



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

## 齋藤経済産業大臣が ICSCoEの秋葉原演習施設をご視察

2024年2月、齋藤経済産業大臣がICSCoEの秋葉原演習施設を視察されました。

今回の視察では、中核人材育成プログラムのアドバンスコースにおける演習の一環として、各業界の受講者たちが、それぞれの業界で起こりうるシナリオを考え、攻撃デモンストレーションを実演しました。



制御システムを狙うサイバー攻撃デモンストレーションを受講者が実演



受講者たちは、攻撃によってもたらされる影響や被害だけでなく、どのように対策をすれば攻撃を防ぐことができるのか、攻撃者の目線も踏まえてグループワークで議論した考えを発表し、解説を行いました。齋藤大臣からは、制御システムに対する攻撃の実態について踏み込んだ質問がなされ、システムが抱えているセキュリティリスクについて懸念を示されました。

また、意見交換の場では、齋藤大臣からは、ICSCoEでの1年間の訓練によりできるようになること、人材育成に掛かる時間とコストの関係、ICSCoEの修了者の活躍状況など、様々な観点から質問をいただき、防御を行うセキュリティ人材の育成を進めていく重要性をあらためて強調されました。



意見交換の場ではセキュリティ人材育成の重要性をあらためて強調されました

# 超高精細映像を用いた広域映像配信実証実験

2024年2月、国立研究開発法人情報通信研究機構（NICT：エヌアイシーティー）が主催した「超高精細映像を用いた広域映像配信実証実験」に、中核人材育成プログラムの修了者、受講者、講師混成のセキュリティペネトレーションテストチームが参加しました。

2019年から始まり今年で6年目となる今回の実証実験のポイントについて、リーダーの井上さんにお話を伺いました。

## ■ Purple team testのイメージ

テスターは、「そのサイバー攻撃の成立条件をどこで断ち切ることができるか」を常に頭に入れた上で、テスト計画を立案し、実行し、導入していたセキュリティ製品での検知／防御状況を同時に評価する。



## 実施する目的・メリット

- どのセキュリティ対策が最も現実的かつ有効なのか、求めやすくなる。
- システムオーナー（SIerや製品メーカー）にとって、何をどのように対策すれば良いかがより分かりやすくなる。
- 一連のインシデント対応を想定しやすくなる。



井上 裕司 さん(2期生)

今年も、今後業界のスタンダードになっていく映像伝送技術、制御機材、バックボーンなどに対するペネトレーションテストを行いました。昨年までは攻撃側のRed teamと防御側のBlue team、それぞれに分かれて実験を行っていましたが、今年は攻撃も防御も合わせて1つのチームで検討する、Purple team testの考え方を取り入れました。

Purple team testでは、映像業界でビジネスを行う企業（ビジネスオーナー）の方、システムオーナーの方（SIerなど）、私たちペネトレーションテストチームが一体となり、三つ巴で議論をしました。映像配信や放送の分野でPurple team testを実践することはまだ珍しいのですが、従来のように、攻撃と防御に分かれていてはできない議論もあります。今回は、たとえば悪意のある第三者から攻撃されるシナリオを考えたとき、それが成立したらどれだけの事業インパクトがあるのか、シナリオが成立する条件を断ち切るためにはどう対策をすれば良いかなど、三者が一体となって議論をすることで、より質の高い検証ができたと考えています。また、机上の話で終わらせず、そのシナリオを再現・実演し、より深い議論まで発展させることもできました。

また、今年はさらに質の高い議論ができるようシナリオを精査しました。事業インパクトが大きいシナリオにしっかりと時間を掛けて検証を行うことで、三者それぞれの視点で活発に意見を出し合い、十分な議論を行い、最終的に全員にとって納得感のある結論を導き出せるような、まさにPurple teamならではの結果を出すことができたと考えています。ビジネスオーナーやシステムオーナーの方々が懸念するシナリオが、私たちが考えている視点と同じであると確認できたことは、今回の実証実験で得られた大きな収穫でした。

早いものでこの実証実験に参加するのは、今年で6年目となりました。自身の知見向上はもちろん、これまでお世話になった通信業界やICSCoEの先生方に恩返しをしたいというモチベーションで続けてきました。ここ数年は、参加している現役の受講者の成長を目の当たりにでき、修了者や講師陣も刺激を受けています。初めはできることが少なくても、各自が共通の課題認識を持ち、チームで行動し、日が経つにつれて出来ることが増えていきます。また、今年はビジネスオーナーへ自分達が立案したリスクシナリオとデモの説明まで体験してもらいましたが、それに向かう目の色が変わっていくところは、ICSCoEならではの感覚を感じて見ました。

最後になりますが、今回のPurple teamの方々には、急なお願いにもかかわらず快く実験の趣旨に賛同いただき、長時間の議論にも積極的にご参加いただきました。Purple team testとして大きな成果を出すことができたのは、まさにチームの力だと考えています。この場を借りて深く感謝申し上げます。



映像制御機器やネットワーク機器に対する様々なセキュリティ脆弱性検証を実施(2/5～2/8、4日間(32時間/1名あたり)の参加)

## 国内最大級のOTセキュリティコンファレンスにICSCoE関係者が登壇



制御システムセキュリティに関わる多くの方が参加

2024年2月、「第8回重要インフラサイバーセキュリティコンファレンス、第5回産業サイバーセキュリティコンファレンス」が、コロナ後初の対面方式（於：東京コンファレンスセンター品川）およびウェビナーにて開催され、中核人材育成プログラムの修了者をはじめとして、ICSCoEの関係者が多数登壇しました。

パネルディスカッション「サイバーセキュリティのエコシステム／組織間連携の構築～地域コミュニティの発展から読み解く～」のセッションでは、中核人材育成プログラムの講師を担当している目黒有輝氏がパネラーとして、中核人材育成プログラム修了者（2期生）である長谷川弘幸氏がファシリテーターとして登壇しました。ディスカッションの中では、人材育成は各地域や組織の中で良い循環サイクルを回すことが重要であること、サイバー攻撃対策の底上げには、各企業だけでなく地域全体として取り組む必要があることなど、登壇者各々が地域の活動に対して熱い思いを語りました。



中核人材育成プログラム 講師  
目黒 有輝 氏

地域コミュニティの在り方について話題が上がった際には、目黒氏は「コミュニティを担っていく中心は、運営する側ではなく参加する側であり、どのように参加する人材を確保し、連携していくのかを検討する必要がある」と語りました。また、自身がコミュニティを運営する立場として、運営側の世代交代を考慮しながらコミュニティを継続していくことの苦勞や重要性などを、実体験に基づいて語りました。



中部電力パワーグリッド株式会社  
長谷川 弘幸 氏(2期生)

セッションの終盤、ファシリテーターとして長谷川氏は、「組織と組織が結びつく要因として、コミュニティが効果的であるということが再度認識できた」とまとめました。また、コミュニティを運営する担当者の熱い思いに敬意を払うとともに、聴講者へのメッセージとして、「コミュニティに参加したい、自分でコミュニティを立ち上げたいという思いがある方は是非、今回の議論や事例を参考にしてほしい」と語り、今後のコミュニティ活動を活発化するべく、セッションを締めくくりました。

# ICSCoEの短期プログラムご紹介

産業サイバーセキュリティセンターでは、サイバーセキュリティ対策に必要な組織を守るためのスキルを短期間で習得いただけるプログラムを、年間で多数実施しております。今回は、2024年1月～2月に実施した2つのプログラムをご紹介します。

## 責任者向けプログラム サイバーセキュリティ企画演習 (CyberSPEX)



2024年1月から2月に掛けての計4日間で、サイバーセキュリティ企画演習(CyberSPEX)を開催しました。本プログラムは2023年度に新設されたプログラムで、主に社会インフラ・産業基盤に関わる企業・団体の方々に参加いただきました。

本プログラムは、責任者として必要なサイバーセキュリティや事業継続に関する知識を習得し、企画立案の演習を行います。サイバーセキュリティ推進のために必要な企画(体制、予算、ポリシーなど)スキルを習得するだけでなく、経営層を説得するための考え方やロジカルシンキングの手法を身につけることができます。

演習ではグループに分かれ、企画書の作成から模擬役員会における経営者(講師が担当)の説得まで、一連の業務のシミュレーションを通して実践いただきました。参加者は演習中に習得したノウハウを駆使しながら、グループワークを通してスキルアップを図りました。

また、演習後の情報交換の場では、和やかな雰囲気の中、人脈形成やそれぞれの経験談の共有などを目的に、受講者同士積極的なコミュニケーションが図られました。



CyberSPEXの模擬役員会の様子

## 責任者向けプログラム サイバー危機対応机上演習 (CyberCREST)



2024年1月から2月に掛けての計3日間で、サイバー危機対応机上演習(CyberCREST)を開催し、国内外にサプライチェーンを展開する企業や制御システムを有する企業・団体のサイバーセキュリティ責任者等に参加いただきました。

本プログラムは、産業用制御システムを狙うサイバー攻撃者の戦術や技術、地政学的視点から見たサイバー脅威の動向と対策のあり方、近年急速に発展する生成AIの活用に伴うサイバーセキュリティへの影響などを学びながら、サイバー攻撃に対する企業の適応能力、回復力を強化するための実践的なスキルを習得することができます。

演習最終日の3日目には、サイバー攻撃が発生したことを想定したシナリオを用いて机上演習を実施しました。これまで学んだことを実践すべく、参加者は本番さながらの様子で対応策等を検討し、責任者として行すべき意思決定や対応策について、互いに発表を行いました。



CyberCRESTの机上演習の様子

## 2024年度 短期プログラム 年間スケジュール (2024年5月時点)



	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
<b>責任者向け</b> 業界別サイバーレジリエンス強化演習 (CyberREX)		<b>東京</b> 5/16(木)～5/17(金) 対象業界: 自動車(製造)、ファクトリーオートメーション、 鉄道、船舶、物流、医療、電気通信・放送				<b>東京</b> 9/5(木)～9/6(金)予定 対象業界(予定): 電力、ビル、石油、 化学、ガス、医療			<b>大阪</b> 11/21(木)～11/22(金)予定 対象業界(予定): 鉄道、船舶・物流、医療、 その他追加予定			
<b>実務者向け</b> 制御システム向けサイバーセキュリティ演習 (CyberSTIX)		<b>大阪</b> 5/27(月)～5/28(火)				<b>東京</b> 9/30(月)～10/1(火)予定					<b>未定</b> 未定	

※その他の短期プログラムについては、実施時期が決まり次第公開いたします。

