NIDS 防衛研究所
The National Institute for Defense Studies

複雑化するサイバー規範プロセスの動向

原田　有　政策研究部グローバル安全保障研究室

NIDSコメンタリー
第 118 号 2020 年 6 月 2 日

はじめに

本コメンタリーでは、サイバー空間での責任ある行動に関する国際規範の形成や伝播を促すプロセス（規範プロセス）につき、近年の変化とその課題等を論じる。規範プロセスとは、規範の形成・伝播がいかなるアクターによって、どこで、いつ、どのように進められるのか、その具体的取組を捉える概念であり、規範の内容と並んで研究上で着目すべき論点となる[1]。以前のコメンタリーでも主要なプロセスを概観したが[2]、その後、特に 2018 年から 2019 年にかけて注目すべき変化がみられた。そこで本稿では、岐路を迎えたともされる[3]規範プロセスの近年の動向と課題を国連の内外に分けて概観した上で、そこから示される幾つかの論点をまとめとして簡単に考察したい。

国連内の規範プロセスの変化

国連内の重要な規範プロセスとして、第 1 委員会（軍縮・国際安全保障問題を所掌）の下にある政府専門家会合（GGE）での取組が挙げられる。そもそも国連でサイバーに関する議論が本格化したのは、1998 年 12 月にロシアが提案した決議「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」[4]の採択を契機とする。以降も内容を漸進的に修正した同様の決議がロシアの提案を受けて採択されたが、GGE の設置は 2001 年の決議に盛り込まれたものであり[5]、1 回目の会合は 2004 年から 2005 年にかけて開かれた。その後、断続的に開催されてきた会合は 2019 年から開催中のものを含めて 6 回目を迎え[6]、国家の責任ある行動に関する規範の在り方、信頼醸成や能力構築等について議論を重ねてきた[7]。GGE 参加国は米英仏ロ中、並びに会合ごとに各地域から衡平に選出される国々によって構成され、現在は 25 か国が参加している[8]。

GGE での議論の結果は、参加国のコンセンサスが得られた場合にのみ報告書として国連総会で公表される。これまで第 2 回（2010 年）・第 3 回（2013 年）・第 4 回（2015 年）、計 3 つの GGE で報告書が公表されているが、中でも第 3 回の報告書でサイバー空間に「国際法、特に国連憲章が適用可能（applicable）」であると明記されたこと[9]、そして第 4 回の報告書で国家の責任ある行動に関して 11 項目からなる規範が明示されたことは[10]、GGE の具体的な成果として高い注目を集めている。

他方、発足から 15 年以上経つ GGE プロセスは重要な局面を迎えている。第 6 回 GGE は会期を従来の 1 年から 2 年に延長、2021 年 9 月に報告書を公表予定であるが、第 5 回 GGE（2016 年～2017 年）に引き続き報告書の公表に至らない事態となれば、GGE の機能不全を指摘する声は強まりかねない。慶応義塾大学の土屋大洋教授が指摘されるように「第 4 回の GGE 報告書で、できるところまではやってしまったという側面も強い」[11]とみられる中、既存の国際法の具体的な適用方法等、各論に関して依然大きい諸国間の見解の隔たりをいかに縮められるかという難題に GGE は直面している。

また GGE は、かねてより指摘されてきた参加国の限定という問題も抱える。そこで第 6 回 GGE では、欧州連合（EU）や ASEAN 地域フォーラム（ARF）といった地域機構との対話、並びに全ての国連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が施されたが、サイバー空間で重要な役割を果たす非国家主体のプロセスへの参加の在り

方は課題として残る。

GGE が正念場を迎える中、国連内規範プロセスに「突然の局面変化」[12]が訪れた。2018 年 11 月、GGE と同様の議題を扱いながらも別の枠組みとなるオープンエンド作業部会（OEWG）を第 1 委員会の下に設置することが国連での投票を経て決定されたのである。

OEWG の新設は国連での議論を「より民主的、包摂的、透明性のあるもの」とすべく[13]、ロシアが中国等の支持を得ながら提案したものである。実際、OEWG は GGE とは異なり、全ての国連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を設ける点に特徴を有する。当該会期間会合は 2019 年 12 月、110 以上の非国家主体が参加して開催済みであり、OEWG での議論は 2020 年 9 月の報告書の公表に向けて進行中である。

国連内規範プロセスの変化として今一つ注目すべきものに、国連サイバー犯罪条約の策定を視野に入れた取組の推進もある。これもまたロシアが中国等の支持を受けながら進めているものであり、「情報通信技術の犯罪目的での利用に対処するための包括的な国際条約を検討」すべく「オープンエンド・アドホック政府間専門家委員会」の設置を求める決議が 2019 年 11 月に採択された[14]。ロシアはかねてから自らが作成した条約草案を示すなど[15]、サイバー犯罪に関して国連で新たな取組を進めることに積極的であり、2020 年 8 月の準備委員会を経て本格的に始動予定の同専門家委員会はその推進力となり得るものである。

こうした近年の変化には懸念も示されている。例えば、OEWG 設置によって非国家主体も国連内規範プロセスに参加する機会が生まれたことに対しては、期待とともに、非国家主体側の提言が全体的な議論に十分に反映されるとは限らないという疑念もある[16]。事実、非国家主体の本会合への参加は制限されており、またロシアと中国の非国家主体に関しては会期間会合への参加も限られていた[17]。そもそも両国の基本的立場がサイバー空間での国家の役割、例えばインターネットを介した情報通信を政府が統制する社会を重視するものであることを踏まえても、両国が推進する OEWG が非国家主体の国連内規範プロセスへの関与を促す実質的な機能を果たし得るかは不透明である。

さらに新たなプロセスの導入は、既存のプロセスとの関係性に不明確な部分を残す点にも問題を抱える。既述の通り GGE と OEWG は多くの議題を重複させおり、その相互関係性は論点となる。国連サイバー犯罪条約策定に向けた取組も、欧州評議会版のサイバー犯罪条約（ブダペスト条約）、並びにサイバー犯罪の包括的な対処策を検討すべく国連に 2011 年に設置済みの「サイバー犯罪に関するオープンエンド政府間専門家会合」と競合するようにみえる。

この点をまさに日米欧諸国は問題視し、OEWG の設置や国連サイバー犯罪条約策定に向けたプロセスの推進に反対、一方ロシアや中国等はむしろ GGE 継続に反対するなど、両者の対立は鮮明化した。日米欧諸国からみれば、新たなプロセスの導入には既存の取組を反故にし、自らにとって好ましい規範を形成しようとするロシアや中国等の思惑があると映ったといえる。2019 年 9 月には日米欧諸国を中心とした 27 か国は連名で文書も公表、サイバー空間にルールに基づく秩序を作り出そうとする従前のプロセスの成果を確認しながら、GGE、並びにこの時には既に設置が決まっていた OEWG へのコミットメントを謳うとともに、自由で開かれた安全なサイバー空間を守る自己の役割を再確認した[18]。

こうした状況から国連は両者の戦場になってきたとも評されたが[19]、少なくとも GGE と OEWG をめぐっては決裂した訳ではない。日米欧諸国は OEWG へ、ロシアと中国は第 6 回 GGE へそれぞれ参加し、現在のところ OEWG の開催はポジティブに受け止められているようである。とはいえ、今後本格化するサイバー犯罪に関する取組も含めて、多様化するプロセスの関係性を 1 つの争点に国連を舞台とする両者の角逐が強まっていく可能性は否定できない。

国連外の規範プロセスの変化

規範プロセスの変化は国連外でもみられた。以前

のコメンタリーでは、2011 年に英国で開催されたサイバー空間に関する国際会議を嚆矢とするロンドン・プロセス[20]、並びに世界情報社会サミット（WSIS）の提案に基づき 2006 年から設置されているインターネット・ガバナンス・フォーラム（IGF）に触れたが、その後、前者については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）の設置、後者に関してはエマニュエル・マクロン仏大統領による「パリ・コール（Paris Call）」の提唱といった動きがあった。

GCSC は 2017 年に世界中の有識者を集めて発足したものであり、その特徴は国家主体に限定されないマルチ・ステークホルダーで規範の形成・実践等の推進を図る枠組みになっている点にある[21]。それは GCSC が既存の 2 つのプロセスの系譜に連なる取組であることに由来し、うち 1 つがマルチ・ステークホルダーによる議論を特徴としたロンドン・プロセスである。他方は 2014 年 1 月、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（Centre for International Governance Innovation）と英国のチャタム・ハウス（Chatham House）の 2 つのシンクタンクが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（Global Commission on Internet Governance）」である。この 2 つのプロセスを敷衍させる形で、オランダが 2017 年のミュンヘン安全保障会議で設置を提唱したのが GCSC であった。

その GCSC は 2019 年 11 月に最終報告書を公表、取組に 1 つの区切りをつけたが、一連の取組は 2 つの点で意義深いものとなった。第 1 は、世界中の有識者たちが一堂に会して既存の取組を充実化する各種の提言を行ったことである。例えば GCSC は 8 つの規範を示したが、それらは GGE 等での議論に基づきつつ、インターネットの公共的な核心（Public Core of Internet）の保護[22]や選挙プロセスの保護[23]といった、GGE が示した規範にはない新たな要素を含むものとなっている。提言はマルチ・ステークホルダーによる協力の必要性を強調するものともなっており、規範の形成と実践における非国家主体の能動的関与を促すところに GCSC の 2 つ目の意義が見出せる。

GCSC とともに、国連外での新たな規範プロセスとして注目を集めたものにパリ・コールの提唱もある。パリ・コールは 2018 年 11 月にパリで開かれた IGF の講演でマクロン大統領がサイバー空間の信頼性と安全性を確保すべく提案したものであり、国際法の適用やサイバー犯罪対処におけるブダペスト条約の役割等を確認しつつ、全てのステークホルダーが順守すべき 9 つの原則を示す内容となっている[24]。原則では、例えば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、また国際規範の促進等が謳われているが、それらは GGE や GCSC といった既存の取組を反映したものである。なお 1 周年となる 2019 年 11 月には、マルチ・ステークホルダーによるプロジェクト推進体制、通称「パリ・コールコミュニティ」を原則ごとに設ける考えも示された[25]。

GCSC やパリ・コールをみると、欧州が国連外規範プロセスの大きな推進役を担ってきたことに気付かされる。パリ・コールを提唱したフランスは GCSC のパートナー国ともなっており、そもそも GCSC がロンドン・プロセスに連なるものであることは既述の通りである。こうした欧州による取組は、規範プロセスの両輪となるべき国家主体と非国家主体との連携を促すものであるとともに、国連で高まるロシアや中国等のプレゼンスを相対化する意義を有するとも考えられる。今やパリ・コールには 78 の国、644 の企業と 349 の市民団体等が参加し、大きな潮流を作り出しつつある。

他方、GCSC やパリ・コールには課題も指摘されている。例えば GCSC に関しては弱点として、自らは提言内容を実践する機能や権限を有していないため、提言が GGE 等、他の取組に受容されることが必須である点が挙げられている[26]。この文脈で、GCSC の議論の成果がパリ・コールや OEWG

に会期間会合を通じてインプットされたことは注目に値する。しかし、例えば OEWG に関しては既述の通り非国家主体側の提言が全体的な議論にどの程度の影響を及ぼし得るかは不透明であり、GCSC の取組が国連内規範プロセスにどのように効果的な形で取り込まれるかは注目点となる。

パリ・コールに関しては、米国やロシア、中国等の大国が不参加であることが問題視されている。ロシアと中国については、規範の在り方に対する立場が一致しないフランスが主導する取組に消極的な態度を示すことは不思議ではない。既述の通り、両国は国連を舞台に新たなサイバー犯罪条約の策定を目指しているところ、パリ・コールではブダペスト条約が重視されているところに参加に向けた 1 つの障壁があるとの見方もある[27]。より違和感を覚えるのは、フランスと同様に自由で開かれた安全なサイバー空間を標榜する米国の不参加である。パリ・コールの重要な推進役を担うマイクロソフトのブラッド・スミス社長がインタビューに答えたところによれば、米国政府は同社の説得にもかかわらず参加を見送ったのであり、それはドナルド・トランプ政権の多国間主義に対する消極的な態度に起因するとされる[28]。

さらにパリ・コールには、内容に対する誠実なコミットメントを賛同者に期待できるかという課題もある。それはパリ・コールが法的拘束力を有さないことはもとより、門戸を広く開く故に誠実なコミットメントに疑念を残すアクターも賛同者に含まれかねないことが懸念されているからであり、このことは 2019 年 8 月の中国ファーウェイ社のパリ・コールへの参加を引き合いに指摘されている[29]。

まとめ

以上、本コメンタリーでは国連内外の規範プロセスについてその課題も含めて概観したが、そこから示される 3 つの論点を以下で簡単に考察、本稿のまとめとしたい。

1 つ目の論点は、複数のプロセスの相互関係性である。既に観察できるように、多様なプロセスは互いの成果を参照する形で相互補完的な関係性を築き得る。またプロセスの多様化には、規範の多角的な検討と理解の深化、参加者範囲の拡大といったメリットもあると指摘されている[30]。他方、そこにはアクターが自らの要求を満たすプロセスを選択するが故に規範形成の困難さが増す、いわゆるフォーラムショッピングの懸念も存在する。従って、プロセスの相互補完性を強化するような設計を講じることが課題となり[31]、とりわけ非国家主体の能動的関与を促す仕組み、より具体的には GCSC やパリ・コールといた国連外プロセスと国連内のプロセスとの連関の在り方は重要な点になると考えられる。

2 つ目の論点は、規範プロセスをめぐる国家間関係の展望である。例えば国連内での事例では、主導権を発揮するロシアを中国が支持するという場面が目に付いた。先端技術でも連携する両国間にはあたかも[32]、規範作りの面ではロシアを、技術面では 5G を含む情報通信に係る技術を高める中国を推進力とし、両国が重視する、インターネットを介した情報通信を政府が強く統制する社会を、より盤石かつグローバルに広げていく協力関係が存在するかのようである。さらに、日米欧諸国の反対にもかかわらず各種決議が採択された事実は、一定数の国がそうしたロシアや中国を与する立場にあることを意味するものでもある。一国一票制度を旨とする国連の規範プロセスを左右する存在として「デジタル・ディサイダーズ」とも称される中小国グループに焦点が当てられることがあるが[33]、ロシアや中国はそうした国々を取り込む形で巧みにプロセスを主導してきたといえる。

もっとも、鮮明化した日米欧諸国とロシアや中国との対立構造は二項対立で捉えられる程に単純ではない。ロシアにとっては国内はもとより、中国製品に深く依存する情報通信インフラが自らの影響力を保ちたい中央アジアでも普及する状況は好ましくないはずであり[34]、露中のサイバー分野での協力関係は盤石とは言い難い。また日米欧諸国側で

も、安全保障等を目的に情報通信の政府による規制が一定程度必要との認識が高まってきている現状を踏まえ、依然としてロシアや中国とは政策的距離は大きいものの、論点は二項対立的な様相から、政府がどの程度関与すると過多なのかという程度の問題に移っているとの見方も示されている[35]。「デジタル・ディサイダーズ」の動向も含めて、複雑な国家間関係が規範プロセスにどのように投影されるのかは引き続き注目される。

3 つ目の論点として、規範の順守をいかに図るかという点も挙げられる。規範は各アクターが自発的に順守することが理想であるが、その実現は容易ではない。そのため、規範から逸脱する行為をチェックし、必要に応じて逸脱行為にチャレンジする取組が必要になる。この点は特に国家間関係において重要になるといえるが、この文脈で興味深いのは EU によるサイバー制裁レジームの導入である[36]。こうした規範の実践を図るための試みがどのような発展をみせるのかも、規範の形成や伝播に関して考察を深めるべき重要な政策・研究上の課題となる。

（2020 年 5 月 15 日脱稿）

---

[1] Martha Finnemore and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity," *The American Journal of International Law* 110, no. 3 (July 2016), 425-479, https://doi.org/10.1017/S0002930000016894.

[2] 原田有「サイバー空間のガバナンスをめぐる論争」『NIDS コメンタリー』第 43 号、2015 年 3 月 20 日。

[3] Christian Ruhl, Duncan Hollis, Wyatt Hoffman, and Tim Maurer, "Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads," Carnegie Endowment for International Peace Working Paper, February, 2020, https://carnegieendowment.org/files/Cyberspace_and_Geopolitics.pdf.

[4] UN General Assembly (UNGA), Resolution 53/70, Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/RES/53/70 (January 4, 1999), https://undocs.org/A/RES/53/70.

[5] UNGA, Resolution 56/19, Developments in the Field of Information and Telecommunications in the Context of International Security, para. 4, UN Doc. A/RES/56/19 (January 7, 2002), https://undocs.org/A/RES/56/19.

[6] GGE の第 2 回会合は 2009 年から 2010 年、第 3 回は 2012 年から 2013 年、第 4 回は 2014 年から 2015 年、第 5 回は 2016 年から 2017 年にかけてそれぞれ開催された。

[7] GGE の議題は第 1 委員会の所掌に合わせたものとなっており、同委員会の所掌外にある諜報活動やインターネット・ガバナンス、プライバシーといった議題は GGE では扱われない。

[8] GGE の参加国数は当初 15 か国であったが、4 回目で 20 か国、5 回目からは 25 か国に拡大された。

[9] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, para. 19, UN Doc. A/68/98 (June 24, 2013), https://undocs.org/A/68/98.

[10] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, para. 13, UN Doc. A/70/174 (July 22, 2015), https://undocs.org/A/70/174.

[11] 土屋大洋「外交の長い道のり―サイバースペースに国際規範は根付くか」『ニューズウィーク日本版』、2018 年 10 月 26 日。

[12] Samuele De Tomas Colatin, "A Surprising Turn of Events: UN Creates Two Working Groups on Cyberspace," The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) INCYDER, November 3, 2019, https://ccdcoe.org/incyder-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace/.

[13] UNGA, Resolution 73/27, Developments in the Field of Information and Telecommunications in the Context of International Security, para. 5, UN Doc. A/RES/73/27 (December 11, 2018), https://undocs.org/A/RES/73/27.

[14] UNGA, 74th Session Third Committee Agenda Item 107, Countering the Use of Information and Communications Technologies for Criminal Purposes, para. 2, UN Doc. A/C.3/74/L.11/Rev.1 (November 5, 2019), https://undocs.org/en/A/C.3/74/L.11/Rev.1.

[15] UNGA, 72nd Session, Third Committee Agenda Item 107, Annex to the Letter Dated 11 October 2017 From the

Permanent Representative of the Russian Federation to the United Nations Addressed to the Secretary-General, "Draft United Nations Convention on Cooperation in Combating Cybercrime," UN Doc. A/C.3/72/12 (October 16, 2017), https://undocs.org/A/C.3/72/12.

[16] Josh Gold, "A Multistakeholder Meeting at the United Nations Could Help States Develop Cyber Norms," Council on Foreign Relations (CFR) Blog, January 16, 2020, https://www.cfr.org/blog/multistakeholder-meeting-united-nations-could-help-states-develop-cyber-norms; François Delerue, "From Multilateral to Multistakeholder? New Developments in UN Processes on Cybersecurity," CFR Blog, January 27, 2020, https://www.cfr.org/blog/multilateral-multistakeholder-new-developments-un-processes-cybersecurity.

[17] Gold, "A Multistakeholder Meeting at the United Nations Could Help States Develop Cyber Norms."

[18] "Joint Statement on Advancing Responsible State Behavior in Cyberspace," U.S. Department of State, September 23 2019, https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/.

[19] Justin Sherman, and Mark Raymond, "The U.N. Passed a Russia-baked Cybercrime Resolution. That's Not Good News for Internet Freedom," *The Washington Post*, December 4, 2019.

[20] 同国際会議はその後、ブダペスト（2012 年）、ソウル（2013 年）、ハーグ（2015 年）、ニューデリー（2017 年）と都市を変えて継続的に開催され、一連の取組を指してロンドン・プロセスと称されている。

[21] 委員を務めるのは元政府高官や学者、企業関係者等、様々な国の専門家たちであり、委員会のパートナーとしてオランダとフランスの外務省、シンガポールのサイバーセキュリティ庁等が、またスポンサーとして日本の総務省等が名を連ねる。なお、GCSC の歴史については次を参照。Global Commission on the Stability of Cyberspace (GCSC), "Advancing Cyberstability: Final Report," November, 2019, pp. 46-47, https://cyberstability.org/wp-content/uploads/2020/02/GCSC-Advancing-Cyberstability.pdf.

[22] GCSC, "Call to Protect the Public Core of Internet," November, 2017, https://cyberstability.org/wp-content/uploads/2018/07/call-to-protect-the-public-core-of-the-internet.pdf. なお、インターネットの公共的な核心は、ドメインネームシステムや通信ケーブル等、インターネットの運用に欠かせない要素を指す。

[23] GCSC, "Call to Protect the Electoral Infrastructure," May, 2018, https://cyberstability.org/wp-content/uploads/2018/05/GCSC-Call-to-Protect-Electoral-Infrastructure.pdf.

[24] "The 9 Principles," Paris Call: For Trust and Security in Cyberspace, November 12, 2018, https://pariscall.international/en/principles.

[25] John Frank, "Paris Call: Growing Consensus on Cyberspace," Microsoft Blog, November 12, 2019, https://blogs.microsoft.com/on-the-issues/2019/11/12/paris-call-consensus-cyberspace/.

[26] Ruhl, Hollis, Hoffman, and Maurer, "Cyberspace and Geopolitics," p. 10.

[27] Ibid., p. 12.

[28] "Exclusive: Microsoft's Brad Smith on the White House's Refusal to Back His Cyber Warfare Treaty," NS Tech, November 3, 2019, https://tech.newstatesman.com/security/microsofts-brad-smith-explains-why-he-thinks-trump-hasnt-signed-un-cyber-agreement.

[29] Ruhl, Hollis, Hoffman, and Maurer, "Cyberspace and Geopolitics," p. 12.

[30] Ibid. pp. 13-15.

[31] Ibid.

[32] Keegan Elmer, "China and Russia Plan to Boost Scientific Cooperation with Focus on Artificial Intelligence and Other Strategic Areas," *South China Morning Post*, December 28, 2019.

[33] Robert Morgus, Jocelyn Woolbright, and Justin Sherman, "The Digital Deciders: How a Group of Often Overlooked Countries Could Hold the Keys to the Future of the Global Internet," New America, October 22, 2018, https://www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/.

[34] Valentin Weber, "The Sinicization of Russia's Cyber Sovereignty Model," CFR Blog, April 1, 2020, https://www.cfr.org/blog/sinicization-russias-cyber-sovereignty-model.

[35] Justin Sherman, "How Much Cyber Sovereignty is Too Much Cyber Sovereignty?" CFR Blog, October 30, 2019, https://www.cfr.org/blog/how-much-cyber-sovereignty-too-much-cyber-sovereignty.

[36] EU の制裁レジームについては次を参照。Patryk Pawlak and Thomas Biersteker, eds., *Guardian of the Galaxy: EU Cyber Sanctions and Norms in Cyberspace*, The European Union Institute for Security Studies (EUISS) Chaillot Paper 155, October 31, 2019, https://www.iss.europa.eu/content/guardian-galaxy-eu-cyber-sanctions-and-norms-cyberspace.

プロフィール profile

政策研究部

グローバル安全保障研究室

主任研究官　　原田　有

専門分野：海洋安全保障、サイバーセキュリティ

防衛研究所企画部企画調整課
直　通：03-3260-3011
代　表：03-3268-3111（内線 29171）
ＦＡＸ　：03-3260-3034
※ 防衛研究所ウェブサイト：http://www.nids.mod.go.jp/