セキュリティ運用サービス月次レポート
2025年9月

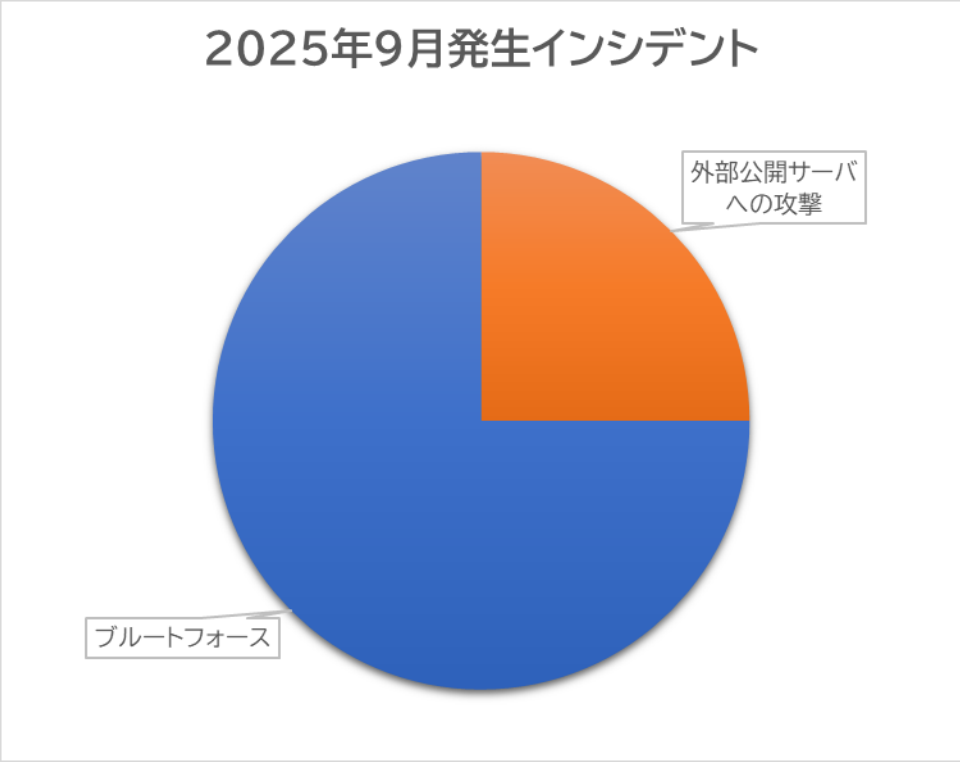
２０２５年１０月３０日

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9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。

・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

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-2025-20362	Cisco	Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense	Cisco Secure Firewall Adaptive Security (ASA) Appliance and Secure Firewall Threat Defense (FTD) Missing Authorization Vulnerability
CVE-2025-20333	Cisco	Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense	Cisco Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD) Buffer Overflow Vulnerability
CVE-2025-20352	Cisco	IOS and IOS XE	Cisco IOS and IOS XE Software SNMP Denial of Service and Remote Code Execution Vulnerability
CVE-2025-10585	Google	Chromium V8	Google Chromium V8 Type Confusion Vulnerability
CVE-2025-38352	Linux	Kernel	Linux Kernel Time-of-Check Time-of-Use (TOCTOU) Race Condition Vulnerability
CVE-2025-32463	Sudo	Sudo	Sudo Inclusion of Functionality from Untrusted Control Sphere Vulnerability

今月は特別に注目されたり社会的な影響が大きい脆弱性はありませんでした。

3.サイバーセキュリティ関連ニュース

アサヒHDを攻撃したランサムグループ「Qilin」とは

グループの特徴
Qilinは、2022年に登場したロシア語圏発のランサムウェアグループでRaaS（Ransomware-as-a-Service）モデルを採用。
高度な暗号化技術と検知回避機能を備え、企業のシステムを侵害してデータを暗号化・窃取し、二重または三重の恐喝を行う。製造業や医療、公共インフラなどを標的に活動しており、2025年にはLockBitなど他グループとカルテルを結成し、攻撃の効率化を図ってる。

被害組織
アサヒグループホールディングス、宇都宮セントラルクリニック、新興プラスチックス等

主な攻撃手法
・漏えいした認証情報を使った不正アクセス
・VPNやRDP等のリモートアクセス経路からの侵入
・脆弱性を突いた侵入（CVE-2024-55591等）
・ソーシャルエンジニアリング

対策
・ASM等を用いた露出の認知と脆弱性管理
・ゼロトラストモデルによる認証、認可
・EDR等セキュリティ製品による脅威の検出、監視
・従業員の教育
・適切なバックアップ

RaaS（Ransomware-as-a-Service）

RaaS運営者（Qilin）：
ランサムウェアや周辺システムの開発、管理しアフィリエイトにサービスとして提供する。成果を出したアフィリエイトに身代金を山分けする。

RaaS利用者：
通称アフィリエイト。攻撃担当。侵入できそうな標的を探し、いろいろな手段でランサムウェアに感染させる。

得意分野に分業する事でメリットがある
・開発速度、品質向上
・同時並行で多数の標的を攻撃
・摘発時のリスク軽減

3.サイバーセキュリティ関連ニュース

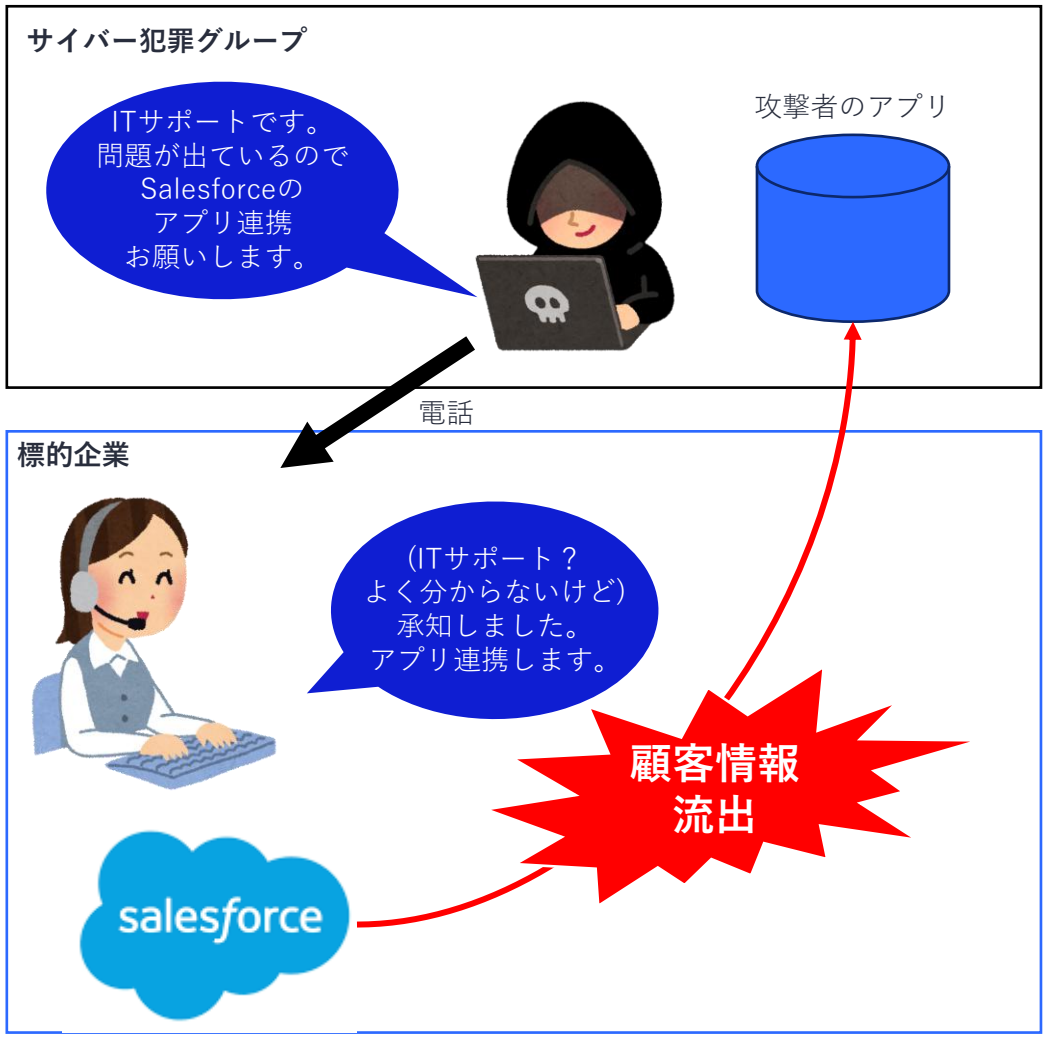
Salesforceを標的としたVishing攻撃による被害拡大

概要
Vishingはボイスフィッシングを短縮した造語であり、電話を用いた詐欺の一種。
サイバー犯罪グループがVishing を用いてSalesforce CRMに不正アクセスし、
企業の顧客情報を盗み出した。
複数の企業が被害を受けており10億件以上の顧客情報が漏えいした。

被害組織
Google,Hulu,トヨタ(海外)等(一部は攻撃者側の申告であり各社公式発表ではない)
※Vishingの特性上、日本企業の被害は現状少ない

攻撃手法
・Salesforceを使っている標的企業に対して関係者を装って攻撃者が電話をかける
・Salesforceと攻撃者が用意したツールを連携するよう仕向ける
・ツールを経由してSalesforceの情報が攻撃者に連携、流出する
・流出した情報を使って標的企業を脅迫

対策
・ソーシャルエンジニアリング攻撃に関する教育や訓練
・事例の共有
・Salesforceの連携アプリの制限
・Salesforce Shieldの導入
・SSPM(SaaS Security Posture Management)による設定管理



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
2025/9/2	国内における脆弱性関連情報を取り扱う全ての皆様へ – 情報セキュリティ早期警戒パートナーシップガイドラインに則した対応に関するお願い –	JPCERT/CC	https://www.jpcert.or.jp/press/2025/PR20250909_notice1.html
2025/9/9	情報セキュリティ白書2025	情報処理推進機構（IPA）	https://www.ipa.go.jp/publish/wp-security/2025.html
2025/9/10	インターネット定点観測レポート（2025年 4～6月）	JPCERT/CC	https://www.jpcert.or.jp/tsubame/report/report202504-06.html
2025/9/11	TSUBAMEレポート Overflow（2025年4～6月）	JPCERT/CC	https://blogs.jpcert.or.jp/ja/2025/09/tsubame-overflow20250406.html
2025/9/11	解説：脆弱性関連情報取扱制度の運用と今後の課題について（前編）～公益性のある脆弱性情報開示とは何か～	JPCERT/CC	https://blogs.jpcert.or.jp/ja/2025/09/handling_vul_info_1.html
2025/9/12	解説：脆弱性関連情報取扱制度の運用と今後の課題について（後編）～脆弱性悪用情報のハンドリングと今後の課題～	JPCERT/CC	https://blogs.jpcert.or.jp/ja/2025/09/handling_vul_info_2.html
2025/9/19	サイバー警察局便りR7Vol.6「身近にサイバー攻撃の危険が迫っています！」	警察庁	https://www.npa.go.jp/bureau/cyber/pdf/R7_Vol.6cpal.pdf
2025/9/26	Cisco ASA、FTD、IOS、IOS XEおよびIOS XRにおける任意のコード実行の脆弱性（CVE-2025-20363）について	JPCERT/CC	https://www.jpcert.or.jp/newsflash/2025093001.html
2025/9/30	国内における脆弱性関連情報を取り扱う全ての皆様へ – 情報セキュリティ早期警戒パートナーシップガイドラインに則した対応に関するお願い –	JPCERT/CC	https://www.jpcert.or.jp/press/2025/PR20250909_notice1.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