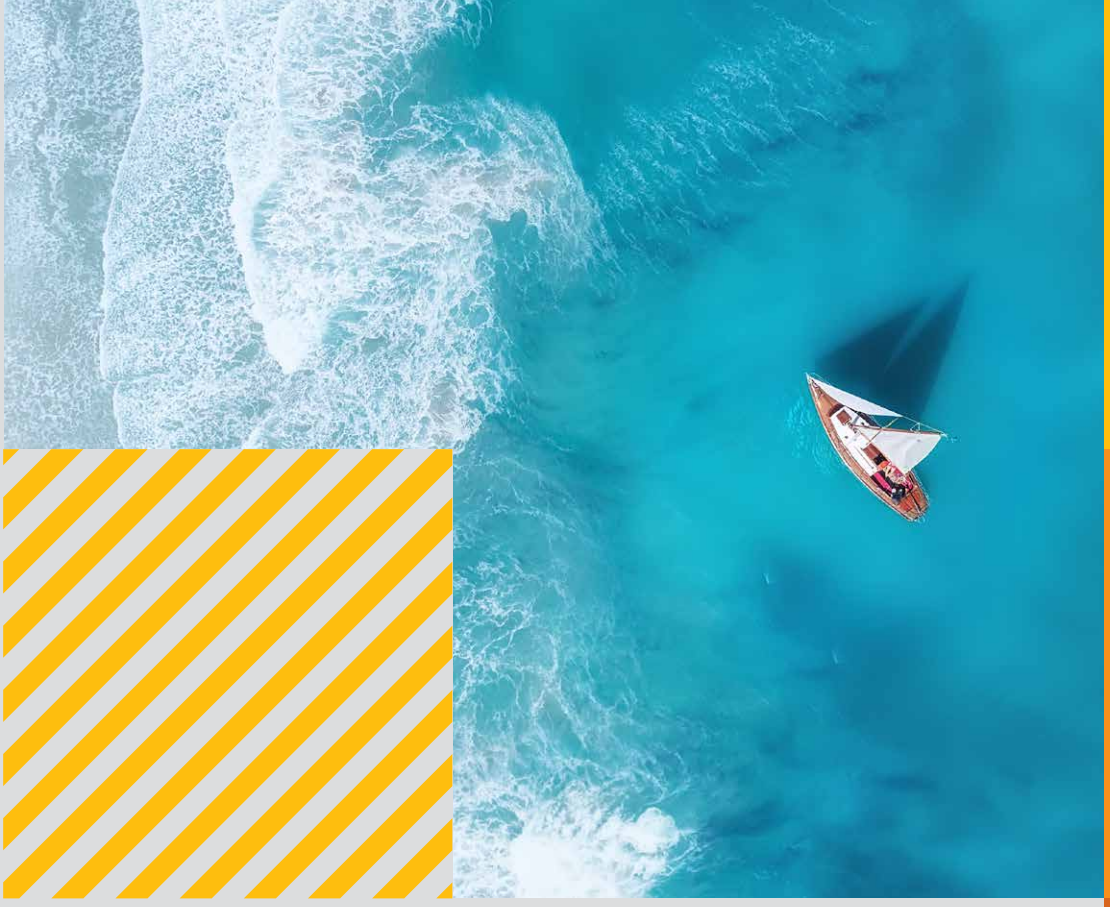


サイバー脅威

——2024年を振り返る

pwc

www.pwc.com/jp

エグゼクティブサマリー

本レポート「サイバー脅威――2024年を振り返る」の目的は、2024年全体の状況を振り返り、直近の傾向やテーマを明確にすることです。これは、PwCのサイバー脅威インテリジェンスチームが追跡してきたあらゆる地域と動機にわたる膨大な脅威活動を要約することにもつながります[1]。

本レポートの知見は、2024年を通じて、直接的な情報収集と、PwCのグローバルインシデント対応チームおよびマネージドセキュリティチームとの緊密な連携により実施された分析から得られたものですが、現在検出されていない活動が存在する可能性もあります。私たちは、2024年の主な傾向を把握することで、2025年以降に組織が防衛力を強化し、状況をよりよく認識するために活用できる実用的な知見を提供することを目指しています。

2024年を振り返ると、サイバー脅威をもたらす活動は世界中で展開されており、一貫して活発な状況だったことが明らかになりました。重大な脆弱性が話題となる中、2024年のサイバー活動の動向は、主に不安定な地政学的情勢を含むいくつかの重要な出来事を反映したものとなりました。インシデント対応調査から得られた知見によると、ランサムウェアの蔓延とサイバー詐欺が相変わらず大きな影響を及ぼしていることが確認されました。

また、容易にアクセス可能な悪意あるコードベースの増加や、脅威アクターが攻撃を行うためのリソースが一般的に入手可能になったことも、サイバー脅威を巡る状況に影響を与えました。フォーラムやオープンソースのサイトには、安価な情報窃取マルウェアからAIを活用したフィッシングキット、ランサムウェアの暗号化バイナリ、概念実証済みのエクスプロイトコードまで、あらゆる「エコシステム」で溢れています。その恩恵を最も受けているのは、高度な技術を持たない脅威アクターたちです。

技術的水準がさほど高くない、サイバー犯罪の脅威活動が席巻する中、すでに諜報活動に従事している多くの者は、2024年を通じて新たなツール、テクニック、手順（TTP）の開発に取り組んでいました。この傾向は今後数年間、脅威の状況に影響を与えると考えられます。このような活動には、中国を拠点とする脅威アクターによる商用プロキシネットワークの広範な適用が含まれます。

1　PwCは脅威を与える活動の動機を「諜報活動」、「犯罪」、「ハクティビズム」、「妨害行為」の4つのカテゴリーに分類している。これらの定義の詳細については、本レポートの付属資料Aを参照。

また、北朝鮮を拠点とする脅威アクターは、大規模サプライチェーンへの攻撃から、より従来型の活動を全体的に増加させる傾向にあります。

さらに変化の激しい「海域」では、前年からの積極的なサイバー活動がほとんど衰えることなく続いており、その多くがより広範な地政学的要因によって引き起こされていることが観察されました。ロシアを拠点とする脅威アクターによる攻撃の多くは、引き続きウクライナとNATO加盟国を標的としたものでした。一方、イランを拠点とする脅威アクターによる侵入は、当該地域で深刻化する地政学的危機へのイランの関与を反映していました[2,3]。諜報活動を動機とする脅威アクター以外にも、ランサムウェア-アズ・ア-サービス（RaaS）エコシステムによる脅威は、2020年に主流となって以降、リークサイトに投稿された被害者数が過去最大となっています[4]。

被害を受けていない「海域」もありましたが、深刻な被害を受けているところもありました。従来の偽情報工作は2024年にも活発に行われ、ロシアやイランを拠点とする脅威アクターは、（年間を通じて行われた数々の選挙に関連する活動など）今後の状況に影響を与える目的で、典型的な諜報技術を活用しました。営利目的の諜報ウェアアクターのプロキシネットワークなど、以前から観察されていた新たな手法も、2023年と同様の形で「海域を濁らせるような」役割を果たしました。

2024年には、より従来型の手法への回帰として[5]、別の脅威アクターを装いながら活動を実行することを目的に、脅威アクターが別の脅威アクターのインフラを侵害する行為も見られました。2024年はまた、政府発行の脅威インテリジェンス報告書に、詳細な技術報告書を作成して対抗するという手法が導入されました。偽情報はその性質上、政治に関するものが多いと考えられていますが、中国を拠点とする脅威アクターの侵入をめぐって主導権を握ろうとする中国政府と米国政府による情報公開の応酬は[6,7]「海域」を汚染し、脅威にさらされた情報空間の透明性を低下させる新たな行為となりました。

PwCについて

PwCは世界149カ国で18万社を超えるクライアントにサービスを提供しており、世界有数の規模を誇るグローバルなプロフェッショナル・サービス・ネットワークという優位性を活かして、各クライアントに合わせたグローバルな脅威インテリジェンスサービスを各地域のクライアントに提供しています。PwCが実施する調査は、PwCのセキュリティサービスを支えるものであり、世界各地の公共・民間部門の組織において、ネットワークの保護、状況認識、戦略情報の提供に利用されています。

PwC サイバー脅威インテリジェンスは、PwCの検出能力と、脅威に焦点を当てた調査や新たな問題を認識する積極的活動を組み合わせ、悪意ある活動の検出における課題を特定・対策し、脅威に関する知識を深め、実用的な情報をレポートとしてまとめています。PwCの脅威インテリジェンスチームは、オーストラリア、カナダ、チェコ、ドイツ、イタリア、オランダ、ノルウェー、スウェーデン、英国、米国などグローバルなメンバーで構成されています。

また、PwCのメンバーファームのインシデント対応チーム、特にオーストリア、ブラジル、中東欧諸国、ドイツ、香港、アイルランド、日本、ノルウェー、英国のインシデント対応チームの貢献と知見も得ています。

2 'Risk of long-feared regional war rises as Israel and Iran swap threats',Al Jazeera, https://www.aljazeera.com/news/2024/10/2/risk-of-long-feared-regionalwar-rises-as-israel-and-iran-swap-threats (2nd October 2024)

3 'Iran shifted focus of cyberattacks from US to Israel,Microsoft says',Iran International, https://www.iranintl.com/en/202410165266 (16th October 2024)

4 アナリスト注記：機密データがリークサイトに掲載される前に指定された身代金を支払った組織が存在するほか、リークサイトを運営していないランサムウェアの脅威アクターも多数存在するため、リークサイト被害者の合計はランサムウェアの全ての被害者を網羅しているわけではない。（参照：'More LockBit 3.0 in the Asia Pacific',PwC Threat Intelligence,CTO-TIB-20241125-01A）.

5 'Hijacking of Iranian hacking infrastructure',Council on Foreign Relations, https://www.cfr.org/cyber-operations/hijacking-iranian-hacking-infrastructure (October 2019)

6 'People's Republic of China-Linked Actors Compromise Routers and IoT Devices for Botnet Operations',Joint Cybersecurity Advisory (US), https://media.defense.gov/2024/Sep/18/2003547016/-1/-1/0/CSA-PRC-LINKED-ACTORS-BOTNET.PDF (18th September 2024)

7 'Report reveals more conspiracies behind U.S.“ Volt Typhoon” misinformation campaign',Ministry of Public Security (CN), https://www.mps.gov.cn/n2255079/n6865805/n7355748/n7355818/c9806794/content.html (14th October 2024)

目次

セクション 1

大海原を超えて

2024年の特徴として、全ての動機において、サイバー脅威アクターの活動が全体的に増加していることが挙げられます。これは、不安定な地政学的情勢、政治におけるリーダーシップの変化、あらゆる動機における脅威アクターの利用可能な新規／従来型のツール、テクニック、手順（TTP）の増加が複合的に影響したものです。

前年から続く戦争は、引き続きこれに関わる脅威アクターが活動する重点的な領域となりました。その一方で、新たな紛争地域では、諜報活動、ハクティビスト、妨害行為といったさまざまな動機によるサイバー活動が増加しました。一方、サイバー犯罪エコシステムに関しては、テイクダウンのための努力が頻繁に講じられたにもかかわらず、ランサムウェアのリークサイト数やアクティブなアフィリエイトの数は2024年に過去最多を更新しました。

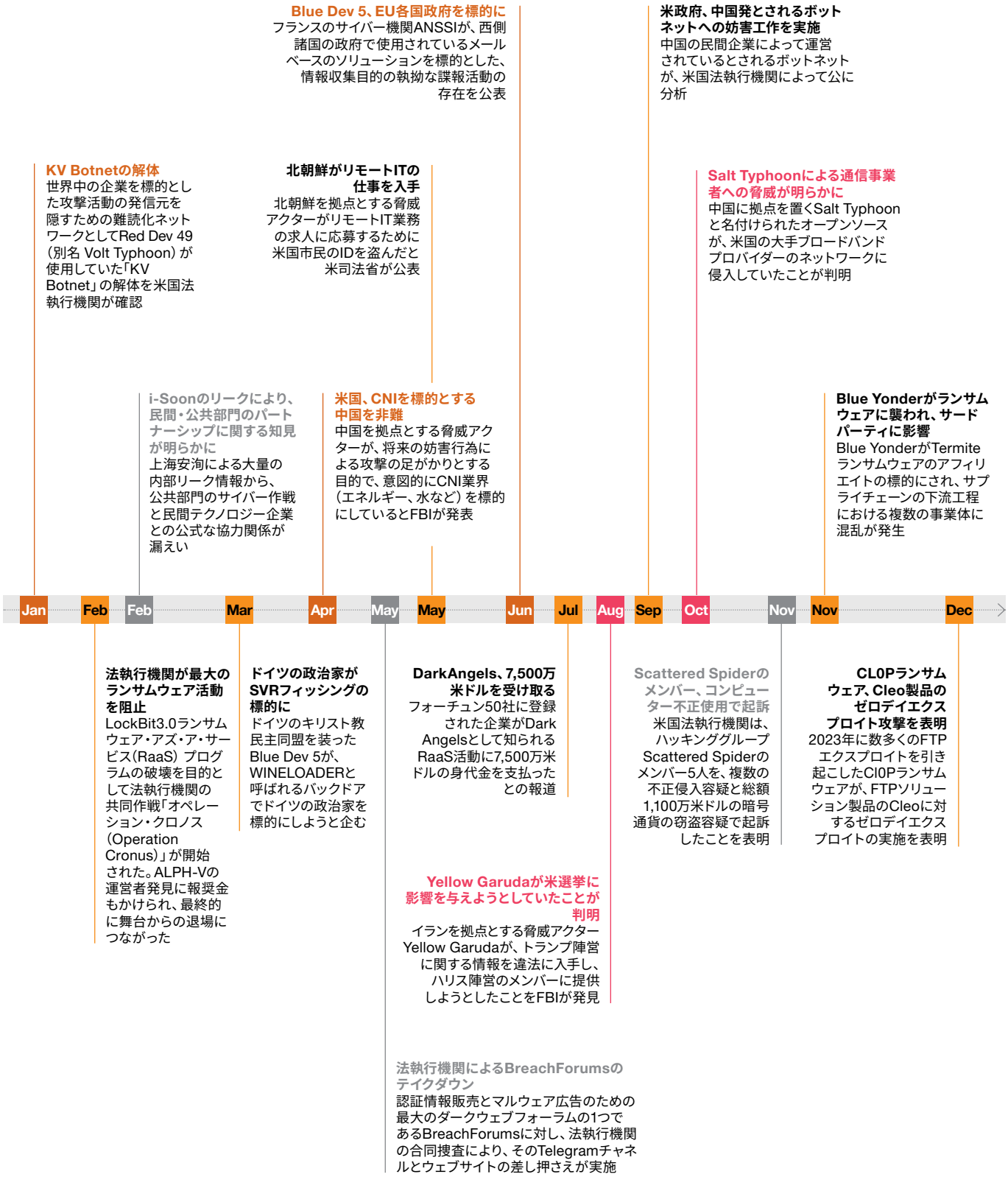
2024年のサイバー事象

次のページでは2024年における最も重大なサイバー事象を挙げています。年間を通じて見られたサイバー活動の活発化という傾向の中で、重要な事例を浮き彫りにしたものです。地政学的に不安定な状況が続く中、技術的水準の高いアプローチがより簡単に入手できるようになったこと、斬新なツールやテクニックの使用、妨害にあった場合の回復力が特徴として挙げられます。2024年は、欧米各国政府の法執行機関による、犯罪および諜報関連の脅威アクターを標的とした活動が活発だったことも特徴です。欧米の政府機関がこのような公的な作戦行動に積極的であることは、世界中の政府がサイバー脅威に対してより積極的なアプローチを採用していることを示しており、緊張が高まる世界を反映するものと言えます。

2024年も脆弱性の公開とそれが悪用された事例の両方が増加傾向にありました。この統計によると、2024年に公表された脆弱性の数は前年から31%増加し、これらの脆弱性の多くが幅広い業界に影響を及ぼしていることが明らかになりました[8]。

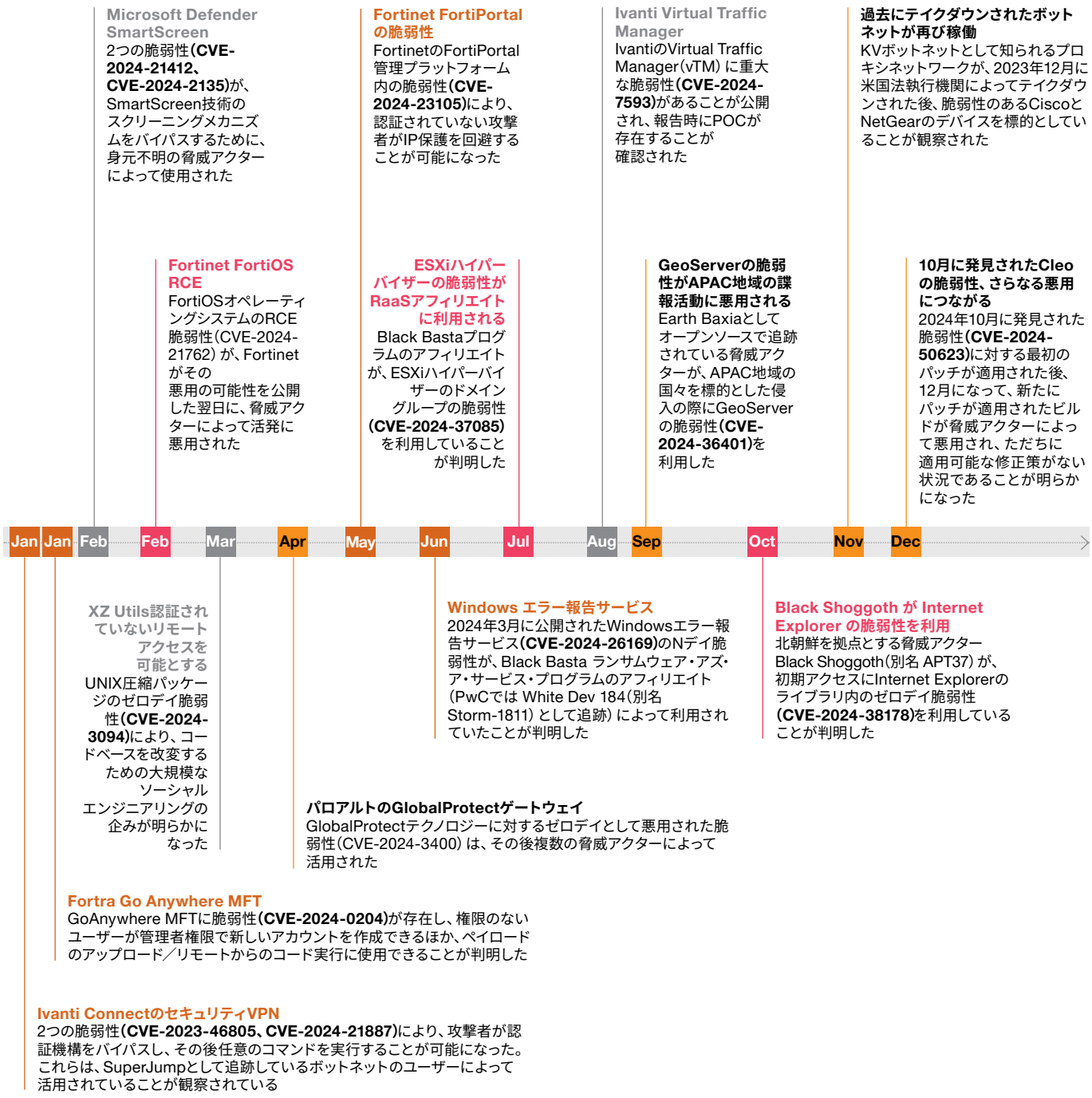
8　NVD、https://nvd.nist.gov/

図表1-2024年の主なサイバー事象



2024年に報じられた攻撃活動のうち最も重大な2つの事案は、Salt Typhoonによる世界的な通信事業者への侵害[9]と、CL0PによるCleoファイル転送プロトコル悪用の公表[10,11]でした。2024年末に発生したこれらの出来事は、2025年には動機を問わず初期アクセスを実施した脅威アクターによって、重要なシステムが引き続き悪用される可能性が高いことを示しています。

図表2-2024年に悪用された重大な脆弱性



9 The emerging Salt Typhoon', PwC Threat Intelligence, CTO-SRT-20241126-02A

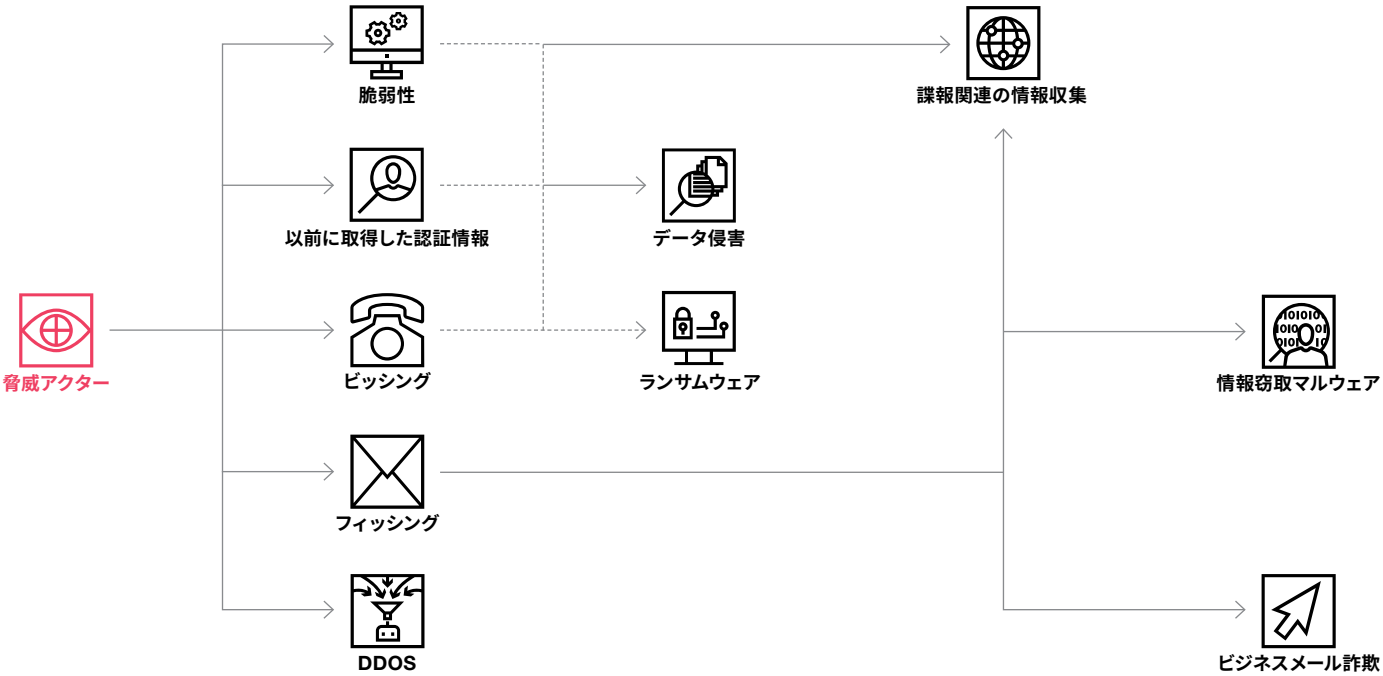
10 'Active exploitation of Cleo zero-day', PwC Threat Intelligence, CTO-TIB-20241212-01A

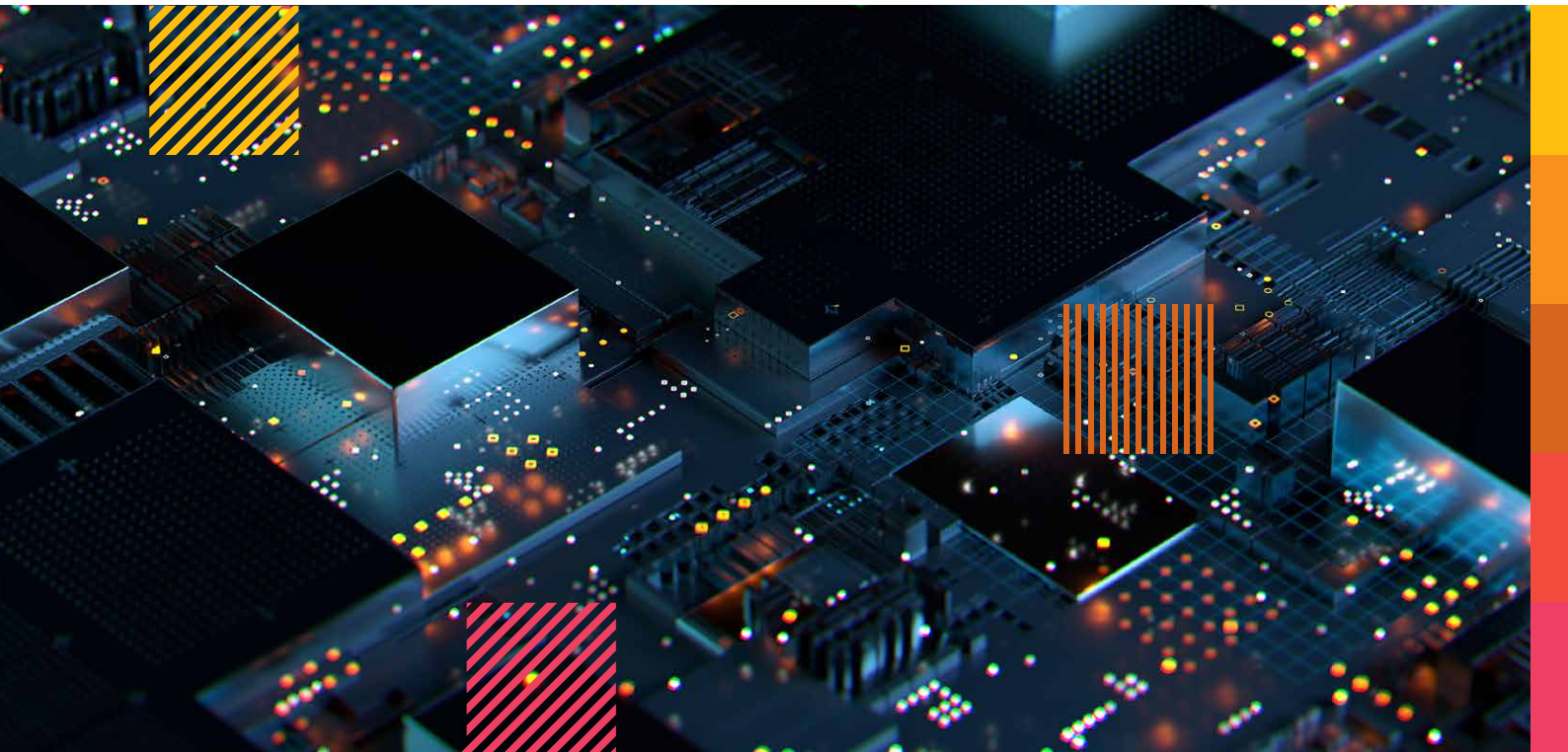
11 'Clop ransomware claims responsibility for Cleo data theft attacks', Bleeping Computer, https://www.bleepingcomputer.com/news/security/clop-ransomwareclaims-responsibility-for-cleo-data-theft-attacks/ (15th December 2024)

現場から見た2024年-インシデント対応チームからの報告

PwCのサイバー脅威インテリジェンスチームは、2024年にPwCグローバルネットワーク全体でインシデント対応チームと緊密に連携し、犯罪行為と諜報活動を動機とする脅威アクターに見られるいくつかの傾向を観察しました。私たちのデータによれば、ランサムウェアとビジネスメール詐欺（BEC）が引き続き最大の脅威ですが、技術的水準の低いデータ侵害とそれに関連する恐喝行為も観察されています。

図表3-2024年にPwCのインシデント対応調査で観察された最も重大な初期アクセスベクターとそれに伴う侵入





ランサムウェアやデータ侵害のケースにおいて、フィッシングのテクニックが含まれているケースはかなり少なく、その一方で、初期アクセスブローカー（環境にログインするために購入した認証情報）や脆弱性を利用するケースが多くなっています。これらのケースの大半は、ゼロデイではなく、以下に挙げるように、すでにパッチが適用された古い脆弱性[12]を狙ったものでした。

- Ivanti VPN Appliance
- Oracle WebLogic Server
- FortiClient EMS
- VEEAM
- ESXi NAS
- FortiGate SSLの脆弱性

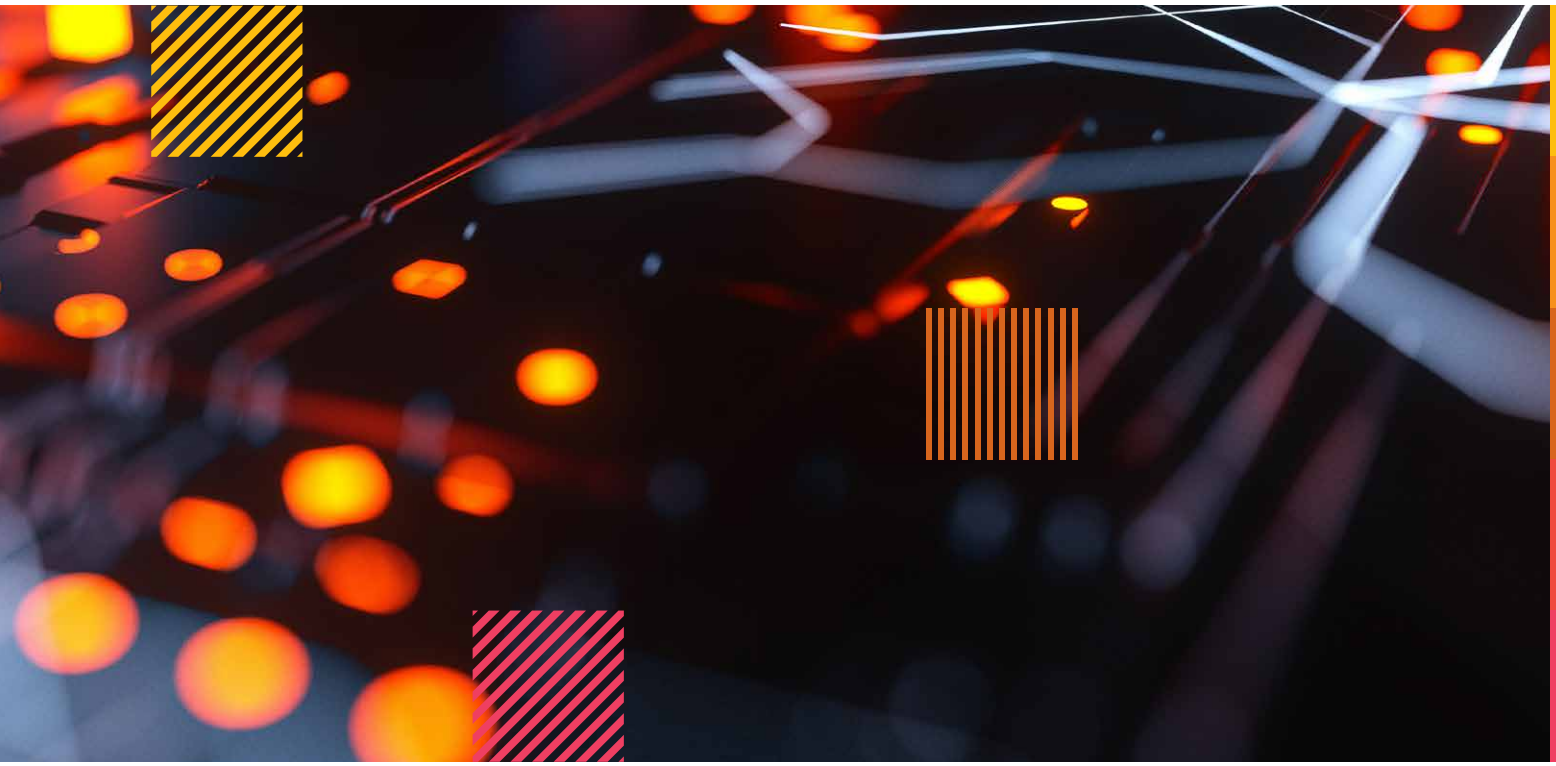
これらのデバイスの多くはエッジデバイスと呼ばれ、組織の周辺に置かれ、多くの場合、ネットワークアーキテクチャのインベントリから除外され、所有者がまだ稼働していることを知らないシャドーITとなります。このようなデバイスはパッチ配布の対象とならない場合が多く、外部からの脆弱性スキャンの餌食となります。

この傾向を示す顕著なケースとして、White Rabbit ランサムウェアが挙げられます。現実的な確率を考慮すると、侵害が発生した当時に新たに公開された2024年のFortiGateの脆弱性を脅威アクターが悪用したと考えられます。

70

「既知の脆弱性の悪用（Known Exploited Vulnerabilities）」カタログに追加されたCVEのうち、2024年より前に公表されたCVEと関連性があるものの件数

出所：https://www.cisa.gov/known-exploited-vulnerabilitiescatalog (data accessed 16th January 2025)



12 アナリスト注記：インシデント対応事例から観察したこの傾向は、西側諸国の諜報機関から発表された（以下のような）広範な過去のデータと必ずしも一致していない。「（2023年に）最も頻繁に悪用された脆弱性の大半は、当初ゼロデイとして悪用されたものであり、2022年から増加している。2022年は、悪用された主な脆弱性でゼロデイは半数以下であった」（参照：「日常的に悪用される主な脆弱性（2023年）」、共同サイバーセキュリティ勧告，https://media.defense.gov/2024/Nov/12/2003581596/-1/-1/0/CSA-2023-TOP-ROUTINELY-EXPLOITED-VULNERABILITIES.PDF（2024年11月12日））2024年の比較データはまだ入手できていないが、現実的な確率を考慮すると、2023年のデータから得られた主な教訓、つまりゼロデイ悪用が全ケースの大半を占めるということは、2024年も同様であると評価している。私たちの調査結果と諜報機関の調査結果との食い違いは、a) サンプルサイズ、b) サンプルの多様性によるものだと評価している。PwCが観察したインシデント対応事例のほとんどは、犯罪を動機とするものであり、関連するTTPは技術的水準が比較的低いものであった。このような脅威アクターは、ゼロデイの悪用を研究開発するためのリソースや能力を持ち合わせているとは考えにくいため、被害者の環境にアクセスするためには、古い概念実証や以前に提供された脆弱性のコードスニペットに頼らざるを得ない。インシデント対応の事例において、諜報活動を動機とする脅威アクターが関与していると評価されるケースでは、ゼロデイを活用するケースが見受けられた。これは、より一般的な脆弱性を使用していく傾向と整合するものである。

ケーススタディ

White Rabbitランサムウェア

2024年、PwCのインシデント対応チームは、White Rabbitとして知られる暗号化バイナリを活用した脅威アクターによる侵入を調査し、トリアージを行いました。まれに、暗号化バイナリの発動前ではなく、発動後に被害者の情報の流出が起こることがありました。

侵害に関連して最も早期のアクティビティが確認されたのは暗号化の3日前であり、脅威アクターがユーザーアカウント（アカウント1）を使用してFortiGateネットワーク・セキュリティ・アプライアンスにログインしたときでした。

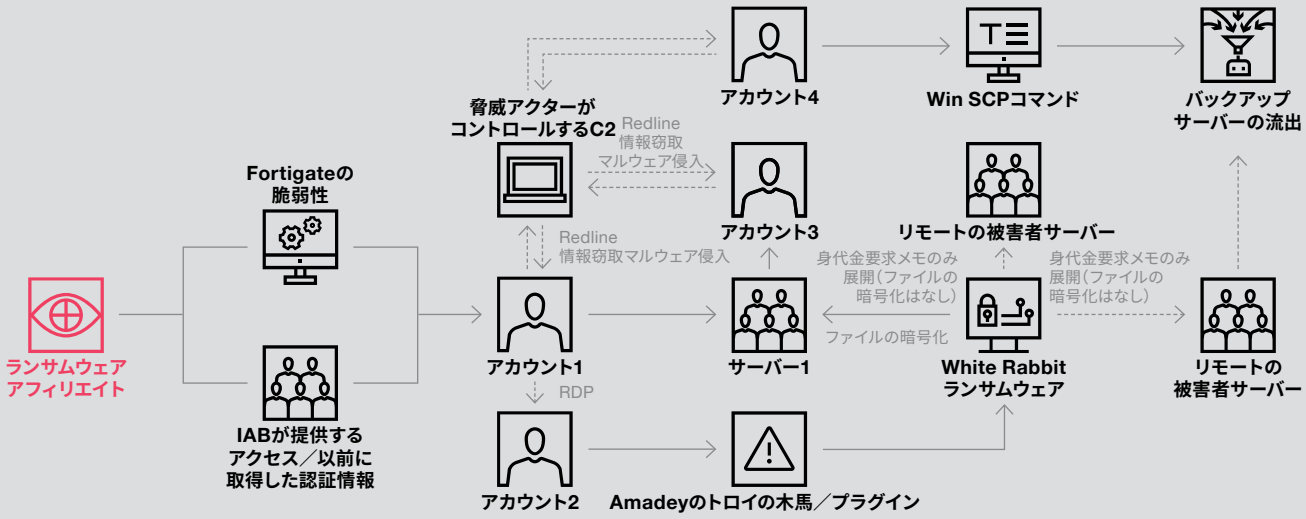
- 脅威アクターがどのようにしてアクセスできたかはすぐには特定できませんでしたが、現実的な確率を考慮すると、脆弱性が妥当性の高い侵入経路であったと考えられます。関連するFortiGateアプライアンスは、侵入の前後に直近で公開された2件の重大な脆弱性を持つバージョンを実行していたため、どちらかが悪用されてアクセスされた可能性があります。
- また、脅威アクターが初期アクセスブローカーを通じて認証情報を事前に入手した可能性もあります（利用可能なダークウェブフォーラムでの販売は確認されませんでした）。被害者はシステム内にアカウント1が存在することに気づいていなかったため、権限の可視性と認識が欠如していたことで、気づかないうちに脅威アクターによる環境への侵入を許していた可能性もあります。

この最初の侵害行為の1日後、アカウント1がRedLine認証情報窃取マルウェアの亜種をダウンロードしていたことが判明しました。

その後2日間、動きはありませんでしたが、新たに侵害されたドメインアカウント（アカウント2）を通じて、脅威アクターが被害者サーバー（サーバー1）にリモート接続しました。その後、脅威アクターはAmadeyボットネットの亜種を展開し、そのボットネットの名前はsvchost.exeに変更されました。Amadeyインスタンスの機能は、次の段階のペイロードをダウンロードして実行することでした[13]。分析時点ではこのファイルはシステムから削除されていましたが、ログ分析から得られたフォレンジックエビデンスにより、次の段階のペイロードはWhite Rabbit暗号化バイナリの亜種である可能性が高いとPwCは考えました。ローカルフォルダへの身代金要求メモのドロップや、特定のバイナリの暗号化のタイムラインは、ペイロードの実行と一致しています。

おそらく、被害者のファイルシステムに対する暗号化が完全に計画どおりには機能しなかったため、脅威アクターは1日後に当該環境に戻ってきました。1台のESXiと1台のWindowsサーバーだけが暗号化され、他の全てのリモートサーバーと仮想サーバーは手つかずのままだったことが原因と思われます。調査中にアカウント3としたアカウントは、前述のRedLine情報窃取マルウェアバイナリをダウンロードしていたことが判明し、アカウント4とした4番目のアカウントは、脅威アクターが制御するリモートサーバーへのファイル転送に正規のWinSCPツールを使用して、3つのバックアップディスクをダウンロードしていました。この挙動は、脅威アクターが暗号化後の被害者の環境に足場を確保しようとしていたことを示しています。

図表4-PwCのインシデント対応チームが観察したWhite Rabbitランサムウェアによる侵入の視覚化



13 アナリスト注記：被害者の環境にAmadeyのプラグインが残っていたことから、脅威アクターは被害者のフィンガープリントをさらに利用し、その持続性を高めるためにAmadeyのプラグインを使用した可能性があった。詳細はこちらを参照：'I Amadey-ngerous stealer', PwC Threat Intelligence,CTO-TIB-20241209-01A

2024年が終わり、不確実な新年がスタート

あらゆる振り返りと同様に、1年を通して学んだことや気づいたことは、数カ月先を見通す際にも活用できます。2024年は、地政学的緊張がほぼ全ての主要地域で高まるとともに、予想された、または予定外の選挙や政治的混乱が相次ぎ、例年以上に多くの国で指導者の交代が行われました。このような緊張と変化が2024年のサイバー領域での活動に影響を与えましたが、それは2025年を通して続くと思われます。

犯罪

- サイバー犯罪エコシステムについては、法執行機関によるテイクダウンや妨害が成功したにもかかわらず、前例のない数のランサムウェアリークサイトが構築され、ほぼ全ての業界にとって重大な破壊要因の1つであり続けています。
- また、2024年は、多額の身代金支払いとそれに伴うサプライチェーンの問題を抱えた著名な被害者が出た年でもありました。これは、あらゆる規模の組織が引き続きランサムウェアの脅威にさらされていることを物語っています。
- 法執行機関によるテイクダウンに直面してなお示された回復力により、ランサムウェアのエコシステムは2025年においても、あらゆる規模の、あらゆる業界にとって最大の脅威であり続ける可能性が高いと私たちは評価しています。

私たちは、サイバー領域では2025年も政治的緊張が支配的であり、サイバー脅威の状況も同様の影響を受ける可能性が高いと評価しています。

中国と台湾

- 中国を拠点とする脅威アクターは、今後も台湾を拠点とする組織・企業を諜報活動の標的とし[14,15,16,17]、特に防衛機関や政府機関を標的とする可能性が高いと思われます。また、脅威アクターが足がかりを作る目的で重要な国家インフラネットワークに侵入し、必要に応じて妨害行為に利用される可能性もあります[18]。
- 2024年末に中国軍（人民解放軍）が実施した軍事演習は、2025年においても中国政府が東シナ海の領土に引き続き関心を寄せることを示唆するものであり[19]、サイバー活動を伴うことはほぼ間違いないと考えられます。

中国と米国の関係

- 中国拠点の脅威アクターによる米国とその同盟国に対する活動は、2024年以前からすでにかなりの規模に達しており、その大部分は政府機関や防衛関連機関を標的とした世界規模の諜報活動で構成されていましたが、2024年にはその規模が拡大しました。コンピューター・ネットワーク・エクスプロイト（CNE）を目的とした商用プロキシネットワークの多用など、これまでの傾向は2024年においても顕著であり、敵対国の重要な国家インフラを危険にさらすことへの関心が高まっています。
- また2024年には、中国とのつながりがある活動に対処する米政府当局と、米政府機関による攻撃活動を警戒する中国当局による共同勧告の数も増加しました[20]。中国政府による声明には不満も追加されており、西側諸国による中国の諜報活動の報告を「操作行為だ」と非難しています[21,22]。現実的な確率を考慮すると、中国と米国の緊張が続けば、サイバーに関する報告とそれに対する反論の応酬は2025年も続くと評価されますが、これが両国の攻撃的なサイバー活動に大きな影響を与えるとは予想していません。

---

14 'PingPong pings on FortiGates in Taiwan' ,PwC Threat Intelligence,CTO-TIB-20241204-01A

15 'Into the Spyder-verse' ,PwC Threat Intelligence,CTO-TIB-20240620-01A

16 'Look what the ToddyCat dragged in' ,PwC Threat Intelligence,CTO-TIB-20240524-01A

17 'New targets, same Moros' ,PwC Threat Intelligence,CTO-TIB-20240219-01A

18 アナリスト注記：中国を拠点とする脅威アクターは、歴史的にも2024年においても、将来の妨害工作の足がかりを作るという目的のために、重要な国家インフラのネットワークに侵入していることが判明している。2024年の活動については、以下を参照。'PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure' ,CISA, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a (7th February 2024)

19 'Big Chinese naval exercise leaves Taiwan and US struggling for response' ,Financial Times, https://www.ft.com/content/025a81f1-2cb2-459d-8427-46fd44b1b2c3 (14th December 2024)

20 'CNCERT发现处置两起美对我大型科技企业机构网络攻击事件' ,CNERT/CC, https://www.cert.org.cn/publish/main/49/2024/20241218184234131217571/20241218184234131217571_.html (18th December 2024)

- 中国政府と米国政府やその他の西側諸国政府との緊張が高まるにつれて、中国を拠点とする脅威アクターと米国を拠点とする脅威アクターの活動ペースについては、重要な国家インフラの傘下にある業界を標的としたものが増加する、あるいは増加し始める可能性が高いと私たちは評価しています。

アジア広域

- 中国とインドの間の地域的力学は、2024年においても引き続き複雑であり、両国が緊張状態に陥ったことで、中国拠点の脅威アクターとインド拠点の脅威アクターは、相手に対してだけでなく、他のアジア諸国をも巻き込んだ諜報活動関連の目的に重点を置くようになりました[23,24,25,26]。このような傾向が続けば、インドと中国の政治的力学は、2025年以降もそれぞれの国の脅威アクターのサイバー活動に大きな影響を与える可能性があると私たちは評価しています。
- 2024年には、北朝鮮を拠点とする脅威アクターが前年よりも活発化し、大規模なサプライチェーン攻撃から、より従来型の侵入活動へと移行しました。IT労働者のスキャンダルは2024年からの新たな現象ではありませんがより活発なキャンペーンの1つとなり、経済的利益（正当な賃金や恐喝行為）と被害者から機密データを収集するための諜報活動を組み合わせたものとなりました。

ロシア、ウクライナ、NATO

- 2024年に観察されたロシアを拠点とする活動の多くは、ウクライナやNATO圏など、ロシアの外交政策の優先順位に沿って行われました[27,28]。
- ロシアを拠点とする脅威アクターは、ウクライナを拠点とする機関、特に政府機関、防衛機関、重要な国家インフラを標的とし、ウクライナに軍事支援をする同盟国も標的とする可能性が高いと私たちは評価しています。

中東

- イランを拠点とする脅威アクターは、2024年も中東情勢と歩調を合わせ、その活動ペースを上げました。また、トルコやアゼルバイジャン[29]、オマーンやアラブ首長国連邦[30]など、中東の広い地域の組織・企業も標的にされました。
- 対照的に、イランを拠点とするグループ（Grey KarkadannやGrey Hadesなど）と連携する地域のアクターによるサイバー脅威活動は、この1年で大幅に減少しました。この減少は、これらのグループが拠点を置いているとされる国々の物理的インフラをイスラエルが集中的に標的にしたことと整合しています[31]。

21 'China hits out at US and UK over cyber hack claims' ,BBC, https://www.bbc.com/news/world-asia-china-68655786 (24th March 2024)
22 'The Scapegoat Strikes Back' ,Beijing Review, https://www.bjreview.com/Opinion/Pacific_Dialogue/202410/t20241028_800381804.html (28th October 2024)
23 'Red Ishtars snea-key return' ,PwC Threat Intelligence,CTO-TIB-20240215-01A
24 'Red Lich' s Nim-ble Loaders' ,PwC Threat Intelligence,CTO-TIB-20241223-01A
25 'SuperJumping to Connect Secure' ,PwC Threat Intelligence,CTO-QRT-20240124-01A
26 'The elephant in many rooms-a technical analysis' ,PwC Threat Intelligence,CTO-TIB-20241118-01A
27 'Blue Dev 8' s net on Ukraine' ,PwC Threat Intelligence,CTO-TIB-20240520-01A
28 'Blue Athena Dumps Webhooks into the Water' ,PwC Threat Intelligence,CTO-TIB-20240214-01A
29 'There' s plenty more SeaSickle on the C2' ,PwC Threat Intelligence,CTO-TIB-20241218-01A
30 'Muddy, muddle tools and trouble; FranChis loader, SeaSickle, Bubble' ,PwC Threat Intelligence,CTO-TIB-20241030-01A
31 'Battlefield setbacks reduce cyber capacities for Hamas and Hezbollah but not Iran' ,PwC Threat Intelligence,CTO-SRT-20241213-01A

セクション 2

全ての船を揺り動かす上げ潮

2024年における脅威アクターの活動の大部分を支えてきたのは、オープンソースのコードとツールの普及、そしてこれらのツールが巧妙化し、使いやすくなっていることが挙げられます。この状況は、特に犯罪行為において、技術的水準の低い脅威アクターに大きな利益をもたらしています。攻撃者は、オープンソースのコードベースから独自のマルウェアやアフィリエイトを容易に作成することができ、開発やメンテナンスに必要な技術的能力は比較的低くなっています。

脅威アクターの活動は、以下の事象によって大きな影響を受けました。

- AIが生成したツール。ほとんどの場合、ソーシャルエンジニアリングの領域で使用されてきましたが、ツール開発中に脅威アクターが使用したエビデンスも存在します。
- 技術面の脆弱性を研究する有能な個人が増加していると考えられ、ゼロデイ脆弱性とNデイ脆弱性の概念実証（POC）およびソリューションの数が全体的に増加しています。バグ報奨金プログラムの普及や、エクスプロイトに関する研究のトレーニング、スキルアップ手段へのアクセスが容易になったことが、その主な要因と思われます。
- 脆弱性については、概念実証（POC）エクスプロイトコードや、コードベースを悪用するための新たな手段を模索する個人（セキュリティ研究者と脅威アクターの両方を含む）の活発なコミュニティ形成により、より幅広い範囲の脅威アクターがアクセスしやすくなっています。
- ランサムウェアや情報窃取マルウェア市場など、不正行為を可能とするエコシステムの全体的な成長。悪意ある活動に関わる犯罪者や個人が増え、より多くのツール群やアイデアが生み出され、それがさらなる細分化をもたらし、より大量の活動が開始されたことで、今後数年間は抑制が困難と思われる状況が作り出されています。

AIの介入

AIは、サイバーセキュリティの領域では以前から研究や投資が行われてきており、2024年に新たに生まれた技術ではありません。しかしながら、脅威アクターの活動という観点から見ると、2024年はAIが今後の主流となる可能性が示された年でした。容易に利用可能なAI駆動型技術の進歩は、特に攻撃チェーンの初期段階（偵察や初期アクセスなど）において、脅威アクターが利用可能な数多くの手段を生み出しています[32]。脅威アクターが初期アクセス技術を実験し続けることが予想される一方で、アプローチや技術が他の手段よりも成功することが証明されるにつれて、標準化されたTTPが増える可能性も高くなります。そのため、2025年にはAIツールの実験が継続的に行われ、技術的水準がさほど高くない脅威アクターの大半に人気のある先駆的なツールが登場すると考えられます。

表1-AIが生成したコンテンツと脅威アクターによる利用に関する開発と検知

AIが作成したコンテンツの種類	テキスト：コミュニケーション	テキスト：コンピューターコード	画像	音声	動画（音声あり・なし）
脅威アクターによる生成コンテンツの利用例	侵入を試みるフィッシングメールと金銭的な動機による攻撃	マルウェア開発	偽情報工作	金銭的動機に基づく攻撃における会社重役のディープフェイク音声	金銭的動機に基づく攻撃でのビデオ通話における会社重役のディープフェイク映像
コンテンツ生成の難易度	トレーニングデータを備えた多数のツールを利用可能、トレーニングデータの追加が可能	多数のツールを利用可能、トレーニングデータの追加が可能	トレーニングデータを備えた多数のツールを利用可能	自然な音声でテキストを読み上げるツールを利用可能、音声サンプルをトレーニングデータとして追加可能	トレーニングデータを備えた利用可能なツールは限定的
技術的手段によらないコンテンツ検出の難易度	高いメディアリテラシーが必要。一般的に生成されたコンテンツが不正確または不規則であることが必要	コード内の不規則性やエラーを検出する能力が必要	生成AI技術の進歩により、検出可能な指標は減少傾向	生成AI技術の進歩により、人間の声とほぼ区別できないサンプルを生成可能	生成時の矛盾点は、一般的な認知度が比較的低いことにより相殺
技術的手段による検出の難易度	さまざまな精度のツールが多数存在	さまざまな精度のツールが多数存在	さまざまな精度のツールが限定的に存在	さまざまな精度のツールが限定的に存在	さまざまな精度のツールが限定的に存在

低難度　中難度　中難度／高難度　高難度　超高難度

特にソーシャルエンジニアリング、さらに初期アクセスに関連するAIは、犯罪アクターにとってはすでに組織への一般的な侵入手段となっていましたが[33,34]、2024年にはかなり活発な利用が観察されています。White Dev 164（別名 Scattered Spider）によるものに限らず、ランサムウェアのアフィリエイトやビジネスメール詐欺（BEC）のアクターは、被害者を脅す手段としてAIが生成したメールのテキスト、音声、さらには動画メディアを使用しています[35,36,37,38]。AIが生成したマルウェアも2024年にはトレンドとして確立され、大規模言語モデル（LLM）を使用して作成されたさまざまなローダーやPowerShellスクリプトが発見されています[39,40,41]。

32 'The Evolution Of Social Engineering And Phishing In The Age Of Artificial Intelligence',Lumen, https://blog.lumen.com/the-evolution-of-social-engineeringand-phishing-in-the-age-of-artificial-intelligence/ (5th August 2024)

33 'Scattered Spider',US CISA, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a (16th November 2023)

34 'Business Email Compromise-A Primer',PwC Threat Intelligence,CTO-TIB-20240729-01A

35 'White Dev 184's ScreenConnect Obsession',PwC Threat Intelligence,CTO-TIB-20240827-01A

36 'UK engineering firm Arup falls victim to £20m deepfake scam',The Guardian, https://www.theguardian.com/technology/article/2024/may/17/uk-engineeringarup-deepfake-scam-hong-kong-ai-video (17th May 2024)

37 '#StopRansomware: Black Basta',US CISA, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a (8th November 2024)

38 ''Quishing', 'vishing' and AI scams-the new cybercriminal techniques duping Australians',The Guardian, https://www.theguardian.com/technology/2024/nov/20/quishing-vishing-and-ai-scams-the-new-cybercriminal-techniques-duping-australians (19th November 2024)

39 'Security Brief: TA547 Targets German Organizations with Rhadamanthys Stealer',ProofPoint,10th April 2024

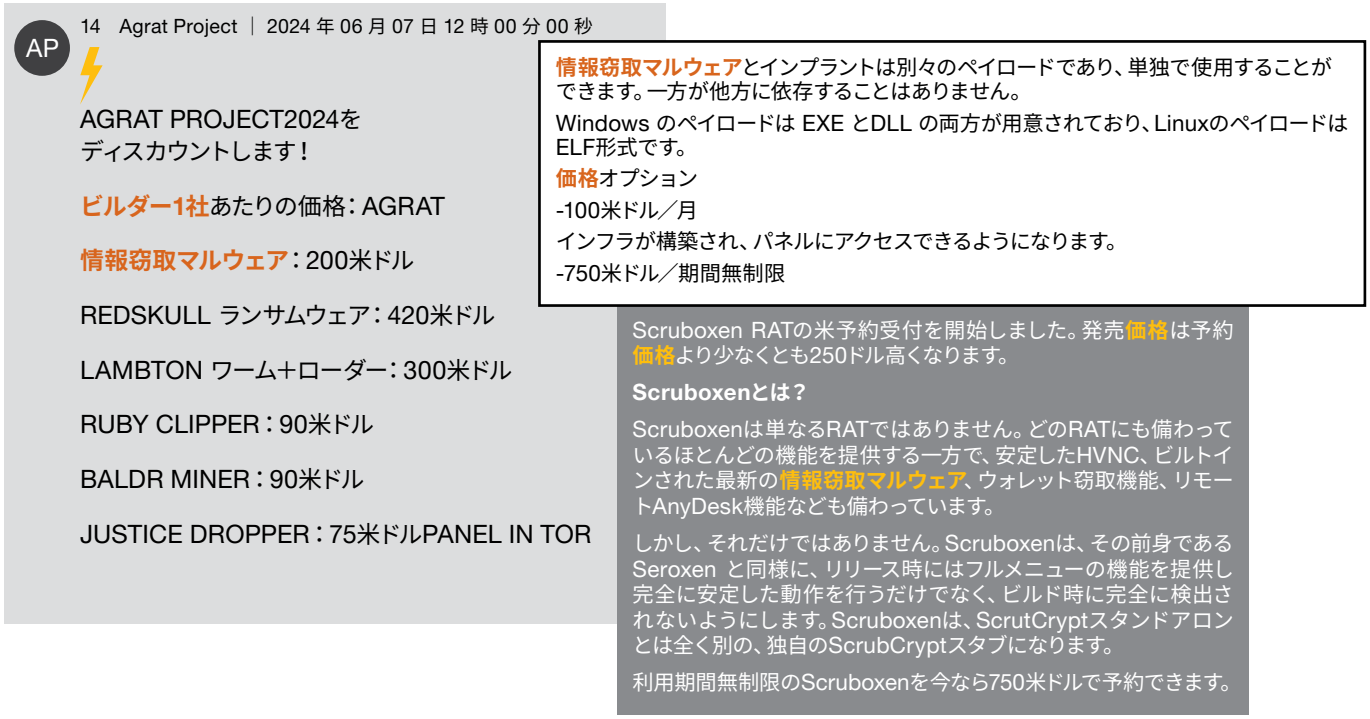
40 'Threat Insights Report: September 2024',HP Wolf Security, https://threatresearch.ext.hp.com/wp-content/uploads/2024/09/HP_Wolf_Security_Threat_Insights_Report_September_2024.pdf (24th September 2024)

41 'An update on disrupting deceptive uses of AI',OpenAI, https://openai.com/global-affairs/an-update-on-disrupting-deceptive-uses-of-ai/ (9th October 2024)

AIに関連するこれらの傾向は、2024年に影響を与えた他の変化と並行して存在しています。規制の緩いLLMの創設[42]、ツールレベルでのサイバー犯罪エコシステムの全体的な成長、2024年を通してのPOCの存在感の拡大は、技術的水準がさほど高くなく、「参入障壁の低い」脅威アクターと、より確立された侵入セットの双方が、活動の初期アクセス段階でより高い成功レベルを見出す未来を示唆しています。

- **脅威への参入障壁の低さ:** このような脅威アクターは、AIが生成したフィッシングやソーシャルエンジニアリングと、オープンソースまたは安価な情報窃取プログラムを組み合わせて認証情報を取得し、多数の攻撃を実現すると考えられます[43]。これらはダークウェブで一括して販売されることもあれば、初期アクセス仲介手段として個別に販売されることもあります。この種の侵入がより一般的になる可能性が高く、AIを活用した要素が加わることで、活動がより効果的になる可能性があります。

図表5-2024年にさまざまなダークウェブフォーラムで宣伝された情報窃取マルウェアの例



- **より巧妙な脅威:** このような脅威アクターはTTPをあまり変更しない可能性が高く、その代わりに攻撃プロセスの継続的な反復を頼みとしています。ソーシャルエンジニアリングや脅迫行為、標的に関する効果的な情報収集の手段は、容易にアクセス可能なLLMや生成AIツールの恩恵を受けることができるため、この傾向は活動の偵察と初期アクセスの段階で続くと考えられます。
  - 2024年には、ランサムウェアのアフィリエイトやより一般的な犯罪の脅威（情報窃取マルウェアやBEC指向の脅威など）において、サイバー犯罪エコシステム内で多くの日和見型攻撃が見られました。これには、認証情報の購入とそれに続くクレデンシャルスタッフィングの試み、脆弱性のスキャンとそれに続く悪用の試み、さらには大規模なフィッシング攻撃などの手法が含まれていました。

42 Dark LLMs aka BlackHat GPTs and Malicious AIs' ,GitHub, https://github.com/cybershujin/Threat-Actors-use-of-Artifical-Intelligence/blob/main/Dark%20LLMs%20and%20Malicious%20AIs.MD (15th May 2024)

43 'Breaking down the -as-a-Service industry' ,PwC Threat Intelligence,CTO-SIB-20240814-01A

– AI駆動型ツールは、これらの手法の全てに何らかの形で役立ちますが、重要なのは、用途に関連するAI駆動型ツールの出現によって標的が絞られる可能性が高まり、「ビッグ・ゲーム・ハンティング」が復活することが考えられます[44]。2024年は、ビッグ・ゲーム・ハンティングがいかに儲かるかを示す年となりました[45,46]。私たちは現実的な確率に基づき、現在のAIの状況はこの種の攻撃にとってこれまで以上に大きな機会を提供していると評価しています。

ゼロデイのスキル格差の縮小

- 「2023年を振り返る」というレポートでは、初期アクセス手段として脆弱性を利用するケースが増加し、それがサイバー犯罪の分野で最大の懸念事項であることを述べました[47]。
- 2024年にはこの傾向が継続するだけでなく、諜報活動や犯罪を動機とするグループによる、ゼロデイまたはNデイの利用を伴うインシデントの数に顕著な増加が見られます[48,49,50]。このデータによると、2023年から2024年にかけて、武器化された脆弱性の数は20%増加し[51]、開示された脆弱性の数は31%増加しています[52]。
- ゼロデイを研究・開発する能力を備えていると評価された脅威アクターは、実際にゼロデイ攻撃を実施しています。一方、犯罪グループ、特にランサムウェアのアフィリエイトは、最初の情報公開後に利用可能な概念実証コードを利用していました[53,54,55]。
- しかしながら私たちは、技術的水準がさほど高くない脅威アクターが、初期アクセス段階で過去の脆弱性を活用していることを観察しました[56,57]。技術的水準がより高く、諜報活動を動機とする脅威アクターについては、最初の侵入後に脆弱性を利用することが少ない傾向が見られました[58]。過去の脆弱性を継続的に利用することにより、特にパッチが適用されないまま放置されがちな保守期間が終了したエッジデバイスを中心に、被害者の環境で侵入の足がかりが迅速に構築される可能性が高いと私たちは評価しています。

---

44 アナリスト注記：ビッグ・ゲーム・ハンティングとは、特にこの例ではランサムウェアに関連した、個々の（特定の）事業体を標的とした侵入を指す用語であり、多くの場合、活動の偵察段階とリソース開発段階でかなりの労力を費やす。ビッグ・ゲーム・ハンティングの目的は、1回の侵入にできるだけ多くのリソースを配置し、侵入成功とその後の利益獲得のチャンスを最大化することである。

45 'Dark Angels ransomware receives record-breaking $75 million ransom',Bleeping Computer, https://www.bleepingcomputer.com/news/security/dark-angelsransomware-receives-record-breaking-75-million-ransom/ (30th July 2024)

46 アナリスト注記：これは、日和見型攻撃が利益を上げていないということを意味するものでない。Change Healthcareに対しランサムウェアの侵入を成功させ、2,200万米ドルの身代金を奪った脅威アクターは、初期アクセス手段として認証情報スタッフィングを使用した（参照: 'Testimony of Andrew Witty Chief Executive Officer, UnitedHealth Group Before the House Energy and Commerce Committee Subcommittee on Oversight and Investigations "Examining the Change Healthcare Cyberattack"',TechCrunch, https://www.documentcloud.org/documents/24626988-uhgs-witty-house-testimony (1st May 2024))

47 "Cyber Threats 2023: A Year in Retrospect",PwC Threat Intelligence,CTO-YIR-20240624-01A

48 'Breaking down the -as-a-Service industry',PwC Threat Intelligence,CTO-SIB-20240814-01A

49 '541 Jump street',PwC Threat Intelligence,CTO-TIB-20241121-01A

50 'Ransomware operators exploit ESXi hypervisor vulnerability for mass encryption',Microsoft, https://www.microsoft.com/en-us/security blog/2024/07/29/ransomware-operators-exploit-esxi-hypervisor-vulnerability-for-mass-encryption/ (24th July 2024)

51 2024 Trends in Vulnerability Exploitation',VulnCheck, https://vulncheck.com/blog/2024-exploitation-trends (3rd February 2025)

52 NVD, https://nvd.nist.gov/

53 'SonicWall SSLVPN access control flaw is now exploited in attacks',Bleeping Computer, https://www.bleepingcomputer.com/news/security/sonicwall-sslvpnaccess-control-flaw-is-now-exploited-in-attacks/ (6th September 2024)

54 'Critical Veeam Vulnerability Exploited to Spread Akira and Fog Ransomware',The Hacker News, https://thehackernews.com/2024/10/critical-veeamvulnerability-exploited.html

55 'CISA confirms critical Cleo bug exploitation in ransomware attacks',Bleeping Computer, https://www.bleepingcomputer.com/news/security/cisa-confirmscritical-cleo-bug-exploitation-in-ransomware-attacks/ (13th December 2024)

56 'A look into an affiliates operations',PwC Threat Intelligence,CTO-TIB-20240426-02A

57 Threats Under the Spotlight 2024 Issue 4,PwC Threat Intelligence,CTO-TUS-20240607-01A

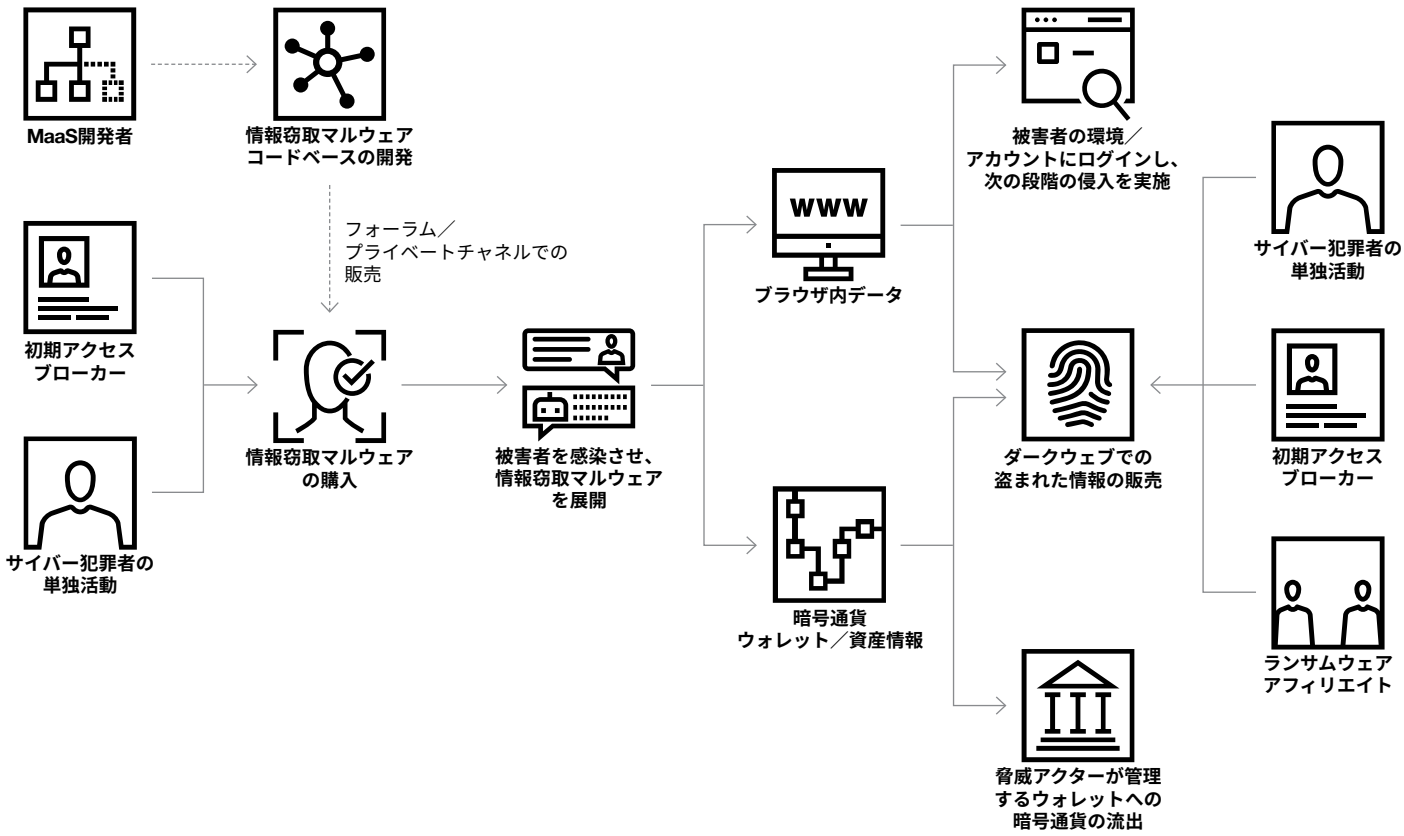
58 アナリスト注記：ロシアを拠点とする脅威アクターBlue Dev 5（別名APT29、Midnight Blizzard）に見られるように、該当しない場合もある。以下を参照：'Update on SVR Cyber Operations and Vulnerability Exploitation',Joint Cybersecurity Advisory, https://www.ic3.gov/CSA/2024/241010.pdf (10th October 2024)

サイバー犯罪エコシステムの成長：

2024年のサイバー犯罪市場は、オープンソースコードベースの増加や、TTPを継続的に改良できる能力を備え、統合化が進んだプレイヤーの成熟度向上により拡大しました。このような状況がもたらした結果は、例えば、犯罪の現場で利用可能なツールの数が増加していることからも容易に観察できます。このようなツールは、合法的な市場と同じように、健全な市場競争によって進歩し、使いやすさ、価格、機能性が脅威アクターに対する主なセールスポイントとなっています。

情報窃取マルウェアの市場とランサムウェアのエコシステムは、いずれも2024年に大きな発展を遂げましたが、その一因となったのは、新たな脅威アクターが古いコードベースを活用できるようになったことでした[59,60,61]。これとは対照的に、StealC、DarkGate、Latrodectusなど[62,63]、より確立されたプログラムは、反復的な開発サイクルに依存しており、これらの開発者は常に新しい機能を取り込むよう情報窃取マルウェアのコードベースを更新しています。

図表6-広範囲のサイバー犯罪エコシステムにおいて情報窃取マルウェアが果たす役割



59 The Curious Case of an Open Source Stealer:Phemedrone',SpyCloud, https://spycloud.com/blog/phemedrone-stealer/ (6th September 2024)

60 'Kematian-Stealer : A Deep Dive into a New Information Stealer',Cyfirma, https://www.cyfirma.com/research/kematian-stealer-a-deep-dive-into-a-newinformation-stealer/ (6th July 2024)

61 'RansomHub Ransom Run', PwC Threat Intelligence,CTO-TIB-20241108-01A

62 Closing the DarkGate after the horse has DanaBot(ted)',PwC Threat Intelligence,CTO-TIB-20241203-01A

63 'Digging through a Badgers (data)Sett',PwC Threat Intelligence,CTO-TIB-20241015-02A

注目のテーマ：StealC

StealCは、2023年1月にRussian Marketplaceのダークウェブフォーラムで初めて宣伝され、2024年を通じて最も人気のある情報窃取マルウェアの1つです。StealCの開発者（PwCでは White Dev 183として追跡されています）は、Vidar、Raccoon、Mars、Redlineといった他の情報窃取マルウェアのコードベースから着想を得たことを認めています。

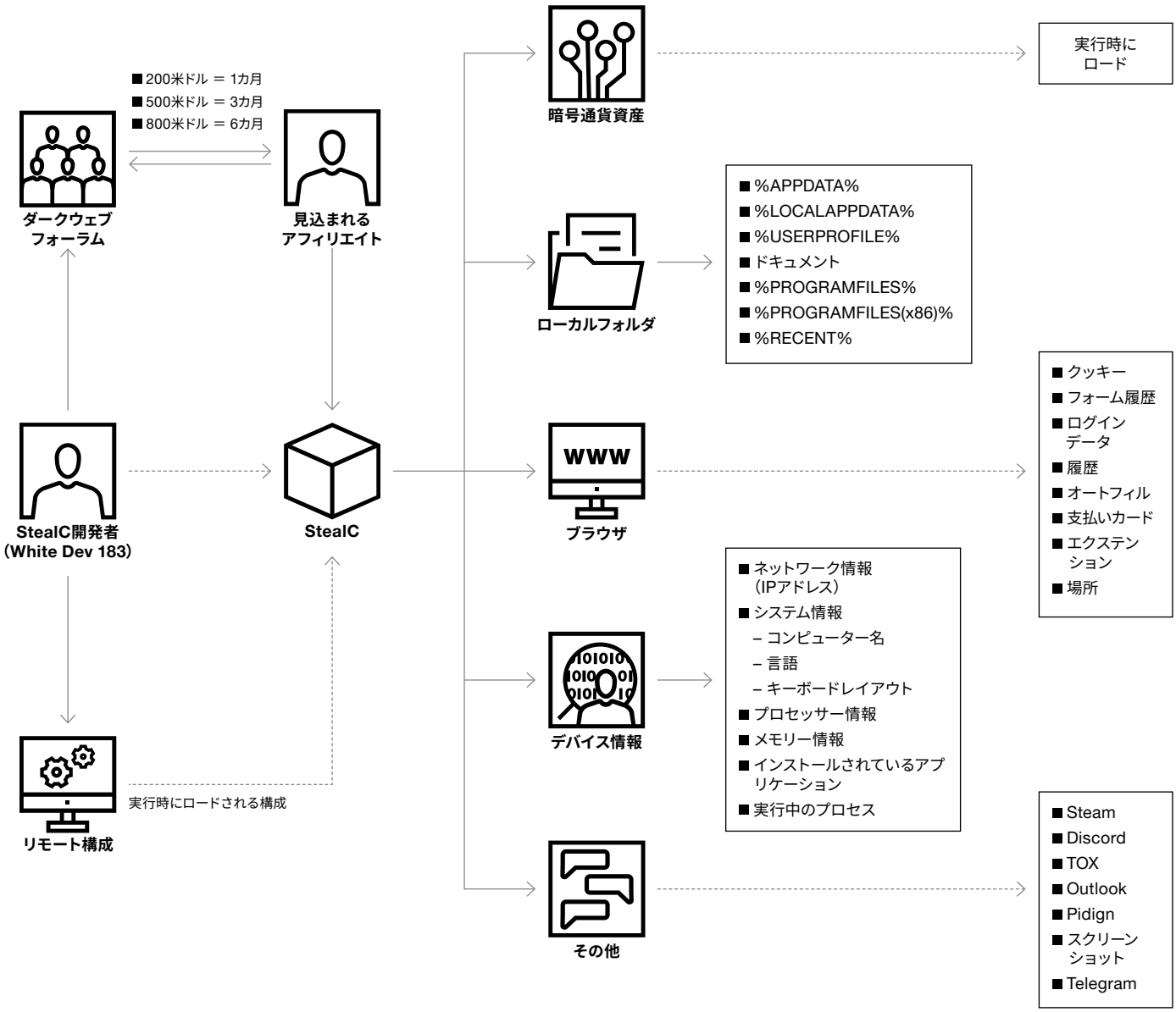
図表7-StealC開発者によるXSSフォーラムへの投稿からの抜粋

> stealは、柔軟なデータ収集設定と便利な管理画面を備えたノンレジデント型情報窃取マルウェアです。私たちは現在市場に出回っているVidar、Raccoon、Mars、RedLineを活用し、このソリューションを開発しました。

最も人気のある情報窃取マルウェアと同様、StealCはサブスクリプションモデルで販売されています。料金は、1カ月間のアクセスで200米ドル、3カ月間のアクセスで500米ドル、6カ月間のアクセスで800米ドルとなっています。これには、アフィリエイトが取得したログを検索・解析する機能を提供するグラフィカル・ユーザー・インターフェイス・パネルが含まれます。このパネルでは、どのプラットフォームで情報を窃取するか、ログをどこに送信するかなど、アフィリエイト自身がマルウェアのビルドをカスタマイズすることができます。また、オプションで追加機能（マルウェアがスクリーンショットを撮影する機能、ディスクから自身を削除する機能など）を構成することもできます。

StealCは、（コードベースにハードコードするのではなく）実行時にモジュールと情報窃取機能をダウンロードするというユニークな機能を持つことをセールスポイントにしています。すなわち、情報窃取マルウェアは理論上、常に最新の機能で実行されます。StealCの窃取動作は、（ブラウザなどの）あらゆるカテゴリーの要素からデータを窃取する前に、POSTリクエストを使用して指定されたコマンド・アンド・コントロール（C2）サーバーと接続し、窃取対象に関する情報をサーバーから取得するよう構成されています。その後、窃取動作を完了し、C2と再び通信して結果を送信します。

図表8-StealICの機能概要



StealICプログラムのより興味深い要素の1つは、それに付随する公式ダークウェブフォーラムのチャットです。これには、運営効率を最大化するためにStealICと複数の情報窃取マルウェアを連携して使用することに関する会話が含まれています。ランサムウェアのエコシステムと同じような作用をする市場（競合者が全て同じアフィリエイトのプールを争っている市場）において、このような協力は驚くべきことです。全ての情報窃取マルウェアの開発者がこのような方法で活動するわけではありませんが、StealICは2024年に最も人気のある情報窃取マルウェアの1つとなりました。その理由は、使いやすさ、価格、開発者とアフィリエイトのコミュニケーションにあると思われます。

情報窃取マルウェアは数多く存在しますが、StealICはその1つであり、より多くのコードベースのリークまたはオープンソースでの公開、熟練した開発者間でのテクニックの共有が行われるので、常に新しいプレイヤーが登場し、市場は拡大しています。これらの情報窃取マルウェアの多くに同一ではないにせよ類似した機能が存在することから（利用可能なコードベースから分岐したバージョンであることが多いため）、プログラムの成功を決定するのは、使いやすさとともに、製品を効果的に販売する脅威アクターの能力による場合が多くなっています。

セクション 3

静かな水は深く流れる

2024年に出現した、より新しくより明白な傾向として、またそれ以前から引き継がれた傾向として、脅威アクターのツール、テクニック、手順（TTP）が微妙に変化しているということがあります。これは2024年を支配するほど重大な傾向ではないものの、脅威の状況を重要な形で変化させました。

最も大きな注目を集めたのは、中国を拠点とする脅威アクターによる商用プロキシネットワークを活用した行為です。この傾向は、2021年に複数のグループがRedRelayネットワークを採用したことで初めて確認されました。2024年にはこのようなネットワークの利用が急速に拡大し、中国を拠点とする多くの脅威アクターが、難読化ネットワークの仕組みを利用して活動するようになりました[64,65,66,67,68]。

注目のテーマ：中国を拠点とするプロキシネットワーク

中国を拠点とする脅威アクターによるサイバー侵入の方法とそのための共有ツールはこれまでも存在しましたが、プロキシネットワークという事象はこれに新たに加わるものです。プロキシネットワークの前には、8.tの武器化攻撃フレームワーク[69]があり、それ以前にもPlugX[70]、PoisonIvy[71]、ShadowPad[72]などの共有マルウェアファミリーが存在していました。侵入のためのTTPの統合と共有は、個々の侵入を行うために必要なリソースの削減だけでなく、攻撃元を不明瞭にしてアトリビューションの試みを妨げることを目的とした、より広範な試みの一部であると評価されてきました。

64 'Red Vulture & Red Dev 38: Covert Network Links',PwC Threat Intelligence,CTO-TIB-20240129-01A
65 'Scratching a Lich',PwC Threat Intelligence,CTO-TIB-20240829-01A
66 'A New MONSOON Season',PwC Threat Intelligence,CTO-TIB-20240628-03A
67 'When it rains, it DOWNPOURs',PwC Threat Intelligence,CTO-TIB-20240517-01A
68 'Just our LuckyORB',PwC Threat Intelligence,CTO-TIB-20240802-01A
69 'On the RoyalRoad again',PwC Threat Intelligence,CTO-TIB-20211222-01A
70 'An xWav on Kyrgyzstan',PwC Threat Intelligence,CTO-TIB-20210222-01A
71 'Beware the GreenHugeMan',PwC Threat Intelligence,CTO-TIB-20221103-02A
72 'Whats dat malware',PwC Threat Intelligence,CTO-TIB-20230821-01A

プロキシネットワークは、この傾向の延長線上にあるものですが、さらに発展したものでもあり、いろいろな意味で進化したものと言えます。これらのネットワークに関する設計、トポロジー、能力、使用方法は、過去の活動で存在した従来型ツールの範囲を超えて大幅に進化しており、それぞれが独自の機能や使用目的を持つ、階層化された大規模なインフラストラクチャのセット（エントリーノード、中間「ホップ」ノード、エグレスノードなど）で構成されています[73]。

2021年にRedRelayと呼ばれるプロキシネットワークの使用が確認されて以来（実際は2018年の時点で使用されていました）、プロキシネットワークのエコシステムは飛躍的な成長を見せています。

図表9-プロキシネットワークのさまざまな形態

プロキシネットワークは結局のところ、アトリビューションに対する難読化を行うために使用されます。2024年におけるこのインフラの使用方法は、現在観察されているTTPの稼働傾向という点で、中国を拠点とする脅威アクターの状況に対する私たちの見方を変えました。

- 初期アクセスについては、ターゲットに対する悪意ある文書の使用やフィッシングの試みが激減していることが観察されています。その一方で、現在では、既知のNデイ脆弱性とゼロデイ脆弱性を利用した脆弱性の悪用が増加しています[74]。
- この変化には、高度に標的化された攻撃と、（脆弱性が公表された直後、あるいは場合によっては公表される前の）大規模な悪用の両方が含まれます。これらのデバイスは複数の業界で幅広く使用されているため、選択およびリサーチされる可能性が高く、たった一度の悪用でかなりの数の侵害の機会を作り出しています。2024年のセキュリティに関する公的なリサーチ[75]に見られるように、製品自体にも大きな攻撃対象領域が存在するように見受けられます。つまり、脆弱性のパッチが適用されても、同じプロダクトが別の、しかし類似した悪用の対象となる可能性が高くなっているのです。

73 'Into the Spyder-verse',PwC Threat Intelligence,CTO-TIB-20240620-01A

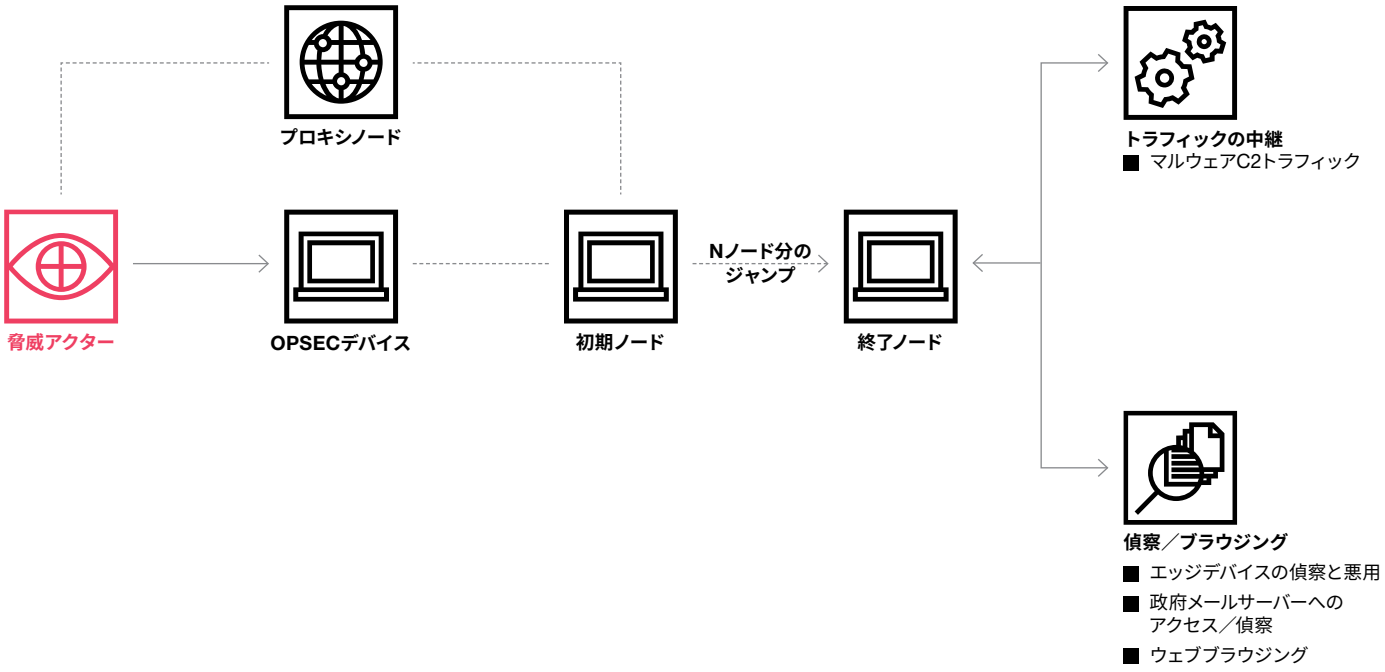
74 'Defending against the zero-day deluge',PwC Threat Intelligence,CTO-SIB-20231212-01A

75 'Hop-Skip-FortiJump-FortiJump-Higher - Fortinet FortiManager CVE-2024-47575',watchtower Labs, https://labs.watchtowr.com/hop-skip-fortijump-fortijumphigher-cve-2024-23113-cve-2024-47575/ (15th November 2024)

- このような初期アクセスを狙った攻撃で標的とされることの多いデバイスは以下のとおりです。
  - マイクロソフト製品（Windows、Exchange、SharePointなど）
  - セキュリティデバイスとエッジデバイス
  - 仮想プライベートネットワーク（VPN）
  - ファイアウォール
  - 仮想化インフラ
- 中国を拠点とする脅威アクターは、初期アクセスの後、カスタムバックドアを使用する代わりに、管理者レベルのアカウントの侵害やPowerShellといったネイティブユーティリティの悪用など、環境寄生型手法の使用を続けています[76]。このような初期アクセス後の活動は、2024年に始まったことではなく、中国を拠点とするアクターが長年にわたって侵入チェーンの中で一貫して行ってきたことではありますが、脅威アクターが被害者の環境内で足場を固める際の効率の良さが、2024年の話題となりました。

プロキシネットワークの組織モデルを構築する意義は、難読化という要素以外に、中国を拠点とする脅威アクターの攻撃方法を根本的に転換させることにある。

図表10-PwCサイバー脅威インテリジェンスが追跡しているプロキシネットワークの視覚化



このようなネットワークを活用する脅威アクターの数は多く（以前はネットワークを活用していなかった者も存在します）、これが「着想を得る」行為を超えるものであることを示しています。私たちは、この手段が標準的な運営手順の一部として定着している可能性が高いと評価しています。

中国を拠点とするエコシステムは、過去と同様のTTP（足場固めの後の手順）を用いて、高い稼働水準で推移しています。プロキシネットワークの広範な採用により、ネットワークを防御する側がこれらの侵入に備え、影響を軽減する方法は根本的に変化しており、脅威インテリジェンスコミュニティやアトリビューション方法に新たな課題をもたらしています。

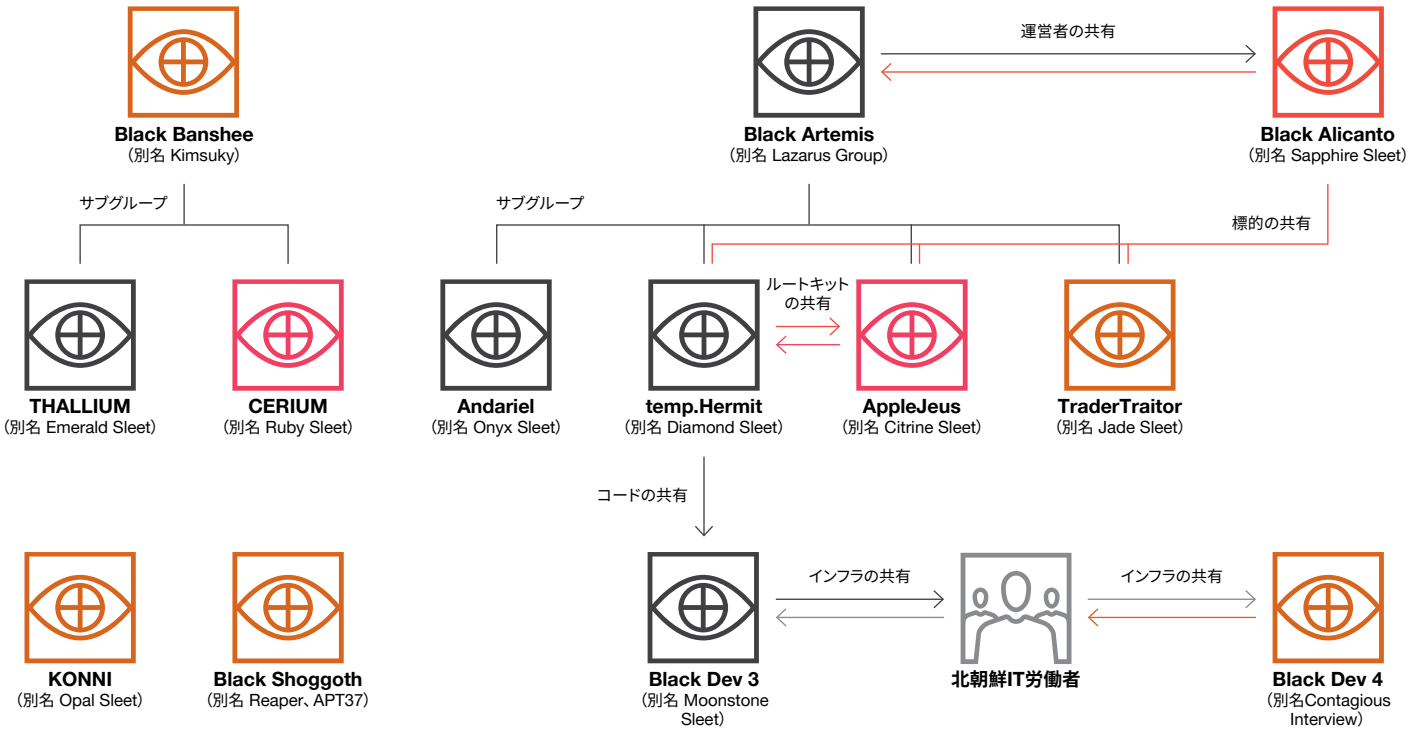
76 'CISA and Partners Release Advisory on PRC-sponsored Volt Typhoon Activity and Supplemental Living Off the Land Guidance',US CISA, https://www.cisa.gov/news-events/alerts/2024/02/07/cisa-and-partners-release-advisory-prc-sponsored-volt-typhoon-activity-and-supplemental-living-land (7th February 2024)

ネットワークを防御する部門にとって、侵入の防御は内部環境の安全確保から始まります。組織のアーキテクチャを全体的にマッピングし、その後、全てのデバイス（特に境界の「エッジ」にあるデバイス）があらゆるテクノロジーの最新バージョンにパッチされていることを確認します。セキュリティの追加対策として、信頼できる情報源からリリースされたガイダンスに沿ってエッジデバイスの一貫したログ分析を行うことで、ゼロデイ悪用の際に侵害を判断できる可能性が高まります。

注目のテーマ：北朝鮮の脅威

中国を拠点とする脅威アクターによるプロキシネットワークの拡散と同様に、北朝鮮を拠点とする脅威アクターも2024年にTTPを整備していることが観察されており、これには商用VPNプロキシ活動のより広範な利用が含まれます[77]。また、従来のマルウェアの亜種[78]や全く新しいバックドア[79,80]を組み合わせることで、マルウェアや標的が複数の異なる侵入セットで共有されるようになりました。また、Black Alicanto（別名 Sapphire Sleet）のような脅威アクターが、MacOSシステムを標的とする能力を強化し続けている傾向も観察されています[81]。

図表11-PwCの遠隔測定による北朝鮮の脅威アクターと個々の関係の視覚化



77 'DPRK proxying activity' ,PwC Threat Intelligence,CTO-TIB-20240502-01A

78 'New FASTCash malware Linux variant helps steal money from ATMs' ,Bleeping Computer, https://www.bleepingcomputer.com/news/security/new-fastcashmalware-linux-variant-helps-steal-money-from-atms/ (14th October 2024)

79 'SHROUDED#SLEEP: A Deep Dive into North Korea's Ongoing Campaign Against Southeast Asia' ,Securonix, https://www.securonix.com/blog/shroudedsleep-a-deep-dive-into-north-koreas-ongoing-campaign-against-southeast-asia/ (3rd October 2024)

80 'APT Actors Embed Malware within macOS Flutter Applications' ,Jamf, https://www.jamf.com/blog/jamf-threat-labs-apt-actors-embed-malware-withinmacos-flutter-applications/ (12th November 2024)

81 'A video call with Black Alicanto' ,PwC Threat Intelligence,CTO-TIB-20241211-01A

これは、2023年に北朝鮮を拠点とする脅威アクターによって、前例のない数のサプライチェーン指向の侵入が行われたことを背景としたものです[82,83,84]。この傾向は強力であり、2024年も主要な活動手法として継続する可能性が高いと評価します[85]。TTPの統合におけるシフトは、活動の技術的水準と安全性を高めようとする試みの表れと考えられます。

図表12-北朝鮮を拠点とする脅威アクターのTTPの概要

	Diamond Sleet	Jade Sleet	Citrine Sleet	Onyx Sleet	Black Dev 3	Black Dev 4	Black Alicanto	北朝鮮IT労働者
メールによるスピアフィッシング	✓			✓	✓	✓	✓	
ソーシャルメディアによるスピアフィッシング	✓	✓			✓	✓	✓	
戦略的なウェブ侵害				✓				
脆弱性の悪用	✓		✓	✓				
サプライチェーンへの攻撃	✓	✓	✓					
トロイの木馬型バイナリ	✓	✓	✓		✓	✓	✓	
悪意のあるnpm / PyPi パッケージ		✓	✓		✓	✓		
直接雇用					✓			✓

このような従来型TTPへの回帰では、初期アクセスで過去に利用してきたソーシャルエンジニアリングに再度注力する姿勢が見られます。例としては、北朝鮮を拠点とする脅威アクターが防衛分野の個人を対象とした偽の求人広告を作成するといったものがあります[86]。ソーシャルエンジニアリングのアプローチ自体も進化しており、北朝鮮を拠点とする脅威アクターは、アクセス権を得るために斬新な手法を取り入れています。これは、自己の国籍を偽り、関心のある組織のリモートワークのポジションに応募するというもので、2022年に活動の一部となり[87]、2023年も引き続き観察されました[88]。前年のIT労働者の事象と2024年の活動との違いは、規模と組織であり、「労働者」チーム内で働いていると考えられる個人は1万人を超えていました[89,90]。

82 'North Korea: supply chain attacks and cryptocurrency targeting' ,PwC Threat Intelligence,CTO-SIB-20231024-01A

83 '3CX Supply Chain Compromise' ,PwC Threat Intelligence,CTO-QRT-20230330-01A

84 'Black Artemis CyberLink supply chain compromise' ,PwC Threat Intelligence,CTO-QRT-20231124-01A

85 'Cyber Threats 2023: A Year in Retrospect' ,PwC Threat Intelligence,CTO-YIR-20240627-01A

86 'Bluenoroff recruitment drive' ,PwC Threat Intelligence,CTO-TIB-20190605-01A

87 'Guidance On The Democratic People's Republic Of Korea Information Technology Workers' ,US DOJ, https://ofac.treasury.gov/media/923126/download?inline (16th May 2022)

88 'Additional Guidance on the Democratic People's Republic of Korea Information Technology Workers',FBI, https://www.ic3.gov/PSA/2023/PSA231018 (18th October 2023)

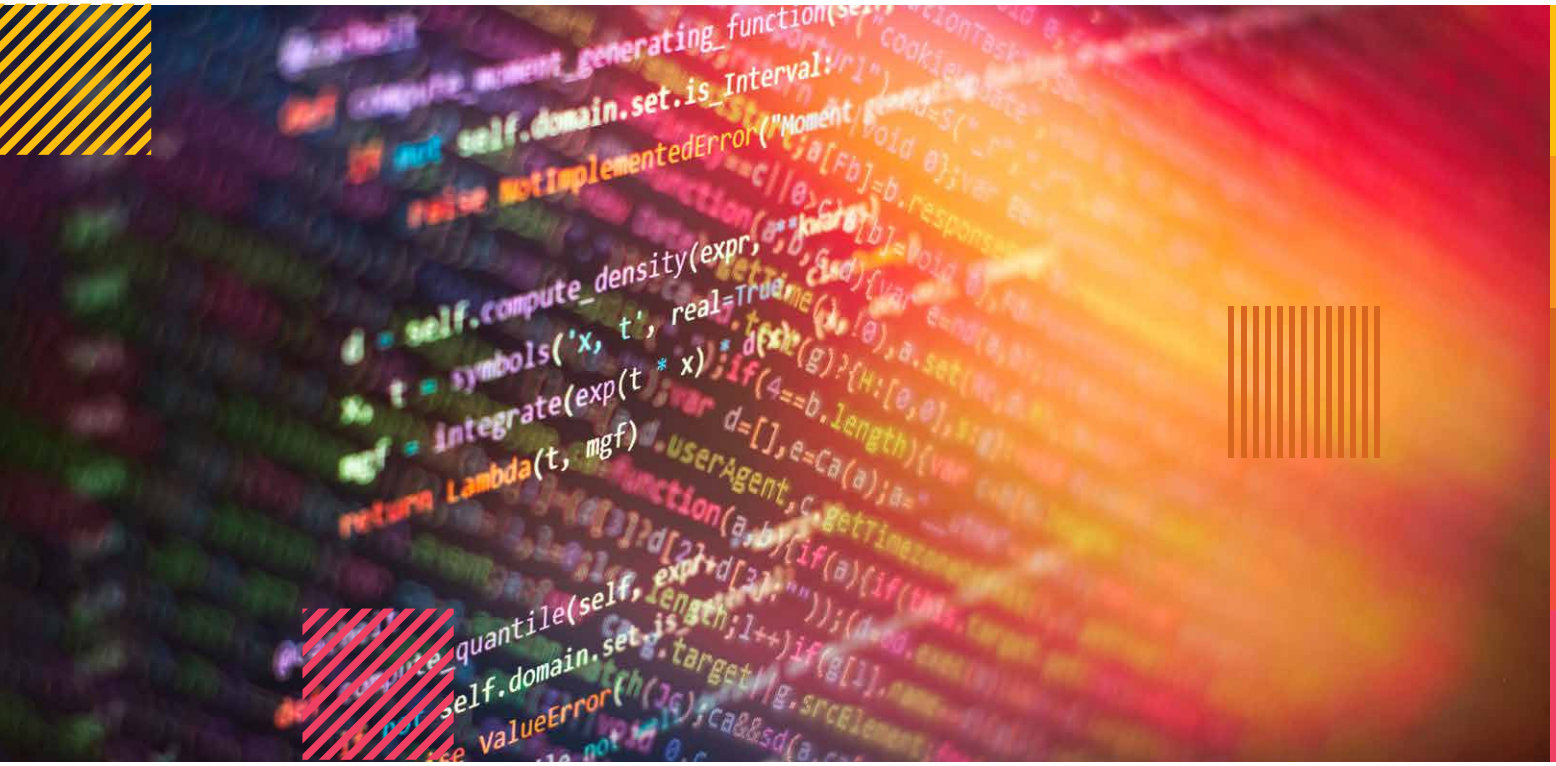
89 'Advisory on Democratic People's Republic of Korea (DPRK) information technology (IT) workers' ,Australian Government (Department of Foreign Affairs and Trade), https://www.dfat.gov.au/international-relations/security/sanctions/guidance/advisory-democratic-peoples-republic-korea-dprk-information-technologyit-workers (26th August 2024)

90 'Black Dev 4 is hiring' ,PwC Threat Intelligence,CTO-TIB-20240625-01A

以前から現在に至るまで暗号通貨ベンダーを標的として実施されてきた活動に比べれば、金銭的にはあまり利益が上がらないように見えるかもしれませんが[91,92]、この手法の成長は大きな意味を持ちます。正式な雇用を通じて多額の収入を得ることができるのはもちろんのこと、北朝鮮を拠点とする者が作業者として雇用されれば、企業諜報や恐喝が可能となります。これは追加の収益獲得ルートを提供するだけでなく、北朝鮮を拠点とする「脅威アクター像」を変えることにもなります。

比較的小規模なサプライチェーン攻撃が統合されつつ、従来の標的が維持されていること（活動のペースも増していること）は、北朝鮮を拠点とする複数の侵入組織が（暗号通貨を扱う組織のみを標的とするのではなく）情報収集に重点を置くことを望んでいる、あるいは潜在的にその必要性があることを示している可能性が高いと考えられます。これはIT労働者キャンペーンにも見られ、脅威アクターは機密データを流出させるとともに、侵害後の恐喝行為や正当な賃金による収益を得る可能性を生み出しました。

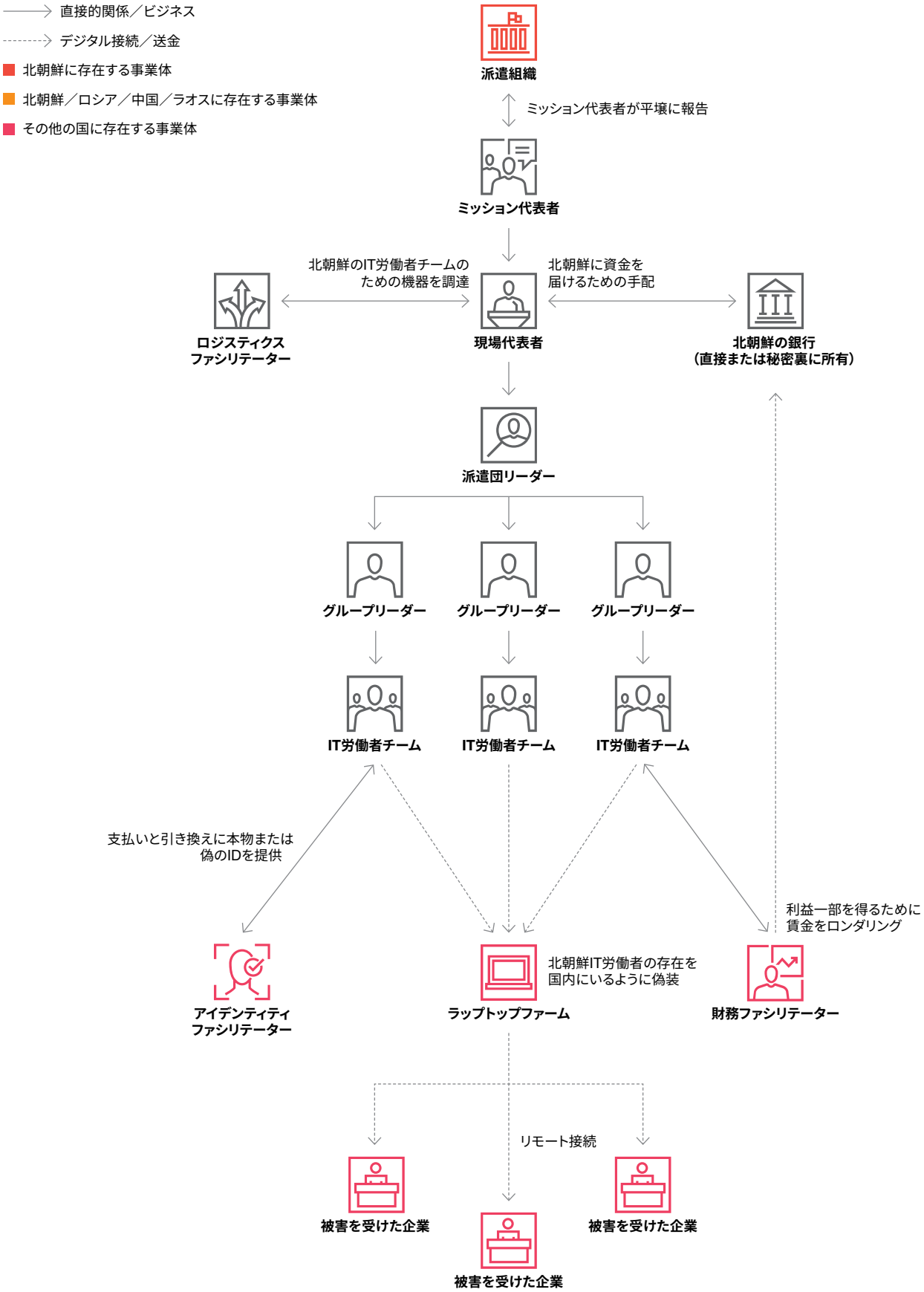
IT労働者事象の出現により、ネットワークを防御する側は従来の検知ルールやポリシーに注力するだけでなく、インサイダーの脅威にも注意する必要に迫られます。



91 'Black Artemis CyberLink supply chain compromise',PwC Threat Intelligence,CTO-QRT-20231124-01A

92 'DPRK Supply Chain Attacks',PwC Threat Intelligence,CTO-SIB-20231024-01A

図表13-北朝鮮IT労働者キャンペーンの運営に必要なインフラの上下関係



2023年には、北朝鮮を拠点とする脅威アクターが大規模なサプライチェーン攻撃を行ったことが複数の主要メディアで報じられました[93,94]。しかしながら、2024年にはこれに匹敵する事例はほとんど見られませんでした。その一方で、情報収集、特に軍事と防衛に関する情報収集に注目が集まりました[95]。ネットワークインフラストラクチャーのTTPが強化されたことに加え、諜報活動を動機とする活動の規模が拡大し、重点が置かれるようになったことで、2024年は北朝鮮を拠点とする脅威の評価方法全般に変化が生じました。北朝鮮を拠点とする脅威アクターの活動の背後にある動機は同じであることが多い一方で、私たちが追跡している侵入セットでは、その手法やテクニックが変化していることが観察されています。そのため、個々の活動間でのアトリビューションの実行や、どの脅威アクターが現在どのような任務を担っているのかを見分けることが困難になっています。

93 'North Korean hackers breach software firm in significant cyberattack' ,CNN, https://www.cnn.com/2023/04/20/politics/north-korea-hacking-supply-chain-3cx-mandiant/index.html (20th April 2023)

94 'North Korean hackers breached a US tech company to steal crypto' ,Reuters, https://www.reuters.com/technology/n-korea-hackers-breached-us-itcompany-bid-steal-crypto-sources-2023-07-20/ (20th July 2023)

95 'NCSC and partners issue warning over North Korean state-sponsored cyber campaign to steal military and nuclear secrets' ,UK NCSC, https://www.ncsc.gov.uk/news/ncsc-partners-vigilant-dprk-sponsored-cyber-campaign (25th July 2024)

セクション 4

荒れ狂う海

地政学的状況はデジタル化の黎明期からサイバー活動を形作ってきましたが、2022年以降になって初めて、紛争時に「サイバー領域」がどのように利用されるかという現実を目の当たりにしました。2024年には、拡大の一途をたどる紛争（イラン・イスラエル間の緊張の高まりなど）や収まる兆しもない紛争（現在では北朝鮮の関与が認められているロシアのウクライナ侵攻など）があり、「戦時下」の活動が全般的に活発化しています[96]。

さらには、米中間で非難の応酬がエスカレートし、その多くがサイバー領域に関する問題に集中しており、目に見える脅威の勢力が変化しています。活動が次々と公にされる中で、そのテンポは全体的に、このような政治的駆引きや国家関係の変化に著しく左右されることがあります。

ランサムウェアエコシステムについても、法執行機関がその効力を抑制しようと試みたにもかかわらず、2024年にはかつてないほどに活発な動きを見せました。リークサイトは膨大（記録開始以来最高）にありますが、それは全体像の半分に過ぎません。ランサムウェアの活動件数からも、このエコシステムの回復力と適応力が際立っていることは明らかです。

ロシア―ウクライナ：消耗戦が継続した1年

ロシアのウクライナに対する軍事作戦が、急速な占領地拡大から複数の戦線にわたる段階的な前進にシフトしたことに合わせて、サイバー活動も変化しました。

96 'North Korea goes to Russia', PwC Threat Intelligence, CTO-SIB-20241113-01A

戦争の初期段階において、ロシアを拠点とする脅威アクターは、ウクライナの重要な国家インフラを標的とした破壊的なワイパーを展開するとともに[97,98]、防衛機関[99]、政府機関[100]、関連機関に対する情報収集活動を行っていたことが観察されました[101]。2023年には、ワイパーの使用は目に見えて減少し、代わりにより従来型の諜報活動が活発化しています。標的もまた、喫緊の政治経済に沿って穀物取引に関連する食品・農業分野などの民間組織にまで拡大されました[102,103]。

予想されていたとおり、2024年にはロシアを拠点とする脅威アクターがウクライナを主な対象として情報収集活動を継続しました。私たちが追跡しているロシアを拠点とする多くのグループのTTPは、2022年以降も変わっていません。

- Blue Callisto（別名 COLDRIVER、Star Blizzard）は、PDF形式のおとり文書ほか、リモート・テンプレート・インジェクションを悪用したインフラやフィッシングメールを用い、NGOやシンクタンクを標的として活動を続けていました[104]。
- Blue Dev 8とBlue Athena（別名 Forest Blizzard、BlueDelta）も、ウクライナを拠点とする防衛機関や政府機関を特段の標的としてBlue Callistoと同様の活動を実施しました[105,106]。
- Blue Dev 5（別名 NOBELIUM、Midnight Blizzard）は、2024年を通して例年と同じマルウェアを使用していることが観察されており、EnvyScoutと呼ばれるHTMLスマグリングマルウェアのテーマとしてNATOとウクライナを使用し、次の段階でCobalt Strikeペイロードをロードしています[107]。
- Blue Otso（別名 Gamaredon Group）は、2024年のウクライナを標的にした活動展開時の従来のインフラとTTPを維持しており、PowerShellとMSHTAファイルを組み合わせてCloudflare Tunnelの悪用を継続しています[108]。

Blue Athena（別名 APT28）をはじめとするその他の脅威アクターは、西側諸国の外務省を標的にして従来の活動を継続しています[109]。またBlue Dev 5は、西側諸国やその同盟諸国の防衛機関、NGO、教育機関などを標的にした活動を継続していることが観察されています。2024年末時点で西側諸国高官らが数々の妨害行為についてモスクワを非難していたような[110,111]ロシアとNATO加盟国の関係から考えると、このレベルの活動は、拡大することはなくとも今後も継続すると予想されます。

97 Ukraine One Year On' ,PwC Threat Intelligence,CTO-TIB-20230428-01A

98 'Cyber Threats 2022: A Year in Retrospect' ,PwC Threat Intelligence,CTO-YIR-20230403-01A

99 'Blue Dev 4 phishing operations in 2022' ,PwC Threat Intelligence,CTO-QRT-20220303-01A

100 'Blue Otso retains Ukraine interest' ,PwC Threat Intelligence,CTO-TIB-20220203-01A

101 'The Nearest Neighbor Attack: How A Russian APT Weaponized Nearby Wi-Fi Networks for Covert Access' ,Volexity, https://www.volexity.com/blog/2024/11/22/the-nearest-neighbor-attack-how-a-russian-apt-weaponized-nearby-wi-fi-networks-for-covert-access/ (22nd November 2024)

102 'Cyber Threats 2023: A Year in Retrospect' ,PwC Threat Intelligence,CTO-YIR-20240627-01A

103 'Russian threat actors dig in, prepare to seize on war fatigue' ,Microsoft, https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/russian-threat-actors-dig-in-prepare-to-seize-on-war-fatigue (7th December 2023)

104 'Does this phish smell Blue to you?' PwC Threat Intelligence,CTO-TIB-20240205-01A

105 'Blue Dev 8' s net on Ukraine' ,PwC Threat Intelligence,CTO-TIB-20240520-01A

106 'Making a Mock(er)y of credential harvesting' ,PwC Threat Intelligence,CTO-TIB-20240702-01A

107 'RSVP at your peril!' ,PwC Threat Intelligence,CTO-TIB-20241018-02A

108 'Blue Otso with chance of TryCloudflare' ,PwC Threat Intelligence,CTO-TIB-20241030-02A

109 'Blue Athena Dumps Webhooks into the Water' ,PwC Threat Intelligence,CTO-TIB-20240214-01A

110 ''UK spy chief says Russia behind 'staggeringly reckless' sabotage in Europe' ,Reuters, https://www.reuters.com/world/europe/russia-behind-staggeringlyreckless-sabotage-europe-uk-spy-chief-says-2024-11-29/ (29th November 2024)

111 'Finlandization: More Please' ,CEPA, https://cepa.org/article/finland-challenges-russian-sabotage/ (30th December 2024)

中東—紛争の年

2024年を通じて、中東で進行する戦争行為はサイバー領域でも同様に存在しており、2023年10月7日から同年末にかけて活動の一部として観察されていました。イランを拠点とする脅威アクターは、イスラエルの機関を特段の標的として、認証情報のフィッシング、バックドア、妨害行為など、過去数年にわたって観察されてきた従来の活動を活発化させるとともに、イスラエル国民を狙った心理学的な活動を大幅に拡大したりするなどして引き続き活動を続けています[112]。この活動は、オマーン、UAE、ヨルダンなどの近隣の敵対国家だけでなく、米国などの世界中の敵対国家も標的にしています。

イランの外交政策と中東での野心が大きな困難に直面した年に、イランを拠点とする脅威アクターの活動が活発化しました。これは、サイバー作戦が国家の力を誇示する重要な手段という説を裏付けるものです[113]。2024年末に起きたアサド政権崩壊の直接的な原因が、イランがシリアへのリソース投入を迅速に行えなくなったことなどにあると多くの人が指摘している点を踏まえると、イランを拠点とするサイバー脅威が2025年にどのように影響を及ぼすかは不透明なところであるものの、引き続きイラン政府の外交政策目標に沿う可能性が高いと見られます。

2024年の出来事を振り返った上で2025年を見据えると、ハマスのサイバーインフラ、特にパレスチナに拠点を置くサイバーインフラの多くは機能しなくなる可能性が高いと思われます。しかしながら、それと同時に、イスラエルによる掃討作戦の及ばない安全な場所にいる部隊が10月と11月のような作戦を継続して展開する可能性が高いと評価しています。ヒズボラとつながりのある脅威アクターに及んだ影響は全体的に少ないと見られ、2025年に継続的な行動が見られた場合には、現実的な確率に基づくと活動が再開されることが見込まれます。

北朝鮮—もはや隠遁者ではない

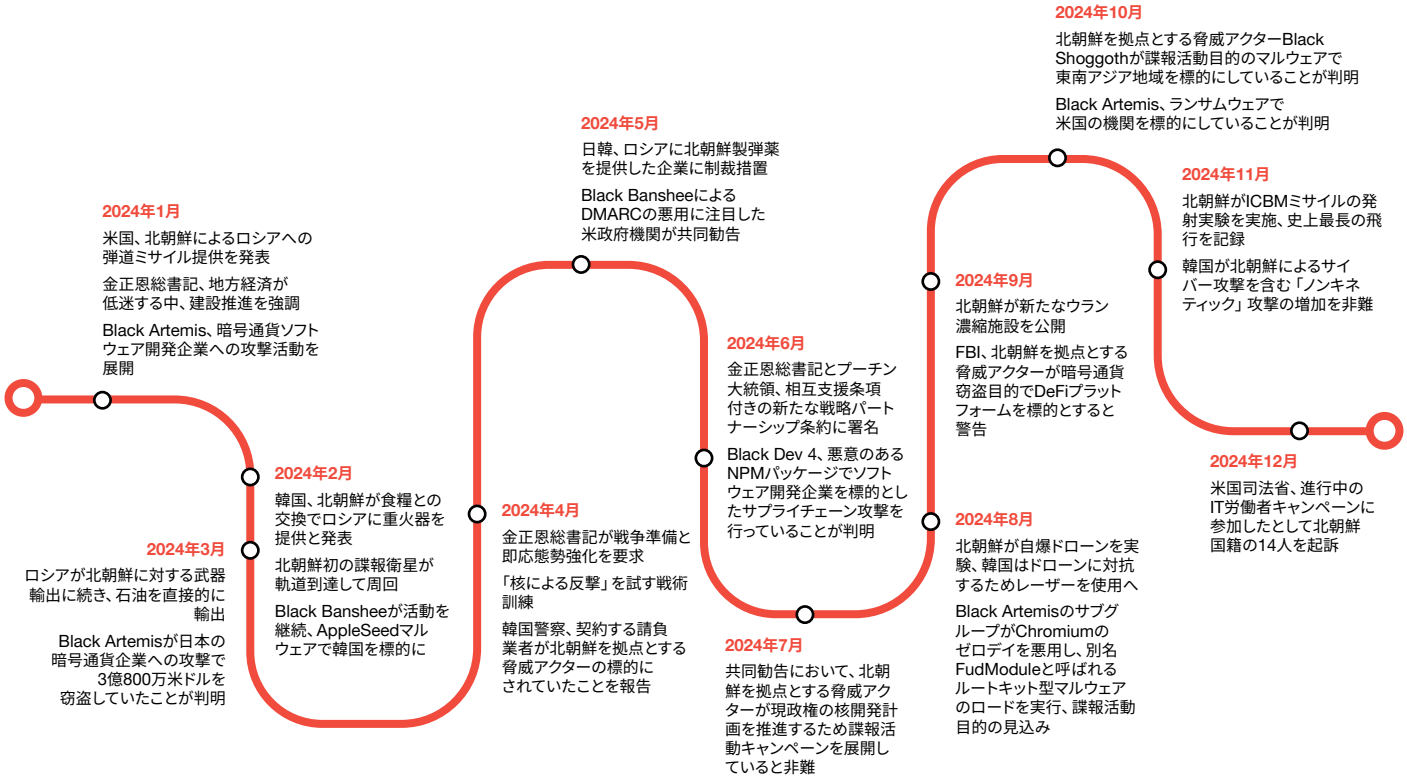
北朝鮮を拠点とする脅威アクターの2023年の活動と言えば、諜報活動と犯罪行為（暗号通貨の窃盗など）の両方を目的とした有名サプライチェーンのセキュリティ侵害の数々が挙げられます[114]。しかし、このような頻繁な活動と外交上の政治工作に全ての侵入行為が直接関連するわけではないと思われることから、その多くは北朝鮮の困窮した経済状況に資するものとして行われた可能性が高いと思われます。ただし、2024年には活動の頻度が上がり、外交政策も大幅に強化されています。

112 'Yellow Dev 19 influence campaign goes ballistic' ,PwC Threat Intelligence,CTO-QRT-20241029-01A

113 'IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities' ,US CISA, https://www.cisa.gov/newsevents/cybersecurity-advisories/aa23-335a (18th December 2024)

114 'Cyber Threats 2023:A Year in Retrospect' ,PwC Threat Intelligence,CTO-YIR-20240627-01A

図表14-2024年における北朝鮮の主要な政治工作のタイムライン



PwCサイバー脅威インテリジェンス

諜報活動を動機とする侵入は、防衛、航空宇宙、テクノロジー、建設、農業など、北朝鮮が存続するために重要と言える分野での技術力不足の補填に貢献している可能性が高いと見られます[115,116,117]。これに対し、犯罪組織は現政権への資金提供を継続する可能性が高いと見られます。

私たちは、ここ数年のサイバー領域での成功が最終的には金正恩政権による2024年の強硬的な外交政策につながった可能性が高いと評価しています。技術盗用による戦闘面での技術力の向上[118,119]、核兵器プログラムのアップグレード[120]、諜報活動を動機とする侵入を通じた政治的敵対国に対する知見の深化[121]がこの動向における重要な要因であったと思われます。

115 North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs',Joint Cybersecurity Advisory, https://media.defense.gov/2024/Jul/25/2003510137/-1/-1/1/Joint-CSA-North-Korea-Cyber-Espionage-Advance-Military-Nuclear-Programs.PDF (25th July 2024)

116 'An Offer You Can Refuse: UNC2970 Backdoor Deployment Using Trojanized PDF Reader',Mandiant, https://cloud.google.com/blog/topics/threat-intelligence/unc2970-backdoor-trojanized-pdf-reader (17th September 2024)

117 'APT Group Kimsuky Targets University Researchers',Resilience, https://www.cyberresilience.com/threatintel/apt-group-kimsuky-targets-universityresearchers/ (7th August 2024)

118 'North Korea's first spy satellite is 'alive', can manoeuvre, expert says',Reuters, https://www.reuters.com/technology/space/north-koreas-first-spy-satellite-isalive-can-manoeuvre-expert-says-2024-02-28/ (28th February 2024)

119 'South Korea says DPRK hackers stole spy plane technical data',BleepingComputer, https://www.bleepingcomputer.com/news/security/south-korea-saysdprk-hackers-stole-spy-plane-technical-data/ (12th August 2024)

120 'North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs',US CISA, https://www.cisa.gov/newsevents/cybersecurity-advisories/aa24-207a (25th July 2024)

121 '코니(Konni)위협 세계관의 확장 분석 리포트 - Expanded Analysis of Konni Threat Universe',Genians, https://www.genians.co.kr/blog/threat_intelligence/konni_universe (September 2024)

2024年末に北朝鮮がロシアのウクライナ侵攻に軍需品と兵士を提供して正式に参加しましたが、これは、比較的孤立状態にある両国の軍事協力関係の拡大を象徴しています[122]。2025年には、北朝鮮を拠点とする脅威アクターが、暗号通貨の窃盗を中心に、独自の諜報技術を活用するために企業を標的にした活動を引き続き展開する可能性が高いと見られます。IT労働者の利用[123]など2024年に主流であった手法が今後も継続するかは別として、違法な資金流入が必要であるため、今後も北朝鮮を拠点とする悪質なサイバー上の攻撃活動が継続する可能性は高いと見られます。

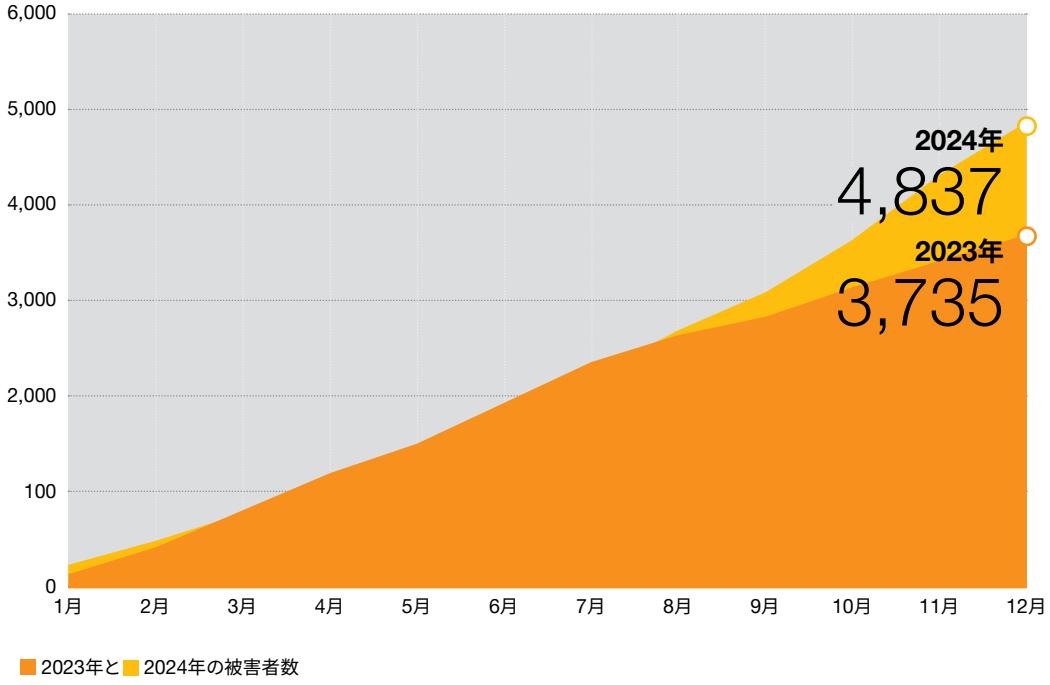
29.5%

ランサムウェアリークサイトの被害者数が2023年比で増加した割合

ランサムウェア—止められない止まらない

ランサムウェアエコシステムは、環境に依存しない脅威の筆頭として注目され続けており、官民を問わずあらゆる業界に影響を与えています。リークサイトの件数では、2024年9月には2023年の実績に到達しており[124]、2024年はRaaSの活動が記録上最も活発な年となりました[125]。

図表15-2023年と2024年のリークサイト総数の比較



122 'North Korea goes to Russia' ,PwC Threat Intelligence,CTO-SIB-20241113-01A

123 'A video call with Black Alicanto' ,PwC Threat Intelligence,CTO-TIB-20241211-01A

124 'Ransomware report: 2024 Issue 9' ,CTO-CTS-20241029-01A

125 Ransomware statistics taken from leak sites do not tell the whole story, as there are multiple entities which are subject to a ransomware intrusion that will either pay before the data is published on a leak site, or are impacted by a ransomware attack that does not have a double extortion component. As with any collation of ransomware statistics, we assess the number to be higher than the one produced by amalgamating individual leak site statistics alone.

2024年第1四半期に行われた法執行機関の取り組み（オペレーションエンドゲームと、ALPH-Vの情報に関連する報奨金から生まれる圧力の両方を含む[126,127]）は、ランサムウェアエコシステムの真の回復力を確認するには絶好の機会でした。2大プログラムが市場から排除されたことで、その影響を受けるアフィリエイトは、別のRaaSの下で継続するか、法執行機関の追加措置による逮捕に怯えながら活動を停止するかのいずれかを迫られます。オペレーションクロノスの作戦開始後、逮捕者と有罪判決者が出ましたが[128]、エコシステムは市場主導型であり、標準的な運営手順が十二分に確立されているため、妨害工作が行われても通常の運営に長期的な影響を与えることはないだろうというのが当初の見立てでした[129]。

185%

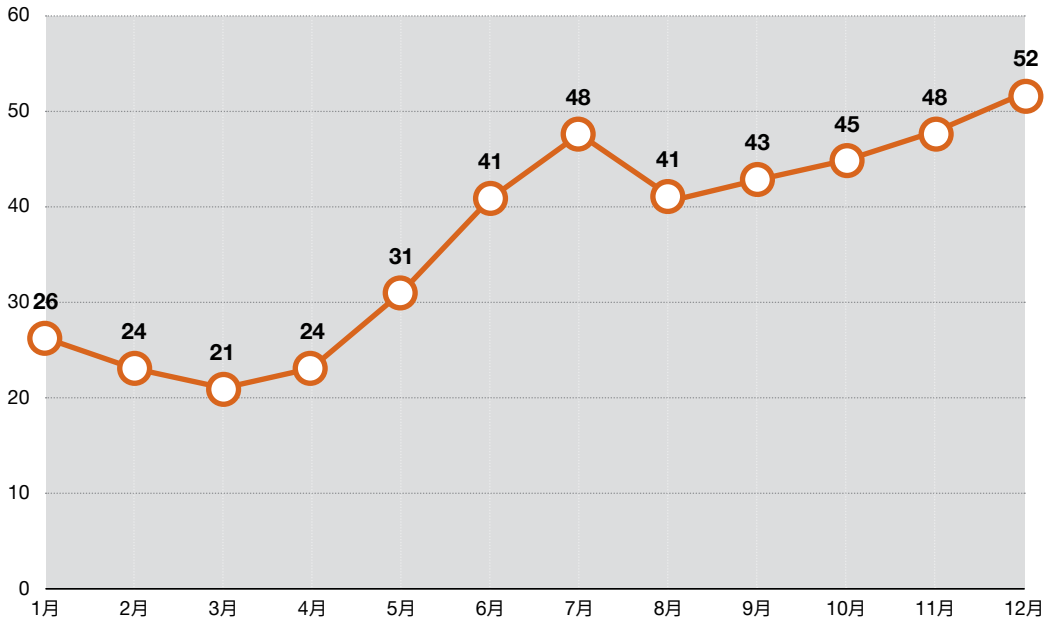
リークサイトの活動数が増加した割合

2024年の残りの期間で明らかになったことは、この見立てをさらに悪化させた結果でした。法執行機関によって後退を余儀なくされたにもかかわらず、リークサイトの件数は過去最多に達しました。ただし、この年について最も重要なポイントは有効なプログラムの件数であると評価しています。

2024年1月には、26種類のランサムウェアの脅威アクターによる被害が生じていました。特に3月以降（オペレーションクロノス後のエコシステムが落ち着き始めたと思われる時期）、有効なRaaSプログラムの件数は着実に増加し、12月には52の脅威アクターが専用かつ有効なリークサイトを持ち、ピークに達しました。

このようなプログラムには、何年にもわたって活動しながらいまだ法執行機関の正式な標的になっていない確立済みの「ブランド」（PLAYやBlackByteなど）、限定的な成功を収めた新しいプレイヤー（DragonForceやSpace Bearsなど）、成功がより顕著な新しいプレイヤーが混在しています。

図表16-2024年の月別ランサムウェアリークサイト数



126 'The NCA announces the disruption of LockBit with Operation Cronos' ,UK NCA, https://www.nationalcrimeagency.gov.uk/the-nca-announces-the-disruptionof-lockbit-with-operation-cronos

127 'BlackCat was its own bad omen' ,PwC Threat Intelligence,CTO-SIB-20240322-01A

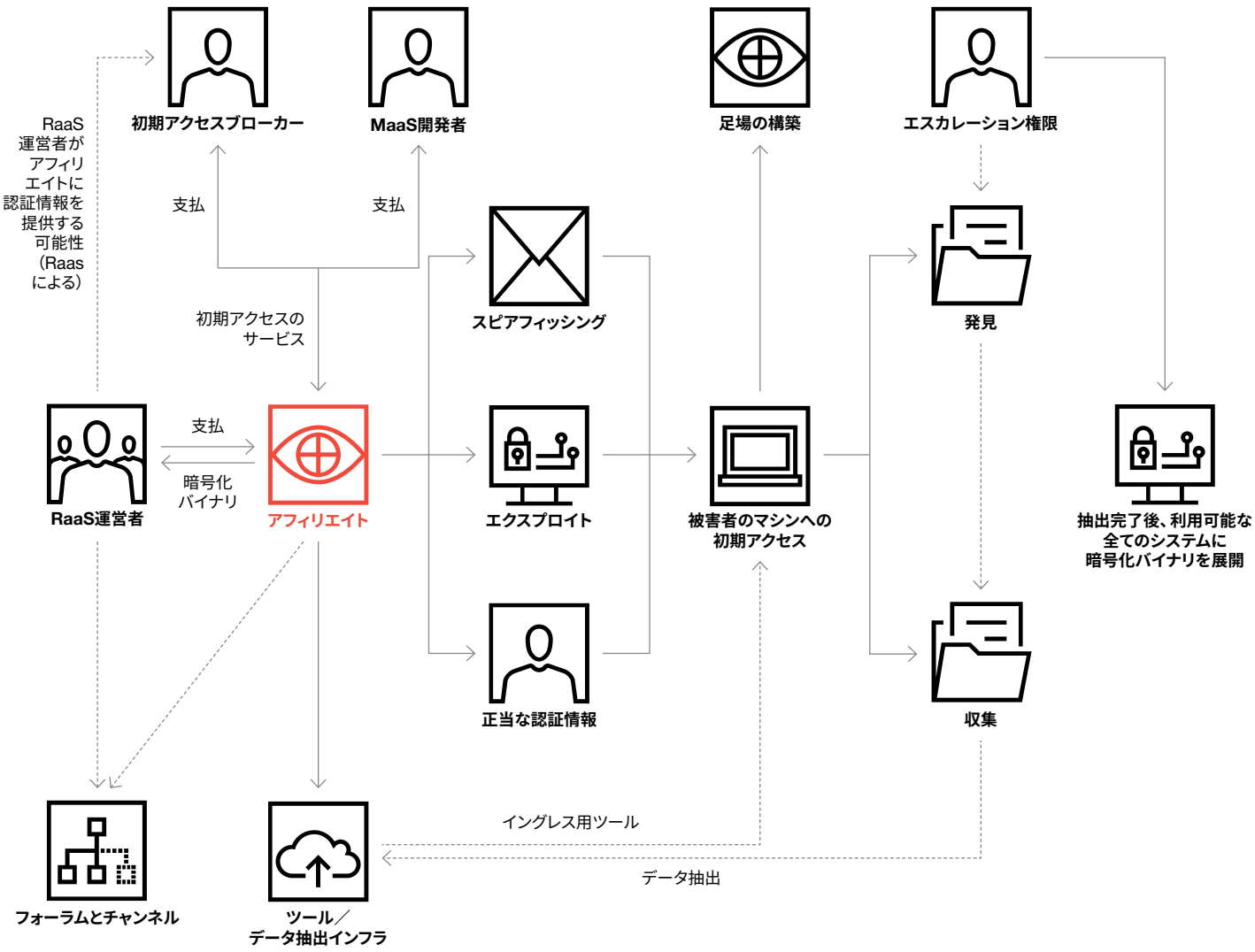
128 'Two Foreign Nationals Plead Guilty to Participating in LockBit Ransomware Group' ,US DOJ, https://www.justice.gov/opa/pr/two-foreign-nationals-pleadguilty-participating-lockbit-ransomware-group (18th July 2024)

129 'Ransomware report 2024 Issue 2' ,PwC Threat Intelligence,CTO-CTS-20240404-01A

2024年のリークサイトデータから見る限り、有効な小規模プログラムの数がランサムウェアの状況を大きく変えたことは明らかです。プレイヤー数が少なかった2023年には、LockBit 3.0がエコシステムを支配して被害者全体の27%を占め、それに続くALPH-Vは10%でした。2024年の被害者の分布はこれに比してはるかに均等で、Ransomhubの被害件数が最多であったものの、全体の11%に過ぎませんでした（LockBit 3.0は10%で2位）。

2024年2月まで存在しなかったRaaSプログラムであるRansomhubが2024年にリークサイト数のトップに立ったのは特筆すべき事項です。RaaSの運営全体を見渡すと、支払交渉、アフィリエイト管理、コードベースやツールのメンテナンスなど、かなりの数の実働部門が存在し、効果的な運営を行うにはそれらに対応した運営手順が必要となります。これは、合法的な企業と変わりません。ランサムウェアの事業体は、犯罪組織であり、さまざまな専門性を持った無数の個人で構成されている点が、ランサムウェアの運営をより一層困難にしているものの、このような新しいプレイヤーは上述のような能力を発揮しています。

図表17-ランサムウェア・アズ・ア・サービス（RaaS）の運営モデルの概要



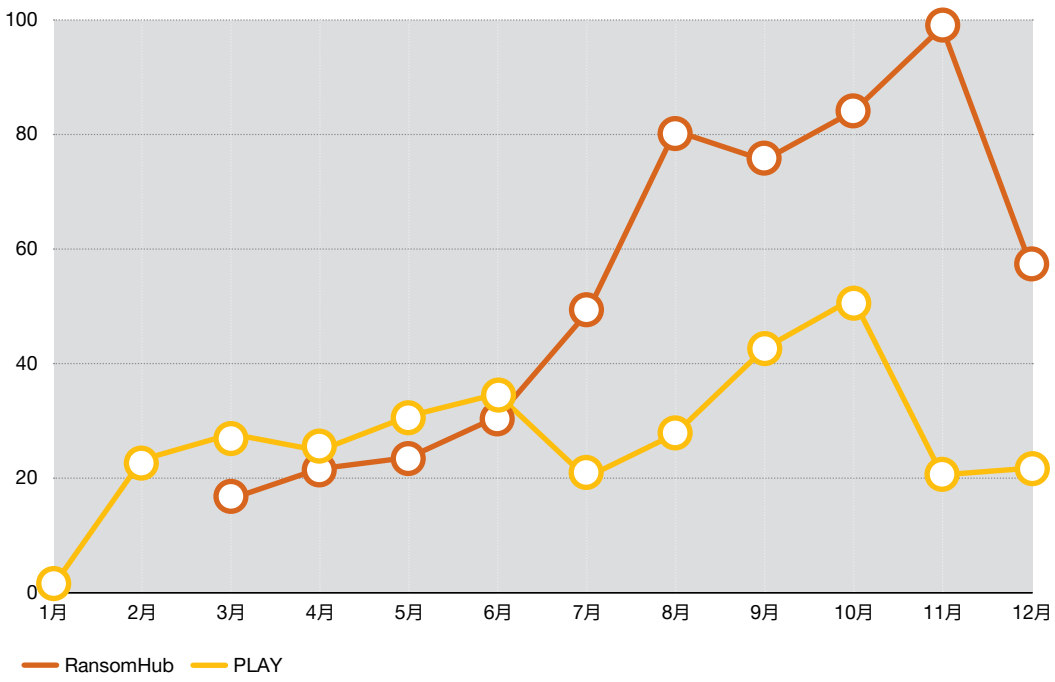
これは重要なことです。というのも、過去を振り返って見ても、ランサムウェアの運営期間中、継続的にリークサイトの被害者数を持続できた事業体はわずかに過ぎず、そのようなレベルの仕組みを得るには相当な時間がかかるためです[130]。2024年には、この従来の論理にやや反するRaaSプログラムが複数登場し、運営開始から数カ月で40件以上の被害者を出しました。

注目のテーマ：RansomHub

RansomHubは、2024年2月2日に地下組織のRAMPフォーラムで初めて発表されました。発表元は「koley」というペルソナを持つユーザーで、このユーザーは2023年5月3日に同フォーラムに登録したと見られています。この発表の大部分は以前観察されたRaaS関連のフォーラムへの投稿と一致していましたが、RansomHub RaaSの収益の90%をアフィリエイト、10%を開発者に分配する構造を主張した点が際立っていました[131]。

最終的なコードベースがKnightランサムウェアのソースコードと重複していること、さらにLockBitとALPHVの構成オブジェクトキーへのリンクが複数追加されていること[132]といった暗号化バイナリの技術的な要素が明らかになる一方で、注目を集めている点は、RansomHubが短期間で最も成功したプログラムになったスピードです。

図表18-RansomhubとPLAYのランサムウェアリークサイト統計の不一致



130 アナリスト注記：流出したContiのファイルからは、Conti（2020年から2022年にかけて圧倒的に最大規模を誇ったRaaS）ほどの大規模なRaaSプログラムを実行するために必要とされる仕組みの広がりについて深い知見が得られた。参照先: 'Negotiation tactics and internal dynamics' ,PwC Threat Intelligence,CTO-SIB-20220324-01A

131 アナリスト注記：RaaS運営の経済性に関連する情報は断片的で、その多くは運営者（あるいは時にアフィリエイト）によるフォーラムへの投稿、リークされた個人的な議論、または珍しい例としてメディアとのインタビューに基づいた情報である

132 'RansomHub Ransom Run' ,PwC Threat Intelligence,CTO-TIB-20241108-01A

例えば、PLAY RaaSのような、RansomHubよりはるかに長く運営されているプログラムと比較すると、リークサイトは膨大にあります。このデータから結論を導き出すには注意が必要です。RansomHubにとどまらず、RaaS運営の大部分は、その内情が謎に包まれているためです。しかし、このような前例のない成長には相関的な要素が複数必要であると私たちは評価しています。

2024年には、外圧に対するRaaSエコシステムの回復力と適応力が判明した。巧妙かつ集団的に行われてきた法執行機関の取り組みをもってしても、侵入件数と運営プレイヤー数双方の増加を食い止めることができなかった

- **市場の隙間：**RansomHubが前例のない上昇を遂げた最も大きな要因は、RansomHubの最初のオファーが背景にあると見られます。犯罪エコシステムに導入後、数日のうちに法執行機関によるLockBit 3.0への妨害工作が行われ、さらにはALPHVが解体されました。当時の2大プログラムがこのような状態になったことで、アフィリエイトにはある種の空白が生まれました。
- **魅力的な提案：**RaaSのエコシステムは限られた数のアフィリエイトで構成されています。この数は従来より増えているものの、RansomHubの運営者は活動を実行するために、すでに他のプログラムの一部となっているアフィリエイトの基盤を引き付ける必要があります。90/10の収益分割広告を使用することで、すでに確立されたアフィリエイトをRansomHubプログラムに誘導することができ、特に、新しい機会を探しているアフィリエイトが複数存在した可能性が高いと見られます。
- **使いやすく、理解しやすい：**RaaSプログラムを成長させるには、できるだけ多くのアフィリエイトを引き付ける必要があります。このようなアフィリエイトの全てが同じ技術的水準を有していることはなく、White Dev 164（別名 Scattered Spider）のように、侵入の手法を統合した熟練したチームもあれば、新参のチームもあります。RansomHubのコードベースは、他のランサムウェアプログラムからコマンドフラグを借用しており、構成可能な機能を相当備えているため、既存の活動に比較的簡単に組み込むことができます。
- **効果的な経営：**合法的な企業と同様に、RaaSプログラムの有効性は、基盤となる構造に依存します。ランサムウェアプログラムの機能がリークサイトの管理にとどまらず、より多くの側面から構成されていることについてはご承知のとおりです。RansomHubをこれほど急速に拡大できるようにするには、運営者には、ランサムウェア分野で経験を積んだ個人か、プログラムをあらゆる要素において円滑に運営できる多様なスキルを備えたチームが担当する必要があります。

RansomHubの台頭は、機会の到来といったような歴史的な要因だけによるものではなく、統合や組織化などの現実的な要素に後押しされた部分があると見られます。RaaSエコシステムが長く存在すればするほど、標準的な運営手順が定着し、現場の個人はプログラムの運営方法について経験をますます重ね、より効率的な侵入ツールを開発するようになります。こうしてアフィリエイトとプログラム運営者の双方が運営再開や通常どおりの継続に慣れてくることから、法執行機関による妨害工作が及ぼす影響は少なくとも技術レベルでは時間の経過とともに小さくなる可能性があります。

悪事に埋もれて：ポジティブな収穫

この統計ではランサムウェア運営者にとってやや儲けの多い年であったことが明らかになっています。ただし、リークサイト数の多さにやや埋もれてしまっていますが、注目すべきは法執行機関の成功です。2024年2月以前、LockBit 3.0は、数年間にわたる運営で最多の被害者を出したRaaSプログラムでした[133]。その被害件数は約3年間で3,000件近くにものぼりました。

133 'Ransomware report for November 2023' ,PwC Threat Intelligence,CTO-SRT-20240103-01A

オペレーションクロノスは、法執行機関にとって意義のある勝利でした。その意義は、リークサイト数の増加を食い止めることに成功しただけでなく、振り返ってみれば、RaaS環境を基本的に把握していることを示せたという点にあります。LockBitプログラムのアフィリエイトはオペレーションクロノスの基本的な要素と見なされており、以前に実施されたこの種の作戦行動ではそれほど重視されていませんでした。

また、法執行機関はLockBitの運営者（ロシア国籍のドミトリー・ユリエヴィチ・ホロシェフと判明）を十分に把握していたように思われます。これは、オペレーションクロノス実行中に行った措置に対する彼の反応から伺うことができます。オペレーションクロノスのいずれの段階においても、情報公開はドミトリーからの望ましい反応を引き起こしたようで、リークサイトに以前の被害者が再度投稿されたり、金銭を支払ったと思われる被害者が追加されたりしました[134]。LockBit 3.0は2024年末時点で厳密にはまだ稼動しており、2025年初頭にLockBit 4.0をリリースするとしていましたが[135]、2024年12月にリークサイトに投稿された被害者はわずか4件で、稼動中のRaaSプログラムとしてはほとんど機能していませんでした。

このような儲けがより大きい運営者に対する一般的なイメージを弱めることで、すなわち、外圧がかかると自らのビジネスモデルを損なうほどの無謀な戦術を展開する（例：身代金の支払いが済んでいる被害者を再度投稿する）運営者が存在するという事実を示すことで、最終的に取引内容を守らないランサムウェアの運営者への送金をやめるよう、組織への後押しとなったことは、望ましい結果であったと思われます。

オペレーションクロノスの影響を完全に定量的に把握することは、身代金の支払いに関する完全なデータセットがないため不可能と思われます。本節冒頭で述べたように、2024年のリークサイトの被害者数は、市場シェアに関係なく、2つのRaaSプログラム（ALPH-Vを含む）のテイクダウンを実行したとしても防ぐことのできない回復力を示すものです。しかし、法執行機関はこうしたプレイヤーを排除することで、ランサムウェアの作成、拡散、メンテナンスの責任を、経験が浅く、理論上能力の低い運営者に押し付けることになります。

観察されたアフィリエイトプログラムの多くが、オープンソースとして入手可能で再利用されたコードベースを活用していることから[136]、脅威アクター側がイノベーション不足に陥っている状況が期待されます。その結果、ネットワーク防御チームやアンチウイルスベンダーに時間的余裕が生まれ、これらの古いコードベースを解読するためのより確実な手段の作成、またはランサムウェアの発動が成功してしまった後に適用可能で包括的な修正プランの作成に着手できることも期待されます。

134 アナリスト注記：これはオペレーションクロノスの調査結果によって裏付けられた。指定された身代金を支払った組織のデータが引き続きLockBitのバックエンドサーバー上に置かれていることが判明した。。参照先: 'International investigation disrupts the world' s most harmful cyber crime group' ,UK NCA, https://www.nationalcrimeagency.gov.uk/news/nca-leads-international-investigation-targeting-worlds-most-harmful-ransomware-group (20th February 2024)

135 'LockBit Admins Tease a New Ransomware Version' ,Infosecurity Magazine, https://www.infosecurity-magazine.com/news/lockbit-admins-tease-a-new/ (20thDecember 2024)

136 アナリスト注記：RaaSプログラムには、Babuk、LockBit 3.0、Phobosなど、古いコードベースが数多く流通している

セクション 5

濁った海

敵対国側で広まっている状況をコントロール、支配、または混乱させるために、キャンペーンやテクニックを活用する戦略が例年以上に広まりました。これらの活動は、誤情報とサイバーに依存した偽情報の組み合わせによって行われます[137]。

脅威インテリジェンスアナリストにとって、このような悪意のあるキャンペーンで課題の1つとなるのがアトリビューション部分の調査です。脅威アクターは、ソーシャルメディアのサードパーティがホストするインフラを使用して意図的に偽アカウントまたはボットアカウントに隠れて活動しています。このため、最終的に得られた証拠だけでは活動の発信元を適切に特定できない場合があります。

「海を濁す」という行為は、20年近く前の歴史的な傾向であり[138,139,140]、関与する脅威アクターは、敵対国側の拡大意欲（またはその欠如）とソーシャルメディアの可変性の両方を、これらのキャンペーンを展開するための最善の方法を決定する変数として活用しながら、時間をかけてそのテクニックを学習し、適応させてきました。2024年には、このような従来の脅威アクターに特定の活動を実施するための好機（すなわち、地政学的に分断された世界を背景に行われる選挙や複数の国際的なイベント）が数度にわたり提供され、採用されるアプローチや手法の多様性とともに、このような戦略の拡散を増大させることにつながりました。

137 アナリスト注記：一般的に、誤情報とは、判断を誤った個人が悪意なく共有する正しくない情報を指し、これに対し偽情報とは、意図的に聴衆を惑わす目的で共有される虚偽の情報を指す。大きく分類すると、この種の活動は、サイバーによって有効になるもの（例えば、ソーシャルメディアなどのデジタルチャネルを活用した従来のプロパガンダ手法）と、サイバーに依存するもの（ネットワーク侵入など）に分けられる。PwCが追跡している活動の多くは、サイバーに依存したキャンペーンに関するものである。

138 'The Russian Hybrid Warfare: Case of Estonia' ,The Foreign Policy Council, https://foreignpolicycouncilcom.wordpress.com/2021/11/04/the-russian-hybrid-warfare-case-of-estonia/ (4th November 2021)

139 'Treasury Sanctions Iran Cyber Actors for Attempting to Influence the 2020 U.S. Presidential Election' ,US Department of the Treasury, https://home.treasury.gov/news/press-releases/jy0494 (18th November 2021)

140 'Pro-PRC DRAGONBRIDGE Influence Campaign Leverages New TTPs to Aggressively Target U.S. Interests,Including Midterm Elections',Mandiant, https://www.mandiant.com/resources/blog/prc-dragonbridge-influenceelections (26th October 2022)

従来の誤情報は、ロシアやイランを拠点とする脅威アクターによる例年どおりの継続的な活動で観察されていました。

- DoppleGangerとして知られる、ロシアを拠点とした活動が活発な脅威アクターは、2022年5月から活動を開始していますが、2024年にかけて多数のキャンペーンを展開していたことが判明し、最終的に欧米諸国の政府による制裁とテイクダウンにつながりました[141]。
- イランを拠点とする脅威アクターであるYellow Dev 19（別名 Emennet Pasargad、Cotton Sandstorm）は、パリ五輪期間中、イスラエル選手団にまつわる誤情報を拡散していたことが判明しました[142]。フランスの極右運動を装った偽の脅迫的な投稿は、イスラエル国民を標的と思わせ、心理的に悪影響を及ぼすことを意図したものであった可能性が高いと見られます。
  - Yellow Dev 19が心理的に悪影響を及ぼす目的で誤情報を利用した例はこれにとどまりません。2024年10月にこの脅威アクターはハイファ港で働くイスラエル人労働者に港湾インフラをハッキングしたとする内容のSMSメッセージを送信しました。このメッセージは、港がまもなくミサイルの標的になるためハイファ港湾の労働者に避難するよう警告していました[143]。

図表19-ハイファ港湾の労働者に対するミサイル攻撃を警告するYellow Dev 19が送信した脅迫メッセージ

141 'Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere' ,USDOJ, https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence (4th September 2024)

142 'Yellow Dev 19' s Olympic influence campaign' ,PwC Threat Intelligence,CTO-SRT-20240730-01A

143 'Yellow Dev 19 influence campaign goes ballistic' ,PwC Threat Intelligence,CTO-QRT-20241029-01A

2024年は「選挙の年」とよく言われるほど、多くの国で多くの選挙が（場合によっては予定外の選挙も）行われましたが[144]、その多くで選挙期間中に誤情報の拡散が行われました。誤情報の拡散と悪意のある影響力の行使を組み合わせることで、米国の選挙結果に影響を与えようというすでに詳細に記録された事例[145,146]以外にも、主流となっている考え方に影響を与え、結果を左右しようとする試みは年間を通じて数多く見られました。

- ジョージアの選挙期間中、NATO諸国がロシアに対する第2戦線を開く手段として同国を利用しようとしているとして、ジョージア国民を説得しようとする複数の主張がソーシャルメディアを通じて広まりました[147]。
- モルドバでは、偽情報が拡散されただけでなく[148]、有権者に対する詐欺も積極的に試みられました[149]。
- 1月に行われた台湾の選挙では、ソーシャルメディアで多数の偽情報が拡散されましたが、これは中国を拠点とする脅威アクターによるものだったことが報告されています[150]。トピックには、生物兵器分野での米台協力、米国から輸入した豚肉の汚染、ディープフェイク動画や選挙候補者の政治的中傷などが含まれていました[151,152]。
- ルーマニアの大統領選挙は、選挙資金調達の不正と並んで、選挙結果に影響を及ぼすことを目的とした悪質なサイバー上の攻撃活動の展開に関する十分な証拠が見つかったため、憲法裁判所によって無効とされました[153]。

プロキシネットワークと難読化ネットワークの利用については、中国と北朝鮮を拠点とする脅威アクターが2024年の活動を難読化する目的で、商用と特注のORBネットワークとプロキシネットワークを利用しているとすでに述べたとおりです。しかし、このような活動を行うのはこれらの脅威アクターだけでなく、その範囲は大きく広がり、2024年にはピークに達します。

- Grey Anqa（別名 NSO Group）やGrey Mazzikim（別名 Candiru）などの商用スパイウェアのクオーターマスターは、顧客ベースに登録された身元と拠点の保護を目的とするビジネスモデルを持っています。Pegasusのような技術的水準が高い製品[154]をゼロクリックエクスプロイトやワンクリックエクスプロイトと併用すると、顧客は（理論上）匿名のまま、標的に対して情報収集を行うことができます。
  - 2024年に実施した調査を通じて、これらの顧客の活動を観察し、匿名化ネットワークがどのように機能しているかについての知見を得ました[155]。

144 'The 2024 election cyber threat stress test' ,PwC Threat Intelligence,CTO-SIB-20240520-01A

145 'FBI links video falsely depicting voter fraud in Georgia to 'Russian influence actors' ,Associated Press, https://apnews.com/article/fbi-russia-georgia-frauddisinformation-eebea4ab200682ccd3e97fb9f164e6ca (1st November 2024)

146 'Sanctions in Response to Attempted Iranian and Russian Interference in U.S. General Election' ,USDOJ, https://www.state.gov/sanctions-in-response-toattempted-iranian-and-russian-interference-in-u-s-general-election/ (31st December 2024)

147 '"Global War Party," "Second Front," "Unprecedented election meddling" from the West, and other propaganda narratives dominating Georgian information space in the run-up to the key 2024 elections' ,EDMO, https://edmo.eu/publications/global-war-party-second-front-unprecedented-election-meddling-fromthe-west-and-other-propaganda-narratives-dominating-georgian-information-spa/ (25th October 2024)

148 'Moldova' s pro-Western president wins reelection in runoff shaken by alleged Russian meddling' ,PBS, https://www.pbs.org/newshour/world/moldovas-prowestern-president-wins-reelection-in-runoff-shaken-by-alleged-russian-meddling (3rd November 2024)

149 'Moldovans are voting in a pivotal presidential runoff. But voter fraud threatens its democracy' ,Associated Press, https://apnews.com/article/moldovademocracy-election-russia-disinformation-corruption-0a23e330da7121dbc34b085fc5d0d8ad (2nd November 2024)

150 'DPP wins historic third presidential term' ,PwC Threat Intelligence,CTO-SIB-20240125-01A

151 'China bombards Taiwan with fake news ahead of election' ,Politico, https://www.politico.eu/article/china-bombards-taiwan-with-fakenews-ahead-of-election (10th January 2024)

152 'As Taiwan voted, Beijing spammed AI avatars, faked paternity tests and 'leaked' documents' , Australian Strategic Policy Institute, https://www.aspistrategist.org.au/as-taiwan-voted-beijing-spammed-ai-avatars-faked-paternity-tests-and-leaked-fake-documents/ (18th January 2024)

153 'The Romanian 2024 Election Annulment: Addressing Emerging Threats to Electoral Integrity' ,IEFS, https://www.ifes.org/publications/romanian-2024-electionannulment-addressing-emerging-threats-electoral-integrity (20th December 2024)

154 'Spyware among us' ,PwC Threat Intelligence,CTO-SIB-20231201-02A

155 'Uncovering Grey Anqa' ,PwC Threat Intelligence,CTO-TIB-20240903-01A

- 昨年の「2023年を振り返る」[156]では、スパイウェアの能力に対する社会的な監視の目が年々厳しくなっていくだろうと予想されていました。この予想はある程度の範囲においては、おおむね真実だったようです。深い分析や詳細な情報を含む出版物[157]に加え、裁判でもこれらのクオーターマスターが引き続き注目を集めていました[158]。ただし、特に年末にかけては、訴訟や裁判の取下げや却下を示唆する兆候がいくつか見られ[159,160]、スパイウェア問題はサイバーセキュリティのニュースの中で後回しにされるようになりました。

■ 2024年にマイクロソフトが報告した、ロシアを拠点とする脅威アクターBlue Python（別名 Secret Blizzard）が、パキスタンを拠点とし、White Dev 55と密接な関係にある脅威アクターStorm-0156（別名 Operation SideCopy）のインフラを利用し、彼らになりすましてアジア太平洋地域で活動を行ったという珍しい事例があります[161]。

- この手口は、Blue Pythonがウクライナに侵入した際にも繰り返されました。マイクロソフトが追跡している犯罪組織として知られるStorm-1919になりすまして被害者の情報を収集し、次の段階のペイロードをダウンロードするために、特定のAmadeyボットの亜種を使用していました[162]。

（2023年に初めて使用された後）2024年に流行した新たな誤情報の形態として、西側諸国の政府から公表された情報が敵対国によってその影響力を削がれる例があります。

■ 米国政府機関と民間業界のパートナーが共同で、中国を拠点とする脅威アクターRed Dev 49（別名 Volt Typhoon）が2023年から2024年にかけて米国内の重要インフラを狙ったサイバー侵入を行ったとする複数の報告書を発表しました[163]。当初の発表後、中国メディアはこれに反論したにとどまらず、Volt Typhoonが実際には中国を巻き込むために米国がでっち上げたものであるとの主張を積極的に試みました[164]。

■ これまで、企業諜報や情報収集の告発に対しては、メディアによる声明やプレスリリースのほか、政治家によるソーシャルメディア上での批判が典型的な反応でした。しかし、Volt Typhoonのケースでは、中国国家コンピューターウイルス緊急対応センター（CVERC）が公式調査を実施し、3件の報告書が発表されました。これらの報告書のシリーズ名の下には次のようなタイトルが付けられています。〈嘘をつくな〉

■ これらの報告書の意義は、そのタイトルが示すとおり、単にアトリビューションに関する主張を積極的に濁らせるだけでなく、「Red Dev 49」が実際には米国政府が主導した作戦行動であるかのように筋書きを変えようとすることにあります。

■ これらの報告書はそれまでの否定とは異なり、標準的な脅威情報報告書の形式を用いた技術的に詳細で長々とした内容です。このような形式をとる目的は、中国と西側諸国の一般市民に向けてその内容を正当化することにあると考えられますが、ほとんどの市民は主張自体を分析するほどの専門知識を備えていません。

156 'Cyber Threats 2023: A Year in Retrospect' ,PwC Threat Intelligence,CTO-YIR-20240624-01A

157 'Global: A Web of Surveillance–Unravelling a murky network of spyware exports to Indonesia' ,Amnesty International, https://www.amnesty.org/en/latest/news/2024/05/unravelling-a-murky-network-of-spyware-exports-to-indonesia/ (2nd May 2024)

158 'US judge finds Pegasus spyware maker liable over WhatsApp hack' ,The Guardian, https://www.theguardian.com/technology/2024/dec/20/whatsapppegasus-spyware-nso-group-hacking (20th December 2024)

159 'Thai court dismisses activist' s spyware suit' ,The Bangkok Post, https://www.bangkokpost.com/thailand/general/2907406/thai-court-dismisses-activistsspyware-suit (23rd November 2024)

160 'Apple seeks to drop its lawsuit against Israeli spyware pioneer NSO' ,Washington Post, https://www.washingtonpost.com/technology/2024/09/13/applelawsuit-nso-pegasus-spyware/ (13th September 2024)

161 'Frequent freeloader part I: Secret Blizzard compromising Storm-0156 infrastructure for espionage' ,Microsoft, https://www.microsoft.com/en-us/security/blog/2024/12/04/frequent-freeloader-part-i-secret-blizzard-compromising-storm-0156-infrastructure-for-espionage/

162 'Frequent freeloader part II: Russian actor Secret Blizzard using tools of other groups to attack Ukraine' ,Microsoft, https://www.microsoft.com/en-us/security/blog/2024/12/11/frequent-freeloader-part-ii-russian-actor-secret-blizzard-using-tools-of-other-groups-to-attack-ukraine/ (11th December 2024)

163 'Volt Typhoon' ,PwC Threat Intelligence, CTO-QRT-20230525-01A

164 'Who is Volt Typhoon? A State-sponsored Actor? Or Dark Power?' ,Natto Thoughts, https://nattothoughts.substack.com/p/who-is-volt-typhoon-a-statesponsored (12th June 2024)

- 報告書内で使われている表現もほぼ間違いなく意図的に、社会的にも学術的にも激しく議論が交わされている米国における政府不信をめぐる現代のネット上の言説に寄りかかったものです。
- 報告書の技術的な形式と意図的な表現を組み合わせることで、米国の共同勧告報告書に対するこれまでにない反論の形態が生み出されています。CVERCの報告書の意図は、単に否定するだけでなく、最初に提供された報告書や責任のある機関に対する信頼を明らかに低下させることであり、これはエスカレートする非難の応酬であると評価しています。
- 2025年における米中関係の行方はまだ定かでありません。しかし、中国を拠点とする脅威アクターと関係があると評価される活動については、米政府機関が共同勧告を発表する傾向が強まっています。このような情報公開は今後も続き、2025年も2024年と同じレベルで米中の緊張が続けば、CVERCの報告書に記載されるような同様の反論が引き続き行われると現実的な確率で予測されます。

2024年には、ほとんどの社会で誤情報と偽情報の蔓延が当たり前のものとなりました。これは同年に実施された選挙の多さが一因であると思われますが、私たちの評価ではそれだけが要因ではありません。多くの民主主義国家では、政府機関への信頼が全般的に低下しています[165,166,167]。その原因は、過去の誤情報工作や偽情報工作、政府全体の不安定さ、近視眼的と思われる政策決定[168,169]のほか、人々の関わり方を根本的に変えてしまった新しいテクノロジーの出現が挙げられます。このような現状は、脅威アクターが悪用する手段を見つけ、さらに不信感を増大させるという循環的なスパイラルを生み出しています。このように、特定の人々の間では懐疑的な見方が強いため、CVERCのような出版物は5年前よりも確実に注目を集め、その影響力を増しています。

誤情報による工作活動は2025年も継続する可能性が高く、ソーシャルメディアプラットフォームは、脅威アクターが状況を混乱させる目的で民衆に対する工作活動の効果を最大化させるための主要な手段であり続けると見られます。また、情報公開と各国の関わり方は、公的なチャネルを通した短い形式の反論というこれまで受け入れられてきた方法に戻るのではなく、2024年に観察された形式に近くなると予想されます。

165 アナリスト注記：ピュー・リサーチ・センターの最新の世論調査の統計によると、政府への信頼度は2023年から「緩やかな上昇」を示し、政府全体で22%（その内訳として、民主党支持者が35%、共和党支持者が11%）となったが、引き続き驚異的な低さと評価されている（参照 'Public Trust in Government:1958-2024', Pew Research Center, https://www.pewresearch.org/politics/2024/06/24/public-trust-in-government-1958-2024/ (24th June 2024)）

166 'Trust and confidence in Britain's system of government at record low',National Centre for Social Research, https://natcen.ac.uk/news/trust-and confidencebritains-system-government-record-low (12th June 2024)

167 'In welche der folgenden Institutionen und Berufsgruppen haben Sie großes Vertrauen?', Statista,https://de.statista.com/statistik/daten/studie/1283706/umfrage/vertrauen-in-institutionen-in-deutschland/ (January 2024)

168 'German Chancellor Olaf Scholz loses confidence vote',BBC, https://www.bbc.com/news/articles/ckg36pp6dpyo (16th December 2024)

169 ''Macron's brutal dissolution of the Assemblée resulted in the dissolution of his majority'',Le Monde, https://www.lemonde.fr/en/politics/article/2024/07/01/macron-s-brutal-dissolution-of-the-assemblee-resulted-in-the-dissolution-of-his-majority_6676300_5.html (1st July 2024)

付属資料

付属資料A―手法

PwCは、年間を通じて、顧客や利害関係者、セキュリティ業界全体の専門家と協力し、情報要件の検証や改善を行いながら、独自の可視性、特注ツール、戦術、分析の取り組みを顧客向けの実用的な情報に変換しています。本報告書では、2024年に行われた分析の一部を抜粋しています。PwC独自の機能と商用ツールおよびオープンソースへのアクセスに加えて、インシデント対応ケースなどの業務においてはPwCグローバルネットワークのメンバーファームと緊密に連携しています。

推定に関する表現

推定的または確率的な表現（例：「可能性が高い」、「ほぼ確実」）の解釈はさまざまです。誤解を避けるため、本報告書では、可能性の表現および信頼性評価に言及する場合、次のような定性的な用語を使用しています。特に断りのない限り、当社の評価は統計分析を基にしたものではありません。

可能性の表現

定性的用語	対応する確率
程遠い、可能性が非常に低い	10% 未満
ありそうにない、可能性は低い	10-25%
現実的な確率	26-50%
有力、可能性が高い	51-75%
高確率	76-90%
ほぼ確実	91% 以上

信頼度

レベル	説明
低	基盤となる情報源は限られており、情報には多くの欠落部分があり、さらなる分析が不可能である
中	中程度の信頼性を持つ情報源（例：間接的な情報入手）が利用可能だが、情報には欠落部分があり、追加的な分析は不可能である
高	信頼性の高い情報源（例：情報への直接アクセス）が利用可能で十分な裏付けが取れており、徹底的な分析が可能である

付属資料B―脅威アクターのリファレンス

PwCは、27カ国以上のさまざまな脅威アクターを追跡し、その脅威アクターの拠点場所を示す色で構成された命名規則を採用しています。評価中の脅威には、地理的起源に基づいて「White」という色を指定しています。その他の色分けについては下表に示します。色に続いて、神話上の人物を割り当て、脅威アクターの固有の名前を確立します。既知の団体に帰属しない活動が観察された場合、開発と分析の継続を円滑に進めるためクラスターを「dev set」と呼びます。さらには、分析の結果、最終的なアトリビューション評価が得られた場合は、「dev set」を名前付きセットにアップグレードする場合もあります。PwCの調査と他社の調査との間でアトリビューションが重複する場合は、それぞれの脅威アクター名を記載しています。

北朝鮮を拠点（黒）	ロシアを拠点（青）	中国を拠点（赤）	イランを拠点（黄）
パレスチナ自治区を拠点とするグループ（ベージュ）	ファイブアイズを拠点（マゼンタ）	トルコを拠点（ターコイズ）	場所が不明、または複数国を拠点（グレー）

付属資料C―脅威アクターのリファレンス

本報告書において言及した全ての脅威アクターを以下に示します（本文または脚注で名前が挙げられています）。これらには、PwC脅威アクターの名前、既知の別名、脅威アクターの動機の評価が含まれます。

PwCサイバー脅威インテリジェンスチームの脅威アクターが既知の脅威アクターの別名を持っている場合がありますが、必ずしも名前が1対1に対応することを意味するものではありません。PwCは、可視性に基づいて活動の追跡、クラスター化、アトリビューションを行っています。

脅威アクター	別名	動機
Black Alicanto	Dangerous Password、LeeryTurtle、CryptoMimic、CryptoCore、Black Dev 1、Black Dev 2、COPERNICIUM、Sapphire Sleet、TA444、Stardust Chollima、Bluenoroff、Alluring Pisces、Genie Spider	サイバー犯罪
Black Dev 4	Contagious Interview、Famous Chollima、DEV#POPPER、Storm-1877	サイバー犯罪
Blue Athena	Fancy Bear、APT28、Pawn Storm、Sednit、STRONTIUM、TG-4127、Swallowtail、apt_tipsy_bear、Group 74、Crisis4、Sofacy、Tsar Team、SNAKEMACKEREL、IRON TWILIGHT、Forest Blizzard	諜報活動
Blue Callisto	Grey Pro、REUSE、Callisto Group、COLDRIVER、SEABORGIUM、Star Blizzard、BlueCharlie、TAG-53	諜報活動
Blue Dev 5	NOBELIUM、BoomBox、NobleBaron、Midnight Blizzard、BlueBravo	諜報活動
Blue Dev 8	該当なし	諜報活動
Blue Otso	Gamaredon、Gamaredon Group、Dancing Salome、Shuckworm、ACTINIUM、IRON TILDEN、Primitive Bear、Aqua Blizzard	諜報活動
Grey Anqa	NSO Group、Night Tsunami	諜報活動
Grey Hades	Gaza Hacker Team、Molerats、Gaza Cybergang	諜報活動
Grey Karkadann	AridViper、APT-C-23、Desert Falcon、Mantis	諜報活動
Grey Mazzikim	SOURGUM、Candiru	諜報活動
Red Dev 38	BackdoorDiplomacy、CloudComputating	諜報活動
Red Dev 49	Volt Typhoon、BRONZE SILHOUETTE、Vanguard Panda、VOLTZITE、Insidious Taurus、UNC3236、TAG-87	諜報活動

脅威アクター	別名	動機
Red Ishtar	Red Dev 26、Earth Preta、UNC4191、Stately Taurus、CeranaKeeper	諜報活動
Red Lich	Mustang Panda、BRONZE PRESIDENT、Red Delta、DarkPeony、Twill Typhoon	諜報活動
Red Vulture	APT25、Ke3chang、APT15、Vixen Panda、BRONZE PALACE、Mirage、Nylon Typhoon	諜報活動
White Dev 101	ALPHV-ng、ALPHV、BlackCat、Noberus	サイバー犯罪
White Dev 164	該当なし	サイバー犯罪
White Dev 183	plym0uth、Plymouth、Steal-C	サイバー犯罪
White Dev 184	UNC4393、Storm-1811	サイバー犯罪
White Dev 55	Operation Sidecopy	諜報活動
White Eloko	Volatile Cedar、Lebanese Cedar	諜報活動
White Enbarr	RansomHub	サイバー犯罪
White Janus	LockBit 3.0	サイバー犯罪
White Peryton	PLAY	サイバー犯罪
Yellow Dev 19	DEV-0198、ViceLeaker、Cotton Sandstorm、Emennet Pasargad、Ilia Net Gostar Atiq、Ilia Net Gostar Iranian Telecommunication and Electronic	妨害行為、諜報活動
Yellow Garuda	APT35、Charming Kitten、Newsbeef、Phosphorus、Mint Sandstorm、UNC788、ITG18、COBALT ILLUSION、TA453、Newscaster、APT42	諜報活動

pwc

日本のお問い合わせ先

PwC Japanグループ

www.pwc.com/jp/ja/contact.html

www.pwc.com/jp

本報告書は、PwCメンバーファームが2025年4月に発行した『Cyber Threats 2024:A Year in Retrospect』を翻訳したものです。翻訳には正確を期しておりますが、英語版と解釈の相違がある場合は、英語版に依拠してください。
オリジナル（英語版）はこちらからダウンロードできます。
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect.html

日本語版発刊年月：2025年7月　　管理番号：I202504-09