「我が国のサイバー安全保障の確保」事業　政策提言

“外国からのディスインフォメーションに備えを！
～サイバー空間の情報操作の脅威～”

2022年２月

公益財団法人　笹川平和財団
安全保障研究グループ

【提言のポイント】（詳細は第４章をご参照ください）

① ディスインフォメーション対策を行う情報収集センターを設置する。
（１）ディスインフォメーションを用いた外国勢力の干渉に関する情報収集センターを設置する。
（２）事後制裁および国際法上許容される対抗措置を行うことを可能にする法律の制定を検討する。
② 選挙インフラを重要インフラに指定する。
③ 情報操作型サイバー攻撃に対するアクティブ・サイバーディフェンス（ACD）実施体制を整備する。
④ 政府とプラットフォーマーによる協同規制の取り組みと行動規範の策定を推進する。
⑤ メディアリテラシー教育環境を拡充する。

表1　欧米アジア各国・地域と日本のディスインフォメーション対策の比較表

	米国	英国	ドイツ	フランス	シンガポール	EU	台湾	日本
１－１ ディスインフォメーションによる干渉を検知、モニタリングする機関や制度があるか	○	○	△	△	○	○	○	×
１－２ 選挙等の民主主義プロセスについて干渉があったか否かを調査し処罰する法律があるか	○	△	△	△	○	△	○	×
２ 選挙インフラが重要インフラに指定されているか	○	×	×	×	×	△	×	×
３ 選挙干渉行為に対し国家としてサイバー攻撃による反撃、防衛を行うことができるか	○	△	△	×	×	×	×	×
４ 選挙干渉等に関連しプラットフォーマーを規制する法律があるか	△	△	○	○	○	○	△	×
５－１ ディスインフォメーション対策としてメディアリテラシー教育を行っているか	○	○	△	△	○	○	○	×
５－２ 行政府による／行政府から独立した、ファクトチェック機関があるか	○ （１＋61）	○ （０＋７）	○ （１＋６）	○ （０＋17）	○ （１＋２）	○ （１＋１）	○ （１＋４）	○ （０＋３）

注：○印は「はい」、△印は「部分的に『はい』、または検討中」、×印は「いいえ」、
５－２欄の数字は「ファクトチェック機関の総数（行政府によるファクトチェック機関＋行政府から独立したファクトチェック機関）」を表す。

政策提言要旨

サイバー攻撃は、今や人類最大の懸案事項の一つである。テロリストによるサイバー攻撃は、大規模自然災害に匹敵する規模の被害を社会にもたらし、国家によるサイバー攻撃は、諜報活動、知財窃取、機能妨害、破壊行為、情報操作等により社会の基盤を脅かす。サイバー攻撃の主体の多様化や攻撃手法の高度化が進み、今やサイバーセキュリティの領域はインターネット空間の安全確保（Security of Internet）にとどまらない。重要インフラなどの物理空間およびネット空間とつながる人間といった社会層を含むサイバー空間の安全確保（Security of Cyberspace）、また、いわゆるフェイクニュース（偽情報）などに影響を受ける個人の認知の安全保障（Cognitive Security）、さらには、インターネット情報に影響を受ける民主主義プロセスの安全確保や社会の信頼・統合・安定の安全保障（Security of Democratic Society）までを含むようになり、それらが世界的な課題となっている。

2016年の米国大統領選挙を端緒に、欧米やアジア各国・地域の選挙等において、サイバー空間を用いる情報操作によって外国勢力が民主主義プロセスに干渉し、広範な影響工作を行う事案が頻発している。国家の意思決定プロセスに対するサイバー攻撃は、民主主義社会を危機に陥らせかねない重大な脅威であり、国家安全保障上の課題として対処することが急務である。しかしながら、このような外国勢力による干渉や影響工作に対して、民主主義国家が「目には目を」という形で反撃を行うことは許されておらず、その対応は難しい。

こうした情報操作型のサイバー攻撃では、偽情報が拡散されたり、真の情報であっても誤った文脈や操作された文脈で拡散されたりする。これら真偽にかかわらず社会、公益への攻撃を目的とした害意のある情報を指す言葉が「ディスインフォメーション（Disinformation）」である。この言葉の定義については第１章３項で詳述するが、本提言では、選挙干渉や社会の不安定化等、安全保障上の問題となりうるディスインフォメーションに限定して日本の備えるべき対策を具体的に論じる。

近年、欧米やアジア各国においては、情報操作型のサイバー攻撃に対応するため、ディスインフォメーション対策を重視した法制度等の整備が進められている。その類型は３つに大別される。すなわち、第１が欧州連合（EU）諸国にみられるプラットフォーマー規制型、第２が米国や台湾で採用されている外国勢力の介入に対する事後制裁型、そして第３がシンガポールやマレーシアで採用されている虚偽情報全般規制型である。これらに加えて、ニュース記事のファクトチェックやメディアリテラシー教育等を組み合わせて、各国が特色のあるディスインフォメーション対策を行なっている（表１参照）。

しかしながら、我が国ではこうした対策の検討は進んでいない。その理由として、サイバー空間を用いた外国からの情報操作、すなわち選挙干渉、影響工作の重大な事例がまだ明確には確認されていないことがあげられる。また、日本語という独特の言語空間が、他国からの情報操作型の攻撃の防塁となって我が国のサイバー空間を守ってきた側面もある。ところが、近年の人工知能（AI）翻訳等の技術的進歩に伴い、ソーシャルネットワークサービス（SNS）でのチャット

等が自然な会話調で和訳されるようになるなど、言語の防塁は簡単に乗り越えられるようになってきている。そのため、今後は我が国においても、選挙にとどまらず、改憲のための国民投票といった重大な民主主義プロセスにおけるサイバー空間を用いた外国からの干渉や影響工作の排除、セキュリティ確保が重要な優先事項となる。

我が国においては、総務省が主導して2017年から「インターネットメディア連絡会」が、さらに2018年から「プラットフォームサービスに関する研究会」が開催されている。これら総務省の検討では、ディスインフォメーションに対しては、プラットフォーマー事業者の自主的な取り組みがまずは期待されており、それが機能しない場合、行政の一定の関与という形で規制を図ることを中心に議論されている。現時点では法整備に落とし込む段階までは進んでいない。我が国のディスインフォメーション対策に関わる法整備は、欧米各国に比べさまざまな点で立ち遅れている。

我が国では、日本国憲法第21条が定める表現の自由や通信の秘密が重視されており、広範なディスインフォメーション対策を講じることが難しく、また、情報操作型のサイバー攻撃に対する積極的サイバー防御（Active Cyber Defense： ACD）の手段も取りにくい現状がある。憲法に定められる表現の自由は民主主義の根幹であり、みだりに規制すべきではない。しかし、この権利はあくまでも内国民に保障されたものであり、外国勢力が表現の自由を濫用し、ディスインフォメーションを用いて民主主義プロセスに介入することを許容するものではない。

こうした論点を踏まえ、世界的に拡大するディスインフォメーションを用いた情報操作型サイバー攻撃に対応するために、政府に対し、サイバーセキュリティ戦略にディスインフォメーション対策を書き込むとともに、以下の取り組みを進めることを提言する。第１にディスインフォメーション対策を行う情報収集センターの設置、第２に選挙インフラの重要インフラへの指定、第３に情報操作型サイバー攻撃に対するACDを実施する体制の整備、第４にディスインフォメーションを防ぐためのプラットフォーマー規制の導入、そして第５にメディアリテラシー教育の環境整備による外部の影響工作に抗堪性のある国民意識の醸成である。

※本政策提言におけるディスインフォメーションの定義（第１章３項で詳述）

「ディスインフォメーション」は、社会、公益への攻撃を目的とした害意のある情報で、情報自体が偽であるだけでなく、情報自体は真であるが誤った文脈や操作された内容で拡散されるものなど、真偽どちらもありうる、と定義される。本提言で対象とする「ディスインフォメーション」は、情報操作を目的として外国政府により流布される情報で、選挙干渉をはじめとする民主主義プロセスへの介入を目的としたものや、社会の不安定化を意図して流布され安全保障上の脅威となり得るものに限定している。ただし本提言では、各国の事例・対策の説明に際して、当該国で「フェイクニュース」「偽情報」が一般的に使われている場合などについては、便宜的に「フェイクニュース」「偽情報」と表記している。

目次

第１章　ディスインフォメーションによる民主主義プロセスへの攻撃の現状と分析の視座

１．サイバー攻撃と民主主義プロセスへの攻撃の現状

サイバー攻撃は、今やわれわれの社会を脅かす脅威となりつつある。

米国のサイバー対策ソフト大手マカフィー社とシンクタンク戦略国際問題研究所（CSIS）による最新のレポート[1]（2020年12月）によれば、2020年のサイバー攻撃の被害額は世界全体で年間約１兆ドル（約110兆円）に達し、2018年の約600億ドルからほぼ倍増している。

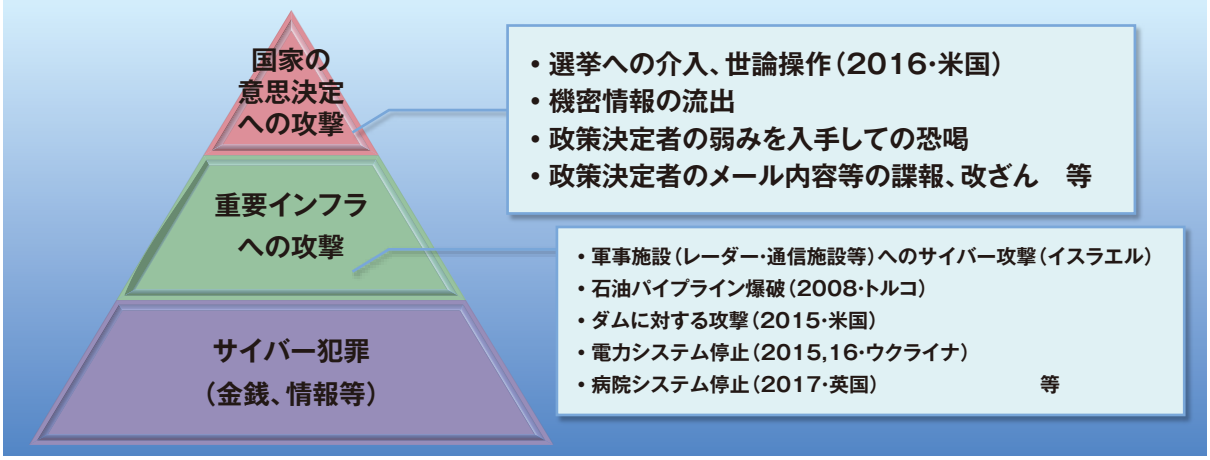
ここ数年、身代金要求型ウイルス「ランサムウェア」攻撃により、医療や地方自治体のみならず、エネルギーなどの重要インフラへの脅威が高まっている。2017年５月には、ランサムウェアのワナクライ（WannaCry）が世界150カ国に広がり、英国では国民保健サービス（NHS）のコンピュータが多数停止して医療サービスが行えなくなる病院も現れた。ランサムウェア攻撃は、特に2019年以降、欧米の医療機関で猛威を奮っている。2020年９月には、全米最大手の医療グループユニバーサル・ヘルス・サービス（Universal Health Services）が攻撃を受け、運営する400の病院でITシステムへのアクセスができなくなった。2021年５月には、アイルランドの国民健康サービス（Irish Health Service）が攻撃を受け、国の医療システムが停止した。2021年５月には、米大手石油パイプライン企業コロニアル・パイプラインが攻撃を受け、米国の石油パイプラインが停止し、首都ワシントンを含む東部の州で一時的にガソリンの供給が滞り、市民生活に大きな影響が出た。また、仮想通貨取引所や金融機関へのサイバー攻撃が国家やテロ組織により行われており、それらの重要な資金源となっているとの報道もある。

知的財産や国家機密に対するサイバー攻撃もある。2021年４月20日、警視庁は宇宙航空研究開発機構（JAXA）等日本の企業・組織へのサイバー攻撃に関与したとして、中国籍の男を検察庁に書類送検した。警察庁は、約200の国内企業等に対する一連のサイバー攻撃が「Tick（ティック）」と呼ばれるサイバー攻撃集団によって実行され、同集団には中国人民解放軍の戦略支援部隊ネットワークシステム部、第61419部隊が関与している可能性が高い、と発表している。Tickは防衛、航空、化学、宇宙（衛星）等の高度な技術を保有する日本企業を狙っており、2019年に大手電機メーカーや防衛産業にも攻撃を行なっている。世界各国の知的財産や特許を狙った情報窃取型のサイバー攻撃には、Tick以外にも30以上の中国のサイバー攻撃集団が従事していると分析されている[2]。サイバー空間は陸海空、宇宙に次ぐ「第５の戦場」といわれるように、軍事面での重要性も年々高まっており、米国、中国、北朝鮮等でサイバー攻撃を専門とする部隊（サイバー軍）が相次いで創設されるなど、軍事面におけるサイバー対処も必要とされている。

サイバー攻撃の被害は、経済的損失にとどまらない。情報操作により社会を撹乱する攻撃も増えている。新型コロナウィルス流行下では、ワクチンの信用を貶める情報操作や新型コロナウィルスの起源をめぐるフェイクニュースがSNS上で流布された。2016年の米国大統領選挙では、立候補者に対する情報操作型サイバー攻撃が行われた。フェイクニュースが流布され、サイバー攻撃により窃取された機密情報が意図的に公開されるなどし、大統領選挙の最終結果に大きな影響

を及ぼしたとされる。この選挙の事例では、窃取した情報をSNSやウェブメディア等を通じて拡散し、また並行して個人を狙い撃ちにしたマイクロターゲティング広告に出資して特定意見を流布するといったオペレーションにより、標的とする社会の分断を煽る手法が中心であった。しかし、最近では、このようなディスインフォメーションを用いた攻撃においては、実際のサイバー攻撃を伴わない事例もあり、特にSNSにおける影響工作のウェイトが大きくなっている。2017年のドイツの総選挙前には、アンゲラ・メルケル首相とイスラム教移民との関係を誤解させるフェイクニュースがSNS上で流布されている。こうしたディスインフォメーションを用いた民主主義国における選挙への介入や撹乱、社会の信頼や統合の毀損を企図した事例が増えてきている。

図1　さまざまなサイバー攻撃の脅威



出典：「サイバー空間の防衛力強化プロジェクト　政策提言　“日本にサイバーセキュリティ庁の創設を！”」2018年、笹川平和財団、２頁。

選挙への介入や世論操作は国家の意思決定への攻撃であり、安全保障上の観点から看過できない問題である（図１参照）。先に述べたように、そのような情報操作型サイバー攻撃による選挙干渉が注目を集めたのは、2016年の米国大統領選挙であるが、以後、諸外国においても選挙およびその他の民主主義プロセスに介入が疑われる事例が増えてきている。これらをまとめたのが図２と表２である。図２から、ロシアが欧州への影響力を強めつつアフリカ諸国にまで影響を及ぼしていること、中国がアジア太平洋地域を中心に影響力を行使しようとしていることが読み取れる。また、干渉国側にとって影響力を行使する意義の大きい米国や台湾などは、民主主義プロセスにおいて度重なる干渉を受ける事態となっている。このようなディスインフォメーションによる国家の意思決定への攻撃は、アメリカのみならず、欧州諸国でも安全保障上の課題として認識され始めており、我が国においても早急に対策を検討すべき状況にある。

図2　2016年以降のディスインフォメーションによる民主主義プロセスへの干渉とみられる事例

出典：各種報道資料、政府発表資料をもとに笹川平和財団安全保障研究グループ「我が国のサイバー安全保障の確保」事業事務局（以下、事務局）作成。

表2　2016年以降のディスインフォメーションによる干渉とみられる事例一覧

年　月　日	国・地域名	事　例　名	干　渉　国
2016年１月16日	台湾	台湾総統選挙・立法委員選挙	中国
2016年６月23日	英国	EU離脱の是非を問う英国民投票	ロシア
2016年11月８日	米国	米国大統領選挙	ロシア
2017年５月７日	フランス	フランス大統領選挙	ロシア
2017年９月24日	ドイツ	ドイツ連邦議会選挙	ロシア
2017年９月25日	イラク	クルディスタン地域独立の是非を問う住民投票	ロシア
2017年10月１日	スペイン	カタルーニャ自治州独立の是非を問う住民投票	ロシア
2018年７月29日	カンボジア	カンボジア国民議会（下院）議員選挙	中国
2018年９月30日	マケドニア、ギリシャ	国名を「北マケドニア」に変更するかを問うマケドニア国民投票	ロシア
2018年９月30日	日本	沖縄県知事選挙	不明 （※国外勢力か国内勢力かも現時点では不明）
2018年11月６日	米国	米国中間選挙	ロシア、中国、イラン
2018年11月17日	フランス	フランスの反政府運動「黄色いベスト運動」	ロシア
2018年11月24日	台湾	台湾統一地方選挙、高雄市長選挙	中国
2019年３月３日	エストニア	エストニア議会選挙	ロシア
2019年３月31日より	香港	香港民主化デモ	中国
2019年５月18日	オーストラリア	オーストラリア連邦議会選挙	中国

年　月　日	国・地域名	事　例　名	干　渉　国
2019年５月23～26日	EU	欧州議会議員選挙	ロシア
2019年10月18日より	チリ	チリ暴動	ロシア
2019年10月30日 （※干渉行為が公表された日時）	アフリカ諸国	―	ロシア
2020年１月11日	台湾	台湾総統選挙 立法委員選挙	中国
2020年11月３日	米国	米国大統領選挙	ロシア、（中国）、イラン

出典：各種報道資料、政府発表資料をもとに事務局作成。

2. ディスインフォメーションと認知領域へのサイバー攻撃

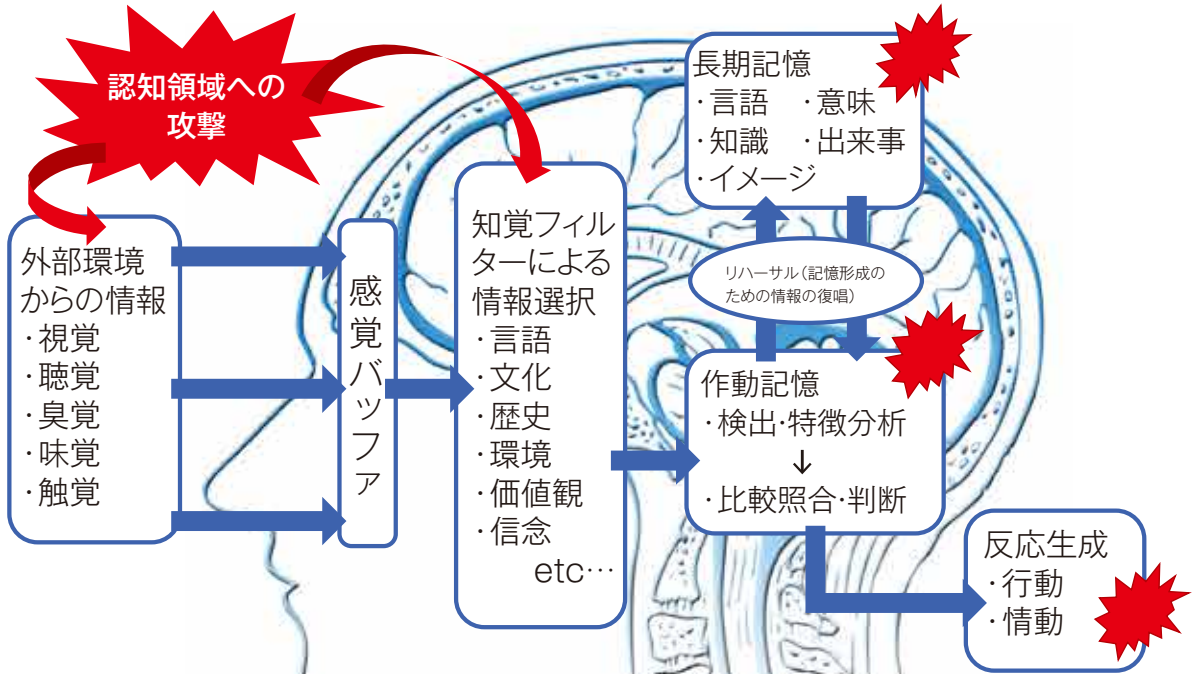
ディスインフォメーションによる国家の意思決定への攻撃では、ウェブメディアやSNSが情報操作の手段として用いられるようになったことで、その攻撃対象は、インターネット情報に影響を受ける民主主義プロセスや社会の信頼・統合・安定、そしてユーザーである各個人の認知領域にまで及ぶようになった。

ヒトの認知情報処理フローは、図３に示すように、感覚入力だけでなく、過去の記憶やイメージによって引き出される記憶系の情報との突合によって反応が生成され、実際の行動が引き起こされる。

ディスインフォメーションによる個人の認知領域への攻撃は、視覚や聴覚といった直接的な感覚入力のみに偽情報をインプットするだけでなく、ナラティブ（物語）を通じて過去の記憶に基づくワーキングメモリ（作動記憶）にも働きかけ、情報の取捨選択を行う認知フィルターを通じて個人の認知領域の中で生み出される現実の解釈（内部表象）に影響を与える。その結果として、個人の感情や行動に影響を与え、攻撃の所与の目的である結果を引き出そうとする。このような認知領域への攻撃は、ロシアが得意としている。図３はそのような認知領域に対するロシアの情報戦のモデルである。

現在では、ネット上のバルク（大量の）データの収集と分析により、ネット閲覧状況などを基に個々人の嗜好や政治的傾向ですら把握が可能であり、ウェブやSNSにおける政治広告や「おすすめ」として提示される記事のようにマイクロターゲティングが行われている。すでに広告の世界でも情報操作の対象はマス（不特定多数）ではなく、マイクロ（個人）であり、個人の認知に直接働きかけるマーケティングが行われている。ディスインフォメーションによる攻撃では、マーケティングと同じ手法が用いられ、国家の意思決定を歪めるために、個人の認知への攻撃が行われているのが現実である。ソーシャルメディア時代におけるディスインフォメーションの本質は、ソーシャルメディアのビジネスモデル自体を逆手にとったものである。実際に、2016年の米国大統領選挙では、ロシア情報機関との関係が疑われるインターネット・リサーチ・エージェンシー（IRA）が、3,393件の政治広告をFacebookに出稿し、1,140万人の米国人がこれを閲覧したと推計されており、マイクロターゲティングの手法を用いてディスインフォメーションによる情報操作を行おうとしていたことが、2017年11月の米下院情報問題常設特別調査委員会（HPSCI）におけるFacebook代理弁護士に対するヒアリングで明かされている[3]。

図3　人の認知処理フローと認知領域への攻撃イメージ



出典：各種資料より事務局作成。

このような認知領域のサイバー攻撃、すなわち情報戦に積極的なのがロシアと中国である。

ロシアによる情報戦は、自国の戦略的優位性を確保するために、敵対する社会体制の情報心理領域でのコントロールを試みる戦い（情報心理戦）であり、ディスインフォメーションはその手段として使われる。情報心理戦には、特定の対象に対する認知を歪曲または隠蔽する「マスキロフカ（欺瞞工作）」として実施される通常戦と、ディスインフォメーション等を用いて自国の戦略的優性を確保しようとする戦略情報戦がある。ロシアの情報戦の特徴は、①相手（国・社会）が内包する矛盾を見極め、②その矛盾をフェイクニュースなどの手段を用いて増幅し、③亀裂拡大により相手社会を自滅に追い込む点にある。ロシアは、国際社会の多極化を地政学的操作余地を拡大する好機と捉えており、情報戦により欧米の弱体化を図り、戦略均衡を達成することを模索している。日米同盟を含む米国の同盟ネットワーク内の不安定さ（例えば北大西洋条約機構［NATO］内で観察されるインバランスなど）や民主主義システムの内包する矛盾を拡大し、つけ入る隙を作り出そうとしている。

ロシアにとっての情報空間は認知空間、サイバー空間、物理空間にまたがる。ソーシャルメディアは、これら３つの空間全てにまたがるため、ロシアにとって情報戦の格好の手段となっている。

また、ロシアの情報戦の独特の概念として、「反射コントロール」がある。相手の「意識」（図３の長期記憶や作動記憶に該当）に働きかけ、人間の認知領域における「刺激－反応」からなる反射サイクルをコントロールし、意思決定サイクルに入り込み、相手が自らの自由意志に基づいて行動しているかのように認識させ、自身に有利な相手の意思決定・反応生成を導く、というものである。

中国もまた、認知領域を戦場と考えている。中国は従来から、孫子の兵法にある「不戦屈敵」の考えをもとに、心理戦、輿論（よろん）戦、法律戦の三戦を重視してきた。2003年には人民解放軍政治工作条例に、「輿論戦、心理戦、法律戦を実施し、瓦解工作、反心理・反策反工作、軍事司法および法律服務工作を展開する」と明記されている。

中国では軍の近代化の過程で、長年「現代条件下の局地戦争」や「ハイテク条件下の局地戦争」に勝ち抜くことが目標とされ、軍隊の機械化や精密誘導兵器の整備を重視してきた。2015年以降は「情報化戦争」での勝利が新たな目標とされ、特に2017年以降は「智能化戦争」、すなわち人工知能および認知領域の戦いでの勝利が重視されるようになってきている。

このうち認知領域の戦いでは「制脳権」が重要とされ、認知空間での優位性確保を重視するようになってきている。敵の認知域を攻撃し、自分の認知域を防御するための具体的な手法として、①敵の状況把握能力を弱体化、喪失させる「認知抑制」、②虚偽情報により敵の意思を挫き、誤った判断を導く「認知形成」、③敵の意思決定メカニズムを改竄する「認知支配」が検討されている。

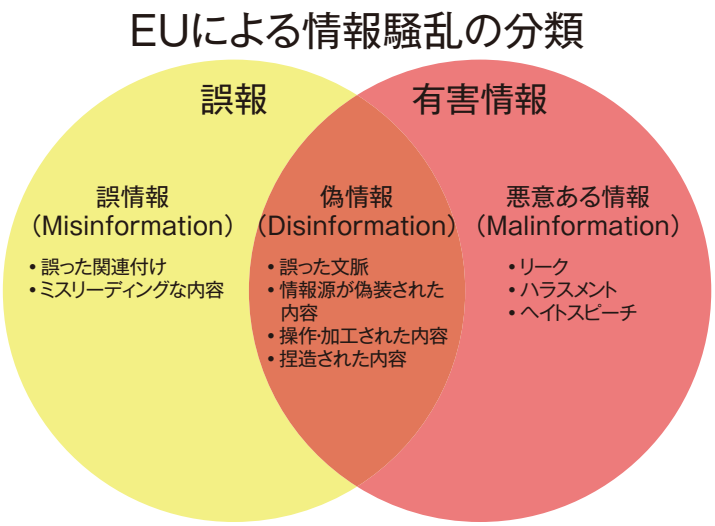
3. ディスインフォメーションの定義と本提言の対象

本提言は、2019年に笹川平和財団安全保障研究グループが立ち上げた情報操作型サイバー攻撃を主たるテーマとする「サイバーフェイクニュース研究会」の議論を土台とする。

研究会の名称に「フェイクニュース」という言葉を用いているのは、本来用いるべき「ディスインフォメーション」よりも一般的に通用している言葉であったためである。しかしながら、当初より研究会では、フェイクニュースという言葉は多義的で曖昧なため、研究会の名称をはじめ議論においても使用すべきではない、という意見が大勢であった。そこで、本提言においても、ディスインフォメーションという言葉を用いる。（ただし、便宜的に「フェイクニュース」という表記も用いている。）

ディスインフォメーションについては、EUの専門家会合が下図４で示す情報混乱を引き起こす情報３分類の一つとされ、３つをそれぞれ次のように定義している。ミスインフォメーションは、事実誤認や過失により誤った文脈で発信される故意や悪意のない誤情報。ディスインフォメーションは、社会、公益への攻撃を目的とした害意のある情報。ここには偽情報だけでなく、誤った文脈や操作された内容で拡散される真の情報も含まれる。そして、マルインフォメーションは、リークやハラスメント等、害意をもって広められる真の情報である。

図4　EUの専門家会合における混乱を引き起こす情報の3分類



出典：Claire Wardle, Hossein Derakhshan, *INFORMATION DISORDER : Toward an interdisciplinary framework for research and policy making*, Council of Europe, September 2017, p.5より事務局にて翻訳・作成。

相手国の意思決定プロセスを害する目的で発信される情報、すなわち情報操作型の攻撃に利用される情報には、偽情報だけでなく害意をもって広められる真の情報もある。そのため、本提言で検討する偽情報の範疇は、EUの専門家会合が定義する「ディスインフォメーション」とほぼ同一である。害意の有無という点では、ディスインフォメーションはマルインフォメーションと重複したり、双方が巧妙に組み合わされたりする場合もある。

EUでは、情報規制の対象を「選挙に影響を与える情報」とし、さらに「検証可能で虚偽または誤解を招く情報」と定義している。なお、最近では、情報規制の対象を、情報の目的や意図、真偽にかかわらず、「有害性」に焦点を当てて“toxic online contents”と定義する動きもある。2019年３月、ニュージーランドのクライストチャーチにおけるモスクで銃乱射事件が起きた際に、そのライブストリーム動画がFacebookやTwitter等のSNSを通じて広まり、動画が削除される前に4,000回以上も閲覧された。この事件を契機に、ニュージーランドのジャシンダ・アーダーン首相とフランスのエマニュエル・マクロン大統領が主導して同年５月に“Christchurch Call[4]”を発表し、テロリストや暴力的な過激派のコンテンツをオンライン上から排除する取り組みを開始した。この宣言には現在、米国やEU諸国、日本など54カ国と、Facebook、Twitter、Google、Microsoft、LINEなど10のテック企業が支持を表明し署名している。ただし、情報規制のみならず、偽情報をとりまく状況は、EUをはじめとした欧米とアジア諸国とでかなり異なる点には、注視しておく必要がある。

こうした動向や研究会での議論を踏まえ、本提言における検討対象は「選挙介入や社会の不安定化などの影響工作も含む安全保障上の問題と考えられる」「外国から情報操作を目的として流布される」情報に限定する。内国民が発信する「フェイクニュース」については、仮に偽情報であっても、憲法第21条が定める「表現の自由」の制限につながりかねないことから一律の規制は困難であり、また必ずしも安全保障上の問題とはならないことから本提言の検討対象から外すこととする。なお、国際法の観点からも、外国からの選挙介入については、原則許されないとされている。

第２章　各国におけるディスインフォメーション事例

米国、英国、ドイツ、フランス、EU、台湾、シンガポール、香港、日本におけるディスインフォメーション事例の調査・分析結果を以下でそれぞれ詳述する。

１．米国

2016年５月、米国民主党全国委員会がサイバー攻撃を受け、委員会幹部の電子メール１万9,000件以上がハッカーによって窃取された。これらのメールは内部告発サイトであるWikiLeaksやDC Leaks.comで公表され、民主党全国委員会の幹部が、大統領指名候補争いでヒラリー・クリントン前国務長官と競っていたバーニー・サンダース上院議員を意図的に落選させるような動きをしていたことが暴露された。このリークにより民主党の全国委員長が全国大会前日に辞任する事態となり、民主党執行部の信頼は失墜した。この攻撃による大統領選投票結果への定量的な影響は未だ明らかにされていないが、結果として下馬評を覆しドナルド・トランプ大統領が選出されることとなった。選挙直後の2016年12月に公表された国土安全保障省（DHS）傘下の国家サイバーセキュリティ通信統合センター（NCCIC）の報告書[5]では、ロシア連邦軍参謀本部情報総局（GRU）が関与する「ファンシーベア」（別名「APT28」）と ロシア連邦保安庁（FSB）が関与する「コージーベア」（別名「オフィスモンキーズ」、「コージーカー」、「コージーデューク」、「APT29」）が、この攻撃に関与していると指摘されている。

また同時に、この選挙においては、TwitterやFacebookをはじめとするSNS上でフェイクニュースの流布やトランプ氏を支持しクリントン氏の評判を下げるディスインフォメーションを発信するかたちでロシアの関与するサイバー攻撃があったことが報告されている。米国上下両院情報委員会の調査[6]では、2,752件のTwitterアカウントおよび470件のFacebookアカウント、約120件のFacebookページおよび関連する80,000件以上のページコンテンツがロシア政府の工作に使われたとされる。また、10万ドル相当を費やしてロシア政府関係機関が3,393件のFacebookの広告枠を購入していたことを同社が認めている。

ネット世論を操作する「トロール部隊」を用いて、こうした虚偽またはトランプ氏支持に偏向した情報の書き込みを組織的に行っていたのが、サンクトペテルブルクにあったInternet Research Agency（IRA）である。表面的には新興財閥出資の民間会社を装っているが、その財閥はGRUやウラジミール・プーチン大統領とも密接な間柄にあることが米国国家情報長官室（ODNI）の報告書[7]で指摘されている。また、これらIRAの活動は民間会社による自主的な愛国活動ではなく、国家的な工作活動であったと評価され、報告書では以下のように述べられている。

「われわれはロシアのウラジミール・プーチン大統領が2016年、米国大統領選挙を標的にした情報戦を指示したと強く確信している。その一貫した狙いは、米国における民主的手続きへの信頼を損ね、クリントン氏を中傷し、大統領当選を妨げることだった。さらに、プーチン大統領とロシア政府は、明らかに次期大統領としてトランプ氏への支持を強めていったと認定している。」[8]

2018年の中間選挙中においても、全国共和党下院委員会（NRCC）に対してサイバー攻撃が行われ、同委員会幹部らのメールが数カ月にわたって窃取されていたことが明らかになっている[9]。しかし、2016年の米国民主党全国委員会への攻撃とは異なり、メールの内容が悪用されたことは確認されていない。これ以外にも、ロシア、中国、イランからサイバー攻撃や影響工作が行われていたことが米情報機関により報告されている[10]。

このような国外勢力の動きに対抗するため、米国は前方防衛（Defense Forward）戦略を採用し、サイバー攻撃への反撃を行っている。米サイバー軍（USCYBERCOM）は、中間選挙当日の2018年11月６日から数日間、ロシアのIRAによるインターネット・アクセスを遮断した。また、こうした選挙干渉に従事するロシアの工作員を特定し、「あなたの工作活動を監視している」「あなたを起訴や制裁の対象とする」といった警告メッセージを画面上に表示させた[11]。これは、国外のアクターによる選挙干渉に対して米軍が防衛行動を起こした初の事例となった。

2020年11月の米国大統領選挙でも、ロシアとイランが選挙への影響力行使を目的としてサイバー攻撃やディスインフォメーション活動を行ったと米情報機関は評価している[12]。中国については、影響工作を検討したものの実際には行わなかった、と評価しているが、同選挙期間前から中国による選挙関係者へのサイバー攻撃は確認されており、影響力を行使しようとする意図、諸活動があったとする情報機関内の少数意見もある。また、同選挙においては、陰謀論を信奉する米国内の運動「Qアノン」が利用されたことが特徴的である。選挙後、Qアノンやトランプ支持の極右勢力のメンバーらが連邦議会議事堂を襲撃するにまで至ったことは、社会矛盾や分断を利用したロシアによるディスインフォメーションがいかに効果的かを端的に示した一例といえる。

2. 英国

2016年６月23日に英国で実施されたEU離脱を問う国民投票では、ロシアの関与が指摘されている。開票結果は、EU残留支持が1,614万1,241票（約48％）、EU離脱支持が1,741万742票（約52％）で、離脱支持側が僅差で勝利した。

しかし、この離脱支持側の世論形成に、米国大統領選挙と同様、ロシアのIRAの関与があったことが、英国下院の文化・メディア・スポーツ委員会の中間報告で明らかにされている[13]。米国大統領選挙でIRAの関与が指摘された約2,700のTwitterアカウントおよび約4,000のFacebookページや広告、アカウント等を調査したところ、これらのアカウントの一部が英国の国民投票においても、EU離脱を支持・誘引する投稿を繰り返し行っていたことが確認されている。また、米国大統領選挙に干渉していないアカウントでも、IRAの関与による英国国民投票への干渉が行われた疑いがあり、同委員会のダミアン・コリンズ委員長は、TwitterおよびFacebookのCEOに、ロシアと関連があるアカウント一覧の提出を要請することとなった[14]。

現時点での調査においては、国民投票における直接のサイバー攻撃は確認されておらず、主にSNSによるディスインフォメーションの流布による干渉であったとされている。

3. ドイツ

2017年９月24日に実施されたドイツ連邦議会選挙（総選挙）では、全709議席のうち、メルケル首相与党のドイツキリスト教民主同盟・キリスト教社会同盟統一会派（CDU/CSU）が246議席（前回311議席）を獲得して第１党となり、メルケル首相が４期目を続投することとなった。

続いて、中道左派の社会民主党（SPD）が153議席（前回192議席）で第２党となった。しかしCDU/CSUの得票率は1949年以来最低、SPDの得票率は1933年以来最低となり、それに応じて両党とも前回から議席を大幅に減らす格好となった。その一方で、EU離脱や難民の受け入れ反対を謳う新興の右派政党・ドイツのための選択肢（AfD）が94議席を獲得し、連邦議会に初めて議席を確保すると同時に第３党に位置するという、大幅な躍進を果たした。

ドイツも英国同様、この選挙においては、2016年の米国大統領選のような直接的なサイバー攻撃はなく、ロシア関連のメディアとIRAによるSNSによるディスインフォメーションの流布による干渉が中心であった。ドイツにおいて特徴的であったのは、ボットアカウントの使用とロシア系メディアによるフェイクニュースの流布である。こうした動きは選挙前からみられ、その典型例が、2016年１月に報道された「リサ事件」である[15]。ロシア系ドイツ人の13歳の少女が難民のアラブ系男性グループに強姦された事件がロシア政府系メディアの第１チャンネル､RT、スプートニクを通じて繰り返し執拗に報道され、SNSの関連アカウントを通じて拡散された。実際は、事件は事実無根であったが、ロシア系のメディアおよび個人アカウントが煽ったことで、実際に各地でこの事件を批判し難民排斥を主張するデモや集会が数多く発生した。

また、2016年３月には、ベルギーの連続爆破テロ事件の犯人によるメルケル首相との自撮りツーショットとされる写真が、犯人の顔写真と共に拡散された。実際には、前者はメルケル首相がベルリンの難民センターを訪れた際、シリア難民の青年と撮影した写真であった。青年が自身のFacebookにアップロードした写真が誤ったキャプションで加工され、ロシア系のソーシャルメディア「フコンタクテ」にあるアノニマス系列のページ「アノニマス　コレクティブ」にアップされると、その記事を起点にSNSで拡散されて、メルケル首相の移民政策批判の材料となってAfDに親和的な言説が拡散されることとなった[16]。

「アノニマス　コレクティブ」にアップされた加工写真の投稿。
（https://vk.com/anonymous.kollektiv?w=wall-86775514_24356）

選挙期間中、AfD支持の書き込みがFacebookに約35万件、Twitterでは他の政党と比較して2.5倍以上の量に上ったことが確認されている[17]。得票率と比較すると相当な量であることから、ロシアに関連付けられるボットアカウントが相当数運用されていたことが窺える[18]。こうしてAfDの政策が支持される流れが意図的に作られていった。

2021年９月26日に実施された連邦議会選挙前、同年初めにCDUと議会に対しハッキング攻撃

があった。また、8月末に、次期連邦議会選挙の公式結果を公表する組織である連邦申告官のウェブサイトが、大量のデータを送り付ける「DDoS」攻撃により一時的に利用できなくなった[19]。さらに、9月までに、国会議員や政党の職員等に対する偽サイトに誘導するなどして情報を詐取する「フィッシング」攻撃が確認されている[20]。選挙直前の9月6日、ドイツ政府は、連邦議会選挙に関連した情報戦の準備となりうる、データ窃取のサイバー攻撃を非難した。ドイツ政府は、これらの活動が「ロシアの国家が関与する主体、特にロシアの軍事情報機関GRUによるもの」と断定できる「信頼できる情報」を持っていると述べ、ロシアにこれらのサイバー攻撃をやめるよう求めた[21]。また、連邦議会選挙管理委員会は、選挙期間中に流布された主なディスインフォメーションについて訂正情報と共に公開[22]しているが、そのうち、郵便投票の不正操作に関するものなどいくつかの言説がAfDによって拡散されていたことも確認されている[23]。

4. フランス

2017年5月に行われたフランス大統領選挙においても選挙干渉があり、その手法は2016年の米国選挙時と同様の類型であった。

まず、選挙の半年ほど前から選挙管理委員会やマクロン氏率いる共和国前進党事務局へサイバー攻撃が行われ、フィッシングメール等により実際にいくつかのデータが窃取されたことが報告されている。

これは、米国の民主党全国委員会にハッキングを行った集団と同一のAPT28によるものである[24]。しかし、米国と違い、明確なスキャンダル情報が入手できず、ロシア側はフェイクニュースの作成・流布もあわせて行った。ロシア政府系メディアのRTやスプートニクのフランス支局の番組や記事では、マクロン氏を指して、「米国金融業界の手先」「ゲイ」「イスラム擁護」といった意見が繰り返し発信され、さらにそれらをSNSで拡散させていったのである。その一方で、イスラム移民による危機を煽り、それを排斥する国民戦線への支持意見もボットアカウントを通じて大量に流布させた[25]。

結果的には、5月7日に行われたフランス大統領選挙の決選投票において、エマニュエル・マクロン氏（共和国前進）が得票率66％（第1回投票では24％）でマリーヌ・ル・ペン氏（国民戦線。得票率33％［第1回投票では21％］）を破り、大統領に就任した。

しかし、決選投票の前の4月23日に行われた第1回投票の選挙結果は類を見ないものであった。右派の共和党と左派の社会党のいずれも決戦投票に候補者を出すことができなかったのは、第五共和政の歴史上初めてのことであったからである。そして、国民戦線が決選投票まで候補者を残したのも史上初のことであった。国民戦線は反EU、移民排斥を掲げているため、ロシアとの政治的距離が近く、また実際にロシア政府から経済的支援を受けている。フランスにおけるロシアの選挙干渉は、マクロン氏を攻撃し、ルペン氏やその他の右派系候補者を支援するものであった。

5. シンガポール

シンガポールでは、2019年の通称フェイクニュース防止法（Protection from Online Falsehoods and Manipulation Act: POFMA）制定以後、情報通信メディア開発庁（Infocomm Media Development Authority）の所掌下にあるPOFMA Office[26]で虚偽情報の監視や通報処理

等を行っており、それら事例の公開も進めている。

公開される事例は、与党への政策批判等に対するファクトチェックといった側面が強く、対象も市民団体や国内メディアが中心で、外国からのディスインフォメーションとされる明確な事例は確認されていない。

直近の2020年７月の総選挙では、労働党、レッドドットユナイテッド、人民の声等の政党になりすましてFacebook上に偽のページが作成されたり、偽の個別メッセージが送信されたりした事案が確認されており[27]、国外勢力か国内勢力かは明らかではないものの、選挙に対する何らかの干渉行為は発生している。

6. EU

2019年の欧州議会選について、欧州委員会の報告書[28]では、欧州議会選の有権者に影響を与える「投票率の低下や投票行動の変化を狙った、ロシアによる継続的な偽情報活動を確認した」と評価されている。欧州委員会の調査において、過激な意見の流布や、移民や宗教の問題で世論を二極化させることを目的とした偽情報がウェブサイト上で1,000件ほど確認され、前年の同時期に比べて２倍に増えたことが判明している。その手法として、SNSのアカウントの使用や、フェイクニュースのサイトの作成によるディスインフォメーションの流布が行われていた。欧州委員会はこうした動きを、EUの価値観を損なう活動として批判するとともに、FacebookやTwitterなどSNSを運営するプラットフォーマー事業者に一層の対策強化を求めている。

7. 台湾

台湾では、総統選挙や地方選挙において、中国からの世論操作型の攻撃があったことが指摘されている。

2016年１月16日の総統選挙では、中国と距離を置く民進党の蔡英文（ツァイ・インウェン）主席が56％の得票率（国民党の朱立倫（チュー・リールン）主席31％、親民党の宋楚瑜（ソン・チューユイ）主席13％）で当選し、中国の影響はなかったように見えた。しかし、選挙前、台湾政府関係者、台湾独立運動家に向けて、特定の組織や個人に偽の電子メールを送り付けて情報を詐取する「スピアフィッシング」攻撃が行われ、中国人民解放軍との関係が濃厚と分析されるハッカー集団「APT12」がこの攻撃に関与していたことが指摘されている[29]。これらの攻撃によるリーク情報を利用したディスインフォメーションの流布、世論操作の類は観測されなかった。また、この選挙直後には、当選した蔡総統のFacebookのコメント欄に５万件にも及ぶ「荒らし」行為があった[30]。

2018年の統一地方選挙では、民進党が大敗を喫し、「最近、中国から事実でない嘘の情報が流れており、それがすべて台湾民主選挙への介入を意図した圧力手段である。これらの状況は各界が皆ともに目撃しており、すでに国際社会の普遍的な公認の事実である」と民進党の報道官がコメントした[31]が、具体的な攻撃内容は明らかにされていない。高雄市長選挙での民進党候補大敗について、対立候補の国民党・韓国瑜（ハン・グオユー）氏の動画共有サイトYou Tubeへの投稿動画に100万件規模の「高評価」がついたことなどから、中国の愛国ネットユーザーが数にものを言わせて台湾世論を引っ張った、と民進党側は解釈している[32]。明示的な攻撃ではなく、特定の候補者への肯定的な意見の大量流布というディスインフォメーションの手法が用いられたと

見られる。

2020年１月11日の総統選挙においては、現職の与党・民進党の蔡総統が、約820万票（得票率57％）を獲得して圧勝した。中国との関係強化が台湾に経済的利益をもたらすと主張する、対抗馬の最大野党・国民党の韓候補の得票数は約550万票（得票率39％）であった。この選挙期間中、蔡総統は「中国は全面的に（台湾社会に）『浸透』している」と、選挙介入への警戒を訴える一方で、野党候補の韓氏は、蔡総統が反中感情をあおって選挙に利用していると批判し、中国の介入について両候補の意見が割れた[33]。

選挙後の台湾当局や米国シンクタンクの分析[34]によると、同選挙でも中国の介入があったとされている。米国のシンクタンク戦略国際問題研究所（CSIS）の分析によれば、中国共産党は、中国本土に居住する台湾国籍者やその家族に、帰国して親中の候補へ投票するよう働きかけを行ったり、台湾の報道機関に潜入し、親中候補者の支持率を高めるために親中報道や自己検閲を行い、世論を操作したりしている。CSISは、結果として中国政府が好む候補者の支持率が高まったと評価している[35]。また、台湾内の報道によると、民進党に対抗する候補者の選挙活動に中国共産党が資金を供与していた容疑で、台湾政府は30件を超える事件を調査している。

中国共産党は、①資金供与によって親中の候補に有利となる偽の調査結果を台湾の報道機関と世論調査会社に作成・公表させる、②コメントの投稿で報酬を受け取れる「五毛党」を組織し、FacebookなどのSNSで反中候補者を攻撃し、親中コメントを投稿させる、等の活動を行っているとされる。実際に「五毛党」による台湾ウェブサイトへの１日当たりの攻撃件数は少なくとも2,500件に及んでいる。

8. 香港

香港においては、特定の選挙ではなく、デモという民主主義プロセスに対して、中国政府が世論操作型の攻撃を行っている。2019年３月、「逃亡犯条例」改正をきっかけに、逃亡犯条例改正案の完全撤回や普通選挙の実現などを目指す香港の民主化デモが始まった。これに対して中国政府は、こうしたデモは西側諸国や過激派の影響を受けたテロリストの扇動による不当なもの、という印象を与えるため、TwitterやFacebook上で国営メディアの記事や配信広告を利用し、世論誘導を試みたとされている[36]。

Facebookでの実際の投稿例。香港のデモ隊をISISを同一視させて扇動する（https://about.fb.com/news/2019/08/removing-cib-china/）。

この情報操作に関連して、Twitterでは963のアカウントが特定され、20万件以上のスパムネットワークが停止された。Facebookでは、5つのアカウントと1万5,000アカウント以上がフォローしていた7つのページ、約2,200アカウントがフォローしていた3つのグループが停止された。いずれの発表においても、これらは中国政府の支援による活動であり、意図的に香港に政治不和を引き起こそうとしたものであると、証拠をもとに評価されている。[37]

9. 日本

日本においては、諸外国とは異なり、明確な外国からのディスインフォメーションの事例は確認されていない。その理由としては、日本語という言語空間の特殊性、日本独自のSNSプラットフォームの存在があげられている。しかしながら、安全保障上懸念される事例が散見されるようになってきている。

2019年10月3日『琉球新報』は、米国が沖縄に新型中距離弾道ミサイル配備を計画しており、すでにロシア側に伝達した、と1面トップで報じた[38]。この報道は、ロシア政府の関係者が『琉球新報』に提供した情報であった。玉城デニー沖縄県知事が訪米中の10月18日、報道について国防総省関係者に確認したところ、そのような配備計画はないと否定されている。この報道に関しては、中距離核戦力（INF）の破棄を懸念するロシア政府が意図的に流したとの見方がなされている。

また、2018年の沖縄県知事選挙の事例もある。外国勢力からのディスインフォメーションと明確には特定されていないが、その類型や発生地点の安全保障上の重要性を考えると、注視して検討しておく必要がある。

2018年の沖縄県知事選挙では選挙中に、「沖縄県知事選挙2018」や「沖縄基地問題.com」というサイトが作成され、これらのサイトが掲載する米軍基地建設反対派である玉城候補（当時）や、同じ反対派の故・翁長雄志前知事を貶めるような「フェイクニュース」が、SNSを通じて拡散された。琉球新報や沖縄タイムスが発信された内容についてファクトチェックを行った結果、それらが「フェイクニュース」であったことが確認されている[39]。しかし、その発信源について、琉球新報が調査を行ったが、解明はされなかった[40]。

流布されたフェイクニュースは、玉城氏陣営に関する誤った情報であり、反玉城氏の姿勢を示していたため、国内の反対派勢力からの発信の可能性が高いといわれている。しかし、ディスインフォメーションは、選挙の結果に疑義を植え付けたり、正当な結果ではないと印象付けたりすることによって、民主主義における選挙の信頼性や正統性を貶めることを目的としてなされることもある。そのため、この事例についても、単なる落選運動の一環ではなく、民主主義を毀損することを目的とする勢力による攻撃の可能性についても考慮しておく必要がある。

そうした観点で考えると、琉球帰属未定論によって沖縄で世論形成を図っていると指摘されている中国[41]、そして沖縄の米軍基地は日露関係に障害であると明言し、近年沖縄に接近を図っているロシア[42][43]等の外国による干渉の可能性は完全には排除できない。

第３章　各国のディスインフォメーション対策

各国のディスインフォメーション対策に関する調査・分析結果（2021年11月現在）は下記の通り。なお、結果をとりまとめた表を各部冒頭に明記し、以下でそれぞれ詳述する。

1．米国

	米国
1-1． ディスインフォメーションによる干渉を検知、モニタリングする機関や制度があるか	○
1-2． 選挙等の民主主義プロセスについて干渉があったか否か調査し処罰する法律があるか	○
2． 選挙インフラが重要インフラに指定されているか	○
3． 選挙干渉行為に対し国家としてサイバー攻撃による反撃、防衛を行うことができるか	○
4． 選挙干渉等に関連しプラットフォーマーを規制する法律があるか	△
5-1． ディスインフォメーション対策としてメディアリテラシー教育を行っているか	○
5-2． 行政府による／行政府から独立した、ファクトチェック機関があるか	○ （1+61）

注：○印は「はい」、△印は「部分的に『はい』、または検討中」、×印は「いいえ」、
5-2欄の数字は「ファクトチェック機関の総数（行政府によるファクトチェック機関＋行政府から独立したファクトチェック機関）」を表す。以下同じ。

（1-1）　ディスインフォメーションによる干渉を検知、モニタリングする機関や制度

2018年５月、国土安全保障省（DHS）は、外国からの影響力行使に係るオペレーションに対処するため、DHS傘下の国家保護・プログラム総局（NPPD）内に、「外国からの影響力に対抗するタスクフォース（Countering Foreign Influence Task Force: CFITF）」を設置した。その後2018年11月に、議会超党派でサイバーセキュリティー・インフラセキュリティー庁（CISA）設置法が成立したことに伴い、NPPDはCISAに改変され、CFITFもCISAの傘下となった。CFITFは、MDM（Mis-, Dis-, Mal-information）と総称される情報操作や外国からの影響工作から国を防護する役割を担い、MDMのリスクや影響に関して、米国市民の理解を促進する、という具体的任務を与えられた。

2021年に、CFITFはCISAのMDMチームに改組され、現在その役割は、MDMに関する情報収集、分析、ファクトチェック結果の公表など多岐にわたる。MDMチームは、悪意あるMDM活動に対する国家のレジリエンスを構築するために、省庁間および民間セクターのパートナー、ソーシャルメディア企業、学界、および国際的なパートナーと緊密に連携し、

その調整役も担っている。

（1-2） 選挙干渉についての調査、処罰

2018年9月トランプ大統領は、米国の選挙（連邦レベル）における外国政府等の干渉に対し制裁を科す、大統領令13848に署名した。選挙結果が出てから45日以内に、当該選挙に干渉があったかどうかを国家情報長官が調査し、その後45日以内に司法長官と国土安全保障長官が制裁発動の是非を判断する。制裁対象者は米国内の資産が凍結され、米国人との取引が禁止される。

2018年の中間選挙においては、調査の結果、投票妨害や集計結果の改竄等は確認されず、また前章で示した通り、ロシア、中国、イランによる影響工作は確認されたものの、それが選挙結果に与えた影響は評価しない、という判断であった。一方、2020年の大統領選挙においては、ロシアおよびイランが影響工作を行ったと評価している。中国については、米中関係を考慮してそうした工作を行わなかったとしているが、少数意見として、いくつかの妨害工作があった点も記されている。ただし、いずれの国による工作においても、米大統領選挙の投票手続きや選挙結果そのものに外国政府が具体的な影響を与えた証拠はないという評価がなされた。

米国各州の州法レベルでは、2019年9月、テキサス州が、選挙の1カ月前に政敵に関する事実を歪めた政治的なディープフェイク（AIを用いた精巧な偽動画）を制作・共有することを軽犯罪行為とする法律を可決した。また同年10月、カリフォルニア州も、選挙候補者の偽装された動画、音声、写真を作成または配布することを違法とする法案を可決している。選挙に影響を与えるディープフェイクも処罰対象として認識され始めている。

（2）選挙の重要インフラ指定

2017年1月6日、DHSは、2001年の同時多発テロを受けて成立した2001年米国愛国者法（The Patriot Act of 2001）に基づいて、選挙を「重要インフラ」（Critical Infrastructure）の一つとして指定した。国土安全保障省（DHS）は重要インフラを「その無力化や破壊が、米国の安全保障、経済、国民の健康や安全を弱体化させると考えられている資産、システム、ネットワーク」と定義し、重点的に保全する対象として16分野を指定している。交通システムや防衛産業基盤、金融サービスなど各分野に担当省庁があり、選挙インフラはDHSが担当し、「政府施設」（Government Facility）分野におけるサブセクター（Election Infrastructure Subsector）として指定されている。これによって、DHSは要請があった場合に選挙管理機関への支援を行うことができるようになり、米国国家情報長官室（ODNI）など他の情報機関との連携、選挙ISAC設置によるサイバー上の脅威、脆弱性やインシデント（事故につながりかねない事態）等についての情報共有も進められることとなった。

（3）サイバー反撃

米国中間選挙が実施された2018年11月6日以後の数日間、USCYBERCOMは、ロシアのIRAによるインターネット・アクセスを遮断した。前章で既述の通り、IRAは2016年の米国大統領選挙等でディスインフォメーション活動により選挙干渉を行っていたとされ、ロシア

政府とのつながりも指摘されている企業である。また、USCYBERCOMは単なるアクセス遮断にとどまらず、相手方にサイバー攻撃に係る警告メッセージを送るといった作戦も実施した。

USCYBERCOMのポール・ナカソネ司令官は2021年３月に、2020年の米国大統領選挙で外国勢力による干渉や妨害の事前阻止を図るため二十数回の作戦を実施したことを、上院軍事委員会の公聴会で明らかにしている[44]。作戦の実態は明らかにされていないが、ロシア、イランや中国の敵対勢力を標的にした作戦であることは明言されており、2018年の中間選挙と同様に、外国勢力の干渉行動に係るハッカーのアトリビューション、戦術把握や相手方への対抗措置であったと考えられる。

（４）プラットフォーマー規制

2017年10月、超党派の議員３名によってネット広告規制法案（Honest Ads Act）が発表された。同法案では、月間5,000万名以上の閲覧者が訪れるプラットフォーム事業者に、年間500ドル以上の広告費を支払った政治広告の内容、対象、閲覧数、広告料、広告主等詳細の記録、開示を義務付けるとともに、米国の有権者に影響を与える目的での外国からの政治広告の購入を防止する措置をとることを求めている。2018年４月にFacebookが同法の支持を表明し、2019年に米国上院議会に提出されたが、法案可決には至らなかった。

2017年10月31日、米連邦政府上院司法委員会の犯罪・テロに関する小委員会が2016年の米大統領選へのロシア介入疑惑に関する公聴会を開き、Facebook、Twitter、Googleの法務顧問を招請して証言をさせ、質疑応答を行った。また2018年９月５日にも、米上院情報委員会にFacebook、Twitter、GoogleのCEOを招請し、最近のSNSでの海外（主にロシア）の影響と、サービスの透明性および責任についての証言を求めた。このように米国では、各プラットフォーマーが議会の公聴会に呼ばれ説明責任を果たすよう求められている。

また、2022年１月現在、1996年通信品位法（Communications Decency Act of 1996; 略称CDA、以下通信品位法と表記）第230条について改正をめぐる様々な動きがある。同条は、ユーザーがオンラインプラットフォーム上で発信する内容について、プラットフォーム企業が発信内容そのものの責任から免責されるよう定めたものである。これについて、近年、SNS上のディスインフォメーションやミスインフォメーションへの対応がプラットフォーマーに求められていることから、この免責要件を縮小もしくは廃止しようという機運が高まっている。2019年６月には、共和党の上院議員により同条の改正案が提出された。同改正案では、一定規模以上のプラットフォーム事業者が、ユーザーが発信した情報やその編集・削除について免責を受けるための要件として、ユーザーの発信した情報を政治的に偏向した方法で調整していないことについて連邦取引委員会の認証を受けることを求めている。これについては、政治的なバイアスの判断を政府機関に委ねることで表現の自由が抑制されるおそれがあるなどとして、当時、利用者団体や業界団体から批判があった。

2020年５月に、トランプ大統領は同条の解釈や施行方法を変更する大統領令13925を発し、Twitter、Facebook、Instagram、YouTubeを名指ししたうえで、プラットフォーマーの責任範囲を明確にして従来の編集者や出版社と同等の責任を課すことを求めた。これにより同条改正の動きが進み、2020年10月には共和党と民主党が同条の再考について合意し、上院通

商・科学・運輸委員会や司法委員会により公聴会が開かれ、Twitter、Google、FacebookそれぞれのCEOに対するヒアリングが行われた。これらの公聴会では、各社とも監視についての透明性を高めることに同意している。2021年には政権交代によりジョー・バイデン政権となったが、バイデン大統領は、同条はただちに廃止すべきと述べており、今後も改正の動きは進んでいくと思われる。

（５-１）メディアリテラシー教育

2017年４月、ワシントン州では、メディアリテラシー教育やインターネットの安全な使用を推進する法律が成立した。同法の下、学校教育でのメディアリテラシー教育の調査・見直しが行われている。同様の法律が、カリフォルニア州、コネティカット州、ロードアイランド州、ニューメキシコ州でも成立し、その他19州でも法案が提出され審議が進んでいる。これらについては、メディアリテラシー教育を推進する民間団体「メディア・リテラシー・ナウ（Media Literacy Now）」がモデル法案を作成して公開することで、同様の法律制定の動きを後押ししている背景がある。

（５-２）ファクトチェック機関

米国デューク大学のデューク・レポーターズ・ラボ（Duke Reporters' Lab）が作成・公開しているファクトチェックサイトデータベースによれば、米国には一定の基準[45]を満たすファクトチェック機関が多数ある。Googleと協力して検索時にファクトチェック結果を表示できる検索エンジンを開発したPoynter IFCNなど計61機関が活動している。

また、政府自体もファクトチェック機能を有しており、上述したCISAのMDMチームは、“Rumor Control[46]” というサイトを開設してファクトチェック情報を発信している。

2. 英国

	英国
1-1. ディスインフォメーションによる干渉を検知、モニタリングする機関や制度があるか	○
1-2. 選挙等の民主主義プロセスについて干渉があったか否か調査し処罰する法律があるか	△
2. 選挙インフラが重要インフラに指定されているか	×
3. 選挙干渉行為に対し国家としてサイバー攻撃による反撃、防衛を行うことができるか	△
4. 選挙干渉等に関連しプラットフォーマーを規制する法律があるか	△
5-1. ディスインフォメーション対策としてメディアリテラシー教育を行っているか	○
5-2. 行政府による／行政府から独立した、ファクトチェック機関があるか	○ （0＋7）

（1-1） ディスインフォメーションによる干渉を検知、モニタリングする機関や制度

2018年1月、英国政府は内閣府にタスクフォース「国家安全保障通信ユニット（National Security Communications Unit）」を設置し、外国勢力によるディスインフォメーション活動と戦っていく、と発表した。このタスクフォースは、サイバー空間上の外国勢力の活動をモニタリングし、分析、評価するとともに、他省庁や国際機関との調整を担う。また、タスクフォースと連携してSNSに特化してモニタリングする「緊急対応ユニット（Rapid Response Unit: RRU）」も設置された。RRUでは、データサイエンティストやメディア専門家などからなるチームが24時間体制でSNSを監視し、SNS上に流布される偽情報や誤報の検知や分析、評価を行っている。

（1-2） 選挙干渉についての調査、処罰

英国では、米国のような外国勢力によるディスインフォメーションキャンペーンを調査、処罰するような法整備を行うまでは至っていない。しかし、2017年1月、下院デジタル・文化・メディア・スポーツ（DCMS）特別委員会が、フェイクニュースによる民主主義への影響について調査を開始し、2018年7月に中間報告書[47]を、2019年2月に最終報告書[48]を公表した。報告書では、2014年のスコットランド住民投票、2016年の英国国民投票、2017年の英国総選挙について、政府が今までどれだけの調査を行ってきたかを公表するとともに、改めて独自の調査を行うように要請している。あわせて、情報操作を目的としてSNS等の情報システムを悪用したユーザーに対しては、より厳しい罰則を定めるよう勧告を行っており、今後、こうした法整備が進んでいくことが予想される。

（２） 選挙の重要インフラ指定

2021年11月時点では、選挙は重要インフラには指定されていない。

（３） サイバー反撃

2021年11月時点では、ディスインフォメーションを対象としたサイバー反撃の法制度は整備されていない。しかし、英国のベン・ウォーレス国防大臣がインタビュー[49]で、敵対国からのサイバー攻撃やディスインフォメーションに対抗してサイバー反撃を行う数千人規模のサイバー攻撃能力を持つデジタル戦センターの設置を英国国防省が計画中であることを明らかにしている。

（４） プラットフォーマー規制

上記のDCMSの最終報告書では、倫理規範の策定、プラットフォーマー企業に対する独立規制機関の確立と監視および執行、プラットフォーマーへの課金や課税についても勧告を行っている。それを受けて英国政府は、プラットフォーマーを監視・規制する専門の新組織を、日本の公正取引委員会にあたる競争・市場庁（CMA）に設け、CMA内に「デジタル市場ユニット（Digital Marketing Unit: DMU）」という組織を2021年４月に発足させると発表した。DMUは、デジタル広告が土台となるGoogleやFacebookなどを含むプラットフォーマー企業を対象に、公正な市場競争の面から問題があると判断される行動の差し止めや、是正措置の命令など各種の法的な権限を持つ。具体的には、サービスや利用者データの扱いに関する透明性を高めることを求める法的ルールを整備する。CMAは報道機関が提供する情報をプラットフォーマーが対価を払わずに利用していることも指摘し、報道機関が正当な対価を得られるよう記事使用の契約内容も監督するとしている。

（５-１） メディアリテラシー教育

上記のDCMSの最終報告書で、国民の情報リテラシー向上の取り組みを勧奨している。また、2018年６月には英国議会の超党派グループであるフェイクニュースと批判的リテラシー教育委員会が「フェイクニュースと批判的リテラシー」と題した最終報告書を公開し、フェイクニュースへの対策として批判的リテラシー涵養の必要性を訴えている。こうした状況を踏まえ、教育省と保健省の共同の取り組みとして、2020年から学校教育にフェイクニュース対策のカリキュラムが導入された。

また、政府コミュニケーションサービス（Government Communication Service: GCS）の新しいプログラム“Accelerate Programme”では、RRUが使用する偽情報や誤報を検知、評価するFACTモデルを用いたメディア担当者向けのトレーニングを特注して開発している。これには、RRUへの一連の出向による研修等も含まれている。こうした取り組みでは、情報の受け手だけでなく発信者を教育訓練する姿勢がみられる。

（５-２）ファクトチェック機関

英国では、BBCやチャンネル４、ロイター、ガーディアンといった報道機関を中心に、７つのファクトチェックサイトが運営されている。個人の寄付をベースとする慈善団体が運営

するフル・ファクト（Full Fact）はGoogleのファンディングを獲得し、テレビの字幕やその他のリアルタイムな情報ソースから自動でファクトチェックを行うLIVE AND TRENDSというツールを開発した[50]。

3. ドイツ

	ドイツ
1-1. ディスインフォメーションによる干渉を検知、モニタリングする機関や制度があるか	△
1-2. 選挙等の民主主義プロセスについて干渉があったか否か調査し処罰する法律があるか	△
2. 選挙インフラが重要インフラに指定されているか	×
3. 選挙干渉行為に対し国家としてサイバー攻撃による反撃、防衛を行うことができるか	×
4. 選挙干渉等に関連しプラットフォーマーを規制する法律があるか	○
5-1. ディスインフォメーション対策としてメディアリテラシー教育を行っているか	△
5-2. 行政府による／行政府から独立した、ファクトチェック機関があるか	○ （1＋6）

（1-1）ディスインフォメーションによる干渉を検知、モニタリングする機関や制度

2021年11月時点では、ドイツには恒常的にディスインフォメーションをモニタリングする機関はない。しかし、2021年9月8日に承認された新サイバーセキュリティ戦略と、それに基づいて策定された連邦選挙のITセキュリティ計画において、連邦情報セキュリティ庁（Bundesamt für Sicherheit in der Informationstechnik: BSI）が主管官庁とされた。同庁においては、選挙期間中のSNSにおいて、自動化されたボットや協調的な不正行為を検出した際には、対応するソーシャルメディアのプロバイダに通知して介入する部署が設置された。また、連邦選挙管理委員会は、選挙プロセス全般に関係するディスインフォメーションを特定し、これに対処する責任を負っており、特定した情報についてはファクトチェックサイトを通じて公表している。

（1-2）選挙干渉についての調査、処罰

ドイツでは、後述するプラットフォーマー規制を中心に対策をとっており、選挙期間中においても、上述のモニタリング調査にとどまっている。現時点では外国勢力のディスインフォメーション活動について調査を行い処罰をするといった事後制裁型の法整備はなされていない。

（2）選挙の重要インフラ指定

2021年11月時点では、選挙は重要インフラには指定されていない。

（3）サイバー反撃

2021年11月時点では、ディスインフォメーションを対象としたサイバー反撃の法制度は整

備されていない。

（４）プラットフォーマー規制

2018年６月、ドイツではSNS における法執行を改善するための法律（SNS執行法［Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerke: NetzDG］）が成立した。国内の利用登録者数が 200 万人以上の SNS 事業者が対象となり、対象事業者は、刑法上違法とされるコンテンツの申告手続き窓口を設け、申告があった場合は直ちに違法性を審査し、所定の期間内（違法性の度合いにより24時間以内または７日以内）に削除またはアクセスを遮断する義務を負う。違法コンテンツに関する苦情を年間100件以上受けた対象事業者は、半年ごとに当該期間を対象とする苦情処理報告書を作成し、連邦官報および自身のウェブサイト上で公表する義務を負う。これらに違反した場合、最大で5,000万ユーロの過料が科される。

2019年７月には、Facebookが提出した削除事案の報告書に対して、一部の事案しか記載されていないなどの不備を司法当局が指摘し、200万ユーロの罰金支払いを命じた[51]。2020年までで、同法に基づき過料が科されたのはこの１件のみである。同法については、削除内容の基準がわかりにくくネット事業者が過度に掲載コンテンツを規制してしまう「オーバーブロッキング」の懸念が指摘されている。そうした状況から、2020年６月に可決された「右翼過激主義と憎悪犯罪に関する法案」を包含する形でSNS執行法も同年に改正され、違法コンテンツの苦情申し立てプロセスを明確化するとともに、削除した違反コンテンツについて連邦刑事庁（Bundeskriminalamt: BKA）への報告が義務付けられた。また、事業者の報告書については、その透明性を高めるため、違法なコンテンツの自動検出アルゴリズムが使用されているかどうか、使用されている場合はそれらがどのように機能するかを報告する義務が加えられ、全体的に規制が厳しくなる方向で改正された。

（５-１）メディアリテラシー教育

ドイツの民間財団Stiftung Digitale Chancen（Digital Opportunities Foundation）が連邦経済エネルギー省および連邦家族・高齢者・女性・青少年省の後援を受け、EU主宰の若者や高齢者向けメディアリテラシー教育プロジェクト “Get your facts straight!” のパートナー機関となってドイツ国内での啓発に努めている[52]。

また、BSIは政治家を対象として、選挙時にメディアリテラシー教育キャンペーンを実施し、セキュリティガイドを作成することなどにより、候補者および選挙関係者のソーシャルネットワークアカウントの安全性を高める方法などについて啓発を進めている[53]。

（５-２）ファクトチェック機関

（１-１）で述べた通り、連邦選挙管理委員会が特定したディスインフォメーションについては、その訂正情報がファクトチェックサイト[54]を通じて公開されている。また民間では、第２ドイツテレビ（ZDF）などの地域由来の放送局、報道機関を中心に、６つのファクトチェックサイトが運営されている。

4. フランス

	フランス
1-1. ディスインフォメーションによる干渉を検知、モニタリングする機関や制度があるか	△
1-2. 選挙等の民主主義プロセスについて干渉があったか否か調査し処罰する法律があるか	△
2. 選挙インフラが重要インフラに指定されているか	×
3. 選挙干渉行為に対し国家としてサイバー攻撃による反撃、防衛を行うことができるか	×
4. 選挙干渉等に関連しプラットフォーマーを規制する法律があるか	○
5-1. ディスインフォメーション対策としてメディアリテラシー教育を行っているか	△
5-2. 行政府による／行政府から独立した、ファクトチェック機関があるか	○ （0＋17）

（1-1）ディスインフォメーションによる干渉を検知、モニタリングする機関や制度

2021年6月、フランス政府は、「国家を弱体化させる」ことを目的とした外国の偽情報やフェイクニュースに対抗する機関（Viginum: Le service de vigilance et de protection contre les ingérences numériques étrangères）を設立する計画を発表した。これは2022年4月に迫る大統領選挙への対策を意識したものであった。同機関は、2021年7月の政令で国防安全保障総局（SGDSN）の下に設置され、同年10月15日から運用が開始された。この機関の任務は、SGDSN長官によれば、「ソーシャルネットワーク上の情報を操作することを目的とした外国のデジタル干渉活動を監視、検出、特徴づけすること」であり、「決して情報の真偽を認定する機関ではない」。情報の真偽の認定は、政治家・メディア・司法の役割として切り分けられ、また、同機関の活動は、議会関係者、司法関係者、外交関係者、メディア関係者、研究者などで構成される倫理委員会によって審査される。

（1-2）選挙干渉についての調査、処罰

フランスでは、米国のような事後制裁型の調査や処罰に係る法整備は行われていない。しかし、2018年に外務省と軍事学校戦略研究所（L' Institut de recherche stratégique de l' École militaire: IRSEM）による報告書『情報操作—我々の民主主義への挑戦』[55]において、政府に対し、2016年米国大統領選挙におけるロバート・ミューラー米特別検察官によるロシア関係者およびロシア関連団体に対する訴追を例に挙げ、選挙期間中などに重大な妨害行為を行った責任者を処罰することを提言している。具体的には、選挙プロセスなどで重大な干渉行為を行った責任者を、責任の所在が明確に特定できる場合には、経済制裁や法的手続きを通じて処罰することに言及しており、今後、米国の事後制裁型と同様の法整備が進むと思

われる。

（２）選挙の重要インフラ指定

2021年11月時点では、選挙は重要インフラには指定されていない。

（３）サイバー反撃

2021年11月時点では、ディスインフォメーションを対象としたサイバー反撃の法制度は整備されていない。

（４）プラットフォーマー規制

2018年11月、情報操作との戦いに関する法律が成立した。選挙期間内に、規定されたフェイクニュースの定義にあてはまる情報が流布されている場合、裁判所は送信防止措置を命ずることができる。また、プラットフォーマーは記事体広告（スポンサードコンテンツ）の資金源や発信主体の公開、ボット対策、リテラシー教育などの協力義務を負い、テレビやラジオについては、外国が経営権を有するメディアがフェイクニュースを報道している場合は、メディア規制機関が放送停止を命ずることができる。

（５-１）メディアリテラシー教育

前掲の報告書『情報操作―我々の民主主義への挑戦』において、青少年だけでなく成人にも同様にメディアリテラシー教育を行うべきだとの提言が政府にされている。

2015年以降、フランス政府はオンラインでのメディアリテラシー向上に関する教育コースへの資金提供を増やしており、毎年約３万人の教師やその他の教育専門家が、このテーマに関する政府のトレーニングを受けている。フランス文化省は、2018年にはコースの年間予算をそれまでの２倍の600万ユーロ（約680万ドル）に増やし、教育省は同様の高校コースを選択科目として国のカリキュラムに追加して、インターネットやその他メディアで数千人が利用できるようにしている。また、同年、政府はジャーナリストや教育者と協力して中学校コースを新設している。さらに、一部の地方自治体では、若い成人が毎月の給付金などの福利厚生を受け取る際にインターネットリテラシーコースを完了していることを要求するなど、全国家的にメディアリテラシー教育の向上に取り組んでいる。

（５-２）ファクトチェック機関

フランスでは、AFPやルモンドなどの報道機関を中心に、17のファクトチェックサイトが運営されており、気候問題や移民問題に特化したファクトチェックサイトも公開されている。

5. シンガポール

	シンガポール
1-1. ディスインフォメーションによる干渉を検知、モニタリングする機関や制度があるか	○
1-2. 選挙等の民主主義プロセスについて干渉があったか否か調査し処罰する法律があるか	○
2. 選挙インフラが重要インフラに指定されているか	×
3. 選挙干渉行為に対し国家としてサイバー攻撃による反撃、防衛を行うことができるか	×
4. 選挙干渉等に関連しプラットフォーマーを規制する法律があるか	○
5-1. ディスインフォメーション対策としてメディアリテラシー教育を行っているか	○
5-2. 行政府による／行政府から独立した、ファクトチェック機関があるか	○ （1＋2）

（1-1）ディスインフォメーションによる干渉を検知、モニタリングする機関や制度

2021年10月、外国干渉防止法（Foreign Interference [Countermeasures] Act : Fica）がシンガポール議会において可決された。同法は敵対的な外国勢力による情報キャンペーン（Hostile Information Campaigns : HIC）および政治的に重要な人物とみなされる国内の代理人を通じて実施される国内政治への干渉を防止、検出し、妨げるための対抗策を導入することを目的としている。

シンガポール内務省によれば、HICは国内の政治的言説に影響を与え、社会的不和を扇動し、政治的主権を弱体化させることを目的とし、外国の利益を促進するための方法として、洗練されたオンラインツールと戦術が用いられるとしている。そのため、HICコンテンツが発生している疑いがある場合、内務大臣は、ソーシャルメディアサービス、関連する電子サービス、インターネットアクセスサービス等について防止措置をとることを命じることができ、そのために内務省は、HICを調査する権限を有している。

（1-2）選挙干渉についての調査、処罰

上記の外国干渉防止法は選挙期間に限ったものではないが、シンガポールの政治プロセスに直接関与している個人および非個人を「政治的重要人物（Politically Significant Persons: PSP）」と定義し、外国からの干渉のリスクを軽減するための対策を講じるとしており、選挙干渉への対策も考慮されている。

PSPは、政党、政治の要職にある者、国会議員、議会のリーダー、野党の党首、選挙候補者およびその選挙代理人を対象とする。さらに、外国からの干渉を受けやすいその他の個人や団体についても、その活動が政治的目的に向けられている場合には、内務大臣が指定する関連する所轄官庁によってPSPとして指定することができる。PSPに指定された個人や団体

は、外国からの影響を受ける可能性があると考えられる寄付を受けた場合や、ボランティアやメンバーとして関わった人々の所属等について公表を求められた場合、開示する義務を負う。

HICに関与していると疑われるウェブサイト等については、アクセス遮断や禁止サイトに認定したうえでの広告収入の遮断といった措置がとられる。PSPについては、外国人の関与を申告せずに情報をオンラインで公開するという違反行為（もしくはその意図があった場合）について、14年以下の懲役と、個人の場合は10万シンガポールドルの罰金、ニュースサイトなどの法人の場合は100万シンガポールドルの罰金が科せられる。

（２）選挙の重要インフラ指定

2021年11月時点では、選挙は重要インフラには指定されていない。

（３）サイバー反撃

2021年11月時点では、ディスインフォメーションを対象としたサイバー反撃の法制度は整備されていない。

（４）プラットフォーマー規制

2019年10月、翌2020年７月の総選挙における虚偽情報対策を見据えて、通称フェイクニュース防止法（POFMA）が施行された。同法は、下記の要件を満たす情報の流布を禁じている：①政府が虚偽と認定した情報、②国の安全保障や公共の福祉を脅かすおそれがあり、集団間の敵意や憎悪を煽ると判断された情報、③選挙の結果に影響を与える可能性がある偽情報、④政府の職務執行能力に対する国民の信頼を損なうおそれのある誤った情報。

また、同法セクション７では、個人が、虚偽であると知りながら、下記の項目に抵触する虚偽の言説（statement）を伝達（例えばリツイートなど）することを禁じている。

・シンガポールの安全保障に悪影響を及ぼす可能性のある言説
・公衆衛生、治安、財政の安定に悪影響を及ぼす可能性のある言説
・シンガポールと他国との友好関係に悪影響を与える可能性のある言説
・大統領選挙、総選挙、補欠選挙、国民投票の結果に影響を与える可能性のある言説
・異なるグループの人々の間に敵意、憎悪を煽る可能性のある言説
・政府機関の義務・機能・執行に対する国民の信頼を低下させる可能性のある言説

セクション７に違反した個人は、５万シンガポールドル以下の罰金および／または５年以下の禁固刑に処される。個人以外、例えば、ハイテク企業が運営するオンラインメディアプラットフォームの場合は、最高50万シンガポールドルの罰金が科せられる。また、偽のオンラインアカウントやボットを使用してそのようなデマを広めた場合、個人の違反者は10万シンガポールドル以下の罰金および／または10年以下の禁固刑に処される。個人以外の場合は、100万シンガポールドル以下の罰金が科せられる。

同法のセクション３では、POFMAの対象となる伝達（communication）を、インターネット、FacebookやTwitterなどのソーシャルメディア、マルチメディアメッセージング

サービス（MMS）やショートメッセージサービス（SMS）を通じて、シンガポールの１人以上のエンドユーザーに伝達された言説と定義している。エドウィン・トン法律担当上級大臣は、POFMAはプライベートなチャットグループやソーシャルメディアグループなどのクローズドなプラットフォームも対象となることを議会で明らかにしている。

シンガポール政府は、同法に抵触する情報を流布する者に対し、当該情報の削除、掲載の停止、および同情報が誤っているという表明をした訂正文の掲載を命ずることができる。また、政府は、SNSのプラットフォームを提供している企業に対しても、当該情報が虚偽であったことを利用者に伝達することを命令する権限を有している。フェイクニュースの認定権限は政府にあり、掲載したインターネット仲介業者に指示を出し、対象アカウントへのサービスの停止、または他のユーザーとのやり取りの禁止を要求することができる。

コンテンツと訂正の内容はシンガポール政府のウェブサイト「ファクチャリー（Factually）[56]」に掲載されるが、虚偽情報であることをウェブ上で表示する際には、政府のサイトへのリンクを貼り付けなければならない。

同法によるプラットフォーマー等に対する法執行の例として、次のようなものがある。

・2019年11月、シンガポール政府がPOFMAに基づき、Facebookに選挙の不正を告発する内容の記事の訂正を指示したことがあげられる。Facebookは訂正した投稿の末尾に「訂正通知」を掲載したが、一方で、同国政府に対し新たな法律を慎重に運用するよう求めた。
・2020年１月、マレーシアの人権団体がFacebookに投稿した「死刑執行時にロープが切れたときのために、シンガポールの刑務官は残酷な執行方法について訓練を受けている」などといった言説に対し、シンガポール政府は「事実ではない」として、同人権団体と人権団体の主張を拡散したサイトに訂正を命令するとともに、国内から同人権団体のウェブサイトへのアクセスを遮断することを接続事業者に命令した。
・2020年７月、野党「ピープルズ・ボイス」のFacebookやリム・ティーン党首のYouTubeにおいて、野党やティーン党首が「外国人に無料の教育機会を提供するため、多額の資金を使っている」という主張を投稿したことに対し、シンガポール政府はPOFMAに基づいて、野党とティーン党首に訂正命令を出した。
・2021年８月、国内で新型ウイルスによる死者が出たとする地元メディア大手が運営するウェブサイトの掲示板への書き込みに対し、シンガポール政府は否定し、掲示板の運営者に訂正を命令した。
・2021年10月、シンガポール保健当局は新型コロナのワクチンが安全ではないと主張するウェブサイト「Truth Warriors」に対し、POFMAを適用し、犯罪捜査を進めると明らかにした。シンガポール保健当局は声明を通じ、「すべて検証されていない虚偽資料」とし、「ウェブサイトの閲覧者を危険に陥れる情報」と指摘するとともに、「POFMAの適用を決めたことにより、同ウェブサイトは読者に『内容に対する虚偽事実』が含まれているという告知を掲載しなければならない」との命令を行った。

POFMAの運用に関しては、特定の情報が虚偽あるいは同法上の「フェイクニュース」であることを認定する権限は政府にあるため、言論弾圧につながるとの批判も起きている。

（５-１）メディアリテラシー教育

2019年１月、文化社会青年省大臣が、同省の主導で「フェイクニュースとの闘い」と題したセミナーを国内の宗教社会団体向けに開催し、セキュリティに関するアドバイザリーブックを作成、配布するという２つの新しいイニシアチブを開始することを発表した[57]。

（５-２）ファクトチェック機関

シンガポールでは、POFMAの規定に基づき、虚偽の可能性のある情報の通報を受け付けている。その通報に基づき、政府が虚偽と認定した情報については、ウェブサイト「ファクチャリー（Factually）[58]」でファクトチェックの結果を公開している。また、民間では、AFPなどの報道機関を中心に、２つのファクトチェックサイトが運営されている。

6. EU

	EU
1-1. ディスインフォメーションによる干渉を検知、モニタリングする機関や制度があるか	○
1-2. 選挙等の民主主義プロセスについて干渉があったか否か調査し処罰する法律があるか	△
2. 選挙インフラが重要インフラに指定されているか	△
3. 選挙干渉行為に対し国家としてサイバー攻撃による反撃、防衛を行うことができるか	×
4. 選挙干渉等に関連しプラットフォーマーを規制する法律があるか	○
5-1. ディスインフォメーション対策としてメディアリテラシー教育を行っているか	○
5-2. 行政府による／行政府から独立した、ファクトチェック機関があるか	○ （1＋1）

（1-1）ディスインフォメーションによる干渉を検知、モニタリングする機関や制度

ロシアの行うディスインフォメーションキャンペーンに対処するため、EUの戦略的コミュニケーションに関する行動計画の一環として、2015年3月に戦略的コミュニケーション・タスクフォース（East StratCom Task Force）が設立された。このタスクフォースは欧州対外行動庁（EEAS）の戦略的コミュニケーション・情報分析部門（AFFGEN.7）に属しており、同部門には、EUのディスインフォメーションに関する緊急警報システム（EU's Rapid Alert System on Disinformation）など、国際協力に重点を置いた連携チームもある。戦略的コミュニケーション・タスクフォースは、ディスインフォメーションの傾向分析と報告、ディスインフォメーションのナラティブの解明、ディスインフォメーションの脅威に対する市民の意識向上を目指したリテラシー教育、情報共有のための国際協力など、多岐にわたる活動を行っている。2021年3月時点で、16名の常勤スタッフと1,100万ユーロの予算を有している。

（1-2）選挙干渉についての調査、処罰

選挙干渉に関しては、主にロシアのディスインフォメーションに対抗するために、欧州委員会を中心としてEU全体での対策が早くから検討されていた。2017年11月にハイレベル専門家グループ（HLEG）を立ち上げ、翌2018年3月にHLEGによる報告書を公表した。その報告書をもとに、4月にフェイクニュース対策に関する欧州委員会声明を公表し、この声明を踏まえて「偽情報に関する行動規範」が作成された。同規範において、SNSやウェブメディアにおける透明性の向上やサイバーハイジーン（衛生管理）確保を目指し、「行動規範」に同意したプラットフォーマーに対して履行を求めている。

こうした流れを背景に、2020年12月に欧州民主主義行動計画（The European Democracy

Action Plan）[59]が公表されている。この計画では、ディスインフォメーションの加害者にコストを科すことも目的の一つとして明示されており、域内のディスインフォメーション活動のモニタリングおよび調査を進めるため、タスクフォースの強化や能力構築支援を行うことを表明している。加害者に対して制裁を科す方向性が示されているものの、その内容までは明らかになっていない。

（２）選挙の重要インフラ指定

2021年11月時点では、EU全体として選挙を重要インフラに指定する制度はない。しかし、2019年、欧州ネットワーク情報セキュリティ庁（European Union Agency for Cybersecurity: ENISA）は、加盟国に対して、選挙システム、選挙プロセス、および選挙インフラを重要インフラとして分類し、必要なサイバーセキュリティ対策を実施するための法的義務を検討する必要があると勧告[60]している。

（３）サイバー反撃

2021年11月時点では、ディスインフォメーションを対象としたサイバー反撃の法制度は整備されていない。

（４）プラットフォーマー規制

EUでは早くからプラットフォーマー規制に取り組んできた。これまでの行動規範では、プラットフォーマーの自主規制に主眼を置き、行動規範に同意したプラットフォーマーに対し、①広告掲載内容や資金提供元の精査、②政治的課題に基づく広告の透明性を高めるような取り組み、③その実施状況についての定例的な報告、を求めてきた。そして2020年12月の欧州民主主義行動計画の策定により行動規範が強化されることとなり、2021年５月には「偽情報に関する行動規範を強化するためのガイダンス[61]」が公表された。同「ガイダンス」では、デジタルサービス法を制定し、以下を定めている。プラットフォーマーとの共同規制体制への移行、プライベートメッセージングサービス業者を含めた署名者の拡大、規範の目的を達成するためのコミットメントの強化、規範実現のための明確な主要業績評価指標を含む強固なモニタリングの枠組み、加盟国ごとに分類された標準的な形式の報告書の提出、透明性センターの設立、規範を進化・適応させるための常設タスクフォースの設立、である。

また、欧州委員会は、スポンサー付きの政治コンテンツの透明性に関する法制化も提案している。

（５-１）メディアリテラシー教育

上記の欧州民主主義行動計画においては、「新しいデジタル教育の行動計画（The New Digital Education Action Plan（2021-2027））」と連携して、ディスインフォメーションに対抗するためのメディアリテラシー教育を行うことを定めている。新しいデジタル教育の行動計画においては、教師と教育スタッフのための共通ガイドラインの策定、通信事業者やジャーナリスト、欧州デジタルメディア観測所（European Digital Media Observatory: EDMO）といったさまざまなステークホルダーとの協働、デジタル教育推進のための教育

団体や研究団体への資金援助等の方向性が示されている。

（５-２）ファクトチェック機関

EU全体のファクトチェック機関としては、EU vs DisinfoとEU factcheckがある。前者は戦略的コミュニケーション・タスクフォースがモニタリングし検証した情報を公開している。行政府から独立した機関ではないが、ロシアを主な対象として体系的なディスインフォメーションのデータベースを公開しており、有益な分析を行っている。後者は欧州ジャーナリズムトレーニング協会（The European Journalism Training Association: EJTA）が母体の民間ベースのファクトチェック団体である。

7. 台湾

	台湾
1-1. ディスインフォメーションによる干渉を検知、モニタリングする機関や制度があるか	○
1-2. 選挙等の民主主義プロセスについて干渉があったか否か調査し処罰する法律があるか	○
2. 選挙インフラが重要インフラに指定されているか	×
3. 選挙干渉行為に対し国家としてサイバー攻撃による反撃、防衛を行うことができるか	×
4. 選挙干渉等に関連しプラットフォーマーを規制する法律があるか	△
5-1. ディスインフォメーション対策としてメディアリテラシー教育を行っているか	○
5-2. 行政府による／行政府から独立した、ファクトチェック機関があるか	○ （1＋4）

（1-1）ディスインフォメーションによる干渉を検知、モニタリングする機関や制度

台湾では、2019年末までに、オードリー・タンデジタル担当政務委員の主導のもと、全ての省庁に「Meme Engineering team（迷因工程團隊）」を配備し、SNSの監視とファクトチェックの結果の発信に努めている。行政院は「2-2-2の原則」を採用し、各省庁のチームが偽情報や誤報を発見した場合、その情報に対する正しい解説を20分以内、200字以内、2枚の画像付きでSNSに公開することが求められている。

（1-2）選挙干渉についての調査、処罰

2019年12月、域外敵対勢力による台湾への介入を防ぐための「反浸透法」が可決され、翌2020年1月に施行された。同法では、域外敵対勢力の指示や委託、資金援助を受けての政治献金や、選挙での宣伝活動、偽情報の拡散、合法的に行われているデモの妨害などを禁止している。これに違反した場合、最高5年の懲役、500万台湾ドル（約1,800万円）の罰金などが科せられることとなる。同法は、外国勢力によるディスインフォメーションキャンペーンのみを射程とするものではなく、外国勢力による台湾への政治介入そのものを防ぐ目的を有している。

（2）選挙の重要インフラ指定

2021年11月時点では、選挙は重要インフラには指定されていない。

（3）サイバー反撃

2021年11月時点では、ディスインフォメーションを対象としたサイバー反撃の法制度は整備されていない。

（４）プラットフォーマー規制

台湾では、SNS上のフェイクニュース等の取り締まりについては、プラットフォーマーを規制する方向性ではなく、あくまでもフェイクニュースの発信者を規制、処罰する方針をとっている。災害防止救助法やラジオテレビ法（廣播電視法）など７つの法律について、フェイクニュース防止のための法改正を行い、また、「社會秩序維護法」においては、「デマの流布」に関わる条項を追加し、フェイクニュースにも適用できるよう対象を拡大、過料や拘留の罰則を強化している。さらに、SNSのプラットフォーマーがフェイクニュースを削除しなかった場合に罰金を科すことなどを含む法改正も検討していると閣僚がコメントをしており、今後、この方向での法改正も進むと考えられる。

（５-１）メディアリテラシー教育

台湾では、政府がFacebook、Google、LINEの３社とメディアリテラシー教育において協力関係を築いており、同３社は、そのための教育プログラムに資金提供している。

（５-２）ファクトチェック機関

台湾では、財団法人台湾媒体観察教育基金会（TAIWAN MEDIA WATCH）と優質新聞発展協会（weReport）が共同で立ち上げた台湾ファクトチェックセンター（Taiwan Fact Check Center）を中心に、４つの団体およびウェブサイトが活動しており、LINEやチャットボットといったコミュニケーションツールも積極的に活用している[62]。

また、上述の通り各省庁が「２-２-２の原則」に基いたファクトチェックの発信に取り組んでいる。この施策では、フェイクニュースや誤報は、センセーショナルな内容であるだけに拡散速度が速いことを意識し、正確な情報がフェイクニュースよりもより広く速く伝わるように「“humor over rumor”（ユーモアが嘘をしのぐ）戦略」を採用している。この「戦略」では、「ミームエンジニアリング」という手法が用いられ、マスコットキャラクターやコミカルな画像など、ユーモアに富んだ内容が、ファクトチェック結果の解説とあわせて発信されている。

8. 日本

	日本
1-1. ディスインフォメーションによる干渉を検知、モニタリングする機関や制度があるか	×
1-2. 選挙等の民主主義プロセスについて干渉があったか否か調査し処罰する法律があるか	×
2. 選挙インフラが重要インフラに指定されているか	×
3. 選挙干渉行為に対し国家としてサイバー攻撃による反撃、防衛を行うことができるか	×
4. 選挙干渉等に関連しプラットフォーマーを規制する法律があるか	×
5-1. ディスインフォメーション対策としてメディアリテラシー教育を行っているか	×
5-2. 行政府による／行政府から独立した、ファクトチェック機関があるか	○ （0＋3）

（1-1）ディスインフォメーションによる干渉を検知、モニタリングする機関や制度

現状では、我が国においてディスインフォメーションによる干渉を検知しモニタリングするような機関や制度はなく、ディスインフォメーションに対応する主管官庁も定められていない。

サイバーセキュリティ基本法第19条では、「国は、サイバーセキュリティに関する事象のうち我が国の安全に重大な影響を及ぼすおそれがあるものへの対応について、関係機関における体制の充実強化並びに関係機関相互の連携強化及び役割分担の明確化を図るために必要な施策を講ずるものとする」と記載するにとどまり、サイバー安全保障を担う行政機関も定まっていない。

2021年９月に閣議決定された「サイバーセキュリティ戦略」においては、サイバー攻撃に対する防御力、抑止力、状況把握力の強化のために、それぞれの主管官庁を「NISC、内閣官房、警察庁、法務省、外務省、文部科学省、防衛省」等として列記している。また、国内プラットフォーマーに対するルール作りについては総務省が「プラットフォームサービスに関する研究会」を立ち上げて検討したが、ディスインフォメーションに対しては、法整備と情報収集や分析、それらをもとにした対抗措置という一連の対策が必要であるが、現状の所掌では一元的な対応が不可能である。

（1-2）選挙干渉についての調査、処罰

現時点では、虚偽情報や悪意ある情報に対する一定程度の規制[63]はあるものの、外国からのディスインフォメーションを調査し、制裁を与える法制度は日本には存在しない。

（２）選挙の重要インフラ指定

2021年11月時点では、選挙は重要インフラには指定されていない。

（３）サイバー反撃

2021年11月時点では、ディスインフォメーションを対象としたサイバー反撃の法制度は整備されていない。

（４）プラットフォーマー規制

プラットフォーマー規制については、総務省主宰のプラットフォームサービスに関する研究会で検討がなされてきた。最終報告書[64]によれば、現状では、各プラットフォーマーによる自主的、自律的取り組みを政府が尊重する方向である。今後、これらの自主的スキームが達成されない場合、あるいは将来的に偽情報の拡散等の問題に対して効果がないと認められる場合には、プラットフォーム事業者に対する行動規範の策定や対応状況の報告・公表など、行政からの一定の関与も視野に入れて検討を行うこととしている。政府主導の積極的な対策は現時点では行われていない。

（５）メディアリテラシー教育およびファクトチェック機関

現在、日本の情報リテラシー教育はプログラミング教育が主体で、公教育の中にディスインフォメーション対策やファクトチェックが入れ込まれていない。また、ファクトチェックについては、表現の自由との兼ね合いもあり政府は行っておらず、民間のファクトチェック・イニシアティブ（FIJ）のほかメディアの自主的な取り組みに委ねられている。

前掲のプラットフォームサービスに関する研究会の最終報告書において、ファクトチェックの推進やICTリテラシー向上の推進が謳われているが、具体的な施策は提示されていない。ファクトチェックに関しては、「政府は、ファクトチェック機関とプラットフォーム事業者の間の協力・連携関係が維持・向上するよう、適切な役割を果たしていくことが適当」であるとし、ファクトチェック機関の主体のあり方や独立性確保については、議論途上であると指摘するにとどまる。同様にICTリテラシーについても、「政府やICTリテラシー向上の取組に関わる関係者は、既存の ICTリテラシー向上施策において、上記の点を踏まえ、偽情報の問題に対応した教材やカリキュラムにアップデートしていくことが適当」、「行政や民間団体のみならず、プラットフォーム事業者と協働したICTリテラシー向上の取組を推進していくことが適当」といった記述はあるものの、どのようなアップデートを行うのか、どのような協働のスキームを作っていくのか具体的な方策についての記述はない。

第４章　政策提言

～サイバー空間を用いる外国からの情報操作に備えを！～

１．ディスインフォメーション対策を行う情報収集センターの設置

（１）民主主義の選挙プロセスにおける、外国からのディスインフォメーションに対応するため、ディスインフォメーションを用いた外国勢力の干渉に関する情報収集センターを設置する。同センターにおいて、外国からのディスインフォメーションに類する活動のモニタリング、調査・分析を行う。また、外国からのディスインフォメーション対応のオペレーションも司法当局とともに担う。こうした活動を効果的に行えるよう特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律（プロバイダ責任制限法）の改正を行う。

（２）ディスインフォメーションによる攻撃に対して事後制裁および国際法上許容される対抗措置を行うことを可能にする法律の制定を検討する。ディスインフォメーションを用いた外国勢力の干渉に対する取り締まりが行えるよう、公職選挙法および日本国憲法の改正手続に関する法律（国民投票法）を改正する。なお、その際、日本国憲法が保障する国民の知る権利に留意し、国は取り締まりに関する情報開示を積極的に行う。

以下、公職選挙法、日本国憲法の改正手続に関する法律、プロバイダ責任制限法の改正案とその根拠を述べる。なお、公職選挙法、日本国憲法の改正手続に関する法律、特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律については、条文改正案を末尾【参考】欄に記載する。

①公職選挙法の改正

改正のポイント

・虚偽事項公表罪、虚偽表示罪に関連して、選挙期間中において虚偽事項の発信や虚偽表示を行った者に対する当局の調査義務を明記する。

・虚偽事項の公表に関して、候補者本人と狭く解釈している対象を、「何人も」に拡大し、外国人も含む解釈とする。具体的に、公職選挙法第235条１項、２項に下線部分を追記（【参考】参照）する。また、選挙の正当性や選挙制度そのものに関して、信頼や信用を失墜させる目的での虚偽事項の公表も禁ずる。なお、虚偽事項に関しては、「検証可能で虚偽または誤解をまねく情報」と定義する。

・インターネットの利用に関して、虚偽事項の掲載禁止を含める。具体的に公職選挙法第142条の７に下線部分を追記（【参考】参照）する。

・外国政府が関与する者の選挙運動の制限を検討する。

現在、選挙中の虚偽情報に関連する規制としては、公職選挙法において虚偽事項公表罪（公職

選挙法第235条２項）において罰則が定められている。また、ウェブサイト上の選挙運動用・落選運動用文書図画において電子メールアドレス等の表示義務を課しており（公職選挙法第142条の３第３項、第142条の５第１項）、違反した場合は氏名等の虚偽表示罪（公職選挙法第235条の５）の対象となる。表示義務違反については、限られた選挙期間中に、真にウェブサイト作成者本人の連絡先であるかを確認するのは容易ではなく、効力に疑問が残る。加えて、公職選挙法では、候補者・政党等以外の者による電子メールを利用する方法による選挙運動は禁止されている一方で、同法上ではSNS上のダイレクトメッセージ等はウェブサイトに分類されており、これらを利用した候補者・政党等以外の者による選挙運動が許されている点も、SNSの利用が当たり前となっている今日、時代錯誤の感が否めない。改正公職選挙法のガイドライン[65]では、「海外のウェブサイトによる情報発信等、取締りに限界があることは事実」と認める一方で、「悪質な誹謗中傷等が選挙期間中になされた場合、（略）ウェブサイトやブログ等で適時適切に正しい情報を有権者に発信しこれに対抗することが可能となる」と述べているが、虚偽情報のほうが真実や訂正の情報よりも拡散速度が速く、拡散範囲が広い、という各種研究結果[66]を踏まえれば、これだけでは対策として十分とは言い難い。そのため、ディスインフォメーションに利用されうる虚偽事項の発信について、上に記した規制を行うことが望ましい。

また、特に、民主主義プロセスに対する外国からのディスインフォメーションに焦点を当てた場合、外国政府の関与がある外国人の選挙運動や落選運動も禁止すべきである。現行の国内法からは、外国人の選挙運動の禁止や外国政府による落選運動を直接禁止する法的根拠を得ることは難しいが、国際法では内政不干渉禁止原則があり、外国政府の影響や選挙運動を制限することができると考えるべきである。改正公職選挙法のガイドラインにおいて、「外国人は、現行法において、選挙運動が禁止されていないため、インターネット選挙運動の解禁後も、同様に、これを行うことができる」と明言されているが、我が国の政治に干渉の意図がある外国政府の関与については、当然に妨げられてしかるべきである。慣習国際法においては内政不干渉原則があり、これをサイバー空間に適用したタリン・マニュアル2.0を参照すると、規則66は「国家は、他国の国内又は対外事項にサイバー手段による場合を含め、干渉してはならない」[67]と記述されている。こうした慣習国際法の解釈を根拠とし、公職選挙法第137条の４（外国政府が関与する者の選挙運動の禁止）を新設する（【参考】参照）ことで、外国政府による我が国の選挙への干渉を禁ずるべきである。外国人の選挙運動の制限については、選挙権は公職選挙法により「日本国民」の権利であると記載されている（第９条、第10条）ことに加え、外国人の政治運動と表現の自由に係る判例では、それらの自由は「権利の性質上日本国民のみをその対象としていると解されるもの」かつ「わが国の政治的意思決定又はその実施に影響を及ぼす活動等」を除いて許されると判示[68]されていることから、選挙期間中に限り外国人の活動を制限することは受忍限度を超えるものではないと考えられ、より実効性のある法整備として将来的な選択肢となろう。

②日本国憲法の改正手続に関する法律の改正

いわゆる国民投票に際して、外国からのディスインフォメーションによる干渉に対応するため、日本国憲法の改正手続きに関する法律に、公職選挙法と同様のネットの適正利用に関する条文を追加する（【参考】参照）。

③ プロバイダ責任制限法の改正

改正のポイント

・ディスインフォメーションに関する効果的なモニタリングを行うため、また、選挙期間におけるディスインフォメーションに関する発信者情報の開示の特例を整備するためプロバイダ責任制限法の改正を行う。あわせて、侵害情報の送信防止措置に対する対応の義務付けも検討する。

プロバイダ責任制限法においては、特定電気通信による情報の流通により他人の権利が侵害されたときに、プロバイダの賠償責任を制限することで、当該情報の送信を防止することや発信者の開示請求に応じることを可能にしている。同法では、第３条の２において、公職の候補者等に係る特例を定め、選挙期間中の名誉侵害等に対する措置における賠償責任の制限も別途設けているが、これらはあくまでも賠償責任の制限にすぎず、こうした措置を義務付けるものではないことに注意が必要である。虚偽情報の削除義務等を定めたドイツのSNS法等と比べると、効力は弱いといえる。

また、公職の候補者等の特例として、候補者等から名誉侵害の申し出を受けた場合の措置対象への同意照会に係る回答期間を「２日」とし（プロバイダ責任制限法第３条の２第１号）、電子メールアドレス等が正しく表示されていない文書図画について、候補者等からの申し出を受けて同意照会なしに削除した場合のプロバイダ等の損害賠償責任の免責規定（同条第３号）があるが、これらもあくまでも免責規定であり義務として課されているものではない。

ついては、権利侵害の申し出に対して、一定期間内の調査対応と、送信防止措置、削除、またはそれらが妥当でない場合の回答等、いずれかの対応を義務付けることとする。加えて、申し出については、現行の公職の候補者等だけでなく、ディスインフォメーションのモニタリング機関や所定のファクトチェック団体等、一定の基準を備えた第三者の通報も可能とする。

さらに、発信者情報等の開示請求については、個人の権利侵害のみならず、「我が国の選挙に対する外国からの干渉行為が発生し、これにより我が国の正当な選挙が脅かされ、国民の参政権が侵されるおそれがある場合」を特例として追記する（【参考】参照）。

憲法は、前文および第１条において、主権が国民に存することを宣言しており、国民は正当に選挙された国会における代表者を通じて行動すると定めていること、そして、第43条１項において、国会の両議院は全国民を代表する選挙された議員でこれを組織すると定め、国民主権・議会制民主主義を採用することを明らかにしていることから、第15条２項において、国民に対しその固有の権利として、両議院の議員の選挙において投票をすることによって国の政治に参加することができる権利を保障していると解される。よって、国は国民の参政権の保障のため、外国からの干渉を受けない「正当な選挙」を実施する義務があると考えることができ、それにもとづいて本件開示請求の特例を制定するものである。

２．選挙インフラの重要インフラ指定

（１）重要インフラへの指定に伴い、深刻度評価による対応を行う。

（２）選挙管理セキュリティ情報共有組織（Information Sharing and Analysis Center: ISAC）の創設、インシデント報告を義務化し共有を行う。

（3）選挙時に、政府は政党や選挙管理委員会に対してサイバーセキュリティ支援を実施する。
（4）選挙結果に影響を及ぼす世論調査システムに対しても適切なサイバーセキュリティ支援を実施する。

選挙インフラを重要インフラに指定し、サイバーセキュリティの重点防護対象とする。地方自治体の選挙管理委員会を構成要員とする選挙管理ISACを創設し、サイバー脅威情報の共有と連携、効果的なセキュリティポリシー（指針）の実践を行う。

具体的には、現在「重要インフラ分野」として特定されている14分野、すなわち「情報通信」、「金融」、「航空」、「空港」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む）」、「医療」、「水道」、「物流」、「化学」、「クレジット」および「石油」のうち、「政府・行政サービス（地方公共団体を含む）」分野の下に「選挙制度」を設定する。その防護対象として、「投開票システム」、「電子投票システム」、「集計システム」、「各選管の情報発信媒体」を定める。

3. 積極的サイバー防御（Active Cyber Defense: ACD）実施体制の整備

（1）ディスインフォメーション実施主体についてアトリビューションを実施する。
（2）平時においても国の正当業務行為としてACDを行うための法整備を行う。
（3）官民が連携して効果的なアトリビューションを実施するため、適切な予算措置を講ずる。

外国からのディスインフォメーションに対抗するため、司法的な事後制裁や取り締まりとは別に、攻撃主体についてアトリビューションの実施を含むACDを行う。また、ACDを国の正当業務行為として行えるよう、法整備を行う。これらの取り組みにあたり、我が国は同盟国と共に、ディスインフォメーションへの対抗措置として、戦略的コミュニケーションをはじめとしたあらゆる手段をとることを明言する。

なお、ACDはサイバー安全保障において広汎な論点を有する大きな課題であることが研究会の議論の中で明らかになった。ACDの実施主体のあり方や実施内容については、今後の笹川平和財団の事業において引き続き調査・研究、議論を深め、適宜発信していく考えである。

4. 政府とプラットフォーマーによる協同規制の取り組みと行動規範の策定

（1）EUや英国の前例を参考に、日本における表現の自由や通信の秘密に係る制約を考慮しつつ、また、プラットフォーマーによる自主的な取り組みを尊重しつつ、政府とプラットフォーマーによるディスインフォメーションの協同規制[69]の体制を検討する。
（2）協同規制の取り組みの方向性を示した、日本におけるプラットフォーマーの行動規範を策定する。この行動規範には、次の項目を盛り込む。①虚偽情報の通報、削除体制の整備、②ボットアカウントの通報、削除体制の整備、③拡散アルゴリズムに関する透明性確保、④政治広告の透明性確保、⑤プラットフォームで既存の報道機関のニュースを転載する際には元記事へのリンクを貼ることを義務付けること。
（3）特定デジタルプラットフォームの透明性及び公正性の向上に関する法律（デジタルプラットフォーム取引透明化法）における「特定デジタルプラットフォーム提供者」として、

SNS事業者を規制対象の事業者として指定し、第５条「特定デジタルプラットフォームの提供条件等の開示」に従い、当該デジタルプラットフォームに係る政治広告等の配信利用について提供条件等の開示が行えるように整備し、政治広告配信の透明化を進める。

５．メディアリテラシー教育環境の拡充

（１）ディスインフォメーションを念頭に、メディアリテラシーを高めるプログラムを、学習指導要領に明記する形で初等・中等教育に導入する。クリティカルシンキング（批判的思考）の涵養、RAVENメソッド（情報真偽分別法）、論理的誤謬の学習、認知領域への攻撃手法に関する知識の普及に取り組む。

（２）選挙時のメディアリテラシーに関するリーフレットを選挙広報とともに作成、配布する。

（３）政府によるファクトチェックのポータルサイトを設置する。政府は内容に関する発信はせずに、あくまでもポータル運営にとどめ、今、どのようなディスインフォメーションが話題になり流布されているのかが、国民にわかる仕組みを創設する。ファクトチェックは民間団体へ委託し、主要メディア・大学・シンクタンクも参加するファクトチェック・プラットフォームを設置する。ポータルサイトは団体を登録する仕組みを備え、さまざまな団体のファクトチェックを比較閲覧できるようにする。また、政府による「ディスインフォメーション白書」を発刊する。

（４）ファクトチェックに必要な費用をまかなうため、ユニバーサルサービス料を用いるなど適切な予算措置を講ずる。

（５）選挙期間中のファクトチェック体制を整備する。米国では、情報機関に国政選挙後45日以内に外国からの選挙干渉の有無について調査を命ずる大統領令が2018年に出されている。米国と同様に、政府が主体となり、選挙期間中に公職選挙法に抵触する虚偽事項の流布が行われていないかチェックを行う。そのために、選挙時にファクトチェック団体の認定を行う。（前掲１（２）①および【参考】の公職選挙法改正案第百四十二条の八（新設）を参照）

【参考】法律改正案

改正提案箇所を下線で示す。

■公職選挙法（提言１（２）参照）

（外国政府が関与する者の選挙運動の禁止）

第百三十七条の四（新設）　何人も、我が国の選挙の公正を害する目的を以て外国政府と通謀する者は、選挙運動をすることができない。

（選挙に関するインターネット等の適正な利用）

第百四十二条の七　選挙に関しインターネット等を利用する者は、公職の候補者に対して悪質な誹謗中傷をする等表現の自由を濫用し、また虚偽事項を公にして選挙の公正を害することがないよう、インターネット等の適正な利用に努めなければならない。」

第百四十二条の八（新設）　前項の目的を達成するため、中央選挙管理会若しくは都道府県の選挙管理委員会若しくは参議院合同選挙区選挙管理委員会若しくは市区町村の選挙管理委員会は、虚偽事項または公職の候補者等（公職の候補者又は候補者届出政党（公職選挙法（昭和二十五年法律第百号）第八十六条第一項又は第八項の規定による届出をした政党その他の政治団体をいう。）若しくは衆議院名簿届出政党等（同法第八十六条の二第一項の規定による届出をした政党その他の政治団体をいう。）若しくは参議院名簿届出政党等（同法第八十六条の三第一項の規定による届出をした政党その他の政治団体をいう。）をいう。）への名誉侵害情報によって選挙の公正を害するインターネット等の利用について、調査を行う団体を認定する。

（虚偽事項の公表罪）

第二百三十五条　何人も、当選を得又は得させる目的をもつて公職の候補者若しくは公職の候補者となろうとする者の身分、職業若しくは経歴、その者の政党その他の団体への所属、その者に係る候補者届出政党の候補者の届出、その者に係る参議院名簿届出政党等の届出又はその者に対する人若しくは政党その他の団体の推薦若しくは支持に関し虚偽の事項を公にし、また公職の候補者もしくは公職の候補者となろうとする者に関して文字・音声・映像等による虚偽の事項を公にした者は、二年以下の禁錮又は三十万円以下の罰金に処する。

２　何人も、当選を得させない目的をもつて公職の候補者又は公職の候補者となろうとする者に関し文字・音声・映像等による虚偽の事項を公にし、又は事実をゆがめて公にした者は、四年以下の懲役若しくは禁錮又は百万円以下の罰金に処する。

３　何人も、選挙および選挙制度の信頼性を失墜させる目的をもつて選挙並びに選挙制度に関し文字・音声・映像等による虚偽の事項を公にし、又は事実をゆがめて公にした者は、四年以下の懲役若しくは禁錮又は百万円以下の罰金に処する。

■日本国憲法の改正手続に関する法律（提言１（２）参照）

第百条の三（新設）

国民投票運動に関しインターネット等を利用する者は、悪質な誹謗中傷をする等表現の自由を濫用し、また虚偽事項を公にして国民投票の公正を害することがないよう、インターネット等の適正な利用に努めなければならない。

第百二十二条の二（新設）

（国民投票運動における虚偽事項の公表）

何人も、多数の投票人に対し、憲法改正案に対する賛成又は反対の投票をし又はしないようにさせる目的で、憲法改正案について文字・音声・映像等による虚偽の事項を公にし、又は事実をゆがめて公にした者は、四年以下の懲役若しくは禁錮又は百万円以下の罰金に処する。

■特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律（提言４（３）参照）

（損害賠償責任の制限）

第三条　特定電気通信による情報の流通により他人の権利が侵害されたときは、当該特定電気通信の用に供される特定電気通信設備を用いる特定電気通信役務提供者（以下この項において「関係役務提供者」という。）は、権利を侵害した情報の不特定の者に対する送信を防止する措置を講ずる義務を負う。ただし、これによって生じた損害については、権利を侵害した情報の不特定の者に対する送信を防止する措置を講ずることが技術的に可能な場合であって、次の各号のいずれかに該当するときでなければ、賠償の責めに任じない。ただし、当該関係役務提供者が当該権利を侵害した情報の発信者である場合は、この限りでない。

一　当該関係役務提供者が当該特定電気通信による情報の流通によって他人の権利が侵害されていることを知っていたとき。

二　当該関係役務提供者が、当該特定電気通信による情報の流通を知っていた場合であって、当該特定電気通信による情報の流通によって他人の権利が侵害されていることを知ることができたと認めるに足りる相当の理由があるとき。

（公職の候補者等に係る特例）

第三条の二　前条第二項の場合のほか、特定電気通信役務提供者は、特定電気通信による情報（選挙運動の期間中に頒布された文書図画に係る情報に限る。以下この条において同じ。）の送信を防止する措置を講じた場合において、当該措置により送信を防止された情報の発信者に生じた損害については、当該措置が当該情報の不特定の者に対する送信を防止するために必要な限度において行われたものである場合であって、次の各号のいずれかに該当するときは、賠償の責めに任じない。

一　特定電気通信による情報であって、選挙運動のために使用し、又は当選を得させないための活動に使用する文書図画（以下「特定文書図画」という。）に係るものの流通によって自己の名誉を侵害されたとする公職の候補者等（公職の候補者又は候補者届出政党（公職選挙法（昭和二十五年法律第百号）第八十六条第一項又は第八項の規定による届出をした政党その他の政治団体をいう。）若しくは衆議院名簿届出政党等（同法第八十六条の二第一項の規定による届出をした政党その他の政治団体をいう。）若しくは参議院名簿届出政党等（同法第八十六条の三第一項の規定による届出をした政党その他の政治団体をいう。）又は選挙の公正を害するインターネット等の利用についての調査団体（同法第百四十二条の八の規定による団体をいう。）をいう。以下同じ。）から、当該名誉を侵害したとする情報（以下「名誉侵害情報」という。）、名誉が侵害された旨、名誉が侵害されたとする理由及び当該名誉侵害情報が特定文書図画に係るものである旨（以下「名誉侵害情報等」という。）を示して当該特定電気通信役務提供者に対し名誉侵害情報の送信を防止する措置（以下「名誉侵害情報送信防止措置」という。）を講ずるよう申し出があった場合に、当該特定電気通信役務提供者が、当該名誉侵害情報の発信者に対し当該名誉侵害情報等を示して当該名誉侵害情報送信防止措置を講ずることに同意するかどうかを照会した場合において、当該発信者が当該照会を受けた日から二日を経過しても当該発信者から当該名誉侵害情報送信防止措置を講ずることに同意しない旨の申し出がなかったとき。

（発信者情報の開示請求等）

第四条の二（新設）　特定電気通信による情報（選挙運動の期間中に頒布された文書図画に係る情報に限る。以下この条において同じ。）であって、選挙運動のために使用し、又は当選を得させないための活動に使用する文書図画（以下「特定文書図画」という。）に係るものの流通によって、我が国の選挙に対する外国からの干渉行為が発生し、これにより我が国の選挙の公正が脅かされ、公務員を選定し、及びこれを罷免する国民の権利が侵されるおそれがある場合、中央選挙管理会若しくは都道府県の選挙管理委員会若しくは参議院合同選挙区選挙管理委員会若しくは市区町村の選挙管理委員会若しくは選挙の公正を害するインターネット等の利用についての調査団体（同法第百四十二条の八の規定による団体をいう。）は、公正な選挙の実施のため必要な調査をするときに限り、当該特定電気通信の用に供される特定電気通信設備を用いる特定電気通信役務提供者（以下「開示関係役務提供者」という。）に対し、当該開示関係役務提供者が保有する当該権利の侵害に係る発信者情報（氏名、住所その他の侵害情報の発信者の特定に資する情報であって総務省令で定めるものをいう。以下同じ。）の開示を請求することができる。

おわりに

サイバー空間では、国家が関与するサイバー攻撃が激しさを増しつつあり、我が国のサイバー防衛に関する体制・組織の整備は焦眉の急となっています。サイバー空間は、通常の安全保障と異なり、平時における空間の状況把握・分析・判断・対処が重要であることから、各国では軍や情報機関と密接に連動する形で、国を挙げたサイバーセキュリティ体制が構築されています。

笹川平和財団では、2019年度から我が国のサイバーセキュリティにおけるディスインフォメーションへの対応に関する課題をテーマに、国内の有識者の方々に参集いただき、「サイバーフェイクニュース研究会」を開催してきました。その研究成果の一端は、すでにサイバーセキュリティセミナーの形で、一般に公開しています。

今般、笹川平和財団安全保障研究グループは「サイバーフェイクニュース研究会」における議論を踏まえ、我が国のサイバー防衛のうち、ディスインフォメーションに関する体制・組織の整備のあり方について、「外国からのディスインフォメーションに備えを！～サイバー空間の情報操作の脅威～」と題して提言を取りまとめました。

本提言の策定にあたり有益なコメントを頂戴したみなさま方に感謝申し上げます。特に、研究会委員として参画いただいた、西川徹矢先生、東秀敏先生、川口貴久先生、高野聖玄先生、土屋大洋先生、中谷昇先生、山本一郎先生、湯淺墾道先生、オブザーバーとして参画いただいた、飯塚恵子様、小川聡様、北本一郎様、斉藤直哉様、津屋尚様、藤田直央様、古田大輔様、また、お名前をあげることは控えますが、ご指導賜りました方々に深謝申し上げます。

研究会の議論の中で、我が国のサイバー安全保障を確実に担保するためには、ACD等、より積極的なサイバー防衛策を検討する必要があることが明らかになりました。本提言で発出した5項目を超えて、将来的には、より前進したサイバー安全保障の法整備を進めるとともに、ディスインフォメーションの検知、情報収集機関にとどまらず、ACDを可能とし、サイバー安全保障を一元的に担う独立した行政庁「サイバーセキュリティ庁」に発展させていくことが、残された課題であると認識しています。なお、本提言の文責は執筆した笹川平和財団安全保障研究グループが負うものであることは、言うまでもありません。

本提言が、我が国のサイバー空間の安全構築の一助となれば幸いです。

2022年2月
笹川平和財団安全保障研究グループ

脚　注

1 Zhanna Malekos Smith, Eugenia Lostri, “The Hideen Costs of Cybercrime,” McAfee and CSIS, Dec 7, 2020（https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf）

2 FireEye「APT攻撃グループ 主要なサイバー攻撃者の素性を解説関与が疑われる国家/組織：中国」（https://www.fireeye.jp/current-threats/apt-groups.html#china）

3 HPSCI Minority Staff, “HPSCI Minority Exhibits During Open Hearing,” 1 November 2017, p.2.（https://intelligence.house.gov/uploadedfiles/hpsci_minority_exhibits_memo_11.1.17.pdf）

4 CHRISTCHURCH CALL（https://www.christchurchcall.com/）

5 National Cybersecurity and Communications Integration Center（NCCIC）, “ GRIZZLY STEPPE - Russian Malicious Cyber Activity,” 29 December 2016（https://us-cert.cisa.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf）

6 U.S. Senate Select Committee on Intelligence, Hearing, 1 November 2017（https://www.intelligence.senate.gov/hearings/open-hearing-social-media-influence-2016-us-elections#）

7 Intelligence Community Assessment, “Assessing Russian Activities and Intentions in Recent US Elections,” Office of the Director of National Intelligence（ODNI）, 6 January 2017（https://www.dni.gov/files/documents/ICA_2017_01.pdf）

8 *Ibid.*, p.ii.

9 Alex Isenstadt, John Bresnahan, “Exclusive: Emails of top NRCC officials stolen in major 2018 hack,” *POLITICO*, 4 December 2018（https://www.politico.com/story/2018/12/04/exclusive-emails-of-top-nrcc-officials-stolen-in-major-2018-hack-1043309）

10 ODNI, “DNI Coats Statement on the Intelligence Community's Response to Executive Order 13848 on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election,” 21 December 2018（https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2018/item/1933-dni-coats-statement-on-the-intelligence-community-s-response-to-executive-order-13848-on-imposing-certain-sanctions-in-the-event-of-foreign-interference-in-a-united-states-election）

11 Ellen Nakashima, “U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms,” *The Washington Post*, 27 February 2019（https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc 9 e-36d 6 -11e 9 -af 5 b-b51b 7 ff322e 9 _story.html?noredirect=on）

12 National Intelligence Council, “Foreign Threats to the 2020 US Federal Elections,” 10 March 2021（https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf）（https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf）

13 House of Commons Digital, Culture, Media and Sport Committee, “Disinformation and ‘fake news’ : Interim Report Fifth Report of Session 2017-19,” House of Commons, February 2019, p.43.ff.

14 https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/171103-Chair-to-Jack-Dorsey-Twitter.pdf

https://www.parliament.uk/globalassets/documents/commons-committees/culture-media-and-sport/171019-Chair-to-Mark-Zuckerberg-Facebook.pdf

15 Committee on Foreign Relations United States Senate, “Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security,” 10 January 2018, p. 129.

16 StopFake, “Fake: Merkel Takes Selfie with Belgian Suicide Bomber,” 27 March 2016（https://www.stopfake.org/en/fake-merkel-takes-selfie-with-belgian-suicide-bomber- 2 /）

17 Thomas Davidson and Julius Lagodny, “Germany's far-right party AfD won the Facebook battle. By a lot,” *The Washington Post*, 26 September 2017（https://www.washingtonpost.com/news/monkey-cage/wp/2017/09/26/germanys-far-right-party-afd-won-the-facebook-battle-by-a-lot/）

18 Mark Scott, “Russian ‘botnet’ promotes far-right messages in German election,” *Politico*, 24 September 2017（https://www.politico.eu/article/russian-botnet-promotes-far-right-messages-in-german-election/）

19 Lars Petersen, “Hacker attack on the Federal Election Commissioner’ s server, ” *Business Insider*, 15 Sep 2021（https://www.businessinsider.de/politik/deutschland/hackerangriff-auf-server-des-bundeswahlleiters/）

20 Tagesschau, “Bundesregierung kritisiert Russland scharf,” 6 September 2021（https://www.tagesschau.de/ausland/cyberangriffe-russland-gru-ghostwriter-101.html）

21 DW, “Federal government urges Russia to end cyberattacks,” 6 September 2021（https://www.dw.com/de/bundesregierung-fordert-von-russland-ende-der-cyberattacken/a-59100108）

22 Der Bundeswahlleiter, “Erkennen und Bekämpfen von Desinformation”（https://www.bundeswahlleiter.de/bundestagswahlen/2021/fakten-fakenews.html）

23 Volker Witting, Ian Bateson, “German election: The postal vote and fraud claims,” DW, 25 September 2021（https://www.dw.com/en/german-election-the-postal-vote-and-fraud-claims/a-58844693）

24 Committee on Foreign Relations United States Senate, “Putin’ s Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security,” 10 January 2018, p.123.

25 Committee on Foreign Relations United States Senate, “Putin’ s Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security,” 10 January 2018, p.122.

26 https://www.pofmaoffice.gov.sg/

27 Hariz Baharudin, “Singapore GE2020: Hackers pretend to be political parties in run-up to elections,” The Straits Times, 28 June 2020

（https://www.straitstimes.com/politics/ge2020-hackers-pretend-to-be-political-parties-in-run-up-to-elections ）

28 European Comission, “A Europe that protects: EU reports on progress in fighting disinformation ahead of European Council,” 14 June 2019（https://ec.europa.eu/commission/presscorner/detail/en/ip_19_2914）

29 Michael Yip, “Taiwan Presidential Election: A Case Study on Thematic Targeting,” *PwC*, 17 March 2016

（https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2016/2016.03.17.Taiwan-election-targetting/taiwant-election-targetting.html.pdf）

30 Nicholas J. Monaco, Google Jigsaw, “Computational Propaganda in Taiwan- Where Digital Democracy Meets Automated Autocracy,” February 2017, p.22.

31 福島香織「中国は台湾を内部崩壊させるのか」『日経ビジネス』2018年11月28日（https://business.nikkei.com/atcl/opinion/15/218009/112700187/）

32 同上

33『日本経済新聞』「台湾総統選『中国選挙介入』巡り論戦　テレビ討論会」2019年12月29日（https://www.nikkei.com/article/DGXMZO53986070Z21C19A 2 FF8000/）

34 インド太平洋防衛フォーラム「2020年の台湾選挙への介入を目的として、政治的影響力という多くの武器を駆使する中国共産党」2019年12月 4 日（https://ipdefenseforum.com/ja/2019/12/2020%E 5 %B 9 %B 4 %E 3 %81%AE%E 5 % 8 F%B 0 %E 6 %B 9 %BE%E 9 %81%B 8 %E 6 % 8 C%99%E 3 %81%B 8 %E 3 %81%AE%E 4 %BB% 8 B%E 5 %85%A 5 %E 3 %82%92%E 7 % 9 B%AE%E 7 % 9 A%84%E 3 %81%A 8 %E 3 %81%97%E 3 %81%A 6 %E 3 %80%81%E 6 %94%BF%E 6 %B 2 %BB%E 7 % 9 A%84%E 5 %BD%B 1 /）

35 United States-China Economic and Security Review Commission, “U.S.-CHINA Relations in 2019: A Year in Review,” Hearing, 4 September 2019（https://www.uscc.gov/sites/default/files/2019-10/September%204,%202019%20Hearing%20Transcript.pdf）

36 Meta, “Removing Coordinated Inauthentic Behavior From China,” 19 August 2019（https://about.fb.com/news/2019/08/removing-cib-china/）

37 Twitter, “Information operations directed at Hong Kong,” 19 August 2019（https://blog.twitter.com/en_us/topics/company/2019/information_operations_directed_at_Hong_Kong）; Nathaniel Gleicher, “Removing Coordinated Inauthentic Behavior From China, ” *Meta*, 19 August 2019

38「米、沖縄に新型中距離弾道ミサイル配備計画　ロシア側に伝達、 2 年以内にも　基地負担大幅増幅恐れ」琉球新報、2019年10月 3 日。https://ryukyushimpo.jp/news/entry-1000469.html

39 藤代裕之「フェイクニュース検証記事の制作過程～2018年沖縄県知事選挙における沖縄タイムスを事例として～」『社会情報学』第 8 巻 2 号、社会情報学会、2019年、143-157頁（http://www.ssi.or.jp/journal/pdf/Vol 8 No 2 _10.pdf）。同稿の主題は沖縄タイムスの事例だが、琉球新報のファクトチェック動向についても触れられている。

40『琉球新報』「知事選に偽情報、誰が？　2サイトに同一人物の名前　正体を追うと…＜沖縄フェイクを追う＞①」2019年1月1日（https://ryukyushimpo.jp/news/entry-856174.html）

41 公安調査庁「『琉球帰属未定論』を提起し，沖縄での世論形成を図る中国」『内外情勢の回顧と展望』2017年1月、23頁（http://www.moj.go.jp/content/001221029.pdf）。なお「琉球帰属未定論」とは、中国共産党の機関紙『人民日報』等で主張されている「米国は，琉球の施政権を日本に引き渡しただけで，琉球の帰属は未定である。我々（中国）は長期間，琉球を沖縄と呼んできたが，この呼称は，我々が琉球の主権が日本にあることを暗に認めているのに等しく，使用すべきでない」といった説である。

42 新垣毅「プーチン大統領側近に独占インタビュー　沖縄の基地は「日ロ関係に障害」 対米従属の弊害を指摘　セルゲイ・グラジエフ氏」『琉球新報』2019年10月7日（https://ryukyushimpo.jp/news/entry-1002716.html）

43 ロシア連邦極東連邦管区大統領全権代表公式ウェブサイトにおいて、ロシア連邦副首相兼極東連邦管区大統領全権代表のユーリ・トルトネフ氏が2018年10月に東京と沖縄を訪問して日本政府や経済界の代表者らと会談し、日本と極東地域の今後の協力について協議する旨が記載されている。“В рамках рабочей поездки Юрия Трутнева пройдет обсуждение сотрудничества России и Японии на Дальнем Востоке,” Официальный сайт полномочного представителя Президента Российской Федерации в Дальневосточном федеральном округе, 26 октября 2018.（http://dfo.gov.ru/trutnev/3157/）

44 Michael Conte, “US conducted more than two dozen cyber operations targeting foreign threats to the 2020 election,” *CNN*, 25 March 2021（https://edition.cnn.com/2021/03/25/politics/us-cyber-operations-election-threats/index.html）

45 このプロジェクトにおいては、各国のファクトチェックプロジェクトを、「すべての政党や立場の人の発言を検証しているか」、「個々の主張を検証し、結論を出しているか」、「情報源を明らかにし、その方法を説明しているか」、「資金や所属を公開しているか」、「ファクトチェックプロジェクトの主な使命がニュースや情報であるかどうか」、「プロジェクトが、プロのジャーナリストや報道機関によって運営されているかどうか」、「学術的なジャーナリズム教育プログラムと提携しているかどうか」といった多様な基準から活動実績を判断し、データベースに登録している。（Bill Adair, Mark Stencel, ” How We Identify Fact-Checkers, Duke Reporters' Lab, 22 June 2016”［https://reporterslab.org/how-we-identify-fact-checkers/］）

46 Rumor Control（https://www.cisa.gov/rumorcontrol）

47 The Digital, Culture, Media and Sport Committee, “Disinformation and ‘fake news’ : Interim Report,” 29 July 2018（https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36302.htm）

48 The Digital, Culture, Media and Sport Committee, Disinformation and ‘fake news’ : Final Report, The House of Commons, 14 February 2019（https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf）

49 Edward Malnic, ” Britain to carry out ‘offensive’ cyber attacks from new £5bn digital warfare centre,” *The Telegraph*, 2 October 2021（https://www.telegraph.co.uk/politics/2021/10/02/britain-capable-launching-offensive-cyber-attacks-against-russia/）

50 Full Fact awarded $500,000 to build automated factchecking tools（https://fullfact.org/blog/2017/jun/awarded-500000-omidyar-network-open-society-foundations-automated-factchecking/）

51 Anne Catherine-Stolz, “Germany: Facebook Found in Violation of ’ Anti-Fake News ‘ Law,” Library of Congress, 20 August 2019（https://www.loc.gov/item/global-legal-monitor/2019-08-20/germany-facebook-found-in-violation-of-anti-fake-news-law/）

52 GET YOUR FACTS STRAIGHT!（GETFACTS）（https://all-digital.org/projects/get-your-facts-straight/）

53 Raquel Miguel, “The battle against disinformation in the upcoming federal election in Germany: actors, initiatives and tools,” EU Disinfo Lab, 24 September 2021（https://www.disinfo.eu/publications/the-battle-against-disinformation-in-the-upcoming-federal-election-in-germany-actors-initiatives-and-tools/）

54 Der Bundeswahlleiter, “Erkennen und Bekämpfen von Desinformation -Desinformation in Social-Media-Kanälen”（https://www.bundeswahlleiter.de/bundestagswahlen/2021/fakten-fakenews.html#b 1 f77833-c 1 f 9 -4167- 9 e83-51019b667552）

55 Jean-Baptiste Jeangène Vilmer, Alexandre Escorcia, Marine Guillaume, and Janaina Herrera, *Iinformation Mnipulation: A Challenge for Our Democracies*, CAPS（Ministry for Europe and Foreign Affairs）and IRSEM（Ministry for the Armed Forces）, August 2018（https://www.diplomatie.gouv.fr/IMG/pdf/information_

manipulation_rvb_cle838736.pdf）

56 Factually（https://www.gov.sg/factually）

57 Venessa Lee, “ 2 initiatives launched to help fight fake news, terrorism,” *The Straits Times*, 13 January 2019（https://www.straitstimes.com/singapore/ 2 -initiatives-launched-to-help-fight-fake-news-terrorism）

58 Factually（https://www.gov.sg/factually）

59 Europian Commission, “European Democracy Action Plan”（https://ec.europa.eu/info/strategy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan_en）

60 European Union Agency for Cybersecurity, “ENISA makes recommendations on EU-wide election cybersecurity,” 28 February 2019（https://www.enisa.europa.eu/news/enisa-news/enisa-makes-recommendations-on-eu-wide-election-cybersecurity）

61 European Commission, “European Commission Guidance on Strengthening the Code of Practice on Disinformation,” Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM/2021/262 final, 26 May 2021（https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX% 3 A52021DC0262）

62 池雅蓉「市民と連携して偽情報と闘う　台湾のファクトチェックの多様な取組み」ファクトチェック・イニシアティブ、2019年10月16日（https://fij.info/archives/3242）

63 虚偽事項や悪意ある情報に関連した規制については、現行法では刑法第230条の名誉棄損、第231条の侮辱罪、第233条の信用棄損および偽計業務妨害による罰則があるが、刑法の属地主義（刑法第１条１項）から、これらはあくまでも日本国内において逮捕、検挙された場合であり、外国からのディスインフォメーションに対しては効力が薄いと考えられる。ただし、最高裁は、2014年に、インターネットを介したわいせつ電磁的記録配信に関する事件において，国外からの配信を国内犯として処罰できるとの判断を示している（最決2014年［平成26年］11月25日刑集68巻９号）。ただし、この判示では、国内犯の判断について「前記の事実関係の下では」と明示しており、無制限に拡大できるものではない。インターネット上の表現における名誉棄損等については、今後の法解釈や判例の蓄積が待たれる。選挙中の虚偽情報に関連する規制としては、公職選挙法において虚偽事項公表罪（公職選挙法第235条２項）、氏名等の虚偽表示罪（公職選挙法第235条の５）がある。

64 総務省「プラットフォームサービスに関する研究会　最終報告書」2020 年２月（https://www.soumu.go.jp/main_content/000668595.pdf）

65 インターネット選挙運動等に関する各党協議会「改正公職選挙法（インターネット選挙運動解禁）ガイドライン　第１版」総務省、2013年４月26日（https://www.soumu.go.jp/main_content/000222706.pdf）

66 代表的なものは以下。Soroush Vosoughi, Deb Roy and Sinan Aral, “The spread of true and false news online,” *Science*, Vol 359, Issue 6380, March 2018, pp. 1146-1151.（https://www.science.org/doi/full/10.1126/science.aap9559）

67 規則の訳文は以下より引用した。

中谷和弘、河野桂子、黒﨑将広著『サイバー攻撃の国際法―タリン・マニュアル2.0の解説』2018年、信山社。

68 最判1979年（昭和54年）10月４日民集第32巻７号1223頁。ただし、この判例自体は、「外国人に対する憲法の基本的人権の保障は、右のような外国人在留制度のわく内で与えられているにすぎないものと解するのが相当であつて、在留の許否を決する国の裁量を拘束するまでの保障、すなわち、在留期間中の憲法の基本的人権の保障を受ける行為を在留期間の更新の際に消極的な事情としてしんしやくされないことまでの保障が与えられているものと解することはできない。在留中の外国人の行為が合憲合法な場合でも、法務大臣がその行為 を当不当の面から日本国にとつて好ましいものとはいえないと評価し、また、右行為から将来当該外国人が日本国の利益を害する行為を行うおそれがある者であると 推認することは、右行為が上記のような意味において憲法の保障を受けるものであるからといつてなんら妨げられるものではない。」として、あくまでも法務大臣の裁量についての合憲性を判断したものであり、外国人の政治活動の合法性には言及していない点には注意が必要である。一方で、「外国人に対する憲法の基本的人権の保障は、右のような外国人在留制度のわく内で与えられているにすぎない」と判示されていることにも留意したい。

69 いわゆる共同規制は、自主規制の自主性・柔軟性を活かしつつその限界を政府が補完する政策手法である。法律で抽象的な規範・原則を定めつつ、その具体化に際しては自主的取組を尊重する仕組みなどがある。この概念は欧州由来の概念であり、生貝直人氏により『情報社会と共同規制―インターネット政策の国際比較制度研究』（2011年、勁草書房）等で紹介された。本研究会では、この共同規制の概念をベースにしつつも、プラットフォーマー規制については規範や原則が明確でないことから、行動規範等の策定段階から政府とプラットフォーマーが協同して取り組むことを重視し、本来的な共同規制よりもややゆるやかな規制態様とし

て、「協同規制」の概念を提唱する。

※上記脚注におけるURLについては、本提言執筆時点(2021年12月現在)に確認したものである。

「我が国のサイバー安全保障の確保」事業　事務局

大澤　　淳　　笹川平和財団安全保障研究グループ　特別研究員
長迫　　智子　笹川平和財団安全保障研究グループ　研究員
多賀井　順子　笹川平和財団安全保障研究グループ　アシスタント
渡部　　弥生　笹川平和財団安全保障研究グループ　アシスタント

政策提言　“外国からのディスインフォメーションに備えを！
　　～サイバー空間の情報操作の脅威～”

2022年 2 月発行
発行者　公益財団法人　笹川平和財団
　　〒105-8524　東京都港区虎ノ門 1 -15-16　笹川平和財団ビル
　　Tel. 03-5157-5430　URL https://www.spf.org/

笹川平和財団