LAC

LAC SECURITY INSIGHT

第 15 号

2026 冬

特集：2026 年の脅威予測

JSOC で観測されたサイバー攻撃傾向

サイバー119 サービスの出動傾向

JSOC JAPAN SECURITY OPERATION CENTER

CYBER EMERGENCY CENTER

DiaForce

2026 年 2 月
株式会社ラック

LAC SECURITY INSIGHT

第 15 号／2026 冬

目　　次

はじめに

本レポートは、ラックの中でもサイバー攻撃の脅威に対して最前線で対応している JSOC およびサイバー救急センター、そして攻撃者が利用するサイバー攻撃手法も活用してお客様のシステムへ侵入テストを行うデジタルペンテスト部において、分析・調査・侵入テストを実施する中で得た、最近の脅威の傾向や特徴を、セキュリティ専門家が「洞察」としてまとめたものです。

日々発生している実際の攻撃やインシデントに根ざしており、また日本の企業や団体を狙った脅威を中心にまとめているため、日本の企業や団体のサイバーセキュリティ担当者が、自組織が直面しているサイバー攻撃や脅威を把握できる内容です。

サイバー攻撃の傾向の変化は年々早く強くなっており、セキュリティ対策も継続的に見直して対応していく必要があり、またそのスピードが求められます。本レポートが、皆さまの継続的なセキュリティ対策の改善に役立てていただけることを願っております。

株式会社ラック
コンサルティング統括部長
内田 法道

サイバー119で出動したインシデント傾向

2025年10月～12月の出動傾向

当該期間では、マルウェアによる被害の相談が 31%、およびサーバ不正利用による被害の相談が44%であり、両者で全体の 75%を占めています。この割合は前四半期（2025 年 7 月から 9 月）68%、および前年同期（2024 年 10 月から 12 月）73%より増加しています。

マルウェア関連の被害では、ランサムウェアによる被害が全体の 16%を占め、前四半期（16%）、および前年同期（16%）と同じ割合でした。依然として最も高い割合を占める脅威であり、不正侵入の経路として SSL-VPN 機器に残存している問題の悪用が継続して確認されています。原因としては、多要素認証（MFA）の未設定、推測されやすいパスワードの使用、SSL-VPN 機器に存在する脆弱性への未対応などが挙げられます。

サーバ不正利用の被害では、OS やミドルウェアといったプラットフォーム（PF）の脆弱性に起因する被害が全体の 12%を占め、前四半期（2%）、および前年同期（5%）から大幅に増加しました。本来公開が不要な検証/開発用途のサーバが誤ってインターネットに公開され、当該サーバを踏み台として組織内 NW へ侵入された事案を確認しています。検証/開発用途のサーバを含め、インターネット全体からアクセスされる必要のないサーバが外部公開されていないかを、サーバの棚卸しや ASM（Attack Surface Management）などで確認し、適切なアクセス制御の適用および不要サーバの撤去を行ってください。

DDoS 被害の相談は全体の 4%を占め、前年同期（5%）と同程度でした。過去 3 年間の傾向から、年末に DDoS による相談が増加する傾向が見られます。年末は大規模セールやホリデーシーズンに伴う EC サイトの繁忙期であり、昨年同期では、旅行需要の高まりに伴うチケット販売システムや長期休暇前に停止するオンラインバンキングが攻撃を受けた事例が確認されています。こうした状況から、繁忙期を狙った意図的な攻撃が継続していると考えられます。

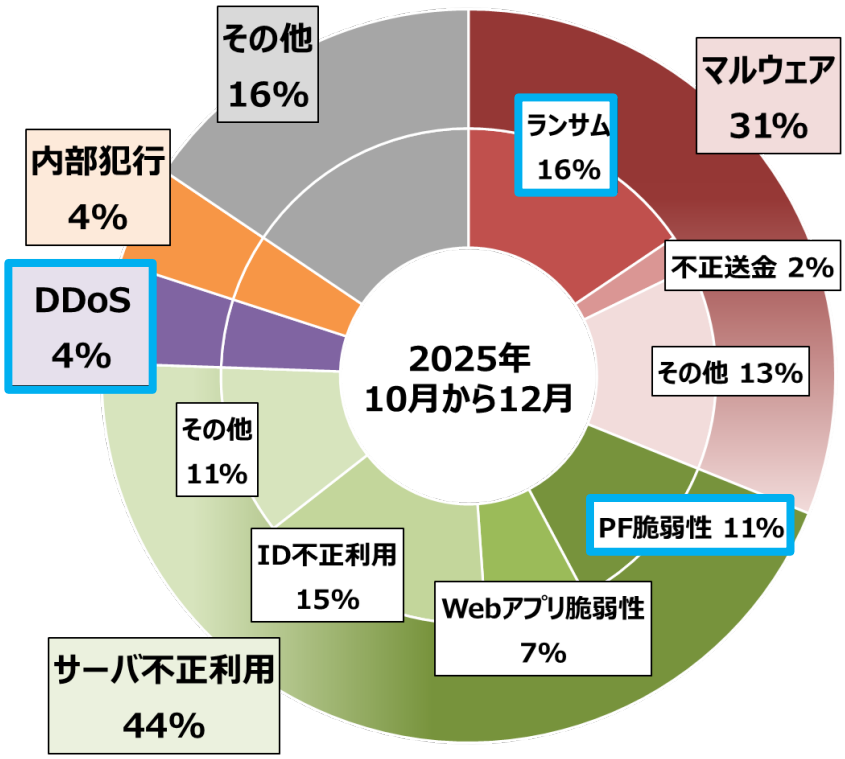

図 1 2025 年 10 月から 12 月の出動インシデントの内訳

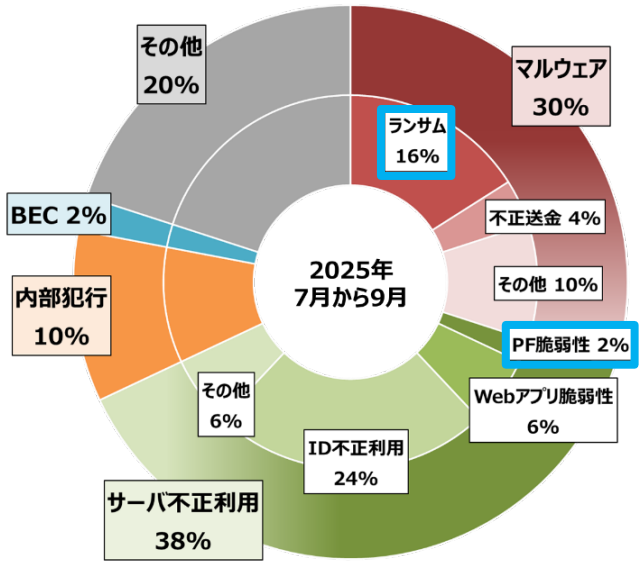

図 2 前四半期（2025 年 7 月から 9 月）

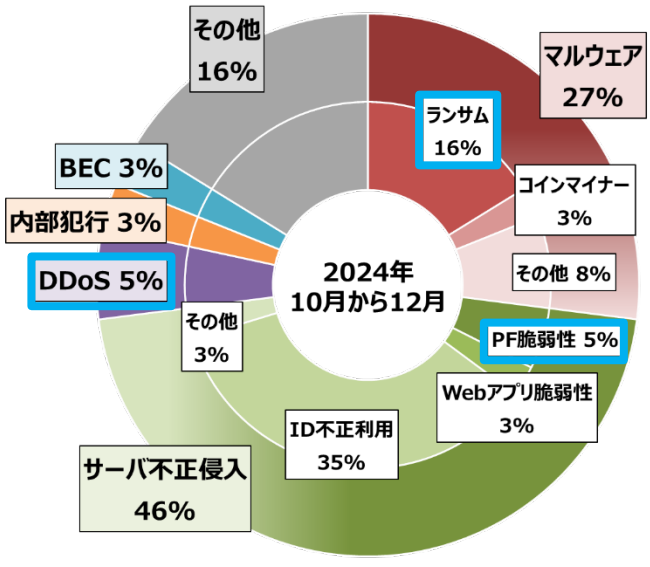

図 3 前年同期（2024 年 10 月から 12 月）

下表は、当該期間（2025 年 10 月～12 月）、前四半期（2025 年 7 月～9 月）および前年同期（2024 年 10 月～12 月）の各期間における相談件数の割合を業種別に集計し、上位 5 業種の推移を示したものです。

情報通信業は当該期間において 28%となり、前四半期（33%）および前年同期（33%）と比較して割合が減少しているものの、依然として高い割合を占めています。当該期間における上位業種の変動としては、「金融業、保険業」が前期以前から徐々に順位を上げ、今期は 3 位へと浮上したほか、「教育、学習支援業」が新たに上位 5 業種に含まれました。一方で、前四半期に上位であった「学術研究・専門・技術サービス業」は、上位から外れました。しかし、業種別の出動インシデントに顕著な特徴は確認されず、引き続き幅広い業種から多様な相談が寄せられている状況に変化はありません。

表 1 上位 5 業種の相談件数割合

順位	当該期間（2025 年 10 月から 12 月）		前四半期（2025 年 7 月から 9 月）		前年同期（2024 年 10 月から 12 月）	
1	情報通信業	28%	情報通信業	33%	情報通信業	33%
2	製造業	15%	製造業	15%	学術研究，専門・技術サービス業	15%
3	金融業，保険業	12%	学術研究，専門・技術サービス業	13%	製造業	9%
4	卸売業，小売業	9%	金融業，保険業	12%	教育，学習支援業	9%
5	教育，学習支援業	8%	卸売業，小売業	8%	卸売業，小売業	7%

【クラウドサービスのアカウント不正利用】

ID 不正利用による被害では、攻撃者に窃取された Microsoft 365 アカウントが悪用されるケースが増加しています。相談の多くでは、不正アクセスを受けたアカウントから他組織宛てに大量のフィッシングメールが送信されていることを確認しました。

不正アクセスの防止を目的として多くの組織で多要素認証（MFA）の導入が進みつつある一方で、被害組織では、全アカウントまたは一部アカウントで MFA が未設定であったことや、MFA を回避できるレガシー認証を有効にしたまま運用していたことにより、被害の発生を防げなかったと考えられます。

レガシー認証は、ID/パスワードのみの SMTP AUTH（基本認証）であり MFA をサポートしていないため、現在は無効化することが推奨されています。Microsoft 365 では 2026 年 4 月までに完全に廃止される予定です。一方で、古い複合機や業務アプリケーションの通知メール機能で依然として利用している組織も多く、不正アクセスの被害を受ける原因の一つとなっています。

MFA を有効化する組織が増加する中、攻撃者は従来の確認コードやプッシュ通知による MFA を回避する Adversary in the Middle（AiTM）攻撃を用いるケースが増加しています。AiTM 攻撃では、フィッシングサイトとリバースプロキシを組み合わせることで、ユーザがフィッシングサイトに入力したユーザ ID、パスワード、MFA コードを即座に正規サイトへ転送し、認証後に発行されるセッション Cookie を窃取します。攻撃者は、このセッション Cookie を用いることで、ユーザになりすまして正規サイトにアクセスし、不正な操作を行うことが可能となります。

AiTM 攻撃の増加要因としては、以下の点が挙げられます。

- PhaaS（Phishing-as-a-Service）の産業化と普及により、MFA 突破を前提とした攻撃キットが流通し、参入ハードルが低下していること
- 生成 AI を利用したフィッシングメール作成の高度化により、自然な文章生成や動的 URL の自動生成を通じたシグネチャ回避が容易になっていること

これらのリスクを低減するためには、従来の確認コード入力型、プッシュ通知型の MFA に依存するのではなく、接続先の正当性を自動的に検証する「フィッシング耐性認証 [1]」を導入することが有効です。これ

---

[1] Microsoft Entra ID で耐フィッシング パスワードレス認証の展開を計画する - Microsoft Entra ID | Microsoft Learn
https://learn.microsoft.com/ja-jp/entra/identity/authentication/how-to-deploy-phishing-resistant-passwordless-authentication
組織のパスキーを有効にする - Microsoft Entra ID | Microsoft Learn
https://learn.microsoft.com/ja-jp/entra/identity/authentication/how-to-enable-passkey-fido2
Okta FastPass | Okta Identity Engine https://help.okta.com/oie/ja-jp/content/topics/identity-engine/devices/fp/fp-main.htm

により、偽サイトへの情報流出を入口で阻止することが可能です。また、「デバイスの制御 [2]」を併用し、組織が許可した端末以外からのアクセスを排除することで、アカウント不正利用に対する防御を一層強化することが可能となります。

【サポート詐欺被害の増加】

当該期間では、サポート詐欺に関する相談件数が増加しています。サポート詐欺とは、Web サイト閲覧中に「ウイルスに感染した」といった偽警告画面を表示し、閲覧者の不安をあおることでサポート窓口を名乗る攻撃者の電話番号へ連絡させ、「LogMeIn Rescue」や「UltraViewer」などの遠隔操作ソフトウェアの導入させるとともに、サポート費用名目で金銭を要求する攻撃手法です。

偽の警告画面が表示される要因としては、ニュースサイトや個人ブログなど正規サイトに設置された広告枠へ悪意あるバナー広告が配信される事例が確認されています。また、近年では生成 AI を悪用した詐欺の巧妙化が顕著となっており、偽警告画面に加え、AI 生成の音声や映像を用いて正規企業のサポート担当者を装うケースも報告されています。ビデオ通話や録音を利用し「緊急対応」を名目に利用者へ圧力をかける事例も報告されており、暗号資産や偽投資を絡めた詐欺で数百万円規模の高額被害が発生しています。

Web サイト閲覧中にウイルス感染などの警告が突如表示された場合には、まずはサポート詐欺の可能性を疑う必要があります。表示された電話番号には連絡せず、落ち着いて Web ブラウザを閉じることで被害は回避可能です。相談の多くは、リモートワーク環境や休日など周囲に相談できない状況下で、利用者が個人で偽警告に対応しようとしたことが発端となります。

組織のセキュリティ担当者としては、ウイルス感染などのセキュリティインシデントが疑われる場合における組織内の報告窓口や相談先などの連絡先を明確に定める必要があります。併せて、それら連絡先を継続的に周知、啓発する運用体制を整備することも重要です。また、セキュリティ教育を実施して利用者にサポート詐欺がどのような事例か認識させるとともに、疑わしい事案が発生した場合には速やかに指定された連絡先に一報を入れるよう周知することも求められます。

---

[2] Microsoft Intune のデバイス コンプライアンス ポリシー - Microsoft Intune | Microsoft Learn
https://learn.microsoft.com/ja-jp/intune/intune-service/protect/device-compliance-get-started
条件付きアクセス ポリシーで条件を使用する方法 - Microsoft Entra ID | Microsoft Learn
https://learn.microsoft.com/ja-jp/entra/identity/conditional-access/concept-conditional-access-conditions
マネージド Windows コンピューターに Okta Device Trust を強制適用する | Okta Classic Engine
https://help.okta.com/ja-jp/content/topics/mobile/okta_mobile_device_trust_windows-desktop.htm
デバイス | Okta Identity Engine https://help.okta.com/oie/ja-jp/content/topics/identity-engine/devices/devices-main.htm

JSOC で観測したサイバー攻撃傾向

重要インシデントのトピックス

2025 年 10 月から 12 月に発生した重要インシデント（検知件数の多寡を問わず攻撃の成功を確認もしくは被害が発生している可能性が高いと判断されるセキュリティインシデント）の合計件数は 157 件でした。内訳はインターネットからの攻撃によるインシデントが 11 件（7.0%）、ネットワーク内部からの通信によるインシデントが 146 件（93.0%）であり、ネットワーク内部からの通信によるインシデントは前四半期と比較して減少しました。

1）インターネットからの攻撃により発生した重要インシデント

React Server Components に存在する脆弱性（CVE-2025-55182）を狙った攻撃によるインシデントが発生しました。本脆弱性を悪用された場合、遠隔の攻撃者によって任意のコードを実行される可能性があります。また、悪用可能な情報が公開された直後から積極的な探査・攻撃活動を多数検知していることから、自組織で利用している製品やソフトウェアの脆弱性が公開された際には業務影響を考慮のうえ、速やかに対策を実施することが重要です。そのほかには第三四半期に引き続き、DNS Amplification 攻撃の踏み台にされた可能性を示す通信によるインシデントが発生しました。今一度、外部に公開しているサーバなど、お客様環境の各機器の設定が適切であるか確認することを推奨いたします。図 4 に 2025 年 10 月から 12 月の重要インシデントの内訳を示します。

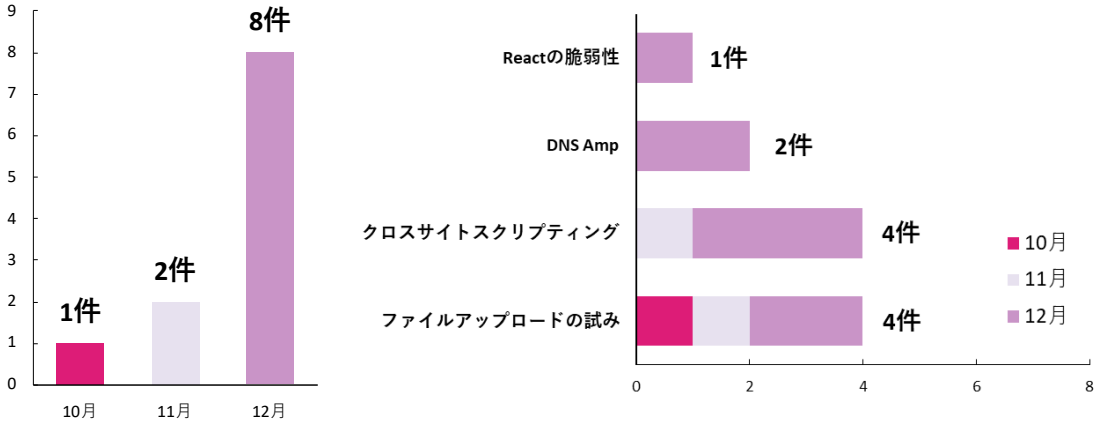

図 4 [外部から] 2025 年 10 月から 12 月の重要インシデントの内訳（月別・種類別）

2) ネットワーク内部から発生した重要インシデント

マルウェア感染に起因する重要インシデントが多く発生しました。発生したマルウェア感染インシデントでは、ハードウェア情報や保存されているログイン情報などの窃取を行う Arechclient2 に感染したことに起因する通信や、ファイル感染型マルウェアの一種である Neshta に感染したことに起因する通信を検知しました。マルウェア以外に分類している重要インシデントは、監視対象ホストから外部に対する不審な通信や不審なドメイン名の名前解決の通信を検知したことによるインシデントのほか、攻撃者がインターネット上に配置した不審なファイルの取得を行う通信を検知したことによるインシデントが発生しました。これらのインシデントの一部は React の脆弱性（CVE-2025-55182）の悪用によって発生した可能性が高いと考えられ、暗号資産のマイニングを行うスクリプトを含むファイルを取得していました。図 5 に 2025 年 10 月から 12 月の重要インシデントの内訳を示します。

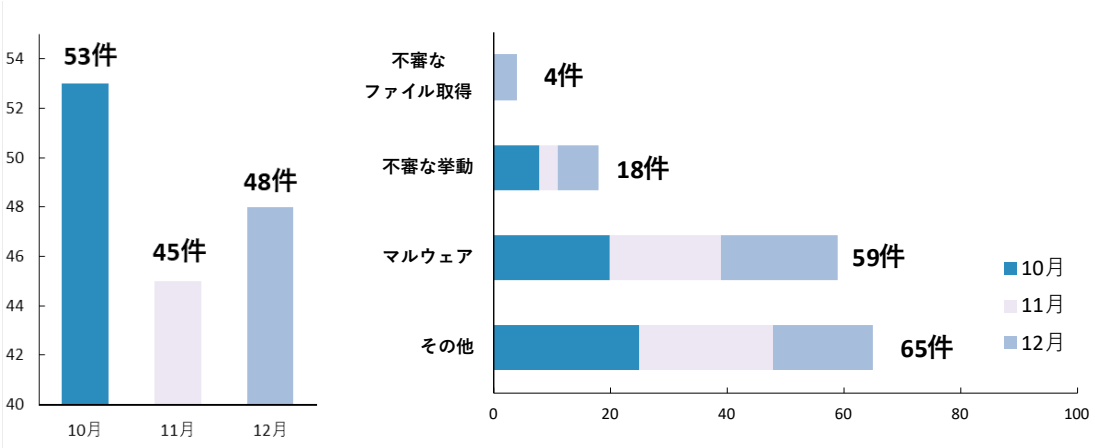

図 5 [内部から] 2025 年 10 月から 12 月の重要インシデントの内訳（月別・種類別）

EDR 製品の検知による重要インシデントは 20 件発生しました。マルウェア感染につながる挙動を検知したことによるインシデントが 2 件、攻撃者によって行われた可能性のある不審な挙動を検知したことによるインシデントが 18 件でした。これらのインシデントの主な発生原因は、ユーザによる不審なファイルの実行によるものと考えます。対策として、インターネット上の身元不明の不審なファイルやメールに添付されているファイルを安易に実行しないように、ユーザへの教育を徹底することが重要です。また、ユーザ操作に起因するインシデント以外に、WSUS の脆弱性（CVE-2025-59287）を悪用したと考えられる重要インシデントも発生しました。本脆弱性が悪用された場合、遠隔の攻撃者により認証不要で任意のコードが実行される恐れがあります。このようなインシデントを未然に防ぐためにも、公開する必要のないソフトウェア・製品の公開方針を見直し、公開が不要であるならばアクセス制限のような対策を講じることが重要です。

注意が必要な通信

注意が必要な通信や、大きな被害には発展していないものの検知件数が多い攻撃通信を、下表で紹介します。

表 2 注意が必要な通信について

概要	JSOC の検知内容	検知時期
GeoServer の脆弱性（CVE-2025-58360）を狙った攻撃	短期間に集中して特定の送信元から GeoServer の脆弱性（CVE-2025-58360）を狙った攻撃を多数検知しました。	12 月 2 日～ 12 月 5 日
アクセス可能な ElasticSearch を探査する目的の通信	特定の IP アドレスレンジから ElasticSearch のインタフェースにアクセス可能か探査する通信を多数検知しました。	9 月 26 日～ 10 月 3 日
SysAid 製品に存在する脆弱性（CVE-2025-2775）を狙った攻撃	短期間に集中して特定の送信元から SysAid 製品に存在する脆弱性（CVE-2025-2775）を狙った攻撃通信を多数検知しました。	11 月 28 日

特集：2026 年の脅威予測 #1

～ JSOC アナリストが考える ～

2025 年の脅威傾向

下図は 2023 年から 2025 年における過去 3 年間の脅威の検知件数を攻撃種別ごとに集計し、総計順で上位 10 位の推移を示したものです。2025 年の攻撃と判断した通信の検知件数は約 29 億件でした。

攻撃種別に着目して分析すると、2025 年と 2024 年との比較では、IoT 機器などを狙ったリモートからの「コマンド実行の試み」を目的とした攻撃が増加したことを確認しています。当該攻撃の増加は台湾製の IoT 機器の脆弱性を狙った攻撃や、無線機器向け SDK に存在する脆弱性を狙った攻撃の増加が原因でした。SDK などサプライチェーンに関連する製品の脆弱性は影響が広範囲に及ぶ可能性があります。セキュリティ対策の強化とともに、セキュリティインシデントに迅速に対処できる体制作りも重要です。

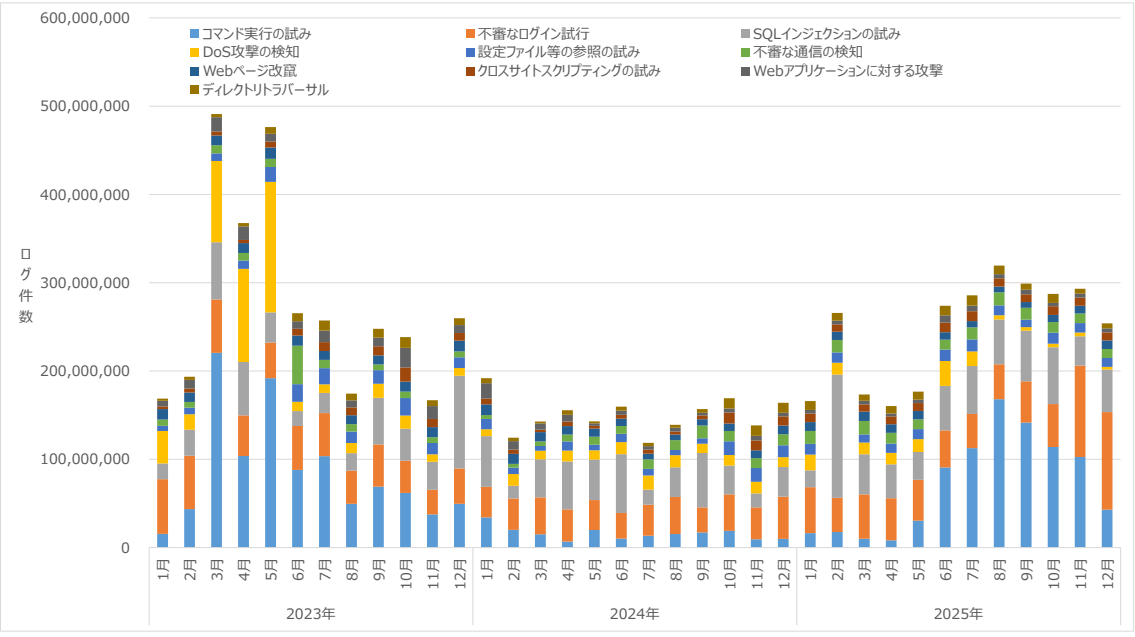

図 6 2023 年から 2025 年の攻撃種別の脅威検知件数

EDR 製品で検知した重要インシデント

2025 年、JSOC ではユーザ操作に起因する重要インシデントを多く検知しました。その多くは最終的にマルウェア感染に至っており、情報窃取などの被害が発生している可能性がある事例も確認しています。このため、ユーザを狙ったこれらの攻撃に対しては細心の注意が必要です。

ユーザ操作に起因するインシデントでは、攻撃者がさまざまな手法でユーザを誘導し、悪性コマンドやスクリプト、不審なファイルを実行させようとする傾向が目立ちました。JSOC で検知した代表的な手口として ClickFix、偽装インストーラー、メールの添付ファイルが挙げられます。ClickFix は、偽の警告や CAPTCHA 画面を装い、ユーザ自身に悪性コマンドなどを実行させる手法です。偽装インストーラーやメール添付ファイルは、正規ソフトウェアや請求書・業務連絡などを装った悪性ファイルをユーザに開かせ、端末をマルウェアに感染させる例が観測されました。特に ClickFix は、ラックでも注意喚起を行いましたが、観光業の業務特性を悪用した攻撃事例も確認されています。この手法は今後さらに高度化・巧妙化することが予想されるため、引き続き警戒が必要です。

ユーザ操作に起因する攻撃への対策として、不審なメッセージやポップアップの指示に従わないことが基本となります。ただし ClickFix のような手法は正規の画面を巧みに模倣するため、見た目だけで不審と判断することは困難です。そのため、Web サイトやポップアップからコマンドのコピー＆ペーストを求められた場合や、PowerShell・「ファイル名を指定して実行」への入力を指示された場合は、安易に従わないよう組織内で注意喚起を行うことが重要です。また、業務影響を考慮する必要はありますが、多くの組織では、PowerShell の実行や「ファイル名を指定して実行」をグループポリシーで禁止することも有効な対策となります。

EDR 製品ではユーザ操作に起因する重要インシデントを多く検知した一方で、システムの脆弱性を悪用して攻撃者の指定するコマンドが実行された事例も検知しています。具体的にはサーバ上実行されているプロセスを介して外部からスクリプトファイルを取得し、実行を試みる挙動を検知しました。JSOC にて当該ファイルの内容を確認したところ、マルウェアと思われる実行ファイルを保存し実行するものでした。

このような脆弱性を悪用した攻撃の対策としては、修正パッチの適用のほか、インターネットを中心とした外部向けに公開しているサーバやサービスなどのアセットを今一度確認し、アセットの公開範囲を再検討することも重要です。不要なアセットは非公開とするか、適切なアクセス制限を設けることで、攻撃者に悪用されるリスクを低減できます。

2026 年はこうなる

2025 年は、2024 年と比較して IoT 機器などを狙った攻撃の検知が増加しました。これらの攻撃の多くはマルウェア感染を試みるものでした。また、EDR 製品についても、マルウェア感染につながる事例を多く観測しました。サイバー空間における攻撃活動は、機器の脆弱性や心理面での脆弱性の両面を積極的かつ巧妙に悪用し続けている状況です。2026 年も、その傾向は継続・拡大すると考えます。

2025 年の傾向を踏まえ、2026 年は以下に記載するような攻撃の増加も懸念されるため、注意が必要です。

人の脆弱性を突く脅威の継続・増加（ソーシャルエンジニアリング）

継続して活発な活動がみられているフィッシング攻撃などのほか、2025 年はユーザが悪性スクリプトなどの実行に誘導されるような攻撃活動が目立ちました。

その代表である ClickFix は、偽の警告や CAPTCHA 画面などで、悪性スクリプトの実行へユーザが誘導させられる手法であり、JSOC でも本手法による攻撃活動を多数観測しました。本手法は、FileFix 等の亜種の登場や、2025 年 10 月の Windows 10 のサポート終了に関連した警告や偽のアップデート画面など、ユーザの心理的脆弱性を巧みに突いた攻撃が次々に現れています。これらはメールやマルバタイジング、SNS を利用して急激に拡散されました。さらに ClickFix を悪用した攻撃が比較的容易に実施できる「ClickFix Generator」が現れ、他のフィッシングと同様にビジネスモデルとして確立されてきています。

ClickFix のように、ユーザの心理的脆弱性を狙った攻撃はソーシャルエンジニアリングと呼ばれており、攻撃者によって積極的に様々な手法が開発されています。ソーシャルエンジニアリングでは、2022 年に公開された手法として「Browser-in-the-Browser」という手法が 2025 年になってから再度使われているとの情報があります。これは、ブラウザの中にログインページなどを模した偽の画面を表示させ、情報を窃取する手法です。この偽の画面は、正規のサイトの URL が表示されており、ブラウザからポップアップしたかのように見せかけられていますが、実際はページ内に表示されているコンテンツです。従来のフィッシング対策の一つである「正規ドメインであるかの確認」ができないことが特徴であり、ClickFix 同様に利用者を巧みにだます手法であるといえます。現在は認証情報の窃取を目的としたフィッシング手法として存在が確認されていますが、今後は類似した手法を用いて最終的にマルウェア感染に至らせる攻撃が現れる可能性も考えられます。さらに人をだますために、AI により自然な日本語の文面で表示するなどの手口を使っていることが垣間見えます。これらのような攻撃者による AI の活用はより進み、攻撃を受ける側が対策しきれなくなるリスクも含んでいるかと考えます。

このような状況の対策としては、ユーザのセキュリティ教育が重要です。一般的なソーシャルエンジニアリング対策に加え、ClickFix や Browser-in-the-Browser のような手法があるという事実を周知し、注意喚起することで、ユーザの意識レベルから対策をする必要があります。

ソフトウェアのプラグインを悪用した攻撃の増加

Edge や Chrome 等のブラウザや Visual Studio Code などのテキスト編集ソフト等には、プラグインによる機能追加に対応しています。これらの多くは専用のプラットフォームに公開されており、ユーザはそのプラットフォームから自由に好きなものを選び、容易にインストール・有効化することが可能となっています。

2025 年においても、これらのプラグインの仕組みを悪用し、無害なプラグインを装って情報窃取を試みる攻撃活動を観測しました。これらのプラグインの中には、公開導入当初は悪性挙動を取らず正規のプラグインとして振る舞い、一定の評価とダウンロード数を得てから、プラグインの更新により悪性化するというものも存在します。

また、ユーザが意図せずに悪意のあるプラグインをインストールしてしまう事例の他にも、マルウェア感染や攻撃後に、さらなる侵害活動として悪意のあるプラグインをソフトウェアに導入・展開するような攻撃も報告されています。プラグインはその性質上、従来の IT 資産管理ソフトウェアなどによるインストール制御が不可能な場合があり、ユーザもプラグインの追加に気づかずにソフトウェアの利用を続行してしまう可能性があるため、こちらも注意が必要です。

またブラウザなどではログインにより、アカウントにて適用していたプラグインが自動で連携され悪意のあるプラグインがインストールされてしまう事例も発生しています。

プラグインは、特に昨今の AI 活用の流れから、既存ソフトウェアに AI 技術を手軽に導入できる手段として注目されている状況であり、様々なものが公開されています。しかし、注目度の高さに伴って、攻撃者も悪意のあるプラグインを配布する場として攻撃活動を活発化させていく可能性があります。

今一度、ソフトウェアに対するプラグインの導入では、導入の必要性を十分に検討した上で、導入当時の評価やレビューの確認が必要です。また、提供元の確認、インストール後も定期的に利用プラグインについての情報収集も重要です。また、必要に応じて、プラグイン利用の制御などもご検討ください。

特集：2026 年の脅威予測 #2

～ サイバー救急センター脅威情報アナリストが考える ～

2025 年の脅威傾向

2025 年は、2023 年からの 3 年を振り返ると出動件数が最も少ない年となりました（図 7）。一方、前年同月比では 9 月以降に明確な増加が見られ、年末（10～12 月）はここ 3 年で最も多い水準となりました。特に、React Server Components の脆弱性（CVE-2025-55182）や、12 月に顕在化した Cisco 製品のゼロデイ脆弱性（CVE-2025-20393）への対応で複数の出動が発生しました。さらに、正規アカウントを悪用した不正侵入事案への対応が増加したことも要因です。

ランサムウェア関連の事案対応は依然として毎月のように発生していますが、出動件数としては減少しています。しかし、2025 年には国内の大手企業における被害が世間の大きな注目を集めました。こうした危機感の高まりを背景に、直接的な侵害を受けていない組織でも、攻撃者の潜伏やバックドアの有無を確認するために、サーバ健全性調査（サーバが侵害されていないことを確認する調査）を実施するケースもありました。

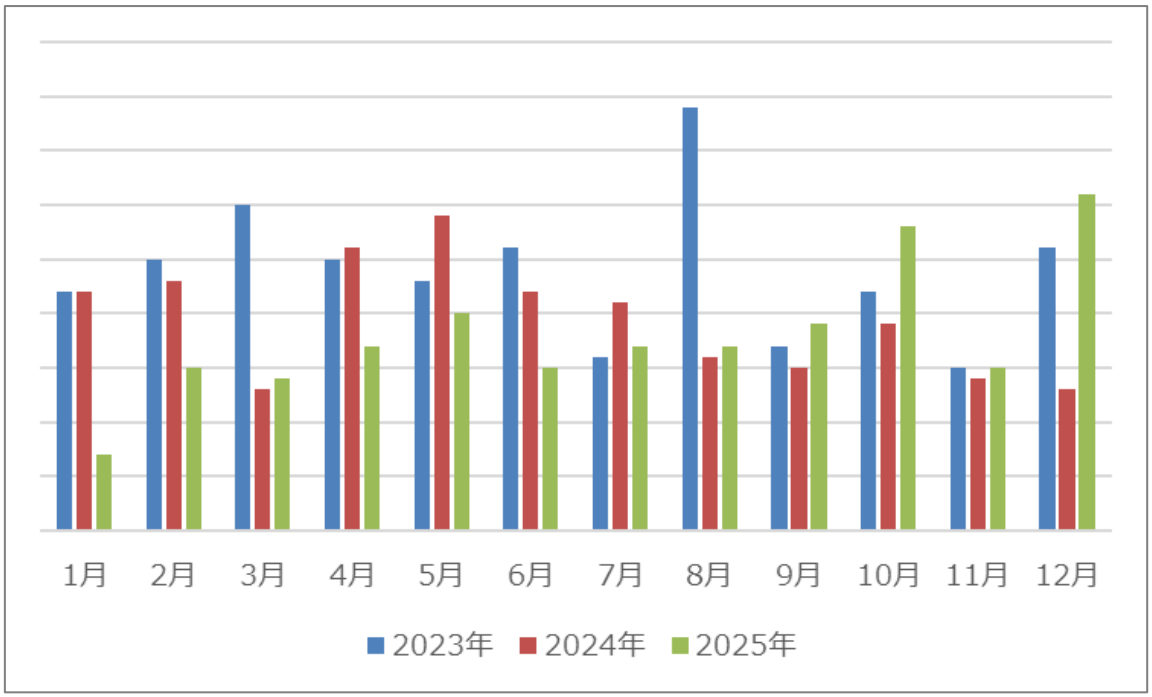

図 7 2023 年から 2025 年の月別件数

2025 年のサイバー救急センターの出動傾向を振り返るにあたり、2023 年以降のインシデント傾向を図 8 に示します。

2025 年におけるマルウェア関連インシデントの出動（全体の 29%）は、ここ 3 年間で減少傾向にあります。一方で、サーバ不正侵入関連のインシデント（全体の 43%）は、過去 3 年間で最も高い水準となりました。実際に、アカウントの不正利用を伴う VPN 経由の侵入など、大規模なインシデントが継続的に発生しています。

マルウェア関連インシデントは、単一端末でのマルウェア感染に起因する出動は減少しており、EDR 製品の導入拡大により、ユーザ組織内での初動対応や EDR 監視の段階でクローズされるケースが増えているものと考えられます。実際、弊社からも注意喚起を行っている ClickFix などの手法を用いた情報窃取型マルウェアに伴う出動は限定的でした。

一方、サーバ不正侵入関連のインシデントは、EDR 監視を契機とする出動では、AD サーバにおける認証情報の取得を試みる動きに関するアラートが複数発生しており、そのまま出動につながった事例も見られました。また、AD サーバの調査を行う中で、EDR 製品を導入できない仮想基盤への侵害が確認されるなど、仮想基盤を起点とした侵害行為を行う傾向にあります。

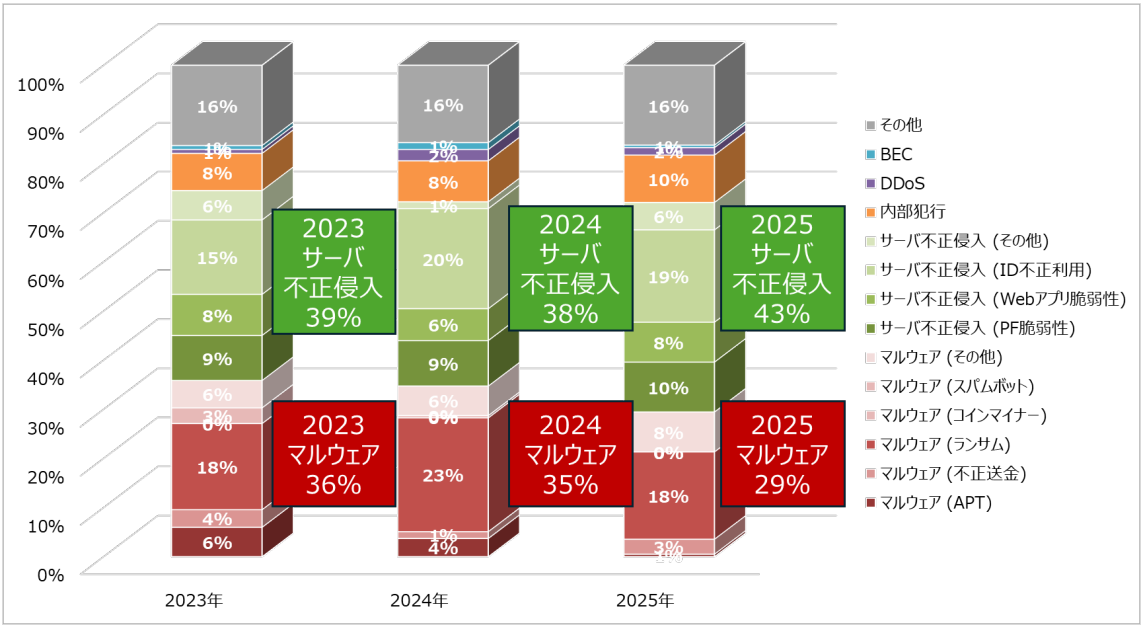

図 8 2023 年から 2025 年のインシデント傾向

マルウェア関連のインシデント傾向

2025 年のマルウェア関連のインシデントで最も多かったのは、ランサムウェアに関する出動でしたが 18%と 2024 年と比較しても 5%低下しています。

APT（標的型攻撃）に関する出動は、2024 年の 4%から 2025 年には 1%へと減少しました。ただし、APT に分類されていなかった事案（サーバ不正侵入のプラットフォーム脆弱性としてご相談いただいたもの）について、詳細調査を実施したところ、Ivanti Connect Secure の脆弱性（CVE-2024-21893 および CVE-2024-21887）を起点に組織内へ侵入され、その後、新たな PlugX 亜種である「MetaRAT[3]」を使用していたことが判明しました。当該事案に対しては、出動対応に加え、大規模な調査を実施しました。その他に、EDR 監視サービスの中で標的型攻撃に利用されるダウンローダや RAT の検知から検体の任意調査を行うものが 10 月以降毎月のように発生している状況です。特定組織に対する標的型攻撃メールも確認している状況であるため、引き続き標的型攻撃にも注意が必要です。

不正送金に関する出動は、2024 年の 1%から 2025 年には 3%へと微増しました。国内における観光業を標的とした攻撃 [4]が 2025 年も継続したことと、ClickFix[5]などの手法を用いた攻撃に関する出動も一定数ありました。ClickFix などの手法を用いた外部サイトからの情報窃取型マルウェアへの感染には、引き続き注意が必要です。

サーバ不正侵入関連のインシデント傾向

サーバ不正侵入関連のインシデントで最も多かったのは、ID の不正利用によるサーバへの不正侵入で、全体の 19%を占めます。前年（2024 年）比では 1%減となったものの、高い水準が継続しており、2025 年も認証情報の不正利用による事案が多発しました。Microsoft 365 では、何らかの手口で窃取された認証情報を悪用し、多要素認証（MFA）の未適用や条件付きアクセスの設定不備を悪用した不正ログインが確認されています。その結果、グローバル管理者アカウントの不正利用や、外部へのスパムメール大量送信といった事案が相次ぎました。

また、AWS でもアクセスキーや API キーの流出による不正アクセスが発生し、環境の不正操作やリソー

---

[3] MetaRAT を利用した日本組織を狙った攻撃キャンペーン
https://www.lac.co.jp/lacwatch/report/20251208_004569.html

[4] 観光業を標的とした攻撃が ClickFix を利用して再来
https://www.lac.co.jp/lacwatch/alert/20250825_004472.html

[5] ClickFix の被害を JSOC の複数のお客様にて観測
https://www.lac.co.jp/lacwatch/alert/20250519_004380.html

スの悪用、スパムメール送信が確認されています。これらは自組織の社会的信用の失墜だけでなく、プラットフォーム側での利用制限や予期せぬコスト負担を招くリスクにもなります。

OS やミドルウェアなどのプラットフォームの脆弱性に関する出動は、前年比（2024 年）比で 1%微増し 10%を占めています。特に多かった相談は昨年に引き続き Ivanti Connect Secure の脆弱性に関するものがありました。その他には、VPN 機器では Array AG の脆弱性を悪用や FortiGate を起点とした侵害のケースもありました。

VPN 機器以外では、Cisco 製品のゼロデイ脆弱性（CVE-2025-20393）や SharePoint の脆弱性（CVE-2025-53770, CVE-2025-53771）、Next.js の脆弱性（CVE-2025-66478）を発端とした出動がありました。

Web アプリケーションの脆弱性に関する出動は、2024 年の 6%から 2025 年には 8%へ微増しています。Movable Type や WordPress 等の CMS（コンテンツ管理システム）における脆弱性や設定不備を突かれ、サイト改ざんやデータベース内のコンテンツ改変、バックドア設置に至る事案が確認されました。また、SQL インジェクションによる被害も依然として継続しています。入力値検証の不備や ORM（オブジェクト関係マッピング）の設定不備を突いた攻撃により、認証情報の窃取や内部データの抽出、WebShell の配置を許す深刻な事例が発生しました。設計・実装上の不備を狙う攻撃は、古典的でありながら、今なお有効な脅威として深刻な影響を及ぼしています。

2026 年はこうなる

2026 年も引き続き大規模なランサムウェア攻撃、正規のアカウントを用いた VPN 経由の不正アクセスが継続すると考えられます。2025 年には、国内の大手企業において、基幹システムの停止に伴う出荷・物流の長期停滞が発生し、サプライチェーン全体を揺るがす深刻な被害が世間の大きな注目を集めました。これらの事案は、ランサムウェアが単なるデータの暗号化にとどまらず、経営基盤を直接破壊する「事業停止リスク」そのものであることを浮き彫りにしました。

侵入経路としては、2026 年でも SSL-VPN 機器が主要なターゲットになると推察しますが、機器自体の脆弱性だけでなく、フィッシングや情報窃取型マルウェアあるいは正規ソフトを模倣した偽アプリによって窃取された「正規アカウント」による不正アクセスにも引き続き対策が必要です。また、昨年は、ネットワークアプライアンスの脆弱性（Cisco 製品の CVE-2025-20393、Array Networks 製品の CVE-2025-66644 等）に加え、React Server Components の脆弱性（CVE-2025-55182）を突く攻撃も確認されました。このようなモダンな Web フロントエンドライブラリの脆弱性からサーバセグメントへ直接侵入する手口にも警戒する必要があると考えられます。

昨今の攻撃者の侵入後の活動として、仮想化基盤（VMware ESXi/vCenter 等）を執拗（しつよう）に狙う傾向があります。攻撃者は仮想基盤に SSH 等で侵入して Web シェルやトンネリングツールを配置し、そこを起点に別拠点の仮想基盤や AD サーバ、ファイルサーバといった重要資産にアクセス可能なノードへ横展開を行います。特に AD サーバへの侵害では、NTDS.dit の取得等によりドメイン特権が奪取され、オンプレミスと連携する EntraID（旧 AzureAD）側へと被害が波及する可能性があります。

このような背景から、インターネットからアクセス可能なすべてのアセットの把握、脆弱性情報の収集とパッチの適用、VPN 等の境界防御の強化、ドメインコントローラを含む全サーバへの EDR 製品の導入およびアカウント管理・運用の徹底が不可欠です。また、攻撃者が組織内のシステムの構成やアカウントなどの情報を入手しているということを前提に多層的に対策を講じた上で、定期的に特定のシナリオに基づいてスレットハンティング（システム内部に既に侵入している脅威を、セキュリティ専門家が能動的に調査する手法）を実施することが組織に求められています。

さらに、技術面以外の課題として、国内で策定した対策が海外拠点の担当者によって確実に実行されないというガバナンスの欠如や、データ越境移転規制（データ主権）により日本側から詳細なフォレンジック調査が行えないといった組織的・法的障壁が被害発生時に挙げられることがあります。このような問題に対して、組織として具体的にどのように対策を講じ、グローバル全拠点で対策の実行力をいかに担保していくかが、今後の事業継続を左右する鍵になると考えられます。

アンケートのお願い

今後のよりよい記事づくりの参考とさせていただくため、以下の URL または QR コードから、アンケートに回答いただけると幸甚です。忌憚のないご意見・ご感想をお寄せください。

https://jp.surveymonkey.com/r/GCMHRBT

【memo】

【memo】

株式会社ラック
〒102-0093
東京都千代田区平河町 2-16-1
平河町森タワー
https://www.lac.co.jp/