越境サイバー行動により生じる主権侵害の評価基準
──政策的必要性から導かれる二元論的理解の修正可能性──

山口　章浩

＜要旨＞

本稿は、越境的なサイバー行動への主権原則の適用をめぐる争点を整理し、その政策的含意を踏まえて、当該法規範の今後の発展について示唆を引き出すことを目的とする。近年、低烈度のサイバー攻撃の違法性を訴える法的根拠として主権原則を援用する国の見解が増えている。一方で、容易に国境を跨いで行われるサイバー行動は、どこからが主権侵害に当たるかについての議論を呼んでいる。国家の見解および学説は、他国のICTインフラへの「無許可のアクセス」を主権侵害の基準とする立場と、最小限の効果しか引き起こさないものは許容されるという立場に大別できる。この解釈の相違は、サイバー諜報活動、越境リモートアクセス捜査、ACD措置といった政策に対する法的評価の相違につながる。本稿は二元論的理解から一歩進め、政策的必要性と法の支配の推進とのバランスを探る道筋として、具体的な行為類型に即した形に議論を修正する可能性を提示する。

はじめに

国境を越えた組織的なサイバー犯罪や、国家支援型のサイバー攻撃の脅威が増大するなか、国際社会ではサイバー空間における法の支配の確立が模索されてきた。国連政府専門家会合（GGE）の報告書は、主権平等、紛争の平和的解決、武力の不行使、人権および基本的自由の尊重、内政不干渉の5つの基本原則が、情報通信技術（ICT）利用における国家の行動にも妥当するとの国際的なコンセンサスを反映している[1]。

また国際法専門家により作成された『タリン・マニュアル』に見られるように、サイバー行動（cyber operations）の文脈での既存の国際法原則の解釈適用に関する議論

1 UN Secretary-General, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/76/135 (July 14, 2021), pp. 17–18.

の精緻化がなされてきた[2]。さらに近年、国連の内外において各国・地域機関がサイバー行動への国際法の解釈適用に関する自らの見解を公式に表明する動きがある。

各国の見解表明は、上述の 5 つの基本原則を含め、サイバー行動に適用される原則や規則についての共通理解を醸成する一方で、個別の規則に関する解釈の差異を際立たせている。なかでもサイバー行動への主権原則の解釈適用に関する相違が注目されてきた。例えば、「サイバー行動の文脈において主権原則は他の実定法上の義務規則を導く原則に過ぎない」との 2018 年の英国の解釈は、「サイバー行動について主権原則は特定の義務を課しているか」との論点について、限定的な分野ながら大きな学術的関心を呼んだ[3]。もっとも、その後に示された多数の国の見解は、主権原則それ自体が特定のサイバー行動を行わないよう義務付けているとの立場を支持している。しかしながら、近年の各国の見解および学説を見ると、主権侵害と評価する基準についてもさらに議論が分かれていることを指摘できる。

まず一方では、主権原則の適用範囲の領域的性格を前提として、領域国の同意なく行われる、あらゆる越境的なサイバー行動は主権侵害に該当するとの主張（純粋主権論（pure sovereigntist））がなされる。この主張の背景には、国家の領域主権原則は国家が他国の領域に同意なく侵入することを一般にその違反としており、サイバー行動においても同様であるとの考えがある。

他方で、越境的なサイバー行動が主権侵害となるかどうかについて、その行動がもたらす効果を基準として評価する主張（相対主権論（relative sovereigntist））もまた唱えられてきた。この解釈によれば、越境的なサイバー行動のうち、物理的な損壊や機器の機能喪失を生じさせるかどうかという点で主権侵害が判断される。

もっとも、相対主権論の立場を採るとしても、越境的なサイバー行動が主権侵害とみなされる程度の効果を伴う場合、「キャッチ・オール」の純粋主権論とはアプローチこそ違えども、導かれる主権侵害との結論は異ならない。両論の有意な差異は、主権侵害と判断するにあたり、一定の効果の閾値を必要とするかである。この点について、いくつかの国は、外国に所在する機器を対象としたサイバー行動であっても、「無視できる、または最小限の効果」しかもたらさない場合は、主権侵害に該当しないとの主張を行っており、そうした閾値未満のサイバー行動の法的評価は、純粋主権論の立場

2 Michael N. Schmitt ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013); Michael N. Schmitt ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017). 本稿では 2017 年版の 2.0 を『タリン・マニュアル』として参照する。

3 黒崎将広「サイバー空間における主権：その論争が意味するもの」森肇志 、岩月直樹編『サブテクスト国際法教科書の一歩先へ』（日本評論社、2020 年）33–34 頁。

からの評価とは異なり得る。

相違する見解の双方の理論的妥当性は先行研究においても取り上げられてきた[4]。しかしながら、後述のように、理論的妥当性をめぐる主張の相違は、究極的に「サイバー空間」の領域性または脱領域性のいずれを重視するかという視点の違いに起因すると指摘でき、確定的な結論を導かない。

そこで本稿が検討すべきは、双方の見解の政策的背景である。特に、相対主権論を支持する国はなぜ「キャッチ・オール」ではない効果の閾値を採用するのかである。本稿では相対主権論が支持される理由として、サイバー諜報活動と、警察によるリモートアクセスを手段とした域外証拠収集（越境リモートアクセス捜査）、および外国からのサイバー攻撃への対抗として、攻撃に利用される機器にアクセスし、その機能を妨げる措置の 3 類型の政策実践を提示する。

近年の研究では、各個別類型の行為に法的評価を与えるにあたり、純粋主権論と相対主権論の二元論的な主権原則の解釈から、異なる評価が導かれることが指摘されてきた[5]。これに対して、本稿の関心は法的評価を与えることそれ自体ではなく、双方の解釈が平行して主張される現在において、これらの実践の蓄積と、それを合法あるいは違法と評価する国家の法的見解の存在が、サイバー行動への主権原則の適用をめぐる議論にいかに反映され、今後の規範形成を方向づけていくかにある。

なお本稿は、サイバー行動に適用される国際法上の主権原則に関する議論を対象とするものであり、サイバー空間のガバナンス論一般や、「サイバー主権」の概念を詳細な検討の対象とするものではない。中国が唱える「サイバー主権」あるいは欧州連合（EU）が唱える「デジタル主権」という言説には、国内の個人・企業が有する ICT 機器やデータに対する国家的管理を正当化し、外国による干渉からの自律性を確保しようとする意図が読み取れる[6]。この点において、当該言説は国際法上の主権概念と一定の意味上の重なりを有する[7]。しかしながら、「サイバー主権」は主として抽象的な政策アジェンダとして用いられており、具体的な権利義務を導く国際法上の主権原則とは

4 See e.g., 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.

5 例えば、石井由梨佳「能動的サイバー防御による他国の主権侵害」経団連総研『地政学的リスクをめぐる諸課題と日本企業の法的対応』（2024 年 3 月 29 日）85–102 頁。

6 See, Julia Pohle and Thorsten Thiel, “Digital Sovereignty,” *Internet Policy Review*, vol. 9, Issue 4 (December 17, 2020), pp. 2–19.

7 Henning Lahmann, “On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace,” *Duke Journal of Comparative & International Law*, vol. 32, no. 1 (Fall 2021), pp. 90–93.

区別されるため[8]、紙幅の都合上、本稿では第 3 節で部分的に言及するに留め、「サイバー主権」の概念の詳細な検討は稿を改めたい。

以下では、まず国際法の基本原理である主権原則がサイバー規範の文脈において改めて注目され、論争の的となっている背景を概観する（第 1 節）。次に『タリン・マニュアル』における主権原則の解釈適用に関する議論と、各国の見解を相対主権論と純粋主権論の枠組みを用いて整理する（第 2 節）。そのうえで、両見解の相違から導かれる、越境的なサイバー行動を伴う政策をサイバー諜報活動、越境リモートアクセス捜査、サイバー攻撃に利用される領域外の機器に対する措置の 3 つの類型に整理してそれぞれの法的評価を明らかにし（第 3 節）、サイバー行動への主権原則の適用に関する今後の国際的な議論のあり得べき方向性を示す。

1．サイバー行動への主権原則の適用に関する議論の規範的背景

（1）サイバー行動の文脈からの主権原則の再訪

国際法規範としての主権原則は、国家の権利・権限および義務を含意する。GGE の報告書は、サイバー行動にも「国家主権および主権から導かれる国際的な規範および原則」が適用されることを再確認している。もっとも、主権は法原則と位置付けられる以上、それ自体が具体的な指示内容を持つわけではない。具体的に行動を許容・禁止する役割は、原則を存在根拠として導かれる法規則に求められる[9]。それにもかかわらず、サイバー行動に適用される国際法をめぐる近年の議論において、国家からも学術上も、侵害的なサイバー行動を国際義務違反と評価する基準として主権原則に改めて注目が集まっている。そこでまず、なぜ抽象的性格の主権原則が改めて注目されるのか、適用の射程がより明確な関連法規則のサイバー行動への適用との関係から、本稿の主たる検討の前提となる議論を整理する。

国際法の最も基本的な原理である主権原則からは、国際法によって規律されていない範囲の事項についての国家の行動の自由と、その反面、主権平等から導かれる国家主権の相互尊重の義務が導かれてきた。主権国家は自国領域内における排他的自由を有するから、国家が外国領域に侵入し、損害を与え、または政治的独立を侵害する行為は違法と評価される。例えば、外国領域への軍隊の派遣と駐留や、軍用機による領

8 Harriet Moynihan, “The Vital Role of International Law in the Framework for Responsible State Behaviour in Cyberspace,” *Journal of Cyber Policy*, vol. 6, Issue 3 (2021), pp. 401–402.
9 小寺彰『パラダイム国際法：国際法の基本構成』（有斐閣、2004 年）29 頁。

空侵犯といった行為類型は、領域国の同意またはその他の違法性阻却事由がない限り、領域国の主権を侵害する違法な行為と認められてきた。

そこで、サイバー行動の文脈においても同様に、外国領域でのサイバー行動は、領域国の主権侵害に該当するかが考えられる。もっとも、被害国はサイバー攻撃の実行主体として外国政府に抗議する場合であっても、ほとんどの場合、「国際法違反」との評価を明示しない[10]。法的評価が帰納的に明らかにされない状況は、サイバー行動に対する主権原則による法的拘束力それ自体に疑問を投げかける。この点、サイバー行動において主権原則は拘束力のある法規則ではなく、違法性の評価は同原則から導かれる内政不干渉原則や武力不行使原則に従って行われるべきとの見解も示されてきた（「原則としての主権アプローチ」）[11]。

もっとも、武力不行使原則や内政不干渉原則の適用の射程は限定的であり、外国政府を背景としたサイバー諜報活動や重要インフラを標的としたサイバー攻撃は常にそれらの原則の違反を構成するわけではない。この点、いくつかの国がエネルギーインフラシステム等に対する攻撃はこれらの原則の違反となり得るとの拡張的な解釈を示していることは注目できるが[12]、普遍的に受け入れられたものとはいえない。こうした状況において、国家が他国に行うサイバー攻撃を違法とする根拠として、武力不行使原則や内政不干渉原則の適用の射程の外にある、外国政府を背景とした悪意あるサイバー行動への法的評価の空白を埋める、「国際法秩序のいわば最後の砦」として主権原則は援用される[13]。ここで主権原則は、武力不行使原則などを導く原理としてだけではなく、それ自体が国家に一定の義務を課す、法的拘束力ある「規則」として援用され、その義務に違背するサイバー行動は国際違法行為と評価される（「規則としての主権アプローチ」）。

ところで、国による越境的なサイバー行動は価値中立的な行為を指すのであり、外国に対するサイバー攻撃に限らず、犯罪の証拠となる国外のサーバーに保存されたデータの収集といった国内法令の執行においても行われることに留意する必要がある。この点から、越境的なサイバー行動は執行管轄権の域外適用としても法的に性格づけら

10 例外的に、国際的な「コミットメント」に言及した抗議として、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); see also, Isabella Brunner, “Attributing Cyber Operations under International Law: Political and Legal Aspects,” *Questions of International Law, Zoom-in*, vol. 110 (2025), pp. 36–43.

11 “Record of UK’s Specific Reservations,” in NATO, *Allied Joint Publications-3.20: Allied Joint Doctrine for Cyberspace Operations* (January 2020), p. v.

12 Attorney General Suella Braverman, “International Law in Future Frontiers,” Speech delivered at Chatham House on May 19, 2022, the transcript is available at: https://www.gov.uk/government/speeches/international-law-in-future-frontiers.

13 黒崎将広「サイバー空間における主権」36–37 頁。

れる[14]。

外国における自国法令の適用（立法管轄権）は、領域国の立法管轄権との衝突が保護主義や効果主義のような判断基準によって調整される一方で、外国の同意なしに外国領域で自国法令を執行する権限（執行管轄権）は認められず、これを行えば、主権侵害に該当するとされてきた[15]。同様に考えれば、サイバー行動の文脈でも、外国領域にあるサーバー等に保存されたデータに領域国の同意なく政府機関がアクセスすれば、執行管轄権の域外行使として主権侵害に該当すると考えられる。しかしながら、次節で検討するように、そのような越境的なサイバー行動であっても許容されるとの意見も示されてきた。

（2）サイバー行動への主権原則の適用おける領域性と脱領域性

前項で述べたように、主権原則は、その一般的性格ゆえに、発展途上のサイバー行動に適用される国際法の空白を埋めるための柔軟な解釈可能性を提供しつつ、他方では義務内容をめぐる解釈論争を生んでいるといえる[16]。さらに、サイバー行動への主権原則の適用の議論を複雑にさせるのは、主権の及ぶ範囲は領域的である一方で、「サイバー空間」を介した行動は脱領域的側面を有するという点である[17]。改めて立ち返ると、「サイバー空間」はコンピューターやサーバーといった物理インフラ（物理層）と、電磁的に記録されたデータおよび電気的な通信（論理層）から成ると理解される[18]。そしてその「空間」は海底ケーブルや通信衛星を介して全地球的に広がっており、通信は容易に越境する。ゆえに、物理インフラの所在という領域的性格と、グローバルな通信という脱領域的性格のいずれを重視して「サイバー空間」を理解するかという視点の相違は、サイバー行動への主権原則の解釈適用に相違をもたらす[19]。

学説上、ケビン・ヘラー（Kevin Jon Heller）は、「サイバー空間がいかに新しく異なっているように見えようとも、サイバー空間は空、海、陸に劣らず領域的ドメインである」

14 和仁健太郎「サイバー犯罪に対する国家管轄権の行使と国際法」『論究ジュリスト』37 号（2021 年 11 月）46–53 頁。

15 See e.g., UN Security Council Resolution 138 (on questions relating to the case of Adolf Eichmann), S/RES/138 (June 23, 1960).

16 Lahmann, “Sovereignty Discourse,” pp. 90–93.

17 黒崎「サイバー空間における主権」41 頁。

18 さらに社会層を加えて理解されることもある。*See*, Przemysław Roguski, “Layered Sovereignty: Adjusting Traditional Notions of Sovereignty to a Digital Environment,” in *11th International Conference on Cyber Conflict: Silent Battle*, ed. Tomáš Minárik, Siim Alatalu, Stefano Biondi, Massimiliano Signoretti, Ihsan Tolga, and Gábor Visky (Tallinn: NATO CCD COE Publications, 2019), pp. 347–359.

19 この視点の相違は、サイバー行動への国際法の適用が論じられ始めた 1990 年代後半において、従来の領域性を基にする国際法の適用が一般的に妥当するかという点について議論が戦わされたことにも見つけられる。Nicholas Tsaugourias, “Law, Boarders and the Territorialization of Cyberspace,” *Indonesian Journal of International Law*, vol. 15, no. 4 (2018), pp. 533–537.

と主張する。つまり、「サイバー空間」といえども、ICT インフラは物理的に存在し、その保護は「レンガやモルタルでできたものを保護する」のと変わりないということである[20]。

これに対して、ゲイリー・コーン（Gary P. Corn）とロバート・テイラー（Robert Taylor）による研究は、「国家が空、宇宙、海域を統治するために大きく異なる体制を発展させてきた」と指摘する。つまり、主権は厳格な規則ではなく、原則であって、それらの空間において主権が国際法にどのように反映されるかは、「領域と国家の実際的な義務に応じて調整される」。ゆえにサイバー空間の「独自の特殊性」へのその適用は、今後の国家実行に委ねられていると述べる[21]。

両論を比較すると、たしかに「サイバー空間」も国家領域内に所在する物理インフラによって構成される以上、領域主権原則が一般法として適用されると考えられる一方で、その「独自の特殊性」を背景とする特別法が形成されることは妨げられないと考えられる。そのような特別の規則として、例えば海洋法について、領海には主権が及ぶ一方で、領土・領空と異なり、他国の軍艦であっても無害通航の権利を有するとの規則が、慣習法上および条約上発展してきた[22]。したがって、サイバー行動を規律する法においても、領域性に基づいた主権原則の適用を修正する特別法が形成されるかは今後の国家実行によると考えられる。次節で参照する相対主権論への支持の広がりは、領域性に基づく判断基準に部分的な修正を加える可能性をもたらす実行といえる。

2．越境的なサイバー行動が主権侵害となる基準についての議論

以上のように、「サイバー空間」を構成する ICT インフラは領域内に物理的に存在する以上、サイバー行動も領域主権に照らして一般に評価できるとの前提に立つとしても、政府によるいかなる越境的なサイバー行動が主権侵害を生じさせるのかが争点となる。政府が外国のサーバーに保存される公開データにアクセスすることは日常的に行われるために許容される一方で、外国へのサイバー攻撃は非難されるべきとして、法的評価の基準はどこに求められるだろうか。

20 Kevin Jon Heller, “In Defense of Pure Sovereignty in Cyberspace,” *International Law Studies*, vol. 97, Issue 1 (October 2021), p. 1469.

21 Gary P. Corn and Robert Taylor, “Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0: Sovereignty in the Age of Cyber,” *AJIL Unbound*, vol. 111 (2017), p. 210.

22 Sean Watts and Theodore T. Richard, “Baseline Territorial Sovereignty and Cyberspace,” *Lewis & Clark Law Review*, vol. 22, no. 3 (2018), pp. 867–868.

この点について『タリン・マニュアル』の起草過程では、引き起こされる物理的・機能的影響の程度を基準とする見方が示された。もっとも、その基準については起草した専門家の中でも意見が分かれている。そして、各国の立場においても同様の見解の相違がある。

（1）『タリン・マニュアル』における議論

（ア）主権侵害の評価基準

『タリン・マニュアル』の解説は、越境的なサイバー行動が主権侵害を構成するかについて、2 つの評価軸を提示している。1 つ目は、「対象国の領土保全（territorial integrity）に対する侵犯の程度」であり、国家はその主権領域への立ち入りを管理するという前提から導かれる。もう 1 つは、「本質的に政府が行う機能に対する妨害または侵奪が行われたか」である [23]。

そこでサイバー行動についても、他国の主権を尊重する義務の 2 つの側面から適用が検討される。第一に、領土保全の側面について、遠隔で行われる越境的なサイバー行動が主権侵害に該当する場合として、引き起こされる効果に応じて段階的に異なる評価が示されている。①物理的損害を直接または結果的にもたらす場合、②物理的損害を伴わないが、機器の機能喪失を引き起こす場合（例えば、オペレーティングシステム（OS）やデータの再インストールが復旧に必要となる場合）、③物理的または機能的影響をもたらさない場合（例えば、システムへのバックドアの設置）である。①が主権侵害に該当することについてはほとんどの専門家が同意したとされるが、②への支持はより少なく、③は一部の専門家の支持に留まったとされる [24]。

第二に、本質的に政府が行う機能、例えば外交や国防、徴税、選挙の実施を妨害するサイバー行動は、物理的損害や機器の著しい機能妨害を伴わない場合であっても主権侵害に該当し得るとされる。さらに、「本質的な政府の機能を他国の領土内で遂行してはならない」という点で専門家の意見は一致し、その例として、他国領域での法執行機能の行使が挙げられた [25]。

（イ）他国領域での執行管轄権の行使

『タリン・マニュアル』は管轄権に関する規則についても、国家は外国政府の同意が

23 *Schmitt, Tallinn Manual 2.0*, p. 20 (Rule 4, para. 10).
24 Ibid., pp. 20–21 (Rule 4, paras. 11, 13–14).
25 Ibid., pp. 21–22 (Rule 4, paras. 15–17).

ある場合に、当該国の領域にある個人、物、およびサイバー行動に管轄権を行使できるとの原則論を維持している。反対に言えば、後述のサイバー犯罪条約のような特別に合意された制度がなければ、「A 国の法執行機関が B 国内にある容疑者のコンピューターに侵入することは、B 国の同意を得なければ違法な域外執行管轄権の行使となる」[26]。

以上のように『タリン・マニュアル』は、越境的なサイバー行動が主権侵害を生じさせる場合について、領域性を 1 つの判断基準として、領土保全の侵犯については一定の効果を基準としたが、どの程度の効果かは、専門家の間で見解が分かれた。本質的に政府が行う機能への妨害は効果に拠らず、他国の領域での同意のない法執行は、サイバー手段によって遠隔で行われる場合でも、主権侵害を生じ得るとする。

（2）各国の見解

サイバー行動の文脈における主権侵害について、各国の見解は、先述のように、主権原則それ自体が具体的な義務を課しているかをめぐり、「原則としての主権アプローチ」と「規則としての主権アプローチ」とに分かれる[27]。もっとも、英国が前者を明示に支持する一方で[28]、他の多くの国は後者の立場、すなわち主権原則が実体規則として機能し、主権侵害は国家責任を生じさせる違法行為であるとみなしている[29]。

しかしながら、主権原則それ自体を規則と見る国の間でも、『タリン・マニュアル』同様に、いかなるサイバー行動が主権侵害となるかについては議論が分かれている。その解釈適用基準についての 2 つの考えは純粋主権論と相対主権論と称されてきた[30]。両論の相違は、「無許可のアクセス」を主権侵害とみなすか（純粋主権論）、あるいは一定の有害な効果を伴う行動に限定するか（相対主権論）にある。以下ではこれらのそれぞれの見解を採る国の立場を概観し、両見解の相違の実践的意味について検討を進める。

（ア）純粋主権論

純粋主権論に整理される国として、これまでフランス、スイス、イランが挙げられてきた[31]。もっとも、フランスの、「自国システムに対するあらゆるサイバー攻撃が主権

26 Ibid., Rule 11, paras. 7–8.
27 両アプローチを端的に整理する論考として次を参照。黒﨑「サイバー空間における主権」31–43 頁。
28 Michael N. Schmitt and Liis Vihul, “Respect for Sovereignty in Cyberspace,” *Texas Law Review*, vol. 95, Issue 7 (2017), pp. 1641–1642.
29 Heller, “Pure Sovereignty,” pp. 1444–1450.
30 Moynihan, “Sovereignty and Non-intervention,” p. 24.
31 Heller, “Pure Sovereignty,” pp. 1458–1459.

侵害を生じる」という表現は抽象的である[32]。主権侵害となる行為の具体的な基準は、外国の ICT インフラへの「無許可の侵入（unauthorized penetration）」というスイスの表現に求められる[33]。

2021 年の「サイバー空間における主権原則の適用に関する中国の立場」はより明確であり、「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「対内的な優位性および対外的な独立性」を侵害する行為は主権侵害になるとして、これに領域内または管轄下の「ネットワークシステムへの無許可の侵入」が含まれると主張する[34]。

さらに、2024 年にアフリカ連合（AU）が採択した、加盟 55 か国の「共通の立場」も、「外国領域にある ICT インフラへの国による、いかなる無許可のアクセス（any unauthorized access）も領域主権を理由に違法である」と評価する。そのうえで、相対主権論が前提とする有害な効果の閾値の存在を否定しており、純粋主権論を積極的に推進する見解として注目される[35]。加えて AU は執行管轄権について次のように説明している。

> 15.　[…] AU は、外国領域から発せられる違法なサイバー活動に対して、当該外国領域において執行権限を行使することを国家に許可していないことを確認する。このことは、国家によるそのような執行権限の行使が、仮想的であれ物理的であれ、外国の領域に対する有害な効果をもたない場合であっても適用される。[…]
>
> 17.　AU は、サイバー空間において適用される国際法の規則の成文化について、国家が外国領域において執行管轄権を行使することを認めるような規則、あるい

32 Ministére des Armées, *Manuel de Droit des Opérations Militaires*, Avril 2022, p. 302; see, Aude Géry, "Navigating France's Views on Sovereignty in Cyberspace: Why Might France Not Be in the 'Sovereignty-As-a-Rule' and in the 'Pure Sovereignty' Camps," EJIL:Talk!, September 19, 2024, https://www.ejiltalk.org/navigating-frances-views-on-sovereignty-in-cyberspace-why-might-france-not-be-in-the-sovereignty-as-a-rule-and-in-the-pure-sovereignty-camps/.

33 Federal Department of Foreign Affairs, "Switzerland's Position Paper on the Application of International Law in Cyberspace," May 2021, p. 3; 同様にイランも「不法な侵入（unlawful intrusion）」に言及する。"General Staff of Iranian Armed Forces Warns of Tough Reaction to Any Cyber Threat," *Nournews*, August 18, 2020, https://nournews.ir/en/news/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat. もっとも、スイスは主権原則の違反を構成するものを定義づけることは難しいとして、解釈議論の余地があるとの不確定的な立場を示している点で純粋主権論の位置づけには疑問が残る。

34 Ministry of Foreign Affairs, "China's Views on the Application of the Principle of Sovereignty in Cyberspace," December 2021.

35 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; *See also*, Kevin Jon Heller, "The African Union (Rightly) Endorses Pure Sovereignty in Cyberspace," Opinio Juris, February 5, 2024, https://opiniojuris.org/2024/02/05/the-african-union-rightly-endorses-pure-sovereignty-in-cyberspace/.

> は国家領域主権の不可侵の規則が保護する範囲を縮小する危害の閾値を定める規則の成文化は、政策的観点から重大な危険性をもたらすことを強調する。国家間の技術的能力に大きな格差があることを考えれば、コルフ海峡事件で国際司法裁判所が留意したように、そのような規則は「物事の性質上、最も強力な国家に留保される」ことになり、国家の独立と主権的平等の原則を損なうような深刻な濫用を引き起こし得るだろう。（下線は引用者）

このように主権侵害と評価する基準として「無許可の侵入やアクセス」が示される。もっとも、いずれの主体による許可が必要とされるのかは明らかでない。ICT インフラへのアクセスを許可する実質的な権限は、その管理者にある一方、主権侵害の有無を第一に判断するのは領域国政府である。政府が管理する ICT インフラの場合は両者が重なるが、民間事業者や個人が管理する場合には異なる。AU が主権の領域性を強調している点からは、私人が管理する ICT インフラへのアクセスにも領域国による許可が必要なことを意味していると解される[36]。

（イ）相対主権論

一方で、『タリン・マニュアル』で多くの専門家が支持したように、引き起こされた物理的損害や機能喪失を評価指標とする見解がより多くの国に見られる[37]。日本をはじめ、多くの国が重要インフラの「機能喪失」をもたらすサイバー攻撃が主権侵害となる可能性を示している[38]。もっともそれらの国の見解からは、『タリン・マニュアル』の専門家の間でも意見が分かれた、物理的損害や機能喪失といった危害に満たない程度のサイバー行動までも主権侵害となるかどうかは明らかではない。

これに対して、いくつかの国は、主権侵害の有無を評価する効果基準には閾値が存在し、閾値以下の効果しかもたらさないようなサイバー行動は主権侵害に該当しないと明言していることは注目される。例えば、2022 年のカナダの立場はこの見方を詳細に説明している[39]。

36 Russell Buchan and Nicholas Tsagourias, “The African Union’s Statement on the Application of International Law to Cyberspace: An Assessment of the Principles of Territorial Sovereignty, Non-Intervention, and Non-Use of Force,” EJIL:Talk!, 20 February 2024, https://www.ejiltalk.org/the-african-unions-statement-on-the-application-of-international-law-to-cyberspace-an-assessment-of-the-principles-of-territorial-sovereignty-non-intervention-and-non-use-of-force/.

37 Government Offices of Sweden, “Position Paper on the Application of International Law in Cyberspace,” July 1, 2022.

38 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。

39 Government of Canada, “International Law Applicable in Cyberspace,” paras. 14–19.

14.　[…] 影響を受けた国の領域主権の侵害が発生したかどうかを判断するためには、[…] 引き起こされた混乱の範囲、規模、影響または深刻さ（scope, scale, impact or severity）を評価しなければならない。

15.　一般に、サイバー行動の影響または深刻さは、物理的活動と同じ方法で、同じ基準に従って評価される。無視できる程度の、または最小限の効果基準（a level of negligible or *de minimis* effects）を超えて、他国の同意なしにその領域内で重大な有害の効果を引き起こすサイバー活動は、その影響を受ける国に対する領域主権規則の違反に該当し得るだろう。[…] さらに、カナダ国内から遠隔で行われ、外国での効果が無視できる程度のサイバー活動は、カナダによる執行管轄権の域外行使を伴うものではない。[…]

17.　領域主権の規則は、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。また、国が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、または国家安全保障上の利益を保護するために、無視できる程度の、または最小限の効果しか及ぼさない措置を講じることは、領域主権の規則によって妨げられることはない。カナダは例えば、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は、おそらく領域主権の侵害に当たらないだろうと考える。

18.　領域主権の侵害を評価するためのもう 1 つの重要な根拠は、サイバー活動が他国の本質的な政府機能を妨害または侵奪するかどうかである。[…] 物理的な損害、傷害、または機能喪失があるかどうかに関係なく、政府機能への影響によって領域主権が侵害される可能性がある。例としては、患者の健康記録や緊急治療室のサービスへのアクセスを阻むことで医療の提供を中断し、患者の健康や生命にリスクをもたらすサイバー活動がある。

19.　重要なことは、サイバー諜報活動のような一部のサイバー活動は、領域主権の侵害、したがって国際法の違反にはならないということである。（下線は引用者）

注目すべきは「無視できる程度の、または最小限の効果」の閾値である。他にも、ニュー

ジーランド[40]、ドイツ[41]やデンマーク[42]も同様の閾値の存在を主張している。また、チェコも同様であり、閾値を超えて主権侵害と見なし得る具体的な例として、「数千世帯に影響を及ぼす深刻な停電を引き起こすサイバー行動」や「政府が使用するコンピューターを暗号化するランサムウェアを展開し、その結果として年金やその他の社会保障給付の支払いが不能になる場合」を挙げている[43]。

（ウ）小括

以上のように、相対主権論と純粋主権論は対比的に捉えることができる。もっとも、両解釈に基づく主権侵害となるサイバー行動の範囲は大きく異なるわけではない。『タリン・マニュアル』が示す主権原則の二側面に沿って整理すると、領土保全の側面について、物理的な損害に加え、大規模な停電のように重要インフラの機能喪失を引き起こすようなサイバー行動を国が行うことは、いずれの見解においても違法な主権侵害と評価され得る。両見解の違いは、一定の効果を閾値としてそれを下回る「無視できる、または最小限の」効果しかもたらさない域外的なサイバー行動は主権侵害とならないか、または領域内または管轄下のICTインフラへの無許可のあらゆる侵入・アクセスが主権侵害とみなされるか、という点にある。

一方で、政府の本質的な機能の妨害または侵奪の側面については、相対主権論の立場からも、物理的損害や機能喪失が引き起こされたかどうかに関係なく認められることが示されており、この限りでは純粋主権論と相違ない。もっとも、この側面において相対主権論の立場からいかなる越境サイバー行動が主権侵害と認められるかについては、個別の文脈による行為が挙げられているに留まり、また挙げられた行為は身体や健康へのリスクや政府サービスの停止といった効果をもとに判断し得るものといえる。損害や機能喪失を引き起こさない、政府システムへの単なる侵入が政府機能の妨害に当たるかは不明である。

加えて、外国での効果が無視できる越境サイバー行動は「執行管轄権の域外適用とならない」というカナダの主張は、執行管轄権の域外適用は許容されないという従来的な見方を維持しつつも、域外性の評価に効果の基準を考慮するものと読める。ゆえに、カナダの主張は、国が法執行目的で外国のICTインフラにアクセスし、しかし何らの

40 New Zealand Ministry of Foreign Affairs and Trade (MFAT), “The Application of International Law to State Activity in Cyberspace,” June 17, 2025, paras. 11–15.
41 Federal Government of Germany, “On the Application of International Law in Cyberspace,” March 2021, p. 4.
42 Jeppe Mejer Kjelgaard and Ulf Melgaard, “Denmark’s Position Paper on the Application of International Law in Cyberspace,” *Nordic Journal of International Law*, vol. 92, Issue 3 (May 2023), p. 449.
43 National Cyber and Information Security Agency, “Czech Republic Position Paper on the Application of International Law in Cyberspace,” March 2024, pp. 3–4.

効果も伴わない場合、主権侵害に当たる執行管轄権の域外適用でも政府機能の侵奪でもないと評価し得る。よって、相対主権論と純粋主権論の注目すべき相違は、「無視できる、または最小限の効果」の閾値にあると改めて確認できる。

3．純粋主権論と相対主権論の実践的意義

では越境的なサイバー行動への主権原則の適用をめぐる議論は今後どのように発展すると考えられるだろうか。これを分析するための 1 つの視座は、法解釈論としての妥当性である。しかしながら、前節で論じたように、主権原則をサイバー行動に適用するにあたり、従来通りの領域性に基づく主権原則の適用か、それともサイバー行動の「独自の特殊性」から適用の修正を必要とするかという根本的な認識の相違がある。

この相違は国家の立場にも見られ、例えば、相対主権論に立つニュージーランドは、明確な領域的つながりを持たないというサイバー空間の性質と、複数の管轄権領域を跨いで行われるというサイバー行動の特徴が、悪意あるサイバー行動に機会を与えており、その防止のためには、主権原則の適用においてこうした特徴を考慮しなければならないと主張する[44]。他方で、純粋主権論を支持する中国は「サイバー主権」を指針として、グレート・ファイアウォールに代表される国境管理型のデジタル政策を推進してきたことを指摘できる。さらに、この認識の相違は、国のサイバー、さらには情報政策全体の底流をなす秩序観ともいえるべきものに関わる。自由民主主義国は、情報の自由の確保の観点からサイバー空間の開放性や脱領域的な接続性を重視する一方で、権威主義国は体制維持のために、国内の監視を含むサイバー・情報空間の領域的な管理を重視するといえる[45]。このように相対主権論と純粋主権論の前提となるサイバー空間に対する認識的相違は、国家制度の根本に結び付く以上、それぞれを支持する国家の見解もまた平行線を辿るだろう。

今後の規範形成の方向性を展望するためのもう 1 つの分析軸は、主権原則の適用がなされる個別の政策実践である。「無視できる、または最小限の効果」の閾値を設定する相対主権論を支持することは、その閾値未満の越境的なサイバー行動の裁量の確保を示唆する。そのような行動として、先行研究ではサイバー諜報活動が取り上げられてきた[46]。これに加えて、相対主権論を支持する国による越境サイバー行動としては、

44 New Zealand MFAT, “The Application of International Law,” para. 13.
45 See, Lahmann, “Sovereignty Discourse,” pp. 67–86.
46 Heller, “Pure Sovereignty,” pp. 1480–1486.

越境リモートアクセス捜査や、サイバー攻撃に利用される外国の機器の機能を妨げる措置も挙げることができる。そこで、以下ではこれら3つの政策類型を順に検討し、相対主権論の主張を動機づけるものであることを示すとともに、純粋主権論を支持する側は、これらの政策をどのように位置づけているかについても短く言及する。

（1）サイバー諜報活動

サイバー諜報活動は、秘匿されたデータにアクセスし、窃取する点で当該データの機密性を損なう。純粋主権論の立場からは、不正アクセスを伴う点で、サイバー諜報活動は違法な主権侵害を構成すると評価される[47]。

一方、サイバー諜報活動はそれ自体として破壊的・妨害的な効果の創出を目的としたものではない。「原則としての主権アプローチ」をとる英国の背景にある政策的考慮として、サイバー諜報活動の自由の確保が指摘されてきたが[48]、相対主権論をとる国も同様の評価を示しており、上掲のカナダの見解に加え、ニュージーランドも、主権原則はサイバー諜報活動それ自体を制限するものではないとの見方を示している[49]。

他方で、これらのファイブ・アイズ諸国は、自らに対するサイバー諜報活動を安全保障上の重大な懸念を生じさせ、また産業情報の窃取は公平な経済競争を歪めるものと非難してきた[50]。つまりこれらの国にとって、サイバー諜報活動が主権原則に制限されないとの立場をとることは、自らの法的主張と実践の整合性を担保しつつも、サイバー諜報活動の自由から得られる利益が、国際的な規制から得られる利益よりも大きいと評価して主権原則による規律を否定する法政策戦略をとっているといえる。

もっとも、サイバー諜報活動はファイブ・アイズ諸国によってのみ行われてきたわけではない。西側諸国は、ロシアや中国、イランなどによる諜報活動を含むサイバー攻撃を暴露・非難してきた[51]。この非難に対して、純粋主権論を主張する中国やイランは、非難された自らの行動をその法的立場から正当化するのではなく、サイバー攻撃

47 Ibid.
48 黒崎「サイバー空間における主権」36–37頁。
49 New Zealand MFAT, “The Application of International Law,” para. 14.
50 ロシアによるサイバー諜報活動に対するファイブ・アイズ諸国による公式の非難がサイバー諜報活動を許容し得ないものと設定するものであったかの論争については、次を参照。瀬戸崇志「国家のサイバー攻撃とパブリック・アトリビューション：ファイブ・アイズ諸国のアトリビューション連合とSolarWinds事案対応」（NIDSコメンタリー第179号）防衛研究所、2021年7月15日、8–10頁。
51 See, e.g., Center for Strategic and International Studies, “Survey of Chinese Espionage in the United States since 2000,” March 2023, https://www.csis.org/programs/strategic-technologies-program/survey-chinese-espionage-united-states-2000; Alexander Martin, “Iranian Cyber Spies Are Targeting Dissidents in Germany, Warns Intelligence Service,” The Record, August 11, 2023, https://therecord.media/charming-kitten-iran-targets-dissidents-in-germany.

の主体を特定することの困難さに基づく「もっともらしい否認」に依拠してきた[52]。これらの国は、自らの主張と行動との矛盾を無視し続けることのコストは小さいと認識していると考えられ、外国によるサイバー諜報活動の違法性を一方的に問う根拠として純粋主権論を採用するインセンティブを有するといえる。

（2）越境リモートアクセス捜査

社会のデジタル化が進む中で、犯罪の証拠となるデータの収集についても越境的な法執行活動の必要性が問われる。原則として外国での犯罪捜査・証拠収集は、当該領域国との国際捜査共助手続に則って行われなければならない。犯罪に関係する電子証拠が海外のサーバーに保存されている場合、当該サーバーの所在国に捜査共助を求めることになる。もしこうした手続を経ずに捜査を実施すれば、外国領域における同意のない執行管轄権の行使であり、主権侵害を構成し得る[53]。

他方で、捜査共助手続は常に迅速な捜査を可能にするわけではない。さらに、クラウドサービスの利用が広がる中で、データが保存されたサーバーが所在する国を確定できないという状況や、複数サーバーの経由による証拠の隠蔽といった、国際共助を通じた捜査の困難さも考慮する必要がある[54]。

そこで、外国にあるデータに捜査当局自らがアクセスすることを一定の条件下で許容する国際的な合意が結ばれてきた。サイバー犯罪に関するブダペスト条約は、データが公開利用に供されている場合（第 32 条 a 項）、またはデータの開示権限を有する者による「合法的かつ任意の同意」がある場合（同条 b 項）に他の締約国領域にあるデータへのアクセスを許容する。

もっとも、開示権限を有する者の「合法的かつ任意の同意」を欠く場合には、証拠の違法収集であるとして刑事裁判で主権侵害の有無が争われることがある。この点について、ノルウェーの警察が、同国企業の外国データに真正の同意なくアクセス・取得したことの適法性が争われた裁判において、ノルウェー最高裁は当該行為が主権侵害に該当するものではないと判断した。この理由の 1 つとして裁判所は、捜査が主権

52 See e.g., Anne Neuberger, “China is Winning the Cyber War: America Needs a New Strategy of Deterrence,” Foreign Affairs, August 13, 2025, https://www.foreignaffairs.com/china/china-winning-cyberwar-artificial-intelligence.

53 竹内真理「リモートアクセス捜査と国家管轄権：最二小決令和 3・2・1」『令和 3 年度重要判例解説（ジュリスト臨時増刊）』1570 号（2022 年 4 月）、248 頁。

54 European Union Agency for Criminal Justice Cooperation, “Second Additional Protocol to the Budapest Convention on Cybercrime and Cross-Border Access to Electronic Evidence,” 23 January 2024, https://www.eurojust.europa.eu/publication/second-additional-protocol-budapest-convention-cybercrime-and-cross-border-access.

侵害となる程度の影響を与えなかったことを挙げた[55]。この判断は、越境リモートアクセス捜査に関して、従来の域外執行管轄権の行使の禁止を画一的に適用するのではなく、対象行為がデータ所在国に及ぼす実質的影響に着目して主権侵害の有無を判断する慣行の萌芽的実行として注目される[56]。

しかしながら、個別の同意を不要とする越境リモートアクセス捜査は、普遍的に支持されているわけではない。むしろ、外国による国内データへのアクセスを全般的に制限する国にとって、領域国の個別の同意を要さないブダペスト条約の規定は望ましいものと見られてこなかった[57]。ロシアや中国は、欧州評議会が採択した同条約の普遍化に反対してきた[58]。一方で、それらの国は国連を場としたサイバー犯罪条約の作成を目指し、2024年末に国連総会で採択されたが、当該条約にはブダペスト条約第32条b項と同様の規定は見られない[59]。

（3）領域外に所在するサイバー攻撃に利用される機器に対する措置

国家関与型のサイバー攻撃や大規模化するサイバー犯罪の増加に対して、被害発生後での関与国に対する非難といった反応的対応による抑止の限界が指摘される。そこで、脅威主体が利用するコマンド・アンド・コントロール（C&C）サーバー等の「攻撃インフラ」に、警察・軍機関などがアクセスし、その機能を妨害あるいは無力化する措置の実施が有用となる。実際に、西側諸国を中心に、この措置を実施する国内法制度を整備する動きが広がっている[60]。措置の名称や法的位置づけは国ごとに異なるが、『タリン・マニュアル』では、「防御するサイバーインフラの外で積極的な（proactive）措置をとること」を「能動的（積極的）サイバー防御（Active Cyber

55 Supreme Court of Norway, HR-2019-610-A (case no. 19-010640STR-HRET), Criminal Case, Appeal Against Order: Tidal Music AS v. The Public Authority, paras. 60–71.

56 域外での執行管轄権の行使に対する評価においても、国籍主義や効果主義といった管轄権行使国と対象の人・行為との紐帯に依拠した立法管轄権の評価基準が導入されていることが指摘される。Cedric Ryngaert, “Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts,” *German Law Journal*, vol. 24, Issue 3 (April 2023), pp. 541–544.

57 Mailyn Fidler, “Fragmentation of International Cybercrime Law,” *Utah Law Review*, vol. 2025, no. 3 (May 2025), pp. 786–789.

58 Eric Siyi Zhang and Rogier Creemers, “Towards a UN-Centric Cybercrime Treaty,” Liden Asia Centre (February 2024), p. xv.

59 UN Convention against Cybercrime in Annex to UN General Assembly Resolution 79/243, A/RES/79/243 (December 31, 2024).

60 日本でも2025年5月にACDの法的基盤として「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」（令和7年法律第42号）（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」（令和7年法律第43号）（整備法）が成立した。諸国の動向を概説するものとして、Sven Herpig, *Active Cyber Defense Operations: Assessment and Safeguards*, Policy Brief Berlin (Berlin: Stiftung Neue Verantwortung, 2021), pp. 7–10, https://www.interface-eu.org/publications/active-cyber-defense-operations-assessment-and-safeguards

Defense: ACD）」と呼んでいる[61]。ただし、ACD は官民連携や防御ツールの提供といった政策・制度にも用いられるため、以下では上記の措置を指して「ACD 措置」と呼ぶ。

留意すべきは、ACD 措置がサイバー攻撃に対する防御措置と位置付けられる限り、一方的、あるいは報復的な攻勢的サイバー作戦とは区別される性格を持つということである。後者は対象国の送配電網の機能を妨害し、停電を引き起こすといったことも選択肢となるが、ACD 措置はそうした重大な効果を意図的に追求するものではなく、あくまで攻撃インフラの妨害に留まると整理される[62]。

ACD 措置の具体的な実施手段は多様である。例えば、攻撃者の C&C サーバーに対する直接の「ハックバック」のみならず、ボットネット化した機器にマルウェアを停止させるコマンドを送信するといった手段も含む。こうした措置は IP アドレス等から機器の所在を確認し、国内の機器に限定して実施することも考えられるが、諸国の ACD 措置に関する制度は国外の機器も措置の対象に含んでいる[63]。

ゆえに、越境的な ACD 措置の実施において主権原則との抵触可能性が検討される。相対主権論の主張からは「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に、最小限の破壊的な効果で必要な措置をとることを国家が禁止するものではない」と主張される[64]。他方で、純粋主権論の側からは「無許可のアクセス」を伴う以上、主権侵害と評価され得る。

もっとも、ACD 措置が仮に主権侵害を構成するとしても、サイバー攻撃に対する防御措置であると性格づけられる以上、対抗措置と緊急避難の抗弁の援用による違法性阻却の可能性を検討し得る[65]。この援用に関する詳細な検討は本稿の射程を超えるが、両制度が ACD 措置の実施をどの程度正当化できるかについては未だ議論の途上にあることを指摘できる。例えば、対抗措置は先行違法行為の存在を前提とするため、未だ被害が発生していない状況での ACD 措置の実施に際しては援用の限界がある[66]。また、緊急避難の援用には先行違法行為の存在を必要としないが、危険を避けるための

61 Schmitt, *Tallinn Manual 2.0*, p. 563 (Glossary).
62 Herpig, “Active Cyber Defense Operations,” p. 18.
63 例えば、日本の「整備法」は警察官職務執行法に第 6 条の 2 を新設し、第 3 項は、攻撃の通信機器が「国内に設置されていると認める相当な理由がない場合」の警察官によるサイバー危害防止措置の権限を定める。同様に新設の、自衛隊法第 81 条の 3 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認められるものが行われた場合」の自衛隊による被害防止の措置を定める。
64 New Zealand, para. 14.
65 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』1613 号（2025 年 7 月）88 頁。
66 Gary Corn and Eric Jensen, “The Use of Force and Cyber Countermeasures,” *Temple International and Comparative Law Journal*, vol. 32 (Spring 2018), pp. 130–131; 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。

唯一の手段であることを説得的に説明する必要がある[67]。

こうした要件を鑑みると、ACD 措置の実施に違法性阻却事由が常に援用できるわけではないといえる。措置を実施する国は、主権原則との整合を図るため、相対主権論の立場をとる政策的なインセンティブを持つといえる。

（4）政策目的の相違から導かれる二元論的理解の修正可能性

以上の 3 類型の政策は、主権原則の適用においては越境的なサイバー行動であるとの共通項で整理されるが、その政策目的に違いがある。サイバー諜報活動から得られる利益は行為国のものであり、政策目的は国際社会の共通利益の追求とはみなされない。被害国がサイバー諜報活動を行った国を非難・抗議する実行がある。一方で、犯罪捜査やサイバー攻撃の防止といった正当な目的において行われる越境リモートアクセス捜査と ACD 措置は、国際社会の共通利益に資するものとみなされる可能性がある。実際にリモートアクセス捜査は、領域国の同意を得ないにもかかわらず、抗議された事例は見られないとされる[68]。こうした政策目的による相違を踏まえれば、それぞれの行為類型を禁止または許容する、具体的な条約あるいは慣習法規則が形成される可能性がある。

この点で注目されるのが、近年発表された、サイバー諜報活動が間接的に引き起こす影響に焦点を当てる国の見解である。オーストリアは物理的損害や機能停止を主権侵害と捉え、また国家によるデータが悪影響を与えることなく他国の ICT インフラを通過するだけでは主権侵害とならないとする。この点、同国の見解は相対主権論に位置づけられるように思われるが、サイバー諜報活動について、政府のみならず民間企業に対するものも含めて、侵害が発見されたなら、システムを完全にシャットダウンし、クリーンアップと復旧までの間、一時的な代替システムを構築する必要があるため、主権侵害に当たると述べる[69]。この見解の妥当性は、サイバー諜報活動が破壊や妨害を目的とするサイバー攻撃と技術的に識別することが困難であるというコスタリカの見解からも支持される[70]。つまり、情報の収集を目的とするサイバー諜報活動それ自体は、機器の機能に影響を与えないものだとしても、それがシステムの完全性にリスクを残

67 Henning Lahmann, “The Plea of Necessity in Cyber Emergencies,” *Nordic Journal of International Law*, vol. 92, Issue 3 (October 2023), pp. 430–433.
68 石井「能動的サイバー防御」101 頁。
69 Austria, “Position Paper of the Republic of Austria: Cyber Activities and International Law,” April 2024, pp. 6–7, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Austrian_Position_Paper_-_Cyber_Activities_and_International_Law_(Final_23.04.2024).pdf.
70 Ministry of Foreign Affairs, “Costa Rica’s Position on the Application of International Law in Cyberspace,” July 21, 2023, https://cyberpolicyportal.org/states/costa-rica.

すために必要となる対応は最小限の効果に留まらない。

この見方は、相対主権論の「効果」アプローチをとりながらも、サイバー諜報活動の禁止を導く点で注目できる。進んで言えば、越境リモートアクセス捜査と ACD 措置は最小限の効果閾値以下であって許容されるが、サイバー諜報活動の間接的な影響は閾値を超えて許容されないという行為類型別の法的評価を可能にするものである。相対主権論と純粋主権論の意見対立が、これらの 3 類型の政策の合法性確保に動機づけられたものであるならば、この見方は二元論的状況に修正を加える可能性がある。

おわりに――サイバー行動への主権原則の適用に関する今後の議論のあり得べき方向性

これまでの検討をまとめると、越境的なサイバー行動への主権原則の適用に関する議論において、武力不行使原則や内政不干渉原則の適用の射程が限定されるために、適用法規の空白を埋める一般法規則として主権原則が注目されてきた。そのなかで、主権原則の抽象的性格と、サイバー行動の脱領域的な性格は、主権原則によって規律されるサイバー行動の範囲について、相対主権論と純粋主権論の解釈論的対立を生じさせてきた。いずれの立場をとるにしても、物理的損害や、重要インフラの機能喪失といった烈度の高い事態は主権侵害と認められる。両論の差異は、「無視できるまたは最小限の効果」の閾値未満の行為を許容するか否かにある。

それぞれの主権論を主張する動機は、サイバー空間をめぐる秩序認識に結び付いていると考えられるが、実践的な差異として、「最小限の効果」閾値の存在から、「キャッチ・オール」の純粋主権論とは異なる法的評価を導く行動に、あえて相対主権論を主張する動機があると考えられる。そこで、閾値以下の効果しかもたらさない行動として 3 類型の政策を提示した。

この検討を踏まえて、最後に今後の規範のあり得べき展開として、次の方向が考えられる。まず、「最小限の効果」しか与えない越境サイバー行動を全般的に許容するとの相対主権論をより多くの国が認める可能性がある。ACD 措置やリモートアクセス捜査の制度の広がりは、主権侵害の閾値の存在への一層の支持を集める可能性がある。一方で、越境サイバー行動の全般的な裁量の余地を残すことに対しては、AU が指摘するように、「最も強力な国家に留保される」との懸念を引き起こすだろう。

西側諸国における ACD 措置やリモートアクセス捜査の制度の広がりとは反対に、

限定的なサイバー能力しか持たない国は、領域国の許可のないアクセスを全般的に主権侵害と評価する純粋主権論を支持するインセンティブを有するといえる。しかしながら、そのサイバー諜報活動やサイバー攻撃が非難されてきた中国やイランも純粋主権論を支持している。これらの国の言行不一致の常態化は、純粋主権論が単なる虚飾と捉えられ[71]、サイバー攻撃の被害国はACD措置などの自助のための選択肢を残すために相対主権論を推進する可能性も考えられる。

相対主権論または純粋主権論が異なる秩序認識と政策利益から主張されることを踏まえれば、いずれかに収束していくことは考え難い。そこで、相対主権論を前提としつつも、特定類型の越境サイバー行動を禁止する形で修正する方向が考えられる。オーストリアとコスタリカが、サイバー諜報活動が引き起こす間接的な影響を考慮して禁止すべきとの主張を行っていることは、この発展方向の萌芽的な動きといえる。

他方では、リモートアクセス捜査やACD措置といった通信を介して行われる域外での法執行活動もなお主権侵害に該当することを前提としつつ、条約規則や、慣習法上の違法性阻却事由の援用によって、それらの行為の合法性を確保するという方向も考えられるだろう。「最小限の効果」の閾値を主張する国であっても、ACD措置の実施に対抗措置や緊急避難が援用可能であると主張していることは、相対主権論と純粋主権論の主張が平行する中で、これらの規則を発展させる方向が実質的な中庸の選択肢となり得ると考えられる。

ゆえに、サイバー諜報活動や、リモートアクセス捜査やACD措置といった政策は、その行為自体は「無視できる、または最小限の効果」しか伴わない越境サイバー行動として位置づけられるとしても、その政策目的や達成のための手段、方法の詳細な検討を基に、行為類型ごとの禁止または許容を明確化していく方向が、サイバー行動への主権原則の適用の実効性を高めるという観点からは望ましいといえる。この議論の方向性からは、リモートアクセス捜査やACD措置に関する各国の国内制度運用や情報公開の適切さを測る国際的な標準づくりが求められよう。これらの在り方については、別稿での検討課題としたい。

（防衛研究所）

71 Peter B.M.J. Pijpers, “Careful What You Wish For: Tackling Legal Uncertainty in Cyberspace,” *Nordic Journal of International Law*, vol. 92, Issue 3 (October 2023), pp. 418–421.

［付記］本稿の執筆にあたり、編集委員ならびに匿名査読者の先生方のご助力に感謝申し上げる。特にお一人の匿名査読者の先生からは、原稿を重ねて細部にわたり精査していただき、本稿の議論を深化させる多くのご助言を賜った。ここに記して深謝を表する。なお、本稿における見解や誤りの責任はすべて著者にある。