

2026 年 7 月 23 日

AI 詐欺から資産形成を守る「奪われない力」

～AI 勧誘・投資詐欺・暗号資産送金が突く個人マネーの盲点～

政策調査部 主席研究員 柏村 祐

(要旨)

- AI の普及により、詐欺メールや偽メッセージは見抜きにくくなっている。しかし、本稿の焦点は、AI 詐欺をメール対策や偽サイト対策として捉えることにはない。より重要なのは、AI によって高度化した詐欺が、個人の資産形成そのものを狙うリスクになっている点である。
- AI 詐欺は、第一に偽広告や偽メッセージを通じて投資家との接点を広げ、第二に投資詐欺として老後資金やインフレ対策への期待を悪用し、第三に暗号資産送金を通じて資金回収を困難にする。AI は詐欺の「入口」を広げ、投資詐欺は資産形成層を直撃し、暗号資産は資金流出の経路になっている。
- 世界銀行 (World Bank) の調査によれば、新興国・途上国を中心とする金融監督当局は、AI 利用によって深刻化し得る詐欺やスキームを、消費者保護上の主要なリスクとして警戒している。AI は詐欺の量産コストを下げ、個人の関心や不安に合わせた対話型の勧誘を可能にすることで、詐欺の入口を広げている。
- 米国連邦捜査局 (FBI) のデータによれば、サイバー空間を利用した詐欺の損失額において「投資詐欺」が最大となっている。日本でも、警察庁の 2025 年確定値では、SNS 型投資詐欺の認知件数と被害額が前年から大きく増加している。さらに金融庁は、AI 診断をうたい文句にウェブサイトに誘導し、分析レポート配信を装って SNS へ誘導する投資勧誘事例を注意喚起している。被害者を信じ込ませる AI と、資金を素早く移転させる暗号資産が結びつくことで、資産形成をめぐる被害はより複雑かつ深刻化している。
- AI 時代の資産形成においては、NISA や iDeCo などを活用して資産を「増やす力」だけでなく、情報の真偽を見極め、送金プロセスの妥当性を確認し、詐欺から資産を「奪われない力」が不可欠になる。金融リテラシーは、もはや「どの商品を買うか」だけではなく、「誰の情報信じるか」「どの経路で資金を送るか」を判断する力まで含むものへと広がっている。

1. AI詐欺は「メール対策」だけでは終わらない

AI の急速な普及により、詐欺メールや偽メッセージはかつてないほど見抜きにくくなっている。従来であれば、不自然な日本語、怪しい送信元アドレス、過度に不安を煽る文面などから、

私たちは直感的に詐欺を疑うことができた。しかし現在のAIは、自然な文章を生成し、実在する金融機関や企業になりすますだけでなく、著名人や専門家の顔・声を模倣した画像、音声、動画まで低コストで作り出せるようになっている。しかし、本稿が焦点を当てるのは、「AIを使った巧妙な詐欺メールをどう見抜くか」という表面的な対策についてではない。より深刻な問題は、AIによって高度化した詐欺が、個人の資産形成そのものを狙うようになっている点にある。老後資金への不安やインフレへの懸念、NISAやiDeCoの普及を背景とした投資への関心の高まりは、本来、望ましい資産形成行動につながるものである。一方で、その投資意欲や将来への不安が、AIを悪用した投資詐欺の標的にもなっている。

ここで問うべきなのは、AIを悪用した詐欺がどれほど巧妙になったかではなく、それがどのような経路を通じて個人の資産形成を脅かすのかという点である。本稿では、この問題を、第一に詐欺の入口となる情報接触の高度化、第二に投資詐欺による資産形成層への被害、第三に暗号資産送金を通じた資金流出という三つの経路から整理する。そのうえで、AI時代の資産形成において求められる金融リテラシーが、従来からどのように変化しているのかを考える。

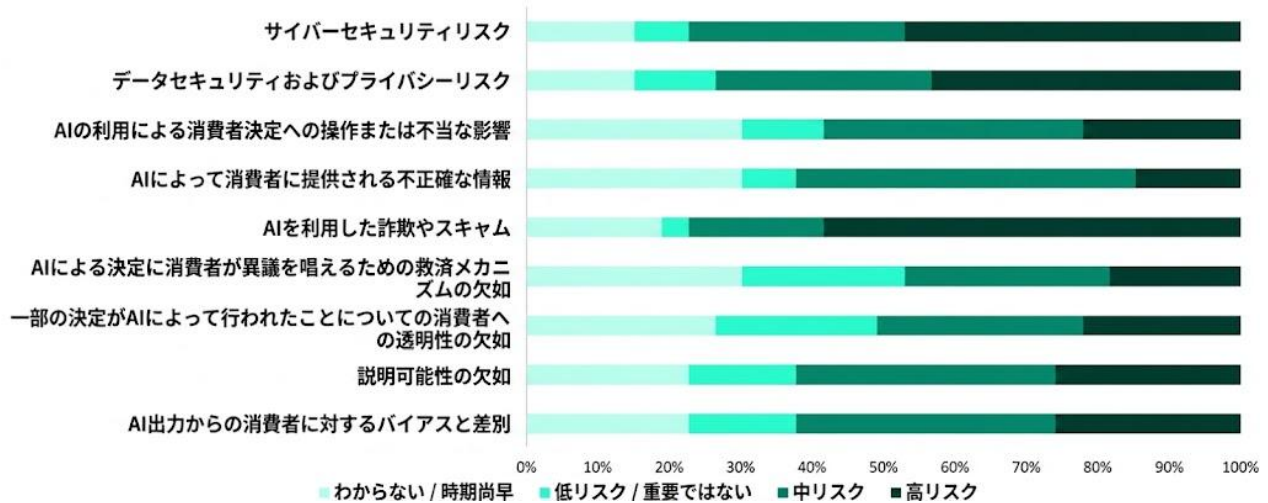
2. AI詐欺はどのように資産形成を脅かすのか

(1) AIは詐欺の「入口」を高度化する

AIは、詐欺師にとって「騙すためのコスト」を劇的に引き下げるツールとなっている。世界銀行（World Bank）が2025年に公表したレポートは、新興国・途上国を中心とする27の金融監督当局を対象に、金融分野におけるAI利用と監督上の課題を調査したものである。同レポートは、AIが金融サービスや監督実務を変革し得る一方で、消費者保護上の新たなリスクをもたらすことを指摘している。資料1は、金融分野におけるAI利用に伴う消費者リスクについて、金融監督当局がどの程度リスクを認識しているかを示したものである。「AIを利用した詐欺やスキーム」は、サイバーセキュリティ、データセキュリティ、消費者プライバシーと並ぶ主要な懸念領域として示されている。世界銀行の本文でも、AIに伴う消費者リスクについて、金融当局が詐欺・スキーム、サイバーセキュリティ、データセキュリティ・プライバシーを強く懸念していることが説明されている。

AIは、詐欺の「入口」をかつてなく広く、巧妙化する。SNS上の情報やメッセージのやり取りを手掛かりに、個人の関心や不安に合わせた対話型の勧誘を大量に生成することが容易になった。著名人を装った偽の投資広告をクリックすると、AIチャットボットが親身なアドバイザーのように振る舞い、ターゲットを偽の投資グループや投資アプリへ誘導する。自然な文面、本人確認を装った手続き、著名人を装った広告、対話型の勧誘が組み合わせられれば、個人が資産形成に向かう過程で偽情報に接触する機会も増えるだろう。

資料 1 AI 利用に伴う消費者リスクへの金融監督当局の認識



(注) 今後 5 年間における、管轄内の金融機関による AI 利用から生じる消費者リスクに対する評価。調査対象は新興国・途上国を中心とする金融監督当局 27 機関。

(出所) World Bank, “Artificial Intelligence for Financial Sector Supervision: An Emerging Market and Developing Economies Perspective,” より第一ライフ資産運用経済研究所作成

(2) 投資詐欺は資産形成層を直撃する

AIによって最適化された詐欺メールや偽広告は、それ自体が終着点ではない。その先で待ち受けているのは、偽の投資プラットフォーム、未公開株の勧誘、あるいは「AIが自動で高利回りを実現する」といった架空の投資案件である。FBIのインターネット犯罪苦情センター（IC3）がまとめた 2025 年版レポートは、サイバー空間を利用した詐欺における投資詐欺の大きさを示している。2025 年の IC3 への苦情は 100 万件を超え、報告損失額は 208 億 7,700 万ドルに達した。犯罪類型別の損失額を見ると、「投資詐欺」は 86 億 4,861 万 7,756 ドルで最大となっている。資料 2 は、サイバー空間を利用した詐欺の犯罪類型別被害額トップ 5 を示したものである。投資詐欺の損失額は、ビジネスメール詐欺や技術サポート詐欺を大きく上回っている。これは、被害者が「騙されている」と気づかないまま、将来のための投資だと信じて、複数回にわたり多額の資金を投じてしまうためである。

日本でも同様の構図はすでに現れている。警察庁の 2025 年確定値によれば、SNS型投資詐欺の認知件数は 9,523 件、被害額は 1,288 億円となり、前年に比べて認知件数、被害額ともに増加した。当初の接触手段では、バナー等広告が 3,785 件、ダイレクトメッセージが 3,549 件であり、これらが全体の約 8 割を占める。警察庁は、YouTubeや投資関連サイトにおけるバナー等広告、Instagram、LINE、Facebookにおけるダイレクトメッセージを当初の接触手段とする被害の増加を指摘している。また、著名人の画像や動画を無断で使用した広告や、「必ずもうかる」「元本保証」などの文言を含む広告も確認されている。金融庁も、動画投稿サイトの広告等からSNSのクロードチャットへ誘導され、講師やアシスタントを装う人物が投資を指南する事例、AI診断をうたい文句にウェブサイトへ誘い込み、分析レポート配信を装ってSNSへ誘導する事例を注意喚起し

ている。これは、AIによって偽広告や偽メッセージの作成が容易になるなかで、投資家との最初の接点がSNS上で広がっていることを示している。

資産形成への関心が広がるほど、投資初心者は詐欺の標的になりやすい。FBIは、投資詐欺においてAIが潜在的な被害者との会話を強化し、相手ごとに異なるように見える大量の会話を素早く生成できると指摘している。また、AIで生成された著名人、経営者、信頼できる人物の動画や音声、偽の投資機会を本物らしく見せるために使われている。資料2が示す投資詐欺の被害規模そのものを、AIの普及だけで説明することはできない。ただし、AIによって勧誘の自然さや個別対応の精度が高まれば、被害者が詐欺を見抜くことは一段と難しくなる。AIの悪用は、既に深刻な投資詐欺被害をさらに拡大させかねない要因として警戒する必要がある。

資料2 サイバー空間を利用した詐欺における犯罪類型別被害額トップ5



(注) 2025 年に IC3 へ報告された Cyber-Enabled Fraud の犯罪類型別損失額。

(出所) FBI IC3, “2025 Internet Crime Report,”より第一ライフ資産運用経済研究所作成

(3) 暗号資産は投資詐欺の送金経路になっている

AIが被害者を信じ込ませ、投資詐欺が資金を引き出す口実を作った後、その資金はどのように移転されるのか。ここで登場するのが暗号資産である。暗号資産自体は、国境を越えた迅速な価値移転を可能にする金融インフラであり、それ自体を一律に否定すべきものではない。むしろ、ブロックチェーン上の送金記録は公開され、取引の追跡自体は可能である。問題は、送金先の本人特定、国外移転後の凍結、資金回収が難しく、一度送金した資金を被害者側の判断だけで取り戻すことが極めて困難になる点にある。FBIの2025年版レポートは、暗号資産関連の苦情件数と被害額が増加していることを示している。2025年にIC3へ報告された暗号資産関連の苦情は18万1,565件、損失額は113億6,600万ドルに達した。前年比では、苦情件数が21%増、損失額が22%増である。

日本のデータを見ても、暗号資産はSNSを起点とする詐欺被害の資金移転経路として存在感を高めている。以下の警察庁の数値はSNS型ロマンス詐欺に関するものであり、投資詐欺に限定した統計ではない。ただし、恋愛感情や信頼関係を形成した後に偽の投資へ誘導する手口も多く、心理的操作と暗号資産送付が結び付く実態を示す資料として重要である。警察庁の2025年確定値では、SNS型ロマンス詐欺における暗号資産送信型の認知件数は2,177件、被害額は247.7億円とな

り、前年から大きく増加した。さらに、振込型における暗号資産振込と合わせると、一次的な主な被害金等交付形態が実質的に暗号資産であるものは、総認知件数の 40.4%、被害総額の 48.6% を占める。これは、暗号資産が一部の投資家だけの問題ではなく、SNSを起点とした心理的操作型の詐欺被害において、資金流出経路として広がっていることを示している。

FBIは、暗号資産投資詐欺について、心理的操作、正当性の演出、暗号資産の利用を組み合わせ、被害者に多額の資金を投じさせる長期型の詐欺だと説明している。典型的には、テキストメッセージ、SNS、広告、マッチングアプリなどを通じて接触し、やり取りをメッセージアプリへ移したうえで、投資グループや専門家を装って被害者を誘導する。その後、被害者は偽の投資プラットフォームやアプリへ暗号資産を送金させられ、画面上では架空の利益を見せられる。出金しようとする、税金や手数料名目でさらに資金を要求され、最終的に資金を奪われる。AI時代の詐欺リスクは、騙す技術だけで完結しない。被害者を信じ込ませる「AI」と、資金を素早く移転させる「暗号資産」が結びつくことで、資産形成をめぐる被害はより複雑かつ深刻化している。

資料 3 暗号資産が関連する苦情件数と被害額の推移



(注) 2017 年から 2025 年までの暗号資産が関連する苦情件数および被害額。2025 年の苦情件数は 18 万 1,565 件、損失額は 113 億 6,600 万ドル。

(出所) FBI IC3, “2025 Internet Crime Report,”より第一ライフ資産運用経済研究所作成

3. AI時代の資産形成には「増やす力」と「奪われない力」が必要になる

AI 詐欺が資産形成を脅かす経路は大きく三つに整理できる。第一に、偽広告や偽メッセージを通じて投資家との接点を広げること。第二に、投資詐欺として資産形成への期待を悪用すること。第三に、暗号資産送金を通じて資金回収を困難にすることである。このように、AI 時代の詐欺リスクは、単なる迷惑メールや偽サイトの問題にとどまらない。個人が資産形成を始め、投資先を判断し、資金を送金するまでの過程に入り込み、その意思決定や行動を歪めるリスクとして捉える必要がある。重要なのは、AI 詐欺のリスクがあるからといって、投資そのものを避けるべきだということではない。むしろ、NISA や iDeCo の普及、投資信託を活用した資産形成の定着、

デジタル金融サービスの浸透によって、個人が資産形成に向き合う機会が増えているからこそ、AIの進化に対応した新たな金融リテラシーが求められている。

目の前の投資アドバイスは、本当に実在する専門家のものなのか。勧誘してくる業者は、金融当局に登録された正規の業者なのか。投資資金の送金先が、不自然な暗号資産ウォレットになっていないか。こうした情報の真偽を見極める力に加え、勧誘から送金に至るまでの手続が適切かどうかを確認する力が、AI時代の資産形成における前提条件となりつつある。特に注意すべきなのは、AI詐欺が人の不安や焦りにつけ込む点である。老後資金への不安、インフレに対する焦り、周囲の人だけが投資で利益を得ているのではないかという焦燥感、専門家に相談して安心したいという心理などが、その対象となる。AIは、相手の感情や置かれた状況に応じて、もっともらしく説得力のある言葉を返すことができる。そのため、詐欺師にとってAIは、単なる文章作成のための道具ではない。被害者の不安や期待に寄り添っているように見せ、信頼させて送金へと誘う「誘導装置」となっている。

AI時代の資産形成では、資産を「増やす力」だけでなく、資産を「奪われない力」が同時に問われる。個人が自らの防衛力を高めることはもちろん、金融機関による異常な送金の検知、暗号資産交換業者による不審な取引の監視、監督当局による登録業者情報の周知など、社会全体で被害を防ぐ仕組みも欠かせない。誰の情報を信じるのか、どのような経路で資金を送るのか、そして、疑問を感じたときに一度立ち止まって確認できるかが重要になる。資産形成は、増やすための知識だけでは成り立たない。情報を疑い、送金を見直し、自らの資産を守る判断力があってこそ、AI時代の資産形成は初めて確かなものとなる。

以 上

【参考文献】

- ・World Bank, “Artificial Intelligence for Financial Sector Supervision: An Emerging Market and Developing Economies Perspective,” 2025.
- ・FBI Internet Crime Complaint Center, “2025 Internet Crime Report,” 2026.
- ・警察庁「令和7年における特殊詐欺及びSNS型投資・ロマンス詐欺の認知・検挙状況等について（確定値）」2026年。
- ・金融庁「それ詐欺です！SNS上の投資勧誘にご注意ください！」2026年更新。