2014 年 12 月 24 日　全 7 頁

求められるサイバーセキュリティの人材育成

環境調査部　主任研究員
町井　克至

［要約］

- サイバー攻撃は、攻撃意図や対象が多様化するとともに手法も複雑化しており、特に経済・生活基盤への攻撃は被害が甚大になることもある。近年では国を越えたサイバー攻撃の例も見られるため、その脅威は世界中で警戒されている。

- 日本では 2014 年 11 月にサイバーセキュリティ基本法が成立した。国においてサイバーセキュリティを推進する体制が整備・強化されるとともに、国、地方公共団体、重要社会基盤事業者、サイバー関連事業者等が連携して対応する方針が示された。

- サイバーセキュリティを推進する上では、人材不足がひとつの課題となっている。高等教育機関卒業後の情報処理・通信技術者への就職者数は、リーマン・ショック前の水準を大きく下回っている。サイバーセキュリティの対象は今後も増え続ける可能性があるため、情報セキュリティ技術者の必要性は増している。

１．世界で高まるサイバーセキュリティのリスク

１－１．サイバー攻撃は大規模・深刻化

「サイバー攻撃」とは一般に、情報システムへの不正侵入などによる電子データの改竄、破壊、窃取や、情報システムや通信ネットワークそのものを機能不全に陥らせたりする行為などを指す。情報通信技術の進展とともに、攻撃の意図や対象、手法などがさまざまに変化しているという特徴がある。インターネットなどの通信ネットワークを経由した攻撃のほか、光学メディアや補助記憶装置（USB フラッシュドライブや SD メモリーカード等）などの媒体を介して悪意のあるコンピュータプログラム等を侵入させる手法なども存在する。そのような脅威に対して、電子データの安全管理や、情報システム及び通信ネットワークの安全性、信頼性を確保するために必要な措置が講じられ、適切に維持管理されていることを、サイバーセキュリティという[1]。

インターネットが普及して、多くの組織の情報システムや個人の情報端末等が通信ネットワ

[1] サイバーセキュリティ基本法（平成 26 年法律第 104 号）第 2 条

ーク上で相互接続するようになるにつれ、サイバー攻撃による被害が顕在化してきている。サイバー攻撃は、当初は愉快犯的なものが多かったが、年々深刻化しており、企業や行政機関等における機密情報や個人情報などのデータの窃取、実社会への悪影響を企図した情報システムの機能不全や破壊など、攻撃意図や対象が多様化するとともにその手法も複雑化している（図表１）。サイバー攻撃による脅威は、個人から企業、そして経済や生活の基盤に広がっており、国家安全保障の観点からもサイバーセキュリティの推進が急務となっている。

図表１　サイバー攻撃の変遷

	2001～2003年	2004年～2008年	2009年～2012年
時代背景	ネットワークウイルスの全盛	内部脅威・コンプライアンス対応	脅威のグローバル化
IT環境	コミュニケーション手段の確立	e-コマースの加速	経済・生活基盤に成長
セキュリティの意味合い	サーバーやPCの保護	企業・組織の社会的責任	危機管理・国家安全保障
攻撃の意図	・いたずら目的	・いたずら目的 ・金銭目的	・いたずら目的 ・金銭目的 ・抗議目的 ・諜報目的
攻撃傾向	ネットワーク上の攻撃	人を騙す攻撃の登場	攻撃対象の拡大
攻撃対象	PC、サーバー	人、情報サービス	・スマートデバイス ・重要インフラ
対策の方向	セキュリティ製品中心	マネジメント体制の確立	・官民・国際連携の強化 ・セキュリティ人材育成強化
主なセキュリティ事件	・Nimda流行（2001） ・Code Red流行（2001） ・SQL Slammer 流行（2003）	・P2Pソフトによる情報漏えい（2005～） ・不正アクセスによる情報流出（2005～） ・スパイウェアによる不正送金（2005～）	・米韓にDDoS攻撃（2009） ・イランを狙ったStuxnet（2010） ・政府機関を狙ったサイバー攻撃（2011） ・金融機関を狙った攻撃（2012）

（出所）独立行政法人情報処理推進機構「2013 年版 10 大脅威　身近に忍び寄る脅威」（2013 年 3 月）

１－２．世界中で発生するサイバー攻撃による被害

現実世界において人や物が移動する際には、港湾施設や国境に税関、セキュリティゲート、検疫所などが設けられ、必要に応じてパスポート等の公的証明書による本人確認などが行われる。しかし、インターネットなどの ICT の世界では、基本的に国境がなく、1 秒以内に地球の反対側へ到達することもでき、パスポートもない[2]。また、通信ネットワークを運用する通信事業者は、「通信の秘密」を保護する観点から、基本的にはどのような通信内容であっても運搬する[3]。

[2] 電子証明書などによって特定を試みる認証技術もあるが、設定が煩雑でコンピュータの取扱いに長けていないとわかりづらいなどの理由から、多くのウェブサイトでは本人確認をパスワード認証などで代替している。

[3] 攻撃者が身元を隠蔽するために、情報セキュリティ対策が十分でない個人の PC 等を乗っ取り、「踏み台」としてサイバー攻撃が行われることもある。そのような踏み台を複数台束ねたネットワークは「ボットネット」と呼ばれ、対策の困難さから世界的に問題となっている。警視庁「ボットネット対策」、警察庁「国際的なボットネットのテイクダウン作戦」など。そのような背景から、通信事業者が通信の秘密に配慮しつつ、サイバー攻撃への適切な対処を行うことが可能となるような検討結果も示されている。総務省「電気通信事業におけるサ

従って、通信ネットワーク経由のサイバー攻撃は現実世界で武力攻撃を行うよりもはるかに容易かつ安価に、対象に到達することができてしまう。情報通信技術が進展し、ICT が世界の経済や生活の基盤として重要な位置を占めるに伴い、特定の国内だけでなく国を越えたサイバー攻撃が行われるようになっており、甚大な被害も発生している（図表２）。ICT 先進国であるほど行政機関、金融、エネルギーなどの社会インフラに情報通信技術を積極的に取り入れており、サイバー攻撃による被害のリスクが大きいことが特徴と言える。

図表２　海外のサイバー攻撃による被害の例

発生年	被害国	内容
2007 年	エストニア	世界初の大規模なサイバー攻撃。約 3 週間の海外からの DDoS(注 1)攻撃などによって政府、金融、通信などのオンラインサービスが機能不全。
2009 年	韓国	政府、金融、放送への DDoS 攻撃によるオンラインサービス機能不全やスパイウェアによる乗っ取り、サーバ等数万台が停止。2011、2013 年にも。
2010 年	イラン	ウラン濃縮用遠心分離器を制御するシステムがコンピュータウィルスに感染して乗っ取られ、遠心分離器が全て稼働停止。
2012 年	イギリス	ロンドンオリンピック大会の期間中、公式サイトに 2 億回を超える攻撃。(注 2)

（注 1）Distributed Denial of Service、分散型サービス妨害。相手のコンピュータやルータ等に不正なデータを送信して使用不能に陥らせたり、トラヒックを増大させて相手のネットワークを麻痺させたりする攻撃を DoS(Denial of Service)攻撃といい、複数のネットワークに分散する大量のコンピュータが一斉に特定のサーバへパケットを送出し、通信路をあふれさせたり、大量の処理を実施させたりすることによって機能を停止させてしまう攻撃を DDoS 攻撃と呼ぶ。総務省「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会第一次とりまとめ」（平成 26 年 4 月 4 日）
（注 2）日本においても、2020 年東京オリンピック・パラリンピックに向けた対応が喫緊の課題とされる。独立行政法人情報処理推進機構　IPA サイバーセキュリティシンポジウム 2014「2012 年ロンドンオリンピックのセキュリティ」（オリバー・ホーア氏講演録）（平成 26 年 2 月 19 日）
（出所）各種報道・公開情報等を基に大和総研作成

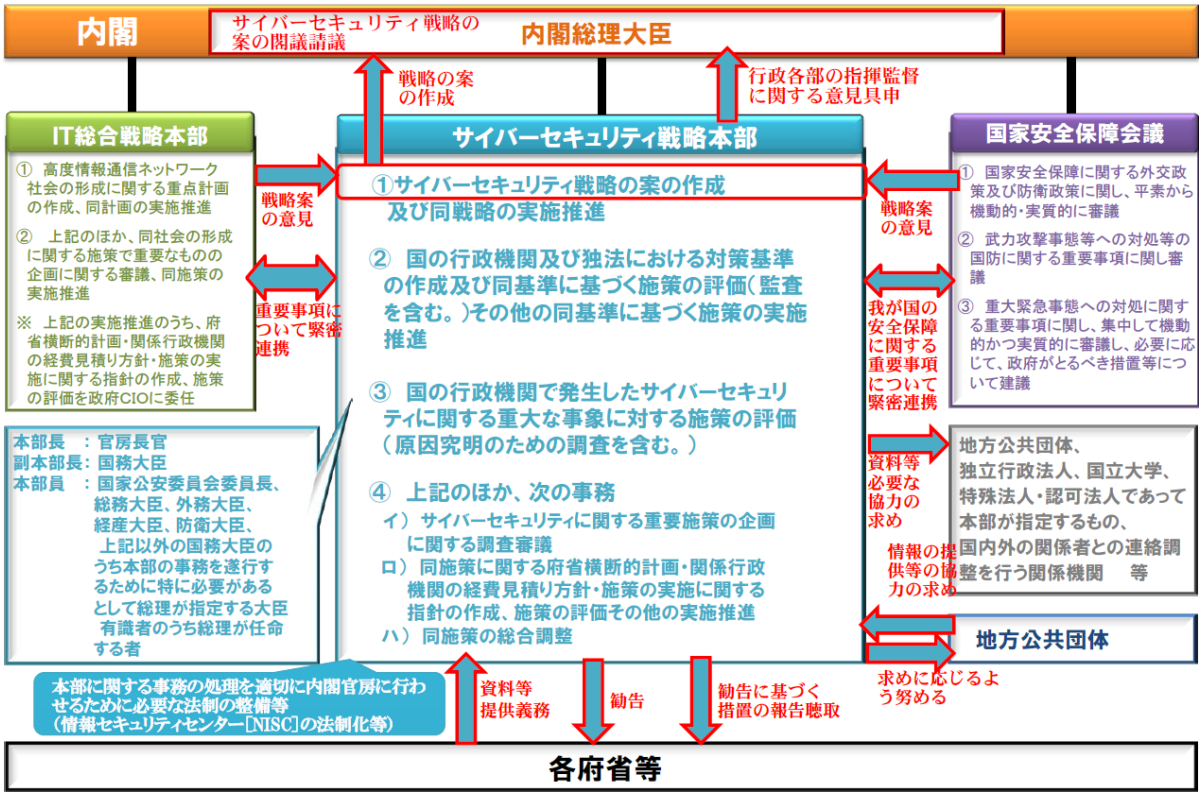
このような国を越えたサイバー攻撃は世界的に脅威と認識されており、世界経済フォーラムにおいてもそのリスクが報告されている [4]。それによると、サイバー攻撃（Cyber attacks）の顕在化リスクは水危機（Water crises）や気候変動（Climate change）と同等程度であり、影響度は政情・社会不安（Political and social instability）や所得格差（Income disparity）と同等程度とされる。また、サイバー攻撃はデータ改竄／窃取（Data fraud/theft）や重要な情報基盤の故障（Critical information infrastructure breakdown）と相互に強く関連しており、それらはテロ攻撃（Terrorist attack）やグローバルガバナンスの機能不全（Global governance failure）のリスクにも直結するとされる。

イバー攻撃への適正な対処の在り方に関する研究会第一次とりまとめ」（平成 26 年 4 月 4 日）
[4] World Economic Forum, Global Risks 2014, Jan. 16th 2014、以降の本文で参照。

２．日本におけるサイバーセキュリティ推進体制の更新

インターネットやその他の高度情報通信ネットワークの活用が進展するに伴い、世界的規模でサイバー攻撃による脅威が深刻となる中、日本においては 2014 年 11 月に、サイバーセキュリティ基本法（以下、CS 基本法）が成立、公布された。CS 基本法成立により、これまで IT 総合戦略本部が担ってきた日本のサイバーセキュリティ推進体制は、サイバーセキュリティに関する機能が新設する「サイバーセキュリティ戦略本部」に移管され、国家安全保障会議を合わせた 3 組織が緊密に連携する体制となる（図表３）。

図表３　サイバーセキュリティ戦略本部の機能・権限（イメージ）



（出所）情報セキュリティ政策会議　第 40 回会合（平成 26 年 7 月 10 日）資料１－２「（参考）『サイバーセキュリティ基本法』の概要」

CS 基本法においては、サイバーセキュリティの推進を国、地方公共団体、重要社会基盤事業者、サイバー関連事業者等の多様な主体が相互に連携して取り組むとしている。この重要社会基盤事業者とは、「国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものに関する事業を行う者」（CS 基本法第 3 条）とされており、具体的には「情報通信」「金融」「航空」「鉄道」「電力」「ガス」「医療」「水道」「物流」「化学」「クレジット」「石油」といった各分野の事業者となる[5]。

[5] 情報セキュリティ政策会議「重要インフラの情報セキュリティ対策に係る第３次行動計画」（平成 26 年 5 月

さらに CS 基本法では、いわゆる武力攻撃事態対処法[6]に規定する「緊急事態」に相当するようなサイバー攻撃の可能性に言及しており、その法制上の措置について検討することとされている（CS 基本法附則第 3 条）。重要社会基盤事業者に対するサイバー攻撃は、「国及び国民の安全に重大な影響を及ぼす」（武力攻撃事態対処法第 24 条）ことも想定され、国家安全保障上もその対策の重要性が認識されている。

３．不足する情報セキュリティ人材

３－１．情報セキュリティ人材の育成が課題

国は 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、国家の安全保障・危機管理、社会経済の発展、国民の安全・安心確保のため、世界を率先する強靭で活力あるサイバー空間を構築し、「サイバーセキュリティ立国」を実現することを基本的な方針としている。

平成 27 年度予算概算要求では、情報セキュリティに関する予算として 367.8 億円が計上されている[7]。主な内訳は、NISC[8]の機能強化、サイバー攻撃複合防御モデル・実践演習／ＩＣＴ環境の変化に応じた情報セキュリティ対応方策の推進事業、ネットワーク監視器材の整備などであり、当面の対処として必要とされる設備・体制の整備等が進められようとしている。

サイバーセキュリティの推進にあたっては、国のそのような対応と並行して、特に重要社会基盤事業者におけるサイバーセキュリティ推進や情報セキュリティ人材の十分な確保が重要であり、積極的かつ継続的な取組みが望まれる。

しかし、日本の情報セキュリティ人材は不足していると指摘されている。独立行政法人情報処理推進機構が 2012 年に報告したアンケート調査結果[9]によると、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、不足する人材数は約 2.2 万人と推計されている。また、技術者約 23 万人中、必要なスキルを満たしていると考えられる人材は 9 万人強であり、残りの 14 万人あまりの人材に対しては更に何らかの教育やトレーニングを行う必要があるとされている。

前述のアンケート調査では企業における情報セキュリティ人材の不足が示されているが、高等教育機関からも人材を供給できていない可能性が推察される。これは、高等教育機関が企業の求める人材像に即したスキルを持つ人材を供出できていない、需要はあるものの本業への注

---

19 日）

[6] 「武力攻撃事態等における我が国の平和と独立並びに国及び国民の安全の確保に関する法律」（平成 15 年法律第 79 号）

[7] 情報セキュリティ政策会議　第 41 回会合　資料３「政府の情報セキュリティに関する予算」（平成 26 年 11 月 25 日）

[8] National Information Security Center、内閣官房情報セキュリティセンター。CS 基本法により法制化を含む措置が講じられる見込み（CS 基本法附則第 2 条）。

[9] 独立行政法人情報処理推進機構「『情報セキュリティ人材の育成に関する基礎調査』報告書について」（2014 年 7 月更新）、以降の本文で参照。

力などの理由から企業が人材獲得の優先順位を下げている、といった理由が考えられる。また、そもそも高等教育機関を卒業する人材が、情報通信業そのものに魅力を感じていないという可能性もある。いずれであっても、サイバーセキュリティを推進する上では課題であろう。

サイバーセキュリティに関する人材育成の観点では、2014 年 7 月に決定された「サイバーセキュリティ 2014」において、20 項目に及ぶ各省庁の施策が盛り込まれている。内閣官房が主導する施策としては、情報セキュリティ政策会議が策定した「新・情報セキュリティ人材育成プログラム」がある。同プログラムでは、情報セキュリティ人材が不足している背景から、サイバーセキュリティに関して高度な専門性及び突出した能力を有する人材や、グローバル水準の人材の必要性を認識し、6 つの取組み方針を示している（図表４）。

図表４　「新・情報セキュリティ人材育成プログラム」における今後の取組方針

（1）経営層の意識改革
①経営戦略の一部としての情報セキュリティ対策の推進
②実務者層のリーダー層に対する組織内部におけるコミュニケーション能力の強化
③調達における情報セキュリティ要件の設定
（2）必須能力としての情報セキュリティ
①情報通信に携わる技術者が情報セキュリティを基礎能力として身につけるための取組
②情報セキュリティ能力の評価基準･資格等の整備
③情報セキュリティのスキル向上のための実践的取組の実施
（3）高度な専門性及び突出した能力を有する人材の発掘･育成
①高度な専門性を持った情報セキュリティ人材育成のための高等教育の強化
②最先端の分野で活躍する突出した人材の発掘及び更なる能力向上
（4）グローバル水準の人材の育成
（5）政府機関等における人材育成
①サイバー空間を取り巻くリスクに対応できる職員の採用･育成
②政府職員全体の情報セキュリティ意識の啓発と研修･訓練の実施
③重要インフラ事業者等における人材育成
（6）教育機関における情報通信技術教育の充実等
①初等中等教育段階における情報通信技術に関する教育の充実
②高等教育段階における実践的能力を高める演習の強化
③情報セキュリティに関する教員の養成
④情報セキュリティ人材のキャリアパス提示

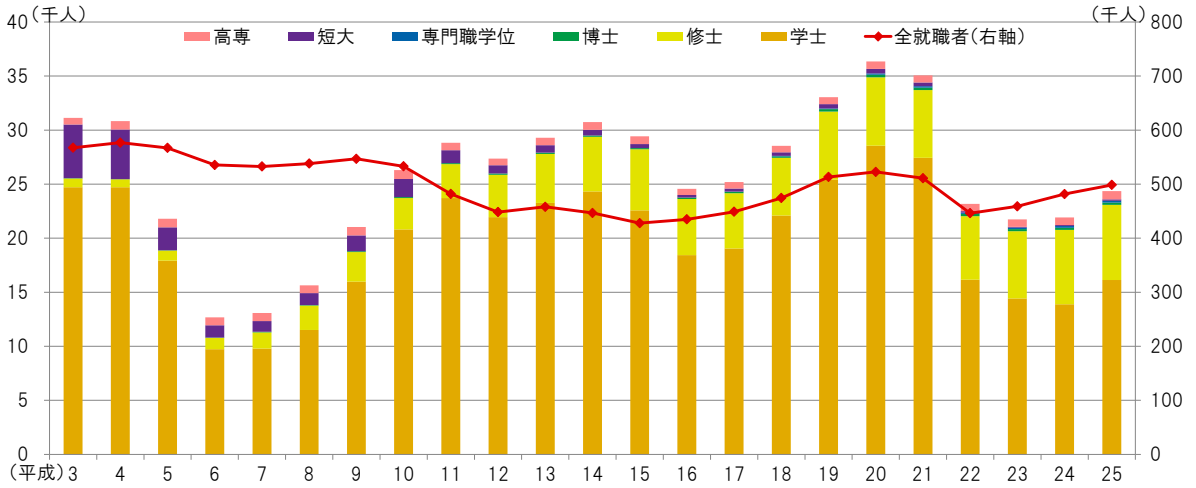
（出所）情報セキュリティ政策会議「新・情報セキュリティ人材育成プログラム」（2014 年 5 月 19 日）より大和総研作成

３－２．回復しない情報処理・通信技術者の就職者数

情報セキュリティ人材の教育・育成は日本のサイバーセキュリティ推進において喫緊の課題である。しかし、高等教育機関からの就職者数を見ると、全就職者数はいわゆるリーマン・ショック後の平成 22 年度に大きく減じたものの平成 25 年度にはリーマン・ショック前の水準に近づきつつあるのに対して、平成 25 年度の情報処理・通信技術者の就職者数は大きく落ち込んだ平成 16 年度の水準を下回っている（図表５）。情報処理・通信技術者の就職者数のうち全てが情報セキュリティ人材として登用されているわけではないため注意が必要だが、図表５の傾

向から、情報セキュリティ人材についても就職者数がそれほど伸びていない可能性が推察される。

図表５　高等教育機関卒業後の「情報処理・通信技術者」就職者数の推移



（注）平成 21 年に日本標準職業分類が一部改訂され、運輸・通信技術者の一部が情報処理技術者と統合されて情報処理・通信技術者となっている。上図は、平成 22 年度までは情報処理技術者、平成 23 年度以降は情報処理・通信技術者を用いている。なお、運輸・通信技術者は上図範囲内の最大で平成 22 年度の 2,570 人。
（出所）総務省「学校基本調査」より大和総研作成

情報セキュリティに関する人材育成では、高度な技術やノウハウといったスキル向上やそのための環境作りに目が行きがちだが、特にこれからのサイバーセキュリティを担うであろう若い技術者や学生にとっては、経済的・社会的に魅力ある職業であることも重要になる。そのためには、例えば、情報セキュリティ人材の認知度や社会的ステータスの向上、処遇を含めた雇用環境の向上などを推進することは、期待される支援となりうるであろう。

ICT の活用は、効率化だけでなく収益増大にも寄与することが期待されることから、今後も官民含めた様々な社会基盤に ICT が実装されていくと想定される。また、前述した重要社会基盤の 12 分野のうち「電力」では、今後市場環境が大きく変化する可能性がある。電力分野では電力システムに関する改革方針が 2013 年 4 月に閣議決定されており、2016 年には小売全面自由化が予定されている。新規事業者の市場参入も想定されるが、重要社会基盤事業者としてサイバーセキュリティが確保されている事が求められるだろう。

このように、サイバーセキュリティを推進すべき対象は、今後増えることはあっても減ることはないであろう。サイバーセキュリティは終わりのない取組みであり、専門従事者の育成を継続的に強化していくことが必要となる。そのためには、CS 基本法にあるように国民一人一人がサイバーセキュリティの重要性に関心と理解を深めるとともに、情報リテラシーを高め、サイバーセキュリティへの取組みや情報セキュリティ人材の必要性を認識することも求められよう。

以上