第4期中核人材育成プログラム

卒業プロジェクトの成果物をWEBサイトで公開中

セキュリティ意識の向上などに一般に活用いただける卒業プロジェクトの成果物をIPAのWEBサイトで公開しています。ぜひご覧ください。

ドローンセキュリティ

急速に普及するドローンを安全に利活用するため「ドローンセキュリティハンドブック」を作成しました。本ハンドブックでは、歴史や基礎的な機能／仕様・法規制・利活用シーン・事故／攻撃と防御事例の紹介、さらにサイバー攻撃（脆弱性）とその対策を検証し、安全に利活用するための勘どころについて取りまとめました。ドローンのSafetyとSecurityの重要性を認識するきっかけとなることを期待します。

カッコいいセキュリティ実行委員会

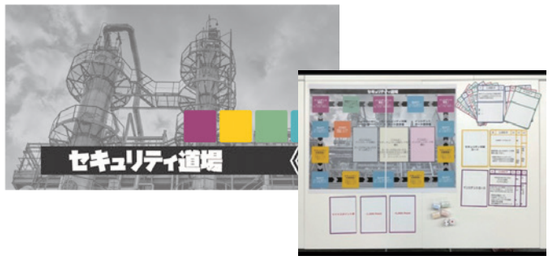
これからの社会全体のセキュリティ意識向上のため、子供たちにサイバーセキュリティについて知ってもらいたいという思いから漫画「エブリデイゼロデイ」を作成しました。専門用語もわかりやすく漫画で表現し、子供たちが楽しみながら読むことでサイバーセキュリティに興味を持つきっかけとすることができます。

ゼロトラストという戦術の使い方
～情報系・制御系システムへのゼロトラスト導入～

「ゼロトラスト」を企業に導入する際の一助となる「ゼロトラスト導入指南書」を作成しました。「ゼロトラスト」で用いられる機能について実際に環境を構築し、システムへの導入検証を実施したことで得られたノウハウをまとめました。また、一般的には情報系システムへの導入を前提として考えられており、制御系システムへの導入は難しい（メリットがない）と思われています。制御系システムについてもIoT機器やクラウドなど、情報系システムとの接続要件がゼロトラストの導入を有効と考え、制御系システムへの導入検証および考察も実施しました。

セキュリティ道場

IoT機器の導入やDXが推進され、産業用制御システムに対するセキュリティの重要度が増す中、工場全体でのセキュリティ意識は十分ではありません。そこで「工場に配属されたばかりの新任の方」などにセキュリティ入門のための教材となるようにクイズ形式のボードゲームを製作しました。楽しく繰り返し学べますので、新入社員研修やセキュリティ教育などに是非ご活用ください。



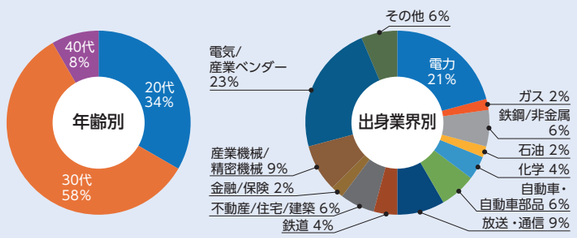
安全・安定操業を脅かした事例10選

制御システムのセキュリティについて考える第一歩となるように「安全・安定操業を脅かした事例10選」を作成しました。国内外で発生した制御システムへのサイバー攻撃の中から10の事例を紹介し、発生する可能性のある被害について解説しました。また、最後に「現場でできる、サイバー攻撃への対策」を紹介しました。是非、制御システムのセキュリティ教育にご活用ください。

▶IPA産業サイバーセキュリティセンター
中核人材育成プログラム 卒業プロジェクト
https://www.ipa.go.jp/icscoe/program/core_human_resource/final_project.html

第5期中核人材育成プログラムが開講

2021年7月、中核人材育成プログラムの第5期が開講しました。サイバーセキュリティ分野における日本の将来を担う中核人材を目指し、様々な業種・業界より48名の受講者がプログラムに参加します。



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3年11月1日
vol. 11
ICSCoE ReportはICSCoEの活動を皆様にご紹介する広報誌です。

第4期中核人材育成プログラム

卒業プロジェクト特集 第2弾

46名の受講者が、15のプロジェクトに取り組みました。前号から引き続いてプロジェクトの一部を紹介します。

ICSペネトレーションテスト評価項目・手順作成

背景・課題

海外ではすでに重要インフラや産業基盤に対するサイバー攻撃が頻発し大きな被害が発生しています。我が国においても工場など産業用制御システムが活用されている企業では、機微な情報を守るため企業グループ内で「ペネトレーションテストを内製化したい」といった要望があります。しかし、現在我が国では標準的なテスト手法がなく、発注者は「指定すべきテスト項目がわからない」、受注者は「具体的なテスト実施方法がわからない」といった悩みがあります。

このため、産業用制御システムにおけるペネトレーションテストの方法を明らかにすることが課題になっています。

課題解決・成果物

今回、発注者及び受注者双方が具体的なテスト手順を明らかにし、テスト内容について共通認識を持つために「テスト項目一覧表」と「個別テスト手順書」を作成しました。

1. テスト項目一覧表

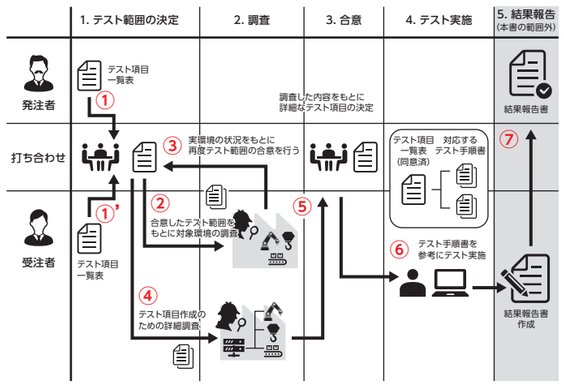
「テスト項目一覧表」作成にあたり、産業用制御システムにおけるペネトレーションテストに関して参考となるガイドラインやナレッジベースなどを調べ、攻撃者の戦略や攻撃手法が体系的に整理されている米国MITRE社の「ATT&CK® for ICS」を参考にして、産業用制御システムのペネトレーションテストで実施すべき項目を一覧表にしました。

テスト項目の目的、技術の概要をわかりやすい表現で記載し、**テスト項目を設定する際に発注者及び受注者双方でどのような項目があるかを確認**できます。

2. 個別テスト手順書

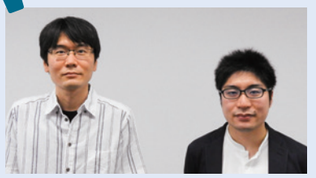
個別テストの実施方法について、機器や環境に左右されない汎用的な手順を作成しました。また、**ICSCoEの模擬プラントなどに対して実際にペネトレーションテストを行った例（手順、結果）を詳細**に記載しました。

発注者及び受注者双方で同じ資料（「テスト項目一覧表」及び「個別テスト手順書」）を参照することで、合意を得ながらテスト範囲の「決定／調査」及びテストの「実施」を進めることができます。このため実際のシステムの状況やビジネスの実態に則したペネトレーションテストの実現が期待できます。



発注者側と受注者側の打ち合わせに一覧表と手順書を使用

修了者インタビュー



左から
通研電気工業株式会社 **坂井 一仁さん**（リーダー）
株式会社中電シーティーアイ **酒井 翔悟さん**

一番の収穫は？

坂井さん 「何をやればいいかわからない」という状態から、模擬プラントを動かしながら、ペネトレーションテストでやるべきことを理解し、明確化できたことですね。

成果物の活用法

酒井さん プロジェクトを進めるうえで身に着けたスキルや考え方を、成果物とともに社内に展開して事業に生かせられると思っています。

ここがICSCoEならでは！

坂井さん 講師陣にペネトレーションテストのプロがいることですね。わからないことをすぐに質問でき、課題をどんどん前に進められました。

酒井さん 模擬プラントの存在です。実際にペネトレーションテストが思う存分できるという環境はなかなか他にないのではと思います。

第4期中核人材育成プログラム 卒業プロジェクト特集

愛されるセキュリティ部署になるには

背景・課題

社内のセキュリティ推進には、セキュリティ部署と現場（他部門）との協力が必要不可欠です。一方で、セキュリティ部署は現場から

「専門用語が多くてわからない」

「なぜ対策しないといけないかわからない」

「何かやろうとすると止められてしまう」

といったネガティブなイメージを抱かれてしまうことも多いのが実態です。現場と協力してセキュリティを推進していくためには、どのようにして双方コミュニケーションを取り、共通認識を持って対策を進めていくかが課題となります。その課題を解決するためにはセキュリティ部署が**今より「頼られ」「愛される」部署になる必要があると考えられ**、このプロジェクトがスタートしました。

課題解決・成果物

取組むべきことを明確にするため、受講者全員に「セキュリティ部署に対してどのようなイメージを抱いているか」についてのヒアリングを実施しました。ICSCoEには**企業や業界の枠を超えて様々なバックグランドを持っている受講者が集まっているため、現場目線の幅広い“生の声（具体的なエピソード）”を集めることができました。**

次に、出現頻度の高いキーワード（現場の声）を4つのレベルに分類し、セキュリティ部署が現場に“どれだけ愛されているか”を測るための指標として「セキュラブモデル」を作成しました。

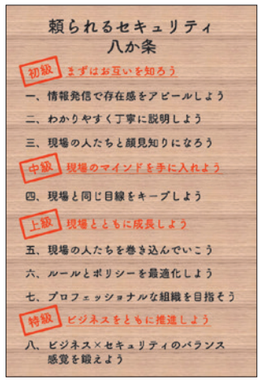
レベル	セキュリティ部署	ワードごとになぜなぜ分析	対策
レベル4 ラブ	相談しやすい、スキル高い、フレキシブル・融通、わかりやすい、感謝、賢い、手伝う、助ける、人当たり、迅速、全体、広い視点、相談、代替案、優秀	→	・対策A ・対策B ・対策C
レベル3 ちょいラブ	～くれる、～してもらう、アラート検知、インシデント対応、教える、最新技術、守る、情報共有、情報発信、専門性、未然に被害を防ぐ	→	・対策A ・対策B ・対策C
レベル2 ちょいネガ	しつこい、ルールガチガチ、形骸、現場と違う方向、現場理解不足、自己保身、属人、秘密主義、複雑、無理なポリシー、融通がきかない・頑固	→	・対策A ・対策B ・対策C
レベル1 ネガティブ	わかりにくい、一方的、押し付ける、急、高圧的、思いやりが無い、上から目線、知ったかぶり、遅い、面倒くさい、余分、理由の説明がない、冷たい	→	・対策A ・対策B ・対策C

セキュラブモデル

また、キーワードごとに「なぜそのように思われるのか」の原因になる要素を分析しました。

さらに、自分たちの分析と並行して「**セキュリティ組織運営**」や「**CSIRT構築**」**における有識者の方々にヒアリングを実施**し、実際に行われている取り組み事例も調査しました。

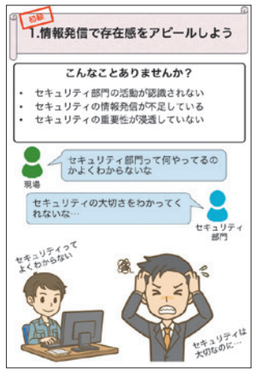
これらの結果から、今よりセキュリティ部署にポジティブなイメージを持ってもらうための方法を検討し、冊子「**頼られるセキュリティ部門への道すじ**」にまとめました。

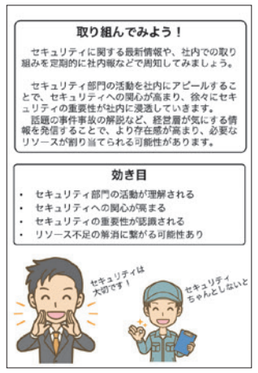


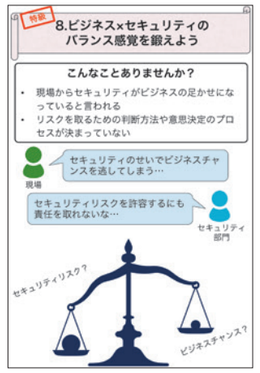
本書では、セキュリティ部署が取り組むべき内容を「**頼られるセキュリティ八か条**」としてまとめました。この八か条では、先に作成した「セキュラブモデル」を基にして「**初級**」**から**「**特級**」**まで4段階のレベル分け**を行っています。難易度が低い項目から順番に対策を実施することで、セキュリティ部署と現場の距離を縮めていく**“道すじ”**となることを想定しています。

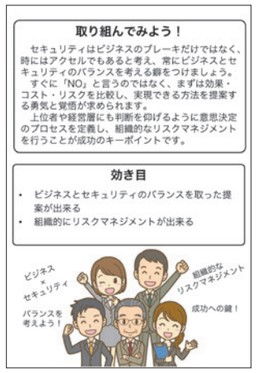
八か条それぞれの内容を説明するページでは、ヒアリングなどから明らかになった、セキュリティ部署が抱えている問題を「こんなことありませんか？（悩み）」として表現しました。次にその悩みに対して、プロジェクト内で検討した「取り組んでみよう！（対応方法）」を例示し、期待できる「効き目（効果）」を記載しています。

冊子全体の一貫したテーマは「**セキュリティ部署と現場とのコミュニケーションを大事にする**」ことです。セキュリティ部署と現場が気軽にコミュニケーションを取り合い、協力して自社のセキュリティ向上を目指していく状態になるために活用されることが期待されます。









「頼られるセキュリティ部門への道すじ」はIPAのWEBサイトに公開しています。次ページでは公開中の卒業プロジェクトの成果物について紹介しています。

修了者インタビュー

左から
関西電力株式会社　**寺本 翼さん**（リーダー）
ANAシステムズ株式会社　**清水 慶太さん**（サブリーダー）

一番の収穫は？

寺本さん　これまでセキュリティ部署と現場との関係性について、漠然とした問題意識を持っていましたが、言語化できていませんでした。それを今回多くの人と共通の課題として共有できて、冊子という形にまとめられたことがよかったと思っています。

成果物の活用法

寺本さん　まずは冊子の内容を共有して、自分の部署でできていること、できていないことを確認したいです。その上で、冊子を使って部署内で共通認識を持った状態を作り、他部署とのコミュニケーションの改善に向けて、具体的な取り組み方について話を詰めていけられたらと思っています。

清水さん　今回の成果物はセキュリティに限らず「他部署と協力関係を作るには」という大きなテーマにも対応するものになったと思っています。いずれ全社的な取り組みを進める機会があれば活用できたらと思っています。

ここがICSCoEならでは！

寺本さん　普段、どうしても自社や業界内での固定観念や常識の枠の中だけで考えてしまい、それに気が付くことも難しいことがあります。ICSCoEではそういった枠の外にいる受講者や講師、有識者から意見を聴けることが良いですね。

清水さん　セキュリティ部署や現場、ITやOTといった様々な背景を持った受講者が集まることによる「多様性」がICSCoEの一つの特徴だと思っています。ともに学ぶことで信頼関係が構築されたうえで、一つの共通のテーマについて率直な意見を出し合えたことで、成果物も多様性をカバーできるようなものにできたと思っています。