サイバー攻撃に備えたBCPを支える“活きた”人材の育成へ

国立大学法人 名古屋工業大学

www.nitech.ac.jp

重要インフラを守るために必要不可欠な“マネジメント力”を高める実践的サイバーセキュリティ演習

国立大学法人 名古屋工業大学 越島研究室では、近年特に重要なテーマとして、サイバー攻撃を対象とした BCP（事業継続計画）に取り組んでいます。そして、万一のインシデントに迅速かつ正確に対応できる人材の育成に適した演習教材として彼らが注目したのが、カスペルスキーの提供する、ゲーム形式の教育用シミュレーションでした。

越島研究室を率いる越島 一郎 教授は「プロジェクトマネジメント技術の開発と応用」を研究テーマとし、製造業などにおける制御システム系のサイバーセキュリティ対策にも早くから注力。制御システム系のサイバーセキュリティのワークショップを開催してきたほか、情報処理推進機構（IPA）が運営する「産業サイバーセキュリティセンター」においてもセキュリティ人材の育成に取り組んでいます。

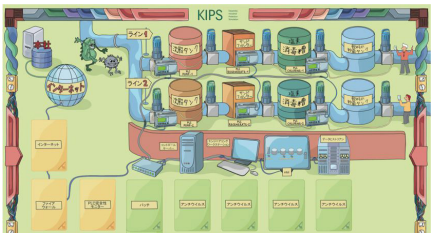
課題

「重要インフラの BCP には、IT の技術だけではなく、現場とコミュニケーションして、マネジメントする能力までが求められるのです」

国立大学法人 名古屋工業大学
教授
越島 一郎 氏

サイバーセキュリティ人材の育成において、もっとも難しい点は「事前にインシデントを経験させることができない」ことにあります。
「実際にインシデントが発生した際には迅速かつ正確な初期対応が重要となりますが、人的ミスから機器のトラブルまで、原因がどこにあるのか簡単には判別できません。そうした時、即座に『サイバー攻撃の可能性』までを想定して検討できるかどうかが、大きな分かれ道になります。こうした対応力……論理的に推察し、判断していく力を養うには、座学よりも演習形式の教育が有効です」（越島教授）
越島研究室が中心となって、IT 企業 2 社の協力の下に開催された「制御系サイバーセキュリティワークショップ」は、2015 年から 2 年にわたり、約半年に一回のペースで開催されてきました。さらに、産業サイバーセキュリティセンターに教授が提供しているプログラムも、演習が中心に構成されており、「演習でやっていることを理解できるように講義の時間を構成している」と言います。
こうして実践を重ねることでサイバーセキュリティ演習の内容はかなり充実してきました。しかし、越島教授が掲げた目標には、いまだ達していないと言います。

「私は米国国土安全保障省（Department of Homeland Security）が 2009 年に主催した大規模なサイバーセキュリティ演習に参加したのですが、その時に大きな違和感を覚えたのです。まるで、各国から集まった CSIRT（Computer Security Incident Response Team）たちがその腕前を競うお祭りのように感じたのです。私は以前、エンジニアリング企業に勤めていましたので、プラントなどの重要インフラがどのように運用されているか、よく知っています。重要インフラの運用は、サイバー空間だけで解決できるものでありません。どうしても、人に頼らざるを得ないのです。つまり、サイバー攻撃に対応して、重要インフラの BCP には、IT の技術だけではなく、現場とコミュニケーションして、マネジメントする能力までが求められるのです」
こうして、より“現実に則した”演習教材を探し求めていた越島教授がたどり着いたのが、カスペルスキーが提供する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

越島教授は、「経営やマーケティングの視点まで組み込まれたシミュレーションを見たのは、KIPS が初めてだった」と振り返ります。
「KIPS が使用されたあるイベントに、研究室の学生たちが参加したことがきっかけでした。このイベントでさらに、学生のチームを成績に応じて何度も組み換えながら実験的に演習を重ねてみたところ、毎回結果が変化していくので、ますます面白く感じました。学生たちがゲームを熟知するほどに実験を重ねたこともあり、今ではもう、自分たちの研究成果と同じような愛着さえ感じています」

越島研究室ではこの KIPS に、過去 4 回開催された制御系サイバーセキュリティワークショップにおいて参加者たちがどのように考え、行動したかを記録したワークフローに、学生たちが解析することで得た知見を加味することで、「KIPS “名工大バージョン”」とも呼べる、新しい演習形式を発案しています。
それが、「各チームの人員を、マネジメント役となる “本社側” と、実際にインシデントに対応する “プラント側” という 2 つのグループに分けて、互いのコミュニケーション手段をチャットに限定する」というものでした。

この新しい演習は、重要インフラ関連事業者を対象とした「シン・ワークショップ」（2017 年 9 月 12 ～ 13 日実施）としてお披露目されました。
“本社側” と “プラント側” の人たちは違うテーブルに分けて座らせた上で、直接対話することを禁止。互いの状況報告からターンごとの行動決定に至るコミュニケーションはすべて、一人一台ずつ用意した PC からチャットで行わせます。
さらに、演習における各自の役割を明確にして、どこの誰に確認をするべきかを真剣に考えられるようにするため、チャットの通信先にはあえて個人のアドレスしか選べないように制限しています。こうした工夫によってワークショップの内容はかつてないほどの深みを示し、最後のラップアップミーティングでは、参加者全員がゲームの順位など二の次にして、「KIPS “名工大バージョン”」による、リアルなシミュレーションの結果を、静かに噛み締めるような発言が続いていました。

「チャットのログを読み返してすぐに気付いたことは、“成績の良かったチームは、ポジティブな会話が多かった”ということです」

国立大学法人 名古屋工業大学
社会工学専攻
経営システム分野
越島研究室
土屋 旭弘 氏

展望

こうして好評のうちに幕を閉じたシン・ワークショップのチャット内容はすべて記録されており、越島研究室の学生たちの手で解析されています。
その中には、成績の良かったチームと、悪かったチームの「違い」が明確に表れていたと、今回の演習形式を提案した学生の一人である土屋 旭弘 氏は説明します。
「チャットのログを読み返してすぐに気付いたことは、“成績の良かったチームは、ポジティブな会話が多かった”ということです。反対に、成績の悪かったチームは、すぐに『すみません』と謝る発言が多かったのです」

越島教授も、「これだけでも、大きな発見だった」と声を揃えます。
「ポジティブなチームは、先に共有すべき情報などの指針をサッと決めて、次に取るべきアクションを明確にしていました。そのため、『次はこうしてみましょうか』『いい線いってますね』といった、ポジティブな言葉が自然と出てきます。一方、目の前の状況を追うだけで精いっぱいなチームでは、お互いにすぐ『すみません』と謝ってしまう状況が頻発し、最終的には全員が“単なる作業者”と化していたのです」

こうした行動の違いをさらに研究していくことで、より実践的なセキュリティ人材育成が実現していくことでしょう。越島教授は、「私たちの取り組みは、新たな MBA コースを作ることに似ている」と話します。
「サイバー攻撃への備えといえども、最後には現場を支える“人の力”に頼る必要があります。決して、サイバー空間だけで完結することはありません。そのためには、『どういう頼り方をすれば、相手が動いてくれるのか』を理解する必要があります。また、人を動かすためには、相応の準備が必要であることも理解しておかなければなりません。さらに言えば、資格をひとつ取得すれば終わり……ということではなく、進化し続けるサイバー攻撃にも柔軟に対応できるように、“論理的に考え、理解していく能力”を高めていくことができる教育を、今後も変わらず目指していきたい。今回のシン・ワークショップを経験したことで、カスペルスキーにお願いしたい、KIPS の改良点も見えてきました。これからのパートナーシップにも、大いに期待しています」

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

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