Ⅱ－7

研究開発体制・人材育成・ITリテラシー・情報倫理

7.1　セキュリティ人材育成

日本では、不足する情報セキュリティ人材の確保・育成のため、「サイバーセキュリティ戦略」(2013年）に基づいた「新・情報セキュリティ人材育成プログラム」(2014年）が策定された。

情報セキュリティに関する脅威が多様化・高度化する中で、企業・政府の情報セキュリティを担う情報セキュリティ人材の確保・育成の必要性が叫ばれている。2012年4月に情報処理推進機構（IPA）が公開した「情報セキュリティ人材の育成に関する基礎調査―調査報告書―」によれば、国内の従業員100人以上の企業において情報セキュリティに従事する技術者は約23万人、不足人材は約2.2万人と推計されている(1)。

政府の情報セキュリティ政策会議が2011年に決定した「情報セキュリティ人材育成プログラム」に基づき、内閣官房情報セキュリティセンター（現：内閣サイバーセキュリティセンター(NISC)）や経済産業省が中心となり、政府機関、企業における人材育成施策を推進してきた。

さらに、情報セキュリティ政策会議が2013年6月に決定した「サイバーセキュリティ戦略」においては、情報セキュリティ人材の不足に対する取組として、①情報セキュリティ従事者の能力の底上げ、②突出した人材の発掘・育成、③グローバル水準で活躍できる人材の育成、④政府機関等における人材育成を掲げている。これらを踏まえ、政府は2014年度から2016年度を対象とした「新・情報セキュリティ人材育成プログラム」において、今後推進すべき新たな人材育成に関する取組の基本方針として、我が国の情報セキュリティの水準を高めるため、人材の「需要」と「供給」の好循環の形成が必要とした。需要に関しては経営層の意識改革による情報セキュリティに対する投資意欲を喚起すること、供給に関しては、人材の「量的拡大」（情報セキュリティを、既存の情報通信技術者の必須能力として位置付ける）と「質的向上」（高度な専門性や突出した能力を有する人材やグローバル水準のレベルで活躍できる人材の育成・発掘を推進する）に向けた取組を推進する方針が示された(2)。

経済産業省では、IT人材の国家試験である情報処理技術者試験の全試験区分において、2014年度以降、情報セキュリティに関する出題の強化・拡充を行っている(3)。さらにITを利用する企業（ユーザ企業）における情報セキュリティ人材不足を解消するため同試験に組織のセキュリティポリシーの策定等に必要となる知識を問う新たな試験区分として「情報セキュリティマネジメント試験」を創設するための検討を開始し、2016年度からの開始を目指している(4)。

教育機関側でも情報セキュリティ人材のニーズが認識されており、大学等において、情報セキュリティに関する専門教育課程の設置や情報処理技術者試験等の活用が進みつつある。

また、IPAのIT人材育成本部HRD（Human Resource Development）イニシアティブセンターでは、2012年度に経済産業省が実施した「情報セキュリティ人材の育成指標等の策定事業」で示されたITスキル標準等の見直し案に基づき、組織の人材育成において情報セキュリティを強化する場合に参照することを目的として、「情報セキュリティ強化対応スキル指標」を作成し、ウェブサイト上で提供している(5)。

政府もセキュリティ人材を確保するために、サイバー空間における攻撃・防御の両面に対して高度な知識を有するホワイトハッカーの直接採用を検討しており、2015年度を目処にNISCの任期付職員や研究員とする方向でサイバー攻撃への対応力の強化を図ると報じられている(6)。

●事例研究

■サイバー演習を通じた現場の人材育成

サイバー演習は、各種情報システムやネットワークにかかわる人材のサイバー攻撃等への対応能力の強化のための人材育成の場としても積極的に活用されている。実際にサイバーセキュリティにかかわる障害や攻撃が発生した際の組織の対応を確認するとともに、情報システムやネットワークの担当者自身が、演習を通じて課題発見することが、演習の重要な意義である。

NISCでは、2006年度からIT障害発生時の重要インフラサービスの維持や早急復旧の向上を目的とした「重要インフラにおける分野横断的演習（Critical Infrastructure Incident Response Exercise: CIIREX）」を実施しているほか、制御システムセキュリティセンター（CSSC）では、2012年度から制御システムを対象としたサイバーセキュリティ演習を実施している。さらに、総務省では2013年度から官公庁・大企業等のLAN管理者のサイバー攻撃対応能力の向上を目的とした実践的サイバー防御演習（CYDER）を開始し、2013年度は計10回の演習に省庁や独立行政法人、民間事業者などから計33組織、292名が参加している(7)。

●海外の状況、技術動向、制度、規制

■セキュリティコンテスト

情報セキュリティ人材の不足は世界共通の課題であり、各国において優秀な人材の確保・育成に力を入れている。こうした人材を発掘する機会として、セキュリティ技術を競うセキュリティコンテストが国内外で開催されている。セキュリティコンテストにおける代表的な競技として、CTF（Capture The Flag）がある。CTFはシステムに隠された情報（Flag）をいかに早く、多く発見できるかを競う競技であり、クイズ形式や実際に参加チームが攻撃・防御をする形式もある。最も有名なCTFは毎年ラスベガスで行われるセキュリティイベント「DEFCON」の中で開催される「DEFCON CTF」であり、1996年から開催されている。各国のセキュリティの専門家、政府関係者、ホワイトハッカーが参加している。

また、将来のサイバーセキュリティ人材として有望な学生を獲得するため、学生向けの競技大会も多く開催されており、米国の大学生向けに開催されるNational Collegiate Cyber Defense Competition（NCCDC）は、主催する防衛企業のRaytheonのほか、米国国土安全保障省（Department of Homeland Security: DHS）や多くのセキュリティ関連企業等がスポンサーとして支援している。

同様のCTFは韓国、フランス、ベルギー、ドイツ、台湾でも開催されている(8)。

---

(1)　情報処理推進機構「情報セキュリティ人材の育成に関する基礎調査―調査報告書―」2012.4, pp.63-64. <http://www.ipa.go.jp/files/000014184.pdf>
(2)　情報セキュリティ政策会議「新・情報セキュリティ人材育成プログラム」2014.5.19, p.11. <http://www.nisc.go.jp/active/kihon/pdf/jinzai2014.pdf>
(3)　「プレス発表　iパス（ITパスポート試験）をはじめとする情報処理技術者試験の出題構成の見直しについて」2013.10.29. 情報処理推進機構ウェブサイト <http://www.ipa.go.jp/about/press/20131029.html>
(4)　経済産業省「経済産業省の情報セキュリティ人材育成等に関する取組みについて」2014.6.18, p.3. 内閣サイバーセキュリティセンターウェブサイト <http://www.nisc.go.jp/conference/seisaku/jinzai/dai11/pdf/shiryou0205.pdf>
(5)　「IT人材における情報セキュリティスキル強化についての取組」2013.9.4. 情報処理推進機構IT人材育成本部HRDイニシアティブセンターウェブサイト <http://www.ipa.go.jp/jinzai/hrd/security/>
(6)　「政府、ハッカー採用へ、サイバー攻撃増に対応、来年度めど」『日本経済新聞』2014.9.7.
(7)　総務省「総務省における人材育成に関する取組―実践的サイバー防御演習「CYDER」―」2014.6.18, p.1. <http://www.nisc.go.jp/conference/seisaku/jinzai/dai11/pdf/shiryou0203.pdf>
(8)　経済産業省商務情報政策局「米国、韓国等におけるハッキングコンテストの概要」2011.3.3, pp.3-5. <http://www.meti.go.jp/committee/kenkyukai/shoujo/cyber_security/003s_02_00.pdf>

7.2　ITリテラシーと情報倫理

子どもから年配者まで幅広い層の様々な人々が情報通信技術の恩恵を享受する中で、情報通信技術を利用する上での基本的な知識や素養である「ITリテラシー」や情報化社会において個人や組織が守るべき規範である「情報倫理」の不足が思わぬ被害を生んでいる。日本国内ではそのような中、政府も民間も様々な取組を行っている。

ITリテラシーはインターネットや各種デバイス等情報通信技術を使う上での基本的な知識や素養であり、情報倫理は情報化社会において個人や組織が守るべき規範を指す(1)。子どもから年配者まで幅広い層の様々な人々が情報通信技術を利用するようになったことで、サイバー犯罪の被害を受けたり、思わぬトラブルに巻き込まれたり、場合によっては意図せず加害者になってしまう事例が増えている。情報通信技術の利用者はその恩恵を享受する一方で、様々なリスクが伴うことを理解し、責任を持った利用をすることが求められている。サイバー攻撃やサイバー犯罪の多くは、ID、パスワードを適切に管理する、不審な電子メールやサイトに注意する等、基本的な対策を実施すれば防ぐことができるものである。また、近年ネットで増加するネットいじめ、嫌がらせ、炎上等のトラブルに関しても、利用者のモラルや情報倫理の欠如に起因するものも多い。製品やサービスの提供者側が利用者に分かりやすく説明することも重要であるが、利用者側も最低限必要となるITリテラシーを習得することが重要である。

このような中、情報セキュリティ関係省庁は、一般利用者に向けた注意喚起や普及・啓発活動に力を入れている。内閣サイバーセキュリティセンター（NISC）では、情報セキュリティに関する総合的な情報ポータルとして、「国民を守る情報セキュリティサイト」を運営し、情報発信を行っている(2)。総務省も、「国民のための情報セキュリティサイト」を運用し、企業・組織、一般利用者、子ども向けのコンテンツを公開している(3)。また、警察庁は、セキュリティポータルサイト「@police（アットポリス）」を運用しており、一般ユーザだけでなく、子どもたちがインターネットの安全な使い方をゲーム感覚で学べるようにしたコンテンツ「キッズ・パトロール」を提供しているほか、保護者や教師に向けたコンテンツも公開している(4)。

一方、民間では、インターネット協会（IAjapan）が「インターネット ルール&マナー検定」を実施しており、大人版、こども版、ビジネス版の3種類を用意している(5)。また、セキュリティ対策推進協議会（SPREAD）は、地域の身近な相談相手として「情報セキュリティサポーター」の育成と支援活動を行っている(6)。さらに、フィッシング対策協議会は、フィッシング詐欺に関する事例情報や技術情報の収集・提供を行っている(7)。

民間企業でも、自社のウェブサイトを通じて顧客や利用者に向けた注意喚起や啓発コンテンツを公開しており、例えば、日本マイクロソフトが提供する「セーフティとセキュリティセンター」では、同社製品に関するセキュリティ情報だけでなく、ネット上の詐欺に対する注意喚起や、子どもや保護者向けにオンラインのリスクを説明するコンテンツ等を公開している(8)。

一方、教育の現場でも、情報化社会で生きるための教育が重視されている。現行の小・中・高等学校の学習指導要領では、情報教育の一環として、情報モラル(9)の指導に留意するよう求めている。情報モラルの指導においては、児童生徒に対して一方的に知識や対処法を教えるのではなく、各教科の学習の中で、情報発信による他人や社会への影響や、ネットワークを利用する上での責任等について、児童生徒が自ら考える活動を重視している。(10)

●事例研究

■情報セキュリティ月間

NISCでは、毎年2月を「情報セキュリティ月間」と定め、例年、様々な形で普及啓発の強化を図っている(11)。2014年2月は、「日本の成長を支えるサイバーセキュリティ」と題したシンポジウムを開催したほか、関連行事として、総務省などが北海道から九州まで11か所でセミナーや講演会を主催した。また、内閣府や経済産業省、文部科学省、都道府県警察、関連諸団体、民間企業などもそれぞれ関連行事を行っている(12)。それ以外にも、「国民を守る情報セキュリティサイト」上において、日替わりで有識者による情報セキュリティに関するコラムを掲載したほか、2013年の情報セキュリティ月間で掲載した「情報セキュリティ川柳」をもとにした「情報セキュリティクイズ」を作成・公開するなどしている。

●海外の状況、技術動向、制度、規制

■STOP.THINK.CONNECT.

一般利用者向けの情報セキュリティ啓発の取組の中で、世界的に広がりを見せているものに「STOP.THINK.CONNECT.」がある。この取組は、フィッシング対策やサイバー犯罪対策を国際的に行っている非営利団体APWG（Anti-Phishing Working Group）と同じく非営利団体であるNCSA（National Cyber Security Alliance）が共同で実施している一般利用者向けの情報セキュリティ啓発活動で、「STOP（立ち止まって理解しましょう）」、「THINK（何が起こるか考えましょう）」、「CONNECT（安心してインターネットを楽しみましょう）」という分かりやすい簡単なキーワードを用いている。この活動に対して日本からはフィッシング対策協議会が正式に協力関係を結んでいる。(13)

---

(1)　情報倫理に関しては、類似の用語として、情報通信におけるルールを指す「情報通信倫理」や、「情報モラル」（後述）等があるが、本項においては、これらを包含する概念として「情報倫理」という用語を用いる。
(2)　国民を守る情報セキュリティサイト <http://www.nisc.go.jp/security-site/>
(3)　国民のための情報セキュリティサイト <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/>
(4)　「@police」警察庁ウェブサイト <http://www.npa.go.jp/cyberpolice/>
(5)　「インターネットにおけるルール＆マナー検定」インターネット協会ウェブサイト <http://rm.iajapan.org/>
(6)　「サポーター制度について」セキュリティ対策推進協議会ウェブサイト <http://www.spread-j.org/supporter/>
(7)　フィッシング対策協議会ウェブサイト <https://www.antiphishing.jp/>
(8)　「セーフティとセキュリティセンター」日本マイクロソフトウェブサイト <http://www.microsoft.com/ja-jp/security/default.aspx>
(9)　文部科学省では、「情報社会で適正に活動するための基になる考え方や態度」と定義している。文部科学省「小学校学習指導要領解説総則編」2008.6, p.81. <http://www.mext.go.jp/component/a_menu/education/micro_detail/__icsFiles/afieldfile/2009/06/16/1234931_001.pdf>
(10)「現行学習指導要領・生きる力」文部科学省ウェブサイト <http://www.mext.go.jp/a_menu/shotou/new-cs/youryou/>; 文部科学省「教育の情報化に関する手引」2010.10.29, pp.117-144. <http://www.mext.go.jp/component/a_menu/education/detail/__icsFiles/afieldfile/2010/12/13/1259416_10.pdf>
(11)「サイバーセキュリティ月間」国民を守る情報セキュリティサイト <http://www.nisc.go.jp/security-site/month/>
(12)「平成25年度情報セキュリティ月間 関連行事」2014.2. 国民を守る情報セキュリティサイト <http://www.nisc.go.jp/security-site/month/images/event201402.pdf>
(13)「フィッシング対策協議会は、STOP.THINK.CONNECT. Messaging Convention Inc.と覚書を締結しました。」2014.2.25. フィッシング対策協議会ウェブサイト <https://www.antiphishing.jp/news/info/stop_think_connect.html>; STOP.THINK.CONNECT. <http://stopthinkconnect.jp/>

7.3　セキュリティ研究開発体制

情報セキュリティ政策会議は2014年7月に「情報セキュリティ研究開発戦略（改定版）」を決定し、2011年版の戦略で示された重点分野を再整理した上で、2014年度から3年程度を見据えた基本的方針を示した。

我が国の情報セキュリティ研究開発は、サイバーセキュリティ戦略本部（2015年1月、内閣に設置され、情報セキュリティ政策会議の決定事項・検討事項を引き継いだ。）が決定する研究開発の全体方針の下、情報セキュリティ庶務協力省庁である経済産業省（情報政策）、総務省（通信・ネットワーク）、防衛省（国家安全保障）、警察庁（サイバー犯罪・攻撃対策）に加え、文部科学省（科学技術）が、各所管分野において実施する体制となっている。省庁のほか、総務省所管の情報通信研究機構（NICT）、経済産業省所管の産業技術総合研究所（AIST）等の独立行政法人も情報セキュリティの研究開発を行っている。

2011年7月、情報セキュリティ政策会議は、「情報セキュリティ研究開発戦略」を決定し、2011年度から2015年度までの5年間及び中長期的な研究開発の課題として12の重点分野を示した。2012年には情報セキュリティ政策会議に設置された技術戦略専門委員会においてロードマップを策定し、達成目標等を取りまとめた(1)。

一方、2013年6月に情報セキュリティ政策会議が決定した「サイバーセキュリティ戦略」においては、研究開発について、我が国のサイバー攻撃に対する防御能力の向上、経済成長につながる新産業創出、サイバーセキュリティ産業の国際競争力の向上のために重要なものであると位置付けられている。また、「サイバーセキュリティ戦略」では、サイバー攻撃の検知、制御システムのセキュリティなど、新たな研究開発分野の具体例も挙げられている(2)。

2011年の「情報セキュリティ研究開発戦略」では情報セキュリティの研究開発予算の充実を掲げているが、政府の情報セキュリティ研究開発予算（2007年度～2014年度）は、2011年度及び2012年度に補正予算等により大幅に研究開発予算が増加した分を除けば、当初予算ベースでは減少基調にあり、直近の2014年度予算は20億円弱となっている。ただし、政府の情報セキュリティ全体に係る予算は増加傾向にあるため、研究開発よりも直近のサイバー攻撃等の脅威に対応するシステムや体制整備等の施策に優先して予算が割り当てられていると考えられる(3)。また、2011年の戦略で示された重要分野の一部は、サイバー攻撃対策を重視する政府方針の中で十分進捗しておらず、一方では、12分野以外に新たに実施すべき研究も出てきている(4)。

前述の状況を踏まえ、情報セキュリティ政策会議は2014年7月に「情報セキュリティ研究開発戦略（改定版）」を決定し、重要分野を再整理した上で、2014年度から3年程度を見据えた基本的方針を示している。特に、民間企業のみでは十分に実施できない研究領域について、産学官が連携して、国の施策として推進すべき重要分野や研究テーマを例示している。同戦略では、情報セキュリティ研究開発の取組方針や施策例を、①サイバー攻撃の検知・防御能力の向上、②社会システム等を防護するためのセキュリティ技術の強化、③産業活性化につながる新サービス等におけるセキュリティ研究開発、④情報セキュリティのコア技術の保持、⑤国際連携による研究開発の強化等の5つの観点で整理し、研究開発を進めるに当たっては、サイバー攻撃を受けた際の被害を極小化させるとともに、攻撃者の攻撃にかかる経済的負担を増大させ

るなど、これまでの情報セキュリティ対策の考え方に囚われない革新的な取組（いわゆるゲーム・チェンジ(5)）に重点を置くとしている(6)。

●事例研究

■サイバー攻撃対策総合研究センター（CYREC）

総務省は、2013年4月、情報通信研究機構（NICT）内に、国内のサイバーセキュリティの研究開発の拠点として、サイバー攻撃対策総合研究センター（Cybersecurity Research Center: CYREC）を設立した。サイバー攻撃の観測技術や防御技術の検証実験などを行うとしている(7)。設立にあたり、総務省は2012年度補正予算から100億円を投じている(8)。

●海外の状況、技術動向、制度、規制

■米国サイバーセキュリティ研究開発戦略

米国連邦政府の情報通信にかかわる分野の研究開発を省庁横断的に取りまとめるネットワーキング情報技術研究開発プログラム（Networking and Information Technology Research and Development: NITRD）の1分野としてサイバーセキュリティと情報保証（Cyber Security and Information Assurance: CSIA）があり、CSIAの参加機関が米国のサイバーセキュリティ研究開発の研究主体となっている。CSIAの主な参加機関は、全米科学財団（National Science Foundation: NSF）、国防総省（Department of Defense: DoD）、国防高等研究計画局（Defense Advanced Research Projects Agency: DARPA）、米国国立標準技術研究所（National Institute of Standards and Technology: NIST）、国土安全保障省（Department of Homeland Security: DHS）等である。

2011年12月、大統領府（Executive Office of the President）の国家科学技術会議（National Science and Technology Council: NSTC）は、CSIAの運営グループ及び省庁間作業部会の検討に基づき、米国のサイバーセキュリティの研究開発戦略「Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity R&D Program」(9)を公表した。同戦略では研究開発の戦略的目標として、①変化の誘発、②科学的な基盤の確立、③研究のインパクトの最大化、④実用への移行の加速、を挙げている。

2014年度のCSIAの予算は7.67億ドル（推計）であり、前年度6.53億ドルから大きく増加している。DoDが1.92億ドル、DoDの研究機関であるDARPAが2.94億ドルと国防関連機関の予算が全体の約63%を占めている。(10)

---

(1)　情報セキュリティ政策会議「情報セキュリティ研究開発戦略」2011.7.8. <http://www.nisc.go.jp/active/kihon/pdf/kenkyu2011.pdf>
(2)　情報セキュリティ政策会議「サイバーセキュリティ戦略―世界を率先する強靭で活力あるサイバー空間を目指して―」2013.6.10, pp.35-36. <http://www.nisc.go.jp/active/kihon/pdf/cyber-security-senryaku-set.pdf>
(3)　情報セキュリティ政策会議「情報セキュリティ研究開発戦略（改定版）」2014.7.10, pp.4-6. <http://www.nisc.go.jp/active/kihon/pdf/kenkyu2014.pdf>
(4)　同上, p.3.
(5)　ここでのゲーム・チェンジとは、攻撃側が防御側よりも圧倒的に有利にあるサイバー攻撃の現状に対して、攻撃者が攻撃を行うことの経済的負担を増大させる「チェンジ」を起こす技術によって、現状の打破を目指す考え方である。
(6)　情報セキュリティ政策会議　前掲注(3), pp.12-19, 25.
(7)　「サイバー攻撃対策総合研究センター（CYREC：サイレック）」情報通信研究機構ウェブサイト <http://nict.go.jp/cyrec/index.html>
(8)　総務省「平成24年度補正予算概要資料」2013.2, p.19. <http://www.soumu.go.jp/main_content/000286358.pdf>
(9)　Executive Office of the President, National Science and Technology Council,“Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program,”December 2011. <http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf>
(10)　The Networking and Information Technology Research and Development,“FY2015 Supplement to the President's Budget,”March 2014, pp.8-9. <https://www.nitrd.gov/pubs/2015supplement/FY2015NITRDSupplement.pdf>

主要事項執筆者一覧

執筆者所属：三菱総合研究所

執筆者	主要事項
情報通信政策研究本部主席研究員　村野（むらの）　正泰（まさやす）	1.3.1, 4.1, 4.2, 4.3, 4.4, 4.6, 5.1.1, 5.1.2, 5.1.3, 5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.3.1, 5.3.2, 6.2.1
情報通信政策研究本部主席研究員　澤部（さわべ）　直太（なおた）	1.3.2, 1.3.3, 1.3.4
情報通信政策研究本部主任研究員　谷田部（やたべ）　智之（ともゆき）	1.1, 1.2.1, 1.2.3, 1.2.4, 1.3.6, 2.4, 6.2.6, 6.2.7
情報通信政策研究本部主任研究員　清水（しみず）　友晴（ともはる）	6.1.1
情報通信政策研究本部研究員　松本（まつもと）　尭（たかし）	1.2.5, 2.1, 2.2, 2.3, 3.1, 3.2, 3.3, 4.5
情報通信政策研究本部研究員　丸田（まるた）　佳織（かおり）	1.2.2, 1.3.5, 5.1.4, 5.2.5, 5.2.6, 6.1.2, 6.2.2, 6.2.3, 6.2.4, 6.2.5, 7.1, 7.2, 7.3

＊ 本稿におけるインターネット情報の最終アクセス日は、原則として、2015年1月13日である。