「タリン・マニュアル 2」の有効性考察の試み
──サイバー空間における国家主権の観点から──

河野　桂子

〈要旨〉

国境をまたがるサイバー攻撃の事案は多発しており、それへの技術的、かつ法的対応は急務である。特に甚大な被害を受けた国は、加害国に対して国際法違反の認定を行うにあたり、その認定基準を精緻にしておかなければならない。そのため各国は、サイバー活動の個々の場面で国際法がいかに適用されるかについて分析及び検討を続けることが重要である。各国がこのような取り組みを行う過程において、「タリン・マニュアル」及び「タリン・マニュアル 2」は有用な参照資料として活用されることが期待される。本稿では「タリン・マニュアル 2」の主要な論点を取り上げ、近年のサイバー攻撃の事案に照らして「タリン・マニュアル 2」に基づく判断と関係国の見解の相違を比較し、「タリン・マニュアル 2」の有効性に関する暫定的な評価を行うこととする。近年の事例としては、ともに 2017 年に起きた「ノットペチャ」及び「ワナクライ」と称されるサイバー攻撃に加えて、非国家主体のサイバー攻撃拠点への対応、中国のサイバー主権の主張、そして主に 2016 年に起きた米国大統領選への選挙干渉を取り上げる。

はじめに

（1）目的

2017 年 2 月、『サイバー活動に適用される国際法タリン・マニュアル 2』[1]（以下、「タリン・マニュアル 2」）は、2013 年の『サイバー戦に適用される国際法タリン・マニュアル』[2]（以下、「タリン・マニュアル」）の続編として刊行された。本文書は、「タリン・マニュアル」と同じくNATO サイバー防衛協力センター（CCD COE）の旗艦事業として行われたものでは

1　Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (Cambridge University Press, 2018).

2　Idem., Tallinn Manual on the International Law Applicable to Cyber Warfare (Cambridge University Press, 2013).

あるが、個人資格で参加した国際法学者らによって作成された学術的な研究成果である[3]。

「タリン・マニュアル」及び「タリン・マニュアル 2」が取り上げたサイバー活動に適用される国際法の問題は、2004 年来、国連の「国際安全保障の文脈における情報及び電気通信分野の進歩に関す政府専門家会合」（以下、国連サイバー GGE）[4] において議論されてきたが、2017 年の会期は報告書の作成に結実しなかった。国連サイバー GGE において 1 つの極を形成していたロシアは、2019 年の国連サイバー GGE の再開を画策していると伝えられているが[5]、ロシアがこれまでの主張[6] を繰り返すことは容易に想像がつくことから、それへの対応を迫られる欧米西側諸国としては、今後より一層この問題に関する考え方を整理しておくことが肝要である。勿論、国連サイバー GGE という当座の対応のみでは十分とは言えない。国境をまたがるサイバー攻撃の事案は多発しており、それへの技術的、かつ法的対応もまた急務である。特に甚大な被害を受けた国は、加害国に対して国際法違反の認定を行うにあたり、その認定基準を精緻にしておかなければならない。そのため、国連における多国間の議論が今後、実際に再開されるか否かにかかわらず、単独、又は同盟・友好国と共に、サイバー活動の個々の場面で国際法がいかに適用されるかについて分析及び検討を続けることが重要である。

各国がこのような取り組みを行う過程において、「タリン・マニュアル」及び「タリン・マニュアル 2」は有用な参照資料として活用されることが期待される。実際に、欧州議会が採択したサイバー防衛に関する決議（2018 年 6 月 13 日）の 47 項は、構成国に対して「タリン・マニュアル 2」に書かれた内容の分析と適用を開始し、さらに国際的行動に関する自発的規範に合意することを要請している[7]。但し「タリン・マニュアル」及び「タリン・マニュアル 2」が今後、各国の公式見解に採用されるか否かは、何よりその内容次第である。「タリン・マニュアル 2」刊行後、まだ 1 年半ほどしか経過していない現時点では、その検証を行うのに

3　なお「タリン・マニュアル 2」プロジェクトには、前編と異なりアジア諸国の専門家が複数参加したことが特筆される。例えば、中谷和弘東京大学教授（日本）、黄志雄（Zhixiong Huang）武漢大学法学院教授（中国）、クリアンサック・キティチャイセリー（Kriangsak Kittichaisaree）国際海洋法裁判所（ITLOS）裁判官（「タリン・マニュアル 2」プロジェクト参加当時は、国連国際法委員会（ILC）委員）（タイ）などである。

4　United Nations Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE).

5　“Russia Proposes Alternatives to International Cyber Norms,” IISS Cyber Report, 6th July 2018, https://www.iiss.org/blogs/cyber-report/2018/07/cyber-report-29-june-to-5-july

6　Andrey Krutskikh & Anatoly Streltsov, “International Law and the Problem of International Information Security,” *International Affairs: A Russian Journal of World Politics, Diplomacy and International Relations*, Vol. 60 (2014), p. 68, https://ccdcoe.org/sites/default/files/multimedia/pdf/International_Affairs_No6_2014_International_Law.pdf

7　European Parliament Resolution of 13 June 2018 on Cyber Defence (2018/2004(INI)), para. 47, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0258+0+DOC+PDF+V0//EN

十分な国家実行は未だ存在しないが、本稿では「タリン・マニュアル 2」の主要な論点を取り上げ、近年のサイバー関連の事案に照らして「タリン・マニュアル 2」に基づく判断と関係国の見解の相違を比較し、「タリン・マニュアル 2」の有効性に関する暫定的な評価を行うこととする。近年の事例としては、ともに 2017 年に起きた「ノットペチャ」及び「ワナクライ」と称されるサイバー攻撃に加えて、非国家主体のサイバー攻撃拠点への対応、中国のサイバー主権の主張、そして主に 2016 年に起きた米国大統領選への選挙干渉を取り上げる。

1.「ノットペチャ」及び「ワナクライ」
——適用される国際法規則は何か——

（1）両事件の経緯と概要

「ノットペチャ」及び「ワナクライ」は、感染端末内のデータを暗号化し、その復旧の条件として金銭の支払いを要求するランサムウェアを用いたサイバー攻撃である。もっとも、両攻撃とも被害者が金銭を支払ったとしてもデータは復旧しないため、損害の種類という観点から分類した場合には、データ破壊を目的とするサイバー攻撃に該当する[8]。

「ワナクライ」は 2017 年 5 月に発生した後、150 カ国の約 30 万台の端末に被害を与え、その被害額は 5 億 9,250 万ドルにも及んだ[9]。特に英国では、国民保険サービス（NHS）トラスト傘下の 34 の病院において医療機器や装置の感染が確認され、患者の情報へのアクセスや医療機器の使用が不可能となる重大な事態が生じた[10]。この攻撃の実行者は、過去にソニー・ピクチャーズ・エンターテイメント（SPE）やバングラデシュ中央銀行への攻撃に関与した「ラザルス」（Lazarus）という組織とされているが、2017 年 12 月 19 日から 20 日にかけて英、米、加、豪、ニュージーランド、そして日本の関係政府当局は、この攻撃が北朝

8　攻撃的な（offensive）サイバー能力を損害という観点から分類すると、サービス妨害（Denial of Services）、ファイル破損、物理的損害の 3 種類に分類される。Max Smeets and Herbert S. Lin, "Offensive Cyber Capabilities: To What Ends?" in Tomáš Minárik, Raik Jakschis and Lauri Lindström, eds., *10th International Conference on Cyber Conflict: CyCon X: Maximising Effects* (NATO CCD COE Publications, 2018), p. 59, Table 1.

9　Press Release: Foreign Office Minister Condemns North Korean Actor for WannaCry Attacks, The UK Government website, 19 December 2017, https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks ; "Toespraak minister Bijleveld tijdens het seminar 'Diplomacy and Defence in Cyber Space' in Den Haag," 20 June, 2018, https://www.rijksoverheid.nl/documenten/toespraken/2018/06/20/toespraak-minister-bijleveld-tijdens-het-seminar-diplomacy-and-defence-in-cyber-space%E2%80%99-in-den-haag

10　UK National Audit Office, *Investigation: WannaCry Cyber Attack and the NHS* (2018), https://www.nao.org.uk/mwg-internal/de5fs23hu73ds/progress?id=AHng2c9GLbcHlVdGpGQIXCN2NQObk9RGFS6zQPfqJCU,

鮮によるものと断定する非難の声明を発した[11]。また、欧州議会も北朝鮮はワナクライによって国際法に違反したことを明確に言及している[12]。

他方、「ノットペチャ」は、2017 年 6 月、ウクライナの金融、エネルギー及び政府部門を直接の標的とするサイバー攻撃ではあったが[13]、ウクライナに事業展開する英国やデンマークなどの民間企業なども数多く感染し、その被害額は 8 億 9,250 万ドルに及んだ[14]。2018 年 2 月 15 日から 16 日にかけて日本を除く前述の 5 カ国の当局は、この攻撃がロシアによるものと断定したほか[15]、2018 年 G7 シャルルボワ・サミットの外相会合共同コミュニケもロシアの責任に言及する G7 伊勢志摩サイバーグループ会合議長報告を「歓迎」し[16]、さらに「ワナクライ」を糾弾した前述の欧州議会の決議も、ロシアの国際違法行為に触れている。

11 Press Release: Foreign Office Minister Condemns North Korean Actor for WannaCry Attacks, The UK Government website ; Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea, The US Whitehouse website, 19 December 2017, https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/; Communications Security Establishment (CSE) Statement on the Attribution of WannaCry Malware, The CSE of Canada website, 19 December 2017, https://www.cse-cst.gc.ca/en/media/2017-12-19: Media release, Prime Minister, Minister for Foreign Affairs: Attributing the 'WannaCry' Ramsomware to North Korea, The Prime Minister of Australia website, 20 December 2017, https://www.pm.gov.au/media/attributing-wannacry-ramsomware-north-korea: News: New Zealand Concerned at North Korean Cyber Activity, The Government Communications Security Bureau (GCSB) of New Zealand website, 20 December 2017, https://www.gcsb.govt.nz/news/media-release-new-zealand-concerned-at-north-korean-cyber-activity/; 日本外務省「米国による北朝鮮のサイバー攻撃に関する発表について（外務報道官談話）」、外務省ウェブサイト、2017 年 12 月 20 日、https://www.mofa.go.jp/mofaj/press/danwa/page4_003563.html

12 European Parliament Resolution of 13 June 2018 on Cyber Defence (2018/2004(INI)), para.53.

13 Press Release: Foreign Office Minister Condemns Russia for NotPetya Attacks, The UK Government website, 15 February, 2018, https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks

14 "UK and US Blame Russia for 'Malicious' NotPetya Cyber-Attack," BBC website, 15 February, 2018, https://www.bbc.com/news/uk-politics-43062113; "Toespraak minister Bijleveld tijdens het seminar 'Diplomacy and Defence in Cyber Space' in Den Haag"; Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Wired website, 22 August, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

15 Press Release: Foreign Office Minister Condemns Russia for NotPetya Attacks, The UK Government website, 15 February, 2018 ; Statement from the Press Secretary, The US Whitehouse website, 15 February, 2018, https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/: CSE Statement on the NotPetya Malware, The CSE of Canada website, 15 February, 2018, https://www.cse-cst.gc.ca/en/media/2018-02-15; Australian Government Attribution of the 'NotPetya' Cyber Incident to Russia, Minister for Law Enforcement and Cyber Security of Australia website, 16 February 2018, https://minister.homeaffairs.gov.au/angustaylor/Pages/notpetya-russia.aspx; News: New Zealand Joins International Condemnation of NotPetya Cyber-attack, The GCSB of New Zealand website, 16 February, 2018, https://www.gcsb.govt.nz/news/new-zealand-joins-international-condemnation-of-notpetya-cyber-attack/

16 G7 Foreign Ministers' Communiqué: Chair's Report of the Meeting of the G7 Ise-Shima Cyber Group, https://g7.gc.ca/en/g7-presidency/themes/building-peaceful-secure-world/g7-ministerial-meeting/g7-foreign-ministers-joint-communique/chairs-report-meeting-g7-ise-shima-cyber-group/

（2）適用される国際法

「ワナクライ」及び「ノットペチャ」が違反した国際法の種類や内容について、各国当局は必ずしも明示していない。その理由としては、根拠が自明であり示すまでもないと各国が考えたか、あるいは根拠についての見解は各国で一様でないため結論のみを示すのが便宜的と考えたかなどの可能性が挙げられるが、実際のところは不明である。但し、後で述べるように、「タリン・マニュアル 2」関係者などによって両事案に適用可能とされた主権原則（規則）に関して、国連サイバー GGE あるいは「タリン・マニュアル 2」専門家らは、いずれも厳密な定義に合意できなかった経緯[17]に鑑みると、各国が国際法上の根拠を示さなかった理由は後者に近いものと推測される。

なお、各国は「ワナクライ」及び「ノットペチャ」がともに国家によって直接行われたか、あるいは国家による指示や承認の下で行われたサイバー攻撃であると認定しており、本稿も同じ前提に立ち議論を進める。また、両攻撃は、加害主体や被害の規模において細部は異なるものの、攻撃の類型（データ破壊）や無差別的性質などの面で共通することから、違反された国際法規則は同一のものと認識されることが多く[18]、本稿でも同じ理解の基で議論を進める。

①「タリン ・マニュアル 2」に基づく評価

「ワナクライ」及び「ノットペチャ」の双方とも、被害の一部として他国の政府機関を含んでおり、この点は「タリン ・マニュアル 2」規則 4 に基づき判断する限り主権侵害に該当する[19]。同規則は、「国家は、他国の主権を侵害するサイバー行動を行ってはならない」[20]と定めるが、そのコメンタリーによれば、本質的な政府の機能の行使に必要なシステムやデータに悪影響をもたらす遠隔サイバー攻撃が、この規則違反に該当するとされている[21]。また、政府機関ではなく、純粋に民間企業が運用する重要インフラシステムやデータに対する遠隔サ

17　Marina Kaljurand, “United Nations Group of Government Experts: The Estonian Perspective,” in Anna-Maria Osula and Henry Rõigas, eds., *International Cyber Norms: Legal, Policy & Industry Perspectives* (NATO CCD COE, 2016), pp. 115 and 121; Schmitt, *Tallinn Manual 2.0*, p.21.

18　News: NotPetya and WannaCry Call for a Joint Response from International Community, NATO CCD COE website, 30 June 2017, https://ccdcoe.org/notpetya-and-wannacry-call-joint-response-international-community.html

19　News: WannaCry Campaign: Potential State Involvement Could Have Serious Consequences, NATO CCD COE website, 16 May 2017, https://ccdcoe.org/wannacry-campaign-potential-state-involvement-could-have-serious-consequences.html; News: NotPetya and WannaCry Call for a Joint Response from International Community.

20　日本語訳は、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）7 頁を参照。

21　Schmitt, *Tallinn Manual 2.0*, pp. 21-22, paras. 15-16.

イバー攻撃であっても、一定の条件を満たせば同様に被害国の主権侵害を構成する。「タリン・マニュアル 2」コメンタリーによれば、その条件とは第 1 に物理的な損害が発生する場合、第 2 にサイバー・インフラの機能が失われる場合である[22]。機能喪失の厳密な基準について専門家らは意見の一致を見なかったものの、少なくともサイバー・インフラの物理的部品の修理又は交換は物理的損害に類似するため、被害国の主権を侵害するものとされている。その具体例として引用されているのがサウジアラビアの石油会社サウジアラムコに対するウィルス攻撃（2012 年）である[23]。

「ワナクライ」及び「ノットペチャ」について「タリン・マニュアル 2」監修者のマイケル・シュミット米海軍大学教授が行った分析によれば（その時点で入手可能な情報に照らしての判断という条件付きではあるが）、「ワナクライ」は認定基準の境界事例にあたるとしつつも、特に医療サービスに必要な機能が著しく損なわれており、また警察力などの本質的な政府の機能が阻害されている[24]、また「ノットペチャ」による被害も、民間部門のサイバー・インフラの深刻な機能低下は一時的なサービス妨害の域を超えている[25]という理由で、両攻撃とも被害国の主権侵害にあたる。他方、ほかに評価基準となりうる主要な国際法規則としては、国内問題不干渉や武力不行使の 2 つが残されているが、シュミット教授によれば「ワナクライ」は条件を満たさずいずれにも該当しないが、「ノットペチャ」は広範囲にわたる経済の混乱を引き起こしたという理由からウクライナが受けた被害は武力行使に該当する余地があると述べている[26]。

②「タリン・マニュアル」と異なる評価

「タリン・マニュアル 2」によれば、「ワナクライ」及び「ノットペチャ」は被害国の主権侵害にあたると評価されうるのに対して、両攻撃の後で声明を出した各国政府の中には別の見方を示唆する国が見受けられる。2018 年 5 月 23 日、英国のジェレミー・ライト法務総裁（政府の最高法律顧問）は、サイバー空間に適用される国際法について初めて英国政府の公式見解を表明した。その中で特に注目されるのは、国内問題不干渉規則の基準に満たない

22　Ibid., pp. 20-21, paras. 11, 13-14.

23　「イラン緊迫、動脈封鎖なら電力危機再燃（真相深層）――日本、LNG 輸送で影響大」『日経新聞』電子版、2012 年 9 月 25 日；Christopher Bronk & Eneken Tikk-Ringas, “The Cyber Attack on Saudi Aramco,” *Survival*, Vol. 55 (2013), pp. 81-96.

24　Michael Schmitt and Sean Fahey, “WannaCry and the International Law of Cyberspace,” Just Security website, 22 December 2017, https://www.justsecurity.org/50038/wannacry-international-law-cyberspace/

25　Michael Schmitt and Lieutenant Colonel Jeffrey Biller, “The NotPetya Cyber Operation as a Case Study of International Law,” Blog of the European Journal of International Law website, 11 July, 2017, https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/

26　Ibid.

サイバー行動の国際法上の規律の問題である。ライト総裁は、「他国の同意なく、その国のコンピュータ・ネットワークを妨害する行為との関連において、『領域主権の侵害』を禁ずるサイバー特有の規則が存在すると主張する国がいるが、英国はそのような規則は存在しないと考える」と述べている[27]。

この発言は、単に他国の閉鎖的コンピュータ・システムへの不正アクセスが国際違法行為に該当しないという意味にとどまらず、特定のサイバー行動を主権侵害として禁止する国際法上の規則はそもそも存在しないという趣旨を述べたものとして一部の学説で受け止められている[28]。同じ内容を説く学説も以前から存在し、また各国政府内外でも難問の 1 つとして解決が先送りされてきた論点である[29]。もっともライト総裁は、「ワナクライ」及び「ノットペチャ」が国際違法行為とみなされる具体的な根拠について言及していないが、「重要医療サービスを攻撃目標とする行為は、それがサイバー手段による場合でも同様に禁止された干渉か、又は武力攻撃にさえ該当する」と述べる箇所もあることから、英国政府の見解としては、両攻撃を国内問題への違法な干渉、及び／又は武力行使若しくはその威嚇として評価したものと推測される（後述のとおり、武力攻撃は武力行使の一形態にあたる）。

③武力行使又はその威嚇への該当可能性

「ワナクライ」及び「ノットペチャ」に対する英国外務大臣の非難声明（注 11，13）は、両攻撃の「無差別性」及び「破壊的性質」に言及してはいるが、これらが武力行使又はその威嚇に該当するとまでは述べていない。また、前述の英国法務総裁のスピーチも、サイバー行動が武力行使又はその威嚇に該当する具体的な基準について触れていない。但し、以下の引用部分では、特に英国が「ワナクライ」攻撃によって受けた被害を想起させる箇所があり、英国政府の評価を分析する際のヒントとなると思われる。

27　Cyber and International Law in the 21st Century, Speech by the Attorney General Jeremy Wright QC MP, 23 May 2018, the UK Government website, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century

28　Isa Qasim, "United Kingdom Att'y General's Speech on International Law and Cyber: Key Highlights," Just Security website, 23 May 2018, https://www.justsecurity.org/56853/united-kingdom-atty-generals-speech-international-law-cyber-key-highlights/; Colonel Gary Corn & Eric Jensen, "The Technicolor Zone of Cyberspace, Part 2," Just Security website, 8 June, 2018, https://www.justsecurity.org/57545/technicolor-zone-cyberspace-part-2/

29　Kaljurand, "United Nations Group of Government Experts: The Estonian Perspective," pp. 115 and 121; Brian J. Egan (Legal Advisor, US Dep't of State), "International Law and Stability in Cyberspace," *Berkeley Journal of International Law*, Vol. 35 (2017), p. 174, https://www.law.berkeley.edu/wp-content/uploads/2016/12/BJIL-article-International-Law-and-Stability-in-Cyberspace.pdf : Gary P. Corn & Robert Taylor, "Symposium on Sovereignty, Cyberspace and Tallinn Manual 2.0: Sovereignty in the Age of Cyber," *American Journal of International Law Unbound*, Vol. 111 (2017), pp. 207-211.

サイバー手段を用いて重要医療施設を攻撃目標とすること、民間航空機を墜落させること、原子力発電所を破壊することは、非サイバー手段による場合と同様に違法であり、強力（robust）かつ正当な対処を受けるに値する[30]。

航空機の衝突又は墜落や原子力発電所の融解の例は、米国国務省の法律顧問ハロルド・コー氏（2012 年時点）によってサイバー攻撃が武力行使になりうる想定事例として挙げられたことが想起される（その他、ダムの放流による住民居住地域の破壊の例も列挙されている）[31]。さらに遡ると 1999 年には米国国防総省が「航空機の管制システムに対するコンピュータ・ネットワーク攻撃は、大多数の死傷者や物理的損害をもたらすことによって武力攻撃に該当することがありうる」と述べているほか[32]、オランダ政府も 2011 年以来この考え方を採る[33]など、サイバー武力行使又はサイバー武力攻撃の古典的想定事例として聞きなれた類型である。

武力行使と武力攻撃は、質的な差ではなく、国際司法裁判所（ICJ）ニカラグア事件本案判決（1986 年）[34]で提示された「規模及び効果」の基準によって判断される程度の差にすぎない。「武力攻撃」は、武力行使の最も重大な形態であり、あるサイバー攻撃が、武力行使か、又は武力攻撃に該当するかの認定も、その攻撃の具体的な状況に照らして重大性が判断される。武力行使と武力攻撃の重大性に基づく区別は、「タリン・マニュアル 2」も踏襲しているが[35]、学説のみならず大多数の国家による支持を得られているものと思われる。

他方、武力行使の該当性基準については、非サイバー手段の文脈においてではあるが、

30　Cyber and International Law in the 21st Century, Speech by the Attorney General Jeremy Wright.

31　Harold Hongju Koh, "International Law in Cyberspace," *Harvard International Law Journal Online*, Vol. 54 (2012), p. 4, http://www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1.pdf

32　U.S. Department of Defense, Office of the General Counsel, ed., An Assessment of International Legal Issues in Information Operations, 2nd ed., November 1999, in *U.S. Naval War College International Law Studies*, Vol. 76 (2002), Appendix, p. 483, http://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1381&context=ils

33　"The Dutch government supports the general conclusions of [the 2011 'Cyber Warfare' report]." "Toespraak minister Bijleveld tijdens het seminar 'Diplomacy and Defence in Cyber Space' in Den Haag"; Advisory Council on International Affairs (AIV) and Advisory Committee on Issues of Public International Law (CAVV), *Cyber Warfare*, No. 77 AIV/No 22, CAVV, December 2011, p. 21, https://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf

34　Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, *I.C.J. Reports 1986*, p. 14.

35　Schmitt, *Tallinn Manual 2.0*, p. 341, Commentary paras. 6-7.

学説上、活発な議論が続けられている[36]。とりわけ有力な説として唱えられているのが、国による他国に対する軍事力の使用は、その重大性のいかんにかかわらず常に武力行使又はその威嚇に該当するという考え方である。例えば、外国領域における外国人の誘拐、軍用機による他国の領空侵犯、他国領海内での潜水艦による潜没航行などが、遭難、不可抗力その他の止むを得ない事情によって正当化されない限り、全てその国に対する武力行使を構成する（さらに重大であれば武力攻撃にさえ該当しうる）[37]。国によるサイバー手段の使用にこの考え方をあてはめた場合には、他国に対する有害なサイバー行動（但し、単なるネットワーク侵入（不正アクセス）は除く）の多くの例が武力の行使又はその威嚇に該当する余地がある。

英国政府が武力行使の認定基準についてどのような見解を有しているか否かは不明だが、2018 年 3 月 4 日に英国ソールズベリーで起きた元ロシアのスパイ及びその娘に対する暗殺未遂事件に関して、メイ首相は「ロシアによる違法な武力の行使」の認定を行っている[38]。このことからは現実に発生した被害の規模にかかわらず、武力行使の存在が認定される可能性が示唆される（2017 年 2 月 13 日にマレーシアで起きた金正男暗殺事件に対するマレーシアの北朝鮮政府に対する対応とは対照的な評価である）。英国の著名な国際法学者も、この暗殺未遂事件で使用された神経剤ノビチョクの無差別性、制御不能な性格によって、数多くの犠牲者が引き起こされる潜在的可能性が存在した状況[39]に照らして、この英国政府の見解は十分に説得力があると評価している[40]。

例えば、「ワナクライ」による英国国民保険サービス（NHS）トラストへのサイバー攻撃の直接の結果として患者が死亡した例は報告されておらず、また「ノットペチャ」そのものがウクライナ市民を殺傷したという事実は存在しないものの、両攻撃の重要インフラに対する無差別的攻撃によって人的・物的の両面で甚大な被害を生む潜在的可能性が存在したことは否定できない。仮に「ワナクライ」及び「ノットペチャ」の双方について国際法上違法な武力

36　Mary Ellen O'Connell, "The Prohibition of the Use of Force," in Nigel D. White & Christian Henderson, eds., *Research Handbook on International Conflict and Security Law: Jus ad Bellum, Jus in Bello and Jus post Bellum* (Edward Elgar Publishing, 2013), pp. 89-119 ; Tom Ruys, "The Meaning of 'Force' and the Boundaries of the Jus Ad Bellum: Are 'Minimal' Use of Force Excluded from UN Charter Article 2(4)," *American Journal of International Law*, Vol. 108 (2014), pp. 159-210.

37　Ibid.

38　「【元ロシア・スパイ】使用された神経剤はロシア製＝英首相」BBC 日本語版ウェブサイト、2018 年 3 月 13 日、https://www.bbc.com/japanese/43381805

39　U.N. Doc., S/2018/218, Annex to the letter dated 13 March 2018 from the Chargé d' affaires a.i. of the Permanent Mission of the United Kingdom of Great Britain and Northern Ireland to the United Nations addressed to the President of the Security Council, 13 March 2018.

40　Marc Weller, "An International Use of Force in Salisbury?," Blog of the European Journal of International Law website, 14 March, 2018, https://www.ejiltalk.org/an-international-use-of-force-in-salisbury/

行使であるとみなした国が欧米西側諸国の中にいたとすれば、それは北朝鮮とロシアの両政府がそれぞれ他国領域に対して、一種の有害行為を行ったという事実、そしてその行為が極めて無差別的であり、潜在的に広範囲の被害をもたらす破壊力を備えていたと推測される状況証拠などを総合して判断した結果であると思われる。こうした考え方とは異なり、「タリン・マニュアル 2」は、非サイバー手段については別として、少なくともサイバー手段が武力行使に該当するためには、ある程度の「規模及び効果」を要するとして一種の重大性基準を採用しているのが際立った特徴である[41]。「タリン・マニュアル 2」が両攻撃を「武力行使」ではなくむしろ「主権侵害」とみなした背景には、このような基本的な思考枠組みも作用していたものと思われる。

2. 非国家武装勢力への対処
――違法性阻却事由か、あるいは合法行為か――

（1）サイバー空間における「相当の注意」義務

イスラム国のように、いずれの国にも帰属しない非国家武装勢力からサイバー攻撃を受けた被害国（甲）が、非国家武装勢力の拠点が置かれた領域国（乙）に対して掃討作戦を依頼したところ拒絶されたと仮定する[42]。被ったサイバー攻撃は武力攻撃のレベルには達しない場合、（甲）は（乙）領域内に置かれた非国家武装勢力のサイバー攻撃拠点に対して、直接サイバー行動を講じることができるだろうか。サイバー攻撃の関連では領域国（乙）の類型は以下の 3 つに分類される。

（ア）非国家主体が現実に所在する領域国（イスラム国の例におけるイラク及びシリア）[43]
（イ）非国家主体は所在しないが領域内端末が悪用された領域国
（ウ）単に有害な通信が経由する通過国

41　但し「その重大性を測るための基準は特段示されておらず、また国家が実際にこの重大性を考慮しているのか否かについても証拠は示されていない」。Nicholas Tsagourias, “The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II- The Use of Force,” *Yearbook of International Humanitarian Law*, Vol. 15 (2012), p. 23.

42　領域国の責任を問う文脈ではないが、非国家主体に対するサイバー行動は既に行われた例が複数存在する。“UK Launched Cyber-Attack on Islamic State,” BBC website, 12 April 2018, https://www.bbc.co.uk/news/technology-43738953

43　2007 年の対エストニア DDoS 攻撃についてロシア政府の相当の注意義務違反の可能性を論じたものとして以下を参照。Russell Buchan, “Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm,” *Journal of Conflict & Security Law*, Vol. 21 (2016), pp. 429-453.

国際法上、「国家は、領域主権の行使により、その国家領域をみずから使用しまたは私人にその使用をゆるすにあたっては、他国の領域その他の国際法上の権利を害する結果にならないよう、一般国際法上の、特別の注意義務を課される」[44]ことは、伝統的に確立した原則である。この注意義務は、「消極的に」ではあるものの前述の国連サイバー GGE の 2015 年報告書でも確認されているほか[45]、学説もサイバー活動に関するこの義務の適用を肯定している[46]。

国連第4会期サイバー GGE　2015 年報告書（抜粋）[47]

・国家の責任ある行動規範（第 3 部）13 項

国家は、自国領域が情報通信技術（ICT）を使用した国際違法行為のために使用されることを知りながら許してはならない。

・現行国際法の適用（第 6 部）28 項

国家は、ICT を使用した国際違法行為を行うためにプロキシを用いてはならない。また国家は、自国領域がそのような国際違法行為を行う非国家主体によって使用されないように努めなければならない。

(2)「タリン・マニュアル 2」における扱い

①「相当の注意」義務

この国連サイバー GGE 報告書と比較すると、「タリン・マニュアル 2」における「相当の注意」義務の位置づけはより積極的である[48]。「相当の注意」原則を扱った「タリン・マニュ

44　山本草二『国際法【新版】』（有斐閣、1994 年）275 頁。

45　Eric Talbot Jensen, "The Tallinn Manual 2.0: Highlights and Insights," *Georgetown Journal of International Law*, Vol. 48 (2017), p. 745; Michael N. Schmitt, "Grey Zones in the International Law of Cyberspace," *The Yale Journal of International Law Online*, Vol.42 (2017), p. 11. とりわけ英国と米国はサイバー活動に関する相当の注意原則の適用について消極的という評価も見られる。Eneken Tikk & Mika Kerttunen, *The Alleged Demise of the UN GGE: An Autopsy and Eulogy* (Cyber Policy Institute, 2017), p. 60.

46　International Law Association (ILA), Study Group on Due Diligence in International Law, Working Session Report, 9 August, 2016, p. 2; Karine Bannelier-Christakis, "Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?," *Baltic Yearbook of International Law*, Vol.14 (2014), pp. 23-39.

47　U.N. Doc., A/70/174, paras. 13(c) and 28 (e).

48　国連サイバー GGE2015 年報告書が「許してはならない」及び「努めなければならない」の文言をともに「should」としているのに対して、「タリン・マニュアル 2」は「must」としている。シュミット教授も自身の論考において「既に他の国際法の分野で確立した原則であるゆえ、それ以外の分野でも、反対の国家実行又は法的確信がない限り、一般原則が適用されるとの推定が働く」と主張する。Michael N. Schmitt, "In Defense of Due Diligence in Cyberspace," *The Yale Law Journal Forum*, Vol. 125 (2015), p. 73, https://www.yalelawjournal.org/forum/in-defense-of-due-diligence-in-cyberspace

アル 2」規則 6 は、「他国の権利に影響を与え重大で有害な結果を生ずる」サイバー行動のために自国領域が使用されることを許さないよう相当の注意を払わなければならない、と定める[49]。規則 6 コメンタリーによれば、A 国領域内に所在するハッカーが C 国のインフラを使って B 国に対する遠隔サイバー攻撃を行う場合、C 国は注意義務を負うと書かれていることから[50]、本節冒頭で列挙した領域国の類型のうち、（ア）のみならず（イ）の領域国もこの注意義務を課されることになる（この場合の C 国を便宜的に（イ）（i）とする）。その一方で同じコメンタリーの別の箇所では、A 国領域内に所在するハッカーが B 国に対して遠隔サイバー攻撃を行うにあたり、多数の国にまたがるボットネットを手段としたが、各ボットは D 国、E 国…など一国毎に見る限り重大な結果を生じていない場合、これらの D 国や E 国などのボット所在国はボット掃討措置をとらなくてもこの義務の違反とみなされないと書かれている[51]。D 国や E 国も、本節冒頭の（イ）に分類されるが、前述の例（（イ）（i））と異なり、領域国であっても責任を問われない場合があることが示唆される（この場合の D 国及び E 国を便宜的に（イ）（ii）とする）。

さらに「タリン・マニュアル 2」は、通過国（ウ）についても「相当の注意」義務の適用を肯定する点でも特筆される[52]。通過国が有害なサイバー通信を検知、認識することは稀ではあるものの、それは「了知」の有無の問題にすぎないという理由である。また、戦時の中立国の防止義務との関連でも、「タリン・マニュアル 2」は「マルウェアは移送時にパケットに分割することができるが、完成品と分割されたパケットを区別すべき理由は存在しない」と述べて、了知と実行可能性を条件として、中立国はその移送を中断させるために措置をとる義務を負うとしている[53]。中立法は、国際武力紛争時の中立国の義務として発達した国際法の一分野ではあるが[54]、そこで確立した「相当の注意」義務は、特段の適用の支障がない限りは非国家主体による加害行為との関係でも存在するものと推定される。それゆえ、サイバー攻撃の文脈における領域国及び通過国（ア）～（ウ）について「タリン・マニュアル 2」専門家らが想定する注意義務も、中立国が負う注意義務とほぼ同じ内容であると推測される。

49　Schmitt, *Tallinn Manual 2.0*, p. 30, Rule 6.
50　Ibid., p. 32, Commentary para. 8.
51　Ibid., pp. 38-39, Commentary paras. 29-31.
52　Ibid., pp. 33-34, Commentary paras. 13-14.
53　Ibid., p. 557, Commentary para. 6. 1907 年陸戦ノ場合ニ於ケル中立国及中立人ノ権利義務ニ関スル条約（ハーグ陸戦中立条約）2 条は「交戦者ハ、軍隊又ハ弾薬若ハ軍需品ノ輸重ヲシテ中立国ノ領土ヲ通過セシムルコトヲ得ス」と定める。サイバー攻撃を目的とする有害通信がこれに該当すれば中立国はそれを阻止する義務を負う。
54　ILA, Study Group on Due Diligence in International Law, 1st Report, 7 March 2014, pp. 2-3.

表1 「タリン・マニュアル 2」の領域国（乙）の分類

	「領域」使用の態様	「相当の注意」義務の有無
（ア）領域国（物理的）	攻撃者や攻撃端末がその国に所在。	○
（イ）領域国（仮想的）	(i) 攻撃者はその国に所在せず、国内の端末を遠隔操作で悪用。	○
	(ii) 攻撃者はその国に所在せず、ボットネットとして国内の端末を遠隔操作で悪用。	×
（ウ）通過国	攻撃者も攻撃端末もその国に所在せず、マルウェアのパケットなどの有害通信がその国のインフラを一時的に通過。	○

注：筆者作成

②被害国による対応の根拠

「タリン・マニュアル 2」によれば、国家に帰属しない非国家主体が国境を越えて遠隔サイバー攻撃を行った場合、被害国との関係において、領域国（ア）及び（イ）(i)、さらに状況次第で通過国（ウ）は、「相当の注意」義務の違反を問われる可能性がある。そして、被害国はこれらの領域国に対して均衡のとれた対抗措置（性質上、サイバーであるか否かを問わない）をとることができる。但し、その対抗措置の均衡性は、被害国が非国家主体から現実に受けた被害によってではなく、領域国が適切な措置を講じなかったことに照らして判断しなければならない[55]。それゆえ、ここで許される対抗措置の内容は非国家主体による攻撃の継続を断念又は中断させるには十分でない恐れがある。

他方、被害国は、被害のレベルに応じて自衛権又は緊急避難を援用することによって、非国家主体のサイバー攻撃拠点に対して直接対応することが許されている[56]。とりわけ武力攻撃のレベルには達しないが、国家の根本的な利益に対する重大で差し迫った危険が存在する場合には、「タリン・マニュアル 2」によれば、被害国は緊急避難を援用することができる（規則 26）[57]。例えば、国の安全保障、経済、公衆衛生、治安又は環境に関係する重要インフラに深刻な被害が生じた場合などである[58]。

以上のような「タリン・マニュアル 2」の扱いを総合すると、少なくとも「タリン・マニュアル 2」においては非国家主体の遠隔サイバー攻撃との関連で「相当の注意」原則が機能する場面は極めて限定的である印象を受ける。領域国は、非国家主体によるサイバー攻撃の態様に応じて、そもそも「相当の注意」義務を負わない場合（（イ）(ii)）もあるが、「相当の注意」義務を適正に遂行して最大限可能な措置を講じた場合であっても、被害国がそ

55 Ibid., p. 130, Commentary paras. 11-12.
56 Ibid., p. 114, Commentary para. 10, and pp. 137-138, Commentary para. 10.
57 Ibid., p. 135, Rule 26.
58 Ibid., pp. 136-137, Commentary para. 5.

れを十分でないと判断すれば緊急避難に基づく越境措置を甘受しなければならないからである（領域国側から見れば同意に基づかない越境法執行措置にあたるが、被害国にとっては違法性阻却事由と整理される）。なお、被害国が緊急避難に基づき講じる措置が武力を伴うものでも良いか、あるいは武力行使未満であるべきかについて「タリン・マニュアル 2」の専門家らは合意に至ることができなかった（但し、少なくとも多数説の結論は消極的であることが示唆される）[59]。

（3）今後の国家実行の展望

まず、サイバー分野における「相当の注意」義務について政府の公式見解を示した国は現時点では数少ないが、2018 年 2 月に公表されたフランスの『サイバー・セキュリティ戦略見直し』では、「サイバー注意」（cyberdiligence）義務に言及した箇所があり注目に値する。この文書で特に言及されているのは自国のサイバー・インフラが有害な目的のために使用された状況の協力義務であり、本節冒頭の領域国（イ）に該当する（（i）、（ii）で区別を設けるかなどの細部は不明である）。この領域国が自国インフラが悪用された事実を了知しながら、要請された措置をなんら講じなかった場合には、フランス政府は被害国としての対抗措置、さらには武力攻撃発生時には自衛権に基づく措置をとる用意があることが確認されている[60]。他方、戦時の中立国の文脈ではあるが、この文書では単なる通過国は、国際人道法上、中立義務に反しないとも書かれており、本節冒頭の通過国（ウ）の注意義務の存在は否定されている[61]。また米国は、2011 年の『サイバー空間国際戦略』が「生まれつつある規範」として「サイバー・セキュリティの相当の注意義務」[62] に言及しているが、国防総省の『戦争法教範』（2015 年）は、「通信目的の機械の設置」及び「開戦前に設置したこの種の機械の利用」のみを禁止事項として列挙しており、領域国（ア）はこれに該当するものの、領域国（イ）が含まれる書きぶりにはなっていない[63]。但し、同教範における「単に中立国通信インフラをあるデータが経由するだけでは、一般的には中立違反を構成しない」[64]

59　Ibid., p. 140, Commentary para. 18.

60　Secrétariat général de la défense et de la sécurité nationale (SGDSN), *Revue stratégique de cyberdéfense,* 12 February, 2018, pp. 83-84 and 86, http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/

61　Ibid., p. 84.

62　The President of the United States of America, *International Strategy for Cyberspace*, May 2011, p. 10, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

63　本文に引用した該当部分は、すべて 1907 年ハーグ陸戦中立条約 3 条の規定文言の引用である。U.S. Department of Defense, Office of the General Counsel, *Law of War Manual*, June 2015, p. 1002.「設置」（erect）の語に、遠隔操作で端末の機能を奪取する、という意味が読み込めない限り、（イ）の領域国が義務違反を問われる可能性は存在しない。

64　Ibid., pp. 1002-1003.

と述べた部分からは、フランスと同様に少なくとも通過国（ウ）について「相当の注意」義務の存在を否定した見解と受け取れる[65]。さらに、1で触れた英国法務総裁のスピーチは、サイバー空間に特有の主権規則は存在しないという見解であったが、本節冒頭の領域国（イ）及び通過国（ウ）のように、サイバー空間に特有の状況において「相当の注意」義務が生じるか否かは慎重に考察すべき論点である。「相当の注意」原則は領域主権原則からの派生的原則であることに鑑みると、サイバー空間そのものに対する領域主権がそもそも存在しないのであれば、その帰結としてサイバー空間に特有の状況における注意義務は発生しないという結論が導かれうる。

これと同様に、被害国がとる措置の根拠も、「主権」の基本的な捉え方によって結論は変わりうる。学説（「タリン・マニュアル 2」専門家らの少数説を含む）の中には、被害国が領域国の同意なく非国家主体のサイバー攻撃インフラに反撃することは国際法上許容されると説くものがある[66]。既に述べたように、（イ）の領域国は自国領域内の端末が遠隔で乗っ取られる事実について、また通過国（ウ）は自国領域内に敷かれた光ファイバー・ケーブル内を有害通信が通過する事実について、それぞれ領域主権を行使していないのであれば、被害国が直接それらの端末やケーブルに対して是正措置を講じても自国の主権が侵害されたことにはならない。それゆえ、被害国がとる措置は、「タリン・マニュアル 2」多数説が違法性阻却と位置付けたのとは対照的に、武力行使のレベルに達しない限りは、それ自体が国際法上、合法的な措置として整理される。

（4）暫定的評価

伝統的な国際法上の主権原則がサイバー空間に特有の状況において、どのように適用されるかという問題について、現時点ではまだ国家実行は未成熟である。但し、さきの英国法務総裁の見解に加え、米国における電子証拠の扱いをめぐる一連の経緯を一瞥した限りでは、その見方は「タリン・マニュアル 2」とは異なる印象を受ける。米国では、海外クラウドサーバに保管された容疑者の電子メールデータを刑事共助条約（MLAT）によらずに、当該サーバを運用する米国の通信事業者を通じて直接入手することの是非をめぐって過去数年間にわたり、複数の事件が連邦裁判所で争われた（「マイクロソフト捜索令状事件」[67]や

65　同じ立場の学説としては以下を参照。Johann-Christoph Woltag, *Cyber Warfare: Military Cross-Border Computer Network Operations under International Law* (Intersentia Publisher, 2014), p. 260 et seq.

66　Jensen, “The Tallinn Manual 2.0,” p. 743; Corn and Taylor, “Sovereignty in the Age of Cyber,” p. 211.

67　In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016).

グーグル社の同種の事件[68]など）。この争いは、2018 年 3 月 23 日にクラウド法（Clarifying Lawful Overseas Use of Data Act（CLOUD Act））[69]が成立したことをもって決着し、同法 2713 条は「電気通信事業者又は遠隔コンピューティング事業者は、通信データその他の顧客情報について、それが米国領域内に置かれているか、又は領域外にあるかにかかわらず、保管、バックアップ、開示する義務を負う」と定めたことによって、海外サーバに保管された電子データの入手はサーバ設置国の領域主権を侵害しないという米国政府の方針が明らかにされた。同法は、属地主義を著しく損なう不当な法執行権限の拡大であるとして多方面から批判を招いている[70]。

「タリン・マニュアル 2」は、データに対する領域主権の行使可能性についての直接の言及を避けているものの、「属地的管轄権は、自国領域内で行われるサイバー活動に従事する自然人及び法人、並びに自国領域内におかれたサイバー・インフラ及びデータに対して適用される」[71]（下線は筆者）と述べる箇所からは、それを肯定しているように見える。仮に米国のクラウド法のような国家実行が今後、多くの国家によって踏襲されていく場合には、それと対極の立場を採用する「タリン・マニュアル 2」の見解は、主権、管轄権、相当の注意義務、対抗措置や緊急避難の範囲など多くの論点にわたり支持されず、修正を受ける可能性があると言えよう。

3. 中国の唱える「サイバー主権」と「タリン・マニュアル 2」の比較

前述の英国政府関係者の「サイバー特有の主権規則は存在しない」という発言箇所の正確な意味は不明だが、もう一つの動機として考えられるのは、主に中国が主張する「サイバー主権」概念の否定である。

68　In re Search Warrant No. 16-960-M-01, 232 F. Supp. 3d 708, 2017 U.S. Dist. LEXIS 15232 (E.D. Pa., Feb. 3, 2017).

69　Chap. 121 of title 18, United States Code. EU における同種の動きについては以下を参照。"E-evidence - Cross-border Access to Electronic Evidence," European Commission website, https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/criminal-justice/e-evidence_en; ; Katitza Rodriguez, "A Tale of Two Poorly Designed Cross-Border Data Access Regimes," Electronic Frontier Foundation website, 25 April, 2018, https://www.eff.org/ja/deeplinks/2018/04/tale-two-poorly-designed-cross-border-data-access-regimes

70　Katitza Rodriguez, "The U.S. CLOUD Act and the EU: A Privacy Protection Race to the Bottom," Electronic Frontier Foundation website, 9 April, 2018, https://www.eff.org/ja/deeplinks/2018/04/us-cloud-act-and-eu-privacy-protection-race-bottom; Théodore Christakis, "Law Enforcement Cross-border Access to Data and Human Rights", Presentation at the 10th International Conference on Cyber Conflict: CyCon X: Maximising Effects, 30 May 2018, Tallinn, Estonia.

71　Schmitt, *Tallinn Manual 2.0*, p. 55, Commentary para. 1.

（1）「タリン・マニュアル 2」における扱い

サイバー手段による電気通信は、伝統的に国際電気通信法の文脈で語られる電気通信に該当する[72]。この分野では国家は古くは主権原則に由来する電気通信停止権を有するとされてきたが（国際電気通信憲章 35 条及び 34 条 2）[73]、「タリン・マニュアル 2」規則 62 は国家がサイバー通信について通信停止権を有するとしている。

> 規則 62（a）国家は、部分的に又は完全に、自国領域内における国際サイバー通信業務を停止することができる。当該停止の即時の通知が他国に対してなされなければならない[74]。

但し、規則 62 における「停止」は、「サービスの一時的な中断」を意味するため、政府が半永久的に特定の通信を遮断することはこの規則の下では許容されない。つまり、規則 62 を読む限り、国家が特に通信内容（コンテンツ）との関係で停止権を行使できるのは、極めて限定的な範囲にとどまる（もっとも、その根拠は示されていない）。国家が包括的に通信規制権を行使することが認められるのは、電気通信事業者の主体とその事業形態に対する規制という文脈においてだけである[75]。

他方、「タリン・マニュアル 2」は、対内的主権の文脈では国家の包括的な規制（停止）権を認めているように受け取れる。規則 2 コメンタリーでは、「国家が対内的主権を享有する結果、国家は自国領域内に所在する人間が特定のオンライン・コンテンツにアクセスすることを部分的に又は全体的に制限することができる」としているからである。国家は、最終的にはその通信規制（停止）権を制限されるとしても、その理由は、国家が適用可能な国際法規範を考慮しなければならないからである。中でも、国際人権諸条約が定める表現の自由はいまや国際慣習法化しており、それゆえ、特定の通信を遮断したいと考える政府は、非差別的な方法で、かつ国内法に基づく形で遮断を実施しなければならない、と「タリン・マニュアル 2」は主張する[76]。

（2）中国の「サイバー主権」

以上のように、「タリン・マニュアル 2」は国家の包括的な通信規制（停止）権を通信内容（コ

72　Ibid., pp. 284-285, para. 3.
73　小寺彰「電気通信と主権――国際電気通信業務分野を対象にして――」『国際法外交雑誌』90 巻 3 号（1991 年）291 - 295 頁。
74　日本語訳は、中谷・河野・黒崎『サイバー攻撃の国際法：タリン・マニュアル 2.0 の解説』63 頁参照。
75　Schmitt, *Tallinn Manual 2.0*, p. 291, Rule 61, Commentary para. 10.
76　Ibid., p. 15, Rule 2, Commentary para. 8.

ンテンツ）を含めて認める点で、一見すると中国政府の主張と似通った内容を備えている。中国はあらゆる機会を捉えて「サイバー主権」の考え方を提唱しており、例えば 2015 年に中国烏鎮で開催された第 2 回世界インターネット会議の開会式において、習近平主席は以下のような発言を行っている。

> 我々は、個別の国家がその国独自のサイバー分野の進展方法、その規律モデル及びインターネットの公共政策を自立的に選択し、同じ立場で国際的なサイバー空間のガバナンスに参加する権利を尊重しなければならない。いかなる国もサイバー分野の覇権を追求し、他国の国際問題に干渉し、又は他国の安全保障を害するサイバー活動に従事、共謀、若しくは支援してはならない[77]。

この引用部分のみをもって、中国政府が具体的に想定するサイバー主権の内容を読み解くのは容易ではないが、その一つとして挙げられるのは、サイバー空間における人権の問題である。

中国は、ロシアを始めとする他の上海協力機構加盟国と共同で 2011 年及び 2015 年に国連事務総長に「情報セキュリティ国際行動綱領」[78] を提出しているが、2015 年版の 2（7）は、以下の通り、オンライン環境上の個人の人権を各国は国際基準に基づき保護する、と定めている。

> 2（7） オフライン環境における個人の権利はオンライン環境でも保護すること、すなわち情報空間における権利と自由を十分に尊重すること（情報を求め、受け、及び伝える自由を含む）。また、市民的及び政治的権利に関する国際規約（自由権規約）が特別の義務及び責任を課していることを考慮する。それゆえ、個人の権利は、法によって定められ、また必要な限りにおいて一定の制限に服する。
>
> （a）・・・（略）
>
> （b）国の安全、公の秩序又は公衆の健康若しくは道徳の保護[79]。

共同提出国の中で中国は唯一、自由権規約の締約国ではないが、この 2015 年版行動綱領の引用部分を見る限り、中国は自発的な国際人権規範の遵守を装いつつ、「国の安全、

77 Remarks by H.E. Xi Jinping President of the People's Republic of China at the Opening Ceremony of the Second World Internet Conference, Ministry of Foreign Affairs of the People's Republic of China website, 15 December, 2015, http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml

78 U.N. Doc., A/66/359 and A/69/723.

79 U.N. Doc., A/69/723, International Code of Conduct for Information Security.

公の秩序」（自由権規約 19 条 3（b））を理由に挙げて人権の制限を正当化しようと画策しているように思われる。

国際電気通信の過去の類例として想起されるのは、1970 ～ 80 年代に衛星による国際直接テレビジョン放送の文脈において米国とソ連が展開した通信主権をめぐる論争である。当時、米国が主要な放送国として情報の自由な流通原則を主張したのに対して、ソ連は放送受信国として通信主権に基づく外部情報の妨害及び統制の権利を主張して双方が歩み寄ることはなかった。結局、1982 年に放送受信国の通信主権の保障を認めた国連総会決議 37/92[80] が採択され、多くの西側諸国は反対票（13 カ国）か棄権票（同）を投じる結果となった[81]。こうした一連の経緯に鑑み、「個人の情報の自由または国家相互間の情報の自由流通の原則が、一般国際法上、外国むけの番組発出の権利をみとめ受信国による妨害を禁止する効果をもつものになっていること」の「立証は困難である」との学説上の評価も見られる[82]。

（3）暫定的評価

英国政府による「サイバー特有の主権規則は存在しない」旨の発言の真意は別として、中国政府による特定の通信の遮断については英国のみならず多くの西側諸国が好ましくないと考えているはずである。但し、国際電気通信法の文脈で語られてきた通信規制（停止）権が、従来から放送国と受信国との間で争われてきた経緯からすると、サイバー通信が新たな電気通信の形態であるという理由だけで主権規則の存在を否定するのは説得力に欠ける。前述のように、中国は自発的に国際人権規範を遵守してサイバー空間上の人権を尊重すると主張しており、表面的に捉えれば西側諸国の主張となんら変わりがない[83]。

4. 残された課題
――サイバー攻撃が国内問題への違法な干渉に該当する基準――

本稿では紙幅の制約から論点の提起にとどめるが、1でも述べた通り、「ワナクライ」攻撃

80　U.N. Doc. A/RES/37/92, Annex: Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting, 10 December 1982.

81　この決議によれば、「国際直接放送衛星業務を設定しようとする場合には、各国はその意思を予定受信国に遅滞なく通報し協議に入るほか、関係国間の協定・取極めの事前締結を義務づけられている（原則 J、13・14 項）。しかもこれらの協定・取極め」は、「番組内容の規制を含む非技術的な合意を含むものと、解されている」。山本草二「国際間情報流通と通信主権の法機能」『ジュリスト増刊』（1984 年）71-72 頁。

82　同上、72 頁。

83　Zhixiong Huang & Kubo Mačák, "Toward the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches," *Chinese Journal of International Law*, Vol. 16 (2017), p. 24.

で発生した「重要医療サービスを攻撃目標とする行為は」禁止された干渉に該当する可能性が指摘されている[84]。とりわけ近年、この論点をめぐって活発な議論が見られるのは、欧米諸国に対してロシア当局が行ったと主張されるサイバー手段を用いた選挙干渉である。2016 年の米国大統領選では、民主党全国委員会のシステムがハッキングされ内部の情報が外部に漏えいしたり、ソーシャルメディアが悪用され偽情報が米国全土に出回る事態が生じた。

禁止された干渉に該当する基準として「タリン・マニュアル 2」は、一方の国による他国の「国内又は対外事項」への意図的な介入であることに加えて、この介入が強制を伴うことを列挙する[85]。但しロシア当局による米国大統領選への干渉行為がこれらの基準を満たすか否かについてシュミット教授は消極的である。その理由は強制性の基準が必ずしも充足されているとは言い難いことに加えて、民主党全国委員会へのハッキングは国際法上必ずしも禁止されない諜報行為に該当するためである[86]。但し、基準が明確でないのはこの強制性の要件についてのみならず、「国内又は対外事項」の範囲も同様である。例えば医療についての政策は国によって異なるところ、公共サービスだけが「国内事項」に該当するのか、あるいは国民の福利厚生という観点から民間のサービスも広く含まれるのか、などの論点である。少なくとも英国法務総裁の言及は、英国が「ワナクライ」により国民保険サービス（NHS）が受けた被害を想定しているものと推測される。

おわりに

本稿では、「タリン・マニュアル 2」で扱われたサイバー活動に適用される国際法のなかでも、特に近年各国政府関係者が言及している関心の高い論点をいくつか取り上げた。具体的には、まず第 1 に 2017 年に世界各国で被害が発生した「ワナクライ」及び「ノットペチャ」などのサイバー攻撃が国際法違反とされる根拠は何かという論点を考察した。各国はその根拠を明確に提示しているわけではないが、「タリン・マニュアル 2」とは異なる根拠が示唆されていることを論じた。このことは、単に違法性の根拠が異なるだけの問題にとどまらない。むしろ、国境を越えて行われるサイバー行動であっても、そもそも国際法上違法とならない場合があると一部の国が考えている可能性があること、もっとも合法と違法との間の境界についても確固とした国際的なコンセンサスが存在しないという、この問題をめぐる国際法の混沌とした状況が確認された。この問題は、本稿で論じた第 2 の論点にも大きく関係する。

84　Cyber and International Law in the 21st Century, Speech by the Attorney General Jeremy Wright.
85　日本語訳は、中谷・河野・黒崎『サイバー攻撃の国際法：タリン・マニュアル 2.0 の解説』71 頁参照。
86　Schmitt, “Grey Zones in the International Law of Cyberspace,” p. 8; Willian Banks, “State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0,” *Texas Law Review*, Vol. 95 (2017), p. 1512.

第 2 の論点として本稿では、非国家武装勢力のサイバー攻撃に対して被害国がどのような国際法規範を根拠として対応可能かという問題を論じたが、「タリン・マニュアル 2」でさえも、この場合に被害国に許容される措置の限界については専門家間で合意に達することができなかったことを認めている。これらの論点は、すべて国際法上の「主権」原則のサイバー空間における意味にかかわる問題である。その端的な例として本稿では、中国政府の主張するサイバー主権の考え方は、実のところ「タリン・マニュアル 2」の「対内的主権」との間で一定の親和性があることを論じた。最後の論点は、深く検討するには至らなかったが、選挙干渉などを目的とする一定のサイバー行動が国際法上禁止された干渉行為に該当する可能性について言及した。「タリン・マニュアル 2」の基準の下では境界事例に該当するため、この基準の確立も今後の国家実行の成熟を待つほかない。このように多岐にわたる論点は、必ずしも各国によって「タリン・マニュアル 2」の記述内容の通りに理解されているとは言い難いが、同文書が各国による発信、また各国相互の対話を促していることもまた事実である。今後は、より具体的な形で、実際のサイバー攻撃事案の文脈における国際法の適用過程が各国によって提示されることを期待したい。

（こうのけいこ　理論研究部政治・法制研究室主任研究官）