［セキュリティ人材育成の現状と実践］

③社会におけるセキュリティ人材育成事例（2）―産業サイバーセキュリティセンターにおける人材育成―

門林雄基 | 奈良先端科学技術大学院大学

産業サイバーセキュリティセンター設立の背景

サイバーセキュリティ分野では従来，情報資産や情報システムを対象としたリスクを取り扱ってきたが，近年，社会インフラ・産業基盤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．すでに海外では社会インフラ・産業基盤の安全が脅かされる事案が発生しており，これらは地政学的な緊張関係が要因だと見られている．このため我が国においても，社会インフラ・産業基盤のサイバー攻撃に対する防護力を強化する必要がある．

たとえば米国では 2003 年に，原子力発電所の制御システムがマルウェアに感染し，原発の制御システムが約 5 時間にわたって停止するという事案が発生した．またウクライナでは 2015 年から 2016 年にかけて，マルウェア感染により変電所が遠隔制御され，数万世帯で 3 ～ 6 時間にわたる大停電が発生した．

電力以外の社会インフラでも問題は顕在化している．ドイツの製鉄所では 2014 年に，何者かが製鉄所の制御システムに侵入し，不正操作をしたため生産設備が損傷する事態となっている．このほか 2017 年には，世界的な海運大手の Maersk，製薬大手のメルクなどで大規模なランサムウェア感染があり，これにより事業継続性に支障をきたす事態となっている．

またオリンピック・パラリンピックを標的としたサイバー攻撃も相次いでいる．ロンドン，リオ，平昌の各大会において大規模なサイバー攻撃が観測されており，東京大会を成功させるためにも社会インフラ・産業基盤のサイバー防護力強化は喫緊の課題となっている．

産業サイバーセキュリティセンターの構想

社会インフラ・産業基盤のサイバー防護力を強化するためには，産業分野ごとのビジネス，組織，文化の違いを尊重し，それぞれの課題と向き合い，現場や経営層と対話を重ねながら課題解決を行うサイバーセキュリティ人材が必要である．またそのような人材には，実効性が明らかでないサイバーリスク対策に満足することなく，現実に存在するリスクと対峙し，対策の実効性を自ら検証できる高い水準の総合的スキルが求められる．さらに，このような人材は圧倒的に数が足りていないため，まずは人材育成に注力していく必要がある．

このような問題意識や，制御システムセキュリティセンターにおける 2012 年からの取組みの経験に基づき，2016 年春から経済産業省において 1 年間にわたって上記の総合的スキルを持つ有識者 5 名を交えて討議が重ねられ，目指すべきセンター像，人材像，制度論などについて構想を固めた．討議における検討

事項は多岐にわたるため，事務局の手腕をもってしても 90 分程度で片付くものではなく，マラソン会議となり 4 時間にも及ぶことも珍しくなかった．

産業サイバーセキュリティセンターの構想にあたっては，個人的には 10 年近くサイバーセキュリティ人材育成に従事してきた経験が役に立った．2008 年度より，文部科学省先導的 IT スペシャリスト育成推進プログラム「社会的 IT リスク軽減のための情報セキュリティ技術者・管理者育成」（通称 IT-Keys）で 2 ～ 3 日間の演習を担当しており，大学院生向けの演習プログラム開発を通じて多くの知見を得ていた．またセンターの講師陣としては IT-Keys 修了生に加えて，奈良先端科学技術大学院大学 インターネット工学講座（現 サイバーレジリエンス構成学研究室）の修了生をイメージすることができ，カリキュラムの具体的検討につなげることができた．それぞれ数百人の修了生を擁しており，我が国の産業サイバーセキュリティ向上に向けてこれらの現有人材を動員すべき時がきた，という思いであった．

具体的なカリキュラムや求められるスキルは日進月歩のサイバーセキュリティの世界では急速に変わるため詳細を割愛するが，構想のポイントは次の 7 項目であったように思う：

1. 流派の異なる講師陣による「道場」が互いに持てるものを出し合って，人材を育成する
2. 1 年間の社会人留学とし，制御系システム（OT）と情報系システム（IT）の両方に明るいサイバーセキュリティ人材を育成する
3. FA（ファクトリオートメーション），PA（プラントオートメーション），BA（ビルオートメーション）等の模擬プラントを整備し，各々の産業分野にとってリアリティのある演習環境を構築する
4. PBL（Project Based Learning，課題解決型学習）やアクティブラーニング等の手法を活用し，自発的な学びを促す
5. 産業分野ごとのビジネス，組織，文化の違いを尊重し，それぞれの課題と向き合うセンターとする
6. 情報の機密性ラベルを策定し，守秘義務を遵守する
7. 社会インフラは輸出産業であるので，国内事情のみに目を向けるのではなく海外動向にも通じたセンターとする

構想に基づき，人材像とカリキュラム，スケジュールとクラス編成，演習環境と模擬プラントなどの具体化を進めた結果，2017 年 4 月に産業サイバーセキュリティセンターを発足させることができた．本センターは制御系システム（OT）と情報系システム（IT）との知見を結集させた世界最高レベルのサイバーセキュリティ中核拠点を目指して，（独）情報処理推進機構（IPA）の新設センターとして設置された．

中核人材育成プログラムの特徴

発足から 2 年間，各産業分野から受講生を募って中核人材育成プログラムを実施し，すでに第 1 期生 76 名，第 2 期生 83 名を輩出した．同プログラムは先鋭的な研究開発を行う研究系大学の人材育成とはきわめて異なる（相互補完的な）特徴を持つ．同プログラムの特徴の中には我々が構想段階で意図したものが多く含まれるが，以下では受講生自らが産業界のセミナーや当センターの機関紙 ICSCoE REPORT[☆1] 等で対外的に発信するなどして客観的に効果が確認できているものを紹介する．

中核人材像に沿った育成プログラム

中核人材にはサイバーセキュリティの技術的能力だけでなく，経営層や現場を巻き込んだ課題解決能力が求められる．また帰任後は事案対処チームを統

[☆1] 産業サイバーセキュリティセンター，"ICSCoE REPORT"，https://www.ipa.go.jp/icscoe/report/index.html

率する立場になる者もいる．このためビジネスマネジメントに関する研修を盛り込んでいる．内容としては困難な状況を想定したロールプレイ型の演習のほか，国内外のガイドラインや法規制への対応なども盛り込んでいる．

また技術的能力としても，ツールや製品を使いこなす能力だけでなく，国内外のベストプラクティスや標準を使いこなす能力も求められる．これらについては後述する．

加えて，必ずしも理想的でない状況においてリスクと対峙し続けるためには，職業人としての倫理感をしっかり持ち続ける必要がある．このため倫理に関する研修も盛り込んでいる．内容としてはメンロ・レポート等の倫理ガイドラインのほか，脆弱性ハンドリングの方法論や守秘義務遵守などを含む．

1年で，初心者からフルスタック人材へ

受講生は，情報系または制御系システムに関する数年程度の実務経験を有する．また受講生には大学等において情報系を専攻としていない出身者も多い．このため情報システム，制御システムのいずれかについて初心者であってもプログラムを修了できるよう，工夫が凝らされている．

たとえば情報システムについては初学者向けの講義に加えて，ラックマウント，配線から始めて，プログラミング，システムの設定などを一通り経験しなければならないようコース設計がなされている．さらに，グループワークによって受講生が自ら構築した模擬的な企業イントラネットに対し，講師陣の采配によってさまざまなインシデントが発生する．受講生はこのような擬似的なインシデントに対する対処や再発防止策を繰り返し重ねることで，さまざまなセキュリティ技術・対応策と，その礎となる情報システムの技術を体験的に獲得する．技術的には一般的な企業の情報システムを構成するあらゆる要素が対象となる．このためネットワークを構成するスイッチ・ルータ群，クライアント・サーバのOSや認証サービス，アプリケーション群，さらにはIoT機器やクラウドにいたるまであらゆる要素を扱うことになる．

近年IT業界の分業化が進み，アプリケーションから物理的なインフラまでを扱えるフルスタック人材の重要性が再認識されているが，本プログラムを修了することでフルスタック人材としての最低限の要件は満たすことになる．

プログラムの進行としては，初学者向けの座学を中心とした「プライマリ」，入門演習の「ベーシック」，発展演習の「アドバンス」，および受講生主導のテーマに取り組む「卒業プロジェクト」の4フェーズに大きく分けられる．具体的なコーススケジュールは毎年改善を重ねているが，「プライマリ」と「ベーシック」の約半年間は知識・スキル獲得が中心であり，「アドバンス」「卒業プロジェクト」は知識・スキルの活用が中心である．ベーシック以降は基本的に，座学の講義は導入や総括など最小限にとどめられ，グループワークを中心としてカリキュラムが構成されている．これは大学とは異なり，知識獲得だけでなくスキル獲得をも目的としている点や，受講生同士で教え合うことによる理解促進，共通の課題に短期間で取り組むことによるチームビルディングなど，さまざまな意味がある．企業におけるセキュリティ対策は「チームスポーツ」であるとよく言われるが，このための協調性やリーダシップ，フォロワーシップを涵養（かんよう）するには数日程度の演習では足りず，数カ月にわたって同じチームで課題に取り組んでもらう必要がある．

ITとOT

本プログラムでは情報系システム（IT）と制御系システム（OT）の双方に明るく，セキュリティとセーフティの両面に通じた人材の育成を行う．このためOTについては手始めに水処理プラントを用いた演習によって制御システムの基本から学び，最終的には電力制御システム，ビル制御システム，自

動車の制御ネットワークなどを対象とした防護演習までをこなすことになる．

IT と OT では守るべきものと優先順位がまったく異なる．近年のコモディティ化により，システムの一部で同種の部材（サーバ等）を用いることはあるが，守るべきものがまったく異なる．たとえば OT では人員の安全とプロセスの保護が最優先であるのに対し，IT ではデータの一貫性と秘匿性が優先であるといわれる．このため IT システムではセキュリティ上の欠陥に対しパッチの即時適用を推奨するが，OT では可用性を優先するため，パッチの適用は後回しである．また IT システムでは通信の遅延やジッタは許容されることが多いが，OT においてはミリ秒単位の遅延やジッタであっても工場やプラントの運転に大きな影響を与える場合がある．このような背景から OT では独自の通信プロトコル（Modbus，DNP3，OPC-UA，PROFINET 等）が用いられることが多い．

このような優先順位の違いから，IT 出身の受講生と OT 出身の受講生ではしばしば意見の対立が見られる．受講生はさまざまな演習を通じて，このような優先順位と立場の違いを互いに認識し，お互いの優先順位を理解した提案を行うスキルを涵養することとなる．これは演習に限らず実ビジネスにも当てはまるスキルであり，帰任後にこのスキルが役に立ったという修了生も多い．

サイバーセキュリティは事業継続性に大きなインパクトを与え得るという意味で重要であるが，同様に自然災害やコンプライアンスリスク，地政学的リスクなどさまざまなリスクも重要である．サイバーセキュリティをほかの関心事とならんで相対化して捉える視点は現場や経営層とのコミュニケーションにおいて不可欠であり，このために OT のセーフティ優先の視点は役に立つ．

また人材の育成とならんで，資格・称号の付与により帰任後の活躍を支援することも重要である．本プログラムの修了生は産業サイバーセキュリティエキスパートとして認定され，IT と OT の双方に通じているということが当センターによって証明される．また修了時には国家資格である情報処理安全確保支援士の申請要件を満たすようカリキュラムが設計されており，修了後に申請すれば資格が得られる．

業界ごとの取組みへの広い視野

社会インフラにおける操業停止はさまざまな産業や国民生活に重大な影響を与えることから，従来より国内の規制やガイドラインの遵守が求められている．近年，サイバーリスクの増大を受けて，それぞれの産業分野の所管省庁におけるサイバーセキュリティへの取組みが本格化している．事業継続性に懸念が生じた場合の政府への報告義務を負う分野は少なくないが，それに加えて，サイバーリスク増大への対策としてサイバーセキュリティに関するガイドラインを発行する所管官庁も増えつつある．また IT 分野のように民間事業者主導の取組みが発達している分野と，歴史的に規制事業であったため所管官庁の動向を見極めようとする分野では官民連携の実態も異なる．このような分野ごとに異なる規制環境や取組みの普遍性・固有性をわきまえ，自らの産業分野における取組み動向と課題感，人的ネットワーク，ガイドラインやベストプラクティス等について広い視野を持つ必要がある．

業界ごとにサイバーセキュリティ成熟度が違い，また守るべきものと優先順位が異なり，さらには技術・制度・市場環境が違うということは一見自明のようであるが，実際にさまざまな分野の工場を訪ね，また各々の分野のサイバーセキュリティ担当者と対話を重ねてみるとその深さを実感する．また，それぞれの産業分野から IT 分野の専門家がさほど信頼されていないということもよく分かる（信頼のおける専門家なら，なぜこのような便利だが危険な技術を作り出したのか？　という疑いのまなざしであろう）．当センターの人材育成事業を通じて，社会インフラの各分野からの信頼を IT 分野が勝ち取るに

は長い年月が必要であろうが，当センターに派遣された受講生は元々各々の産業分野の企業で働き，一定の信頼を勝ち得ているはずであるから，彼らとの信頼関係醸成がまずもって重要である．このような信頼関係を醸成し，お互いに厳しい守秘義務のもとで，本音で業界内の課題感を共有できるようになるまでには１年という期間は最低限必要である．またエネルギー産業と製造業など，つながりの深い産業分野は数多く存在し，これらの隣接分野との取組み動向の情報交換などを通じた信頼関係醸成は，分野をまたがる大規模なインシデントを想定した場合に不可欠である．

海外の取組み動向の把握

本プログラムが対象とする社会インフラ・産業基盤の分野は輸出産業であり，海外に生産拠点を数多く構える企業も珍しくない．このため海外におけるサイバーセキュリティ規制動向や取組み動向を把握することは，海外現地法人を守るため，あるいは海外で製品・サービスを販売する上で不可欠である．また受講生にとっては，自らと同じ産業分野においてサイバーセキュリティを先導する海外企業の取組みは大いに刺激になる．このような観点から，欧州および米国におけるサイバーセキュリティ規制動向や取組み動向の紹介，海外企業における事故事例や取組み事例を含むケーススタディをさまざまな機会を通じて盛り込んでいる．

このため同時通訳を交えての海外からの講師招聘のほか，欧州および米国への海外派遣演習を実施している．海外派遣演習では現地の産官学それぞれのサイバーセキュリティ専門家からのブリーフィングならびに意見交換，あるいは実機とシナリオをまじえた総合的なサイバー演習などを体験することができる．これらは，それまでに獲得した知識を総動員し，かつ英語を駆使してリアルタイムで密なやりとりを行うハイレベルなものであるが，参加者からは多くの気づきが報告されている．それらはたとえば，産官学それぞれのサイバーセキュリティ専門家がサイバーセキュリティを前向きに捉えている点や，それぞれの産業分野においてサイバーセキュリティに関する産官学連携を積極的に推進している点，技術的には当センターの水準が高いため劣後しているとは感じなかった点などである．

サイバーセキュリティの規制環境としては，欧州連合における NIS 指令[1] と GDPR[2] に見られるようなサイバーセキュリティ・プライバシー法整備に基づくアプローチと，米国に見られるような株式市場と公正取引委員会を組み合わせたソフトロー[3] と現行法の援用[4] に基づくアプローチが２つの大きな潮流であると考えられ，このような欧州法と米国法という異なる法的枠組みと，その下でのさまざまな取組みや係争・判例への視野が，帰任後に各国のサイバーセキュリティ規制環境をふまえて対策立案する上で役立つと考えられる．

アウトプット志向の学び

サイバーセキュリティ分野では座学の講義のみで伝えられることは限定的であり，手を動かしながら，受講生同士で議論しながらスキル獲得や概念獲得を促すやり方が効果的である．座学の講義による知識の伝授は教授陣から見て時間効率が良いが，トップレベルの研究系大学のような類いまれな集中力と想像力，質問力を持った優秀な受講生でない限りドロップアウト率が高くなるため，本プログラムのような多様なバックグラウンドと年齢層からなる社会人向けには適さない恐れがある．座学の講義を自習課題によって補うことも考えられるが，自習時間には個人差があり，かつ独習となるため，ドロップアウトにつながる基本的誤解やモチベーションマネジメントの失敗からの復帰が難しい．

このため本プログラムでは教授陣から見た時間効率は悪くなるものの，アウトプットを設定したグループワーク（いわゆる PBL）を中心としてカリキュラムを構成している．IT の基礎からサイバー

セキュリティに至るまでの過程で，多くの基本的概念を獲得する必要があるが，同一グループの他受講生とのやりとりの中で慣れない言葉を正しく使うことを繰り返すうちに，概念獲得が達成される．また短期間で共通の課題に取り組むことによるチームビルディング効果も高く，またこれにより醸成された人間関係を活かした励まし合いの効果も見られる．教授陣には，単に知識を効率良く伝授するだけでなく，グループ内でのやりとりを誘発し，チームマネジメントやモチベーションマネジメントの視点から「効果的な一言」を発するファシリテーションスキルも求められる．また社会人向けプログラムであるので，就業時間内に議論もふくめたグループワークが終了するようなタイムマネジメントも求められる．

グループでの学びにはさまざまな進め方があり，各々の指導陣の裁量に委ねられているが，シナリオや実際の事故事例などを用いたケーススタディ，カードや実際の機器を用いた演習，長期間にわたるチームプロジェクトなどさまざまな形態が用いられる．これについては手法を限定せず，国内外のさまざまな学びの機会から多様な教授方法，演習方法を貪欲に取り入れ，あるいは独自の方法を開発するなどして毎年改善が重ねられている．

このほか受講生主体の自主的勉強会なども行われている．受講生は帰任後の活躍機会を見据えて，カリキュラムにないが自分たちに必要なスキル，知識，人脈などについてギャップ分析を行い，自ら行動して学びの機会をつくり出している．このように，社会人の目的志向の行動力は同一目的の集団となると稀有な力を発揮する．

攻撃者の視点に基づく防御の検証

サイバーセキュリティの分野で最も重要な行動原理は“Trust but verify”である．つまり各種のセキュリティ製品・サービスの効能を鵜呑みにするのではなく，その実効性を自ら検証することができなければならない．

このためには現実に起きているサイバーインシデントや最新の脆弱性情報などのリスク情報に対する感度を高め，サイバースペースが本質的にボーダレス空間であることをふまえ，国内外を問わず情報収集と脅威分析に努める必要がある．そして自らの組織でリスクが発現した場合を想定して，インシデントの未然防止策と発生時の対応策を練る必要がある．

網羅的な脅威分析の手法として，ソフトウェア設計時に用いられるSTRIDE脅威モデル[5]，標的型攻撃の分析モデルであるATT&CK[6]などがある．受講生はFA，PA，BAあるいは一般的な社内ネットワーク等のシステムを想定し，これらの脅威分析の手法を活用していくすべをグループワークで学ぶ．また帰任後に自組織において効果的な対策を講じるためには，さまざまなセキュリティ製品・サービスの知識と利用経験，ならびにそれらの製品・サービスの精度や実効性に関する実務的な知識が不可欠である．受講生はFA，PA，BA等の模擬プラントを防護するためのシステムの構築に取り組み，講師陣とともに精度や実効性の検証に取り組むことで，これらの実務的知識を身につける．

最先端の話題への主体的取組み

受講生は1年間の人材育成プログラムの総仕上げである「卒業プロジェクト」において，主体的に設定した複数のプロジェクトに取り組むことができる．卒業プロジェクトは数名から数十名で取り組む「チームプロジェクト」と，1名で取り組む「個人プロジェクト」に大別され，メンバの総意で規定した機密性レベルのもと，時には業界や各社の事情を色濃く反映したテーマに取り組むことになる．

プロジェクトの内容はきわめて多彩であり，前節で述べた模擬プラントの防護手法の検討のような実践的なトピックのほか，深層学習のセキュリティ応用，ドローンやロボットのセキュリティ，サイバーセキュリティ心理学，サプライチェーン・セキュリ

ティ，SOC オートメーション，OT サイバーセキュリティ演習環境等，さまざまなトピックについて受講生や各社のニーズに合わせた取組みが展開される．受講生は各々のトピックについて最も適したメンター（講師陣）を選ぶことができる．講師陣は，先端的なトピックについては受講生の求めに応じて当該分野の第一人者を受講生とともに訪問し，見学と意見交換の場を設けるなどファシリテーションに努める．

修了生および各界の専門家との人脈形成

受講生の多くは各々の産業分野におけるサイバーセキュリティ対策を先導する人材となるため，産官学それぞれの専門家との人脈形成は重要な課題である．このため卒業プロジェクトや自主的勉強会などの機会を捉えて所管省庁等のサイバーセキュリティ関係者との意見交換を行い，人脈形成をはかる積極的な受講生も多い．また JPCERT/CC や日本シーサート協議会等のインシデント対応組織との関係構築や，業界ごとに存在する ISAC との意見交換なども重要である．またセキュリティ製品・サービスやその基盤となる IT 機器を中心に，脅威情報の調査・分析を行うサイバー技術研究室との人脈形成を重視する者もいる．このほかサイバーセキュリティと深層学習など，先端的トピックについて国内外の第一線で活躍する研究者との人脈構築を重視する者もいる．

サイバーセキュリティ分野ではすべての能力，情報，体制を独力で揃えることは現実的に難しく，また報道されない情報や非公開情報なども活用しながらリスク分析や対策立案を行っていく必要があるため，このような人脈構築を最重要視する受講生も少なくない．一方で，人脈構築において相手にされるためには相応の技術力，組織力，情報発信力などが必要であり，このことがアウトプット志向の学びにおける大きな動機付けとなっている者もいる．

継続的な人脈形成と維持を目的の１つとして，修了生の年次総会も毎年開催している．年次総会を通して，修了生は現場の活躍で得た知見について講師陣をふくむ参加者にフィードバックし，また講師陣は演習や講演などによって修了生に最新情報を提供することができる．年次総会において卒業年次を超えた人脈をつくることによって，業界を横断した制御システムのセキュリティにかかわる連携体制の構築をはかる．

短期プログラム

実際の企業の現場においてものごとを進めていくためには，前章で述べた中核人材に加えて，それをサポートするマネジメント層や現場層においても一定レベルのサイバーセキュリティへの理解が求められる．このため，これらの層を対象とした 2 日間の短期演習プログラムを複数展開している．

責任者向けプログラム 国際トレーニング

制御システムを有する企業のサイバーセキュリティ対策の統括部門の責任者を対象とした短期演習プログラムである．本トレーニングでは，高度なサイバー脅威が増加していること，制御システムを有する企業を守るベストな方法とは何か，そして自社組織に適用可能なサイバーセキュリティ投資の根拠となるリスク分析，インシデント管理の実行フレームワークについて理解することができる．

責任者向けプログラム 業界別サイバーレジリエンス強化演習

本演習では部門責任者層を対象として，業界別のシナリオによる実践的演習の形式で，企業が直面するサイバーリスクへの対応について学ぶ．業界別に考慮すべきセキュリティ要件や，海外子会社や系列企業，サプライチェーン等のビジネスパートナーが直面するサイバーセキュリティ規制などについてシナリオ形式で経験することができる．

制御システム向けサイバーセキュリティ演習

模擬プロセス制御ネットワークを使用して，機器の不正な制御に使用されるサイバー攻撃や対応策による防御を体験することで，制御システムのセキュリティについてより深く理解することができる．IT と制御システムのアーキテクチャ，セキュリティ脆弱性，および制御システムに固有の対策など，産業用制御システムのセキュリティを習得することができる．

このほか，「戦略マネジメント系セミナー」として，2018 年実績では 11 月と 12 月に週 1 回程度でシリーズ開催するプログラムも展開している．これは企業活動における IT 利活用が活発化する中，企業のサプライチェーンやグローバル展開の在り方など，経営の観点から，サイバーセキュリティの重要性を認識していくことが重要であるため開設したものである．企業におけるサイバーセキュリティ対策の機能はダイナミックに変貌する可能性も高く，さまざまな例に触れつつ関係者で認識を深めることがますます重要となっているため，「産業横断サイバーセキュリティ人材育成検討会」の協力を得て，シリーズセミナーとして開講している．

人材育成に求められる要素

本稿では IPA 産業サイバーセキュリティセンターにおける中核人材育成プログラムを中心として紹介した．本プログラムは受講生および派遣元企業からの評価も高いが，これは講師陣がかなりの時間とコストをかけて教材開発や演習・ファシリテーションに取り組んでおり，また運営の前提となるアセットやノウハウ，人脈なども過去 10 年の取組みの成果を活用しているためである．これだけの人的・物的リソースを動員して産業サイバーセキュリティ人材の育成にあたることができたのは，我が国の経済の大きな部分を占め，かつ国民生活にとってなくてはならない社会インフラ・産業基盤の安全性向上と国際競争力向上という大きな目標に対し，産官学が理念で一致し，かつそれぞれの持てるリソースを結集できたところが大きい．

サイバーセキュリティ分野の人材育成は制度論で語られることが多いが，教える側と学ぶ側の熱意に加えて，構想力，咀嚼力，行動力など多様な能力が求められるように思う．また，これらの多くは属人的であり，産官学，国内外にまたがる人脈など容易にはコピーできない要素も多い．このため高等教育機関や民間の教育事業者で同様の取組みを行うことは難しいと思われるが，今後の人材育成のヒントとなれば幸いである．

参考文献

1) European Parliament, NIS Directive, Directive (EU) 2016/1148 (July 2016).
2) European Parliament, General Data Protection Regulation, Regulation (EU) 2016/679 (Apr. 2016).
3) Securities and Exchange Commission , CF Disclosure Guidance : Topic No. 2 — Cybersecurity (Oct. 2011).
4) Federal Trade Commission, D-Link Agrees to Make Security Enhancements to Settle FTC Litigation (July 2019).
5) Adam Shostack, Threat Modeling: Designing for Security (Feb. 2014).
6) Storm, B. E. et al. : Finding Cyber Threats with ATT&CK-Based Analytics, MITRE Technical Report (June 2017).

(2019 年 7 月 23 日受付)

門林雄基（正会員） youki-k@is.naist.jp

博士（工学）．1996 年大阪大学大型計算機センター助手，2000 年奈良先端科学技術大学院大学 情報科学研究科 助教授，2017 年同大学教授，現在に至る．