2024年 攻撃インテリジェンスレポート

Caitlin Condon、脆弱性インテリジェンス担当ディレクター
Stephen Fewer、主任脆弱性リサーチャー
Christiaan Beek、脅威分析担当シニアディレクター

RAPID7

目次

概要

Rapid7は2020年以来、厳選された脆弱性データとエクスプロイトの傾向に関する詳細な分析をまとめた脆弱性インテリジェンスレポートを毎年リリースしています。今年はタイトルを「攻撃インテリジェンスレポート」と改め、調査範囲を広げました。攻撃状況をより包括的に把握できるようにするため、脆弱性とエクスプロイトの調査をRapid7のマネージド検出応答サービス（MDR）部門、脅威分析チーム、新興脅威対応チームからの実践的なデータを活用しています。

2024年版攻撃インテリジェンスレポートでは、セキュリティ担当者が最新のサイバー脅威をより深く理解し、予測するために役立つ洞察とガイダンスをご紹介します。今年のレポートでは、最近の影響の大きい攻撃とCVEの調査に加え、複数年にわたる脆弱性とエクスプロイトの傾向に焦点を当てています。この調査は、2019年末以降に公開された210件以上の脆弱性（2023年および2024年初に悪用された60件以上の脆弱性を含む）に基づいています。脆弱性の選択に関する追加情報については付録をご参照ください。

主な調査結果

2023年には、ゼロデイ脆弱性による大規模な侵害イベントの発生件数がNデイ脆弱性によるものを上回る ー この3年間で2度目2024年初までに新たに発見された広範囲にわたる脅威の脆弱性の53%は、ソフトウェアメーカーが修正を実装する前に悪用されました。この数値は、2022年の若干の小休止（43%）を経て、2021年の広範囲にわたるゼロデイ攻撃の水準（52%）に戻ったことになります。

2023年初からのネットワークエッジデバイスの悪用による大規模な侵害イベントはほぼ倍増し、広範囲に悪用された脆弱性の36%がネットワークエッジ技術内で発生しています。Rapid7が2023年に分析したネットワーク・セキュリティアプライアンスの脆弱性の60%以上が、ゼロデイ攻撃の形で悪用されました。

熟練した攻撃者は依然としてメモリ破損のエクスプロイトを好みますが、過去数年間に広く悪用されたCVEのほとんどは、コマンドインジェクションや不適切な認証の問題など、より単純で簡単に悪用できる原因から発生しています。

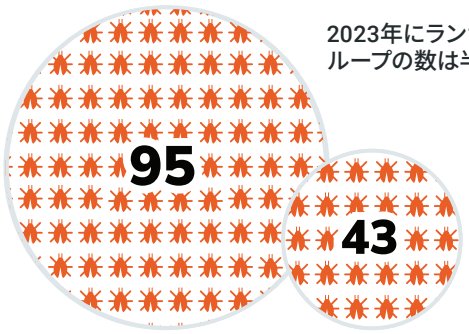
2023年にRapid7 MDRサービスチームが確認したインシデントの41%は、特にVPNと仮想デスクトップインフラストラクチャにおいて、インターネット接続システムの多要素認証（MFA）の実施が不完全か、そもそも実施していないことが原因でした。

Rapid7 Labsは、2023年から2024年の最初の数か月間に5,600件以上のランサムウェアインシデントを追跡しました。2023年に報告されたユニークなランサムウェアグループの数は、2022年の新規グループ数95件から2023年には43件へと半分以上減少しました。

Rapid7 Labsは

5,600

件の2023年から2024年初頭にかけて発生したランサムウェア事件を追跡



2023年にランサムウェアグループの数は半分以下に減少

全体像：脅威環境の変動

過去数年間、Rapid7の研究者は、世界中の多くの組織を脅かしてきた攻撃ベクトルを優先しながら、重大な脆弱性と主要なサイバーインシデントの詳細な分析を定期的に公開してきました。2020年当時、重大な脆弱性のエクスプロイトの「発生」と考えられていた状況下で、当社の研究チームは、広範に悪用されているCVEを、一般に単一の脅威アクターにより実行される限定的な標的型攻撃で使われるCVEとは別に追跡し始めました。Rapid7の最初の脆弱性インテリジェンスレポートには、これらの「広範囲にわたる脅威」、つまり多数の攻撃者と大規模で脆弱な標的層を伴う脆弱性が12件以上含まれていました。その当時、このリスクの高まりは新しいもので、説得力があり、警戒すべきものと見られました。

しかし、2021年以降の状況はそれまでの時期を大幅に上回るもので、「当時」と「現在」の間にはかなり深い隔たりが生まれました。ゼロデイ攻撃は急増し、新たなピークに達した後、高止まりの状況が続いています。数年前から追跡を開始した脆弱性の開示から攻撃までの日数の中央値は、当社の年次データセットのCVE全体で1桁台に留まっています。主要な脆弱性の広範な攻撃は、注目すべきイベントから、あって当然の予測に変わりました。ランサムウェア攻撃は定期的に一般ユーザー向けシステム全体をダウンさせ、この影響が数週間から数か月に及ぶこともあります。国家の支援を受けた攻撃者は、地政学的紛争をスパイ活動、ハクティビズム、サプライチェーンの妨害などの根拠と隠れ蓑の両方として利用し、セクター全体でアクティビティを活発化させています。

Rapid7の研究哲学には、誇大広告に対する心からの軽蔑が根付いています。変化する脅威の環境について語る際には、確固たる証拠、つまり「悪用された」と「悪用されていない」という二項分類を超えて収集・分析された証拠が必要となります。世界が変わったと言うならば、当社の研究理念では、その主張を裏付けるデータを作成することが必須となります。

世界は変わりました。前年と同様、2023年と2024年初に分析した脆弱性に関しては、ゼロデイ攻撃と広範な悪用が依然として一般的でしたが、一部の広範囲にわたる侵害イベントの発生方法には顕著な変化も見られました。

広範囲にわたる脅威のCVEのほぼ4分の1（23%）は「多数の攻撃者と多数の標的」という従来のパターンではなく、綿密に計画され、高度に組織化されたゼロデイ攻撃によるものでした。こうした攻撃では、1人の攻撃者が数十または数百の組織を一度に侵害し、しばしば独自のエクスプロイトやバックドアなどのカスタムツールを使用しています。これらは過去に見られたようなサイバー脅威ではなく、成熟し、高度に組織化されたサイバー犯罪エコシステムであり、アクセスを取得し、持続性を確立し、検知を回避するためのメカニズムがますます高度化しています。

実感として言えば、脅威の環境におけるこれらの複合的な変化を受け、ソフトウェア作成側にもいくらかの退行的な慣行が見られます。経験上、ベンダーがセキュリティ問題を公表することなく黙ってパッチを適用し、アドバイザリやCVEの説明を数日または数週間後まで保留することがよく見られます。多くのベンダーが意図的に脆弱性の詳細を見えにくくし、不明瞭にすることで敵対者を抑止し、ソフトウェアメーカーの評判リスクを軽減できるという、理解はできるものの誤った考えに基づいて、根本原因と攻撃ベクトル情報の公開を拒否しているようにも見えます。

最後に、セキュリティ市場全体が、脆弱性とエクスプロイト情報の民営化へとさらに大きく傾き始めている傾向が見られ、技術的な調査結果が営利目的やその他の理由で公開されず、非公開で共有されることが増えています。2022年後半からのTwitterの終焉の噂がこの傾向を悪化させ、幻滅したセキュリティコミュニティのメンバーの多くが、さまざまな代替プラットフォームや閉鎖的な情報共有サークルへの移行を選択しました。2024年3月現在、National Vulnerability Database（NVD）の将来に対する業界の懸念から、データベースの民間所有への移行が、公的管理の場合と比較して改善されるかどうかについて新たな議論が巻き起こっています。

これらは微妙な課題であり、単純な解決策はありません。多くの場合、疲れ果てたセキュリティ担当者から窮地に立たされているオープンソースの保守担当者、過小評価されている公共部門のアナリストまで、私たちの技術エコシステムの多くが依存している重要な人的インフラストラクチャに対する制度や業界に対するサポートは存在しません。民営化は強力な手段ですが万能ではありません。この選択肢を検討する際は、結果として何を諦めることになるかについても考慮すべきです。

脆弱性悪用の傾向

用語「エクスプロイト」に関する注記

2023年以降に当社のデータで「エクスプロイト」対象として分類された脆弱性は、すべて実際の本番環境で攻撃者により悪用されたことが確認されています。これは、当社脆弱性インテリジェンスデータセット内のCVEの実際の悪用に関する主な情報源として、サードパーティのハニーポットデータを時折使用していた過去数年の慣行とは異なるものです。

過去18〜24か月の間に、特定の攻撃関連用語が業界で広く採用されるようになりました。新しい脆弱性の「大規模なエクスプロイト」や「広範なエクスプロイト」を示唆する主張が増えていますが、さらに調査した結果、こうした「大規模エクスプロイト」が実際は悪用可能なコードパスなしでインターネットに遅延して公開された概念実証を意味していたケースも多数あります。これは、ライブラリの脆弱性やサードパーティコンポーネントの欠陥に関する脅威アクティビティの評価の際に特にリスクとなります。共有コンポーネントはテクノロジースタックにさまざまな方法や場所で実装されているため、多くの場合、リモートでアクセスできず、画一的なエクスプロイトで標的にしにくい傾向にあります。

ハニーポットのデータでは、スキャンや失敗したエクスプロイトの試みと、標的システムに対する真の侵入成功が区別されない（できない）ことが頻繁に観察されています。こうした技術的な制限は理解できるものですが、実環境では成功しそうにない不器用なエクスプロイトの試みが誤って「大規模なエクスプロイト」と解釈される可能性もあります。（公開されている概念実証コードなどを用いた）アクティビティやエクスプロイトの試みのスキャンは、攻撃者の関心の方向性を示す適切な指標となりえますが、攻撃者のスキルを示す指標にはめったにありません。周知のとおり、「脆弱であること」と「エクスプロイト可能であること」は同義ではなく、とりわけ、限られたテストケース外で成功する攻撃を開発および実行する十分な能力がなければ、その傾向が強くなります。インターネットに散らばる**ハニーポットの数が膨大であること**も、普及率の水増しと攻撃情報の不正確さの一因となっています。

本レポートで説明している脆弱性のいくつかはハニーポットの展開でも悪用されていますが、今後は、コード実行、ペイロード配信やその他の侵害の成功を示す忠実な兆候を確認できる場合にのみ、ハニーポットデータを悪用の信頼できる証拠として含めるよう、当社としての慣行を変更しています。これは、当社独自のハニーポットデータだけでなく、サードパーティのフィードにも適用されます。

2023年の広範囲にわたる新たな脅威

Rapid7の脆弱性研究者は、少数の組織にのみ影響する可能性のあるCVEではなく、多数の組織に影響を及ぼしうる可能性のあるCVEを優先します。大規模な攻撃と小規模なエクスプロイトを区別しており、ある脆弱性が悪用され、さまざまな業種や地理的な場所にまたがる多くの組織が侵害された場合、その脆弱性は**広範囲にわたる脅威**であるとみなします。広範囲にわたる脅威イベントの発生時に、組織は、緊急パッチプロトコルの有効化に加え、侵害の指標（IOC）とエクスプロイト後のアクティビティを探すインシデント対応調査の実施を想定する必要があります。

Rapid7の研究者は、2023年から2024年初にかけ広く悪用された30件を超える**新たな脆弱性**を追跡しました。以下のCVEの半分以上（53%）はゼロデイエクスプロイトから発生しており、Rapid7 MDRは顧客の環境で以下の脆弱性の多数が悪用されていることを確認しています。

2023年に多くの業種や標的組織で侵害を引き起こした、広く悪用された脆弱性には次のものがあります。

CVE-2023-0669 Fortra GoAnywhere MFTリモートコード実行	**CVE-2023-3519** Citrix NetScaler ADC/Gatewayのリモートコード実行	**CVE-2023-2868** Barracuda Email Security Gatewayのリモートコマンドインジェクション
CVE-2023-42793 JetBrains TeamCity CI/CDサーバー認証バイパス	**CVE-2023-24489** Citrix ShareFileの不適切なアクセス制御	**CVE-2023-29059** 3CXサプライチェーンの侵害
CVE-2023-34362 Progress Software MOVEit Transfer SQLインジェクション	**CVE-2023-20269** Cisco ASAおよびFTDの不正アクセス	**CVE-2023-46604** Apache ActiveMQのリモートコード実行
CVE-2023-40044 Progress Software WS_FTP Serverの信頼できないデータの逆シリアル化	**CVE-2023-20198** Cisco IOS XE Web UIの権限昇格	**CVE-2023-26360** Adobe ColdFusionの不適切なアクセス制御
CVE-2022-47986 IBM Aspera Faspexの認証されていないリモートコード実行	**CVE-2023-20273** Cisco IOS XE Web UIコマンドインジェクション	**CVE-2023-22515** Atlassian Confluence ServerおよびData Centerのアクセス制御の不備
CVE-2023-4966 Citrix NetScaler ADC/Gatewayバッファオーバフロー	**CVE-2023-46805** Ivanti Connect SecureおよびPolicy Secure認証バイパス	**CVE-2023-22518** Atlassian Confluenceの不適切な認証

CVE-2023-28771 Zyxelの複数のファイアウォールOS コマンドインジェクション	**CVE-2023-32315** Ignite Realtime Openfireパストラバーサル	**CVE-2022-47966** Zoho ManageEngineの認証されていないリモートコード実行
CVE-2023-27532 Veeam Backup & Replicationの リモートコード実行	**CVE-2023-38831** RARLAB WinRARコード実行	**CVE-2022-36537** ZK Frameworkの情報漏えい（ConnectWise R1Soft Server Backup Managerのリモートコード実行）
CVE-2023-27350 PaperCut NGの不適切なアクセス制御の脆弱性	**CVE-2023-24880** Microsoft SmartScreenのセキュリティ機能バイパス	**CVE-2022-44877** CentOS Web Panelの認証されていないリモートコード実行
CVE-2023-3722 Avaya Aura Device ServicesのOS コマンドインジェクション	**CVE-2023-22952** SugarCRMのリモートコード実行	**CVE-2022-46169** Cactiコマンドインジェクション

Citrix NetScaler ADC/Gateway の2つの脆弱性（**CVE-2023-3519**と**CVE-2023-4966**、それぞれ7月と10月に公開）が、2023年後半から2024年初頭にかけて発生したインシデントの原因となりました。JetBrains TeamCity CI/CDソフトウェアの重大な認証バイパス**CVE-2023-42793**は、2023年9月に公開され、**ロシア**と**北朝鮮** の国家支援を受けた脅威アクターにより悪用され、パッチリリースから数か月後に世界中のインテリジェンス機関から**速報**が寄せられました。その後、通信会社3CXのデスクトップアプリケーションに、北朝鮮の脅威キャンペーンが疑われるアクティビティの一環として**バックドアが仕掛けられていた**（CVE-2023-29059）ことが判明し、2023年の2番目の主要なサプライチェーン攻撃ベクトルとしてニュースになりました。

Adobe ColdFusionの**CVE-2023-26360**は、限定的かつ標的を絞った形で悪用されたことが2023年3月に初公表されましたが、この脆弱性は年間を通じて複数のキャンペーンで**初期アクセスベクトル**の役割を果たしており、この中には米国政府のサーバーへの**攻撃**の成功も含まれます。SugarCRMの**ゼロデイ リモートコード実行脆弱性（CVE-2023-22952）は、AWSクラウド環境への初期アクセスの提供に加えて、WebShellとクリプトマイナーの展開に使用されました**。攻撃者はApache ActiveMQのゼロデイリモートコード実行欠陥である **CVE-2023-46604**を悪用し、少なくとも2種類のランサムウェアのほか、**WebShell**、クリプトマイナー、**ルートキット**をドロップしています。

ここ数年、脆弱性の広範な悪用は一般的になってきましたが、過去15か月間で、広範囲にわたる侵害イベントにおける攻撃者の行動に大きな変化が見られました。2023年より前は、日和見的に悪用された脆弱性に対して観察された最も一般的な攻撃パターンは「攻撃者も標的も多数」というものでした。言い換えると、第一波では低スキルなエクスプロイトが次々と発生し、クリプトマイナーやWebShellの配信が頻繁に発生し、その後、これにより巧妙なランサムウェアグループやAPTの悪用が続きました。

しかし、2023年以降、複雑なゼロデイエクスプロイトチェーンやカスタムインプラントを使用する**単一の意欲的な脅威アクター**によって最初のエクスプロイトが組織化され、実行される大規模な侵害イベントが増加しています。

2023年の大規模な攻撃の多くはこのパターンをたどりました。

- Cl0pランサムウェアグループは、新たなゼロデイエクスプロイトを使用して、2つの一般的なファイル転送ソリューションであるMOVEit Transfer（**CVE-2023-34362**）と**GoAnywhere MFT**（**CVE-2023-0669**）を狙い、高度に組織化された「スマッシュ&グラブ」キャンペーンで世界中の何百もの組織に対してデータの漏えいと恐喝を引き起こし、**何千万人も**の消費者に侵害通知が送信される結果となりました。どちらの攻撃も非常に綿密に計画され、実行されたもので、米国の休日の週末に始まったMOVEit Transfer攻撃は、脅威アクターによる**2年近い**偵察とテストの集大成であった可能性もあります。

- Barracuda Networksは、2023年5月から数週間にわたって行われた一連のアップデートの中で、単一の攻撃者がゼロデイコマンドインジェクションエクスプロイト（**CVE-2023-2868**）を使用して、カスタム**バックドア**を備えた大規模なEメールセキュリティゲートウェイ（ESG）アプライアンスを侵害したインシデントについて開示しました。このバックドアは非常に執拗であったため、ベンダーは最終的に顧客に対して物理デバイスを完全に廃棄するように指示しました。2023年12月下旬、同社は**攻撃者によって悪用された**2つ目のゼロデイ脆弱性（**CVE-2023-7102**）について開示しました。

- 2023年10月、Cisco Talosは、**情報共有で**、未特定の脅威アクターが「BadCandy」と名付けられたカスタムインプラントの展開に悪用したCisco IOS XEのゼロデイ脆弱性（**CVE-2023-20198**および**CVE-2023-20273**）に触れました。このインプラントは攻撃者が**業界の検知を回避する**ための変更前に数万台のデバイスに**展開されていたとされています**。このインプラントは現在、少なくとも3回目のイテレーションとなっています。

- 2024年1月にIvanti Connect SecureおよびPolicy Secureゲートウェイに対して行われた「**疑わしいAPT**」攻撃の調査により、ゼロデイエクスプロイトチェーン（**CVE-2023-46805**および**CVE-2024-21887**）の存在が明らかになりました。脆弱なデバイスを侵害するためにこの脆弱性を攻撃者が使用し、その後WebShellを展開して**正規のファイルをバックドア化**するものです。2月中旬の時点で、数千のゲートウェイが後続のCVE開示に対して**脆弱なままでした**。米国政府機関は2月29日に**共同勧告を公開**し、脅威アクターがIvantiのIntegrity Checker Tool（ICT）を欺くことができ、結果として侵害を検知できなかったことを強調しました。この勧告では、「勧告作成組織は、企業環境でのこれらのデバイスの継続使用の可否を決定する際に、Ivanti Connect SecureおよびIvanti Policy Secureゲートウェイへの攻撃者によるアクセスと永続化の重大なリスクを考慮することをすべての組織に強く推奨します」としています。

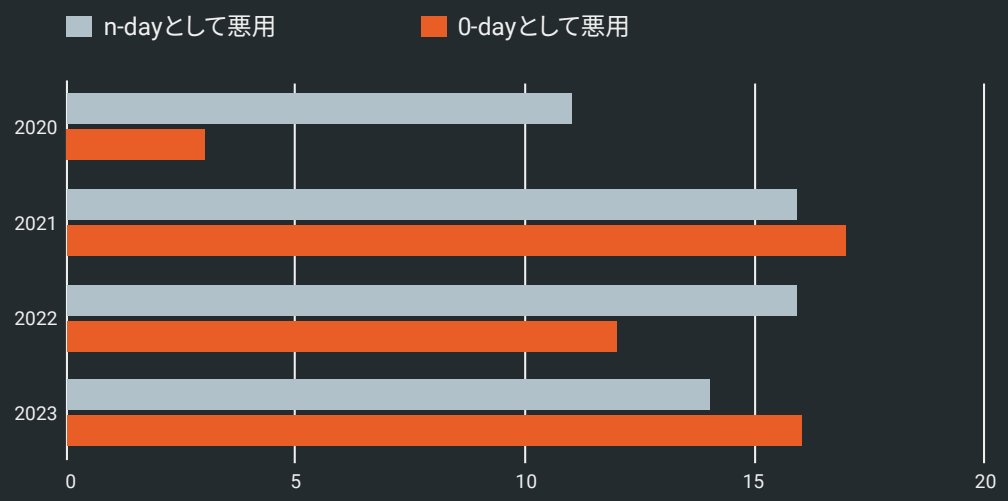
2023年から2024年初頭にかけて、低スキルの機会便乗的な攻撃が数多く見られました。いわゆるスクリプトキディが完全に消えたわけではないということになります。ただ、全体として、上記のようなインシデントで観察されたスキルと洗練度は過去数年よりもはるかに高くなっている傾向にあります。上記の脆弱性はすべて、ネットワークエッジデバイスまたはファイル転送テクノロジーに関係していましたが、攻撃者の行動パターンの変化に対する懸念は、サプライチェーンのセキュリティと内部脅威に関する議論にも浸透しています。そして、2023年の主要なサプライチェーン**攻撃ベクトル**と**主要なインシデント**にも見られるとおり、その懸念には十分な理由があります。

グラウンドゼロ：パッチ適用前のエクスプロイト

2020年末から2021年末にかけて、多くの組織のセキュリティ侵害につながった大規模なインシデントは2倍以上となりました。これらの数値がその後2021年以前のレベルに戻ったことはありません。しかし、さらに懸念されるのは、広範囲にわたるゼロデイ脅威イベントが2021年に5倍以上に増加し、これ以降は主流となっていることです。

2023年には、ゼロデイ脆弱性による大規模な侵害イベントの発生件数がNデイ脆弱性によるものを上回りました。これは3年間で2度目の出来事です。

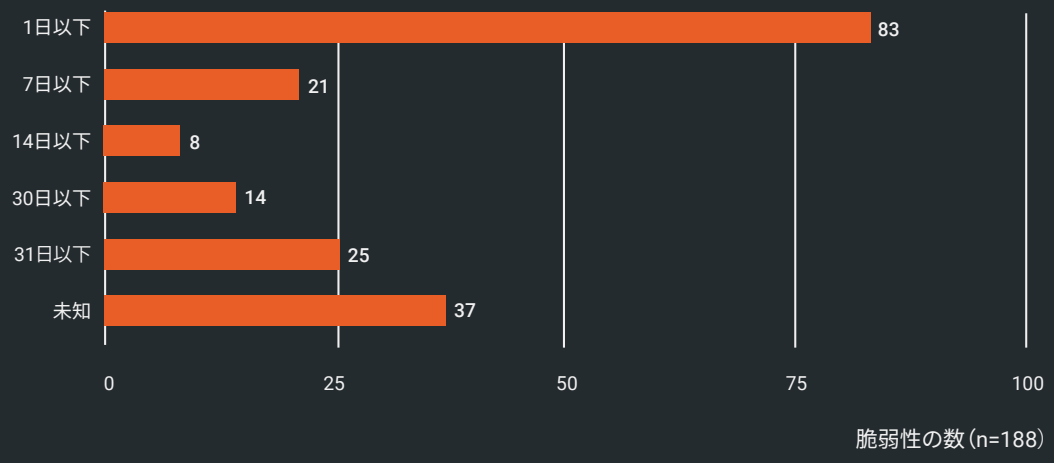
広範囲にわたる脅威のCVE（2020年-2024年）



広範囲にわたる脅威のCVEの数（n=105）

2021年以来、Rapid7の研究者は、脆弱性が一般に知られるようになってから実際に悪用されたと（確実に）報告されるまでの時間を追跡してきました。当社ではこの期間を「悪用が判明するまでの時間（TTKE）」と呼んでいますが、主にゼロデイ攻撃の蔓延により、この期間は過去3年間で大幅に短縮されています。2021年1月以降に当社が報告した既知の悪用されたCVEのうちゼロデイ脆弱性は43%を占め、脆弱性全体の55%は公開から1週間以内に、60%は2週間以内に悪用されています。過去との比較では、**2020年の脆弱性インテリジェンスレポート**ではゼロデイ脆弱性がデータの4 分の1未満に相当し、脆弱性の30%が1週間以内に、32%が2週間以内に悪用されています。

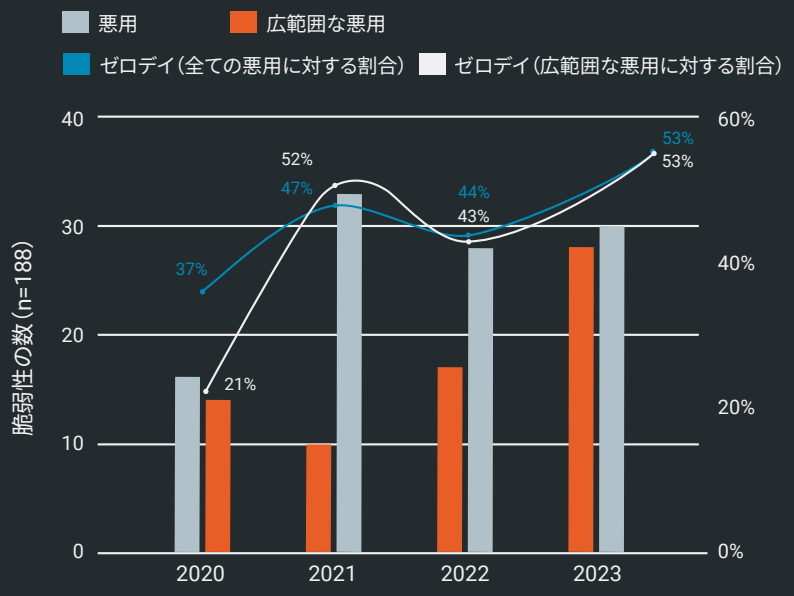
悪用が判明するまでの時間（2020年〜2024年）



TTKEの値の大部分がゼロである場合、悪用が判明するまでの平均時間は指標としてあまり有効でない傾向があります。ただし、TTKE値が判明している当社データ内のCVEの場合、悪用が判明するまでの**平均**時間は**22日**強となります。当社の累積年間データセットが対象の場合、悪用が判明するまでの時間の**中央値**は1日となります。

以下のグラフは、Rapid7が過去4年間に年次調査データセットに含めた脆弱性のうち、悪用された脆弱性と広範囲に悪用された脆弱性をゼロデイ脆弱性として、悪用された脆弱性の割合と併せて検証したものです。当社の脆弱性の分類と選択の方法論は経時的に必然的に厳格化され、規定が厳しくなっています。そのため、以下の2023年のデータは、今日の悪用傾向に関して比較的保守的な分析となっています。

攻撃の規模とスピードの傾向



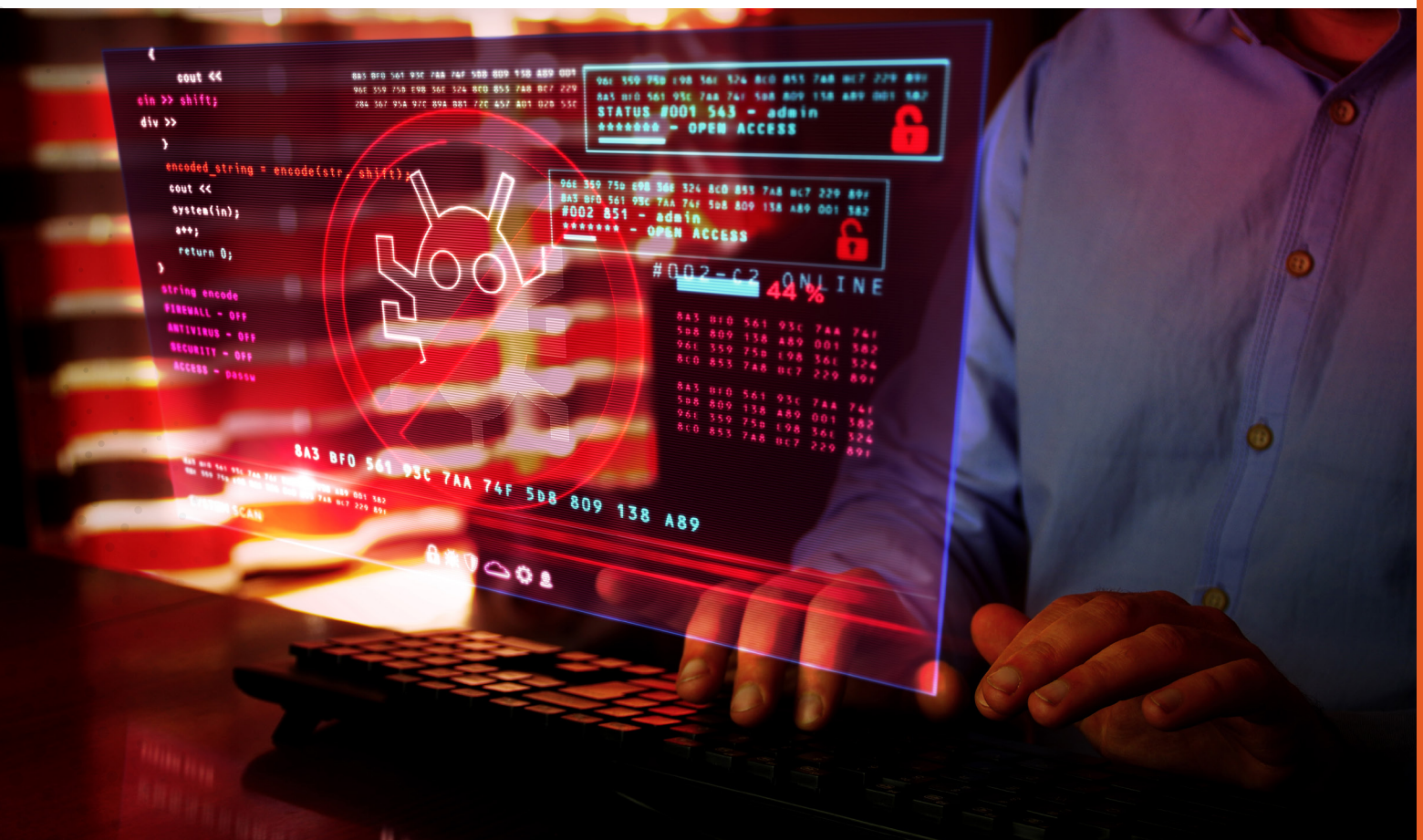
このデータから判明した点は、組織は、新しい脆弱性に迅速にパッチを適用し、インターネットに面したアタックサーフェスを継続的に減らすだけでなく、攻撃者がすでに標的ネットワークにアクセスした後に敵が目標を達成する能力を最小化する補償制御と検知戦略を実装しなければならないという大きなプレッシャーにさらされているということです。エンドポイントディテクションレスポンス（EDR）のような技術は深層防御戦略の重要な構成要素となりますが、企業のリーダーは、現代のサイバー脅威に対抗し、防御するためには、テクノロジーに加えて人間の専門知識が引き続き必要であることを認識すべきでしょう。セキュリティチームの燃え尽き症候群や人材流出は、これまで以上に、十分なリソースと強い動機を持つ攻撃者の活動によるリスクを悪化させています。

データ抽出へのカウントダウン：ファイル転送システムへのハッキング

GoAnywhere MFTの**CVE-2023-0669**とMOVEit Transferの**CVE-2023-34362**に対するCl0p攻撃は、 2023年に世界中の何千万人ものユーザーに侵害通知が絶え間なく送信されたことから、過去1年間のニュース報道を賑わせてきました。しかし、過去1年半の間に金銭目的の攻撃者が悪用したファイル転送テクノロジーはGoAnywhere MFTとMOVEit Transferだけではありません。実際にこうしたインシデントは2023年に十分なパターンとして成立し、Rapid7の研究者は、6つのファイル転送CVEに対して新たに**「スマッシュ&グラブ」**攻撃者ユーティリティカテゴリーを作成しています（本レポート後半の攻撃者ユーティリティを参照）。

CVE-2022-47986は、IBMのAspera Faspexデータ転送ソリューションにおけるYAML逆シリアル化の**問題**であり、**ランサムウェア**とイラン**政府が支援する**脅威アクターの両方によって悪用されました（Rapid7の研究者が**この脆弱性を分析し**「実際の悪用よりも、[アプリケーションの] クラッシュを防ぐことの方が困難だった」としています）。他にも、Progress SoftwareのWS_FTPセキュアファイル転送ツールにおける別の逆シリアル化の問題**CVE-2023-40044**があり、こちらは複数のエクスプロイトチェーンを介して**（ランサムウェアの展開の試みを含め）**攻撃を受けました。興味深いことに、逆シリアル化は、「スマッシュ&グラブ」攻撃の根本原因として頻出しています。逆シリアル化の問題は、GoAnywhere MFTの**CVE-2023-0669**の根本原因でもありました。また、MOVEit Transferの**CVE-2023-34362**自体はSQLインジェクションの欠陥ですが、.NET逆シリアル化の問題も**完全なリモートコード実行攻撃チェーン**の重要な一部となっています。

今年、かろうじて広範囲にわたる脅威リストにランクインしたCitrix ShareFileの**CVE-2023-24489**については、2023年8月に**ハニーポットの悪用活動**が急増しましたが、予想よりも早く減少しました。これは、ベンダーがパッチの適用まで脆弱なコンポーネントへの**アクセスを無効にしていた**ためと考えられます。それでも、この脆弱性は2024年初までに多数のランサムウェアインシデントレポートで引用されており（公開例は**こちら**）、パッチが適用されていないコントローラーが依然として魅力的なターゲットであることを示しています。当社で「スマッシュ&グラブ」の機会として分類した最後のバグ**CVE-2023-43177**は執筆時点ではまだ悪用されていないようですが、CrushFTPの認証されていないリモートコード実行の問題で、**巧妙なエクスプロイトチェーン**が公開されています。



これらのテクノロジーは、機密データを保存する機会が多いため、金銭的動機のあるランサムウェア攻撃者や恐喝キャンペーンが活用しがちです。Rapid7がファイル転送ツールで観測した攻撃の多くは、攻撃者が数分や数時間以内に侵入し、データを盗み、退散するという迅速なものでした。データ漏えいの通知規制に関しては一般的に解釈の余地があるかもしれませんが、ファイル転送アプリケーションからのデータ流出で終わる攻撃については、規制上の報告要件には余地がほとんどありません。

これらの報告要件は、特に副次的被害に関して、セキュリティ企業、メディア、規制当局がこの種の攻撃の被害者を詳細に把握できるようになった一因でもありました。大規模なサイバーセキュリティインシデントの結果として消費者に送信されるのデータ漏えい通知の数は、攻撃の影響を定量化する最良の方法ではないかもしれませんが、「爆発半径」と呼ばれるものを追跡するために非常に効果的です。

明るい兆し

ファイル転送ベンダーは、Cl0pによるMOVEit TransferとGoAnywhere MFTのハッキング（およびその後の多くの被害者に対する広報関連の混乱）によって、当然ながら驚かされました。しかし、「ファイル転送ツールへのハッキングの年」は、良い側面も持っていました。**Rapid7が脆弱性**をファイル転送**ベンダー**に開示した経験から言えば、**ベンダーの対応は非常に迅速**で、開示プロセス全体で高い緊急性を示し、多くのケースで新しい脆弱性の修正を数週間で提供しました。通常の企業がかかる時間の半分以下で報告された脆弱性を修正するケースもありました。

一般的に、最近のCl0p攻撃を契機として、一部のファイル転送ツールベンダーが、脆弱性開示と製品セキュリティの実践を成熟させていると言えます。たとえば、リカバリーのSLAを速めたり、外部のセキュリティ研究者向けの形式の開示メカニズムを確立したり、より頻繁で透明性のあるパッチリリースサイクルを導入したりしています。こうした動きは、攻撃者より先に新しい脆弱性を特定しようとする強力な事前対策と並び、今後のベンダーの脆弱性対応を加速し、合理化するのに寄与する可能性のある前向きな兆しといえます。

2023年に悪用されたその他の脆弱性

次の脆弱性は、2023年または2024年に実際に悪用されたことが知られていますが、2024年2月の時点で、広範囲にわたる脅威に含めるのに十分な大規模攻撃の技術的証拠はありませんでした。

CVE-2023-46747 F5 BIG-IP構成ユーティリティ認証バイパス	**CVE-2023-36845** Juniper Junos OS EXおよびSRX PHP外部変数の変更	**CVE-2023-38035** Ivanti Sentry Admin Portal認証バイパス
CVE-2023-29298 Adobe ColdFusionアクセス制御バイパス	**CVE-2023-7102** Barracuda Email Security Gatewayの任意のコード実行	**CVE-2023-49103** ownCloud Graph APIの重要な情報漏えい
CVE-2023-38203 Adobe ColdFusionの信頼できないデータの逆シリアル化	**CVE-2022-21587** Oracle E-Business Suiteのリモートコード実行	**CVE-2023-28432** MinIOの情報漏えい
CVE-2023-33246 Apache RocketMQのリモートコマンド実行	**CVE-2023-21839** Oracle WebLogic Serverのリモートコード実行	**CVE-2023-37580** Synacor Zimbra Collaboration Suiteのクロスサイトスクリプティング
CVE-2023-41265 Qlik Sense Enterprise HTTPのトンネリング脆弱性	**CVE-2023-20867** Broadcom VMware Toolsの認証バイパス	**CVE-2023-29357** Microsoft SharePoint Serverの権限の昇格
CVE-2023-47246 SysAidパストラバーサル	**CVE-2023-20887** Broadcom VMware Aria Operations for Networksコマンドインジェクション	**CVE-2023-23397** Microsoft Outlookの特権の昇格
CVE-2023-1671 Sophos Web Applianceコマンドインジェクション	**CVE-2023-34048** Broadcom VMware vCenter Serverの領域外書き込み	**CVE-2023-36884** Microsoft Windows Searchのリモートコード実行
CVE-2023-41179 Trend Micro Apex Oneの任意のコード実行	**CVE-2023-35078** Ivanti Endpoint Manager Mobileの認証バイパス	**CVE-2023-28252** Microsoft Windows共通ログファイルシステムドライバー特権の昇格
CVE-2023-27997 Fortinet FortiOSヒープベースのバッファオーバーフロー	**CVE-2023-35081** Ivanti Endpoint Managerモバイルパストラバーサル	
CVE-2022-41328 Fortinet FortiOSパストラバーサル	**CVE-2023-35082** Ivanti Endpoint Manager MobileおよびMobileIron Core認証バイパス	

上記の悪用された脆弱性のほとんどは、ネットワークエッジデバイス、アプリケーション開発および配信テクノロジー、ITセキュリティ管理システムによるものですが、例外的に言及の価値がある脆弱性もいくつかあります。Microsoft SharePointの**CVE-2023-29357**は、当初「差し迫った脅威」リストに掲載されていましたが、本レポートが完成する前に悪用されました。2つの情報漏えいの脆弱性（MinIOの**CVE-2023-28432**およびownCloudの**CVE-2023-49103**）により、攻撃者は認証情報を含むクラウドシークレットにアクセスできるようになりました。データ分析プラットフォームであるQlik SenseのHTTPトンネリングの脆弱性（**CVE-2023-41265**）は、 2023年11月にCactusランサムウェアグループによって企業環境への初期アクセスに**悪用**されました。

標的型のゼロデイ攻撃で悪用される脆弱性には、興味深い裏話がつきものですが、このケースも例外ではありません。上記のリストにある28件のCVEのうち、15件がゼロデイ脆弱性として悪用されました（54%）。注目すべき例をいくつか以下で紹介します。

- **CVE-2023-34048**はVMware vCenter Serverにおけるメモリ破損の問題で、**Mandiantによると**、発見される1年以上前から中国のスパイグループUNC3886によって悪用されていました。
- **CVE-2023-28252**はMicrosoftのCLFS ドライバーの権限昇格の脆弱性**で、Nokoyawaランサムウェアキャンペーン中に発見されました。**
- **CVE-2023-36884**はWindowsの脆弱性で、Microsoftが標的型スパイ活動とウクライナ関連の餌を使った機会便乗型フィッシングキャンペーンの両方で使用されたと**指摘**しています。
- **CVE-2023-23397**はMicrosoft Outlook の重大な権限昇格（NTLMハッシュリーク）バグです。Microsoftによると、このバグは**ロシアを拠点とするAPT**によって1年近くにわたって**政府機関**、重要なインフラストラクチャプロバイダー、軍事サプライヤーへの攻撃に悪用されていました。
- **CVE-2023-47246**はSysAidサーバーのパストラバーサルの脆弱性で、**Microsoftは**このゼロデイ攻撃がCl0pランサムウェアの配布で知られる脅威アクターLaceTempestによるものとしています。

CVE-2023-37580は、2023年6月に攻撃対象として人気のZimbra Collaborationで公開されたクロスサイトスクリプティング（XSS）のバグに関するものです。Googleの脅威分析グループ（TAG）によると、この脆弱性はギリシャ、モルドバ、チュニジア、ベトナム、パキスタンの政府組織を狙った**少なくとも4つのAPTキャンペーンで**使用されました。Googleの分析には、「メールサーバーにおけるXSS脆弱性の定期的な悪用は、これらのアプリケーションのコード監査、特にXSS脆弱性のさらなる監査の必要性も示している」という注釈が含まれています。

最後に、モバイルデバイス管理ソリューションIvanti Endpoint Manager Mobile（旧MobileIron Core）に対する攻撃が相次ぎ、2023年7月以降の10日間に

3つの脆弱性が公開されたことでメディアや業界の注目を集めました。1つ目（**CVE-2023-35078**）は重要な認証バイパスで、ノルウェーの12の**省庁**に対するゼロデイ攻撃で使用されました。CVE-2023-35078の**公開**とパッチのリリースから4日後、Ivantiは、**2回目のアドバイザリ**を公開し、CVE-2023-35078と連鎖して管理者認証をバイパスする可能性のある任意のファイル書き込みの問題**CVE-2023-3508**について発表しました。**CVE-2023-35078**の分析の過程で、Rapid7の研究者は、認証されていないリモートの攻撃者がEPMM管理サーバー上のAPIエンドポイントにアクセスする可能性があることを**発見**しました。この問題には**CVE-2023-35082**が割り当てられました。

国家主導型アクティビティ

Rapid7の研究者は、幅広いソースからデータを収集、分析、精査し、Rapid7の製品とサービスをサポートする中央の脅威ライブラリに追加しています。当社のデータソースには、Rapid7独自のMDRサービスチームからのインテリジェンスに加えて、ダークウェブフォーラム、プライベートメッセージングプラットフォーム（Telegramなど）、公開レポート、民間業界の情報源が含まれます。

このプロセスには、当該キャンペーンの疑わしいソースの詳細と、それに関連するアトリビューションの信頼性に関する厳密な分析が含まれます。当社の分析では、2023年1月から2024年3月までの期間に、APTグループから発信されたと推定されるソースについて、信頼度が中程度から高いものまでを含めて、188件の別々のキャンペーンが特定されました。「中程度の信頼性」とは、観測しているアクティビティが、過去に特定のグループやアクターから観測されたものと類似しているという証拠が相当程度あることを意味します。ただし、誰かが行動を模倣したり、偽旗作戦を行っている可能性は常にあります。

当社の分析によると、上位15グループ全体で、APTグループによる攻撃の30%が中国の支援するキャンペーンから発生したものと結論付けられました。ロシア系グループによるキャンペーンは僅差で2位となり、国家主導型の敵対勢力によるキャンペーンの26%を占め、北朝鮮（14%）とイラン（9%）が3位と4位につけています。

ランサムウェア

ランサムウェアによる支払いは2023年に**10億ドルを超えた**とされており、Cl0pなどのグループは引き続き二重の恐喝攻撃を行って巨額の支払いを手にし、**数億ドルの利益を上げている**とされています。Rhysidaランサムウェアグループは大英図書館への攻撃を実行して何か月も**システムを停止させ**、**LockBitが主犯とされる事件**では英国ロイヤルメールの業務が混乱し、2023年には推定1億人以上の米国の消費者が**医療機関を狙った**ランサムウェア攻撃の巻き添え被害を受けました。

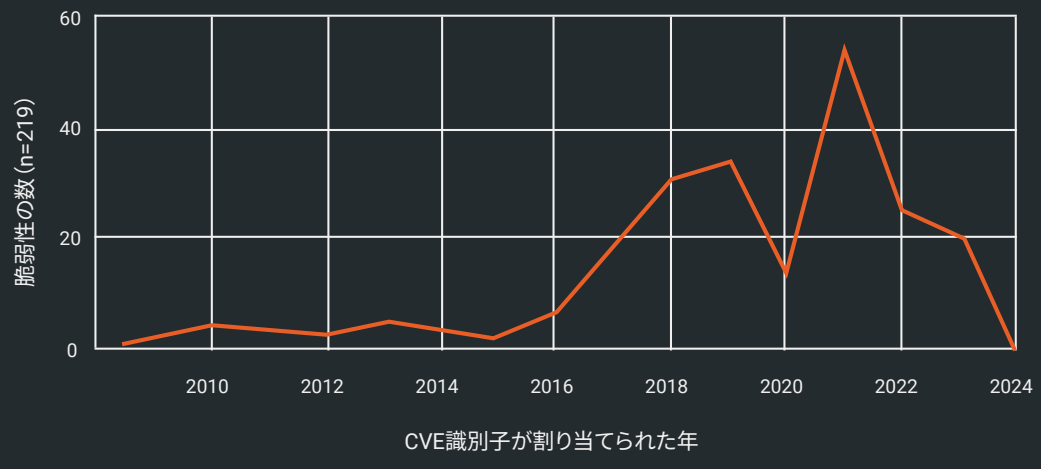
2024年に入ってもランサムウェアのインシデント件数は減少していません。今年すでに、日本の自動車メーカー日産自動車は**Akiraランサムウェアインシデントで**約10万人が影響を受けた旨を公表し、米国政府機関はPhobosランサムウェアアフィリエイト活動に対する防御に関する**共同警告を発表**し、フランスの2つの医療決済プロバイダーへの攻撃では3,300万人の市民の**データが漏洩**しました。2月には、米国を拠点とする医療決済プロバイダーChange Healthcareが、BlackCat（ALPHV）ランサムウェアグループによる**壊滅的な攻撃**の被害に遭っています。2024年3月下旬の時点で、このインシデントは重要な業務を**混乱させ続けており**、**未処理**の膨大な処方箋、決済処理の**遅延**、小規模医療提供機関の**財政危機**の一因となっています。

ランサムウェアの活動阻止を目指す政府の活動も拡大しています。2023年だけでも、米国司法省は、Qakbotマルウェアインフラストラクチャの複数国での**解体**、FBIによる数か月にわたる同グループネットワークへの侵入後のHiveランサムウェアサーバーとサイトの**押収**、BlackCat/ALPHVランサムウェアを阻止するための国際**作戦**、 Contiランサムウェアとtrickbotマルウェア活動に関連する複数の外国人の**起訴**などを相次いで発表しました。

2023年10月、米国サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）は、ランサムウェア情報を既知の悪用された脆弱性（KEV）リストに組み込み始めた旨を**発表しました**。この機能は比較的不透明で、（KEVの他の部分のように）特定のデータソースを掲載することはありませんが、新しい脆弱性のKEVへの追加に対するCISAの極めて保守的なアプローチは、「既知の」ランサムウェアの指定が十分に検証されたものである信頼につながります。

2024年3月中旬の時点で、同KEVリストには、ランサムウェア攻撃での使用が知られている219のCVEが含まれていました。以下の表は、KEVのランサムウェアの脆弱性をCVE識別子の年別に分類したものです。

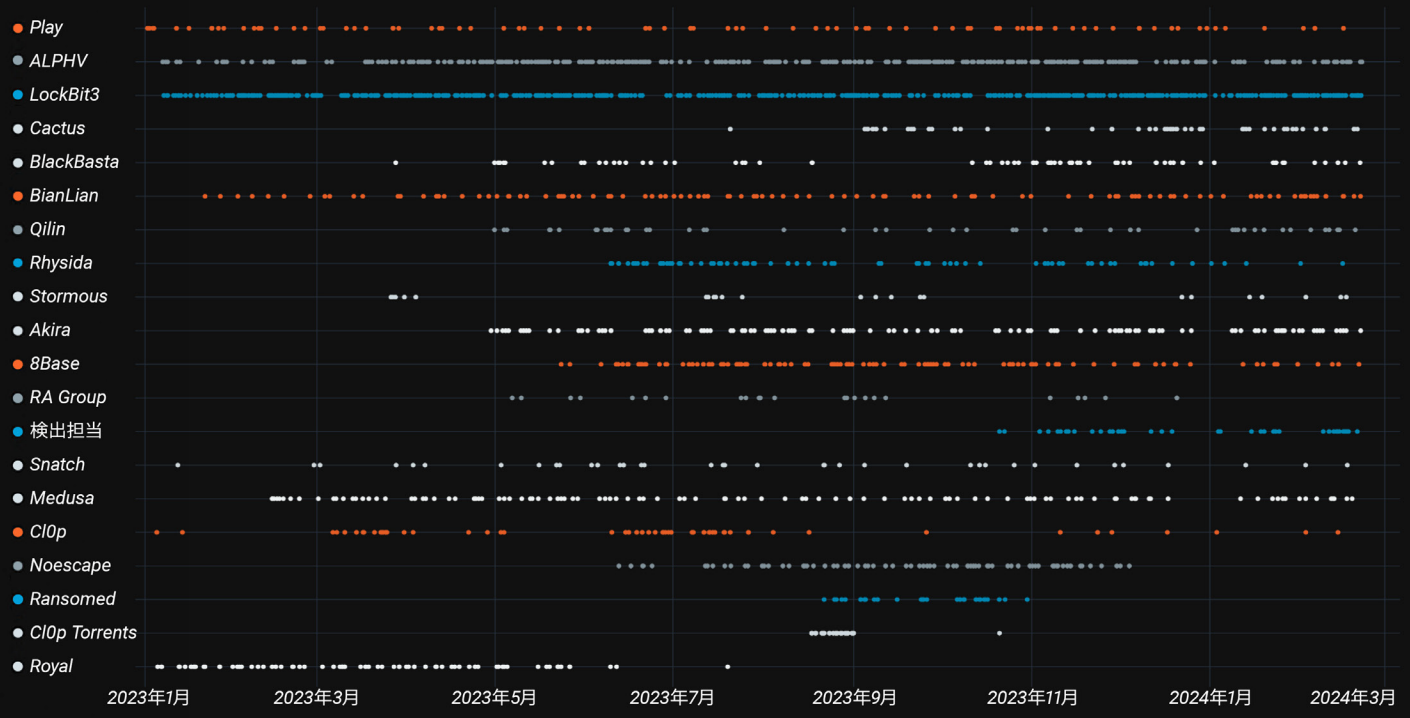
CISA KEVランサムウェアのCVE



Rapid7 Labsは、外部レポートとRapid7 MDRのインテリジェンスの両方から得たデータを使用して、2023年のランサムウェア攻撃の分析を行いました。当社の統合インテリジェンスソースで、2023年1月から2024年2月の間に報告された約5,600件のランサムウェア事件を追跡しました。この数値には、必然的に報告されない攻撃の数々を考慮していません。そのため、公式に発表される数字は実際の発生数よりもはるかに少ないと考えられます。

Rapid7 Labsが2024年1月に**発表した内容**によると、これらのグループが2023年に使用した固有のランサムウェアグループの数は、2022年の新規グループ数95件から2023年にはわずか43件へと半分以上減少しました。この傾向から、現行のランサムウェアグループとビジネスモデルに収益性があり、まったく新しい機能を早急に開発する必要ない可能性があることが分かります。以下の散布図では、漏えいサイトの通信、公開情報、Rapid7のインシデント対応データに基づき、2023年と2024年初頭の上位20のランサムウェアグループに起因するランサムウェアインシデントの数を示しています。

2023年と2024年の上位20グループ別の投稿の経時的な分布



Ransomware-as-a-Service（RaaS）を多用するLockBit 3.0は、活動量の点から見て引き続き首位グループであり続けています。BlackCatとしても知られるALPHVも、米国政府主導の同グループの活動阻止の取り組みにもかかわらず、年間を通じ、そして2024年にかけて高い活動率を維持しました。米国と英国は2024年2月にLockBitランサムウェアの亜種を阻止したことを**発表しました**。米司法省のALPHV阻止に関する**2023年12月のプレスリリース**では、FBIが政府開発の復号ツールを数百の組織に提供し、「約6,800万ドルの身代金要求から複数の被害者を救った」としています。2024年3月27日、米国務省は「正

義への報奨」プログラムの一環として、BlackCatランサムウェアギャングのメンバーの特定や所在確認につながる情報に対して**最大1,000万ドルの報奨金**を出すと発表しました。

前述のように、過去1年の間に、攻撃者が企業ネットワークに迅速にアクセスしてデータを盗み出そうとするファイル転送ソリューションなどのテクノロジーを狙った「スマッシュ&グラブ」攻撃へのシフトが見られました。被害者データを暗号化する「従来型」ランサムウェア事件も多く発生しています。Rapid7 MDRが昨年対応したランサムウェア関連の事件の大半には暗号化が含まれており、恐喝のみで終わったインシデントはごくわずかです。

2023年のランサムウェアや恐喝攻撃では、公開されているアプリケーションを悪用し、有効なアカウントを作成することが初期アクセスベクトルの上位となりました。2023年と2024年初頭にランサムウェアグループによって悪用されたことが知られている脆弱性には、以下のCVEが含まれます（ただしこれらに限定されません）。

CVE-2023-20269 Cisco ASAおよびFTDの不正アクセスの脆弱性	**CVE-2022-47966** Zoho ManageEngineの認証されていないリモートコード実行	**CVE-2023-35078** Ivanti Endpoint Manager Mobileの認証バイパス
CVE-2023-42793 JetBrains TeamCity CI/CDサーバー認証バイパス	**CVE-2023-3519** Citrix NetScaler ADCおよびNetScaler Gatewayの認証されていないリモートコード実行	**CVE-2023-35082** Ivanti Endpoint Manager Mobileの認証されていないAPIアクセス
CVE-2023-0669 Fortra GoAnywhere MFTリモートコード実行	**CVE-2023-4966** Citrix NetScaler ADC/Gatewayバッファオーバフロー	**CVE-2023-38831** RARLAB WinRARコード実行
CVE-2023-34362 Progress Software MOVEit Transfer SQLインジェクション	**CVE-2023-24489** Citrix ShareFileの不適切なアクセス制御	**CVE-2022-21587** Oracle E-Business Suiteのリモートコード実行
CVE-2023-40044 Progress Software WS_FTP Serverの信頼できないデータの逆シリアル化	**CVE-2023-22515** Atlassian Confluence ServerおよびData Centerのアクセス制御の不備	**CVE-2023-24880** Microsoft SmartScreenのセキュリティ機能バイパス
CVE-2022-47986 IBM Aspera Faspexの認証されていないリモートコード実行	**CVE-2023-22518** Atlassian Confluenceの不適切な認証	**CVE-2023-28252** Microsoft Windows共通ログファイルシステムドライバー特権の昇格
CVE-2023-27532 Veeam Backup & Replicationのリモートコード実行	**CVE-2023-47246** SysAidパストラバーサル	**CVE-2022-36537** ZK Frameworkの情報漏えい（ConnectWise R1Soft Server Backup Managerのリモートコード実行）
CVE-2023-32315 Ignite Realtime Openfireパストラバーサル	**CVE-2023-41265** Qlik Sense Enterprise HTTPのトンネリング脆弱性	
CVE-2023-27350 PaperCut NGの不適切なアクセス制御の脆弱性	**CVE-2023-46604** Apache ActiveMQのリモートコード実行	

2023年の初期アクセスベクトル

ランサムウェアグループは、今後も公開アプリケーションの新しい脆弱性や既知の脆弱性を悪用すると予想されますが、ランサムウェアなどの攻撃から身を守るために多くの組織が講じていない基本的な手順はまだあります。Rapid7 MDR が 2023年に観測した**インシデントの41%**は、インターネットに接続されたシステム、特に VPNや仮想デスクトップインフラストラクチャで多要素認証（MFA）が欠落しているか、強制されていないことが原因となっています。この数値は過去1年半にわたって安定しており、**2023年上半期には 39%**となり、その後、同年後半にわずかに上昇しました。

初期アクセスベクトル

出典：Rapid7インシデント対応データ（2024年1月）

Rapid7 MDRのアナリストは、特にランサムウェアインシデントや恐喝攻撃において、脅威アクターが全体的にその作戦スケジュールを早めていることも指摘しています。Rapid7 MDRが過去1年間に調査したインシデントにおいて攻撃者の滞在時間は大幅に異なりますが、当社のアナリストは、攻撃者が最初のアクセスからデータの流出に至るまで、数日や数週間ではなく数分や数時間で移行することが一般的になりつつあることを観察しました。

本レポートの最後には、Rapid7のインシデント対応担当者が遭遇する最も一般的なタイプの攻撃を軽減するための実践的なセキュリティガイダンスが含まれています。

エッジの状況：ネットワークピボット（2020年〜2024年）

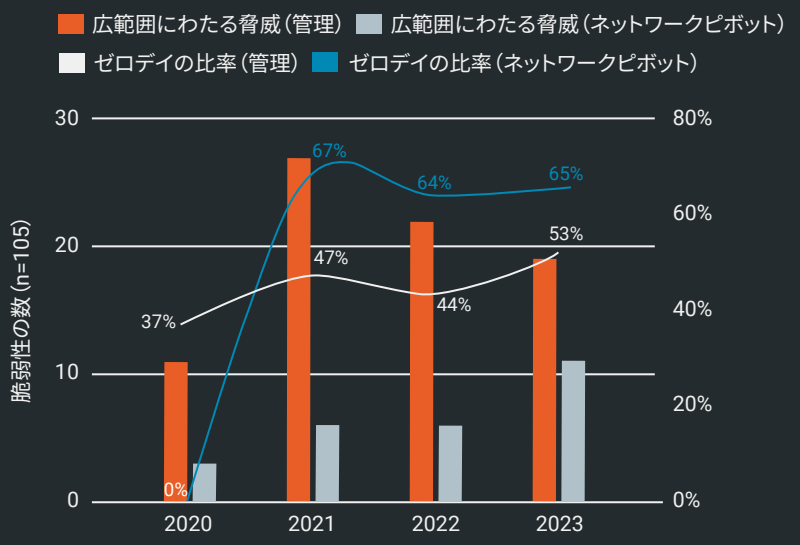
Rapid7が2020年に最初の脆弱性インテリジェンスレポートを公開した際、当社の研究チームは、**ネットワークピボット**として役割を果たし、外部攻撃者が内部ネットワークにアクセスする機会を提供するテクノロジーの脆弱性に関する特定の攻撃者ユーティリティカテゴリーを作成しました。VPN、ファイアウォール、セキュリティゲートウェイに代表されるほとんどのネットワーク機器は、他のいくつかのインターネット向けテクノロジーとともにこのカテゴリーに分類されます。これらの欠陥は、ローカルコード実行の脆弱性やネットワークプロトコルの不具合との組み合わせで、権限昇格や企業ネットワークの水平展開に使用されることがよくあります。

ネットワークエッジテクノロジーは多くの最新ネットワークの運用に不可欠であり、企業環境と個人環境の両方に接続性とセキュリティ機能を提供します。しかし、何年にもわたって大規模に悪用されている事例からも分かりますが、これらのデバイスがサイバーセキュリティ防御の重大な弱点でもあります。あらゆる動機を持つ攻撃者が、これらのデバイスを標的にするとみなすべきでしょう。ランサムウェアグループと国家主導型攻撃者のどちらも、これらのシステムにNデイ攻撃やゼロデイ攻撃を仕掛けるチャンスを狙っています。

2023年には、**Cl0p**、**Inc**、**Bl00dy**、**Akira**、**Play**、**LockBit**などの国家主導型グループやランサムウェアグループを含むさまざまな脅威アクターによるネットワークアプライアンスへの攻撃が急増しました。2023年に公開されたペイロードには、ボットネット**マルウェア**や**クリプトマイナー**のほか、新しい**WebShell**や**独自の バックドア**が含まれていました。

2023年初からのネットワークエッジデバイスの悪用による大規模な侵害イベントはほぼ倍増し、2023年に広範囲に悪用された脆弱性の36%がネットワークエッジ技術内で発生しています。また、ネットワークエッジのCVEは当社データではゼロデイ攻撃に偏っています。過去3年間、Rapid7が毎年ネットワーク・セキュリティ機器に関して分析した脆弱性の60%以上が、ゼロデイ攻撃として悪用されていました。

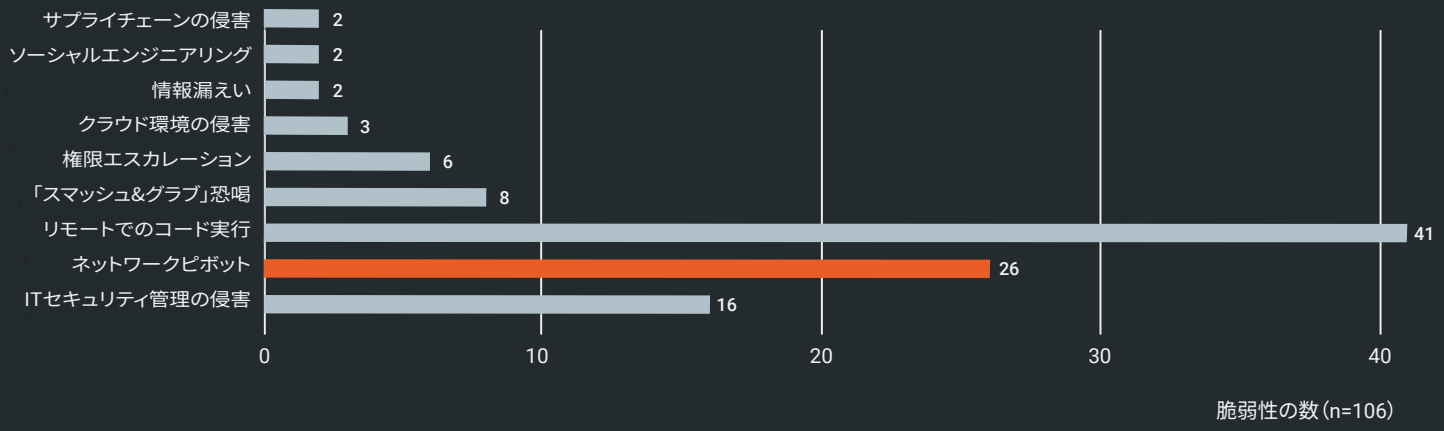
ネットワークピボット悪用の動向（2020年〜2024年）



ネットワークピボットの脆弱性は、過去4年間に累積されたデータセットで悪用された脆弱性の24%を占めており、Rapid7の研究者が2020年以降に追跡した広範囲にわたる脅威の4分の1に及びます。追記として、弊社が知る限りでは、CISA KEVの約19%がネットワークエッジデバイスまたはセキュリティゲートウェイの脆弱性で構成されており、そのうち約半数が2020年以降に公開（および悪用）されました。そのため、当社データにおけるネットワークピボットの普及率はCISAのデータよりも若干高い可能性があります。

以下は、過去4年間の**広範囲にわたる脅威の攻撃者ユーティリティ分布です。**

攻撃者ユーティリティ（2020年～2024年）（広範囲にわたる脅威）



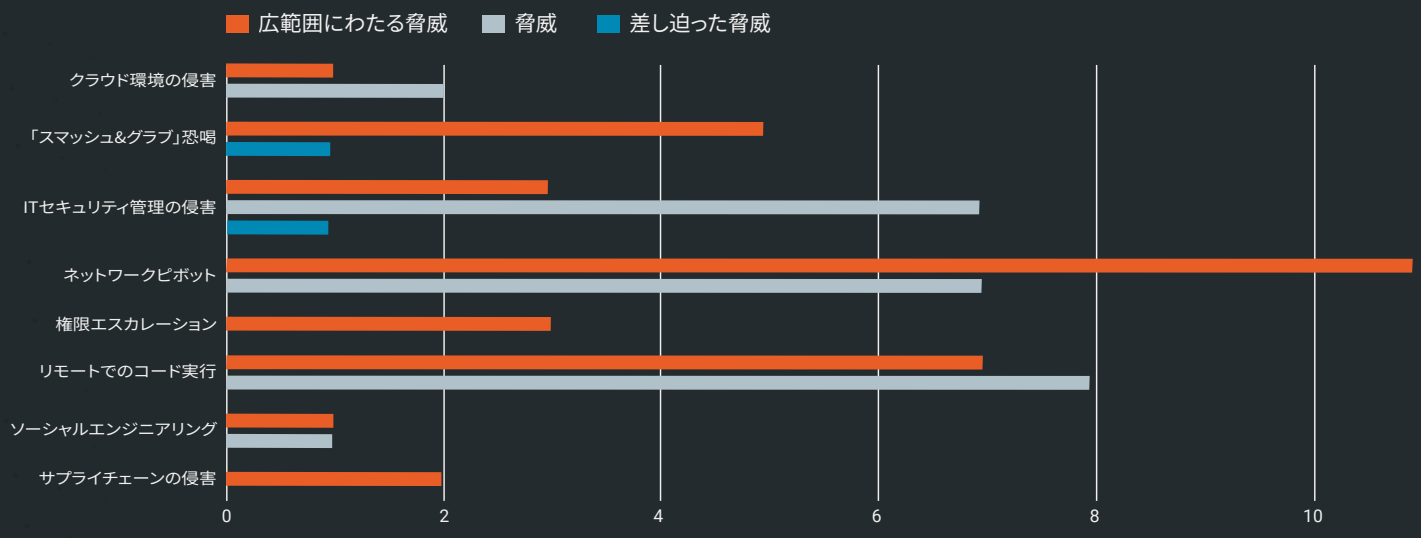
ネットワークアプライアンスへの侵入の検出は非常に困難であることが知られています。ログ記録と脅威検知の機能は、製造元やモデルによってデバイス間で大きく異なり、一部のデバイスでは、重要なイベントがログに記録されなかったり、悪意のあるアクティビティを効果的に検知できなかったりする場合があります。ファームウェアのバージョンやオペレーティングシステムの多様性（その多くがメーカー独自のもの）に加え、ファームウェアや製品全体が暗号化または難読化されている可能性もあることが複雑さに拍車をかけています。監視と保護にデバイスごとに独自のアプローチが必要になる場合があり、使用されているアプライアンスの全範囲をカバーする包括的な戦略の策定を目指すセキュリティチームにとっては課題となります。

攻撃者ユーティリティ

初めてレポートを利用される方のために説明すると、脅威の状態と悪用が判明するまでの時間に加えて、脆弱性データセットに2つの追加タイプのメタデータをマッピングしています。1つ目は研究者が**新たな脅威**を分析する際に定義するメタデータ、**脆弱性のクラス**で、相対的な悪用可能性と利用可能なツールに関する初期評価に役立ちます。2つ目は、攻撃者が悪用成功の結果として得られるものを説明する**攻撃者ユーティリティ**です。

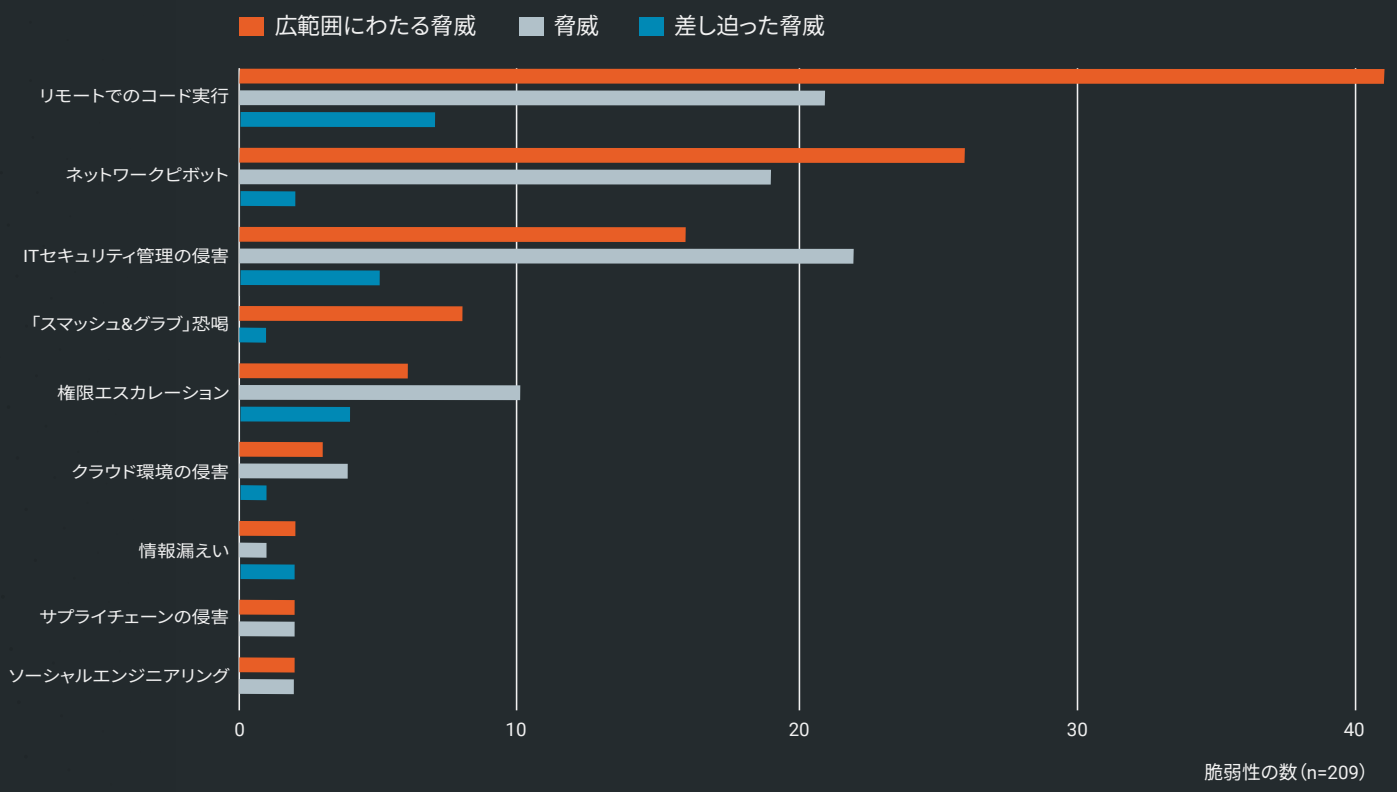
VPNやセキュリティゲートウェイなどのネットワークエッジデバイスは、過去数年間、ゼロデイ攻撃とNデイ攻撃の両方において、価値が高い標的として頻繁に狙われています。この点は2023年のデータセットから明らかで、ネットワークピボットの脆弱性は件数とインシデントの影響の両面で他の攻撃者のユーティリティカテゴリーよりも高くなっています。

2023年の攻撃者ユーティリティ



2020年以降の年次インテリジェンスレポートの脆弱性をすべて網羅するように対象を広げると分布はいくらか変化しますが、リモートコード実行に加えて、ネットワークピボットとITセキュリティ管理の侵害件数は引き続き堅調に推移します。

攻撃者ユーティリティと脅威の状況（2020年〜2024年）



一般的なリモートコード実行の脆弱性（サプライチェーンの侵害や「スマッシュ&グラブ」による恐喝などのより具体的なユーティリティのバケットにマップされないCVE）は、予想どおり、過去4年間の攻撃者ユーティリティの最大のカテゴリーとなっており、ネットワークエッジデバイスの侵害（ネットワークピボット）がそれに続きます。リモートコード実行やネットワークまたはセキュリティ管理ソリューションの乗っ取りを可能にするCVEにマップされるITセキュリティ管理の侵害は過去数年間のゼロデイエクスプロイトによく見られ（Trend Micro Apex OneのCVE-2023-41179、Ivanti SentryのCVE-2023-38035、Zoho ManageEngine ADSelfService PlusのCVE-2022-28810など）、広範囲にわたる脅威のかなりの部分を占めています（CactiのCVE-2022-46169やZoho ManageEngineのCVE-2022-47966など）。

このレポートの脆弱性のほとんどはオンプレミスのテクノロジーに影響しますが、脅威分析ではクラウド環境の侵害がより頻繁に表れ始めています。これらのレポートに含めるCVEの多くは、クラウドベースのバージョンが利用可能な製品にも影響します（例：Atlassian ConfluenceのCVE-2023-22515およびCVE-2023-22518）。ただし、ベンダーの一般的な勧告の文言では、クラウドでホストされているバージョンのソフトウェアは「影響を受けない」とする傾向があります。これは、普遍的に更新が適用されており、顧客が取るべきアク

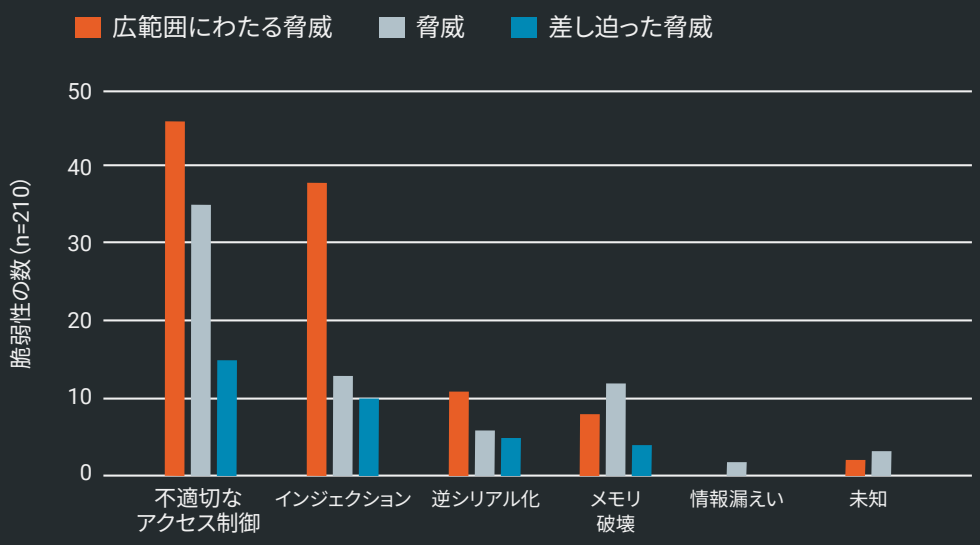
ションがないためです。研究者のWill Dormannが**2023年に指摘した**ように、「影響を受けない」というのは誤った表現の可能性があります。クラウドでホストされているソフトウェアには、ベンダーがその存在を知る前に攻撃者がゼロデイ攻撃で組織を侵害するのを防ぐ万能薬のような要素は存在せず、パッチが利用可能となる前の攻撃によって組織が危険に晒されていないと示唆することは、好意的に見ても誤解を招くものと言えます。

脆弱性のクラス

過去数年と同様に、このレポートのデータセットは一般的なエンタープライズテクノロジーのサーバーサイドの脆弱性に大きく偏っており、その多くが過去にさまざまな脅威アクターの標的となってきました。また、データの収集方法により、特定の脆弱性クラスが他の脆弱性クラスよりも少なくなっています。例えば、Googleが2023年の**「in-the-wild 0day」**リストに含めた脆弱性の75%はメモリ破損の問題から生じたものですが、当社のデータに含まれる脆弱性のうち、メモリ破損の問題が原因であったものはわずか5%です。データセットを拡張してモバイルオペレーティングシステムやブラウザの欠陥などのクライアントサイドの問題を含めれば、根本原因の分布は間違いなくかなり変わるでしょう。

攻撃者は全体として、安定し、信頼できる、そしてちょっとしたエクスプロイト開発ですむような、手軽な脆弱性クラスを好む傾向を示しています。

脆弱性クラスと脅威の状況（2020年-2024年）



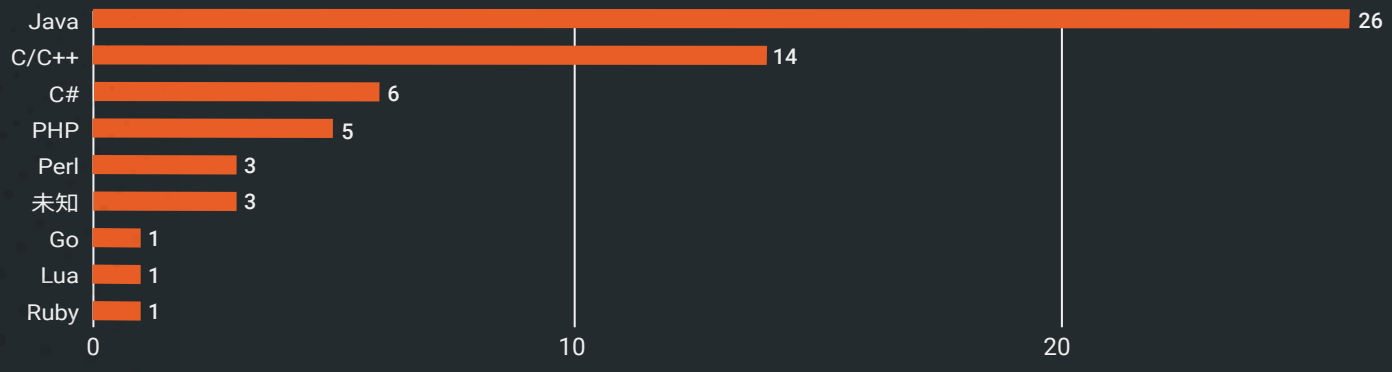
過去4年間に当社が毎年公表している脆弱性インテリジェンスデータセットに含まれるCVEの75%は、2つのスーパークラスの根本原因から発生しています。1つは認証バイパス、不適切な暗号化実装、リモートアクセス可能なAPIなどの**不適切なアクセス制御の**問題、もう1つは **インジェクション**の欠陥です。当社の分類スキーマでは、後者には、SQLインジェクションやコマンドインジェクションに加え、サーバーサイドリクエストフォージェリ（SSRF）や不適切な入力検証などの根本原因が含まれます。**逆シリアル化**の脆弱性は、CWEが1つ（CWE-502）しかないにもかかわらず、注目度が高く、広範に悪用されているCVEに不釣り合いに多く含まれています。

Rapid7の研究者が2020年以降に分析した**メモリ破損**CVEの約80%がネットワークエッジデバイスの脆弱性とオペレーティングシステムレベルの脆弱性（Windows の脆弱性など）であり、その過半（58%）がゼロデイでした。この結果は、APTはメモリ破損エクスプロイトとこの種のターゲットシステム（OSやネットワークアプライアンスなど）の両方を好む傾向があることを考慮すればそれほど驚くに値しませんが、過去数年間のAPT攻撃や国家主導型攻撃の多くで、認証バイパスやエンタープライズWebアプリケーションでのSQLインジェクションの問題など、より単純で簡単に悪用できる脆弱性も利用されています。

プログラミング言語の分布：2023年の脆弱性

Rapid7の研究者は2023年の60件の脆弱性で使用されているプログラミング言語を調べました（2023年のCVEについては2023年の広範囲にわたる新たな脅威と悪用されたその他の脆弱性を参照）。これらの60件のCVEのうち、8つの言語のみが含まれています（3つのCVEで使用されている言語は特定できませんでした）。CとC++はいずれもメモリセーフでない言語で、根本原因分析が同様の方法で行われるため、C/C++としてまとめられています。JavaとC/C++がRapid7の研究者が過去15か月間に分析した注目すべき脆弱性の3分の2を占めており、C#とPHPが大差で続いています。Ruby、Go、Luaは外れ値で、それぞれ1つのCVEに対応します。

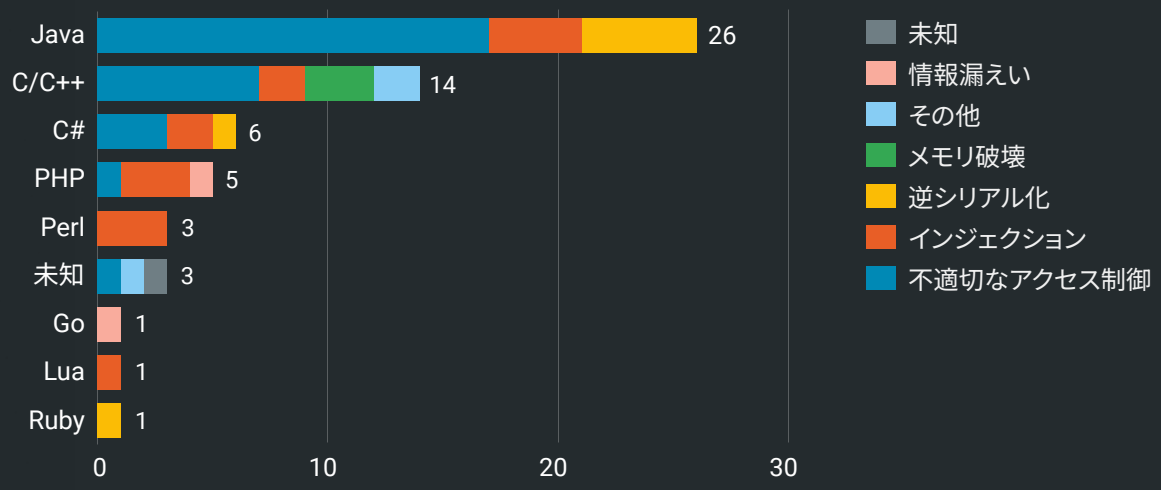
2023年の主要なCVEの言語



当然ながらJavaが最も一般的な言語であり、2023年のCVEデータの43%を占め、2番手の言語グループであるC/C++（23%）のほぼ2倍となっています。エンタープライズアプリケーションの開発言語としてのJavaの人気が続いていることから、当面はJavaとC/C++がエンタープライズソフトウェアの重大な脆弱性の中で最も重要な言語であり続けると予想されます。

データセットに特に欠けているプログラミング言語の1つがRustで、バッファオーバーフローやメモリ解放後使用の脆弱性など、メモリ破損ベースの脆弱性クラスに対する強力な保護を提供する、メモリセーフな汎用プログラミング言語です。Rust の導入はまだ初期段階にあり、オペレーティングシステムやWebブラウザなどに出荷される製品コードの量は限られていますが、増加傾向にあります。当社の調査の過程でRustベースのエンタープライズソフトウェアアプリケーションが実稼働しているのを見たことはありませんが、Rustが今後数年間で安全なソフトウェア開発の重要な部分を占めるだろうことは間違いありません。

2023年の主要CVEの脆弱性クラスと言語



各言語に影響を与える脆弱性クラスを見ると、C/C++ベースの脆弱性のごく一部でのみ**メモリ破損**が根本原因となっていることがわかります。これは、データのコンパイル方法によるところもありますが、攻撃者がエンタープライズソフトウェア悪用の際により簡単で信頼性の高い脆弱性クラスを好むことも示しています。こうした簡単かつ信頼性の高いクラスの最上位にあるのが**インジェクション**で、当社データに含まれるすべての言語で最も一般的なスーパークラスです。実際に、コマンドインジェクションの脆弱性はここ数年非常に一般的となっており、Metasploitは2023年にコマンドインジェクションの悪用を簡素化する **新しい「フェッチ」ペイロード**をリリースしました。

ほぼすべての言語で2番目に多い脆弱性スーパークラスは**不適切なアクセス制御**です。これは、攻撃者がアクセスできないはずのリソースにアクセスできるようにする論理的な問題であり、概して言語に依存しないため、脆弱性クラスとして包括的に緩和することがより困難になります。

逆シリアル化は主にC#やJavaベースの脆弱性に見られ、プログラミング言語が脆弱性のクラス全体を防ぐのに役立つ方法の好例となっています。例えば、.NET 8では、C#コードベースにおける逆シリアル化の脆弱性の根本原因となる可能性が高い**BinaryFormatterがデフォルトで無効に**なっています。また、Java 17ではリフレクションアクセスに制限が導入され、**多くの一般的な逆シリアル化ガジェットが使用不可になっています**。エンタープライズソフトウェアはJavaなどの主要な依存関係の更新が歴史的に遅いため、ソフトウェアエコシステムでより広範囲に逆シリアル化の脆弱性を防ぐ言語固有の保護の採用が遅くなります。とはいえ、ソフトウェア作成者がより優れたランタイム保護の組み込まれたコア依存関係のより新しいバージョンへ移行するにつれて、逆シリアル化の脆弱性の蔓延が経時的に減少することが期待されます。

主要な脆弱性クラスの排除に関する米国政府のガイダンス

過去の数か月間、**CISA**とホワイトハウスの国家サイバー局長室（ONCD）は、メモリ安全性の問題の影響を受けやすい言語（C/C++ など）からJava、C#、Rustなどのメモリセーフな言語への移行の重要性について文書を**公開**してきました。これは全体的に有益なアドバイスであり、近年リスクプロファイルがより不安定になっている重要なインフラストラクチャプロバイダーに向けられている可能性もあります。このガイダンスは、C/C++で記述された一部のネットワークアプライアンスにも関連していますが、2021年以降確認の広範に悪用された脆弱性の大部分がすでにメモリセーフな言語（JavaとC#）で記述された製品に存在したことも注目に値します。

メモリ破損以外の脆弱性は言語レベルで軽減するのがより困難なため、攻撃者には、基盤となる言語に関係なく、ソフトウェアの論理的な問題を悪用する機会が常にあることになります。2024年3月、CISAとFBIは**共同勧告**を発表し、ソフトウェアベンダーに対し、製品のソースコードの正式なレビューを実施してSQLインジェクション（SQLi）の脆弱性を検出し、修正するよう促しました。これは当然ながら一般的によいアドバイスで、SQLiの脆弱性がMOVEit Transferの**CVE-2023-34362**やFortinet FortiClientの**CVE-2023-48788**（後者は、本レポートの校了には間に合いませんでした）などの最近の注目度の高いエクスプロイトチェーンで使用されていることを鑑みればなおさらです。多くのSQLiの脆弱性は、侵入テスター、バグバウンティハンター、製品セキュリティコードレビュー担当者にとって「簡単に解決できるもの」と見なされています。

とはいえ、2023年のCISAのKEVリストに含まれているSQLi脆弱性はわずか3件で、2024年3月の時点でKEVに掲載されているのは1件です。同様に、過去3年間のRapid7脆弱性インテリジェンスデータセットにも主要なSQLi欠陥3件（SonicWall SMA 100シリーズの**CVE-2021-20016**、Progress Software MOVEit Transferの**CVE-2023-34362**、Accellion FTAの**CVE-2021-27101**）のみが含まれていますが、これら3件すべてがゼロデイとして広く悪用され、Accellion FTAとMOVEit TransferがCl0p大量恐喝キャンペーンで使用されたことは見逃せません。

概して、政府のガイダンスの焦点となっている脆弱性クラスと、コマンドインジェクションの問題など、エンタープライズソフトウェアで不均衡に多く見られ、悪用されている脆弱性クラスとの間には、ある程度の差があるようです。しかし、CISA（や他の機関）の任務範囲からすれば、適用により特定のカテゴリーのエンタープライズテクノロジー（ネットワークアプライアンスなど）が恩恵を受ける可能性があったとしても、エンタープライズソフトウェアの脆弱性が政府発行のガイドラインの主な対象とはならない可能性は十分にあります。エンタープライズソフトウェアメーカーは、政府発行のガイダンスに従うと同時に、開発、静的解析やセキュリティテストにおいて、他の一般的な脆弱性クラスも考慮する必要があります。

セキュリティ担当者のための実践的なガイダンス

MFAの実装、テスト、適用を最優先する。2023年にRapid7が調査したインシデントの40%以上は、特に VPN、VDI、SaaS製品でのMFAの欠落や一貫性がないことを理由に発生していました。Rapid7 MDRでは、通知疲れの結果**MFAプッシュ詐欺**が増加していることも確認しています。多くのMFAベンダーは、MFA疲れの予防手段として**数値の一致**を提供しています。組織は、対象となるあらゆる場所でMFAを実装して適用する必要があります。組織が使用する主要テクノロジーでMFAがサポートされていない場合は、サプライヤーに今後のロードマップにこの機能を含めるよう依頼することを検討してください。

盲信せず、検証する。組織は、信頼を前提としたり暗示したりしないモデルに移行し、最小権限の原則を適用する必要があります。例えば、ブロックリストではなく許可リストを標準の運用手順にする、きめ細かいアクセス制御を実装する、ユーザーとアクセスレベルを定期的に確認（加えて削除）するなどの策が考えられます。

インターネットへの露出の継続的な低減に積極的に取り組む。インターネット上に存在する資産は可能な限りオフラインに移行します。ポート、サービス、インターフェイス、コンセントレータ、アプライアンスなど、パブリックインター

ネットに公開されているものはすべて、敵の列挙や悪用、ゼロデイ攻撃の潜在的な標的と見なす必要があります。外部と内部のすべてをスキャンし、オフラインにできない場合は、構成を強化するためのベンダーのガイダンスを参照してください。

クラウド、オンプレミス、その間のあらゆる場所において強力でプロアクティブな脆弱性リスク管理プログラムを必須とする。堅牢な**脆弱性管理**は、セキュリティプログラム成功の基盤の1つとなります。プロアクティブな脆弱性管理の規律と強力かつ日常的な**パッチ管理**慣行がなければ、危機に際して組織が実効性のある緊急パッチ適用へとレベルを上げることは非常に困難です。影響を受ける製品が環境内に存在するかどうかを把握せずに危機時に断固とした行動をとることは難しいため、堅牢なインベントリ・資産管理の実践も不可欠です。セキュリティ境界デバイス、インターネットに接続されたロードバランサー、DevOpsツールとパイプラインソリューション、仮想化インフラストラクチャなど、重要かつ無防備なシステムを特定してカタログ化します。より基本的な情報については、Rapid7の**セキュリティプログラムの基本**に関するガイダンスを参照してください。

重要なテクノロジーに対して「ゼロデイ」パッチ適用手順を実装する。ネットワークエッジデバイスは特にNデイ/ゼロデイ攻撃のリスクに晒されるため、ベンダーが提供するパッチや回避策が利用可能になり次第、これらのデバイスの脆弱性を軽減する必要があります。ログが有効であり、機能していることを確認することで、セキュリティチームはインシデント発生時に侵害の兆候やその他の疑わしいアクティビティをより効果的に探せるようになります。

バックアップ戦略を2倍（または3倍）にする。ランサムウェアの発生状況は世界中でパンデミックレベルに達しており、医療と重要なインフラストラクチャは**特に高いリスクに**晒されています。組織は、オフサイトで企業ネットワークに接続されていないバックアップを含む複数のバックアップを維持することで、ランサムウェアへの備えと回復力を強化できます。これでランサムウェア攻撃を阻止できるわけではありませんが、侵害されていないバックアップがあれば、大規模なインシデントの際に組織の選択肢が広がり、ビジネスリーダーに身代金の支払いを思いとどまらせるのに役立つ可能性があります。

高度で貪欲な脅威エコシステムに直面する組織が壊滅的なデータ盗難や恐喝のリスクを軽減する最も重要な方法の1つは、**可能な限りデータの流出を特定し、防止する対策を講じる**ことです。

これには、以下のような対策が考えられます。

- 異常に大きなファイルのアップロードに際しての警告または制限、単一のIPやドメインへの大量のトラフィックに注意を向ける
- クラウドストレージ（Google Drive、SharePoint、ShareFileなど）への異常なアクセスの監視
- 既知のファイル共有サイト（filetransfer[.]io、anonfiles[.]com、mega[.]nz）をブロックするファイアウォールルールの監視や追加

- データ転送ユーティリティの存在や使用状況の監視（Filezilla、WinSCP/Putty、MegaCMD、BITSなど）
- データアーカイブユーティリティの存在や使用状況の監視（7zip、WinRAR、WinZipなど）
- 出力フィルタリングの実装
- ホストのローカル管理者権限の制限

関連資料

Rapid7の研究者やコミュニティメンバーは、Rapid7の公開リサーチプラットフォーム**AttackerKB**で脆弱性分析を公開しています。これらの分析には、エクスプロイトのタイムラインや攻撃チェーンの分析に加えて、サンプルコードや侵害の兆候が含まれています。Rapid7のAttackerKBへの投稿や通知の配信を登録するには、**こちらから無料アカウントを作成してください。**

Rapid7のゼロデイ脆弱性調査は**こちらで定期的に発表されています。**

新たな脅威が発生した場合、Rapid7は**緊急脅威**セクション（**Rapid7ブログ**）でRapid7顧客向けの対応情報とガイダンスを提供しています。Rapid7をご利用のお客様からのフィードバックをお待ちしております。カスタマーサクセスマネージャー（CSM）またはテクニカルアカウントマネージャー（TAM）にご連絡いただくか、**research@rapid7.comまでお寄せください。**

付録

本レポートの基礎となるデータにはRapid7が特定年に評価したCVEや脅威すべてが含まれているわけではありませんが、広範囲にわたる攻撃に重点を置いた、攻撃者のユースケースやエクスプロイトのケーススタディの多様なサンプルが含まれています。私たちの意図は、特定のCVEまたは脆弱性グループが他のCVEまたは脆弱性グループよりも重要でないことを意味することではありません。セキュリティチーム、ネットワーク管理者、そしてセキュリティ担当者は、概して、自社環境においてどの資産が重要で、取るべきアクションがビジネスの優先事項にどう影響するかを深く理解しています。私たちが提供するのは、攻撃者中心の脆弱性環境に対する見方です。Rapid7のお客様やセキュリティコミュニティは、より大規模な多層防御戦略の一環として採用しているポリシーやプラクティスの参考にするためにこうした視点を活用できます。

方法論に関する注記

本レポートで取り上げているCVEの大半は、2023年と/あるいは2024年の最初の2か月間に実際に悪用されたものです。本レポートで実際に悪用されたものとして分類したCVEの他にも、2023年と2024年に悪用された脆弱性は存在します。例えば、実際に悪用されているリストに頻繁に登場する多くの中小企業向けテクノロジー（中小企業向けルーターなど）は除外しています。また、実際に悪用されていることが判明しているほとんどのブラウザ、モバイル、ホストベースの脆弱性（Internet Explorer、Chrome、Firefox のバグ、iOSおよびmacOS のバグなど）に加え、Adobe Flash PlayerやAdobe Acrobatなどのアプリケーションで悪用された脆弱性も除外しています。Google Project Zeroでは、ブラウザ、モバイル、ホストベースの脆弱性を中心に、2023年に実際に悪用されたその他のゼロデイ脆弱性のスプレッドシートを**こちら**で公開しています。

データの信頼性は重要であるため、実際に悪用されている脆弱性としてリストアップした脆弱性については可能な限り**一次ソース**を引用しています。したがって、脆弱性を検出、検証、報告した組織や個人の悪用に関する直接報告を参照していることになります。本レポート全体で参照されている一次ソースには、既知の悪用に関する米国のサイバーセキュリティおよび諜報機関の警告、インシデント対応やその他の調査中に追跡した脅威と侵害の指標（IOC）に関するセキュリティ企業の分析、実際の悪用について明記しているベンダーの勧告（ゼロデイとして公開されているCVEを含む）などがあります。

読みやすさの向上のため、場合によっては、悪用に関するさまざまなレポートを集約したセキュリティニュース出版物の記事を引用することもあります。これは、特定の脆弱性が広く悪用されており、単一の記事でその脆弱性を文脈に沿って確認することが役立つ場合に特に有用です。読者にエクスプロイトの規模と影響をできるだけ早く理解してもらえることを目指し、ニュースソースを引用しています。

脅威の分類

ほとんどの場合、広範囲にわたる脅威とは、多くの悪意のあるアクターにより攻撃されている脆弱性を指します。2022年1月まで、ランサムウェアは一般的に利益を上げるために量に依存する大規模操作であると考えられていたため、ランサムウェア活動で悪用されたCVEはすべて広範囲にわたる脅威として分類していました。このポリシーは、**標的型ランサムウェア**に関する統計の進化に対応するため2022年に変更されました。2023年以降は、既知の攻撃者の数に依拠せず、**既知の実際の侵害**の数を使用して、広範囲にわたる脅威を他の悪用された脆弱性と区別しています。この変更は主に、単一の脅威アクター（Cl0p など）による組織的な大規模侵害イベントの数の増加に対応するために行われました。

「実際に悪用されている」に分類される脅威は、簡単に言うと、本書の執筆時点では広く悪用されていることは知られていません。より広範な悪用の具体的な技術的証拠が存在するものの、公開されていない可能性があります。同様に、執筆時点では差し迫った脅威カテゴリーに含まれるCVEが実際に悪用されているという証拠はありませんが、証拠がないからといって悪用されていないわけでもありません。

ランサムウェアに関する引用

当社では、ランサムウェアオペレーターによる特定のCVEの使用を記録するため、セキュリティニュース記事を頻繁に使用しています。本レポートでのランサムウェアに関する引用については、ランサムウェアグループによる脆弱性の使用に関する信頼できる**技術的**な証拠がある場合も、そうでない場合もあります。確認されていないということは、CVEがランサムウェア活動で使用されていないことを意味するのではなく、その結論を裏付けるだけの独立検証可能な詳細が確認されていないというだけのことです。信頼できる情報源には通常、独自の分析、リスクに関するより大きなストーリーを構築するために一次情報源を集約したニュース記事、公開プラットフォーム（ソーシャルメディア、ユーザーフォーラム、その他のパブリックコメントなど）の専門家の解説の組み合わせが含まれます。一般に、定評ある専門家ではなく個人やあまり知られていない組織からの報告に関しては、その主張を裏付けるため、ペイロード、観察されたエクスプロイト後の行動、脅威アクターの帰属、IOC、攻撃チェーン分析などの技術情報を探します。

悪用が判明するまでの時間（TTKE）の計算

タイムラインの作成と伝達は、リスク評価で最も難しい部分の1つです。悪用が判明するまでの時間（TTKE）を計算する際は、可能な限り、脆弱性の存在に関する最初の信頼できる公開リファレンスと、実際に悪用されたことに関する最初の信頼できる公開リファレンスを使用するように努めます。多くの場合、新しいCVEの存在に関する最初かつ最も権威のある情報源はベンダーのアドバイザリですが、ゼロデイ攻撃が広まり、公開での議論が盛んな現在では、コミュニティを参照した方がベンダーの速報を待つよりも早い場合があります。最初の2つの**ProxyNotShell**の脆弱性（**CVE-2022-41040** と**CVE-2022-41082**）はその一例です。National Vulnerability Database（NVD）などの情報源を公開の基準日として使用することはほとんどありません。こうした日付は、公開された（攻撃者も含む）情報から数日、または数週間遅れる傾向があるためです。

重要：エクスプロイトに関する最初の報告は、その名のとおり最初の報告にすぎません。公開分析がリリースされる前に悪用が開始された可能性があり、多くの場合、その可能性は高いものです。TTKEデータは、観察された日より前に脆弱性が悪用されなかったという証拠として受け取るべきではありません。

用語集

脅威のステータス

広範囲にわたる脅威：複数の業種や地理的な場所にわたり多くの組織を危険に晒すために使用される脆弱性またはその他の悪用可能な状態。

脅威：サイバー脅威インテリジェンス（CTI）の用語では、脅威は、行動する意図、能力、機会を持つ敵対者がいる場合に発生するとされます。一方脆弱性調査の文脈における「脅威」は、敵対者が実世界の本番環境を悪用するために使用した脆弱性などの攻撃ベクトルを示すために使用され、それが必ずしも多数の組織を侵害するために使用されているとは限りません。また、APTやランサムウェアグループなど、攻撃を行う主体を指すこともあります。

差し迫った脅威：現時点では実際に悪用されたことがまだ知られていないものの、将来悪用される可能性が高いと思われる脆弱性などの攻撃ベクトル。Rapid7の調査に含まれる差し迫った脅威のほとんどは、頻繁に攻撃を受けるテクノロジー（ネットワークエッジデバイスなど）、既知のエクスプロイトやその他のツールが利用可能なテクノロジーの脆弱性です。

攻撃者ユーティリティ

クラウド環境の侵害：リモートでのコード実行や、クラウドアカウント、クラウドゲートウェイ、API管理製品の乗っ取りなど。2023年版よりクラウドインフラストラクチャの侵害に代わり登場しています。

情報漏えい：機密データ（認証情報やその他の機密、環境変数など）を漏えいさせたり、ターゲット上のファイルを列挙したりする能力。情報漏えいの脆弱性は通常、攻撃者に単体でコードを実行させるのではなく、エクスプロイトチェーンの二次的な部分（リモートコード実行など）を可能にするプリミティブとして機能し、認証後の脆弱性を認証前の脆弱性に変えるのに役立ちます。

ITセキュリティ管理の侵害：ネットワーク、デバイス、エンドポイント管理テクノロジーのリモートコード実行や乗っ取り、シングルサインオン（SSO）やActive Directory（AD）管理ソリューションなどのIDおよびアクセス管理ソリューション、その他のセキュリティ製品のリモートコード実行または乗っ取り。2021年版まではネットワークインフラストラクチャの侵害と呼んでいました。

ネットワークピボット：VPN、ファイアウォール、ルーター、その他のゲートウェイデバイスなどのインターネットに接続されたシステムを悪用し、外部ネットワークから内部ネットワークにピボットする機能。ネットワークピボットは、攻撃者に内部トラフィックと外部トラフィックの両方を可視化し、ターゲットネットワーク内でのデータ流出、トラフィックスニッフィングやさらなる攻撃を支援します。

権限昇格：攻撃者がすでに何らかのアクセスを有しているシステム上でローカルにコードを実行する機能。脆弱なアプリケーションを実行しているユーザーとしてコードを実行するなどの目的で使われます。2022年版までローカルコード実行と呼ばれていました。

リモートコード実行（RCE）：リモートターゲットでのコード実行。通常、ターゲットシステム上でペイロードを実行する機能を指し（シェルセッションの取得など）、認証情報の窃取やデータ流出などを支援します。

「スマッシュ&グラブ」恐喝：2023年版から登場した新しい攻撃者ユーティリティ。攻撃者が標的のシステムにアクセスし、潜在的に大量のデータを迅速に流出させることを可能にするファイル共有プラットフォームや安全に管理されたファイル転送アプリケーション（クラウドまたはオンプレミス）の脆弱性に関するものです。ランサムウェアや恐喝攻撃の標的となることがよくあります。

ソーシャルエンジニアリング：ユーザーに悪意のある添付ファイルをクリックさせたりプレビューさせたりする脆弱性など（電子メールベースやドキュメントベースの攻撃など）。

サプライチェーンの侵害：2023年以降のデータに登場した新たな攻撃者ユーティリティ。CI/CDパイプラインやその他の重要なソフトウェアサプライチェーンインフラストラクチャの乗っ取りを可能にする脆弱性、または正当なソフトウェアにバックドアが設けられたり、悪意を持って変更されたりした検証済みのインシデントを指します。

脆弱性のクラス

逆シリアル化は、アプリケーションがデータを移植可能な形式からその言語固有のデータ型に変換できるプロセスです。Java、.NET、Python、Rubyなど、多くの最新言語が逆シリアル化をサポートしています。ネイティブ言語にロードされたデータが悪意のある第三者により改ざんされる可能性がある場合、逆シリアル化プロセスはセキュリティ上の脅威となる可能性があります。一般的な攻撃では、オペレーティングシステムコマンドを実行するために必要な引数を持つメソッドを呼び出すようにデータを構成し、ロード中のアプリケーションのコンテキストでコマンドが実行されます。このセキュリティ問題に対する一般的な解決策には、データの信頼性を確保するためにデータに暗号で署名することや、ロードが許可されているデータ型のホワイトリストを利用することなどがあります。関連CWE：**CWE-502**

不適切なアクセス制御とは、システムへの特定のインターフェイス（ほとんどの場合リモートからアクセス可能なAPI）へのアクセス制御が欠落しているか不十分であることを意味します。認証を目的とした暗号化の不適切な使用もこの脆弱性クラスに該当します。この問題の一般的な解決策としては、すべての機密インターフェースに対する適切な認証、承認、アカウンティングの実装、関連するすべてのシークレットの安全な管理が挙げられます。関連するCWEの例：**CWE-285**、**CWE-200**、**CWE-287**、**CWE-732**

メモリ破損は、さまざまな手段でデータを悪用してメモリを改変し、予期せぬ動作を引き起こす脆弱性の大きなカテゴリーです。この脆弱性クラスには、不適切な境界強制、型の混乱、初期化されていないデータの使用、解放後のデータ使用などが含まれます。これらの脆弱性はメモリセーフではないとされる言語でよく見られるものです。メモリ破損の脆弱性が悪用されると、実行中のアプリケーションのコンテキスト内で任意のコードが実行されたり、未処理の例外によりアプリケーションがクラッシュし、サービス拒否（DoS）状態がトリガーされたりする可能性があります。この問題の一般的な解決策には、通常、データの読み込みや保存に使用されるものなど、主要な操作のパラメーターに対する検証の追加が含まれます。これらのクラスの脆弱性の悪用は、オペレーティングシステム、コンパイラ、アプリケーション用に開発されたさまざまな緩和テクノロジー（kASLR、Control Flow Guard、win32k Type Isolationなど）により、近年複雑になっています。関連するCWEの例：**CWE-787**、**CWE-125**、**CWE-416**、**CWE-190**、**CWE-476**

インジェクションは、関連システムにより特定の方法で解釈される特別に作成された入力に関連する脆弱性の大きなカテゴリーです。Webアプリケーションで最も一般的に見られるインジェクション攻撃は、解釈されるデータの種類（SQL、LDAP、OSコマンドなど）によって細分化されることがよくあります。これらの脆弱性の根本原因は、ほとんどの場合、悪意のある第三者から受け取ったデータのサニタイズが不十分であることです。これらの脆弱性の悪用は確実に実行可能な傾向があり、意図しない限り（SQLやOSコマンド経由など）、サービス低下を引き起こすことはめったにありません。

ロジックが実行されるコンテキストは、通常、ロジックの解釈方法によって異なります。例えば、Webアプリケーションの場合、SQLインジェクションはバックエンドデータベースサーバーで実行され、OSコマンドはフロントエンドWebサーバーでインジェクションされ、JavaScriptはエンドユーザーのブラウザで実行されます。したがって、このクラスの脆弱性は、通常、1つのシステムの脆弱性が他のシステムの整合性を損なうという点で独特です。この問題の一般的な解決策は、通常、許可リストを使用してパラメータに厳格なサニタイズを実装することです。関連するCWEの例：**CWE-79**、**CWE-20**、**CWE-89**、**CWE-94**

参考文献

このリストを作成してくれたRapid7のCynthia Wyreリサーチプロジェクトマネージャーに心から感謝します。

セキュリティ研究は、コミュニティ全体での取り組みです。本レポートは、以下に挙げる各氏を始めとする多数の個人研究者や研究チームの研究内容を活用しています。

Adobe Security Bulletin (2023年)

Adversary Tactics and Intelligence Team, Deepwatch (2023年)

Alexander Martin, The Record, Recorded Future News (2023年)

Alexander Marvi, Brad Slaybaugh, Ron Craft and Rufus Brown, Mandiant (2023年)

Alexander Marvi, Shawn Chew, and Punsaen Boonyakarn, Mandiant (2024年)

Alex Delamotte, SentinelOne (2023年)

Alex Delamotte and Christian Vrescak, SentinelOne (2023年)

米国薬剤師協会 (2024年)

Austin Larsen, John Palmisano, John Wolfram, Mathew Potaczek, and Matthew McWhirt, Mandiant (2023年)

Barracuda (2023年)

Becky Bracken, Dark Reading (2023年)

Benoit Sevens, Google (2023年)

Bill Toulas, Bleeping Computer (2023年)

Bill Toulas, Bleeping Computer (2023年)

Bill Toulas, Bleeping Computer (2023年)

Bill Toulas, Bleeping Computer (2024年)

Bill Toulas, Bleeping Computer (2024年)

boB Rudis, GreyNoise (2023年)

Boris Larin, Kaspersky Securelist (2023年)

Brendan Watters, Rapid7 (2023年)

Caitlin Condon, Infosecurity Magazine (2024年)

Caitlin Condon, Rapid7 (2023年)

Caitlin Condon, Rapid7 (2023年)

Caitlin Condon, Rapid7 (2023年)

Caitlin Condon, Rapid7 (2023年)

Caitlin Condon, Rapid7 (2023年)

Cara Lin, Fortinet (2023年)

CERT Polska, NASK (2023年)

Christiaan Beek, Rapid7 (2024年)

Ciaran Martin, Ciaran's Crispy Cogitations (2024年)

CISA Cybersecurity Advisory (2023年)

CISA Cybersecurity Advisory (2023年)

CISA Cybersecurity Advisory (2023年)

CISA Cybersecurity Advisory (2023年)

CISA Cybersecurity Advisory (2023年)

CISA Cybersecurity Advisory (2024年)

CISA Cybersecurity Alerts (2023年)

CISA Cybersecurity Alerts (2023年)

CISA Cybersecurity Alert (2023年)

CISA Cybersecurity Alert (2023年)

CISA Cybersecurity Alert (2023年)

CISA Cybersecurity Alert (2023年)

CISA Fact Sheet (2022年)

CISA Known Exploited Vulnerabilities Catalog (2023年)

CISA Known Exploited Vulnerabilities Catalog (2023年)

CISA Known Exploited Vulnerabilities Catalog (2023年)

CISA Known Exploited Vulnerabilities Catalog (2023年)

CISA Known Exploited Vulnerabilities Catalog (2023年)

Cisco Talos (2023年)

Cisco Talos (2023年)

Clayton Zechman, Rapid7 (2023年)

Clement Lecigne and Maddie Stone, Google Threat Analysis Group (2023年)

Daniel Lydon and Conor Quinn, Rapid7 (2023年)

Daniella Silva and Aria Bendix, NBC News (2024年)

Devna Bose, The Associated Press (2024年)

Dietrich Knauth, Reuters (2024年)

Drew Burton, Rapid7 (2023年)

Drew Burton, Rapid7 (2023年)

F5 (2023年)

FBI Internet Crime Report (2023年)

Francesco Figurelli and Eduardo Ovalle, Kaspersky Securelist (2023年)

Fortra (2023年)

Fortinet PSIRT (2023年)

Fortinet PSIRT (2023年)

Glenn Thorpe, Rapid7 (2023年)

Glenn Thorpe, Rapid7 (2023年)

Global Threat Intelligence, Fox-IT (2023年)

Google Threat Analysis Group (2023年)

Hans-Martin Münch, Mogwai Labs (2023年)

米国保健福祉省保健セクターサイバーセキュリティ調整センター (HC3) (2023年)

Huntress (2023年)

Ionut Ilascu, Bleeping Computer (2023年)

Ivanti (2023年)

Ivanti (2023年)

Ivanti (2023年)

Jacob Baines, VulnCheck (2023年)

James Nugent, Foti Castelan, Doug Bienstock, Justin Moore, and Josh Murchie, Mandiant (2023年)

James Sadowski and Casey Charrier, Mandiant (2023年)

Jeff Johnson, Fred Plan, Adrian Sanchez, Renato Fontana, Jake Nicastro, Dimiter Andonov, Marius Fodoreanu, and Daniel Scott, Mandiant (2023年)

Jonathan Greig, The Record, Recorded Future News (2024年)

Joint Cybersecurity Advisory, CISA (2023年)

Joint Cybersecurity Advisory, CISA (2024年)

Kaspersky (2024年)

Kate Morgan, Google Threat Analysis Group (2023年)

KFF Health News, U.S. News and World Report (2024年)

Lawrence Abrams, Bleeping Computer (2022年)

Levi Broderick (GrabYourPitchForks) (2020年)

Malpedia (2024年取得)

Mark Ellzey, Censys (2023年)

Margaret Zimmermann, Palo Alto Unit 42 (2023年)

Mathew J. Schwartz, Bank Info Security (2023年)

Mathew J. Schwartz, Bank Info Security (2023年)

Matthew Meltzer, Robert Jan Mora, Sean Koessel, Steven Adair, and Thomas Lancaster, Volexity (2024年)
Microsoft Defender Threat Intelligence (2023年)
Microsoft Incident Response, Microsoft (2023年)
Microsoft Threat Intelligence, Microsoft (2023年)
Microsoft Threat Intelligence, Microsoft (2023年)
Microsoft Threat Intelligence, Microsoft (2023年)
Microsoft Threat Intelligence, Microsoft (2023年)
Microsoft Threat Intelligence, Microsoft (2023年)
Mike Whitehead (2023年)
MITRE (2017年)
MITRE (2022年)
ノルウェー国家安全保障局 (2023年)
米国司法省広報局 (2023年)
米国司法省広報局 (2023年)
米国司法省広報局 (2023年)
米国国務省報道官室 (2024年)
Peter Gimus, Trend Micro (2023年)
Project Zero, Google (2019年)
Rapid7 (2020年)
Rapid7 (2021年)
Rapid7 (2023年)
Rapid7 (2023年)
Rapid7 (2023年)
Rapid7 (2023年)
Rapid7 (2023年)
Rapid7 (2023年)
Rapid7 (2023年)
Rapid7 (2023年)
Rapid7 AttackerKB (2024年)
Rapid7 AttackerKB (2023年)
Rapid7 AttackerKB (2023年)
Rapid7 AttackerKB (2023

Rapid7 AttackerKB (2023年)
Rapid7 AttackerKB (2023年)
Rapid7 AttackerKB (2023年)
Rapid7 AttackerKB (2023年)
Rapid7 AttackerKB (2023年)
Rapid7 AttackerKB (2023年)
Rapid7 AttackerKB (2023年)
Rapid7 AttackerKB (2023年)
Rapid7 AttackerKB (2023年)
Rapid7 AttackerKB (2023年)
Rapid7 AttackerKB (2023年)
Rapid7 AttackerKB (2023年)
Rapid7 AttackerKB (2023年)
Rapid7 AttackerKB (2023年)
Rapid7 AttackerKB (2023年)
Rapid7 AttackerKB (2023年)
Rapid7 AttackerKB (2023年)
Reuters (2024年)
Rodel Mendrez, Trustwave (2024年)
Ron Bowes, Rapid7 (2023年)
Ron Bowes, Rapid7 (2023年)
Ron Bowes, Rapid7 (2023年)
Ron Bowes, Rapid7 (2023年)
Ron Southwick, Chief Healthcare Executive (2023年)
Ryan Emmons and Evan Malamais, Converge Technology Solutions (2023年)
Sandra Radesky and Gabriel Davis, CISA (2023年)
SentinelOne (2023年)
Sergiu Gatlan, Bleeping Computer (2023年)
Scott Downie, Devon Ackerman, Laurie Iacono, and Dan Cox, Kroll (2023年)
Shadowserver (2023年)
Shelby Pace, Rapid7 (2023年)
Sophos X-Ops (2023年)
Stefan Hostetler, Markus Neis, and Kyle Pagelow, Arctic Wolf (2023年)
Stephen Fewer, Rapid7 (2023年)
Stephen Fewer, Rapid7 (2023年)
Stephen Fewer, Rapid7 (2023年)
Tara Seals, Dark Reading (2023年)
Tara Seals, Dark Reading (2024年)
The Censys Research Team, Censys (2023年)
トレンドマイクロセキュリティ速報 (2023年)
Tyler McLellan, John Wolfram, Gabby Roncone, Matt Lin, Robert Wallace, Dimiter Andonov, Mandiant (2024年)
Tyler Starks, Christiaan Beek, Robert Knapp, Zach Dayton, and Caitlin Condon, Rapid7 (2023年)
Unit 42, Palo Alto (2023年)
マサチューセッツ大学ボストン校 (2024年)
米国司法省カリフォルニア州中央地区連邦検事局 (2023年)
Virginia Romero Sanchez-Herrero, S-RM Intelligence and Risk Consulting (2023年)
VMware Security Advisory (2023年)
Will Dorman (2023年)
ホワイトハウスプレスリリース (2024年)

エンドポイントから クラウドまで、 攻撃者の一歩先を。

Rapid7について

Rapid7は、デジタルトランスフォーメーションの加速に直面する組織のセキュリティプログラム強化の支援を通じ、あらゆる人にとってより安全なデジタルの未来を創造しています。最高レベルのRapid7のソリューションポートフォリオは、セキュリティ担当者がリスクを管理し、アプリからクラウド、従来のインフラストラクチャ、ダークウェブに至るまで、脅威のランドスケープ全体にわたって脅威を排除するための支援を提供します。Rapid7は、オープンソースコミュニティと最先端の研究を促進し、得られる洞察を製品の最適化に活用し、最新の攻撃方法に対応する力を世界のセキュリティコミュニティに届けます。世界中の11,000社以上のお客様組織に信頼され、業界をリードするソリューションとサービスで、企業が攻撃者の一歩先を行き、競争に先んじ、常に将来に備えるためのお手伝いをします。

RAPID7

製品

クラウドセキュリティ
XDR & SIEM
脅威インテリジェンス
脆弱性リスク管理
アプリケーションセキュリティ
オーケストレーションと自動化
マネージドサービス

お問い合わせ

rapid7.com/ja/contact

詳細と無償評価版については、https://www.rapid7.com/ja/trial/insight/を参照してください。