防衛研究所 National Institute for Defense Studies
NIDSコメンタリー
第 394 号　2025 年 8 月 29 日

「能動的サイバー防御」導入と国際法上の評価

――特に「アクセス・無害化措置」について*

政策研究部サイバー安全保障研究室　研究員　山口　章浩

要旨

「能動的サイバー防御」を導入する二つの法律が成立した。同制度により安全保障上の重要情報を扱う官民のシステムや、重要インフラに対するサイバー攻撃への対応の強化が図られる。もっとも、同制度の柱の一つである、警察・自衛隊が実施する「アクセス・無害化措置」について、外国の機器を対象とする場合の国際法上の適法性について懸念が示されてきた。

まずアクセス・無害化措置は、武力攻撃に対する自衛権行使という枠組みを前提としていない。他方で国会でも論点となったように、主権侵害となるサイバー行動の範囲については各国の間でも見解の隔たりがあり、広範に侵害を認める立場からは、当該措置が主権侵害に該当すると評価される可能性を否定できない。しかしながら、措置は重大なサイバー攻撃への対応として実施されるものであり、国際法上、対抗措置、あるいは緊急避難（緊急状態）として正当化し得る余地がある。

今後の運用において、国際法上の適法性を確保するためには、多様なサイバー攻撃シナリオを想定した段階的な対応計画の策定、措置の影響を意図した範囲に限定するための事前のテスト、さらに行為の正当性を国際社会に訴えるための一定の情報公開といった取り組みが望まれる。

はじめに

5 月 16 日、「能動的サイバー防御」を導入するための法律が成立した。メディアでも広く報じられたこの法整備は、2022 年 12 月の「国家安全保障戦略」（以下、2022 年戦略）で示された新たなサイバー安全保障方針を実行に移すための法的基盤をなすものである。

「能動的サイバー防御」の方針が採択された背景には、増大するサイバー脅威への強い危機感がある。

企業資産や個人情報の窃取、データを暗号化して復号のための身代金を脅し取るランサムウェア攻撃など、経済目的のサイバー犯罪は一層増加している[1]。サイバー犯罪に加え、外国政府機関、あるいはその支援を受けたとされる主体によるサイバー攻撃事案も過去に多く公表されており、国家安全保障上の脅威として懸念されている。ゆえに制度整備、人材育成、社会全体への啓発を含む広義の「サイバー安全保障」体制の強化が不可欠である[2]。

そこで 2022 年戦略では、サイバー安全保障の強化にあたり目指すべき指標として「対応能力を欧米主要国と同等以上に向上させる」ことが掲げられている[3]。同戦略は、この目標を実現するため「能動的サイバー防御」を導入するとして次の 3 つの施策を掲げている。①サイバー攻撃を受けた民間事業者からの情報共有と、政府による支援の強化。②通信情報を取得することで攻撃の兆候を事前に把握する仕組みの導入。③重大なサイバー攻撃が発生した際に、攻撃に用いられるサーバー等に侵入（アクセス）し、その機能を停止・除去する、アクセス・無害化措置の実施である。これらの施策を制度化するための法的基盤として二つの法律が成立した。「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」（サイバー対処能力強化法）（以下、強化法）と、同法の施行に伴う「関係法律の整備等に関する法律」（以下、整備法）である[4]。

両法は与野党の賛成多数をもって国会で可決された。2024 年 12 月時点の世論調査でも「能動的サイバー防御」導入に賛成する声は約 6 割に上り、国民の間にも一定の支持がうかがえる。しかし、その内容を「知っている」と答えた割合は限定的である[5]。国会審議に際して広く報道がなされたが、制度の背景、サイバー攻撃の手法や対応策に関する技術的知見だけでなく、憲法・行政法を含む国内法や関連国際法の理解を要するため、制度全体を把握することは容易ではない。

両法の成立に至る過程では、法案作成の段階における専門家会合や、国会審議における参考人招致など、専門的知見に基づく議論が積み重ねられた。国会審議では最終的に法案に賛成した会派からも制度の改善の余地を指摘する意見があり、衆議院通過においては将来的な見直しを行うとする修正が加えられた[6]。したがって、両法の成立をもって議論が完結するものではなく、今後も制度の運用状況に応じて継続的な見直しと改善を図っていく必要がある。

国会審議では上記の施策のうち、①官民連携の強化や、②通信情報の取得もまた議論の的となったが、外交・安全保障政策の観点からは③アクセス・無害化措置が特に取り上げられた。中でも焦点となったのは、アクセス・無害化措置が外国のサーバー等に対して実施された場合、国際法の違反にあたるのではないかということである。これに対し、政府は「国際法上、一定の状況においては許容される」と答弁している[7]。

本稿は、このアクセス・無害化措置に対する国際法上の評価と運用の在り方を検討するものである。ま

ず、サイバー攻撃の手法および外国におけるアクセス・無害化措置類似の取り組みを概観し、次に、主に整備法におけるアクセス・無害化措置に関する規定を整理する。これを踏まえ、当該措置が国際法上どのように位置付けられるかを分析し、国際法との整合性を確保するための運用の在り方について検討する。

サイバー攻撃の手法・戦術・「キャンペーン」

まずサイバー攻撃がどのように行われるかを整理しておこう。サイバー攻撃を行う主体としては、個人のサイバー犯罪者のみならず、組織化された犯罪集団、さらには外国政府の情報機関や軍のサイバー部隊などが想定される。ただし、こうした行為主体がサイバー攻撃の「引き金を引く」場面を直接観察することはできないため、攻撃に伴って残された技術的痕跡を分析し、過去の攻撃事例と比較検討するとともに、攻撃の手法や標的となった情報資産の性質等を手がかりに、実行主体の特定（アトリビューション）が試みられる。

政府機関はサイバー攻撃の実行主体を名指し、また関与したとして特定の国を非難する場合がある[8]。さらに、被害国政府は単に非難するだけでなく、中国の Volt Typhoon による米国の重要インフラ等への侵入活動について米国のサイバーセキュリティ当局その他が共同で行った注意喚起[9]のように、行われたサイバー攻撃の戦術や手法といった事案の技術的詳細を含めて公開する場合がある。もっとも、そうした戦術や手法、およびそれらの特徴と実行主体との結びつきといった知識は、サイバーセキュリティ企業が公開するサイバー攻撃の分析報告によって堆積されてきたものである。分析レポートにおいて、企業は独自の分類体系や命名規則に基づいて脅威アクターに名称を付すが[10]、戦略的目的に基づいて継続的なサイバー攻撃を行うアクターは、一般に APT（Advanced Persistent Threats）と総称されている。

そこでサイバーセキュリティ企業や政府機関が公表するサイバー攻撃の報告書から、APT の攻撃手法を読み取ることができる。これらの手法は一様ではないものの、「サイバーキルチェーン」と呼ばれる次の一連の実行段階に模式化できる。情報の窃取を目的としたサイバースパイ活動の場合、①攻撃対象を

選定する「偵察」、②電子メールやサーバーのスキャン等を通じて悪意あるコードを送り込む「デリバリー」、③悪意あるリンクをクリックさせるなどしてマルウェアを感染させる「インストール」、④感染した端末を踏み台にして組織内の他の端末に侵入し、目的のデータを探す「水平展開」、⑤取得したデータを攻撃者の管理するサーバー等に送信する「窃取」、そして、⑥不要となったマルウェアを削除するなどして攻撃の痕跡を消去する「証拠隠滅」という各フェーズで構成される（右図１）[11]。

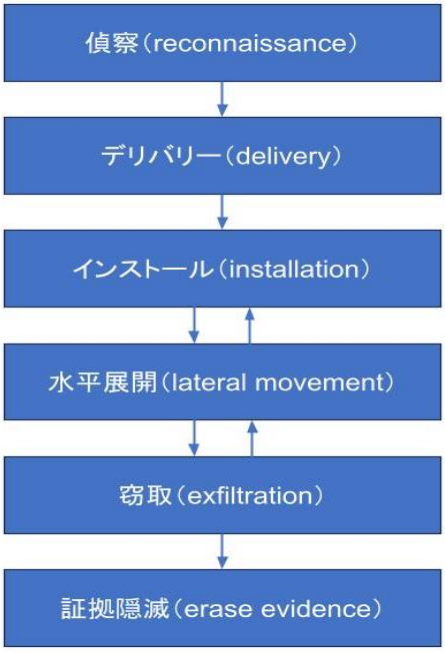

図 1　APT によるサイバースパイ活動の実施段階（キルチェーン）

出典：Timo Steffens (2020) 8 頁を執筆者翻訳。

これは秘密裡に行われるサイバースパイ活動を前提とするが、マルウェアを届け、拡散させる過程はランサムウェア攻撃や、ボットネットを利用した DDoS（分散型サービス拒否）攻撃にも共通する。ここで強調しておくべきは、サイバー攻撃は即時的に実行される行為であるかのような印象で受け止められがちだが、実際にはその目的を達成するまでの準備の過程が必要になるということである[12]。サイバー攻撃の成否は標的となるシステムのセキュリティに依存する以上、高度なセキュリティであるほどに周到な準備が必要となる。その準備には多くの時間のみならず、攻撃環境（例えば攻撃の通信元を隠すために経由する複数のサーバー）の構築、その調達のための資金、ならびに高度な専門技術を有する人員も必要となってくる。

つまり反対に防御側の視点から言えば、攻撃の目的が達成される前の実行段階で中断させることができれば、被害を未然に防止できるだけでなく、攻撃者側が投入した準備をサンクコスト（埋没費用）へと転化させることが可能となる。さらに、複数の政府機関や企業を標的とする一連のサイバー攻撃の「キャンペーン」においては、同一の攻撃手法や攻撃インフラが使い回されることもあり、これらを早期に露呈させることにより、他の潜在的な被害主体の警戒と対応を促すとともに、当該攻撃手法を「陳腐化」させ、攻撃実行に対するコストを増大させることで将来的な抑止につながると考えられている[13]。

外国における「アクセス・無害化措置」類似の取り組み

以上の考えに立てば、継続中のサイバー攻撃を終止、または被害発生前に阻止するアクセス・無害化措

置は、単発的な被害発生・拡大の防止とともに、攻撃主体に対して継続的に技術的障壁・経済的コストを賦課する手法の一つとして位置づけられる。その実施手順としては、まずサイバー攻撃の兆候を検知した上で、不正な通信を発信するサーバーや、「ボット」に感染した IoT 機器等の IP アドレスを特定し、これらにアクセスする。その後、不正なプログラムの内容を確認し、当該プログラムを消去または停止させることによって無害化を図ることが想定されている[14]。

外国におけるアクセス・無害化措置の類例として、有識者会議事務局の資料では、米国当局による KV Botnet に感染した小規模事業者・自宅オフィス向け（SOHO）ルーターを対象とした法執行活動が挙げられている[15]。この取り組みは、中国政府の関与が指摘される Volt Typhoon が、米国内からの通信に偽装し、身元を隠蔽するために、何年も前に製造され、サポートが終了した脆弱な SOHO ルーターをボットネット化して利用したことを背景としている[16]。公開された連邦捜査局（FBI）による捜索押収令状の請求文書によれば、まず FBI は、KV Botnet の通信機能を逆手に利用して、感染したルーターの IP アドレスやポート番号といった機械的情報（non-content information）を集めるコマンドを用い、世界中の感染したルーターのうち、米国内にあるもののみを選別した。なお、感染していないルーターはこのコマンドに応答しないようになっている[17]。

FBI は選別したルーター（Cisco 製と Netgear 製がその大部分を占める）に対して KV Botnet を削除するコマンドを送信した。この際、誤って他の正常なファイルや情報に影響を与えないように、Cisco 製と Netgear 製のあらゆるルーターを用いてテストした[18]。また、ボットを削除したところで旧式のルーターが脆弱であることには変わりないので、再度の感染から防ぎ、攻撃者と通信しないようにするためのコマンドも送信した。もっとも、この効果はルーターの再起動によって無効化できる、可逆的なものであるとされる[19]。当該令状請求はこれらの措置を 14 日間のうちに行うことができるよう求めるとともに、攻撃者が証拠を隠滅し、あるいはルーターの侵害を継続するためのボットの改修を行うといった、法執行活動の妨害を行わせないように、令状の発付から 60 日間の非公開を求めている[20]。また、FBI は侵害されたルーターの IP アドレスを割り当てるインターネットサービスプロバイダー（ISP）業者に通知し、ISP 業者はその顧客に通知することになっている。さらに、注意喚起と当該措置が可逆的であることを周知するため、これらの情報はウェブサイト上で公表される[21]。

この KV Botnet の駆逐は FBI が米国内で実施したものであるが、複数の国の法執行機関が協力してボットネットのテイクダウン（停止措置）を実施した例も存在する[22]。法執行機関から軍機関に視点を移すと、米軍サイバーコマンドによる作戦が関係者の話としてメディアを通じて部分的に明らかにされている。サイバーコマンドがより能動的なサイバー作戦へと 2018 年に戦略を転換した後の最初の例として知られるのが、2016 年の米国大統領選挙に干渉したと報告されているロシアのトロールファーム（偽情報を

SNS 等で拡散する組織）の Internet Research Agency に対する作戦である。2019 年 2 月の報道によれば、2018 年の米国中間選挙の投票日と集計日に、同組織を「オフライン化」したとされる[23]。

日本の「アクセス・無害化措置」の制度概要

以上の事例を踏まえ、ここからは日本におけるアクセス・無害化措置の制度について整理する。（下図 2 参照）

まずその実施主体は警察および自衛隊である。アクセス・無害化措置の制度は、警察官職務執行法（以下、警職法）および自衛隊法その他を一部改正することによって導入される。整備法により新たに設けられた警職法第 6 条の 2 では、サイバー攻撃の発生または疑いを認めたときに、「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」場合、サイバー攻撃の発信源であるサーバー等の機器に記録されている悪意のあるコードを消去するといった措置を、機器の管理者等に対して指示すること、または自らとることができる、とされる。

措置の実施に際しては、まず事前に独立の「サイバー通信情報管理委員会」の承認を得る必要がある。危害防止のための時間的猶予がない特別な場合には事前の承認は不要とされているが、事後に通知する義務があり、委員会によって措置の適切性が審査される。また、措置の対象となった機器の管理者には通知を行う必要がある。

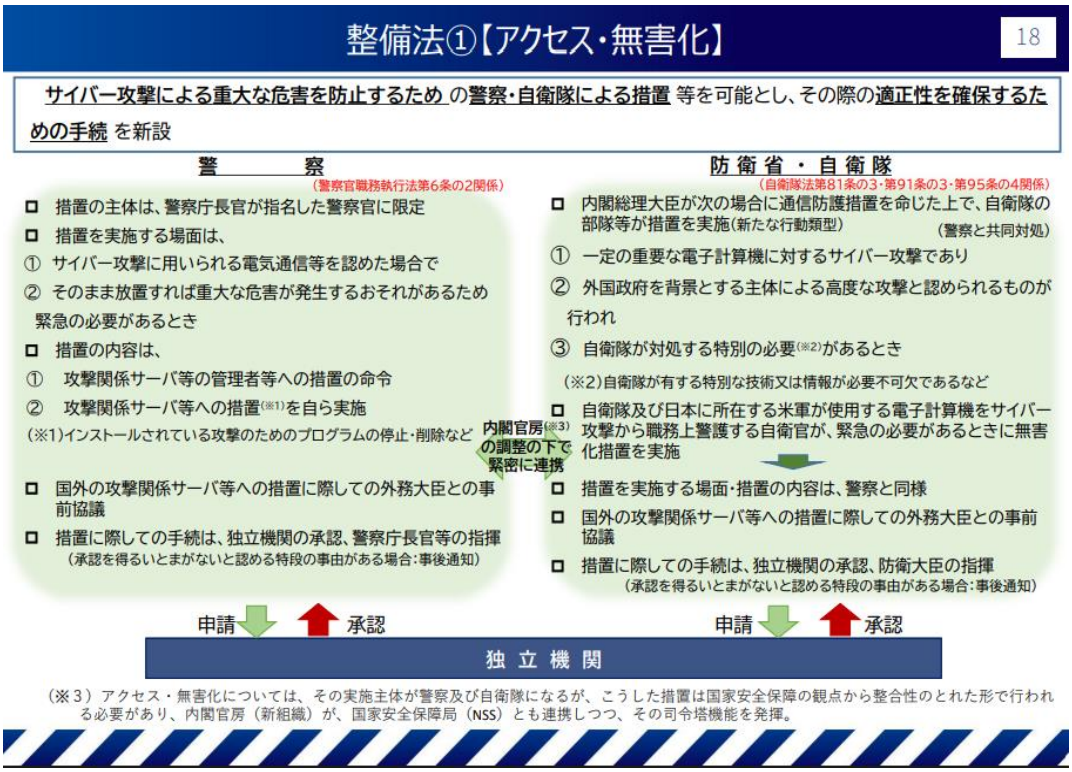

図 2　警察・自衛隊によるアクセス・無害化の概要

出典：内閣官房サイバー安全保障体制整備準備室「サイバー対処能力強化法及び同整備法について」18 頁。

自衛隊によるアクセス・無害化措置については、まず自衛隊が使用する端末・サーバー等に加え、在日米軍が使用するものが警護対象である。後者については、米軍側からの要請があり、かつ防衛大臣が承認した場合に限られる（自衛隊法第 95 条の 4）。さらに、安全保障上の「重要情報」を扱う国・地方自治体・民間のシステム、および重要インフラの制御システムを含む「重要電子計算機」を標的とするサイバー攻撃に対するアクセス・無害化措置が、「通信防護措置」（同法第 81 条の 3）として設けられた。

通信防護措置は、重要電子計算機を標的とする「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」、内閣総理大臣が自衛隊に実施を命ずることができる。その具体的な判断基準としては、以下の三点をすべて満たすことが必要とされる（第 81 条の 3 第 1 項）。

①サイバー攻撃によって「重要電子計算機」の機能が停止または低下し、当該事業の安定的な継続が困難となる結果、国家または国民の安全を著しく損なう事態が生じるおそれが大きいと認められること。②その対処のために自衛隊が有する特別の技術や情報が不可欠であること。③警察庁を所管する国家公安委員会から要請または同意があること。また、内閣総理大臣は実施を命ずるに際し、防衛大臣および国家公安委員会との協議の上で、措置の実施期間その他の実施条件を定めなければならない。

自衛隊がアクセス・無害化措置を実施する場合には、上述の警察官職務執行法第 6 条の 2 第 2 項以下の規定が準用される。すなわち、自衛隊による措置の実施に際しても、民間通信機器に対するアクセスや無害化の手順、監視・審査の枠組みなどについて、基本的に警察による措置の場合と同様の手続に従う必要がある。

このように、アクセス・無害化措置は、全般的には警察が実施するものであり、国外に所在するサーバー等も対象となる。他方、自衛隊によるアクセス・無害化措置は、自衛隊および在日米軍が使用するシステム、重要インフラの制御システム、ならびに安全保障上重要な情報を扱う政府機関・民間事業者のシステムを防護範囲とし、「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た場合に限定して発動される。ここで言う「本邦外にある者による特に高度に組織的かつ計画的な」攻撃とは、外国の国家機関、あるいは国家の支援を受けたサイバー脅威アクターによる行為を想定していると考えられる。

以上を踏まえると、警察によるアクセス・無害化措置は国内外のサイバー犯罪を主たる対象とし、国家関与型のサイバースパイ活動や重要インフラに対するサイバー攻撃の場合には自衛隊による措置実施を念頭に置いた制度設計がなされていると理解できる。もっとも、自衛隊の通信防護措置は単独ではなく、常に警察との共同によって実施されることとされており（第 81 条の 3 第 3 項）、報道によれば警察および自衛隊の合同拠点が設置され[24]、緊密な連携の下での運用が想定される。

連携・調整の観点からはさらに、外国政府が関与するサイバー攻撃への対応としてアクセス・無害化措置を実施することも考えられるところ、外交・安全保障政策全体との整合性を確保しながら措置実施を判断する必要がある。この点、内閣サイバーセキュリティセンター（NISC）を発展させる形で置かれた「国家サイバー統括室（NCO）」が、国家安全保障局（NSS）と調整しサイバー政策の司令塔としての役割を担う[25]。

最後に、サイバー攻撃の発信源となる機器が国外にある場合の措置の実施については、次に述べるように国際法との整合性を確認する必要がある。実施に際してはこれを担保するために、外務大臣との事前協議が義務付けられており、その協議結果を踏まえて独立委員会が承認の可否を判断する仕組みとなっている。

「アクセス・無害化措置」に関する国際法上の評価

これまで見てきたように、警察および自衛隊によるアクセス・無害化措置は、国内だけでなく、国外の機器も対象となる。しかしながら、このような行為を国際法上、適法な範囲で行い得るかといった疑問は国会審議においても繰り返し呈されてきた。

そこで以下では、国際法の観点から外国に所在する機器を対象とするアクセス・無害化措置の実施における適法性の確保について、次の三点を整理、検討する。第一に、アクセス・無害化措置は「武力攻撃」に該当するサイバー攻撃への対応を念頭に置いていない。そこで前提としてどのようなサイバー攻撃が「武力攻撃」に該当し得るのかを最初に確認する。

第二に、武力攻撃に対する自衛権行使の枠組みを念頭に置くものでない以上、アクセス・無害化措置は自衛権による正当化を要する「武力の行使」に該当しないように運用される必要がある。運用上これをどのように確保するかが検討される。もっとも、外国領域にある機器に対する法執行である以上、当該外国の主権との抵触が問題になり得る。いかなる越境的なサイバー行動が違法な主権侵害を構成するかについては議論があるため、これを整理する。

第三に、アクセス・無害化措置の行為自体は主権侵害となる場合であっても、重大なサイバー攻撃への対応という文脈において対抗措置または緊急避難を援用して正当化する余地がある。そこでアクセス・無害化措置の実施にそれらの違法性阻却事由を援用する場合に満たすべき要件を整理し、そのために求められる運用上の取り組みを検討する。

（1）アクセス・無害化措置の前提――「武力攻撃」に至らないサイバー攻撃への対応

アクセス・無害化措置の法的評価についてまず確認すべきは、同措置は「武力攻撃」に至らないサイバー攻撃への対応を念頭に置いていることである[26]。まずその前提として、外国からのサイバー攻撃に対する対応として国際法上想定されるのは、サイバー攻撃を法的に武力攻撃と評価し、自衛権の発動として武力の行使を含む行動をとることである。なお、この場合の反撃手段はサイバーのみに限定されず、物理的な手段も許容されることになる[27]。日本政府もかねてより外国からのサイバー行動が武力攻撃を構成する場合、自衛権を行使できる旨を明言してきた。武力攻撃へのサイバー手段による対応については、2018年の防衛大綱において、有事の際、攻撃に用いられる相手方によるサイバー空間の利用を妨げる能力の保有が明言されている[28]。

ではどのようなサイバー攻撃が、自衛権を発動し得る「武力攻撃」に該当するだろうか。「武力攻撃」に該当する行為を網羅的に挙げる普遍的な国際合意は存在せず、具体的な文脈に即して個別に判断される必要があるが、いくつかの国は、武力の行使や武力攻撃に該当するサイバー行動として、「物理的な武力の行使と同等の規模および効果をもたらす」サイバー行動を挙げている。つまりミサイル攻撃や砲爆撃のように、物理的な破壊や死傷者を伴う攻撃は、一般に、武力の行使、ひいては武力攻撃に当たるが、それと同様の被害をサイバー手段によって引き起こす場合も、手段が異なるというだけで法的評価を変える理由はないということである。例えば、物理的被害をもたらしたサイバー攻撃として、イランのウラン濃縮施設に置かれた遠心分離機を物理的に破壊したスタックスネットの事案はこの基準に該当し得るものと考えられている[29]。

しかしながら、物理的被害を直接引き起こすサイバー攻撃の事例は、これまでスタックスネット事案の他にほとんど観察されてこなかった[30]。一方で、サイバー手段は物理的手段と異なり、国境を越えることなく他国の情報システムに遠隔でアクセスでき、さらに攻撃主体の身元を秘匿しやすいといった特性を有する。このため、社会的混乱を引き起こす妨害工作（sabotage）や、産業秘密や政治・軍事的に機微な情報を標的とするスパイ活動といった目的において実行しやすく、国家間の戦略的競争における優位性を確保する手段として用いられている[31]。

ゆえに、死傷や物の破壊を引き起こす、武力攻撃と認められるサイバー攻撃に対する自衛権の発動という法枠組みは「最後の砦」として留意すべきである一方で、恒常的に繰り返されるサイバー攻撃については、発動要件となる武力攻撃の高い基準を満たさない。そこで外国による低烈度のサイバー攻撃に対する法的規律として、内政干渉または主権侵害に該当するかどうかの評価枠組が用いられてきた。しかしながら、内政干渉や主権侵害に該当するため違法であると評価しても、それは自衛権の行使を正当化するものではないため、武力の行使による対応はできない。よって外交的・司法的対応、そして武力の行使に至らない積極的な無害化の措置が可能な範囲の対応となる。

（2）単独の行為としてのアクセス・無害化措置の法的評価

（ア）「武力の行使」に該当しない想定と運用

アクセス・無害化措置は、外国の機器に対して行われる場合、対象となる外国の主権との関係が問題となる。そこでひとまずサイバー攻撃への対応という文脈から切り離して、単独の行為としての法的評価を検討する。

まずアクセス・無害化措置について、国会審議では以下のような政府答弁がなされている。

> 「今回のアクセス・無害化措置は、公共の秩序維持の観点から、警察権の範囲内で、比例原則に基づきまして、重大な危害の発生を防止するために、攻撃サーバー等にアクセスして不正プログラムを無害化する必要最小限度の措置を取るというところでございます。
>
> 例えば、このアクセス・無害化措置によって、対象となるサーバー等に対し物理的被害や機能喪失等、その本来の機能に大きな影響を生じさせるようなことは想定しておらず、状況をエスカレートさせるようなものにはならないというふうに考えているというところでございます」[32]。

この答弁から、アクセス・無害化措置は、禁止された「武力の行使」に該当しないものと想定して運用されることが読み取れる。前述のように、サイバー攻撃が武力の行使に該当するかについて、引き起こされる影響の程度等が考慮されるが、これはあらゆるサイバー行動（cyber operation）について同様である。物理的な被害は一つの基準点であるが、いくつかの国は物理的な被害に至らない、重要インフラに対する深刻な機能障害、例えば発電所へのサイバー行動によって長期間にわたり電力供給が停止するといったような事態も、武力の行使に該当する可能性があることを示唆している[33]。このように武力の行使となる基準を低く解釈したとしても、アクセス・無害化措置はそもそも外国の重要インフラシステムを対象とするものではないし、機器本来の機能に大きな影響を生じさせない運用がなされるとの前提からは武力の行使に至るものではないと想定される。

もっとも、限定的な影響に留めることを宣言するだけでなく、実際の運用においてこれを担保していく必要がある。特に異なる主体・性質のデータが同一の ICT インフラを共有していることを考えると、意図しない影響拡大を防止するための取り組みが求められる。例えば、米軍サイバーコマンドがテロ組織イスラム国（ISIS）の SNS アカウント等をハッキングしてデジタルコンテンツの利用を妨害した作戦では、ISIS のデータは民間人のコンテンツデータと同じサーバーに保管されていたため、作戦の承認のために正確に ISIS のデータだけを標的とするように示す必要があったとされる[34]。具体的な取り組みとしては、米国の KV Botnet 事例のように、措置によって他のシステムやデータに影響を及ぼさないよう事前

にテストを行うといった技術的調整が必要となろう。

（イ）主権侵害の範囲をめぐる議論と適用

武力の行使に至らないとしても、外国の機器に対するアクセス・無害化措置が、内政不干渉原則の違反あるいは、主権平等原則を支える主権の相互尊重の義務に抵触するかは別途問題となる。外国領域における同意のない法執行活動は、当該外国に対する内政干渉あるいは主権侵害として国際違法行為を構成し、その責任を追及される可能性がある。

あるサイバー行動が違法な内政干渉に至らずとも、主権侵害には該当し得ると解されるように、他国の主権を尊重する義務の適用範囲は広い。もっとも、いかなるサイバー行動が主権侵害となるかについては、各国の見解において大きく二つの見方に分かれている[35]。一つの見方は、サイバー行動によって引き起こされる影響・効果を一つの評価基準として、主権侵害の有無を判断すべきだとするものである。この考え方は、各国の国際法専門家がサイバー行動への国際法の適用について議論した成果文書である『タリン・マニュアル』の作成過程においても、多くの専門家から支持されたとされる[36]。日本政府も「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、場合によっては違法な干渉等にも当たり得るが、いずれにせよ主権の侵害に該当し得ると考える」と表明している点、この効果基準を支持しているものと解される[37]。

さらにこの考えを進めて、ドイツやカナダなどいくつかの国は、「無視し得る、あるいは最小限の効果」（a level of negligible or de minimis effects）にとどまる越境的なサイバー行動は、主権侵害には該当しないとの立場を取っている[38]。つまり、主権侵害と評価するには、当該行為が一定以上の実質的な影響を及ぼす必要があるという、効果に関する「閾値」の存在を前提とする立場である。

これに対して、アフリカ連合が昨年公表した、加盟国の「共通の立場」は、主権侵害に関する効果基準、特に「有害な効果の最小限の閾値」の存在そのものに異議を唱えている。すなわち、外国領域に所在するICT インフラに対して国家が不正にアクセスする行為については、たとえ影響が軽微であっても、主権侵害に該当すると強調している[39]。

また主権の尊重は、領域の不可侵にとどまらず、国家の政治的独立の不可侵も意味することから、国家の自国領域内における排他的な統治権能を損なうような行為は、サイバーの文脈においても主権侵害に該当するとの見解も見られる。例えば中国は、以下のような立場を表明している。すなわち、「領域内のICT 関連インフラ、主体、活動、および関連データ、情報に対する国家主権に基づいて他国が享受している対内的な優位性および対外的な独立性を侵害する場合、国際法上の違法行為となる主権原則の違反となる。そのような行為としては、とりわけ、関連インフラの混乱または損害を引き起こし、またはサイバ

ー空間における国家の排他的な主権的権利を損なう場合、他国の領域内または管轄内のネットワークシステムへの無許可の侵入（unauthorized penetration）が含まれる」[40]。

このように、自国領域内の ICT インフラに領域国の同意なく侵入・アクセスすること自体が主権侵害を構成するのか、同意がないとしても引き起こされる影響が一定の閾値以下であれば主権侵害を構成するのか、各国の見解は分かれている。アクセス・無害化措置について、前掲の国会答弁のように、「攻撃サーバー等にアクセスして不正プログラムを無害化する必要最小限度の措置」であれば、引き起こされる影響は「無視し得る」程度とも捉えられる可能性がある。実際に、影響の一定の閾値を示す解釈は西側諸国に多く、「悪意のあるサイバーアクターの有害な活動から防御するための」最小限の影響しか与えない措置をとることは国際法上禁止されないと主張して自らの行動の正当性を根拠づける、法政策的含意を示す見解もある[41]。一方で、主権の領域的性格はサイバー行動であっても変わらず、領域内の機器への同意のないアクセスそれ自体が主権侵害だと主張する立場の国からは、当該国に対するアクセス・無害化措置が主権侵害であるとの評価を受ける可能性を否定できない。もっとも、これは行為単独での法的評価であって、アクセス・無害化措置は重大なサイバー攻撃への対応措置であるという行為の文脈を考慮した法的評価を検討する必要がある。

（3）行為の文脈を考慮したアクセス・無害化措置の法的評価

これまで見てきたように、アクセス・無害化措置が国際法上、たとえ「武力の行使」に該当せず、また物理的損害が軽微であっても、他国領域内の ICT インフラに対する不正アクセス等の行為が主権侵害と評価される可能性は排除できない。そこで次に検討すべきは、仮にそのようなアクセス・無害化措置が国際法上の義務に反する行為であったとしても、それが実施される個別具体的な状況に照らして、国際法上の正当化根拠により違法性を阻却され得るかという点である。

この文脈において注目される違法性阻却事由には、主に二つの根拠が挙げられる。第一に、「対抗措置（countermeasures）」としての正当化である。これは、相手国による先行する国際違法行為に対抗して、被害国が一時的に国際法上の義務に反して行動することを認める枠組みである。第二に、「緊急避難（necessity）」の弁明であり、差し迫った重大な危険から不可欠の利益を保護するために、他国に対して一時的に国際義務に違反する行為が許容される可能性を含んでいる。

（ア）対抗措置の援用可能性

まず対抗措置としての位置付けの可能性を検討し、その要件および適用可能性について整理する。中央集権構造でない国際社会において、対抗措置は、相手国による国際義務違反に対して、被害国が自らも応報的に国際義務違反を行うことで相手国の責任を追及する、国際法上の認められた自助手段である。

また、外交官の召還や外交関係の断絶といった非友好的ではあるが、それ自体は国際法上禁止されていない（つまり違法行為ではない）「報復（retorsion）」とも区別され、行為それ自体が義務違反にあたるため、対抗措置は濫用防止の観点から均衡性等の要件を満たす必要がある。

このような対抗措置の制度は、重大なサイバー攻撃への反応としてアクセス・無害化措置を正当化するうえで有用に見える。アクセス・無害化措置が相手国による内政干渉や主権侵害といった国際法違反となるサイバー行動への反応であるならば、それを対抗措置と法的に位置づけることにより、違法性を阻却できる可能性がある。

しかしながら、重大なサイバー攻撃に対するアクセス・無害化措置の実施を対抗措置として正当化するには、解釈の不明確さゆえの適用上の困難がある。第一に、対抗措置が認められるためには、相手国による先行する国際法違反が存在している必要がある。一方で、アクセス・無害化措置の前提となるサイバー攻撃は、常に外国政府による国際法違反を構成するわけではない。日本に対する外国からのサイバー攻撃のうち、重要インフラの機能喪失をもたらすようなサイバー攻撃が外国政府によって行われたと判断できる場合、日本政府はそれを主権侵害、場合によっては違法な内政干渉とみなすことができるだろう。他方で先述のように、いかなるサイバー攻撃が主権侵害を構成するかについては各国の中でも議論が分かれており、例えば、その行為が直接に何らかの影響を及ぼすものではないサイバースパイ活動が主権侵害となるかについて評価は分かれる[42]。またこの点について日本政府の立場は明らかでない。

さらに、内政干渉や主権侵害は外国政府による行為に対する評価であり、国家に帰属しない私人による行為はそれ自体として内政干渉や主権侵害を構成するわけではない[43]。経済目的のサイバー犯罪集団やハクティビストといった脅威については、国家がそれらを支援していない限り、主権侵害に対する対抗措置という法枠組みを当てはめられないことになる。この課題に対する法的応答の一つとして、少なくない国が「相当の注意（due diligence）」義務の存在を主張していることは注目される[44]。これは、自国の領域内において私人によるサイバー攻撃が発信されていることを知りながら、その攻撃の終了・防止のためにしかるべき措置をとらなかった国家は、サイバー攻撃を自ら実行した主体でなくとも、「相当の注意」義務に違反し得るというものである[45]。サイバー行動に関する同義務の適用は未だ議論を多く残すものの[46]、アクセス・無害化措置の実施の際、この「相当の注意」義務違反に対する対抗措置として援用する可能性を指摘できる。

アクセス・無害化措置の対象国の違法行為に対する対抗措置の援用について、実践的には、今回の法整備による官民連携の強化や通信情報の取得を通じてインテリジェンスを一層蓄積し、サイバー攻撃の実行主体の特定に活用していく必要がある。サイバー攻撃のキャンペーンを継続的に監視することで、例えば過去に利用された C&C サーバーの再利用といった技術的・戦術的特徴から実行主体の特定に至る場

合がある。もっとも、偽旗作戦によって判断を誤る可能性もあり、問題のサイバー攻撃が外国政府に帰属するものなのか、帰属しない場合に「相当の注意」義務違反として構成し得るのかといった困難な評価判断を運用担当者は迫られることとなろう。

加えて、対抗措置は行われた違法行為に対する反応であるため、サイバー攻撃が発生する「おそれ」がある段階でのアクセス・無害化措置を対抗措置と性格づけられるか検討する必要がある。政府答弁においては、アクセス・無害化措置を実施する緊急の必要がある状況の一例として、「サイバー攻撃に用いられるマルウェアに感染した IoT 機器を発見した場合に、マルウェアはいまだ発動はしていないものの、当該マルウェアと C2 サーバーが定期的に通信を行っているというようなことが認められるため、攻撃者の意図次第でいつでもまさにサイバー攻撃が行えると認められる場合」と説明される[47]。この状況においては、領域内の ICT インフラに対する不正なアクセスそれ自体を主権侵害と判断するのでなければ、当該マルウェアが引き起こし得る損害の範囲や深刻さを評価したうえで、それが主権侵害または内政干渉の基準に相当するか判断する必要がある。そのうえで、当該サイバー攻撃が措置の対象国によると認められる場合、そのようなマルウェアのインストール・拡散がなされている状況をもって違法行為が行われたと判断して、対抗措置を援用することが考えられる。あるいは措置の対象国が過去に行った違法なサイバー攻撃、または他の違法行為により生じた責任が未だ履行されていないことを理由として対抗措置を援用するという可能性も考えられよう[48]。

以上のように、アクセス・無害化措置の実施において対抗措置を援用する場合、先行する違法行為の認定において困難な技術的・法的評価を伴うだろう。サイバー攻撃を検知してから被害が発生するまでの時間が限られている以上、効果的な運用のためには、多様なシナリオを想定し、事前に評価基準となる対応計画を策定する必要があると指摘できる。これは次に検討する「緊急避難」についても同様である。

（イ）緊急避難の援用可能性

緊急避難（「緊急状態」とも呼ばれる）とは、重大かつ差し迫った危険から国家の不可欠な利益を守るため、他国の権利を一時的に侵害する行為を例外的に正当化する法的根拠である。緊急避難は、従来、油濁事故や環境損害への対応において他国の権利を侵害する行為を正当化するために援用されてきた。このように緊急避難は対抗措置と異なり、相手国による国際法違反の存在を前提としない。ゆえに、能動的サイバー防御導入に係る政府有識者会議の提言においても、「『対抗措置』については、相手国の先行する違法行為の存在や被害の程度との均衡性を証明しなければならないなどの点を踏まえると、実務上、援用する違法性阻却事由としては、『緊急状態』の方が援用しやすいものと考えられる」 と、その有用性が注目されている[49]。

日本の他にいくつかの国もサイバー行動における緊急避難の援用可能性を示している。例えばドイツ

は、対抗措置や自衛権の条件が満たされない場合であっても、緊急避難によって国家は限られた状況において、悪意あるサイバー行動に対する能動的な対処行動をとり得ると述べている[50]。もっとも、それらの国による緊急避難の援用への言及は謙抑的な論調である。この点、従来から緊急避難の濫用の危険性が指摘されてきたことが留意される。つまり、原因が相手国にない場合であっても義務の不履行を正当化することができる緊急避難は、援用する国の主観的判断に大きく左右されると指摘されるのである[51]。

そこで緊急避難の援用は複数の要件により制限されている。アクセス・無害化措置への適用について特に検討を要すると考えられるのは、①不可欠な利益を、②重大かつ急迫した危険から保護するために行われる、③唯一の手段であり、④危険の発生に援用国が実質的に寄与していないとの要件である[52]。

① 保護されるべき利益が「不可欠（essential）」なものであること。国家の不可欠な利益とは、存立に関わる安全保障上の利益、国家機能の基本的維持、国民の生命・身体の保護などが典型である。重要インフラの継続的な機能は国家の不可欠な利益を支えるものである。

② 重大かつ急迫した危険（grave and imminent peril）の要件について、オランダ政府の見解によれば、「単なる支障や不便では足りず」、例えば「インターネットへの全面的なアクセス遮断」や「金融市場への深刻な打撃」といった状況がこれに該当し得るとしている[53]。ドイツやチェコも、物理的な損害に限定せず、重要インフラの機能喪失のような場合にも拡張して緊急避難の適用を肯定する立場を示している[54]。

「急迫した」とは、危険がすでに現実化していることまでは必要ではなく、損害の発生が具体的に予測される段階であっても足りる。ただし、その予測が将来の不確かな可能性にとどまる場合には、急迫性を認めることは困難である。先行研究では、重要インフラシステムへのマルウェアの侵入が確認されただけで、その作動条件や想定される損害が一切不明である段階におけるハックバックは、急迫性の要件を満たすとは言い難いとされる[55]。これを踏まえれば、対抗措置の項で例示した、マルウェアが未だ発動していない状況においては、「攻撃者の意図次第でいつでもまさにサイバー攻撃が行える」といった評価をもとに急迫性を認められよう。

③「唯一の手段（only way）」であるとの要件は、緊急避難を援用する上で立証が難しいだろう。この要件は、国家が直面する危険への対応として、当該行為以外の合理的な選択肢をとり得ないことを意味する。すなわち、他の代替的な手段が存在していたとしても、それらが実効性を欠き、危険の回避や軽減には不十分である場合に限り、唯一性が認められる[56]。加えて、先行研究では、唯一性を事後的に評価するにあたり、「後知恵バイアス」が働きやすい点が指摘されている。適切な評価は、行為時点における情報に基づく判断可能性であり、その時点で最も合理的な選択であったと説得できるかどうかである[57]。

サイバー攻撃への他の手段としては例えば、当該マルウェアへの通信の遮断やパッチの適用、司法手続を通じた対応などが挙げられる。これらの手段がアクセス・無害化の必要性を完全に代替し得ない場合、緊急避難としての措置の唯一性が肯定されると考えられる。実践的には複数の対応が並行して実施されるだろう。アクセス・無害化措置の制度を運用するにあたっては、事前に対処のためのリスク評価枠組みや行動計画を策定しておき、措置の実施・承認時には評価されたリスクに応じて、無害化に先立つ手段を講じることで合理的に必要な唯一の手段であることを証明できよう。実施後の評価においても、不公平な後知恵バイアスに基づく評価のリスクを低減し、緊急避難の濫用という懸念・批判にも説得的な弁護を提供し得ると考えられる[58]。

④ 危険の発生に実質的に寄与していないとの要件についても、発生を防止するための手段を合理的な範囲内で尽くしたかが重要となる。寄与の度合いが「実質的に」というのは緊急避難に訴える側の国に全くの落ち度がないことを意味するのではない[59]。例えば周知の脆弱性を利用した攻撃が行われ、事前のパッチ適用で未然に防止できた可能性が高い場合には、緊急避難に訴えることは合理的ではないとの批判を受けよう[60]。本要件を満たすためには不断のセキュリティの強化が求められる。

おわりに

本稿では、新たに成立した「能動的サイバー防御」関連法、とりわけアクセス・無害化措置について、その制度的背景と国際法上の評価を検討してきた。アクセス・無害化措置は、その影響を限定する運用の想定に従えば武力の行使の基準には達しないと解される。一方で、いかなるサイバー行動が主権侵害となるかについて各国の意見は分かれており、他国の ICT インフラに対するアクセス・無害化が主権侵害に該当するとの評価を受ける可能性を完全に否定できない。もっとも、対抗措置あるいは緊急避難といった違法性阻却事由を援用することで、当該措置を法的に正当化する余地がある。

いずれの根拠に基づいて措置の適法性を主張する場合であっても、要件の充足および濫用の懸念の払拭のためには、アクセス・無害化措置の実施において、緊急の対応を判断するための指針となる事前の対応計画の策定やそれを実効的なものとするための訓練・演習が求められよう。

またアクセス・無害化措置、ひいては「能動的サイバー防御」制度の運用は、発展途上にあるサイバー行動に関する国際法の形成に、日本の国家実行として寄与するものである。今回の法整備にあたり、政府有識者会議や国会において主権、対抗措置、緊急避難などに関する詳細な議論が行われた。この蓄積を踏まえ、今後、法の支配とサイバー安全保障の調和を実現するベストプラクティスとして日本の実行を国際社会に示していくことが望まれる。そのためには一定の情報公開が必要である。もっとも、安全保障上

の理由からすべての情報を公開することは困難であるため、個別具体的な事例ごとに公開する情報の範囲が検討されよう。例えば米国の KV Botnet の事例のように、国内に所在する機器を対象とする実施の場合は透明性を重視して、措置の手法も含めて公開する一方、外国国家機関に対して実施する場合は、正当性を訴える意味でも、措置の理由や目的、法的評価について発信することが現実的な選択肢として考えられるのではないだろうか。

（2025 年 8 月 18 日脱稿）

* 初期の草稿に有益な示唆を賜った、原田有主任研究官、瀬戸崇志研究員、佐々木勇人特任研究員、中村和彦先生に記して謝意を申し上げる。本稿における誤りは全て筆者の責任である。

[1] 法務省『犯罪白書　令和 6 年版』第 5 章「サイバー犯罪」第 2 節「不正アクセス行為等」209 頁。

[2] 持永大『能動的サイバー防御――日本の国家安全保障戦略の変化――』（日本経済新聞出版、2025 年）23–34 頁。

[3] 「国家安全保障戦略」国家安全保障会議・閣議決定（2022 年 12 月 16 日）21 頁。

[4] 国際法の論点を含め両法における論点を解説するものとして、『ジュリスト』1613 号（2025 年 8 月）所収の「能動的サイバー防御」特集（61–93 頁）各論考を参照。

[5] 紀尾井町戦略研究所「[オンライン調査] 能動的サイバー防御導入に賛成 59%」（2024 年 12 月 14 日）https://ksi-corp.jp/topics/survey/2024/web-research-79.html。

[6] 千葉卓朗「能動的サイバー防御法案　『通信の秘密』尊重明記　与野党修正で合意」『朝日新聞』2025 年 4 月 3 日、https://www.asahi.com/articles/AST4333PJT43UQIP00LM.html。

[7] 『第 217 回国会衆議院内閣委員会会議録』第 7 号（2025 年 3 月 21 日）平将明サイバー安全保障担当大臣答弁、https://kokkai.ndl.go.jp/txt/121704889X00720250321/165。

[8] 近年の例としては米国のサイバーセキュリティ当局その他が共同で行った、英国・EU・ドイツ・チェコが同時に発表した、ロシア軍参謀本部情報総局（GRU）に紐づけられる Fancy Bear によるサイバースパイ活動への非難声明（Federal Ministry of the Interior and Community, “Cyber Attacks Traced to Russian Military Intelligence Agency,” May 3, 2024, https://www.bmi.bund.de/SharedDocs/kurzmeldungen/EN/2024/05/schutzmassnahmen-cyberangriffe-en.html; Ministry of Foreign Affairs of the Czech Republic, “Statement of the MFA on the Cyberattacks Carried by Russian Actor APT28 on Czechia” May 3, 2024, https://mzv.gov.cz/jnp/en/issues_and_press/press_releases/statement_of_the_mfa_on_the_cyberattacks.html; Council of European Union, “Cyber: Statement by the High Representative on behalf of the EU on continued malicious behaviour in cyberspace by the Russian Federation,” May 3, 2024, https://www.consilium.europa.eu/en/press/press-releases/2024/05/03/cyber-statement-by-the-high-representative-on-behalf-of-the-eu-on-continued-malicious-behaviour-in-cyberspace-by-the-russian-federation/.）、2025 年 4 月に中国の警察当局が米国の国家安全保障局（NSA）に勤務していたとされる 3 名を指名手配したとする中国国営新華社通信の報道（“Chinese police put 3 U.S. operatives on wanted list over cyberattacks”, Xinhua, April 15, 2025,

https://english.news.cn/20250415/e7acc3bf9c404e1db06f2bb678d8e98f/c.html.）が挙げられる。

[9] Cybersecurity and Infrastructure Security Agency, “PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure,” February 7, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

[10] Kevin Townsend, “What’s in a Threat Group Name?: An Inside Look at the Intricacies of Nation-State Attribution,” *Security Week*, October 6, 2021, https://www.securityweek.com/whats-threat-group-name-inside-look-intricacies-nation-state-attribution/.

[11] Timo Steffens, *Attribution of Advanced Persistent Threats: How to Identify the Actors Behind Cyber-Espionage*, (Berlin and Heidelberg: Springer Vieweg, 2020), pp. 7–21.

[12] 一例として、2021 年 4 月にホワイトハウスがロシアの対外情報庁（SVR）によるものと公表した大規模なサイバー攻撃事案では、米国その他の国の政府機関・大企業が使用する SolarWinds 社のネットワーク監視用ソフトウェアのアップデートにバックドア型マルウェアが攻撃者によって組み込まれ、スパイ活動が行われたとされる。侵害されたアップデートは 2020 年 3 月から 6 月にかけて行われたが、発覚したのは同年 12 月であった。さらにこの攻撃のテストが 2019 年 10 月に行われた証拠が報告されており、準備から発覚までに少なくとも 1 年間を要したと報告されている。Eduard Kovacs, “SolarWinds Likely Hacked at Least One Year before Breach Discovery,” SecurityWeek, December 18, 2020, https://www.securityweek.com/solarwinds-likely-hacked-least-one-year-breach-discovery/.

[13] 佐々木勇人、瀬戸崇志「サイバー攻撃対処における攻撃『キャンペーン』概念と『コスト賦課アプローチ』――近年の米国政府当局によるサイバー攻撃活動への対処事例の考察から」『NIDS コメンタリー』第 346 号（2024 年 8 月 6 日）2–4 頁。

[14] サイバー安全保障体制整備準備室「サイバー安全保障分野での対応能力の向上に向けた有識者会議　アクセス・無害化措置に関するテーマ別会合 第 1 回 事務局資料」（資料 6–2）（2024 年 7 月 1 日）。

[15] 同上。

[16] Department of Justice, “U.S. Government Disrupts Botnet People’s Republic of China Used to Conceal Hacking of Critical Infrastructure,” January 31, 2024, https://www.justice.gov/archives/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical.

[17] Federal Bureau of Investigation, *Redacted Affidavit in Support of an Application under Rule 41(b)(6)(B) for a Search and Seizure Warrant*, case no. 4:24-mc-5018, U.S. District Court for the Southern District of Texas, filed January 8, 2024, para. 20.

[18] *Ibid.*, para. 21.

[19] *Ibid.*, para. 22.

[20] *Ibid.*, paras. 27–28.

[21] *Ibid.,* para. 30.

[22] 佐條研「マルウェア Emotet のテイクダウンと感染端末に対する通知」JPCERT/CC Eyes（2021 年 2 月 22 日）https://blogs.jpcert.or.jp/ja/2021/02/emotet-notice.html。

[23] Ellen Nakashima, “U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms,”

February 27, 2019, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

[24] 「警察・自衛隊の合同拠点新設へ　能動的サイバー防御で東京・市谷に」『産経新聞』2025 年 1 月 29 日、https://www.sankei.com/article/20250129-XZR6MBI3FNJH5L5JO3UD2FE7UU/。

[25] 内閣官房国家サイバー統括室「国家サイバー統括室の設置について」2025 年 7 月 1 日報道発表、https://www.nisc.go.jp/pdf/press/NCO0701.pdf。

[26] 「国家安全保障戦略」（2022 年）21 頁。

[27] Michael N. Schmitt ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), p. 349.

[28] 「平成 31 年度以降に係る防衛計画の大綱について」国家安全保障会議・閣議決定（2018 年 12 月 18 日）18 頁。

[29] タリン・マニュアルの作成にあたった専門家は、同事例が武力の行使に該当することで意見が一致した一方、武力攻撃かどうかについては意見が分かれたとされる。中谷和弘、河野桂子、黒崎将広『サイバー攻撃の国際法――タリン・マニュアル 2.0 の解説――[増補版]』（信山社、2023 年）88 頁（担当執筆：黒崎将広）。

[30] 物理的な被害をもたらした数少ない事例の一つとしては、Predatory Sparrow によるイランの鉄鋼メーカー企業へのサイバー攻撃事案がある。Joe Tidy, “Predatory Sparrow: Who are the hackers who say they started a fire in Iran?,” BBC, July 11, 2022, https://www.bbc.com/news/technology-62072480.

[31] *See* Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace* (Oxford: Oxford University Press, 2022).

[32] 『第 217 回国会衆議院内閣委員会会議録』第 6 号（2025 年 3 月 19 日）飯島秀俊（内閣官房内閣審議官）政府参考人答弁、https://kokkai.ndl.go.jp/txt/121704889X00620250319/53。

[33] 例えばシンガポールは次の見解を示している。「また、特定の限定的な状況下では、悪質なサイバー活動は、その規模や効果を考慮して、必ずしも死傷、物理的な損害または破壊を引き起こさない場合でも、武力攻撃に相当する可能性がある。その例としては、シンガポールの重要インフラを継続的かつ長期的に機能不能にする標的型サイバー作戦が考えられる。」Singapore’s Statement in Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security Established Pursuant to General Assembly Resolution 73/266, A/76/136 (July 13, 2021), p. 84.　またオーストリアは、物理的な効果を伴わないサイバー武力行使として次の例を示している。「B 国が A 国にある発電所に対してサイバー活動を実施した。この発電所は A 国の人口と政府インフラの大部分が依存している。結果的に発電所は深刻な損害を受け、電力供給が回復するまで数時間にわたる停電が発生した。このようなサイバー活動は違法な武力の行使に該当する。」”Position Paper of the Republic of Austria: Cyber Activities and International Law,” April 2024.

[34] Dina Temple-Raston, “How the U.S. Hacked ISIS,” NPR, September 26, 2019, https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis.

[35] Harriet Moynihan, “The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention,” Chatham House Research Paper (December 2019), p. 24, https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks.

[36] Michael N. Schmitt ed., *Tallinn Manual 2.0*, pp. 20-21.

[37] 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」 3 頁。

[38] 「いずれの場合においても、ある一定の影響閾値を下回る無視できるほどの物理的影響や機能的障害は、それ自体として、領域主権の侵害を構成するものとはみなされ得ない。」Federal Government of Germany, “On the Application of International Law in Cyberspace,” March 2021, p. 4; 「領土主権の規則は、何らかの機能喪失を含む、他国で効果を生じさせるすべてのサイバー活動に同意を必要とするわけではない。無視できる程度の、または最小限の効果しか及ぼさない活動は、サイバーまたは非サイバーの文脈で行われたかに関係なく、領域主権の侵害を構成しない」。「おそらく領土主権の侵害にあたらない」サイバー活動の例として、OS の再起動または再インストールを必要とするサイバー活動が挙げられている。Government of Canada, “International Law Applicable in Cyberspace,” paras. 14–19, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng, last modified April 22, 2022.

[39] 「サイバー空間において適用される、国家の領域主権を尊重する義務は、外国領域に所在する ICT インフラへの国家による不正なアクセスが、それ以下であれば違法とならないような、有害な効果の最小限の閾値（de minimis threshold of harmful effects）を含まないことを強調する。」African Union, “Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace,” January 29, 2024, para. 16.

[40] Ministry of Foreign Affairs, “China’s Views on the Application of the Principle of Sovereignty in Cyberspace,” December 2021, p.3.

[41] 例えばニュージーランドは、「サイバーの文脈で適用される領域主権のルールは、悪意のあるサイバー主体の有害な活動から防御するために、最小限の破壊的な効果（minimally destructive effects）を伴う必要な措置をとることを国家が禁止するものではない」との考えを示している。Ministry of Foreign Affairs and Trade, “The Application of International Law to State Activity in Cyberspace,” June 17, 2025, para. 14.

[42] 中谷和弘「サイバー諜報と国際法」『国際法外交雑誌』第 122 巻第 1 号（2023 年 5 月）7–11 頁。

[43] Michael N. Schmitt ed., *Tallinn Manual 2.0*, p. 17.

[44] 参照、赤堀毅『サイバーセキュリティと国際法の基本――国連における議論を中心に――』（東信堂、2023 年）40–44 頁。

[45] Michael N. Schmitt ed., *Tallinn Manual 2.0*, Rule 6, p. 30.

[46] どのような場合にサイバー攻撃の防止・終止のための「相当の注意」を払って行動したといえるかは明確でなく、今後の検討課題である。See *Ibid.*, pp. 43–50. その評価は国の能力に照らした相対的なものであると考えられる一方、評価の指標となる規範の形成が望まれる。

[47] 『第 217 回国会衆議院内閣委員会会議録』第 6 号（2025 年 3 月 19 日）飯島秀俊（内閣官房内閣審議官）政府参考人答弁、https://kokkai.ndl.go.jp/txt/121704889X00620250319/51。

[48] 過去の違法なサイバー攻撃について「未だ賠償等による回復を行っていない場合には,,,新たな越境サイバー侵害行動が実行される前であっても対抗措置を援用する余地が存在し得る」との指摘は、中村和彦『越境サイバー侵害行動と国際法――国家実行から読み解く規律の行方――』（信山社、2024 年）160–161 頁。相当の注意義務違反に対する対抗措置については 168–172 頁を参照。「先行違法行為の存在をサイバーの文脈に限らず広く対象所在国に見出すことができるかもしれない」との指摘は、黒崎将広「能動的サイバー防御の国際法枠組み――武力未満と違法性阻却による正当化の可能性――」『国際問題』No. 716（2023 年 12 月）33 頁。

[49] サイバー安全保障分野での対応能力の向上に向けた有識者会議「サイバー安全保障分野での対応能力の向上に向けた提言」（2024 年 11 月

29 日）https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/index.html；酒井啓亘「アクセス・無害化措置と国際法の関係――能動的サイバー防御（ACD）の国際法上の評価――」サイバー安全保障分野での対応能力の向上に向けた有識者会議第 1 回アクセス・無害化措置に関するテーマ別会合資料 6–5（2024 年 7 月 1 日）https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/index.html。

[50] Federal Government of Germany, “On the Application of International Law in Cyberspace,” March 2021, p. 14

[51] 兼原敦子「国家責任の追及要件」柳原正治、森川幸一、兼原敦子『プラクティス国際法［第 3 版］』（信山社、2017 年）180–181 頁。

[52] International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, *Yearbook of the International Law Commission*, 2001, vol. II (Part Two), p. 80.

[53] Ministry of Foreign Affairs, “Appendix to the Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace”, pp. 7–8.

[54] Federal Government of Germany, “On the Application of International Law in Cyberspace,” March 2021, pp. 14–15; Ministry of Foreign Affairs of the Czech Republic, “Position paper on the application of international law in cyberspace,” (September 26, 2019), para.68.

[55] 中村『越境サイバー侵害行動』196 頁。

[56] 先行研究では唯一性について、重大な危険を防ぎ得る同程度の可能性をもつ複数の選択手段があるときに、他国の利益を最も少なく侵害する手段が選ばれるべきだとされる。とはいえ、成功率についての共通の基準はなく、サイバーの文脈における技術的な複雑さやアトリビューションの困難さから、絶対的な成功を求めれば緊急避難の援用は実質的に不可能になるとして、実務的には同様の状況において合理的な国が行動するように行動したが適用基準になるとされる。Louise Arimatsu and Michael N. Schmitt, “The Plea of Necessity: An Oft Overlooked Response Option to Hostile Cyber Operations,” *International Law Studies*, vol. 97 (2021), p. 1192.

[57] Henning Lahmann, “The Plea of Necessity in Cyber Emergencies,” *Nordic Journal of International Law*, vol. 92, issue 3, pp. 430–433.

[58] *Ibid*., pp. 434–435.

[59] ILC, Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, p. 84, para. 20.

[60] 中村『越境サイバー侵害行動』197–198 頁。

PROFILE

山口　章浩

政策研究部サイバー安全保障研究室　研究員

専門分野：国際法、サイバー領域に関する安全保障

防衛研究所企画部企画調整課

直　通：03-3260-3011
代　表：03-3268-3111（内線 29177）
防衛研究所 Web サイト：www.nids.mod.go.jp