論題 Title	選挙介入における偽情報の流布と国際法
他言語論題 Title in other language	Disinformation as a Means of Election Interference and International Law
著者 / 所属 Author(s)	樋山 千冬（HIYAMA Chifuyu）/ 国立国会図書館調査及び立法考査局　外交防衛課長
雑誌名 Journal	レファレンス（The Reference）
編集 Editor	国立国会図書館 調査及び立法考査局
発行 Publisher	国立国会図書館
通号 Number	871
刊行日 Issue Date	2023-7-20
ページ Pages	49-62
ISSN	0034-2912
本文の言語 Language	日本語（Japanese）
摘要 Abstract	選挙介入と呼ばれる国家による非公然のサイバー行動の中でも特に偽情報の流布に焦点を当て、国際法上の武力行使禁止原則、不干渉原則、主権侵害の禁止、内的自決に関して学説を中心に整理する。

選挙介入における偽情報の流布と国際法

国立国会図書館　調査及び立法考査局
外交防衛課長　樋山　千冬

目　　次

キーワード：選挙介入、偽情報、不干渉原則、主権侵害、内的自決

要　旨

① 2016年の米国大統領選挙を始め、選挙の際に外国の機関又は外国のコントロール下にある私人によって、「選挙介入」と呼ばれる非公然のサイバー行動（cyber operation）が行われるようになった。この選挙介入は、ソーシャルメディアを利用した偽情報（disinformation）の流布等から成る。こうした選挙介入について国際違法行為として検討すべきとの見解が現れている。

② 国家によるサイバー行動としての選挙介入には、国際法が適用されると考えられる。学説上は、慣習国際法上の武力行使禁止原則に抵触するか、不干渉義務に違反するか、主権侵害を構成するかという点から専ら検討される。

③ 国際法の学説上、国家によるサイバー行動としての選挙介入は、武力行使禁止原則に直接抵触しているとは考えられていない。不干渉原則違反については、干渉の客観的構成要件である強制（coercion）が論点となる。選挙介入や偽情報の流布が強制に当たるかどうかについては、学説は必ずしも一致をみていない。選挙介入の欺瞞的な性質に照らして、これまでの議論が強制を狭く捉えすぎているとの主張も現れている。

④ 主権侵害に関連した議論は必ずしも十分ではないようであるが、自決権との関係が議論されるようになっている。人民の自決権は内的自決によって充足されるが、内的自決は自由権規約の定める自由権と結び付いており、政治プロセスにおいて事実面で正確な情報が提供される必要があるとして、選挙介入とりわけ偽情報の流布が自決権を侵害し得ると主張される。

⑤ 国家によるサイバー行動としてなされる選挙介入と偽情報の流布に関する各国の国家実行及び法的信念はなお明らかではないが、選挙制度による民主主義制度を採用する国においては、選挙介入や偽情報の流布は内的自決を妨げる行為と考えることもできよう。

はじめに

近年、国政選挙に際して、外国の機関や外国のコントロール下にあるとみられる私人等により、ソーシャルメディアを通じて偽情報（disinformation）が流布されることが相次いでいる。2016年の米国大統領選挙はその最たるものの一つであろう。こうした偽情報の流布は、選挙陣営の秘密情報をハッキングしインターネット上にリークするといった行為等とともに行われ、有権者の判断に影響を及ぼすことで、選挙に介入する、又は選挙結果を自国に有利なものとすることを企図して行われたという(1)。

選挙介入のターゲットとなった国は、偽情報の流布に関与したとみられる国家に対する外交上の非難を行ったり、関与したとの疑いのある個人を制裁の対象としたり、アカウントの窃取等の行為を刑事訴追したりする例があるが(2)、インターネット上で選挙介入の一部として行われる偽情報の流布についても、国家によるサイバー行動（cyber operation）であり国際法に違反する行為として検討すべき旨の指摘がなされるようになってきている(3)。

本稿では、選挙介入とされる問題について、特に偽情報の流布に注目し、問題の概要を振り返る。その上で、そもそも国際法が適用され得るのか、適用可能とすればどのような国際法が適用され、国際法上どのように評価されるかについて、学説を中心に整理を試みる。

Ⅰ　選挙介入における偽情報の流布とは何か

1　「偽情報」の定義

「偽情報」は、国際法上は一意の定義はなされているとはいえない。ただし、偽情報の流布をめぐる一連の事態を受け、国際組織によって作成された文書の中に、定義を試みているものがある。

その代表的な例として、2017年の欧州評議会（Council of Europe）による定義では、事実に反する文脈、偽の内容、操作された内容、捏造された内容で構成され、意図的に個人、社会集団、組織又は国に害を与えるために作られた情報が「偽情報」であるとされている。誤った論理や誤解を招く内容から成るものの害をもたらす意図を伴わずに作り出される「誤情報」

＊　本稿におけるインターネット情報の最終アクセス日は、2023年6月2日である。

(1)　米国のシンクタンクである大西洋評議会（Atlantic Council）による2018年のレポートでは、2014年のウクライナ大統領選挙、2016年の英国のEU脱退に関するレファレンダム、2016年の米国大統領選挙において、本質的に虚偽であるか、又は歪曲された事実が蔓延したという。Laura Galante and Shaun Ee, “Defining Russian election interference: An analysis of select 2014 to 2018 cyber enabled incidents,” *Issue Brief*, Atlantic Council, 2018.9.11, pp.5, 7. <https://www.atlanticcouncil.org/wp-content/uploads/2018/09/Defining_Russian_Election_Interference_web.pdf>

(2)　U.S. Department of Justice, Office of Public Affairs, “Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election,” 2018.7.13. <https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election>; U.S. Department of the Treasury, “Treasury Escalates Sanctions Against the Russian Government's Attempts to Influence U.S. Elections,” 2021.4.15. <https://home.treasury.gov/news/press-releases/jy0126>; Thomas Rid, *Active measures: the secret history of disinformation and political warfare*, New York: Farrar, Straus and Giroux, 2020, pp.414-415.

(3)　Judit Bayer et al., “Disinformation and propaganda: impact on the functioning of the rule of law in the EU and its member states,” *European Parliament Study*, 2019, p.139.（なお、同著者による2021年版のレポートでは国際法上の論点は扱われていない。）ほかに、飯塚恵子『ドキュメント誘導工作―情報操作の巧妙な罠―』中央公論新社, 2019, p.55; Kate Jones, “Legal loopholes and the risk of foreign interference,” *In Depth Analysis*, Directorate-General for External Policies, European Parliament, 2023.1, p.15.

（misinformation）とは区別されている(4)。また、欧州連合（European Union）の執行機関に当たる欧州委員会（European Commission）は、2018年の欧州議会、欧州理事会、欧州経済社会評議会及び地域委員会へのコミュニケーションにおいて、「偽情報は、経済的な利得のために又は意図的に公衆を欺くために作成され、提示され、拡散され、かつ公共に害を与えるかもしれない、誤りと証明できる、又は誤解を生む情報と理解される。公共への害は、民主的な政治及び政策決定の過程に対する脅威、EU市民の健康、環境及び安全といった公共財に対する脅威から成る」(5)と述べている。こうした定義は、しばしば政治的な文脈で用いられる表現であるフェイクニュース（fake news）とも異なり、内容が真か偽かというだけでなく、政治過程にどのような影響を及ぼすかをも考慮したものとなっているといえる。

2　選挙介入と偽情報の流布

前述の偽情報とその流布は、インターネット及びソーシャルメディアの普及に伴って、主としてソーシャルメディア上で展開される選挙介入（election interference）の一部として問題視されるようになった。

この選挙介入は、冷戦期における偽情報の流布(6)とは様相が異なり、国の機関やそのコントロール下にある私人による他国に対する非公然のサイバー行動(7)（covert cyber operation）として行われるが、その内容は、おおむね次のようなものである(8)。

・個人に関する、又は保護された情報を入手するためにハッキングを行い、個人、公人、企業又は政府に損害を与えるために当該情報を公表する。
・他の国において、選挙を含む国内政治に影響を及ぼすために偽情報を流布する。
・DDoS攻撃(9)又は類似の技術を用いて、情報通信システムを混乱させる。

また、ソーシャルメディアが欺瞞的な偽情報の伝達手段となっているとの前提に立ち、その手法は次のように解されている(10)。

---

(4)　Claire Wardle and Hossein Derakhshan,“Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking,”*Council of Europe report*, DGI(2017)09, 2017.9.27, p.20. <https://rm.coe.int/information-disorder-toward-an-i,nterdisciplinary-framework-for-researc/168076277c>

(5)　European Commission,“Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Tackling online disinformation: a European Approach,”COM(2018) 236 final, 2018.4.26, pp.3-4. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0236>

(6)　冷戦期における偽情報の流布については、例えば、Ashley Deeks et al.,“Addressing Russian influence: what can we learn from U.S. Cold War counter-propaganda efforts?”2017.10.25. Lawfare website <https://www.lawfareblog.com/addressing-russian-influence-what-can-we-learn-us-cold-war-counter-propaganda-efforts>

(7)　サイバー行動とは、一般に、「サイバー空間において、又はサイバー空間を通じて、目的を達成するためにサイバー能力を行使すること」と定義される。Michael N. Schmitt, ed., *Tallinn manual 2.0 on the international law applicable to cyber operations*, 2nd ed., Cambridge: Cambridge University Press, 2017, p.564.

(8)　David P. Fidler, *Advanced introduction to cybersecurity law*, Cheltenham: Edward Elgar, 2022, p.101.

(9)　「分散型サービス拒否」。インターネットに接続された多数のデバイスから、特定のサーバーやネットワーク等に対し、一斉に負荷をかけてサービスを停止させる。「DDoS攻撃とは？」2022.8.13. NTT東日本ウェブサイト <https://business.ntt-east.co.jp/content/cloudsolution/column-331.html> 悪意ある第三者が多数のパソコンにコンピューターウイルスを送り込んで感染させ、それらを踏み台として行われることもある。「分散型サービス拒否攻撃」『デジタル大辞泉』JapanKnowledge (小学館), 2023.5.

(10)　Samuel C. Woolley and Philip N. Howard,“Computational propaganda worldwide,”Samuel C. Woolley and Philip N. Howard, eds., *Computational propaganda: political parties, politicians, and political manipulation on social media*, New York: Oxford University Press, 2019, pp.4-5. 真偽を取り混ぜた「ナラティブ」の形を取ることもある。川口貴久「権威主義国家によるデジタル影響工作と民主主義」一田和樹ほか『ネット世論操作とデジタル影響工作―「見えざる手」を可視化する―』原書房, 2023, p.209.

・ソーシャルメディアのネットワーク上で、誤解につながる情報を意図的に操作し流布させるために、アルゴリズム、自動化、人の手によるキュレーション(11)を用いる。
・特定の政治的なメッセージを増幅したり抑えたりするために、実在する人間と同じように振る舞うボット（例えば、自動的にオンラインでの会話を生成したり応答したりする。）を作成し、ソーシャルメディア上に展開する。
・オンライン上の情報を操作し、人々の意見、究極的には行動を変容させることを目標とする。

3　選挙介入を受けた国の反応と国際法

選挙介入を行う動機と能力を有する最大の脅威は、国家であると評される(12)。こうした国家による選挙介入は、国際政治や各国の軍事戦略に関する議論の中では、誘導工作(13)、ハイブリッド戦（hybrid warfare）や情報戦（information warfare）(14)といった国家によるサイバー行動の一環として捉えられる。

一方、国際法上はどのように評価されるであろうか。その手掛かりとなるのが選挙介入を受けた国の公式レベルの反応である。一般的に、対外的に国を代表する国家元首の行為などは、国の態度又は意思表明として、国際法上、慣習国際法の客観的要素である国家実行（state practice）と考えられる(15)。選挙介入を受けたとされる側の国の公式レベルの反応もまた国家実行と呼び得るであろう。こうした反応は、選挙介入に関して国際法が適用されない、適用可能な国際法がそもそも存在しない、あるいは、選挙介入が国際法に違反しないとのいずれの考えによるものか、慣習国際法の主観要素である法的信念（opinio juris）(16)を知る手掛かりとなろう。

2016年の米国大統領選挙の後、バラク・オバマ（Barack Obama）大統領（当時）は、当該の選挙への介入が外国の機関による活動であると判明したとして、そうした活動が「確立した行動規範を蝕み」、「民主的なガバナンスへの介入」であるとして反対するとする非難声明を発出した(17)。この声明には、明確な形で国際法違反と指弾する表現は含まれていなかった。また、米国務省法律顧問は、同意のないサイバー行動が他の国の主権を侵害するか否かは米国政府内の法律家が注意深く研究すべき、かつ、各国の国家実行及び法的信念を通じて解かれるべき問

⑾　インターネット上の情報の収集、分類、再構築をいうが、美術館や博物館での展示の意から転用されて肯定的な文脈で用いられていた。「キュレーション」『日本大百科全書』JapanKnowledge (小学館), 2023.5.

⑿　川口貴久･土屋大洋『現代の選挙介入と日本での備え―サイバー攻撃とSNS上の影響工作が変える選挙介入―』2019, p.16. 東京海上日動リスクコンサルティングウェブサイト <https://www.tokio-dr.jp/service/politics/rispr/pdf/pdf-rispr-01.pdf>

⒀　飯塚　前掲注⑶著者は、「外国が別の国に対し、主に情報を使って政治や社会に影響を与えようとする動き」の中に、「敵意ある政治目的のため、偽情報や偏向ニュースを広範かつ意図的に拡散すること」とする「情報操作」（information manipulation）の定義とともに、偽情報の定義を紹介している。同, pp.52-53.

⒁　例えば、廣瀬陽子『ハイブリッド戦争―ロシアの新しい国家戦略―』講談社, 2021, pp.103-104; Scott Jasper, *Russian cyber operations: coding the boundaries of conflict*, Washington D.C.: Georgetown University Press, 2020, p.121.（日本語訳：スコット・ジャスパー（川村幸城訳）『ロシア・サイバー侵略―その傾向と対策―』作品社, 2023.）

⒂　浅田正彦編著『国際法　第5版』東信堂, 2022, p.42; Michael Wood, "State practice," Rüdiger Wolfrum, ed., *Max Planck encyclopedia of public international law*, vol.9, Oxford: Oxford University Press, 2012, pp.510-511.

⒃　岩沢雄司『国際法』東京大学出版会, 2020, p.58.

⒄　"Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment," Dec. 29, 2016. Office of the Press Secretary, White House website <https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity#:~:text=All%20Americans%20should%20be%20alarmed,levels%20of%20the%20Russian%20government>

題だと述べるにとどまった[18]。

このように選挙介入を受けたとされる側の国が曖昧な方針とされる態度をとる理由については、情報技術の進展による不確実性に対応するために、各国は自由に行動できる余地をあえて残しているためだという解釈がある[19]。また、国際法上の干渉（後述）に相当するかを直接判断せずに、強制を伴わなくとも影響力を行使しようとする行為について「選挙介入」という表現が用いられているとも評されているところである[20]。

しかし、明確に国際法の観点から問題視する動きも出てきている。欧州議会（European Parliament）[21]は、2022年3月に採択した決議「欧州連合におけるあらゆる民主的プロセスにおける外国の介入」において、外国による情報操作（information manipulation）等の介入の手法が市民の投票行動に影響を与え、対立的な論争、社会の分断・分極化を深め、民主的な選挙やレファレンダムの公正さを損ない、政府への不信などを招くものであるとして国際法違反を構成する、との認識を示している[22]。ただしこの決議も、選挙介入がどのような国際法違反となるのかは明示していない。

Ⅱ　国際法上の論点

本章では、選挙介入、また選挙介入における偽情報の流布について、国際法上の学説を中心に整理する。学説は慣習国際法の証拠の一つであるとされるので[23]、学説について改めて検討を加えることで、選挙介入に関する現時点での国際法上の評価について、明らかにできると考えられよう。

1　国際法の適用可能性

まず、国家による他国へのサイバー行動に対して国際法が適用可能であるか（適用可能性）について確認しておきたい。この国際法の適用可能性については、国家間で一応の合意が存在すると考えられる。

国際連合総会（以下「国連総会」）は、「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に関する政府専門家グループ」（Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: UNGGE）による会合を、2004年から5回にわたり断続的に設けてきている[24]。UNGGEは2013年及び2015

⑱ Brian J. Egan, “International Law and Stability in Cyberspace,” *Berkely Journal of International Law*, 35(1), 2017, p.174. <https://www.law.berkeley.edu/wp-content/uploads/2016/12/BJIL-article-International-Law-and-Stability-in-Cyberspace.pdf>

⑲ Dan Efrony and Yuval Shany, “A rule book on the shelf? Tallinn Manual 2.0 on cyberoperations and subsequent state practice,” *American Journal of International Law*, 112(4), 2018.10, p.588.

⑳ Chimène I. Keitner, “Foreign election interference and international law,” Duncan B. Hollis and Jens David Ohlin, eds., *Defending democracies: combating foreign election interference in a digital age*, New York: Oxford University Press, 2021, p.189.

㉑ 欧州議会は、欧州連合において欧州理事会（Council of the European Union）とともに立法機能を有する。

㉒ “Foreign interference in all democratic processes in the European Union: European Parliament resolution of 9 March 2022 on foreign interference in all democratic processes in the European Union, including disinformation,” 2020/2268(INI), para. E. <https://www.europarl.europa.eu/doceo/document/TA-9-2022-0064_EN.pdf>

㉓ 国際司法裁判所規程第38条第1項(d); 岩沢　前掲注⑯, p.72; 酒井啓亘ほか『国際法』有斐閣, 2011, pp.172-173.

㉔ United Nations Office of Disarmament Affairs, “Fact sheet: developments in the field of information and telecommunication in the context of international security,” 2019.7. <https://front.un-arm.org/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf>

年に国家によるサイバー行動に国際法が適用されるとする旨の報告書[25]をそれぞれ提出し、国連総会はこれらの報告書を歓迎する決議を採択した[26]。2019年にはすべての加盟国に開かれた「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に関するオープン・エンド作業部会」（Open-ended working group on developments in the field of information and telecommunications in the context of international security: OEWG）と「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に関する政府専門家グループ」（Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security: GGE）とを別に設け、2021年にはOEWGとGGEが報告書をそれぞれ国連総会に提出し、国際法の適用可能性が改めて確認されている[27]。

また、NATO（北大西洋条約機構）のサイバー防衛協力センター（Cooperative Cyber Defence Centre of Excellence: CCDCOE）の支援の下で、NATO加盟国でない国の出身者も参加した国際法の専門家グループにより、サイバー行動に関する慣習国際法を確認し条文の形で記述することを目指して『タリン・マニュアル2.0』[28]が2017年に刊行された。この『タリン・マニュアル2.0』は、法的な拘束力は持たないものの、この分野で一定の権威を有すると評されている[29]。同書は、サイバー空間が国際法上の主権原則に服する理由として「サイバー行動は、国家が主権的権限を行使する領域において行われ、及び国家が主権的権限を行使する物に対して行われ、又は国家が主権的権限を行使する人若しくは組織によって行われる」と述べて[30]、国際法の適用可能性を確認している。

２　国家によるサイバー行動としての選挙介入と関係する国際法の諸原則

国家によるサイバー行動としての選挙介入は、国家責任法[31]の枠組みから捉えると、国家の機関による行為、国家の指揮又はコントロール下にある私人による行為、又は国家の是認した私人の行為のいずれかであり[32]、その責任は国家に帰属する。国際法の主体である国家は、

⑵⑸　UNDoc. A/68/98, para.16. <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf?OpenElement>; UNDoc. A/70/174, paras.24-29. <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement> これらの報告書においては、国家による情報通信技術の使用について国際法が適用可能であるかが述べられているところであるが、国家によるサイバー行動への国際法の適用可能性について述べたものと解されている。例えば、François Delerue, *Cyber operations and international law*, Cambridge: Cambridge University Press, 2020, p.5; Henning Lahmann, *Unilateral remedies to cyber operations: self-defence, countermeasures, necessity, and the question of attribution*, Cambridge: Cambridge University Press, 2020, p.21. 日本政府による解釈については次を参照。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』2021.5.28, p.1. <https://www.mofa.go.jp/mofaj/files/100200951.pdf>

⑵⑹　UNDoc. A/RES/68/243. <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/454/03/PDF/N1345403.pdf?OpenElement>; UNDoc. A/RES/70/237. <https://daccess-ods.un.org/tmp/9941848.51646423.html>

⑵⑺　UNDoc. A/75/816, para.34. <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/068/72/PDF/N2106872.pdf?OpenElement>; UNDoc. A/76/135, para.69. <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/075/86/PDF/N2107586.pdf?OpenElement> 一連の経緯については次を参照。“Developments in the field of information and telecommunications in the context of international security.” United Nations Office for Disarmament Affairs website <https://disarmament.unoda.org/ict-security/>

⑵⑻　Schmitt, ed., *op.cit.*(7)

⑵⑼　中谷和弘ほか『サイバー攻撃の国際法―タリン・マニュアル2.0の解説―』信山社, 2018, p.v.

⑶⓪　同上, p.5.

⑶①　国家責任法は、国が国際違法行為を行ったときに、他国がその責任を追及し、原状回復、金銭賠償などを請求する際の要件、効果、手続等を定める。岩沢　前掲注⑯, p.560.

⑶②　サイバー行動は、国家のコントロール下にない私人又は私人の集団により行われることがある。こうした私人の行動は、国家に帰属しない限りは国際法の規律するところではないが、他国の権利に反するような重大で有害な結果をもたらすサイバー行動が行われ、国家が当該の私人又は私人の集団に対して自国の領域の使用を許容す

国際法上の違法行為について責任を負う。つまり、ある行為が国家に帰属し、当該行為が国際義務違反（国際違法行為）である場合に国家責任が生じる。

この国際義務違反を規律する淵源には、条約、慣習国際法、法の一般原則等があるが(33)、サイバー行動について直接に規律するような条約は今のところ存在せず、一般国際法である慣習国際法に照らして議論されることになる(34)。こうした議論において国際義務違反の有無について検討される慣習国際法上の原則は、サイバー行動の烈度（intensity）(35)とそのもたらす侵害（harm）の大きいものから、武力行使禁止原則、不干渉原則、主権侵害の禁止であり、とりわけ選挙介入について問題とされるのは後2者である。以下、各原則についての議論を整理するとともに、より新たな議論として自決権に関するものを取り上げる。

（1）武力行使禁止原則（jus ad bellum; jus contra bellum）

国際連合憲章第2条4項は、「すべての加盟国は、その国際関係において、武力による威嚇又は武力の行使を、いかなる国の領土保全又は政治的独立に対するものも、また、国際連合の目的と両立しない他のいかなる方法によるものも慎まなければならない」と定め、武力の行使を一般的に禁止した（武力行使禁止原則）。この武力行使禁止原則は、1970年の国連総会決議「友好関係原則宣言」(36)等を通じて確認され、国際司法裁判所は1986年のニカラグア事件判決（本案）において武力行使禁止原則が慣習国際法であるとした(37)。

この武力行使禁止原則がサイバー行動にも適用される点については、各国の見解は一致しているという(38)。『タリン・マニュアル2.0』は、「いかなる国家の領土保全若しくは政治的独立に反する、又は国連の目的と両立しない他のいかなる方法による威嚇若しくは武力の行使を構成するサイバー行動も、違法である」として、武力行使禁止原則がサイバー行動にも適用されることを確認し（規則68（武力による威嚇又は武力の行使の禁止））(39)、「サイバー行動は、その規模及び効果が武力の行使の水準に至る非サイバー行動に比肩し得る場合、武力の行使に該当する」として、ニカラグア事件判決の採用した規模及び効果（scale and effects）基準(40)を準用している（規則69（武力の行使の定義））(41)。このようにサイバー行動のもたらす効果に着目し武力行使に相当するか否かを判断する考え方は、2013年の『タリン・マニュアル』（初版）

るような場合に、相当の注意義務（due diligence）違反が成立し、国家責任が生じる可能性がある。Delerue, *op.cit.*(25), pp.210-211.『タリン・マニュアル2.0』は、私人又は私人の集団の行動がある国の領域のみならずその国の政府の支配下にあるサイバーインフラにおいて展開される場合も考慮に入れ、当該国の国家責任について検討している（規則6）。

(33) 岩沢　前掲注(16), p.575; 浅田編著　前掲注(15), p.175.

(34) 例えば、Duncan Hollis, “The Influence of war; the war for influence,” *Temple International and Comparative Law Journal*, 32(1), 2018.4, p.39.

(35) 例示を試みたものとして、Terry D. Gill, “Non-Intervention in the Cyber Context,” Katharina Ziolkowski, ed., *Peacetime regime for state activities in cyberspace: international law, international relations and diplomacy*, Tallinn: NATO CCD COE Publication, 2013, p.234.

(36) 「国際連合憲章に従った諸国間の友好関係及び協力についての国際法の原則に関する宣言」UNDoc. A/RES/2625(XXV).

(37) Military and paramilitary activities in and against Nicaragua (Nicaragua v. US)(Merits, Judgement), *ICJ Reports* 1986, para.188.

(38) Marco Roscini, “Cyber operations as a use of force,” Nicholas Tsagourias and Russell Buchan, eds., *Research handbook on international law and cyberspace*, 2nd ed., Cheltenham: Edward Elgar, 2021, pp.297-298.

(39) 中谷ほか　前掲注(29), pp.74-75.

(40) *ICJ Reports*, *op.cit.*(37), para.195.

(41) 中谷ほか　前掲注(29), p.75.

から採用されていた(42)。

サイバー行動が国際法の禁じる武力行使に相当する場合があるとの考え方は、幾つかの国によって明確に支持されている。例えばドイツは、サイバー行動がより広範な物理的な（kinetic）力による武力攻撃の一環としてなされる場合や、サイバー攻撃それ自体が多数の犠牲者を出すような損害を与える場合に武力の行使となり得るとして武力行使禁止原則に抵触するとの考えを示している(43)。またオランダも、サイバー行動の規模及び効果が非サイバー行動における武力の行使の水準に匹敵する場合があるとする(44)。オーストラリアも同様の考え方を既にとっており、行動の規模及び効果が国際法における武力の行使の水準に達する伝統的な物理的行動に比肩し得るか否かを考慮すべきとする(45)。このように、サイバー行動が財産を損壊し人を殺傷する物理的な攻撃に匹敵する場合、国連憲章第２条４項の禁じる武力行使に該当するとの一般的な合意があるとされる。しかし、インフラを物理的に破壊せずに機能を失わせる場合についての合意は存在しないという(46)。

ともあれ、選挙介入ひいては偽情報の流布に関する国際法上の議論では、選挙介入は武力行使とされる閾値（threshold）――この問題自体が国際法上の重要な論点であるが(47)――を超えないものとしているか(48)、武力行使禁止原則についてはそもそも直接検討していないかのいずれかである。少なくとも選挙介入や偽情報の流布といった行為が単独で武力不行使原則に抵触するとは考えられていないものと思われる。

(2) 不干渉原則（principle of non-intervention）

サイバー行動は、武力行使でなく、なおかつ国連憲章第２条４項違反となる行為ではなくとも、不干渉原則の違反に相当する場合がある(49)。サイバー行動による選挙介入や偽情報の流布についての議論では、専ら国際法上の不干渉原則への違反に当たるか否かが論点となっている。

前提として、国は他国の国内問題に干渉してはならない（不干渉原則）。干渉（intervention）は、一般に、ある国による、特定の行為や結果を他国に強要することを目的とする、当該他国の国内事項又は対外事項における強制的（forcible）又は命令的（dictatorial）な介入（interference）と捉えられる(50)。不干渉原則は、国家の権利つまり主権、領土的一体性、政治的独立性から

---

(42) 『タリン・マニュアル 1.0』規則 11. この考え方については次の資料も参照。Johann-Christoph Woltag, *Cyber warfare: military cross-border computer network operations under international law*, Cambridge: Intersentia, 2014, pp.143-146.

(43) Federal Government, "On the application of international law in cyberspace: position paper," 2021.3, p.6. Federal Foreign Office of Germany website <https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf>

(44) "Appendix: international law in cyberspace: Letter to the parliament on the international legal order in cyberspace," 2019.7.5, pp.3-4. Government of the Kingdom of the Netherlands website <https://www.government.nl/binaries/government/documenten/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace/international-law-in-the-cyberdomain-netherlands.pdf>

(45) Australian Government, "Australia's international cyber engagement strategy," 2017, p.90. <https://www.internationalcybertech.gov.au/sites/default/files/2020-11/The%20Strategy.pdf>

(46) Roscini, *op.cit.*(38), pp.305, 308.

(47) 必ずしもサイバー行動に限定した議論ではないが、武力行使にその下限（de minimis use of force）が存在するか否かについて、Christian Henderson, *The use of force and international law*, Cambridge: Cambridge University Press, 2018, pp.65-68.

(48) 例えば、Harriet Moynihan, "The application of international law to state cyberattacks: sovereignty and non-intervention," *Chatham House Research Paper*, 2019, p.3. また、Olivier Corten, *The law against war: prohibition on the use of force in contemporary international law*, 2nd ed., Oxford: Hart, 2021, pp.104-105 も参照。

(49) Roscini, *op.cit.*(38), p.313.

(50) Robert Jennings and Arthur Watts, eds., *Oppenheim's international law*, 9th ed., vol.1, Oxford: Oxford University Press, 2008, pp.430, 432; 岩沢　前掲注(16), p.169.

導かれる。国際司法裁判所は、1947年のコルフ海峡事件判決(51)、1986年のニカラグア事件（本案）判決(52)において、主権侵害（後述）と並び不干渉原則について判示している。一般に、国内問題は国際法によって規律されない留保領域（domaine réservé(53)）に属する事項とされているが、「友好関係原則宣言」が「いかなる国又は国の集団も、理由のいかんを問わず、直接又は間接に、他国の国内又は対外の事項に干渉する権利を有しない。したがって、国の人格又はその政治的、経済的又は文化的要素に対する武力干渉及びその他いかなる介入若しくは威嚇の試みも、国際法に違反する」と掲げていることを挙げ、ニカラグア事件判決はこれに外交政策を加えている(54)。さらに国際司法裁判所は、2005年のコンゴ領域における軍事活動事件（本案）判決において、友好関係原則宣言及びニカラグア事件判決に言及し、「不干渉原則は国家に対し、国家の国内反対勢力を支持し、軍事力を伴い又は伴うことなく、直接的に又は間接的に干渉」することを禁じている旨、改めて判示した(55)。

『タリン・マニュアル2.0』は、不干渉原則がサイバー行動に適用されることを確認しつつ、「国家は、他国の国内又は対外事項に、サイバー手段による場合を含め、干渉してはならない」としている（規則66）(56)。

選挙介入ひいては偽情報の流布の対象が選挙であり、選挙が留保領域に属することについては、論者の間での見解はほぼ一致している（偽情報の流布がソーシャルメディア上で行われ、ソーシャルメディアの運営主体が国際法上は非国家主体であるプラットフォーマーであることから留保領域との線引きが困難とする見方はあるが、結局は選挙の問題に帰着するといえる(57)。）。一方、干渉の構成要件とされる強制（coercion）については、必ずしも一致をみていない。

選挙介入における偽情報の流布が顕在化するより前、2010年代半ばまでの議論では、サイバー行動による情報の流布について、プロパガンダ（政治的な目的のために態度及び行動を形成するためのコミュニケーション）と結び付けて検討されていた(58)。この文脈において強制は、国家の自由な意思決定過程に対して圧倒的に力が加えられる局面に限って生じるとされ(59)、プロパガンダによってコミュニケーションの受け手の選択肢が極めて限定的なものとなるような場合に、プロパガンダがニカラグア事件判決でいう干渉として不干渉原則に違反し得ることがあるとされていたところであった(60)。その後の議論においては、外国による選挙介入とされる行為について、ハッキングやスピアフィッシング(61)による秘密情報の窃取と暴露、ソー

---

(51) Corfu Channel case, Judgment of April 9th, 1949, *ICJ Reports* 1949, p.35.

(52) *ICJ Reports*, *op.cit.*(37), para.205.

(53) 1923年常設国際司法裁判所チュニス・モロッコ国籍事件判決。Nationality Decrees Issued in Tunis and Morocco (Advisory Opinion) [1923], *PCIJ Series* B No. 4, p.24.

(54) *ICJ Reports*, *op.cit.*(37), para.205; 岩沢　前掲注(16), pp.167-168.

(55) Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, *ICJ Reports* 2005, para.164.

(56) 中谷ほか　前掲注(29), p.71.

(57) Ido Kilovaty,“The international law of cyber intervention,”Tsagourias and Buchan, eds., *op.cit*.(38), pp.103-105.

(58) Sean Watts,“Low-intensity cyber operations and the principle of non-intervention,”Jens David Ohlin et al., eds., *Cyberwar: law and ethics for virtual conflicts,* Oxford: Oxford University Press, 2015, p.261.

(59) Katharina Ziolkowski,“Peacetime cyber espionage: new tendencies in public international law,”Ziolkowsiki, ed., *op.cit*.(35), p.433.

(60) Watts, *op.cit.*(58), pp.261-262.

(61) 特定の個人や組織を狙い、電子メールやSNS等のオンラインコミュニケーションを通じ、職業上の知己や家族を装って個人情報やアクセス権限を明かすよう確信させたり、正当又は必要と装ってマルウェアをインストールさせたり、標的となるシステムのセキュリティを破壊しようとする行為。Paul J. Springer, ed., *Encyclopedia of cyber warfare*, Santa Barbara: ABC-CLIO, 2017, pp.274-275.

シャルメディアを通じた偽情報の流布とが併せて論じられることがあり、偽情報の流布が単独で評価されているわけでは必ずしもない点に注意が必要であるが、選挙介入が先述の強制に相当する、ひいては干渉となり得るとする議論は、次のようなものである。選挙介入は反論の余地があるプロパガンダとは異なるものであって、介入がなければ生じ得なかった展開を招き得ることから強制性を持つと考える(62)。また、民主的プロセスの正統性への信用を毀損する行為が強制に相当するとの主張もある(63)。さらに、そもそも選挙介入は欺瞞的なものであるので、有権者が情報の是非を公正に判断できないような状況を作り出していることが強制に当たり得る、ともされる(64)。

これに対して、とりわけソーシャルメディアを通じた偽情報の流布については、選挙陣営の秘密情報の漏えいと異なり（ターゲットが限定されていないので）、強制性を有していない(65)、不干渉原則違反を構成しない旨の否定的な見解もある(66)。また、ターゲットが「進んで」行動をとるよう仕向けることは強制に当たらないことが示唆される(67)といった指摘もある。

上記のような国際法上の議論の争点は、結局のところ、選挙介入が強制に相当するかであったといえるが(68)、一貫性のある明快な基準はまだ存在しないとみられる(69)。オランダは、強制の明確な定義は“結晶化”していないとしている(70)。『タリン・マニュアル 2.0』は、「強制について国際法は定義を有していない」とする一方、「特定の国の選択の自由を奪うこと、又はその国の意思に反する結果を引き起こすことを企図した積極的な行為を広く指す」とする(71)。マニュアル作成に参加した専門家の間には、問題となる事項について国家からコントロールを奪えば強制といえるとの意見もあったという(72)。また、強制については、その効果が実際に損害を与えるかどうかではなく国の主権行使の自由意思を奪うために加えられる圧力として「強制的な行動」（coercive behaviour）の事実があれば足りるとする主張(73)や、そもそ

---

(62) Michael N. Schmitt, “Grey zones in the international law of cyberspace,” *Yale Journal of International Law online*, 42(2), 2017.10, p.8.『タリン・マニュアル 2.0』も、プロパガンダについて「相手国の選択の自由が奪われない限り、強制的な干渉になることはない」とする。中谷ほか　前掲注(29), p.72.

(63) Steven J. Barela, “Cross-border cyber ops to erode legitimacy: an act of coercion,” 2017.1.12. Just Security (the Reiss Center on Law and Security at New York University School of Law) website <https://www.justsecurity.org/36212/cross-border-cyber-ops-erode-legitimacy-act-coercion>; Steven Wheatley, “Foreign interference in elections under the non-intervention principle: we need to talk about “Coercion”,” *Duke Journal of Comparative & International Law*, vol.31, 2021, p.194.

(64) Michael N. Schmitt, ““Virtual” disenfranchisement: cyber election meddling in the grey zones of international law,” *Chicago Journal of International Law*, 19(1), Summer 2018, pp.50-51. <https://chicagounbound.uchicago.edu/cjil/vol19/iss1/2/>; Björnstjern Baade, “Fake news and international law,” *European Journal of International Law*, 29(4), 2018.11, p.1363. <https://doi.org/10.1093/ejil/chy071>

(65) Jens David Ohlin, “Did Russian cyber interference in the 2016 election violate international law?” *Texas Law Review*, 95(7), 2017.6, pp.1592-1593. <https://doi.org/10.31228/osf.io/3vuzf>

(66) Ido Kilovaty, “Doxfare: politically motivated leaks and the future of the norm on non-intervention in the era of weaponized information,” *Harvard National Security Journal*, vol.9, 2018.8, p.147. <https://ssrn.com/abstract=2945128>; Lahmann, *op.cit.*(25), pp.37-38.

(67) Hollis, *op.cit.*(34), p.41.

(68) Samuli Haataja, *Cyber attacks and international law on the use of force: the turn to information ethics*, New York: Routledge, 2019, p.173.

(69) Ido Kilovaty, “The elephant in the room: coercion,” *AJIL Unbound*, vol.113, 2019.3, p.90. <https://doi.org/10.1017/aju.2019.10>

(70) “Appendix,” *op.cit.*(44), p.3.

(71) 中谷ほか　前掲注(29), p.72. そもそも、サイバー行動に限らず、強制については一般的な判断基準が存在していないともいう。Philip Kunig, “Intervention, prohibition of,” Rüdiger Wolfrum, ed., *Max Planck encyclopedia of public international law*, vol.6, Oxford: Oxford University Press, 2012, p.290.

(72) Schmitt, ed., *op.cit.*(7), p.318.

(73) Moynihan, *op.cit.*(48), p.33. なお、オーストラリアは、「禁止される干渉は（主権の本質に固有の問題をコントロールしたり決定したりする能力を他国から事実上奪うという意味において）強制的な手段（coercive means）による

も強制の概念の拡張が必要かもしれないとの指摘もある(74)。

(3) 主権侵害の禁止（prohibition of violation of sovereignty）

不干渉義務違反については、干渉の構成要件である強制をめぐって、強制と判断されるに至るまでの何らかの閾値が存在し選挙介入や偽情報の流布がその閾値に達することは稀であると考えられることに対して(75)、より広く、主権侵害とサイバー行動の関係を論じるものがある。『タリン・マニュアル 2.0』は、「専門家集団は、あるサイバー行動が本規則［規則 66］で禁止される干渉を構成しなくても、それが非強制的な主権侵害となりうることに留意している」と述べる(76)。

一般に、国家は、その主権の属性として、政治的、経済的、社会的、文化的体制、外交政策のような事項について自ら決定する権利を有し、これらの事項への介入は主権の侵害となり得る(77)。しかしながらサイバー行動と主権侵害の関係に関する各国の見解は必ずしも一致していない。英国は、法務総裁が 2018 年に行った演説で、不干渉原則のほかにはサイバー行動を禁止するルールは存在しないとし(78)、主権は国際法の原則であるがそれ自体が国際義務違反を規律する一次規則ではないという旨の立場にある。一方、フランス(79)やドイツ(80)、カナダ(81)、オランダ(82)等は、サイバー行動が主権侵害となり得るとの立場を取る。こうした見解の違いについて、サイバー行動が主権侵害に相当するかについて各国が武力行使と同様に烈度を基準に考えているためであるとの指摘がある(83)。

『タリン・マニュアル 2.0』は、対内的主権及び対外的主権について確認するとともに（規則 2 及び 3）(84)、「国家は、サイバー行動による主権侵害を行ってはならない」としてサイバー行動による主権侵害を禁止する（規則 4）(85)。その上で、主権侵害の禁止の観点から選挙にも言及するが、例示しているのは、本質的な政府の機能の行使に必要なデータやサービスを妨げるサイ

介入」としている。Australian Government, *Australia's international cyber engagement strategy: 2019 International law supplement*, p.5. <https://www.internationalcybertech.gov.au/sites/default/files/2020-11/2019%20Legal%20Supplment_0.PDF>

(74) Henning Lahmann,“Information operations and the question of illegitimate interference under international law,”*Israel Law Review*, 53(2), 2020.7, p.216.

(75) Michael N. Schmitt and Liis Vihul,“Sovereignty in cyberspace: lex lata vel non?”*AJIL Unbound*, vol.111, 2017.8, pp.213-214. <https://doi.org/10.1017/aju.2017.55>; Kilovaty, *op.cit.*(66), pp.168-169.

(76) 中谷ほか　前掲注(29), p.73.

(77) Jennings and Watts, eds., *op.cit.*(50), pp.430-431.

(78) Jeremy Wright,“Cyber and international law in the 21st century,”2018.5.23. GOV.UK website <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century> 米国が英国に近い立場を取っている旨の見解としては、Paul C. Ney,“DOD General Counsel remarks at U.S. Cyber Command legal conference,”2020.3.2. U.S. Department of Defense website <https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference>

(79) Ministère des Armées de la République Française, *Droit international appliqué aux opérations dans le cyberespace*, 2018, pp.6-7. <https://www.defense.gouv.fr/sites/default/files/ministere-armees/Droit%20international%20appliqu%C3%A9%20aux%20op%C3%A9rations%20dans%20le%20cyberespace.pdf>

(80) Federal Government, *op.cit.*(43), p.3.

(81) Government of Canada,“International law applicable to cyberspace,”2022.4.22, paras.10-21. <https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng#a3>

(82) “Appendix,”*op.cit.*(44)

(83) Fidler, *op.cit.*(8), p.124. 主権の侵害についても閾値が存在するとすれば不干渉原則違反に近似したものとなるとの指摘もある。Moynihan, *op.cit.*(48), p.48.

(84) 中谷ほか　前掲注(29), pp.6-7.

(85) 同上, pp.7-8.

バー行動の一つとしての選挙に関するデータの改変・削除であり(86)、選挙介入や偽情報の流布ではなかった。

学説上は、選挙介入とされる行為の中でも、他国の領域に所在する情報システム・ネットワークへの侵入が主権侵害を構成するとされる(87)。また、公然となされるプロパガンダではなく有権者の意思を操作したり候補者の印象をゆがめたりすることが主権侵害となり得るとの主張もある(88)。

いずれにせよ、選挙介入と主権侵害との関係については、サイバー活動と主権侵害との関係も踏まえた更なる議論が必要であろう。

(4) 自決権（right of self-determination）

選挙介入に関する国際法上のより新しい議論は、自決権の観点からのものである。市民的及び政治的権利に関する国際規約（自由権規約）(89)第 1 条 1 項は「すべての人民は、自決の権利を有する。この権利に基づき、すべての人民は、その政治的地位を自由に決定」するとし、同第 1 条 3 項は「この規約の締約国…（中略）…は、国際連合憲章の規定に従い、自決の権利が実現されることを促進し及び自決の権利を尊重する」とする。さらに同第 25 条 (a) は、すべての市民は「直接に、又は自由に選んだ代表者を通じて、政治に参与する」権利と機会を有する旨を定める。

自決には、植民地人民が独立を達成するという外的自決と、内的自決（人民が代表性のある民主政府を求める権利(90)）の意味があるが(91)、議論の基礎となるのは内的自決である。内的自決は自由権（表現の自由、集会の自由、参政権等）が保障されて初めて可能となる(92)。

選挙介入が自決権を侵害し得るとの考え方の前提は、政治への参与と熟慮のプロセスを意義のあるものとするためには、政治的課題に関して事実の面で正確な情報が提供されることが必要であり(93)、情報操作は市民の集合的な権利（としての自決権）を侵害し得るというものである(94)。その上で、国家主権と人民が政体を選ぶ権利とが分かち難く結び付いており、不干渉原則によって自決権も保護されるとし、情報操作が一定の烈度にあって、人民の政治的意思の形成を妨げれば主権侵害を構成し得ると考える説がある(95)。

もう一つは、自国の選挙民になりすまして政治的議論に参加することが情報の受け手を欺き、

---

(86) 同上, p.8.
(87) Kilovaty, *op.cit.*(66), p.169.
(88) Schmitt, ed., *op.cit.*(7), p.45; Moynihan, *op.cit.*(48), pp.42-43.
(89) 2023 年 2 月 21 日現在の締約国は 173 か国であるが、例えば、中華人民共和国やキューバは署名したが批准していない。ブータン、ブルネイ、マレーシア、ミャンマー、サウジアラビア、アラブ首長国連邦、シンガポール等は署名も加入もしていない。“Status of ratification: International Covenant on Civil and Political Rights.”United Nations Office of the High Commissioner for Human Rights (OHCHR) website <https://indicators.ohchr.org/>
(90) 浅田編著　前掲注(15), p.93.
(91) 岩沢　前掲注(16), p.139. 外的自決が達成された後も、自決権は残存し人民に帰属し、人民は自決権を政府に移行させ、政府は外部の主体との関係において権利を行使する、と説明される。Daniel Thürer and Thomas Burri, “Self-determination,”Wolfrum, ed., *op.cit.*(15), p.119; Samantha Besson,“Sovereignty,”*ibid*., p.375.
(92) 岩沢　前掲注(16), p.391.
(93) Bayer et al., *op.cit.*(3), pp.61-62.
(94) Lahmann, *op.cit.*(74), p.204.
(95) Nicholas Tsagourias,“Electoral cyber interference, self-determination and the principle of non-intervention in cyberspace,” Dennis Broeders and Bibi van den Berg, eds., *Governing cyberspace: behavior, power, and diplomacy*, London: Rowman & Littlefield, 2020, pp.51-52.

人民の自決権そのものを侵害すると考えるものである[96]。自決権は、人民に対して民主的な政体をとる権利を付与するものでは必ずしもないが、人民の意思を代表する政府を保証する制度は、民主国家にあっては選挙であり、有権者が投票行動をとる際の熟慮をゆがめるような外国による情報操作から選挙は保護されるべきであるという[97]。この説は、自由権規約の当該規定が締約国でない国をも拘束し得るか（慣習国際法の内容を反映しているか）という問題を含むようにも見え、現行法（lex lata）ではなくあるべき法（lex ferenda）について論じているようにも思われるが、少なくとも選挙介入を行う国が自由権規約の締約国である場合には規約第1条3項の自決権の尊重義務に違反するといえる[98]。また、自由権規約を始め人権条約は締約国が自国の領域内で自国民に人権を保障することを約束し合うもので[99]、自国民の人権保障はその国家によって最もよく実現される[100]とすれば、他国に対する選挙介入は、介入を受ける国における自決権の保障を妨げる行為と考えることもできよう。

おわりに

国家によるサイバー行動としてなされる選挙介入、またその際に行われる偽情報の流布については、国際法が適用されるとの前提の下で、学説上は、慣習国際法の諸原則つまり不干渉原則、主権侵害の禁止、更に内的自決から評価される。

選挙介入は単独で武力行使禁止原則に直接抵触しているとは考えられていない。干渉の構成要件である強制に相当するかについては、選挙介入が有する欺瞞的な性質が強制性を有すると考えるか、従来の強制の概念を拡張することによって規律すべきと考える等、議論が分かれているところである。主権に関連した議論は必ずしも十分ではないようであるが、関連して自決権との関係が議論されており、選挙制度による民主主義制度を採用する国においては選挙介入や偽情報の流布は、その内的自決を妨げる行為と考えることもできよう。

現実の選挙介入や偽情報の流布については、各国がケースごとに是非を判断するのだとしても、慣習国際法の成立に当たって必要とされる国の国家実行及び法的信念については、いまだ必ずしも明確ではない。

今後は、更に新しく登場するであろう情報技術を利用したサイバー行動の不確実性にも対応できる国際法上の枠組みについての議論も求められよう。

（ひやま　ちふゆ）

⑼⑹ Jens David Ohlin, "Election interference: the real harm and the only solution," *Cornell Law School research paper*, No.18-50, 2018, pp.10, 12-13; *idem*, *op.cit.*⑹⑸, pp.1580-1581.

⑼⑺ Jens David Ohlin, *Election interference: international law and the future of democracy*, Cambridge: Cambridge University Press, 2020, pp.101-102.

⑼⑻ *ibid.*, pp.114-115.

⑼⑼ 岩沢　前掲注⑴⑹, p.100.

⑽⑽ 酒井ほか　前掲注⑵⑶, p.590.