平成 25 年度
内閣官房情報セキュリティセンター
委託事業

平成 25 年度
情報セキュリティに係る研究開発及び人材育成に関する
調査・検討
調査報告書
＜要約版＞

平成 26 年 3 月

株式会社 NTT データ経営研究所

目次

1. 調査の概要

1.1. 背景と目的

本調査は、サイバーセキュリティ戦略（2013 年 6 月 10 日情報セキュリティ政策会議決定）の「研究開発」及び「人材育成」の取組について、情報セキュリティを取り巻く現状や課題等についての調査、分析を行い、内閣官房情報セキュリティセンター（以下、「NISC」という。）が行う今後の情報セキュリティ研究開発・人材育成に係る政策の在り方について基礎材料を調査するものである。

サイバーセキュリティ戦略に基づく年次計画であるサイバーセキュリティ 2013 には、情報セキュリティ研究開発戦略に基づく研究開発を推進するとともに、その進捗状況の把握を行いつつ、次期の研究開発戦略のための見直し方針を作成するとされている。また、情報セキュリティを取り巻く最新の状況を踏まえ、情報セキュリティ人材育成プログラムの改訂を行うとされている。

研究開発については、情報セキュリティ研究開発戦略に示されている 12 の重要分野について、各国における情報セキュリティの研究開発についての取組状況を調査するとともに、急速に変化する情報セキュリティ情勢等を踏まえ、基本的な技術体系と新しい技術課題を包含する体系を見直し、また、国の施策としての取組と、民間等による研究開発の取組等を俯瞰し、情報セキュリティに関する技術開発に関する施策の組合せ（ポートフォリオ）が有効に構成されているか、重要な技術分野が網羅されているかを確認し、次期の研究開発戦略の策定の見直し方針として考慮する必要がある。

人材育成については、現在、国内における情報セキュリティに従事する技術者は約 26.5 万人といわれているが、うち 16 万人あまりの人材に対しては何らかのトレーニングを行う必要があると考えられる他、さらに潜在的には約 8 万人の人材が不足している状態にある（「サイバーセキュリティ戦略（平成 25 年 6 月 10 日情報セキュリティ政策会議決定）」）。

このような課題に対して、我が国の情報セキュリティのレベル向上を図るため、システムエンジニアを中心とした IT 人材の素養を底上げし、システム設計・開発の段階で情報セキュリティに十分な配慮がなされるようにすること等が重要であると考えられる。

一方、我が国で情報セキュリティの知識を有する人材は、前述の不足感にも関わらず、実際の求人・処遇は必ずしも高くなく、情報セキュリティについて学ぶインセンティブが働きづらい状況である。この原因として、経営層の情報セキュリティに関する意識が依然として低いことや、情報セキュリティを強化するための教育プログラムや能力評価基準が不充分であること等が考えられる。

これを踏まえ、今後取り組むべき人材育成のあり方を検討し、「情報セキュリティ人材育成プログラム（平成 23 年 7 月 8 日情報セキュリティ政策会議決定）」の見直しを行うに当たり、欧米における情報セキュリティ人材の需要および活用の状況、能力の評価基準となる資格要件の設定等について調査を行う。

1.2. 調査概要

本事業は、米国、欧州連合、英国、韓国の 4 カ国（地域含む）を対象に、以下の調査テーマごとに設定した調査項目について、文献調査（有識者へのヒアリング調査含む）及び現地訪問調査を行い、各国の取組みや成果等の実態について取りまとめるものである。

調査テーマ	調査項目	主たる調査観点
情報セキュリティに係る研究開発に関する調査	(1)情報セキュリティ分野の技術開発体系と取組	• 政府の技術開発戦略と技術開発分野の体系 • 研究開発に係る組織体制と取組 • 技術開発成果の移転及び情報共有の仕組み
	(2)特徴ある事例、成功事例	• 政府機関の取組事例 • 産官学連携等の取組事例 • 個人や組織ニーズから研究開発テーマを反映させる仕組み
	(3 技術開発分野の取組の変遷	• 取組の変遷 • 取組で重視していた開発分野や目標等
	(4)我が国の情報セキュリティ研究開発戦略に記載の 12 の重要分野に対応する競合研究等	• 調査対象国の技術研究開発分野との比較
情報セキュリティに係る人材育成に関する調査	(1)情報セキュリティ人材の雇用の実態	• 情報セキュリティ人材のマクロ統計 • 官・軍・民の人材流動の実態
	(2)政府戦略及び教育プログラム	• 政府の情報セキュリティ人材育成戦略 • 教育プログラム
	(3)経営層の情報セキュリティに対する意識の醸成状況	• 経営層の情報セキュリティ人材に対する意識 • 経営層の取組にインセンティブを与える制度等の枠組み
	(4)情報セキュリティに係る能力を評価するための基準・資格の活用状況	• 社内における情報セキュリティ人材の人事評価制度 • 資格及び IT スキルに関わるフレームワーク
	(5)政府調達等における情報セキュリティ資格要件の設定等の取組	• 政府調達の際に要求する情報セキュリティ資格要件
	(6)その他、情報セキュリティ人材を育成するため国・民間で行われている取組	• 政府機関の取組 • 民間の取組 • 大学の取組 • 官民連携等の取組

2. 情報セキュリティに係る研究開発及び人材育成の取組

2.1. 情報セキュリティに係る研究開発の取組

各国の情報セキュリティに係る研究開発の取組を以下に概観する。

2.1.1. 米国の取組

米国では、電力・水道・通信・交通・金融等の重要インフラを支えるコンピュータやネットワーク、そして政府機関の保有する情報システムへの不正アクセスをはじめとするサイバー脅威が年々増加傾向にあり、オバマ政権は、これまでに主要な政府情報システムおよび重要インフラに対するサイバーセキュリティ対策に取り組んでいる。まずサイバーセキュリティに関する施策として最初にオバマ政権が着手したのは、ブッシュ政権が策定した Comprehensive National Cybersecurity Initiative(CNCI)の内容を見直す Cyberspace Policy Review である。これは、前政権の政策内容を見直すもので、先に述べた急速なサイバー脅威の変化に対応することを目的に、現在のサイバー空間の脅威実態を踏まえ、早急に取り組むべきアクションプラン等を示している。その他、Cyberspace Policy Review 以降、政府機関内で様々なサイバーセキュリティの取組が具体化されてきた。例えば国土安全保障省（DHS）の Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise や国防総省（DoD）の Department of Defense Strategy for Operating in Cyberspace が挙げられる。

これら戦略に基づいて、米国の研究開発は、複数のセキュリティ専門の機関及び政府部門の連携、その他多くの支援体制によって取り組まれている。そこには、2 つの特徴が確認できる。1 つ目は、連邦政府の全省庁を統括するガイドラインやプログラム（FISMA：Federal Information Security Management Act of 2002)や、FIPS：連邦情報処理標準）に基づいたトップダウン型研究開発の仕組みである。NITRD（省庁横断ワーキンググループ）は、連邦政府内の各省庁の R&D の情報を集約し、予算も取りまとめ、連邦政府全体の R&D を牽引する機関として機能している。これらのガイドラインやプログラムに沿って、DHS や DARPA 等の各省庁が研究開発に取り組んでいる。2 つ目は、多くの重要インフラが民間部門によって運営されていることから、官民連携で行われる取組あるいは官民で技術や知見を共有する機能が整備されている。情報連携の取組には InfraGard（FBI）、JCSP（DoD&DHS）が、民間の研究開発支援としては SBIR 及び STTR や In-Q-Tel（CIA）などが挙げられる。また、重要インフラに関する情報セキュリティについて官民が大規模に情報を共有する DoD が提供する Cybersecurity Reference & Resource Guide の仕組みや、DHS が取り組む、R&D 成果を民間へ移転する Transition to Practice（TTP）の仕組みも構築・運用されている。

2013 年 2 月に、オバマ政権第二期の取組として、重要インフラのサイバーセキュリティ強化に向けた大統領令（ Executive Order ）13636 号が発行されていることからも、

米国内ではサイバーセキュリティに対する研究開発への期待は大きく、そのことは NITRD のサイバーセキュリティ研究を担う CSIA の予算額が年々増加していることからも伺える。

2.1.2. 欧州連合の取組

欧州連合（以降 EU）では、2008 年の経済・金融危機による影響や、グローバリゼーション、資源争奪、高齢化といった長期的課題を背景に、2020 年に向けた EU 加盟国の経済戦略として Europe2020 を策定している。ここで掲げる主要な戦略テーマに、情報通信技術（以降 ICT）の促進が含まれている。この戦略テーマの一つに「欧州におけるデジタル・アジェンダ（A digital agenda for Europe：DAE）」が掲げられ、その行動計画の中で、「基盤整備や ICT 関連の欧州市場統一、技術的強みの強化、民間企業（中小企業）の成長促進のための研究開発基金の改革、ICT 領域への支援増強」といった ICT 全般に対する取組方針が示されている。

サイバーセキュリティに特化した戦略としては、「Cybersecurity Strategy of the European Union(以下 EU サイバーセキュリティ戦略)」が欧州委員会により策定されている。この戦略では、優先事項の 1 つに「サイバーセキュリティのための産業および技術資源の開発」が挙げられており、EU においてサイバーセキュリティ分野の研究開発が重要視されていることが伺える。また、この戦略において研究開発に関連する具体的取組としては、サイバー犯罪の削減を目的とした EC3（European Cyber Crime Center）における研究開発支援、欧州におけるサイバーディフェンス能力技術の開発と発展、サイバーセキュリティ製品の単一市場構築、促進を目的とした技術標準等の開発、研究開発技術の事業化やイノベーションへ繋げるための投資拡大といった事項が設定されている。

EU では、これらの戦略に基づき、研究開発を支援する枠組みが策定されており、サイバーセキュリティ分野の研究開発についても、この枠組みの下で推進されている。主なものとして、欧州委員会の研究・イノベーション総局（DG RTD）が管轄する Horizon2020 がある。この Horizon2020 は、EU 全体の経済戦略 Europe2020 の研究開発の資金調達環境の向上に基づき、これまで EU で別々に実施されてきた FP、CIP、EIT による支援の 3 つの枠組みを 1 つにまとめ、刷新する形で 2014 年から開始されている。Horizon2020 では、より国際的で複数機関、事業者による連携的な研究開発の促進、研究開発の資金的な支援だけでなく、開発技術の商用化（製品化、事業化）、市場ニーズの研究開発テーマへの取り込みといった市場との相互作用を促す取組を行うこととしている。

この支援枠組みの下、EU では、JRC（Joint Research Center）の IPSC や EIT（European Institute of Innovation & Technology）の ICT Labs といった公的機関や、Fraunhofer(FKIE)研究所等の民間事業者がサイバーセキュリティ分野の研究開発に取

り組んでいる。この中で、EU の政策、戦略を最も強く反映していると考えられる JRC の IPSC では、不正検知、検出や重要インフラの防衛、個人のプライバシー保護に関する技術開発が研究テーマに掲げられて取り組まれている。

2.1.3. 英国の取組

英国政府は、2008 年に発表した国家安全保障政策（The National security Strategy）において、サイバー犯罪及びサイバー攻撃を脅威の一つと捉えたが、その後 2010 年に発表された同政策では、サイバーセキュリティを国家的対応における最優先事項としており、その重要度が増してきていることが伺える[1]。このような状況の下、サイバーセキュリティに特化した政策として「The UK Cyber Security Strategy (以下 UK サイバーセキュリティ戦略)」が英国政府により策定されている。2011 年に発表された最新の戦略では、サイバー空間への依存の高まりと共に、サイバー空間で新たに出現する脅威への迅速で柔軟な対応の必要性が述べられている。更に、英国企業に対するサイバーセキュリティ分野のビジネス促進支援や、英国企業、組織とビジネスを行うサイバー空間を世界で最も安全で開かれたものとするべく、国際的連携を推進することが示されている。この戦略に基づく取組は、「NCSP（National Cyber Security Programme)」として 4 年間で約 6.5 億ポンドの予算規模の下で進められる。

研究開発に関する戦略としては、「サイバーセキュリティ分野の中核となる専門家の育成」の中で、大学での高度なサイバーセキュリティ教育と研究開発の促進といった内容が掲げられている。この戦略からも伺える通り、英国におけるサイバーセキュリティ分野の研究開発は各大学で実施されている。UCL（University College London）やオックスフォード大学等では、この分野に特化した研究組織が設置されている。この他、サイバー攻撃やその他の脅威への対応を実施する DSTL（防衛科学技術研究所）や GCHQ、MI5、MI6、重要インフラの保護を行う CPNI といった組織においても、実際の脅威への対抗を中心とした研究開発が行われている。一方、ビジネス・イノベーション職業技能省（BIS）傘下の工学・物理科学研究評議会（EPSRC）では、他分野とサイバーセキュリティ分野を組み合わせたテーマでの研究開発が行われており、サイバーセキュリティ戦略にも挙げられている、この分野のビジネス促進を意識した、より応用的な研究開発を行っていることが伺える。

英国では、これら研究開発の支援策も実施されている。代表的なものでは、BIS による民間の研究開発への投資支援策 Solution for funded by government がある。このような施策費用を含め政府の研究開発費は、2011 年度で民間事業に 64%、次いで大学等の高等教育機関へ 26%となっており、民間による研究開発が重視されていることが伺える。

一方、開発技術の民間、高等教育機関への移転、研究成果の事業化も、BIS や大学発の技術移転機関及び、元は政府機関であり民営化されて設立された BTG（British

[1] 「サイバー攻撃の実態と防衛」2013 年 5 月， 21 世紀政策研究所

Technology Group）等で実施されている。この他、内務省によるサイバー犯罪削減パートナーシップ(CCRP)では、警察官協会、国家詐欺当局、英国銀行協会連合会、大学、その他中小企業の代表者間での研究開発成果や脅威に関する情報共有が行われるなど、政府の取組が民間と情報共有・連携を経て進められていることが確認できる。

2.1.4. 韓国の取組

韓国の政府主導による科学技術計画の歴史は比較的歴史が浅く、2001 年に制定された「科学技術基本法」に基づき、5 年を一区切りに策定し、その下で R&D 投資の拡充や基礎研究に取り組んでいる。現在「第三次科学技術基本計画（2013-2017）」が 2013 年に誕生したパク政権の下で取り組まれ、そこでは、世界の科学技術強国トップ 7 の仲間入りすることを目標に、30 の重点国家戦略技術が示されている。現政権が目指すゴールは、2017 年までに国民一人当たりの所得を 3 万ドルとし、64 万人分の雇用創出である。

この重点国家戦略技術の一つに、情報セキュリティ技術が位置づけられており、「総合セキュリティ産業発展総合対策」内に具体化されている。

情報セキュリティ技術の開発体系は、基盤分野として、「暗号」、「認証」、「探知」、「認識」、「監視」、新成長分野では、「モバイル端末」、「Internet of Things/M2M」、「クラウドコンピューティング」、「ITS」、「社会基盤」で構成される。さらに、ここで取り組まれる成果は、将来マーケットの成長潜在力、技術力、波及力、革新性を考慮して、以下の 10 製品への展開を明確にしている。

10 製品とは、基盤分野では、「次世代暗号ソフトウェア」、「セキュリティ専用 OS 組込チップ」、「モバイルセキュリティソフトウェア」、「スマートセキュリティソフトウェア」、「アンチウイルスソフトウェア」、応用分野では、「バイオ認識」、「デジタル・フォレンジック」、「社会基盤セキュリティ」、「自動ハッキング探知」、「次世代映像監視」である。

以上の R&D 戦略領域に対して、新政権下で設立された未来創造科学部が主導し、傘下の 39 の研究機関のなかで、所掌領域ごとに取り組まれる。なかでも情報、通信、電子、放送関連の融合・複合技術分野の産業技術開発を担当する韓国電子通信研究院（ETRI）は、先導的な技術開発により、科学技術計画の歴史が浅いにも関わらず、政府の強力なトップダウン型の政策遂行によって、2012 年実績で既に米国において特許登録件数世界第一位となっている。

このように韓国の R&D の取組は、国内市場における R&D 成果の利活用や産業促進面だけではなく、グローバルマーケットでいかに通用させられるか、という目的をもって取り組んでいるようである。

R&D の成果がマーケットに受け入れられるものとするためにも、R&D テーマの設定には、未来創造科学部が主管部署となって、関係部署だけでなく、一般国民、民間専門家、言論機関などとの公聴会、討論会を経ながら取り組むという仕組みがある。

さらに、R&D 成果の技術移転を実効的なものにするためにも、民間への R&D 成果の移転の仕組みが、先に紹介した ETRI が運営者となって実施されている。

2.2. 情報セキュリティに係る人材育成の取組

各国の情報セキュリティに係る人材育成の取組を以下に概観する。

2.2.1. 米国の取組

米国における情報セキュリティ人材（専門職）の数は年々増加しているものの、米国全体としては情報セキュリティ人材の不足が顕著である。このような状況を受けて、米国政府は国民全体にサイバー脅威に対する意識の向上と情報セキュリティ人材の育成について、全省庁的な政策として「National Initiative for Cyber security Education：NICE(2011 年 8 月)」を展開している。NICE は啓発、教育、体系、研修・訓練の 4 つの方針で構成され、担当省庁の役割を定め、役割に応じた取組を推進している。なかでも NICE は政府機関及び民間部門における人材育成の共通言語となるよう、情報セキュリティ人材像をフレームワーク化して明示（7 業務、31 専門領域）しており、このフレームワークに沿って各省庁は教育プログラムを導入・展開している。この取組は、大きく 2 種類に大別できる。1 つは教育プログラムを直接提供するものである。「Advanced Cyber Security Center」（USDA）や「NIETP」（NSA）、連邦職員の教育も担う Graduate School USA 等がある。もう 1 つは奨学金制度、研究補助資金支給制度である。「Homeland Security Center for Excellence」（DHS）、や「Federal Cyber Service: Scholarship for Service」（NSF）等が挙げられる。その他、育成だけではなく、人材確保のための取組も存在する。「Cyber Challenge」は全米の有能なサイバーセキュリティ人材を発掘して、専門教育を行い、政府機関、大学あるいは民間企業への就職活動を支援することを目的とするコンテストである。勝者は様々な教育あるいは就職に関する特典を獲得する。また、米国にはサイバーセキュリティに関連する資格（「CISSP」「GIAC」「ISACA の認定資格」「CompTIA の認定資格」など）が複数存在する。それぞれがサイバーセキュリティに関する試験を提供して合格者に資格を発行するが、資格の維持には定期的な教育プログラムを受けなければならない設計になっており、常に資格所有者に対して最新のセキュリティ関連情報を備えることを求める資格の枠組みとなっている。

サイバー攻撃の脅威や情報漏洩に対して危機感を持つ民間企業では、社員へ資格取得の支援を行っている。また、資格の中には政府内で情報を扱う業務従事者（職員・外部委託業者含む）に対して取得を義務付けているもの（例えば Directive8570）もある。その他、米国は学校機関でのセキュリティの専門知識や学位授与の機会も充実していることから、人材育成環境は充実しているといえる。

一方で米国における経営層の情報セキュリティに関する意識は欧州より高いものの、それほど高い状況に無いとの国内事情がある。そこで NIST は、経営層が自身の組織の

情報セキュリティの取組の現状を理解したうえで、意識向上に寄与する枠組み（Cyber Security Framework）を 2014 年 2 月に構築した。この仕組みにより、今後経営層に気付きを与え、情報セキュリティ人材採用の受け皿が民間領域においても拡大し、育成供給面と需要面とのバランスが好循環につながることが期待されている。

2.2.2. 欧州連合の取組

欧州における情報セキュリティ人材の数は年々増加しているものの、依然として需要が供給を上回り、EU 全域で不足している状況にある。この状況を受け、EU では 2013 年 2 月に「Cybersecurity Strategy of the European Union(以下 EU サイバーセキュリティ戦略)」を公表し、その中で情報セキュリティ素養を有する人材の育成の強化が方針として明記された。

欧州の人材教育に関しては、EU がそのフレームワークを策定し、各加盟国がそれに対応した各国プログラムを策定の上、学校教育、職業教育訓練、高等教育、成人教育等を行っている。情報セキュリティ人材育成プログラムとしては、EU 域外も含めた欧州各国の大学間で行われる学生や教員の交換プログラムである「Erasmus-Mundus」の中で、情報セキュリティに関わる各種コースが設定されている。同プログラムは、2014 年 1 月から、他のプログラムと統合され「Erasmus+」という新プログラムに移行しており、2014 年～2020 年の 7 年間で総額 147 億ユーロの資金を割り当て、総計 500 万人への支援を目指している。

欧州では、EU の IT スキルに係るフレームワークとして、2008 年 10 月に「European e-Competence Framework (e-CF)」が公開されている。これは、EU 各国に存在する様々な IT スキル標準を比較可能とするもので、各国の IT スキル標準の共通指標として活用されている。また、サイバーセキュリティに関するスキル標準についても、同 e-CF にて業務プロセス毎に要求されるスキルが定義されている。

一方、民間部門については、2009 年に EU の約 15%の事業者が情報セキュリティに関する事故を経験したという調査結果が出ており、これらの情報セキュリティ・リスクに対処するため、EU の民間事業者の約 27%が、自社の公式な情報セキュリティ・ポリシーを策定し、定期的に見直している。また経営層は社員に ICT セキュリティに関わる責務を認識させるべく、様々なアプローチをとっているという。これらの取組が行われている背景として、EU が戦略や法的な罰則規定を用いて加盟国を規制していることが挙げられる。

戦略面では、先述の「EU サイバーセキュリティ戦略」において、産業界の CEO や役員等の経営層がイニシアチブをとって情報セキュリティに取り組むよう要請している。他方、法規制に関しては、1995 年の「EU データ保護指令」によって、加盟国が、情報セキュリティ事故に関する罰則を自国法に規定することを要請している。

上記に加え、欧州では、EU 機関の個々の政府調達において従事予定者の情報セキュ

リティに関する専門性を要求することで、民間事業者における情報セキュリティ人材の育成・確保を促すことにつながっていると考えられる。

以上、欧州の情報セキュリティ人材の育成に関しては、EU がそのフレームワークや目標を示し、それに到達するための手段である具体的な施策やプログラムについては各国の裁量に任せている。また規制に関しても、法的枠組みのみを規定し、具体的な罰則等の規定については各国法に委ねている。したがって、欧州における情報セキュリティ人材の育成については、EU における取組と共に、次項の英国等、各加盟国の取組を理解することで、その全体像の把握が可能となる。

2.2.3. 英国の取組

英国では、ICT 人材の数は年々増加しているものの、サイバーセキュリティ人材は、インターネットの著しい成長に対応するほどには増加しておらず、この人的スキルの不足が、同国がサイバー空間において自衛し、将来的にもインターネットの利用を促進することの阻害要因となっている。そこで、英国は、2011 年の「The UK Cyber Security Strategy (以下 UK サイバーセキュリティ戦略)」において、情報セキュリティ人材育成の必要性を喫緊の課題として提示すると共に、それに関わる具体的なマイルストーンや施策を掲げている。

英国の情報セキュリティ人材の育成及び職業訓練については、多くの関係機関が詳細に定義された責任範囲を持って活動する体制となっている。まず、就業前の育成プログラムについては、主に大学機関が主体となり、大学の 2 学年から情報セキュリティをコンピュータ・サイエンスの学位を取得するためのカリキュラムに組み込み、学士、修士、博士の各課程において継続的な専門教育を行っている。一方、既に IT に関する職務経験のある人材に対する情報セキュリティ教育については、大学におけるプログラムのほか、CESG 等の各関連機関でも行われている。

英国では、従来、職業能力の評価や資格に関しては民間任せであり、様々な分野の業界団体が独自の評価基準のもとに資格を創設・授与していたために、秩序だった整理や理解が困難な「資格ジャングル」と言われる状況に陥っていた。政府はこのような状況に対応し、雇用創出が可能となるような教育・訓練政策の必要性から、1986 年以降、職業資格の整理・統合等の資格制度の整備に着手し、現在では欧州のフレームワークとの対応付けや、職業資格とアカデミックな資格の統合も完了している。IT スキル標準についても、BCS、SFIA、CESG 等の情報セキュリティ人材育成関係機関がそれぞれ開発しているが、情報セキュリティに関しては、InfoSec Skills 社が、それぞれのスキル標準を関連付けて、情報セキュリティのキャリアパスとして公表している。

民間部門においては、経営層に向けてサイバーセキュリティに関する取組を要請する政府文書の公表や、EU 指令を受けて改正された「データ保護法」に基づく、情報セキュリティ事故に関する厳しい罰則規定等により、積極的な取組がなされている。英国で

は、自社に閉じたプログラムだけでなく、産官学が連携したプログラムが多く実施されていることが特徴であり、最近では、一流企業と政府機関が共に、サイバーセキュリティ分野における学位レベルの実習プログラムを開発し、その予算も企業側が多く負担するなど、情報セキュリティ人材育成のための投資にも積極的な姿勢がうかがえる。

以上、英国では、情報セキュリティ人材不足という産官学共通の危機感の下、各種教育プログラムの実施、資格制度の確立、職業訓練プログラムの開発等、情報セキュリティ人材育成に向けた体制が充実してきており、産官学が一体となり国家全体で取り組んでいる状況である。

2.2.4. 韓国の取組

韓国では、頻発する政府機関や金融機関へのサイバー侵害を受け、専門組織及び専門人材が不足していることが各方面から指摘されている。この人材不足は政府機関の他、軍及び民間部門でも同様である。

そこで、2013 年に誕生したパク政権では、情報セキュリティ産業発展総合対策を 2013 年 7 月に公表し、最精鋭の情報セキュリティ専門家を養成する様々な人材養成プログラムにより、2017 年までにサイバーセキュリティ専門担当者を養成する。人材養成のための供給体系として「Security Scholarship システム（SS システム）」を提唱しており、2013 年 11 月現在、さっそく上記システムの整備に着手にかかった。SS システムとは、小中学校の段階から社会人に至るまでの各年齢別に幅広く情報セキュリティ教育を支援する体系である。そこでは教育支援だけでなく、サイバーハッキングや防御に係る実践訓練場等のインフラ環境を提供する。SS システムは、ソフトとハードの一体的な構造となっている点が特徴的である。

これら政府政策はパク政権下で設置された未来創造科学部が中心となり、傘下の各研究所が所管産業界に対してトップダウンで育成等に取り組む体制となっている。

一方、民間部門においては、企業経営層の情報セキュリティに対する被害認識の不足に加え、情報セキュリティ予算のかけ方が米国の比率の半分以下であるとの韓国科学技術院の報告があり、人材育成に対する取組意欲も低いと推察する。

しかし韓国では、情報セキュリティの取組を民間部門の取組を待つことなく、政府がトップダウンによって、アメとムチ（インセンティブと制度要求の面）でうまく取組を促している。

インセンティブ面としては、ISMS 認証の仕組みを活用し、認証取得によって、様々な特典（たとえば保険料金の割引や、入札時の評価加点等）を与える。制度要求面としては、金融機関に CSO の設置の義務付けなどを求めている。このような政府主導による民間部門の情報セキュリティの取組を促す枠組みのもとでは、民間部門が自ら情報セキュリティ人材を重用するような人事評価の仕組みは今回の文献調査からは確認できなかった。韓国において採用時の条件は、情報セキュリティ関連の資格保有は優遇措置程度

の扱いであり、学位所持者や経歴要件が主流である。しかし一方で、韓国インターネット振興院は、現在の情報セキュリティ人材の不足状況を解消するために、これまで国家公認の民間資格であった情報セキュリティ専門家（SIS）資格を情報セキュリティ分野の国家資格制度に格上げする計画を発表し、この資格制度の位置づけ変更によって、採用条件が変わるかについて、動向を注視する必要があるかもしれない。

また、政府は情報セキュリティの民間部門の取組を促す枠組みとして、政府調達の際に調達先に対して、情報セキュリティ人材の資格を求めることはしないものの、情報セキュリティ適合検証制度によって、情報セキュリティ機能に対する安全を求める仕組みを構築している。この制度は、国家サイバー安全センタが求める情報セキュリティシステム（2014 年現在 28 種類）には、必ず安全性が確認された認証製品であることを求めるものである。このため、当該製品に関係する企業に対しては、民間企業の情報セキュリティ投資を下支えすることにつながるとともに、韓国の政府調達製品には、情報セキュリティを重視していることが伝わってくる。

以上、韓国では、情報セキュリティに係る人材育成の取組は、政府機関自らがサイバー攻撃の標的となっていることを受け、政府機関自身の情報セキュリティ確保のための人材の充実に加え、民間部門に対しても人材養成の取組を支援する環境や取組インセンティブなどの施策をトップダウンで取り組んでいる。そこで求める人材像は、米国連邦政府が推進している NICE（National Initiative for Cyber Security Education）を参考にしつつ、産学官の連携など様々な協力関係に基づいて教育プログラムを提供した環境にある。

平成25年度　内閣官房情報セキュリティセンター委託事業
「平成25年度　情報セキュリティに係る研究開発及び人材育成に関する調査・検討」

調査報告書（要約版）

平成26年3月
株式会社ＮＴＴデータ経営研究所

〒102-0093
東京都千代田区区平河町2-7-9　JA共済ビル10階
TEL：03-5213-4209　FAX：03-3221-7022