国立国会図書館 調査及び立法考査局

Research and Legislative Reference Bureau
National Diet Library

論題 Title	第 2 章　デジタル影響工作をめぐる動向と対応
他言語論題 Title in other language	Chapter 2 Digital Influence Operations: Recent Trends and Responses in Japan
著者 / 所属 Author(s)	久古聡美（KYUKO Satomi）／国立国会図書館調査及び立法考査局外交防衛課
書名 Title of Book	デジタル時代の技術と社会　科学技術に関する調査プロジェクト報告書（Technology and Its Social Implementation in the Digital Era）
シリーズ Series	調査資料 2023-5（Research Materials 2023-5）
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
刊行日 Issue Date	2024-3-26
ページ Pages	29-48
ISBN	978-4-87582-923-2
本文の言語 Language	日本語（Japanese）
摘要 Abstract	デジタル影響工作の概念や主要な実施主体の動向を整理し、ディスインフォメーションとナラティブを切り口としてデジタル影響工作の展開を概観した後、民主主義国家における主な対応策を示す。

第2章　デジタル影響工作をめぐる動向と対応

国立国会図書館　調査及び立法考査局
外交防衛課　久古　聡美

目　　次

【要　旨】
インターネット及びデジタル技術の発展を背景に、近年、国際テロ組織及びロシアや中国などの国家によるデジタル影響工作の事例が相次いでいる。近年利用が浸透したソーシャルメディアにおける情報伝達の双方向性等の特性や仕組みは、情報環境を複雑化させ、影響工作の展開に都合の良い環境をもたらしている。デジタル影響工作においては、虚偽の情報を中心とするディスインフォメーションや意見・価値判断に基づくナラティブの流布・拡散などが行われる。これまで、民主主義国家における対応策として、情報の遮断、情報の真偽の検証、プラットフォーム企業による対応の促進等、戦略的な情報発信、実施者に対する懲罰、国民の情報リテラシーの向上などが行われてきた。デジタル影響工作は今後も巧妙化しつつ展開されていくと予想され、表現の自由等の民主的価値を守りつつ、透明性のある形で対応していくことが求められる。

はじめに

近年、インターネット及びデジタル技術の発展等を背景として、国外からソーシャルメディア等を用いた影響工作（influence operation）が行われる事例が相次いでいる。国家や非国家主体が標的とする人々に対して、ソーシャルメディアやインターネット上で、虚偽の情報や意見・価値判断が織り交ざった情報を流通させる。民主主義国家においては、こうした「デジタル影響工作」によって、人々の認知や世論が誘導され、社会の混乱や政治的分断の助長がもたらされるリスクが広く認識されるようになり、対応の在り方が議論となっている。

本稿では、まず、デジタル影響工作の概念、経緯及び主要な実施主体の動向を整理する。次に、デジタル影響工作の展開を、ディスインフォメーション（Ⅱ2で後述）とナラティブ（Ⅱ3で後述）という2つの種類のコンテンツを切り口として概観する。最後に、民主主義国家におけるデジタル影響工作への主な対応策を行為の種類によって類型化し、それぞれに関する基本的な議論にも触れる。

Ⅰ　デジタル影響工作の広がり

1　影響工作及び隣接する概念

(1) デジタル影響工作とは

国家等の主体が人々の認知や世論を誘導するための活動を行うことは、特段新しい現象ではない。いわゆる「フェイクニュース」[(1)]や虚偽の情報の流布は、その1つの形である[(2)]。また、一部の事実を隠す、偏った意見・価値判断に基づく情報を流布する、悪意をもって機密文書や通信文を一般に暴露するといった形がとられることもある[(3)]。こうした活動は、影響工作のほか、心理作戦、情報作戦、政治戦、世論操作などと様々に呼ばれてきた[(4)]。

＊本稿におけるインターネット情報の最終アクセス日は、令和5（2023）年11月20日である。

(1)　フェイクニュースとは、誤った情報を含んだニュースなどをいうが、この語の曖昧さや単に好ましくない報道を排除するために使用されてきた経緯があることなどから、最近では使用が控えられることもある。例えば、次を参照。European Commission, *A Multi-dimensional Approach to Disinformation: Report of the Independent High Level Group on Fake News and Online Disinformation*, 2018, pp.5, 10. <https://data.europa.eu/doi/10.2759/739290>

(2)　齋藤孝道「デジタル影響工作のプレイブック」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.53.

(3)　一田和樹「デジタル影響工作とはなにか」同上, p.22; James J. F. Forest, *Digital Influence Warfare in the Age of Social Media*, Santa Barbara: Praeger Security International, 2021, p.27.

影響工作について、2009年、米国のランド研究所の研究者らは、指導者個人、特定の集団などから大衆までのいずれを標的とするかを問わず、「標的とされた人々（target audience）に影響を与える取組」のことであり、主に、非物理的（non-kinetic）で、コミュニケーション関係の、情報に関する活動から成ると説明した[5]。Meta社（旧Facebook社）は、2021年、影響工作を「戦略的目標のために、公的な議論を操作又は腐敗させるための組織的な取組」と定義している[6]。様々な影響工作の定義の間には、意図・手段の性質（欺まんなどの悪意が伴うものに限定するか等）や標的（国外に限定するか）などの点で相違もあるが、実施主体の目標のために標的に影響を与えるための活動とする点はおおむね共通している[7]。

本稿では、「影響工作」を、意図・手段の性質や標的を限定せずに、実施主体（国家や非国家主体）が自らの目標に望ましい状況を作り出すため、国内外の標的に対して影響を与えるために行う活動を指すものとして用いる。また、影響工作のうち、主にソーシャルメディアやインターネット上で行われるものを「デジタル影響工作」と呼ぶこととする。影響工作の形態としては、虚偽の情報を中心とするディスインフォメーションと意見・価値判断に基づくナラティブの流布・拡散に焦点を当てる（よって、機密文書等の暴露については特に扱わない。）。

(2) 隣接する概念との関係

影響工作と重複又は隣接する概念は多くある。例えば、情報作戦（information operation）、情報戦（information warfare）、プロパガンダ（propaganda）、ディスインフォメーション・キャンペーン（disinformation campaign）、広報外交（public diplomacy）、戦略的コミュニケーション（strategic communication）等が挙げられる[8]。

各概念が指す内容は、定義の仕方によっても異なるが、基本的にいずれも、自らの利益にとって望ましい外部環境を構築することを目的とし、「結果として他国の世論、つまり「人間の認知」領域に影響を与え得る」活動である[9]。一方、実施主体の意図・手段に悪意や不正があるか又はそれらが無いかのどちらかに限定するものと、限定しないものとが混在している[10]。例えば、一般的な解釈では、ディスインフォメーション・キャンペーン[11]には欺まんなどの悪意が伴う

---

(4)　*ibid*., p.2; Alicia Wanless and James Pamment, "How Do You Define a Problem like Influence?" *Journal of Information Warfare*, vol.18 no.3, Winter 2019, pp.1-14.

(5)　Eric V. Larson et al., *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities*, Santa Monica: RAND Corporation, 2009, pp.2-3. <https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG654.pdf> さらに、米国を実施主体とした影響工作の定義として、「米国の利益と目標を促進するような態度、行動、意思決定を国外の標的とする人々に促すために、平時、危機時、紛争時及び紛争後において、国家の外交、情報、軍事、経済、その他の能力を組織的、統合的、同期的に用いること」としている。*ibid*., p.2.

(6)　Nathaniel Gleicher et al., "Threat Report: The State of Influence Operations 2017-2020," May 2021, p.11. Meta Website <https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf>

(7)　Wanless and Pamment, *op.cit*.(4), pp.7-8.

(8)　*ibid*., pp.1-2; 桒原響子「外交と偽情報」小泉悠ほか『偽情報戦争―あなたの頭の中で起こる戦い―』ウェッジ, 2023, pp.23-28; 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」一田ほか　前掲注(2), p.204.

(9)　桒原　同上, p.27. 人間の認知に関わる領域のことを「認知領域」と呼び、陸・海・空、宇宙、サイバーなどに次ぐ、新たな戦争の領域とする見方がある。François du Cluzel, "Cognitive Warfare," November 2020, p.25. Innovation Hub Website <https://www.innovationhub-act.org/sites/default/files/2021-01/20210122_CW%20Final.pdf> なお、認知とは、事象について知識を得ること又はその過程であり、知覚だけでなく、推理・判断・記憶などの機能を含み、外界の情報を能動的に収集し処理する過程をいう。松村明・三省堂編修所編『大辞林　第4版』三省堂, 2019, p.2097.

(10)　桒原　同上

(11)　ディスインフォメーション・キャンペーンとは、「経済的・政治的目的を達成するため、意図的に世論を欺くために作り出されたディスインフォメーション（偽情報）を拡散し、公共に害を与える活動」を指す。同上, p.24.

が、透明性や正当性が求められる戦略的コミュニケーション[12]にはそれが伴わない[13]。影響工作の意図・手段の性質をⅠ1（1）のとおりに広く捉える場合には、隣接する各概念を影響工作の中に含むものとして解釈することも可能である[14]。

2　デジタル影響工作をめぐる経緯

(1) 情報通信技術の発展と影響工作―前史―

人々の認知や世論を誘導するために情報を流通させる活動を、プロパガンダ（宣伝活動）[15]の歴史としてたどると、その語源はカトリック教会の布教活動にあるとされるが[16]、影響工作が本格的に行われるようになったのは20世紀に入ってからである[17]。国民を巻き込む総力戦となった第1次世界大戦では、参戦国の間で、自国の士気を高めたり敵国の兵士の士気をくじいたりするために、組織的かつ大規模にプロパガンダが行われた。その際、政府によって公式に承認された情報を広めるため、媒体として、新聞・雑誌、ビラ（紙）、ポスター、映画などが用いられた。第2次世界大戦では、これらに加え、ラジオも用いられるようになった。1950年代以降になるとテレビが次第に普及し、多くの人々に対して大量の情報伝達を可能とするラジオやテレビは、冷戦期を通じて、東西陣営のプロパガンダの手段として活用された[18]。

このように、影響工作で用いられる媒体は、情報通信技術の発展とともに変化してきた。技術発展によって伝達される情報の量、速度、範囲等が向上するにつれ、これらのメディアが世論を導く力は大きくなり、影響工作が及ぼし得る効果の程度も大きくなっていった[19]。

(2) ソーシャルメディアとデジタル影響工作

1990年代以降のインターネット及びデジタル技術の急激な発展、また、特に2010年頃からのソーシャルメディアの利用の浸透を背景に、近年、デジタル影響工作が活発化している。ソーシャルメディアとは、ユーザー生成コンテンツの作成・交換を可能にするインターネットベースのアプリケーション群を指し、代表的な例として、Wikipedia、Facebook、YouTube、X（旧Twitter）、Instagram等が挙げられる[20]。新聞、ラジオ、テレビ等の伝統的なメディアでは、発信者から受信者への一方向の情報伝達が行われるのに対し、ソーシャルメディアでは、ユーザーがコンテンツを生成可能で、情報伝達は双方向となる。この変化は、Ⅱ1で後述するように、

⑿　戦略的コミュニケーションとは、「自らの政策目標の達成の助力となるように、言葉、行動（あるいは非行動）、イメージやシンボルを用い、相手の行動や態度を変更させることを目的とした外交・安全保障政策の実施」を指す。青井千由紀『戦略的コミュニケーションと国際政治―新しい安全保障政策の論理―』日本経済新聞出版, 2022, p.23.

⒀　棗原　前掲注⑻, p.27; 同上, pp.44-45.

⒁　Larson et al., *op.cit.*⑸, pp.3-5; 棗原響子「「人間の認知」をめぐる介入戦略―複雑化する領域と手段、戦略的コミュニケーション強化のための一考察―」『Roles Report』12号, 2021.7, pp.6-9. <https://roles.rcast.u-tokyo.ac.jp/uploads/publication/file/19/publication.pdf>

⒂　プロパガンダとは、「不特定多数の大衆を一定の方向に導き、行動を起こさせるため、社会心理的な手法で特定の考え方や価値観を植え付ける組織的な活動」を指す。棗原　前掲注⑻, p.24.

⒃　Lawrence Freedman, *Strategy: A History*, New York: Oxford University Press, 2013, p.339; David Welch, "A Brief History of Propaganda," Timothy Clack and Robert Johnson, eds., *The World Information War: Western Resilience, Campaigning and Cognitive Effects*, Abingdon, Oxon; New York: Routledge, 2021, p.23.

⒄　Welch, *ibid*., p.21; 中西寛「あなたと情報」『外交』80号, 2023.7・8, pp.7-8.

⒅　*ibid*., pp.24-29; Forest, *op.cit.*⑶, pp.34-36.

⒆　Welch, *ibid.*, p.29; 中西　前掲注⒄

⒇　Andreas M. Kaplan and Michael Haenlein, "Users of the World, Unite! The Challenges and Opportunities of Social Media," *Business Horizons*, vol.53 iss.1, 2010.1-2, p.61. <https://doi.org/10.1016/j.bushor.2009.09.003>

情報環境を複雑化させ、影響工作の展開に都合の良い環境をもたらしている。

プリンストン大学の紛争実証研究プロジェクトの調査によれば、2011年から2022年にかけて62か国を対象に調査した結果、ソーシャルメディアを含むメディアチャネルを用いた国家主導の影響力行使（influence efforts）として特定された事例の数は、対外の事例が93件、対国内の事例が34件であった[21]。また、オックスフォード大学のインターネット研究所の調査によれば、2020年において、ソーシャルメディアを用いて政治に関するプロパガンダやディスインフォメーションを拡散したことが確認された国は、ロシア、中国、イラン、サウジアラビア、米国、英国を含む81か国に及んだ[22]。現在では、影響工作の「主戦場」は、伝統的なメディアからソーシャルメディアへと移りつつあるとされる[23]。

3　主要な実施主体の動向

(1) 国際テロ組織

中東などの世界各地を拠点に活動する国際テロ組織がテロリスト同士や世界中の人々とのコミュニケーション手段としてインターネットを利用していることは、2004年頃から広く懸念されるようになった[24]。マスメディアに頼ることなく、組織が希望するメッセージを人々に直接伝えることができるインターネットは、国際テロ組織にとって強力なツールとなる。組織の要求内容やプロパガンダを広めるほか、資金を集め、人材を勧誘するための媒体として、ウェブサイト、チャットルーム、オンライン掲示板等が用いられた。1998年に12サイトであったテロ組織のウェブサイトの数は、2006年に4,800サイト以上に急増したとされる[25]。

国際テロ組織は、標的の政策や行動に影響を及ぼすため、次第に恐怖やパニックを引き起こす手法を多用するようになった。2015年1月、IS（イスラム国）は、同組織に対する空爆作戦中にシリアで墜落したヨルダン軍の戦闘機の飛行士1名を拘束し、残虐な方法で殺害する映像を複数のウェブサイトやソーシャルメディア上に投稿した。こうした映像の流布・拡散は、復しゅうの物語を宣伝することでISの戦闘員を奮い立たせるとともに、海外での外国人戦闘員の勧誘を促すといった目的にも資するものであったとされる[26]。

---

[21] Diego A. Martin et al., “Online Political Influence Efforts Dataset, Version 4.0,” March 24, 2023, p.2. Empirical Studies of Conflict Project Website <https://esoc.princeton.edu/publications/trends-online-influence-efforts> この調査には、1,200点以上の報道記事と630点の研究報告等に基づいて影響力行使の事例を特定し、その進捗状況の追跡等を行った結果がまとめられている。ソーシャルメディア以外に用いられたメディアチャネルとしては、報道機関のニュースサイト、偽のウェブサイトなどがある。

[22] Samantha Bradshaw et al., “Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation,” 2021.1, pp.i, 1-3. Oxford Internet Institute Website <https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/02/CyberTroop-Report20-Draft9.pdf> この調査には、政府や政党関係のアクターでソーシャルメディアを用いた世論操作を任務とする「サイバー部隊」（cyber troop）の活動について、①ニュース記事の体系的な内容分析、及び、②政府やシンクタンク等による報告書などの2次文献のレビューを行い、それらに基づいてサイバー部隊の活動に関する国別の事例研究を行い、専門家によるレビュー等を受けた結果がまとめられている。①②で用いられた記事・文献は合計で1,300点以上となっている。なお、本稿の本文中に例示した6か国は、この調査でサイバー部隊の能力が高い国として評価されている17か国のうち、主要な国や日本との関係が深い国である。

[23] Forest, *op.cit.*(3), p.26; 川口　前掲注(8), p.202.

[24] Jacob T. Rob and Jacob N. Shapiro, “A Brief History of Online Influence Operations,” October 28, 2021. Lawfare Website <https://www.lawfaremedia.org/article/brief-history-online-influence-operations>

[25] “Militants Weave Web of Terror,” *BBC News*, 14 July 2004. <http://news.bbc.co.uk/2/hi/technology/3889841.stm>; David Talbot, “Terrorists Increasingly Turn to the Internet,” February 21, 2006. MIT Technology Review Website <https://www.technologyreview.com/2006/02/21/101062/terrorists-increasingly-turn-to-the-internet/>

[26] Forest, *op.cit.*(3), pp.62-63.

(2) ロシア

ロシアはソビエト連邦時代から積極的に影響工作を展開し、近年もデジタル影響工作を活発に実施している。プリンストン大学の紛争実証研究プロジェクトの調査によれば、国家主導の対外的な影響力行使の事例（2011～2022年）の約61%（93件中の57件）をロシアが占めている[27]。

ウラジーミル・プーチン（Vladimir Putin）大統領の下で2000年9月に制定された「情報セキュリティドクトリン」には、情報領域を紛争の場と捉え、敵対勢力によるプロパガンダ、情報・心理作戦に積極的に対抗するための方法と手段を改善していく方針を含め、ロシアのデジタル影響工作のアプローチが示されていた[28]。2013年2月のワレリー・ゲラシモフ（Valery Gerasimov）ロシア軍参謀総長による論文「先見の明における科学の価値」は、政治的・戦略的目標を達成するに当たって非軍事的手段の役割が大きくなり、その有効性は多くの場合に武器の力を超えていると論じている。非軍事的手段の中には、「政治的な反勢力の形成」や「反勢力の行動」といった影響工作に当たる事柄も挙げられた[29]。非軍事的手段を重視する同論文の内容は、その後、「国家安全保障戦略」（2021年7月改定）等の公式の戦略文書に反映されている[30]。

ロシアが2016年の米国大統領選挙に影響を及ぼすための活動をしたことは米国政府の調査等で明らかにされた。サンクトペテルブルクを本拠とするIRA（Internet Research Agency）などの工作組織とその従業員は、米国の活動家が米国の政治・社会の問題を取り上げているように偽るソーシャルメディアのアカウントやグループページを運用し、選挙に際して、これらを足掛かりに、ドナルド・トランプ（Donald Trump）候補を支持しヒラリー・クリントン（Hillary Clinton）候補を中傷する内容の投稿を繰り返した[31]。オックスフォード大学のインターネット研究所の報告によれば、2015年から2017年にかけて、3000万人を超える米国内のユーザーが、IRAのFacebook及びInstagramの投稿を友人や家族と共有したり、「いいね」をしたり、評価したり、コメントをしたりした[32]。ロシアは、2016年の英国のEU離脱をめぐる国民投票、2017年のフランス大統領選挙、2022年の米国中間選挙にも介入していたことが指摘されている[33]。選挙等への介入を行うロシアの意図は、ロシアの政策目標の達成にとって障害となる国において、人々の行動に影響を及ぼすのみならず、人々の間に混乱、両極化、敵意、不信を引き起こすことにあるとみられている[34]。

また、ロシアは2014年、クリミアでロシア軍が活動しているという現地の情報に対して、

---

(27) Martin et al., *op.cit.*(21), p.2.

(28) "Information Security Doctrine of the Russian Federation, Approved by President of the Russian Federation Vladimir Putin on September 9, 2000." International Telecommunication Union Website <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf>; Forest, *op.cit.*(3), p.52. なお、近年、ロシアでは、安全保障会議が策定する「国家安全保障戦略」が最上位の戦略文書として置かれ、それを受けて分野別の戦略文書が策定されており、「情報セキュリティドクトリン」もその1つである。

(29) Valery Gerasimov, Robert Coalson, translator, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations," *Military Review*, January-February 2016, pp.23-29. <https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf>; 佐々木孝博「ロシアによるデジタル影響工作」一田ほか　前掲注(2), pp.175-178.

(30) 同上, pp.167-175.

(31) Robert S. Mueller, III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election,* Volume I of II, March 2019, pp.14-15. U.S. Department of Justice Website <https://www.justice.gov/archives/sco/file/1373816/download>

(32) Philip N. Howard et al., "The IRA, Social Media and Political Polarization in the United States, 2012-2018," 2018.2, pp.3, 7. Oxford Internet Institute Website <https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2018/12/The-IRA-Social-Media-and-Political-Polarization.pdf>

ロシア軍と関係ない組織であると偽る投稿を繰り返すといったディスインフォメーション・キャンペーンを繰り広げ、混乱の間にウクライナからクリミアを併合した[35]。2022年2月のウクライナ侵攻に際しても、国営メディアやソーシャルメディアを利用した影響工作を展開した。ロシア政府が侵攻前に「軍事演習終了後に軍隊をウクライナ国境付近から撤退させている」とする事実に反する発表をしたこと、「ロシアはナチス・インターナショナルと戦っている」といった侵攻を正当化する内容の主張を行ったことはその例である[36]。

(3) 中国

中国も、ソーシャルメディア等を用いたデジタル影響工作を様々に実施している。プリンストン大学の紛争実証研究プロジェクトの調査では、ロシアより少ないものの、国家主導の対外的な影響力行使の事例（2011～2022年）の約8.6%（93件中の8件）を中国が占めている[37]。

2003年12月、中国共産党は「人民解放軍政治工作条例」において、影響工作に関わる「世論戦」と「心理戦」、及び、「法律戦」から成る「三戦」を人民解放軍が実施していくことを正式に規定した[38]。また、中国の軍関係者らの間では、戦争の領域には、物理領域及び情報領域と並んで認知領域があり、認知領域において優勢になることが他の領域で優勢になる上でも重要になるとする考えが繰り返し論じられている[39]。2014年には、相手国の世論に攻勢をかけて認知を操作したり、メディア等を通じた宣伝によって歴史的記憶に関するナラティブを歪曲したりする手法などを通じて、未来の戦争で「制脳権」を奪取するといった考えが示された[40]。

---

(33) House of Commons, Digital, Culture, Media and Sport Committee, "Disinformation and 'Fake News': Interim Report, Fifth Report of Session 2017-19," HC 363, July 29, 2018, pp.43-52. <https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf>; Centre d'analyse, de prévision et de stratégie et L'Institut de recherche stratégique de l'École militaire, "Les manipulations de l'information: Un défi pour nos démocraties," 2018.8, pp.108-119. Ministère de l'Europe et des Affaires étrangères Website <https://www.diplomatie.gouv.fr/IMG/pdf/les_manipulations_de_l_information_2__cle04b2b6.pdf>; "US Warns about Foreign Efforts to Sway American Voters," October 4, 2022. Associated Press Website <https://apnews.com/article/2022-midterm-elections-russia-ukraine-campaigns-presidential-ea913f2b3b818651a9db1327adaa330a>; 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, pp.85-89; 市原麻衣子「中ロの選挙介入に揺れる米国」『外交』80号, 2023.7・8, pp.46-51;「米中間選挙、介入認める　ロシア大統領に近い実業家プリゴジン氏」『時事通信』2022.11.8.

(34) Forest, *op.cit.*(3), p.56; David Patrikarakos, *War in 140 Characters: How Social Media Is Reshaping Conflict in the Twenty-first Century*, New York: Basic Books, 2017, p.150.

(35) Jill Dougherty, "Everyone Lies: The Ukraine Conflict and Russia's Media Transformation," *Discussion Paper Series*, D-88, July 2014, pp.3-4. Harvard Kennedy School Website <https://shorensteincenter.org/wp-content/uploads/2014/07/d88-dougherty.pdf>; Keir Giles, "Russia's Hybrid Warfare: A Success in Propaganda," *Security Policy Working Paper*, no.1/2015, p.3. Bundesakademie für Sicherheitspolitik Website <https://www.baks.bund.de/sites/baks010/files/arbeitspapier_sicherheitspolitik_1_2015_eng.pdf>

(36) "Ukraine Crisis: Russian Claim of Troop Withdrawal False, Says US," *BBC News*, 17 February 2022. <https://www.bbc.com/news/world-europe-60407010>; "Disinfo: President Zelenskyy Has Left Kyiv," February 28, 2022. EUvsDisinfo Website <https://euvsdisinfo.eu/report/president-zelenskyy-has-left-kyiv>; "Disinfo: Russia Is Fighting the Nazi International," February 12, 2023. *ibid*. <https://euvsdisinfo.eu/report/russia-is-fighting-the-nazi-international>

(37) Martin et al., *op.cit.*(21), pp.40-76. 中国よりも件数の多い国には、ロシアのほか、イランがある（93件中の13件）。

(38) Forest, *op.cit.*(3), pp.48-49; 大治朋子『人を動かすナラティブ―なぜ、あの「語り」に惑わされるのか―』毎日新聞出版, 2023, pp.246-247.

(39) 飯田将史「中国が目指す認知領域における戦いの姿」『NIDSコメンタリー』177号, 2021.6.29, pp.1-4. <http://www.nids.mod.go.jp/publication/commentary/pdf/commentary177.pdf>

(40) 「制脳権」の概念は、2014年刊行の国防科技大学人文社会科学学院院長の曾華鋒らによる書籍（『制脳権―全球時代的戦争法則與国家安全戦略―』）の中で提唱されたとされる。「制脳権」を有する状態とは、認知空間において敵の戦力よりも優勢を確保し、敵から大きな妨害を受けることなく諸作戦を実施できる状態を指すものと考えられる。土屋貴裕「ニューロ・セキュリティ―「制脳権」と「マインド・ウォーズ」―」『Keio SFC Journal』15巻2号, 2015, pp.12-31. <https://doi.org/10.14991/003.00150002-0012>

中国は、2019年末からの新型コロナウイルス感染症の拡大に伴って積極的に影響工作を展開した。英語版国営メディアのFacebookページや外交官及び大使館のTwitterアカウントを用いて、新型コロナウイルス感染症に関する中国共産党にとって好ましいシナリオを増幅させる公然の活動が行われた[41]。2020年3月、中国外交部の趙立堅報道官がTwitterに「武漢に伝染病を持ち込んだのは米軍かもしれない」と投稿したことはその例である[42]。並行して、Twitterの偽アカウントを利用した国家主導の非公然の活動も行われ、中国共産党のパンデミック対応を称賛し、米国、香港、台湾などの対応を批判する内容が繰り返し投稿された[43]。中国が行う影響工作の目標は、中国への支持を広め、敵対国の正当性を損なうような形で、国内外の世論に影響を与えることにあるとみられている[44]。

中国は、2019年から2020年にかけての香港での抗議運動や2020年の台湾総統選挙に際してもデジタル影響工作を展開してきた[45]。最近では、2022年の米国中間選挙等に際して、中国の政治的利益のために活動しているとみられるドラゴンブリッジと名付けられた集団が、投票を思いとどまらせようとするコンテンツの流布などを通して、米国の政治制度や民主的プロセスへの信頼性を傷つけようとする活動を行っていることが指摘されている[46]。

Ⅱ　デジタル影響工作の展開

1　ソーシャルメディア時代の情報環境

インターネット及びソーシャルメディア上では、生成されたコンテンツを、無料で、即座に、世界中に広めることが可能である[47]。また、誰もが情報発信できるというソーシャルメディアの特性は、人々の自由な意見表明を可能にした一方、事実と虚偽、証拠に基づく議論と偏った意見など、様々な情報がフィルターにかけられることなく流通するという点で社会に不安定さももたらしている[48]。それまでの情報環境には、政府と伝統的なメディアが報道倫理等を守る上での「ゲートキーパー」（門番）として一定の役割を果たすという構図があったが、ソーシャルメディアは基本的にそのような統制が及ぶ範囲外に置かれてきた[49]。

ソーシャルメディアの仕組みは、情報環境を更に複雑化させている。ソーシャルメディアのプラットフォームを運営する企業（プラットフォーム企業）は、ユーザーの関心を引き付ける広告やコンテンツを提供することで利益を得ることを基本的な収益モデルとする。そのため、いわゆる「アテンションエコノミー」（関心を競う経済）と呼ばれる、コンテンツが真実か真

---

(41) Renée DiResta et al., "Telling China's Story: The Chinese Communist Party's Campaign to Shape Global Narratives," 2020, pp.34-36. Hoover Institution Website <https://www.hoover.org/research/telling-chinas-story-chinese-communist-partys-campaign-shape-global-narratives>

(42) *ibid*., p.35.

(43) *ibid*., pp.34, 36-39.

(44) Forest, *op.cit.*(3), p.49.

(45) DiResta et al., *op.cit.*(41), pp.19-32.

(46) Mandiant, "Pro-PRC Dragonbridge Influence Campaign Leverages New TTPs to Aggressively Target U.S. Interests, including Midterm Elections," October 26, 2022. <https://www.mandiant.com/resources/blog/prc-dragonbridge-influence-elections>

(47) Arild Bergh, "Understanding Influence Operations in Social Media: A Cyber Kill Chain Approach," *Journal of Information Warfare*, vol.19 no.4, Fall 2020, p.113.

(48) Forest, *op.cit.*(3), p.26; 大治　前掲注(38), pp.135-138.

(49) *ibid*., p.108; Patrikarakos, *op.cit.*(34), pp.9-13; 中西　前掲注(17), pp.8-9.

実でないか、有益か有害かよりも、人々の注目・関心を集めることに経済的価値が見いだされる状況が生まれている[50]。また、アルゴリズム（データの計算や処理の手順）を用いて、ユーザーのインターネット上における行動パターンや志向を分析し、個々人の関心を引き付ける広告やコンテンツを自動的に選択し表示する仕組みが構築されている。ユーザーが特定のコンテンツを「いいね」やリツイートを通じて評価することで、そのコンテンツが更に拡散する効果もある[51]。こうした中で、人々が自分の意見や興味に合う情報ばかりを評価したり共有したりしているうちに、異なる考え方に触れる機会が少なくなる、いわゆる「エコーチェンバー」（反響室）状態に陥り、世論の分断を深める結果となることも指摘されてきた[52]。

以上のようなソーシャルメディアの特徴を利用すると、標的を絞って効果的に影響工作を展開することも可能となる。2015年の研究によれば、特定の人のFacebookの「いいね」を10個分析することで職場の同僚と同程度に、150個分析することで家族と同程度に、300個分析することで配偶者と同程度に、その人の性格を判断できるという[53]。実際に、内部告発によれば、ケンブリッジを拠点とする英国の世論分析企業ケンブリッジ・アナリティカ（2018年5月に破産申請）は、Facebookのアカウントやその他の情報源から大量の個人データを入手し、人々の属性や性格を分析した。その上で、2016年の米国大統領選挙等に際して、分析を通じて特定した「衝動的怒りや陰謀論に傾きやすい集団」などを標的とし、グループページ、広告、記事を経由して操作したコンテンツを流布する活動を行った[54]。また、身元を偽ることが可能なソーシャルメディアでは、影響工作の実施者や背後の実施主体を特定することが難しく、実施主体の側にとっては、少ないリスクで他国の政治システムの弱体化などを図り得ることとなる[55]。ソーシャルメディアの「兵器化」が指摘されるように、ソーシャルメディア時代の情報環境は、人々の認知や世論を誘導する活動を展開するに当たって都合の良い場になっていると言えよう[56]。

2　ディスインフォメーション

(1) ディスインフォメーションとは

影響工作で流布・拡散されるコンテンツの種類の1つに、ディスインフォメーション（disinformation）がある。ディスインフォメーションとは、欧州委員会が設置したフェイクニュースに関する専門家委員会（High Level Expert Group: HLEG）の報告書によれば、「意図的に公衆に危害を及ぼすため又は利益を得るために設計、提示、宣伝された、あらゆる形態の虚偽、不正確又は誤解を招くような情報」である[57]。完全に虚偽の情報のみならず、事実が混合された

---

(50) P. W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media*, Boston: Mariner Books, 2019, pp.20-21, 120; Bergh, *op.cit.*(47), p.116; Forest, *ibid*., p.2.

(51) Bergh, *ibid*., p.114.

(52) Singer and Brooking, *op.cit.*(50), pp.121-127; 笹原和俊『フェイクニュースを科学する―拡散するデマ、陰謀論、プロパガンダのしくみ―』化学同人, 2018, pp.82-98; 大治　前掲注(38), p.99.

(53) Wu Youyou et al., "Computer-based Personality Judgments Are More Accurate than Those Made by Humans," *PNAS*, vol.112 no.4, January 27, 2015, pp.1036-1040. <https://doi.org/10.1073/pnas.1418680112>

(54) Christopher Wylie, *Mindf*ck: Inside Cambridge Analytica's Plot to Break the World*, London: Profile Books Ltd., 2020, pp.95-132.

(55) Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare*, London: Profile Books Ltd., 2021, p.7; Forest, *op.cit.*(3), p.108.

(56) Forest, *ibid*.; Bergh, *op.cit.*(47), p.110; Singer and Brooking, *op.cit.*(50), pp.1-4.

(57) European Commission, *op.cit.*(1), pp.5, 10-11.

ねつ造された情報も含み、かつ、その形態には、ニュースのような形をとるもののほか、ボット（自動で投稿するプログラム）、偽のフォロワーのネットワーク、ねつ造又は操作された動画、標的型広告、組織的なトローリング（荒らし行為）といった手法も含むとされている[58]。なお、ディスインフォメーションは、一般に、意図せずに誤った情報を流通させる誤情報（misinformation）や、危害を及ぼすために事実に基づく情報を流通させる悪情報（malinformation）とは区別されている[59]。

ディスインフォメーションの例として、Ⅰ３（3）で述べた、中国外交部の報道官による新型コロナウイルスの起源として米国を示唆する内容の Twitter の投稿が挙げられる。2016 年の米国大統領選挙に際して、ローマ法王がドナルド・トランプ氏の支持を表明した、ヒラリー・クリントン氏が IS に武器を販売したなどとするデマを伝える記事がニュースサイトに投稿され、Facebook 上で大量に拡散されたことも、ディスインフォメーションの流布・拡散の例である[60]。また、ドイツでは、2016 年に国内外で起きたテロ事件に関連し、事件とは無関係のシリアからの難民がアンゲラ・メルケル（Angela Merkel）首相と撮った自撮り写真が、メルケル首相がテロの実行犯と関係があったような形で Facebook 上に拡散される事例があった[61]。

⑵ ディスインフォメーションの流布・拡散とその影響

Twitter の投稿の拡散様式に関する研究では、ディスインフォメーションは、情報の目新しさなどから、事実よりも速く多く遠くまで拡散されることが指摘されている[62]。ディスインフォメーションの拡散を促す要因には、人の認知特性も関係している。例えば、人は特定の情報に繰り返し遭遇すると、それが虚偽であっても、真実であると認識しやすくなるとされる[63]。また、テロ攻撃、パンデミックといった危機時において、人は不信感や不安感を抱えやすく、その心理状態がディスインフォメーションに反応しやすくさせることも指摘される[64]。

ディスインフォメーションが多く流通する情報環境において、民主主義国家は相対的に脆弱であるとみられている。ディスインフォメーションが氾濫すると、人々が十分な情報を得た上で意思決定をする能力が阻害され、民主的な政治の健全性が損なわれかねない[65]。そもそも、

58　*ibid*., p.10. ディスインフォメーションは、この報告書の解釈が示すように、日本語に訳した場合の「偽情報」よりもやや広い概念を指す語として用いられることが多くなっている。

59　Claire Wardle and Hossein Derakhshan, “Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making,” *Council of Europe Report*, DGI (2017) 09, September 27, 2017, pp.20-21. <https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c>

60　Craig Silverman, “This Analysis Shows How Viral Fake Election News Stories Outperformed Real News on Facebook,” *BuzzFeed News*, November 17, 2016. <https://www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook>; Hannah Ritchie, “Read All about It: The Biggest Fake News Stories of 2016,” December 30, 2016. CNBC Website <https://www.cnbc.com/2016/12/30/read-all-about-it-the-biggest-fake-news-stories-of-2016.html>

61　“The Face of Terrorism Wants His Life Back,” *Wired*, March 8, 2017. <https://www.wired.com/2017/03/the-face-of-terrorism-wants-his-life-back/>

62　Soroush Vosoughi et al., “The Spread of True and False News Online,” *Science*, vol.359 iss.6380, 2018.3.9, pp.1146-1151. <https://doi.org/10.1126/science.aap9559>; 笹原　前掲注(52), pp.45-48.

63　Nadia M. Brashier et al., “An Initial Accuracy Focus Prevents Illusory Truth,” *Cognition*, vol.194, January 2020, Article 104054, pp.1-6. <https://doi.org/10.1016/j.cognition.2019.104054>; Bergh, *op.cit.*(47), p.120; 同上, pp.58-61.

64　Thomas Colley et al., “Disinformation’s Societal Impact: Britain, Covid, and Beyond,” *Defence Strategic Communications*, vol.8, Autumn 2020, pp.98-99. <https://stratcomcoe.org/pdfjs/?file=/publications/download/colley_web.pdf>; 楽原響子「ディスインフォメーションの脅威と国際協力」『国問研戦略コメント』2021.5.17. <https://www.jiia.or.jp/strategic_comment/2021-02.html>

政策に透明性が求められる中で、自ら意図的にディスインフォメーションを流布する対応はとれない[66]。他方、ディスインフォメーションに対抗して流通する情報を統制しようとすると、民主的な社会が尊重する言論・表現の自由や報道の自由といった権利を侵害しかねないことが指摘されている[67]。

3　ナラティブ

(1) ナラティブとは

影響工作で流布・拡散されるコンテンツの種類には、ナラティブ（narrative）もある。ナラティブとは、「出来事について説得力がある形で説明でき、また、そこから推論を導くことができる、人を引き付ける物語の筋立て」を指す[68]。自然発生的なものではなく、他者の反応を形成する目的で意図的に設計され又は育まれる[69]。文字情報のほか、図、絵、写真、映像の形をとることもある[70]。

語り手の主観が反映されるナラティブには、意図の有無によらず、虚偽、事実誤認、論理的矛盾、偏った価値判断が含まれ得る[71]。感情に訴えたり、疑わしい歴史的類推に頼ったりする場合もある[72]。ただし、ナラティブと事実とのかい離が大きいと、語り手に対する信頼が失われるため、ナラティブは、事実に一定程度裏付けられている必要がある[73]。

ナラティブの例として、アルカイダは「イスラム世界は屈辱や差別にさらされ、不当な扱いを受けている。その責任は西洋の側にある」、「イスラム教徒は西洋の影響をイスラム世界から排除するための聖戦に参加する義務がある」などとする趣旨の情報を流布して、信奉者を説得しようとしてきた[74]。また、ロシアによるウクライナ侵攻の当日（2022年2月24日）、プーチン大統領の演説で述べられた「現在起きていることは、…（略）…ウクライナを人質にとり、我が国と我が国民に対し利用しようとしている者たちから、ロシア自身を守るためである」[75]

---

(65) 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, April 26, 2018, pp.1-4, 16. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0236&rid=2>; Laura Rosenberger, "Making Cyberspace Safe for Democracy: The New Landscape of Information Competition," *Foreign Affairs*, vol.99 no.3, May/June 2020, p.147; Rid, *op.cit.*(55), pp.10-11; 桒原　前掲注(14), p.17.

(66) Rid, *ibid*., p.11; 青井　前掲注(12), pp.10, 44-45.

(67) Rosenberger, *op.cit.*(65)

(68) Lawrence Freedman, "The Transformation of Strategic Affairs," *Adelphi Paper*, vol.45 no.379, 2006, p.22.

(69) *ibid.*

(70) 長沼加寿巳「認知領域における戦い―物語（ナラティブ）、感情、時間性―」『NIDS コメンタリー』163号, 2021.3.14, p.3. <http://www.nids.mod.go.jp/publication/commentary/pdf/commentary163.pdf>

(71) 長沼加寿巳「安全保障や防衛におけるナラティブ」『NIDS コメンタリー』155号, 2021.1.15, p.10. <http://www.nids.mod.go.jp/publication/commentary/pdf/commentary155.pdf>; 川口貴久「ウクライナ戦争と「ナラティブ優勢」をめぐる戦い」2022.5.21. SYNODOS ウェブサイト <https://synodos.jp/opinion/international/28156/>

(72) Freedman, *op.cit.*(68), p.23. なお、ある程度事実に裏付けられた既存のナラティブの枠組みを利用してディスインフォメーションが流布される場合などもあり、ナラティブとディスインフォメーションは相互に関連し得る。また、おおむね事実関係に関する情報であるがナラティブの要素も持つような情報もあることなどから、両者を明確に区別できないこともある。James Pamment et al., "Countering Information Influence Activities: The State of the Art," 1 July 2018, pp.26-30. Swedish Civil Contingencies Agency Website <https://rib.msb.se/filer/pdf/28697.pdf>; 川口　前掲注(8), pp.209-211.

(73) 青井　前掲注(12), pp.7-8; Lawrence Freedman, "The Possibilities and Limits of Strategic Narratives," Beatrice De Graaf et al., *Strategic Narratives, Public Opinion, and War: Winning Domestic Support for the Afghan War*, Abingdon, Oxon; New York: Routledge, 2015, p.33.

(74) 同上, pp.137-140.

といった侵攻を正当化する内容の主張も、ナラティブの例である[76]。また、中国の習近平国家主席が提唱する「中国の夢」、日本政府が提唱する「自由で開かれたインド太平洋」（Free and Open Indo-Pacific: FOIP）といったフレーズも、自国の価値観や利害を表明し、他者の共感を呼んだり、他国との連携を広げたりするために利用されるナラティブの一種である[77]。

(2) ナラティブの流布・拡散とその影響

人々を引き付ける効果的なナラティブには、シンプルさ、共鳴、目新しさという特徴があるとされる[78]。複雑さを避け、伝えるべき重要なメッセージに焦点を当てて単純化すると、人々の理解を得やすくなる[79]。また、ソーシャルメディア上において、感情に訴えかけるコンテンツの投稿は、中立的なコンテンツに比べ、より頻繁かつ迅速に共有される傾向があるとされる[80]。感情の中でも、怒りや不安などの感情を招く情報は、喜びなどの前向きな感情を招く情報よりも、速く遠くまで拡散される傾向にあることも指摘される[81]。さらに、人々の注意を引くには、新たに意外な要素を取り入れたり、話の構造にひねりを加えたりすることが有効となる[82]。

近年の国際関係においては、対抗するナラティブの影響力を弱め、自らのナラティブの影響力を高めるため、認知領域で争いが起きているとの見方が広がっている[83]。ソーシャルメディアの強い拡散性は、ナラティブの影響力を高める目的で効果的に利用し得る[84]。そして、現代の紛争に関しても、「勝利はしばしばどの軍隊が勝ったかではなく、誰の物語（story）が勝ったかで決まる」[85]と言われるように、物理的な争いだけでなく、ナラティブをめぐる争いで優勢となることの重要性が高まっていると考えられている[86]。

Ⅲ　デジタル影響工作への対応策

1　情報の遮断

デジタル影響工作への対応策として、相手から発信される情報を遮断する方法が挙げられる。

---

(75)　「【演説全文】ウクライナ侵攻直前 プーチン大統領は何を語った？」2022.3.4. NHK ウェブサイト <https://www3.nhk.or.jp/news/html/20220304/k10013513641000.html>

(76)　青井　前掲注(12), pp.132-134; 大治　前掲注(38), pp.56-57.

(77)　青井　同上, pp.122-128, 145-149.

(78)　Singer and Brooking, *op.cit.*(50), pp.158-161.

(79)　*ibid*., pp.158-159; Freedman, *op.cit.*(73), p.33.

(80)　Stefan Stieglitz and Linh Dang-Xuan, “Emotions and Information Diffusion in Social Media: Sentiment of Microblogs and Sharing Behavior,” *Journal of Management Information Systems*, vol.29 no.4, Spring 2013, pp.217-247. <https://doi.org/10.2753/MIS0742-1222290408>; Forest, *op.cit.*(3), pp.131-134; Singer and Brooking, *ibid*., pp.161-165.

(81)　Rui Fan et al., “Anger Is More Influential than Joy: Sentiment Correlation in Weibo,” *PLOS ONE*, vol.9 iss.10, October 2014, pp.1-8. <https://doi.org/10.1371/journal.pone.0110184>; Singer and Brooking, *ibid*., p.162.

(82)　Freedman, *op.cit.*(16), p.621; Singer and Brooking, *ibid*., p.160.

(83)　川口　前掲注(71)

(84)　加藤太輔・平泉竜也「ソーシャル・メディア時代における戦略的情報発信―「客体からの拡散」によるナラティブの定着へ―」『海幹校戦略研究』12巻1号, 2022.6, p.143. <https://www.mod.go.jp/msdf/navcol/assets/pdf/ssg2022_06_08.pdf>

(85)　Joseph S. Nye, Jr., “The Information Revolution and Power,” *Current History*, vol.113 iss.759, January 2014, p.20. <https://doi.org/10.1525/curh.2014.113.759.19>

(86)　Freedman, *op.cit.*(68), pp.77-78; Patrikarakos, *op.cit.*(34), pp.3-5; Singer and Brooking, *op.cit.*(50), p.160. コソボ紛争（1998～1999年）、対テロ戦争（2001年～）、イラク戦争（2003～2011年）などに関しても、物理面の争いだけでなく、ナラティブをめぐる争いで優勢になることの重要性への指摘がなされている。

ロシアによるウクライナ侵攻が起きた翌週の2022年3月1日、EUは、ロシア政府系メディア「RT」（旧Russia Today）及び「スプートニク」による域内での放送等を禁じる理事会規則を制定した。ケーブルテレビ、衛星放送、インターネットの動画共有プラットフォームを含む、あらゆる手段での放送・配信が対象となった[87]。EUは、その理由を、ロシアが侵攻を正当化するためにEU及び近隣諸国を標的とした継続的で組織的なプロパガンダを行い、事実を著しく歪曲してきたとし、そのことがEUの公共の秩序と安全に対する重大で直接的な脅威であると説明した[88]。これに対し、報道関係機関などからは、最善の対応方法は権威主義国家が手段とするような「放送禁止や検閲」ではなく、多元的なメディア環境を育むことであるとする指摘もなされた[89]。

ウクライナは、ロシアによる侵攻から4日後の2022年2月28日、「プロパガンダやディスインフォメーションを防ぐ」ことを目的に、ドメイン名やIPアドレスなどのインターネット基盤資源を管理・調整する2つの主要な非営利組織（ICANN及びRIPE NCC）に対し、ロシアのドメイン（「.ru」等）の無効化などによって、ロシアのインターネットサービスを世界の他の国々から遮断するよう要請した[90]。両組織とも、インターネット通信の安定性を促進する使命があることなどから、要請に応じることは拒否した。ICANNは返答で、インターネットの仕組みは政治利用されるべきではなく、「人々が信頼できる情報と多様な視点を入手することができるのは、インターネットへの広く自由なアクセスを通じてのみ」とする見解を示している[91]。

情報の遮断は、相手による情報の流布・拡散を阻止することができるが、言論・表現の自由や報道の自由を一部制約する強力な措置であるため、どのような場合にどのようなレベルの措置が許容されるかは議論の余地があろう。

2　情報の真偽の検証

ディスインフォメーションの流布・拡散への対応策として、ファクトチェックや、より広義に、情報の真偽を検証する活動を行うことが挙げられる。ファクトチェックとは、「社会に広がっている情報・ニュースや言説が事実に基づいているかどうかを調べ、そのプロセスを記事化して、正確な情報を人々と共有する営み」である[92]。「非党派性と公平性」、「資金・組織の透明性」など5つの国際標準的な原則が定められており[93]、ファクトチェックの公平性等を保つため、

87　"Council Regulation (EU) 2022/350 of 1 March 2022, Amending Regulation (EU) No 833/2014 concerning Restrictive Measures in View of Russia's Actions Destabilising the Situation in Ukraine," OJ L65, 2022.3.2, pp.1-4. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0350>

88　*ibid*., p.2.

89　"Fighting Disinformation with Censorship Is a Mistake," 2022.3.1. European Federation of Journalists Website <https://europeanjournalists.org/blog/2022/03/01/fighting-disinformation-with-censorship-is-a-mistake/>; "Statement on Banning of RT and Sputnik," 2022.3.4. International Press Institute Website <https://ipi.media/ipi-statement-on-banning-of-rtand-sputnik/>

90　ICANNに宛てた書簡として、次を参照。[Letter from Mykhailo Fedorov, Deputy Prime-Minister of Ukraine to Göran Marby, President and Chief Executive Officer of ICANN], 2022.2.28. ICANN Website <https://www.icann.org/en/system/files/correspondence/fedorov-to-marby-28feb22-en.pdf>

91　ICANNからの返答の書簡として、次を参照。[Letter from Göran Marby, President and Chief Executive Officer of ICANN to Mykhailo Fedorov, Deputy Prime Minister of Ukraine], 2022.3.2. ICANN Website <https://www.icann.org/en/system/files/correspondence/marby-to-fedorov-02mar22-en.pdf>

92　「ファクトチェックの定義など」ファクトチェック・イニシアティブウェブサイト <https://fij.info/introduction/basic>

報道機関や民間の非営利組織などが主な担い手となってきた。なお、ナラティブは、語り手の意見や価値判断に基づくものであるため、基本的にファクトチェックの対象とされない[94]。

EUは、ロシアのディスインフォメーション・キャンペーンに対抗するため、2015年9月、EUの外務省に当たる欧州対外活動庁（European External Action Service）内に「東方戦略的コミュニケーションタスクフォース」（East StratCom Task Force: ESTF）を設置した[95]。ESTFは、主力プロジェクトとしてEUvsDisinfoというウェブサイトを運営し、EU加盟国や近隣諸国に広がる親ロシアのメディアに由来するディスインフォメーションを識別・検証して発表する取組を行っている[96]。ESTFの取組には、ロシアのディスインフォメーションの影響への認識を高めたとする評価がある一方[97]、EUにとって好ましくない意見を虚偽の情報と判定するなど、公平性に問題のある事例があるとする指摘も出ている[98]。

ロシアによるウクライナ侵攻に関連した情報の真偽の検証も様々に行われている。侵攻開始前の2022年2月15日、ロシアの国防省報道官は、Ⅰ3（2）で述べたように、軍事演習終了後にウクライナ国境付近から軍を撤退させていると発表したが、欧米諸国では、各国政府、報道機関、衛星画像等のオープンソースの情報を分析する研究者らがその真偽を検証し、ロシア軍がむしろ国境付近に兵力を結集させているとする判断を一致して示した[99]。近年では、軍やインテリジェンス機関のみならず、一市民や民間の研究者らが衛星画像やグーグル・ストリート・ビューを含むインターネット上の各種の公開情報を用いて情報の真偽を検証して報告し、国家が発信するディスインフォメーションに対抗する動きも見られる[100]。

情報の真偽を検証して広く公表することによって、ディスインフォメーションの流布・拡散による影響を軽減することが期待される[101]。一方、ディスインフォメーションの流布自体を減らす効果はないこと、また、政府などの公的機関が資金を拠出する形のファクトチェックは政

---

(93) 国際ファクトチェックネットワーク（International Fact-Checking Network: IFCN）は、ファクトチェック活動に関する原則として、「非党派性と公正性」、「情報源の基準と透明性」、「資金・組織の透明性」、「検証方法の基準と透明性」、「オープンで誠実な訂正方針」の5つを掲げている。これらの原則を満たすとIFCNへの加盟が認められる（2023年10月時点で105団体が加盟）。“The Commitments of the Code of Principles.” International Fact-Checking Network Website <https://www.ifcncodeofprinciples.poynter.org/know-more/the-commitments-of-the-code-of-principles>

(94) 笹原　前掲注(52), p.158.

(95) Naja Bentzen, “Online Disinformation and the EU’s Response,” *At A Glance*, 2019.2.14. European Parliament Website <https://www.europarl.europa.eu/RegData/etudes/ATAG/2018/620230/EPRS_ATA(2018)620230_EN.pdf>

(96) “EUvsDisinfo.” <https://euvsdisinfo.eu/> 2023年10月時点で、15,000件以上の事例が収録されている。

(97) European Commission and High Representative of the Union for Foreign Affairs and Security Policy, “Joint Communication to the European Parliament, the European Council and the Council: Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats,” JOIN (2018) 16 final, 2018.6.13, p.2. <https://www.eeas.europa.eu/sites/default/files/joint_communication_increasing_resilience_and_bolstering_capabilities_to_address_hybrid_threats.pdf>

(98) Paul Robinson, “The Disinformation Industry: A Cure Worse than the Disease?” January 25, 2022. Centre for International Policy Studies Website <https://www.cips-cepi.ca/2022/01/25/the-disinformation-industry-a-cure-worse-than-the-disease/>;「EU「偽」断定で波紋」『毎日新聞』2018.5.19.

(99) Peter Aldhous and Christopher Miller, “How Open-Source Intelligence Is Helping Clear the Fog of War in Ukraine,” *BuzzFeed News*, March 2, 2022. <https://www.buzzfeednews.com/article/peteraldhous/osint-ukraine-war-satellite-images-plane-tracking-social>; *BBC News*, *op.cit.*(36)

(100) Patrikarakos, *op.cit.*(34), pp.167-202; Singer and Brooking, *op.cit.*(50), pp.71-77; 樋口敬祐「ロシアのウクライナ侵攻に関する情報戦」外交政策センター編, 川上高司ほか編著『2023年野蛮の時代―米中激突第2幕後の世界―』創成社, 2022, pp.247-248.

(101) 実際に、ファクトチェックが誤った情報に対する信用を減らすという実証研究がある。Ethan Porter and Thomas J. Wood, “The Global Effectiveness of Fact-checking: Evidence from Simultaneous Experiments in Argentina, Nigeria, South Africa, and the United Kingdom,” *PNAS*, vol.118 no.37, September 10, 2021, pp.1-7. <https://doi.org/10.1073/pnas.2104235118>

治的に偏る可能性があり、そもそも政治的な言説のファクトチェックから党派的な偏りを排除する難しさがあることなどから、効果に一定の限界があることも指摘される[102]。

3　プラットフォーム企業による対応の促進等

デジタル影響工作による情報環境の悪化への対応策として、プラットフォーム企業に対し、自主的なコンテンツのモデレーション（投稿の監視・削除等）を促したり、モデレーション等の実施に関する法的義務を課したりする方法が挙げられる。政府がソーシャルメディア上のコンテンツの投稿や拡散に直接対処できない中、プラットフォーム企業の不作為は、意図せずとも影響工作の実施を助けてしまう[103]。そこで、プラットフォーム企業が、虚偽の情報等の投稿を禁止するポリシーの策定、悪用を検知するツールの作成、ポリシーに違反したコンテンツの削除やアカウントの停止・削除などを行うことが期待されている[104]。

2016年以降、米国大統領選挙への介入を契機にディスインフォメーションの脅威への認識が高まる中で、プラットフォーム企業は今日では国家に比類するほどの大きな影響力を持っており、コンテンツのモデレーションや情報開示の強化を通じて社会的責任を果たしていくべきとする見方が広がった[105]。こうした動向も背景に、プラットフォーム企業は自主的な対応を重ねてきている。例えば、2019年10月、Facebook社（現Meta社）は、Facebook上において国家が関与する4つのディスインフォメーション・キャンペーンを発見して投稿を削除したことを公表するとともに、身元の偽装や外国政府又はその代理人が組織的に人々を欺く行為を含む、偽装行為（inauthentic behavior）を禁止するポリシーを策定した[106]。他の主要なプラットフォーム企業も、ポリシーに違反するアカウントの停止・削除、ディープフェイク動画（AIを用いて人物の画像や音声を合成した偽の動画）の投稿の禁止、合成・操作されたコンテンツや誤解を招くコンテンツをユーザーが報告したりプラットフォーム側がラベル付けしたりする機能の導入などを行ってきている[107]。

従来、主要国におけるプラットフォーム企業に対する法的規制は、明らかに違法なコンテンツを知った場合に削除を義務付けるなど、コンテンツの作成者と同じ責任を負わせずに一定の免責を与える観点から行われるにとどまり、その下で、企業による自主的な対応が期待されて

---

(102)　藤代裕之「日本のニュース生態系と影響工作」一田ほか　前掲注(2), pp.133-135; 鍛治本正人「偽情報対策としてのファクトチェックの有効性と限界（後編）―事例からみる選挙および政治的混乱に際しての傾向と課題―」『国際情報ネットワーク分析』2022.7.11. 笹川平和財団ウェブサイト <https://www.spf.org/iina/articles/kajimoto_02.html>; 佐々木孝博『近未来戦の核心サイバー戦―情報大国ロシアの全貌―』育鵬社, 2021, pp.220-221. 2019年以降、インド、タイ、ベトナムなどのアジア諸国において、政府主導のファクトチェック部門の設立が相次いでおり、ファクトチェックが政治的に濫用される可能性が懸念されている。鍛治本正人「偽情報対策としてのファクトチェックの有効性と限界（前編）―アジア地域における選挙をめぐる取り組み―」『国際情報ネットワーク分析』2022.7.5. 笹川平和財団ウェブサイト <https://www.spf.org/iina/articles/kajimoto_01.html>

(103)　大澤淳ほか「座談会　戦場はスマホの中に―「ナラティブ」が情報戦の最前線―」『外交』80号, 2023.7･8, p.13.

(104)　Forest, *op.cit.*(3), p.232.

(105)　例えば、次を参照。Francis Fukuyama et al., "How to Save Democracy from Technology," *Foreign Affairs*, vol.100 no.1, January/February 2021, pp.98-104, 106-110; Ian Bremmer, "The Technopolar Moment: How Digital Powers Will Reshape the Global Order," *Foreign Affairs*, vol.100 no.6, November/December 2021, pp.112-128; Singer and Brooking, *op.cit.*(50), pp.267-271; 小宮山功一朗「民主主義の危機をもたらすサイバー空間」小泉ほか　前掲注(8), pp.194-196.

(106)　"Facebook Finds New Disinformation Campaigns and Braces for 2020 Torrent," *New York Times*, October 22, 2019; "Inauthentic Behavior." Meta Website <https://transparency.fb.com/ja-jp/policies/community-standards/inauthentic-behavior>

(107)　Forest, *op.cit.*(3), pp.232-233.

きた[108]。こうした立場より踏み込んだ対応がとられた例がドイツにある。2017年7月成立（同年9月公布、10月施行）の「ネットワーク執行法」（NetzDG）は、「違憲組織及びテロ組織のプロパガンダ資料の頒布」などの違法コンテンツを特定した上で、国内登録者数が一定以上のプラットフォーム企業に対して、明らかに違法なコンテンツを苦情到達から24時間以内に削除すること等を義務付け、義務に違反した場合には罰金を科すことを規定している[109]。

EUも、2022年10月に「デジタルサービス法」（Digital Services Act）を制定し、プラットフォーム企業に違法コンテンツの排除等に向けた法的義務を課す方向へと転換した（一部施行を経て、2024年2月17日に全面施行予定）[110]。同法は、EU域内でオンライン仲介サービス（ソーシャルメディア、オンラインマーケットプレイス、検索エンジン等）を提供する企業に対し、その規模や影響力に応じて、ディスインフォメーションやヘイトスピーチなどの違法コンテンツを排除するための措置や透明性の確保を義務付けることを主な内容としている[111]。非常に大規模なオンラインプラットフォーム及び検索エンジン（Facebook、Twitter、Google検索を含む19のサービス[112]）に対しては、ディスインフォメーションや欺まん的なコンテンツの拡散を軽減する措置や、紛争、テロ、パンデミック等の危機時に欧州委員会の要求に基づいてディスインフォメーションの拡散を制限する措置（モデレーションのプロセスやアルゴリズムを適応させること等）などを講ずるよう追加的な義務を設け、義務の不履行に対して高額の罰金（最高で全世界での年間売上高の6%）を課すことを規定している[113]。

プラットフォーム企業がコンテンツのモデレーション等を行うことで、情報環境の悪化が抑制されることが期待される一方、表現の自由を侵害する可能性も懸念されている[114]。企業が自主的にモデレーションを行う場合についても、私企業に情報の真偽や違法性に関する判断を下す責任を負わせるべきか、そもそも適切に判断できるのかについて議論がある[115]。

---

(108)　小西葉子「偽情報と日米独のプラットフォーマー規制」『外交』80号, 2023.7・8, pp.52-57.

(109)　Netzwerkdurchsetzungsgesetz vom 1. September 2017 (BGBl. I S. 3352). <https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html>; 同上, pp.54-56. なお、ネットワーク執行法はEUのデジタルサービス法の全面施行と同時に廃止される予定であり、国内法としてデジタルサービス法を補完する内容の法律案の検討が進められている。“BMDV legt Entwurf für ein Digitale-Dienste-Gesetz vor,” 2023.8.4. Bundesministerium für Digitales und Verkehr Website <https://bmdv.bund.de/SharedDocs/DE/Pressemitteilungen/2023/079-wissing-digitale-dienste-gesetz.html>

(110)　乗原　前掲注(8), pp.41-43.

(111)　“Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act),” OJ L277, 2022.10.27, pp.1-102. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065> なお、違法コンテンツは、同法上では特定されておらず、EU及び加盟国国内の法律の規定に基づく。

(112)　“Digital Services Act: Commission Designates First Set of Very Large Online Platforms and Search Engines,” 25 April 2023. European Commission Website <https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413>

(113)　デジタルサービス法の施行をめぐっては、EUがXによるモデレーション等の対応が十分かどうかをめぐって調査を始めることを発表するなどの動きがある。「偽情報対策、EUとX火花」『日本経済新聞』2023.10.27.

(114)　笹原　前掲注(52), pp.172-173; 成原慧「インド太平洋地域におけるディスインフォメーションの流通とその対策―米国政府とプラットフォーム事業者による対策に着目して―」『国際情報ネットワーク分析』2022.12.5. 笹川平和財団ウェブサイト <https://www.spf.org/iina/articles/narihara_01.html>; “Op-Ed: Don’t Be Too Tempted by Europe’s Plan to Fix Social Media,” *Los Angeles Times*, 2022.12.23. <https://www.latimes.com/opinion/story/2022-12-23/europe-digital-services-act-social-media-regulation-free-speech>; “Germany: Flawed Social Media Law: NetzDG Is Wrong Response to Online Abuse,” February 14, 2018. Human Rights Watch Website <https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law>

(115)　Nicol Turner Lee and Samantha Lai, “Commentary: Is There Too Little Oversight of Private Tech Companies in the Russia-Ukraine Conflict?” March 30, 2022. Brookings Institution Website <https://www.brookings.edu/articles/is-there-too-little-oversight-of-private-tech-companies-in-the-russia-ukraine-conflict/>; 手賀洋一「フェイクニュース対策と民主主義―メディアプラットフォームの社会的責任―」『千葉商大紀要』60巻1号, 2022.7, pp.28-30.

4　戦略的な情報発信

デジタル影響工作への対応策として、積極的な情報開示や対抗的なナラティブの発信などを通じ、戦略的に情報発信を行うことが挙げられる(116)。

米国は、ロシアによるウクライナ侵攻が起きる前、ロシアが虚偽の情報を発信していることを示す形で、積極的な情報開示を行った(117)。例えば、2022年1月14日、ホワイトハウスの報道官は、ロシア政府がウクライナ侵攻を命令する口実を与え得る事件を演出するため、ウクライナ東部に破壊工作員を派遣していると発表した(118)。ディスインフォメーションが提示される前に、惑わされる可能性があることを人々に認識させる事前暴露（prebunking）と呼ばれる手法で、ディスインフォメーションの定着を防ぐのに有効とされる(119)。また、2022年2月18日、ロシア側が侵攻の意図を否定する中、ジョー・バイデン（Joe Biden）大統領は、プーチン大統領がウクライナ侵攻を決断したかを問われた際、「彼が決断したと確信している。そう信じる理由がある」と述べた(120)。

ロシアによる侵攻を受けてウクライナが行ってきた情報発信は、ロシアの影響工作に対抗する上で、一定の成功を収めたと考えられている。ロシア側は、ヴォロディミル・ゼレンスキー（Volodymyr Zelenskyy）大統領が国外に逃亡したとする虚偽の情報や、ゼレンスキー大統領が国民に武器を置いて投降を呼びかける内容のディープフェイク動画などを流布した。これに対して、ウクライナのゼレンスキー大統領らは、キーウ市内から「私たちはここにいる」と訴えかけるメッセージ動画を速やかに投稿し、また、ロシア側が否定する侵攻や市民への攻撃の事実をソーシャルメディア上で発信するなどして、ウクライナ国民や国際社会に対して積極的に情報を発信し続けた。また、ゼレンスキー大統領が米国、英国、ドイツ、日本等の各国議会で行った演説は、相手国民の感情に訴えるようなキーワードを用いて自国の立場を訴え、ウクライナに対する支持や援助を得る上で効果的であったとみられている(121)。

戦略的な情報発信は、自国の情報環境を守るとともに、自国の立場への国内外からの支持を得る手段となることが期待される。他方、自国にとって好ましくない情報を封じ込めるために情報統制や検閲を行い得る権威主義国家に対しては、その効果は限定的なものにとどまる可能性がある(122)。また、民主主義国家が自国の正当性を発信することは、方法や程度によっては異論の排除や言論統制につながるリスクをはらむため、慎重な調整が求められる(123)。

---

(116)　本稿では、「戦略的な情報発信」を単に戦略的に情報を発信するという意味で用いる。よって、国家の政策決定の時点から政策の一部として行われるよう調整されることを要件とする「戦略的コミュニケーション」には必ずしも当たらない。青井　前掲注(12), pp.23-27.

(117)　川口貴久「ウクライナ米欧vsロシア―認知空間での闘いの内幕―」2022.4.29. Wedge Onlineウェブサイト <https://wedge.ismedia.jp/articles/-/26519>; 髙木耕一郎「米国が制したウクライナ情報戦」『外交』80号, 2023.7・8, pp.34-36; 大治　前掲注(38), pp.57-61; 佐々木　前掲注(29), pp.196-197.

(118)　"U.S. Says Moscow Sent Saboteurs to Roil Ukraine," *New York Times*, January 15, 2022.

(119)　Stephan Lewandowsky, "Disinformation and Human Cognition," 13 August 2019. Security and Human Rights Monitor Website <https://www.shrmonitor.org/disinformation-and-human-cognition/>

(120)　"Remarks by President Biden Providing an Update on Russia and Ukraine," February 18, 2022. White House Website <https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/02/18/remarks-by-president-biden-providing-an-update-on-russia-and-ukraine-2/>

(121)　小泉悠・楽原響子「ポスト「2016」の世界」小泉ほか　前掲注(8), pp.139-147; 青井　前掲注(12), pp.6-8; 川口　前掲注(117); 佐々木　前掲注(29), pp.195-196.

(122)　小谷賢「解説　ソ連・ロシアの恐るべき積極工作」トマス・リッド（松浦俊輔訳）『アクティブ・メジャーズ―情報戦争の百年秘史―』作品社, 2021, p.471.（原書名：Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare*, London: Profile Books Ltd., 2021.）

5　実施者に対する懲罰

選挙介入等を目的としてデジタル影響工作を実施した組織や個人等に対し、既存の制定法に基づき刑事上の責任を問う、又は、刑事訴追や経済制裁を行うための法整備を行う動きがある。

米国では、2018年2月、司法省が、2016年の米国大統領選挙に際して「米国に対する情報戦」を行い、米国の政治制度に干渉しようとして連邦犯罪を犯したとして、IRAを始めとするロシアの3団体とロシア人13人を起訴した[124]。また、2018年9月に大統領令13848号が制定され、連邦の公職者の選挙終了後45日以内に国家情報長官が外国政府やその代理人等による選挙介入に関する情報を評価すること、選挙介入が明らかになった場合は関与した者に対して制裁（資産凍結等）を課すことなどが規定された[125]。

台湾においても、選挙や新型コロナウイルス感染症に関するディスインフォメーションを流布・拡散する行為に対して、噂の拡散によって公共の安定に影響を及ぼす行為を禁じる社会秩序維護法の規定に基づく訴追が行われている[126]。また、2019年12月には、選挙に関するディスインフォメーションの拡散を含め、外部の勢力による選挙運動やロビー活動を禁じる「反浸透法」が成立した（2020年1月公布・施行）[127]。

懲罰的措置を採ることによって、将来的にこうした行為を実施しようとする組織や個人の行動を一定程度抑止することが期待されている[128]。訴追後に実施者の処罰に至らない場合でも、実施者の不正行為や背後にいる国家などを指摘し公表することで名指しと辱め（naming and shaming）を与え、以後に実施者らが検知されずに活動する能力を制限することが期待されている[129]。懲罰的措置を行うための前提としては、ソーシャルメディア上での影響工作を検知する能力や、実施者及び実施主体を特定する能力が必要となることが指摘されている[130]。なお、

---

(123)　川口　前掲注(71)

(124)　“Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System,” February 16, 2018. U.S. Department of Justice Website <https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere> 米国に対する犯罪又は米国を欺くことの共謀（合衆国法典第18編第371条）を始めとする、複数の連邦犯罪を犯したものとされている。

(125)　“Executive Order 13848: Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election,” September 12, 2018. U.S. Government Publishing Office Website <https://www.govinfo.gov/content/pkg/DCPD-201800593/pdf/DCPD-201800593.pdf> 同大統領令の効力は以後延長されている（現時点で2023年9月12日から1年間まで有効）。“Press Release: Notice on the Continuation of the National Emergency with Respect to Foreign Interference in or Undermining Public Confidence in United States Elections,” September 7, 2023. White House Website <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/09/07/press-release-notice-on-the-continuation-of-the-national-emergency-with-respect-to-foreign-interference-in-or-undermining-public-confidence-in-united-states-elections/>

(126)　「社會秩序維護法」全國法規資料庫ウェブサイト <https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=D0080067>; 陳德顥「台湾における偽情報の対策および現況」2023.3.13, p.3. 情報法制研究所ウェブサイト <https://jilis.org/report/2023/jilisreport-vol5no7.pdf>

(127)　「反滲透法」全國法規資料庫ウェブサイト <https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030317>; 陳　同上, p.4.

(128)　David Salvo and Joshua Kirschenbaum, “No Time for Complacency: How to Combat Foreign Interference After the Midterms.” German Marshall Fund Website <https://www.gmfus.org/news/no-time-complacency-how-combat-foreign-interference-after-midterms>

(129)　Elizabeth Bodine-Baron et al., *Countering Russian Social Media Influence*, Santa Monica, CA: RAND Corporation, 2018, pp.32-38. <https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2740/RAND_RR2740.pdf>; “Indictment Bares Russian Network to Twist 2016 Vote,” *New York Times*, February 17, 2018.

(130)　Tomoko Nagasako, “Global Disinformation Campaigns and Legal Challenges,” *International Cybersecurity Law Review*, vol.1, October 2020, p.134. <https://doi.org/10.1365/s43439-020-00010-7>; 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―』東京海上日動リスクコンサルティング, 2019, pp.45-46. <https://www.tokio-dr.jp/service/politics/rispr/pdf/pdf-rispr-01.pdf>

反体制的な言論を政府が違法と認定して罰する場合など、方法によっては、言論・表現の自由を侵害する可能性も懸念される(131)。

6　国民の情報リテラシーの向上

デジタル影響工作による人々の認知や世論への影響を抑制するための方法として、国民の個々人のレベルで情報リテラシーの向上を図っていくことが挙げられる(132)。

スウェーデンは、地理的に近接するロシアからの影響工作等に対抗し、自由で民主的な社会を守るため、2022年1月、国防省の下に心理防衛庁（Myndigheten för psykologiskt försvar）を設立した。同庁は、国外からの悪意のある情報の特定、分析、対抗と並んで、情報リテラシー教育を強化する施策を含め、悪影響を与えるキャンペーンやディスインフォメーションを発見し抵抗する国民の能力を強化するための取組を行っている(133)。

情報の信頼性の判断には高度な技能を要し、現在の情報リテラシー教育の効果には限界があることも指摘されるが(134)、表現の自由などの民主的価値の根幹を守りつつ、中長期的ながらもより根本的な問題の解決となることが期待されている(135)。また、情報リテラシーが社会に行き渡り、デジタル影響工作の効果が見込めないことが実施主体の側に伝われば、実施するインセンティブを失うという意味で、一定の抑止効果を持つ可能性も指摘されている(136)。

おわりに

影響工作は情報伝達に関わる技術の発展に伴って変化してきており、インターネット及びデジタル技術の発展を背景とした現在のデジタル影響工作も、その通過点としてみることができる。今後も、生成AIなどの新しい技術を取り込み、巧妙さを増しながら影響工作が展開されていくことが予想される(137)。

国民の情報リテラシーの向上以外の5つの対応策は、デジタル影響工作による情報環境の悪化の防止や抑制を図ろうとするもので、表現行為の規制につながる要素を含んでいる。そのため、影響工作に対応しようとして、程度や方法を間違えば、民主的な社会が尊重してきた権利を侵害してしまうという基本的なジレンマが存在する。デジタル影響工作に対応するに当たっては、政府、プラットフォーム企業、報道機関、市民社会などが適切に役割分担し連携した上

---

(131)　アジア諸国でも、シンガポールの「オンライン虚偽情報及び情報操作防止法」（Protection from Online Falsehoods and Manipulation Act 2019）など、政府が公共の利益に反する虚偽の情報だと認定したコンテンツの発信者を禁固・罰金刑に処すことができる法律の制定事例があり、言論の自由を侵害する可能性が懸念されている。*ibid.*, pp.134-135; “Singapore: Social Media Companies Forced to Cooperate with Abusive Fake News Law,” February 19, 2020. Amnesty International Website <https://www.amnesty.org/en/latest/news/2020/02/singapore-social-media-abusive-fake-news-law/>

(132)　佐々木　前掲注(29), pp.194-195.

(133)　“Om oss,” 18 September 2023. Myndigheten för psykologiskt försvar Website <https://www.mpf.se/om-organisationen/>;「スウェーデン　露の偽情報対策強化　「心理防衛庁」を新設」『産経新聞』2022.1.25.

(134)　藤代　前掲注(102), pp.130-133, 136; 手賀　前掲注(115), pp.22-23; Singer and Brooking, *op.cit.*(50), pp.271-272.

(135)　桒原響子「カナダの偽情報対策にみる成果と課題―日本へのインプリケーション―」『Roles Report』25号, 2023.6, p.15. <https://roles.rcast.u-tokyo.ac.jp/uploads/publication/file/56/publication.pdf>

(136)　佐々木　前掲注(102), pp.220, 224-225.

(137)　Forest, *op.cit.*(3), pp.228-231; Singer and Brooking, *op.cit.*(50), pp.248-257; 川口貴久「誰もが当事者に―生成AIによる影響工作「新時代」―」2023.7.10. Wedge Online ウェブサイト <https://wedge.ismedia.jp/articles/-/30776>

で、表現の自由等の民主的価値を守りつつ、各国の選択に応じて、透明性のある形で行っていくことが求められよう。そして、価値を同じくする国家、民間組織、研究者などの様々なアクター同士が連携し、国際的に知見を共有していくことも必要となろう。

（きゅうこ　さとみ）