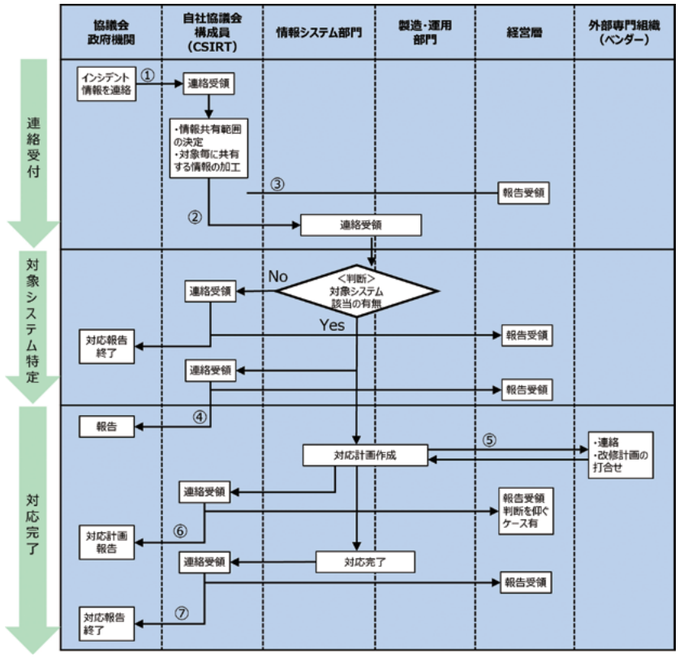


協議会経由の情報共有フローの一例(運用フロー例)

これらの成果は、実務者向けの対応指針をまとめたドキュメントに反映しました。作成したドキュメントは、実務者が法の全体像を把握したうえで、自社の現状と照らし合わせ、今、何を優先して取り組むとよいかを判断するための指針として使えることを特徴としています。法の全体像と施行までの道筋に加え、ギャップ分析から見えた課題、ベンダー視点での支援の論点、運用モデルと代表的な対応フローを整理し、自助(事業者自身が取り組む準備)・共助(業界全体での知見共有と足並み揃え)・公助(国に求める基準の早期提示と支援)の3つの枠組みによる提言を収録しました。

修了者インタビュー

一番の収穫は?

当初は、「新たな義務が課されるので対応しなければならない」という、ぼんやりとした理解にとどまっていました。本プロジェクトを通じて、本法において何が明確に定義され、何がまだ明確になっていないのか、というところまで理解を深めることができたことが、一番の収穫です。明確になっていない部分を見極められたことで、確定を待つべき事項と、先んじて準備を進められる事項を切り分けて考えられるようになりました。

成果物の活用方法

作成したドキュメントには、事業者へのアンケートを通じて得られた法対応における共通課題と、その課題への解決策の提案、主な義務に対する運用モデルや運用フロー例をまとめています。帰社後は、自社が同様の課題を抱えていないかを確認する際のチェックとして、また自社で運用フロー策定時の参考として活用したいと考えています。

ここが ICSCoE ならでは!

様々な背景を持つ受講生と、同じテーマを本気で議論し続けられる環境は、ICSCoEならではだと感じました。また、ICSCoEの講師陣にご紹介いただき、欧米の有識者やE-ISACなどの海外コミュニティと直接意見を交わせたことは、国内の情報だけでは得られない視点に触れることができ、他では得難い貴重な経験となりました。技術的な内容から経営層向けの戦略提言まで幅広いカリキュラムを受けられること、そして普段は得られない外部の知見を取り込めたことが、今回のプロジェクトの成果につながりました。こうした多様な学びと人脈形成ができたことこそが、ICSCoEならではの価値であり、ここで得たつながりを今後の業務にも活かしていきたいと考えています。

高橋 佑馬さん(前列右から3番目)とメンバーの皆さん

独立行政法人
情報処理推進機構
Innovation Platform 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

ICSCoE HP

卒業プロジェクト

VEGETABLE OIL INK
FSC ミックス 紙|責任ある森林管理を支えています FSC® C008111

独立行政法人
情報処理推進機構
Innovation Platform Agency, Japan

ICSCoE Industrial Cyber Security Center of Excellence

ICSCoE REPORT

Industrial Cyber Security Center of Excellence

令和8年8月31日

vol. 27

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

第9期中核人材育成プログラム　卒業プロジェクトの取り組み紹介　第1弾

若年層から始めるセキュリティ人財育成

背景・課題

近年、AIをはじめとする技術革新が加速しており、企業が競争力を維持するためには、新たな技術に継続的に対応していくことが不可欠です。一方で、サイバー攻撃も高度化・複雑化しており、企業には新技術の活用とセキュリティの強化を両立することが求められています。しかし、双方を担える人財は不足しており、外部からの確保も容易ではありません。

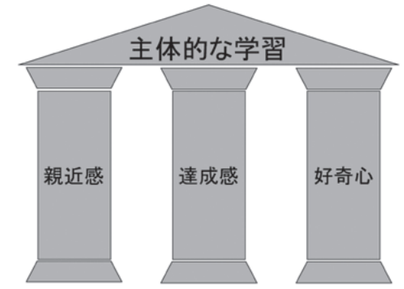
そのため、社内での人財育成が重要となります。しかし、従来のセキュリティ研修は知識の伝達にとどまりやすく、受講者がリスクを自らの問題として捉え、行動を変えるまでには至らない場合があります。その結果、過失の防止や内部不正の抑止は企業の課題として残存し続けています。また、それらのような人の判断や行動に起因する問題は、技術的な対策だけで完全に防ぐことは困難です。対策を追加し続ける方法にも、費用と運用の両面で限界があります。

これらの課題に共通する背景の一つは、新たな技術や脅威に応じて、適切に判断・行動するためのセキュリティリテラシーが、組織内に十分定着していないことです。そこで本プロジェクトでは、人の意識と行動、ならびに時代とともに変化する技術や脅威に着目し、新たなアプローチを検討しました。

課題解決・成果物

本プロジェクトでは、デジタル社会の最先端にいる「高校生」をメインターゲットに設定しました。幼少期からスマートフォン等に触れる彼らはサイバー脅威に直面しやすく、また、次世代への早期教育が社会全体のセキュリティ底上げに繋がると考えたためです。

教育を実施する上で最も注力したのは、生徒の「主体的な学習」を促すコンテンツの作成です。堅苦しく敬遠されがちなセキュリティ分野を自ら進んで学べるよう、「**親近感**」「**達成感**」「**好奇心**」を刺激する3つのアプローチを取り入れました。



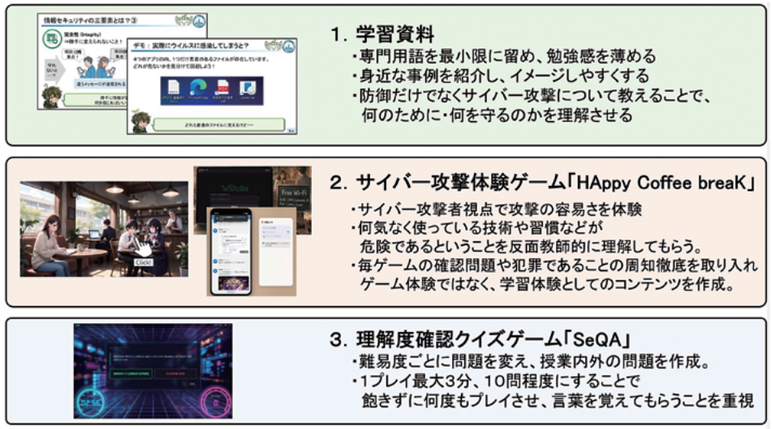
■**親近感**
・専門用語を最小限にする
・事例や脅威を身近なモノに絡める

■**達成感**
・途中でクイズを交えることで自身で理解度把握
・クリア者や正解者を授業内で称える

■**好奇心**
・ゲームやクイズなどのハンズオンを増やす
・セキュリティという分野の魅力を伝える

主体的な学習を支える3アプローチ

これらのアプローチを具現化し、基礎知識を学ぶ「学習資料」や、実践的に学べる「サイバー攻撃体験ゲーム」「理解度確認クイズゲーム」を制作しました。これらを用いて実際に学校で出張講義を実施し、座学と体験型ゲームを組み合わせることで当事者意識の醸成を図りました。



作成したコンテンツ

講義後は、生徒へのアンケート結果やゲーム進行度などのデータを用いて、効果分析を行いました。この分析結果は、本プロジェクトの成果として用いるだけでなく、今後の教育に活用できるようご協力いただいた学校へ提供しています。

今回開発した学習アプローチや実証データは、教育機関にとって有益な知見となるだけでなく、企業での従業員教育の改善や、国レベルでのセキュリティリテラシー底上げにも幅広く応用できると想定しています。

修了者インタビュー

一番の収穫は？

本プロジェクトを通じた最大の収穫は、「ハンズオン（体験型学習）」がいかに教育効果を最大化するかを実証できたことです。一般的な社会人のセキュリティ教育は、業務の合間に行うe-learningが主体であり、実践的と銘打たれたものでも、実態は座学の延長で少し考える時間が設けられている程度のものが少なくありません。しかし今回、ゲームなどの体験を通じて主体的に学ぶ仕組みを取り入れたことで、本来なら興味を持ちにくい分野であっても新たな関心を引き出し、効率的かつ深く理解を促せることを実感しました。この「能動的な学習がもたらす効果」への気づきは、教育機関での活用にとどまらず、自組織におけるセキュリティ強化や人財育成にも直接生かせる重要な知見であると感じています。

成果物の活用方法

新入社員研修や社内の教育ポータルサイトに展開することで、従業員に自主的に体験（プレイ）してもらい、セキュリティへの理解を深めるツールとして活用できます。さらに、専門知識のないご家族でも、一緒に楽しみながら学べるように設計されています。企業という組織の安全を守るためだけでなく、身近なサイバー脅威から「個人の生活を守るセキュリティ学習」としても、本教材の積極的な活用を強く推奨いたします。このような活用が普及することで、セキュリティの考え方が「常識・文化」として次世代の人財に根付くことを期待しております。


鳴島 俊哉さん（前列真ん中）とメンバーの皆さん

ここが ICSCoE ならでは！

この1年間は、セキュリティという広大な領域を網羅的に学べる非常に貴重な期間でした。自身の知識が定着していなかった分野についても、第一線のスペシャリストから直接指導を受けることができました。また、多様なバックグラウンドを持つ受講生と共に学びを深められたことで、ICSCoEならではの実践的な知見を得ることができました。

その中でも最大の成果は、専門分野の垣根を越えてセキュリティについて語り合える「同期との繋がり」ができたことです。「企業や社会、そして人々の生活を守る」という共通の目標を持ち、互いに協力し、時には切磋琢磨できる仲間との出会いは、他では決して得ることのできない、かけがえのない財産になったと感じています。

守る法対応から、強くなる法対応へ
― サイバー対処能力強化法への対応指針 ―

背景・課題

主に国外を起点とする高度なサイバー攻撃が、重要インフラの安全保障上のリスクとなっています。これに対応するため、サイバー対処能力強化法及び同整備法が制定され、2026年10月1日に施行されます。対象は、経済安全保障推進法で定める基幹インフラ15分野のうち特定重要電子計算機を使用する基幹インフラ事業者（特別社会基盤事業者）を中核とし、これに製品・サービスを供給するベンダー（電子計算機等供給者）も関係者として位置付けられます。

しかし、対象事業者・ベンダーでありながら、具体的な対応内容を定めるガイドラインが未確定であるために、何に取り組めばよいか分からず「待ち」の状態に陥りやすい状況がありました。加えて、対象事業者の所属する業界によって運用環境や体力、負う義務も異なります。「法が何を定めるか」は条文で分かっても、「自社が何を・いつまでに・どのように対応すべきか」が見えないことが、対象事業者・ベンダーに共通する課題でした。

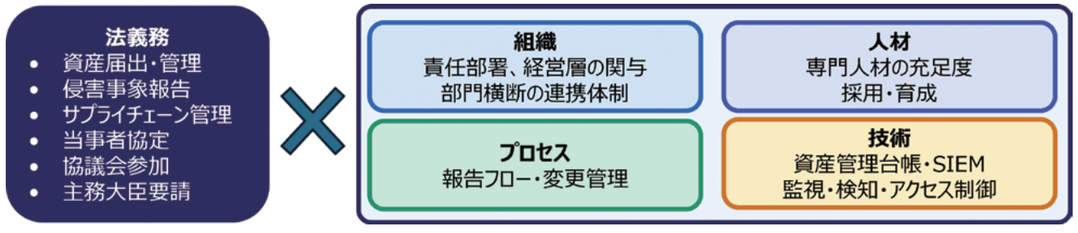
本プロジェクトは、この課題に対して「待つ」のではなく「無駄のない先手を打つ」という立場で臨みました。

課題解決・成果物

本プロジェクトでは、本法対応を「義務だから守る」で終わらせず、現場が疲弊しない形で自社のセキュリティを強くする契機と捉える「法対応を通じたセキュリティ向上」をコンセプトに掲げ、**❶法制度の共通認識**、**❷ギャップの可視化**、**❸疲弊しない運用設計**、の3つの軸で取り組みを進めました。

プロジェクトの３つの軸と成果物

対象事業者・ベンダーに対して、法義務の各項目を「組織・人材・プロセス・技術」の4つの軸で評価する業種横断のギャップ分析を行い、法が求める姿と各社の現状とのギャップを可視化したところ、最大の課題は技術力やリソースの不足ではなく、要求事項に未確定の部分が残ることもあり、法の要求を社内の手順や運用に落とし込めていないことにある、という構造が明らかになりました。裏を返せば、多くの企業は「ゼロから」ではなく、既存の体制を土台に再構成することで対応できるという見通しも得られました。



ギャップ分析のフレームワーク（法義務項目×４軸で対応状況を評価）

検討にあたっては机上の整理にとどめず、海外CSIRT・業界団体との意見交換、国家サイバー統括室との面談、Interopへの出展を通じた来場者ヒアリングなどを実施し、国内外の知見と現場の声を取り込みました。