

セキュリティ運用サービス月次レポート

2025年6月

2025年7月28日

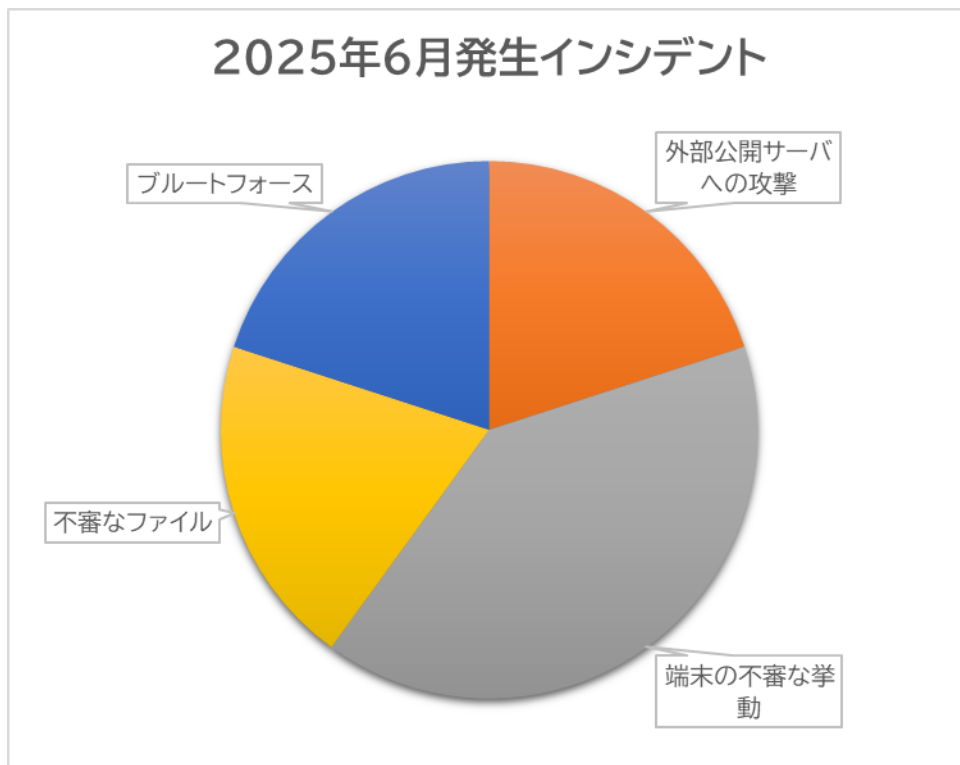
NEC ネットエスアイ株式会社

目次

1. サイバー攻撃検知状況
2. 脆弱性情報
3. サイバーセキュリティ関連ニュース
4. 公的機関のお知らせまとめ
5. 最後に

1. サイバー攻撃検知状況

当社SOCにおいて2025年6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

特定の端末がネットワーク内部をスキャンするような挙動を行いました。
また、特定の端末が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ような挙動がありました。

- ・ 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の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6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-2025-43200	Apple	Multiple Products	Apple Multiple Products Unspecified Vulnerability
CVE-2021-32030	ASUS	Routers	ASUS Routers Improper Authentication Vulnerability
CVE-2023-39780	ASUS	RT-AX55 Routers	ASUS RT-AX55 Routers OS Command Injection Vulnerability
CVE-2025-6543	Citrix	NetScaler ADC and Gateway	Citrix NetScaler ADC and Gateway Buffer Overflow Vulnerability
CVE-2019-6693	Fortinet	FortiOS	Fortinet FortiOS Use of Hard-Coded Credentials Vulnerability
CVE-2023-0386	Linux	Kernel	Linux Kernel Improper Ownership Management Vulnerability
CVE-2025-33053	Microsoft	Windows	Microsoft Windows External Control of File Name or Path Vulnerability
CVE-2023-33538	TP-Link	Multiple Routers	TP-Link Multiple Routers Command Injection Vulnerability

Citrix NetScaler ADC/Gatewayにて深刻なDoS脆弱性(CVE-2025-6543)が報告されています。

6月時点でKEVには掲載されていないものの、同月同製品でCitrix Bleed2と呼ばれる別の重大な脆弱性(CVE-2025-5777)も見つかっており、旧バージョンのリスクが特に上がっているため同製品を利用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

ディープフェイクとZoomを用いた高度なソーシャルエンジニアリング

北朝鮮のハッカー集団BlueNoroffがディープフェイクを用いた高度なソーシャルエンジニアリング攻撃を行っていると報告[1]されています。

ディープフェイクは、AI（特に深層学習）を用いて画像や動画を改ざんし、実在しない情景や人物の発言を生成する技術です。

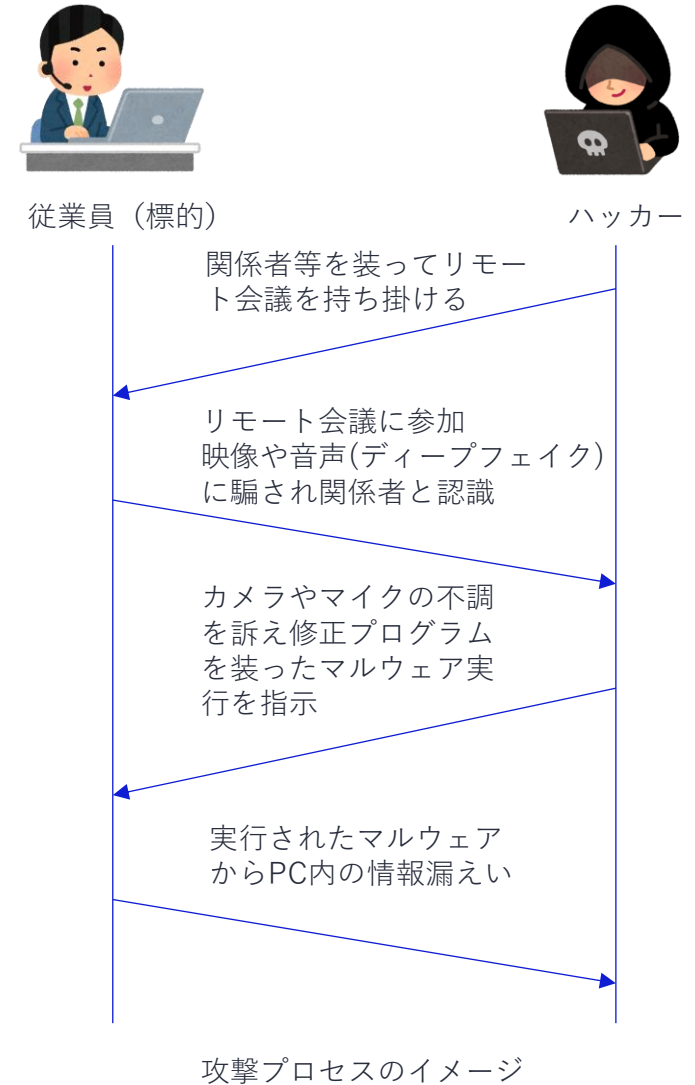
例えば、有名人の顔を進化や別の文脈の表情にしたり、音声を模倣して偽のスピーチを作ったりできます。

具体的には、攻撃者は標的の関係者や知り合いになりすましてZoom等のリモート会議に誘い出し、ディープフェイクを悪用してカメラの映像や音声も関係者本人かのように偽装する事で標的の信用を得ます。

その後、カメラやマイクの不調を訴え、標的に対して不調を解消するプログラムを装ってマルウェアをインストールさせ、PC内の情報を窃取するとの事です。

ディープフェイクは現時点では高度な攻撃手法と言えますが、遠くない将来コモディティ化し当たり前のように詐欺行為に利用されるようになるかも知れません。

[1]Bleeping Computer : North Korean hackers deepfake execs in Zoom call to spread Mac malware(<https://www.bleepingcomputer.com/news/security/north-korean-hackers-deepfake-execs-in-zoom-call-to-spread-mac-malware/>)



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
2025/6/6	JPCERT/CC インターネット定点観測レポート [2025年1月1日～2025年3月31日]	情報処理推進機構 (IPA)	https://www.jpccert.or.jp/tsubame/report/report202501-03.html
2025/6/6	JPCERT/CC Eyes「TSUBAMEレポート Overflow (2025年1～3月)」	情報処理推進機構 (IPA)	https://blogs.jpccert.or.jp/ja/2025/06/tsubame-overflow20250103.html
2025/6/27	サイバーセキュリティ戦略本部第44回会合を開催	国家サイバー統括室	https://www.nisc.go.jp/council/cs/previous/index.html#cs44
2025/6/27	サイバーセキュリティ対策推進会議(CISO等連絡会議)第21回会合を開催	国家サイバー統括室	https://www.nisc.go.jp/council/cs/taisaku/index.html#ciso21

6/27にサイバーセキュリティ戦略本部会合が行われ、日本におけるサイバーセキュリティ対策の活動報告資料が公開されました。
<https://www.nisc.go.jp/pdf/policy/kihon-s/250627cs2025.pdf>

2024年に国内で発生した主なセキュリティインシデントの他、今後実施していく対策等が示されています。

国が行うセキュリティ対策は一企業においても参考になるかと思えますので最終ページのエグゼクティブサマリーだけでも目を通しておくと、今後のセキュリティに役立てる事ができるかも知れません。

サイバーセキュリティ2025のポイント (「エグゼクティブ・サマリー」)

- 巧妙化・高度化したサイバー攻撃や国家を背景とした攻撃キャンペーン等により、国民生活・経済活動及び安全保障に対し、深刻かつ致命的な被害を生じさせるおそれがあることや、その標的・被害が急速に多様化・複雑化していることが、国内においても、これまで以上に顕在化。
- 政府においては、政府機関等のセキュリティ確保に係る取組や、近時のサイバー攻撃に係る注意喚起、脅威アクター対応からルールメイキングまで幅広く国際連携の強化を実施。
- サイバー対処能力強化法等^{※1,2} (令和7年5月16日成立、同月23日公布) 施行に向けた施策及び「サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項」に掲げられた施策を、2025年度の「特に強力に取り組む施策」に位置づけるとともに、新たなサイバーセキュリティ戦略を2025年内目途に策定。

2024年度における主な国内のサイバー攻撃事案

- 中国の関与が疑われるサイバー攻撃グループ「MirrorFace」による、安全保障や先端技術に係る機密情報の窃取を狙う攻撃キャンペーン
- 北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」による、暗号資産関連事業者からの暗号資産窃取
- 金融機関や地方公共団体等からの受託企業に対し、個人情報等を漏えいさせたランサムウェア攻撃
- 出版事業等を行う大手企業に対し、提供するウェブサービスの停止や、書籍の流通事業等に影響を生じさせたランサムウェア攻撃
- 航空会社の国内便・国際便の遅延や、インターネットバンキングへのログイン障害等、複数の重要インフラ分野に対するDDoS攻撃 等

政府のサイバー攻撃への対応

- 政府機関等のセキュリティ確保に係る取組
 - アタックサーフェスマネジメント及びIPDNSの導入による機密監視の強化
 - 「政府機関等の対策基準策定のためのガイドライン」の一部改定
 - 生成AIを含む約取型のサービス等の業務利用に係る注意喚起 等
- サイバー攻撃に係る注意喚起
 - Living Off The Land戦術等を含む最近のサイバー攻撃に関する注意喚起
 - MirrorFaceによるサイバー攻撃に関する注意喚起
 - DDoS攻撃への対策に関する注意喚起 等
- 国際連携の強化
 - 「TraderTraitor」に係る米共同のバリエーション
 - 「APT40 Advisory PRC MSS tradecraft in action」の共同署名
 - 日印アフリカ連合の下でのG7サイバーセキュリティ作業部会の設立・参画 等

特に強力に取り組むべき施策

サイバー対処能力強化法^{※1}及び同整備法^{※2}の施行に向けた施策

「サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項」 (2025年5月29日サイバーセキュリティ戦略本部決定)

- ・ 新たな司令塔機能の確立
- ・ 巧妙化・高度化するサイバー攻撃に対する官民の対策・連携強化
- ・ 官民連携エコシステムの実現
- ・ 政府機関・重要インフラ等を通じた機密的な対策の強化
- ・ 政府機関等のセキュリティ対策水準の向上及び実効性の確保
- ・ サイバーセキュリティを支える人的・技術的基盤の整備
- ・ 我が国の対応能力を支える技術・産業育成及び先進技術への対応
- ・ 国際連携を通じた我が国のプレゼンス強化

期限を設けて取り組むべきとされた事項

- ・ インシデント報告様式の統一 (本年10月から)
- ・ JC-STARの政府機関等における選定基準への反映 (本年度内)
- ・ 官民共通の「人材フレームワーク」の策定 (本年度内)
- ・ 脅威ハンティングの行動計画の基本方針の策定 (来年度目途)
- ・ 重要インフラ事業者等のサイバーセキュリティ対策に係る基準の策定 (来年度内)
- ・ 中小企業の対策のための環境整備 (サイバーセキュリティ強化に向けたセキュリティ対策評価制度は来年度内)
- ・ 量子計算機暗号 (PQC) の移行の方向性の検討 (本年度内目途)

新たな「サイバーセキュリティ戦略」を2025年内目途に策定

国家サイバー統括室：サイバーセキュリティ2025（2024年度年次報告・2025年度年次計画）より

5.最後に

NECネット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。

NEC

\Orchestrating a brighter world