セキュリティ運用サービス月次レポート
2025年5月

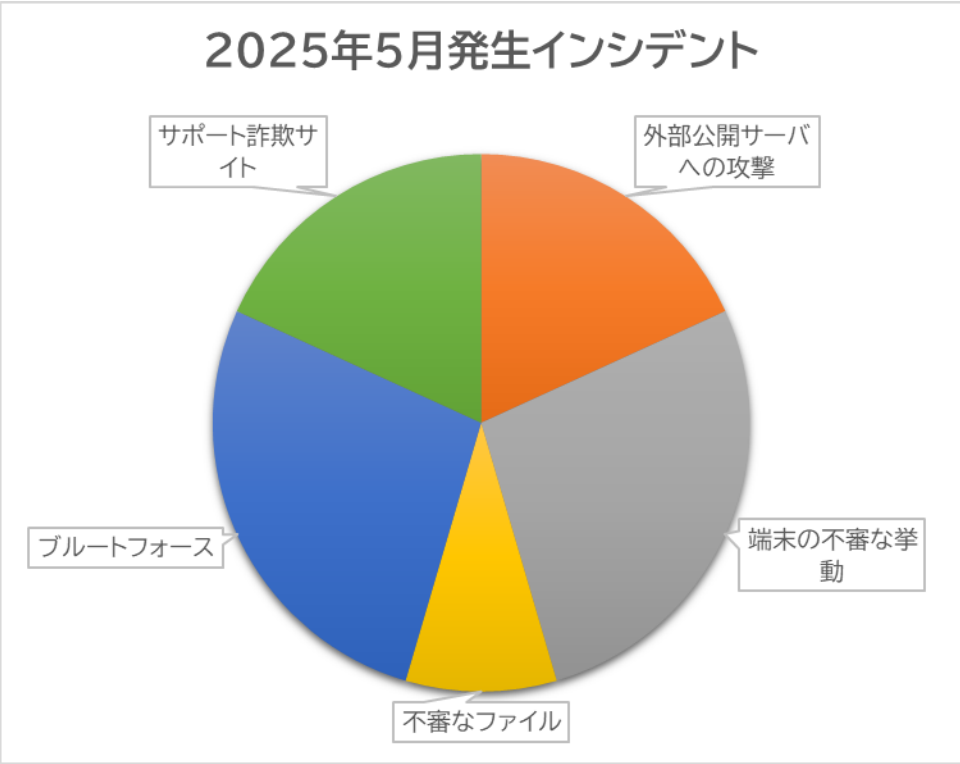
２０２５年６月２３日

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5月は以下のような種類のインシデントが発生しました。



・外部公開サーバへの攻撃
外部公開サーバが、OpenVASやNessus等のツールを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。

・端末の不審な挙動
一部のお客様の端末でWindowsの認証情報が窃取された可能性がある不審な挙動を検知しました。
当SOCの判定基準に照らし合わせ**緊急レベル**で対応しました。

・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5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-2024-38475	Apache	HTTP Server	Apache HTTP Server Improper Escaping of Output Vulnerability
CVE-2025-32756	Fortinet	Multiple Products	Fortinet Multiple Products Stack-Based Buffer Overflow Vulnerability
CVE-2025-4428	Ivanti	Endpoint Manager Mobile (EPMM)	Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability
CVE-2025-4427	Ivanti	Endpoint Manager Mobile (EPMM)	Ivanti Endpoint Manager Mobile (EPMM) Authentication Bypass Vulnerability
CVE-2025-32709	Microsoft	Windows	Microsoft Windows Ancillary Function Driver for WinSock Use-After-Free Vulnerability
CVE-2025-30397	Microsoft	Windows	Microsoft Windows Scripting Engine Type Confusion Vulnerability
CVE-2025-32706	Microsoft	Windows	Microsoft Windows Common Log File System (CLFS) Driver Heap-Based Buffer Overflow Vulnerability
CVE-2025-32701	Microsoft	Windows	Microsoft Windows Common Log File System (CLFS) Driver Use-After-Free Vulnerability
CVE-2025-30400	Microsoft	Windows	Microsoft Windows DWM Core Library Use-After-Free Vulnerability
CVE-2025-42999	SAP	NetWeaver	SAP NetWeaver Deserialization Vulnerability
CVE-2023-44221	SonicWall	SMA100 Appliances	SonicWall SMA100 Appliances OS Command Injection Vulnerability

2025年5月は業界で話題となるような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

情報窃取系マルウェアLumma Stealerのテイクダウン

5月21日、マイクロソフト社及び法執行機関によってLumma Stealerがテイクダウンされました。
Lumma StealerはC2サーバ等システムを構成するインフラが押収され、機能不全となっているようです。
情報窃取系マルウェアは、昨今被害が拡大しているクレジットカード不正利用、証券会社の不正アクセスの原因の一つと考えられています。情報窃取系マルウェアの中でも特にLumma Stealerは勢力を急拡大しており、当SOCでも度々検知がありました。

Lumma Stealerのロゴ

セキュリティ要件適合評価及びラベリング制度本格始動

5月21日、経済産業省による信頼できるIoT製品の評価制度JC-STARの適合製品が初めて公開されました。
IoT製品(ルータや監視カメラなど)は色々な企業が製造/販売していますが、各製品がどの程度セキュリティを意識して作られているか、知識の乏しいユーザにとって判断が難しい状況にありました。JC-STARでは★の数でセキュリティレベルが分けられており、機器導入部分の重要度に応じて適切な製品を選ぶ事ができるようになります。
製品ベンダーにセキュアバイデザインを促すものであり、制度が浸透していけば製品導入時の要件として指定されるようになるかも知れません。

JC-STARのロゴ(情報処理推進機構より)

[情報処理推進機構]セキュリティ要件適合評価及びラベリング制度（JC-STAR）
https://www.ipa.go.jp/security/jc-star/index.html

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
2025/5/2	サイバー警察局便りR7Vol.2「証券会社をかたるフィッシングに注意！」	警察庁	https://www.npa.go.jp/bureau/cyber/pdf/R7_Vol.2cpal.pdf
2025/5/27	「2024年度 中小企業における情報セキュリティ対策に関する実態調査」報告書を公開しました	情報処理推進機構（IPA）	https://www.ipa.go.jp/security/reports/sme/sme-survey2024.html
2025/5/29	「令和6年度セキュリティ人材活用促進実証」報告書を公開しました	情報処理推進機構（IPA）	https://www.ipa.go.jp/security/reports/sme/riss-katsuyo2024.html
2025/5/29	サイバーセキュリティ戦略本部第43回会合を開催	内閣サイバーセキュリティセンター（NISC）	https://www.nisc.go.jp/council/cs/index.html#cs43

5/29にサイバーセキュリティ戦略本部会合が行われています。
会合の決定文書によると「サイバーセキュリティ対策を強化するための監査に係る基本方針」が更新され、
従来2つだった監査内容（「マネジメント監査」と「ペネトレーションテスト」）に加えて「レッドチームテスト」が追加となっています。
「レッドチームテスト」は実際の攻撃者が行う様々な攻撃手法を使って組織全体の防御能力を評価する高度なテストであり、効果が見込める分期間もコストも多くかかります。
国の行政機関や独立行政法人向けの方針ではありますが、高いセキュリティが求められる民間企業でもレッドチームテストの需要が増えるかも知れません。

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