
サイバー国際規範をめぐる規範起業家と規範守護者の角逐

原田 有

<要旨>

本稿の目的は、サイバー空間の規範形成プロセスが複雑化してきた過程とその要因を、規範の形成や伝播に向けたアクターの活動や戦略に着目するコンストラクティビズム研究の視座から分析することにある。具体的には、国家によるサイバー空間の統制に資する新たな規範を求める主にロシアの規範起業家としての試みを、情報の自由な流通や表現の自由等を含む既存の国際法の適用を重視する米国等の規範守護者が阻むことで、プロセスが複雑化してきたことを論じる。また、フランスが非国家主体と連携する形で、複雑さの解消に向けた役割を果たしつつある点も指摘し、こうした調整者の機能の分析が今後の研究課題となることを述べる。本研究は、論点や関与するアクターが多様かつ現在進行中の規範形成プロセスの一端を考察するにとどまるが、コンストラクティビズム研究の射程をサイバー空間という新たな事例にも広げるところに意義がある。

はじめに

サイバー空間でのアクターの責任ある行動に関する規範形成に向けた取組（規範形成プロセス）が複雑さを増している。国際連合（国連）では2019年、2004年からある政府専門家会合（GGE¹）に加えて、議題を重複させるオープン・エンド作業部会（OEWG²）も新設された。OEWGはGGEとは異なり、国連全加盟国に加えて、非国家主体の参加も一定程度認める点を特徴とした。注目されたのは、そのOEWGがサイバー空間での国家の役割を重視するロシアによって提起され、非国家主体との連携も重視する欧米諸国はむしろ参加国すらも限定されるGGEを重視したことである。このねじれ現象は、なぜ生じたのか。国連外での取組も視野に入れるとより浮き彫りになるプロセスの錯綜状態には、アクターのどのような活動や戦略が反映されているのか。

1 Group of Governmental Experts の略称。

2 Open-ended Working Group の略称。

本稿の目的は、サイバー空間の規範形成プロセスが複雑化してきた過程とその要因を、規範の形成や伝播に向けたアクターの活動や戦略に着目するコンストラクティビズム研究の視座から分析することにある。具体的には、国家によるサイバー空間の統制に資する新たな規範を求める主にロシアの「規範起業家」³としての試みを、情報の自由な流通や表現の自由等を含む既存の国際法の適用を重視する米国等の「規範守護者」⁴が阻むことで、プロセスが複雑化してきたことを論じる。また、フランスが非国家主体と連携する形で、複雑さの解消に向けた役割を果たしつつある点も指摘し、こうした調整者の機能の分析が今後の研究課題となることを述べる。本研究は、論点や関与するアクターが多様かつ現在進行中の規範形成プロセスの一端を考察するにとどまるが、コンストラクティビズム研究の射程をサイバー空間という新たな事例にも広げるところに意義がある。

サイバー空間をめぐる国際規範というテーマは、多様に研究されてきた。例えば、規範が論争化してきた歴史的背景や推移を記述する論考⁵、既存の国際法の適用方法等を議論する論考⁶、国際レジーム論の観点からサイバー空間のガバナンスを考察する論考⁷がある。また、それらの議論の射程外にある、規範の形成や伝播のプロセス、そこでのアクターの活動や戦略に着目する研究も一部にあり、規範ライフサイクル・モデル(後述)や規範起業家の役割が論点となっている⁸。しかし、規範守護者や調整者といった、コンストラクティビズム研究で注目されてきたその他のアクターにも着目した分析視角を取り入れた研究は見当たらず、議論の余地を残す。

そこで本稿では、まず次節で、サイバー空間での規範形成プロセスを捉える分析視角を示すべく、規範起業家、規範守護者、そして調整者の活動や戦略に着目するコン

3 Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52, no. 4 (Autumn 1998), pp. 896–899.

4 足立研幾「新たな規範の伝播失敗——規範起業家と規範守護者の相互作用から——」『国際政治』176号(2014年3月)1–13頁。

5 例えば次を参照。土屋大洋『サイバークレートゲーム——政治・経済・技術とデータをめぐる地政学——』(千倉書房、2020年)131–156頁; 土屋大洋「サイバースペース——深刻化するセキュリティと決定力を欠くガバナンス——」西谷真規子、山田高敬編著『新時代のグローバル・ガバナンス論——制度・過程・行為主体——』(ミネルヴァ書房、2021年)315–324頁。

6 例えば次を参照。Michael N. Schmitt, ed., *Tallin Manual on the International Law Application to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Center of Excellence* (New York: Cambridge University Press, 2013).

7 Joseph S. Nye, Jr., "The Regime Complex for Managing Global Cyber Activities," *Global Commission on Internet Governance Paper Series*, no. 1, May 2014, https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.

8 Tim Maurer, "Cyber Norm Emergence at the United Nations: An Analysis of the UN's Activities Regarding Cyber-security," *Belfer Center for Science and International Affairs Harvard Kennedy School Discussion Paper*, September 2011, <https://www.belfercenter.org/sites/default/files/files/publication/maurer-cyber-norm-dp-2011-11-final.pdf>; Martha Finnemore and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity," *The American Journal of International Law* 110, no. 3 (July 2016).

ストラクティビズムの既存研究を整理する。続く第2節で、国連内外の主たるプロセスを通時的に事例研究する。具体的には、GGE、OEWG、ロンドン・プロセス、サイバー空間の安定性に関するグローバル委員会（GCSC⁹）、パリ・コールを取り上げる。そして第3節で、プロセスが複雑化してきた要因を、規範起業家たるロシアと規範守護者たる米国等の戦略の相互作用に着目して分析する。最後に、本研究の結果をまとめるとともに、調整者の役割への着目が今後の研究課題になることを述べる。なお事例研究に際しては、国連の議事録や報告書といった一次資料と、歴史的事実等を記述した二次資料を用いる。

1. 規範形成プロセスを捉える分析視角

コンストラクティビズム研究では、新しい規範の形成や伝播を担う規範起業家の存在が注目されてきた。しかし研究が進むにつれて、規範起業家の試みに対抗して既存の規範を守ろうとする規範守護者や、規範形成プロセスが複雑化した際の調整者の役割も注目されるようになった。以下で、この3つのアクターの活動や戦略について述べる。

（1）規範起業家

規範起業家は、新たな規範の形成や伝播において重要な役割を果たすアクターを指す¹⁰。規範の形成や伝播に関する代表的なモデルである規範ライフサイクル・モデルでは、規範起業家によって規範が生成される段階、規範が急速かつ広く受け入れられる段階、規範が当然のものとして内面化する段階が示されている¹¹。そして、規範起業家の活動や戦略に関する研究が進められてきた。例えば規範起業家は、規範を作り出したい 이슈に他のアクターの注意を引きつけたり、イシュー自体を自ら作り出したりすることで、問題の所在を示す「フレーミング」を行う¹²。フレームは、その問題に対して誰がどのように対処していくべきかを示す¹³。それは粘着性がある、除去が難しい故に、その後の規範形成や伝播に大きく影響するものとなる¹⁴。

9 Global Conference on Cyberspace の略称。

10 規範起業家については次を参照。Finnemore and Sikkink, “International Norm Dynamics and Political Change,” pp. 896–899; Finnemore and Hollis, “Constructing Norms for Global Cybersecurity,” pp. 446–453; 足立研幾「新たな規範の伝播失敗」2–4 頁。

11 Finnemore and Sikkink, “International Norm Dynamics and Political Change,” pp. 894–909.

12 Ibid., p. 897.

13 Finnemore and Hollis, “Constructing Norms for Global Cybersecurity,” p. 447.

14 Ibid.

また、規範起業家は「接ぎ木」と呼ばれる戦略を実行する¹⁵。自らが提唱する新たな規範を、広く受け入れられつつある既存の規範や組織に結びつけることで、他のアクターからの支持を得やすくしようとするのである。この戦略によって、新しい規範は「正統性のオーラ (aura of legitimacy)」¹⁶をまとうことが期待される。

他のアクターを取り込むための規範起業家の手段としては、インセンティブ付与、説得、社会化もある¹⁷。インセンティブ付与とは、規範起業家が、他のアクターに報酬や罰を与えることで、自らが提唱する規範を広げようとする手段を指す。説得とは、規範起業家が提唱する規範への支持を他のアクターに依頼したり、その規範がいかに正当であるかを示す手段である。また規範起業家は、社会化のプロセスを巧みに利用し得る。例えば、アクターがある集団に属そうとしていて、当該アクターはその集団で重視されている規範に、その内容の是非とは関係なく、適合しようとする場合を想定する。こうした場合、規範起業家は、何が重視すべき規範であるかを示したり、当該規範に適合しようとするアクターに技術的な支援を講じる、といった方法を通じて、自らにとって望ましい規範を伝播することが期待できる。

こうした活動や戦略をとる規範起業家にとって、自らの取組を推進する舞台、すなわち組織的プラットフォームも重要になる¹⁸。その一例として、アンリー・デュナン(Henry Dunant)が、戦場での負傷者と病人を敵味方の区別なく救護するという規範を作り出すべく、赤十字国際委員会を新設したことが挙げられる¹⁹。このように、新たに組織が設けられることもあれば、既存の組織に結びつける接ぎ木戦略を用いて、規範の形成や伝播が試みられることもある²⁰。

(2) 規範守護者

規範守護者は、規範起業家の戦略に対抗することで、新たな規範の形成や伝播を阻み、既存の規範を擁護しようとするアクターを指す²¹。規範守護者が注目されるよう

15 Richard Price, "Reversing the Gun Sights: Transnational Civil Society Targets Land Mines," *International Organization* 52, no. 3 (Summer, 1998), p. 617, pp. 627–631. 「接ぎ木」に関しては、既存の規範が具体的にどのようなもので、新たな規範といかに共鳴するのかに意識的である必要性が指摘されている。この点については次を参照。政所大輔、赤星聖「コンストラクティビズム研究の先端——規範のライフサイクル・モデルを超えて——」『神戸法学雑誌』67巻2号(2017年9月)157–158頁。

16 Finnemore and Hollis, "Constructing Norms for Global Cybersecurity," p. 468.

17 これらの手段については次を参照。Ibid., pp. 449–453.

18 Finnemore and Sikkink, "International Norm Dynamics and Political Change," pp. 899–901.

19 Finnemore and Hollis, "Constructing Norms for Global Cybersecurity," p. 448.

20 Ibid.

21 規範守護者については次を参照。Alan Bloomfield, "Norm Antipreneurs and Theorising Resistance to Normative Change," *Review of International Studies* 42, no. 2 (2016), pp. 310–333; 足立「新たな規範の伝播失敗」1–13頁。なお、規範起業家に対抗するアクターは、足立論文では規範守護者(norm protector)、ブルームフィールド論文では規範アンチプレナー(norm antipreneur)と表現されている。本稿では、足立の研究に基づき、規範守護者と表現する。

になった背景には、従前の研究が、規範起業家の活動や戦略を焦点に、規範の伝播が成功した例に偏重してきたことに対する批判がある。規範守護者の活動や戦略に着目する研究は、そうすることで、規範起業家による規範の伝播が失敗した事例にも研究の射程を広げて、規範形成プロセスへの理解をより深めようとしたのである。

規範守護者は既存の規範を守るべく、規範起業家の試みに対して「フレーミング破壊」や「接ぎ木の切断」といった戦略をとる²²。フレーミング破壊とは、例えば、「核兵器問題を人道の観点からフレーミングし、『核兵器を廃絶すべき』と訴える規範起業家」の試みを、規範守護者が「人道の観点からフレーミングしてその是非を論ずることは不適切であると訴え」て阻もうとするような戦略である²³。また、接ぎ木の切断とは、例えば、対人地雷禁止規範という既に広く受け入れられつつある規範に接ぎ木することで、クラスター弾禁止の規範に正統性を持たせようとする規範起業家に対して、「クラスター弾と対人地雷の相違を強調」して、その試みを阻む戦略を指す²⁴。さらに、規範守護者は、規範起業家が自らの提唱する新たな規範に正統性を持たせようとするための先例の蓄積を阻止したり、拒否権プレーヤーの立場を活かして規範起業家の試みを阻むといった行動に出る²⁵。

こうした戦略をとる規範守護者の立場は、既存の規範が広く受け入れられている程、規範起業家に対して優位になるとの想定もある²⁶。他方、危機や構造的変化といった既存の規範を揺るがすような事態は、規範起業家に新たな規範を提唱・推進する機会を与えて、規範守護者は守勢に転じ得る²⁷。

(3) 調整者

規範形成プロセスは他のプロセスとの間で、競合や相互補完性、あるいは相乗性といった関係性を持ち得る²⁸。そうした関係性を調整する、いわば調整者の役割もコンストラクティビズム研究で注目されてきた。例えば規範起業家は、自らが提唱する新たな規範と、競合する他の規範とを調整する役割を果たす場合がある²⁹。理論上は、規範守護者が調整者となって、既存規範と、規範起業家が提唱する新たな規範との関係性の構築を図ることも考えられよう。

22 足立「新たな規範の伝播失敗」3-4頁。

23 同上、3頁。

24 同上、4頁。

25 Bloomfield, "Norm Antipreneurs and Theorising Resistance to Normative Change," pp. 324-326.

26 Ibid., p. 312.

27 Ibid., p. 332.

28 西谷真規子「国際規範とグローバル・ガバナンスの複合的発展過程」、西谷真規子編著『国際規範はどう実現されるか—複合化するグローバル・ガバナンスの動態—』（ミネルヴァ書房、2017年）8-9頁。

29 政所、赤星「コンストラクティビズム研究の先端」159頁。

また調整は、オーケストレーターと呼ばれるアクターによって行われる場合もある。ガバナンスの手法には、オーケストレーションという「指針や原則等のソフトローとソフトな誘因（説得・交渉・支援等の非強制的手段）を多用して、多様な関係者の利害を調整し目標へと誘導する」手法がある³⁰。近年、この概念をより精緻化したオーケストレーション・モデルが提起されており、オーケストレーターが、目的を共有する中間組織を用いて、対象となるアクターに働きかけて調整を行う状況が想定されている³¹。同モデルの特徴は、オーケストレーターが「中間組織の自発性に依存した非強制的な手段を用いて、間接的に目標達成しようとする点」にある³²。

以上、コンストラクティビズム研究から示される、規範起業家、規範守護者、調整者の役割に着目した分析視角を念頭に置きつつ、次節以降、サイバー空間の規範形成プロセスに関する事例を通時的に記述した上で、プロセスが複雑化してきた要因を分析する。

2. サイバー空間の規範形成プロセスの多様化

サイバー空間のガバナンス、そこでのアクターの役割や責任ある行動の在り方に関して、主要な規範形成プロセスとなってきたのは国連である³³。その端緒となったのは、ロシアによる決議案「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展」の国連総会での採択（1998年12月）³⁴であった。

ロシアによれば、この提案は次の理由からなされた³⁵。すなわち、情報通信技術の発展は「情報兵器（information weapon）」の軍拡競争を招き、兵器がテロや犯罪、軍事目的で使用されれば、大量破壊兵器並みの壊滅的な結果が生じ、国際的な安全や国家主権の平等、内政不干渉等の諸原則も脅かされる。こうした状況が懸念されるに

30 西谷真規子「多中心的なガバナンスにおけるオーケストレーション——腐敗防止規範をめぐる国際機関の役割——」西谷真規子編著『国際規範はどう実現されるか』203頁。

31 同上。

32 同上。

33 後述するように、国連での規範に関する議論は、国際法の具体的な適用方法と、法の欠缺を埋めるための規範の在り方という、2項目に細分化されている。もっとも、両項目ともサイバー空間でのアクターの責任ある行動の在り方を検討する点で同様であるため、本稿では、既存の国際法の適用に向けた取組も、新たな規範作りに向けた取組も、規範形成に向けた取組・プロセスとして総称する。

34 United Nations General Assembly (UNGA) Resolution 53/70, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/53/70 (4 January 1999), available from undocs.org/A/RES/53/70.

35 UNGA, *Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Secretary-General*, A/54/213 (10 August 1999), available from undocs.org/A/54/213.

もかわらず、既存の国際法では情報兵器の開発や使用を規制し難いため、国際的な法的文書（multilateral international legal instrument）の策定も視野に入れた取組が必要だと、ロシアは訴えた。こうした主張の背景には、米国等の優れた情報通信技術力が自国の安全保障を脅かし得ることに対するロシアの危惧があったといえる。

さらに注目されるのは、ロシアが、国家主権や内政不干渉等の原則を強調した点である。決議案が提出された当時、ロシアはアジア通貨危機の影響も受けて深刻な財政危機に陥っていた。そのため、技術発展が促す情報の自由な流通は、ロシアにとって、国内政治をより不安定化させかねない懸念材料であったことは想像に難くない。だからこそロシアは、国家が情報通信を管理し、国外からの干渉も排除できるような新たな法的枠組みを求めたのであり、この姿勢は現在も一貫している³⁶。国家の役割を重視するロシアにとって、国家が中心となって機能する国連は、まさにルール作りの舞台として相応しい場であった。

他方、米国等はロシアの取組に対して消極的な態度を示した³⁷。具体的にはまず、ロシアが決議案で用いた「情報セキュリティ（information security）」という言葉が、国家による情報通信の検閲を含意し、表現の自由や情報の自由な流通を脅かしかねないことを欧米諸国は懸念した。さらに、米英は、国家による軍事分野での情報通信技術の活用が生む問題は、武力紛争法の適用に関わる問題だと主張した³⁸。すなわち両国は、新たな条約等の策定ではなく、既存の国際法の適用を検討すべきとの立場をとった。また、米英は、国家よりもテロリストや犯罪者が情報通信技術を悪用することの方が脅威だと訴えて、この問題に対処するための取組が既に国連外で、例えば欧州評議会でのサイバー犯罪条約のように進んでいることも主張した³⁹。米国等は、国家による情報通信の統制はもとより、その技術の国家による利活用も規制し得る点も問題視して、ロシア案を拒否したことが分かる。

米国のロシアの取組に対する態度は、際立って厳しかった。国連を舞台とする規範形成プロセスに関して米国は、既存の活動を妨げかねない取組を国連が講じることは

36 Elaine Korzak, "Russia's Cyber Policy Efforts in the United Nations," *Tallinn Paper*, NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE), No. 11 (2021), p.17, https://ccdcoe.org/uploads/2021/06/Elaine_Korzak_Russia_UN.docx.pdf.

37 2000年代前半にみられた、サイバー空間の規範形成に向けた国連でのロシアと欧米諸国の角逐については次を参照。Eneken Tikk-Ringas, "Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012," *ICT4Peace Cyber Policy Process Brief*, 2012, pp. 4-5, <https://ict4peace.org/wp-content/uploads/2012/08/Eneken-GGE-2012-Brief.pdf>.

38 UNGA, *Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Secretary-General*, A/59/116/Add.1 (28 December 2004), p. 4, available from undocs.org/A/59/116/Add.1; UNGA, *Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Secretary-General*, A/59/116 (23 June 2004), p. 11, available from undocs.org/A/59/116.

39 A/59/116/Add.1, pp 3-4; A/59/116, pp. 11-12.

「極めて賢くない (highly unwise)」と訴えた⁴⁰。米国の頑なな態度は、ロシアの決議案に対する投票行動にも現れた。ロシアは1998年以降、毎年、内容を修正しながら先の決議案を提出し、2001年版には、国連での検討を支援する組織として国連第1委員会の下にGGEを2004年に設置することも盛り込み⁴¹、いよいよ議論を本格化させようとした。こうしたロシアの動きに対して唯一米国だけが、2005年から2008年にかけて決議案に反対票を投じた⁴²。

しかし米国の態度は2009年以降一転し、2010年にはロシアの決議案の共同提案国にすらなった⁴³。この時期、ロシアの関与が疑われるサイバー攻撃が、エストニア(2007年)、ジョージア(2008年)と続いた。また米国でも、中国の関与が疑われるサイバースパイ活動によってF-35戦闘機に関する情報流出が発生したとされる(2007年)など、様々な被害が報告されていた⁴⁴。こうした状況を受けて、米国としても、ロシアが求める方向での新たなルール作りには反対しつつも、サイバー空間での国家の責任ある行動に関して、既存の国際法の適用や法の欠缺を埋めるような規範の形成に向けた取組の必要性に対する認識を強めたと考えられる。折しも米国では、2009年1月、サイバーセキュリティとその国際的な議論への関与に関心を示すバラク・オバマ(Barack Obama)政権が発足したタイミングでもあった。

米国の政策転換は国連での議論の活発化を促し、GGEでの取組も次第に成果を生み始めた。そもそもロシアの呼びかけで2004年から2005年まで、米英仏露中を含む15か国が参加⁴⁵して開かれたGGE第1会期は、参加国のコンセンサスによって公表される仕組みになっている報告書の公表には至らなかった。しかし、2009年から2010年にかけての第2会期で、GGEは初めて報告書の公表に成功し、規範に関する議論の継続が確認された⁴⁶。さらに2012年から2013年に開かれた第3会期では、サ

40 UNGA, *Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Secretary-General*, A/54/213 (10 August 1999), p. 13, available from undocs.org/A/54/213.

41 UNGA Resolution 56/19, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/56/19 (7 January 2002), available from undocs.org/A/RES/56/19.

42 “Voting Data,” UN Digital Library, <https://digitallibrary.un.org/search?ln=en&cc=Voting+Data&p=Developments+in+the+Field+of+Information+and+Telecommunications+in+the+Context+of+International+Security&f=&rm=&ln=en&sf=year&so=d&rg=50&c=Voting+Data&c=&of=hb&fti=0&fti=0>.

43 UNGA, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/C.1/65/L.37 (15 October 2010), available from undocs.org/A/C.1/65/L.37.

44 これまでの主要なサイバー事案については、次を参照。“Significant Cyber Incidents Since 2006,” Center for Strategic and International Studies (CSIS), https://csis-website-prod.s3.amazonaws.com/s3fs-public/211217_Significant_Cyber_Events.pdf?crRc3OVYs1hgHthZyNSwL7bW.Ey30S1G.

45 GGEの参加国は、米英仏露中の常任理事国5か国の他、会合ごとに各地域から衡平に選出される国によって構成されている。

46 UNGA, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General*, A/65/201 (30 July 2010), available from undocs.org/A/65/201.

イバー空間に「国際法、特に国連憲章が適用可能 (applicable)」であることが報告書に明記された⁴⁷。欧米諸国はサイバー空間への既存の国際法の適用を強く求めており、そうした内容が報告書に盛り込まれたことを米国も評価した⁴⁸。

この結果を受けて GGE での議論は、法の欠缺部分を埋めるような規範の在り方と、既存の国際法の適用方法とに細分化されることになった。そして前者に関しては、参加国数を 20 か国に拡大して開催された 2014 年から 2015 年の第 4 会期の報告書で、11 項目からなる規範・ルールへの提示に成功した⁴⁹。国連総会は 2015 年 12 月、加盟国がこの第 4 会期の報告書に沿う (to be guided) ことを要請 (calls upon) する決議も採択している⁵⁰。

一方、既存の国際法の適用方法については、欧米諸国と露中等との見解の隔たりは大きく、議論は難航した。2016 年から 2017 年に参加国を 25 か国に拡大して開かれた GGE 第 5 会期は、国際人道法や自衛権の適用の在り方といった点で見解がまとまらず、再び報告書を公表できなかった⁵¹。米国は「明確かつ直接的に」国際法の適用の仕方を示そうと試みたが⁵²、露中を含む一部の国は、そうした試みはむしろサイバー空間上での事案に仮託した軍事的活動を正当化しかねないとして反対したのである⁵³。欧米諸国にとっては、ロシアが関与したとされる、2016 年米国大統領選挙時のサイバー攻撃や世界中に被害をもたらしたノットペーチャ (NotPetya) 事案が発生する中、既存の国際法の適用を精緻化し、必要な措置を講じられるようにすることは喫緊の課題であった⁵⁴。他方、露中にとっては、サイバー攻撃に対する通常戦力による自衛権行

47 UNGA, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General*, A/68/98 (24 June 2013), available from undocs.org/A/68/98.

48 Jen Psaki, "Statement on Consensus Achieved by the UN Group of Governmental Experts on Cyber Issues," United States (US) Department of State, June 7, 2013, <https://2009-2017.state.gov/r/pa/prs/ps/2013/06/210418.htm>.

49 UNGA, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General*, A/70/174 (22 July 2015), available from undocs.org/en/A/70/174.

50 UNGA Resolution 70/237, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/70/237 (30 December 2015), available from undocs.org/A/RES/70/237.

51 Ann Väljataga, "Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly," NATO CCDCOE, January 9, 2017, <https://ccdcoe.org/incyber-articles/back-to-square-one-the-fifth-un-gge-fails-to-submit-a-conclusive-report-at-the-un-general-assembly/>.

52 Michele Markoff, "Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Tele," US Mission to the UN, June 23, 2017, <https://usun.usmission.gov/explanation-of-position-at-the-conclusion-of-the-2016-2017-un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-tele/>.

53 Michael Schmitt, "The Sixth United Nations GGE and International Law in Cyberspace," Just Security, June 10, 2021, <https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/>.

54 Michael Schmitt, "The Defense Department's Measured Take on International Law in Cyberspace," Just Security, March 11, 2020, <https://www.justsecurity.org/69119/the-defense-departments-measured-take-on-international-law-in-cyberspace/>.

使が認められることになれば、米国優位な通常戦力の不均衡の是正に資するサイバー攻撃の利点が損なわれ得る点で、また、軍民を区別することを義務付ける国際人道法の適用もサイバー攻撃能力の向上を妨げ得る点で問題であった⁵⁵。

確かにロシアは、GGE 第3会期で国際法の適用可能性を示した報告書を支持したが、それはあくまで国家主権の尊重という文脈でのことであり、欧米諸国が求めるような精緻な適用に対しては消極的であった⁵⁶。このことはロシアが、中国、タジキスタン、ウズベキスタンとともに、第3会期 GGE に先駆けた 2011 年 9 月に国連に提出した「情報セキュリティのための国際行動規範」⁵⁷からも読み取れる。行動規範では、国連憲章に則ることや、人権や基本的自由の尊重が言及されつつも、全体的な趣旨はサイバー空間での国家主権を重視するものであった。その後、行動規範は、カザフスタンとキルギスも提案国に加えた上での修正版も 2015 年 1 月に国連に提出された。修正版には、「オフライン環境での個人の権利は、オンライン環境でも保護されなければならない」といった、欧米諸国からの支持も得られるような文言が追加されたが、国家の役割に重きを置く内容に変わりはない⁵⁸。

こうした中、国連外ではウィリアム・ヘーグ (William Hague) 英外相 (当時) の呼びかけで、2011 年 11 月にサイバー空間に関するロンドン会議が開催されるという動きがあった。この国際会議はその後、ハンガリーのブタペスト (2012 年)、韓国のソウル (2013 年)、オランダのハーグ (2015 年)、インドのデリー (2017 年) と続き、一連の取組はロンドン・プロセスと称された。その大きな特徴は、GGE 等の既存の取組に基づきつつも、多様なアクターが参加するマルチ・ステークホルダー形式とし、多様な観点から規範の在り方等を議論する場を提供した点にあった。

ロンドン・プロセスは既存の取組に基づくものとはいえ、国家中心の国連を舞台とした規範形成プロセスとは一線を画するものであり、両者の間には一定の緊張関係があった。実際、ロシアや中国からのロンドン・プロセスへの参加者は、サイバー空間での国家主権の尊重や行動規範に基づく議論の必要性を主張し、国連こそが問題を討議する最適な場であることを強調した⁵⁹。なおロンドン・プロセスは、デリー会議後、

55 Arun M. Sukumar, "The UN GGE Failed. Is International Law in Cyberspace Doomed as Well?" Lawfare, July 4, 2017, <https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well>.

56 Korzak, "Russia's Cyber Policy Efforts in the United Nations," p. 16.

57 UNGA, *International Code of Conduct for Information Security*, A/66/359 (14 September 2011), available from undocs.org/A/66/359.

58 UNGA, *International Code of Conduct for Information Security*, A/69/723 (13 January 2015), available from undocs.org/A/69/723.

59 外務省「サイバー空間に関するブタペスト会議」(平成 24 年 10 月 10 日)、https://www.mofa.go.jp/mofaj/gaiko/soshiki/cyber/cyber_1210.html; 外務省「サイバー空間に関するソウル会議」(平成 25 年 10 月 22 日)、https://www.mofa.go.jp/mofaj/gaiko/page18_000084.html。

主催国が決まらず取組は止まった状態にある⁶⁰。

3. サイバー空間の規範形成プロセスの複雑化

動きを停滞させたロンドン・プロセスではあるが、その系譜に連なる新たなプロセスとして、サイバースペースの安定性に関するグローバル委員会（GCSC）が出現した。GCSCはロンドン・プロセスのハーグ会議を経た2017年に、オランダ政府が支援して設立された有識者会議であり、サイバー空間の規範を議論する新たな場となった⁶¹。GCSCは、11項目からなる規範を示したGGE等の既存の取組を踏まえつつ、インターネットの公共的な核心（public core of internet）の保護や選挙プロセスの保護といった新たな要素を含む規範を示すなど、具体的な成果を収めた⁶²。加えてGCSCは、規範形成プロセスにおける非国家主体の能動的関与を促す取組であった点でも意義あるものであった。そのGCSCは、2019年11月に最終報告書を公表して取組に1つの区切りをつけた。

GCSCの最終報告書が公表されたのは第2回パリ平和フォーラムであったが、前年にあたる2018年11月の第1回フォーラムでも、規範形成プロセス上の注目すべき出来事があった。同フォーラムと平行して開催されたインターネット・ガバナンス・フォーラム（IGF）⁶³で、エマニュエル・マクロン（Emmanuel Macron）仏大統領が、サイバー空間の信頼性と安全性の確保を目指すパリ・コールを提唱したのである。パリ・コールは、既存の国際法の適用や欧州評議会で策定されたサイバー犯罪条約の重要性を確認しつつ、全てのステークホルダーが順守すべき9つの原則を示した⁶⁴。原則には、保護する対象として個人やインフラ、インターネットの公共的な核心、選挙プロセスが挙げられており、GGEやGCSCの成果を反映したものとなっている。80の国、露中系を含む706の企業と390の市民団体等が賛同を表明（2021年12月時点）してい

60 土屋『サイバークレートゲーム』134頁。

61 GCSCは、ロンドン・プロセスの他に、カナダのセンター・フォー・インターナショナル・ガバナンス・イノベーション（CIGI）と英国のチャタム・ハウス（Chatham House）が2014年1月に協力して立ち上げたインターネットガバナンス・グローバル委員会（GCIG）の系譜も汲む。GCSC設立の背景は次を参照。GCSC, “Advancing Cyberstability: Final Report,” GCSC, November, 2019, pp. 46–47, <https://cyberstability.org/wp-content/uploads/2020/02/GCSC-Advancing-Cyberstability.pdf>.

62 GCSC, “Advancing Cyberstability.”

63 Internet Governance Forumの略称。IGFは、主にインターネットのガバナンスを議論する場として設けられたフォーラムである。設立の経緯については次を参照。一般社団法人日本ネットワークインフォメーションセンター（JPNIC）「IGFとは（Internet Governance Forum）」（2011年3月）、<https://www.nic.ad.jp/ja/newsletter/No47/0800.html>.

64 “The 9 Principles,” Paris Call: For Trust and Security in Cyberspace, November 12, 2018, <https://pariscall.international/en/principles>.

るパリ・コールは、国家のみならず、非国家主体も巻き込んだ取組となっている⁶⁵。

GCSC とパリ・コールは、その内容はもとより、国連外の規範形成プロセスにおいて欧州諸国が重要な役割を果たしてきたことを示す点で興味深い。特に近年、フランスが存在感を高めていることは注目に値する。

一方、時期を同じくして、国連内でも大きな変化があった。GGE 第5会期が報告書の公表に至らず、議論は次なる GGE に持ち越されるものと考えられた中、2018年10月、ロシアは中国等とともに OEWSG という新たな会合の設置を求める決議案を提出したのである⁶⁶。OEWSG は GGE とは異なり、国連全加盟国の本会合への参加を認め、さらに企業や非政府組織、学術界等の非国家主体も参加できる会期間会合も設ける点を特徴とした。ロシア案は2018年12月の国連総会での表決の結果、欧米や日本を含む46か国が反対するも、119か国が賛成し、採択された⁶⁷。

これに対して欧米諸国は、2018年10月に「国際安全保障の文脈におけるサイバー空間での責任ある国家の行動の進展」と題した決議案を示して、GGE 第6会期開催を推進した⁶⁸。これまで GGE 設置に関する決議の題目は、1998年のロシアの決議案のタイトルである「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展」を受け継いできた。今般、欧米諸国が敢えてタイトルを変えたところに、露中との角逐が現れていた。欧米諸国が提案した第6会期は、これまでの GGE とは異なり、欧州連合や ASEAN 地域フォーラムといった地域機構との対話、並びに国連全加盟国を交えた非公式会合も実施することで門戸を広く開く工夫を施した点を特徴とした。この決議案も2018年12月の国連総会で表決され、露中を含む12か国が反対したものの、欧米や日本を含む138か国が賛成し、採択された⁶⁹。

その結果、国連には GGE と OEWSG の二重プロセスが登場した。これは、次の2点で興味深い出来事であった。1つは、もともと国連での議論に消極的であった米国が、今や GGE 推進に転じたことである。既存の国際法の適用を重視する米国にとって、このことを明記した報告書の公表に成功した GGE は重要な規範形成プロセスになっている。2つ目は、参加国が限定される国家中心の GGE を欧米諸国が推進し、マルチ・ステークホルダー協力に資する OEWSG を露中等が推進するという、ねじれ現象が生

65 “Paris Call: For Trust and Security in Cyberspace,” Paris Call, <https://pariscall.international/en/>.

66 UNGA, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/C.1/73/L.27/Rev.1 (29 October 2018), available from undocs.org/A/C.1/73/L.27/Rev.1.

67 UNGA Resolution 73/27, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/73/27 (11 December 2018), available from undocs.org/en/A/RES/73/27.

68 UNGA, *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/C.1/73/L.37 (18 October 2018), available from undocs.org/A/C.1/73/L.37.

69 UNGA Resolution 73/266, *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/RES/73/266 (2 January 2019), available from undocs.org/A/RES/73/266.

じたことである。OEWG の会期間会合は 2019 年 12 月、110 以上の非国家主体が参加して開催され、先述の GCSC も参加、議論の成果を国連の規範形成プロセスにインプットする好機を得た⁷⁰。

二重プロセスは相互補完的な機能の発揮が期待されたが、実際には規範形成に向けた取組を煩雑、非生産的にしかねない状況が続いた。2019 年、米露は前年の決裂状態を回避する道を検討したが調整はつかず⁷¹、やはり 2 つの決議が総会で採択された⁷²。翌年も同様の状況となった。ロシアは中国等とともに、早くも OEWG 第 2 会期（2021 年～2025 年）開催を盛り込んだ決議案を提出し⁷³、2020 年 12 月の総会でその採択にこぎ着けた⁷⁴。他方、欧米諸国は、OEWG や GGE 第 6 会期での議論が続いている中でのこの動きに反対し、議論の結果をまって今後の取組を決めるべきとする決議案を提出⁷⁵、こちらも総会で採択された⁷⁶。

こうした状況を受けて、二重プロセスに代わる第 3 の選択肢を示すべく、OEWG では「行動プログラム (POA)」⁷⁷ 導入が、フランスを筆頭とする幾つかの国の連名で提案された。POA は、国連でこれまでも小型武器や差別、ヘイトスピーチといった分野で設けられてきた方式であり、コンセンサスが得られる事項から協力を進めようとする、法的拘束力はないながらも政治的拘束力は期待される枠組みを指す⁷⁸。フランスらはこの枠組みをサイバー空間にも設けることで、これまでの GGE 等で合意済みの事項から実践を図ろうとしたのである。

70 “Global Commission to Host Lunch Session During UN Open-ended Working Group Intersessional Consultative Meeting,” GCSC, November 22, 2019, <https://cyberstability.org/news/global-commission-to-host-lunch-session-during-un-open-ended-working-group-intersessional-consultative-meeting/>.

71 UNGA, *Official Record*, A/C.1/74/PV.25 (6 November 2019), pp. 11–12, available from undocs.org/A/C.1/74/PV.25.

72 米国の草案に基づく決議は、UNGA Resolution 74/28, *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/RES/74/28 (18 December 2019), available from undocs.org/A/RES/74/28. ロシアの草案に基づく決議は、UNGA Resolution 74/29, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/74/29 (18 December 2019), available from undocs.org/A/RES/74/29.

73 UNGA, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/C.1/75/L.8/Rev.1 (26 October 2020), available from undocs.org/en/A/C.1/75/L.8/Rev.1.

74 UNGA Resolution 75/240, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/75/240 (4 January 2021), available from undocs.org/en/A/RES/75/240.

75 UNGA, *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/C.1/75/L.4 (5 October 2020), available from undocs.org/en/A/C.1/75/L.4.

76 UNGA Resolution 75/32, *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/RES/75/32 (16 December 2020), available from undocs.org/en/A/RES/75/32.

77 Programme of Action の略称。“The future of discussions on ICTs and cyberspace at the UN,” UN Office for Disarmament Affairs Open-ended Working Group, December 2, 2020, <https://front.un-arm.org/wp-content/uploads/2020/12/joint-contribution-PoA-future-of-cyber-discussions-at-the-un-2-2-2020.pdf>.

78 POA には定まった仕組みはないが、既存のものは概ね、協力事項の実行状況を確認する作業部会と、POA の有効性の評価等を行うレビュー部会とで構成され、その過程では非国家主体とも連携し、また必要に応じて国連総会に新たな会合の設置を求めたりするとされる。この点については次を参照。Aude Géry and François Delerue, “A New UN Path to Cyber Stability,” *Directions: Cyber Digital Europe*, October 6, 2020, <https://directionsblog.eu/a-new-un-path-to-cyber-stability/>.

その後、OEWGと第6会期GGEはそれぞれ報告書の公表には成功した。OEWGの報告書では規範に関して、従前のGGEの成果に加えて、「インターネットの一般的な可用性と完全性を確保する」として、インターネットの公共的な核心の保護を求めたGCSCやパリ・コールの成果も間接的ながら盛り込まれた⁷⁹。さらにPOAについても、OEWG第2会期で更に検討していく方針が示された⁸⁰。またGGEの報告書では、OEWGの成果も踏まえつつ、国際法の適用に関しては議論を進展させて、「武力紛争時のみ」と限定しつつも国際人道法の適用が明記された⁸¹。第5会期GGEが国際人道法の適用の在り方を1つの課題として報告書の公表に至らなかったことを踏まえれば、第6会期は大きな成功を収めたといえる。もっとも、二重プロセスの展望は、POAの動向も含めて依然として不透明である。

4. 規範形成プロセスの複雑化の要因分析

なぜ、サイバー空間をめぐる規範形成プロセスは複雑化してきたのか。確かに、そもそも論点とステークホルダーが多様であるため、プロセスは自ずとレジーム・コンプレックス⁸²状態にならざるを得ない。とはいえ、国際的な規範を作り出そうとしながらも、そのための検討の場すら流動的な現状からは、プロセスの錯綜状態が印象付けられる。さらには、ロシアがマルチ・ステークホルダー協力を体現するOEWGを、米国が国家中心のGGEを推進する、ねじれ現象が生じたことも興味深い。本節では複雑化の要因を、第1節で示した分析視角のうち、規範起業家と規範守護者の活動や戦略に着目して分析する。

サイバー空間において、国家の役割に重きを置いた新たな規範形成を目指して国連での規範形成プロセスを推進してきたロシアは、規範起業家と位置づけられる。規範起業家たるロシアは、次のようなフレーミングを行った。まず、ロシアは他国の注意を喚起すべく、決議案「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展」を継続的に提出した。そして、情報通信技術の発展が国際的な安全や国家主権等の諸原則にとって新たな脅威をもたらしており、既存の国際法では対処しきれないため新

79 UNGA, *Final Substantive Report*, A/AC.290/2021/CRP.2 (10 March 2021), para. 26, <https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf>.

80 A/AC.290/2021/CRP.2, para. 77.

81 “Advance Copy: Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security,” UN Office for Disarmament Affairs, 28 May, 2021, para. 71(f), <https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf>.

82 Nye, “The Regime Complex for Managing Global Cyber Activities.”

たな規範が必要だと、問題の所在を示した。加えて、国連を舞台とした取組とすることで、ロシアは規範形成プロセスへの参加者を国家に限定しようとしたのである。

ロシアによる行動規範の提起は、そうしたフレーミングをより具体化するとともに、他国の取り込みを図ろうとする取組であった。行動規範については、支持する国が限定されているため、取組上の意義を疑問視する見方もあるが⁸³、上海協力機構の加盟国、特に中国を巻き込むことで、ロシアの取組の地盤を着実に強化するものであったと見ることもできる。また、行動規範の提起は、条約といった法的拘束力を伴うハードローではなく、拘束力を伴わないソフトローでの規制も重視する最近のグローバル・ガバナンスの潮流を反映したものとも評されており⁸⁴、ロシアは規範起業家としての役割を巧みに果たそうとしてきたといえる。

さらに、ロシアは接ぎ木戦略も採用した。国連第1委員会へのGGE設置は、その好例である。国連という権威ある舞台を組織的プラットフォームとして利用することで、ロシアは正統性をもって規範の形成を進めようとした。さらに、ロシアが新たな規範形成を志向しつつ、第3会期GGEの報告書や行動規範の中で、既存の国際法、特に国連憲章との関連性に意識的であった点も接ぎ木戦略の一環と捉えられる。こうすることで、自国にとって望ましい規範形成に向けた取組に「正統性のオーラ」をまとうせようとしたと解せる。

こうしたロシアの取組に対抗してきた欧米諸国、特に米国は、規範守護者と位置付けられる。ロシアの取組に対して、当初米英が、武力紛争法の適用で事足りるため新たなルールは必要ないとの立場を示したことや、問題の焦点をテロや犯罪行為に局限しようとしたことは、両国によるフレーミング破壊戦略と解せる。加えて、米国は、国連を舞台にした取組が国連外での取組を妨げかねないことを理由にロシアの接ぎ木を切断しようとし、実際に2005年から2008年にかけてロシアの決議草案に反対票を投じた。

さらに、英国から始まったロンドン・プロセスもまた、規範守護者側の対抗戦略と捉えられる。マルチ・ステークホルダー形式を特徴とするロンドン・プロセスは、議論への参加者を国家に限定する国連のプロセスを相対化するとともに、論点も多様化させた点で、ロシアのフレーミングの破壊を試みるものであった。また、GGEとは異なる新たな組織的プラットフォームの構築は、ロシアの接ぎ木を切断する潜在的意義も有したのである。

83 Korzak, "Russia's Cyber Policy Efforts in the United Nations," pp. 7–8.

84 Mark Raymond, *Social Practices of Rule-Making in World Politics* (New York: Oxford University Press, 2019), p. 228.

もっとも 2000 年代半ばを過ぎると、米英はロシアの取組への対抗戦略の再検討を迫られた。国家の関与が疑われるサイバー攻撃の被害報告が増えるにつれて、国連での規範形成プロセスの正統性は高まった。米英等としても、ロシアが求める方向での新たなルール作りには反対しつつも、サイバー空間での国家の責任ある行動の在り方に関する議論を深める必要性に対する認識を強めた。また、米英は国連での取組に並ぶような組織的プラットフォームを作り出すことができなかった。その候補であったロンドン・プロセスはデリー会議以降、開催されていない。同プロセスの系譜に連なる GCSC も、GGE を代替するものではなかった。

とはいえ、米英によるロシアへの対抗が緩んだ訳ではない。むしろ特に米国は、既存の国際法のより精緻な適用を訴えることでロシアへの対抗を鮮明化させた。既存の国際法の適用に焦点を当てることは、新たな規範の必要性を主張するロシアに対するフレーミング破壊戦略となる。加えて、精緻な適用を追求することには、ロシアの接ぎ木戦略を妨げる意義もある。先述の通り、ロシアは自らの取組に正統性を持たせるべく、既存の国際法、特に国連憲章に接ぎ木する戦略を採用している。ここで注目すべきは、ロシアにとってこの戦略は、サイバー空間でも国家主権が尊重されるという文脈でのいわば「浅い」接ぎ木である限り有効だと考えられる点である。換言すれば、国際人道法や自衛権といった個別具体的な国際法の適用の在り方まで問うような「深い」接ぎ木は、ロシアにとって、望ましい規範形成に向けた取組のむしろ妨げになる。米国はまさにこのことを逆手に取り、接ぎ木を切断するのではなく、より深く接ぎ木することでロシアの戦略を無効化しようとしていると捉えられる。その米国にとって、GGE 第3 会期で既存の国際法の適用が確認されたことは大きな意味を持ち、米国はこの成果に接ぎ木して、GGE でより精緻に国際法の適用の在り方を検討しようとしている。規範起業家たるロシアが組織的プラットフォームとして作り出した GGE は、今や規範守護者たる米国のプラットフォームと化したのである。

だからこそロシアは、GGE に代わる新たな組織的プラットフォームを求め、OEWG を新設したと理解できる。ここでの注目点は、ロシアが OEWG という形式を選択したことである。OEWG は、2016 年に核軍縮交渉分野で、国連加盟国だけでなく、非国家主体も参加して開催された実績がある⁸⁵。この前例に接ぎ木し、参加国が限定されている GGE とは違い、多様なアクターの参加を広く認める枠組みとすることで、ロシアは新たなプラットフォームの設置に「正統性のオーラ」をまとうせようとしたようにみえる。そしてロシアは現在、OEWG 第2 会期の開催を早急に求め、こ

85 外務省「多国間核軍縮交渉の前進に関するオープン・エンド作業部会（OEWG）」（平成 28 年 9 月 27 日）、https://www.mofa.go.jp/mofaj/dns/ac_d/page25_000544.html。

の新たな組織的プラットフォームを根付かせようとしている。

もっとも OEWG が、ロシアにとって好ましいプラットフォームとして機能するかは予断できない。そもそも国家の役割を重視するロシアにとって、OEWG のプロセスに非国家主体が積極的に参加する状況は好ましくない。ロシアはあくまで、取組に正統性を持たせるとの目的の下に非国家主体の参加を認めているに過ぎないのであり、欧米諸国が重視するマルチ・ステークホルダー形式を受け入れた訳ではない⁸⁶。要するにロシアが採用した OEWG の設置という接ぎ木戦略は、既存の国際法への接ぎ木戦略と同様、その「浅さ」が要点となる。この点を逆手にとった規範守護者たる米国等が、非国家主体の OEWG への積極的参加を促す「深い」接ぎ木を追求し始めれば、規範起業家たるロシアの戦略は、GGE と同様に頓挫する可能性がある。ロシアが接ぎ木戦略を追求すればするほど、規範守護者たる米国等に対する戦略上の脆弱性が生まれる構図は、サイバー空間での規範形成プロセスの1つの特徴となっている。

おわりに

本稿では、コンストラクティビズムの分析視角からサイバー空間での規範形成プロセスを考察した。その結果、規範起業家たるロシアと規範守護者たる米国等の戦略の相互作用が、プロセスを複雑化してきたことが示された。参加国が限定される GGE を米国が求め、マルチ・ステークホルダー協力を具現化する OEWG をロシアが求めるという、ねじれが生まれた要因もこの相互作用に求められた。

この研究結果は、コンストラクティビズムの分析視角がサイバー空間での規範形成プロセスを論考するにおいても有効であることを示す。一部の研究では、プロセスのダイナミクスを生む要因として、ロシアの「持続的かつ一貫性がある、長期的な志向を持った」取組が論じられている⁸⁷。確かに、GGE や OEWG といった国連を舞台とする取組をけん引してきたロシアの取組は、プロセスの展開を説明するための重要な要因である。しかし、本研究が示したように、規範起業家たるロシアの取組は、規範守護者たる米国等の取組の対抗を受けて変化を余儀なくされてきた。この両者の角逐を捉えることなくして、プロセスのダイナミクスを把握することはできないのであり、ここにコンストラクティビズム研究の射程をサイバー空間という新たな事例にも広げる意義を見出せる。

86 Korzak, "Russia's Cyber Policy Efforts in the United Nations," pp. 18–19.

87 Ibid., p. 19.

そしてコンストラクティビズムに基づく分析視角の有効性は、規範起業家と規範守護者以外のアクターにも目を向けた更なる研究の必要性を示唆する。第1節で述べたように、コンストラクティビズム研究では、規範形成における調整者の役割も注目されている。実際、本稿の事例研究でも示されたように、近年フランスはパリ・コール提唱やPOAの導入提案を通じて、複雑化してきたプロセスの調整を図る姿勢を顕著にしている。フランスの取組の特徴は、パリ・コールやPOAといった法的拘束力に欠くソフトな手段を用いつつ、取組に賛同する国家や非国家主体の自発的な協力を通じて多様なアクターの利害調整を試みるところにあり、オーケストレーション・モデルを印象付けるものである。規範形成プロセスの動向は規範起業家と規範守護者との角逐という視点からだけでなく、調整者の機能、そこでの国家主体と非国家主体との連携といった点からも分析される必要があり、こうした研究を進めることが今後の研究課題となる。

（防衛研究所）

[付記] 本稿の完成にあたり、査読者の先生方から貴重な修正のご提案とご指導を頂いた。記して感謝申し上げたい。