産業サイバーセキュリティセンターの取り組み

IPA 産業サイバーセキュリティセンター 副センター長 片岡 晃

2017年4月に「産業サイバーセキュリティセンター（Industrial Cyber Security Center of Excellence, ICSCoE）」（以下「センター」）が設立された。本稿では、センター設立の背景、センターが提供する価値について紹介する。

1 センター設立の背景

近年、社会インフラに物理的なダメージを与えるサイバー攻撃のリスクが増大している。海外においては、既に、ほかの国家などからのサイバー攻撃により、重要インフラや産業基盤の安全が脅かされる事案が発生している。幸い日本では、重要インフラを著しく破壊するようなサイバー攻撃はいまだ確認されていないが、2020年の東京オリンピック／パラリンピックを控えた今、我が国の経済や社会を支える重要インフラや産業基盤のサイバー攻撃に対する防御力を抜本的に強化する必要がある。

実際、2012年ロンドンオリンピック／パラリンピックでは、毎秒1万件の不正通信が行われ、更に開会式会場の電力システムへの攻撃情報が寄せられたことから、直前に手動システムに切替えを行うなどの処置を講じた。2016年リオオリンピック／パラリンピックでは、大会運営に大きな影響を及ぼすサイバー攻撃はなかったものの、大規模なDDoS攻撃が行われたほか、開催期間中には約400万もの脅威が発見され、対処に追われたという。

本センターでは、サイバーセキュリティ人材の育成にかかわる事業を行うと共に、実際の制御システムの安全性・信頼性の検証や、最新の攻撃情報の調査・分析などを通じて、サイバーリスクに対応する人材・組織・システム・技術を生み出し、官民が共同してサイバーセキュリティ対策強化を図るための中核拠点となることを目指していく（図1）。

2 センターが提供する価値

まず、「人材育成事業」について、実際にどのように人材育成を行っていくのかを紹介したい。本センターでは、情報系システムから制御系システムまでのシステム全体の安全性・信頼性を客観的に評価し、サイバーセキュリティ確保に必要な技術・コストの精査を行い、総合的な戦略として経営幹部に働きかけを行っていくことができる人材、更に、日々高度化を続けるサイバー攻撃について、最新のトレンドに精通し、他業界や海外の対策状況を把握すると共に、それらを自社の対策立案に効果的に反映することができる人材を育成していく。

具体的には、民間企業から派遣された研修生に対し、「中核人材育成プログラム」と呼ばれる約1年の教育プログラムを提供する（図2）。情報系システム及び制御系システムのテクノロジースキル講座を核とし、約1年間にわたって下記のような様々なコースが展開される（図3）。

① 制御システム固有のセキュリティ（CSS）関連技術及びマネジメントを理解し、模擬システムなどを用いた演習及びアクティブラーニングを通し、CSSの計画立案・対策に関する理解度を高めるコース

② 制御システムにおけるサイバーインシデントを想定した社内の対応体制と指揮について、必要な知識・ルール・スキルを網羅的に習得し、インシデント発生時の緊急体制への切替えタイミングとその際の情報共有、そのために日頃か

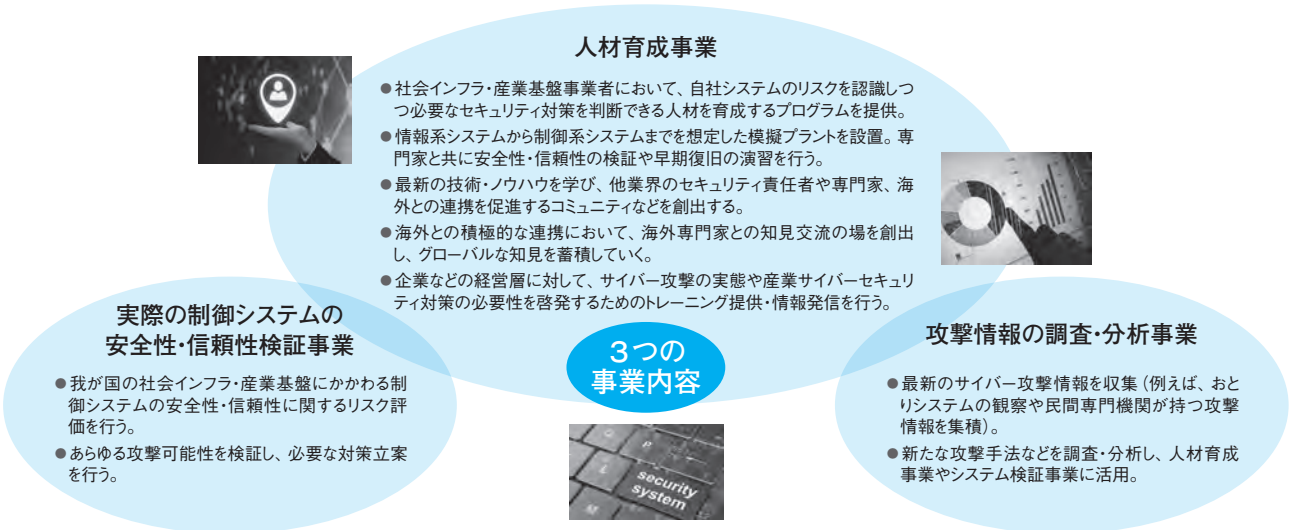

図1 産業サイバーセキュリティセンターの事業内容

（出典）IPA作成 産業サイバーセキュリティセンター設立にあたってのパンフレットより

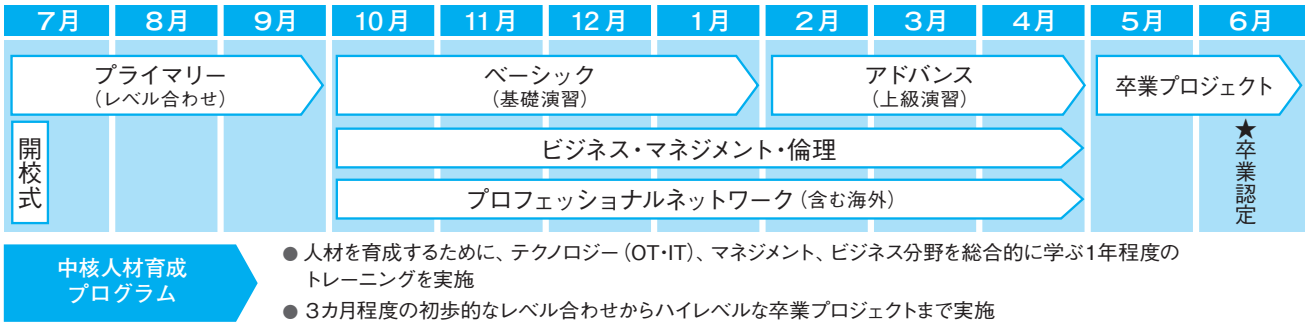

図2　産業サイバーセキュリティセンター 中核人材育成プログラムの流れ

（出典）IPA作成 産業サイバーセキュリティセンター設立にあたってのパンフレットより

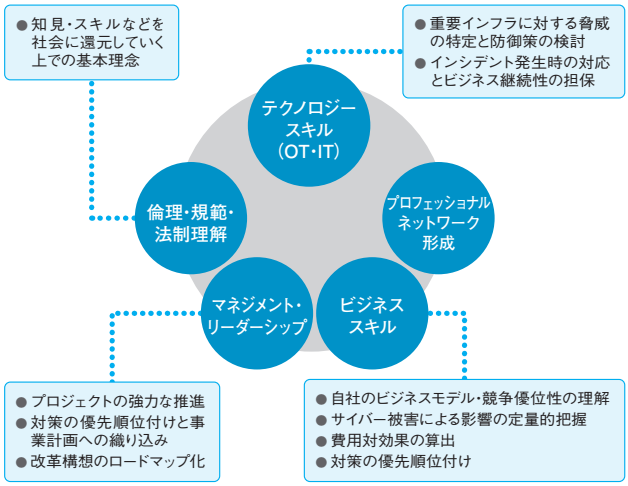

図3　産業サイバーセキュリティセンター 中核人材育成プログラムの内容

（出典）IPA作成 産業サイバーセキュリティセンター設立にあたってのパンフレットより

ら行っておくべき対応など総合的なマネジメントの理解を深めるコース

③ サイバーセキュリティに関するガバナンス、リスクマネジメント、インシデント対応、脅威情報の共有及びセキュリティ技術など、組織をサイバー攻撃から守る上で必要な知識をハンズオン形式も取り入れることにより網羅的に習得するコース

など、実践力を強化するための内容を多く盛り込んでいる。

更にサイバー被害による影響の定量的把握や費用対効果の算出方法、対策の優先順位付けと事業計画への織り込みなどを学ぶビジネスマネジメントコース、倫理・規範・法制理解を促すコースなども設けている。加えて、世界最先端の知見を獲得できる場も不可欠であるとして、現在、米国国土安全保障省（Department of Homeland Security, DHS）と共に演習プログラムを実施する予定で調整を進めているほか、欧州の国際標準などにフォーカスしたクラスの提供や、成績優秀者などを対象とした海外学会への参加などを検討していく。

そして、卒業前最後の2カ月間は、個人やグループで総合的なプロジェクトに取り組むこととし、各研修生が自社に戻った際、より実践的なサイバーセキュリティ対策を構築できるよう支援をしていく。

受講生は、1年間という長期プログラムであることを活かすことで、業界の壁を越えて交流し、講師である専門家、海外コミュニティも巻き込みながら、将来にわたっての協力関係・プロフェッショナルネットワークを構築していくことが期待される。

また、本センターでは、企業の経営層などを対象とした短期プログラムを開催する。このプログラムでは、最新のインシデント事例、セキュリティ脅威に対する戦略的視点、リスクに対処するための最先端アプローチの紹介を行う、また、セキュリティインシデントを特定、管理、解決するために備えるべき検討事項を取り上げ、インシデント管理のあり方や改善方法についての考え方を共有すると共に、擬似的なサイバー攻撃のシナリオと、それに基づいて発生し得るイベントに沿ってグループ学習を行う。更に、業界別に企業のCIOやCISOが直面するサイバーセキュリティ上の具体的な課題（法的規制への対応、体制整備、人材確保、人脈構築、技術確保、社内文化醸成など）についてのトレーニングなどの内容についても検討を進めている。企業の経営層が、迅速にサイバーセキュリティ対策の指揮を執り、組織体制の変革を行うことは、サイバーセキュリティ人材が社内で正しく評価されることにつながり、より効率的な対策の実装につながっていくと期待する。

次に、「実際の制御システムの安全性・信頼性の検証事業」を紹介する。この事業では、重要インフラや社会基盤を支える民間企業において、実際に使用されている制御系システムの安全性や信頼性を検証するためのリスク評価（ペネトレーションテスト）を実施する。テストにおいては、あらゆる攻撃可能性を検証し必要な対策立案を行うと共に、そこで得られた知見を用い、業界全体向けのガイドラインを整備し、サイバーセキュリティ対策の総合的なノウハウを創出していくことを目指す。

最後に、「最新の攻撃情報の調査・分析事業」を紹介する。この事業では、本センターに所属する専門家が中心となり、民間専門機関が持つ攻撃情報の収集や最新のサイバー攻撃情報収集などを実施していく。今年度はIPA内部の関連組織と連携をしながら、まず体制の構築を進めていく。

このように、産業サイバーセキュリティセンターは、我が国におけるサイバーセキュリティ対策強化のための中核拠点となるべく、人材育成事業から調査分析事業に至るまで、多角的機能を担っていく。官民が有機的に連携することで、サイバーセキュリティ対策の効率的かつ効果的な実装を促し、強靭な重要インフラや社会基盤を構築していきたいと考えている。