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。

【提言のポイント】

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

民主主義の選挙プロセスや社会の安定性を毀損す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、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、対応を行う。あわせて、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。国民の知る権利に留意しつつ、ディスインフォメーションを用いた外国勢力の干渉を取り締まれるよう、公職選挙法や日本国憲法の改正手続に関する法律（国民投票法）、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 選挙インフラを重要インフラに指定

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セキュリティ情報共有組織（Information Sharing and Analysis Center: 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。

③ 情報操作型サイバー攻撃に対するACD実施体制の整備

外国からのディスインフォメーションを用いた攻撃に対抗するため、攻撃主体に対して、アトリビューションの実施を含むACDの実施体制を整備する。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。

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の推進

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[i]のあり方を検討する。我が国におけるプラットフォーマーの行動規範を策定し、虚偽情報の削除の義務化や政治広告の透明性確保を求めるとともに、プラットフォームが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。こうした取り組みによりファクト補完対策および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

ディスインフォメーションやマイクロターゲティング広告による影響工作は、国民一人ひとりの認知領域をターゲットにした攻撃でもある。そのため、個人がニュース等の情報に接した際に、情報のソースやバイアス等を確認するリテラシーの涵養が重要である。政策決定者などの政官財の要人に対しても、外国からのディスインフォメーションを想定した訓練の実施が望まれる。また同時に、広く流布してトレンドとなっている情報については、その正誤を確認できるファクトチェック体制を整備するなど、ファクトチェックを習慣化しやすい環境を整備する。選挙時においては政府が主体となり、公職選挙法に抵触する虚偽の流布が行われていないか、チェックを行う。

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。

i　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。