能動的サイバー防御の地平
──国際法上の可能性と取り得る措置の選択──

原田　有

＜要旨＞

日本のサイバーセキュリティ政策において、「能動的サイバー防御（ACD）」が政策的議論の的になっている。そもそも ACD という概念は、受動的防御（セキュリティプログラムのアップデートなど）では対処できない脅威の増大を背景に生み出された。しかし、攻撃に当たる措置も含むのかといった点で共通理解に欠くなど、ACD は「受動的防御を超えた何らかの能動的措置」を意味するにとどまる不定形な概念となっている。加えて、能動的措置を他国領域で実施する際の国際法上の整理が未確定であることもあって、ACD の効果や抱えるリスクは見通せない部分も残す。それゆえ、ACD は特効薬と呼べるような取組とは言い難い一方、高まる脅威への現実的な対処策と捉えられている。日本としても国際法の可能性と取り得る措置を探りながら、許容できるリスクの程度やその他の国情に照らして自国にとり適切な ACD の地平を切り開いていくことが求められている。

はじめに

日本の 2022 年 12 月改定の『国家安全保障戦略』での言及を受けて[1]、「能動的サイバー防御（ACD）」[2] が注目を集めている。先行研究の中には、日本の ACD を、米国が導入する、攻撃源のより近く、他国領域での展開を前提とする「前方防衛」（後述）と近似した構想と位置付ける論考もある[3]。その背景には、同戦略で、ACD に資する措置の 1 つとして、「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」することが言

1 内閣官房『国家安全保障戦略』（2022 年 12 月）21–22 頁、https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-j.pdf。なお、本稿は 2024 年 12 月までの事象を踏まえて執筆したものである。
2 Active Cyber Defense の略称。
3 永野秀雄「我が国における能動的サイバー防御の構築に伴う法と組織―米国との比較を踏まえた基本的検討―」金沢工業大学国際学研究所編『分断・多元化世界と国際関係』（内外出版株式会社、2023 年）179–216 頁。

及された事実がある[4]。他方、日本政府が立ち上げた ACD に関する有識者会議での「侵入・無害化」措置に関する議論をみると、確かに他国領域での活動も論点に含めつつ、必ずしもそうした活動を所与としていないようにも見受けられる[5]。日本における ACD の構成要素は議論の途上といえるが、そもそもサイバーセキュリティに関する一般的な議論を参照しても、ACD に含まれる措置や意義は自明ではない。ACD は、受動的防御（セキュリティプログラムのアップデートやファイアウォール設置など）では対処できない脅威の増大を背景に登場した概念だが、例えば攻撃者のネットワークへ侵入・反撃するような攻撃的な措置も ACD に含むか否かといった点で論者によって見解が分かれるなど、その定義は明確ではない。

こうしてみると、「ACD はどのような取組と理解でき、いかなる課題を抱えるのか」という疑問が浮かぶ。ACD に関する一般的な理解を深めることは、日本の取組を検討する際の資となる。そこで本稿では、ACD の概念や国際法上の論点を整理するとともに、事例として取組を先駆的に進めてきた米国をとりあげる。それによって、ACD は特効薬ではなく、むしろ不透明な効果と見通せないリスクを抱えているものの、高まる脅威への現実的な対処策となっていることを論じる。そして、各国は国際法の可能性と取り得る措置を探りながら、許容できるリスクの程度やその他の国情に照らして適切な ACD の地平を切り開いていくことが求められていることを示し、本稿を通じて日本の取組への示唆を得たい。

以下、第 1 節では、ACD の概念と国際法上の論点について先行研究を踏まえながら概観する。ACD は、想定される措置や実施主体といった点で定義が明確ではなく、敢えて概念化すれば、「受動的防御を超える何らかの能動的措置によって、攻撃による被害を未然に防ぐ、あるいは被害の拡大を防いで、サイバー空間上の脅威に対処しようとする取組」を指す。そうした取組の効果は自明ではなく、また、特に自国領域外での能動的措置の国際法上の合法性は議論の途上にあることもあって、ACD は想定外の事態のエスカレーションを招くリスクも抱える。他方、高まる一方のサイバー脅威にもはや受動的防御だけでは対処しきれない現状もある。第 2 節では、ここ 10 年ほどで先駆的に能動的措置を講じてきた米国を事例研究する。米連邦捜査局（FBI）

4『国家安全保障戦略』21–22 頁。

5　有識者会議の提言書では、「攻撃主体や攻撃に用いられるサーバなどの機器が海外に所在」した場合に「アクセス・無害化は国境を越えて実施され得る」（提言書では「侵入」ではなく「アクセス」との表現が用いられている）と記述されており、「侵入・無害化」措置が実施されるあらゆる場合に他国領域での活動が前提となる訳ではないことを示唆している（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]10–14 頁、https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/koujou_teigen/teigen.pdf）。有識者会議の詳細は次を参照。「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」内閣官房、https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/index.html。

と米サイバー軍（USCYBERCOM）が即応性をもってより能動的な措置を講じられるよう、その権限が整備され、実任務へと反映されてきたことを踏まえつつ、米国内での論争、特に日本にも示唆的な事項について確認する。そして最後に、本稿から導出される日本の取組に関する気付きを示してまとめとする。

1．ACD の概念と国際法上の論点

（1）不定形な ACD の概念

ACD の概念についてよく参照される先行研究の 1 つに、2016 年に米ジョージワシントン大学サイバー・国土安全保障センター（CCHS）が公表した報告書がある[6]。同報告書において ACD は、受動的防御と攻撃の狭間に位置する、先回り的に実行される措置と位置付けられた。受動的防御とは、防御者自身のネットワーク内で実施される措置で、ファイアウォールの設定、ウィルスソフトのインストールなどを指す。一方の攻撃は、防御者自身のネットワーク外で実施される措置で、「行為を強制する、コストを課す、能力を削ぐ、あるいは許可なく保護されている情報にアクセスする」ことを目的とする。具体的には、相手に損害を与えるべく実施されるハックバックやマルウェアの使用などが該当する[7]。

一部の先行研究では攻撃的な要素を含むところにこそ ACD の意義はあるとされるが[8]、CCHS の報告書では ACD はあくまで攻撃には至らず、受動的防御により近く実行時のリスクが低いものから、攻撃により近くリスクの高いものまでの幅広い措置が想定されている。例えば、防御寄りの措置には、脅威に関する情報の共有、ネットワーク上の隔離された領域での攻撃者の行動の観察・情報収集（サンドボックスやハニーポット）、偽情報を掴ませることで攻撃者に混乱を与える欺瞞などがある。他方、攻撃寄りの措置としては、マルウェアに感染したコンピュータを特定し、防御すべきネッ

6 “Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats,” Center for Cyber and Homeland Security (CCHS), The George Washington University (October 2016), https://wayback.archive-it.org/5184/20190103002934/https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/CCHS-ActiveDefenseReportFINAL.pdf.

7 Ibid., p. 9. なお同報告書では ACD ではなく、能動的防御（Active Defense）と表現されている。

8 Robert S. Dewar, “The ‘Triptych of Cyber Security’: A Classification of Active Cyber Defence,” in *Proceedings: 2014 6th International Conference on Cyber Conflict*, eds., P.Brangetto, M.Maybaum, and J.Stinissen (June 2014), p. 13, https://ccdcoe.org/uploads/2018/10/CyCon_2014.pdf. 日本のサイバーセキュリティ専門家も、ACD に関する昨今の議論は攻撃的なオペレーションを含むものへと変化してきたことを指摘する（佐々木勇人「『能動的サイバー防御』は効果があるのか？－注目が集まる offensive なオペレーションの考察－」JPCERT/CC［2023 年 8 月 29 日］、https://blogs.jpcert.or.jp/ja/2023/08/effectiveness-of-active-cyber-defense.html.）。

トワークとの接続を切断する行為（ボットネットのテイクダウン）、攻撃者やその背後にいる他国政府を対象とする経済・金融制裁、攻撃者のネットワークに侵入して窃取された情報の救出を試みる行為などが挙げられている[9]。

なお、ACD の実行主体は理論上、国家に限定されるとは限らない。米国では最近、ACD は非国家主体による取組の文脈で言及されることが目に付き、CCHS の報告書も民間セクターによる措置を念頭に置くものであった。さらに 2019 年には、採決には至らなかったものの、企業などによる ACD を可能にするための「能動的サイバー防御確実性（ACDC）法」案も米議会下院の委員会に付託されている[10]。

こうしてみると ACD は、含まれる措置や実施主体の面で考え方に幅がある、不定形な概念であることが分かる。敢えていえば、ACD は「受動的防御を超える何らかの能動的措置によって、攻撃による被害を未然に防ぐ、あるいは被害の拡大を防いで、サイバー空間上の脅威に対処しようとする取組」といえる。多様な措置を含み得る概念であることもあって、ACD がサイバーセキュリティ上でどのような効果を生むのかは自明ではなく、議論の的になっている[11]。例えば、脅威情報の共有には一定の効果が期待できそうであるが、攻撃自体を停止できる訳ではない。一方、ボットネットのテイクダウンは攻撃の停止も含むより高い効果を生み出しそうであるが、攻撃の停止は一時的なものにとどまる可能性がある。その上、防御側のネットワーク外、特に自国領域外での措置となれば国際法上の合法性も問題となるなど付随するリスクは高くなる。

（2）ACD に関連する国際法上の論点

サイバー空間への国際法の適用方法は議論の途上にあるが、ACD の文脈では特に、「国際法上の武力攻撃には至らないサイバー攻撃に対する自国領域外での措置」の合

9 “Into the Gray Zone,” pp. 9–12. 攻撃者のネットワークに侵入して窃取された情報の救出を試みる行為は前述のハックバックと似ているが、救出行為が純粋に盗まれた情報の救出を目的とするのに対して、ハックバックは攻撃者のネットワークに損害を与えることに目的を置く点で異なっていると CCHS の報告書では整理されている（Ibid., p. 12.）。

10 “US HR3270: Active Cyber Defense Certainty Act,” Bill Track (June 2019), https://www.billtrack50.com/BillDetail/1133039.

11 佐々木勇人「『積極的サイバー防御』（アクティブ・サイバー・ディフェンス）とは何か―より具体的な議論に向けて必要な観点について―」JPCERT/CC（2022 年 9 月 21 日）、https://blogs.jpcert.or.jp/ja/2022/09/active-cyber-defense.html#footnote_1。

法性が争点となる[12]。その際の第一の論点は、武力攻撃未満のどのようなサイバー攻撃が国際法上の違法行為となるのかである。国家責任条文草案によると、国際違法行為は、国際法上で国家に帰属し、かつ国際義務に違反する行為である場合に存在する[13]。受けたサイバー攻撃が国際違法行為を構成するのであれば、被害国は、通常であれば違法行為に当たるような対抗的な措置を講じたとしてもその違法性が阻却され得る。

より具体的にみると、先行研究では国際義務に違反する行為に関しては主権原則が注目されている。タリン・マニュアルに関する議論をけん引してきた英レディング大学教授のマイケル・シュミット（Michael Schmitt）によれば、主権原則に反するサイバー攻撃には、標的国に物理的損害や死傷を与える行為はもとより、当該国の情報通信インフラの機能を特に永続的に喪失させる行為も含まれ得る。その他にも、本質的な政府の機能（国家のみが行使できる権限）である選挙、法執行活動、国防などに介入する行為も主権原則に反し得る。例えば、選挙に用いられる機器の妨害や軍の早期警戒レーダーへの介入、許可を得ずに他国の領域内で実施される遠隔捜査などが該当する[14]。もっとも、どのような行為が主権原則に反するかについての統一的な理解はまだなく、例えばフランスは主権侵害の閾値をより低く設定している。すなわち、他国が関与する、フランスのデジタルシステムに対するサイバー攻撃やデジタル的な手段でフランス領域内に効果を及ぼす行為も主権の侵害に当たるとする[15]。

他方、国際法上の違法行為を不干渉原則の観点から議論する立場もある。例えば英国は、「主権と不干渉原則は同じコインの表と裏」とした上で、不干渉原則に抵触する行為こそが違法行為に当たるとし、平時にあってはたとえ敵対的な行為であったとし

12 現時点で国際社会に国際法の適用に関する統一的な見解は存在しない。本稿では主として、日本や米英などの政府見解や専門家の見解を参照する。日米英豪を含む各国のサイバー空間への国際法の適用に関する見解がまとめられた資料は次を参照。United Nations General Assembly, *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), available from undocs.org/A/76/136.

13「国際違法行為に対する国家責任（国家責任条文草案）」第 3 条、University of Minnesota Human Rights Library、http://hrlibrary.umn.edu/japanese/JWrongfulActs.html。

14 Durward E. Johnson and Michael N. Schmitt, “Responding to Proxy Cyber Operations Under International Law,” *The Cyber Defense Review* 6, no. 4 (Fall, 2021), pp. 15–33, especially, pp. 18–19; Michael Schmitt, “NATO Response Options to Potential Russia Cyber Attacks: Understanding the Legal Framework,” Just Security (February 24, 2022), https://www.justsecurity.org/80347/expert-backgrounder-nato-response-options-to-potential-russia-cyber-attacks/.

15 ”International Law Applies to Operations in Cyberspace Submitted by France,” UN Office for Disarmament Affairs (UNODA) (December 2021), p. 3, https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf.

ても違法な干渉でなければ必ずしも違法行為には当たらないとする[16]。そもそも違法な干渉とは、国家の留保分野に対する他国の強制的な干渉を指し[17]、不干渉原則に抵触するサイバー攻撃とは強制性の要件を満たす攻撃となる。英国は強制性の定義は広く捉えることができるとして、例えば、「エネルギー安全保障、必須の医療、経済的安定、民主的プロセス」などを妨害するサイバー攻撃も不干渉原則に抵触するとの見方を示している[18]。英国の見解は、フランスの立場や、違法な干渉に当たらずとも主権侵害を構成するサイバー攻撃が存在するとの日本の立場[19]とは異なっている。なお北大西洋条約機構（NATO）のドクトリンも、武力行使や武力攻撃に該当せずとも主権原則に反するがゆえに国際法違反となるサイバー空間上の活動も存在し得るとの立場に立つが、加盟国内で英国のみそうした立場を留保し、違法な干渉を違法行為の基準にすべきとしている[20]。違法性が問われる余地を局限しようとする英国の際立った立場からは、サイバー空間上での活動の自由を最大化することでサイバーセキュリティ上の活路を見出そうとする英国の姿勢が垣間見える。

主権原則・不干渉原則以外にも、武力行使禁止原則に抵触するサイバー攻撃も国際義務の違反を構成し得る。武力行使の中でも「最も重大な形態」は武力攻撃に該当し、個別的・集団的自衛権の発動対象となる[21]。一方、武力攻撃には至らないものの、武力行使には該当するために違法性が問われる行為も存在する[22]。

16 Attorney General's Office and the Rt Hon Suella Braverman KC MP, "Speech: International Law in Future Frontiers," Gov. UK (May 2022), https://www.gov.uk/government/speeches/international-law-in-future-frontiers.

17 留保分野とは、国家の政治的・経済的・社会的、及び文化的システムの選択並びに、外交政策の策定といった、国際法上で国家の管轄事項となっている分野を指す。この点は次を参照。Johnson and Schmitt, "Responding to Proxy Cyber Operations Under International Law," p. 19; 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―』（信山社、2018 年 4 月）71–73 頁。

18 Attorney General's Office and the Rt Hon Suella Braverman KC MP, "Speech: International Law in Future Frontiers."

19 外務省『サイバー行動に適用される国際法に関する日本政府の基本的な立場』（2021 年 5 月 28 日）2–3 頁、https://www.mofa.go.jp/mofaj/files/100200951.pdf。

20 NATO Standardization Office, "NATO Standard AJP-3.20: Allied Joint Doctrine for Cyberspace Operations," Edition A Version 1 (January 29, 2020), pp. V, 20, https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf. なお、サイバー空間への主権原則の適用に関する米国の見解は明確ではないが、ドクトリンで示された NATO としての考え方に英国のような留保は示していない。他方で米国は、「他国の領域に所在するコンピュータやネットワーク機器も含む遠隔サイバーオペレーションは、当然に国際法違反を構成しない」との考えも示している。また、インターネットの仕組み上、他国の領域にある程度侵入することはやむを得ないとし、特に「他国領域に何らの影響も与えない、あるいは大した効果を与えない」活動は許容され得るとの立場に米国はある。米国の主張は次を参照。A/76/136, p. 140.

21 中谷、河野、黒崎『サイバー攻撃の国際法』77–79 頁。

22 あるサイバー攻撃が武力の行使に当たるか否かは、攻撃の「規模及び効果」に基づき事例ごとに判断される（Johnson and Schmitt, "Responding to Proxy Cyber Operations Under International Law," p. 19.）。なお、「ある政府への信頼を揺るがすことだけを企図した非破壊的な心理的サイバー行動や、経済への負の影響を引き起こすことを企図した電子商取引の禁止だけでは武力の行使にならない」とされる（中谷、河野、黒崎『サイバー攻撃の国際法』75 頁）。

なおシュミットは、受けたサイバー攻撃の違法性を問うに際しては、主権原則の適用が現実的との見方を示している。それは、不干渉原則では強制性が、武力行使禁止原則では相対的に重大な危害が標的国に加えられることが要件となるため、これら原則に基づく形では相手国の違法行為を認定するハードルが高くなってしまうからである[23]。

さて先の国家責任条文草案にある通り、受けたサイバー攻撃を国際違法行為と認定するためには、当該攻撃が国際義務違反に当たることに加えて、当該攻撃の責任を国家に帰属できるかどうか、いわゆるアトリビューションも要件となる。シュミットらによれば国際法の理論上では、当該攻撃者が国家の指示や指揮・統制下で活動している場合、組織や資金、作戦内容の面で国家に完全に依存している場合、国家から権限を付与されているといった場合には、攻撃の責任を国家に帰属できる余地が生まれる[24]。

しかし、実際に帰属を証明することは難しい。そこで欧米諸国は、被害国の政治的な判断としてサイバー攻撃の責任を特定の国家に帰属させる、政治的アトリビューションの意義を主張する。その際、被害国は、技術的な情報だけでなく、インテリジェンス活動から得られた情報なども加味した総合的な判断を行うことになる。なお米英は、そうしたアトリビューションの実施には慎重な判断が求められるとしつつも、判断の証拠を公表する国際法上の義務はないとの立場も示している[25]。

もっとも、政治的アトリビューションを可能にする情報や体制をすべての国が備えている訳ではない。そこでアトリビューション問題の現実的な打開策として、「相当の注意」義務のサイバー空間への適用も提起されている。「相当の注意」義務とは、非国家主体による行為が「国の行為に帰属しないときでも、つまり、あくまで私人の行為にとどまる」ときでも、「国家が私人の侵害行為を防止するために適当な措置をとらなかったとき」には「当該国家の国際法上の責任」を問うことができるというものである[26]。日本はこの考え方をサイバー空間にも適用し、「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

23 Michael Schmitt, “Three International Law Rules for Responding Effectively to Hostile Cyber Operations,” Just Security (July 13, 2021), https://www.justsecurity.org/77402/three-international-law-rules-for-responding-effectively-to-hostile-cyber-operations/.
24 より詳細な議論は次を参照。Johnson and Schmitt, “Responding to Proxy Cyber Operations Under International Law,” pp. 20–22.
25 A/76/136, pp. 117, 141.
26 杉原高嶺『基本国際法』第3版（有斐閣、2018年）275–276頁。

信源となる領域国の国家責任を追及できる」ようにすべきとの考えを示している[27]。

受けたサイバー攻撃が国際違法行為に該当する場合、あるいはしない場合であっても、被害国が取る措置の国際法上の根拠も論点となる。この根拠について、既存研究では主に次の 3 点が議論されている[28]。

1 つ目は「報復」である。報復は、相手国に対する外交官の追放や往来禁止といった非友好的な措置を指す[29]。その特徴は、非友好的な措置ながらも国際法には反しない行為であり、その実行に際しては必ずしも相手国の違法行為を前提としなくてもよい点にある。アトリビューション問題などが理由で、受けたサイバー攻撃の責任を特定の国家に追及できないような場合にも実行でき、あらゆる場合に選択可能な措置とされる[30]。

2 つ目は「対抗措置」である。対抗措置は、相手国の先行違法行為に対して、その違法行為を止めさせる目的で実施されるものであり、被害国が取る措置は、本来は違法行為に当たる行為であったとしてもその違法性が阻却される。もっとも被害国の措置は、受けた損害と均衡していなければならず、武力の行使を含んではならないとの見方もある[31]。また、例えば米英は、サイバー手段を用いた国際違法行為への対抗措置として被害国は非サイバー手段も用いることができるとの見解を示している。さらに、対抗措置を実行する前に相手国に対して違法行為を止めるよう働きかける必要があるか否かが 1 つの論点となるところ、米英は、すべての場合でそうした働きかけが必要ではないとする[32]。

3 つ目は「緊急避難」である。シュミットらによれば、被害国は受けたサイバー攻撃が国際違法行為を構成しない場合でも緊急避難を講じることができる。一見、報復と似ているが、緊急避難では、本来ならば違法行為に当たるような措置も講じることができる点で両者は異なる。ただし緊急避難は、被害国の「根本的な利益」に対する

27 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』5 頁。なお「相当の注意」義務のサイバー空間への適用の妥当性は各国によって見解が分かれており、また適用に際して議論を詰めるべき事項は多い。この点については次を参照。Andraz Kastelic, *Due Diligence in Cyberspace: Normative Expectations of Reciprocal Protection of International Legal Rights*, United Nations Institute for Disarmament Research (November 2021), https://unidir.org/sites/default/files/2021-11/SecurityTechnology_DueDiligence_Report.pdf.

28 Johnson and Schmitt, “Responding to Proxy Cyber Operations Under International Law,” pp. 22–28. なお、他国からのサイバー攻撃が国際法上の武力攻撃に該当する場合には自衛権の発動が可能となるが、本稿は武力攻撃未満のシナリオにおける ACD を論点とするため、自衛権の発動に関する議論は割愛する。

29 一例として、ロシア政府による 2020 年の米大統領選挙へのサイバー攻撃やソーラーウィンズ社事件への関与を理由に 2021 年 4 月にジョー・バイデン（Joe Biden）米大統領が実施した、ロシア外交官の追放などが挙げられる（「アメリカ、ロシア外交官 10 人を国外追放―サイバー攻撃や選挙介入めぐり制裁―」BBC News Japan、2021 年 4 月 16 日、https://www.bbc.com/japanese/56768589）。

30 Johnson and Schmitt, “Responding to Proxy Cyber Operations Under International Law,” p. 22.

31 Ibid., p. 24.

32 対抗措置に関する米英の主張についは次を参照。A/76/136, pp. 118, 142.

「重大かつ差し迫った危険」がサイバー攻撃によって発生しており、「他に手段がない場合」にのみ実行できる[33]。なお国際法上で「根本的な利益」は明確に定義されてはおらず、また、国家がある情報通信インフラを重要インフラと位置づけたからと言って、そのインフラが国際法上の「根本的な利益」と位置づけられる訳でもない[34]。さらに、報復やバックアップシステムの利用で「根本的な利益」を守れる場合や、他国の「根本的な利益」を害し得る場合には、緊急避難は講じるべきではないとされる[35]。情報通信ネットワークがグローバルかつ複雑に接続されていることを踏まえれば、予期せず他国に害を与えてしまう可能性も否定できない。緊急避難は相手国の先行違法行為を前提とせずに、報復の水準にとどまらない措置を講じられる点を特徴とするが、その分、発動の要件は厳しいといえる[36]。

（3）小結

本節でみてきたように、ACD は特効薬と呼べるような個別具体的な措置を指す訳ではなく、「受動的防御を超えた措置」を意味するにとどまる概念である。幅広い措置の実行が ACD として想定されるが、その効果は自明ではない。攻撃寄りの措置を取ろうとすれば付随するリスクは高くなり、仮に講じた措置によって攻撃を無害化できたとしても、それは一時的なものにとどまる可能性もある。

さらに、情報通信機器はグローバルかつ複雑に接続されていることに加えて、ACD をめぐる国際法上の整理がなされていないこともあって、予期しない事態のエスカレーションも生じ得る。この文脈で、特にロシアや中国などは技術的アトリビューションの困難さ、どのような行為が国際違法行為に該当するかの共通理解の欠如、アトリビュートする際の具体的な証拠を提示する必要性などを理由に、サイバー空間への既

33 Johnson and Schmitt, “Responding to Proxy Cyber Operations Under International Law,” p. 27; 中谷、河野、黒崎『サイバー攻撃の国際法』27–28 頁。

34 なお、「根本的な利益」を構成し得る要素には、「国家の経済的健全性、公衆衛生や安全、通信、発電、国家安全保障」があるとされる（Johnson and Schmitt, “Responding to Proxy Cyber Operations Under International Law,” p. 27）。

35 Johnson and Schmitt, “Responding to Proxy Cyber Operations Under International Law,” p. 28.

36 ACD に関する日本の有識者会議の提言では、「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」対抗措置に比して、「実務上、援用する違法性阻却事由としては、『緊急状態（Necessity）』の方が援用しやすい」との見解が示されている（『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』、12 頁）。被害国が取る措置の法的根拠を「緊急避難」に求めることの是非は論点となるが、ACD をめぐる国際法上の整理が途上である中で、日本の解釈や立場を示していくことは日本の利益にかなう新たな規範の創出に向けた取組として重要といえる。

存の国際法の適用に対して厳しい姿勢を示していることは注目される[37]。ロシアや中国などはもともとサイバー空間における国際的なルールの必要性を主張してきたが、日米欧諸国を中心に既存の国際法の適用を主とするルール作りが進み始めると、そうした取組に対しては一転して慎重な立場をとった。その背景には、既存の国際法が適用されれば、従前はグレーゾーンの範疇にとどまっていた行為に対する国家責任が問われ、さらに日米欧諸国はより多様な対抗的な措置を講じるようにもなり、これまで培ってきたハイブリッド戦も含むデジタル技術の国内外の政策への活用の再考が迫られかねないとのロシアや中国等の懸念があると推察される[38]。諸国間で見解の隔たりが大きい状況にあって、特に他国領域で実施される ACD にかかわる措置が事態のエスカレーションにどのような影響を与えるかは予断できない。ACD の導入に当たっては、不透明な効果と見通せないリスクの存在を加味する必要がある。

他方、もはや受動的防御だけでは脅威に対処できず、議論の成熟を待っている余裕がない現状もある。実際ここ 10 年ほどで米国は、必ずしも ACD とは銘打っていないものの、複数の政府機関が有機的に連携しながらより能動的な措置を講じるようになってきた。次節では、その中心にある FBI と USCYBERCOM の具体的な取組を概観しつつ、小結として米国が抱える課題のうち日本にも関係するだろう事項について触れる。なお本事例研究は、米国の取組を網羅するものではなく、公開情報から示される米国の特徴的な取組に焦点を当てたものである。

2．米国での能動的措置の展開

（1）国内の脅威対応で中心的役割を果たす FBI

米国には、国防総省やインテリジェンス機関のアセットを除く米国の情報通信ネッ

37 アトリビューション問題に関するロシアの見解は例えば次を参照。Russian Federation, “Statement on Applicability of International Law by Russian Federation,” UNODA (March 7, 2023), https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Russian_statement_How_international_law_applies.pdf; 中国の見解は例えば次を参照。“Statement on Applicability of International Law by China,” UNODA (December 16, 2021), https://documents.unoda.org/wp-content/uploads/2021/12/Statement-of-China_ICT-OEWG-7th-plenary-meeting_international-law_DEC-16-AM_CHN.pdf.

38 原田有「サイバー国際規範をめぐる交錯」大澤傑編著『デジタル権威主義―技術が変える独裁の “ かたち ”―』（芙蓉書房出版、2024 年）177–201 頁、特に 191–192 頁。

トワークでの重大なサイバーインシデント[39]対応を念頭に、連邦政府の諸機関が果たすべき役割を示した「国家サイバーインシデント対応計画（NCIRP）」（2016年12月）がある[40]。同計画では政府が取り組むべき事項の1つとして「脅威対応」が挙げられている。具体的には、「捜査、鑑識、分析、（被害の）緩和に向けた活動、脅威アクターの阻止、（攻撃源に関する）帰属情報の提供」（丸括弧内は執筆者追記）などを指す[41]。前節のACDの概念に関する議論を踏まえると、「脅威対応」は攻撃寄りの措置も含む取組と理解することができ、その主幹機関としては法務省、特にFBIが指定されている。FBIは、サイバー脅威の捜査に資する情報の調整・統合・共有などのために国防総省も含む30以上の機関で構成され、2008年に新設された「国家サイバー捜査合同タスクフォース（NCIJTF）」の主幹機関でもある[42]。

実際に近年、米国を標的とするロシアや中国によるサイバー攻撃に利用された米国内のボットネットをFBIが中心となってテイクダウンさせる事例が相次いで公表されている[43]。ボットネットのテイクダウンはより攻撃に近いACDに分類できるが、そうした措置の国内法上の根拠は、「連邦刑事訴訟規則のルール41『捜索と押収』」である[44]。2016年12月のルール41の改正でFBIは、例えば被害を受けたコンピュータが5以上の管轄区にまたがって存在している場合に、事案が発生した管轄区の治安判事の令状を得れば、当該管轄区外も対象にボットネット化している装置に遠隔アクセスし、マルウェアを除去することが可能になった[45]。米国には、日本のいわゆる「不正アクセス禁止法」に相当する「コンピュータ詐欺と濫用に関する法律（CFAA）」もあり、管理者の許可なくコンピュータにアクセスして情報を取得することや損害を与えるこ

39 NCIRPでは重大なサイバーインシデントは、「米国の国家安全保障上の利益、対外関係、経済、あるいは米国民の信頼、市民の自由、公衆衛生と安全に明らかな損害を生む可能性が高いインシデント」と定義されている（“The National Cyber Incident Response Plan [NCIRP],” Cybersecurity and Infrastructure Security Agency, U.S.Department of Homeland Security [December 2016], p. 8, https://www.cisa.gov/sites/default/files/2023-01/national_cyber_incident_response_plan.pdf）。

40 NCIRPは2016年、バラク・オバマ（Barack Obama）政権時に策定されたものであり、現在はその改定に向けた取組が進められている。

41 その他、政府が取り組むべき事項には「アセット対応」、「インテリジェンス支援」、「影響を受けた組織自身による対応」がある（NCIRP, pp. 11–12）。

42 “Justice Department’s Role in Cyber Incident Response,” Congressional Research Service (CRS) Report R44926, Updated December 18, 2020, pp. 3–4, https://sgp.fas.org/crs/misc/R44926.pdf.

43 一例として次を参照。”Press Release: Justice Department Conducts Court-Authorized Disruption of Botnet Controlled by the Russian Federation’s Main Intelligence Directorate of the General Staff (GRU),” U.S. Department of Justice (February 15, 2024), https://www.justice.gov/opa/pr/justice-department-conducts-court-authorized-disruption-botnet-controlled-russian.

44 “Federal Rules of Criminal Procedure, Rule41: Search and Seizure,” Legal Information Institute, Cornell Law School, https://www.law.cornell.edu/rules/frcrmp/rule_41.

45 Ibid., para. (b)(6)(B).

とは禁じられている[46]。ただし同法上、合法的に権限を付与された米国の法執行機関やインテリジェンス機関による活動は例外扱いとなっている[47]。

NCIRP の指針に沿って FBI は「脅威対応」の主幹として、能動的措置を国内で実施し、そのための国内法の整備も行われてきたことが分かる。他方で USCYBERCOM もまた、能動的措置を講じるようになってきた。

（2）対外的な能動性を増す USCYBERCOM

ポール・ナカソネ（Paul Nakasone）USCYBERCOM 前司令官（米国家安全保障局〈NSA〉長官を兼任）によれば、同軍はもともと「受動的な部隊」であった[48]。というのも軍の当初の主目的は、国防総省のネットワーク防御（受動的防御の意）と、特にイラクやアフガニスタンでの戦闘支援にあったからである。そうした部隊の性格は、2018 年 3 月に公表された USCYBERCOM のコマンド・ビジョンで示されたように[49]、平時にあっては、武力紛争に至らない水準で相手に「持続的に関与」し、「前方防衛」するものへと変化した[50]。その背景には、ロシア、中国、北朝鮮、イランによるサイバー攻撃の被害・頻度の増加があった。そうした状況にあって、米国自身のネットワーク上で防御するだけでは十分ではなく、敵のネットワーク上で作戦を展開する必要性が高まったのである。2011 年の『サイバー戦略』で国防総省は既に ACD という表現を用いて、自身のネットワークやシステムに影響が及ぶ前にサイバー攻撃を捕捉・停止させるとしていた[51]。他方、現在では ACD ではなく「前方防衛」との表現を用いて、USCYBERCOM は「敵に可能な限りに近い」ネットワーク上で展開する部隊となった[52]。

USCYBERCOM が取り組み始めた能動的措置は、例えばロシアからのサイバー攻撃への対処に確認できる。報道によれば、バラク・オバマ（Barack Obama）政権末期では、USCYBERCOM の活動は主にロシアのネットワーク上での監視活動レベル

46 “18 U.S. Code § 1030 - Fraud and Related Activity in Connection with Computers,” Legal Information Institute, Cornell Law School, https://www.law.cornell.edu/uscode/text/18/1030.
47 Ibid., para. (f).
48 Paul M. Nakasone, “A Cyber Force for Persistent Operations,” *Joint Force Quarterly* (1st Quarter 2019), pp. 10–14, especially p. 11, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1736950/a-cyber-force-for-persistent-operations/.
49 “Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command,” U.S. Cyber Command (March 2018), https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf.
50 Nakasone, “A Cyber Force for Persistent Operations,” p.12.
51 “Department of Defense Strategy for Operating in Cyberspace,” U.S. Department of Defense (July 2011), https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.
52 Nakasone, “A Cyber Force for Persistent Operations,” p. 13.

にとどまっていた[53]。しかし、2018年の大統領選挙時にUSCYBERCOMは、ロシアの手先となって選挙干渉を行っているとされた組織のネットワーク接続を妨害した[54]。さらに新生USCYBERCOMを印象付ける取組に、「ハント・フォワード作戦」もある。同作戦は、サイバー攻撃を受けている米国の同盟国やパートナー国からの依頼を受けてUSCYBERCOMの部隊を派遣し、そうした国々を技術・情報面で支援するとともに、収集した攻撃手法などの情報を自国の安全保障だけでなく、一般的なサイバーセキュリティにも役立てることを目的に実施されている[55]。

そうした活動の要が、USCYBERCOMの「サイバー国家任務部隊（CNMF）」である[56]。そしてUSCYBERCOM、特にCNMFは、FBIの取組も支援している。近年、米国は同盟国の諸機関とも連携してサイバー攻撃に関する注意喚起を実施しているが、事案によっては米国の機関としてFBIやNSAなどに加えてCNMFも連携機関に加わっている[57]。さらにナカソネ前司令官の議会報告によれば、USCYBERCOMとNSAは、詳細は不明ながらも、ランサムウェアや暗号化資産の窃取などの犯罪を取り締まるFBIの取組にも協力している[58]。

このようにUSCYBERCOMは、サイバー脅威に「持続的に関与」し、「前方防衛」する組織となってきたが、既存研究ではそうした活動の基盤となる主たる国内法上の根拠として、「国防権限法（NDAA）2019」とドナルド・トランプ（Donald Trump）政権が2018年に発出した「国家安全保障大統領覚書（NSPM）13」が注目されてきた[59]。まず、NDAA2019のセクション1642によれば、ロシア、中国、北朝鮮、あるい

53 David E. Sanger and Nicole Perlroth, “U.S. Escalates Online Attacks on Russia’s Power Grid,” *The New York Times* (June 15, 2019).

54 Ellen Nakashima, “U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms,” *The Washington Post* (February 26, 2019).

55 Jeff Kosseff, “The International Legal Framework for Hunt Forward and the Case for Collective Countermeasures,” in *CyCon 2024: Over the Horizon 16th International Conference on Cyber Conflict*, eds., C. Kwan, L. Lindström, D. Giovannelli, K. Podiš and D. Štrucl (NATO CCDCOE, 2024), pp. 221–234, https://ccdcoe.org/uploads/2024/05/CyCon_2024_Kosseff-1.pdf.

56 USCYBERCOMの編成などについては次を参照。“Defense Primer: Cyberspace Operations,” CRS, IF10537, Updated November 29, 2024, https://crsreports.congress.gov/product/pdf/IF/IF10537; “NEWS: CNMF Marks a Decade Defending the Nation,” USCYBERCOM (January 17, 2024), https://www.cybercom.mil/Media/News/Article/3647031/cnmf-marks-a-decade-defending-the-nation/.

57 “Joint Cybersecurity Advisory: Hunting Russian Intelligence ‘Snake’ Malware,” U.S. Cybersecurity and Infrastructure Security Agency (May 9, 2023), https://www.cisa.gov/sites/default/files/2023-05/aa23-129a_snake_malware_2.pdf.

58 “2023 Posture Statement of General Paul M. Nakasone,” U.S. Cyber Command (March 7, 2023), https://www.cybercom.mil/Media/News/Article/3320195/2023-posture-statement-of-general-paul-m-nakasone/.

59 USCYBERCOMの対外的活動の国内法上の根拠に関しては例えば次を参照。Robert Chesney, “The Domestic Legal Framework for US Military Cyber Operations,” Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2003 (July 29, 2020), https://www.hoover.org/sites/default/files/chesney_webreadypdf.pdf; 永野「我が国における能動的サイバー防御の構築に伴う法と組織」189–198頁。

はイランが「サイバースペースにおいて、米国の政府や市民を対象に、また米国の選挙や民主的な政治プロセスに影響を与えようとする企みも含めて、能動的、システマティック、かつ継続的な攻撃キャンペーン」を行っている場合、そうした攻撃を「妨害、打破、抑止する」ために、「国家指揮権限は国防長官に、USCYBERCOM 司令官を通じて、外国のサイバースペースで適切かつ均衡性のある行動をとる」ことを許可できる[60]。またNSPM13では、機密文書のため非公開となっているものの一部報道によれば、武力行使には至らない水準、あるいは死亡者を出したり、破壊や重大な経済的損失を与えたりしない水準のサイバー作戦に関しては、大統領の許可を都度得ることなく実施可能とされている模様である[61]。USCYBERCOM はここ数年で、攻撃も含むより能動的な措置を実施できるよう国内法上の手当がなされてきたことが分かる。

なお USCYBERCOM の活動は、先述の CFAA の規定に抵触し得るのであり、CFAA の規定上、国防総省・軍は法執行機関やインテリジェンス機関のような例外扱いとはなっていない。さらにいえば、米国では「民警団法」上、法律や憲法で明示的に許容されていない限りは、国内法の執行のために連邦軍を動員できないことになっている。他方、NDAA2019 や NSPM13 にみられるように、議会・行政府双方で USCYBERCOM が能動的なサイバー作戦を実施することを認めてきた事実に照らせば、USCYBERCOM が実施する作戦への CFAA の適用は想定されていないと考えられている[62]。また「民警団法」に関しても、重要インフラに対するサイバー攻撃のような場合は例外的に連邦軍の動員が可能だともされる[63]。要するに米国の安全保障上、極めて重要度の高い事案において、USCYBERCOM は FBI などによる米国内の法執行活動の支援も含めて、幅広く活動できる仕組みになっていると解せる。

60 “H.R.5515: An Act to Authorize Appropriations for Fiscal Year 2019 for Military Activities of the Department of Defense, for Military Construction, and for Defense Activities of the Department of Energy, to Prescribe Military Personnel Strengths for such Fiscal Year, and for Other Purposes,” Congress. Gov, section 1642, https://www.congress.gov/115/statute/STATUTE-132/STATUTE-132-Pg1636.pdf.

61 Ellen Nakashima, “White House Authorizes ‘Offensive Cyber Operations’ to Deter Foreign Adversaries,” *The Washington Post* (September 20, 2018). なお NSPM13 では、大統領の許可を得ずに USCYBERCOM が実施できる対外的作戦として、時間的に制約がある作戦が想定されているとされる。もっとも、「時間的な制約」の定義は明らかではない。この点については次を参照。Robert Chesney, “The Pentagon’s General Counsel on the Law of Military Operations in Cyberspace,” Lawfare (March 9, 2020), https://www.lawfaremedia.org/article/pentagons-general-counsel-law-military-operations-cyberspace.

62 Chesney, “The Pentagon’s General Counsel on the Law of Military Operations in Cyberspace.”

63 例外的に連邦軍の国内動員が認められる場合として、法執行機関では事態を収拾できないような危機的状況に対処する場合、州政府では連邦政府の財物や機能を保護できない、保護する意思がない場合があり、重要インフラに対するサイバー攻撃対処事案はそうした例外に該当し得ると考えられている。Jay P. Kesan, and Carol M. Hayes, “Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace,” *Harvard Journal of Law and Technology* 25, no. 2 (Spring, 2012), p. 523.

（3）小結

本節でみてきたように、米国ではFBIやUSCYBERCOMが即応性をもってより能動的な措置を講じられるよう、その権限が整備され、実任務へと反映されてきた。そうした米国の取組は、前節で触れたCCHSの報告書で提示されたACDの概念に基づけば、攻撃により近いACD、あるいは攻撃に該当する措置を含むものと解せる。その背景には、国際法の適用方法などに関する議論の成熟を待っている余裕がないほどに脅威が高まっている現状がある。米国のように、自国にとってのレッドラインを超える行為に具体的に対応していくことは、サイバー攻撃の予防に向けた将来的な行動規範の形成に資するとの見方もある[64]。

このように、米国の取組はACDに関連する取組を先駆的に導入してきた事例として注目されるが、国によって国内法の在り方や国際法の解釈、保有する能力等は異なっているのであり、日本を含むその他の諸国に米国の取組が直ちに参考例として当てはめられる訳ではない。実際、例えば英国におけるACDは受動的防御により近い取組と整理されており[65]、米国の取組とは異なっている。ACDの概念が不明確であり、その効果と伴うリスクも不透明である中にあって各国は、国際法の可能性と取り得る措置を探りながら、それぞれの国情に照らして意義が見出せ、かつ許容できるリスクの程度も考慮に入れたACDの在り方を検討することが求められているといえる。

他方、先駆的事例と位置づけられる米国で提起されてきたACDに関する多様な論点は、他国にとっても参考になるところがある。以下で日本にも示唆的な幾つかの事項を取り上げる。

まず、能動的措置の是非である。例えばFBIの国内での遠隔アクセスを可能にしたRule41については、令状の獲得が前提とはいえ、政府の「大量ハッキング」を招きかねないとの批判は強く、政府が取る措置を監督する仕組みの重要性が強調されている[66]。また、遠隔アクセスの付随的被害の抑制が難しい点も問題視されている[67]。さらに

64 川口貴久「国家によるサイバー攻撃からのセキュリティ」SYNODOS（2020年3月18日）、https://synodos.jp/opinion/politics/23376/。

65 Tim Stevens, Kevin O'Brien, Richard, Overill, Benedict Wilkinson, Tomass Pildegovičs, and Steve Hill, *UK Active Cyber Defence: A Public Good for the Private Sector*, King's College London, The Policy Institute Cyber Security Research Group (January 2019), p. 10, https://www.kcl.ac.uk/policy-institute/assets/uk-active-cyber-defence.pdf.

66 Jennifer Daskal, "Rule 41 Has Been Updated: What's Needed Next," Just Security (December 5, 2016), https://www.justsecurity.org/35136/rule-41-updated-needed/; Timothy Edgar, "Recent Botnet Takedowns Allow U.S. Government to Reach Into Private Devices," Lawfare (March 13, 2024), https://www.lawfaremedia.org/article/recent-botnet-takedowns-allow-u.s.-government-to-reach-into-private-devices.

67 Ed Amoroso and Randal S. Milch "Hack-to-Patch by Law Enforcement Is a Dangerous Practice," Just Security (April 30, 2021), https://www.justsecurity.org/75955/hack-to-patch-by-law-enforcement-is-a-dangerous-practice/.

一部報道によれば、米国務省を含む一部政府機関も、NSPM13 に基づき USCYBERCOM の裁量が拡大されたことに外交への影響といった観点から懸念を示している [68]。

次に、企業などによる自力救済の是非である。そもそも米国では 1990 年代末時点で既に、企業による外部ネットワークへの侵入を伴う措置が必要だとし、免許制度の導入も含めて、そうした措置を監督するメカニズムの構築の必要性が提起されていた [69]。その後も企業がハックバックできる条件など、非国家主体による自力救済措置は論点であり続けている [70]。また先述のように、企業などによる能動的措置に関する法案も 2019 年に米下院の委員会に付託されている。結果的に同法案が採決に至らなかった事実が表すように、非国家主体に自力救済措置を認めることに慎重な声も強い。企業によるハックバックを認めるようになれば、事態がより複雑化しかねないことが懸念されている [71]。もっとも、政府が十分な対策を講じることができないのであれば、非国家主体による自力救済措置の必要性を求める声は高まりかねず、官民の連携、中でも民が官の取組を信頼できるかが 1 つの要点となっている。

さらに、国外で実施する能動的措置、特に攻撃寄りの措置の国際法上の根拠も争点となる。米国は政治的にアトリビュートしてロシアや中国などの責任を問いながら「前方防衛」しているが、その際の個別具体的な作戦の国際法上の根拠は必ずしも明確ではない。前節で触れたようにサイバー空間への既存の国際法の適用については一致した見解がないこともあって、特に武力攻撃未満の攻撃に対する処置の法的根拠の説明は難しい現状がある。そうした中での越境的な措置の実施は、予期しない事態のエスカレーションをもたらしかねないとの危惧を生んでいる [72]。他方、米国の取組は脅威が高まる一方にあっては現実的ともいえ、将来的な攻撃の抑止や規範の創出に資する側面も併せ持つ点も見過ごせない。

68 Suzanne Smalley, “Biden Set to Approve Expansive Authorities for Pentagon to Carry out Cyber Operations,” CyberScoop (November 17, 2022), https://cyberscoop.com/biden-nspm-13-pentagon-cyber-operations/.

69 Stevan D. Mitchell, and Elizabeth A. Banker, “Private Intrusion Response,” *Harvard Journal of Law and Technology* 11, no. 3 (Summer 1998), pp. 699–732.

70 非国家主体による能動的措置に関する議論は例えば次を参照。”The Hackback Debate,” Steptoe (November 2, 2012), https://www.steptoe.com/en/news-publications/cyberblog/the-hackback-debate.html; Jeremy Rabkin and Ariel Rabkin, “Hacking Back Without Cracking Up,” *A Hoover Institution Essay: Aegis Paper Series*, no. 1606 (June 28, 2016), https://www.hoover.org/sites/default/files/research/docs/rabkin_webreadypdf.pdf; Dennis Broeders, “Private Cyber Defense and (International) Cyber Security: Pushing the Line?” *Journal of Cybersecurity* 7, no. 1 (2021), pp. 1–14, https://academic.oup.com/cybersecurity/article-pdf/7/1/tyab010/37019168/tyab010.pdf.

71 James Rundle, “Letting Businesses ‘Hack Back’ Against Hackers Is a Terrible Idea, Cyber Veterans Say,” *The Wall Street Journal* (July 8, 2021).

72 Jack Goldsmith and Alex Loomis, “‘Defend Forward’ and Sovereignty,” A Hoover Institution Essay: Aegis Paper Series, no. 2102 (April 29, 2021), https://www.hoover.org/sites/default/files/research/docs/goldsmith-loomis_webreadypdf.pdf.

おわりに

ACD は「受動的防御を超えた措置」を意味するにとどまる明確な定義を欠く概念であり、どのような措置が ACD に当たるのかは国や議論によっても変わる。また、その効果は不透明さを残し、サイバー空間への既存の国際法の適用の仕方が議論の途上にあることもあって、見通せないリスクも抱える。他方、受動的防御では高まる脅威に十分に対処できない現状もある。本稿では、ACD の概念や国際法上の整理が定まらないこと示しつつ、そうした中で先駆的に取組を進めてきた米国を事例としてとりあげることで、国際法の可能性と取り得る措置を探りながら、許容できるリスクの程度やその他の国情に照らして適切な ACD の在り方を検討し、その地平を切り開いていく必要があることを示した。

その必要性に日本も今まさに直面している。例えば、『国家安全保障戦略』は「可能な限り未然に攻撃者のサーバ等への侵入・無害化」[73] することを ACD の 1 つの措置として示しているが、ここで強調されるべきは、そうした措置は国の内外で実施され得るという点である。ACD に関する措置が他国領域での活動を必ず含む訳ではないのであり、日本の取組が米国の前方防衛に類似したものになるとは限らない。また、一部に ACD と専守防衛との整合性を問う声もあるが [74]、米国内での FBI の遠隔アクセスの例が示すように、「侵入・無害化」措置は、必ずしも専守防衛との整合性が問われるような対外的措置のみで構成される訳ではないのである。日本でも既に「NOTICE」という呼称の下、情報通信研究機構（NICT）が容易に推測可能なパスワードの入力などによって遠隔アクセスし、攻撃に利用されかねない国内のルーターなどを洗い出す、防御寄りの ACD に当たる国内措置が実施されている [75]。そうした取組では、米国の事例研究が示すように、国内法の整備や政府機関の活動をチェックする安全装置が欠かせないのであり、日本でも検討すべき事項は残されている [76]。

73『国家安全保障戦略』21–22 頁。

74「能動的サイバー防御 – 国民の理解が前提条件だ –」毎日新聞（2023 年 8 月 17 日）、https://mainichi.jp/articles/20230817/ddm/003/070/079000c.

75 遠隔アクセスができてしまった場合には、インターネットサービスプロバイダ経由で当該機器の利用者に注意喚起がなされる（「NOTICE について」NOTICE、https://notice.go.jp/）。

76 例えば「不正アクセス禁止法」では「何人も、不正アクセス行為をしてはならない」（第 3 条）とされ、米国のように法執行機関などを例外とする規定はない。そうした中、「NOTICE」での機器へのアクセスは「国立研究開発法人情報通信研究機構法（NICT 法）」で「特定アクセス行為」と位置づけられ、「不正アクセス」の例外とされている。しかし、米国の取組を参照すれば、「NOTICE」のような取組は「不正アクセス禁止法」の中で例外として位置づけられるべきとも考えられる。また、日本においてはその他にもいわゆる「通信の秘密」との整合性といった国内法上の課題も指摘されており、ACD に資する措置の地理的射程を国内に限定したとしても検討すべき問題は多い。ACD にかかわる日本の課題については例えば次を参照。野呂瀬葉子「日本のサイバーセキュリティ政策」大澤『デジタル権威主義』69–80 頁。

国内で実施できる措置が存在するとはいえ、より効果的な ACD を日本が目指すのであれば、自ずと自国領域外での活動も視野に入ってくる。そうした活動の国際法上の合法性は議論の余地を残すが、自国の国際法の解釈を整理し、それに基づいて敢えて対外的措置を講じていくことも、自国の安全保障、ひいては新たな国際規範の創出のための一案となる。その際には同盟国や同志国との連携が欠かせず、それら諸国との合同による対抗措置の実施の是非なども議題となろう[77]。

さらに、既に米国で議論されているように、非国家主体による自力救済措置の在り方も日本での論点になり得る。『国家安全保障戦略』では、「侵入・無害化」措置の権限は政府のみに付与されることが想定されている[78]。非国家主体による自力救済措置を認めると事態の収拾がつかなくなりかねないことから、そうした方針は適当といえる。他方、政府による対応が十分ではなかったり、官民間に信頼が築けなかったりした場合には、非国家主体による自力救済措置の是非も論点化する可能性がある。現在、日本ではまさに ACD の導入に向けた検討が行われているが、その効果やリスク、関連する事情などを踏まえた多角的な議論が期待される。

（防衛研究所）

77 Kosseff, “The International Legal Framework for Hunt Forward and the Case for Collective Countermeasures.”
78『国家安全保障戦略』22 頁。