九州大学におけるサイバーセキュリティ教育の紹介

岡村耕二（九州大学サイバーセキュリティセンター）

Introduction of the Cybersecurity education in Kyushu University

Koji OKAMURA (Cybersecurity Center, Kyushu University)

はじめに

九州大学では平成29年度から全学生を対象にしたサイバーセキュリティ教育を開始する。近年の世界規模でのサイバー犯罪の急増と悪質化、サイバー人材需要の急速な増加、サイバーセキュリティ基本法の施行による法律に基づいた日本国全体のセキュリティ力の増強などを鑑みて、大学におけるセキュリティ教育も見直されるべきである。このような背景で、本稿では九州大学ではじまるサイバーセキュリティの全学的な教育について、その準備や課題などを述べる。

全学サイバーセキュリティ教育の必要性

従来の一般的な学生を対象としたセキュリティ教育や情報倫理教育は、ネットワーク利用のリテラシ教育の延長上にあり、学生が外部に対して加害者にならないことが主な目的であった。例えば、20世紀の終わりの Web 発明を契機としたインターネットの急速な普及時期における学生のインターネット使用上のマナー向上や、その後のファイル交換ソフトウェアの使用による著作権侵害を防ぐためのリテラシ教育が主であった。ところが、近年では急増するセキュリティ脅威によって、学生が被害者にならない教育を行う必要性が急速に高まった。急増し、悪質化するセキュリティ脅威のために、九州大学では IDS (Intrusion Detection System) や、次世代ファイアウォールの導入を行ってきた。導入時にはある程度の効果を得たものの、標的型攻撃、マルバタイジング攻撃、といったセキュリティ対策機器では対処不可能な攻撃の出現によって、全く別のアプローチを取らざるを得ない状況になってきた。このような状況で九州大学では、平成26年度から学生がサイバーセキュリティ脅威から自らを守るための知識と技術を身につけるための方策として、全学サイバーセキュリティ教育の実施の検討を始めた。

全学サイバーセキュリティ基礎論の試行

平成26年度の前期には、サイバーセキュリティ基礎の講義のシラバスや教材の準備を行い、平成26年度後期より、自主開講という形で「サイバーセキュリティ基礎論」を試行的に開講した。サイバーセキュリティ基礎論では、文系、理系を問わず、また、学生の前提知識にも依存せずに、学生が学べるようなカリキュラムを設計した。開講した平成26年度は受講数が38名であったが、平成27年度前期は55名、後期は115名となり、平成

28 年度前期の受講数は 220 名となった。受講生も、歯学部を除く全学部からの受講となった。九州大学の 1 年生は平成 28 年の時点で約 2,600 名であり、これを 200 名の 13 クラスで実施する計画を立てていたため、平成 28 年度では必須化した時の大人数クラスを想定した講義を行うことができた。

サイバーセキュリティ基礎論のカリキュラム

サイバーセキュリティ基礎論では NICE (The National Initiative for Cybersecurity Education) などを参考にしてサイバーセキュリティ教育の一般的な科目構成から、不正プログラム対策、アクセス制御など、専門性を必要とする内容を割愛し、学生がサイバー被害者にならず、また、サイバーセキュリティに関して最低の技術的な知識・リテラシを身につけることを目標とした。必須化する平成 29 年から九州大学はクオーター制になるため、8 週（1 単位）でカリキュラム設計をしている。内容は、1. 講義ガイダンス・サイバーセキュリティの事例、2.3. サイバーセキュリティ技術(1,2)、4.サイバーセキュリティにかかる法律、5.研究倫理・情報倫理、6.著作権、7.暗号技術、8.サイバー空間と社会科学である。これらのカリキュラムは、平成 26～28 年度の試行期間で得られた知見に基づくものである。当初は導入として事例の紹介を多用したが、事例の紹介は話としてはしやすいが、学ぶ学生が習得する内容が少なく、最低限に切り詰めることにした。サイバーセキュリティ技術は、WIFI やスマートフォンなどの ICT 機器の利用にかかる実用的な内容を扱うが、このような講義は初めにした方がよかったという意見が多数あったため、前半に行うことにした。情報倫理に加えて、将来研究者になることを想定して、研究倫理もしっかりと教育することした。セキュリティに関する用語の習得、理解は、もはや、文系の学生でも必要であるので、セキュリティの 3 要素（機密性、完全性、可用性）や、共通鍵暗号、公開鍵暗号などの解説も採り入れた。最後に、SNS にかかる問題を教育するために社会科学に関する講義も行っている。

まとめと今後の課題

試行期間の最初は講義の最終週に記述方式による試験を実施したが、各週で全く異なることを扱うため、1 回の試験ですべての内容をカバーするのは困難であったため、各会に小テストを行うことにした。当初は記述方式の問題を採用していたが、大人数を公平に評価するために、選択肢問題を採用することとした。サイバーセキュリティ基礎論を受講すれば、IPA が実施している IT パスポートのセキュリティに関する設問は理解できると考えられるので、セキュリティ分野では IPA IT スキル レベル 1 程度は身につけることができると自己評価している。

今後の課題ひとつは、サイバーセキュリティ科目の必須化によって、九州大学全体のセキュリティ力がどの程度向上したか定量的な評価を行うことである。今後も新しい概念・技術を導入し、よりよいセキュリティ教育を永続的に行う予定である。