研究開発体制・人材育成・ITリテラシー・情報倫理

要　旨

サイバー攻撃等の脅威が急速に増す一方で、日本の情報セキュリティ研究開発予算は年々減少傾向にある。サイバー防御能力の向上、新産業創出、国際競争力の向上の観点で、国として支援すべき研究開発への投資を拡大し、大学や企業がサイバーセキュリティ分野の産業創出につながる成果を出せるよう柔軟な研究開発の支援体制を整備していく必要がある。さらに、深刻化する情報セキュリティ人材の量的・質的な不足を解消するため、官民を挙げた人材の育成、確保が急務となっている。また、安全・安心な情報通信技術の利用を実現するためには国民全体のITリテラシー・情報倫理を向上させることも重要な対策である。

現在、サイバーセキュリティはITに拘らずあらゆる分野において必須の概念であり、産・官・学が連携して、国のサイバーセキュリティレベルの向上に取り組むことが急務となっている。サイバーセキュリティの取組は、対策技術の開発や法制度を整備する「守る側」の取組だけでは不十分であり、「守られる側」である情報通信技術の利用者がその取組の必要性を理解して初めて機能するものである。そこで、本論では、我が国のサイバーセキュリティレベルの向上を基本的な視点とし、具体的な課題として、より高度な技術を実現するための研究開発体制と今後のサイバーセキュリティを担う人材の育成について国内外の動向を取り上げるとともに、国民のサイバーセキュリティに対する意識の底上げの必要性について、特にITリテラシーと情報倫理の観点から論じる。

なお、本論では「サイバーセキュリティ」の課題として上記の課題を取り上げるが、参照する政府の文書等で「情報セキュリティ」という用語が固有名詞的に用いられている場合は、本文中の表現もそれに準じることとする。

I　研究開発体制

1　我が国におけるサイバーセキュリティの研究開発の現状

2013年6月に情報セキュリティ政策会議において決定された「サイバーセキュリティ戦略」では、サイバーセキュリティの研究開発は①我が国のサイバー防御能力の向上、②経済成長につながる新産業創出、③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(1)。

(1)　政府の研究開発の状況

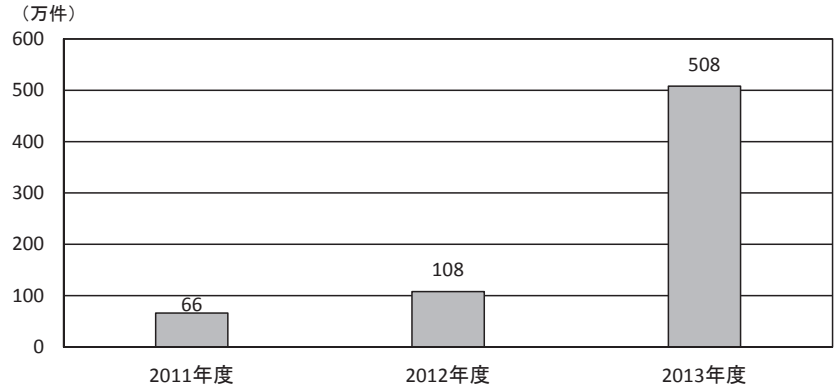
①のサイバー防御能力の向上は、国家の安全保障・危機管理の観点からも重要な課題であり、実現のためには特に政府機関におけるサイバー攻撃等に対する対応体制の整備とともに、監視・観測、検知、解析、防御に関する幅広い研究開発が必須となる。

＊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。

(1)　情報セキュリティ政策会議「サイバーセキュリティ戦略」2013.6.10, pp.35-36. <http://www.nisc.go.jp/active/kihon/pdf/cyber-security-senryaku-set.pdf>

政府機関情報セキュリティ横断監視即応チーム（GSOC）が設置している情報収集監視機能GSOCセンサーにおいて、2013年度に認知された政府機関への脅威の件数は約508万件であり、2012年度の約108万件と比較して、5倍近くに急増している（図1参照）。これは、約6秒に1件脅威を検知していることになり、常時サイバー攻撃を受けている状態と言える。

図1　GSOCセンサーで認知された政府機関への脅威の件数の推移



（出典）情報セキュリティ政策会議「2013年度サイバーセキュリティ政策に係る年次報告（2013年度）」2014.7.10, p.9. <http://www.nisc.go.jp/active/kihon/pdf/jseval_2013.pdf> を基に三菱総合研究所作成。

こうした状況の中、政府の情報セキュリティ予算は2013年度の当初予算額239.9億円に対して2014年度の当初予算額は542.3億円と2倍以上の規模に増加しており、表1に示すように2014年度予算においては、関係省庁においてサイバー攻撃に関する情報収集、検知、対応能力の強化を目的とした施策が掲げられた。このほか、2012年6月には省庁横断でサイバー攻撃対応を行うための情報セキュリティ緊急支援チーム（CYMAT）が設置され、2014年4月には自衛隊にサイバー防衛隊が設置されるなど、政府のサイバー攻撃への対応体制の整備も進んでいる。

表1　2014年度情報セキュリティに関わる政府の主な施策と予算額

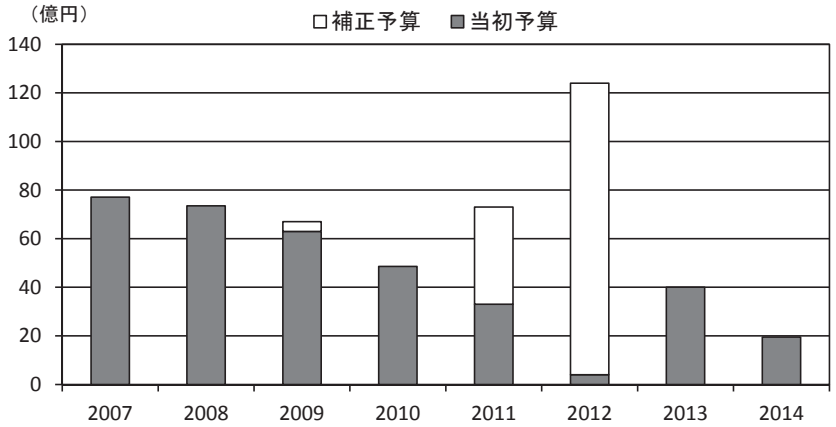
内閣官房	政府機関・情報セキュリティ横断監視・即応チーム（GSOC）の運用	6.3億円
警察庁	大規模サイバー攻撃事態に対処するための機能の強化	3.8億円
総務省	サイバー攻撃複合防御モデル・実践演習	4.5億円
外務省	情報セキュリティ対策の強化	4.0億円
経済産業省	サイバーセキュリティ経済基盤構築事業	17.4億円
経済産業省	独立行政法人情報処理推進機構運営費交付金	37.4億円
防衛省	防衛情報通信基盤（DII）の整備（器材の整備）（クローズ系）	127.6億円
防衛省	サイバー情報収集装置の整備	12.2億円

（出典）内閣官房情報セキュリティセンター「政府の情報セキュリティに関する予算について」（第38回情報セキュリティ政策会議資料7）2014.1.23, p.1. <http://www.nisc.go.jp/conference/seisaku/dai38/pdf/38shiryou0700.pdf>を基に三菱総合研究所作成。

一方で、政府の情報セキュリティの研究開発予算については図2に示すとおり、2011年度及び2012年度に補正予算等により大幅に増加している分を除けば、当初予算ベースでは年々減少基調にあり、直近の2014年度予算は20億円弱となっている。研究開発予算が減少している理由について、2014年に情報セキュリティ政策会議で決定された「情報セキュリティ研究開発戦略（改定版）」では大規模サイバー攻撃事態に対処するための機能の強化、サイバー情報収集装置の整備等、より実践的な施策の推進に重点を置いた結果と説明されている(2)。

一方、海外の状況に目を向けると、米国、欧州、韓国において情報セキュリティの研究開発予算は年々増加している(3)。米国の2014年度のサイバーセキュリティの研究開発予算は7.67億ドル（約890億円）(4)（推定）であり、前年度6.53億ドル（約760億円）から大きく増加している(5)。なお、米国のサイバーセキュリティ政策全体の予算も2013年度は120億ドル（約1兆4000億円）、2014年度は130億ドル（約1兆5000億円）と増加傾向にある(6)。米国においても日本と同様にサイバーセキュリティの研究開発においてサイバー防衛能力の向上が最大の課題となっており、2014年度のサイバーセキュリティ研究開発予算7.67億ドル（約890億円）のうち、国防総省が1.92億ドル（約220億円）、国防総省の研究機関である国防高等研究計画局（Defense Advanced Research Projects Agency: DARPA）が2.94億ドル（約340億円）と国防関連省庁の予算が全体の約63%を占めている(7)。

図2　日本政府の情報セキュリティ研究開発予算の推移



（出典）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, p.4. <http://www.nisc.go.jp/active/kihon/pdf/kenkyu2014.pdf> を基に三菱総合研究所作成。

(2)　民間の研究開発の状況

一方、②経済成長につながる新産業創出、③国際競争力の向上の観点では、民間分野における積極的な研究開発の実施が必須である。しかし、国内の情報セキュリティ事業者は厳しい状況に立たされている。2014年の国内の情報セキュリティ市場規模は7978億円と予測されてお

(2)　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, p.6. <http://www.nisc.go.jp/active/kihon/pdf/kenkyu2014.pdf>

(3)　内閣官房情報セキュリティセンター「各国の情報セキュリティ研究開発に係る状況について」（内閣官房情報セキュリティセンター委託事業（委託先：NTTデータ経営研究所））（情報セキュリティ政策会議第23回技術戦略専門委員会参考資料1）2014.4.4. <http://www.nisc.go.jp/conference/seisaku/strategy/dai23/pdf/23sankou01.pdf>

(4)　日本円への換算は、日本銀行基準外国為替相場及び裁定外国為替相場（2015年1月中において適用）に基づき計算：1ドルについて本邦通貨116円。

(5)　The Networking and Information Technology Research and Development Program,“FY2015 Supplement to the President's Budget,”March 2014, pp.8-9. <https://www.nitrd.gov/pubs/2015supplement/FY2015NITRDSupplement.pdf>

(6)　“Obama Boosts Pentagon Cyber Budget Amid Rising Attacks,”April 11, 2013. Bloomberg Website <http://www.bloomberg.com/news/2013-04-10/lockheed-to-general-dynamics-target-shift-to-cyber-spend.html>

(7)　The Networking and Information Technology Research and Development Program, *op.cit*. (5)

り、近年は5%前後の成長を続けている(8)が、2014年の世界全体の情報セキュリティ市場は711億ドル（約8兆2500億円）と予測されており、2013年からの成長率は8%近くに達し、また2014年から2015年にかけても8.2%の成長が予想されている(9)。世界市場と比べて国内市場の成長率が鈍化してしまう要因として、国内の需要側で情報セキュリティ対策の必要性が認識されず適切な投資がなされていないという問題と、供給側の国内の情報セキュリティ事業者が技術力の高い製品やサービスを提供できていない可能性とがある。2010年度に情報処理推進機構（IPA）が実施した調査では、国内の情報セキュリティ企業における研究開発の課題として、資金や人材の確保が難しく研究開発が十分に行えないという実態が指摘されている(10)。

人材に関しては、「Ⅱ 人材育成」に示すとおり、近年、情報セキュリティ人材の不足状況が続いており、人材の「需要」と「供給」のバランスを確保していく取組が別途必要となる。

資金に関しては、一部の大手のセキュリティベンダやセキュリティサービス事業者であれば、売上に対して一定の割合を研究開発投資に割り当て、そこで得られた成果をビジネスに活用するという取組が可能であるが、資金不足で研究開発を十分に実施できないベンダや事業者は製品やサービスにおいて技術優位性を保てず、業界における競争力を失い、ますます研究開発の資金が不足するという悪循環に陥ることが容易に想像できる。日本の情報セキュリティ産業の現状は、大手システムインテグレータや主要なセキュリティ対策ツールを供給する海外ベンダが市場を占有する一方で、参入事業者の数では事業規模が小さい中小事業者が多くを占めるのが実態である。本来、技術力を経営の軸とし、研究開発に積極的に投資すべきベンチャー企業や中小企業においても、資金の確保が困難でそれを実践できない状況にある(11)。

近年では、サイバーセキュリティ分野で世界的な大手ベンダによるM&A（合併・買収）が相次いでおり(12)、大手と事業規模で差をつけられた国内事業者は厳しい環境に立たされている。

国内の情報セキュリティ産業の競争力低下を阻止するためにも、革新的なテーマに関するハイリスクな研究や、直接的にはビジネスにはつながりにくいが長期の継続的な取組が必要な研究分野など、民間企業だけでは経済性の観点で資金の調達が困難な分野に関しては、国が積極的に予算を投入していくことが必要となる。

すでに民間企業が技術開発に対して公的資金を活用する仕組みはあるが、前述のとおり、国の情報セキュリティの研究開発予算自体が年々縮小しており、また、こうした資金の柔軟性や融通性が低いため、民間企業の技術開発に対する支援制度として十分に機能していないという課題もある。また、ベンチャーキャピタル等の企業・産業育成型資金の供給が限定的であるため、有望な技術を持つベンチャー企業であっても、成長が困難といった状況もある。(13)

---

(8)　日本ネットワークセキュリティ協会「2013年度情報セキュリティ市場調査報告書（V1.0）」2014.5, p.3. <http://www.jnsa.org/result/2014/surv_mrk/2013_mrk-report_v1.0.pdf>

(9)　Gartner Inc.,“Gartner Says Worldwide Information Security Spending Will Grow Almost 8 Percent in 2014 as Organizations Become More Threat-Aware,”August 22, 2014. <http://www.gartner.com/newsroom/id/2828722>

(10)　情報処理推進機構「情報セキュリティ産業の構造と活性化に関する調査報告書」2011.6, pp.26-27. <http://www.ipa.go.jp/files/000024418.pdf>

(11)　同上, p.26.

(12)　2010年情報セキュリティ製品大手企業SymantecがVerisignのセキュリティ事業（個人認証・電子証明事業）を買収、2011年にはIntelが情報セキュリティ製品大手企業McAfeeを買収している。

(13)　情報処理推進機構　前掲注(10), pp.i, 74-75.

2　政府の取組

「サイバーセキュリティ戦略」では、サイバー攻撃が複雑・巧妙化する中で、「変化の激しい情勢に適切に対応できる、創意と工夫に満ちた情報セキュリティ技術」(14)を生み出すことが重要としている。「情報セキュリティ研究開発戦略（改定版）」では、サイバーセキュリティ戦略の指摘を踏まえ、今後の日本の情報セキュリティ研究開発の推進方針を整理している（表2参照）。

さらに、研究開発の効果・成果を高めるための方策として、研究成果の社会還元を推進する仕組みや、国の研究開発予算の増加、研究者が研究資金や支援制度を利用しやすい仕組みの強化等が掲げられている(15)。

表2　情報セキュリティ研究開発の推進方針

1. サイバー攻撃の検知・防御能力の向上 研究開発における実際のサイバー攻撃情報等の重要性に鑑み、分散しているサイバー攻撃情報等の共有のための組織等の連携強化、可能な範囲・方法・条件で研究者等へ政府の有する標的型攻撃等の検体等の提供等を検討。
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 社会システム等を構成する制御システム等のセキュリティ技術の研究開発に当たっては成果の早期実用化が重要であることに鑑み、国際標準化・認証制度につながるよう推進。
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 産業活性化・国際競争力の強化の観点から、今後発展が期待されるICT利用分野で企画・研究開発・設計段階等上流工程からセキュリティ品質を組込み等の取組を促進。
4. 情報セキュリティのコア技術の保持 暗号等の基礎研究を始め情報セキュリティのコア技術の保持は、我が国の新規産業創出や安全保障等の観点から重要であり、大学・公的研究機関等の役割も含めて維持・強化。
5. 国際連携による研究開発の強化等 サイバーセキュリティに係る高度な技術の研究開発に向け、各国が「強み」を有する技術を組み合わせ発展させるなどのため、研究者受け入れを含め国際連携を推進。

（出典）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.12-19. <http://www.nisc.go.jp/active/kihon/pdf/kenkyu2014.pdf>を基に三菱総合研究所作成。

また、民間企業では十分に研究開発が実施されていない分野については、政府や公的研究機関（情報通信研究機構（NICT）、産業技術総合研究所（AIST）、防衛省技術本部等）、大学等がそれぞれの役割において研究開発に取り組むことが重要としている。特に、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た（表3参照）。

(14)　情報セキュリティ政策会議　前掲注(1), p.35.
(15)　情報セキュリティ政策会議　前掲注(2), pp.20-23.

表3　情報セキュリティの研究開発において国として推進すべき重要分野

(1) 情報通信システム全体のセキュリティの向上 ① サイバー攻撃の検知／防御 ② ID連携／認証／アクセス制御 ③ ITサービスのセキュリティ（スマートフォン／クラウド等） ④ 次世代ネットワークセキュリティ
(2) ハードウェア・ソフトウェアのセキュリティ向上 ⑤ 制御システムセキュリティ ⑥ セキュリティデバイス ⑦ ソフトウェアの安全性確保
(3) 個人情報等の安全性の高い管理の実現 ⑧ プライバシー保護／パーソナルデータ利活用のための技術 ⑨ フォレンジック（＊）等を支援するためのデータ管理・追跡技術
(4) 研究開発の促進基盤の確立と情報セキュリティ理論の体系化 ⑩ 情報セキュリティ理論の体系化／調査研究 ⑪ 標準化／評価／制度／基盤整備 ⑫ 暗号技術
(5) 発展が期待される応用分野でのセキュリティ確保 ⑬ 医療健康分野、農業分野で必要となるセキュリティ技術 ⑭ 次世代インフラで必要となるセキュリティ技術 ⑮ ビッグデータにおける情報の秘匿化、暗号化などのセキュリティ技術 ⑯ 家電、自動車等のネットワーク接続で必要となるセキュリティ技術

（＊）犯罪行為や法廷紛争における原因究明、証拠発見のための分析のこと。機器や電子データに対するものをデジタルフォレンジック、ネットワークに対するものをネットワークフォレンジックなどと呼ぶ。
（出典）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, p.25. <http://www.nisc.go.jp/active/kihon/pdf/kenkyu2014.pdf>を基に三菱総合研究所作成。

Ⅱ　人材育成

本章では、情報セキュリティ人材が不足する現状及び、政府及び教育機関による情報セキュリティ人材の育成、発掘に関わる取組・課題について取り上げる。

1　情報セキュリティ人材の現状

情報セキュリティの脅威の高まりに伴い、政府や企業等の組織で情報セキュリティ対策を担う人材、また情報セキュリティ産業において商品やサービスを開発・販売する人材の不足が深刻化している。2012年4月に情報処理推進機構（IPA）が公表した「情報セキュリティ人材の育成に関する基礎調査」の結果によれば、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23万人であり、不足人材は約2.2万人と推計されている（図3参照）。なお、23万人のうち情報セキュリティのスキルを満たしている人材は約9.3万人にとどまり、残りの約13.7万人はさらにスキルの育成が必要とされると推計されている。(16)

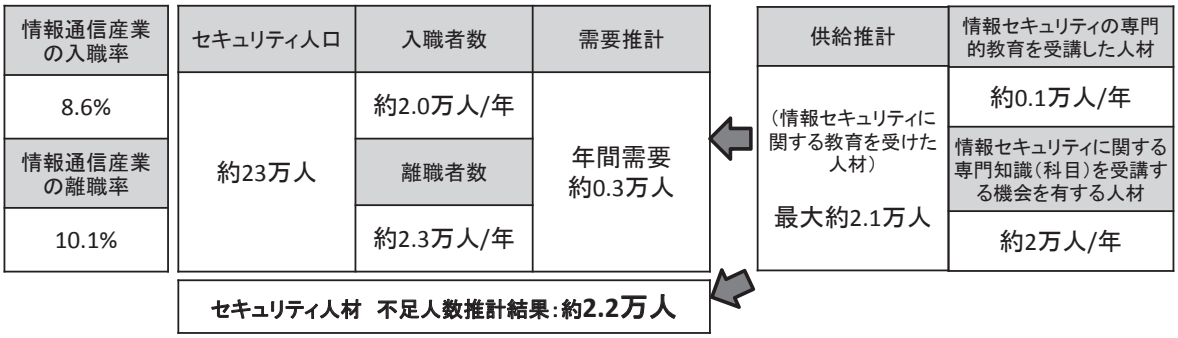
一方、国内で情報セキュリティの専門的教育を受講している人材は年間約1,000人で、情報セキュリティの専門知識（科目）を受講する機会を有する（科目を選択可能）人材は年間約2万人と推計されている。つまり、教育機関が産業界に供給しうる情報セキュリティに関する教育

(16) 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.63-66. <http://www.ipa.go.jp/files/000014184.pdf>

を受けた人材は、最大でも年間約2.1万人となる。(17)

さらに、情報通信産業の入職率と離職率を元に推計すると年間の情報セキュリティ人材の新規需要数は約0.3万人とされ、前述のとおりすでに約2.2万人の人材が不足しているため、調査実施時点（2011年12月）の情報セキュリティ人材の需要数は約2.5万人と推計される。しかし、前述の情報セキュリティに関する教育を受けた人材（最大年間約2.1万人）のうち、実際に需要側の企業や団体に雇用される人材は一部であり、需要数を満たすには不十分である。今後、早期に情報セキュリティ人材不足を解消するため、政府及び教育機関として情報セキュリティの専門的教育の拡充や専門的教育の受講機会の増加による情報セキュリティ人材の供給量の増加策が急務となっている。(18)

図3　情報セキュリティ人材の需給に関する分析



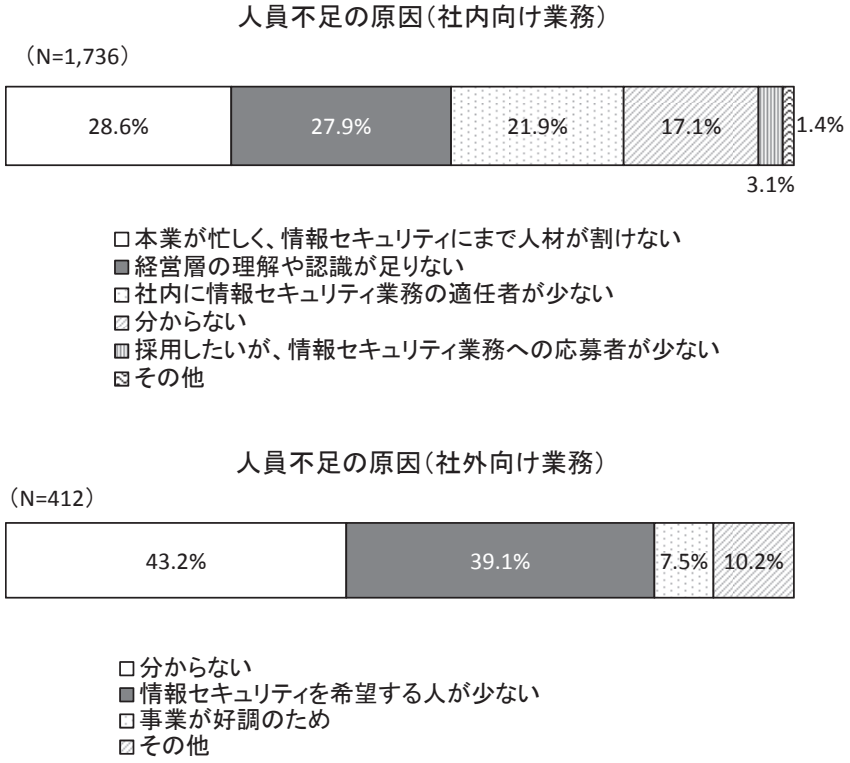
（出典）情報処理推進機構「情報セキュリティ人材の育成に関する基礎調査―調査報告書―」2012.4, pp.75-76. <http://www.ipa.go.jp/files/000014184.pdf>を基に三菱総合研究所作成。

また、同調査で実施したアンケート調査では、情報セキュリティ人材の不足の原因として、社内向けの情報セキュリティ業務を行う担当者に関しては、「本業が忙しく、情報セキュリティまで人材が割けない」、「経営層の理解や認識が足りない」、「社内に情報セキュリティ業務の適任者が少ない」などが挙げられている。また、社外に情報セキュリティを業務として提供しているベンダ等の担当者に関しては、「情報セキュリティを希望する人が少ない」という意見が挙げられている（図4参照）(19)。

こうした結果は情報セキュリティが経営上の優先課題として認識されていないことが原因にあると考えられ、組織内、特に経営層等上位層の意識改革が必要とされている(20)。

(17)　同上, pp.69-74.
(18)　同上, pp.75-76.
(19)　同上, pp.45-46.
(20)　同上, pp.67-68.

図4　情報セキュリティ人材不足の原因



（注）自社の情報セキュリティ人材の人数が足りていないと回答した回答者に対する設問。数字は回答者の割合（%）。
（出典）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.45-46. <http://www.ipa.go.jp/files/000014184.pdf>を基に三菱総合研究所作成。

国際的にもサイバーセキュリティの人材不足は課題となっている。米国でも近年サイバーセキュリティ人材の需要が急速に増えたことから2007年頃から人材不足が顕在化している。特に、民間企業に比べて報酬が少ない政府機関の国家安全保障や諜報機関に従事する人材不足が深刻化している(21)。

日本では、2020年に東京でオリンピック・パラリンピックが開催されることが決定し、国際的にも日本の情報通信技術の利活用能力やサイバー攻撃に対する防御能力を高めることが求められており、それを支えるサイバーセキュリティ人材の育成は今後ますます必要となってくると考えられる。

2　サイバーセキュリティ人材の育成・確保に係る政府・教育機関の取組・課題

(1)　サイバーセキュリティ人材の育成・確保のための政府戦略

「サイバーセキュリティ戦略」では、情報セキュリティ人材の不足解消に向けた積極的取組として、サイバーセキュリティ従事者の能力の底上げ、突出した人材の発掘・育成、グローバル水準で活躍できる人材の育成、政府機関等による情報セキュリティ人材の外部登用等を掲げている(22)。

(21) Martin C. Libicki et al.,“H4CKER5 WANTED: An Examination of the Cybersecurity Labor Market,”June 18, 2014, p.xii. <http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf>
(22) 情報セキュリティ政策会議　前掲注(1), pp.36-37.

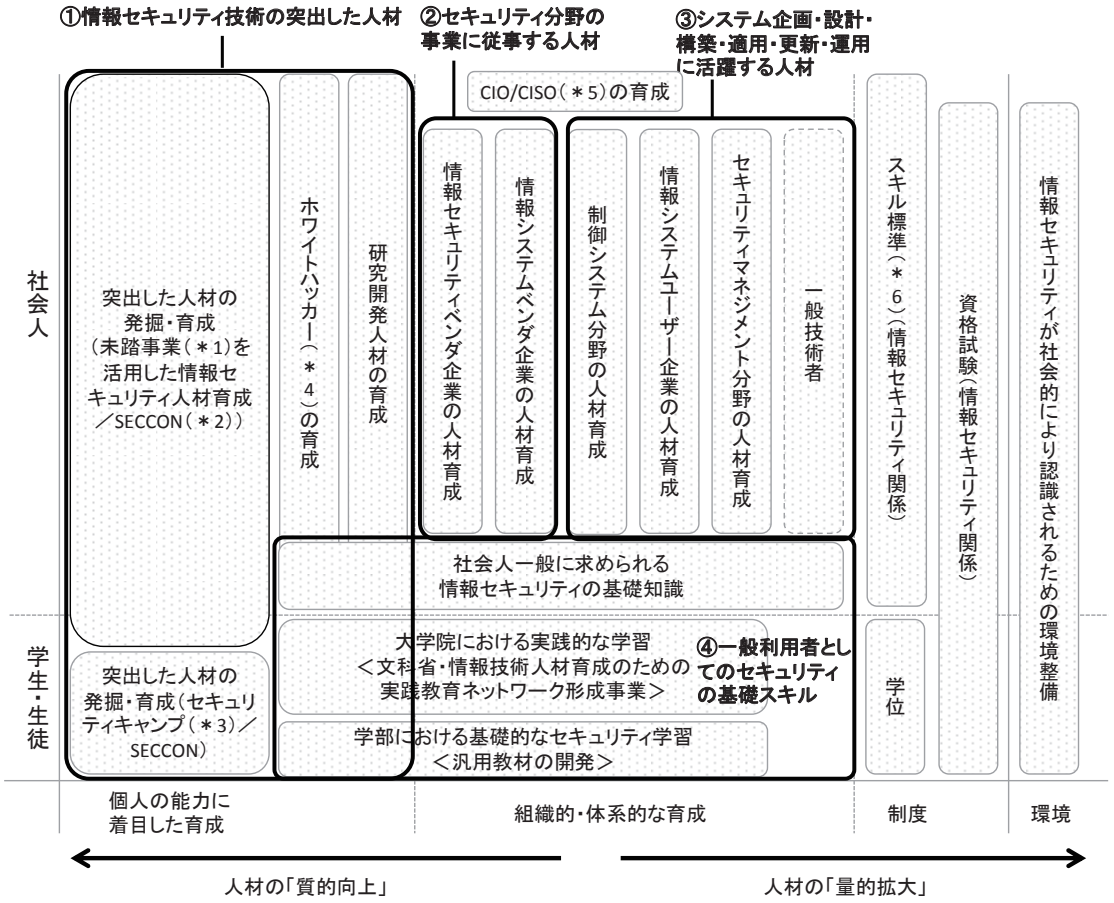
2014年5月に情報セキュリティ政策会議が決定した「新・情報セキュリティ人材育成プログラム」においては、「我が国の情報セキュリティの水準を高めるため、人材の「需要」と「供給」の好循環を形成。」[23]とする基本方針が示された。

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[24]。

情報セキュリティ人材と一括りにしても、情報セキュリティに関わる技術的な研究を行う研究者や、製品・サービスを開発するベンダの人材、情報システムを利用する企業や組織における情報セキュリティの担当者、また、情報セキュリティに関わる業務に直接携わることはないものの情報システムを利用する中で情報セキュリティの基礎的な知識が求められる人材まで多種多様であり、それぞれの属性に合った育成方法を考える必要がある。2012年に公表された「産業構造審議会情報経済分科会人材育成WG」の報告書では、図5に示すように情報システムのライフサイクル（システムの企画から、開発、運用、保守に至るまでの一連の過程）に注目して情報セキュリティ人材を、①情報セキュリティ技術の突出した人材、②セキュリティ分野の事業に従事する人材、③システム企画・設計・構築・適用・更新・運用に活躍する人材、④一般利用者としてのセキュリティの基礎スキルという4つに整理している[25]。

(23) 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>
(24) 同上, pp.5-8.
(25) 経済産業省商務情報政策局情報処理振興課「産業構造審議会情報経済分科会人材育成WG報告書―次世代高度IT人材像、情報セキュリティ人材、今後の階層別の人材育成」2012.9.14, p.27. <http://www.meti.go.jp/committee/sankoushin/jouhoukeizai/jinzai/pdf/report_001_00.pdf>

図5　情報セキュリティ人材の整理



（＊1）　情報処理推進機構が2000年から実施する、独創的なアイディア・技術とこれらを活用する優れた能力を持つ若い人材を発掘・育成することを目的とした事業。
（＊2）　日本ネットワークセキュリティ協会が2012年から実施する、セキュリティの攻撃と防御の立場における能力を競う競技イベント。
（＊3）　情報処理推進機構が2004年から実施する、次世代を担う日本発で世界に通用する若年層の情報セキュリティ人材を発掘・育成するため、産業界、教育界から結集した講師によって実施されるキャンプ・勉強会。
（＊4）　ネットワークやコンピュータに関する高度な知識や技術を持つ者を意味する「ハッカー」のうち、特にその技術を善良な目的に活かす者のこと。
（＊5）　CIOは、Chief Information Officerの略で、最高情報責任者のこと。組織内の情報システムや情報流通を統括する。CISOは、Chief Information Security Officerの略で、最高情報セキュリティ責任者のこと。組織内の情報管理及びその運用を担当し、情報セキュリティを統括する。
（＊6）　情報処理推進機構が策定するIT関連サービスの提供に必要とされる能力を明確化・体系化した指標。
（出典）経済産業省商務情報政策局情報処理振興課「産業構造審議会情報経済分科会人材育成WG報告書―次世代高度IT人材像、情報セキュリティ人材、今後の階層別の人材育成―」2012.9.14, p.27. <http://www.meti.go.jp/committee/sankoushin/jouhoukeizai/jinzai/pdf/report_001_00.pdf>を基に三菱総合研究所作成。

(2)　具体的施策の例

すでに行われている政府の取組として、人材の「量的拡大」に関連したものでは、年間約50万人が受験するIT人材の国家試験である情報処理技術者試験において、情報セキュリティに関する出題を拡充するほか、既存の「情報セキュリティスペシャリスト」に加え情報セキュリティに関する新たな試験区分の新設が検討されている(26)。こうした国家試験を有効に活用する

(26)　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」（情報セキュリティ政策会議第11回普及啓発・人材育成専門委員会資料2-5）2014.6.18, p.3. <http://www.nisc.go.jp/conference/seisaku/jinzai/dai11/pdf/shiryou0205.pdf>

ため、政府の調達を行う際に、契約相手に情報セキュリティスペシャリスト試験合格者や、さらに国際資格であるCISSP（Certified Information Systems Security Professional）等の資格保有者を求める事例もある(27)。

また、情報セキュリティ人材のニーズの高まりを受けて、大学等の教育現場でも情報セキュリティに関する専門教育課程・科目の設置や情報処理技術者試験の講義への活用等の取組が進みつつある（表4参照）。

表4　情報セキュリティ教育の取組事例

情報セキュリティ教育を行う教育課程等の区分	大学・学部名	特徴
情報セキュリティに関する専門教育課程	電気通信大学 （情報理工学部総合情報学科）	ネットワークセキュリティ、ソフトウェアセキュリティ、暗号理論、コンテンツセキュリティ等のセキュリティ関連の講義を幅広く開講。（学科定員150名）
	情報セキュリティ大学院大学、中央大学、東京大学 （修士課程）	2008年度から開始された、3大学と8企業の産学連携による情報セキュリティ分野における世界最高水準の人材を育成するためのプログラム「研究と実務融合による高度情報セキュリティ人材育成プログラム」（ISSスクエア）の中で、セキュリティの研究と実務を融合した教育プログラムを提供。（2009年3月以降2013年11月まで、145名が教育プログラムを修了）
	奈良先端科学技術大学院大学、京都大学、大阪大学、北陸先端科学技術大学院大学 （修士課程）	2007年度から開始された、関西圏を中心とした4大学と4企業等が連携し、情報ネットワークの管理・運用の現場で活躍できる技術者・実務者を育成するプロジェクト「IT Keys」の中で、高度かつ実践的な教育プログラムを提供。（毎年4大学で20名程度が参加）
MBAコース	中央大学 （戦略経営研究科）	選択科目として、「ネットワーク時代のセキュリティとガバナンス」（2単位）を開講。
	青山学院大学 （国際マネジメント研究科）	選択科目として、「情報セキュリティ」（2単位）を開講。

（出典）内閣官房情報セキュリティセンター「情報セキュリティ人材育成に係る現状と今後の検討課題について」（情報セキュリティ政策会議第7回普及啓発・人材育成専門委員会資料4）2013.11.6, p.6. <http://www.nisc.go.jp/conference/seisaku/jinzai/dai7/pdf/shiryou04.pdf>等を基に三菱総合研究所作成。

人材の「質的向上」に関連したものでは、ITに対する意識の高い若者に対して合宿形式で情報セキュリティやプログラミングに関する高度な教育を実施するセキュリティキャンプ（2004年開始）やセキュリティの攻撃と防御の立場における能力を競う競技イベントSECCON（2012年開始）等が開催されている(28)。

また、各分野におけるサイバーセキュリティ担当者の技術力や対応能力向上のため、各種の演習も活用されている。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））ではIT障害発生時における重要インフラサービスの維持や早期復旧能力の向上

(27) 内閣官房情報セキュリティセンター「情報セキュリティ人材の必要性について」2012.11, p.23. <http://www.nisc.go.jp/security-site/glossary/nisc.pdf>

(28)「セキュリティ・キャンプ」情報処理推進機構ウェブサイト <https://www.ipa.go.jp/jinzai/camp/index.html>;「SECCON とは」SECCON CTFウェブサイト <http://www.seccon.jp/p/seccon.html#consortium>

を目的に2006年度から毎年、全重要インフラが参加した「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[29]、制御システムセキュリティセンター（CSSC）は2012年度から制御システムにおける脅威の認識、インシデント対応の妥当性検証のためのサイバーセキュリティ演習を実施している[30]。また、総務省でも2013年度から、官公庁や大企業等のLAN管理者のサイバー攻撃への対応能力向上のため、組織内ネットワークを模擬した大規模環境による実践的なサイバー防御演習「CYDER（CYber Defense Exercise with Recurrence）」を実施し、多くの組織が参加している[31]。文部科学省においても、15の大学が参加した、最先端の情報技術を実践的に活用することができる人材育成プログラム「分野・地域を越えた実践的情報教育協働ネットワーク（Education Network for Practical Information Technologies: enPiT）」を2012年から開始している[32]。このほか、個別分野や大学、企業等様々な単位で、演習を実施する動きが広がっている。

政府機関における人材育成の取組としては、情報セキュリティ担当者に関わる組織の人事ローテーションの工夫や、専門的な知識・経験を持つ外部人材の活用、公務員採用時における情報セキュリティ関連素養の確認を行う等の取組が行われている[33]。

さらに、政府は2015年度を目処にホワイトハッカーをNISCの任期付職員や研究員として採用する方針と報じられている[34]。しかし、能力が高く、かつ政府機関の職員として適正な人材を確保することは簡単ではない。

すでにホワイトハッカーを政府で積極的に採用している米国においても、政府機関では公務員規則（Civil Service Rules）によって、階級ごとに給与の上限が定められていたり、給与基準の柔軟性が低いことで、民間で高い報酬を受け取るだけの能力ある人材を確保することが難しくなっている。サイバーセキュリティに関わる人材不足は、国家安全保障の観点でも大きなリスクとなりうるため、公務員規則の緩和についても検討の必要があるとされており、実際に米国国家安全保障局（National Security Agency: NSA）では特別手当を支給したり、特に能力の高い人材については、上長よりも高い基準の給与支給を可能とする等柔軟な対応を行っている[35]。

また、政府機関のサイバーセキュリティに係る業務に必要となる能力や適性を図る指標の一つとして、エシカル・ハッカー[36]の認定資格（Certified Ethical Hacker: CEH等）が用いられているなど[37]、米国ではホワイトハッカーの重要性が広く認識されている。

---

(29)「重要インフラグループの取組」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/active/infra/torikumi.html>

(30) 制御システムセキュリティセンター「サイバーセキュリティ演習」2014.6. <http://www.css-center.or.jp/pdf/cybersecurity-exercises_outline.pdf>

(31) 総務省情報流通行政局情報セキュリティ対策室「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」―」（情報セキュリティ政策会議第11回普及啓発・人材育成専門委員会資料2-3）2014.6.18. <http://www.nisc.go.jp/conference/seisaku/jinzai/dai11/pdf/shiryou0203.pdf>

(32)「4つの分野」分野・地域を越えた実践的情報教育協働ネットワークウェブサイト <http://www.enpit.jp/fields/>

(33) 内閣官房情報セキュリティセンター「政府機関の情報セキュリティ担当者の育成等に関する事例について」（第8回情報セキュリティ対策推進会議参考資料1）2012.10.26. <http://www.nisc.go.jp/conference/suishin/ciso/dai8/pdf/s1.pdf>

(34)「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.

(35) Martin C. Libicki et al., *op.cit*. (21), pp.63-64.

(36) 倫理的ハッカー。ホワイトハッカーと同義。

(37) 例えば、国防総省の情報保証に関わる職員のベースラインスキルやそれを証明する資格等を示した国防総省指令8570（Department of Defense Directive 8570: DoDD 8570）におけるComputer Network Defenseカテゴリの資格としてCEHが採用されている。“Dept of Defense Directive (DoD) 8570.”EC-Council Website <http://www.eccouncil.org/Support/dod-8570>

III　ITリテラシー・情報倫理

本章では、国民のサイバーセキュリティに対する意識の底上げの重要性と政府の主な取組について、特にITリテラシーや情報倫理の観点から取り上げる。

1　ITリテラシーの重要性

ITリテラシーとは、インターネットや各種デバイス等の情報通信技術を使う上での基本的な知識や素養であり、一方、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。なお、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として「情報通信倫理」や、「情報モラル」等があるが、本章においては、これらを包含する概念として「情報倫理」の語を用いる。

増加するサイバー犯罪やインターネット上の様々なトラブルを防ぎ、情報通信技術を安全・安心に利用するためにも、情報通信技術の恩恵を受ける利用者全てが、このITリテラシーと情報倫理を習得することが重要である。しかし、急速に進展する情報通信技術に対して、多くのユーザのITリテラシーと情報倫理のレベルが追いついていないのが現状である。

近年増加するサイバー犯罪やインターネット上のトラブルは、利用者のITリテラシーや情報倫理の欠如に起因するところも大きい。特にスマートフォン等の高機能端末の一般ユーザへの急速な普及に伴い、トラブルが目立つようになってきた。スマートフォンの場合は、従来の携帯電話（フィーチャーフォン）と比較して、好きなアプリを入れてカスタマイズができるなど利用者の自由度が高い反面、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重要である。アプリの中にはスマートフォンの機能や端末の情報（端末のID、電話番号、電話帳の連絡先データ、端末の位置情報等）へのアクセスを求めるものもある。本来であれば、事業者側がこれらの情報の取得について、利用者にわかりやすく説明し、利用者が同意した上で利用されるべきであるが、利用者が想定していない動作を行う不正なアプリも横行しており、現時点では利用者自身が十分注意することが必要となっている。

また、SNSに関しても、利用目的や利用範囲によって自身の情報の公開範囲やプライバシーの設定を判断すべきであるが、こうした機能や設定を十分理解せずに使っているケースも多い。

最近では、SNSの利用を通じて情報倫理に対する意識の低さが露見してしまう事例も起きている。2013年に相次いで注目されたSNSでの不適切投稿によって発生した「炎上」トラブル（表5参照）を見ても、投稿が不特定多数から閲覧できること、発信者個人の情報が容易に特定できる状態であること、そもそも投稿が組織や社会に与える影響の大きさについて、発信者の考えが及んでいないことがうかがえる。不適切投稿による「炎上」トラブルの中には、数名のアルバイトの行為が原因で大企業が大きな損害を受ける結果となった事件もある。影響の大小はあるものの、ブログやSNS等個人の情報発信の場において、所属する組織や仕事に関する内容を発信して問題になるケースは一般の企業でも多く起きている。また、政府、企業においては個人が所有するスマートデバイスを業務で利用するBYOD（Bring your own device）の導入が進んでおり、ITリテラシー・情報倫理に関して、政府機関、企業内でも改めて教育を行う動きも広がっている。

表5　SNSを通じた炎上事件の事例

時期	事例の概要
2013年7月15日	高知県のコンビニエンスストアの店員がアイスクリームケースの中に入っている写真がインターネット上（Facebook）に公開される。コンビニエンスストアはその店員を解雇し、当該店舗とのFC契約を解除し、当該店舗の休業を決定した。
2013年9月3日	石川県の餃子店にて、来店した客が不適切な行為を行った上、当該画像を撮影し、インターネット上（Facebook）に公開した。この件を受け、餃子店側が客を告訴し、客9人が威力業務妨害と公然わいせつの疑いで逮捕、書類送検された。その後9人は軽犯罪法違反罪で略式起訴され、科料の略式命令を受けた。威力業務妨害については、嫌疑不十分として不起訴処分となり、公然わいせつ容疑については、軽犯罪法違反罪に切り替えられた(*1)。
2013年9月3日	北海道で女性が衣料品店で購入した商品を不良品と訴え、従業員に土下座させた上、その様子を撮影した写真をインターネット上（Twitter）に公開した。さらに自宅に来て謝罪するよう約束させたとして、その女性は強要容疑で逮捕された。その後女性は名誉毀損罪で罰金の略式命令を受け、強要罪では不起訴処分（起訴猶予）となった(*2)。

（＊1）「「餃子の王将」裸ネット画像：店内で全裸撮影、男9人略式命令－－金沢簡裁」『毎日新聞』（石川版）2013.12.20.
（＊2）「土下座写真をツイッター投稿、札幌の女に罰金30万円命令　強要容疑は不起訴」『朝日新聞』（北海道版）2013.10.26.
（出典）総務省編「第1部第4章第3節安心・安全なインターネット利用環境の構築」『平成26年版情報通信白書―ICT白書―』日経印刷, 2014, p.292. <http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h26/pdf/26honpen.pdf>ほか各種資料を基に三菱総合研究所作成。

2　政府の主な取組事例

2013年6月に高度情報通信ネットワーク社会推進戦略本部（IT総合戦略本部）が決定した「世界最先端IT国家創造宣言」（2014年6月改定）においては、「ITの利活用により子どもから高齢者まで、そのメリットを享受して豊かに生活を送ることができるよう、情報モラルや情報セキュリティに関する知識を含め、国民全体の情報の利活用力の向上を図る」(38)という国の方針が示された。現行の小学校・中学校・高等学校、特別支援学校の学習指導要領では、各教科において情報モラル教育の実施を求めている。また、小学校・中学校の道徳の学習指導要領において、情報モラルの指導に留意するよう明記されている。例えば、小学校における具体的な指導の例として、各教科においては正しい情報収集の方法や、情報を引用する際のルール、著作権に関する指導、道徳においては対面によるコミュニケーションとネット上の顔の見えないコミュニケーションの違いを題材とした指導等が想定されている(39)。

また、NISCでは一般向けに情報セキュリティの重要性について、国民の関心を高め、理解を深めるために「国民を守る情報セキュリティサイト」を運営している(40)。さらに、情報セキュリティ関連省庁では、国民に対する情報セキュリティに関する普及啓発強化のため、毎年2月を「情報セキュリティ月間」として、情報セキュリティに関わる関連行事を集中的に開催している。特に子どもたちをインターネット上のトラブルから守るために、主に保護者や教職員向けにインターネットの安全な利用に向けた啓発として、「イーネット安心講座（e-ネットキャラバン）」を全国で開催している。

(38)「世界最先端 IT 国家創造宣言の変更について」（平成26年6月24日閣議決定）p.24. <http://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20140624/siryou1.pdf>
(39)　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>
(40)　国民を守る情報セキュリティサイト <http://www.nisc.go.jp/security-site/>

2014年からは内閣府、総務省、経済産業省、内閣官房IT総合戦略室、警察庁、消費者庁、法務省及び文部科学省の連携事業として、学生等、多くの青少年が初めてスマートフォン・タブレット等を使い始める春の卒業・進学・新入学の時期に特に重点を置き、サービス提供事業者、関係団体、学校等、保護者が一体となって、普及啓発活動を行う「春のあんしんネット・新学期一斉行動」も開始されている。

そのほか、インターネット上で様々なサービスを提供する事業者自身も、トラブルを避けるための適切な利用方法について普及啓発を行っている。各事業者の取組をつなぎ効果的に活動を行うため、2009年には、主要なインターネット事業者からなる「安心ネットづくり促進協議会」が設立され、学校や地域において出前講座を提供するなどの普及啓発活動を行っている(41)。

執筆：株式会社三菱総合研究所　情報通信政策研究本部　研究員　丸田（まるた）　佳織（かおり）
監修：奈良先端科学技術大学院大学　教授　山口（やまぐち）　英（すぐる）

(41)「無料出前講座一覧」安心ネットづくり促進協議会ウェブサイト <http://www.good-net.jp/lectures/>