NIDS 防衛研究所 National Institute for Defense Studies
NIDSコメンタリー
第 442 号　2026 年 7 月 3 日

認知戦における「修正ナラティブ」と政府信頼性

――社会的レジリエンスの観点から

先進領域研究部防衛基盤研究室　主任研究官　牛若　健悟

はじめに

2022 年 2 月、ロシアはウクライナへの全面侵攻を開始したが、認知戦はそれ以前から始まっていた。侵攻の数ヶ月前からロシアは正当化ナラティブを流布し、侵攻直前にはウクライナ政府の公式サイトには「お前たちの個人情報は公開された。最悪を恐れよ」という脅迫メッセージが表示されるサイバー攻撃が行われた[1]。これはロシアが仕掛けたサイバー攻撃と心理戦の組み合わせであり、実際の戦闘の前に“認知領域”では既に開戦していたといえる。

認知領域における現在の日本の対策を見ると、政府が一体となって対処する運用体制は未だ確たるものとはなっておらず、SNS 上での偽情報拡散等への備えは十分とは言えない。こうした状況に対し、国家安全保障戦略（2022 年 12 月閣議決定）においては、「我が国周辺で偽情報の拡散等を通じた情報戦が恒常的に生起し、平時と有事の境目を曖昧にしている」[2]とした脅威認識を踏まえ、政府は 2026 年 5 月、インテリジェンスの司令塔機能を担う「国家情報会議」と、内閣情報調査室を発展的に解消して設置される「国家情報局」を定めた国家情報会議設置法を成立させた[3]。これは外国情報活動への対処を含むインテリジェンス機能の強化として位置付けられ、制度整備の観点からは一歩前進といえる。しかしながら、認知戦対策の実務においては、現状では偽情報が拡散した後にその真偽を確認する「ファクトチェック」に重点が置かれている印象は否めない。認知戦の目的や効果を考慮した場合、「情報の真偽を判別し、正しい情報を出せるか」という問いだけでは不十分であり、より本質的には、「その情報が社会に受け入れられるか」、すなわち「社会に受け入れられるだけの発信者の信頼と検証の基盤を平時から積み上げられているか」という点が問われる。

本稿の主眼は、この問いに正面から向き合うことにある。昨今の事例としての台湾とウクライナの経験は、貴重な手がかりであり、本稿では両事例を検討した上で、日本が取り組むべき課題を整理したい。

1　認知戦における「修正ナラティブ」の重要性

（**1**）認知戦は「情報の量」ではなく「認識の形成」を争う

偽情報対策の議論では、しばしば「いかに速く、いかに多くの訂正情報を出すか」という量的競争の発想に陥りがちである。しかし、認知科学と情報行動の研究が示すように、訂正情報を出すだけでは十分ではない。

訂正情報があっても、偽情報の影響は直ちには消えない。心理学では「真実の錯覚効果（Illusory Truth Effect）」として知られているが[4]、繰り返し見聞きした情報は、その真偽に関わらず、脳が「馴染みのある情報＝正しそうな情報」と処理してしまう傾向がある[5]。つまり、偽情報が先に大量に拡散されると、その後に訂正情報を出しても人々の記憶には偽情報の方が残ってしまう。

訂正の効果を高める要点としては、誤りの理由を説明し、事実を踏まえた代替説明を与え、適切に反復することである。つまり、単なる「それは嘘だ」という否定だけでなく、「では実際には何が起きているのか」という納得できる説明を繰り返し提示できるか、ということである[6]。

さらに、訂正情報の拡散それ自体が予期せぬ影響を持つ場合もある。COVID-19 初期のトイレットペーパー不足を分析した東京大学院飯塚隆介教授らの研究では、デマそのものよりも訂正情報の拡散が人々に不足の存在を認識させてしまい、結果として、（政府として抑制したかった）購買行動を刺激した可能性を示している[7]。

つまり、認知戦は情報量の多い方が勝つゲームではなく、どのような「認識の方向性」を社会の中に根付かせるか、という「認識形成の戦い」といえる。

（**2**）なぜ「修正ナラティブ」が必要なのか

上記を踏まえると、政府に求められる対策は、単純な「否定の繰り返し」ではなく、事実・意味づけ・行動指針を一体として提示する「修正ナラティブ」の構築であるといえる[8]。

「ナラティブ（物語）」という言葉は一般的にはあまり認識されていないかもしれないが、人間は事実の羅列よりも「物語」として提示された情報の方を理解しやすく記憶に影響を与えやすいことが示されている[9]。認知戦を仕掛ける側はこの性質を知り抜いた上で、「ロシア系住民はウクライナ政府に迫害されている」（ロシアのウクライナ侵攻前の宣伝）、「米国は台湾を捨てる気だ」（対日認知戦の典型的想定文言）といった、感情に訴える強力な物語を創り送り込んでくる。

こういったナラティブに対抗するには、同じ「物語の言語」で応じることが有効と考えられ、「それは嘘だ。事実はこうだ」という否定に加えて、「では私たちは何のために、何と戦っているのか」という意味の軸を示し、「だから今、国民として何をすればよいのか」という具体的な行動の指針まで一体で提示する、それが修正ナラティブである。

（**3**）「誰が語るか」が認知戦の帰趨を左右する

もっとも、修正ナラティブがいくら優れていても、「誰が語るか」によって、その受容度は劇的に変わる。

人は情報の内容を丁寧に吟味する余裕がないとき、「誰が言っているか」という発信者への信頼感を手がかりに真偽を判断しようとする[10]。政府への信頼が高い社会では、有事の際に政府が「これは偽情報です」と発信すれば、多くの国民はその判断を受け入れる。しかし政府不信が根強い社会では、その政府の発信が「政府がそう言うなら、出回っている情報はむしろ本当のことかもしれない」と疑われかねない。

OECD の 2023 年調査によれば、日本の中央政府に対する市民の信頼度は 33.6%であった[11]。これは先進国平均（38%台）と比較しても高水準とは言い難い。「どうせ政府は本当のことを言わない」という諦念が広がる社会では、たとえ政府が真実を語っても、それが認知戦の防衛壁として機能しにくい。

つまり、認知戦への耐性は、ファクトチェックを行う技術的な対策だけでは完成せず、平時から積み上げられた「発信者（政府）への信頼」こそが、偽情報に惑わされない社会の最大のレジリエンスになり得るのである。

2　台湾・ウクライナに見る「信頼」の役割

（**1**）台湾の事例――分散型の検証基盤が守ったもの

①　制度的な防護線の整備

台湾は中国による認知戦と長年にわたって向き合ってきており、その経験から学んだ最大の教訓の一つは、「政府単独では認知戦に対抗できない」というものである。

制度的な基盤として、台湾は「反滲透法」を整備している。これは、外国の敵対勢力による政治献金・選挙介入・ロビー活動などを規制する法律で、外からの干渉に対する制度的な防護線として機能する[12]。これに加えて、国家安全機関（NSB）は外国発の影響工作を監視・分析し、偽情報の主要手口（候補者を

標的とした偽ミーム・動画の大量投稿、台湾市民へのなりすまし等）を定期的に公表することで、市民への警戒喚起を担っている[13]。

② **2024** 年総統選挙での「分散型検証」の実力

2024 年 1 月の台湾総統選挙は、台湾の認知戦対処能力の「実地試験」の機会となった。選挙直後から、「投票集計不正を示唆する切り取り動画」や「選挙は操作された」という風説が中国発・国内発の双方から拡散した。台湾当局によれば、中国由来の「虚偽または偏向した情報」の検知件数が前年比 60%増の 216 万件に上ったと公表している[14]。

しかし、投票の正統性は揺らがなかった。AP 通信は「台湾が中国発・国内発の偽情報を押し返し、選挙の完全性を維持した」と報じた[15]。その鍵を握ったのは、政府単体の力ではない。台湾ファクトチェックセンター（TFC）、MyGoPen、Cofacts という三つの民間ファクトチェック団体と、中国の影響工作を調査・可視化する研究機関 Doublethink Lab が、メディアやプラットフォームと連携して偽情報検証の主軸を担い、政府はその成果を公式発信として活用する形となっていたことが挙げられる[16]。

③ 平時からの「信頼の蓄積」とプレバンキングの実装

台湾の成功は選挙時の対応だけで成し遂げられたわけではない。デジタル大臣（当時）オードリー・タン氏らが推進した、市民がオンラインで政策立案に参加できるプラットフォーム「vTaiwan」に代表される市民参加型のデジタル民主主義、透明性の高い行政データの公開、デジタル時代の市民リテラシー教育など、平時からの参加型ガバナンスの積み重ねが、政府への信頼形成に寄与したと指摘されている[17]。

また、台湾は“事後の訂正”となるファクトチェックだけでなく、「プレバンキング（prebunking：事前免疫形成）」の手法も積極的に採用していることも重要である。プレバンキングとは、偽情報に実際に接触する前に、典型的な手口や操作パターンをあらかじめ市民に知らせることで、心理的な「抗体」を形成するアプローチである。2024 年総統選を前に、台湾のメディア・ファクトチェック機関・選挙当局は、中国発の偽情報が選挙期に使いがちな典型的ナラティブ（「投票は操作される」等）を予測し、その手口を事前に市民と共有した。これにより、実際にそうした偽情報が拡散されても、多くの市民は予め「免疫」を持った状態で接することができ、偽情報に踊らされる可能性を低減した[18]。また、台湾は教育省が 2023 年に「デジタル時代メディアリテラシー教育白書」を策定し、批判的情報リテラシーを 12 年間の国民基礎教育に組み込む方針も打ち出しており[19]、プレバンキングを社会全体で制度化しようとする意図を明確に示している。

（**2**）ウクライナの事例――見えるリーダーが保った「国家意思の一体性」

① 「情報の戦場」は軍事行動の前から始まっていた

ロシアは 2022 年 2 月の侵攻に先立ち、数ヶ月前から認知戦を展開していた。「ウクライナ政府はネオナチに支配されている」「東部ではロシア系住民に対するジェノサイドが起きている」という正当化ナラティブを繰り返し発信し、軍事行動への「大義」を関係国や国際世論に植え付けようとした[20]。そして、侵攻直前にはウクライナ政府ウェブサイト約 70 か所が改ざんされ[1]、市民に心理的な恐怖を植え付けるサイバー攻撃が重なり、情報空間は混乱に陥った。

侵攻開始後も認知戦は続き、「ゼレンスキー大統領は国外逃亡した」という偽情報が SNS で拡散し、3 月には大統領が兵士に武器を置いて投降するよう呼びかける偽のディープフェイク動画がウクライナのニュースサイトに掲載・拡散された[21]。

② 「見える指導者」が強力な修正ナラティブになった

これに対するウクライナ側の最も効果的な対応は、政府の公式声明よりも、ゼレンスキー大統領自身の行動だった。大統領が首都中心部で「私はここにいる。首都キーウにいる」と語り掛けるスマートフォンの自撮り動画は、「政府は逃げていない」という最重要事実を、いかなる長文の公式発表よりも雄弁に証明し、結果としてこの発信は強力な修正ナラティブとして機能した[22]。

ディープフェイク動画への対応も素早かった。テレビ局、SNS プラットフォーム、国防省、そして大統領本人が即座に「この動画は偽物だ」と発信し、被害の拡大を最小限に抑えた[23]。大統領が侵攻前から「ロシアがディープフェイクを使ってくる」と警告していたプレバンキングも、市民の免疫形成に貢献したとされる[24]。

③ 制度・同盟・社会との「接続」が修正ナラティブを強化した

ウクライナの対応が優れていたのは、可視的なリーダーの発信を制度・同盟・社会の仕組みと組み合わせていた点だ。

ロシアによる全面侵攻（2022 年 2 月）に先立つ 2021 年 3 月、ウクライナは国家安全保障防衛評議会の下に「対偽情報センター」を設置するとともに、「戦略的コミュニケーション・情報安全保障センター」も同年に立ち上げた[25]。これらの機関は、戦時には国際発信の窓口として機能を拡充した。ウクライナは 2024 年 6 月、米国・ポーランドをはじめ 10 カ国以上の政府と NATO・EU が参加する「Ukraine Communications Group」を立ち上げ、ロシアの偽情報への国際的反駁能力を高めた[26]。また、欧米諸国が自国の情報機関の保有するロシア侵攻に関する機密情報を異例の速さで公開し[27]、ロシアからの情報発

信に先手を打ったことも、国際世論でのナラティブ形成に大きく貢献した。

さらに国内社会においては、Telegram が主要な情報インフラとして広く利用される一方で、国家機関の公式端末での Telegram 使用を 2024 年に制限したことだ[28]。「便利であるが安全ではない」という判断を、利便性の圧力に屈せずして下した。Telegram はロシア系の暗号化通信アプリであり、通信内容がロシア情報機関に傍受・解析されるリスクが指摘されていた。国家機関の内部通信が Telegram を通じて漏洩すれば、作戦・人員情報が敵側に渡るだけでなく、虚偽の命令や撹乱情報を注入される経路ともなりかねない。内部からの認知的撹乱リスクを遮断するためのこの判断は、認知戦対処における組織的合理性を持つものといえる。

ここまで見てきたように、ウクライナの教訓が示す危機時の信頼とは、ゼレンスキー氏の「人気」や「好感度」の問題ではない。所在確認（「私はここにいる」）・継続発信（繰り返す自撮り動画）・代替説明（偽動画への即時反証）・同盟との反証連携（Ukraine Communications Group）という行為を組み合わせて初めて、偽情報に対抗できる修正ナラティブの基盤が形成されるのである。

（**3**）両事例から見えてくる共通原則

台湾とウクライナの経験は、認知戦への対処において共通する三つの原則を浮かび上がらせる。

第一に、「政府単独型」の対応は限界がある。台湾では、政府の国家安全機関が外国由来の影響工作を監視・公表する一方で、実際の情報検証の主軸を担ったのは、台湾ファクトチェックセンター、MyGoPen、Cofacts といった民間検証組織だった。政府はその検証結果をメディアやプラットフォームと連携して流通させる役割を果たした。ウクライナでも、ディープフェイク動画への反証はテレビ局、SNS プラットフォーム、国防省、大統領本人が即座に対応し[23]、さらに Ukraine Communications Group によって、ロシアの偽情報への国際的反駁が政府間で調整・発信された[25]。どちらの事例も、「政府が全部やる」のではなく、それぞれの場面で「政府・民間・国際パートナーなどが協調する」という構図である。

第二に、「見える」ことと「継続する」ことが信頼を生む。ゼレンスキー大統領の自撮り動画は、内容よりも「首都に留まっているという事実の可視化」に力がありそれが継続発信されたことで国民の信頼を高めた。台湾の「vTaiwan」も、政府が市民と双方向的かつ継続的に対話するプロセス自体が市民に一体感を生ませ、信頼を育てた。

第三に、平時の「信頼と免疫力の蓄積」が危機時の「認知的レジリエンス」になる。台湾においては、ファクトチェック文化と市民参加を平時から育てていたことが、中国からの情報に対する免疫力を高め、認知戦が集中する選挙という局面で、“市民が偽情報に踊らされない”という形で機能した。ウクライナにおいては、戦前から偽情報対策機関を整備していたことが、平時のうちから市民の偽情報に対する免疫

力を高め、開戦後の情報空間の混乱の中で活用できた。認知戦への備えは、危機が顕在化してから構築できるものではない。台湾とウクライナがともに示しているのは、平時の信頼形成と免疫力の蓄積こそが、最大の認知的防衛線になるという点である。

台湾とウクライナの事例が示すのは、認知戦対策の本質が単なる情報訂正能力ではなく、平時から蓄積された政府・社会間の信頼を基盤として、修正ナラティブを社会に浸透させる能力にあるという点である。

3　日本における課題

（1）社会的不信と認知戦耐性――日本の「弱点の構造」

①　政府不信という「最大の弱点」

前述のとおり、日本の政府への信頼度（OECD 調査：33.6%）は先進国の中でも高水準とは言えない[11]。度重なる政治スキャンダル・官僚の不祥事・説明責任の不足が重なり、「どうせ政府は本当のことを言わない」という諦念が広がっている。

この状況が認知戦において如何に危険かを、具体的に考えてみよう。仮に台湾有事が発生し、「日本政府は戦況を隠蔽している」、「米軍は手を引き戦域から離脱した」という偽情報が SNS で拡散したとき、政府が公式に「それは偽情報です」と発信したとしても、政府不信が根強い国民の多くは「政府の言うことだから信じない」と反応するかもしれない。

これは「情報の問題」ではなく「信頼の問題」である。政府への信頼が低い社会では、政府が正確な情報を発信しても「政府の言うことだから額面通りに受け取れない」という認知フィルターが先に働く。その結果、敵対勢力が流す「政府が隠していること」を暴くという形式の偽情報の方が、かえって「真実らしさ」を帯びやすい。つまり政府不信は、認知戦にとって最も利用しやすい社会的土壌なのである。

②　「空気」に流されやすい同調傾向

「大多数がそう言うから正しい」という同調圧力は、多くの社会に見られる認知傾向だが、日本においてはその影響が社会行動として顕在化した事例が繰り返し記録されている。東日本大震災直後の買い占め騒動や、COVID-19 禍でのトイレットペーパー不足デマへの過剰反応は[7]、批判的思考を経ずに周囲の行動に盲目的に追随する「同調行動」の典型として報告されている。こうした同調圧力の回避には、個人

の批判的思考力の強化と、信頼できる公的情報源の確立が不可欠である。

この傾向は、認知戦の攻撃者にとって「格好の弱点」となり得る。ボットによって人工的に「多数派の意見」を演出することは技術的に容易であり、「SNS でみんなが言っているから本当だ」という判断に流れやすい社会では、大量のスマホなどの基板を集めた施設で大量の偽アカウントを自動操作する"スマホ農場"[29]を用いることなどで、社会全体の世論を動かす「多数派幻想」を作り出すことが可能となる。

③ 外的環境が「弱点」を増幅する

昨今、日本を取り巻く国際環境も、認知戦の弱点を増幅させる方向に変化している。日中関係の悪化は中国が対日認知戦を仕掛ける動機を高め[30]、米国の対外コミットメントへの不確実性は「米国は当てにならない」、「日本は米国の代理戦争に巻き込まれている」というナラティブが浸透しやすい素地を生む可能性がある[31]。

さらに深刻なのは、日本語という「言語の壁」が急速に低くなってしまったことだ。かつては、高度な日本語運用能力を持つ工作員を大量に育成するコストが、対日認知戦の事実上のハードルとなっていた。しかし大規模言語モデル（LLM）の登場により、敵対勢力は従来と比較して大幅に低コストかつ容易に、流ちょうな日本語コンテンツを大量生産できるようになった[32]。

実際、すでに日本の選挙においても、外国からの影響工作の「足跡」が観測されはじめている。2026 年 2 月の衆議院選挙期間中、政府の政策を批判して不安を煽る投稿が X の複数のアカウントから集中的に出回り、SNS 分析会社ジャパン・ネクサス・インテリジェンス（JNI）の調査でその一部は外国からの影響工作である可能性が浮かび上がった[33]。また日本サイバーディフェンスの名和利男氏は、「海外からの世論誘導は日本の選挙でも起きている。衆院選では数千の中国系アカウントが特定の政治家批判の投稿を行った」と指摘している[34]。いずれも今次選挙の結果を左右するほどの効果はなかったとされるが、認知戦の「試射」が行われていると見るべきであろう。

（**2**）「安心優先型コミュニケーション」の限界

前章で見た台湾・ウクライナの事例に共通するのは、政府が「社会の不安を最小化する」ことを優先するのではなく、「（市民が）事実として判断できる情報」に正面から答えるという「情報優先型」のコミュニケーションをとっていた点である。台湾当局は認知攻撃の規模を数値（「前年比 60%増の 216 万件」）で公表し[14]、民間検証組織と連携して具体的な偽情報の手口を名指しで示した。ウクライナのゼレンスキー大統領は自撮り動画で「私はここにいる」という事実と「共に戦う」という意思を繰り返し可視化した[22]。どちらも、「安心させる言葉」ではなく「事実として判断できる情報」を優先する姿勢だった。

これと比較したとき、日本政府の情報発信が持つ構造的な課題が浮かび上がる。

日本政府の情報発信には、これまで「社会不安を最小化する」ことを優先する傾向が繰り返し指摘されてきた。COVID-19 における「現時点では問題ない」「冷静に対応してほしい」という発信パターンや、東日本大震災後の「ただちに健康に影響はない」という表現が典型例として記憶に残っている。これらは虚偽ではないものの、「では実際に何が起きているのか」「なぜそう言えるのか」「自分は何をすればよいのか」といった市民の求める「事実として判断できる情報」の問いに答えない「安心優先型」の典型として批判を受けた[35]。

この「安心優先型」アプローチが認知戦の文脈で持つ問題は、単に「情報が足りない」ということにとどまらない。市民は政府の発信を漠然と受け取りながらも、「結局、実際には何が起きているのか」「政府は何かを隠しているのではないか」という疑念が残る。この疑念の「隙間」こそが、偽情報の付け入る最大の空間である。「政府が言わないことを私は知っている」という形式で語りかけてくる偽情報は、「安心優先型」の政府発信が残した疑念の空白を埋めるものとして、真実らしさを帯びやすい構造が生まれるのである。

したがって、日本の認知戦コミュニケーションに求められるのは、「安心させる言葉」から「事実として判断できる情報」を優先する姿勢への転換である。その際には、台湾・ウクライナの事例が示す「事実の公表・意味の提示・行動指針の一体的発信」という修正ナラティブの構造が、具体的な手本となる。

（**3**）政府発信の一体性――縦割り構造の克服

台湾では、国家安全機関が偽情報の規模を定期的に一元公表し、選挙当局・ファクトチェック機関・メディアが連携して同じ内容の反証を同時発信することで、市民の信頼を維持した[14,18]。ウクライナでは、「Ukraine Communications Group」を通じて反駁窓口を一元化し[25]、ディープフェイク動画への反証もテレビ局・国防省・大統領本人が即座に同一のメッセージを発した[23]。この「発信の一体性」が、偽情報に対抗する修正ナラティブの説得力を高めた重要な要因である。

翻って日本を見ると、有事における「発信の一体性」の確保は深刻な課題だ。COVID-19 対応においては、専門家会議・厚生労働省・内閣官房・各都道府県が各々の立場から異なるタイミングで情報を発信したことで、市民は「どれが公式見解なのか」を判断しにくい状況が生じた。これを教訓として、政府自身が設置した「新型コロナウイルス感染症対応に関する有識者会議」も、2022 年の報告書において、関係省庁が一体的に取り組む司令塔組織の整備を中長期的な課題として指摘している[36]。なお、こうした縦割り発信が市民の政府不信を深める側面については、前節で論じたとおりである。

また東日本大震災における原子力事故対応では、経済産業省原子力安全・保安院・内閣府・東京電力が

各々の発表を行ったことで、「官邸・経産省・東電のどれを信じればよいのか」という混乱が国民に広がり、かえってデマや風評被害の土壌となった経緯がある[37]。

2026 年 5 月に成立した国家情報会議設置法に基づく国家情報局の設置は、この「縦割り発信」の構造的問題を解消する制度的な一手として期待される[3]。ただし発信体制の整備は必要条件であって、その内容が「安心優先型」から脱却しなければ、課題の本質は解消されない。

（**4**）国家レジリエンスへの影響――「強さ」が問われる三つの層

これらの課題を整理すると、日本の認知戦への社会的レジリエンスは、三つの層で弱さを抱えていることが見えてくる。

個人の層：批判的思考とメディアリテラシーの不足。偽情報を見抜く個人の能力が、社会全体として十分に育まれていない。例えばフィンランドにおいては、幼児教育から成人教育まで、メディアリテラシーを幅広く扱っているのと対照的に、日本の情報教育は世代間格差が大きく、中高年層へのリテラシー教育や体系的なカリキュラムが不十分である[38]。

社会の層：政府への信頼の低さ。信頼できる情報の基盤となる機関が脆弱であれば、人々は偽情報を見分ける基準を失う。「誰の言うことを信じればいいのか分からない」という状態こそ、認知戦が最も機能しやすい環境である。

制度の層：偽情報対処の包括法・常設組織の整備の遅れ。欧州が DSA（デジタルサービス法）によってプラットフォームへのリスク評価義務を制度化している一方、日本の対応は遅れてきた[39]。2026 年 5 月に成立した国家情報会議設置法により、今後は国家情報局がインテリジェンスの総合調整と外国による影響工作への対処において主導的な役割を担うものと考えられる。防衛省は 2024 年度に「情報戦対応班」と情報本部の専門部署を新設したが[40]、政府全体を横断する国家情報局[3]との連携の在り方については、引き続き整備が求められる。

この三層すべての弱さが重なったとき、敵対勢力からの認知戦が最大の効果を発揮する。個人が偽情報を見抜けず、市民は政府の正確な情報を信頼せず、制度は迅速な対処ができなくなる。したがって、この「三重の脆弱性」の構造を認識することが、対策の出発点になると考えられる。

おわりに

台湾は分散型の検証基盤と迅速な訂正で選挙の正統性を守り、ウクライナは指導者の可視的な継続発信と同盟連携で国家意思の一体性を保った。どちらも「有事になってから対策を始めた」のではなく、むしろ、平時から信頼を積み上げ、民間との協働の仕組みを育て、偽情報への感受性を高めていたため、認知戦が集中した局面でその備えが機能したといえる。

日本に必要なのは、台湾・ウクライナの手法をそのまま模倣することではなく、日本の法制度と行政文化に適合させながら制度的な基盤を構築することである。その際、大前提として押さえておくべきは、政治への信頼性向上なしには、いかなる技術的対策も“砂上の楼閣”にすぎないという点だ。透明性ある説明・誤りの誠実な訂正・説明責任の徹底こそが、有事に国民が政府を信頼する土台となる。その上で、具体的には以下の方向での取り組みが求められる。

第一に、国家情報局を中心とした政府の統一的な情報発信体制の整備。2026 年 5 月に成立した国家情報会議設置法により、国家情報局が内閣官房に設置され、警察庁・外務省・防衛省・公安調査庁など各省庁の情報を集約・分析・総合調整する機能が付与された[3]。有事に際して各省庁が同一の事実関係を即時共有し一体で発信できる体制への整備は、この新機関が主導的に担うことが期待される。その際、防衛省の「情報戦対応班」や外務省の対外発信機能との有機的な連携の仕組みを早期に構築することが肝要である。

第二に、プレバンキングを軸としたコミュニケーション設計。「被害が出てから訂正する」事後対応から、「典型的な偽情報の手口を事前に市民に知らせる」予防型への転換。これはケンブリッジ大学の van der Linden 博士らが実証してきた心理的ワクチン接種（Psychological Inoculation）理論に基づくアプローチであり、台湾でも実装が進んでいる[41]。誤情報対策は事後訂正だけでなく、典型的な操作手口を事前に学ばせて心理的抵抗力を高める「プレバンキング」も含むべきであり、ゲーム型教材や簡易な事前警告は、その具体的手法になり得る。

第三に、独立したファクトチェック機関や友好・同盟国との恒常的連携。訂正の信頼性は、政府が自分で「これは偽情報です」と言うより、独立した第三者機関の検証や友好国からの発信が高いと考えられる。日本版ファクトチェックセンター（JFC）や欧米諸国との平時からの情報発信に関する連携体制を公式化することが有効である[42]。

認知戦への備えとは、危機時の反論技術ではなく、平時からの信頼の備蓄である。それは軍事力と並ぶ「抑止力」であり、「社会のレジリエンス」そのものが認知戦への防衛投資になる時代が到来している。

[1] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), *Ukraine as the Frontline of European Cyber Defence*, Tallinn Paper No. 15 (Tallinn: CCDCOE, 2025), p. 5, https://ccdcoe.org/uploads/2025/07/Tkachuk_N_Tallinn_Paper_15_Ukraine-as-the-Frontline-of-European-Cyber-Defence.pdf.
[2] 内閣官房『国家安全保障戦略』(2022 年 12 月 16 日閣議決定)、4 頁。
[3] 国家情報会議設置法(令和 8 年法律第 28 号)、2026 年 5 月 27 日参院本会議可決・成立。https://elaws.jp/view/508AC0000000028.
[4] Hasher, L., Goldstein, D., and Toppino, T., "Frequency and the Conference of Referential Validity," *Journal of Verbal Learning and Verbal Behavior*, vol. 16, no. 1 (February 1977), pp. 107–112.
[5] Fazio, L. K., Brashier, N. M., Payne, B. K., and Marsh, E. J., "Knowledge Does Not Protect Against Illusory Truth," *Journal of Experimental Psychology: General*, vol. 144, no. 5 (October 2015), p. 993.
[6] Lewandowsky, S., Cook, J., Ecker, U. K. H., et al., *The Debunking Handbook 2020* (2020), https://www.climatechangecommunication.org/wp-content/uploads/2023/09/DebunkingHandbook2020.pdf?
[7] 飯塚隆介・池田朋貴・斉藤和也・橋本幸士「訂正情報がもたらす社会的混乱――コロナ禍のトイレットペーパー不足に関する分析」東京大学大学院工学系研究科プレスリリース、2022 年 4 月 28 日、https://www.t.u-tokyo.ac.jp/press/pr2022-04-28-003.
[8] Lewandowsky et al., *The Debunking Handbook 2020*(前掲)。なお、認知戦における対抗ナラティブの重要性については、NATO Strategic Communications Centre of Excellence, *ZAPAD 2021 Communication Analysis: Messages, Narratives, (Dis)Information* (Riga: NATO StratCom COE, 2022) を参照。
[9] Green, M. C. and Brock, T. C., "The Role of Transportation in the Persuasiveness of Public Narratives," *Journal of Personality and Social Psychology*, vol. 79, no. 5 (November 2000), pp. 701–721.
[10] Petty, R. E. and Cacioppo, J. T., *Communication and Persuasion: Central and Peripheral Routes to Attitude Change* (New York: Springer, 1986).
[11] OECD, Government at a Glance 2023, OECD Publishing, 2023, Japan Chapter. https://www.oecd.org/gov/government-at-a-glance/
[12] 台湾法務部「反滲透法」(2020 年 1 月 15 日施行)公式法令データベース。https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030317
[13] National Security Bureau (NSB), Taiwan. "China's Disinformation Dissemination Patterns in 2024." National Security Bureau, January 2025. https://www.nsb.gov.tw/en/assets/documents/%E6%96%B0%E8%81%9E%E7%A8%BF/1eeba30c-ebf8-459a-8fe3-ed2a54cb4ca0.pdf.
[14] "Taiwan Says China Is Redoubling Efforts to Undermine Democracy with Disinformation," *AP News*, January 4, 2025, https://apnews.com/article/3f05dac36399bf672a702100147bf8fa.
[15] "How Taiwan beat back disinformation and preserved the integrity of its election," *AP News*, January 27, 2024. https://apnews.com/article/taiwan-election-china-disinformation-vote-fraud-4968ef08fd13821e359b8e195b12919c?
[16] "From Beef Noodles to Bots: Taiwan's Factcheckers on Fighting Chinese Disinformation and 'Unstoppable' AI," *The Guardian*, June 5, 2024, https://www.theguardian.com/world/article/2024/jun/05/from-beef-noodles-to-bots-taiwans-factcheckers-on-fighting-chinese-disinformation-and-unstoppable-ai. なお、本文中に登場する各組織の概要は以下の通り。台湾ファクトチェックセンター(TFC):2018 年設立、IFCN 認証取得のファクトチェック機関。LINE・Facebook 等と連携。MyGoPen:2015 年設立の民間ファクトチェック団体。登録者 40 万人超、年間 130 万件以上の検証依頼を処理。Cofacts:ボランティア 2,000 人超が運営する LINE チャットボット型プラットフォーム。Doublethink Lab:中国の影響力を 82 カ国で追跡・公表する非営利調査研究機関。
[17] Polly Curtis, "How Taiwan Bucked a Global Trend – and Restored Voters' Trust in Politics," *The Guardian*, July 22, 2024, https://www.theguardian.com/commentisfree/article/2024/jul/22/taiwan-bucked-global-trend-trust-politics-hired-protesters.
[18] "How Media in Taiwan Has Adapted to Combat Electoral Disinformation," International Journalists' Network (IJNet), April 17, 2024; "Lessons from Taiwan's Resistance to an Election Disinformation Wave," Global Investigative Journalism Network (GIJN), April 15, 2024.
[19] Taiwan Ministry of Education, "Digital Era Media Literacy Education White Paper 2023," Ministry of Education, March 2023, https://globaltaiwan.org/2024/03/media-literacy-education-taiwans-key-to-combating-disinformation/.
[20] European External Action Service (EEAS), "EUvsDisinfo: Pro-Kremlin Disinformation Narratives on Ukraine," EEAS, https://euvsdisinfo.eu/.
[21] James Pearson and Natalia Zinets, "Deepfake Footage Purports to Show Ukrainian President Capitulating," *Reuters*, March 16, 2022.
[22] "In Unlikely Wartime Role, Zelenskyy Gives Ukrainians Hope," *AP News*, March 3, 2022.
[23] "Deepfake Video of Zelenskyy Could Be 'Tip of the Iceberg' in Info War, Experts Warn," *NPR*, March 16, 2022; Matyáš Boháček and Hany Farid, "Protecting President Zelenskyy against Deep Fakes," arXiv:2206.12043, 2022, https://arxiv.org/abs/2206.12043.

[24] "A Zelensky Deepfake Was Quickly Defeated. The Next One Might Not Be," *WIRED*, March 17, 2022, https://www.wired.com/story/zelensky-deepfake-facebook-twitter-playbook.
[25] "About the Center," Center for Countering Disinformation (CCD), National Security and Defense Council of Ukraine, https://cpd.gov.ua/en/docs/about-center-for-countering-disinformartion/; "Ukraine's Hard-Won Approach to Strategic Communications and Counter-Disinformation," Tech Policy Press, March 12, 2025. 両機関ともに 2021 年 3 月設立。
[26] AP, "US and Poland launch center to fight Kremlin disinformation about Ukraine war," June 11, 2024. https://apnews.com/article/poland-us-ukraine-disinformation-war-1da53518252ce6a123f2fcf2cade6bd2?
[27] "Intelligence Disclosure as a Strategic Messaging Tool," *NATO Review*, December 16, 2024, https://www.nato.int/docu/review/articles/2024/12/16/intelligence-disclosure-as-a-strategic-messaging-tool/index.html; 防衛研究所「Weaponized Disclosure of Intelligence in the Russia-Ukraine War」『NIDS コメンタリー』第 224 号（2024 年）、https://www.nids.mod.go.jp/english/publication/commentary/pdf/commentary224e.pdf.
[28] Reuters, "Ukraine bans official use of Telegram app over fears of Russian spying," September 21, 2024. https://www.reuters.com/technology/cybersecurity/ukraine-bans-official-use-telegram-app-over-fears-russian-spying-2024-09-20/?
[29]「扉の先 SNS 世論操る『農場』」『朝日新聞』2026 年 4 月 28 日、1・2 面。
[30] "Japanese Seafood Caught up in Escalating Diplomatic Dispute with China," *Reuters*, November 19, 2025.
[31] "Unpacking a Trump Twist of the National Security Strategy," Council on Foreign Relations, December 6, 2025, https://www.cfr.org/expert-brief/unpacking-trump-twist-national-security-strategy.
[32] Josh A. Goldstein, Girish Sastry, Micah Musser, Renée DiResta, Matthew Gentzel, and Katerina Sedova, "Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations," arXiv:2301.04246, January 2023, https://arxiv.org/abs/2301.04246.
[33]「衆院選中不安あおる投稿 外国からの工作か」朝日新聞 2026 年 3 月 4 日付、27 面。
[34]「扉の先 SNS 世論操る『農場』」『朝日新聞』前掲。なお名和利男氏（日本サイバーディフェンス専務理事）の発言も同記事による。
[35] 木下冨雄「リスクコミュニケーションの理論と実践」『日本リスク研究学会誌』（2011 年）。
[36] 新型コロナウイルス感染症対応に関する有識者会議「新型コロナウイルス感染症へのこれまでの取組を踏まえた次の感染症危機に向けた中長期的な課題について」2022 年 6 月 15 日、20 頁「次の感染症危機に対する政府の体制づくり」。https://www.cas.go.jp/jp/seisaku/coronavirus_yushiki/pdf/corona_kadai.pdf.
[37] 福田充「3.11 後のリスクコミュニケーション――原子力災害における政府・東電・メディアの情報発信の分断」『マス・コミュニケーション研究』82 号、日本マス・コミュニケーション学会、2013 年。
[38] "Media Literacy and Education in Finland," Finland Toolbox / Ministry of Education and Culture, March 2024, https://toolbox.finland.fi/life-society/media-literacy-and-education-in-finland/; Open Society Institute, *Media Literacy Index 2023* (Sofia: Open Society Institute, 2023).
[39] "The Digital Services Act," European Commission, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act.
[40] 令和 6 年版防衛白書（防衛省、2024 年）。
[41] Sander van der Linden, Anthony Leiserowitz, Seth Rosenthal, and Edward Maibach, "Inoculating the Public against Misinformation about Climate Change," *Global Challenges*, vol. 1, no. 2 (May 2017), https://pubmed.ncbi.nlm.nih.gov/29191898/; Jon Roozenbeek and Sander van der Linden, "Fake News Game Confers Psychological Resistance against Online Misinformation," *Humanities and Social Sciences Communications*, vol. 6, no. 1 (August 2019), https://www.nature.com/articles/s41599-019-0279-9.
[42] 一般社団法人セーファーインターネット協会「Japan Fact-Check Center（JFC）運営開始について」セーファーインターネット協会、https://www.factcheckcenter.jp/about/.

PROFILE

牛若　健悟

先進領域研究部防衛基盤研究室　主任研究官

専門分野：認知戦

防衛研究所企画部企画調整課

直　通：03-3260-3011
代　表：03-3268-3111（内線 29177）
防衛研究所 Web サイト：www.nids.mod.go.jp