博士請求論文要旨

「高校生に対する情報セキュリティ教育の教授法に関する研究 ーインストラクショナルデザインによる実践-」

情報セキュリティ大学院大学 増山 一光

要旨

近年、インターネットや情報機器が社会に広く普及している。特に高校生は大人と同様にインターネットを利用し、携帯電話の保有率は95%を超えている。

こうした状況の中で、インターネット上のトラブルや問題行動に関連する行為を経験した高校生の割合が高まっており、高校生が情報セキュリティに関する事件を引き起こして逮捕される事件も発生している。そのため、高校生への情報セキュリティ対策が必要になってきている。実際に、内閣府の青少年のインターネット利用環境実態調査によると高校生が情報セキュリティに関する学習をしている場は、学校が最も多くなっており、学校で更なる情報セキュリティに関する学習を行いたいという学習ニーズが強くなっている。

そこで、本論文の研究では、高等学校での情報セキュリティ教育のカリキュラム開発を 行い、高校生の情報セキュリティに関する能力開発と適切な態度の育成を行うことができ る教授法を確立することを目的とする.

そこで、まず、大学 2 年生程度までの各教育機関における情報セキュリティ教育の先行 実践例と海外における情報セキュリティ教育のカリキュラムの比較や検討を行った.これ により、各教育機関で扱われている情報セキュリティ教育内容には大きな差はみられず、 その内容は多岐に渡っていることが判明した.このことは、情報セキュリティ教育は水平 拡散型のカリキュラムとしての特徴を有している.

次に、こうした先行実践例と小・中学校での実践を参考にして、高等学校における情報セキュリティ教育の在り方を示した。その基本は、高等学校で行われるべき情報セキュリティ教育が、高校生の発達段階に応じて情報モラルを踏まえつつ、情報セキュリティに関する技術、経営、法制度などの内容は初学者であることを考慮して導入のみとして扱い、情報社会における情報セキュリティに関する能力と態度を育成することが必須であるという考え方である。

具体的に,本論文では高校生に育成すべき能力としては次のようものを想定している.

情報セキュリティインシデントへの対策能力

- 情報セキュリティに関わるリスクを想定する能力
- ・ 情報セキュリティに関する情報収集能力

そして、高校生に育成すべき態度としては次のようものを想定している.

- ・ 情報セキュリティ意識
- ・ コンプライアンス
- 情報倫理

これらを踏まえて、神奈川総合産業高校における学校設定科目「情報セキュリティ」の カリキュラム開発を行った。この科目の目標は、「情報セキュリティに関する基本的な知識 を学び、情報システムのセキュリティポリシーの策定および実施、分析、見直しができる ようにする」ことである。

そして、高等学校での情報セキュリティ教育に求められる「教育はいかにあるべきか」 という教育観と「学習とはどのようなものか」という学習観について検討を行った。そし て、これらを踏まえた情報セキュリティ教育の要件としての能力と態度の育成の方略につ いて示した。

情報セキュリティ教育における教育観は、文部科学省の委託事業であった「情報モラル」 キックオフガイドにあるように、情報社会における安全教育に主眼が置かれることになる。 安全教育の視点からみた情報セキュリティ教育の目的としては、次の2点が挙げられる。

第 1 に、生徒を被害者にしないために、情報社会での護身術として情報セキュリティを 学ぶということである. これは、高校生にとってリスクの存在を把握して情報社会で安全 を確保することは、適切な社会生活を営むうえでも重要になると考えられるからである.

第 2 に、生徒を加害者にしないために、適切な情報セキュリティに関する知識・技能を 身に付けた上での行動できるようにすることである.これは、情報機器やインターネット の利用環境を適切に整え、自らの振る舞いが第三者にどのような影響を与えるのかを考慮 させつつ行動することによって、適切な行為を身に付けさせることができると考えられる からである.

情報セキュリティ教育における学習観という視点からは、学習内容や学習成果に多様性が求められている。その理由として、わが国でも実施されている国際的な学力評価として OECD 生徒の学習到達調査 (PISA) において、知識や技能を、実生活の様々な場面で直面 する課題にどの程度活用できるかどうかが評価されており、新しい学力として注目されているからである.

これまでの学習観には、行動主義、認知主義、状況主義といったものがある.これらの基となった学習理論の概要は次の通りである.

- ・行動主義 学習は刺激と反応の連合であり、経験による行動の変容である.
- ・認知主義 学習は理解によって知識が獲得されるので認知の変容である.
- ・状況主義 学習は学び合う共同体に参加することで形成されるものである.

情報セキュリティ教育における学習観は、上記の学習観のどれか一つだけに依拠することで形成することは困難である。そこで、インストラクショナルデザインにおける学習支援に役立つ基礎理論などを適材適所で活用するという折衷主義に基づいて、それぞれの学習観を組み合わせることが必要になる。

具体的には、基礎的な知識習得の学習活動については、行動主義に基づくものが中心となる. さらに情報セキュリティという特質から適切な状況認識に基づく行動力、リスクに対する問題解決能力、情報セキュリティインシデントに対するグループによる新たな知見の創造などが求められることから、認知主義、状況主義による学習も重要になる.

こうした情報セキュリティ教育の教育観,学習観を踏まえた,情報セキュリティ教育の 要件として掲げられる情報セキュリティに関する能力と態度の育成について,行動主義, 認知主義,状況主義の視点からみると次のようになる.

情報セキュリティに関する能力に関して、ベースとなる情報セキュリティに関する基礎知識については行動主義に基づいて効果的な学習を行わせ、リスクの想定や状況の判断については認知主義に基づいて問題解決型学習などを通じて、領域の移転など考える能力を身に付けさせる。その上で、実際の情報セキュリティインシデントへの対処能力については、行動主義に基づいて刺激一反応によるアプローチから育成する。

情報セキュリティに関する態度は、状況主義に基づいて協働学習などを通じてグループ の構成員が相互に気づきあいや教えあいをして、長期間にわたる議論や討論を通じて効果 的であると考えられる。また、こうした教育活動は、個人の情報セキュリティに対する「心の教育」や組織の情報セキュリティに対する「理念の教育」になると考えられる。

実際に高等学校における情報セキュリティ教育の要件を実現するために、教育設計であるインストラクショナルデザインにおける教授方略の開発手法により、次のような情報セキュリティ教育における4つの教授法を提案した.

① 行動主義に基づく情報セキュリティの基礎知識に関する教授法

情報セキュリティに関する基礎知識の教授にあたっては、授業内容の細分化をして、教授の最小単位を構成する.これを効果的に教えるために、新たに開発した教授法である3段階教授法を用いる.この教授法により、情報セキュリティが高校生にとって初めての学習内容であっても学習のプロセスを見失うことなく、学習内容を理解でき

る量での教授の実践によって、確実な知識の習得と定着を目指す.

- ② 認知主義に基づく情報セキュリティインシデントの想定や判断に関する教授法 情報セキュリティインシデントに対しての想定や判断する事案を提示し、認知の変 容や移転を促すために課題解決プロセス(双方向指導、グループワークなど)を行う. 加えて、学習成果としてのふりかえり学習では自分の考え方や知識がどのように変容 したかを認識させ、自らの変容とメタ認知が把握できるようになることを目指す.
- ③ 行動主義に基づく情報セキュリティインシデントに対する行動習得に関する教授法 情報セキュリティインシデントの想定や判断を踏まえて、実際に情報セキュリティ インシデントが発生する恐れのある時や発生した時に取るべき行動や具体的な手法を 習得させるもので、情報セキュリティインシデントに対する事前対策もしくは事後対 策の習得を目指す.
- ④ 状況主義に基づく情報セキュリティへの態度を育成する教授法

情報セキュリティへの態度として情報セキュリティ意識, コンプライアンス, 情報 倫理の育成を目指して, 状況主義に基づいて小グループによるコミュニティを形成させ, リアリティのある学習課題で協働学習を行う. さらに, ここで実践されたグループごとの学習を, 全体で共有することで新たな知見により, 適切な態度や考え方を形成させることを目指す.

インストラクショナルデザインを進める上で基本となるプロセスモデルである ADDIE モデルに沿って、この4つの教授法を用いて3つの教育実践を示した.

これらの教育実践で、共通しているのは①行動主義に基づく情報セキュリティの基礎知識に関する教授法の実践を行ったことであり、基礎的な内容の理解を促して、その上で能力や態度の育成を図った.

第 1 の教育実践はコンピュータウィルス対策教育である. ここでは,②認知主義に基づく情報セキュリティインシデントの想定や判断に関する教授法を用いて,生徒のプリコンセプションやバグルールの変容を目指して,コンピュータウィルスの事前対策・事後対策の重要性と手法について実践的に教授を行った.

この授業の 2 ヵ月後に学校設定科目「情報セキュリティ」の授業内で調査の結果,授業前よりも対策能力が向上したことを確認できた.加えて,情報セキュリティの学習を進め

ていくなかで、学習したコンピュータウィルスの事前対策と事後対策を他の情報セキュリティインシデントへの対策にも移転することができるようになったという副次的な効果もあった.

第 2 の教育実践はアンチボット教育である. ここでは, 多くの生徒がボット自体の存在を知らない状況のなかで, ③行動主義に基づく情報セキュリティインシデントに対する行動習得に関する教授法を用いて, ボットによる感染を検知する方法の教授を行った. こうした検知能力を身に付けさせて, 実際の家庭の PC 環境においても検知活動を行わせることができた.

第 3 の教育実践はフィッシング詐欺対策教育である. ここでは、フィッシング詐欺の危険を感知できるようにするため、URL からフィッシングサイトを判断する e ラーニングによる基礎知識の習得を行った. その後、情報セキュリティ意識の形成を目指して、④状況主義に基づく情報セキュリティへの態度を育成する教授法による協働学習を行った. この協働学習では、フィッシング詐欺サイトであるかどうかを他のメンバーの考えなどを参考にして判断する行為を通じて、情報セキュリティに関する状況や問題の所在を明らかにすることを目指した.

こうした学習成果によって情報セキュリティ意識の形成を確認するために,因子分析を 用いることで,発生と被害の認識,自己防衛,自己責任,許せない行為という因子を選出 した.

本論文の特徴は、これまでの教育実践を、インストラクショナルデザインの基礎理論である教育工学におけるデザイン実験を用いて、情報セキュリティ教育での 4 つの教授法の考察および評価を行ったことである。デザイン実験とは、理論を背景に、特定の現場で具体的なものを開発し、改善しながら現場に役立てるものにするというアプローチである。

具体的に、教育実践を踏まえて、デザイン実験における理論的なフィードバックを行うために、次の3つの視点から考察および評価を行った。第1に学習のプロセスの視点からは、4つの教授法を組み合わせることで知識、能力、態度の育成に寄与することを明らかにした。第2にガニェの9つの教授事象とケラーのARCSモデルの視点からは、教授事象から学習者の適切な学習プロセスと動機づけを実現することができることを示した。第3にガニェの学習成果の5分類の視点からは、4つの教授法から得られる学習成果がガニェの学習成果に対応しているとともに、情報セキュリティ教育における態度の育成に貢献していることを示した。

これらの評価を総合して,4つの教授法を用いた学校設定科目「情報セキュリティ」での 教育実践は十分有効であり、今後の実践に関する有益な知見を得ることができたと結論づ けることができよう. こうした知見は高等学校で行われる様々な形態での情報セキュリティ教育に適用して利活用できるものと考えられる.

Abstract

In recent years, the Internet and information devices are widely used in society. Focusing on high school students, the Internet utilization rate of high school students is almost same as that of adults. Furthermore, the prevalence of mobile phones is more than 95%.

In such a situation, many high school students have experienced information security problems on the Internet. And a few of high school students have been arrested for causing the incidents related to information security. Therefore, information security education has become necessary in high school. In fact, high school students are studying information security mainly at school, but they are wanting to learn more on the information security.

The purpose of this thesis is to develop information security curriculum in high school, and to establish pedagogy fostering attitudes and developing abilities for information security within high school students.

Firstly, I surveyed the practical examples of information security education in various educational institutions in our county and information security curriculum overseas, and discussed information security education in high school. From these surveys, I found that information security education in the high school must be made based on information ethics in accordance with the stage of growth of students. The contents of information security education should consist of an introduction to information security technology, management, and related law. Moreover, this education should aim at fostering attitudes and developing abilities about information security in corresponding to the student's aptitude and career.

Based on these, I developed the curriculum of school setting subject "information security" in Kanagawa Sogo Sangyo High School. The goal of this subject is such that students learn the basic knowledge of information security for developing and enforcement of information security policy, and for analyzing and reviewing the information security.

Then, I examined educational outlook and learning outlook required for

information security education in high school. From the educational outlook in information security education, it is essential that safety education would be a major challenge in the information society. The purpose of information security education from the viewpoint of safety education can be summarized as the following two points.

First, in order that students would not become victims of security incidents, they have to learn information security as a self-defense in the information society and have ability to identify the existence of risk. This possible should be attained for students to ensure the safety of the information society and are engaged in appropriate social life.

Second, in order that students would not become assailants of security incidents, they have to learn knowledge and skills about information security. This purpose is inevitable for students to be able to consider the impact of their behavior and behave in appropriate about an information security viewpoint.

For the learning outlook in information security education, the diversity of learning the contents and learning outcomes should be ensured. This purpose should be attained for students to acquire a fundamental knowledge about information security through learning activities based on behaviorism. In addition, information security education is required for students to acquire abilities on appropriate recognition behavior, problem-solving skills for the risks, learning measures of information security incidents in cooperation with others. Therefore, it is particularly important that the information security education is based on cognitivism and situationism.

From the educational outlook and learning outlook, as a requirement of information security education for fostering attitudes and developing abilities about information security must be consider from the viewpoint of behaviorism, cognitivism, and situationalism.

A abilities of information security includes basic knowledge, assumptions and judgments, incident measures. Basic knowledge of information security is formed by effective learning based on behaviorism. Assumptions and judgments of risk are developed by transformation and transfer of cognition through learning by problem-solving based on cognitivism. And, measures ability of actual information security incidents is developed by from stimulus and reaction approach based on behaviorism.

The attitude of information security is fostered through discussions and debates

over a relatively long period of time. There the students learn as a member of study group and teach each other to notice through collaborative learning based on situationalism. These educational activities are intended to foster "education of philosophy" for the organization's information security and the "education of the heart" for the security of their own personal information.

Actually, in order to achieve the aim of information security education in high school, I proposed following pedagogy of information security education by making use of the method of instructional design:

-Pedagogy of basic knowledge of information security based on behaviorism.

Teaching basic knowledge of information security is performed by using the smallest units of lesson contents, which are subdivision of overall lesson contents. In order to teach this effectively, a three-step teaching method is used as a newly developed method. This method is helpful so that students would never lose sight of the learning process. Further in the pedagogy, an appropriate amount of lesson contents are presented so that students would understand well, aiming at the acquisition and establishment of knowledge.

-Pedagogy of assumptions and judgments of information security incidents based on cognitivism.

At the beginning of lesson by the pedagogy, information security incidents are presents for students to exercise assumptions and judgments in regard to information security. For this case, problem-solving learning (interactive teaching, group work, etc.) is given to promote the transfer and transformation of cognition. In addition, looking back at learning on learning outcomes, students review how their ideas and knowledge transformed, to understand the transformation of their own cognition and metacognition.

-Pedagogy of learning behavior for information security incidents based on behaviorism.

Based on the assumptions and judgments of information security incidents, students learn the techniques and specific actions to be taken when information security incidents are supposed to occur in the near future or when they actually occurred. More specifically, this pedagogy aims at the acquisition of proactive or reactive measures against information security incidents.

-Pedagogy of fostering for information security attitudes based on situationalism.

The attitudes required for information security are thought to include information security awareness, compliance, and information ethics. This pedagogy aims to foster these attitudes by the small communities that are formed by dividing students into small groups, based on situationalism. In the communities, collaborate learning is performed with practical tasks. Additionally, it aims for students to find new knowledge through the collaborate learning of each group, and to get appropriate attitude and approach by sharing the learning results of every group.

Along the ADDIE model, which is an underlying process model in promoting instructional design, I showed three types of educational practice by making use of pedagogy of four. In these educational practices, I have always used pedagogy of basic knowledge of information security based on behaviorism. This is because the basic knowledge of information security based on behaviorism is fundamental for students to understand every learning contents. Moreover I aimed at developing abilities and fostering attitude about information security.

The first educational practice is anti computer viruses education. The aim of the practice is transformation of both pre-conception and bug rule among students. Using the pedagogy of information security incidents assumptions and judgments based on cognitivism, I made the educational practice of proactive and reactive measures of computer viruses. Two months later from this practice, in the class of school setting subject "information security", I conducted a questionnaire survey on results of the above practice and verify that students' ability of measures for information security had been improved. In addition, it is confirmed that students can transfer the learned measures of computer viruses to those of other information security incident in the continuous learning process of information security.

The second educational practice is anti-BOT education. Many students did not know the existence of BOT itself. Using the pedagogy of learning behavior for information security incidents based on behaviorism, I made the educational practice of how to detect BOT infection. I gave the lesson for acquiring BOT detection ability to students. As a result, they became to be able to perform BOT sensing activities in the home PC environment as well.

The third educational practice is anti-phishing education. In order for the students

to be able to identify the danger of phishing, I carried out the acquisition of basic knowledge through e-learning to determine phishing sites from URL. This practice brought about the same learning outcomes as that of using the pedagogy of learning behavior for information security incidents based on behaviorism. After the lesson, I made collaborative learning by the pedagogy fostering for information security attitudes based on situationalism, aiming to the formation of information security awareness. Through the act of judgment with reference to the ideas of other members, such as whether it is a phishing site, collaborative learning is aimed to clarify situations and whereabouts in question related to information security. I examined the security awareness of students by conducting a questionnaire survey and analyzed the survey result by factor analysis and verified the learning outcomes.

From these educational practices, the proposed pedagogy of four of information security, which are design by the theory of instructional design, are examined and evaluated. And ,as results of these examination and evaluation, I found that pedagogy of four contribute for students to acquiring knowledge, developing abilities and fostering attitudes about information security. Thus, I confirmed them to be an effective pedagogy in information security education in high school.

Furthermore, I examined the effectiveness pedagogy of four by referring to nine events of instruction (R.M.Gagné) and the ARCS model (J.M.Keller), and confirmed that pedagogy of four actually achieved learning outcomes from viewpoints of the appropriate learning process and students' motivation. And, finally, I also made it clear that the learning outcomes by pedagogy of four correspond to the five major categories of learning outcomes (R.M.Gagné).