IPA Better Life with IT

ICSCoE REPORT

Industrial Cyber Security Center of Excellence

平成29年10月2日

vol. 01

ICSCoE ReportはICSCoEの活動を皆様にご紹介する広報誌です。
今回は4月の発足式典からトレーニングの様子までをお伝えします。

産業サイバーセキュリティセンター 発足（2017年4月）

中西産業サイバーセキュリティセンター長

教育プログラムの講師陣とカリキュラム紹介の様子

世耕経済産業大臣

平成29年4月、独立行政法人情報処理推進機構（IPA）に産業サイバーセキュリティセンター（Industrial Cyber Security Center of Excellence, ICSCoE）が発足しました。

4月24日（月）にイイノホール（東京都千代田区）にて開催された発足記念シンポジウムおよび式典には、国会議員や政府関係者、電力、ガス、鉄鋼、石油、化学、自動車、鉄道、放送・通信など、社会インフラや産業基盤を担う企業の経営層や、本センターの人材育成プログラムの受講予定者など、業界の枠を越え約300名にご来場いただきました。

シンポジウムでは、慶應義塾大学名誉教授土居範久氏のご挨拶に続き、内閣官房内閣サイバーセキュリティセンター内閣審議官三角育生氏をはじめ、国内有数の有識者の方々にご登壇いただきました。式典では、世耕経済産業大臣（当日のごあいさつを4ページに紹介）、丸川東京オリンピック・パラリンピック担当大臣、藤井国土交通大臣政務官などをお招きし、経営層への期待を込めたご挨拶をいただきました。また、受講者派遣企業の代表として、勝野電気事業連合会会長（中部電力株式会社代表取締役社長）からもご挨拶をいただき、分野を越えた人材のネットワーク構築などへの期待も寄せられました。

IPA富田理事長

土居慶應義塾大学名誉教授

丸川東京オリンピック・パラリンピック担当大臣（当時）

藤井国土交通大臣政務官（当時）

勝野電気事業連合会会長
（中部電力株式会社代表取締役社長）

産業サイバーセキュリティセンター　長期プログラム　1年間

◆中核人材育成プログラム開講（2017年7月）

IPA産業サイバーセキュリティセンターでは、人材育成事業として、社会インフラ・産業基盤を有する事業者におけるサイバーセキュリティの中核人材を一年かけて育成する「中核人材育成プログラム」を7月3日（月）より開講しました。

7月3日は同プログラムの開講式が行われ、経済産業省の安藤久佳商務情報政策局長（当時）、産業サイバーセキュリティセンターの中西宏明センター長（株式会社日立製作所取締役会長）からの挨拶に引き続き、プログラムを担当する講師陣からそれぞれのカリキュラムについてガイダンスが行われました。

開講初日の様子。中西センター長からの挨拶では、センター設立の背景のほか、本年5月に猛威を奮ったランサムウェア「ワナクライ」に関する話もありました。

インタビュー 1

はじめに、みなさまがこれまで会社で何をしていたか、どんなふうにしてこのプログラムに参加することになったかをお聞かせ願えますでしょうか。

A氏【鉄　道】：ITシステム会社への出向経験とOTシステム（運行管理システム）の運用経験の両方があります。上司からは「セキュリティはITばかりではだめだ。君にはIT・OT全体を統括するホワイトハッカーになってもらう。マネジメントも重要だ」と内示されたのが印象に残っています。

B氏【電　力】：発電所で制御装置などのメンテナンスを担当していました。上司からは「発電所のセキュリティの先生になってくれ。君はOT担当だけど、IT担当者も派遣するので、チームで会社全体を守ってくれ」と言われました。

C氏【自動車】：私の場合、もともとIT系で、インシデントレスポンスやセキュリティの機器の導入などを担当していました。工場で組立作業をやったこともありますが、OTの経験はほぼなく、OTも含めセキュリティを勉強できる大きなチャンスと感じました。

D氏【鉄　鋼】：本社のIT企画担当でした。実は製鉄所に行ったこともなかったのですが、会社が発電事業に参入するにあたり、制御系を含め、新しいセキュリティルールの整備が必要になり、全社の様々な事業に横串を刺せるポリシー作りが課題となる中で、このプログラムに派遣されました。

産業サイバーセキュリティセンター　短期プログラム　2日間

◆「業界共通トレーニング」を実施（2017年7月）

7月14日（金）～ 15日（土）にかけて、社会インフラ・産業基盤を有する事業者のCIO（最高情報責任者）、CISO（最高情報セキュリティ責任者）向けの短期プログラムが実施されました。講師・ファシリテーターとして米国のサイバーセキュリティ専門家ら７名が来日し、電力、石油、化学、鉄鋼、ガス、自動車、製造、製薬などの業界から18名が受講しました。

机上演習（ウォーゲーム・セッション）では、受講者は6名のグループに分かれ、2020年東京オリンピック・パラリンピックを想定した社会インフラ・産業基盤に対するサイバー攻撃のシナリオをもとに、CISOや広報担当、事業部長などの役割を交代で演じ、経営判断まで含めたインシデント対応のプロセスを疑似体験しました。

今年度はさらに2回を実施予定です。次回は10月13日（金）～ 14日（土）で、米国電力会社等のサイバーセキュリティ対策責任者を歴任し、現在は、リーバイス（Levi Strauss & Co.）のチーフ・セキュリティ・アーキテクトを務めるスティーブ・ザルースキー氏が来日します。

インタビュー 2

プログラムが始まって２か月が経ちました。
いまはまだレベル合わせの期間（プライマリー）ですが、実際のトレーニングはいかがですか。

A氏【鉄　道】：ゲームスタイルのインシデントレスポンス演習（KIPS）がよかった。インシデントレスポンスで考えるべきことを網羅できて、会社に戻ってから自分の業務にも役立ちそうですし、社のセキュリティトレーニングを検討するヒントにもなりました。

B氏【電　力】：フランス派遣演習で9月末に渡仏します。これまでの講義でも海外の情報が扱われ、欧州などは規格策定などで先進的と感じているため、その肌感覚を得て電力事業に生かしたい。フランス原子力庁（CEA）など人脈作りも頑張りたいです。

C氏【自動車】：越島先生の輪読は相当大変でしたが、産業制御システム（ICS）のセキュリティは初めてで大変勉強になりました。ITセキュリティの考え方をOTに適用するにあたってのジレンマなど、取り組む課題の難しさを感じました。

D氏【鉄　鋼】：座学も、ITの基本を網羅できました。OTも、そもそもOTとは何かというところから入ったので、レベル合わせになりました。工場見学ではOT担当者の説明を受け、ITセキュリティをやってきた人間としてギャップを実感する機会となりました。

工場見学の様子。
発電所の現場を初めて見学した受講者も。

〔トレーニングの一例〕
越島一郎先生による輪読

4～5名1チームとして、“Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions”を輪読し、毎週要旨をPowerPointで発表する。

タイトル：
Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions
著　者：
Clint Bodungen, Bryan Singer, Aaron Shbeeb, Kyle Wilhoit, Stephen Hilt
出 版 社：
McGraw-Hill Education; 1版 (2016/9/13)

インタビュー 3

今後のトレーニングへの期待は？

A氏【鉄　道】：セキュリティではマネジメントも重要ですが、技術的な裏付けをしっかり得たいです。プラント演習でしっかりと実機に触れていければと思います。

B氏【電　力】：会社に戻ってサイバーセキュリティの文化を築きたいと思っています。プラント演習を通じて、攻撃者目線を理解し、防御の勘所をおさえながら、会社をリードする人材となりたいです。

C氏【自動車】：そういう意味では、経営者目線でビジネスリスクを分析し、橋渡しをしていくことも重要です。国内外の著名人や専門家との人脈作りも欠かせないと感じています。

D氏【鉄　鋼】：どこが狙われやすいのか、現場の人にきちんとわかってもらうことが重要です。後進育成もミッションなので、学んだことの横展開も意識していきたいと思います。実は、このプライマリー期間で、自分の会社の何を守るべきか、意外にも、自社をよく理解できていなかったことに気が付きました。自社の状況もしっかり確認し、このプログラムを有効活用したいです。

◆「業界別トレーニング」を実施（2017年8月）

8月25日（金）～ 26日（土）にかけて、「電力業界、不動産・ビル管理業界」のサイバーセキュリティ対策を現場で統括するCISO/CIO補佐、系列企業のCISO/CIOを担う方などを対象とした短期プログラムが実施されました。

様々なリスクに関するシナリオを用いた演習がグループワーク形式で行われ、受講者は、欧米の最先端のフレームワークを用いた仮想企業のサイバーセキュリティ成熟度評価も行いました。

今年度さらに2回（秋・冬各1回）を実施予定で、ファクトリー・オートメーション（FA）、自動車、プロセス・オートメーション（PA）などの分野を対象とする方向で検討中です。

電力、不動産・ビル向けセミナーの様子。
経済産業省の伊東寛大臣官房サイバーセキュリティ・情報化審議官も演習に参加。

業種の枠を越えた幅広い連携と サイバーセキュリティの強化・人材育成の重要性

経済産業大臣　世耕弘成

産業サイバーセキュリティセンター発足記念式典にあたり、一言ご挨拶申し上げます。私は以前より、サイバーセキュリティの強化には、我が国の企業が業種を越えて幅広く連携して対処することが必要と考えておりました。経済産業大臣に就任してからも、サイバーセキュリティ戦略本部の場で、業種の枠を越えた分野横断的な連携と人材育成の重要性を訴えてまいりました。

今回この産業サイバーセキュリティセンターには、電力、ガス、鉄鋼、石油、化学、自動車業界のほか、鉄道、ビル、空港、放送、通信、住宅業界などからも研修生が集まりました。当省の枠を越えた幅広い分野の企業が、このセンターの趣旨に賛同し研修生を派遣していただいたことは、大変喜ばしいことと考えております。

しかし、これは第一歩に過ぎません。2020年の東京オリンピック・パラリンピックを控え、重要インフラ・産業基盤のサイバーセキュリティ対策は極めて重要です。経営者の皆様一人一人が、このセンターを活用しつつ、サイバーセキュリティ対策を自らの経営戦略の根幹をなす一つのテーマとして認識し、人的・経済的な投資をしっかりと行っていただくことがこれまで以上に重要になります。

このセンターでの研修が価値ある人材投資となるよう、研修生を派遣していただいた各社におかれましては、研修生を派遣して終わりにするのではなく、将来の役員になるキャリアパスの一つとして認識いただき、卒業生が存分に活躍できるよう、社内の体制や人事制度を整えていただきたいと思います。

また、サイバーセキュリティは本質的に国際的な取組であり、この活動は日本だけで閉じてはなりません。このセンターでは是非グローバルな視野で、米国等の先進的な知見の取込みもしっかり進めていただきたいと思います。今年度は米国との共同演習等にも力を入れて取り組んでいくと承知しております。経済産業省としても、政府レベルでこうした国を越えた取組をしっかりと応援していきます。

そして、今回栄えある一期生となられた研修生の皆様には、我が国の各界でのサイバーセキュリティの強化に向けての先頭集団という気概で頑張っていただきたいと思います。ここに集まったことにより、業界を越えた人的ネットワークを築くとともに、自社に帰った後は、ここで学んだことを活かして我が国のサイバーセキュリティを牽引する存在として活躍していただきたいと思います。今年は約80名でのスタートですが、今後できるだけ早い段階で、研修生も数倍、数十倍という規模に広げていきたいと考えています。日本が必要としているサイバーセキュリティ人材は数十万人単位であり、そこに早く到達できるよう努めてまいります。

そして、各社から高い能力と志ある人材にお集まりいただいている中、中西センター長のリーダーシップの下で最高レベルの教育訓練が行われるよう、IPA及び講師陣の皆様の活躍にも期待しています。

今回の約80名の第一期研修生には、メイフラワー号でアメリカに渡った人たちのように、先頭を切って、日本のサイバーセキュリティの歴史に残るような人材になっていただきたいと考えています。これから数十年後に、あのとき日本が守られたのはあの80名が先頭を切ってくれたおかげだと記録に残るようなセンターにしていきたいと思います。研修生の皆様、そして講師陣の皆様のご尽力に期待を申し上げまして、私からのご挨拶とさせていただきます。ともに頑張っていきましょう。

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18階
Tel. 03-5978-7554　Fax. 03-5978-7513
VEGETABLE OIL INK 環境にやさしいインキを使用しています。
R70 古紙パルプ配合率70%再生紙を使用
リサイクル適性Ⓐ この印刷物は、印刷用の紙へリサイクルできます。