『境界研究』No. 5(2015) pp. 29-56

サイバー空間と国家主権

塩原 俊彦

はじめに

人類は核兵器という技術に直面し、その安全保障政策を一変させた。同じように、インターネットに代表される新しい技術に基づいて、「サイバー空間(cyberspace)」という、サイエンス・フィクションに由来する新しい現象が人類の安全保障政策に変革を迫っている。核兵器にかかわる安全保障問題はすでに拙著『核なき世界論』で取り上げたが、本稿はこの新しい事態であるサイバー空間を、その境界設定＝国家主権の行使の問題として論じるものである(1)。

まず、サイバー空間をめぐる先行研究を整理したい。とくに重要なのは米国政府のサイバー空間に対する認識の転換である。この方針転換こそ、その後、筆者が「現実主義的アプローチ」と呼ぶ、サイバー空間のインフラストラクチャに対する国家主権の行使につながっている。この点を裏づけるために、陸・海・空・宇宙といった空間の境界設定と国家主権との関係を概観する。そのうえで、サイバー空間について、近年、どのような現実主義的アプローチがとられてきたかを俎上に載せる。最後に、若干の結語を用意している。現実主義的アプローチは実は、米国政府の方針転換に依拠しており、ドワイト・アイゼンハワーが危惧した軍産複合体を利するように進んでいるようにみえる。そして、それは、覇権国による政治的決断によってなされたものであって、はからずもウクライナ危機が明らかにしているように、決して望ましいものではないと思われる(2)。

(1) 筆者が国家主権を強く意識するようになったのは、「腐敗」をめぐる筆者の最新の研究成果を執筆する過程においてであった。拙著は「腐敗」を、敵か味方を判別する互酬的交換とみなし、「人間の安全保障」の面から、世界史的観点にたって腐敗の規準がどう構成されてきたかについて論じたものである。その過程で、国家主権が腐敗規準の設定にきわめて大きな影響をおよぼしたことに気がついた。そこから、国家主権が空間をめぐる境界設定におよぼした影響についても重大な関心を寄せることにつながった。Toshihiko Shiobara, *Anti-Corruption Policies* (Tokyo: Maruzen Planet, 2013).

(2) ウクライナ危機は、米国政府がウクライナの過激なナショナリストを抱き込んで行った、民主国家の転覆劇であったと理解することがもっとも妥当であろう。その目的は米国産シェールガス由来のLNGによる欧州市場の奪取であったり、米軍事費の拡大であったりする。それを主導したのがいわゆる「ネオコン」の残党(ヴィクトリア・ヌーランドら)であった。ネオコンは「世界の民主化」という理念を掲げその実現のためには武力行使をいとわないとする人々であり、そこに軍事優先という価値観が現れている。彼らはいわゆる「デジタル外交」(インターネットやソーシャル・ネットワーク・サービスを利用した情報操作外交)により、武力による政権転覆に成功したのである。弱体化したとはいえ、依然として覇権国でありつづける米国に逆らうことが困難なドイツなど欧州各国は、米国による「ロシア離れ」の強制に屈服せざるをえなかったのだ。この点について詳しくは、拙稿『ウクライナ・ゲート：「ネオコン」の情報操作と野望』社会評論社、2014年を参照のこと。

1．サイバー空間をめぐる議論

人間は認識しにくい事象を、隠喩を使って想像することでそれへの理解を深めようとしてきた。「サイバー空間」についても同じである(3)。この言葉は1980年代のサイエンス・フィクションで使われはじめ、インターネット普及を通じて人口に膾炙するに至った(4)。これまでにさまざまな定義が試みられている。たとえば米国政府は「近代社会のほぼすべての面にかかわる、地球規模で相互に結ばれたデジタルな情報やコミュニケーション・インフラストラクチャ」と定義している(5)。英国政府は「ネットワークされたデジタルな活動のすべての形態で、デジタル・ネットワークを通じてなされる行動やその内容を含む」とサイバー空間を定義している(6)。他方、カナダ政府は「情報技術の相互に結ばれたネットワークおよびそのネットワーク上の情報によって創造される電子世界」とみなす(7)。

こうしたさまざまのサイバー空間概念を検討したデイヴィド・ベッツとティム・スティヴンスによると、サイバー空間にインフラを含めるケース（包含モデル）と含めないケース（排除モデル）に大別されるという(8)。インフラを排除するモデルでは、サイバー空間の「中に」いるという経験が物理的空間の多くの属性をもつとみなし、このヴァーチャルな環境が物理的世界よりも「リアル」でないということではなく、双方とも「アクチャル」な世界の要素とみるのである。その典型が1996年に公表された、ジョン・バーロウの「サイバー空間の独立宣言（A Declaration of the Independence of Cyberspace）」であろう。サイバー空間は「心の新しいホーム（new home of Mind）」であり、そこには主権は存在しない(9)。あるい

(3) すでに東浩紀が隠喩としてのサイバー空間の問題に真正面から取り組んでおり、興味深い分析を行っている。東浩紀『サイバースペースはなぜそう呼ばれるか＋』河出書房新社、2011年。

(4) そもそも「サイバー」とは、ノーバート・ウィナーらによってつくられた、動物と機械における制御と情報交換をめぐる「統治管理の術」、「サイバネティクス」に由来する。Adrian Mihalache, “The Cyber Space-Time Continuum: Meaning and Metaphor,” *The Information Society: An International Journal* 18, no. 4 (2002), pp. 293–301.「サイバー」は「舵をとる者」を意味するギリシア語の「キベルネテス（kybernetes）」からとられた（ロシア語では、サイバー空間はкиберное пространство と翻訳されることが多いが、このкиберが「サイバー」にあたり、サイバネティクスを想起させている）。それが「サイバー」と「パンク」を合成した「サイバーパンク (cyberpunk)」という言葉になって、1980年のブルース・ベスキによる同名の短編小説のタイトルに使われた。加えて、ウィリアム・ギブソンが1982年に著した短編小説『クローム襲撃（*Burning Chrome*）』で「サイバー空間」という言葉を使用し、1984年の『ニューロマンサー（*Neuromancer*）』でも使用して有名になった。なお、前注3の東浩紀の著作は、「サイバー空間」という言葉が『ニューロマンサー』で初めて用いられたと述べているが、これは誤りである。

(5) White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington D.C.: US Government Printing Office, 2009), p. iii.

(6) Cabinet Office, *Cyber Security Strategy of the United Kingdom: Safety Security and Resilience in Cyber Space* (Norwich: The Stationary Office, 2009), p. 7.

(7) Public Safety Canada, Canada’s Cyber Security Strategy: For a Stronger and More Prospective Canada (Ottawa: Government of Canada Publications, 2010), p. 2.

(8) David J. Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power* (The International Institute for Strategic Studies, 2013) [Kindle version].

(9) John Perry Barlow, “A Declaration of the Independence of Cyberspace” [https://projects.eff.org/~barlow/Declaration-Final.html] (2014年1月21日閲覧).

は、ディヴィド・ジョンソンとディヴィド・ポストは「ネット上のメッセージの移動の費用および速度が物理的位置からほぼ独立している」ことを理由に、「サイバー空間は領土に基礎づけられた境界をもたない」と主張する(10)。だが、それはサイバー空間という、隠喩から出発した概念に対する不十分な理解の結果であるとの批判を受けることになる(11)。

こうして現在では、インフラを含めたサイバー空間を前提とする議論が主流となっている。たとえば、ジョセフ・ナイは、サイバー空間には、物理的インフラ層とヴァーチャル層ないし情報層があると指摘している(12)。あるいは、マーチン・リビスキは、サイバー空間には、基本的に物理層、統語層、意味層の三層があると考えている(13)。物理層は電話線、ルーター、スウィッチなどからなる。統語層はつながるための情報のフォーマットや宛先(TCP/IP)などにかかわっている。意味層は人間ないし接続装置にとって意味をもつ情報を含んでいる。ローレンス・レッシグは、サイバー空間が本質的かつ不可避的に自由であったとしながらも、そのコントロールの必要性を説き、憲法、制定法に加えて「コード」による規制を主張している(14)。

サイバー空間に何らかのインフラを含めて考えると、その境界設定は容易に問題化してしまう。そして、それは国家主権との関係を問うことにつながる。ゆえに、包含モデルは既存の国家主権によるサイバー空間への干渉を当然のこととして受け入れている。問題はサイバー空間にどう境界を設定し、どのように国家主権を行使するかにかかっている。他方、排除モデルでは、サイバー空間は国際政治制度における主権をもった実体として認知されるべきだという主張になる(15)。そこでは、サイバー空間は伝統的な法的主権を超えたグローバルな空間として事実上の地位を授けられる。本稿では、過去の先行研究が、包含モデルの前提にたち、サイバー空間を「戦場」に向けて位置づけようとするものと、排除モデルに近い立場から、サイバー空間を「平和の場」として構築しようとするものに大別できることを示したい。

米国政府は2003年の段階ですでに、サイバー空間を国の重要な官民のインフラの「神経

(10) David R. Johnson and David Post, "Law and Borders: The Rise of Law in Cyberspace," *Stanford Law Review* 48, no. 5 (1996), p. 1370.

(11) たとえば、Julie E. Cohen, "Cyberspace As/And Space," *Columbia Law Review* 107 (2007), pp. 210–256を参照。この中で彼女は、サイバー空間を「分離された空間」とみる人々がサイバー空間の利用者の身体で具体的に感じられ、場所に関連した経験、および、リアルな地勢とデジタルな地勢との間の複雑な相互作用の両方を軽視していると批判した。

(12) Joseph S. Nye Jr., "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly*, 5, no. 4 (2011), p. 19.

(13) Martin C. Libiski, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge: Cambridge University Press, 2007), pp. 8–9. 同書の中で、彼は三層に加えて、「プラグマティック層」という、メッセージがなぜ発せられたのか、ないし送られたのかを文脈において理解するための層があると厳密化している。*Ibid*., pp. 236–240.

(14) Lawrence Lessig, *Code, version 2.0* (New York: Basic Books, 2006).

(15) これは「サイバー空間主権(Cyberspace Sovereignty)」なるものを認めるべきか否かという議論につながっている。Timothy S. Wu, "Cyberspace Sovereignty? The Internet and the International System," *Harvard Journal of Law & Technology* 10, no. 3 (1997), pp. 648–649.

システム」であるとしたうえで、その重大なインフラを稼働させる、多数の相互接続されたコンピューター、サーバー、ルーター、スイッチ、光ファイバーケーブルからなっていると定義している(16)。サイバー空間にインフラを強く結びつけることで、国家がその安全を保障する必要性があることを印象づけようとしているかにみえる。ただし、後述するように、2005年の米国の「国家防衛戦略」では、宇宙、公海、空域、サイバー空間を「グローバル・コモンズ」とみなしており、一国だけの境界設定を主張していたわけではなかった。その見方がオバマ大統領就任後、転換されるのである。

2006年12月、アメリカ統合参謀本部議長によって承認された「サイバー空間作戦向け国家軍事戦略」では、サイバー空間は「ネットワーク・システムと関連する物理的インフラを経由してデータを保存・修正・交換するために電磁波およびエレクトロニクスの使用によって特徴づけられている領域」と定義されている(17)。2008年1月にジョージ・W・ブッシュが署名した国家安全保障大統領指令54では、サイバー空間は「情報技術インフラの独立したネットワーク」を意味し、「インターネット、通信ネットワーク、コンピューター・システム、埋め込まれたプロセッサー、および重要産業のコントローラーを含む」とされたという(18)。ここで紹介したような米国政府の基本的な考え方が官民の分野にまたがるサイバー空間の安全保障をどう守るかという課題に突き当たっているのである(19)。

こうした包括的モデルに基づくサイバー空間への理解が広がるなかで、つぎに課題となったのが「サイバーパワー (cyberpower)」をめぐる問題である。陸・海・空・宇宙という空間に対応して、ランドパワー (landpower)、シーパワー (seapower)、エアーパワー (airpower)、スペースパワー (spacepower) といった、国家主権が各種空間におよぼす権能、権力といった「力」が国家安全保障上の課題となったことから、サイバー空間におけるサイバーパワーが議論の対象となったわけである(20)。

(16) The White House, *The National Strategy to Secure Cyberspace* (Washington, D.C.: The White House, 2003), p. 1.

(17) Peter Pace, *The National Military Strategy for Cyberspace Operations* (Washington, D.C.: The White House, 2006), p. 3.

(18) Daniel T. Kuebl, "From Cyberspace to Cyberpower: Defining the Problem," in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, eds., *Cyberpower and National Security* (Washington, D.C.: National Defense University Press & Potomac Books, 2009), p. 26.

(19) たとえば、米国政府の軍事・諜報上の情報交換の90%から95%は民間に所有されたシステム上を移動している。Jack Goldsmith, *The Cyberthreat, Government Network Operations, and the Fourth Amendment* (Washington, D.C.: The Brookings Institution, 2010), p. 2. ゆえに、政府は民間のインフラの安全保障にも無関心ではいられない。ただ、比較的問題なく安全対策のしやすい公的部門の利用するネットワークについては、2002年以降、米国政府は「アインシュタイン・プログラム」と呼ばれる政策を国土安全保障省が主導して推進している。簡単に言えば、単なるトラフィックの流れをモニターするもの(Einstein 1)からウィルス、ワームなどのmalwareの侵入・探知(Einstein 2)に、さらにmalwareと思われるパケットをブロックしようとするもの(Einstein 3)にまで進化しつつある。ただし、これは基本的には公的部門のネットワークの安全保障をはかるものであり、民間との連携強化が課題となっている。

(20) 四つのパワーについては次節で考察するが、本稿では、ランドパワーを陸軍力、シーパワーを海軍力のように軍隊の能力に限定して使用しようとするものではないことに注意を喚起しておきたい。こうした狭義の見方に基づいて、陸・海・空を論じた参考文献として以下を参照。長尾雄一郎、石津朋之、立川京一「陸と海と空と、そして…：軍事力の具体的形態と統合」『防衛研究所紀要』5巻2号、2003年、111–171頁。

ナイはサイバーパワーを、「電子的に相互接続された、サイバー領域の情報資源の使用を通じて優先的な結果を獲得する能力」であり、その資源は電子やコンピューターに基づく情報の創出・統御・コミュニケーションに関連しており、具体的にはインフラ、ネットワーク、ソフトウェア、人的力量といったものだとしている(21)。一方、「すべての運用環境における出来事や権力手段に対して影響をおよぼしたり優位を生み出だしたりするためにサイバー空間を利用する能力」という定義もある(22)。

いずれにしても、国家が大衆をコントロールすることでランドパワーを、シーラインを守ることでシーパワーを強化したように、国家が何らかの方法でサイバーパワーを強化することが必要だとの認識が広がっている。その方法として、技術進歩、オペレーションのスピードと範囲、サイバー空間の重大な資産である物理的インフラ(海底光ファイバーケーブル、通信衛星など)、国家動員などにおいて国家によるサイバーパワーの強化が課題とされるようになる(23)。この背景には、年々、増加傾向をたどったサイバー空間上の「攻撃」がある。サイバー空間上での「攻撃」によって、その安全保障が脅かされる事態が起きている。軍事機密や民間の重要情報などをねらった諜報活動のほか、特定の装置を破壊するためのスタックスネット(Stuxnet)というワームまで使われるに至っている(24)。

こうしたなかで、サイバー空間の安全保障問題により大きな関心が寄せられるきっかけとなったのは、長く国防総省やホワイトハウスに勤務し、クリントン政権下で安全保障・インフラ防衛・反テロ担当の「ナショナル・コーディネーター」に任命されたリチャード・クラークらによる『サイバーウォー(*Cyber War*)』という本であったと思われる(25)。同書では、サイバー戦争がリアルなものであり、グローバルなものであり、すでに始まったとされている(26)。サイバー戦争を「損害ないし破壊を引き起こす目的のために他の国家のコンピューターないしネットワークに侵入する国民国家による行動」と定義した上で、その論点として、核兵器と比較しながら抑止や先制攻撃などについて論じている(27)。

(21) Joseph S. Nye Jr., *The Future of Power* (New York: Public Affairs, 2011), p. 123.

(22) Kuebl, "From Cyberspace to Cyberpower" (前注18参照), p. 38.

(23) Gregory J. Rattray, "An Environmental Approach to Understanding Cyberpower," in Kramer, Starr and Wentz, eds., *Cyberpower and National Security* (前注18参照), pp. 262–272.

(24) スタックスネット・ワームは2010年6月に発見された。そのワームは産業のコントロールシステムをターゲットにし、イランの核プログラムをねらっていたと広く信じられている。大部分の作成者が国家の支援を受けた専門家ではないかという疑いが生じた。当時のアフマディネジャド大統領は、攻撃の背後にイスラエルと西側がいたとして非難した。スタックスネットはイスラエルと米国による共同で開発され、ナタンズ工場を攻撃したとされる。同工場の約千のIR-1遠心分離機が短期間に取り替えられた。そのワームはイランの核設備に、感染したUBSを経由して侵入したと思われる。最初の攻撃は2008年か。Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Vienna: Cyber Conflict Studies Association, 2013), pp. 344–349など。

(25) Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: HaperCollins Publishers, 2010).

(26) *Ibid*., pp. 30–31.

(27) *Ibid*., pp. 6, 189–217.

もちろん、これ以前にも、サイバー空間やその代表的存在であるインターネットの統治をめぐって国家主権がかかわる議論が存在した[28]。だが、サイバー空間での「戦争」までを想定した議論がその後、急速に広がることになったのである。

これに対して、上述した排除モデルに基づいて、国家主権が行おうとしていることを批判しているのがジェフリー・ヘレラである。彼は、サイバー空間が領土的なものではなく、ネットワークをめぐる電子形態の情報でしかないと主張する[29]。しかし、国家はサイバー空間によってもたらされた脅威に対応して、①部分的な国家自体の非領土化、②部分的なサイバー空間の再領土化、③サイバー空間と情報技術のコントロールしやすい領域への配置という三つの戦略をとろうとしているという[30]。あるいは、新しい軍事力推進の形態である「サイバー産業複合体(Cyber-Industrial Complex)」の支援のもとに国家が脅威を煽る現象(「脅威インフレーション」)を引き起こしていると批判するブリオ・ワトキンスの見解もある[31]。ゆえに、彼らは、健全な政策が提案・執行される前に、人々はサイバー上の脅威の機密扱いの証拠へのアクセスや、そうした脅威によってもたらされるリスクのさらなる検討の機会をもつべきだとのべている[32]。

さらに、トーマス・リドは、サイバー空間は空間でさえなく、インターネットの広がる適用範囲を記述するための目下の共通する隠喩にすぎないとして、排除モデルの立場をとりながら、結局のところサイバー攻撃は存在しないし、サイバー攻撃で人命が失われたことも傷つけたこともないし、建物が重大な被害を受けたこともないと断言している[33]。そのうえで彼は過去の経験された記録の注意深い評価などを通じて冷静な対応を求めている。

だが、日本の場合をみると、サイバー空間における地道な平和構築の必要性を説く主張はほとんど見受けない。原田泉・山内康英の編集による『ネット社会の自由と安全保障：サイバーウォーの脅威』(2005年)、『ネット戦争：サイバー空間の国際秩序』(2007年)、伊東寛による『「第五の戦場」サイバー戦の脅威』(2012年)、土屋大洋による『サイバー・テロ 日米vs.中国』(2012年)、谷口長世による『サイバー時代の戦争』(2012年)にしても、タイトルが物語っているようにサイバー空間が隠喩にすぎず、過去の現実の「戦争」とはまったく別の事態であることに留意すべきであるにもかかわらず、その空間であたかも「戦

(28) インターネット・ガバナンスと国家主権をめぐっては、以下の文献を参照のこと。Milton L. Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge: The MIT Press, 2010); Lee A. Bygrave and Jon Bing, eds., *Internet Governance: Infrastructure and Institutions* (New York: Oxford University Press, 2009).

(29) Geoffrey L. Herrera, "Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space" (Paper presented at the 1st International CISS/ETH Conference on "The Information Relations and the Changing Face of International Relations and Security," Lucerne, Switzerland, 23-25 May 2005) [http://kms2.isn.ethz.ch/serviceengine/Files/CRN/46419/ieventattachment_file/1443347D-7CD7-40E2-871D-33202AA7A91E/en/CISS-ETH_Herrera.pdf], p. 30.

(30) *Ibid*.

(31) Ferry Brio and Tate Watkins, "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy," *Harvard National Security Journal* 3 (2011), pp. 39–84.

(32) *Ibid*., p. 84.

(33) Thomas Rid, *Cyber War Will Not Take Place* (New York: Oxford University Press, 2013), p. 166.

争」が生じるかのように安易に考えているように思われる(34)。この点に警鐘を鳴らすことが本稿の目的にほからならない。

2．境界設定：国家主権の行使

つぎにサイバー空間に境界を設定する問題を国家主権の行使の観点から考察したい。過去において陸・海・空・宇宙という空間が国家主権の行使のもとにどのように境界設定されてきたかを振り返り、唯一の人為空間であるサイバー空間における境界設定問題を考えるヒントにしたい。他方、サイバー空間を「共有地」ないし「コモンズ(commons)」とみなす見解についても検討を加えたい。いずれも先行研究の整理を兼ねている。

分析を行う前に主権国家そのものについて簡単に説明をしておく必要がある。だが、紙幅の関係で、最小限にとどめたい。

「主権」とは、英語でsovereigntyのことである。「ある国家自身ないし別の国家を統治するための国家の権限」とでも訳すべき意味をもつ言葉である。この主権は永久性と絶対性という本質的な特徴をもっているとされる。これは、主権が国家を土台としている以上、国家が永続的であるのと同じように主権も永続的であり、また、主権は法によって拘束されず絶対的であることを意味している。重要なことはアレクサンダー・ダントレーヴが指摘するように、永久性も絶対性も権力が最高あるいは究極的でなければならないこと、つまり、それより上位にある何らかの権力から派生したものではあってはならないという条件を満たすべき点である(35)。こうした条件が徐々に満たされ、主権概念が見出されたのだが、それはstateを国家とみなすようになる時期(16 〜 17世紀)に対応している。主権がなくてはstateという国家は存在しなかったのである。ゆえに、ジョセフ・ストレイヤーは「われわれが主権と呼ぶ権力の集中は国家の存在にとって絶対必要であった」と指摘する(36)。

主権の背後には、ローマ法の研究を通じて生じた、共同体のどこかに、国民か君主か、それとも君主と国民が一体になったものか、いずれにしても国家の精髄たる権力があるとみなす考え方がある。法はこの最高の権力、至高の意志を背景に、共同体の変化に応じて行使される道具として統制されるのであれば、有効な諸規則とみなすことができるとみなすのである。この至高の意志は、それが最高であるがゆえに、自己以外の何物にも責任を負わないという理由によって法を超越する意志であり、それは、それより上位にある何らかの権力から派生したものではあってはならないという条件を満たすことで永久性と絶対

(34) 国際社会経済研究所監修、原田泉、山内康英編著『ネット社会の自由と安全保障：サイバーウォーの脅威』NTT出版、2005年；原田泉、山内康英編著『ネット戦争：サイバー空間の国際秩序』NTT出版、2007年；伊藤寛『「第五の戦場」サイバー戦の脅威』祥伝社、2012年；土屋大洋『サイバー・テロ 日米vs中国』文藝春秋、2012年；谷口長世『サイバー時代の戦争』岩波書店、2012年。

(35) A. P. ダントレーヴ著、石上良平訳『国家とは何か：政治理論序説(新装版)』みすず書房、2002年。

(36) J. R. Strayer, *On the Medieval Origins of the Modern State* (Princeton: Princeton University Press, 1970), p. 108.

性という主権の特徴を担保することになる。ここに、主権が成立する[37]。

国際的な面では、欧州におけるカトリックとプロテスタントの戦争を終結に導いた、複数の国家による1648年のヴェストファリア条約の締結が主権の確立につながった。もちろん、この条約によってすぐに主権が確立したわけではない。ヴェストファリア講和は、欧州の安定的な国際体系の構築に基礎的条件を提供したが、主権国家によって構成される近代主権国家体系へと変容する過渡的な出来事であったと理解できる[38]。

ここまでの国家主権に対する理解を前提に、陸・海・空・宇宙という空間に対する国家主権による境界設定の問題を個別に考察することにしよう。次いで、サイバー空間を「コモンズ」とみなす見方について若干の検討を加えたい。

2.1 陸・海・空・宇宙

国家主権は陸・海・空・宇宙という空間ごとに、そこでのパワーを強化し、国家主権の維持・拡大につなげてきた。ここでは、サイバーパワーを理解し、サイバー空間での国家主権の行使問題を論じるために、過去の四つの空間における「力」と国家主権とのかかわりについて考察したい。

(1)陸

陸上におけるランドパワーの議論で最初に注目を集めたのは、現代地政学の祖と呼ばれるハルフォード・マッキンダーである。彼は北極海と内陸以外に流れ込む川をもたない地域、かつアムール川上流以西からヨーロッパ東部に至る地域で、南はイラン高原以北を、「ハートランド(the Heartland of the Continent)」と呼んだ[39]。鉄道や電信にみられる、急速な産業化や技術そのものが軍事作戦の速さや規模を転換させるのを促すことに注目して、マッキンダーは、新しい輸送やコミュニケーションの利用に「ハートランド」の資源を動員する能力こそ「ハートランド」の諸国が通信防御ラインを創出し、それらの諸国が選んだ場所で軍事作戦に迅速に従事することを可能にすると予測した[40]。つまり、彼は陸軍の「力」といった狭いパワーではなく、産業や技術のもつ「力」も含めた広義のランドパワーの重要性によく気づいていたことになる。

その一方で、政治的・戦略的に重要な地域の周辺部(リムランド：rimland)を重視するニ

(37) 主権国家の生成をめぐっては、以下の文献が参考になる。同書にあるように、15世紀のイタリアで主権国家体系が準備されたと考えるべきであろう。山影進編著『主権国家体系の生成：「国際社会」認識の再検証』ミネルヴァ書房、2012年。

(38) 久保田徳仁「ウェストファリア国際体系の実像：1648年はどのような意義をもつ年なのか」山影編『主権国家体系の生成』、177頁。

(39) ハルフォード・ジョン・マッキンダー著、曽根保信訳『マッキンダーの地政学：デモクラシーの理想と現実』原書房、2008年、90-95頁。本書の英語原著は1919年刊。ただし、邦訳が参照した原典は1942年刊のもの。

(40) Rattray, “An Environmental Approach to Understanding Cyberpower” (前注23参照), p. 258.

コラス・スパイクマンの見方もある(41)。彼は、ユーラシア大陸の周辺部である、西ヨーロッパ半島や東アジアにある人口や物財に「力」の源泉を見出したのである。陸上を拠点とした空軍力のような軍事作戦上の発展が周辺地域の諸国による重要拠点での「力」の行使を可能とするからだ。彼はとくに通信を重視しており、コミュニケーション可能な範囲こそ軍事力の行使に重要であることに気づいていた。

上記二人はともにランドパワーを陸軍力に限定せず、「力」の源泉となる資源を特定し、一定の地域や場所を重視する考え方をとり、それを国家主権が「力」によって守ることを重視していたことがわかる。そう考えると、サイバーパワーを想定するとき、その「力」の源泉としての主たる資源を特定したり、サイバー空間における移動のための一定の重要な場を確保したりすることに国家主権がかかわる必要性があることがわかる(42)。

(2)海

実は、ランドパワーという、陸軍力を超えた広義の「力」が注目されるようになったのは、シーパワーという広義の「力」の重要性が知られるようになってからのことであった。つまり、広義のシーパワーの重要性が理解されるようになって以降、ランドパワーという新しい概念の必要性もまた認識されるに至ったのである。

アルフレッド・マハンが1890年に提示した「シーパワー」とは、「武力によって海洋ないしはその一部分を支配する海上の軍事力のみならず、平和的な通商及び海運をも含んでいる」(43)。狭義のシーパワーとしては、①海軍、②漁船隊、③商船隊、④海洋調査船隊などが考えられることになる。彼はそのうえで、シーパワーに影響をおよぼす一般的条件として、①地理的位置、②自然的形態(それに関連して天然の産物および気候を含む)、③領土の範囲、④人口の数、⑤国民性、⑥政府の性格(国家の諸制度を含む)を挙げている(44)。彼の主張に従えば、国家はシーパワーを発展させるために、海軍力だけでなく、民間商船の保護・育成はもちろん、安全な貿易そのものの確保も重要な課題となる。

これは、陸地戦から海戦への変化に対応している。16世紀以来、ヨーロッパ大陸の諸国は生まれたばかりの主権国家同士の関係として陸上の戦争を想定するようになっていたが、国家にとっての海戦の重要性が増し、それが陸地戦ではその重要性が理解されていなかった貿易などの重要性に気づかせたのである(45)。

ここで英国が世界帝国として世界の覇権を握ったことで、二つの無関係な国際法が並存

(41) Nicholas Spykman, *Geography of the Peace* (New York: Harcourt and Brace, 1944).
(42) Rattray, "An Environmental Approach to Understanding Cyberpower" (前注23参照), p. 258.
(43) アルフレッド・T・マハン著、北村謙一訳『マハン海上権力史論(新装版)』原書房、2008年、46頁。本書の英語原著は1890年刊。
(44) 同上、47頁。
(45) カール・シュミット著、生松敬三、前野光弘訳『陸と海と:世界史的考察』慈学社出版、2006年、100–101頁。本書の独語原著は1942年刊。

するようになったとするカール・シュミットの興味深い主張を紹介しておきたい(46)。西欧中心的世界秩序は生成するや否や海陸に分裂し、陸は主権国家の閉鎖的領土に分割され、海は国家から自由となったとする。つまり、フランスが中心の陸を基軸とする国際法とイギリスが中心の海を基軸とする国際法という二つの対立する法概念の世界があるという。そして、海洋は国家から自由であるという、海洋国家である英国がほぼ19世紀をとおして世界をリードし、国際法でも幅を利かすようになる。このシーパワーを根本から支えたのは蒸気船に代表される機械であり、その機械製造という経済力は後述するエアーパワーやスペースパワーにおいても重要な役割を果たすことになる。この延長線上に、電信、無線、電話、インターネットなどが位置づけられるのであり、これらに覇権国となった米国が深くコミットすることになる。こうした文脈に沿って、サイバー空間の問題を考察することが必要になるのである。

英国海軍の理論家ジュリアン・コルベットはマハンやドイツのカール・クラウゼヴィッツの影響を受けて、第二次世界大戦の勃発前に英国の成功が海運・軍事・経済・外交上の資源の統合の結果であることを指摘していた(47)。つまりシーパワーという広義の「力」に注目すると、シーパワーこそ地球規模の作戦行動にかかわる問題ということになる。

ここで、海洋空間への国家主権の干渉について簡単に説明したい。国家の領域は国家主権に服し、その国家による管轄権には、領域管轄権、人的管轄権、公役務管轄権といった区分がある。また、国家管轄権は、立法的管轄権ないし執行的管轄権として行使される。領域管轄権はその領域を構成する空間内において行動する国家の法上の権能を意味しており、国家の領土はその管轄権に含まれるのが当然とされる。だが、海や空についてはどう規定すべきかが問題になってきた(48)。1982年に採択された「海洋法に関する国際連合条約

(46) カール・シュミット著、長尾龍一訳『現代帝国主義論：戦争と平和の理論的考察』福村書店、1972年、140頁。本書の独語原著は1940年刊。

(47) Julian S. Corbett, *Some Principles of Maritime Strategy* (Annapolis: U.S. Naval Institute, 1988). 本書の英語原著は1911年ロンドン刊。

(48) ローマ法では、海は全人類に共有のものとされ、皇帝ユスティニアヌス(483-565AD)は海とその魚はだれもが利用できるものであって、いかなる国も沿岸を超えて管轄権をのばすことはできないと法に定めた。その後、ローマ帝国が没落すると、地中海での支配権を強めたヴェネツィアは1269年までにアドリア海のすべての船舶に通行料を課すようになった。その支配は17世紀まで継続した。14世紀になると、イタリアの法律学者が二日間以内の短期の船旅の範囲内として沿岸から100マイルのまでの領有権を主張するようになる。一日以内の60マイルという主張も生まれた。他方、新大陸の領有を争うスペインとポルトガルは1494年にトルデシリャス条約を、1529年にザラゴザ条約を締結するなどして海洋を含む領有権が問題化した。国際法の父とされるフーゴー・グロティウスは、海は所有の対象とされないとして、国家主権や教会による海洋支配を否定した。Susan A. Buck, *The Global Commons: An Introduction* (Washington D.C.: Island Press, 1998), pp. 76, 79. しかし、海洋がもたらす利益に気づいたイングランドは海賊や敵国の攻撃から自国の船舶を守る必要性から、沿岸から一定の範囲を領海として管轄する権限を国家に認めることを主張するようになる。この主張は賛同者を集めたが、問題は沿岸からの距離であった。砲弾に石を使うか鉄球を使うか、大砲の種類などによって沿岸から海を攻撃できる範囲が異なっていたから国によって意見が異なったのである。1782年にイタリアのガリアーニが射程距離3海里を限界とする説を主張し、19世紀中はこの説が支配的だった。1921年にソ連は12海里までの領海を主張するようになるが、1958年に作成され、1962年に発効した公海条約が最初の広範な合意となった。

(国連海洋法条約)」では、国家の領域管轄権に属する海(領域管轄権に服する内水、群島水域、領海、および限定された領域管轄権に服する排他的経済水域[接続水域を含む]、大陸棚)と国家の領域管轄権が及ばない海(公海[深海底を含む])を区分している。これは、第二次世界大戦以前にあった海洋を領海と公海に分けて国家主権の制限と海洋の自由を原則とする原理から、沿岸国の管轄権を空間的に拡大し、海洋空間における国家の経済・政治的利益の保護・調整を優先する原理への移行を意味している(49)。

ただし、国家主権による分断的空間秩序が整備されているわけではない。境界画定において隣接する国家間や複数の沿岸国間で空間的範囲が重複する場合がその例である。生態学的考慮の欠如も問題とされている。ゆえに、近年、「海洋空間計画(Marine Spatial Planning)」と呼ばれる海域管理手法が検討されている(50)。さらに、海の生物資源の枯渇に対処するためには国家主権の優先という現状は不適切なのではないかという見方もある。ゆえに、主権の原理と自由の原理を基礎として空間を区分するのではなく、空間の区分を認めつつ、同時に当該空間全体を国際社会の共通の利益を実現するための場(「国際利益空間」)とみる見方が現れている(51)。海洋空間をめぐる議論は未だに決着をみていないことになる。

(3)空

エアーパワーの理論に貢献したのは、まずイタリアのジュリオ・ドゥーエであろう。彼は、「飛行機をもってすれば、戦闘の影響は火砲の最大射程を超えて、数百キロメートルにも広がり相手の全領域におよぶ」としたうえで、「戦場に限界はなく、戦時には国境の内側の全域が戦場となり、すべての国民が敵の直接攻撃に曝されるため全国民が戦闘員となり、戦闘員と非戦闘員の区別はなくなる」と指摘している(52)。無差別爆撃により、住民の戦意を低下させ民間人に死者は増えるものの、戦争を早期に終結できることで全体としては死傷者を少なくできると主張している(53)。1918年に創設された王立空軍の参謀長ヒュー・トレンチャードも、爆撃機は空を支配し、防衛によって効果的に止められることはないだろうと考えていたという(54)。米国のウィリアム・(ビリー)・ミッチェル将軍も爆撃機の重要性を確信し、軍航空、民間航空、商業航空を統括する航空省の創設を主張した(55)。

こうなると、エアーパワーは領土や領海といった空間を超えて、直接、「力」を行使できるだけの作用をおよぼせることになる。それは、攻撃と防衛という相互関係をどうするか

(49) 田中嘉文「国連海洋法条約体制の現代的課題と展望」『国際問題』617号、2012年、7頁。
(50) 太田義孝「海洋空間計画(Marine Spatial Planning)の国際的動向とわが国での有効性の考察」『海洋政策研究』11号、2013年、1–14頁。
(51) 田中「国連海洋法条約体制の現代的課題と展望」、9–11頁。
(52) 瀬井勝公編『戦略論体系 ⑥ ドゥーエ』芙蓉書房出版、2002年、23頁。本書の伊語原著は1921年刊。
(53) 荒井信一『空爆の歴史:終わらない大量虐殺』岩波書店、2008年、9頁。
(54) Rattray, "An Environmental Approach to Understanding Cyberpower" (前注23参照), p. 260. ただし、この段階では、ミサイルなどによる防衛といった技術的発展を予想していたわけではなかった。
(55) William (Billy) Mitchell, *Skyways: A Book on Modern Aeronautics* (Philadelphia: J.B. Lippincott, 1930).

という問題や、どの分野に予算を傾斜配分すべきかといった問題を惹起する。これはサイバー空間における国家主権の対応の問題にもかかわることになる。

空をめぐっては、1899年にハーグで開催された列国平和会議で、飛行船や気球からの爆弾投下を念頭においた空爆の禁止宣言が出された(56)。一般住民を殺傷する可能性の大きい行為を避けるためである。第一次世界大戦中の空爆については、それまでの陸戦・海戦に関する国際法(「ハーグ陸戦法規と慣例条約」、「海軍力の砲撃に関する条約」など)の類推適用で間に合わせたが、戦後、ワシントン会議(1921-23)で、戦争法規の改正のための法律家委員会の設置・審議が決められた。1923年、ハーグ法律家委員会で「空戦規則」案が作成された。この案は条約化までは至らなかったが、第二次世界大戦勃発当時、空戦規則案は各国の空戦規範ないし指針として機能していたから、慣習国際法(「空戦に関する規則」)として定着したとみなすことができる(57)。以後、空爆については、国際軍事裁判所(IMT: The International Military Tribunal)憲章(1945年)における「人道の罪」(すべての民間人に対して行われた非人道的行為)、国際人道法(ジュネーブ条約、1949年)、ジュネーブ条約の追加議定書である「国際武力紛争の犠牲者の保護に関する追加議定書」(1977年)などで取り上げられている。

他方、領空については、まず、許可なしの気球による飛行が禁止されるというところから問題が始まった。1784年、パリでのことである(58)。その後、1891年以降、イタリア、フランス、ドイツで航空をめぐる法律問題が論文として公刊されるようになる。すでに、1870-71年の普仏戦争において気球を兵器として使用するようになっていたから、問題は深刻であった。国際法の分野では、国際法研究所で議論がなされるようになり、1902年、ポール・フォシーユらは「空の自由」を主張した(59)。1910年には、フランスの要請で空への国家主権の管轄をめぐって国際会議が開催された。

しかし、海洋と同じく領空問題も簡単には決着しなかった。空への国家管轄権のおよぶ航空領域はいわば、国際慣習法上確立していったにすぎない。1919年のパリ条約では、領土の上空に対する国家主権が完全な形で認められたが、これは第一次大戦前の原則を確認したにすぎない。締約国による上空通行の自由が当該国の許可を前提に認められた。ただし、戦争目的で通行することは禁止された。その後も、イベロ・アメリカ条約(1926年)、パン・アメリカ条約(1928年)などの条約が締結される一方で、民間航空機の安全確保のための航空法専門家国際技術委員会によるルールづくりが進んだ。パリ条約は1944年に署名

(56) 荒井『空爆の歴史』、9頁。

(57) 荒井信一によれば、日本だけでなく、各国は1940年春ころまでは、主義としては軍事目標以外の爆撃については抑制的な態度を公表していたが、戦争が進むにつれて、各国ともに軍事目標主義を骨抜きにして、実質的に無差別攻撃を意味する地域攻撃に傾斜していったという。同上、74、79頁。

(58) Peter H. Sand, Jorge de Sousa Freitas and Geoffrey N. Pratt, "An Historical Survey of International Air Law before the Second World War," *McGill Law Journal* 7, no. 1 (1960-61), p. 25.

(59) *Ibid*., p. 28.

された、国際民間航空を実現させる法制度であるシカゴ条約に踏襲されたが、戦争目的などのない自由な通行権については認められず、この議論は国際民間航空機関(ICAO)に委ねられた。加えて、シカゴ条約は、航空機が国家に登録し、運航許可を必要とすることとし、各締結国は軍事上の必要または公共の安全のため、一定の区域の上空の飛行を一律に禁止する、あるいは制限することもできるとされた。

すでに紹介した、1994年に発効した国連海洋法条約では、領海の上空については国家管轄権がおよぶとされた(第2条)。排他的経済水域、大陸棚、公海については上空飛行の自由が認められている(第58、78、87条)。ただし、2013年に中国と日本などとの間で問題化した防空識別圏のような問題や、つぎに取り上げる宇宙に対する国家主権の範囲といった問題がまだ残されている。加えて、米国は国連海洋法条約に署名すら行っておらず、本条約の遵守および執行には疑問符がついている。

(4)宇宙

スペースパワーは上空の範囲をめぐる問題であり、エアーパワーと深い関係をもっている。具体的には1957年10月4日、ソ連による初の人工衛星スプートニクの打ち上げ成功によって宇宙に対する国家主権による管轄権が現実的な問題として意識されるようになる。大陸間弾道ミサイルの発明もこれに拍車をかけた。技術発展で国家が宇宙空間に関与できるようになったから、当時のソ連と米国は国家安全保障上の競争の場として宇宙に関心を寄せたのである。米国のドナルド・レーガン大統領が「戦略防衛イニシアティブ」のなかでソ連から発射される核弾頭を搭載した大陸間弾道ミサイルを衛星で破壊するシステムを開発しようとしたのも、宇宙利用と国家管轄権のおよぶ範囲の論争を引き起こした[(60)]。

航空機が当初、偵察用に使用され、その後爆撃にも活用されたことを考慮すると、人工衛星も偵察を主眼に発展し、その後攻撃や防御にも使われる可能性があることになる。ただ、ライト兄弟が最初に飛行してから最初の航空機による戦闘までには10年かからなかったが、スプートニクの宇宙飛行から50年たっても宇宙は非武装のままである[(61)]。

国家主権に注目すると、当初、ソ連も米国もそれぞれの領土から衛星を発射する前に他国に許可を求めず、その飛行に抗議しなかったし、国連は宇宙における国家主権の原則は暗黙裡に拒否されているとの決議を通過させた[(62)]。1967年には、宇宙条約の通称をもつ、

(60) この論争については以下の文献を参照のこと。Philip W. Quigg, "Open Skies and Open Space," *Foreign Affairs* 37, no. 1, (1958), pp. 95–106; David E. Lupton, *On Space Warfare: A Space Power Doctrine* (Alabama: Air University Press, 1998); 福島康仁「宇宙空間の軍事的価値をめぐる議論の潮流」『防衛研究所紀要』15巻2号、2013年、49–64頁。

(61) Karl P. Mueller, "Totem and Taboo: Depolarizing the Space Weaponization Debate," in John M. Longsdon and Gordon Adams, eds., *Space Weapons: Are They Needed?* (Washington, D.C.: The George Washington University, 2003), p. 30.

(62) Quigg, "Open Skies and Open Space," pp. 97–98.

「月その他の天体を含む宇宙空間の探査および利用における国家の活動を律する原則に関する条約」が発効した。第1条で、宇宙空間の探査・利用は全人類に認められた活動分野とされ、「宇宙空間は、すべての国がいかなる種類の差別もなく、平等の基礎に立ち、かつ、国際法に従って自由に探査・利用できる」ことと定められた。ただし、ここで宇宙と翻訳されたouter spaceが具体的にどんな範囲を意味しているかの定義はない。1976年に発効した、いわゆる「宇宙物体登録条約」（衛星などの宇宙空間に打ち上げられる物体の登録などを定めた条約）も、空気の層と宇宙との間の境界を明確に定めていない。実は、国連には1959年に設置された宇宙平和利用委員会があり、その法律小委員会はこの境界をめぐる議論を進めているが、問題解決には至っていないのである(63)。

登録制により、宇宙空間上の物体を管理するという発想は海と空ですでに実践されてきた経緯がある。海では、1962年発効の公海条約第5条、1994年発効の国連海洋法条約第91条で、各国は船舶に対する国籍の許与、自国の領域内における船舶の登録、自国旗を掲げる権利に関する条件を定めることができるとされた(64)。2002年にはテロ対策として、300総トン数以上の国際航海する船舶に自動船舶識別装置の導入を義務づけることが海上人命安全条約の改正によって実現した。空については、1919年のパリ条約で航空機の国籍許与が定められ、シカゴ条約にも踏襲された。航空機の運航に伴い同機が他国の主権管轄にさらされる度合が高いことを考慮すると、国家に対する航空機の帰属が明確であることが船舶以上に重要になる。海賊行為に類似するハイジャックに対しては航空機不法奪取防止条約（ハイジャック防止条約、1970年）や民間航空不法行為防止条約（モントリオール条約、

(63) Patrick W. Franzese, “Sovereignty in Cyberspace: Can It Exist?” *The Air Force Law Review*, 64 (2009), p. 26.

(64) こうした制度は、海賊に対する安全をどう確保するか、それに国家主権がどう関与するべきかという問題に対する回答として長い時間をかけて整備されてきたものである。これは、海洋における旗国主義の大原則と呼ばれている。海上（特に公海）においては、従来から、船舶が所属する国（旗国）がその国内法（旗国法令）によって船舶を介した活動を規制し、これを通じて海上秩序の維持が図られてきた。奥脇直也「海上テロリズムと海賊」『国際問題』583号、2009年、21頁。旗国が旗国船を規制・保護することで、他国の艦船によるその船への介入が禁止された。ただ、旗国主義の埒外にあった海賊対策の必要から、1932年にはハーバード・ロー・スクールの研究グループによる「海賊に関する条約草案」が提案された。公海上で海賊船に遭遇した艦船は、海賊行為を制圧することが「普遍的管轄権」として国際法上認められている。現実には、海賊に関する国際法の規範が、実効的な取締を実現するほどまでには具体化されていない。岡野正敬「海賊取締りに関する国際的取り組み」『国際問題』583号、2009年、36頁。たとえば国際連合海洋法条約の第100条では、海賊行為抑止のための協力の一般的義務を規定しているが、各国が行なうべき協力の具体的な方法は定めていない。第105条は、いずれの国も海賊を逮捕・訴追・処罰することができるとしているが、締約国の取締義務を定めたものではない。1988年のシージャック対策向けの海洋航行不法行為防止条約（SUA条約）でも、現場での執行管轄権を締約国に付与しているわけではない。旗国主義がとられていても、船籍は形骸化している。「便宜置籍船」（1922年にパナマで登録されたのが最初とされ、1940年代末以降、世界に広がった、各国の船主が税金の安い国へ船籍を移し、同時に国際安全法規、定員法、最低賃金制等の制約から逃れて運航経費を切り詰めようとする船）がその典型である。公海条約第5条では、船舶と旗国との間に「真正な関係」の存在を求めているが、その実効性は疑わしい。最近では、「第二船籍制度」（本来の船舶登録制度とは別に特定地域を定め、そこに登録された船舶について、配乗要件、船舶税制、船員税制、社会保障制度などを緩和する制度）を導入する国が増えている。これも、船籍制度の形骸化とみなすことができる。

1971年）などがある。だが、海、空、宇宙をめぐる過去の登録制の経験はサイバー空間における主体の帰属問題の解決につながりそうもない。「攻撃」がどこからきたか、その主体はだれでどこに帰属するのかを短時間に判断するのは困難だからである(65)。

2005年の米国の「国家防衛戦略」では、宇宙、公海、空域、サイバー空間を「グローバル・コモンズ」とみなし、そこからの、また、そのなかでの作戦能力が重要であると規定している(66)。そのうえで、国際空域と宇宙からの作戦能力は共同作戦面から依然として重要なままであると指摘している。とくに、宇宙に基づくシステムへの国家の依存が増しつづけているため、新しい弱点に対して備えるとの方針が示されている。これは、中国の宇宙開発に対する警戒感を暗示している(67)。

2.2 サイバー空間：「コモンズ」としての空間

すでに指摘したように、サイバー空間にインフラを関連づけるかどうかによって、主権がおよぶかどうかの見方が異なってくる。これに対応して、インフラを排除して考える排除モデルでは、サイバー空間を「共有地（コモンズ）」とみなし、インフラを含んで考える包括モデルでは、単純なコモンズとはみなしていないようにみえる。排除モデルを支持するバーロウの「サイバー空間の独立宣言」には、コモンズという言葉はない。ただ、「すべての人々が人種によって授けられた特権ないし偏見なしに入ることのできる世界をつくろうとしている」という表現から類推すると、サイバー空間は「非所有（オープン・コモンズ）」

(65) たとえば、「分散型サービス拒否（DDoS: Distributed Denial of Service）」攻撃と呼ばれるものは、首謀者がコンピューター・ウィルスを不特定の人々のコンピューターに感染させ、感染したコンピューターが特定の日時に標的となるコンピューターのサーバーなどに一斉にアクセスするものである。ゆえに、たとえ何らかのサイバーオペレーションがある国家に存在するサイバーインフラを使ってなされたとしても、そのオペレーションがその国家に帰属するものだという十分な証拠とはなりえない（後述するタリン・マニュアルのルール8）。DDoS攻撃はエストニアやグルジアに対する攻撃が有名である。2008年8月9日、グルジア政府は大統領のウェブサイトを含む重要な政府のインターネットサービスを米国にあるチューリップ・システムズ（TSHost）に移した。Joshue E. Kastenberg, “Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law,” *The Air Force Law Review* 64 (2009), p. 60. その後も、モスクワやサンクトペテルブルクからのDDoS攻撃がTSHostのサーバーにもつづけられた。前日には、グルジア政府は外務省や政府のニュースサイトをグーグルのブログスポットに移動していた。つまり、グーグルやTSHostは米国政府の承認や関与を受けないままグルジアを支援したことになる。これは、米国のサイバー上の中立性を危険にさらす出来事であった。1907年のハーグ条約では、交戦国が同国の陸軍ないし海軍と情報交換するために中立国領内に無線局ないしその他の設備をつくることを禁止している。当時、ロシアとグルジアは交戦状態にあったから、グルジアの米国内でのウェッブサイト立ち上げはこの規定に違反していたとみることもできる。ただ、DDoS攻撃の主体の帰属先は不明であり、ロシア政府と米国政府がこの問題で対立することはなかった。

(66) The National Defense Strategy of the United States of America (March 2005) [http://www.defense.gov/news/mar2005/d20050318nds1.pdf], p. 13 (2014年9月3日閲覧).

(67) 中国の宇宙戦略については、David J. Thompson and William R. Morris, *China in Space: Civilian and Military Developments* (Alabama: Air University Press, 2011) を参照。より最近の状況については、Ajey Lele and Gunjan Singh, *China's Space Strategy and Modernization* (New Delhi: Observer Research Foundation, ORF Issue Brief, 49, 2013) を参照のこと。

と考えられているように思われる。

これに対して、包括モデルの立場をとるナイは、「サイバー空間はその一部が主権の支配下にあるので公海のようなコモンズではない。せいぜい、それは十分に発展したルールのない、『不完全なコモンズ』ないし共同所有のコンドミニアムにすぎない」と主張している(68)。だが、米国政府はすでに指摘したように、2005年の「国家防衛戦略」では、宇宙、公海、空域、サイバー空間を「グローバル・コモンズ」とみなしていた。あるいは、同じ2005年に国防総省がまとめた「本国防衛と民間支援のための戦略」においても、「グローバル・コモンズは公海、空域、宇宙、サイバー空間からなる」と明言している(69)。OECDの定義にしたがえば、「グローバル・コモンズは公海、宇宙、南極のような国家管轄権の外にある自然財産」ということになる(70)。この解釈にしたがってサイバー空間をグローバル・コモンズに含めると、そこで国家管轄権を行使するのは困難となりかねない。これは米国政府がサイバー空間への規制に慎重な姿勢をとってきたことに対応している。実際、とくにインターネット規制に対して、米国政府は慎重であった。インターネットの広範な規制を求めるロシアに対して、米国はインターネット上の検閲を合法化するような協定に反対の姿勢を長く示してきた(71)。

興味深いのは、オバマ大統領になって、政府の方針に明らかな変化がみられることである。それは、2009年5月の発言に現れている。彼は、「今後、毎日、我々が依存しているネットワークやコンピューターといったデジタルなインフラはあるべきもの、すなわち、戦略的財産として取り扱われるだろう」としたえで、「こうしたインフラを守ることが国家安全保障の優先課題となるだろう」と明言した(72)。あるいは、2011年にホワイトハウスが公表した「サイバー空間の国際戦略」では、サイバー空間を「クローバル・コモンズ」とする見方がない。「すべての国にとって、デジタルインフラは、国家資産(national asset)になっているか、または、なりつつある」として、むしろ、国家管轄権のおよぶ国家資産としてサイバー空間をとらえようとしている。つまり、サイバー空間をコモンズとはみなさいという方針転換を行ったように思われる。これに呼応するかのように、米国政府はロシアとの非公式の協議を開始した(73)。

(68) Nye, *The Future of Power* (前注21参照), p. 143.

(69) Strategy for Homeland Defense and Civil Support (June 2005) [http://www.defense.gov/news/jun2005/d20050630homeland.pdf], p. 12 (2014年9月3日閲覧).

(70) Glossary of Statistical Terms: global commons [http://stats.oecd.org/glossary/detail.asp?ID=1120] (2014年1月21日閲覧).

(71) Shalini Venturelli, "Information Liberalization in the European Union: Conflicting Models of State and Society," in Brian Kahin and Ernst J. Wilson, eds., *National Information Infrastructure Initiatives: Vision and Policy Design* (Cambridge: MIT Press, 1997), pp. 457–489; Nye, *The Future of Power* (前注21参照), p. 149.

(72) Remarks by the President on Securing Our Nation's Cyber Infrastructure (29 May 2009) [http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure] (2014年1月21日閲覧).

(73) Nye, *The Future of Power* (前注21参照), p. 149.

コモンズを「共有」とみるか、「非所有」（オープン・コモンズ）とみるかの微妙な違いに注意を向けたい。もっと正確に言えば、「共有」は「共同所有権に基づくが、その利用に使用料は課されない」（たとえば入会地）、「共同所有権に基づくが、その利用に使用料が課される」（自動車を共同購入し利用ごとに使用料をとり、保険料や減価償却費に充当するようなケース）に分けることができる。「非所有」は「だれも所有権をもたず、ゆえに利用も無償」（公海、宇宙、アインシュタインの相対性理論など）ということになる。

有名な「コモンズの悲劇」では、複数の農民が自由に無償で放牧地（コモンズ）において牛を放牧することが認められるとき、つまり、オープン・アクセスという前提で「非所有」のコモンズが想定されるとき、悲劇が到来するとされる(74)。農民としては自分の牛を増やさないと他の農民の牛が増え、自身の利益が減ってしまいかねないため、牛を無尽蔵に増やそうとし、その結果、牧草地は荒れ果ててすべての農民が被害を受けることになるからである。これを避けるには、牧草地を私的所有の対象として売り払ってしまうか、あるいは、公的所有の対象と位置づけ、利用権を配分するといった方法が考えられる。

ガレット・ハーディンの「コモンズの悲劇」に対して、エリノア・オストロムは別の議論を提起した(75)。彼女は、湖、大海、魚場、森林、大気のようなものを「コモンプール資源（CPR: common pool resources）」と呼び、その特徴を、一度資源が供給されると利用者を排除したり制限したりするのが難しくなる点に見出している(76)。このCPRについて、「コモンズの悲劇」を回避するには、コモンズの境界を明確化したうえで利用者間の利用ルールを、地域条件を考慮して決定し、ルール違反者への懲罰や紛争解決メカニズムを構築し、利用状況の監視を行うといったコモンズの資源利用者の共同体（コミュニティ）による解決を主張している(77)。彼女はいわば、第三者による「上」からの中央司令者による組織化ではなく、共同体の自己組織化を通じた適応システムを信頼することで問題解決をはかろうとしていることになる(78)。だが、こうした議論はコモンズを構成する要素に私的なものや公的なものが含まれているかどうかの考慮がなされておらず、インターネットのようなサイバー空間の議論には必ずしも十分ではない。

つぎに、ネグリとハートの主張を検討したい。コモンズのある「共」のレベルと、「私」や「公」のレベルが異なっていると主張しているからである。これは、サイバー空間を代表するインターネットというコモンズをどうとらえるべきか、という議論に関係している。彼らは、「＜共＞（共通の知識や文化など）と＜公＞（すなわち＜共＞へのアクセスを規制しよ

(74) Garrett Hardin, “The Tragedy of the Commons,” *Science* 162, no. 3859 (1968), pp. 1243–1248.

(75) Elinor Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action* (Cambridge: Cambridge University Press, 1990); Elinor Ostrom, “Coping with Tragedies of the Commons,” *Annual Review of Political Science* 2 (1999), pp. 493–535.

(76) Ostrom, “Coping with Tragedies of the Commons,” p. 497.

(77) Ostrom, *Governing the Commons*, p. 90.

(78) Ostrom, “Coping with Tragedies of the Commons,” pp. 520–521.

うともくろむ制度編成)を、常に概念的に区別しておくことが重要である」と指摘したうえで、「私」、「公」、「共」という三者の関係は三角形という、同じレベルにあって、「共」が他の二者に挟まれる形でとらえるのではなく、「＜共＞は＜私＞と＜公＞とは別の平面に存在し、その二つからは根本的に自律している」とみている(79)。実は、これは、インターネットにおいて、①物理層(通信を運ぶ電線、無線、コンピューターなど)、②コード層(ハードウェアを動かすコード)、③コンテンツ層(デジタル画像、テキストといった内容)という三層構造があることを前提にした見方に対応している(80)。インターネットの物理層は電線などの通信手段に対する政府の規制などによってコントロールされている。コンテンツ層もネット上で市販されているものもあるから、財産権が認められており、私的にコントロールされている。だが、コード層はフリーであり、開かれた共有地、「オープン・コモンズ」とみなすことができる。

ネグリとハートは、技術革新によってインターネットが「共」の領域を大幅に広げた点に注目し、強力な「共」が存在するようになった結果、今度は工業がこうした「共」、すなわち、インターネットに代表されるネットワークや、知的・文化的回路、イメージなどを組み合わせて、生産に活用する必要性に迫られていると主張している。

ただし、コモンズを「共有」とみるか、「非所有」(オープン・コモンズ)とみなすかの違いがもう一つ別の「コモンズの悲劇」をもたらすことに十分な注意が払われているとは言えない。コモンズを共有とみなすと、その共有する範囲が必ず問題になり、その共有権を主張する「怪物」が猛威をふるうのに対して、非所有であるかぎり、その範囲を決めることさえできないから、その心配は少ないという点に気づくことが重要なのである。

ここで興味深い例を示そう。commonの語源はラテン語のcommunis(共通の)だが、ごく初期の社会的区分をさす形容詞・名詞としてこの言葉が用いられる場合、貴族と対比して使われ、commonsは「平民」を意味していた。あるいは、共同体(community)やその構成員とみなされたから、英国の下院がHouse of Commonsと呼ばれるようになったのには、深い含意が込められている。地域共同体(Commons)を母体とする議会こそ国家の繁栄の基本組織と位置づけられたことになる。

ところが、マッキンダーは、国家が永続きするためには、その組織は「いわゆる国民全体の“利害(インタレスツ)”を考えの基本にしてはならない」という(81)。現代を生きる多くの人々は彼らが属する国家の利害・利益を意味する国益を国民全体のものとして安易に前提にしてしまっている。その結果、人々はもともとの地域共同体およびその構成員を軽視するように

(79) アントニオ・ネグリ、マイケル・ハート著、水嶋一憲監訳、幾島幸子、古賀祥子訳『コモンウェルス 下』NHK出版、2012年、130頁。
(80) ローレンス・レッシグ著、山形浩生訳『コモンズ：ネット上の所有権強化は技術革新を殺す』翔泳社、2002年、45–46頁。
(81) マッキンダー『マッキンダーの地政学』(前注39参照)、218頁。

なる。この変化はcommonという言葉が国家に結びつくことによって起きたことに注意しなければならい。commonはcommune weale（公共の福祉）、のちのcommonwealth（「生活共同体」と「政治的共同体」の一体性が崩れ、社会と国家に分化し、後者の意味に近づく）に転じた。それは、国家が平民のものになったことを示唆しているのだが、そこに、「公」と「私」の二極化が持ち込まれ、「共」という概念が急速に失われる契機があった。コモンズを「共有」とみなす意識に傾くと、どこまでが共有の対象範囲であるかが問われることになり、しかもその共有部分を国家という「公」のものとみなすようになる。それは、地域共同体から選ばれた平民が議会を構成し国家全体を考えるようになると、「国民全体の利害」という虚構（「公」）を重視することで、結局、地域住民を苦しめ、それが国全体（「共」）を疲弊させることにつながるという機制と同じである。

「共」とは、空気、水、大地の恵みといったあらゆる自然の賜物だけでなく、知識や言語、コード、情報、情動といった社会的生産の諸結果を意味している(82)。公私の区分の明確化は私的所有権の保護を前提とし、法も政治も所有権の不可侵性のもとに成り立つように構成されるようになる。そのとき、その所有権の網を「共」に向け、「共有」という概念を主張することで国家が介入しやすくなる。この国家の介入を避けるためには、「共」は「非所有」とする見方が必要になる。

どうして「共」を「共有」としてとらえると国家が介入しやすくなるのかと言えば、それは国家という観念にある二つの系譜、すなわちstatus（stato）の系譜につらなる国家＝機関説ともいうべき観念と、公共の事柄（res publica）という内容をもつキヴィタス（civitas）の系譜が合わさったものとして近代ヨーロッパの国家概念が生まれたことにかかわっている(83)。後者の系譜が公共を理由に共有部分に対する所有権を「公」として主張することを可能にしているからである。もっとわかりやすく言えば、ホッブズの国家観に示されているように、国家は「可死の神」という「神」であるのだからすべてをつくり出したのであって、それゆえに人間の所有権のおよばない「共」についても口を挟めることになるのだ。

こうした国家観に裏づけられて、国家主権は「共」の部分に介入しつづけてきたと言える。そうであるならば、こうした国家観自体を根本的に問わなければ、サイバー空間における平和の構築もできないのではないか。こうした視角で論じることは本稿では紙幅の関係でできないが、筆者は拙著『サイバー空間の平和学』でこの問題を検討する予定である。ここでは、現実がどう進もうとしているかについて、現実主義的アプローチとして検討するにとどめたい(84)。

(82) アントニオ・ネグリ、マイケル・ハート著、水嶋一憲監訳、幾島幸子、古賀祥子訳『コモンウェルス 上』NHK出版、2012年、14–15頁。

(83) 廣松渉『唯物史観と国家論』講談社、1989年、173頁。

(84) ただ、「理想主義的アプローチ」として筆者が想定しているイメージを簡単に説明しておくほうが親切かもしれない。グローバリゼーションの過程で、①国家主権を支える国家の徴税権が揺らいでおり、②国家の通貨発行権に対する挑戦が継続しており、③重国籍の導入が世界的に進んでいる。たとえば、①について

3．現実主義的アプローチ

サイバー空間をめぐっては、その影響力の拡大による重要性の高まりから、国家による干渉が現実主義的な立場から行われている。それは、欧州評議会閣僚委員会によって2001年に採択され、その後、2004年7月に発効したサイバー犯罪条約(Convention on Cybercrime)に具体的に現れている(表を参照) (85)。ここで問われたのは、サイバー空間をめぐる「犯罪」に対する国家の管轄権を法的にどう根拠づけるかであり、管轄権のおよぶ領域の外にそれをどう適用するかがとくに問題となった。サイバー空間での違法な行為が複数の国家領域にかかわることになりやすい状況下で、民事・刑事にかかわる犯罪をどう国際的に規制していくべきかが懸案となったわけである。同条約では、一定の犯罪行為の共通定義を定め、各国の国内法の統一化を可能にすることに主眼が置かれている。サイバー空間上での犯罪捜査のための各国刑事手続法の接近も試みられている。

ただし、米国は同条約が米国憲法に抵触するかもしれないことや、米国内のプロバイダーに代表されるインターネットサービス提供者の反対などから、同条約の批准が遅れた。他方で、たとえば、ロシアはサイバー犯罪条約に署名していない。国内の犯罪捜査権への介入を恐れているためである。

海上において海賊対策が問題になったのと同じように、まずサイバー空間上の犯罪への対処が急がれた。サイバー空間が当初、インターネットを利用したコミュニケーションや経済活動のための空間と想定されていたために、経済的な権利などを保護する法令が強く求められたのである。その後、サイバー空間における「攻撃」への対処などをめぐって、各

は、タックスヘイブンへの規制強化が国際協調のもとに進められる一方で、欧州での金融取引税の導入や、グローバルな累進資本税(a progressive global tax on capital)の提案がなされている。Thomas Piketty (Translated by Arthur Goldhammer), *Capital in the Twenty-First Century* (Cambridge: Harvard University Press, 2014). ②については、ビットコインやそれに対抗するライトコイン(Litecoin)やリップル(Ripple)という「通貨」が登場している。③については、ワシントンの移民政策研究所の調査によると、2008年の段階で、世界のほぼ半数の国が何らかの形態で二重国籍を大目にみていたことが分かっている。"Dural Citizenship: Dutchmen grounded," *The Economist*, no. 8766 (2012), p. 48. 以上のことなどから、国家主権の弱体化が進んでいる。同時に、国家主権の形成に深くかかわってきた人間の主体性の崩壊にかかわる現象も広がっている(この点については、前注3で紹介した東浩紀の著作が参考になる)。こうした事態が意味しているのは、国家主権に代わる新しい統治機構の可能性を吟味することの「有意味性」である。たとえば、二重国籍あるいは多重国籍を当たり前にすれば、国家が国家主権を振りかざそうとしても、人間の側が少なくとも国家主権から逃れることができる。二重国籍は、「公」の領域を二重化することで、「公」の権力作用を弱め、「共」の領域の拡大へと結びつけるねらいがある。まさに、共同体としての国家を超えた空間としての「共」を想定することができるのである。その重国籍の一つとして「無領土国家」にも国籍がもてるようになれば、国家主権による世界支配という、「リヴァイアサン」を前提とした、これまでの世界体制に風穴を開けることができるのではないか。この無領土国家にサイバー空間上の「諸紛争」を委ねることができれば、「共」による問題解決につなげることができるのではないか。それが筆者の考えている理想主義的アプローチである。

(85) サイバー犯罪条約については、以下の文献を参照のこと。Miriam F. Miquelon-Weismann, "The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?," *The John Marshall Journal of Information Technology & Privacy Law* 23, no. 2 (2005), pp. 329–361; 王志安「条約によるサイバー空間の規制:新しい国際協力レジームの現実性と課題」『駒澤法学』3巻1号、2003年、131–167頁。

表　米国、英国、日本、NATO、EUなどの主たるサイバー安全保障政策

2001年11月	欧州評議会閣僚委員会、サイバー犯罪条約を採択。
2003年02月	ホワイトハウス、「サイバー空間の安全保障のための国家戦略」（米国の重大インフラへのサイバー攻撃を防止し、サイバー攻撃に対する脆弱性を減らし、損害を最小化する）を策定・公表。
2004年01月	欧州評議会サイバー犯罪条約発効。同年、欧州ネットワーク・情報安全保障庁をEU内に設置。
2006年07月	ASEAN地域フォーラムで、各国の条件に従ってサイバー犯罪・安全保障法を整備する必要性で合意。
2006年03月	サイバー条約追加議定書発効。
2006年08月	米国上院、サイバー犯罪条約を批准。
2007年01月	米国でサイバー犯罪条約発効。
2008年01月	NATO、「サイバー防衛政策」を承認し、迅速で効率的なサイバー防衛を開始・調整する責任を負う、サイバー防衛マネジメント機関（CDMA: Cyber Defence Management Authority）を設置（活動開始は同年半ば）。
2009年05月	ホワイトハウス、「サイバー空間政策レビュー」を公表。
2009年12月	米政府のサイバー政策を一括して管轄・調整するポスト（サイバー安全保障調整官）をホワイトハウスに新設。
2009年09月	国際情報安全保障の保障分野協力に関する上海協力機構加盟国政府間合意を締結。
2010年03月	「包括的国家サイバー安全保障イニシアティブ」の改定版を公表（当初、2008年に策定されていたが、2010年3月になって一部が公表）。
2010年05月	米軍サイバー司令部設置が発表され、11月から正式に活動開始。
2010年05月	日本政府の情報セキュリティ政策会議、「国民を守る情報セキュリティ戦略」を策定・公表。
2010年09月	米国土安全保障省が主導して、「国家サイバー攻撃対応計画」策定。
2011年02月	「ドイツのためのサイバー安全保障戦略」を閣議決定。
2011年05月	ホワイトハウス、「サイバー空間の国際戦略」を策定・公表（2010年の国家安全保障戦略を受けてまとめた）。
2011年07月	米国防総省、「サイバー空間作戦戦略」を策定・公表。
2011年09月	ロシア・中国・ウズベキスタン・タジキスタン、国連総会に「情報安全保障のための国際行動規範」を共同提案。
2011年11月	英国内閣府主導で、「サイバー安全保障戦略：デジタル世界における英国の防衛と振興」を策定・公表。
2013年02月	EU委員会主導で「EUサイバーセキュリティ戦略」を策定・公表。
2013年03月	三年ほどかけて策定された「サイバー戦に適用可能な国際法に関するタリン・マニュアル」が公表。
2013年06月	日本政府の情報セキュリティ政策会議、「サイバーセキュリティ戦略」を決定。

出典：Alexander Klimburg, ed., *National Cyber Security: Framework Manual* (Tallin: NATO Cooperative Cyber Defence Centre of Excellence, 2012), pp. 23–25, 53–55を中心に筆者作成。

国別ないし国家間でさまざまな安全保障政策が模索されている。

サイバー空間をめぐる法規制をめぐっては、憲法、著作権やプライバシー保護などの専門家など（ハーバード・ロー・スクールのローレンス・レッシグやジャック・ゴールドスミスなど）が発言することが多かったが、他方で、武力行使に関する国際法の専門家など

(マイケル・シュミット米海軍戦争大学国際法部門長など)による「サイバー攻撃」などを問題視して「犯罪」ではない、戦時国際法の策定をめざす方向性が明確になりつつある[86]。それがいわゆる「タリン・マニュアル」である。人道法国際研究所が「海上での武装紛争に適用可能な国際法に関するサンレモ・マニュアル」、ハーバード人道政策・紛争研究所プログラムによる「空中戦およびミサイル戦に適用可能な国際法マニュアル」の策定が戦時国際法の条約化に向けて一定の役割を果たしてきたことに対応して、北大西洋条約機構(NATO)の共同サイバー防衛センターが主導して専門家グループからなる会合を2009年9月から始め、2010年から2012年にかけて各三日間の八回にわたる会合を行い、2012年7月の最終会合で「サイバー戦に適用可能な国際法に関するタリン・マニュアル」にまとめたのである[87]。ここではタリン・マニュアルのうち、本稿のこれまでの論述に深くかかわる一部のみを紹介しながら、サイバー空間規制の向かおうとしている現実を考察したい。

タリン・マニュアルは最初に「ルール1　主権」において、「国家はその領土主権の範囲内でサイバーインフラと活動に対するコントロールを執行できる」と規定している[88]。やはり、インフラを含む包含モデルを採用することでインフラにかかわる国家の管轄権を認めようとしているのだ。その注釈によれば、国家はサイバー空間自体に対する主権を主張するものではないが、国家の領土に位置する、いかなるサイバーインフラに対する主権上の特権を行使できるし、そのサイバーインフラに伴う活動についても同様であるというのが本規定の趣旨とされている。陸上の領土、内海、領海(海底および心土を含む)、群島水域、ないし領空におかれたサイバーインフラは領土国家の主権の対象となる。領土内のサイバーインフラに対する国家主権は、サイバーインフラが政府に属すのか、あるいは民間実体ないし個人に属するのかどうかにかかわらず、サイバーインフラを防衛する。

領海下の海底に対する沿岸国家の主権は国家がその上の海底ケーブルの設置に完全なコントロールを行うことを可能とする[89]。これは海底のケーブルが最近、インターネット・コミュニケーションの大部分を運んでいるという事実からみて重要な権利ということになる。領海を超えた海底ケーブルについては、国連海洋法条約第79条2項で沿岸国は大陸棚における海底パイプラインの敷設または維持を妨げることができないとされているが、同パイプラインからの汚染の防止・軽減・規制のために適当な措置をとる権利を有する。

「ルール2　管轄権」では、国家管轄権の執行対象として、①領土でサイバー活動に従事する人に対して、②領土に配置されたサイバーインフラに対して、③国際法に従って、域外適用されるものに対してという三つが挙げられている。ここでの問題はすでに説明した

(86) Mary Ellen O'Connell, "Cyber Security without Cyber War," *Journal of Conflict & Law* 17, no. 2 (2012), p. 204.
(87) Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013).
(88) *Ibid*., p. 15.
(89) *Ibid*., p. 17.

国家主権による立法的管轄権ないし執行的管轄権という管轄権の行使の問題として論じることができる。そこで、スティーブン・クラズナーの議論に倣って国家主権を区分し、その変化に注目する見方を紹介し、国家管轄権の行使問題に関連づけて論じてみたい。

クラズナーは、主権を国内主権(domestic sovereignty)、ヴェストファリア主権(Westphalian sovereignty)、国際法主権(international legal sovereignty)の三つに大別する(90)。さらに、相互依存主権(interdependence sovereignty)を付加する見方もある(91)。たとえば、台湾はヴェストファリア主権をもつが、国際法主権を有していない。1990年代のソマリアは国際法主権をもっていたが、国内主権が確立していない混沌とした状態にあった。問題は在来型主権が必ずしも成功しておらず、さまざまな支援を必要としている点にある。統治支援(governance assistance)、移行行政府(transitional administration)、事実上の信託統治(de facto trusteeship)に加えて、共同主権(shared sovereignty)といった支援方法まで存在する。ヴェストファリア主権は国家が特定の物質的領土を伴って存在確認できることに基礎を置いており、領土のなかでは国内の政治的権威が制度的組織や政策の唯一の合法的源泉であると考えられる。ゆえに、別の国に配置された資産に対するコンピューター・ネットワーク・オペレーションはアプリオリにヴェストファリア主権に違反しているとみなすことが可能になる(92)。「サイバースパイ」もまた、そのターゲットが別の国にあれば、ヴェストファリア主権に違反している。

ここで、1648年のヴェストファリア条約が国家間の勢力均衡という外的な安全保障と、国内秩序の維持という内的な安全保障のもとに成り立っており、それが国家主権の成立を支えていたことを想起する必要がある(93)。つまり、国内主権とヴェストファリア主権はセットになっているとみなさなければならない。そう考えると、サイバー空間は国内の権威とコントロールに大きな影響をおよぼすから、国内主権もサイバー空間の統治に向けた対応を模索する必要性に迫られる(94)。以上の考察から、タリン・マニュアルにおける管轄権

(90) クラズナーの主張が通説となっているわけではないが、前注62に示したパトリック・フランゼスのように、クラズナー説をとる者は増えており、有力な学説であることは間違いない。Stephen D. Krasner, "Pervasive Not Perverse: Semi-Sovereigns as the Global Norm," *Cornell International Law Journal* 30, no. 3 (1997), pp. 561–680.

(91) Stephen D. Krasner, *Power, the State, and Sovereignty: Essays on international relations* (London: Routledge, 2009).

(92) Betz and Stevens, *Cyberspace and the State*(前注8参照).

(93) 市野川容孝「安全性の論理と人権」『人権の再問』法律文化社、2011年、214頁。

(94) たとえば、英国では2009年に内閣府にサイバー安全保障部(Office of Cyber Security)がつくられ、2010年にサイバー安全保障・情報保証部(OSCIA: Office of Cyber Security and Information Assurance)に改組された。OCSIAの役割は、サイバー空間活動の規制に対する権威を広げるために公的・私的部門の幅広い範囲と相互作用し、英国の国家主権の行使を行うことである。サイバー空間を実際にコントロールするのは、警察、安全保障サービス、軍のような国家の通常の機関や、テレコミュニケーション・オペレーターを監視する情報通信庁(Ofcom)のような機関だが、政府通信本部(GCHP: Government Communications Headquarters)の中に2009年に新設されたサイバーセキュリティ運用センター(CSOC: Cyber Security Operations Centre)もある。CSOCは攻撃と防御の能力を有し、重要な情報インフラ、とくに政府システムや民間ビジネス・パートナーのシステムへの外国からの脅威を緩和する役割を負っている。このように、英国は国内主権の整備を通じて、サイバー空間への規制を強めている。

はヴェストファリア主権の侵害に対処する権利という面をもっていることがわかるが、それは国内主権との強い連携のもとで初めて執行可能となることを忘れてはならない。

つぎに、「ルール10　武力による威嚇ないし武力行使の禁止」について取り上げたい。武力による威嚇ないし武力行使を構成する、あるいは国連の目的と矛盾するサイバーオペレーションを不法とみなし、自衛権の行使問題へと展開させることになる。国連憲章第2条第4項は、すべての加盟国が武力よる威嚇または武力の行使を慎まなければならないと規定している。これは、あくまで加盟国を律するものであり、個人、犯罪組織、テロ組織といった非国家主体の行為に適用されるわけではない。

国連憲章第2章第4項の武力の行使ないし武力による威嚇に対する禁止が適用されない二つの例外がある。集団的安全保障作戦の一部となる行動および自衛でなされる行動である。第一の例外は国連憲章の第39条にあたる(95)。第39条は安全保障理事会に平和に対する脅威、平和の破壊または侵略行為の存在を決定し、並びに、国際の平和及び安全を維持しまたは回復するために、勧告をし、または第41条および第42条に従っていかなる措置をとるかを決定する権限を与えている。国連憲章第2章第4項の第二の例外は第51条に記されており、それは武力攻撃が起きた場合の個別自衛権ないし集団的自衛権を妨げるものは既存の国連憲章に存在しないと規定している(96)。ゆえに、武力行使ないし武力による威嚇と武力攻撃との違いが問題になる。武力攻撃は武力の行使であるが、武力攻撃に欠けている何らかの行動が武力行使を構成することになる。もちろん、人間を殺傷したりモノを破壊したり傷つけたりする行為は武力行使にあたるが、それ以外のサイバーオペレーションであっても武力行使にあたる可能性があるとして、タリン・マニュアルは「規模と効果」の観点から武力を評価するための影響力の要因として、①結果の深刻さ、②緊急性、③直接性、④侵入性、⑤結果の計測可能性、⑥軍事的性格の有無、⑦国家の関与度合い、⑧推定に基づいた合法性を挙げている(97)。

つぎに、武力攻撃に対する自衛権が問題になる。国連憲章第51条で、加盟国に対して武力攻撃が発生した場合には、安全保障理事会が国際的な平和および安全の維持に必要な措置をとるまでの間、個別的または集団的自衛の固有の権利を害するものではないとされているためである。武力行使を超えて武力攻撃と認定するには、規模と効果の規準に基づく線引きが必要になる。タリン・マニュアルを定めた専門家グループは人間を殺傷したり、財産を損傷・破壊したりする武力行使はいかなるものであっても規模と効果の条件を満た

(95) Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue and Julia Spiegel, "The Law of Cyber-Attack," *California Law Review* 100 (2012), p. 843.

(96) *Ibid*., p. 844.

(97) Schmitt, ed., *Tallinn Manual* (前注87参照), pp. 48–51. タリン・マニュアルに深くコミットしているシュミットは、当初⑥と⑦を除いた六つの要因を想定していた。Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *The Columbia Journal of Transnational Law* 37 (1999), p. 914.

すことに同意し、武力攻撃とした(98)。また、情報収集やサイバー空間上での盗みは、あまり重要でないサイバー活動の短期間の遮断といったオペレーションと同じく、武力攻撃の条件に欠けるという見方で一致した。だが、ニューヨーク証券取引所に対するサイバー空間を利用した何らかの事件で相場が暴落しても、それを武力攻撃とみなせるかについては専門家の意見は一致していない(99)。国家Aによる国家Bに対するサイバー諜報活動が予期せぬ損害をBのサイバー関連インフラにおよぼした場合を仮定すると、武力攻撃としてサイバーオペレーションを条件づけるのにその意志の有無は無関係であり、規模と効果が重要だから同事件は武力攻撃であるとみなす専門家が多い半面、武力攻撃とするのに躊躇する専門家もいる(100)。2007年のエストニアへのサイバーオペレーションについては、専門家は武力攻撃と位置づけるほどの規模と効果に達していないとみなしている(101)。半面、スタックスネットについては、若干の専門家は武力攻撃にあたるという見解をとっている(102)。

いずれにしても、タリン・マニュアルは「武力攻撃であるかを区別するために効果を重視するアプローチ(effects-based approach)」をとっていることになる。これは「どんな道具で攻撃するかを重視するアプローチ(instrument-based approach)」と「攻撃目標が何かを重視するアプローチ(target-based approach)」の中間に位置するアプローチということになる(102)。興味深いのは、国連憲章第41条が武力行使を伴わない措置として経済関係および鉄道、航海、航空、郵便、電信、無線通信その他の運輸通信の手段の全部または一部の中断ならびに外交関係の断絶を含むものを挙げている点だ。サイバー空間にかかわる道具は武力行使

(98) Schmitt, ed., *Tallinn Manual* (前注87参照), p. 55.

(99) *Ibid*., p. 56.

(100) *Ibid*., p. 57. この攻撃における意志の有無の問題の重要性に光を当てるために歴史を紐解いてみたい。1940年8月24日夜のドイツによる空爆がテムズ川沿いの製油所をねらったものであったのにもかかわらず、計測の間違いで、ロンドンの中心部をねらった爆撃と誤解された。これを契機にウィンストン・チャーチル英首相は制裁としてベルリン攻撃を命じた。Stewart Baker, "Denial of Service" *Foreign Policy* (2011) [http://www.foreignpolicy.com/articles/2011/09/30/denial_of_service] (2014年1月21日閲覧). それが今度はドイツ側を怒らせ、ドイツによるロンドンへの無差別攻撃をもたらした。こうした歴史を考慮すると、意志の有無は決して無視できないように思われる。

(101) 2007年4月末から、エストニアはDDoSによる攻撃の対象となり、それは銀行システム、多くの政府サービス、および多くのメディアに停止をもたらした。といっても、エストニア最大の銀行のオンライン・サービスができなくなったのは、5月9日の90分と10日の二時間にすぎない。重大なインフラは危うくならなかったが、駐車場から銀行業や投票まで、すべてインターネットに依存するエストニアのようなハイテクに依存する国にとって攻撃は、重大な破壊を引き起こした。クレムリンで当時大統領府副長官を務めていたヴラジスラフ・スルコフが支援していた「ナーシ」という若者の集団のメンバーは、攻撃の背後に自分たちがいたことを認めたが、ロシア政府の命令があったことは否定している。Healey, ed., *A Fierce Domain: Conflict in Cyberspace* (前注24参照), pp. 344–399など。

(102) Schmitt, ed., *Tallinn Manual*, p. 58. 他方で、スタックスネットのワームは疑いなく武力使用に当たるだろうと思われるが、その攻撃の規模や効果は武力攻撃に匹敵するだけの十分な深刻さをもっていないように思われる。Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge: Cambridge University Press, 2012), p. 82.

(103) Hathaway *et al*., "The Law of Cyber-Attack," pp. 845–847.

をそもそも伴わない道具に近く、軍事的強制を伴った物的特徴が不足しており、伝統的軍事兵器を使用しているとはみなされていないことになる。ただ、大部分の学者は第41条そのものが危険なほど時代遅れとみなしており、instrument-based approachは劣勢にある。

target-based approachは重要な国家システムの積極的な防衛を許容するという「ベネフィット」があるが、それは広範囲の自衛を誘発し、サイバー上の対立が破壊的な在来型軍事対立にエスカレートする可能性を増大させることになりかねない(104)。このアプローチは戦争をより起こりやすくすることで、国際コミュニティの安全保障を傷つけるものであり、インフラ重視の国家管轄権を標榜する立場が広がりをみせていると懸念される。他方、effects-based approachは、サイバー攻撃を、その効果の程度に基づいて武力攻撃と分類しようとするものだ。道具重視と目標重視のアプローチの間の中間の立場をとることで、もっとも幅広く受け入れられているアプローチである。ただ、このアプローチの問題点は自衛を正当化するための効果のタイプを事前に想定し、武力攻撃に対する自衛権の発動を合法化しようとするねらいが最初から前提とされていることにある。

結びにかえて

ここで紹介したタリン・マニュアルが今後、サイバー空間上の「攻撃」や「戦争」をめぐる議論において重要な役割を果たすのは確実だろう。このマニュアル自体に、現実主義的な国際法学者や軍事専門家が深くコミットしており、意図的ないし無意識に「好戦的」な内容に傾いていると指摘せざるをえない。そう感じさせるのは、だれのものでもない、隠喩としてのサイバー空間に、それを構成する一部としてのインフラへの国家主権による管轄権を振りかざすという姿勢のためである。しかも、こうした議論を好む人々はサイバー空間をめぐる安全保障問題の重要性を喧伝することで、大きな利益を得られるビジネス関係者、学者、政治家、軍人などに多くみられる。

これは、ドワイト・アイゼンハワー大統領が「巨大な軍事エスタブリシュメントと大規模な武器産業の結合」として警告した軍産複合体(military-industrial complex)ならぬ、「サイバー産業複合体(cyber-industrial complex)」ないし「軍・サイバー・諜報のどろどろした固まり(military-cyber-intelligence mash-up)」の出現を想起させる(105)。アイゼンハワーは政府、軍、産業が不要な軍事力の拡大、過剰な国防支出、さらに政策作成過程におけるチェック・アンド・バランスの崩壊につながりかねないことを恐れていた(106)。同じような事態がサイバー関連産業を巻き込んで起こりつつあるのではないか。その証拠に、2009年には、

(104) *Ibid*., pp. 846–847.

(105) Jerry Brito and Tate Watkins, "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy," *Harvard National Security Journal* 3 (2011), pp. 61–62.

(106) Eisenhower's Farewell Address to the Nation (17 January 1961) [http://mcadams.posc.mu.edu/ike.htm] (2014年1月21日閲覧).

ロッキード、シマンテック、デル、ヒューレット・パッカード、インテル、マイクロソフトなどを含む国防・安全保障・ハイテク企業が研究開発のためのサイバー安全保障のための技術的提携をはじめた(107)。さらに、国家安全保障局長官や国家情報長官を歴任したジョン・マコーネルは国防・安全保障関係の請負業者として有名なブーズ・アレン・ハミルトン(Booz Allen Hamilton)社の副社長を務めている(108)。こうした現実は米国だけでなく、日本でも同じである(109)。

実は、電信、無線、電話といった技術進化にかかわるインフラに国家がどう主権を行使してきたかをみると、米国は英国と異なり無線や放送は公共財として政府の管轄下に入ったものの、電信、ケーブル、電話などのサービスは国有化されて政府の全面的管理下に置かれることはなかったことがわかる(110)。無線にしても米国のラジオビジネスは私的に運営され、限定された国家規制のもとで混合形態によるコントロールがなされただけだった。

電信を意味するtelegraphもまた隠喩として発明された言葉であることを思い出してみよう。ギリシア語で、teleは「遠く」を、grapheinは「書くこと」意味するから、「遠くから送られた、書かれたメッセージ」をする比喩こそ電信のもとであり、電気信号によるtelegraphは1825年に英国の発明家によって発想され、1830年に米国で具現化された。1837年、英国の発明家ウィリアム・クックとチャールズ・ウィートストーンが電信の特許を取得した(111)。この電信を支える重要なインフラは電線(ケーブル)であった。

米国では、サムエル・モールスが1835年、電線を信号が伝わることを証明し、その後、政府はワシントンとヴォルティモアを結ぶ電線敷設(完成は1844年5月)に資金提供するなどして、徐々に電信の重要性が認知されるようになった。1851年には、電信ビジネスが開始された。南北戦争によって電信による情報伝達の重要性が広く認識されるにつれて、電信ビジネスが全米に広がった。こうした変化のなかで、海底ケーブルを使った電信も開始

(107) Brito and Watkins, “Loving the Cyber Bomb?” p. 69.

(108) ブーズ・アレン・ハミルトンは、2008年に投資家グループであるカーライル・グループが買収した。同グループのアドバイザーやボードメンバーにジョージ・ブッシュやジョージ・W・ブッシュ、ジェームズ・ベーカーなどが含まれていたことは有名である。Ryan Singel, “White House Cyber Czar: ‘There Is No Cyberwar’” *Wired* (2010) [http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar] (2014年1月21日閲覧).

(109) やや古い資料だが、2006年度の防衛省の三菱重工業との契約額は2,776億円で、同社の自民党(国民政治協会)への政治献金は3,000万円、同省からの天下りは62人と突出している。日本電気との契約額は831億円、同献金は1,820万円、同天下りは40人、富士通との契約額は441億円、同献金は1,680万円、同天下りは16人であった。この天下りの実数は、富士通(2005年10月)を除き2006年4月現在のものである。このように情報産業も「サイバー産業複合体」の一翼を担っている。「軍需上位15社、防衛省天下り475人／受注7割、自民に多額献金」『しんぶん赤旗』2007年10月28日。

(110) 近く上梓する拙著『サイバー空間の平和学』のなかで論じる予定。

(111) D. De Cogan, “British Empire Cable Communications (1851-1930): The Azores Connection,” *Arquipélago*, núm. especial (1988), p. 167.

(112) *Ibid*., p. 173.

される。そのパイオニアとなったのは英国のジョン・ペンダーである(112)。彼は大西洋のケーブル敷設に資金援助し、その成功によっていくつもの電信会社を創設し、それらがやがて電信建設保守会社(Telcon: Telegraph Construction & Maintenance Company)に統合されることになる(113)。彼は同社の最初の会長に選任された。同社こそ、20世紀初期に海外でのケーブル敷設を支配するのだ。他方で、英国政府は1872年に内陸部の電信会社を国有化したが、ペンダーは同年に四社を統合する形で新会社、東方電信会社(Eastern Telegraph Company)を設立した。その後、1883年になると、スウェーデンの会社との間で極東への新しい海底ケーブル敷設などで協力する協定を締結、それが東方電信会社の急成長につながった。1884年には海底ケーブル保護条約が締結された。英米ともに同条約に署名・批准したが、米国は1994年に発効した国連海洋法条約に署名しておらず、同条約で定められている海底電線および海底パイプラインを敷設する権利(第112条)などの権利を国際慣習法で守る姿勢をとっている。これは米国の単独行動主義(ユニラテラリズム)の残滓とも言える。

過去の電信、無線、電話などの新技術によってもたらされた環境の大きな変化のなかで、各国とも主として安全保障にかかわる軍事的理由や自国企業の発展を名目として、民間のビジネスに干渉してきたという事実がある。だが、米国政府だけは民間ビジネスとの「距離」を必要に応じてとってきた。その米国政府の方針が変化したところに、今回のタリン・マニュアルの作成が可能となったと考えられるのではないか。この米国政府の方針転換は、「グローバル・コモンズ」にサイバー空間を含めることをやめ、同空間を支えるインフラに対する国家管轄権の行使を容易にするというものであった。転換自体は2009年のオバマ大統領就任以降になされたものであり、タリン・マニュアルの協議も同年9月から開始された。2010年1月21日、ヒラリー・クリントン国務長官は、「インターネットの自由」という有名な演説で、「我々はグローバルなサイバー安全保障を強化する外交的解決法を見出すために政府として、そして国務省としてステップを踏んできた」と指摘し、国家によるサイバー空間への干渉の姿勢を明確に示している。オバマ政権の政治的決断がタリン・マニュアルの背後にあるとすれば、そこでの結論は覇権を何とか保っている米国政府に都合のいい結果をもたらしているにすぎない。だからこそ、逆に、本稿でいう「非所有」としての「共」にサイバー空間を位置づける努力(理想主義的アプローチ)に別の可能性を見出す努力が必要なのではないか。これが筆者の期待である。

(付記)本稿は平成23～25年度科学研究費補助金基盤研究(C)「ロシアと中国の安全保障をめぐる比較体制分析」の研究成果の一部である

(113) Ken Beauchamp, *History of Telegraphy* (London: The Institution of Engineering and Technology, 2001), p. 169.