# セキュリティ運用サービス月次レポート
# 2025年8月

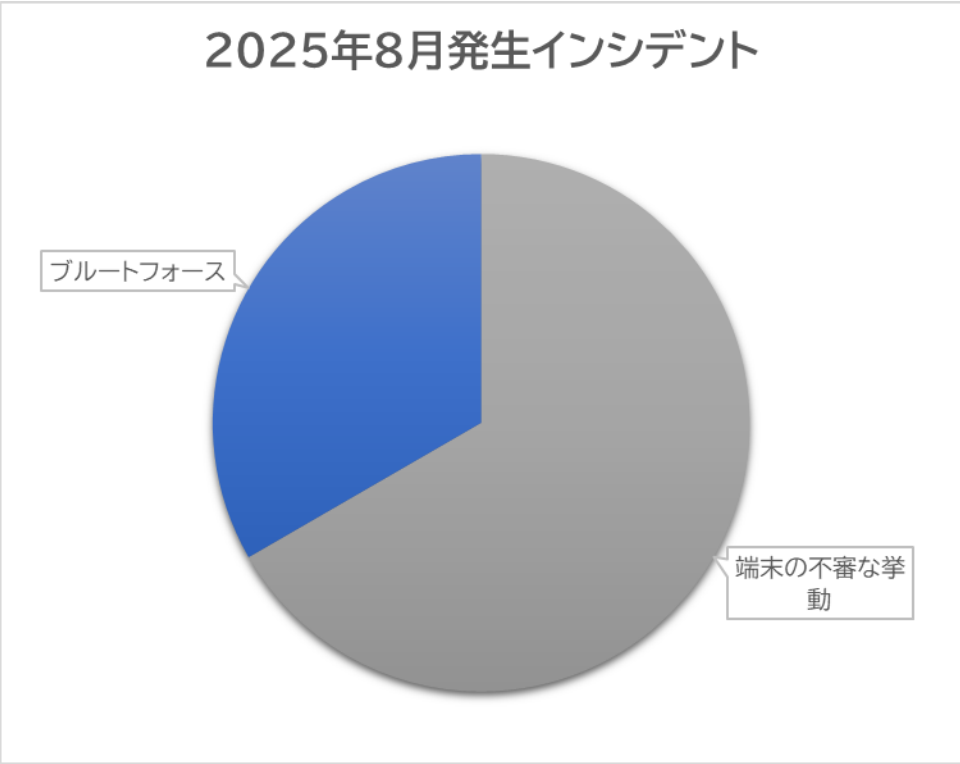
２０２５年１０月４日

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8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

当月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-2022-40799 | D-Link | DNR-322L | D-Link DNR-322L Download of Code Without Integrity Check Vulnerability |
| CVE-2025-8088 | RARLAB | WinRAR | RARLAB WinRAR Path Traversal Vulnerability |
| CVE-2007-0671 | Microsoft | Office | Microsoft Office Excel Remote Code Execution Vulnerability |
| CVE-2013-3893 | Microsoft | Internet Explorer | Microsoft Internet Explorer Resource Management Errors Vulnerability |
| CVE-2025-54948 | Trend Micro | Apex One | Trend Micro Apex One OS Command Injection Vulnerability |
| CVE-2025-7775 | Citrix | NetScaler | Citrix NetScaler Memory Overflow Vulnerability |
| CVE-2025-48384 | Git | Git | Git Link Following Vulnerability |
| CVE-2025-43300 | Apple | iOS, iPadOS, and macOS | Apple iOS, iPadOS, and macOS Out-of-Bounds Write Vulnerability |

8月はSuica等の電子決済に使われるFeliCaのICチップに脆弱性があると大々的に報道がありました。
情報処理推進機構(IPA)は報道以前から脆弱性を認識していたようですが、あえて広く公開はしていなかったようです。
にもかかわらず、各報道機関が断りなく報道したため9月9日に国家サイバー統括室（旧：内閣サイバーセキュリティセンター）が報道機関にくぎを刺すような注意喚起を出しています。
これは、情報の公開方法やタイミングによっては実際の影響度合いに対して過剰な混乱を社会にもたらす可能性があるためと思われます。

また、国内企業(株式会社ディー・オー・エス)が提供する資産管理ツール「SS1」に緊急レベルの脆弱性が発見されているため導入している場合はご注意ください。

# 3.サイバーセキュリティ関連ニュース

## 日本企業のランサムウェア被害増加中

8月19日、Cisco社が日本のランサムウェア被害状況についてレポートを公開しました。

レポートによると2025年上半期、日本ではランサムウェア攻撃が前年同時期比で約1.4倍に増加し、68件が確認されています。 特にQilin(麒麟)と言うグループによる被害が多くなっている一方、昨年まで目立っていたLockBitや8baseと言ったグループは、法執行機関の摘発により減少しました。

最も影響を受けたのは製造業（全体の18.2%）。次いで自動車、商社、建設、運輸などが続き、被害企業の69%は資本金10億円未満の中小企業という事です。
記事中では中小企業が標的になっているとされていますが、筆者としては中小企業は大企業と比較して母数が多いため被害を受ける確率も高いのではないかと考えています。

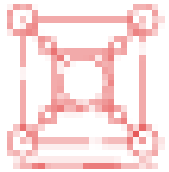
読者の皆様に置かれましては、引き続き以下のような対策をご検討ください。
・最新の侵入、攻撃手法のキャッチアップと対策
・バックアップの多重化、アクセス権管理
・職員の教育、訓練
・インシデント発生時の対応手順、体制整備

自組織のみでの対策に不安がある場合は、ぜひ弊社にお声かけ下さい。

参考記事：https://blog.talosintelligence.com/ransomware_incidents_in_japan_during_the_first_half_of_2025/


**Qilin**
**被害組織：アサヒHD(25年10月)等**
**2025年活動活発化**

**LockBit**
**被害組織：名古屋港運協会等**
**24年12月の摘発後活動縮小**



**8Base**
**被害組織：イセトー等**
**警視庁が複合ツール配布**

# 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 |
|---|---|---|---|
| 2025/8/1 | 2025年度 夏休みにおける情報セキュリティに関する注意喚起 | 情報処理推進機構（IPA） | https://www.ipa.go.jp/security/anshin/heads-up/alert20250801.html |
| 2025/8/6 | トレンドマイクロ製企業向けエンドポイントセキュリティ製品における複数のOSコマンドインジェクションの脆弱性に関する注意喚起 | JPCERT/CC | https://www.jpcert.or.jp/at/2025/at250016.html |
| 2025/8/7 | CyberNewsFlash「SSL-VPN機能が有効化されたSonicWall製ファイアウォールGen 7以降を標的とする脅威活動について」 | JPCERT/CC | https://www.jpcert.or.jp/newsflash/2025080701.html |
| 2025/8/14 | JPCERT/CC Eyes「Cobalt Strike Beaconの機能をクロスプラットフォームへと拡張するツール「CrossC2」を使った攻撃」 | JPCERT/CC | https://blogs.jpcert.or.jp/ja/2025/08/crossc2.html |
| 2025/8/28 | サイバー警察局便りR7Vol.5「SNS等のアカウントの乗っ取りに警戒を！！」（R7.8.28） | 警察庁 | https://www.npa.go.jp/bureau/cyber/pdf/R7_Vol.5cpal.pdf |
| 2025/8/28 | インターネットサービスへの不正ログインによる被害が増加中 | 情報処理推進機構（IPA） | https://www.ipa.go.jp/security/anshin/attention/2025/mgdayori20250828.html |
| 2025/8/28 | 「企業における営業秘密管理に関する実態調査2024」報告書 | 情報処理推進機構（IPA） | https://www.ipa.go.jp/security/reports/economics/ts-kanri/tradesecret2024.html |
| 2025/8/29 | Citrix Netscaler ADCおよびGatewayの脆弱性（CVE-2025-7775）に関する注意喚起 | JPCERT/CC | https://www.jpcert.or.jp/at/2025/at250018.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