参議院常任委員会調査室・特別調査室

論題	能動的サイバー防御の実施と国際法上の主な論点
著者 / 所属	寺林　裕介 / 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	479 号
刊行日	2025-10-28
頁	70-80
URL	https://www.sangiin.go.jp/japanese/annai/chousa/rippou_chousa/backnumber/20251028.html

※ 本文中の意見にわたる部分は、執筆者個人の見解です。

能動的サイバー防御の実施と国際法上の主な論点

寺林　裕介
（外交防衛委員会調査室）

１．はじめに

近年、サイバー攻撃による被害が多発し、消費者向けサービスの停止など国民生活に直接影響を生じさせる事例も増えている。また、その標的として国家の重要インフラが狙われており、そのようなサイバー攻撃が実行されることがあれば、国家の安全保障が脅かされることになる。その攻撃者についても、具体的に中国や北朝鮮などの国家の関与が疑われる事例が公表されている。

このような状況を踏まえ、日本政府は、サイバーセキュリティ政策の一環として、重大なサイバー攻撃を未然に防ぐこと、さらには被害の拡大を防ぐことを目的とした「能動的サイバー防御」を導入するために法制化を進めた。そして、2025年５月16日、第217回国会（常会）において、「サイバー対処能力強化法」（令和７年法律第42号）及び「サイバー対処能力強化法整備法」（令和７年法律第43号）が成立した[1]。後者の整備法により、警察官職務執行法及び自衛隊法の一部が改正され、サイバー攻撃による重大な危害を防止するため、警察と自衛隊による「アクセス・無害化措置」を可能とする規定が新たに設けられた。

日本政府が実施することになるアクセス・無害化措置は、公共の秩序の維持という観点か

[1] 両法律の正式な題名は、「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」及び「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」。2026年11月までに施行。なお、国会における議論を整理した榎本尚行「能動的サイバー防御２法案の国会論議（１）～（３）」『立法と調査』No.476,477（2025.7）、柿沼重志「能動的サイバー防御の導入」『立法と調査』No.474（2025.4）も参照されたい。

ら、警察権の範囲内で必要最小限度の措置として行うものであり、攻撃サーバ等にアクセスして不正プログラムを無害化する措置等が想定されている。しかし、このアクセス・無害化措置の実施が、外国に所在する攻撃サーバ等に対する行為であった場合、そのサーバ所在国から領域主権を侵害していると受け止められることがあり得る。また、こうして国際違法行為であると主張されたサイバー行動について、違法性阻却事由の要件に該当するのはいかなる場合か、各国において十分な国家実行が積み重ねられているわけではなく、どのような考え方が認められるのか判然としていない[2]。

以上の問題関心から本稿では、まず２.で日本が直面するサイバー攻撃事案について概観し、これまでの警察による対処を確認する。続く３.で、多発するサイバー攻撃に対抗するため、日本がどのような能動的サイバー防御の仕組みを構築したのか、そのアクセス・無害化措置がどのように実施されるのかを解説する。次に４.では、日本が外国に所在する攻撃サーバにアクセス・無害化措置を実施した場合、サーバ所在国はそれをどのように受け止める可能性があるのか、国際法上の論点を確認する。その上で５.では、日本の能動的サイバー防御が外国から国際違法行為とみなされたとき、違法性阻却事由が認められる余地があるのか、若干の検討を加えたい。

２．日本が直面するサイバー攻撃事案とその対応

日本社会のデジタル化の進展とともに、サイバーセキュリティ対策の重要性が一層高まっている。最近では、サイバー攻撃関連通信数や被害数が増加した。国立研究開発法人情報通信研究機構（ＮＩＣＴ）によれば、2024年のサイバー攻撃関連通信数は、観測開始以降最も多い値である１ＩＰアドレスあたり約243万パケットであり、観測パケット数の増加傾向が見られる[3]。これは各ＩＰアドレスに約13秒に１回の頻度で攻撃が試みられたことを示している。サイバー攻撃の標的として国家の重要インフラが狙われることも増えており、内閣サイバーセキュリティセンターに報告があった重要インフラ事業者等へのサイバー攻撃による被害件数は、2024年度で123件であった[4]。また、高度な技術を悪用したサイバー攻撃も目立っており、例えば、2024年におけるランサムウェアの被害報告件数は222件と高水準で推移している[5]。

警察によれば、脆弱性探索行為等の不審なアクセスの大部分は、海外を送信元とするアクセスで占められている[6]。この不審なアクセスについて、踏み台（ボット）となっているケースも含めた送信元としては、米国、中国、ブルガリア、オランダ、ロシア、ドイツといった国々が挙げられている[7]。こうしたサイバー攻撃には、具体的に中国、ロシア、北朝鮮などの国家の関与が疑われる例も数多く指摘されており、中国の関与が疑われる情報窃

---

[2] 国際法上の論点について詳しくは酒井啓亘「能動的サイバー防御の国際法上の意義と課題」『法律時報』No.1221（2025.10）、西村弓「能動的サイバー防御に関する国際法上の論点」『ジュリスト』No.1613（2025.8）、山口章浩「「能動的サイバー防御」導入と国際法上の評価」『NIDSコメンタリー』No.394（2025.8.29）など。

[3] 国立研究開発法人情報通信研究機構『NICTER観測レポート2024』（2025.2.13公開）１～２頁

[4] 第217回国会衆議院本会議録第９号17頁（令7.3.18）

[5] 警察庁サイバー警察局『令和６年におけるサイバー空間をめぐる脅威の情勢等について』（2025.3）１頁

[6] 同上５頁

[7] 同『令和７年上半期におけるサイバー空間をめぐる脅威の情勢等について』（2025.9）54頁

取を目的とした組織的なサイバー攻撃、重要インフラの機能停止等を企図したとみられるロシアや中国の関与が疑われるサイバー攻撃、暗号資産等の窃取による外貨獲得を目的とした北朝鮮の関与が疑われるサイバー攻撃の例が報告されている[8]。

このようなサイバー攻撃に対し、これまで警察では、サイバー攻撃を受けたコンピュータや不正プログラムを解析し、攻撃者の発信元を分析してきた。攻撃者のほとんどは、乗っ取った機器、すなわち踏み台（ボット）を通じて攻撃を実行しており、多段階の踏み台を組み合わせたボットネットが構築されている。国内のボットについて警察は、任意でサーバの管理者にその機能停止を依頼し、管理者の協力のもとでサーバ内の不審ファイル等の削除を試みていた。ボットが国外にも存在する場合には、国際刑事警察機構（ＩＣＰＯ）などを通じて、海外の捜査機関との間で国際捜査協力を進めるとともに、重要インフラ事業者等に情報提供を行い、類似の事案への警戒を呼びかけるなどの対応を行ってきた。また、パブリック・アトリビューションとして、攻撃者やその背後にいる国家を名指しで公表することにより、更なるサイバー攻撃の抑止を図ってきた。

しかし、近年のサイバー攻撃の巧妙化・深刻化は、防御としてのセキュリティ強化策に負担を強いており、このような攻撃への対処には限界もある。そのため、上記の対応に加え、2022年12月16日に閣議決定された国家安全保障戦略には、「能動的サイバー防御」を導入することが明記された。同戦略は、国や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アクセス・無害化措置が実施できるように、政府に必要な権限が付与されることを求めた。こうしてサイバー対処能力強化法及び同整備法が成立したことにより、サイバー攻撃による重大な危害を防止するため、警察官職務執行法第６条の２に基づく警察によるアクセス・無害化措置、また、自衛隊法第81条の３等に基づく自衛隊によるアクセス・無害化措置が実施できるようになった。

３．日本の能動的サイバー防御（アクセス・無害化措置）

次に、日本のサイバー攻撃事案を踏まえて法制化された能動的サイバー防御（アクセス・無害化措置）について解説する。

（１）サイバー攻撃の検知

警察がアクセス・無害化措置を実施する場面は、①サイバー攻撃又はその疑いがある通信・データを認めた場合であって、②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、である（警職法第６条の２第２項）。

まず、上記①について、サイバー攻撃に用いられる通信・データ又はその疑いがある通信・データを検知する必要がある。検知に必要な情報を把握するため、サイバー対処能力強化法により官民連携の強化が図られた。その一つとして、基幹インフラ事業者[9]は、特定

[8] 同上６～７頁

[9] 特別社会基盤事業者。経済安全保障推進法に基づき指定された特定社会基盤事業者（15分野の基幹的なイン

重要電子計算機のサイバーセキュリティが害されたこと又はその原因となり得る一定の事象の発生を認知したときは、所管の大臣に報告しなければならない旨が規定され(サイバー対処能力強化法第５条)、こうして政府にインシデント情報が集約されることとなる。

また、サイバー攻撃の攻撃者を追跡し、その特定を進めるため、サイバー対処能力強化法が成立したことにより通信情報の利用が可能となった。政府は、サイバー通信情報監理委員会[10]の承認を受け、通信情報を取得する[11]（同第17条、第18条、第32条、第33条)。取得した通信情報については、人による知得を伴わない自動的な方法により、調査すべきサイバー攻撃に関係があると認めるに足りる機械的情報[12]のみに選別され（同第22条、第35条)、分析が行われる。

アクセス・無害化措置の実施に当たっては、これらの情報のほか、警察庁、防衛省等が独自に収集した情報や、外国政府から提供された情報なども活用し、総合的に分析・判断されることとなる[13]。

（２）警察によるアクセス・無害化措置

上記のプロセスを経てサイバー攻撃、もしくはその予兆を認知したとき、サイバー対処能力強化法整備法による改正後の警職法第６条の２に基づき、サイバー攻撃に使用されているサーバ等が国内にある場合には、サイバー危害防止措置執行官として指名された警察官は、そのサーバの管理者や関係者にアクセス・無害化措置を命じるか、又は当該警察官自らがアクセス・無害化措置をとることができるようになった。

具体的なアクセス・無害化のイメージは次のとおりである。まずアクセス・ステップとして、攻撃に使用されているサーバに遠隔からログインを実施し、そのサーバにインストールされているプログラムを一覧し、攻撃のためのプログラムを確認する。次に無害化ステップとして、その攻撃のためのプログラムを停止・削除したり、攻撃者が当該サーバにアクセスできないよう設定を変更したりするなどの措置をとることが想定されている[14]。

また、サイバー攻撃に使用されているサーバが国外にある場合には、外務大臣と協議した上で、警察庁のサイバー危害防止措置執行官のみが当該サーバへのアクセス・無害化の処置をとることができる。すなわち、国外にあるサーバに対してアクセス・無害化措置を実施するときには、警察権を外国で執行することになる。この点について、警察法第64条第１項では、重大サイバー事案への対処に必要な職務を行う警察庁の警察官は当該職務に必要な限度で職権を行う旨が規定されているが、その職権を行う地理的範囲に関して国内

フラ事業を行う257者（2025年７月31日時点)）のうち、特定重要電子計算機を使用するもの。

[10] サイバー対処能力強化法に基づいて独立機関として設置され、通信情報取得の審査・承認やその取扱いに対する検査のほか、アクセス・無害化措置に際しての審査・承認等の事務を担う。

[11] 通信情報の利用について、サイバー攻撃関連通信の99.4％は国外に所在する攻撃用インフラから行われることから外外通信、外内通信、内外通信を対象とし、国内のみで閉じた内内通信は対象外となる。

[12] 機械的情報とは、コミュニケーションの本質的な内容ではない情報であり、例えばＩＰアドレス、送受信の日時、通信量、コマンド（指令情報)、ソフトウェアの種類、個人を識別できないように加工されたメールアドレスなど。他方、メールの本文・件名、添付ファイル、Webサイトの文章・画像などは含まれない。

[13] 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13頁（令7.4.3)

[14] 第217回国会衆議院本会議録第９号８頁（令7.3.18)

法上の制限はない。また、警察法第61条では、都道府県警察が管轄区域外にも権限を及ぼすことができる旨が規定されているが、この管轄区域外の範囲には外国の領域も含まれると解されており、警職法に基づいた権限も含めて警察力の外国における行使は国内法上否定されているものではない[15]。ただし、国内法上許されたとしても実施するためには外国の同意を必要とする[16]。なお、アクセス・無害化措置はサイバー攻撃の現実的、具体的な危険性や緊急性が認められる場合に即時強制として行われる[17]。

警察官が上記のアクセス・無害化措置をとる場合には、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。ただし、サイバー攻撃により現に重大な障害が発生している場合や、その他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、委員会に事後通知を行う。この特段の事由の例としては、攻撃の敢行予定日時が判明したが既に予定時刻が切迫している状況などが想定されている[18]。

（３）自衛隊によるアクセス・無害化措置

上記の警察による措置に加え、自衛隊法の改正により、自衛隊法第81条の３に新たな行動類型として通信防護措置が創設され、自衛隊がアクセス・無害化措置を実施できるようになった[19]。

自衛隊が通信防護措置を実施する場合、その対象は、一定の重要電子計算機（国の行政機関等、地方公共団体、基幹インフラ、防衛産業の重要な電子計算機）に対するサイバー攻撃に限られる。加えて、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と認められるものが行われた場合とする要件がある。これは、主に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が想定されている。ただし、ほかの主体によるものであっても上記の要件に当てはまれば法文上排除されていない[20]。さらに、①サイバー攻撃を受け、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が大きく、②自衛隊が有する特別の技術又は情報が必要不可欠であり、③国家公安委員会から要請又はその同意がある場合に該当することにより、自衛隊が対処を行う特別の必要があると認めるとき、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じることができる。

通信防護措置をとるべき旨を命ぜられた部隊等は、警察と共同して当該通信防護措置を実施するとともに、その職務の執行について改正後の警職法が準用される（自衛隊法第91条の３）。サイバー攻撃に使用されているサーバが国外にある場合には、処置をとる自衛官は、あらかじめ、防衛大臣を通じて、外務大臣と協議しなければならない。また、上記の

---

15 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16頁（令7.5.13）
16 第140回国会衆議院予算委員会議録第７号11～12頁（平9.2.5）
17 即時強制として行うべきであるとの考えから、警職法において即時強制の手段を規定している第４条から第６条の次に第６条の２として設けられた経緯がある（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17頁（令7.4.3））。なお、アクセス・無害化措置は、警職法第７条に規定する武器の使用に当たるものとは考えられていない。
18 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13頁（令7.4.3）
19 通信防護措置の新設のほか、在日米軍が使用する一定の電子計算機の警護のための権限規定（自衛隊法第95条の４）等が新設・追加された。自衛隊法の改正について詳しくは、藤川隆明「サイバー空間における自衛隊のアクセス・無害化措置」『立法と調査』No.477（2025.7）を参照されたい。
20 第217回国会衆議院本会議録第９号８頁（令7.3.18）

処置をとる当該部隊等の自衛官は、あらかじめ、防衛大臣を通じて、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。ただし、当該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はこの限りでない。

（４）武力攻撃事態との関係

能動的サイバー防御は、国家安全保障戦略において「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」を前提として導入することが明記された。このことから、アクセス・無害化措置は、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される。

日本政府は、サイバー攻撃のみであっても、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、これが相手方により組織的、計画的に行われる場合には武力攻撃に当たり得るとの考えを示している[21]。仮にサイバー攻撃が武力攻撃に当たる場合には、武力攻撃事態対処法、自衛隊法等に基づいて対応することになる。なお、防衛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・無害化措置に係る権限を行使できる。

４．日本の能動的サイバー防御に対する外国政府の受け止め

上記の能動的サイバー防御（アクセス・無害化措置）を日本が実施する際に、それが外国に所在する攻撃サーバ等に対する行為であった場合、サーバ所在国はこれをどのように法的に位置づけるのであろうか。以下に、サーバ所在国が主張し得る日本の国際法上の義務違反の可能性について確認していきたい。

（１）国家の主権侵害

第一に、サイバー攻撃を企図した攻撃国に対してでも、乗っ取られたコンピュータの所在国に対してでも、ある国家の領域内にあるサーバ等を標的としてアクセス・無害化措置を行ったことが、当該国家の主権侵害を構成すると主張される可能性がある。

国家主権の２つの側面（対内主権、対外主権）のうち、対内主権は領域主権とも呼ばれ、原則として国家は領域内の人や事物について管轄権を行使する（属地主義）。同時に、国家は他国の領域主権を尊重する義務を負う。タリン・マニュアル[22]では、規則１で国家主権の原則はサイバー空間において適用される、また、規則４で国家は他国の主権を侵害するサイバー行動を行ってはならない、としている。その上で、主権侵害の例として、物理的損害が生じた場合と機能の喪失が生じた場合とが挙げられている。

前記３.（２）で日本が実施する具体的な無害化のイメージを確認したように、アクセス・無害化措置では、そのサイバー攻撃のためのプログラムを停止・削除したり、攻撃者が使

---

[21] 第217回国会衆議院内閣委員会議録第７号17頁（令7.3.21）

[22] 『タリン・マニュアル2.0』は、サイバー行動に適用される国際法規について、各国の国際法専門家が検討した結果をまとめた文書。本稿では、この文書を要約した中谷和弘、河野桂子、黒﨑将広『サイバー攻撃の国際法 増補版』（信山社、2023年）の規則と解説を引用・参照した。

用しようとしているサーバにアクセスできないよう設定を変更したりするなどの実際の措置をとることになる。日本政府は、日本が実施するアクセス・無害化措置について、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われるものであり、措置の対象となるサーバ等に、物理的危害や機能喪失など、その本来の機能に大きな影響が生じることは想定していないと説明している[23]。しかし、現代ではインターネットのネットワークは複雑かつ広範に連結されて多くの活動が存在しており、日本が実施した措置によっては、その意図に反して予期しない形で相手国に被害を与える可能性もあろう。

また、サイバー空間における各国の主権侵害に関する考え方も異なっている。例えば、日本はタリン・マニュアルの考え方と同様に「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」が主権侵害に該当し得るとの立場を示している[24]。しかし、ブラジルは「他国の領域内にある情報システムに対するサイバー行動が主権侵害を構成する可能性がある」と主張し[25]、フランスは「フランスのデジタル・システムに対するいかなるサイバー攻撃も、又は国家の統制の下で行動する個人によるデジタル手段によってフランス領域内に生じるいかなる効果も、主権侵害を構成する」[26]として、より広い範囲で主権侵害を認める立場を明らかにしている。

（２）内政不干渉義務違反

第二に、国家主権のもう一つの側面である対外主権の観点から、内政不干渉義務の違反が主張される可能性がある。対外主権とは、国家が外部権力から支配を受けることなく意思を決定する権限を持つことを意味し、国家は他国の国内問題に干渉してはならないという不干渉義務が導かれる。国際司法裁判所（ＩＣＪ）は、自由な選択に関して強制の手段を用いるときに干渉は違法であると述べた[27]。

サイバー空間においても、タリン・マニュアルでは規則66で、国家は、他国の国内事項又は対外事項に、サイバー手段による場合を含め、干渉してはならない、としている。また、この干渉については、他国の国内事項又は対外事項への意図的な介入であること、さらにそれが強制を伴う介入であることを要すると説明した。

なお、タリン・マニュアルは留意事項として、あるサイバー行動が干渉を構成しなくても、それが非強制的な主権侵害となり得ることを示した。しかし、イギリスは、内政不干渉義務違反の例として、敵対的なサイバー行動による他国の選挙制度の操作、金融システムの不安定化、医療サービスへの攻撃を示しながら、その一方で、主権に関する一般原則それ自体は、内政不干渉義務を超える特定的又は追加的な禁止事項が導かれるのに十分な根拠となり得ないとした[28]。

---

[23] 第217回国会衆議院本会議録第９号８頁（令7.3.18）
[24] 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』(2021.5.28) ３頁
[25] U.N. Doc. A/76/136, United Nations General Assembly, 13 July 2021, p.18.
[26] “International Law Applies to Operations in Cyberspace,” Paper shared by France with OEWG established by resolution 75/240, UNODA, 2021, pp.2-3.
[27] ＩＣＪニカラグア判決、I.C.J. Reports 1986, p.108, para.205.
[28] U.N. Doc. A/76/136, pp.116-117. イギリスの立場は、主権の抽象概念を根拠に無限定に禁止が広がることを避け、サイバー上のスパイ行為やその他の越境措置を合法的に行う余地を残すための政策的配慮による

（３）武力行使禁止原則違反

第三に、国連憲章第２条４（武力行使禁止原則）違反である。日本政府は、日本が実施するアクセス・無害化措置について、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４が禁止する武力の行使に当たることはないとの考えを表明している[29]。しかし、一般に、いかなる行為が武力の行使に該当するのかは国際法上明確に定義されておらず、日本が実施したアクセス・無害化措置を相手国がどのように認識するかは一様ではない[30]。

もとより、日本政府は、「サイバー行動であっても、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」との立場を示している[31]。タリン・マニュアルでは規則69で、サイバー行動が武力の行使に該当するか否かの基準について、「規模及び効果」を採用している。規則71では、場合によっては「規模及び効果」ゆえにサイバー攻撃が国連憲章の定める「武力攻撃」になることを認めた。すなわち、あくまでもサイバー行動それ自体によって引き起こされる効果が武力攻撃となるものに比肩しているかどうかが、武力攻撃となるか否かを判断する決定的要因となる。なお、日本のアクセス・無害化措置には、公共の秩序の維持を目的とし、比例原則に基づいてその目的を達成するために必要最小限度の措置として行われるとする歯止めが存在することが、国会審議の中で強調された[32]。

５．違法性阻却事由（対抗措置、緊急避難）の援用

日本の能動的サイバー防御（アクセス・無害化措置）が、仮にサーバ所在国から主権侵害に該当するとして国際違法行為とみなされた場合でも、違法性阻却事由を援用してその正当化を図ることが考えられる。国家責任条文[33]は、違法性阻却事由として同意、自衛、対抗措置、不可抗力、遭難、緊急避難の６つを掲げた（国家責任条文第20条から第25条）。サイバー空間においても、タリン・マニュアルは規則19で同様の事由を列挙し、これらに該当する場合、サイバー行動を含む行為の違法性が阻却されるとした。日本政府も、国際違法行為に対して一定の条件の下で対抗措置をとること、あるいは緊急状態（緊急避難）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説明している[34]。

（１）対抗措置をとる場合の論点

国家の行為が違法な行為であっても、当該行為が対抗措置（countermeasures）を構成す

とされる（西村弓「越境サイバー対処措置の国際法上の位置づけ」『国際法研究』No.14（2024.3）68～69頁）。

29 第217回国会衆議院本会議録第９号６頁（令7.3.18）

30 国会の審議では、「日本の措置を武力の行使であるとして批判する国が、一般論として、今後出てくる可能性は理論的には否定できない」との意見陳述があった（第217回国会衆議院内閣委員会議録第９号３頁（令7.3.28）黒﨑将広参考人）。

31 前掲注24、６頁

32 第217回国会衆議院本会議録第９号11頁（令7.3.18）、参議院本会議録第14号15頁（令7.4.18）等

33 国家責任条文は、国家責任に関する一般的規則をまとめたものであり、国連の国際法委員会（ＩＬＣ）で起草され、2001年に国連総会で採決された。法的拘束力を持たないが、その多くは慣習国際法を反映している。

34 第217回国会衆議院本会議録第９号８頁（令7.3.18）

る場合には、その違法性は阻却される（国家責任条文第22条）。

第一に、対抗措置は、国際違法行為の責任を負う国に対してその義務の履行を促すためにのみとることができる（同第49条１）。対抗措置の対象は違法行為の責任を負う国家であるが、サイバー攻撃については、攻撃者の帰属（アトリビューション）の問題が惹起される。すなわち、たとえ攻撃者の発信元を特定できたとしても、国家の行為として実行されたものであるのか、政府とは関係のない私人によるものなのかを特定することが困難である。また、その責任の帰属についても、発信元が攻撃国であるのか、踏み台（ボット）として乗っ取られたコンピュータの存在する第三国なのかを区別する必要がある。タリン・マニュアルの規則20では、第三国が攻撃しているとの誤った判断に基づいて対抗措置をとった場合には違法性は阻却されないとの多数意見を示した。

他方、当該第三国には、踏み台とされていることを知りながらそのサイバー行動を終了させるために実行可能なすべての措置をとる相当の注意義務が求められる（タリン・マニュアル規則６，７）。日本政府も「たとえ国家へのサイバー行動の帰属の証明が困難な場合でも、少なくとも、相当の注意義務への違反として同行動の発信源となる領域国の国家責任を追及できる」との考え方を示している[35]。ただし、各国の見解は分かれており、例えば米国は、相当の注意義務がサイバー行動に適用されることを否定しつつも、通報された場合には合理的な措置をとるべきと主張した[36]。

第二に、対抗措置は、攻撃国によってすでにサイバー攻撃が実行されて国際違法行為が存在するときにとることができる。国際違法行為が中止された場合には遅滞なく停止しなければならない（国家責任条文第52条３）。このことから、すでにサイバー攻撃が開始されており、継続していたのであれば問題はないが、未だサイバー攻撃が実行されておらず、攻撃サーバ等を探知して可能な限り未然にアクセス・無害化を実施しようとする場合、違法性阻却事由として対抗措置を援用することが困難となる。ただし、過去に同一の攻撃国がサイバー攻撃等を繰り返し行ってきた場合など一定の要件を満たせば、対抗措置を援用する余地が存在し得るとの指摘もある[37]。

第三に、対抗措置に訴えるためには、責任を負う国に対して対抗措置をとることを通告し、当該国に交渉を申し出なければならない（同第52条１）。この手続的要件について、攻撃サーバに遠隔からログインを実施し、攻撃のためのプログラムを無害化する能動的サイバー防御の性質を考えれば、事前に攻撃国に通告することはその意義を失わせることになる。この点に関してイギリスは、事前通告は機密性の高い能力を暴露し、対抗措置の有効性そのものを損なう可能性があるとして、対抗措置をとる国が、すべての状況において事前通告を行う法的義務があるとは認識していないとの見解を表明している[38]。

---

[35] 前掲注24、６頁
[36] U.N. Doc. A/76/136, p.141.
[37] 中村和彦『越境サイバー侵害行動と国際法』（信山社、2024年）160～161頁
[38] U.N. Doc. A/76/136, p.118.

（２）緊急避難を援用する場合の論点

緊急避難（necessity）は、当該行為が、重大かつ急迫した危険から根本的利益を守るための唯一の方法であり、相手国等の根本的利益を大きく損なうものでないといった一定の要件を満たす場合に、違法性が阻却されるという考え方である（国家責任条文第25条１）。相手国の行為を理由とする対抗措置と異なり、緊急避難は外在的な事情による違法性阻却事由の一つである。

国家責任条文は、緊急避難の援用の要件として、①国の「根本的利益」を守るため、②その利益が「重大かつ急迫した危険」によって脅かされ、③「唯一の方法」であり、④相手国の根本的利益を大きく損なうものでなく（以上、同第25条１）、⑤その国が緊急避難の発生に寄与していない（同第25条２）、との５つを規定している。ＩＣＪはガブチコボ・ナジュマロシュ計画事件において、これらの要件すべてが満たされなければならないと判示した[39]。

上記の要件のうち、①の「根本的利益」については、タリン・マニュアルでは規則26で、銀行システムや防空システムなどの例に加えて、国家の安全保障等に関係する重要インフラに深刻な被害が生じた場合に援用できると説明されている。さらに、例えばドイツはサイバー攻撃の標的とされたインフラの種類やそのインフラが持つ国家全体にとっての重要性が参照されると説明し、また、オランダは電力網、給水、銀行システムなどはその範疇に入るとの見解を示している[40]。

②の「重大かつ急迫した危険」については、日本政府は、日本が実施するアクセス・無害化措置は、攻撃者が利用しているサーバ等を発見した上で、いつサイバー攻撃が行われ、重大な危害が発生してもおかしくない緊急の必要がある状況において講じることが想定されているとして、国際法上の緊迫した危険という要件を満たすと説明した[41]。しかし、中国が背景にあると指摘される組織のボルト・タイフーンの事例では、重要インフラに長期間にわたり潜伏する形でネットワーク機器への侵害行為が準備されていた。このように潜伏したマルウェアを検知したとき、どの段階で急迫性の要件を満たしているとするかは、技術的な側面も含めて難しい判断となるだろう。加えてタリン・マニュアルの規則26では、急迫性は攻撃を回避する「最後の好機」でなければならないと説明されている。

③の「唯一の方法」という要件については、その国の一方的な行動に限定されず、他国との協力行動や国際機関を通じた行動も含み得るとされる[42]。同様にタリン・マニュアルでも、他国や国際機関からの協力が得られる場合は、まずそれを利用しなければならないとする。日本政府は、アクセス・無害化措置は、例えば相手国に協力を要請するのでは被害の発生を未然に防ぐことができないなど、当該措置をとる以外に選択肢がない状況においてとられるものであると説明した[43]。

---

[39] ＩＣＪガブチコボ・ナジュマロシュ計画事件判決、I.C.J. Reports 1997, pp.40-41, para.51-52.
[40] U.N. Doc. A/76/136, pp.42,63.
[41] 第217回国会衆議院内閣委員会議録第10号９～10頁（令7.4.2）
[42] ＩＬＣ国家責任条文コメンタリ、Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, p.83, para.(15) (Article 25).
[43] 第217回国会参議院内閣委員会会議録第14号16頁（令7.5.15）

なお、サイバーセキュリティに関する国連政府専門家会合（ＧＧＥ）に提出された国際法の適用に関する各国の国別見解では、緊急避難を援用することを認めるとの意見を提出したのは15か国のうち日本、ドイツ、オランダ、ノルウェーの４か国であり、他の国の見解には言及がなかった[44]。緊急避難が主張されたとしても、ガブチコボ・ナジュマロシュ計画事件判決で違法性阻却としての援用の際の要件が慎重に検討され、結論として否定されたことからも、国際裁判所が実際に緊急避難を認めることについては、極めて慎重な態度をとっていることが指摘されている[45]。

６．おわりに

サイバー空間における国際法の適用について各国の意見に相違がある中で、アクセス・無害化措置についても、2024年に米国が実施したボルト・タイフーンによるボットネットに対する無害化措置、2019年以降にカナダが実施した攻撃者の海外サーバに対する無害化措置などの事例はあるが、各国の取組の詳細は明らかにされておらず、能動的サイバー防御が国際社会でどのように評価されるのか定まっていない。このような状況下で日本が、近年のサイバー攻撃の巧妙化・深刻化に対応するため、能動的サイバー防御を導入し、アクセス・無害化措置を実施することは、国際ルール形成への影響も大きいと考えられ、その運用が注目される。

また、能動的サイバー防御を実行していくにあたり、サイバー攻撃は各国に所在するボットを通じて実行されるケースが多いことから、第三国との協力関係や、場合によってはサイバー能力の技術支援も求められる。日本としては、サイバー攻撃への対処を強化するとともに、途上国支援を含めて同盟国・同志国との連携を通じ、日本がアクセス・無害化措置を効果的に実施できるように各国との協力関係を進めておくことも重要であろう。

【参考文献】

岩沢雄司『国際法 第２版』（東京大学出版会、2023年）
中谷和弘、河野桂子、黒﨑将広『サイバー攻撃の国際法 増補版』（信山社、2023年）
中村和彦『越境サイバー侵害行動と国際法』（信山社、2024年）
赤堀毅『サイバーセキュリティと国際法の基本』（東信堂、2023年）

（てらばやし　ゆうすけ）

[44] U.N. Doc. A/76/136.
[45] 岩沢雄司『国際法 第２版』（東京大学出版会、2023年）566頁