INODS UNVEIL

新領域安全保障研究所 2024

新領域安全保障研究所2024

INODS UNVEIL

新領域安全保障研究所

INODS UNVEIL

新領域 安全保障研究所 2024

注目すべき動向

一田 和樹

２０２４年度は偽・誤情報、デジタル影響工作、認知戦に焦点を当てた活動を行ってまいりました。現在、この領域では見直しが始まっています。大きな方向として、個別の偽・誤情報に対応するのではなく、総合的な対策へのシフトがあげられます。具体的には、偽・誤情報の検知や削除を行うよりも信用できる情報へのアクセスの確保を優先する、海外からの干渉への対応と国内問題への対処を統合的に行うことなどがあげられます。

オペレーション・オーバーロードは世界のファクトチェック団体、メディア、研究者に、自分たちが拡散した偽情報の検証を依頼して負荷を高め、結果を発表させることでさらなる拡散を狙った（CheckFirst）

世界でもっとも研究されたロシアのドッペルゲンガーはパーセプション・ハッキングであった可能性がある（Meta）

2016年1月から2018年12月までの3年間にわたる、アメリカ人の1日のPC、モバイル、テレビのメディア消費を調査した結果、誤・偽情報摂取量はわずか0.15%だった（Jennifer Allen他）

背景には、多くの脅威がパーセプション・ハッキングを狙ったもので、各国で警戒主義が台頭していることがあります。過度の警戒主義を避けるためには、実態の把握と検証を行い、偽・誤情報、デジタル影響工作の影響は喧伝されているよりはるかに少なく、対策は逆効果になっていることを明らかにしなければなりません。

警戒主義は、分断と社会への不満を増大し、結果として分散型テロリスト＝TikTokテロリストなどの過激派の台頭を許しています。

また、これまでの攻撃の知見を生かした企業を狙ったデジタル影響工作が増加しており、日本企業も標的になっています。

我々はもぐら叩き（個別の偽・誤情報への対応）はもうしない（CISA）

Alicia Wanlessは偽・誤情報対策のフレームワークを変える必要がある、と断言し、誤・偽情報は情報環境における小さな側面であり、小さな問題にすぎないと語った

狙われているのは国内問題である以上、国内問題への対処も必要（ISD）

目次

事業紹介

新領域安全保障研究所では次の事業を行っております。

INODS UNVEIL（https://inods.co.jp）の運営

新領域安全保障研究所が運営するＷＥＢサイト INODS UNVEIL (https://inods.co.jp) はサイバー空間における新領域の脅威情報をワンストップで入手できる国内唯一の情報提供サービスです。

海外の最新情報や研究成果および国内の専門家をネットワークし、横断的な脅威情報を網羅し、企業および関係機関のリスク対策や予防を支援いたします。

ウェビナーの開催

新領域の安全保障をテーマにほぼ毎週ランチウェビナーを開催しているほか、月に1回時間の長いウェビナーを開催しています。多彩なゲストをお招きし、毎回30人から１５０人の視聴者にご愛顧いただいています。

独自研究

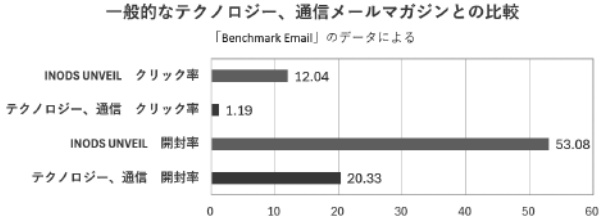
国内の第一線の研究機関あるいは研究者の方に、新領域安全保障に関わるテーマの研究を委託しており、その結果の要旨はネット上に公開し、本年鑑に収録しています。本報告書については協賛していただいた方のみご利用いただけます。

利用者の傾向について

新領域安全保障研究所をご利用なさっている方々の傾向は次ページの通りです。きわめてロイヤリティが高く、実務でこの領域に携わっていらっしゃる方々にご利用いただいています。

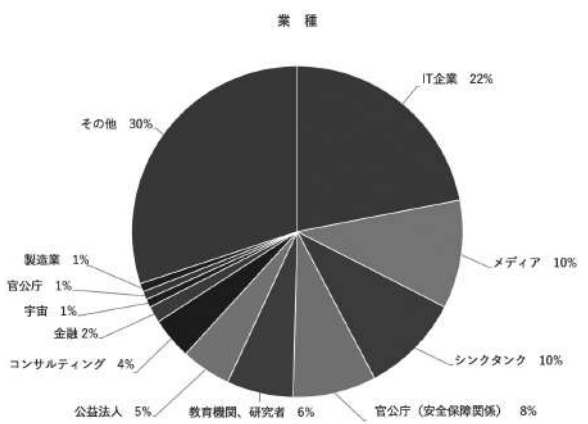
ロイヤリティの高い利用者

ほぼ毎週実施しているランチウェビナー参加者……毎回20名〜150名
ウェビナー参加登録と同時に
　他のウェビナーに登録する率……80%
　メールマガジンに登録する率……82%
WEBサイト……平日毎日更新
メールマガジン……開封率50%以上、クリック率10%以上（一般的なメールマガジンの26.5倍）



利用者の概要

IT企業、官公庁、シンクタンクなどの担当者中心にロイヤリティの高い層が集まっています。



協賛のご案内

新領域安全保障研究所では協賛を募っております。独自研究の本報告書のご利用およびINODS UNVEIL やウェビナーでのPRなどの特典がございます。くわしい内容についてはお気軽にお問合せください。

電話　03-6435-6906
メール　info@inods.co.jp

ふたつの独自研究

日本企業が直面している影響工作の脅威
SNS（X）のハッシュタグとボットの株価への影響

要旨

新領域安全保障研究所代表取締役　齋藤 孝道

中国国家安全部の関与するサイバー分野における影響工作の研究

要旨

株式会社サイント　岩井 博樹

巻頭特集

INODS

ここにご紹介するのは、株式会社新領域安全保障研究所が２０２４年に行った委託研究報告書の要旨です。
本報告書は、ご協賛いただいた企業に限定して配布いたします。
協賛については、下記もしくは電子メール（info@inods.co.jp）でお問合せください。
当研究所では定期的に独自研究を行ってゆく予定です。

お問合せフォーム
https://inods.co.jp/contact/

独自研究

日本企業が直面している影響工作の脅威

SNS(X)のハッシュタグとボットの株価への影響

新領域安全保障研究所　齋藤 孝道

要旨

近年、SNSやメディアを利用した影響工作による世論操作や偽情報の拡散が深刻な問題となっている。特に、悪意の情報拡散が企業の株価を意図的に操作する手段として利用されることが懸念されている。過去の研究では、SNSの投稿内容と株価の変動の間に有意な関連が見られ、ボットによる大量投稿がその原因の一部であることが示されている。

本研究では、「企業に対して意図的な干渉を行う脅威が存在し、その兆候は株価操作を目的としたSNS上でのボット活動などに現れている可能性がある」という仮説に基づき、下記の検証・提言を行った。

・上記結果から可能性のある影響工作主体についてのアトリビューション
・検知と対策についての提言

1．8つの事例について、SNS(X)上における株価とボット、ハッシュタグ利用の関係

その結果、SNS(X)上における株価とボット、ハッシュタグ利用には有意な関係があり、意図的に操作することが可能であることがわかった。そのような操作が行われていた場合、調査対象としたSNS(X)のみでなく、他のSNSやオフラインでの影響工作も含んだハイブリッドな作戦であり、SNS(X)はその兆候と考えられる。

特定の企業に関するSNS(X)上の炎上、8ケースに注目し、特にハッシュタグの使用状況やボットアカウントの割合、そしてそれらが株価変動にどのような影響を与えているかを分析した。

次ページの表に、対象とした8つのケースにおけるポスト数、ボットの数、ハッシュタグの状況と炎上後の株価の変化について動きの様子を示す。（本報告書では、データセットの欄は具体的な炎上を特定される情報が記載されている。）

その結果、不買運動など、特定企業を標的とした協調的な活動において、特定のハッシュタグ

を使った情報拡散や、大量のボットアカウントを利用した意図的な情報操作が確認された。調査対象のうち半数の4つのケースでは、影響工作により、企業の評判に悪影響を与え、最終的には株価にも大きな影響を与える可能性があることが示唆された。

株価操作を狙った影響工作は、週末など閲覧される可能性の高いタイミングを狙って開始され、ボットやハッシュタグを駆使して拡散が試みられる。偶発的なものを除き、炎上を人為的に起こすのにはコストが掛かるので、影響工作を行う者は利害関係者である可能性が高い。また、「ここぞ」の時に炎上を起こされる。よって、それを踏まえた事前の対策が求められる。

8つのケースでのポスト、ボット、ハッシュタグの状況と炎上後の株価

	不買運動			
データセット	A	B	C	D
ピーク時のポスト数	80,000	1,300	8,000	40,000
ボットアカウントの割合	0.351	0.349	0.381	0.26
1ポストあたりのハッシュタグ数	1.99	2.04	2.32	1.62
関係ないハッシュタグ	有	有	無	有
値下がりの時系列パターン	ポストの後	ポストの後	ポストの後	ポストの前

	不買運動		その他	
データセット	E	F	G	H
ピーク時のポスト数	800	6,000	350,000	25,000
ボットアカウントの割合	0.355	0.294	0.255	0.215
1ポストあたりのハッシュタグ数	2.93	1.06	0.52	0.22
関係ないハッシュタグ	無	–	–	–
値下がりの時系列パターン	ポストの後	–	ポストの前	ポストと同時

※「ピーク時のポスト数」の数値はおおよその値です。

2. 影響工作主体のアトリビューション

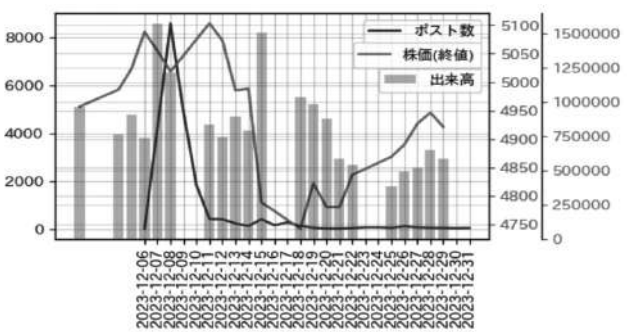
SNSの操作には多大なコストと知見が必要である。そのため、影響工作の主体は、株価の変動から利益を得ることができ、影響工作の知識を持って計画的に実行できる(もしくはその能力を持った組織に委託できる)ものと推定される。

これらの条件を満たす主体には、たとえば下記が挙げられる。あくまで一例であり、他にも可能性のあるアクターが存在する。

- **外資系ファンド**　日本国内には影響工作を実施するための知見を持ち、巨額の資金を動かせる主体は限られるが、海外にはそうした主体が日本よりも多く影響工作の委託先も多数存在する。

影響工作が観測されたケースの例

以下の図は、食品のCMに起用したタレントに関連する炎上の際の株の値動きを示す。閲覧者が増える週末に一気に関連投稿が増え炎上した。翌週、ネガティヴなマインドが株価下落に影響を与えた可能性がある。



多くの大手日本企業はすでにSNSリスニングなどのサービスを導入しているものの、総合的な影響工作には脆弱であり、ネット以外のメディアの利用、経営者への個人攻撃など多彩な方法を駆使された場合、対処できない場合も多い。

・我が国に干渉する敵対国　我が国に干渉する敵対国は複数存在し、それらの国の影響工作の能力は我が国より高く、必要があれば充分な資金を投入できる。わが国の特定の企業や産業にダメージを与える。国際的なレピュテーションを下げるなどの目的のためにこうした影響工作を行う可能性が考えられる。

ただし、経営にダメージを与えたり、レピュテーションを下げたりすることは当然ながら多くの注目をあつめるため、日本政府やメディアなどによる調査が行われ、アトリビューションが特定されるリスクが高い。あらかじめ主体が特定されることを想定したうえで攻撃してくるのは、たとえば台湾併合にそなえてゆさぶりをかける場合や、日本のウクライナ支援にゆさぶりをかけるような場合が考えられる。KADOKAWAへのサイバー攻撃がロシアからのシグナリングという可能性と同様である。

3. 検知と対策

検知と対策には、定常的な早期警戒システム、リスクマネジメントチームが必要であり、社外の専門機関との連携も不可欠となる。

早期警戒システムには、前項に書いた外資系ファンドや敵対国などの動向を常時把握しておくことも含まれる。いわゆるインテリジェンスに類する情報収集と分析が必要になってくる。

本調査研究は、株式会社新領域安全保障研究所から資金提供を受けて行ったものである。

新領域安全保障研究所　代表取締役
明治大学理工学部情報科学科　教授、博士(工学)
明治大学サイバーセキュリティ研究所　所長
レンジフォース株式会社　代表取締役
齋藤孝道

独自研究

中国国家安全部の関与するサイバー分野における影響工作の研究

株式会社サイント　岩井 博樹

要旨

本研究では、中国の国家安全部（ＭＳＳ）が関与するサイバー領域における影響工作について調査した。ＭＳＳは対外諜報活動や政治的安全保障に関わる業務で知られているが、以前から政治家などエリート層への影響工作にも従事していることが確認されている。近年では、公安部（ＭＰＳ）と連携し、デジタルプラットフォームやソーシャルメディアを利用した情報操作が活発化している可能性がある。その手法の進化はＩＴ技術の発展とともに加速しており、特に偽情報の拡散や影響力のあるＳＮＳアカウントの乗っ取りが新たな戦略として採用されている。

情報配信プラットフォームを利用した影響工作

１つ目の調査では、情報配信プラットフォームを利用した影響工作について紹介する。韓国ＮＣＳＣやトロント大学のCitizen Labが報告したＰＲ企業を利用した影響工作キャンペーンと類似性のある、未認知のメディア配信企業を通じた影響工作キャンペーンを発見し、調査分析を行なった。

その結果、これらのメディア配信プラットフォームはテンプレート化されたウェブサイトを用いることで、大量のコンテンツが生成されていた。また、日本語のコンテンツには生成ＡＩを利用した偽情報を含む記事が確認され、元首相・鳩山由紀夫氏を題材にするなど実験的な要素も見受けられた。

この調査では、安全保障分野の１つであるサイバーセキュリティ分野にも言及している。中国共産党（ＣＣＰ）に近いインテリジェンス企業は、意図的に中国に有利な脅威情報を積極的に配信することで、西側諸国の脅威データベースに偽情報を組み込むことに成功している。

これは、ＡＩが一般に普及しつつある現代において、データ学習が阻害されることを意味しており、新たな脅威となり得る。

中国国内において発生している反体制派のソーシャルメディアアカウントの乗っ取りによる影響工作

2つ目の調査では、中国国内において発生している反体制派のソーシャルメディアアカウントの乗っ取りによる影響工作について調査を行なった。題材として、今年5月頃に話題となっていた中国・反体制派のX（旧Twitter）アカウント「李老师不是你老师」の乗っ取りを目的としたサイバー攻撃を取り上げる。

李老师不是你老师は、彼を支援する反体制派らが、中国国内の状況を撮影した写真や動画を海外からXへ投稿していたことで知られる。この活動内容を鑑みると、公安部（MPS）が関与している可能性が想起されるが、サイバー領域においてMSSとMPSが協力関係にあることや、標的ユーザーが海外在住であることを踏まえると、MSSの関与が疑われる事例である。

また、この攻撃に悪用された悪性コードを分析したところ、今年2月に情報流出によりMSSやMPSの請負事業者であることが明らかになった安洵信息（I-SOON）の開発したツールが使用されていた可能性が示唆されている。

これまでも親中派インフルエンサーを利用して中国に有利な情報を発信する手法はたびたび見られていたが、今回の事例では反体制派の象徴的なアカウントを乗っ取り、標的ユーザーの中国国内の支援者を摘発すると共に、世論操作を行うことが目的であったと推察される。

MSSが仕掛けるサイバー空間における影響工作は、その影響力を拡大し続けている。これらの脅威はサイバーセキュリティ上の重大な問題であり、国家として取り組むべき課題だ。今後、MSSおよびMPSによる影響工作はさらに高度化することが予想されており、我が国はこれに対し、抜本的な対策を講じる必要がある。

本調査研究は、株式会社新領域安全保障研究所から資金提供を受けて行ったものである。

株式会社サイント
経済産業省情報セキュリティ対策専門官
千葉県警察サイバーセキュリティ対策テクニカルアドバイザー
情報セキュリティ大学院大学客員研究員
岩井博樹

独自研究
中国国家安全部の関与するサイバー分野における影響工作の研究
目次

安全保障の新たなフロンティア
デジタル影響工作を読み解く

齋藤 孝道

ハイブリッド脅威

現代の安全保障において、サイバー脅威はますます複雑化しており、領域横断的な「ハイブリッド脅威」の一部として注目されている。ハイブリッド脅威の一例として、２０１４年のクリミア併合におけるロシアが行った「ハイブリッド戦」が知られている。ロシアは軍事的な進攻に加えて、サイバー攻撃や情報戦を駆使して、国際社会の反応を操作したとされている。

しかしながら、「ハイブリッド脅威」とは、軍事的な攻撃とサイバー攻撃だけでなく、情報操作、経済的圧力、政治的な影響力行使など、多岐にわたる手段を用いてターゲットの安定を揺るがすより広範な脅威概念である。欧州ＮＡＴＯハイブリッドＣＯＥ（※1）では、ハイブリッド脅威について図１に示すような概念モデルを提唱している。軍事、サイバー攻撃や情報戦に加えて、外交、政治、文化、社会、法律、宇宙、行政、インフラ、経済、諜報などといったより多くの領域に跨ぎ、それらを複合的に駆使して、ターゲットの優位性を貶める。

ハイブリッド脅威の観点から見れば、現在我々が目にしているさまざまな脅威は、より大きな枠組みにおいて形成される脅威の顕在化している一つのもしくは一部に過ぎない。

図1 ハイブリッド脅威の概念図
（出典：文献(1)を著者が翻訳）

脅威アクターは、ターゲットに対し、図１に示した、複数のドメインを跨ぐ形で「干渉」（interference）を行う。しかしながら、脅威を脅威と認識させない。それゆえ、ターゲットは状況認識の共有が困難となり、対抗措置がとれない。さらには、ターゲットは、脅威アクターにとって有利な意思決定を誘発されてしまう。

デジタル影響工作の事例とその考え方

次に、ハイブリッド脅威の一つ、デジタル影響工作の考え方を整理する。ここでは、影響工作を、「国家・非国家間での競争(戦い)における情報戦の一種で、競争相手国の意思決定に影響を与え、ターゲットの行動の変容を促す一連の行為」とする。その上で、SNS、AI、および、アドテクを戦術的手段として用いる影響工作を、デジタル影響工作とする。

デジタル影響工作において、SNS、AI、および、アドテクの役割は大きい。SNSは、アテンションエコノミー(※2)に基づくので、SNSプラットフォームには、情報の拡散力にだけでなく、利用者の注意を惹きつける仕組みがビルトインされている。このことが、それまでのメディア、すなわち、新聞、ラジオ、映画、テレビとの違いである。また、アドテクの代表には、マイクロターゲッティング広告(※3)がある。マイクロターゲッティング広告は、高い宣伝効果を持つだけでなく、ターゲット以外に顕在化することがないステルス性を持つ。さらに、昨今の生成AIの台頭により、さまざま偽コンテンツの生成の増加が想定される。それ以上に注目すべきAI技術として、ターゲットの心理モデルの悪用である。AIによる心理モデルにより、マニュピュレート、すなわち、ターゲットの行動変容を促すことを可能とする。

行動変容手法：反射統制

つぎに、反射統制(Reflexive Control)という概念を用いて、ターゲットの行動変容を促す方法について説明する。反射統制とは、1960年代、旧ソビエト連邦でスタートした、影響工作の理論である。ターゲットが特定の状況をどのように評価し、どのような行動を取るかを予測し、その行動を自分に有利な方向に導くための情報操作である。具体的には、敵の認識や意思決定に影響を与えるために、虚偽の情報や心理的な操作を用いる(図2参照)。

たとえば、ルビンの壺。これは、一つの画像を異なる視点から見ることで、異なる認識を引き出すことができる例として知られている。ルビンの壺の画像は、「二つの人の顔」と「壺」の両方の解釈が可能であり、視点を変えることでその認識も変わる。すなわち、影響工作では、このような人間の気質を利用してターゲットの「認識を変えさせること」で、意思決定や判断にも影響を与え、最終的には行動変容を促す力を生み出す。

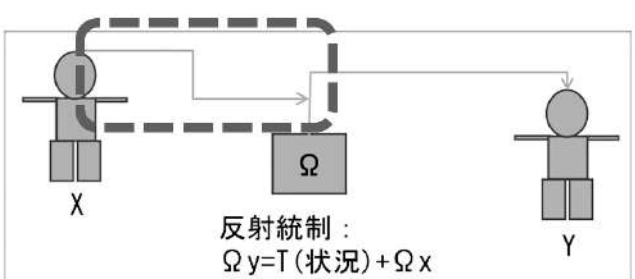


図2 反射統制の概念(出典：文献(2)を著者が一部改変)

このように、影響工作では、偽情報・誤情報を提供するだけでなく、「考え方を変えさせる情報」を提供することにより、ターゲットの行動変容を促す。

「核の冬」は、ナラティブ!?

影響工作では、ナラティブを用いて世論や政策決定に影響を与えることがある。ここで、ナラティブは、必ずしも現実に即しているわけではなく、政治的な意図を含み、「考え方を変えさせる情報」を提供する手段の一つである。つぎに、ナラティブを用いた影響工作の例を紹介する。

１９８３年ごろ、学校の廊下には、「核の冬」のポスターが貼られていた。「核の冬」とは、核爆発によってチリが舞い上がり、太陽光を遮って、地球規模の気候変動を引き起こし、深刻な食糧不足や生態系の崩壊をもたらすとの言説である。当時、ソ連の軍事力の優位性に対抗するため、欧州は米国製の核兵器を持ち込むという計画が持ち上がった。ソ連は、この軍事力増強の動きを阻止するために「核の冬」の恐怖を利用した。実際、ＫＧＢの将校が暴露したところによれば、ソ連はＮＡＴＯが欧州に核ミサイルを配備する計画に対抗して、「核の冬」という概念をナラティブ(※4)として広めたのである。ソ連は「核の冬」の恐ろしさを強調し、特に欧州の人々に核軍縮の必要性を訴えた。その結果、「核の冬」に怯えた市民が「反戦」を訴え、ＮＡＴＯの軍事力拡大が妨害された。これにより、ソ連は軍事的優位性を保つことに繋がったのである。

日本の歴史問題もまた、ナラティブとして利用されることが多い。日本と近隣諸国との間で歴史認識の違いのあるナラティブを巧みに利用して、外交関係に影響を与えることは知られている。クリティカルシンキングの教育が系統立てて行われていない日本では、特定グループのナラティブを用いた影響工作に対して、耐性が低い。実際、海外からの商業的なプロモーションに簡単にのせられてしまうことは関係者には知られている。

選挙ハッキング、選挙セキュリティ

影響工作による民意の誘導は、民主主義の基盤を揺るがす可能性がある。特に、選挙という社会的意思決定プロセスへの干渉は最大の脅威であり、民主主義の核心を直接揺さぶるものである。選挙結果の正当性への疑念が広がると、国民の間に深刻な不信感が生じ、政治システム全体への信頼が揺らぐ。

このような背景から、米国のインテリジェンスコミュニティでは、選挙セキュリティ対策が重要視されている(図3参照)。選挙に対する攻撃は、国家の政治プロセスに対する信頼を損ない、市民の意思決定を歪めるリスクがあるため、その防止は緊急かつ重要な課題とされている。

２０１６年の米国大統領選挙におけるロシアの介入は、デジタル影響工作を用いた選挙セキュリティの典型的な事例である。ロシアは、ＳＮＳを通じて偽情報・誤情報や悪意の暴露情報を拡散し、選挙結果に影響を与えようと試みた。米国の国際法の専門家であるマイケル・シュミット氏によれば、議論の余地はあるとの前置きがあるものの、「有権者が自分自身の判断に基づいてメッセージを評価する能力を操作されることは、選挙の結果に影響を与えた可能性があり、したがって違法な干渉を構成するものである」と指摘している(4)。

この種の試みは、選挙プロセスの信頼性を低下させ、社会の分断を促進することを目的としていた。これにより、米国社会に深刻な影響を及ぼし、選挙セキュリティ対策の重要性が認識される契機となった。

「米国選挙に対する外国の影響と干渉は、我が国の民主主義に重大な脅威をもたらす。情報機関コミュニティ（IC）は、外国の影響と干渉から我々の民主主義のプロセスと制度を保護することに尽力している。選挙セキュリティは永続的な課題であり、ICにとって最優先事項である」

図3　インテリジェンスコミュニティによる選挙セキュリティの宣言
（出典：文献(3)を抄訳）

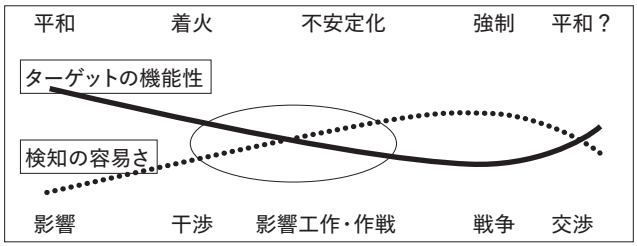


図4 ハイブリッド脅威の概念図（出典：文献(1)を著者が一部改変）

求められる「顕在化しない脅威」への対処能力

現代の安全保障環境において、デジタル影響工作などハイブリッド脅威への対処は重要性を増している。しかしながら、ミサイルドンパチ系の軍事的脅威とは違い、ハイブリッド脅威は、その脅威が顕在化する前に、ターゲットへダメージを与える。

再度、文献(1)にある概念を用いて、ハイブリッド脅威におけるダメージの高まりとその顕在化までの関係を用いて説明する（図4参照）。

ハイブリッド脅威では、「着火（※5）」や「不安定化」といったフェーズが進むにつれて、干渉や影響工作が徐々に強化されていく。しかし、脅威が顕在化（点線）する前に、ターゲットの機能性（実線）が徐々に低下してしまう。この現象は、古来の諺にある「茹でガエル」のようにゆっくりと進行する「サイレントインベージョン（沈黙の侵略）」であるため気づきにくいものである。また、この種の脅威の議論は、陰謀論と見做されてしまうことがあり、対抗のコンセンサスを獲得

することが難しい。しかしながら、豪州では、サイレントインベージョンへの対抗を実施した。

安全保障の観点から、今後、このような「顕在化しない脅威」に対する感度を高め、その対処を始めることが求められる。早期に対応策を講じることで、国家の機能低下を防ぎ、ハイブリッド脅威からのダメージを最小限に抑えることができる。具体的には、情報収集と分析を強化し、潜在的な脅威を早期に察知することが重要である。また、社会全体での防御意識を高め、脅威に対する迅速な対応が可能な体制を整えることが求められる。

2024年6月30日配信

参考

(1) European Commission, & Hybrid CoE, The Landscape of Hybrid Threats: A Conceptual Model Public Version, 2021

(2) ロシアの情報兵器としての反射統制の理論、２０２２、五月書房新社

(3) https://www.dni.gov/index.php/who-we-are/organizations/mission-integration/es/election-security-who-we-are

(4) Michael Schmitt, "'Virtual' Disenfranchisement": Cyber Election Meddling in the Grey Zones of International Law," Chicago Journal of International Law, Vol. 19, 2018

※1 欧州Hybrid CoE（ハイブリッド脅威対策センター：Center of Excellence for Countering Hybrid Threats）は、ハイブリッド脅威に対する対策を研究・実施するための組織であり、フィンランドに拠点を置く。

※2 アテンションエコノミーとは、ユーザーの注意時間を収益化するビジネスモデルである。広告収入を増やすため、ユーザーをより長くアプリやサイトに留めることを目的とする。

※3 マイクロターゲッティング広告とは、個人の行動データや興味に基づいて、特定のユーザー層に対して最適な広告を配信する手法である。これにより、広告の効果を高め、より高いコンバージョン率を実現する。

※4 「核の冬」への恐怖感は、ソ連が生み出したものではなく、当時、市民が誰でも潜在的に持っていたものであり、それを、ナラティブとして悪用した。

※5 ターゲットの活動を混乱させて不安定化に向けた、干渉や影響工作を実施する行為。たとえば、文化や価値観の議論となる争点を投入し炎上を煽る世論分断工作などがある。

陰謀論に特効薬はないという論文

INODS UNVEIL ニュース担当

「クリスマスのディナータイムを台無しにすることなく、『トカゲ人間の陰謀論者になった親戚』と会話する方法」

夏休みに久々の帰省をしたら両親や親戚が、あるいは親しかった友人が、すっかり陰謀論者になっていたという経験を持つ人は少なくないだろう。それは世界中の「あるある」エピソードとなっている。英語圏では冬になると「クリスマスのディナータイムを台無しにすることなく、『トカゲ人間の陰謀論者になった親戚』と会話する方法」などといったタイトルの記事も増える。

また昨今では「どのようなタイプの人が陰謀論に陥りやすいのか」「人が陰謀論を信じてしまう生活的な要因にはどのようなものがあるのか」といった内容の研究論文が発表される機会も多い。そして「あなたの大切な人を陰謀論の世界から連れ戻す方法」についても、様々な見解やアイディアが語られてきた。しかし本当に効果的で実戦的でお手軽な対処法が実在していたら、世界は現在のような状況にはなっていなかっただろう。

今回は、米国で最も古い科学雑誌のひとつ「Scientific American」のオンライン版に掲載されたStephanie Pappas氏の記事を紹介したい。少々古い記事だが（2023年4月掲載）、いくつかの具体的な指摘や注意点が示されている。それは陰謀論によって引き起こされるお盆シーズンの家庭崩壊、あるいは友情の終焉を防ぐためのヒントになるかもしれない。

特効薬はない

残念ながら、この記事は冒頭から「陰謀論の落とし穴に落ちた人を、そこから救い出すための有効な方法は（現在のところ）ほとんどない」という見解を示しており、その根拠としてアイルランドのコーク大学Cian O'Mahony氏が発表した新しい研究結果を紹介している。

Mahony氏の研究チームは、過去に発表された様々な「陰謀論に関する研究論文」を見なおし研究したうえで、「陰謀論に対抗するための一般的な戦略はいずれも、ほとんど人の信念を変える

ことができない」という結論を導き出した。

最も効果のない手法

たとえば「プライミング（目的とは直接的に関係のない特定の刺激や情報を利用して、人の考え方を変えようとする）」と呼ばれる介入法がある。わざと読みづらいフォントで文章を読ませ、「文章の内容を理解するための労力」を増やすことにより、分析的な思考を相手に促すなどの手法だ。それらは有効だったものの、少しの効果しか得られないことが示された。

事実のみを根拠として陰謀論に反論する戦略も、わずかな効果しかないことが確認された。ちなみに、陰謀論の信奉者と議論をするうえで最も効果がなかったのは「相手の共感性に訴えかける」もの、そして「相手の信奉を嘲笑する」ものだったという。

自分にとって大切な誰かが陰謀論に陥ったとき、多くの人は、相手の語っている陰謀論の誤りを事実ベースで指摘し、荒唐無稽さを笑い、さらに「あなたがこの陰謀論を信じると、こんな悪影響が出てしまう」「私はあなたを心配している」と感情に訴えながら説得しようとするだろう。彼らの研究によれば、まさしくそれらは徒労に帰す可能性が高い。

有効な「予防」

彼らのチームが有効だと評価したのは、陰謀論の予防に関する研究だった。つまり事前に「あなたは（近い将来）このような内容の陰謀論を耳にする可能性がありますよ」と警告し、その陰謀論への反論を示しておく手法だ。それは中等度〜高度に陰謀論への信奉を低下させる効果があることが分かった。事後の対応に勤しむよりも「予防」に注力するほうが望ましい、ということになる。

予防の問題点

しかし、この手法は裏目に出る可能性も指摘されている。陰謀説を流布する側が、その特定的な予防プランに警戒して「予防への予防」を取り入れた場合には効果がなくなってしまう。ややこしいので、ここでは陰謀論を単純なデマに置き換えて説明したい。

たとえば「今年の八月、日本中の店からトイレットペーパーが消える、いますぐ買い占めろ」というデマが発生したとする。そのデマを自分の両親が聞いてしまう前に「最近、トイレットペーパーがなくなるというデマが流れているよ」と注意を促し、それが間違いだと分かる根拠（たとえば現在の紙生産が安定している事実を示した数字など）を教えておくことは有効だ。家族や友人

だけでなく、メディアもデマの拡散防止に貢献することができるだろう。

しかしデマを流す側が、その介入を特定的に認識し、警戒した場合は厄介なことになる。「きっとあなたは近い将来、このグラフを提示され、現在の紙生産は安定していると説明され、『トイレットペーパーが市場から消えることは有り得ない』という嘘の主張を聞かされるでしょう。これは捏造されたデータです。市民を騙すことで利益を得る人たちが、このインチキなグラフを拡散しています」などといったフレーズを追加してデマを流すようになる。これにより、予防的な介入方法は一気に効力を失う。むしろかえって逆効果になってしまう可能性もあるだろう。

地道な努力

結局、彼らが「最も効果が高い」と分析したのは、科学と疑似科学を見分けるために行なわれた教育だった。具体的には、大学で3人の講師が3ヵ月間に渡り「人間の認識や論理における誤りを理解できるようにするための、批判的思考のスキル」を学生に教えたというものだ。つまり専門家による適切な教育が、最大の護身術だった。

それは新しい特効薬や銀の弾丸ではない。労力と時間が大きく費やされる地味な手段だ。まるで「健康を保つには、バランスの良い食事と適度の運動、そして規則正しい睡眠が重要です」と説かれるような、あまり楽しくない結論だと感じる向きもあるだろう。

しかし教育を通して思考力を鍛える訓練は、特定の陰謀論だけを払拭するものではない。どんな陰謀論にも陥りにくい人間を作る堅実な対策で、万能薬のような効果が得られるだろう。長期的に考えるなら、確実な成果に期待できる唯一の対策と言えるのかもしれない。年老いた自分の両親に対し、それを実践できるのかどうかは別として。

2024年7月18日配信

ロシアのサイバー攻撃を通したシグナリング
KADOKAWA事件の「B面」

齋藤 孝道

はじめに

2024年6月、KADOKAWAへのサイバー攻撃があった。同社が多岐にわたる事業を展開する著名な企業であることと、その被害の大きさからサイバーセキュリティ業界の話題を独占した。特に、子会社のドワンゴが運営する「ニコニコ動画」が停止し、社内業務にも大きな影響が出たことが注目された。報道によれば、攻撃はランサムウェアを用いたもので、BlackSuitと名乗るハッカーグループが1.5テラバイトのデータを盗んだとされる。

しかし、話題のほとんどは攻撃手法や被害に関するものであり、その意図についての分析は少ないのが現状である。本稿では、KADOKAWAへのサイバー攻撃アクターの意図を読み解くことを試みる。

日本政府の制裁に対するロシアの反応

KADOKAWAへのサイバー攻撃の議論に先立ち、2022年のロシアのウクライナ侵攻からの関連出来事を、時系列で振り返る。

2022年2月24日、ロシアはウクライナへの侵攻を開始した。この侵攻は、2014年のクリミア侵攻以降、ロシアとウクライナの対立が次の段階に入った瞬間であった。これに対し、国際社会は迅速に反応し、日本政府も2月25日にロシアに対する最初の制裁措置を講じた。日本の制裁措置は、ロシアの金融機関やエネルギー産業に対する経済制裁を中心としたもので、国際的な協調の一環として行われた(※1)。

こうした緊張の中、2月26日には日本国内の小島プレス工

業がサイバー攻撃を受けた(※2)。この攻撃は、高度な手法を用いたもので、その背後にはロシアの関与が疑われた。小島プレス工業は自動車部品の製造で知られ、日本の産業基盤の一角を担う企業であり、この攻撃は日本の経済に対する直接的な脅威として認識された。5月、ロシア政府は日本の個人制裁に関連し、岸田総理大臣や林外務大臣を含む63人の日本国民のロシアへの入国を無期限で禁止することを発表した(※3)。

2023年5月、BlackSuitの活動が観測され始めた(※4)。このグループは、ロシアの支援を受けていると見られている。BlackSuitは、日本の企業や政府機関に対するサイバー攻撃を強化し、日本の情報インフラに対する脅威として浮上した。さらに、この時期に、イランやBRICS諸国の公的メディアの連携が推察される情報発信の増加がHamilton 2.0 Dashboardで確認され、ロシアの情報戦のフェーズが変化し、国際的なプロパガンダ活動の活発化が示唆された。

2024年1月、ロシアの影響を受けたとされるデモが欧州で激化し、国際的な情勢はさらに緊迫した。これらのデモは、著者が現地の関係者に聞いたところ、ロシアが欧州の政治的不安定を助長するために工作活動を実施している可能性があるとのことである。2月にはBlackSuitがアメリカの非営利団体「Campaign for Tobacco-Free Kids」に対するサイバー攻撃を実行し、その活動が活性化していることが示された。

2024年6月13日から開催された先進7か国(G7)首脳会議にて、岸田首相は新たな経済制裁の実施を発表した(※5)。この制裁には、ウクライナ侵略を巡り初めて中国国内の企業を対象とするものが含まれており、日本政府の姿勢が一段と強硬になったことを示している。

その経済制裁に先立ち、6月8日未明に、KADOKAWAへのサイバー攻撃が発生したとされている(※6)。なお、同時期の6月19日には、全米の自動車ディーラーにサービスを提供するCDKグローバルが、BlackSuitによるランサムウェア攻撃を受けた(※7)。これにより、CDKグローバルのサービスが停止し、大きな被害を及ぼされた(※8)。

シグナリングの効果と戦略的コミュニケーション

ここで、ロシアによる我が国へのサイバー攻撃について、文献(1)に基づき、シグナリングの観点で分析する。

ロシアのウクライナ侵攻以降、KADOKAWAへのサイバー攻撃までの系譜

シグナリングの効果は、それがどのように受け入れられるかどうかにかかっている。例えば、1948年のベルリン封鎖の際、アメリカがB29を英国に派遣することでソ連に「真剣さ」を伝えたように、シグナリングが成功するためには、他の誰もがそのシグナルを理解される必要があるとされる。国家が自国の艦隊をトラブルスポットに派遣することが効果的なシグナルであるのも、対象国家・非国家がその行動をシグナリングとして受け取る確信があるからである。

しかし、サイバー空間では、シグナリングへのコンセンサスはほとんどないとされる。DDoS攻撃などのサイバー攻撃は、実際の効果よりもシグナリングとして解釈される方が適しているかもしれないが、根拠がない限り、そのシグナルが適切に受け取られるという確信を持つことは難しい。このため、サイバー空間におけるシグナリングの信頼性は低く、その有効性も限られているとされている。

しかしながら、シグナリングは、一般に、敵国や同盟国に対するメッセージを明確に伝える手段として機能するとされる。高度な情報戦を仕掛けられているという認識の下で行われる場合、国際社会における力のバランスを保つために有効である。

BlackSuitによるKADOKAWAに対するサイバー攻撃は、ロシアからのシグナリングとして、再び示されたといえる。この一連の出来事は、ロシアが日本に対して断続的に圧力をかけ続け、

シグナリングとは

シグナリング（signaling）とは、国家や軍事組織が他国や組織に対して特定の意図や能力を伝えるために行う行動やメッセージを指す。これは、直接的な軍事行動を伴わずに戦略的なメッセージを伝える手段として存在する。シグナリングは一般的にリーダー向けのものであり、ナラティブは一般大衆向けのものである点が特徴である(1)。

正確には、戦略的レベルと作戦・戦術レベルでは違いがあるが、以下、筆者の認識に基づきその目的と例を示す。

シグナリングの目的

抑止（Deterrence）：敵対国や潜在的な敵に対して、自国の軍事力や決意を示し、攻撃を思いとどまらせる。

威嚇（Coercion）：特定の行動を取ることによって、相手に圧力をかけたり、特定の行動を取らせないようにする。

安心感の提供（Reassurance）：同盟国や友好国に対して、自国の支援や防衛の意志を示すことで安心感を与える。

交渉の強化（Bargaining Power）：交渉の場で有利な立場を得るために軍事力を誇示する。

シグナリングの例

軍事演習：軍事演習を行うことで、軍事力の準備状況や能力を示す。

兵器の配備：新型兵器の配備や既存兵器の移動を公表することで、軍事力の強化を示す。

軍事同盟の強化：同盟国との共同軍事演習や協定の締結を通じて、連携の強さを示す。

公開声明：政府や軍の高官が特定の軍事行動や政策について公に発言することで、意図や立場を明確にする。

報復：軍事作戦、テロリズムの実行は自分たちが犠牲になるということを示す。

シグナリングを通じてその意図を示している。ロシアのシグナリングは、日本に対する警告や威嚇としてだけでなく、国際社会に対する影響力を誇示している。「シグナリングはエスカレーション管理にも不可欠である」(2)とあるように、ロシアが戦略的環境をどのように形成しようとしているかが推察される。

ハイブリッド脅威時代の国家安全保障

岸田政権がロシアに経済制裁を実施するたびに、ロシアからのサイバー報復攻撃が行われるという構図が観察された。これは、ロシアのシグナリングに対して適切に対応できるかどうかが問われている状況である。

たしかに、「サイバー空間はノイズが多いため、核兵器問題では容易に理解できるシグナルも、微妙なシグナル(と思われるもの)は、新しいメディアではほとんど解読できないかもしれない」(1)とされている。しかし、外交政策が民間企業に被害をもたらしているにもかかわらず、その認識の欠如があるとすれば、政府の課題が浮き彫りになっているのではないだろうか。サイバー攻撃を通したシグナリングは未だ確立した手段とは言えないが、デジタル影響工作における戦術的手法であり、今後、そのシグナリングの意図を読み解く力、その対応力が日本にも求められていくのであろう。本稿で取り上げたロシアの即応性の高いシグナリングは「能力の誇示」(3)である。その見落としや誤解は、エスカレーションを誘発し、ロシアはレッドラインを徐々に押し上げていくだろう(※9)。

ハイブリッド脅威時代においては、複数の分野にまたがる複合的な視点が必要であり、断片的な知識や対応では不十分である。国家の安全を確保するためには、より広範で統合的なアプローチが求められるのである。

2024年8月2日配信

参考

(1) Martin C. Libicki, Cyberspace in Peace and War, Naval Institute Press, 2021.

(2) The Cyberspace Solarium Commission report, 2020, https://www.solarium.gov/report

(3) Kyle Haynes, "SIGNALING RESOLVE OR CAPABILITY? THE DIFFERENCE MATTERS ON THE KOREAN PENINSULA", 2017. https://warontherocks.com/2017/05/signaling-resolve-or-capability-the-difference-matters-on-the-korean-peninsula/

※1 https://www.mofa.go.jp/mofaj/gaiko/bluebook/2023/pdf/pdfs/1_3.pdf p.16.

※2 https://jp.reuters.com/article/idUST9N2UW01X/

※3　https://www.mofa.go.jp/policy/other/bluebook/2023/pdf/pdfs/2023_all.pdf　p.152
※4　https://www.trendmicro.com/ja_jp/jp-security/24/g/expertview-20240716-01.html
※5　https://www.mofa.go.jp/ecm/ec/pageite_000001_00395.html
※6　https://tp.kadokawa.co.jp/.assets/240614-2_release_B3q7k4.pdf
※7　https://www.reuters.com/technology/cybersecurity/why-hack-cdk-global-is-casting-shadow-us-auto-sales-2024-07-01/
※8　7月8日付日本経済新聞によれば、被害のあった6月にはGMら顧客の売り上げが5〜6%減、3週間で1500億円の被害とされている。
※9　このくだりは、一田和樹氏との議論による。

共感格差

データをいろいろ見てみる

国内問題である社会による共感の格差は、安全保障上の問題になりうる。
私は、2022年9月に共感格差というタイトルのブログ記事を書いた。その内容を要約する。

共感格差とは

共感格差というブログ記事の内容を箇条書きにすると以下のようになる。

- （社会的）共感は政治的・社会的リソースである。

●物理的資産がリソースであるのと同様だ。
●共感はアイデンティティごとに分配される（女性黒人ＬＧＢＴ、労働者階級、白人子供etc）。
●共感は物理的資産と同じく分配に差がある。
●共感の分配は主にマスメディアによってなされる。
●トランプ大統領が当選する以前、労働者階級に関するメディアのツイートは60件、同性愛ＬＧＢＴに関するツイートは、９６６４件であった。
ツイートの比率は、労働者階級60対ＬＧＢＴ９６６４で１６１倍だ。
ツイートの差を共感の差だとみなせば、労働者階級とＬＧＢＴで大きな格差がある。
●共感の格差を放置すれば、そこはポピュリストにつけこまれる。
●もしあなたがポピュリストになりたければ、次のターゲットを狙うと良い。
ある程度人口ボリュームがある。
実際に困難の中にいる。
マスメディアは彼らの困難や存在を無視する（他のマイノリティグループの困難は盛んに取り上げているのに）。
●これらの人をターゲットにすれば、少ない労力で多くの支持を得られる。

もう少し長く要約すると以下のようになる。

共感は、政治的社会的リソースである。共感を与えられないものにはなかなか寄付も、政治的な支援も得られない。例えば、絶滅しそうな動物種（レッドリスト）でも共感を得られる哺乳類と共感を得られない虫や爬虫類の間で寄付額に差がある。人間でも共感の分配に差がある。紛争地域でも少女からのtweetには関心や共感が集まる。

トランプが大統領になれたのは白人労働者を味方につけたからだとよく言われる。アメリカの主要メディアのtweetを調べた所、労働者階級やブルーカラーに関するtweetが他のマイノリティグループに比べて極端に少なかった。白人に関しては白人に寄り添うよりは、白人特権を糾弾するツイートのほうが多かった。つまり、メディア（社会）は白人労働者に共感を寄せなかった。

トランプは、その共感を寄せられないと感じている人々の絶望を利用することで大統領になったのではないか？　ポピュリストの振る舞いを見ると、多くの政治家に票田とみなされていない「忘れられた人々」をターゲットにしているように見える。忘れられた人々を放置すればポピュリストの伸張を許すことになるだろう。

というものだ。

共感はメディアによって不平等に分配される。

社会の共感がどの属性に向けられているか？　直接調査することは難しい。しかし、マスメディアがどの属性の人たちの問題を、「問題として取り上げ報じる」かは調査することができる。私は、アメリカの大手マスメディアのツイートを調査してどの属性の問題を取り上げているかを調査した。

私は、アメリカの大手マスメディアのSNSアカウント（日頃は自社のニュースをツイートしている）が2010年から2015年の間に、どの属性に言及したツイートが何件あるかをカウントした。

対象の大手メディアは、ワシントン・ポスト、ニューヨークタイムス、フォックス・ニュース、ハフポスト、WSJ、USA Today、ABC news、CBS news、NBC news、CNNの10媒体だ。それぞれのフォロワー数は、最大5000万フォロワー。最小でも400万フォロワーを超える。10メディアの平均のフォロワー数は2106万だ。

右記の10メディアがツイートした属性の数を調査した結果、下表のようになった。

最小の労働者階級・ブルーカラーの60ツイートに対して、同性愛・LGBTへの言及ツイートは9664件であった。161倍の開きがあった。トランプが2016年に選挙に勝利したのは、ラストベルトの労働者の支持が影響したと言われている。2010年・2015年の上記10メディアが、ラストベルトに言及した数は12件であった。

同性愛・LGBTへの言及ツイートが9664件、黒人への言及が3436件であることと比較すると、マスコミはラストベルトの労働者に興味はなかった。ラストベルトの労働者も問題を抱え苦しんでいたのに。

上記で書いたように、共感は社会的・政治的リソースだ。社会問題を解決するためにまずそこに社会問題があることが人々に認知されなければならない。LGBT問題も黒人問題もそこに社会問題がある事自体は認知されている（改善も遅々としてであるが進んでいる）。一方、労働者・ブルーカラーの問題は、マスコミによって認知されてなかった。

属性	言及ツイート数	労働者の何倍
労働者階級・ブルーカラー	60	1倍
白人	77	1.28倍
同性愛・LGBT	9664	161倍
黒人	3436	57倍
移民	1792	29倍

ポピュリストは忘れられた人々を票田に変える

その様に無視された人たちは、困難の中に居た。しかし、マスメディアや主要な政党は彼らに興味はなかった。マスコミは上記のように、LGBTには9664回言及する一方、労働者階級・ブルーカラーには60回しか言及していない。イギリスの例であるがブレイディみかこ「労働者階級の反乱」でも、大政党に見捨てられてきた地区には、UKIPやBNP（共に右翼政党）しか活動していなかったとの記述がある（p55）。

また、2016年、トランプが選挙戦を闘っていたとき、トランプ陣営の最大支出項目が野球帽だとニュースのコメンテーターがバカにしたことがあった。そのことについてマイケル・ムーアは以下のように述べた。

> 俺は35歳以上の怒った白人男性で、高卒だ。つまり、典型的な「トランプ支持の人口動態」に属する。そこで育ち、そこに暮らし、今もそこで生きている。大統領選の数週間前のこの番組で、トランプ陣営の最大の支出項目が野球帽だということを取り上げていた。そこでコメンテーターたちは「野球帽？ハッ（笑）」と馬鹿にしたんだ。俺は思った。「ああ、こいつらは（浮世から隔絶された）バブルの中で生きているんだ。（労働者階級にとっての野球帽の意味を）理解できないんだ」と思った。自分もいつも野球帽をかぶってきたし今もかぶってる。このとおり。これが俺たちの生き方だ。それを彼らは嘲笑したんだ。
> トランプ批判のマイケル・ムーアはリベラルか？

トランプはよく野球帽を被って我々の前に現れる。これは彼が、そうすれば（マスコミなどから）忘れられた人々の関心が買えると思ってのことではないだろうか？　そして、事実、2015年には泡沫候補に過ぎなかったトランプは第45代のアメリカ大統領となった。

以上が、共感格差についての要約だ。

最初に書いたように共感は有限のリソースだ。共感や同情は政治的・社会的リソース分配に影響する。共感や同情の分配は不平等だ。その不平等さは分配から漏れた人々の心を傷つける。リソースがなく誰にも分配されないよりも、彼らだけにはリソースが分配されないという方がよりひとの心を傷つける。

ポピュリストと同様に敵対勢力は、「忘れられた人々」を政治的リソースにするだろう

上記でポピュリストが、社会から共感や同情を与えられない人々を票田（政治的リソース）とし

て扱うという話をした。そして、この忘れられた人々を政治的なリソースとして扱うのは必ずしもポピュリストに限らないのではないか？　国外の敵対的勢力も彼らを利用できる。つまり、テロなどの社会不安定化要員として利用できるのではないか？

敵対的な勢力にとって有利な点はいくつかある。例えば、ソーシャルメディアの発達により、低コストで彼らのような忘れられた人々にダイレクトにアプローチできるようになったこと。そしてもう一つは、動員のためにかける労力が少なくて済むことだ。もしある人たちをテロリストに育てようと思ったら社会に対する不信感から育てなければならない（今の社会に満足しているならテロを行う必要はない）。しかし忘れられた人々は社会から顧みられず、すでに不信感を持っている。彼らがペインを感じており、そして社会が彼らを顧みないのは事実だからだ。敵対勢力のエージェントは彼らに承認を与えるだけで良い。言うならばすでにガソリンは充満しており、そこにマッチを擦って火を投げ入れれば良いようなものだ。

私達が、国内にいる社会から共感も同情も与えられてない人たちを包摂しないなら、彼らは国外の敵対的な勢力によって社会的不安定要員の候補者にされるだろう。

2024年8月13日配信・8月14日更新

サウスポートの暴動と報道

INODS UNVEIL ニュース担当

事件のあらまし

イギリスのサウスポートで少年が起こした事件に関する偽情報がSNS上で拡散し、翌日極右グループを中心とした人々が騒動を起こした。日本でもいくつかのメディアで取り上げられた。この暴動は偽情報と極右のどちらを主として報じるかで印象がだいぶ違う。この場合は、極右を主に報じるべきだろう。なぜなら今回の場合、偽情報だけでは暴動は起きなかった可能性が高いが、極右は極右だけで騒動を何度も起こしている。日本では1紙が極右に全く触れていない報道を行っていた。

２０２４年7月29日、イギリスのサウスポートで17歳の少年が刃物で多数を死傷させる事件が起きた。ＩＳＤの分析によれば、この事件の直後、事件現場に居合わせたという人物が犯人は移民で国境を封鎖すべきだという書き込みがあった。犯人の名前や素性も明らかにされた（もちろんでたらめだが）。その後、他のアカウントによって拡散された。そこで名指しされた犯人の名前はX上で18,000のアカウントから3万回以上使われた。

これにより、XとTikTokではアルゴリズムによって、トレンド入りしたり、推奨投稿になったり、さらに拡散した。

翌日になると、極右ネットワークが仲間にオフラインの抗議活動を呼びかけた。きわめて短時間に多数が動員され、攻撃活動を追悼集会を襲撃し、50人以上の警察官に負傷を負わせる事態にまで発展した。

暴動の原因

暴動の原因は最初の偽情報と、それを利用した極右ネットワーク（English Defence League. EDL）を中心とした極右の抗議活動だった。主要な海外メディアではこの暴動の報道には偽情報と極右がセットになって出てくる。そうしないと、事件の本質を見誤るからだ。極右ネットワークによる組織的な動員があったことに触れないと、まるで一般市民が反移民の抗議活動を行っているかのように受け取られる可能性がある。

1紙だけが極右の関与に触れていなかった

現時点での報道の内容を確認してみたところ、下表のようになった（暴動を記事化していなかった場合は「記事」に○がついていません）。なぜか、1紙だけが、極右あるいはEnglish Defence League（ＥＤＬ）の関与に言及していなかった。

メディア名		記事	極右	ELD
国内紙	A	○		
	B	○	○	
	C			
	D	○	○	
	E			
海外紙	ワシントン・ポスト	○	○	○
	ニューヨークタイムズ	○	○	○
	BBC	○	○	○
	CNN	○	○	
	Bloomberg	○	○	○
	Al Jazeera	○	○	○

メディアはなにを取り上げ、なにを取り上げないかを決めている。その判断基準は外部からはよくわからないし、説明しようとする姿勢もない。

その一方で、ＳＮＳプラットフォームは政府や世論の要請に応じて、アルゴリズムを始めとする透明性の向上を行っている（充分とは言えないが、やらないよりははるかにマシ）。ＡＰＩや統

計の取れるツールまで公開している企業もある。メディアはこうしたことを一切行っていないし、代わりに文書や資料を公開することもない。こうした透明性の低さがメディア不信につながり、認知戦やデジタル影響工作のターゲットにされる隙を作っている。特に今回のように意図的に騒ぎを大きくしようと考えているアクターがいる場合は注意が必要だ。

2024年8月4日配信・8月5日更新

続報はこちら
イギリス各地を暴力に巻き込んだ反体制ポスト組織ネットワーク
https://inods.co.jp/news/3330/

偽・誤情報対策が開く思想統制への道

藤代 裕之

前回迷走していると指摘した総務省の有識者会議「デジタル空間における情報流通の健全性確保の在り方に関する検討会」と「ワーキンググループ（WG）」のとりまとめ案が7月末に公表された。300ページを超えるボリュームで、様々な角度から偽・誤情報の要因や対策を記述しているが、思想統制につながりかねない危険な記述もある。

対象を制限する工夫は見られるが…

本検討会の問題意識としては、「デジタル空間における情報」そのものや様々な主体による

表現の場としての「情報空間」の健全性ではなく、「デジタル空間における情報流通」、すなわち、情報システムや情報通信ネットワーク等により構成され、多種多様の情報が流通するインターネットその他のグローバルな仮想的空間であるデジタル空間における情報の流通の在り方について、その健全性の確保を目的とした検討を行うものである。

『デジタル空間における情報流通の健全性確保の在り方に関する検討会とりまとめ（案）』

とりまとめ案の冒頭、「はじめに」には上記のような記載がある。ネット企業だけでなく、既存メディア、企業、国や自治体、さらには利用者まで対象にしたことでネット全体を対象にした議論では表現規制に歯止めが効かなくなってしまう。コンテンツを含めればダイレクトに表現規制につながるため、流通の在り方が対象だと改めて整理したものだ。しかしながら、そう簡単な話ではない。

検討会は２０２３年11月に設置され６回、ＷＧは13回、本検討会とＷＧの合同で19回の計38回の会合を開催する異例の展開をみせている。各会合で説明された関係団体や専門家による考え、構成員による議論などに大変な時間と労力が費やされたことは間違いない。そのことには敬意を評したい。

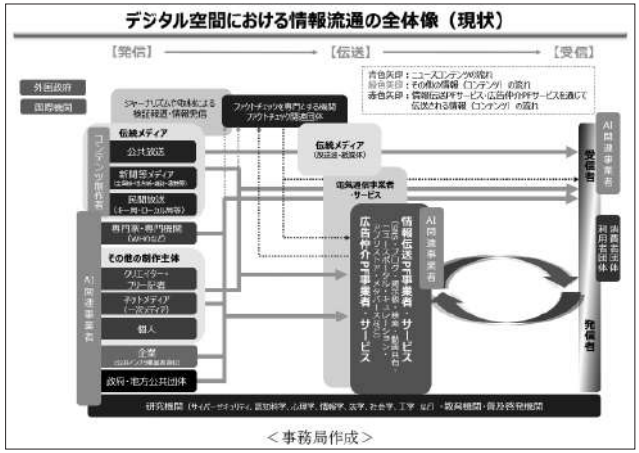
筆者は４月12日のＷＧで説明する機会を得た。そこで話したことは「ニュース」「コンテンツ」「広告」に分け、中でも「広告」にフォーカスした対策を行う必要があるということだ。コンテンツの中身を議論することになるため危険性があるが、議論の対象を制限することで、ネット空間全てを対象にするよりもリスクが低下すると考えたのだ。

発表資料　偽・誤情報とフェイク ニュース対策の方向性
https://www.soumu.go.jp/main_content/000942298.pdf

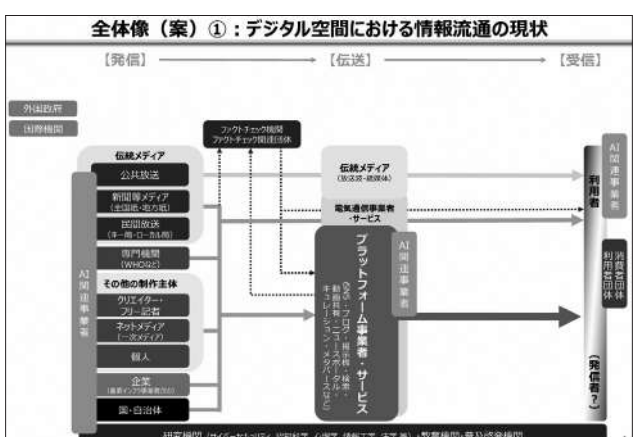
筆者の説明が反映されたのかは不明だが、まとめ案に示された図を見ると当初示されたものと異なっていることが分かる。中心に置かれた「プラットフォーム事業者・サービス」が、「情報伝送ＰＦ事業者・サービス」と「広告仲介ＰＦ事業者・サービス」という2種類に分けられている。だからといって、表現規制が遠ざかったというわけではない。

対策はメディア規制に利用されている

「フェイクニュース」という言葉が２０１６年のアメリカ大統領選挙で注目されて以降、各国で



図：まとめ案に示されたデジタル空間



図：1月25日版

対策が議論されているが、一部の国ではフェイクニュース対策の名のもとにメディア規制が行われている。対策そのものに危険性があるということを押さえる必要がある。

ロシアでは軍事行動に関する情報について当局が「偽」であると判断すれば、記者に禁固刑を科すことができる。先日、米露で行われた囚人の身柄交換で釈放されたウォール・ストリート・ジャーナルのエバン・ゲルシコビッチ記者は禁錮16年を言い渡されて収監されていた。

対策を口実にメディアや表現を統制しようという動きは、ロシアだけではない。

シンガポールでは2019年に「オンライン虚偽情報・情報操作防止法（POFMA）」が成立、違反した企業に罰金、個人は罰金または懲役刑がある。2022年には海外から世論への干渉を防ぐ「外国介入対策法（FICA）」も成立している。どちらも適用の基準が曖昧であり、表現の自由を制限する危険性が指摘されている。マレーシアでも「フェイクニュース対策法」が制定され、用語の定義が曖昧なために恣意的な運用が懸念されている。

まとめ案においても各国の対策が取り上げられており、シンガポールやマレーシアの事例が紹介されているが、懸念については記載されていない。有識者が対策の危険性を知らないはずがなく、あえて記載されてないと考えるのが妥当だろう。

偽・誤情報対策のような一見「良いこと」のように思われるテーマこそ危険である。「子どもた

ちに悪影響がある」や「教育上問題である」といったことから表現規制につなげようとしてきた動きも過去にはあった。だからこそ、慎重に議論されてきたはずではなかったか。３００ページもあれば、どこかに何らかの表現規制につながる記述が紛れ込む可能性が高い。

プレバンキングという危険な考え

筆者は6章「総合的な対策」に書かれているあるワードに注目した。それは「プレ（プリ）バンキング」という考えだ。初めて聞いたという方も多いかもしれないが、フェイクニュースに騙されない免疫をつける予防接種などと紹介されることがある。

まとめ案では、「一度正しいと受け入れられた偽・誤情報等の流通・拡散による影響を訂正によって事後的に修正することは容易ではない場合には、偽・誤情報等の発生に予め備えるプレバンキングが重要になってくる。」と記載されている。

ケンブリッジ大学、ＢＢＣ、グーグルのシンクタンク部門 Jigsaw が制作した「誤情報のプリバンキング実践ガイド」が発行されている。ガイドには、注意点や限界についても記載されているが、「介入」や対象者の「意識を変える」「行動を変える」という言葉が出てくる。つまり人の内心に踏み込み、意識や行動を変えるということである。

ハンドブックには効果がなかった事例として「白人至上主義のストーリーをプレバンキングするメッセージは、極右主義者に効果がありませんでした」と記載されているが、どのような思想や主義に基づいて実施するのか、正しさや間違いは誰が決めるのか、国や一部のプラットフォームがそれを決めることにはならないのか、など懸念は強い。また、説明が不十分なまま対象者が知らない間に実施されてしまうかもしれない。

この「プレバンク」はリテラシー界隈などの一部に評判が良いようだが、人の内心に踏み込むことを「良いこと」としている時点で非常に危険である。にもかかわらず、まとめ案には効果の限界についての記載はあるが、手法そのものの危険性は記載されていない。

筆者は「プレバンク」に注目したが、他にもある可能性がある。ファクトチェックについてもファクトチェック団体から疑問の声があがっている。

参考資料　誤情報のプリバンキング実践ガイド

https://interventions.withgoogle.com/static/pdf/A_Practical_Guide_to_Prebunking_Misinformation_ja.pdf

表現の自由を守る意識があったか

まとめ案は、多様な角度から分析をしており、真剣に取り組んだことはうかがえるのだが、総務省の有識者会議はこれからの政府の方針に大きな影響を与えることになる。ネット全体に「健全化」を持ち込むこと自体、表現の自由が危ういという意識が有識者会議のメンバーにあったのだろうか。総務省の設定したアジェンダについて疑問を提示するのも有識者会議の役割ではないのだろうか。

議論がスタートして能登半島地震が発生し、パキスタンやイランなど海外からのインプレッション稼ぎにより国民の注目も集まり、さらに実業家の堀江貴文氏や前澤友作氏が自由民主党の会合で対策を訴えるなど、何らかの対策を行う必要に迫られた状況はあるだろう。だが、公開されている議事録を読んでも、懸念を述べているのは一部の委員にとどまり、それぞれの問題関心をプレゼンテーションしているだけのように思える。拙速な議論は未来に表現規制の種を撒くことになる。

2024年8月27日配信

新潮流になるか？
AIにより生成されたペルソナを活用した影響工作

岩井 博樹

大手メディアが関与する偽情報配信とAIによる情報拡散

生成AIにより生成された架空のオンライン人格（偽ペルソナ）たちが、ソーシャルメディアへ偽情報を次々と投稿し、世界を作り話で染めていく。その黒幕はなんと大手メディアだった。まるでSF小説のようなことが現実となり始めている。

7月9日、米国連邦捜査局（FBI）およびサイバー国家ミッションフォース（CNMF）は、オランダ、カナダと連携し、ロシアの国家支援メディアであるRT（旧ロシア・トゥデイ）とその関連会社が、AI搭載のボットファーム生成を行うソフトウェア「Meliorator」を影響工作に活用し

ているとの勧告を発表した(※1)。このMeliorator は、偽情報を拡散することを目的として開発され、管理パネル「Brigadir」を通じて、オンライン人格たちの行動を自動化している。オンライン人格の作成、自動化されたインタラクション、コンテンツの増幅などの機能を持つ同ソフトウェアの投稿は、一見、実在する人物が投稿したように見える。図1はMeloratorの生成したオンライン人格の一例だ。オンライン人格の思想モデルは、何パターンか用意されているようで、自己紹介文も様々だった。

Meliorator が生成した架空のオンライン人格例

今回の勧告は、上述した通り、Meliorator により複数国籍の架空のオンライン人格を作成し、X(旧Twitter)上で偽情報を増幅していたことに対するものである。その標的国は、米国、ポーランド、ドイツ、オランダ、スペイン、ウクライナ、イスラエルなどだ。日本語の投稿は確認されていないため、日本への影響は単純に測れるものではない。しかし、他国が、ロシアによるこれらの手法を模倣する可能性は、国際情勢動向や模倣に必要な技術的障壁の観点から比較的高いとみられる。そのため、私見ではあるが、本勧告を国家の情報安全保障上の課題として捉えるべきものだと考えている。

図1 Meliorator が生成した架空のオンライン人格例

ロシア国営空母メディアが仕掛ける親ロシア・ストーリーの拡散

RTは、中国が「空母メディア」と揶揄するロシアの国際ニュースチャンネルだ。世界100カ国以上に7億人以上の視聴者がいるとされる同チャンネルは、2005年12月の開局以来、メディア融合の手段を駆使してロシアの対外宣伝を行ってきた(※2)。2019年には、ロシアがRTを介して偽情報を配信していることが報じられ、ロシアの影響工作を支援していることが明らかとなっている(※3)。

ロシアにとってMeliorator の利用メリットの1つは、架空のオンライン人格(ペルソナ)の生成により、西側諸国の追跡を回避できる点だろう。X上で、オンライン人格がリポストした内容には、RTのコンテンツも含まれていたと推察されるわけだが、現在、一部の国家はRTのチャンネルをブロックしている。そのような場合においても、オンライン人格を介してコンテンツを投稿、拡散することで確実にXユーザへアプローチすることができる。その結果、図2のように一部のXユーザがMeliorator のボットに反応し、他のユーザへと影響が広がっていく。

ソーシャルメディア上での影響工作の効果を認識していた中国

RTは早くからXやGoogle+、InstagramなどのSNSにチャンネルを持ち、2007年にはYouTubeに参入している。このRTのソーシャルメディアへの参入に対して、中国の国防科技大学の马建光教授は、中国人民解放軍のニュースポータル「中国军网」への寄稿（2016年12月）で、ロシア国内はもとより、西側諸国においてもネチズンを惹きつけていると指摘している（※4）。この指摘は、中国人民解放軍は、少なくとも2016年にはソーシャルメディア上でのRTの活動が、いわゆる「情報兵器（※5）」として機能していることを認識していたことを示唆している。

また、ロシアは西側諸国からのメディア戦への対策も迅速だった。ロシアは、すぐにネットメディアの規制を国家レベルにまで引き上げ、情報安全保障の立法を整備している。2022年に、米メタ・プラットフォームズ社のロシア連邦領域におけるFacebookおよびInstagramの製品販売活動に対して、「過激派活動」を理由に禁止したのも安全保障上の理由とみられる（※6）。

これまでのロシアと中国の活動や方向性を勘案すると、両国ともソーシャルメディアの影響力については早くから認識し、対応していたことが分かる。

図2 Xユーザによるペルソナへの反応例（出典：X.com）

ロシアの影響工作への中国の関心度

中国は、これまでもロシアのプロパガンダの拡散手法を参考に実施しているように見受けられる。実際に中国が、XやFacebook、Instagramなどを影響工作に活用し出したのは、前述の中国軍网を含む関連の論文の寄稿後であり、2019年の香港デモに関連する情報戦が契機となったと考えられる。これらのことを勘案すると、中国がMeliorator を模倣した類似システムを利用し、ソーシャルメディア上で影響工作キャンペーンをいつ実施していても不思議ではない。（もっとも、既に始まっている可能性もあるが。）RTがMeliorator を活用したように、外国語チャンネルを有するメディアがAIを活用するケースが模倣されることを想定した場合、中国国営メディアの動向からは目が離せない。

なお、現在、中国による影響工作のＡＩの活用は、「Spamouflage」や「Dragonbridge」の呼称で知られるグループが、ＡＩで生成したコンテンツを利用し、中国にとって有利なストーリーを投稿していたことが知られている(※7、※8)。加えて、台湾の総統選挙でもＡＩを利用した偽情報や偽動画が多く確認されたことも記憶に新しい(※9)。ただし、これらはいずれも大手メディアが直接関わったものではない。

中国製ＡＩが影響工作に利用される可能性

中国発の影響工作への利用が懸念されているシステムの1つは、北京智源人工知能研究院(BAAI)の開発した、「悟道2.0(認識への道)」である(※10)。同システムは、マルチモーダルＡＩモデルを採用しており、テキスト生成、画像生成、自然言語処理といった複数の種類のデータ種別を一度に処理できる。さらに、大規模なデータセットにより学習が行われており、4.9テラバイトの画像とテキストデータによりトレーニングした結果、1・75兆のパラメータを持っている。

言うまでもなく、この言語モデルに対し、欧州や米国の有識者たちは、強力な偽情報やプロパガンダ・マシンとして使われる可能性に対して警鐘を鳴らしている(※11)。現時点では、悟道が実際にプロパガンダや偽情報の配信に悪用されたとの報告は無い。

ちなみに、日本への影響のみを考えた場合、ロシア製と中国製のソフトウェアから想定される脅威を比較すると、国家戦略とツールの特性上、悟道が活用される可能性が高いことは言うまでも無いだろう。仮に中国でMeliorator(※6)のようなボットファームが開発されるとすると、悟道をベースとしてプロパガンダ、偽情報が生成されるのかもしれない。

情報安全保障上の課題と予想される脅威

日本でも誤情報・偽情報の拡散は大きな問題となっており、総務省が「令和3年度 国内外における偽情報に関する意識調査」という調査報告を公開している(※12)。同報告書によれば、偽情報を見かけたメディア・サービスのSNSだったという。ちなみに、2位にはテレビが入っており、民放における外資系メディアとの関係を鑑みると、非常に興味深い結果となっている(※13)。つまり、この結果だけ踏まえれば、日本には既に前述したロシアの手口により、誤情報・偽情報が拡散する土壌があると言えそうだ。これは、日本にとっては情報安全保障の観点で弱点となる。

安全保障面だけでなく犯罪対策としても重要

Melioratorを利用したキャンペーンは、２０２２年から開始されたとみられ、発覚までに約2

年かかっている。そのため、現状では、架空のオンライン人格をすぐに発見することは難しいとみられる。

Meliorator のようなソフトウェアは、一般組織でもインフルエンサーとして利用できる可能性がある。オンライン人格（ペルソナ）を大量に生成して、それらに特定ブランドや商品のポジティブな意見を拡散させることは容易に想像のつくことだ。ただし、このような手法には倫理的な問題が伴う。架空のインフルエンサーによるマーケティングは消費者を欺くリスクがあり、悪用される可能性もある。その観点では、Meliorator に関する報告は、近い将来の犯罪行為に対しても警鐘を鳴らすものであると考えられる。

大国の仕掛ける影響工作は、メディアを利用して自国の都合の良い情報を配信するだけのものから、架空のオンライン人格（ペルソナ）を大量生成し、ソーシャルメディア上で間接的に拡散する手口へとシフトしている。現時点では、投稿内容の１つ１つを見ると、違和感を覚えるものが多いと思う。しかし、架空のオンライン人格が数年をかけて有識者やインフルエンサーの立場となった場合、どのような世界になるかは想像もつかない。ＡＩの生成する架空のオンライン人格に日本の情報安全保障が脅かされる時代はすぐそこまで来ているのかもしれない。

２０２４年９月10日配信

参考

※１ https://www.ic3.gov/Media/News/2024/240709.pdf
※２ https://www.rt.com/about-us/distribution/ , https://www.rt.com/on-air
※３ https://www.theguardian.com/commentisfree/2019/jul/26/russia-disinformation-rt-nuanced-online-ofcom-fine
※４ https://perma.cc/M72E-PRVQ
※５ https://medium.com/dfrlab/question-that-rts-military-mission-4c4bd9f72c88
※６ https://jp.reuters.com/article/idJPKBN2R61T9/
※７ https://therecord.media/openai-report-china-russia-iran-influence-operations
※８ https://downloads.ctfassets.net/kftzwdyauwt9/5IMxzTmUclSOAcWUXbkVrK/3cfab518e6b10789ab8843bcca18b633/Threat_Intel_Report.pdf
※９ https://www3.nhk.or.jp/news/html/20231223/k10014297431000.html
※10 https://perma.cc/7ENH-64LD
※11 https://www.politico.eu/article/meet-wu-dao-2-0-the-chinese-ai-model-making-the-west-sweat/
※12 https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/html/nd123140.html
※13 https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/html/datashu.html#f00027

サブカルチャーと情報工作

藤田 直哉

INODS UNVEILをお読みの皆さん、はじめまして、の方は、はじめまして。

藤田直哉と申します。サブカルチャーやネットカルチャーを中心とした批評を書いたり、映画の大学で教員をやらせていただいたりしております。

そんな人間が、どうしてサイバーセキュリティや、安全保障に関するコラムを書くのか？　とお思いになられる方もいらっしゃるだろうと思います。なので、初回は、自己紹介も兼ねて、この連載コラムで何をしようと思っているのかを、説明していくところから始めようと思います。

世論戦と認知戦の時代に

現在の安全保障やサイバーセキュリティが、いわゆる兵器による物理的な戦いや、コンピュータにハッキングするようなもの〝だけ〟ではないことは、既に多くの方々がご存知のことかと思います。

「世論戦」「認知戦」と呼ばれる、世論や人々の考え方に影響を与える工作も広く知られておりますし、たとえばある重要なインフラなどを担う会社の株をある国が買い占めて影響を行使することを防ぐ「経済安全保障」なども、よく聞く言葉になっているのではないでしょうか。

防衛大学校安全保障学研究会編著『新訂第5版　安全保障学入門』には、「偽情報」について、このような言及があります（ここから、「ですます」調ではなくなりますが、ご容赦を）。「インターネットとソーシャルメディアが世界に普及している現代においては、政治的な意図を有した個人、組織、国が、いわゆるフェイク・ニュースや偽投稿を大量に流し、自動的にそのツイートの拡散さえできる。それを見た者が偽モノと見抜けないほど巧妙に仕組む。それが他国からの介入となると、２０１６年の米大統領選へのロシアの介入のように、国家間の争点、対立の原因になる。『偽情報』も相手国に多大な影響をもたらす点においてパワーの行使であり（……）サイバー攻撃の一つになる」（p123）。

インターネットなどにおける情報工作、世論誘導は、防衛大学の研究会がこう書くほどの安全保障上の脅威なのである。

この連載コラムでは、「世論戦」「認知戦」などの、新しい領域における攻撃を、サブカルチャーやネットカルチャーなどの観点から分析し、なるべく現代的・同時代的な題材を元に論じていこうと思っている。

どうして、サブカルチャーと安全保障が関係あるのか？　その説明を、次節で行う。

現実から逃げ込む誘惑のある者たちへの工作

ジョンズ・ホプキンス大学教授トマス・リッドが世界の積極工作についてまとめた『アクティブ・メジャーズ』には、ＣＩＡが、東ベルリンに自分たちの「自由」の思想を広めるため、ゴシップ、占い、ジャズなどの、ライフスタイルやエンターテインメントを扱う雑誌を創刊して利用したケースが紹介されている。

それは、「モスクワ共産主義に対する攻撃のために西側が使える効果的な力」(p100)であった。その手法は「個人が過去の経験や希望と、日常生活の厳しい現実との折り合いがつけにくいような――それゆえにこの現実から『迷信やファンタジー』に逃げ込む誘惑がある」(p100)人々を狙ったものだった。

サブカルチャーは、良くも悪くも「個人が過去の経験や希望と、日常生活の厳しい現実との折り合いがつけにくいような――それゆえにこの現実から『迷信やファンタジー』に逃げ込む誘惑がある」人の需要に応えるジャンルである。だから、その愛好者は、様々な工作のターゲットとなってきた現実がある。

２０１６年のアメリカ大統領選では、トランプ当選に向けてロシアが工作したことが判明しているが、トランプ陣営は「弱者男性」向けに、カエルのペペなどのネットミームを駆使した選挙戦を行ったことが分かっている(アーサー・ジョーンズ監督『フィールズ・グッド・マン』、アーサー・ジョーンズ、ジョルジョ・アンジェリーニ監督『アンチソーシャル・ネットワーク：現実と妄想が交錯する世界』など)。

２０２１年アメリカ合衆国議会議事堂襲撃事件を起こしたQアノンたちが育まれたのは、日本の影響も非常に強いオタク的な匿名掲示板である4chanやRedditだった。Qアノンの源流には「ゲーマーズゲート事件」があり、サブカルチャーの愛好者と、このような過激派や陰謀論者たちにはなんらかのつながりがあると見做され、アメリカでは安全保障上の問題になっている。

マイアミ大学教授ジョセフ・ユージンスキは、トランプを「陰謀論を用いて政治方針や政府の

行動を正当化する大統領」(p159)と断定し、「トランプの陰謀論は(……)反主流派のアウトサイダーには熱狂する人たち――の心にうまく入り込んだ」(p165)と述べている。

サブカルチャーは、「サブ」、つまり、「副」の文化である。対義語はメインカルチャーで、主流の文化とは、学校や企業などにおける「正しい」「規範的」な価値観のことである。「サブ」カルチャーを愛好する者たちは、だから、基本的に、アウトサイダー的な自己認識と気質を持っている傾向がある。つまり、主流の世界を支配している価値観――リベラルや、エスタブリッシュメントと彼らは呼ぶが――に対して、アイデンティティ的に反発してしまいやすい心の癖を持つ傾向がある。

ユージンスキは、「陰謀論は敗者のもの」であると述べている。選挙で、負けた方の政党の支持者は、選挙に対する陰謀論を唱えやすいという世論調査の結果がある。そして、「無力感、社会的疎外感、自信のなさ、不安感、コントロールができないという気持ちは、陰謀信念と相関関係がある」(p108)。

陰謀論は、社会的に劣位の弱い境遇に置かれた者が抱きやすいのだ。これだけ日本が衰退し、中国やその他の国が成長するなかで停滞を続けているがゆえにアイデンティティや誇りが保ちにくく、不安になり、生活が苦しい者が増えている現在、同じような陰謀論の誘惑に屈しやすくなっている者は日本でもたくさんいるだろうと思われる。ここには深刻な安全保障上のリスクがあるのだ。

人生に意味を与える「物語」

陰謀論や過激派の背景に、ゲームの影響を指摘する論者も少なくない。

ワシントン&ジェファーソン大学英語学科特別研究員のジョナサン・ゴットシャルは『ストーリーが世界を滅ぼす』の中で、2018年10月27日にピッツバーグ郊外のツリー・オブ・ライフ・シナゴーグで起こった銃乱射事件について書いている。

犯人は46歳の男性で、11人が殺害された。銃乱射を行った理由は「ユダヤ人が、事実上のアメリカ侵略と白人種に対する緩慢なジェノサイドを進めている」(p20)という陰謀論だった。

ゴットシャルはこう書く。「事件の犯人は、ユダヤ人は邪悪だとする古来のフィクションの単なるマニアではなかった。どこかの時点で、彼は登場人物としてそのフィクションの中に入り込んだ。彼は壮大な歴史叙事詩の悪を倒す英雄にみずからを仕立て上げた。悪夢のようなLARP(ライブRPG〔引用者註、ゲーム世界の設定を再現して遊ぶ体験型ゲーム〕)ファンタジーにとらわれていたのだ。『ダンジョンズ&ドラゴンズ』の物語世界を演じながら楽しく森を駆け抜ける大人

たちのように。／だが、彼に撃たれた被害者たちは現実の存在だった」(p23)

ゴットシャルは、陰謀論は単純な二項対立の物語だと述べた上で、「流行るのは陰謀物語がたいてい、気持ちをわくわくさせる虚構のスリラーだからである。信者の多い陰謀物語はほぼすべて、ハリウッド映画として大ヒットするはずだ。それに対して、陰謀物語の嘘を暴く検証記事のほとんどは、公共放送ＰＢＳのまあまあ悪くないドキュメンタリーにしかならないだろう」(p121)「世俗的な地球平面説信者〔引用者註、陰謀論者の一例〕はＳＦとミステリーとスリラーが入り混じった世界に生きている。世俗派たちは手がかりをつなぎ合わせ、犯人を暴き、その隠れた動機を解明するという探偵のような仕事を求められているのだ」(p128)と分析する。

二項対立で単純な「物語」を好むという志向性においても、サブカルチャーのファンと陰謀論者が重なりやすい側面は確かにあるだろう。筆者も、たくさんこういう物語を楽しんできた。「世界の真実を暴く」「陰謀を見抜く」「世界の危機に身を投げ出して戦う」物語も大好きである。

それが、リアルタイムの相互作用ゲームである点を、ゴットシャルは強調している。今が歴史の変わり目、運命が決する瞬間であり、そこに自分が「戦士」として参加しているというロールプレイの感覚こそが、自分自身の生や存在に意義や価値を与え、高揚感を齎してくれる点が重要なのだという。

おそらくそれが、ゲーマーゲート事件はじめ、ＳＮＳや掲示板を舞台にしているゲーム的な政治が力を持ちやすい理由であり、その背後には無力感や孤独感、無意味感が存在していると推測される。

ＳＮＳにおける対立と分断への介入

サブカルチャーの愛好家だけではないが、ＳＮＳを見ていると、人種だけではなく、ジェンダーや貧富などの差を利用して、単純な二項対立の「物語」が跋扈しているのが観察できる。

その「物語」は、基本的に、「あなたは悪くない」「悪いのはあいつらだ(倒せばユートピアが訪れる)」という物語により、自尊心を鼓舞し、自己肯定感を得て、自己正当化の免罪符を与えられる構造になっていることが多い。本当にそうなのか、自分に問題がないのか、敵は本当に彼らなのかの検討は甘い傾向がある。往々にして人はその物語を演じ、「戦士」として戦うことで、使命感や生の意味を獲得してしまう。

このようなＳＮＳというメディアに適合したポピュリズム政治が蔓延する現代ではあるが、対立と分断に介入する工作に利用されてしまう可能性について、本気で検討しなくてはならない。

２０１６年5月21日、テキサス州のイスラム教ダアワセンターで、テキサスの伝統を称える保

守主義者「ハート・オブ・レキサス」というグループと、移民の権利を支持する「ユナイテッド・ムスリムズ・オブ・アメリカ」というグループのデモ隊が衝突した。これはどちらも、ロシアにあるインターネット・リサーチ・エージェンシー（ＩＲＡ）が作ったフェイスブックグループだった。前者はメンバー数25万人、後者は30万人。つまり、積極工作＝アクティブ・メジャーズだったのだ。

ロシアによる２０１６年のアメリカ大統領選への介入について、ジョナサンはこう表現する。「あれは物語の電撃戦だった。物語と物語に対する人間の生来的な弱さの兵器利用だった。（……）長期的な目標は、同族意識から生まれる憤りに火をつけることによって、アメリカに長引くダメージを与えることだった」「ロシアの諜報機関はミーム、インフォグラフィック、フェイクニュースなどあらゆる武器を使った。そのすべてに共通していたのは、対立するナラティブを作り出してぶつけ合い火花を散らさせ、やがてアメリカ人同士を反目させて、自分の尻に噛みつこうと体をひねって追いかけるうちに目を回してふらふらになっていく犬のようにする企みだった」(p101)

私たちは、ＳＮＳを見ていると様々な義憤に駆られることがある。もちろん、それによって改善されたり、正義が実現したこともいっぱいあるだろう。しかし、このような事例がある以上、私たちはネットに触れるとき、それに反射的に反応したくなったとき、もう一呼吸おいて、メタ認知をし、反省的にリアクションする必要があるのではないだろうか。そこにある「物語」について、距離を置いて疑う目線が重要なのだ。

ＳＮＳにおける影響工作

TikTokやインスタグラム、YouTubeなども、もちろん、この「戦場」の例外ではない。

保坂三四郎『諜報国家ロシア』によると、ＫＧＢの教本に、積極工作として次のような行為が行われると書いてあるという。「『偽情報』の他、米国やその同盟国の『陰謀』を暴いて反米感情を煽り、ソ連に有利な外国勢力を形成する『暴露』、敵国の政府、政治家、反ソ組織に倫理的ダメージを与える『コンプロマット』」(p101)がある、と。

プーチンは、ＫＧＢの若手幹部として、「積極工作が最も狡猾だった時代に、とくに西独に対する積極工作を行うために設置されたドレスデン支局に勤務したこともある」(トマス・リッド『アクティヴ・メジャーズ』p343)人物である。冷戦崩壊で下火になった不正工作を１９９０年代に復活させたのは彼だと言う。では、そのプーチン政権の今、どんな工作が行われているのか。

ＩＲＡにおいて、「サンクトペテルブルク国立大学の現役学生や卒業生などが１シフト１２０人の三交替制で勤務し（……）運営者の指示に沿って、ニュース記事に１人当たり１日１００件程

度のコメントを書いていた」(『諜報国家ロシア』p166)。彼らは、「米国が抱える主要な社会問題」の知識を持ち、急進リベラルや急進保守になりかわり、双方の感情を刺激し煽り炎上させていった。

2021年にカーディフ大学の研究所が、YAHOOのコメント欄をロシアが利用しているとする報告書を出しているが、日本でもそれらニュースサイトのコメント欄だけではなく、X(旧ツイッター)や5ちゃんねるなどでこのような工作が行われているだろうと推測するのが当然だろう。

そして、動画配信者、インフルエンサーとして情報工作が行われる場合もある。「ナーシは、クレムリンから資金提供を受け、プーチンを題材にしたポップな動画やユーモアと陰謀論の境界が曖昧な『おもしろ動画』を作成するとともに、プーチンの動画が上位に入るようにSEO(検索エンジン最適化)対策のプロを雇った」(p165)

気軽に動画を観ているだけでは、もはや危険なのだ。受動的にネットを消費すること自体が、自分たちの破滅を招くかもしれない。私たちが巻き込まれている「新冷戦」と呼ばれる戦争は、残念ながら、そのような、情報や信念などを奪い合う、そうであるがゆえに何が本当なのかの安心を得にくい状態になってしまう戦争なのだ。

文学、芸術、人文学、幸福、愛着、存在論的安心による安全保障

では、どうすれば良いのだろうか。様々な規制や、サイバーセキュリティの強化などはもちろん必要だろう。しかし、ここでは、あくまで、文化という角度から考えてみたい。

中曽根平和研究所主任研究員の大澤淳は「文学や芸術が社会に浸透して創作活動が活発な、文化の層の厚い社会をつくることが、人々がナラティブに乗らないような多層的で寛容な社会をつくれるのではないでしょうか」(『外交』vol.80、p20)と述べている。筆者もそれに賛成である。

サブカルチャーは単純な物語が多い上に、ルサンチマンなどを晴らすナラティヴがパターンとなっている。そのようなファンタジーによって心のバランスを取ることが、生きるために必要な者たちは確実にいる。サブカルチャーに限らず、宗教なども、そのような物語かもしれない。

そのような「物語」を相対化したり、複雑性や多様性を知ったり、「物語」と現実の違いを検討できる能力が大衆的に普及することが、情報工作を通じた民主主義のハッキングに抗うために必要である。迂遠な道ではあるが、文学や芸術や人文学の豊かさや複雑さを享受できるものを増やす協力が、偽情報の影響、過激化、民主主義の破壊を防ぎうる、単純かつ有効な道ではないだろうか。

そして、多くの者が陰謀論的な信念を必要としてしまう状況を改善していくことが必要である。陰謀論を信じることと、存在論的不安や、適切な愛着関係を築けないことには関係があると言わ

れている。とすれば、なんらかの方法で、存在論的安心や、安定した愛着や愛情関係を手に入れることができれば、陰謀論や過激派の影響は低下していくのではないだろうか。

その方法論が、福祉なのか、結婚率をあげることなのか、共同体やそれに代わるつながりを作ることなのか、宗教やナショナリズムなどの「物語」を利用することなのか（それは副作用も大きいだろう）、筆者には分からないが、安全で健全な形で自尊心と幸福が手に入るようになっていけば、これらの破壊工作は機能しにくくなっていくはずだ。絶望や貧困への介入は、単純に金銭や物質的なものだけではなく、愛着や愛情、幸福などと関連する、「存在論的安心」を提供できるような国家・社会・経済・地域・家族などの仕組みにしたほうが良いのではないか。「陰謀論」を信じることと、愛着のあり方に関連があるという知見が正しければ、論理的に考えて、そのような方向の「安全保障」がありうるのだと考えを変えなくてはならない。

では、それを実現するためにどうしたら良いのか――などは、おいおい考えていくことにしよう。本稿はとりあえず、サブカルチャー・ネットカルチャーなどを、新領域の安全保障との関連で論じる必然性について簡単に前提確認をした。なお、本稿と重複する内容は、6月末に刊行される、『現代ネット政治＝文化論――AI、オルタナ右翼、ミソジニー、ゲーム、陰謀論、アイデンティティ』（作品社）でより詳しく論じているので、ご興味をお持ちの読者はぜひそちらを読んでいただければと思う。

2024年8月6日配信

巨大化する中国の情報・工作機関

黒井 文太郎

ＳＮＳを利用した世論操作など、国家機関が密かに進める〝誘導工作〟が注目されている。もともとロシアが先行していたが、中国も本格的に始めているようだ。

こうした工作は、各国の情報・工作機関が行なう。では、中国にはどのような組織があるのか。種類と活動内容をみていきたい。

中国国内の情報工作を行う巨大省庁「公安部」

政府機関でもっとも強力なのは、１９０万人の要員を擁する巨大省庁「公安部」である。公安部はつまりは警察だが、その守備範囲は広く、担当するのは治安維持の一般的な警察業務だけでない。共産党政権の維持を目的とする政治警察であり、反体制運動の芽を刈り取る公安警察でもある。

そもそも公安部の筆頭部局である第１局は、別名「政治安全保衛局」という政治・公安警察だ。この第１局（政治安全保衛局）は基本的には国民の監視を行なうが、内部部局である「対外連絡処」「民族宗教領域案件偵察処」「反破壊活動偵察処」「境外非政府組織管理弁公室」、あるいは統括下に置く「香港マカオ台湾事務弁公室」などが、監視対象への偵察活動と同時に、対象に対する誘導工作も行なっているとみられる。

また、第１局以外でも部分的に監視対象への誘導工作を行なっているとみられる部局がある。メディア監視を任務とする「新聞宣伝局」、法輪功などを監視する「第４局」（反邪教局）、イスラム過激派などを監視する「第６局」（反テロ局）、ネット検閲が担当の「第11局」（ネットワーク安全保障局）、盗聴・ハッキング活動を行なう「第12局」（技術偵察局）などだ。

これらの監視対象は中国国内に留まらず、国外の中国人社会に及ぶ。つまり、国際的なインテリジェンス活動であり、誘導工作も世界規模になる。ただし、公安部の監視対象への誘導工作は、あくまで反体制分子のネットワークの摘発を目的としたものが主で、監視対象そのものの考えを

誘導し、コントロールしようという性質のものではない。

公安部の国内監視技術から発展したサイバー管理技術

なお、公安部の本省の下には、各省・自治区に「公安庁」、直轄市である北京市、上海市、天津市、重慶市に「公安局」があり、それぞれの筆頭部局である政治警察「敵偵処」が各地域の監視対象への浸透工作を行なっており、その過程で誘導工作も行なっている。

現在の誤情報・偽情報を駆使する誘導工作はサイバー空間が主になっているが、技術的にはサイバー・スパイの応用であり、それももともとはサイバー監視の技術である。中国の情報機関・工作機関の特徴のひとつは、サイバー分野の管理技術が国内監視主導で発展してきたことだ。つまり、サイバー領域での誘導工作はサイバー監視の技術が基になっており、サイバー監視は中国では公安部が主導してきた。現在も、たとえば上海のサイバー・セキュリティ企業である「ランダソフト」や「i-SOON」などが開発した監視ソフトウェアが中国政府・軍のサイバー監視を支えているが、その最大の顧客こそ公安部である。i-SOONは流出した内部資料から、世論操作ツールまで開発したことがわかっている。

世界規模で活動するサイバー民兵を擁する「国家安全部」

他方、国務院（政府）の省庁として対外的なインテリジェンス活動を担当するのは「国家安全部」（略称「国安」）である。国安はいわゆる情報機関だが、防諜や誘導工作も担当する。とくに外国の情報機関の活動を監視しており、その延長で、中国国内で外国人をスパイ活動容疑で摘発する事案が増えてきている。

国安は自前でサイバー活動を行なっているが、国内のハッカー・グループを使ったサイバー・スパイ活動も活発に行なっている。こうした国家機関に所属しないが協力関係にあるハッカー集団を「サイバー民兵」というが、中国には主業務が国家機関・軍の下請けの、いわば国のフロント企業のようなサイバー民兵が非常に多い。たとえば、世界各地で技術情報を狙う「APT41」（別名「バリウム」「ダブルドラゴン」）という有名なハッカー・グループは国安の下請けとみられている。なお、前出・i-SOONの顧客リストには国安もある。

中国軍の筆頭スパイ機関「連合参謀部情報局」

インテリジェンス活動はどの国でも、政府機関と軍の2系統がある。中国軍の筆頭スパイ機関は「連合参謀部情報局」だ。世界各地の在外公館に派遣している駐在武官はもとより、偽装した工

作員を多数投入し、世界規模でスパイ活動をしている。もちろん軍事情報がメインだが、政治情報や経済的利益目的での最新技術情報も狙う。ただし、近年は政治情報や経済技術情報のスパイは国安が主導するようになってきているようだ。

この連合参謀部情報局はヒューミント（人的情報活動）と連動したサイバー・スパイも行なっているが、中国軍のサイバー工作は、ここよりもサイバー戦の専門部隊が主導している。ときおり米国で中国のサイバー・スパイ活動が摘発されることがあるが、たいてい中国本国にいるサイバー部隊のチームである。

「サイバースペース部隊」が軍のサイバー攻撃・防御を主導する

こうしたサイバー・スパイはこれまで「戦略支援部隊」内のネットワークシステム部が担ってきたが、２０２４年４月にその戦略支援部隊が廃止され、同・宇宙システム部は「軍事宇宙部隊」として独立し、ネットワークシステム部は「情報支援部隊」と「サイバースペース部隊」に分割された。情報支援部隊は軍の通信ネットワークの保全（電子戦含む）を主に担当する部隊であり、サイバー戦はサイバースペース部隊が受け継いだ。サイバースペース部隊は、軍のサイバー攻撃とサイバー防御を主導する部隊だが、サイバー攻撃の一部としてサイバー・スパイにも力を入れている。

この部隊にはもともと外国の通信傍受を担当していた要員も多く、その中には対象国の言語や国内事情、習慣などに通じている隊員もいる。サイバー・スパイは単にハッキング技術が優れているだけでは不充分で、フィッシングで標的に浸透する際にいわゆる〝成りすまし〟技術が必要になる。ハッキングで入手する情報を有効に分析するにも、そうした〝文系〟要員が必要だ。もともと戦略支援部隊ネットワークシステム部は、軍情報機関の文系のプロと、理系のサイバー戦のプロを組み合わせて強力なサイバー部隊を作るのが目的のひとつで創設された部隊だったが、現在のサイバースペース部隊はそれを受け継いでいる。サイバー経由の誘導工作にももちろん力を入れているはずである。

このように、中国軍のサイバー工作はサイバースペース部隊が主導しているが、その傘下に多くのサイバー民兵がいる。サイバー・セキュリティ企業の看板を掲げているグループが多いが、大学の研究機関などでも協力関係にあるところは多い。また、中国各地の軍の各戦区司令部、各軍司令部にも情報部があり、そのサイバー部門をサイバースペース部隊は実質的に指揮下に置いている。

なお、旧・戦略支援部隊には、ネット世論操作など誘導工作を主任務とする心理戦部隊「第３１１基地」が、台湾に近い福州に置かれていたが、この部隊もおそらくサイバースペース部隊

に引き継がれている。

誘導工作で大きな力を持つ、党「中央統一戦線工作部」

前述のように、通常、国家の情報機関は政府と軍の2系統で、中国の場合は以上の「公安部」「国家安全部」「連合参謀部情報局」「サイバースペース部隊」になる。ただし、中国の場合、それ以外にも誘導工作で大きな力を持つ組織がある。党の「中央統一戦線工作部」（統戦部）だ。

統戦部は敵の弱体化を目的に海外に友好勢力を獲得する機関で、世界各地でリベラル派のグループに接近し、親中派ネットワークを拡大する工作を実施している。この要員は、友好団体などに身分を偽装して各国に浸透し、人脈を作る。とくにスポーツや文化活動、学術交流、メディア、職能団体などを通じて友好関係を広げる「全国政治協商会議」は統戦部とリンクしている。中国の地方政府の経済団体などによる経済交流も、じつは背後に統戦部がいることが少なくない。

たとえば中国は世界の優れた科学技術の移転を目的に、外国の一流研究者を高額報酬でスカウトする「千人計画」を進めている。表向きは国務院工業情報化部の事業とされているが、背後に統戦部がいる可能性は高い。中国はまた世界各地で中国語・中国文化を広めるために教育機関「孔子学院」を運営している。国務院教育部が運営しているが、統戦部が関与しているのではないかとの疑惑も指摘されている。こうした活動を効果的に進める目的で、工作対象の意識を誘導する情報操作は当然、行なっているだろう。

そもそも中国の親中派スカウト工作は、国務院の「外交部」（外務省）や党「中央対外連絡部」も昔から力を入れてやっている。誘導工作も裏工作以前に大っぴらに党「中央宣伝部」（国務院新聞弁公室と同一）や党「中央対外宣伝弁公室」が行なってきた。これらの各省庁・機関は現在も親中派スカウト工作に邁進しているが、連動して誘導工作も進めているとみていいだろう。

軍の「政治工作部」も誘導工作は主任務だが、対外部門は戦略支援部隊に移管され、現在はサイバースペース部隊が引き継いでいるとみられる。軍政治工作部の現在の活動は国内での誘導工作ということになっているが、なにせ心理戦の専門家集団である。ネット経由であれば国内外の垣根は低く、実際には多少は対外誘導工作をやっている可能性がある。

以上のように、中国では誘導工作に関与しているとみられる組織は多い。工作に携わっている人員も巨大な数になるだろう。これらの工作を各自バラバラに行なうと、場合によっては方針がズレて、足を引っ張り合うようなこともあり得るかもしれない。

そうしたことがないよう、習近平政権は2014年に設立した「中央国家安全委員会」により、各省庁・軍・党組織の機関を統括している。同委員会は国家安全保障に関する最高指導機関だが、

サイバー工作・誘導工作などの新領域についても、習近平自らがしばしば言及し、統合的な工作方針を示して指導している。

大量の人員で膨大な情報を吸い上げ本国で分析する

最後に、中国のインテリジェンス活動全体の大まかな動向について記しておきたい。

中国のスパイ活動は冷戦時代からもともと活発だが、旧ソ連/ロシアと違い、核心情報にアクセスできる獲物を狙い撃ちでリクルートするようなピンポイントなやり方ではなく、情報の一部を持ってそうな多くの人間に広く浅く接触し、膨大な情報をとにかく吸い上げる。そして、本国の巨大な分析機関が分析する。そのため、日本でも米国でも欧州でも、旧ソ連/ロシアのスパイと違い、中国のスパイが摘発される事案はきわめて少なかった。活動が違法でないことが多かったからだ。

現在も、凄まじい勢いで広く浅くサイバー・スパイを行なっている。米国FBIも中国のサイバー・スパイの量の多さを指摘している。大量の人員動員で勝負するメンタリティは、これまで同様でもある。ただし、その技術は格段に向上している。

ひと昔まえ、中国の軍事力について「量は凄まじいが、質に劣る」と軽く見る論調が多かったが、もう完全に古い認識となった。経済力をバックに軍拡をひたすら進めてきた現在の中国の軍事力は、脅威である。現在のサイバー戦力にもそれは言える。

誘導工作では、従来の中国のやり方というのは、ストレートに中国の正当性を宣伝し、西側を批判することが多かった。近年も一時期、外交部報道官の攻撃的なプロパガンダ発信が「戦狼外交」などと呼ばれた。そういう点では、活動主体をごまかしての裏工作が得意な狡猾な旧ソ連/ロシアよりもわかりやすく、素直ともいえる。

しかし、米大統領選などへのロシアの介入を見て、最近は真似を始めているとみられる。自分たちの関与を隠してのネット活動や、中国の正当性主張よりも西側の社会分断の扇動などを狙った誘導工作だ。実際、中国がそうした工作に乗り出した事案が、最近は目立つようになってきた。

巨額の予算と人員動員による誘導工作の脅威

海千山千のロシアに比べ、誘導工作の分野では中国はまだビギナーではある。しかし、中国にはなんといっても巨額の予算がある。前述したように、習近平は盛んに対西側での新領域での活動の強化を掲げている。今後はサイバー・スパイに限らず、中国による誘導工作が格段に強化され、高度化されるものと考え、警戒すべきだろう。

近年観測される中国によるサイバー誘導工作の〝主体〟は不明なケースがほとんどだが、明確に任務として取り組んでいるのは、おそらく国安とサイバースペース部隊だろう。筆者は、国安の場合はサイバー民兵を使うことが多いのではないかと推測している。

また、中国の対外工作の特徴として、リアル社会での影響工作には長い蓄積があり、それとサイバー分野の誘導工作を連携させると高い効果が期待できる。そうしたリアル社会での工作では党中央統一戦線工作部の役割が大きいが、それとサイバー工作を連携させることは当然、考えているだろう。

2024年10月15日配信

米国のデジタルプラットフォーム（DPF）規制と大統領選挙

川口 貴久

ソーシャルメディアやメッセージングアプリといったデジタルプラットフォーム（DPF）と国家の対立はますます先鋭化している。Meta Platform会長兼CEOのマーク・ザッカーバーグ（Mark Zuckerberg）は8月26日付の米下院司法委員会宛の書簡で、バイデン（Joe Biden）政権幹部から新型コロナウイルス感染症（COVID-19）に関する一部コンテンツを検閲するよう「圧力」を受けた、と述べ物議を醸した（※1）。米国外でも、ブラジルではX（旧Twitter）の利用が禁止され、フランス当局はTelegram社CEOのパヴェル・ドゥロフ（Pavel Durov）を逮捕した。

各国政府はDPFが偽情報拡散や犯罪の温床となり、ユーザや他の事業者の諸権利を侵害して

いる（恐れがある）という理由から、またこれら問題に対するＤＰＦ各社の対応とガバナンスが不十分との理由から、ＤＰＦ規制を強化している（※2）。

本稿は米国のＤＰＦ規制の現状と見通しを紹介する。まず米国におけるＤＰＦ規制の争点を俯瞰した上で、特に規制強化が進展し、11月の大統領選挙を経て政策転換の可能性がある競争政策に焦点を当てる。

米国におけるＤＰＦ規制の争点

ＤＰＦ規制は様々な観点から論じられているものの、米国では少なくとも相互に関連する4つの領域が存在する。第一に、ＤＰＦ上で拡散する偽情報や有害情報（外国による影響工作を含む）のコンテンツモデレーションに関する規制である。これは、ＤＰＦ上の情報コンテンツに関する運営事業者の免責を定めた通信品位法２３０条と深く関わる。通信品位法２３０条は「インターネットを創造した26ワード（※3）」とも呼ばれ、２３０条の免責条項があったからこそ、米国のインターネット産業とＤＰＦは発展したとの見方が強い。現代では２３０条は共和党・民主党の双方から批判され、修正法案等も提案されてきたが、表現の自由等を保障する合衆国憲法修正第一条との関係から進展は芳しくない。

第二に、個人データの取り扱いとプライバシー保護に関するものだ。よく知られているように、米国には連邦法レベルでの包括的な個人情報保護規制、つまり日本の個人情報保護法や欧州連合の一般データ保護規則（GDPR）に相当するものは存在しない（※4）。近年では、米国データプライバシー保護法（ADPPA）の成立が期待されたが、不成立に終わった。こうした個人データ保護規制の不在こそが、ＤＰＦの成長を支えてきたことも事実だ。

第三に、ＤＰＦ上の公正な競争環境整備等に関するもので、具体的には反トラスト法（日本の独占禁止法に相当）とその執行である。反トラスト法とはシャーマン法、クレイトン法、連邦取引委員会法等から構成される総称で、取引制限、独占、不公正な競争方法等を禁じる。この規制と執行は、ＤＰＦの競争力に影響を与え、ビジネスモデルを根底から覆す可能性を持つ。

第四に、第三の点とも関連して、ＤＰＦから伝統的メディアの独立性・自律性を保護するための法整備であり、米国では米ジャーナリズム競争・保護法案（JCPA）という形で審議された。具体的には、GoogleやMeta等に対する伝統的メディアの交渉力（掲載価格、掲載条件等）を強化するものだ。米国では法案は成立しなかったが、欧州連合、豪州、カナダでは既に同様の法案が成立している。この他、ＤＰＦ各社の大規模言語モデル開発時におけるニュース収集の制限等もこのカテゴリに含んで良いかもしれない。

バイデン政権下の反トラスト法執行強化と新ブランダイス学派

これらの内、最も規制強化が進展し、米国大統領選挙による政策転換の可能性が大きいものは、特に第三の点である。

まず注目すべきは、バイデン(Joe Biden)政権がその競争政策を従来のものから大きく転換させたことだ(※5)。ただし、それは新法制定や法改正ではなく、反トラスト法の解釈変更や執行強化である。

その背景には、反トラスト法の解釈について従来と異なる考え方を持つ「新ブランダイス学派」の台頭がある。新ブランダイス学派とは、約100年前に米国最高裁判所判事を務めたルイス・ブランダイス(Louis Brandeis)に思想的潮流を持ち、企業の独占行為を厳格にとらえる立場である。新ブランダイス学派によれば、1970年代以降の反トラスト法解釈の主流であったシカゴ学派は市場価格等の「消費者」の厚生基準を重視したが、これは現代の企業独占・寡占の特徴や競争上の優位性を過少評価している。ビッグテック企業が消費者にサービスを安価に(場合によっては無料で)提供していることは、「価格」を重視するシカゴ学派にとっては競争上の問題はないが、新ブランダイス派は、ビッグテック企業が安価ないし無料のサービスを提供する一方で、市場や競争環境を支配している、という。さらに言えば、ビッグテックをはじめとする巨大企業の独占・寡占は純粋に経済学上の問題ではなく民主主義への挑戦であり、反トラスト法の運用は「市民」の厚生基準に立脚すべきである(※6)。

バイデン政権は新ブランダイス学派の専門家を登用した。それを象徴するのは2021年6月、32歳という若さで連邦取引委員会(FTC)委員長に就任したリナ・カーン(Lina Khan)であり、政権初期に約2年間、技術・競争政策担当大統領特別補佐官を務めたティム・ウー(Tim Wu)、司法次官補(反トラスト担当)のジョナサン・カンター(Jonathan Kanter)らである。

そして、バイデン政権の競争政策の焦点の一つはDPFをはじめとするビッグテック企業である。大統領令14036号で「支配的なインターネット・プラットフォーム」に焦点を当て、実際、FTCや司法省反トラスト局等はGoogle、Meta、Amazon、Appleを反トラスト法違反の疑いで提訴してきた。また、FTCと司法省が2023年12月に公表した、新たな「企業結合ガイドライン」最終版では、指針第11項目で「企業結合がマルチサイドプラットフォームを含む場合」を掲げ、競争法上の問題が生じるケースを列挙している(※7)。

ただし司法はシカゴ学派が浸透しているとされ、状況が異なる。企業結合やビッグテック訴訟に関する裁判所の判断・見解とFTCや司法省(新ブランダイス学派)の見解が一致するかは分からない。

米国大統領選挙による影響

米国大統領選挙の結果はＤＰＦを含む競争政策にどのような影響を与えるだろうか。

ハリス（Kamala Harris）政権であれば、予見可能性は高い。基本的にはバイデン政権下のカーン路線を踏襲・強化するだろう。なお反トラスト法の執行機関としてＦＴＣや司法省反トラスト局に加えて、各州の司法長官が規定され、ハリス候補はカリフォルニア州司法長官を二期（２０１１年１月～２０１７年１月）務めた。彼女の任期後であるが、カリフォルニア州もＤＰＦ各社を反トラスト法違反の疑いで提訴している。

他方、トランプ（Donald J. Trump）政権の競争政策は不確実性が大きい。なぜなら、共和党内では既存のカーン路線に対して二つの考え方があるからだ。

一つは共和党の伝統的な立場であり、連邦政府の権限や企業活動の規制は縮小すべきとの考え方で、カーン路線を支持しない。この立場は新ブランダイス学派が（競争による）価格への影響のみならず、労働問題等に焦点を当てることを「左派」的と批判する。事実、トランプ陣営の公約の一つは、ＦＴＣの権限縮小である。トランプ政権が樹立されれば、ＦＴＣや連邦通信委員会（ＦＣＣ）等の独立規制機関を「合衆国憲法に従い、大統領権限下に戻す。こうした機関が、（立法・行政・司法に次ぐ）第４の政府機関として独自に規則や決定を発出することは許されない。…中略…我々は、諸機関が検討している全ての規制をホワイトハウスに提出することを要求する」という（※8）。

もう一つの立場は、カーンＦＴＣ委員長を支持する保守派・共和党議員の立場、いわゆる「カーンサバティブ（Khanservatives）」である。「カーンサバティブ」とはカーンＦＴＣ委員長と保守主義者（conservatives）をあわせた造語であり、「より若く、よりトランプ的な傾向があり、自由な市場に疑問を持ち、大企業を有権者にとって敵対的な存在と見なす（※9）」。ロイター通信によれば、カーンサバティブな連邦議員はミズーリ州選出のジョシュ・ホーリー（Josh Hawley）やフロリダ州選出のマット・ゲイツ（Matt Gaetz）下院議員だが、最も影響力のある人物はＪ・Ｄ・ヴァンス（James David Vance）副大統領候補である。ヴァンス副大統領候補は現行のＦＴＣ路線に同意し、２０２４年２月にはＸ（旧Twitter）上で「Googleを解体する時がきた」と述べた。トランプ政権の競争政策は今後、「カーンサバティブ」がどれほどの影響力を持つかに依存するだろう。

このように米国ではいくつかの領域でＤＰＦ規制が議論されている。その中でも、ＤＰＦを含む反トラスト法関連規制はバイデン政権下で強化された。政権の反トラスト法の解釈見直しと執行強化の焦点の一つはＤＰＦであったと言っても過言ではない。こうした動向が次期政権でも継

続するのか、あるいは変化が生じるのかは大きな注目点である。

2024年10月15日配信

参考

※1 Colin McCullogh, "Mark Zuckerberg says Meta was 'pressured' by Biden administration to censor Covid-related content in 2021," CNN (August 27, 2024).

※2 日米欧の概況は、川口貴久「民主主義国家とデジタルプラットフォーム規制」地経学ブリーフィング、No.199(2024年4月10日)。

※3 Jeff Kosseff, The Twenty-Six Words That Created the Internet (Cornell University Press, 2019).

※4 正確に言えば、米国には金融、医療、児童等の特定業界・領域に関する連邦レベルでの包括的個人データ保護法やカリフォルニア州消費者プライバシー法(CCPA)に代表される州レベルでの包括的個人データ保護州は存在するが、連邦レベルでの包括的な個人データ保護法制は存在しない。

※5 以降の記述は、「競争政策」、佐橋亮(監修)、川口貴久、柴田慎士、八代慈瑛、覃文婷、高橋あゆみ「米中関係2024-2028」(東京海上ディーアール株式会社、2024年10月1日公開)、18〜19頁を大幅に加筆したものである。

※6 新ブランダイス学派に関しては、ティム・ウー(秋山勝訳)『巨大企業の呪い：ビッグテックは世界をどう支配してきたか』(朝日新聞出版、2021年)を参照。

※7 Merger Guidelines, U.S. Department of Justice and the Federal Trade Commission (December 18, 2023), pp.23-26. なお新ガイドラインの2010年版からの主な修正点の一つは「市場集中度(market concentration)」に関する基準の変更であり、今後、調査対象・違法となる結合が増加する可能性がある。

※8 "Agenda47: Liberating America from Biden's Regulatory Onslaught," Agenda 47, (April 16, 2023).

※9 Molly Ball and Brody Mullins, "Biden's Trustbuster Draws Unlikely Fans: 'Khanservative' Republicans," Wall Street Journal (March 25, 2024). とはいえ、保守派や共和党内での「カーンサバティブ」に対する批判は根強い。Joseph V. Coniglio, "'Khanservatives' Are Wrong About Big Tech," Information Technology and Innovation Foundation (May 1, 2024).

※10 Jody Godoy, "Trump VP pick supports Big Tech antitrust crackdown," Reuters (July 16, 2024).

※11 JD Vance(@JDVance) posted on X that "Long overdue, but it's time to break Google up" on February 23, 2024.

●EU選挙で偽情報の組織的な大洪水に飲まれたX　7月19日
●トランプ暗殺未遂事件で陰謀論はどれくらい広がっているのか？　7月18日・7月20日更新
●陰謀論に特効薬はないという論文　7月18日・7月19日更新
小児病院へのミサイル攻撃にともなう反ウクライナ・ナラティブ拡散　7月17日
●トランプ暗殺未遂で広がる共和党と民主党の陰謀論と分断の構図　7月16日・7月19日更新
●TikTokにAIコンテンツファームの大規模な投稿　億単位の再生　7月15日
●ウクライナは情報統制と誤・偽情報対策の貴重な先行事例　7月14日・7月22日更新
●ファクトチェックアワード2024発表　7月12日
●ゼレンスキーの妻がブガッティを購入したというデマがグーグルトップに　7月12日・7月13日更新
●陰謀論者かつ名門出身で知られるケネディ・ジュニアが大統領になったら政府の機密文書を公開すると発言　7月11日
●ライブ配信されたインディアナ州銃乱射事件の動画が、XやFacebookに拡散　7月10日
●ロシアによるフランス選挙への干渉　7月10日
●フランスの極右政党が選挙戦でAIを活用　7月9日
●米国に広がる誤・偽情報対策の後退 SIOは選挙に関する研究を中止　7月7日・7月10日更新
●トランプの危険な「ほしいものリスト」Project2025　7月5日
●米国務総省がコロナ禍で中国の弱体化を狙って反ワクチンのデジタル影響工作　フィリピンで多数の被害者！？　7月4日
●メディア偏向検知システム公開　7月3日・7月6日更新
●ChatGPTに提携先へのリンクを張らせるのはOpenAIにも無理だった　7月2日・7月16日更新
●世界のファクトチェック団体などが参加する国際サミットGlobalFact 11 においてサラエボ宣言を発表　7月1日

●ファクトチェックはメディア贔屓のトラフィックを稼ぐネタなのか？　6月30日・7月3日更新
●NewsGuardの一連の生成AIリスクに関する記事の意図　6月30日・8月4日更新
●陰謀論的思考の予測因子を解析したグラフ　6月28日・6月30日更新
●生成AIで進化するアメリカの過激派　6月27日・7月12日更新
●AfDがTikTokでドイツ最強政党になる　6月25日・7月1日更新
●捏造セレブ発言を使ったロシアのドッペルゲンガー・キャンペーン　6月25日・6月30日更新
●欧米に広がる青少年をSNSから保護する動き　今度は米公衆衛生局長官が発言　6月25日・6月30日更新

催　8月28日
●トランプ銃撃事件後、生成AIによる偽・誤情報が拡散　デジタル・フォレンジック・リサーチラボがレポート　8月28日
●Telegramに増殖する分散型コレクティブ・ネオファシストTerrorgramをISDが分析　8月27日
●英暴動は極右の結束を強めた　新しい形の暴力への対抗策をISDが提案　8月24日
●英国の図書館で進む「検閲」によるLGBTQ+関連書籍の排除　8月23日
●米国選挙へのイランの干渉についてODNI、FBI、CISAが共同声明　8月22日
●破天荒は親譲り Grokはデマ画像生成に最適　8月21日
●Meta2024年Q2の脅威レポートを公開　パーセプション・ハッキングを警告　8月20日・8月21日更新
●トランプが撃たれても「本日晴朗ナレドモ波高シ」のQアノン　8月20日　8月21日
●TikTokでは中国政府への批判は抑制されているという調査結果　8月17日
●アイルランドで極右が台頭　反中絶運動が広がる　8月15日
●「あの愚か者は唯一のチャンスを逃した」トランプ暗殺についてのオバマのディープフェイク音声が拡散　8月14日
●マイクロソフト脅威分析センターがイランによるアメリカ選挙への干渉をレポート　8月10日
●英暴動をめぐりSNSへの批判強まる　8月9日
●トランプ暗殺未遂事件の混乱下で、中国が「バランスの取れた」印象操作作戦を展開　8月8日
●イギリスの暴動はロシアの情報工作が発端だった？　8月8日・8月10日更新
●パリ五輪を貶めるロシアの活動　8月7日
●イギリス全土に広がった暴動　警察では歯が立たず常備軍設置　8月6日

●イギリス各地を暴力に巻き込んだ反体制ポスト組織ネットワーク　8月5日
●ISDによるTikTokでのネオナチ系ネットワークの調査報告　8月5日・8月8日更新
●日本ファクトチェックセンターが認定試験を開始　8月5日
●サウスポートの暴動と報道　8月4日・8月5日更新
●トランプ暗殺未遂事件直後に親中派ネットワークが活発に活動　8月2日
ロシアに踊らされる米政府、調査機関、メディア　罠に引きずり込まれる日本政府　8月1日
●アメリカのリベラル、民主党が拡散する誤・偽情報　7月31日
●TikTokが米国利用者の銃規制、中絶、宗教などセンシティブな意見を収集　米司法省　7月30日
●イランによる親パレスチナ・反イスラエル影響工作を、アメリカ国家情報長官が警告　7月29日
●ファクトチェックは重要な事実を隠すことがあるというコロンビア・ジャーナリズム・レビューの指摘　7月28日
●ハリス大統領候補をめぐるロシアの誤・偽情報　7月27日
●ドイツの若い有権者を極右政党へ誘導するTikTokのアルゴリズム　7月26日
●中国のNGOファクトチェック団体「China Fact Check」　7月25日
●ビッグテックにハブられるEU　7月24日
●アルカイダやISがTikTokの「オリジナルサウンド」を使ってメッセージを拡散　7月24日
●絆は弱いほうが強い？「よく知らない人が共有したフェイクニュース」は信頼されやすい　7月23日
●ニュースの見出しに使われる動詞によって、読者が客観的と感じるかどうかが変わるという論文　7月22日
●トランプ暗殺未遂事件の陰謀論について質問された10の代表的な生成AIモデルは57%の確率で検知も反証もできなかった　7月19日・7月22日更新

変更　9月12日
●米の対応の効果は限定的「ロシアの影響工作は重要だが、国内問題もきわめて重要だ」ISDがNBCに語る　9月11日
●データボイド脆弱性の危険性　「偽・誤情報の棚卸し2024」第3回　9月11日・9月13日更新
●各国で進むSNSプラットフォームへの取締強化は怠惰な慣習にすぎなかった　9月10日
●誤情報に対抗するための「信頼の構築」とは？　「偽・誤情報の棚卸し2024」第2回　9月9日・9月13日更新
●米大統領選を前にロシアの選挙干渉に制裁　危ういバイデンの選択　9月6日・9月11日更新
●メディア報道で拡散する偽・誤情報　「偽・誤情報の棚卸し2024」第1回　9月6日・9月13日更新
●Data & Societyによる「偽・誤情報の棚卸し2024」　9月6日・9月13日更新
●グローバルサウスに広がる極右のオンライン脅威　9月5日
●Graphikaが米選挙をターゲットにしたスパモフラージュをレポート　9月4日・9月5日更新
●インドネシアの選挙法改正案と抗議デモ　声をあげるVtuberたち　9月4日
●SNSで行政の透明性を実現する3つのモデル　オランダの調査から　9月2日
●テックに強い過激な白人至上主義者グロイバー軍団　9月1日
●ロシア・ウクライナ戦争の偽・誤情報の42％はTelegramから　8月31日
●グーグル広告で収益をあげるインドのデマサイト　8月30日
●政府の秘密のエージェントやマイクロ波の標的となった人びと＝TIsのネットコミュニティをISDが分析　8月30日
●米選挙目前、共和党に送ったザッカーバーグのメッセージ　8月29日
11月3，4日に日本初の偽情報対策ハッカソンをCode for Japanが開

しい措置　9月28日
●20年間しぶとく生きのびたアルカイダのデジタル生態系をISDがレポート　9月27日
●ベリングキャットが新しいOSINTツールキットを公開　9月26日
Xがイーロン・マスク買収後、初めての透明性レポートを公開　9月26日
●子供の貧困が示す「かつて裕福だった国」の末路　9月25日
●Facebookに選挙広告を掲載できる偽IDのアカウント世界中でセール中　9月21日
●陰謀論者が我に返るAIチャットボット？　9月20日
マイクロソフトMTACのレポートは、偽・誤情報の「戦場の霧」で迷走　9月19日
●ファクトチェック団体とメディアをターゲットにした「オペレーション・●オーバーロード」のアップデート　9月18日
●Metaがロシアの国営メディアを排除　9月18日
●選挙への関心の高まるほど、情報を正しく評価しなくなるという報告　重要なのは動機だった　9月18日
●TikTokとメッセージアプリで拡大する10代の分散型テロリスト　9月17日
●ISDのレポート　TikTokで白人至上主義者はVIP待遇　9月15日
●米国務省がロシアのRTによる影響工作とサイバー攻撃、軍事装備調達を暴露　9月15日
●米司法省が訴追したテネット・メディアでは、なにが語られていたのか　9月14日
●米NewsGuardコメンタリーが指摘するロシアの雇われバカと役に立つバカ、ただのバカ　9月13日
●極右の偽情報が拡大した本当の理由　「偽・誤情報の棚卸し2024」第4回　9月13日
●Telegramを中心に活動していた過激派コレクティブTerrorgramのリーダーが逮捕　9月12日
●米CISAが偽・誤情報対策を信用できる情報へのアクセス確保に

これまでのINODS UNVEILの記事一覧

寄稿記事

日付は配信日。すべて2024年。

●陰謀論と愛着スタイル（藤田 直哉） 9月17日
●誤情報に対処するより、正しい情報を支持する方が効果的であるという論文（P.N.G.） 9月13日
●新潮流になるか？AIにより生成されたペルソナを活用した影響工作（岩井 博樹） 9月10日
●偽・誤情報対策が開く思想統制への道（藤代 裕之） 8月27日
●メディアの否定的な報道がSNSポリシーに与える影響についての論文（P.N.G.） 8月25日
●中国人民解放軍の改編にみる新領域における戦略方針（岩井 博樹） 8月20日
●共感格差（データをいろいろ見てみる） 8月13日・8月14日更新
●サブカルチャーと情報工作（藤田 直哉） 8月6日
●ロシアのサイバー攻撃を通したシグナリング：KADOKAWA事件の「B面」（齋藤 孝道） 8月2日
●検証された脅威や効果はない？ 誤・偽情報、認知戦、デジタル影響工作についての過去の研究（一田 和樹） 7月31日・8月25日更新
●右派左派ともに政権から離れるほど陰謀論を信じやすくなる 26カ国約10万人調査のnature論文（P.N.G.） 7月30日
●ALPS処理水放出ネガティブキャンペーンに隠された狙い～BRICS影響拡大戦略とサイバー空間での情報戦～（齋藤 孝道） 7月29日
●迷走する政府の偽・誤情報対策（藤代 裕之） 7月23日
●米国の主要放送メディアは誤情報の問題について党派性のある議論でプラットフォームをやり玉にあげているという論文（P.N.G.） 7月22日
●誤・偽情報、デジタル影響工作、認知戦を知るうえで読むべき定期レポート（2） NewsGuardのReality Check（一田 和樹） 7月2日・7月17日更新
●安全保障の新たなフロンティア：デジタル影響工作を読み解く（齋藤 孝道） 6月30日・8月15日更新
●誤・偽情報、デジタル影響工作、認知戦を知るうえで読むべき定期レポート（1） Metaの四半期脅威レポート（一田 和樹） 6月30日
●安全なデジタル社会を作り、日本を前進させ続けるエルテス社（一田 和樹） 6月30日・7月6日更新

ニュース・海外論文レポート紹介記事

INODS UNVEIL ニュース担当
日付は配信日。すべて2024年。カッコ内は更新日。

●ロシアのドッペルゲンガー実施企業Social Design Agencyの2.4GB漏洩文書 10月2日
●公人標的のディープフェイクは1年間で38カ国82件 Inskit Groupが発表 9月30日
●米大統領選に干渉する中国のSpamouflageのネットワーク 9月30日
●世界でもっとも有名な情報源評価データベースのNewsGuardのDBを検証した論文 9月29日
●米に蔓延する警戒主義を象徴するアドビ社の大統領選と偽・誤情報についてのレポート 9月29日
●米FTC、AI取締強化の「Operation AI Comply」を発動し、5社に厳

取材。NTTレゾナントに転職し、ニュース編集やNTT研究所のR&D支援（gooラボ）、新サービス開発などを担当した。2013年から法政大学社会学部メディア社会学科准教授、2020年に教授。日本ジャーナリスト教育センター（JCEJ）代表理事。著書に『ネットメディア覇権戦争　偽ニュースはなぜ生まれたか』（光文社）、編著に『フェイクニュースの生態系』（青弓社）などがある。

黒井 文太郎

軍事ジャーナリスト。NY、モスクワ、カイロを拠点に紛争地多数を取材。帰国後、月刊『軍事研究』特約記者、『ワールド・インテリジェンス』編集長などを経て現職。現在、『軍事研究』誌などで国際紛争全般をカバーしており、情報戦分野の執筆も多い。著書・編共著に『イスラムのテロリスト』『北朝鮮に備える軍事学』『日本の情報機関』（以上、講談社）、『生物兵器テロ』『プーチンの正体』（以上、宝島社）、『インテリジェンス戦争?対テロ時代の最新動向』（大和書房）、『日本の防衛と世界情勢』（秀和システム）など。近刊は『工作・謀略の国際政治?世界の情報機関とインテリジェンス戦』（ワニブックス）。

川口 貴久

1985年福岡生まれ。東京海上ディーアール株式会社ビジネスリスク本部主席研究員、マネージャ。専門は国際政治・安全保障、リスクマネジメント。修士（政策・メディア）。主な著作に『ハックされる民主主義：デジタル時代の選挙干渉リスク』（土屋大洋との共編著、千倉書房、2022年）等多数。この他、一橋大学法学研究科非常勤講師（2022年4月～現在、ただし4-9月に限る）、慶應義塾大学グローバルリサーチインスティテュート（KGRI）特任准教授（2023年10月～2024年2月）、「サイバー安全保障分野での対応能力の向上に向けた有識者会議」構成員（2024年5月～現在）等。※2024年9月現在。

データをいろいろ見てみる

主にSNSの分析を個人の趣味として行っている。X(旧twitter)などを中心に分析しているがその他マスメディアが何に言及したかなどの調査をしている。
興味があるのは、マスメディアによるアジェンダ設定とその影になる誰かの問題は社会問題にならないのか？という設問である。
計算機自体が好きで、特に発表するあてもないデータを集計しては喜んでいる。
X（旧ツイッター）アカウントは shioshio38 。お気軽にフォローしてもらえると嬉しい。今回紹介した共感格差は、こちら https://shioshio3.hatenablog.com/entry/2022/09/03/191426
で全文が読める。

●INODS UNVEIL ニュース担当

江添 佳代子、miyajima、一田 和樹

●INODS UNVEIL Report Reviews担当

P.N.G

2003年生まれ。神戸生まれ神戸育ちの神戸っ子。非軍事的な分野における安全保障に対して広く興味を有しており、現在は偽情報及び誤情報が民主主義に齎す影響を一橋大学グローバル・ガバナンス研究センター(GGR)において研究中。専攻以外では、ヴァイマル共和政期のドイツや国際政治・国際法について独自に勉強している。
X(旧Twitter)アカウントは @pax_silverna、主に自分が書いた胡乱な文章のことをつらつら呟いているが、稀に自身の専攻やその外で興味を持っていることについて四方山話を話しているので、気軽にフォローしていただきたい。

●INODS UNVEIL編集部

一田 和樹、小林 愛、平湯 あつし

新領域安全保障研究所の概要

正式名称　株式会社新領域安全保障研究所
略称　INODS（アイノッズ）
設立　2024年（令和6年）5月28日
代表取締役　齋藤 孝道

メンバー

●代表取締役

齋藤 孝道

明治大学理工学部情報科学科・教授、博士（工学）。明治大学サイバーセキュリティ研究所・所長。レンジフォース株式会社・代表取締役。専門は、情報セキュリティ技術全般。特に、デジタル影響工作、Web追跡技術、AI技術応用。著書:『マスタリングTCP/IP情報セキュリティ編・第2版』（オーム社）、『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）。

●UNVEIL担当

一田 和樹

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。代表作として『原発サイバートラップ』（集英社）、『天才ハッカー安部響子と五分間の相棒』（集英社）、『フェイクニュース　新しい戦略的戦争兵器』（角川新書）、『ネット世論操作とデジタル影響工作』（原書房）など。
10年間の執筆活動で40タイトル刊行した後、デジタル影響工作、認知戦などに関わる調査を行うようになる。

●リサーチフェロー

岩井 博樹

2000年より株式会社ラック、2013年よりデロイトトーマツにおいてセキュリティ分野の業務に携わり、これまでセキュアサイト構築、セキュリティ監視、フォレンジック、コンサルティング、脅威分析などを担当する。現在は、脅威分析や安全保障分野を中心とした戦略系インテリジェンス生成を専門とするサイントを設立し、主にアジア諸国を中心に日夜分析に勤しんでいる。
経済産業省情報セキュリティ対策専門官、千葉県警察サイバーセキュリティ対策テクニカルアドバイザー、情報セキュリティ大学院大学客員研究員などを拝命する。
著書に『動かして学ぶセキュリティ入門講座』、『標的型攻撃セキュリティガイド』、『ネット世論操作とデジタル影響工作』（共著）などがある。

藤田 直哉

1983年、札幌生まれ。批評家。博士（学術）。日本映画大学准教授。著書に『現代ネット政治＝文化論』『攻殻機動隊論』『虚構内存在 筒井康隆と〈新しい《生》の次元〉』『シン・ゴジラ論』『新海誠論』（作品社）『新世紀ゾンビ論』（筑摩書房）『娯楽としての炎上』（南雲堂）『シン・エヴァンゲリオン論』（河出書房新社）『ゲームが教える世界の論点』（集英社新書）、編著に『３・１１の未来』（作品社）『地域アート』（堀之内出版）『東日本大震災後文学論』（南雲堂）など。１９９５年からインターネットに触れ、「ネット万華鏡」（共同通信）「ネット方面見聞録」（朝日新聞）などネット時評も担当。
https://x.com/naoya_fujita

藤代 裕之

法政大学社会学部メディア社会学科教授
広島大学文学部哲学科卒業、立教大学21世紀社会デザイン研究科前期課程修了。徳島新聞社で記者として司法・警察や地方自治などを

新領域安全保障研究所2024

2024年10月24日　発行
新領域安全保障研究所　UNVEIL編集部　編
発行者　齋藤 孝道

株式会社新領域安全保障研究所
info@inods.co.jp
150-0042 東京都渋谷区宇田川町3番7号
ヒューリック渋谷公園通りビル5F-95
電話番号　03-6386-5966