サイバーセキュリティと国際法・国際政治

情報セキュリティ大学院大学　名誉教授　林（はやし）　紘一郎（こういちろう）

1. はじめに

本稿は、筆者が日本ITU協会第84回情報通信研究会（2019年9月27日）において行った、標題の講演を要約したものである。インターネットのガバナンスと国際政治には、a) 権威が一意に確定せず分散しており、b) マルチ・ステーク・ホルダーの合意形成方式はそれなりに機能しているものの、c) かといって国境や主権といった伝統的な概念を無視できない、という3つの共通点がある。日本国内では、三権が分立し法律（例えば刑法）が厳格に執行されているのに反して、国際政治や国際法の分野は合意に達しても実効性に難があるため、理系の方々には「頼りない」ものと映るかもしれない。しかし、少なくともそれが上記のa)～c)と連動していることを、理解していただければ幸いである。

2. グローバル化した国際関係の見方

複雑な国際関係を見る視点は様々なものがあろうが、最近の動向を捉えたものとして私の心に響いたのは、『グローバリゼーション・パラドクス』の著者であるロドリックのトリレンマ（三方一両得ではなく、三者鼎立（ていりつ）は不可能）という概念である。邦訳者の1人である柴山教授によれば、その考え方は以下のように要約される（訳者あとがき）。

「本書の核となるアイディアは、市場は統治なしには機能しない、というものだ。（中略）市場と統治という視点に立つと、グローバル経済が抱える根本的な問題が見えてくる。グローバル市場では、その働きを円滑にするための制度がまだ発達していない。全体を管理するグローバルな政府も存在していない。一国レベルでは一致している市場と統治が、グローバルなレベルでは乖離しているのだ。貿易や金融は国境を越えて拡大していくが、統治の範囲は国家単位にとどまっている。ここにグローバル経済が抱える最大の『逆説』がある、というのが著者の問題意識である。

グローバリゼーションのさらなる拡大（ハイパーグローバリゼーション）、国家主権、民主主義の3つのうち2つしか取ることができない、という本書の『トリレンマ』に従うなら、今後の世界には3つの道がある。①グローバリゼーションと国家主権を取って民主主義を犠牲にするか、②グローバリゼーションと民主主義を取って国家主権を捨て去るか、③あるいは国家主権と民主主義を取ってグローバリゼーションに制約を加えるか、である。

3. インターネットの理想と現実

インターネットは「自律・分散・協調」を基本理念に、中央集権的な管理機関を排した全員参加型（あるいはe2e）のメディアとして誕生し、発展してきた。それを徹底すれば、「インターネット自治圏」が国家の統制のない形で成立する（governance without government）のが理想になる。現にJohn Perry Barlow（Electronic Frontier Foundationの共同設立者）が起草し、インターネット商用化直後の1996年に発表された「サイバースペース独立宣言」は、「国家はインターネットの領域に入るべからず」と、「治外法権」を高らかに宣言するものであった（https://www.eff.org/cyberspace-independence）。

しかし、こうした「インターネット原理主義」とも言える主張も、翌年の「通信品位法」の制定（一部は憲法違反で効力を停止されたが）、1998年の「デジタル・ミレニアム著作権法」によるISPのnotice-and takedownの義務化等*1により次第に制限され、逆に「インターネットは特別な領域ではなく、従来の法律が適用される」という理解が広まっていった。

そして、インターネット治外法権説に決定的に不利となったのが、サイバー犯罪やサイバー攻撃の頻発と深刻化であった。「自律」を目指すインターネットは、簡便で安価な通信手段として重厚長大の電話ネットワークに取って変わったが、その陰でセキュリティに対しても「自律的」に対応する（つまりはエンド・ユーザーに任せる）ことを是とせざるを得なかった。その結果、巧妙な発信者が匿名性を悪用して攻撃を仕掛けるのに対して、防御側が発信者を特定できず*2、圧倒的に不利になる状況「非対称性」をもたら

*1　わが国のプロバイダ責任（制限）法の、手本になった仕組みである。
*2　インターネットや国際政治の世界では、attribution問題という。

した*3。

しかも20世紀中の攻撃は、ハッカー（という個人）の自己顕示欲が動機であったため、被害はさほど深刻ではなかったが、21世紀に入る頃から「サイバー攻撃で金儲けができる」ことが明らかになって、職業的攻撃が一般的になった。さらに2010年代には、金銭動機に加えて政治目的（ハクティビズム）や国家安全保障への挑戦などの新しい目的が付加され*4、攻撃に特定の国家が関与しているとの指摘が否定できない状況になっている*5。

4. サイバー攻撃に対する自衛権の行使とTallinn Manual

防御側は、上記のような「非対称」を甘受し、放置していたわけではない。特に顕著な反撃姿勢を示したのが、米軍である。2011年に米国防総省は、サイバー空間を陸・海・空・宇宙空間に次ぐ「第5のdomain」と定義し、2019年には、11（地域別に6+機能別に5）ある統合軍（Unified Combatant Command）の1つに昇格させた。

また法律面では、サイバー空間上の攻撃（kineticでなくても深刻なものを含め）には、武力をもって対峙すると宣言している。米国はもともと、国連憲章における自衛権発動の要件としてarmed attackとuse of forceを区分せず、いずれに対しても自衛権の行使は可能であると解釈してきた*6。そしてオバマ政権は、サイバー領域においても同様であるという態度を示していた*7。

なお、国連憲章51条において「（個別的・集団的）自衛権の行使」は、限定的な条件の下で認められている。同条の原文は、以下のとおりである。

‘Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.’

しかし現実問題として、「自衛権の行使がどこまで認められるのか」の判断には、常にグレイゾーンが避けられない。しかも国連憲章上「自衛権の行使」は、「安全保障理事会が必要な措置をとるまで」の暫定的な合法性しか持たないが、その理事会が紛糾すれば事実上放置され、「自衛権の行使」が実行上継続する。特にkineticなものではないサイバー上の自衛権は「目に見えない」ものであるだけに、脱法行為の温床になりかねない。そこで、サイバーに特化した国際紛争の処理方式を明確にしようという動きが生じ、少なくとも西欧先進国間ではTallinn Manualの編纂というプロジェクトにつながっていった。

タリン・マニュアルの作業は、米国海軍大学校のMichael Schmitt教授を中心として進められ、まず2013年には、95の規則からなる「サイバー戦に適用される国際法に関するタリン・マニュアル」（第1部「国際サイバー安全保障法」、第2部「サイバー武力紛争法」）が刊行された。このマニュアルが「有事（戦時）」を対象としたものであったのに対して、その後「平時」におけるサイバー活動が諸分野の国際法の観点からどう評価されるかという新たな作業が行われた。その成果が2017年2月に刊行された「サイバー行動に適用される国際法に関するタリン・マニュアル2.0」である。

タリン・マニュアル2.0の原著は600ページに及び、154の規則とその詳細なコメントを含むもので、この短文の中で

＊3　攻撃者優位は、①攻撃の成否、②手段の入手、③対応組織・要員、④予備要員、⑤国際連携、⑥国家の潜在的支援、⑦CPUパワーと制御、⑧行為者の特定の8点に及び、特に最後の点が顕著である。

＊4　政府に対する攻撃事例：2007エストニアに対するDDoS攻撃、2010年イランの核施設に対するStuxnet攻撃、2015年米国OPMからの人事情報流出、2015/16年ウクライナ停電、etc.

＊5　政府支援の下で実行されたと思われる事例：2014年米司法省が中国人民解放軍の将校ら5人を不正アクセス・情報窃取で起訴、2018年米司法省は北朝鮮籍のPark Jin Hyokを、SPE事件・バングラデシュ中央銀行事件・ワナクライによる攻撃の3件に主要な役割をはたしたとして起訴。

＊6　国連憲章の該当条文（2条4項）は、以下のとおり。All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.

＊7　当時の国務省法律顧問Harold Kohの講演（http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/）参照。

要約することは不可能である。そこで、国際法上最もシリアスな事態である「武力攻撃」に関連する規則の部分だけを紹介すれば、以下の枠内のようになる（邦訳は、中谷・河野・黒崎［2018］[5]による）。

規則68（武力による威嚇又は武力の行使の禁止）
いかなる国家の領土保全若しくは政治的独立に反する、又は国連の目的と両立しない他のいかなる方法による武力による威嚇若しくは武力の行使を構成するサイバー行動も、違法である。
規則69（武力の行使の定義）
サイバー行動は、その規模及び効果が武力の行使の水準に至る非サイバー行動に比肩しうる場合、武力の行使に該当する。
規則70（武力による威嚇の定義）
サイバー行動又はサイバー行動の威嚇は、その威嚇行為がもし実行されれば違法な武力の行使となる場合には、違法な武力による威嚇になる。
規則71（武力攻撃に対する自衛）
武力攻撃の水準に至るサイバー行動の目標となる国家は、固有の自衛権を行使することができる。サイバー行動が武力攻撃に該当するか否かは、その規模及び効果による。
規則72（必要性及び均衡性）
自衛権の行使として国家によってとられるサイバー行動を含む武力の行使は、必要かつ均衡のとれたものでなければならない。
規則73（急迫性及び即時性）
自衛の際に武力を行使する権利は、サイバー武力攻撃が発生した場合又は急迫した場合に生じる。この権利はさらに即時性の要件に従う。

5. 不確実性の中で、わが国にできること

タリン・マニュアル2.0は、よくできた規則集であるが、残念ながらロシア・中国などは参加しておらず、その有効性も認めていない。ロシアからすれば、「国連でインターネットの行動規範（code of conduct）を作るべきだ」と先に主張したのは自分たちの方で、それを優先すべきだと言いたいところだろう。

ところが、そのロシアの主張を入れて2004年から2017年まで5次にわたって断続的に開催されてきたGGE（Group of Government Experts）会合は、最終的な合意に至らなかった。対立点の核心を前述のロドリックのトリレンマで表せば、ロシアと中国等は①グローバリゼーションと国家主権を取って民主主義を犠牲にすることを厭わないのに対して、西欧諸国は③国家主権と民主主義を取ってグローバリゼーションに制約を加える、という道を選ぶしかないからであろう。なぜなら民主主義国家は、インターネットの国家的監視などは容認できないからである。

それでも、現実の国際政治や国際貿易が動いているのはなぜかと言えば、両陣営とも「対立がこれ以上先鋭化する」ことは避けたいので、「国連憲章がインターネットにも適用される」といった最低限の合意で、際どいバランスを保っているからである*8。しかし、ここで1点注意すべきことは、このような際どいバランスは、国連ほかの議決方式である「多数決原理」の下では、いとも簡単に破棄されてしまいかねないことである。どんな小国であれ、それぞれが1票を持つ仕組みにおいては、西欧先進国も小国の1つと変わらない。こうした多数決原理の陥穽（かんせい）に関して、本誌の読者であるITU関係者には、WCIT-12（World Congress on IT、2012年）におけるInternational Telecommunication Regulation改定の経緯を思い出していただくだけで十分だろう（出口［2013］[4]）。

さて、国際秩序とインターネット・ガバナンスは、governance without governmentという点で共通項があり、マルチ・ステークホルダー・プロセスという時間と労力のかかる手順に拠らなければならない。しかも、「インターネットは民主主義と同義に近く、国家主権よりも優先する価値がある」と考える西欧先進国と、「国家主権あってのインターネット」と考える中国・ロシア等の国々の調整は不可能に近い。このような「乱世」の中で、わが国が何らかの役割を果たす

*8 GGEが失敗に終わった直後の、次のブログの記述が、その間の事情を物語っている（https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well）。'The controversy is "manufactured" because both the 2013 and the 2015 GGEs declared that "international law, and in particular the Charter of the United Nations," were applicable to cyberspace. It does not seem to be any country's position that the right to self-defense-the inclusion of which some states opposed in the current report-does not apply in response to cyber operations that meet the threshold of an "armed attack" under Article 51 of the UN Charter.'

余地はあるのだろうか。

秩序が乱れている中で「分不相応」なことをすれば、「天に唾する」ようなもので自分に降りかかってくる。「唯一の被爆国」でありながら、核拡散防止でリーダーシップを発揮できない国にやれることは限られている。まず、わが国のサイバー・レジリエンス力を客観的に理解することが前提で、「できる範囲でできることをする」が基本とならざるを得まい。

ここで参考となる情報として、次の2つがある。1つは、国家のサイバーセキュリティ戦略の成熟モデルとして評価の高い、Oxford大学のCMM（Cybersecurity Capacity Maturity Model for Nations）による国際比較（https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cybersecurity-capacity-maturity-model-nations-cmm）である。このモデルに基づいて、筆者がわが国の成熟度を試算したところ、先進諸国に比してかなりの劣位にあると認識せざるを得なかった（林・田川［2018］[9]）

他の1つは、笹川平和財団の提言「日本にサイバーセキュリティ庁の設置を」の前提になっている、サイバーセキュリティ政策の各国比較表である（https://www.spf.org/global-data/20181029155951896.pdf）。その結果は、上記における筆者の試算よりもさらに厳しく、わが国は「サイバーセキュリティ庁を含めて、早急に体制の整備が必要」との結論を導いている。

これらは、主観的要素を多分に含んだ分析に過ぎないが、それにしても「まず己の実力を知る」ことの必要性を訴える点では価値のあるものと思われる*9。

6. 国際法は無能か：まとめに代えて

世界統一国家が不在の中で、国際秩序を定立し維持していくためには、主権国家の間の合意を形成し、不断に確認していくことが不可欠である。国際法がしばしば慣習法として成立し、強制力を持たないまま一定の効力を有し続けているのは、このような理解が主権国家の間で共有されていることの証である。セキュリティ分野では常識化しているソフト・ローという概念*10も、主として国際法から出たものであり、マルチ・ステークホルダー・プロセスに適合的である。

しかし、制定法（大陸法）に慣れた日本人から見れば、法の最大の特徴は「強制力」にあることは否定できず、それを欠く法は「いかにも頼りない」印象は否めない。北朝鮮等のrogue statesに対して有効な制裁を加えられないのは、その端的な事例である。Tallinn Manual 2.0に関しても中谷教授は「タリン・マニュアルは、サイバー攻撃に関する国際法を『作成』するものではない。既に慣習国際法（一般国際法）が存在するという前提の下に、それを『確認』して『記述』するという作業である」としている（前掲書「はしがき」）。

理系の方から見れば、このような国際政治や国際法の現状は、時間と労力の無駄と映るかもしれない。しかし、インターネットのガバナンスと国際政治は、a）権威が一意に確定せず分散しており、b）マルチ・ステーク・ホルダーの合意形成方式はそれなりに機能しているものの、c）かといって国境や主権といった伝統的な概念を無視できない、という3つの共通点を持っている*11。

日本国内では三権が分立し、法律（例えば刑法）が厳格に執行されていることと対照的に、国際政治や国際法の分野は曖昧さを伴わざるを得ない。理系の方々のみならず、法律を研究対象にしている筆者にとってさえ、このような現状は理想からほど遠いが、それが上記のa）～c）と連動していることを理解していただければ幸いである。インターネットが「ベスト・エフォート」で成り立っているのと同様、国際秩序も「ベスト・エフォート」に期待せざるを得ないのである。

（2019年9月27日 情報通信研究会より）

引用・参考文献

［1］ 小宮山功一朗［2019］「サイバーセキュリティにおけるインシデント対応コミュニティの発展」『情報通信学会誌』Vol. 37, No. 1

［2］ 田川義博［2013］「インターネット利用における『通信の秘密』」『情報セキュリティ総合科学』Vol. 5、情報セキュリティ大学院大学

＊9 電気通信の関係者には、本文で紹介した2つのモデルよりも、ITU-Dが定期的に発表するGCI（Global Cybersecurity Index）の方がなじみがあるかもしれない。しかし、2017年版では12位であった英国が、2018年版では首位になるなど不安定であることと、D（開発）に主眼があることから、本文では触れなかった。

＊10 法的な強制力がないにもかかわらず、現実の経済社会において国や企業が何らかの拘束感をもって従っている規範。

＊11 小宮山［2019］[1]によれば、後者には「国際関係の安定や国の安全保障という論点が加わる」点で違いがあるが、近年その点が曖昧になっていることも認めている。

http://www.iisec.ac.jp/proc/vol0005/tagawa13.pdf
［3］ 田川義博・林紘一郎［2017］「サイバーセキュリティのための情報共有と中核機関のあり方 ―3つのモデルの相互比較とわが国への教訓―」『情報セキュリティ総合科学』Vol. 9、情報セキュリティ大学院大学
http://www.iisec.ac.jp/proc/vol0009/tagawa-hayashi17.pdf
［4］ 出口岳人［2013］「世界国際電気通信会議（WCIT-12）結果報告（総括）」『ITUジャーナル』Vol. 43, No. 3
［5］ 中谷和弘・河野桂子・黒崎将広［2018］『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
［6］ 林紘一郎［2014］「サイバーセキュリティと通信の秘密」土屋大洋（監修）『仮想戦争の終わり』角川学芸出版
［7］ 林紘一郎［2016］「サイバーセキュリティ事故情報共有のあり方」『情報通信学会誌』Vol. 34, No. 3
［8］ 林紘一郎・田川義博［2016］「サイバーセキュリティにおけるバルクデータの意義」『情報セキュリティ総合科学』Vol. 8、情報セキュリティ大学院大学
http://www.iisec.ac.jp/proc/vol0008/hayashi-tagawa16.pdf
［9］ 林紘一郎・田川義博［2018］「サイバー攻撃の被害者である民間企業の対抗手段はどこまで可能か：日米比較を軸に」『情報セキュリティ総合科学』Vol. 10、情報セキュリティ大学院大学
http://www.iisec.ac.jp/proc/vol0010/hayashi-tagawa18-2.pdf
［10］ ロドリック、ダニ、柴山桂太・大川良文訳［2014］『グローバリゼーション・パラドクス』白水社