

## 巧妙化する手口でビジネスパーソンが標的に SNS型投資詐欺

iDeCoやNISAの登場により投資が身近なものとなった昨今、SNSを悪用した投資詐欺の被害が急増しています。これらの詐欺は非常に巧妙で、1件当たりの被害額が1,000万円を超えるなど、高額になる場合もあるそうです。このようなSNS型投資詐欺は、どのように注意したらいいのでしょうか。

### ■SNS型投資詐欺とは？

SNS(Facebook、X(旧Twitter)、Instagramなど)を通じて「必ず儲かる」などと投資を勧誘し、金銭をだまし取る詐欺です。著名人の名前や写真を悪用した偽広告やメッセージなどで信用させ、最終的に「投資金」や「手数料」などの名目で振込を求められます。被害は急増しており、2025年5月には単月で被害額が83.2億円に達しました。

### ■主な手口と特徴

#### ① DM(ダイレクトメッセージ)による接触

- ・「副業に興味ありませんか？」「簡単に稼げる方法があります」などの甘い誘い文句。
- ・有名人や投資家を装った偽アカウントなどを使用。

#### ② 少額の成功体験を演出

- ・最初に少額を投資させ、実際に「利益が出た」と見せかけて信頼を得る。
- ・利益を出金できたように見せる偽アプリや画面を使用。

#### ③ 高額投資への誘導

- ・「もっと稼ぐには追加投資が必要」「手数料を払えば出金できる」と言って、次々と送金を要求。

#### ④ 最終的に連絡が途絶える

- ・出金できないまま、アカウントが削除されるか、ブロックされて音信不通に。

### ■実際の被害事例（警視庁特殊詐欺対策ページより）

#### ✂ 事例① SNS広告からの誘導

50代女性がSNS広告をきっかけに、著名人を名乗る偽アカウントに誘導され、投資グループに参加。やり取りを重ねるうちに信用し、1億円以上を指定口座に振り込んでしまった。

#### ✂ 事例② SNSで知り合った人物からの勧誘

70代男性がSNSで知り合った女性から暗号資産投資を勧められ、専用アプリを使用。取引の中で「保証金」や「税金」などの名目で複数回送金し、合計1億円以上をだまし取られた。



## ■被害に遭わないためのチェックポイント

### ☒ 投資先の信頼性を確認

→ 金融庁の登録業者かどうかを公式サイトで確認しましょう。

(金融庁サイト<https://www.fsa.go.jp/ordinary/chuui/highrisk.html>)

### ☒ 「必ず儲かる」「あなただけ」などの甘い言葉に注意

→ 詐欺師は巧みに心に入り込みます。まず疑う姿勢を。

### ☒ 著名人のなりすましに注意

→ 著名人本人の公式アカウントかどうかを必ず確認しましょう。

### ☒ 暗号資産や投資アプリの実在性を確認

→ 勧められた名称をネットで検索して調べましょう。

### ☒ 振込先口座が不自然でないか確認

→ 振込先が個人名義であったり毎回異なる口座は要注意です。

## ■誰もが被害者になり得る時代に

SNS型投資詐欺は、投資に関心を持つすべての人が被害に遭う可能性があります。特に、資産形成を意識し始めた若年層や、まとまった資金を持つ中高年層、そして副業や資産運用を検討するビジネスパーソンや中小企業の役員・社員も例外ではありません。

## ■SNSを通じた詐欺は、企業経営にとって脅威

SNSを通じた詐欺は、投資詐欺に限らず、恋愛感情を利用したロマンス詐欺や闇バイトの勧誘、ビジネスメール詐欺(BEC:企業の取引先や自社の経営者になりすまして偽のビジネスメールを送信し、金銭をだまし取る)、企業のアカウントの乗っ取りによる情報漏洩や金銭的損失など、形を変えて広がっています。これらは企業の信用や業務にも影響を及ぼす可能性があり、もはや個人だけの問題ではなくなってきました。

企業としては、SNS利用に関するガイドラインの策定や従業員へのリテラシー教育、アカウントのセキュリティ強化(多要素認証やパスワード管理の徹底)など、日常的に企業全体で意識していくことが重要です。

また、従業員一人ひとりが情報保護への意識を持ち、業務上不要な個人情報の収集を控えることも、リスク低減に有効です。こうした被害から企業と従業員を守るために、新たな制度や技術の導入など、企業としてできることから対策を講じていくことが、リスク回避への第一歩となるのではないのでしょうか。

## 警察庁特殊詐欺対策ページ

<https://www.npa.go.jp/bureau/safetylife/sos47/>