

デジタル安全意識に関する消費者調査 「2026年版 アバスト セーフテックレポート」を発表

日本における成人の44%が「説得力のある AI 生成・加工コンテンツを見抜ける自信がない」と答える中、

31%がチャットボットへの機密性の高い可能性がある情報の共有を経験または検討。

AI による偽情報を見抜く自信の低さとは裏腹に、個人情報の共有には抵抗感が薄い傾向に

※世界12か国調査を実施し、本レポートでは日本国内のデータのみを抽出しています。

Gen (NASDAQ: GEN) の消費者向けサイバーセーフティブランドであるアバストは、日本を含む世界12か国で消費者を対象に実施したデジタル安全意識に関する消費者調査「2026年版 アバスト セーフテックレポート」を発表しました。

本調査では、日本では AI による偽情報を見抜く自信がないと答えた人の割合が高いにも関わらず、個人情報を守るための意識が低い行動を取る傾向にあることが明らかになりました。これは、AI に対する自信のなさが必要以上に安全な行動につながるわけではないことを示唆しています。以下は、日本人の成人における回答を抽出し、レポートしています。アバストは、個人情報の共有を最小限に抑え、不審な要求を疑い、詐欺に関する知識を家族や友人と共有することの重要性を呼びかけています。



※AI によって修正または生成されたコンテンツを含みます。

<サマリー>

●「説得力のある AI 生成・加工コンテンツを見抜ける自信がない」が「自信がある」を上回る結果に

- ◆ 「説得力のある AI 生成・加工コンテンツを見抜ける自信がある」・・・56%
- ◆ 「説得力のある AI 生成・加工コンテンツを見抜ける自信がない」・・・44%

●機密性の高い可能性がある情報が共有されている

「AI チャットボットに少なくとも1つの機密性の高い情報を共有した、または共有を検討したことがある」・・・31%

上記のうち実際に AI に共有された内容として、以下が挙げられた。

- ◆ 「プライベートなメッセージや、メールのスクリーンショットの共有」・・・15%
- ◆ 「仕事の書類」・・・11%

●AIを活用した詐欺はより精巧になり、見逃すリスクが高まっている

詐欺の恐れがあるサインではあるものの、見過ごしやすいこととして以下が挙げられた。

- ◆ 「確認目的として個人情報を求められること」・・・42%
- ◆ 「知っている名前、声、ブランドだが、どこか違和感がある」・・・34%
- ◆ 「好条件すぎるオファー」・・・31%
- ◆ 「急いで行動するよう求められること」・・・30%

AI 生成コンテンツを見抜く自信の無さと、AI 活用の実態にギャップ

AI 生成コンテンツが日常生活に広がる中、21%が「説得力のある AI 生成・加工コンテンツを見抜ける自信がある」と回答し、44%が「見抜く自信がない」と答えています。米国では「AI 生成コンテンツを見抜く自信がない」と答えた人は13%にとどまり、日本は特に、不安を感じている人が多い傾向にあります。

一方で、31%が、「AI チャットボットに少なくとも1つの機密性の高い情報を共有した、または共有を検討したことがある」と回答しました。具体的には、15%が、プライベートなメッセージやメールのスクリーンショットを共有または共有を検討したことがある、11%が「仕事の書類」について、共有または共有の検討をした経験があると答えています。

AI の偽情報を見抜く自信の有無にかかわらず、個人情報をどのように扱うかについては、別の注意が必要です。AI ツールに入力した情報は、利用するサービスの設定やデータの取り扱い方針によって、会話の終了後も保存・利用される恐れがあります。メールやチャット上のメッセージ、仕事の書類には、氏名、連絡先、職歴、勤務先に関する情報など、きわめて秘匿性の高い情報が含まれる場合があり、共有前に情報の必要性やサービスのプライバシー設定を十分に確認することが重要です。

アバストの Global Head of Scam Research である Leyla Bilge は、次のように述べています。

「AI による偽情報を見抜けるか不安を感じているにもかかわらず、機密性の高い情報を AI に預けることには抵抗が薄い——そこに、日本のユーザーが抱える新たなリスクがあります。AI を見抜く自信がないのであれば、自分のデータを AI に預ける際にも、同じくらい慎重になる必要があります。」

オンライン上で何かが不審だと感じた場合でも、見逃しやすい詐欺手口が横行

AI を悪用した詐欺では、精巧な画像や音声だけでなく、相手に行動を急がせたり、個人情報を提供させたりする手口にも注意が必要です。

調査によると、日本の成人の42%が「確認目的として個人情報を求められること」を最も見過ごしやすいサインとして挙げました。また、34%が「知っている名前・声・ブランドなのに、どこか違和感があること」、31%が「通常より良すぎるオファー」、30%が「急いで行動するよう求められること」も、「不審だ」という自身の直感を見逃しやすくする可能性があるかと答えています。

Gen Threat Labs による偽の有名人動画や AI 生成詐欺コンテンツに関する研究でも、現実的な顔や声は詐欺を信じ込ませるための入り口であり、実際には魅力的すぎるオファーや緊急性、「確認するだけ」といった要求が、人々を行動へ誘導する重要な要素となっていることが示されています。

詐欺の知識は広がる一方、家族や友人へ共有するなどの注意喚起には繋がっていない

不審なメッセージや電話、DMを受け取った際、36%が「誰にも話さず削除する」、29%が「自分で調べる」と回答しました。自分で対処する行動が見られる一方、その行動が自身で得た情報を周囲と共有する機会損失へ繋がっています。

80%は、詐欺を扱った犯罪ドキュメンタリーやポッドキャスト、シリーズを見たり聞いたりしたことがあると回答しました。その中で、52%が「普段のデジタルライフで詐欺への警戒意識が高まった」、51%が「以前よりメッセージや仕事に関連するオファーを疑うようになった」と答えています。一方で、詐欺に関するコンテンツを何らかの形で見聞きしたことがある人のうち、それを友人、パートナー、家族との会話のきっかけにした人は48%にとどまりました。

こうした結果は、詐欺に関する知識が個人の注意喚起にはつながっているものの、周囲の人々と共有する行動には必ずしも結びついていないことを示しています。自分が見聞きした詐欺の手口を家族や友人と話し合うことは、同様の被害を防ぐための大切なきっかけとなります。

AI時代に個人情報を守るための重要なアクション

アバストは、AIによる偽情報や詐欺から身を守り、個人情報を安全に扱うために、以下の行動を推奨しています。

1. AIツールに共有する情報を最小限にする

- ・履歴書、仕事の書類、個人情報などを入力する前に、本当に共有が必要か確認する
- ・利用するAIサービスのプライバシーポリシーやデータの保存・利用設定を確認する
- ・第三者に知られたくない情報は、原則として入力しない

2. 精巧な画像や音声だけで信用するのではなく、何か要求されているのかを確認する

- ・AI生成画像や音声が本物に見えても、それだけで信用しない
- ・「今すぐ対応してほしい」「確認のために個人情報が必要」といった要求には注意する
- ・不審な連絡は、公式サイトや信頼できる連絡先から別途確認する

3. 好条件すぎるオファーや支払いの要求を疑う

- ・異常に魅力的な条件や、大幅な割引には慎重に対応する
- ・信頼できる販売店のみを利用し、購入前に他の利用者のレビューを確認する

4. 不審な体験や詐欺の知識を周囲と共有する

- ・怪しいメッセージや電話を受け取った際は、必要に応じて家族や友人に相談する
- ・詐欺に関するニュースや動画で学んだ手口を、身近な人との会話のきっかけにする
- ・「困ったときに誰に相談するか」をあらかじめ決めておく

5. セキュリティ対策を日常の習慣にする

- ・デバイスやアプリを最新の状態に保つ
- ・信頼できるセキュリティソフトやブラウザの保護機能を活用する
- ・重要なアカウントには強固で固有のパスワードと多要素認証を設定する

AI を安全に活用するためには、すべての偽情報を見抜けるようになることだけが重要なではありません。共有する情報を慎重に選び、不審な要求に対して確認する習慣を持ち、得た知識を周囲と共有することが、自分自身と大切な人を守ることに繋がります。

「アバスト セーフテックレポート」について

「2026年版 アバスト セーフテックレポート」の詳細や、AI の脅威、詐欺から身を守るためのアドバイスについては、[\[レポート掲載ページのリンク\]](#) をご覧ください。

本調査は、Dynata により2026年5月29日から6月13日まで、日本国内で18歳以上の成人1,000人を対象にオンラインで実施されました。データは必要に応じて年齢、性別、地域によってウェイトバックされ、調整されています。

アバストについて

アバストは、デジタルセキュリティとプライバシーのリーダーであり、信頼できる消費者向けブランドを通じてデジタルの自由の実現を目指すグローバル企業 Gen (NASDAQ: GEN) の一員です。アバストは、モバイル、PC、Mac 向けの製品・サービスを通じて、世界中の何億人ものユーザーをオンライン上の脅威から保護しています。

アバストの製品・サービスは、VB100、AV-Comparatives、AV-TEST、SE Labs などの第三者評価機関から高い評価や認証を受けています。また、アバストは Coalition Against Stalkerware、No More Ransom、Internet Watch Foundation のメンバーです。詳しくは、[アバスト.com](#) をご覧ください。