SFC研究所日本研究プラットフォーム・ラボ

ワーキングペーパーシリーズ　No. 8

防衛省とサイバーセキュリティ

―日本のサイバーセキュリティに関する進展と落とし穴―

ポール・カレンダー*

2013年12月

「新しい『日本研究』の理論と実践」

SFC研究所日本研究プラットフォーム・ラボ

本稿は、2010～2013年度に実施した文部科学省私立大学戦略的研究基盤形成支援事業「新しい『日本研究』の理論と実践」による研究成果である。

The MoD and Cybersecurity:

Progress and Pitfalls with Japan's Cybersecurity

Paul KALLENDER

Keio University Graduate School of Media and Governance

* 慶應義塾大学大学院政策・メディア研究科後期博士課程在学中（kallen@sfc.keio.ac.jp）

防衛省とサイバーセキュリティ

―日本のサイバーセキュリティに関する進展と落とし穴―

ポール・カレンダー

概要：

過去 3 年間、日本は、サイバーセキュリティに関する対策と政策を大幅に前進させた。これと合わせて、日本の防衛省はサイバー防衛方針を発表している。また、サイバーセキュリティ問題に対応するため、サイバー防衛隊も設置することにした。しかし、深刻な問題は依然として存在している。まず、サイバーセキュリティに対応するための人員と資金が不足している。また、防衛省が日本の重要インフラを保護するために専門的技術を使用するにあたっての行政的および法的制限がある。本論文では、サイバー防衛を改善するために、日本のさまざまな組織や政府機関が行った最近の進展をまとめ、次に、防衛省のサイバーセキュリティ政策の進展と落とし穴について述べる。そして、海外の政策と軍との簡単な比較をし、サイバー攻撃を阻止し、国を守る能力を向上させるには、防衛省の現在の政策をさらに強化することが必要であると結論付ける。

キーワード：

サイバーセキュリティ、日本、防衛省、自衛隊

1. サイバー攻撃とサイバー戦争に関する問題

過去 20 年にわたる情報技術（IT）革命の後、情報通信網によるデジタル経済は、グローバル経済の重要インフラとなった。しかし、研究者たちは 20 年前に、IT 革命によってセキュリティが必要になること、そして、紛争に関してサイバースペースを媒体として認識する必要が増すことに気付いていた[1]。サイバースペースの安定性と安全性を維持することが、政策立案者にとって重要な課題となった。また、軍事作戦において、サイバースペースでの作戦能力が極めて重要になった。このため、サイバーセキュリティは国家安全保障に関する最も重要な問題に数えられるようになっている[2]。これはまた、さまざまな国がサイバー攻撃能力を開発する原因ともなっている。電気、ガス、金融、通信など、重要インフラに対するサイバー攻撃は、社会と経済の機能に大幅な打撃を与える可能性がある。また、指揮命令系統が IT に強く依存している脆弱な軍も、攻撃を受けやすくなるだろう。「第一次サイバー戦争」が 2007 年のエストニアと 2008 年のグルジアで勃発して以来、軍のサイバー政策は、広範囲な民間および軍事 IT インフラに対するサイバー攻撃を抑止する目的で発展してきた。近年、サイバーセキュリティは防衛政策の 5 つの作戦領域の一つとなった。このグローバル経済と通信インフラにおけるサイバーセキュリティの役割は、それが国家安全保障において最も重要な問題の一つとなったことを意味している[3]。

2. サイバー攻撃とは何か？

2.1. 高度化し、複雑化するサイバー攻撃

インターネット関連技術は常に進化している。それに伴いサイバー攻撃も増加し、より高度で複雑になってきている。インターネットは TCP/IP プロトコルを基本として構築されており、セキュリティでなく利便性を目的として設計されている。このため、攻撃を阻止する対策を講じたとしても、比較的悪用されやすい。サイバー攻撃は悪意のあるコードを

[1] John Arquilla, David Ronfeldt, “Cyberwar is Coming!” *Comparative Strategy*, Vol. 12, No. 2 (Spring 1993), pp. 141–65.
[2] “Remarks by the President on Securing Our Nation’s Cyber Infrastructure,” 29 May 2009 <http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/>.
[3] 橋本靖明「サイバー・セキュリティの現状と日本の対応」『国際安全保障』第 41 巻第 1 号、27～44 頁。

使用し、技術に依存している企業やネットワークを意図的に攻撃する。ウェブサイト改ざん、サービス拒否（DoS)、分散サービス拒否（DDoS）を行い、個人情報窃盗、詐欺、恐喝、ファーミング（pharming）攻撃、フィッシング（phishing）詐欺、スパミング、なりすまし、スパイウェア拡散などを行う。恐らく最も深刻なコンピュータ・ネットワーク攻撃の形態として増加しているのは、APT（Advanced Persistent Threats）攻撃であろう。これにはデータ偽造や、ネットワークや通信機能を破壊・損傷をするために使用されるような「バックドア」や論理爆弾などのいくつかの手法が関連している。サイバー攻撃には多数の者が関与している。多くの場合は匿名であるため、検出するのが難しく、攻撃者が優位な立場にある（この状態は「攻撃者の優位性」とも呼ばれている)。攻撃者は個人のハッカーから、組織的なゲリラハッキンググループ、国が資金供与している部隊まで、さまざまである。攻撃者は隠れ、身分を偽ることができるので、技術的にも、また政策の点からも、攻撃者を検出して阻止することは難しい。リチャード・A・クラークはサイバー戦争を「国家が他国のコンピュータまたはネットワークに、破壊または妨害目的で侵入する行為」として定義した[4]。これに対して、米国国家情報長官のジェームス・クラッパーは、サイバー戦争をサイバースパイ活動とサイバー攻撃に分類した。限られた軍事目的と広範囲にわたる重要インフラ目的の両面において、兵器輸送機の技術データを盗むスパイ活動から、現実、仮想、または潜在的な敵の弱点を利用することまで、目的はさまざまである。

2.2. 増大する APT の脅威

サイバー脅威の本質は、APT の増加により、組織間の軍備拡張競争へと変化した。APT に関与する組織は、目標を執拗に効果的に搾取しようとする意図を持ち、その能力も持つ。2012 年 2 月、米国に拠点を置くサイバーセキュリティコンサルタント会社のマンディアント社は、大規模サイバー攻撃の増大に中国人民解放軍の第 61398 部隊が組織的に関与していることを発表し、この部隊を「APT1」と名付けた[5]。APT1 は IT、宇宙、航空、交通、建設、製造業界の非常に戦略的な組織を中心に、少なくとも 20 の業界、141 組織に侵入した。マンディアント社の調査結果によると、中国の APT1 部隊は、特定のターゲットから 10 か月にわたり 6.5TB ものデータを盗んでいた。

---

[4] Richard A Clarke, Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It,* Harper Collins, 2010, pp.179-228.
[5] "APT1: Exposing One of China's Cyber Espionage Units," February 18, 2013, Mandiant Corporation <http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf>.

さらに最近では、組織的な専門ハッカーグループによるゲリラ APT が、APT の主流となっている[6]。このようなグループは、高い価値があるターゲットに素早くアクセスし、「ヒット&ラン」スタイルでネットワークから抜ける。4,000 以上の IP アドレスのデータを汚染し、韓国、日本（2011 年の国会、2013 年のフジテレビへの攻撃）、米国、オーストラリア、カナダ、英国、イタリア、ドイツ、オーストリア、シンガポール、ベラルーシ、マレーシアの数百の犠牲者をターゲットとした。これは APT の活動の「氷山の一角」である。

このような問題に対する米国での認識は、重大な転機に達した。最近の米国議会の報告書では、大規模なサイバースパイ活動とサイバー戦争の脅威の両方について中国を名指しした[7]。米国は自国の防衛と通信のサプライチェーンの保全性に疑いを持っている。米国は中国が将来、複数の国々で、混乱を生じさせる「全面攻撃（空、海、陸、宇宙、サイバースペースの 5 つの領域における）」の一環として、重要インフラや軍部の IT システムを目標にしているのではないかと疑っている。米国は、中国のファーウェイ（Huawei）社と中興通訊（ZTE）社との取引を米国企業と政府が避けるべきとの結論を出した。この 2 社は、中国製の電気通信部品やシステムに「キルスイッチ（電源などを遮断して停止させる装置）」を組み込んでおり、重大局面や戦時下において、中国政府が重大な国家安全保障システムを停止したり、妨害したりできるように設計されているため、米国の国家安全保障に対する脅威となると疑われている。

さらに、最近のイランのスタックスネットの例では、戦争でサイバースパイ活動や破壊活動が既に実施されていることがわかった。その結果、多くの国家や軍が、軍事政策として、物理的攻撃とサイバー攻撃を統合している、またはこれから統合しようとしている。これにより政府と民間セクターの両方を統合した総合的な対応が必要となる。

2.3. 日本に対する攻撃

世界第 3 位の名目 GDP、第 4 位の購買力平価を持つ日本にとって、サイバーセキュリティが重要であることは明らかである。最近日本では、APT 攻撃が急増している。日本最大の防衛関連請負業者である三菱重工業は、2011 年 8 月、日本全国 11 か所のシステムからウイルスを検出した。これは従業員がマルウェアを含んだ電子メールをうっかり開いた時

[6] Motohiro Tsuchiya, "Patriotic Geeks Wanted to Counter a Cyber Militia," *AJISS-Commentary*, 17 February 2012 <http://www2.jiia.or.jp/en_commentary/201202/17-1.html>.
[7] "2011 Report to Congress of the U.S. China Economic and Security Review Commission, One Hundred Twelfth Congress, First Session, November 2011," pp. 215-6 <http://www.uscc.gov/content/2011-annual-report-congress>.

に感染したもので、ウイルスの数は少なくとも 8 種類あり、サーバー45 台と PC38 台が被害を受けた。また IHI、川崎重工業も同様の攻撃を受けた。日本の宇宙開発組織の中核である宇宙航空研究開発機構（JAXA）も APT のターゲットとなったことを公に認めた。

経済産業省は、重要インフラ防護を担当する省庁の 1 つだが、2010 年 9 月以降、特に日本に向けられた高度な APT 攻撃が 6 倍に増加したとしている。これら APT のほぼ 37%が日本のインフラ、特に発電所や製造業で使用される制御システムをターゲットとしている。経済産業省がサイバーセキュリティシステムの防御が比較的脆弱であると報告したように、これは特に問題となっている。日本に対する攻撃は、APT が日本の機関や組織を標的としていることを示している。

三菱重工業に対する APT 攻撃に対して、防衛省の対応は教訓的であった。防衛省はマスメディアを通じて三菱重工業の事件を知った。このニュースにより防衛省は、早急にサプライヤー契約を改訂せざるを得なくなった。内容はセキュリティをあまり厳格にするのではなく、基本的なセキュリティ対策を実施するというものである。また、防衛省は主要サプライヤーにセキュリティ侵害に関して即刻連絡をするように命じた。2011 年 10 月、政府の情報セキュリティ政策会議の「官民連携の強化のための分科会」は、政府内の情報の分断を避けるため、政府全体で、CSIRT（Computer Security Incident Response Team、コンピュータセキュリティ問題対策チーム）を設立するよう提言した[8]。

これと共に、防衛省の対策は、我々に重要な疑問を抱かせた。なぜ三菱重工業は防衛省に問題を報告しなかったのだろうか。なぜ防衛省は政府に CSIRT 体制の改革と、各省庁および機関の間の協力を求めたのだろうか。APT に対する日本の制度上の準備はどうなっているのだろうか。実際、防衛省の対応は、2011 年の日本がいかに、それぞれ異なる政府組織のすべてを統制し、中央管理をし、効果的な対応で防衛を強化する確固としたリーダーシップが必要であったかということを示している。2014 年を目前に控え、サイバーセキュリティ規定の向上という点に関して、日本は大幅な進歩を遂げた。しかし、2011 年から 2 年経過したいまでも、防衛省の防衛省と日本の重要インフラを防護する能力は制限されている。このことについて以下で述べることにする。

[8] 情報セキュリティ対策推進会議官民連携の強化のための分科会「情報セキュリティ対策に関する官民連携の在り方について」平成 24 年 1 月 19 日<http://www.nisc.go.jp/conference/seisaku/dai28/pdf/28shiryou1-1.pdf>。

3. 日本の対応：基本構造と政策

3.1. 日本のサイバーセキュリティ体制

基礎的な日本の IT 政策は、高度情報通信ネットワーク社会形成基本法（IT 基本法）、2000 年 2 月に設置された内閣官房情報セキュリティ対策推進室、2001 年に初めて掲げられた e-Japan 構想を土台としている。IT 基本法第 22 条は、高度情報と電気通信ネットワークのセキュリティと信頼性の保証と、個人情報保護について規定している[9]。2005 年までの政策は、IT を効率化のためのツールとして推進することを重点にしてきた。2004 年 12 月に高度情報通信ネットワーク社会推進戦略本部により発行された「情報セキュリティ問題に取り組む政府の役割・機能の見直しに向けて」を受けて、日本の情報セキュリティ政策を指揮するために、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それぞれ 2005 年 4 月と 5 月に設立された。

内閣官房の高度情報通信ネットワーク社会推進戦略本部の下に設置された情報セキュリティ政策会議が、日本のサイバーセキュリティの基礎戦略を決定する。そして NISC は事務局として、戦略ロードマップを作成し、サイバーセキュリティに関する政府全体の枠組みと対応を整備し、重要インフラ防護を実施し、日本の情報戦略を策定する。また警察庁は、犯罪とみなされるサイバー攻撃を起訴する。防衛省下にある自衛隊が国家安全保障への脅威の対応を担当する。攻撃を事前に対処する方法に関するインテリジェンス活動は警察庁、防衛省などが担当しているが、NISC 自体は行っていない[10]。NISC の下、2009 年から 2010 年の改革を踏まえ、日本の重要インフラ防護は、警察庁、総務省、経済産業省、防衛省の 4 つの異なる組織が担当することとなった（後に外務省も加わっている）。それぞれが別途予算を管理しており、民間企業、種々雑多な協力団体、政策に対して、独自のアプローチと繋がりがある。

日本のサイバーセキュリティ政策は、脅威に対する認識の変化、米国からの外交圧力、日本の政治システムの安定化を受けて、より深くセキュリティに焦点をあてるように 2010 年から改正されてきた。2009 年 7 月の韓国と米国に対する一連の広範囲な攻撃により、日本のサーバー利用に関して、サイバーセキュリティ規定の有効性を再考せざるを得なくな

---

[9] 首相官邸「高度情報通信ネットワーク社会形成基本法」
<http://www.kantei.go.jp/foreign/it/it_basiclaw/it_basiclaw.html>。

[10] Motohiro Tsuchiya, “Cybersecurity in East Asia: Japan and the 2009 Attacks on South Korea and the United States,” Chapter in *Cybersecurity, Public Threats and Responses,* ed. Kim Andreasson, CRC Press, 2012, p. 61.

った。2009 年の選挙で選出された民主党の「スクラップ・アンド・ビルド」アプローチにより、情報セキュリティ政策会議は 2009 年 2 月に発表した「第 2 次情報セキュリティ基本計画」を廃止し、代わりに 2010 年 5 月の「国民を守る情報セキュリティ戦略」で始まる 3 か年計画の新しい枠組みに変更した。新戦略では、国の重要インフラへの大規模なサイバー攻撃に対する準備と対応の重要性を初めて認めている。

情報セキュリティ政策会議が事業仕分けの一環として民主党に廃止を命じられることを恐れて数か月間会議を中止している間に、NISC はサイバーセキュリティを促進する勢いを失った。しかし、2011 年に明らかになった APT 攻撃、米国からの圧力、日本のサイバーセキュリティ政策を国際標準に適合させる必要性の増加、そして 2012 年に選出されたより安定した自民党政権により、新たな変化がおきた。

こうした状況下において、NISC は日本のサイバーセキュリティを向上させるために尽力した。NISC は「情報セキュリティ」に関する年次計画を 2010 年、2011 年、2013 年に発表している。2012 年の年次計画は APT に焦点をあて、いかに公共および民間部門が重要インフラを防護すべきかについて述べ、原子力発電所、ガス供給ネットワーク、電気通信の作業員は、大規模攻撃に備えた訓練をすべきであると勧めている。2013 年 3 月に、韓国の金融業界とメディア業界が大規模なサイバー攻撃を受け、情報セキュリティ政策会議にまた注意を促すこととなった。

自民党は 2012 年 12 月に選挙で勝利を収め、2013 年 7 月 21 日の参議院選での勝利により、両院における支配を確固たるものにした。これにより、APT、重要インフラ保護、制度改革に対する注目がますます高まることとなった。2011 年の日本の国会におけるセキュリティ侵害（今では APT 攻撃の氷山の一角とみられている）が明らかになった数日後、自民党の政務調査会により設置された IT 戦略特別委員会は、情報セキュリティ向上のため、16 の活動項目を提示した。自民党は 2012 年 2 月に「情報セキュリティに関する提言」を提出し、この中の多くの政策が、NISC による 2013 年サイバーセキュリティ戦略に反映されている。

2011 年の攻撃は、外務省が、日本のサイバーセキュリティ政策を国際的に整備する原因となった。2012 年 2 月、外務省は篠塚保大使の指揮下でサイバーセキュリティ問題への対応を強化した。外務省が新たに興味を持ったことの表れとして、当時の玄葉光一郎外務大臣は、2012 年 1 月、初めて情報セキュリティ政策会議に参加した。そして、4 月の会議で外務大臣は日本のサイバー攻撃に対する軍事対応の方針について説明している（これにつ

いては後述)。2011 年以来、外務省は国際的な行動指針を策定するよう、米国とヨーロッパの政策に則した国際規則の推進をより活発に行ってきた。例えば、2012 年 10 月のブタペストにおけるサイバースペースに関する国際会議など、主要な国際政策会議で米国を支持している[11]。2013 年 10 月に NISC により発表された全く新しい国際政策の一部として、日本は特に防衛省と米国国防総省との情報共有を進め、共同訓練を増加させるために、日米 IT フォーラムや日米サイバー対話などの対話を推進するものとしている。

2011 年の攻撃を受けて、重要インフラを防護する組織は、それぞれの立場と協力を向上しようとした。2012 年、警察庁は、サイバー攻撃を分析するサイバーテロ対策技術室（通称「サイバーフォースセンター」）を設置した。13 の地区のセンターで、140 名のスタッフが、オンラインポストを監視し、電力、ガスなどの公益企業やハイテク企業を含む 4,000 社を超える企業と情報を共有している。NISC は情報セキュリティ緊急支援チーム（CYMAT）を設置し、情報の縦割りによる分断を回避するよう、省庁間の連携を推進した[12]。2011 年 10 月には、経済産業省は全ての戦略セクターが、サイバー攻撃と政策に関する情報を共有できるサイバー情報共有イニシアティブ（J-CSIP）を設置した。J-CSIP は部門ごとのグループで構成されており、電力、ガス、石油、化学部門など重要インフラ製造企業や防衛関連企業が主導している。

さらに 2012 年、経済産業省と総務省の傘下にある 4 つの情報セキュリティ関連組織が、サイバー攻撃解析協議会を設置した。また 2011 年以来、経済産業省は米国の国土安全保障省、エネルギー省、国防総省と情報共有するよう、実務者レベルの関係を深めた。最後に、新しく設立された重要インフラ防護機関を支援するために、2013 年 4 月、18 の組織と共に制御システムセキュリティセンター（CSSC）が設置された。ここでは、産業制御システムのセキュリティ検証と試験機関を支援するために、(1) 排水・下水プラント、(2) ビル制御システム、(3) 組立プラント、(4) 火力発電所訓練シミュレータ、(5) ガスプラント、(6) 広域制御（スマートシティ）、(7) 化学プラントの小型の模型設備を提供する。2013 年度には、この模型設備が実際のシミュレーションに使用される。

2013 年 6 月 10 日に発表したサイバーセキュリティ戦略で、情報セキュリティ政策会議は「サイバーセキュリティ」という用語を初めて使用した。この戦略において、NISC を

---

[11] The Rt Hon William Hague MP, “Security and freedom in the cyber age - seeking the rules of the road,” 04 February 2011 <https://www.gov.uk/government/speeches/security-and-freedom-in-the-cyber-age-seeking-the-rules-of-the-road>.
[12] 「国民を守る情報セキュリティ戦略」<http://www.nisc.go.jp/active/kihon/pdf/senryaku.pdf>。

2016 年 3 月までに「サイバーセキュリティセンター」として再組織して、重要インフラに対するセキュリティを向上させ、同時に重要インフラのカテゴリー数を増加させるとしている。また、警察庁はサイバー犯罪に対して日本版 NCFTA（National Cyber-Forensics and Training Alliance）を設立する予定である。

3.2. 日本の防衛省とサイバーセキュリティ

現在の防衛省のサイバーセキュリティに関する対策は、2000 年の IT 基本法を土台にしている。最初の「e-Japan 構想」の後、当時の防衛庁は、2000 年 12 月に情報セキュリティ規定を盛り込んだガイドラインを採択した。防衛省の最初のサイバー監視ユニットは、航空自衛隊内に設置され、その後、陸上自衛隊と海上自衛隊に別のユニットが設置された。

防衛省（2006 年まで防衛庁）に対する情報セキュリティに対する圧力の変化は、主に米国の情報保証への懸念が原因となっている[13]。2006 年から 2007 年の間、セキュリティ問題対応に関して大きな変化があった。2006 年 4 月、「情報保証とコンピュータ・ネットワーク防御における協力に関する了解覚書」により、情報保証と情報セキュリティを改善しようとした[14]。2007 年 8 月に、日本は軍事情報の交換を活発化するために、「日米軍事情報包括保護協定」に署名した。そして 2007 年 5 月、日米安全保障協議委員会（2+2）は、日米が BMD（弾道ミサイル防衛）と関連作戦情報を互いに直接、リアルタイムで継続的かつ恒常的に共有することを約束し、これにより防衛省はさらにサイバーセキュリティ対策を活発化させることとなった。また 2007 年には、防衛省は脅威に対処するため、防衛情報通信基盤（DII）と呼ばれる統合ネットワークを設置した[15]。2008 年 3 月には、防衛省と自衛隊は自衛隊指揮通信システム隊を発足させた[16]。

防衛省の現在のサイバーセキュリティの基本は、2011 年から 2015 年の中期防衛整備計画と防衛省の 2010 年版防衛白書に記載されたサイバー防衛に関する「6 つの柱」である。現在の中期防衛整備計画は、初めてサイバースペース・セキュリティを重要なセキュリティ問題として認識し、サイバー防衛について取り上げたものである。本計画は、サイバー

---

[13] Emma Chanlett-Avery, "The U.S.- Japan Alliance," *Congressional Research Service*, 18 January 2011 <http://www.fas.org/sgp/crs/row/RL33740.pdf>.

[14] 防衛庁プレスリリース「日本国防衛庁と米国国防省の情報保証とコンピュータ・ネットワーク防御における協力に関する了解覚書（MOU）の締結について」2006 年 4 月 18 日<http://www.mod.go.jp/j/press/news/2006/04/18a.html>。

[15] 「防衛庁・自衛隊における情報通信技術革命への対応に係る総合的施策の推進要綱～　情報優越のための基盤構築を目指して」<http://www.mod.go.jp/j/approach/others/security/it/youkou/index.html>。

[16] 防衛省ウェブサイト「『自衛隊指揮通信システム隊（仮称）』の新編」<http://www.clearing.mod.go.jp/hakusho_data/2007/2007/html/j22c1000.html>。

スペースのセキュリティを宇宙、海洋保全、気候変動と並ぶ日米協力の焦点だとしている。中期防衛整備計画は、防衛省に「日本政府全体」による活動の一環としてのネットワーク保護システムの強化、サイバー防衛能力の開発、政策の策定、サイバー防衛に関する統合した指揮管理系統の設置を要請している。これは「サイバー防衛隊」と呼ばれている[17]。

2010 年に、防衛省はサイバーセキュリティに関するサイバーセキュリティ規定の大幅な整備を開始した。2010 年版白書では初めて、外国の軍隊による国際的な動きを、政策策定の参照として言及した。また白書では初めて以下の「6 つの柱」に基づいた具体的なサイバーセキュリティ対策実施計画に焦点をあてた。1.情報通信システムの安全性向上、2. 防護システムの整備、3. 規則の整備等、4. 人材育成、5. 情報共有等の推進、6. 最新技術の研究である。

2010 年以降に設定された防衛省の新しいサイバースペース政策と規定は、米国、NATO、韓国、英国における展開を政策ベンチマークとして使用した。ここでも、米国からの圧力が、防衛省の（そして日本の）サイバーセキュリティへのフォーカスを形成するのに、重要な役割を担った。2010 年 6 月 21 日、ワシントン DC で 2+2 は、ワシントン DC で日米韓、日米豪間の 3 か国連携を主要な目標として定め、宇宙とサイバースペースに関する協力を初めて重要なアジェンダとして取り上げた。これは米国が、インテリジェンス、監視、海上保全と広範囲な戦争の抑止において、次世代の相互運用性を構築するにあたり、日本にもっと深く関与させる必要性を感じたことを反映している。

これに対応して、2011 年度版防衛白書英語版では、防衛に対する脅威として、サイバースペースの脅威を大量破壊兵器の拡散と国際テロよりも優先順位が高いと位置づけた。スタックスネットが使用されたことに関して、白書は同盟国政府がますます統合と集中管理を進める努力をしていることと、国際協力強化の必要性を述べている。また国際的にみて、インフラのサイバーセキュリティは、国家防衛政策に組み込まれていることについても述べている。さらに白書では、攻撃者の特定、抑止、対応の困難さを含め、教義的な問題についても初めて触れており、国際社会ではサイバー攻撃を武力攻撃として認識するという合意がないこと、これにより既存の交戦規定（SROE）を適用することが難しく、行動規範がないことについて言及している[18]。

---

[17] “Mid-Term Defense Program (FY2011- FY2015) (approved by the Security Council and the Cabinet on December 17, 2010) <http://www.mod.go.jp/e/d_act/d_policy/pdf/mid_termFY2011-15.pdf>.

[18] “International Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World,” May 11, President of the United States <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>.

2012 年、日本政府はサイバー攻撃に対する政府の準備姿勢について公的に説明した。2012 年 4 月の情報セキュリティ政策会議において玄葉外務大臣は、「基本的には、サイバー空間にも従来の国際法が当然適用されるとの立場を取るのが適当と考える」と発言した。そして 2012 年 7 月、防衛省は、「防衛力の在り方検討に関する中間報告」を発表した。このなかで、優先項目リスト上位 10 項目であるサイバー攻撃の対処、宇宙利用促進、海上保全強化に対応し、ISR（インテリジェンス、監視、偵察）能力強化を最優先事項として位置付けるとした。

2012 年 9 月、ようやく防衛省はサイバー防衛戦略に関して 2 つの措置をとった。第一に、防衛省は「防衛省・自衛隊によるサイバー空間の安定的・効果的な利用に向けて」を発表し、初めてサイバー防衛に関する準備方針について言及した。第二に、防衛省はサイバー防衛隊を設立するため、212 億円の予算を要求した[19]。サイバー防衛隊は共同サイバー特別部隊とも呼ばれている。防衛大臣に直接報告をし、情報の縦割り回避の対応をする。

「防衛省・自衛隊によるサイバー空間の安定的・効果的な利用に向けて」は防衛省が初めて公に発行したサイバー攻撃の対応方法についてのガイドラインである。この中では、軍事活動方針の基本骨子も提示されている。武力攻撃の一環として、サイバー攻撃が行われた際は、防衛省と自衛隊が対応を行うものとしている。ただし、これにはサイバー攻撃が防衛省と自衛隊のシステムに対するものである場合のみという重要な条件が付いている[20]。

方針は次のように記載している。「武力攻撃の一環としてサイバー攻撃が行われた場合、自衛権発動の第一要件を満たすことになる。」また、本方針では、サイバー攻撃を軍の中枢インフラを危険に陥れることができる攻撃であるとみなしている。そのため、サイバー攻撃はケースバイケースで検討されるべきであると配慮されているが、インフラへの悪意ある攻撃に対して反撃する権利を日本は有しているということを、本方針では明らかにしている。また、オンライン攻撃への対処についてより詳細な法的枠組みと、サイバー防衛隊の設立について考慮するものとしている。さらに 4 つの「最優先項目」と 5 つの「優先項目」を提示し、以前に策定したイニシアティブ、特にサイバー防衛隊についての条項を具体化して、防衛省のサイバー防衛の姿勢を強化した。

米国との協力は最も重要である。2011 年 6 月の 2+2 声明に関する記載で示したように、

---

[19] Paul Kallender-Umezu, "Experts: Japan's New Cyber Unit Understaffed, Lacks Skills," *Defense News*, 09 July 2013
<http://www.defensenews.com/article/20130709/DEFREG03/307090007/Experts-Japan-s-New-Cyber-Unit-Understaffed-Lacks-Skills>.

[20] "Toward Stable and Effective Use of Cyberspace," Ministry of Defense, Japan, September 2012, pp.1-4 <www.mod.go.jp/e/d_act/.../stable_and_effective_use_cyberspace.pdf>.

防衛省はサイバーセキュリティについての 2 国間戦略的政策についての対話を推進し、二国間協力を推進すると述べた。例えば、サイバー攻撃による被害を受けた環境を想定した演習への参加などである。米国だけでなく、防衛省は英国、オーストラリア、シンガポール、NATO とも対話を通じて協力を強化するとしている。

これを受け、2013 年度版防衛白書英語版は、政府と軍のネットワークおよび重要インフラに対するサイバー攻撃は、国家の安全に多大な影響を及ぼすとしている。またオーストラリア、NATO、韓国、英国、米国での活動について言及している。ここでもサイバースペースについて明確な定義を与えており、領域として定義付けている。防衛省はその立場の正当性を、サイバー戦争と APT 脅威の規模と本質について、最長にして詳細な概要によっても主張している。

4. 防衛省のサイバーセキュリティ規定の課題

統合されたサイバー防衛の指揮系統と方針の両方の設立に関して、防衛省は今までに重大な、しかし制限付きの措置を打ち立てている。さらに、防衛省は制度と憲法の両面から厳しく制限されている。第一に、防衛省の政策はインフラ保護に関して決定的に新しい措置に欠けている。サプライチェーンリスクを軽減するために、防衛省は、情報セキュリティ緊急支援チーム（CYMAT）と民間パートナーがより緊密に協力するようにしているだけである。

第二に、サイバー防衛隊は、スタッフを配置転換された自衛隊員に依存しており、新規増員は少ないと見られている。これでは不適切で、同盟国の整備よりはかなり遅れをとっているのではと批判を受けている。日本の規定は、米国の規定はいうまでもなく、韓国の整備や同等のものと比較すると、確実に劣っている。例えば米国のサイバーコマンドはホワイトハットハッカーなどの 4,000 名のサイバー専門家を雇用する予定である。さらには、日本は 80,000 人の技術専門家が不足していると言われている。このため情報セキュリティ政策会議の構成員だった土屋大洋は海外の同等機関と互角になるよう「愛国心のあるハッカー」の基幹人員を積極的に雇用するように要求している。現在、防衛省では積極的に米国へ訓練のために人員を送り、米国のサーバー机上演習への参加を増やしている。しかし、これら一連の動きをみると、疑問を感じずにはいられない。小規模なのではないか、遅すぎないか、という疑問である。

第三に、防衛省は日本の重要インフラ防護に関しては、小さな役割しか担っていない。これは日本の縦割り行政が原因である。このため、互いに競争する政府部門が重要インフラ防護に関してそれぞれ独自の方針とプログラムを持っており、これを調整しているのはNISC だけである。これに対して、将来のサイバーセキュリティセンターがこれらのアプローチをどれくらい合理化し、どの程度合理化に成功するかが、依然として重要な問題である。

また緊急時に自衛隊が民間の重要インフラを防護するために、法改正が必要であることも明白だ。例えば、自衛隊による災害復興について網羅し、原子力事故、海外での日本人移送などの特例について触れている自衛隊法第 94 条の項目としてサイバー攻撃を追加し、サイバー脅威に対応することができる。

第四に、防衛省は第 9 条により明らかに動きを妨げられている。集団的自衛権を行使する能力が大きく制限されていて、米国への依存が高いままである。例えば、防衛省の方針は米国国防総省のサイバースペース優位性の方針の一部である積極的なサイバー防衛方針にかなり遅れをとっている。現在防衛省は、米軍の主な任務である 2011 年の「サイバースペースのおける作戦戦略（Strategy for Operating in Cyberspace）」に追随している[21]。2011 年 9 月の米国国防総省の「サイバースペース政策報告書（Cyberspace Policy Report）」は、コンピュータ・ネットワーク戦争の理論的根拠と方針についてまとめている。ここで、米国は自国、同盟国、パートナー国をサイバースペースで防御するために、物理的対応や攻撃活動を含むあらゆる必要な手段を使用する権利を有するものとしている。また国防総省はネットワークに関する作戦と防衛の交戦規定を、「既存の方針と法規制」の計画と作戦に統合させた。さらにアフガニスタンの戦場で活動していたメディアのシニアスタッフの例から明らかなように、メディアに対しても活動を開始した。最後に、2013 年、米国統合参謀本部が、国家安全保障会議の承認なしに、軍に反撃を許可する新しい交戦規定を採択した。現在では、規定の適用が開始されている。

これに対して防衛省の方針では事実上、サイバー防衛隊の活動範囲を、サイバー攻撃に「対抗かつ抑制」し、攻撃中に攻撃者のサイバースペースの使用を「拒否」し、自衛隊が「迅速に復興」できるようにすることに限定している。米国は重要インフラの破壊行為を（例えば原子炉の炉心溶解をひき起こすような行為）、サイバースペースでの「武力行使」

[21] Irving Lachow, "Active Cyber Defense: A Framework for Policymakers," *Center for a New American Security*, 22 February 2013 <http://www.cnas.org/files/documents/publications/CNAS_ActiveCyberDefense_Lachow_0.pdf>.

と見なしている。一方、日本はどこで線を引くか曖昧である。

防衛省は、武力攻撃の一環であるサイバー攻撃に対する自衛権があるとしているが、サイバー攻撃を行ったどの武力攻撃について「状況を考慮し」判断する必要があるのかは規定していない。しかし、どうすれば武力攻撃となるかを判断するのは難しい。特定のサイバー作戦は、国連憲章第 2 条 4 項における武力の行使の禁止にあたると同意が得られている。しかし、どのようなサイバー攻撃が禁止された武力の使用にあたるかを判断するのに、国家がどのような基準を用いるのかをあらかじめ知ることは難しい。総じて米国では、とにかく物理的損害や人的被害の原因となるサイバー活動は、武力の行使とみなすという見解が承認されつつある[22]。

防衛省は、先に行動を起こして攻撃を阻止すべきか、その阻止方法、そして通常の（物理的な）先制攻撃の間の活動役割についても明確でない。防衛省は、抑止力の定義として、同等またはより大規模な損害を与えるような攻撃に対する処罰および拒否による阻止であるしている。しかし、攻撃者が国家でなく、脅すことができる資産を所有していない場合、阻止をすることは困難である。これに関して、引き続き攻撃者の特定が基礎的な問題となる。サイバー攻撃を武力攻撃としてみなすかどうかを含め、国際法に従ったサイバー攻撃の定義とステータスに対して、防衛省では同意に達していない。防衛省は既存の交戦規定にサイバー攻撃を適用するのは難しいとだけ述べている。

サイバー攻撃の匿名性のため、報復の警告を行うことは、反撃するための高度な能力がなければ方針として不十分である。反撃するための高度な能力は、防衛省が攻撃的なネットワーク作戦計画を準備したとみなされると、日本国憲法に違反することになる。そのため防衛省の方針と、安倍政権が今後提出する制限された形態での集団的自衛権を許可する提案の関係も不明瞭である。このように防衛省の活動における機能は憲法の制限に従い、防衛目的の使用のみに制限されている。しかし、防衛省が敵を抑止するまでセキュリティレベルを向上させることができるとは期待し難い。このため、「耐えられない損害」を生じさせるという脅しにより攻撃をあきらめさせ、または特定の攻撃を物理的に拒否する能力で攻撃者が目標を達成できる可能性を低くし、相手の費用計算に影響を与えようとする防衛省の現在の方針は、明らかに不十分である。このため、このような複雑な仕組みにおいて、防衛省がいかに現実的に敵を抑止し、どれだけ反撃をし、いつ先制的な作戦を実施で

[22] Andrew C. Foltz, "Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate," *JFQ*, Issue 67, 4th Quarter 2012 <http://www.au.af.mil/au/awc/awcgate/jfq/foltz_stuxnet_schmitt_oct2012.pdf>.

きるかは、いまだに基本的に明らかではない。