第5期中核人材育成プログラム 卒業プロジェクト

ログ分析・SIEM

背景・課題

ログ分析は、セキュリティインシデントの発生時に被害状況と攻撃経路を明確にすることで、被害拡大の抑制や、再発防止策の提案を実現できます。

一方で、ログ分析を自組織に取り入れる際には「TCP/IPの基礎スキルを有し、さらにレイヤーをまたがって幅広い知識を持った人材が必要」「手作業でのログ分析では時間的に限界がある」といった課題が見受けられます。

そのような課題を踏まえ、下記の２つを目標に据えて当プロジェクトを開始しました。

- ログ分析の基礎となる様々なレイヤーのITスキルを身につけ、複数のNW・セキュリティ機器のログからインシデントの痕跡を発見できるようになる。
- ログ分析ツールSIEM*の導入判断及びルール検討ができるようになる。

*SIEM（Security Information and Event Management）
各種機器やアプリケーション等から集められたログ情報に基づいて、異常があった場合に管理者に通知したり対策を知らせたりする仕組み

課題解決・成果物

「ハンズオンによって知見を深めたい」という大きな方針の下で学習を進めました。

取り組みプロセス

1. **基礎学習**：書籍や文献から情報収集
2. **模擬ネットワーク構築**：実践環境の構築
3. **ペネトレーションテスト**：攻撃シナリオを検討、実行
4. **ログ分析実践**：ログを調査し、攻撃の痕跡を記録
5. **SIEM実装・検知ルール検討**：分析結果を元に検知ルールを考案・実装・検証

取り組みの結果、成果物として２つの資料を作成しました。

標的型攻撃に対するログ活用ツールの活用方法

ペネトレーションテストにおける**手動でのログ分析の方法**と、SIEMやEDR*を活用することによって**自動的・効率的にログを確認する方法**をまとめました。ログ分析の初級者に向けて足掛かりとなる資料としています。

*EDR（Endpoint Detection and Response）
コンピュータシステムのエンドポイントにおいて脅威を継続的に監視して対応する技術

ログ連携・SIEM検知ルール設定手順書

フリーソフトのSIEM製品を使用し、ログ連携や検知ルールを設定する方法をまとめました。**運用者向けにログ連携に必要な手順を提供**するとともに、セキュリティ担当者向けに**SIEM検知ルールの考え方と実装方法を提供**する資料になっています。実際のSIEM導入・検証に役立てられることが期待されます。

修了者インタビュー

株式会社オプテージ
佐治 勇樹さん

一番の収穫は？

ITスキルを幅広く学べたことです。今回、サーバを構築してネットワークをつなぎ、SIEMをインストールするなど、環境構築から検証まで一通り自力で行いました。自社ではCSIRTとして幅広い分野の相談を受けることがありますが、その経験のおかげでシステムについて一貫したイメージを持ちながら対応することができています。

成果物の活用法

例えば、ログ分析の初学者の教育や、実務者間の認識合わせに使うことができます。私も新任の後輩に対しての説明に使用します。また、設定手順書にはフリーソフトのSIEMを動かすための方法をまとめているので、商用SIEM導入の検討中の段階に活用できます。

ここがICSCoEならでは！

一番は他のメンバーとのつながりができたことです。通常、社会人になったら1年間同じメンバーと学習するということはあり得ないです。決して表面的ではなく、深いところで話せる人脈が構築できました

また、プログラム全体を通して、スキルが飛躍的に向上し、「自社に貢献していける」「主体的に関わっていける」と感じられるようになりました。その意識の変化もICSCoEならではだと感じます。

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

IPA Better Life with IT
ICSCoE Industrial Cyber Security Center of Excellence
ICSCoE REPORT
令和4年11月21日
vol. 13

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

第５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５期は21件のプロジェクトがあり、そのうち3件をご紹介します。

セキュリティエンジニアのための English Reading

背景・課題

サイバーセキュリティの世界の特質として「変化が早い」「国境がない」という2点が挙げられ、セキュリティエンジニアにおいては世界中の情報を早く的確に利用する必要があり、英語の読解力が不可欠になっています。

その一方で我が国のセキュリティエンジニアの多くは英語に苦手意識を持っているという現状が見受けられます。本プロジェクトは、セキュリティエンジニアの**英語読解力の意欲・能力向上**を目指して企画されました。

課題解決・成果物

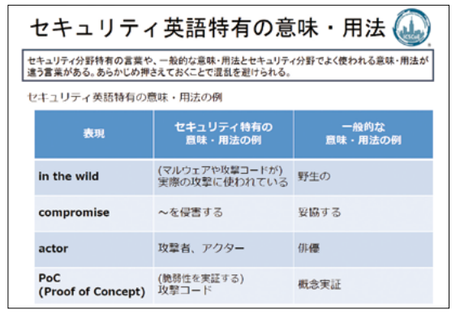
今回は特に、世界中の情報を的確に収集し、実務に活用できる「**情報収集力**」と、英語で得られる豊富な情報を活用し、エンジニアとしてさらに能力向上できる「**成長力**」の2つの力を向上させることを目指し、２つの成果物を作成しました。

英語読解力向上のための学習ガイド

英語の読解力、情報収集力向上のための様々なヒントを凝縮した資料を作成しました。

英語学習を3つの柱でモデル化

「Awareness」「Practice」「Training」の3つの柱で英語の学習をモデル化して、能力向上への道筋を解説しています。



資料の内容　英文を読むための様々なコツをまとめています

セキュリティ英単語集

セキュリティエンジニア向けに特化した英単語集を作成しました。海外のセキュリティニュース記事を分析し、出現数や使われ方を考慮して頻出の330語あまりを厳選しています。さらに実際の記事での使われ方に基づき、訳語と使用例を作成しているので、すぐに実務に役立てることができます。

単語集はPDFファイルの他、CSVファイルでも作成しているため、アプリケーションに取り込むなど様々な方法で暗記学習に活用することが可能になっています。

特徴１　セキュリティニュースで「実際に使われている」単語を厳選
特徴２　セキュリティならではの意味・使用例を掲載

動詞

単語	意味	関連語	使用例
include	～を含む	【名】Inclusion: 包含、含まれるもの 【形】Inclusive: すべてを含んだ	the email including a malicious macro 悪意のあるマクロを含むメール
steal	～を盗む		steal sensitive information 機密な情報を盗む
exploit	(脆弱性)を突いて攻撃する 【名】エクスプロイト(コード)	【名】exploitation: (脆弱性を突く)攻撃 【形】exploitable: 悪用可能な	actively exploited vulnerability 広く攻撃に使われる脆弱性
release	～を入手可能な状態にする 【名】(記事やプログラムの)リリース		update released today 今日リリースされたアップデート
target	～を標的とする 【名】標的	【形】targeted: 狙われた、標的型の	targeted attack 標的型攻撃
allow	～を可能とする、許可する	【名】allowlist: 許可リスト	the bug allowing attackers to execute arbitrary code 攻撃者に任意のコード実行を許すバグ

「セキュリティエンジニアのための English Reading」はICSCoEのWEBページでも紹介しています。ガイド資料、英単語集をダウンロード可能です。また、当プロジェクトはWEBニュースでも紹介されました。

https://www.ipa.go.jp/icscoe/program/core_human_resource/final_project/english-reading.html

第5期中核人材育成プログラム 卒業プロジェクト

制御システムのペネトレーションテストのノウハウ習得

背景・課題

たった一度のサイバー攻撃の成功も許容されない重要インフラにおいて、ペネトレーションテスト（以下、「テスト」）はリスク評価の有効な手段となっています。一方、その効果はテスターのスキルに大きく依存するという課題があります。

当プロジェクトでは「ICSCoEだからこそできること」と「帰任後の業務に直結すること」に取り組みたいといった観点から、OTに対するテストのノウハウ習得をテーマにしました。

ICSCoEだからこそできること	•模擬プラントの利用 •テストシナリオの作成・実行 •有識者からの高度なアドバイス
帰任後の業務に直結すること	•テスト計画／評価の目利き力 •テストシナリオ作成のノウハウ •テスト項目の実行スキル

課題解決・成果物

今回のプロジェクトの主な目的は

- テスト業務を推進または実行するために、テストシナリオ作成の勘所やテスト計画／評価の目利き力、およびテスト実行スキルを習得する
- テスト業務担当者へ知見を共有し、組織的に活用するためのノウハウを作成する

として、以下の５つのステップで知見を深め、成果物の作成に取り組みました。

STEP 1 基礎学習

まずは限られたプロジェクト期間の中で、メンバー間で建設的かつ具体的な議論を行うためには、基礎知識を持つことが必要と考えました。基礎知識・スキル習得のために、資料（NIST SP800-115やMITRE ATT&CK for ICSなど）を用いた**勉強会やIT系でのテスト体験を実施**しました。

STEP 2 テスト計画書／報告書作成

テスト計画書および報告書作成のための基礎知識を学びました。その際に、テストの難しさを認識するとともに実践的な気付きを得るために、ICSCoE秋葉原拠点にある**模擬プラント（電力システム）を活用**しました。

テストに使用した模擬プラント

STEP 3 テストシナリオ作成・実行

フレームワークの一つであるCCE*を活用してシナリオを作成し、テスト計画書に反映しました。また、**模擬プラントに対して実際にシナリオを実行**し、その結果についてテスト報告書を作成しました。

*CCE（Consequence-driven Cyber-informed Engineering）
発生してほしくない事象からテストシナリオを作成する米国アイダホ国立研究所が開発した手法

STEP 4 テスト項目検証

高度で効果的なテストを実現するために、より多くのテスト項目を選択肢として持つことを目指しました。模擬プラントを利用して様々なテスト項目を検証し、試行検証する中で、**テスト項目の実行方法や実行時の注意点について習得**し、テスト項目集にまとめました。

テスト項目集の一例

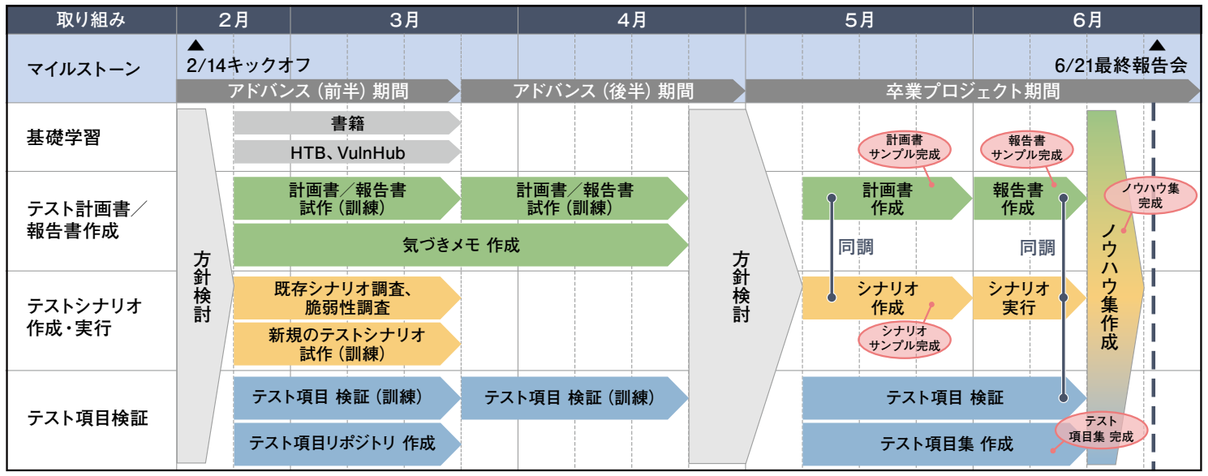
STEP 5 ノウハウ集作成

知識・スキルの定着化を図るとともに、共有可能な状態にするため、**テスト計画書・報告書やテストシナリオを実際に作成・実行することを通じて獲得したノウハウをまとめてノウハウ集を作成**しました。実際のテスト時にはノートのように参考にして活用することを想定しています。内容にはシステム管理者、テスト管理者、テスト実施者の異なる3者の視点から見た注意事項も記載しています。

成果物一覧

- テストノウハウ集
- テスト項目集
- テスト計画書のサンプル
- テストシナリオのサンプル
- テスト報告書のサンプル

プロジェクトの完成まで



修了者インタビュー

一番の収穫は？

プラント実機を使用したハンズオンを通して、テストの具体的なイメージを持てたことです。これまでの業務ではマネジメントの立場から、必ずしも細かな技術的な内容など把握しきれているわけではありませんでした。今はそういったところも理解した上で全体を見られるようになりました。

成果物の活用法

成果物はさっそく社内に展開しています。更にノウハウやテスト項目など、今回のプロジェクトで得たノウハウで社内の資料を更新しています。また、プロジェクト発足時、必ずしもテストに詳しいメンバーで始めたわけではなく、丁寧に理解を進め、資料を作成していったので、成果物のターゲットである新人や若手社員の教育に活用できます。

ここが ICSCoE ならでは！

やはり、模擬プラントと先生の存在です。

一般的に、自社に実践的にテストを演習できるプラントは無いと思います。今回、模擬プラントを使って何度も試せたからこそ、本当に価値のある知見を得られました。

また、プロジェクトを進める上で、テストのプロである先生方から助言や提案いただいたことは全て試そうと思って取り組みました。その結果、自分たちの予測だけでは決してたどり着けない深みのある知見を得ることができました。

帰任後の感想

一年学んだことで、サイバーセキュリティのエキスパートになったという手ごたえが得られ、自身のキャリアで大きな分岐点となったと感じています。セキュリティに携わる者として新しいスタートを切ったと思い、帰任後の業務に挑んでいます。

プロジェクトメンバーの皆さん