IPA Better Life with IT

ICSCoE Industrial Cyber Security Center of Excellence

ICSCoE REPORT

Industrial Cyber Security Center of Excellence

令和7年8月29日

vol. 22

ICSCoE ReportはICSCoEの活動を皆様にご紹介する広報誌です。

ASEAN諸国の実務者を対象に OTセキュリティトレーニングを実施

2025年7月21日から23日にかけて、「日 ASEAN サイバーセキュリティ能力構築センター（AJCCBC：ASEAN-Japan Cybersecurity Capacity Building Centre）」と連携し、タイ・バンコクにて、ASEAN 加盟国の政府関係機関やインフラ関連組織の実務者を対象とした「OT（Operational Technology）セキュリティトレーニング」を実施しました。

OTセキュリティトレーニング受講者およびICSCoE講師陣

サイバー・フィジカル融合が急速に進む現代社会において、OT 技術はエネルギー、水道、交通、製造など、社会基盤を支えるインフラの中核として、その重要性を増しています。一方で、それらを狙ったサイバー攻撃のリスクも高まっており、各国の現場担当者のスキル向上と、地域全体のセキュリティおよびレジリエンス強化が喫緊の課題となっています。

今回のトレーニングは、こうした背景を踏まえ、OT セキュリティに関する基礎知識から実践的なスキルまでを体系的に学ぶ機会として企画されました。

ASEAN 加盟国のタイ、フィリピン、ベトナム、インドネシア、マレーシア、ブルネイ、カンボジア、ラオスの8か国から集まった18名の参加者が、3日間にわたって講義と演習を通じて OT 環境に特有のリスクと対策を学びました。

初日は、ICSCoE 講師である奈良先端科学技術大学院大学 門林 雄基先生による基調講演が行われ、日本における OT セキュリティ人材育成の取り組みとその知見を紹介しました。続いて実施されたワークショップでは、仮想企業を題材にしたシナリオを用い、奈良先端科学技術大学院大学の門林先生・政策研究大学院大学の宮本 大輔先生、タイ・マヒドン大学の講師らの指導のもと、参加国・業界ごとの課題やベストプラクティスを参加者同士が共有し合い、活発な意見交換が行われました。

OT環境（水位・流量制御）模擬プラントを用いた攻撃デモ演習

2日目と3日目には、実際の OT 環境を模したツールやシナリオを用いたハンズオン演習が行われ、ICSCoE 講師の東洋大学 満永 拓邦先生、岡田 怜士先生、渡會 航生先生の指導のもと、参加者は攻撃デモやインシデント対応を体験しながら、実践的な知識と対応力を身につけました。

参加者からは、「ハンズオン演習など、非常に実践的で有意義だった」「他国の参加者とのディスカッションを通じて様々な視座が得られた」といった声が多く寄せられ、トレーニングの効果が高く評価されました。

「日ASEANサイバーセキュリティ能力構築センター」は、2018年に設立され、日本政府はASEAN事務局及びタイ政府とともに、地域のサイバーセキュリティ能力向上を目的としたトレーニングを継続的に展開しています。同センターでは、サイバー防御演習などの実践的なトレーニングを通じて、ASEAN 地域の人材育成と知見の共有を継続的に推進しています。

ICSCoE は、日本と深い経済的結びつきを持つ ASEAN 地域における OT セキュリティの強化と、持続可能な人材育成を支援すべく、継続的な能力構築支援と情報共有の取り組みを進めていく予定です。

「Interop Tokyo 2025」出展

業界を超えた「絆」が力に。現場で活躍するICSCoE修了者たち

2025年6月、「Interop Tokyo 2025」が開催され、IPA/ICSCoE のブースでは中核人材育成プログラムの修了者や講師によるプレゼンテーションが行われました。

金融業界全体のセキュリティ教育に貢献

「SECURITY ASSEMBLE- 研修は旅の始まりだった…!現場に戻った ICSCoE 3期生の奮闘記 -」と題した発表では、修了後5年間の活動を通じて「共助」の関係が築かれてきたことを4名が報告しました。

かんぽシステムソリューションズの田中 克享さんは現在、かんぽ生命の SOC 業務を担う SOC 室、および社内 CSIRT を担うサイバーセキュリティ室の立ち上げから中心的に活動し、教育と実務の両面で重要な役割を担っています。

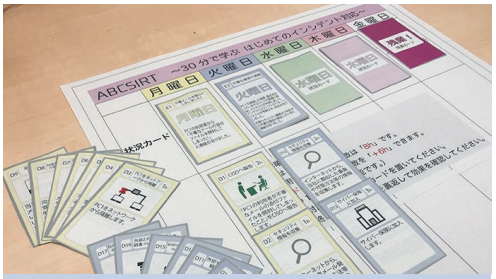
田中さんが紹介したのは、卒業プロジェクトで開発された「ABCSIRT」という教育ツールの金融業界での展開です。ABCSIRT は、セキュリティインシデント対応をカードゲーム形式で学べるツールで、架空の銀行を舞台に、限られた時間内でインシデント対応の優先順位を判断する実践的な内容となっています。

金融機関では突然の配置転換が珍しくない中、このツールは、専門知識がなくても業務のイメージを掴むのに役立ちます。金融ISACを通じて業界全体に展開され、その後5年間で標的型攻撃、DDoS、フィッシングなど、金融業界に親和性のある5つのシナリオを開発。2024年には「金融 ISAC アワード」を受賞しました。

田中さんは中核人材育成プログラムの日々を振り返り、「個人にとっても人材を派遣する企業にとっても、とてもよいプログラムだったと思います。特に鍛えられたのは、課題に対してすぐアウトプットを出すということ。この姿勢は今も意識しています。プログラムの説明で『OT（制御技術）と IT（情報技術）双方にわたる技術的なスキル』と謳っていることから、OT を持たない企業では“関係ないプログラムだ”と思われるかもしれませんが誤解です。OT の知識が生きる場面は出てきます」と語ります。

そして、「引き続き金融業界に貢献するのはもちろんですが、ICSCoE3期生だけでなく、他の期とも合流して、日本の重要インフラ業界全体の底上げに少しでも貢献できればと思います」という言葉からは、使命感がひしひしと伝わってきました。

かんぽシステムソリューションズ株式会社
田中 克享 さん（3期生）



CSIRTの業務をゲーム形式で体験・学習するツール。

目的
・インシデント発生時のCSIRTの活動を理解する。
・限られたリソースの中で対応を迫られる状況を体験する。

詳しくは▶ IPA ABCSIRT

卒業プロジェクトとして制作されたABCSIRT（エービーシーサート）

業界を超えた共助でASM導入の課題を解決

TOPPAN ホールディングスの坂田 尚さんは現在、ASM（Attack Surface Management、攻撃対象領域管理）、脅威インテリジェンス、工場セキュリティ、CERT を担当しています。

坂田さんの卒業プロジェクトは「サイバー脅威インテリジェンスの活用」でした。この知見を生かし、帰任後すぐに公開情報を収集・分析する OSINT（Open Source Intelligence）チームを結成して ASM 活動を開始。「セキュリティ経験2年目でプログラムに参加しましたが、すぐに実践できる基礎能力が身につきました」と語ります。さらに、「ICSCoE で得た一番大きな価値は『絆』。一年にわたる研修で人となりを知っているので、引き続きリアルな会話ができます」と強調します。

この絆が見て取れるのが、坂田さんがプレゼンで紹介した、ICSCoE 修了者の連携により実現した ASM の導入事例です。

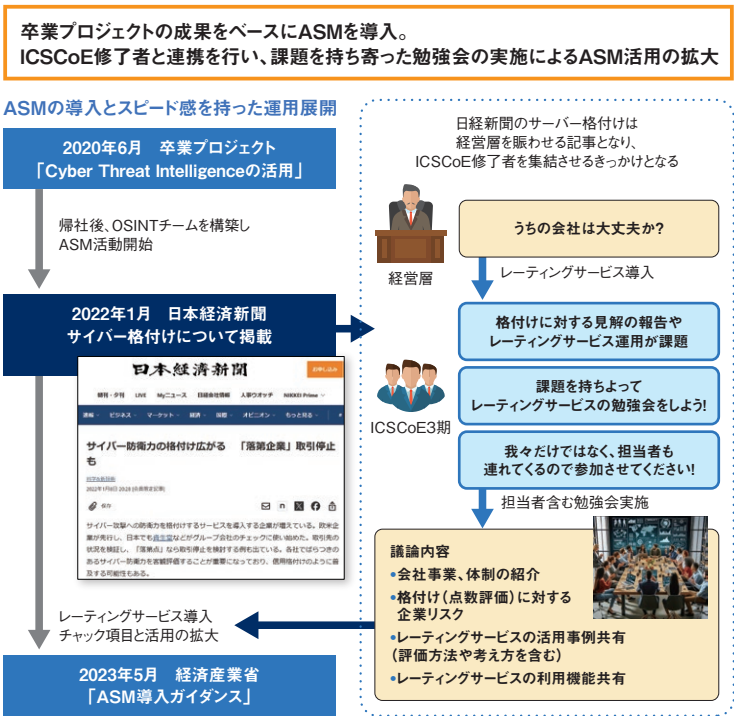
TOPPANホールディングス株式会社
坂田 尚 さん（3期生）

2022年、新聞報道をきっかけに、多くの企業がサイバーセキュリティの格付け対応に追われました。当時、「格付けに対する見解を経営層に報告しないといけない」、「レーティングサービスを導入したけれど、どう活用すればいいの?」という企業が多かったことから、坂田さんはICSCoEの同期生と共に勉強会を企画。業界を超えて修了者が集まり、さらに各社の担当者や上司も巻き込んで議論を重ねました。

「それぞれの知見を持ち寄ると、業界が違っても抱える課題は共通していることが分かり、解決策が見えてきました」と坂田さんは振り返ります。

この勉強会での知見をもとに、坂田さんはTOPPANグループでのASM活用を拡大。現在では、グループ264社のうちコーポレートドメインを管理している136社を対象に、年間を通じて是正指示・支援を行っています。また、個人情報や経済安保法で規定された機密情報を扱う委託先には、ASMと監査による認定制度を導入しました。

現在、業界横断の勉強会がさまざまなテーマで行われ、ICSCoEの期や業界を超えて協力し、課題の解決を図っています。



研修成果と修了者連携とASM導入

OTセキュリティ人材を全国各地に広げる「可搬型模擬プラント」を開発

ICSCoE中核人材育成プログラムの設立当初から、制御システムのセキュリティ演習を指導してきた講師の目黒 有輝さん。株式会社トインクスで制御システムに対するペネトレーションテストやリスクアセスメント、セキュリティトレーニングに従事する実務家でもあり、「攻撃者の視点でリスクを見つける」という実践的な教育方針のもと、多くの修了者を送り出してきました。

ICSCoEでは中核人材育成以外のプログラムも提供しており、東京・秋葉原にある模擬プラントを活用した、制御システムに対するサイバーセキュリティ演習も実施。ただ、東京から遠い地域の企業にとっては負担が大きく、多数のセキュリティ人材を育成したくても二の足を踏むことがありました。

そこで、目黒さんが今回紹介したのは、「可搬型模擬プラント」という、全国各地でOTセキュリティの演習を可能にする新たな教育ツールです。

モデルとしたのは、2基の発電機（各2,500kW）を持つ発電所。標準的なサーバーラックサイズではあるものの、PLCなどの実機が収められ、機能面では既存の模擬プラントと同等以上の性能を実現しました。

演習シナリオは、実際に起きた攻撃事例をもとにした12種類を用意。制御システムの脆弱性を狙って停電を引き起こす過程や、システムの改ざん手法などを、実機による演習を通して理解し、防御側として何をすべきかを実感を持って学べます。2025年3月に名古屋市の企業で実施された演習では、参加者から「こんなに簡単にハッキングできてしまうことが分かり、攻撃者側の視点からも知見が得られました」、「実機を使うことで、より現実味を帯びた演習を行うことができました」といった声が上がったそうです。

この可搬型模擬プラントの実機は、2025年3月にIPAとして初めて公開したばかり。目黒さんは、「このような東京から離れた地域で活用いただけるようなリソースがあることを、ぜひ知っていただきたいです」と呼びかけました。

今後、トレーニングにおけるブルーチーム（防御側）向けの攻撃検知・ログ分析訓練、レッドチーム（攻撃側）向けのペネトレーションテスト技術習得、パープルチーム（攻撃と防御の両面）での実践的な攻防演習、さらには管理職・現場作業員向けの脅威体験など、多彩なユースケースでの活用を構想しています。


独立行政法人情報処理推進機構
産業サイバーセキュリティセンター
目黒 有輝さん


可搬型模擬プラント

第8期中核人材育成プログラム修了式

2025年6月、第8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。57名が一年間のプログラムを修了し、産業サイバーセキュリティエキスパートとして新たな一歩を踏み出しました。

修了者代表挨拶

> 「一番大きかった存在は、
> この一年間を共に過ごした受講者同士のつながりです。
> サイバーセキュリティは、一人ではできない
> ということを一年間通して学びました。」

名古屋鉄道株式会社
朝倉 大智 さん

私たち8期生57名が修了式を無事に迎えることができたのは、先生方、講師の皆様、事務局の皆様、経済産業省様、各派遣元企業の皆様の支えがあったからです。心より感謝申し上げます。

この一年間を振り返りますと、改めて濃密な時間であったと感じます。一年前の開講式の中で、いただいたお言葉の中に、「プログラム修了後は、産業サイバーセキュリティエキスパートとして様々な場面で力を必要とされる人財であり、派遣元企業のみならず、産業会全体、日本全体、さらにはグローバルを舞台に活躍される人財になられることを心から願っている」と力強い激励をいただきました。私は楽しみな半面、自分がそのような人財になれるだろうかという不安半面であったことを思い出します。

受講者の中には、セキュリティの経験の浅い方もおりましたが、基礎演習から実践演習、国際派遣演習などを通してより中核人材として求められる知識と技術を身につけることができました。4月からは自社の課題、講義や演習を通じて見つけた課題をテーマとして研究する卒業プロジェクトに取り組んでまいりました。トレンドである、生成AIやDX化などをテーマとするプロジェクトや、生成AIを使って壁打ちを繰り返しイラストや文章、動画等を作成し、うまくプロジェクトの成果物に反映させているプロジェクトなどがあり、無事に成果を残すことができました。

このプログラムに参加する中で先生方・講師の方が、受講者の学びたい熱意をくみ取ってくださり、熱心に応えてくださいました。また、必要とあれば外部の有識者や関係者との打ち合わせを設定してくださいました。

一番大きかった存在は、この一年間を共に過ごした受講者同士のつながりです。幅広い世代や企業界の垣根を越えて深く議論できたことは貴重な経験になりました。これからもこの関係を大事にしていきたいです。

サイバーセキュリティは、一人ではできないということを一年間通して学びました。このプログラムを通じて出会った仲間とともに産業界の発展をサイバーセキュリティの面から支えていきます。また、この一年間学んだことを派遣元企業に持ち帰り、帰社後の業務に取り組んでいきます。ありがとうございました。

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