セキュリティ運用サービス月次レポート
2025年2月

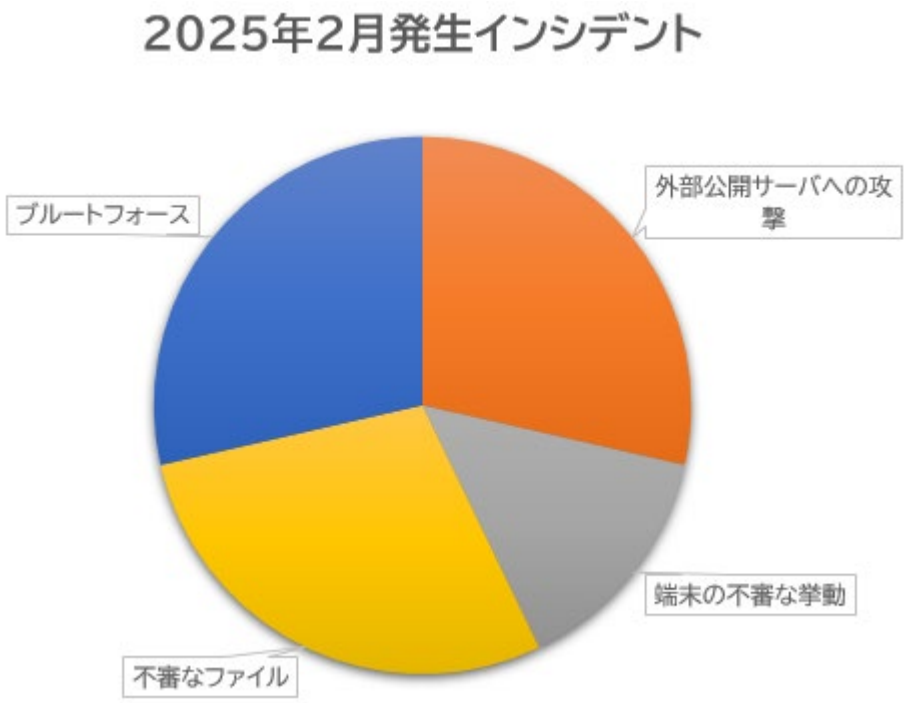
２０２５年３月２４日

ＮＥＣネッツエスアイ株式会社

目次

1. サイバー攻撃検知状況

当社SOCにおいて2025年2月は以下のような種類のインシデントが発生しました。



当月は取り上げるような目新しいインシデントはありませんでした。

2.脆弱性情報

米国CISA(サイバーセキュリティー・インフラセキュリティー庁)が公開しているKEV(悪用が確認されている脆弱性一覧)から2025年2月に追加されたものを抽出しました。
JPCERT/CC等の日本国内組織からも注意喚起されている脆弱性は赤文字としています。

脆弱性番号	ベンダー	製品	脆弱性名称
CVE-2025-0411	7-Zip	7-Zip	7-Zip Mark of the Web Bypass Vulnerability
CVE-2017-3066	Adobe	ColdFusion	Adobe ColdFusion Deserialization Vulnerability
CVE-2024-45195	Apache	OFBiz	Apache OFBiz Forced Browsing Vulnerability
CVE-2025-24200	Apple	iOS and iPadOS	Apple iOS and iPadOS Incorrect Authorization Vulnerability
CVE-2024-53104	Linux	Kernel	Linux Kernel Out-of-Bounds Write Vulnerability
CVE-2024-49035	Microsoft	Partner Center	Microsoft Partner Center Improper Access Control Vulnerability
CVE-2025-24989	Microsoft	Power Pages	Microsoft Power Pages Improper Access Control Vulnerability
CVE-2025-21418	Microsoft	Windows	Microsoft Windows Ancillary Function Driver for WinSock Heap-Based Buffer Overflow Vulnerability
CVE-2025-21391	Microsoft	Windows	Microsoft Windows Storage Link Following Vulnerability
CVE-2024-21413	Microsoft	Office Outlook	Microsoft Outlook Improper Input Validation Vulnerability
CVE-2024-29059	Microsoft	.NET Framework	Microsoft .NET Framework Information Disclosure Vulnerability
CVE-2025-0111	Palo Alto Networks	PAN-OS	Palo Alto Networks PAN-OS File Read Vulnerability
CVE-2025-0108	Palo Alto Networks	PAN-OS	Palo Alto Networks PAN-OS Authentication Bypass Vulnerability
CVE-2024-53704	SonicWall	SonicOS	SonicWall SonicOS SSLVPN Improper Authentication Vulnerability
CVE-2020-15069	Sophos	XG Firewall	Sophos XG Firewall Buffer Overflow Vulnerability
CVE-2020-29574	Sophos	CyberoamOS	CyberoamOS (CROS) SQL Injection Vulnerability

JPCERT等から注意喚起は出ていませんが、PAN-OSの脆弱性CVE-2025-0108は条件がそろうとルート権限が取得できる可能性があるため要注意です。
WebGUIを外部に公開していなければ攻撃を受けるリスクは低いものの、アップデートして対策する方が確実なためPalo Alto Networks社のNGFWを導入されている場合はアップデートをご検討ください。

3.サイバーセキュリティ関連ニュース

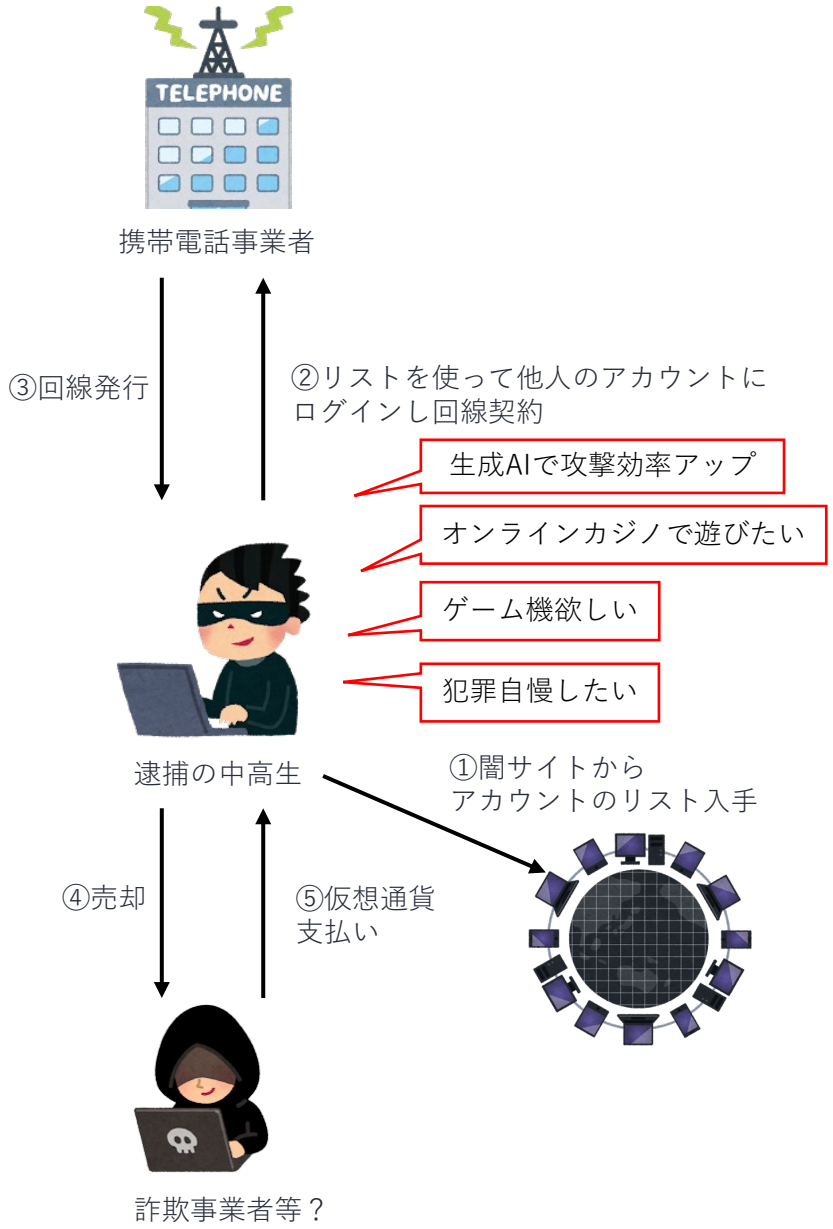
当月発生したサイバーセキュリティ関連のニュースから筆者が気になったものを紹介します。

生成AIを活用した不正アクセスで中高生逮捕

2025年2月27日、携帯電話事業者に対して不正アクセスを行い不正に回線契約を行ったとして中高生3人が逮捕されました。

高度なサイバー犯罪を3人の中高生が行っている点、生成AIを活用している点、闇バイトでも注目されていたオンラインカジノがここでも登場している点が印象的でした。
生成AIによって犯罪行為を実行するための知識や技術を補完できるようになって以降、サイバー犯罪の敷居が下がっているのかも知れません。

今回の事例の教訓として、多要素認証によって被害を軽減できていた可能性が高いため、外部からログイン可能なシステムがある場合は多要素認証必須化の検討などがあるかと思います。



4.公的機関のお知らせまとめ

公的機関が発するセキュリティ関連の注意喚起や定期レポートをまとめた一覧を示します。※筆者独自に取捨選択しています。

公表	タイトル	提供元	URL
2025/2/3	2025年サイバーセキュリティ月間特集ページを公開しました	情報処理推進機構（IPA）	https://www.ipa.go.jp/security/seminar/cybersecurity-month.html
2025/2/4	DDoS攻撃への対策について	JPCERT/CC	https://www.nisc.go.jp/pdf/news/press/20250204_ddos.pdf
2025/2/6	DeepSeek等の生成AIの業務利用に関する注意喚起	デジタル庁	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/d2a5bbd2-ae8f-450c-adaa-33979181d26a/e7bfeba7/20250206_councils_social-promotion-executive_outline_01.pdf
2025/2/7	重要電子計算機に対する不正な行為による被害の防止に関する法律案等が閣議決定されました	情報処理推進機構（IPA）	https://www.cas.go.jp/jp/houan/217.html
2025/2/12	JPCERT/CC Eyes「Ivanti Connect Secureの脆弱性を利用して設置されたマルウェアSPAWNCHIMERA」	JPCERT/CC	https://blogs.jpcert.or.jp/ja/2025/02/spawnchimera.html
2025/2/18	制御システムセキュリティカンファレンス 2025 講演資料を公開	JPCERT/CC	https://www.jpcert.or.jp/present/#year2025
2025/2/26	「コンピュータウイルス・不正アクセスの届出状況［2024年（1月～12月）］」を公開しました	情報処理推進機構（IPA）	https://www.ipa.go.jp/security/todokede/crack-virus/about.html#section19
2025/2/26	JPCERT/CC Eyes「JSAC2025 開催レポート～DAY 1～」	JPCERT/CC	https://blogs.jpcert.or.jp/ja/2025/02/jsac2025day1.html
2025/2/28	「情報セキュリティ10大脅威 2025」解説書を公開しました	情報処理推進機構（IPA）	https://www.ipa.go.jp/security/10threats/10threats2025.html
2025/2/28	JPCERT/CC インターネット定点観測レポート［2024年10月1日～2024年12月31日］	JPCERT/CC	https://www.jpcert.or.jp/tsubame/report/report202410-12.html
2025/2/28	JPCERT/CC Eyes「TSUBAMEレポート Overflow（2024年10～12月）」	JPCERT/CC	https://blogs.jpcert.or.jp/ja/2025/02/tsubame-overflow20241012.html

その他、今月は所謂「能動的サイバー防御」実現に向けた法案の提出も印象的でした。
現実問題としてどの程度実効性のあるアクションが取れるかは未知数ですが、少なくとも対応の根拠となる法案が整備される事は対策に向けて一歩前進だと思います。(趣旨に沿った運用がなされる事を祈ります・・・)

5.最後に

NECネッツエスアイではセキュリティ運用サービス（SOC）の他、Webアプリケーションファイアウォール、侵入防御システム、各種セキュリティ対策製品の導入支援や、お客様のシステム環境に最適な解決策のご提案を行うセキュリティコンサルティングサービスを提供しております。お問い合わせフォームからお気軽にご相談ください。

\Orchestrating a brighter world