日経・CSISバーチャル・シンクタンク
CSIS-NIKKEI VIRTUAL THINKTANK

安全保障戦略としてのサイバーセキュリティー強化

―― 国民を守るために ――

2014年6月3日

土屋大洋　アカデミックアドバイザー

サイバーセキュリティー戦略タスクフォース

エグゼクティブサマリー

サイバー空間は現代社会を構成する重要な社会インフラとなっており、その安全性が悪意ある攻撃によって失われれば国民一人ひとりの生活が脅かされるだけでなく、経済の仕組みや国家の安全保障までが危機に瀕する。日本政府は現行法制のもとでサイバーセキュリティー強化に向けて可能な施策を積み上げてきたが、日本を守るとともにグローバルなサイバー空間の安全に貢献するためには、立法や法改正を含めたいっそうの取り組みが必要になる。本提言では特に国家安全保障の観点から、以下の 7 点を提言する。

1. 「内閣官房情報セキュリティセンター（NISC)」の基盤と権限を大幅に強化し、日本の情報セキュリティー戦略の司令塔としての位置づけを明確にすべきである。安全保障政策としてのサイバーセキュリティー戦略の立案・実行に関しては、国家安全保障会議（NSC）との組織的整合性や業務の切り分けを早急に検討する必要がある。
2. 2014 年 3 月に発足した自衛隊の「サイバー防衛隊」は防衛省･自衛隊の情報システム・通信ネットワークの防御をその使命とするが、サイバー攻撃への対応を迅速かつ正確にするためには、他省庁・企業との情報共有の推進や米軍との共同対処要領の策定といった「横の連携」を意識した運用を目指すべきである。同時に、これに関して国内法上の制約がある場合は、その改善に向けた議論を政府全体として進める必要がある。
3. 外国からのサイバー攻撃に対して国家はどのように反撃できるか、といった基本的な問題について明確な国際ルールはまだ確立していない。日本は国連などの場で国際的なルール作りに積極的に参加し、より安全な世界を作るための貢献をすべきである。
4. サイバー攻撃を抑止するには、不正な通信を探知･解析して予防的な措置を取ることが重要になる。基本的人権としての「通信の秘密」を保護しつつ、サイバー攻撃を未然に防ぐための方策と制度を検討すべきである。
5. 金融・輸送・エネルギー・水道・プラントなど各種の社会インフラを制御するための情報システムもサイバー攻撃の標的となりうる。とりわけ情報通信、電力、防衛産業といった、自衛隊や在日米軍の円滑なオペレーション遂行に必要なインフラを新たに一つのグループとして定義し、セキュリティー基準の厳格化や障害発生時の監督官庁などに対する報告の義務化、自衛隊や在日米軍との共同訓練の実施などについて議論を進めるべきである。
6. 政府は安全保障政策としてのサイバーセキュリティー強化と並行して、グローバルな視点からのサイバー犯罪対策にも積極的に取り組む必要がある。諸

外国は国境を越えたリアルタイムの情報交換と国際共同オペレーションを強力に展開しつつあり、日本もこうした連携強化の流れに積極的に関与・参画し、体制強化を図る必要がある。

7. 日本のサイバーセキュリティーを全体として高めるには、この分野に関する研究開発の積極的な推進と人材の育成が必要になる。政府職員に奨学金を与え、大学で専門的な学位を取らせるといったような制度を警察や防衛省･自衛隊に導入する余地がある。長期的な国益を考えた人材育成策をまとめる時にきている。

1. 問題意識

インターネットや携帯電話といった情報通信技術は、重要な社会インフラストラクチャになっている。しかし、そのセキュリティーが脅威にさらされ、国家の安全保障、国民生活や経済にまで影響するようになっている。

サイバー攻撃の事例としては、2007 年のエストニアや 2009 年の米韓に対する大規模な DDoS 攻撃、2010 年のイランの核施設の制御システムに対する STUXNET 攻撃、2011 年の日本の三菱重工業に対する標的型メール攻撃などがよく知られている。2013 年には米国のマンディアント社による中国のサイバー攻撃に関する報告書が話題となり、韓国に対する北朝鮮のサイバー攻撃も注目された。もはや日常的にサイバー攻撃は行われている。

「サイバー攻撃」が、従来の安全保障概念と照らし合わせて「攻撃」といえるかどうかは検討の余地がある。直接的な死傷者の発生や物理的な破壊につながるようなサイバー攻撃はほとんど行われていない。しかし、将来においてもそうであるとは限らない。米国のレオン・パネッタ前国防長官は繰り返し「サイバー真珠湾攻撃」の可能性を指摘した。米国をはじめとするいくつかの国ではサイバー軍が設置され、国連総会では安全保障問題としてサイバーセキュリティーが議論されるようになっている。

日米同盟という文脈でも、サイバーセキュリティーにおける協力の拡大が求められている。日米サイバー対話が東京とワシントン DC で開催され、両国政府の関係機関が一同に揃って問題意識の共有を行った。東アジアはサイバー攻撃の頻発地の一つであり、その影響はグローバルに及んでいる。

日本政府は 2013 年 6 月に新たなサイバーセキュリティー戦略を発表した。2005 年に内閣官房情報セキュリティセンター（NISC）と情報セキュリティ政策会議が設置されて以来、日本政府は現行法制下で可能な施策を積み上げてきた。しかし、日本を守るとともに、グローバルなサイバー空間の安全に貢献するためには、立法や法改正を含めたいっそうの取り組みが必要になっている。本提言書はその中でも特に必要とされている項目について取り上げた。

立法や法改正にあたっては憲法の精神を尊重し、特に国民のプライバシーに配慮しながらも、新たな脅威とリスクに対処するのに必要な場合には柔軟な対応がとれるようにすべきである。技術は日進月歩であり、硬直的な対応では国民の生命・財産を守ることはできない。社会が情報通信技術に依存すればする

ほど、それにつけ込んだサイバー攻撃は社会的に大きな被害をもたらすことになる。安全保障と各種の人権の間でバランスをとりながら、新たな脅威に対応する施策を検討する必要がある。

2. 体制整備

日本のサイバーセキュリティーないし情報セキュリティー政策の司令塔になるべき機関は内閣官房情報セキュリティセンター(NISC)である。しかし、NISCは内閣総理大臣決定だけに依拠する組織であり、その基盤は弱い。専従の職員はおらず、各省と民間企業からの出向者で成り立っている。職員は 2 年程度のローテーションで異動する。

また、NISC はインテリジェンス機関ではない。2013 年末に特定秘密保護法は成立したものの、セキュリティー・クリアランスの導入は必ずしも徹底されていないため、諸外国との窓口としての機能を十分に果たすことができずにいる。2013 年 6 月に決定された政府の新しいサイバーセキュリティー戦略でも NISC の組織強化および将来的な組織変更が打ち出されたが、内閣官房の中で NISC をどう位置づけるかを考えなくてはならない。特に、既存の体制においては、大規模サイバー事態が発生し、官邸に対策本部が立ち上がる場合、事案対処に係る調整は NISC ではなく当該対策本部が担うこととなるが、サイバー攻撃への対処を日常的に行っている NISC がより主体的な役割を果たす必要がある。

昨年設置された日本版国家安全保障会議（NSC）は、政府の安全保障政策全体の司令塔となり、現在の議論では、サイバーセキュリティーについても所管している。したがって、サイバーセキュリティー政策の司令塔である NISC との組織的整合性や業務の切り分けを早急に検討する必要があるだろう。

NISC の課題の一つは調査権限の欠如である。サイバーセキュリティーの司令塔としての役割を期待されながら、自ら能動的に調査することはできず、情報は関係省庁（総務省、経済産業省、防衛省、外務省、警察庁等）からの自主的な提供に頼らざるを得ない。そこで、NISC の下に国家行政組織法第 3 条に基づく委員会、いわゆる「3 条委員会」を設置し、サイバーセキュリティー関連の事案があった場合には、事後的にではあっても、主体的に調査できるようにすべ

きである。3 条委員会の例としては、国土交通省下の運輸安全委員会が知られている。同委員会は、交通・運輸関連の重大インシデントの原因究明調査を行っており、例えば、航空機に関わる重大事故が起きた場合に主体的に情報収集と分析を行う。これと同様に、サイバーセキュリティー関連の重大インシデントの原因究明調査を行える 3 条委員会を設置すべきである。安全保障全般を扱う NSC とサイバーセキュリティーに特化した NISC との間でスムーズに情報共有・意思疎通・決定伝達が行われなければならない。

3. 防衛省・自衛隊による取組み

防衛省・自衛隊において、2014 年 3 月にサイバー防衛隊が発足した。これは、自衛隊として初となるサイバー攻撃対処を専門に行う部隊であり、日常的なサイバー攻撃に関する情報収集・分析や自己のネットワークの常続的な監視、事案発生時における防護等の対応など、防衛省・自衛隊全体のサイバー攻撃対処に関する役割を担っている。サイバー防衛隊の任務については、今後実際の運用を進める中で具体化されていくことになると思われるが、2013 年 12 月に閣議決定された「中期防衛力整備計画（平成 26 年度～平成 30 年度）」において、「相手方によるサイバー空間の利用を妨げる能力の保有の可能性」、すなわち反撃能力保有の可能性について記述があることから、今後、同部隊に対して反撃能力を与えることに関する議論が進むことが考えられる。技術的な実行可能性についてはさておき、法的な面からいえば、現在、国際法上はサイバー犯罪条約、国内法上は刑法や不正アクセス禁止法などによりこうした手段の保有や実施について大きな制限があるのが現状であり、国際社会や国内関係機関と並行して議論を進めていく必要がある。

また、上述の中期防や、同時に策定された「国家安全保障戦略」、「平成 26 年度以降に係る防衛計画の大綱」で、関係機関との連携強化や役割分担の明確化が求められている。この関係機関との連携の中でも、特に情報共有体制について、安全保障に対し重大な影響を及ぼし得るサイバー攻撃事案が発生した場合は、何より防衛省・自衛隊や警察庁といった事案対処省庁が迅速かつ正確な情報を入手することが最重要であることから、現在のような NISC による一元的な情報提供の枠組に加え、防衛省と他省庁、防衛省と企業といった、情報共有

ラインの複線化を図ることで、スピードと正確性の両面を担保していくべきである。

さらに、防衛省・自衛隊は、2014 年 2 月に第 1 回会合を行った日米サイバー防衛政策ワーキンググループ等の枠組みで、サイバーセキュリティーに関する日米防衛協力強化の検討を鋭意進めているところであるが、人材育成における協力などに加え、サイバー攻撃に対する抑止力の強化が重要な課題でありことから、米軍によるサイバー策源地攻撃の担保など、サイバー攻撃への反撃に関する米軍との機能・役割分担について早急に議論を進めるべきである。加えて、サイバー攻撃への適切な対応は全世界共通の課題であることを踏まえれば、英国やオーストラリアといったいわゆる関係各国に加え、他国に対するサイバー攻撃を行うだけでなく他国からのサイバー攻撃の被害にも頭を悩ませている中国やロシアといった国々との間でも、ホットラインの構築など、防衛当局同士の信頼醸成を進める可能性を追求すべきである。

4. 国際規範の構築と国際協力

北大西洋条約機構（NATO）の協調的サイバー防衛研究拠点（CCD COE）がまとめた「タリン・マニュアル」では、95 個のルールのうち、第 1 のルールとして、サイバー空間における国家主権の問題が指摘されている。将来のサイバー戦争において国家はどのような位置づけになり、どのような対応がとれるのか、国際的な規範はどうあるべきかが、国連総会第一委員会の政府専門家会合（GGE）や 2013 年 10 月の韓国でのサイバー空間会議でも検討されてきた。日本が国際規範の構築にどう貢献し、国際協力を進めていくのかを検討すべきである。

国連 GGE の報告書は 2013 年 9 月の国連総会後に公表されたが、そこでは国連憲章等の既存の国際法が適用可能であること、また、いかなる規範が国家の行為等に対して適用されるかという共通の認識にはいっそうの検討が必要であることなどの記述があった。したがって、この国連 GGE 報告書により、国連憲章第 51 条により禁じられている「武力攻撃」に該当するサイバー攻撃が発生した場合は、自衛権の行使が可能であることについて国際的な合意があったと解釈できるが、「武力攻撃」に該当するサイバー攻撃とは何か、どのような形態の

個別的・集団的自衛権の行使が可能か、「武力攻撃」に該当しないサイバー攻撃に対して国際法上合法的に反撃できるのか、といった点についての国際的な合意は得られていない。特に日本は、日米同盟の下でサイバーセキュリティーにおける防衛協力を進めていく中で、この問題にどう取り組むかを考えて行く必要がある。

国際協力という点では、JPCERT コーディネーションセンター（JPCERT/CC）はすでに東南アジアにおいて CERT 構築支援や人材育成支援を展開している。CERT や CSIRT の取り組みは、信頼醸成措置の一環としても注目を集めている。JPCERT/CC は、資金的に経済産業省の支援を受けながらも、一般社団法人として政府からは独立した組織である。しかし、中国の CNCERT/CC 等は、政府の一部門として機能している。こうした形態の違いはあるにせよ、政府間では協議しにくい問題でも CERT・CSIRT 間では電話や電子メールで日常的に議論され、技術的な問題の解決が行われている。こうしたチャンネルの有効活用と支援の拡充が必要である。

5. 探知・解析能力の向上と通信の秘密

日本国憲法第 21 条と電気通信事業法第 4 条は、通信の秘密を保障しており、戦後の日本はこの規定を厳しく守ってきた。1999 年に成立した「犯罪捜査のための通信傍受に関する法律」は犯罪を立証するための通信傍受（いわゆる「司法傍受」）を認めたものだが、犯罪の未然防止のための通信傍受（いわゆる「行政傍受」）は認められていない。そのため、日本国内では不正な通信が通信網に流れていても、利用者と事業者の間に事前の合意・契約等がなければ、それを探知・解析することは認められず、その結果として阻害・停止させることもできない。

電気通信事業法第 4 条には第 1 項と第 2 項があり、第 1 項がいわゆる「通信の秘密」の保護を規定しており、第 2 項は「他人の秘密」と呼ばれる条項である。他人の秘密とは、郵便の例でいえば、封書の中身と宛名書き等として容易に分けて考えられる。封書の中身は郵便事業者とても読むことは許されていないが、宛名書きは郵便事業者が読まなければそもそも届けることができないため、それを読むことが認められていたが、しかし、他人に漏らすことは認めら

れていなかった。例えば、ある人のところに大量の郵便物が来ているとか、特定の人から毎日のように郵便が来ているということは秘密とされていた。

一般的に、電話においては、通信の秘密と他人の秘密を分けず、一体不可分のものとして扱われてきた。しかし、インターネットの時代になって、それらを分けて考えることができるようになっている。

米国の中央情報局（CIA）の元職員であり、国家安全保障局（NSA）の契約職員だったエドワード・スノーデンが暴露したところによれば、NSA は、通信の秘密にあたる部分にアクセスしながらも、むしろ、他人の秘密であるヘッダー情報を集積したメタデータを活用しているとことが分かってきている。

NSA や英国の政府通信本部（GCHQ）など、諸外国のインテリジェンス機関はサイバーセキュリティー対策として通信傍受を活用している。日本は国際通信の 95%以上を海底ケーブルに依存している。例えば、海底ケーブルを通じて外国から入ってくる通信のヘッダー部分だけでも見ることができれば、ある程度の探知・解析ができるものと考えられる。

無論、ヘッダー情報だけだとしても、それはプライバシーの侵害になる恐れは十分ある。人権としての通信の秘密とのバランスをとりながら、治安・安全保障目的の通信のモニタリングを可能にする方策と制度を検討すべきである。

そのためには、政府の中でどのような権限を持った人が通信にアクセスできるのか、そして、モニターされた通信の内容が第三者に漏れないように、あるいは政治目的で使われないように監視する制度も同時に作らなくてはならない。行政府の行き過ぎを監視する立法府と司法府の役割が欠かせない。特に立法府である国会は、情報委員会を設置し、さまざまな分野における行政府の行き過ぎを監視する体制を整えるべきである。有効な対策の実施と、その行き過ぎを是正するための監査制度を同時に拡充していくべきである。

6. 制御システムと重要インフラストラクチャ防護

イランに対するスタックスネットの攻撃に代表されるように、インターネットにつながっていないシステムでもサイバー攻撃の対象になり得る。そもそも多くの重要インフラストラクチャの制御システムは意外な形でネットワークにつながっていることがある。これまで NISC が行動計画の対象としていた情報

通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流といった 10 分野に加えて、2014 年 3 月の「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」においてクレジット、化学、石油の 3 分野が新たにその対象となったところであるが、今後、港湾なども含めた幅広いインフラストラクチャの制御システムとそのセキュリティーについて検討すべきである。

メールの送受信、文書作成など一般の事務を行うシステムとしての情報系システムに対するサイバー攻撃はすでに広く行われるとともに、認識もされている。いわゆる標的型電子メール攻撃は情報系システムに対して行われている。ところが、インフラストラクチャに基づくサービスを提供するための機器・システムなどを管理・制御するシステムを制御系システムは、一般にはそれほど注目されていない。

制御システムは、従来、インターネットにつながっていないから安全とされてきたが、深夜に遠隔地からリモート操作でメンテナンスできるようにするためなど、いくつかの理由で実際にはインターネットにつながっていることが多い。いったん制御系システムの中にウイルスやワームが入り込むと、特定の標的を探索し、不具合を起こさせることが可能になる。

その不具合も多様である。シャットダウンさせたり暴走させたりする場合もあるだろうが、ほんのわずかな誤作動を長期的に引き起こすことで、工場の歩留まり率を原因不明の形で下げさせ続けるといったことも可能である。むしろ、攻撃されていることが分からない形で攻撃を続けられることが、攻撃者にとっては望ましいこともある。あるいは、長期に侵入させておき、いざというときに破壊・暴走させることもあり得る。

制御系システムの開発業者はそれほど多くないため、システムの多様性も大きくない。いったん一つの制御系システムが攻略されれば、同じ会社が納品するシステムに広く被害が及ぶ可能性も高い。この問題は制御系システムの開発業者および利用者の双方に対策を求める必要がある。

特に今後考えるべきは、すでに作られた制御系システムの脆弱性探しだけではなく、そもそも脆弱性の低い、攻撃されにくいシステムの開発であり、そのための研究を政府が主導すべきである。すでに経済産業省の取り組みとして宮城県多賀城市に制御システムセキュリティセンター（CSSC）が設置され、2013 年 5 月から運用が始まっている。CSSC には世界でも屈指の設備が作られてい

るが、予算が不足気味であり、取り扱っている分野も経済産業省関連のものに限られている。また、国土交通省が管轄する交通システムは取り扱われていない。国全体で制御系システムを守る取り組みを始めるべきである。

なお、これまで NISC が防護の対象としている「重要インフラ分野」は、その情報システムの障害が国民生活及び社会経済活動に多大な影響を及ぼすおそれのあるインフラ分野である。他方、大規模サイバー攻撃事態に際しては、弾道ミサイル攻撃等の物理的な脅威も同時に発生することが考えられるため、国民の生活等への影響を最小限にすると同時に、自衛隊や在日米軍による日本防衛に係るオペレーションへの影響も極小化する必要がある。したがって、これまでの国民生活及び社会経済活動に多大な影響を及ぼす重要インフラストラクチャという枠組みに加え、新たに安全保障上重大な影響のある重要インフラストラクチャという枠組みを設け、情報通信、電力、防衛産業といった、自衛隊や在日米軍の円滑なオペレーション遂行に必要不可欠なインフラストラクチャについて、セキュリティー基準の厳格化や、障害発生時の監督官庁等に対する報告の義務化、自衛隊や在日米軍との共同訓練の実施等について議論を行っていく必要がある。

7. サイバー犯罪対策の拡充

サイバー空間は、社会経済活動を支えるインフラとして、そして国民生活の日常に不可欠なサービスを展開するものとして欠かせない存在となっている。サイバー空間の安全と安心は、社会経済活動を活性化するだけでなく、国民生活を守るという点においても第一に考えなければならない課題である。安全保障と犯罪対策は一線を画するものであるが、密接な領域でもあるため、ここで触れておく。

社会経済活動や国民生活がサイバー空間に依存するようになると、犯罪を企図する者にとってもサイバー空間はターゲットとしての魅力を増し、サイバー空間の安全・安心に対する脅威は深刻化している。サイバー空間は、物理的・時間的な制約を受けず低コストでの情報やサービスの提供を可能として新たなビジネスモデルを出現させたが、その一方で、金銭的な利益は犯罪者らを惹きつけ、組織化・グローバル化させる結果となった。政府は外国やテロリスト集

団からの攻撃に対処する安全保障政策としてのサイバーセキュリティーを充実・強化するのに加え、グローバルな視点からのサイバー犯罪対策にも積極的に取り組む必要がある。

ウイルスを作成するグループ、ボットネットを展開・運用するグループ、ハッキングツールを作成するグループ等、犯罪者らはターゲットに応じて必要なツールや情報を集めて犯行に及ぶ。 犯行によって得られた収益は関係者に分配され、犯罪者を利するウイルスやツールの開発に充てられて手口はさらに高度化・巧妙化する。犯罪者らは、どこに拠点を置いていてもアンダーグラウンドなチャンネルを通じて連絡を取ることができ、グループ間の緩やかな繋がりによって犯罪インフラが構成される。

数年前から欧米で大規模な被害を発生し続けているオンラインバンキングにおける不正アクセス・不正送金事案では、銀行側のセキュリティー対策を回避するあらゆる技術が駆使されている。その被害は莫大であり、犯罪組織に巨額の収益をもたらしているといわれる。これらオンラインバンキングに対する不正アクセスは日本にも波及しており、警察庁がまとめた統計によれば、2013（平成 25）年中、14 億円を超える被害を発生し、過去最悪となっている。問題の本質は、偶然に日本の銀行に被害が発生したのではなく、日本の銀行のオンラインバンキングの仕組みを事前に研究し、そのセキュリティーを回避するように作成された、すなわち日本用にカスタマイズされた手口が用いられた点である。我々は、犯罪者にとって日本が魅力的なターゲットに映っているということを理解する必要がある。

法執行機関の取組みは、こうした現状に必ずしも十分に対応できるものとはなっていない。国境の壁、技術の壁、そして匿名化の壁は、犯罪者にとって摘発されるリスクを低減する好材料であり、サイバー空間は法執行機関よりもサイバー犯罪者に有利な、非対称の空間となっている。

2013 年 1 月、EU では、ユーロポールにサイバー犯罪対策を専門とするヨーロッパサイバー犯罪対策センター（EC3: European Cyber Crime Center）を設置した。2014 年秋には、インターポールがサイバー犯罪捜査の国際的な調整を図るための組織として、デジタル犯罪センター（IDCC: INTERPOL Digital Crime Center）を立ち上げる予定である。サイバー空間を取り巻く脅威に対して、諸外国では国境を越えたリアルタイムの情報交換と国際共同オペレーションを強力に展開しつつある。サイバー犯罪のターゲットとなっている日本にあ

って、こうした国際的な法執行機関間の連携強化の潮流に乗り遅れることはできない。積極的に関与、参画し、態勢強化を図る必要がある。

これら国際的な連携強化の一環として、諸外国の法執行機関ではカウンターパートとなる国にリエゾンを派遣し、リアルタイムの情報共有と共同オペレーションを可能とする体制を整備している。日本も、早期に協働できる体制として、リエゾン等の人的なつながりを確保する取組をスタートすべきである。

国際的な枠組みで交換されるさまざまな情報は、サイバー犯罪者の検挙だけでなく、被害の未然防止の観点からも極めて有用である。犯罪捜査の視点から情報の管理は徹底されるべきであるが、日本を守るという観点において、従来の内閣官房を中心とした政府及び民間企業における情報収集に加えて、法執行機関が有する情報のいっそうの活用のための方策を模索するべきである。このような情報の一元化と多層的な分析体制の確保、そして犯罪インフラの根絶に向けた法執行機関による国際的なオペレーションへの参画こそ、日本のサイバーセキュリティー戦略を支える基盤となり得る。

8. 研究開発と人材育成

諸外国でのサイバーセキュリティー向けの研究開発費は増大中だが、日本では減少中である。大学の教育課程においても、コンピュータ・サイエンスの人気は下がり気味である。この分野にどのように研究開発費を振り向け、どのような人材を育てるかを検討する必要がある。いわゆる「ホワイトハットハッカー」育成に必要な措置としてどのようなものがあるか、そして、そうした人材が政府や企業の中でどのようなキャリアパスを描けるかも検討すべきである。

若者がサイバーセキュリティーを学ぼうとしないのは、それを学んでも、有望な職に就けないからであり、就けたとしても収入や出世が期待できないからである。しかし、サイバーセキュリティーは一種の専門職であり、ローテーション人事で務まるものではない。一種の天賦の才が求められる分野でもある。セキュリティーに係る仕事は、安全であって当たり前であり、何かインシデントが起きれば責任を問われてしまうという意味で、常に損な役割を担わされる。

さらには、どれだけ投資すれば 100%安全になるのか分からないという問題もある。近年のサイバー攻撃の事例を見れば、いったん狙われてしまえばいつ

か攻略されてしまうと見るほうが正しいだろう。しかし、全くの無防備では攻撃のコストを下げることになる。できるだけ狙われにくく、仮にセキュリティーが破られても被害を最小化するための取り組みは、専門的な見地から実行されなければならない。

米国や韓国では、政府職員に奨学金を付けて大学の学部や大学院で専門的な学位を取らせ、復職後は一定期間の勤務を求める制度がある。一定期間経過後は、そうした人材は高給を求めて民間に転出することが多いが、それは民間部門のセキュリティー向上にもつながり、政府部門には人材が滞留せずに、新しい知見・技能を持った人材が入ってくるという良いサイクルが生まれている。

もちろん、こうした制度を可能にするには予算が必要であり、人材のバックグランド調査もしっかり行われる必要があるだろう。しかし、長期的には政府部門と民間部門の両方のレベル向上につながり、国全体のサイバーセキュリティーの向上につながるとすれば、こうした制度を、日本の警察や防衛省・自衛隊、情報機関などにも導入する余地はある。特に、警察庁によるサイバー攻撃特別捜査隊の設置、防衛省・自衛隊によるサイバー防衛隊の設置といった、政府全体でサイバー関連組織が新たに生まれている現状では、そうしたニーズは高い。長期的かつ広い意味での国益を考えた人材育成策をまとめるべきである。

自国で人材を育成できなければ、外国にサイバーセキュリティーを依存せざるを得なくなる。しかし、報酬体系が国家公務員法に依拠することになれば、民間市場で多額の報酬を得られる人材が政府で働くインセンティブは少ない。安全保障のために自らの能力を用いることを誇りとする人材が求められている。