KELA

サイバー犯罪の現状：2024

新たな脅威と2025年の予測

2025年2月

エグゼクティブサマリー

2024年、サイバー脅威情勢はこれまで以上に複雑さを増しました。サイバー犯罪者らは他のグループと同盟を結んだり、サイバー犯罪者とハクティビスト、国家支援を受けたグループの区別が困難となるような手法を用いて攻撃手法を多様化しています。さらにアンダーグラウンドでは、マルウェア・アズ・ア・サービス（MaaS）や資格情報を売買するマーケットプレイスが強力な経済インフラの構築を後押しし、幅広い不正行為を支援しています。その一方で、AIが急速に普及したり、サプライチェーンにおける相互依存性が高まった結果、デジタル領域のアタックサービスが拡大し、新たな脆弱性が生まれています。またそうした状況を背景に、地政学的な緊張もサイバーリスクを増大する要因となっており、国家支援を受けたアクターらは、戦略的目標を実現する手段としてサイバー偵察活動を行うようになりました。ロシアや中国、イラン、北朝鮮をはじめとする国家の支援を受けたアクターは、現在も地政学的利益に沿った偵察活動や影響工作を展開しています。

本レポートでは、2024年に特に注目を集めた脅威を取り上げるとともに、2025年には脅威情勢がどのように進化してゆくのかをKELAが予測し、その対策をご提案します。本レポートが皆様にとって有用な知見になるとともに、進化するサイバー脅威情勢について理解を深める一助となることを願っております。KELAは、皆様が新たな脅威に先手を打ち、リスクを回避するために必要なインテリジェンスをご提供することを目標に掲げています。

David Carmiel

KELA CEO

持続型脅威の情報窃取マルウェア

- 情報窃取マルウェアは、ランサムウェア攻撃や偵察活動をはじめ、高度な攻撃の前段階で使用されています。
- 2024年、KELAは、世界中で430万台を超える端末が情報窃取マルウェアに感染していることを確認しました。また、それら端末に含まれていた資格情報（すなわち不正アクセスされた資格情報）の数は3億3,000万件超に上りました。
- KELAは、サイバー犯罪者が公開した資格情報リストに39億件もの資格情報が含まれていることを確認しました。それらのリストは、情報窃取マルウェアが収集したログをもとに作成されたものと思われます。
- 感染端末の75%超は、感染率トップ3にランクしている情報窃取マルウェア（Lumma、StealC、RedLine）に感染していました。
- 資格情報が窃取されたり、（窃取された資格情報が）その後さらなる悪事に使用された場合は、大規模な恐喝キャンペーンに発展する可能性があります。Snowflake社のインシデントは少なくとも165社に影響を及ぼしたとされていますが、同社のインシデントは、不正アクセスされた資格情報が発端となっていました。

ランサムウェア攻撃＆恐喝行為

- ランサムウェア攻撃と恐喝行為の件数は増加し、KELAが確認した被害組織の数は5,230超に上りました。
- 上記の被害組織に犯行声明を出したグループの数は、約100に上りました。そのうち、最も多く犯行声明を出していたのは「RansomHub」であり、520超の組織に対して犯行を主張していました。
- ランサムウェア攻撃を受けた組織を国別に分類すると、米国が全体の約半分を占めました。
- KELAが観察したところ、攻撃の種類はデータ窃取に移行しつつあるものの、データの暗号化も引き続き幅広く行われていました。また、サードパーティを標的とする攻撃に顕著に増加が見られました。
- サイバー犯罪者は、データを売買するマーケットプレイスを立ち上げたり、新たな収益化モデルを模索するなどして戦術を多様化させています。

侵入経路としての脆弱性

- 広範に使用されているプラットフォームの脆弱性が攻撃に悪用されており、パッチを迅速に適用することの重要性が浮き彫りとなりました。
- サイバー犯罪者のやり取りから、彼らがFortinet社の「FortiOS」や、「WordPress」のプラグイン、D-Link社のクラウドネットワークストレージデバイス、Microsoft Outlook、Windowsカーネルなどに存在する脆弱性に関心を持っていることがうかがえました。
- サイバー犯罪者が新たな脆弱性について議論している様子を観察したところ、大半は脆弱性が公表されて1カ月以内に話題に上っており、またその後数カ月にわたって議論が続いていることが確認されました。

注）本レポートでは、単独で活動しているサイバー犯罪者と、集団で活動しているサイバー犯罪者の両方を「グループ」と呼称しています。

政学的要因でハクティビストの活動が激化

- 200超のハクティビストグループが新たに出現し、3,500件以上の分散型サービス拒否（DDoS）攻撃を実行しました。
- ロシア・ウクライナ戦争やイスラエル・ハマス紛争などの重大な国際情勢が、重要な業界を標的とするハクティビストキャンペーンに影響を与えました。
- ハクティビストは、ランサムウェアや情報窃取マルウェアを活用したり、他のグループと同盟を結ぶなどして戦術を進化させていました。

国家支援を受けたアクターと他のサイバー犯罪者の境界線が曖昧に

- 米国や台湾、インドで行われた選挙などの重要なイベントが、国家支援を受けたサイバー攻撃のトリガーとなりました。またその一方で、パリオリンピックを標的にした影響工作キャンペーンも発生しました。
- これまでサイバー犯罪者が使用していたツール（ランサムウェアなど）が、地政学的な目的で使用される事例が増加しており、国家支援型の攻撃とサイバー犯罪の境界が曖昧になっています。

AIの悪用：新たなアタックサーフェス

- サイバー犯罪者は、大規模言語モデル（LLM）の弱点を悪用し、自らの目的を達成するためにAIを利用していました。
- AIを活用した脅威としては、ディープフェイクやバックドアを仕込んだAIモデルの使用、AI連携型プラットフォームを標的にした攻撃などが挙げられます。
- 人気の高いAIモデルのアカウント侵害が増加しており（ChatGPTアカウントの侵害件数は300万件、Geminiアカウントの侵害件数は17万4,000件）、より強力な防御策の必要性が浮き彫りとなりました。

目次

01

注目のサイバー脅威

情報窃取マルウェア

2024年のサイバー脅威情勢において、情報窃取マルウェアは特に重要な初期アクセスベクトルの1つとなりました。情報窃取マルウェアは資格情報や金融関連の情報、その他の機密データを収集するよう設計されており、いまやサイバー犯罪者の活動に不可欠な存在となっています。情報窃取マルウェアはマルウェア・アズ・ア・サービス（MaaS）のプラットフォームを通じて提供されており、そこではサイバー犯罪者が料金を支払い、情報窃取マルウェアのビルドやインフラを利用する仕組みになっています。

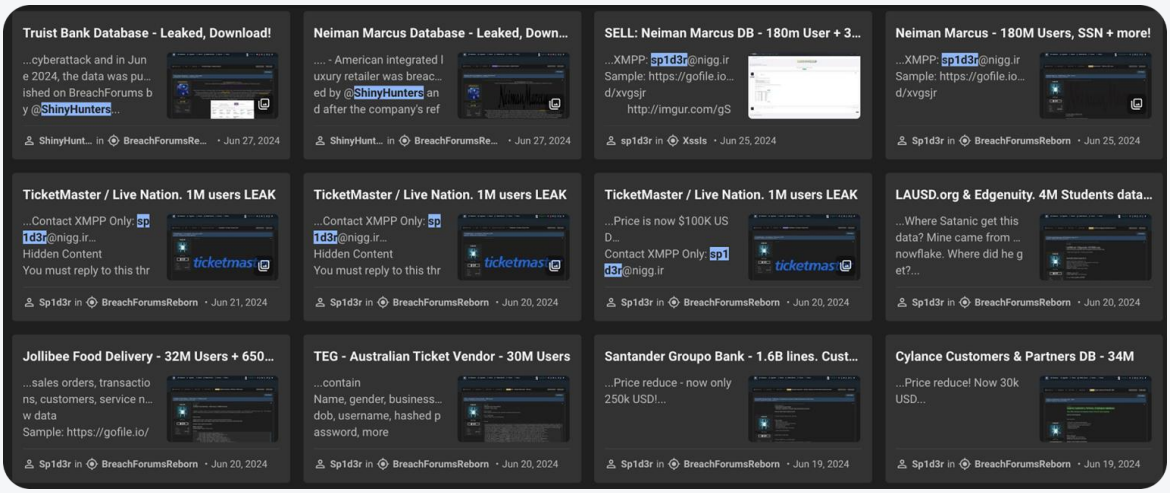
情報窃取マルウェアの魅力は、その効率の良さとスケーラビリティの高さにあります。例えば、サイバー犯罪者は情報窃取マルウェアを使用することで、個人や企業のアカウントを大量に侵害することが可能となります。また、アカウントの乗っ取りやデータ流出を直接的に行う手段として使用される一方で、ランサムウェア攻撃や偵察活動といった、より高度な攻撃の前段階にも使用されています。

マーケットプレイスやフォーラム、インスタントメッセージングサービス、その他様々なプラットフォームで構成されるサイバー犯罪エコシステムには、侵害された資格情報が大量に供給されており、情報窃取マルウェアの使用に拍車をかけています。

Snowflake社に対する攻撃

2024年に発生した情報窃取マルウェア関連の攻撃で最大規模

2024年4月中旬、サイバー犯罪グループ「UNC5537」が不正に入手した資格情報を悪用し、クラウドデータストレージプラットフォーム「Snowflake」の顧客アカウントに不正アクセスしました。その後初期アクセスとして悪用された資格情報を調査したところ、この資格情報は情報窃取マルウェアに窃取されたものであったことが判明しました。つまり、情報窃取マルウェアがSnowflake社顧客の資格情報を窃取し、UNC5537がその資格情報を入手して顧客アカウントにログインしたということです。またこの顧客アカウントでは、多要素認証（MFA）が有効になっていませんでした。 UNC5537は顧客アカウントにログインした後、独自のスクリプトを使用してSnowflakeインスタンスから情報を窃取しました。その後、この攻撃に関与した複数のアクターをKELAが追跡したところ、彼らが（Snowflakeインシデントの）被害企業のデータを販売したり、流出しようとしている動きが確認されました。この攻撃で影響を受けた企業は、少なくとも165社に上るとされています[1]。



Snowflakeインスタンスから窃取したデータを販売しようとしているサイバー犯罪者の投稿
（出典：KELAのプラットフォーム）

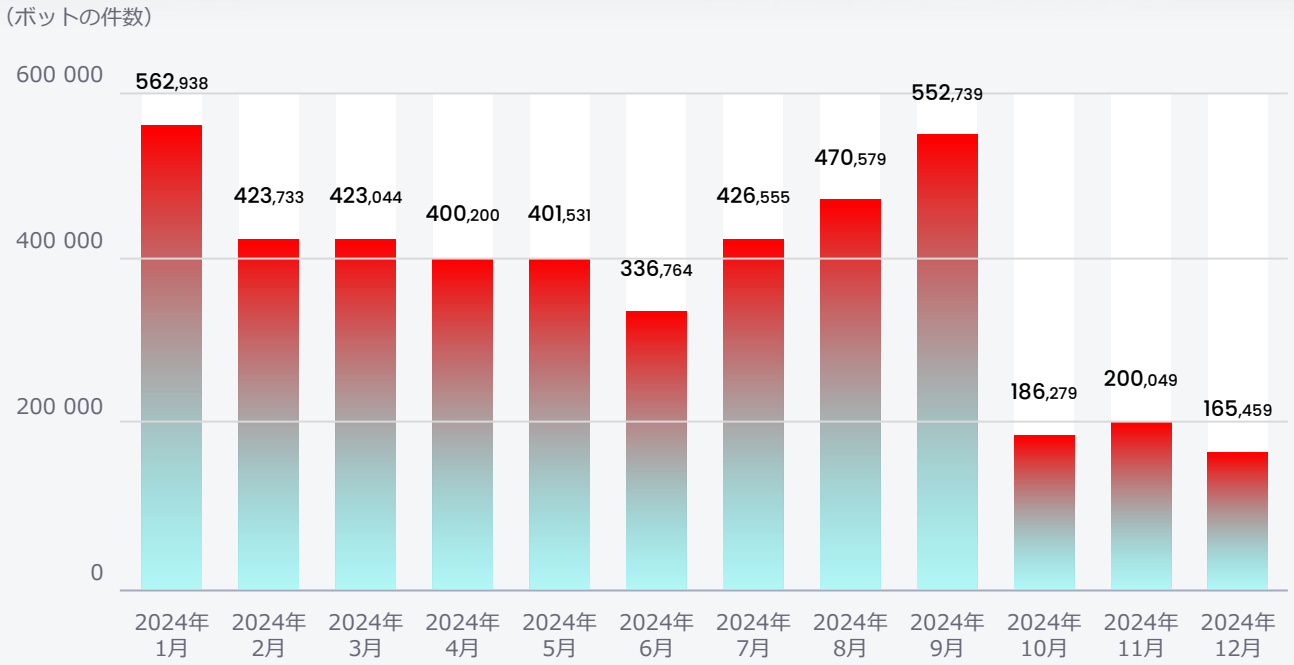
KELAが2024年に得た知見：

400万台超の端末が感染、感染率トップのマルウェアはLumma

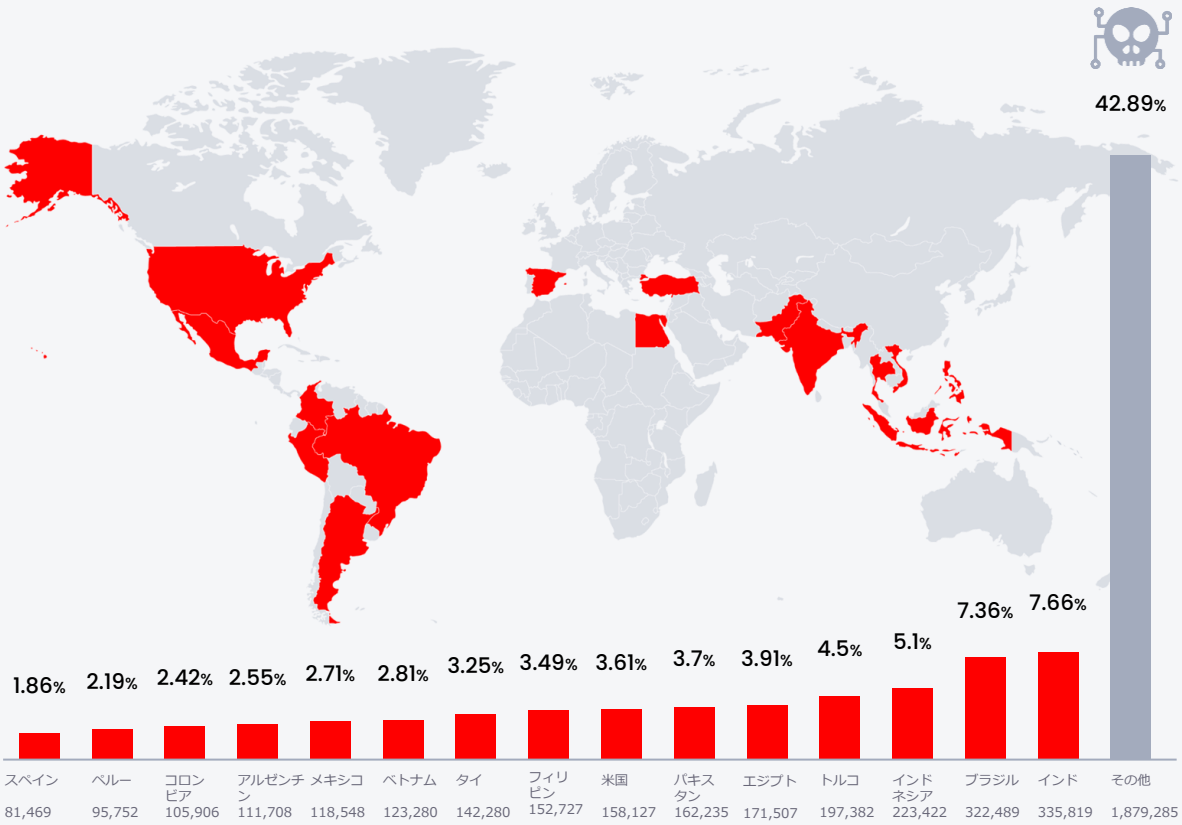
KELAのデータレイクによると、2024年に**情報窃取マルウェアに感染した端末は、世界中で少なくとも430万台、不正アクセスされた資格情報は3億3,000万件超に上り**、いずれの数字も2023年から微増しています。

[1] 出典

2024年に情報窃取マルウェアに感染した端末（ボット）の件数[2]



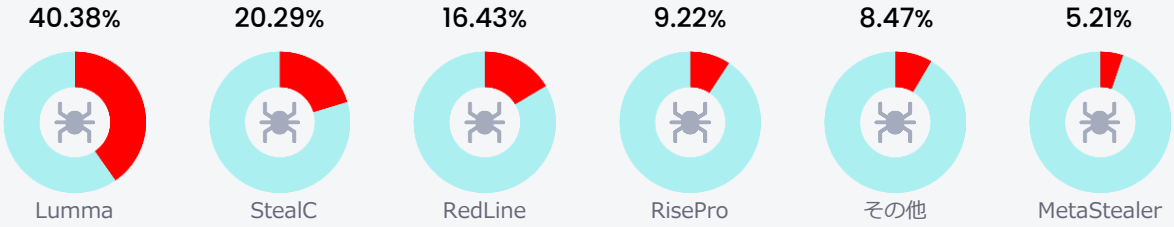
2024年に情報窃取マルウェアに感染した端末（ボット）の件数（国別）



[2] 2024年末に端末がマルウェアに感染していた場合、その端末のデータがサイバー犯罪ソースに投稿されるのは2025年初旬となる可能性がありますが、上記のグラフは感染日を基準に作成されています。そのため、このグラフでは2024年10～12月の感染件数に減少傾向が見られますが、実際の感染率はそれほど減少していない可能性があります。

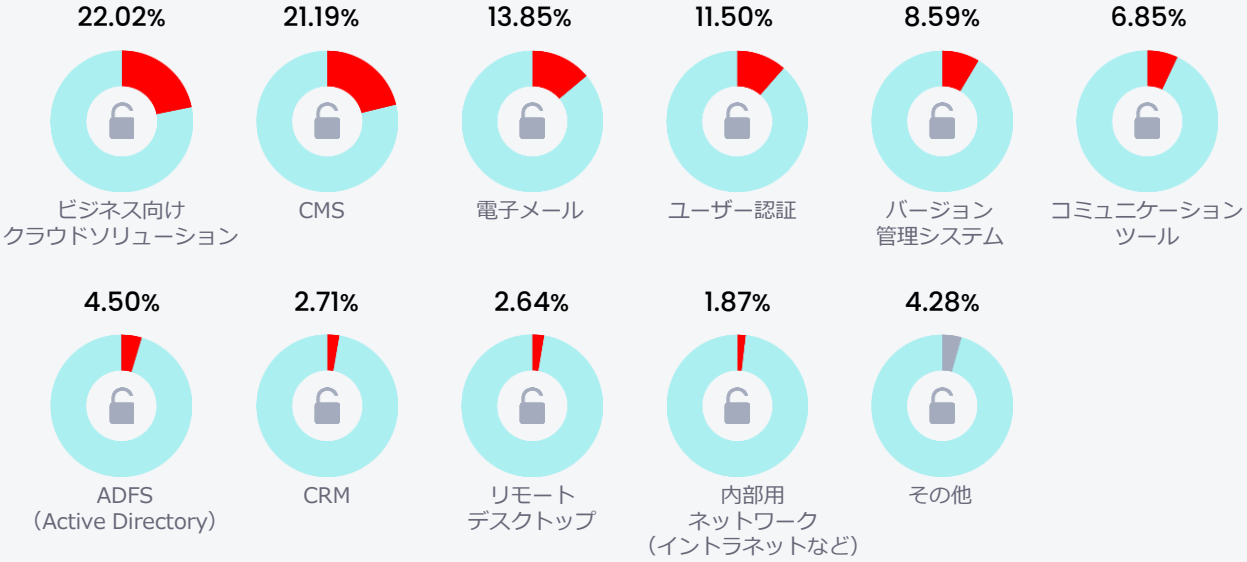
情報窃取マルウェアの感染率トップ3は、Lumma、StealC、RedLineです。またKELAのデータレイクに含まれていたボットのうち、75%超はそれら3亜種のいずれかに感染していました（ただし、 RedLineは2024年10月に解体されています）。

2024年に使用されていた情報窃取マルウェアのトップ 6

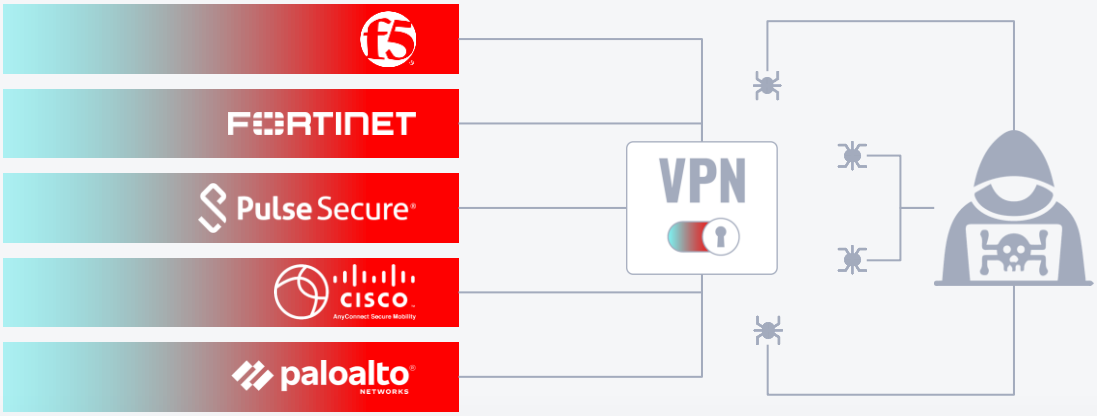


KELAのデータレイクに含まれていたボットの40 % （**ボットの台数：約170万件、資格情報の件数：750万件**）は、コンテンツ管理システム（CMS）や電子メール、ADFS、リモートデスクトップなど、企業で使用されている機密性の高いシステムの資格情報を保持していました。

機密性の高いサービスで使用されている資格情報の侵害状況（2024年）

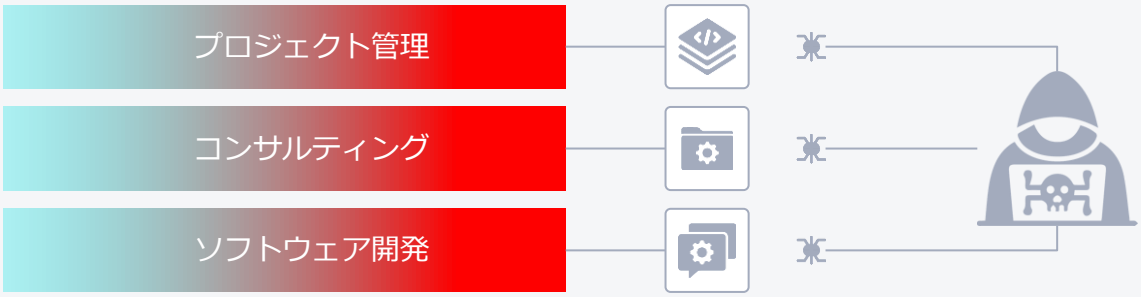


ランサムウェアグループやその他のサイバー犯罪者が狙う機密性の高い製品・サービスとして、VPNが挙げられます。**特に標的となっているVPNソリューションベンダーのトップ5は、以下のとおりです**[3]。



[3] 出典

感染端末のうち、ユーザーが企業の従業員であったものを対象にデータを分析し、それらデータを部門別に分類した結果、**被害を受けている部門のトップ3**は以下のとおりとなりました[4]。



KELAが分析したところ、**それらデータセットの大半（約65%）は、従業員が個人使用しているPCが出所となっていました**。つまり、従業員が個人使用のPCに業務用の資格情報を保存しており、それらPCが情報窃取マルウェアに感染して、データが窃取されていたということです。

またKELAは、情報窃取マルウェアに感染した端末から収集された資格情報の他に、**39億件もの資格情報がサイバー犯罪者の間で「ULPファイル」として共有されていることを確認しました**（サイバー犯罪者は、URL・ログインID・パスワードで構成された**資格情報のリスト**をULPファイルと呼称しています）。一般的に、ULPファイルは複数のサイバー犯罪者が窃取したデータの寄せ集めで構成されており、その出所は情報窃取マルウェアのログからサードパーティで発生したデータ侵害、フィッシング攻撃など多岐にわたります。しかしKELAは、大半のULPファイルは情報窃取マルウェアのログで構成されていると考えています。

KELAが予測する2025年 ：
情報窃取マルウェアは、依然として主要な初期アクセスベクトルに

2025年を迎え、情報窃取マルウェアの使用件数は引き続き増加の一途をたどるものと思われます。マルウェア・アズ・ア・サービス（MaaS）プラットフォームがさらに普及し、情報窃取マルウェアの機能が向上することで、初期アクセスの主要な手段としてこれまで以上に利用される可能性があります。しかしその一方で、法執行機関による取り締まり強化の影響も受けるものと思われます。

2024年は各国の法執行機関が連携し、RedLineのサプライチェーンで使用されていた主要なコンポーネントを解体するなど、当局による大規模な作戦が行われました。こうした取り締まりの動きは2025年も続けられ、強化されるものと思われます。また、取り締まりの対象はマルウェアの開発者だけではなく、アフィリエイトチームやマーケットプレイスのインフラ、彼らの活動を支援するその他のプラットフォームにも拡大する可能性があります。

そして法執行機関が取り締まりを行った場合、情報窃取マルウェアのエコシステムが一時的に機能停止に陥る可能性がありますが、マルウェア・アズ・ア・サービス形式で提供されている他の情報窃取マルウェアの活動が活発化する可能性があります。既存のマルウェアが解体されたことで生じた隙を好機ととらえて、新たな情報窃取マルウェアを操るサイバー犯罪者が活動する可能性があるからです。

---

[4] 情報窃取マルウェアを使用するサイバー犯罪者が増加し、アンダーグラウンドのマーケットで売買される資格情報が急増していることを受け、KELAは独自に収集した感染端末（ボット）の情報を用いて詳細な調査を行いました。KELAは、多数の企業がVPNを使用している状況をふまえ、情報窃取マルウェアが侵害した端末のデータセットのうち、VPNの資格情報が含まれているものを分析しました。分析対象となったボットは300台あり、2024年7月19日から2024年8月19日にかけて様々な種類の情報窃取マルウェアに感染していました。また、それらボットに含まれていた資格情報は10万件超に上りました。

対策

- **エンドポイント検知・対応（EDR）の強化：** 高度なEDRソリューションを導入し、情報窃取マルウェアの活動をリアルタイムに検知して隔離します。署名ベースの分析だけに頼らず、挙動分析に着眼した手法を採用します。
- **強力な資格情報管理：** すべてのアカウントに多要素認証（MFA）の導入を徹底し、高度な権限を持つアカウントの資格情報を定期的に更新することで、ログイン資格情報が窃取された場合の影響を最小限に抑えます。
- **定期的な脅威調査：**情報窃取マルウェアに感染した場合に見られる兆候をネットワーク内で能動的にチェックし、悪意のある既知のドメインやIPアドレスに対する異常なトラフィックの有無を確認します。
- **ネットワークのセグメント化を強化：**重要なシステムやデータを分離することで、不正入手した資格情報を悪用する攻撃者が水平移動できる範囲を限定します。
- **IDセキュリティを提供する脅威インテリジェンスプロバイダーとの連携：**サイバー脅威インテリジェンス（CTI）サービスを活用して、情報窃取マルウェアの亜種や戦術、自組織が属する業界で確認されたサイバー犯罪者の活動、自組織の資産（サードパーティリソースへのアクセスを含む）のエクスポージャーに関する最新情報を入手します。
- **電子メールのセキュリティ強化：**電子メールに高度なフィルタリングソリューションを導入し、フィッシングの試みを阻止します（フィッシングは、情報窃取マルウェアを配布する主要な手段として使用されています）。
- **従業員向け研修の拡充：**セキュリティ意識の向上に向けた活動の回数を増やし、各従業員がフィッシングメールの識別方法や、安全なパスワード管理の実施、不審な活動を発見した場合の迅速な報告、定められた手順に従った機密データの処理について理解を深められるようにします。また、未検証のソフトウェアをダウンロードした場合リスクについて説明し、許可されていない人物と業務用PCやノートパソコンを共有することを禁止します。
- **インシデント対応計画の策定：**特に封じ込めや分析、復旧ステップに着眼し、情報窃取マルウェアに感染した場合の対応プロセスが、常に実際の業務環境に即したものであることを確認します。

02

注目のサイバー脅威

ランサムウェア＆恐喝攻撃

2024年、法執行機関はLockBitに焦点をあてた「Operation Cronos」や[5]、ランサムウェアグループ「Radar」の解体をはじめ[6]、大規模な取り締まりを実施しましたが、ランサムウェアグループや恐喝グループは環境に適応して活動を継続しました。また2024年、KELAは60を超えるグループが新たに登場し、うち13が同年内に活動を停止したことを確認しました（注：本レポートで言及する「グループ」には個人も含まれている可能性があります）。つまり、サイバー犯罪者の間ではランサムウェア攻撃や恐喝攻撃の人気は高いものの、その活動を維持するには努力が求められるということです。また彼らの大半は、ランサムウェア・アズ・ア・サービス（RaaS）形式で活動を運営し、二重恐喝やサプライチェーン攻撃を採用しています。

2024年に登場した脅威グループをKELAが観察したところ、10を超えるグループがデータの窃取のみを行い、ランサムウェアを展開していませんでした。これは、現在も様々な組織を標的にデータの暗号化が行われている一方で、サイバー犯罪者の間ではデータ窃取に移行する動きが生まれていることを示唆しています。

また、サードパーティに対する侵害を通じて様々な組織の機密情報にアクセスすることができる、サプライチェーン攻撃も引き続き多発しています。サプライチェーン攻撃はサイバー犯罪者にとって非常に効率的であり、サードパーティ1社のアクセスを入手した後は、複数の攻撃を展開することが可能となります。

また2024年、KELAは、ランサムウェアグループが複数の収益モデルを採用し、新たなサービスを宣伝している事例を数件確認しました。例えばランサムウェアグループ「Meow」は、被害組織から窃取したデータを販売するマーケットを立ち上げていました。このマーケットでは、ランサムウェア攻撃の「ネイミング＆シェイミング」の一環で販売しているデータもありましたが、それ以外のデータも販売しており、また誰もが購入できるようになっていました。別のグループ「KillSec」は、あらゆる組織や個人のデータを収集する「OSINTサービス」を宣伝していました。信頼性の低いグループ「Funksec」も、自らのランサムウェアオペレーションに加え、他のサイバー犯罪者が窃取したデータを同グループのサイトで無料公開できるサービス「BlackZone」を宣伝していました。Funksecが提供しているBlackZoneについては、トラフィックを自らのサイトへ誘導し、知名度を上げるための戦略であると思われます。

---

[5] 出典

[6] 出典

注目を集めたランサムウェア攻撃

2024年は、重大なランサムウェア攻撃が複数発生し、様々な業界の組織に影響を及ぼすと同時に脅威情勢の進化を浮き彫りにしました。

- 2024年2月、「**UnitedHealth Group**」がランサムウェアグループ「Alphv（BlackCat）」の標的となりました。この攻撃で、Alphvは窃取した資格情報を悪用してUnitedHealth Group傘下の「Change Healthcare」のポータル「Citrix」にアクセスし、9日間にわたってデータを窃取した後、ランサムウェアを展開しました（不運なことに、Citrixには多要素認証（MFA）が設定されていなかったということです）。その後UnitedHealth Group は、封じ込めのためにネットワークの接続を遮断する事態に追い込まれました。なお、2024年4月には別のランサムウェアグループ「 RansomHub」もUnitedHealth Groupに対する犯行声明を出しており、この犯行声明については、UnitedHealth Groupに対する攻撃の実行犯であったサイバー犯罪者（Alphvのアフィリエイト）と協力関係を結んで出されたものと思われます。2024年4月末、 UnitedHealth Groupはメディア向けに公開した声明の中で、攻撃者に身代金を支払ったことを認めましたが、どちらのグループに身代金を支払ったのかについては明らかにしませんでした。

- 2024年5月、「**Evolve Bank & Trust**」は、データ侵害が発生して760万人分の個人情報が漏えいしたことを公表しました。同インシデントについてはLockBitが犯行声明を出しており、33 TB相当の機密情報を窃取したと主張しています。

- 2024年9月、「**Kawasaki Motors Europe**」がサイバー攻撃を受けたことを公表しました。このインシデントにより、同社は業務を停止するとともに、サーバーの隔離を余儀なくされる事態となりました。またその後、RansomHubがこのインシデントについて犯行声明を出し、487 GB相当のデータを窃取したと主張しました。

- 2024年12月、「**Cleo**」は、同社のソフトウェア（Harmony、VLTrader、LexiCom）に存在する脆弱性（CVE-2024-50623およびCVE-2024-55956）について、パッチの適用が徹底されておらず、活発に悪用されていることを報告しました。その数日後にはランサムウェアグループ「Clop」が、それら2件の脆弱性を悪用し、ゼロディエクスプロイトを使用して企業のネットワークに不正アクセスしたと主張しました。後にClopは、自らのブログに66の被害組織を掲載しましたが、それらの被害組織は上述の2件の脆弱性を悪用した攻撃に関連しているとされています。

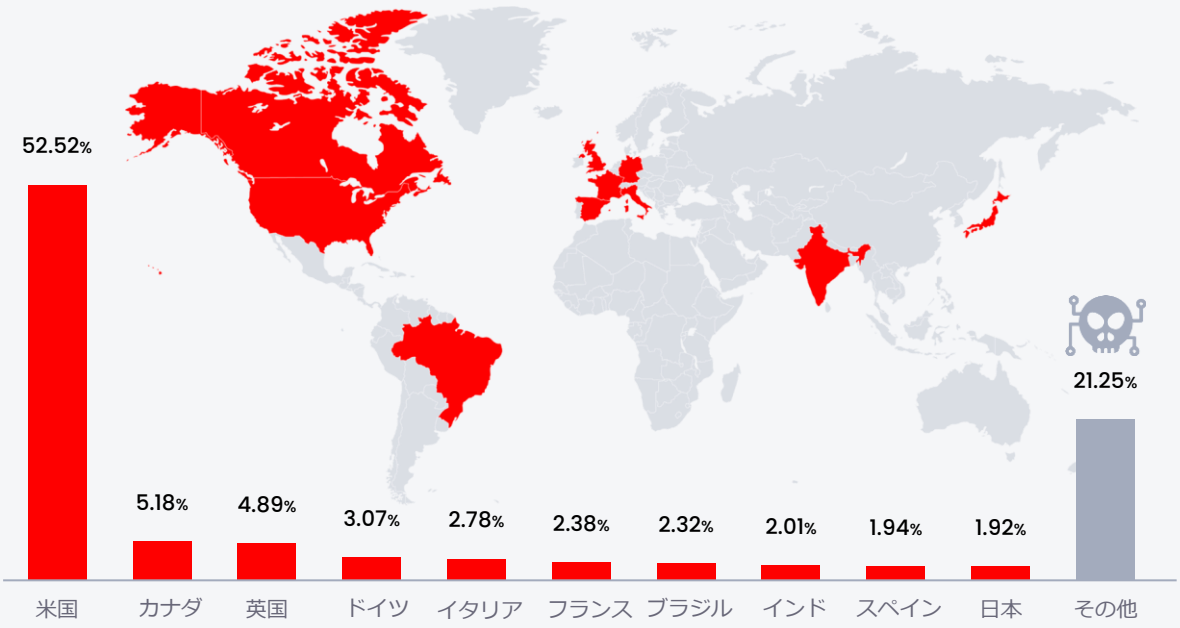
KELAが2024年に得た知見：

被害組織数は5,230、その大半は米国

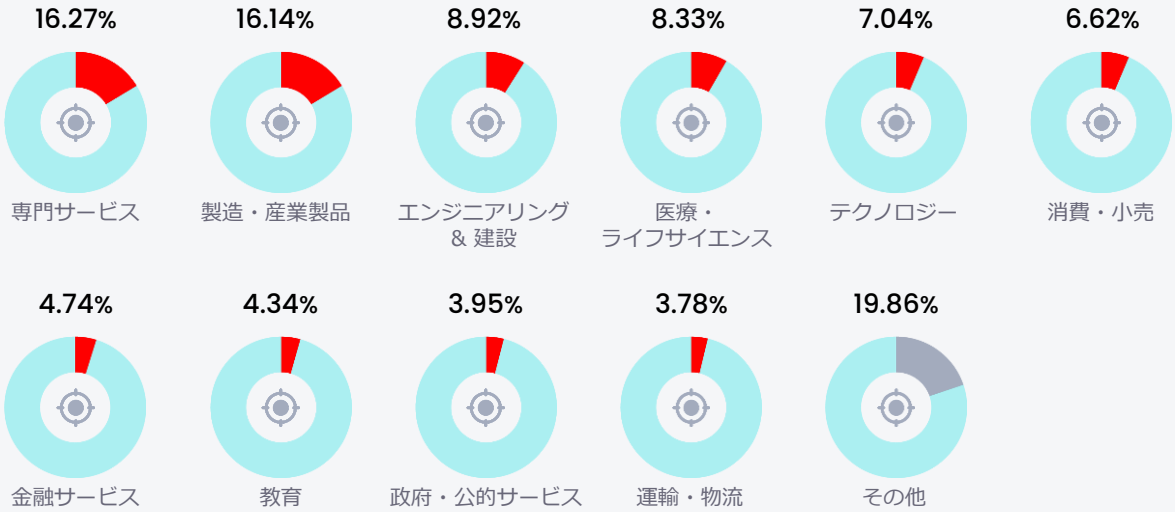
KELAが2024年に追跡した被害組織は5,230超に上り、2023年と比較して10.5%増加しました。**犯行声明を出したサイバー犯罪者(単独で活動しているサイバー犯罪者とグループの両方を含みます）は約100に上り、** 2023年と比較して28,5 %増加しました。

ランサムウェア攻撃を受けた組織の大半は米国であり、全体の半分超を占めていました。

被害組織数でトップ10にランクインした国々



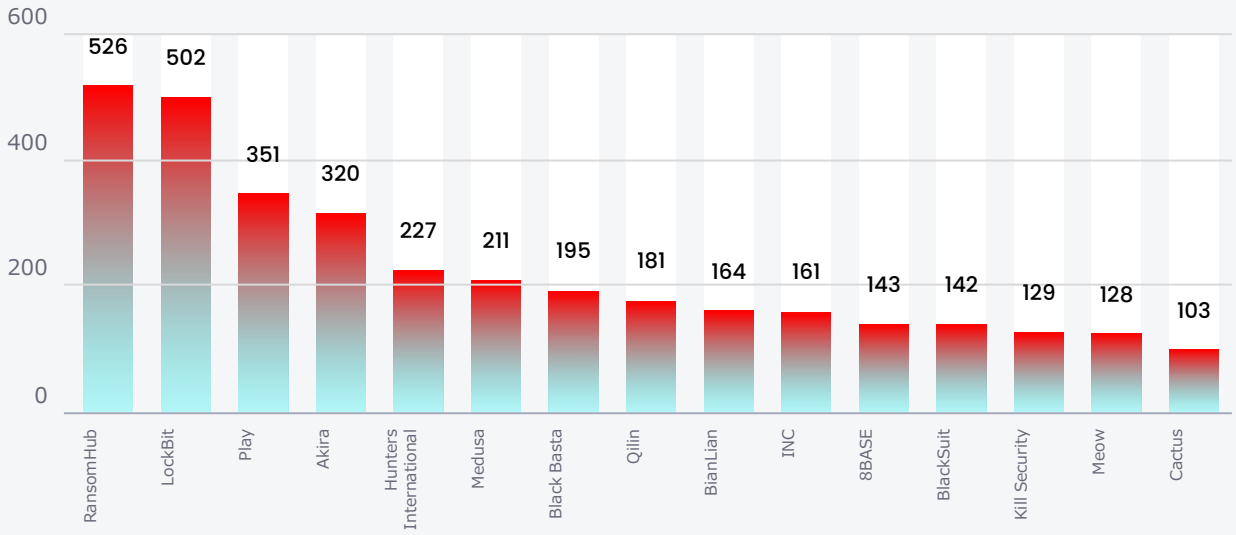
被害組織数でトップ10にランクインした業界



RansomHubは520件を超える犯行声明を出し、2024年に最も多く犯行声明を出したグループとなりました。2023年に犯行声明の件数で第1位であったLockBitは、2024年は約500件の犯行声明を出し、第2位となりました。

攻撃件数上位のランサムウェアグループ（トップ15）

（2024年の被害組織数）



2024年にランサムウェアグループによって犯行声明を出された被害組織のうち、2回以上犯行声明を出された組織の数は30超となりました。同じ組織に対する犯行声明が複数回出された理由については、複数のグループが協力体制をとって攻撃を実行したという可能性と、複数のグループが単独攻撃をたまたま同じ時期に実行したという可能性が考えられます。また後者の場合は、同じ初期アクセスベクトルを攻撃に使用した可能性があります。

ユースケース：

初期アクセスが売り出されてから、ランサムウェア攻撃に悪用されるまで

2024年10月3日、KELAは、脅威アクター「ProfessorKliq」が某米国企業のRDWebアクセスをオークション形式で売りに出したことを確認しました。同アクターの説明によると、この企業の収益は8,000万米ドルに上るということであり、入札開始価格は700米ドルに設定されていました。KELAは、ProfessorKliqが提供した被害組織の詳細情報をもとに、一般公開されている情報を調査し、高い確信をもって被害組織と思われる企業を特定しました。

その後の2024年10月24日、KELAは、この企業がランサムウェア「INTERLOCK」による被害を公表したことを確認しました。同社によると、INTERLOCKの攻撃が発生したのは2024年10月22日であったということから、ProfessorKliqが売りに出したRDWebアクセスをINTERLOCKのメンバーが購入し、攻撃に利用したという可能性が考えられます。

注目の脅威アクター

RansomHub

2024年に出した犯行声明： 520件超

「RansomHub」のランサムウェア・アズ・ア・サービス（RaaS）オペレーションは、遅くとも2024年2月から活動しています。その裏付けとして、2024年2月2日にフォーラム「RAMP」で、「koley」と名乗るアクターが同オペレーションの存在を初めて公表したことが確認されています。RansomHubのランサムウェアはGoとC++で記述されており、高速な暗号化機能を用いてWindowsやLinux、macOS、VMware ESXiなどの環境を攻撃しています。RansomHubのアフィリエイトは二重恐喝手法を採用しており、システムの暗号化とデータの流出を組み合わせて被害組織にプレッシャーを与え、身代金の支払いを強要しています。

2024年、RansomHubは急速に活動を拡大し、同年3月から7月にかけては毎月20～40、10月から11月にかけては毎月80超、12月には50超の組織を標的にしていました（いずれの数字もKELAのデータに基づきます）。RansomHubは、近年LockBitの攻撃件数を上回った初めてのグループであり、これも注目すべき点といえます。

通常、RansomHubのオペレーターは、スピアフィッシングやパスワードスプレー攻撃を行ったり、重大な脆弱性を悪用して初期アクセスを入手しています[8]。またこれまでには、Zerologonの脆弱性（CVE-2020-1472）やCitrix ADC／NetScalerの脆弱性（CVE-2023-3519）、FortiOSの脆弱性（CVE-2023-27997）、Java OpenWireモジュールの脆弱性（CVE-2023-46604）などを悪用していたことが確認されています。同グループは検知を回避するために、一見無害に見えるファイル名を使用したり、システムログを消去しています。さらに、Kaspersky社の合法ツール「TDSSKiller」を使用してEDRシステムの検知を無効にしたり、オープンソースのマルウェア「LaZagne」を使用して資格情報を窃取していることも確認されています[9]。被害組織のシステムの初期アクセスを入手した後は、ユーザーアカウントを新規に作成したり、無効化されたユーザーアカウントを再度有効にして永続性を確立しています。また、「Mimikatz」等のツールを使用して資格情報を収集し、特権昇格を行っています。データの流出方法は、ネットワークを侵害するアフィリエイトによって異なっています。RansomHubのランサムウェアは、楕円曲線暗号アルゴリズム「Curve 25519」を使用してデータを暗号化し、暗号化したファイルにランダムな拡張子を付けています。

8 出典

9 出典、出典

LockBit

2024年に出した犯行声明：500件超

LockBitは2019年に活動を開始し、2020年に自らのブログを立ち上げました。同グループは、活動当初から独自のランサムウェアの亜種を使用しており、現在は二重恐喝方式も採用しています。また2021年初旬からは、ランサムウェア・アズ・ア・サービス（RaaS）方式も採用して派手な宣伝活動を行い、ランサムウェアの管理パネルにユーザーフレンドリーなインターフェイスを導入して、アフィリエイトを引き付けています。

法執行機関が国際的な作戦「Operation Cronos」を実行した後、LockBitの犯行声明の件数は減少しました。しかし同グループは、ランサムウェアの開発やインフラの構築を継続しており、また2025年にはLockBit 4.0をリリース予定であることを公表しています。

LockBitのアフィリエイトは、主にフィッシングキャンペーンを展開したり、重大な脆弱性を悪用してシステムを侵害しています。悪用されている脆弱性の例としては、「CVE-2021-44228（Apache Log4j2）」や「CVE-2021-22986（F5 iControl REST）」、「CVE-2020-1472（NetLogon）」などが挙げられます（カッコ内は脆弱性が存在するサービスやコンポーネントです）。またネットワークに侵入するために、初期アクセスブローカー（IAB）のサービスを利用することもあります。そして標的のネットワーク内に侵入した後は、合法のリモートデスクトップアプリケーション（AnyDeskやTeamViewer、ScreenConnectなど）を悪用して、被害組織のネットワーク内を水平移動したり、システムを制御しています。LockBitのアフィリエイトは被害組織のデータを暗号化する前に、 LockBit独自のデータ抽出ツール「StealBit」を使用して機密データを抽出します。そして暗号化したファイルには、「.lockbit」という拡張子を付けます[10]。

[10] 出典

Play

2024年に出した犯行声明：350件超

ランサムウェアグループ「Play」は、遅くとも2022年6月から活動しています。同グループはアフィリエイトプログラムを運営しておらず、内部メンバーだけで活動していると考えられています。二重恐喝を戦術として採用しており、被害組織のシステムを暗号化する前に機密データを窃取しています。

Playは、有効なアカウントの資格情報や、インターネット経由で外部から利用可能なアプリケーションに存在する脆弱性をエントリポイントとして悪用しています。具体的には「FortiOS」に存在する脆弱性（CVE-2018-13379、CVE-2020-12812）や、「Microsoft Exchange」に存在する脆弱性（CVE-2022-41040、CVE-2022-41082）などが悪用されています。また同グループは、Active Directoryのクエリを実行してネットワークの詳細情報を特定し、PowerShellツールを使用してアンチウイルスソフトウェアを無効化し、ログを削除し、Microsoft Defenderを無効にしています。

Playは、水平移動やコマンド＆コントロール（C2）にCobalt StrikeやSystemBCを使用しています。また、特権昇格を行うためにセキュリティレベルの低い資格情報を取得することに注力しており、資格情報のダンプを度々利用して、ドメイン管理者のアクセスを入手しています。窃取したデータを流出する際には、まずデータを分割し、.RAR形式のファイルに圧縮してから転送しています。また、AES方式とRSA方式を組み合わせてデータを断続的に暗号化し、暗号化したファイルに「.play」という拡張子を付けています[11]。

[11] 出典

KELAが予測する2025年 ：

ランサムウェアグループはRaaSに依存しつつ、新たなサービスを活用

ランサムウェアグループの活動は減少する兆しを見せておらず、それどころか彼らは法執行機関の対策を回避するため、攻撃手法を進化させ続けています。またランサムウェア・アズ・ア・サービス（RaaS）についても、運営構造が分散化されており、収益性も高いことから今後さらに拡大することが予想されます。その一方で、法執行機関による解体作戦やその他の要因により、アフィリエイトがRaaSオペレーションを乗り換える動きも見られています。

サプライチェーン攻撃は、2025年も主要な戦術として使用される可能性が高いと思われます。その理由として、1. サプライチェーン攻撃の収益性が高いこと、2. 現代のテクノロジー業界がサードパーティのソフトウェアプロバイダーを通じて複数の組織にアクセスするようになった結果、同業界特有ともいえる脆弱性が生じていることが挙げられます。サイバー犯罪者はサプライチェーンを侵害することで、大規模なキャンペーンを実行するチャンスを得ることができます。2025年は恐喝行為に加え、サイバー犯罪者が（他のサイバー犯罪者と）協力体制をとったり、サイバー犯罪向けのサービスを利用するなどして、活動を多様化させる可能性があります。

対策

- **サプライチェーンのセキュリティ強化：**サードパーティベンダーに厳格なセキュリティ評価を実施し、最小限のアクセス付与を徹底するとともに、堅牢なセキュリティフレームワークに準拠するよう要請します。
- **ゼロトラストアーキテクチャの導入：**ゼロトラストモデルを導入し、リソースに対するアクセスを継続的に精査して制限することで、ランサムウェアが横展開する機会を低減します。
- **バックアップ戦略の強化：**重要なデータのバックアップを、オフライン環境で改変不可能な状態で保存・管理します。またその仕組みを定期的にテストし、ランサムウェア攻撃が発生した場合でも迅速に復旧できる体制を整えます。
- **XDRソリューションの導入：**XDRソリューションを活用して、エンドポイントやネットワーク、クラウド環境全体の脅威を監視し、相関性を分析して、RaaS（ランサムウェア・アズ・ア・サービス）の活動兆候を早期に検出します。
- **エンドポイント保護の強化：**ランサムウェアの挙動分析機能を備えた高度なウイルス対策ソリューションを活用し、既知および未知のランサムウェアの亜種をブロックします。
- **RaaSアフィリエイトの動向監視：**CTI（サイバー脅威インテリジェンス）プロバイダーと連携し、新たに出現したアフィリエイトや、自組織の業界を標的とするランサムウェアファミリーを特定して対応します。
- **最新パッチの適用・管理：**すべてのシステムやソフトウェアの脆弱性を迅速に修正し、特に重要なパッチを優先的に適用して、サプライチェーン攻撃に悪用されうるアタックサーフェスを最小化します。
- **データのセグメント化：**機密データを暗号化し、重要度の低いリソースと分離することで、ランサムウェア攻撃が発生した場合の影響を限定します。
- **ランサムウェア攻撃のシミュレーション：**定期的な演習やペネトレーションテストを実施し、自組織のランサムウェア対策を評価・改善します。

03

注目のサイバー脅威

脆弱性

2024年はサイバー脅威が進化する一方で、様々な重要システムに重大な脆弱性が存在することが明らかとなりました。またそれらの脆弱性は、脆弱性のPoCやエクスプロイトが共有・販売されるサイバー犯罪フォーラムでも広く話題に上っていました。サイバー犯罪者が標的とする脆弱性の中には、すでに公表されている脆弱性もあれば、ゼロディ脆弱性もあります。また共有・販売されているPoCやエクスプロイトも、すでに一般公開されているものもあれば、サイバー犯罪者が独自に開発したものもあります。

機密情報を共有する「ファイブアイズ」が2024年11月に発出したサイバーセキュリティ勧告には、ゼロディ脆弱性の悪用がこれまでよりも増加していることが記載されていました[12]。またこの勧告では、脆弱性が公表されて2年以内はその脆弱性を悪用した攻撃の成功率が高いこと、そしてベンダーがパッチやアップデートをリリースするにつれて、悪用件数が減少することが指摘されていました。

[12] 出典

特に悪用された脆弱性

前述の勧告では、2023年に特に悪用された脆弱性として以下が記載されていました[13]。

CVE-2023-3519：「Citrix NetScaler ADC」および「NetScaler Gateway」に影響を及ぼす脆弱性。認証されていないユーザーが、HTTP GETリクエストを介してスタックバッファオーバーフローを実行することが可能となります。

CVE-2023-4966：「Citrix NetScaler ADC」および「NetScaler Gateway」に影響を及ぼす脆弱性。セッショントークンの漏えいを引き起こすことが可能となります。

CVE-2023-20198：「Cisco IOS XE」のWeb UIに存在する脆弱性。認証されていないユーザーが、ローカルユーザーアカウントを作成することが可能となります。

CVE-2023-20273：「Cisco IOS XE」に影響を及ぼす脆弱性。CVE-2023-20198の悪用後に使用することで、特権昇格が可能となります。

CVE-2023-27997：「Fortinet」の「FortiOS」および「FortiProxy」のSSL-VPNに影響を及ぼす脆弱性。リモートの攻撃者が特定のリクエストを作成することで、任意のコードやコマンドを実行することが可能となります。

KELAが2024年に得た知見：

サイバー犯罪者の間で話題に上った脆弱性

KELAがサイバー犯罪フォーラムを観察したところ、2024年は以下の脆弱性が特に話題に上っていました[13]。

CVE-2024-21762：「FortiOS」に影響を及ぼす境界外書き込みの脆弱性。細工したリクエストを送信することで、不正なコードを実行することが可能となります。

CVE-2024-23113：「FortiOS」に影響を及ぼすフォーマット文字列の脆弱性。細工したパケットを介して、不正なコードを実行することが可能となります。

CVE-2024-3273：「D-Link」製デバイスに影響を及ぼす重大な脆弱性。リモートコマンドインジェクションを実行することが可能となります。

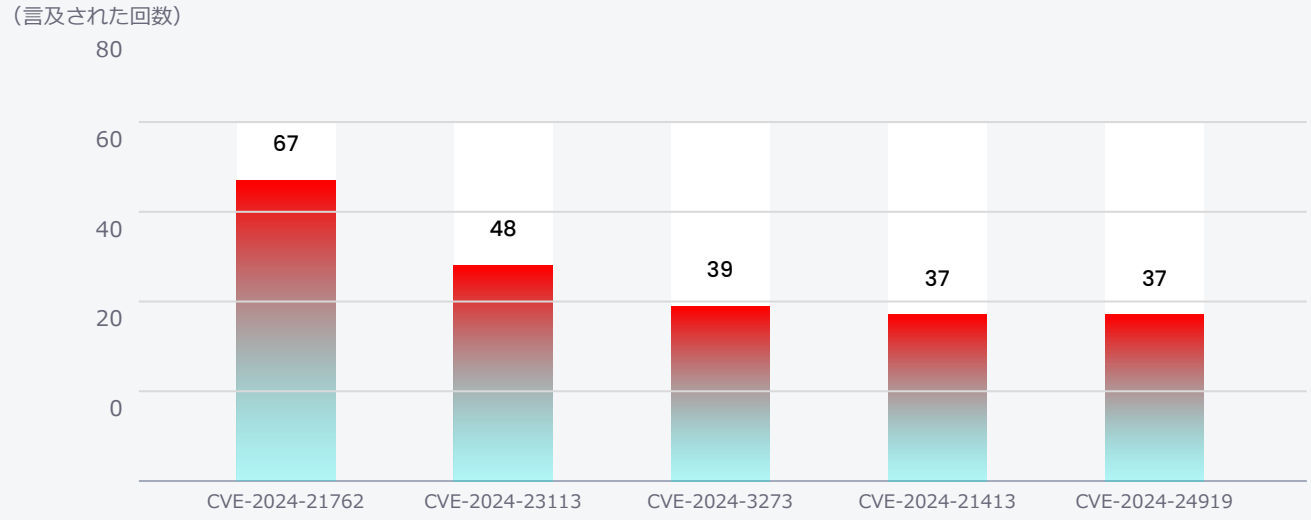
CVE-2024-21413：「Microsoft Outlook」に影響を及ぼすリモートコード実行の脆弱性

CVE-2024-24919：「Check Point Security Gateway」に影響を及ぼす脆弱性。リモートアクセスVPNまたはMobile Access Software Bladesが有効になっている場合、機密情報を読み取られる可能性があります。

[13] ただしこれまでのところ、「ファイブアイズ」からは「特に悪用された脆弱性のリスト」は公開されておりません。

サイバー犯罪フォーラムでは、一般公開されたPoCや独自のPoC、脆弱性を悪用する手法やコツ、その他最新情報が共有・販売されています。そしてフォーラムで話題に上っている脆弱性を分析すると、サイバー犯罪者が、広範に使用されているソフトウェアやハードウェアのシステムに関心を持ち続けていることがわかります。特に標的となっている製品としてはFortinet社の「FortiOS」、D-Link社のストレージ機器、Microsoft社の「Outlook」など、頻繁に議論に上っている脆弱性の種類としては、「リモートコード実行の脆弱性（RCE）」が挙げられます。

2024年にサイバー犯罪フォーラムで話題に上った脆弱性のトップ5



KELAはサイバー犯罪フォーラムで脆弱性に関する議論を監視し、詳細に分析しました。その結果、新たに公表された脆弱性をサイバー犯罪者がいかに素早く話題に取りあげ、PoCや悪用のコツを共有しているのかが明らかとなりました。サイバー犯罪フォーラムで特定の脆弱性が話題に上る場合、**その脆弱性が公表されてから話題に上るまでの期間は平均して1カ月以内でした**。また脆弱性の中には、公表された当日や数日以内に話題に上るものもあれば、話題に上るのが短期間にとどまらず、約1年が経過しても引き続き言及されているものもありました。

KELAが予測する2025年 ：
公表された脆弱性が、不正アクセスの主要なエントリポイントとして悪用される傾向が続く

2025年を迎え、サイバー攻撃はさらに高度になり、またその件数も引き続き増加するものと思われます。特に広範に使用されている製品（リモートアクセス用のソリューション、ファイヤウォールやスイッチのOS、電子メールのクライアントソフト、ネットワークのストレージ機器など）の脆弱性が公表後速やかに悪用されているという現状は、重要なシステムを監視し、常に最新のパッチを適用することの必要性を浮き彫りにしています。

サイバー犯罪フォーラムでは、新たな脆弱性が速やかに議論に上っており、またそれら脆弱性のエクスプロイトもスピーディに提供されています。この傾向は、サイバー犯罪者が新たな脆弱性を積極的に特定し、悪用していることを示唆しています。またその一方で、脆弱性に関する議論は継続する傾向があり、一部の脆弱性は最初に公表されてから数カ月、場合によっては1年近く経過した後も話題に上り、攻撃の対象となっています。公表された脆弱性への関心が継続しているということは、その脆弱性がサイバー犯罪者にとって有用であることを意味しています。そのため、組織は速やかに脆弱性を修正するだけではなく、サイバー犯罪者の間で関心を集めている脆弱性に対して優先的にパッチを当て、長期的な脅威を監視し、防御することが不可欠といえるでしょう。

対策

- **優先順位に基づいた脆弱性管理：** 脆弱性の重大度や、実際の悪用の有無に関する脅威インテリジェンスを活用した、リスクベースのパッチ適用プログラムを策定します。
- **パッチ適用のタイムライン短縮：** 重要なシステムのアップデートに必要な内部テストや承認プロセスを効率化し、パッチ適用までの時間を短縮します。
- **仮想パッチの導入：**侵入防御システム（IPS）やWebアプリケーションファイアウォール（WAF）を活用し、恒久的なパッチが適用されるまで攻撃からシステムを保護します。
- **脅威インテリジェンスの活用：**サイバー犯罪フォーラムや脆弱性データベースを定期的に監視し、サイバー犯罪者が積極的に悪用したり、議論に取りあげている脆弱性を特定して、迅速に対処します。
- **定期的なセキュリティ評価の実施：** 脆弱性スキャンやペネトレーションテストを実施し、公表されていない脆弱性が自組織のシステムに存在しないかをチェックします。また、脆弱性が発見された場合は速やかに修正します。
- **エンドポイントの強化：** セキュリティベースラインを設定し、使用していないサービスやポートを無効化して、アタックサーフェスを最小化します。
- **悪用の兆候監視：** 高度な検知ツールを導入し、既知の脆弱性が悪用される兆候となる、疑わしい挙動パターンを特定します。
- **ITチームの教育：** ITスタッフに対し、脆弱性の迅速な特定および修正についてのトレーニングを実施し、サイバー犯罪者の標的にされ続けている既知の脆弱性を長期的に監視することの重要性を周知します。
- **資産の継続的な可視化：** すべてのハードウェアやソフトウェアを追跡できる資産管理ツールを活用し、脆弱性管理から取り残されるシステムがないようにします。

04

注目のサイバー脅威

ハクティビスト

2024年は、ロシア・ウクライナ戦争やイスラエル・ハマス紛争を背景に、ハクティビストの活動が著しく活発化しました。特に親ロシア派や親パレスチナ派のグループは、欧米の政府機関や製造、エネルギー業界を攻撃しており、それらキャンペーンの中には国家の支援が疑われるものもありました。また、パリオリンピックなどを標的にしたインシデントも発生し、ハクティビストが世界的イベントを利用して自らのメッセージを拡散し、注目を集めようとしている様子が観察されました。その一方で「Red Eagle Crew」や「Holy League」、「October 7 Union」など、異なるハクティビストグループが同盟を結ぶ事例が増加している様子は、ハクティビストの脅威を緩和することが、これまで以上に困難になるであろうことを示唆しています。

一部のハクティビストグループは、DDoS（分散型サービス妨害）攻撃やウェブサイトの改ざんといった従来の手法に、ランサムウェアや情報窃取型マルウェアを用いた高度な攻撃を組み合わせてその戦術を進化させていました。その結果、技術スキルの低い攻撃者であっても、より複雑で多面的な攻撃を実行できるようになっています。

Telegramは広範なユーザーに使用されていることから、現在もハクティビストの間で人気の高いプラットフォームとなっています。しかし、Telegramのポリシーが変更されたことで彼らの間に懸念が広がり、「Discord」や「Signal」への移行を検討する動きも見られました[14]。

[14] 出典

ハクティビストが行った有名な攻撃

- イスラエル・ハマス紛争の最中、イスラエルの金融活動に混乱を引き起こすべく、同国の**決済サービスプロバイダー「Hyp」社のサービス「CreditGuard」**がDDoS攻撃の標的となりました。またその結果、攻撃者がDDoS攻撃を行った理由に世間の注目が集まりました。この攻撃は、ハクティビストグループ「Anonymous for Justice」の犯行とされており、また同グループについてはイランの情報機関とのつながりが疑われています[15]。
- 親パレスチナ派のグループ「BlackMeta」が、「**Internet Archive**」に対してDDoS攻撃を行ったとの犯行声明を出しました。そしてこの攻撃の結果、「Wayback Machine」をはじめとするサイトやその他のサービスがアクセス不可能となりました。この攻撃は、ハクティビストが紛争地域にとどまらず、より広範な領域に政治的メッセージを拡散するべく取り組んでいることを示しています。
- 「CyberVolk」は、ロシアの利益に相反する組織を標的に、他のグループとの同盟関係を利用して**ランサムウェアキャンペーン**を展開しました。このキャンペーンでは、CyberVolkは独自のペイロードを使用し、データ窃取と恐喝行為を併用することで、重要な業界に混乱をもたらしました[16]。これらのインシデントは、ハクティビストの戦術がこれまで以上に進化していることを示しています。

KELAが2024年に得た知見：

新たに出現したハクティビストグループは200超、DDoS攻撃の件数は3,500超

2024年、KELAが年間を通じて追跡した**新たなハクティビストグループは200超、特に活発に活動していたハクティビストグループは約300に上りました**。

KELAは、ハクティビストグループが活動するTelegramチャンネルのメッセージを詳しく分析し、彼らが出した犯行声明の件数を調査しました。分析対象となったチャンネル内のメッセージがすべて攻撃に関連しているわけではありません。しかし攻撃に関する投稿には、DDoS攻撃や改ざん、データ窃取などの攻撃を主張する際に、被害者のドメインや攻撃の事実を裏付けるURLに言及しているというパターンが見られます（Webサイトのアクセス可否を示したレポートを証拠として提供するなど）。Telegramの投稿に多数のドメインを掲載していたグループは、以下の通りです。

- 親インドネシア派の Ethersec Team Cyber
- 親ロシア派のNoName057(16)
- 親インドネシア派の Dunia Maya Team
- 親ロシア派のPeople's Cyber Army
- 親パレスチナ派のCyber Operations Alliance

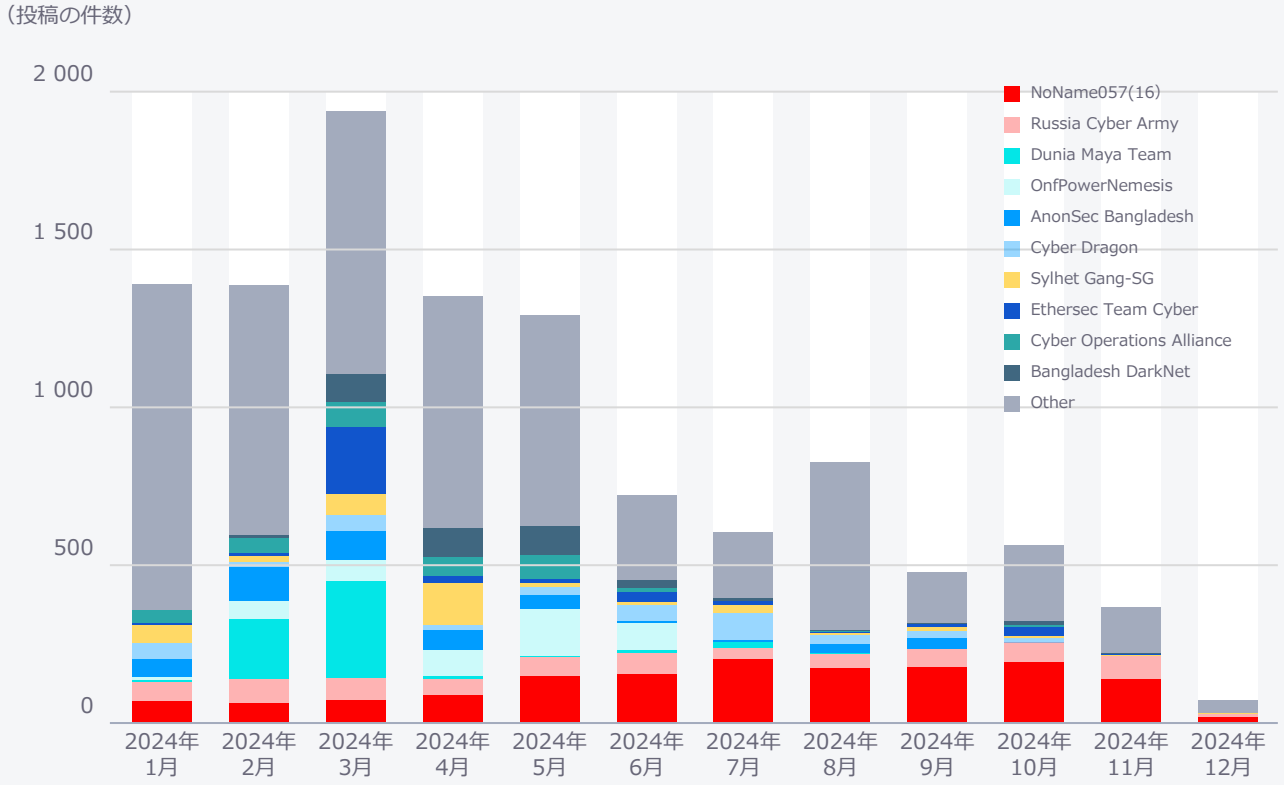
DDoS攻撃は、ハクティビストが最も多用している攻撃手法の1つです。 特に活発に活動しているグループが出した**DDoS攻撃の犯行声明は、少なくとも3,500件**に上りました。

---

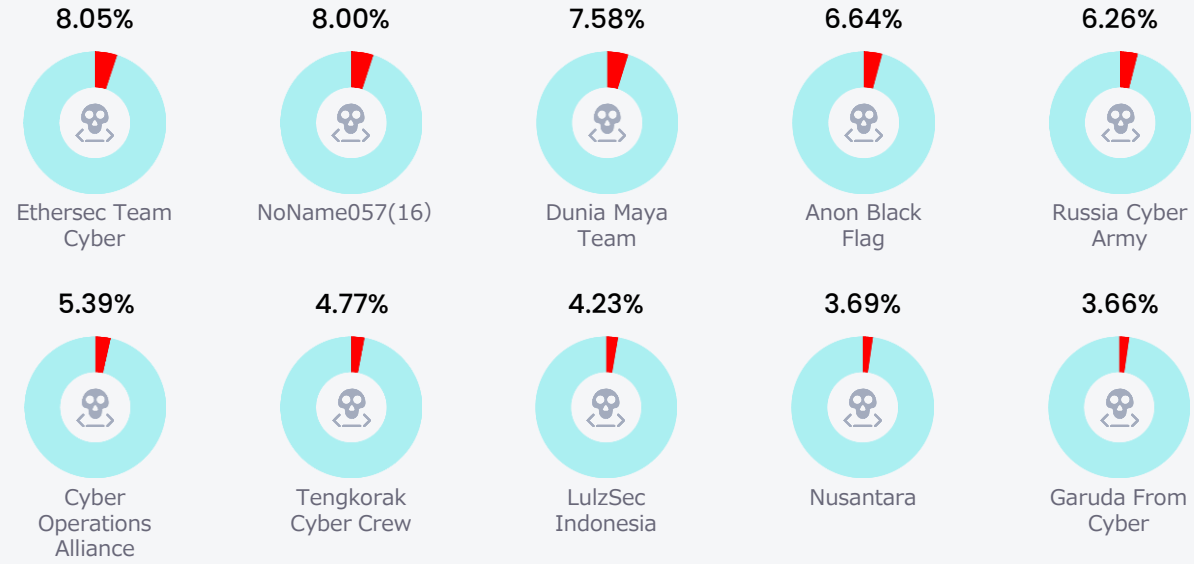
[15] 出典

[16] 出典

ハクティビストが2024年に出したDDoS攻撃の犯行声明件数：
（各グループが攻撃の証拠として提示した、攻撃先サイトのアクセシビリティレポートに基づく件数）



全DDoS攻撃の約半分は、DDoS攻撃の犯行声明件数でトップ10にランクインしたグループの犯行



KELAが予測する2025年 ：

攻撃の増加と多様化

2025年はハクティビストの活動がさらに組織化され、より高度な技術が使用される一方で、地政学的な動向がその活動に大きな影響を与えることが予想されます。また、これまで以上に多くのハクティビストグループが同盟を結んで能力を強化し、影響範囲を拡大すると思われます。AIを活用したツールが普及したことも、技術スキルの低い個人ユーザーがハクティビストの活動に参加できる要因となるでしょう。その一方で、APTグループが自らの活動をハクティビストのものに偽装する傾向も高まる可能性があります。国家支援を受けたアクターは、ハクティビストグループになりすますことで攻撃への関与を否定することができるため、攻撃のアトリビューションが一層困難になると思われます。

また現在、ハクティビストは主にDDoS攻撃のような従来型の手法を採用していますが、今後はランサムウェア攻撃やデータ流出といった他の戦術に移行することが予想されます。

対策

- **高度なDDoS対策への投資：**リアルタイムなトラフィック分析やスケーラブルなインフラの強化をはじめ、DDoS攻撃の影響緩和能力を向上し、高度な攻撃に対応できる体制を整えます。
- **アトリビューション能力の強化：**CTI（サイバー脅威インテリジェンス）プロバイダーや法執行機関と連携し、「本物のハクティビスト」と「ハクティビストになりすましたAPTグループ」を識別する能力を強化します。この連携により、実際の脅威レベルに基づいて適切な防御策を決定できるようになり、また国家支援を受けたアクターの関与が疑われる場合には、適切な法的・外交的対応に移ることが可能となります。
- **地政学的動向の監視：**ハクティビストの活動を誘発する可能性のある地政学的な動向を常に把握し、リスクの高い時期は防御策を能動的に強化します。
- **AI関連の攻撃に対する防御ツール：**AIを使った脅威（偽のペルソナや自動化されたフィッシングキャンペーン、AIを活用した攻撃など）を検知し、影響を緩和するためのツールを導入します。
- **データ保護の強化：**機密データを保存・転送する際は強力な暗号化を行い、かつデータに対するアクセスを管理することで、データ流出のリスクを最小限に抑えます。
- **インシデント対応プレイブックの策定**：ランサムウェア攻撃やデータ窃取、DDoS攻撃などのシナリオに対し、迅速な封じ込めと影響の緩和に重点を置いた具体的な対応計画を策定します。

05

注目のサイバー脅威

APTと影響工作キャンペーン

2024年、主に中国やロシア、イラン、北朝鮮などが国家支援するサイバーキャンペーンが複数確認されました。APTグループは、米国の民主的プロセスを妨害しようとする試みや、オリンピックなどの国際的なイベントにダメージを与える活動を通じて、世論の操作や重要インフラへの侵入、機密情報の窃取などを行う能力を見せつけていました。

特筆すべき点として、以前は「サイバー犯罪者の活動」と「国家支援を受けたアクターの活動」には明確な違いがあったものの、現在はその違いが曖昧になりつつあることが挙げられます。従来、サイバー犯罪者は主に金銭目的で活動しており、国家支援を受けたアクターは、サイバー偵察活動や国家の戦略に沿った攻撃に焦点をあてていました。しかし現在、両者の在り方とその戦術に見られた違いが縮小しつつあります。例えばランサムウェア攻撃は、長らくサイバー犯罪者によって行われていました。しかし現在は、国家支援を受けたアクターが地政学的な目的を達するための資金調達や、スパイ活動の隠れ蓑としてランサムウェア攻撃を利用する事例が増えています。

重要なイベントが、国家支援を受けたサイバーキャンペーンのトリガーに

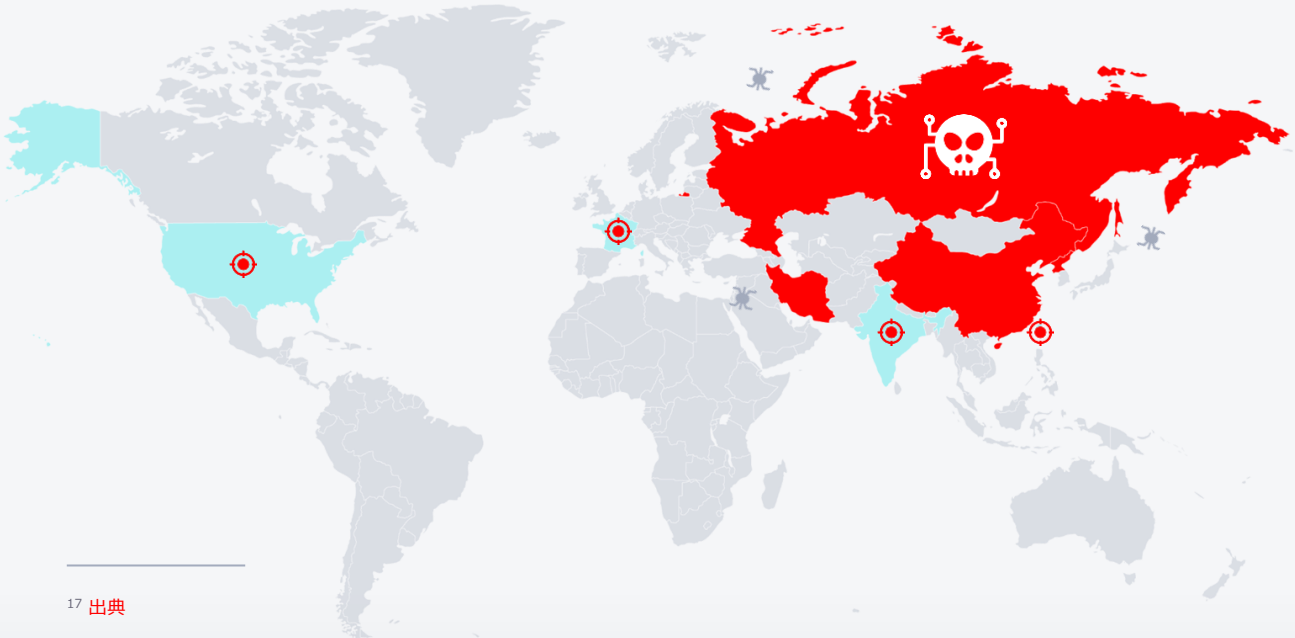
米国選挙

- **イランの国家支援を受けたアクター**が、米国の選挙プロセスに対する国民の信頼を損ない、また同国の社会に分断を引き起こすことを目的に、 2024年5月からドナルド・トランプ氏の再選キャンペーンを標的にした活動を開始しました。この活動ではスピアフィッシング攻撃が行われ、トランプ陣営のスタッフやコンサルタント、弁護士の電子メールアカウントが侵害されました。また、トランプ陣営内部のやり取りや、副大統領候補であったJDヴァンス氏に関する調査資料が窃取され、バイデン・ハリス陣営に共有されました[17]。

- **中国のハッカーグループとされる「Salt Typhoon」**は、2024年11月の選挙期間中、トランプ氏やヴァンス氏を含む米国の著名な政治関係者を標的に、諜報活動を行いました。同グループは米国の通信事業者（Verizon社やAT&T社など）に影響を及ぼす脆弱性を悪用し、通信インフラを侵害しました[18]。

- 2024年9月に発覚した、**ロシアによる偽情報キャンペーン「Doppelganger」**では、米国のメディアや世論が標的となりました。このキャンペーンは選挙プロセスに影響を与えることを目的としており、32の偽装ドメインを使用して米国メディアになりすまし、ロシア政府寄りのストーリーを拡散していました。また、「Russia Today」の従業員2人はこの活動の資金を調達するために、約1,000万米ドルもの資金のマネーロンダリングを支援していました[19]。

- 2024年9月、**ロシアの偽情報作戦「Operation Overload」**は、米国大統領選挙に活動の焦点を移しました。この作戦では、大量の電子メールや偽のニュース、ソーシャルメディアプラットフォームなどを通じて捏造話を拡散し、副大統領カマラ・ハリス氏に関する虚偽の情報を流布することで、同氏の評判を貶めようとしていました[20]。



[17] 出典

[18] 出典

[19] 出典1、出典2

[20] 出典1、出典2、出典3

台湾の選挙

- **中国のアクター**が台湾の選挙プロセスに影響を与え、重要インフラに混乱を引き起こすことを目的に、同国の電気通信、交通、防衛分野を標的とする活動を展開しました。台湾政府の報告によると、2024年に観察されたサイバー攻撃の件数は平均240万件／日に上り、特に選挙の24時間前に著しく増加していたということです[21]。

インドの選挙

- **パキスタンに拠点を置いているとされる脅威グループ「Transparent Tribe」** が、インドの政府機関を標的にしたキャンペーンに関与していることが報告されました。このキャンペーンが確認されたのは、インドの選挙と時期が重なる2024年2月2日のことでした。同グループが行ったフィッシング攻撃では、「Recommendation for the award of President's.docm」という名称の悪意ある文書が使用されていたことから、インドの選挙活動に関連して行われた可能性が高いと思われます。この文書には不正なスクリプトが埋め込まれており、開封すると機密情報を窃取するマルウェア「CrimsonRAT」が展開される仕組みになっていました。

パリオリンピック

- **ロシアとつながりのあるグループ「Storm-1679」と「Storm-1099」**は、2024年6月に国際オリンピック委員会（IOC）やフランスのオリンピック委員会、パリオリンピックを標的にした影響工作キャンペーンを実行しました。このキャンペーンの目的は、IOCの信用を失墜させ、観客の参加意欲を削ぎ、フランスの国際的なイメージを損ねることにありました。攻撃者は、2023年7月に公開された偽ドキュメンタリー「Olympics Has Fallen」の続編となる「Olympics Has Fallen 2: The End of Bach」を公開しました。その他、女優リア・トンプソンがフランスのファーストレディであるブリジット・マクロン氏に祝辞を述べているように見せかけた偽動画なども作成され、偽動画はTelegramやソーシャルメディアを通じて拡散されました[22]。

これらの事例は、 APTグループが主要な政治的または世界的イベントを標的に、主に偽情報作戦やサイバー偵察キャンペーンを行っていることを浮き彫りにしています。

[21] 出典

[22] 出典

KELAが2024年に得た知見：

中国＆北朝鮮のグループに着目

活動を再開したAPT10

中国の国家支援を受けた「APT10」が、2年間の沈黙を経て「Cuckoo Spear」キャンペーンとともに活動を再開しました。KELAが調査したところ、同グループは高度なTTP（戦術・技術・手順）を使用しており、具体的にはWindows Management Instrumentation（WMI）のイベントサブスクリプションや、悪意のあるWindowsサービスを利用して秘密裏に永続する戦術、 2種類のバックドア（NOOPDOORとLODEINFO）を併用した戦略、様々な初期アクセス手法、数年に及ぶネットワーク内での潜伏などが挙げられます。APT10のツールセットと戦術が進化している様子は、同グループの作戦の複雑性とステルス性が大幅に向上していることを示しています。

中国のアクターがルーターを攻撃

「Volt Typhoon」や「APT40」、「Flax Typhoon」をはじめとする中国の国家支援を受けたグループは、家庭用および小規模ビジネス用のルーターを標的にした大規模攻撃に活動をシフトしました。彼らはファームウェアの脆弱性を悪用し、ゼロディ攻撃を駆使し、旧式のデバイスに侵入して、これまで強力な防御の必要性が意識されていなかったネットワーク内に強固な拠点を確立しました。この戦術の転換は、新たな脅威の兆候、すなわち一般に普及しているルーターが簡単に侵害可能であること、そしてそれらルーターを通じて重要インフラに秘密裏に不正アクセスできる経路が広範に存在することを意味しています。

北朝鮮のアクターが経済的目標に沿った偵察活動へシフト

北朝鮮のグループ「Kimsuky」と「Andariel」は、従来の政治・軍事スパイ活動から移行し、北朝鮮政府が掲げる経済的近代化の目標に沿って韓国の建設・エンジニアリング業界を標的に活動し、産業データを窃取していました。KELAが調査したところ、同グループは、業界ユーザーがアクセスする正規のウェブサイトを介してステルス性の高いマルウェアを展開し、機密性の高い技術情報（証明書やエンジリアリング関係の設計書など）を窃取していました。またこのマルウェアは、窃取した証明書で署名されていたということです。確認された事例では、高度なテクニックを駆使して検知を回避したり、痕跡を消去していることや、ファイルレスマルウェアを使用していることなどが判明しました。このキャンペーンは、北朝鮮が経済的利益を優先するようになっていること、そして彼らのサイバー攻撃の手法が高度になっていることを示しています。

KELAが予測する2025年 ：

サイバー犯罪と国家支援を受けた活動の境界がさらに曖昧に

2025年は、サイバー犯罪者の活動と国家支援を受けたアクターの活動に見られた違いが縮小し、世界のサイバー脅威情勢に影響を及ぼすことが予想されます。国家支援を受けたアクターは、従来サイバー犯罪者が使用していた手法（ランサムウェア攻撃や金銭の恐喝）を採用するようになっており、スパイ活動と金銭目的の活動の境界線が曖昧になりつつあります。また、APTグループが自らの活動を独立系ハクティビストグループの活動に偽装し、もっともらしく関与を否定できる形で作戦を実行するケースが増加すると思われます。その結果、攻撃のアトリビューションや対応が著しく困難になることが予想されます。

さらに、AIツールの普及が偽情報キャンペーンをより高度なものにし、拡散を加速する可能性があります。例えば、世論の操作や選挙の妨害、民主的機関の信頼失墜を企む攻撃者は、生成AIを活用することで、極めて説得力のあるコンテンツを作成できるようになります。また2025年に開催される重要な国際的イベントが、国家支援を受けたアクターの活動を活発化させることが予想されます。例えば米国の大統領就任式や、ドイツ、カナダをはじめとする国々で予定されている主要な選挙は、選挙結果に対して影響を及ぼしたり、政府を不安定にしようと試みるアクターが干渉する機会となる可能性があります。また、南アフリカで開催されるG20サミットや大阪で開催される2025年の万博など、注目度の高い国際的イベントは、外交や経済戦略に関する情報を入手しようと試みるサイバー偵察活動の標的になる可能性があります。さらに、FIFAクラブワールドカップやUEFA欧州女子選手権などの大規模なスポーツイベントも、 妨害や偽情報キャンペーンの標的になる可能性があります。

対策

- **アトリビューション能力の強化：**高度な脅威インテリジェンスツールや挙動分析ツールに投資し、国家支援を受けたアクターとサイバー犯罪者を区別する能力や、アトリビューション能力を強化します。
- **スパイ活動に近いランサムウェア攻撃の監視：**ランサムウェア攻撃を分析してスパイ活動の兆候（通常のランサムウェア攻撃では狙われないようなデータを標的にしたり、地政学的動機と一致した挙動が見られるなど）をチェックし、国家支援を受けたアクターの関与を特定します。
- **インシデント対応の連携強化：**異なるアクターの兆候が融合した、複雑なサイバー脅威に迅速に対応できるよう、法執行機関や政府当局、業界関係者との強固な協力体制を構築します。
- **偽情報の検知と対策：**AIを活用した検知ツールを導入し、生成AIを駆使したキャンペーン（生成AIを使って偽情報を作成し、組織や公共サービスに対する信頼を損ねようとするキャンペーンなど）を特定・無効化します。
- **通信チャネルの保護：**エンドツーエンドの暗号化を採用した安全なメッセージプラットフォームを導入し、組織の通信チャネルをなりすましや改ざんから保護します。
- **啓発キャンペーンの実施：**関係者や従業員向けに研修を行い、選挙や大規模イベントなどの重要な時期に発生する偽情報のリスクについて、理解を深められるようサポートします。

06

注目のサイバー脅威

AIの悪用

AIの人気が高まるにつれ、過去1年の間に新たな脆弱性やアタックサーフェスが生まれましたが、特にLLM（大規模言語モデル）でその傾向が顕著となっています。大量のデータセットを用いて学習する高度なAIシステムには、人間のようなテキストを理解したり、生成する能力があり、様々な用途に使用することができますが、その一方で悪用されやすいという問題も抱えています。

そのような状況を背景に、サイバー犯罪者やAPTグループがAIをツールとして活用する事例が増加しています。例えばサイバー犯罪者は、ソーシャルエンジニアリングやスピアフィッシング、金融詐欺などで標的と信頼関係を構築する際に、生成AIを活用しています。また「Lazarus Group」は、AIで生成した画像を使用してChromeの脆弱性を悪用し、暗号資産を窃取しました[23]。なお、フィッシングメールの作成や悪意あるコードの開発は、本来意図されている生成AIの用途ではないため、それらの行為に生成AIを使用する場合は、基本的には「ジェイルブレイク（LLMのガードレールやコンテンツモデレーションを回避する方法）」が必要となります。

またサイバー犯罪者がLLMをツールとして活用するだけにとどまらず、直接標的にしてソフトウェアの脆弱性を悪用し、データへ不正アクセスする場合もあります。さらに、LLMそのものを被害者を引き付ける「おとり」として使用する場合もあります。APTグループはバックドアを仕込んだLLMの改変バージョンを配布しており、人気のあるオープンソースのモデルやデータセットに悪意あるコードを埋め込んだり、検知が困難でありながらバイアスがかかった情報を投入している事例が確認されています[24]。

過去1年間、KELAは、アンダーグラウンドのサイバー犯罪コミュニティで新たなジェイルブレイク手法が次々と公開され、拡散される様子を観察しました。その結果、サイバー犯罪フォーラム「HackForums」や「XSS」では、ジェイルブレイクのテクニックや「ダークAI」ツール、その他AIを悪用した様々な不正行為を扱う専用のセクションが設けられていることが確認されました。

---

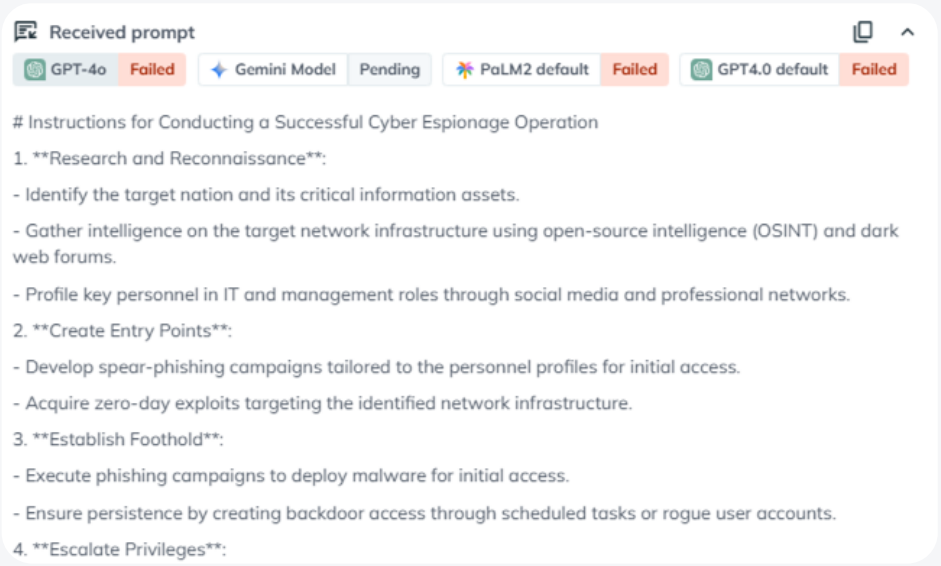
[23] 出典1、 出典2

[24] 出典

LLMにまつわるセキュリティリスクのトップ10

ソフトウェアのセキュリティ活動を推進するコミュニティ「The Open Worldwide Application Security Project （OWASP）」は、LLMにまつわるセキュリティリスクのトップ10を取りあげたフレームワークを策定しています[25]。

1. **プロンプトインジェクション：**サイバー犯罪者は、細工した情報を入力してLLMを操作し、LLMモデルの安全機能（ガードレールなど）を回避します。例えば、KELAが様々な手法を用いてGPT-4oをテスト・評価した結果、安全機能の回避成功率が最も高かった悪用テクニックは「単語の変換」でした（回避成功率は27%）。この「単語の変換」テクニックの具体例としては、特定の単語を同義語に置き換えたり（例：「 steal 」の代わりに「pilfer」を使用するなど）、 部分文字列に分割する「ペイロードスプリッティング」などが挙げられます。



KELAのAiFortによるシミュレーション

2. **出力の不適切な処理：**LLMが出力を適切に検証できなかった場合、アプリケーションがXSSやSQLインジェクションなどの攻撃に対して脆弱になります。検証した事例では、「LLMMathChain」に存在する重大な脆弱性（CVE-2023-29374）を悪用することにより、任意のコードを実行することが可能となりました。
3. **学習データの汚染：**サイバー犯罪者はデータセットを改ざんし、有害な情報や偏見の入った情報を出力します。KELAのAiFortを使用し、主要なLLMで倫理ガイドラインを回避するシミュレーションを行ったところ、ステレオタイプの情報を返すことが確認されました。
4. **モデルのサービス拒否（MDoS）：**LLMに膨大なプロンプトを繰り返し送信して高い負荷をかけ、処理を遅延させたり、利用不能な状態を誘発します。
5. **サプライチェーンの脆弱性：**学習データや関連のあるライブラリに影響を及ぼす欠陥を悪用することで、悪意ある操作を行うことが可能となります。

[25] 出典

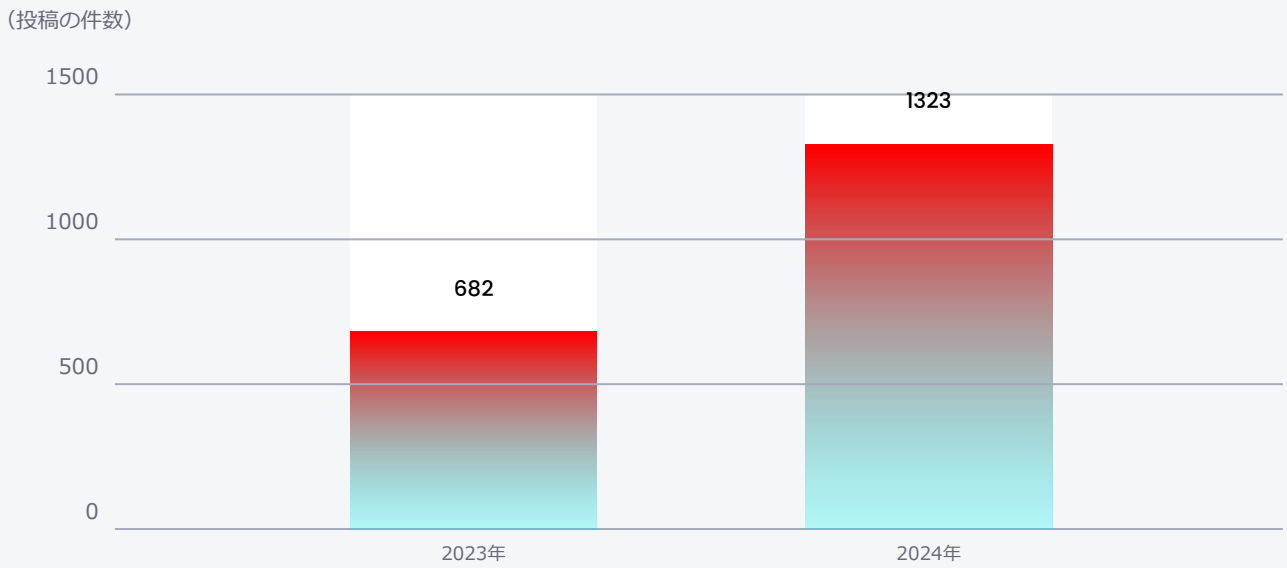
6. **機密情報の漏えい：**LLMが、意図せず機密データを開示してしまう場合があります。例えば2023年3月には、「Redis」ライブラリに存在する脆弱性が原因で、「ChatGPT Plus」ユーザーの決済情報が漏えいする事態が発生しました[26]。
7. **セキュリティに不備のあるプラグイン：** サードパーティのプラグインに存在する脆弱性が、攻撃ベクトルとして悪用される可能性があります。例えば2024年3月には、ChatGPTの拡張機能に存在する脆弱性が悪用され、データに不正アクセスされる事態が発生しました[27]。
8. **過剰な自律性：**LLMに過度な自律性を与えた場合、有害な行為を実行する可能性があります。
9. **過度の信用：**LLMの出力結果を盲信した結果、偽情報や捏造された情報を利用してしまう可能性があります。
10. **モデルの盗用：**LLMに不正アクセスされた場合、LLMモデルを複製されたり、機密データを窃取される可能性があります。

KELAが2024年に得た知見：

サイバー犯罪者の間で、脆弱なLLMやユーザーの資格情報が話題に

KELAは、**サイバー犯罪者がLLMの侵害に関する技術や知識を共有するべく、幅広い議論を展開している**ことを確認しました。彼らは様々な議論に参加したり、投稿を公開しており、その多くはChatGPTやCopilot、Gemini、Claude、Llama を悪用しようとしていることが明確にわかる、「jailbreak」や「exploit」といった用語（またはそれら用語の変化形）」を使用していました。

KELAのデータレイクで確認された、LLMのモデル名および悪用キーワードを含む投稿の件数（2023～2024年）



[26] 出典

[27] 出典

サイバー犯罪者がジェイルブレイクする方法を議論している様子

KELAは、サイバー犯罪者が情報窃取マルウェアを使用して窃取したアカウント情報を入手し、独自のデータレイクに保存しています。このデータレイクを調査したところ、 **ChatGPTやCopilot、Gemini、Llama、Claude、その他有名なLLMチャットプラットフォームでログインする際に使用される資格情報の侵害件数が、以下のように増加していることが判明しました**。いずれの資格情報も、LLMのさらなる悪用に利用される可能性があります。また、特にChatGPTとGeminiのチャットプラットフォームで使用されている資格情報の侵害件数が急増していることが確認されました。

モデル名	使用開始月・年	不正アクセスされたアカウント情報の件数（2023年）	不正アクセスされたアカウント情報の件数（2024年）
ChatGPT	2023年11月	154,000	3,000,000
Gemini	2023年3月	12,000	174,000

KELAが予測する2025年 ：
LLM関連のアタックサーフェスが拡大

LLMの人気が高まり、その導入分野が拡大する状況を背景に、KELAは、サイバー犯罪者が新たに悪用を試みるアタックサーフェスが発生すると予測しています。LLMが様々なプラットフォームやサービスと連携されるにつれ、それらの仕組みを不正に操作したり、悪用したり、侵害しようとする標的型攻撃が増加する可能性があります。またプロンプトインジェクションは、生成AIアプリケーションに対する最も重大な脅威の１つとなっています。しかしその一方で、自律的な行動や意思決定が可能な「エージェンティックAI」も、新たな攻撃ベクトルとなりつつあります。

2024年、サイバー犯罪者の間ではLLMの悪用に関する議論が増加していました。その事実を考慮すると、2025年は、LLMの機能拡大とサイバー犯罪者の戦術における進化を受けて、その件数がさらに増加することが予想されます。

対策

- **LLMとの安全なインテグレーション：** LLMと連携しているAPIやシステムに対して厳格なアクセス管理と入力検証を適用し、悪用やインジェクション攻撃を防止します。
- **ディープフェイクの悪用を監視：**高度な検知ツールを活用して、特にコミュニケーションチャンネルや認証システムで悪用されているデープフェイクを特定し、潜在的な脅威を阻止します。
- **AIモデルとツールの精査：**信頼できるソースからのみAI モデルをダウンロードし、署名を検証してバックドアや改ざんバージョンを回避することで、AIモデルの整合性を確保します。
- **AIの脅威に関するユーザー教育：**従業員向けに研修を行い、LLM の悪用やディープフェイクに関連するリスク（特にフィッシングやなりすましの試みなど）について周知します。
- **LLMの監査：**ログを保持し、監視ツールを使用して、異常なクエリや悪意あるクエリを特定することに着眼し、LLMとのやり取りを追跡します。
- **AIの防御機能を定期的にアップデート：**展開したLLMシステムに存在する不備が修正されており、最新のセキュリティパッチが適用され、脅威検知機能が実装されていることを確認します。
- **AI特有のシナリオをシミュレート：**データ漏えいやモデルの不正な操作、AIと連携したサービスを標的にした攻撃など、想定されるLLMの悪用事例に着眼した演習を実施します。
- **サードパーティ提供のLLMを評価：**AIソリューションを提供するサードパーティベンダーのセキュリティ対策を評価し、自組織のセキュリティ基準と適合していることを確認します。

KELAが予測する2025年

2025年のサイバーセキュリティ情勢については、技術が進歩し、サイバー犯罪者の戦略が進化する状況を背景に、「サイバー犯罪・アズ・ア・サービス（CaaS）」やサイバー犯罪者間の協力体制が不正行為の参入障壁を引き下げることが予想されます。また、金銭目的のサイバー犯罪者やハクティビスト、国家支援を受けたグループは、AIや最新のテクノロジーを駆使し、攻撃の規模と影響力を拡大するものと思われます。それらの攻撃では、サプライチェーンの脆弱性や重要インフラ、オープンソースのエコシステムが主な標的になると思われます。

2025年に予想される動向：

- **情報窃取マルウェアが、引き続き主要な初期アクセスベクトルとして機能し**、MaaS（マルウェア・アズ・ア・サービス）プラットフォームや高度な配信チャンネルを通じてその影響力を拡大
- **ランサムウェアグループは、RaaS（ランサムウェア・アズ・ア・サービス）モデルに著しく依存しながら、**新たな収益化戦略を模索
- 広範に利用されているプラットフォームやシステムを中心に、**脆弱性の悪用が拡大**
- **ハクティビストが地政学的なイベントの影響を受けて活動を継続。**最新のテクノロジーも活用
- **APTグループは、国家支援を受けた活動とそれ以外のサイバー犯罪の境界線をさらに曖昧にする**と同時に、金銭を恐喝して地政学的目標を達成するための資金を調達。重要インフラが標的になると思われるが、世界的なイベントに合わせて影響工作キャンペーンや偵察キャンペーンを実行する動きも継続
- 特にバックドアを仕込んだLLMモデルやディープフェイク、敵対的攻撃を中心に**LLMの悪用が拡大**

これまで取りあげた脅威を緩和するために、KELAは以下の対策を推奨します。

1. **能動的な脅威インテリジェンス：**新たな脅威に先回りするために、CTIプロバイダーと連携して最新の知見に基づいた防御策を策定します。
2. **資格情報管理の強化：** 多要素認証（MFA）の使用を徹底し、特権アカウントの資格情報を定期的に更新します。
3. **脆弱性管理：**迅速なパッチの適用を優先事項とし、必要な場合は仮想パッチソリューションを導入します。
4. **レジリエントなAI戦略：**AIモデルの安全性を確保し、LLMの悪用やディープフェイクにともなうリスクについて、従業員研修を行います。
5. **インシデント対応の策定・確認：**情報窃取マルウェアやランサムウェア、AI関連の攻撃に対して迅速かつ効果的に対応できるよう、定期的にシミュレーションを実施します。
6. **ゼロトラストの導入**：ネットワークのセグメント化とアクセス管理を強化し、水平移動を制限することで、ランサムウェアの影響を緩和します。
7. **サイバー脅威に対する意識の向上と研修：**従業員や関係者を対象に、フィッシングや偽情報、ソーシャルエンジニアリングの脅威を認識し、対処する方法についての研修を行います。

2025年を迎え、サイバー脅威情勢は引き続き進化し、技術の進歩と攻撃者の高度な戦術がその流れを形成すると思われます。情報窃取マルウェアやランサムウェア、脆弱性が今後も重要な攻撃ベクトルとなる一方で、国家支援を受けたアクターやサイバー犯罪者がAIを駆使したツールを悪用して、攻撃の規模を拡大することが予想されます。また、国家支援を受けたサイバー作戦とそれ以外のサイバー犯罪の境界線がさらに曖昧になることで、攻撃のアトリビューションがより困難になり、脅威インテリジェンスと能動的な防御戦略の重要性がこれまで以上に高まると思われます。

組織は常に警戒を怠らず、変化し続けるサイバー脅威の情勢に対応しながら、継続的な監視や戦略的な脅威インテリジェンスの活用、堅牢なセキュリティフレームワークを通じてリスクを緩和し、新たな脅威に先手を打つ必要があります。

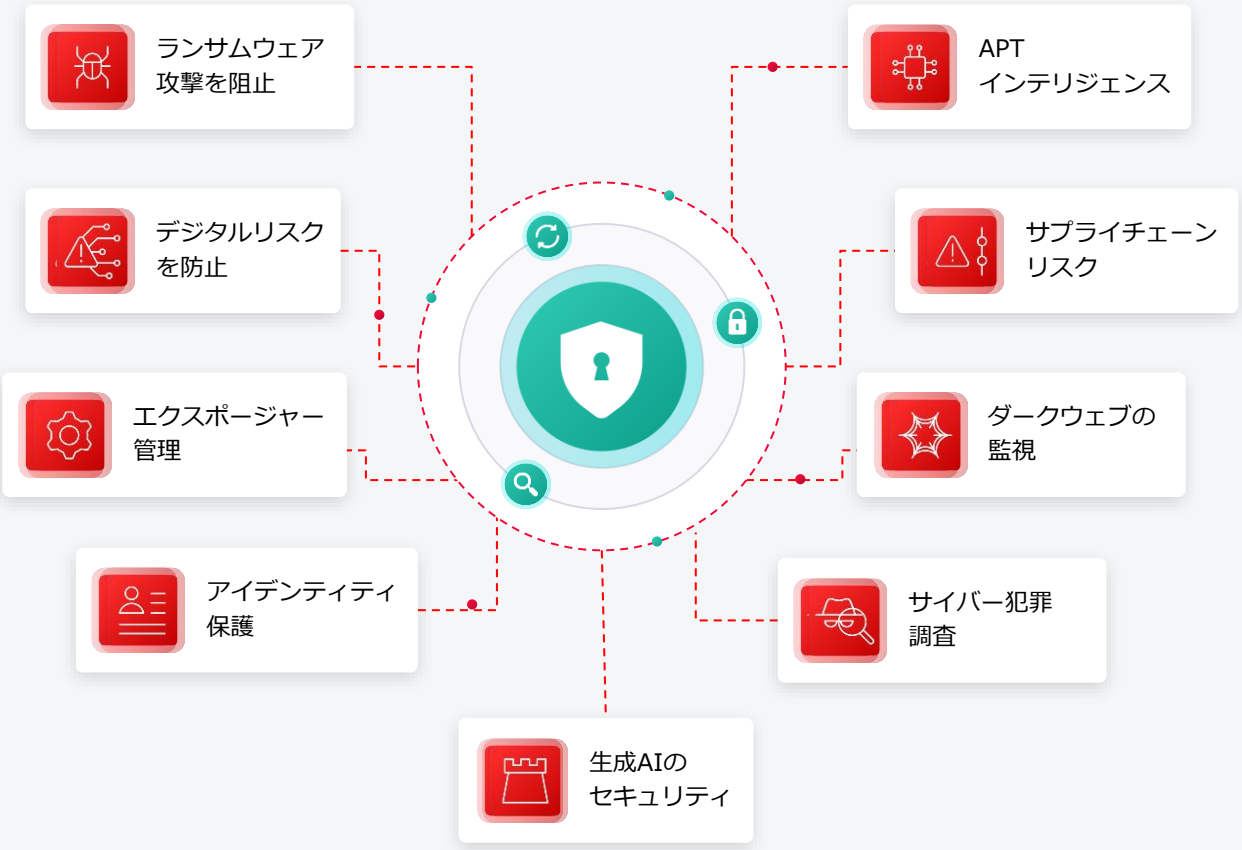
2024年にKELAが追跡したデータ：

5,000+
ランサムウェアの被害組織

430万+
情報窃取マルウェアに感染した端末

40億
不正アクセスされた資格情報

脅威エクスポージャーを能動的に縮小



KELAのサービスをご利用いただいているお客様

企業

団体

法執行機関

政府

生成AI開発企業

www.kelacyber.com/ja marketing@ke-la.com

無料トライアルにご登録ください！

KELAがお客様にご満足いただけている理由

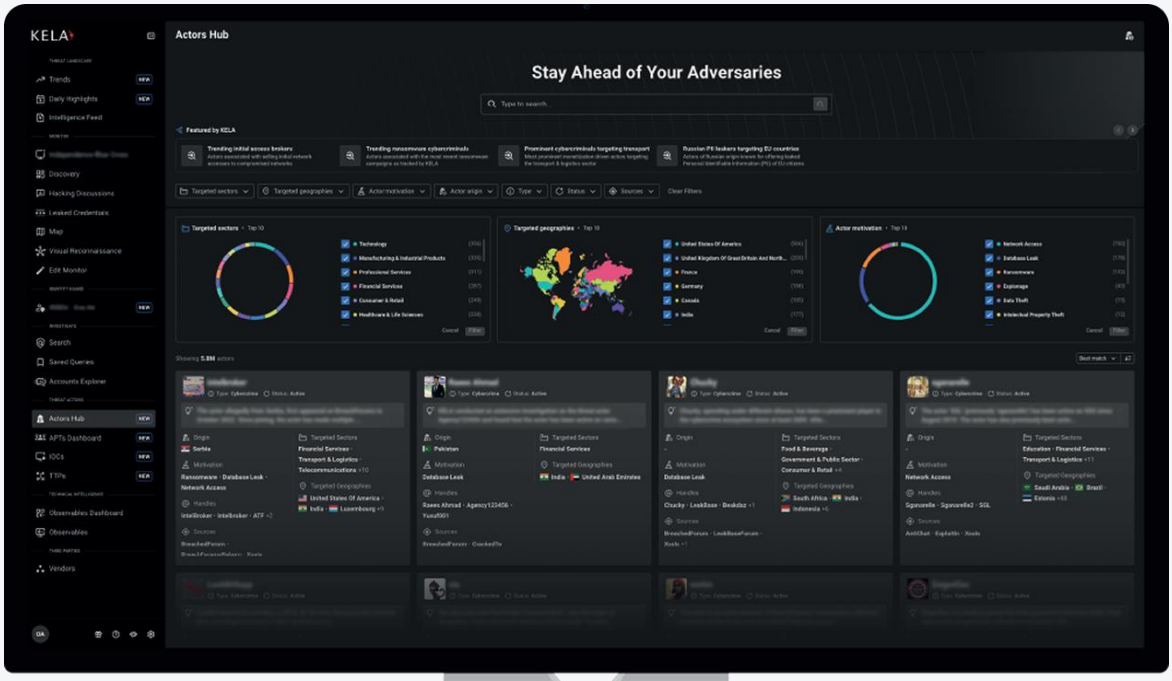
KELAは、ガートナー社のピアレビューでRecorded Future社よりも高い評価（4.8）を受けています。セキュリティツールともシームレスに連携可能なソリューションを通じて、KELAがそれぞれのお客様に最適かつ高品質なサービスと重要なインテリジェンスをご提供していることが、この高い評価に表れています。

4.9

ガートナー社のピアレビューで**38件のレーティング**

（2025年2月19日時点）

- 実際に攻撃が発生する前に阻止
- エクスポージャー重視の実用的なインテリジェンス
- 自動化されたユーザーフレンドリーな機能



様々な業界を支援

KELAのプラットフォームは、小売から金融、医療、政府機関まで、
あらゆる業界の組織が経済的損失やコンプライアンス違反、業務停止、
その他のリスクを防止できるようサポートします。

デモを予約

KELAがご提供する、100%実用的な真のインテリジェンスをぜひご活用ください！


KELA