東京大学公共政策大学院 研究論文
Master Thesis
Graduate School of Public Policy
The University of Tokyo

サイバー空間をめぐる規範形成過程
―国連サイバー犯罪新条約の作成過程に着目して―
The Process of Making Law for Cyberspace
―The Case Study of Elaborating a Comprehensive International Convention on Countering the Cybercrime―

山本 愛 Kana Yamamoto
学籍番号 51-228039
公共政策学専攻国際公共政策コース修士２年

指導教官　中谷和弘教授
Supervised by Professor Kazuhiro Nakatani

目次

はじめに

近年、サイバー空間における脅威に注目が集まっている。ロシアによるウクライナ侵略は、サイバー空間から始まったと言っても過言ではない。ウクライナ国内では、侵略の開始される1か月ほど前から、「DDos 攻撃」による主要省庁及び大手銀行のサイトダウンや、大手企業におけるコンピュータウイルスの感染などが相次いだ[1]。これらはロシアによるものと見られている。これらを国際法上どのように議論するか。「サイバー空間」は、陸、海、空、宇宙に続く第5の作戦領域であり、また初めての人工領域であることから、新しい規範形成の可能性が議論されてきた。規範形成に消極的な日欧米諸国と、積極的な中露や新興国。「サイバー空間」においては従来からある対立構図である。平行線をたどる両者だが、このウクライナ侵略の最中にあって、再度の合意形成を試みている。本稿で取り上げる「犯罪を目的とした ICT 利用に対処するための包括的な国際条約作成に向けたアドホック委員会」（Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes）こそ、その試みの舞台である。

本稿では、いわゆる国連サイバー犯罪新条約に係るアドホック委員会を題材に、サイバー空間の規範形成過程について考察する。第1章では、同委員会の設立に至る経緯を踏まえ、サイバー空間の規範形成過程における同委員会の位置づけを検討する。そのうえで、第2章では、同委員会の第1回会合から第6回会合にかけて交わされた各国の意見を念頭に、同委員会の論点を抽出する。第3章では、抽出された論点が、従来の学説を踏まえてどのように捉えられるか検討する。第4章では、「サイバー犯罪」をめぐる規範形成過程を、これと類似の経緯を有する「テロリズム」をめぐる規範形成過程と比較し、その特徴を検討する。その上で、今後、サイバー犯罪、あるいはサイバー空間の規範形成に向けて必要と考えられる要素について考察することとしたい。

[1] 松原実穂子「『第五の主戦場』サイバー攻撃応酬の脅威」『外交 Vol72』（都市出版，2022年）32-39頁。

第１章　アドホック委員会の位置づけ
――サイバー空間の規範形成過程から

第１節　アドホック委員会の概要

「犯罪を目的とした ICT 利用に対処するための包括的な国際条約作成に向けたアドホック委員会」（Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, 以下、アドホック委員会。）の設立は、国連総会決議 74/247 に基づき決定された[2]。同決議は、2019 年 12 月、国連総会で、賛成 79、反対 60、棄権 33、無投票 21 で採択された。第 73 回国連総会の第 3 委員会におけるロシアの提出案によるものである。日本は、同決議の採択に欧米諸国と共に反対票を投じた。これらの国々は、従来から、サイバー犯罪に関する条約（略称：サイバー犯罪条約（通称：ブタペスト条約），以下、ブタペスト条約。）の普遍化を念頭に、サイバー犯罪対策を目的とする新条約の作成に反対していた。この立場をとる背景には、ロシアや中国、さらに両国に連なる「新興国及び途上国は非民主主義国家であって電子情報を国家統制したがり、新条約には情報統制条項の挿入を要求することが予期され、これは情報の自由を損なうものとなりかねない」との懸念があった[3]。これに対し、ロシアや中国といった国々は、ブタペスト条約は、あくまでも地域条約であり、また同条約の第 32 条 b 項の規定が主権の侵害につながり得るとして、新条約作成の必要性を主張していた[4]。以上のような対立構図にあって、同決議は、ロシアや中国の主張を実現する足掛かりとなった。同決議の採択以来、アドホック委員会のモダリティを決定する会合等を経て、

---

[2] United Nations General Assembly (UNGA) Resolution 74/247, *Countering the use of information and communications technologies for criminal purposes*, A/RES/74/247 (27 December 2019) available from http://undocs.org/A/RES/74/247 (last visited 30 November 2023)

[3] 中谷和弘「サイバー攻撃と国際法」『国際法研究』第 3 号（2015 年 3 月）89 頁。

[4] サイバー犯罪条約 第 32 条 b　蔵置されたコンピュータ・データに対する国境を越えるアクセス（当該アクセスが同 意に基づく場合又は当該データが公に利用可能な場合） 締約国は、他の締約国の許可なしに、次のことを行うことができる。（略）自国の領域内にあるコンピュータ・システムを通じて、他の締約国に所在する蔵置されたコンピュー タ・データにアクセスし又はこれを受領すること。ただし、コンピュータ・システムを通じて当該デー タを自国に開示する正当な権限を有する者の合法的なかつ任意の同意が得られる場合に限る。
「サイバー犯罪に関する条約」和文テキスト（訳文）外務省より。
https://www.mofa.go.jp/mofaj/gaiko/treaty/treaty159_4.html（2023 年 11 月 26 日最終閲覧）

途中、COVID-19 による延期がなされながらも、2021 年 5 月には、総会決議 75/282 が採択された[5]。同決議に基づき、2022 年 1 月から、国連薬物犯罪事務所（United Nations Office on Drugs and Crime, 以下、UNODC。）を事務局とするアドホック委員会が設置され、条約交渉が開始された[6]。なお、同委員会の意思決定においてコンセンサスが成立しない場合は 3 分の 2 多数決を用いることとされた。

アドホック委員会は、2024 年までに 10 日間の会合を 6 回以上開催し、第 78 会期での条約案提出を目指している。2023 年 11 月 13 日現在、第 1 回会合から第 6 回会合までが実施済みであり、翌 2024 年 1 月 29 日から最終会合が、米・ニューヨークにて開始される予定である[7]。第 1 回会合から第 6 回会合にかけて、その参加国・地域、団体（NGO・NPO、学会など）・個人（研究者や国会議員など）は様々であるが、毎度の会合に、平均 25 の国と地域、10 の団体・個人が参加し、その数は回を追うごとに増加傾向にある。

第 2 節　国連サイバー犯罪新条約の作成交渉に至る経緯
――第 12 回国連犯罪防止・刑事司法会議

第 12 回国連犯罪防止・刑事司法会議（United Nations Congress on Crime Prevention and Criminal Justice（通称：コングレス））における「サルバドール宣言」の採択は、アドホック委員会設立の契機となった。2010 年 4 月 12 日から 19 日にかけてブラジルのサルバドールで開催され、約 100 か国の司法大臣や検事総長といった政府代表及び NGO 関係者等、総勢約 3000 人が参加した同会議は、サイバー犯罪対策に向けた新条約の作成について、中露等と日欧米諸国を含む各国が一定の一致を見せた、初めての事例である。同会議のアジェンダのひとつとして、サイバー犯罪対策があり、「サルバドール宣言」の採択にあたっては、国際協力と技術支援が言及されるとともに、アルゼンチンをはじめとする新興国からサイバー犯罪に関する国際条約の必要性が指摘された。これに対しては、ブタペスト条約の締約

---

[5] UNGA, *Countering the use of information and communications technologies for criminal purposes*, A/RES/75/282 (26 May 2021), available from undocs.org/A/RES/75/282 (last visited 30 November 2023)

[6] United Nations, “Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes”, available from https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home (last visited 30 November 2023)

[7] アドホック委員会は、第 1 、 3 、 6 回会合をアメリカのニューヨークで、第 2、4, 5 開会合をオーストリアのウィーンで開催された。

国であった日欧米諸国を中心に、批判的な見解が示されたものの、最終的には、「サイバー犯罪に対する既存の、また新たな、国内的及び国際的な法律的対応並びにその他の対応を強化するための選択肢を検討する」（examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime）という文言で合意に至った[8]。さらに、この検討に向けた「オープンエンド政府専門家会合」の立ち上げも勧告された。このように、アドホック委員会設立の契機は、およそ 10 年前、新興国によってなされていたのである。以来、新条約賛成派と反対派の主張は平行線をたどったが、近年に入り、新興国を味方につけた中露等を中心とする賛成派の動きが活発化した。2018 年、ロシアは、第 73 回国連総会の第 3 委員会において、犯罪目的の情報通信技術に対抗する（Countering the use of information and communications technologies for criminal purposes）旨の決議案を提出し、同年 12 月に国連総会決議 73/187 が採択されている。こうした動きが、2019 年の総会決議 74/247 の採択に繋がり、アドホック委員会の設立を後押ししたと考えられる。

第 3 節　サイバー空間の規範形成過程

これまで、サイバー空間の規範形成は、中露を中心とする地域枠組み、日欧米諸国を中心とする地域枠組み、そして、中露と日欧米諸国が共に参加する国連及び各種国際会議において、各国が独自の立場を主張し、その相違を明らかにしつつも、相乗的に目指されてきた。その端緒として、1998 年 12 月にロシアから国連総会に提出された決議案「国際安全保障の文脈における情報及び電気通信分野での発展（Development in the Field of Information and Telecommunications in the Context of International Security）」がある。同決議案は、国際社会で初めて、サイバー空間の諸問題を全ての加盟国の共通利益（the common good of all States）として、国際法制度の形成可能性（developing international legal regimes）に向けて、多数国間レベル（multilateral levels）で協議する必要性に言及した。しかし、最終的に採択された国連総会決議 53/70 では、同決議案にあった、「『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

---

[8] 大谷潤一郎「『サルバドール宣言』の意義と概要」『ジュリスト 特集・第 12 回国連犯罪防止・刑事司法会議』No.1411（2010 年 11 月）42-47 頁。
なお、同会議は、国連総会決議に基づき、5 年ごとに開催される刑事司法分野における世界最大規模の会議であり、1995 年に第 1 回会議がジュネーブで開催されて以来、各国間で犯罪対策・刑事司法分野における意見交換や助言・提言が行われる場となっている。同会議の事務局もまた、アドホック委員会と同じく UNODC が担っている。

流通を脅かしかねない 」として日欧米諸国から懸念が示され、国際法制度の形成可能性への言及は避けられた[9][10]。元来、ロシアの主張する「情報セキュリティ（information security）」は、後述する「サイバーセキュリティ」と呼ばれるサイバー空間を使用するネットワークやコンピュータ・システムそのもののセキュリティに加え、コンテンツ（サイバー空間を行き交う中身）のセキュリティをも含んでいると言われてきた[11]。ロシアによる新条約の作成に向けた動きには、このようなコンテンツ、すなわち、自国では管理しきれない、越境的な性質を持つ、サイバー空間における情報を、統制する狙いが窺える。

ロシアの動きを前に、日欧米諸国を中心とする欧州評議会は、1997 年から、ブダペスト条約の起草作業に着手した。同条約は、2004 年に発効し、現在、G 7 諸国を含む 68 か国が締約国となっている。同条約は、前文と全 48 条から成り、サイバー犯罪の対処に向けた国際協力を目的に、条約上対象とする犯罪及び捜査・訴追について規定している。なお、同条約は、起草・発効当時から現代にかけての情報技術分野の急速な発展に伴い、2017 年から締約国間で捜査協力の深化を目的に再度交渉が進められ、2021 年 11 月に第 2 追加議定書が採択されるに至った。

これに対し、ロシアは、ブダペスト条約の第 32 条 b 項の規定が主権の侵害につながり得るとして同条約に加盟せず、上海協力機構（Shanghai Cooperation Organization, 以下、SCO。）を舞台に、新条約の作成に向けた動きを活発化させた。SCO は「テロリズム・分離主義・過激主義…に共同して対応するための方策を開発し実施すること」[12]を目的としてお

---

[9] 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」『安全保障研究』 2 巻 2 号（2022 年）233-250、239 頁。
https://www.nids.mod.go.jp/publication/security/pdf/2022/202203_12.pdf（2023 年 11 月 26 日最終閲覧）

[10] UNGA, *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 (last visited 30 November 2023)

[11] 佐々木孝博「サイバー空間の施策に関するロシアと欧米諸国のアプローチ」『日本大学大学院総合社会情報研究科紀要』14 号（2013 年）1-12 頁
https://gssc.dld.nihon-u.ac.jp/wp-content/uploads/journal/pdf14/14-001-012-Sasaki.pdf
（2023 年 11 月 26 日最終閲覧）

[12] 最上敏樹『国際機構論講義』（有斐閣、2016 年）228 頁。
また、上海協力機構（SCO）とは、2001 年に設立され、2023 年現在、中国、ロシア、カザフスタン、ウズベキスタン、タジキスタン、キルギスタン、インド、パキスタンを加盟国とする国際機構である。

り、その観点から、2001 年の発足以来、「ビシュケク宣言」[13]や「ウファ宣言」[14]といった各種の声明で、それぞれ、サイバー空間における脅威への協力や、新条約作成の必要性を掲げている。2009 年 6 月には、SCO 加盟国で「国際情報セキュリティを確保する分野における協力に関する協定（Agreement on Cooperation in Ensuring International Information Security between the Member States of the SCO）」が署名された[15]。また 2011 年 9 月には、SCO 加盟国のうち、中国、ロシア、タジキスタン、ウズベキスタンが、国連総会に「情報セキュリティのための国際行動綱領（International Code of Conduct for Information Security）」を提出した[16]。この 2 つの文書では、同国が「他国の政治・社会・経済システム、精神的・道義的・文化的サークルを害する情報の散布」を、情報セキュリティ分野における主要な脅威のひとつとして、「関連する国内法令に従うことを前提として、情報空間における権利及び自由を十分に尊重すること」、「他国の政治的、経済的及び社会的安定性を損なう情報の流布を禁止することに協力する」ことといった文言を掲げ、国内の情報統制を念頭に置いた主張を繰り返している[17]。

情報の取扱いを中心に、日欧米諸国と中露等の主張が平行線をたどる一方、両者の合意形成に向けた動きも国連及び国際会議で進められた。その動きは、2000 年代に入って顕著になった。国連では、2004 年に政府専門家会合（Group of Governmental Experts,以下、GGE。）が、2018 年には議題の重複するオープンエンド作業部会（Open-ended Working Group，以

---

[13] Shanghai Cooperation Organization (SCO), “Bishkek Declaration by the Heads of the Member States of the SCO” (August, 2007), available from http://eng.sectsco.org/documents/ (last visited 26 November 2023)

[14] SCO, “Ufa Declaration by the Heads of the Member States of the SCO” (July, 2015) , available from http://eng.sectsco.org/documents/ (last visited 26 November 2023)
同文書には、「The member states support the elaboration of a universal code of rules, principles and standards of the responsible behavior by states in the information space, and consider a new version of the “Rules of conduct in the field of international information security” circulated in January 2015 on behalf of the SCO member states as an official UN document, as an important step in this direction.」とある。（下線は筆者）

[15] SCO, Agreement on Cooperation in Ensuring International Information Security between the Member States of the SCO, (2009), available from http://eng.sectsco.org/documents/ (last visited 26 November 2023)

[16] UNGA, *International code of conduct for information security* , A/66/359 (14 September 2011) available from undocs.org/A/66/359 (last visited 26 November 2023)

[17] 中谷和弘「前掲論文」（注 3）91 頁。

下、OEWG。）が、新設された。GGE は、安保理常任理事国と地理的配分を考慮した 15 ないし 25 の国から集った外交官を主とする各国の専門家によって構成された。2004 年から 2021 年にかけて、計 6 期にわたって活動し、第 5 期を除くすべての会期で報告書が作作成され、国連総会に提出され、これを歓迎する総会決議がコンセンサスで採択された。報告書を通して、各国は、既存の国際法の適用可能性と、追加の「自発的で非拘束的な規範（further voluntary, non-binding norms）」形成の必要を共有した[18]。前者は具体的に「国連憲章及び他の国際法の原則」すなわち、主権平等、国際紛争の平和的解決、武力行使の禁止、人権および基本的自由の尊重、国内事項への不干渉が挙げられた[19]。後者は、「国際法に合致する行動を制限したり禁止するものではなく、それらは国際共同体の期待を反映するものであり、責任ある国家行動の基準を設置するもの」と位置付けられている。また、第 4 期に中露の提案に基づき、11 項目に及ぶ具体的な規範内容が示された。一方、国際法がどの範囲でどのように適用されるかをめぐっては、国家責任法や国際人道法、国際人権法等、分野ごとに議論が異なった。

議論の複雑化に伴い、第５期ＧＧＥでコンセンサスの形成に失敗すると、アメリカが第６期ＧＧＥの設置を目指す一方で、ロシアがＯＥＷＧの設置を主導した。第６期ＧＧＥ報告書には、任意に提出された国際法の適用に関する見解（国別見解）が集約された[20]。日本もまた「サイバー行動に適用される国際法に関する日本政府の基本的な立場」を提出している[21]。

---

[18] 「自発的で非拘束的な規範」は、森肇志「国家間のサイバー攻撃をどう規制するか？―国連における ICTs 規制論議の経緯・現状・課題」東京大学法学部「現代と法」委員会編『まだ、法学を知らない君へ―未来をひらく 13 講』（2022 年、有斐閣）194 頁からの訳出。なお、第 2 回報告書パラ 16、第 3 回報告書パラ 19-21、第 4 回報告書パラ 9-15 にかけて言及がある。UNGA, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Scurity*, A/64/201 (30 July 2010), p.8 available from undocs.org/A/65/201；UNGA, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Scurity*, (24 June 2013), p.8 available from undocs.org/A/68/98；UNGA, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Scurity* , (22 July 2015), p.8, available from undocs.org/A/70/174

[19] A/70/174（para26）

[20] 赤堀毅『サイバーセキュリティと国際法の基本―国連における議論を中心に―』（東信堂、2023 年）222 頁。

[21] 外務省「サイバー行動に適用される国際法に関する日本政府の基本的な立場」（2021 年 5 月 29 日）https://www.mofa.go.jp/mofaj/gaiko/page3_003059.html（2023 年 11 月 30 日最終閲覧）

ＯＥＷＧでは、国連全加盟国に参加が認められており、実際に 68 か国が参加し、報告書はコンセンサスで採択された[22]。同報告書の内容は、従来からの GGE で合意された内容から大きな進展があったとは言えないが、GGE と比較して多くの国が参加する対話の場が与えられたこと、そうした場において、GGE における以前の作業が確認された点には意義があった[23]。なお、ＧＧＥやＯＥＷＧは、規範形成だけでなく、信頼醸成措置や能力構築支援等、国際法以外の取り組みをも扱っていたことに留意したい。また、GGE と OEWG は、対立関係にあるアメリカとロシアによってそれぞれ設立されたため、しばしば二重プロセスとして議論の停滞を示すものと扱われるが、これに代わる第 3 の選択肢として「行動プログラム（Program of Action）」の導入も検討されている。POA は、コンセンサスが得られる事項から協力を進める方針であり、これまでに小型武器や差別、ヘイトスピーチ等の分野で設けられてきた。

さらに、国連外の主要な取組として、ウィリアム・ヘーグ（William Hague）英外相（当時）による、中露等を含む各国への呼びかけで、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動きがあった[24]。以来、ブタペスト、ソウル、ハーグ、デリーにおいて、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で、国際会議が開催され、一連の取組はロンドン・プロセスと呼ばれている。

その他、2009 年には、『タリン・マニュアル』が刊行された。同文書は、エストニアの首都タリンに本部を置く、北大西洋条約機構（NATO）サイバー防衛センター（Cooperative Cyber Defense Centre of Excellence , CCDOE）による支援の下、専門家が個人的資格で集まり、サイバー攻撃に適用される慣習国際法を抽出したものである[25]。2013 年には「有事・戦時」を念頭に置いた『タリン・マニュアル 1.0』が、2017 年には「平時」を念頭に置いた『タリン・マニュアル 2.0』が、それぞれ Cambridge University Press から刊行された。同作業に、日欧米諸国出身の専門家だけでなく、中露等出身の専門家が携わった点は注目される。

第 4 節　アドホック委員会の位置づけ

第 1 節、第 2 節で見たアドホック委員会の設立に向けた動きは、第 3 節で見たサイバー空

---

[22] 森肇志「前掲論文」（注 18）194 頁。

[23] 森肇志「前掲論文」（注 18）195 頁。

[24] 原田有「前掲論文」（注 9 ）242 頁。

[25] 中谷和弘、河野桂子、黒崎将広『サイバー攻撃の国際法 タリン・マニュアル 2.0 の解説 増補版』（信山社、2023 年） 1 頁。

間の規範形成過程において、どのように位置づけられるのだろうか。

まず、アドホック委員会は、日欧米諸国と中露がサイバー空間に係る条約作成を目指す、初めての場となった。これまで、サイバー空間に係る条約は、先述のブタペスト条約のみであり、その締約国に中露は含まれていない。各国が、新条約作成の要否とは別に、サイバー犯罪対策をめぐる国際協力の重要性で比較的一致しやすかったことが、同委員会の設立に繋がったと考えられる。

また、「サルバドール宣言」に見るように、新条約作成の契機を新興国が担った点や、アドホック委員会に国・地域だけでなく、個人も参加している点は注目される。GGE や OEWG 等、2000 年代以降、サイバー空間のステークホルダーが拡大している状況を同委員会にも見ることができる。

他方、アドホック委員会が、COVID-19 やロシアによるウクライナ侵略、イスラエル・パレスチナ情勢悪化の中で、進められている点も注目される。特に、同委員会の設立を推進したロシアが、ウクライナに侵略した点、さらにこの侵略がサイバー攻撃から始まったとされている点からも、同委員会の持つ意義は大きい。

第２章　アドホック委員会における議論

第１節　議論の全体像

アドホック委員会において、各国は、第１回会合で、各会合間の作業計画（mode of work）を決定し、条約の目的（objective）、適用範囲（Scope of application）及び構成（Structure）について大枠の合意形成を目指した後、第２回会合以降では各論へと移っていった。第１回会合、第２回会合、第３回会合では、各国が意見書を提出した。なお、ロシアは、第２回会合で、ベラルーシ、ブルンジ、中国、ニカラグア、タジキスタンを、第３回会合では、ベラルーシ、ブルンジ、中国、マリ、ニカラグア、タジキスタンを、代表して意見書を提出している。第４回会合及び第５回会合では、今後の交渉のベースとなる議長による統合交渉テキスト（Consolidated Negotiation Text）が計２点まとめられた。その後、第６回会合で、条約ドラフト（Draft text of the convention）を元に交渉が進められた。最終会合は、2024 年１月 29 日から２月９日にかけて行われる予定である。

第６回会合でまとめられた条約ドラフトは、全 67 条からなり、議題ごとに「一般規定（General provisions）」、「犯罪化（Criminalization）」、「管轄権（Jurisdiction）」、「手続措置及び法の執行（Procedural measures and law enforcement）」、「国際協力（International cooperation）」、「防止措置（Preventive measures）」、「情報交換を含む技術支援（Technical assistance, including information exchange）」、「実施方法（Mechanism of implementation）」、「最終規定（Final provisions）」という９つの章で整理されている。第２回会合及び第４回会合では「一般規定」、「犯罪化」、「管轄権」、「手続措置及び法の執行」が、第３回会合及び第５回会合では、「国際協力」、「防止措置」、「情報交換を含む技術支援」、「実施方法」、「最終規定」及び「前文」が議論された。

第１回会合から第６回会合にかけて、日欧米諸国と中露等の対立構図は、これまでと同様に継続した。一方で、同志国との協力体制よりも各国の刑事手続きに係る国内法制に重きを置いた議論が展開されることで、その対立が相対化する場面も生じた。他方、統合交渉テキストや条約ドラフトは、ブタペスト条約のほか、従来の捜査協力に係る条約である「国際的な組織犯罪の防止に関する国際連合条約（United Nations Convention against Transnational Organized Crime，以下、UNTOC。）」や「腐敗の防止に関する国際連合条約（United Nations Convention Against Corruption，以下、UNCAC。）」を基礎とする内容が含まれていた。

以下では、第２回会合及び第４回会合の議論と、第３回会合及び第５回会合の議論に分けて、第１回会合を踏まえつつ、提出された意見書や統合交渉テキストから、各国の立場を分析する。さらに、第６回会合に向けて提出された条約テキストやそれに対する各国の立場

を考察する。

第２節　第２回会合及び第４回会合[26]

――「一般規定」、「犯罪化」、「手続措置及び法の執行」

第２回会合、及び第４回会合では、「一般規定」、「犯罪化」、「手続措置及び法の執行」について議論された。なお、条約ドラフト案では、第４章で見るように、「引渡しか訴追か（aut dedere aut judicare）」の選択義務に関して「管轄権」に係る規定も含まれている。

「一般規定」に係る議論では、「条約の目的（Statement of Purpose）」、「用語法（Use of terms）」、「適用範囲（Scope of application）」、「主権の保護（Protection of sovereignty）」、「人権の尊重（Respect for human rights）」が、扱われている。「条約の目的」は、日欧米諸国と中露等の主張に概ね一致が見られたが、「用語法」及び「適用範囲」については、双方の主張に相違があった。特に「用語法」については、日欧米諸国の言う「computer system」が中露等では「ICTs（Information and communications technology devices）」、「Computer data」が「Digital Information」、「cybercrime」が「use of ICTs for criminal purposes」、というように双方に違いが見られた。なお、日欧米諸国や中露等に分類されない、エジプトやブラジル等のいわゆる新興国では、内容が比較的、日欧米諸国寄りであっても、中露等の用語法に依拠する等、中立性を維持する要素として用語法を活用していると考えられる。同様に、「主権の保護」は中露等が、「人権の尊重」は日欧米諸国が、強く主張していた。

次に、「犯罪化」に係る議論を検討する。「犯罪化」は、第２回会合及び第４回会合において、日欧米諸国及び中露等が最も対立した分野である。犯罪化の対象を限定的に捉えたい日欧米諸国に対し、広く解釈しようとする中露等の対立が見られた。

---

[26] 本節では、以下の文書を参照した。
・第２回会合―UNGA, *Compilation of proposals and contributions submitted by Member States on the provisions on criminalization, the general provisions and the provisions on procedural measures and law enforcement of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes*, A/AC.291/9 (21 April 2022), available from http://undocs.org/A/AC.291/9 (last visited 30 November 2023)
・第４回会合―UNGA, *Consolidated negotiating document on the general provisions and the provisions on criminalization and on procedural measures and law enforcement of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes*, A/AC.291/16（7 November 2022）, available from http://undocs.org/A/AC.291/16 (last visited 30 November 2023)

日欧米諸国は、ブタペスト条約に定める犯罪化規定を基礎とし、その内容から対象が拡大されることに反対する立場をとっていた。各国は、犯罪化の対象を、①「cyber-dependent crime（offence)」と②「cyber-enabled crime（offence)」に分けた上で、①は全面的に、②は一定の限度（a limited range）で犯罪の対象に含まれる、としている[27]。①は、「すべての締約国が受け入れ可能で、この分野における既存の国際協定と整合性のある記述と定義（descriptions and definitions that are acceptable to all parties, and which are consistent with existing international agreements in this area)」を持つものをいう[28]。②は、「情報通信ネットワークが提供するスピード、匿名性、広範な到達範囲によって、その範囲、規模、実行の容易さのすべてが著しく増大した『伝統的な犯罪』（some "traditional" crimes whose scope, scale and ease of commission have been drastically increased by the speed, anonymity and widespread reach that information and communications networks provide)」を言う[29]。具体的には、「違法なアクセス（illegal access)」、「違法な干渉（illegal interception)」、「データの妨害(illegal interference data)」、「システムの妨害(illegal interference of computer system)、「装置の濫用（Misuse of devices)」は前者に、「偽造・詐欺等（forgery, fraud)」、「児童の性的搾取・虐待など（child sexual abuse and exploitation)」、「著作権侵害（infringements of copyright)」等は②に含まれる。各国とも、①の分類はブタペスト条約で犯罪化された対象に依拠していたが、②の分類には表現やその内容に若干の違いが見られた。欧州連合に至っては、②の具体例につき言及していない。このような限定的な立場を主張する理由として、短期間に多くの国で締結可能な条約作成が必要であること、既存の国内法や国際法との義務の抵触を避ける必要があること、電子情報の国家統制とその手段として同条約が悪用されないようにする必要があることが考えられる。その一環として、アメリカは、意見書において、サイバー犯罪の取締りは政府の責任であるのに対し、サイバーセキュリティは官民の様々な主体の責任であるとしている[30]。

---

[27] UNGA, *Compilation of proposals and contributions submitted by Member States on the provisions on criminalization, the general provisions and the provisions on procedural measures and law enforcement of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes*, A/AC.291/9(21 April 2022), p.41, available from http://undocs.org/A/AC.291/9（ニュージーランドの意見書）(last visited 30 November 2023)

[28] Ibid., pp.58-60.（イギリスの意見書）

[29] Ibid., p.5.（オーストラリアの意見書）　＊下線は筆者によるもの。

[30] Ibid., pp.63-69（アメリカの意見書）

一方で、中露等の主張する犯罪化の対象には、しばしば、日欧米諸国の主張する犯罪化の対象には無い対象を含んでいた。その例として、「重要情報インフラに対する違法な干渉（Unlawful interference with critical information infrastructure）」と「過激主義関連犯罪（Extremism-related offences）」がある[31]。日欧米諸国は「重要情報インフラに対する違法な干渉」は、「サイバーセキュリティ」や「サイバーガバナンス」に係る事案であり、新しい犯罪類型として新条約を適用する必要はないと主張していた。同対象の犯罪化は、サイバー空間には既存の国際法が適用されない、とする従来からの中露等の主張を代表する姿勢であり、日欧米諸国が警戒したと考えられる。また、「過激主義関連犯罪」は、情報通信技術

---

[31] 第1回会合の意見書として、ロシアは「代理大使が国連事務総長に宛てた2021年7月30日の書簡（A/75/980）」と同じ内容を提出した。第11条と第21条は以下のとおりである。
UNGA, *Letter dated 30 July 2021 from the chargé d'affaires a.i. of the Russian Federation to the United Nations addressed to the Secretary-General*, A/AC.291/9(21 April 2022), pp.7-9, available from http://undocs.org/A/75/980
Article 11 Unlawful interference with critical information infrastructure
1. Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law the intentional creation, distribution and/or use of software or other digital information knowingly designed to interfere unlawfully with critical information infrastructure, including software or other digital information for the destruction, blocking, modification, copying of information contained therein, or for the neutralization of security features.
2. Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law the violation of the rules of operation of media designed for storage, processing and transfer of protected digital information contained in critical information infrastructure or information systems or information and communication networks that belong to critical information infrastructure, or the violation of the rules of access to them, if such violation damages the critical information infrastructure.
Article 21 Extremism-related offences
1. Each State party shall adopt such legislative and other measures as are necessary to establish as an offence or other illegal act under its domestic law the distribution of materials that call for illegal acts motivated by political, ideological, social, racial, ethnic, or religious hatred or enmity, advocacy and justification of such actions, or to provide access to such materials, by means of ICT.
2. Each State party shall adopt such legislative and other measures as are necessary to establish as an offence or other illegal act under its domestic law humiliation by means of ICT of a person or group of people on account of their race, ethnicity, language, origin or religious affiliation.

.

に基づく情報の生成・頒布への規制を内容とし、先述の SCO の取り組みを想起させる。この規制は、何が過激主義にあたるかの判断を各国政府に委ね統制を強化するものであり、日欧米諸国の警戒する、偽情報の頒布や人権侵害のおそれが生じる。「重要情報インフラに対する違法な干渉」は第 4 回会合の議長統合テキスト、及び第 6 回会合の条約ドラフト案においても「犯罪化」の対象として残った。一方、「過激主義関連犯罪」に関しては、第 6 回会合の条約ドラフト案においては言及が無くなった。

他方、「児童の性的虐待・搾取製造関連犯罪」については、各国国内法制との関係で、中露等だけではなく、日欧米諸国の間においても、児童の年齢制限や、製造物と「表現の自由」との関係等で議論があった。

「手続措置及び法の執行」に関しては、第 6 回会合において、条約ドラフトの人権保障措置（第 24 条 Condition and safeguards）を、主権侵害のリスクを念頭に手続措置に限定して講じるべきとする中露等と、条約全体に拡大して講じるべきとする日欧米諸国で溝が明らかとなった[32]。

---

[32] 条約ドラフト第 24 条は以下のとおりである。条約ドラフトへ各国コメントを付した作業文書（Plenary working documents, 注 36 参照。）では、「chapter」を「convention」に変える変更や、「international human rights law」への言及が西側諸国を中心になされており、これに反対する中露等の構図がうかがえる。

Article 24. Conditions and safeguards

1. Each State Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this chapter are subject to conditions and safeguards provided for under its domestic law, which shall be consistent with its obligations under international human rights law, and which shall incorporate the principle of proportionality.

2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent review, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3. To the extent that it is consistent with the public interest, in particular the proper administration of justice, each State Party shall consider the impact of the powers and procedures in this article upon the rights, responsibilities and legitimate interests of third parties.

（和訳）

第 24 条　条件及び保障措置

１．締約国は、この章に定める権限及び手続の設定、実施及び適用が、自国の国内法に定める条件及び保障措置であって、国際人権法上の義務に合致し、かつ、 比例原則を含むものに従うことを確保する。

２ 1 に規定する条件及び保障措置には、該当する権限又は手続の性質にかんがみ適当な場合には、特に、 司法上の又は他の独立した審査、適用を正当化する事由並びに当該権限又は手続の

このように、第2回会合及び第4回会合においては、「一般規定」における用語法や「犯罪化」の対象となる行為の抽出方法、「手続措置及び法の執行」を中心に、従来からの日欧米諸国対中露等との対立が目立った。

適用範囲及び期間に関する制限を含む。

3 締約国は、公共の利益、特に司法の適切な運営に反しない限り、この章に定める権限及び手続が第三者の権利、責任及び正当な利益に及ぼす影響を考慮する。

第３節　第３回会合及び第５回会合[33]

――国際協力，技術支援を含む情報交換，予防措置等

第３回会合、と第５回会合では、「国際協力」、「情報交換を含む技術支援」、「予防措置」、「実施メカニズム」、「最終規定」が議論された。また「前文」も取り扱われた。

第３回会合において、各国は、UNTOC、UNCAC、ブタペスト条約の内容に沿った意見書を提出していた。他方、中露等の共同案を前に、細部において、日欧米諸国間のずれが目立った。また、双方の主張においては、日欧米諸国より中露等が、締約国に対する義務を広く求める傾向にあった。以下では、日欧米諸国間、あるいは日欧米諸国と中露等の間で主張の違いを見せた主要な分野として、「国際協力」、「情報交換を含む技術支援」、「予防措置」について詳細を検討する。

「国際協力」の分野では、「一般規定（General Principles of International cooperation）」、「個人情報の保護（Protection of personal data）」、「犯罪人引渡し（Extradition）」、「受刑者移送（Transfer of sentenced persons）」、「刑事手続きの移管（Transfer of criminal proceedings）」、「相互援助に関する一般規定及び特別規定」「法執行に係る協力」、「犯罪収益等の回復」が、取り扱われた。「個人情報の保護」に関しては、日欧米諸国間で違いがあった。ＥＵは第３回会合の提出意見において、ブタペスト条約第２追加議定書等を念頭に、個人情報保護の観点から、国家間のデータ移転にはデータ保護の水準が同等であるべきと主張した。また、「犯罪人引渡し」については、保障措置の水準や拒否事由について、死刑制度や属人的管轄権の設定の有無、政治犯の取扱い等、国内法制の観点から各国独自の主張があった。「受刑者移送」に関しては、国内法制における受刑者の更生等を念頭に置いてお

---

[33] 本節では、以下の文書を参照した。

・第３回会合―UNGA, *Compilation of proposals and comments submitted by Member States on provisions on international cooperation, technical assistance, preventive measures and the mechanism of implementation, the final provisions and the preamble of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes*, A/AC. 291/12 (3 August 2022), available from http://undocs.org/A/AC.291/12 (last visited 30 November 2023)

・第５回会合―UNGA, *Consolidated negotiating document on the preamble, the provisions on international cooperation, preventive measures, technical assistance and the mechanism of implementation and the final provisions of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes*, A/AC.291/19 (19 December 2022), available form http://undocs.org/A/AC.291/19 (last visited 30 November 2023)

り、サイバー犯罪の特殊性を強調する必要性がないとして日・EU が同規定の設置に反対した。一方、中露等の意見書では、UNCAC や UNTOC の規定と異なり、受刑者移送や刑事手続きの移管を「義務化（shall の使用等）」する動きが目立った。また、新興国を中心に、刑事共助の枠組みの外で情報交換できる規定を目指す国も多くあったが、日欧米諸国は、情報交換の名のもとに過度な情報の共有がなされ得るとの慎重な姿勢を見せた。「相互援助に関する一般規定、及び特別規定」に関しては、各国とも、犯罪化の対象によって主張が異なった。特に「蔵置されたコンピュータ・データに対する国境を超えるアクセス」に係る議論は注目される。これはブタペスト条約第 32 条の規定を念頭に置いているが、従来から中露等の反対があった。背景には「国境を超えるアクセス」は主権の侵害につながり得るとの見方がある。実際、第 6 回会合の条約ドラフト案では、削除された。この他、「犯罪収益等の回復」については、米国が暗号資産を含む犯罪化収益の回復等の規定を求め、また豪州がランサムウェアによる恐喝に対する規定を求めるなど、日欧米諸国の中でも、ブタペスト条約に特定して規定されていない内容に言及する国とこれに慎重な姿勢を示す国で違いが生じた。特に日本をはじめ、犯罪被害財産や国庫に帰属した財産等を没収・返還し得ないとする国内法制である場合、調整が必要となる。その際、条約内に留保規定を導入するか否かも議論の余地があろう。条約法条約 19 条では、いわゆる「条約の趣旨・目的との両立性」基準を定めているが、本条約でどのように適用可能なのかは未だ明らかではないため、条約内で留保規定を確保することが考えられる。

「情報交換を含む技術支援」や、「予防措置」に関しては、日欧米諸国側が、民間企業への働きかけや責任追及等、民間企業への負担が増えることに慎重な姿勢を示した。背景には、日常的に民間企業への規制を強める中露の国内法制が念頭にあると考えられる。

以上の検討から、日米欧州諸国対中露等といった「犯罪化」の対象に代表される議論に引き続き影響されつつ、各国の議論は、第 3 回会合及び第 5 回会合において、自国の国内法制との整合性により重点を置いた議論を展開したことが分かる。

第 4 節　第 6 回会合に見る各国の動き[34]

今年 8 月 21 日から 9 月 1 日にかけて行われた第 6 回会合においては、第 1 回会合から第

[34] 第 6 回会合―UNGA, *Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*, A/AC.291/22 (29 May 2023), available from http://undocs.org/A/AC.291/22 (last visited 30 November 2023)

５回会合までの議論を踏まえて議長の下で予め作成され、６月に開示された条約ドラフト案に対し、各国がコメントを付す形で議論された。さらに、９月には、各国コメントを集めた同会合の作業文書（Plenary Working Document）も開示され、中露等を中心に、条約ドラフトには採用されなかった案の再提案や、これまで議論されてこなかった新出の提案等がなされ、これに日欧米諸国が対抗する構図が明らかとなった[35]。現在、本会合とは別に論点ごとに複数のグループを形成し、それぞれに非公式協議が設けられ、コンセンサスに向け議論が継続されている。

６回の会合を通じて、一貫して論点として残ったのは、「用語法」と「犯罪化」に係る部分であった。まず、用語法においては、日欧米諸国と中露等で、「computer system」/「information and communications technology device」や、「cybercrime」/「the use of information and communications technologies for criminal purposes」など文言に違いがあった。日欧米諸国は、中露等の主張する用語法について、「information and communications technologies」はコンピューターに限らず、衛星や電話等も含まれ、犯罪化の対象を拡大化させる表現で、サイバーガバナンス等、アドホック委員会のマンデートを超える点に懸念がある。これは第 1 回会合以降、常に議論され第６回会合においても条約ドラフトが併記されることとなったように、平行線をたどった。次に、「犯罪化」に関しては、その対象が引き続き論点となった。犯罪化の対象の幅いかんによっては、国内法の整備を要し得るとともに、国際協力の適用範囲にも影響するからである。第６回会合で提示された条約ドラフトでは、妥協策として以下のとおり「第 17 条」が提示された。

> Article 17. Offences relating to other international treaties
>
> States Parties shall adopt such legislative and other measures as may be necessary to ensure that offences established in accordance with applicable international conventions and protocols also apply when committed through the use of [a computer system] [an information and communications technology device].
>
> （和訳）第 17 条
>
> 締約国は、適用可能な国際条約及び議定書の適用に従って定められる犯罪が、［コンピュータ・システム］［情報通信技術機器］の使用を通じて行われる場合におい

[35] UNGA, *Plenary Working Document, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*,(2 September 2023),available from https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/DTC/DTC_rolling_text_02.09.2023.pdf (last visited 30 November 2023)

ても適用されることを確保するための立法そのほかの適切な措置をとる。

第 17 条は、犯罪化の対象を限定化する流れを作り得る一方で、「applicable」等、不明瞭な表現により拡大化の流れをも作り得る規定であった。現に、日欧米諸国は、「applicable」を削除し、国連条約や議定書（United Nations convention and protocol）に定められる犯罪、という限定を加えるべきとの立場を示した[36]。

このように、第 6 回会合において提示された条約ドラフトは、合意形成の難しさを明らかにした。やはり、条約の適用範囲として、犯罪化の対象は、その後に続く法の執行や手続措置、国際協力の適用範囲にも関連する議題であり、その範囲をめぐって議論が硬直化したことがうかがえる。

[36] Ibid.,（注 35）pp.22-23

第３章　「サイバー犯罪」の定義
――アドホック委員会における議論から

第１節　アドホック委員会で残った主要な論点

アドホック委員会では、「犯罪化の対象」がその主要な論点として残った。すなわち、「サイバー犯罪」をどのように定義するか、という問いである。同論点を、従来の学説等から検討し、同委員会で交わされた各国の意見について考察することとしたい。

上記に見るように、「サイバー犯罪」の国際法上の定義は未だ確立していない。アドホック委員会における議論は、同論点をめぐって硬直化した。条約上の対象となる犯罪の特定は、締約国の捜査、訴追、及び国際協力に係る国内法制に影響を及ぼすため、各国は自国の主張に固執する傾向にある。その傾向は、第２章で見たように、日欧米諸国に顕著であった。これらの国々は、「サイバー犯罪」の定義を限定的に解し、その説明として、「サイバー犯罪」を「サイバーセキュリティ」や「インターネットガバナンス」と比較した。米国は、「両者は、コインの表裏として見られることが多いが、サイバー犯罪の取締りは基本的に政府の責任であるのに対し、サイバーセキュリティは官民の様々な主体の責任である（Although often seen as two sides of the same coin, cybercrime enforcement is essentially a governmental responsibility, whereas cybersecurity is the responsibility of a range of public and private actors.)」と述べている[37]。また、日本や英国、豪州や EU は、「他のフォーラムで扱われているような、より広範なサイバーセキュリティの問題を取り上げるべきではない（It should not addressed broader cybersecurity issues that are addressed in other forums)」との姿勢を示している[38]。

なお、日本政府の政策担当者によると、アドホック委員会の事務局である UNODC は確実にコンセンサスされる限りで議論を止める傾向にあり、最終的には「犯罪化の対象」に係る論点をペンディングした上で同委員会を閉める方針なのではないか、との見方を示している。だが、これまでの同委員会の議論に見るように、同論点は、今後も幾度となく浮上し得る。また、続く第４章に見るように「サイバー犯罪」の規範形成過程の特徴を捉える上で

---

[37] UNGA, *Compilation of views submitted by Member States on the scope, objectives and structure (elements) of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes*, A/AC.291/4, p.64, (17 November 2021),available from http://undocs.org/A/AC.291/4 (last visited 30 November 2023)

[38] Ibid., p.61; A/AC.291/9, pp.35-38

同論点は注目される。

以下では、第２節で「サイバー犯罪」の定義を、アドホック委員会の議論のほか、従来の学説等を踏まえて検討する。第３節では、同論点からさらに抽出される論点である、「サイバー犯罪」の国家責任論における帰属と主権侵害可能性について、従来の学説を振り返る。第４節では、以上の検討を踏まえて、同委員会における、「サイバー犯罪」をめぐる日欧米諸国と中露等の主張について、再度考察する。

第２節　「サイバー犯罪」の定義

「サイバー犯罪」は、一般的にコンピュータ・システムに対する犯罪及びコンピュータ・システムを利用した犯罪を表す用語とされている。条約ドラフトでは、「サイバー犯罪」を、日欧米諸国側と中露側がそれぞれ主張する、「cybercrime」と「the use of information and communications technologies for criminal purposes」という２種類の用語で併記しているがその意味するところは明らかではない。アドホック委員会をはじめ、これまでＧＧＥやＯＥＷＧ、ＳＣＯ規則等でも、「サイバー犯罪」の定義を明示した事例は確認できない。

他方、『タリン・マニュアル 2.0』では、定義とまでは行かずとも、比較的明示的な「サイバー犯罪」に係る取扱いを見ることができる。同著は、「主権侵害は、国家によってのみ成し得（規則４）」、「非国家主体による有害なサイバー行動は主権侵害とは言えず、国家責任の観点から国家に相当の注意義務が発生し得る（規則 37）」と示した上で、「サイバー犯罪は、国家に帰属しない限り主権侵害とはいえない」としている[39]。なお、「サイバー犯罪」それ自体とは別に、「サイバー犯罪」の捜査では、捜査当局（国家）が、他国への主権侵害、及び私人へのプライバシー権をはじめとする人権侵害を生じさせるリスクがあり、留意が必要である。

以上を踏まえて、「サイバー犯罪」の定義として、国家の「帰属」を証明できない「非国家主体」によるもので「主権侵害」の文脈から国際法上の責任を問うことができない行為とすることが考えられる。

なお、GGE と OEWG の双方に日本政府の代表として深く関与した赤堀毅審議官（大使）は、著書において、「烈度の高いサイバー攻撃は単に民間の（私人間の）問題に終わらない場合が多」く、「自然人のサイバー行動を国家に帰属させることに困難が伴うのであれば、各国でサイバー犯罪法制を整備し適切に処罰することはサイバーセキュリティの実現にと

[39] 中谷『前掲書』（注 25）17-18, 51-52 頁。

っても重要である」と指摘しており、「烈度」もまた検討され得る[40]。

第３節　「サイバー犯罪」の国家責任論における帰属の問題と主権侵害可能性

第２節で抽出した「サイバー犯罪」の定義では、国家責任論における帰属の問題と、主権侵害可能性がさらなる論点となる。

どの程度の有害なサイバー行動が国家に帰属せず、またその主権を侵害しないのか。

国家責任条文８条は、「人又は人の集団の行為は、事実上国の指示に基づき、又は国による指揮若しくは統制の下で行動していた場合には、国際法上当該国の行為とみなされる。」と規定している[41]。「指示」と「指揮若しくは統制」のうち、ニカラグア事件判決に言う、具体的な支配命令関係を求める「実効的支配」基準は後者にあたる[42]。有害なサイバー行動はどの程度の立証で国家に帰属するのか、についてこれまでに一致した見解は存在しない。だが、間接証拠や状況証拠の許容可能性について、コルフ海峡事件判決やオイルプラットフォーム事件判決を念頭に、被害国が有害なサイバー行動に「使用されたアカウントや IP アドレスの相互関連やマルウェアの類似性、関連の個人や団体を取り巻く状況に関する情報等、相互に結び付けられる単一の結論のような多くの間接証拠・状況証拠を提示する一方、疑いをかけられた国が証拠の提出に消極的である場合、それらの間接証拠や状況証拠が証拠として一定の重みを与えられる可能性がある」と指摘されている[43]。

有害なサイバー行動が国家の主権を侵害するか否かという問いは、サイバー空間において国家の主権が認められるのかという問いと、認められる場合、どの程度の有害なサイバー行動が国家の主権を侵害するのかという問いで構成される。『タリン・マニュアル 2.0』は、「国家は、他国の主権を侵害するサイバー行動を行ってはならない（規則４）」とする[44]。そのうえで、ある国家の機関が他国領域内に物理的に存在する間にサイバー行動をとることの他、遠隔サイバー行動にいたっては、物理的損害のみならず、ウイルス感染や社会保障や

---

[40] 赤堀『前掲書』（注 20）23, 79-82 頁。

[41] 植木俊哉、中谷和弘『国際条約集』（2023 年、有斐閣）110 頁。

[42] 岡田洋平「63 帰属（２）―ジェノサイド条約適用事件（ボスニア対セルビア）」『国際法判例百選［第３版］』（有斐閣、2021 年）133 頁。
なお、タディッチ事件 ICTY 上訴裁判部判決（2000 年）では、「実効的支配」基準を否定し、「全般的支配」基準を適用したが、後者が前者より緩やかな基準とは必ずしも言えない。

[43] 御巫智洋「サイバー攻撃に対する国家責任の追及に伴う課題」岩沢雄司・岡野正敬編『国際関係と法の支配―小和田恒国際司法裁判所裁判官退任記念』（信山社、2021 年）951 頁。

[44] 中谷『前掲書』（注 25）17-18, 81-83 頁。

選挙、徴税、外交、国防等に関するデータの改変・削除等もまた、内政不干渉の文脈から主権侵害を構成する（規則 4、66）[45]。一方、2018 年 5 月 23 日、チャタムハウスで行われた英国法務総裁（Attorney General's Office）のスピーチでは、「サイバー空間」においても「領域主権」が存在すると述べた上で、「禁止された干渉を超えるサイバー行動について特別な規則や追加的な禁止事項を、主権という一般原則から推測できるとすることは、現在のところ説得性を欠く（…I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention.）」とした[46]。前者は、二次規則を広く捉えて一次規則としての主権原則に「『最も重大な超えてはならない一線』を明示」するべきとの立場から、「他国を排除して国家の諸機能を行使できる権利（パルマス島事件仲裁裁定）」まで主権の内容を拡大し、サイバー空間にも他の空間と変わらず国際法上の主権原則が適用されるとする見方である[47]。「タリン・マニュアル 2.0」は、主権侵害の程度を測る要素として、「物理的損害」や「機能喪失」を挙げた[48]。なお、サイバー諜報に係る国家実行について、国際法に違反しないものの、それを遂行する方法は、主権侵害を構成し得、国際法違反となり得るとする、「タリン・マニュアル 2.0」の記載は注目される[49]。後者は、主権原則（principle of sovereignty）は、サイバー空間の独自の（sui generis）性格に即した規則（rule）が規定されなければ適用されず、未だこれが規定されていない以上、主権の残余原理（ローチュス号 PCIJ 判決）から、有害なサイバー行動が国家の主権を侵害するとは言えないとする見方である。[50]

第 4 節　アドホック委員会における議論

第 3 節で抽出した、定義、国家責任論における帰属の問題、そして、主権侵害可能性の論点を踏まえて、以下ではアドホック委員会における日欧米諸国と中露等の構図を考察する。

---

[45] 中谷『前掲書』（注 25）17-18 頁。

[46] Attorney General's Office and Jeremy Wright, "Cyber and International Law in the 21st Century" (23 May 2018) https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century (30 November 2023)

[47] 黒﨑将広「サイバー空間における主権」『サブテキスト国際法―教科書の一歩先へ―』（日本評論社、2020 年）34-43 頁。

[48] 中谷『前掲書』（注 25）17-18

[49] 中谷『前掲書』（注 25）42-43 頁；中谷和弘「サイバー諜報と国際法」『国際法外交雑誌』第 122 巻第 1 号（2023 年 5 月）1-21 頁。

[50] 黒﨑将広『前掲書』（注 47）34-43 頁。

上記の論点のうち、比較的明確な議論の違いを見せるのは、主権侵害可能性に係る問いである。主権侵害肯定説と主権侵害否定説、両者の違いを日欧米諸国と中露等の立場に当てはめる。主権侵害肯定説をとると、主権が侵害される行為と、侵害されない行為が存在することとなり、第2節で取り出した定義に沿って見れば、「サイバー犯罪」と「サイバーセキュリティ」を主権侵害の有無で区別することを可能とする点で、日欧米諸国の主張を担保する。一方、主権侵害否定説をとると、主権が侵害される行為と、侵害されない行為が区別できず、中露等の主張が導かれる。だが、これでは、第2章で見たように、アドホック委員会で中露等が強く主張してきた「主権の保護」の必要を言うことができない。「主権の保護」を主張する背景には、ブタペスト条約第32条に規定されている捜査機関による「国境を越えるアクセス」が、執行管轄権の域外適用として主権侵害に当たるとする中露等の立場がある[51]。このような立場を主張する以上、中露等は、「サイバー空間」における主権侵害可能性を肯定する立場にあるといえる。また、中露等は、同委員会で「過激主義関連犯罪」の導入を主張し、同犯罪の結果として生じる国家統制への被害を「主権侵害」と捉えていると考えられる。国家統制への被害は、国家の物理的領域のみを念頭に置く「領域主権」だけでなく、機能不全を含む「主権」への侵害結果を指すとも取れる。一方で、中露等のとる「新条約の推進」の立場では、「主権侵害否定説」に言う「サイバー空間」における「規則（rule)」が不在である現状を言う点で一致し得る。

以上の思考に照らせば、中露等の「サイバー犯罪」の定義をめぐる主張は、これまでの「主権の保護」に係る立場と相反することになる。

---

[51] なお、日本は、同条約第18条及び第32条の担保法として、刑事訴訟法を改正し、同法第99条の2に記録命令付差押えを新設しているが、同条に基づいて、域外のデータに、域内の捜査機関がアクセスし記録することは主権の制約に当たらないとの見方を示している。(第177回国会衆議院法務委員会議録第15号14頁（平23.5.31))

第４章　「サイバー犯罪」をめぐる規範形成過程の特徴
――「テロリズム」をめぐる規範形成過程との比較を通して

第１節　「サイバー犯罪」と「テロリズム」

以下では、第 1 章から第 3 章にかけて検討した「サイバー犯罪」をめぐる規範形成過程の特徴を捉え、今後の規範形成に必要な要素を検討することとしたい。その試みとして、「サイバー犯罪」をめぐる規範形成過程と、「テロリズム」をめぐる規範形成過程を比較する。

「サイバー犯罪」と「テロリズム」は、犯罪行為が複数国にまたがって構成される越境的な側面を有している一方、捜査や逮捕、訴追といった国家の執行管轄権の行使が、各国領域内に限定されており、多数国間の刑事司法協力及び捜査共助を必要としている点で、その性質が一致している。国際法上、両者は、「国際犯罪」、特に「諸国の共通利益を害する犯罪」に分類される。一般に、「諸国の共通利益を害する犯罪」とは、ひろく多数の諸国または人類が共通の利害関係をもつ特定の法益を害する行為であって、国際慣習法または条約で犯罪として処罰すべきものと定めており、これを受けて各国が刑罰法規を制定し、その実行行為者を訴追し処罰することとした犯罪をいう[52]。

このように、「サイバー犯罪」と「テロリズム」は、一見、同様の性質を有する犯罪行為である。だが、その規範形成過程には相違点も多い。そこで、第２節で「テロリズム」をめぐる規範形成過程を概観した後、第３節で両者の相違点として、定義と、国家責任論における帰属に関する議論、さらに、「引渡しか訴追か（aut dedere aut judicare）」の選択義務について検討する。第４節では、第３節までの議論を踏まえて、「サイバー犯罪」、あるいは「サイバー空間」における規範形成に必要な要素を検討する。

第２節　「テロリズム」をめぐる規範形成過程

「テロリズム」の防止・処罰のため、第２次世界大戦後、国連及び国際機関、あるいは地域的枠組みの下で、規範形成が図られてきた。

国連及び国際機関の下で採択された 14 本の条約は、一般的に「テロ防止関連諸条約」と呼ばれている。その内容は、①国際交通に関するも（航空関連犯罪、海上犯罪）、②人の保護に関するもの（人質、外交官等保護）、③テロの手段に着目するもの（核テロ、爆弾テロ）、④テロ行為の支援に関するもの（テロ資金供与）にわたる[53]。1960 年代以降世界的に

---

[52] 山本草二『国際法』（有斐閣、1994 年）50 頁。

[53] 竹内真理「Theme 9 テロ関連諸条約――条約制度の限界を克服するための国際社会の取組み」『分野別　国際条約ハンドブック』137 頁。

航空機の不法奪取（ハイジャック）が多発したことを踏まえて採択された 1970 年のハーグ条約（いわゆる「ハイジャック防止条約」）、及び、翌 1971 年に採択されたモントリオール条約（ハイジャック以外の航空機の安全を損なう行為、機内での暴力行為、爆発物の持込みなどの防止を目的とする）が、今日に至るまでのテロ防止関連条約の基本パターンを提供したという意味で重要な意義を有する[54]。これらの条約は特定行為を「犯罪」として定義し、不処罰（impunity）を許さないよう、締約国に、国内法制を整備する義務と「引渡か訴追か（aut dedere aut judicare）」の選択義務を課している。

地域的枠組みの下では、米州機構（Organization of American States：OAS）の米州テロ行為防止条約（1971 年）、欧州評議会（Council of Europe：CoE）の欧州テロリズム条約（1977 年）、アラブ連盟(League of Arab States：LAS)のテロリズム防止アラブ条約（1998 年）などがある[55]。

以上の条約が 1990 年代に形成されていたものの、2001 年 9 月 1 日には、米国同時多発テロ事件が発生したことを受けて、現在に至るまで、さらなる規範形成が目指されている。

第 3 節　両者の相違点

「サイバー犯罪」をめぐる規範形成過程と「テロリズム」をめぐる規範形成過程を比較すると、定義と、国家責任論における帰属に関する議論から主要な相違点を抽出できる。

まず、両者の定義に関する議論について検討する。「サイバー犯罪」の国際法上の定義は未だ確立していない。この点は、第 2 章と第 3 章で見たように、国連サイバー犯罪条約の作成に向けた議論を進めるにあたって、常に足かせとなっていた。各国は、条約ドラフト内で、

＊なお、同著には 13 本の条約として以下を記載している（括弧内は採択年/条約名は略称）。①航空機内の犯罪防止条約〔東京条約〕（1963 年）；②航空機不法奪取防止条約〔ヘーグ条約〕（1970 年）；③民間航空不法防止条約〔モントリオール条約〕（1971 年）；④国家代表等犯罪防止処罰条約（1973 年）；⑤人質行為防止条約（1979 年）；⑥核物質防護条約（1980 年）；⑦空港不法行為防止議定書（1988 年）；⑧海洋航行不法行為防止条約（1988 年）；⑨大陸棚プラットフォーム不法行為防止議定書（1988 年）；⑩プラスチック爆弾探知条約（1991 年）；爆弾テロ防止条約（1997 年）；⑫テロ資金供与防止条約（1999 年）；⑬核テロリズム防止条約（2005 年）。同著の列挙のほか、⑭国際民間航空についての不法な行為の防止に関する条約〔北京条約〕（2011 年）も、テロ防止関連諸条約に含まれる。

[54] 小松一郎『実践国際法（第 3 版）』（信山社、2022 年）41 頁。

[55] 中谷和弘「第 6 章　テロリズムに対する諸対応と国際法」山口厚・中谷和弘編『安全保障と国際犯罪』（東京大学出版会、2005 年）、106-109 頁。同著には、地域的枠組みの下に形成された「テロリズム」防止・処罰のための諸条約として、上記以外の条約も複数取り挙げている。

「サイバー犯罪」を定義することを目指さず、むしろ具体的な行為を条約上の対象犯罪と規定し、コンセンサスを試みている。同様に、「テロリズム」の国際法上の定義も未だ確立していない。1996 年 12 月 17 日の国連総会決議 51/210 によって創設されたテロ問題に関するアドホック委員会において包括的テロリズム防止条約の作成が審議されてきたが、テロリズム行為の定義（この条約上の対象犯罪）について一致できず、まとまるには至っていない[56]。特に、パレスチナ紛争を「占領地における自決権行使のための正当な闘争」と捉えるアラブ諸国と、「テロリズム」と捉える米国やイスラエル等の構図があった[57]。そこで、条約の作成にあたっては、テロリズムを一般的に定義することを避ける一方で、テロ現象を構成する個別の要素（行使の対象や手段など）を取り上げて、規制の対象とする手法がとられてきた[58]。

このように「サイバー犯罪」と「テロリズム」は、定義をめぐる議論が、その規範形成を硬直化させた。一方、両者の違いは、定義をめぐる議論の構図に見ることができる。「サイバー犯罪」の定義をめぐっては、限定的に解釈したい日欧米諸国と、拡大的に解釈したい中露等の構図があった。新興国の多くは、自国の国内法制を踏まえて、両者のうち、どちらか一方に全面的に肩入れするような立場を示していない。一方、「テロリズム」の定義をめぐっては、限定的に解釈したいアラブ諸国と、拡大的に解釈したい米国やイスラエル等の構図があった。さらに興味深いことに、ロシアは米国と同じ後者の立場である。2000 年代初頭、2001 年の 9・11 米国同時多発テロ事件を受けて「テロとの戦い」に挑む米国と同じく、ロシアもまた、チェチェン問題を抱え、テロリズムの防止が課題であった。米露協調と評され、2002 年には、両者の利害が一致し、NATO・ロシア理事会が設置され、米国を含むＮＡＴＯ諸国とロシアがテロ対策で協力する枠組みが構築された[59]。しかし、昨年 2 月から始まったロシアによるウクライナ侵略にあっては、かねてからあった NATO の東方拡大へのロシアによる懸念が再燃し米露協調の実態ではもはやなくなっている。

---

[56] 中谷『前掲論文』（注 55）104-106 頁。

[57] 中谷『前掲論文』（注 55）104-106 頁。

[58] 竹内真理『前掲』論文（注 53）137 頁。

[59] チェチェン問題：ロシア連邦内では、イスラム系のチェチェン共和国が分離独立を求める運動を続けており、これまでに 1994 年と 1999 年にロシア政府と大規模な武力衝突が生じている。これらの武力介入は、欧米諸国からの批判を浴びている側面もある。他方で、現在に至るまで、チェチェン共和国の分離独立を求めたテロ事件が起きるなどしており、ロシアにとって、「テロリズム」の定義を拡大的に解釈することで、事件防止につなげたい考えがあったといえる。

次に、国家責任論の観点から、「サイバー犯罪」と「テロリズム」の双方とも、犯罪行為の国家への帰属の有無が問題となる。国家責任は「国の行為」であることを要件とする（国家責任条文２条)。「私人の行為」に国家責任を言う場合には、国家への帰属が必要である。双方とも、その規範形成過程に見るように、処罰・防止に向けた国際協力の実現を目的としており、「私人の行為」を想定している。だが、現実は、これらの犯罪行為に国家の関与が疑われる場合が多い。他方、帰属を立証できずとも、国家による不作為として、相当の注意（due diligence）を問う余地はある。双方とも、帰属の立証が困難であり、立証できたとしても帰属する国家が「崩壊国家」である場合には、「相当の注意」義務さえ追求できない場合も考えられる。このように、「サイバー犯罪」と「テロリズム」を国家責任論から見ると、国家行為の同定を要件とする国家責任論に、実態との乖離が生じていることが明らかとなる。

さらに、「引渡しか訴追か（aut dedere aut judicare)」の選択義務について検討する。先述のとおり、「テロ防止関連諸条約」では多くの場合、不処罰（impunity）を許さぬよう、締約国に、「引渡しか訴追か」の義務を課してきた。例えば、航空機の不法な奪取の防止に関する条約（通称：ハーグ条約）には、４条２項に

> Each Contracting State shall likewise take such measures as may be necessary to establish its jurisdiction over the offence in the case where the alleged offender is present in its territory and it does not extradite him pursuant to Article 8 ¥to any of the States mentioned in paragraph 1 of this Article.
>
> （和訳）犯罪行為の容疑者が領域内に所在する締約国は、1 (a)、(b)又は(c)の場合に該当する他のいずれの締約国に対しても第８条の規定に従ってその容疑者を引き渡さない場合に当該犯罪行為につき自国の裁判権を設定するため、必要な措置をとる[60]。

と定めている。他方、ブタペスト条約では、22 条３項に

> Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for

---

[60] 「航空機の不法な奪取の防止に関する条約」。外務省 HP。https://www.mofa.go.jp/mofaj/gaiko/treaty/pdfs/B-S46-0241.pdf（2023 年 12 月 6 日最終閲覧。）

extradition.

（和訳）締約国は、容疑者が自国の領域内に所在し、かつ、引渡しの請求を受けたにもかかわらず当該容疑者の国籍のみを理由として他の締約国に当該容疑者の引渡しを行わない場合において第24条1に定める犯罪についての裁判権を設定するため、必要な措置をとる。[61]

と規定している。同様に、条約ドラフトでは、22条1項に、

Each State Party shall adopt such measures as may be necessary to establish its jurisdiction over the offences established in accordance with articles 6 to 16 of this Convention when

(a) The offence is committed in the territory of that State Party; or

(b) The offence is committed on board a vessel that is flying the flag of that State Party or an aircraft that is registered under the laws of that State Party at the time when the offence is committed.

（和訳）締約国は、次の場合においてこの条約の6条から16条に従って定められる犯罪についての自国の裁判権を設定するため、必要な措置をとる。

(a) 犯罪が自国の領域内で行われる場合

(b)犯罪が、当該犯罪の時に自国を旗国とする船舶内又は自国の法律により登録されている航空機内で行われる場合において

と定め、また同条3項に

For the purposes of the article on extradition of this Convention, each State Party shall take such measures as may be necessary to establish its jurisdiction over the offences established in accordance with articles 6 to 16 of this Convention when the alleged offender is present in its territory and it does not extradite such person solely on the ground that the person is one of its nationals.

（和訳）犯罪人引渡しの規定の適用上、締約国は、容疑者が自国の領域内に所在し、かつ、容疑者が自国の国民であることのみを理由として当該容疑者の引渡しを行わない場合においてこの条約の6条から16条に従って定められる犯罪についての自国の裁判権を設定するため、必要な措置をとる。

---

61 「サイバー犯罪に関する条約」。外務省HP。https://www.mofa.go.jp/mofaj/gaiko/treaty/pdfs/B-H24-006.pdf（2023年12月6日最終閲覧。）

と規定しており、これは UNCAC42 条 3 項に類似する[62]。

このように、サイバー犯罪対策においても、「テロ防止関連諸条約」と同様に、「引渡しか訴追か」の選択義務が挿入されている。ただし、同義務の対象となる犯罪の範囲は先に挙げたそれぞれの条約により異なるため、条約ドラフトが全面的に同義務を採用しているとすることは難しいとも言える。確かに、「引渡しか訴追か」の選択義務は、「不処罰」を防止し得る点で条約の実効性が期待できる。だが、引渡請求が拒否された場合に締約国内で十分な訴追がなされない可能性や、管轄権の設定にあたり締約国に国内法整備の必要性が生じ条約の普遍性が損なわれる可能性もある。テロリズムの防止には、規範形成の観点だけではなく、いわゆる失敗国家（failed State、ともすれば失敗国家が締約国に含まれる場合さえ考えられる）において醸成されるテロの温床をいかに断ち切るかといった観点が不可欠であり、「いわば刑法的対応がテロリズム行為に対する唯一の対応となっているわけではない」点からも、サイバー犯罪対策において同義務の挿入のあり方が、捜査・訴追に係る現状や、今後締約国の協力度合いによって異なる点は自然とも言える[63]。

第 4 節　「サイバー犯罪」をめぐる規範形成に必要な要素

以上の検討を踏まえて、「サイバー犯罪」をめぐる規範形成に必要な要素として、1）合意可能な規制対象となる犯罪行為の抽出と、2）犯罪行為の処罰・防止に向けた動きの定式化が挙げられる。第 2 章から第 3 章にかけて見たように、「サイバー犯罪」をめぐる規範形成ではその定義付けが論点となった。合意形成にかけては、第 3 章で検討したように、各国の主張を、従来の学説に照らし、その齟齬を減らす取組みのほか、各国の主張で合意可能な規制対象を抽出し続ける作業を通して、一貫した基準を見出すことが考えられる。また、犯罪行為の抽出と並行して、同行為の処罰・防止を、本章で検討したようなテロ関連諸条約を念頭に置いて定式化する方法が考えられる。定式化にあたり、本稿のアドホック委員会にお

---

[62] UNCAC42 条 3 項は、下記のとおりである。

3. For the purposes of article 44 of this Convention, each State Party shall take such measures as may be necessary to establish its jurisdiction over the offences established in accordance with this Convention when the alleged offender is present in its territory and it does not extradite such person solely on the ground that he or she is one of its nationals.

（和訳）第 44 条の規定の適用上、締約国は、容疑者が自国の領域内に所在し、かつ、容疑者が自国の国民であることのみを理由として当該容疑者の引渡しを行わない場合においてこの条約に従って定められる犯罪についての自国の裁判権を設定するため、必要な措置をとる。

「腐敗の防止に関する国際連合条約」。外務省 HP。https://www.mofa.go.jp/mofaj/gaiko/treaty/pdfs/B-H29-012.pdf（2023 年 12 月 7 日最終閲覧。）

[63] 中谷和弘『前掲論文』（注 55）106-109 頁。

いて第6回会合に見るような条約ドラフトの作成は重要な前例になる。だが、同ドラフトは第2章に見たように、ブタペスト条約に含まれている第 32 条の内容を挿入できないなど、コンセンサスに向けた消極的な定式化に終始している。他方、各国で国内法制に係る事情が異なる現状を踏まえると、多数国間条約の定型化ではなく、各国が独自に二国間条約を蓄積させることも一案であろう。すでに、日本は、中国やロシアを含む計7つの国・地域と二国間における刑事共助条約を締結している。同条約はテロリズムの防止・処罰を念頭に置いていることから、テロ関連諸条約等の多数国間条約との相関関係も期待できる。

おわりに

以上、第1章から第4章にかけて、アドホック委員会を題材に、サイバー犯罪、及びサイバー空間をめぐる規範形成過程の特徴を検討し、今後の合意形成に必要な要素について考察した。

国際法上の領域概念ではとらえきれない「越境性」の要素が大部分を占めるサイバー空間にあって、その規範形成過程は、これまでになく特殊である。第1章では、サイバー空間における規範形成の担い手が、先進国だけでなく、新興国、さらに個人にまで広がっている点を確認した。第2章から第3章にかけては、アドホック委員会における議論を念頭に、その合意形成の足かせとして、条約上の対象犯罪、すなわち「サイバー犯罪」の定義に着目した。上記をめぐっては、限定的に解釈したい日欧米諸国と、拡大的に解釈したい中露等の構図があった。新興国の多くは、自国の国内法制を踏まえて、両者のうち、どちらか一方に全面的に肩入れするような立場は示していない。この構図は、第4章で見たように、「テロリズム」の定義に係る議論とも異なる部分であった。そこで、本稿では、「サイバー犯罪」の定義を、『タリン・マニュアル2.0』を踏まえて、国家の「帰属」を証明できない「非国家主体」によるもので「主権侵害」の文脈から国際法上の責任を問うことができない行為、とした上で、従来の学説を振り返ると共に、アドホック委員会における各国の主張を再検討した。そして、中露の、「サイバー犯罪」の定義を拡大的に解釈する姿勢は、いわゆる主権侵害否定説と関連するが、同国が従来から「主権の保護」を強く主張してきた点を踏まえると、一貫性を欠く点に言及した。また、国家責任論における帰属に関する議論では、国家行為の同定を要件とする同議論にサイバー空間における現状との乖離を言うことができる。以上の点を踏まえて、今後のサイバー犯罪における合意形成において、さらなる議論の蓄積と、定型化、その他、多数国間条約だけでなく二国間条約の有効性を検討した。

同時に、サイバー犯罪は、その性質から、判例の蓄積が期待できない分野である。そのため、日欧米諸国と中露にとっては、新興国を積極的に取り入れ、いち早く自国に有利な合意形成を実現することが一層重要になる。その際、本稿で取り扱った、アドホック委員会で得られたコンセンサス部分と棚上げされた部分を、いかに効果的に用いるかは、各国において考慮されることになるだろう。

他方、サイバー空間において、対日欧米諸国の筆頭としてロシアがあがる一方で、中国がある種の中立的立場を模索しているようにうかがえる点は、注目される。すなわち、技術的かつ経済的にもロシアに対し優越している中国が、サイバー空間に関しては、ある種、対米の色をロシアより薄めており、いわば新興国にとって近づきやすい中立性を演出し得る点

である。

なお、サイバー犯罪を国際刑事裁判所の対象とするといった議論もある。同議論について本稿では検討しないが、規範形成の方法のひとつとして考えられるだろう。

以上、アドホック委員会に着目してサイバー空間の規範形成過程を検討した。同アドホック委員会は、翌 2024 年 1 月 29 日から最終会合が予定されており、本稿で題材として扱ったものの、未定の要素が強い。今後も動向を注視し、サイバー空間の規範形成過程についてさらに考察することとしたい。

文献表

（１）国連総会決議

- United Nations General Assembly (UNGA) Resolution 74/247, *Countering the use of information and communications technologies for criminal purposes*, A/RES/74/247 (27 December 2019) available from http://undocs.org/A/RES/74/247
- UNGA, *Countering the use of information and communications technologies for criminal purposes*, A/RES/75/282 (26 May 2021), available from undocs.org/A/RES/75/282
- UNGA, *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
- UNGA, *International code of conduct for information security* , A/66/359 (14 September 2011) available from undocs.org/A/66/359
- UNGA, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Scurity*, A/64/201 (30 July 2010)
- UNGA, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Scurity*, (24 June 2013), available from undocs.org/A/68/98
- UNGA, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Scurity* , (22 July 2015), available from undocs.org/A/70/174

（２）アドホック委員会の各会合における意見書と統合交渉テキスト、条約ドラフト

- United Nations, “Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes,” available from https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home
- 第１回会合―UNGA, Compilation of views submitted by Member States on the scope, objectives and structure (elements) of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, A/AC.291/4, (17 November 2021), available from http://undocs.org/A/AC.291/4
- 第２回会合―UNGA, *Compilation of proposals and contributions submitted by Member States on the provisions on criminalization, the general provisions and the provisions on procedural measures and law enforcement of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes*, A/AC.291/9 (21 April 2022), available from http://undocs.org/A/AC.291/9
- 第３回会合―UNGA, *Compilation of proposals and comments submitted by Member States*

on provisions on international cooperation, technical assistance, preventive measures and the mechanism of implementation, the final provisions and the preamble of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, A/AC. 291/12 (3 August 2022), available from http://undocs.org/A/AC.291/12

- 第 4 回会合—UNGA, *Consolidated negotiating document on the general provisions and the provisions on criminalization and on procedural measures and law enforcement of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes*, A/AC.291/16（7 November 2022）, available from http://undocs.org/A/AC.291/16
- 第 5 回会合—UNGA, *Consolidated negotiating document on the preamble, the provisions on international cooperation, preventive measures, technical assistance and the mechanism of implementation and the final provisions of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes*, A/AC.291/19 (19 December 2022), available form http://undocs.org/A/AC.291/19
- UNGA, *Letter dated 30 July 2021 from the chargé d'affaires a.i. of the Russian Federation to the United Nations addressed to the Secretary-General*, A/AC.291/9(21 April 2022), pp.7-9, available from http://undocs.org/A/75/980
- 第 6 回会合—UNGA, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, A/AC.291/22 (29 May 2023), available from http://undocs.org/A/AC.291/22
- UNGA, *Plenary Working Document, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*,(2 September 2023),available from https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/DTC/DTC_rolling_text_02.09.2023.pdf

（3）書籍・論文他

- Attorney General's Office and Jeremy Wright, "Cyber and International Law in the 21st Century" (23 May 2018) https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century（2023 年 11 月 30 日最終閲覧）
- 「サイバー犯罪に関する条約（略称：サイバー犯罪条約（通称：ブダペスト条約））」。外務省 HP。(2023 年 12 月 6 日最終閲覧。) https://www.mofa.go.jp/mofaj/gaiko/treaty/treaty159_4.html
- 「サイバー行動に適用される国際法に関する日本政府の基本的な立場(2021 年 5 月 29 日)」。

外務省 HP。https://www.mofa.go.jp/mofaj/gaiko/page3_003059.html（2023 年 11 月 30 日最終閲覧。）
- 「航空機の不法な奪取の防止に関する条約」。外務省 HP。https://www.mofa.go.jp/mofaj/gaiko/treaty/pdfs/B-S46-0241.pdf（2023 年 12 月 6 日最終閲覧。）
- 「腐敗の防止に関する国際連合条約」。外務省 HP。https://www.mofa.go.jp/mofaj/gaiko/treaty/pdfs/B-H29-012.pdf（2023 年 12 月 7 日最終閲覧。）
- 赤堀毅。『サイバーセキュリティと国際法の基本―国連における議論を中心に―』。東信堂，2023 年。
- 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」。『安全保障研究』２巻２号（2022 年３月）：233-250 頁。https://www.nids.mod.go.jp/publication/security/pdf/2022/202203_12.pdf（2023 年 11 月 26 日最終閲覧。）
- 小松一郎。『実践国際法（第３版）』。信山社，2022 年。
- 黒﨑将広、坂元茂樹、西村弓、石垣友明、森肇志、真山全、酒井啓亘。『防衛実務国際法。弘文堂，2021 年。
- 黒﨑将広。「サイバー空間における主権」。『サブテキスト国際法―教科書の一歩先へ―』所収，34-43 頁。日本評論社，2020 年。
- 松原実穂子。「『第五の主戦場』サイバー攻撃応酬の脅威」。『外交 Vol72』（都市出版，2022 年）：32-39 頁。
- 御巫智洋。「サイバー攻撃に対する国家責任の追及に伴う課題」。岩沢雄司・岡野正敬編『国際関係と法の支配―小和田恒国際司法裁判所裁判官退任記念』所収，937-958 頁。信山社，2021 年。
- 御巫智洋。「インターネットの利用に関する国際的なルールにおいて領域主権が果たす機能」。『国際法外交雑誌』第 121 巻第１号（2022 年５月）：1-29 頁
- 最上敏樹。『国際機構論講義』。有斐閣，2016 年。
- 中谷和弘、河野桂子、黒崎将広。『サイバー攻撃の国際法 タリン・マニュアル 2.0 の解説増補版』。信山社，2023 年。
- 中谷和弘。「サイバー諜報と国際法」。『国際法外交雑誌』第 122 巻第１号（2023 年５月）：1-21 頁。
- 中谷和弘。「サイバー攻撃と国際法」。『国際法研究』第３号（2015 年３月）：59-101 頁。
- 中谷和弘。「第６章　テロリズムに対する諸対応と国際法」。山口厚・中谷和弘編『安全保障と国際犯罪』103-126 頁。所収，東京大学出版会，2005 年。
- 岡田陽平。「63 帰属（２）―ジェノサイド条約適用事件（ボスニア対セルビア）」。『国際法判例百選［第３版］』所収，132-133 頁。有斐閣，2021 年。
- 大谷潤一郎「『サルバドール宣言』の意義と概要」。『ジュリスト 特集・第 12 回国連犯罪防

止・刑事司法会議』No.1411（2010 年 11 月）：42-47 頁。
- 佐々木孝博。「サイバー空間の施策に関するロシアと欧米諸国のアプローチ」。『日本大学大学院総合社会情報研究科紀要』14 号（2013 年 7 月）：1-12 頁。https://gssc.dld.nihon-u.ac.jp/wp-content/uploads/journal/pdf14/14-001-012-Sasaki.pdf（2023 年 11 月 26 日最終閲覧。）
- Shanghai Cooperation Organization (SCO), "Bishkek Declaration by the Heads of the Member States of the SCO" (August 2007), available from http://eng.sectsco.org/documents/ (last visited 26 November 2023)
- SCO, "Ufa Declaration by the Heads of the Member States of the SCO" (July, 2015) , available from http://eng.sectsco.org/documents/ (last visited 26 November 2023)
- SCO, Agreement on Cooperation in Ensuring International Information Security between the Member States of the SCO, (2009), available from http://eng.sectsco.org/documents/ (last visited 26 November 2023)
- 竹内真理。「Theme 9 テロ関連諸条約――条約制度の限界を克服するための国際社会の取組み」。『分野別　国際条約ハンドブック』所収，136-151 頁。有斐閣，2020 年
- 土屋大洋。『サイバーグレートゲーム――政治・経済・技術とデータをめぐる地政学』千倉書房，2020 年。
- 植木俊哉、中谷和弘。『国際条約集』有斐閣，2023 年。
- 山本草二。『国際法』。有斐閣，1994 年。
- 柳原正治、森川幸一、兼原敦子編。『プラクティス国際法講義〈第 3 版〉』信山社，2017 年

謝辞

論文の執筆にあたり、御指導を賜りました中谷和弘先生に、心より感謝申し上げます。また、外務省の赤堀毅地球規模課題審議官、在ウィーン国際機関日本政府代表部の今西靖治公使、内閣府の山田哲也参事官、外務省の待鳥紗慧主査におかれましては、お忙しい中お時間をお取りくださり、サイバー空間をめぐる国際情勢や、国連サイバー犯罪新条約作成に向けた交渉等について、詳細に御教示いただきました。誠にありがとうございます。

そして、修士課程に在籍しながら働くことに御理解と御支援を賜りました職場の皆様に、御礼申し上げます。

最後に、これまでの学生生活を温かく支えてくれた家族と友人たちにも感謝の意を表します。