日米サイバーセキュリティ協力の課題

慶應義塾大学
土屋大洋

1. はじめに

いわゆる「サイバー攻撃（cyber attack）」は、人命に危害を及ぼしたり、物理的な破壊をしたりする本物の兵器というよりも、「大量迷惑兵器（Weapons of Mass Disturbance: WMD）」とでも呼べる手法を用いてきた。マスメディアで報じられるサイバー攻撃のほとんどはサイバー犯罪やサイバーエスピオナージ（スパイ活動）の変種に過ぎない。しかしながら、本来のサイバー攻撃、つまり、「攻撃的にせよ、防衛的にせよ、人を傷つけたり殺したり、あるいは物体に損害や破壊をもたらしたりすることが合理的に期待されるサイバー作戦（cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects[1]）」の可能性を将来にわたって否定することはできない。イランの核施設に対するスタックスネット（STUXNET）攻撃が露見してから 6 年近くが経っており、他の国や非国家主体がそうした強力なサイバー兵器を用いることが可能になっていてもおかしくない。

日本政府に対する最初の大きなサイバー攻撃は 2000 年に見られた。いくつかの政府省庁のウェブ・サイトが乗っ取られ、改ざんされた。この事案は、政府がサイバー・テロに対する対策を発表した直後に行われた。しかし、この事案は技術的な問題だとされ、社会や経済に影響する国家安全保障の問題とは捉えられなかった。今日、サイバー犯罪やサイバーエスピオナージを含む広い意味でのサイバー攻撃は、日本でも世界でも日常茶飯事になっている。ウェブの改ざんだけではなく、重要インフラストラクチャの機能不全や金融市場の混乱、防衛システムの故障なども、可能性のあるリスクとして視野に入ってきている。

日米間のサイバーセキュリティ協力については、米国戦略国際問題研究所（CSIS）から 2015 年 11 月に提言が出ており、（1）十分な資源の割り当て、（2）日米安保条約第 5 条の適用の明確化、（3）情報共有と協力のためのメカニズムの創設、（4）共同訓練・演習、（5）民間の重要インフラストラクチャの保護とカウンター・エスピオナージ、（6）北東アジアにおける信頼醸成措置（CBM）の調整、という六つの点が指摘されている[2]。

---

[1] Michael N. Schmitt, ed., *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, New York: Cambridge University Press, 2013, Rule 30.
[2] James Andrew Lewis, "U.S.-Japan Cooperation in Cybersecurity: A Report of the

本稿では、(1) 日米防衛協力指針、(2) 海底ケーブル保護、(3) SIGINT (Signal Intelligence) 活動という三つの点から検討してみたい。

2. 日米サイバーセキュリティ協力

2.1. 日米防衛協力のための指針（ガイドライン）

日米両国政府は「日米防衛協力のための指針（ガイドライン）」をこれまで 1978 年、1997 年、2015 年に策定してきた。言うまでもなく、1978 年と 1997 年のガイドラインにはサイバーセキュリティは盛り込まれていない。2015 年のガイドラインは八つの章を持つが、その第 6 章で宇宙とサイバースペースの協力が論じられている。その該当部分はそれほど長くないので引用しよう[3]。

> 日米両政府は、サイバー空間の安全かつ安定的な利用の確保に資するため、適切な場合に、サイバー空間における脅威及び脆弱性に関する情報を適時かつ適切な方法で共有する。また、日米両政府は、適切な場合に、訓練及び教育に関するベストプラクティスの交換を含め、サイバー空間における各種能力の向上に関する情報を共有する。日米両政府は、適切な場合に、民間との情報共有によるものを含め、自衛隊及び米軍が任務を達成する上で依拠する重要インフラ及びサービスを防護するために協力する。
>
> 自衛隊及び米軍は、次の措置をとる。
>
> - 各々のネットワーク及びシステムを監視する態勢を維持すること
> - サイバーセキュリティに関する知見を共有し、教育交流を行うこと
> - 任務保証を達成するために各々のネットワーク及びシステムの抗たん性を確保すること
> - サイバーセキュリティを向上させるための政府一体となっての取組に寄与すること
> - 平時から緊急事態までのいかなる状況においてもサイバーセキュリティのための実効的な協力を確実に行うため、共同演習を実施すること
>
> 自衛隊及び日本における米軍が利用する重要インフラ及びサービスに対するものを含め、日本に対するサイバー事案が発生した場合、日本は主体的に対処し、緊密な二国間調整に基づき、米国は日本に対し適切な支援を行う。日米両政府はまた、関連情報を迅速かつ適切に共有する。日本が武力攻撃を受けている場合に発生するものを含め、日本の安全に影響を与える深刻なサイバー事案が発生した場合、日米両政府は、緊密に協議し、適切な協力行動をとり対処する。

CSIS Strategic Technologies Program," Center for Strategic and International Studies <http://csis.org/files/publication/151105_Lewis_USJapanCyber_Web.pdf>, November 2015.

[3] 防衛省・自衛隊「日米防衛協力のための指針」防衛省 <http://www.mod.go.jp/j/approach/anpo/shishin/>、2015 年 4 月 27 日（2016 年 2 月 4 日アクセス）。

これらのうち、最も重要なのは最後の段落である。特に、「日本の安全に影響を与える深刻なサイバー事案が発生した場合」が何を意味するのかが重要である。日本の防衛省と米国の国防総省はどのようなサイバー事案で自衛隊と米軍を展開できるのか、まだ詳細を詰められていないようである。

狭義のサイバー攻撃においては、人的な被害や物的な破壊を伴うことになる。そうした攻撃が国連憲章でいう武力行使や武力攻撃にあたるのかは解釈の余地があるだろう[4]。少なくとも、誰がそのサイバー攻撃を行ったのか、その意図は何かという点について確定しない限り、適切な対応は難しい[5]。しかし、大きな被害が出れば、そのまま自衛権の行使につながる事態になる。人的・物的な被害のないサイバー攻撃は、多くの場合、サイバー犯罪あるいはサイバーエスピオナージでしかなく、自衛隊や米軍を展開するのは難しいだろう。その代わりに、法執行機関やインテリジェンス機関が対応することになり、起訴や経済制裁が行われることになるだろう。

一つの可能性のあるシナリオは、防衛のための指揮通信システムに対するサイバー攻撃である。そうしたシステムがサイバー攻撃によって機能しなくなり、潜在的な敵国が軍を動かしているという事態になれば、反撃が考慮されることになるかもしれない。しかし、そうした危機にどうすれば相応の対応がとれるかは慎重な考慮が必要になる。双方が十分に理解していなければ、サイバー紛争が物理的な紛争や戦争にエスカレートすることになりかねない。

考慮すべきアイデアは、領空侵犯と領海侵犯の概念である[6]。データの置かれている場所という観点からサイバースペースを考えると、サイバースペースにおける国境を特定するのはきわめて難しくなる。しかしながら、設備の場所という観点から考えるならば、国境を特定し、法管轄を考えるのは容易になる。国境内の設備に対して危害が加えられた場合には、国内法で対応することができる。

領空侵犯の考え方では、事前許可なくいかなる航空機も領空の中に入ることは許されない。対照的に、危害のない形で船舶が領海に入ることは通常認められている。無害な通信がデフォルトで許されているという点では、サイバースペースは領空よりも領海の考え方に近い。しかしながら、設備ベースのサイバースペースにおける有害なデジタル・ビット

---

[4] 真山全「原子力施設に対するサイバー攻撃と国際法」『読売クオータリー』第 21 号、2012 年、84～93 頁。
[5] 中谷和弘「サイバー攻撃と国際法」『国際法研究』第 3 号、2015 年 3 月、59～101 頁。
[6] 土屋大洋「非伝統的安全保障としてのサイバーセキュリティの課題」渡邉昭夫、秋山昌廣編著『日本をめぐる安全保障　これから 10 年のパワー・シフト　その戦略環境を探る』亜紀書房、2014 年、第 9 章。

に対応する権利は依然として保持されている。このアイデアは、日米間を含む国際的な協力を容易にする可能性がある。

2.2. 海底ケーブル保護

日米という文脈において特に注目したいのが海底ケーブルの保護である。図 1 が示すように、太平洋にはたくさんの海底ケーブルが敷設されている。米国はグローバルなインターネット接続の中心に位置する。日本は、世界の成長の中心であるアジアへの入り口に位置している。両国の間の接続は、アジア太平洋地域の自由な情報の流通に不可欠の役割を果たしている。民間企業がほとんどのケーブルと陸揚げ局を所有している。われわれの通信は人工衛星よりも海底ケーブルに頼るようになっているため、そうしたケーブルの物理的な保護はますます重要になっている。日本の場合には、国際通信の 99%が海底ケーブルを通っている。軍事通信や金融の通信もまた高速のケーブルに多くを頼っている。

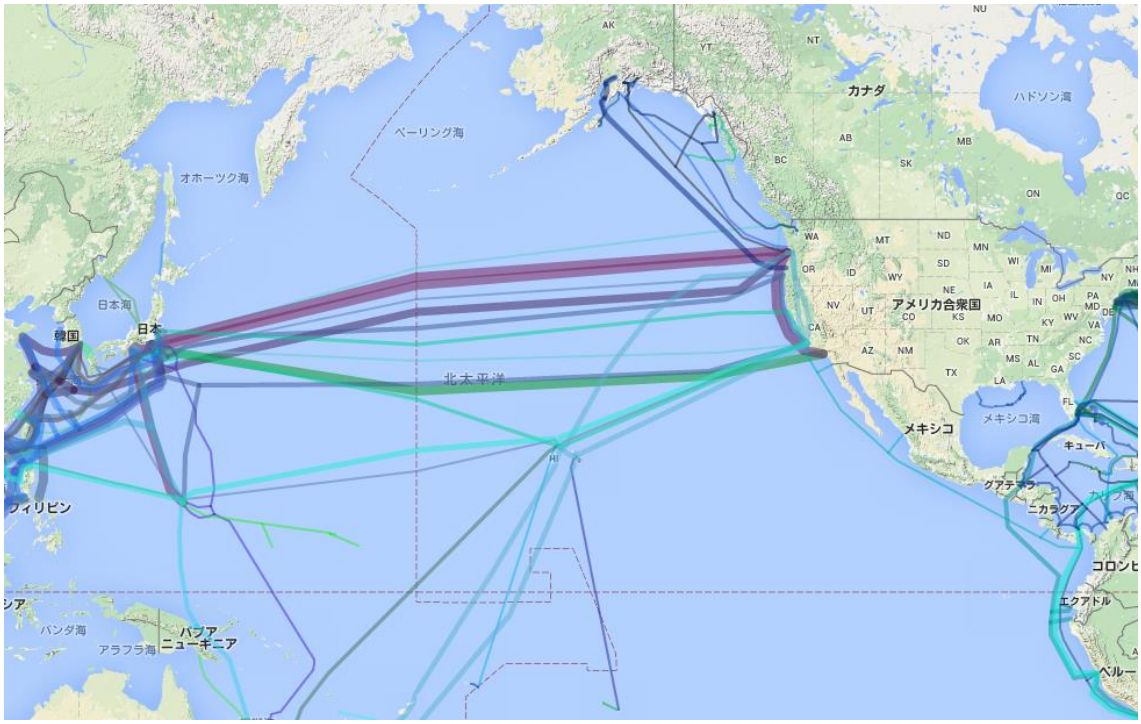

図 1：日米間の海底ケーブル

出所：Greg's Cable Map <http://www.cablemap.info/>

民間企業が保有しているために、海底ケーブルに関わる設備を自衛隊や米軍が 24 時間防衛することは難しい。しかし、社会的、経済的、そして軍事的な影響の大きさから海底ケ

ーブルは戦略的な攻撃の標的になっている可能性がある[7]。人工衛星の基地局なども含めて、通信インフラストラクチャ保護のための施策の検討が必要である。

2.3. SIGINT 活動

2013 年に米国家安全保障局（NSA）の契約職員だったエドワード・スノーデン（Edward Snowden）がトップシークレット情報を暴露して以来、米国の NSA や英国の政府通信本部（GCHQ）は批判の的になってきた。しかしながら、日本政府の SIGINT 能力はきわめて限定されてきた。第二次世界大戦の敗戦後、日本のインテリジェンス機関は廃止され、連合国の連合国最高司令官総司令部（GHQ）がその権限を引き継いだ。1952 年にサンフランシスコ講和条約が発効するまで、ダグラス・M・マッカーサー（Douglas M. MacArthur）司令官の下、チャールズ・A・ウィロビー（Charles A. Willoughby）准将が日本におけるインテリジェンス活動を掌握した。

講和条約成立の少し前、吉田茂首相の秘書官を務めていた村井順が日本のインテリジェンス活動を再構築する考えを抱いていた[8]。彼は、吉田首相および緒方竹虎副首相とともに日本版 CIA（Central Intelligence Agency）を組織しようとした。しかし、後に吉田と緒方が仲違いしてしまう。村井の計画は政治的な争いのために完全には実現されなかった。村井は調査局（現在の内閣情報調査室）のトップになるが、その能力は限定的なものになった。今日の日本の HUMINT（Human Intelligence）活動は、内閣情報調査室の他、公安調査庁、警察庁警備局などによってカバーされているが、HUMINT のスケールは日本経済や人口の規模に合致しているとはいいがたい。

冷戦終了後の 1998 年、北朝鮮が日本列島を横切る形でテポドン・ミサイルを発射した。この出来事は、日本が IMINT（Imagery Intelligence）活動のためにスパイ衛星を持つべきだとする議論のきっかけとなった。日本はそれまで IMINT においては米国に依存していた。いついかなる時でも北朝鮮を監視するというニーズは、衛星の展開要求を加速させたが、日本政府の方針では宇宙の軍事利用は認められていなかった。そこで、政府は、多目的の情報収集衛星を打ち上げた[9]。

---

[7] David E. Sanger and Eric Schmitt, “Russian Ships Near Data Cables Are Too Close for U.S. Comfort,” *New York Times* <http://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html>, October 25, 2015.

[8] 松本清張「内閣調査室論」『松本清張全集 31』文藝春秋、1973 年、483～498 頁。吉田則昭『緒方竹虎と CIA―アメリカ公文書が語る保守政治家の実像―』平凡社新書、2012 年。

[9] 春原剛『誕生 国産スパイ衛星 独自情報網と日米同盟』日本経済新聞社、2005 年。

日本のインテリジェンス活動で最後にかけているパートは SIGINT である[10]。日本国憲法第 21 条は通信の秘密を保護している。第二次世界大戦の終結後、政府、郵政省、通信事業者は法的な規制を厳しく守ってきた。通信分野においては、電気通信事業法第 4 条もまた通信の秘密を厳しく保護している[11]。

1999 年、国会は犯罪捜査のための通信傍受に関する法律を可決させたが、その活用は組織犯罪や麻薬取引といった深刻な犯罪に限定されている。同法は、法執行機関が令状に基づいて通信を傍受することを認めている。しかし、同法があっても、通信事業者依然として法執行機関への協力に躊躇している。現在でも通信傍受は年間数十件であり[12]、携帯電話に限定されている。通信傍受の規模は英米といった諸外国と比べて非常に小さい。

インターネットにおける SIGINT 能力の欠如は、サイバーセキュリティという点では深刻になりつつある。SIGINT 能力は物理的なテロや戦争、そのほかの外交的なサプライズを防止するために使われてきた。しかし、今日ではサイバー攻撃を防止したり、隠密に行われるサイバー作戦を検知したりするために使われている。それなくしては、サイバー・インシデントに絡むアトリビューション問題を解決するのはきわめて難しい。

2015 年サイバーセキュリティ戦略[13]は、「通信の秘密」に直接的には触れていないが、深刻なサイバー作戦やサイバー攻撃を予見する能力を持つ点については重視している。

3. おわりに

高い壁を作りその後に隠れるよりも、他にやるべきことがサイバーセキュリティにはある。相互接続された社会の価値は、自由な情報の流通からもたらされる。悪玉ハッカーたちは要塞のほんの小さな穴を見つけ出し、そこから侵入し情報を盗み出していくため、完璧な防衛システムは存在しない。

2015 年のサイバーセキュリティ戦略で求められているように、まずは政府と民間の両方

---

10 日本周辺の、特に外国発信の通信の傍受は合法的に可能であり、防衛省のインテリジェンス機関である情報本部等で行われている。しかし、国内の有線通信においては厳しく法的な規制かかけられている。

11 林紘一郎「サイバーセキュリティと通信の秘密」土屋大洋監修『仮想戦争の終わり―サイバー戦争とセキュリティ―』KADOKAWA、2014 年、第 5 章。

12 2013 年は 12 事案について 64 件の請求があった。法務省「平成 25 年中の通信傍受の実施状況等に関する公表」法務省<http://www.moj.go.jp/keiji1/keiji11_00007.html>、2014 年 2 月 7 日。

13 内閣サイバーセキュリティセンター「サイバーセキュリティ戦略」内閣サイバーセキュリティセンター<http://www.nisc.go.jp/active/kihon/pdf/cs-senryaku.pdf>、2015 年 9 月 4 日。

で働く高度な能力を持つ人材の育成に努め、情報共有のためにセクショナリズムを廃し、個人レベルでも組織レベルでも協力関係を結ばなければならない。それは日米関係においても同じである。

日米間においては、「日米サイバー対話」および「インターネットエコノミーに関する日米政策協力対話」という正式な枠組みがある。2015 年 4 月、安倍晋三首相がバラック・オバマ大統領と会談した際の日米共同ビジョン声明では、「情報の自由な流通に基づくサイバー空間の安全で安定した利用及び開かれたインターネットを確かなものとする」と述べられた[14]。

2020 年の東京オリンピックを控え、サイバー攻撃の影響を考えないわけにはいかない。この分野における日米協力の強化は、短期的にオリンピックの成功に資するだけでなく、長期的にグローバルなサイバースペースのセキュリティを向上させることにもなるだろう。

14 外務省「日米共同ビジョン声明」外務省 <http://www.mofa.go.jp/mofaj/na/na1/us/page3_001203.html>、2015 年 4 月 28 日（2016 年 2 月 4 日アクセス）。