加速するサイバー攻撃のライフサイクルを解読

Rapid7 2026年版グローバル脅威動向レポートに関するCISOのための概要

経営幹部の視点：スピードはもはや強みではない

2025年のセキュリティが失敗に終わったのは、防御側の動きが遅かったからではありません。スピードが差別化要因ではなくなったためです。

今年の脅威データの特徴は加速です。攻撃者は根本的に新しい手法に頼るのではなく、既知のプレイブックをより速く、大規模に、より厳格な運用規律で実行しています。自動化、人工知能（AI）、サイバー犯罪エコシステムの産業化により、エクスポージャーから影響までの時間が短縮され、かつては数週間かかったことが、今では数日、時には数分で済むこともあります。

CISOにとって、これは運用モデルの変革の必要性を意味します。重要な問題は、もはやどれだけ早く対応できるかではなく、攻撃者が悪用する前にどれだけエクスポージャーを減らすことができるかです。

1. 予測の窓は閉ざされた

2025年の最も重大な変化は、防御側が攻撃を予測、検知、軽減する時間が事実上失われたことです。新たに公開された**CVSS 7–10の脆弱性の悪用が確認された件数は前年比で105%増加（2024年は71件、2025年には146件）しました。**2022年から2025年までの4年間で悪用された脆弱性は7件から146件に増加し、公開件数に対する悪用率は0.1%未満から0.8%に上昇しました。

対応までの期間も短縮されました。公開からCISAの「既知の悪用済み脆弱性（KEV）」リストへの登録までの期間の中央値は8.5日から5.0日に、平均値は61.0日から28.5日に短縮されました。一方、「高リスクだがまだ悪用されていない」というカテゴリーは、ほぼ消滅しました。2024年には、悪用予測スコアリングシステム（EPSS）スコアが0.7以上でありながら悪用が確認されていない脆弱性が338件ありましたが、2025年にはわずか65件に減少しました。Emerging Threat Responseのデータセットでは、**「リスクは高いがまだ悪用されていない」脆弱性は15件から1件に減少し、**悪用が確認された脆弱性は5件から22件に増加しました。

重大な脆弱性の存在は、もはや確率ではなく、運用上の前提条件となっています。従来の優先順位付けサイクルは攻撃者のタイムラインと整合していません。2025年、SOC は処理量の多さに圧倒されることはなかった。速度で圧倒されました。

2. 攻撃者は管理されていないエクスポージャーを収益化

2025年の侵入事件の多くは、新たなゼロデイ攻撃ではなく、防ぐことができたはずの脆弱性の暴露から始まっていた。**多要素認証のない有効なアカウントはインシデントの43.9%を占めています。**脆弱性の悪用は24.6%、露出したサービスは7.0%でした。

アンダーグラウンド市場の動向も同様のパターンを示しています。**出品のうち、リモートデスクトッププロトコル（RDP）アクセスが21.2%、VPNアクセスが12.8%、RDWebが11.2%を占めました。**ドメインレベルの権限が広く提供されており、アクセス権は日常的にパッケージ化されて販売されていました。わずか6ヶ月間で、DarkForumsには221件、RAMPには208件のアクセス提供情報が掲載されました。被害を受けた組織からの平均推定売上高は32億ドルを超え、出品1件あたりの平均基本価格は113,275ドルでした。初期アクセスブローカーはエクスポージャーを産業化しています。彼らは認証情報を収集し、アクセスを検証し、それを在庫として販売しており、合法的な企業が行うような方法で活動しています

3. 攻撃は、確実に悪用できる脆弱性クラスに集中している

重大および最重要のCVEの総数は前年比で約16,200件から18,100件に緩やかに増加しましたが、悪用の規模は均等ではなく、攻撃は、限られた数の確実な脆弱性クラスに集中していました。

2025年には、CWE-502（デシリアライゼーション）が最も多く悪用された根本原因であり、認証バイパスやメモリ破損も一貫して上位にランクインした。注目度の高いランサムウェア攻撃は、ファイル転送システム、コラボレーションプラットフォーム、エッジアプライアンスにおけるデシリアライゼーションの脆弱性と認証バイパスを標的としていた。

対照的に、クロスサイトスクリプティングやSQLインジェクションといった大量の情報漏洩は、確認された攻撃事例ではかなり少なかった。攻撃者は信頼性、事前認証アクセス、そしてスケーラブルなリモートコード実行を優先しています。

脆弱性管理プログラムでは、単なるCVEの数ではなく、悪用可能性、資産の役割、エクスポージャーのコンテキストに基づいて優先順位付けを行う必要性を強調しています。

4. ランサムウェアは スピード重視のアクセス経済へと成熟

2025年もランサムウェアは依然として主要な攻撃手法であり、**Rapid7 MDR 調査件数の42%を占めました**。リーク投稿は2024年の6,034件から2025年には8,835件に増加し、**46.4%**の増加となりました。アクティブなランサムウェアグループは102から140に増加し、グループあたりの平均投稿数も増加しました。

リーク投稿数ではQilinが1,029件でトップとなり、AkiraとCl0pがそれに続きました。二重恐喝とサービスとしてのランサムウェア（RaaS）モデルがエコシステムを支配しました。データ窃盗は暗号化に先行することが多く、これは迅速に最大限の交渉力を得るために考案された、「スマッシュ＆グラブ」恐喝戦術を反映しています。

重要なのは、ランサムウェア インシデントのほとんどが、侵入認証情報、公開されたVPNまたはRDPサービス、パッチが適用されていないエッジインフラストラクチャなどの予測可能な経路から発生していることです。これは単なるランサムウェアの問題ではなく、管理が行き届いていない脆弱性が悪用され、金銭的利益が得られる段階なのです。

5. 「戦略的リスク」を決定づけるのは、境界の侵害ではなく、内部への侵入である

企業の伝統的な境界は消滅しました。攻撃者は、IDシステム、クラウドコントロールプレーン、コラボレーションプラットフォーム、ネットワークエッジインフラストラクチャを標的にしています。このような環境では、合法的なアクティビティと悪質な行為の境界線が曖昧になり、検知と封じ込めが複雑になります。

国家と連携するアクターは、長期的な活動継続のために、通信、クラウド環境、インフラストラクチャ内に事前に拠点を構築している。犯罪者も同様に、これらの環境を利用して収益化を図っている。2025年に観測された事例としては、侵害されたSOHOルーターから構築された運用リレーボックスネットワーク、コマンド＆コントロールのためのコラボレーションプラットフォームの悪用、GraphQL APIの悪用、産業制御システムを標的とするFrostyGoopなどの専用マルウェアなどが挙げられます。

加速レイヤーであると同時にアタックサーフェスともなるAI

AIは、まったく新しい攻撃手法を導入するのではなく、既存の攻撃手法を強化したため、結果として、初期アクセスから被害発生までの時間が短縮されました。これは、脅威アクターが生成AI を使用してフィッシングと偵察の規模を拡大し、スクリプトを改良し、ランサムウェアの運用を加速させたことを示しています。

同時に、AI インフラが攻撃の標的となり、急速に進化するAI エコシステム内部で、これまで見られた弱点が露呈し始めていることが示されています。当社のデータからは、モデルサーバーにおける不適切なデシリアライゼーション、セルフホスト型プラットフォームにおけるトークンの漏洩、オーケストレーションフレームワークへのインジェクションリスク、および悪意のあるpostmark-mcp パッケージのようなサプライチェーンの侵害がすべて確認されました。

したがって、AI は特権的なインフラストラクチャとして管理されなければなりません。適切なインベントリ管理、アクセス制御、セグメンテーション、およびトークン監視は不可欠です。同時に、敵のスピードに追いつくために、AI で強化されたセキュリティ運用の必要性が高まっています。

業界別および地域別のターゲティング

北米が観測されたインシデントの82%を占め、米国はリーク投稿の約70%を占めています。製造業、ビジネスサービス、小売業が最も標的とされた業界であり、ヘルスケアと政府も大きな影響を受けました。

これらのセクターは、機密データ、財務的資金力、サプライチェーンへの影響力を兼ね備えており、恐喝や戦略的な事前配置の両方において魅力的な標的となっています。

2026年の戦略的ガイダンス

データは、攻撃の速度と従来の防御プロセスとの間に構造的な不一致があることを浮き彫りにしています。そのギャップを埋めるためには、運用モデルとして先制的セキュリティへの移行が必要です。

2026年にはCISO に以下のことを推奨します。

- アセットとアイデンティティの継続的な可視性の優先
- 一貫した多要素認証の実施
- エッジインフラストラクチャの強化
- SaaS とAI を本番環境で最も重要なシステムとして扱う
- 自動化とAI で検知と対応のワークフローを強化し、調査タイムラインを高速化

一部のエクスポージャーは悪用されるでしょう。現時点では、それはサイクルの自然な部分です。したがって、レジリエンス計画はその点を考慮に入れる必要があります。イミュータブルバックアップ、テスト済みの復旧手順、認証情報のリセット、インシデント対応プロセスの練習は不可欠な保護手段です。

最終的な結論

2026年の脅威状況は、加速化が特徴です。攻撃はより迅速になり、アクセスは商品化され、ランサムウェアは産業化されています。

しかし、根本的な脆弱性は新しいものではありません。弱い認証情報、公開されたセッション、パッチが適用されていないエッジシステムは、依然として一貫して使用されるベクトルです。変わったのは、そうした弱点が特定され、パッケージ化され、武器化されるスピードです。

CISO にとっての競争優位性は現在、エクスポージャーの明確さにあります。継続的にアタックサーフェスを理解し、悪用される前にリスクを軽減する組織は、加速するサイバー攻撃サイクルに最もよく耐えられる立場にあるといえます。

レポートを入手

RAPID7 について

Rapid7, Inc. (NASDAQ: RPD) は、AIを活用したマネージドサイバーセキュリティオペレーションのグローバルリーダーとして、組織のサイバーレジリエンス強化に貢献しています。オープンかつ拡張性のあるRapid7 Command Platformは、セキュリティデータを統合し、それをAI、脅威インテリジェンス、25年にわたる専門知識とイノベーションで強化することで、リスクを低減し攻撃者を阻止します。先制型マネージド検知/対応 (MDR) の分野で認められたリーダーとして、Rapid7はエクスポージャー管理と検知を統合し、世界11,500社を超えるお客様のサイバーセキュリティ運用を変革しています。詳細については、当社のWebサイトにアクセスするか、ブログをチェックするか、LinkedIn または Xでフォローしてください。

RAPID7

セキュリティを確保

クラウド | アプリケーション | インフラストラクチャ | ネットワーク | データ

加速を支援

Command Platform | エクスポージャー管理 | アタック・サーフェス管理 | 脆弱性管理 | クラウドネイティブアプリケーション保護 | アプリケーションセキュリティ | 次世代SIEM | 脅威インテリジェンス | MDRサービス | インシデント対応サービス | MVMサービス

攻撃者を凌駕するために構築されたセキュリティ

当社のセキュリティプラットフォームをリスクなしでお試しいただけます。
rapid7.comでトライアルを開始