プラス・セキュリティ人材育成

背景・課題

現在、セキュリティの担当部署以外においてもセキュリティを意識して業務遂行できる「プラス・セキュリティ人材」の不足が問題になっています。具体的には、セキュリティを自分事だと認識できていない方が多いこと、セキュアバイデザインの考え方が浸透していないことなどが挙げられます。このような背景から、企画・開発、設計・構築、運用部門などのセキュリティ意識の向上、インシデントが発生した場合の被害の理解、セキュアなシステム構築のための具体的な作業の把握等を目指して、本プロジェクトを実施しました。

課題解決・成果物

①ハンズオン研修

模擬的にインシデントを経験し、その原因と対策を検討できるハンズオン形式の研修を開発しました。本研修を受講することで、サイバー攻撃の危険性や、攻撃の起点となりやすいポイントを理解できるとともに、実務においてセキュアバイデザインを意識した設計、構築、運用を実施できるようになります。また、グループワークである本研修では、複数部門からの参加によって、異なる部門ごとの知識や思いも踏まえた対策を検討する機会とすることも狙っています。

項番	教えたい内容	セキュリティホール	シナリオ
①	フィッシングメールの危険性	－	フィッシングメールが感染源による情報漏洩という重大なインシデント
②	認証情報の管理	認証情報（ログイン用のID,パスワード）を記載したファイルをデスクトップに保管	感染した端末に保管されている認証情報でより上位の端末に不正アクセス
③	パスワードの使い回しの危険性	他アカウントでも同じパスワード利用	パスワードの使い回しによる横展開、NW深部への侵入
④	権限の最小化	過大な権限の与えられたアカウントの存在	本来閲覧権限のないファイルを閲覧、編集により暗号化
⑤	アクセス制御設定	不要なFW設定が入っている	サーバ管理用NWから外部NWへのアクセス制御が甘い

研修で使用するシナリオの例

②セキュリティ事項検索ツール

取り組むべき具体的なセキュリティ対策が分からない方向けに、自身の業務で考慮すべきセキュリティ事項について理解するための検索ツールを作成しました。本ツールは、「業務内容」「事故事例」「単語検索」の３つのアプローチで検索を行うことができ、必要な情報にアクセスしやすいよう工夫しています。また、それぞれの項目の理解だけでなく、セキュアなシステム構築・運用の重要性への気づきも目的としています。

ツール画面イメージ

修了者インタビュー

株式会社オプテージ
西口 朋哉さん

一番の収穫は？

リーダーを経験して、チームをまとめ上げるマネジメント力が身についたことです。一般的には、組織においてリーダーになるためにはある程度の年齢や経験が求められ、若手は任せてもらいにくいかと思います。私もこれまで経験がありませんでしたが、せっかくの機会と捉えリーダーを務めました。初めは論理的に物事をまとめられないことからチームの合意を取れず、プロジェクトを進められないという苦い経験もしましたが、試行錯誤しながらなんとかやり切ることができました。プロジェクトの方向性を決める、リーダーとしての決断力の重要性に気付くことができたのも、大きな収穫だと考えています。

成果物の活用法

ハンズオン研修のシナリオを増やすなど、自社向けにカスタムを行うことで、自社内で研修を行いたいです。また、セキュリティ事項検索ツールは、自社内で展開し、事故事例を定例ミーティングで紹介する等の活用を考えています。

ここが ICSCoE ならでは！

所属する企業はもちろん、職種や年齢もバラバラな仲間と気兼ねなく話せる環境は、他にはないここだけの特長だと思います。卒業プロジェクトでも、様々な分野で広く交流を深めることができました。同期からのアドバイスで今まで触れることのなかったOTについて知見を深められたことなど、自社で業務を行っているだけでは絶対に経験できなかったことばかりで、大変有意義でした。

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 vol.17
令和5年10月26日

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

第６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

「卒業プロジェクト」は、１年間のカリキュラムで習得した知識や経験を活かし、企業や業界のための課題を設定してグループワークを中心として取り組むものです。第６期は 22 件のプロジェクトがあり、そのうち４件をご紹介します。その他の公開プロジェクトも IPA サイトで閲覧できます。

セキュリティ投資を得る方法

背景・課題

昨今、サイバー犯罪およびその被害は増加の一途をたどっており、各企業においても情報セキュリティ関連費用の増加が予測されています。一方で IT 予算に占めるセキュリティ関連費用の割合は減少の傾向も見られており、将来的にセキュリティ対応が後手に回る恐れがあります。

今回、組織内での継続したセキュリティ投資（予算や協力）を得ることを課題と捉え、仕方なしに支払う「コスト」ではなく、自発的に行う「投資」として実現することを目標としてプロジェクトを発足しました。

課題解決・成果物

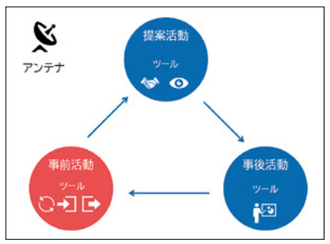
課題解決に向けて、16 社の企業のセキュリティ担当者や経営層にインタビューさせていただきました。インタビュー内容を基にメンバー内で議論、分析を行いました。

それらの活動を通して、セキュリティ担当者がセキュリティ投資を継続的に得るために活用できる方法、ツール、ベストプラクティスをまとめた参考資料「セキュリティ投資を得る方法」を作成しました。

まず、投資を得る方法の全体像を、下の図のように主たるプロセスを「事前活動」「提案活動」「事後活動」に分類し、さらに社内外の情報を取得する「アンテナ」を定めています。

成果物では、それぞれの項目について具体的な手段や例を示しています。例えば「事前活動」では、投資の得やすさの土壌づくりの方法として、経営層の巻き込み方や情報提供方法、社外とのつながり方を示しています。

WEB では、セキュリティ投資の「提案活動」に着目したサイトは見つかりますが、今回の成果物では提案活動のみならず、日々の心がけから投資獲得後の活動までを一貫して示しており、それが大きな特徴になっています。



投資を得る方法の全体像

成果物をダウンロード

アズビル株式会社 **上田 祐司さん**
（前列左から２番目）とメンバーの皆さん

修了者インタビュー

一番の収穫は？

言わば「セキュリティ流のステークホルダー・コミュニケーション」を考えられたことです。目まぐるしく変化するセキュリティ環境において、各部署や経営層の方々とどのように関わっていけば良いかという点をまとめられました。対面にこだわってインタビューさせていただいたことで、各企業の実際の取り組みなどリアルな事例だけでなく、担当者、経営層の方々のセキュリティに対する姿勢、想いに触れることができ、知見を深められました。

成果物の活用法

特に他部署や経営層の方々に、セキュリティを自分事にしてもらうための活動の検討に利用できます。例えば単に予算の獲得という観点だけだと、予算がついてもセキュリティが全社的な取り組みにならないことがあります。予算だけでなく、協力を得る、という観点も盛り込んでいることが特徴です。

ここが ICSCoE ならでは！

ICSCoE の受講者はニュートラルな存在で、第一線で活躍されている方々に構えられることなくアクセスできる点です。今回インタビューで中核人材育成プログラムの修了者の方々を中心にお会いして、我々が目指す中核人材としてのあるべき姿や ICSCoE の仲間としてのつながりを感じられました。

建設業とサイバーセキュリティ

背景・課題

建設業界では DX 活用などにより業務効率化が図られ、建築物の快適性、利便性、安全性の向上も進められる一方で、サイバーセキュリティについてはその意識付けや対策に課題が見受けられます。

課題解決・成果物

本プロジェクトでは建設業界のセキュリティ向上のため、２つのテーマを設定し、それぞれ成果物を作成しました。

テーマ1 建設業とサイバーセキュリティ教育

建設業ではサプライチェーンの中で広くセキュリティ意識を向上させることが重要と考え、関係者がセキュリティを身近に感じる機会を増やすことができる教育動画を作成しました。動画では建設業界で実際に起こったインシデントや起こりうる事例等をストーリー形式で説明しています。

また、そのような教育動画を誰でも低コストで迅速かつ容易に作成・修正できるように、マニュアルにその手法をまとめました。

テーマ2 ビル設備におけるサイバーセキュリティ

ビルにおける長期間のライフサイクル(設計～廃棄) を通して､各ステークホルダに対して必要となるサイバーセキュリティ対策を検討・整理しました。セキュアなビルを考える上での検討ポイントについて、２つの成果物を作成しました。

①セルフチェックシート

設計・仕様、建設といったビルのライフサイクルにおける各段階で、その担当者が検討・実施しておくべきことを記載したチェックシートを作成しました。設問ごとに対象となるステークホルダを示しており、関係者間での認識合わせに活用できます。

②設問項目ガイド

セルフチェックシートの設問項目についての「背景・目的」、実施されなかった場合の「想定されるリスク」、設問項目を達成する上で重要な「内容解説・施策例」をまとめました。

成果物をダウンロード

株式会社きんでん
菊川 智史さん(前列中央)
建設業に関連するゼネコン、サブコン、ベンダー、メーカー及びユーザー企業
９名のメンバーで実施

修了者インタビュー

一番の収穫は？

講師の方に丁寧にレビューいただき、的確なアドバイスをいただくことで、新しい視点を得られたことですね。例えば､チェックリストにおいてステークホルダとライフサイクルの観点で考えるということは、講師の方との対話の中でアイデアが生まれました。

成果物の活用法

動画については､例えばデジタルサイネージで流してセキュリティ意識の啓発を図れます。また安価で早く動画を作る方法を確立したので、例えば新しいインシデント事例が出た場合に、すぐに動画を作って社内で注意喚起することが可能です。チェックシートについては、建設業は様々な立場の方が絡み合っている中で、いつ、誰が、誰と対策を検討・実施すればよいかのヒントになります。

ここが ICSCoE ならでは！

受講者同士のつながりで活動の幅が広がることです。例えば今回、受講者がそれぞれのつながりを活かしてオフィスビルの見学や業界団体へのヒアリング、修了者の方から成果物へ意見いただくことなどが実現したことで、より広い視野や深い知見を得ることができました。

海外セキュリティ統制

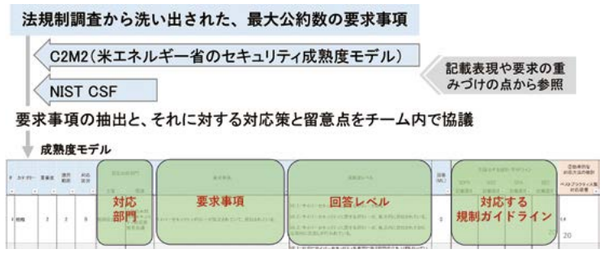
背景・課題

現在、グローバルでの企業経営・システム統合が進む中で、サイバーセキュリティの強化は企業グループ全体の課題になっています。同時に、欧米では高水準の規制・ガイドラインが公開され、日本企業も対応することが求められています。しかし、海外拠点のセキュリティ対策の実態は把握しづらく、規制・ガイドラインの全体像や具体施策への適用もしづらいといった問題があります。本プロジェクトでは、海外の高水準のセキュリティ要件に対応し、海外拠点を含めた企業全体のセキュリティレベル向上に貢献するために、２点の成果物「成熟度モデル」及び「ベストプラクティス集」を作成しました。

課題解決・成果物

①成熟度モデル

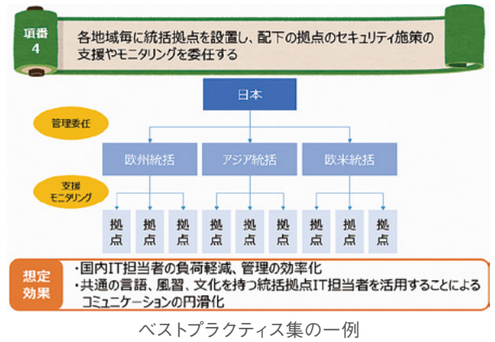
自社海外拠点の現状把握や、ベンチマークの提供ができる成熟度モデルを作成しました。作成に当たっては、海外の代表的な規制･ガイドラインを中心に読み込み、実業務で重要視されるセキュリティ要求事項を 75 項目抽出しました。このモデルでは、要求される対応策に加え、国際標準や文献等から調査した結果を評価軸として設定しています。さらに、各項目に対して重要度、適用範囲を記載することで、よりユーザが理解しやすいよう工夫しました。



成熟度モデルの作成過程とモデルの概要

②ベストプラクティス集

セキュリティの企画担当者が、具体的施策を考案する際のリファレンスとすることを主な目的として、調査した結果を事例集として取りまとめました。海外拠点の成熟度レベル向上のため、国内拠点側から行う具体施策集となっており、本成果物を活用することで、国内・海外拠点が相互に協力しながら成熟度レベルを上げていく関係性を構築することが可能となっています。



ベストプラクティス集の一例

修了者インタビュー

左から
株式会社荏原製作所 **後藤 菜穂さん**
ダイキン工業株式会社 **友藤 了佑さん**

一番の収穫は？

友藤さん：講師の先生方、同期の受講者や修了者をはじめとした人脈が広がり、自社のセキュリティ事情や知見等、気になったことをすぐに、気軽に聞ける環境を得られたことが大きな収穫でした。例えば、通常では知ることができない海外拠点のセキュリティ対策事情などについてもうかがう機会があり、大変参考になりました。今後、この人脈は、自分にとっても所属企業にとっても最大の武器になると思います。

成果物の活用法

後藤さん：自社で成熟度モデルとベストプラクティス集を使用することで、まずは各拠点のレベルを知って、理想と現実でどれくらいズレがあるのか調査したいと思います。調査の結果を見ながら、海外での現地対応やグローバル連携に備え、足掛かりになる対策を企画していければと考えています。

ここが ICSCoE ならでは！

友藤さん：通常の業務から離れて、１年間腰を据えて幅広い分野を学ぶことができました。セキュリティが関わってくる対象は多岐に渡り、今後あらゆる分野に手を付けていくべきだと思うので、これから経験しなくてはならないことを先取りして学べたことは大きな収穫でした。

後藤さん：私は実は文系の出身なのですが、体系的に組まれたカリキュラムを通して、今後、中核人材として活躍するために学んでいくべきポイントを理解できました。また、インシデント対応の実践的な演習は、ここでしか経験することができないものです。多くのステークホルダと連携しながら、情報収集から判断、対応までの一連の流れを身をもって体験できたことは、今後の実務に直結する貴重な財産になると考えています。