「スマートフォン利用シーンに潜む脅威 Top10 2023」ガイド

【第二回】フェイクニュース・ディープフェイク対策

【第一版】

2024 年 3 月 31 日

日本スマートフォンセキュリティ協会（JSSEC）
利用部会

文書管理番号 JSSEC-R-20240331-2

■制作■

JSSEC スマートフォン利用シーンに潜む脅威 Top10 2023 選定委員

委員長	松下 綾子	アルプスシステムインテグレーション株式会社
構成員	北村 裕司	サイバートラスト株式会社
	中村 丈洋	株式会社 SHIFT SECURITY
	本間 輝彰	KDDI 株式会社
	三池 聖史	ユニアデックス株式会社

（社名五十音順）

文書管理番号 JSSEC-R-20240331-2

目 次

1. はじめに

1.1. はじめに

一般社団法人日本スマートフォンセキュリティ協会（JSSEC：会長 佐々木 良一）は、2011 年に設立されました。それ以来、急速に普及したスマートフォンは、ビジネスや個人の生活において重要な役割を果たしてきました。

利用部会（部会長：松下 綾子）は、利用者の視点からセキュリティに関する検討を行い、この 10 年以上の間に脅威がどのように変化しているかを再評価することの重要性を認識しました。その結果、「スマートフォン利用シーンに潜む脅威 Top10 2023」（以下、スマホ利用 10 大脅威 2023）を選定し、2023 年 2 月 28 日に発表しました。

さらに、スマホ利用 10 大脅威 2023 で選定された脅威に対処するため、被害を未然に防ぐ方法や被害発生時の対処方法を利用者視点で提唱する必要があると考え、JSSEC 会員企業の有志とワークショップを開催しました。このワークショップでは、各利用シーンにおける経験談の共有や安全対策に関する議論を行い、それらをもとに本ガイドが作成されました。

本ガイドは、スマホ利用 10 大脅威 2023　第 3 位のディープフェイクと第 7 位の SNS フェイクニュースに焦点を当てて作成したもので、詐欺被害の影響をできるだけ抑制するための手助けとなる内容となっています。

1.2. 本ガイドの利用にあたって

本ガイドは、利用部会で行われた JSSEC 会員によるワークショップでの意見をまとめたものです。

「スマートフォン」と「タブレット」を包含する言葉として「スマートフォン」を用います。

また、特に注意記載がない場合は、「フェイク画像」「フェイクニュース「フェイク系に関する情報一般」「ディープフェイク」「ディープフェイクに関する情報一般」を包含する言葉として、「フェイク」を用います。

なお、記載された内容は今後の状況によって変更の可能性があります。

1.3. 本ガイドの目的

スマートフォンを安全に利用するにあたっては、技術的対策で 100%防ぐことは不可能であり、利用者一人一人がスマートフォン利用時の危険性を十分理解し、適切な判断を行うことが重要です。

利用者一人一人が、今回選定した脅威について十分理解していただけることを期待しています。

さらには、若い世代に対して企業や組織、両親や教育関係者が適切な指導ができず、相談すべき相手が友人しかいないという問題も明らかであることから、企業や組織の責任者・担当者や教育関係者や保護者の方々には、是非現状を理解した上で、適切な指導に役立てていただきたいと考えています。

1.4. 想定読者

本ガイドは、主に以下の読者を対象としています。

(1) 企業や組織においてスマートフォンを導入する責任者・企画担当者
(2) 企業や組織においてスマートフォンを導入する際にセキュリティポリシーを策定する責任者、担当者
(3) 企業や組織においてワークスタイル変革を推進する責任者・企画担当者
(4) スマートフォンの利用者
(5) スマートフォン利用者の指導者、教育関係者、保護者

1.5. 対象とする範囲

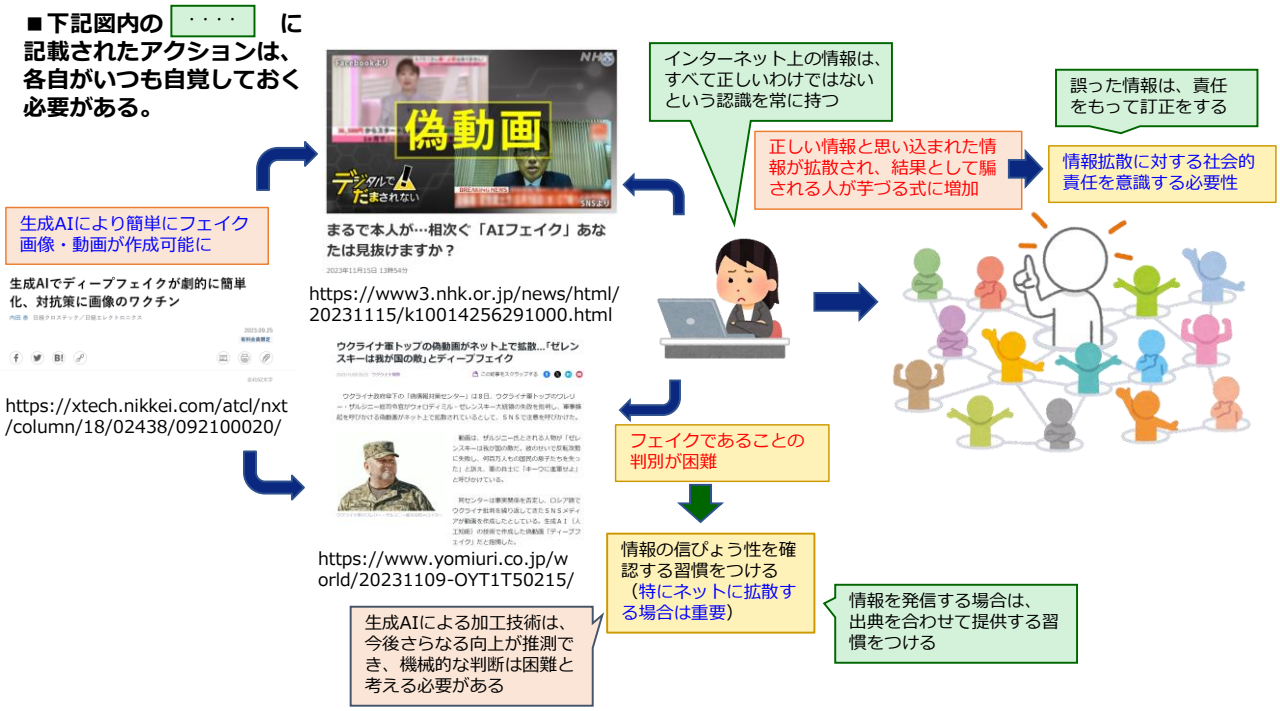
本ガイドは、スマートフォンを利用する個人が対処できる範囲と、それを取り巻く環境について解説しています

2. フェイクニュースを取り巻く、「情報」と「人」の相関図

フェイクニュース・ディープフェイク（以下、フェイクニュース）は凄まじいスピードで進化しており、利用者にとって、ひと目では気付くことが難しくなってきました。被害最小化に向けた対策を検討するために、まず、「情報」と「人」の相関を、図 2-1　フェイクニュースを取り巻く、「情報」と「人」の相関図の通りまとめました。

本ガイドの内容は、この相関図をもとに解説しています。

図 2-1　フェイクニュースを取り巻く、「情報」と「人」の相関図



3. 被害にあわないための対策

フェイクニュース対策を検討するにあたり、最初に、自分や周囲の体験談、および、その時の一次対応内容を議論しました。

3.1. 周囲での体験

フェイクに遭遇した経験については、一人もいないという結果となりました。しかしながら、単に気づいていないだけで、もしかしたら遭遇していたのではという意見も散見されました。

これらの議論を踏まえて、意見として挙がった事例について、表 3-1　遭遇したフェイク事例 の通りまとめました。

表 3-1　遭遇したフェイク事例

	事例
事例 1	● 実際に遭遇したことはない。 ➢ 気付いていないだけかもしれない。➡気にしながら情報に接しなければいけない。 ➢ 気付いているが、実害がないので見て見ないふり。➡一部の人以外には無害なことが多いが、有害なこともあるという認識が必要。もし自分に不利益があると思っても、無条件には信じないようにする。 ➢ 子どもや高齢者などがフェイクを信じてしまわないか心配。➡デジタルリテラシーが低い人は、とくに要注意。例）「当選しました」
事例 2	● 鯖缶がなくなるニュースが出回ったが、フェイクニュースだったものと思われる。
事例 3	● 台風のときに養生テープが必要と言われたが効果がない。　➡伝言ゲームになっていて、目的と効果などの情報が正しく伝わっていない。情報の切り取り方が悪いと、結果としてそれがフェイクニュースのような状況となる。 ➢ 正しい情報か否かがわからない。 例）養生テープの効果は、ガラスが割れた際の離散を防ぐためであり、窓を割れるのを防ぐものではない。 ➢ 情報の効用が不明確な場合、その人の便益に繋がらないこともある。本来の情報と異なる受け取り方をされるケースは要注意。 ➢ 善意を持って発信されているニュースでも、切り取り方によってはフェイクになり得る点に注意が必要。
事例 4	● Facebook で「ともだち申請」した時、写真が明らかに本人とは違う顔だった。 ➢ これもフェイクというのか？しかしそもそも、本人なのかどうか未だに確認しておらず判らない。

事例 5	● トランプ大統領のフェイクがあると聞いた。 ➢ 自分が欲しいと思った情報を探したときに、出てくると思うとこわい。

3.2. フェイクが増えている背景

フェイクが増えている要因として、SNS の普及により、情報を自由に発信できる環境が整ったことが挙げられます。また、インフルエンサーと呼ばれる人々の発信が、それを閲覧する多くの人々の信条や行動に影響を与えることから、誤った情報は、より広まりやすくなります。

近年は「認知領域を含む情報戦（認知戦）」として、国レベルでの偽情報の流布も行われており、さらに状況を複雑にしました（※1）。

AI 技術の進化により、生成系 AI などの新しい技術の普及が進み、本物そっくりな偽情報が作成しやすくなったことも大きな要因の一つです。

加えて、スマートフォンの普及により人々が日常的に情報に触れる機会が増えたことや 、様々なサービスを利用することが容易になったことなど、生活習慣を通してフェイクを広めやすい環境が整いました。これらの要因が合わさり、フェイクが拡散しやすい状況を生み出しています。

※1： 参考サイト/防衛省「認知領域を含む情報戦への対応」
https://www.mod.go.jp/j/approach/defense/infowarfare/index.html

表 3-2　フェイクが増加している背景

	事例
意見 1	● メディアの情報などが信用できなくなってきた。何を信じていいのか分からなくなってきている状態を、悪用している。
意見 2	● 有名な人が言うと、間違った情報でも正しい情報と思い騙されやすい。
意見 3	● 生成系 AI の技術の進歩を感じている。簡単に作れるツールも出てきている。 ➢ 人の音声をまねする音声エンジンは、その人の声など 5 分～10 分の元データが必要だったが、現在は数十秒で作れる。 ➢ 電話の先が AI なのか本人なのか、非常に聞き分けづらくなっている。 ➢ 画像 1 枚あれば、会話しているような映像はすぐ作れる。 ➢ 会議で最初に顔出しした時に、その人に気づかれずにフェイク画像を作ることもできる。
意見 4	● お金の送金について、昔は銀行振り込みや ATM が必須だったのに、今はスマートフォ

	ンだけで出来るようになった。 ➢ 送金の指示（依頼）を受けた時、気軽に送金できるようになってしまい、犯罪に巻き込まれることが増えた。 ➢ 便利になった分、そのニュースが正しいか否かを一人ひとりが気にしなければいけなくなった。

3.3. 求められる対策

フェイクに騙されないための対策は、多岐に渡ります。

まず、技術の進化を楽しむ一方で、その悪用にも警戒心を持つ必要があります。AI の進展や犯罪に協力する人々の増加により、「変な日本語を見つけて見分ける」という対策は効果が薄くなっており、情報の信頼性を確認することが肝要です。信頼できる情報源かどうかを確認し、公式の報道機関や信頼性のあるメディアからの情報を優先しましょう。また、衝撃的な情報や驚くような主張があった場合は、複数の情報源から、その情報が裏付けられているかを確認することが重要です。

さらに、フェイクが多い時代において、ネット上の情報は取捨選択し、確証の持てない情報は拡散しないよう努める必要があります。ニュースであれば出元の情報源を調査し、1 社からしか出ていない場合は信用しないようにしましょう。「自身の意見や信念に合う情報のみを信じる」ということをせず、客観的な視点を持つことが大切です。

また、啓発の機会を増やし、「インターネットの情報は、必ず正しいとは限らない。」という危機感をきちんと伝えるための情報発信（特集記事）を行ったり、学校での啓発活動を増やしたりすることが、被害を最小限に防ぐために重要です。特に、若年層に対する啓発活動は効果的です。

情報の正当性を図る上では、SNS やウェブサイトで情報を発信している個人や組織について調査し、信頼性や専門性を確認することも大切です。

騙されてしまった場合は、間違いを公表することで二次被害を防ぐことができます。情報の真偽を確認し、誤情報に対して積極的に正しい情報を発信、共有することが重要であり、これらの対策を実践することで、フェイクによる被害を最小限に抑えることができます。

上述について、挙がった意見を以下の表 3-3　フェイクについての注意点 の通りまとめました。

表 3-3　フェイクについての注意点

	事例
注意点１	● いろいろな技術が出てきて面白い時代だが、犯罪に悪用されていることを認識しておく必要はある。
注意点２	● AI の発達や悪行に協力する日本人の増加により、「変な日本語を見つけて見分けましょう」という対策も、今は効果が薄くなった。
注意点３	● フェイクは誰もが容易に発信できる。
注意点４	● 技術の進展により、情報の真偽が確認しづらく、フェイクが見破られにくい時代になってきた。
注意点５	● プラットフォームに「利用者が情報の信頼性を判断するための材料」を通知する仕組みが求められている。 ➢ X（Titter)の例 ①リツイート（RT)に対処していなかったことが問題になり、RT 時にアラームがでるようになった。 ②コミュニティノートが X に追加された。内容の出典などをコメントで残せる。「この投稿の真実度は２％」「AI が作った」など、明記されるようになった。

上記の注意点を踏まえた対策について、以下の表 3-4　フェイクに騙されないための対策について（技術的対策以外)、の通りまとめました。

表 3-4　フェイクに騙されないための対策について

	事例
対策１	● 確証が持てない情報は拡散させない。 ➢ ニュースであれば、出元の情報源を調べる。1 社からしか出ていない場合は信用しない、など。 ➢ 出典などの「情報の信頼性を判断するための材料」を活用する。
対策２	● 騙されたときは、間違いを公表することで二次被害を防ぐ。
対策３	● デマも多い。ネット上の情報は「得る」のではなく「取捨選択して捨てる時代」
対策４	● 啓発の機会を増やす。「インターネットの情報は必ず正しいとは限らない。」という危機感をきちんと伝えることが重要。 ➢ テレビなどでの啓発特集、学校・教育現場・企業での勉強会。 ➢ 若年層のフェイクニュース拡散が多いため、学校で啓発活動は効果的。 ➢ 情報を自ら取りに来る人はよいが、そうでない人もいるので広くリーチさせる。
対策５	● 啓発のための資料や学習教材などを作って提供する。

3.4. フェイク増加における課題

フェイクが増える中、その対策を行うための課題として挙げられている項目の一つが、デジタルデータの真正性の担保です。

生成 AI を使って動画が簡単に作成されるようになった現代では、情報の信頼性や真偽の判断が難しくなっています。このため、デジタルデータの真正性をどのように確保するかが重要となります。

さらに、言論の自由とファクトチェック（事実確認）に関しては、自由と公序良俗、公益などとのバランスを取ることが求められます。フェイクに対する、法的な取り締まりや処罰の在り方についての検討も必要です。

なお、特に SNS の利用にあたっての注意事項は、刻々と変化していることもあり、参考情報が少ないのも現実です。自分が利用しているサービスの利用規約や注意喚起の連絡等を、確実に確認することが大切です。

上述の課題を、以下の表 3-5　フェイクに対する課題　にまとめます。

表 3-5　フェイクに対する課題

	事例
課題 1	● デジタルデータの真正性をどう担保するか？ ➢ 生成 AI を使って動画を簡単に作れる時代。その情報の証拠能力が問われる時代になる。
課題 2	● 言論の自由とファクトチェック（事実確認）に、どう折り合いをつけるか？ ➢ 自由と公序良俗・公益などには正面から向き合う。自由であることと、社会的な意義は常に念頭に置く必要がある。 ➢ 表現の自由があり、フェイクニュース自体に違法性がないという専門家もいる。 ➢ フェイクを見つけた時、報告し取り締まる場がネットの世界にはない。（サービスごとの個別対応） ➢ 内容次第では業務妨害、名誉棄損などで処罰されることがあるが、日本で処罰される際の刑罰が軽い。 ➢ この件に限らず、罰金が少なく、強烈な抑止力にはならない。
課題 3	● フィッシング詐欺メールに関する情報については参考サイトがあるが、SNS 関連の情報については適切な参考サイトがない。

4. おわりに　～　いま私たちにできること

フェイクの情報がますます増える中、情報に騙されないためには以下の点に留意することが重要です。
法整備が追いついていない現状を踏まえ、情報収集には最大限の注意を払いましょう。

1. 情報収集においては、インターネットだけに頼らず、複数の情報源を活用しましょう。

2. インターネットの情報は必ずしも正しいとは限らないことを、常に意識しておきましょう。

3. 誰もがフェイクを容易に作成でき、手軽に発信できることを念頭に置いておきましょう

4. インターネットの情報を利用する際には、情報元を十分に精査し、出典も明確に記載しましょう。
   発信（リツイート）する時も同じです。

5. もし誤った情報を拡散したと分かったら、勇気と責任を持って、速やかに訂正しましょう。