防衛研究所 National Institute for Defense Studies
NIDSコメンタリー
特集：「新領域の安全保障」vol.4
第 322 号　2024 年 5 月 21 日

サイバー国際規範をめぐる戦い

――国連を舞台とした日米欧諸国と露中等との対立

政策シミュレーション室/サイバー安全保障研究室　主任研究官　原田　有

はじめに

デジタル技術の進歩は、サイバー攻撃を駆使した戦いだけでなく、サイバー空間での責任ある行動に関する国際的な規範（サイバー国際規範）[1]の在り方をめぐる、もう一つの戦いも生んだ。どのような規範が形成・適用されるかは、各国のサイバー安全保障政策の策定・実行にかかわる問題となる。それゆえ国際場裏では、規範の「内容」はもとより、自らにとって好ましい規範形成を推進するための「場」の創出をめぐっても国家間対立が発生し、特に日米欧諸国と露中等とが対峙する構図が鮮明化してきた。既存の国際法の適用を主にサイバー国際規範を検討すべきとする前者と、デジタル技術の特性を理由に新たな条約等の策定を目指す後者との角逐は、「法的闘争（legal power play）」や「法戦（lawfare）」とも形容され[2]、サイバー国際規範の動向に影響を与える要因と目されている。本コメンタリーでは、両者が国際連合（国連）を主たる舞台に繰り広げてきた「場」をめぐる争いを概観する。

国連で長らくサイバー国際規範形成に向けた「場」となってきたのは、2004 年から始動した国連政府専門家会合（GGE）[3]であった。2019 年からは扱う議題を重複させるオープンエンド作業部会（OEWG）[4]も新設され、GGE の取組が 2021 年に一区切りをつけるまでの間、GGE と OEWG が併存するデュアル・プロセス状態となった。取組を非効率的・非生産的にしかねないと懸念された 2 つの「場」の設置は、ともにロシアが主導したものであり、そうした取組を中国等は支持する一方、日米欧諸国はほとんどの場面で消極的な姿勢、ないしは反対の意を示してきた。その日米欧諸国は、2025 年に OEWG が閉会する機会を捉えて、目下、新たな「場」となる行動計画（PoA）[5]と呼ばれる枠組みの導入を推進している。これに対して特にロシアは強く反対して OEWG 継続を訴えており、PoA と OEWG が併存するデュアル・プロセスの再現が懸念されている。サイバー国際規範を形成する必要性が認識されながら、それを議論するための「場」すらも争う現状に目を向けるべく、以下ではこれまでの経緯を簡単に振り返ったうえで、PoA をめぐる直近の動向を俯瞰する。そして、PoA は露中等にとって好ましい「場」として機能し得る可能性もあり、日米欧諸国に利する「場」となるかは予断できないことを指摘する。

規範形成プロセスの複雑化－デュアル・プロセスの出現

国連でのサイバー国際規範をめぐる議論は、1998 年にロシアが提出した決議案「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」[6]が国連総会で無投票採択されたことを受けて本格化した。情報通信技術の発展が生む新たな脅威の高まりに既存の国際法では十分に対応できないとして、ロシアは国際的な法的枠組みを設ける必要性を訴えた[7]。折しも米国では同年、「情報作戦に関する統合ドクトリン」が策定された[8]。情報通信技術の軍事利用が進む中、ロシアとしては米国との二国間対話で情報通信技術に関するセキュリティの在り方を検討しようとしたが期待する成果が得られなかったため、国連を舞台とするルール作りを志向するようになったとされる[9]。

そのロシアが問題を議論する「場」として開催を提案したものが GGE であった[10]。2004 年から 2005 年にかけて初めて開催された GGE はその後、2021 年までの間にさらに 5 回、計 6 回の会期を開き、参加国も当初の 15 か国から 20 か国、そして 25 か国へと拡大させていった[11]。GGE は参加国のコンセンサスに基づき議論の成果が報告書として公表される仕組みとなっており、これまで第 2 会期～第 4 会期と第 6 会期の計 4 回、報告書の公表に成功している。中でも第 3 会期（2012～2013 年）と第 4 会期（2014～2015 年）はそれぞれ、サイバー空間に「国際法、特に国連憲章が適用可能」であることを確認した点、任意で拘束力は無いながらも国家の責任ある行動に関しての 11 の行動規範を示した点で大きな成果を収めた会合となった。

国連を舞台にしたロシアの取組を初期段階から支持してきた国の 1 つが中国である。ロシアの決議案「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」は国連に毎年提出されているが、同案が初めて複数国による共同提案となった 2006 年から最新の 2023 年の決議案に至るまで、中国はほぼ一貫して共同提案国となっている。中国が共同提案国とならなかったのは、日米欧諸国とロシアが共同提案する形となった例外的な 2021 年の決議案だけである。さらに中国は、2011 年と 2015 年にはロシア等と「情報セキュリティのための国際行動規範」も国連に提出している[12]。この提案は折しも、2011 年の「アラブの春」と 2014 年の香港での学生・民主派団体による政府への抗議活動と時を同じくして行われた。国外からだけでなく、国内からのデジタル手段を用いた脅威にも対処できるようなルール作りを国連を舞台に進めていく点で、露中の利害は一致してきたといえる。

他方、そうした露中等の取組に日米欧諸国は消極的な姿勢、ないしは反対してきた。特に当初、米国の反発は強かった。2005 年から 2008 年にかけてロシアが主導する決議案「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」が国連で投票にかけられた際には、唯一米国だけが反対票を投じている。また、GGE が第 1 会期（2004～2005 年）を開催すると米国も会合に参加したものの、モスクワ国際関係

大学（MGIMO）のレポートによれば、参加 15 か国中、米国だけが軍事・政治的側面に関する項目への言及に反対したため、報告書の公表に至らなかったとされる[13]。

国連を自らにとって好ましい規範を形成するための「場」と位置付けた露中等に対して、日米欧諸国は初め、国連外の「場」を重視する姿勢を示した。英国が呼びかける形で、サイバー空間に関する国際会議が開催され、2011 年にロンドンで初めて開かれた会議はその後、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。日米欧諸国は非国家主体とも協力するマルチ・ステークホルダー形式を重視しており、同形式を体現するロンドン・プロセスは、露中等が推進する国家中心の国連を舞台とする取組を相対化するものといえた。換言すれば、日米欧諸国にとって非国家主体との協力は、サイバーセキュリティの実務上で欠かせないだけでなく、露中等の取組に対抗する外交カードにもなってきたとみることができる。それに対して露中は、ロンドン・プロセスに参加しながらも、「情報セキュリティのための国際行動規範」に基づく新たな規範の策定や国連を議論の「場」とする必要性を訴えて、自らの取組の正当性を主張した[14]。

このように 2000 年代初頭、国連内外でサイバー国際規範の形成に向けた取組が進められたが、次第に議論の「場」としての比重を増したのは GGE であった。ロンドン・プロセスは停滞した一方、GGE は先述の通り、既存の国際法の適用や 11 の行動規範を示した報告書の公表に成功するなど、着実に成果を収めていったのである。

そうした矢先、「場」をめぐる争いは突如として新たな局面を迎えた。GGE 第 5 会期（2016～2017 年）が成果報告書の公表に至らずに閉会すると、2018 年、ロシアは中国、キューバ、北朝鮮、イラン、シリアなどを共同提案国として決議案「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」を提出し、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、新たに OEWG の設置を求めたのである。OEWG は、参加国が限定されていた GGE とは異なり、国連全加盟国の参加を可能とし、加えて非国家主体の参加も限定的ながら認める点に特徴があった。同決議案には日米欧諸国等 46 か国が反対したが賛成多数で可決され、2019 年～2021 年にかけての OEWG 開催が決まった[15]。

一方、日米欧諸国は同じく 2018 年に、露中等の取組に対抗して GGE 継続を求める決議案「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」を提出した。同決議案は、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す内容となっており、OEWG を意識したものであった。同決議案も、露中、キューバ、北朝鮮、イラン、シリア等の 12 か国が反対するも賛成多数で可決され、2019 年～2021 年にかけての GGE 第 6 会期の開催が決定された[16]。

日米欧諸国と露中等との対立の結果、サイバー国際規範の形成に向けた国連での取組は OEWG と GGE から成るデュアル・プロセス状態に至り、取組の非効率性・非生産性が懸念される事態に陥った。興味深い点は、マルチ・ステークホルダー形式を体現する OEWG を露中等が推進し、同形式を推進してきた日米欧諸国はむしろ参加者が国家に限定される GGE の継続を訴えて OEWG の開催に反対するという、ねじれが生じたことである。

この矛盾を解くカギは、露中等にとって好ましいサイバー国際規範を推進するための「場」であったはずの GGE が、第 3 会期でサイバー空間に「国際法、特に国連憲章が適用可能」であることを確認したことを経て、既存の国際法の適用を重視する日米欧諸国に利する「場」と化したことに見出せる。GGE を日米欧諸国に乗っ取られた結果、露中等は、全加盟国と非国家主体にも門戸を開く比較優位性を打ち出して OEWG を設置する正当性を演出し、自らにとって好ましい「場」を新たに設けたといえる[17]。

その後、デュアル・プロセスをより建設的な取組にしようとする兆しもみられたが[18]、両者が対立する基本的な構図は変わらなかった。第 1 回 OEWG と GGE 第 6 会期とで議論が続く最中の 2020 年、2 回目の OEWG を 2021 年～2025 年に開催することを提案する決議案を露中等が国連に提出すると日米欧諸国は時期尚早として反対、同提案は賛成多数で可決されるも両者は再び鋭く対立した[19]。一転、2021 年には、第 1 回 OEWG と GGE 第 6 会期がそれぞれ報告書のコンセンサス採択に成功したともに、日米欧諸国とロシアが共同提案国に名を連ねて決議案「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」を提出するという、両者の接近もみられた。しかしそれは、それぞれが推進する「場」で成果を収めたい双方の実利が一致した結果といえ、実質的な歩み寄りを意味するとは捉え難かった。実際、第 2 回 OEWG が始まると両者の対立は再燃した。

分断の深化が懸念される現状－デュアル・プロセス **2.0** の出現？

第 2 回 OEWG は開催当初から、日米欧諸国と露中等が非国家主体の参加形態をめぐって対立する状況となった。既述の通り、前者はマルチ・ステークホルダー形式を、後者は国家中心の枠組みを重視する立場にある。それゆえ、一見すると微々たるようにもみえるこの論点は、OEWG が自身に利する「場」となるか否かを決する両者にとっての要点であり、新たな会合の開催に当たって改めて争点化したのである。

そもそも、非国家主体にも参加の門戸を開く OEWG を推進してきたのは露中等であったが、その念頭にはあくまで、非国家主体の「限定的」な参加があった。第 1 回 OEWG でも、非国家主体はオブザーバー参加を基本とし、国連経済社会理事会との協議資格を得ている非政府組織（NGOs）[20]は別として、資格を得ていない組織については国連加盟国からの反対がなければ公式会合への参加が可能という形態で

あった[21]。実際には協議資格を持たない NGOs の参加希望は一部加盟国によって拒否され、その理由も不透明という状況にあった[22]。協議資格に関係なく、多様な NGOs が参加できたのは公式会合の合間に開かれる非公式会合に限られていたのである。この参加形態を第 2 回 OEWG でも踏襲することが検討されていたが、これを日米欧諸国は不服とし、協議資格を有さない NGOs の公式会合への参加も認めるとともに、参加の拒否は透明性をもって行われるべきことを求めた[23]。他方、露中、キューバ、イラン、シリア等は前回と同様の参加形態にすべきとして日米欧諸国の提言に反対した[24]。

非国家主体の参加形態についての方針がようやく定まったのは、第 3 会期（2022 年 7 月）を控えた 2022 年 4 月のことであった。同方針では、引き続き協議資格の有無で NGOs の扱いを分けた上で、資格のない組織の参加への反対は慎重に行うことを加盟国に奨励するとともに、反対の理由を任意で OEWG 議長に知らせるべきことが示された[25]。新たな方針は基本的には前回の参加形態を踏襲しつつも、反対のハードルを少し上げるという、妥協の産物となったことが分かる。実際のところ、同方針が適用されて以降も参加を拒否される NGOs は引き続き多く出た。なお、欧米系組織の参加はロシア等が拒否しているとされる[26]。拒否の理由は明らかではないが、一般論として、国連での議論への参加を求める欧米系の NGOs は国家が情報通信を強く統制することには反対であるため、国家による統制を重んじるロシア等にとってその存在は都合が悪い。加えて、日米欧諸国に連なりかねない非国家主体の参加を許すことで、OEWG が自身に利する「場」として機能しなくなることをロシア等は懸念したとも考えられる。

参加者の範囲という基本的事項から議論を紛糾させた第 2 回 OEWG はその後、具体的な成果も収めつつ[27]、2024 年 3 月に第 7 会期を開催、2025 年の最終報告書の公表に向けてプロセスは終盤を迎えている。もっとも、OEWG も GGE と同様にコンセンサス方式が導入されているため、無事に最終報告書が公表されるかは予断できない。そして今まさに、コンセンサスを難しくしかねない問題として争点となっているのが、第 2 回 OEWG 後の「場」の在り方である。

OEWG 後の「場」について、日米欧諸国は 2022 年と 2023 年、行動計画（PoA）と呼ばれる新たな協力枠組みの立ち上げとその常設化を盛り込んだ決議案を提出し、いずれも 160 か国近い賛成を得て採択された[28]。大多数の国が新たな枠組みの導入を支持していることが分かるが、露中、北朝鮮、イラン、シリアといったごく一部の国は反対票を投じ、代わりに、PoA の立ち上げを前提とはせず、第 2 回 OEWG で新たな「場」について議論を深めていく必要性を訴える決議案を提出している[29]。露中等の提案に日米欧諸国を中心とした 50 か国以上は反対票を投じるも、同決議も賛成多数で採択され、決議が競合する局面が再び訪れた。

もともと PoA は 2020 年に、フランスとエジプトが主導し、日本や欧州諸国を中心とした 40 か国以上が賛同して導入が提案されたものであり、GGE と OEWG のデュアル・プロセスに終止符を打って、国連

に新たな常設の「場」を設けようとする試みであった。より具体的には PoA は、合意済みの事項から実際の適用・具体的な協力を進めつつ、変化する脅威に応じて追加的な規範の検討も視野に入れるとともに、非国家主体との協力も重視する内容であった[30]。PoA は合理的な取組であるといえた一方、新たな条約等の策定を早急に求めるロシア等の取組をけん制する点では日米欧諸国に利する「場」を提供し得る取組でもあった。先述の通り、こうした提案の最中にロシアは 2 回目の OEWG 開催を推進したのであり、PoA をめぐる議論も第 2 回 OEWG へ持ち越されることとなった。

PoA の在り方は現在まさに議論中であり、その細部は未定である。日米欧諸国間でも PoA の在り方についての統一的な見方がある訳ではないが、おおよそのところ、既存の国際法の適用に関する検討の推進、非国家主体がより積極的に関与できる参加形態の導入、一連の取組を推進するための定期的な会合の設置、そして効果的な能力構築支援の実施が目指されている[31]。他方、フランスとともに PoA を主導したエジプトは、法的拘束力のある義務の策定も視野に入れるとともに、非国家主体の参加形態については第 2 回 OEWG の形式を踏襲して極力限定することを志向している[32]。

そうしたエジプトの立場は、PoA に反対するロシアの立場に近い。PoA を西側諸国の政治的な意味合いが込められた取組とみなすロシアは[33]、2023 年、ベラルーシ、キューバ、北朝鮮、シリアなどとともに OEWG の常設化を提案した。同提案は、将来的な条約の策定を視野に入れるとともに、非国家主体の常設 OEWG への参加は厳しく限定（国連加盟国の承認をうけた組織のみ公式なイベントにオブザーバー参加を認め、それ以外の組織については会期間会合といった非公式会合への参加のみ認める）する内容となっている[34]。ロシアは同年、この提案に先駆けて、ベラルーシ、北朝鮮、ニカラグア、シリア、ベネズエラとともに最新の条約案も公表している[35]。ロシアは、PoA の枠組み導入が大多数によって支持されている状況、そしてウクライナ侵略による国際的な信頼の失墜もある中で、自身の主導権を確保しようと躍起になっているようにみえる。

ここで興味深い点は、OEWG の常設化と最新の条約案に関するロシアの提案に中国は共同提案国として名を連ねていないことである。さらに言えば中国は、ロシアとは異なり、PoA の枠組み導入には必ずしも明確に反対はしていない。露中間には微妙な立場の違いが観察でき、両者の間で意見相違が生じている可能性や、ロシアによるウクライナ侵略もある中で中国はロシアの取組を表立って支持することに慎重になっている可能性などが考えられる。もっとも、中国は国連での投票といった節目ではロシアを支持している。また中国は、第 2 回 OEWG の最新の会合となる第 7 会期において、OEWG 後の国連での取組は新たな規範や法的枠組みの策定を視野に入れたものであるべきことや[36]、ロシア等が提案する条約案は新たな法の策定に向けた議論の良い土台になるとの見解も示している[37]。中国の政策的立ち位置は依然として日米欧諸国よりもロシアに近く、日米欧諸国と露中等とが対立する構図に変わりはない。

デュアル・プロセスを終わらすべく提案されたはずの PoA は、日米欧諸国と露中等との対立を背景に、今やデュアル・プロセスを再来させかねない争点となっている。対立の狭間に置かれている国からは、こうした現状に対する懸念が示されており、例えばブラジルは「場」を争う各国に自制を求め、まずは第 2 回 OEWG での議論に集中すべきであると訴えている[38]。冗長的なプロセスは、国連を通じた取組に割ける資源が限られている小国や途上国の議論への効果的な参加を難しくする。また対立による分断の深まりは、サイバー国際規範の普遍性や意義も損ないかねない[39]。サイバー空間に起因する脅威への対処に国際的な協力が不可欠であるといわれて久しいが、対話の「場」すら定まらない現状からは協力に向けた道のりの険しさがうかがえる。

おわりに

本コメンタリーでは、デジタル技術をめぐるもう一つの戦いである、サイバー国際規範の形成に向けた「場」をめぐる日米欧諸国と露中等との対立を概観してきた。両者の対立は、米国が露中等の権威主義国によるデジタル技術の悪用への対抗を鮮明にさせてきたことも相まって[40]、さながら「民主主義陣営」対「権威主義陣営」の様相を呈している。もっとも、実際の状況は特定の政治体制でグループ化できるほどに単純ではなく、そもそも各陣営の足並みも一致している訳ではない。従って、二項対立的な言説は実態と乖離した、無用な対立を助長しかねない見方とも解されている[41]。他方、「場」をめぐる争いという具体的な問題を通してみたとき、両者の対立は言説にとどまらない具体像としても捉えられる。両者は、陣営内の見解相違よりも陣営間の見解相違の方を際立たせており、その対立関係は、大国間競争という時代背景とも相まって、その他の国々も巻き込みながら規範形成の動向に影響を与えてきた。対立軸の鮮明化は、国際社会の分断を深化させかねない懸念を生むのであり、むしろ戦いを言説レベルにとどめておけるかが要点になるともいえる。そして両者の歩み寄りが求められる中、デュアル・プロセスを終わらせるべく導入の検討が始まった PoA がその当初の目的を果たし、国連での取組が普遍的で意味あるサイバー国際規範の形成へと向かっていくことが期待される。

両者の歩み寄りという文脈で注目されることは、日米欧諸国も露中等もお互いの取組に反発しつつも、ひとたび「場」が設けられれば、そこに参加して積極的に発言するプラグマティックな態度を示してきた事実である。そうした経緯を踏まえれば、PoA に特に反発しているロシアも、いざ PoA の枠組みが立ち上がれば、そこへ参加することになろう。実際のところ、デュアル・プロセスの解消を目指して発案された PoA は露中等に利する「場」として機能する可能性もある。PoA に関する決議では「追加的な法的拘束力のある義務」も必要に応じて検討することも視野に入れられているが[42]、これはおそらく新たな条約等の策定を目論む露中等の歩み寄りを促す目的だと考えられる。さらに、既述の通りエジプトが想定す

る PoA の在り方はロシアの立場に近い。PoA の詳細は今後の議論によって決まるのであり、果たして日米欧諸国に利する「場」となるかは予断できない。日米欧諸国には、サイバー国際規範の普遍性や意義を損ないかねない国家間の分断の深化を避けながら、自らにとって好ましい規範形成に向けた潮流を確たるものにする「場」として PoA を機能させていくための難しいかじ取りが求められている。PoA を当初から支持してきた日本としても、サイバー安全保障政策の策定・実施に関わる問題にいかに建設的に貢献していけるかは重要な課題となる。

1 サイバー空間のガバナンスに関して、例えば GGE における議論では「既存の国際法の適用」と「任意の法的拘束力のない規範」とに論点が分けられ、国際法と規範は別の項目として整理されている。他方、国際法も規範も「サイバー空間に関するアクターの適切な行為基準」を示すものであることから、本稿では両者を包括的に扱って「サイバー国際規範」と表現する。

2 Peter B.M.J. Pijpers, "Legal Power Play in Cyberspace: Authoritarian and Democratic Perspectives and the Role of International Law," *Hybrid CoE Paper* 19 (February 2024), https://www.hybridcoe.fi/wp-content/uploads/2024/02/20240222-Hybrid-CoE-Paper-19-Legal-powerplay-in-cyberspace-WEB.pdf.

3 Group of Governmental Experts の略称。

4 Open-ended Working Group の略称。

5 Programme of Action の略称。

6 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.

7 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), pp. 8-10, available from undocs.org/A/54/213.

8 Joint Chiefs of Staff, "Joint Pub 3-13: Joint Doctrine for Information Operations" (9 October 1998), https://www.c4i.org/jp3_13.pdf.

9 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), p. 3, https://ict4peace.org/wp-content/uploads/2012/08/Eneken-GGE-2012-Brief.pdf.

10 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.

11 GGE には、各国の専門家が個人の資格で参加する仕組みとなっている。

12 UNGA, *International Code of Conduct for Information Security*, A/66/359 (14 September 2011), available from undocs.org/A/66/359; UNGA, *International Code of Conduct for Information Security*, A/69/723 (13 January 2015), available from undocs.org/A/69/723.

13 A.V. Krutskikh and E.S. Zinovieva, eds., *International Information Security: Russia's Approaches*, Moscow State Institute of International Relations (MGIMO) (2021), p.12, https://mgimo.ru/upload/iblock/b82/g6094u9tlacl34xj4ew6juxd6p508cug/%D0%94%D0%BE%D0%BA%D0%BB%D0%B0%D0%B4%20%D0%B0%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9.pdf.

14 外務省「サイバー空間に関するブダペスト会議」（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。

15 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/A/RES/73/27.

16 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.

17 この点については次を参照。原田有「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」『安全保障戦略研究』第 2 巻第 2 号（2022 年 3 月）、233～250 頁、https://www.nids.mod.go.jp/publication/security/pdf/2022/202203_12.pdf。

18 2019 年、ロシアが主導する決議案「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」では OEWG と GGE 双方の重要性が示され、国連総会での採択においては、米英、カナダ、イスラエル等の 6 か国は引き続き反対するも、日豪や多くの欧州諸国は棄権に回った。UNGA, *Official Records*, A/74/PV.46 (12 December 2019), p. 6, available from undocs.org/A/74/PV.46.

19 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/A/RES/75/240.

20 Non-governmental Organizations の略称。

21 第 1 回 OEWG での非国家主体の参加形態については次を参照。"Letter from the Chair," UN Office for Disarmament Affairs (UNODA) (15 November 2021), especially footnote no.1 , https://documents.unoda.org/wp-content/uploads/2021/11/OEWG-2021-2025_Chairs-letter_final.pdf.

22 Josh Gold, "A Multistakeholder Meeting at the United Nations Could Help States Develop Cyber Norms," Council on Foreign Relations (16 January 2020), https://www.cfr.org/blog/multistakeholder-meeting-united-nations-could-help-states-develop-cyber-norms.

23 "Letter from the Multistakeholder Community to the OEWG Chair," EU Cyber Direct (13 December 2021), https://eucyberdirect.eu/news/letter-from-the-multistakeholder-community-to-the-oewg-chair.

24 第 2 回 OEWG への非国家主体の参加形態に対する各国の見解や一連の流れは、次のウェブサイトに詳しい。"Modalities of Multistakeholder Participation," Digital Watch (13 December 2021), https://dig.watch/event/un-oewg-2021-2025-1st-substantive-session/modalities-of-multistakeholder-participation.

25 "Letter from the Chair," UNODA (22 April 2022), https://documents.unoda.org/wp-content/uploads/2022/04/Letter-from-OEWG-Chair-22-April-2022.pdf.

26 なお MGIMO などロシア系の組織の参加も拒否されており、ウクライナが拒否権を行使しているとみられる。非国家主体の参加形態に関する方針決定後の状況については例えば次を参照。"Results of the Accreditation of Stakeholders to the OEWG 2021-2025 Raises Concerns," Digital Watch (21 Jul 2022), https://dig.watch/updates/results-of-the-accreditation-of-stakeholders-to-the-oewg-2021-2025-raises-concerns; "Stakeholder Engagement," What's New with Cybersecurity Negotiations: The OEWG 2021–2025 Annual Report Adopted, Diplo (13 August 2022, updated 4 April 2024), https://www.diplomacy.edu/blog/whats-new-with-cybersecurity-negotiations-the-oewg-2021-2025-annual-report-adopted/.

27 主要な成果には例えば、信頼醸成措置の一環として、インシデント発生時などに国家間で意思疎通を図れるようにするための各国の連絡窓口（Global POC Directory）の整備が挙げられる。

28 UNGA Resolution 77/37, *Programme of Action to Advance Responsible State Behaviour in the Use of Information and Communications Technologies in the Context of International Security*, A/RES/77/37 (12 December 2022), available from undocs.org/A/RES/77/37; UNGA Resolution 78/16, *Programme of Action to Advance Responsible State Behaviour in the Use of Information and Communications Technologies in the Context of International Security*, A/RES/78/16 (6 December 2023), available from undocs.org/A/RES/78/16.

29 UNGA Resolution 77/36, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/77/36 (12 December 2022), available from undocs.org/A/RES/77/36; UNGA Resolution 78/237, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/78/237 (28 December 2023), available from undocs.org/A/RES/78/237.

30 "The Future of Discussions on ICTs and Cyberspace at the UN," UNODA (2 December 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.

31 PoA の在り方に関する各国の見解については次を参照。"Programme of Action to Advance Responsible State Behaviour in the Use of Information and Communications Technologies in the Context of International Security: Report of the Secretary-General," United Nations Digital Library, A/78/76 (18 April 2023), https://digitallibrary.un.org/record/4015040?ln=en&v=pdf.

32 Ibid., pp. 36-39.

33 Ibid., pp. 74-75.

34 "Concept Paper on Establishing a Permanent Open-Ended Working Group by Russian Federation (co-sponsors: Belarus, Burundi, Cuba, DPRK, Eritrea, Myanmar, Nicaragua, Syrian Arab Republic, Sudan, Venezuela, Zimbabwe)," UNODA (15 December 2023), https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_paper_on_a__Permanent_Decision-making_OEWG.pdf.

35 "Updated Concept of the Convention of the United Nations Ensuring International Information Security Submitted by Russian Federation (Cosponsors: Belarus, DPRK, Nicaragua, Syria, Venezuela)," UNODA (29 June 2023), https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_of_convention_on_ensuring_international_information_security.pdf.

36 "Regular Institutional Dialogue: The Fight for a Single-Track Process," OEWG's Seventh Substantive Session: The Highlights, Digital Watch (28 March 2024), https://dig.watch/updates/oewgs-seventh-substantive-session-the-highlights.

37 "Agenda Item 5: Day 3 Morning Session," UN OEWG 2021-2025 7th Substantive Session, Digital Watch (6 March 2024), https://dig.watch/event/un-oewg-2021-2025-7th-substantive-session/agenda-item-5-day-3-morning-session.

38 "Statement by the Brazilian Delegation on Explanation of Vote on Draft Resolutions L.11, L.13 and L.60 on ICTs," Journal of the United Nations (2 November 2023), https://estatements.unmeetings.org/estatements/11.0010/20231102150000000/BJU6e4qeGNyT/NxVkWpC7qvaV_en.pdf.

39 Pavlina Pavlova, "United Nations OEWG on ICT Security: Working Group Ramps Up Ambition as Time Presses Delegates to Reach Consensus on Future Dialogue," EU Cyber Direct (5 April 2024), https://directionsblog.eu/united-nations-oewg-on-ict-security/.

40 "Building Digital Solidarity: The United States International Cyberspace and Digital Policy Strategy," US Department of State (6 May 2024),

https://www.state.gov/building-digital-solidarity-the-united-states-international-cyberspace-and-digital-policy-strategy/.

41 大澤傑「デジタル技術が促進する新たな『たたかい』－流動化する国際秩序とデジタル権威主義」NIDS コメンタリー第 310 号（2024 年 4 月 19 日）、https://www.nids.mod.go.jp/publication/commentary/pdf/commentary310.pdf。

42 A/RES/78/16, PP10, OP3 (b).

PROFILE

原田　有

政策シミュレーション室/サイバー安全保障研究室　主任研究官

専門分野：海洋安全保障、サイバーセキュリティ（ガバナンス）

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 29177）
防衛研究所 Web サイト：www.nids.mod.go.jp