<施設管理（ビル）業界の受講生チーム>

## 3 施設管理（ビル）業界におけるセキュリティ水準向上を目指して

### 概要

近年、ビルのシステム運用効率化ニーズやIoT導入を背景として、インターネットを経由したリモート監視や、リモートメンテナンスを実施する例が増えてきています。また、個別の設備システムを統合ネットワークに接続し、機能を連携させる運用なども行われています。このように、ビルを取り巻く環境の変化があることに加え、経済産業省から、ビルシステムのセキュリティ確保を目的としたガイドライン*が公開されるタイミングであったことが活動の契機となり、本プロジェクトを始めました。

*ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン
https://www.meti.go.jp/press/2019/06/20190617005/20190617005.html

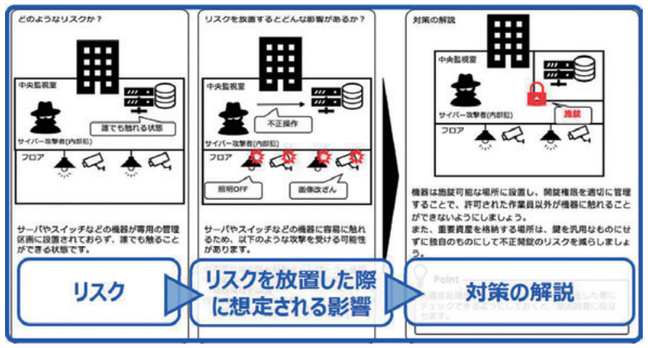
本プロジェクトでは、パブリックコメントの提出を通して、業界の各ステークホルダーがセキュリティのことを自分事として理解されるガイドラインとなるよう、多くの提言を行いました。また、本ガイドラインの業界全体への普及、実践のための理解促進、そして対策推進の第一歩を踏み出す手助けとなることを目的として、ガイドラインの解説書を作成しました。解説書では、独自に以下のコンテンツも提供しています。

**① ガイドラインを活用した対策の進め方の提案**
**② 対策マップ（機器ごとの管理策の対策箇所を可視化）**
**③ 対策カタログ（リスク／インシデント／対策を図を交えて解説）**
**④ リスク分析の事例紹介**

**担当者より**

このプロジェクトには、ビルに関わる様々な業界の受講生が集まりましたが、ICSCoEの受講生同士、派遣元企業の枠を超え、フラットな立場で取り組むことができました。解説書はプロジェクトメンバ全員の結束力がなくては完成できなかったですし、ICSCoEにおける1年間の学びの集大成でもあります。業界内で、これからセキュリティに取り組む担当者には、ぜひ読んでいただきたい内容となっています。
ICSCoEで培った知見を活かして、ビル業界におけるサイバーセキュリティ意識の向上と、ステークホルダー間での理解の輪の形成に少しでも貢献できれば嬉しく思います。

解説書（対策カタログ）の構成例




## 4 サプライチェーンセキュリティ研究

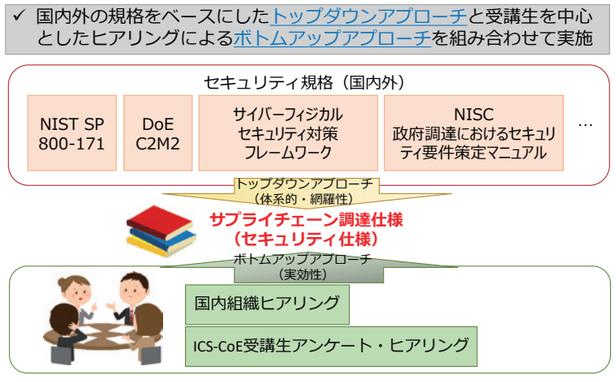
<電力業界の受講生チーム>

### 概要

発注から納品までのサプライチェーンにおける不正コード・マルウェア混入を想定したリスクに対処するため、電力業界の受講生を中心に、重要インフラ事業者やベンダ等の受講生とともに、サプライチェーンに特化した調達仕様書を作成しました。

作成にあたっては、国内外のセキュリティ規格をベースにして体系的・網羅的に調達仕様へ反映させていくトップダウンアプローチと、ICSCoE受講生や国内企業へのヒアリングによって調達仕様の実効性を強化するボトムアップアプローチを組み合わせながら進めており、理論だけでなく、実際に使用するところまでを意識した調達仕様書になっていることが大きな特長です。

調達仕様書作成のポイント





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
Industrial Cyber Security Center of Excellence
ICSCoE REPORT
令和元年9月30日
vol. 05
ICSCoE ReportはICSCoEの活動を皆様にご紹介する広報誌です。


# 中核人材育成プログラム第３期が開講

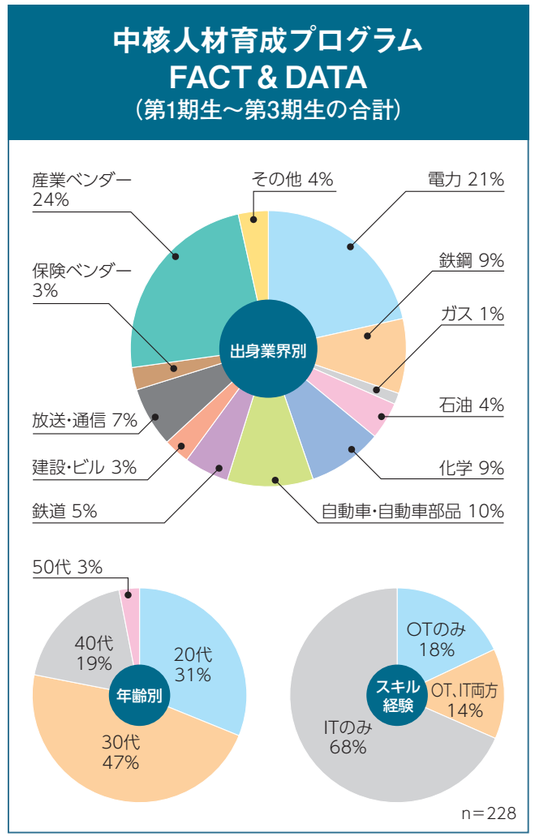
受講生を激励する遠藤センター長

2019年7月、産業サイバーセキュリティセンターは、中核人材育成プログラムに69名の第3期生を迎えました。開講初日の7月1日、受講生全員が決意を新たにする第一歩として、開講式が執り行われました。

IPA 富田理事長からは「これまで自社で培ってきた自分の強みを生かしながら、多くの仲間とともに高みを目指してほしい」と温かいメッセージが贈られました。

産業サイバーセキュリティセンター 遠藤センター長からは、技術革新がめざましい昨今、攻撃者からシステムを守るため、コレクティブ・ディフェンス（集団防御）の重要性が示されました。1年間時間をともにすることで醸成される信頼関係は非常に強固であること、その信頼できる仲間との結束は、日本を守る大きな力になることが力強く語られました。

来賓の経済産業省商務情報政策局長 西山圭太氏は、受講生の顔を見渡しながら、「1年間やっていけるか不安に思うこと。それで良く、それが大事なのです」と語り掛けました。この1年の研修は、いままでの自分を変えることが目的であり、またそのために、産業サイバーセキュリティセンターでは、世界の中でここにしかないプログラムを提供していると受講生を鼓舞しました。




3期生69名が開講式に臨みました

# 第2期中核人材育成プログラムが修了しました。

## 第2期中核人材育成プログラム修了式（2019年6月）

2019年6月、第2期中核人材育成プログラムが修了しました。修了式では、来賓の方々からの激励の言葉に加え、世耕経済産業大臣（当時）から、各修了生に宛てられた激励文が交付されました。これらを踏まえ、修了生を代表して中部電力株式会社の長谷川弘幸さんがこの1年を振り返り、修了生に付与される称号「産業サイバーセキュリティエキスパート」としてこれからどう活動していくのか、決意を新たに表明しました。

### 修了生代表挨拶

（中部電力株式会社　長谷川弘幸さん）

この1年間、本プログラムを受講して非常に思い出に残ったことが3点ございますので、本日は簡単にご紹介したいと思います。

1つ目が技術スキルの習得になります。チーム制の演習の中で、色々な方々が能動的に知識を教え合い、高め合っていくことが出来ました。受講生の中にも自分の持っていないスキルを沢山持っている人がおり、アクティブラーニングを通じて、それらの知識を身に着けることができました。

2つ目が海外の経験です。私はフランス・イギリスへの海外派遣演習に加え、米国国土安全保障省が開催していたトレーニングへ申し込み、アメリカ人38名の中に日本人2名が飛び込んでサイバー攻撃対応の演習を一緒に行うという経験をさせていただきました。フランスでは、産官学の連携が非常に進んでおり、特に企業が研究分野に対し力を入れていました。イギリスでは、スタートアップ企業に対して英国政府の投資があることや、情報連携の枠組みがかなり進んでいることが印象的でした。アメリカでは、講義中に受講生同士でディベートが始まり、講師もそこに入り込んでいく体験をしました。講義を双方向に作り上げていくような文化が根付いているのだと思いますが、このような文化に根付いたコミュニケーション力を、日本にもうまく取り入れていきたいと思っています。

3つ目はコミュニケーションについてです。私は2期の83名全員で最高の仲間になりたいという思いを持っており、昨年7月の講義初日に、全員の顔付名簿を作りましょうですとか、全員で飲み会をしましょうといったことを提案して実行しました。開講式の来賓の方の挨拶で伺ったように、1期生がアメリカ大陸を発見したコロンブスであるならば、私たちはアメリカ大陸を大いに発展させた2期生でありたい、それが私の原動力でした。途中、様々な意見を言い合ったりもしましたが、どれも建設的であり、互いに刺激しあいながらセキュリティだけでなくプロジェクトを進める上でのノウハウも身に着けることができました。課外の部活動は20を超え、忘年会や解散会は先生方も含めて100人で盛り上がりました。通常であれば、企業と企業の関係が前提になるため、このように腹を割って話し合える深い関係までいくには非常に時間が掛かっていたと思いますし、この強い横の繋がりは、派遣元に戻ってからも、きっと業界や地域を超越し、日本のサイバーセキュリティにも貢献をしていけるのではないかと思っております。

業界、地域並びに日本、世界まで我々の貢献先を着実に広げて、今の時代のサイバーセキュリティに貢献できる人材になっていきたいと思っております。本当にありがとうございました。

## 経営層へ向けてサイバーセキュリティ人材育成の今を生討論（2019年5月）

中核人材育成プログラムの修了式を目前に控えた2019年5月、経団連主催の「第5回サイバーセキュリティ経営トップセミナー」にて、受講生3名がパネルディスカッションに登壇しました。門林先生をモデレータとした本セッションでは、CoEで1年間学んだことをフル活用しながら、大変ライブ感溢れるディスカッションが展開されました。

モデレータ：奈良先端科学技術大学院大学　門林雄基 教授
パネリスト：NTTコミュニケーションズ株式会社　井上裕司さん／株式会社ラック　郷晴奈さん／中部電力株式会社　長谷川弘幸さん

**主な討論内容**

**ITとOT**　ITと同じ考え方でOTのセキュリティを考えてはいけないという共通認識のもと、受講生自身の所属業界の特徴にも触れながら、IT／OTそれぞれの立場の違い、抱える課題、セキュリティ対策の実現に向けて必要な視点などが語られました。

**海外の取組み**　海外派遣演習等を通して学んだ、諸外国におけるサイバーセキュリティ政策、重要インフラ企業を巻き込んだセキュリティ関連法の整備状況、情報共有体制などの知見を披露しながら、日本の産業界における今後の課題等が議論されました。

**自主的取組み**　講演や執筆活動による積極的な情報発信、ガイドラインの普及を通した、自身が所属する業界のセキュリティ意識向上のための活動、第2期の受講生はもちろん、講師陣、1期生、3期生など縦横の繋がりを広く強固にするネットワーキングの仕組み構築など、各々の熱い思いが込められた活動が紹介されました。

**ここがICSCoEならでは！**

- 検索エンジンでもヒットしない、教科書にも載っていないサイバーセキュリティの実態を理解することができました。
- 多業種のセキュリティ人材が集まっており、会社間・業界間の垣根を超えた関係を構築することができました。
- 競合他社であっても、高いセキュリティ意識を持った仲間として、ひとつの目的に向けて協働できたことは大変貴重な機会でした。

## 第2期生の卒業プロジェクトを紹介します。

69社83名の受講生が、約35のチームプロジェクトに取り組みました。この内、4つについてご紹介します。

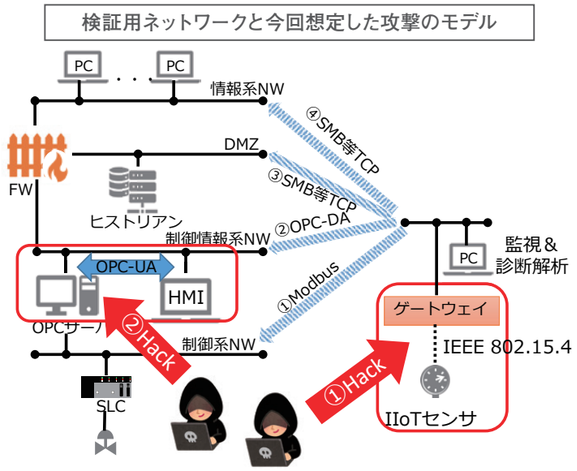
### 1 ＜化学・ガス業界の受講生チーム＞ IIoT & OPC-UAセキュリティ検証

**概要**

化学業界をはじめとした様々な業界において、産業用IoTの活用推進が盛んですが、セキュリティ対策は十分に検討されておりません。また、プラントで使用される通信プロトコルについて、従来のものから、理論上セキュアと言われるOPC-UAへの移行が進むと予想されますが、現場からみて本当にセキュアなのか、設定等に落とし穴はないのか、不安がありました。

そこで本プロジェクトでは、模擬プラントを含めた検証用環境を構成し、産業用IoT機器およびOPC-UAに対して、セキュリティ検証を実施しました。

検証用ネットワークと今回想定した攻撃のモデル




産業用IoT機器に対する検証では、機器のセキュリティ耐性の評価を実施し、システムがDoS攻撃を受ける可能性や、取得データが改ざんされる可能性があることを実証しました。また、報告書の中では、機器を不用意に制御系ネットワークや制御情報系ネットワークにつなぐことの危険性について、提言を行いました。

OPU-UAに対する検証では、OPC-UAのセキュリティ設定ごとにペネトレーションテストを実施し、どのような危険があるのか評価しました。結論として得られた「OPC-UA導入＝セキュアではない」ことを広く周知するため、OPC-UA導入時の注意点を7カ条にまとめました。

**OPC-UA導入時の注意点　7カ条**

1. 「Security Policy：None」は**ダメ。ゼッタイ。**
2. 「None＋Anonymous」はもっと**ダメ。ゼッタイ。**
3. 使わないSecurity Policyは潰しておこう
4. 秘密鍵（証明書）の管理は適切に
5. それでもDoSは防げない
6. その他のセキュリティ対策も忘れずに
7. OPC-UA製品にも脆弱性はある

**担当者より**　重要インフラ事業者として、利便性、効率性を求めるだけでなく、機器のセキュア仕様のリスクポイントを把握することが重要です。攻撃者側が圧倒的に有利と言われている中、ICSCoEでの研修を通して攻撃者目線での考え方を学べたことは、今後セキュリティ対策を検討する上で、非常に有意義でした。
さらに、業界を跨いで密な連携ができる人脈を形成できたことも、ICSCoEならではの大きな成果だと考えています。

### 2 ＜電力業界の受講生チーム＞ 電力システムセキュリティ製品検討

**概要**

電力会社でOT（Operational Technology）を担当している受講生の「技術知識を深め、システムベンダと対等に交渉ができるようになりたい」という強い思いに、他の電力会社からの受講生たちが賛同し、本プロジェクトが発足しました。

プロジェクトの目的は、セキュリティ製品を導入する際の実践的な目を養うこと、ユーザ企業の技術レベル向上を図ることとし、そのうえで保守のしやすさや機能調査の観点から調査項目を検討し、様々な製品を検証しました。

検証結果を派遣元企業でも再現可能かつ技術を理解しやすいように、検証状況や製品の設定等を動画で解説するレポートを作成しました。

**担当者より**　過去に、自分のスキル不足が要因でベンダの方と十分な意思疎通ができず、本当に欲しかった機能を持つ製品を購入できなかった経験がありました。その苦い経験から、ユーザ側の技術レベルを上げたいという思いがずっとあったのですが、本レポートを使うことで、自社の技術レベルを底上げできるのではと考えています。本レポートを有効に活用し、技術をキャッチアップし、また維持してもらいたいと思います。