二つ目は、模擬プラントを用いた運用検証です。プロジェクトメンバーがそれぞれの実務経験を踏まえて課題を提起し、対応案を議論することで、OT-SOC運用における具体的な課題と解決アプローチを共有しました。机上の検討にとどまらず、模擬環境でシナリオを体験的に検証したことで、成果物はより実務に即した内容となりました。

成果物は、OT-SOC導入担当者がライフサイクルごとに直面する課題や検討ポイントを把握しやすいよう整理されたドキュメントです。導入プロセスを進める際の参考資料として、プロジェクトメンバーが派遣元企業で社内関係者との議論や検討を進める上での手助けとなることを目指しました。特に、実務担当者が限られた時間で効率的に論点を整理できるよう、視覚的に理解しやすい表やフローチャートを取り入れた点も特徴です。

修了者インタビュー

高橋 勝さん

1番の収穫は？

漠然としていたOT-SOCの進め方や導入・運用上の課題が、企業ヒアリングや模擬プラントでの検証を通じて明確になり、プロジェクトメンバーが派遣元企業で推進に活かせる知見を獲得できたことです。特に、注意すべき点やよくある課題、実務上の工夫を事前に知ることができたことで、今後の活動の品質向上に貢献できると考えています。OT-SOCのモデルとそれぞれのメリット・デメリットを整理できた点も、派遣元企業で適したモデルを検討する際の有益な参考資料となると感じています。

成果物の活用方法

派遣元企業でOT-SOCを検討・導入する担当者が利用することを想定しています。導入から運用に至るライフサイクルの各段階で生じる課題や検討ポイントを整理する参考資料として活用できます。特に、実務担当者が社内の関係者と議論を進めたり、導入に向けた検討の下地を作る際に役立つ内容となっています。

ここが ICSCoE ならでは！

多様な背景を持つプロジェクトメンバー同士の議論と、実践的な環境、そして講師陣からの専門的支援がICSCoEならではと感じました。

本プロジェクトには、様々な業種の企業からプロジェクトメンバーが集まり、その中にはIT領域に精通した専門家と、OT領域を主軸とする実務者が混在していました。ITが重視する「機密性・可用性」と、OTが最優先する「安全性」という異なる価値観が交わったことで、どちらか一方に偏らない、バランスの取れた議論と成果につながりました。

加えて、講師陣からはOT領域監視に関する専門的な知見を直接学ぶことができ、理解を深める大きな助けとなりました。さらに、実施した企業ヒアリングは講師陣のご紹介によって実現したものであり、OT-SOC運用企業・MSS事業者・ソリューションベンダーといった多様な立場から生の声を伺うことができました。

模擬プラントを活用したシナリオ検証と併せて、こうした学びと交流の機会を得られたことが、ICSCoEだからこそ実現できた最大の価値だと感じています。

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

VEGETABLE OIL INK
R60 古紙パルプ配合率 60%再生紙を使用
リサイクル適性Ⓐ この印刷物は、印刷用の紙へリサイクルできます。

IPA Better Life with IT

ICSCoE Industrial Cyber Security Center of Excellence

ICSCoE REPORT

Industrial Cyber Security Center of Excellence

令和7年10月24日

vol. 24

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　卒業プロジェクトの取り組み紹介　第2弾

ゲームで掴む！セキュリティのお仕事

背景・課題

セキュリティ人材の不足により、多くの企業でITの知識や経験を持たないままセキュリティ部門へ配属される方が一定数存在しているという現状があります。

一方でセキュリティ部門の業務はIT知識を前提とした専門性の高い業務も多く、初級者には業務イメージが掴みづらいものとなっています。

こうした状況を踏まえ、本プロジェクトでは「ITの経験が無くてもセキュリティの業務イメージがなんとなく掴める楽しいコンテンツを作成する」ことを目的にしました。

課題解決・成果物

成果物はステップ別に分け、「業務を知る」コンテンツとして「セキュリティの業務例一覧」と、「業務を掴む」コンテンツとして「３つのゲーム」を用意しました。

－セキュリティ業務の一覧－

「セキュリティの業務例一覧」では代表的なセキュリティ業務を洗い出し、概要編と詳細編の両面1枚（A3想定）でまとめています。表面は専門知識を使わない形で初級者に分かりやすい説明にし、裏面は詳細化して専門的な業務の説明をしています。

－セキュリティ戦略ボードゲーム セキュる？－

本ゲームはセキュリティ戦略を体験できるボードゲームです。3-5人の協力プレイ型で、利益を最大化するように議論しながら戦略を立てていくものになります。利益だけ追い求めると、インシデントが発生し、せっかく獲得した資産を大幅に減らしたり、最悪の場合倒産する可能性があります。自社のリスクの状況を鑑みて利益追従とセキュリティのバランスを取りながら行動を選択していくゲームとなっています。

－フォレンジック調査ボードゲーム フォレジスト！－

本ゲームはフォレンジック調査を体験できるボードゲームです。3-5人の協力プレイ型で、インシデントの全容を正確に、早く調査するものになります。手元にある簡易的なログから怪しい動きを読み取り、関係者へのヒアリング内容と整合性を確認することで全容解明を目指すゲームとなっています。

－セキュリティ業務体験シミュレーションゲーム シンギュラリティ－

本ゲームはOJTを通して業務体験するといった設定のシミュレーションゲームです。１人からPCでプレイでき、途中で出てくるクイズで正しい選択肢を選んで進めていくものになります。平時の業務の他、インシデントが発生した際の業務も出てくるため、広くどんな業務があるのかプレイしながら掴めるゲームとなっています。

渡邊 晃大さん
（前列右から2番目）とメンバーの皆さん

修了者インタビュー

１番の収穫は？

セキュリティ業務を整理し、モデル化できたことです。セキュリティの業務を洗い出してみるととても幅広く、そして専門性の高い分野であることを再認識しました。今回ゲーム化した業務では「作業」と「価値」を切り分けて考え、単なる「作業」の体験ではなく、「価値」を生み出す行動の体験としてモデル化を意識しており、メンバーがセキュリティ業務の大事なポイントを幅広く学ぶことができたと思っています。

成果物の活用方法

成果物は「セキュリティ業務ってどんなことをするのか」を知ってもらう場面で有効に活用いただけます。学生向けのインターンや新入社員教育でのワークショップで活用いただいたり、セキュリティ以外の部署の方に業務を知ってもらうツールとして活用することもできます。

ゲームとしても楽しいものになっておりますので、シンプルにセキュリティ部署内でコミュニケーション活発化のために活用していただくこともできます。

ここが ICSCoE ならでは！

本プロジェクトは業界を跨いだ共通課題に立ち向かえたと考えております。自動車、電力、鉄道、金融など、幅広い業界のメンバーが意見を出し合うことで業界を特定せずに活用できる成果物が作成できました。

また本プロジェクトは一般の方も参加できるゲーム体験会を開催した他、InteropのIPAブースにて展示・紹介させていただき、我々としてもICSCoEならではの体験をさせていただきました。

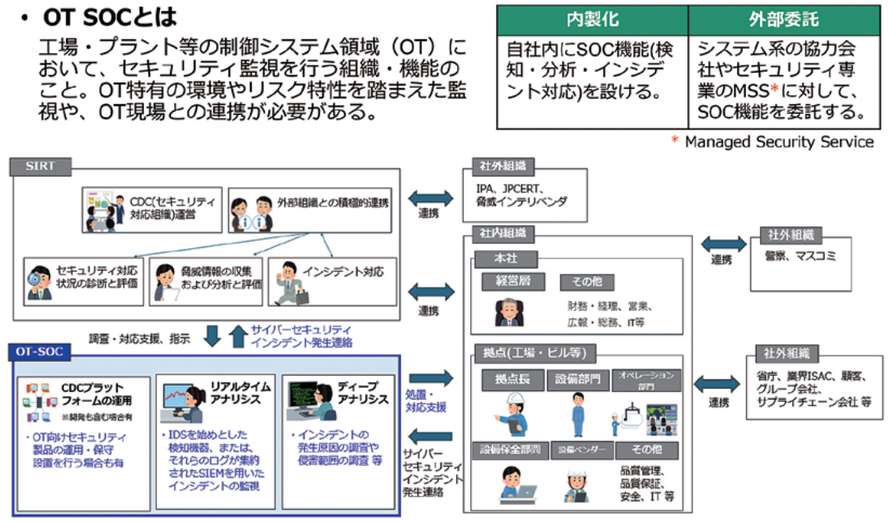
プロジェクトの活動に限らず、ここに来なければ出会うことはなかった講師陣、専門家、そして受講生の方々と非常に綿密で濃い１年間を過ごせたことがなによりの財産となっております。学んだこと、そして人脈をフルに活用しながら、自社のセキュリティのレベルアップに貢献したいと思います。

OT 環境におけるサイバー攻撃監視構築運用ガイド（OT SOC）

背景・課題

近年、OT領域におけるサイバー攻撃リスクが高まっています。従来は外部から隔絶されていた工場やプラントの制御システムも、DXやリモート保守の普及に伴い、ITネットワークやクラウドと接続するケースが増えています。その結果、従来のITセキュリティでは想定していなかった攻撃経路やリスクが顕在化しています。

一方で、OT領域のセキュリティ対策はまだ発展途上であり、IT領域に比べて体系的な知見や実践事例が十分に蓄積されていないのが現状です。その中でも、OT特有のシステム・運用特性を踏まえたSOCの在り方は、多くの企業にとって検討が始まったばかりのテーマです。そこで本プロジェクトでは、OT-SOCの導入および運用に関する実践的な知見を獲得することに着目し、活動を進めました。

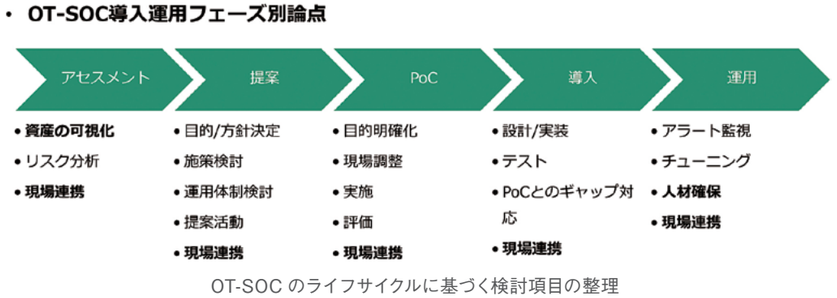


OT-SOC の概念図

課題解決・成果物

本プロジェクトの目的は、OT-SOCに関する知見をプロジェクトメンバーが派遣元企業に持ち帰り、今後のセキュリティ強化に活かすことにあります。そのために、私たちは二つの活動を中心に進めました。

一つ目は、OT-SOCに関与する立場の異なる10社以上への企業ヒアリングです。OT-SOC運用企業に加え、MSSを提供する事業者や監視・可視化ソリューションベンダーにもご協力いただき、実務に携わる方々から課題や対応アプローチを幅広く収集しました。得られた情報は、OT-SOCの導入から運用に至るライフサイクルに沿ってマッピングし、各段階での論点や共通課題を整理しています。こうした整理により、導入担当者が自らの状況を客観的に把握し、次に検討すべきステップを考える上での道しるべとなるよう工夫しました。



OT-SOC のライフサイクルに基づく検討項目の整理