



対応力の高いセキュリティ人材を KIPS 活用によって継続的に育成



鶴岡高専

National Institute of Technology, Tsuruoka College

www.tsuruoka-nct.ac.jp

大規模かつ深刻なインシデントを 想定したサイバーセキュリティ演習を、 山形県警察本部サイバー犯罪対策室と共催

鶴岡工業高等専門学校 佐藤淳教授は、学生たちに組み込みシステムやIoTに関する教育を行いながら、山形県警のサイバー犯罪対策テクニカルアドバイザーを兼任。2018年には県警と共同で、地域の重要インフラ事業者や中小企業を対象にサイバーセキュリティ演習を実施しています。この時、教材として活用されたのが、カスペルスキーの提供するシミュレーションでした。

「組み込みシステムの研究と教育」を研究テーマとして、学生たちにソフトウェア工学やデジタル制御システム、総合技術論などを教える佐藤淳教授は、将来、重要インフラや産業設備のエンジニアとして巣立っていく学生たちの必須スキルとなる「サイバーセキュリティ」の継続的な教育に注力。山形県警との相互連携によって、学生たちがサイバーセキュリティを学ぶ機会を増やしています。



「このゲームの興味深い点は、模範回答を示さないことです。現実と同じように手探りで攻撃を推察し、対応していく力が養われます」

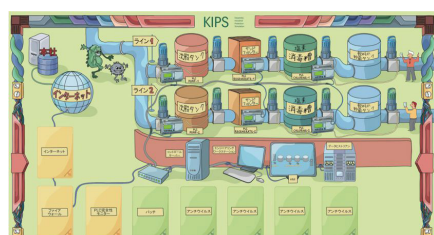
独立行政法人国立高等専門学校機構
鶴岡工業高等専門学校
創造工学科電気電子コース長
教授 博士(工学)
佐藤 淳 氏

課題

電気・ガス・水道・通信などの施設や、企業の生産設備など重要な設備は、サイバー攻撃の格好の標的となります。電気や水道が止まれば地域の生活は混乱し、生産設備が停止すれば企業は大きな損害を被るでしょう。損害を最小限に抑えるには、サイバー攻撃の可能性をいち早く察知し、適切な初動対応を行う必要があります。その時に求められるサイバーセキュリティのスキルや一定の知識に基づく理解は、少数の“専門家”だけではなく、制御システムに携わる“エンジニア”たちや、“マネジメント”を行うすべてのメンバーに求められています。

佐藤淳教授は次のように話します。
「サイバーセキュリティの教育に関しては、“専門家”を育成するだけではなく、重要インフラや産業設備に関わるエンジニアたちに必要なITスキルの一環として、継続的な教育を行うことが重要です。しかし今の日本では、残念ながらITスキルの教育そのものが不足している状況にあり、サイバーセキュリティに対応する能力を含めて、全体のITスキルを底上げしていく必要性を強く感じています。そして今、国立高等専門学校機構全体としても、拠点校および実践校を中心としてサイバーセキュリティの専門家教成と、一般的なITスキルとしてのサイバーセキュリティ教育の両輪を回すことを強く意識して、取り組みを進めているところです」

しかし、知識習得中心の座学講習を増やすだけでは、最新の攻撃手法によって引き起こされる大規模で深刻なインシデントに、柔軟かつ適切に対応する能力を養うことは困難です。そこで、より実用的な教育手段を求めた鶴岡工業高等専門学校が導入したのが、カスペルスキーが提供する、ボードゲーム形式の教育用シミュレーション「Kaspersky Interactive Protection Simulation (以下、KIPS)」でした。



Kaspersky Interactive Protection Simulation : KIPS

■ゲームの目的

- プラントのサイバーセキュリティチームとして自社資産を保護
- 2つの生産ラインの稼働を保ち、5ターン（＝5週間）の間に、できるだけ多くの収入を上げる
- ゲーム終了時の合計収入によって順位を決定

Kaspersky Lab のソリューション

KIPS は、サイバー攻撃による被害を抑えて、「本来得られるべきビジネス収益」を守ることを目的としたシミュレーションであり、ターンごとに、手持ちのカードから適切なアクションを選んで実施します。シナリオは「水処理施設」や「発電所」、「金融」に「行政」など6つが用意されています。

佐藤教授は、「非常に良く出来たシミュレーション」と KIPS を評価しています。「現実的なシナリオに沿って、ここまで具体的にサイバーセキュリティの考え方を学べる演習プログラムは、KIPS 以外に知りません。」

このゲームの興味深い点は、ターンごとの結果はシステムが自動的に採点して成績順を表示しますが、『どのような行動を取れば良かったのか?』という模範回答は示さないことです。現実と同じように、自分たちが最初に選んだ行動の影響を次のターンに引きずりながら、『次は何をするべきか?』を手探りで考え、能動的にアクションを選択していくことで、攻撃を推察し、対応していく力が養われます。これまで、本校の学生たちを対象に4回の演習を行ったほか、九州地区で開催された演習なども見てきましたが、初心者から上級者まで幅広い層に学びを与える演習だと実感しています」

ターンごとに選択した行動によっては、プラントが爆発炎上したり、生産システムがすべて停止して莫大な損害を被るといった事態も発生します。こうした、重大インシデントが発生する状況を疑似的に体験できることが、「学生にとっても、社会人にとっても、得難い体験になる」と佐藤教授は続けます。「KIPS のシナリオはどれも良く出来ています。実際に生産システムなどに携わっている社会人は、現場を想像しながら『起きてはいけない事態』に至る工程をイメージ出来ます。一方、現場を知らない学生たちも、対応を誤ればどのような事態を招いてしまうのか、座学よりもはるかに明確なイメージを得ることが出来るでしょう」。

展望

佐藤教授は、山形県警察本部サイバー犯罪対策室と共同開催した「サイバー攻撃への対処能力向上を目的としたサイバーセキュリティ演習」でも、KIPSを活用しています。県内を4つの地域に分けて、各地域の重要インフラ事業者や各企業の担当者等を対象としたこの演習は、今後、回を重ねる要望があるといいます。

2018年2月20日に開催された1回目の演習では、地方公共団体及びインフラ事業担当者をはじめとする約30名が8つのチームに分かれて対戦。どのテーブルも、対応策を協議する真剣な表情に溢れていました。地域でサイバーセキュリティに関連する人材の交流と、実践的な学習を同時に満たすことが出来たこの演習の満足度は高く、好評のうちに幕となりました。

佐藤教授は言います。

「本校の学生たちには、すでに4回、KIPSの演習を体験させていますが、チームを変えて繰り返し体験することで、学習の成果もより高くなっていくことを実感しています。県警と共催した今回のような会を頻繁に開催するのは難しいかも知れませんが、継続的な開催を検討する価値は、十分にあると思います。

産業に関して言えば、日本国内にはまだまだネットに接続していない設備が数多くありますが、これからインダストリー4.0の波が国内にも浸透し、IoT（Internet of Things：モノのインターネット）も普及していく中で、サイバーセキュリティの重要性は一層増していきます。そうした中で、KIPSを活用して、質の高い演習を手軽に実施出来ることは、私たち教育者にとっても、学ぶべき学生にとっても、スキルを高めたい社会人にとっても、非常にありがたいことだと感じています」



Kaspersky Security Awareness:

<http://www.kaspersky.co.jp/enterprise-security/cybersecurity-awareness>

サイバー脅威のニュース: www.securelist.com

#truecybersecurity

www.kaspersky.co.jp

©2018 Kaspersky Lab. All rights reserved.

KasperskyおよびカスペルスキーはKaspersky Labの商標登録です。その他記載された会社名または製品名などは、各社の登録商標または商標です。なお、本文中では、TM、®マークは明記していません。

KASPERSKY lab

株式会社カスペルスキー

〒101-0021

東京都千代田区外神田3-12-8

住友不動産秋葉原ビル 7F

jp-sis@kaspersky.com