参議院常任委員会調査室・特別調査室

論題	サイバー攻撃の脅威とサイバー安全保障 －能動的サイバー防御の制度構築に向けた課題－
著者 / 所属	森　　秀勲 / 第一特別調査室
雑誌名 / ISSN	立法と調査 / 0915-1338
編集・発行	参議院事務局企画調整室
通号	462 号
刊行日	2023-12-18
頁	114-129
URL	https://www.sangiin.go.jp/japanese/annai/chousa/rippou_chousa/backnumber/20231218.html

サイバー攻撃の脅威とサイバー安全保障

― 能動的サイバー防御の制度構築に向けた課題 ―

森　秀勲
（第一特別調査室）

１．はじめに[1]

2022（令和４）年12月、政府は、新たな「国家安全保障戦略」を閣議決定した[2]。同戦略では、現在の安全保障環境について、「軍事と非軍事、有事と平時の境目が曖昧になり、ハイブリッド戦が展開され、グレーゾーン事態が恒常的に生起している」との認識を示した上で、国や重要インフラ等の安全等を確保するために、「サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させる」との方針を掲げた。また、具体的な方策として、重大なサイバー攻撃を未然に排除し、被害の拡大を防止するために「能動的サイバー防御」の導入をうたった（同戦略21頁）。

2023（令和５）年１月31日、内閣官房にサイバー安全保障体制整備準備室が設置され、能動的サイバー防御に必要な措置の実施や、サイバー安全保障分野の政策を一元的に総合調整する司令塔となる新たな組織の立ち上げ、それらに必要となる法整備等について検討が進められている。報道によると、内閣サイバーセキュリティセンターを改組してサイバー

[1] 本稿は、令和５年11月28日脱稿時の情報（インターネットを含む。）に基づく。本文中における年号の表記は西暦を基本とし、日本の事柄については和暦を併記する。ただし、引用する文書、文献等の年号は、参照の便宜のため、原則として当該文書等における表記に従うものとする。
[2] 「国家安全保障戦略について」（令和４年12月16日国家安全保障会議決定・閣議決定）

安全保障分野の司令塔とし、自衛隊や警察庁を統括するとされる[3]。

本稿では、サイバー安全保障[4]に関して、サイバー空間における安全保障上の脅威と安全保障上の懸念を生じさせるサイバー攻撃の事例、我が国及び主要国におけるサイバー安全保障体制、能動的サイバー防御をめぐる課題について整理する。

２．サイバー脅威の現状

（１）サイバー空間における安全保障上の脅威

サイバー空間上の情報資産やネットワークを侵害するサイバー攻撃は、社会に深刻な影響を及ぼす可能性があり、安全保障にとって現実の脅威となっている[5]。サイバー攻撃の種類としては、不正アクセス、マルウェア（不正プログラム）による情報流出や機能妨害、情報の改ざん・窃取、大量のデータの同時送信（ＤＤｏＳ攻撃など）[6]による機能妨害のほか、電力システムや医療システムなど重要インフラのシステムダウンや乗っ取りなどが挙げられる。サイバー攻撃の対象は、各国の政府機関や軍隊のみならず民間企業や学術機関などにも広がっており、重要技術、機密情報、個人情報などが標的となる事例も確認されている。サイバー攻撃は、攻撃主体の特定や被害の把握が容易ではないことから、敵の軍事活動を低コストで妨害可能な非対称的な攻撃手段として認識されており、多くの外国軍隊がサイバー攻撃能力を開発しているとみられている。例えば、中国は、人民解放軍（戦略支援部隊）及び国家安全部、これらの組織から委託を受けた企業、サイバー犯罪者等が中心となって、平素から機密情報の窃取を目的としたサイバー攻撃などを行っていると見られている[7]。ロシアについては、軍参謀本部情報総局、連邦保安庁、対外情報庁がサイバー攻撃に関与しているとの指摘があるほか、軍のサイバー部隊の存在が明らかとなっている。また、北朝鮮には、偵察総局、国家保衛省、朝鮮労働党統一戦線部及び文化交流局の四つの主要な情報機関並びに対外情報機関が存在しており、情報収集の主たる標的は韓国、米国及び我が国であるとされる。

---

[3] 「自衛隊、民間企業をサイバー防護　防衛産業など対象、機密情報の流出防ぐ　24年にも制度」『日本経済新聞』(2022.12.31)。政府は新たに有識者会議を設置して法的な課題の精査などを行い、来年の通常国会に必要な改正案の提出を目指す見通しとされていた（山下毅「「能動的サイバー防御」導入へ　背景と課題」(2023年８月17日ＮＨＫ解説委員室）<https://www.nhk.or.jp/kaisetsu-blog/100/486718.html>)。しかし、本稿執筆時点で、有識者会議は設置されておらず、政府・与党で公式な議論が始まっていない（「サイバー法整備、先送り論が浮上　24年通常国会提出へ議論始まらず」『日本経済新聞』(2023.11.24))。

[4] 「国家安全保障戦略」では「サイバー安全保障」について別段の説明はない。他方、同戦略の英語版では「サイバー安全保障」の訳として日本語の「サイバーセキュリティ」と同じ“cybersecurity”が用いられている。本稿では、暫定的に、「サイバー安全保障」を、安全保障の側面から見たサイバーセキュリティないしサイバーセキュリティを通じた安全保障の確保と捉えておくこととする。

[5] 以下、防衛省『令和５年版防衛白書』（令5.7）175～177頁を参照して記述。

[6] 特定のコンピュータに大量のデータを送信して負荷をかけるなどして、そのコンピュータによるサービスの提供を不可能にする「ＤｏＳ攻撃」、複数のコンピュータから一斉にＤｏＳ攻撃を行う「ＤＤｏＳ攻撃」(″Distributed Denial of Service″の略）が知られている。

[7] 例えば、2021年７月、米英政府などは、「ＡＰＴ40」と呼ばれる中国サイバー脅威主体がサイバー空間の安全等を脅かしているとする声明を発表。我が国政府（外務省報道官談話）も、「ＡＰＴ40」は中国政府を背景に持つものである可能性が高いと指摘している（公安調査庁「サイバー空間における脅威の概況2023」10頁<https://www.moj.go.jp/content/001396422.pdf>、「中国政府を背景に持つＡＰＴ40といわれるサイバー攻撃グループによるサイバー攻撃等について」（令和３年７月19日外務報道官談話）<https://www.mofa.go.jp/mofaj/press/danwa/page6_000583.html>)。

（２）安全保障上の懸念を生じさせるサイバー攻撃の事例

安全保障上の懸念を生じさせるサイバー攻撃の事例として、ここでは、米国における重要インフラに対するサイバー攻撃事案、中国軍による我が国の防衛関連システムへの侵入に係る報道の二つを紹介する。

ア　重要インフラに対するサイバー攻撃（コロニアル・パイプライン事案）

安全保障上の懸念を生じさせる重要インフラに対するサイバー攻撃の事例としては、2021年５月に米国のコロニアル・パイプライン社（以下「ＣＰ社」という。）がランサムウェアによるサイバー攻撃[8]を受けた事案が挙げられる[9]。同年５月７日、石油パイプライン事業最大手のＣＰ社は、ランサムウェア攻撃を受け、パイプラインの操業を停止した。ＣＰ社のパイプラインはテキサス州からニュージャージー州に及ぶ石油供給の45％を担う大動脈であり、米国東部の燃料不足が懸念される事態となった。

５月10日、連邦捜査局（ＦＢＩ）はRaaS（Ransomware as a Service：顧客である犯罪者にランサムウェア攻撃の手段を提供）をビジネスとする東欧系ハッカー集団DarkSideによる攻撃であることを確認した。本事案で名指しされたDarkSideは、「攻撃の目的は金銭であり政治的混乱を起こす意図はない」とする声明を発表した。ロシアの関与の証拠はないとされたが、バイデン米国大統領は「ロシアが一定の責任を負う」とコメントした。

５月11日、ＦＢＩとサイバーセキュリティ・インフラセキュリティ庁（ＣＩＳＡ）は更なるランサムウェア攻撃への対処について注意喚起を行った。ＣＰ社は停止したパイプラインの再稼働を12日から始めるとし、フル稼働までには時間がかかるとしたものの、燃料不足の懸念はひとまず沈静化した。このコロニアル・パイプライン事案により、攻撃主体が非国家・金銭目的であっても、重要インフラの防御が脆弱であれば、被害の影響が深刻なものとなり得ることが露呈することとなった。５月12日、バイデン政権は、2020年末から米国で相次いで発生したサイバー事案[10]を受けて、サイバーセキュリティに関する大統領令[11]に署名したが、図らずもコロニアル・パイプライン事案が発生した直後のタイミングとなった。

重要インフラの脆弱性を突いたサイバー攻撃の可能性は、米国において今もなお重大な脅威として捉えられている。2023年５月25日、米国国務省のミラー報道官は記者会見

---

[8] データを暗号化するなどして使用不能にし、その復元等の対価として金銭を要求するサイバー攻撃。

[9] 以下、コロニアル・パイプライン事案については、独立行政法人情報処理推進機構（ＩＰＡ）『情報セキュリティ白書2021』（2021.7）105～106頁、「米燃料パイプライン停止の影響広がる、全面復旧にはなお時間」『ビジネス短信』（ジェトロウェブサイト、2021.5.14）〈https://www.jetro.go.jp/biznews/2021/05/8855e399f1f07274.html〉を参照して記述。

[10] SolarWinds事案では、2020年12月に発覚した連邦政府機関及びフォーチュン500に掲載される企業等を一斉に狙った過去最大規模のサプライチェーン攻撃があった。また、Microsoft Exchange事案では、2021年３月、Exchangeサーバ上でリモートコード実行が可能になる脆弱性を突いた攻撃によりパッチ未適用のExchangeサーバを持つ米国の中小企業、自治体、学校等少なくとも３万の組織がメール通信を窃取された可能性があるとされた（『情報セキュリティ白書2021』（前掲注９）104～105頁）。

[11] 政府と契約する情報通信サービス企業との間で、サイバーセキュリティ分野での官民連携を深めることを内容とする（「バイデン米大統領、サイバーセキュリティを強化する大統領令に署名」『ビジネス短信』（ジェトロウェブサイト、2021.5.14）〈https://www.jetro.go.jp/biznews/2021/05/35e8aca1614f6fe5.html〉）。

において、米国情報機関は、中国がほぼ確実に、米国内の石油・ガスパイプラインや鉄道システム等、重要インフラサービスを混乱させるサイバー攻撃を行う能力があると評価している旨発言している[12]。また、同年７月29日、米紙ニューヨークタイムズは、中国が台湾に対する行動等の際に米軍の配備や補給活動を妨害したり、遅らせたりするため、米国の重要インフラにマルウェアを広範に仕掛けており、米国政府がこうした中国製マルウェアの除去に乗り出すと報じている[13]。

なお、ランサムウェア攻撃は我が国でも多数発生しており、自動車関連企業とその海外拠点、医療機関に対する攻撃が相次いだ[14]。2023（令和５）年７月４日には、名古屋港の五つのコンテナターミナル及び集中管理ゲートで運用されている名古屋港統一ターミナルシステム（ＮＵＴＳ）がランサムウェア攻撃を受けて停止し、約３日間にわたり名古屋港のコンテナの搬入・搬出が止まるなど物流に大きな影響を及ぼすこととなった。本事案は、我が国の港湾施設に対する初めての大規模なサイバー攻撃となった[15]。現在、港湾は、サイバーセキュリティ基本法に基づく重要インフラ[16]や経済安全保障推進法[17]に基づく基幹インフラとしては位置付けられていない。この点について、斉藤国土交通大臣は、港湾機能の安定的な確保に向けて、サイバーセキュリティ基本法と経済安全保障推進法の法令上の位置付けに港湾を追加するかも含めて、関係省庁等と連携し、有識者会議等での議論を含め必要な対応を検討していく旨述べている[18]。

イ　中国軍のハッカーが防衛機密を扱うシステムに侵入したとする報道

2023（令和５）年８月７日、米紙ワシントンポストは、中国人民解放軍のハッカーが日本政府の防衛機密を扱うシステムに侵入していたことを、2020（令和２）年秋に米国国家安全保障局（ＮＳＡ）が発見していたと報じた[19]。ブリーフィングを受けた米国陸軍

---

[12] 米国国務省ウェブサイト "Department Press Briefing - May 25, 2023" <https://www.state.gov/briefings/department-press-briefing-may-25-2023/>、内閣サイバーセキュリティセンター「重要インフラを取り巻く情勢について」（令5.9.7）４頁<https://www.nisc.go.jp/pdf/council/cs/ciip/dai34/34shiryou03.pdf>

[13] David E. Sanger and Julian E. Barnes, "U.S. Hunts Chinese Malware That Could Disrupt American Military Operations," New York Times, July 29, 2023 <https://www.nytimes.com/2023/07/29/us/politics/china-malware-us-military-bases-taiwan.html>;「中国　米インフラも標的　「広範囲にマルウェア」」『読売新聞』(2023.8.9)、「中国からのサイバー攻撃　米、インフラ侵入警戒」『日本経済新聞』(2023.8.10)

[14] 「サイバー空間における脅威の概況2023」（前掲注７）４頁

[15] 国土交通省「コンテナターミナルにおける情報セキュリティ対策等検討委員会中間取りまとめ① 名古屋港のコンテナターミナルにおけるシステム障害を踏まえ緊急に実施すべき対応策について」（第２回コンテナターミナルにおける情報セキュリティ対策等検討委員会（令和５年９月29日）で公表）１頁<https://www.mlit.go.jp/kowan/content/001633393.pdf>

[16] 本稿３.（１）を参照

[17] 本稿３.（２）を参照

[18] 国土交通省ウェブサイト「斉藤大臣会見要旨」(2023.7.18) <https://www.mlit.go.jp/report/interview/daijin230718.html#gm3>。基幹インフラに指定されれば事業者はシステムなど設備を新しく導入する際に国の事前審査を受ける必要があるなど負担も生じるため、脅威の切迫度と事業者等の負担のバランスをいかに図るかという点も課題となろう。ＮＵＴＳの事案を含め、港湾施設に対するサイバー攻撃への対応については、山越伸浩「インフラ分野に関する安全保障上の課題－国土交通分野を中心とした一考察－」『立法と調査』No.461（2023.11）104～107頁に詳しい。

[19] Ellen Nakashima, "China hacked Japan's sensitive defense networks, officials say," Washington Post, August 7, 2023 (Updated August 8, 2023) <https://www.washingtonpost.com/national-security/2023/08/07/china-japan-hack-pentagon/>;以下、同記事を参照して記述。同記事については、2023年８月９

高官の一人によると、このハッキングは「衝撃的なほどひどいものだった」という。ナカソネＮＳＡ長官兼サイバー軍司令官らが来日し、日本政府に「日本の近代史で最も大きな被害を与えるハッキングだ」と警告したものの、バイデン政権が発足した2021（令和３）年初めの段階で、中国がまだ日本政府のネットワークに入り込んでいることが判明したとされる。オースティン米国国防長官は、日本側に「日本のネットワークの安全性が強化されなければ、高度な軍事作戦を可能とするデータ共有の強化が遅延する可能性がある」と示唆したという。米国サイバー軍は、日本のネットワークから中国のマルウェアを除去するため、ウクライナなどにも派遣している「前方追跡（hunt forward）」チームの派遣を申し出たが、日本側が自国のネットワークに外国軍が入り込むことに抵抗感を持ったため、結局、日本側が国内の事業者を使って脆弱性の評価を行い、ＮＳＡ・サイバー軍の共同チームがその評価結果を精査するという形に落ち着いた。2021年秋の段階で中国の侵入が依然として防げていなかったことから、同年11月、米国国家安全保障会議（ＮＳＣ）でサイバーセキュリティを担当するノイバーガー氏が来日して日本政府関係者と協議を行ったが、米国側は情報源と手法を守るため、どうやって中国の侵入を見つけたのかを明示的に示すことができなかったことから、日本側に疑念が残ったとされる。

中国軍のシステム侵入に関する報道について、浜田防衛大臣（当時）は、令和５年８月８日の記者会見で、「我が国と米国は平素から様々なレベルで緊密にやり取りしており、その詳細については事柄の性質上お答えを差し控える。サイバー攻撃により、防衛省が保有する秘密情報が漏洩したとの事実は確認していない。」と述べた[20]。

本報道が事実であれば、日本政府の中でも最も堅牢であるはずの防衛機密を含むシステムの脆弱性がさらされたことになり、同盟国や日本と緊密な関係にある各国の信頼を失うことも懸念され、サイバー対策の強化を急ぐべきとの論説も見られた[21]。

３．現行の我が国のサイバー安全保障体制

サイバーセキュリティに関する国の体制のうち安全保障に関連する主な制度・組織について簡単に紹介する。

（１）サイバーセキュリティ基本法に基づくサイバーセキュリティ政策推進体制

増大するサイバーセキュリティに対する脅威に対応するため、2014（平成26）年11月、サイバーセキュリティに関する施策を総合的かつ効果的に推進することを目的とした「サイバーセキュリティ基本法」（平成26年法律第104号）が成立した[22]。同法に基づき、2015（平成27）年１月には、内閣にサイバーセキュリティ戦略本部が、内閣官房に内閣サイバーセキュリティセンター（ＮＩＳＣ）が設置され、サイバーセキュリティに係る政策の企画・

日～10日新聞各紙で報道。

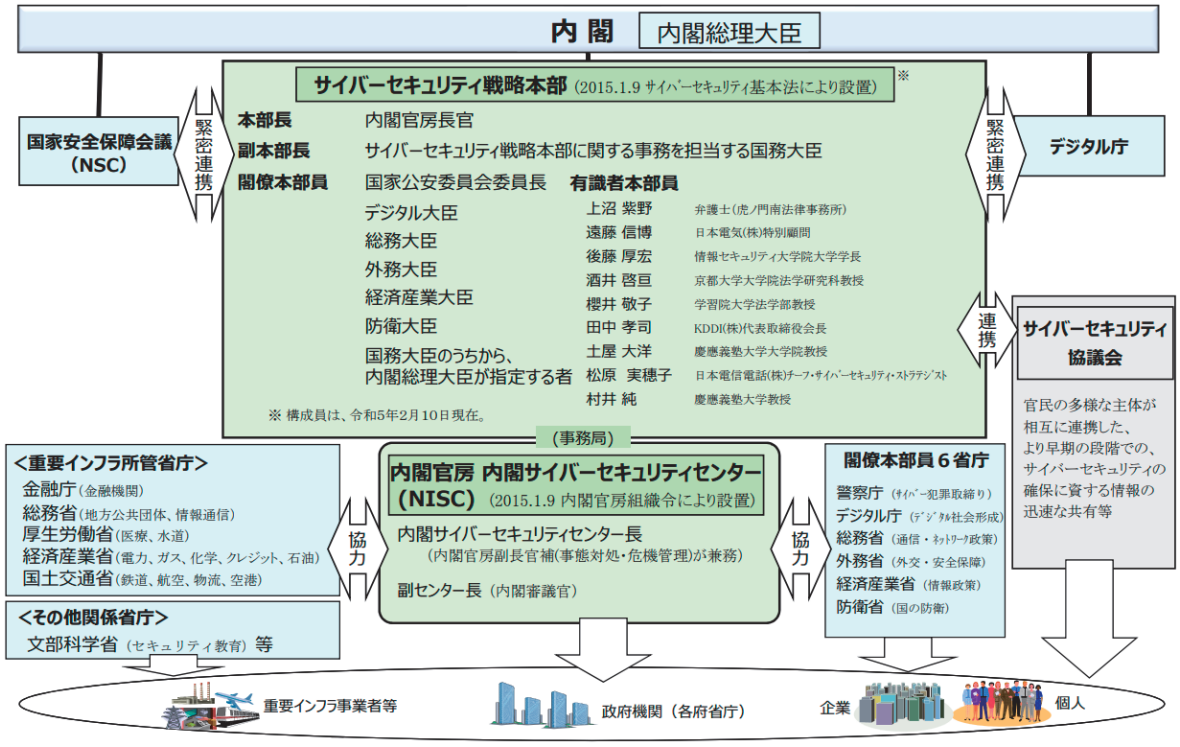
[20] 防衛省ウェブサイト「防衛大臣記者会見」（令5.8.8）〈https://www.mod.go.jp/j/press/kisha/2023/0808a.html〉

[21] 「防衛機密侵入　日本の信頼を揺るがす事態だ」『読売新聞』社説（2023.8.10）

[22] 以下、『令和５年版防衛白書』（前掲注５）297頁を参照して記述。

立案・推進と、政府機関、重要インフラ[23]などにおける重大なサイバーセキュリティインシデント対策・対応の司令塔機能を担っている。さらに、平成30年の同法改正[24]で、官民を含めた多様な主体が情報を迅速に共有することにより、サイバー攻撃による被害及びその拡大を防ぐことを目的とした「サイバーセキュリティ協議会」が創設された（図表１参照）。

図表１　我が国におけるサイバーセキュリティ政策推進体制



（出所）内閣サイバーセキュリティセンターウェブサイト

（２）経済安全保障推進法第３章に基づく基幹インフラ役務の安定的な提供の確保[25]

「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律」（令和４年法律第43号。経済安全保障推進法）のうち基幹インフラ役務の安定的な提供の確保に関する制度（第３章）は、基幹インフラの重要設備が我が国の外部から行われる役務の安定的な提供を妨害する行為（サイバー攻撃等）の手段として使用されることを防止するため、特定社会基盤事業者[26]による重要設備の導入・維持管理等の委託に当たって、各インフラの

---

[23] 重要インフラを担う「重要社会基盤事業者」は、国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものに関する事業を行う者と規定されている（同法第３条）。さらに、「重要インフラのサイバーセキュリティに係る行動計画」（2022年６月17日サイバーセキュリティ戦略本部）別紙１「対象となる重要インフラ事業者等と重要システム例」に、情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット、石油の計14分野の重要インフラ分野が掲げられている。

[24] サイバーセキュリティ基本法の一部を改正する法律（平成30年法律第91号）

[25] 以下、「ＩＣＴサイバーセキュリティ総合対策2023」（2023年８月総務省サイバーセキュリティタスクフォース）５～６頁<https://www.soumu.go.jp/main_content/000895981.pdf>を参照して記述。

[26] 同法第50条第１項では、基幹インフラを担う「特定社会基盤事業者」は、同項各号に定める14の事業（電気、

所管省庁による事前審査や勧告・命令等の措置を規定している[27]。

2023（令和５）年４月、同法に基づき「特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する基本方針」が閣議決定された。同法では通信・放送を含む基幹インフラ14分野が規定されており、同基本方針において、①規制対象となる事業者等を定める際には、事業者の負担に配慮しつつ規制対象を適切に定めていくこと、②近年サイバー空間においては、特に国家の関与が疑われるサイバー活動も行われるものとみられており、国民生活及び経済活動の基盤となる役務の安定的な提供が妨害され、社会的に大きな混乱が生ずる事案も発生している中で、我が国の外部にある主体から強い影響を受けている事業者からの設備の導入等について慎重な審査を行う必要があるなど、サイバーセキュリティの観点を含め、審査に当たって考慮する要素などが定められている。今後、2024（令和６）年春頃の制度運用開始に向けて、特定社会基盤事業者の指定基準、特定重要設備等を定める政省令の策定などの準備が順次進められている[28]。

（３）防衛省・自衛隊

防衛省・自衛隊は、サイバー防衛隊を隷下に有する自衛隊指揮通信システム隊の体制を見直し、2022（令和４）年３月17日、陸海空自衛隊の共同の部隊として、「自衛隊サイバー防衛隊」を新編した。この部隊の新編により、従来保有していたサイバー防護機能に加え、実戦的な訓練環境を用いて自衛隊のサイバー関連部隊に対する訓練の企画や評価といった訓練支援を行う機能を整備するとともに、隊本部の体制強化を図るほか、より効果的・効率的にサイバー防護が行えるよう、陸海空自衛隊のサイバー部隊が保有するサイバー防護機能を同隊へ一元化するなど、陸海空を統合した体制強化も図った。任務としては、主にサイバー攻撃などへの対処を行うとともに、防衛省・自衛隊の共通ネットワークである防衛情報通信基盤（ＤＩＩ）の管理・運用などを担っている[29]。

現在、防衛省・自衛隊は、おおむね10年後までに、サイバー攻撃を受けている状況下においても、指揮統制能力及び戦力発揮能力を保全し、自衛隊の任務遂行を保証できる態勢を確立しつつ、自衛隊以外へのサイバーセキュリティを支援できる態勢を強化するとしている。また、我が国へのサイバー攻撃に用いられる相手方のサイバー空間の利用を妨げる

ガス、石油、水道、鉄道、貨物自動車運送、外航貨物、航空、空港、電気通信、放送、郵便、金融、クレジットカード）から政令で絞り込んだ対象分野のうち、国民生活及び経済活動の基盤となる役務であって、その安定的な提供に支障が生じた場合に国家及び国民の安全を損なう事態を生ずるおそれがあるものの提供を行う者と規定されている。

[27] 本制度によって防止を図る「特定妨害行為」の具体的内容については、小林経済安全保障担当大臣（当時）は、「外国政府などが特定重要設備の供給者からその設備の脆弱性に関する情報の提供を受けて、その脆弱性を利用してウイルスに感染させることや、外国政府などの指示を受けて、特定重要設備の供給者がその設備にあらかじめ不正プログラムを埋め込んで、そのプログラムによって設備を停止させること、重要維持管理などの委託を受けた者が外国政府などの指示を受けて、その委託を受けた重要維持管理などの業務を放棄することで設備の機能を失わせることを想定している」旨答弁した（第208回国会衆議院内閣委員会議録第12号36頁（令4.3.25））。

[28] 経済安全保障推進法の施行状況については、内閣府ウェブサイト「経済安全保障」<https://www.cao.go.jp/keizai_anzen_hosho/>、柿沼重志・小林惇「経済安全保障推進法制定後の動きと今後の課題－経済的威圧に対抗するための体制構築に向けて－」『立法と調査』No.461（2023.11）３～18頁を参照。

[29] 防衛省『令和４年版防衛白書』（令4.7）207頁

能力の構築に係る取組を強化するとし、これらの取組を行う組織全体としての能力を強化するため、2027（令和９）年度を目途に、自衛隊サイバー防衛隊などのサイバー関連部隊を約4,000人に拡充し、さらに、サイバー関連部隊の要員と合わせて防衛省・自衛隊のサイバー要員を約２万人体制とし、将来的には、更なる体制拡充を目指すとしている[30]。

（４）警察

警察では、サイバー事案への対処能力の強化を図るため、警察法等の改正[31]により、2022（令和４）年４月、警察庁にサイバー警察局、関東管区警察局にサイバー特別捜査隊が新設された。サイバー特別捜査隊は、重大サイバー事案への対処を担う国の捜査機関として、外国捜査機関等との強固な信頼関係を構築し、サイバー攻撃集団により国境を越えて敢行されるサイバー事案等に対処すべく、国際共同捜査に積極的に参画することとしている[32]。

また、警察庁の令和６年度概算要求では、新たなサイバー脅威に先制的かつ能動的に対処するため、増員や捜査や情報技術解析用の資機材など、人的・物的基盤の強化を図る予算要求がなされている[33]。組織改正ではサイバー特別捜査隊を「サイバー特別捜査部」に格上げするとともに、サイバー関連部門全体で約35人増員し、うち一部を同特別捜査部に配置し約300人の態勢を敷くとの方針が報じられている[34]。

４．主要国におけるサイバー安全保障体制

（１）米国

米国では、サイバーセキュリティや重要インフラのセキュリティ政策は、国防総省、国土安全保障省、司法省で分担して行われている。2018年11月に制定された法律により、国土安全保障省に設置されていた国家防護プログラム局（ＮＰＰＤ）がサイバーセキュリティ・インフラセキュリティ庁（Cybersecurity and Infrastructure Security Agency：ＣＩＳＡ）に改組され、同省の連邦緊急事態管理庁（ＦＥＭＡ）、沿岸警備隊、シークレットサービスなどと並ぶ独立性の高い組織となった[35]。

ＣＩＳＡは、連邦政府のネットワークの防護、主要インフラの防護の調整、官民の調整等の機能を果たすため、2018年の発足時には既に3,400名弱の人員を擁し、下部組織として、サイバーセキュリティ部、インフラセキュリティ部、緊急コミュニケーション部、国家リ

---

30 『令和５年版防衛白書』（前掲注５）298～299頁

31 令和４年法律第６号。警察庁ウェブサイト「警察法の一部を改正する法律案（概要）」<https://www.npa.go.jp/laws/kokkai/220128/05_gaiyou.pdf>を参照。

32 関東管区警察局ウェブサイト「サイバー特別捜査隊」<https://www.kanto.npa.go.jp/about/syoukai10.html>。外国当局との連携は、捜査機関以外のサイバーセキュリティ関連機関も含めて行われている。例えば、2023（令和５）年９月、警察庁及びＮＩＳＣは、米国のＮＳＡ、ＦＢＩ及びＣＩＳＡと連携して、中国を背景とするサイバー攻撃グループ「BlackTech」（ブラックテック）によるサイバー攻撃に関する合同の注意喚起を発出している（「中国を背景とするサイバー攻撃グループBlackTechによるサイバー攻撃について」（令和５年９月27日警察庁・内閣サイバーセキュリティセンター）<https://www.npa.go.jp/bureau/cyber/pdf/20230927press.pdf>）。

33 警察庁「令和６年度予算概算要求の概要」11頁

34 「警察庁、サイバー特捜隊強化　「部」に昇格、人員・機材拡充」『日本経済新聞』（2023.8.31）

35 廣瀬淳子「【アメリカ】サイバーセキュリティー・インフラセキュリティー庁設置」『外国の立法』No.278-2（2019.2）６頁

スク管理部等を有している。ＣＩＳＡは、重要インフラ情報法（2002年）に基づき民間部門から任意の情報提供を受けるとともに、その情報システムを直接監視し、連邦政府各機関や民間組織と協調・協力してサイバー攻撃から非政府民間部門の重要インフラを防護している。ＣＩＳＡは、サイバー軍による作戦活動に達しない水準で、保有する能力を駆使して積極防衛を行っていると推定されている（ただし、ＣＩＳＡ自身は捜査等を行う法執行部門を持っていない。）[36]。また、ＣＩＳＡによって創設された共同サイバー防衛連携（Joint Cyber Defense Collaborative：ＪＣＤＣ）を通じて、政府機関や民間企業のネットワーク・オペレーターとの情報共有や調整が行われている[37]。

他方、米軍においては、2018年５月に統合軍に格上げされたサイバー軍（Cyber Command）が、サイバー空間における作戦を統括している[38]。同軍は、国防総省の情報環境を運用・防衛する「サイバー防護部隊」、国家レベルの脅威から米国の防衛を支援する「サイバー国家任務部隊」及び統合軍が行う作戦をサイバー面から支援する「サイバー戦闘任務部隊」などから構成されている。これら３部隊は「サイバー任務部隊」と総称され、25の支援チームを含め全体として133チーム、6,200人規模である[39]。サイバー軍の司令官は、国防省傘下の情報機関である国家安全保障局（ＮＳＡ）の長官が兼任しており、サイバー軍の本部もメリーランド州フォート・ミードにあるＮＳＡ本部に置かれている[40]。

大統領府においては、2021年１月にサイバー・先端技術担当国家安全保障副補佐官のポストが新設された。また、2021年度国防授権法により大統領府において大統領に対してサイバーセキュリティ政策及び戦略に関して助言を行う国家サイバー長官職が創設された[41]。

（２）英国

英国では、政府は、2016年10月の「国家サイバーセキュリティ戦略2016」に即して、シギント（ＳＩＧＩＮＴ：通信・電波傍受による情報活動）を扱う情報機関である政府通信本部（ＧＣＨＱ）の傘下に、新たに国家サイバーセキュリティセンター（ＮＣＳＣ）を設立した。民間や諸外国のカウンターパートと対外的な活動を行う既存のサイバー関連組織の機能を一本化し、サイバーセキュリティに関して政府として統一した助言、指針、支援、

---

[36] 松村昌廣「我が国のサイバーセキュリティ戦略の欠点と展望―「平和国家」体制の桎梏への対応を考える」『情報通信政策研究』５巻２号（2022年）Ⅲ-15～16頁

[37] 「個別調査分析２ サイバーセキュリティ領域」国立大学法人政策研究大学院大学政策研究院『「我が国が戦略的に育てるべき安全・安心の確保に係る重要技術等の検討業務」報告書』（令5.3）９～10頁<https://www8.cao.go.jp/cstp/stmain/pdf/20230314thinktank/seikabutsu/shiryou3-1-01.pdf>（同報告書は、内閣府の令和４年度科学技術振興調査等委託事業委託費による委託業務の成果を取りまとめたもの）。ＣＩＳＡウェブサイトのJoint Cyber Defense Collaborative関連ページ<https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative>

[38] 米軍の運用は、軍種ごとではなく、軍種横断的に編成された統合軍（Unified Combatant Command）の指揮のもとで行われており、統合軍は、機能によって編成された４機能統合軍（サイバー軍はこれに該当）と、地域によって編成された７地域統合軍から構成されている（『令和５年版防衛白書』（前掲注５）53～54頁）。

[39] 『令和５年版防衛白書』（前掲注５）177～178頁

[40] 山﨑治「自衛隊、米国軍等のサイバー攻撃対処能力の強化」『レファレンス』832号（2020.5）18頁

[41] 防衛省『令和３年版防衛白書』143頁<https://www.mod.go.jp/j/press/wp/wp_2021.html>。2021年７月にクリス・イングリス氏が初代国家サイバー長官に就任した（総務省ウェブサイト「世界情報通信事情－米国」８頁<https://www.soumu.go.jp/g-ict/country/america/pdf/001.pdf>）。

サイバー攻撃対策を行う体制を整備した。ＮＣＳＣはＧＣＨＱ傘下に置かれていることから、ＧＣＨＱの情報やスキル・経験を活用できることが強みとされる。大規模なサイバー攻撃やサイバー犯罪からの防御はＮＣＳＣの役割であるが、「戦争行為」に当たるような相手国へのサイバー攻撃は国防省及び軍のサイバー部隊の役割と位置付けられている[42]。

国家の安全保障に関わるサイバー戦略の最終責任を担うのは、安全保障に関係する限られた閣僚[43]で構成される国家安全保障会議（ＮＳＣ）で、下部組織としてサイバー部会（NSC Cyber）が設置されている。日々の業務や政策調整は内閣府担当大臣が担当する。政府自身のサイバーセキュリティ対策は内閣府内に設置されたサイバー・政府安全局（Cyber and Government Security Directorate：ＣＧＳＤ）が中央省庁間の調整に当たる。ＣＧＳＤは関連省庁や情報機関からの出向者約50人の陣容となっている。ＣＧＳＤが掌握するのは中央省庁の範囲のみであり、各省庁の管轄下にある機関や、民間への委託事業などのサイバーセキュリティについての最終責任は各担当省庁に帰属する。

（３）ドイツ

サイバーセキュリティについて、ドイツ連邦政府内においては、防衛事態（武力攻撃が生起）・緊迫事態（防衛事態の前段階の危機状況）では連邦国防省・連邦軍がサイバー防衛を担い、平時においては連邦内務省がサイバーセキュリティを担当する。連邦首相府は、サイバーセキュリティに関して、連邦情報局（対外情報活動を担当）を隷下に置くほか、連邦内務省と連邦国防省の総合調整を行う。連邦内務省の下には連邦情報技術安全庁、連邦憲法擁護庁（国内情報活動を担当）、連邦警察、連邦刑事庁などの関連組織がある。連邦情報技術安全庁は連邦内の通信網におけるサイバー脅威の阻止を任務としている。このほか、2011年の閣議決定に基づき設置された「国家サイバー防御センター」は、サイバーセキュリティの省庁・機関間連絡・調整プラットフォームであり、連邦情報技術安全庁が事務局となっている。各省庁等は連絡官を出し、日次ブリーフィング、作業部会等を通じてドイツ国内のサイバーに係る犯罪、防衛、諜報等事案の情報共有・対策のハブとして活動している[44]。

連邦軍は、サイバー防衛を新たな重要任務と位置付けており、国家サイバー防御センターとも協力体制を築いている。連邦軍による軍事的なサイバー活動の法的規律について、ド

---

[42] 以下、日本貿易振興機構（ジェトロ）ロンドン事務所海外調査部欧州ロシアＣＩＳ課「英国のサイバーセキュリティ体制の現状と課題―中小企業の事業リスクの観点から―」（2018.3）<https://www.jetro.go.jp/ext_images/_Reports/01/427a23803575001d/20170120.pdf>を参照。

[43] 2023年10月19日現在、国家安全保障会議は、首相（議長）、副首相、財務大臣、外務大臣、内務大臣、国防大臣、科学・イノベーション・技術大臣、法務長官、安全保障担当大臣、開発・アフリカ担当大臣の10人で構成されている（List of Cabinet Committees（GOV.UKウェブサイト）<https://www.gov.uk/government/publications/the-cabinet-committees-system-and-list-of-cabinet-committees>）。

[44] 小橋史行「【研究ノート】ドイツのサイバー・スペースのガバナンス―国防省及び連邦軍のサイバー部門の機能強化を中心に―」『防衛研究所紀要』第22巻第１号（2019.11）137～138頁、公益財団法人日工組社会安全研究財団「諸外国におけるサイバー事案の捜査手法等に関する調査研究報告書」（2023.3）28～29頁<https://www.syaanken.or.jp/wp-content/uploads/2023/03/cyber202303_01.pdf>、松浦一夫「ドイツにおけるサイバー安全保障と防衛憲法―政府による取組と議会における論義を中心に―」『憲法研究』54巻（2022年）２～３頁を参照して記述。

イツ政府は、連邦議会において、原則的には新規の独自のルールに従うことはないと説明しており、出動の根拠は従来どおり基本法（憲法）にあるとしている[45]。

５．能動的サイバー防御

（１）能動的サイバー防御の概念

新たな「国家安全保障戦略」では、前述（本稿１．及び２.）のとおり、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させるための具体的な方策として、「能動的サイバー防御」の導入を掲げている（図表２参照）。

図表２　「国家安全保障戦略」における能動的サイバー防御の内容

１　能動的サイバー防御の対象となるサイバー攻撃
- **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**

２　能動的サイバー防御の目的
- **１のサイバー攻撃を未然に排除する。**
- **１のサイバー攻撃が発生した場合の被害の拡大を防止する。**

３　能動的サイバー防御の導入に際しての取組
- **サイバー安全保障分野における情報収集・分析能力を強化する。**
- **能動的サイバー防御の実施のための体制を整備するため、以下の（ア）～（ウ）を含む必要な措置の実現に向け検討を進める。**
  - **（ア）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。**
  - **（イ）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。**
  - **（ウ）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。**

（出所）「国家安全保障戦略」（令和４年12月16日国家安全保障会議決定・閣議決定）21～22頁より筆者作成

「国家安全保障戦略」で掲げられた「能動的サイバー防御」（英語版では"active cyber defense"）とはどのような概念であろうか。「国家安全保障戦略」には、サイバー攻撃を未然に排除するため、未然に攻撃者のサーバ等への侵入・無害化する権限を政府に付与することが掲げられているが、それ以上の詳細な内容は明らかになっていない。

「能動的サイバー防御」ないし"active cyber defense"という用語には一貫した定義がないと言われている[46]。この用語が初めて登場した戦略文書と言われる米国の「国防総省サイバー戦略2011」では、国防総省がそのネットワークやシステムに対する侵入を防ぐため

[45] このサイバー活動の憲法上の評価については、国境のないサイバー空間において、出動が国内か国外かをどのように区別するか、それぞれの場合の憲法上の根拠、防衛事態・緊迫事態の発動要件などについて判例や学説上議論がある（松浦・前掲注44　３～17頁）。

[46] 「個別調査分析２　サイバーセキュリティ領域」（前掲注37）34頁

に採用している能動的サイバー防御は、脅威と脆弱性を発見、検出、分析、緩和するための同期化されたリアルタイムの能力であるとされており、未然に無害化する等の事前対応の記述は含まれていなかった[47]。我が国の「サイバーセキュリティ戦略」では「脅威に対して事前に積極的な防御策を講じていく取組」として「積極的サイバー防御」という用語が用いられているが、攻撃者に対する事前の対応に関する記述はない[48]。

国立大学法人政策研究大学院大学政策研究院による報告書（内閣府委託調査）では、アクティブ・サイバー・ディフェンス（ＡＣＤ）は一般に、サイバーインシデントの発生前・発生中・発生後に、組織がリアルタイムでネットワークをサイバー脅威から防御するために使用する運用上のインシデント対応プロセス及び技術的能力を指し、進行中の特定の脅威とは別に存在する受動的な防衛活動（例えば、脆弱性へのパッチ適用やファイアウォールの強化）とは区別されるとする。ＡＣＤとは、従来のパッシブ・ディフェンス（攻撃を受けてから対応）とオフェンス（攻撃）の間に位置するサイバーセキュリティ対策を捉えた用語であり、敵対者のネットワークを混乱させるように設計されているが、ハッキングバック（反撃）には至らない活動を意味し、両者を同義に用いるべきではないとする[49]。

（２）能動的サイバー防御を担う主体と権限

能動的サイバー防御には、悪用が疑われるサーバ等の検知（図表２の３（イ））や攻撃者のサーバ等への侵入・無害化（図表２の３（ウ））といった措置をとることが検討されている[50]。まず、これらの措置を担う主体と権限について考察する。

「国家安全保障戦略」では、能動的サイバー防御の対象となるサイバー攻撃について、「武力攻撃に至らない」ものを前提とする記述となっている[51]。武力攻撃に至らないサイバー攻撃に対して、同戦略では「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」と記述している[52]。報道によれば、同組織の下で実動部隊となるのが自衛隊や警察であると考えられている[53]。

このうち自衛隊については、政府は、2024（令和６）年に成立を目指す法整備により、自衛隊が防衛省・自衛隊のシステムに限定していたサイバー防護の対象を2028年(令和10)

---

47 Department of Defense Strategy for Operating in Cyberspace (July 2011) p.7 <https://csrc.nist.gov/csrc/media/projects/ispab/documents/dod-strategy-for-operating-in-cyberspace.pdf>

48 平成30年の「サイバーセキュリティ戦略」（平成30年７月27日閣議決定）では「サイバー関連事業者等と連携し、脅威に対して事前に積極的な防御策を講じる「積極的サイバー防御」を推進する」との記述があった（20～21頁）。この「積極的サイバー防御」は「サイバー攻撃に対して能動的に防御していく取組」とされている。最新の「サイバーセキュリティ戦略」（令和３年９月28日閣議決定）では、「国は、深刻なサイバー攻撃への対処を実効たらしめる脆弱性対策等の「積極的サイバー防御」に係る諸施策（中略）等について関係府省庁間で連携して検討する」と記述されており、「積極的サイバー防御」は「サイバー関連事業者等と連携し、脅威に対して事前に積極的な防御策を講じていく取組のこと」をいうとされる（同23頁）。

49 「個別調査分析２ サイバーセキュリティ領域」（前掲注37）34～35頁

50 「国家安全保障戦略」（前掲注２）21頁

51 同上。サイバー攻撃が武力攻撃に該当する場合、武力攻撃事態として自衛隊による対処（防衛出動）となる。なお、サイバー攻撃の武力攻撃該当性について、防衛省は、「一般論として、物理的な攻撃と同様な大きな被害が生ずるような場合には、そのサイバー攻撃が我が国の武力行使の前提となる相手による武力攻撃を構成することもあり得る」旨答弁している（第208回国会衆議院外務委員会議録第６号７頁（令4.3.23））。

52 「国家安全保障戦略」（前掲注２）22頁

53 『日本経済新聞』(2022.12.31)（前掲注３）

度以降に電力や交通、通信といった重要インフラ事業者に広げることを検討しているとの報道がある[54]。また、サイバー要員について、防衛省・自衛隊は、現在約890人のサイバー専門部隊を2027（令和９）年度までに約4,000人に拡充し、サイバー関連業務に従事する要員を含めて約２万人の態勢を整えるための予算要求がなされている[55]。

仮に自衛隊が能動的サイバー防御として「可能な限り未然に攻撃者のサーバ等への侵入・無害化」[56]を行うとする場合、そのためには自衛隊の任務に重要インフラの防護を追加するなど「必要な権限」を付与する法整備が必要となると思われる。特に無害化については、武器の使用に相当するような物理的な破壊を伴うのかどうかが問題となる。岸田内閣総理大臣は、「武力攻撃に至らない場合の措置として実施する能動的サイバー防御が武力の行使に該当することは想定していない」旨答弁している[57]が、武力行使に至らない烈度の武器使用に相当する措置が想定されているのかは明らかではない。武器使用相当の措置が想定されるのであれば、その権限についても明記することが考えられる。自衛隊による武力攻撃には至らない侵害への対処については、現行法上、海上警備行動や治安出動などの制度が存在し、警察比例の原則[58]による武器使用権限が規定されている[59]。

能動的サイバー防御のうち、悪用が疑われるサーバ等の検知や攻撃者のサーバ等への侵入といった措置（図表２の３（イ）及び（ウ））については、憲法第21条によって保護されている通信の秘密を侵害することにならないかという問題が指摘されている[60]。さらに、現行法上、電気通信事業者の取扱中に係る通信の秘密の保護について定める「電気通信事業法」[61]第４条、本来アクセスする権限のないコンピュータを利用する行為を禁じる「不正アクセス禁止法」[62]第３条等、電磁的記録不正作出及び供用（コンピュータ・ウイルスの作成・供用等）の罪を定める「刑法」[63]第161条の２などに抵触するおそれがある点が指摘されている[64]。

---

54 同上

55 防衛省「令和６年度概算要求の概要」21頁

56 「国家安全保障戦略」（前掲注２）21～22頁

57 第211回国会参議院本会議録第18号11頁（令5.4.26）

58 ①必要性の原則、すなわち目的達成のために必要な場合でなければならないという原則と、②過剰規制の禁止、すなわち、必要性が認められても目的と手段が相応していなければならないという原則からなる（永福誠也「領域警備―その概念と法制度等」『ＮＩＤＳコメンタリー』第169号（2021.6.8）５頁<https://www.nids.mod.go.jp/publication/commentary/pdf/commentary169.pdf>）。

59 海上警備行動については、自衛隊法（昭和29年法律第165号）第82条に規定されている。治安出動は同法第78条・第81条）に規定。武器の使用についてはいずれも警察官職務執行法（昭和23年法律第136号）第７条等を準用し、警察比例の原則に従うものとされている。

60 「（憲法を考える）サイバー攻撃対処、はらむ懸念　政府が法整備を検討、入り組む論点」『朝日新聞』（2023.10.31）

61 昭和59年法律第86号

62 不正アクセス行為の禁止等に関する法律（平成11年法律第128号）

63 明治40年法律第45号

64 渥美友里「日本企業のサーバーが「誤爆」される恐れはないのか、能動的サイバー防御の課題を探る」『日経クロステック』(2023.10.31)<https://active.nikkeibp.co.jp/atcl/act/19/00517/091100003/>。国民の権利・自由との関係について、内閣官房は、国会において、「サイバー安全保障分野での対応能力の向上のための具体的な取組内容については現時点で決定していない。安全保障上の必要性を踏まえるとともに、国民の権利や自由が不当に侵害されることのない取組内容となるように検討を進めてまいりたい」と答弁している（第211回国会衆議院総務委員会議録第12号12頁（令5.4.27））。

これらの点については、今後の法制度の整備に向けた有識者会議における検討等の動きの中で明らかになると思われる。

次いで、能動的サイバー防御として検討されている措置のうち政府と民間事業者等の連携（図表２の３（ア））についてはどうか。現行の体制ではサイバーセキュリティ協議会（本稿３.（１）参照）が官民連携の仕組みを担っているが、米国のＪＣＤＣや英国のＣＧＳＤ、ドイツの国家サイバー防御センター（本稿４．参照）のような類似の取組と比較して、実効的な連携をどのように図っていくかが課題となると思われる。

（３）国際法上のルールとの関係

能動的サイバー防御の手段として行う攻撃者による悪用が疑われるサーバ等の検知や攻撃者のサーバ等への侵入・無害化は、国際法上のルールに抵触する可能性はあるのか。この問題について、サイバー行動に適用される国際法に関して、日本政府の現時点での基本的な立場をまとめた「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日日本国外務省）（以下「基本的な立場」という。）[65]とＮＡＴＯサイバー防衛協力センターの支援により日本等のＮＡＴＯ以外の国籍を有する専門家が個人的資格で作成した「タリン・マニュアル2.0」[66]を材料として、武力の行使、不干渉原則、主権侵害、対抗措置の点から検討する。

ア　武力の行使

まず、武力の行使について、「基本的な立場」は、サイバー行動[67]であっても、一定の場合には、国連憲章第２条４が禁ずる武力による威嚇又は武力の行使に当たり得るとしている[68]。「タリン・マニュアル2.0」の規則69[69]では、「その規模及び効果が武力の行使の水準に至る非サイバー行動に比肩し得る場合は、武力の行使に該当する」とする。いかなる活動が武力の行使になるのかについて、人を殺傷し又はものを物理的に損壊する行為が武力の行使であることに専門家集団は同意したが、それ以外の場合は定かでなく、「規模及び効果」のアプローチ以外に明確な法的基準も存在しないとしている。

イ　干渉、主権侵害

「基本的な立場」は、「不干渉原則については、サイバー行動が、威圧など、ニカラグア事件判決（1986年）[70]で明確化された要件を満たす場合には違法な干渉となり得るとす

---

[65] 2021（令和３）年５月に我が国外務省が、国連事務総長によって任命された政府専門家からなる「国際安全保障の文脈における情報通信分野の発展に関する政府専門家グループ」（ＧＧＥ）に提出した文書<https://www.mofa.go.jp/mofaj/files/100200951.pdf>

[66] 北大西洋条約機構（ＮＡＴＯ）のサイバー防衛センター（エストニアの首都タリン）に法律専門家が個人的資格で集まって、サイバー攻撃に関する国際法のルールをコメンタリーとともに記述したものが「タリン・マニュアル」である。2013年に刊行された「タリン・マニュアル1.0」に続いて、「平時」におけるルールにつき検討がなされ、2017年に「サイバー行動に適用される国際法に関するタリン・マニュアル2.0」として刊行（Cambridge University Press）された。154の規則とコメンタリーからなる。中谷和弘・河野桂子・黒﨑将広『サイバー攻撃の国際法―タリン・マニュアル2.0の解説― 増補版』（信山社、2023年）は、これを要約し、解説を加えたものである。

[67] 同文書において「情報通信設備及び技術を利用した行動」とされる（１頁）。

[68] 「基本的な立場」（前掲注65）６頁

[69] 中谷ほか・前掲注66　85～86頁

[70] 同事件（1986年本案判決）において、国際司法裁判所は、ニカラグアに対する米国の軍事的活動等の違法性

る[71]。「タリン・マニュアル2.0」の規則66[72]では、例として、特定国への国家承認を撤回させるためのＤＤｏＳオペレーションを実行する場合や電子投票結果を改ざんするサイバー行動を秘密裏に実施して本来であれば当選しないはずの候補者が選挙に勝利した場合も強制的な干渉を構成するとする。

主権侵害については、「基本的な立場」は、日本政府としては、不干渉原則により禁じられる違法な干渉とは必ずしも一致しない主権侵害が存在すると考えているとし、医療機関を含む重要インフラに対するサイバー行動によって物理的被害や機能喪失を生じさせる行為は、主権の侵害に該当し得る（場合によっては違法な干渉等にも当たり得る）としている[73]。「タリン・マニュアル2.0」でも、あるサイバー行動が規則66で禁止される干渉を構成しなくても、主権侵害にはなり得るとしている[74]。例えば、サイバー・インフラの物理的損害（例：冷却機能停止による部品の溶解）がなくても、機能の喪失が生じた場合（例:2011年にサウジ国営の原油精製企業「サウジアラムコ社」のシステムが「シャムーン」ウイルスにより被害）も主権侵害となるとされる。

ウ　サイバー諜報

「タリン・マニュアル2.0」規則32[75]では、「国家による平時のサイバー諜報はそれ自体は国際法に違反しないが、それを遂行する方法は国際法違反となりうる」としている。国際法に違反する手段として、他国領域内のサイバー・インフラへのハッキングにより当該インフラの機能が停止した場合は主権侵害となり違法とされるような場合が挙げられる。他方、国家が自国領域内にハニーポット（侵入者に仕掛けたおとり）を構築することは主権の行使として合法であり、侵入した国が被害を受けてもその責任は侵入者にあるとされる。

エ　対抗措置

「基本的な立場」は、国際違法行為に対し対抗措置をとることは、一定の条件（強行規範に反しないこと、均衡性等）の下で、国際法上認められているとする[76]。「タリン・マニュアル2.0」規則20～25[77]は、サイバー攻撃についても同様の対抗措置が可能となることを示している。

を認定した（森川幸一・兼原敦子・酒井啓亘・西村弓『国際法判例百選 第３版』（別冊jurist No.255）（有斐閣、2021.9）220～221頁）。武力不行使原則に関するリーディングケースとして知られるが、不干渉原則についても主要な判例とされている。藤澤巌『内政干渉の国際法―法の適用問題への歴史的視座』（岩波書店、2022年）の「第５章　ニカラグア事件本案判決における不干渉原則」（341～349頁）を参照。

71 「基本的な立場」（前掲注65）２頁

72 中谷ほか・前掲注66　81～83頁

73 「基本的な立場」（前掲注65）２～３頁

74 「タリン・マニュアル2.0」規則66（中谷ほか・前掲注66　83頁）。規則４（主権の侵害）については同17～18頁。これに対して、英国は、「他国のネットワークに同意なく侵入することは、禁止される干渉に当たらない場合であっても、主権侵害として禁止される」という見解に否定的な立場を示した。本件は、黒﨑将広「サイバー空間における主権」森肇志・岩月直樹編『サブテキスト国際法』（日本評論社、2020年）31～43頁）に詳しい（英国の見解については33頁）。

75 中谷ほか・前掲注66　42～43頁

76 「基本的な立場」（前掲注65）４頁

77 中谷ほか・前掲注66　32～37頁

６．制度構築に際しての課題―むすびに代えて―

能動的サイバー防御の詳細な制度構築については、今後、有識者会議などで政府から案が示され、議論されていくものと思われる。ここでは、能動的サイバー防御の導入に際して、現段階で課題と考えられる点について、簡単に触れたい。

サイバー空間における行動は、通常目に見えない。その中で「未然に攻撃者側のシステムに侵入し、無害化する」措置に関して、どのような具体的な手法や行動基準が定められるのか、攻撃者の特定や攻撃者の行為の特定の国への帰属をどのように検知し証明するのか、国際的なルールへの抵触の有無をどのように確認するのか、といった疑問がある。

また、サイバー攻撃の手法として、事前にマルウェアをシステムに侵入させて、後に発動させる事例（例：イラン核施設の破壊[78]）がある。能動的サイバー防御の手法として、物理的な破壊に至らないとしても、何らかのマルウェアの使用は許されることになるのか、仮に能動的サイバー防御の措置を武力の行使に至らない程度にとどめる留意規定を置いたとしても、実際の運用において他国のインフラの物理的な破壊に至ってしまった場合の責任をどのように整理するのか。

組織面では、「軍事と非軍事、有事と平時の境目が曖昧」という環境の中で、軍事部門（防衛省・自衛隊）と非軍事部門（警察等）の役割分担をどのように図っていくのか。リアル空間では例えば装備面などで区別ができても、サイバー空間では難しいのではないか。

さらに、平時における対応として我が国がとった能動的サイバー防御の措置によって事態がエスカレートし、武力の行使に匹敵するようなサイバー攻撃を招来する危険性はないのか[79]。その点で、我が国の危機管理体制において、国家安全保障会議と、ＮＩＳＣの後継となる新たな司令塔組織、自衛隊や警察などの実動部隊、それぞれの関係をどのように規律するのか、民主的な統制をいかに図るのか、具体的な制度設計が問われる。

以上のような課題をクリアしつつ、「グレーゾーン事態が恒常的に生起している安全保障環境」と、「攻撃側が防御側に対して優位にあるサイバー空間」[80]という状況認識を踏まえ、安全保障を実効的に確保するために、どのようなサイバー安全保障体制を構築していくべきなのか、活発な議論が期待される。

（もり　ひではる）

---

[78] 2010年６月、インターネットに接続されていないイランの核施設のシステムが「Stuxnet」（スタックスネット）と呼ばれるマルウェアに感染し、遠心分離装置が破壊されたと言われている。本事案については、須江秀司「コンピューターウィルスStuxnetによるイラン核関連施設攻撃～核不拡散政策からの視点～」『ＮＩＤＳコメンタリー』第20号（2011.5.16）<https://www.nids.mod.go.jp/publication/commentary/pdf/commentary020.pdf>に詳しい。

[79] サイバー空間におけるエスカレーションリスクについて、高橋杉雄『日本で軍事を語るということ　軍事分析入門』（中央公論新社、2023年）226～231頁を参照。

[80] 「サイバー空間はネットワークによって相互に繋がり、常時接続している必要がある。その結果、攻撃は任意の手法でいつでも好きな時に実行できるのに対して、防御はそれに対してあらゆる場所で常に備えていなければならないため、相対的に多大な費用、人員とエネルギーを要する。つまり、費用対効果の点から、攻撃側が防御側に対して非常に優位にある」とされる（松村・前掲注36　Ⅲ－８頁）。