第4期中核人材育成プログラム

IMANE-CARD、PC機能改善

◆背景・課題

現在、企業に対するセキュリティの脅威の実情に目を向けると、特に従業員（個人）をターゲットにした脅威が増加しています。そのため、従業員が能動的に取り組むことができて、高い教育効果が見込まれるセキュリティ教育を提供できるかが課題になっています。そこで、**アクティブラーニング形式で従業員向けのセキュリティ教育を提供できる演習教材『IMANEシリーズ』[*1]をより使いやすく改善**することにしました。

『IMANEシリーズ』とは、名古屋工業大学　橋本芳宏教授の研究室で開発された演習教材で、中核人材育成プログラムの中でもOTインシデント対応・BCP[*2]を学ぶ演習で使用されています。シリーズの中の「IMANE-CARD」はカードを並べるグループワークで、インシデント時に求められる組織間連携を議論しながら考察する演習が可能です。また「IMANE-PC」では、PCゲーム形式でインシデント発生時の対応をシミュレーションできるとともに、プレーヤーの行動内容などが可視化されるので、具体的な行動をもとに振り返って学ぶことができます。

*1 Incident MANagement Exercise
*2 Business continuity planning 事業継続計画

- **IMANEシリーズ**
  サイバーインシデント発生時の対応方法がシミュレーションできる演習教材
  演習用シナリオを入れ替える事によって様々なインシデントへ対応が可能
  - **IMANE-CARD**
    インシデント発生時の企業としての対応の流れを「アクションカード」を並べることによって俯瞰して見ることができる
  - **IMANE-PC**
    PCのブラウザを用いた演習教材
    インシデント発生時の組織間連携をシミュレーションできる
  - **IMANE-DRAW**
    PC用のシナリオを作成するソフトウェア
    Draw-IOとExcelマクロを組み合わせてシナリオデータを作成する

IMANEシリーズ 全容

◆課題解決・成果物

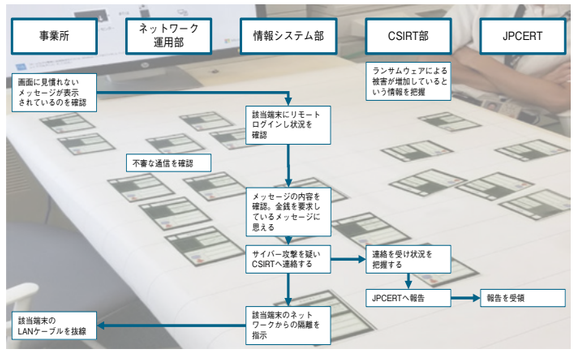
1. ファシリテーター向けマニュアル

企業内の研修でIMANE-CARD、PCを用いて、**誰が講師役になっても効果的な進行ができるように、マニュアルを作成**しました。作成にあたっては、参加者同士で活発に議論をしたり、振り返りをできるように、演習を進める側と参加する側の両者の目線に立って内容を検討しました。特に演習後の振り返りにおいて、どのような議論をすれば参加者の考えが深まるかを検討し、進め方の具体例を挙げて解説しています。

2. IT企業向けの新シナリオ作成と機能追加

IMANE-CARDにて、**事業所にあるPCがランサムウェアに感染するインシデントが発生した際の対応を学べるシナリオを作成**しました。そのために改めてインシデント発生時に取るべき行動を見直し、演習可能な形に落とし込みました。

また、より効果的な演習にするには対応方法をテンプレート的に覚えてしまうのではなく、臨機応変に行動できるようになることが重要と考え、**行動の背景にあるリスクの可能性についても考えて進められるように、IMANE-CARDに新たな機能を考案し、実装**しました。従業員個々のセキュリティ脅威への対応力向上に向けて活用されることが期待されます。



シナリオの例　インシデント発生時の対処法を学ぶことができます

修了者インタビュー

株式会社NHKテクノロジーズ
牛山 卓也さん

◆一番の収穫は？

インシデントへの適切な対応について、完璧な正解はないですが、例えば避難訓練と同じようにシミュレーションしておくことはとても大事だと実感できました。また、今回は初めて教材を作る側に立ったことで、現場を含めて社内のセキュリティ意識を高めていくことの重要性や方法論について、IMANEシリーズに限らず、より広い視野を持てるようになりました。

◆成果物の活用法

セキュリティの研修で使われるように自社内で提案していきたいです。また、他の企業でも使用してもらい、社会全体のセキュリティ意識の向上に貢献できたら素晴らしいと思っています。

◆ここがICSCoEならでは！

本プロジェクトは4期生としては私一人で取り組んだものでした。しかし実際には名古屋工業大学の橋本先生の研究室の皆さんと協力して進められました。普段働いているとなかなか接することのないアカデミックな世界の方々と接することで、知識を得るとともにさまざまな刺激を受けることができました。

IPA 独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan
〒113-6591 東京都文京区本駒込 2-28-8
文京グリーンコート センターオフィス17F
TEL 03-5978-7554　FAX 03-5978-7513

IPA Better Life with IT
ICSCoE Industrial Cyber Security Center of Excellence
ICSCoE REPORT
令和3年8月31日
vol. 10
ICSCoE ReportはICSCoEの活動を皆様にご紹介する広報誌です。

第4期中核人材育成プログラム 修了

2021年6月、第4期中核人材育成プログラムの修了式が執り行われました。今年は新型コロナウイルス感染防止対策を十分に実施したうえで外部会場にて開催し、派遣元企業の方々にもご参列いただき、修了者の1年間の成長を感じていただく機会になりました。

式典では、梶山弘志経済産業大臣から修了者に向けてのビデオメッセージが上映される一幕もありました。梶山大臣は、ビデオメッセージの中で、修了者に対し、「デジタル社会における力を持った守護者であるということを自覚し、日本社会全体のセキュリティを担う存在としてご活躍いただきたい」と激励の言葉を贈られました。

梶山大臣からのビデオメッセージによる激励

ICSCoE 遠藤センター長（左）から修了証書を授与される秋間 和兵さん（右）（J-POWERテレコミュニケーションサービス株式会社）

修了者代表挨拶

日本製鉄株式会社
玉田 耀さん

本日は、修了者代表として皆さまにお話したいことが3点ございます。

1点目は、コロナ禍でも研修に参加できたことへの感謝です。実機でしか学べない、手を動かす実践的なカリキュラムを続けられるように尽力してくださった関係者の皆さまに感謝申し上げます。

また、1~3期生は海外に出向いての演習がありましたが、4期では全てリモートでの開催となりました。ただ、リモートだからこそ、海外の方の講演を聴きながら、わからない単語をその場で調べて理解も深まり、質問もしやすかったという利点がありました。ハンズオンの演習では、海外の演習環境とオンラインでつながっていたため、何度も反復学習して理解度を高めることができました。日本にいながら、海外演習についても充実した学びを得ることができました。

2点目は、受講者同士のコミュニケーションについてです。カリキュラムではグループワークが多く、情報系・制御系出身のメンバーがお互いの得意、不得意分野を埋めながら課題に取り組みました。多種多様な業界の受講者が集まっていたことで、知見を集めて成果を出すことができました。また、グループワークを通して親睦を深められ、業界や年齢に関係なく、プライベートから業務の話まで、何でも話し合える仲間を得ることができました。

3点目は、今後の抱負です。1年前の開講式当時、私自身はセキュリティに関する知識がほぼ有りませんでした。

しかし、今では知識がついてきて、このメンバーともっと勉強したい、修了したくない！という気持ちも、本音ではあります。一方で、帰社してからセキュリティ対策としてやりたいこと、やらねばならないと思えることが、たくさん出てきました。ここにいる4期生はみな同じ気持ちだと思います。そんな私たち4期生には、ICSCoEの先輩方・講師の皆様、有識者の方々とのつながりがあります。これほど心強いものはありません。このメンバーで業界だけにとどまらず、社会インフラ・産業基盤のサイバーセキュリティ対策の強化を目指し、強い使命感を持って、帰社後の業務に取り組んでまいります。1年間、本当にありがとうございました。

卒業プロジェクト特集

46名の受講者が、15のプロジェクトに取り組みました。取り組みの一部を2号に渡って紹介します。

サプライチェーン末端までのセキュリティレベル向上

背景・課題

現在、事業を進めるためには自社（発注者側）だけでなく、取引先や関連会社、グループ会社など（受注者側）を含めたサプライチェーン全体のセキュリティ対策を考える必要に迫られています。本プロジェクトは「サプライチェーン全体のセキュリティレベルの向上」という目的のもと発足しました。

まずは、課題抽出のために、サプライチェーンに対するガイドラインや国の施策、中小企業を支援する制度を調べるなど勉強会を行いました。次に、中小企業のセキュリティ対策の実情を知るために、公的機関、大学、企業グループ、支援機関、中小企業の5つのカテゴリーで合計15団体へヒアリングを行いました。その結果、7項目の課題が抽出されました。

1. セキュリティ意識の向上
2. 中小企業のセキュリティインシデント事例の集約と発信
3. セキュリティ対策の見える化
4. 支援機関のセキュリティ勉強の負担軽減
5. セキュリティ専門家の活用
6. セキュリティ対策のメリット
7. 大企業（発注企業）の宣言

課題解決・成果物

課題を解決するために商工会議所の会報誌での執筆を行うとともに、サプライチェーンサイバーセキュリティ対策評価フレームワークを作成しました。

1. 商工会議所の会報誌での執筆

「中小企業のセキュリティ意識　ゼロから0.1に！」を目的にして、中小企業数の多い大阪、札幌、名古屋の商工会議所にそれぞれの地域の中小企業におけるセキュリティ対策の実態をヒアリングしました。そして**会報誌の読者である企業が抱える課題に則して、わかりやすい表現でセキュリティに関するコラムを執筆し、掲載を実現**しました。この活動によって中小企業のセキュリティ意識の向上への貢献が期待されます。


大商ニュース　令和3年(2021年)7月10日　土曜日　(4)

あなたの会社を守る <2>

サイバーセキュリティの第一歩
「守りたい資産を見つける」

八木 晴信

大阪商工会議所の会報誌「大商ニュース」（2021年7月10日号）への掲載


専門家からの助言者

やってみましょう！セキュリティアクション！

村上 幸司

セキュリティ対策、何からやればいいの？

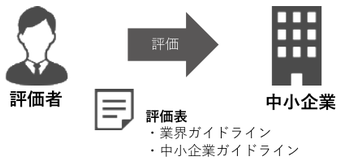
札幌商工会議所の会報誌「さっぽろ経済」（2021年7月号）への掲載

▶大阪商工会議所HP「大商ニュース」
https://www.osaka.cci.or.jp/index3-07.html

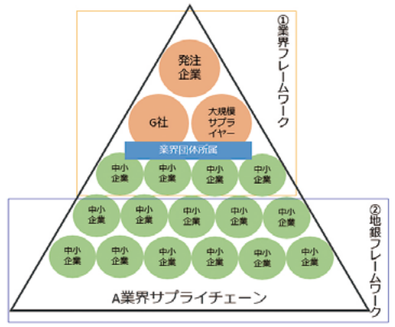
▶札幌商工会議所HP「さっぽろ経済」
https://www.sapporo-cci.or.jp/web/public/index.html

2. サプライチェーンサイバーセキュリティ対策評価フレームワーク

中小企業のセキュリティ対策の状況を、評価表を使って第三者が評価し、その結果を中小企業との取引時に使用する枠組みを作成しました。



フレームワークの種類は2つあり、ひとつは各業界共通のガイドラインで企業の対策状況を評価する「業界フレームワーク」です。発注者が中小企業の信用度を調査するために使用することを想定しています。次に、中小企業にとっての身近な相談相手である地方銀行（以降、地銀）が、企業の対策状況を評価する「地銀フレームワーク」です。評価には中小企業向けに作られたガイドラインを使用します。その評価結果は地銀の与信審査として使用されることを想定しています。作成したフレームワークは実際に経済産業省や金融業界に紹介され前向きなフィードバックを得ることができました。



フレームワークの全容

また今回のプロジェクトメンバーは修了者コミュニティ「叶会」において「サプライチェーンサイバーセキュリティ対策部会」を発足しました。修了者のつながりを活用して、引き続きフレームワークの推進と、中小企業のセキュリティ意識向上を目的とした活動を継続させていく予定です。

卒業プロジェクトの成果を発表


持ち運び可能な模擬プラントによるデモンストレーション

修了式に引き続き、同会場で卒業プロジェクトの成果発表が4件行われました。現場のセキュリティ意識向上を目的として、スーツケースに格納して持ち運び可能な模擬プラントを作成したプロジェクトでは、実際に会場でその模擬プラントを組み立て、正常稼働する様子や教育シナリオのデモンストレーションを披露しました。また、ドローンのセキュリティについて調査し、対策をまとめたプロジェクトでは、会場でドローンを飛ばして模擬攻撃を実演しながら、脆弱性や対策について調査結果を発表しました。

臨場感あふれる発表となり、修了者を派遣された企業の方々や来賓の方々に、1年間の成長をアピールすることができました。


テントの中でドローンを飛行させて模擬攻撃を実演

修了者インタビュー

左から
日本電気株式会社　**江村 勇紀さん**
東海旅客鉄道株式会社　**八木 晴信さん**（サブリーダー）
北海道電力株式会社　**村上 幸司さん**（リーダー）
電源開発株式会社　**河谷 浩司さん**

リーダーの村上さんに伺いました

一番の収穫は？

サプライチェーンのサイバーセキュリティを考える上で視野が広がったところですね。様々な立場の方々の話を聞けたことで、発注者だけでなく、受注者の目線でも考えられるようになりました。

成果物の活用法

私自身、帰社後もサプライチェーンにまつわる業務に携わる予定です。特に「業界フレームワーク」で定義した考え方は、これからサプライチェーンセキュリティの対策について検討していくうえでのベースとして活用できると思っています。

ここがICSCoEならでは！

経済産業省や地方の経済産業局、商工会議所など様々な企業・団体と短期間で即座に出会えて“活きた”話を聞かせてもらえたということがICSCoEでないと実現できなかったと思っています。