デジタル影響工作対策の課題

―なぜ EU・アメリカは中露イランの手法に対応できないのか？

一田和樹
（明治大学サイバーセキュリティ研究所客員研究員）
2024 年 3 月 11 日

要旨

EU やアメリカで行われているデジタル影響工作対策は偽情報への対処を中心としたもので、それに関連して海外からの干渉や大手 SNS プラットフォームなどへの対処が含まれている。しかし、中露伊（中国、ロシア、イラン）の作戦の主たる狙いは相手国の国内にすでに存在する分断や不信を広げることであり、偽情報や大手 SNS プラットフォームの利用はその方法のひとつにすぎない。中露伊は他の選択肢を用いて EU やアメリカの対策を回避できるため EU やアメリカの対策の効果は限られた範囲に留まっている。

攻撃主体の狙いが相手国内の分断や不信である以上、防御側にとって自国の社会全体を含めた状況の把握は対処ならびに調査研究の前提となる。しかし実際の調査研究ではケーススタディが多く、全体像が調査研究されることは稀であるため有効な知見が乏しい。

全体像を欠いた対症療法となっている現在の対策は無差別な警告を発する警戒主義に陥りがちで、結果として分断と不信を広げている可能性がある。デジタル影響工作への対策においては全体像の把握と共有を優先することが重要である。

中露イランによるデジタル影響工作の変化

欧州連合(European Union: EU)やアメリカによるデジタル影響工作への対策の多くは偽情報対策(誤情報含む)に焦点を当てている。そのために海外からの偽情報を利用した干渉を阻止し、大手 SNS プラットフォームや大手アドネットワークに対処を徹底するよう要請している。EU では大手の SNS プラットフォームやアドネットワークへの規制を導入し、アメリカサイバー軍(United States Cyber Command、通称サイバーコム)はロシアなどに対して能動的な防衛手段を講じた。

しかし、この対抗策は攻撃側である中露伊(中国、ロシア、イラン)の目的ではなく、個別の攻撃手法に対応しているため回避されやすい(デジタル影響工作の手法については表1を参照)。2023 年 12 月 11 日に公開されたアメリカ国家情報会議(National Intelligence Council)のレポートなどから中露伊の新しい手法に対応できていない状況がわかる[1]。

表1 共通化されてきたデジタル影響工作の TTPs(戦術、技術、手順)と対策

攻撃手法	概要	対策の効果
国営メディア・外交官	国営のメディアや外交官など正規のルートからの情報発信。政府の外交関係者のアカウントや投稿された情報は SNS から削除されにくい。	× 外交官などへの対応は難しいことが多い。
プロキシ	表向き政府の関与がないように見せているが、実際には政府が関与しているシンクタンク、NPO、メディアなどからの情報発信。ロシアの Election Watch、Lies of Wall Street といったドッペルゲンガーや News Front などが有名。	△ プロキシの実態はだいぶ把握されてきている。
AI の活用	LLM を活用した画像や動画テキストを生成して利用。	? 手法が開発途上
CIB	SNS の不正利用。ボットやトロール、アカウン	◎

[1] National Intelligence Council,"Foreign Threats to the 2022 US Elections," December 11, 2023. (https://www.odni.gov/files/ODNI/documents/assessments/NIC-Declassified-ICA-Foreign-Threats-to-the-2022-US-Elections-Dec2023.pdf)；一田和樹「陰謀論とロシアの世論操作を育てた欧米民主主義国の格差」,Newsweek 日本版(2023 年 5 月 10 日)。(https://www.newsweekjapan.jp/ichida/2023/05/post-46.php);Rossine Fallorina, Jose Mari Hall Lanuza, Juan Gabriel Felix Ferdinand Sanchez II , Jonathan Corpus Ong, Nicole Curato, "The Evolution of Disinformation in Three Electoral Cycles," Internews (June 29, 2023). (https://internews.org/resource/from-disinformation-to-influence-operations-the-evolution-of-disinformation-in-three-electoral-cycles/); Samuel Woolley, *Manufacturing Consensus* (New Haven: Yale University Press, 2023) ; Brad Smith, "Defending Ukraine: Early Lessons from the Cyber War," Microsoft, June 22, 2022. (https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/);一田和樹「マイクロソフト社のレポートは影響工作に焦点を当てていた『Defending Ukraine:Early Lessons from the Cyber War』」一田和樹のメモ帳(2022 年 7 月 2 日)。(https://note.com/ichi_twnovel/n/n2cd93a5de9ab)

攻撃手法	概要	対策の効果
(Coordinated Inauthentic Behavior)	ト乗っ取りなど様々な方法がある。中国の Spamouflage が有名。	有効な対処方法が確立されつつある。
ハック&リーク	ハッキングして盗んだ情報を公開することで影響を与える。ロシアの Tainted Leaks や民主党へのハッキングが有名。盗んだ情報を悪用する事もある。	◎ 有効な対処方法が確立されつつある。
小規模 SNS、メッセンジャー利用	規制が厳しくなってきた SNS ではなく規制の緩い小規模 SNS を利用する。また Telegram のように暗号化されているメッセンジャーを使う事が増えている。	×× 実態の把握や対処方法が確立されていない。
大手 SNS と連動	上記活動と合わせて、小規模 SNS やメッセンジャーの投稿を大手 SNS に転載する。関係者が行うだけでなく、相手国の同調者が協力することもある。	×× 実態の把握が難しいうえ、同調者が自国民である場合対処が難しい。
分散化	上記活動と並行して数十の SNS などに分散して活動するよう変化した。	△ 大手 SNS には対処可能。
相手国の同調者と連動	中露イランは相手国の国内の個人やグループ、メディアが同調しやすいナラティブを拡散し、自らも相手国内の都合のよいナラティブを拡散する。相手国内の反主流派(RMVEs、陰謀論者、右派など)とは共鳴しやすい。	×× 自国民を利用された場合、言論や表現の自由との兼ね合いもあり、対処が難しい。
インフォメーション・ロンダリング	発信した情報を相手国のメディアに転載させることで、信用を得やすくする。	× 現在対処していない。
パーセプションハッキング	影響工作が露見した際、逆にそのことを広めることで、相手国内にあらゆる情報に対する不安と不信を募らせる。最近では、「やっていない」サイバー攻撃や影響工作を自ら公表し、パーセプション・ハッキングの効果を狙う手口もある。	×× 原理的に対処不能。

出典:一田和樹「2024 年選挙の年、世界のあり方が変わるかもしれない」Newsweek 日本版、2024 年 1 月 10 日(https://www.newsweekjapan.jp/ichida/2024/01/2024.php)に加筆。

ロシアは 2016 年のアメリカ大統領選でも相手国であるアメリカ国内の分断と不信を広げよう

とし[2]、それに先立つ BLM(Black Lives Matters)運動でも同様だった[3]。ヨーロッパに対しては相手国内の極右や独立運動を支援するなどの影響工作を以前から行ってきていた[4]。EU とアメリカはそのことがわかっているにもかかわらず、有効に対処できず、いまだに偽情報を中心とした対症療法を行っている。相手国の国内の分断や不信を利用するには、相手国内のグループや個人を扇動、協力、支持表明すればよい(表2タイプ 3 と 4)。あくまで主体は相手国の国内グループや個人になる。

表2 デジタル影響工作の 4 分類

攻撃主体の活動		判断	欧米による対策の対象		現状の対策
			国内	国外	
タイプ 1	自ら実行	明確な敵対的干渉	デジタル影響工作対策の対象になっていない。	○	○
タイプ 2	指示、命令	干渉と判断		○	○
タイプ 3	扇動、協力	グレーゾーン		△	×
タイプ 4	支持表明、間接的支援	グレーゾーン		×	×

注:水色部分=非難はできるが、強制力を持つ対策は難しく、否認可能性も高い。
出典:一田和樹「今年の振り返り 周回遅れの情報戦対策と攻撃の深刻な乖離が進む」一田和樹のメモ帳、2023 年 12 月 28 日(https://note.com/ichi_twnovel/n/n3b271f0fe338)を修正。

一方、旧来のタイプ 1 や 2 の手法である「協調的な不正行為(Coordinated Inauthentic Behavior:CIB)なども併用されており、こちらに対しては EU とアメリカによる対策で成果をあげることができる。その他の攻撃には対処できていないが、成功した結果だけが公表されるため

[2] Renee DiResta, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright, Ben Johnson, "The Tactics & Tropes of the Internet Research Agency," Congress of the United States (October 2019). (https://digitalcommons.unl.edu/senatedocs/2/); Philip N. Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly, Camille François, "The IRA, Social Media and Political Polarization in the United States 2012-2018," University of Oxford (October 2019). (https://digitalcommons.unl.edu/senatedocs/1/)

[3] 2015 年 4 月 17 日、ZeroFOX 社がボルチモア市長にメールで送った"Crisis Manegemt"の中にロシアの干渉についての記載がある。現在、"Crisis Manegemt"は削除されている。; 一田和樹、江添佳代子『犯罪「事前」捜査 知られざる米国警察当局の技術』(角川新書、2017 年)第一章;Donie O'Sullivan, Dylan Byers, "Exclusive: Fake black activist accounts linked to Russian government," CNN 8September 27, 2017). (https://money.cnn.com/2017/09/28/media/blacktivist-russia-facebook-twitter/index.html)

[4] Alina Polyakova, Marlene Laruelle, Stefan Meister, Neil Barnett,"The Kremlin's Trojan Horses," Atlantic Council (November 15, 2016). (https://www.atlanticcouncil.org/in-depth-research-reports/report/kremlin-trojan-horses/);Alina Polyakova, Markos Kounalakis, Antonis Klapsis, Luigi Sergio Germani, Jacopo Iacoboni, Francisco de Borja Lasheras, Nicolás de Pedro, "The Kremlin's Trojan Horses 2.0," Atlantic Council (November 15, 2017). (http://www.atlanticcouncil.org/publications/reports/the-kremlin-s-trojan-horses-2-0);Alina Polyakova, Flemming Splidsboel Hansen, Robert van der Noordaa, Øystein Bogen, Henrik Sundbom, "The Kremlin's Trojan Horses 3.0," Atlantic Council (December 4, 2018). (https://www.atlanticcouncil.org/in-depth-research-reports/report/the-kremlins-trojan-horses-3-0/)

一見うまくいっているように見えてしまう。代表例が 2021 年 1 月 6 日のアメリカ連邦議事堂襲撃だ。2020 年アメリカ大統領選挙では、中露のデジタル影響工作抑止に一定の成果があったとされたが、翌年 1 月 6 日に Q アノン（QAnon）などの国内グループの暴徒がアメリカ連邦議事堂を襲撃した。その背後に中露のデジタル影響工作があったことがスーファン・センター（Soufan Center）のレポートで明らかにされている[5]。このレポートには異論もあるが、Q アノンと中露の結びつきについては注 11 にあげた他のレポートでも指摘されており、なんらかの関与はあったと考えられる。

近年はアメリカ国内のデジタル影響工作対策の後退が起きている[6]。さらに 2024 年の大統領選挙においては結果の如何によらず混乱が起きることが予想されるほどアメリカ国内の分断と不信は悪化した[7]。

中露伊の干渉だけでアメリカの分断と不信が悪化しているわけではないが、三国はその一端を担っている。最近ロシアはアメリカの選挙へのサイバー攻撃を控えているが、その理由はアメリカ国家情報会議（National Intelligence Council）のレポートによるとデジタル影響工作の方が低リスクで高い効果を得られると判断したためである[8]。

国内の分断と不信が広がっているのはアメリカだけの問題ではなく、他の多くの民主主義国においても同様であり、ポピュリズムの台頭や権威主義化につながっている[9]。それを推進するグループは白人至上主義グループなど人種あるは民族的偏見に基づく過激派の RMVEs（Racially or Ethnically Motivated Violent Extremists）や陰謀論者、極右など多様だが、全く異な

---

[5] Jason Blazakis, Mohamed H. El Shawesh, Naureen Chowdhury Fink, Leela McClintock, Mollie Saltskog, Zach Schwitzky, “QUANTIFYING THE Q CONSPIRACY: A Data-Driven Approach to Understanding the Threat Posed by QAnon,” Soufan Center (Arpil 21, 2021). (https://thesoufancenter.org/research/quantifying-the-q-conspiracy-a-data-driven-approach-to-understanding-the-threat-posed-by-qanon/);Zachary Cohen, “China and Russia ‘weaponized’ QAnon conspiracy around time of US Capitol attack, report says”, CNN (April 19, 2021). (https://edition.cnn.com/2021/04/19/politics/qanon-russia-china-amplification/index.html)； 一田和樹「コロナ禍で中国やロシアが広めた QAnon の陰謀論」一田和樹のメモ帳（2022 年 10 月 9 日）。(https://note.com/ichi twnovel/n/ne1c8818d9a5c)

[6] 一田和樹「アメリカの偽情報対策が直面している問題」『一橋大学グローバル・ガバナンス研究センター Issue Briefing』No.32、2023 年 9 月 1 日、(https://ggr.hias.hit-u.ac.jp/2023/09/01/problems-facing-us-disinformation-measures/)

[7] Ian Bremmer, Cliff Kupchan「ユーラシア・グループ 2023 年 10 大リスク」ユーラシア・グループ（2024 年 1 月）。
(https://www.eurasiagroup.net/siteFiles/Media/files/Top%20Risks%202024%20JPN.pdf)

[8] National Intelligence Council,“Foreign Threats to the 2022 US Elections,” (December 11, 2023). (https://www.odni.gov/files/ODNI/documents/assessments/NIC-Declassified-ICA-Foreign-Threats-to-the-2022-US-Elections-Dec2023.pdf);一田和樹「米国インテリジェンス・コミュニティの評価の変化からわかる新しい認知戦のトレンド」一田和樹のメモ帳（2024 年 1 月 7 日）。
(https://note.com/ichi twnovel/n/n30ab8574915c)

[9] Jon Henley, “How Europe’s far right is marching steadily into the mainstream,” The Guardian (June 30, 2023). (https://www.theguardian.com/world/2023/jun/30/far-right-on-the-march-europe-growing-taste-for-control-and-order);Pankaj Mishra, “Europe’s Far Right Isn’t So Fringe Anymore,” Washington Post (July 19, 2023). (https://www.washingtonpost.com/business/2023/07/19/europe-s-far-right-putin-allies-are-rising-in-popularity/286def02-25ef-11ee-9201-826e5bb78fa1_story.html);Tim Gosling, “Nationalist, populist, far-right parties eye rising support across Europe,” Aljazeera (September 20, 2023). (https://www.aljazeera.com/features/2023/9/20/nationalist-populist-far-right-parties-eye-rising-support-across-europe)

るグループではなく重複している可能性が高い。主張は異なるものの現状を否定する点で共通しており、同じ層が活動の時期によって主張を変えている[10]。コロナ禍で反ワクチンを主張していた人々が、ウクライナ侵攻が始まった際、一斉に親ロシア、反ウクライナの主張を開始したことでもわかる[11]。中露はこれらのグループをうまく利用している。

全体像把握の必要性に関する既存の研究

デジタル影響工作への対策が対症療法に留まっているという問題はこれまでも指摘されてきた。アリシア・ワンレス(Alicia Wanless)は、全体像を見ることの重要性を繰り返し訴えてきている[12]。ワンレスによれば、選挙や紛争などメディアで注目される事例のケーススタディや実験、調査が現在の主流となっており、原因はもちろん全体像を把握することができておらず、情報の生態系をとらえるべきであるとしている。だが、全体像を明らかにする試みには資金調達や複数の専門分野にまたがるという難しさもある。それよりはロシアや 4chan などのせいにする方がはるかに簡単でわかりやすい結果を出せる。

---

[10] Aoife Gallagher, Ciarán O' Connor, Francesca Visser, "Uisce Faoi Thalamh: Summary Report," Institute for Strategic Dialogue (November 20, 2022). (https://www.isdglobal.org/isd-publications/uisce-faoi-thalamh-summary-report/);Jan Rathje, "From the Crisis to the Reich Post-Pandemic Developments of 'Reichsbürger' and Sovereignists in Germany," Center for Monitoring, Analysis and Strategy (November 5, 2023). (https://cemas.io/en/publications/from-the-crisis-to-the-reich/);一田和樹「ISD の一連の報告書は情報のエコシステムの包括的調査だった」一田和樹のメモ帳(2023 年 11 月 28 日)。(https://note.com/ichi_twnovel/n/n6c8c44b74953)

[11] Elise Thomas, "QAnon goes to China – via Russia," Institute for Strategic Dialogue (March 23, 2022). (https://www.isdglobal.org/digital_dispatches/qanon-goes-to-china-via-russia/);一田和樹『ウクライナ侵攻と情報戦』(扶桑社新書、2022 年);一田和樹「世界各地で同時発生した反ワクチンから親ロ発言への転換」一田和樹のメモ帳(2022 年 3 月 31 日)。(https://note.com/ichi_twnovel/n/nce3b3fc468a7);Mark Hay, "Pandemic and Anti-Vaxxer Conspiracy Theorists are Making the Ukraine Crisis All About Them," Daily Beast (March 22, 2022). (https://www.thedailybeast.com/pandemic-and-anti-vaxxer-conspiracy-theorists-make-ukraine-crisis-all-about-them);Laura KayaliI, Mark Scott,"Anti-vax conspiracy groups lean into pro-Kremlin propaganda in Ukraine,", POLITICO (March 17, 2022). (https://www.politico.eu/article/antivax-conspiracy-lean-pro-kremlin-propaganda-ukraine/); Josh Butler, Sarah Martin, "Australian online anti-vaccine groups switch to Putin praise and Ukraine conspiracies," The Guardian (March 1, 2022). (https://www.theguardian.com/australia-news/2022/mar/02/australias-anti-vaccine-groups-switch-focus-to-putin-praise-and-ukraine-conspiracies);Graig Graziosi, "Anti-vax conspiracy theorists in US turning to antisemitic pro-Putin propaganda, report says," The Independent (March 2, 2022). (https://www.independent.co.uk/news/world/americas/us-politics/putin-propaganda-usa-conspiracy-theorist-b2027230.html);Sheera Frenkel, Stuart A. Thompson, "How Russia and Right-Wing Americans Converged on War in Ukraine," The NewYork Times (March 23, 2022). (https://www.nytimes.com/2022/03/23/technology/russia-american-far-right-ukraine.html)

[12] Alicia Wanless, "Seeing the Disinformation Forest Through the Trees: How to Begin Cleaning Up the Polluted Information Environment," The Forum Network (November 13, 2023). (https://www.oecd-forum.org/posts/seeing-the-disinformation-forest-through-the-trees-how-to-begin-cleaning-up-the-polluted-information-environment);Alicia Wanless, "There Is No Getting Ahead of Disinformation Without Moving Past It," Lawfare (May 8, 2023). (https://www.lawfaremedia.org/article/there-is-no-getting-ahead-of-disinformation-without-moving-past-it)

リー・チアン・テー(Li Qian Tay)らは、論文「誤情報について明確に考える(原題:Thinking Clearly about Misinformation)」において、因果推論に注目して課題を整理し、デジタル影響工作の効果と対策を考えるには因果関係の把握が必要であるが、さまざまな調査研究が異なる仮説と因果モデルを提示し、異なる結論を出していると論じる[13]。テーらによると、偽・誤情報あるいは陰謀論は、格差や分極化、ポピュリズムの台頭などといった社会的な背景や制度への不信から発生しているという仮説と前提、誤情報がその原因になっているという仮説、そうした背景と誤情報が相互に影響を与え合っているという仮説もあるという。仮説が異なれば結論が異なるのは当然だ。この論文は、因果ダイアグラムを使いランダム化比較実験(Randomized Controlled Trial: RCT)を用いたデータ解析において発生する要因の見落としを指摘している。調査方法の利便性や実現性を優先した結果、生じる問題だ。そこでテーらは、実態に沿った手法、因果推論に基づいた包括的なアプローチ、認知科学の知見の活用を提言している。

デジタル影響工作への対策には因果関係の推論が必要になるが、そこにはやっかいな問題がある。ジューディア・パール(Judea Pearl)が指摘しているように、因果推論の結果は分析者が主観によって選んだ因果モデルに則ったものであり、異なる分析者が異なる因果モデルを用いれば異なる結果となることもあり、どちらも正しいのだ[14]。さらに多くの場合、包括的なモデルではない方が責任の所在がはっきりし、対処もしやすい。「科学的」に正しさが検証されているなら既存の組織と方法論を適用できる包括的ではないモデルを使いたくなる(実際ほとんどはそちらだ)。問題に対して最適な解決方法を選択するよりも、既存の組織と方法論に最適化されたアプローチで問題を定義して対処しがちになる。包括的ではないモデルからは部分最適の対策が導かれ、全体に対してマイナスの効果を与える可能性もある。

効果の低い対策がもたらす悪影響

問題をさらに複雑にしているのが、対策や報道がもたらす悪影響だ。偽情報の脅威を無差別に発信する者を警戒主義者(Alarmist)と呼ぶが、警戒主義者の発する警告によって民主主義そのものや報道に対する満足度が下がることが指摘されている[15]。このメカニズムは 2016 年にすでにロシアが使用していたパーセプション・ハッキングと呼ばれる手法に近い。パーセプション・ハッキングとは、「デジタル影響工作が行われていた」ことを知るだけで、情報やメディアに懐疑的にな

[13] Li Qian Tay, Stephan Lewandowsky, Mark J. Hurlstone, Tim Kurz, Ullrich K. H. Ecker, "Thinking clearly about misinformation," *Commun Psychol,* 2-4 (2024). (https://doi.org/10.1038/s44271-023-00054-5)

[14] 「因果的情報に含まれる主観性が、必ずしも時間とともに減衰していかない点も重要だ。たとえデータ量が増えていったとしても、主観性は減らないのである。二人の研究者がそれぞれまったく別の因果ダイアグラムを作って同じデータを解析することも可能であり、その場合はおそらく両者の得る結論は同じにならないだろう。解析するデータがどれほど大きくても同じことだ。科学は絶対に客観的なものであるべきという考えを持つ人にとって、これは恐ろしいことに違いない。」(ジューディア・パール、ダナ・マッケンジー『因果推論の科学 「なぜ?」の問いにどう答えるか [Kindle 版]』(文藝春秋、2022 年)、166 ページ)

[15] Andreas Jungherr, Adrian Rauchfleisch,"Negative Downstream Effects of Alarmist Disinformation Discourse: Evidence from the United States," *Political Behavior* (2024). (https://doi.org/10.1007/s11109-024-09911-3);一田和樹「偽情報への注意喚起や報道が民主主義を衰退させる=警戒主義者のリスク」一田和樹のメモ帳(2024 年 1 月 17 日)。(https://note.com/ichi_twnovel/n/n02d7e7230e8b)

り、不信感を抱くように仕向けることを指す。

2016 年以降、政府やメディアによる無差別な警告が続いたことが民主主義の後退を招いた一因になっている可能性がある。たとえば日本では総務省が偽情報対策に積極的だが、当然ながらその中に安全保障は含まれていないし、原則としてタイプ 3 や 4 も含まれていない。アメリカの選挙ではサイバーコムが対処に当たっているが、中心は偽情報であり、さらに自国内からの干渉は範囲外になっている。日米いずれも偽情報に焦点をあてており、それ以外の問題にはあまり触れていない。結果としてバランスを欠いた偏った警告を発信していることになり、警戒主義によるリスクを高める。対象外の問題が受け手には見えなくなり、矮小化された部分的な問題が全てであるかのように誤解されるリスクもある。

近年ではレピュテーション・マネジメント企業などの民間企業に偽情報対策を委託する政府や企業が増加しており、これらの企業は営業上の要請から偽情報の脅威をアピールしたレポートを公開したり、メディアの取材に対して脅威を語り、対策の必要性を訴えたりして悪影響を広げる。

結論

以上、見てきたように現在のデジタル影響工作対策は全体像をとらえるのが難しいため、既存の組織と方法論が適用できる範囲で問題をとらえて対処しているのであり、問題に対して最適な解決方法を選択しているわけではない。莫大なデータを解析してもその前提となる問題のとらえ方が調査研究ごとに異なっているため知見を統合できず、議論も空回りする。組織や規制が整備され、対抗策が講じられ、ファクトチェックや偽情報発信者のテイクダウンなどが行われているので成果があがっているように見えるが、実質的には改善されていない。逆効果になっている可能性もある。一方、攻撃側である中露伊および他の権威主義国のデジタル影響工作は、手法を進化させ、効果のある攻撃手法を相互に参照しており、TTPs（Tactics, Techniques, Procedures：戦術、技術、手順）が類似してきている。

欧米および日本では、効果の期待できない規制強化に向かう可能性が高い。テーらによる前掲論文では警戒主義によって規制への同意が増加することが論じられている。その際焦点が当てられる対象が偏っているため、さらに警戒主義が悪化する。また、増加する偽情報の規制にはシステム的な対処が必要となることが多いが、こうしたシステムの導入を行うと、権威主義に向かう可能性が高い。なぜならあらゆるシステムには設計時および開発時点で思想と意図が織り込まれており、そのシステムを運用することはその思想と意図に従うことを意味するからだ。イデオロギーが仕様に強く結びついていることは世界国際電気通信会議（WCIT-12）で端的に示された[16]。警戒主義者の向かう先は検閲の強化と言論の抑制である。

早期に包括的なアプローチに切り替え、全体像を把握したうえでの対策を講じることが必要とされている。

[16] 日本ネットワークインフォメーションセンター「ドメイン名を中心としたインターネットポリシーレポート 2013 年 1 月号―WCIT 2012 の結果について」（https://www.nic.ad.jp/ja/in-policy/policy-report-201301.pdf）；出口岳人「世界国際電気通信会議（WCIT-12）結果報告（総括）」『ITU ジャーナル』43（2）、2013 年。（https://www.ituaj.jp/wp-content/uploads/2013/05/WCIT12.pdf）

一田和樹プロフィール

複数の IT 企業の経営にたずさわった後、2011 年にカナダの永住権を取得しバンクーバーに移住。同時に小説家としてデビュー。リアルに起こり得るサイバー犯罪をテーマにした小説とネット世論操作に関する著作や評論を多数発表している。近年はデジタル影響工作に関する著作が多い。