IPA Better Life with IT

ICSCoE REPORT

Industrial Cyber Security Center of Excellence

令和2年12月11日

vol. 07

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　開講

2020年7月、産業サイバーセキュリティセンター（ICSCoE）において、第4期中核人材育成プログラムの開講式が執り行われ、今後の日本における社会インフラのサイバーセキュリティを担うことが期待される47名の受講者を新たに迎えました。

メッセージを贈る遠藤センター長

今年度は新型コロナウイルス感染症（COVID-19）の流行がある中で、参加者はマスク着用の徹底、座席間隔の確保、演台へのアクリル板の設置など、感染防止対策を行ったうえでの開催となりました。

IPA 富田理事長は、コロナ禍の状況でも各々がミッションを自覚し、目標を立てて主体的に取り組むことで充実した一年を過ごしてほしいと強調しました。

産業サイバーセキュリティセンターの遠藤センター長は、社会が「情報化社会」から「データ社会」へ移ろうとしており、データを扱う上でのセキュリティの重要性が増していることに触れました。その中で、この一年を通して「強い意志をもって企業全体、業界、更には国をけん引するトップクラスのリーダーを目指していただきたい」と語り掛けました。

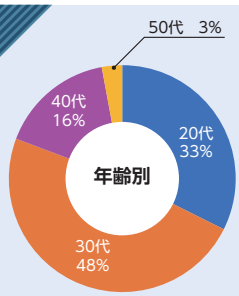
受講者同士の自己紹介の様子

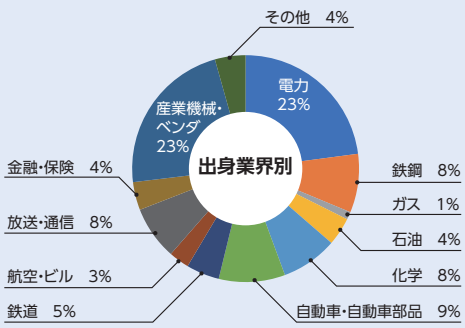
来賓の経済産業省商務情報政策局長の西山圭太氏（当時）は、新たな出会いの中で、知識を学ぶだけでなく、これまでの会社人生で作り上げてきた考えを一度壊し、新しく組み立てなおす機会にしてほしいと激励されました。

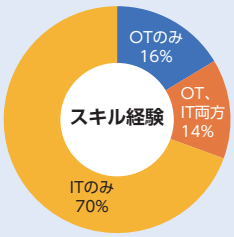
式典の後は講師の紹介や、受講者同士の自己紹介を行うなど、これから一年に渡る学びに向けてスタートを切りました。

中核人材育成プログラム 参加実績

第1期～第4期 合計







第3期中核人材育成プログラムが修了しました

第3期中核人材育成プログラム修了式（2020年6月）

2020年6月、第3期中核人材育成プログラム修了式が執り行われました。修了式では梶山弘志経済産業大臣から修了者へ宛てられたビデオメッセージが届き、「日本社会全体のセキュリティを担う中核人材として社会の各方面でご活躍していただきたい」と激励の言葉が贈られました。修了者からは、東海旅客鉄道株式会社の安藤聡さんが代表してこれまでを振り返り、新たな決意を力強く述べられました。

修了者代表 挨拶

東海旅客鉄道株式会社
安藤 聡さん

修了者代表として3つお話したいことがあります。

まず1つ目が、修了式を迎えられたことへの感謝です。新型コロナウイルスの感染拡大を受けて、緊急事態宣言が出てからは完全にリモートでの受講となり、修了できるのか不安もありました。そのような中で、無事に本日を迎えられたのは、継続のために尽力いただいた方々のおかげです。心から感謝申し上げます。

2つ目はこの1年の振り返りです。1年前の開講式を思い出すと、とても心細かった記憶があります。日本の重要インフラをサイバーセキュリティの面から支える人材になってほしいと言われ、本当にそうなれるのか不安でした。周りを見渡してもみんな硬い表情をしており、それが不安に拍車をかけました。それから1年です。この場にいる全員が卒業プロジェクトで優れた成果を出し、中核人材として活躍できる能力を証明しています。

振り返るとまずは素晴らしい教育プログラムがありました。経験が浅くともステップを踏んで学ぶことができました。また実際の現場に近い環境で、「手を動かす」実践演習にみっちりと取り組みました。一方で、経営層と現場層をつなぐ中核人材として必要なソフトスキルについても学びました。さらに国際事例演習では、日本だけに目を向けていることの視野の狭さを知ることができました。

また、講師の方々が、受講者の学びたい気持ちに熱意を持って応えてくれるところがありがたく感じました。もっと知りたいという受講者がいれば、外部有識者による特別講義をセッティングしてくださったり、ご自身で時間外に講義をしてくださったりしました。とことん付き合ってくれる姿勢がとても頼もしかったです。

そして、一番大きかったのは受講者同士の関わりです。様々な業界から個性豊かな69人が集まりました。日中はカリキュラム内で議論を重ねて切磋琢磨し、業務時間後はフットサルなどで懇親を深めてきました。リモートワークになった際も、コミュニケーションを取り続け、最終的に卒業プロジェクトを完成させることもできました。学びになる、刺激になる、そして頼れる仲間たちに囲まれて、1年を過ごせたことが本当に幸せでした。

さて最後の3つ目は、これからに向けた決意です。我々が帰る先には大変過酷な状況が待っていると言えます。ですが、我々3期生は69人の仲間がいます。さらには1、2期生の150人を超える先輩たち、そして講師の先生方をはじめとする有識者との繋がりもあります。これらの仲間たちとであれば、どのような状況にも立ち向かっていけると信じています。日本の重要インフラをサイバーセキュリティの面から支えるという使命感を持って、帰社後の業務に取り組んでいきます。本当にありがとうございました。

梶山弘志経済産業大臣からのビデオメッセージ

第3期生 卒業プロジェクトのご紹介

全25のプロジェクトの中から一部をご紹介します。

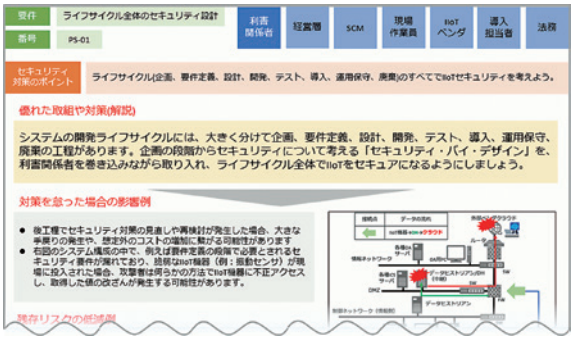
1 IIoTを導入する際のセキュリティ

製造業におけるDX（Digital Transformation）への取り組みの一環として、工場内への産業用途でのIoT（IIoT：Industrial Internet of Things）の導入や活用が期待されています。一方、工場内システムには工場外ネットワークへの接続を前提とせず設計されたものもあり、IIoT導入時のセキュリティ検討が重要な課題の一つになっています。

そこで本プロジェクトでは、IIoT導入時のセキュリティ検討に焦点を当て、新規導入時の業務フローとセキュリティ対策ガイドラインの解説書を作成しました。

無線通信や電池での稼働が可能なIIoT機器は、大掛かりな工事を伴わずに設置可能なものもあり、セキュリティ検討での見落としが生じることも考えられるため、早い段階で導入担当者からセキュリティ担当者へ相談が来るように業務フローを整理しました。

また解説書では、ENISA発行の「スマートマニュファクチャリングにおけるIoTセキュリティのグッドプラクティス」に記載のセキュリティ対策を分かりやすく説明するだけでなく、連携が必要な利害関係者の例示、対策を怠った場合の影響を追加するなど、リスクを具体的に検討して対策を推進できるようにしました。



担当者から

本プロジェクトは、「IIoTセキュリティのガイドラインを読むだけでは、リスク分析を上手く進められなかった」「視点が異なるガイドラインが複数あり、一括で読むのは困難だった」「自社導入時の土台となるものをまとめたい」という課題意識から始まりました。ICSCoEでの学びを生かし、作成した解説書を自社のビジネスに合わせて活用することで、セキュリティ担当者として貢献したいと考えています。

2 制御システムにおける資産管理の効率化

IoTの普及やDXの進展に伴い、生産性向上のため製造現場の制御システムを情報ネットワークへ接続する機会が増加しています。このような製造現場においてサイバーセキュリティリスクを最小化するには、ISO31000で定義されている「組織の状況の確定」、すなわちリスクマネジメントにおける資産管理(保護資産の明確化)が必須となります。しかし、制御システムにおける資産管理について具体的な方法と課題に触れているガイドラインは見受けられず、また製造現場での資産管理は、手作業が多いことやサイバーセキュリティの観点が含まれていないといった課題があります。

本プロジェクトでは、制御システムにおける資産管理の必要性や方向性を示すガイドライン、具体的活動を促す手引き書やチェックリストをまとめ、組織のサイバーセキュリティ向上に貢献することを目指しました。またネットワーク接続されている機器を把握・可視化するツールも作成し、資産管理自動化の有効性を検証しました。

なお、本プロジェクトの成果物である「制御システムにおける資産管理ガイドライン」「制御システムにおける資産管理チェックリスト」および「制御システムにおける資産管理ガイドラインの活用の手引き」は、産業サイバーセキュリティセンターのWebサイトでご紹介しています。また上記ツールも外部サイトで公開されています。

〈産業サイバーセキュリティセンター　中核人材育成プログラム 卒業プロジェクト 紹介ページ〉
https://www.ipa.go.jp/icscoe/program/core_human_resource/final_project.html

担当者から

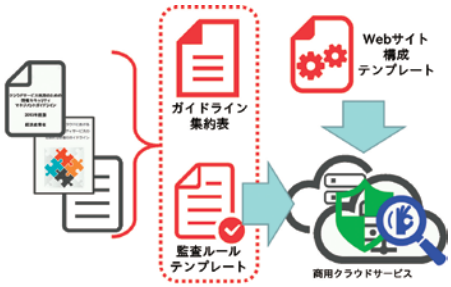
本プロジェクトの成果であるガイドラインやツールが、制御システムにおける資産管理の重要性に気づく、あるいは資産管理を実践するきっかけになれば幸いです。また、作成したツールの有効性検証には、模擬プラント環境を利用しました。こういった検証作業ができることも、ICSCoEでの学びならではだと思います。

3 クラウドセキュリティガイドライン

DXの基幹技術であるクラウドについては、国内外で様々なセキュリティガイドラインが公開されており、利用を推進する企業も増えています。一方、「それぞれのガイドラインの指針や活用対象者が異なっている」、「社内のセキュリティポリシーにおいて統一的な指針が未整備あるいは周知が不充分」といった課題が見られます。

そこで、「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」(2013年度版 発行：経済産業省)をベースに、「クラウドにおけるセキュリティサービスの効果的な管理のガイドライン」(発行：日本クラウドセキュリティアライアンス)の内容と、AWSやAzureといった商用クラウドサービスの監査ルールをマッピングし、「ガイドライン集約表」を作成しました。本表は、利用者目線で定量的に判断できる内容を選別して集約しており、各ガイドラインやルールの記載内容を併せて確認できるようになっています。さらに、各クラウドサービスにおいてセキュアなWebサイトを自動構築可能とする「Webサイト構成テンプレート」、及び各クラウドサービスが備えている監査機能を利用してガイドラインに則ったルールの自動設定を可能とする「監査ルールテンプレート」を作成しました。

これらの成果物は、修了者、受講者及び派遣元企業で利用可能であり、企業が利用するクラウド環境のセキュリティレベル向上が期待されます。



担当者から

本プロジェクトでは、ガイドラインの集約にとどまらず、AWSやAzureで活用いただけるテンプレートを併せて作成できたことで、セキュアなクラウド環境利用の土台作りに貢献できたと考えています。また各クラウドサービスはいずれも日々進化しており、「これだけやれば問題ない」という考えは通用しないため、利用者として変化に順応していく必要性も実感しました。

4 OT ATTACK

セキュリティ担当者として、「自社製品や導入する製品に対する高度なペネトレーションテストを実施できるようになりたい」、「自社のプラントをどのように守るかについて、具体的に提案するスキルを身に着けたい」という思いから本プロジェクトがスタートしました。

そのためにまず、セキュリティ製品やネットワーク製品についてのDoSテストの手法を整理し、ペネトレーションテストツールを作成しました。さらに作成したツールで実製品へペネトレーションテストを実施してツールの有効性を確認するとともに、リスクの回避策や改善策を検討しました。作成したツールと習得したスキルを組み合わせて活用し、帰任後は自社製品や導入する製品の頑健性評価や対策提案ができることが期待されます。

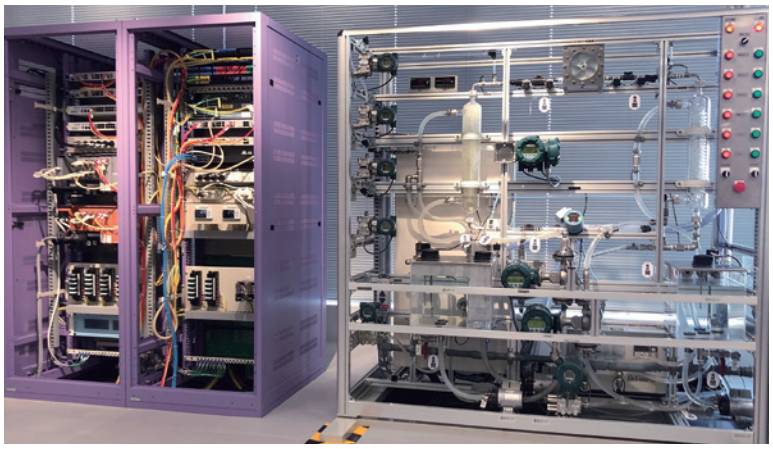
また模擬プラントを題材に、プラントごとに想定される脅威を洗い出し、攻撃シナリオ案を作成しました。作成した攻撃シナリオ案から防御手法を整理して実装し、SOARの基本的な考えに基づいて対策の自動化を検討しました。これらの活動を通じて身に付けた防御手法を提言するスキルや、対策自動化の基本的な考え方によって、プラントのセキュリティの向上に寄与できることが望まれます。

担当者から

ICSCoEで高度なペネトレーションテスト手法を学ぶ中で、自社製品や自社で導入する製品に対しても高度なペネトレーションテストが必要ではないかと考えるようになりました。本プロジェクトで作成したツールを用いて自社内でテストし、その結果に基づいて対策を講じることで、今まで以上に製品の頑健性の向上に貢献が出来るのではと考えています。

産業サイバーセキュリティセンター（ICSCoE）に新たなプラント「熱資源活用制御システム」を構築

ICSCoEでは、秋葉原UDXに新たな演習装置として、液体や気体などの流体を一元的に制御するPA（Process Automation）プラントを構築しました。「**熱資源活用制御システム**」と名付けられた新たなプラントは、システムを構成する要素それぞれがフィードバックを行いながら制御を行う**分散制御システム**（**DCS**：Distributed Control System）となっており、今後の演習の幅がさらに広がることとなります。以下では新プラントの概要、意義についてQ&A形式でご紹介いたします。



温度差発電プラント

Q1 なぜ「熱資源活用制御システム」なのか？

PAプラントの導入は、ICSCoE設立当初からずっと検討し続けてきました。しかしながらオフィスビルに危険な薬品を使用する化学プラントを設置することはできません。設置可能でPA制御の演習が実現できるシステムを考えたとき、答えとして挙がったものが「水の加熱・冷却・撹拌」の制御を行う「熱資源活用制御システム」でした。

Q2 どのようなシステムなのか？

2つの異なる機能を持つプラントと、それらを統括して制御するシステムで構成されています。

まず、「**温度差発電プラント**」では水より沸点の低い物質を、温水の熱で気体化させることでタービンを回して発電します。また、気体化した物質を冷水で冷やして液体に戻し、再び発電に利用しています。

次に、「**熱資源循環プラント**」は定められた水質、温度にて温水を循環させるプラントになっています。温水の濁度やpH、塩素濃度などを計測し、それに応じて薬品の混合・撹拌を行うなど水質を一体的に制御できるようになっています。また、昇温機の稼働や、冷却水や温水の注入により、定められた温度になるように制御しています。

さらに、「**熱資源活用制御システム**」が上記2つのプラントをつなぎ、温水（熱資源）を受け渡しするなど、全体を連続的かつ自動的に制御しています。

熱資源循環プラント

Q3 演習の範囲はどのように広がるのか？

電力、ガス、石油、化学等の各分野を対象に、DCSを用いた総合的な制御の演習が可能になります。特に、流体を扱う制御の演習が、机上演習ではなく、物理的に装置として実施できるようになります。

Q4 この新たなプラントを用いた演習の意義は？

DCSは産業の様々な分野で使われていますが、ひとたびサイバー攻撃を受けると甚大な被害となる大きなリスクを抱えています。この新たなプラントを用いた演習を通じて対策を学ぶことができるようになることは、日本の社会インフラ・産業基盤における防護力の強化にとって大変意義のあることだと考えています。

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