Research report

Online Fraud and Scams in Japan

Safer Internet Lab

ONLINE FRAUD AND SCAMS IN JAPAN

Safer Internet Lab

A Research Report by Safer Internet Lab

The views expressed here are solely those of the author(s) and do not represent an official position of SAIL, CSIS, Google, or any other organization. Please contact the author(s) directly with any comments or questions.

Online Fraud and Scams in Japan

Daichi Ishii[15]

PATTERNS & TRENDS

From 2024 into 2025, both the incidence and the monetary losses of online fraud in Japan have reached record highs. Provisional statistics released by the National Police Agency show that total losses from “special fraud” in 2024 amounted to ¥ 721.5 billion, a year-on-year increase of 59.4 percent, while recognized cases rose to 20,987; there is still no sign of decline as 2025 unfolds (National Police Agency 2025a).

Among these crimes, “SNS-based investment and romance scams,” in which perpetrators impersonate celebrities on social media and promise high returns, accounted for 9,265 cases and ¥ 114.1 billion between January and November 2024, making them the chief driver of the overall surge (Itakura 2025). The same scam type has continued at pace in 2025: losses in March alone reached ¥ 5.53 billion, up ¥ 2.37 billion from the previous month and sharply reversing the decline seen through February (National Police Agency 2025a).

According to the Anti-Phishing Council Japan, 2023 set an all-time record with 1.19 million reported phishing incidents; in 2024 the monthly total has repeatedly exceeded 180,000, indicating a persistent upward trend (Anti-Phishing Council 2024).

The contact channels used by scammers have shifted dramatically. In 2023 roughly half of investment scams began via banner advertisements, but after mass takedowns by platforms, scams initiated through direct messages (DMs) overtook ad-based fraud from July 2024 onward. Matching apps, Instagram, and Facebook now rank as the top three channels through which victims are approached (National Police Agency 2024a). Because DMs draw victims into semi-closed spaces that are harder to monitor, this channel shift is cited as a cause of soaring losses.

Real-world cases confirm the escalating damage. In Ibaraki Prefecture, a woman in her seventies who was lured through a LINE group transferred ¥ 809 million in just a few weeks (Furusho & Tokonami 2024). In Hokkaido, a man in his seventies lost ¥ 240 million after being deceived by a DM from someone posing as a “famous analyst” (NHK 2024).

Generative-AI tools are making attacks more sophisticated. A McAfee risk survey found that deep-fake images and names of influential Japanese figures such as Fusaho Izumi (a Japanese politician) and Takafumi Horie (a Japanese famous entrepreneur) are being widely reused, and it concludes that Japanese users’ high level of trust in local celebrities amplifies scam persuasiveness (McAfee 2024). Scammers have already been detected playing synthetic voices of famous investors during LINE calls to coax victims into investing, bringing “personal appearances” generated by AI into the real world (Kansai Television 2024).

The victim profile is changing as well. Whereas people aged 65 and over once comprised the vast majority, men in their fifties now account for 29 percent of SNS investment-scam victims, followed by those in their sixties at 27 percent; being defrauded is no longer limited to the elderly (National Police Agency 2024a). Geographically, roughly 65 percent of losses are concentrated in seven prefectures—

[15] Research Consultant, Safer Internet Lab

including Tokyo, Kanagawa, and Osaka—highlighting the vulnerability of major metropolitan areas (National Police Agency 2025b).

Taken together, Japan's online-fraud landscape is defined by four overarching trends:

1. Record-high total and per-case losses
2. A shift toward closed contact channels
3. Greater technical sophistication enabled by generative AI
4. An expanding age range of victims

PATTERNS & TRENDS

Although Japan has rolled out a variety of regulations and administrative measures to address online fraud, the growth in both losses and prosecutions continues to outpace legislation and policy implementation.

In April 2024, the Ministry of Economy, Trade and Industry (METI) and the Ministry of Internal Affairs and Communications (MIC) issued *AI Service Provider Guidelines 1.0*, positioning deep-fake risk management at each stage of development, provision, and use (Ministry of Economy, Trade and Industry and Ministry of Internal Affairs and Communications 2024). An AI Bill subsequently cleared the House of Representatives on 24 April 2025, establishing a framework that allows the government to request investigative cooperation from service providers when serious incidents occur and—via an accompanying resolution—assigns explicit state responsibility for countering deep-fake pornography (Murai 2025).

The government also adopted a *Comprehensive Strategy to Protect Citizens from Fraud* in June 2024, designating SNS-based investment scams as a top-priority offense and allocating an extra ￥650 million in the supplementary budget (Prime Minister's Office 2024). According to National Police Agency statistics, 232 SNS investment-and-romance scams were prosecuted and roughly 1,000 related bank accounts were frozen during 2024 (National Police Agency 2025b). The Financial Services Agency (FSA) has opened a *Fraudulent Investment Consultation Dial*, although detailed call statistics have yet to be released.

As an anti-phishing measure against spoofed government websites, the Digital Agency is designing a new authenticity icon for public-sector sites, with pilot deployment targeted in fiscal-year 2025 (Digital Agency 2025a).

Some local governments are taking their own initiatives. Tottori Prefecture enacted an ordinance effective 1 April 2025 that bans the creation, distribution, or provision of AI-generated pornographic images using real children's faces; violations carry penalties of up to one year's imprisonment or a fine of up to ￥500,000 (Tottori Prefecture 2025).

International collaboration is also advancing. At the minister-level UK–Japan Digital Partnership meeting in January 2025, the two countries agreed to co-develop deep-fake verification benchmarks between their respective AI Safety Institutes (Digital Agency 2025b). Japan likewise joined the United States, Australia, and six other countries in co-signing an international advisory that explicitly named the China-linked hacker group APT40, strengthening information-sharing on cryptocurrency-based money-laundering techniques (National Police Agency 2024b).

Even so, these efforts alone cannot fully address the rapid evolution of generative-AI-enabled fraud and the anonymity of cross-border transfers via crypto-assets. Agile regulation that keeps pace with technological advances, together with real-time mechanisms for tracking damage, remains essential.

PRIVATE-SECTOR INITIATIVES

Major platforms are likewise strengthening their defenses against online fraud. In July 2024, Meta further disclosed a pilot program for the Japanese market that withholds ad revenue for 90 days and refunds it to victims; during that pilot the company disabled the same **5.27 million** scam ads and **5,400** accounts between 5 March and 1 June 2024 (Meta 2024). **LINE Yahoo** has launched a cross-functional project that flags unverified accounts and tightens ad screening, outlining the measures on its corporate blog (LY Corporation 2025).

The trend is not confined to Japan. Google's **"Ads Safety Report 2024"** states that the company permanently terminated **more than 700,000** malicious advertiser accounts worldwide and cut reports of celebrity deep-fake ads by **90 percent** year on year (Google 2024).

On the financial-infrastructure side, the **Japanese Bankers Association** put a **fund-transfer-freeze API** into operation in October 2024, enabling real-time blocks through bank–police cooperation. In the crypto-asset arena, the industry body **JVCEA** is preparing to introduce **real-time KYT (Know Your Transaction)**, with joint investigation of suspicious transfers emerging as a key challenge (Chainalysis 2025).

Prominent individuals are also pushing back: billionaire **Yusaku Maezawa** (a Japanese famous entrepreneur) and others have announced plans to sue Meta, marking new cases in which celebrities exploited in scams take legal action (Toyo Keizai Online 2024).

Yet, as noted earlier, fraud now originates not only from banner ads but increasingly from **direct messages**. Capturing the full picture of these harder-to-see schemes will be a critical challenge going forward.

RECOMMENDATIONS

To shift Japan's response to online fraud from *after-the-fact crackdowns* to *anticipatory prevention*, three pillars should be advanced in parallel.

Pillar 1 – Stronger platform duties and built-in advanced detection

Platforms could be required to auto-forward metadata on suspected scam DMs to the National Police Agency's special task force. In cooperation with the entertainers' guild, a **"celebrity-image whitelist"**—authentic photos hashed to boost AI-based verification—could further raise detection accuracy. On the user side, the moment an ad or DM triggers a fraud signal, platforms could display "typical scam phrases" and real-time loss statistics, delivering behavioral-science-based warnings that stop victims before they act.

Pillar 2 – Open, API-linked data infrastructure

An infrastructure that continuously links public- and private-sector data via APIs and shows it in a public dashboard is worth considering. For example, the Digital Agency might host a weekly-updated dashboard of KPIs—loss amounts, case counts, ad takedowns—pulled from the National Police Agency, Financial Services Agency, and major platforms, while supplying reusable APIs for researchers and journalists.

Pillar 3 – Education

Although the payoff is long-term, bolstering educational initiatives is essential for raising society-wide resilience. Programs that let students *experience* AI-powered scam scenarios through hands-on learning could be one promising approach.

Interlocking these multilayered measures would position Japan to build one of the world’s strongest defense nets against “AI-era” fraud. A concerted effort by government, industry, and academia is now called for, ensuring that the next generation can enjoy digital life in safety.

REFERENCES

Anti-Phishing Council Japan. 2024. 「フィッシングレポート2024」. https://www.antiphishing.jp/report/phishing_report_2024.pdf

Chainalysis. 2024. 「日本における暗号資産のマネーロンダリング: 日本の視点から見たグローバルの共通問題」. https://www.chainalysis.com/blog/crypto-money-laundering-japan-japanese/.

Chainalysis. 2025. 「2024年の暗号資産詐欺: 詐欺産業がAIを活用し巧妙化する中、ロマンス詐欺は前年比でほぼ40 %増加」. https://www.chainalysis.com/blog/2024-pig-butchering-scam-revenue-grows-yoy-japanese/.

Digital Agency. 2025a. 「公的サイトの真正性確認に関する新アイコン導入方針」. https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5ecac8cc-50f1-4168-b989-2bcaabffe870/8b045435/20250315_auth_icon.pdf.

Digital Agency. 2025b. 「第3回日英デジタルパートナーシップ政務級会合の結果」. https://www.digital.go.jp/news/02d07f5c-0301-48ba-9150-7119457195f8.

Financial Services Agency. 2024. 「『詐欺的な投資に関する相談ダイヤル』の開設について」. https://www.fsa.go.jp/news/r5/sonota/20240619/toshisagi.html.

Financial Services Agency. 2025. 「暗号資産に関連する制度のあり方等の検証」. https://www.fsa.go.jp/news/r6/sonota/20250410_2/crypto_dp.html.

Furusho, Noboru, and Koichi Tokonami. 2025. 「SNS型詐欺など昨年の被害額は年比2倍超に　被害は若者にも拡大」. *Asahi Shimbun Digital*. https://www.asahi.com/articles/AST1P45P7T1PUJHB001M.html.

Google. 2025. “2024 Ads Safety Report.” https://services.google.com/fh/files/misc/ads_safety_report_2024.pdf.

Itakura, Daichi. 2025. 「特殊詐欺とSNS型投資・ロマンス詐欺　被害は2千億円、過去最悪」. *Asahi Shimbun Digital*. https://www.asahi.com/articles/AST253Q7TT25UTIL01NM.html.

Kansai Television. 2024. 「AIを使ったフェイク動画・音声で　堀江貴文氏かたる投資勧誘　SNS投資被害で5260万円被害」. https://www.ktv.jp/news/feature/240415/.

LY Corporation. 2025. 「『LINE』における詐欺行為の撲滅に向けた取り組み」. https://www.lycorp.co.jp/ja/story/20250331/snsscam.html. https://www.lycorp.co.jp/ja/story/20250404/snsscam2.html

McAfee. 2024. 「マカフィー、『2024年オンライン詐欺で悪用されやすい日本の著名人TOP10』を発表」. https://www.mcafee.com/ja-jp/consumer-corporate/newsroom/press-releases/2024/20241024.html.

Meta. 2024. 「詐欺広告に対する取り組み強化について」. https://about.fb.com/ja/news/2024/07/updates_on_tackling_scams/.

Ministry of Economy, Trade and Industry. 2025. 「2024年度 デジタルプラットフォームの透明性に関する評価報告書」. https://www.meti.go.jp/policy/mono_info_service/digitalplatform/evaluation.html.

Ministry of Economy, Trade and Industry and Ministry of Internal Affairs and Communications. 2024. 「AI事業者ガイドライン（第1.0版）」. https://www.meti.go.jp/press/2024/04/20240419004/20240419004.html.

Murai, Naoko. 2025. 「AI法案が衆院可決　付帯決議でディープフェイクポルノ対策求める」. *Asahi Shimbun Digital*. https://www.asahi.com/articles/AST4S1GLCT4SULFA009M.html.

National Consumer Affairs Center of Japan. 2024. 「SNSをきっかけとして…勧誘される金融商品・サービスの消費者トラブルが急増」. https://www.kokusen.go.jp/pdf/n-20240529_1.pdf.

National Police Agency. 2024a. 「令和6年11月末におけるSNS型投資・ロマンス詐欺の認知・検挙状況等について」. https://www.npa.go.jp/bureau/criminal/souni/sns-romance/sns-touroma2024.pdf.

National Police Agency. 2024b. 「豪州主導のAPT40グループに関する国際アドバイザリーへの共同署名について」. https://www.npa.go.jp/bureau/cyber/koho/caution/caution20240709.html.

National Police Agency. 2025a. 「令和7年3月末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」. https://www.npa.go.jp/bureau/safetylife/sos47/new-topics/250428/02.html.

National Police Agency. 2025b. 「令和６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（暫定値版）」. https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/hurikomesagi_toukei2024.pdf.

NHK (Japan Broadcasting Corporation). 2024. 「SNS投資詐欺で2億4 000万円余の被害 道内被害で最高額」. https://www3.nhk.or.jp/sapporo-news/20241204/7000071781.html.

Nozomi Sogo Law Office. 2023. 「改正電気通信事業法による外部送信規律（日本版Cookie規制）」. https://www.nozomisogo.gr.jp/newsletter/9660.

Prime Minister’s Office. 2024. 「国民を詐欺から守るための総合対策2.0」. https://www.kantei.go.jp/jp/singi/hanzai/kettei/250422/honbun-1.pdf.

Shinya, Chifumi. 2024. 「『株投資の勉強会』と誘導され2億円超の詐欺　利益18億円が一転」. *Asahi Shimbun Digital*. https://www.asahi.com/articles/ASSD42S8XSD4IIPE00HM.html.

Tottori Prefecture. 2025. 「知事定例記者会見（2025年1月14日）」. https://www.pref.tottori.lg.jp/320891.htm.

Toyo Keizai Online. 2024. 「Facebookで『詐欺広告』が放置され続ける真因」. https://toyokeizai.net/articles/-/750379.

Safer Internet Lab

saferinternetlab.org

Jl. Tanah Abang III no 23-27
Gambir, Jakarta Pusat. 10160

Find Us On

CSIS Indonesia | Safer Internet Lab