未来の社会発展を支えるサイバーセキュリティ人材の育成

Training of Cybersecurity Human Resources to Support Future Social Development

奥原　雅之　　佳山　こうせつ　　三村　智彦　　鈴木　拓也

あらまし

これからの社会の発展を支える高度な技術を持ったセキュリティ技術者の育成は，国内外を問わず重要な課題となっている。このような人材を確保・育成していくためには，企業の枠を越えて産業界・公的機関・教育機関などと幅広く協調できる，エコシステムの形成が求められる。これまで，富士通は様々な組織と連携したセキュリティ技術者育成の活動を行ってきた。その事例として，九州大学における富士通スペシャリスト育成研究部門の設置，産業横断サイバーセキュリティ人材育成検討会のセキュリティ人材定義作業への参画，および愛媛大学・愛媛県警と共同で開催したハンズオンセミナーなどがある。

本稿では，これら組織との連携によるセキュリティ技術者育成に対する三つの取り組みと，その成果について述べる。

Abstract

The training of security engineers with advanced technological capabilities to support future social development is a key issue, both in Japan and overseas. Securing and developing such human resources requires the formation of an ecosystem where organizations can cooperate broadly beyond corporate borders with the industrial world, public bodies, and educational institutions. Up until now, Fujitsu has carried out activities to train security engineers in cooperation with various organizations. Examples include the establishment of the Fujitsu Specialist Training Research Division at Kyushu University, participation in the task of defining security human resources by the Industry Cross-Sectoral Committee for Cybersecurity Human Resources Development, and a hands-on seminar held jointly with Ehime University and Ehime Prefectural Police. This paper describes the three activities for training security engineers through cooperation with these organizations and their results.

1. まえがき

高度な技術を持ったセキュリティ技術者の育成は，国内外を問わず重要な課題となっている。日本では，経済産業省が独立行政法人情報処理推進機構（IPA）と共同で策定したITスキル標準[(1)]において，「自社の経営戦略やIT戦略の一環として情報セキュリティ戦略（対策）を，立案・推進する役割を担う人材を育成等の方法により確保すべき」としている。更に，これに併せて情報処理技術者試験を制度化している。

富士通グループでは，国内外の既存の人材モデルを参考に，日本とグローバルの双方に適用できる独自の人材モデルを定義している。この人材モデルでは，国内外の技術者スキルモデルの知見に加えて，富士通グループ内で実際にビジネスに携わっている人材の活動様式を参考にして役割や必要なスキルを定義しており，実践に裏付けされた人材定義となっている。更に，それに基づいてセキュリティ技術者のスキルを認定する「富士通セキュリティマイスター認定制度」の運用を2014年から開始している。[(2)] 本制度では，2018年10月現在で3,700名を超えるセキュリティ技術者を認定しており，2021年度末までに11,000名の技術者を育成・認定することを目標としている。

しかし，このようなセキュリティ技術者を確保・育成していくためには，企業の枠を越えて産業界・公的機関・教育機関などと幅広く協調できる，エコシステム（人材を育成・雇用・活用し続ける循環）の形成が必要になってくる。

その理由として，将来セキュリティ技術者になり得る素養を持つ若者に対するセキュリティ技術への意識啓発が挙げられる。国家公安委員会などの報告[(3)]によると，不正アクセス禁止法違反の検挙者数が年々増加しており，このうち特に14～19歳が増加傾向にある。また，検挙されたサイバー犯罪者の多くは，その知識を独学で得たという事実が指摘されている。[(4), (5)]

この背景には，好奇心に駆られて若者が独学で技術を習得し，それを安易に犯罪に利用してしまう危険性が根本にある。インターネットで流通している情報から独学で技術のみを習得し，法規制に関する知識やモラルを備えることなく人知れずサイバー犯罪予備軍になるという構図がうかがえる。これを解決するためには，若者を早い段階で社会全体のセキュリティ技術者育成のエコシステムに巻き込む必要がある。

本稿では，富士通グループが産業界・公的機関・教育機関などのグループ外の組織と連携して行っている，サイバーセキュリティ人材の発掘と育成について述べる。また，その事例として，九州大学，産業横断サイバーセキュリティ人材育成検討会，および愛媛大学・愛媛県警のそれぞれと連携した技術者育成活動を紹介する。

2. 九州大学との連携

本章では，九州大学サイバーセキュリティセンターに設置された，サイバーセキュリティ人材の育成を目的とした「富士通スペシャリスト育成研究部門」における取り組みを紹介する。

2.1 富士通スペシャリスト育成研究部門とは

九州大学は，2014年12月にサイバーセキュリティセンターを設置し，大学が担うべきサイバーセキュリティ対策の強化に向けた教育・研究に積極的に取り組んでいる。特に，全学部共通で行われるサイバーセキュリティの基礎教育を目的とした教育コースの研究開発と実施は，広くセキュリティ対応力の底上げに寄与している。

2016年6月には，同センターに富士通の寄附による「富士通スペシャリスト育成研究部門」を設置した。この研究部門は，サイバーセキュリティに関する教育手法の構築や実用的な教材の研究開発を通じて，人材育成のための教育モデルの確立に取り組んでいる。また研究面では，安全なセキュリティ空間を実現するためのフレームワークおよび実践的なアプリケーションの研究開発を行っている。

2.2 設置の狙い

富士通は，この研究部門を設置することで，九州大学のサイバーセキュリティ教育の研究活動と，それに基づくセキュリティ人材の育成が更に加速する

ことを期待している。また，研究部門で得られた教育手法や人材育成のための教育モデル，教育効果の評価手法などを自社の技術者育成に活用することで，セキュリティ対応力の底上げを目指している。同時に，このことにより企業における教育モデルの実践事例を九州大学に提供できる。

2. 3 これまでの取り組み

この研究部門は，2016年10月からセキュリティ人材の育成を目的とした講座を開講している。以下に，主な講座の概要を紹介する。

(1) サイバーセキュリティ基礎論

九州大学の全学部を対象として，共通で行われるサイバーセキュリティの基礎教育講座である。この講座は，学年や理系・文系を問わず，今後のICT社会で活躍するためにサイバーセキュリティの基礎を身につけることを目的としている。身近なパソコンやスマートフォンといった機器のパスワード管理やデータ管理といった基礎知識から，法律や倫理に至るまで幅広く学ぶことができる。年間350～400名(2クラス) の学生が受講する。

(2) セキュリティエンジニアリング演習

ものづくりを志す学生を対象として，学部を限定せずにセキュリティエンジニアリングの実践を学ぶ講座である。この講座では，サーバやネットワークなどに対するサイバー攻撃のリスクと防御の必要性を学ぶ。

その中で，IoTセキュリティに関する講座では，IoTを活用したものづくりを実際に体験すると同時に，サイバー攻撃手法とその防御を体験できる。各講座で約40名の学生が受講する。図-1は，この講座で使用している演習教材の例である。学生は，センサーなどのIoTデバイスを搭載した自走ロボットのプログラミングを体験しながら，Wi-Fiルータや IoTデバイス，データ収集サーバなどへの攻撃と防御の方法を学ぶことができる。

(3) enPiTおよびenPiT-Pro PBL演習

enPiT (Education Network for Practical Information Technologies) は,文部科学省が2018年度から開始した教育プロジェクトであり，ビッグデータ・AI (人工知能)，セキュリティ，組込みシステム，ビジネスシステムデザインの四つの分野で構成されている。九州大学は，セキュリティ分野の連携校として，課題解決型 (PBL：Project Based Learning) 演習[6] を行っている。

PBL演習は，九州大学の学生に限定せず，他大学の学生もセキュリティエンジニアリングの実践を学べる講座である。短期間での集中講座として開講され，セキュリティエンジニアリング演習と同様に，ものづくりとサイバーセキュリティを体験できる。

社会人向けには，enPiT-Pro PBL演習[7] として大学院レベルの講座を提供している。

(4) 教職員向けの情報セキュリティ教育・訓練

本研究部門では，2017年度から学内の全教職員を対象に情報セキュリティのeラーニングを実施している。そのコンテンツと確認テストには，学内で実際に起こったセキュリティインシデントの事例を踏まえて，教職員が起こしやすいインシデントの内容を取り入れている。

また，標的型攻撃メールに対する訓練を実施している。この訓練は，実際に九州大学に送られてきた悪意のあるメールの内容を踏まえ実施することで，教職員が実際の標的型攻撃を体験できる。その結果，メール内に記載されているリンクや添付資料の開封が確認でき，対象者には注意事項などをフィードバックしている。教育と訓練はどちらも，対象者へのフィードバックを工夫することで，情報セキュリティに対する意識付けの強化を図っている。

※Raspberry Pi (シングルボードコンピュータ) を使用。

図-1　セキュリティ演習教材

2.4 今後の取り組み

富士通スペシャリスト育成研究部門では，セキュリティに関する教育手法の構築や実用的な教材の研究開発を通じて，セキュリティ人材育成のための教育モデルの確立を目指している。今後，教育効果の可視化による教育支援の仕組みづくりなどに，九州大学と連携して取り組んでいく。

3. 産業横断サイバーセキュリティ人材育成検討会との連携

本章では，富士通もメンバーとして参加しており，産業界を横断して推進している「産業横断サイバーセキュリティ人材育成検討会」の取り組みについて述べる。

3.1 産業横断サイバーセキュリティ人材育成検討会とは

2015年2月に，日本経済団体連合会から「サイバーセキュリティ対策の強化に向けた提言」[8]が公開された。この提言で重要視された課題の一つに人材育成がある。この課題を実際に検討する場として，2015年6月に「産業横断サイバーセキュリティ人材育成検討会」が発足した。本検討会には，重要インフラ分野を中心とした各業界の主要企業を中心に，約50社の企業が参加している。

3.2 産業横断で対応する必要性

近年，同じ業界の民間事業者同士でサイバーセキュリティに関する情報を共有し，サイバー攻撃への対応力を高めることを目指すISAC（Information Sharing and Analysis Center）団体の活動が活発となってきている。その一方で，あらゆる企業やあらゆるモノがネットワークにつながるにつれて，それぞれの業界や企業にとって守るべき対象が拡大している。それらは，世界中の攻撃者の更なる興味を引くとともに攻撃の動機を与えており，産業界全体に危機感が急激に広まりつつある。

このように，セキュリティ対策には，業界や企業の垣根を越えた産業横断によるセキュリティ対応力向上への取り組みが不可欠である。それを実現するためには，産業界の協力体制構築や情報共有，新しい課題に対応できる人材育成が重要である。

3.3 産学官連携～学生向けサイバーセキュリティセミナー～

本検討会による各種リファレンスは，産業界に向けたものだけではなく，国や地方自治体，大学や研究機関にも提供していくことで，より効果的な産学官連携の実現を目指している。以下，大学や研究機関との連携の一例を紹介する。

将来のセキュリティに携わる人材の卵を増やすためには，より多くの学生にICTに必要なセキュリティに触れる機会を設けて，セキュリティに関心を持ってもらうことが肝要である。そこで，サイバーセキュリティに少しでも興味のある全国の大学に声をかけ，学生向けセミナーを開催した。第一線で活躍するセキュリティ技術者による技術動向や仕事内容の紹介を通じて，スペシャリストへの入り口を提示することを目的としたものである。セミナー後に行ったアンケートの結果，8割強の学生が「サイバーセキュリティに関心を持つ良い機会になった」と感じていることが分かった。

4. 愛媛大学・愛媛県警と連携した人材育成活動

富士通は，愛媛大学・愛媛県警と連携して，愛媛県内の若者を中心としたセキュリティ技術者の育成活動を行っている。本章では，その活動のセキュリティシンポジウム道後ハンズオンセミナー（以下，道後ハンズオンセミナー）ついて述べる。

4.1 道後ハンズオンセミナーとは

セキュリティ技術者を目指す若者の成長過程において，それにふさわしいセキュリティ技術を体験する場が提供されるべきである。特に人格形成に重要な十代の時期には，良質な指導者の下でセキュリティの体験が行われないと，興味半分でいわゆる「悪の道」に走ってしまう恐れがある。倫理観があるセキュリティ技術者の育成のためには，その卵の時代から，継続的に良質なセキュリティに触れる機会を提供することが重要である。

道後ハンズオンセミナーは2017年から開始した。

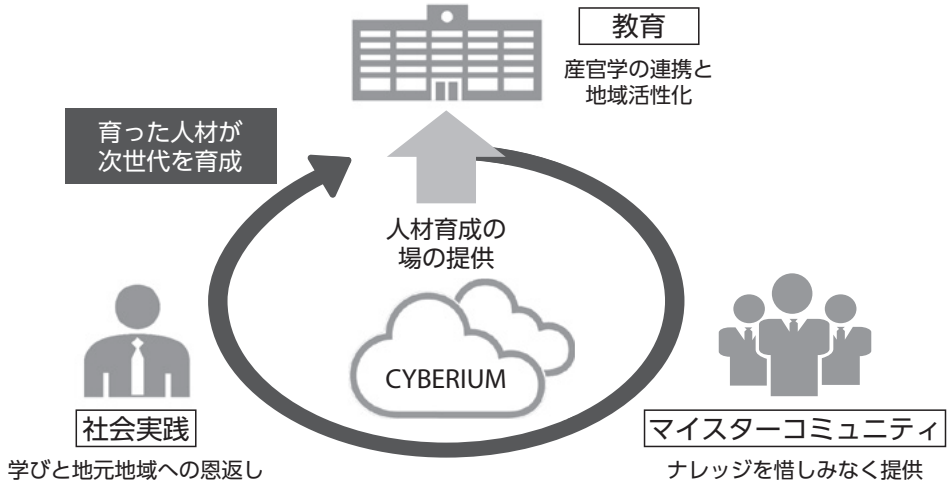

図-2　世代をつなげる人材育成サイクル

開催に当たっては，若者たちが警察署の柔道や剣道教室で汗を流し技と心を研鑽し成長するように，コンピュータとセキュリティに触れる場作り，技術を習得することを目指した。そこで，富士通の国産サイバーレンジCYBERIUMを提供し，セキュリティを学び，体験し，考える場，そして先人の成功や失敗を共有する場とした。

また，このような場作りは一過性のものでは意味がなく，地域に根付いた継続的な活動にすることが重要である。道後ハンズオンセミナーをはじめ，各地域の活動で育った先輩たちが次の世代を育てる「世代間の人材育成サイクル」を確立することが求められている。更に，若者たちが技術の習得を通じて社会に貢献することの素晴らしさを感じ，将来は地域に就職するなど，地域活性化へとつながることも期待できる（図-2）。

4.2 ハンズオンセミナーの実施とその成果

2017年2月に，愛媛県松山市で実施した道後ハンズオンセミナーでは，高校生・大学生・社会人など約70人が参加した。本セミナーでは，ラジコンカーをハッキングし，目的の場所まで動かすプログラムを組むことなどを通じて，ネットワークの脆弱性についての理解を深めるとともに，セキュリティ技術を実体験した。

このハンズオンセミナーの参加者アンケートの結果によれば，今回のイベントがセキュリティ技術に触れる機会になったという回答が98％に達しており，本取り組みが好評であったことが分かる。

5. むすび

本稿では，富士通が行っている業界団体や教育機関などと連携したサイバーセキュリティ人材の発掘と育成の取り組みについて紹介した。

このように，幅広い協調がセキュリティ技術者の人材育成エコシステムを形成していく。富士通は，これからもセキュリティ技術者育成のための協調を通じて，社会に貢献していく。

参 考 文 献

(1) 独立行政法人情報処理推進機構：IT人材における情報セキュリティの育成ニーズ・課題調査最終報告書（詳細版）．平成26年3月．
https://www.ipa.go.jp/files/000039527.pdf

(2) 佳山こうせつほか：サイバー社会に求められるセキュリティ技術者育成の実践．FUJITSU，Vol.67，No.1，p.83-89（2016）．
http://www.fujitsu.com/jp/documents/about/resources/publications/magazine/backnumber/vol67-1/paper13.pdf

(3) 国家公安委員会，総務大臣，経済産業大臣：不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況．平成30年3月．

http://www.meti.go.jp/press/2017/03/20180322004/20180322004.html
(4) ITMedia：17歳が教育システムに不正アクセス 攻撃用プログラムで脆弱性つく「能力にちょっと驚く」と馳文科相.
http://www.itmedia.co.jp/news/articles/1606/30/news092.html
(5) 佐賀新聞：ウイルス作成容疑、高3摘発 宮崎県警、独学で技術習得.
https://www.saga-s.co.jp/articles/-/79161
(6) 九州大学：enpit2.
https://cs.kyushu-u.ac.jp/enpit2/
(7) 九州大学：enpit pro security.
https://cs.kyushu-u.ac.jp/enpit-pro/
(8) 日本経済団体連合会：サイバーセキュリティ対策の強化に向けた提言.
http://www.keidanren.or.jp/policy/2015/017.html

著者紹介

奥原　雅之（おくはら　まさゆき）
富士通（株）
サイバーセキュリティ事業戦略本部
サイバーセキュリティ人材戦略企画に従事。

佳山　こうせつ（かやま　こうせつ）
富士通（株）
サイバーセキュリティ事業戦略本部
サイバーセキュリティ人材戦略企画に従事。

三村　智彦（みむら　ともひこ）
富士通（株）
サイバーセキュリティ事業戦略本部
サイバーセキュリティ人材戦略企画に従事。

鈴木　拓也（すずき　たくや）
富士通（株）
グローバルサイバーセキュリティビジネスグループ
セキュリティに関する国際標準戦略業務に従事。