研究班番号【55】

高校生への情報セキュリティ教育の実践

社会班：山田 夏輝

要旨

この研究は、2022年度より高等学校で行われる「情報」の科目のうち、「情報セキュリティ」の分野を、実際に学校で授業が行われるのより一足早く授業を行い、その課題について考察したものである。結果的に、高校生は「情報セキュリティ」の分野の関心が低いことが判明した。そしてその最大の課題となるのが学生にいかにして興味と危機感を抱かせるかである。

1. はじめに

2022年度より新たに入学する高校生は「情報」が必修になるなど、現在世界では急速に情報化が進んでおり、日々の生活でも情報分野の技術に触れない日はほとんどない。しかし、情報化によって便利になる一方で、毎年のようにサイバー攻撃の数は増えており、個人情報の流出などといった新たな脅威にさらされている。

右図1のグラフは、総務省サイバーセキュリティ―タスクフォース事務局が2020年に公表した資料である。この資料から分かるように、サイバー攻撃の回数は2016年から2019年の3年間で2.6倍に上昇している。また、情報セキュリティ会社のTREND MICRO社は、「2020 年、インバウンド攻撃を示唆するイベントの件数は、2019 年の約 3 倍以上に増加しました。同様にアウトバウンド攻撃を示唆するイベントの件数も、2019 年の 2 倍近くに達していました。さらに、インバウンド攻撃の可能性を検知したデバイスの数と、アウトバウンド攻撃の可能性を検知したデバイスの数も、双方とも増加していました。」(TREND MICRO,2021,46ページ目)と2021年3月に公表した資料で述べている。これらから考えられるのは、学生がサイバー攻撃の被害に遭う可能性が上昇しているということである。

図1

総務省(2020),『サイバー攻撃の最近の動向について』

本研究では、上記のような現状を踏まえた上で、**2022年度から高校生に必修となる「情報」の内容から**抜粋し、一足早く高校生に情報セキュリティ教育を実践し、その結果を考察する。その後、情報セキュリティ教育の課題について考える。

2. 研究手法

まず高校生がどの程度情報セキュリティの意識・知識を持っているかを調査する（調査１）。その後、調査１の結果を踏まえ、動画形式の授業を行い、それによる理解度を問題形式によって調査する（調査２）。調査１の対象は大阪府立高津高校の全校生徒で、調査２は同高校の１学年及び2学年である。

≪調査1≫

- この調査は授業内容を決定するために行う。
- 意識調査は4問で「パスワードをかけているか」などの最低限の対策を行っているか調査する。
- 知識調査は高校生には解けてほしい3問、知識のレベルを知るための高難易度の問題3問である。

≪授業≫

授業内容は以下のとおりであり、調査1と文部科学省の「高等学校情報科『情報Ⅰ』教員用研修教材」を参考にした。

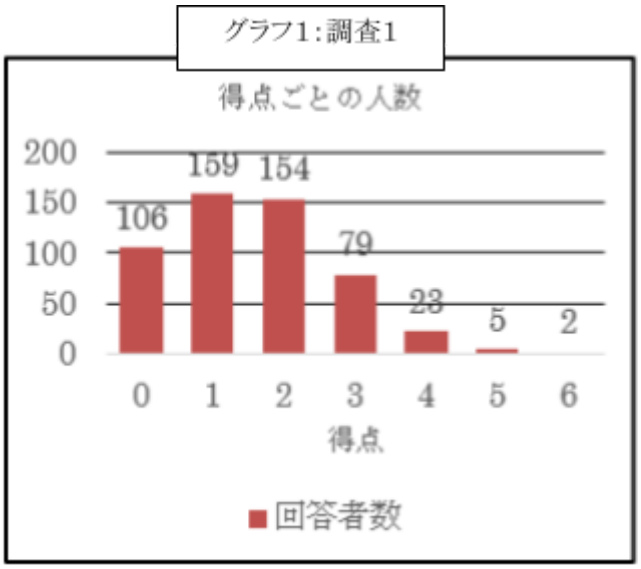
- マルウェア
  - コンピュータウィルス
  - トロイの木馬
- サイバー攻撃の手口
  - 標的型攻撃
  - フィッシング攻撃
- ソーシャルエンジニアリング
  - ショルダハッキング
  - トラッシング

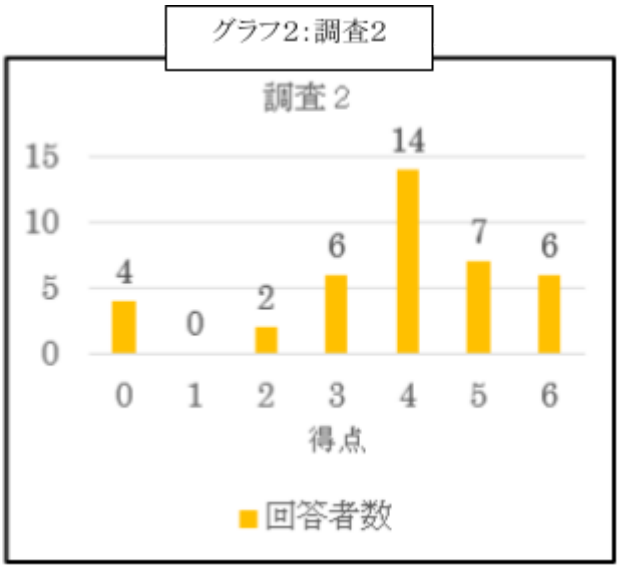
≪調査2≫
- 調査2は、調査1の結果を踏まえた上で行った授業の理解度を考察するために行う。
- 授業で解説した内容から6問出題する。

3. 結果

≪調査1≫　下グラフ1
- この調査では、全体の48.9%にあたる528人から回答を得た。
- 意識調査では4問中3問で「対策を行っている」に該当する回答が全回答者の過半数を超えた。
- 知識調査では平均点が1.58/6点、中央値が1/6点、最頻値が1点の159人であった。
- 知識調査では、0点の者が全体の約20%占めていた。

≪調査2≫下グラフ2
- この調査では、全体の5.14%にあたる37人から回答を得た。
- 平均点は3.70/6点、中央値は4/6点であった。
- 回答者が少なかったため、本調査の点数結果は補足的に用いる





両グラフともに、縦軸は「回答者数」、横軸は「得点」を表す。

4. 考察

調査2より、「高校生は情報セキュリティに対して意識や危機感がほとんどない」ことがわかる。しかし、調査1の結果を踏まえると、「高校生は社会常識のような情報セキュリティの対策(端末にパスワードをかけるなど)を行っている」ということも事実である。また、一方で授業方法にも問題があったとみることができる。動画形式で授業を行ったことが、回答数が少なかった原因の一つに考えられ、この方法は学生の主体性に頼りきってしまっている。これでは、問題意識がない生徒が自ら主体的に動画を見るとは考えにくい。

私は、この問題を解決するためには「アクティブラーニング」や「実習」が効果的なのではないかと考える。ア

クティブラーニングは主体性を重視した学習方法であり、これを行うことによって学生の主体性を養い、情報セキュリティに対する意識を構築できる。増山(2013)は、「今後は、こうした情報セキュリティインシデント（標的型攻撃などのサイバー攻撃のこと）に対するリスクを認識させる教育実践が大切になるのであろう。」と述べており、実習では、サイバー攻撃などを疑似的に体験することにより、危機感の構築もできるのではないかと考えている。

5. 結論

高校生は一定レベルの情報セキュリティの対策を行ってはいる。しかし、現在、社会で求められる知識はそのもう一歩先のものであり、それらが欠如していることは調査1の結果からわかった。もちろん、それらは「情報」の授業を行えば解決できる。しかし、本研究では「高校生は情報セキュリティに対して意識や危機感がほとんどない」ことが浮き彫りになった。学生の意識がこの状態では、授業や定期テストなどを行ったとしてもその場凌ぎになり定着しないことが予想される。つまり、学生がサイバー攻撃に遭う可能性が下がらないことになる。よって今後必要となるのが、学生に意識や危機感を持たせることであり、これらの問題を解決する足掛かりとなるのが「アクティブラーニング」や「実習」である。しかし、まだ実証されたわけではなく、あくまで理論的なものにすぎないため、今後はこれら2つを用いた研究がさらに求められる。

6. 引用文献

TRENDO MICRO(2021),『コロナ禍の法人を脅かす境界線内外の攻撃　2020 年年間セキュリティラウンドアップ』,46
総務省(2020),『サイバー攻撃の最近の動向について』,5
増山一光 (2013).「情報セキ ュリティ標語による高校生の情報セキュリティ意識に関する考察」,日本教育情報学会　第29回年会,4

7. 参考文献ならびに参考Webページ

文部科学省(2018),『高等学校情報科[情報Ⅰ]教員用研修教材』
インセプト. https://e-words.jp/.2022年4月26日
総務省,「国民のための情報セキュリティサイト」,
https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/.2022年4月26日