総務省 学術雑誌『情報通信政策研究』 第５巻第２号
Journal of Information and Communications Policy Vol.5 No.2

調査研究ノート（査読付）

我が国のサイバーセキュリティ戦略の欠点と展望
―「平和国家」体制の桎梏への対応を考える

松村昌廣 [1]

要　旨

近年、我が国政府のサイバーセキュリティ政策に対する取り組みは、一見かなり充実してきた様相を呈している。しかし、日本国内の専門家の評価は全く逆の非常に否定的な評価が顕著である。なぜか。

本研究は先ず米国のサイバー政策における主要な戦略概念をその変移の背景、長短そして含意を焦点に分析した。次に、日本が米国と政策連携・協調を行う上で制約条件となる既存の日本のサイバーセキュリティ戦略・体制の特徴を分析した。最後に、そうした特徴と日本のサイバーセキュリティ政策における展望と施策を踏まえて、サイバーセキュリティとその領域を横断する総合的な政策提言を行った。

本研究の結果、我が国のサイバーセキュリティ体制・戦略が長年の努力にも拘わらず、日本国憲法による「平和国家」体制の下、非常に歪な形で形成されてきた現状が明らかになった。戦略・政策文書は充実してはいるが、縦割り行政の克服や抑止力の保有・行使の点で、かなり未発達な状態に陥ったままである。もちろん、根本的な解決は改憲を含む「ビックバン」によって可能だとは予見できるが、その実現は軍事安全保障・防衛における集団的自衛権に基づく武力行使と同様、非常に困難である。

従って、今後のサイバーセキュリティ政策は既存の体制・組織を前提に漸進的に改善・強化していかざるを得ない。具体的には、内閣サイバーセキュリティ・センター（NISC）を危機管理権限、組織、人員・能力の点で強化しつつ、「サイバーセキュリティ庁」の実現を模索する一方 、サイバー攻撃の阻止やその被害を限定する拒否的抑止を強化することになる。ただ、サイバー攻撃による懲罰的抑止は行わず、その代わり、米国の「サイバーの傘」の下に入り、その有効性を高めるよう対米政策連携・協力を推進することになるだろう。

今後の日本のサイバー戦略は、情報通信機器・システムと情報通信ネットワークに関するサイバーセキュリティ政策では、米国その他の主要同盟国の動向に立ち遅れないように努力する一方、法執行や外交など非サイバー政策手段を総動員して総合的な取り組みを行うことが最も望ましい。特に、依然我が国が部分的に比較優位を保持する半導体や通信機器等、サイバー関連のハードウェアの技術や生産を通じてサイバーセキュリティを強化し、この分野におけるパワーと影響力を高めることが望まれる。

キーワード：サイバーセキュリティ、NISC 体制、抑止と報復、
サイバーセキュリティ庁構想、サイバーの傘

[1] 桃山学院大学法学部教授（国際政治学・国家安全保障論）

１．序論 ― 問題の設定と分析アプローチ

近年、我が国政府のサイバーセキュリティ政策に対する取り組みは、一見かなり充実してきた様相を呈している。長年の取り組み、とりわけサイバーセキュリティ基本法の制定（2014 年 11 月）、内閣サイバーセキュリティセンター（NISC）の設置（2015 年 1 月）、「サイバーセキュリティ戦略」の策定・改定（2015 年及び 2018 年）、更には充実した具体的方針・政策文書及び評価書・関連資料等は主要国と比しても遜色がない。実際、今のところ、管見では最も詳細且つ体系的に従来の日本の施策を調査・分析した中国の研究者、韓寧『日本網絡安全戦略研究』（北京：時事出版社、2017 年）は日本の施策を非常に高く評価し、警戒の念さえ表明している。

しかし、日本国内の専門家の評価は全く逆の非常に否定的な評価が顕著である。2018 年 10 月、笹川平和財団の政策提言書『日本にサイバーセキュリティ庁の創設を！』は米英独仏日の主要 5 カ国のサイバーセキュリティ政策について詳細な比較分析を行った結果、体制整備、法整備そして産業育成・人材育成の全てにおいて、我が国が極めて脆弱な状態にあると評価した[2]。さらに、伊東寛、土屋大洋、山田敏弘、渡部悦和等による著作でも一様に同様の非常に低い評価を下している[3]。

こうした状況に陥った日本のサイバーセキュリティ政策はその総合的国力や議院内閣制を考えると、欧州主要国（特に、英国）の事例の方がより参考になる点も多いと思われるが、周知のように、覇権国であり我が国にとって唯一の同盟国である米国との関係が最も深いことから、この分野においても米国の圧倒的な影響を受けて来たのではないかと思われる。

実際、日米両政府は 2010 年から毎年 1 回開催され、2020 年で第 11 回目となった「インターネット・エコノミーに関する日米政策協力対話」局長級会合を通じて、米国主導の下、民生分野に主眼を置いて、インターネット通信のセキュリティに関する具体的施策を協議して政策連携を深めてきた。他方、従来から日米安保条約体制の下、日米安全保障協議委員会（所謂、2＋2）を通じて、米国主導で安全保障問題を協議してきたところ、2013 年の共同発表により「日米サイバー対話」を定例化し、サイバー分野での連携・協力の方針を明示した上で、日米サイバー防衛政策作業部会（Cyber Defense Policy Working Group: CDPWG）を設けた。その後、原則的に毎年、「日米サイバー対話」は開催され、日本はサイバーセキュリティ政策上の具体的な取り組みを強化してきた。

さらに 2020 年、日本はオンラインで開催された、米国主導のファイブアイズ（米英加豪新のアングロサクソン 5 カ国による通信傍受・諜報同盟）[4]国防大臣会合（Five Country

---

[2] 自由民主党は安倍政権に「サイバーセキュリティ庁」の創設を提言した。「サイバーセキュリティ庁創設を首相に提言 自民」、『NHK 政治マガジン』、2019 年 5 月 14 日、https://www.nhk.or.jp/politics/articles/statement/17565.html。

[3] 例えば、伊東寛『「第 5 の戦場」－ サイバー戦の脅威』祥伝社新書、2012 年、第 5 章。土屋大洋『サイバーセキュリティと国際政治』千倉書房、2015 年、194 頁～204 頁。山田敏弘『サイバー戦争の今』ベスト新書、2020 年、第 8 章。渡部悦和『自衛隊が中国人民解放軍に敗北する！？』扶桑社、2020 年、220 頁～299 頁。

[4] ファイブアイズに関しては、松村昌廣『軍事技術覇権と日本の防衛 － 標準化による米国の攻勢』芦書房、2008 年、第 9 章。なお、高い通信傍受能力を有する機関は当然サイバーセキュリティ対策の中心になっている。この点に関して、茂田忠良「サイバーセキュリティとシギント機関 ― NSA 他の UKUSA 諸機関の取り組み」『情報セキュリティ総合科

Ministerial）に参加するとともに、「送受信両者間の暗号化と治安に関する共同声明」に加わった[5]。こうした経緯と背景を踏まえれば、日本はこの約十年間、多くの国々とサイバー分野での二国間協議・対話等を行って来たとはいえ、[6]日本のサイバーセキュリティ戦略・政策は多分に米国の強い影響力を受けて形成されて来たと言えるだろう。

したがって、本研究の目的はますます厳しくなる国際安全保障環境の中、米国覇権の下、日米同盟における両国間の著しく非対称的な力関係に如何に上手く対処すれば、日本が自国の安全を保障できるのかを、サイバー分野で模索することにあり、決してサイバー超大国である米国との比較において、日本のサイバーセキュリティ政策の優劣を論じることにはない。逆に、本研究が英独仏その他の主要国との比較分析に関心がないのは、日本が二国間同盟を介して覇権国である米国に国家安全保障の点で全く依存している一方、英独仏はＮＡＴＯの多国間同盟の枠組みを有しており、基本的な存在条件を全く異にしているからである。また、シンガポール、韓国、台湾などは、日本と比して米国の世界戦略における位置付けや重要性の点でかなり劣位にあることから、これまた基本的な存在条件を全く異にしている。したがって、これらの国々との比較分析から日本にとってサイバー政策における個別分野の具体的施策で参考になる教訓を引き出すことは多分にあり得るとしても、基本戦略の次元では参考にはならないと判断した。要するに、本研究は国際権力政治の厳しい現実を前提に国策としてのサイバー戦略の基本方針の在り方を探求しているのであって、主要国のケースとの比較分析を通じて各論レベルで様々な教訓を汲み上げて、漸進的に政策面で改善していくことに全く関心はない。重ねて言えば、本論で米国を比較対象としているのは、そこから何らかの知見を得て政策面で改善したいという動機付けに基づいているのではなく、或る意味で頼りになるが、同時に大変困った存在である米国に如何に対処すればよいのかを模索せざるを得ないとの認識に基づいている。

そこで先ず本稿では、米国のサイバー政策における主要な戦略概念をその変移の背景、長短そして含意を焦点に考察する。次に、日米政策連携・協調において制約条件となる既存の日本のサイバーセキュリティ戦略・体制の特徴を分析する。最後に、日本の抱える問題と課題を踏まえて、サイバーセキュリティ政策における展望と施策、そして他の政策領域を横断する総合的な基本政策方針を提言する[7]。

付言すれば、本研究はサイバーセキュリティ戦略における日米同盟関係の枢要性を踏まえ、抑止論とそのサイバー分野への適応、抑止論を軸にした米国のサイバー戦略の展開とサイバー政策体制・組織改編を分析・考察して、その後、その変化に対応せざるを得ない日本の実態と具体的政策課題の指摘に関する分析・論述に繋げている。つまり、そうした限定的

学』第 11 号、2019 年 11 月。

[5] Five Country Ministerial, “International Statement: End-To-End Encryption And Public Safety,” October 20, 2020, https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety.

[6] 外務省、「日本のサイバー分野での外交　二国間協議・対話等」、2020 年 1 月 30 日、https://www.mofa.go.jp/mofaj/fp/nsp/page24_000687.html。

[7] つまり、本研究は政治指導者や当該政策担当者に有効な課題解決方針・方法を提示することを目的とする政策提言論文であり、政策問題/課題の提示、その背景その他必要な経緯の説明、分析の枠組み（用いられる主要な分析概念や理論）、可能な政策選択肢の提示、妥当な選択基準とそれに基づくと特定の選択の推奨から構成される。

な目的のため、本研究は日米サイバー戦略・政策連携を進めて行く上で、米国の戦略的視点から主要な障害になる課題のみを取り上げる。従って、本研究はそうしたアプローチで従来繰り返し指摘されてきた「平和国家」体制の桎梏が課す制約や既に断片的に存在する部分的な分析や提言を総合して、我が国のサイバーセキュリティ政策の基本的な方向性やその概括的な内容を提言するところに特徴がある。

２．米国のサイバー戦略における主要戦略概念の変移 ― 拒否的抑止（積極防衛）から懲罰的抑止（報復能力保持）へ[8]

２．１．従来の欠点・弱点と 2018 年度版「国家サイバー戦略」の意義

トランプ政権が 2018 年に公表した「国家サイバー戦略（National Cyber Strategy: NCS）」は、それまで国防、国土安全保障その他連邦政府の情報システム、重要インフラ、サイバー犯罪、事案報告、人材育成、国際政策等の分野別、所管官庁の縦割りでなされてきた戦略・施策の策定を、事実上初めて総合的に整理して提示した[9]。さらに、同戦略は 2017 年に同政権が公表した上位戦略文書である「国家安全保障戦略（NSS）」で重要政策概念として言及した「（サイバー領域における）抑止」をやや詳細に説明して、その後に次々と策定された分野別の下位戦略・政策文書の基礎となった。特に、従来使用されてきた「サイバーセキュリティ戦略」が「サイバー戦略」に取って代わられたことは、以下で述べるように基本的な発想が拒否的抑止（積極防衛）から懲罰的抑止（報復能力の保持と行使）に重点が移ったことを端的に示している。この点、トランプ政権は様々な政策分野において従来の路線を踏襲せず、大きく逸脱・変更したが、NCS-2018 はこれまでの経緯と知的蓄積を十分踏まえた上で、劇的に脅威が強まった新たな状況に対応すべく策定されたと言える。

こうした変化は、G.W.ブッシュ、オバマ両政権が 2001 年の同時多発テロ以後、国際テロリズムの脅威に対処するために採った戦略・政策を踏まえている。

具体的には、2003 年、G.W.ブッシュ政権はサイバー攻撃への防衛を念頭に国土安全保障省主導で「サイバースペースの安全確保のための国家戦略（National Strategy to Secure Cyberspace）」を公表し、これに実効性を持たせるため、2008 年、二つの大統領令（NSPD-54/HSPD-23）を発して「包括的国家サイバーセキュリティ政策（Comprehensive National Cybersecurity Initiative）」を策定した。その結果、連邦政府の情報通信ネットワークと関連施策の防御方針が具体的に設定されたものの、重要インフラ等、民間部門のサイバーセキュリティには言及されなかった。

---

[8] 本論では、伝統的な抑止論に沿って、①消極的抑止（passive deterrence）、②積極的抑止（active defense）又は拒否的抑止（deterrence by denial）、③懲罰的抑止（deterrence of punishment）を用いている。アクティブ・サイバー・ディフェンス（Active Cyber Defense: ACD）は②の分類に属する概念であり、「高度なサイバー攻撃を探知し防御する」ことである。” Active Cyber Defense (ACD)”, National Security Agency Central Security Service, https://apps.nsa.gov/iad/programs/iad-initiatives/active-cyber-defense.cfm.

[9] 情報通信機器・システムと情報通信ネットワークに関するサイバーセキュリティ戦略文書は 2003 年に初めて発行された。https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/UnitedStates_2003_cyberspace_strategy.pdf。

オバマ政権は NSS-2010 と NSS-2015 でサイバーセキュリティの重要性に言及し、その下位戦略として、2011 年の「(国防総省) サイバー空間作戦戦略 (DoD Defense Strategy for Operating in Cyberspace)」を踏まえた 2015 年の「(国防総省) サイバー戦略 (DoD-CSS)」を策定したが、抑止を作用させるための反撃に関する作戦ドクトリン・理論の整備や実践に言及しなかったために、実質的には従前のサイバー防衛 (拒否的抑止/積極防衛) に徹する結果を生むものであった[10]。実際、サイバー反撃には依然として 2013 年にオバマが発した大統領政策指令 (PPD) 20 に則り大統領の許可が必要であり、サイバー攻撃が一見明白に戦争や武力紛争の一部を構成する場合以外、自衛権の行使としてサイバー反撃を行なうことはできなかった。つまり、そのレベルに満たない、圧倒的多数の深刻なサイバー攻撃には、迅速に大統領からの許可を確保できないことから、対処できないままであった。

従って、2018 年度「国家サイバー戦略」と「(国防総省) サイバー戦略」が中国、ロシア、北朝鮮、イラン、その他非国家行為主体を対象とするサイバー攻撃と抑止重視を強調したことは画期的であった。また、下位文書として、サイバー・コマンドが指揮ビジョン文書[11]を策定し、相手方の情報通信システムに入り込んで未然に攻撃を防ぐ (defend forward : 前進防衛) こと、さらに常時、サイバー反撃を行う態勢を維持すること (「継続的従事 (persistent engagement)」戦略) を基本方針としたことは注目に値する[12]。これに実効性を与えるため、トランプ大統領は安全保障政策覚書 (NSPM) 13 を発して、従来必ず大統領の承認がなければサイバー攻撃をできなかったところ、迅速に対処しなければならない状況では一定の手続きと制約条件の下で国防長官に発動権限を与え、サイバー・コマンド司令官に作戦指揮権を付与した[13]。つまり、死者、施設破壊、重大な経済インパクトがなければ、国家安全保障会議の協議や関係省庁との調整を経ることなく、迅速にハッキングや敵の攻撃システムへの攻撃を行えることとなった[14]。

---

[10] Jeffrey L. Caton, *Evaluation of the 2015 DOD Cyber Strategy: Mild Progress in a Complex and Dynamic Military Domain,* U.S. Army War College, 2017.

[11] "Achieve and Maintain Cyberspace Superiority: Command Vision for the U.S. Cyber Command," 2018.

[12] "An Interview with Paul M. Nakasone," *Joint Force Quarterly,* 1st Quarter, 2019; Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Ibid.*

[13] 現時点では、NSPM13 は秘密指定されているが、その主要な内容は以下の文献から分かる。Paul C. Ney, Jr, DOD General Counsel Remarks at U.S. Cyber Command Legal Conference, March 2, 2020, https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/; Mark Pomerleau, "CYBERCOM: New authorities mean lots of new missions at Cyber Command," *Fifth Domain,* May 8 ,2019, https://www.fifthdomain.com/dod/cybercom/2019/05/08/new-authorities-mean-lots-of-new-missions-at-cyber-command/; and, Mark Pomerleau, "Defense officials taking advantage of new cyber authorities, " *Fifth Domain,* November 27, 2018, https://www.fifthdomain.com/dod/cybercom/2018/11/27/defense-officials-taking-advantage-of-new-cyber-authorities/.

[14] 茂田、前掲、81 頁。Ellen Nakashima、"White House authorizes 'offensive cyber operations' to deter foreign adversaries", *Washington Post,* September 21, 2018, https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html.

組織・能力面でも、サイバー・コマンドはこの 10 年間で顕著に強化されてきた[15]。従来、戦略軍の下位の統合部隊であったが、2010 年には独立した統合コマンドとなり、直属の部隊と陸海空軍・海兵隊のサイバー・コマンド関連部隊から構成される[16]。サイバー・コマンドは未だ独立した軍種ではないが、直属分だけでも要員 6200 人とサイバー任務部隊（Cyber Mission Force: CMF）133 個チームを有する。また、陸海空軍・海兵隊のサイバー・コマンドとその隷下部隊が擁する要員を加えると、膨大な数となる。その内訳は、①広範なサイバー攻撃に対処する国家的任務チーム 13 個、②最重要の国防総省通信情報ネットワークとシステムを主要な脅威から防衛するサイバー防衛チーム 68 個、③作戦計画や有事の作戦を支援するために組織化されたサイバー攻撃を行うサイバー支援チーム 27 個、④分析・計画支援を②と③の両チームに与えるサイバー支援チーム 25 個、となっている[17]。米国に対する武力攻撃は多分に重要インフラへのサイバー攻撃と並行して或いは時間的に前後して組み合わせて行われるであろうから、防御・攻撃双方の手段を用いた重要インフラの防衛も任務に含まれる[18]。

重要インフラ等の民間部門に対しては、2018 年、トランプ政権は国土安全保障省の国家防衛・プログラム局（National Protection and Programs Directorate: NPPD)を発展的に解消して、外局としてサイバーセキュリティ・インフラセキュリティ庁（Cybersecurity & Infrastructure Security Agency: CISA）を設置した。同庁は連邦政府と重要インフラの情報通信システムのサイバーセキュリティ、官民の全てとの関連事項に関する連絡調整、危機対応、調査研究、そしてこれらのための利害関係者との関与・ネットワーク形成（stake-holder engagement）を行う組織と人員を擁するだけでなく、同庁設置法により官民の全てより必要な情報を収集する権限を有する。つまり、米国において軍事分野を除くサイバーセ

---

15 コマンド（command）は指揮官と幕僚から成る指揮組織と下級部隊から成る。したがって、ここではサイバー司令部或いはサイバー軍と訳すと不正確になるので、サイバー・コマンドと表記する。

16 具体的には、サイバー・コマンド司令官が国防総省情報ネットワーク（DoD Information Network: DoDIN）司令官/国防情報システム庁（Defense Information System Agency: DISA）長官兼務を経由して実行する。”Norton passes command of JFHQ-DODIN and directorship of DISA to Skinner,” US Cyber Command, March 1,2021, https://www.cybercom.mil/Media/News/Article/2520043/norton-passes-command-of-jfhq-dodin-and-directorship-of-disa-to-skinner/.

17 U.S. DoD Defense Cyber Strategy, 2015, p. 6 ; U.S. Cyber Command Public Affairs, “Cyber Mission Force achieves Full Operational Capability,” May 18, 2018, https://www.cybercom.mil/Media/News/News-Display/Article/1524492/cyber-mission-force-achieves-full-operational-capability/; “United States Cybersecurity Policy and Threats”, Hearing before the Committee on Armed Services, September 29, 2015, https://www.govinfo.gov/content/pkg/CHRG-114shrg22270/html/CHRG-114shrg22270.htm.

18 サイバー空間における攻撃任務を明記した文書は稀であるが、例えば、米海軍艦隊サイバー・コマンド（Fleet Cyber Command）の「サイバー攻撃活動 63」にその片鱗は窺える。Winter Griffith, “Commander of Cyber Strike Activity 63 Reflects on Her Career and Women’s History Month,” *CHIPS: The Department of the Navy Information Technology Magazine,* April 3, 2018, https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=10196.

キュリティの一般主務官庁は国土安全保障省であり、その具体的担い手が同庁である。

なお、これまでのところ、発足して間もないバイデン政権は基本的にトランプ政権のサイバー戦略を踏襲しており、本研究で取り上げるべきものはない[19]。

したがって、この分野で日本が対米政策連携・協調を行っていくには、こうした米国のサイバー戦略・政策における基本方針と体制の大きな変化がどのような前提、発想、理論に基づいているのか、またそこに陥穽はないのかについて把握しなければならない。

２．２．概念整理と理論的背景

２．２．１．サイバー空間の特徴

コンピューター機器のネットワークにより形成されるサイバー空間は物理的な現実世界にはない独特の特徴を有しており、有効なサイバー政策の策定を難しくしている。

第一の特徴は、サイバー空間へ入ることは、パソコン（端末機器）から回線を用いてサイバー空間へアクセスするだけであり、従来の兵器の操作と比して、極めて簡単且つ安価であり、非常に容易である。つまり、軍事安全保障・防衛分野では、高価な兵器を大量に保有する必要がある。また、兵器はある種の特注品であるのに対して、サイバー機器は殆ど民生品である上、操作員に対する教育が一般的な民間でのスキルと余り変わらない、つまり、民間のハッカーを利用すると安くつく。さらに言えば、このことは、戦争行為が従来の専用の高価な兵器を用いるプロの兵士だけでなく、安価なパソコンを駆使するハッカーその他民間人によって可能となったことを意味する。

第二には、攻撃者がその発信元 IP アドレスを偽造し、事実上、匿名とできるため、それを特定するのは容易ではない。また、仮にそこまで辿れたとしても、その端末の物理的所在を探し出すのは容易ではない。確かに、通常はログ（利用・データ更新の記録）により使用端末までは辿り着けることもあるが、それが乗っ取られた踏み台端末（所謂、ボットネット

---

19 バイデン政権は未だ「国家安全保障戦略（NSS)」も「国家サイバー戦略」も策定しておらず、戦略レベルで言及すべき点はない。確かに、2021 年 3 月には「暫定国家安全保障戦略（Interim National Security Strategic Guidance)」を策定したが、サイバー戦略分野に関しては、基本的にトランプ政権の戦略を踏襲している。これに関しては、Herb Lin, “How Biden’s Cyber Strategy Echoes Trump’s”, *Lawfare*, March 10, 2021, https://www.lawfareblog.com/how-bidens-cyber-strategy-echoes-trumps.

さらに、2021 年 5 月、米国のコロニアル・パイプライン社のシステムがロシアのハッカー集団から大規模なサイバー攻撃を被った際、バイデン政権は米サイバー・コマンドによる反撃を加えたと思われる。これは、同政権がトランプ前政権による『国家サイバー戦略（2018 年)』を踏襲していることを反映している。これに関しては、David E. Sanger and Nicole Perlroth, “Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity”, *New York Times*, June 8 ,2021, https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html.

さらに言えば、2021 年 5 月、バイデン政権は大統領令（Executive Order）14208「国家のサイバーセキュリティの向上」を策定したが、これは「国家サイバー戦略」（2018 年）及びその他トランプ政権時代迄の下位戦略・政策を具体化する施策方針であるから、戦略次元の分析・考察を行う本研究で詳説する必要はない。
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[botnet]による遠隔操作）である場合は、容易に真の攻撃者の端末は判明しない。特に、攻撃者が複数の踏み台端末を経由した場合には、一層困難になる。付言すれば、ログを見てパケットの発信元 IP アドレスを確認しても、それが虚偽のものに書き換えて送信されていれば、攻撃者 IP アドレスを特定することはできない。さらに、攻撃が The Onion Router（Tor）などの匿名通信システムを利用してなされた場合には、攻撃者 IP アドレスを特定するのは極めて困難となる [20]。

第三には、仮想空間であるサイバー空間自体には、排他的管轄権（主権）を行使して取り締まる主体はいないし、定義上、その主体と締結する国際条約も存在しない [21]。そのため、取り締まりは攻撃者が居る国家の当局によるものとならざるを得ないが、取り締まる意志或いは能力がない場合、特にその国家自身が直接に攻撃に従事していたり、攻撃を支持したりしている場合には、取り締まる術はなくなる。その結果、どのように対処するかは国際法の合法性や国際政治の利害得失の点で非常に厄介な問題となる。それを回避しようとすれば、明白な戦争や武力行使の一環としてなされるようなサイバー攻撃以外は、容易には強力なサイバー反撃や経済・武力報復に訴えることはできず、結果的に泣き寝入りすることになりがちである。つまり、一般論としては、サイバー攻撃は現実世界の武力行使へエスカレートしにくい。[22]

第四には、サイバー空間はコンピューター通信ネットワークによって相互に繋がり、常時接続している必要がある。その結果、攻撃は任意の手法でいつでも好きな時に実行できるのに対して、防御 [23]はそれに対してあらゆる場所で常に備えていなければならないため、相対的に多大な費用、人員とエネルギーを要する。つまり、費用対効果の点から、攻撃側が防御側に対して非常に優位にある。

２．２．２．サイバー事案の尺度・分類と対応責任・危機対処段階

ここまで、曖昧に「サイバー攻撃」と表記してきたが、有効なサイバー戦略・政策を策定するには、その規模や烈度によって事態を分類した上で、各々の条件に則して対処する必要がある。バンクス氏が、米国の国土安全保障省の下に置かれた連邦緊急事態管理庁（FEMA）が天災等の緊急事態への対処する長年に亘る経験に基づいた分類に準じて整理したのが

---

[20] このような場合でも、一般に警察の捜査手法や諜報機関の分析手法として知られるプロファイリング手法を使うことにより真の攻撃者を推定することは一定程度可能ではある。

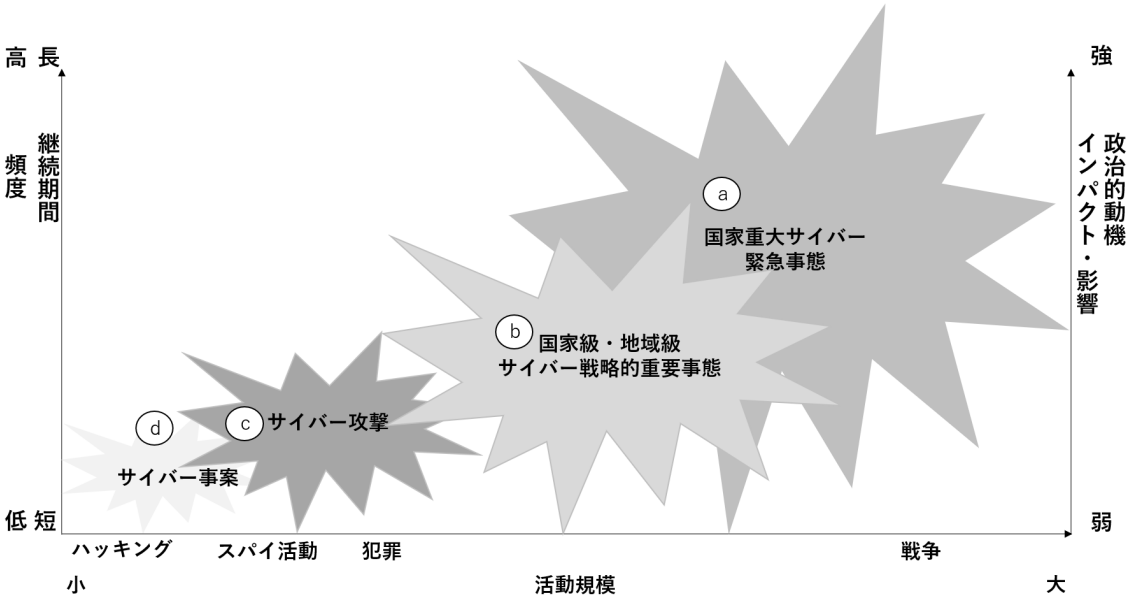
[21] とはいえ、サイバー空間を物理的に形成しているのは、個々の機器・機材、海底ケーブルであり、これらとその所有者には、所在国の国家主権や管轄権は及ぶ。ブダペスト条約は規制対象にサイバー犯罪に限定し、特定の締約国間で有効である。この他、法的拘束力の有無が確認されないが、中露間には何らかのサイバー攻撃を禁止する合意或いは申し合わせがあると思われる。Olga Razumovskaya, “Russia and China Pledge Not to Hack Each Other, *Wall Street Journal*, May 11, https://www.wsj.com/articles/BL-DGB-41673.

[22] Thomas Rid, “Cyber War Will Not Take Place” *Journal of Strategic Studies,* Vol. 35, No. 1, 2012.

[23] 一般に、サイバー上の防御は、①攻撃に対する予防、②攻撃の探知、③攻撃の阻止、④被害システムの復旧、⑤反撃、に準備せねばならない。②③に関しては、少なくとも、侵入検知システム（Intrusion Detection System: IDS）やファイアウォールが必要であるが、高度なサイバー攻撃には、バックアップ/無停止システム、独自の通信プロトコール/データ形式、高度な暗号の技術の利用、が必要となる。伊東寛、前掲書、92 頁～93 頁。

「図１：悪意あるサイバー活動（Cyber-enabled Malicious Activity: CEMA）の等級」である[24]。つまり、規模、継続期間/頻度、影響力/効果/政治的動機付けを、程度の高いものから低いものへ、ⓐ国家重大サイバー緊急事態（Cyber Incident of National Significance: CINS）、ⓑ国家級・地域級戦略的重要サイバー事態(National or Regionally Strategically Momentous CEMA)、Ⓒサイバー攻撃(Cyber Attack)、ⓓサイバー事案（Cyber Incident)となっている。ⓐ～ⓓ は連続的であり、前後の分類と多分に重複するが、少なくとも概念的に峻別できる。ⓐが昂じて、現実の物理的世界の武力行使と一体化すれば、戦争に分類できるだろう。ⓐでは、サイバー・コマンドにより、攻撃者の情報システムに対してサイバー攻

図１：悪意あるサイバー活動の等級



（出典）Ronald Banks, *Confronting the Cyber Storm; A Coercive Cyber Strategy to Defend the Nation,* independently published through Amazon.co.jp. 2020, p.39、を一部修正

撃がなされる。さらに昂じて戦争となれば、サイバー攻撃は武力攻撃と一体化して[25]、人の殺傷や物理的破壊を含むものとなる。ⓑは国土安全保障の観点からサイバーセキュリティ・インフラセキュリティ庁（CISA）が対処するが、ⓐに近づけば、当然、サイバー・コマンドとの連絡・調整から連携・協力に移行することになる。Ⓒは程度の低いものは情報システムやデータ情報に対するスパイ活動であり、さらに昂じれば対象情報システムの機能妨害

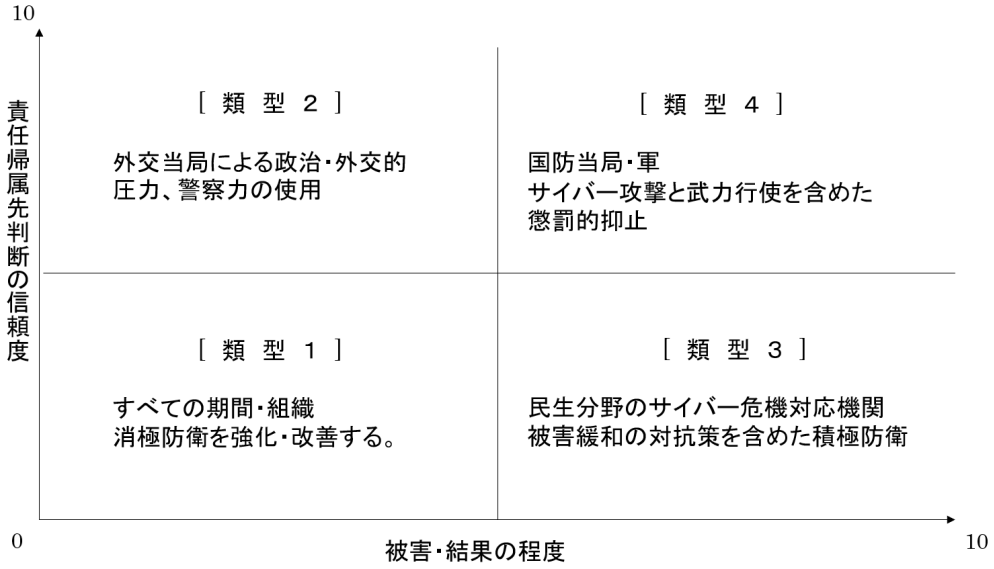
[24] Ronald Banks, *Confronting the Cyber Storm: A Coercive Cyber Strategy to Defend the Nation,* on-demand publication by Amazon.co.jp, 2020, p.39.

[25] より正確に言えば、サイバー攻撃が実空間での侵略国の武力行使と同時並行的に一体化する状況、或いは時間軸で武力行使と前後し、一体化する状況など、日米安保条約第５条事態に当て嵌まる場合がある一方、実空間での武力行使その他武力行使と同程度の人的・物理的被害を伴わず、第５条事態に当て嵌まらない場合がある。この点は、「図１：悪意あるサイバー活動の等級」により明らかである。例えば、この峻別は尖閣有事では非常に重要であるが、「当て嵌まる」か否かについての米国による判定や、その具体的条件や手続きについて日米間の擦り合わせには今後課題が多く、日本へのサイバー攻撃に対して自動的に或いは高い確率で米国が集団自衛権を行使するわけではない。

や情報・データの窃盗等のサイバー犯罪となる。ⓓは愉快犯的なハッキング（不正アクセス）である[26]。

これを対処責任者/機関と対処様態の組み合わせに落とし込むためには、横軸に被害・結果の程度、縦軸に責任帰属先の判断に関する信頼度とする、シュワブ氏による CEMA の四類型、「図２：行為主体と責任帰属先判断」が大変役立つ[27]。現実には、ここでも容易には境
界ケースを分類できないが、少なくとも概念的には明快である。四類型に対して複数の対処方法が同時に用いられても構わないが、類型別に示された当該対処方法が最も有効である。「類型１」（図１のⓓに相当）は被害も責任帰属先判定の信頼性も低い場合で、全ての機関・組織が各自で消極防衛を強化・改善する。「類型２」（図１のⒸに相当）では、被害は限定的

図２：行為主体と責任帰属先判断



（出典）Gary Schaub, Jr., ed., *Understanding Cyber Security: Emerging Governance & Strategy,* Rowman & Littlefield International, 2018, p. 194.

であるが、責任帰属先がかなり判別できる場合であり、外交当局による政治・外交的圧力或いは警察力を用いて攻撃を止めさせる。「類型３」（図１のⓑに相当）では、各国政府の民生分野のサイバー危機対応機関（米国の場合は、国土安全保障省/CISA）が被害緩和のための対抗策を含めた積極防衛を行う。最後に、「類型４」（図１のⓐに相当）では、国防当局・軍が懲罰的抑止のためにサイバー攻撃だけではなく武力行使を含めた攻撃を行う。

---

26 サイバー危機対処に対する主体については、その緊急度によって、緑、青、黄、橙、赤の五段階に分けられる。つまり、（緑）当該事業体/組織の単体で対処→（青）情報共有など当該部門の保有するリソースで対処→（黄）法令に則り当該部門外のリソースを用いて事態の緊急度を緩和する支援→（橙）当該産業が危機対処を行うが、新たに或いは徐々に政府のサイバー危機管理組織が支援する→（赤）当該産業自身による危機対処が不可能となり、政府の危機管理組織が国家安全保障上の事態として対処する。Banks, *op.cit,* p.258.

27 Gary Schaub, Jr., ed., *Understanding Cyber Security: Emerging Governance & Strategy,* Rowman & Littlefield International, 2018, p. 194.

留意すべきは、「図 2」の四類型や「図１」の四類型が実際には連続的で密接に繋がっており、概念的にはともかく、実践的には明確に分別不可能なことである。

懲罰的抑止を利かせるには、サイバー攻撃能力を保有した上で、どこにどのようなコンピューターやコンピューター・ネットワークがあり、どのような脆弱性があるのか等、予め攻撃対象の実態を把握せねばならない。具体的に言えば、それは事前に潜在的攻撃対象のネットワークに侵入して、マルウェアを埋め込むなどして、そのシステムの仕組みを掴んでおかねばならない。さらに言えば、そうしたスパイ活動に乗じて、そのシステムの機能を低下或いは破壊するため、コンピューター・ウイルス等を埋め込んでおき、任意のタイミングで外部からの指令で作動させる状況、つまりシステム管理ソフトを乗っ取る状況にしておくことが望まれる[28]。つまり、潜在的攻撃対象に対するハッキング、スパイ活動、サイバー犯罪はサイバー手段による積極防衛や懲罰的抑止にとって不可欠である。したがって、軍のサイバー部隊は独自にサイバー・スパイ能力を保有していなければならないし、かなりの程度、諜報機関のサイバー及び非サイバー・スパイ能力に依存することとなる。また、軍だけでなくサイバー諜報機関もサイバー攻撃能力を保有することを意味する。したがって、軍と諜報機関の双方がサイバー・スパイ能力とサイバー攻撃能力を持つのであり、両者は役割・能力保有・権限分担や予算・人員保有に関して緊張や対立を生じがちとなる[29]。さらに言えば、サイバー防御能力は多分にハッキング、スパイ活動、サイバー攻撃による経験、技術、技能に裏打ちされたものであるから、両者は表裏一体であり[30]、そもそも防御に専心すること、つまり専守防衛など成り立たないと言える。

---

[28] 例えば、「中国レノボ(Lenovo)製 PC のスパイ疑惑と NEC・富士通。ThinkPad のバックドア問題とは？」、『Gadgeblo』、2021 年 4 月 21 日、https://www.gadgeblo.com/lenovo/。こうした事態が、外為法（2019 年 11 月改正）基づき、外資による IT 機器メーカーの M&A を抑制する政策を取るようになった大きな理由であろう。

とはいえ、事前にシステムの仕組みを掴んでおくことと、予め攻撃のための何かを仕込んでおくことは明確に区別すべきではあろう。国際法上、システムの仕組みを調べるスパイ行為はある程度相互に許容されているが、相手方のシステムを破壊するウイルスの仕掛けをしておくことは、発見された場合、重大な外交事案となるリスクを孕んでいる。従って、敢えてそうしたリスクを犯すか否かは政策上の決断である。

もっとも、相手側のシステムに侵入するリスクを犯さずとも、相手方のシステムの仕組みを掴むためには、調達に際しての入札で公開されているシステム要件を残らず写しとり、同様のシステムを組み上げればよい。その上で、相手方のシステムにピン（Ping）を打って返信の有無やその内容を見るだけでも何某かの情報を得ることができる。

[29] 軍と諜報機関の役割等の切り分けは国家安全保障事案か否かを巡るものとも言えよう。

[30] 日米同盟の観点から日本のサイバーセキュリティ体制の整備・強化において参照すべき重要な米国のケースでは、米サイバー・コマンド司令官と通信傍受分野の軍諜報機関である国家安全保障局（NSA）長官が兼務であること、陸海空軍・海兵隊のサイバー・コマンドが必ず諜報活動を担う情報作戦コマンド（information operation command）を隷属させていることからも明らかである。Griffith, *op.cit.*

もっとも、英国のサイバー情報機関である政府通信本部（Government Communications Headquarters：GCHQ）が形式的には外務省傘下の組織であることと、米国の諜報機関が第二次世界大戦時から軍の傘下にあることに鑑みると、サイバー分野での軍と諜報機関の関係は多分に歴史的な経緯に左右されると見ることもできる。

２．３．困難な責任帰属先判定（attribution）とその克服への道

サイバー分野での抑止を考える際、一般に、①攻撃の利益が抑止の費用よりも高く、攻撃に有利である、②攻撃で利益を得る蓋然性が高ければ高いほど、抑止は難しい、③防御者が攻撃者に課すコストが高ければ高いほど、抑止の蓋然性は高くなる、④この蓋然性が高いと敵対者が見做せば見做すほど、抑止の蓋然性は強くなる、と言える

とはいえ、軍事安全保障研究で発展してきた抑止論、特に核抑止論には厚い知的蓄積が存在するが、それをサイバー分野に当て嵌めるには、以下の事情からかなり注意が必要である。先ず、現実の物理的世界の軍事安全保障では、専ら兵器の数量増加による報復能力の向上によって抑止効果を高めることができるが、サイバー分野においては、ハードフェア、ソフトウェア、技術者の人員などの投入資源増によって情報システムのセキュリティを大幅に強化しようと試みても、敵対者がそれを打ち破る技術能力を持てば拒否的抑止は効かない。さらに、サイバー攻撃者がどこに存在するのかが分からなければ、報復攻撃を行うことができない一方、攻撃者が誰なのかが分からなければ、現実の物理的世界での懲罰的報復、あるいは法執行上の処罰はできない[31]。留意すべきは、国外からのサイバー攻撃において、同盟国であれば協力関係を結び捜査を続行できる一方、敵国や第三国を経由された場合、捜査は断念せざるを得ない[32]。つまり、一般論としては、サイバー攻撃は実世界の武力行使にエスカレートしにくい[33]。しかし、誤った責任帰属先判断で、無実の潜在敵対者/国や第三者に報復攻撃を行った場合、当然、相手側は先制攻撃を被ったと理解し、反撃を行う可能性が排除できない。その結果、攻撃・反撃の連鎖が一気にエスカレートするリスクを犯すことになる。その際、反撃がサイバー/電子的手段に留まらず、経済制裁、その他政治外交的な敵対行為の形を取れば、武力紛争・戦争となる可能性が大きい。最悪、反撃が核兵器その他の大量破壊兵器の指揮統制システムに対するものであったり、或いはそう受け止められたりすれば、大量破壊兵器による応酬に発展するかもしれない。

それでは、責任帰属先判定の信頼度を高めることはできるだろうか。否であれば、エスカレーションのリスクが高いために、容易には報復はできず、その結果、いくら報復能力を持っていても使えず、サイバー空間での抑止は効かないこととなる。既に言及したように、ボットネットや深層ウェブやダークネット[34]の使用のため、サイバー空間における責任帰属先判定は容易ではない。とはいえ、既に米国の軍事諜報コミュニティーが開発・実践しているように、諜報機関と協力して、攻撃のパターン分析や使用ウイルスその他のソフトウェア

---

31 Charles L. Glaser、”Deterrence of Cyber Attacks and U.S. National Security”, Report GW-CSPRI-2011-5, June 1, 2011, https://cspri.seas.gwu.edu/sites/g/files/zaxdzs1446/f/downloads/2011-5_cyber_deterrence_and_security_glaser_0.pdf.

32 国内事案であるが、こうした事案例のイメージについては、神保哲生『PC 遠隔操作事件』、光文社、2017 年。

33 Rid, *op.cit.*

34 深層ネット（Deep Web）とは、World Wide Web 上にある情報の中で、通常の検索エンジンによって収集されない情報である。ダークネット（darknet）とは特定のソフトウェア、構成、承認でのみアクセス可能な非標準の通信プロトコールとポートを用いるオーバーレイ・ネットワーク（或るコンピューター・ネットワークの上に構築された別のコンピューター・ネットワーク）である。

技術情報に加えて、知覚的、行動上の文脈を総合的に分析・理解すれば、判定の確度はかなり高まる。行動影響分析（Behavioral Influences Analysis: BIA）として知られるこの手法は、社会学、文化人類学、心理学やオペレーション・リサーチを組み合わせて、攻撃者や潜在的敵対者の動機、世界観、行動予測などを行う[35]。

２．４．評価と課題

ここまで見てきたように、米国のサイバー戦略は、同国が近年ますます高い頻度で深刻なサイバー攻撃を被るようになったことから、従来の積極防衛重視から抑止と報復の方向へ大きく舵を切った。確かに、行動影響分析によってサイバー攻撃者を誤判定するリスクをかなり減じることができるようになったが、リスクは完全に排除できる訳ではない。

敢えてこのリスクを看過するとしても、サイバー戦略の柱として抑止と報復を据えた結果、軍と民生危機管理官庁、つまりサイバー・コマンドと CISA との役割分担、特にどちらが主導し、どちらが補助するかについて、そのタイミングや移行手続きに焦点を絞って決めねばならない。しかし、既に言及したように、双方ともサイバー攻撃とサイバー諜報の能力を保有し、競合状態にあることから、全面的な連携・協力は容易ではない。

日本は、こうしたリスクと課題を抱えた米国のサイバー戦略・政策から多大の影響を受けつつ、様々な国内の制約条件の下で自国のそれを策定していかねばらない。それでは、どのような具体的な制約があり、何がどこまで可能なのであろうか。

３．日本のサイバーセキュリティ戦略・体制の欠点

３．１．2018 年版『サイバーセキュリティ戦略』

この文書は第 4 章でサイバー空間における防衛・防御の方針・施策がある程度詳細に記述されている。

同章第 2 項「国民・社会を守るための取り組み」は具体策として、①積極的サイバー防御（サイバー攻撃の脅威に対して事前に能動的に防御する取組）と②サイバー犯罪への対策を推進することを求めている。その上で同項では、「サイバー空間と実空間の双方の危機管理に臨む」必要があるとの認識に立って、「大規模サイバー攻撃事態等への対処態勢の強化」のための具体策の方針に言及している。

同章 3 項では、国家安全保障にとってサイバー戦略・政策が極めて重要であると位置付けた上で、「国際社会の平和・安全及び我が国の安全保障への寄与」が必要と捉え、「国家の強靭性」を確保するとしている。具体的には、①政府機関、特に自衛隊に必要な人材、装備、ネットワーク、情報システム、インフラ、サプライチェーンなどを確保すること、つまり任務保証、②我が国の先端技術・防衛関連技術の防護、③サイバー空間を悪用したテロ組織の活動への対策を求めている。また、「サイバー攻撃に対する抑止力の向上」のために、①実効的な抑止のための対応と②信頼醸成措置の重要性に言及している。さらに、「サイバー空間における状況把握の強化」のために、①関係機関の能力向上と②脅威情報連携の重要性にも触れている。とはいえ、肝心の報復や情報収集・分析に関する手段やリソースの確保の点

[35] Banks, *op.cit,* p.248.

で具体性を欠いている[36]。

しかし、これではサイバー攻撃を受けてからの対処、つまり攻撃を受けることを前提に防御しか考えていない。換言すれば、どのようにすればサイバー攻撃を被らないようになるのか、或いは少なくともどのようにすれば、その被害の程度や頻度の点で減じることができるのかが言及されていない。他方、サイバー攻撃を抑止するために、どのようなサイバー/非サイバー的手段による反撃・報復能力を保有・強化するのか、更に如何にそれを使用・行使するのかに関する方針が欠落している。両面を総合的に見れば、日本はサイバー空間のセキュリティを極めて受け身で防御するサイバーセキュリティ戦略を持っていても、国家安全保障の観点から軍事、外交、経済その他のパワーを駆使して総合的にサイバーによる脅威に対抗するサイバー戦略を持っていない。この状況は、本質的には国防における「専守防衛」と同じである。

それでは、防衛省・自衛隊の方針はどうなっているのか。実は、サイバー攻撃事態は2005年の「国民保護に関する基本指針」（閣議決定、2005年3月）には全く言及されていなかったところ、2012年に策定された「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」（以下、「当該文書」）では言及された。[37]

これは、日米各々の政策文書の策定と、両国間の政策協議の過程を踏まえると、米国から多大な影響を受けたと思われる。米国は従前から安保・サイバー分野で各種戦略文書を策定してきたところ、2010年版「国家安全保障戦略」でサイバー空間における脅威を国家安全保障上のそれと位置付け、同年の「（日米）2+2」の共同発表で脅威認識の共有が確認された一方、日本は同年の「防衛大綱」で「サイバー空間の安定的利用に対するリスク」を安全保障上の課題として明記した。2011年には、米国が「（国防総省）サイバー空間作戦戦略」を発表し、2012年には、日本が「当該文書」を策定した。その上で、2013年の「2+2」の共同発表はサイバーセキュリティでの協力・調整の方針に言及した。

「当該文書」は、①サイバー空間を陸海空、宇宙に次ぐ第5の作戦領域として初めて位置付け、②「武力攻撃への対処に際し自衛隊がこれを効果的に排除するため、相手方によるサイバー空間の利用を妨げることが必要となる可能性にも留意」するとし、サイバー攻撃の権利を留保し、③「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見做すと判断」し、単なる受け身の防御から反撃・報復への志向を明らかにした。もっとも、ここでは「武力攻撃の一環」の意味が不明である一方、武力攻撃事態が発生した場合、サイバー攻撃の有無に関わらず、自衛権は発動されるから、単なる同義反復とも言える。

しかし、この志向は『サイバーセキュリティ戦略』（2018年度版）でも、2018年度「防

---

36 この状況は、サイバーセキュリティ基本法第19条（我が国の安全に重大な影響を及ぼすそれのある事象への対応）「国は、サイバーセキュリティに関する事象のうち我が国の安全に重大な影響を及ぼす恐れがあるものへの対応について、関係機関における体制の充実強化並びに関係機関相互の連携強化及び役割分担の明確化を図るために必要な施策を講ずるものとする」を満たしていない。同法ができて既に8年を経過していることを踏まえると、この不作為は非常に深刻である。

37 「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（概要）」、防衛省、2012年9月、
https://www.nisc.go.jp/conference/seisaku/dai31/pdf/31shiryous04.pdf.

衛大綱」でも何ら具体化されないままとなっている。つまり、サイバー空間における反撃・報復は依然として戦略方針に沿った形で実行できない。というのは、通常、戦略の策定には、脅威の定義やその特徴、勝利或いは優勢確保のための方法、行動・能力行使の判断基準、実施の主体の特定そして権限の付与が具体的且つ明確に規定される必要がある。逆に言えば、こうした細部が欠落している上記文書は立派に見えても到底戦略とは呼べない代物であり、曖昧な政策指針程度の内容しか有していない。猶、法的制約については、後述する。

もちろん、こうした欠点・短所は、NISC ホームページに掲載されているサイバー分野の文書・資料の充実振りを見れば、当該文書を策定した政策担当者の知見や分析・考察力の欠如に起因すると捉えるのは誤りであろう。そこで、次に制度面や組織面での制約条件を米国のケースと比較分析してみることとする。

３．２．NISC 体制と自衛隊サイバー防衛隊

サイバー分野における日米の体制の差異は政府民生部門の危機管理組織と軍担当部隊の間の役割分担と付与権限の差異を把握すればよい。つまり、前者は内閣サイバーセキュリティ・センター（NISC）と連邦サイバーセキュリティ・インフラセキュリティ庁（CISA）であり、後者は自衛隊サイバー防衛隊と米サイバー・コマンドである。

CISA は連邦政府のネットワークの防護、主要インフラの防護の調整、官民の調整等を担っている。その機能を果たすため、2018 年の発足時には既に 3400 名弱の人員を擁し[38]、下部組織として、サイバーセキュリティ部（Cybersecurity Division）、インフラ・セキュリティ部（Infrastructure Security Division）、緊急コミュニケーション部（Emergency Communications Division）、国家リスク管理部（National Risk Management Division）に相当な要員、情報分析能力、事案対処能力と、防護活動を実施或いは支援する機能を有している。特筆すべきは、重要インフラ情報法（2002 年）と下位政令等に則り、CISA は民間部門から任意の情報提供を確実にする制度を確保した上で、その情報システムを直接に監視し、連邦政府各機関や民間組織と協調・協力してサイバー攻撃から非政府民間部門の重要インフラを防護している点にある（同庁設置法、2018 年制定・発効）[39]。とはいえ、CISA はサイバー・コマンドによる作戦活動に達しない水準で、保有する能力を駆使して積極防衛を行っていると推定される。つまり、CISA はサイバー分野における国全体の危機管理をしている。他方、米サイバー・コマンドはサイバー分野における軍事作戦活動を担っている。

したがって、重要インフラを巡るサイバー危機対処においては[40]、CISA とサイバー・コマンドが曖昧な分担で所管しているが、そこに外交部門は組み込まれておらず、危機対処の政策決定と執行における統合されたサイバーセキュリティ組織・枠組みは存在しない。その結果、サイバー攻撃に対する抑止や報復のための強制外交（coercive diplomacy）の実行においては、制度上、必要な行動の統一性は担保されていない。要するに、米国は未だサイバ

---

38 2018 年、CISA が従前の諸組織から引き継いだ人員数は 3374 名である。

39 これらの下部組織の具体的な諸機能や技術力に関しては、https://www.cisa.gov/cybersecurity、を参照せよ。但し、CISA 自身は法執行部門を持っていないため、捜査その他の法執行は行わない。

40 大災害に関する危機対応に関しては、連邦緊急事態管理庁（Federal Emergency Management Agency: FEMA）が所管している。

一分野において総合的な国家強制戦略（national coercive strategy）を有していないし、そのために必要な国家的意思を未だ十分固めていない[41]。

他方、我が国では、NISC が省庁その他政府機関の情報システムに対する不正な活動を監視・分析する役目を担い、必要な助言、情報その他の援助を提供する。また、行政各部のサイバーセキュリティ政策の統一性を保つための監査、調査研究、企画、立案そして総合調整に関する事務を担っている（内閣官房組織令第 4 条）。つまり、NISC は行政府のサイバーセキュリティ政策関連事務を所管するだけで、立法府や司法府のそれを所管しない。

また、重要インフラを含め民間部門のサイバーセキュリティに関しては、NISC は任意の情報の収集・分析・共有で連携、協力、援助するのみである。サイバーセキュリティ基本法は行政各部や民間組織に各々の保有する能力で危機対応することを求めている。したがって、国の機関や重要インフラに対する大規模サイバー攻撃に対する対処責任の主体は曖昧であり、国が主導的役割を果たす体制になっていない。実際、NISC は人員・予算で極めて小規模であり、そうした能力を有さない[42]。

つまり、NISC は連絡・調整機関に過ぎないのであって、残念ながら、日本にはサイバー分野における国全体の危機管理を所管する官庁・機関が存在しない。具体的には、総務省が情報通信技術分野、経済産業省が重要インフラ分野、警察庁がサイバー犯罪と重要インフラへのサイバーテロ攻撃を縦割りの形で所管しているに過ぎない。また、自衛隊サイバー防衛隊は防衛省・自衛隊の情報通信システムのみを防護している[43]。

３．３．法的制約

こうした安全保障面における日本のサイバーセキュリティ戦略・体制の歪さは、既に触れたように、懲罰的抑止を焦点とした戦略的転換を阻む憲法第 9 条に起因していることは多言を要しない。自衛隊法改正を含む平和安全法制（2015 年）の下では、厳しい制約条件と手続きの下、自衛権に基づく武力行使を行うこととなっている。ところが、前述したように、サイバー分野における自衛権はそうした条件・手続きを満たすことができないことから、依然として発動できないままである。実際、国民保護法第 32 条に基づき策定された「国民の保護に関する基本指針」（閣議決定、2005 年 3 月 25 日）において、武力攻撃事態 4 類型及

---

41 詳しくは、Banks, *op.cit,* pp. 213-217. なお、政府横断的な情報共有・危機対処連携は、国土安全保障省（DHS）傘下の国家サイバーセキュリティ・コミュニケーション統合センター（National Cybersecurity and Communication Integration Center: NCCIC）が行うことになっているが、各種機関が分散して所管・対処権限を有し競合しているため、容易には統合された対処が実現できていない。

42 2018 年現在、NISC の職員数は僅か 191 人（常勤 109 人、非常勤 82 人）に過ぎない。第 197 通常国会　衆議院内閣委員会議事録、第 6 号、2018 年 11 月 22 日。

43 サイバー防衛隊に関しては、内部組織等の細部について公表されておらず、具体的な分析・考察は非常に困難である。とはいえ、防衛省・自衛隊から NISC に人員を派遣しており、その主力である同部隊からの出向者が監視要員や分析要員を担っている。一般に、防衛省・自衛隊の情報システムは比較的堅牢に守れており、直接のサイバー攻撃は困難であると考えられるから、防衛産業その他重要インフラの情報システムに侵入し、そこから迂回した形で攻撃のリスクがあると思われる。したがって、同部隊は NISC の出向により知見・技能を高めていると考えられる。

び緊急対処事態 2 類型（及び例示）にはサイバー攻撃は含まれていない[44]。さらに、自衛隊や法執行機関によるサイバー分野における警察行動も厳格に「正当防衛・緊急避難」や「警察比例の原則」の遵守を求める。確かに、2018 年に公表された「防衛大綱」では「自衛隊の情報通信ネットワークを常時継続的に監視するとともに、我が国への攻撃に際して当該攻撃に用いられる相手方によるサイバー空間の利用を妨げる能力等、サイバー防衛能力を抜本的に強化」する方針に明らかにしているものの、サイバー空間の利用を「妨げる能力」の保有が限定的にサイバー反撃・報復を行う方針を意味するとは解釈できない。

さらに言えば、日本には主要国のような真正の諜報機関とそれを可能にするための法制が存在しないため、情報収集やそれに伴う諜報活動ができず、ハッキングなどを利用した積極的なサイバー情報収集活動が容易には許容されない。その結果、しばしばサイバー攻撃その他不正な活動の責任帰属先の判定ができず、抑止や反撃ができない。

具体的には、攻撃者/潜在的攻撃者のサーバーへの侵入は一定のケースを除いて憲法第 21 条 2 項「通信の秘密」への抵触となるであろうし、国境を越えた侵入であれば、主権侵犯に当たる虞が強い[45]。ただし、サイバー情報収集のためのボットネット作成はウイルス作成罪に該当し、さらにその情報を使って攻撃者のシステムに侵入すれば、不正アクセス禁止法に該当するであろう。所管官庁は既存の業法による安全基準の設定や事業者に対する指示、命令、行政指導をおこなっているが、米国の重要インフラ情報法に当たる法律がないことから、事業者は物理的な障害発生後の報告義務しかない。つまり、情報システムに侵入されても、物理的な障害その他実害が顕在化しない限り、報道や社会的非難を恐れて報告せず、隠蔽する可能性が極めて高い。

もちろん、日本政府が単に腕を拱いてきたわけではない。総務省は電気通信事業法の適用に関しては、「通信の秘密ガイドライン」を見直して、約款による規定を当事者の同意と見做し、サイバー事案に関する所定の調査等は通信の秘密の侵害に当たらないとの解釈に変更した[46]。これにより、攻撃者/潜在的攻撃者に関する情報の入手が可能となり、責任帰属先を判定する能力は高まった。また、情報通信研究機構（NICT）法が改正され、同機構が IoT 機器の脆弱性に関する調査を合法的に行えるように 5 年間の時限措置を講じた[47]。と

---

44 「武力攻撃事態の類型ごとの特徴」、内閣官房国民保護ポータルサイト、http://www.kokuminhogo.go.jp/gaiyou/tokucho.html。

45 言うまでもなく、「通信の秘密」は「信書の秘密」よりも広い概念である。従来の「通信の秘密」に関する整理については、小向太郎「犯罪捜査における国外データへのアクセス」、総務省通信法学研究会　新領域分科会資料、2019 年 10 月 16 日、https://www.soumu.go.jp/main_content/000652702.pdf。ただし、最高裁決定（令和 3 年 2 月 1 日）は、「電磁的記録を保管した記録媒体が同条約（サイバー犯罪に関する条約）の締約国に所在し，同記録を開示する正当な権限を有する者の合法的かつ任意の同意がある場合に，国際捜査共助によることなく同記録媒体へのリモートアクセス及び同記録の複写を行うことは許される」とし、「通信の秘密」に抵触しない条件を示した。

46 「電気通信事業における個人情報保護に関するガイドライン」、総務省告示第 695 号、2004 年 8 月 31 日、https://www.soumu.go.jp/main_content/000507469.pdf。「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」における法的整理について」、総務省、2019 年 4 月 19 日、https://www.soumu.go.jp/main_content/000616163.pdf。

47 総務省 サイバーセキュリティ統括官室、「電気通信事業法及び国立研究開発法人情報通

はいえ、こうした動きは既存のサイバーセキュリティ体制の枠組みにおける漸進的な改善策、弥縫策に過ぎず、急速に深刻となるサイバー危機管理と米国による抑止重視のサイバー戦略への転換に直面する中、現体制が抱える根本的な解決には繋がらないことは明白であろう。

４．課題と展望

ここまで見て来たように、我が国のサイバー危機管理は技術水準、要員の質量、組織・体制整備、そして予算規模の点で非常に多くの課題を抱えている。特に、サイバー分野での法的な制約は強く、サイバー攻撃等に対して抑止力を十分発揮できない一方、危機管理体制は縦割りの弊害が強いため、政府横断的なアプローチを採ることが極めて困難な状態に陥っている。

もちろん、こうした状況を克服する方策は論理的には非常に簡単で、憲法改正その他の法制を整備し、それに基づく大幅な財源・人員を増加するビックバン・アプローチを実施すればよい。しかし実際には、これが不可能ではないにしても極めて困難であることは、ここ数十年に亘る軍事安全保障・防衛政策、とりわけ武力行使を巡る議論を見れば明らかである。既に考察したように、この議論とサイバー攻撃・抑止を巡るそれとは本質的に同じであることから、サイバー分野の政策努力も憲法第 9 条の制約を前提にそれを非常に抑制的に再解釈し、細かく状況を分類し、許容される対応を網羅的な列挙方式で立法する同様の形、つまりポジティブ・リスト方式で漸進的に進むと思われる。この過程において、政府は問題点を明らかにし、国家安全保障の点から必要なサイバー戦略・政策の変化に向けた自助努力を重視すべきことは言うまでもない。

しかし、それができなければ、そしてその蓋然性は高いと思われるが、変化に向けた原動力は安保・防衛政策の変容と同様、国際安全環境の変化を背景とした米国からの影響・圧力になるであろう。この点は既に分析したように、米国におけるサイバー戦略・政策の変化が日米間の政策協議・対話を介して我が国のそれを大きく変容させてきたことから明らかである。とはいえ、米国は自国或いは米軍に影響がなければ、敢えて日本に圧力を加えることはないであろうし、日本のサイバー能力を高めることに繋がる機微な関連情報を提供することもないであろうから、外圧依存のアプローチは次善の策に過ぎない。

４．１．「サイバーセキュリティ庁」構想

現在の我が国政府のサイバーセキュリティ体制は行政各部の縦割りが顕著で、政府内の意思統一が容易ではない。NISC はこの構造的問題に対処するために設置された機関であるが、権限と人員・予算の点で、そうした機能を十分には果たすことができていない。また、行政府のサイバーセキュリティを所管としており、重要インフラを含め国全体のサイバーセキュリティを確保する権能を付与されていない。NISC は小規模な組織であり、独自/プロパーのサイバー危機管理人材を擁しておらず、事実上、実務はサイバーセキュリティ業界

信研究機構法の一部を改正する法律（平成 30 年法律第 24 号）の施行に伴う省令の制定について（NICT 法の一部改正に伴う識別符号の基準及び実施計画に関する規定整備関係）」、2018 年 8 月、https://www.soumu.go.jp/main_content/000579753.pdf。

からの少人数の出向者に依存している状態にある[48]。他方、警察はサイバー犯罪の捜査は行っても、サイバー危機管理を行ってくれるわけではないから、結局、この構造は民間主導のサイバーセキュリティの確保を想定していると言わざるを得ない[49]。

とはいえ、これは行政機構上の問題であり、憲法上の問題を含んでいないから、論理的には顕著な改善は十分実行可能である。ただし、ますます逼迫する財政緊迫の中、必要な財源を十分確保することは容易ではないから、現実には極めて困難である。

この点、笹川平和財団がインターネット通信に通信量単位当たりで少額の賦課金を徴収する方式で2000億円/年を捻出し、2000人の要員を確保する「サイバーセキュリティ庁の創設」を提言したことは注目に値する。この規模の組織能力を保有すれば、常時、国家の安全保障を脅かすサイバー事案の危機管理に備えて対応チームを待機させることは可能であるから、ここにサイバー危機管理における命令権を付与してもよいだろう。また、米国の重要インフラ情報法に類する立法を行い、重要インフラのサイバー事案に関して「サイバーセキュリティ庁」が分析、判断、対処が可能となるように、検知その他の事実の報告義務を課することもできる。とはいえ、「サイバーセキュリティ庁」が実現するまでは、2021年9月に発足したデジタル庁にライフサイクル・セキュリティの観点から堅牢なシステムを構築するよう期待するしかない。このシステムが脆弱で使い勝手が悪ければ、わが国政府のサイバーセキュリティは却って悪化するであろう。

しかし、仮に行政機構上の課題が改善されても、サイバー攻撃に対する抑止を確保するためのサイバー攻撃能力の保有とその使用に関する法的な制約は、憲法第9条や第21条2項「通信の秘密」に基づいているため、改憲若しくは解釈改憲をしなければ、取り除いたり、緩和したりできない。日本にとって政策上、現実的な選択肢は何であろうか。

４．２．米国による「サイバーの傘」

現在、自衛隊サイバー防衛隊は約300人の人員を擁しているが、2019年「中期防衛力計画整備計画」では、同隊を1個隊（約1000名）に増強するとしている。サイバー空間での防御と攻撃が技術的には表裏一体であることから、この増強により同部隊は相当な潜在的サイバー攻撃力を持つことになり、法整備が行われれば、現在行われていない同部隊との連

---

48 既に註42で言及したように、非常勤の者（技術・非技術要員を含む）は100名に満たない。24時間3交代制であるとすれば、極めて限定された能力しかないことは容易に推定できる。

49 確かに、経産省所管の独立行政法人・情報処理推進機構セキュリティセンターはコンピューター・ウイルス、不正アクセス、脆弱性についての発見や被害届出受付等、限定的機能を有する。しかし、個別のサイバー危機事案は専ら各企業・組織の緊急事態対応チーム（Computer Security Incident Response Team: CSIRT)が脅威インテリジェンス能力を提供する民間サイバーセキュリティ会社との委託・コンサルティング契約等を利用しながら行う一方、更に高度な情報・知見・技術の共有に関しては、政府や企業から独立した（一般社団法人）JPCERT/CC（Japan Computer Emergency Response Team Coordination Center）が担う場合がある。なお、主要な民間サイバーセキュリティ会社56社（2021年5月末現在）による日本セキュリティ事業者協議会（ISOG-J）がある。人材育成・啓発に関してはやはり民間主導で、日本ネット・セキュリティ協会（JNSA、2021年4月現在、会員企業246社）や情報セキュリティ教育事業者連絡会（ISEPA）などがある。

携によるサイバー空間での相当な攻撃、反撃、制裁が可能となると思われる。

しかし、今のところ、日本政府がそうした大胆なサイバー政策の路線変更に乗り出す気配はない。実際、2021 年 5 月 13 日、政府のサイバーセキュリティ本部が公表した「次期サイバーセキュリティ戦略の骨子について」（以下、「骨子」）は既存の体制とアプローチを変更せず、漸進的に従来の施策を強化するアプローチを明確にした。特に、抑止力の必要性を述べておきながら、攻撃力の保有、行使方法そして必要な法的整備については全く具体的な言及がない。また、体制整備については、添付された「推進体制」の図には、「政府関係機関・情報セキュリティ横断監視・即応監視チーム（GSOC）」や「情報セキュリティ緊急支援チーム（CYMAT）」の用語が確認でき、「国全体として網羅的な対処が可能となる、ナショナルサート（CSIRT/CERT）の枠組みを整備（する）」との記述があるが、「サイバーセキュリティ庁」や重要インフラ情報法など、実効化に要する法律、財源、組織・要員に関して具体的な言及がない。要するに、依然、総合調整・情報共有機能しか有さない NISC を中核とした体制を維持することから[50]、残念ながらこのままでは、「次期サイバーセキュリティ戦略」は妥当な政策目標を曖昧に記した優れた官僚作文の域を出ないものとなるであろう。

注目すべきは、「骨子」がサイバー空間における抑止を実現するために、日本自身のサイバー手段による抑止力、つまりサイバー報復・攻撃力の保持に言及せず、実質的に米国に抑止力に依存する方針を明らかにした点にある。すなわち、2019 年 4 月 19 日の日米「2＋2」の共同発表において、米国が日米安保条約第 5 条の対日防衛義務をサイバーにも適用する場合があることが確認された[51]。この選択は、日本が米国の「核の傘」だけでなく「サイバーの傘」にも入り、国家の安全を保障することを意味する[52]。もちろん、米国のサイバー攻撃能力が世界最高レベルにあることから、一応、現時点では、日本が自前のサイバー攻撃能力を政治的意思と技術力の両面で保有しない方針である以上、次善の策であると言えよう。

しかし、政治的には、この対米依存は日本の独立性に疑問を投げかける。さらに、仮に「サイバーの傘」が想定する攻撃者/潜在的攻撃者に対して有効に機能するとしても、諜報活動は同盟国・友好国の間にもなされることが常であることから、米国から我が国に対するサイバー・スパイ活動その他不正な活動にはかなりの程度無防備になることを意味する。客観的には、サイバー攻撃による国家安全保障上の被害は、例えば、中国よりも米国にやられる方が「まし」だと判断するのと同義となる[53]。

更に戦略的には、サイバー攻撃の責任帰属先判定に不確実性が伴うことから、誤判定から

---

50 猶、東京オリンピックに備えて、2017 年 9 月から警察庁にセキュリティ情報センターが、2019 年 4 月から内閣官房にサイバーセキュリティ対処調整センターが設置されていたが、これが恒常的な組織に改編されるか否かは不明である。「2020 年及びその後を見据えたサイバーセキュリティの在り方（案） －サイバーセキュリティ戦略中間レビュー」、https://www.nisc.go.jp/conference/cs/dai14/pdf/14shiryou03.pdf。

51 註 25 に同じ。

52 山田、前掲書、223 頁～233 頁。

53 スノーデン氏は「米国によって、送電網やダム、病院などの社会インフラに不正プログラムが仕込まれ、もし日本が同盟国でなくなったら不正プログラムが起動し、日本は壊滅する」と証言した。「オリバー・ストーンが明かした“日本のインフラにマルウェア”のスノーデン証言」『週刊新潮』（電子版）、2017 年 2 月 2 日、https://www.dailyshincho.jp/article/2017/02020557/?all=1。

生じた攻防によるエスカレーションから米国の始めた戦争に巻き込まれるリスクが排除できない。紙幅の制約のため、ここでは簡単に言及するに留めるが、「核の傘」と同様に、米国が自国への反撃のリスクを犯しても日本のために攻撃するとの言質に対する信頼性の問題が「サイバーの傘」にも存在する[54]。

４．３．綜括と展望

ここまで、本稿では我が国のサイバーセキュリティ体制・戦略が長年の努力にも拘わらず、日本国憲法による「平和国家」体制の下、非常に歪な形で形成されてきた現状を分析・考察してきた。つまり、戦略・政策文書はかなり充実してはいるが、縦割り行政の克服や抑止力の保有・行使の点で、依然かなり未発達な状態に陥ったままである。もちろん、根本的な解決は改憲を含む「ビックバン」によって可能となると予見できるとは言え、その実現は軍事安全保障・防衛における集団的自衛権に基づく武力行使に関する経緯と同様、非常に困難である。

従って、今後のサイバーセキュリティ政策は既存の体制・組織を前提に漸進的に改善・強化していくことにならざるを得ないだろう。具体的には、NISC を危機管理権限、組織、人員・能力の点で強化しつつ、「サイバーセキュリティ庁」の実現を模索する一方[55]、拒否的抑止、つまりサイバー攻撃の阻止や被害限定を強化することになる。ただ、サイバー攻撃による懲罰的抑止はおこなわず、その代わり、米国の「サイバーの傘」の下に入り、その有効性を高める対米政策連携・協力を推進することになるだろう。

とすれば、今後、日本のサイバー戦略は、情報通信機器・システムと情報通信ネットワークに関するサイバーセキュリティ戦略(cybersecurity strategy)では、米国その他の主要同盟国の動向に立ち遅れないように努力する一方、法執行や外交など非サイバー政策手段を総動員して綜合的な取り組みを行うことが最も望ましい。つまり、我が国は従来からのサイバーセキュリティ戦略に国防、外交その他の戦略を加味して、できるだけ米国流のサイバー戦略(cyber strategy)に近づけることが求められる。特に、依然我が国が部分的に比較優位を保持する半導体や通信機器等、サイバー関連のハードウェアの技術や生産を通したサイバーセキュリティを強化し、この分野におけるパワーと影響力を高めることが望まれる[56]。
脚註の URL は 2021 年 9 月 13 日現在すべて有効であった。

---

54 「サイバーの傘」の実効性を担保し、日米共同対処における日本のサイバー能力を向上するため、自衛隊サイバー部隊から米国サイバー・コマンド、特に実際の活動を担う陸海空軍・海兵隊隷下の部隊に、技術・訓練研修の目的で相当数の隊員を継続的に派遣すべきであろう。

55 ただし、本稿で考察したように、サイバー分野で専守防衛は成り立たないことから、同庁設置に際して、限定的なサイバー諜報活動を許容する制度が不可欠である。

56 本稿のテーマを逸脱するため、産業面での分析・考察は今後の論考に譲りたい。手がかりとしては、以下の文献がある。平井浩治『経済安全保障リスク　米中対立が突き付けたビジネスの課題』、育鵬社、2021 年。渡邉哲也『米中決戦後の世界地図　日本再興が始まる』徳間書店、2020 年。宮本雄二・伊集院敦（編著）『技術覇権　米中激突の深層』日本経済新聞出版社、2020 年。深田萌絵『日本の IT 産業が中国に盗まれている』WAC、2019 年。同『米中 AI 戦争の真実』育鴻社、2019 年。同『「５G 革命」の真実　５G 通信と米中デジタル冷戦の全て』WAC、2019 年。

謝辞

本稿は、電気通信普及財団からの研究助成をうけた「サイバー空間のセキュリティとサイバー攻撃事態への対処の枠組みに関する研究」〔2019 年度～2020 年度〕の研究成果である。記して感謝申し上げる。

参考文献

Brantly, Aaron F, ed, *The Cyber Deterrence Problem,* Rowman & LittlefIeld International, 2020.

Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2nd. Edition, 2017.

Whyte, Christopher, and Brian Mazanec, *Understanding Cyber Warfare: Politics, Policy and Strategy,* Routledge, 2019.

程琳（主编）『中美网络安全比较研究』中国人民公安大学出版社、2017 年

『日本にサイバーセキュリティ庁の創設を！』、笹川平和財団、2018 年 10 月。

中谷 和弘、河野 桂子 、黒崎 将広『サイバー攻撃の国際法―タリン・マニュアル 2.0 の解説』信山社、2018 年。

（掲載決定日：令和３年 12 月 27 日／オンライン掲載日：令和４年１月 13 日）