セキュリティ運用サービス月次レポート
2025年4月

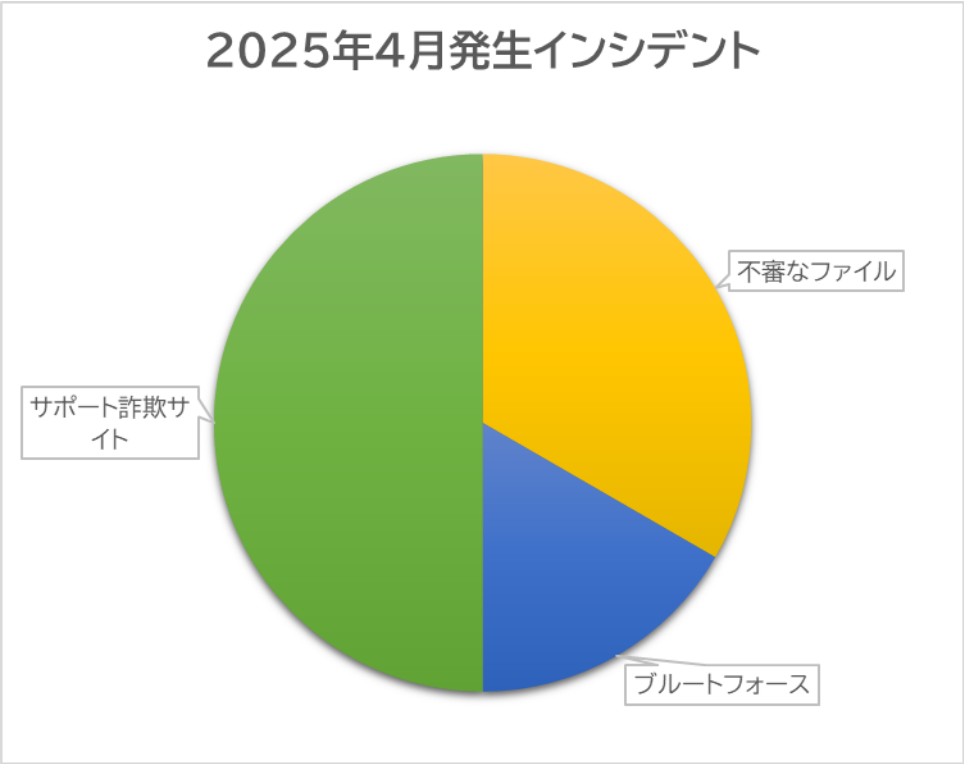
２０２５年５月２３日

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4月は以下のような種類のインシデントが発生しました。



・サポート詐欺サイト
ここ数年、サポート詐欺サイトによる被害は個人組織問わず度々被害が報道されており危険です。 SASE、プロキシ、UTM等で検知します。

・不審なファイル
ウイルス対策ソフトやUTMでマルウェアの可能性があるファイルを検知すると危険度判定のうえ通報を実施します。アドウェア等脅威度の低い検体であったり過検知のケースもよくあります。

・ブルートフォース
認証を繰り返すことでパスワードを特定しようとする攻撃(ブルートフォース)を検知、通報しています。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4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-2025-24813	Apache	Tomcat	Apache Tomcat Path Equivalence Vulnerability
CVE-2025-31201	Apple	Multiple Products	Apple Multiple Products Arbitrary Read and Write Vulnerability
CVE-2025-31200	Apple	Multiple Products	Apple Multiple Products Memory Corruption Vulnerability
CVE-2025-22457	Ivanti	Connect Secure, Policy Secure, and ZTA Gateways	Ivanti Connect Secure, Policy Secure, and ZTA Gateways Stack-Based Buffer Overflow Vulnerability
CVE-2024-53150	Linux	Kernel	Linux Kernel Out-of-Bounds Read Vulnerability
CVE-2024-53197	Linux	Kernel	Linux Kernel Out-of-Bounds Access Vulnerability
CVE-2025-29824	Microsoft	Windows	Microsoft Windows Common Log File System (CLFS) Driver Use-After-Free Vulnerability
CVE-2025-24054	Microsoft	Windows	Microsoft Windows NTLM Hash Disclosure Spoofing Vulnerability
CVE-2025-42599	Qualitia	Active! Mail	Qualitia Active! Mail Stack-Based Buffer Overflow Vulnerability
CVE-2025-31324	SAP	NetWeaver	SAP NetWeaver Unrestricted File Upload Vulnerability
CVE-2021-20035	SonicWall	SMA100 Appliances	SonicWall SMA100 Appliances OS Command Injection Vulnerability

CVE-2025-42599は、IIJ社メールセキュリティサービスの情報漏えい事故の原因となった脆弱性として特に日本国内で話題になりました。
その他、個人向け製品ではありますがASUS社製ルータにて日本国内でも被害が出ている脆弱性が公表されていますので次ページで紹介します。

2.脆弱性情報

Active! Mail 6のバッファオーバーフローの脆弱性

脆弱性番号	CVE-2025-42599
対象製品	Active! Mail 6
想定被害	Active! Mailにアクセスできる第三者が認証を回避して任意のコードを実行したりDoS攻撃できる
対象バージョン	6.60.05008561 以前のバージョン
対策	バージョンアップ
アドバイザリ	https://www.qualitia.com/jp/news/2025/04/18_1030.html
筆者所感	認証回避＋任意のコード実行が可能な脆弱性は危険度が高い。 実際に大きな被害も出ており利用している場合はバージョンアップ推奨。

ASUS社製ルータの認証回避の脆弱性

脆弱性番号	CVE-2025-2492
対象製品	AiCloud機能を持つASUS製ルータ（RTシリーズ、TUFシリーズ等）
想定被害	AiCloud機能を有効にしているとインターネット経由で設定変更されたりマルウェアに感染させられる可能性がある
対象バージョン	AiCloud バージョン 2.0.2.36 およびそれ以前
対策	ファームウェアバージョンアップ
アドバイザリ	https://www.asus.com/content/asus-product-security-advisory/
筆者所感	認証を回避して 個人向け製品のため法人が利用している可能性は低い。 国内でも被害が報告されている。

3.サイバーセキュリティ関連ニュース

侵害された事があるFortiGateにバックドアが残されている可能性

2025年4月10日、Fortinet社のブログにてFortiGateに対する新たな攻撃手法が観測されている旨が注意喚起されました。

既知の脆弱性（FG-IR-22-398、FG-IR-23-097、FG-IR-24-015など）を悪用して不正アクセスし、シンボリックリンクを利用してバックドアを残すとの事です。
実際、日本国内でバックドアが稼働しているFortiGateが確認されています。

この手法のユニークな点は、
・対策前のFortiOSにバージョンアップしてもバックドアが維持される
・対策前のFortiOSではバックドアを検知できない
と言う点です。

SSL-VPN機能を使った事があるFortiGateを運用されている場合は、被害を受け続けている可能性があるため対策済みFortiOSへのバージョンアップをご検討ください。
ただし、アンチウイルス/IPSのライセンスを購入している場合は、シグネチャのアップデートでも検知、削除可能との事なので必ずしもFortiOSのバージョンアップが必要では無いようです。

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
2025/4/9	JPCERT/CC Eyes「RightsCon 2025参加記」	JPCERT/CC	https://blogs.jpcert.or.jp/ja/2025/04/rightscon-2025.html
2025/4/15	セキュリティインシデント対応机上演習教材	情報処理推進機構（IPA）	https://www.ipa.go.jp/security/sec-tools/ttx.html
2025/4/17	JPCERT/CC 活動四半期レポート［2025年1月1日～2025年3月31日］	JPCERT/CC	https://www.jpcert.or.jp/pr/index.html
2025/4/17	JPCERT/CC インシデント報告対応レポート［2025年1月1日～2025年3月31日］	JPCERT/CC	https://www.jpcert.or.jp/ir/report.html
2025/4/17	CyberNewsFlash「AiCloudが稼働するASUS製WiFiルーターからの通信の観測」	JPCERT/CC	https://www.jpcert.or.jp/newsflash/2025041701.html
2025/4/21	ゴールデンウイークにおける情報セキュリティに関する注意喚起を公開しました	情報処理推進機構（IPA）	https://www.ipa.go.jp/security/anshin/heads-up/alert20250421.html
2025/4/22	「映像で知る情報セキュリティ」スライド教材を公開しました	情報処理推進機構（IPA）	https://www.ipa.go.jp/security/videos/list.html
2025/4/24	サイバー警察局便りR7Vol.1「銀行から電話・・・はたして本物？企業の資産が危ない！」	警察庁	https://www.npa.go.jp/bureau/cyber/pdf/R7_Vol.1cpal.pdf
2025/4/24	JPCERT/CC Eyes「Ivanti Connect Secureに設置されたマルウェアDslogdRAT」	JPCERT/CC	https://blogs.jpcert.or.jp/ja/2025/04/dslogdrat.html
2025/4/25	「暗号鍵管理ガイダンス Part 2」を公開しました	情報処理推進機構（IPA）	https://www.ipa.go.jp/security/crypto/guideline/ckms.html
2025/4/30	「米国におけるクラウドサービスのセキュリティ評価に係る手続・評価手法等に関する調査（2024年度）」を公開しました	情報処理推進機構（IPA）	https://www.ipa.go.jp/security/reports/cloud_oversea.html

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