

6. 考察

アンケート結果より，各授業の理解度は 9 割以上が「理解できた」であり，「言葉だけでは分からないが，体験することで危険性がよく分かる」というような感想も多くみられ，体験型授業の教育効果は大きいと思われる.

「体験したような被害に合わないためにどうすればよいか知りたい」という感想が多くみられたことから，今後の取り組みとして，2 時限の授業の一方をサイバー攻撃の実践，もう一方をその対処方法の実践というように 1 セットの授業の実施方法が考えられる． 対処方法の実践としては，アンチウイルスソフトがマルウェアを駆除する動きを確認する内容等が考えられる.

7. おわりに

当初懸念のあった，サイバー犯罪に興味を持ってしまう等の悪影響については，乗っ取りやチートに興味本位な関心を示すような自由記述が 6 名程度確認できた. しかし，そのような生徒にも法と倫理について説明できたこと，これまでサイバーセキュリティに関心を持たなかった生徒のセキュリティに対する意識が大きく高まったことから，悪影響よりも好影響の効果の方がはるかに大きいと感じており，本実践授業は有益であったと考えている.

高校生に対する『攻撃体験−対処法体験−法・モラル学習』を一体とした，「体験型のサイバーセキュリティ技術実践授業」の取組みを今後も試みて行きたい.

[8] HTTP 通信を確認し，改ざんする Proxy 機能が利用できる脆弱性診断に使用されるソフトウェア， PortSwigger Ltd._ https://portswigger.net/(2016-12-21 参照)

Copyright ©2017 Information Processing Society of Japan.
All Rights Reserved.