博士論文

自衛隊が行うサイバー作戦における情報法制上の課題

Tetsunosuke Jinnai

陣内　徹之助

情報セキュリティ大学院大学
情報セキュリティ研究科
情報セキュリティ専攻

２０２４年３月

目　次：

Ⅰ　序　論

1.1　サイバー空間における紛争と法規制

サイバー空間[1]における紛争[2]は、国家にとって安全保障上の重大な脅威となっている。サイバーセキュリティ戦略本部が 2021 年に発表したサイバーセキュリティ戦略は、「サイバー空間の状況は、それ自体が国家的な緊急事態にまでは至らないものの、もはや純粋に平時のものとみなすことはできない」[3]との情勢認識を示す。実際、サイバー空間では平時から国家による様々な活動が行われているが、その活動には有害な物も含まれている[4]。ランサムウェア等による金銭的利益獲得を目的とした犯罪行為を国家が支援するケースも存在するが[5]、それ以外にも cyber espionage[6]（以下、「espionage」と略。）と呼ばれる情報集活動やディスインフォメーション活動による選挙妨害等の影響力作戦[7]とよばれる国益追及を目的にした活動が平時から活発に行われている。さらに、サイバー作戦は国家間紛争を直接的に有利にする手段としても使用

---

[1] サイバー空間とは、「コンピュータやネットワーク上に構築された仮想的な空間」の意味で使用する。インターネットを含むすべてのネットワーク空間を指すほか、コンピュータ内部における論理的な空間も包含する概念である。なお、米軍教範では cyberspace の定義として、「インターネット、通信ネットワーク、コンピュータシステム、組み込みプロセッサやコントローラなど、情報技術インフラと常駐データの相互依存ネットワークからなる情報環境内のグローバルドメイン」と規定する。U.S. Joint Chiefs of Staff, "Joint Publication 3-12 Cyberspace Operations" (June 18, 2018).

[2] 国際法上、紛争とは「二当事者間の法または事実の論点に関する不一致、法的主張ないし利害の衝突、対立である」とされる。 PCIJ Series A, No. 2 at 11.

[3] サイバーセキュリティ戦略本部「サイバーセキュリティ戦略」2021 年 9 月 28 日（閣議決定）8 頁。

[4] 日本においても、2016 年から 2017 年にかけて JAXA 及び防衛関連企業等に行われた大規模なサイバー攻撃への中国人民解放軍の関与が明らかにされている。日本経済新聞「JAXA などにサイバー攻撃か－中国共産党員を書類送検」2021 年 4 月 20 日 <https://www.nikkei.com/article/DGXZQOUE200CS0Q1A420C200000/>。

[5] 著名な例として、北朝鮮政府に支援された BlueNoroff と呼ばれるハッカー集団が 2016 年 2 月にバングラデシュ銀行から約 8,100 万米ドルを不正に盗み出したとされる事例が存在する。*See* U.S. Department of the Treasury, "Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups" (September 13, 2019),online: <https://home.treasury.gov/news/press-releases/sm774>.

[6] cyber espionage は「秘密裏に、または偽って、サイバー機能を用いて情報を収集する、または収集しようとする行為」と定義される。*See* Michal N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017) at 168.

[7] 影響力工作の定義に「平時、危機、紛争、紛争後において、国家主体の安全保障政策目標を達成する目的で、政治指導者、国民、特定のターゲット集団（専門家、軍人、メディアなど）の意思決定、認識、行動に影響を与えることを目的とした、国家の外交、情報、軍事、経済、その他の能力の調整、統合、同調した適用」が挙げられる。Sean Cordey, "Cyber Influence Operations: An Overview and Comparative Analysis" (October, 2019) at 10, online: Center for Security Studies (CSS) ETH Zürich <https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-10-CyberInfluence.pdf.>. 影響力工作におけるサイバー作戦の代表的な例として、2016 年の米大統領選に対するロシアの選挙干渉が挙げられる。Samuli Haataja, *Cyber Attacks and International Law on the Use of Force - The Turn to Information Ethics* (Routledge, 2019) at 192-202.

される場合もあり、とりわけ重要インフラ[8]を対象にしたサイバー攻撃[9]は短期間で莫大な被害が発生し国家機能が麻痺する可能性すら考えられる重大な脅威である。また、国家間紛争がエスカレートし、武力紛争に至った場合においても、サイバー空間は従来の陸海空領域に並ぶ新たな戦場として考えられており、軍事作戦に占めるサイバー作戦[10]の重要性が増している。実際、2022年2月24日に勃発し、現在も継続中のロシアによるウクライナへの軍事進攻（以下、ウクライナ紛争）では、ロシア、ウクライナ両国による活発なサイバー作戦が展開されている。

これらのサイバー空間における活動には国家の様々な組織が関与していると考えられるが、多くの国家において軍隊を中心とする軍事組織[11]がその中核を担っていることは否定できない。実際に、多くの国が自国の軍隊のサイバー作戦能力向上に多大な努力を傾注しており、様々な場面で軍の関与が疑われるサイバーインシデントが発生している。これらの活動は、従来の軍隊による活動と大きく性格が異なり、表面上に明確に表れることが少ないため、対応が難しい。特に、特筆すべき点として挙げられるのが、平時と有事の境目が曖昧となっていることである。一般的な認識である有事、いわゆる戦争状態とは、国際法上は国家間武力紛争が生起している状態と認識され、適用される法体系が平時とは大きく異なる[12]。しかしながら、通常の軍事作戦と異なり、人の殺傷や物の破壊といった目に見える物理的被害が生じないサイバー作戦の場合、国家間武力紛争が生起しているかどうかを明確に判断することが難しく、平時でも有事でもない状態、いわゆるグレーゾーンの事態[13]（以下、「GZ事態」と略。）となっている。

---

[8] 重要インフラの定義は、サイバーセキュリティ戦略本部「重要インフラの情報セキュリティ対策に係る第4次行動計画（以下、第4次行動計画）」（2020.2.1改定）による。

[9] サイバー攻撃の定義は様々であるが、本稿では、サイバー犯罪と国際紛争上の手段としてのサイバー攻撃を区分し「サイバー攻撃とは、政治的または国家安全保障上の目的で、コンピュータネットワークの機能を低下させるために行われるすべての行為を指す」とする定義を採用する。*See* Oona A. Hathaway, "The Law of Cyber-Attack" (2012) 100(4) *California Law Review* 817 at 86.

[10] 本稿では政府機関等の公的組織がサイバー空間上で行う活動を総称し「サイバー作戦」とし、とりわけ軍隊が実行するサイバー作戦に焦点をあてる。なお、米軍教範においては、cyberspace operationsとして、「cyberspaceおける、またはcyberspaceを通じて目的を達成することを主目的としたcyberspace capabilityの使用。COとも呼ばれる。」とする。*See* U.S. Joint Chiefs of Staff, *supra* note 1.

[11] 本稿において軍事組織とは、軍隊を中心に、準軍事的活動を行う情報機関、あるいは政府の統制下にある民兵組織を含む概念の意味で使用する。

[12] 国家間武力紛争が生起している間は、国際人道法が主たる法規範として適用され、一定の制限の下、戦闘行為が正当化される。

[13] 防衛白書においては、グレーゾーンの事態とは「純然たる平時でも有事でもない幅広い状況を端的に表現したもの」とされ、「国家間において、領土、主権、海洋を含む経済権益などについて主張の対立があり、少なくとも一方の当事者が、武力攻撃に当たらない範囲で、実力組織などを用いて、問題にかかわる地域において頻繁にプレゼンスを示すことなどにより、現状の変更を試み、自国の主張・要求の受入れを強要しようとする行為が行われる状況」を例示する。防衛省「令和4年度版防衛白書」2022年1頁。

サイバー空間における法規制は国際法及び国内法の両分野において依然として発展途上にあり、数多くの曖昧性が存在する。一部の国は、この曖昧性を利用し、国益追及あるいは力による現状変更の観点から様々な活動をサイバー空間で行っている。一例として、いわゆる「ハイブリッド戦」におけるサイバー作戦が挙げられる。「ハイブリッド戦」とは、「軍事と非軍事の境界を意図的に曖昧にした手法」により「相手方に軍事面にとどまらない複雑な対応を強いる」ものとされ、GZ 事態を活用した戦術であるが、その中でもサイバー作戦は主要な要素として位置付けられている[14]。また、GZ 事態に限らず、紛争が国家間武力紛争に発展した場合においても、民用物に対するサイバー攻撃等といった、従来の法規制が上手く機能しない事例が数多く発生している。

国際法の分野では、2000 年前後より、サイバー空間への国際法適用を巡り国際連合（以下「国連」と略する。）をはじめとした様々な枠組みで各国による議論が行われてきた。また、国連だけでなく国際法学者等による学術分野においても非常に活発な議論が行われ、現状として、既存の国際法の各種規則がサイバー空間においても適用される、とする国際社会における共通認識は確立されたように見受けられる。しかしながら、実際に国際法上の各種規則をサイバー空間に適用するにあたっての細部の具体的論点に関しては、各国及び学術上の見解は依然として一致しない点が数多く存在する。このため、国際社会の幅広い支持を得た、サイバー空間を規制する明文上の国際条約等が早期に締結される可能性は極めて低いと言わざるを得ない。逆に言えば、形成途上であるが故に自国に有利な国際法秩序を形成する好機であるとも言うことが出来、今後各国の積極的な法解釈に対する主張が予想される。

1.2　日本の対応状況

日本は、サイバー空間への国際法適用に関する議論については、数度にわたるサイバーセキュリティに関する国連政府専門家会合への参加等、比較的積極的に関与していると言えるであろう[15]。一方で、国際法領域における活動に比し、国内法領域における取組みは活発とは言えない状況である。特に、サイバー空間における安全保障（以下、「サイバー安全保障」と略する。）に

[14] ハイブリッド戦の例として「国籍を隠した不明部隊を用いた作戦、サイバー攻撃による通信・重要インフラの妨害、インターネットやメディアを通じた偽情報の流布などによる影響工作を複合的に用いた手法」が挙げられる。防衛省・前掲注 13。

[15] サイバー空間に適用される国際法に関する日本の取組みについては外務省 HP を参照。外務省「日本のサイバー分野での外交　多国間会議等」2023 年 6 月 20 日（更新）<https://www.mofa.go.jp/mofaj/fp/nsp/page24_000686.html>。

関する国内法整備は、各国に比し大きく出遅れていると言わざるを得ない。日本においても「平成 31 年度以降に係る防衛計画の大綱」に「相手方によるサイバー空間の利用を妨げる能力（以下、妨げる能力）」が明記され、攻撃的なサイバー作戦能力の整備を始めとするサイバー空間の脅威に対する各種対応が進められている。しかし、現状の日本のサイバー空間における紛争（以下、「サイバー紛争」と略する。）への対応能力は周辺国に比して十分ではないと考えられ、特に、法整備の遅れが足枷となっている感は否めない。実際、各国のサイバー能力の格付けを行っている英国の研究機関 IISS(International Institute for Strategic Studies)は、中国及びロシアをそれぞれ Tier 2 に位置付ける一方、日本を最下層の Tier 3 とし、その理由の一つとして憲法上の制約による攻撃的能力の制限を挙げている[16]。このため、令和４年１２月１６日に閣議決定された国家安全保障戦略は、「能動的サイバー防御」構想を打ち出し、その実施のために必要な権限を政府に対し付与することを検討する旨が明記された[17]。これは、日本のサイバー安全保障の観点から大きな前進であると評価できる。一方で、能動的サイバー防御構想を具体化し、周辺国と同等のレベルでのサイバーセキュリティ態勢・体制を実現するにあたっては、乗り越えなければならない様々な法的課題が存在すると考えられる。

特に、国内法整備にあたっては日本の独特な法環境が大きく影響を及ぼす点は考慮が必要である。日本では伝統的に行政機関による権限行使に対しては、憲法・行政法による強い制約を課しており、特に通信分野では「通信の秘密」を始めとする様々な独特な規制が存在する。また、安全保障法制に関する検討自体も第 2 次世界大戦以降の歴史的経緯もあり、十分な研究の蓄積がなされているとは言えない状況である。加えてサイバー空間自体が比較的新しい概念であることもあり、サイバー安全保障に関する法整備を進め、能動的サイバー防御構想を実現することは容易ではないと考えられる。

1.3　本研究の目的、問題認識及び論文構成

本稿は、サイバー紛争の法規制に対する日本の対応、特に平素・有事を問わず自衛隊が行う（行うべき）サイバー作戦に対する法的課題を国際法及び国内法の双方の観点から論ずるものである。その目的は、日本がサイバー安全保障において取り組むべき法的課題を明らかにするとともに、当該課題に対する具体的な提言を行うことにある。全般的な問題認識としては、下記の

[16] *See* International Institute for Strategic Studies(IISS), "Cyber Capabilities and National Power: A Net Assessment" (Jun 28, 2021), online: IISS <https://www.iiss.org/blogs/research-paper/2021/06/ cyber-capabilities-national-power>.
[17] 内閣官房「国家安全保障戦略」2022 年 12 月 16 日（閣議決定）21 頁。

三つが存在する。

一つ目の問題は、日本のサイバー安全保障における府省庁の役割区分が不明確である点である。象徴的な例として、サイバーセキュリィティ基本法 19 条は、サイバー安全保障における各府省庁の役割区分等について「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。」としたままであり、現状では法的に未確立な状態が継続している[18]。前述の新安全保障戦略においても、この問題点は解消されておらず、具体的な役割分担は明らかにされていない。特に、安全保障の中核を担う自衛隊の任務・権限が不明確である点は、最も重大な懸念事項である。自衛隊は軍事組織ではあるが、国内法上の地位は一行政機関にすぎず、その活動の根拠は国内法である。一方で、現行法制上、自衛隊に対しサイバー空間での活動に対する法的根拠を付与する明確な条文は存在しないため、自衛隊がサイバー空間において行使できる権限が不明確な状態となっている。サイバー安全保障を実効的なものとするためには、この問題については早急に取組むことが求められる。

二つ目は、サイバー空間に適用される国際法の解釈が極めて曖昧であり、違法性を判断する基準が不明確であるという点である。国際法は、執行管轄権を行使する、あるいは有権解釈等を行える機関が存在せず、基本的に各国の合意に基づき運用される。また、明文上の条約等が無い慣習法に依拠する部分も大きく、本質的に曖昧性を有すると言える。加えてサイバー空間という新たな領域に対する適用という観点から、意見が統一されないことはある意味止むを得ないとも言える。重要なことは、形成途上である点や曖昧性を有するという状況を積極的に捉え、日本にとって有利な戦略環境を醸成するために積極的に国際法解釈について日本の立場を主張していくことであると考える。日本は、前述の通り、日本は国際法適用に関する議論の場に積極的に関与しているが、国際社会における日本の立場の主張という観点からは十分ではないと考えられる。国益に沿った、自国に有利な法環境の形成という観点からは、日本としての立場をより積極的に、かつ能動的サイバー防御構想と密接に関連させた上で発信していく事が重要であると考える。

三つ目は、国際法と国内法の不整合である。日本の国内法に関し、国際法における議論が着実に国内法に反映されているかという点は極めて疑問である。日本国内において防衛省・自衛隊を始めとする各行政官庁が権限を行使

[18] サイバーセキュリティ基本法第 19 条は「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おそ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。」とし、各省庁の役割分担が依然として不明確であることを示す。

するためには、国内法上の根拠が必要であり、国際法と整合を図りつつ国内法整備を進めていくことが必要である。従来、日本においては国際法と国内法が別々に議論される傾向が存在し、特に安全保障法制に関する議論ではその傾向が顕著である。一例として、日本国内の研究においても、武力紛争を題材とした国際法研究はかなりの数が存在する事に対し、武力攻撃事態[19]における国内法を取り扱った研究は極めて数が少ない。本来、国家と国家の関係を律する国際法と、国家と国民あるいは国民相互の関係を律する国内法とでは根本的に性格が異なり、国際法上の権利・義務を必ずしも国内法で規定する必要性はないことは当然ではある。一方で、安全保障に関する法制は、国家と国家の関係を含むものであり、国際法と国内法に差異があることは大きな問題となる可能性がある。平時～GZ 事態～有事に至る一連の流れにおいて、国際法と国内法が齟齬なく整合が適合する切れ目のない国内法整備が行われることが安全保障分野では重要となる。特に、サイバー空間では、明確な国境が存在しないことから、国際法と国内法の適用が交錯する場面が生じることが考えられる。両者に不整合が存在することは、適切な法の適用という観点からは、大きな障害となる可能性がある。

上記三つの問題認識に基づき、本稿では国際法の解釈において日本が取り得る立場を明らかにすること、国内法の観点からは自衛隊の任務・役割・権限の具体化すること及び国際法と国内法の不整合是正する観点から必要な法改正の提言を行うことを焦点としている。具体的な論文構成として、まず続く第Ⅱ章及び第Ⅲ章において、法的課題を議論する際の前提となる軍隊が行うサイバー作戦の概要及びサイバー抑止理論についてそれぞれ分析を行う。第Ⅳ章では、サイバー空間に適用される国際法及び国内法の双方についての全体像を概観し、平時から有事に至る法的枠組みの変化を確認する。第Ⅴ～Ⅷ章は本稿における本論に該当し、サイバー作戦を行うための法的課題を明らかにする。第Ⅴ、Ⅵ章がいわゆる GZ 事態であり、平時から武力紛争に至らない事態における様々な国際法、国内法上の課題を明らかにする。続く第Ⅶ、Ⅷ章は武力紛争間における国際法、国内法上の課題を扱う。最後に第Ⅸ章において、結論として日本が取り得るべき政策及び必要な法改正の提言を行う。

なお、自衛隊の合憲性に関し、現在においても議論が存在し、違憲論が根強く存在することは確かである。しかしながら、本稿においては「自衛のための必要最小限度の実力」は、憲法９条２項前段の「戦力」にあたらず、自

[19] 武力攻撃事態等及び存立危機事態における我が国の平和と独立並びに国及び国民の安全の確保に関する法律（以下、「事態対処法」と略する。）２条２項が定める「武力攻撃が発生した事態又は武力攻撃が発生する明白な危険が切迫していると認められるに至った事態」

衛隊は、「自衛のための必要最小限度の実力」であるため合憲、とする政府見解[20]を踏襲する。また、努めて現実的かつ早期に実現可能な提言を行うという観点から、憲法改正等の議論には踏み込まず、飽くまで現行憲法の枠組み内での法改正等を議論の前提としている。

安全保障領域では憲法改正に対する様々な意見や見解が存在する。しかしながら、2015 年の第二次安部晋三内閣の下での平和安全法制[21]の成立以降、憲法改正に対する議論が特段盛り上りを見せる状況ではなく、憲法改正に対しては引き続き高いハードルがあるものと認識する。このため、喫緊の課題に対応する観点から憲法改正についての議論を含めることは現実的でないと考えられる。また、憲法改正はサイバー空間に留まらない幅広い領域に影響を及ぼす論点であり、本稿の趣旨にそぐわないと判断したものである。

1.4 先行研究の概要及び評価

サイバー空間における国際法の適用を巡っては、様々な先行研究が存在する。代表的なものとして、NATO サイバー防衛センター（NATO CCD COE）が 2017 年に公表した Tallinn Manual 2.0 が存在する[22]。同書は、条約のような拘束力は有しておらず、かつロシア・中国を含む西側諸国以外の支持まで得ているとは必ずしも言えない側面もある。しかしながら、西側諸国の著名な国際法学者らが結集して作成した研究成果という点において、一定の権威及び影響力を有すると言える。

また、上記 Tallinn Manual 2.0 の編者でもある Michael N. Schmitt は武力紛争法から国家責任法に至る幅広い領域で研究成果を公表している。米国では Michael N. Schmitt を始め、Gary Corn といった多くの軍と関係が深い法学者が積極的に意見を発表していることは印象深い。彼らの特徴として、現実的な国益追及の観点から国家の意見を代弁するものが多く、前方防衛を始めとする現在の米国の積極的なサイバー抑止策に対する理論的根拠を与えている。また、上記のいずれの法学者も、武力攻撃の基準に至らない低強度のサイバー攻撃に対する対抗措置の活用を主張している点は興味深い[23]。一方、赤十字国際員会等は、より人道的見解から文民及び紛争犠牲者保護を重視した見

---

[20] 防衛省 HP<https://www.mod.go.jp/j/policy/agenda/kihon02.html>.

[21] 「我が国及び国際社会の平和及び安全の確保に資するための自衛隊法等の一部を改正する法律（平成 27 年（2015 年）9 月 30 日法律第 76 号）」（通称 平和安全法制整備法）と「国際平和共同対処事態に際して我が国が実施する諸外国の軍隊等に対する協力支援活動等に関する法律（平成 27 年 9 月 30 日法律第 77 号）」（通称 国際平和支援法）の総称

[22] Michal N. Schmitt, *supra* note 6.

[23] 一例として、Gary Corn and Eric Talbot Jensen, “The Use of Force and Cyber Countermeasures” (2018)32-2 Temple International & Comparative Law Journal 127.

解が多く、Knut Dörmann、Nils Melzer らが代表的である[24]。また、国際人道法の大家でもある Yoram Dinstein もサイバー空間への適用に関し、論文を発表している[25]。その他の著作物としては、Heather Harrison Diniss[26]や Marco Roscinni[27] 等が武力の行使及び武力紛争に関わる法とサイバー作戦の関係について総合的に論じた著書を執筆している。このように、海外においては活発な研究が行われ、多数の先行研究が存在する一方で、日本国内においては、当該分野での先行研究数は多いとは言えない状況である[28]。

次に国内法分野の先行研究の状況であるが、自衛隊が行うサイバー作戦に関する研究は極めて少ない[29]。特に、有事におけるサイバー作戦に適用される国内法についての研究例は、管見の限りでは存在しない。元来、有事法制研究自体が戦後長らくタブー視されたこともあり、自衛隊法をはじめとする武力攻撃事態における国内法全般に関し、研究数自体がそもそも極端に少ない。加えて、サイバー空間が新しい領域であり、サイバー空間における安全保障概念及びそれに伴う法制度自体が形成途上であることも要因と考えられる。興味深い点は、前述のようにサイバー空間における国際法適用については、少数ながら日本人学者による先行研究が存在するのに対し、対応する国内法についての研究がほぼ存在しないという点である。当該事実が国際法と国内法の研究が別々に行われおり、両者に乖離が生じていることを雄弁に物語っていると考えられる。

これまで述べてきた先行研究に対する評価を踏まえるならば、自衛隊が行うサイバー作戦の法的課題を国際法及び国内法の双方の観点から研究した論文として、本稿は新規性及び有益性があるものと思料する。

Ⅱ　サイバー空間における軍事作戦の概要

2.1　軍事作戦としてのサイバー作戦

---

[24] それぞれの著作について Knut Dormann,　“Applicability of the Additional Protocols to Computer Network Attacks” *Internati　onal Committee of the Red Cross* (November 19, 2004), online: ICRC <https://www.icrc.org/en/doc/reso urces/documents/misc/68lg92.htm>; Nils Melzer, “Cyberwarfare and International Law” *The United Nations Institute for Disarmament Research* (February 11, 2011), online: *UNIDIR* <https://unidir.org/publication/cyberwarfare-and-international-law>.

[25] Yoram Dinstein, “Computer Network Attacks and Self Defense” (2002)76, in Michael N Schmitt and Brian T. O’Donell, eds, International Law Studies: Computer Network Attack and International Law 99.

[26] Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge: Cambridge University Press, 2012).

[27] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford: Oxford University Press, 2014).

[28] 国内におけるサイバー作戦に関わる国際法研究としては、岩本誠吾「サイバー問題における国際法の課題」外交第 24 巻 88 頁（2014）及び河野桂子「サイバー攻撃に対する自衛権の発動」江藤淳一編『国際法学の諸相：到達点と展望:村瀬信也先生古稀記念』（信山社、2015 年）等が存在するが、極めて少数である。

[29] 自衛隊の行うサイバー作戦に関連する国内法を取り扱った研究は管見の限り福留俊幸「サイバー対抗措置の可能性と限界」防衛法研究第４０号（防衛法学会、2016）のみである。

本章では、法制度上の問題点を論じるにあたって、その前提となる軍事作戦としてのサイバー作戦の概要について説明する。まず、サイバー作戦が実行される作戦環境は、基本的には論理的な仮想空間であり、他の領域の作戦とは大きく異なる特性を有することへの理解が必要である。また、サイバー作戦は、平時から有事にかけてのあらゆる紛争スペクトラムで使用され[30]、軍事作戦のみで使用されるものではなく、実行主体も、軍隊に留まらず、情報機関や警察組織が行う場合もある。このため、法の適用を考えるにあたっては、まず作戦環境としてのサイバー空間の特性及び軍事作戦としてのサイバー作戦の特性を理解することが必要である。

本稿は自衛隊が行うサイバー作戦に関する研究であり、本来は自衛隊のサイバー作戦について説明を行うべきであるが、現状として自衛隊に配置された各種サイバー部隊の活動についての詳細は公表されていない。このため、各国のサイバー部隊及びサイバー作戦等に関する教範等を参考にせざるを得ない。各国のサイバー組織の在り方は国によって様々であり、任務・権限もそれぞれ異なっている。このため、一様にサイバー作戦として一括りにし、自衛隊に当てはめることは難しい。しかしながら、サイバー作戦はやや特殊な機能であり、教義や運用場面に類似性があると考えられること、特に西側諸国の軍隊では、作戦環境の捉え方、目的・組織・権限等の教義に関する点で多くの共通点が見られることから、自衛隊が行うサイバー作戦を検討する上で外国のサイバー作戦に関する教義を確認することは十分に参考になると考えられる。このため、本章では米軍及び北大西洋条約機構（以下、「NATO」と略する。）等の教範を中心としたサイバー作戦環境への認識、サイバー作戦の目的及び区分等について概要を説明する。また、軍事的なサイバー作戦の背景事項であり、教義とも密接な関係を有するサイバー抑止概念との関係についても言及する。

2.2 サイバー作戦環境

サイバー空間は、他の領域と異なり、人工の仮想空間である。サイバー空間における存在は論理的なものであり、物理的な位置とは必ずしも一致しない。従って、地理的な意味での境界が存在せず、速度や時間を超越して行動可能である。一方で、実際にサイバー空間を構成する物理的構成要素を考え

[30] 米国国家情報会議が発行する情勢見積では、今後２０年にわたる予想において、サイバー作戦があらゆる紛争スペクトラムにおいて大きな考慮事項となることを示唆する。*See* U.S. National Intelligence Council, “Global Trends 2040: A More Contested World” (March 2021), online: ODNI <https://www.intelligence.gov/publics-daily-brief/public-s-daily-brief-articles/1055-national-intelligence-council-releases-global-trends-report-on-the-more-contested-world-of-2040>, p. 104.

た場合、常にいずれかの所有者が存在する空間でもあり、空間への侵入は当該領域の所有者によるアクセス制限が存在する。この点で陸・海・空・宇宙のような物理的かつ公的領域が存在する領域とは大きく異なる。サイバースペースは、米軍及び NATO 軍のマニュアルでは、物理層、論理層、及び Cyber-persona 層の３層で説明できるとされる（図１参照）[31]。

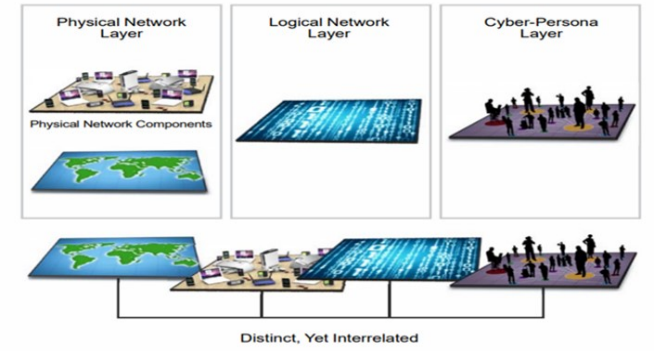

図１「サイバー作戦環境」

U.S. Joint Chiefs of Staff,“ Joint Publication JP 3-12 Cyberspace Operations”(June 2018)より引用

最後の Cyber-persona 層は、バーチャルな人格を表す層であり、実在の人物や組織で構成されるのではなく、電子メールアドレス、ユーザーID、ソーシャルメディア・アカウント等を指す。このため、一人の人間や組織が複数の Cyber-persona を持つことができる。逆に、複数の人格または組織が、実際はたった一人によって保有・運用されている場合もある。サイバー空間は、これらの３つの層の結びつきで構成されており、理論上は各層ごとに区分して考察することは可能ではある。しかしながら、実際は様々な要素が極めて複雑に入り組んでおり、明確にそれぞれの層を区分することは困難である。特に、論理的な概念である IP アドレスやドメイン名が物理的な位置や人物を表しているわけではないことは注意が必要である。一例として、外国のドメイン名を有するデータの論理的所在地が物理的には国内のサーバに存在する場合や、IP アドレス、FQDN[32]が偽装されているケースはごく一般的に存在する。また、各国間で送受信されるデータは複数の国家のサイバーインフラを通過することから、どの時点でどの国にデータが位置するかを判別することは極めて困難である。加えて、犯罪等で使用される匿名プロキシサーバ等の活用により通信伝達経路自体も隠蔽される場合が多く、追跡は困難である。法律上は、地理的概念で国外と国内を区別し、それぞれ国際法、国内法の領域と

[31] *See* JP 3-12, *supra* note 1. *See also* U.K. Ministry of Defence, “Allied Joint Doctrine for Cyberspace Operations ”(2020), online: U.K. Ministry of Defence <https://www.gov.uk/government/publications/-allied-joint-doctrine-for-cyberspace-operations-ajp-320>, hereinafter AJP-3.20.

[32] FQDN： Fully Qualified Domain Name「完全修飾ドメイン名」

する。しかし、上記特性を有するサイバー空間において、実務上一つの情報を国外・国内で区別することは極めて難しい問題である。そこで米軍及びNATO は、サイバー空間を単純化し、所有権に基づく区分を用いる。自国政府やパートナーに所属し、主に防護対象となる論理空間を Blue Cyberspace と表現し、逆に敵対組織が所有又は支配する論理空間を Red Cyberspace と表現する。Blue と Red のどちらにも当てはまらないすべてのサイバースペースは、Grey Cyberspace と呼ばれる[33]。

前述の通り論理、物理及び Cyber-persona の各層では所有者や人格が一致しない可能性があり、法の適用にあたって上記分類がそのまま適用できるかは検討を要する。しかしながら論理的には非常に明快であり、軍事的なサイバー作戦の特性を理解する上で有益な概念と考えられる。すなわち、Blue Cyberspace は自軍陣地を、Red Cyberspace は敵軍陣地を、そしてその間に彼我が明確でない Grey Cyberspace が広がっているという状況である。しかしながら、通常の軍事作戦では彼我の物理的な境界は比較的明快であるが、サイバー空間においてはその境界は極めて不鮮明であり、Blue Cyberspace の中に Red Cyberspace が混在する場合や、Grey Cyberspace にもレッド寄りの場合やブルー寄りの場合が存在し、かつその色が日替わりで変化するという事態も考え得る。実際に目視で確認することが出来ないため、その把握は他の軍事作戦に比し難しいと言える。この作戦環境の特殊性がサイバー作戦に他の軍事作戦と異なる様々な特色を持たせている。

一般的なサイバー作戦の特色として、次のようなものが考えられる[34]。

① 脅威の幅広さ

サイバー攻撃は、これまでの通常の軍用兵器と異なり、誰でも、どこからでも攻撃が行えるという特性が挙げられる。このため、サイバー空間における脅威の主体は、軍隊及び情報機関等の国家機関から個人の犯罪者に至るまで極めて幅広であり、その事が法的整理を困難にする。

② 匿名性・帰属の困難性

Cyber-Persona が現実の人物とは必ずしも一致しないことや、地理的な特定が困難であることは、そのままサイバー空間の高い匿名性に繋がっている。この匿名性は、軍事作戦としてサイバー作戦を発動するにあたっての前提となる法的判断に大きく影響する。すなわち、行為の責任を国家に帰属させる行為、帰属（以下、「attribution」と略する。）の困難性という問題である。

③ 地理的無制限性

物理空間では、基本的に地理的境界により国際法と国内法の適用が区分さ

[33] *See* JP 3-12, *supra* note 1.

[34] *See* JP 3-12, *supra* note 1. *See* also AJP-3.20 *supra* note 31.

れる。しかしながら、サイバー空間においては国内と国外の切り分けは簡単ではない。海底ケーブルの陸揚局等の物理層で区分することは理論的には明快ではあるが、地理的概念を超えて広域に分散された大量のデータの存在や、様々な経路において高速にやり取りされるパケット通信等の性格を考慮すれば、物理層をそのまま法の適用区分とすることは現実的ではない。実際、近年においては外国からのサイバー攻撃であっても攻撃対象国の国内に拠点を設け、国内通信基盤を活用して攻撃を実行するパターンも存在し[35]、作戦上も物理層を基準に国内と国外を切り分けること難しくなっている。

④　民間セクターの協力

現実のサイバー作戦は民間セクターの協力が不可欠であり、実態としてほぼすべてのサイバー作戦に民間セクターの技術者（あるいは犯罪者）が関与する。人だけでなく、使用される通信インフラも大半が軍民共用である。武力紛争間においては、文民と戦闘員あるいは民用物と軍事目標を明確に区別することが求められるが、サイバー作戦ではその識別は極めて難しく、複雑な法的問題を生起させる[36]。

これらのサイバー作戦の特色は、サイバー空間における法規制を極めて複雑な問題とするとともに、後述するサイバー抑止政策にも大きな影響を及ぼしている。

2.3　サイバー作戦の目的と軍隊の任務・権限

軍隊内のサイバー組織の任務は、一般的には軍隊内のネットワークの安全確保・防護、軍が行うその他の軍事作戦の支援及びサイバー作戦単独での直接的軍事効果の獲得等が考えられる。さらには重要インフラを始めとする国

---

[35] James Baker and Matt Morris “Defend Forward and the FBI”, in Jack Goldsmith, ed., *The United States' Defend Forward Cyber Strategy - A Comprehensive Legal Assessment* (Oxford: Oxford University Press, 2022) 114 at 122.

[36] その他一般的に言われる特性として、攻撃の優位性がある。これは前述の匿名性により攻撃側は攻撃前に防御側の情報を十分に収集できるのに対し、防御側は殆ど攻撃者の情報を入手できないという情報の不均衡による。また、防御側の規模が大きくなるほど防護対象が拡大し、セキュリティが脆弱になるのに対し、攻撃側はどこか一ヵ所を突破すれば攻撃を成功させることができるという資源分配の問題でもある。すなわち、同じ資源を有していれば、攻撃側が圧倒的に有利である、というものである。川口貴久「サイバー領域における安全保障の現状と課題－サイバー領域の抑止力と日米同盟－」『平成 25 年度外務省外交・安全保障調査研究事業（調査研究事業）「グローバル・コモンズ（サイバー領域、宇宙、北極海）における日米同盟の新しい課題」』（公益財団法人日本国際問題研究所、2013 年）<https://www2.jiia.or.jp/pdf/resarch/H25_Global_Commons/03-kawaguchi.pdf.> 14 頁。サイバー空間における攻撃の優位性は川口を始め多くの者が指摘をしている。しかし、近年、防御技術の発達により、その差異は縮小しつつあるともいわれる。米国のシンクタンクである戦略国際問題研究所問題（Center for Strategic and International Studies, CISI）Jim Lewis は、ロシア-ウクライナ紛争において従来言われていた攻撃の優位性が効果的な防御により減じつつあることを指摘している。*See* James A. Lewis, “*Cyber War and Ukraine*” Center for Strategic and International Studies (June 16, 2022), online: CISI <https:// www.csis.org/analysis/cyber-war-and-ukraine>.

家サイバーインフラの防衛や犯罪対策、ディスインフォメーション対策等も軍に担わせる国も存在し[37]、その場合は外国だけでなく国内も対象とした幅広い情報収集活動が行われることになる。ただし、西側諸国の軍隊内サイバー組織が行うサイバー作戦の主たる対象は飽くまで国外からの脅威であり、国内に対しては情報収集・監視等の抑制的な作戦に留まる場合が多い。一例として、米国では国内の重要インフラ防護は国土安全保障省（United States Department of Homeland Security: DHS）隷下のサイバーセキュリティ・社会基盤安全保障庁（Cybersecurity and Infrastructure Security Agency: CISA）、サイバー犯罪への対応は司法省隷下の FBI 連邦捜査局（Federal Bureau of Investigation: FBI）が担っており、国内における Cyber Command の関与は上記組織への情報共有を含む支援的任務を行うにとどまる[38]。フランスにおいても国防省隷下のサイバー防衛軍（Commandement de la cyberdéfense）は国防省内ネットワークの防護、軍事作戦支援及びディスインフォメーション対応含む情報作戦の任務を有するが、国内では特別な権限は保有していないとされる[39]。この点では、英国の体制は独特であり、2020 年に設立された国家サイバー部隊（National Cyber Force: NCF)は、政府通信本部（GCHQ）、国防省、秘密情報部（SIS）から人員を集めた集合体組織であり、英国に対する脅威からの防衛、英国の外交・安全保障政策の推進、軍事作戦支援、重大犯罪の防止等の幅広い任務を有し、任務及び状況に応じて権限を使い分ける形となっている[40]。

2.4 サイバー作戦の区分

サイバー作戦に適用される法体系を考える際に、サイバー作戦をどのような区分で整理するかは極めて重要な課題である。サイバー作戦は、平時から武力紛争までのすべての紛争スペクトラムで行われる作戦であり、様々な区分が考えられる。一般的に軍事作戦は、目的・形態・態勢等により区分されるが、米軍では主に目的の観点からサイバー作戦を、以下のように区分する

---

[37] 一例として、米軍のサイバー作戦に関するマニュアルには、サイバー軍（U.S. Cyber Command、以下「Cyber Command」と略する。）司令官の任務として①国防総省内ネットワークの運用、安全確保、防衛、②サイバー空間における攻撃からの国家の防衛、③統合軍指揮官への必要なサイバー空間支援を定めている。*See* JP 3-12, *supra* note 1.

[38] 原則的に米連邦軍による国内法執行活動は The Posse Comitatus Act is a United States federal law (18 U.S.C. § 1385.)により禁止されている。

[39] The 2023 USCYBERCOM Legal Conference において仏国サイバー防衛軍法律顧問 Thomas Graindorge 氏より直接聞き取り（March 19,2023）。

[40] Gov.UK, “The National Cyber Force: Responsible Cyber Power in Practice”(March 2023), online: Gov.UK <https://www.-gov.uk/government/organisations/national-cyber-force>.

（図２参照）[41]。

① 国防総省内のネットワークにおけるセキュリィティ確保を狙いとした活動（The Department of Defense Information Network operations: DODIN)、
② Blue Cyberspace 及び Grey Cyberspace(国防総省及び防護対象ネットワーク）を特定の脅威からを防護すること目的とした防勢的サイバー作戦（Defensive Cyberspace Operations: DCO)
③ Red Cyberspace において、当該ネットワークの所有者に不利益を与える攻勢的サイバー作戦（Offensive Cyberspace Operations: OCO)。

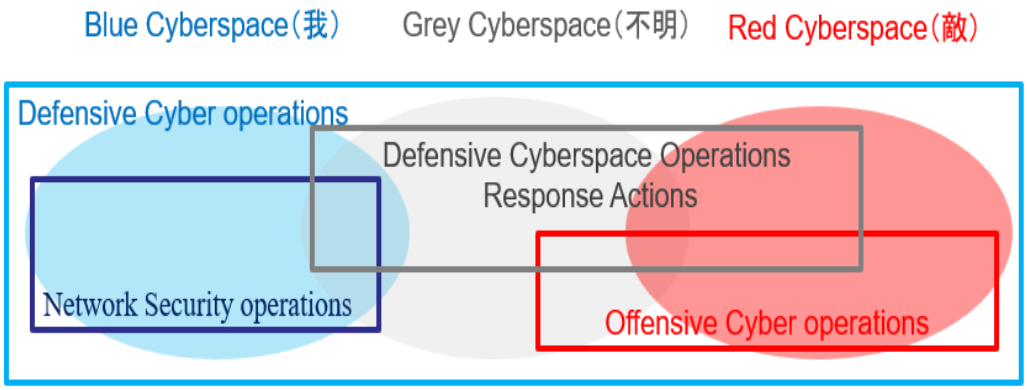

図２「サイバー作戦の区分」

このうち、②の防勢的サイバー作戦は、脅威への対応として、Red Cyberspace に侵入して行う防御的サイバー作戦対応行動（Defensive Cyberspace Operations Response Actions, DCO-RA）を含む。これには、敵システムの物理的損害や破壊を伴う「武力の行使」レベルの行動が含まれる場合があるとされる[42]。他の軍事作戦と同様に考えれば、①及び②が防御行動に該当し、③が攻撃行動に該当することになるであろう。②のうち、相手側のネットワークに侵入した行う DCO-RA は、いわゆる Active Cyber Defense (以下、「ACD」と略する。)[43]及び前方防衛の概念を具体化するものであると考えられるが、OCO とは異なるものと説明される[44]。しかし、OCO は、使用される手段は攻勢的サイバー作戦と重複するとされており、実態として外形上

[41] *See* JP3-12, *supra* note 1. *See also* AJP-3.20, *supra* note 31.
[42] *See* JP3-12, *supra* note 1.
[43] ACD の概念の詳細について次章を参照
[44] OCO は、「サイバー空間における現在進行中または差し迫った脅威から Blue Cyberspace を防衛する以外の目的で、指揮官の意思により Blue Cyberspace の外で実施されるすべての CO ミッションは、OCO ミッションである」、と説明される。*See* JP3-12, *supra* note 1.

区分することは困難である。ACD 及び前方防衛において、どのような手段が法的に許容されるかという点は依然として多くの議論が存在する[45]。

次に、主に攻撃様相の観点から過去の大規模サイバー攻撃事案を分類すると、大きく以下５つの類型に区分されると考えられる。

① espionage:知的財産の窃取を含む情報収集活動
② 犯罪支援：金銭収奪目的のランサムウェア攻撃、あるいは暗号資産窃取
③ 影響工作：有利な戦略環境情勢を狙いとした情報操作
④ 示威又は威嚇:外交目的達成のための明示的あるいは黙示的恫喝
⑤ 純軍事作戦：武力紛争における軍事的利益獲得のための軍事作戦

①の espionage は、最も日常的に行われている形態である。2020 年に米国で発生した SolarWinds[46]事案は espionage の典型的な例であり、バックドアの設置によるサプライチェーン攻撃により政府機密情報が窃取された。また、2014 年に発生した米国による中国人民解放軍 61398 部隊の起訴事案[47]では、知的財産を含むビジネスデータが対象となった案件であり、国家が政治・軍事目的以外での経済領域においてもサイバー作戦を活用していることが明らかになった。

②の犯罪支援は、国家が外国の領域において刑事犯罪に加担するというやや特殊なケースであるが、世界規模の被害が発生した 2017 年の WannaCry 事案[48]では、北朝鮮政府の支援を受けたハッカー集団 Lazarus Group による犯行と推測され、米国が公式に非難する事態となった[49]。同グループは 2016 年のバングラデシュの中央銀行からの通貨窃取への関与も疑われており、日本でも同グループの関与が疑われる被害が発生したことから、日本政府も公式に

---

[45] 高橋郁夫「続アクティブサイバーディフェンスの概念」2022 年 9 月 19 日、株式会社 IT・リサーチアート<https://itresearchart.biz/?p=4167>。ただし、純粋に軍事作戦の概念から言えば、本来、作戦において許容される手段は最終的に達成すべき作戦目標及び作戦環境により軍が決定するものである。具体的には、作戦の都度政治的・法的要素を含めて作成された部隊行動基準（ROE）が命令（自衛隊の場合、自衛隊は行政機関であるので、命令の位置付けは行政法上の通達等に該当することになる。）として示され、当該命令により細部の権限が律せられる。作戦の種類に応じて異なる手段が法的に規定されるものではないことは理解が必要である。簡単に言えば、法は軍が作戦を行う是非等の大枠を定めるものであり、作戦における手段等を法律で律するということは通常はあり得ないということである。

[46] NATO Cooperative Cyber Defence Centre of Excellence International Cyber Law: Interactive Toolkit, “SolarWinds_(2020)” online: CCDCOE <https://cyberlaw.ccdcoe.org/wiki/SolarWinds_(2020)>.

[47] NATO Cooperative Cyber Defence Centre of Excellence International Cyber Law: Interactive Toolkit, “Chinese_PLA_Unit_61398_indictments_(2014)”, online : CCDCOE <https://cyberlaw.ccdcoe.org/wiki/Chinese_PLA_Unit_61398_indictments_(2014)>.

[48] NATO Cooperative Cyber Defence Centre of Excellence International Cyber Law: Interactive Toolkit “WannaCry_(2017)”, online : CCDCOE <https://cyberlaw.ccdcoe.org/wiki/WannaCry_(2017)>.

[49] Gregory Korte, “White House plan to 'shame' North Korea shows complexities of responding to cyberattacks” (December 19, 2017) *Usa Today,* online : USA TODAY<https://www.usatoday.com/story/news/politics/2017/12/19/white-house-strategy-punish-north-korea-wannacry-attack-were-going-shame-them/964116001/>.

非難を行っている[50]。

③の影響工作は、いわゆるディスインフォメーション活動等による情報操作として行われるサイバー作戦であり、2016 年及び 2018 年の米国大統領選への選挙介入が著名な例である[51]。また、2014 年及び 2021 年のロシア - ウクライナ紛争でも、武力紛争中の他の軍事作戦と連携する形で情報操作型のサイバー攻撃が行われている。これらの軍事的利益の追求を目的として行われる情報操作は一般的には情報作戦と言われるが、その定義や影響工作との差異は明確ではない[52]。本稿では情報機関等が政治的目的で行う情報操作を影響工作、軍が主に武力紛争間に軍事的利益追求で行う情報操作を情報作戦と区分する。情報作戦は、戦略環境の醸成というよりは、直接的な軍事的利益獲得の観点が強いことから、⑤の類型に分類されると考えられる。ロシア - ウクライナ紛争における情報操作は両類型が混在していると考えられる。

④の示威又は威嚇行動として典型的な例は 2007 年に発生したエストニアへの大規模 DDoS 攻撃である。本事案は、本格的な国家規模での被害を生じたサイバー攻撃の最初の例であり、発端となった対独戦勝記念の銅像の移動問題をめぐる政治的摩擦や、徐々に高度化した DDoS 攻撃の手法からロシア政府の関与が疑われた[53]。また、2014 年に発生した北朝鮮を風刺した映画の公開を巡るソニーピクチャーズ事案では、攻撃対象は国家ではなく映画配給会社であったが、国家による他国に対する政治的圧力の手段としてサイバー作戦が使用されたとも言えることから当該ケースに分類されると考えられる。また、最も著名なサイバー攻撃事案である Stuxnet 事案は、過去のサイバー攻撃において唯一「武力の行使」に該当する可能性があると考えられている例であるが、イランの核開発の停止又は遅延が目的とされており、武力紛争とは無関係に実行されていることから分類としては本類型に区分されると考えられる。

⑤の純軍事作戦等は、まさに現在継続中のロシア - ウクライナ紛争におけ

---

[50] *Supra* note 5. なお、日本政府による非難の詳細については以下を参照。NHK サイバー取材班「日本政府が名指し 北朝鮮ハッカー「ラザルス」とは何者か？」2022 年 11 月 14 日、NHK　NEWS WEB　<https://www3.nhk.or.jp/news/-html/20221114/k10013890411000.html>。

[51] 2016 年米大統領選への選挙介入については、*See* Samuli Haataja, *supra* note 7 at 167-191. 川口貴久「ロシアによる政治介入型のサイバー活動～2016 年アメリカ大統領選挙介入の手法と意図～」2020 年 3 月 30 日、国際情報ネットワーク分析 IINA・笹川平和財団<https://www.spf.org/iina/articles/kawaguchi_01.html>。2020 年については、U.S.National Intelligence Council, “Foreign Threats to the 2020 US Federal Elections”(March 10, 2021) , online: ODNI <https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf>.

[52] 当該類型に関しては、影響工作又は影響作戦（influence operation）、情報作戦(information operation)、情報戦(information warfare)及び認知戦(cognitive warfare)等の用語が混在し混乱が生じているが、基本的にはいずれもネットワークを通じた心理戦の派生型と考えられる。定義については注 7 を参照。

[53] NATO Cooperative Cyber Defence Centre of Excellence, “Cyber attacks against Estonia (2007), ” online: CCDCOE <https://cyberlaw.ccdcoe.org/wiki/Cyber_attacks_against_Estonia_(2007)>.　*See also* Samuli Haataja, *supra* note 7 at 111-135.

る両国のサイバー作戦が典型的例として考えられる。しかし、他の類型に比較し、当該類型に該当する例は極めて少なく、2008 年のジョージア紛争[54]及び 2016 年に米国が ISIS に対し行った Operation Glowing Symphony [55]が確認できる程度である。一方で、ロシア - ウクライナ紛争におけるサイバー作戦の様相は、現代の武力紛争がサイバー作戦抜きでは考えられないことを示唆しており、自衛隊にとっても極めて重要な類型である。

上記分類は、網羅的ではなく、重複等も考えられる。特に、サイバー作戦は多くの場合詳細が不明であり、正確な分類は困難である。一例として 2017 年にウクライナを中心として発生した NotPetya[56]では、使用されたウイルスは、ランサムウィルスの外形を有し、ターゲットコンピュータのハードディスクを暗号化して、ビットコインで身代金を要求するものであった。この場合は②の類型となる。一方で、被害者が身代金を支払っても、攻撃者はこれを復号化する仕組みがなかったことから、身代金目的であるランサムウェアのビジネスモデルとして破綻しており、ロシアによるウクライナへの経済的混乱の作為等の別の意図が推測されている[57]。この場合は④の類型にあたる。あるいは 2014 年より続くロシア - ウクライナ間の国際武力紛争の一環としておこなわれた軍事作戦と考えれば⑤にも該当することになる。このような現実の複雑さや、そもそも国家が行うサイバー作戦の大部分が国家機密に該当するため正確な事実確認ができないことも相まって、現実的にサイバー作戦の正確な分類を行うことは極めて困難ではある。しかしながら法適用を考察するにあたっては、ある程度単純化し類型に区分すること有意義であると考え、上記区分化を行った。

2.5 小　結

本章は、法的検討の前提となる、軍隊が行うサイバー作戦の作戦環境上の特性及び作戦区分について分析を行った。特にサイバー作戦環境が、陸海空の他の領域と異なり、物理世界と仮想世界で不一致があることは十分に認識をすることが必要である。サイバー空間における領域区分は論理的な区分で

---

[54] NATO Cooperative Cyber Defence Centre of Excellence, “Georgia Russia conflict (2008), ” online : CCDCOE <https://cyberlaw.ccd coe.org/wiki/Georgia-Russia_conflict_(2008)>.

[55] NATO Cooperative Cyber Defence Centre of Excellence, “Operation Glowing Symphony (2016),” online : CCDCOE <https://cyberlaw.ccdcoe.org/wiki/Operation_Glowing_Symphony_(2016)>.

[56] NATO Cooperative Cyber Defence Centre of Excellence, “NotPetya_(2017)”, online: CCDCOE<https://cyberlaw.ccdcoe.org/wiki/NotPetya_(2017)#cite_note-2>.

[57] 川口貴久「国家が支援するランサムウェア：2017 年の WannaCry と NotPetya の意図に関する分析（前編）」2021 年 3 月 19 日、国際情報ネットワーク分析、IINA・笹川平和財団 <https://www.spf.org/iina/articles/kawaguchi_02.html>。

あり、現実の地理的境界とは異なる。特に、国外と国内の区分が曖昧であることは、サイバー空間における法適用を考える上で国際法と国内法を同時に考察することを要求するものであり問題が複雑化し易いと考えられる。

Ⅲ　サイバー空間における抑止理論

3.1　サイバー抑止論の意義

上記分類においても明らかであるが、サイバー作戦の特性が最も有効に活用できるのは平時からＧＺ事態の間である。実際、著名なサイバー攻撃事案の殆どが武力紛争以外の状況で生起しており、安全保障上の観点からのサイバー脅威への各国の関心は、平時からＧＺ事態における武力攻撃の烈度に至らない、すなわち自衛権発動の対象とならない外国からの有害なサイバー攻撃にどのように対処するかということが中心となっている。このような文脈において、いかに敵対国がサイバー攻撃を行うことを思い留まらせるかという、いわゆるサイバー抑止は重要な論点であり、安全保障及び立法政策に大きな影響を及ぼす要素である。本章では、サイバー抑止理論に関する先進国である米国の議論を確認し、サイバー抑止理論が日本の安全保障及び立法政策に及ぼす影響を考察する。

3.2　米国におけるサイバー抑止理論の発展

3.2.1 オバマ政権以前

第二次世界大戦以降の抑止の概念は、主に冷戦期の核戦略と結びつけられ発展してきた[58]。しかし、冷戦が終結して超大国間の核戦争の脅威が薄れるにつれ抑止理論は他の問題領域へと拡がり、インターネットの普及に伴い安全保障への懸念が広がりつつあったサイバーセキュリティの分野にも応用されるようになったとされる[59]。特に米国では活発にサイバー抑止に関する議論が行われ、様々な研究成果の蓄積がなされている。一方、日本においては抑止概念が核戦略と結びつけて考えられることが多く、唯一の被爆国という

[58] 川口貴久「米国におけるサイバー抑止政策の刷新 : アトリビューションとレジリエンス米国におけるサイバー抑止策」KEIO SFC JOURNAL15 巻 2 号(2015)、80 頁。
[59] 栗田真広「サイバー攻撃に対する「抑止」の現状 ―米国の安全保障政策の事例から―」『情報通信をめぐる諸課題・科学技術に関する調査プロジェクト調査報告書』(2014)、158 頁。

歴史的経緯もあり多くの者が核に対する拒絶反応を示す中で、抑止理論そのものに関する議論・研究は戦後長らく不活発な状態が続いた[60]。近年、日本においてもサイバーセキュリティに関する懸念が深まるにつれ状況は変化しつつあり、サイバー抑止に関する研究や議論が徐々にではあるが行われるようになってきているものの[61]、議論の多くは米国のサイバーセキュリティ政策等の発表に併せた一過性の現象に過ぎない観もあり、日本の政策としてサイバー抑止に関する真面目な議論が蓄積されているとは言い難いと感じる。しかしながら、能動的サイバー防御構想の発表をうけ、日本においてサイバー抑止に関する議論が今後活発化する可能性は十分にあり、サイバー抑止とサイバー作戦の関係を確認することは重要と考える。なお、サイバー抑止とは、白紙的には①サイバー攻撃以外も含めた脅威全般に対するサイバー作戦による抑止、②サイバー攻撃の脅威に対するサイバー作戦による抑止、③サイバー攻撃の脅威に対するサイバー作戦以外の手段を含めた抑止、の３つの意義合いを有すると考えられるが、本稿では、主に②のパターンにおけるサイバー抑止を焦点とする。

抑止の概念として、米軍では「受け入れがたい対抗措置を取るという信頼性のある威嚇か、ある行動を取るコストが予期される利得を上回るとの考えによって、その行動を防止すること」として定義付けている[62]。一般的に抑止戦略には、拒否的抑止と懲罰的抑止という二つの要素があると考えられている[63]。ここでいう、懲罰的抑止とは、「耐えがたい打撃を加える威嚇に基づき、敵のコスト計算に働きかけて攻撃を断念させるもの」であり、拒否的抑止とは、「特定の攻撃的行動を物理的に阻止する能力に基づき、敵の目標達成可能性に関する計算に働きかけて攻撃を断念させるもの」であるとされる[64]。冷戦時代は、弾道ミサイル迎撃の困難性等により懲罰的抑止が主流の概念であった。しかし、核抑止理論に基づく懲罰的抑止をサイバー空間に応用することに関しては、様々な疑問が提示された[65]。その主な理由は、サイバー空間に特有の攻撃の優位性、attribution の困難性といった観点から懲罰的抑止は有効に機能し得ないのではないか、という疑念であった[66]。また、懲罰的抑止が効果を発揮するためには、何が許され、何が禁止されるのかの規範が必

---

[60] 後瀉桂太郎「抑止概念の変遷 ― 多層化と再定義 ―」海幹校戦略研究 5 巻 2 号(2015)、21 頁。
[61] 川口・前掲注 36。
[62] U.S. Joint Chiefs of Staff, *Joint Publication 3-0: Joint Operation* (August 2011).
[63] Martin C. Libicki, “Cyberdeterrence and cyberwar” (2009), online: RAND <https://www.rand.org/pubs/monographs/MG877.html>.
[64] 「平成 22 年度版防衛白書」(2010)、263 頁。
[65] リチャード・クラーク、ロバート・ネイク（北川知子ほか訳）『核を超える脅威 世界サイバー戦争：見えない軍拡が始まった』（徳間書店、2011 ）、228 頁。
[66] 栗田・前掲注 59、161 頁。

要とされる。しかし、サイバー空間における国際法及び国際規範[67]は形成途上であり、未だに明確でないことも理由として指摘されている[68]。

このため、米国においては、オバマ政権以前は Blue Cyberspace における活動を主体としたセキュリティ強化等による拒否的抑止が主流の考えとなっていた[69]。このような流れで具体化されたものが、「積極的サイバー防衛（active cyber defense（以下、「ACD」と略する。））」であるとされる。2011 年に発表された「サイバー空間における作戦に係る国防総省戦略」（2011.7）は、国防総省は、「国防総省のネットワーク及びシステムへの侵入を予防し、侵入した敵対行為を打破する積極的なサイバー防衛を展開する」とし、ACD を「脅威と脆弱性を発見し、検知し、分析し、被害を低減するためのシンクロナイズドされた、リアルタイムの能力」と定義する[70]。この時点では ACD とはサイバー攻撃を事前に検知することにより阻止を図る拒否的抑止の範囲での概念であったと考えられる[71]。つまり、当時の ACD の概念は飽くまで国防総省ネットワークの境界部での脅威の早期発見であり、レッドサイバーゾーンに踏み込んだ作戦を行うものではなかったと考えられる[72]。しかし、ACD という用語の意味はその後徐々に変遷し、bot-net の take down や White-hat Ransomware の使用、さらには搾取された情報を取り返す hack back にまで含む概念として使用される場合もあるなど[73]、定義に混乱が見られる[74]。このため、ACD という用語の使用には十分な注意を要すると考える[75]。

また、サイバー空間における拒否的抑止力のメカニズムには大きな弱点が存在することが指摘されている。すなわち、どれだけ強固な防衛力を整え、攻撃側が得られる利得を極限まで小さくしたところで、サイバー空間におい

---

[67] ここで言う国際規範とは、国家による責任ある行動に関する拘束力のない自発的な規範のことであり、具体的には 2015 年の第 4 回国連国際連合（以下「国連」と略する。）政府専門家会合（the Group of Governmental Experts (GGE)）報告書に記載された内容等を指す。*See* UN Doc. A/70/174 (July 22, 2015).

[68] U.S. Congressional Research Service,"Cybersecurity: Deterrence Policy"(January18, 2022), online: CRS <https://crsreports.congress.gov/product/pdf/R/R47011> at 9.

[69] 川口・前掲注 36、18 頁。

[70] U.S. Department of Defense, "Department of Defense Strategy for Operating in Cyberspace" (July 2011), online: DoD <https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf > at 7.

[71] 川口・前掲注 58、84 頁。

[72] Jeff Kosseff, "The Contours of 'Defend Forward' Under International Law"(June 2019), online: CCDCOE < https://ccdcoe.org/uploads/2019/06/Art_17_The-Contours-of-Defend-Forward.pdf> at 3.

[73] Center for Cyber and Homeland Security(CCHS) "Into the Gray Zone: The Private Sector and Active"(October 2016), online: CCHS <https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/CCHS-ActiveDefenseReportFINAL.pdf>.

[74] 佐々木勇人「「積極的サイバー防御」（アクティブサイバーディフェンス）とは何か ―より具体的な議論に向けて必要な観点について―」JPCERT/CC Eyes 2022 年 9 月 21 日、JPCERT/CC＜https://blogs.jpcert.or.jp/ja/2022/09/active-cyber-defense.html＞。

[75] 日本の能動的サイバー防御構想も ACD と訳されるが、後述する前方防衛と混同される場合も多く、用語の定義の混乱がさらに日本の能動的サイバー防御構想を不明確なものとしている可能性は否めない。

ては、攻撃を実行するコストが低く、攻撃を思い留まる要因にはならないということである[76]。このため、その後の報復を可能にする attribution 能力の向上等も相まって、米国は再び懲罰的抑止の概念を取り入れるようになる。前述の「サイバー空間における作戦に係る国防総省戦略」のわずか４か月後に公表された同じく国防総省の政策文書「国防総省サイバー空間政策報告」（2011.11）には、「サイバー空間における抑止力は、他の領域と同様に、敵対者の目的を否定することと、必要であれば敵対者の攻撃に対してコストを課すという 2 つの主要なメカニズムに依存する。」とし、サイバー空間での抑止が、懲罰的抑止と拒否的抑止の両方の形態を取り得ることを明示している[77]。特に、特筆すべき点は、「大統領は、サイバー空間における敵対行為から我が国、同盟国、パートナー、および我が国の利益を守るために、あらゆる必要な手段を用いて対応する権利を留保する。」とし、「大統領の指示により、対応オプションには、国防総省が提供するサイバーおよび物理的能力を使用することが含まれる。」とし、対応手段としてサイバー作戦だけでなく、通常の軍事作戦のオプションが含まれることを示唆した点である。こうした流れを受けオバマ政権下では、米国の安全保障、外交、経済を脅かす外国からのサイバー攻撃に対する、資産凍結、取引停止、渡航禁止等の制裁措置の発動が進むことになった[78]。

3.2.2　前方防衛及び継続的従事戦略

しかし、このような懲罰的抑止は、有効に機能していないという多くの批判にさらされることになる。上院軍事委員会委員長（当時）であったジョン・マケイン上院議員は、2017 年 3 月の公聴会において「（米国には）確固たるサイバー抑止政策がないため、敵対国は米国に対して比較的平気でサイバー攻撃を仕掛けることができる」とし、別の機会においても「米国の敵がサイバー空間で主導権を握る中、前政権（オバマ政権）は真剣なサイバー抑止政策と戦略を提示しなかった」 と繰り返し批判した[79]。 実際、オバマ政権下

---

[76] 栗田・前掲注 59、74 頁。

[77] U.S. Department of Defense, “Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934”(November 2011), online: DoD <https://irp.fas.org/eprint/dod-cyber.pdf> at 2.

[78] 川口・前掲注 58、87 頁。

[79] Joseph Marks, “Shoddy U.S. Cyber Deterrence Policy Emboldens Adversaries, Lawmakers Say”(March 2, 2017), online: Nextgov<https://www.nextgov.com/cybersecurity/2017/03/shoddy-us-cyber-deterrence-policy-emboldens-adversaries-law makers-say/135853/>; Morgan Chalfant, “McCain Hits Trump over Lack of Cyber Policy,” (August 23, 2017), online: The Hill <https://thehill.com/policy/cybersecurity/347660-mccain-hits-trump-over-lack-of-cyber-policy/>.

で実施された北朝鮮に対する経済制裁は有効な効果を発揮しているとは言い難く、北朝鮮は国際取引所や暗号通貨取引所を標的としたサイバー作戦により核および弾道ミサイル開発に関する資金を継続的に獲得しているとみられる。経済制裁だけでなく、米国内法による訴追や public attribution といったその他の制裁措置も十分な効果をあげているとは言い難い[80]。訴追に関し、Garrett Hinck と Tim Maurer は、「既存の記録に基づいて、外国のハッカーやオンライン影響力の運営者に対して刑事告発を行うことは、敵対者にさらなる悪意のある活動をやめるように説得するのに十分なコストを課すようには見えない」と結論付ける。また public attribution に関しては、オバマ大統領自身が"何らかの形で公的な羞恥心が効果を発揮するという考えは、ロシアの思考プロセスをうまく読み取っていないと思う。"と疑問を呈している[81]。

この理由として、継続的従事戦略の主唱者である Michael P. Fischerkeller 及び Richard J. Harknett は、サイバー空間においては、抑止に関する戦略的曖昧性がその有効性を阻害していること、及び時間の経過が抑止を行う側にとって必ずしも有利とはならないことを指摘する[82]。まず、戦略的曖昧性であるが、抑止を有効たらしめるためには、抑止される側が、禁止された行為を行なえばかならず報復を受けるという確証を持つことが必要である。そのためには明確な基準や具体的な報復措置が明示される必要がある。しかし、それは同時に、抑止を試みる側は、抑止される側が基準を超えた場合、必ず報復を行わなければならない、という義務に拘束されることを意味する。米国は伝統的に抑止の実効性を減じてでも義務に拘束されることを嫌い、戦略的曖昧性を保持してきたと Michael P. Fischerkeller 及び Richard J. Harknett は主張する[83]。つまり、具体的な基準や報復措置を示さず、曖昧な態度に終始してきたことが、結果として低レベルのサイバー攻撃を誘発してきたということである。サイバー空間への国際法適用に関する国際的な議論においても、米国が拘束力ある条約の成立よりも拘束力のない国際規範の形成を重視していることは、この戦略的曖昧性への指向が影響している可能性は否定できない[84]。

---

[80] Tim Maurer and Garrett Hinck, “Persistent Enforcement: Criminal Charges as a Response to Nation-State Malicious Cyber Activity” (2020) 10 Journal of National Security Law and Policy 525.

[81] Politico,“Full Transcript: President Obama’s Final End-of-Year Press Conference”(December16, 2016), online: Politico <https://www.politico.com/story/2016/12/obama-press-conference-transcript-232763>.

[82] Michael P. Fischerkeller and Richard J. Harknett, "Initiative Persistence as the Central Approach for U.S. Cyber Strategy" the Institute for Defense Analysis (July 2021), online: IDA <https://ida.org//media/feature/publications/i/in/initiative-persistence-as-the-central-approach-for-us-cyber-strategy/d-22719.ashx> at. 7.

[83] *Ibid*.

[84] 実際、国際連合（以下「国連」と略する。）政府専門家会合（the Group of Governmental Experts (GGE) において議長アドバイザーを務めた Jim Lewis は、U.S. Cyber Command legal Conference (2023) において条約化を主張するロシアを牽制するため、米国が敢えて拘束力のない国際規範の成立を意図的に推進したと証言する。Jams Lewis, 2023 U.S. Cyber Command legal Conference Fireside Chat: Using Laws and Norms to Govern

総括すれば、敵対国から見れば、武力攻撃に匹敵する烈度のサイバー攻撃を行った場合、米国による強烈な報復が行われるかもしれない、という恐れはあっても、低強度のサイバー攻撃に対する米国からの報復措置に関しては、実行性が無いと判断している可能性があるということである[85]。

また、次の時間の経過が抑止を行う側にとって必ずしも有利とはならない、という点についてであるが、本来、経済制裁、起訴、public attribution といったソフトな制裁は、即効性は無いものの、影響は時間とともに累積し、相手の戦略を変更し得るコストに到達するという考えが理論的根拠となっている[86]。しかし、攻撃にほとんどコストが掛からないサイバー戦略環境では、時間の経過は、作戦を制約する方向ではなく、より作戦を継続し、戦略的利益を獲得する方向に働きかけることになる。逆に、経済制裁等の効果は制裁を受ける側が回避策を見出すにつれ効果は薄まっていく。このため、制裁の累積効果は、敵対国が武力衝突によらない継続的なサイバー作戦によって獲得する累積的利益を相殺することは不可能であるとする[87]。総括するならば、抑止の戦略的アプローチは、軍事化された危機や武力紛争において、敵が武力攻撃と同等のサイバー作戦やその他の軍事的武力行使を行うことを思いとどまらせる強制的アプローチとしては有効であるが、武力攻撃に至らない、低烈度のサイバー攻撃を抑止するためには無力であるというのが両名の結論である。

こうしたオバマ政権のサイバー政策への批判を受けて登場したのが、トランプ政権下の 2018 年に Cyber Command が公表した「サイバースペース優位の達成と維持（Achieve and Maintain Cyberspace Superiority）」において示された「前方防衛」概念及びその中核となる理論である「継続従事戦略」である[88]。当該文書は、サイバー空間が「優位性が常に危険にさらされる、活発で競争の激しい作戦空間」と捉え、優位性を維持するためには、「強靭性の増強」、「前方防衛」及び「常続的な関与（交戦）」が必要とする。その上で、「前方防衛」

Cyber, online Dvids (April 19, 2023) <https://www.dvidshub. net/feature/CYBERLEGAL2023>.

[85] Jams Lewis は、ロシア連邦保安庁とつながりのある対話者と議論した際、その人物が"（2016 年の）選挙干渉の後、米国の対応を待っていたが、何も起こらなかったので驚いた "と漏らしたと証言する。また、Lewis は、中国のある将軍が、サイバー空間で米国と交戦するリスクについて質問された際、米国には "偉大な能力があるが、意志がない "と答えたとも証言する。 James Andrew Lewis, “Strategy After Deterrence” Center for Strategic and International Studies (March 11, 2020), online: CISI <https://www.csis.org/analysis/strategy-after-deterrence>.

[86] *See* U.S. DoD, s*upra* note 79 at 6.

[87] *Ibid*, at 9. 経済制裁による効果に関する研究については *See* Gary Hufbauer, Jeffrey Schott, Kimberly Elliott and Barbara Oegg, *Economic Sanctions Reconsidered*, 3rd Edition (Washington, DC: Peterson Institute for International Economics, 2007).

[88] U.S. Cyber Command, “Achieve and Maintain Cyberspace Superiority Command Vision for US Cyber Command”(March 2018), online: Cyber Command <https://nsarchive.gwu.edu/document/16477-united-states-Cyber Command-achieve-and-maintain> at ６.

の概念として、「敵の活動の発信源にできるだけ近い前方で防御することで、敵の弱点を暴き、敵の意図と能力を知り、その発信源に近い場所で攻撃に対抗することができるようになる。」とする。「常続的な関与」に関しては、「戦術的な摩擦と戦略的なコストを敵に課し、敵の資源を防衛にシフトさせ、攻撃を減らすように仕向ける。」とともに、「持続的な行動と武力紛争のレベル以下での、より効果的な競争を通じて、敵の計算に影響を与え、侵略を抑止し、サイバー空間における許容できる行動と許容できない行動の区別を明確にさせることができる」とする[89]。

Michael P. Fischerkeller 及び Richard J. Harknett は、サイバー作戦の大半は、武力攻撃の閾値を下回る暗黙の「合意された競争」であり、継続的な交渉（交戦）を通じてサイバー空間における競争において、許容される行動と許容されない行動についての暗黙の了解が得られるとし、その暗黙の了解が米国の優位の維持とサイバー空間の安定化につながると主張する[90]。前方防衛及び継続的従事戦略の最も大きな特色は、平時からの常続的な Grey Cyberspace 及び Red Cyberspace におけるサイバー作戦の実行にあり、従来の Blue Cyberspace 周辺における拒否的抑止とソフトな制裁手段による懲罰的抑止施策から大きな変換を遂げたと評価できる。また、Cyber Command の作戦権限も見直された。従来は大統領政策指令 20 号（Presidential Policy Directive 20: PPD-20[91]）に基づき、他の政府機関の活動に影響を及ぼす等の重大な影響を及ぼすサイバー作戦は大統領の承認が必要であるとし、加えて他の政府機関の活動に影響を及ぼす作戦は、政府全体での調整が必要とされていた。しかし、2018 年に PPD-20 が廃止され、代わりに国家安全保障大統領覚書 13（NSPM13）に基づきより自由度の高い作戦権限が Cyber Command に付与されることになった。当該文書は非公開であるが、「武力の行使」または死や破壊、著しい経済的影響を引き起こすレベルに満たないサイバー作戦の場合以外は、これまで長期間を要したきた承認プロセスなしに軍が作戦を実行することが可能になったとされる[92]。

前方防衛及び継続的従事戦略の評価は定まってはいないが、Cyber

---

[89] *Ibid*.

[90] *See* Michael P. Fischerkeller and Richard J. Harknett, “Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace” Lawfare (November 9, 2018), online: Lawfare <https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace#>.

[91] U.S. government “Presidential Policy Directive/PPD-20” Federation of American Scientists(16 October 2012), online: FAS <https://irp.fas.org/offdocs/ppd/index.html>.

[92] Ellen Nakashima, “White House authorizes ‘offensive cyber operations’ to deter foreign adversaries”The Washington Post (September 20, 2018), online: The Washington Post <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>.

Command 司令官の Paul M. Nakasone 将軍は、FBI 及び CIA を始めとする国内関係機関と密接に連携し、2020 年の大統領選、2022 年の中間選挙の防衛に大きな成果を挙げたとする[93]。また、前方防衛及び継続従事戦略に基づき、パートナー国の要請を受けてサイバーセキュリティのエキスパートから構成されるハント・フォワード・チームを派遣するハントフォワード作戦[94]を実行し、また、ウクライナにもチームを派遣し、ウクライナ防衛に大きな成果を挙げているとする[95]。しかし、いずれも Cyber Command 側からの評価であり、客観的かつ正確な評価がなされるためには今しばらく時間が必要であろう。特に、前方防衛及び継続的従事戦略に対する法的評価は現在に至るまで定まってはおらず、国際法及び米国内法上の課題は引き続き議論が継続していることは注意を要する[96]。

また、前方防衛及び継続的従事戦略と抑止理論の関係についても依然として明確ではない。Michael P. Fischerkeller 及び Richard J. HarknettDoD は継続従事戦略は抑止戦略が有効でないことから生まれた、抑止戦略に「取って替わる」新たな戦略である、と主張する。また、DoD 及び Cyber Command も、前方防衛は、「サイバー抑止とは補完的ではあるが別の戦略である」、として考えているようである。しかしながら、White House 内の政策担当者は、「前方防衛は抑止施策の一部である」と考えているとも受け取れる発言をしており、混乱が見受けられる[97]。懲罰的抑止と拒否的抑止の間での揺らぎから、前方防衛及び継続的従事戦略の発表に至る米国のサイバー抑止理論の変遷をみると、抑止理論の先進国である米国においても、サイバー抑止に関する議論や政策が必ずしも一貫性をもって継続されてきたわけではなく、技術の進展や脅威の動向に影響を受け二転三転しならが進んできたこと、そして現在にいたるまで理論として確立しているものではないことが理解できる。

3.2.3 多層的サイバー抑止（Layered Cyber Deterrence）と新国家サイバーセキ

[93] U.S. Congress, "Statement of General Paul M. Nakasone commander United States cyberspace command Before the house committee on armed services subcommittee on intelligence and emerging threats and capabilities"(March 4, 2020), online CONGRESS.GOV <https://www.congress.gov/116/meeting/house/110592/witnesses/HHRG-116-AS26-Wstate-NakasoneP-20200304.pdf>.

[94] U.S. Cyber Command "CYBER 101: Hunt Forward Operations" (November 15, 2022), online : U.S. Cyber Command <https://www.cybercom.mil/Media/News/Article/3218642/cyber-101-hunt-forward-operations/>.

[95] U.S. Senate Committee on Armed Services, "Posture statement of General Paul M. Nakasone commander United States cyberspace command Before the 118th Congress senate committee on armed services"(March 7, 2023) , online: Senate Committee on Armed Services <https://www.armed-services.senate.gov/>.

[96] *See* Kosseff, *supra* note 72 at 5. 及び高橋・前掲注 45。

[97] トランプ政権下での John Bolton 国家安全保障担当補佐官の発言は明確に前方防衛を抑止に含めている。Sean Lyngaas, "White House announces federal cyber strategy, vows to go on offensive" CYBERSCOOPCyberscoop (September 20, 2018), online: SNG <https://cyberscoop.com/white-house-cyber-strategy-john-bolton-announcement/>.

ユリティ戦略

前述のような状況を受け、2019 年度米国国防権限法は、規範、拒否、抑止をめぐる政策の検討を明示的に指示[98]し、検討の枠組みとしてサイバースペース・ソリウム委員会が設立された。同委員会は 2020 年に最終報告書を連邦議会に対し提出、当該最終報告書の中で、重要な結果を生じるサイバー攻撃の蓋然性と影響を減少させる「多層的サイバー抑止（Layered Cyber Deterrence）」という戦略的アプローチを打ち出した。報告書では、多層的サイバー抑止の目的を達成するため、以下の３つ方針が推奨されている[99]。

① 行動の形成：パートナーと協力し、サイバー空間における各国等の行動に影響を及ぼす。
② 利益の拒否：重要なネットワーク（インフラや政府など）を保護し、サイバー空間における体系的なセキュリティと強靭性を生み出すため努力する。
③ コスト負荷：サイバー空間を利用して米国に損害を与える悪意ある行為者に対して報復を行う。

各方針は、政府の構造改革を基盤とし、その上にそれぞれ政策の層を構成するとしており、これが多層的サイバー防御の意味となっている（図１参照）。各層は更に６つの柱により具体化されている[100]。

基盤層：政府の構造改革
　柱①　米国政府のサイバー空間に関する構造・組織改革
第１層：行動の形成
　柱②　規範と非軍事的手段の強化
第２層：利益の拒否
　柱③　国家として強靭性の向上
　柱④　より安全化するためのサイバーエコシステムの再形成
　柱⑤　民間セクターとのサイバーセキュリティ協力の運用化
第３層：コスト負荷
　柱⑥：実力行使のための軍事手段及びあらゆるレベルにおけるサイバー攻撃を抑止するための手段の保持と運用

[98] The John. S. McCain National Defense Authorization Act for Fiscal Year 2019 (FY2019 NDAA, P.L. 115-232) Sec 1652.
[99] *See* U.S. Cyberspace Solarium Commission, “Cyberspace Solarium Commission Official Report” (March 2020), online: Cyberspace Solarium Commission <https://www.solarium.gov/report> at 1.
[100] *Ibid*., at 2-6.

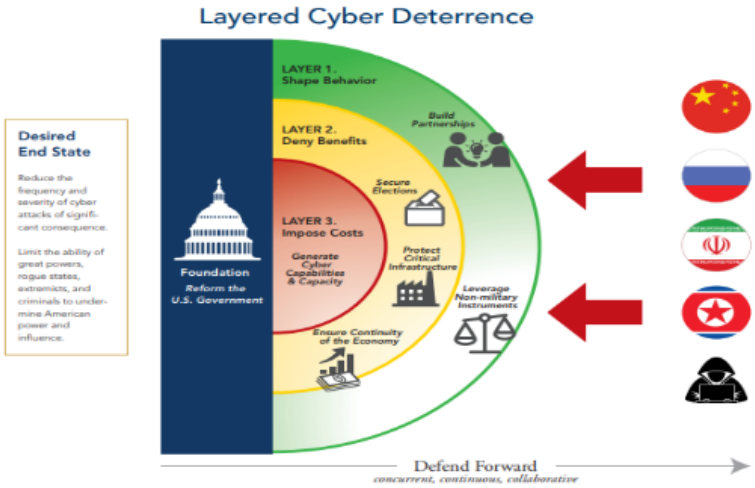

図３　多層的サイバー抑止の全体像

U.S. Cyberspace Solarium Commission, “Cyberspace Solarium Commission official Report” (March 2020), online:Cyberspace Solarium Commission <https://www.solarium.gov/report> at. 7.

更に同委員会は具体的な行動として、109 条に及ぶ立法政策提言を行っている[101]。これらの提言において、同委員会は、「(抑止は) アメリカの永続的な戦略である」との考えを示しつつ、同委員会の提言の多くが、拒否的抑止に依拠していることを認めている[102]。ただし、同委員会は、当該戦略においても前方防衛や継続的従事戦略の重要性を認めており、これらが抑止においても重要な一部を形成するものだとしている。多層的サイバー抑止の概念は、大きな理論的変換ではなく、過去の議論を包括的に取り込んだ上でサイバー抑止実現に向け実行可能なあらゆる手段を使用するという姿勢を強調しているものである、との印象を受ける。特に、政府内、官民及び同盟国とのパートナーシップ強化を重視していることは、民間事業者及び同盟国を取り込み、より総合的かつ効率的なサイバーセキュリティ態勢の構築を図ること狙いとしているものと考えられる。

現状、米国のサイバーセキュリティ政策は概ね同委員会の提言に沿った形で進んでおり、2023 年 4 月に公表された国家サイバーセキュリティ戦略[103]も上記内容の多くを取り込んでいる。新しい国家サイバーセキュリティ戦略は、以下の５つの柱をあげる。

①　重要インフラの防衛：重要分野に求める最低限のサイバーセキュリティー基準を拡

[101] Cyberspace Solarium Commission, “Cyberspace Solarium Commission legislative proposals” (July 2020), online: Cyberspace Solarium Commission <https://www.solarium.gov/>.
[102] *See supra* note 99 at 2.
[103] U.S. Government, "National Cybersecurity Strategy"the white house(October 2022), online: the white house < https://www.- whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>.

大する。官民協力を迅速かつ大規模に進める。連邦政府のネットワークの防衛と現代化を進めるとともに、危機対応政策を更新する。

② 脅威ある行動者への対抗：国家権力で利用できる全てのツールを戦略的に活用する。ランサムウェアの脅威に連邦政府として包括的に対処するとともに、国際的パートナーと強固に連携する。

③ 安全と強靭性を促進させるための市場形成：個人データのプライバシーと安全保障を促進する。安全な開発慣行を促進するために、ソフトウェア製品・サービスに責任を課す。連邦の補助金プログラムを確保する。

④ 強靭な未来への投資：インターネットの構造的・技術的な脆弱（ぜいじゃく）性を減少させ、越境するデジタル脅威に対する強靭性を高める。ポスト量子暗号やデジタル個人認証、クリーンエネルギーインフラなど次世代技術のためのサイバーセキュリティーにかかる研究開発を優先する。

⑤ 共通する目標を追求する国際パートナーシップの構築：デジタルエコシステムへの脅威に対抗するために、有志国による国際連携を強化する。平時と非常時いずれにもパートナー国がサイバー脅威に対して自らを防衛できる能力を向上させる。

一見して、多層的サイバー抑止の概念が取り込まれていることが明らかであるが、前戦略に比べ、ランサムウェアの脅威及び対応が強調されている。これは、2021 年にバイデン政権が発足した直後にコロニアルパイプラインを始めとする重要インフラへのランサムウェア攻撃が相次ぎ、対応を余儀なくされたことが影響しているものと考えられる。ただし、前方防衛についても継続していくとされており、Cyber Command の運用方針に大きな変化は無いと考えられる[104]。

また、昨年度公表された米国家防衛戦略では、新たに「統合抑止」及び「campaigning」の概念が示された[105]。統合抑止は、抑止の方策として「拒否(Denial)による抑止」、「強靭性(Resilience)による抑止」、「直接的及び集団的なコスト賦課(Direct and Collective Cost Imposition)による抑止」の３要素からなるとし、特に攻勢的サイバー作戦を直接的コスト賦課による抑止に含めていることは注目に値する。また、同盟国との連携についても統合抑止の重要な要素として度々触れている。「campaigning」は、日本語ではしばしば「戦役」と訳され、戦略的目標を達成するため、一連の作戦行動を連続して行うことである。国家防衛戦略では、campaigning とは「戦略的に整合した目的を長期的に達成するために、論理的にリンクした軍事活動の順序を決定し、実施すること。」としている。文書内では、特に、平時から GZ 事態に掛けての

[104] *Ibid*., at 14.

[105] U.S. Department of Defense,“National Defense Strategy”(October 2022), online: DoD <https://media.defense.gov-/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF>.

campaigning を強調しており、サイバー作戦により、敵の活動を抑制することが記載されている。これらの記述には、前方防衛や継続的従事戦略の概念の影響が見て取れる。このことから、新な国家防衛戦略においても多層的サイバー抑止構想及び前方防衛に対する考え方は変化していないと考えられる。

総括するならば、米国のサイバー抑止論の変遷を見ると、第一にサイバー空間が他の領域とは異なる特性を有し、これまでの懲罰的抑止だけでは対応が困難であるということ、第二に、武力攻撃に至らない低烈度なサイバー攻撃に対応するためには、平時からの常続的なサイバー空間における実力行使が必要であるということ、第三として、そのためには、軍や情報機関だけでなく、あらゆる政府機関、民間事業者及び同盟国との連携強化が必要である、ということを強く示唆しているものと考えることが出来る。

3.3 米国のサイバー抑止策が及ぼす影響－能動的サイバー防御への影響

昨年度公表された日本の能動的サイバー防御と米国のサイバー抑止に関する議論との関係は不明確であるが、ACD や前方防衛といった概念の影響を受けていることは間違いないと考えられる。しかし、日本の能動的サイバー防御に関しては、米国と異なり、政策の下地となるべき学術的な理論研究及び議論が公表されていないため、多くの者が能動的サイバー防御において実行される具体的な行為をイメージ出来ないでいる。能動的サイバー防御が従来の抑止の範囲に収まるものなのか、あるいは米国の前方防衛と同じく平素からの Red Cyberspace に侵入し活動を行うことまで要求する概念なのか、現状では明らかではない。

新たな国家安全保障戦略において、能動的サイバー防御の概念は以下のように示される[106]。

武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入する。

重要な点は、従来は対応が難しいとされた武力攻撃に至らない低強度のサイバー攻撃に対しても対応を行っていくとしていることと、実際の被害が発生する前に「未然に排除」すると謳っていることである。その上で、能動的サイバー防御の実施のための体制整備として、以下の要素を含む必要な措置

[106] 前掲注 17。

を行うとする[107]。

① 重要インフラ分野を含め、民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有や、政府から民間事業者等への対処調整、支援等の取組を強化するなどの取組を進める。
② 国内の通信事業者が役務提供する通信に係る情報を活用し、攻撃者による悪用が疑われるサーバ等を検知するために、所要の取組を進める。
③ 国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃について、可能な限り未然に攻撃者のサーバ等への侵入・無害化ができるよう、政府に対し必要な権限が付与されるようにする。

①は、民間事業者との情報共有を含めた協力枠組みの構築を目指すものであり、これまでの政策と大きな方向性の違いはないと考えられる。一方、②は、事業者に対、サービス利用者の情報を政府に提供させる枠組みの構築を図るようにも捉えられ、ACD と同様、積極的な attribution による脅威の早期発見と排除を目指すものと推測される。それが強制的なものを意味するのか、あるいは事業者の任意によるものなのかは不明であるが、いずれにせよ事業者が違法性を問われる、あるいは訴訟に巻き込まれる等の懸念なく、安心して情報を提供できる法的枠組みの確立が不可欠であろう。最も注目すべき点は、③の未然に攻撃者のサーバ等への侵入・無害化が出来るようにするとの表現である。当該表現では、Red Cyberspace に侵入してのサイバー作戦を行うことを許容するものと考えられる。しかし、これが、前方防衛と同様に平時から Red Cyberspace 常在し、継続的関与を図るサイバー作戦の実行を意味するものなのか、あるいは相手の脅威を察知した後、限定された OCO-RA として一時的に反撃が許容されるに過ぎないものなのか、具体的な態様は明確ではない。いずれの場合にせよ、どのような基準に基づき、どの時点から対応措置が可能となるのか、その判断は誰が行うのか、具体的な実力行使は誰が行うのか、結果に対する説明責任はどうするのか、といった様々な課題が存在する。

今後具体化に当たっての様々な議論が行われるであろうが、その際においては、特に米国との戦略環境の違いを意識することが必要であろう。特に、米国との技術・資源の違いは重要な課題である。米国は現時点でサイバー空間における優位性を保持しているとの認識のもと、どのようにしてその優位性を維持するかという議論が根底にある。一方で、対象国のサイバー作戦能力を考えれば、日本は現時点で劣勢な状況であり、積極的に Red Cyberspace

[107] 前掲注 17。

において作戦を行うことにより、強烈な報復を受ける可能性は十分に考慮すべきである。また、法的環境の違いも十分に考慮すべきである。特に、国内法においては通信の秘密に対する考え方の違いや、自衛隊が関与する場合は、憲法との関係及び具体的な作戦実行権限の法的根拠等が異なるため、米国の議論そのまま日本に当てはめることは無理がある。

また、米国の多層的抑止において国際規範の形成が重視されていることも留意が必要である。これまで見てきた通り、本来、抑止を有効に行うためには条約等による明確な基準を国際社会が共有することが必要である。しかしながら米国が拘束力を有する条約化を目指すのではなく、曖昧性を含む国際規範の形成を指向していることは前述の通りであり、日本も米国の路線に追従し、曖昧な形の国際規範化を目指すのか、あるいは拘束力を有する条約化を目指すかを判断することも必要であろう。また、米国が主張する国際規範が世界的に受け入れられているわけではなく、ロシア・中国側に賛同する国は多数存在することは認識をしておくことも必要である。日本としての戦略環境を踏まえた議論が期待される。

3.4 小　結

本章では、米国におけるサイバー抑止理論の発展及び日本の能動的サイバー防御構想に及ぼす影響を考察した。能動的サイバー防御構想が、米国の前方防衛のように平素から Red Cyberspace に常在し、対象国との継続的な交戦を行うことまで想定しているのか、あるいは、武力攻撃に至らないサイバー攻撃に対しても反撃を行うという、報復的抑止に留まるのかは定かではない。しかし、重要なことは、サイバー空間における抑止とは、核抑止等のこれまでの抑止概念とは異なり、平時から対象国の Red Cyberspace に影響を及ぼす実効的なサイバー作戦の遂行を要求する、実際に行使する抑止でなければならない、ということである。

Ⅳ　サイバー紛争に適用される法の概観

4.1 法的枠組みの全体像

本章では、サイバー空間に適用される国際法及び国内法の枠組みについて概観する。まずサイバー空間を規制する国際法及び国内法がどのように発展・形成されてきたかという経緯を確認する。その上で現状の国際法と国内法それぞれのサイバー空間に対する適用要領、特に平素から有事に至る流れ

の中での国際法と国内法の相違点について焦点をあてる。

前述の通り日本においては国際法と国内法はそれぞれ別個に議論される場合が多く、特にサイバー空間における紛争に関して国際法と国内法の両分野を統合した研究は極めて少ない。しかし、サイバー紛争への法の適用にあたっては、サイバー空間の特性である地理的無制限性から国際法と国内法の双方を同時に考慮しなければならない場面が生起し易い。国際法と国内法では、その形成過程や考え方が異なる部分が多く、常に両者の規定が一致するわけではない。また、サイバー紛争の法規制にあたっては、国際法及び国内法の区分だけでなく、平時から有事に至る紛争烈度の変化軸を捉えることが必要になる。紛争烈度とは、大きく平時、GZ 事態及び有事の３つの区分が考えられるが、それぞれの区分において適用される具体的な条約や法令が変化し、その境界が必ずしも国際法と国内法で整合している訳でもないという、混沌とした状況を呈している。このため、本章ではまずサイバー空間の規制に向けた国際法及び国内法の経緯を確認し、次に平素、GZ 事態及び有事の法的意義づけ及びそれぞれの状況でサイバー空間において適用される国際法及び国内法の確認を行う。

4.2　サイバー空間の法規制の発展

4.2.1　サイバー空間への国際法適用を巡る議論の経緯

サイバー空間への国際法適用に関する議論は、1998 年にロシアによる国連総会での決議案提出を受け本格化し[108]、国連総会第 1 委員会の下にサイバーセキュリティに関する国連政府専門家会合（以下「GGE」という[109]。）が設置された。GGE は、2004 年に第 1 回会期が実施されて以降、最終的に 6 回の会期で開催され、2021 年に最終報告書が採択され終了した[110]。GGE は、サイバー空間にも既存の国際法が適用されることについて概ね各国のコンセンサスを獲得するとともに、遵守されるべき国際規範を提示する等、一定の成果を獲得したと言える。こうした状況の中、GGE とは別の検討枠組みを模索するロシアは、2018 年に国連全加盟国が参加可能な形でのオープン・エンド作業部会（「国際安全保障の文脈における情報及び電気通信分野での発展に関するオープン・エンド作業部会（以下「OEWG」という[111]。）」を設置する決議案

[108] U.N. Doc. A/C.1/53/L.17/Rev.1(22 July 2015).

[109] GGE: U.N. Groups of the Group of Governmental Experts on Advancing responsible State behavior in cyberspace in the context of international security.

[110] U.N. Doc. A/76/135.

[111] OEWG: U.N. Open-ended Working Group on Developments in the Field of Information and Telecommunications

を提出し、採択された[112]。OEWG においても、国際法の適用に関する議論が行われ、2021 年に最終報告書が提出された。当該最終報告書は、サイバー空間においても既存の国際法が適用されること確認したほか、GGE と同じく国際規範についても言及している[113]。一方で、上記の国連内における議論は、端的に言えば「総論賛成、各論反対」の状況であり、サイバー空間においても既存の国際法が適用されるとの各国の共通認識は確立された一方で、具体的な各論事項の合意には至らなかったとも言える。特に、サイバー空間における主権、武力の行使の禁止原則、国際人道法及び国際人権法等に関しては、ロシア・中国等の国の見解と、西側諸国との見解との隔たりは大きく、第 5 回 GGE では、武力の行使及び国際人道法の適用に関しロシア・中国と西側諸国との合意が図れず、実質的な報告書を採択できない事態に陥った[114]。

また、上記国連での国際法適用に関する議論と並行し、国境を越えたサイバー犯罪に対する対策に関する検討もおこなわれた。1990 年代後半より、欧州評議会を中心として国境を越えたサイバー犯罪への対策が検討され、2001 年にサイバー犯罪に関する条約（以下、「サイバー犯罪条約」と略する。）が成立した。サイバー犯罪条約は、不正アクセス等一定の行為の犯罪化、データ保全等に係る刑事手続の整備、犯罪人引渡し等に関する国際協力等を規定する。現在、全ての G7 諸国を含む 68 か国が締約国となり、日本も 2012 年に批准をした[115]。また、より迅速かつ円滑な手続による電子的形態の証拠の収集を可能にすること等を目的として、2021 年に「協力及び電子的証拠の開示の強化に関するサイバー犯罪に関する条約の第二追加議定書」が採択され、日本は 2022 年署名している[116]。このように、主に欧米諸国を中心としたサイバー犯罪対策のための協力枠組み作りが進展する一方で、ロシア及び中国は当該条約の未締約国であることは、当該条約の効果を限定的なものとしている。特に、ロシアは、同条約が、同意の無い他の領域国内へのデータ・アクセスを認めているとし、国際法上の主権原則に反するとともに、コンピュー

---

in the Context of International Security.

112 U.N. Doc. A/RES/73/27

113 U.N. Doc. A/AC.290/2021/CRP.2.　なお OEWG の枠組みは 2025 までの予定で継続中である。

114 Michael N. Schmitt and Liis Vihul, “International Cyber Law Politicized: The UN GGE’s Failure to Advance Cyber Norms” (30 June 2017) *Just Security*, online: Reiss Center on Law and Security <https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/>.

115 外務省 HP <https://www.mofa.go.jp/mofaj/gaiko/soshiki/cyber/index.html>。日本では、2004 年 4 月に国会で批准の承認を得たものの、法整備上の問題のため未批准であった。しかし、2011 年 6 月に情報処理の高度化等に対処するための刑法等の一部を改正する法律が成立し条件が整い、2012 年 7 月 3 日に欧州評議会事務局長へ条約の受託書を寄託して批准したことから、2012 年 11 月 1 日から日本国についても効力が生じることとなった。

116 外務省 HP <https://www.mofa.go.jp/mofaj/ila/st/page24_002143.html>。

ターテロや情報通信技術の「侵略的な利用」を増長する」として反発[117]、新たに犯罪目的での情報通信技術の利用への対策名目で、中国等と連携し、サイバー空間における主権原則の徹底及び国家による統制強化を主張する条約案を提示する等、積極的に行動している[118]。とりわけ、この条約を検討すべくロシアが主導した新たな検討枠組みの設置を求める決議が 2019 年 に欧米諸国の反対にも関わらず採択されたことは、必ずしもロシア・中国が孤立している訳でないことを示している[119]。

現状として、サイバー空間への法規制は発展途上であり、具体的な拘束力を有する条約はサイバー犯罪条約に留まる。上記で述べた通り、既存の国際法の具体的な適用に関しては各国、特にロシア・中国と欧米諸国の思惑が大きな隔たりがあり、国際社会として確立された統一見解は存在しない[120]。また、近い将来において新たに拘束力ある条約が成立する可能性は低いと考えられる。このため、既存の国際法がどのようにサイバー空間に適用されるかを積極的に主張することや国際規範の浸透要領について、更に検討することが重要であり、日本も積極的な関与を図っていくべきと考える。

4.2.2 サイバー空間を規制する国内法の発展

次に国内法の状況について確認する。日本のサイバーセキュリティ法制は、基本的に憲法 21 条後段で規定される「通信の秘密」及びその内容を具体化する電気通信事業法、有線電気通信法、電波法等の通信行政への規制が基盤となって発展してきたと言える。これらは、主に政府及び公的性質をもつ電気通信事業者が通信の信頼を維持するために遵守すべき事項が規定されたものであった。一方、これとは別に、1980 年代後半から新たに出現し始めたコンピュータ犯罪を取り締まるための刑法の改正が行われる等、サイバー犯罪への取組が進んだ。まず、1987 年に電磁的記録に関する罪が新たに規定され、それまで法的に曖昧な位置づけであったコンピュータウィルスが不正指令電磁的記録として定義された。また、1999 年には不正アクセス行為の禁止等に

---

[117] 佐々木孝博「サイバー空間の施策に関するロシアと欧米諸国のアプローチ」日本大学大学院総合社会情報研究科紀要 14 号 1-12 頁(2013)。

[118] U.N. Doc. A/RES/75/282 (May 21, 2021).

[119] 原田有「複雑化するサイバー規範プロセスの動向」NIDS コメンタリー第 118 号、防衛研究所（2020 年 6 月 2 日）＜http://www.nids.mod.go.jp/publication/commentary/pdf/commentary118.pdf>。

[120] サイバー空間における既存の国際法の適用に関し、NATOのサイバー作戦に関する研究機関CCDCOEが主催し、既存の国際法の適用に対する西側国際法学者の見解を取りまとめたTalinn Manualが有名であり、一定の権威があるものとして認識されている。2017年には続編となるTalinn Manual 2.0が刊行された。*See* Michael N. Schmitt, *supra* note 6. しかしながらTalinn Manualは飽くまで西側諸国の見解であり、必ずしもロシアや中国に受け入れられているものではないことは注意を要する。

関する法律が制定され、ハッキング等の不正アクセス行為が新たに規制されることとなった。その後現在に至るまで数度の改正を経つつ、サイバー犯罪に対応するための刑法の整備が続いている。

また、サイバーセキュリティ全般を統括する基本法として、2014 年にサイバーセキュリティ基本法が制定され、サイバーセキュリティに関する政府及び民間事業者等の役割が規定されることになった。ただし、サイバー安全保障に関する具体的な法整備はほとんど実施されていない。冒頭に述べた通りサイバー安全保障についてはサイバーセキュリティ基本法 19 条に一文が記載されているにとどまり、かつ同条は極めて不十分な状態にとどまっている。このため、サイバー安全保障を強化するための態勢・体制整備を求める声が高まり、特に米国におけるランサムウェアの被害等から、重要インフラ防護の重要性が強く主張されるようになった。こうした声を受け、令和 4 年の警察法改正において「重要サイバー事案」の概念が創設され、重要インフラ防護への警察の関与が明確化された[121]。更に冒頭に述べた新たな安全保障戦略においてサイバー安全保障としての能動的サイバー防衛構想が示され、内閣官房に設置されたサイバー安全保障体制整備準備室において実現に向けた法制度の検討が現在行われている[122]。ただし、本論文の執筆時点においてはその全容は明らかになっていない。特に、総務省が主管として管轄してきた伝統的な通信行政への規制と、官邸が主導する安全保障上の各種権限の新設とは相いれない部分も多く、検討が難航する恐れもあり、今後の議論の進展を慎重に見極めることが必要である。

4.3　平時・GZ 事態・有事の法的意義

サイバー空間における国際法及び国内法の発展と現状を確認したが、国際法及び国内法双方の様々な条約や法令が混在し理解することは容易ではない。また、サイバー作戦は、平時から有事に至る間のあらゆる紛争スペクトラムで使用されるため、それぞれの事態で適用される法令及び事態と事態の移行や連接を把握することが重要である。次章以降で、具体的にどのような法令が適用され、どのような問題点が存在するかを述べるが、その前にこれまで使用してきた平時、GZ 事態及び有事といった用語がサイバー空間においてどのような状況を指すのか、適用される法の変化という観点から、それぞれの意義を確認する。

---

[121] 警察庁「警察法の一部を改正する法律案」（令和 4 年 1 月 28 日成立）。
[122] 日本経済新聞「『能動的サイバー防御』準備室、内閣官房に新設　政府」2023 年 1 月 31 日<https://www.nikkei.com/article/DGXZQOUA3186D0R30C23A1000000/>.

4.3.1 有　事

まず「有事」について確認する。「有事」とは、一般的には「戦争や事変など、非常の事態が起こること」とされる。しかし、国際法上、上記の意味をそのまま表現する用語はない。国連憲章 51 条は、国家が自衛権を発動する条件を外国からの「武力攻撃（armed attack）」の発生と規定する[123]。しかし、上記は飽くまで自衛権発動の正当性を判断する条件を規定するものであり、実質的な戦争状態の発生を必ずしも意味するわけではない。

国際法上の戦争状態とは、一般的には「武力紛争（armed conflict）」と呼称され、特に二国間以上の武力紛争を国際的武力紛争（international armed conflict）と定義する[124]。実質的な国際的武力紛争が生起している場合、国際人道法と呼ばれる、戦闘の手段方法及び犠牲者保護を定める特別な法体系が適用される。この国際人道法の適用開始時期は、自衛権の発動とは無関係であり、両者は必ずしも一致しないことは注意を要する。国際人道法が適用された場合、戦闘員と文民の区別が明確化され、一定の制限の下、軍隊に所属する戦闘員が行う戦闘行為は合法化される。また、文民に対する保護が適用される。

次に国内法上の有事であるが、国内における安全保障に関する議論の文脈では、有事とは自衛隊法（以下、「隊法」と略する。）76 条による防衛出動命令が下令されている事態として使用されている[125]。防衛出動は、「武力攻撃事態」が認定されていることが前提となっている[126]。防衛出動下令時は、隊法 88 条による「武力の行使」権限が自衛隊に付与されるほか、各種行政法上の適用が除外される。これらの防衛出動時の枠組みは、国際人道法と同様に軍隊（自衛隊を含む）の戦闘行為を合法化する為の規定である。しかし、両者は異なる性格を有する。国際人道法における戦闘行為の規制は基本的に違法

---

123 日本語の「武力攻撃事態」に対する一般的な訳語には armed attack situation が充てられている法務省日本法令外国語訳データベースシステムでは、「武力攻撃事態における捕虜等の取扱いに関する法律」を“Act on the Treatment of Prisoners of War and Other Detainees in Armed Attack Situations”と訳している。

124 戦地にある軍隊の傷者及び病者の状態の改善に関する 1949 年 8 月 12 日のジュネーブ条約（以下「GC Ⅰ」と略する。）第２条「二以上の締約国間に生ずるすべての宣言された戦争又はその他の武力紛争」

125 「有事という言葉は法令上の用語ではございませんで、その意味は必ずしも一義的であるわけではございませんが、有事法制研究という有事につきましては、同研究は、自衛隊法第 76 条によりまして防衛出動命令が下令されました時点以降における自衛隊の円滑な任務遂行に係る法制上の問題点の整理を目的としておりまして、その意味で、ここで言う有事といいますのは、防衛出動命令下令事態ということになるわけでございます。」第 146 回衆議院国会安全保障委員会瓦力防衛庁長官答弁（1999 年 11 月 18 日）。

126 事態対処法２条４項が定める「存立危機事態」においても防衛出動は可能であるが、同概念については様々な議論があり具体的なケースを想定することが難しいことから、本稿では考察外とする。なお「武力攻撃予測事態」、すなわち「武力攻撃事態には至っていないが、事態が緊迫し、武力攻撃が予測されるに至った事態」を併せて「武力攻撃事態等」と呼称する。

となる行為を規定するネガティブリスト方式であり、原則、軍隊による戦闘行為は合法との認識に立つ。一方で隊法の規定は、一定の場合に許容される行為を示すポジティブリスト方式で規定される。特に、隊法 88 条は、一定の条件下に自衛隊の戦闘行為に対する刑法上の法令行為としての違法性阻却事由を認めるものであり、上記条件に合致しない場合は平時の行政法・刑法が適用されることを示している。いずれにせよ、サイバー空間における軍事作戦には、国際人道法及び隊法の各種規定が適用されることになる。

有事におけるサイバー空間の状況として、本稿においては、国際法上はサイバー空間以外の状況を含めて国家間武力紛争が生起している状況であり、国内法上は武力攻撃事態が認定されている状態を想定する。第二章におけるサイバー作戦の分類に従えば、純軍事作戦としてサイバー作戦が行われている状態と言える。上述の通り、有事におけるサイバー作戦の法的枠組みでは、平時及びＧＺ事態と異なり、純粋な攻撃目的のサイバー行為が合法化される一方で、行為主体が軍隊等に所属し戦闘員資格を有する者に限定されるほか、攻撃目標等にも国際人道法等による制約が課せられる、といった点において、次項で述べるＧＺ事態や平時とは大きく異なる性格を有する枠組みと言える。

4.3.2　GZ 事態

次に、GZ 事態である。確立された定義は存在しないが、防衛白書では「純然たる平時でも有事でもない幅広い状況を端的に表現したもの」とし、「武力攻撃に当たらない範囲で、実力組織などを用いて、問題にかかわる地域において頻繁にプレゼンスを示すことなどにより、現状の変更を試み、自国の主張・要求の受入れを強要しようとする行為が行われる状況」と説明される[127]。定義としてはあまりに漠然としており実用的とは言えない。簡単に言えば「「武力攻撃」には至らないものの、強制や威圧を伴う国家による実力行使が行われている状態」と考えることが妥当であろう[128]。

GZ 事態を国際法の観点から見るならば、「主権侵害」から「武力の行使」に至るまでの何らかの国家による国際法上の義務違反が生じている状態であ

[127] 前掲注 13。

[128] オーストラリア国防大学が提供するオンライン教育サイトでは、GZ 事態の定義として「グレーゾーンの活動は、戦争に至らない強制的な国家運営行動である。グレーゾーンは、主に非軍事的な人間活動の領域であり、国家が国家資源を用いて意図的に他国を威圧する。国家は、戦争の閾値以下において、複数の一見無関係で合法的あるいは帰属困難で、相互に連携・同期する国家行為実行のための技術を使用して、グレーゾーンの目標を達成する。グレーゾーン・キャンペーンは、敵の弱点を突く、あるいは敵の対応策を抑制しつつ、具体的な国家戦略目標を達成することを目指す。」とする。“Grey Zone Activities and the ADF-A Peary Group Report” gray zone, online: The Forge <https://theforge.defence.gov.au/sites/default/files/2020-10/Grey%20Zone_0.pdf>.

り、国家責任法によって規制される領域となる。国家責任法とは、「国家の国際法上の義務違反によって生じた法的不正常を解消し、法適合状態を回復するための条件と手続きを定める国際法の規則」[129]とされる法体系であるが、明文上の拘束力を有する他国籍間条約等がなく、基本的には慣習法あるいは個別の２国間条約等で構成される[130]。このため、各国の解釈に差異が大きい分野であり、サイバー空間への適用にあたっても、様々な議論が存在する。

国内法の観点からは、上記国家責任法に該当するような包括的に適用される統一された法体系や法令はなく、複数の事態や法令が乱立しており、整理はさらに難しい。一例として、事態対処法では、武力攻撃事態に至らない状態として、武力攻撃予測事態及び緊急対処事態[131]を定める。また、隊法は、防衛出動以外の特別な行動として、治安出動、警護出動等の様々な行動類型を定める[132]。その他にも警察法５条６項で定める「重大サイバー事案」、同法 71 条が定める「緊急事態」等が存在する。個々の法令がそれぞれ異なる主体に対し異なる権限を規定しており、さらにそれぞれの事態の関連性が不明確であることから、まさに法律上もグレーな状況となってしまっている。今後、これらの乱立する事態を整理することが求められるであろう。

サイバー空間の状況に当てはめれば、第二章の分類における示威又は威嚇型のサイバー攻撃等が発生している状態が想定される。2007 年に発生したエストニア対する大規模 DDoS 攻撃では、明確な attribution には至らなかったものの、DDoS 攻撃の直前にロシアとエストニアの間での政治的な摩擦が生じており、ロシアの関与が強く疑われている。上記状況のように、何らかの外交目的達成のために武力攻撃に至らない実力行使を行うことは典型的なGZ事態の手法といえ、物理的被害が生じにくいサイバー攻撃は最も効果的な手段と考えられる。また、犯罪支援型あるいは情報操作型のサイバー攻撃であっても、攻撃の態様や程度により国家責任法が規定する国際法上の義務違反に該当する場合はＧＺ事態に該当する可能性があり、平時との区別は極めて曖昧である。能動的サイバー防御は主にこのＧＺ事態への対応を焦点にしていると考えられる。

4.3.3　平　時

---

[129] 杉原高嶺『国際法学講義[第２判]』（有斐閣、2013）509 頁。
[130] 国際連合国際法委員会（ILC）は 2001 年に,「国際違法行為に対する国家の責任に関する 条文」（以下「国家責任条文」と略する。）を採択したが、条約化は見送られた。UN Doc. A/RES/56/10.しかし、国家責任条文の大部分は慣習法を反映していると考えられている。*See Michael N. Schmitt*, *supra* note 6 at. 79.
[131] 田村重信『新・防衛法制』（内外出版、2018）58 頁。
[132] その他にも重要影響事態、防衛出動待機命令、国民保護活動等が存在するがサイバー空間との関連性が薄いため本稿では考察外とする。

上記を踏まえれば、「平時」とは、有事でも GZ 事態でもない状態となるが、具体的に言えば武力紛争及び強制や威圧を伴う国家による実力行使が行われていない状況であり、国際法上は国家責任法が適用されるような国家による国際法上の義務違反が生起していない状況である。国内法上は、GZ 事態を示す上記の特別な事態の認定が無い状況であり、いわゆる平素の状態である。サイバー空間においては、第二章において区分した現状のサイバー攻撃の大部分を占める espionage 型、犯罪支援型あるいは情報操作型のサイバー攻撃が行われている状況であり、最も普遍的な状況であると言える。

国際法の観点からは、espionage 型のサイバー攻撃に関しては、現状、国際法上は違法ではないとされている[133]。また、犯罪支援型及び情報操作型のサイバー攻撃は、当該サイバー行為が国家責任法で言う国際法上の義務違反に該当するかが第一に問題となる。主権侵害あるいは違法な干渉等に該当しない程度の行為の場合、あるいは attribution が困難な場合、国際法上の違法性を問うことは難しい。国家責任法上の違法性が問えない場合、資産凍結、禁輸措置等の経済制裁等による合法的手段よる報復、あるいは国際司法裁判所への提訴等の司法的解決、外交交渉、周旋、仲介、審査、調停のような平和的解決を図ることになる。また、拘束力はないものの、国際規範を根拠とした公的な名指しでの批判、いわゆる public attribution の手法も近年では行われている。

国内法の観点からは、犯罪支援型のサイバー攻撃は多くの場合、国内刑法違反となる。また、情報操作型のサイバー攻撃の場合、不正アクセス行為等を伴う場合は刑法違法に該当する可能性がある。しかし、外国領域において当該領域国の同意なく執行管轄権を行使することは主権侵害に該当する可能性があるため、実態として外国からのサイバー犯罪を捜査し、容疑者を逮捕することは困難である。米国では、外国政府関係者等のサイバー犯罪の容疑者に対し、身柄を確保しない状態での米国内裁判所への起訴を行っているものの、前章で述べた通り明白な効果が発揮されているとは言い難い状況である。このため、外国からのサイバー犯罪に対しては、国家間での捜査協力義務を定めたサイバー犯罪条約等の枠組みが重要となるが、非加盟国であるロシア、中国及び北朝鮮といった国々が捜査に協力する可能性は低いであろう。加えて、影響力工作等の情報操作型のサイバー攻撃は、国内法上も違法性を問えない場合が大部分である。このため、上記のような平時における国外からのサイバー攻撃は現状として国際法上も国内法上も対処が非常に難しい状

[133] espionage の詳細については *See* Tallinn Manual 2.0 *supra* note 6 at 168.

況となっている。

4.4　小　結：サイバー空間に適用される法の特性

本章においては、サイバー空間における法規制の発展状況及び平時から武力紛争に至る紛争スペクトラムの中でのサイバー空間の状況及び適用される法的枠組みについて確認した。サイバー空間に適用される国際法及び国内法が形成途上にあり依然として明確な基準が確立されていないこと、適用される法的枠組みは紛争スペクトラムに併せて変化しかつその境目が曖昧であること、及び国際法と国内法においての差異が大きいことは、サイバー空間への法適用を困難にする大きな要因であるとともに他の陸海空領域と大きく異なる点である。このため、法的な分析を行うにあたっては、前提条件、特に分析対象となる事象がどの紛争スペクトラムに位置するのか、という点を明らかにするとともに、国際法及び国内法の双方の観点から分析することが求められる。次章以降、具体的な法的課題について検討を行うが、平時・ＧＺ事態・有事の内、有事については法的枠組みが大きく変化することから、平時～ＧＺ事態と有事の二区分に分け、それぞれ国際法及び国内法の双方の観点から分析を行う。なお、図４はサイバー空間における平時・GZ 事態・有事において適用される国際法及び国内法の全体像を示す。

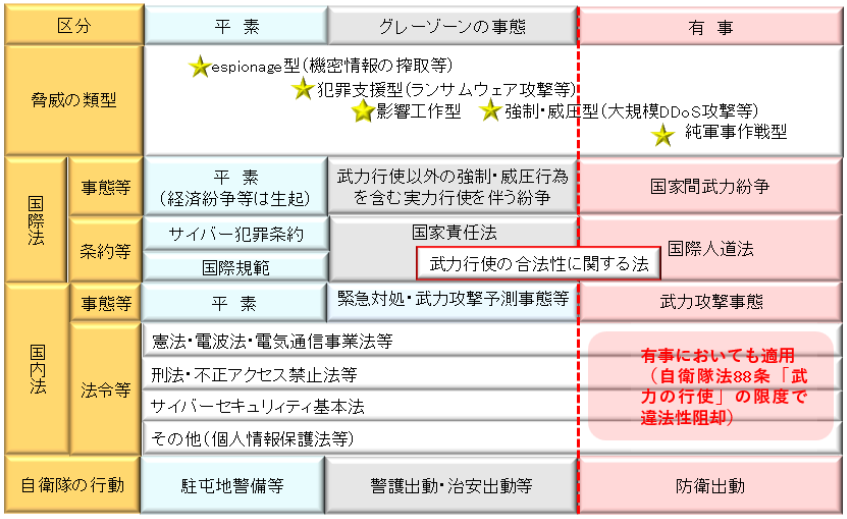

図４「サイバー空間に適用される法の全体像」

Ⅴ　平時～GZ 事態におけるサイバー攻撃への対応（国際法）

5.1　国際法適用上の課題

平時～GZ 事態におけるサイバー作戦においては、武力攻撃の基準に至らない低強度のサイバー攻撃が行われるが、このような低強度のサイバー攻撃に対する国際法上の対応には様々な議論が存在する。以下、論点を概観する。

第一に、低強度サイバー攻撃に対する自衛権の適用の問題がある。一般的に、武力攻撃に至らないサイバー攻撃に対しては、国連憲章 51 条で規定される自衛権による対応は出来ないと考えられている。一方で、一部の国や法学者は、国連憲章上の自衛権とは別に慣習法上の自衛権が存在し、武力攻撃に至らない「武力の行使」に対しても自衛権の行使が可能と主張していることから、武力攻撃に至らない「武力の行使」レベルの低強度のサイバー攻撃に対する自衛権の適用の可能性について、多くの議論が存在する。

次に、「対抗措置」及び「緊急状態」の適用に関する議論である。自衛権が適用されない場合であっても、武力攻撃に至らない国際違法行為に対しては、2001 年に国連総会で採択された国家責任条文 22 条で規定される違法性阻却事由である「国際違法行為への対抗措置（以下、「対抗措置」と略する。）」、あるいは同条文 21 条が定める「緊急状態」による対応が可能性とされている。しかし、「対抗措置」や「緊急状態」では、「武力の行使」に該当する対応行動は同条文で禁止をされている。このため、相手側からの「武力の行使」に該当する国際違法行為に対し、被害国は「武力の行使」未満のレベルでした対応ができず、不均衡が生じているとの批判が存在する。加えて、これらの違法性阻却事由の適用に当たっては様々な要件が規定されており、実際にサイバー空間に適用するにあたり、上記要件をどのように判断するかが課題となっている。特に、attribution が出来ない場合の対応が大きな課題となる。

最後に、国際違法行為に該当しないサイバー攻撃への対応である。前章で述べた通り espionage 型のサイバー攻撃は、国際法上は違法とされていない。また、犯罪支援型及び情報操作型においても、国際法上の義務違反が生じていない場合には国家責任法による対応は出来ない。このため、経済制裁等による報復や紛争の平和的解決を図る必要性があるが、これらの効果的な運用について検討を行うことが必要である。

5.2　サイバー空間における国際違法行為

国家責任法を適用するためには、国際違法行為が存在することが必要であ

る。このため、サイバー空間における国際違法行為と具体的にどのような行為かということを明らかにすることが重要となる。国家責任条文は国の国際違法行為の要素として、作為又は不作為からなる行為が、①国際法に基づき当該国に帰属（attribution）でき、かつ②当該国の国際義務の違反を構成することを挙げる[134]。

5.2.1 attribution

第一の条件である attribution は、匿名性が高いサイバー空間においては、極めて重要な課題である。国際法の法主体は、原則としては主権国家であり[135]、非国家主体の責任を直接問うことは例外的な状況であると考えられる[136]。一方で、サイバー空間において、特に平時～GZ 事態においてはサイバー攻撃の行為主体は、外見上は非国家主体によることが大部分である。したがって、どのような場合に非国家主体による違法なサイバー行為に対する国家主体への attribution が出来るかを考察することが重要になる。一般的には、ある行為が国家に帰属できる場合とは、①国家機関が自ら行う行為、②国家の指揮下にある非国家主体の行為、あるいは③非国家主体の行為に対し国家による是認がある場合等が考えられる[137]。①のケース、すなわち軍隊及び情報機関のサイバー作戦が、当該組織が所属する国家に帰属できることに議論はない。一方で、②、③のケースでは、サイバー空間における常套的な手段であるプロキシの使用、すなわちハッキング集団等の非国家主体によるサイバー攻撃等を国家が密かに支援する場合、あるいは黙認する場合等が該当する。②のケースの場合、attribution を成立させるためには、国家責任条文はニカラグア事件判決[138]で示された「実効的支配基準」に基づき、非国家主体に対する国家の「指示、指令または支配」があることが必要とする[139]。一例として、ハッキング集団がサイバー攻撃を行うにあたって、国家機関が作成したマルウェアを使用したとする。この場合、実行的支配基準に基づけば、マルウェアを供給する行為自体は実効的支配には至っていないと考えられ、攻撃時期場所等の具体的な指示が必要とされる。しかし、匿名性の高いサイバー空間においては、上記のような証拠を入手することは極めて困難である[140]。実行的

---

[134] 国家責任条文第 2 条。
[135] 杉原・前掲注 129、56 頁。
[136] 非国家主体の責任を直接問う法分野として国際人道法及び国際刑事法が存在する。しかし、いずれも武力紛争やジェノサイド等の極めて限定的な状況における適用を想定したものであり、例外的と言える。
[137] 杉原・前掲注 129、514 頁-516 頁。
[138] ニカラグア事件判決　*See* Case Concerning Military and Paramilitary Activities in and against Nicaragua, Merits, Judgement, [1986] I.C.J. Reports 1986, paras. 93-122.
[139] 国家責任条文案 8 条。
[140] *See Michael N. Schmitt, supra* note 6 at 97.

支配基準に対し、旧ユーゴ刑事裁判所（International Criminal Tribunal for the former Yugoslavia: ICTY）におけるタジッチ事件判決は、非国家主体が組織化された軍事的団体である場合については、財政・装備の支援を超えて軍事作戦の組織・調整・計画という「全般的支配」があればよく、特定の命令や指示は必ずしも必要ないとする「全般的支配基準」の考え方を示した[141]。その後、国際司法裁判所はジェノサイド条約適用事件において同基準は、非国家武力紛争の国際化という武力紛争の性質を判断するためには有効であるかもしれないが、国家責任を認定するための基準としては不適切であるとし、「『全般的支配』の基準は国家責任法の基本原則を踏み越えて責任の範囲を拡大する重大な欠陥をもつ」として批判した[142]。しかし、匿名性の高いサイバー空間という特性を踏まえれば、attribution の基準を現実的なものにすることが必要であり、APT 攻撃を行うハッキング集団等に対しては全般的支配基準に近い新たな基準を検討することも一案ではないかと考えられる[143]。

また、attribution には、法的側面、政治的側面、技術的側面[144]があるといわれ、それぞれの性格により基準及び証拠開示の必要性は変化すると考えられる。技術的 attribution とは、セキュリティ会社やインシデント対応機関等による attribution を指し、サイバー攻撃に用いられたマルウェアそのものやサイバー攻撃の指令を送るサーバの通信ログ等の技術的観点から攻撃者を特定するものである。政治的 attribution とは、いわゆる public attribution を行う場合等に、国家間紛争や外交上の緊張関係の有無といった政治的要因を加味した上で行う attribution である。最後の法的側面は、国家及び個人の法的責任を問う際の attribution であり、容疑者を刑事訴追する場合、あるいは国家責任法に基づく国際違法行為の認定及び対応を行う際の攻撃者の特定である。

いずれも明確な基準は存在しないが、法的 attribution においては、少なくとも攻撃を実施した個人または組織を特定し、第三者が納得し得る程度の証拠が必要と考えられる[145]。ただし、個人の刑事訴追と国家の法的責任追及場合では、必要とされる証拠のレベルは異なることは注意が必要である。直接個人の人権を侵害する恐れのある刑事訴訟においては、より厳格な証明が求められものであり、国家責任追及の場合はそれよりも緩やかな証明になると考え

---

[141] *See Prosecutor v. Dusko Tadic*, IT-94-1-A, ICTY, Appeals Chamber, Judgment (15 July 1999), para. 145.
[142] *See Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia Montenegro)*, Judgement, [2007] I.C.J Reports 2007 at 210, para. 406.
[143] Nicholas Tsagourias and Michael Farrell, "Cyber Attribution: Technical and Legal Approaches and Challenges" (2020) 941 The European Journal of International Law 31-3 at 961-965.
[144] 外務省「サイバー行動に適用される国際法に関する日本政府の基本的な立場」（2021 年 5 月 28 日）。
[145] *See* Kristen E. Eichensehr, "The Law and Politics of Cyberattack Attribution" (2018) 520 U.C.L.A. Law Review 67 at 561.

られる[146]。自衛に関する ICJ の判例は、「明確かつ説得力ある」証拠基準（clear and compelling evidence standard)を支持していると言われる。この基準は、刑法で採用されている合理的疑いを超える基準よりも低く、無いよりまし程度の「証拠の優越性（preponderance of evidence)」基準よりも高いものであると考えられる。要するに、「明確かつ説得力のある」基準は、「立証責任を負う当事者が主張する事実が、真実である可能性がそうでない場合よりも実質的に高いことを、当該裁定者に納得させる」程度と言われる[147]。また、ICJ は、 2007 年の「ジェノサイドの犯罪の防止及び処罰に関する条約の適用に関する事件」（ボスニア・ヘルツェゴビナ対セルビア・モンテネグロ）において、裁判所は、「例外的な重さの罪を伴う国家に対する請求は、完全に決定的な証拠によって証明されなければならない」[148]とし、さらに別の表現で、裁判所は、ジェノサイドが発生したことを 「完全に確信」しなければならず、「このような行為に対する帰属の証明にも同じ基準が適用される」と説明する[149]。ジェノサイド条約事件が示す証拠基準は、主張される犯罪の重大性に基づいて証明の程度が変化することを示しており、より重大な違法性を証明する場合には、より精度の高い証明が必要であることを示しているように思われる[150]。仮にそうだとするならば、武力攻撃より重大性の低いサイバー攻撃に対する attribution においては、「明確かつ説得力ある」証拠基準よりさらに低い証明の程度で良いということになる可能性がある。しかし、どの程度証明の程度が下がるかはケースバイケースの判断とならざるを得ないであろう。Tallinn Manual 2.0 では、証明基準はケースバイケースとしつつ、違法なサイバー作戦に対する attribution においては、「国家は、合理的な国家が同一または類似の状況において行うように行動しなければならない。」とする[151]。つまり、通常の合理的な国家が確信を持てる程度の証拠が揃えば良いと考えているとも受け取れる。

また、attribution においては、証拠を開示する必要性があるか、という点も議論となる。Tallinn Manual 2.0 では、現状として、attribution における証拠開示を義務づける確立された根拠は存在しないとする。証拠開示により自己の収集能力が暴露する懸念から、諸外国は積極的ではない。一方で、ある程度の証拠開示が無ければ信憑性が損なわれ、国際社会の支持が得難いことも事

[146] 稲角光恵「国際法上の犯罪に対する国家責任と個人責任と企業責任」金沢法学 57 巻 1 号 1-27 頁（2014）10-11 頁。
[147] *See* Eichensehr, *supra* note 145 at 561.
[148] *See supra* note 142 at 129, para. 209.
[149] *Ibid.*, at 130, para. 210.
[150] *See* Eichensehr, *supra* note 145 at 560.
[151] *See* Michael N. Schmitt, *supra* note 6 at 82.

実であり、証拠開示による利点・欠点を慎重に検討することが求められる。

いずれにせよ、現状、attribution に関する事項は極めて不明確であり、技術進展の動向も踏まえつつ、国際社会における一定の基準確立を目指して議論を継続することが望ましい。また、証拠を公表するかどうかとは別に、サイバー攻撃に対し実際的な対応を行うならば、政府内で一定の基準を整備することは重要であろう。なお、直接の行為者の行為を国家に帰属できない場合、当該行為者が所在する領域国家に対し、後述する相当の注意義務違反を追求していくことになる。

5.2.2 国際義務違反

第二の要件である国際義務への違反について、国家責任条文 12 条は「国の行為が国際義務により当該国に要求されているものと一致しないときは、当該義務の淵源又は性質に関係なく、国による国際義務の違反が存在する。」と規定する。一般にサイバー紛争の文脈で関連する義務としては①主権尊重義務、②不干渉義務、③武力攻撃及び武力の行使を慎む義務、及び前述した④相当の注意義務等が存在すると考えられる。以下、それぞれの義務について概要を確認する。

主権尊重義務

サイバー空間においても主権尊重義務が存在することは概ね各国の合意が確立していると言える[152]。ただし、サイバー空間における主権が意味するところは明確ではない。特に、次に述べる不干渉原則との差異は曖昧である。主権尊重義務への違反、すなわち主権侵害について、常設国際司法裁判所は、ロチュース号事件判決において、他国領域内での権力行使は国際法上禁止されると判示する[153]。また、パルマス島事件仲裁判決において、仲裁裁判所は主権を次のように定義する。「国家間の関係においては、主権とは独立を意味する。地球の一部分に関する独立とは、他のいかなる国家をも排除して、そこにおいて国家の機能を 行使する権利である。」[154]上記を踏まえれば、主権とは国家が自らの領域内において排他的に行使する権限であり、ある国が他

[152] *See* Michael N. Schmitt, *supra* note 6 at 11. ただし、英国は、主権尊重義務は原則に過ぎず、国際法上の義務には至っていないとの見解を示す。UK The Attorney General's Office, Attorney General's speech at the International Institute for Strategic Studies (11 January 2017). <https://www.gov.uk/government/speeches/attorney-generals-speech-at-the-international-institute-for-strategic-studies>

[153] The Lotus case, PCIJ, Series A, No. 10, 1927, at 18-19.

[154] Island of Palmas Case, Award, RIAA, Vol. II, at 838.

国の領域内で権限行使を行うことは主権侵害となり得る。しかし、サイバー空間のように地理的境界が不明確な状況において、いかなる行為が権限行使に該当するのかについては一致した見解は存在しない。Tallinn Manual 2.0 では、サイバー空間における主権侵害の態様を領土に対する完全性への侵害及び本質的な政府機能への妨害または簒奪に区分する。その上で、前者の領土への完全性への侵害については、①物理的被害、②機能喪失、③機能喪失の閾値を下回る領土の完全性に対する侵害の３つのレベルに区分され、①②に関しては多くの法学者が主権侵害に該当すると肯定した一方で、③の場合に関しては意見が一致しなかったとする[155]。③に該当する例としては、機能喪失等にはいたらないものの、重要インフラ事業者等が保有するデータ等の削除や改竄があった場合等が考えられる。後者に関しては、前者のような被害のレベルに関係なく主権侵害に該当するとする。一例として、政府が保有する住民データ等への削除や改竄が考えられる。国防に関する機能も本質的な政府機能であり、国防に関係するデータ改竄等も本区分に該当するであろう[156]。これらの議論を踏まえれば、政府機能に無関係な民間事業者及び個人の SNS 等への不正アクセス行為や情報操作等に関しても機能喪失以上の効果を伴わない場合は主権侵害には該当するとは言えない可能性が高い。また、データの削除や改竄を伴わない espionage に関しても主権侵害には該当しないと考えられる。

ただし、espionage に関しては、espionage そのものは違法でなくとも、espionage を行うためのサイバー作戦の手法によっては主権侵害を構成する可能性はある[157]。一例として、外国領域において公務員等が USB 等を使用して直接情報を窃取する行為は主権侵害となり得る[158]。一方、遠隔地からハッキング等による情報窃取については、Michael N. Schmitt は、脆弱性を特定するためのネットワークへのハッキングなども、主権侵害となるとの考えを示す[159]ものの、Tallinn Manual 2.0 は遠隔地からアクセスによる espionage の違法性に関し、専門家は合意に至らなかったとする[160]。各国による他国のサイバーインフラに対するハッキング行為は常態化している現状では、espionage 目的

---

[155] *See* Michael N. Schmitt, *supra* note 6 at 19-21.
[156] *Ibid.*, at 22.
[157] *Ibid.*, at 170.
[158] *Ibid.*, at 171. また、Francois Delerue は国家による他国領域における領域国家の承認を得な如何なる権力行使も主権侵害を構成するとする。Francois Delerue, *Cyber Operations and International Law* (Cambridge University Press, 2020) at 212.
[159] Michael N. Schmitt によれば 2012 年にサウジアラビアの石油会社サウジアラムコのハードディスクを物理的に破壊することなく何千台ものハードディスクを消去した Shamoon ウイルス攻撃も、主権を侵害したとみなされるべきであるとする。Michael N. Schmitt, "'Below the threshold' cyber operations: the countermeasures response option and international law" (2014) 697 Virginia Journal of International Law at 705.
[160] *See* Michael N. Schmitt, *supra* note 6 at 170.

での遠隔地からハッキングが違法と言える国家実行及び法的確信は確立していないものと考えられる。

不干原則

不干渉原則は、国家は他国の国内管轄事項に関し干渉してはならないとする原則であり、サイバー空間において本義務が適用されることに議論はない[161]。一方で、何が国内管轄事項かという点に関する各国の合意は確立していない[162]。ただし、1981 年の国連総会における干渉不許容宣言は、不干渉義務が適用される対象とし、以下の諸権利の保護が含まれるとした[163]。

- 主権、政治的独立、領土保全、国家的統一と安全保障
- 自国の政治的、経済的、文化的、社会的制度の決定、また天然資源に対する永久主権の行使に関する不可譲の権利
- 世界人権宣言等の条項に基づく自国の政治的、経済的、文化的利益のための情報への自由なアクセス、情報システムとマス・メディアの発展の権利

一般に、ある行為が不干渉義務に違反するかの判断は、上記国内管轄事項に関連し、さらに当該行為が本質的に強制的要素を持つかどうかで判断される[164]。強制要素のない介入は違法な干渉には該当しないとされる[165]。サイバー紛争の場合、ある国に軍事同盟から離脱を強要するため政府機関等に大規模な DDoS 攻撃を仕掛ける場合、あるいは特定の選挙結果を求め他国の選挙システムに侵入し改竄を図る行為等は違法な干渉となる可能性がある。前者に関しては、2007 年のエストニアに対する DDoS 攻撃は典型的な例として挙げられるであろう。また、2014 年のソニーピクチャースエンターテイメントに対するサイバー攻撃に関し、当該サイバー攻撃は、外見上は映画の配給停止を目的とした民間事業者へ攻撃と考えられるものであった。しかし、米国は、当該サイバー攻撃は「単なる一企業へのサイバー攻撃にとどまらない、表現の自由や生き方に対する攻撃でもある」と非難した[166]。当該ケースは、前述の干渉不許容宣言における保護を受ける国内管轄事項の観点からは不干渉原則違反ともとれなくはない。

---

[161] *Ibid.,* at 313. ;杉原・前掲注 129、 177-180 頁。
[162] *Ibid.,* at 314.
[163] *See* U.N. Doc. A/RES/36/103 (9 December 1981).
[164] *See supra* note 138, *para*. 205.
[165] *See* Michael N. Schmitt, *supra* note 6 at 317.
[166] *See* Francois Delerue, *supra* note 158 at 239. *See* also "Statement by Secretary Johnson on Cyber attack on Sony Pictures Entertainment"US Homeland Security (December 19, 2014), online: US Homeland Security <https://www.dhs.gov/news/2014/12/19/statement-secretary-johnson-cyber-attack-sony-pictures-entertainment>.

後者に関しては、選挙結果の改竄には至らないものの、選挙プロセスの一部に影響を及ぼす情報操作型のサイバー攻撃において特に関係が深い類型である。2016 年の米国大統領選における民主党本部へのハッキング事件では、ロシアは不正アクセスにより窃取した機密情報を暴露し、民主党に不利な影響を及ぼそうとしたとされる[167]。このような機密情報の暴露による輿論操作は、選挙のような国内管轄事項に対する干渉であっても、強制要素を満たすかどうかが問題となる。Tallinn Manual 2.0 では多くの学者が、「対象国が本来望んでいなかった決断を行った」という点で強制に該当すると判断したとする[168]。しかし、何が国内管轄事項あるいは強制に該当するかは、依然として不明確である。特に民間事業者・個人のホームページ・SNS 等の改竄、メールによるフェイクニュース流布等のディスインフォメーション活動が強制に該当するかは依然として多くの議論が存在し、明確とは言えない状況である。

また、後述する国内法においては、特定の場合を除きディスインフォメーション活動は違法ではないことにも留意が必要である。

武力攻撃及び武力の行使を慎む義務

国連憲章第 2 条 4 項は違法な武力の行使を禁止する。一方で、国連憲章第 51 条は「武力攻撃が発生した場合」にのみ個別又は集団的自衛権の発動を認めている。この武力の行使と武力攻撃の差異については、様々な議論があるが、ニカラグア事件判決においては武力攻撃を武力の行使の最も重大な形態とし、両者を区分する考えを示した[169]。その上で、軍隊の越境行為は武力攻撃に該当する可能性があるとしつつ、具体的にある行為が武力攻撃に該当するかどうかは「規模及び効果」を考慮しなければならないとした。しかし、いかなる行為が「規模及び効果」の基準を満たすかは判決では明示されなかった。しかし、その後、国際司法裁判所は 2003 年のオイルプラットフォーム事件においては、軍艦一隻の触雷が武力攻撃に該当する可能性があることを示しており[170]、必ずしもその基準が壊滅的な被害を要求するような高いものではないことを示している。この点に関し、Dinstein は、生命維持に関係するコンピュータの制御機能を喪失させることにより人の死傷を引き起こすサイバー攻撃の内、①大規模な電力網の停止（ブラックアウト）による多大な悪

---

[167] *See* Peter B.M.J. Pijpers, *Influence Operations in Cyberspace and the Applicability of International Law* (Northampton: Edward Elgar, 2023) at 112-124.
[168] *See* Michael N. Schmitt, *supra* note 6 at 320.
[169] *See supra* note 138, paras. 194-195.
[170] *See Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America)*, Merits, Judgement of 6 November 2003, [2003] I.C.J. Rep. 161, paras. 64, 72.

影響、②水道やダムを制御するコンピュータの停止による居住地域の洪水、③意図的に操作された、例えば、航空機のコンピュータに誤った情報を送り込むことによる墜落、さらに最も重大なものとして、④原子力発電所の炉心溶融を意図的に引き起こし、放射性物質を放出させ、近隣の住人に多数の死傷者を出すもの、等が武力攻撃に該当すると例示した[171]。この Dinstein の基準は米国国防総省の戦争法マニュアルにおいても同様の基準が示されており、また日本の国会答弁でも引用されている[172]。しかし、現実問題として上記のような損害を引き起こす可能性があるサイバー攻撃を実行することは極めて困難であり、実際、過去のサイバー攻撃の事例において武力攻撃の閾値を満たした攻撃は存在しないと考えられている。一例として、多くの国際法学者が、Stuxnet は、唯一明確な物理的被害が生じ「武力の行使」基準を満たすと考える一方、武力攻撃の基準には至っていないと考えている[173]。

次に、「武力の行使」に関する基準であるが、現状、サイバー攻撃により通常兵器による攻撃と同等の人の死傷や物の破壊を伴う物理的被害が生じた場合、当該サイバー攻撃は「武力の行使」の基準を満たす可能性があることは概ね共通認識が確立されていると考えられる[174]。しかし、物理的被害は生じないサイバー攻撃に関しては意見が分かれる。一部の者は、国家にとって重要なインフラの機能の麻痺が武力の行使に含まれると主張する[175]。特に、フランスは、政府のサイバーインフラへの不正アクセスの時点で武力の行使に該当する可能性があるとする見解を示す[176]。Tallinn Manual 2.0 は、あるサイバー行為が「武力の行使」の閾値を満たすかどうかを判断するための基準として上記ニカラグア判決における「武力攻撃」の基準である「規模及び効果」基準を「武力の行使」にも適用することを提唱する[177]。その上で、具体的な考慮事項として①重大性②結果発生の緊急性③直接性④侵犯性⑤効果の測定可能性⑥軍事的性格⑦国の関与⑧合法性の推定等をあげる。

いずれの見解も、国際社会における共通認識としての地位に至っているものはなく、サイバー空間における「武力攻撃」及び「武力の行使」の基準は依然として未確立な状況である。特に、「武力攻撃」の基準は、後述する自衛

---

171 *See* Yoram Dinstein, *supra* note 25 at 105.
172 *See* U.S. Department of Defense, *Law of War Manual* (2015) at 998.; 第 201 回国会衆議院安全保障委員会第 4 号（令和 2 年 4 月 7 日）河野国務大臣答弁。
173 *See* Michael N. Schmitt, *supra* note 6 at 342.
174 *Ibid.,* at 330-337.
175 Herbert S. Lin, "Offensive Cyber Operations and the Use of Force" (2010) 4 Journal of National Security Law & Policy 63 at 74.
176 NATO Cooperative Cyber Defence Centre of Excellence,"National_position_of_France_(2019)" online: CCDCOE <https://cyberlaw.ccdcoe.org/wiki/National_position_of_France_(2019)#Self-defence,_armed_attack_and_use_of_force >.
177 *See* Michael N. Schmitt, *supra* note 6 at 331.

権と密接な関連を有することから、公表するかどうかは別に、一定の基準となる考え方を政府内で確率しておくことが必要と考えられる。

相当の注意義務

最後の相当の注意義務は「国は、他国の利益を害する目的のために自国の領土を使用することを許可してはならない」とする義務である。具体的には、国家は自国領域内の非国家主体による外国・外国人の権益の侵害を防止するための相当の注意を払わなければならず、また侵害が発生した場合には、適切な救済措置を講ずる義務があるとするものである[178]。ただし、この取締り義務は、国家の現実の能力を超えてまで要求される絶対的性質のものではなく、合理的に期待し得る防止措置をもって足りるとする意味で「相当の注意」義務とされたものと言われる[179]。

本義務に関し、明文上の規則はないものの、広く慣習法化していると認識されている。国際司法裁判所は、1949 年のコルフ海峡事件において「領域を他国の権利に反する行為にそれと知りつつ使わせてはならないすべての国の一般的義務」の存在に言及している[180]。また、GGE の最終報告書において提唱された国際規範にも同内容が含まれている[181]。一方で、その細部の要件や射程は不明確である[182]。サイバー空間において相当の注意原則を活用する最大の利点は、attribution を行うにあたって、違法行為の実行者と領域国家との間に「実効支配基準」のような厳格な証明を必要としないことであると考えられる。ハッキング集団等の非国家主体国際法上の義務違反となり得るサイバー攻撃がある領域国家から生じ、当該行為に対する領域国家の関与が不明確な場合であっても、被害国からの再三の取締り要請にも関わらず当該領域国が何等対応を行わない場合等は相当の注意原則違反として当該領域国の責任を追及できる可能性がある。本点に関し、日本は外務省が 2021 年に公表した文書「サイバー行動に適用される国際法に関する日本政府の基本的な立場」において、「相当の注意義務は、国家に帰属しないサイバー行動に対しても、同行動の発信源となる領域国に対して、国家責任を追及する根拠となり得ると考えられる。」との立場を表明している[183]。

---

178 杉原・前掲注 129、515 頁。
179 杉原・前掲注 129、516 頁。
180 *Corfu Channel case*, Judgment of 9 April 1949, [1949] I.C.J. Reports 244 at 22.
181 前掲注 67。
182 *See* Michael N. Schmitt, *supra* note 6 at 43.
183 外務省・前掲注 144、4-5 頁。

5.3 サイバー空間における国際違法行為への対応

次に、国際違法行為への対応要領について検討する。国際紛争の解決にあたって国連憲章 33 条は紛争の平和的解決手段を定めるが、現実のサイバー紛争においては有効に機能しているとは言い難い状況であり、より強力な対応手段が求められる。このため、特に他国の国際義務違反に対応する観点からは、国家責任条文が定める各種の違法性阻却事由を活用が考えられる。違法性阻却事由は、本来であれば国際違法行為となる行為であっても、一定の状況下ではその違法性が阻却されるとするものである。つまり、違法性阻却事由が得られる特定の状況下においては、本来は国際義務違反となるレベルでの対応行動が許容される可能性があるということである。国家責任条文では「同意」「自衛」「対抗措置」「不可抗力」「遭難」及び「緊急事態」の６つの類型が定められている。本稿では、「自衛」及び「対抗措置」について焦点を当て検討を行う。

5.3.1 サイバー攻撃への自衛権適用

自衛を利用した場合、「武力の行使」を含む強力な反撃と集団的自衛権の行使が可能となり、紛争を早期に終了させ、被害を最小限にする可能性がある。また、一定の場合、非国家主体に対して行使し得る可能性もあり、[184]自衛権の適用には多くの利点が存在する。しかし、国連憲章上、自衛権の行使は武力攻撃が発生した場合にのみ可能とされ、武力攻撃の閾値に至らない武力の行使レベルのサイバー攻撃がおこなわれた際は、自衛権による対応は出来ないことになる。その場合、後述する国家責任法上の対抗措置を取り得る可能性がある。一方で、一般的見解では対抗措置においては武力の行使に該当する行為は行えないとされている。つまり、武力攻撃には至らないが、武力の行使の閾値を満たすサイバー攻撃に対し、同等の強度での反撃は出来ないというギャップが生じている[185]。この問題に対し、アプローチとしては、以下の３つが考えられる。

① 武力攻撃に至らない武力の行使に対しても自衛権の発動を認める

---

[184] 2001 年 9 月 11 日の同時多発テロ事件以降、非国家主体に対する自衛権の行使に関する学説に変化が見られ、領域国が自国から行われる非国家主体による武力攻撃に実行的に対応する能力及び意思を欠く場合は自衛権行使が認められるとする説が有力に唱えられるようになった。*See* The Chatham House, “Principles of International Law on the Use of Force in Self-defence” (2006) 55(4) *The International and Comparative Law Quarterly,* 963-972.

[185] 当該ギャップに関しては以下を参照 Sean Watts, "Low-Intensity Computer Network Attack and Self-Defense" (2010) 87 *International Law Studies* 59-87.

② 武力攻撃の閾値を下げ、自衛権の適用を容易にする。
③ 対抗措置の手段に武力の行使を認める。

①のアプローチに関しては、米国は武力攻撃と武力の行使を区別せず、「武力の行使」に対しても自衛権を行使可能と主張する[186]。また、国連憲章とは別に慣習法の自衛権が存在し、武力攻撃に至らない武力の行使に対しても慣習法上の自衛権の行使が可能とする、いわゆるマイナー自衛権の議論が存在し[187]、日本政府の見解も「武力攻撃に至らない武力の行使に対し、自衛権の行使として必要最小限の範囲内において武力を行使することは一般国際法上認められる」とする[188]。上記を踏まえれば、国際法上、武力攻撃に至らない低強度のサイバー攻撃に対しても自衛権適用が完全に排除されるわけではないと考えられる。

②のアプローチは、「人の死傷や、物の破壊」といった従来の武力攻撃の閾値に至らないサイバー攻撃、特に、重要インフラに対する攻撃による重大な経済的損害等に対しても自衛権の適用を認めようとするものである。フランスは、国の活動全体を麻痺させるよう重大な経済的損失に対しては、武力攻撃の閾値を満たし、自衛権を適用する可能性があることを示唆する[189]。前述した通り、サイバー空間における武力攻撃と武力の行使の概念は未確定であるが、自衛権発動の要件となる武力攻撃に関しては、通常兵器による攻撃と同等の物理的損害が必要との意見が一般的である。しかし、近年は社会における ICT への依存の高まりにより、変化が見られる。Michael N. Schmitt は近い将来、経済的なサイバーインフラへの攻撃や経済システムを破綻させるようなサイバー攻撃は、武力攻撃と認定されるだろうと評価する[190]。国内においても、サイバー空間における attribution の困難性や攻撃の優位性という観点から、サイバー攻撃に関しては、他の物理的な武力攻撃と区別し、より幅広い自衛権の適用を考慮すべきとする意見も根強い[191]。

ただし、上記①、②の見解は、いずれも一般的な見解とは言えない。特に、

---

[186] *See* U.S. DoD, *supra* note 172 at 47.
[187] Julius Stone, "Law, Force and Survival" (1961) 39(4) foreign Affairs 553-557 <https://www.jstor.org/stable/20029510>.
[188] 第 143 回国会衆議院外務委員会議録第 4 号（1998 年 9 月 18 日）高村正彦外務大臣答弁。なお、当該見解は飽くまで一般国際法上の解釈であり、国内憲法上の解釈とは異なることに注意が必要である。本議論の詳細に関しては、村瀬信也編『自衛権の現代的展開』（東信堂,2007）259-265 頁参照。
[189] *See* CCDCOE, *supra* note 176.
[190] *See* Michael N. Schmitt, “International Law and Cyber Warfare” (March 28, 2013), online: C-SPAN <https://www.c-span.org/video/?311806-1/international-law-cyber-warfare>.
[191] 一例とし、安保克也「日本国憲法と安全保障-サイバー戦の視点から-」『憲法論叢』15 号 101-126 頁（関西法政治学研究会、2008）。また、意味するところは不明確であるが、自由民主党「自民党サイバーセキュリティ対策本部：第一次提言～リスクの最小化に向けて。「コスト」から投資への意識改革を～」（2018.4.24）<https://www.jimin.jp/news/policy/137263.html>は、「サイバー自衛権」創設を提唱する。

①のアプローチは国連憲章上の解釈とは異なることから、賛同する意見は少ない。一方で②のアプローチは、将来的に社会における ICT への依存度の更なる高まり等により変化する可能性は十分に存在するが、現状として一般的な見解とは言えない。また、低強度のサイバー攻撃に対する自衛権適用は、法的な観点からだけでなく、現実の紛争におけるエスカレーションコントロールの観点からも留意が必要である。自衛権適用を公式に表明し「武力の行使」に踏み切ることは、本格的な武力紛争にエスカレートする危険性が極めて高いことは認識されなければならないであろう。

また、日本の場合、国内法の観点からは、憲法解釈との整合性が問題となる。現状の日本政府のサイバー攻撃と自衛権の行使との関係に関する見解は、国連憲章及び従来の憲法解釈に準じた極めてオーソドックスなものである。すなわち、具体的な基準については個別の状況に応じて判断すべきものとし明言は避けつつ、「武力攻撃の一環としてサイバー攻撃が行われた場合には、自衛権を発動して対処することは可能と考えられる。」[192]とし、また、サイバー攻撃と武力攻撃の基準との関係に関し、「物理的手段による攻撃と同様の極めて深刻な被害が発生し、これが相手方によって組織的、計画的に行われている場合」[193]は武力攻撃に該当する可能性があるとする。これらの日本政府の解釈を考慮した場合、上記①②のアプローチは従来の見解を大きく変化させるものであり、憲法との抵触も懸念される。憲法改正に係わる議論を伴えば議論の長期化は避けられず、日本周辺の安全保障環境の急激な変化に対応するという観点からは、やや現実的とは言い難いであろう。

5.3.2 対抗措置による対応

残る③は、①②の自衛権の適用による対処と異なり、対抗措置による対応を目指すアプローチである。対抗措置は、「武力の行使」から主権侵害まで幅広い国際違法行為に適用可能であり、かつ紛争のエスカレーションを避けつつ、本来では国際違法行為とされるような、ある程度の強硬な実力行使が可能であることから、被害国にとって有力な選択肢となる可能性がある。この点で、対抗措置は経済制裁等の国際法上合法な行為による対応である「報復（retorsion）」とは区別される[194]。一方、前述の通り、対抗措置として武力の

---

[192] 内閣衆質 189 第 71 号「衆議院議員緒方林太郎君提出サイバー攻撃と自衛権との関係に関する質問に対する答弁書」（2015.2.24）。
[193] 前掲注 172。
[194] 相手国による国際違法行為または違法でないが非友好的な行為に対し、経済制裁等の国が裁量によってとる国際法上合法ではあるものの非友好的な措置は、報復と呼ばれ対抗措置とは区別される。黒崎将広ほか『防衛実務国際法』（弘文堂、2021）772 頁。

行使が可能かは意見が分かれるほか、対抗措置の実行に当たっては様々な要件が存在する。国家責任条文で定められた要件は以下のものである。

外国からの国際違法行為の存在及び継続

対抗措置は、外国からの国際違法行為に対応するために特別に違法性が阻却されるものであるため、外国からの国際違法行為が現に存在することが要件である。国家責任条文 49 条 1 項は対抗措置の目的を「(責任国が) 義務に従うように促すためにのみ対抗措置を取ることができる。」とし、責任国の国際違法行為が終了した後の報復目的の行為を禁止する。つまり、対抗措置を実行するためには、違反国の国際違法行為が継続することが要件となる。国際違法行為の継続に関し、同 14 条 2 項は、「継続的性質を有する国の行為による国際義務の違反は、その行為が始まる時点で生じる」とし、行為が開始された時点から国際違法行為が認定される。また、「違反が行われる時間は、その行為が継続し及び国際義務と一致しない状態が続く全期間に及ぶ」とし責任国が義務に復帰した時点をもって終了となることを示す。ただし、サイバー空間においては、状況はやや複雑である。まず、高度なサイバー攻撃は、ある程度侵害行為が進展し明確な損害が出ない限り被害国が気付かない場合もあり、どの段階から国際義務違反が生じていたかを判断するのが困難である。また、サイバー攻撃が反復的かつ継続的に実施される場合、個別のサイバー攻撃が終了した時点を終期とするか、一連のサイバー攻撃が全て終了した時点をもって終期とするかで判断が難しい。同 15 条 2 項は、複合的な行為の場合、個々の行為が繰り返されかつ国際義務と一致しない状態が続く限り継続するとするが、個々の行為の関連性をどのように判断するのかは不明確である。特に、DDoS 攻撃が複数の領域国のドメインから行われた場合や、特定のサイバー攻撃が期間を空けて実行された場合に、それぞれの個々のサイバー攻撃を一連行為として見なすための客観的指標が存在しないことは、継続性を判断する上で大きな課題である。

均衡性

対抗措置においては、先行する国際違法行為の違法性との間に均衡性が要求される。しかし、均衡性に関する具体的な判断基準は明確ではない。国家責任条文 51 条は、均衡性について「国際違法行為の重大性及び関連する権利を考慮して、被った侵害に見合ったものでなければならない」とする。簡単に言えば、相手側の国際違法行為により生じる損害と同程度の被害を及ぼす

程度の対抗措置ならば許容されると考えられる[195]。しかし、均衡性とは相手の国際違法行為を停止させるために必要な限度のことであるとする意見も存在し、見解は一致しない[196]。米国は、国家責任条文の起草過程において、国家責任法における均衡性には、受けた被害との均衡性に加え、違反国を義務に復帰させるために必要な程度との均衡性の二つの側面があると指摘し、国家責任条文は一面しか見ていない不十分なものであると批判した[197]。

均衡性で特に問題となるのは、相当の注意義務違反の場合である。一般的な見解に立つ場合、相当の注意義務違反を理由に違反国に対抗措置を行う場合は、受けたサイバー攻撃の程度ではなく、違反国の防止義務違反の程度に応じた対抗措置しか取れないことになる。一方、米国の見解に立てば、当該サイバー攻撃を停止させるための防止義務を領域国が果たすように強制するのに必要な限度で対抗措置が行なえることになる。また、その手段に特に制限はないとされ、サイバー攻撃に対し、サイバー空間以外での物理的措置を対抗措置として行うことも可能である。

武力の行使の禁止

国家責任条文 50 条は、対抗措置は、武力による威嚇または武力の行使を慎む義務に影響を与えるべきではないとし、「武力の行使」に該当する行為を対抗措置として行うことは出来ないとする。従って、同規定をそのままあてはめれば武力の行使に該当するサイバー攻撃に対し、被害国は武力の行使未満の行為しか対抗措置として取ることは出来ない。しかし、国家責任条文は拘束力を有する条約ではなく、全ての条文が慣習法を反映している訳ではない。同規定が、慣習法としての性格を有しているか、という点について疑義があり、対抗措置に武力の行使が含まれるとする説を取る者も存在する[198]。とりわけ、前述のオイルプラットフォーム事件における Simma 判事の個別意見[199]は、自衛権行使と対抗措置との法的間隙が、国際違法行為を助長する可能性があることを指摘し、武力攻撃の閾値以下の「武力の行使」に対しては、軍

---

[195] *See* Michael N. Schmitt, *supra* note 6 at 130.
[196] 岩月直樹「現代国際法上の対抗措置制度における均衡性原則－国際紛争処理過程における対抗措置の必要性に照らしたその多元的把握の試み」立教法学第 78 号 206‐299 頁（2010） 223 頁。代表的な論者として、*See* Elisabeth Zoller, *Peacetime Unilateral Remedies : An Analysis of Countermeasures* (Martinus Nijhoff Publishers, 1984) at 46-75, 131-137.
[197] "United States: Comments on the draft articles on state responsibility"(1998) 37(2) International Legal Materials 468 at 471.
[198] 宮内靖彦「自衛の発動要件にとっての非国家的行為体の意味－国際判例の観点からの分析－」村瀬信也編『自衛権の現代的展開』（東信堂, 2007）153-158 頁。
[199] See Oil Platform case, *supra* note 170, Separate Opinion of Judge Simma, paras. 11-12.

事的性質を持つ「比例的対抗措置」を取ることができるとの見解を示し、大きな影響を与えた。Tallinn Manual においても、少数の専門家が対抗措置に武力の行使を含めることを主張したとする。日本政府も国際法上の解釈として武力の行使が含まれる可能性があるとする見解を示している[200]。ただし、これらの意見は現状として多数派とは言えず、一般的には対抗措置として武力の行使に該当する行為は実施できないと考えられている。

対抗措置における武力の行使の禁止は、前述の均衡性及びサイバー空間における武力の行使の概念との関係に大きな影響を及ぼす。特に課題となるのは、重要インフラへのサイバー攻撃である。近年では、重要インフラへのサイバー攻撃が「武力の行使」の基準を満たすとする見解が増加しつつある。仮に、責任国が重要インフラへのサイバー攻撃を「武力の行使」と見做すと宣言する一方で、対抗措置を実行する被害国が物理的被害を伴わないサイバー攻撃は「武力の行使」ではないと判断していた場合、両者の見解に相違が出る。対抗措置を受けた責任国は、違法な「武力の行使」を受けたと判断し、紛争がエスカレーションする可能性は否定できない。

要請、事前通告及び交渉提案の義務

また、国家責任条文 52 条 1 項では、対抗措置を実施する前に責任国に義務に復帰するよう要請をすること、対抗措置を取る旨の通告、交渉提案等を行うことを定める。このうち、対抗措置を取る旨の通告及び交渉提案義務は、続く２項において緊急の場合は免除されると規定されている。サイバー作戦は、進展が極めて速く、多くの場合は緊急の場合に該当すると考えられる。また、事前に交渉を行うことは相手に対抗措置の実行を予期させ、対応の暇を与えることにより対抗措置の効果を減ずる可能性があることから、サイバー空間における上記義務の存在に関しては、多くの国際法学者が否定的な見解を示している[201]。

集団的対抗措置

上記要件とは別に、集団的対抗措置の可否について議論が存在する。自衛においては、ある国家が武力攻撃を受けた場合に直接に攻撃を受けていない第三国が共同で防衛対処する集団的自衛権が認められる。同様に、武力攻撃に至らない国際違法行為に対し、第三国が対抗措置を行うという考えが集団

[200] 第 143 回国会衆議院外務委員会議録第 4 号（1998 年 9 月 18 日）14 頁東郷条約局長答弁。
[201] *See* Michael N. Schmitt, *supra* note 6 at 120.

的対抗措置である。集団的対抗措置は様々な利点が考えられる。特に、サイバー作戦は地理的な制限がなく、物理的に離隔した国からも実行可能であることから、第三国の関与が容易であり、より実効性ある枠組みとなる可能性がある。また、被害国が技術的に責任国に対し劣る場合に、より優れた技術を保有する第三国に対抗措置を依頼することも可能となる。

しかし、現状、対抗措置が国際法上合法として許容されるかは明確ではない。前述のニカラグア事件判決では、集団的対抗措置は明確に否定されており[202]、Tallinn Manual 2.0 でも大多数が否定的見解であることを示している[203]。しかしながら、国家責任条文は、49 条において対抗措置を取り得る国を被侵害国に限定する一方、48 条において特定の場合には被侵害国以外の第三国が責任国の責任を追及できる枠組みを示し、集団的対抗措置が許容される余地を残しているようにも見受けられる。また、集団的対抗措置の必要性を主張する見解は多数存在し[204]、2019 年の CyCon[205]では、エストニアの Kaljulaid 大統領が集団的対抗措置の必要性を訴える演説を行っている。サイバーセキュリティ政策の最前線にいる NATO 加盟国の大統領が、集団的対抗措置の利用を明確に促したことは注目に値する。

特に、現状、対象国に比し劣勢なサイバー作戦能力しか有しない日本にとって、非常に強力なサイバー作戦能力を有する米国との同盟関係を生かすためには対抗措置は極めて有益な法的枠組みであり、積極的に合法化を推進すべきである。

5.4　対抗措置適用にあたっての具体的課題

平時～GZ 事態における対応において、対抗措置を活用することは様々な利点が存在する。第一の利点として、対抗措置は、主権侵害から武力の行使に至る幅広い国際法違反に対応可能である。第二の利点として、相当の注意原則を活用することにより、attribution 問題を回避できる可能性がある点も有利である。第三の利点として、最も重要な利点であるが、紛争のエスカレーションを防止しつつ、低強度の侵害に実効性ある対応が可能であるという点である。特に三つ目の利点は重要であり、平時からＧＺ事態においては、外国からの低強度の侵害に対応することも重要ではあるが、最も優先すべきは武力紛争へのエスカレーションを避けることである。その意味において、責任

[202] *See supra* note 138, paras. 248-249.
[203] *See* Michael N. Schmitt, *supra* note 6 at 132.
[204] Gary Corn and Eric Talbot Jensen *supra* note 22; Jeff Kosseff *supra* note 72.
[205] NATO Cooperative Cyber Defence Centre of Excellence's annual Cyber Conference.

国の国際違法行為の継続や武力の行使の禁止といった制約は逆にエスカレーションを防止の観点からは有益なものと考えられる。一方で、実際にサイバー攻撃に対し対抗措置を適用するにあたっては、様々な課題が存在する。

5.4.1 attribution の法的基準

第一に、attribution の問題である。相当の注意原則の活用により、ある程度緩和される可能性があるとは言え、サイバー空間において attribution を可能にするレベルの情報収集活動を行うことは極めて高い技術レベルが要求される。技術的な問題に加え、証明基準に関する法的曖昧性は、対抗措置の実効性を損なう大きな課題である。明確な基準が無いことは、ケースバイケースの判断が求められることを意味する。ケースバイケースの判断は一見柔軟性があるように思われる。しかし、実際には、事案が発生した際に個別の状況に応じて一から基準を判断することを意味し、迅速な対抗措置発動を阻害する可能性が高い。サイバー作戦は進展速度が他の領域における作戦よる早く、急速に被害が拡大する可能性が高い。また、対抗措置自体が責任国の国際違法行為が継続している間しか発動出来ないため、迅速に決心し、実行に移す必要がある。attribution には精密だけでなく、適時性も要求されることを意識することが必要である。

5.4.2 武力の行使の禁止

本章の冒頭で述べた通り、武力攻撃に至らないものの、武力の行使に相当するサイバー攻撃に対し、対抗措置では武力の行使に至らない程度の行為でのみしか対応できない。このため、責任国を義務に復帰させる強制力が不足をする可能性がある。また、サイバー空間における武力の行使の定義によっては、被害国による対抗措置の実行が、逆に違法な武力の行使と認定される可能性も否定できない。本課題に対する効果的な対応策を見出すことは困難であるが、重要なことは対抗措置としてサイバー作戦を実行する際は、効果をコントロールすることが重要であること認識する必要がある。意図した効果を高い精度で実現できるならば、強制力の不足を補える可能性があり、かつ違法な「武力の行使」との誤解を避けることが可能である。このため、サイバー作戦をコントロースする技術力の向上とともに、相手の弱点や重心をピンポイントで攻撃するための情報収集能力の向上が必要不可欠である。

5.4.3　集団的対抗措置の合法性

集団的対抗措置の合法性が不明確であることも大きな課題である。対抗措置は低強度とは言え、実力行使を伴うものである。サイバー攻撃に対し、被害国がサイバー作戦により対抗措置を行う場合、責任国に対しサイバー作戦能力が圧倒的に劣る場合は対抗措置の実行可能性すら危ういものとなる。優れたサイバー作戦能力を有する第三国による集団的対抗措置が合法化されれば、対抗措置の実効性や信頼性が格段に増すことが予想される。一方で、容易に集団的対抗措置を認めることは、濫用の可能性を増加させる。特に匿名性の高いサイバー空間では、集団的対抗措置の名目で違法なサイバー作戦が容易に実行される可能性がある。このため、集団的対抗措置を実現するにあたっては、少なくとも集団的自衛権の行使と同程度の明確性をもつ要件を確立し、濫用を防止する枠組みを設ける必要があるであろう。

国際違法行為に該当しないサイバー攻撃への対応

また、国際違法行為に該当しない espionage やディスインフォメーション活動への対応は、対抗措置以外の法的対応を考える必要がある。特に、espionage に関しては、国家運用において必要悪として見る考えもあり、条約等により違法化する方向性は考え難い。このため、どこまでが許容され、どこからが許容されないのか、という基準を明確化する国際規範を形成していくことが重要である。関係国と共同し、国際規範の浸透を図り、Public attribution や報復、あるいは実行犯の国内訴追といった非友好的ではあるが合法的な措置を組み合わせることでルール整備を行っていくことが重要である。

ディスインフォメーション活動への対応については、表現の自由との関係が問題となり、国際法上も国内法上も法規制が難しい問題である。前述したように、ディスインフォメーション活動を含む影響力工作が、選挙介入等の違法な干渉に該当する場合は、国家責任法による対応が可能であると考えられる。しかし、どのような場合に違法な干渉となるかは依然として明確ではない。まずはどのようなディスインフォメーション活動が違法な干渉に該当するか、という点について共通認識を確立することが必要であろう。その上で、国際違法行為に該当しない影響力工作についても、外交政策等を通じた国際規範の形成等によるルール整備図っていくことが必要である。しかしながら、国際法による対応は政治情勢やパワーバランス等の影響を受けることから即効性や有効性が期待できない可能性が高く、過度に期待することは避けなければならない。このため、国内法整備による対応を検討することや、

政府の透明性及び説明責任の状況改善、国民の情報リテラシー向上といったresilience の向上等の国内における総合的な対策を早急に検討していく必要があるであろう。

ディスインフォメーションを巡る問題については、現状では法的規制が難しい問題であることから、本稿では詳細には触れない。しかしながらサイバー作戦の法規制を考慮するうえで重要な問題であることは間違いなく、残された課題として今後検討が行われるべきと考える。

5.5 小　結：日本が取り得るべき措置

日本の観点からみれば、対抗措置の活用は、自衛と異なり憲法との抵触が無いことは具体的な適用を追求する上で有利な点である。一方で、後述するが、現状日本の国内法には対抗措置を実行するための根拠法が存在しない。このため、対抗措置を実行するためには第一に国内法の整備が必要となる。また、国内法整備に併せ、上記課題に関連し、現状として不明確な対抗措置の要件及び基準等について、日本に有利な解釈が一般化するよう積極的に主張を行っていくべきである。特に、対象国に比し現状として相対的に劣勢なサイバー作戦能力しか保有しない日本にとって、集団的対抗措置の合法化を進めることは重要である。米国を始めとする関係国と密接に連携し、ルール整備を進めていくべきである。

Ⅵ　平時～GZ 事態におけるサイバー攻撃への対応（国内法）

6.1　サイバー空間の脅威に対する日本の安全保障体制

本章では、前章に引き続き平時～GZ 事態を扱い、特に国内法上の課題について述べる。従来の日本の安全保障法制は、平時と有事を明確に線引きしている。紛争のエスカレーションに応じ段階的に事態認定がなされ、それに伴い政府及び防衛省・自衛隊の権限が拡大していく態勢となっている。このため、GZ 事態のように明確な事態認定が困難な状況、あるいはサイバー攻撃のように急激に事態が進展する状況への対応が難しい。また、サイバー安全保障における日本の各府省庁の役割区分の不明確性も大きな課題である。冒頭で述べた通り、サイバーセキュリティ基本法 19 条で示されるサイバー安全保障における各府省庁の役割区分は現在に至るまで法的に未確立な状態が継続している。加えて、日本の国内法はサイバー空間における行政機関の活動

に対し「通信の秘密」を始めとする極めて厳しい制約を課しており、各行政機関がサイバー攻撃に対し柔軟かつ迅速に対応することが難しい状況となっている。このような状況において、能動的サイバー防御構想が発表されたわけであるが、政府及び防衛省・自衛隊に付与される具体的な権限については依然として明らかにされていない。

6.1.1 能動的サイバー防御構想

能動的サイバー防御構想は、ＧＺ事態を念頭に置いた概念と考えられる。しかしながら、従来は、自衛隊による他国が所有するネットワークへの侵入・無害化を図る「妨げる能力」の使用は、武力攻撃事態以降が想定されてきた[206]。仮に、平時からＧＺ事態においても「妨げる能力」を行使するならば、安全保障における従来の姿勢を大きく転換するものであり、大きな前進であると評価できる一方で、法的な問題は多数存在すると考えられる。また、内閣サイバーセキュリティセンター（以下、「NISC」と略。）を発展的に改組し、新たな組織を設ける構想も明らかにされているが[207]、従来の安全保障態勢との関係や、各関係省庁の役割分担、特に警察と自衛隊の役割分担等を含めて組織編成上の課題も大きいと考えられる。

6.1.2 サイバー領域における自衛隊の任務・権限の不明確性

前述の通り、サイバー攻撃は、一旦攻撃が発覚したならば極めて急速に進展し一挙に被害が拡大するため、防御側は迅速な対応が求められる。しかし、各省庁間の役割未分化は、サイバー攻撃に対する迅速な対応を阻害する可能性が高い。現状、NISC に調整機能、警察及び自衛隊のそれぞれに対処組織が存在するが、各組織の役割分担が不明確であれば事態に直面した際に有効に連携して対処することは難しいと考えられる。重要インフラ防護に関しても状況は同じであり、具体的な事態対処要領に関し、各省庁の任務・役割区分等は明確化されていない。特に問題となるのは、国防の中枢を担う自衛隊に対し平素サイバー空間において付与される任務及び権限が不明確であることである。

従来、自衛隊の任務の基本は外国からの武力攻撃への対処であり、武力攻

---

[206] 第 201 回国会参議院外交防衛委員会会議録第 9 号槌道明宏防衛省防衛政策局長答弁（令和 2 年 4 月 16 日）。

[207] 国家安全保障戦略は「能動的サイバー防御を含むこれらの取組を実現・促進するために、NISC を発展的に改組し、サイバー安全保障分野の政策を一元的に総合調整する新たな組織を設置する。」とする。前掲注 17 22 頁。

撃事態が認定されるまでは、対処の主体は警察及びその他の組織が担うとされてきた。サイバー空間においても同様であり、武力攻撃に至らないサイバー攻撃は、犯罪として扱われ、警察及びNISCが対応の中心となってきた[208]。しかし、３章で述べた米国のサイバー抑止理論の発展が示すように、国家が関与するサイバー攻撃は、たとえ武力攻撃に至らない場合であっても安全保障上の重大脅威となる可能性があり、平素から自衛隊を有効に活用することが本来望ましいと考えられる。一方で、自衛隊には、平素サイバー空間における具体的な任務・役割及び権限は、少なくとも明示的には付与されていない。

自衛隊の各種行動及び権限は自衛隊法（以下、「隊法」と略。）によって規定される。しかし、隊法にサイバー空間での行動権限を明示的に規定する条文はない。武力攻撃事態が認定され隊法 76 条の「防衛出動」が発令された場合は、隊法 88 条が定める包括的な作戦行動権限である「武力の行使」の権限に基づき「妨げる能力」の使用が想定される[209]。しかし、防衛出動が発令されるまでは、自衛隊がサイバー作戦を行うための法的根拠は不明確である。この点に関しては、国家安全保障戦略においても具体的な記述は見られないが、仮に能動的サイバー防御構想において何らかの役割を自衛隊に期待するならば、本論点は重要な課題になると考えられる。

6.1.3　サイバー空間における自衛隊の権限

自衛隊は強力な兵器を保有する一方で、国内法上の地位は一行政機関に過ぎず、他省庁と同様にその活動は行政法上の各種原則に基づくことが求められる。自衛隊の行動は、隊法第６章「自衛隊の行動」において具体的に規定されており、外国からの武力攻撃に対応する防衛出動、間接侵略その他の緊急事態等に対応する治安出動、自衛隊施設及び米軍基地をテロ行為から防護する警護出動等が定められている。続く隊法第７章「自衛隊の権限等」では、各行動の際に認められる権限が規定されるが、防衛出動以外の各種行動における権限の大部分は「武器の使用」（以下、「武器使用」と略。）として規定されている。従って、この「武器使用」権限がサイバー空間においてどのような意義を持つかを検討することが重要である。

また、「武器使用」を適切に行うためには行為者の特定が不可欠であり、そのためには性格な情報を入手することが必要であるが、自衛隊が平素行う情報収集活動は根拠法令が不明確という課題も存在する。外国からのサイバー

[208] 前掲注 3 19-28 頁。
[209] 前掲注 206。

攻撃に対しては、国際法上の attribution の観点からも正確な情報入手が必要不可欠であり、平素の情報収集活動に対する法的根拠の不存在は深刻な課題と考えられる[210]。

このため、本項では、まずサイバー空間における自衛隊による平素の情報収集活動についての法的課題を明らかにする。次に、比較対象として米国連邦法におけるサイバー作戦の法的位置付けを考察する。その後、「武器使用」とサイバー作戦の関係について整理を行い、さらに安全保障上の重要問題である重要インフラ防護を例として、自衛隊のサイバー空間における任務・役割を論じる。その上で、本章の結論として、能動的サイバー防御を行う上での自衛隊のあるべき任務、役割、権限及び必要な法改正等について提言を行う。

6.2　自衛隊が行う情報収集活動の法的根拠

平素より自衛隊は、航空機・艦船及びレーダー等による領海・領空の警戒監視及び外国軍事通信の傍受等、様々な情報収集活動を行っている。しかし、自衛隊が平素行う情報収集活動に明文上の根拠規定はない。自衛隊の情報収集活動の根拠として防衛省設置法４条が規定する調査・研究を挙げる場合があるが[211]、設置法は行政組織の任務・所掌を規定するものであり、具体的な権限を付与するものではなく判例上も否定されている[212]。このため、第一に自衛隊が行う情報収集活動の法的位置付けを明らかにすることが必要である。

6.2.1 任意調査としての情報収集活動と「通信の秘密」

任意手段と強制手段

一般に、行政機関によって行われる、行政目的達成のための調査（情報収集）活動を行政調査と呼ぶ[213]。行政調査は、強制調査、間接強制を伴う調査、任意調査に区分される。強制調査は、相手方に義務を課し、または相手方の抵抗を排除しても行うことが出来る調査である。また、間接強制を伴う調査とは、罰則により担保された調査の事を指す。いずれも、法律による根拠が

[210] attribution に関する議論の詳細は前章を参照
[211] 内閣衆質 201 第 9 号（2020.1.31）「衆議院議員櫻井周君提出自衛隊の中東海域への派遣の法的根拠に関する質問に対する答弁書令」。
[212] 仙台地判平成 24 年 3 月 26 日判例時報 2149 号 99 頁。
[213] 宇賀克也『行政法概説 I 行政法総論』第 7 版（有斐閣、2020）146 頁。

必要とされるが、隊法にはこのような権限を規定した条文はない[214]。一方で任意調査は、相手方の任意の協力を得て行われる調査であり、個別具体的な法律の根拠は必要ないとされる[215]。従って、行政法の観点から見れば、自衛隊の情報収集活動は任意調査と位置付けることが出来ると考えられる。

しかし、任意調査においては、強制にわたる手段（以下、「強制手段」と略。）は使用できないとされる[216]。特に重要な点は、行政機関がプライバシーあるいは私的領域を侵害する行為は、強制手段に該当すると解されていることである[217]。「通信の秘密」や「プライバシー」という重要な権利・利益を実質的に侵害する行為は、対象者が認識をせず、意思が制圧されているとは言えない状況であっても黙示的な意思に反し、強制手段に該当すると考えられている。GPS 捜査事件判決[218]では、憲法 35 条が、「住居、書類及び所持品」に準ずる私的領域に「侵入」されることのない権利を保障しているとし、そのような私的領域を侵す行為は強制にわたると判示した。この点を踏まえれば、任意調査活動においては通信の秘密を侵害する行為は出来ないと考えられる。実際、自衛隊情報保全隊による自衛隊イラク派遣への反対活動に対する監視活動の合法性が問われた監視活動停止等請求事件では、情報収集全般の必要性は認めつつも、収集した個人情報と収集目的に関連性が認められない場合は違法となり得ることを判示した[219]。従って、サイバー空間においても、自衛隊が個人のプライバシーを侵害するような情報収集活動を行うことは強制手段に該当し、特別な法令根拠なしには難しいと考えられる。また、個人情報の保護に関する法律（令和３年改正）64 条は、行政機関に対し「偽りその他不正の手段により個人情報を取得してはならない。」とし、ハニーポットのような受動的手段であっても、身分を偽り相手に通知することなく個人情報を収集する手段については慎重な検討が必要と考えられる。

また、強制手段に該当しなければ、どのような情報を収集しても良いわけではない。国内の反自衛隊活動に関する情報収集が問題となった自衛隊情報保全隊事件では、自衛隊が行う情報収集活動自体の合法性は否定されなかったものの、その収集内容の必要性、特に目的との関連性が問われた[220]。判決

---

214 他に警察官職務執行法が準用される場合に職務質問、立ち入り等が可能であるが、これらも任意調査であり、かつ平素は行使できない。

215 塩野宏『行政法 I〔第六判〕行政法総論』（有斐閣、2015）259 頁。田村正博『警察行政法解説』第 2 版補訂版（東京法令出版、2019）333 頁。仙台高判平成 28 年 2 月 2 日判例時報 2293 号 18 頁。

216 最判昭和 53 年 9 月 7 日刑集 32 巻 6 号 1672 頁。

217 最大判平成 29 年 3 月 15 日刑集 71 巻 3 号 13 頁

218 最大判平成 29 年 3 月 15 日刑集 71 巻 3 号 13 頁

219 仙台高判・前掲注 215。

220 仙台高判・前掲注 215。判決は「行政機関が行う情報収集活動について、常に個々の法律上の明文規定が必要とまでは解されない。」とした上で、一部の収集内容について必要性を認め難く、違法と判断した。本事件の詳細については安保克也「行政機関と個人情報－自衛隊情報保全隊事件を題材に－」防衛法

では、情報収集行為の合法性判断について「情報収集行為の目的、必要性、態様、情報の管理方法、情報の私事性、秘匿性の程度、個人の属性、被侵害利益の性質、その他の事情を総合考慮する必要がある」とした。調査活動に限らず、任意活動の限界は、①当該行政機関の任務・所掌の範囲内であること、②事実上の強制にわたることの禁止及び③法令に違反することの禁止、とされる。加えて、任意活動であっても国民に実質的な不利益を与えるものについては、与える不利益を上回る公益上の必要性が求められるとされる[221]。なお、自衛隊の情報収集活動の根拠として防衛省設置法第４条が規定する調査・研究を挙げる場合がある。しかし、設置法は行政組織の任務・所掌を規定するものであり、具体的な権限を付与するものではない。このため、任意活動が設置上の責務の範囲であることの言い換えであり、直接の各種行動の根拠としている訳ではないことは注意が必要である[222]。

通信の秘密との関係

プライバシーの侵害と同様に、憲法 21 条 2 項後段で規定される「通信の秘密」を侵害する行為についても同様に強制手段に該当するとされている[223]。

上述の通り、任意調査活動において通信の秘密を侵す活動は出来ない。従って、サイバー空間において何が通信の秘密に該当するかを明らかにすることが必要となる。一般に通信とは特定者間の情報の交換であり[224]、特定者間の電気通信を傍受し、内容を取得することは通信の秘密を侵す行為となる。一方で、自身が通話者の一方に該当する場合は通信の秘密の保護は及ばない。従って、防衛省・自衛隊宛の電気通信を分析し、所要の情報を収集することに違法性はない。ただし、収集する内容が個人情報に該当する場合は、個人情報の保護に関する法律（以下、「個人情報保護法」という。）の規定に留意が必要である。なお、通信当事者の一方の同意がある場合の傍受については、意見が分かれるが、同意がある場合は違法性が阻却されるという意見が多い[225]。ただし、既に通信が終了し、通信当事者の所有となったデータ等の提供

学会編『防衛法研究』第 43 号（2019 年）、岡山公法判例研究会「情報保全隊による情報収集・保存が違法とされた事例」岡山大学法学会編『岡山大学法学会雑誌』第 63 巻第 1 号（2013 年 8 月）参照

[221] 田村正博・前掲 215 172 頁。

[222] 前掲注 211。

[223] 最決平成 11 年 12 月 16 日刑集 53 巻 9 号 1327 頁。川出敏裕『判例講座刑事訴訟法〔捜査・証拠編〕〔第 2 版〕』（立花書房、2021）228 頁。また、刑事訴訟法 222 条の 2 も電気通信の傍受を強制処分と定める。

[224] 曽我部真裕・林秀弥・栗田昌弘『情報法概説[第 2 版]』（弘文堂、2019 年）48 頁。

[225] 宍戸常寿「通信の秘密について」早稲田大学 21 世紀 COE《企業法制と法創造》総合研究所編『企業と法創造』第 9 巻第 3 号（2013 年）。その他、田川義博「インターネット利用における「通信の秘密」」『情報セキュリティ総合科学』第 5 号（2013 年）、情報セキュリィティ大学院『「インターネットと通信の秘密」研究会報告書：インターネット時代の「通信の秘密」再考』（キャノングローバルセキュリィティ研究所、

を受けることは問題ないと考えられる。

サイバー空間においてどのような情報が「通信の秘密」に該当するかは様々な議論があり一様には言えないが、通信の秘密の保障範囲は通信内容に留まらず、発信日時、発信・宛先 IP アドレス、パケットのヘッダー情報、ネットワークトラフィック等の外形事項まで含むとされる[226]。従って、自己の所有するネットワーク外において、ネットワークの所有者の同意なく、パケット、トラフィックデータ等を収集・分析することであっても通信の秘密を侵す行為と成り得る[227]。ホームページ等の「公然性を有する通信」に関しては意見が分かれるが、個々の通信の構成要素の伝送等に関しては該当すると考えられる[228]。通常、サイバー作戦においては平素の段階から対象国のネットワーク内部に侵入し、作戦に必要な対象国の脆弱性等に関する情報を収集する cyber exploitation[229]と呼ばれる活動（以下、「exploitation」と略。）が必要とされる[230]。exploitation では、IP アドレスの特定に留まらず、ネットワーク構成、個々の端末の OS・アプリケーションの種類・脆弱性、パスワード情報等を収集する。しかし、上記「通信の秘密」の一般的見解に従えば、当該 exploitation で収集する情報の大部分は「通信の秘密」侵害に該当すると考えられる。

また、電気通信事業者を通じて当該情報を入手する場合、電気通信事業法において通信の秘密を漏洩することを厳しく禁じられており、公益上の必要性との観点で対立が生じる。実務上は、電気通信事業者は通信の秘密に該当する内容の捜査機関に対する情報提供に関し、記録命令付差押許可状等の令状が必要としている[231]。ただし、個々の通信と無関係な契約者情報等は任意調査である捜査関係事項照会書等での提供が可能とされている。

なお、外国政府や軍事組織等の国家機関が行う通信に関しては、国と国の関係を律するのは国際法であり、憲法上の保護は及ばないと考えるのが自然であろう。しかし、日本国内に所在する外国人（あるいは団体・組織）に対

2013 年）<https://cigs.canon/article/20130625_1964.html>等。

226 芦部信喜・高橋和之補訂『憲法 第 8 版』（岩波書店、2023 年）243 頁。曽我部真裕「通信の秘密の憲法解釈論」『季刊 Nextcom』Vol.16（2016 年）。

227 曽我部真裕ほか・前掲注 224、51 頁。一方で、外形事項は通信の秘密に含まれないとする意見も存在する。高橋郁夫・吉田一雄「『通信の秘密』の数奇な運命（憲法）」『情報ネットワークローレビュー』5 号（2006）44 頁。

228 海野敦史「憲法上の通信の「秘密」の意義とその射程」『情報通信学会誌』第 32 巻 2 号（2014 年）。同『「通信の秘密不可侵」の法理』（勁草書房、2015 年）。

229 *See* JP 3-12, *supra* note 1.

230 *See* Aaron Brantly and Max Smeet, "Military Operations in Cyberspace" in Anders McD Sookermany, ed., *Handbook of Military Sciences* (Springer, August 2020).

231 丸橋透「プロバイダの捜査対応，ログ保存，被害抑止協力の実務と考え方」『比較法雑誌』第 49 巻第 4 号（2016）。

しても通信の秘密による保護が及ばないのか、という点については、これまで殆ど議論がされてこなかった論点とも言える。また、外国が関与する通信という観点からは、通信技術の発展に伴い、通話者の所在地・国籍及び通信経路・手段等の要素が組み合わされることによって、従来にはない様々なケースが考えられるようになってきている。一例として、サイバー空間の特性を考えれば、仮に国外領域における外国人同士であっても、通信経路の位置が日本国内を通過することは十分に考え得ることであり、そのような通話が外国人同士であるからといって通信の秘密に対する保護の対象外とは簡単には言えないであろう。特に、通信の秘密は基本的人権の重要な一部であることを考えれば、このため、単に非日本国籍保有者であるということをもって、通信の秘密による保護が及ばないと機械的に見做すことは難しく、それぞれの個別のケースに応じた判断が求められると考えることが必要であると考えられる。

また、外国領域に所在する非日本国籍保有者は、国際法上の国家管轄権の観点からみて日本国憲法の保障が及ばないと考えられる一方で、収集手段によっては当該領域国の国内法に違反する可能性があるほか、国際人権法への考慮も必要であることは注意を要する[232]。総括するならば、単に外国人（あるいは外国籍の団体・組織）であるという理由のみをもって即座に通信の秘密の保障外に置かれると考えることは出来ず、個別のケースに応じた慎重な判断が必要であるということである。

6.2.2 刑法の適用

加えて、exploitation は外国政府を含む第三者のネットワークに侵入して情報収集活動を行うことから、一般的に不正アクセス行為やスパイウェア等のマルウェア[233]の使用が想定されている。しかし、これらの行為の大部分は刑法に抵触するため、自衛隊の情報収集活動にあたっては刑法との関係を考察することも必要である。

サイバー犯罪に適用される刑法は複数存在する。特別刑法である不正アクセス行為の禁止等に関する法律は、不正アクセス行為、他人の識別符号を不正に取得・保管・要求する行為、不正アクセス行為を助長する行為を禁止する。また、刑法の不正電磁指令記録に関する罪では「不正指令電磁的記録作

[232] 国際人権法上も通信の秘密は保護されるとするのが多数説である。ただし、安全保障及び公の秩序維持のために一定の制限は認められるとされる。しかし、その程度等は不明確である。 *See* Michael N. Schmitt, *supra* note 6 at 187-208.

[233] 本稿では、ユーザーに迷惑をかける不正なソフトウェア全般を「マルウェア」とする。

成等罪」（168 条の 2）によりマルウェアの作成、提供、供用が禁止され、「不正指令電磁的記録取得等」（168 条の 3）によって取得・保管が禁止される[234]。上記罪の構成要件に該当する行為を行う場合は、行政機関の行為であっても何らかの違法性阻却事由に該当しなければ違法性を免れ得ない。違法性阻却事由には正当防衛、緊急避難及び正当行為（正当業務行為及び法令行為）が存在するが、法律の留保[235]の原則を考慮すれば、行政機関の行為は法令行為に該当することが基本となるべきであろう。

自衛隊の場合、サイバー攻撃への対策を行うにあたり、自衛隊内部で研究及び訓練用にマルウェアを作成し自らの組織内で研究・訓練で使用する行為は、同条で規定する目的要件、即ち「人の計算機における実行の用に供する目的」を欠くことから違法性はないと考えられる[236]。また、防衛出動が発令され、隊法 88 条「武力の行使」が適用される場合、サイバー作戦は作戦行動の一環として法令行為に該当し、その限度において違法性は阻却されると考えらえる[237]。

しかし、前述の通り、防衛出動以外において自衛隊に付与される権限は主に「武器使用」という形で規定をされている。「武器使用」とサイバー作戦の関係は次々項で詳細に検討するが、仮にサイバー作戦が「武器使用」に含まれない場合、自衛隊には、平素サイバー作戦の実行に際し、法令行為としての違法性阻却を得る明確な法的根拠が存在しないことになる。その場合、exploitation を行うことは、違法と見做される可能性が極めて高い。仮に外国に所在するサーバ等に対するサイバー作戦であっても、着手行為が国内である限り、属地主義の観点から刑法の適用は免れないと考えられる[238]。

6.2.3 グレーな手段による情報収集

明確には刑法に抵触しないが、行政機関が行うことが適切ではないと考えられるグレーな活動の合法性についても検討が必要である。具体的には以下のような行為が考えられる。

---

234 コンピュータ犯罪に適用される刑法についての 詳細は川村博・上富敏伸・島田健一『概説サイバー犯罪』（青林書院、2018）参照。

235 「法律の留保」の概念については、宇賀克也・前掲注 213。

236 鎮目征樹ほか『情報刑法Ⅰ‐サイバーセキュリィティ関連犯罪』（弘文堂、2022）171 頁。川村・前掲注 234、21‐22 頁。

237 第 154 回国会衆議院武力攻撃事態への対処に関する特別委員会議録第三号（平成 14 年 5 月 7 日）中谷元防衛庁長官答弁。ただし、隊法 88 条による違法性阻却が及び程度・範囲は不明確である。第 154 回国会衆議院武力攻撃事態への対処に関する特別委員会議録第五号中谷元防衛庁長官発言（平成 14 年 5 月 9 日）。

238 前田雅英『刑法総論講義』第 3 版（東京大学出版、1998）91 頁。

ソーシャルエンジニアリング

ソーシャルエンジニアリングは、「人間の行動的側面・心理的側面を巧みに利用し、情報の取得・改竄・破棄を受動的、能動的に実施させる手段」とされ、ショルダーハッキング、トラッシング、フィシングメール等により重要な情報を引き出す行為が含まれる。 いずれの行為においても、パスワード等を不正に取得することは不正アクセス禁止法に抵触する。また収集する情報に個人情報が含まれる場合は、個人情報の保護に関する法律（令和３年改正、以下「個人情報保護法」という。）第 64 条に規定される、「偽りその他不正の手段」に該当する可能性がある。 しかし、倫理的問題は別にすれば、行政機関が個人情報を含まない、単なるネットワーク構成、IP アドレス等の周辺情報をソーシャルエンジニアリングにより入手する行為自体は違法ではないと考えられる[239]。

ハニーポットの設置

自ら、あるいは同意を得た他者のネットワークにハニーポットを設置する行為に関しては受動的な情報収集に留まる限り問題がないと考えられる。仮に行政機関が偽りのサイトを立ち上げ、そこに攻撃者を誘引するような外見を有していたとしても、国民の権利を侵害する可能性は低く、さらにアクセス側に悪意がある可能性が高いことなどから、正当な責務の範囲であれば任意調査活動として許容される可能性は高いと考えられる。ただし、 ソーシャルエンジニアリングと同様に、本人の同意なく個人情報を所得する場合は、個人情報保護法 64 条に定める「偽りその他不正の手段」に抵触する可能性がある。また、当然ではあるが、パスワードを入力させ不正に取得することは不正アクセス禁止法に抵触する。このように、判断が難しい場合も考えられることから導入にあたっては慎重な判断が必要であろう。

ダークウェブを介した情報収集活動

ダークウェブによる情報収集は民間のセキュリティ企業等でも行われている活動であり、直ちに違法とは言えない。仮に、行政機関の職員が架空の身

[239] ただし、取得する情報の内容によりプライバシーへの侵害となる可能性も考慮することが必要である。実態としてソーシャルエンジニアリングにおいて個人情報保護及びプライバシー侵害に該当しない情報を収集することは意味が薄いと考えられること、特に行政機関が詐術を使用すること等の倫理的問題を考慮すれば活用は難しいであろう。

分を装いダークウェブで情報収集をしたとして、正当な責務の範囲であれば容認される可能性はある。しかし、仮に実在する他人の名義やパスワードを使用してダークウェブにアクセスした場合、あるいは何等かの犯罪に無自覚で加担してしまう可能性があることから、慎重なリスクの検討が必要と考えられる。

6.2.4 情報収集活動の根拠規定新設

情勢判断はもとより、「妨げる能力」の行使にあたっても正確な情報の入手は前提であり、サイバー空間における情報収集活動の権限を整備することは極めて優先順位の高い課題であると考える。これまで自衛隊は明確な法的権限がないなかで任意調査活動として情報収集活動を行ってきた。しかし、サイバー空間においては「通信の秘密」及び各種刑法上の規定の制約により、任意調査活動では期待されるような情報収集活動は困難であり、明確な法的根拠を整備することが求められる。方向性としては、サイバー空間以外の全ての領域での情報収集活動を根拠づける包括的な情報収集活動権限を創設する案と、サイバー空間のみに限定する案が考え得る。

前者はサイバー空間に限らず航空機や艦船等による自衛隊の情報収集活動全般の根拠規定となることから、武器使用権限等も考慮する必要がある。近年では、尖閣諸島周辺における中国艦船の領海侵入に対応するため、領域警備に関する議論がしばしば国会でも行われており、自衛隊に対する警戒監視活動の権限付与する案についても実際に法案が提出されている。2021 年に日本維新の会、国民民主党及び無所属クラブの議員が議員立法として提出した「自衛隊法及び海上保安庁法の一部を改正する法律案」（令和 3 年令和 3 年 12 月 16 日提出、現在閉会審査中）には、以下のような条文の案が記載されている[240]。

第八十四条の四の二 防衛大臣は、公共の秩序の維持を図るため、自衛隊の部隊に対し、必要な情報の収集その他の警戒監視の措置を講じさせることができる。

上記に記載された「必要な情報の収集」として、サイバー空間における情報収集活動を根拠づけることも一案として考え得る。情報収集活動はサイバー空間に限定されるものではないため、サイバー空間に限定しない包括的な情報収集権限を創設することは自衛隊の作戦能力向上に大きな効果が期待できる。ただし、離島周辺における権限行使とサイバー空間における権限行使

[240] 参議院、議会情報第 208 回国会（常会）<https://www.sangiin.go.jp/japanese/joho1/kousei/gian/208/meisai/m208090207009.htm)>.

では質的に大きな乖離があり、国民の権利侵害の様態・程度も異なることから、領域警備に関する議論にサイバー空間を含めることは、複雑な議論を生起させる可能性がある。

後者の場合は、今後予想される能動的サイバー防御の実現に向けた様々な法案整備の中で自衛隊法の一部改正として含めることにより、大きな議論を引き起こすことなく実現できる可能性が高い。ただし、前述の通り、政府全体としてどのような権限が必要であるか等は現時点で不明確であり、立法措置の具体的方向性が見えていない。仮に自衛隊に対しては現状とかわらず何等特別な任務・権限が付与されないとなった場合は実現困難である。また、仮に実現できた場合であっても、サイバー空間以外での自衛隊が行う情報収集活動については引き続き根拠法令が無い状態が継続するため、根本的な解決とはならない可能性が高い。

いずれの場合においても自衛隊に具体的な権限を付与するものであり、自衛隊法の改正が必要と考えられるが、憲法及び他の関係法令との整合を十分に図ることが必要である。特に、第三者のネットワークに侵入して行う通信の秘密、あるいは刑法等との関係を整理し、国民の権利を侵害しないように最大限の注意を払うことが必要である。

一案として、exploitation に関しては、特定の対象国をリスト化し、当該対象国の国家機関等との関連が明確に疑われるもののみに情報収集の対象を限定することが考えられる。この点で参考となるのは米軍のサイバーに関する権限を規定した米国の連邦法である。2019 年度国防権限法は、1642 条で「サイバー空間におけるロシア、中国、北朝鮮、イスラム国及びイランに対するサイバー空間におけるアクティブ防衛」に関する条文を置いている（1642 条)。同条では、ロシア、中国、北朝鮮、イスラム国及びイランが、積極的かつ組織的にサイバー攻撃を行っている、政府に対する積極的、組織的、継続的な攻撃キャンペーン（を実施している、または米国政府または国民に対する積極的、組織的、継続的な攻撃キャンペーン選挙及び民主的政治過程に影響を与えようとすることを含む）)を実施していると判断した場合、米軍に対して当該サイバー攻撃を中断、撃退、抑止する権限を付与している。日本においても同様の限定を明確化した上で、情報収集活動を行う法的権限を設けることは不可能ではないと考えられる。

6.3 米国連邦法における位置付け

ここで、上記に関連し、比較の観点から米国の状況について考察する。前述のように、サイバー作戦が「武器使用」に含まれない場合、自衛隊には、

平素サイバー作戦の実行に関しては法令行為としての違法性阻却事由を得られる明確な法的根拠が存在しない。これに対して米国の連邦法においては、連邦軍の一般的な権限に関する規定に加えて、サイバー及び情報に関する作戦の章が置かれており、国防長官の権限が以下のように明確に規定されている[241]。

国防長官は、「外国勢力[242]によって米国または米国人に対して行われた悪意のあるサイバー活動に対応することを含め、米国およびその同盟国を守るために、サイバー空間における秘密軍事活動または作戦を目的としたすべての軍隊を開発、準備、調整し、そのための準備を行い、適切に権限が与えられる場合には、実施しなければならない。」[243]

この場合、連邦議会は戦争権限法[244]に定める敵対行為が生じているときだけではなく、敵対行為が生じていないサイバー空間におけるものも含めて、軍事活動または作戦、環境整備、情報活動、兵力保護、抑止、または対テロを目的とする作戦を許容するものとされている[245)]。また秘密軍事活動または作戦[246)]についても、「サイバースペースにおける秘密の軍事活動または作戦は、1947年国家安全保障法第503条(e)(2)（50 U.S.C. 3093 (e)(2)）における従来の軍事活動としてみなされるものとする。」として許容されている[247]。

したがって、「敵対行為が発生していない領域」でのサイバーに関する権限が明確に規定されている点で、米国連邦法の規定は日本の現行の法制とは異なっている。今後、日本が能動的サイバー防御実現に向けた法整備を進める上で、米国連邦法の状況を参考にすることは極めて有意義と考える。ただし、「敵対行為が発生していない領域」にも連邦軍の出動権限が認められていることから、アメリカにおいても犯罪と戦争権限法に定めるような「戦争」との境界が明確でない点があることが指摘されている点には留意が必要である[248]。

6.4「武器使用」とサイバー行為

---

[241] 10 USC. Ch. 19.
[242] 1978年外国情報監視法（50 U.S.C. 1801）の第101条で定義されているもの。
[243] 1978年外国情報監視法（50 U.S.C. 1801）の第101条で定義されているもの。
[244] 50 USC. Ch. 33.
[245] 10 USC. Ch. 19, §394 (b).
[246] 大統領または長官によって許可されたサイバースペースで実施される軍事活動または軍事作戦、あるいは関連する準備行動で極秘に行うことが許容されるもの。10 USC. Ch. 19, §394 (f) (1).
[247] 10 USC. Ch. 19, §394 (b).
[248] Liam P. Bradley, “Was the Colonial Cyberattack the First Act of Cyberwar Against the U.S.? Finding the Threshold of War for Ransomware Attacks” (2022) 96(2) St. John's Law Review 487 at 499.

6.4.1 「武器使用」の行政法上の位置付け

次に、日本における「武器使用」とサイバー行為の関係について考察する。まず、「武器使用」の行政法上の位置付けであるが、隊法の「武器使用」は、行政法上の分類では即時強制の一種として考えられる。即時強制とは、緊急の場合等において、事前に対象者に義務を課すことなく行使可能な権限であり、対象者の同意無しに強制手段が採り得る。緊急の場合であることから、刑事訴訟法上の強制処分のような令状の発行は必要とされない[249]。一方で、司法による事前確認の枠組みを欠き行政による権利濫用を招き易いことから、使用に当たっては厳格な要件が規定されている。ここで問題となるのは果たしてサイバー作戦が「武器使用」に該当するのか、という点である。

6.4.2 サイバー作戦と武器の概念

国際法上の cyber weapons の定義

サイバー作戦と「武器使用」について論じた研究は国内では例が少なく、議論も殆ど行われていない。一方で、国外においては cyber weapons の定義に関する議論が活発に行われており参考となる。国際法上の議論は、主に国際人道法の観点から cyber weapons がジュネーブ諸条約第一追加議定書（Protocols Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (Protocol I) （以下、「AP Ⅰ」と略。））第 36 条に規定する兵器審査の対象となるかが焦点となっている[250]。米国を始めとしてサイバー攻撃能力を保有する多くの国がある種のサイバー作戦が上記兵器審査の対象となるとする[251]。しかし、cyber weapons はもとより、「武器」に関しての定義すら国際法上では未確立である[252]。この点に関し、サイバー空間への国際法適用に関し著名な研究である Tallinn Manual 2.0 では、武器及び cyber weapons を以下のように定義する。

武器とは、一般に、物への損害や破壊、人への傷害や死亡を引き起こすために使用さ

---

[249] 田村正博・前掲注 215 145 頁。
[250] AP Ⅰ 36 条は、締約国に対し、「新たな兵器又は戦闘の手段若しくは方法の研究、開発、取得又は採用」が条約上禁止されないかどうかを決定することを義務付ける。
[251] NATO Cooperative Cyber Defence Centre of Excellence, “Legal review of cyber weapons, means and methods of warfare”, online: CCDCOE : <https://cyberlaw.ccdcoe.org/wiki/Legal_review_of_cyber_weapons,_means_and_methods_of_warfare>.
[252] 化学兵器等の個別の兵器の定義は存在するが、武器そのものの定義がないことは注目に値する。

れるシステムとしての側面、と理解される[253]。

cyber weapons とは、人への傷害、死亡、物への損害、破壊を引き起こすために使用、設計、または使用されることを意図したサイバー戦の手段であり、すなわち、サイバー作戦を攻撃と認定するために必要な結果をもたらすものである[254)]。

上記定義に対し、Gary D. Brown は、武器の定義に設計目的の概念が欠けていることを指摘し、cyber weapons を含めて武器の定義を「殺傷、傷害、損傷または破壊を主目的として設計され、開発または入手された物体」と提唱する[255)]。この点に関しては、「武器」の定義に設計目的が必要であるとする Gary D. Brown の指摘は妥当であると考えられる。一例として、自衛隊で使用される携帯ショベルは近接戦闘において絶大な威力を発揮する装備であるが、「武器」に該当するとは考えられていない。同様に他の装備品等でも使用法によっては攻撃能力を発揮するものは多数あり、これらを「武器」に含めることはあまりにも広範になり定義の意味を為さなくなる可能性がある。

次に、議論がある点は、「武器」が及ぼす危害の閾値及び無体物の「武器」への該当性である。前者については、Tallinn Manual 2.0 は「人への傷害、死亡、物への損害、破壊」といった物理的損害が必要としており、Gary D. Brown の定義においても同様である。一方で、米空軍のように機能の「無力化」を含む見解も存在し[256]、明確な結論は得られない。他方、国際法上 espionage は違法とされていないこと[257]、国際人道法においてデータが目標としての価値を有するかは疑念が提起されている現状を鑑みれば[258]、単なる情報収集及びデータ操作を行うものは、「武器」に必要な危害の敷居を満たさないと考えることが現状では妥当であろう。

後者は、ソフトウェアやデータといった無体物を運用する行為であるサイバー作戦が「武器」の概念に含められるのか、という問題である。この点に関し、Tallinn Manual 2.0 は、有体物ではない「サイバー戦の手段」を cyber weapons に含める。Gary D. Brown も、自らの「武器」の定義にサイバー戦の手段を含めることに何等疑義を示していない[259]。各国がサイバー作戦を、cyber weapons の定義に関わらず兵器審査の対象となることを認めている点も考慮すれば、国際人道法上は、サイバー作戦が「武器」としての設計目的と

---

[253] *See* Michael N. Schmitt*, supra* note 6 at 452.
[254] *Ibid.*
[255] Gary D. Brown & Andrew O. Metcalf, "Easier Said Than Done: Legal Reviews of Cyber Weapons" (2014) 7 Journal of National Security Law & Policy 115 at 135.
[256] U.S. Air Force, Air Force Instruction 51-402 Legal Reviews of Weapons and cyber capabilities (2011).
[257] *See* Michael N. Schmitt*, supra* note 6 at 168.
[258] *Ibid.,* at 437.
[259] *See* Gary D. Brown, *supra* note 255 at 135-137.

危害の閾値を満たす場合、有体物あるいは無体物の区分に拘わらず、「武器」に該当すると整理することが一般的と考えられる。

国際法上の議論の国内法への展開

一方、国内法上は「「武器」という用語は、種々の法令又は行政運用の上において用いられており、その定義についてはそれぞれの法令等の趣旨によって解釈すべきもの」とされ、隊法における定義は以下のように示される[260]。

隊法上の「武器」とは「火器、火薬類、刀剣その他等直接人を殺傷し、又は武力闘争の手段として物を破壊することを目的とする機械、器具及び装置等」である。

本定義を見ると、設計目的及び危害の閾値が必要である点で国際法上の議論と一致する[261]。しかし、国内法上「機械、器具及び装置等」あるいは「道具」に、有体物ではないサイバー作戦が含まれるかどうかは、国際法上の議論とは区分し、慎重に判断する必要であろう。日本の国内法は、伝統的に有体物と無体物を区分しており、特に刑法は情報を財産権の客体である「財物」からは明確に除外する[262]。マルウェアについても、刑法は不正電磁指令電磁的記録[263]とし、飽くまで不正な命令を記述したプログラムとして扱い、他の有体物とは明確に区別する。

注意すべき点は、国際人道法における議論の焦点は、AP I 36 条の兵器審査の対象へのサイバー作戦の該当性に係るものであり、同条はそもそも「武器」に留まらず「戦闘の手段若しくは方法」を審査の対象に含めている点である。このため、各国はサイバー作戦への兵器該当性に関する検討を回避することが可能である。また、国際人道法は国家間武力紛争において適用されるものであり、平素から GZ 事態には適用されないという点、あるいは国家を対象とする国際法と個人の権利を対象とする国内法では求められる解釈の厳格性や精度に本質的に差異があり、直接個人の権利を侵害する恐れのある国内法の解釈はより厳格であることが求められる、といった点に関しても留意すべきである[264]。

---

[260] 第 77 回国会衆議院予算委員会義録第 18 号（昭和 51 年 2 月 27 日）三木武夫内閣総理大臣答弁
[261] なお、本定義が危害の閾値に機能の「無力化」を含めない点には留意が必要である。
[262] 東京地判昭和 59 年 6 月 28 日判例時報 1126 号 3 頁。
[263] 不正電磁指令電磁的記録の定義に関しては刑法 168 条の 2　1 項 1 号参照。
[264] 稲角・前掲注 146 10 頁。また、この点に関し、国際刑事法の形成にあたって国際人道法を個人の刑事責任追及に適用することへの批判から、国内法と同程度の人権保護機能を実現するための具体化が図られた歴史は、国際法と国内法の性格の差異を理解する上で参考になる。猪又和奈「刑事国際法における構成要件の考察（上）－旧ユーゴスラヴィア国際刑事裁判所及びルワンダ国際刑事裁判所判例の国際刑事裁判所規程形成への影響一」一橋大学編『一橋法学』第 2 巻第 1 号（2003）。

この点において隊法は特殊な性格を持つ。諸外国の軍隊は、基本的に「武器使用」を含む個々の作戦行動は国際法に準拠した部隊行動基準によって律され、隊法のように国内法で細かく規定する国は管見の限り存在しない[265]。つまり、諸外国は「武器」とサイバー作戦の関係について国内法上の定義に拘る必要性が薄い。しかし、隊法は本質的に行政法であり、特に、対外的な実力行使である「武力の行使」と異なり「武器使用」は国民への実力行使を念頭においた警察作用である[266]。このため、国際法を行動規範とする諸外国の軍隊と国内法上の警察作用の延長線上にある自衛隊を同列に考えることは難しく、隊法の「武器使用」は刑法等の他の国内法上の規定と齟齬がないように厳格に解釈することが妥当と考えられる。従って、サイバー作戦、あるいはマルウェアのような無体物を、国際法と同様に国内法上の「武器」に含める解釈には否定的にならざるを得ない。

仮にマルウェアを保管するホスト端末や記憶媒体が装置等にあたると解釈した場合であっても、実務上は様々な問題が予想される。まず、管理面での困難性がある。マルウェアは自己増殖・拡散する性格を有し、かつ、プログラムは継続的に修正を伴うものであることから、対象を特定することが困難である。あるいは DDoS 攻撃のようにマルウェアを使用しないサイバー作戦を規制の対象とすることも困難である。加えて、運用上の問題も考えられる。隊法は「武器使用」にあたって、極めて抑制的な要件を課しており、サイバー作戦を「武器使用」に含めることは逆にサイバー作戦を行う機会を奪いかねないという懸念を生ずる。一例として、平素における武器等防護の為の「武器使用」である隊法 95 条の使用要件には、警察比例の原則に基づくことのほか、防護対象の退避が可能な場合、あるいは防護対象が破壊された場合は使用が出来ない等の厳しい制約が存在すると解釈されており[267]、当該規定をサイバー空間において適用される状況を想定することは困難である[268]。95 条以外の「武器使用」にも同様の制約が存在し、サイバー空間への適用は難しいと考えられる。本来、対象を視認した上で使用される「武器」に対する規定を仮想空間で展開されるサイバー作戦と結びつけること自体に本質的に無理があると考えられる。

ただし、「武器使用」としてサイバー作戦を規定することは困難であると考えられるが、それが自衛隊による平素のサイバー作戦の実行は絶対に出来な

---

265 この点に関しては、各国の防衛法制を比較した以下の研究が参考になる。熊取谷行他「日本と諸外国の防衛法制の比較研究」『海幹校戦略研究』第 11 巻第 1 号（2021)

266 宮崎弘毅「防衛二法と自衛隊の任務行動権限-3-」『国防』（1978）94 頁。

267 田村重信・前掲注 131、275 頁。

268 一例として、隊法 95 条の武器使用要件をそのままサイバー攻撃に当てはめた場合、仮に防護対象がネットワークから隔離可能であれば、その時点で武器使用要件を満たさなくなる。

い、ということを意味するわけではない。行政法上の原則に立ち返り、比例原則の範囲内で緊急性、非代替性等が満たされる場合、あるいは、私人と同様に正当防衛・緊急避難に該当する場合は使用が認められる可能性は否定できない。ただし、直接の法令根拠がないことは、個々の判断が現場で求められることを意味する。法律の専門家ではない自衛官が比例原則に基づく法益の比較考慮といった複雑な法的判断を現場で即座に下すことは容易ではない。従って、「武器使用」ではない、新たな根拠条文を創設することが望ましいと考えられる。

6.5　重要インフラ防護と自衛隊の役割

6.5.1　重要インフラ防護施策の現状及び自衛隊の役割

重要インフラに対するサイバー攻撃は、国民の生活に極めて大きな影響を及ぼすだけでなく、本格的な武力攻撃が開始される前の準備行為として実施される可能性もあり、安全保障上の重大な脅威である[269]。

重要インフラ防護に関する各関係省庁の役割に関し、サイバーセキュリティ戦略は、主担当及び関係府省庁を定める[270]。また、第４次行動計画は重要インフラ所管省庁及び事案対処省庁を指定する[271]。しかし、ここでも、それぞれの関係や連携要領は明確化されていない。

警察に関しては令和４年の警察法改正において「重要サイバー事案」の概念が創設され、重要インフラ防護への警察の関与が明確化された[272]。一方で、防衛省・自衛隊の役割は依然として判然としない。サイバーセキュリティ戦略においては、重要インフラ防護の担当府省庁から防衛省・自衛隊は除外されている[273]。一方で、自衛隊・米軍による重要インフラ防護の共同演習の推進に関する記述が同戦略内に確認できる[274]。また、「日米防衛協力のための指針」では、サイバー領域に関する協力として、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サイバー事案への対象が謳

---

269 一例として、現在継続中のロシア・ウクライナ紛争が参考になる。ロシア・ウクライナ紛争では、2022年2月24日の地上部隊による国境を越えた侵攻が開始される前からサイバー攻撃が実施されていた。*See* Microsoft, “Special Report: Ukraine” Microsoft on the Issues (April 27, 2022), online: Microsoft <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd>.

270 サイバーセキュリティ戦略本部・前掲注3、26頁。

271 サイバーセキュリティ戦略本部・前掲注8、31・59頁。

272 前掲注121。

273 サイバーセキュリティ戦略本部・前掲注3別紙「担当府省庁一覧」。

274 サイバーセキュリティ戦略本部・前掲注3、31頁。

われている[275]等矛盾が存在する。この点に関し、重要インフラ防護に関する米軍との連携が強調されていること、また「妨げる能力」の使用は防衛出動発令以降と想定されていること等から、自衛隊に期待される役割が、平素における実効的な対処ではなく、飽くまで有事を念頭においた抑止にあるため、と考えられる。

実際、仮に武力攻撃事態認定以前に自衛隊にサイバー攻撃に対する重要インフラ防護の任務を付与しようとしても、現行法制上は困難である。隊法上、自衛隊が自衛隊施設以外の民間施設を警護出来るのは防衛出動を除けば隊法78条及び同81条に規定される治安出動のみである[276]。しかし、治安出動の発令要件は①間接侵略その他の緊急事態であり、②一般の警察力をもっては、治安を維持することができないと認められる場合と極めて制約的であり、サイバー攻撃のみによってそのような状態が生起することは想定しづらい。

6.5.2 重要インフラ防護における自衛隊のあるべき役割

しかし、仮に自衛隊が重要インフラの防護を命ぜられた場合であっても、法制度の観点のみでなく、実務上の観点からも自衛隊が行い得ることは限定される。防護対象が備えるシステム等に対する知識や習熟の程度を考えれば、現場の自衛官が防護対象システムを直接監視・操作するような状況はまず考えられない。

上記観点からも、本来自衛隊に求められる役割は、重要インフラを直接「防御」することではなく、「妨げる能力」による抑止の役割を担うことと考えられる。サイバーセキュリティ戦略が、抑止に関し「妨げる能力」も活用する、と記述することもこの見解を裏付けるものと考えられる[277]。

一方で、現状、自衛隊が十分な抑止力として機能するかという点は疑問である。サイバー空間における抑止は、従来の抑止概念と異なり、実際に使用することによる抑止効果が必要とされる[278]。しかし、自衛隊が防衛出動下令前に「妨げる能力」を運用することは現状では制度上も法令上も想定されていない[279]。このため、対象国が武力攻撃に満たないサイバー攻撃を継続する限り、一方的に攻撃を受ける可能性が高い。武力攻撃の準備行為としてサイバー攻撃が行われた場合であっても有効な反撃が出来ず、抑止としても機能

---

275 「日米防衛協力のための指針」（2015年4月27日）16､17頁。
276 隊法 90 条は、治安出動における施設警護のための武器使用を定めており、自衛隊が自衛隊施設以外の施設等を警護することが認められている。
277 サイバーセキュリティ戦略本部・前掲注3、32頁。
278 川口貴久・前掲注36。
279 前掲注206。

し得ない。

攻撃が圧倒的優位を有するサイバー紛争の特性を考えれば、重要インフラ防護を有効たらしめるためには、実際に対象国の活動を妨害・停止させる、あるいは更なる攻撃を思い留まらせる実力行使が必要と考える。つまり、重要インフラ防護において自衛隊に最も期待されるべき役割、すなわち「あるべき姿」は、平素から GZ 事態においても、「妨げる能力」を活用し対象国のサイバー攻撃を妨害・停止し、更なる事態拡大を抑止するという、「実際に行使可能な抑止力」というものになるべきであろう。従来の抑止の概念を一歩進め、外国からの国際法上・国内法上「武力攻撃」と評価されるには至らないサイバー攻撃に対し、実際に「妨げる能力」を行使し、対象国にサイバー攻撃を停止させる、あるいはエスカレーションを防止する役割が自衛隊の「あるべき姿」と考える。

一方で、従来の安全保障体制、特にサイバー空間以外での役割と大きな齟齬が生じることは避けるべきである。米国の前方防衛と同様に、自衛隊が常時 Red Cyberspace においてサイバー作戦を展開することは、これまでの安全保障体制・態勢との整合性確保が困難であると考えられる。また、重要インフラ防護等をはじめとしたサイバーセキュリティ全般の任務を平時から自衛隊に付与することも、現行の安全保障法制の枠組みを大きく変化させることになり望ましくないと考えられる。自衛隊が保有する強力な装備・能力が国内において行使される場合、国民の権利を侵害する危険性が極めて高く、自衛隊の出動は努めて抑制的に考えられなければならないことは原則事項である。サイバー空間においても、現在の安全保障体制・態勢における基本的枠組みは維持されるべきであり、自衛隊の関与は必要最小限に留めるべきであろう。

従って、違法なサイバー行為が発生した場合であっても、当該サイバー行為への国家の関与が想定されない犯罪に留まる場合は、警察が主な対応を行うべきである。自衛隊は、国外からの国家が関与する重大なサイバー攻撃に対し、反撃能力を行使することにより、エスカレーション及び今後のサイバー攻撃拡大を防止する抑止力に留まるべきである。具体的には、自衛隊は、NISC の後継となる新組織[280]の統制のもと、情報共有等を図りつつ、必要な時期・場所において「妨げる能力」を機能として提供する形が最も現実的であろうと考える[281]。

---

[280] 前掲注 207。

[281] 実態として、平時からの国内の重要インフラ防護の責任を自衛隊に任務として負わせることは大幅なサイバー作戦要員の増員及び予算付与が必要であり、現実的とは言えないとも考えられる。

6.5.3 サイバーセキュリティ基本法の改正

上記構想の具体化にあたっては、サイバーサイバーセキュリィティ基本法の改正が必要不可欠である。NISC 後継組織の名称や所管すら定まっていない現状では、具体的な条文まで想定することは困難であるが、サイバーセキュリティ基本法第 19 条を改正し、サイバー安全保障に関する各省庁の役割区分を明確化し、事態に即応できる態勢・体制の確立、特に、防衛省・自衛隊の任務を明確化することが必要である。方向性としては、国内で唯一公式に保有が認められた、自衛隊の「妨げる能力」を平素から活用することである。

サイバー特に、以下の内容が明記されることが必要であろう。

○　NISC 後継組織による一元的な総合調整の下、各関係機関が密接に連携して対応する。
○　NISC 後継組織が関係機関に対する統制権限を有する。
○　各関係機関は、情報共有を積極的に図る義務を有する。政府と民間事業者との情報共有の深化を図る旨についても記載
○　外国政府の関与の疑いがないサイバー攻撃への対応は一義的には警察が責任を負う。
○　外国政府が関与する武力攻撃に至らないサイバー攻撃に対しては、対抗措置として自衛隊が「妨げる能力」を行使し対処する。

任務・役割を明確化した上で、次に、当該任務を果たすために自衛隊に必要な権限を考察する。必要な権限とは、情報収集活動及びＧＺ事態における「妨げる能力」行使に係る権限である。

6.5.4 「サイバー対抗措置」行動の創設

このような重要インフラへの外国からのサイバー攻撃に対し反撃のためのサイバー作戦を行うことは、平時又は GZ 事態であったとしても、国際法上は対抗措置として容認される可能性がある[282]。しかし、国内法には対抗措置を行うための直接の根拠法令は存在しない。隊法には、間接侵略に対応するための治安出動が規定されており「武器使用」が認められる。対抗措置実行の国内法上の根拠を同規定に置くとする案も白紙的には考えられるが、前述の通り「武器使用」をサイバー空間に適用することや、治安出動の発令に対する高いハードルを踏まえれば、現実的には困難であろう。従って、国際法

[282] 国家責任条文第２章参照。

上の対抗措置を実効し得る国内法上の根拠規定を新たに設けることが望ましいと考えられる。

一案としては、隊法 84 条が定める「領空侵犯に対する措置」と同様に必要な措置を取る権限を規定しつつもその態様や方法を具体的に規定しない方法が考えられる。隊法 84 条は、以下のように規定する。

防衛大臣は、外国の航空機が国際法規又は航空法その他の規定に違反して我が国の領域の上空に侵入したときは、自衛隊の部隊に対し、これを着陸させ、又は我が国の領域から退去させるための必要な措置を講じさせることができる。

本条は、他の行動類型のように武器使用等に関する権限が具体的に規定されているわけではない。しかし、条文中にある「必要な措置」には、誘導、無線などによる警告、武器使用などが含まれると解釈される[283]。これは、対領空侵犯措置は警察作用ではあるものの国際の法規慣例を踏まえて行われるべきものであり、かつ警察比例の原則になじまないことから、権限規定を設けず「必要な措置」とするに留めたから、とされる[284]。サイバー領域においても、外国政府からのサイバー攻撃は本来国際法の領域であり、警察比例の原則に馴染まない等の共通点があり、同様の規定を有する「サイバー対抗措置行動」の創設を検討することを提言する。

実際の規定を考える上で、国家責任条文上の対抗措置の様々な要件をどのように表現するかという点が第一に問題になるであろう。また、発令権者を誰（内閣総理大臣又は防衛大臣）にするといった点についても検討が必要である。本稿では、以下の条文案を提言する。

（サイバー対抗措置）

八十四条の六　防衛大臣は、重要インフラ等に対し、外国政府が関与する国際法規に反する不正なサイバー攻撃が発生したときは、対抗措置として、自衛隊の部隊に対し、これを阻止し、あるいは停止させるため必要な措置を講じさせることができる。

国家責任条文における対抗措置の要件の規定については、条文中に「対抗措置」であることを明確に謳うとともに、最も重要な先行する国際違法行為の存在及び報復目的の禁止を不正なサイバー攻撃の「阻止」または「停止」に限定することで表現し、その他の細部要件は国家責任条文の要件に準じた内容を防衛省内で規則として定める要領を提案する。また、発令権者については、外国への実力行使という点を踏まえれば内閣総理大臣が適切とも考えられる。一方で、迅速な対処が必要というサイバー攻撃の特性は、対領空侵

283 田村重信・前掲注 131、240 頁。
284 田村重信・前掲注 131、239 頁。

犯対処や弾道ミサイル等に対する破壊措置行動と類似しており、上記行動と同様に防衛大臣を発令権者とすることも合理性が無いとは言えないことから、本稿では防衛大臣とする案を提言する。

6.6 小　結

本章ではこれまで、現行法制上、平素から GZ 事態において、自衛隊がサイバー空間において何をどこまで実行可能なのかを考察してきた。総括すれば、自衛隊は平素から GZ 事態においては、サイバー空間における特別な任務・行動権限を何等有せず、新安全保障戦略で示された能動的サイバー防御を自衛隊が担うことは、現行法上は困難と考えられる。このため、能動的サイバー防御を具現化するために、自衛隊がどのような役割を担い、その役割を果たすためにどのような権限を保有すべきかを明確にすることが第一歩と考える。特に、サイバーセキュリティ基本法改正による各府省庁の役割区分明確化と自衛隊への任務付与、自衛隊法改正による情報収集活動の根拠規定新設、「サイバー対抗措置」行動規定新設を提言し、本章の結論とする。また、本章内で若干触れた個人情報保護やプライバシー保護を巡る問題は、行政機関による情報収集活動において大きな論点となり得る問題点と認識する。本稿は自衛隊が行うサイバー作戦を焦点としているところ、個人情報保護やプライバシー保護はサイバー手段にとどまらず情報収集活動全般に関連する問題点であることから詳細には触れないが、今後検討すべき重要な課題と考える。

Ⅶ　有事対応における国際法上の課題

7.1　武力紛争下のサイバー作戦

現代の武力紛争は、陸海空のみならず、宇宙・サイバー・電磁波といった新たな領域を組み合わせたものとなっている。しかし、これまでの各国の紛争におけるサイバー空間の利用は、情報収集や影響力工作等が主体であり、実際の武力紛争における活用例は限定されていた[285]。しかし、2022 年 2 月 24 日から開始されたロシアによるウクライナ侵攻（以下「ロシア - ウクライナ紛争」という。）では、ロシア - ウクライナの両紛争当事国が活発なサイバー

[285] 武力紛争下で行われたサイバー作戦の例としては 2008 年の南ジョージア紛争、2014 年のクリミア侵攻等が存在するが、これらの少数例を除けば、サイバー作戦の大部分が武力紛争の文脈外で実施されている。

空間における作戦を展開している。その意味において当該紛争は、大規模なサイバー作戦の応酬を伴う初めての国家間武力紛争であるとも考えられる[286]。ロシア - ウクライナ紛争におけるサイバー作戦の詳細な実態は現在も継続中の紛争であることもあり、必ずしも明らかではない。しかし、限られた資料からも、従来の武力紛争と異なる特筆すべき点が確認でき、サイバー作戦への国際法適用に影響を及ぼす可能性がある。

また、同時並行して、日本国内においては、令和 4 年 12 月 16 日に安全保障三文書が閣議決定された[287]。上記文書には能動的サイバーディフェンスを始めとするサイバー空間における安全保障に関する記述が随所に盛り込まれており、武力攻撃事態等におけるサイバー作戦に関連する議論が高まることが期待される。

本章は、ロシア - ウクライナ紛争における両国のサイバー作戦を題材に、国際法及び国内法の双方の観点から分析し、武力紛争下で行われるサイバー作戦の法的課題について明らかにするとともに、日本が取るべき対応策に関し、具体的な提言を行うものである。

7.2 武力紛争間のサイバー作戦への国際法適用

7.2.1 武力紛争に適用される国際法とサイバー作戦

次に、武力紛争に適用される国際法をサイバー作戦との関係から概観する。武力紛争に適用される法は戦争法 Law of War と呼ばれ、国際法における①武力の行使の合法性に関する法、②国際及び非国際武力紛争における敵対行為の遂行、戦争犠牲者の保護及び交戦国の占領に関する法（交戦法規）、並びに③交戦国、中立国及び非交戦国の間の関係を規制する部分（中立法）をいう[288]。一般的に①を *jus ad bellum*、②③を *jus in bello* と呼称する。

jus ad bellum は、具体的には、ある国家の行為が、国連憲章第２条４項で規定される武力の行使禁止原則への違反という観点からの議論が中心となる。サイバー作戦の文脈においては具体的にどのようなサイバー空間における行為が武力の行使に該当するかという点、また被害国による自衛権の適用の正当性が問題となる。

---

[286] *See* James Andrew Lewis, *supra* note 36.

[287] 安全保障三文書とは「国家安全保障戦略」、「国家防衛戦略」及び「防衛力整備計画」の三つの政府文書を指す用語。いずれも令和 4 年 12 月 16 日閣議決定。

[288] *See* U.S. DoD, *supra* note 172 at 7-8. なお、戦争法は戦時国際法あるいは武力紛争法とも呼称され、その場合は *jus ad bellum* を含まない意味で使用される場合が多い。また、国際人道法は、武力紛争法に比して狭義であり、中立法を含まない用例で使用される場合が多い。

一方、*jus in bello* の内、交戦法規は、国際人道法とも呼ばれ、武力紛争における交戦国の戦闘行為を規律する法であり、*jus ad bellum* 上の違法性とは無関係に、すべての交戦国に平等に適用される。国際人道法の適用にあたっては武力紛争の発生が要件となるが、サイバー攻撃がどの時点で武力紛争となるのかという点については不明確である。また、国際人道法は、軍事的必要性、人道性、区別及び均衡性原則等の各種原則が存在し、軍事作戦の遂行にはこれらの原則を満たすことが求められる。しかし、サイバー作戦とのこれらの原則の関係についても確立した共通見解は存在しない。

中立法は、戦争が違法化される前の伝統的戦時国際法の下で発展した法体系であり、交戦国に対する公平な対応及び戦闘への不関与を基本とする交戦国と中立国の関係を律するものである[289]。戦争の違法化、特に国連憲章の成立以降、安全保障理事会が違法な武力の行使の発生を認定及び強制措置を決定したならば、国連加盟国は当該決定に拘束されるため、違反国との間に中立関係は成立しないことになる[290]。しかし、安全保障理事会においてそのような決定が為されない場合の関係については不明確であり、依然として中立法が適用され得る可能性は存在するとも考えられる。仮に中立法が適用されるとした場合、地理的国境の概念のないサイバー作戦はその性質上、第三国を巻き込む可能性が高く、中立法上の問題を生じる可能性がある[291]。

次に、上記の国際法適用の観点から、ロシア - ウクライナ紛争におけるサイバー作戦の状況を見ていく。

7.2.2 ロシア - クライナ紛争におけるサイバー作戦の特性と法的課題

ロシアは過去様々なサイバー作戦を遂行してきたと言われる。2007 年のエストニアに対するサイバー攻撃及び 2016 年米大統領選への干渉等はロシア政府の関与が強く疑われている。ロシアのサイバー作戦は、サイバー攻撃単独で行われるだけでなく、通常の軍事作戦の一部としても実行される。典型的な例として、2008 年の南オセチア紛争であり、陸海空戦力の軍事進攻と効果的に連動したサイバー作戦が実施され、ジョージア政府及び軍の国内外通信の遮断と混乱に成功、ロシアの短期間で戦略目標達成に貢献した[292]。同様の

---

289 杉原高嶺・前掲注 129、662 頁。

290 杉原高嶺・前掲注 129、664 頁。

291 一方、現状のロシア-ウクライナ紛争では、米国が公然と対露サイバー作戦の実行を宣言する等、各国が積極的なウクライナ支援を展開しており、実態として中立法の適用は考慮されていない状況である。このため、学術的には非常に興味深い題材ではあるが、本稿では中立法に関する議論は割愛する。

292 *See* David Hollis, “Cyberwar Case Study: Georgia 2008” Small War Journal (June 1, 2011), online: Small Wars Foundation <https://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008>.

作戦は 2014 年のクリミア侵攻でも使用され[293]、情報作戦と効果的に連動させることで戦闘を交えることなくクリミア半島の占領に成功した。ロシアは実戦を通じて通常の軍事作戦と連携したサイバー作戦の運用能力を着実に向上させてきたと言えるであろう。

2022 年２月から開始された今回の侵攻作戦においても、同様の戦術が使用されている。まず、通常戦力の侵攻の数か月前より偵察及びマルウェアのインストトールを目的とした exploitation 活動が行われ、更に、侵攻直前にマルウェアによるデータ消去等を狙った大規模なサイバー攻撃が政府機関、軍事施設及び重要インフラに加えられた[294]。また、同時並行的に、市民の混乱を企図した金融機関及び報道機関等への DDoS 攻撃等[295]も行われている。これらのサイバー攻撃は、通常戦力の侵攻と連接し、その侵攻を容易にしようとしたものと推測される。特に、侵攻と同時に行われた、Viasat Inc.の KA-SAT 衛星への標的型攻撃により数日間にわたりサービスを停止させたことはロシアのサイバー作戦の最大の成果であろう[296]。しかし、ロシア側のサイバー作戦は、2008 年の南オセチア紛争及び 2014 年のクリミア侵攻に比し、有効な効果を発揮できていないとされる[297]。様々な要因が考えられるが、第一にはロシア側の準備不足とウクライナの防衛力に対する過小評価が挙げられる[298]。次に、ウクライナ側の有効な防御及び効果的な反撃である。特に、ウクライナ側は 2014 のクリミア侵攻以降、継続的なサイバー攻撃を受けたことから、官民一体となった防衛体制の構築に努めた[299]。結果として、たとえロシア側によるサイバー攻撃を受けた場合でも、迅速に普及し影響を最小限にとどめる強靭な防衛体制を構築し得たことが大きい。また、IT 軍の創設を宣言する

---

[293] *See* Jen Weedon, “Information Operations in Ukraine” in Kenneth Geers, ed, *Cyber War in Perspective: Russian Aggression against Ukraine* (Tallinn: NATO CCD COE Publications, 2015), 67. <https://ccdcoe.org/library/publications/cyber-war-in-perspective-russian-aggression-against-ukraine/>.

[294] 米 Microsoft 社が 2022 年 4 月に公表したレポートでは、ロシアによる大規模サイバー攻撃に向けた準備活動は遅くとも 2021 年 3 月には開始されていたとする。
See Microsoft, *supra* note 269 at 5.また、同じく Microsoft 社が 6 月に公表したレポートにおいては、地上部隊が侵攻を開始する前日 2 月 24 日に、"Foxblade "と呼ばれるワイパーソフトによるサイバー攻撃が、ウクライナ全土の 19 の政府機関および重要なインフラ事業体に対し行われていたことを明らかにしている。
See Microsoft, “Defending Ukraine: Early Lessons from the Cyber War” *Microsoft on the Issues* (22 June 2022), online: Microsoft <https://blogs.microsoft.com/on-the-issues/> at 7.

[295] *See* James Andrew Lewis, *supra* note 36 at 2.

[296] *See Ibid.*, at 1; *See also* Rachel Jewett, “Viasat Details KA-SAT Cyberattack That Affected Thousands of Modems in Ukraine” Via Satellite (30 March 2022), online: Via Satellite <https://www.satellitetoday.com/cybersecurity/2022/03/30/viasat-details-ka-sat-cyberattack-that-affected-thousands-of-modems-in-ukraine/>.

[297] *See* James Lewis Andrew, *supra* note 36 at 2; *See also* Kristen Eichebsehr, “Ukraine, Cyberattacks, and the Lessons for International Law” (2022) 116 *American Journal of International Law Unbound* 145 at 146.

[298] *See* James Andrew Lewis, *supra* note 36 at 4.

[299] *See* Microsoft, *supra* note 269 at 2; See also Kristen Eichensehr, *supra* note 297 at 146-147.

等、国内外の民間人を活用したサイバー作戦による反撃も行っている[300]。このようなウクライナ側からの反撃は、直接の軍事的・政治効果は顕著ではないが、ロシア側にセキュリティへの人的資源充当を強要し、攻撃を鈍らせる効果を有する可能性も指摘されている[301]。そして、最大の要因として挙げられるのは、米国をはじめとする西側諸国及による支援である。米国は情報提供・技術支援にとどまらず、Cyber Command によるロシアに対する攻撃的なサイバー作戦の実行を公表する等、積極的な支援を展開している[302]。政府のみならず、民間 IT 企業による支援も行われており、マルウェアの解析、駆除からデータの海外移転等の幅広い分野で協力が行われている。特に米マイクロソフトの支援は極めて重要な役割を果たしていると考えられる[303]。セキュリィティ分野のみならず、アメリカのスペース X 社によるスターリンク衛星通信網も提供され、戦場通信網の維持に大きな効力を発揮している[304]。

ロシア及びウクライナ両国のサイバー空間における試みは、武力紛争における本格的なサイバー作戦運用を象徴するものであり、戦術面から見ても極めて興味深い。一方で、これらのサイバー作戦の特性は、国際法から見た場合、新たな問題を提起する可能性がある。まず、*jus ad bellum* の観点からは、ロシア側の地上侵攻開始前のサイバー攻撃の法的性格が問題になるであろう。ウクライナ側からすれば、どの時点から自衛権による対応が可能となるのか、特にサイバー攻撃に対し自衛権を発動できるのか、という問題が考え得る。また、*jus in bello* の観点からは、国際人道法の適用開始時期が問題となるであろう。更に、民要物へのサイバー攻撃の合法性や民間ＩＴ企業及び個人によるサイバー作戦への参加についても通常兵器とは様相の異なる問題を提起するであろう。特にこの問題は、第三国の領域からサイバー攻撃が行われた場合、さらに複雑化する。以下、それぞれの問題の細部について確認する。

武力侵攻開始直前の大規模サイバー攻撃

---

300 ウクライナ IT 軍の詳細について *See* Stefan Soeasanto, "*The IT Army of Ukraine: Structure, Tasking, and Ecosystem*" Center for Security Studies (CSS) (June 2022), online: ETH Zürich <https://css.ethz.ch/en/Themes/Cybersecurity/all-publications/details.html?id=/t/h/e/i/the_it_army_of_ ukraine>.

301 NHK, "WEB 特集「見えてきたサイバー戦:ハイブリッド戦、ウクライナで激しい攻防」" NEWSWEB (27 June 2022), online : NHK <https://www3.nhk.or.jp/news/html/20220627/k10013690111 00.html>.

302 *See* Callie Patteson, "US using hack attacks to support Ukraine against Russia, general says" *New York Post* (June 1, 2022), online: New York Post <https://nypost.com/2022/06/01/us-supporting-ukraine-against-russia-with-cyber-attacks/>.

303 米マイクロソフト社の支援内容に関しては *See* Microsoft, *supra* note 294.

304 *See* Ariel Zilber, "Elon Musk's Starlink satellites helping Ukraine drones destroy Russian tanks: report" *New York Post* (March 21, 2022), online: New York Post <https://nypost.com/2022/03/21/elon-musks-starlink-satellites-helping-ukraine-drones-destroy-russian-tanks-report/>.

本紛争において、ロシアは通常戦力による武力侵攻開始に先立って大規模なサイバー攻撃をウクライナに対し実施している。サイバー作戦を通常戦力による侵攻に先立つ準備攻撃として使用することは、戦術的には極めて合理的であると考えられるが、国際法の観点からは *jus ad bellum* 及び *jus in bello* の双方の観点から問題を有すると考えられる。

jus ad bellum の観点からは、ロシアによるサイバー攻撃の武力の行使禁止原則違反が問われることになる。前述の通り、ロシアは、約 1 年間から exploitation 活動を行い、地上部隊侵攻開始数週間前より政府機関報道機関及び銀行 Web サイト等に対する DDoS 攻撃、あるいは Wiper と呼ばれる強力なマルウェアをウクライナの金融、政府、エネルギー、情報技術、農業など民間事業者に送り込みデータ消去を試みた[305]。これらの攻撃が、武力攻撃に該当するかどうかが問題となる。仮に、武力攻撃に該当するならば、本来ウクライナは当該サイバー攻撃を受けた段階で自衛権を発動できたことになる[306]。

結論から言えば、2 月 24 日以前のロシアによるサイバー攻撃に関し、武力の行使の基準を満たし、国連憲章第２条４項違反を構成するような攻撃はなかったということになるであろう。この点に関し、Michael N. Schmitt は、サイバー攻撃の武力の行使該当性に関する基準は明確ではないと認めつつ、ロシア側のいずれのサイバー攻撃も非破壊的かつ非侵害的であったことを挙げ、武力攻撃への該当性を否定する[307]。一部の国は、物理的被害を与えないサイバー作戦であっても武力攻撃に該当する可能性があると主張する[308]。しかし、その場合であっても、少なくとも被害の程度は通常兵力による武力の行使に匹敵する「規模と効果」を満たすレベルが想定されている[309]。局所的な被害に留まった今回のロシアによる事前のサイバー攻撃は、そのようなレベルには至っていないと考えられる。従って、ウクライナ側から見た場合、2 月 24 日の通常兵力による侵攻が開始されるまでの間は、自衛権による反撃は法的に許容されず、「武力の行使」に至らない程度の反撃を行う対抗措置のみが可

---

[305] *See* Microsoft, *supra* note 269 at 7.

[306] 国際法上は、国際連合憲章第 51 条に基づき、武力の行使と武力攻撃を区分し、武力攻撃の基準を満たす場合のみ被害国は自衛権の発動が許されるとするのが一般的見解。*See supra* note 138, paras. 205.

[307] *See* Michael N. Schmitt "Russian Cyber Operations and Ukraine: The Legal Framework" *Articles of War* (16 January 2022), online: The Lieber Institute for Law & Warfare at West Point <https://lieber.westpoint.edu/russian-cyber-operations-ukraine-legal-framework/>.
なお、Michael N. Schmitt は、2014 年のロシアによる非サイバー手段による軍事進攻によってウクライナの自衛権は発動されており、ウクライナによる反撃の合法性は純粋に必要性と均衡性の観点から判断されるべきと主張する。

[308] *See* the French Ministry of Armed forces, "International Law Applied to Operations in Cyberspace" the French Ministry of Armed forces (September 9, 2019), online: <https://www.justsecurity.org/wp-content/uploads/2019/09/droit-internat-appliqu%C3%A9-aux-op%C3%A9rations-cyberespace-france.pdf> at 8-9. ※仏語

[309] 武力攻撃と武力の行使の違い、「規模と効果」基準等の詳細に関しては *See* Michael N. Schmitt, *supra* note 6 at 339-348.

能であった、ということになるであろう[310]。

次に、*jus in bello* の観点からは、国際人道法の適用開始時期が問題となる。先ほどの Michael N. Schmitt によれば、ロシアとウクライナ間にはすでに 2014 年から国家間武力紛争が継続していることになるため、その時点で国際人道法が適用されていることになるため何等問題は生じないとする。しかし、そのような既存の武力紛争が存在しない場合、通常兵器による侵攻に先立つサイバー攻撃に国際人道法が適用されるかどうか、という点は非常に興味深い問題である。本問題は、攻撃における各種国際人道法規則の適用及び捕虜資格の有無に大きな影響を及ぼす。仮に国際人道法が適用されないならば、各種の違法なサイバー攻撃は国家責任法上の問題であり、個人の戦争犯罪責任が問われることはない。また、サイバー攻撃に関与した者が紛争相手国に拘束された場合、正規の軍人であっても捕虜としての資格は生じない。

API 第３条によれば、国際紛争における国際人道法の適用開始時期は、国家間武力紛争の事実上の発生と同時である[311]。従って、国家間武力紛争の発生条件が問題となる。ジュネーブ諸条約共通 2 条によれば、国家間武力紛争とは、「二以上の締約国の間に生ずるすべての宣言された戦争又は、その他の武力紛争」と位置づけられ[312]、国家間の紛争という国際性及び武力紛争に該当する武力の使用が必要であるとされる[313]。特に武力の使用という要素では、武力という言葉の解釈を巡って議論が存在し[314]、この論点はサイバー空間では特に重要な要素となる。学説では、一定の烈度を超えた暴力が必要とする烈度説と[315]、赤十字国際委員会（以下「ICRC」）等が主張する、暴力行為の烈度に関わらず国家間武力紛争は存在し得るとする初撃説とに区分される[316]。それぞれの説の中においても様々な幅の解釈が存在し、共通見解は確立されていない。ことサイバー空間への適用に関しても、Marco Roscini 等は烈度説

---

310 仮に、サイバー攻撃を含む当時の全般状況が通常兵力による侵攻の着手行為として見なせるならば、武力攻撃が真に急迫している状況として実際の被害の発生を待たずに自衛権の発動が認められる可能性は否定できない（いわゆる先制自衛（preemptive self-defense）の問題）が、サイバー特有の問題ではないため本稿では除外する。その他、累積理論（Accumulation of Events Theory）等の問題も考え得るが、同様の理由により本稿では除外する。

311 API art. 3; *See also* Michael N. Schmitt, *supra* note 6 at 375. .

312 国際人道法の根幹を為す 1949 年に成立したジュネーブ条約は第 1-4 条約まで存在するが、それぞれ第１から第３条までは共通項目となっている。*See* Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field of 12 August 1949[GC I]), art. 2.

313 *See* Michael N. Schmitt, *supra* note 6 at 380.

314 学説の詳細については、黒崎将広ほか・前掲注 194、268-277 頁。

315 *See* Mary Ellen O'connell, “Introduction: Defining Armed Conflict in the Decade after 9/11”, in Mary Ellen O'Connell, ed., *What is War? : an investigation in the wake of 9/11* (Arnhem: Martinus Nijhoff, 2012) at 10.

316 *See* Jann S. Pictet et all. eds., *The Geneva Conventions of 12 August 1949: Commentary I: Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field of 12 August 1949*(Geneva: ICRC, 1952) at 32.

を唱える方[317]、Michael N. Schmitt は文民保護の重要性から ICRC の見解を有利とする等[318]、様々である。なお、Tallinn Manual 2.0 は両説の対立について言及しつつ、結論は明確にせずケースバイケースの対応が必要とする[319]。しかし、仮に初撃説に立った場合であっても、武力紛争であるためには国家による何等かの暴力行為が必要とされることは間違いなく、国家の関与があるサイバー攻撃であればどのようなものでも国家間武力紛争を引き起こすものではない。そのため、ICRC の見解によれば、烈度以外の基準として、サイバー作戦の結果の一定の重大性、採用された手段、敵対的作戦への軍または政府機関の関与、標的の性質（軍事目標かどうか)、作戦の持続時間などが含まれるとする[320]。2 月 24 日以前のロシア - ウクライナ紛争の状況において、ロシア側の複合的な軍事力を使用した恫喝下で行われた各種サイバー攻撃は、初撃説に立った場合は国際人道法適用のトリガーとなった可能性がある。いずれにせよ、国際法上は *jus ad bellum* と *jus in bello* は切り離されて考えられ、*jus ad bellum* 上の武力攻撃に至らず、自衛権が発動されていない状況下において、実質的な国家間武力紛争が生起していた場合は国際人道法が適用されることになる。このことは、後述する国内法上の問題の問題を引き起こす可能性がある。

7.3 民用物へのサイバー攻撃

7.3.1 攻撃の定義とサイバー作戦

ロシア - ウクライナ紛争においては、ロシアは、ウクライナ政府及び軍のるサイバーインフラにとどまらず、原発を含む重要インフラ、電気通信サービスプロバイダー、金融機関、報道機関、さらには個人のソーシャルネットワーク（以下「SNS」）アカウントに至るまでサイバー攻撃の対象としている。一方、ウクライナ側もロシアの重要交通インフラ及び報道機関等に対しサイバー攻撃を行っているとの報道がなされている[321]。国際人道法は、軍事目標以外への攻撃を禁止する[322]。しかし、上記サイバー攻撃の目標の中には、金融機関や個人の SNS アカウント等、従来の概念では軍事目標とは言い難い目

[317] *See* Marco Roscini, *supra* note 27 at 134-136.
[318] Michael N. Schmitt, "The Law of Cyber Warfare: Quo Vadis?" (2014) 25 Stanford Law & Policy Review 269 at 291.
[319] *See* Michael N. Schmitt, *supra* note 6 at 384.
[320] Cordula Droege, "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians" (2012) 94 International Review of the Red Cross 533 at 547-548.
[321] *See* NHK, *supra* note 301.
[322] AP Ⅰ art. 52.

標が存在する。これらのサイバー攻撃の違法性はどのように評価されるべきであろうか。

ここで疑問となるのが、果たしてサイバー攻撃が国際人道法上の攻撃に該当するのか、という点である。AP I第49条は、攻撃の定義として、「攻撃防御を問わず敵に対する「暴力行為」を攻撃とする」と規定する。サイバー攻撃が当該定義に該当しない場合、国際人道法上の「攻撃」に課せられた予防措置等の各種制約を免れることになり、軍事目標以外へのサイバー攻撃も許容される可能性が大きくなる[323]。

問題は、何が「暴力行為」に該当するか、という点である。一般的には「暴力行為」とは必ずしも物理的暴力の使用を必要とせず、引き起こされた結果の観点から、人の死傷や物の物理的破壊といった物理的暴力に伴う影響と同等であれば足りると認識されているようである（Effects-based approach）[324]。しかし、このアプローチは攻撃の概念を、暴力行為を超えて「拡張」するものではなく、人の殺傷や物の破壊等の物理的効果を伴うサイバー攻撃がAP I 49条1項の意味における「暴力行為」に該当するとしているにすぎない[325]。問題は、電力供給の遮断やデータ消去による機能停止及び無力化等の非物理的効果のみを生じるサイバー攻撃の暴力行為への該当性である。この点に関し、学説は分かれる。

ICRC及び一部の専門家は、機能の喪失の程度にかかわらず、対象となったサイバーインフラの可用性が失われたことをもって攻撃となると主張する[326]。「暴力行為」に無力化を含むべきとする論者の主な論拠は、AP I第52条2項における軍事目標の定義において、軍事的利益の中に当該目標の「無力化」を「破壊」及び「奪取」と並列で含んでいる点が挙げられる[327]。従って、電力網の遮断のような対象物を破壊することなく単に無力化することも、攻撃に該当することになる。

一方で、反対意見としては、攻撃を「暴力行為」と見なすためには、その行為自体ではなく、少なくともその結果が暴力的でなければならないことが必要とし、何らかの物理的損害、あるいはそれに匹敵する苦痛・損害が必要と解釈する[328]。これらの意見は、国際人道法における均衡原則を示したAPI

---

[323] ただし、「攻撃」に該当しない場合であっても、後述するように、敵対行為、あるいは軍事作戦に該当する場合は一般的な文民保護義務の遵守が求められることは留意が必要である。

[324] *See* Michael N. Schmitt, *supra* note 6 at 415.

[325] *See* Nils Melzer, *supra* note 24 at 26.

[326] *See* Michael N. Schmitt, *supra* note 6 at 418; *See also* ICRC, "International humanitarian law and the challenges of contemporary armed conflicts Challenges Report" *ICRC* (October 31, 2015), online: <https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts> at 41.

[327] *Ibid.*: *See also* Knut Dormann, *supra* note 23 at 4.

[328] *See* Michael N. Schmitt, "Wired Warfare: Computer Network Attack and Jus in Bello" (2002), 84 International

の各規定が、「文民の死亡、文民の障害、民用物の損傷」を例示する一方で、「無力化」を含まない点を挙げる[329]。また、これまでの伝統的な国際人道法の解釈では、サイバー攻撃と同様の性質を有するプロパガンダの流布等の非物理的手段による心理戦や経済戦、あるいはジャミング等の電磁波作戦は攻撃と見做されていなかった点についても根拠として挙げる[330]。

Tallinn Manual 2.0 では、大多数の意見として、単なる不便や不快を与えるだけのサイバー行為は、攻撃のレベルには達しないこと、また、暴力行為の基準として、あるシステムへのサイバー攻撃において、当該システムの機能修復に物理的な部品交換が必要とされるレベルであれば攻撃となり得るとする意見に大多数が賛同したとする[331]。さらに、現行法が非物理的な被害を禁止する程度にまで拡充されているとは言えないとする[332]。

本論点に関し、明確な回答は依然として存在せず、各国の見解も分断された状態である[333]。しかし、これまでの国家慣行、特にロシア - ウクライナ紛争におけるサイバー作戦の現状を鑑みれば、少なとも現行法制下において非物理的効果のみを伴うサイバー攻撃を AP 1 上の攻撃に含めるとする法的信念が確立しているとは言い難く、この点に関する国際法は形成途上にあると言える。

7.3.2 データと軍事目標

もう一つ、根本的な問題として、データが軍事目標、あるいは民用物等の保護対象（以下「対象物」という。）に成り得るのか、という問題がある。デ

Review of the Red Cross 365 at 377; *See also* Marco Roscini, *supra* note 27 at 179.

[329] 均衡原則は、攻撃によって生じた付随的損害が得られる軍事的利益と比較して過度にならないことを定める原則であり、AP Ⅰ 51 条 5 項(b)及び同 57 条 2 項に規定されている。*See* Nils Melzer, *supra* note 24 at 26; *See also* Michael Schmitt, ""Attack" as a Term of Art in International Law: The Cyber Operations Context" in *Christian Czosseck,* et all. eds., *Proceedings of the 4th International Conference on Cyber Conflict* (Tallinn: NATO CCD COE Publications 2012) 283 at 291.

[330] *See* Michael N. Schmitt, *supra* note 6 at 418; *See also* Michael N. Schmitt, "Cyber Operations and the Jus in Bello: Key Issues" (2011) 87 Naval War College International Law Studies 89 at 93.

[331] *Ibid.*

[332] *Ibid*., at 417-418.

[333] 本論点に関する国家の支持についても学説と同様に分断している。フランス、ドイツは ICRC のアプローチを支持する。フランスの見解について *See* the French Ministry of Armed forces, *supra* note 308 at 13. ドイツの見解について *See* the Federal Government of Germany, "On the Application of International Law in Cyberspace" (March 2021) at 8 <https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf>. 一方、米国及びイスラエルは AP Ⅰ 上の攻撃の概念を拡大することには否定的見解を示す。米国の見解について *See* U.S. DoD, *supra* note 172 at 1005; *See also* Brian J. Egan, "International Law and Stability in Cyberspace" (2017) 35 no.1 Berkeley J. Int'l Law 169 at 9-10; イスラエルの見解について *See* Roy Schondorf, "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations" (2021) 97 International law Studies 395 at 399-401.なお、日本の外務省は前者に近い立場に見える。外務省・前掲注 144、7 頁。

ータが対象物であるならば、対象となるデータ削除や改ざんといった行為は攻撃と認定される要件となり得る。一方で、データが対象物でない場合には、データ消去等により物理的破壊や人員の殺傷等の損失が生じない限り、データに対するいかなる操作も禁止されないことになる。

Nils Melzer は、データが軍事目的となり得るすべての定義要素を満たさない限り、合法的な攻撃対象とはならない、すなわち、保護対象であるとする。従って、別の軍事目標への攻撃に際し付随的損害として生じる民間データの削除や変更は、与えられた損害の性質を適切に考慮した上で、均衡性判断に加味されなければならないと主張する[334]。

一方で、Michael Schmitt は、この問題に関し、明確な合意は存在しないことを踏まえ、データを目標として扱うことに対しては慎重であるべきと主張する[335]。その理由として、電子メールを削除したり、テレビ放送を一時的に中断させたりするサイバー攻撃を違法な攻撃と見做すことは行き過ぎであり、現状においても民間のメディアを混乱させるために電子戦を用いる作戦が合法であることを考えれば、このような作戦と同様の効果を得るサイバー作戦を区別することは意味がないと主張する[336]。Tallinn Manual 2.0 の見解では、大多数の専門家は、少なくとも現行法において目標の概念がデータを含むと解釈されないという点で一致したとする[337]。この点に関しても、現行法制上、データを対象物とするという解釈が慣習法化しているとは言えない状況である。

しかし、データの重要性は増々高まっており、武力紛争下においてもデータを狙った攻撃が増加することは確実である。ロシア - ウクライナ紛争では、ロシアのミサイル攻撃の初期の標的は、ウクライナ政府のデータセンターであり、さらに、ロシア軍はデータを破壊するマルウェア「ワイパー」によるサイバー攻撃も行っている。ロシア側がデータの軍事的な価値をいかに重視しているかがわかる[338]。また、ウクライナ側も事前に政府の重要データを public cloud に避難させることで上記攻撃の被害を免れていることから、データの重要性を認識していたと考えられる[339]。しかし、このような対策は民間のデータと軍事データの混在を招き、増々識別を困難にする。データ破壊は市民生活に及ぼす影響は極めて深刻であり、かつ public cloud にまで戦火が波及した場合、影響を受ける対象は世界中に拡大する。今後、武力紛争におけ

[334] *See* Nils Melzer, *supra* note 24 at 31.
[335] *See* Michael N. Schmitt, *supra* note 330 at 96.
[336] *Ibid*.
[337] *See* Michael N. Schmitt, *supra* note 6 at 437.
[338] *See* Microsoft, *supra* note 294 at 5.
[339] *Ibid*.

るデータの扱いについては慎重に議論されなければならない課題であると認識する。

7.3.3　無差別攻撃及び均衡性判断

例えサイバー攻撃であっても、物理的な被害が生じる場合はAPⅠ上の攻撃に該当するということに異論はない[340]。この場合、攻撃の実行者は、国際人道法で定められた様々な義務の遵守が求められることになる。しかし、現実問題として明確な物理的被害を生じさせたサイバー攻撃が過去殆ど存在しないことから、これらの義務の具体的な適用は依然として不明確である[341]。特に、サイバー空間においては軍事目標かどうかの識別が困難であり、かつ影響が拡散し易いという特性を有することから、APⅠ上の攻撃に該当するサイバー攻撃を実施する場合は、無差別攻撃の禁止[342]及び均衡性判断[343]について慎重に考慮することが求められる。

無差別攻撃

サイバー攻撃を行う場合、現状の技術では、必ずしも目標とする特定のネットワークに対してのみ効果を得られるとは限らないのが実情であり、目標を視認して攻撃する通常兵器に比し、攻撃精度が落ちる可能性が高い。また、世界中の端末が接続されるインターネットの存在により、予期せぬ付随的損害を生じさせる可能性は十分にある。仮に目標とするデータとは異なるデータを消去又は破壊し、結果として軍事的利益とは無関係な重大な被害が生じた場合、これを特定の軍事目標を対象としない無差別攻撃として解される可能性が多分に存在する。

APⅠ第51条4項は無差別攻撃に該当する場合として以下の例を挙げる。

① 特定の軍事目標のみを攻撃の対象としない攻撃
② 特定の軍事目標のみを対象とすることのできない戦闘の方法及び手段を用いる攻撃
③ この議定書（AP１）で定める限度を超える影響を及ぼす戦闘の方法及び

---

340 *See* Michael N. Schmitt, *supra* note 6 at 416.
341 武力紛争間ではないが、現状として明確に物理的被害が出たケースは 2010 年にイランのナタンツに所在するウラン濃縮施設で約 1000 台の遠心分離機を損傷させた Stuxnet による攻撃のみとされる。*See* Samuli Haataja, *supra* note 7 at 146.
342 無差別攻撃とは、APⅠ51 条4項に規定される「軍事目標と文民又は民用物とを区別しないでこれらに打撃を与える性質を有する」攻撃をいう。
343 均衡性判断とは均衡性原則の適用に係る判断を言う。均衡性原則については後述.

手段を用いる攻撃

①の場合は、本来であれば特定の軍事目標を対象とできる場合において、あえて広範な地域を対象とするような攻撃である。サイバー作戦の文脈においては、特定のネットワークの一部のみを対象とする攻撃が出来る場合においてネットワーク全体を対象とするようなサイバー攻撃を行う場合が該当すると考えられる[344]。

②は使用しようとする兵器及び戦闘の方法及び手段が、特定の目標を対象と出来ない、本質的に無差別なものかどうかという問題である。サイバー作戦においては、特定のネットワークや器材を対象とすることが出来ないものでないかどうか、ということが問われる[345]。DDoS 攻撃等の特定のネットワークを対象とするものは当該カテゴリーには区分されない。また、近年のマルウェアは特定の動作環境でのみ動作するように作成されているものが多く、この点からも本質的に狙いがつけられない無差別兵器に該当するものは少ないと考えらえる。

一例として、ロシア - ウクライナ紛争では、ロシアは 2017 年のウクライナに対する NotPetya 攻撃と異なり、破壊的なマルウェア「ワイパー」による攻撃をウクライナ国内の特定のネットワークドメインに慎重に限定していたとされる。特定のネットワークを狙ったが、何らかの錯誤が発生し、予期に反し民間インフラ等にも被害が拡大したような場合は、均衡性判断における付随的損害の問題となる。

次に、③の場合は、特定の目標を対象とすることが出来るものの、その影響が当該目標以外にも伝搬し、制御不能になるような兵器である。サイバー作戦においては、マルウェア等が、NotPetya のように kill switch を備えず、手当たり次第に感染し、被害が拡大するような場合が考えられる[346]。ただし、ここでいう被害とは、後述する付随的損害に匹敵する程度のものであること

---

[344] *See* Michael N. Schmitt, *supra* note 6 at 467-469.

[345] *Ibid.,* at 456.

[346] *Ibid*., at 456-457.　2017 年に世界最大規模の感染被害を引き起こした WannaCry では、特定の環境で以外では活動を停止する kill-Switch domain が発見され、感染拡大を制御することが出来た。しかし、kill-Switch の用途は不明であり、意図的に感染が制御されていたとは言い難い。*See*　Lily Hay Newman "How an Accidental 'Kill Switch' Slowed Friday's Massive Ransomware Attack" Wired(13 May 2017), online: Wired <https://www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/>.
一方で、同じく 2017 年に世界最大額の被害を出した Notptya は、Wannacry と異なり、明確な kill-Switch は確認されていない。*See* Paul Haskelli-Dowland, "Three ways the 'NotPetya' cyberattack is more complex than WannaCry" The Conversation(30 June 2017), online: The Conversation <https://theconversation.com/three-ways-the-notpetya-cyberattack-is-more-complex-than-wannacry-80266>. 仮に Nottya のような形態でのサイバー攻撃が武力紛争間に実施され、多数の物理的被害が生じた場合は無差別兵器に該当するかもしれない。一方、Stuxnet は目標以外にも感染が拡大したが、特定の環境下のみで動作するよう設計されていたため、目標以外に対する大きな被害は生じなかった。このような場合は無差別攻撃には該当しないと考えらえる。*See* Michael N. Schmitt, *supra* note 6 at 457.

が必要であり、単に不便又は迷惑な程度の影響は損害とは見なされないと考えられていることには注意が必要である[347]。

均衡性判断

AP I で規定される均衡性原則とは、「予期される具体的かつ直接的な軍事的利益との比較において、巻き添えによる文民の死亡、文民の障害、民用物の損傷又はこれらの複合した事態を過度に引き起こすことが予測される攻撃」を禁止する原則である。ここで比較されるのは「予期される具体的かつ直接的な軍事的利益」と「巻き添えによる文民の死亡、文民の障害、民用物の損傷又はこれらの複合した事態」であり、後者が前者を「過度」に上回る攻撃が禁止されることになる。

後者を一般に付随的損害と呼ぶが、この付随的損害に重要インフラ等の機能停止等の非物理的損害が含まれるかどうかは意見が分かれる。Tallinn Manual 2.0 は、状況により機能喪失も付随的損害に含まれることに合意があったとする一方で、単なる不便や不快を生じる被害は損害に含まない、ともしており、その境界は曖昧である[348]。米国の見解によれば、本来付随的損害にはインターネット・ サービスの軽微で短時間の混乱及び民間事業者の経済的損害等は考慮する必要はないとする[349]。一方で、Marco Roscini 等の多数法学者は明確に重要インフラの機能喪失は付随的損害に含まれると主張する[350]。現状としてサイバー攻撃における付随的損害に関する明確な基準は存在しないが、将来的にネットワークインフラの重要性が増々増大することを鑑みれば、人の死傷や物の損壊等の物理的損害にとどまらず、それらに匹敵する程度の重大な非物理的損害は付随的損害に含むものとして考えることが妥当であろう。また、付随的損害には直般的に直接的な攻撃による被害に加え、攻撃を計画する時点で予想可能な間接的被害も含まれるとするのが法学者の間では多数説となっている[351]。総合すれば、サイバー攻撃においては、重要インフラの機能喪失等に伴う非物理的損害は、直接的であれ間接的であれ、攻撃開始時点で予測可能なものは付随的損害として考慮していくべきであろう。しかし、条文の解釈において注意しなければならないことは、均衡性原則という名がついているものの、実際は付随的損害が「過度」に軍事的利益を上回る攻撃のみが禁止されている、という点である。この「過度」という表現

[347] *Ibid*., Michael N. Schmitt, at 457.
[348] *Ibid*., Michael N. Schmitt, at 472.
[349] *See* U.S. DoD, *supra* note 172 at 1004.
[350] *See* Marco Roscini, *supra* note 27 at 222.
[351] *Ibid*, at 220; *See also* Michael N. Schmitt, *supra* note 6 at 472.

が如何なる程度かについては明確な基準は存在しない。

均衡性判断の基準に関する違法判断として、ユーゴスラビア連邦共和国に対する NATO 空爆作戦に関する旧ユーゴスラビア国際戦犯法廷（ICTY）検察官部検討委員会報告書は、ICTY に提出した報告書において「合理的な軍事指揮官（reasonable military commander)」基準を提唱した[352]。これは、異なる背景を有する軍事指揮官の意見が常に一致するわけではないことを認めつつ、合理的な判断力を有する軍事指揮官の目から見て明らかに過度と判断できるような場合に均衡性違反が認定されるとするものである。合理的な軍事指揮官とは具体的にどのような要素なのか、という点については、その後の判例も含めて明らかではないが、①適切な判断に必要な軍事的経験を有する、あるいは訓練を受けている者の判断であり、②純粋に軍事的観点からの判断であり、かつ③その判断が軍事の素人である裁判所を納得させられる合理性を有することが求められると考えられる[353]。

サイバー作戦における均衡性判断については国際裁判等の判例もなく、今後の国家慣行及び判例の出現を待たざるを得ない。しかし重要なことは、作戦実行を決断する軍事的指揮官は、自らが適切な判断を行うとともに、その意思決定に対する説明責任を果たせるように日頃から研鑽を積むことである。

文民・民用物の一般的保護

民用物へのサイバー攻撃に関し、前述のように攻撃の定義への該当性や均衡性判断が曖昧な中においては法的な位置づけを確立することは困難である。しロシア - ウクライナ紛争の現状を見れば、民用物に対するサイバー作戦が必要不可欠な軍事作戦であり、今後も継続される可能性が高いと考えられる。サイバーインフラやデータの価値が極めて高くなっている現代において、こういった目標に対する攻撃が文民に及ぼす影響は無視できない。仮にサイバー攻撃により長期にわたり電力供給が遮断されるような事態が発生したならば、死傷者が出ないまでも、多くの文民が経済的損失や安定した生活環境を失い、小規模な物理的被害を上回る損害が生じる可能性がある。従って、サイバー作戦に関連した文民及び民用物の実際的な保護について考えることは極めて重要である。

---

[352] International Criminal Tribunal for the former Yugoslavia (ICTY), Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia (8 Jun 2000), para. 28, <https://www.icty.org/en/press/final-report-prosecutor-committee-established-review-nato-bombing-campaign-against-federal>.

[353] 「合理的な軍事指揮官」に関する議論の詳細は *See* Ian Henderson and Kate Reece, “Proportionality under International Humanitarian Law: The “Reasonable Military Commander” Standard and Reverberating Effects” (2018) 51(3) Vanderbilt Journal of Transnational Law 835.

この点に関し、AP Ⅰ第51条1項は、原則として「文民たる住民及び個々の文民は、軍事作戦から生ずる危険からの一般的保護を受ける。」とし、直接の攻撃からだけでなく軍事作戦全般からの一般的保護を定める。従って、例えサイバー攻撃が AP Ⅰ第 49 条でいう攻撃に該当しない場合であっても、この原則的事項は遵守されなければならない。一般的保護の具体的な内容に関しては、現状議論が存在する。ICRC の見解では、例え攻撃に該当しない場合であっても、区別原則が適用され、民用物に対するサイバー攻撃は禁止されるとする[354]。Nils Melzer や Harrison Dinnis は更に区別原則にとどまらず、攻撃に該当しないサイバー攻撃であっても、敵対行為に関する規制全般が適用されると主張する[355]。一方で、Michael Schmitt 及び Marco Roscini は、AP Ⅰは攻撃とその他の軍事作戦を区別しており、均衡性原則や無差別攻撃の禁止は攻撃にのみ適用されると主張する[356]。結論は出ない問題であるが、AP Ⅰの規定を見る限り、攻撃を特別に他の軍事作戦と区別していることが明白であること、また、国家慣行や法的確信の観点からも、前者の意見を支持する実例はないことから、現状では後者の意見が妥当と考えられる。

しかし、武力紛争に直接関連のない、あるいは何ら軍事的利益が得られないサイバー作戦は、当該一般的保護に違反するとの解釈が成り立つ可能性はあることは注意が必要である。また、Michael Schmitt は、上記のような一般的保護を条約としてではなく、規範として整備していくことを提案する[357]。

7.4 民間事業者及び個人のサイバー作戦への関与

現代戦においては、サイバー空間に限らず様々な領域において民間アクターが関与している。特に、サイバー空間においては、民間事業者・技術者の関与無しにサイバー作戦を行うことは不可能と言っても良い状況ある。実際にロシア - ウクライナ紛争においては、双方が各種民間事業者及び技術者を使用している。ウクライナは、自国だけでなく、マイクロソフトを始めとする国外企業の協力を得てサイバーインフラの防衛を行っている。防衛にとどまらず、IT 軍の創設を宣言し、民間人の参加を募り、一部は実際にロシアに対するサイバー攻撃に参加していると考えられる。また、ロシア側も積極的にプロキシと呼ばれる非国家組織を活用した攻撃を展開している。特に、ロ

[354] *See* ICRC , *supra* note 326 at 42.
[355] *See* Nils Melzer, *supra* note 24 at 27.; *See* also Heather Harrison Dinniss, *supra* note 26 at 200-202.
[356] *See* Michael N. Schmitt, *supra* note 329 at 292-293; *See also* Marco Roscini, *supra* note 27 at 181.
[357] Michael Schmitt “Wired warfare 3.0: Protecting the civilian population during cyber operations”(2019) 101 International Review of the Red Cross 333 at 347-352.

シアのサイバー作戦に関しては、平素より高度標的型（Advanced Persistent Threat）攻撃と呼ばれるサイバー攻撃を行うハッキング集団の関与が根強く言われており、今回の紛争でも関与が疑われている[358]。しかし、民間事業者や犯罪集団等の非国家組織や個人によるサイバー作戦への関与は法的には複雑な問題を生起する。特に、これらの関与が第三国の領域から行われた場合、問題は極めて複雑化される。

7.4.1　サイバー作戦に参加する民間事業者従業員の法的地位と保護

第一に問題となるのは、これらのサイバー作戦に関与する文民の法的地位及び保護である。ジュネーブ第Ⅲ条約 4 条は捕虜資格を定めるほか[359]、AP Ⅰは第 43-47 条において戦闘員及び捕虜の法的地位を規定する。戦闘員資格は捕虜資格の裏返しとして認識されており、戦闘員資格を有する者は攻撃の対象とされる一方で、敵対行為に合法的に直接参加する権利を有する。従って、敵に拘束された場合においても捕虜となる権利を有し、国際法を順守する限り、国内法上の訴追を免れる。つまり、敵対行為に直接参加するためには戦闘員資格が必要ということである。サイバー作戦においていかなる行為が敵対行為への直接参加となるかは次項で論じるが、紛争当事国と契約し、サイバー作戦を行う民間事業者やハッキング集団等の非国家組織が敵対行為への直接参加と見なされる攻撃的なサイバー作戦に参加するためには、当該組織の要員には戦闘員資格があることが条件となる。その場合、法的には文民ではなく戦闘員として扱われることになる。

戦闘資格に大きく２つのカテゴリーが存在する。一つは軍隊の正規の構成員及びその軍隊の一部をなす民兵隊及び義勇隊の構成員である[360]。他方は、紛争当事国に属するその他（上記以外）の民兵隊及び義勇隊の構成員で、以下の条件を満たす者である[361]。

① 部下について責任を負う一人の者が指揮していること
② 遠方から認識することができる固着の特殊表章を有すること
③ 公然と武器を携行していること。
④ 戦争の法規及び慣例に従って行動していること

第１のカテゴリーは、民間事業者の従業員が身分を変えて、あるいは並行

---

[358] *See* Microsoft, *supra* note 269 at 5.
[359] *Geneva* Convention relative to the Treatment of Prisoners of War. Geneva, 12 August 1949[GCⅢ]art 4.
[360] GCⅢ art 4(1) , APⅠart 43(2).
[361] GCⅢ art4(2).

的に正規の軍隊の構成員に所属する場合であり、予備役の兵士と同様、通常の戦闘員として扱われる。

第２のカテゴリーは、軍隊には正規に所属しない場合であり、抵抗組織等の武装集団、あるいは民間軍事会社が戦闘行動に従事する場合が考えられる。サイバー作戦であれば、ロシアや中国のようにハッキング集団を前面に出して攻撃的なサイバー作戦を行うような場合が該当するであろう[362]。このカテゴリーで最初に問題となるのは紛争当事国に所属するとはどういうことかが問題となる。Tallinn Manual 2.0 は、紛争当事国と当該組織の間に事実上の指揮命令関係があれば所属すると言え、当該関係が黙示的なものであっても良いとする[363]。仮に、契約等により何らかの指揮命令関係が認められた場合、次の４つの要件を満たすかどうかが問題となる。一般的なプロキシとして使用される犯罪組織が、明確な組織性を有し、部下について責任を負う一人の者が指揮することや、戦争の法規及び慣例に従って行動していること等の条件を満たす可能性は極めて低いであろう。ある程度の規模・組織を有する企業が攻撃的なサイバー作戦の一部を請け負う場合、指揮官の存在や国際法の遵守といった条件を満たす可能性はあるかもしれないが、遠方から認識することができる固着の特殊表章を装着、公然と武器を携行することといった条件を、をサイバー作戦の文脈に当てはめることは容易ではない[364]。また、AP Ⅰ第 44 条は「攻撃または攻撃の準備のための軍事作戦に従事している間は、自己と文民たる住民とを区別する」義務を定めるが、この義務の適用も問題となるであろう[365]。従って、第２のカテゴリーをサイバー作戦に適用することはやや困難であり、仮に国際人道法を遵守しつつ、民間事業者等に攻撃的なサイバー作戦を実行させるならば、正規の軍隊の組織に所属させ、戦闘員として扱うことが必要と考えられる。その場合は戦闘員として合法的な攻撃目標となる一方、敵国に拘束された場合であっても、識別義務を果たす限り、捕虜としての待遇を得る権利を有することになる。

7.4.2 文民の敵対行為への直接参加

---

[362] 本ケースでは、特に民間軍事会社と傭兵との差異が問題となるかもしれない。しかし、AP Ⅰ第 47 条に定める傭兵の定義は外国籍であることや、一般兵士より高い報酬等、非常に狭く定められていることから大部分の民間軍事会社は該当しないとされる。黒崎将広ほか・前掲注 194、268・352 頁。

[363] *See* Michael N. Schmitt, *supra* note 6 at 404.

[364] *Ibid*., at 406. 仮にコンピュータやソフトウェアを武器と見做せるとしても、実態としてサイバー作戦に従事する非国家組織をこのカテゴリーに区分することは難しいとする。ただし、サイバー作戦と無関係に個人用の自衛火器を装備することは考えられるかもしれない。

[365] Nils Melzer はハッカーの制服の着装や背信行為との関係等、このカテゴリーのサイバー作戦への適用について多くの疑問が存在することを述べる。*See* Nils MELZER, *supra* note 24 at 29.

敵対行為への直接参加の概念

では、戦闘員資格を有しない文民による攻撃的なサイバー作戦への参加はどのように評価されるであろうか。AP1 第 52 条は、文民は「敵対行為に直接参加（Direct Participation in Hostilities、以下「DPH」という。）していない限り」保護を受けるとする[366]。従って、戦闘員資格を有しない文民が DPH を行なえば、当該文民は保護を失い、直接攻撃の対象となり得ることになる。ICRC の見解によれば、DPH を構成するには、以下の３つの基準があるとする[367]。

① 当該行為は、武力紛争当事者の軍事作戦もしくは軍事能力に不利な影響を及ぼすおそれがあるか、または直接の攻撃から保護される人や物に対して、死、傷害もしくは破壊を与えるおそれがあるものでなければならない（危害の敷居）。

② 当該行為と、当該行為または当該行為が不可分の一部をなす協同軍事作戦のいずれかから生じるおそれのある危害との間に、直接的な因果関係の結びつきがなければならない（直接因果関係）。

③当該行為は、一方の紛争当事者を支援しかつ他方の当事者を害する形で必要な危害の敷居を直接引き起こすことが明確に意図されたものでなければならない（交戦者とのつながり）。

第１の条件に含まれる「軍事能力に不利な影響を及ぼすおそれがある」場合に関しては注意を要する。この概念は AP Ⅰ第 49 条の「攻撃」よりも幅広いものであり、死傷や破壊等の物理的損害を与えるだけでなく、交戦国の軍事作戦や軍事能力に悪影響を与える可能性のあるあらゆる行為を含むとする。サイバー行為による通信の妨害等であっても、軍事作戦に不利な影響を及ぼす行為であった場合は危害の敷居を満たすことになる[368]。

しかし、交戦国の軍事作戦及び軍事能力不利な影響を及ぼすすべての活動が DPH と見なされるわけではない。第２の条件によれば、発生した、あるいは生じる恐れのある危害と行為の間に直接的な因果関係が必要とする。従って、味方の作戦に連動し、敵のコンピュータ制御のレーダーや兵器システム、物流供給や通信ネットワークを混乱あるいは無力化すること、あるいは情報収集であっても直接作戦に寄与し、敵に損害を生じさせる場合は DPH と見なされる可能性がある[369]。

議論が生じる可能性があるのがマルウェアの作成であろう。ICRC の見解で

---

[366] AP Ⅰ art 52(3).
[367] Nils Melzer, "Interpretive Guidance on the Notion of Direct Participation in Hostilities under IHL" *ICRC* (1 July 2009), online: ICRC <https://www.icrc.org/en/doc/resources/documents/publication/ p0990.htm> at 47–48.
[368] *See* Michael N. Schmitt, *supra* note 6 at 429.
[369] Michael N. Schmitt, *supra* note 330 at 101.

は、武器および軍事装備の設計、生産および輸送、ならびにインフラの整備といった一般的な戦争遂行努力への寄与は間接的であり、DPH とは見なされないとする[370]。当該見解によればマルウェアの作成であっても単に作成するだけでは DPH とは見なされないことになり、Tallinn Manual 2.0 においても、同様の見解が示されている[371]。

第３の条件では、文民による行為が、武力紛争の文脈において、いずれかの交戦国を支援し、かつ他方の当事者を害することが明確に意図されたものであることが必要とする。従って、武力紛争と無関係に行われるサイバー犯罪等は、例え重大な結果が生じ、それによっていずれかの交戦国に不利益が生じたとしても敵対行為への直接参加とは見なされないことになり、文民としての保護は失わない。ただし、それらの行為が許容されるわけではなく、国際人道法ではなく、管轄を有する国の国内法により取り締まられることになる[372]。

文民保護の回転扉

次に、問題となるのは、DPH を行う文民が保護を失う期間である。AP Ⅰ は、「敵対行為に直接参加している間は直接の攻撃からの保護を失う」とする。ICRC の見解は、通常の文民と、非国家間紛争における組織された武装集団の構成員を区分して考える[373]。後者の場合においては、継続的戦闘任務を有する限り、文民ではなく戦闘員と見なされることから常時攻撃の対象となるとする。一方で、前者の場合は、敵対行為に直接参加している期間、ICRC の解釈では個々の敵対行為の準備行為・展開・帰還に関わる間であるが、当該期間を除き、引き続き文民としての保護を享受することになる。つまり、敵対行為への直接参加に従事する期間に応じて当該文民が保護を喪失したり回復したりする、いわゆる文民保護の「回転扉」理論を提唱する[374]。しかし、この回転扉理論は多くの批判の的となっている[375]。つまり、常時攻撃対象となる正規軍兵士と、行為の間のみ攻撃対象となる敵対行為に直接参加する文民

---

[370] *See* Nils Melzer, *supra* note 367 at 50.
[371] *See* Michael N. Schmitt, *supra* note 6 at 430; *See* also Michael N. Schmitt, *supra* note 330 at 101.
[372] *Ibid.,* at 430.
[373] *See* Nils Melzer, *supra* note 367 at 69-73. 国家間武力紛争においても、独立した非国家組織が当事者として発生し、交戦国の何れか一方、あるいは双方と敵対関係に陥る場合がある。この場合、非国家間紛争と国家間紛争が混在することになり、法的関係は極めて複雑となる。特に、ICRC の見解に従えば、直面する状況により DPH の扱いが変化することになるが、やや非現実的と言える。
[374] *Ibid.,* at 70.
[375] *See* Michael N. Schmitt, *supra* note 330 at 102; *See* also Michael N. Schmitt, *supra* note 6 at 43; *See* also Emily Crawford, *Identifying the Enemy: Civilian Participation in Armed Conflict* (Oxford: Oxford University Press, 2015) at 84.

とでは著しく不均衡が生じているというのが主な理由であり、むしろこのような解釈は文民が積極的に敵対行為に参加することを促し、かえって文民の保護を怪しくする可能性もあると考えられる。批評家の見解では、これらの文民は、定期的に敵対行為を行っている間は、当該一連の活動期間の終始を通じて直接参加とみなされるべきで、個別の行為の間に攻撃から免れる期間はないはずであるとする[376]。特に、サイバー作戦においては、この問題は非常に重要である。なぜなら、主要な機材はコンピュータであることから、どの時点を敵対行為の開始時期及び終了時期とするかは判別が困難だからである。極論すれば直接的なサイバー攻撃を行っている期間とは、マウスをクリックした瞬間のみととらえることも理論的には可能であり、また論理爆弾のように行為が行われた瞬間と結果が出るまでの間に乖離がある場合は、その全期間を通じ保護を失うのか、という問題も存在する。Michael Schmitt は、「サイバー紛争環境では、「そのような時間の間」の唯一の妥当な解釈は、サイバー直接参加者がサイバー作戦を繰り返している間の全期間を含むということである。」とし、Tallinn Manual 2.0 においても同様の見解が述べられている[377]。

第三国領域からの敵対行為への直接参加

サイバー作戦の典型的な特性は、地理的領域を無意味にすることである。ロシア - ウクライナ紛争においても双方に対し紛争当事国以外の第三国領域から様々な敵対的なサイバー行為が行われているが、それらの行為の法的性格を明らかにしていくことが必要である。特に既存の国家間武力紛争が継続するなか、外見上文民による DPH が第三国領域から行われた場合、当該行為の発信地である領域国家との関係で問題は非常に複雑化する。白紙的には国家の関与の様態に応じて以下のケースが考えられる。

Ａ国とＢ国の間に国家間武力紛争が生起している状況において、第三国であるＣ国領域から以下の行為が行われた場合を想定する。

① Ｃ国政府の命令指示等によるＣ国文民によるＡ国へのサイバー攻撃
② Ｃ国文民が独自の判断で実施するＡ国へのサイバー攻撃
③ Ｂ国政府の命令指示等に基づく、Ｃ国文民によるＡ国へのサイバー攻撃

本論点に関しては、サイバー攻撃以外の通常の敵対行為手段においても共通する論点であるが、従来考えられなかったような遠隔地から敵対行為に参

[376] See Michael N. Schmitt, supra note 330 at 102; *See also* Michael N. Schmitt, *supra* note 6 at 432.
[377] *See* Michael N. Schmitt, *supra* note 6 at 432.

加できることに加え、個人でも敵対行為に容易に参加できるサイバー攻撃の特性は、これまでの敵対行為への直接参加の概念では対応を困難にする可能性があると思料する。以下、ケースごとに考察する。

① Ｃ国政府の命令指示等によるＣ国文民によるＡ国へのサイバー攻撃

本ケースは、Ｃ国政府がＢ国を支援する目的で、領域内の非国家組織や個人に命令・指示等を与え、Ａ国にサイバー攻撃を行うケースである。

当該行為は、外形上は既存の国家間武力紛争に関連した DPH に類似するが、実態はＣ国とＡ国との新たな紛争であり、既存のＡＢ間の国家間武力紛争とは切り離された形となる。*jus ad bellum* の観点から見れば、当該サイバー攻撃が武力攻撃の閾値に達しているかどうかが重要な問題である。武力攻撃の閾値に達していればＡ国は自衛の措置を取り得る。また、*jus ad bellum* とは別に新たな国家間武力紛争が生起しているかどうかという *jus in bello* 上の問題も生起する。仮に、国家間武力紛争が生起していれば、新たなＡＣ間の国家間武力紛争における DPH の問題となる。

②　Ｃ国文民が独自の判断で実施するＡ国へのサイバー攻撃

Ｃ国所在の非国家組織又は個人が独自の判断でＢ国を支援する目的でＡ国にサイバー攻撃を行う場合である。国際人道法の適用は、実態としての国家間武力紛争の存在が条件であり、地理的制限はないと考えられる。従って、理論上は、当該行為が前述の DPH の要件を満たす場合は、Ａ国はＣ国文民に対し国際人道法の規定による攻撃を行うことが可能である。しかし、当該国際人道法はＡＢ間の武力紛争を律するものであり、Ｃ国との関係を免責するものではない。従って、仮にＡ国がＣ国領域内の文民に武力の行使を行ったならば、Ｃ国との関係では国家責任法上の国際違法行為と見做される可能性はある。従って、実際上は、Ａ国は、Ｃ国にＣ国の国内法による対処を要請し、あるいは同意を得た上で直接対処することが求められるであろう。仮に、当該Ｃ国が無政府状態あるいはＣ国政府が同意を拒否する等の能力あるいは意思が欠如する場合は、受けたサイバー攻撃の状況により自衛権の発動あるいは対抗措置等による対処が可能と考えられる[378]。

③ Ｂ国政府の命令指示等に基づく、Ｃ国文民によるＡ国へのサイバー攻撃

基本的に②と同様であるが、B 国政府の関与があることから、既存の国家武力紛争との関連が明確であり、DPH に該当する可能性がより高まると考え

[378] 黒崎将広ほか・前掲注 194、231 頁。

らえる。本ケースは、ロシア - ウクライナ紛争において現実化しており、日本でもウクライナ IT 軍に参加する日本人の報道がなされている[379]。紛争当事国の第三国領域の使用が明確であれば、中立法上の問題も関係する可能性があり、複雑性が増すほか、被害国による対応がより強硬なものになる可能性もある。また、特に問題となることは、第三国の領域を活用することで、DPH の実施者は、自らが攻撃の対象となる可能性を著しく減少させつつ、安全に DPH を行えることになることである。特にサイバー攻撃は領域国政府に探知されることなく実施できる可能性が非常に高い手段であり、今後交戦国が積極的に第三国の領域を利用することの誘因となる可能性がある。このことは、既存の国家間武力紛争とは別に新たな紛争を引き起こす危険性を高め、より国際関係を不安定化させる可能性がある。

7.4.3 付随的損害と均衡性判断への影響

これまで、攻撃的なサイバー作戦に従事する文民への法的地位を確認してきた。しかし、ネットワーク・セキュリィティ等の防御的な作戦に従事する文民の法的地位はどのようなものになるであろうか。ネットワークの監視、保守等の活動は敵対行為への直接参加とは言い難く、文民としての保護を失う可能性は低いと考えられる。一方で、軍の施設や部隊の近傍で勤務する場合は、当該施設等を狙った攻撃に巻き込まれる危険性が常に存在する。
前述の通り、国際人道法においては、軍事目標に対する攻撃に伴って生ずる付随的損害は、得られる軍事的利益との比較において、それが過度でない限りは許容される。仮に、民間事業者の従業員が軍事施設内においてサイバーインフラの保守・点検を行う場合、当然当該施設が攻撃を受ければ付随的損害が生じる可能性は極めて高い。しかし、本来であれば防御側は軍事目標と民用物（文民含む）を離隔する攻撃の影響に対する予防措置を行う義務を負うのであり[380]、防御側が義務に違反した状態となる。これが均衡性の判断にどのような影響を及ぼすかは諸説存在する。

条文上、紛争当事者は相手側が軍事目標に文民を意図的に配置している人間の盾のような状況であっても、均衡性原則を含む予防措置を免除されないと規定される[381]。しかし、多くの法学者の意見及び各国のマニュアル等には、均衡性判断における付随的損害の計算を、防御側の違反の分だけ緩やかに判

[379] NHK, *supra* note 301.
[380] AP Ⅰ art 58.
[381] AP Ⅰ art 51(8).

断することが出来るとする[382]。また、米国や一部の学者は、軍事目標が攻撃を受けやすいことを知りながら軍事目標内に身を置く民間人労働者、GCⅢ第4条4項で規定する軍に随伴する者は付随的損害の対象とならないとする[383]。従って、軍事施設内で軍用サイバーインフラ等の維持管理に携わる文民は、直接攻撃の対象にはならないが、軍事施設への攻撃の巻き添えになる可能性が極めて高くなると考えられる。

本論点は決してサイバー作戦特有の問題ではなく、軍需工場等における勤務員や基地施設内で勤務する民間従業員も同様の問題に直面することになる。しかし、現代戦においてはサイバーインフラの軍事的価値が極めて高くなっており、特にデータセンター等は真っ先に物理的攻撃の対象となる可能性がある。仮に、public cloud を使用して軍事データを退避させていた場合、当該軍事データを管理するサーバが所在するデータセンターは軍事目標となる可能性がある。紛争地域から遠く離隔した場所において、管理企業の従業員がそのような被害にあう可能性が存在することを認識しているかどうかは疑問であろう。今後文民をサイバー作戦に関与させる場合は、上記のような付随的損害の危険性についても十分に周知するとともに、被害を極限する要領を検討しておくことが求められるであろう。

7.5 小　結

本章は、現在形で進行中のロシア - ウクライナ紛争における両国のサイバー作戦を題材に、武力紛争下でのサイバー作戦の国際法の観点から分析したものである。サイバー空間への国際法の適用は、議論が活発に行われているにもかかわらず、各国の態度は足並みが揃わない状況である。言い換えれば依然として形成途上であるということが言え、積極的にルール形成を主導していくことが求められるであろう。日本にとっては、今後整備していく自国のサイバー作戦能力の発揮を阻害しない形でのルール形成を目指し、我が国に有利な国際法環境の醸成の観点から、各種解釈に関する積極的な主張を行っていくことが必要である。

特に、日本にとって地理的距離に影響を受けないサイバー攻撃は、現状では唯一の敵国本土への反撃能力である。人道上の観点のみを追求し、不要な制約を自衛隊のサイバー作戦に課すことは避けなければならない。一例とし

---

[382] *See* U.K. Ministry of Defense, *The Manual of The Law of Armed Conflict* (Oxford: Oxford University Press, 2004) at 64.

[383] *See* U.S. DoD, *supra* note 172 at 243-244; *See also* Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (Cambridge: Cambridge University Press, 2004) at 129.

て、物理的被害を伴わないサイバー攻撃能力等への国際人道法適用にあたっての解釈は、より慎重に行うべきである。また、サイバー作戦に関与する文民の保護についても、民間事業者については積極的保護を図る一方で、個人による関与は努めて排除し、国内法による取締りを強化する等の適切なルール作りを主張すべきである。なお、文民保護に関しは、次章で述べる国際法と国内法のギャップについても大きな課題である。

ロシア - ウクライナ紛争においては、サイバー作戦が極めて大きな存在感を示す一方で、様々な法的課題が明らかになった。今後、その教訓を生かした規範作りが加速する可能性は否定できない。他国の国家慣行及び法的信念の確立状況を見極めつつ、外務省及び防衛省を始めとする関係省庁が密接に連携し国益に沿う国際法解釈についての共通認識を確立し、国際会議等において日本に有利な解釈を積極的に情報発信していくことが必要と思料する。

また、本稿では詳細には触れないが、近年問題提起されるようになった課題として、武力紛争間における個人情報保護及びプライバシー保護の問題がある。国際法、特に国際人道法は個人情報保護及びプライバシー保護に関しほとんど規定をしていない。一方で、占領地等において住民の生体情報を大規模に収集し活用することや、捕虜の動画等をネット上に公表することに関し個人情報保護やプライバシー保護の観点からの問題が指摘されている。この点についても今後検討が必要な問題と考える。

Ⅷ　有事対応における国内法上の課題

8.1　武力紛争に関連する国際法と国内法

通常、各国の軍隊は武力紛争のような国家の非常事態においては、緊急事態条項等により既存の国内法上の枠組みが停止あるいは制限され、主に国際法（主に武力紛争法）に基づき行動することになる。一方、憲法に緊急事態条項の無い日本の場合は、国際法上の武力紛争下においても、基本的には既存の国内法秩序が適用され続けることになる。日本の行政機関の活動の法的根拠は原則として国内法であり、これは平素・有事を問わない。従って、国際法上許容される行為が当然に国内法においても合法とされる訳ではないことに注意が必要である[384]。自衛隊も例外ではなく、自衛隊法（以下、「隊法」という。）に基づく法令行為として違法性が阻却される場合や、行政法上の適

[384] 自衛隊法策定に携わった宮崎弘毅は、自衛権発動に基づく自衛隊の行動権限は国際法に基づく行動が準則になるとする一方、国民に対しては国内法によるべきことが当初より想定されていたとする。宮崎弘毅「防衛二法と自衛隊の任務行動権限-1-」朝雲新聞社編『国防』（1978）96 頁。

用除外等が得られる特別な場合を除き、例え国際法上の武力紛争下にあっても、憲法、刑法及び各種行政法等の国内法の遵守が求められることになる。従って、国際法と国内法を照らし合わせ、国際法上の権利及び義務がしっかりと国内法上担保されることが必要である。

一方で、国内法の整備状況を振り返れば、新たな国家安全保障戦略において記載された能動的サイバー防御構想を含む、サイバー安全保障に係る内容及び議論の多くは武力攻撃事態に至らないGZ事態を意識したものであり[385]、ロシア - ウクライナ紛争のような本格的な国家間武力紛争における法整備については、十分に検討されているとは言い難い状況である。日本においては武力紛争の法制度は国際法と国内法の議論が別々に行われる傾向があり、国際法上の様々な権利や義務が国内法で具体化されていないものが多い。サイバー作戦に関する法制度は、新たな領域であることも相まって、特にその傾向が強い。

8.2 武力攻撃事態認定を巡る問題

国際法上は *jus ad bellum* とは無関係に、現実として武力紛争が存在すれば武力紛争法 *jus in bello* が適用されることになる。しかし、国内法ではその区分は明確ではなく、*jus ad bellum* の問題である自衛権の適用の有無が、*jus in bello* の問題となる自衛隊の作戦行動の権限の有無に直接影響を及ぼす。簡単に説明すれば、事態対処法に基づく政府の武力攻撃事態の認定がなされ、隊法第 76 条に基づく防衛出動命令が下令されることにより、始めて自衛隊は隊法第 88 条に基づく武力の行使が可能になる。隊法第 88 条は「武力の行使」を定めるが、ここでいう「武力の行使」とは自衛隊が防衛のために行う作戦行動全般を指すものであり、*jus ad bellum* としての自衛権に基づく「武力の行使」及び*jus in bello* で規定される各種の軍事作戦の双方を含む概念である[386]。武力攻撃事態の認定及び防衛出動命令の下令がない場合、実態として国家間武力紛争が存在している場合であっても、国内法上の制約により自衛隊は国

[385] 前掲注 17 参照。特に、能動的サイバー防御に関しては「武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある 場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入する」としており、焦点がグレーゾーンの事態にあると考えられる。

[386] 国内法における *jus ad bellum* と *jus in bello* の概念の混交は隊法 88 条の解釈においても顕著に表れている。隊法第 88 条 2 項は武力攻撃事態における武力の行使について「事態に応じて合理的に必要と判断される限度を超えてはならないものとする。」と定める。当該条文の意味は jus ad bellum 上の自衛権発動の要件である均衡性を表したものと説明される場合がある一方（第 186 回国会衆議院予算委員会議録 16 号小野寺五典防衛大臣答弁（平成 26 年 5 月 28 日））、自衛隊の個々の作戦行動における jus in bello 上の限度を示すものとも説明される（前掲注 237）等、*jus ad bellum* と *jus in bello* の明確な区別が行われていないことは明らかである。

際法上の軍隊としての地位に基づく軍事作戦を行なえず、飽くまで警察権限で対応することになる。

一方で、前述したとおり、国際法上は国家間武力紛争が存在する場合は、*jus ad bellum* 上の違法性判断とは別に、自動的に *jus in bello* である国際人道法が適用される。つまり、国際法と国内法に乖離が生じていることになる。特にサイバー作戦は、武力攻撃事態が明確に認定出来ないようなグレーゾーンの事態に適した行動であり、おける自衛隊対応に影響を及ぼすことは勿論であるが、文民保護や捕虜の取扱いといった武力紛争間における人道処置においても問題を生ずる可能性が高い[387]。

また、国家間武力紛争においては、国際人道法は戦闘の手段・方法を規制するだけでなく、捕虜の取扱いや文民を始めとする非戦闘員の保護を細部にわたり規定している。国際人道法の規定の多くは国内法でも担保はされているが、具体的な適用についての検討が不十分である。特に、国際人道法上の付随的損害と国内刑法の違法性阻却との関係、あるいは DPH の問題等課題は多い。ロシア - ウクライナ紛争の状況からも、サイバー作戦が、文民の関与や民用物へ攻撃等これまでにない大きな影響を文民に及ぼす可能性があることは明らかである。国際法の適用を検討するだけにとどまらず、適切に国内法に反映をしていくことが実効性を担保する上で極めて重要である。

8.3 武力侵攻前の大規模サイバー攻撃と日本の安全保障態勢・体制

５章、６章では、意図的に武力攻撃に至らない提度のサイバー攻撃を実行することによりエスカレーションを避けつつ、国益の追求を図ろうとするサイバー攻撃を主に念頭においていた。しかし、ロシア - ウクライナ紛争でみられた地上侵攻前のサイバー攻撃は、その後に続く通常兵器による地上侵攻との密接な連携が企図されており、当初からエスカレーションを予期したものであった。この点で、いわゆるハイブリッド戦とはやや趣が異なったものであったと考えられる。外形上武力攻撃と明確には認定しがたい手段をとることにより自衛権の発動を躊躇わせることは共通するが、その後の通常の軍事作戦に対する補助的な手段として利用されており、より純軍事的な性格が強いものであったと考えられる。大規模なサイバー攻撃が実際の武力攻撃の開始直前に行われ、引き続く通常戦力による本格的な進攻を容易にする戦術

[387] 日本の有事法制は、隊法だけではなく、武力攻撃事態及び存立危機事態における捕虜等の取扱いに関する法律（以下「捕虜取扱い法」という。)」、あるいは「国際人道法の重大な違反行為の処罰に関する法律」等、国際人道法を国内法上担保する立法を行っている。しかし、これらの法律が適用される枠組みもまた、隊法 88 条と同じ武力攻撃事態の認定以降となっている。

は、新たな慣用戦術となる可能性が高い。

一方で、これまで述べてきた通り、日本の安全保障態勢は事態認定に応じて段階的に拡張される。武力攻撃事態が認定され防衛出動が下令されるまでは、自衛隊による「妨げる能力」の行使は実施できないと考えられる[388]。平時のサイバー攻撃への対応は主に警察の役割であるが、警察の役割は飽くまでサイバー犯罪の取締りによる治安維持であり、外国からの軍事作戦として行われるサイバー攻撃に対応できるとは考えづらい。特に、Red Cyberspace に侵入して外国からのサイバー攻撃を未然に防止するような攻撃的なサイバー作戦を武力攻撃事態認定前に行うことは、現状では警察でも自衛隊でも想定していないと考えられる[389]。

サイバー攻撃は、兆候を発見することが難しく、攻撃を受けたことが判明した時点で既に広範囲に侵入を許しており、大規模な被害が短期間で生ずる可能性がある。従って、なんらかの緊急事態発生後、閣議を開き事態認定を行う現行の安全保障体制では対応が難しいと考えられる。仮に、武力侵攻前に電力等の重要インフラに対する大規模なサイバー攻撃が行われた甚大な被害を被った場合、今後の防衛出動下令以降の戦闘の初動において自衛隊は大きな不利を被る可能性が極めて高い。

能動的サイバー防御構想が、具体的にどのような場面を想定しているかは定かではないが、ロシア - ウクライナ紛争の教訓から、平時から GZ 事態のサイバー攻撃が即座に有事に移行する状況を想定して置くことが重要である。このため、Ⅴ章での述べた通り、平時から自衛隊にサイバー空間における任務・役割・権限を付与し、武力攻撃事態にエスカレーションした際の対応をシームレスに行えるようサイバー安全保障体制を整える必要があると考えられる。この際、警察との役割区分を明確にし、警察と自衛隊及び関係省庁が密接に連携できるよう着意することが必要である。

なお、「妨げる能力」の行使にあたっては、警察に同等の能力を保有させ対処させるという案も考えうる。警察は令和４年に警察庁に「サイバー警察局」を、その指揮下に重大事件の捜査を担う「サイバー特別捜査隊」を発足させ、専従の対処組織を保有しており、能力・装備上も可能性として考え得る。しかながら、上記で述べた通り、国家が関与する大規模なサイバー攻撃は軍事進攻の準備攻撃の可能性があり、武力攻撃事態認定以降の自衛隊の作戦行動との連接を考慮すれば望ましいとは言い難い。法制度の観点からみた場合、外国からのサイバー攻撃に対して警察権の行使を理由に実力を行使することは警察法の観点から説明が難しいと考えられる。また、上記の一部の組織を

[388] 前掲注 206。
[389] 第 208 回国会衆議院内閣委員会議録第 5 号緒方林太郎委員答弁（令和 4 年 3 月 2 日)。

除き、警察組織の主体は自治体警察であり、外国の軍隊等が行うサイバー作戦に対し組織的に対応させることも現実的ではないと考えられる。このため、国外に対する平時からＧＺ事態における「妨げる能力」の行使は飽くまで自衛隊の専従任務とし整備していくことが望ましいであろう。

8.4　捕虜等の取扱い

実際の紛争場面、特に国際人道法の適用についても問題が生じる可能性が高い。特に顕著な問題が捕虜の問題である。国内法における「捕虜」とは捕虜取扱い法で規定される、抑留資格認定又は採決を受けて抑留される者を指すが[390]、この捕虜取扱い法が適用されるのは武力攻撃事態の認定以降である。武力攻撃事態が認定される前は国内法違反者として扱われる。しかし、国際法上では既に武力紛争の存在と同時に武力紛争法が適用されるわけであるから、抑留者は当然に捕虜の権利を主張することになる。国際法に従うならば、捕虜資格が不明な場合であっても、それが明確になるまでは捕虜として取り扱うことが必要である[391]。サイバー攻撃においては、国外サーバが攻撃の開始点となる場合においても、最終的には国内サーバを経由する可能性が高く、当然当該国内サーバを直接操作する要員が事前に配置され、潜伏しつつ活動を行う可能性もあると考えられる。仮にサイバー作戦に参加する敵国兵士が、武力攻撃事態認定前に日本国内において活動し、サイバー攻撃に加担した容疑で警察に拘束された場合、当該被拘束者が武力紛争法に基づく捕虜の待遇を求めた場合の対応は複雑になることが予想される。

8.5　隊法第 88 条「武力の行使」の射程

8.5.1　隊法第 88 条による違法性阻却

軍隊の戦闘員は国際人道法において戦闘員資格を付与されている。しかし、国際人道法において戦闘員資格を有することだけをもって、国内法上も合法に戦闘に参加できることを意味するわけではない。本来、戦闘行為への参加は、国内法においては、刑法に規定される様々な罰条に触れる行為であることは言うまでもない。ただし、自衛隊員の場合は、隊法第 88 条の存在により、刑法第 35 条の正当行為（法令行為）として違法性が阻却されると考え得る[392]。

---

390 捕虜取扱い法第 3 条 7 項。
391 GCⅢ第 5 条。
392 詳細については、久保田隆「自衛官による加害行為と刑法 35 条に基づく違法性阻却：防衛出動等における武力の行使を中心に」法学政治学論究第 120 号（2019）。

しかしながら、違法性が阻却される程度は無制限ではない。隊法第 88 条は、以下のように記述される。

第 76 条

第一項の規定により出動を命ぜられた自衛隊は、わが国を防衛するため、必要な武力を行使することが出来る。

２　前項の武力の行使に際しては、国際の法規及び慣例によるべき場合にあってはこれを遵守し、かつ、事態に応じて合理的に必要と判断される限度を超えてはならないものとする。

第 88 条第 2 項は、前段において国際法遵守の旨を謳うとともに、後段において武力の行使の要件を規定する構造となっている。後段部分の「事態に応じて合理的に必要と判断される限度」とはいかなる限度を指すのかが重要であるが、前段の「国際の法規及び慣例」の限度がそのまま後段の限度にあてはまるとは条文構造上考えづらい。このため、国内法の観点からその限度を読み解いていくことが求められるであろう。しかし、現行法制下において武力紛争を経験していない日本においては、当然ではあるが、この点に関する判例等は存在しない。また、先行研究等も極端に少ないことから、実用的な尺度を見出すことは極めて困難である。この点に関しては、過去の国会答弁等においても、度々議論がなされている[393]。

この問題は、サイバー作戦に限らず、自衛隊のすべての作戦行動に付随する問題であるが、サイバー作戦においては特に複雑な問題となると考えられる。第一に、地理的な適用範囲が問題となるであろう。過去の国家答弁では、隊法第 88 条の適用は、基本的に戦闘が行われている地域に限られ、それ以外の地域において行政法規等の法令を遵守するとする発言[394]が為されている。しかし、地理的空間に縛られないサイバー空間で行われるサイバー作戦に従来の戦闘地域の概念が適用できるのか、という点は疑義が生じるであろう。

仮に、離島部に敵が侵攻し、武力攻撃事態が認定されたというような場合は極めて判断が難しくなるであろう。この場合、戦闘地域は極限され、国内の大部分が平素の行政活動及び経済活動を維持している場合が想定される。上記状況において、隊法 88 条の適用が当該離島部に留まると判断するならば、自衛隊のサイバー作戦は極めて限定されることになる。一方で、サイバー空間への隊法第 88 条の適用には地理的制限が及ばないとし、あらゆるネットワ

393 前掲注 237。

394 前掲注 237。中谷元防衛庁長官（当時）は、「正当行為でもいろいろなケースがあって決め切れませんし、世界じゅうどんな国でも、先生のおっしゃるような、88 条がどこでも使えるという国家は恐らくなく、やはり、これは適切に戦闘行為が行われる地域のみの規定でありますし、それ以外の地域におきましては、国民の人権や、また法規を尊重して、できるだけ国民に要らぬ迷惑をかけないように速やかに敵に対峙するというのがこの自衛隊法でございます。」と答弁している。

ークでの活動に隊法第 88 条が適用されるとした場合であっても、当然無制限に活動できるわけではなく、飽くまで「事態に応じて合理的に必要と判断される限度」であることが求められる。戦闘地域が極限され、多くの国民が通常の社会活動を継続する中において、自衛隊が国内のあらゆる民間ネットワークに自由に侵入し、情報収集あるいはマルウェアをインソールするといった作戦が、安全保障上の理由というだけ許容されるかは疑問である。

8.5.2 「通信の秘密」及び刑法との関係

「事態に応じて合理的に必要と判断される限度」を考えるにあたっては、明確な基準や判例があるわけではないため、行政法の基本に立ち返り、基本的人権に対して許される制約の限界と公益上の必要性を比較する比例原則[395]から考えるしかないであろう。つまり、個別具体的な状況に応じ、自衛隊のサイバー作戦により得られる公益と、それにより侵害する基本的人権を比較考慮して、その限度を判断していくしかない。そのためには、サイバー作戦により得られる公益とは何か、また自衛隊のサイバー作戦がどのような規定に抵触し、それぞれの規定が本来保護する保護法益とは何か、を慎重に検討することが求められる。

まず、サイバー作戦により得られる公益について考える。インターネットを介して行われるサイバー作戦は、例え海外から行われたものであっても、国内サーバを経由する場合、あるいは日本国内のボットネットを活用する場合が考え得る。また、これらの活動を行うために、敵対国が日本国内で偽装レンタルサーバ店を経営する等により隠密に通信拠点を整備する可能性も考え得るであろう[396]。軍事的な観点からは、国内のネットワークを監視し、不審な挙動を行う IP アドレスの追跡、サーバの位置の特定、被害識別を行い、当該サーバに対するサイバー攻撃、場合によっては物理的な攻撃を行う必要性が生じる可能性は否定できない。得られる公益は、妨害を排除することにより得られる作戦効果となる。加えて、警察権限では対処できない緊急性、

---

[395] 田村正博・前掲注 215、49 頁。

[396] 武力攻撃事態における国内ドメインを用いたサイバー攻撃は、国外ドメインからのサイバー攻撃に比し、より慎重な対応が求められる可能性がある。平素であれば、警察の捜査権が及ばない国外ドメインからのサイバー攻撃の方が、圧倒的に対応が難しいと考えられる。一方で、国家間武力紛争下（国内法上の武力攻撃事態）では、国外ドメインであれば、交戦国の関与の推定が比較的容易であり、反撃を行う場合であっても一定の付随的損害が許容される国際人道法の問題となる可能性が高い（ただし、前述の通り第三国領域を使用された場合、問題はより複雑化する。）。しかし、国内での対応は、敵国の関与が明確でなく、かつ行政機関が平常通り機能している場合、刑事訴訟法に基づく犯罪捜査手続きが求められる可能性がある。自衛隊法上は、隊法第 88 条が及ばない地域であっても、隊法第 92 条「公共の秩序維持」が適用される。しかし、この権限には犯罪捜査権は含まれていないことには注意が必要である。

非代替性の説明も求められるであろう。

一方で、権利の侵害は広範なものとなるであろう。特に大きな問題となるのは、自衛隊側の物理的な攻撃によって人の死傷や物の破壊等の付随的損害が発生するケースであるが、非物理的な損害であっても誤って無関係なネットワークにデータ消去型マルウェアを拡散し、医療データ等の人命にかかわる重要データの消去や、取引データ消失による莫大な経済的損害が発生するケースも考え得る。現行法制上は、サイバー作戦に必要なネットワークへの侵入、マルウェアのインストール等のほぼすべての行為が憲法及び電気通信事業法が規定する通信の秘密及び刑法上の不正指令電磁的記録に関する罪、不正アクセス禁止法等に触れる行為であるが、これらの保護法益を考慮しなければならない。

加えて、攻撃目標や彼我識別の困難性も問題となるであろう。そもそも高い匿名性を有するサイバー空間においては、サーバ及び端末の正確な位置の特定及び彼我識別が非常に困難という特性があり、上記のような誤射や付随的損害を防止するためには、サイバー空間における情報収集を徹底することが求められる。しかし、それは同時に幅広く個人のプライバーの侵害、「通信の秘密」を侵害することにつながるおそれがある。サイバー空間における「通信の秘密」の保護対象には様々な議論が存在するが、一般的解釈では、通信内容等の中身に留まらず、IP アドレス、ネットワークトラフィック等の通信の外形事項まで保護が及ぶとされる。つまり、第三者間の通信内容を監視することすら「通信の秘密」の侵害と判断させる可能性がある。個人のプライバシー侵害まで含めれば、もはや侵害する権利の全体像をつかむことは不可能に近い。

個別のケースバイケースで合法性を判断するということは、上記の比例原則に基づく判断を現場の自衛隊の指揮官に委ねることを意味する。国際人道法における均衡性判断も同様の側面を有するが、判例及び学説が多数存在する国際法と比較し[397]、国内法上の判断は上述のように極めて複雑困難である。法律の専門家ではない自衛隊の指揮官にこれを求めることは過度な負担となるであろう。従って、どのような場合に、サイバー空間において隊法 88 条による違法性阻却が可能となるかについては、事前に検討し、ある程度の基準なりモデルなりを明らかにしておくことが必要であろう。また、サイバー作戦に特有の問題ではないが、これらの国内法に違反した場合の刑事責任の追

[397] 国内世論の動向を踏まえれば、国際人道法における均衡性判断の基準「合理的な軍事指揮官」基準がそのまま国内法に適用されるとは考えづらい。

及[398]、あるいは賠償・補償についても未整備な課題である[399]。

8.6 サイバー作戦に従事する民間事業者の保護

8.6.1 国内法における分類

日本の有事法制において、大きな課題になると考えられるのが、武力攻撃事態における自衛隊の作戦に関係する民間人の法的位置位置付けとその保護であると考えられる。特に、サイバー作戦においては、民間技術者の関与は不可欠であり、その保護は極めて重要な問題である。前述のように、武力紛争法上、文民の保護は細かい規定が整備されている。しかし、国内法上の扱いは明確ではない。国内法上、民間人が自衛隊の作戦に関与するケースは、①予備自衛官が招集され自衛官になる場合②防衛事務官及び技官が関与する場合③自衛隊と民間事業者との請負契約により民間技術者を従事させる場合④個人による自発的な参加による場合、等が考えられる。①のケースは防衛招集以降は通常の自衛官と同様の扱いであり、問題は生じない。②③のケースは、国際法上の観点からは、軍隊の正規の構成員とみるか、軍隊に随伴するものとみるかで法的位置づけと保護は異なってくるが、国内法の地位との関係をどのように整理するかが課題となるであろう。④は国際法上の DPH に該当するかどうかが問題となり、次項で検討する。

②のケースでは、防衛事務官及び防衛技官（以下、「非自衛官」という）は自衛隊法上の自衛隊員[400]であるが、戦闘行為に従事する自衛官とは異なり、国実力行使に参加すること及び第一線で勤務することはない、とされている[401]。このため、防衛事務官及び防衛技官は、衛生要員及び宗教要員と同様、国際法上の軍隊に所属する非戦闘員[402]と見做すか、あるいは軍隊の随伴する者[403]に該当することになる。いずれにせよ、非自衛官が攻撃的なサイバー作戦に関与することは出来ない。これは、③のケースである民間技術者も同様である。一方、高度な技術力を有するサイバー技官等の活用が出来ないことは、自衛隊のサイバー作戦実行能力に影響を及ぼす可能性がある。仮に、合

---

398 明確に違法性阻却が得られない例として、故意に行った行為、あるいは命令違反等が挙げられる。前掲注 237。
399 付随的損害が合法とされた場合においては、国家賠償ではなく損失補償の問題となるが、武力攻撃事態における損失補償については、戦後復興の一環として検討されるとして、具体的な法令は未整備である。前掲注 237。
400 隊法 2 条 5 項。また、国家公務員法 2 条第 3 項 16 号の規定に基づく特別職の国家公務員でもある。
401 第 61 回国会参議院内閣委員会議録第 17 号有田喜一防衛庁長官答弁（昭和 44 年 5 月 8 日）。
402 AP Ⅰ art 43(2).
403 GCⅢ art. 4 A (1).

法的に攻撃的なサイバー作戦に関与させたい場合は、正規の自衛官に登用する、あるいは予備自衛官制度の活用検討が求められる。

DPHとは見なされないネットワークの維持・管理といった業務においても、付随的損害に見舞われる蓋然性があることは注意が必要である。自衛隊の基地・駐屯地で勤務する場合は当然であるが、仮に自衛隊関連施設あるいは戦闘地域から離隔したデータセンター等であっても、自衛隊が使用するデータを取り扱う場合は軍事目標に該当する可能性は否定できず、その場合は正当な攻撃対象となり付随的損害が発生する可能性がある。非自衛官の場合は、自衛官と異なり戦闘行為による死傷が想定されていないため、公務災害補償において自衛官と差異が生じる可能性があることも問題となるであろう[404]。

③の請負契約により業務を行う民間技術者の場合は、そもそもそのような危険性を認識した上で契約する企業や技術者が国内に存在するか、という問題に加え、請負契約であっても危険な職場環境において労働に従事させたことにより安全配慮義務違反に基づく民法上の損害賠償を求められる可能性を考慮しておくことが必要であろう[405]。

サイバー作戦において、非自衛官及び民間力の活用は極めて重要であるが、十分な活用のためには、十分な保護及び補償制度が整備されることが前提であることは言うまでもない。今後、自衛隊がサイバー作戦を実効性あるものとするには、本課題は最優先に取り組むべき課題と認識する。

8.6.1 DPH の国内法上の評価

④のケースである DPH であるが、国内法の観点からは、国内に所在する個人及び団体等が、自衛隊を含む日本に対し行う場合、敵対国に対し行う場合、及び別の外国間で行われる国家間武力紛争のいずれかの交戦国に行う場合、の３つのケースが考え得る[406]。DPH は、戦闘員資格を有しないものによる戦闘行為であることから、国内法刑法違反に該当する場合は、それぞれの罰条により処罰される可能性がある。

まず、国内に所在する文民（外国人含む）が自衛隊を含む日本政府等に対しサイバー攻撃等を行う場合である。本来、国際人道法では、DPH を行う文民は、当該行為に従事している間は合法的な攻撃目標であり、物理的手段を

[404] 防衛出動時の公務災害補償制度については細部整備が進んでいないため詳細な検討は困難であるが、非自衛官の場合は前線での勤務が想定されておらず、行動時に自衛官に認められる傷病補償年金、障害補償又は遺族補償の特例の対象外となり、自衛官と差異が生じる可能性がある。国家公務員災害補償法20条の2及び防衛省職員の災害補償に関する政令2条

[405] 労働契約法5条（労働者の安全への配慮）

[406] 国外に所在する者による DPH も考え得るが、国内法の問題ではなく国際法上の問題となる。

含む攻撃が可能であるが、国内法上このような対応が許容されるかは難しい問題であろう。従って、可能な限り、警察あるいは自衛隊警務隊により逮捕し、刑法上の処分を行うことになるであろう。適用される刑法は、DPH 行為の内容により変わるが、不正アクセス禁止法、刑法上の不正指令電磁的記録に関する罪、電子計算機損壊等業務妨害罪等が代表的なものとして考えられる。加えて、武力攻撃事態であることから、状況により刑法 81 条外患誘致罪及び同 82 条の外患援助罪に問われる可能性は否定できない。外患に関する罪は、未遂に加え予備又は陰謀罪が規定され、特に外患誘致罪の法定刑は死刑のみである。

次に、敵対国に対し、自発的にサイバー攻撃等を行う場合であるが、この場合であっても前項と同様に刑法に違反する行為であった場合は罪に問われることになる。加えて、前述の通り、国際法上は敵対国軍隊から合法的な攻撃対象となり、また相手国に拘束された場合は、敵対国の国内法で処罰されることになる。

最後に、日本以外の外国間で行われる武力紛争に関与してサイバー攻撃等を行う場合である。現在も継続中のロシア - ウクライナ紛争においても、ウクライナ側の呼びかけでロシアに対するサイバー攻撃に加担する日本人に関する報道がなされており、現実的な問題である。この場合も上記と同様の罪に問われる訳であるが、状況により刑法 93 条私戦予備及び陰謀罪に問われる可能性も否定できない。また、個人の問題にとどまらず、被害国との関係において、日本政府が国際法上の相当注意義務違反を問われる可能性があり、問題が極めて複雑・深刻化する。

サイバー攻撃の低い敷居は、個人による武力紛争への参加を容易にしてしまう可能性がある。いずれの場合においても、刑法上の罰則にとどまらず、相手国からの攻撃の可能性、更には国家間での新たな紛争を引き起こす可能性があることを十分に周知徹底することが必要である。このような事態を避ける上でも、知識の普及を図るとともに、武力攻撃事態においても、努めてサイバー空間における違法行為の取締りは積極的に行い、攻撃の対象となる前に逮捕・拘束することで逆に保護していくといった積極的な対策が必要になるかもしれない。

8.7 小　結

日本においては、元来有事法制の検討が低調であったことに加え、学術分野においても国際法と国内法が別々に議論されることが多く、国際法と国内法の関係が明確になっていない、あるいは国際法の規定が国内法で担保され

ていない等の問題が多数存在する。実際、前章でみた国際人道法を始めとする武力紛争に適用される国際法の活発な議論に比し、国内法の議論は極めて低調である。

武力攻撃事態における国内法整備は、サイバー分野にとどまらず、安全保障法制全体の課題であるが、地理的境界が存在せず、かつ匿名性の高いサイバー空間においては特に影響が顕在化し易いと考えられる。しかし、戦争放棄を標榜し、緊急事態条項を持たない日本国憲法の特性を踏まえれば、自衛隊が武力紛争を戦うのは日本国内に限定され、実際に適用される法は国内法であることは明らかである。このため、国際法と同レベルの国内法規定を整備しておくことが本来必要であると考えられる。特にサイバー空間においては彼我の識別が困難であるとともに地理的な区分も困難であることを踏まえれば、国際法と国内法に差異がある状況は早急に解消すべきである。特に、武力攻撃事態認定と国際人道法の適用時期の整合、隊法第 88 条の適用要件について具体化及び④サイバー作戦に関与する文民保護の具体化といった点は優先的に取組むべき課題と認識する。

また、第 6 章及び前章で述べた個人情報保護及びプライバシー保護の問題は、本章でも共通する課題である。特に、日本の個人情報保護制度は有事対応をほとんど考慮せず策定されており武力攻撃事態における自衛隊の情報収集活動が大きく制約される可能性があることは今後の検討課題として認識されるべきであろう。

Ⅸ　結　論

9.1　日本の課題と対応の方向性

本稿では、平時から有事に至る紛争スペクトラムにおいて、自衛隊がサイバー作戦を行う上での国際法及び国内法双方の課題を検討してきた。第１章から第３章にかけて、導入部として現状及び問題認識、サイバー空間における軍事作戦及びサイバー抑止理論の概要等の背景事項を説明した。第４章からは本論とし、サイバー紛争に適用される法を俯瞰したのち、平時～有事の流れの中での国際法及び国内法の適用における課題を論じてきた。第５章及び６章では平時～GZ 事態、すなわち有事には至らないものの純粋な平時とも言えないという、まさにグレーな状態における法適用の困難性に焦点をあてた。とくに第６章の部分は能動的サイバー防御構想において自衛隊が果たすべき役割まで踏み込んだ議論を行った。さらに第７、８章においては有事における国際法及び国内法の適用を焦点とし、国際法整備に向けた日本が行うべき主張の方向性を示すとともに、早急な国内法整備の必要性について明ら

かにした。とくに、第８章で述べた有事、すなわち武力攻撃事態における国内法は国際法と比較しても整備が極めて不十分であり議論が必要であることを明らかにした。末章である本章（第９章）では、あらためて法的課題の再確認をおこなうとともに、それぞれの課題に対し、本論内で取り上げた提言等を整理・再提示を行うことにより、本稿の主張をより明確化することを試みる。また、最後に本稿では十分に検討できなかった残された課題についても付言する。

本稿では国際法及び国内法の双方の観点から様々な論点に触れたが、これらの課題は、大きく区分するならば、以下の三つの領域に分類されると考えられる。一つは国内法の観点であり、自衛隊の任務・役割及び権限の不明確性という問題である。二つ目は、国際法の観点からはサイバー空間への国際法適用にあたって解釈の曖昧性が挙げられる。三つ目として、国際法と国内法の整合性が不十分であることである。

国内法上の課題は、主に平時～GZ 事態における問題であるが、第一に日本のサイバー安全保障における各省庁間の役割分担が不明確であることが根本的な課題である。能動的サイバー防御を現実のものとするためには、新たに設置される NISC 後継組織を含めた、サイバー安全保障態勢・体制の構想を早急に確立することが必要である。特に、安全保障の中核となる自衛隊が能動的サイバー防御構想においてどのような任務・役割が期待されるかを明確にするとともに、サイバー空間における情報収集活動及び、平時～GZ 事態における「妨げる能力」行使するための法的権限の創設が求められる。

国際法上の課題に関しては、解釈が曖昧という現実を積極的に捉え、日本に有利な国際法解釈の主張の好機とすることが必要である。特に、以下の内容を主張していくことが必要である。まず平時～GZ 事態における対抗措置の問題が挙げられる。特に、集団的対抗措置の合法性については、日本にとって重要な論点である一方で、専門家の間でも意見が分かれる問題である。次に、有事におけるサイバー作戦への国際人道法適用にあっての解釈の問題が挙げられる。特に、民用物への物理的効果を伴わないサイバー攻撃の合法性を積極的に主張しなければならない。

国際法と国内法の整合性に関しては、武力紛争間に適用される国際人道法と国内法の整合を取ることが求められる。特に、国内法である隊法 88 条と国際人道法の各種規定との関係を明らかにすることが必要である。また、武力紛争間におけるサイバー作戦に関与する民間事業者の保護は、国際法と対応する国内法規定が欠落しており、早急に整備が必要である。

9.2　能動的サイバー防御構想における自衛隊の任務・役割・権限の明確化

9.2.1　サイバーセキュリティ基本法を改正し自衛隊の任務・役割を明確化

本稿Ⅵ章において詳細な検討を行ったが、第一にサイバーセキュリティ基本法を改正し自衛隊の任務・役割を明確化することが必要である。特に、自衛隊の役割が抑止力にあるとしつつ、平時から実効的に行使する抑止力であることを明らかにする必要がある。具体的には、以下の内容を明記することを提言する。

○　NISC 後継組織による一元的な総合調整の下、各関係機関が密接に連携して対応する。
○　NISC 後継組織が関係機関に対する統制権限を有する。
○　各関係機関は、情報共有を積極的に図る義務を有する。
○　国内における対応は一義的には警察が責任を負う。
○　外国政府が関与する武力攻撃に至らないサイバー攻撃に対しては、対抗措置として自衛隊が「妨げる能力」を行使し対処する。

想定する具体的な対処組織の在り方としては、NISC 後継組織がサイバー安全保障に関する総合調整機能を担い、警察・自衛隊をはじめとする関連組織が情報共有を図りつつ、防護及び反撃をできる体制・態勢を構築する。

第一に全関係府省庁が参加する情報共有の枠組みが必要である。必要な情報に関しては強制的に共有させる法令根拠を設けることも一案と考える。ただし、自衛隊には国外及び国内の外国政府関係者を主対象とした強制手段を含む情報収集の権限を付与すべきである。

全般的な警察と自衛隊の役割は基本的には現状と変わらず、外国政府が関与しないサイバー犯罪等に対する対応は引き続き警察が担い、外国政府が関与するサイバー攻撃は自衛隊が対処を担うことが妥当である。その上で、後者に関しては現状では有事以降でしか対応できないところ、平素から「妨げる能力」による反撃あるいは未然の阻止を含む任務を自衛隊が負うことが可能とする。しかしながら、平素においては、反撃の必要性を含め全般の対応方針はNISC後継組織が総合調整役を担うべきであり、自衛隊単独が独自に判断し反撃・眠前阻止を行う態勢は避けるべきであろう。また、警察は基本的には国内のみの活動が想定され、捜索・差押えを含む強力な捜査権限を有することから「妨げる能力」保有の必要性は薄いと考える。外国所在のハッキング集団等に対処する必要性がある場合、NISC 後継組織の総合調整のもと、省庁間協力の枠組みで自衛隊が「妨げる能力」の行使を行う態勢で対応が可

能と考える。図５は現状から能動的サイバー防御態勢・体制における NISC、防衛省・自衛隊及び警察の各組織の保有機能に関する一案を示す。

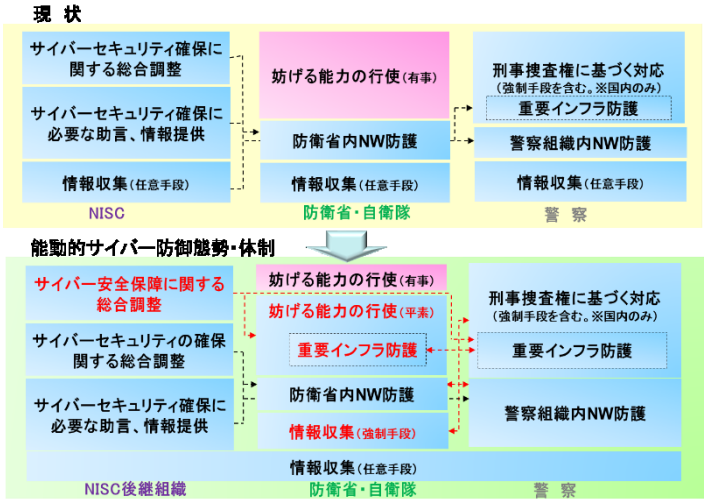

図５「能動的サイバー防御態勢・体制における各組織の保有機能（提言）」

9.2.2　自衛隊法改正により情報収集活動の法的根拠を付与

情報はあらゆる行動の基礎となる。軍事作戦においても、あらゆる作戦は適切な情報収集により支えられるが、サイバー空間における情報収集は時間を要し、一朝一夕で成果が上がるものではない。特に、「妨げる能力」を実際に行使するには、相手の脆弱性を事前に把握しておくことが必要であり、平時からの情報収集活動は必要不可欠である。一方、隊法には情報収集活動を行うにあたっての根拠規定が存在しない。本文中でも述べた通り根拠規定がないことが直ちに情報収集活動が行なえないことを意味するわけではないが、極めて厳格な日本のサイバー空間への法規制を踏まえれば、明確な根拠規定の整備が第一に求められる。

本稿ではVI章において述べた通り、サイバー空間に限定されない包括的な情報収集活動の根拠規定の新たな設置を提言する。具体的には、2021 年に日本維新の会、国民民主党及び無所属クラブの議員が議員立法として提出した以下の条文の案中の「必要な情報の収集」として、サイバー空間における情報収集活動を根拠づけるものである。

第八十四条の四の二 防衛大臣は、公共の秩序の維持を図るため、自衛隊の部隊に対し、必要な情報の収集その他の警戒監視の措置を講じさせることができる。

しかし、艦船や航空機による情報収集活動と異なり、目に得ないサイバー空間における情報収集活動はそれだけに国民に不安を与える可能性が高い。

このため、実際にサイバー空間において情報収集活動を行うにあたっては、「通信の秘密」、各種刑法規定、個人情報保護法等の保護法益と安全保障上の必要性を十分に加味した上で適切な規則を防衛省・自衛隊内で制定し、公表すべきと考える。特に、対象となるサイバースペースを特定の国家に指定し、公表する等の処置を検討することが必要と考える。

9.2.3　自衛隊法改正により「サイバー対抗措置行動」を新たに規定

Ⅴ章において武力攻撃の閾値に至らないサイバー攻撃への対応として、国際法上の対抗措置の活用を提言するとともに、国内法上の根拠規定の不存在を指摘した。続くⅥ章において、平時～GZ 事態において「妨げる能力」を行使するための根拠法令の創設を提言したが、これらは実態として同一の内容を国際法及び国内法の双方観点から区分して述べたものであり、国際法と国内法の整合性確保の観点からも望ましいものと考える。本稿では、以下の条文案を提言した。

（サイバー対抗措置）
八十四条の六　防衛大臣は、重要インフラ等に対し、外国政府が関与する国際法規に反する不正なサイバー攻撃が発生したときは、対抗措置として、自衛隊の部隊に対し、これを阻止し、あるいは停止させるため必要な措置を講じさせることができる。

上記案は、隊法 84 条が定める「領空侵犯に対する措置」を参考に、必要な措置を取る権限を規定しつつもその態様や方法を具体的に示さない規定の定め方とした。また、国家責任条文に規定される対抗措置の要件については、特に重要な目的要件を焦点に条文に含ませ、その他の要件は防衛省内における規則として定める方式を想定している。サイバー空間の特性を踏まえ、努めて実効性があり、かつ技術進展等に対し容易に陳腐化しないように配慮したものである。しかしながら、要件及び権限が極めて曖昧であり、必要性及び緊急性等の要件に対する歯止めが不十分との批判は免れないものと考える。検討にあたっては、更なる考察が必要と認識する。

9.3　日本に有利な国際法解釈の主張

サイバー空間に適用される国際法は形成途上にあり、自国に有利な戦略環境を構築するために積極的に国際法解釈を行い、議論を主導していくことが望まれる。現状においても外務省は積極的に活動をしていると評価できるが、将来の戦略環境への展望や国内における自衛隊のサイバー作戦への影響等が

しっかりと考慮されているとは言えない状況である。国内情勢及び国内法との整合を意識した上で国際法解釈を主張していくことが求められる。

9.3.1 集団的対抗措置の合法性

対抗措置の欠点の一つは、対抗措置においては「武力の行使」に該当する行為は禁止されている点である。このため、責任国が悪意あるサイバー行為をやめ、義務に復帰するよう促すための強制力が不足することであり、特に被害国の技術レベルが十分ではない場合にこの問題は顕著となる[407]。

現状の日本が保有するサイバー作戦能力の実態は不明であるが、組織及び予算規模等を考慮すれば対象国が保有するサイバー能力に比し、特に攻撃面においては劣勢となる可能性が高い。そのような場合、米国のような高い技術力を有する同盟国との間での集団的対抗措置が認められれば非常に有利である。集団的対抗措置の合法性については、現時点では否定的な意見が多いことは事実である。一方で、多くの国際法専門家は、国家が集団的対抗措置をとることを可能にする新たな法的枠組み構築の必要性を認識し、主張している。日本はこれらの意見に明確な支持を表明し、積極的に議論をリードすべきである。

9.3.2 サイバー攻撃への国際人道法適用にあたっての解釈

サイバー空間への国際人道法の適用は依然として様々な不明確性が存在する。特に、サイバー攻撃と攻撃の定義の関係を整理することは重要な課題である。国際人道法は、軍隊が攻撃を行う場合、軍事目標に限定すること、あるいは攻撃に巻き込まれる文民や民用物も極限といった様々な規制を課している。従来の国際人道法の解釈においては、人の死傷や物の破壊といった物理的な被害が生ずるもののみを攻撃として整理しおり、電磁波による通信障害、あるいは心理戦といった非物理的損害のみを生じる作戦行動は攻撃には該当しないと整理していた。しかし、サイバー攻撃に関しては、近年、重要インフラ等へのサイバー攻撃の影響の大きさ等から、目標の機能停止等の無力化のみの効果を生ずる場合であっても攻撃に含めるべきとの見解が主張されており、一定の指示を得ている。ICRC や国際法学者に留まらず、一部の国家もこの見解を支援しており、日本の外務省の見解も当該解釈を支持しているよう

[407] サイバー攻撃の特性として、効果をコントロールすることの困難性が挙げられる。武力の行使に至らないよう、所望の目標に対し限定された効果を生じさせるためには高度な技術力が必要と考えられる。

に見受けられる[408]。しかし、上記見解を採用した場合、サイバー作戦の対象は軍事目標に限定され、付随的損害等の考慮も必要となり、作戦の実行そのものが大きく制限されることになる。仮に自衛隊が将来的にサイバー作戦を積極的に行う構想を保持していた場合、上記解釈と採用することは、自衛隊の作戦構想を阻害する可能性が生ずる。サイバー攻撃は地理的な制限を超えて相手国の領域を攻撃できる可能性を秘めており、想定される対象国に比し装備・戦力に劣る自衛隊にとっては貴重な戦力となり得る。国際人道法は、文民及び戦傷者等の非戦闘員の保護を目的とするが、飽くまで軍事的合理性とのバランスの上で成り立つものであり、国際人道法の解釈によって自らの手足を縛ることにならないよう十分な配慮が必要であろう。

9.4 国際法と国内法の整合

国際法の解釈を主張することと並行的に、国内法を整備し、国際法上の内容が具体的に国内法で担保されるよう努めることが必要である。特に、武力攻撃事態における国内法整備は、サイバー空間に限らず安全保障法制において最も具体的な検討が進んでおらず国際法との差異が大きい分野であると考えられる。新安全保障戦略においても、武力攻撃事態への対応に関しては殆ど触れられておらず、今後の具体化が求められる。

通常、各国の軍隊は武力紛争のような国家の非常事態においては、緊急事態条項等により既存の国内法上の枠組みが停止あるいは制限され、主に国際法（主に武力紛争法）に基づき行動する。一方、憲法に緊急事態条項の無い日本の場合は、国際法上の武力紛争下においても、基本的には既存の国内法秩序が適用され続けることになる。従って、国際法と国内法を照らし合わせ、国際法上の権利及び義務がしっかりと国内法上担保されることが必要である。特にサイバー作戦は地理的境界ない、非物理的効果が主体、多くの民間事業者や技術者の関与等の従来の作戦にはない特徴があることから、問題が複雑化し易い。サイバー作戦において特に明確化すべき点として、国際人道法と隊法 88 条の関係、サイバー作戦に関与する文民保護の問題がある。

9.4.1 国際人道法と隊法 88 条の関係整理

隊法 88 条は自衛隊の包括的な作戦行動を規定する唯一の国内法上の権限規定である。しかし、これは、サイバー作戦に限らずあらゆる作戦形態に共通

[408] 外務省・前掲注 139。

する課題であるが、隊法 88 条の具体的な適用要領は明確ではなく、特に国際人道法との関係は極めて曖昧である。前述の通り、通常交戦国の軍隊は国際人道法に基づいて行動する。一方、自衛隊の場合は、有事においても法的根拠は国内法であり、個々の作戦行動、すなわち「武力の行使」についても、その根拠は隊法 88 条のみである。しかし、隊法 88 条の規定は極めて曖昧であり、個々の作戦行動に対する合法性の判断としては不十分である。一方で、国際人道法は戦闘の方法・手段に対し様々な規制を設けており、ある程度の基準を明示しており、自衛隊の法務に関する教育においても、戦闘間の行動に関しては基本的には国際人道法に基づく教育が行われている。一方で、国際人道法の規定を遵守すれば、隊法 88 条の要件を満たすことになるのか、あるいは別途隊法 88 条独自の基準が存在するのかについて明確な見解は存在しない。サイバー作戦においては、特に地理的な適用範囲が問題となるであろう。仮に島嶼部等に戦闘地域が極限されている場合であっても、サイバー作戦は日本全域で行われる可能性がある。国際人道法には適用にあたっての地理的制限はない。一方で、隊法 88 条は戦闘行為が行われている地域のみの規定とする見解もあり[409]、サイバー空間における適用の有無は明確ではない。仮に、隊法 88 条の適用が物理的な戦闘地域に限定される場合、その他の地域では刑法上の違法性阻却は得られないことになる。従って、国内ネットワーク内における自衛隊のサイバー作戦は極めて大きな制約を受ける可能性が生ずる。この問題は、サイバー作戦に限らず自衛隊の作戦行動全般に影響を及ぼす重要な課題であり、早急に解消すべき課題である。具体的には、隊法 88 条を改正し、具体的な基準を明示する、あるいは個々の作戦行動の具体的な基準は国際人道法に依る等の政府解釈を明らかにする等の対応が必要であろう。通常、出動要件を除いた戦闘間における軍隊の行動規範は国際法であり、国内法により個々の作戦行動権限を規定する自衛隊は極めて特殊であるという点を踏まえれば、国際人道法を判断基準とする後者の方向性が望ましいと考えられる。また、実際に、自衛官が行った戦闘行為に対する違法性が問われた場合、自衛隊には軍法会議が存在しないことから、当該自衛官は国内法による訴追を受ける。つまり、最終的判断は司法が負うことになるわけであるから、行政に留まらず司法の意見も交えた総合的な検討が必要であろう。

9.4.2 サイバー作戦に従事する文民の保護の具体化

日本の有事法制において、大きな課題になると考えられるのが、武力攻撃

[409] 前掲注 237。

事態における自衛隊の作戦に関係する民間人の法的位置位置付けとその保護であると考えられる。特に、サイバー作戦においては、民間技術者の関与は不可欠であり、その保護は極めて重要な問題である。武力紛争法上、文民の保護は細かい規定が整備されている。しかし、国内法上の扱いは明確ではない。特に、防衛事務官及び防衛技官の法的位置付けや、民間技術者が許容される作戦への関与の程度について真剣に検討することが必要である。特に、国際人道法上は、文民であっても自衛隊の作戦に関与していると判断された場合は、文民の敵対行為への直接参加として攻撃の対象となること、また敵対行為の直接参加とはならない場合であっても、自衛隊施設内及び周辺で勤務する場合は攻撃に巻き込まれる高い蓋然性があることは十分に周知徹底し、事前に合意を得た上で契約・従事させることが必要である。この際、相手側からの攻撃により死傷した場合における適切かつ十分な補償制度を確立することが必要である。これらの具体化なしに部外力の活用を図ることは難しいであろうと考えられる。

また、個人によるサイバー作戦への参加を防止することについても検討することが必要である。サイバー攻撃は個人でも比較的容易に実施できるため、文民による敵対行為への参加を誘発し易いという特性がある。特に、第三国間で武力紛争が生起し、自国が戦場となっていない場合は、武力紛争に参加しているという意識を持たずに実行してしまうケースが考えられるが、前述したように一定の要件に該当する場合は、国際人道法上は攻撃の対象とされる場合がある。また敵対行為を行った文民が所在する領域国と被害を受けた交戦国との間に新たな国際紛争を引き起こす危険性も存在する。

実際に武力紛争が生起した場合には、相手国側、あるいは自衛隊を支援する目的で個人がサイバー攻撃を行う可能性は十分に考えられる。しかし、国際人道法は一般的な認知度が高いとは言えないことため、サイバー攻撃を行うことによって保護を失い、直接攻撃の対象になる可能性があることを認識する者は極めて少数であろう。政府として知識の普及を図り、上記行為を防止していくことが必要である。また、国内法上も刑法及び不正アクセス禁止法に違反に該当することから、有事であっても積極的な取り締まりを行うことも、相手国による攻撃を事前に防止するという観点からは、ある意味文民保護になり得ると考えられる。

9.5　残された課題

本稿では自衛隊が行うサイバー作戦の法的課題を焦点としたものであり、主にサイバー手段に伴う法的課題に絞って検討を行ってきた。このため、本

文中でいくつか言及した通り、極めて重要な課題であるが本論では十分に検討できなかった課題が存在する。本稿ではそれらを「残された課題」とし、今後の研究課題として簡単に付言する。具体的には「ディスインフォメーション対策」と「個人情報保護及びプライバシー保護」の問題が考えられる。

9.5.1 ディスインフォメーション対策

ディスインフォメーションを含む影響工作や情報作戦はサイバー作戦における重要な要素となりつつある。しかしながら、本質的には古くから行われてきた心理戦の発展形であると考えられ、サイバー空間特有の課題とは言い難い[410]。また、国際法及び国内法の両分野においてもディスインフォメーションを規制する法律は存在しない。

一方で、生成 AI をはじめとするフェイク技術の発展によりフィクションと現実を見分けることを困難になっていることに加え、micro-targeting 能力の向上は特定の人物に対し偏った情報を提供し意図的に filter bubble 現象を生み出すことを可能にするなど、新しい技術はより効果的に人々に影響を及ぼすことを可能としつつある[411]。これらの新しい技術を活用することにより、他国の意思決定を妨害・誘導する等の安全保障上の脅威となる活動が行われる可能性が高まっていることから、対策は必要不可欠と考える。検討すべき論点としては以下のようなものが存在する。

ディスインフォメーションの違法性及び規範違反性

第一に、そもそもディスインフォメーションが違法なのか、あるいは道徳や倫理上からも非難の対象であり、規制の対象とすべきか、という点が問題となる。

違法性に関しては、本論で述べた通り、国際法ではディスインフォメーションを規制する条約等はなく、また今後も制定される可能性は低いと考えられる。一部、情報操作や選挙妨害は主権侵害及び違法な干渉に該当する可能性は指摘されているが、単に偽情報を流布する行為自体を規制する法的枠組みは存在しない。一方、国内法では一部名誉棄損や威力業務妨害等に該当する場合は法的な対応が可能である。しかしながら、外国からのディスインフ

---

[410] 津屋尚「偽情報がもたらす脅威～情報戦への備えを」2023 年 8 月 18 日 NHK 解説委員室< https://www.nhk.or.jp/kaisetsu-blog/100/486848.html >。

[411] Tim Hwang, *Maneuver and Manipulation: On the Military Strategy of Online Information Warfare* (Pennsylvania: US Army War College Press, 2019) at 1.

ォメーションに対しては国内法では対処が難しく、実効性を伴わないという問題がある。

法的規制以前に、規範の観点からも規制の対象となるのか、という論点も考え得るであろう。ディスインフォメーション自体は紀元前から行われてきた活動であり、国家間紛争において自国に有利な情報操作を行うことは国家として国益擁護の観点から当然の行為であるという意見も存在するであろう。また、国内法的にも具体的な被害が生じる場合はすでに刑法あるいは民法等での対応が可能であるところ、あえて明確な被害がないディスインフォメーションを規制する必要があるのかという議論も考え得る。

表現の自由と法規制との関係

仮に法規制を必要とした場合であっても、代表的な基本的人権である「表現の自由」との抵触が問題となる。国際法においても国際人権法において表現の自由は規定されているが[412]、主に問題となるのは国内法であろう。

日本国憲法 21 条は表現の自由を保障する。憲法上、表現の自由といった精神的自由に関する規制は二重の基準の理論等でも知られるように経済的自由等よりも厳格に審査される。とくに公権力による規制は、21 条後段の「検閲の禁止」及び「通信の秘密」に関する規定を見てもその厳格な制約が存在することが見てとれる。

しかしながら、表現の自由が決して無制限な自由を意味するわけではなく、公共の福祉に反する、外国政府からの干渉といった情報までを規制することが叶わないわけではないと考えられる。一方で、外国からの情報に外国政府の関与があるかどうかを識別することは極めて困難である。国民が外国からの情報を入手する自由を保障することは、政府による情報統制を排し、健全な民主主義を維持するために不可欠な要素であるという側面もあり、一律に外国からの情報を遮断することは不可能であり、かつ望ましくないであろう[413]。

---

412 市民的及び政治的権利に関する国際規約 17 条

413 外国人の人権保障についてはマクリーン事件判決（最大判昭 53 年 10 月 4 民集第 32 巻 7 号 1223 頁）が著名であるが、当該判例は外国人であっても基本的人権の保障は政治活動の自由を含めて及ぶとする一方で、その制限に関する国の大きな裁量権を認めていることを踏まえれば、外国からの情報発信を遮断する権限についても国家の裁量として認められる可能性が高いと考えることもできる。しかしながら、上記判例には批判も多く存在することに加え、学説上も国家による外国人に対する表現の自由あるいは外国からの情報に対するアクセス権の制限についての評価は定まっていない。戦前のような国家による恣意的な情報遮断につながる可能性等も存在することを踏まえれば、例え安全保障の観点によるディスインフォメーション対策であっても、情報遮断等の強力な情報統制権限を国家の裁量の余地として認めることには慎

したがって、現行の国内法制で規制される場合以外で新たに法的規制を設けるならば、どのような場合に規制が許されるかを詳細に検討することが必要であろう。特に、誰がどのような基準で、かつどのような規制を行うかという具体的な規制要領を明らかにすることが必要であろう。

9.5.2　個人情報保護及びプライバシー保護

2001 年の米国同時多発テロ以降、テロリズムへの対応（以下「テロ対応」と略する。）との名目のもと、軍や情報機関による大規模な個人情報の収集が日常化するようになった。テロ対応だけでなく、国家間武力紛争の場面においても、個人情報は積極的に活用されており、安全保障領域における個人情報の収集・利用は必要不可欠な要素となっているといっても過言ではない。しかし、政府による個人情報の収集は多くの場合、プライバシーの侵害にあたる可能性が高い。国際法はこの点についてほとんど規定を定めていないが、戦場や占領地における住民監視や個人情報の大規模収集の是非が議論され始めている[414]。また、各国の国内法において政府による安全保障を理由とした個人情報の収集及びプライバシーの侵害に対しては様々な議論が存在する。日本の国内法においても、警察や自衛隊による情報収集活動に対する個人情報保護法違反やプライバシー侵害に対する訴訟が実際に生起している[415]。一方で日本の個人情報保護法制は有事に関する規定が一切なく、プライシーに関しても有事法制と絡めた議論はほとんど行われていない。このことは、安全保障及び情報法制上きわめて大きな問題であると考える。主要な論点とは以下のものが考えられる。

武力紛争におけるプライバシーの侵害

武力紛争における情報の価値は飛躍的に高まっており、軍事目標や戦闘員にとどまらず交戦国領域内に所在するあらゆる組織、人物が情報収集の対象

重さが求められるべきと考える。

414 一例として Russell Buchan and Asaf Lubin, eds., “The Rights to Privacy and Data Protection in Times of Armed Conflict” (2022), online: CCDCOE <https://ccdcoe.org/upl oads/2022/06/The-Rights-to-Privacy-and-Data-Protection-in-Armed-Conflict.pdf.>

415 代表的なものとして、防衛庁（当時）・自衛隊が情報公開請求を行った者をリスト化し部内で閲覧可能な状態にしていたことが問題となった防衛庁リスト事件、海外におけるイスラム過激派の活動激化に伴い、国内におけるイスラム教徒の動向を監視した情報が流出した公安テロ情報流出被害国家賠償請求控訴事件（東京地判平成 26 年 1 月 15 日判例時報 2215 号 30 頁及び東京高判平成 27 年 4 月 14 日／平成 26 年（ネ）1619 号）、風力発電所建設を巡る反対活動に対し公安情報として個人情報の提供を警察が企業に依頼した大垣警察市民監視国家賠償請求事件（岐阜地判令和 4 年 2 月 21 日判例時報 2548 号 60 頁）及び本論でも言及した自衛隊保全隊による監視活動等停止請求事件（前掲注 215）等が存在。号

となっているといっても過言ではない。特に、24 時間上空監視が可能な偵察衛星・無人偵察機の普及、サイバー手段による大規模収集及び AI を活用した膨大なデータの短時間で処理が可能となったことは、直接戦闘と無関係な文民のプライバシー侵害という新たな課題を生み出している[416]。また、ロシア‐ウクライナ紛争では捕虜や戦闘員のセンシティブな個人情報をインターネット上で暴露する戦術が使用されているが[417]、捕虜のプライバシーを不必要に侵害している可能性があるほか、紛争終了後も個人に対する影響が残りかねない、いわゆるディジタルタトゥーの問題等への指摘も考え得る。

政府による安全保障を理由とした同意のない個人情報の収集・利用

近年、欧米諸国を中心に各国で個人情報保護法制の整備が進んでいる。しかしながら、大部分の国は政府による安全保障上の活動を個人情報保護の規制の対象外とし、別途政府による情報収集に対する個別の根拠法を設けて権利濫用を防止する等の処置対策を行っている[418]。一方、日本の個人情報保護法は安全保障に関する規定が一切なく、自衛隊法上も適用除外が規定されておらず、かつ情報収集に関する法的根拠が存在しないことから、有事においても平素と同様の規制が自衛隊による情報収集活動に適用される。

これは、自衛隊等による情報収集活動に大きな制約を課す可能性がある一方で、逆に明確な基準がないことにより、行き過ぎた情報収集による権利侵

---

416 武力紛争において監視・情報収集活動が個人情報・プライバシー保護の観点から問題となった例としては、イラクやアフガニスタンにおいて米軍等が行った生体認証プログラムの例が存在する。一般住民に紛れて潜伏したテロリストの身元判別を目的として、光彩、指紋、顔の画 像などの情報を採取し数百万人分のデータベースを作成し、テロリストの身元を割り出しに活用されたとされる。Thom Shanker “To Track Militants, U.S. Has System That Never Forgets a Face” (July 13, 2011), online: The New York Times <http://www.nytimes. com/2011/07/14/world/asia/14identity.html>.; “The Eyes Have It: Biometric Data and the Afghan War” (July 7, 2012), online: The Economist <http://www.economist.com/node/21558263/print>.上記例では、戦闘に直接無関係な文民の個人情報を無差別に収集し保有することに対する批判がなされ、複数の人権団体が米国国防長官に対して見直しの要請を行ったこととされる。

417 "Ukraine: Respect the Rights of Prisoners of War" (March 16, 2022), online: Human Rights Watch <https://www.hrw.org/news/2022/03/16/ukraine-respect-rights-prisoners-war>.

418 一例として、EU では一般データ保護規則（GDPR）23 条は安全保障等の領域では国内法による個人情報保護の制限を認めており、これを受け、EU 加盟各国の国内法は安全保障上の政府の活動は個人情報保護の対象外とする 。また、政府等による情報収集に関する権限法の一例として英国は、「捜査権限規制法」（RIPA） により国内外の通信傍受を規定し、さらに 2016 年には「調査権限法 」を成立させ政府の権限を拡大している。ドイツでは、「信書、郵便及び電気通信の 秘密の制限に関する法律」（基本法 10 条関係法）に基づく国内の通信傍受が、また、対外的な情報収集に関して連邦情報庁（BND)による同法及び「連邦情報庁法」（BNDG）に基づく監視活動が可能となっている。米国ではプライバー保護法（The Privacy Act of 1974 ）が政府等によるプライバシーを侵害する情報の収集を禁止しているが、刑事捜査及び対外諜報活動に関しては例外規定が設けられている。また、政府による情報収集の権限を定めたものとして、外国の情報収集活動に関する法的枠組みである外国情報監視法(FISA)及び令状無しでの米国民の通話記録収集を禁止する米国自由法（USA Freedom Act)等が存在し、取得可能な情報に関する制限を設けている。

害の発生を助長する可能性があると考える。安全保障上の必要性と権利侵害の程度とのバランスを適切に定めた法的基準や行政機関の情報収集活動をコントロールする枠組みの検討が必要であると考える。

9.6 終わりに

本稿では、自衛隊の行うサイバー作戦における法的課題について、国際法及び国内法の双方の観点から検討を行い、能動的サイバー防御構想の実現に向けて日本が取り組むべき政策を明らかにしてきた。新安全保障戦略は、従来の消極的な姿勢を大きく転換し、実効性あるサイバー安全保障態勢・体制を確立するための大きな転換点となる可能性があると評価し得る。一方で、本論で述べた通り実現に向けた法的な観点からは取り組むべき課題は山積みである。これらの課題は、防衛省・自衛隊だけでなく、関係省庁を含めた政府全体の課題であり、総合一体的に取組むことが求められるであろう。

参考文献

Ⅰ　英語文献

1. 書 籍

Buchan, Russell, and Asaf Lubin, editors. *The Rights to Privacy and Data Protection in Times of Armed Conflict*. CCDCOE, 2022. https://ccdcoe.org/upl oads/2022/06/The-Rights-to-Privacy-and-Data-Protection-in-Armed-Conflict.pdf.

Crawford, Emily. *Identifying the Enemy: Civilian Participation in Armed Conflict*. Oxford University Press, 2015.

Czosseck, Christian, et al. *4th International Conference on Cyber Conflict. Proceedings 2012*. NATO CCD COE Publications, 2012. https://ccdcoe.org/library/publications/4th-international-conference-on-cyber-conflict-proceedings-2012/.

Delerue, Francois. *Cyber Operations and International Law*. Cambridge University Press, 2020.

Dinniss, Heather Harrison. *Cyber Warfare and the Laws of War*. Cambridge University Press, 2012.

Dinstein, Yoram. *The Conduct of Hostilities under the Law of International Armed Conflict*. Cambridge University Press, 2004.

Geers, Kenneth, editor. *Cyber War in Perspective: Russian Aggression against Ukraine*. NATO CCD COE Publications, 2015. https://ccdcoe.org/library/publications/cyber-war-in-perspective-russian-aggression-against-ukraine/. Web.

Goldsmith, Jack, ed. *The United States' Defend Forward Cyber Strategy - A Comprehensive Legal Assessment*. Oxford: Oxford University Press, 2022.

Haataja, Samuli. *Cyber Attacks and International Law on the Use of Force - The Turn to Information Ethics*. New York: Routledge, 2019.

Hufbauer, Gary, et al. *Economic Sanctions Reconsidered*. 3rd ed., Peterson Institute for International Economics, 2007.

Hwang, Tim. *Maneuver and Manipulation: On the Military Strategy of Online Information Warfare*. US Army War College Press, 2019.

Kosseff, Jeff. *The Contours of 'Defend Forward' Under International Law*. NATO CCD COE Publications, 2019, https://ccdcoe.org/uploads/2019/06/Art_17_The-Contours-of-Defend-Forward.pdf.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. the RAND Corporation, 2009, https://www.rand.org/pubs/monographs/MG877.html.

Melzer, Nils. *Cyberwarfare and International Law*. UNIDIR, 2011. https://unidir.org/publication/cyberwarfare-and-international-law.

O'connell, Mary Ellen, editor. *What Is War?: An Investigation in the Wake of 9/11*. Martinus Nijhoff,

2012.

Pijpers, Peter B. M. J. *Influence Operations in Cyberspace and the Applicability of International Law*. Edward Elgar, 2024.

Pictet, Jann S., editor. *The Geneva Conventions of 12 August 1949: Commentary I: Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field of 12 August 1949*. ICRC, 1952.

Schmitt, Michal N, ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.

Sookermany, Anders McD, editor. *Handbook of Military Sciences*. Springer, 2020.

U.K. Ministry of Defense. *The Manual of The Law of Armed Conflict.* Oxford University Press, 2004.

Roscini, Marco. *Cyber Operations and the Use of Force in International Law*. Oxford University Press, 2014.

Zoller, Elisabeth. *Peacetime Unilateral Remedies: An Analysis of Countermeasures*. Martinus Nijhoff Publishers, 1984.

2. 学術誌

Bradley, Liam P.. “Was the Colonial Cyberattack the First Act of Cyberwar Against the U.S.? Finding the Threshold of War for Ransomware Attacks.” *St. John’s Law Review*, vol. 96, 2, 2022, pp. 487–515.

Brown, Gary D., and Andrew O. Metcalf. “Easier Said Than Done: Legal Reviews of Cyber Weapons.” *Journal of National Security Law & Policy*, vol. 7, 2014, pp. 115–138.

Corn, Gary, and Eric Talbot Jensen. “The Use of Force and Cyber Countermeasures.” *Temple International & Comparative Law Journal*, vol. 32, 2, Apr. 2018, p. 127.

Dinstein, Yoram. “Computer Network Attacks and Self Defense.” *International Law Studies: Computer Network Attack and International Law*, edited by Brian T O’Donell, vol. 76, p. 99.

Droege, Cordula. “Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians.” *International Review of the Red Cross*, vol. 94, 2012, pp. 533–578.

Egan, Brian J. “International Law and Stability in Cyberspace.” *Berkeley J. Int’l Law*, vol. 35, no. 1, pp. 169–180.

Eichensehr, Kristen E. “The Law and Politics of Cyberattack Attribution.” *U.C.L.A. Law Review*, vol. 67, 2020, pp. 520–598.

Eichebsehr, Kristen E. “Ukraine, Cyberattacks, and the Lessons for International Law.” *American Journal of International Law Unbound*, vol. 116, pp. 145–149.

Hathaway, Oona A, Rebecca Crootof, Philip Levitz, Haley Nix, William Perdue, and Julia Spiegel. “The Law of Cyber-Attack.” *California Law Review,* vol 100, 4, Aug. 2012, p. 817.

Maurer, Tim, and Garrett Hinck. “Persistent Enforcement: Criminal Charges as a Response to Nation-State Malicious Cyber Activity.” *Journal of National Security Law and Policy*, vol. 10, Jan. 2023, p. 525.

Lin, Herbert S. “Offensive Cyber Operations and the Use of Force.” *Journal of National Security Law & Policy*, vol. 4, 2010, pp. 63–86.

Schmitt, Michael N. “‘Below the Threshold’ Cyber Operations: The Countermeasures Response Option and International Law.” *Virginia Journal of International Law*, vol. 54, no. 3, 2014, pp. 697–732.

Schimitt, Michael N. “Cyber Operations and the Jus in Bello: Key Issues.” *Naval War College International Law Studies*, vol. 87, 2011, pp. 89–110.

Schmitt, Michael N. “The Law of Cyber Warfare: Quo Vadis?” *Stanford Law & Policy Review*, vol. 25, 2014, pp. 269–299.

Schmitt, Michael N. “Wired Warfare: Computer Network Attack and Jus in Bello.” *International Review of the Red Cross*, vol. 84, 2002, pp. 365–400.

Schmitt, Michael N. “Wired Warfare 3.0: Protecting the Civilian Population during Cyber Operations.” *International Review of the Red Cross*, vol. 101, 2019, pp. 333–355.

Schondorf, Roy. “Israel’s Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations.” *International Law Studies*, vol. 97, 2021, pp. 396–405.

The Chatham House. “Principles of International Law on the Use of Force in Self-Defence.” *The International and Comparative Law Quarterly*, vol. 55, 4, Oct. 2006, pp. 59–87.

“United States: Comments on the Draft Articles on State Responsibility.” *International Legal Materials*, vol. 37, 2, Mar. 1988, pp. 468–487.

Tsagourias, Nicholas, and Michael Farrell. “Cyber Attribution: Technical and Legal Approaches and Challenges.” *The European Journal of International Law*, vol. 31, 3, 2020, pp. 941–97.

Watts, Sean. “Low-Intensity Computer Network Attack and Self-Defense.” *International Law Studies*, vol. 87, Oct. 2010, pp. 59–87.

3. 政府刊行物

The French Ministry of Armed forces. *International Law Applied to Operations in Cyberspace*. 7, 2019. ttps://www.justsecurity.org/wp-content/uploads/2019/09/droit-internat-appliqu%C3%A9-aux-op%C3%A9rations-cyberespace-france.pdf.

The Federal Government of Germany. *On the Application of International Law in Cyberspace*. Mar. 2021, https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf.

U.K. Government. *The National Cyber Force: Responsible Cyber Power in Practice*. March 2023.

U.K. Ministry of Defence. *Allied Joint Doctrine for Cyberspace Operations (AJP-3.20)*. 2020,

https://www.gov.uk/government/publications/allied-joint-doctrine-for-cyberspace-operations-ajp-320.

U.S. Air Force. *Air Force Instruction 51-402 Legal Reviews of Weapons and Cyber Capabilities*. 27 July 2011, https://irp.fas.org/doddir/usaf/afi51-402.pdf.

U.S. Congressional Research Service. *Cybersecurity: Deterrence Policy*. 18 January 2022. https://crsreports.congress.gov/product/pdf/R/R47011.

U.S. Congress. *Statement of General Paul M. Nakasone commander United States cyberspace command Before the house committee on armed services subcommittee on intelligence and emerging threats and capabilities*. March 4, 2020. https://www.congress.gov/116/meeting/house/110592/witnesses/HHRG-116-AS26-Wstate-NakasoneP-20200304.pdf.

U.S. Cyber Command. *Achieve and Maintain Cyberspace Superiority Command Vision for US Cyber Command*. March 2018. https://nsarchive.gwu.edu/document/16477-united-states-cyber-command-achieve-and-maintain.

U.S. Cyberspace Solarium Commission. *Cyberspace Solarium Commission Official Report*. March 2020. https://www.solarium.gov/report. U.S. Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*. July 2011. https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace. pdf.

U.S. Cyberspace Solarium Commission. *Cyberspace Solarium Commission legislative proposal*s. March 2020. https://www.solarium.gov/report.

U.S. Department of Defense. *Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934*. November 2011. https://irp.fas.org/eprint/dod-cyber.pdf.

U.S. Department of Defense. *National Defense Strategy*. October 2022. https://media.defense.gov-/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF.

U.S. Government. *National Cybersecurity Strategy*. October 2022. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

U.S. Government. *Presidential Policy Directive/PPD-20*. October 16, 2012. https://irp.fas.org/offdocs/ppd/index.html.

U.S. Government, *National Cybersecurity Strategy*. March 1, 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

U.S. Joint Chiefs of Staff. *Joint Publication JP 3-0 Joint Operation.* August 2011. https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/.

U.S. Joint Chiefs of Staff. *Joint Publication JP 3-12 Cyberspace Operations*. June 2018. https://dl.acm.org/doi/book/10.5555/3285221.

U.S. National Intelligence Council. *Foreign Threats to the 2020 US Federal Elections*. 2021. https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.

U.S. National Intelligence Council. *Global Trends 2040*: *A More Contested World*. March 2021. https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040.pdf.

U.S. Senate Committee on Armed Services. *Posture statement of General Paul M. Nakasone commander United States cyberspace command Before the 118th Congress senate committee on armed services.* March 7, 2023. https://www.armed-services.senate.gov/.

4. Web サイト等

Center for Cyber and Homeland Security (CCHS). Into the Gray Zone: The Private Sector and Active, Center for Cyber and Homeland Security (CCHS), Oct. 2016, https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/CCHS-ActiveDefenseReportFINAL.pdf.

Chalfant, Morgan. "McCain Hits Trump over Lack of Cyber Policy." *The Hill*, 23 Aug. 2017, https://thehill.com/policy/cybersecurity/347660-mccain-hits-trump-over-lack-of-cyber-policy.

Cordey, Sean. "Cyber Influence Operations: An Overview and Comparative Analysis." Center for Security Studies (CSS) ETH Zürich, 2019, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-10-CyberInfluence.pdf. ETH Zürich.

Dormann, Knut. "Applicability of the Additional Protocols to Computer Network Attacks." *International Committee of the Red Cross*, 19 November. 2004, https://www.icrc.org/en/doc/resources/documents/misc/68lg92.htm.

Fischerkeller, Michael P., and Richard J. Harknett. "Initiative Persistence as the Central Approach for U.S. Cyber Strategy." *IDA*, the Institute for Defense Analysis, July 2021, https://ida.org//media/feature/publications/i/in/ initiative-persistence-as-the-central-approach-for-us-cyber-strategy/d-22719.ashx.

Fischerkeller, Michael P., and Richard J. Harknett. "Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace." *Lawfare*, The Lawfare Institut, 9 Nov. 2018, https://www.lawfareblog.com/ persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace#.

Haskell-Dowland, Paul. "Three Ways the 'NotPetya' Cyberattack Is More Complex than WannaCry." *The Conversation*, The Conversation, 30 June 2017, https://theconversation.com/three-ways-the-notpetya-cyberattack-is-more-complex-than-wannacry-80266.

Henderson, Ian, and Kate Reece. "Proportionality under International Humanitarian Law: The 'Reasonable Military Commander' Standard and Reverberating Effects." *Vanderbilt Journal of Transnational Law*, vol. 51, no. 3, 2018, pp. 835–855.

Hollis, David. "Cyberwar Case Study: Georgia 2008." *Small War Journal*, Small Wars Foundation, 1 June 2011, https://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008.

Human Rights Watch. "Ukraine: Respect the Rights of Prisoners of War." *Human Rights Watch*, 16 Mar. 2022, http://www.nytimes. com/2011/07/14/world/asia/14identity.html.

ICRC. "International Humanitarian Law and the Challenges of Contemporary Armed Conflicts

Challenges Report." *ICRC*, ICRC, 31 Oct. 2015, https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts.

International Institute for Strategic Studies (IISS). "Cyber Capabilities and National Power: A Net Assessment," June 28, 2021. https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.

Jewett, Rachel. "Viasat Details KA-SAT Cyberattack That Affected Thousands of Modems in Ukraine." *Via Satellite*, Via Satellite, 30 Mar. 2022, https://www.satellitetoday.com/cybersecurity/2022/03/30/viasat-details-ka-sat-cyberattack-that-affected-thousands-of-modems-in-ukraine/.

Korte, Gregory. "White House Plan to 'shame' North Korea Shows Complexities of Responding to Cyberattacks." *Usa Today*, Usa Today, 19 December. 2017, https://www.usatoday.com/story/news/politics/2017/12/19/white-house-strategy-punish-north-korea-wannacry-attack-were-going-shame-them/964116001/.

Lewis, James A,. "Cyber War and Ukraine." Center for Strategic and International Studies, CISI. 16 June 2022, https://www.csis.org/analysis/cyber-war-and-ukraine.

Lewis, James A,. "Strategy After Deterrence" Center for Strategic and International Studies. March 11, 2020. https://www.csis.org/analysis/strategy-after-deterrence.

Lewis, James A. "2023 U.S. Cyber Command Legal Conference Fireside Chat: Using Laws and Norms to Govern Cyber." *Dvids*, 19 Apr. 2023, https://www.dvidshub.et/feature/CYBERLEGAL2023.

Lyngaas, Sean. "White House announces federal cyber strategy, vows to go on offensive Cyberscoop." September 20, 2018. https://cyberscoop.com/white-house-cyber-strategy-john-bolton-announcement/.

Marks, Joseph. "Shoddy U.S. Cyber Deterrence Policy Emboldens Adversaries, LawmakersSay." Nextgov. March 2, 2017. https://www.nextgov.com/cybersecurity/2017/03/shoddy-us-cyber-deterrence-policy-emboldens-adversaries-lawmakers-say/135853/.

Melzer, Nils. "Interpretive Guidance on the Notion of Direct Participation in Hostilities under IHL." *ICRC*, ICRC, 1 July 2009, https://www.icrc.org/en/doc/resources/documents/publication/p0990.htm.

Microsoft. "Defending Ukraine: Early Lessons from the Cyber War." *Microsoft On the Issues*, Microsoft, 22 June 2022, https://blogs.microsoft.com/on-the-issues/.

Microsoft. "Special Report: Ukraine (27 April 2022." *Microsoft On the Issues*, Microsoft, 27 Apr. 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

Nakashima, Ellen. "White House Authorizes 'Offensive Cyber Operations' to Deter Foreign Adversaries." *The Washington Post*, The Washington Post, 20 Sept. 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.

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). “International Cyber Law: Interactive Toolkit.” https://cyberlaw.ccdcoe.org/wiki/Main_Page.

Newman, Lily Hay. “How an Accidental ‘Kill Switch’ Slowed Friday’s Massive Ransomware Attack.” *Wired*, Wired, 13 May 2017, https://www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/.

Patteson, Callie. “US Using Hack Attacks to Support Ukraine against Russia, General Says.” *New York Post*, New York Post, 1 June 2022, https://nypost.com/2022/06/01/us-supporting-ukraine-against-russia-with-cyber-attacks/.

Politico. “Full Transcript: President Obama’s Final End-of-Year Press Conference.” December 16, 2016. https://www.politico.com/story/2016/12/obama-press-conference-transcript-232763.

Schmitt, Michael N. “International Cyber Law Politicized: The UN GGE’s Failure to Advance Cyber Norms.” *Just Security*, Reiss Center on Law and Security, June 30, 2017. https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.

Schmitt, Michael N. “International Law and Cyber Warfare.” *C-SPAN*, 28 Mar. 2013, https://www.c-span.org/video/?311806-1/international-law-cyber-warfare.

Schmitt, Michael N. “Russian Cyber Operations and Ukraine: The Legal Framework.” *Articles of War*, The Lieber Institute for Law & Warfare at West Point, 16 Jan. 2022, https://lieber.westpoint.edu/russian-cyber-operations-ukraine-legal-framework/.

Shanker, Thom. “To Track Militants, U.S. Has System That Never Forgets a Face.” *The New York Times*, The New York Times, 11 July 2009, http://www.nytimes.com/2011/07/14/world/asia/14identity.html.

Soeasanto, Stefan. “The IT Army of Ukraine: Structure, Tasking, and Ecosystem.” *Center for Security Studies（CSS）*, ETH Zürich, June 2022, https://css.ethz.ch/en/Themes/Cybersecurity/all-publications/details.html?id=/t/h/e/i/the_it_army_of_ ukraine.

The Forge, “Grey Zone Activities and the ADF - A Peary GroupReport.” https://theforge.defence.gov.au/sites/default/files/2020-10/Grey%20Zone_0.pdf.

UK The Attorney General’s Office, Attorney General’s speech at the International Institute for Strategic Studies (11 January 2017). <https://www.gov.uk/government/speeches/attorney-generals-speech-at-the-international-institute-for-strategic-studies>

U.S. Cyber Command. “CYBER 101: Hunt Forward Operations” U.S. Cyber Command. November 15, 2022. https://www.cybercom.mil/Media/News/Article/3218642/cyber-101-hunt-forward-operations/

U.S. Department of the Treasury. “Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups,” July 13, 2019. https://home.treasury.gov/news/press-releases/sm774.

US Homeland Security. “Statement by Secretary Johnson on Cyber attack on Sony Pictures Entertainment. ” 19 December 2014. https://www.dhs.gov/news/2014/12/19/statement-secretary-johnson-cyber-attack-sony-pictures-entertainment.

Zilber, Ariel. “Elon Musk’s Starlink Satellites Helping Ukraine Drones Destroy Russian Tanks: Report.” *New York Post*, New York Post, 21 Mar. 2022, https://nypost.com/2022/03/21/elon-musks-starlink-satellites-helping-ukraine-drones-destroy-russian-tanks-report/.

5. 国連文書

U.N. Doc. A/RES/36/103 (9 December 1981)

U.N. Doc. A/C.1/53/L.17/Rev.1 (2 November 1998).

UN Doc. A/RES/56/10.

UN Doc. A/70/174 (22 July 2015).

U.N. Doc. A/76/135 (14 July 2021).

U.N. Doc. A/RES/73/27

U.N. Doc. A/AC.290/2021/CRP.2.

6. 国際裁判判例等

Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia Montenegro), Judgement, [2007] I.C.J Reports 43.

Case Concerning Military and Paramilitary Activities in and against Nicaragua, Merits, Judgement, [1986] I.C.J. Reports 14.

Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America), Merits, Judgement of 6 November 2003, [2003] I.C.J. Reports 161.

Corfu Channel case, Judgment of 9 April 1949, [1949] I.C.J. Reports 244.

Island of Palmas case (Netherlands v. USA), Award of 4 April 1928, [2006] Reports of International Arbitral Awards, Vol.II pp. 829-871.

Prosecutor v. Dusko Tadic, IT-94-1-A, ICTY, Appeals Chamber, Judgment of 15 July 1999.

The Case of the S.S. "LOTUS", Collections of Judgements, PCIJ, Series A, No. 10, (7 September 1927).

International Criminal Tribunal for the former Yugoslavia (ICTY), Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia (8 Jun 2000), para. 28, <https://www.icty.org/en/press/final-report-prosecutor-committee-established-review-nato-bombing-campaign-against-federal>

Ⅱ　日本語文献

1. 書　籍

芦部信喜・高橋和之補訂『憲法 第 8 版』（岩波書店、2023）

宇賀克也『行政法概説Ⅰ行政法総論』第７版（有斐閣、2020）
海野敦史「『「通信の秘密不可侵」の法理』（勁草書房、2015）
河野桂子「サイバー攻撃に対する自衛権の発動」江藤淳一編『国際法学の諸相 ： 到達点と展望:村瀬信也先生古稀記念』（信山社、2015）。
川口貴久「サイバー領域における安全保障の現状と課題－サイバー領域の抑止力と日米同盟－」『平成 25 年度外務省外交・安全保障調査研究事業（調査研究事業）「グローバル・コモンズ（サイバー領域、宇宙、北極海）における日米同盟の新しい課題」』（公益財団法人日本国際問題研究所､2013）。
川出敏裕『判例講座刑事訴訟法〔捜査・証拠編〕〔第２版〕』（立花書房、2021）。
川村博・上富敏伸・島田健一『概説サイバー犯罪』（青林書院、2018）
栗田真広「サイバー攻撃に対する「抑止」の現状 ―米国の安全保障政策の事例から―」『情報通信をめぐる諸課題・科学技術に関する調査プロジェクト調査報告書』（国立国会図書館、2014）。
黒崎将広ほか『防衛実務国際法』（弘文堂､2021）
杉原高嶺『国際法学講義[第２判]』（有斐閣、2013）
塩野宏『行政法Ⅰ〔第六判〕行政法総論』（有斐閣、2015）
曽我部真裕・林秀弥・栗田昌弘『情報法概説』第２版（弘文堂、2019 年）
田村正博『警察行政法解説』第２版補訂版（東京法令出版、2019）
田村重信『新・防衛法制』（内外出版、2018）
前田雅英『刑法総論講義』第７版（東京大学出版、2019）
鎮目征樹ほか『情報刑法Ⅰ - サイバーセキュリィティ関連犯罪』（弘文堂、2022）
宮内靖彦「自衛の発動要件にとっての非国家的行為体の意味－国際判例の観点からの分析－」村瀬信也編『自衛権の現代的展開』（東信堂，2007）153－158 頁
リチャード・クラーク、ロバート・ネイク（北川知子ほか訳）『核を超える脅威 世界サイバー戦争：見えない軍拡が始まった』（徳間書店、2011 ）

2. 学術誌

安保克也「行政機関と個人情報－自衛隊情報保全隊事件を題材に－」防衛法学会編『防衛法研究』第 43 号（2019）
安保克也「日本国憲法と安全保障-サイバー戦の視点から-」『憲法論叢』15 号 101-126 頁（2008）
稲角光恵「国際法上の犯罪に対する国家責任と個人責任と企業責任」金沢法学 57 巻 1 号 1-27 頁（2014）
猪又和奈「刑事国際法における構成要件の考察（上）－旧ユーゴスラヴィア国際刑事裁判所及びルワンダ国際刑事裁判所判例の国際刑事裁判所規程形成への影響－」一橋法学第 2 巻第 1 号（2003）
岩月直樹「現代国際法上の対抗措置制度における均衡性原則－国際紛争処理過程におけ

る対抗措置の必要性に照らしたその多元的把握の試み」立教法学第 78 号 206‐299 頁（2010）
岩本誠吾「サイバー問題における国際法の課題」外交 24 巻 88-91 頁（2014）
海野敦史「憲法上の通信の「秘密」の意義とその射程」情報通信学会誌第 32 巻 2 号（2014 年）
後瀉 桂太郎「抑止概念の変遷 ― 多層化と再定義 ―」海幹校戦略研究 5 巻 2 号 21-44 頁（2015）
岡山公法判例研究会「情報保全隊による情報収集・保存が違法とされた事例」岡山大学法学会編『岡山大学法学会雑誌』第 63 巻第 1 号（2013）
川口貴久「米国におけるサイバー抑止政策の刷新 : アトリビューションとレジリエンス米国におけるサイバー抑止策」KEIO SFC JOURNAL　15 巻 2 号 78-96 頁（2015）
久保田隆「自衛官による加害行為と刑法 35 条に基づく違法性阻却：防衛出動等における武力の行使を中心に」法学政治学論究第 120 号（2019）
熊取谷行他「日本と諸外国の防衛法制の比較研究」海幹校戦略研究第 11 巻第 1 号（2021)
佐々木孝博「サイバー空間の施策に関するロシアと欧米諸国のアプローチ」日本大学大学院総合社会情報研究科紀要 14 号 1-12 頁（2013)
宍戸常寿「通信の秘密について」企業と法創造第 9 巻第 3 号（2013）
曽我部真裕「通信の秘密の憲法解釈論」Nextcom 第 16 巻（2016 年）
高橋郁夫・吉田一雄「『通信の秘密』の数奇な運命（憲法)」情報ネットワークローレビュー第 5 号 （2006）
田川義博「インターネット利用における「通信の秘密」」情報セキュリティ総合科学第 5 号（2013）
福留俊幸「サイバー対抗措置の可能性と限界」防衛法研究第 40 号 39-58 頁（2016)。
丸橋透「プロバイダの捜査対応，ログ保存，被害抑止協力の実務と考え方」比較法雑誌第 49 巻第 4 号（2016）
宮崎弘毅「防衛二法と自衛隊の任務行動権限-1-」国防（1978）
宮崎弘毅「防衛二法と自衛隊の任務行動権限-3-」国防（1978）

3. 政府刊行物

外務省「サイバー行動に適用される国際法に関する日本政府の基本的な立場」（2021 年 5 月 28 日)。
サイバーセキュリティ戦略本部「サイバーセキュリティ戦略」（2021 年 9 月閣議決定)。
サイバーセキュリィティ戦略本部「重要インフラの情報セキュリティ対策に係る第 4 次行動計画」（2020.2.1 改定)。
防衛省「令和 4 年度版防衛白書」（2022）

防衛省「平成２２年度版防衛白書」（2010）
「国家安全保障戦略」（令和４年 12 月 16 日閣議決定）
「日米防衛協力のための指針」（2015 年 4 月 27 日）

4. Web サイト

川口貴久「国家が支援するランサムウェア：2017 年の WannaCry と NotPetya の意図に関する分析（前編)」国際情報ネットワーク分析 IINA・笹川平和財団（2021.3.19）
https://www.spf.org/iina/articles/kawa- guchi_02.html
川口貴久「ロシアによる政治介入型のサイバー活動～2016 年アメリカ大統領選挙介入の手法と意図～」国際情報ネットワーク分析 IINA・笹川平和財団（2020.3.30）
https://www.spf.org/iina/articles/kawaguchi_01.html
佐々木勇人「「積極的サイバー防御」（アクティブサイバーディフェンス）とは何か ―より具体的な議論に向けて必要な観点について―」JPCERT/CC Eyes (2022.9.21) JPCERT/CC https://blogs.jp cert.or.jp/ja/2022/09/active-cyber-defense.html
自由民主党「自民党サイバーセキュリティ対策本部：第一次提言～リスクの最小化に向けて。「コスト」から投資への意識改革を～」（2018.4.24）<https://www.jimin.jp/news/policy/137263.html>
高橋郁夫「続アクティブサイバーディフェンスの概念」（2022.9.19）株式会社 IT・リサーチアート https://itresearchart.biz/?p=4167
日本経済新聞「JAXA などにサイバー攻撃か　中国共産党員を書類送検」（2021.4.20）
https://www.nikkei.com/article/DGXZQOUE200CS0Q1A420C2000000/
日本経済新聞「『能動的サイバー防御』準備室、内閣官房に新設政府」（2023.1.31）
https://www.nikkei.com/article/DGXZQOUA3186D0R30C23A1000000/
原田有「複雑化するサイバー規範プロセスの動向」NIDS コメンタリー第 118 号、防衛研究所（2020 .6.2）
http://www.nids.mod.go.jp/publication/commentary/pdf/commentary118.pdf
情報セキュリィティ大学院「『インターネットと通信の秘密』研究会報告書：インターネット時代の「通信の秘密」再考」（キャノングローバルセキュリィティ研究所、2013 年）<https://cigs.canon/article/20130625_1964.html>
NHK サイバー取材班「日本政府が名指し 北朝鮮ハッカー「ラザルス」とは何者か？」NHK　NEWS WEB（2022.11.14）<https://www3.nhk.or.jp/news/html/20221114/k10013890-411000.html>
NHK「WEB 特集『見えてきたサイバー戦:ハイブリッド戦、ウクライナで激しい攻防』」NHK　NEWSWEB (2022.6.27) <https://www3.nhk.or.jp/news/html/20220627/k10013690111 00.html>.

5. 国会答弁

第 61 回国会参議院内閣委員会議録第 17 号有田喜一防衛庁長官答弁（1969.5.8）
第 77 回国会衆議院予算委員会義録第 18 号三木武夫内閣総理大臣答弁（1976.2.27）
第 143 回国会衆議院外務委員会議録第 4 号高村正彦外務大臣答弁（1998.9.18）
第 143 回国会衆議院外務委員会議録第 4 号東郷条約局長答弁（1998.9.18）
第 146 回衆議院国会安全保障委員会第 4 号瓦力防衛庁長官答弁（1999.11.18）
第 154 回国会衆議院武力攻撃事態への対処に関する特別委員会議録第三号中谷元防衛庁長官答弁（2002.5.7）
第 154 回国会・衆議院武力攻撃事態への対処に関する特別委員会議録第五号中谷元防衛庁長官発言（2002.5.9）
第 186 回国会衆議院予算委員会議録 16 号小野寺五典防衛大臣答弁（2014.5.28）
第 201 回国会衆議院安全保障委員会第 4 号河野国務大臣答弁（2020.4.7）
第 201 回国会参議院外交防衛委員会会議録第 9 号槌道明宏防衛省防衛政策局長答弁（2020.4.16）
第 208 回国会衆議院内閣委員会議録第 5 号緒方林太郎委員答弁（2022.3.2)
内閣衆質 189 第 71 号「衆議院議員緒方林太郎君提出サイバー攻撃と自衛権との関係に関する質問に対する答弁書」（2015.2.24）
内閣衆質 201 第 9 号「衆議院議員櫻井周君提出自衛隊の中東海域への派遣の法的根拠に関する質問に対する答弁書令」（2020.1.31）

6. 判　例

最判昭和 53 年 9 月 7 日刑集 32 巻 6 号 1672 頁
最大判昭 53 年 10 月 4 民集第 32 巻 7 号 1223 頁
東京地判昭和 59 年 6 月 28 日判例時報 1126 号 3 貢
最決平成 11 年 12 月 16 日刑集 53 巻 9 号 1327 頁
仙台地判平成 24 年 3 月 26 日判例時報 2149 号 99 頁
東京地判平成 26 年 1 月 15 日判例時報 2215 号 30 頁
東京高判平成 27 年 4 月 14 日／平成 26 年（ネ）1619 号
仙台高判平成 28 年 2 月 2 日判例時報 2293 号 18 頁
最大判平成 29 年 3 月 15 日刑集 71 巻 3 号 13 頁
岐阜地判令和 4 年 2 月 21 日判例時報 2548 号 60 頁