九州大学サイバーセキュリティセンターの紹介

岡村耕二 橋口勝弘 上拾石弥好 新里亜希

九州大学 サイバーセキュリティセンター

oka@ec.kyushu-u.ac.jp

Introduction of Cybersecurity Center of Kyushu University

Koji OKAMURA, Katsuhiro Hashiguchi, Yayoi Kamijukkoku and Aki Niisato

Cybersecurity Center, Kyushu University

概要

2014 年に設置された九州大学サイバーセキュリティセンターは、サイバーセキュリティに関する教育、研究、外部連携、社会貢献を柱にして幅広く活動を行っている。本稿では、本センターの活動内容について紹介する。

1. はじめに

九州大学では、2014 年に、基幹教育から専門教育にわたって国際標準となるようなサイバーセキュリティ教育プログラムに基づいた教育に重点を置きつつ、サイバーセキュリティに関する様々な脅威を対応できる次世代的なセキュリティ技術ならびにサイバー空間を絶対的に頑健にする先進的基盤研究、ならびに国内外との組織と連携し法制度や社会現象に関するサイバー空間そのものの研究を持続的に行うセンターを設置し、サイバーセキュリティに関する教育・研究を集約した活動を開始した。本センターの目的は、社会に輩出する全学生のセキュリティリテラシの絶対的な向上、高度で先進的な教育を受けたセキュリティの専門家の育成、先端かつ包括的なセキュリティ研究を持続的に行うことである。本稿では、九州大学サイバーセキュリティセンターの設置以来の教育、研究、社会貢献について総括して紹介する。

2. サイバーセキュリティ教育

九州大学では、全学部の新入生約 2,700 名に対して、春学期に必修授業としてサイバーセキュリティ基礎論を 2017 年度から開講している[2]。サイバーセキュリティ基礎論は、2014 年度から 3 年間は選択科目として開講し、講義で扱う内容の検討や、教材ならびに学生評価のための小テストなどの開発を行った[1]。

サイバーセキュリティ基礎論は、１クオータ（8 週）で開講される。講義の内容は、[1]サイバーセキュリティ最新情報、 [2] 安全な設定(1) [3]安全な設定(2)、 [4] 研究倫理・情報倫理、 [5] 暗号技術を知る、 [6] サイバーセキュリティと法律、 [7] 著作権 [8] 社会科学である。それぞれの講義は 90 分のうち 70-80 分座学を行い、最後に確認の小テストを行う。小テストは、各回 5～10 問程度であるが、この講義が月曜から金曜まで全 15 クラスで開講されていることから、異なるクラスの学生間で小テストの問題が共有されないように、設問は 15 問～30 問用意され、受験者ごとにランダムに異なる問題が出題される。

サイバーセキュリティ基礎論は実践的な教育であるので、教わった内容の理解が小テストによる定着度の評価のみで、後はなにもないのでは不十分である。つまり、習ったことが自分の実生活で役に立つことを実感できることが重要である。そのためには、講義時間外の時にもサイバーセキュリティについて気に掛ける習慣を

つけることが必要である。そのようなことは通常、予習、復習という形で行われるが、学生に無条件に自主的な自学を期待することは容易ではない。

このような背景で、GRCS 社が開発したシリアスゲームを導入している。このシリアスゲームは、図 1 に示されるよう、ゲーム感覚で自分のスマートフォンでも利用可能であるため、講義時間外に時間も場所も選ばずに自学が可能である。我々はシリアスゲームの利用が講義時間外にサイバーセキュリティのことを気に掛ける習慣作りのきっかけになるのではないかと考えた。シリアスゲームはパソコン上のみならず、スマートフォンでも動作可能であるため、学生が帰宅後あるいは通学中にあえて受講させるために、回答開始時刻を 4 時間目終了からある程度時間の経過した 17 時からとし、終了時刻を翌日の 13 時として、実施することにした。また、シリアスゲームが復習や自学を促す効果があったのか評価を行い、結果、シリアスゲームが復習をするきっけかになったなどの前向きな結果が得られている[2][3]。

図 1: シリアスゲームの画面

さて、九州大学の基幹教育で、サイバーセキュリティを基幹教育に必須として採り入れる時に、どの科目に入れるべきか、議論が行なわれ、プログラミングなどの単位のある理系ディシプリン科目に入れたらどうかという意見もあったが、理系ディシプリンの単位は文系の学部では選択になっているため、適切ではなかった。そこで、理系・文系ともに必須であり、セキュリティを学ぶにふさわしい科目として、新たに「サイバーセキュリティ科目」が新設された。なお、基幹教育でサイバーセキュリティ科目以外のものは、基幹教育セミナー、課題協学科目、言語文化科目、文系ディプリン科目、理系ディシプリン科目、健康・スポーツ科目、総合科目、高年次基幹教育科目がある。サイバーセキュリティ科目で、サイバーセキュリティ基礎論以外の講義としては、夏学期と冬学期に開講される「企業から見たサイバーセキュリティ」と、集中講義で開講される「サイバーセキュリティ演習」がある。

企業から見たサイバーセキュリティは、選択科目で、春学期のサイバーセキュリティ基礎論の応用的な授業の位置づけである。ヤフー株式会社の現場で勤務している社員が毎週オムニバス形式で、実際のインターネット関連業務を通じて得た知見に基づいて、サイバーセキュリティに関する講義を行っている。さらに、受講者から数名を選抜して夏季休暇および春季休暇の間、東京にあるヤフー株式会社の本社に会社訪問を行い、そこでさらなる実践的にセキュリティや ICT 企業について学ぶ機会を提供している。図 2 は、2019 年度夏季休暇中の会社訪問の様子である。

図 2: 2019 年度夏季休暇中の会社訪問の様子

サイバーセキュリティ科目の一つであるサイバーセキュリティ演習も選択科目で、座学よりもさらに実践的なサイバーセキュリティの演習をハンズオン形式で受講できる。演習の内容は次に紹介する enPiT の内容と共通的である。

専門的なサイバーセキュリティ教育としては、文部科学省「成長分野を支える情報技術人材の育成拠点の形成/Society5.0 に対応した高度技術人材育成」事業の一環で、工学部電気情報工学科 3 年生、4 年生を主に対象とした enPiT2 [4][5]と、社会人を対象として、大学院システム情報科学府の講義で行う enPiT Pro [6]に参加している。図 3 は、九州大学で開催された enPiT2 の様子である。演習は、仮想計算機などを利用してメモリオーバーフロー脆弱性を狙った攻撃を実際に体験し、その対策を学ぶ基礎的なことを主眼においている。演習は、PBL 形式でグループワークを想定しているが、結局、個人個人が端末の画面とのにらめっことなり学生間でのコミュニケーションの機会が自然には発生にしにくいので、演習の合間に定期的にグループワークを行うことで、学生同士で話し合う機会を設けている。

図 3: enPiT2 の様子

3. 国際共同研究

九州大学サイバーセキュリティセンターは、2016 年より JST 国際科学技術共同研究推進事業 SICORP の国際共同研究拠点として、インド工科大学デリー校と「安全・安心な IoT サイバー空間の実現」に関する共同研究に取り組んでいる。

IoT 空間は、様々な情報を収集し、それらの情報を高度に解析した結果をフィードバックすることによって、人々の生活を劇的に変化させることができることから第４次産業革命とも呼ばれ、その実用化が世界中で期待されている。IoT 空間の実用化の鍵はセキュリティの確保にある。本研究の目的は、IoT 空間を安全にするための研究開発を総合的に行い、「安全な IoT サイバー空間を実現」することである。本研究では、複雑な IoT 機器、ネットワーク、サーバおよび様々な情報で構成される IoT 空間のセキュア化を、インド工科大学デリー校と九州大学のそれぞれ得意とする研究領域を融合させ実現する。本研究では、IoT 空間サービスを提供する人間やそのサービスを利用する人間が安全に IoT 空間を利用するための訓練や教育を含めている所も特徴の一つである。本研究によって IoT 空間そのものの実用化と、IoT 空間を安全に利用するための人間のリテラシの向上が同時に可能となり、真の IoT 時代の到来を加速させることが期待できる。特に、インドでは多くの社会インフラへの ICT による支援が期待されているため、本研究成果の還元によるインド社会への貢献が大いに期待できる。本研究では、IoT 空間を安全にするための 6 つの研究課題を決定し、それぞれの課題を担当する WP(Working Package) を日本側、インド側のメンバーで構成した。

- WP1: IoT 用の安全な組み込みシステム
- WP2: セキュリティ指向低消費エネルギー IoT プロセッサシステム
- WP3: 安全な IoT 空間クラウド
- WP4: 安全な IoT アプリケーション
- WP5: 脅威情報を利用した IoT 専門教育
- WP6: サイバー演習装置を用いた IoT スペ

シャリスト育成教育

各 WP のこれまでの研究成果を簡単に紹介する。IoT の設計レベルでのセキュリティ向上を目指している WP1 は、ドメイン特化モデリング言語を用いて、セキュリティ、プライバシ要件を満たさなくなると実行できなくなる機能を持つ IoT デバイス用のモジュールを開発可能とする開発環境のプロトタイプを開発した。アーキテクチャレベルでのセキュリティ向上を目指し安全な IoT プロセッサの開発を行っている WP2 は、マイクロプロセッサチップが提供するパフォーマンス・モニタリング・カウンタ(PMC)の情報を人工知能を用いて、特徴量を抽出し、プログラムの実行時にプロセッサが脅威を動的に検出できる機能の開発を行った。IoT で用いられるデータのセキュリティの研究を行っている WP3 は、IoT での脅威検知技術を軽量化するために深層学習画像分類機を基づく IoT 環境での軽量なマルウェア検知システムを開発している。IoT セキュリティにおけるフレームワーク及びアプリケーションの研究開発に取り組んでいる WP4 は、ブロックチェーン技術を利用した安全な IoT フレームワークを実現するために、IoT に適したブロックチェーンの改良を行っている。そのために、ブロックチェーンのデータサイズの肥大化する問題を解決する技術、IoT 環境において安全に分散計算を行える技術、さらに、ブロックチェーンに利用されている合意形成アルゴリズムを IoT に合わせた軽量なアルゴリズムの開発を行った。IoT セキュリティ専門教育のための教材開発と教育実践を目的としている WP5 では、他の WP の研究成果を逐次反映した教材開発を進めている。そのために IoT 脅威情報の素材データを蓄積・管理するデータベースの、そのデータを教材として統合表示するオーサリングシステムを開発している。さらに LA(Learning Analytics)を可能とするウェブ教材閲覧システムや IoT のシリアスゲーム教材の開発を行っている。IoT システムの管理者などのスペシャリストの教育のための研究を行っている WP6 は、サイバーセキュリティ演習装置で、IoT セキュリティについて短時間で教育可能な演習コース、効率的な自学を行うために IoT デバイスの仕様書などから選択式の小テスト問題を自動的に作成する技術を開発している。さらに、スペシャリストの教育としてペネトレーションテストに注目し、IoT システム全体のペネトレーションテストを行えるツールの開発を行っている。このプロジェクトの重要な技術革新は、IoT のセキュリティに対する一般的なアプローチである。これら、本プロジェクトで開発された様々な教材は、近い将来 IoT を安全に使用するための教育分野の拡大に今後大きな需要があると期待できる。

図 4 は、インド工科大学デリー校でワークショップを行った際の集合写真である。

図 4: インド工科大学デリー校でのワークショップ集合写真

九州大学サイバーセキュリティセンターは、設置当時からアメリカ・メリーランド大学ボルチモア校と深く連携している。図 6 は、2015 年 1 月に開催された九州大学サイバーセキュリティセンター開所式にあわせてメリーランド大学ボルチモア校から表敬訪問を受けた際の写真である。加えて、オーストラリアニューサウスウ

ェールズ大学、イギリス・ロンド大学ロイヤルホロウェイ校とも定期的な国際サイバーセキュリティワークショップを開催している。

図 5: 九州大学サイバーセキュリティ開所式

4. 社会貢献

九州大学サイバーセキュリティは、設置当時より「せきゅトーク」という一般市民向けのサイバーセキュリティセミナーを企画・実施している。このセミナーは総務省のサイバーセキュリティ月間の関連行事でもある。本セミナーでは、本センターが包括的に連携をしている福岡県警、企業から見たサイバーセキュリティを担当しているヤフー株式会社、本センターに寄付研究部門を設置している富士通株式会社、地元通信事業者である Qtnet などからの一流の外部講師を招聘し、実践的な内容を扱っている。図 6 に、せきゅトークの会場の様子を示す。

図 6: 一般市民向けサイバーセキュリティ講座「せきゅトーク」の様子

5. おわりに

九州大学サイバーセキュリティセンターは、教育、研究、外部連携、社会貢献を柱にサイバーセキュリティに関する様々な活動を幅広く行っている。本稿ではその一部を紹介した。年次大会ではポスター展示を行っているので、より詳しい情報はそこで聞き出して頂きたい。

参考文献

[1] 岡村耕二, “九州大学におけるサイバーセキュリティ教育の紹介”, 一般社団法人大学 ICT 推進協議会 2016 年度 年次大会 論文集

[2] 岡村耕二, “サイバーセキュリティ基礎教育へのシリアスゲームの導入効果に関する研究”, 一般社団法人大学 ICT 推進協議会 2017 年度 年次大会 論文集

[3] 岡村耕二, “サイバーセキュリティ教育授業アンケートの分析に関する研究”, 一般社団法人大学 ICT 推進協議会 2018 年度 年次大会 論文集

[4] 曽根秀昭,” 実践的セキュリティ人材育成に関する取り組み”, 一般社団法人大学 ICT 推進協議会 2018 年度 年次大会

[5] 山本雅基、岡村耕二、他,”大学学部生を対象とした実践的 IT 人材育成プログラム enPiT2 と評価” 電子情報通信学会 SS 研究会論文集 SS2018-82, 2019 年 3 月

[6] 湯浅墾道、小出洋、他, “社会人エンジニアのための実践的な情報教育”, 一般社団法人大学 ICT 推進協議会 2019 年度 年次大会 論文集

謝辞

本研究は九州大学サイバーセキュリティセンター 平成元年度国立大学法人運営費交付金機能強化経費の助成ならびに JST SICORP、JPMJSC16H3 の支援を受けたものである。