セキュリティ運用サービス月次レポート
2025年7月

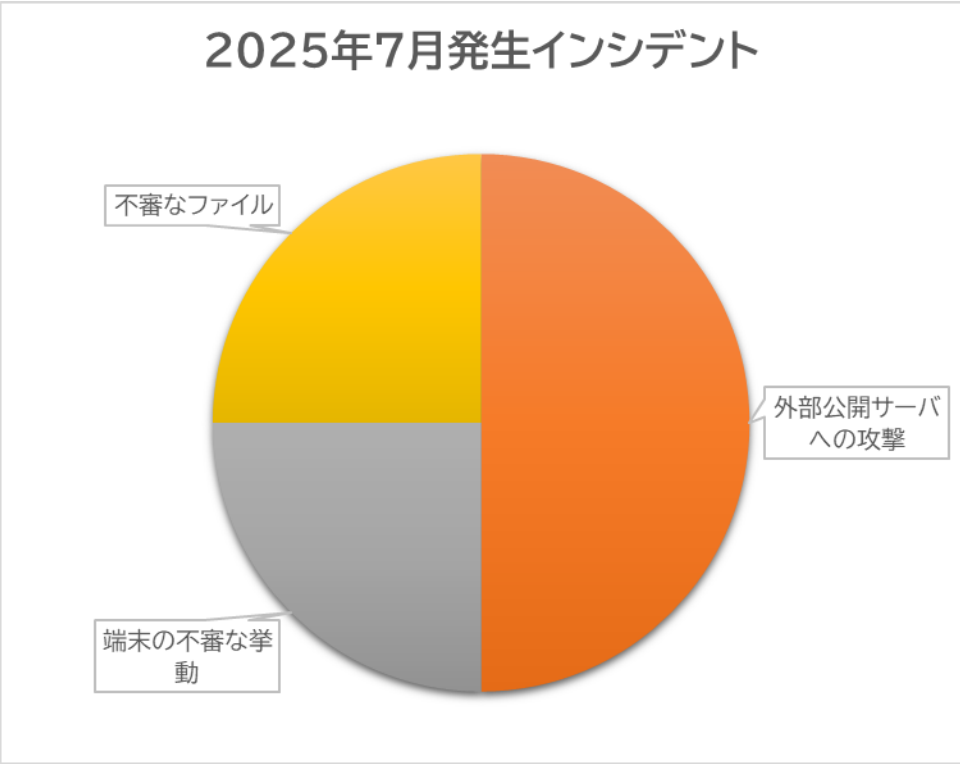
２０２５年８月２７日

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7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
インストールされたセキュリティソフトをアンインストールする等、不審な挙動を行う端末がありました。

・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。

2.脆弱性情報

2025年7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-2025-20337	Cisco	Identity Services Engine	Cisco Identity Services Engine Injection Vulnerability
CVE-2025-20281	Cisco	Identity Services Engine	Cisco Identity Services Engine Injection Vulnerability
CVE-2025-5777	Citrix	NetScaler ADC and Gateway	Citrix NetScaler ADC and Gateway Out-of-Bounds Read Vulnerability
CVE-2025-25257	Fortinet	FortiWeb	Fortinet FortiWeb SQL Injection Vulnerability
CVE-2025-6554	Google	Chromium V8	Google Chromium V8 Type Confusion Vulnerability
CVE-2025-6558	Google	Chromium	Google Chromium ANGLE and GPU Improper Input Validation Vulnerability
CVE-2025-53770	Microsoft	SharePoint	Microsoft SharePoint Deserialization of Untrusted Data Vulnerability
CVE-2025-49704	Microsoft	SharePoint	Microsoft SharePoint Code Injection Vulnerability
CVE-2025-49706	Microsoft	SharePoint	Microsoft SharePoint Improper Authentication Vulnerability
CVE-2019-5418	Rails	Ruby on Rails	Rails Ruby on Rails Path Traversal Vulnerability

7月は**ToolShell**と呼ばれるSharePointのゼロデイ脆弱性CVE-2025-53770が特に話題になりました。
オンプレミス版SharePointにアクセスできる環境であれば、「/_layouts/15/ToolPane.aspx」に対して細工したリクエストを投げるだけで認証を回避してリモートでコード実行できるという事で非常に危険な脆弱性と考えられます。
SharePointをインターネットに公開していない限りリスクは限定的ですが、リスク回避の観点からアップデートしておいた方が良いと思います。

3.サイバーセキュリティ関連ニュース

サイバー空間における認知戦の拡大

7月20日に行われた参院選選挙に先立って、SNS上で外国勢力による選挙介入が行われていると言う調査記事が公開され話題になりました。
選挙への介入は日本に限らず他国でも疑わしい事象が観測されており問題視されています。

具体的には以下のような手法が用いられたようです。
・偽のニュースサイトやSNSで感情を煽るような文体を用いて偏った情報を投稿する
・ボットを使い大量の「いいね」やリポストを行う
・SNSが関連する投稿を機械的にトレンド入りさせる
・偏った情報を多くの人が目にする
・偏った情報を真に受ける人が現れる
・偏った意見を持つ人が増えて社会が不安定になる

このようにSNSやメディアを使って人の認知や判断をコントロールする戦略は認知戦と呼ばれており、目に見える形で行われる事もあれば密かに行われるものもあります。
調査記事が事実なのかはさておき、悪意を持った個人や組織が標的を炎上させたり評価を貶める際にも活用できる手法でもあるため自組織で炎上などのインシデントが発生した際は留意した方が良いかも知れません。

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
2025/7/17	JPCERT/CC 四半期レポート［2025年4月1日～2025年6月30日］	情報処理推進機構（IPA）	https://www.jpcert.or.jp/qr/index.html
2025/7/17	ソフトウェア等の脆弱性関連情報に関する届出状況［2025年第2四半期（4月～6月）］	情報処理推進機構（IPA）	https://www.jpcert.or.jp/report/press.html
2025/7/18	JPCERT/CC Eyes「Ivanti Connect Secureの脆弱性を起点とした侵害で確認されたマルウェア」	情報処理推進機構（IPA）	https://blogs.jpcert.or.jp/ja/2025/07/ivanti_cs.html
2025/7/17	サイバー警察局便りR7Vol.3「ランサムウェア（Phobos/8Base）により暗号化されたファイルを復号！！」	警察庁	https://www.npa.go.jp/bureau/cyber/pdf/R7_Vol.3cpal.pdf
2025/7/24	サイバー警察局便りR7Vol.4「中小企業で被害多数 ランサムウェア」	警察庁	https://www.npa.go.jp/bureau/cyber/pdf/R7_Vol.4cpal.pdf

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