

社会動向レポート

国際比較を通じた日本人の偽・誤情報に対する意識と取り組むべき対策

—企業・組織や個人を狙う偽・誤情報への対策が急務—

デジタルコンサルティング部

上席主任コンサルタント 中 志津馬

上席主任コンサルタント 石岡 宏規

COVID-19等の社会的事案に関連して、オンライン上では偽・誤情報が広がっている。

欧米諸国と比べると日本は偽・誤情報の実態について情報が十分に蓄積されておらず、不明なことが多い状況にある。このような状況を受け、弊社は過去複数年にわたり、総務省から偽・誤情報の実態把握のための調査を受託し、大規模なアンケート調査を通じて、日本人の偽情報への接触状況について国際的な比較を行ってきた。さらに、令和3年度には総務省は弊社に発注した調査の一環として、我が国の偽・誤情報に関する第1線の専門家の協力の下、個人向けのメディアリテラシー向上のための教材を開発した。

本レポートは偽・誤情報の実態把握や対策で先行する諸外国の事例を紹介しつつ、弊社のこれまでの経験を踏まえ、今後、取り組むべき対策について考察を行ったものである。

構成は以下の通りである。

第1章では前提となる情報として、偽・誤情報の国際的な定義、さらに過去の調査結果から日本人の偽・誤情報に対する意識や行動特性について解説を行った。

第2章では、偽・誤情報が広がることで社会にどのような悪影響を及ぼす可能性があるのかについて、企業、個人それぞれについて、具体的事案とともに整理を行った。

第3章は、2章で示した偽・誤情報による悪影響を最小限に抑えるため企業・個人がそれぞれどのような取組を行うべきか、諸外国の先行事例も参考にしつつ有効な対策案について考察を行った。企業に関しては、先行する米国を参考に、組織内の情報セキュリティの取組との一体化について紹介した。個人については、第1線の専門家の協力により開発されたメディアリテラシー教材の紹介とその活用について紹介した。

1. 偽・誤情報とそれに対する日本人の意識や接触状況

(1)概要・定義

偽・誤情報に対する議論が先行する欧州では、偽・誤情報のことを「情報障害(Information Disorder)」と総称しており、そのうち、偽情報を

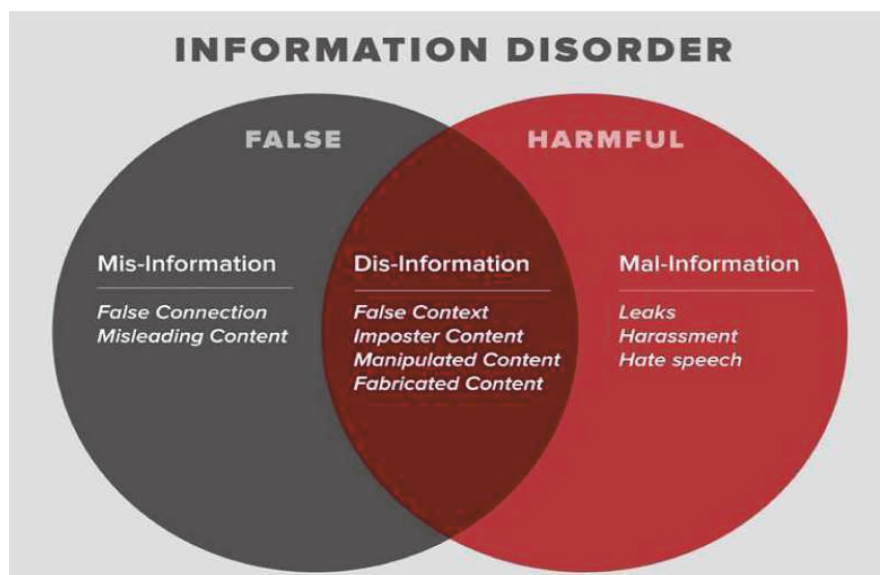
「Dis-information」、誤情報を「Mis-information」と称している。それぞれの具体的な定義は図表1のように定義されている。偽情報とは、第三者や社会に危害を加えることを意図して用いられる虚偽情報のことをいい、虚偽情報であるが危害を加える意思で作成されたものではないものは誤情報として区別される。さらに、事実

基づく情報であるが、危害を加えることを目的として用いられる場合は「悪意ある情報(Mal-information)」と整理されている。ただし、このように偽・誤情報は、定義としていくつかに分類されるものの、実際の偽・誤情報を分類するには、意図性があるものなのか、たんなる勘違いによるものなのかを判断する必要があり、専門家の間でも非常に難しいとされている。

なお、米国前大統領が使用したことで日本でも知られるようになった「Fake News（フェイクニュース）」という言葉は、その定義があいまいなこともあり、昨今の偽・誤情報の定義としては主流ではないのが実態である。また、偽・誤情報は、文字、音声、画像・動画等の様々な表現方法で伝達されている。

図表1 偽・誤情報等の定義

区分	内容
Dis-information (偽情報)	個人、社会集団、組織または国に危害を与えるため、虚偽、かつ故意に作成された情報。 例：虚偽の文脈、偽のコンテンツ、加工されたコンテンツ、操作されたコンテンツ等。
Mis-information (誤情報)	虚偽の情報ではあるが、危害を引き起こす意図で作成されたものでない情報。 例：文脈のミスリーディング等。
Mal-information (悪意ある情報)	事実に基づく情報であるが、個人、組織、または国に危害を加えるために使用される情報。 例：リーク(漏えい)、ハラスメント、ヘイトスピーチ



(資料) 欧州評議会「Information Disorder」(2017年9月27日)⁽¹⁾を元に、みずほリサーチ & テクノロジーが簡易翻訳

(2)日本人の偽・誤情報に対する意識や行動特性

弊社では、総務省の委託調査研究として、我が国の生活者の偽・誤情報への意識や接触状況を把握するためのアンケート調査を定点観測的に過去数回実施してきた。本節では、これら調査結果を踏まえた、日本人の偽・誤情報に対する意識や行動の特性について紹介する。

①偽・誤情報を拡散した経験がある人の特徴

ここでは、2020年2月に実施した「偽情報に関するアンケート調査」⁽²⁾の結果のうち、偽・誤情報を拡散した経験の有無等について紹介する。なお、調査実施当時は、偽・誤情報という言葉ではなく、両者をあわせた意味の言葉として「フェイクニュース」という用語を使用したものであることに留意されたい。

アンケート回答者に偽・誤情報の拡散経験を尋ねたところ、全体では「拡散したことはない」

との回答が約70%と最も高くなり、「拡散した経験がある」との回答は約15%であった。さらに、偽・誤情報の拡散手段を見ると、「家族や知人に直接会って話した、もしくはメッセージアプリやメール、電話で直接伝えた」(約5%)⁽³⁾、「Facebookのシェアや、Twitterのリツイートを行ったことがある」(約5%)が回答として挙げられている(図表2)⁽⁴⁾。直接会って口頭で伝えることや、電話を使用して伝える等、インターネット以外の手段によっても、偽・誤情報が拡散されていることが伺える。

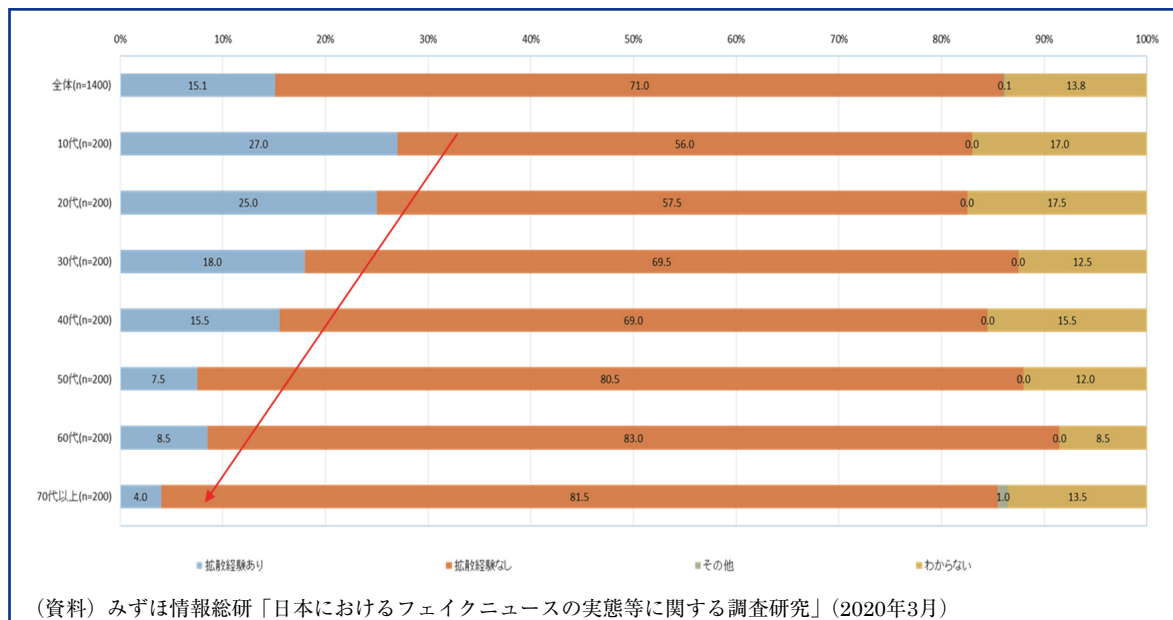
さらにこの調査では、「若い世代の人」、「フェイクニュースを見分ける自信のある人」、「身近な人との雑談に役立つかどうかで記事の見出しをクリックしている人」はそれ以外の人と比べて相対的に、フェイクニュースの拡散経験が多い傾向が見られた(図表3、図表4、図表5)。

図表2 フェイクニュースの拡散経験・拡散手段(複数回答)

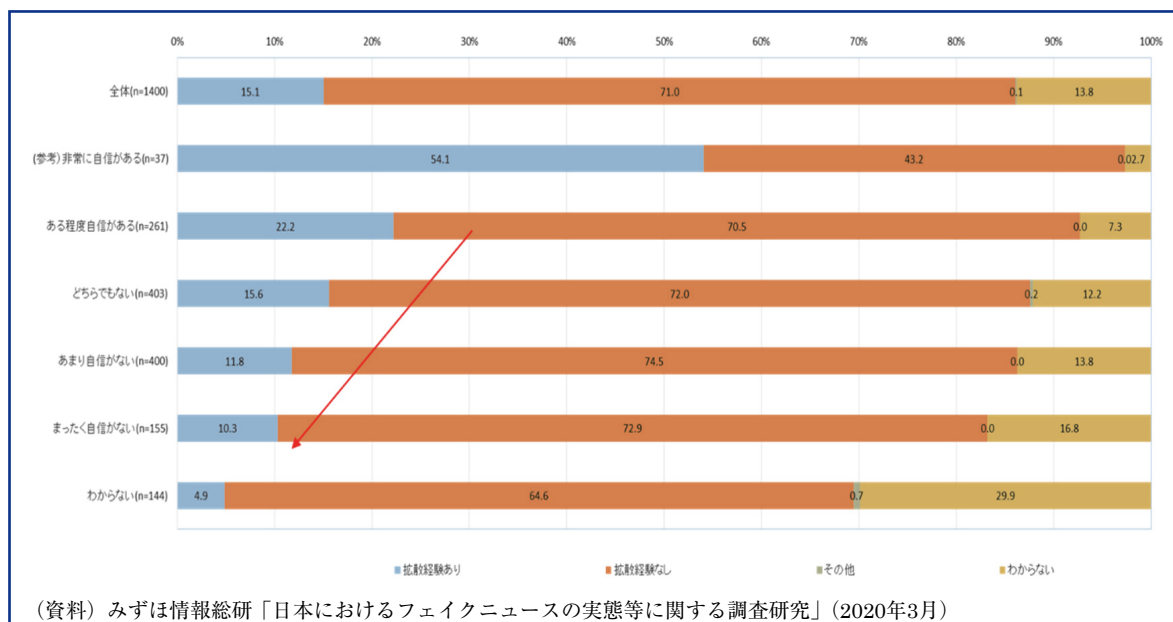
	(%)	Facebookのシェアや、リツイートを行ったことがある	ソーシャルネットワーキングサービス(SNS)上に投稿したことがある	ブログなど、ソーシャルネットワーキング上に投稿したことがある	メール、電話で直接伝えたことがある	インターネットでは拡散しなかったが、知人に直接会って話したことがある	拡散したことはない	その他	わからない	拡散した経験がある
全体	全体(n=1400)	5.9	3.8	3.4	5.4	5.9	71.0	0.1	13.8	15.1
年代	10代(n=200)	14.0	9.0	6.0	7.0	9.5	56.0	0.0	17.0	27.0
	20代(n=200)	9.0	5.5	6.5	9.5	8.0	57.5	0.0	17.5	25.0
	30代(n=200)	8.0	5.5	6.0	7.5	69.5	0.0	12.5	18.0	18.0
	40代(n=200)	5.0	3.5	2.5	6.0	65.0	0.0	15.5	15.5	15.5
	50代(n=200)	3.0	1.0	1.5	3.5	80.5	0.0	12.0	7.5	7.5
	60代(n=200)	1.0	2.0	1.5	4.0	83.0	0.0	8.5	8.5	8.5
	70代以上(n=200)	1.0	0.0	0.0	1.5	81.5	1.0	13.5	4.0	4.0

※拡散した経験がある：全体から、拡散したことはない、その他、わからないの回答を除いた値
 (資料) みずほ情報総研(現みずほリサーチ&テクノロジーズ)「日本におけるフェイクニュースの実態等に関する調査研究」(2020年3月)

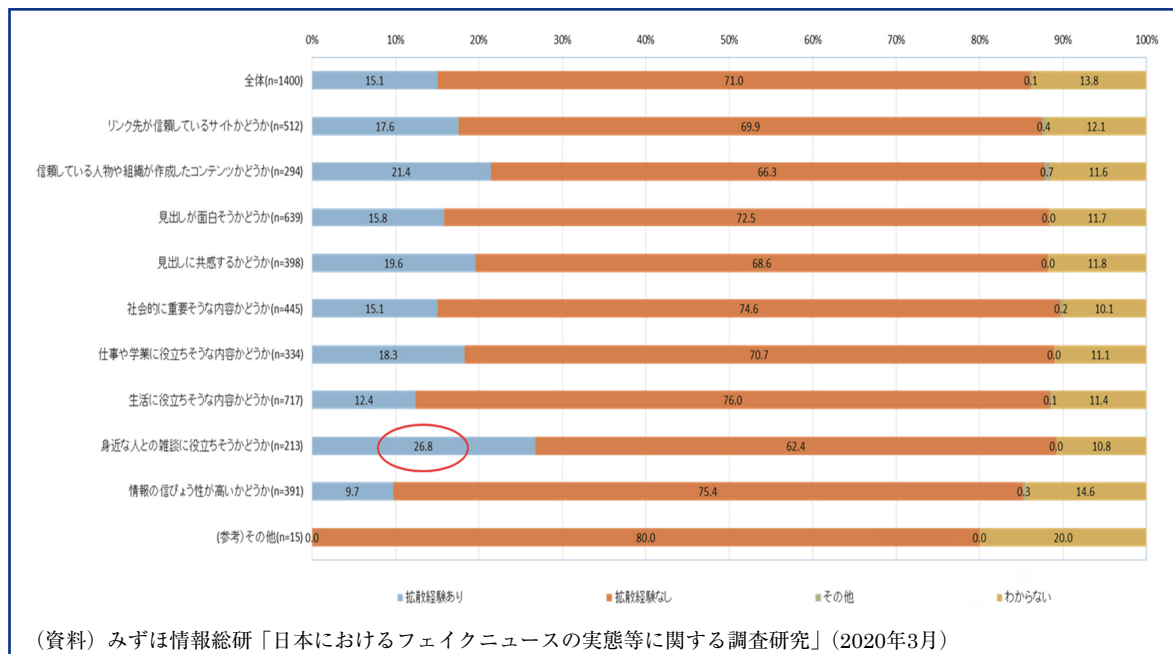
図表3 偽・誤情報を拡散した経験がある人の特徴(年代)



図表4 偽・誤情報を拡散した経験がある人の特徴(フェイクニュースを見分ける自信)



図表5 偽・誤情報を拡散した経験がある人の特徴(記事の見出しをクリックする基準)



② 国際比較による日本人の偽・誤情報に関する特徴

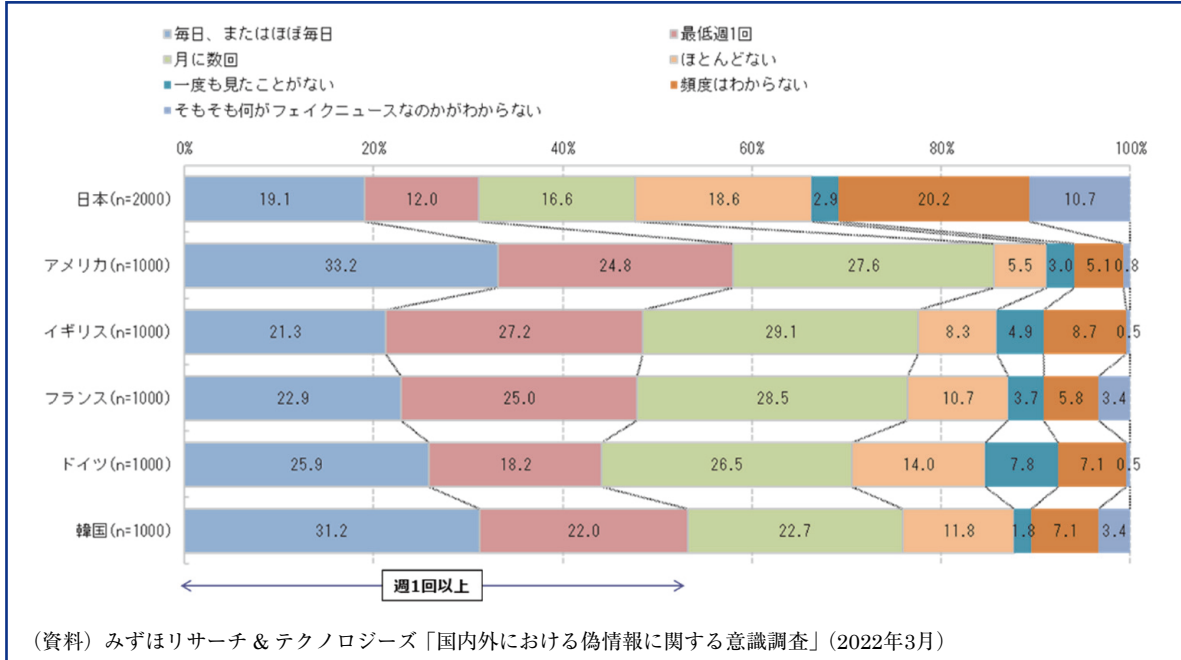
次に、2021年度に実施したアンケート調査結果を取り上げたい。これは、日本と諸外国における偽情報に関する実態把握を目的としたものであり、日本と5カ国の生活者を対象とした偽情報に関する意識調査である⁽⁵⁾。本節では、同調査のうち、偽情報を見かける頻度、真偽を見分ける自信、情報の真偽を確かめた経験についての国際比較結果を紹介する。

まず、SNSやブログなどインターネット上のメディアにおいて、どのくらいの頻度で偽・誤情報⁽⁶⁾を見かけているかを尋ねた結果は図表6のとおりである。「週1回以上」に着目すると、日本の回答割合は約30%台であり、その他の対象国(約40~50%台)と比べて低くなった。

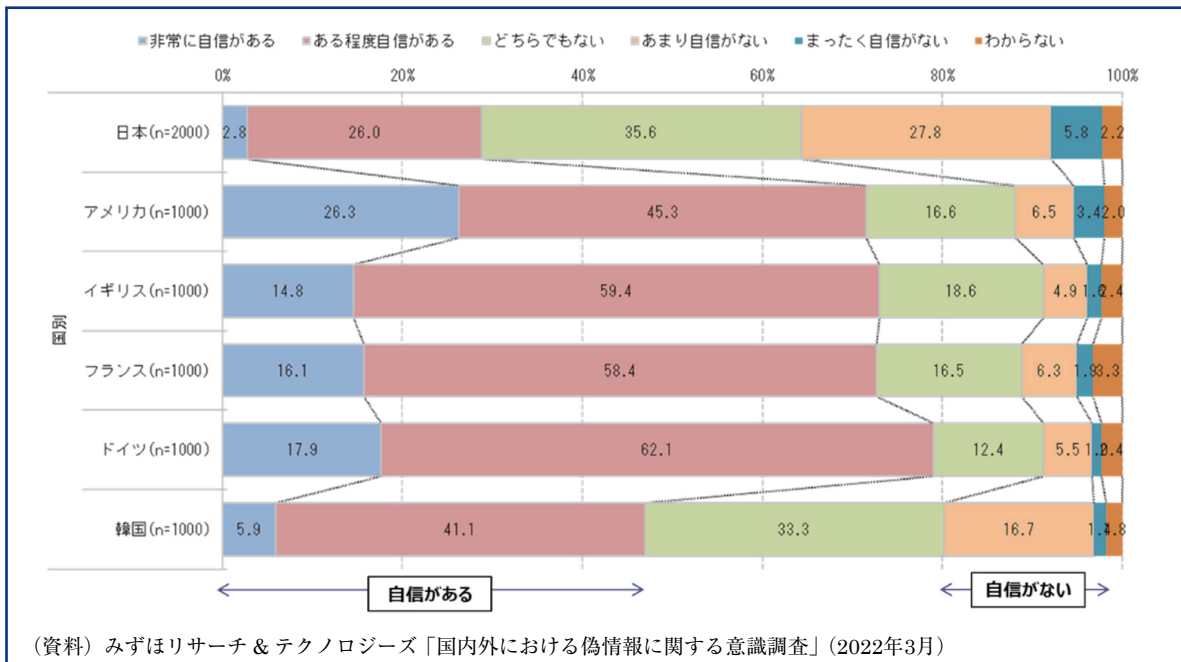
また、情報の真偽を見分ける自信を尋ねた(図表7)。ここでインターネットやメディアで流れる情報全般を対象に「(見分ける)自信がある」⁽⁷⁾と回答した結果に着目すると、諸外国の回答は約40~60%程度であるのに対して、日本は約30%未満となり、全対象国の中で回答割合は最も低くなった。

最後に、情報が怪しいと思った場合、情報の真偽を確かめた経験の有無について尋ねた(図表8)。情報の真偽を「調べる」との回答は、ドイツ、アメリカ、フランス、イギリスの欧米諸国は約40~50%台と高く、日本、韓国のアジア諸国では約30%台と低い。アジア諸国の回答者は欧米諸国と比べると、自らで情報の真偽を調べていないことが明らかとなった。

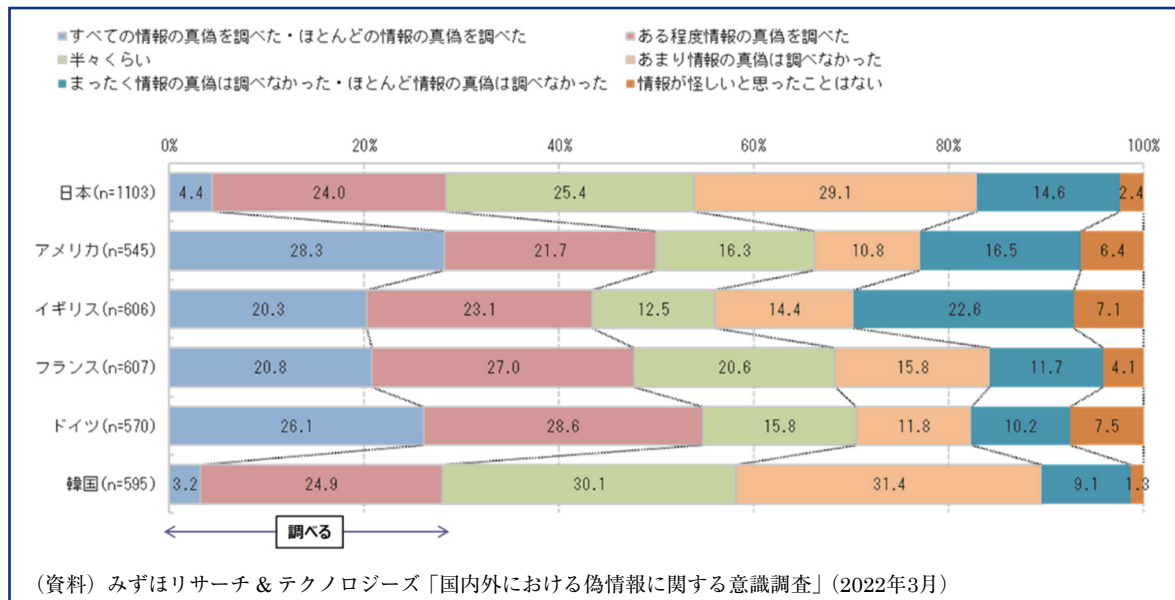
図表6 どのくらいの頻度で偽・誤情報を見かけているか



図表7 情報の真偽を見分ける自信



図表8 情報の真偽を確かめた経験の有無



③両調査から浮かび上がる日本人の偽・誤情報に対抗するための課題

ここまで紹介した2つの調査結果を通じて、日本人は比較的、偽・誤情報に対する接触機会は少ないこと、また拡散は行っていないこと、そして情報に対して慎重に接している様子が分かった。ただし一方では、怪しいと思った情報に対しての真偽を積極的に確認しようとしていないとも考えられ、いわば情報に対して受け身な状況ともいえる。そのため、もし仮に今後欧米並みに真偽が怪しい情報が身の回りで増加した場合の対処には課題が残るものと言えよう。

2. 偽・誤情報の与える社会的影響

「人は自らの見たいもの、信じたいものを信じる」という心理的特性を有しており、これは「確認バイアス(Confirmation bias)」と呼ばれる。インターネット上のSNS等のサービスは、利用者の興味・関心事を学習し、独自のアルゴリズムによって利用者にあった情報を提示している。この機能によって利用者は、インターネッ

ト上の膨大な情報の中から、自身が求める情報を得ることができる。

一方で、同じような情報が提供され続けることで、自身の関心分野の情報のみしか目にできない、まるで膜の中に包み込まれた状態となる「フィルターバブル(Filter Bubble)」や、SNS上で自身の意見を発信すると似た意見のみが戻ってくる「エコーチェンバー(Echo Chamber)」現象が生じる懸念がある。利用者は、同じ情報を繰り返し目にするによって、それがインターネット上の偽・誤情報であったとしても信じてしまう傾向があると言われている。

本章では偽・誤情報を信じてしまうことで、企業活動や国民生活に対してどのような影響が起りうるか、具体的な事例を示す(図表9)。

企業活動において、企業が偽・誤情報によって被害を受ける場合がある。例えば、①偽情報による攻撃を受けて企業価値が下落する、②偽情報発信サイトへの広告出稿により、偽情報を発信する活動に無意識な金銭的支援をしてしまい、そしてこれに伴い企業・ブランドイメージ

図表9 偽・誤情報による社会的影響の例

社会的影響		関連事案例
企業活動	①偽情報による攻撃を受け企業価値が下落する	・通信社のSNS アカウントが乗っ取られ、偽情報が配信された結果、平均株価が急落した
	②偽情報発信サイトへの広告出稿により、無意識な金銭的支援を行うことになり、企業・ブランドイメージが低下する	・ブランドセーフティ検出技術が十分に機能せず、偽情報を広めるサイト上に大手企業の広告が表示された
	③偽音声・動画による人やシステム等の誤認識を誘発する	・ディープフェイクで作成した偽音声を用いた振り込め詐欺。例えば、エネルギー企業のCEOに、親会社のCEOから電話があり、指定先への振込指示があったが、これはフェイク音声を用いた詐欺であった ・ディープフェイク動画として、口座開設等のオンライン認証が突破できる可能性があるとの論文が発表された
	④ディープフェイクで作成した人物を、自社社員や顧客と偽り、偽情報を発信	・テック企業のCEOが発言したことがない内容の動画が公表（実際は、芸術イベント向けの作品として制作された動画）された ・ディープフェイクで作成した架空の人物を、自社ウェブサイト上でサービス・製品を使用したお客様の声として掲載
国民生活	⑤偽情報による消費行動の影響操作を受ける	・商品が不足するという偽情報により、店頭でトイレトペーパーを求めて多くの人が集まった
	⑥動画の改変によって人物の印象が操作され、イメージダウンやプライバシー侵害された	・公務中の議員が、あたかも酔っ払っているように見える動画が公表された ・女優のディープフェイクポルノ動画が公表された
国民生活 / 企業活動	⑦AIの教師データに偽・誤情報が混入することで、性能低下・誤動作がおきる	・AIの画像判定用に使われるメジャーな学習用教師データ(AIデータセット)に「誤情報」が混入された ・AIが人間をゴリラと誤認識してタグ付けされた

※関連事案例には代表的な例を抽出した。なお、新型コロナワクチン、気候変動問題、ロシアのウクライナ侵攻等関連の内容は含まれていない。
(資料) 各種情報よりみずほリサーチ & テクノロジーズ作成

が低下する、③偽音声・動画による人やシステム等が誤認識を誘発する等が挙げられる。また、企業自体が偽・誤情報を用いて混乱を引き起す場合もある。例えば、④ディープフェイクで企業自体が作成した人物を自社社員や顧客と偽り、偽情報を発信してしまうこと等が該当する。

また、個人等の国民生活では、⑤偽情報による消費行動への影響操作を受けることや、⑥自身の動画が改変され人物の印象を操作され、イメージダウンやプライバシー侵害を受けること等が挙げられる。

さらに、我々の経済・社会において、AIが様々な場面で活用され始めているが、企業活動や国民生活に共通する影響としては、⑦AIが学習するための教師データに、偽情報が混入することで、AIの性能低下・誤動作が起こり得ること等が挙げられる。

これらのことが頻繁に起きるようになると、人々はインターネット等の情報空間やデジタル技術に対する信頼を無くしてしまい、社会全体にとって大きな損失につながる恐れがあると考えられる。

3. 対処方策

これまで述べたように、偽・誤情報は経済活動や社会に様々な影響を与える可能性がある。そこで本章では、組織・企業及び個人に向けて早急に着手することが望ましい偽・誤情報への対処方策について示す。

(1) 組織・企業のサイバーセキュリティの観点から

2022年2月、米国政府のセキュリティ対策の専門機関である CISA (The Cybersecurity and Infrastructure Security Agency: 米国国土安全

保障省サイバーセキュリティインフラセキュリティ庁)は、ソーシャルメディアやオンラインプラットフォームを介した情報操作によるリスクを軽減するために、重要インフラ事業者を含む組織が実行できる手順をまとめ、「Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure」として公表⁽⁸⁾した。本レポートでは、5つの実施事項として、①情報環境の評価、②脆弱性の特定、③コミュニケーションチャネルの強化、④積極的なコミュニケーションの実施及び、⑤インシデント対応計画の策定が示されている(図表10)。この中では、ソーシャルメディアとオンライ

図表10 CISA の情報操作に対するリスク軽減のためのレポートの概要

軽減手順	実施事項概要
①情報環境の評価	<ul style="list-style-type: none"> ・業界の偽・誤情報の前例の調査や、ステークホルダーや顧客とのコミュニケーションの状況把握を通じて、偽・誤情報への対応策を検討する。 ・問い合わせや検索の急増等、オンラインの活動の変化を監視する。 ※本実施事項は、オンラインのレピュテーション監視(オンラインで言われていることをキャッチアップ)を意図している。
②脆弱性の特定	<ul style="list-style-type: none"> ・偽・誤情報に悪用される可能性のある脆弱性を特定する。 ※偽・誤情報ナラティブの評価にあたっての基準が必要であるが、本レポートでは、自組織への偽・誤情報ナラティブによる悪影響に基づいたレベルが例示されている。
③コミュニケーションチャネルの強化	<ul style="list-style-type: none"> ・ステークホルダーを巻き込んだコミュニケーションチャネルの整備や、組織の Web サイトを整備し、情報の更新と透明性を高める。 ・自組織のソーシャルメディアアカウントの整備、アクセス権などのセキュリティを再確認する。 ※顧客やビジネスパートナーと定期的にコミュニケーションを取って信頼を築くことを意図している。
④積極的なコミュニケーションの実施	<ul style="list-style-type: none"> ・ステークホルダーやコミュニティとのコミュニケーション方法(ニュースレター、報告書、ブログ、イベント、ソーシャルメディア活動等)を見直し、メッセージの発信力を強化し、信頼されるネットワークを構築する。
⑤インシデント対応計画の策定	<ul style="list-style-type: none"> ・偽・誤情報のインシデント対応プロセスを整備する。 ・担当者を任命し、役割を割り当てる。 ・ソーシャルメディア企業、政府、法執行機関への報告手順について、スタッフを特定し、教育する。 ・複数の担当者が交代で監視する必要があるインシデントを特定し、情報共有と対応を明確にするための社内調整チャネルとプロセスを検討する。 ・情報操作とサイバー攻撃を組み合わせた活動に対する組織的な対策を促進するための組織内の調整が必要となる。

(資料) 「Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure」よりみずほリサーチ & テクノロジーズ作成

ンプラットフォームを活用した情報操作に関するリスクを認識し、その対処として、組織外のステークホルダー等を含むインシデント対応体制の整備と組織構成員への教育の重要性等に言及されている。

一方で、NIST (National Institute of Standards and Technology : 米国国立標準技術研究所) Cybersecurity Framework⁽⁹⁾等に見られるように、昨今のサイバーセキュリティ対策では、サイバー攻撃を完全に防止することは難しいとの前提のもと、その影響軽減と迅速な事業復旧を重視するレジリエンスの概念が重視されている。組織トップがサイバー攻撃を経営リスクの一部として認識し、自組織の構成員に加えてサプライチェーンを巻き込んだ関係者の能力向上とインシデント対応体制整備が重要とされている。

この様に見ると、偽・誤情報自体の発生を組織が制御することが難しいように、サイバー攻撃の発生自体を防止することは難しいこと、リスク評価、関係者への教育、インシデント対応体制の整備等の偽・誤情報とサイバー攻撃への対処には、多くの類似性を見出すことが出来る。サイバーセキュリティ対策と偽・誤情報対策を一体的に取り組むことが、レジリエンスの強化につながり、効果的な組織への悪影響の低減とパフォーマンスの向上をもたらすのではないだろうか。

(2)個人のリテラシー向上の観点から

当社は、2021年度に「国内外における偽・誤情報対策を中心としたメディア情報リテラシー向上施策の現状と課題等」の調査研究を総務省から受託⁽¹⁰⁾し、この中で、偽・誤情報に関する欧米各国の政策や、民間企業及び大学等による偽・誤情報への取組を整理した。各国の取組において確認できた共通点は、リテラシー向上の

ための教育訓練の重要性であった。例えば、EUが2020年に公表した「Digital Education Action Plan」では、優先事項の一つとして、学習者が情報に批判的にアプローチして、フィルタリングを行い、評価する能力を発達させることを挙げている。本計画では特に、「アルゴリズム」や「エコーチェンバー」等による影響を考慮して、EU市民がオンライン世界で適切な判断を行えるよう、批判的思考スキルを身に付けるための教育機会の重要性について言及している。

また、2022年2月のロシアによるウクライナへの軍事侵攻では、諸外国に対してプロパガンダ活動が行われ、偽情報が兵器化しているとの指摘がある。ターゲットとなったEU地域では、情報を受け取る市民のメディアリテラシー⁽¹¹⁾を向上させるための継続的取組の重要性が改めて認識されている。このような取組は、生活者である個人に限定されるものではなく、民間企業などの組織構成員にも同様に必要であると考えられる。偽・誤情報のリスクが高まり、組織構成員が業務遂行時に、疑わしいオンライン情報に接する機会が増えているが、3.(1)で述べた通り、情報操作を検出し、データ侵害や誤情報の拡散から自身と組織を守るために、予防措置として偽・誤情報の教育訓練が重要な役割を担うと言える。

先に紹介した総務省の調査研究では、偽情報の専門家を中心とした研究会(座長:国際大学グローバル・コミュニケーション・センター 山口真一 准教授)を開催し、教材を制作した(参考資料1、参考資料2)⁽¹²⁾。この偽・誤情報に関する普及啓発用教材「インターネットとの向き合い方～ニセ・誤情報に騙されないために～」は、無償で利用でき、各ページの内容をわかりやすく説明するための講師用の台本も付属している。また、受講者が学びたい部分を理解度に合わせて抜粋したり、加筆したりすることがで

きるよう、Microsoft PowerPoint の形式で提供する等、利用のしやすさを促す工夫を行った。本教材は、2022年6月に総務省のウェブサイトにおいて公表された⁽¹³⁾。

個人また組織は、個々人の意識啓発を継続し自覚を高めるためにも、こういった教材を有効に活用し、組織内のセキュリティ研修と一体で偽・誤情報の教育を進めることが望ましい。

(参考資料1) 研究会構成員

氏名	所属
上沼 紫野	虎ノ門南法律事務所 弁護士
小木曾 健	国際大学グローバル・コミュニケーション・センター 客員研究員
齋藤 長行	東京国際工科専門職大学工科学部 教授
坂本 旬	法政大学キャリアデザイン学部 教授
瀬尾 傑	スローニュース代表(スマートニュース メディア研究所 前所長)
安野 智子	中央大学文学部 教授
(座長) 山口 真一	国際大学グローバル・コミュニケーション・センター 准教授

(参考資料2) インターネットとの向き合い方～ニセ・誤情報に騙されないために～



(資料) 総務省ウェブサイト

注

- (1) 欧州評議会「Information Disorder」(2017年9月27日)
- (2) 過去1年間にインターネットの各種サービスを利用したことがある1,400名(日本の15~70代以上の男女)を対象としたウェブアンケート調査。みずほリサーチ&テクノロジーズ「日本におけるフェイクニュースの実態等に関する調査研究 ユーザのフェイクニュースに対する意識調査」(2020年3月)〈https://www.soumu.go.jp/main_content/000715293.pdf〉
- (3) 拡散経験がある／ないの回答を100%としたうちの割合となる。拡散経験ありのみの割合ではない点に留意いただきたい。
- (4) 当該質問は回答者の自己申告であることから、「拡散したことはない」と回答した者の中には、フェイクニュースかどうかは気がつかず拡散している場合も含まれる点に留意が必要。
- (5) 普段インターネットを1週間に1回以上かつ1日数分以上利用している人(15~60代以上の男女)を対象としたウェブアンケート調査(ただし、電子メールのみの利用者は調査対象外)。なお、回答者数は、国別に、日本：2,000名 アメリカ・イギリス・フランス・ドイツ・韓国：各1,000名。みずほリサーチ&テクノロジーズ「国内外における偽情報に関する意識調査」(2022年3月)〈https://www.soumu.go.jp/main_content/000820953.pdf〉
- (6) アンケートでは「虚偽又は誤解を招くと考えられる情報/ニュースをフェイクニュース」と補足説明し回答を促した。
- (7) アンケートの選択肢「非常に自信がある」と「ある程度自信がある」の回答を合わせたものを「自信がある」とする。
- (8) <https://www.cisa.gov/uscert/ncas/current-activity/2022/02/18/cisa-insights-foreign-influence-operations-targeting-critical>
- (9) <https://www.nist.gov/cyberframework>
- (10) 〈https://www.soumu.go.jp/menu_news/s-news/index.html〉
- (11) 偽情報の研究・監視機関である European Digital Media Observatory (EDMO)の「偽情報とウクライナ戦争に関するタスクフォース」が2022年6月29日に公表したレポート。本レポートでは、メディアリテラシーには、デジタル、クリティカル、ニュース・情報リテラシーなども含まれている。〈<https://edmo.eu/2022/06/29/10-recommendations-by-the-taskforce-on-disinformation-and-the-war-in-ukraine/>〉
- (12) 発行者は、総務省 情報流通行政局 情報流通振興課。監修は、山口真一(国際大学グローバル・コミュニケーション・センター 准教授)、小木曾健(国際大学グローバル・コミュニケーション・センター 客員

研究員)。

- (13) なお、本教材は、総務省の偽・誤情報啓発教育教材担当への一報することで、無償で利用可能である。〈https://www.soumu.go.jp/use_the_internet_wisely/special/nisegojouhou/〉