セキュリティ運用サービス月次レポート
2025年3月

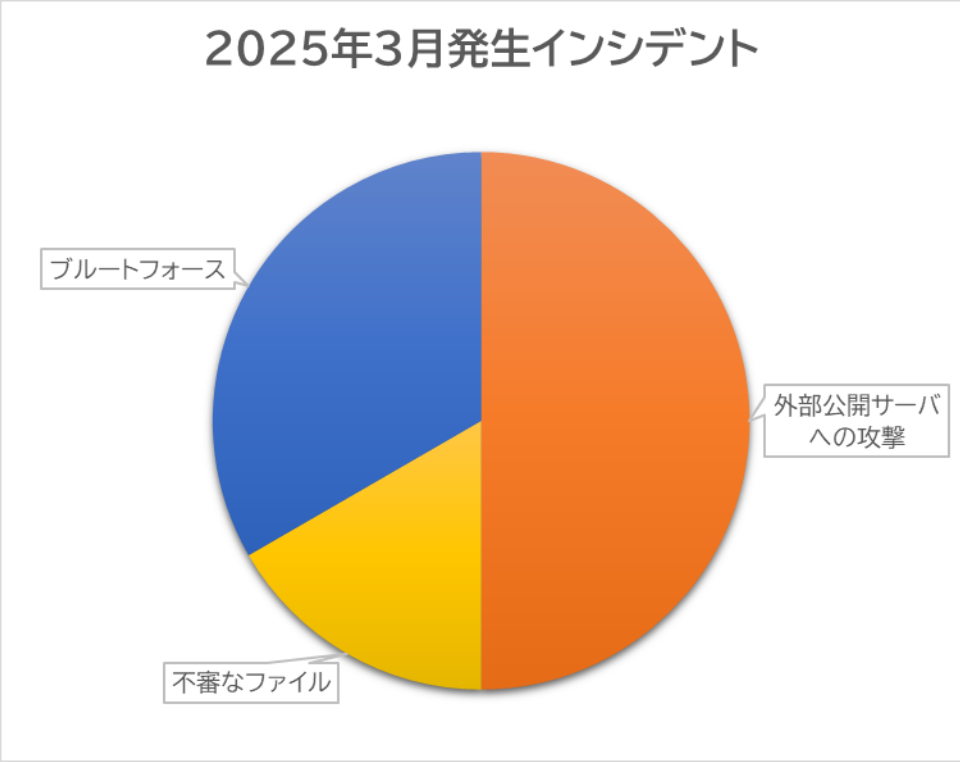
２０２５年４月１６日

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3月は以下のような種類のインシデントが発生しました。



・一部ユーザの外部公開サーバが、OpenVASやNessus等のツールを置用いたと思われる脆弱性調査を受けました。インターネットにサーバを公開する場合、このような通信は度々発生します。

・マルウェアの可能性があるファイルを検知しました。危険なマルウェアの可能性がある一方、アドウェア等脅威度の低い検体であったり過検知の可能性もあります。

・内部IP間の通信で発生した連続した認証失敗をブルートフォース攻撃として検知しました。実際の攻撃の可能性のほか、プロトコルによってはちょっとした設定ミスで発生する事もあります。

2.脆弱性情報

2025年3月にKEVに追加された脆弱性から日本国内で影響がありそうなものを抽出しました。
※米国CISAが公開している悪用確認済みの脆弱性一覧

脆弱性番号	ベンダー	製品	脆弱性名称
CVE-2025-24201	Apple	Multiple Products	Apple Multiple Products WebKit Out-of-Bounds Write Vulnerability
CVE-2025-24472	Fortinet	FortiOS and FortiProxy	Fortinet FortiOS and FortiProxy Authentication Bypass Vulnerability
CVE-2025-2783	Google	Chromium Mojo	Google Chromium Mojo Sandbox Escape Vulnerability
CVE-2022-43769	Hitachi Vantara	Pentaho Business Analytics (BA) Server	Hitachi Vantara Pentaho BA Server Special Element Injection Vulnerability
CVE-2022-43939	Hitachi Vantara	Pentaho Business Analytics (BA) Server	Hitachi Vantara Pentaho BA Server Authorization Bypass Vulnerability
CVE-2024-13161	Ivanti	Endpoint Manager (EPM)	Ivanti Endpoint Manager (EPM) Absolute Path Traversal Vulnerability
CVE-2024-13160	Ivanti	Endpoint Manager (EPM)	Ivanti Endpoint Manager (EPM) Absolute Path Traversal Vulnerability
CVE-2024-13159	Ivanti	Endpoint Manager (EPM)	Ivanti Endpoint Manager (EPM) Absolute Path Traversal Vulnerability
CVE-2025-21590	Juniper	Junos OS	Juniper Junos OS Improper Isolation or Compartmentalization Vulnerability
CVE-2024-50302	Linux	Kernel	Linux Kernel Use of Uninitialized Resource Vulnerability
CVE-2025-24993	Microsoft	Windows	Microsoft Windows NTFS Heap-Based Buffer Overflow Vulnerability
CVE-2025-24991	Microsoft	Windows	Microsoft Windows NTFS Out-Of-Bounds Read Vulnerability
CVE-2025-24985	Microsoft	Windows	Microsoft Windows Fast FAT File System Driver Integer Overflow Vulnerability
CVE-2025-24984	Microsoft	Windows	Microsoft Windows NTFS Information Disclosure Vulnerability
CVE-2025-24983	Microsoft	Windows	Microsoft Windows Win32k Use-After-Free Vulnerability
CVE-2025-26633	Microsoft	Windows	Microsoft Windows Management Console (MMC) Improper Neutralization Vulnerability
CVE-2018-8639	Microsoft	Windows	Microsoft Windows Win32k Improper Resource Shutdown or Release Vulnerability
CVE-2017-12637	SAP	NetWeaver	SAP NetWeaver Directory Traversal Vulnerability
CVE-2025-22226	VMware	ESXi, Workstation, and Fusion	VMware ESXi, Workstation, and Fusion Information Disclosure Vulnerability
CVE-2025-22225	VMware	ESXi	VMware ESXi Arbitrary Write Vulnerability
CVE-2025-22224	VMware	ESXi and Workstation	VMware ESXi and Workstation TOCTOU Race Condition Vulnerability

注目度の高い脆弱性は見受けられませんでした。

3.サイバーセキュリティ関連ニュース

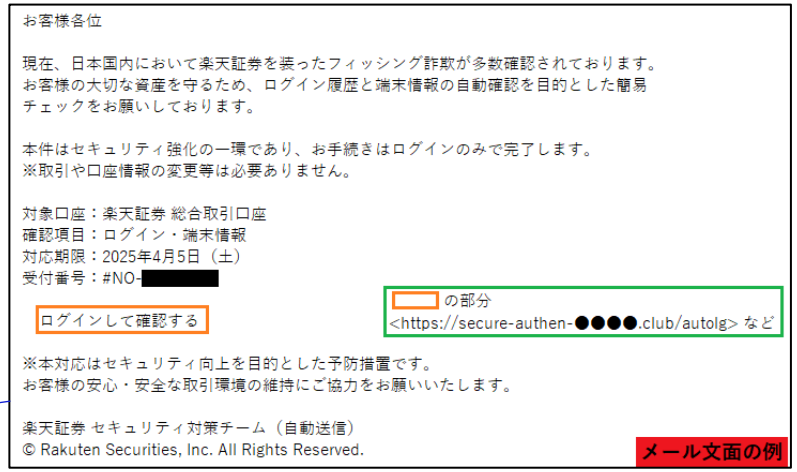
大手証券会社に対する不正アクセス

2025年3月下旬、大手証券会社の一部口座が不正アクセスを受け、特定の中国株の売買が行われた結果損失が発生したと話題になりました。
本件を受けて証券会社は、証券会社を騙るフィッシングメールに対する注意喚起を出しています。

本件について筆者は以下のような感想を持ちました。

- **攻撃者は何故か口座所有者の認証情報を持っている**
- **フィッシングメール起因の漏えいは一定数ありそう**
  →証券会社を騙るフィッシングメールが1月ごろから増えている
  →生成AIによりフィッシングメールのクオリティが上がっている
- **マルウェア起因の漏えい説は違和感ない**
  →24年後半から偽CAPTCHA等を使った**ClickFix**が増えており
  情報窃取系マルウェアの感染が増えている可能性がある
- **証券会社から漏えいした可能性は低い**
  →複数の証券会社が被害を訴えている
  →漏えいを疑う証拠は現状報告されていない

特にClickFixは既存の防御手段の多くを回避する比較的新しい攻撃手法です。
標的は組織・個人を問わないためご注意ください。


お客様各位

現在、日本国内において楽天証券を装ったフィッシング詐欺が多数確認されております。
お客様の大切な資産を守るため、ログイン履歴と端末情報の自動確認を目的とした簡易チェックをお願いしております。

本件はセキュリティ強化の一環であり、お手続きはログインのみで完了します。
※取引や口座情報の変更等は必要ありません。

対象口座：楽天証券 総合取引口座
確認項目：ログイン・端末情報
対応期限：2025年4月5日（土）
受付番号：#NO-[redacted]

ログインして確認する

[redacted] の部分
<https://secure-authen-●●●●.club/autolg> など

※本対応はセキュリティ向上を目的とした予防措置です。
お客様の安心・安全な取引環境の維持にご協力をお願いいたします。

楽天証券 セキュリティ対策チーム（自動送信）
© Rakuten Securities, Inc. All Rights Reserved.

メール文面の例

フィッシングメールの例（フィッシング対策協議会
楽天証券をかたるフィッシング（2025/04/01)より）

偽CAPTCHAによるClickFix攻撃画面

3.サイバーセキュリティ関連ニュース

一般的なClickFixの流れ

①Webサイト訪問すると突然右のような画面に遷移
※経験上海外のWebサイトで遭遇しやすい

Webサイトのイメージ(AI生成)

突然遷移

偽CAPTCHA

要約：
ページを参照するには以下を実行してください
1.Win+Rを押す
2.CTRL+V
3.Enter

②正規CAPTCHAと誤認して偽CAPTCHA指定の操作を実施

よくある正規CAPTCHAの例

③マルウェア感染
→ユーザ自らコマンド実行する形となりセキュリティ製品で検知しづらい
→SASEやブラウザで広告をブロックしたりEDRで不審なコマンド実行を検知してある程度対策可能
→当SOCでは情報窃取系マルウェアを検知するケースが多い

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
2025/3/5	JPCERT/CC Eyes「JSAC2025 開催レポート～DAY 2～」	情報処理推進機構（IPA）	https://blogs.jpcert.or.jp/ja/2025/03/jsac2025day2.html
2025/3/12	インターネットの安全・安心ハンドブック Ver5.10を公開しました	内閣サイバーセキュリティセンター	https://security-portal.nisc.go.jp/guidance/handbook.html
2025/3/12	JPCERT/CC Eyes「JSAC2025 開催レポート～Workshop & Lightning Talk～」	情報処理推進機構（IPA）	https://blogs.jpcert.or.jp/ja/2025/03/jsac2025-workshop-lightning-talk.html
2025/3/13	不正アクセス行為対策等の実態調査・アクセス制御機能に関する技術の研究開発の状況等に関する調査	警察庁	https://www.npa.go.jp/bureau/cyber/pdf/R6countermeasures.pdf
2025/3/13	サイバー警察局便りR6Vol.17「あなたの家のIoT機器が悪用されている!?」	警察庁	https://www.npa.go.jp/bureau/cyber/pdf/R6_Vol.17cpal.pdf
2025/3/24	サイバー警察局便りR6Vol.18「サイバー防犯ボランティア活動の推進」	警察庁	https://www.npa.go.jp/bureau/cyber/pdf/R6_Vol.18cpal.pdf
2025/3/24	JPCERT/CC Eyes「制御システムセキュリティカンファレンス2025 開催レポート」	情報処理推進機構（IPA）	https://blogs.jpcert.or.jp/ja/2025/03/ics-conference2025.html
2025/3/5	JPCERT/CC Eyes「JSAC2025 開催レポート～DAY 2～」	情報処理推進機構（IPA）	https://blogs.jpcert.or.jp/ja/2025/03/jsac2025day2.html

今月は、「インターネットの安全・安心ハンドブック」が2年ぶりにアップデートされました。
近年注目されている生成AIやサプライチェーン攻撃の内容が追加されているようです。
ページ数は多いものの攻撃手法や対策を読みやすくまとめてあるため、情報セキュリティ対策の参考資料として活用できるかと思います。

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