IPA Better Life with IT

ICSCoE REPORT
Industrial Cyber Security Center of Excellence
令和6年12月24日
vol. 20

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

第８期中核人材育成プログラム開講

2024年７月１日、産業サイバーセキュリティセンター（ICSCoE）は、これから日本の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57名を迎え、第８期中核人材育成プログラム開講式を行いました。

IPA齊藤理事長は、自分が何を果たすべきかを考えながら自己研鑽に励んでほしいと激励するとともに、受講者同士お互いを高め合いながら、業界の垣根を超えた横のつながり、第１期から第７期までの縦のつながり、国内外の専門家とのネットワークを広く構築していってほしいとエールを送りました。

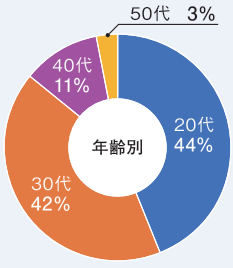

受講者に語り掛ける澤田センター長

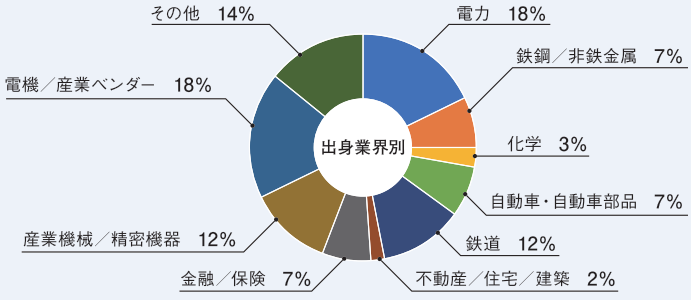
新たに着任した産業サイバーセキュリティセンター澤田センター長からは、受講者に対して２つの期待が語られました。一つめは、昨今の攻撃はAIも活用されますます高度になっており、これまでの知識だけでは太刀打ちができなくなってきていることから、主体的に自分で考えながら対処できるようなトップクラスのリーダーを目指してほしいということ。二つめとして、修了者や講師の方々とのネットワークを活用しながら、57名の８期生の同期同士、お互いに切磋琢磨して成長してほしいと語り掛けました。

来賓の経済産業省商務情報政策局長 野原諭氏からは、プログラムを修了した後は、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材であり、派遣元企業のみならず、産業界全体、日本全体、さらにはグローバルを舞台に活躍される人材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。

第８期中核人材育成プログラム 参加実績

サイバーセキュリティ分野における日本の将来を担う中核人材を目指し、様々な業種・業界より57名の受講者がプログラムに参加します。





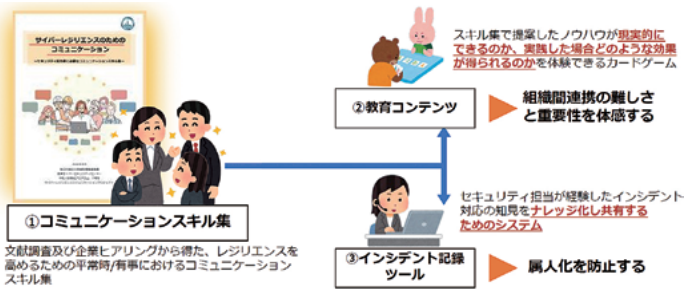
サイバーレジリエンスのためのコミュニケーション

◆背景・課題

サイバーインシデントが発生した際、速やかに回復するにはインシデント対応を行う部署が他部署と正確に情報をやりとりし、状況把握・指示をすることが必要です。本プロジェクトでは、インシデント発生時だけでなく平常時にも注目し、組織で連携して柔軟にインシデントに対応する力や、サイバーレジリエンスを高く維持するためのコミュニケーションテクニックを明らかにし、対策等を取りまとめました。

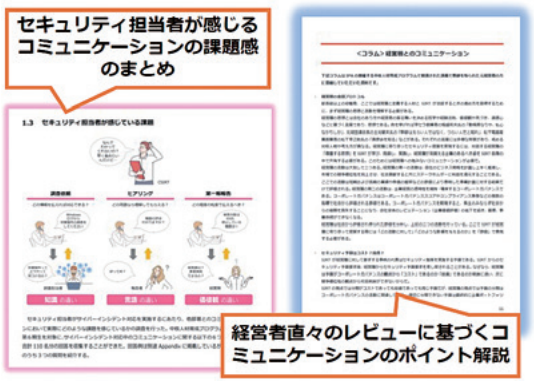
◆課題解決・成果物

本プロジェクトでは、サイバーセキュリティに関するインシデント対応に関係のある全ての方向けに、コミュニケーションスキル集、教育コンテンツ、インシデント記録ツールを作成しました。



成果物の概要

文献調査及び企業ヒアリングから得たレジリエンスを高めるための平常時／有事におけるコミュニケーションテクニックを整理し、コミュニケーションスキル集として１冊に集約しました。スキル集には、サイバーレジリエンスに関する解説やセキュリティ担当者によるコミュニケーションの課題の調査結果、企業ヒアリングデータ、経営層とのコミュニケーションテクニックなど、さまざまな情報を記載しています。このスキル集を成果物の中心として、実際にスキルを実践するためのコンテンツとして教育コンテンツ、経験した知見をナレッジ化、共有するためのシステムとしてインシデント記録ツールをそれぞれ作成しました。教育コンテンツの詳細については次ページ「セキュリティ啓発コンテンツ作成プロジェクト」を参照ください。



コミュニケーションスキル集の一部抜粋

修了者インタビュー

西日本旅客鉄道株式会社　**西澤 優里さん**
（前列中央）とメンバーの皆さん

一番の収穫は？

セキュリティに関する学んだ知識や技術を会社の中でどのように活用していくかを、ICSCoEの同期、講師陣や先輩方から学べたことが一番の収穫でした。セキュリティ対応の必要性や価値観を様々な部署や立場の方と共有することは一筋縄ではいかない場合もあります。多種多様な立場に立った情報共有の仕方を行う、分かりやすい事例を提示するなど、様々な知識や技術の活用パターンを教えていただき、現在の業務に役立てています。

成果物の活用法

セキュリティに関するコミュニケーションを行う上での軸として使用いただければと考えています。セキュリティを強化し、自社を守っていくには、どのように周りを巻き込んでいくかが重要となります。自分の所属している部署、あるいは企業だけで守ろうとした場合、必要な情報共有がなく、インシデントが発生した際に初動が遅れてしまうことがあります。周りの部署や企業も仲間意識をもって情報共有をすることで、より早く対処方法を検討することが可能となります。そんな場面で是非、本成果物を使用いただければと考えています。

ここが ICSCoE ならでは！

１つ目は、攻撃者目線で、実機での実際の挙動を確認しながら防御を検討することができるところです。攻撃を経験したことによって、攻撃者の心理状態を考慮するなど考え方の幅が広がり、どこまで対策を検討すればよいかの判断ができるようになりました。

２つ目は、幅広い人脈を形成できることです。今までは自社やグループ会社としか話す機会がありませんでしたが、同業他社や異なる業界の方々と話すことで、セキュリティ対策の考え方や方法が全く異なることに気づくことができました。また、ICSCoEで培った人脈から相談できる人が増え、今では外部の方とも協力しながらセキュリティを検討することができるようになりました。

３つ目に、社会への影響の大きさです。この成果物を発表した後、とあるセキュリティの講習に参加したところ、この成果物を引用元とした資料がまとめられ、研修資料として活用されている場面に遭遇しました。このように自社だけでなく“セキュリティ”という観点から広く社会に貢献できる機会があるということがこのICSCoEならではであると考えています。

セキュリティ啓発コンテンツ作成プロジェクト

◆背景・課題

近年、サイバーインシデントに関する対応の重要性が増してきておりますが、対策をどれだけ実施してもサイバー攻撃を100%防ぐのは困難です。また、企業等で行う一般的なサイバーインシデント訓練は、想定内の事象に対してマニュアルで定めた対応を確認する形式的なものが多く、コミュニケーションの課題を発見しにくいといった課題があります。実際のインシデント対応では想定外事象も発生し、多くの関係者で対応するため、情報連携が必要不可欠となりますが、各組織がどのような情報を所有しているか、どのような情報が必要なのか、見えづらいのが現状です。これらを解決するために、インシデント時に発生する組織間の情報連携の流れを再現し、コミュニケーションにおける課題を発見できる啓発コンテンツを開発しました。

◆課題解決・成果物

本プロジェクトでは、OT/ITいずれにも被害が発生するシナリオを、カードゲーム形式でシミュレーションできる教材を作成しました。

カードの一例

シミュレーションを通じてインシデント対応を疑似体験し、情報連携の重要性や課題を理解してもらうことが目的です。シミュレーション終了後には、振り返りとして自社との比較や改善点を議論することで課題を抽出し、解決のアクションに繋げます。

ゲーム内では、自分の得た情報を誰が必要としているのか考えさせられるようになっているため、情報の連携ミスがあった場合は参加者自身が気づき、今後の検討材料とすることができます。

自社想定時の振り返り時の参考項目（抜粋）

チェック項目	☑
NIST "Computer Security Incident Handling Guide"	
コミュニケーションツールの優先順位が確立され、関係者に周知されている	
緊急時の連絡先情報が用意されており、常に最新情報に更新されている	
連携が必要な外部機関およびその連絡先が整理されている	
インシデントの重要度を決める指標があり、関係者に周知されている	
SANS Institute "Incident Handler's Handbook"	
演習を通じてインシデント対応組織の課題を発見し改善する仕組みがある	
インシデント対応を記録するフォーマットがあり分析できる仕組みがある	
誰がどのようにインシデントを報告するか、どの情報を含めるべきか定められている	

振り返りシートの抜粋

修了者インタビュー

大阪ガス株式会社　**辰巳 大祐さん**
（前列左から２番目）とメンバーの皆さん

一番の収穫は？

プロジェクトリーダーを務めることができたことです。自分が学んだ知識を自社や産業界に還元したいという気持ちがあり、自分からリーダーに立候補しました。プロジェクト内でのタスクの洗い出しやメンバへの割り当て、進捗管理など、マネジメント面で成長できたのではないかと感じています。

成果物の活用法

帰社後、既に自社内で活用しているメンバーもいます。対象としては、まずはセキュリティ担当者に活用いただき、自社内のセキュリティ研修や関係各所への啓発活動に役立てていただきたいと考えています。その後は、ぜひ中間管理職の方々にも活用いただきたいと思います。自社内にサイバーインシデント訓練があっても、形式的なもので対応方法の確認にしかなっていない場合、実際にインシデントが起こっても、指示・報告など求められる適切な行動が取れないことがあるためです。より多くの方々に、まずは１度体験いただきたいと考えています。

ここが ICSCoE ならでは！

経験したすべてがICSCoEならではと感じましたが、一番は講師や受講者同士の人間関係だと思います。１年という長い期間、業務の壁を越えて構築される密な関係は、ほかではなかなか作ることができないと思います。自社での通常業務では関わることがなかった方々と深くコミュニケーションを図ることができ、自社や自分の業界に籠っていては知り得なかったことまで知識の幅を広げることができました。特に、他の企業・業界のセキュリティに関する取組みに触れ、理解できたことは、今後、企業や業界をまたいで活動する上で、大きな糧になると思います。

第７期中核人材育成プログラム修了式

遠藤センター長（当時）

産業サイバーセキュリティセンターの遠藤センター長（当時）より、激励のご挨拶をいただきました。

今期は卒業プロジェクトをはじめとして自立的に学習いただくことが増え、受講者の皆さまは毎晩夜遅くまで取り組んでいたとお聞きしております。人が自立をする上では、判断・決断をするために自らの判断基盤を持つことが重要ですが、１年間、ご自身や業界の抱える課題に目を向けてしっかりと取り組んでいただいたということで、判断基盤の幅を一段と広げることができたのではと確信しています。

皆さんは１年間を共にして、信頼がおけるたくさんの大切な仲間をお持ちになりました。サイバー攻撃は、一企業だけでは言うに及ばず、一国でも守ることは困難です。ICSCoEで築いたネットワークをフルに活用し、異なる業界も含めて縦横のつながりを強固にし、海外とも連携しながら、協力して守っていくことが重要になってきます。皆さまにはこれから、現場と経営者を結びつける役割だけでなく、会社や業界をまたいで、我が国全体のサイバーセキュリティ、レジリエンス力の強化をけん引するリーダーとして活躍していただくことを大いに期待しております。本日は中核人材育成プログラムの修了、誠におめでとうございます。

阪急阪神ホールディングス株式会社
久保 貴司さん

修了者代表として、久保貴司さんにご挨拶いただきました。

私たち65名の中には、初めてセキュリティに触れる受講者も多くおりました。不安を抱えながらのスタートだった方もいたと思いますが、ICSCoEでは、先生方に基礎から丁寧に指導をいただき、仲間とともに日々演習に励むことで、全員で今日という日を迎えることができました。

先生方に用意いただいたカリキュラムは、知識の習得に留まらず、ハンズオン演習を通じて実践的なスキルを磨くと共に、中核人材としてのリーダーシップ能力、コミュニケーション能力、問題解決能力を養うことができる大変貴重なものでした。自身の会社にいると本音でぶつけられない意見も、ここでは世代や企業の垣根を超えて存分に議論でき、非常に良い経験になったと感じています。

教室の外においても、海外派遣演習やハードニング競技会、各産業分野の施設見学など、手を上げれば自立的に様々なことにチャレンジできる環境は、遠藤センター長もおっしゃっていたとおり大変貴重で、刺激的なものだったと感じています。

これからは、プログラムを通じて出会った仲間と共に、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。そのためにも、これからも常に学び続け、挑戦し続けるという強い意思を持って、帰社後の業務に励んでいく所存です。１年間大変ありがとうございました。

卒業プロジェクト代表報告会

中部電力株式会社（当時）　**鵜飼 大介さん**

修了式後には代表として選出された卒業プロジェクトの発表が行われました。「Visionary Security ～ Zeroから始めるセキュリティ対策～」の発表では、鵜飼大介さんがプロジェクトリーダーとして登壇し、新たに設立した事業会社やスケールし始めたスタートアップ企業など、セキュリティリスクが高まるタイミングで必要な対策がされていないという課題が示されました。この課題に対し、プロジェクトでは「必要なセキュリティ対策の整理・体系化」「セキュリティマインド醸成のための発信活動、仕掛けづくり」「セキュリティ対策がされたIT環境のスターターキット構築」の３つの解決策を仮説として設定し、それぞれの活動内容を発表いただきました。

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