2026 年 5 月 14 日
BBSS 株式会社

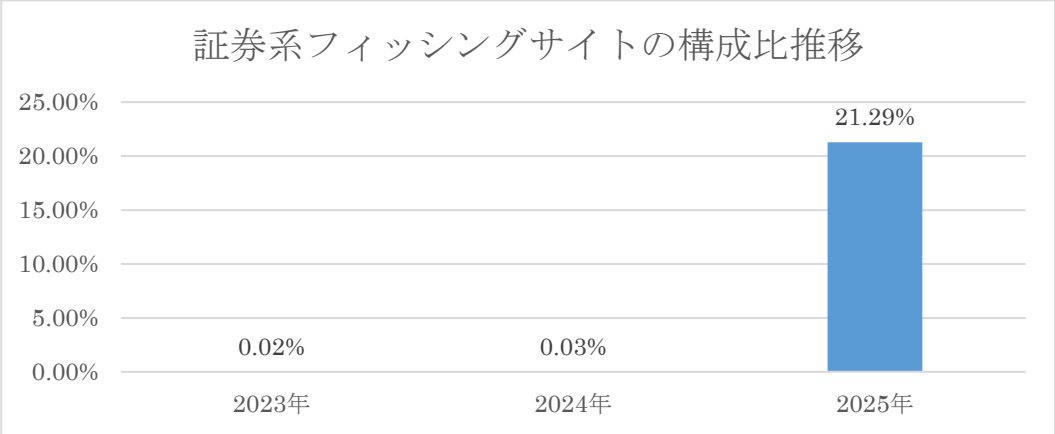
ネット詐欺リポート 2025 年
証券系フィッシングが前年比約 960 倍に増加

ネット詐欺リポートは毎月調査・収集した詐欺サイトを分析し、傾向をまとめたリポートです。本リポートは、2025 年 1 月～12 月のネット詐欺リポートの傾向をまとめた年間版です。

目次：

■2025 年は証券系フィッシングが急増、前年比約 960 倍に、不正取引被害は 7000 億円以上

2025 年は、証券会社を狙ったフィッシングサイトが大幅に増加し、前年比で約 960 倍に達しました。背景には、2024 年 1 月に開始された新 NISA により証券口座を開設する人が増加したことがあり、口座保有者を狙った攻撃が活発化した可能性があります。



主な被害の手口としては、アカウントを乗っ取られた後に保有株式を売却され、その資金で海外株式を購入されるケースが確認されています。金融庁によると不正取引の総額は 7,000 億円以上にのぼります。

また、多くの証券会社で導入されている二要素認証を悪用した「リアルタイムフィッシング」の手口も確認されています。これは「認証コードを入力してください」といった画面表示でユーザーに認証コードを入力させ、そのコードを犯人がリアルタイムで正規サイトに入力することでログインを完了させる手口です。

特に SBI 証券やマネックス証券を装ったフィッシングサイトの増加が目立っていますが、ほぼすべての証券会社が標的となっています。

SBI 証券のフィッシングサイト

マネックス証券のフィッシングサイト

※画像は詐欺・危険サイトのイメージであり、本文内容とは関係ありません。

■インターネット詐欺の手口は偽販売・違法販売が 8 割以上

インターネット詐欺の手口の中では、偽販売サイトが 8 割以上を占めています。

これらのサイトでは「商品が届かない」「粗悪品が送られてくる」「個人情報を詐取される」といった被害に遭う可能性があります。ブランド品から日用品まで、さまざまな商品を対象に偽販売サイトが作成されています。

また、フィッシング詐欺の構成比は減少しているものの、証券会社を装ったフィッシングサイトの増加に伴い、報告件数は実数ベースで前年比 60%以上増加しています。

	2023年	2024年	2025年
フィッシング	22.80%	20.77%	17.69%
偽販売違法販売	62.48%	75.74%	80.86%
ワンクリック詐欺/不当請求	0.00%	0.00%	0.01%
Web改ざん	0.00%	0.00%	0.00%
公文書違反	0.00%	0.00%	0.00%
著作権侵害	0.05%	0.14%	0.06%
違法行為	0.00%	0.02%	0.00%
不正サイト	0.01%	0.22%	0.50%
アダルトサイト	0.00%	0.00%	0.00%
偽警告サイト	1.01%	3.04%	0.85%
偽ブランド販売	0.03%	0.03%	0.03%

■2025 年フィッシング詐欺カテゴリ

フィッシング詐欺のカテゴリ別では、「Web サービス」が 26%で最多となりました。

具体的には、Apple ID を狙う手口や、東京電力（TEPCO）や ETC 利用照会サービスを装い、ログイ

ン情報を詐取するケースが報告されています。
次いで、クレジットカードが 2 位となり、三井住友カードや楽天カードなどのブランドを装ったフィッシングサイトが多数確認されました。
また、3 位は証券分野で、前年度から大きく増加しています。

	2023年	2024年	2025年
銀行	21.65%	14.49%	8.23%
携帯キャリア	14.54%	10.44%	1.55%
クラウドサービス	1.62%	0.13%	0.00%
消費者金融/キャッシング	0.00%	0.77%	0.18%
クレジットカード／ファイナンス	20.28%	31.51%	25.09%
出会い系	0.00%	0.02%	0.03%
ECサイト	7.91%	15.32%	9.30%
ギャンブル	0.00%	0.00%	0.00%
オンラインゲーム	0.04%	0.01%	0.40%
違法広告	0.00%	0.00%	0.00%
フィッシングリンク	0.22%	0.00%	0.00%
ポータルサイト	0.19%	0.24%	0.04%
プロバイダ	1.16%	1.43%	1.51%
官公庁	16.05%	2.56%	4.74%
株／証券	0.02%	0.03%	21.29%
SNS	0.29%	0.72%	0.51%
仮想通貨	0.06%	0.08%	0.08%
Webメール	0.06%	0.03%	0.06%
Webメールユーザ	0.00%	0.00%	0.00%
Webサービス	15.49%	22.08%	26.23%
その他	0.43%	0.14%	0.77%

■2025 年フィッシングサイトブランドランキング

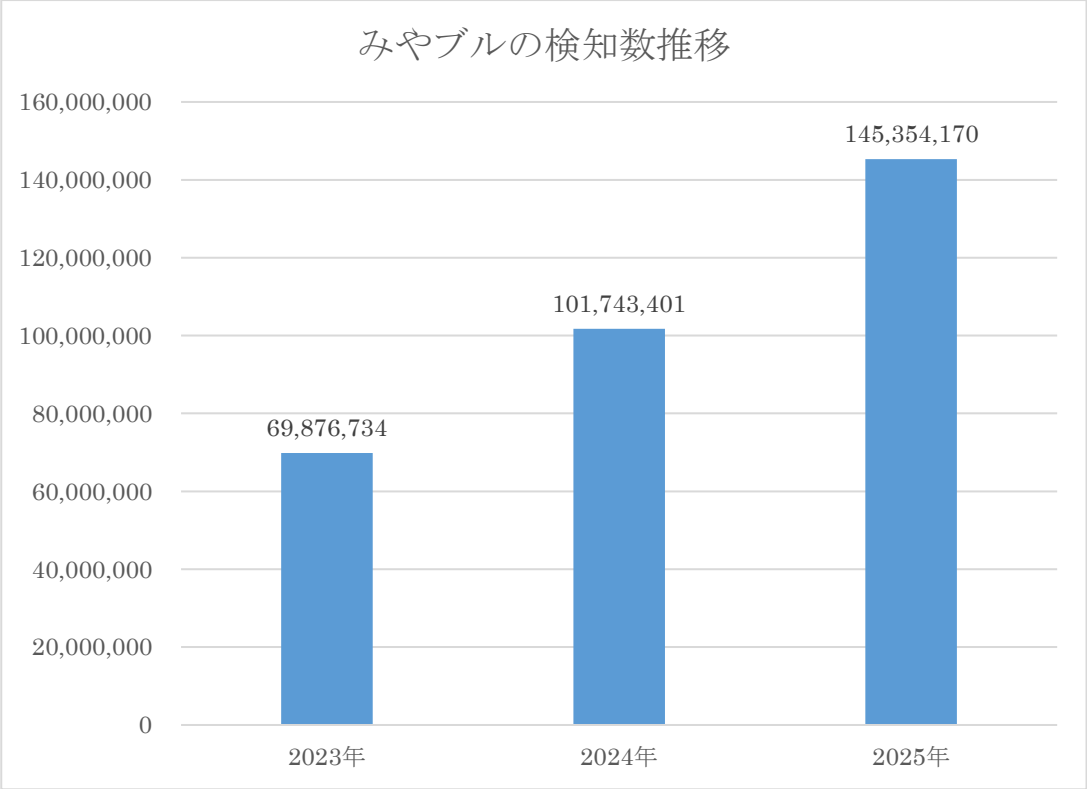
2025 年は、利用者の多い Apple ID を狙ったフィッシングが 1 位となりました。 Apple 関連のフィッシングは従来から継続的に確認されており、引き続き主要な標的となっています。
また、証券会社を装ったフィッシングも増加しており、ランキングでは 2 位に SBI 証券、5 位にマネックス証券が入っています。6 位の国税庁を装ったフィッシングについては、確定申告の時期に合わせて増加する傾向が見られます。
銀行を装ったフィッシングでは、これまで中心だった大手銀行に加え、JA バンクやゆうちょ銀行、地方銀行などへターゲットが広がる傾向も確認されています。また 2025 年は国勢調査の実施に伴い、国勢調査を装ったフィッシングサイトも出現しました。このように社会的なイベントに合わせてばらまかれるフィッシングに注意が必要です。

2023年		2024年		2025年	
イオン銀行	19.2%	三菱UFJ銀行	9.98%	Apple	11.47%
SoftBank	11.6%	三井住友カード	8.38%	SBI証券	9.17%
三井住友カード	7.4%	イオンカード	8.09%	Amazon	7.81%
Amazon	6.6%	Amazon	7.83%	三井住友カード	6.73%
国税庁	5.3%	Apple	7.80%	マネックス証券	5.71%
SAISON CARD	5.2%	SoftBank	7.02%	国税庁	3.97%
えきねっと	4.5%	メルカリ	6.67%	JCB	3.48%
日本年金機構	4.1%	えきねっと	6.00%	JAバンク	3.42%
ETC利用照会サービス	3.3%	SAISON CARD	4.42%	TEPCO	3.18%
エポスカード	3.3%	TEPCO	3.86%	ヤマト運輸	2.76%

■みやブル（旧詐欺ウォール）の検知数の推移

2025 年にネット詐欺対策ソフト「みやブル（旧詐欺ウォール）」が検知した詐欺・不正サイトは 145,354,170 件で、前年比で 43%増加しました。

特に違法アップロードサイトや偽販売サイトなどの検知が上昇しています。2026 年も同様の傾向が続く可能性があり、引き続き注意が必要です。



■2025 年まとめ

フィッシング詐欺は、メールの文面の自然さが向上し 、不自然な日本語や文法の違和感が少なくなっています。背景には、生成 AI の活用が進んでいる可能性も指摘されており、本物との見分けがより難しくなっています。

またフィッシングサイトには「偽の認証画面※1」が表示されるケースもあり、ユーザーが正規サイトと誤

認してしまうリスクが高まっています。
ネット詐欺は手口が複雑化しており、ID やパスワードの窃取だけでなく、「LINE へ誘導する」、「偽のサポートを装って電話をかけさせる」など複数の手法を組み合わせるケースが増えています。
加えて、首相の名前を利用した投資詐欺や、警察・検察を装って連絡させ金銭をだまし取る詐欺など、多様な手口も確認されています。

2026 年は、より人間の心理につけ込むネット詐欺が増えると考えられます。
特に注意すべきなのは、「すぐにログイン」「すぐに連絡」「すぐに支払い」といった緊急性を強調する内容です。こうした手口は、利用者を焦らせ冷静な判断を妨げることを目的としています。そのため「正規サイトで詐欺の手口を確認する」「公式サポートに連絡してメールの内容を確認する」など、必ず一度立ち止まり確認することが被害防止につながります。

※1 偽認証

※画像は詐欺・危険サイトのイメージであり、本文内容とは関係ありません。

■フィッシング詐欺被害防止のポイント

1. メールや SMS で案内された URL が正規の URL か確認する
   メールや SMS メッセージ上のリンクはクリックせず、事前に登録しておいたブックマークやウェブ検索で正規サイトへアクセスしましょう。 怪しいサイトを診断する無料サービスを利用し、事前に URL をチェックすることも有効です。

2. 個人情報やクレジットカード番号の入力を促すメール・SMS に注意する
   クレジットカード会社などでは、個人情報やクレジットカード情報などについてメール・SMS での問い合わせは行っていないため、情報入力させるページに誘導するメールには細心の注意を払いましょう。

3. ログイン ID・パスワードの使い回しを控える

複数のサービスサイトで同じログイン ID・パスワードを使い回していると、フィッシング詐欺によってログイン ID・パスワードが詐取された場合、他のサービスサイトの不正利用被害に遭う可能性が高まります。被害を最小限に抑えるためにもログイン ID・パスワードの使い回しはせず、サービスごとに登録内容を変更し管理を行うようにしましょう。

4. セキュリティソフトやネット詐欺対策ソフトを導入する
   犯罪者の手口は日々巧妙化しており、今まで意識してきた対策が通用しなくなる可能性があります。日々進化するネット犯罪に対抗するにはセキュリティソフトを導入することも必要です。不審なサイトにアクセスした際に注意喚起を行ってくれます。

■詐欺サイトを無料で診断「詐欺サイトチェッカー」

不審なサイトの安全性を確認したい場合は、無料で利用できる「詐欺サイトチェッカー」 を活用する方法もあります。

ネット詐欺対策ソフトの「みやブル」及び官公庁などから収集したブラックリストの情報をもとに判定を行うもので、気になるサイトの URL がネット詐欺サイトとして報告されているかをチェックすることができます。

サイト URL:https://checker.miyabull.jp/

■森 達哉教授のコメント

2025 年最大の特徴である証券系フィッシングの急増は、2024 年の新 NISA 開始をきっかけに急拡大した新規口座を計画的に標的にしたものと考えられます。フィッシングを足がかりとして、アカウント乗っ取り後に保有株式を売却し海外株式の購入に充てる多段階攻撃へと進化した点は、特に注視が必要です。一方で、2026 年に入ってからは証券系フィッシング全体が昨年のピーク比 7 分の 1 以下まで減少しており（2 月度リポートご参照）、パスキー（FIDO2）導入や多要素認証必須化といった業界横断の対策が効果を発揮し始めていることもまた、本年の重要な変化と言えます。

過去 1 年のデータを俯瞰すると、攻撃者の標的選定は「権威性（公式らしさ）」「生活必需性（誰もが使うサービス）」「時節性（社会的関心が高まるタイミング）」の三軸の掛け合わせで読み解けます。Apple ID（iPhone など Apple 社製品)は「生活必需性」、銀行・証券は「権威性」と「生活必需性」、国税庁、国勢調査、首相官邸、警察検察を装う詐欺は「時節性」と「権威性」の組み合わせと、いず

れの事例もこうした枠組みで説明可能です。さらに生成 AI による文面の自然化や、LINE 誘導、偽サポート電話との複合化と相まって、「日本語の不自然さで見抜く」という従来の防御指針はもはや有効でない段階に入ったと考えるべきでしょう。

2026 年は、こうした三つの観点を組み合わせた手口がさらに巧妙化し、季節や社会的イベントに合わせて標的を切り替えるキャンペーンが続くと見込まれます。利用者側の備えとしては、メールや SMS のリンクは決してクリックせず、必ず公式アプリやブックマークから正規サイトへアクセスすること、そして「至急」「未払い」「本人確認」といった緊急性を強調する文言を見たときほど、一拍置いて公式窓口に確認することの二点に尽きます。本リポートの内容をご家族や周囲の方々と共有し、攻撃者の手口に先んじて備えていただければと思います。

■監修者プロフィール

森 達哉
早稲田大学 理工学術院 教授
「令和 7 年度科学技術分野の文部科学大臣表彰 科学技術賞（研究部門）」受賞
NICT サイバーセキュリティ研究所 招へい専門員

＜会社概要＞

社名　　：BBSS 株式会社
所在地　：東京都港区海岸 1 丁目 7 番 1 号 WeWork 東京ポートシティ竹芝
代表者　：代表取締役社長 兼 CEO　本多 晋弥
設立日　：2006 年 1 月 17 日
株主　　：SB C&S 株式会社　100%
事業内容：コンシューマ向けソフトウエア、および IoT サービスの企画・開発・提供、法人向けライセンス販売
URL　　：https://www.bbss.co.jp/