参議院常任委員会調査室・特別調査室

論題	サイバー空間における自衛隊のアクセス・無害化措置 －能動的サイバー防御導入に伴う自衛隊法改正の概要と国会論議－
著者 / 所属	藤川　隆明 / 外交防衛委員会調査室
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	477 号
刊行日	2025-7-25
頁	44-62
URL	https://www.sangiin.go.jp/japanese/annai/chousa/rippou_chousa/backnumber/20250725.html

※ 本文中の意見にわたる部分は、執筆者個人の見解です。

サイバー空間における自衛隊のアクセス・無害化措置

― 能動的サイバー防御導入に伴う自衛隊法改正の概要と国会論議 ―

藤川　隆明
（外交防衛委員会調査室）

１．はじめに

第217回国会（常会）において、能動的サイバー防御の導入に係る①重要電子計算機に対する不正な行為による被害の防止に関する法律案（閣法第４号）及び②重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律案（閣法第５号）が国会に提出され、衆参の審議を経て[1]、2025年５月16日、参議院本会議において多数をもって可決、成立した。②の法律案は、その内容に自衛隊法の改正[2]も含まれており、自衛隊は平素から、国、基幹インフラ等をサイバー攻撃から守るため、一定の措置をとることが可能となる。本稿では、自衛隊法の改正内容等を国会審議の内容を整理しつつ概観する[3]。なお、文中の名称、肩書等はいずれも当時のものである。

[1] 衆参両院において、①及び②の両法律案に附帯決議が行われた（内容については、衆議院は<https://www.shugiin.go.jp/internet/itdb_rchome.nsf/html/rchome/Futai/naikakuBA0D8D2CD956E38749258C65002D638F.htm>を、参議院は<https://www.sangiin.go.jp/japanese/gianjoho/ketsugi/217/f063_051501.pdf>をそれぞれ参照されたい。なお、最終アクセスは2025年７月３日で、以下ＵＲＬの最終アクセスの日付はいずれも同日。）。①の法律案は、衆議院の審議において修正がなされたものの、自衛隊法改正を含む②の法律案は修正がなされていない。

[2] 施行期日は、①の法律の公布の日（2025年５月23日）から起算して１年６月を超えない範囲内において政令で定める日である。

[3] 警察官によるアクセス・無害化措置その他の法案の内容については、本号掲載の榎本尚行「能動的サイバー

２．自衛隊法における行動規定と権限規定

（１）自衛隊法第６章及び第７章について

自衛隊法は、自衛隊が法律によって認められる行動を分類して個別に規定し、かつ、当該行動において、自衛隊が行使できる権限についても個別に規定している。自衛隊の行動については、同法第６章（自衛隊の行動）において、防衛出動、治安出動等の行動類型が規定されている。自衛隊の権限については、同法第７章（自衛隊の権限）において、個々の行動ごとに個々に権限が規定されている。

（２）能動的サイバー防御導入に伴う自衛隊法の改正概観

自衛隊法第６章及び第７章における自衛隊の行動及び権限という観点からは、今般の能動的サイバー防御導入に伴う自衛隊法の改正の主な内容は、**図表１**のように、同法第６章の行動規定において通信防護措置（詳細は**４（１）**参照）という新たな行動類型が創設され、同法第７章の権限規定において、①通信防護措置の際の権限規定の新設、②自衛隊又は在日米軍が使用する特定電子計算機[4]の警護のための権限規定の新設のほか、③治安出動時の権限規定の改正、④防衛出動時の公共の秩序維持のための権限規定の改正が行われたものである。

図表１　能動的サイバー防御導入に伴う自衛隊法第６章及び第７章における主な改正

自衛隊法第６章 （自衛隊の行動）	自衛隊法第７章 （自衛隊の権限）
防衛出動（自衛隊法第 76 条）	○防衛出動時の公共の秩序の維持のための権限（自衛隊法第 92 条） ・一定の自衛官の職務執行について、警職法・自衛隊法・海上保安庁法の一部の規定の準用 ・追加　一定の自衛官の職務執行について、警職法第６条の２第２項から第 11 項までの規定の準用【アクセス・無害化措置】 ○防衛出動時の緊急通行（自衛隊法第 92 条の２）
治安出動（自衛隊法第 78 条・第 81 条）	○治安出動時の権限（自衛隊法第 89 条） ・一定の自衛官の職務執行について、警職法（第６条の２を除く。）の規定の準用 ・追加　一定の自衛官の職務執行について、警職法第６条の２第２項から第 11 項までの規定の準用【アクセス・無害化措置】
新設　重要電子計算機に対する通信防護措置（自衛隊法第 81 条の３）	新設　重要電子計算機に対する通信防護措置の際の権限（自衛隊法第 91 条の３） ・一定の自衛官の職務執行について、警職法第６条の２第２項から第 11 項までの規定の準用【アクセス・無害化措置】）
－	新設　自衛隊等が使用する特定電子計算機の警護のための権限（自衛隊法第 95 条の４） ・一定の自衛官の職務執行について、警職法第６条の２第２項から第 11 項までの規定の準用【アクセス・無害化措置】）

（出所）筆者作成

防御２法案の国会論議（３）―アクセス・無害化措置の概要と論点―」を参照されたい。

[4] 「特定電子計算機」とは、不正アクセス行為の禁止等に関する法律第２条第１項に規定する特定電子計算機をいい（自衛隊法第95条の４第１項）、不正アクセス行為の禁止等に関する法律第２条第１項に規定する特定電子計算機とは、電気通信回線に接続している電子計算機をいう。

なお、通信防護措置は、自衛隊法第３条第１項の「従たる任務」に、該当する[5]。

このほか、通信防護措置の創設に伴い、特別の部隊の編成に関する規定（自衛隊法第22条）や関係機関との連絡及び協力に関する規定（自衛隊法第86条）が改正されている[6]。

３．能動的サイバー防御における自衛隊のアクセス・無害化措置

（１）アクセス・無害化措置の具体的手法等

自衛隊法改正により、自衛隊は、一定の場合、アクセス・無害化措置を実施することが可能となる。同措置は、武力攻撃事態に至らない平素の段階から公共の秩序の維持を目的として行うものであり、第一義的には公共の安全と秩序の維持を責務とする警察が実施するものと説明される[7]。政府は、同措置の具体的な内容について、まず、攻撃に使用されているサーバー等に対し遠隔からログインを行い、当該サーバー等にインストールされているプログラムなどを確認した上で、当該サーバー等が攻撃に用いられないよう、インストールされている攻撃のためのプログラムの停止、削除や、攻撃者が当該サーバーなどへアクセスできないような設定変更などの措置を行うことを想定しており、具体的な手法については、個別具体の状況に応じて適切に判断をする旨見解を示している[8]。なお、国会審議では、関連論点として、マルウェアを活用することがあるのかが問われたが、措置の詳細の説明は、手のうちを明らかにすることにもつながるとして答弁が控えられている[9]。

同措置を実施する自衛隊の部隊は、自衛隊サイバー防衛隊[10]が念頭に置かれている[11]。

---

[5] 自衛隊法第３条は、自衛隊の任務を規定する。同条に規定される任務は、自衛隊の存立目的を規定したものであり、実務上は、自衛隊の「本来任務」と称される。
同条に規定される「本来任務」は「主たる任務」と「従たる任務」に分けられる。同条第１項において、「自衛隊は、我が国の平和と独立を守り、国の安全を保つため、我が国を防衛することを主たる任務とし、必要に応じ、公共の秩序の維持に当たるもの」とされ、自衛隊は、我が国の防衛を「主たる任務」とし、「必要に応じ」公共の維持に当たることとなる。一般に、前者（我が国の防衛）が「主たる任務」、後者（公共の秩序維持）が「従たる任務」と呼称される。国の防衛という「主たる任務」は、唯一自衛隊のみが果たし得る任務であるのに対し、公共の秩序維持は、第一義的には警察機関の任務であり、警察機関のみでは対処困難な場合等に自衛隊が対処することとなる。

[6] 自衛隊法第 22 条第１項は、内閣総理大臣が防衛出動等を命じた場合に、自衛隊法に規定のない部隊を特別に編成すること等ができる旨規定している。内閣総理大臣が命じる防衛出動等において、自衛隊法に定める部隊編成によるだけではなく、事態に的確に対応する行動をとることができる特別の部隊を編成することが必要となる場合があり、こうした場合に、特別の部隊の編成を認める規定であるが、今般、通信防護措置が創設されるに当たり、内閣総理大臣が通信防護措置を命じた場合にも、内閣総理大臣が特別の部隊の編成等をすることができるように改正されている。
また、自衛隊法第 86 条は、防衛出動命令等下令時の関係機関との間の連絡及び協力の規定である。命令を受けて行動する自衛隊の部隊等と、関係のある機関（警察機関等）との間で相互に緊密に連絡し、協力することを定めているところだが、同条の改正により、通信防護措置の実施における連絡・協力も第 86 条で規定されることとなる。

[7] 第217回国会衆議院内閣委員会議録第10号（2025.4.2）家護谷昌徳防衛省大臣官房サイバーセキュリティ・情報化審議官答弁

[8] 第217回国会衆議院本会議録第９号（2025.3.18）石破茂内閣総理大臣答弁

[9] 第217回国会参議院外交防衛委員会会議録第12号（2025.5.13）大和太郎防衛省防衛政策局長答弁

[10] 防衛大臣の直轄部隊であり、自衛隊のサイバーの中核を担う高度専門部隊として、陸・海・空自衛隊の各サイバー部隊等から特に選抜されたハイレベル人材が登用されている（防衛省資料「防衛省・自衛隊におけるこれまでの取組等」〈https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/dai2/siryou6-4.pdf〉４頁）。

[11] 第217回国会衆議院本会議録第９号（2025.3.18）中谷元防衛大臣答弁

（２）アクセス・無害化措置の性質－武力の行使に当たるのか－

政府は、アクセス・無害化措置について、武力攻撃事態に至らない状況下における対処を念頭に、平素の段階から公共の秩序の維持を目的として実施するものであり、自衛権ではなく警察権の行使として、比例原則に基づき、目的を達成するために必要最小限度の措置として行う旨説明する[12]（具体例は（１））。その上で、政府は、アクセス・無害化措置は、人を殺傷し又は物を破壊するという戦闘行為には当たらず日本国憲法第９条に規定する武力の行使には当たらない旨[13]、通常兵器による有形力の行使と同様の深刻な被害を伴うことは想定されず、国連憲章第２条第４項が禁ずる武力の行使に当たることはない旨[14]、ましてや武力攻撃にも当たることはない旨[15]、日本国憲法第９条や国連憲章に規定する武力の行使と評価されるようなものではないという意味で、専守防衛[16]を踏み越えるといった指摘も当たらない旨[17]説明している。さらに、政府は、アクセス・無害化措置が、違法な先制攻撃とみなされることも否定した[18]。

４．自衛隊がアクセス・無害化措置を行う４つの場合

公表されている政府資料[19]においては「防衛省・自衛隊によるアクセス・無害化措置」として、通信防護措置（自衛隊法第81条の３及び第91条の３）と自衛隊又は在日米軍が使用する特定電子計算機の警護（自衛隊法第95条の４）のみが記載されている。

しかし、今般の自衛隊法改正は、上記の政府資料に記載されている、①通信防護措置、②自衛隊又は在日米軍が使用する特定電子計算機の警護の場合のほかにも、③治安出動、④防衛出動時の公共の秩序維持の場合においても、警察官のアクセス・無害化措置に係る規定である警察官職務執行法第６条の２第２項から第11項までの規定を準用し（自衛隊法第89条、第91条の３、第92条及び第95条の４）、自衛隊はサイバー空間での措置をとるとされている（準用される警察官職務執行法第６条の２の各規定の概要は、**図表２**のとおりである）。このように、上記①から④までの４つの場合の改正は、法制度上は、防衛省・自衛隊によるアクセス・無害化措置を実施することを可能とする改正と考えることができる。

実際、国会において、政府は、治安出動時や防衛出動時（の公共の秩序維持）の状況においては、物理的な空間のみならず、サイバー空間においても措置をとる必要があるという場合が想定され、今般、アクセス・無害化措置をこのような場合にもとれるように所要

---

[12] 第217回国会衆議院本会議録第９号（2025.3.18）石破茂内閣総理大臣答弁
[13] 第217回国会衆議院本会議録第９号（2025.3.18）石破茂内閣総理大臣答弁
[14] 第217回国会衆議院本会議録第９号（2025.3.18）平将明国務大臣答弁
[15] 第217回国会衆議院内閣委員会議録第11号（2025.4.4）平将明国務大臣答弁
[16] 「専守防衛」とは、相手から武力攻撃を受けたときに初めて防衛力を行使し、その防衛力行使の態様も自衛のための必要最小限度にとどめ、また保持する防衛力も自衛のための必要最小限度のものに限るなど、憲法の精神にのっとった受動的な防衛戦略の姿勢をいうものと説明される（第94回国会参議院予算委員会会議録第13号10頁（1981.3.19）大村襄治防衛庁長官答弁等）。
[17] 第217回国会参議院内閣委員会、総務委員会、外交防衛委員会連合審査会会議録第１号（2025.5.13）平将明国務大臣答弁
[18] 第217回国会衆議院本会議録第９号（2025.3.18）石破茂内閣総理大臣答弁
[19] 内閣官房資料<https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/pdf/setsumei.pdf>の右肩番号「20」を参照されたい。

の改正を行う旨答弁[20]している。

図表２　自衛隊がアクセス・無害化措置を行う際に準用される
警察官職務執行法第６条の２第２項～第11項の規定の概要

各項の規定	概要
第２項	警察庁長官が指名する警察官（サイバー危害防止措置執行官）は、サイバー攻撃又はその疑いがある通信等を認めた場合であって、そのまま放置すれば、人の生命、身体又は財産に対する重大な危害が発生するおそれがあるため緊急の必要があるときは、攻撃関係サーバー等の管理者等に対し、危害防止のため通常必要と認められる措置であって電気通信回線を介して行うものをとることを命じ、又は自らその措置をとる旨の規定
第３項	処置の対象たる電子計算機が国内に設置されていると認める相当な理由がない場合には、警察庁の警察官のみが処置をできることとし、あらかじめ、警察庁長官を通じて、外務大臣と協議しなければならない旨の規定
第４項	サイバー危害防止措置執行官が、第２項の規定による処置をとる場合には、あらかじめ、サイバー通信情報監理委員会の承認を得なければならないこととし、サイバー通信情報監理委員会の承認を得るいとまがないと認める特段の事由がある場合にはこの限りでない旨の規定
第５項	第３項に規定する場合における第４項の承認の求めは、第３項の規定による協議の結果を添えて行う旨の規定
第６項	サイバー通信情報監理委員会は、第４項の承認の求めがあった場合において、当該求めが第２項及び第３項の規定に照らして適切と認めるときは、当該承認をする旨の規定
第７項	サイバー危害防止措置執行官は、第２項の規定による処置をとるに際しては、みだりに関係者の正当な業務を妨害してはならない旨の規定
第８項	サイバー危害防止措置執行官は、第２項の規定による処置をとったときは、攻撃関係サーバーの管理者に同項に規定する措置をとることを命じた場合を除き、遅滞なく、当該管理者に通知をする旨の規定
第９項	サイバー危害防止措置執行官は、サイバー通信情報監理委員会の承認を得ないで第２項の規定による処置を行ったときは、速やかに、当該処置について同委員会に通知をする旨の規定
第10項	第９項の規定による通知を受けたサイバー通信情報監理委員会は、必要があると認めるときは、警察庁長官等に対し、必要な措置をとるべきことを勧告する旨の規定
第11項	サイバー危害防止措置執行官は、措置の実施について、警察庁長官又は都道府県警察本部長の指揮を受けなければならない旨の規定

（出所）筆者作成

そこで、以下、今般の自衛隊法改正の主要な点を、自衛隊法第６章に規定する行動と第７章に規定する権限の区分の観点から、（１）通信防護措置、（２）自衛隊又は在日米軍が使用する特定電子計算機の警護、（３）治安出動、（４）防衛出動（時の公共の秩序維持）の順に確認する。

（１）通信防護措置

新たな行動類型として創設される通信防護措置は、国や基幹インフラ等の一定の重要な電子計算機に対し、本邦外にある者による特に高度に組織的かつ計画的なサイバー攻撃が行われ、自衛隊が有する特別な技術又は情報が必要不可欠であるなど自衛隊が対処を行う特別な必要があるときに、内閣総理大臣の命令に基づき、自衛隊が警察と共同して当該電子計算機への被害を防止するための措置をとるものである[21]。通信防護措置については、自

[20] 第217回国会参議院外交防衛委員会会議録第12号（2025.5.13）飯島秀俊内閣官房内閣審議官答弁
[21] 第217回国会衆議院内閣委員会総務委員会安全保障委員会連合審査会議録第１号（2025.4.3）平将明国務大臣答弁

衛隊法第６章の行動規定及び第７章の権限規定ともに条文が新設された。

ア　自衛隊法第６章関係－通信防護措置に関する行動規定の新設－

通信防護措置は、自衛隊が警察と共同して公共の秩序の維持のために実施するものであることを踏まえ、内閣総理大臣が特別の必要を判断し、自衛隊の部隊等が内閣総理大臣の通信防護措置命令に基づき行う。通信防護措置は、一般の警察力が維持されていることが前提であり[22]、内閣総理大臣が命令を出すことで、自衛隊と警察の適切な役割分担を実施することとなり、そのための要件が自衛隊法第81条の３に規定されている[23]。

具体的には、内閣総理大臣は、重要電子計算機[24]に対する特定不正行為[25]であって、「本邦外にある者による特に高度に組織的かつ計画的な行為[26]」と認められるものが行われた場合において、次の**図表３**のいずれにも該当することにより自衛隊が対処を行う特別

---

[22] 他方、治安出動時や防衛出動時（の公共の秩序維持時）は、一般の警察力では治安の維持ができないような場合に、自衛官が公共の秩序の維持を目的として活動する（第217回国会参議院外交防衛委員会会議録第12号（2025.5.13）飯島秀俊内閣官房内閣審議官答弁）。

[23] 第217回国会参議院外交防衛委員会会議録第12号（2025.5.13）飯島秀俊内閣官房内閣審議官答弁

[24] 政府は、重要電子計算機の例として、国会審議において、大きく３つの類型を示した（①国の行政機関などが使用する電子計算機であり、このうち、そのサイバーセキュリティが害された場合において、その機関などにおける重要情報の管理又は重要な情報システムの運用に関する事務の実施に重大な支障が生ずるおそれがあるもの、②基幹インフラ事業者が使用する電子計算機であり、このうち、そのサイバーセキュリティが害された場合において、特定重要設備の機能が停止し、又は低下するおそれがあるもの、③重要情報を保有する事業者が使用する電子計算機であり、このうち、そのサイバーセキュリティが害された場合において、当該事業者における重要情報の管理に関する業務の実施に重大な支障が生ずるおそれがあるもの）上で、これら３類型の重要電子計算機は、サイバー攻撃を受けた場合に、国家及び国民の安全を害し、又は国民生活若しくは経済活動に多大な影響を及ぼすおそれがあることから、法律を通じ、サイバー攻撃による被害の防止を図っていく必要があるとしている（第217回国会参議院内閣委員会会議録第10号（2025.4.22）小柳誠二内閣官房内閣審議官答弁）。

[25] 重要電子計算機に対する不正な行為による被害の防止に関する法律第２条第４項に規定する「特定不正行為」をいい、電気通信回線を介して行われるものに限る。この「特定不正行為」とは、①刑法第168条の２第２項の罪に当たる行為、②不正アクセス行為（不正アクセス行為の禁止等に関する法律第２条第４項に規定する不正アクセス行為）、③電子計算機を用いて行われる業務に係る刑法第２編第35章の罪に当たる行為であって、当該電子計算機のサイバーセキュリティを害することによって行われるもの（当該電子計算機に接続された電気通信回線の機能に障害を与えることによって行われるものを含む。）をいう。

[26] 「本邦外にある者による特に高度に組織的かつ計画的な行為」に該当するサイバー攻撃として、政府が主に念頭に置いているのは、例えば、国家のリソースを投じることなどにより、対象システム内に長期潜伏できる高い組織性や計画性を備え、堅牢な攻撃インフラを構築し、そして、未知の脆弱性等の高度な手法を用いるなどの特徴を有しているものであり、そして、このような特徴を有した行為の趣旨を簡明に説明する表現として、政府は、「国家を背景とする主体」という表現を用いている（第217回国会衆議院内閣委員会総務委員会安全保障委員会連合審査会議録第１号（2025.4.3）中谷元防衛大臣答弁）。通信防護措置は、このような「国家を背景とする主体」による高度なサイバー攻撃を念頭に置いて対処することとしているところ、自衛隊法第81条の３の条文には、「本邦外にある者」と規定することによって、攻撃主体が我が国に所在するものではないということを明確にし、さらに、「特に高度に組織的かつ計画的な行為」と規定することによって、個人や活動家、また犯罪組織、民間団体が通常行い得るものではなくて、国家のリソースを投じるなどにより実現されることが想定される高度な行為が対処の対象であることを明確にしたとされている（第217回国会衆議院内閣委員会議録第７号（2025.3.21）本田太郎防衛副大臣答弁）。

ただし、政府は、「本邦外にある者による特に高度に組織的かつ計画的な行為」という（条文の）要件について、（現時点においては、国家を背景とする主体による高度なサイバー攻撃が当該要件に該当することを主に想定しているが、）ほかの主体によるものであっても、その組織性、計画性、攻撃手法やその態様といった観点から、本邦外にある者による特に高度に組織的かつ計画的な行為と認められる場合においては、内閣総理大臣が自衛隊に通信防護措置を命じることは法文上排除されていない旨見解を示した（第217回国会衆議院本会議録第９号（2025.3.18）石破茂内閣総理大臣答弁）。

の必要があると認めるとき[27]は、部隊等に当該特定不正行為[28]による当該重要電子計算機への被害を防止するために必要な電子計算機の動作に係る措置であって電気通信回線を介して行うもの（「通信防護措置」）をとるべき旨を命ずることができる（自衛隊法第81条の３第１項）。当該発令は、内閣の首長として行うものであることから、閣議決定に基づいて行うことになり、そのため、通信防護措置の発令の際は、その都度閣議決定がなされる[29]。

図表３　自衛隊が対処を行う特別の必要に関する要件

①当該特定不正行為により重要電子計算機に特定重大支障（重要電子計算機の機能の停止又は低下であって、当該機能の停止又は低下が生じた場合に、当該重要電子計算機に係る事務又は事業の安定的な遂行に容易に回復することができない支障が生じ、これによって国家及び国民の安全を著しく損なう事態が生ずるものをいう。②において同じ。）が生ずるおそれが大きいと認めること。 **②特定重大支障の発生を防止するために自衛隊が有する特別の技術又は情報が必要不可欠であること。** **③国家公安委員会からの要請又はその同意があること。**

（出所）筆者作成

なお、**図表３**③の国家公安委員会の要請又は同意について、通信防護措置が公共の秩序の維持のために自衛隊が警察と共同して実施するものであることを踏まえ、第一義的に責任を有する国家公安委員会を関与させる規定が設けられた[30]。国家公安委員会は、警察のみでは対処が困難又は時間を要するため自衛隊が対処に加わる特別の必要があるかについて判断することとなる[31]。

また、内閣総理大臣は、部隊等に通信防護措置をとるべき旨を命ずる場合、あらかじめ、防衛大臣と国家公安委員会との間で協議をさせた上で、**図表４**に掲げる事項を指定しなければならない[32]（自衛隊法第81条の３第４項）。

---

[27] 通信防護措置は自衛隊が対処する特別な必要がある場合の措置であるところ、自衛隊と警察の能力にどのような差異があるのか。この点、政府は、①警察は、これまでのサイバー攻撃の捜査、その他の対処や外国治安機関等との連携を通じて積み上げてきた不正プログラムの解析等の高度なフォレンジック能力や、攻撃者や手口等を解明する高度な情報分析能力等を有している旨、②自衛隊は、武力攻撃事態等における高烈度なサイバー攻撃に対処するために構築してきた高度なサイバー防衛能力や、米軍等との訓練、協力によって獲得しているサイバー攻撃対処手法等を有している旨の認識を示している（第217回国会参議院内閣委員会会議録第11号（2025.4.24）飯島秀俊内閣官房内閣審議官答弁）。

ただし、平国務大臣は、基本的な認識として、警察と自衛隊どちらが上という認識を政府は持っておらず、警察は警察、自衛隊は自衛隊で持っている情報ネットワークも違い、対応してきた技術の練度も違うことから、その意味では、その組織に合わせた得意な部分を担うこととなる旨述べている（第217回国会衆議院内閣委員会議録第11号（2025.4.4））。

[28] 当該特定不正行為を行った者による同種の特定不正行為を含む（自衛隊法第81条の３）。

[29] 第217回国会参議院外交防衛委員会会議録第12号（2025.5.13）大和太郎防衛省防衛政策局長答弁

[30] 第217回国会衆議院内閣委員会議録第10号（2025.4.2）坂井学国家公安委員会委員長答弁

[31] 第217回国会参議院内閣委員会会議録第11号（2025.4.24）坂井学国家公安委員会委員長答弁

[32] 政府によれば、指定を今後どうしていくかは更に検討することとなるが、「期間」についていえば、「無期限」という指定ではなく、有限の期間を指定するする見込みである（第217回国会参議院外交防衛委員会会議録第12号（2025.5.13）大和太郎防衛省防衛政策局長答弁）。

一方で、仮に有限の期間を指定したとして、その間に、対象とすべきサイバー攻撃を探知、対処できなかった場合は、もう一度、期間を指定する（すなわち通信防護措置の発令をもう一度行う）旨説明されている（第217回国会参議院外交防衛委員会会議録第12号（2025.5.13）大和太郎防衛省防衛政策局長答弁）。

図表４　通信防護措置の実施に当たりあらかじめ指定する事項

①通信防護措置により対処を行う特定不正行為及び防護の対象となる重要電子計算機 ②通信防護措置として実施すべき措置に関する事項 ③通信防護措置の期間 ④警察庁等と共同して通信防護措置を実施する要領その他の警察庁等との連携に関する事項 ⑤その他必要な事項

（出所）筆者作成

さらに、内閣総理大臣は、**図表４**③の期間内であっても、通信防護措置の必要がなくなったと認める場合には、速やかに、部隊等に通信防護措置の終了を命じなければならない（自衛隊法第81条の３第５項）。

イ　自衛隊法第７章関係－通信防護措置に関する権限規定の新設－

通信防護措置は、その権限に関する規定が、自衛隊法第７章に第91条の３として新設された。同条は、内閣総理大臣から通信防護措置をとるべき旨を命ぜられた部隊等の自衛官の職務の執行について、警察官職務執行法第６条の２第２項から第11項までの規定を準用する旨規定している[33]。

政府は、自衛隊による通信防護措置のために認められている権限や措置の影響は、警察が実施するものと同等であり、警察官職務執行法第６条の２に基づく措置は行使するものの、武器使用は認められていないという観点から、国民の権利義務に与える影響は限定的である旨説明している[34]。そして、通信防護措置は、あくまで重要電子計算機に対する危害を防ぐため、ネットワークを介して行う必要最小限度の措置であるとし、必要最小限度の措置の具体的な程度は、個別具体的な状況に応じて異なり一概に述べることは困難としつつ、ネットワーク、システムを壊さない程度のものである旨の見解が示された[35]。

（２）自衛隊又は在日米軍が使用する特定電子計算機の警護のための権限規定

自衛隊法第７章において、自衛隊又は日米安全保障条約に基づき我が国にある米軍が使用する一定の電子計算機を、サイバー空間において武力攻撃に至らない侵害から警護するための権限を規定する第95条の４が新設された。

ア　改正の背景

当該規定は、昨今、我が国の防衛力を構成する自衛隊や我が国に所在する米軍が使用

---

[33] 政府は、通信防護措置において、警察官職務執行法第６条の２を準用することについて、おおむね①一般の警察力が機能していることが前提にある状況において、本来であれば公共の秩序の維持の第一義的に責任を有する警察が実施する事務を自衛隊にも行わせるものであり、その際の権限規定については警察官職務執行法第６条の２を準用する、②共同して対処する警察が警察官職務執行法に基づいて活動する、③公共の秩序の維持を目的とする自衛隊の他の行動類型、例えば、治安出動や警護出動等も警察官職務執行法の権限を準用していることを踏まえれば、通信防護措置の際の権限についても警察官職務執行法第６条の２を準用することは、自衛隊法の他の規定とも整合的である旨説明をしている（第217回国会衆議院内閣委員会議録第10号（2025.4.2）家護谷昌徳防衛省大臣官房サイバーセキュリティ・情報化審議官答弁）。

[34] 第217回国会衆議院内閣委員会総務委員会安全保障委員会連合審査会議録第１号（2025.4.3）中谷元防衛大臣答弁

[35] 第217回国会衆議院内閣委員会議録第10号（2025.4.2）家護谷昌徳防衛省大臣官房サイバーセキュリティ・情報化審議官答弁

する特定電子計算機に対してサイバー攻撃が生じる可能性が高まっていることを踏まえて新設されており[36]、現行の自衛隊法第95条において、自衛隊の武器等という我が国の防衛力を構成する重要な物的手段を防護するために武器の使用が認められている（いわゆる武器等防護）という考え方が参考にされている[37]。

イ　自衛隊又は在日米軍が使用する特定電子計算機の警護のための権限規定の運用

警察官職務執行法第６条の２第２項から第11項までの規定は、**図表５**に掲げる特定電子計算機をサイバーセキュリティ[38]を害することその他情報技術を用いた不正な行為から職務上警護する自衛官の職務の執行について準用する（自衛隊法第95条の４第１項）。**図表５**②に掲げる特定電子計算機に対する警護は、アメリカ合衆国の軍隊から要請があった場合であって、防衛大臣が必要と認めるときに限り、自衛官が行う（自衛隊法第95条の４第２項）。

図表５　対象となる特定電子計算機

①自衛隊が使用する特定電子計算機 **②日本国とアメリカ合衆国との間の相互協力及び安全保障条約に基づき日本国にあるアメリカ合衆国の軍隊が使用する特定電子計算機**

（出所）筆者作成

自衛隊法第95条の４の措置は、平時、有事関係なく、自衛隊や在日米軍のサーバーを防御するために行う措置である[39]。なお、在日米軍が使用する特定電子計算機の平素からの警護は、要請の判断主体は米軍となるが、当該要請に基づく自衛隊による警護の実施については、防衛大臣が国際情勢や米軍の状況等を踏まえ、その必要を判断するものであり、アクセス・無害化措置に当たっても、防衛大臣の指揮を受けることとなるのであり、我が国が米軍の指揮下に入るわけではない旨説明されている[40]。

---

[36] 第217回国会参議院外交防衛委員会会議録第12号（2025.5.13）飯島秀俊内閣官房内閣審議官答弁

[37] より具体的な説明として、政府は、我が国の防衛力を構成する重要な物的手段である自衛隊が使用する特定電子計算機について、サイバー空間において武力攻撃に至らない侵害から警護するため、極めて受動的かつ限定的な必要最小限度の措置を講ずる権限を平素から自衛官に付与する旨（第217回国会参議院外交防衛委員会会議録第12号（2025.5.13）飯島秀俊内閣官房内閣審議官答弁）、日米安全保障条約に基づき、我が国に所在する米軍が使用する特定電子計算機の使用が阻害された場合には、米軍の運用が妨げられることとなり、ひいては、日米の共同運用能力の低下につながり、我が国の防衛に支障が生じることになりかねず、その上で、サイバーセキュリティは平素から確保されることが極めて重要であることを踏まえ、我が国に所在する米軍が使用する特定電子計算機は、我が国の防衛力を構成する重要な物的手段に相当するものと評価し、新設する自衛隊法第95条の４における警護の対象とした旨（第217回国会衆議院内閣委員会議録第６号16頁（2025.3.19）家護谷昌徳防衛省大臣官房サイバーセキュリティ・情報化審議官答弁）説明している。

[38] 自衛隊法第95条の４第１項に規定する「サイバーセキュリティ」とは、サイバーセキュリティ基本法第２条に規定するサイバーセキュリティをいい、これは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（「電磁的方式」）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体（「電磁的記録媒体」）を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていることをいう。

[39] 第217回国会衆議院内閣委員会総務委員会安全保障委員会連合審査会議録第１号（2025.4.3）平将明国務大臣答弁

[40] 第217回国会衆議院本会議録第９号（2025.3.18）石破茂内閣総理大臣答弁

（３）治安出動

今般の自衛隊法の改正により、治安出動を命ぜられた自衛隊の自衛官のうち一定のものは、アクセス・無害化措置をとることができる。

ア　改正の背景

政府は、治安出動時は、一般の警察力では治安を維持することができないような場合に、自衛官が公共の秩序の維持を目的として活動するところ、こうした状況においては、物理的な空間のみならず、サイバー空間においても措置をとる必要があるという場合が想定されるとし、こうした状況でも適切に対応できるよう、今般、アクセス・無害化措置がとれるように所要の改正を行った旨説明している[41]。

イ　自衛隊法第６章関係－改正なし－

治安出動は、自衛隊法第６章に規定されている（自衛隊法第78条及び第81条）が、今般、これらの規定について、改正は行われていない。

ウ　自衛隊法第７章関係－治安出動時の権限の改正－

治安出動時の権限に関する自衛隊法第89条が改正された。同改正により、命令による治安出動（自衛隊法第78条第１項）又は要請による治安出動（自衛隊法第81条第２項）を命ぜられた自衛隊の自衛官のうち、自衛隊法第89条第１項において準用する改正後の警察官職務執行法第６条の２第２項の規定による処置を適正にとるために必要な能力を有する部隊等として防衛大臣が指定する部隊等に属するものの職務の執行について、警察官職務執行法第６条の２第２項から第11項までの規定が準用される。

（４）防衛出動時の公共の秩序の維持のための権限の追加

今般の自衛隊法の改正により、自衛隊法第76条第１項の規定により防衛出動を命ぜられ公共の秩序の維持のために職務を執行する自衛隊の自衛官のうち一定のものは、アクセス・無害化措置をとることができる。

ア　改正の背景

上記（３）アと同様である。政府は、防衛出動時（の公共の秩序の維持を行う場合）は、自衛官が、一般の警察力では治安を維持することができないような場合に、公共の秩序の維持を目的として活動するところ、こうした状況においては、物理的な空間のみならず、サイバー空間においても措置をとる必要があるという場合が想定されるとし、こうした状況でも適切に対応できるよう、アクセス・無害化措置がとれるように所要の改正を行った旨説明している[42]。

イ　自衛隊法第６章関係－改正なし－

防衛出動は、自衛隊法第６章に規定されている（自衛隊法第76条）が、今般、当該規定について、改正は行われていない。

ウ　自衛隊法第７章関係－防衛出動時の公共の秩序の維持のための権限の改正－

防衛出動時の公共の秩序の維持のための権限に関する自衛隊法第92条第２項が改正さ

---

41 第217回国会参議院外交防衛委員会会議録第12号（2025.5.13）飯島秀俊内閣官房内閣審議官答弁
42 第217回国会参議院外交防衛委員会会議録第12号（2025.5.13）飯島秀俊内閣官房内閣審議官答弁

れた。同改正により、同法第76条第１項の規定により防衛出動を命ぜられた自衛隊の自衛官のうち同法第92条第２項において準用する警察官職務執行法第６条の２第２項の規定による処置を適正にとるために必要な能力を有する部隊等として防衛大臣が指定する部隊等に属するものが自衛隊法第92条第１項の規定により公共の秩序の維持のため行う職務の執行について、警察官職務執行法第６条の２第２項から第11項までの規定が準用されることとなる。

５．自衛隊によるアクセス・無害化措置の手続

（１）警察官職務執行法の規定の準用によるアクセス・無害化措置の手続

既述のとおり、自衛隊がアクセス・無害化措置をとる場合には、警察官職務執行法第６条の２第２項から第11項までの規定が準用される。具体的には、主に以下の手続をとった上で権限を行使することとなる。

ア　外務大臣との協議

自衛隊が国外に所在するサーバーなどにアクセス・無害化措置を行うに当たり、国際法上許容される範囲内で行うことを確保する観点から、措置を命ぜられた部隊等の自衛官は、防衛大臣を通じて、あらかじめ外務大臣と協議を行う（自衛隊法第89条第１項、第91条の３、第92条第２項及び第95条の４第１項の規定による警察官職務執行法第６条の２第３項の規定の準用）。外務大臣は、その措置が国際法上許容される範囲内のものかどうかに限り判断をする[43]。そして、外務大臣が、国際法上違法であって、その違法性を阻却できないと判断する措置の実施に同意することはなく、そのような措置が実施されることはないとされる[44]。

なお、たとえ、今般の法改正で設置される独立監視機関のサイバー通信情報監理委員会の承認を得るいとまがない場合（下記**イ**）でも、国外サーバー等に対するアクセス・無害化措置は、外務大臣との協議を要する[45]。

イ　サイバー通信情報監理委員会からの事前承認

アクセス・無害化措置の実施に当たり、事前承認を得るいとまがないと認める特段の事由がない限り、防衛大臣を通じて、今般の法改正で設置される独立監視機関のサイバー通信情報監理委員会による事前承認を得る必要があり、**ア**に記載の外務大臣との協議の結果を添えなければならない（自衛隊法第89条第１項、第91条の３、第92条第２項及び第95条の４第１項の規定による警察官職務執行法第６条の２第４項及び第５項の規定の準用）。事前の承認については、自衛隊がアクセス・無害化措置を実施するに当たり、同委員会に、①サイバー攻撃に利用されているサーバー等であると認めた理由、②サイバー攻撃による危害の防止という目的を達成するために取り得る措置の内容等を示し、サイバー通信情報監理委員会は、その承認の求めが警察官職務執行法等の規定に照らして適

---

[43] 第217回国会衆議院内閣委員会議録第11号（2025.4.4）石破茂内閣総理大臣答弁
[44] 第217回国会参議院本会議録第14号（2025.4.18）岩屋毅外務大臣答弁
[45] 第217回国会衆議院内閣委員会議録第７号５頁（2025.3.21）飯島秀俊内閣官房内閣審議官答弁

切かどうかを判断するとされる[46]。あらかじめ高い独立性を持つ同委員会の承認を得なければならない手続とすることで、当該措置が法律にのっとって適切に実施されることや措置の適正性を確保する旨説明されている[47]。

一方、事前承認を得るいとまがないと認める特段の事由がある場合[48]は、防衛大臣を通じて同委員会への事後通知を行うことで足りる（自衛隊法第89条第１項、第91条の３、第92条第２項及び第95条の４第１項の規定による警察官職務執行法第６条の２第９項の規定の準用）。ただし政府は、このような事後の通知による運用が常態化することはないとしている[49]。加えて、通知を受けた同委員会は、実施された処置が適切かどうかを確認し、必要があると認めるときは防衛大臣に勧告することができることとされており（自衛隊法第89条第１項、第91条の３、第92条第２項及び第95条の４第１項の規定による警察官職務執行法第６条の２第10項の規定の準用）、政府は、このような手続を設けることにより、権利の濫用の抑止を図り、措置の適正性を十分に確保することができる旨説明している[50]。

ウ　防衛大臣による指揮[51]

自衛隊がアクセス・無害化措置を実施する際には、権限行使の適正性を組織的に判断するため、防衛大臣による指揮を受けなければならない[52]（自衛隊法第89条第１項、第91条の３、第92条第２項及び第95条の４第１項の規定による警察官職務執行法第６条の２第11項の規定の準用）。準用する警察官職務執行法等の要件を満たすかという判断は、組織的に慎重になされることが適当であるので、措置の実施主体は防衛大臣の指揮を受けることとされている[53]。政府は、アクセス・無害化措置を実施した結果は、一義的には行政機関の個々の職員ではなく、措置を実施した行政機関が責任を負う旨説明した[54、55]。

---

[46] 第217回国会衆議院本会議録第９号（2025.3.18）石破茂内閣総理大臣答弁

[47] 第217回国会参議院本会議録第14号（2025.4.18）石破茂内閣総理大臣答弁、第217回国会衆議院本会議録第９号（2025.3.18）石破茂内閣総理大臣答弁

[48] 特段の事由がある場合の例として、政府は、サイバー攻撃により基幹インフラ事業者に現に重大な障害が発生している状況、攻撃者によるサイバー攻撃の敢行予定日時等が判明したが、既にその予定時刻が切迫している状況等が想定される旨説明している（第217回国会参議院内閣委員会会議録第14号（2025.5.15）飯島秀俊内閣官房内閣審議官答弁）。

[49] 具体的には、サイバー攻撃では、その予兆を把握してから実際の攻撃まで時間的余裕が限られていることが予想されるので、原則は事前承認としていても、実際には事後通知が常態化することにならないかとの懸念に対し、石破内閣総理大臣が、サイバー通信情報監理委員会の委員には、法律や情報通信技術に関して専門的知識等を有する者が就くことから、迅速かつ的確に承認が行われるものと想定しており、事後の通知が常態化することはないと考えている旨説明している（第217回国会衆議院本会議録第９号（2025.3.18））。

[50] 第217回国会衆議院本会議録第９号（2025.3.18）石破茂内閣総理大臣答弁

[51] 自衛隊法第８条は、「防衛大臣の指揮監督権」として、防衛大臣が自衛隊の隊務を統括する旨を規定するが、ここでは、自衛隊のアクセス・無害化措置における警察官職務執行法第６条の２第11項の規定の準用に係る防衛大臣の指揮を意味する。

[52] 第217回国会参議院本会議録第14号（2025.4.18）石破茂内閣総理大臣答弁

[53] 第217回国会参議院内閣委員会会議録第14号（2025.5.15）飯島秀俊内閣官房内閣審議官答弁

[54] 第217回国会参議院内閣委員会会議録第14号（2025.5.15）飯島秀俊内閣官房内閣審議官答弁

[55] 万が一、仮に誤って実施したアクセス・無害化措置によって対象サーバー等の管理者等に損害、損失が生じた場合について、政府は、個別具体的に判断する必要があり、一概には言えないが、①国内にあるサーバーなら、国家賠償法による損害賠償責任の問題として、②国外に所在するサーバー等に対して誤った措置を行った場合には、あくまで一般論だが、国家責任条文の関連する規定等を踏まえて対応していく旨説明している（第217回国会衆議院内閣委員会総務委員会安全保障委員会連合審査会議録第１号（2025.4.3）飯島秀俊内閣

なお、サイバー通信情報監理委員会の承認を得るいとまがない場合（上記**イ**）であっても適正に措置が行われるよう、平素から訓練、研修を徹底するとともに、適切に指揮を行う旨説明されている[56]。

（２）アクセス・無害化措置の手続に入る前の手続

アクセス・無害化措置を行うに当たり、自衛隊は、少なくとも（１）の手続をとるが、政府によれば、当該手続の前にも、政府における手続が存在する。つまり、国、基幹インフラ等に対する一連の重大なサイバー攻撃(いわゆるサイバー攻撃キャンペーン)ごとに、国家安全保障会議（ＮＳＣ）４大臣会合が、サイバー安全保障担当大臣、国家公安委員会委員長も参加の上で開催され、そこで「対処方針」が決定され、その後に、サイバー安全保障担当大臣の指導の下で、個別の無害化措置についての手続に入る[57]。当該「対処方針」とは、当該サイバー攻撃キャンペーンへの対応における基本的な方針であり、外交的観点[58]を踏まえたものとなる。外務大臣は、この「対処方針」を審議するＮＳＣ４大臣会合に出席し、主に外交政策上の観点から議論に参加する[59、60]。

なお、ＮＳＣで決定した総論的な「対処方針」に基づくアクセス・無害化措置が、サイバー通信情報監理委員会に承認されなかった（（１）**イ**）場合には、当該措置は実施されない[61]。

（３）アクセス・無害化措置の迅速性

ア　（１）及び（２）の手続とアクセス・無害化措置の迅速性への影響

自衛隊がアクセス・無害化措置をとるには、少なくとも上記の手続が必要となる。一方で、サイバー攻撃では、実際の攻撃までに自衛隊がアクセス・無害化措置をとるには時間的余裕が限られていることが予想されるところ、迅速な措置が可能なのかは論点となり得る。

この点、石破内閣総理大臣は、内閣総理大臣が議長を務める国家安全保障会議で「速やかに」審議をした上で総論的な「対処方針」を定めるとしている[62]。また、（１）の手続については、防衛省は、①防衛省・自衛隊がこれまでに培ってきた能力を基礎としつつ、自衛隊によるアクセス・無害化措置が防衛大臣の指揮の下で十分なスピード感を持っ

官房内閣審議官答弁)。

56 第217回国会参議院本会議録第14号（2025.4.18）石破茂内閣総理大臣答弁

57 第217回国会衆議院内閣委員会議録第11号（2025.4.4）室田幸靖内閣官房内閣審議官答弁

58 当該観点について政府は、一概には述べられないが、その時々の外交政策において外務大臣が有している情報、あるいは外務大臣が抱えている案件との関係について、アクセス・無害化措置をどのように行うかの方針に、必要に応じて反映する旨説明がなされている（第217回国会参議院内閣委員会会議録第11号（2025.4.24）室田幸靖内閣官房内閣審議官答弁)。

59 第217回国会衆議院内閣委員会議録第11号（2025.4.4）室田幸靖内閣官房内閣審議官答弁

60 以上から、外務大臣は、まずはＮＳＣ４大臣会合において、外交的観点からアクセス・無害化措置の方針について議論をし、国外サーバー等に措置が行われる際には、国際法上の観点から、警察官職務執行法に基づいた協議を行うこととなる。

61 第217回国会参議院本会議録第14号（2025.4.18）石破茂内閣総理大臣答弁

62 第217回国会参議院本会議録第14号（2025.4.18）石破茂内閣総理大臣答弁

て適切になされるよう、平素から体制の整備、人材の育成、訓練といった各種施策に取り組み、万全を期し、②サイバー通信情報監理委員会は、法律や情報通信技術に関して専門的知識等を有する者が委員となることから、原則である事前の承認は迅速かつ的確に行われるものと認識しており、また、③外務省とは平素から緊密に連携することで、外務大臣との協議を適切かつ迅速に行うことができるように取り組む旨見解を示した[63]。

イ　通信防護措置命令の発令要件の迅速性への影響

通信防護措置には、内閣総理大臣の命令が必要であり、当該命令の迅速性も論点である。通信防護措置命令は、国家公安委員会からの要請又はその同意があることが要件となる（**図表３**）が、坂井国家公安委員会委員長は、実務上、速やかに対応するよう工夫することが必要であると認識している旨、国家公安委員会においては、緊急の事態に際しての意思決定手続を定めているところ、こうした意思決定手続の活用も含め、法施行までの間に検討を進めるほか、平素から内閣官房や防衛省との間で情報共有を緊密に行うよう警察庁を指導し、必要な措置が適時適切に行われるように努める旨認識を示した[64]。また、**図表３**に示した３要件が全て満たされない限り内閣総理大臣が命令を発することができないのは厳格すぎるのではないかとの指摘がなされた。防衛省は、国家を背景とした平素からのサイバー攻撃による重要インフラ等の機能停止等の試みという例示の上で、このような攻撃によって、通信防護措置の発令要件の一つである国家及び国民の安全を著しく損なう事態が生じるおそれは平素から生じ得るとして、そのような攻撃が一度認知されれば、重大な被害が発生する前から自衛隊が対処できるよう、内閣総理大臣が通信防護措置をちゅうちょなく発令することが重要である旨認識を示している[65]。

６．自衛隊のアクセス・無害化措置に関する主要な議論

第217回国会での議論を中心に、自衛隊のアクセス・無害化措置に関する主要な議論を以下に整理する。

（１）自衛隊がアクセス・無害化措置を行う４つの場合の比較

既述のとおり、今般の自衛隊法改正により、自衛隊が、①通信防護措置、②自衛隊又は在日米軍が使用する特定電子計算機の警護、③治安出動、④防衛出動時の公共の秩序維持の４つの場合において、アクセス・無害化措置を実施することが可能となるが、①の通信防護措置の場合は、②、③及び④の場合と比べて、以下の特徴がある。

自衛隊が通信防護措置をとるには、内閣総理大臣による通信防護措置命令が必要となる（自衛隊法第81条の３）が、②、③及び④の場合は、内閣総理大臣による通信防護措置命

---

[63] 第217回国会衆議院内閣委員会議録第６号８頁（2025.3.19）家護谷昌徳防衛省大臣官房サイバーセキュリティ・情報化審議官答弁

[64] 第217回国会参議院内閣委員会会議録第11号（2025.4.24）

[65] 第217回国会衆議院内閣委員会議録第８号（2025.3.26）家護谷昌徳防衛省大臣官房サイバーセキュリティ・情報化審議官答弁。なお、同答弁において、ちゅうちょなく発令するために、政府として必要な情報収集、分析に万全を期す旨見解が示されている。

令は不要で、対象となるサイバー攻撃が、「本邦外にある者による特に高度に組織的かつ計画的な行為」という要件も不要とされる[66]。この通信防護措置について、政府は、治安出動がかかっている状況でも、防衛出動がかかっている状況でもない、言わば「平素に近い状況」で、高度な組織的かつ計画的な、そして国家を背景とした主体によるサイバー攻撃が行われた場合に、自衛隊において必要最小限の措置として、警察官職務執行法に基づき、アクセス・無害化が行われる旨説明している[67]。逆に、政府は、治安出動が発令された際に、同時に自衛隊法第81条の３に基づく通信防護措置が発令される可能性は基本的にない旨見解を示した[68]。通信防護措置は、治安出動等が発令されるような状況、すなわち「一般の警察力では治安を維持することができないような事態」に発令されるものではない旨説明もされた[69]。

（２）通信防護措置の条文に規定されなかった国会承認及び逐次の国会報告

通信防護措置については、内閣総理大臣が命令権者となるが、国会の承認は条文上必要とされていない。この点は、防衛出動や命令による治安出動と異なる（**図表６**）。

図表６　通信防護措置と内閣総理大臣が命令権者である他の行動類型との比較

行動類型	命令権者	国会承認	任務の性質
防衛出動（自衛隊法第76条）	内閣総理大臣	必要	我が国の防衛
命令による治安出動（自衛隊法第78条）	内閣総理大臣	必要	公共の秩序の維持
要請による治安出動（自衛隊法第81条）	内閣総理大臣	不要	公共の秩序の維持
警護出動（自衛隊法第81条の２）	内閣総理大臣	不要	公共の秩序の維持
通信防護措置（自衛隊法第81条の３）	**内閣総理大臣**	**不要**	**公共の秩序の維持**

（出所）筆者作成

政府は、通信防護措置について事前の国会承認を設けた場合、攻撃者は自衛隊による措置が講じられることを認知し、対策を講じるなど、結果的に攻撃者を利することにもなる旨説明している[70]。また、中谷防衛大臣が、①通信防護措置による国民の権利義務に与える影響[71]及び②措置の実効性の確保[72]という観点から、通信防護措置の終了後に一律に国会報告を行うことは法定する必要はなく、また適切でないと考えており、この考え方を前提としつつ、通信防護措置の実施に当たっては、内閣総理大臣の命令に基づき、防衛大臣による指揮を受けることを法定し、この点から、シビリアンコントロールの観点からも適切な

---

66 第217回国会参議院外交防衛委員会会議録第12号（2025.5.13）大和太郎防衛省防衛政策局長答弁
67 第217回国会参議院外交防衛委員会会議録第12号（2025.5.13）大和太郎防衛省防衛政策局長答弁
68 第217回国会参議院外交防衛委員会会議録第12号（2025.5.13）大和太郎防衛省防衛政策局長答弁
69 第217回国会衆議院内閣委員会総務委員会安全保障委員会連合審査会議録第１号（2025.4.3）中谷元防衛大臣答弁
70 第217回国会参議院内閣委員会会議録第14号（2025.5.15）飯島秀俊内閣官房内閣審議官答弁
71 自衛隊が通信防護措置をとるために認められている権限や措置の影響は警察が実施するものと同等で、警察官職務執行法第６条の２に基づく措置は行使するものの、武器使用などは認められておらず、国民の権利義務に与える影響は限定的である旨説明されている。
72 通信防護措置の実施後の国会報告は、当該措置の内容を明らかにし、当該措置を受けた攻撃者が自衛隊による措置であると認知し対策を講じるなど、結果的に攻撃者を利することにつながるおそれがある旨説明されている。

措置が確保されていると考えている旨見解を示している[73]。

（３）アクセス・無害化措置と国際法

アクセス・無害化措置は、国外のサーバー等に処置をすることがあるところ、この場合において、我が国が処置するアクセス・無害化措置の国際法上の評価が議論となった。

ア　政府の見解

石破内閣総理大臣は、個別のアクセス・無害化措置に関する国際法上の評価は、それぞれの具体的な状況に応じて判断されるため、一概に答えることは困難だが、外国に所在する攻撃サーバー等にアクセスし、これを無害化する際に、国際法上許容される範囲内で行うことは当然のことであり、①そもそも国際法上禁止されていない合法的な行為に当たる場合や、②仮にサーバー所在国の領域主権の侵害に当たり得るとしても、その違法性を阻却できるような措置に限って無害化措置を実施する旨説明している[74]。また、そのような実施を確保する観点から、自衛隊は防衛大臣を通じて、あらかじめ外務大臣と協議しなければならないこととなっている（５（１）ア）。

②の場合において、政府は、実際の事案に即して仮定の議論を当てはめることは差し控えつつも、一般論として、外国に所在する攻撃サーバー等へのアクセス・無害化措置が仮にサーバー所在国の領域主権の侵害に当たり得るとしても、例えば、国際違法行為に対し一定の条件の下で対抗措置をとること、あるいは国際法上の緊急状態という考え方を援用することは、サイバー空間における国際法の適用についても認められているとの見解を示した[75]。また、緊急状態を援用する場合には、外務大臣との協議を通じて、国家責任条文第25条の要件に合致するということを確保して措置する旨説明している[76]。なお、国家責任条文第25条の要件など（いわゆる切迫性、代替不能性、相当性）は、法律全体で十分担保されている旨見解が示されている[77]。

イ　アクセス・無害化措置を行った相手国から国際法上の違法等の指摘を受ける可能性

アにおいて政府の見解を確認した。また、３（２）に既述したように、政府は、アクセス・無害化措置は国連憲章で禁止されている武力の行使に当たらない旨、武力攻撃にも当たらない旨強調している。一方で、他国との関係を考えた場合、我が国がどのように主張しようとも、結局はアクセス・無害化措置を受けた相手国の認識や恣意的なものを含めた反応次第ではないのかとの疑問は残る。この点に関する国会論議を簡単に確認したい。

アクセス・無害化措置は、可能性としては、①Ａ国がＡ国の領域にあるサーバーから我が国にサイバー攻撃等をする場合や、②Ａ国が第三国であるＢ国の領域にあるサーバーを乗っ取って、Ｂ国から我が国にサイバー攻撃等をする場合が想定される。我が国

---

[73] 第217回国会衆議院内閣委員会総務委員会安全保障委員会連合審査会議録第１号（2025.4.3）中谷元防衛大臣答弁
[74] 第217回国会衆議院本会議録第９号（2025.3.18）石破茂内閣総理大臣答弁
[75] 第217回国会衆議院本会議録第９号（2025.3.18）石破茂内閣総理大臣答弁
[76] 第217回国会衆議院内閣委員会議録第10号（2025.4.2）岩屋毅外務大臣答弁
[77] 第217回国会参議院内閣委員会会議録第11号（2025.4.24）平将明国務大臣答弁

は、①の場合は、A国の領域のサーバーにアクセス・無害化措置を行い、②の場合はB国の領域のサーバーにアクセス・無害化措置を行うこととなるが、相手国から国際法上の違法等の指摘を受ける可能性はあるのだろうか。

①の場合について、平国務大臣が、(アクセス・無害化措置を)された方(国)が抗議をしてくる可能性について、基本、現状は言ってこない旨の認識を示し、自分たちがやっていると自ら自白するようなものなので、そこ[78]が言ってくることはないと、理由にも言及した[79]。なお、①の場合について、我が国を攻撃しようとしている国はサーバーがその国にあることは少ないとの見解も示している[80]。

また、②の場合について、平国務大臣は、アクセス・無害化措置は、(多くは)その対象である相手サーバーが、我が国を攻撃しようとしている国ではない国にあり、乗っ取られている状況にあることを説明し[81]、上記B国から抗議を受けることには「なかなかなりにくい」との見解を示している[82、83]。

ウ　複数の行為が累積をして武力攻撃と評価され得るという議論

複数の行為が累積をして武力攻撃と評価され得るという議論についても政府が言及をしている。政府は、そのような議論があることは承知をしているが、仮にそのような議論を前提とした場合であっても、アクセス・無害化措置によるサーバー等の物理的破壊等は想定されず、我が国の措置が武力攻撃と評価されるとの主張には「説得力がない」と考えている旨、その上で、法案上、アクセス・無害化措置を行うに当たっては、このような点も含め国際法上許容される範囲内で行うことを留意する観点から、あらかじめ外務大臣と協議を行うこととしており、さらに、国際法上許容される範囲内で行うものであるという点も含め、アクセス・無害化措置の性質について国連を始めとする様々な場を活用して積極的に説明をしていきたい旨見解を示した[84]。

---

78 答弁において、「そこ」の詳細は述べられていないが、文脈からすると、我が国にサイバー攻撃等を行ったために、我が国からアクセス・無害化措置をされた国を念頭においた答弁と考えられる。

79 第217回国会参議院内閣委員会会議録第11号(2025.4.24)

80 第217回国会参議院内閣委員会会議録第11号(2025.4.24)平将明国務大臣答弁

81 第217回国会参議院内閣委員会会議録第11号(2025.4.24)、第217回国会参議院内閣委員会会議録第14号(2025.5.15)

82 第217回国会参議院内閣委員会会議録第14号(2025.5.15)

83 一方で、サーバーのオーナーについては、平国務大臣は、「そのサーバーがどこかから乗っ取られていて、そこから攻撃されるものを無害化するので、サーバーのオーナーから何てことをしてくれるんだということはないです、基本的には。乗っ取られているんですから、それを無害化するので。」と一度は述べている(第217回国会参議院内閣委員会会議録第11号(2025.4.24))が、別の機会の答弁において、「多分、私の発言は、サーバーのオーナーからというよりは、日本を攻撃をしようとしている国から何てことをしてくれるんだという、そういう発言だったというふうに承知をしております。サイバー攻撃への関与を明かした上で無害化措置へ抗議等をすることがないと私が申し上げたのは、サーバーの管理者のついてではなくて、サイバー攻撃主体や攻撃に関与する国でありますので、そうしたサイバー攻撃主体等である国は、攻撃への自らの関与が発覚した場合には、国際社会において厳しい非難を受けることとなるため、サイバー攻撃においては、複数の国にまたがる踏み台となるサーバーを悪用し、自らの関与が発覚しにくいように攻撃を行うことが通常であります。こうした事情を背景に、委員会での私の発言は、重大なサイバー攻撃が行われた際に、サイバー攻撃主体等である国が、その原因となるサーバー等が自らの支配下にあることを積極的に認め、その上で無害化措置を行った主体を非難するということは考えにくいと、そういう趣旨で申し上げました。」と述べている(第217回国会参議院内閣委員会会議録第14号(2025.5.15))。

84 第217回国会衆議院内閣委員会議録第11号(2025.4.4)平将明国務大臣答弁

（４）自衛隊法改正に際しての自衛隊法上の「武器」概念の変更の有無

自衛隊法上の「武器」の概念は、「火器、火薬類、刀剣類その他直接人を殺傷し、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、装置等」であるとするのが従来からの政府統一見解[85]である。今般、サイバー空間における自衛隊の権限が検討され法改正がなされたが、自衛隊法上の「武器」の概念に変更はあったのかが問われた。政府は、自衛隊法上、「武器」とは、火器、火薬類、刀剣類その他直接人を殺傷し、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、装置等であると解しているところであり、一般的に、電子計算機やソフトウェアそのものは、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、装置などとは解されないことから、武器には当たらないと考えている旨、自衛隊法における「武器」の概念に変更はない旨明言している[86]。

（５）アクセス・無害化措置と相手方のサイバー空間の利用を妨げる能力

今般の自衛隊法改正により、自衛隊は、アクセス・無害化措置を実施することができるようになった。

一方で、政府は、国会審議で、武力攻撃事態における武力の行使の一環として自衛隊が行うサイバー攻撃への対処については、旧防衛計画の大綱（2018年12月18日国家安全保障会議決定及び閣議決定）及び国家防衛戦略（2022年12月16日国家安全保障会議決定及び閣議決定）に基づき、2019年度以降整備してきた相手方のサイバー空間の利用を妨げる能力を用いることを含め、物理的手段を講ずることも排除されていない旨見解を示している[87]。

相手方のサイバー空間の利用を妨げる能力は、有事に際して、相手方の武力攻撃に用いられるシステム等に対し、ネットワークを通じて電子情報を送信することによって当該システム等の機能発揮に支障を生じさせることで、相手方がサイバー攻撃を行うこと自体を阻止する、又は相手方の戦力の円滑な機能発揮を妨害する能力で[88]、あくまでも武力行使の三要件を満たす場合に限って自衛のための必要最小限度の範囲で行うものである[89]。政府は、当該能力を用いることにより、相手方の攻撃、武力攻撃に用いられるシステムが物理的に破壊されたり、破壊と同視し得る程度に機能を喪失したりする場合もあり得る旨説明している[90]。

相手方のサイバー空間の利用を妨げる能力に関する当該説明は、武力攻撃事態に至らない状況下での通信防護措置が、ネットワークを壊さない、システムを壊さない程度のものである旨の説明と対極をなすものである。

---

85 第77回国会衆議院予算委員会議録第18号17頁（1976.2.27）三木武夫内閣総理大臣答弁
86 第217回国会参議院外交防衛委員会会議録第12号（2025.5.13）大和太郎防衛省防衛政策局長答弁
87 第217回国会衆議院内閣委員会議録第11号（2025.4.4）家護谷昌徳防衛省大臣官房サイバーセキュリティ・情報化審議官答弁
88 第208回国会衆議院安全保障委員会議録第３号８頁（2022.3.15）岸信夫防衛大臣答弁
89 第204回国会参議院外交防衛委員会会議録第８号14頁（2021.4.20）岸信夫防衛大臣答弁
90 第204回国会参議院外交防衛委員会会議録第８号14頁（2021.4.20）岸信夫防衛大臣答弁

７．おわりに

以上、自衛隊によるアクセス・無害化措置を可能とする自衛隊法の改正について概観した。自衛隊がアクセス・無害化措置を実施する根拠法は整備された。本稿では、自衛隊がアクセス・無害化措置を行う際に警察官のアクセス・無害化措置に係る規定である警察官職務執行法第６条の２の規定を準用している点と、政府の国会答弁から、自衛隊がアクセス・無害化措置をとる場合は４つあると紹介した。通信防護措置は、一般の警察力が維持されている「平素に近い状況」での自衛官による措置であった。これは、一般の警察力では治安の維持ができないような場合に、自衛官が公共の秩序の維持を目的に出動する治安出動等とは異なった性質の行動類型である。また、自衛隊法第95条の武器等防護の考え方を参考に、自衛隊又は在日米軍が使用する一定の電子計算機も警護の対象となった。このほか、治安出動時及び防衛出動時の公共の秩序維持のための権限行使を、自衛隊が行うアクセス・無害化措置として紹介をした。そして、手続の点で自衛隊がアクセス・無害化措置を迅速にとれるのかという国会審議も紹介した。

アクセス・無害化措置は、国外のサーバーに対しても実施し得るところ、国会審議では、相手国との関係を含め多くの議論がされた。政府は、アクセス・無害化措置が武力の行使に当たらないこと、違法性が阻却される場合があること等を都度説明し、国際法上許容される範囲内でアクセス・無害化措置を実施することを強調し、我が国のアクセス・無害化措置について、サイバー攻撃主体や攻撃に関与する国から違法性等の指摘をうける可能性は低い旨説明している。なお、**６（３）ウ**に紹介した答弁で、複数の行為が累積をして武力攻撃と評価され得るという議論に対し、我が国の措置が武力攻撃と評価されるとの主張に「説得力がない」という見解が示されたことは注目される。我が国がどのように論理構成をしても、相手国が我が国の立場とは相いれない何らかの主張を表明する可能性は排除できないかもしれない。ただし、当該主張は「説得力がない」と、国際社会に受け入れられる主張を我が国ができるかが重要になるだろうし、この点は、そのほかの場面でも当てはまるのではないだろうか。政府の説明ぶりが重みを増すだろう。

（ふじかわ　たかあき）