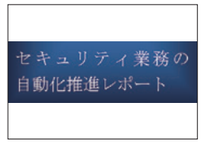
第7期中核人材育成プログラム WEB公開中の卒業プロジェクト

今回ご紹介した他にも一般に活用いただける卒業プロジェクトの成果物を
ICSCoEのWEBサイトで公開しています。ぜひご覧ください。

セキュリティ業務の自動化推進



セキュリティ業務の自動化を進める上で役立つ知識として、戦略的な実施順序や考慮事項、技術的なアプローチ手段についてまとめました。

Visionary Security ～Zeroから始めるセキュリティ対策～

Visionary なスタートアップ企業がより事業創出に集中できるよう、業界の特性に応じた市場に刺さりやすくなるためのセキュリティ対策などを整理し、動画を作成しました。

脆弱性対応におけるリスク評価手法のまとめ（脆弱性対応管理PJ）

脆弱性対応管理業務におけるリスク評価に着目した内容をまとめました。当該業務の工数を削減するためには、優先度を考慮した適切なリスク評価が必要です。本書では、CVSS や EPSS 等の各リスク評価指標の特徴・役割および運用例を記載しています。

実務者のためのサプライチェーンセキュリティ

自社のサプライチェーンセキュリティにこれから携わる方や、サプライチェーンセキュリティの推進に悩まれている方を対象に、サプライチェーンセキュリティに関する考え方や取り組みの流れについて整理しました。

448時間かけて分かったセキュリティルールに感じる“もやもや”の正体とは？（By 侵入と対策の研究プロジェクト）

「情報セキュリティルール」こんな言葉を聞くと守らなきゃいけない固い存在に感じませんか？理由がわからず「守らされている」という状態では「もやもや」を感じる方もいらっしゃるでしょう。そんな「もやもや」に注目し「すっきり」解消したい、と考えて本書を作成しました。

セキュリティ啓発コンテンツ（インシデント演習・IoT/DXに関するセキュリティ対策）

防御・対応の観点から、以下の２つの啓発コンテンツを作成しました。
(1) インシデント対応における情報連携にフォーカスしたカードゲーム
(2) IoT やDXに関するサイバー被害と対策を学ぶカードゲーム

制御システムへのリモートアクセスに関するセキュリティ対策指南書

制御システムへのリモートアクセスを安全第一に導入・運用するために、企業アンケートから課題を整理し、リモートアクセス方式、リスク分析手法、セキュリティ対策、システムの検討プロセスなどを「指南書」としてまとめました。

セキュリティ・バイ・デザイン「システム開発のセキュリティ向上0.0」

主に設計開発者・品質保証担当者向けに、システム開発チームの初学者向けのセキュリティ教育ドキュメントを作成しました。ありがちなミスがセキュリティ事故に繋がるアンチパターンや、セキュリティ・バイ・デザインを実践する上でやってはいけない事を学べます。

セキュリティ・アクション・ラボ ～実践的な学びのためのプロジェクト～

社員のセキュリティ意識・知識向上に悩んでいるIT システム関連企業のために、「環境構築から疑似攻撃、セキュリティ対策まで一貫して実践できる研修コンテンツ」及び「セキュリティインシデントの被害を被った後の自分を疑似体験できる啓発漫画・動画」を作成しました。

サイバーレジリエンスのためのコミュニケーション

サイバーインシデントに対して迅速かつ柔軟な対応をするために、セキュリティ担当者が意識するべきコミュニケーションの取り方について整理し、「サイバーレジリエンスのためのコミュニケーション ～セキュリティ担当者に必要なコミュニケーションスキル集～」を作成しました。

戦いの原理・原則とサイバーセキュリティ ～軍事のフレームワークと攻撃者の視点を参考に適切なセキュリティ対策の考え方を理解する～

軍事組織のフレームワーク「戦いの原理・原則」をサイバーセキュリティに適用した冊子を作成しました。複雑化するサイバーセキュリティの環境において、自分で考え行動する力を身に付けたい方、サイバー攻撃者の理解を深めたい方にご一読いただきたいです。

SBOM導入・運用の手引き

実務者が SBOM を導入・運用する際の実施事項、ノウハウをまとめました。ガイドラインでは、各フェーズにおける実施事項をチェックリストとしてまとめています。

クラウドセキュリティ（クラウドセキュリティの歩き方）

クラウドのセキュリティ向上を目指し、ポータルサイト「クラウドセキュリティの歩き方」を公開しました。ガイドラインを一元化・可視化し、ユーザーが迅速にニーズに合ったガイドライン等へアクセスできるようサポートします。

Webページでの閲覧は

中核人材育成プログラム 卒業プロジェクト　検索

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

Industrial Cyber Security Center of Excellence

令和7年3月28日

vol. 21

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

第７期中核人材育成プログラム　卒業プロジェクトの取組み紹介

脅威インテリジェンス導入・運用ガイドライン作成プロジェクト

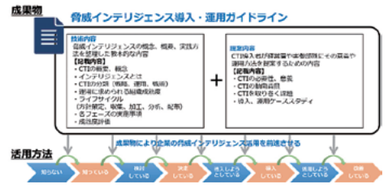
▶背景・課題◀

昨今の脅威の複雑化や産業活動のシステム化に伴い、脅威をベースとしたセキュリティ対策を実施する脅威インテリジェンス*（CTI：Cyber Threat Intelligence）がホットワードの1つとなっています。多くの企業はまだ脅威インテリジェンスの実態を把握しきれていないのが現状ですが、脅威インテリジェンスの活用を促進することは、日本の重要インフラ企業にとって大きな課題となっています。そこで本プロジェクトでは、脅威インテリジェンスの実態と運用方法、活用方法を整理し、導入・運用を支援する「脅威インテリジェンス導入・運用ガイドライン」を作成しました。

*サイバーセキュリティに関する脅威情報を収集・加工し、またそれらを分析することによって得られるインテリジェンスに基づく組織のセキュリティ対応における意思決定のライフサイクル

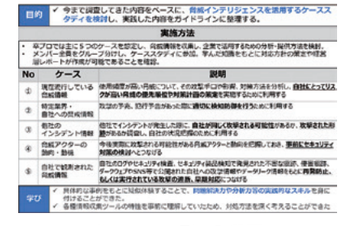
▶課題解決・成果物◀

ガイドラインの作成に当たっては、文献調査や輪読会を実施して脅威インテリジェンスの最新動向を把握するとともに、企業の脅威インテリジェンスの実施状況や抱えている課題を把握するためヒアリングを実施し、より実用的なものとなるよう努めました。今回作成したガイドラインは、概念や実践的な内容（技術内容）に加えて、脅威インテリジェンス運用者（導入担当者）が経営層や実働部隊にその効果や目的、実施方法を具体的に示す提案内容を含めたものとなっています。本ガイドラインを活用することで、企業が抱える課題を解決するとともに、脅威インテリジェンスの活用を次の段階へ前進させることを目標としています。(右上図参照)



ガイドラインの構成

上記で調査した内容をベースに、脅威インテリジェンスを活用するケーススタディを検討し、ガイドラインに整理しました。今回は５つのケースを想定していますが、過去のインシデント事例を元に検討することで、実業務に落とし込んだ時の具体的なフローを提示することができました。脅威インテリジェンスを自社の業務に落とし込む際の課題を発見したり、体制面・運用面の具体的なイメージをすることができるので、ぜひ活用いただきたいと思います。



ケーススタディの概要

修了者インタビュー

関西電力株式会社
二本松 立朗さん

一番の収穫は？

新規でガイドラインを作成した経験が大きな収穫となりました。現在までのところ、国内で標準的に利用されているガイドラインはあまり見受けられないため、どのように情報や経験を落とし込んでいくべきかなど、作成は困難を極めましたが、何とか完遂することができました。調査・ヒアリングを通して自身やプロジェクトメンバーの知識の底上げにもなりましたし、脅威インテリジェンスの導入が今後自社だけでなく、業界内で進んでいけばと考えています。

成果物の活用法

脅威インテリジェンスを自社の業務に落とし込む際の課題発見や、体制面・運用面の具体的なイメージをすることができたので、帰社後は実際の業務に盛り込んで活用していきたいと考えています。一方で、自社で効果的に活用するには「人材確保」「組織的な体制構築」の両面で課題が多く、難易度がかなり高いと感じているので、より多くの関係者で協力して進めていきたいと考えています。

ここが ICSCoE ならでは！

人脈の広さが ICSCoE ならではと感じました。プロジェクト序盤、脅威インテリジェンスの企業への浸透性についてチームで調査をしていた際、文献調査だけではなかなか実態が分からず悩んでいたことがあったのですが、メンターの先生方に相談したところ、実際に脅威インテリジェンスを導入している企業の担当者だけでなく、この分野の参考書を執筆されている著名な先生もご紹介いただきました。このつながりから、ガイドライン作成に関する意見交換をさせていただき、成果物のレビューにもご協力いただくことができました。このような関係構築は、自社の業務に従事しているだけではなかなか実現することができなかったと思います。

鉄道業界のサイバーセキュリティ強化し隊 ～気づいて守ってヨシ！～

背景・課題

近年、サイバー攻撃の被害は増加の一途をたどり、従来安全といわれていた制御システムにおいてもサイバー攻撃の対象となっています。海外では鉄道システムに対するサイバー攻撃が多く発生しており、今後日本においてもサイバー攻撃を受ける可能性が十分に考えられるものの、現状十分な調査体制（組織・解析環境）が整備されていません。本プロジェクトではこれらの背景から、「許容できない事象」に着目し、リスク分析からセキュリティ対策までの検討手段を示した「サイバーセキュリティ強化書」、サイバー攻撃発生時の検知・対応・復旧に必要な技術面・組織面における課題抽出を行う「サイバー攻撃に備えたログ活用のすゝめ」の２点を制作しました。

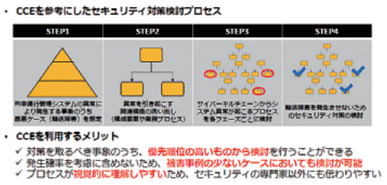
課題解決・成果物

○サイバーセキュリティ強化書

鉄道分野では、セキュリティ対策についてガイドラインによる網羅的な管理策の提示はされていますが、必要な対策について優先度を考慮して実施できていない場合があります。「サイバーセキュリティ強化書」では、リスクベースアプローチである CCE [*1] をベースに、列車運行管理システム [*2] のリスクの洗い出しからセキュリティ対策の立案まで検討し、鉄道分野のセキュリティレベル向上を図りました。

[*1] Consequence-driven Cyber-informed Engineering：2016 年にアイダホ国立研究所が開発したセキュリティ対策検討手法

[*2] 計画ダイヤを基に各種システムなどを一括管理・制御するコンピュータシステム

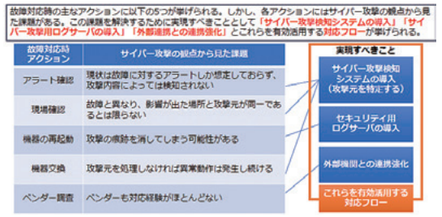


リスクベースアプローチによるセキュリティ対策

ここでは許容できない事象を「列車運行管理システム異常による輸送障害」と定め、リスク分析からセキュリティ対策までの検討プロセスを STEP 別に示しました。立案したセキュリティ対策については、費用、労力、技術的実現性および効果の４つの観点でスコアリングし、セキュリティ水準に応じた対策が行えるよう優先順位付けを行いました。また、本書では、ガイドラインに抽象的に記述されたセキュリティ対策項目について、一部を具体化して提示することにより、対策が取り組みやすくなるよう工夫しました。

○サイバー攻撃に備えたログ活用のすゝめ

現状の鉄道制御システムには、システムに異常動作が発生した場合に、サイバー攻撃と機器故障を見分けることができないという問題、また制御システムへのサイバー攻撃の対応フローが明確でないという問題があります。本資料には、鉄道制御システムが攻撃を受けた場合に、それがサイバー攻撃であると判断し、適切に対応するための提言を、技術面･組織面の両面から記載しています。



サイバー観点から見た故障対応の課題と実現すべきこと

現在の鉄道業界では、現場の担当者だけでなく、セキュリティ部門や保守ベンダー含めて、各関係者が相互に情報共有・連携をしながら運用を行っています。本プロジェクトでは、この運用の中でサイバー攻撃に対応するために、攻撃の検知やログを採取できるような装置を導入し、これらを有効活用するインシデント対応フローを作成しました。このフローでは、これまで明確にできていなかった、どうなったらサイバー攻撃といえるのか、対処後はどのタイミングで通常運用を再開すればよいのか、といったことを見える化しています。また、作成したフローを用いて、実際に鉄道業界で起こり得る攻撃シナリオを用いた演習を実施しました。演習のフィードバックを取りまとめることで、より多様なシナリオに対応できるようフローの改善を実施しました。

修了者インタビュー

阪急阪神ホールディングス株式会社
久保 貴司さん

一番の収穫は？

実機のシステムを使って検証できたことが一番の収穫でした。自社のシステムでは試せないことを実施し挙動を確かめられたことは、非常に貴重な経験でした。また、プロジェクトリーダーを経験できたことも大きな収穫でした。これまで自社ではマネジメントを経験したことがなかったのですが、自分の業界に特化したプロジェクトでリーダーを経験することで、今後の業界に生かせる良い機会になったと感じました。

成果物の活用法

サイバーセキュリティ強化書は、自社や業界内の関係各所でセキュリティ対策を検討する際に使用していきたいと考えています。サイバー攻撃に備えたログ活用のすゝめは、まずは自社でインシデント対応の演習を行う中で使用したいと考えています。いずれの成果物も、多くの関連部門に共有し、更にはよりその効果を高めるため、自社にあったものにカスタマイズしていければと考えています。

ここが ICSCoE ならでは！

各専門分野の先生方にお話を聞けたことや、他社・外部機関との連携など、人脈の広さに大変恩恵を受けました。自社で業務に従事しているだけでは、他社の経営層など決定権を持つ方々と繋がりを持つようなことは難しく、非常に良い経験となりました。また、受講者は様々な業界から派遣されているため、鉄道以外の業界の最新情報を共有いただくことができたのは非常に有意義だったと思います。業界が違うとセキュリティ対策方法も大きく異なることが理解できましたし、特に電力やガス業界の話題は、鉄道業界にとって大変示唆に富むものでした。

生成AIのセキュリティリスクと対策 ～今、企業に必要なガイドラインとは？～

背景・課題

JIPDEC の調査によれば、69.5% の方が勤務先企業にて生成 AI を使用している、または導入を進めていると回答しており、今後もより多くの企業で導入されていくことが想定されています。しかし一方で、現在の日本企業では、生成 AI の導入に関するルール整備があまり進められていません。また、生成 AI を活用する際には様々なセキュリティリスクがあり、リスクを適切に把握・軽減することが重要になってきます。これらの背景から、本プロジェクトでは企業のセキュリティリスク低減を目的とした、テキスト生成 AI 導入・運用ガイドラインを策定することとしました。

課題解決・成果物

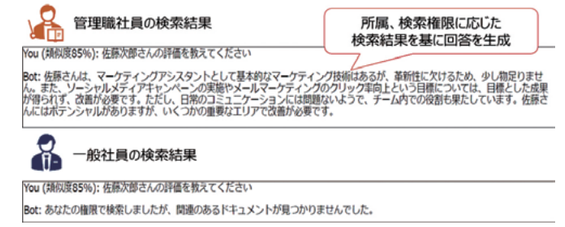
本プロジェクトでは大きく分けて、①セキュアな生成 AI 構築の検証、②テキスト生成 AI 導入・運用ガイドラインの策定を行いました。

生成 AI におけるセキュリティ対策は、既存のセキュリティ対策と同様、多層防御の考え方が重要となりますが、①セキュアな生成 AI 構築の検証では、LLM [*1] セキュリティガードレールの効果と、メタデータを活用した RAG [*2] における情報アクセス権限管理の有効性を検証しました。前者については、ガードレールを用いることで、LLM が本来は回答できない悪意のある質問等に対しても回答してしまう、敵対的プロンプト [*3] などの攻撃に一定の効果があることを確認できました。また後者では、同じ質問でも、管理職や一般社員など、質問する人の役職によって回答結果を変化させることが可能であることを確認できました。

[*1] 何十億、何百億もの文章データから学習を重ねることで、人間並みの自然な言語の理解と生成が可能になった AI のモデル

[*2] 外部ソースを LLM に渡して回答の精度を高めるために使用される

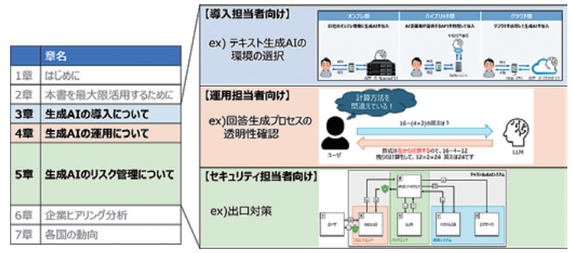
[*3] ユーザーが会話でモデルを誘導し、本来なら意図しない結果を生成するようなプロンプト



メタデータを活用した RAG を使用した際の同一質問に対する回答例

②テキスト生成 AI 導入・運用ガイドラインの策定に当たっては、はじめに生成 AI を導入済みの企業や自治体にヒアリングを行い、脅威と感じているリスクや共通の課題をまとめるところから着手しました。ヒアリングの結果から、企業は情報漏洩とハルシネーション [*4] によるリスクを重要視すること、共通課題としては、利用率や期待値コントロールなど、ユーザの生成 AI の理解度・認知不足による課題が多いことなどが分かっており、ガイドラインはこれらの悩みを解決できるような内容としました。なお、本ガイドラインは生成 AI を導入する利用者向けとしておりますが、中でも導入担当者・運用担当者・セキュリティ担当者の３つの観点で、それぞれの担当者が考慮すべきこと、他の担当者と連携すべきことについて記載しています。

[*4] 生成 AI モデルが事実とは異なる不正確な回答を生成する問題



ガイドラインの内容ピックアップ

修了者インタビュー

一番の収穫は？

私はこれまで、普段の業務でAI を取り扱う機会はなく、ICSCoE7 期生全体で見ても AI を業務で取り扱っている方はいなかったのですが、卒業プロジェクトを通して AI を深く学ぶ機会をいただき、知見を深めることができたことは大きな収穫だったと考えています。特に、実際に生成 AI を動かして体験しながら学ぶことで、座学だけでは得られない、より実践的な技術を習得することができました。また、プロジェクトのリーダーを務めることができたことも大きな収穫でした。社会人になってからプロジェクトをまとめた経験等はなく、リーダーとしての在り方など分からないことだらけでしたが、失敗してもよい、ここなら色々なことに挑戦できると考え立候補しました。ガイドラインをより多くの人に使っていただくため、様々な企業や自治体、また多方面の業界から派遣されている受講者など幅広くヒアリングを行い、それらをまとめることに努めましたが、実際はメンバーに助けられた部分も多かったです（笑）。プロジェクトでのこれらの経験が、今後の活動につながればと考えています。

成果物の活用法

まずは、ガイドラインを自社や関係者で利用いただくことを想定しています。生成 AI サービスに関する大規模な被害事例は現時点で限定的ですが、潜在的リスクは徐々に認知されつつあり、今後セキュリティ対策の重要性がさらに高まることは確実です。本書を活用いただくことで、早期から適切な対策を講じる一助としていただければと考えています。

株式会社オプテージ
辻村 凱さん

ここが ICSCoE ならでは！

多くの企業や自治体など、関係する方々へ広くヒアリングをすることができたのは、メンターの講師や IPA 含めた様々な人脈のおかげで、ICSCoE ならではだと思います。特に、ヒアリング先に悩んでいた際、ICSCoE の人脈から経済産業省の担当者へ直接ヒアリングの機会をいただけたことは大変大きく、企業等とは違う観点でご意見をいただくことができました。いただいたコメントを盛り込むことで成果物の完成度を大きく高めることができ、大変感謝しています。