サイバー空間での規範形成に向けた取組の現状と展望に関する実験的考察
──自由主義陣営と権威主義陣営が繰り広げる「両性の闘い」に着目して──

原田　有

＜要旨＞

サイバー空間での規範形成に向けた多様な取組が進む昨今、目下の状況をどう捉え、その展望をいかに描くかはより重要な論点となっている。その背景には、規範の基調に自由･開放（含むマルチ･ステークホルダー協力）を据える日米欧の自由主義陣営と、国家主権や政府による情報通信統制に重きを置く露中等の権威主義陣営との、規範の内容はもとより、その形成や伝播のプロセスをめぐる対立もある。それは2019年に顕著となり、両者はあたかも「ゼロサム」状態にあるかのように捉えられた。しかし、そうした見方は時期尚早である。そこで本稿は、両陣営は対立を深めながら調整を続ける「両性の闘い」状態にあるとの仮説に立ち、その妥当性を事例研究で検証することにした。その結果、目下の状況には仮説が成り立つ余地があり、また両陣営の調整には「主権・統制」を基調とした規範形成に向けた潮流が観察できることが示された。そしてこの潮流に抗するためには、非国家主体の役割は大きく、その存在も加味した研究が今後の課題になる。

はじめに

近年、サイバー空間での規範形成に向けた多様な取組が進む目下の状況をどう捉え、その展望をいかに描くかはますます研究上の関心を集めている。その一因は、規範形成の論点がインターネットガバナンスや責任ある行動の在り方等多岐にわたることにある。レジーム・コンプレックスとも称される状況への理解を深めることは、かねてから課題となってきた[1]。さらにもう一つの要因として、日米欧の自由主義陣営と露中等の権威主義陣営との対立も挙げられる。前者は規範の基調に「自由･開放」を据える。具体的には、情報の自由な流通や表現の自由の保障、非国家主体も含む様々な主体（マ

1　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.

ルチ･ステークホルダー）による協力の必要性、並びに既存の国際法の適用等を掲げる。一方、後者は「主権・統制」を基調とすることを目指す。すなわち、サイバー空間での国家の主権や役割を強調し、政府による情報通信の統制等も許容されるような新たなルールの策定も視野に入れる。両者は規範の内容はもとより、自らにとって望ましい規範の形成や伝播を促す取組の推進、すなわちサイバー規範プロセス（Cybernorm Process）[2] をめぐっても角逐してきたのであり、それは昨今より顕著になっている。本稿は、そうした両者の対立と協調に実験的な考察を加えて、今後の研究の資を得ようとするものである。

2019 年は、サイバー規範プロセスをめぐる両陣営の対立が目立つ年となった。国連では露中等が推進して、規範を検討する新たなプロセスであるオープンエンド作業部会（OEWG[3]）が設けられ、国連サイバー犯罪条約作りを視野に入れた決議も採択された。対照的に日米欧諸国は、既存のプロセスである、国連政府専門家会合（GGE[4]）や欧州評議会サイバー犯罪条約（ブダペスト条約）を重視し、「自由、開放、安全なサイバー空間」の擁護に向けた自らの役割を改めて強調する 27 か国連名の文書も策定した [5]。また国連外では、欧米の取組に連なる、マルチ・ステークホルダー協力を体現する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[6]）が、GGE 等の既存の成果に基づく規範も提起した。こうした中、特に国連を舞台にした対立を受けて一部では、「国際機関は『グローバル・開放』インターネットモデルと『主権・統制』アプローチとの争いの戦場と化した」[7] とも評された。あたかも自由主義陣営と権威主義陣営は、「協力して、双方にとってよりよい社会状態を実現したり維持することは不可能」[8] な「ゼロサム」状態に陥っているかのように捉えられたのである。

しかし、そうした議論が妥当かは議論の余地を残す。一般的に、規範は普遍性を有する方が好ましいはずであり、両者は決裂を回避するインセンティブをもつ。従って、種々のプロセスの混在が直ちに「ゼロサム」を意味するとは限らない。さらに言えば、自由主義陣営すらも安全保障等の観点から「主権・統制」的側面を重視し始めている

2 サイバー規範プロセスに関しては次を参照。Martha Finnemore and Duncan B. Hollis, “Constructing Norms for Global Cybersecurity,” *The American Journal of International Law,* Vol. 110, no. 3 (July 2016), pp. 425-479, https://doi.org/10.1017/S0002930000016894.

3 Open-ended Working Group の略称。

4 Group of Government Experts の略称。

5 “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/.

6 Global Commission on the Stability of Cyberspace の略称。

7 Justin Sherman, and Mark Raymond, “The U.N. Passed a Russia-backed Cybercrime Resolution. That’s Not Good News for Internet Freedom,” *Washington Post,* December 4, 2019, https://www.washingtonpost.com/politics/2019/12/04/un-passed-russia-backed-cybercrime-resolution-thats-not-good-news-internet-freedom/.

8 山本吉宣『国際レジームとガバナンス』（有斐閣、2008 年）、78 頁。

として、規範形成上の論点は今や「自由・開放」か「主権・統制」かではなく、「どの程度のサイバー主権だと過大か」[9]という程度の問題に移ってきたとの見方もある。中には、自由主義陣営が権威主義陣営に接近することで、民主主義の根幹が揺らぐ最悪のシナリオも示されている[10]。

こうしてみると、そもそも両陣営にどのような対立と協力の関係があるのかという問いが浮かぶ。当該関係性は国際レジーム論で利益構造（ゲーム理論でいう、利得を最大化しようとするプレイヤー間のゲームの型）と呼ばれることがあり、規範やルールのセットたるレジームの形成や変化の要因になると目されている[11]。従って、この利益構造に着目して目下の状況を捉える視点も必要である。だが、既存研究の焦点は多様なプロセスの相互関係性の在り方、あるいは望ましい規範形成に向けたアクターの戦略や行動に当てられている。従って、新たな視点を取り入れた研究がまたれている。

そこで本稿は、両陣営の利益構造は対立を深めながら調整が続く「両性の闘い」で捉えられるとの仮説に立ち、その妥当性を事例研究で検証する実験的考察を行うことにした。事例としては、目下の状況の把握という本稿の趣旨に照らし、2019 年の主たるサイバー規範プロセスである、GGE・OEWG、国連サイバー犯罪条約に関連した決議の採択、GCSC を取り上げる。そして仮説が成り立つとすれば、両陣営は「自由・開放」と「主権・統制」を両極端とする線上で調整することが想定されるが、目下の状況にはいずれを基調とした規範形成に向けた潮流が観察できるのか、その際の自由主義陣営の政策課題は何かについて探求した。

分析結果を先取りすれば、GGE・OEWG と GCSC の事例では仮説が成り立つ余地が見出せ、両陣営の調整には「主権・統制」を基調とする規範形成に向けた潮流が観察できるとの結論が得られた。また本研究からは、権威主義陣営のリーダーたるロシアの規範起業家（Norm Entrepreneurs）としての存在が際立った。自由主義陣営としてはこの潮流に抗するためには、今一つの重要な規範起業家である非国家主体との協力が課題になる。

もっとも本研究は、サイバー規範プロセスに係る 2 つの陣営の利益構造に焦点を絞っているため、複雑な現実を単純化しているところに課題を残す。言うまでもなく、各陣営内の諸国家も含めて、サイバー空間に関わるアクターの立場や態度は一様ではない。また、本研究からその重要性が示唆された非国家主体、あるいは、いずれの陣営

9 Justin Sherman, “How Much Cyber Sovereignty is Too Much Cyber Sovereignty?” Council on Foreign Relations (CFR) Blog, October 30, 2019, https://www.cfr.org/blog/how-much-cyber-sovereignty-too-much-cyber-sovereignty.
10 Alexander Klimburg, *The Darkening Web: The War for Cyberspace* (NY: Penguin Press, 2017), pp. 365-366.
11 山本『国際レジームとガバナンス』、76-86 頁。

にも属さず、一国一票を旨とする国連での規範形成において存在感を発揮する「デジタル・ディサイダーズ（Digital Deciders）」[12] と称される第 3 の諸国群を含めた視点も必要である。さらに、本研究では国連サイバー犯罪条約の事例では「ゼロサム」的様相が観察できるとしたが、他の 2 事例と組み合わせて考えれば異なった見方も可能かもしれず、様々な事例を一連のプロセスとして捉えた考察も求められる。加えて、規範の順守に係るプロセスも加味した研究もまたれる [13]。こうした限界を認識しつつも、本稿のような実験的考察には既存研究の議論を深め、政策的含意を得られる意義があると考え、今後の研究に向けた一歩と位置付けたい。

次節以降、まず先行研究を概観しつつ問題の所在と分析枠組みを示した上で事例研究を実施、それを踏まえた仮説の検証と包括的な考察を行う。そして最後に、今後、本研究の課題を検討する際に注目される事象やそこでの自由主義陣営の政策的課題について簡単に触れ、本稿を締めくくる。

1．問題の所在と分析枠組みの提示

（1）問題の所在

規範、あるいは規範やルールのセットであるレジームは、かねてからある国際政治学の一大研究テーマである [14]。それら論考では、規範の具体的内容だけでなく、規範の形成や伝播がいつ、どのように進むのか、そのプロセスにも焦点が当てられ、プロセスを左右する規範起業家の戦略や行動も注目されてきた。規範起業家になり得るのは国家に限定されず、特に非政府組織（NGO[15]）や企業等の非国家主体がどのようにして国家の政策にすら影響を及ぼし得るのかは論点となってきた [16]。

12 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, last updated October 23, 2018, https://www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/.

13 プレイヤーが問題領域ごとに繰り広げるゲームの体系的な把握、並びに交渉段階での調整ゲームとその履行を図る段階での「囚人のジレンマ」ゲーム（本稿の脚注 30 を参照）を分けて捉える必要性については、例えば次の論考が参考になる。James D. Fearon, “Bargaining, Enforcement, and International Cooperation,” *International Organization,* vol. 52, no. 2 (Spring, 1998), pp. 269-305.

14 規範やレジームを論じた著名な論考として例えば次を参照。Stephen D. Krasner, “Structural Causes and Regime Consequences: Regimes as Intervening Variables,” *International Organization,* vol. 36, no. 2, International Regimes (Spring, 1982), pp. 185-205; Martha Finnemore and Kathryn Sikkink, “International Norm Dynamics and Political Change,” *International Organization,* vol. 52, no. 4 (Autumn, 1998), pp. 887-917; 山本『国際レジームとガバナンス』。

15 Non-Governmental Organization の略称。

16 Margaret E. Keck, and Kathryn Sikkink, *Activists Beyond Borders: Advocacy Networks in International Politics* (Ithaca and London: Cornell University Press, 1998); Richard Price, “Reversing the Gun Sights: Transnational Civil Society Targets Land Mines,” *International Organization,* vol. 52, no. 3, (Summer, 1998), pp. 613-644.

興味深い点は、こうした議論の地平が近年、サイバー空間での規範形成というテーマにも広がりをみせていることである。もともと同テーマの大きな焦点は、国際法の適用方法等の規範の具体的内容に当てられてきた。しかし、どのようにして規範の形成や伝播が進むのか、規範起業家の動向も含むサイバー規範プロセスに目を向ける必要性も提起され始めたのである[17]。そして冒頭で述べたように、多様なプロセスが混在する状態がより複雑さを増す状況にあって、この現状に評価を加えたり、望ましいプロセスの創出に向けたアクターの戦略や行動を考察する研究がみられるようになっている。

現状の評価に関して注目される最新の論考に、カーネギー国際平和財団（Carnegie Endowment for International Peace）が実施したワークショップの報告書がある[18]。当該報告書は、GGE や OEWG、GCSC 等、目下で進む幾つかのプロセスを俯瞰的に捉えて、それらの相互関係性に検討を加える内容になっている。そして、多様なプロセスが併存している現状には、アクターが自らにとって好ましいプロセスを選択して規範形成に向けた取組が分散してしまうフォーラムショッピングの懸念があるとする[19]。他方でそうした状況には、規範に対する理解の深化や参加者の範囲の拡大、あるいは特定の分野での議論の停滞が全体的な議論の停滞を招く事態を回避できるメリットもあるとする[20]。そしてこのメリットを強化すべく、種々のプロセスの相互補完性を計画的に確保する必要性を指摘する[21]。こうした論考は、その相互補完性にどのようなアクターのいかなる利益が反映されるのかという疑問を生む。しかし、この点は同報告書では十分に議論されていない。

そこで注目されるのが、望ましいプロセスの創出に向けたアクターの動向に関心を寄せる研究である。かねてから規範形成をめぐる米露中の角逐は論点となってきたが[22]、最近の興味深い論考としては例えば米国のシンクタンクのニュー・アメリカ（New America）の研究が挙げられる[23]。そこでは独自の指標を用いながら、インターネットガバナンスに関する諸国の動向を自由主義陣営（同研究上では「グローバル・開放」陣営）と権威主義陣営（同研究上では「主権・統制」陣営）、並びにいずれにも属さな

17 Finnemore and Hollis, “Constructing Norms for Global Cybersecurity.”
18 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, February 26, 2020, https://carnegieendowment.org/files/Cyberspace_and_Geopolitics.pdf.
19 Ibid., p. 13-15.
20 Ibid.
21 Ibid.
22 例えば次を参照。Klimburg, *The Darkening Web*. また、日本の研究では慶応義塾大学の土屋大洋教授の論考が参考になる。一例として次を参照。土屋大洋『サイバーセキュリティと国際政治』（千倉書房、2015 年）、特に第 6 章。
23 Morgus, Woolbright, and Sherman, “The Digital Deciders.”

い諸国から成る第 3 群に分類している。そして第 3 群を「デジタル・ディサイダーズ」と位置付け、両陣営が対立する構造にあって、自由主義陣営側の政策課題はこの第 3 群の取り込みにあると論じる。

また、アクターの動向をより一般化して「サイバー外交（Cyber Diplomacy）」という概念で捉える研究も主に欧州でみられる。サイバー外交とはその先駆的論考によれば、「外交的資源の活用や外交的機能の発揮を通じて、サイバー空間に係る国益を確保すること」[24] を意味する。それは、「サイバーセキュリティ、サイバー犯罪、信頼醸成、インターネット利用の自由とガバナンス」[25] といった技術的アプローチのみでは解決できない問題に取組むべく展開されるものとされる。またそれらの問題は非国家主体との協力なくして解決できないため、各国にとっては他国だけでなく、非国家主体との協力も政策課題になると指摘されている [26]。

これら論考は先に触れた規範起業家の戦略や行動に焦点を当てる研究と位置付けられるが、目下の状況やその展望を検討するにおいて、少なくとも次の 2 つの課題が指摘できる。第 1 に、このような論考では、自らにとって望ましい規範の形成を目指すアクター間の利益構造が見過ごされている。既述の通り、同構造はレジームの形成と変化の要因として着目が欠かせない要素である。例えば、アクター間に自らにとって最も望ましい結果が一致する構造（「調和」）や、利害が真っ向から対立する構造（「ゼロサム」）がある場合、レジームは形成されない [27]。先のニュー・アメリカの研究に目を戻せば、自由主義陣営と権威主義陣営はあたかも「ゼロサム」状態にあるようにみえるが、仮にそうだとすれば、理論上、両者を包摂するレジームは形成されないことになる。しかし、このように結論付けることは現段階では時期尚早である。両陣営間の利益構造に注目して目下の状況を捉える研究が求められている。

第 2 に、規範起業家の今一つの重要アクターである非国家主体の戦略や行動を捉える視点も必要である。そもそもサイバー空間の中心的アクターは非国家主体であり、安全保障の確保等を目的に次第に国家主体も存在感を強めてきたという経緯を踏まえても、非国家主体の役割は軽視できない。実際、例えばマイクロソフト社は 2017 年に「デジタル版ジュネーブ条約（Digital Geneva Convention）」[28] の策定を提唱し、規範形

24 André Barrinha and Thomas Renard, “Cyberdiplomacy: The Making of an International Society in the Digital Age,” *Global Affairs,* Vol. 3, no. 4-5, 2017, p. 355.
25 Ibid.
26 Shaun Riordan, *Cyberdiplomacy: Managing Security and Governance Online* (Cambridge: Polity Press, 2019), pp. 51-52.
27 山本『国際レジームとガバナンス』、77-78 頁。
28 “A Digital Geneva Convention to Protect Cyberspace,” Microsoft, https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace.

成に一石を投じている。その他、GAFA（Google、Amazon、Facebook、Apple）等の存在も大きく、これら非国家主体の規範起業家としての役割は論点となる[29]。

要するに既存研究からは、アクター間の利益構造の検討や非国家主体の動向の考察といった研究課題が浮かび上がる。従って、例えば規範形成をめぐる自由主義陣営と権威主義陣営、並びに非国家主体との三つ巴の利益構造の考察が必要になる。そこで本稿では研究の初めの一歩として、まずは両陣営の利益構造に着目して目下の状況を捉える研究を行う。非国家主体はその際の検討材料として扱うにとどめ、三つ巴の関係性の考察は今後の課題とする。

（2）分析枠組み

さて冒頭で述べたように本稿では、自由主義陣営と権威主義陣営の利益構造が「両性の闘い」状態にあるとの仮説に立ち、その妥当性を GGE・OEWG、国連サイバー犯罪条約に関連した決議の採択、GCSC を事例に検証する分析枠組みを取り入れる。

そもそもゲーム理論でいう「両性の闘い」とは、双方のプレイヤーにとって相手を裏切るよりも協力した方が利得が高まるゲームを指す。協力には、自己の利得がより高まる場合と、相手の利得がより高まる場合の 2 通りがあり、自己の利得の最大化を目指すプレイヤー間で激しい対立が生じることになる。このゲームの特徴は、仮に相手のプレイヤーの利得が高くなる形での協力に至ったとしても、もう一方のプレイヤーの利得は裏切るよりも協力した方が高くなるところにある。2 人のプレイヤー間のゲームとして著名な「囚人のジレンマ」ゲーム[30]と比べた時、同ゲームでは「合意を得るのはやさしいが、それを守ることが困難」[31]であるのに対して、「両性の闘い」では「合意を得るのは難しいが、いったん合意（ルール）ができてしまえば、それは自動的に守られる」[32]という違いがある。

この「両性の闘い」ゲームで自由主義陣営と権威主義陣営の利益構造を捉えて、各陣営の選択（規範の基調に「自由・開放」と「主権・統制」のいずれを据えるか）とその利得を示したものが表 1 である。同表は、両陣営の選択が一致するセル A では「自由・開放」を基調とする普遍的な規範が、セル D では「主権・統制」を基調とする普遍的な規範が形成されることを表す。他方、両陣営の選択が不一致となるセル C では

29 Tim Maurer, “Private Companies Take the Lead on Cyber Security,” *War on the Rocks,* May 4, 2018, https://warontherocks.com/2018/05/private-companies-take-the-lead-on-cyber-security/.

30「囚人のジレンマ」とは、他のプレイヤーを裏切ることで自己の利得を最大化できるが、双方ともに利得を最大にすべく裏切りを選択すると、協力する場合よりも利得が減ってしまうゲームを指す。詳細については例えば次を参照。岡田章『ゲーム理論･入門（新版）―人間社会の理解のために』（有斐閣アルマ、2014 年）、第 5 章。

31 山本『国際レジームとガバナンス』、83 頁。

32 同上。

自由主義陣営は「自由・開放」に基づく規範を、権威主義陣営は「主権・統制」に基づく別の規範を形成することが想定される。同様に選択が不一致となるセル B では、自由主義陣営は「主権・統制」に基づく規範を、権威主義陣営は「自由・開放」に基づく別の規範を形成することになる。

表1　「両性の闘い」で捉えた自由主義陣営と権威主義陣営の利益構造

		権威主義陣営	
		自由・開放	主権・統制
自由主義陣営	自由・開放	Ⓐ 4 / 3	Ⓒ 2 / 2
	主権・統制	Ⓑ 1 / 1	Ⓓ 3 / 4

（注）各セル内斜線左下の数字は自由主義陣営の利得を、右上は権威主義陣営の利得を指す。また数字が高い程、各陣営にとっての利得が高いことを表す。
（出所）山本吉宣『国際レジームとガバナンス』、78 頁を参考に筆者作成。

ここで各陣営の選択とその利得について、より具体的にみてみたい。そもそもこのゲームでは、両陣営の利得は選択が一致する場合（セル A、D）、すなわち普遍的な規範が形成される方が、選択が不一致となって、異なった規範が併存する場合（セル B、C）よりも利得が高くなる。実際、規範が普遍性を有することは、両陣営にとって、両者間の関係の安定化に資するだけでなく、例えば企業が提供するサービスの享受という点でも望ましいといえる。国や地域で適用される規範が異なれば、それがビジネスの障害となって、規範が一致していれば実現したであろうサービスが得られない事態も想定できよう。

こうした中、自由主義陣営の利得が最も高くなるのは「自由・開放」で両陣営の選択が一致する場合（セル A）であり、次点は「主権･統制」で選択が一致する場合（セル D）となる。同陣営がセル D の結果を受け入れかねないとの懸念が一部で示されていることは、冒頭で触れた通りである。もっとも同陣営にとって「主権･統制」の選択は、自らの旗印を下げることだけでなく、「主権・統制」に対して強い抵抗感を有する非国家主体[33]を裏切って、マルチ・ステークホルダー協力を損なうことも意味する。従っ

33　この点は、2018 年 11 月にフランスのエマニュエル・マクロン大統領が演説で、インターネットに関する一定の規制の必要性に言及したことに対して、インターネット関係者が不信感を露わにした例に端的に示される。同演説の状況については次を参照。「パリ・コールとマクロン大統領の演説―IGF パリで始まった大きなうねり」JPNIC、2018 年 12 月 7 日、https://blog.nic.ad.jp/2018/2050/。

てその選択には慎重になるはずであり、特に両陣営の選択が不一致となって規範の分裂が生じる場合には、自らは「自由・開放」を追求する方（セル C）が、その理念に反した選択を行うこと（セル B）よりも利得は高くなる。

一方、権威主義陣営にとっては「主権・統制」で両者の選択が一致する場合に利得が最も高くなり（セル D)、普遍的な規範を求めるにおいては、「自由・開放」で選択が一致する場合（セル A）が次点に高くなる。実際、同陣営は必ずしも「自由・開放」の必要性を全否定している訳ではない。例えば米英仏露中を中心に 20 か国程が参加してきた GGE は、2015 年に 11 項目から成る規範を示したが、その目的の一つには、開かれた情報通信技術環境の促進が含まれている [34]。さらに 2015 年、露中等の上海協力機構加盟国（除くインドとパキスタン）が国連で提案した「情報セキュリティに関する国際行動規範」では、情報空間での自由の尊重や非国家主体との協力も触れられている [35]。もっとも、そこには国内外の安全保障や国内治安の確保といった前提条件が付されているといえ、権威主義陣営が「自由・開放」を選択するにおいては、これら懸念の払しょくという難しい課題が解決される必要がある。そしてもしかかる課題が解決されない中で規範の分裂が生じるとすれば、権威主義陣営にとっては「主権・統制」を追求する方（セル C）が、「自由・開放」を選択する場合（セル B）よりも利得が高くなる。

両陣営の利益構造がこうした「両性の闘い」状態にあるとすれば、あたかも「ゼロサム」にもみえるサイバー規範プロセスに係る目下の状況には、鋭く対立しつつも決裂を回避する形で調整が進む様子が見出せるはずである。果たしてこの仮説は 3 事例で成り立つか。成り立つとすれば、「自由・開放」と「主権・統制」を両極端とする線上で進む両陣営の調整には、いずれを基調とした規範形成に向けた潮流が観察できるのか。次節ではまず各事例を概説した後、包括的な考察を行って仮説を検証する。

34 United Nations General Assembly (UNGA), 70th Session, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, p. 7, UN Doc. A/70/174 (July 22, 2015), https://undocs.org/A/70/174.

35 UNGA, 69th Session, International Code of Conduct for Information Security, para. 7, para. 9, UN Doc. A/69/723 (January 13, 2015), https://undocs.org/A/69/723.

2．事例研究を通じた仮説の検証

（1）事例研究

（ア）GGE と OEWG

国連第 1 委員会（軍縮・国際安全保障問題を所掌）の下に設置される GGE は、国連の主要なサイバー規範プロセスであり、国家の責任ある行動に係る規範の在り方や信頼醸成、能力構築等を検討する場となってきた。そもそも国連でのサイバーに関する議論の本格化は、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」[36] の採択に遡る。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、2001 年の決議に GGE の設置が盛り込まれた経緯がある [37]。GGE は 2004 年から 2005 年にかけての第 1 回会合を皮切りに、2019 年から開催中の第 6 回会合に至るまで断続的に開催され、当初 15 か国であった参加国数は、第 4 回会合で 20 か国に、そして第 5 回会合以降は 25 か国に拡大している [38]。

GGE はこれまで、先に触れた 11 項目から成る規範の提示といった具体的な成果を生んできたが、初会合から 15 年以上経ち、難しい局面を迎えている。第 5 回 GGE では国際法の適用の在り方等について議論がまとまらず、参加国のコンセンサスを条件とする報告書の公表に至らなかった。この結果を受けて GGE は失敗に終わったとも評された。また、「2015 年の第 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」[39] とも指摘された。

議論は次なる GGE に持ち越されるものと考えられた中、状況は一変した。ロシアが中国等の支持を得て、サイバー空間での規範を議論する新たな場として OEWG の設置を提案、国連第 1 委員会での決議の結果、賛成 109 か国、反対 45 か国（棄権 16 カ国）で設置が決定されたのである [40]。OEWG の特徴は、国連での議論を「より民主的、包摂的、透明性のあるもの」[41] とすべく、GGE とは異なり全ての国連加盟国の議論へ

36 UNGA, 53rd Session, 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.

37 UNGA, 56th Session, 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.

38 参加国は米英仏露中に加えて、各地域から衡平に選出される国々から成る。

39 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、https://www.newsweekjapan.jp/tsuchiya/2018/10/post-30.php.

40 UNGA, 73rd Session, Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the First Committee, pp. 2-3, UN Doc. A/73/505 (November 19, 2018), https://undocs.org/A/73/505.

41 UNGA, 73rd Session, 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.

の参加を可能にし、またNGOや企業等の非国家主体との意見交換の機会も設ける点にあった[42]。露中等には、サイバー空間の規範形成に関して共通の利害関係を持つものの、これまで国連での議論に十分に参加できてこなかった国々を交渉の場へ組み込むことで、自陣営の交渉力を強化しようとする思惑があったようにもみえる。その後OEWGは、2019年12月に非国家主体も参加した会期間会合を開催する等、2020年9月の報告書公表に向けてプロセスが進行中である。

日米欧諸国は今でこそOEWGに参加しているが、設置案には反対票を投じていた。その背景には、OEWG新設にはGGE等での議論を振り出しに戻して、自らに望ましい規範の形成につなげようとする露中等の目論見があるとの懸念があったといえる。また、一定数の国が露中等に与することで自由主義陣営の交渉力が低下しかねないとの危惧もあっただろう。そこで日米欧諸国は第6回GGEの開催を提案、賛成139か国、露中を含む反対11か国、棄権18か国でGGEの開催にこぎ着けた[43]。新たなGGEはこれまでの議論の継続に加えて、欧州連合（EU[44]）やASEAN地域フォーラム（ARF[45]）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ての非公式会合の開催も実施する工夫が施されており、2021年9月に報告書を公表予定である。

（イ）国連サイバー犯罪条約の策定を視野に入れた国連決議の採択

OEWGの新設と合わせて注目された出来事に、やはりロシアが提案し中国等が支持した国連サイバー犯罪条約の策定を視野に入れた国連決議もあった。賛成88か国、反対58か国、棄権34か国で採択[46]（2019年11月）された国連第3委員会での決議は、「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」[47]すべく「オープンエンド・アドホック政府間専門家委員会」[48]の設置を求めている。現在のところ、2020年8月に準備委員会が開催予定である。

そもそもサイバー犯罪に関してはブダペスト条約が既にあり、日米欧諸国を含む計65か国がこれまでに批准してきた。同条約は改善の余地を残すものの、サイバー犯罪

42 Ibid.
43 UN Doc. A/73/505, pp. 3-4.
44 European Unionの略称。
45 ASEAN Regional Forumの略称。
46 UNGA, 74th Session, Countering the Use of Information and Communications Technologies for Criminal Purposes: Report of the Third Committee, para. 10, UN Doc. A/74/401 (November 25, 2019), https://www.undocs.org/A/74/401.
47 UNGA, 74th Session, 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.
48 Ibid.

に関する唯一の法的拘束力のある条約として重要な役割を果たしてきた[49]。加えて、国連には既に「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」もある。当該会合は 2011 年 1 月以来、継続的に開催され、サイバー犯罪の包括的な対処策を検討する舞台となってきた。

こうした既存の取組にもかかわらず、ロシアは先の決議を提案した訳だが、国連サイバー犯罪条約の策定に向けたロシアの取組は今に始まったことではない。ロシアはかねてからサイバー空間における国家主権、政府による統制に重きを置く「国連サイバー犯罪条約草案」を提示してきた[50]。決議に基づき設置される政府間専門家委員会は、まさにこの草案を結実させる大きな推進力となり得る。

こうしたロシアの動きに日米欧諸国は強く反発した。それは、サイバー犯罪に関する新たなプロセスの導入は既存のプロセスを弱体化させ、権威主義陣営にとって都合の良い規範作りを目指すものと捉えられたからといえた。また、サイバー空間の自由や開放性を損なう結果を招きかねないことへの懸念もあっただろう。米国は決議の投票に際し、この提案は「サイバー犯罪の対処に向けたグローバルな努力を窒息させるのみ」[51] だと批判した。また非国家主体も同様に厳しい立場をとった。2019 年 11 月の決議の投票に際して 36 団体は連名で、決議や草案にある用語は曖昧であり、「人権の行使、並びに社会的・経済的発展の促進に向けたインターネットの利用を損なう」[52] として、各国に反対票を投じることを呼びかけたのである。

（ウ）GCSC による最終報告書の公表

2019 年には国連外でも GCSC が 11 月に最終報告書を公表し、2017 年以来の取組に区切りをつける注目すべき動きがあった。GCSC はマルチ・ステークホルダーを体現するプロセスであり、オランダのハーグ戦略研究所（Hague Centre for Strategic Studies）と米国のイースト・ウェスト・インスティテュート（EastWest Institute）が事務局機能を担っている。委員会メンバーには日米欧諸国のみならず、露中等、様々

49 Allison Peters, “Russia and China Are Trying to Set the U.N.’s Rules on Cybercrime: At the United Nations General Assembly, the United States Must Push Back Against Their Agenda,” *Foreign Policy,* September 16, 2019, https://foreignpolicy.com/2019/09/16/russia-and-china-are-trying-to-set-the-u-n-s-rules-on-cybercrime/.

50 UNGA, 72nd Session, Draft United Nations Convention on Cooperation in Combating Cybercrime, UN Doc. A/C.3/72/12 (October16, 2017), https://undocs.org/A/C.3/72/12.

51 “Statement on Agenda Item 107 ‘Countering the Use of Information and Communications Technologies for Criminal Purposes,’” United States Mission to the United Nations, November 18, 2019, https://usun.usmission.gov/statement-on-agenda-item-107-countering-the-use-of-information-and-communications-technologies-for-criminal-purposes/.

52 “Open letter to UN General Assembly: Proposed International Convention on Cybercrime Poses a Threat to Human Rights Online,” Association for Progressive Communications, November 2019, https://www.apc.org/en/pubs/open-letter-un-general-assembly-proposed-international-convention-cybercrime-poses-threat-human.

な国々の専門家たちが名を連ねる。また委員会にはパートナーとスポンサーも存在し、前者には例えばオランダ政府やフランス外務省が、また後者には日本の総務省が含まれている。

こうした仕組みになった理由は、GCSC が既存の 2 つの取組の系譜に連なって設立されたことにある[53]。1 つ目の取組は、2014 年 1 月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[54]）と英国のチャタム・ハウス（Chatham House）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（GCIG[55]）である。GCIG が発足した背景には、権威主義諸国の政策が自由で開かれ、普遍的なインターネットの利用を脅かすとの懸念があり、2016 年に「ワン・インターネット（One Internet）」と題された最終報告書を公表してその取組は区切りを迎えた[56]。

2 つ目の取組は、2011 年に英国が主導して開催されたサイバー空間に関する国際会議である。同会議はその後、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、一連の取組はロンドン・プロセスと称されている。このプロセスはマルチ・ステークホルダーによる参加を特徴としており、国連等の国際機関で国家が中心となった議論を重視する露中の取組とは対照的な取組であった。

これら 2 つのプロセスを発展させる形で、オランダが 2017 年のミュンヘン安全保障会議で提唱して形成されたのが GCSC であり、2019 年 11 月に最終報告書を公表するに至ったのである。GCSC の成果の 1 つとして、GGE 等の既存の取組に基づきつつ、8 つの項目からなる規範を提起したことが挙げられる[57]。かかる規範には、例えばインターネットの公共的な核心（Public Core of Internet）の保護や選挙に欠かせない技術インフラの保護といった、GGE の規範にはない独自の要素も含まれていた。またもう 1 つの成果は、マルチ・ステークホルダーによる関与や国際法の順守といった要素を含む「サイバー安定化枠組み」を提示したことである[58]。そして、これら規範や枠組みの実践には「調和的かつグローバルなマルチ・ステークホルダーによる努力が欠かせない」[59] として、そこに推進力を与えるところに GCSC は自らの取組の意義を見

53 GCSC の歴史については次を参照。“Advancing Cyberstability: Final Report,” GCSC, November, 2019, pp. 46-47, https://cyberstability.org/wp-content/uploads/2020/02/GCSC-Advancing-Cyberstability.pdf.
54 Centre for International Governance Innovation の略称。
55 Global Commission on Internet Governance の略称。GCIG については例えば次を参照。“Global Commission on Internet Governance,” Chatham House, https://www.chathamhouse.org/about/structure/international-security-department/global-commission-internet-governance-project.
56 “One Internet,” CIGI and Chatham House, https://www.chathamhouse.org/sites/default/files/publications/research/2016-06-21-global-commission-internet-governance.pdf.
57 GCSC, “Advancing Cyberstability,” pp. 21-22.
58 Ibid., p. 14.
59 Ibid.

出すのである。

こうした成果は、必ずしも自由主義陣営にのみ裨益するものではない。むしろ GCSC は、両陣営の対立から距離をとって、サイバー空間が生み出す利益を確保するために双方がともに擁護すべき基本事項を示すことに力点を置いたと解せる。とはいえ、マルチ・ステークホルダー協力を体現するプロセスは自由主義陣営の取組に連なるものであり、委員会のパートナーやスポンサーをみても、同陣営により親和性のあるプロセスだと指摘されている [60]。このようにみると GCSC のプロセスには自由主義陣営の思惑、すなわち非国家主体も巻き込むことで国際場裏での交渉力を強め、それによって特に国連で強まる権威主義陣営の存在感を相対化しようとする意向が投影されているように見受けられる。

（2）仮説の検証と事例を踏まえての包括的な考察

以上の事例研究を踏まえて仮説の妥当性を検討してみると、国連サイバー犯罪条約に関連した決議の採択事例だけをみれば、現状、仮説は成り立たず、両陣営の利益構造は「ゼロサム」のようにみえる。開催予定のオープンエンド・アドホック政府間専門家委員会の準備委員会に対して、既に日米英豪加と EU は、議論は透明性をもって参加国のコンセンサスに基づき進められるべきとのコメントを公表し、権威主義陣営側を強くけん制している [61]。同委員会の今後の展開は予断できないが、権威主義陣営を利するプロセスになりかねないとの懸念から、両陣営は真っ向から対立している。

しかし、「ゼロサム」ゲームでは、OEWG と GCSC に関する両陣営の動きは説明できない。その理由としてはまずもって、両陣営は対立しながらも議論を続けている事実が挙げられる。両者は GGE と OEWG に関する決議において互いに反対票を投じるも、結局のところ自由主義陣営は OEWG へ、権威主義陣営は第 6 回 GGE へ参加した。仮に両者がそれぞれが主導するプロセスへの参加を固辞したとすれば、そうした事態は表 1 のセル B・C にある結果をもたらし得るのであり、両陣営は自らの利得を最大化する機会を逸することになる。利得の最大化を目指すのであれば、両者はそれぞれのプロセスに参加し、自らにとって好ましい結果（自由主義陣営にとってはセル A、権威主義陣営にとってはセル D）がもたらされるよう取組む方が良い。両陣営の GGE や OEWG への参加には、まさにこうした利益構造が現れている。

さらに、権威主義陣営が設置を提案した OEWG に、自由主義陣営側が重視するマ

60 Ruhl, Hollis, Hoffman, and Maurer, “Cyberspace and Geopolitics,” p. 10.

61 各国のコメントは次のサイトで確認できる。“Ad Hoc Committee Established by General Assembly Resolution 74/247: Comments from Member States,” UN Office on Drugs and Crime, https://www.unodc.org/unodc/en/cybercrime/cybercrime-adhoc-committee.html.

ルチ・ステークホルダー協力を促す仕組みが導入されたことも、仮説の妥当性を印象付けた。国家の役割を重視する権威主義陣営の立場を踏まえれば、OEWG への非国家主体の参加を認めない選択もあったと考えられる。仮にそうなれば、マルチ・ステークホルダーを体現する GCSC プロセスとの競合は際立つ。だが、同プロセスには自由主義陣営の交渉力強化という側面も見出せる故に、権威主義陣営が敢えてそうした選択を行ったとしても不思議ではなかった。しかし実際には権威主義陣営は、会期間会合といえど、非国家主体も OEWG に参加できる機会を設けた。そしてこれによって GCSC は、その成果を国連のプロセスにインプットする好機を得たのであり[62]、それは提言を実践する機能に欠く GCSC の弱点[63]を補う意義を有するものとなったのである。

こうしてみると、権威主義陣営は、自由主義陣営に対する譲歩、あるいは協力する意図があることを示すシグナルを発したとも解釈できる。表 1 に当てはめれば、セル C の結果が招かれる可能性もあった中、権威主義陣営は自らの利得の最大化を目指してセル D を追求したといえる。もっとも、OEWG がマルチ・ステークホルダー協力を促進する実質的機能を果たし得るかには、会期間会合へのロシアや中国といった国々からの非国家主体の参加が限定的であったこともあって疑念が残される。今後の動向によっては、プロセスをめぐる両陣営の角逐が先鋭化し得る点には留意が必要である。

こうした結果を念頭に置いて、「自由・開放」と「主権・統制」を両極端とする線上で進む両陣営の調整は、いずれを基調とした規範形成へと向かい得るかを考えてみると、目下の状況には「主権・統制」へと向かう潮流が観察できるといえる。事例研究やこれまでの考察からは、権威主義陣営がけん引する形で「両性の闘い」ゲームが進んできたことが浮き彫りになる。特に各種国連決議を主導したロシアは規範起業家として目を引く役割を果たしてきたといえ、「デジタル・ディサイダーズ」を巧みに取り込んできたと指摘できる。

この潮流に自由主義陣営が抗するためには、やはり「デジタル・ディサイダーズ」の取り込みを視野に入れつつ、非国家主体との協力を深めていくことが課題になる。先行研究を概観した際に触れたように、非国家主体は国家の政策にも影響を与える重要な規範起業家として機能し得る。マイクロソフトや GAFA といった強力なアクターが存在するサイバー空間ではなおさらその存在は大きい。この点に検討を加えるためには、2 つの陣営に非国家主体も含めた三つ巴の関係性を捉える視点が必要といえ、それは既述のように今後の課題となる。

62 “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/.

63 Ruhl, Hollis, Hoffman, and Maurer, “Cyberspace and Geopolitics,” p. 10.

おわりに

本稿を締めくくるに当たり、ここでは本研究の今後の課題を検討する際に注目される事象やそこでの自由主義陣営の政策課題について簡単に触れたい。

まず自由主義陣営と非国家主体との協力の深化が求められるという点では、2018 年 11 月にフランスのエマニュエル･マクロン（Emmanuel Macron）大統領が提唱した「サイバー空間の信頼性と安全性のためのパリ・コール」[64] が注目される。パリ・コールは、既存の取組に基づきつつサイバー空間の規範に関する 9 つの基本原則を掲げるものであり、ブダペスト条約の重要性も再確認する内容となっている。その最大の特徴は、80 近くの国家と、600 以上の企業等を賛同者に含めていることにあり [65]、マルチ･ステークホルダー協力の一大潮流を生み出す可能性を秘める。自由主義陣営としては、こうしたプロセスに「デジタル・ディサイダーズ」も取り込むなどして、国連を舞台とする権威主義陣営の巧みな外交戦術を相対化することが求められる。それにもかかわらず、露中は当然としても、米国も賛同者に含まれていない点は問題であり、その参加を促すことが自由主義陣営にとっての喫緊の課題となる。

この文脈で米国の同盟国であり、かつ GCSC やパリ･コールといったマルチ･ステークホルダー協力を積極的に支持する日本の役割は大きい。加えて、日本は「デジタル・ディサイダーズ」の取り込みという点でもその役割が期待される。より具体的には、ASEAN への関与である。ニュー・アメリカの研究は、国際場裏での存在感を加味して、自由主義陣営が特に関与を強めるべき第 3 群として 20 か国を挙げる。そこにはインドネシア、シンガポール、マレーシアも名を連ねており、ASEAN は注目すべき対象となっている [66]。実際、第 6 回 GGE と OEWG の設置に関する決議で ASEAN 諸国は興味深い投票行動を示した。前者に関しては、多くの ASEAN 加盟国が賛成に回った中、中国との関係が強いとされるカンボジア、ラオス、ミャンマーは棄権した [67]。また後者に関しては、全 ASEAN 諸国が賛成票を投じている [68]。こうした投票行動を示す ASEAN を、権威主義陣営に与しないよう仕向けることは容易ではない。とはいえ、サイバーセキュリティ能力構築支援を実施するなど、ASEAN との信頼関係を地道に構築してきた日本が「デジタル・ディサイダーズ」の中でも重要な位置にある ASEAN にどう関与するかは、自由主義陣営の一員として問われる課題となる。

64 “Paris Call: For Trust and Security in Cyberspace,” Paris Call, November 12, 2018, https://pariscall.international/en/.
65 Ibid.
66 Morgus, Woolbright, and Sherman, “The Digital Deciders,” pp. 32-34.
67 UN Doc. A/73/505, p. 4.
68 Ibid., pp. 2-3.

さらに本稿では規範形成に焦点を当てたが、規範の順守も論点となる。理論上、「両性の闘い」においては、アクターは決定された規範から「逸脱するインセンチィブをもたない」[69] ため、「とくにルールを守らせるための装置は必要ではない」[70] ことになる。ここで考慮すべきは、規範形成に係る利益の分配問題と、その順守に係る「囚人のジレンマ」問題との間には一定のトレード・オフが存在することである。例えば、自由主義陣営が譲歩して「主権・統制」を基調とした規範形成が進むのであれば、規範の順守において権威主義陣営側が裏切るリスクを局限できるかもしれず、その逆もしかりである。もっとも裏切りの可能性が否定できない以上、「囚人のジレンマ」ゲームではプレイヤーに規範を順守させる仕組みが欠かせない [71]。この文脈で EU が 2019 年 5 月に導入したサイバー制裁レジームがどのような発展をみせ、また同レジームをめぐって自由主義陣営がいかに協力していけるかは注目に値する [72]。

（防衛研究所）

69 山本『国際レジームとガバナンス』、83 頁。
70 同上。
71 同上、82 頁。
72 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.

［付記］本稿の完成にあたり、査読者の先生から細部に至るまで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。