IIPS Institute for International Policy Studies
世界平和研究所研究ノート

2015 年 4 月 22 日

防衛省・自衛隊によるサイバーセキュリティへの取組と課題

公益財団法人 世界平和研究所
主任研究員 松﨑みゆき

はじめに

2014 年 12 月以降に限ってみても、ソニー・ピクチャーズエンタテインメントに対するサイバー攻撃、「サイバーカリフ（Cyber Caliphate）」と名乗るハッカー集団による米中央軍の Twitter アカウント及び YouTube アカウントの乗っ取りなど、多様な形のサイバー攻撃が生起している。2015 年 2 月に発表された米情報コミュニティによる脅威評価において、サイバーが第 1 にとりあげられ、最も多くの字数が割かれていることからも明らかなように[1]、サイバー攻撃に対する米国の危機感は高まっている。それに伴い、オバマ政権は、2015 年に入り、サイバーセキュリティを強化する取組を相次いで発表している。日本においても、2015 年 1 月にサイバーセキュリティ戦略本部が設置されるなど、サイバーセキュリティへの取組が進展している。

本稿は、我が国の防衛省・自衛隊によるサイバーセキュリティへの取組の現状について論じ、今後の課題について考察することを目的とする。国防省による取組を中心とした米国のサイバーセキュリティ政策を分析することによって、防衛省・自衛隊による取組の課題を明確にする。経済・人口など国家規模の差に加え、特に軍／自衛隊や情報機関の役割・能力・規模等に関する日米の違いは大きく、米国の取組をそのまま適用することは不可能かつ不適切である。しかし、サイバーセキュリティの分野においても他国に先んずる米国の例を見ることによって、得るものは大きいと考える。

1 日本におけるサイバーセキュリティ

（1）サイバーセキュリティの新たな体制

「国家安全保障戦略」において、「サイバー空間の防護は、我が国の安全保障を万全にするとの観点から、不可欠である[2]。」との認識が示されているとおり、日本の安全保障におけるサイバーセキュリティの重要性は増大し、政府はサイバーセキュリティ政策を進展させている。例えば、現在政府は、2013 年に発表されたサイバーセキュリティ戦略に代わる新たな戦略の策定に取り組んでいる。

また 2015 年 1 月、サイバーセキュリティ基本法の施行に伴い、サイバーセキュリティ戦略本

[1] James R. Clapper, Director of National Intelligence, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee, February 26, 2015.
[2] 国家安全保障会議決定、閣議決定.「国家安全保障戦略について」. 平成 25 年 12 月 17 日、p.8.

部が設置された。事務局として内閣サイバーセキュリティセンター（NISC: National center of Incident readiness and Strategy for Cybersecurity）が発足した。同センターは、2005 年に設置された内閣官房情報セキュリティセンター（NISC: National Information Security Center）を、法的に格上げしたものである。

日本におけるサイバーセキュリティ関係省庁は、警察庁（サイバー犯罪の取締り）、総務省（通信・ネットワーク政策）、外務省（国際連携）、経済産業省（情報政策）及び防衛省（国の安全保障）であり、それぞれの立場からサイバーセキュリティを担っている[3]。さらに、重要インフラ所管省庁として金融庁（金融）、総務省（情報通信、地方公共団体）、厚生労働省（医療、水道）、経済産業省（電力、ガス、化学、クレジット、石油）及び国土交通省（航空、鉄道、物流）がサイバーセキュリティに取り組んでいる[4]。このように、多数の行政機関がサイバーセキュリティに携わる中、NISC は、内閣官房情報セキュリティセンター当時から関係行政機関を統括し、総合調整にあたってきた。関係行政機関から NISC への資料等の提出及び NISC から関係行政機関への勧告は、従来法的権限に基づいたものではなかったが、サイバーセキュリティ戦略本部設置に当たり、法的根拠が与えられた。

（2）防衛省・自衛隊におけるサイバーセキュリティ

ア　防衛省にとってのサイバー空間の位置付け

2013 年に閣議決定された「平成26年度以降に係る防衛計画の大綱」において「宇宙空間及びサイバー空間における対応」は、自衛隊の体制整備にあたって重視すべき機能・能力の一つと位置付けられている[5]。また防衛省は、サイバー空間を「陸・海・空・宇宙と並ぶ一つの『領域』」と定め、「サイバー空間における活動の成否は、陸・海・空・宇宙の領域におけるそれと並び重要」との認識を示している[6]。

サイバー空間の特性としては、一般的に攻撃の主体・手法・目的が多岐にわたるという「多様性」、攻撃源の偽装が容易という「匿名性」、及び攻撃の存在を察知することが困難という「隠密性」が挙げられる[7]。これらの一般的特性に加え、軍事的観点からは「攻撃側の優位性」及び「抑止の困難性」という特性が存在する。防衛省は、攻撃手段の入手が容易、ソフトウェアの脆弱性を完全に排除することは困難等の理由により、「サイバー空間においては、攻撃

---

3 防衛省運用企画局情報通信・研究課．“防衛省のサイバーセキュリティへの取組”．平成 26 年 4 月．http://www.nisc.go.jp/conference/seisaku/ituse/dai2/pdf/siryou0200.pdf（2015 年 3 月 27 日参照）p.8.

4 内閣サイバーセキュリティセンター、“重要インフラ防護に対する考え方”．http://www.nisc.go.jp/active/infra/outline.html（2015 年 3 月 27 日参照）

5 国家安全保障会議決定、閣議決定．「平成２６年度以降に係る防衛計画の大綱」平成 25 年 12 月 17 日、p.18.

6 防衛省．“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”．平成 24 年 9 月、http://www.mod.go.jp/j/approach/others/security/cyber_security_sisin.html（2015 年 3 月 26 日参照）

7 同上。

側が防御側に対して圧倒的な優位にある。」とみなしている。さらに、この「攻撃側の優位性」を踏まえると、攻撃主体が報復対象となることを恐れない場合等に攻撃を断念させることは難しいため、サイバー攻撃の抑止は困難と認識している[8]。これらサイバー空間の特性は、自衛隊がサイバー攻撃に対処するにあたり、「陸・海・空」という伝統的な領域における運用とは異なる課題をもたらしている。

イ　防衛省・自衛隊によるサイバーセキュリティへの取組

防衛省は、日本のサイバーセキュリティ政策の中で、「国の安全保障」という観点からサイバー攻撃に対処するため、自衛隊の能力・態勢強化に取り組んでいる。防衛省・自衛隊によるサイバーセキュリティへの取組は、①防衛省・自衛隊の能力・態勢強化、②民間も含めた国全体の取組への寄与、③同盟国を含む国際社会との協力の3つに大きく分けられる[9]。

2014 年 3 月に新編されたサイバー防衛隊は、自衛隊によるサイバー攻撃対処の態勢強化の一例である。サイバー防護隊は情報収集・共有、防護、技術支援、調査研究、訓練を任務とし、防衛省・自衛隊のネットワークの監視を行い、事案に対処する[10]。サイバー防衛隊の新編により、それまで各自衛隊が保有していたサイバー攻撃等に関する脅威情報を省全体として保有することが可能となった。重要インフラ対策は引き続き NISC や所管省庁が担い、サイバー防衛隊は重要インフラ関連企業、防衛産業のシステム・ネットワークは防護しない。

2011 年 8 月、三菱重工業がサイバー攻撃を受け、潜水艦、ミサイルなどを含む研究・製造拠点でのウイルス感染の確認が報道された[11]。また、感染は確認されなかったものの、三菱電機、IHI 及び川崎重工業も同様の攻撃を受けていたことが判明した[12]。本事案は、防衛産業に対するサイバー攻撃の未然防止及び攻撃された場合の情報共有のために、防衛省と防衛産業の連携を強化する必要性を改めて示すものとなった。

2013 年 7 月、防衛省は民間企業との連携強化策の一つとして、防衛省及び防衛産業のサイバー攻撃対処能力向上を目的とした「サイバーディフェンス連携協議会」（CDC: Cyber Defense Council）を設置した。CDC は、防衛省がハブとなり、参加企業間の情報共有を促進する取組である。CDC への参加企業は「サイバーセキュリティに関心の深い防衛産業 10 社程度」と発表されているが[13]、具体的な企業名は明らかにされていない。その理由として防衛

8 同上。
9 同上。
10 防衛省運用企画局情報通信・研究課．“防衛省のサイバーセキュリティへの取組”．p.11.
11 三菱重工にサイバー攻撃　防衛・原発関連など 11 拠点 産業スパイの可能性も．日本経済新聞の電子版サイト．2011 年 9 月 19 日 18:17、http://www.nikkei.com/article/DGXNASDG1900N_Z10C11A9000000/ （2015 年 4 月 1 日参照）
12 2011 年 9 月 21 日　日本経済新聞、読売新聞、朝日新聞
13 防衛省運用企画局・経理装備局．“サイバーディフェンス連携協議会（ＣＤＣ）の設置・取組について”．平成 25 年 7 月、http://www.mod.go.jp/j/approach/others/security/cyber_defense_council.pdf（2015 年 4

省は、「①防衛産業側の円滑な協力が得られるように取り組む必要があること、②率直な意見交換、情報共有等を行いやすい環境を整備する必要があること、③CDC に参加することにより企業活動に何らかの影響を及ぼさないようにする必要があること」と説明している[14]。

防衛省はまた、シンガポール、ベトナム、インドネシア、英国、エストニア、韓国の防衛当局及び NATO との間に IT・サイバー協議の場を設けるなど、国際社会との協力を進めている。中でも、同盟国である米国との間では、2013 年 10 月の「2＋2」会合において、サイバー空間における協力向上に合意したことに加え、「日米防衛協力のための指針」の見直し作業において「同盟の文脈での宇宙及びサイバー空間における協力」の重要性を確認するなど、サイバー空間における協力が一層進んでいくものと推測できる。

2 米国におけるサイバーセキュリティ―国防省による取組を中心として

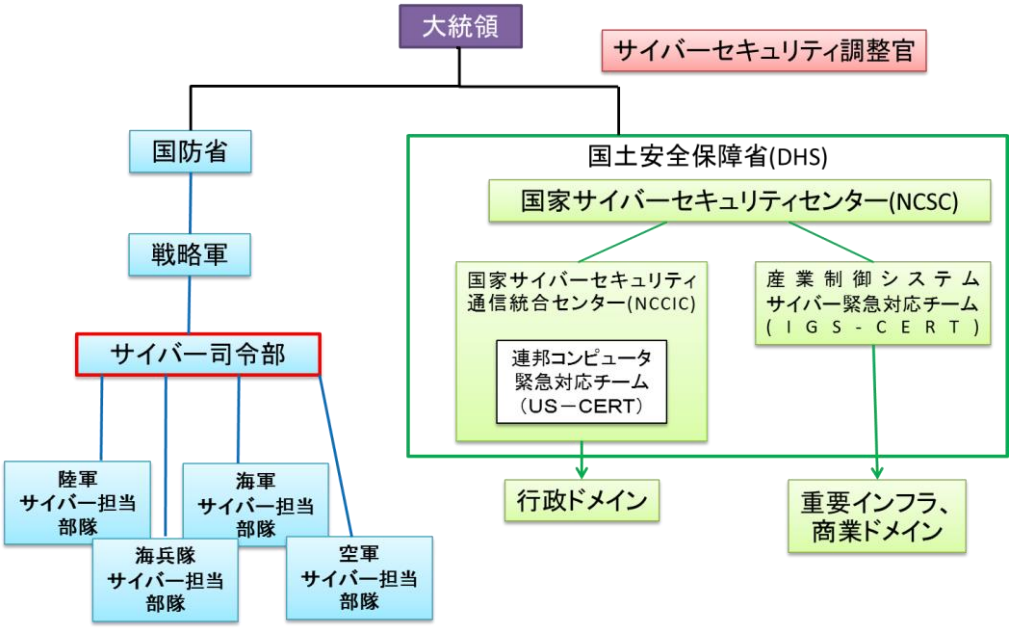
（1）サイバーセキュリティ関連組織

米国政府では、国土安全保障省（DHS: Department of Homeland Security）と国防省がサイバーセキュリティ政策において中心的役割を担っている。DHS は、国防関係を除く連邦政府のネットワーク及び民間の重要インフラシステムの保護など、国土安全保障の実現という観点から、連邦政府のサイバーセキュリティ全般を所掌している。国防関係以外の連邦政府機関及び重要インフラのサイバーセキュリティを DHS が一括して担っている点が、米国と日本の大きな違いである。

一方国防省は、国家防衛及び安全保障という観点から、サイバー司令部を中心として、国防関連のサイバーセキュリティを担当している。2009 年 12 月には、国防省と DHS の枠を超えた政府全体のサイバーセキュリティ政策の調整のため、サイバーセキュリティ調整官のポストが新設された。

月 1 日参照） p.4.

14 同上。



（米国のサイバーセキュリティ関連組織概念図）

（2）サイバー空間における戦略

2009 年 1 月、オバマ大統領は就任に当たり、サイバーセキュリティを政権の優先課題と位置付け、サイバーセキュリティ戦略の見直しを指示した。その結果、オバマ政権第１期には、サイバー空間における戦略が相次いで策定され、重要な指針が示された。

2011 年 5 月にホワイトハウスが“International Strategy for Cyberspace”「サイバー空間のための国際戦略」を、続いて国防省及び DHS がそれぞれ 7 月と 11 月に“Department of Defense Strategy for Operating in Cyberspace”「サイバー空間の作戦のための戦略」及び“Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise”「国土安全保障事業者のためのサイバーセキュリティ戦略」を発表した。

ア　ホワイトハウス「サイバー空間のための国際戦略」

「サイバー空間のための国際戦略」は、米国初のサイバー空間の包括的国際戦略文書であり、米国のサイバーセキュリティ政策の基礎となる重要な方針を示したものである。同戦略では、ネットワーク防護にあたっての脅威対象は、「テロリスト、犯罪者、国家及び国家の代理人[15]」のすべてであり、サイバー空間における敵対行為には、「他の脅威への対応と同様に、自衛権に基づき対応する[16]」と述べられている。また、防護対象としては「国家、同盟国、パートナー国及び国益[17]」が示され、米国のみならず同盟国等も対象となることが明記された。さら

15 The White House, International Strategy for Cyberspace, May 2011, p.12.
16 Ibid.,p.14.
17 Ibid.

に、サイバー攻撃対処のための手段として、「国際法に基づくすべての必要な手段（外交、情報、軍事、及び経済）を使用する権利を留保する[18]」と記し、軍事的手段が含まれることを明確に規定した。

イ　国防省「サイバー空間における作戦のための戦略」、「サイバー空間政策報告」

国防省は、ホワイトハウスが示した戦略の下位文書として、サイバー空間における国防省の戦略及び政策を発表している。2011 年 7 月に「サイバー空間における作戦のための戦略」を発表し、サイバー空間を陸、海、空、宇宙空間と同様の作戦領域の一つと位置付けた[19]。さらに同年 11 月、国防省は、“Cyberspace Policy Report”「サイバー空間政策報告」を発表した。同報告では「大統領は、サイバー空間の悪意ある行為から、合衆国、同盟国、パートナー、国益を守るために必要とされるあらゆる手段を用いて対応する権利を持つ[20]」と記し、「サイバー空間のための国際戦略」で示された方針を踏襲している。サイバー攻撃対処として、軍事的手段が選択され得ることについては「サイバー空間のための国際戦略」においても述べられていたが、「サイバー空間政策報告」では、軍事的手段にはサイバー上の能力に加え、物理的能力を用いた対処を含むことが初めて明示された[21]。

（3）サイバーセキュリティに関する最近の動向

ア　サイバー司令部（US　CYBER　COMMAND）

サイバー司令部（US　CYBER　COMMAND)は、サイバー空間における作戦能力の強化を目的として設置され、2010 年に運用を開始した。従来米軍では、陸海空及び海兵隊が個別にサイバー部隊を運営していたが、同司令部は、各軍種のサイバー部隊を統括し、国防省のネットワーク防護に責任を持つこととなった。

2014 年 3 月時点で約 900 人態勢であったサイバー司令部は、2016 会計年度末までに 6200 名規模に増強される予定である[22]。サイバー司令部は「国家任務部隊」(National Mission Forces)、「戦闘任務部隊」(Combat Mission Forces)、「サイバー防護部隊」(Cyber Protection Forces)から構成され、それぞれ重大な結果が生じた場合のサイバー攻撃対処、任務部隊指揮官の補佐、国防省内ネットワークの運用・防護を担当するように計画されている[23]。なお、サ

---

18 Ibid.

19 Department of Defense, Department of Defense Strategy for Operating in Cyberspace, July 2011, p.5.

20 Department of Defense, Department of Defense Cyberspace Policy Report, November 2011, p.2.

21 Ibid.,p.4.

22 Statement of Admiral Michael S. Rogers, Commander, United States Cyber Command, Before the House Committee on Armed Services Subcommittee on Emerging Threats and Capabilities, March 4, 2015. p.7.

23 Department of Defense, Office of the Under Secretary of Defense (Comptroller)/(CFO), February 2015, Fiscal Year 2016 Budget Request Overview, http://comptroller.defense.gov/Portals/45/documents/defbudget/fy2016/fy2016_Budget

イバー司令部司令官マイケル・S・ロジャーズ大将の議会での証言を踏まえれば[24]、「国家任務部隊」が担当する「重大な結果が生じた場合のサイバー攻撃対処」とは、重要インフラがサイバー攻撃を受け、「重大な結果が生じた場合の」対処を指すと思われる。

イ　サイバーセキュリティとインテリジェンス

サイバーセキュリティとインテリジェンスは密接な関係にあり、それを端的に示しているのが、国家安全保障局(NSA : National Security Agency)とサイバー司令部は同一基地に所在し、NSA 長官とサイバー司令部司令官は同一人物が務めているという事実である。NSA とサイバー司令部は任務上のパートナーにあたり、NSA はサイバー空間における外国からの脅威情報の収集・解析を実施している。元 NSA 外部契約社員エドワード・スノーデンによる漏えい事件の後、NSA の改革に関する議論の中で、NSA 長官とサイバー司令部司令官の兼任の是非が論じられた。現在も議論は継続しているが、現長官兼司令官であるロジャーズ大将は、両機関の強化のためには、兼任を強く推奨すると議会で証言している[25]。

サイバーセキュリティとインテリジェンスの関係を強化する新たな取り組みとして、2015 年 2 月、オバマ大統領は、「サイバー脅威情報統合センター」Cyber Threat Intelligence Integration Center(CTIIC)の創設をクラッパー国家情報長官に指示した。CTIIC 自体は情報収集を実施せず、DHS、FBI(連邦捜査局)、国防省、NSA、CIA(中央情報局)などが個別に収集しているサイバー脅威情報を集約し、攻撃者の特定や分析を実施することによって、迅速に対応策を講じることを目的としている[26]。

ウ　政府と民間企業との連携

2015 年 1 月、オバマ大統領は、サイバーセキュリティに関する官民での情報共有推進を目的とした法案を提案すると述べ[27]、一般教書演説においても議会に対し、法案通過を促した。オバマ政権は、2011 年から重要インフラに関連する企業を中心とした民間企業に、サイバーセキュリティ対策について政府への報告を義務付ける「サイバーセキュリティ情報共有法案」を提案しているものの成立に至っていない。その背景には、個人情報保護の問題に加え、産業界及び共和党が政府による民間企業の監視を懸念していることがある。

_Request_Overview_Book.pdf, p.5-5. （2015 年 4 月 10 日参照）

24 Admiral Michael S. Rogers, Commander, U.S. Cyber Command and Director, National Security Agency, “Cybersecurity Threats: The Way Forward,” Hearing of the House (Select) Intelligence Committee, November 20, 2014.

25 Statement of Admiral Michael S. Rogers, March 4, 2015, p.16.

26 The White House, FACT SHEET: Cyber Threat Intelligence Integration Center, www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center（2015 年 4 月 3 日参照）

27 The White House, Remarks of the President at the National Cybersecurity Communications Integration Center, January 13, 2015, https://www.whitehouse.gov/the-press-office/2015/01/13/remarks-president-national-cybersecurity-communications-integration-cent（2015 年 4 月 3 日参照）

また 2015 年 2 月に発した大統領令[28] において、オバマ大統領は、官民及び民間企業間の情報共有促進を目的として、民間企業間でサイバー情報を共有する「情報共有・分析機関」(Information Sharing and Analysis Organizations)の自発的な創設を促した。アップル、VISAなどの企業が協力を表明したものの、企業は株主や世論の批判を恐れ、サイバー攻撃を受けた場合も公表に消極的と言われており、実現は容易ではないことが推測される。

エ サイバー攻撃への対応

①2014 年 中国人民解放軍当局者起訴

2013 年 6 月の米中首脳会談においてサイバー攻撃が主要議題の一つとなり、7 月にはサイバー攻撃問題について協議する初の作業部会を開催するなど、米国は中国との間でサイバー攻撃についての協議を実施している。そのような中で、2014 年 5 月米司法省は米国企業にサイバー攻撃を行ったとして、産業スパイ及び商業機密窃盗などの罪状で、中国人民解放軍サイバー部隊の当局者5名を起訴したと発表した[29]。これは、サイバー空間において、米国企業の秘密情報を商業目的で窃取した国家機関当局者を起訴した初の事例である。

2015 年 2 月に公表された「国家安全保障戦略」には、中国の民間セクターもしくは中国政府による、サイバーを通じた商業目的での企業秘密窃取から、米国企業を防護するために必要な措置を講ずるという方針が示されており[30]、人民解放軍当局者の起訴はその方針を目に見える形で表したものと言える。

②2015 年ソニー・ピクチャーズエンタテインメントへのサイバー攻撃に対する金融制裁

2015 年 1 月、オバマ大統領はソニー・ピクチャーズエンタテインメント(SPE)に対するサイバー攻撃への対抗措置として、北朝鮮政府・朝鮮人民軍及びその関連企業・同関係者に金融制裁を科す大統領令に署名した[31]。サイバー攻撃によって米企業に大規模な経済上の損失を与えたこと、関係者の言論の自由を制限したことが、制裁の理由とされている[32]。

---

28 The White House, Executive Order-Promoting Private Sector Cybersecurity Information Sharing-, February 13, 2015, www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity, (2015 年 4 月 3 日参照)

29 The Department of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage, May 19, 2014, http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor (2015 年 4 月 3 日参照)

30 The White House, National Security Strategy, February 2015, p.24.

31 The White House, Executive Order-Imposing Additional Sanctions with Respect to North Korea, January 02, 2015, https://www.whitehouse.gov/the-press-office/2015/01/02/executive-order-imposing-additional-sanctions-respect-north-korea (2015 年 4 月 3 日参照)

32 The White House, Statement by the Press Secretary on the Executive Order Entitled "Imposing Additional Sanctions with Respect to North Korea," January 02, 2015,

2つの事例は、攻撃主体は外国政府、被攻撃主体は米民間企業という共通点を持つ一方、サイバー攻撃の目的は、一方が企業秘密の窃取による商業上の利益であったことに対し、米国による発表のとおり北朝鮮政府による攻撃であるならば、他方は恐らく映画の公開妨害を目的としていたという相違も存在する。

2015 年 4 月、オバマ大統領は、サイバー攻撃に関与した海外の個人・団体が米国に所有する資産の凍結を可能にする大統領令を発した[33]。本大統領令は、米国が通常の法律で取り締まることが難しい海外の個人・団体を対象としており、制裁が科され得るサイバー攻撃として「米国の安全保障、外交政策、経済・金融の安定」に対し「重大な脅威」となる、「重要インフラへの攻撃」「ネットワーク妨害」「個人情報、金融データ、企業秘密、知的財産の窃取」などが示されている。米国政府は、米国が直面するサイバー脅威に対応するためには、外交、司法、経済、軍事、インテリジェンスのあらゆる手段を必要としており、この大統領令はその手段の一つであると説明している[34]。

2つの事例及び新たな大統領令を踏まえると、今後米国は、攻撃主体、被攻撃主体及び攻撃の目的等が様々なサイバー攻撃に対し、幅広い手段を用いて対処していくものと考えられる。

3 今後の課題

(1)サイバー攻撃への対処

サイバー空間における国際的規範は現在確立の途上にあり、サイバー攻撃対処に係る法的裏付けは国際社会共通の課題である。国連総会第一委員会のサイバーセキュリティに関する政府専門家会合の報告書に、国連憲章を含めた既存の国際法体系はサイバー空間に適応可能と記されたことから[35]、国連憲章で認められている「武力攻撃」に対する自衛権の行使は、サイバー空間での攻撃にも適用できるとの国際的な共通認識は存在する。

---

https://www.whitehouse.gov/the-press-office/2015/01/02/statement-press-secretary-executive-order-entitled-imposing-additional-s (2015 年 4 月 3 日参照)

33 The White House, Executive Order -- "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," April 01, 2015, https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m (2015 年 4 月 3 日参照)

34 The White House, On-the-Record Press Call on the President's Executive Order, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," https://www.whitehouse.gov/the-press-office/2015/04/01/record-press-call-president-s-executive-order-blocking-property-certain-, April 01,2015 (2015 年 4 月 3 日参照)

35 United Nations General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, .June 24, 2013 https://ccdcoe.org/sites/default/files/documents/UN-130624-GGEReport2013_0.pdf (2015 年 4 月 3 日参照)

しかし、サイバー攻撃の態様及び被害の規模・性質が多岐にわたる中で、どのようなサイバー攻撃が自衛権の行使を主張し得る「武力攻撃」に相当するかについての定義は確立されていない。防衛省は「何らかの事態が武力攻撃に当たるか否かは、個別具体的な状況を踏まえて判断すべきもの」としたうえで、「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と考えられる。」との基本的見解を示している[36]。そしてサイバー攻撃及び対処に関する法的位置付けについては、検討を継続するとしている[37]。法的位置付けを初めとして、サイバーセキュリティをめぐる論点は多数考えられるが、本稿では「第3国のサーバーを経由して攻撃が行われた場合の第3国への対処」及び「サイバー空間における攻撃」を例としてとりあげる。

サイバー攻撃に特有な事例として、第3国のサーバーを経由して行われる攻撃が存在する。米国防省は、第3国経由でサイバー攻撃が行われた場合の第3国への対処の基準例として、「第3国が自国のサーバー経由で攻撃が行われていることに気づいていたか」「第3国自身が何らかの役割を果たしたのか。果たしていたとすれば、その役割は何か」「悪意のあるサイバー活動に効果的に対応するための、第3国の能力及び意志の有無」を挙げている[38]。このように、米国は第3国への対処を否定していない。米国は、サイバー攻撃に対する軍事的手段として物理的な反撃を選択肢の一つとしているが、特に第3国への対処としても、物理的な軍事攻撃という選択肢を排除しないのであれば、さらに難しい問題が提起されるであろう。

また現在、サイバー空間における攻撃の是非について、米国政府内で議論が行われている[39]。ロジャーズサイバー司令部司令官は、これまで同司令部はサイバー防御力に重点を置いてきたが、抑止の有効性という意味では、攻撃力の増大を検討する必要があると述べている[40]。2016 会計年度国防予算案において、サイバー空間での「防御」「攻撃」能力を増大すると記されており[41]、攻撃のための能力は強化されている一方で、サイバー司令部司令官に攻撃実施の権限を与えるかについて、オバマ大統領の決定は保留されている[42]。

---

36 防衛省.「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」. ここでいう「自衛権発動の第一要件」とは「我が国に対する急迫かつ不正の侵害があること」であるが、2014 年 7 月 1 日の閣議決定を受けた「新たな三要件」の一つとして「我が国に対する武力攻撃が発生したこと、または我が国と密接な関係にある他国に対する武力攻撃が発生し、これによりわが国の存立が脅かされ、国民の生命、自由および幸福追求の権利が根底から覆される明白な危険があること」が示された。

37 同上。

38 Department of Defense Cyberspace Policy Report, A Report to Congress, November 2011, p.8.

39 Barack Obama Says Cyber Security is More Like Basketball Than Football, Re/code, http://recode.net/2015/02/14/how-cyber-security-is-like-basketball-according-to-barack-obama/（2015 年 4 月 7 日参照）

40 Statement of Admiral Michael S. Rogers, March 19, 2015, pp.27-28.

41 DoD, Office of the Under Secretary of Defense (Comptroller)/(CFO), 5-5

42 Admiral Michael S. Rogers, Commander, U.S. Cyber Command and Director, National Security Agency, Committee on Armed Services, United States Senate, Hearing to Receive Testimony on U.S. Strategic Command, U.S. Transportation

第3国への対処及びサイバー空間における攻撃に関する防衛省・自衛隊内での検討状況を公開されている情報から推測することは難しいが、仮にまだ十分に議論されていないとすれば、今後検討すべき課題となることが予想される。通常の攻撃と比べ、サイバー攻撃は技術の進歩が速く、技術の進展に伴い新たな課題が出現するものと考えられる。そのため、自衛権発動の要件を満たすサイバー攻撃の要件及び攻撃への対処手段等について、あらかじめ厳密に規定することは難しい上に適当でないと言えよう。しかしその一方で、その時点において考えうるあらゆる事態を想定し、対処方針等について検討を行う必要があろう。

（2）サイバー攻撃対処とインテリジェンス

サイバー攻撃の未然に防止とともに、攻撃を受けた場合の適切な対処には、攻撃元となり得る国・組織及び個人のサイバー能力等に関する情報収集・分析が不可欠である。サイバーセキュリティの効果的実施に向け、政府全体でサイバー脅威に関する情報収集・分析能力の強化を図るとともに、各情報機関が個別に実施しているとみられる情報収集・分析結果を集約し、共有する取組が必要とされる。

また、米国における NSA とサイバー司令部の例を見るまでもなく、サイバー防衛担当部隊と情報機関の間の緊密な連携が重要である。サイバー防衛隊と情報機関の連携の現状について、公開情報から推測することは難しいが、仮に十分な協力態勢にないならば、関係強化に努める必要がある。そして、防衛省・自衛隊内にとどまらず、関係省庁及び民間企業との間でも可能な限りサイバー脅威情報の共有が図られることが望まれる。

（3）重要インフラのサイバーセキュリティと防衛省の役割

これまで見てきたとおり、重要インフラのサイバーセキュリティは NISC 及び所管省庁が担っており、現状では防衛省が関与する余地は限られている。しかし、重要インフラと国の安全保障は密接に関係するため、重要インフラのサイバーセキュリティに関し、防衛省の積極的関与が求められる。「サイバーディフェンス連携協議会」（CDC）における取組に見るように、防衛省と防衛産業の関係は強化されつつあり、それを例として重要インフラ関連企業との連携も促進する必要があろう。

おわりに

米国防省が、2016 会計年度予算要求においてサイバー能力向上のために 55 億ドル（6600 億円）を計上しているのに対し[43]、防衛省の 27 年度予算要求におけるサイバー関連予算は

Command, and U.S. Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2016 and the Future Years Defense Program, March 19, 2015, p.28.

[43] DoD, Office of the Under Secretary of Defense (Comptroller)/(CFO), February 2015, Fiscal Year 2016 Budget Request, http://www.defense.gov/pubs/FY16_Budget_Request_Rollout_Final_2-2-15.pdf （2015 年 4 月 10 日参照）, p.8.

103 億円にとどまっており[44]、米国は日本の約 64 倍となっている。国防／防衛予算の規模が異なるため、金額を比較する意味は大きくないかもしれないが、米国防予算と日本の防衛予算の差が約 14 倍であることを考えると[45]、日本のサイバー関連予算は十分とは言い難いのではないだろうか。また、米国のサイバー司令部が 6300 人態勢に増強される予定である一方、自衛隊のサイバー防衛隊は約 90 人態勢であり、人員規模の比較でみても約 70 倍の差が生じている。このような数値を見るに限っても、米国と比較した場合のみならず、日本の安全保障上にとって不安定要因となり得る国家のサイバー関連予算・人員等との比較においても、日本の予算・人員は不十分であると言わざるを得ない。

サイバーセキュリティに関する予算・人員の制約は、防衛省を初めとする関係省庁だけの問題ではなく、民間を含めた日本全体の課題である。その中で日本のサイバーセキュリティを強化していくには、政府内の関係組織のうち重複する機能を統合したうえで、各組織で情報共有を進めるなど、予算・人員の効率化をはかることが現実的な解決策となろう。加えて情報共有及び人材育成にあたっては、民間企業、特に重要インフラ関連企業・防衛産業との連携強化が重要である。

（本稿に示された見解は執筆者個人のものであり、所属組織の見解を示すものではありません。）

44 防衛省．「我が国の防衛と予算　平成 27 年度概算要求の概要」．
http://www.mod.go.jp/j/yosan/2015/gaisan.pdf（2015 年 4 月 10 日参照）、p.15.
45 米国約 5853 億ドル（約 69 兆円）、日本約 4 兆 9800 億円