世界初800GbE相互接続伝送実証実験の動態展示を実施

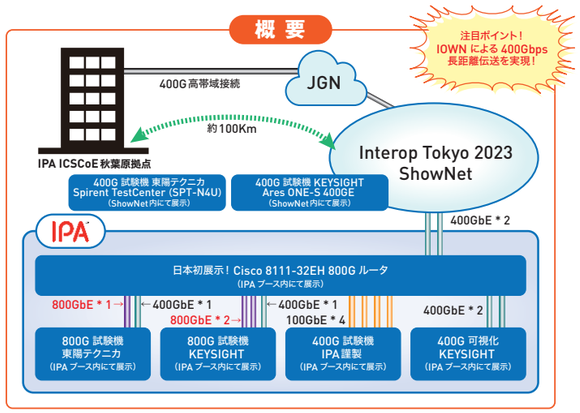
Interop Tokyo 2023のIPAブース内において、複数メーカーの800GbE対応機器を組み合わせた世界初となる相互接続・伝送実証実験の動態展示を実施しました。

本実験はICSCoEが中心となり「シスコシステムズ合同会社」（Cisco 8111-32EHを提供）「Keysight Technologies, inc.」（Keysight AresONE 800G を提供）「Spirent Communications, inc.」「株式会社東陽テクニカ」（Spirent B2 800Gイーサ アプライアンス を提供）（アルファベット順）の協力のもと、各社がリリースまたは開発中となる最新の800GbE対応機器をIPAブースに集結することで、まさにInteropともいえる相互接続性の確認及びセキュリティの観点を踏まえた評価検証を実現することができました。

またICSCoE秋葉原拠点と幕張メッセのIPAブース間を、NTTグループが取り組むIOWN*の400G対応実証ネットワークを活用し、ShowNetを経由して400Gで接続しました。その接続性を活かし、ICSCoEが独自に開発したトラフィック生成装置による400Gbpsトラフィックの生成及び制御を行うセキュリティ実験を実施いたしました。IOWNの400Gの公開実証は初めての試みであり、NTTが提唱するAPN（All-Photonics Network）への取り組みにも貢献しています。
*IOWN: Innovative Optical and Wireless Network

さらにICSCoEは「Keysight Technologies, inc.」および「Spirent Communications, inc./株式会社東陽テクニカ」が実施するブース関連系実験についても協力をしました。ShowNetのネットワーク上に設置された各社の装置（Keysight AresONE 400G および Spirent TestCenter SPT-N4U）と IPAブース内の各社装置との間においてトラフィックの生成と伝送を支援し性能評価等に貢献しています。

これらの取り組みについてはInterop Tokyo 2023 実行委員やアワード審査員の方々から高く評価いただき、４つのアワードを受賞し、協力いただきました４社からも満足のいく実験結果が得られたとのコメントを頂きました。来年度以降においてもICSCoEの持つ技術力と魅力を存分に発揮することで、新しい価値を提供できるように準備していきます。



担当者より

ICSCoEでは激甚化するサイバー攻撃に対するサイバーセキュリティ対策の強靭化に対応するため、最新の技術や設備を導入してメーカー等と協力しながら実機を用いたセキュリティ対策や製品の検証ができる環境構築及び人材育成を行ってきました。

このような取り組みが評価され、今回Interop Tokyo 2023では、各メーカーが開発中のまさに最先端である800Gイーサネット機器を取り集めて性能の評価やセキュリティに関する評価、世界初となる多メーカー装置を組み合わせた動態展示を実現できたと実感しています。

このような取り組みを続けること、その成果こそが我々の価値であることを認識し、今後もメーカー等と関係強化を図り、新しい価値を生み出し続けられるよう努めてまいります。

ICSCoE サイバー技術研究室　松本 智

第６期中核人材育成プログラム 修了

2023年６月、第６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。48名が１年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。

株式会社オプテージ
村上 由佳 さん

修了者代表挨拶

この１年間は、社会人生活の中で重要な節目となり、成長と学びの機会がたくさん詰まった期間でした。

今年は新型コロナウイルスの影響も落ち着きを見せ、第６期の海外派遣演習には多くの受講者が参加しました。私はフランス派遣演習に参加し、現地の最新動向を実感したことで、今後の自己研鑽の糧となりました。会社ではなかなか経験できない海外でのフォーラムの参加や海外セキュリティの実情について生の声を聴くことができ、非常に良い経験となりました。

また、普段の研修では、実際の現場に近い環境で１からステップを踏んで学ぶことで、攻撃者目線でリスクをとらえるようになるなど、セキュリティについての多くの知見を得ることができました。

さて、サイバーセキュリティは日々進化し続ける領域です。技術の発展と共に複雑化し、同時に新たな脅威も出現しています。この急速な変化に対応するためには、セキュリティ対策も進化を続けなければなりません。そのためにはこの１年で得たつながりを今後も活用して情報収集をすることが必要になります。そのようなつながりこそ、最も貴重な財産として大切にしていきたいです。

今後は、培った知識やスキルを活かし、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取り組んでまいります。また、同期や先輩方、講師の方々とのつながりを大切にし、さらなる成長と学びを追求していきます。１年間本当に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

IPA Better Life with IT
ICSCoE Industrial Cyber Security Center of Excellence
ICSCoE REPORT
令和5年8月31日
vol. 16
ICSCoE ReportはICSCoEの活動を皆様にご紹介する広報誌です。

「Interop Tokyo 2023」出展 サイバーセキュリティ人材育成への取り組みが注目される

2023年６月「Interop Tokyo 2023」が開催され、ICSCoE が出展しました。「中核人材育成プログラム」の受講者および修了者がブースプレゼンを行い、卒業プロジェクトの成果などについて発表しました。

Interop Tokyo は、インターネットテクノロジーと応用ビジネスに焦点を当てる歴史あるイベントです。ICSCoE は、中核人材育成プログラムの成果発表や知見の還元の場として参加しました。会場内のステージでは、修了者のコミュニティである叶会（かなえかい）のメンバーと、中核人材育成プログラムを受講中（2023年６月時点）の第６期生のメンバーの、合計20名が登壇。各自のプレゼンテーションでは、卒業プロジェクトから得られた技術的成果や、サイバーセキュリティに対する洞察が公開され、中核人材育成プログラムの意義をイベント参加者に強く印象づけることができました。

キッズ向けサイバーセキュリティ漫画、修了後の反響も大

東海旅客鉄道株式会社
八木 晴信 さん（第４期修了者）

展示ブースにおいて、１年間の教育プロジェクトの成果発表が行われ、JR 東海の八木さんが登壇しました。第４期生で修了者である八木さんの発表は、２年前に行ったキッズ向けのサイバーセキュリティ漫画の制作プロジェクトと、その後の成果についてでした。このプロジェクトの目的は、子供たちがサイバーセキュリティに興味を持ち、必要性を認識してもらうことで、子供たちが活躍する将来の日本のサイバーセキュリティレベルを向上させるというものです。「これまでのサイバーセキュリティ漫画は、“やっちゃダメ”という内容のものが多く、セキュリティとの距離を遠ざけていました」と八木さんは語ります。この問題を解決するため、セキュリティ技術をキャラクター化し、サイバー攻撃に対してどのように対処しているかを親しみやすく表現。サイバーセキュリティを身近な存在にすることに焦点を当てたといいます。プロジェクトの成果として、漫画を読んだ子供たちに対してアンケートを実施した結果、読書前よりも格段にセキュリティに対する理解が高まり、そのイメージが向上したことが発表されました。さらに、将来の職業としてサイバーセキュリティ分野を選ぶことに興味を持つ子供が増えたという効果もあったといいます。この作品『エブリデイ ゼロデイ』はオンライン書店にて無料で入手でき、日本語版だけではなく英語版も公開されています。「修了者のコミュニティである叶会の中で、若年層の啓発部会を立ち上げ、卒業プロジェクト終了後もキッズ向けのサイバーセキュリティの活動を続けています。修了後もつながりを持って、取り組みを続けていけるので、このプロジェクトの目的が達成できると信じています。」と八木さんは語ります。

▼IPAのWEBページでも紹介しています。
https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2021/index.html

次のページでは、第６期受講者によるブースプレゼンの内容を掲載しています。

OTインシデント対応訓練プログラムを作成、修了後も継承

JFEスチール株式会社
川上 理香 さん（第６期生）

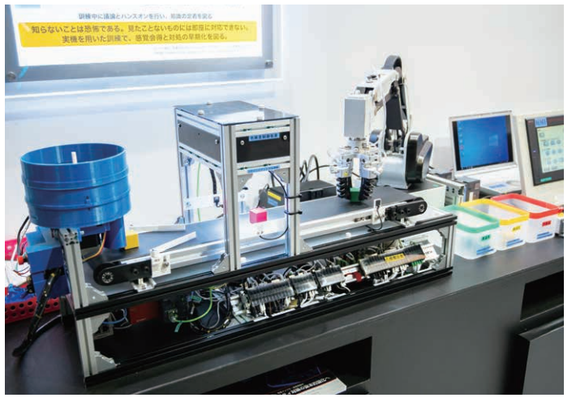
株式会社日立ソリューションズ
太田 悟 さん（第６期生）

近年、サイバー攻撃の対象が情報システムに限定されず、インターネットに直接接続していない制御系システムにまで広がっています。甚大な被害を引き起こす制御系への攻撃を防ぐため、実際のセキュリティインシデント発生時の早期対応や復旧が求められています。こうした問題意識を背景に、第６期生の川上さん、太田さんの卒業プロジェクトでは、OT 系 IT システムのセキュリティインシデントの対応のための訓練プログラムの作成が実施されました。この訓練プログラムの目的は、制御系の担当者が実際のインシデント発生時に、社内のセキュリティ部署と連携を図り、早期に対応・復旧が行えるスキルと気づきの感覚を習得するというものです。ブース会場では当プロジェクトで作成した模擬プラントも設置され、参加者は実演の様子をうかがい知ることができました。

作成されたプログラムの内容は、ネットワーク、ログ分析、脅威分析、防御製品、法規、教育・訓練、BCP、攻撃手法などの一連の訓練を通して体験するというものです。

プログラムでは「不正機器による誤動作の誘発」「不信 USB によるプラントの停止」「非管理 Wi-Fi からの不正侵入」「制御機器へのランサムウェア感染」「VPN 装置からの不正侵入」という５つのシナリオが用意されました。企業の検査ラインのロボットアームとコンベアにより構成された検査プラントを想定し、対応を実施するというものです。可搬型機器の環境による実践的な作業により、シナリオごとの収束と復旧の行動議論、早期対応・復旧スキルの習得が行われました。

川上さん、太田さんは「制御系システムの防御には全社的な対応が必要であり、IT と OT の総合的な知識が求められます。それぞれの専門的な組織との連携が必要です」と語り、IT と OT の連携による防御戦略の重要性を強調しました。このプロジェクトの成果は、卒業後もメンバーが活用できるものにしていき、今後もさらに充実させていくと述べ、プレゼンを締めくくりました。

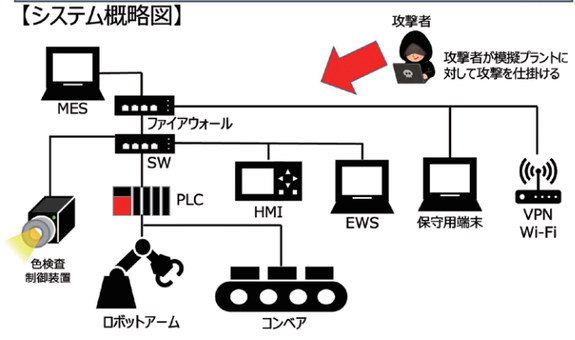


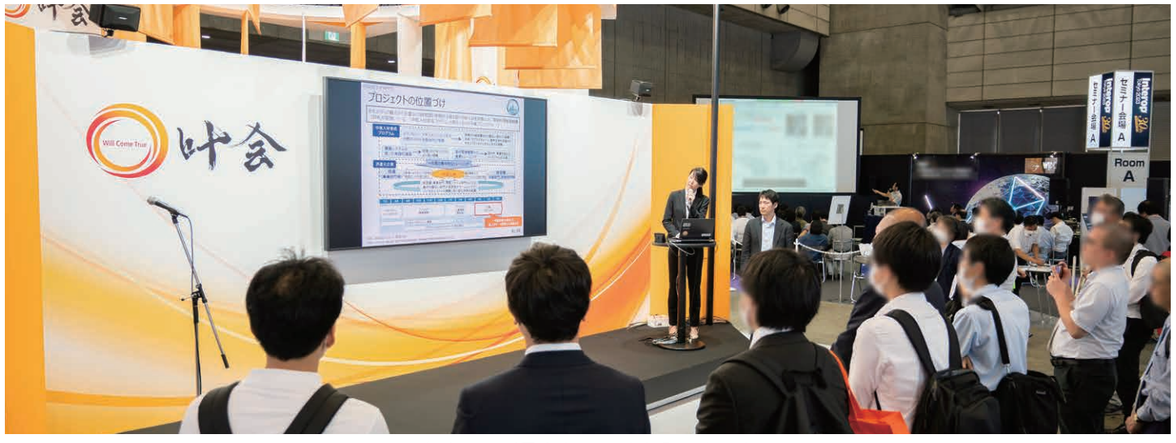
プロジェクトで作成した模擬プラント

システム構成

企業の検査ラインのロボットアームとコンベアにより構成された検査プラントを想定した
現場のアクチュエータからPLC、HMI、MESまで導入し、実際の制御システムに近づけた構成とした

【システム概略図】





多くの方が足をとめて聴き入りました

脆弱性対応のベストプラクティスを成果物に

中部電力株式会社
山本 真也 さん（第６期生）

第６期生の受講者である山本さん、渡邉さんによる卒業プロジェクトの発表テーマは、「脆弱性ハンドリング」というものでした。IPA が発表した「情報セキュリティ 10大脅威2023年版」において、システム内に潜在する脆弱性を悪用した脅威が多くランクインしている事実を背景とし、これらの脅威への対策状況の整理とベストプラクティスの提供が目的となっています。

このプロジェクトの枠組みでは、IT と OT の対策実施状況に焦点を当て、脆弱性の対象範囲を「脅威源」「脆弱性の状況」「システム」「ステークホルダー」の４つの評価軸により分類しました。これによって、各項目に対する具体的な対策が整理され、効果的な対応が可能となります。

また、インプットされる脆弱性情報をどのように扱って判断するかという観点で、SSVC*というフレームワークを用いた効果や生じた問題について詳しく説明されました。さらに、抽出された対策ポイントの OT への適用検討、各対応に要する日数の想定方法なども明らかにされ、環境構築から導入、運用に至るまで一貫した実践に必要な具体的なノウハウが紹介されました。最後に、山本さんは「今回の卒業プロジェクトの成果物や知見・ノウハウは、今後も継続してメンバー間で共有し、さらなる活用を目指す」と締めくくりました。

住友化学株式会社
渡邉 琢也 さん（第６期生）

*SSVC：Stakeholder-Specific Vulnerability Categorization

本ガイドの対象

✓ 本ガイドで取り扱う「脆弱性」の対象範囲を脅威源・脆弱性の状況・システム・ステークホルダーの4要素で分類し、以下の通り設定した。

項目	対象	
脅威源	外部からの攻撃	内部からの攻撃
脆弱性の状況	既知	未知
システム	IT	OT
ステークホルダー	ユーザ企業	ベンダ企業

組織的な脆弱性を行うためのベストプラクティス（第1ゴール）

ITの検討内容をそのままOTへ適用したいが、、、 ？ 環境上の制約や脅威が異なる ✗

OTへの適用する際に注意すべきポイントの整理（第2ゴール）
→ コラムへ記載

実践的な演習環境により、ガイドラインと教育コンテンツを生む

西日本旅客鉄道株式会社
上池 雄一郎 さん（第６期生）

第６期生の上池さん、金子さん、福田さんの３名の発表は「クラウドセキュリティ設定ミスとの付き合い方」というもの。はじめに上池さんは「メンバーは、このプロジェクトへの参加以前はセキュリティの知識は浅かったのですが、６期生として頑張ることで成果物を生み出すことができました」と語りました。

プロジェクトの背景は、クラウドサービスが高度化し、企業の DX 推進に欠かせない基盤となっている一方、クラウドにおけるセキュリティインシデントが数多く発生していることだと言います。その原因は、単なる設定ミスであることがほとんどであり、その割合は2020年時点では95% を占め、2025年時点では99% を占めると予想されることから、「クラウドサービスの設定ミスによるインシデントを防ぐ取り組みが急務だ」と上池さんは語ります。

プロジェクトの目的は、設定ミスに対する考え方や効果的な対策について重要なポイントを解説したガイドの作成、設定ミスのリスクと対策を体系的に学べるハンズオン教育のための教育コンテンツ作成というものです。プロジェクトメンバーによる文献調査、ソリューションを活用している企業へのヒアリング、技術検証を行い、メンバーのディスカッションを経てベストプラクティスを導出し、成果物としてガイドと教育コンテンツがまとめられました。

ガイドでは、「設定ミスはヒューマンエラーであり防ぐことは困難なので、問題発生を受け入れて発見是正する仕組みが重要」という基本姿勢のもと、「予防的統制」「発見的統制」の２つの分類から課題を整理。CCoE、CSPM、IaC * の実践のポイントを解説しています。

三菱電機株式会社
金子 英司 さん（第６期生）

株式会社オプテージ
福田 哲也 さん（第６期生）

また、教育コンテンツでは予防的統制や発見的統制を利用したガードレール型セキュリティや、設定ミスによるクラウドのリスクを実体験として知ってもらうための演習環境が作成されました。クラウド環境によるハンズオン演習やグループワークによって、実践的な技術が習得できる形式になっていると言います。

この卒業プロジェクトにより、演習用クラウド環境を構築することで実践的な技術検証が可能となり、ガイドラインの作成と教育コンテンツを生み出すことができたと、上池さんは語ります。

*CCoE:Cloud Center of Excellence、CSPM:Cloud Security Posture Management、IaC:Infrastructure as Code

必要な2つの統制

予防的統制	発見的統制
不正な操作・設定を事前に防止し、インシデント発生を未然に防ぐこと	リソースが不正な状況になっていないかを継続的に監視し修正すること
例）セキュリティポリシーの作成	例）外部および内部脅威の監視・分析
例）最小権限の原則管理	例）セキュリティ設定の監視・検証
例）セキュリティチェック	
例）設定ミスに対する教育	

発見的統制は、完璧に実施することが難しい予防的統制を補完する役割