IPA Better Life with IT

ICSCoE Industrial Cyber Security Center of Excellence

ICSCoE REPORT

Industrial Cyber Security Center of Excellence

令和7年8月29日

vol. 23

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1弾

脅威インテリジェンスを活用したセキュリティ強化のためのアプローチ

背景・課題

近年、クラウド、IoT、AIなどの先端技術が急速に導入され、企業の情報システムは利便性を高めると同時に複雑性を増しています。一方で、サイバー攻撃の手法もますます高度化・巧妙化しており、従来のツール依存型かつ受動的な防御モデルだけでは、こうした複雑かつ多様な脅威への対応が困難になりつつあります。

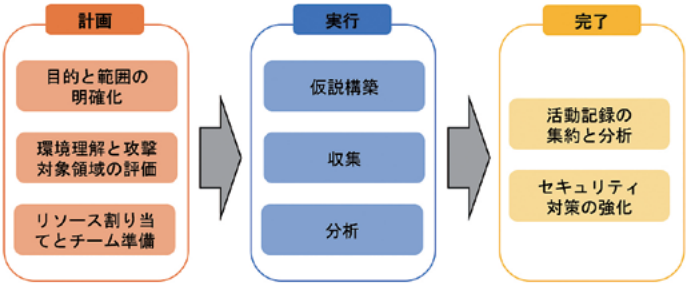
また、SOC（Security Operation Center）では、日々膨大なログやアラートの処理に追われる中で、監視負荷の増大や人材不足といった課題から、重要なインシデントの兆候を見逃すリスクが顕在化しています。加えて、正常な通信を装うマルウェア活動や、未知の手口による攻撃は、既存の検知技術では見逃されやすく、対応が後手に回る恐れがあります。

こうした状況を踏まえ、本プロジェクトでは「脅威ハンティング」に着目しました。これは、システム内部を能動的に調査し、顕在化していない脅威の兆候を探索する手法であり、従来型の防御モデルを補完・強化するアプローチとして注目されています。

本プロジェクトでは、脅威ハンティングを組織の実運用にどう組み込むかをテーマに、理論と実践の両面から検証を行いました。

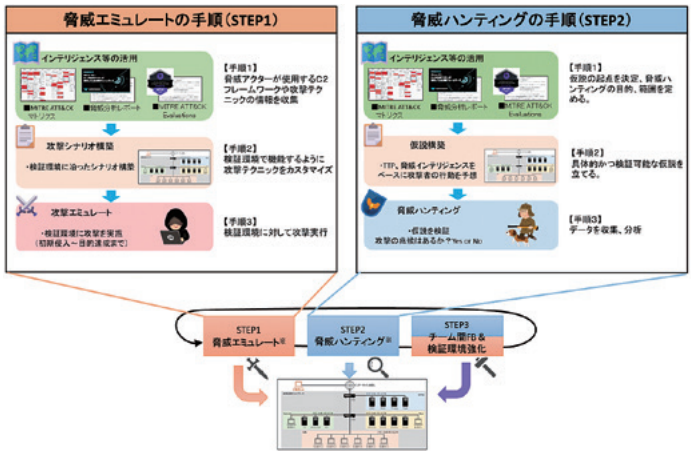
課題解決・成果物

プロジェクト活動においては、まず文献調査を通じて脅威ハンティングの基本概念や仮説構築のプロセスについて理解を深めました。次に、既存のハンティングフレームワークを分析し、それらに共通する主要なプロセスを整理。理解しやすさと汎用性を意識した独自のライフサイクルモデルを作成しました。



プロジェクトで整理したライフサイクルモデル

さらに、模擬環境にて従来のセキュリティ対策を回避する攻撃シナリオを再現し、仮説に基づいて攻撃の痕跡を探索する複数のハンティングアプローチを実践・検証しました。これにより、仮説構築時の留意点や、アプローチごとの特徴といった、実運用に資する知見を得ることができました。



実践検証のイメージ

これらの成果をまとめたレポート『脅威ハンティング実践のすゝめ』では、基本概念から実践手法、組織導入における要点までを体系的に整理しています。

脅威ハンティングの導入を検討している方はもちろん、既存運用の見直しにも役立つ参考資料として活用できることを想定しています。

修了者
インタビュー

尾上 将征さん（前列左から2番目）とメンバーの皆さん

一番の収穫は？

最大の収穫は、「攻撃者の視点」に立つことの重要性を実感できたことです。攻撃者がどのように侵入し、検知技術をどのように回避しようとするのかを理解することで、従来の守る側の視点だけでは見落としがちなリスクにも気づくことができました。こうした気づきや学びは、本プロジェクトを通じて得られた大きな成果であり、今後の自組織のセキュリティ強化に活かせる知見だと感じています。

成果物の活用法

本レポートでは、脅威ハンティングの基本的な考え方や実施手順に加え、プロジェクト活動を通じて得られた知見や検証結果を反映した内容を体系的にまとめています。これにより、実践的な手法やその有効性を理解するための参考として活用いただけることを目指しています。

特に、脅威ハンティングの導入を検討されている方や、既存の監視体制に課題を感じている方にとって、現実的な実践に向けた具体的な方向性や、セキュリティ対策の改善へのヒントとなる内容を提供できればと考えています。

ここが ICSCoE ならでは！

ICSCoEでの1年間は、単なる知識の習得にとどまらず、「自ら考え、試し、形にする」力を実践的に養うことができた貴重な期間でした。多様なバックグラウンドを持つ受講生との知見の共有や、知見豊富な講師陣からの専門的なフィードバックを通じて、セキュリティに対する多角的な視点が身についたと感じています。

中でも、卒業プロジェクトを通じた議論の深まりは、日常業務では得難い学びの場となり、課題解決に向けた柔軟なアプローチや広い視点を得る貴重な経験となりました。今後は、こうした学びを自組織におけるセキュリティ対策や人材育成などに活かしていきたいと考えています。

さらに、セキュリティの重要性がますます高まる中で、ICSCoEで得た知見を業界全体のレベル向上にも役立てられるよう、積極的に貢献していきたいと考えています。個々の組織だけでは対応が難しい課題も多いため、業界全体で連携し、情報を共有しながら取り組んでいく姿勢がこれまで以上に求められています。

今後もこうした視点を大切にしながら、セキュリティの強化に向けた活動を継続していきたいと思います。

企業戦略に基づくセキュリティ戦術の策定　～生成AIとセキュリティガイドラインの考察～

背景・課題

企業のデジタル依存が進む中、サイバー攻撃の高度化により、セキュリティはIT部門だけでなく経営層の課題となっています。しかし、経営層が示す戦略や方針は抽象的になりがちで、多くの現場の担当者はその意図を正確にくみ取り、適切なガイドラインを選定・適用することに苦慮しているのが実情です。

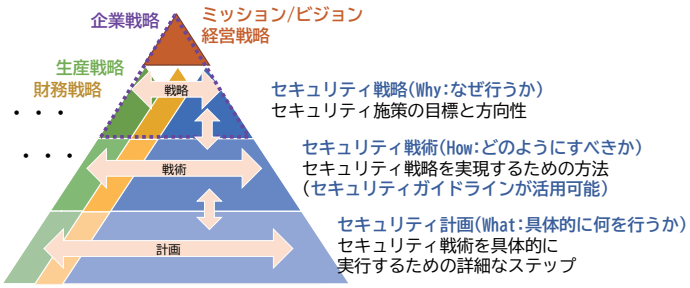
そこで本プロジェクトでは、NIST CSF等のガイドラインや生成AIの活用により、より効果的なセキュリティ戦術策定を目指すための考察を行うことで、実務者にとって実践的な指針となることを目的としました。

課題解決・成果物

本プロジェクトではまず、セキュリティ戦略、セキュリティ戦術が何から導き出されるのかを明らかにしました。

その結果、セキュリティ戦略は、企業全体のミッションやビジョン、そして経営戦略に基づいて策定されるべきものであり、単独で存在するものではないことを再確認しました。セキュリティ戦略は経営戦略から導き出され、経営目標の達成に貢献するものでなければなりません。この関係性は、頂点に「ミッション/ビジョン、経営戦略」、その下に具体的な「セキュリティ戦略」が導出され、さらに「セキュリティ戦術」、そして「セキュリティ計画」へと具体化されていく階層構造として捉えられます。これらの要素は相互に連携し、上位の戦略・方針との整合性を保つことが重要です。

提言として､セキュリティ戦略は経営戦略の達成を支援･推進するものであり、そこから導き出される必要があること、そしてセキュリティ戦術は最終的に経営戦略の実現に寄与すべきであることが挙げられています。



経営戦略と各機能別戦略の関係性

次にセキュリティガイドラインの活用方法について明らかにしました。

ガイドラインは、経営・セキュリティ戦略を具体的なセキュリティ戦術へ落とし込む枠組みであり、単なるチェックリストとは異なるものです。

更にセキュリティに関する用語や考え方を標準化することで、社内外ステークホルダーとの共通理解を促進し、円滑な意思疎通や対外的な信用獲得にも繋がるものです。

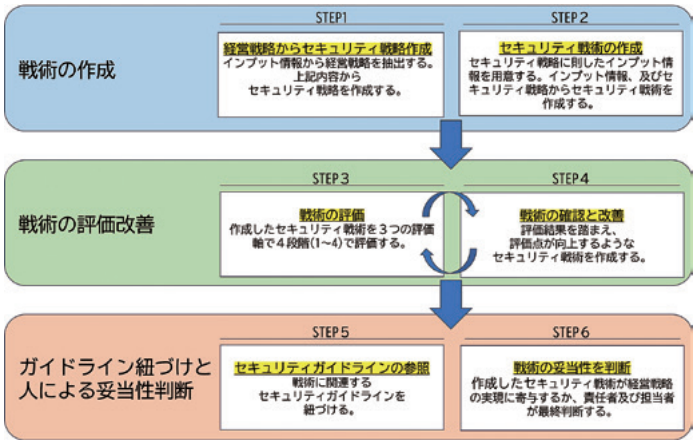
ここまでで、セキュリティ戦略、セキュリティ戦術、及びセキュリティガイドラインについて明らかにしたものの、実業務では多種多様な経営戦略、セキュリティガイドラインがあります。その中で、「情報整理と理解」のための時間短縮のみならず、セキュリティ戦術の妥当性確認のための「第三者による評価」のために、生成AIを活用しました。

その上で、生成AIによるセキュリティ戦術策定について考察しました。具体的には、以下のステップでアプローチしました。

- **STEP１：経営戦略からセキュリティ戦略の出力**
- **STEP２：セキュリティ戦術の作成**
- **STEP３：セキュリティ戦術の評価**
- **STEP４：セキュリティ戦術の確認と改善**
- **STEP５：セキュリティガイドラインの参照**
- **STEP６：戦術の妥当性判断**

本プロジェクトを通して、生成AIがセキュリティ戦術のドラフト作成やアイデア出しに有効であることを確認しました。

このように、生成AIの活用によりセキュリティ戦術のドラフト作成は効率的に、素早く行える一方で、生成AIはインプットに依存すること（想像力の限界）から、生成AIの出力は人間の評価と補完が不可欠であると結論付けました。



生成 AI によるセキュリティ戦術策定作成プロセスの活用例

修了者
インタビュー

川崎重工業株式会社　**神納 実良さん**（左から1番目）とメンバーの皆さん

一番の収穫は？

セキュリティ戦略･戦術について改めて考えることができたのが収穫でした。これまで、企業におけるセキュリティ戦略はセキュリティガイドラインを広く、深く知ることが重要と考えていました。これは重要なポイントではあるものの、真に重要なのは、企業戦略との整合性だったことを発見できたことが一番の収穫でした。また、限られた時間、リソースの中で、生成AIの活用により戦略・戦術の策定に有用であると気づけたことも大きな収穫でした。

成果物の活用法

組織内のセキュリティ戦略・戦術を策定する際に改めて見ていただき、正しく導出できているか、ガイドラインの活用方法について問題がないかセルフチェックをしてもらいたいと考えています。

また、生成AIを活用する際に、どの様に活用するべきか迷ったときに参考としてもらいたいです。

ここが ICSCoE ならでは！

まず、実機を用いた演習を通じて、机上の知識を実践的で「地に足のついた」経験を得ることができました。これにより、単なる知識としてではなく、具体的な対策へと落とし込む力が養われました。

次に、幅広い人脈が形成できたことです。サイバーセキュリティというデリケートな内容について、他社のみならず、一流の講師陣の方々と意見交換や、相談ができたことは他では得難い経験でした。

これらの経験は、自社組織のサイバーセキュリティ強化においてより説得力のある提案ができるようになると考えています。

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