2025. 12

AhnLab

2025年のサイバー脅威動向
2026年の展望

概要

目次

概要

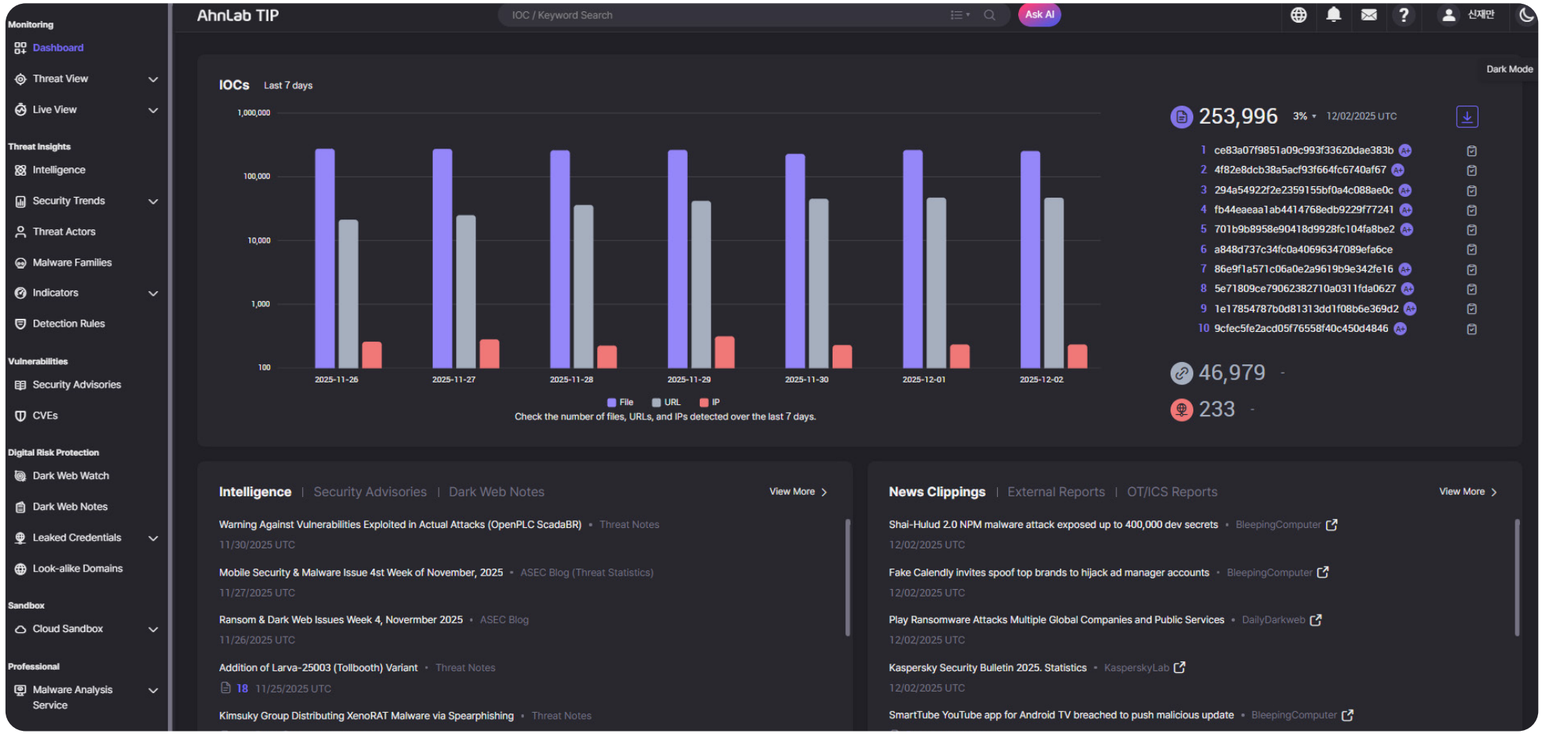
レポート紹介

本レポートは、アンラボの脅威インテリジェンスプラットフォーム「AhnLab TIP」を通じて提供されるセキュリティコンテンツに基づき、2024年第4四半期から2025年第3四半期までの様々なセキュリティ課題とトレンドを紹介し、2026年のサイバーセキュリティ脅威を展望する。

AhnLab TIP は、複数の情報源からマルウェア、侵害事故、脅威アクター、脆弱性、侵害指標（IoC）、セキュリティニュースなど多様な脅威情報を収集、分析、分類する。これにより、顧客が脅威インテリジェンスに基づいてセキュリティ戦略を策定し、意思決定を行えるようサポートする。

AhnLab TIP の詳細については、アンラボの公式ホームページおよびAhnLab TIP ポータルで確認できる。

→ アンラボのホームページへ
→ AhnLab TIP ポータルへ



[画像] AhnLab TIP ダッシュボード

概要

数字で見るアンラボの脅威インテリジェンス

2,258件
脅威インテリジェンス投稿

AhnLab TIP の 「Intelligence」 掲示板には、過去1年間で2,258件のコンテンツが投稿された。コンテンツの種類は以下の通りである。

- **ASEC Notes**: 脅威情報を最も迅速に提供
- **ASEC Blog**: 最新の脅威を迅速に分析
- **Dark Web Notes**: ディープウェブ／ダークウェブにおける脅威と高リスク情報の提供
- **動向レポート**: マルウェア、ダークウェブなど多様な動向を分析
- **分析レポート**: APTグループ、攻撃手法などの深層分析

661件
セキュリティ勧告

セキュリティ勧告は、ソフトウェアの脆弱性や組織のセキュリティを脅かす問題について、迅速な情報と対応ガイドを提供する。

毎日数千〜数万件 IoC
30% - アンラボ独自の IoC

悪性ファイル、URL、IP、ドメインなど、毎日数千〜数万件の IoC を提供し、顧客が脅威対応に活用できるようにしている。

アンラボは国内最大規模の脅威検知と対応センサーネットワークを有しており、これにより**アンラボの IoC の約30%は、OSINT では入手困難な独自情報で構成されている。**

404件 – 脅威アクター
1,051件 – マルウェアファミリー

アンラボは脅威アクターおよびマルウェアファミリを継続的に追跡し、分析情報を　AhnLab TIP を通じて提供している。

Threat Actors 掲示板では、脅威アクターの詳細情報に加え、関連する TTP、IoC、最新記事などを閲覧できます。

マルウェアファミリー掲示板では、マルウェアの特徴、手法、作成者などに基づいて分類したマルウェア群の情報を提供します。

2,216件
ニュースクリッピング

国内外の主要メディアやベンダーが公開したセキュリティニュースと技術文書を提供します。各ニュースには関連するIoC情報を併せて掲載し、企業のセキュリティ担当者が対応に活用できるようにしています。

2,970件 – 外部レポート
19,679件 – ソーシャルメディア投稿

国内外のセキュリティ企業と専門家のセキュリティレポート、X（旧 Twitter）から選別したセキュリティレポート及び動向情報を提供する。該当コンテンツも関連する IoC を提供し、顧客の脅威把握及び対応をサポートする。

2025年のサイバー脅威動向

→ 主要事件

→ 攻撃グループの動向

- ダークウェブ Top 8
- 国別APTグループ

→ ランサムウェアの動向

- 主要グループ活動 Top 10
- 主要被害産業群
- 主要被害国

→ 主要脅威の動向

- マルウェア Top 9
- 攻撃手法 Top 10
- 脆弱性 Top 10
- モバイル Top 6

→ 攻撃総計

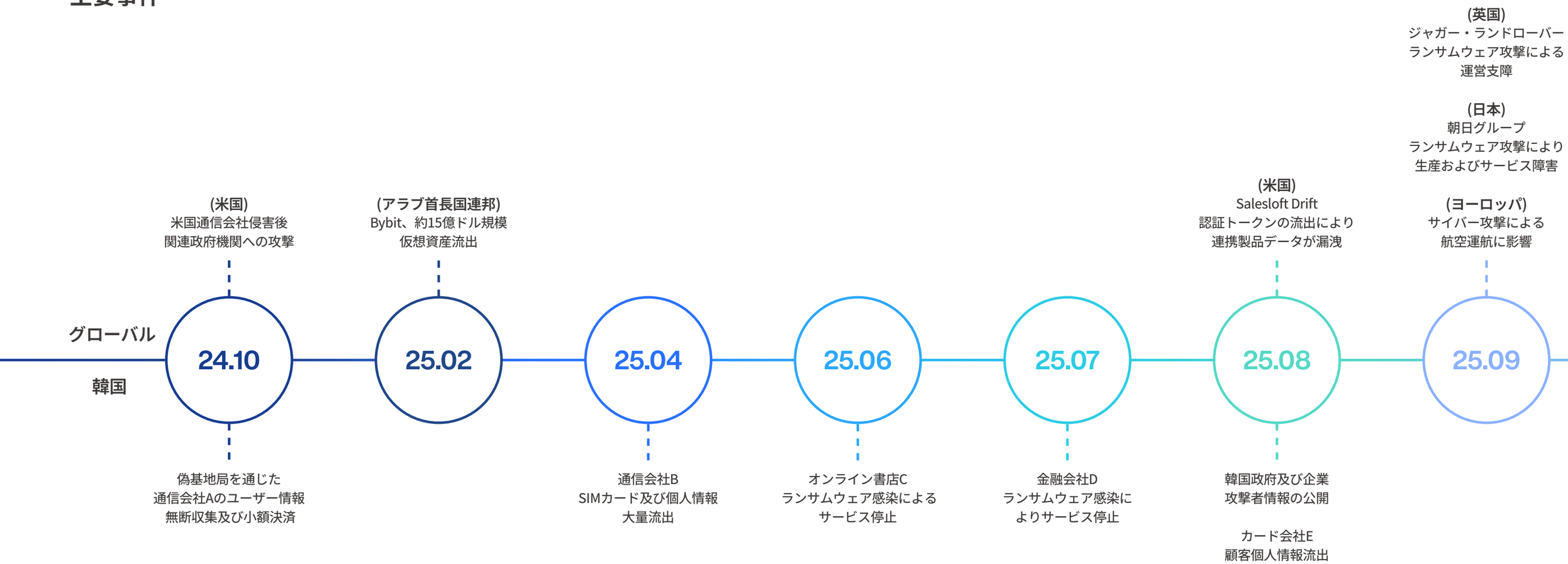
- 攻撃タイプ

AhnLab

2025年のサイバー脅威動向 & 2026年の展望

2025年のサイバー脅威動向

主要事件



2025年のサイバー脅威動向

主要事件：グローバル

24年10月 米国通信会社侵害後、関連政府機関を標的とした攻撃発生

ハッキンググループ「Salt Typhoon」が、米国の主要通信事業者少なくとも8社を侵害し、捜査機関の盗聴システムや機密通信インフラに不正アクセスした。

彼らは Ivanti VPN（CVE-2023-46805、CVE-2024-21887）、Fortinet EMS（CVE-2023-48788）、Sophos Firewall（CVE-2022-3236）、Microsoft Exchange ProxyLogon などの脆弱性を悪用して侵入した。侵入した通信網を経由して米国政府機関の通信を傍受し、裁判所命令に基づく傍受データにも不正アクセスしていたことが確認されている。

攻撃者は GhostSpider、SnappyBee、Masol RAT などの高度なバックドアを使用して、密かに長期間内部に潜伏した。長期間にわたり潜伏し続けた。一部の政府ウェブサイトも攻撃を受けていたことが明らかになっている。

25年2月 Bybit、約15億ドル相当の仮想資産流出

ドバイの仮想通貨取引所 バイビット(Bybit) は、約15億ドル相当の暗号資産が盗まれる被害に遭った。この攻撃は、**Lazarus グループによるものと**推定される。

攻撃者はコールドウォレット (cold wallet) からホットウォレット (hot wallet) への資金移動プロセスを狙った。内部の開発者向けシステムを侵入するか、セーフウォレット (safe wallet) プラットフォームの署名インターフェースを操作し、マルチシグ（Multisig）ウォレットのトランザクションを偽造した。 この過程で悪意のある JavaScript コードを署名ホストに挿入し、正常なアドレスを偽装した後、実際には攻撃者のウォレットへ資産を転送した。奪取された資産はイーサリアム（ETH）、ステーキングイーサリアム（stETH）などであった。バイビット (Bybit) は補償プログラムなどを実施した。

25年8月 Salesloft Drift、認証トークン流出で連携製品データが暴露

セールスロフト(Salesloft)の Drift AI チャットボット統合機能がハッキングされ、OAuthトークンが漏洩。セールスフォース(Salesforce)を含む**700社以上の顧客データが**奪取された。

攻撃者はまずセールスロフトの GitHub アカウントを侵害し、内部コードを不正取得した。その後、Drift の AWS 環境へ移動し、OAuth トークンを収集した。このトークンを利用してセールスフォースインスタンスにアクセスし、顧客情報やアカウントなどを窃取した。

攻撃者は AWS キー、パスワード、Snowflake トークンなども収集したと伝えられている。セールスフォースとセールスロフトは Drift アプリを AppExchange から削除し、すべての接続を遮断した。さらに、被害企業への通知とトークンの無効化を実施した。

主要内容

- Salt Typhoon、米国通信社への侵入後、捜査機関の盗聴システム及び通信インフラに不正アクセス
- ドバイに本拠を置くバイビット（Bybit）、約15億ドル相当の暗号資産が盗まれる被害– Lazarus による犯行と推定
- Salesloft の Drift AI チャットボットがハッキングされ OAuth トークンが流出、700社以上の顧客データが盗まれる

2025年のサイバー脅威動向

主要事件：グローバル

25年9月 日本アサヒグループランサムウェア被害

日本の代表的な食品飲料企業であるアサヒグループは、**キリン(Qilin)ランサムウェアの攻撃を受け、全国30工場の生産・物流システムが停止した。**

攻撃者はアサヒの日本国内ITインフラを暗号化し、一部データを外部に流出させた後、金銭を要求した。アサヒスーパードライ、ドラフトビール、ドライゼロなどの主要製品の生産・出荷が停止し、コールセンターと注文システムもオフライン状態が続いた。 キリン(Qilin) ランサムウェアグループはGolangとRustベースの高度なランサムウェアを使用するサービス型ランサムウェア（RaaS）組織で、二重恐喝（ダブルエクストーション）の手法を活用する。アサヒグループは外部専門家と協力し復旧を進めている。一部工場は10月初旬から部分的に稼働を再開した。

25年9月 英国 Jaguar Land Rover ランサムウェア 被害

ジャガー・ランドローバー（Jaguar Land Rover、JLR）は、Scattered SpiderおよびLapsus$と関連すると推定される組織によるランサムウェア攻撃を受け、全世界の生産が停止した。

攻撃者は**JLRの内部ITシステムを停止させ、英国国内の主要工場とグローバル生産ラインを5週間以上停止させた。**3万人以上の従業員と20万人規模のサプライチェーン関係者が影響を受けた。総被害額は約19億ポンド（約3.3兆ウォン）と推定される。

JLRは顧客データの流出はないと表明したが、生産停止と納期遅延、部品供給の支障による経済的影響は甚大であった。英国政府は15億ポンド規模の緊急融資保証を提供し、産業安定化に乗り出した。

25年9月 サイバー攻撃による欧州空港障害発生

欧州の**空港がコリンズ・エアロスペース（Collins Aerospace）のMUSEソフトウェアに対するランサムウェア攻撃により大規模な障害が発生した。**同ソフトウェアは空港の電子チェックイン、手荷物処理、搭乗券発行などを提供している。

今回の攻撃により、ロンドン・ヒースロー、ブリュッセル、ベルリン、ダブリン空港などで数百便のフライトが遅延または欠航した。

攻撃者はコリンズ・エアロスペースの欧州データセンターを経由して侵入したと推定される。一部のシステムは復旧中に再感染し、復旧が遅延。数千人の乗客が手動チェックインと長時間の待機で不便を強いられた。

主要内容

- 日本のアサヒグループ、キリン(Qilin)ランサムウェア攻撃を受け、30工場のシステムが停止
- ジャガー・ランドローバー、ランサムウェア攻撃で英国とグローバル生産ラインが5週間以上停止 – 被害額約19億ポンドと推定
- コリンズ・エアロスペース、ランサムウェア攻撃を受け欧州主要便に遅延・欠航

2025年のサイバー脅威動向

主要事件：韓国

24年10月 通信会社A、偽基地局によるユーザー情報不正収集及び少額決済被害

通信会社Aの一部ユーザーを対象とした偽基地局を利用したサイバー攻撃事件が発生した。約2万2千人の個人情報が流出、368人に数億ウォン規模の不正な少額決済による被害が発生した。

攻撃者は2024年10月から偽基地局で被害者の携帯電話を自動接続させ、IMSI などの加入者識別情報を窃取した。その後、複製端末の作成や認証手順の回避などを通じて小額決済を行ったとみられる。

警察は一部の容疑者を検挙し、機器の一部を確保した。政府は官民合同調査団を構成し、原因究明に乗り出した。該当通信会社は新たなフェムトセルの接続を遮断、少額決済限度額縮小、USIM 保護サービス拡大、被害者への返金・補償措置を実施中である。

25年4月 通信会社B、SIM カード及び個人情報の大規模流出

通信会社Bは約2,300万人の顧客個人情報が流出する大規模なハッキング被害を受けた。流出情報には加入者電話番号、IMSI、IMEI、SIM 認証キー（K値）など SIM の核心識別情報が含まれていた。これにより、SIMスワッピング、名義盗用などの二次被害の懸念が提起された。

攻撃には Linux ベースの BPFDoor バックドアが使用された。このバックドアはカーネルレベルパケットフィルタを活用して検知を回避し、特定のマジックパケット受信時のみに活性化する。攻撃者はウェブシェル及びリモートコード実行(RCE)脆弱性を通じて内部システムに侵入した。その後、HSS サーバーに BPFDoor をインストールし、SIM 情報を窃取したことが確認された。

25年6月 オンライン書店C、ランサムウェア感染によりサービス停止

韓国1位のオンライン書店であり、チケットプラットフォームであるC社は、**ランサムウェア攻撃によりウェブサイトとモバイルアプリが4日にわたり停止した。**攻撃者は重要な内部ファイルと管理者アカウントを暗号化し、システム全体を封鎖し、金銭を要求した

約2,000万人のユーザーが書籍購入、公演予約、コミュニティ利用などで大きな不便を被り、コンサートやファンミーティングが中止・延期される事態も発生した。

主要内容

- 通信会社A、偽基地局を利用したサイバー攻撃 - 被害者携帯電話の自動接続後、加入者識別情報を窃取
- 通信会社B、顧客2,300万人の個人情報流出 – Linux ベースの BPFDoor マルウェアを使用
- オンライン書店C、ランサムウェア感染 – ウェブサイトとモバイルアプリが4日間停止

2025年のサイバー脅威動向

主要事件：韓国

25年7月 金融会社D、ランサムウェア感染によりサービス停止

金融会社Dは**Gunra ランサムウェアに感染し、コンピュータシステムが停止する**大規模なサイバー攻撃を受けた。攻撃者は SSL VPN 機器の SSH ポートに対するログイン試行を行い、内部ネットワークに侵入した。その後、管理者権限を取得しランサムウェアを配布した。

このランサムウェアは ChaCha8 + RSA 暗号化アルゴリズムを使用し、主要ファイルを条件別に精巧に暗号化し、.ENCRT 拡張子を付加した。ランサムウェア感染により、賃貸資金保証、携帯電話開通、融資保証などの金融サービスが中断された。一部支店では手作業で対応する事態も発生した。**幸い、復旧ツールを製作しシステム復旧に成功した。**

25年8月 韓国政府及び企業攻撃者「APT Down」情報公開

グローバルハッキングカンファレンス DEF CON 33で発表された報告書「APT Down: The North Korea Files」は、韓国を攻撃した APT グループの実態を明らかにした。報告書はハッカーのワークステーションから抽出された8.9GB分のデータを基に、**韓国政府機関・選挙管理委員会・メディア・通信会社への長期潜入の状況を記載している。**

攻撃者はフィッシング、証明書窃取、内部ネットワーク横移動（Lateral Movement）など高度な手法を使用した。また、北朝鮮・中国共同攻撃の状況も確認された。韓国政府は一部機関を通じて対応に乗り出した。**アンラボは当該攻撃を分析した「Larva-25010 – APT Down 攻撃者 PC 分析報告書」を公開した。**

25年8月 カード会社E、顧客個人情報流出被害

カード会社Eは297万人の顧客個人情報が流出する大規模なセキュリティ事故が発生した。このうち28万人はカード番号、有効期限、CVC、パスワードなど決済に直接使用可能な機密情報も流出した。攻撃者はオンライン決済サーバーにマルウェアと Web シェルを仕込んでデータを窃取した。合計200GBの情報が外部に流出したことが確認された。

E社は被害顧客へのカード再発行、年会費免除、無利息分割払い、全額補償などの措置を実施し、今後5年間で1,100億ウォン規模のセキュリティ投資を約束した。

主要内容

- 金融機関D、Gunraランサムウェアに感染 – 金融サービス中断を経験したが復旧ツールで復旧成功
- 攻撃グループ APT Down による韓国企業や機関への長期潜伏 – アンラボの分析レポートを発行
- カード会社E、297万人の顧客個人情報流出 – 合計200GBに及ぶ情報が外部に流出

2025年のサイバー脅威動向

攻撃グループの動向 - ダークウェブ Top 8

アンラボはダークウェブでサイバー脅威関連の問題を監視・分析し、AhnLab TIP でコンテンツとして提供している。以下は、最近1年間のダークウェブ動向を通じて把握した攻撃グループ関連のインサイトである。

1. ランサムウェア生態系の分断化と小規模グループの増加

2025年、ランサムウェア生態系は根本的な構造変化を経験した。ロックビット（LockBit）などの大型グループが捜査機関の集中取り締まりで大きく萎縮し、ランサムハブ（RansomHub）が内部対立で公式活動を停止したためである。

その反動で40以上の小規模・新興グループが大量に登場した。過去の少数大型グループ体制が Akira、Qilin、Play、Gunra などに再編されたのである。小型グループは既存の流出 LockBit 3.0、Conti ソースコードなどを再利用しながら独自ブランドで活動する。彼らは大型攻撃グループよりも攻撃的で予測不可能な交渉戦略を駆使する。一部は復号化ツールすら提供せず、被害が拡大している。

ランサムウェアの生態系は、中央集権型から分散型へと進化している。従来の IoC ベースの検知が限界に達する中、既存の防御戦略も全面的な再構築が必要だ。

2. RaaS・ホワイトラベルベースのランサムウェアカルテル

2025年のランサムウェア生態系における最大の変化は、ホワイトラベルモデルに基づく「ランサムウェアカルテル」の登場である。**このモデルでは、中央プラットフォームが暗号化ツール、データ流出インフラ、交渉ツールを提供し、加盟組織は自社ブランドで攻撃を実行し、収益の20%のみを支払う。**これは既存の RaaS における30〜40%の収益分配よりもはるかに有利な条件となっている。 このモデルは Global Group、Anubis などランサムウェア生態系全体に広かった。

攻撃者は技術的専門性やインフラ構築の負担なく「フランチャイズ」形態で攻撃を実行可能となり、参入障壁が低下した。その結果、攻撃頻度と多様性が増加し、攻撃者のブランドだけでは攻撃グループの特定が困難になった。

主要内容

- ランサムウェア生態系の分断化 - LockBit などの大型ランサムウェアグループの縮小は、複数の小規模グループの台頭につながっている
- ホワイトラベルモデルに基づくランサムウェアカルテル – 系列会社に有利な収益分配、手軽なフランチャイズ形態での攻撃実行

2025年のサイバー脅威動向

攻撃グループの動向 - ダークウェブ Top 8

3. 国家支援型 APT とランサムウェア生態系の融合

2025年、**国家が支援する APT グループが民間ランサムウェア生態系に本格参入した。**国家レベルのサイバースパイ活動と金銭的サイバー犯罪の境界が崩壊したことを意味する。

Microsoft は、北朝鮮 APT グループ Moonstone Sleet が自社のランサムウェア FakePenny に代わり、ロシア系 Qilin ランサムウェアの配布を開始したと発表した。北朝鮮系グループ Andariel が Dtrack バックドア設置後に Play ランサムウェアを配布した事例もあった。**APT グループが初期侵入を担当し、RaaS 系列組織が金銭強要を担う分業構造が確認されたのである。**

APT グループの高度な侵入技術と RaaS の効率的な金銭要求メカニズムが結合されると、攻撃成功率と被害規模を急増させる可能性がある。防御側の分析は困難になり、国際社会の制裁対象国が体系的な収益源として利用するリスクも高まる。

4. 国際捜査協力と生態系の再編

2025年、捜査機関間の国際協力はサイバー犯罪生態系に大きな打撃を与えた。**通称エンドゲーム作戦（Operation Endgame）は2024年5月に開始され、2025年5月に第2段階へ拡大。DanaBot、Qakbot、Trickbot など主要マルウェアインフラを集中攻撃した。**

2025年5月だけで300台のサーバーと650のドメインを遮断した。サイバー犯罪者20名に対する国際逮捕状を発付し、約405万ドル相当の暗号資産を押収、総押収額は約2,453万ドルに達した。

BreachForums 運営者5名とXSSフォーラム管理者を逮捕するなど、ダークウェブインフラにも打撃を与えた。**これは LockBit、RansomHub などの大型攻撃グループの崩壊につながった。**

5. ランサムウェアグループ内部の分裂

2025年、ランサムウェアの生態系は内部信頼の崩壊により大きな打撃を受けた。代表的な事件は5月に発生した **LockBit 管理者パネルのハッキングである。ビットコインウォレットアドレス6万件、被害者・系列会社との交渉記録208件、および系列会社のアカウント情報が流出した。**Qilin と Black Basta の内部ツールとチャットログが流出することで、運営方式が競合他社に晒される事態も生じた。

さらに、被害企業が身代金を支払っても正常に動作しない復号ツールを受け取るか、全く受け取れないケースも増加した。これにより、ランサムウェア系列組織間の運営者不信が高まり、独立して活動したり競合グループに移籍して内部情報を流出させる裏切りが日常化した。こうした内部分裂が小規模グループの乱立の原因となった。

主要内容

- 国家が支援する APT とランサムウェア連合 – APT グループが初期侵入、ランサムウェアグループが金銭要求を担当
- 国際捜査機関の連携でサイバー犯罪生態系を集中攻撃 – LockBit、RansomHub などが崩壊
- ランサムウェアグループ間のハッキング及び内部分裂、小規模グループの乱立へとつながる

2025年のサイバー脅威動向

攻撃グループの動向 - ダークウェブ Top 8

6. サプライチェーン攻撃の高度化と拡大

2025年のサプライチェーン攻撃は2024年比で高度化・大規模化した。ソフトウェアを超え、クラウドサービス、MSP、セキュリティソリューション提供企業にまで拡大している。 最も代表的な事例は攻撃グループ CLOP によるCleo MFT プラットフォームのゼロデイ脆弱性悪用である。今年1月には、たった一度の攻撃で182社を同時に侵入する大規模攻撃を敢行した。また、CLOP による Oracle EBS 脆弱性悪用も増加した。CISA は Oracle Cloud 認証情報の流出による連鎖的侵害リスクを公式に警告した。

攻撃グループ DragonForce と Scattered Spider はクラウド MSP を直接標的にした。SimpleHelp の脆弱性を悪用し、ソーシャルエンジニアリング手法で IT 管理者を騙してリモートアクセス権限を確保した。その結果、一つの MSP 侵害で数十の顧客企業が同時に被害を受ける「連鎖サプライチェーン攻撃」が実現した。

7. ダークウェブ生態系の不安定性

2025年、ダークウェブ生態系は前例のない不安定性を経験した。従来の捜査機関対犯罪組織の構図から、犯罪組織間の攻撃まで日常化する中、生態系自体が混乱に陥った。

今年3月、攻撃グループ DragonForce は競合グループRansomHub のデータ流出サイト（Data Leak Site, DLS）をハッキングした。 4月には BlackLock と Mamona の DLS も改竄（deface）し、内部チャットログとバックエンド設定を流出させた。研究者らはDragonForce が競合グループの AI 生成バックエンドコードの脆弱性を悪用したと明らかにした。 興味深いのは、Everest と LockBit のサイトが同じメッセージ「Don't do crime CRIME IS BAD xoxo from Prague」で改ざんされた点だ。これは攻撃グループに対する組織的な攻撃の可能性を示唆している。

8. 地政学的紛争に連動したハクティビスト活動の急増

2025年には、地政学的紛争のサイバー空間への拡散が大幅に激化し、組織化進んだ。 親ロシア攻撃グループ NoName057(16)は NATO 諸国を継続的に攻撃した。Dark Storm Team は NATO の電力インフラを攻撃し、物理的影響を及ぼす段階にまで至った。 対抗陣営では、IT Army Ukraine がロシア通信会社 UIS に DDoS 攻撃を行い、72時間にわたるサービス障害を引き起こした。

中東ではイラン・イスラエル戦争が激化する中、ハクティビスト活動が増加した。Holy League や 313 Team などの攻撃グループがイスラエルの病院や中央銀行を攻撃した。 #OpIsrael 2025キャンペーンは大規模サイバー攻撃を予告し、実際に医療機関が DDoS 攻撃を受ける事態も発生した。このほか、インド・パキスタン紛争局面では Indian Cyber Force がパキスタン銀行と警察庁のハッキングを行ったと主張した。

主要内容

- サプライチェーン攻撃、ソフトウェアからクラウド、MSP などへ拡大 – 1社の侵害で多数の顧客企業に打撃
- DragonForce、競合グループ RansomHub の DLS をハッキング – 攻撃グループ間の組織的攻撃の可能性
- ロシア対ウクライナ＋NATO、イラン-イスラエル、インド-パキスタンなどでハクティビスト活動が急増

2025年のサイバー脅威動向

攻撃グループの動向 – APT：全体動向

2025年は昨年と同様に北朝鮮 APT グループの活動が活発だった。最も多く報告されたグループはラザルス（Lazarus）で、計31件の情報が公開された。このグループは複数のサブグループが存在するため言及が多く、サブグループを区別すれば件数は変わる可能性がある。 次いでキムスッキー（Kimsuky）が27件、TA-RedAnt が17件言及された。中国とロシアのAPT グループの活動も活発だった。マスタングパンダ（Mustang Panda）が11件、APT 28が10件、ガマレドン（Gamaredon）も10件の情報公開があった。 このほか、インドとパキスタンの APT グループの活動も継続的であり、**地政学的対立の高まり**が要因と見られる。パキスタンの Transparent Tribe グループが17件で顕著であった。

同じ期間の APT グループ活動を国別に集計した結果、北朝鮮が86件で最多となった。中国が27件、ロシアとインドが18件、パキスタンが17件で続いた。 イランは9件と比較的少なかった。これらの主要国以外の攻撃グループも32件存在した。グローバルな脅威環境において、多様な国家ベースのグループが活発に活動していることがわかる。また、報告書の公開回数が少ないからといって活動が少ないと断言できない。密かに活動する APT グループは関連情報が確認されない場合もある。さらに、政府機関に対する攻撃は政策上公開しないこともある。

	APTs	10/24	11/24	12/24	01/25	02/25	03/25	04/25	05/25	06/25	07/25	08/25	09/25
North Korea (86)	Andariel	2		1	1	1							
	Kimsuky	3	4	6	2	2	2			2	2	2	2
	Konni	2					2	1	1				
	Lazarus	5	2	2	4	3	4	1		2	2	4	2
	TA-RedAnt	2	1		2	1	4		1		2	3	1
China (27)	APT41	1	1					1	1	1	1	1	
	MirrorFace		2		1		1	1					
	Mustang Panda				2	2		3		1			3
	Salt Typhoon		1			1			1	1			
Russia (18)	APT28	2	1						3	1	2		1
	Gamaredon			4			1	1			1	1	
Iran (9)	Charming Kitten		2	1					1				
	MuddyWater		1			1					1	1	1
India (18)	Bitter	1	1	1					1	1		1	
	SideWinder	1					1		2			1	2
	Viceroy Tiger	1	1		1	1					1		
Pakistan (17)	Transparent Tribe		1	1			1	1	4	4	2	3	

[表] 国別APTグループ月別活動件数 (2024年10月～2025年9月)

2025年のサイバー脅威動向

攻撃グループの動向 – APT：全体的な動向

APT グループは地政学的紛争地域を中心に活動する。韓国-北朝鮮、インド-パキスタン、中国-東南アジア、ロシア-ウクライナ、イスラエル-中東などでサイバー攻撃が集中する理由だ。**政府、軍、外交、防衛産業、金融、エネルギー、通信、教育、NGO など高価値組織を**標的とする。

初期侵入手法は、依然としてメールベースのスピアフィッシングが主流である。LNK、ISO、MSC、PDF、CHM、ZIP など多様な形式の悪性添付ファイルが使用される。ソーシャルエンジニアリング技法を活用し、偽の採用情報、政策文書、セキュリティ通知、公文書などに偽装し、カスタマイズされた餌文書やイベントを用いる。

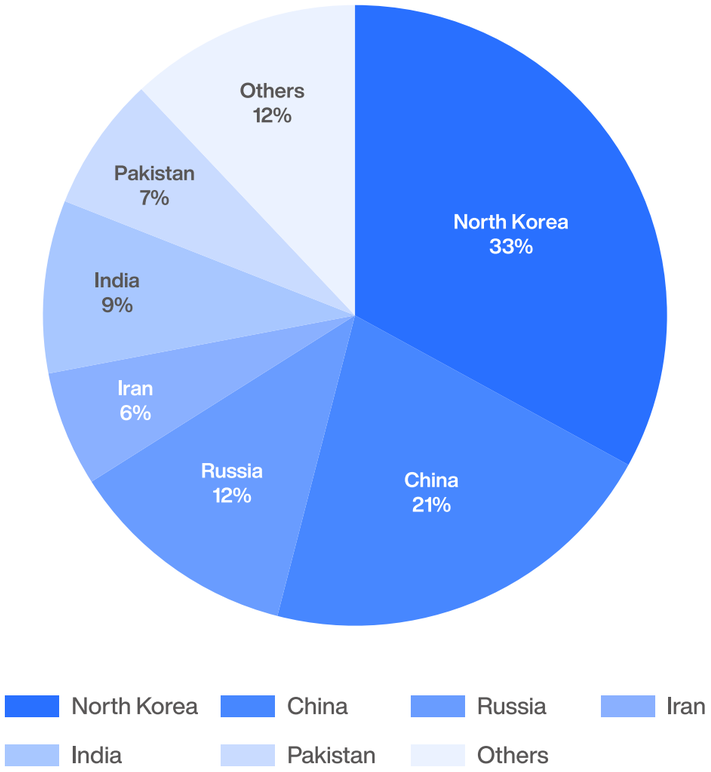
これに加え、**多様なマルウェアと正規ツールを使用する。**マルウェアは主にリモートコントロール、バックドア、キーロガー、情報窃取型マルウェアを活用する。PowerShell、VBS、バッチスクリプト、オープンソースツール（Sliver、Mimikatzなど）も攻撃プロセスに含まれる。マルチプラットフォームキャンペーンのため、Windows、Linux、macOS、Android 向けマルウェアを状況に応じて活用する

また、これらは持続性の維持、検知回避など高度な手法で武装している。以下はAPTグループが主に使用する攻撃手法である。

- タスクスケジューラ/レジストリ登録
- サービス/オブジェクトモデル(COM)ハイジャック
- UAC（ユーザーアカウント制御）の回避
- ファイルレス実行
- DLLサイドローディング
- JPEG ステガノグラフィ
- VM/サンドボックス検知回避
- ログ削除

GitHub、Dropbox、Google Drive、Telegram、Cloudflare、Outlook などの正規サービスとクラウドインフラを活用して C2 通信やデータ漏洩を行うこともある。また、DNS/DoH、TOR、VPN などを活用して攻撃活動を隠蔽する。

彼らの最新の攻撃手法のトレンドとしては、AI を利用したディープフェイク、MFA 回避（AiTM、OTP 窃取）、サプライチェーン攻撃、ウォーターホール攻撃、IoT 機器への侵入、攻撃の自動化・大量化、正常サービスへの偽装などがある。公開されたツールと独自開発のマルウェアを組み合わせて使用している。

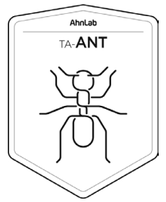


[図] 国別APTグループ活動割合 (2024年10月～2025年9月)

2025年のサイバー脅威動向

攻撃グループの動向 – APT：北朝鮮

北朝鮮の APT グループは、政治・外交・金融・暗号通貨など様々な産業を対象に金銭的利益と情報収集を狙う。 スピアフィッシング、サプライチェーン攻撃、マルチプラットフォームマルウェア、権限昇格、MFA 回避など高度な攻撃手法を活用するのが特徴である。また、正規文書及び署名の悪用、ステガノグラフィー、ファイルレス実行、多段階難読化を通じて検知を回避し、長期的な侵入基盤を確保する。



北朝鮮

Kimsuky

2025年、Kimsuky グループは様々な国と産業を標的とした高度なサイバー攻撃を実行した。**講演依頼書やインタビュー要請を装ったスピアフィッシングを通じて、ISO、LNK、MSC など多様な形式のファイルを**配布した。MSC ファイルを活用した Google ドライブベースのフィッシングと VbsEdit 署名の悪用が特徴的であった。

GitHub、Facebook、Telegram など多様なチャネルを活用した多段階攻撃と AI ベースの偽造身分証使用も新たに確認された。また、PebbleDash、RDP Wrapper、Proxy マルウェアを通じて遠隔制御を強化した。日本対象攻撃では AsyncRAT の亜種を使用することもあった。

Kimsuky には複数のサブグループが存在する。Larva-24005 は Kimalogger を利用してユーザーのキー入力を収集した。Larva-24009 は LNK ベースの攻撃を実行し、QuasarRAT や UltraVNC などを活用した。Larva-25001 は正常な文書を装った LNK ファイルで HttpSpy やMemload などのマルウェアを感染させた。

Andariel

Andariel グループは複数の国を対象に金銭的目的の攻撃を継続している。2024年の米国司法省による起訴後も活動を停止していない。**米国民間企業を対象に Preft および Nukebot バックドアを活用した侵入を行った記録がある。**Sliver、Chisel、PuTTY などのオープンソースツールとキーロガー、Mimikatz を活用した資格情報窃取手法を用いた。**Play ランサムウェアインフラを通じてランサムウェアを配布したこともある。**

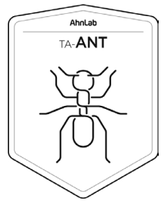
韓国では資産管理及び文書中央化ソリューションを対象に ModeLoader 及び SmallTiger マルウェアを配布した。RDP アクセス及び隠しアカウント生成を通じて長期的な侵入基盤を構築した。Apache Tomcat 脆弱性を悪用した Web シェル設置、Advanced Port Scanner によるネットワーク探索なども確認されている。 特に、RID ハイジャック手法で低権限アカウントを管理者権限に昇格させ、CreateHiddenAccount ツールでバックドアアカウントを追加した点は注目に値する。PsExec によるリモートコマンド実行、REGINI を活用した SAM レジストリ操作など、高度な内部侵入技術も使用した。韓国セキュリティ企業S社の証明書を窃取し、マルウェアに署名する手法で信頼基盤を悪用した事例も確認されている。

主要内容

- Kimsuky、スピアフィッシングによる多様なマルウェア拡散、偽装ドメイン及び悪意のある文書活用を継続
- Kimsuky は複数のサブグループを擁し、より多様なサイバー攻撃を仕掛ける
- Andariel、米国民間企業を対象にバックドアを利用した侵入
- Play ランサムウェアインフラを通じてランサムウェアを配布

2025年のサイバー脅威動向

攻撃グループの動向 – APT：北朝鮮



北朝鮮

Konni

Konni は昨年末から2025年まで、**ウクライナを含む高価値標的に対し、LNK ファイルベースのスピアフィッシング攻撃を集中的に展開した。**攻撃は、税務・市場分析などのキーワードを活用したソーシャルエンジニアリング手法と、PowerShell および AutoIt スクリプトを通じて悪意のあるペイロードを密かに実行する仕組みだった。特に、ZIP 圧縮ファイルに偽装したショートカットを含め、ユーザーが実行時に多段階ロードされるようにしてマルウェアを配布した。

Konni は WordPress ベースの C2 インフラを活用し、Konni RAT、Amadey、Lilith RAT、AsyncRAT など多様な遠隔制御型マルウェアを配布した。感染持続性の維持のために、Avast アンチウイルスの検知回避、スタートアップディレクトリの自動実行、隠しディレクトリの生成、レジストリキーの登録などの手法を使用した。また、大量の悪性サンプルを自動生成して異なるタイミングで配布し、検知回避のために難読化と暗号化を組み合わせたペイロードを使用した。

ソーシャルエンジニアリングの側面では、韓国政府を装ったメールやウクライナ政府を標的とした攻撃が確認された。 PHPMailer を活用して送信者情報を偽装し、正常な文書に悪意のあるスクリプトを組み込み、被害者を欺いた。Konni は単純な情報窃取を超え、システム制御、資格情報の収集、ネットワーク偵察を実行し、長期的な侵入のための持続性確保戦略を強化した。

Lazarus

Lazarus グループは2024年から2025年にかけて、暗号通貨、金融、IT、防衛など様々な産業を対象に攻撃を拡大した。**特に macOS と Linux に対応するマルチプラットフォームマルウェアを多数開発した。**Electron とTauri フレームワークを活用した新たなバックドア及び情報窃取ツールも公開した。 主なマルウェアには InvisibleFerret、BeaverTail、OtterCookie、CookiePlus、FrostyFerret などがある。これらのマルウェアはキーロギング、クリップボード監視、ブラウザキャッシュ及び暗号通貨ウォレット情報窃取機能を含む。攻撃手法ではサプライチェーン攻撃とウォーターホール攻撃が顕著であった。

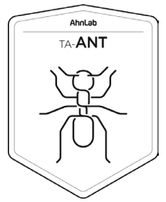
韓国ではソフトウェアの脆弱性を悪用した Operation SyncHole キャンペーンを通じて、少なくとも6つの産業組織が侵害された。また、npm、PyPI、GitHub などのオープンソースエコシステムを通じて悪意のあるパッケージを配布し、開発者と企業を感染させた。ソーシャルエンジニアリングの手法も進化し、ClickFix & ClickFake Interview などの偽の面接キャンペーンと高度な心理戦術で被害者を誘引した。 技術的には、多段階難読化、VMProtect・Confuse r難読化、拡張属性(xattr)隠蔽、JPEG ステガノグラフィー、ファイルレス実行、DLL サイドローディング、TxF ベースの Process Doppelganging など、検知回避及び持続性確保技術が目立った。また、MFA 回避、OTP 窃取、クラウドインフラ悪用なども主な変化として現れた。

主要内容

- Konni、LNK ファイルベースのスピアフィッシング攻撃を集中的に展開
- WordPress ベースの C2 インフラを活用し、様々なリモートコントロール型マルウェアを配布
- Lazarus、macOS と Linux に対応するマルチプラットフォームマルウェアを多数開発
- 韓国でソフトウェア脆弱性を悪用した Operation SyncHole キャンペーンにより、少なくとも6つの産業組織を侵害

2025年のサイバー脅威動向

攻撃グループの動向 – APT：北朝鮮



北朝鮮

TA-RedAnt

TA-RedAnt は2024年から2025年にかけて、東アジア、南アジア、中東、ヨーロッパなど様々な地域へ攻撃を拡大した。該当地域では**政治・外交・国防・金融・医療・エネルギー・教育など多様な産業を標的とした。** TA-RedAnt もまた、ScarCruft（APT37）、SideWinder、Transparent Tribe（APT36）、UNC3886（Fire Ant）など複数のサブグループを含む。

スピアフィッシング、ウォーターホール攻撃、採用偽装、悪性文書（HWP、PDF、ISO、LNKなど）、悪性インストールファイル及び圧縮ファイル（EGG、ZIP）、クラウドリンク、Github/Dropbox ベースの C2 など多様な攻撃手法を使用する。 特に、JPEG 画像にマルウェアを隠すステガノグラフィー、ファイルレス実行、DLL サイドローディング、TxF ベースのプロセスドッペルゲンガー、トランザクテッド・ホローイングなど、高度化された隠蔽および持続性確保技術を新たに導入した。

新たに確認された内容としては、Rust ベースのバックドア（Rustonotto、CHILLYCHINO）、VCD ランサムウェア、PubNub/Ably メッセージングC2、LLM ベースのマルウェア（LAMEHUG）、MFA 回避（AitM、OTP 窃取）、A I画像・音声改ざん、Python コード難読化などがある。 また、.desktop ファイルを活用した Linux 攻撃、WebSocket ベースの C2、Google ドライブを介したペイロード伝達など、マルチプラットフォーム攻撃が増加したことも特徴である。

彼らのソーシャルエンジニアリング手法も進化を続けている。実在人物のなりすまし、学術イベントやニュースレターの偽装、メッセンジャーのグループチャット活用、リンクのないメールなどで疑念を最小化する。攻撃の自動化と検知回避能力も強化した。正常な文書・アプリ・署名プログラムの偽装、クラウド・正常サーバーベースのC2構築、多段階復号化・難読化、自己削除及び一時フォルダ隠蔽などの技術も使用する。

TA-RedAnt は様々なマルウェアやツールを活用し、認証情報、システム情報、暗号通貨、文書、オーディオ、USB/MTP データなどを窃取した。**一部の被害組織にはランサムウェアを感染させ、金銭的被害をもたらした。** 今後も攻撃手法を継続的に進化させ、主要なグローバル脅威として定着する見込みである。

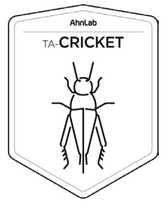
主要内容

- 政治、外交、国防、エネルギーなど多様な産業を標的
- スピアフィッシング、悪意のあるインストールファイル、クラウドベースの C2 など多様な攻撃手法を使用
- JPEG ステガノグラフィー、ファイルレス実行、DLL サイドローディングなど、隠蔽および持続性確保技術の高度化
- 一部の被害組織にはランサムウェアを感染させ、金銭的被害を与えた事例が存在

2025年のサイバー脅威動向

攻撃グループの動向 – APT：中国

中国の APT グループは政府機関、外交、軍事、産業分野を対象に長期的・戦略的な情報収集及び監視を実施する。ゼロデイ脆弱性、サプライチェーン攻撃、マルチプラットフォームマルウェア、クラウドインフラ悪用など高度化された技術を活用し、検知回避能力を強化する。ソーシャルエンジニアリング手法とAIベースの自動化ツールを組み合わせて、標的型フィッシング及び攻撃キャンペーンを大量実行し、地政学的・経済的利益を同時に追求する。



中国

APT41

APT41 は過去1年間、グローバルな政府機関および産業を対象に高度な攻撃を継続した。Google Calendar を悪用した TOUGHPROGRESS キャンペーン、ClickOnce ベースの OneClik 攻撃、RunnerBeacon バックドア、Anatsa(TeaBot)トロイの木馬など多様な手法を活用し、政府機関、エネルギー・石油・ガス産業、金融機関を集中攻撃した。 また、日本企業を対象に偵察ツールと暗号化された Web シェルを配布し、アフリカ政府の IT インフラを狙った攻撃も並行して行った。**特に2024年7月には、Fortinet VPN クライアント（FortiClient）認証後にメモリに残った資格情報を抽出するゼロデイ脆弱性を悪用した事例がある。**

WordPress ベースの C2 インフラ、暗号化された HTTPS トラフィック、TLS プロトコル偽装を通じて検知を回避した。また、攻撃自動化のために大量の悪性サンプルを生成し、複数の時点にわたり配布した。 サプライチェーン攻撃とモバイルプラットフォームへの侵入を同時に行うことが特徴である。特に、iOS と Android デバイス向けに情報窃取用のカスタムマルウェアアプリを配布し、クラウドサービスアカウントを乗っ取って企業内部ネットワークへ攻撃を拡散させる。攻撃対象の言語や文化的特性を反映したソーシャルエンジニアリング手法を使用し、AI ベースの自動化ツールを活用してフィッシングコンテンツを大量生産する状況も確認された。

MirrorFace

MirrorFace は2024年6月以降、日本を中心に台湾、インド、欧州の外交機関まで攻撃対象を拡大した。**初期侵入はスピアフィッシングメールと OneDrive リンクを介した ZIP ファイル配布方式で行われる。**ZIP 内部にはマクロ文書(ROAMINGMOUSE)、ショートカットファイル、SFX 実行ファイルなどが含まれる。 SSL VPN およびファイル保存サービスのゼロデイ脆弱性（CVE-2023-28461、CVE-2023-27997など）を悪用して初期アクセスを試み、MirrorStealer、Lodeinfo、Cobalt Strike を通じて資格情報の窃取およびAD（Active Directory）サーバーへの侵入を実行する。 マルウェアは ANEL バックドア最新バージョンと NOOPDOOR、NOOPLDRなどの新規マルウェアを活用。攻撃自動化のため PowerShell スクリプトと WMI ベースのコマンド実行を組み合わせた。さらに Base64/HEX エンコーディング、WMI 実行、UAC 回避、サンドボックス回避などの検知回避手法も強化した。

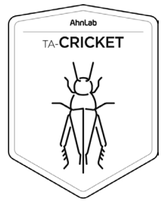
日本国内の政治家やジャーナリストを対象とした標的型フィッシングキャンペーンも実施した。攻撃インフラとしてクラウドサービスと CDN（コンテンツ配信ネットワーク）を活用し、正常なトラフィックに偽装した。日本の警察は、彼らの活動が組織的な情報収集の試みである可能性が高いと警告した。

主要内容

- APT41、FortiClient の認証情報を抽出するゼロデイ脆弱性悪用事例を報告
- WordPress ベースの C2 や暗号化 HTTPS トラフィック、TLS プロトコル偽装を用いて検知を回避
- MirrorFace、スピアフィッシングなどを通じた初期アクセス及びゼロデイ脆弱性の悪用による侵入試行
- 日本を中心に政治家やジャーナリストを対象とした標的型フィッシングキャンペーンを展開

2025年のサイバー脅威動向

攻撃グループの動向 – APT：中国



中国

Mustang Panda

Mustang Panda は2024年から2025年にかけて、東南アジア、北東アジア、ヨーロッパ、南米など様々な地域の政府、外交、軍事、NGO、学界などを対象に攻撃を拡大した。**スピアフィッシングメールと悪性文書（LNK、CHM、OneNote、PDF、HTML、ISO など）を活用して初期侵入を試みた。HTML Smuggling、USBワーム（SnakeDisk）、クラウドベースフィッシングなど多様な攻撃手法を導入した。**

マルウェアは PlugX、TONESHELL、Bookworm、PUBLOAD、MQsTTang、CCoreDoor、ShadowPad など多様なバックドアと RAT を使用した。StarProxy、PAKLOG/CorKLOG、SplatCloak、Yokai など新規ツールも多数確認された。これらは横移動、キーロギング、EDR 回避、USB 拡散機能を備えている。 検知回避手法も高度化した。正常プロセス（MAVInject.exe など）を介した DLL インジェクション、WriteProcessMemory ベースの反射型 DLL インジェクション（Reflective DLL Injection）、FakeTLS および TLS-like ヘッダーを活用した C2 トラフィック隠蔽、Cloudflare CDN・Google Drive・Box などのクラウドインフラを通じたペイロード伝達が主な特徴である。 ソーシャルエンジニアリング手法も強化した。台湾大統領選挙、モンゴル洪水、ASEAN 会議、チベット行事など地域イシューを活用したカスタマイズ型おとり文書を使用した。WebSocket C2、AES/DES ベースの多段階暗号化、Kavach OTP 奪取による MFA 回避なども新たに登場した手法である。

Salt Typhoon

Salt Typhoon は2024年から2025年にかけて、米国、アジア、中東、アフリカの通信事業者・政府・軍事・NGO を対象に長期的な監視および情報収集活動を実施した。**公開されたサーバーおよびネットワーク機器の脆弱性（CVE-2018-0171、CVE-2023-20198など）を悪用して初期アクセスを確保した。** 内部では WMIC.exe、PSEXEC.exe を活用した横方向移動を実施した。攻撃者は AD 環境における権限昇格のため、Kerberos チケット操作と Pass-the-Hash 手法を使用した。さらに、**検知回避のために正規管理ツールを悪用する Living-off-the-land（LOTL）戦略を強化した。**

悪性コードは主に GHOSTSPIDER、SNAPPYBEE、MASOL RAT を使用した。特に GHOSTSPIDER はモジュール型設計と TLS 暗号化により分析を困難にした。 また、SNAPPYBEE はクラウド API 呼び出しによるデータ漏洩を実行し、MASOL RAT はファイルレス実行と PowerShell 難読化を組み合わせて検知を回避した。2025年5月には Commvault Metallic SaaS プラットフォームのゼロデイ脆弱性(CVE-2025-3928)を悪用し、Microsoft 365 環境を侵害した。 このほか、ShadowPad・SoftEther VPN による C2 隠蔽、CAB ファイルを活用した DEMODEX Rootkit のインストール手法改良、そして正常プロセスへのインジェクションによる持続性確保技法を導入した。攻撃インフラは CDN とクラウドストレージを活用し、正常トラフィックに偽装した。攻撃自動化のため、Python ベースのスクリプトと AI 生成フィッシングコンテンツを組み合わせた状況も捕捉された。

主要内容

- MustangPanda、スピアフィッシングメールと悪性文書を活用した初期侵入。HTML Smuggling など多様な攻撃手法の導入
- 既存のツールとインフラを再利用しながら、新たなマルウェアと隠蔽技術を導入し、精巧さを強化
- Salt Typhoon、公開サーバーおよびネットワーク機器の脆弱性を活用して初期アクセスを確保
- 検知回避のための LOTL 戦略強化、マルウェア開発、トラフィック偽装、攻撃自動化など多様な戦術の高度化を進行

2025年のサイバー脅威動向

攻撃グループの動向 – APT：ロシア

ロシア APT グループは地政学的紛争を利用し、政府・軍事・外交・戦略機関を対象に長期的/組織的な攻撃を実施する。メールフィッシング、公開脆弱性悪用、クラウドインフラベースの C2 隠蔽、ファイルレス実行など高度な手法を使用し、検知回避能力が卓越している。心理戦と政治的影響力拡大のためにカスタマイズされたキャンペーンを展開し、情報窃取を超えインフラ攻撃まで図る。

ロシア

APT28

APT28 はウクライナ、NATO、東欧を中心に政府、軍事、防衛産業、技術分野を対象とした攻撃を継続した。 地政学的紛争を悪用した標的型フィッシングキャンペーンを展開し、**ロシア・ウクライナ戦争や NATO 首脳会議関連文書を偽装して利用した。**初期侵入ではメールフィッシングと脆弱性（CVE-2023-38831、CVE-2023-23397など）の悪用が顕著だった。Outlook、Roundcube、Zimbra などのメールサーバー脆弱性も積極的に悪用した。

LLM ベースのマルウェア（LAMEHUG）を使用して、コマンド自動生成と情報収集を試みた。MFA 回避（AiTM）、COM ハイジャック、UAC 回避など持続性確保技術を強化した。また、Google Drive などのクラウドインフラを活用し C2 通信を隠蔽、正常トラフィックに偽装して検知を回避した。 Python スクリプトと PowerShell 難読化を組み合わせ、悪性サンプルを大量生成する方式で攻撃を自動化した。 主なマルウェアとして HeadLace、GooseEgg、MASEPIE が確認された。これらは資格情報窃取、ネットワーク偵察、横移動機能を含む。また、Cobalt Strike、Sliver などのオープンソース攻撃フレームワークを活用し攻撃チェーンを高度化した。最近では HTML Smuggling、ファイルレス実行、JPEG ステガノグラフィによるペイロード隠蔽手法も利用した。

Gamaredon

Gamaredon グループはウクライナおよびロシア語圏のユーザーを対象に、高度化されたスピアフィッシングと情報収集活動を展開している。初期侵入は LNK、HTA、XHTML ファイルを活用したフィッシングキャンペーンを通じて行われた。ファイル実行時、PowerShell ベースのマルウェアがロードされ、システム情報を収集し追加ペイロードをダウンロードした。Cloudflare Tunnels、DNS over HTTPS（DoH）などの外部インフラを利用し C2 検知を回避した。 さらに、攻撃の自動化のために Python スクリプトと PowerShell の難読化を組み合わせた。**新規マルウェアである GammaDrop、GammaLoad、GammaSteel は、難読化、レジストリ隠蔽、USB ドライブの武器化など、精巧な手法を使用した。**特に GammaSteel は、ファイルレス実行と多段階暗号化により分析を難しくした。

モバイルプラットフォームへの攻撃も強化した。BoneSpy、**PlainGnome などの Android 監視マルウェアを通じてロシア語圏ユーザーを標的とした。**一部は Samsung Knox を偽装して企業システムを不正にアクセスした。 悪性アプリは通話記録、メッセージ、位置情報を収集し、カメラ・マイクを遠隔操作した。2025年にはウクライナ駐留の西側軍人を対象に PowerShell ベースの情報窃取を実行した。これらは単純な情報収集を超え、軍事・外交情報収集と心理戦目的の攻撃を並行する。ロシア連邦保安庁（FSB）傘下の第18情報保安センターとの連携も推定される。

主要内容

- APT28、フィッシングキャンペーンを展開、ロシア・ウクライナ戦争及び NATO 首脳会議関連文書を偽装して利用
- LLM ベースのマルウェア(LAMEHUG)を使用して、コマンド自動生成と情報収集を試みる
- Gamaredon、難読化、レジストリ隠蔽、USB ドライブの武器化など高度な手法を実行するマルウェアを使用
- モバイル向け攻撃を強化、Android 監視マルウェアを通じてロシア語圏ユーザーを狙った

2025年のサイバー脅威動向

攻撃グループの動向 – APT：イラン

イランの APT グループは中東とヨーロッパを中心に、外交、メディア、人権団体及び政府機関を対象とした長期攻撃を展開している。スピアフィッシング、HTML Smuggling、ファイルレス実行、MFA 回避、OTP 窃取など高度な手法を使用する。クラウドインフラとステガノグラフィーを通じて検知回避能力も強化した。Android マルウェアと AI ベースのフィッシングコンテンツを組み合わせ、モバイル端末まで攻撃範囲を拡大した。

イラン

Charming Kitten

Charming Kittenは中東とヨーロッパを中心に、外交、メディア、人権団体を標的とした攻撃を実行した。初期の侵入にはソーシャルエンジニアリング手法に基づくフィッシングと悪意のある文書の配布が活用された。**LNK ファイルと PowerShell を組み合わせた多段階ロード手法も新たに追加された。**JPEG 画像にステガノグラフィを仕込み、マルウェアを隠蔽して検知を回避のため、ファイルレス実行手法が積極的に活用された。

Charming Kittenは、**MFA 回避と OTP 窃取技術で認証体系**を無力化し、AiTM（中間者攻撃）ベースのフィッシングサイトを運営してリアルタイムでセッションをハイジャックした。クラウドベースの C2 通信は Dropbox、Google Drive、Telegram API を活用し正常トラフィックに偽装した。さらに TLS 暗号化と DNS over HTTPS（DoH）を組み合わせてネットワーク検知を回避した。 悪性コードは主に POWERSTATS、NokNok、CharmPower を使用し、キーロギング、ブラウザクッキー窃取、システム情報収集機能を含む。

MuddyWater

MuddyWater は中東、欧州、南アジア地域の政府、外交、通信、産業組織を標的とした攻撃を続けた。**彼らは Living-off-the-land（LOTL）手法を積極的に活用し、PowerShell や MSHTA などの正規ツールを用いて初期侵入とコマンド実行を行った。**スピアフィッシングメールを通じて悪性 LNK ファイルを配布し、正規文書と悪性スクリプトを結合することで検知を回避した。 さらに、Ligolo、SimpleHelp、Venom Proxy などの**オープンソースツールを活用した C2 通信を強化した。VPN とリモート管理ツール（RMM）を介した内部拡散も確認された。**特に、BugSleep（MuddyRot）バックドアを使用して既存の Atera RMM を置き換え、攻撃の自動化のために Python ベースのスクリプトと PowerShell の難読化を組み合わせた。 ファイルレス実行とメモリ内マルウェアロード方式もこれらの攻撃の主要な特徴である。検知回避には正常プロセスへのインジェクションとUAC 回避技法が使用された。

主なマルウェアとしてMuddyC2Go、BugSleep、SimpleHelp RAT が確認された。これらのマルウェアは資格情報の窃取、キーロギング、ネットワーク偵察機能を含む。また、DNS over HTTPS（DoH）と TLS 暗号化を活用して C2 トラフィックを隠蔽し、クラウドサービス（Google Drive、Dropbox）を通じてペイロードを配信した。 攻撃インフラでは、CDN と正規ウェブサイトを悪用したウォーターホール攻撃手法が使用された。

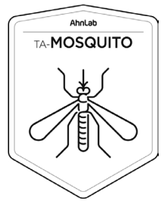
主要内容

- Charming Kitten、ソーシャルエンジニアリング手法に基づくフィッシングと悪意のある文書の配布 - LNK ファイルと PowerShell を組み合わせた多段階のロード方式を新たに追加
- MFA 回避と OTP 窃取技術による認証システムの無力化
- MuddyWater、LOTL 手法を活用し正常ツールで初期侵入とコマンド実行
- オープンソースツールを活用した C2 通信の拡張、VPN とリモート管理ツールによる内部拡散

2025年のサイバー脅威動向

攻撃グループの動向 – APT：インド

インド APT グループは南アジア・中東地域の政府・軍事・外交機関を標的とした長期攻撃を展開している。スピアフィッシング、HTML Smuggling、PowerShell難読化、DLLサイドローディング等の高度化手法を活用し、クラウドインフラとステガノグラフィーを通じて検知を回避する。Android マルウェアを使用したマルチプラットフォーム攻撃を実行し、AI ベースのフィッシングコンテンツの組み合わせなどを通じてソーシャルエンジニアリング手法も高度化している。



インド

Bitter

Bitter は南アジアと中東地域の政府、軍事、外交機関を継続的に攻撃を展開した。初期の侵入は悪意のある文書と LNK ファイルを活用したメール攻撃を通じて行われた。**HTML Smuggling と PowerShell ベースのマルウェアを新たに使用し、検知回避能力を強化した。**正規文書に悪性スクリプトを組み込み、被害者を欺いて多段階ロード手法でペイロードを隠蔽した。

Bitter は、**Android マルウェアを活用し、モバイル端末まで攻撃範囲を拡大した。彼らの悪性アプリは金融情報、メッセージ、位置データを窃取し、カメラ・マイクを遠隔操作する機能も備えていた。**クラウドベースの C2 通信は Google Drive、Dropbox、Telegram API を活用し、正常なトラフィックに偽装した。TLS 暗号化と DNS over HTTPS(DoH) を組み合わせ、ネットワーク検知を回避した。 AiTM（中間者攻撃）ベースのフィッシングサイトと OTP 窃取により MFA を回避した。マルウェアは主に AridViper 亜種、BitterRAT、VajraSpy を使用した。これらはキーロギング、ブラウザクッキー窃取、システム情報収集機能を提供する。 Python スクリプトとPowerShell の難読化を組み合わせて大量の悪性サンプルを生成し、攻撃を自動化した。ソーシャルエンジニアリングに基づくカスタマイズされたおとり文書も多様化した。特に、政府政策文書、外交交渉資料、軍事報告書を装ったメールが多数発見された。

Sidewinder

Sidewinderグループは南アジア、東南アジア、中東地域の政府、軍事、外交、エネルギー、教育機関を対象に攻撃範囲を広げた。**ウォーホーク系マルウェアを中心に、USB ワーム、キーロガー、情報窃取機能を含む多様なモジュールを開発した。**多段階ロード手法とファイルレス実行を組み合わせ、検知回避能力も強化した。 初期侵入にはスピアフィッシングメールによる悪性 LNK ファイル配布及び HTML Smuggling 手法を活用した。

PowerShell 難読化、DLL サイドローディング、TxF ベースのプロセスドッペルゲンガーなど高度な手法で検知を回避した。 さらに、Cloudflare CDNとGoogle Drive を活用して C2 通信を隠蔽し、TLS 暗号化と DNS over HTTPS(DoH) を組み合わせてネットワーク上での検知を回避した。 WarHawk、SideWinder RAT、SplatCloak マルウェアを主に使用し、これらはキーロギング、ブラウザクッキー窃取、システム情報収集、USB 拡散機能を提供する。**ソーシャルエンジニアリング手法は実在人物のなりすまし、学術イベントの偽装、グループメッセージルームの悪用などへ進化した。**攻撃者は被害者と信頼関係を構築するため、多段階にわたりメールを交換した。また、攻撃自動化のために Python ベースのスクリプトと AI 生成フィッシングコンテンツを組み合わせた状況も確認された。

主要内容

- Bitter、HTML Smuggling とPowerShell ベースのマルウェアを新たに使用し、検知回避能力を強化
- Android マルウェアアプリ、金融情報、メッセージ、位置データの窃取、カメラ・マイクの遠隔制御
- SideWinder、WarHawk 系マルウェアを中心に、USB ワーム、キーロガー、情報窃取機能を含む多様なモジュールを開発
- 実在人物のなりすまし、学術イベントの偽装、グループメッセージルームの悪用などソーシャルエンジニアリング手法の進化

2025年のサイバー脅威動向

攻撃グループの動向 – APT：パキスタン及びその他

パキスタン APT グループはインド、パキスタン、中東、アフリカの政府・軍事・教育・NGO を対象に長期攻撃を展開している。複数のマルウェアを活用し Windows、Linux、Android 環境を同時に攻撃した。MFA 回避及び WebSocket ベースの C2 通信で検知を回避する。クラウドインフラとステガノグラフィーで悪意のあるペイロードを隠蔽し、カスタマイズ型フィッシング、AI ベースのコンテンツ生成などソーシャルエンジニアリング手法を高度化する。

パキスタン

Transparent Tribe

Transparent Tribe はインド、パキスタン、中東、アフリカ地域の政府、軍事、教育、NGO を対象とした攻撃を継続した。彼らは CapraRAT、CrimsonRAT、**ObliqueRAT など様々な RAT を活用し、Windows、Linux、Android 環境を同時に攻撃した。**特に Linux 環境では「.desktop」 ファイルベースの攻撃を新たに実行した。 WebSocket を利用した C2 通信で検知回避能力を強化し、Kavach OTP の窃取を通じてMFA を回避した。AiTM ベースのフィッシングサイトを活用し、リアルタイムセッションハイジャックも実行した。

Transparent Tribe はクラウドベースのインフラを積極的に活用した。Google Drive、Slack、Telegram API を介した C2 通信を強化し、TLS 暗号化と DNS over HTTPS（DoH）を組み合わせてネットワーク検知を回避した。主なマルウェアとしては CrimsonRAT、CapraRAT、ObliqueRAT に加え、Android 向け悪性アプリも確認された。攻撃者は正規アプリを装った悪性アプリを配布し、APK ファイルにステガノグラフィーを適用して悪性ペイロードを隠蔽した。さらに、カスタマイズされたおとり文書を用いてソーシャルエンジニアリング手法を多様化した。 外交交渉資料や学術イベント招待状などを装ったメールが多数発見され、被害者と信頼関係を構築するため多段階のメール交換を行った。また、攻撃自動化のために Python ベースのスクリプトと AI 生成フィッシングコンテンツを組み合わせた状況も確認された。

その他

その他に分類された APT グループは、国家ベースの分類が困難なほど活動様相が複雑多岐にわたる。政府、国防、金融、通信、教育、NGO など多様な産業を標的とし、アジア、中東、ヨーロッパ、アメリカなど全世界で活動する。これらは**共通してソーシャルエンジニアリングベースのスピアフィッシングと多様な文書フォーマットを活用した初期侵入手法を用いる。**さらに、PowerShell などのスクリプトベースのマルウェアを多段階でロードする。クラウドサービスとオープンソースインフラを積極的に活用し、特に GitHub、Dropbox、Google Drive、Telegram などを C2 として利用するケースが多い。また、Rust、Go、Python など**多様な言語で開発されたマルウェアを通じて、Windows、Linux、macOS、Android などのマルチプラットフォームを同時に攻撃する。**

高度な検知回避技術を使用する。難読化、暗号化、ファイルレス実行、DLL サイドローディング、COM ハイジャック、ログ削除、タイムスタンプ改ざんなど多様な手法が確認されている。特に、LLM ベースのマルウェア（LAMEHUG）、ClickFix、HTML Smuggling などの最新ソーシャルエンジニアリング手法や、MFA 回避、セッションクッキー窃取などの認証体系無力化技術を新たに実行した。 一部のグループは他グループのインフラを掌握したり、偽装工作（False Flag）戦略を通じて混乱を引き起こす。

主要内容

- Transparent Tribe、多様な RAT の活用および Windows、Linux、Android 環境への同時攻撃
- クラウドインフラを活用した C2 通信の強化とネットワーク検知回避
- その他のグループは共通してソーシャルエンジニアリングベースのスフィアフィッシングと多様な文書フォーマットを活用した初期侵入手法を使用
- 多様な言語で開発されたマルウェアを通じ、Windows、Linux、macOS、Android などマルチプラットフォームを同時攻撃

2025年のサイバー脅威動向

ランサムウェアの動向

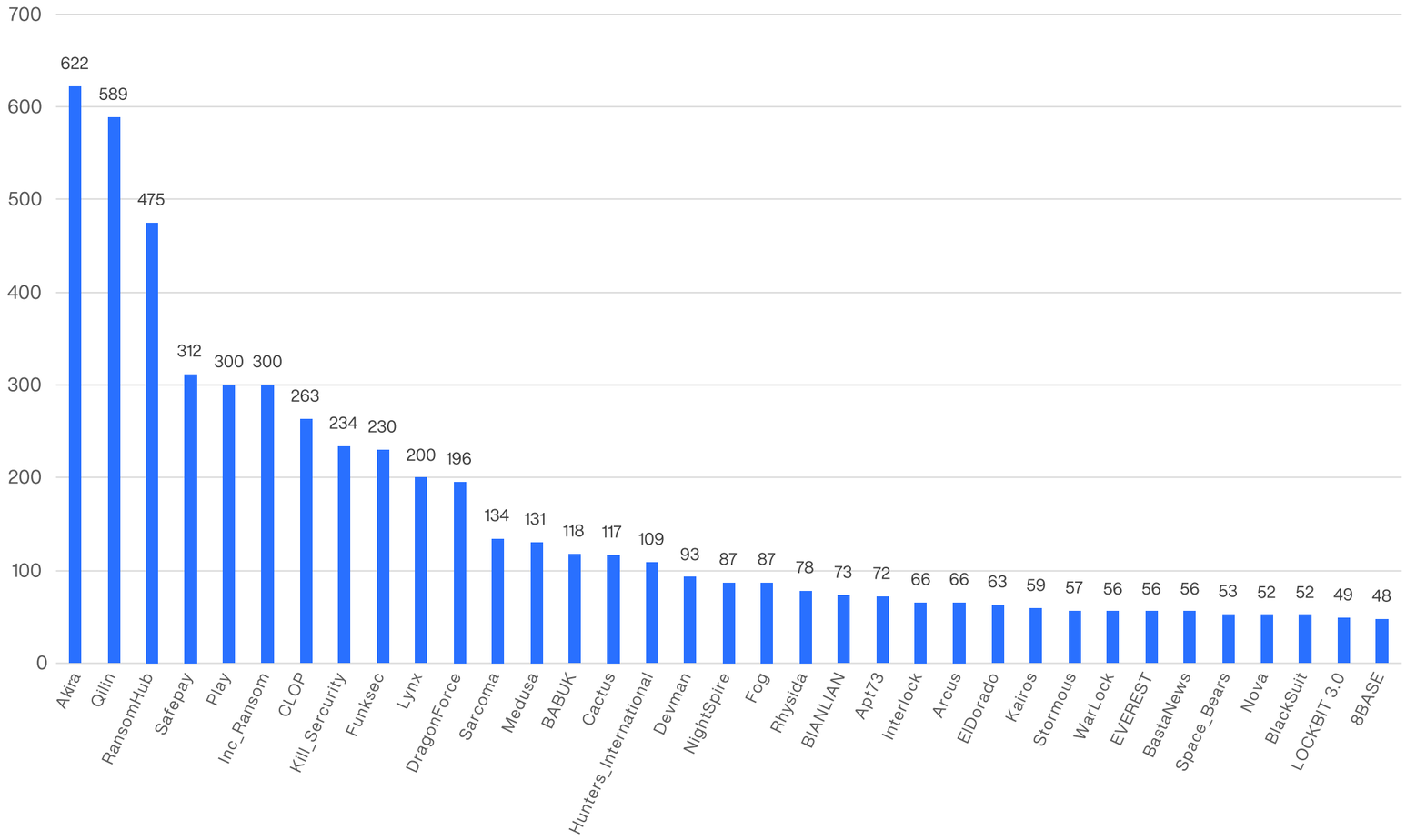
概要と動向

2025年の**ランサムウェア生態系は前年比38%拡大し、爆発的に成長した。**取り締まりなどで主要組織が被害を受けたが、活動グループ数は96件に達し、前年比26%増加した。生態系の断片化が加速した。

攻撃グループの順位にも大きな変化があった。622件の被害事例を引き起こした**Akira は前年4位から1位に躍進した。**Qilin は589件で11位から2位に急浮上した。CLOP も43位から7位に上昇した。一方、2024年1位だった LockBit は Operation Cronos の余波で30位圏外に転落した。

北朝鮮の背後にある Andariel と Moonstone Sleet が Play およびQilin ランサムウェアを配布し、**国家支援攻撃グループが RaaS に組み込まれカルテル化する様相を見せた。**金銭的利益と国際制裁回避のための新たなモデルを提示した。

2025年のランサムウェアグループ別被害企業掲載件数



2025年のサイバー脅威動向

ランサムウェアの動向

捜査機関の取り締まりと限界

今年、捜査機関のランサムウェア対応は強化されたが効果は限定的だった。Operation Cronos で打撃を受けた LockBit は2025年9月、LockBit 5.0 を発表し復活を宣言した。特に原子力・火力発電所など重要インフラ攻撃を明示的に許可し、より攻撃的な戦術へ回帰した。

RansomHub は今年4月、突然の活動停止を宣言した。2024年に攻撃回数1位だった組織が完全に消滅したのである。DragonForce が吸収を主張したが、RansomHub は DragonForce の法執行機関との協力疑惑を提起し、分裂する姿を見せた。

RansomHub の提携組織は Qilin、DragonForce、 Lynx へ移り、生態系が再編された。RaaS 生態系の強い回復力と適応力が改めて示された。

主要攻撃戦術

ランサムウェア攻撃手法は「三重搾取戦術」へと進化した。 データ暗号化・流出に加え、被害組織の顧客やパートナーに連絡して追加圧力をかける方式である。医療・金融分野では評判毀損の最大化のために集中的に使用された。

ランサムウェア攻撃手法は「三重恐喝戦術」へと進化した。データ暗号化・流出に加え、被害組織の顧客やパートナーに連絡して追加圧力をかける方式である。医療・金融分野では評判毀損の最大化のために集中的に使用された。

ゼロデイから 1-Day 脆弱性攻撃への移行も注目すべき変化だ。CLOP は Cleo MFT のゼロデイ脆弱性で400組織を侵害し、Akira は SonicWall SSL VPN 脆弱性を集中攻撃した。MFT プラットフォームと VPN 機器が新たな核心攻撃ベクトルとして台頭した。

対応策及び展望

ランサムウェアは AI ベースの自律攻撃システムと LLM を活用した戦術が高度化し、暗号化されていないデータを狙った攻撃が増加すると予想される。北朝鮮の事例をきっかけに、国家支援ハッカーとサイバー犯罪組織の協力が強化される見通しだ。

このような**ランサムウェア対策には、多層的な防御体系を構築する必要がある。** ゼロトラストアーキテクチャの導入、VPN と RDP に対する多要素認証（MFA）の適用、VMware ESXi などのハイパーバイザー環境の保護、ネットワークのマイクロセグメンテーションによる被害拡散の防止も重要である。 脅威インテリジェンスに基づく24時間365日の監視により、IAB（Initial Access Broker）の販売と実際の攻撃の間に生じる18日の時間差を活用した早期検知が必要である。物理的に分離されたオフラインバックアップと不変バックアップの確保も不可欠である。

主要内容

- 大型ランサムウェアグループは縮小したが、RaaS エコシステムは高い回復力を示す
- ランサムウェア攻撃手法は三重恐喝戦術へ進化 – データ流出脅迫に加え顧客とパートナーまで圧迫
- 進化するランサムウェア対策には多層防御システムが必要 – ゼロトラスト、MFA、TI ベースのモニタリングなど

2025年のサイバー脅威動向

ランサムウェアの動向 - 主要グループ活動 Top 10

1. 日本企業を標的とした攻撃の増加

日本は2024年10月～**2025年9月の1年間で、前年同期比で217%増加するランサムウェア攻撃を受けた。**攻撃件数が最も多かったのは Qilin で、Lynx、Nightspire、RansomHub、Akira などもセキュリティが脆弱な中小企業を標的とした攻撃を仕掛けた。

新規攻撃グループ Kawa4096 は6月末に登場直後に2つの組織を攻撃し侵害した。このグループの KaWaLocker ランサムウェアは Salsa20 暗号化、マルチスレッディング、ファイル名ハッシュ機能を備え、7月にリリースした2.0バージョンで機能を強化した。製造業が最も大きな被害を受け、中小企業が被害の大半を占めた。

2. Qilin - 圧倒的な支配力の確立

2024年に韓国と日本で報告された攻撃が確認されなかった Qilin は、2025年に数十件の攻撃を記録し、両国で最も活発な活動を示した。RansomHub が消えた空白を迅速に埋め、行き場を失っていたアフィリエイトを多数取り込んだ。**韓国では「Korean Leak」キャンペーンで IT サプライチェーンを狙い、29社の中小資産運用会社に攻撃を仕掛けた。**

特に、**北朝鮮の背後にある Moonstone Sleet は2月から Qilin ランサムウェアを配布し、国家支援型脅威グループへと発展した。**9月には DragonForce、LockBit とカルテルを形成し、市場支配のための協力体制を構築した。

3. Play - 北朝鮮 Andariel との結合

Play ランサムウェアは2024年10月、北朝鮮の背後にいる Andariel との協力が確認された。**国家支援グループがRaaSインフラを活用した初の事例であった。**Andariel は5月に被害組織に侵入後、Sliver C2 フレームワークと Dtrack バックドアを配布して潜伏し、9月に Play ランサムウェアを最終配布した。

2025年上半期、FBI は約900の組織が Play ランサムウェアの被害を受けたと発表した。北朝鮮は WannaCry 以降、ランサムウェアを資金調達手段として活用しており、Play との協力は国際制裁を回避する新たな戦略と評価されている。

主要内容

- 日本を標的としたランサムウェア攻撃が前年同期217%増加 - 製造業が最も大きな打撃を受け、中小企業の被害も多数
- 北朝鮮の背後にいる Moonstone Sleet が2月から Qilin ランサムウェアを配布し、国家支援型脅威グループへ発展
- Play ランサムウェア、北朝鮮の Andariel と協力 - 国家支援グループが RaaS インフラを活用した初の事例

2025年のサイバー脅威動向

ランサムウェアの動向 - 主要グループ活動 Top 10

4. Akira – SSL VPN 攻撃

Akira は2025年、着実な成長率を維持し攻撃数で1位に立った。2024年の散発的な大量データ流出パターンから脱却し、2025年第1四半期からは定期的な少量流出へ戦術を変更した。

最も注目すべき事件は、7月から始まったソニックウォール SSL-VPN 機器への集中攻撃である。CVE-2024-40766 脆弱性を悪用し、世界的に攻撃を仕掛けた。8月には米国組織において、ネットワークスキャン、横移動、権限昇格、データ流出が連鎖的に確認された。

VMware ESXi 仮想化環境への攻撃にも特化しており、クラウドインフラを広く暗号化する能力を有していた。Rust ベースの新種（Akira v2）を開発し、高度な難読化技術を適用した。また、PowerTool 悪用、ログ削除など多様な EDR 回避技術を駆使した。 製造業、教育、医療分野を主な標的とし、2025年上半期に数十の組織を攻撃し、代表的な攻撃グループとしての地位を確立した。

5. Lynx - 製造業への集中攻撃

Lynx は2024年7月、INC ランサムウェアコードをリブランディングして登場した。2025年の被害者数は96件（1月）から300件（8月）へ急増した。6月から Sinobi という名称で複数ブランド戦略を展開し始めた。**製造業と建設業を主な標的とし、米国が全被害国の60%を占めた。**

1月には米国の法律事務所を攻撃し顧客の機密情報を窃取、12月にはルーマニアのエネルギー供給会社を停止させた。倫理的ハッキングを標榜するが、実際には二重恐喝戦術を用い、機会主義的で無差別な攻撃を仕掛ける。

6. LockBit – バージョン5.0で復活

LockBit は2024年2月の「Operation Cronos」以降、深刻な打撃を受けた。その後2025年9月、6周年を迎え LockBit 5.0 として復活を宣言した。**新バージョンは Windows、Linux、VMware ESXi を同時に狙うクロスプラットフォーム戦略を強化した。**また、DLL リフレクションローディング、ETW パッチングなど高度化されたアンチ分析技術を適用した。

最も注目すべきは、提携者に対しこれまで対外的に自制してきた原子力発電所、火力発電所などの重要インフラ攻撃を明示的に許可した点である。

主要内容

- Akira ランサムウェア、SonicWall SSL VPN 機器の脆弱性を悪用し世界的な攻撃を仕掛ける
- Lynx ランサムウェア、製造業と建設業を主な標的に攻撃 – 米国が全被害国の60%を占める
- LockBit 5.0、Windows、Linux、VMware ESXi を同時に狙うクロスプラットフォーム戦略を強化

2025年のサイバー脅威動向

ランサムウェアの動向 - 主要グループ活動 Top 10

7. DragonForce - カルテル戦略

2023年末に登場した DragonForce は、2025年3月に「ランサムウェアカルテル」を宣言し、生態系の再編を試みた。**提携組織が自社ブランドで活動しながら DragonForce インフラを活用できるホワイトラベルモデルを導入した。** 収益の80%を提携者に分配し、ペタバイト級ストレージ、24時間監視、ブログ及びファイルサーバーを提供した。2025年4月、RansomHub インフラを吸収したと主張した。ただし、RansomHub 側は DragonForce が捜査機関と協力していると反論し、対立が表面化した。

8. CLOP - Cleo MFT攻撃

CLOPは2025年第1四半期に劇的に復活した。**その中心にはCleo MFTソリューションの2つのゼロデイ脆弱性（CVE-2024-50623、CVE-2024-55956）を悪用した攻撃があった。** 10月にCleoが最初の脆弱性をパッチ適用したが、CLOPは11月にパッチ回避に成功し、12月には2つ目のゼロデイを発見して攻撃を継続した。約400組織が侵害された。 CLOPは、2023年に2,000以上の組織を侵害したMOVEit攻撃の経験を活かし、MFTプラットフォームの脆弱性攻略に特化した専門性を示した。1月からアルファベット順に被害者リストを公開し、最終的な被害規模は数百件を超えた。

9. RansomHub –栄光と没落

RansomHub は90%という破格の提携者収益分配率と210以上の組織侵害により、2025年第1四半期まで最多の活動を継続した。しかし4月1日、突然活動が完全に停止した。

RansomHub の崩壊は、数百人のアフィリエイトが Qilin、DragonForce、Lynx などへ移る大規模な生態系再編を引き起こした。 これは2024年の LockBit 「Operation Cronos」 以降で最大の構造的変化であり、ランサムウェア生態系の不安定性とダイナミズムを改めて証明した。

10. Gunra - 韓国金融界への侵入

Gunra は2025年4月に初めて発見された新規ランサムウェアグループで、韓国、日本、ブラジル、トルコ、台湾を主な標的とした。被害国に米国が含まれていないことが特徴である。Conti v2 のソースコードを基に開発された。

最大の特徴は、わずか5日という非常に短い交渉期限を設けている点で、被害組織に心理的圧迫をかける。ダークウェブではメッセンジャー「WhatsApp」スタイルの交渉ポータルを運営し、マネージャー役を置くなど組織的に運営している。

Gunra ランサムウェアは Windows と Linux の両方を攻撃できる。 特に、最大100個の同時暗号化スレッドをサポートする高性能 Linux 亜種を持っている。Linux 版は ChaCha20 暗号化を使用しており、実装過程で暗号化の脆弱性が発見された。これにより、韓国の保証保険会社は復号化に成功した。

主要内容

- DragonForce、提携先が自社ブランドで活動しながら DragonForce インフラを活用できるホワイトラベルモデルを導入
- CLOP ランサムウェア、Cleo MFT ソリューションのゼロデイ脆弱性を攻撃 – 約400組織が侵害される
- Gunra ランサムウェア、Windows と Linux の両方を攻撃可能- Linux 版は暗号化実装過程で脆弱性発見

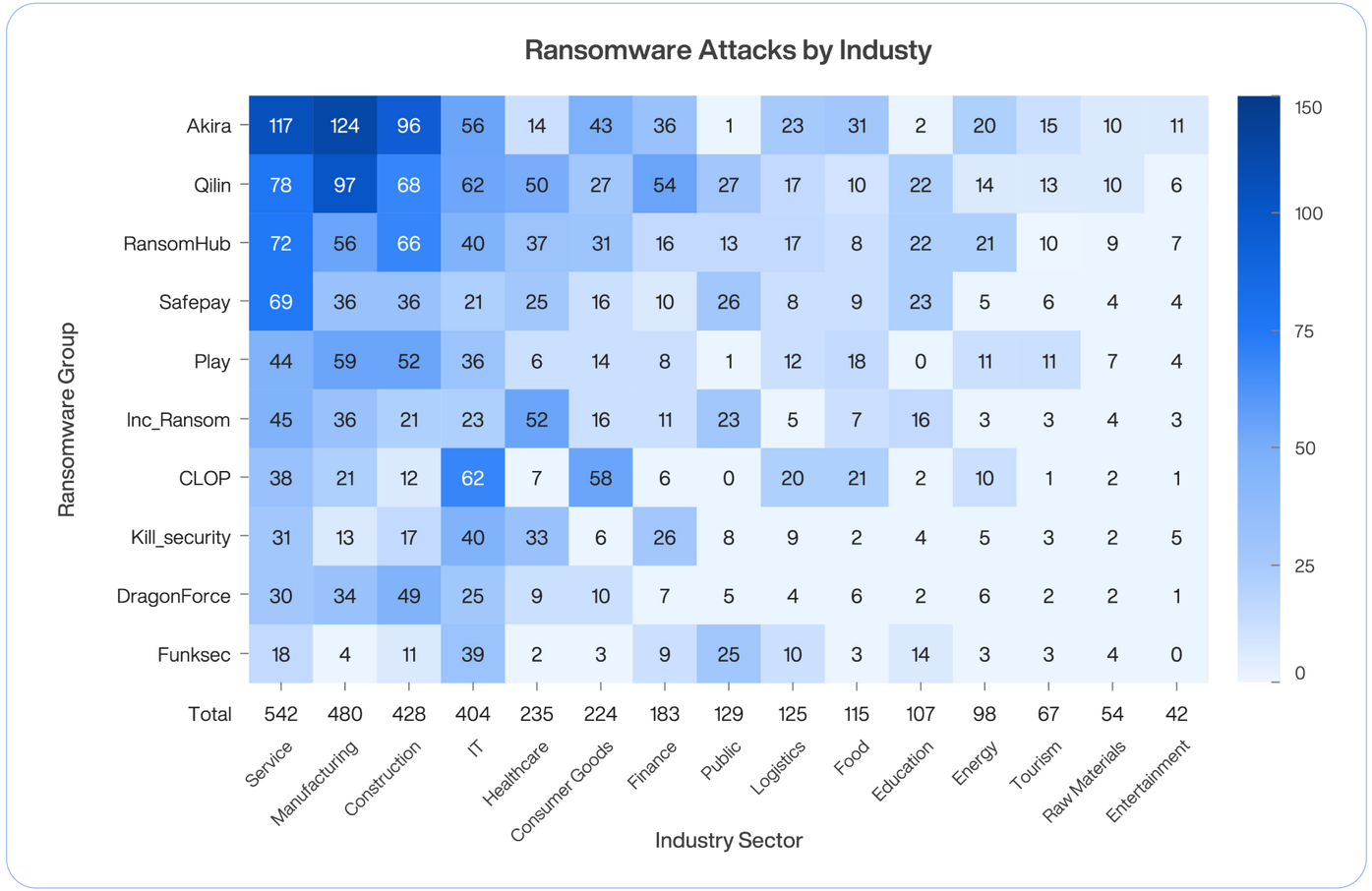
2025年のサイバー脅威動向

ランサムウェアの動向 – 主要被害産業群

2025年のランサムウェア攻撃グループ別主要被害産業データ分析の結果、サービス、製造、建設、IT分野が主な攻撃対象であった。**最も注目すべき変化は、サービス産業が最大の被害を受ける分野となった点である**。COVID-19 以降、デジタルトランスフォーメーションによりサービス産業の IT 依存度が高まり、システム停止時の売上損失など即時的な被害を受けるためである。

製造と建設は依然として主要な標的であった。製造業はスマートファクトリーとサプライチェーン管理システムの拡大により攻撃対象領域が広がった。生産ライン停止時には大きな損失が発生し、復旧費用を支払う可能性も高い。建設はプロジェクト日程遅延に伴う違約金と法的紛争リスクが大きいため、復旧を迫られる圧力が強い。IT も大規模な顧客データを保有しているため、攻撃者から継続的に狙われている。

最も懸念される変化は医療分野への攻撃増加だ。この分野は暗黙のうちに攻撃がタブー視されてきたが、2025年に完全に崩壊した。例えば、BlackCat は2024年の捜査機関作戦で壊滅した後、復活し病院攻撃禁止令を解除して攻撃を奨励した。 患者の生命に直結するため復旧遅延が不可能で、機密医療情報漏洩時には法的・倫理的責任が重く、攻撃者にとって高収益を狙える標的となった。一方、食品・観光などは攻撃頻度が低かった。デジタル依存度が低く伝統的な運営方式を追求するため、攻撃者が主要ターゲットとはしていないと解釈される。



[図]ランサムウェアグループ別産業分野攻撃状況 (2024年10月～2025年9月)

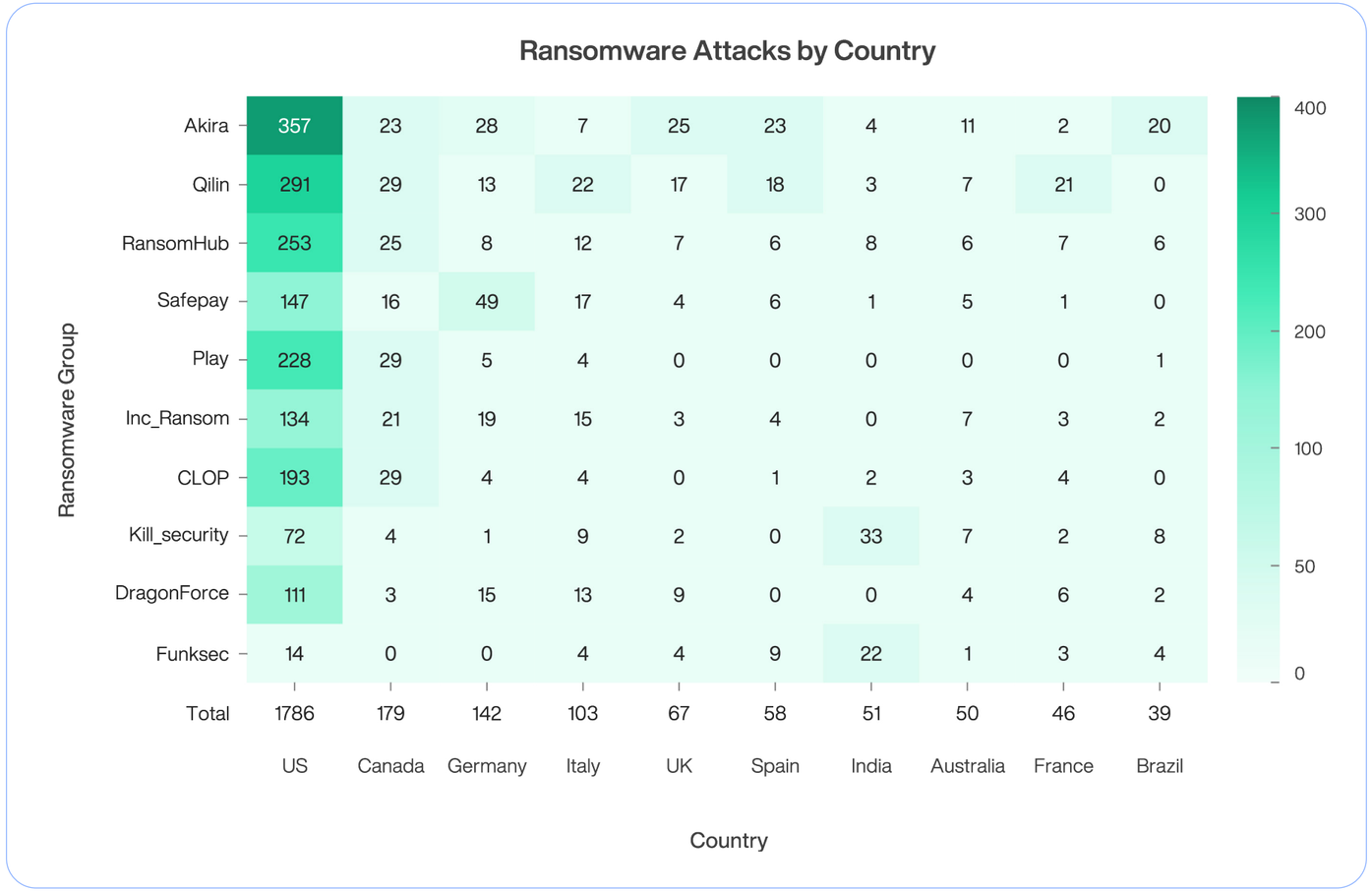
2025年のサイバー脅威動向

ランサムウェアの動向 – 主要被害国：全世界

2025年の統計によると、米国は依然として最も多くのランサムウェア攻撃を受けている。**Akira と Qilin は着実に攻撃を継続し、RansomHub は4月の活動停止前まで米国企業・機関を標的とした。**米国は世界最大の経済大国であり、製造、IT、医療、金融などの高付加価値産業が集中している。そのためデジタル依存度が高く、サイバー脅威にさらされやすい構造を抱えている。大規模な顧客データと機密情報がクラウドに集中しているため、データ漏洩や二重・三重の恐喝の主要な標的となる。

欧州とアジア地域の攻撃パターンの多様化も注目に値した。ドイツはSafepay と Akira の集中攻撃を受け、前年比で被害が増加した。特にデータ流出を迫る型攻撃が目立った。フランスと英国も持続的な打撃を受けた。**アジアではインドが Kill_Security と Funksec の拠点として台頭し、新たな攻撃対象として浮上した。**カナダは米国と隣接する地理的特性と類似した経済構造により、依然として被害が多かった。

スペイン、イタリア、ブラジルなども主要な被害国として浮上した。 欧州では Qilin と Akira がスペインとイタリアを継続的に攻撃した。南米ではブラジルが Akira の集中攻撃を受けた。アジア太平洋地域ではオーストラリアと日本が主要被害国と確認された。米国政府と同盟国はランサムウェア生態系に対し、国際協調による捜査と制裁で積極的に対応している。ただし、攻撃者は法的管轄の隙間を利用し、海外インフラを基盤に攻撃を実行することで制裁を回避している。



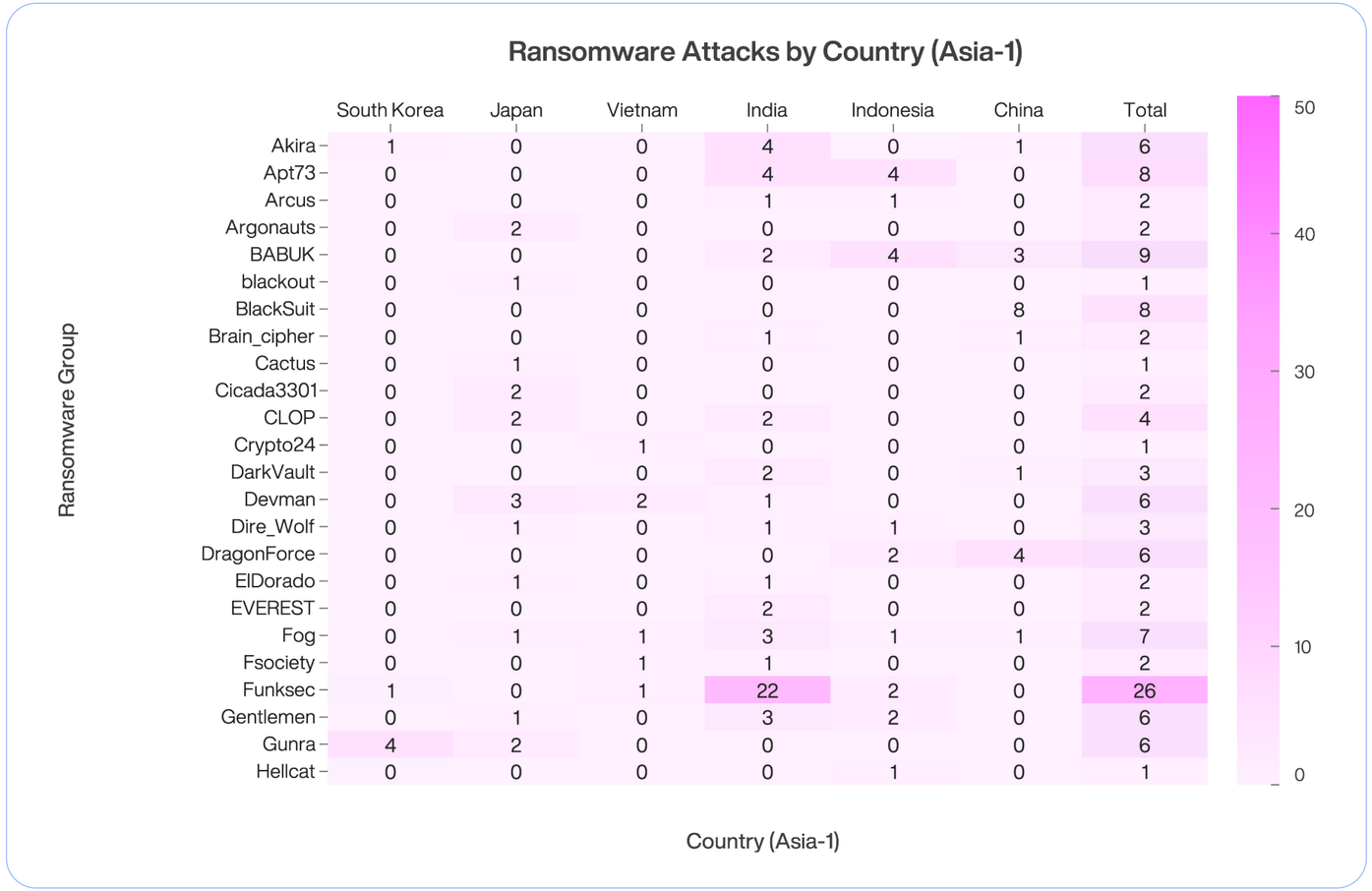
[図] 国別ランサムウェア攻撃被害状況 (2024年10月～2025年9月)

2025年のサイバー脅威動向

ランサムウェアの動向 – 主要被害国：アジア (1)

2025年のアジア各国別ランサムウェア被害分析の結果、**インドが日本を抜いて主要ターゲットとして急浮上した。このほか、台湾、韓国、日本が同程度の被害件数を記録した。**全体の事件数は前年比で急激な増加傾向を示した。

興味深い点は、国ごとに脅威の集中度に違いがみられる点だ。韓国と中国では少数の強力なグループへの偏りが顕著である。一方、日本とインドネシアは比較的分散型の脅威構造を示した。この場合、多様な攻撃グループが使用する侵入戦術に備える必要がある。



Ransomware Group	South Korea	Japan	Vietnam	India	Indonesia	China	Total
Akira	1	0	0	4	0	1	6
Apt73	0	0	0	4	4	0	8
Arcus	0	0	0	1	1	0	2
Argonauts	0	2	0	0	0	0	2
BABUK	0	0	0	2	4	3	9
blackout	0	1	0	0	0	0	1
BlackSuit	0	0	0	0	0	8	8
Brain_cipher	0	0	0	1	0	1	2
Cactus	0	1	0	0	0	0	1
Cicada3301	0	2	0	0	0	0	2
CLOP	0	2	0	2	0	0	4
Crypto24	0	0	1	0	0	0	1
DarkVault	0	0	0	2	0	1	3
Devman	0	3	2	1	0	0	6
Dire_Wolf	0	1	0	1	1	0	3
DragonForce	0	0	0	0	2	4	6
ElDorado	0	1	0	1	0	0	2
EVEREST	0	0	0	2	0	0	2
Fog	0	1	1	3	1	1	7
Fsociety	0	0	1	1	0	0	2
Funksec	1	0	1	22	2	0	26
Gentlemen	0	1	0	3	2	0	6
Gunra	4	2	0	0	0	0	6
Hellcat	0	0	0	0	1	0	1

[図] アジア主要国におけるランサムウェアグループ別攻撃状況 (2024年10月～2025年9月、連続画像P32-P33)

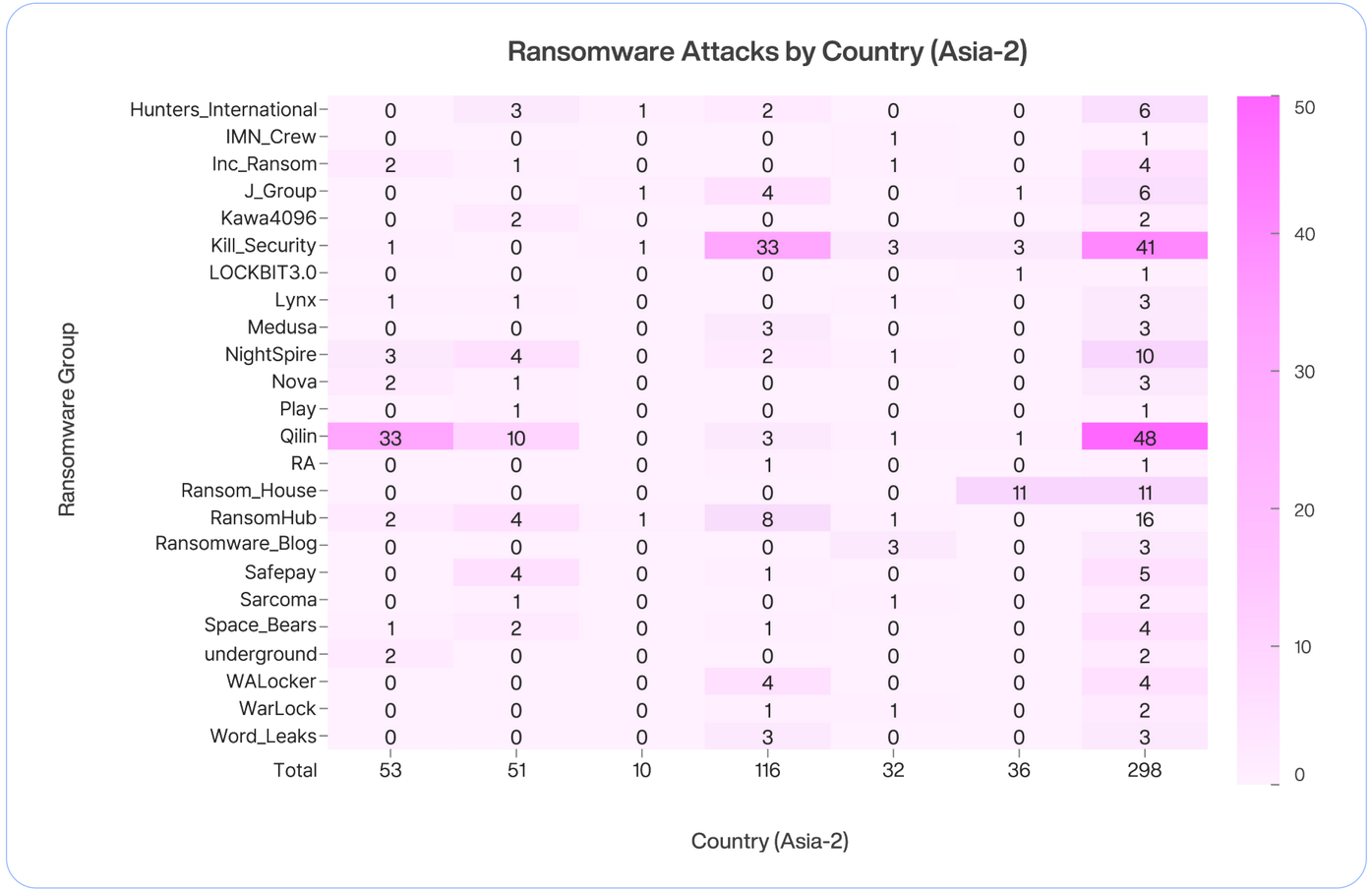
2025年のサイバー脅威動向

ランサムウェアの動向 – 主要被害国：アジア (2)

攻撃グループの活動を見ると、**Qilin が今年アジア圏で最も活発な動きを示した。特に韓国と日本で集中的な活動が確認された。**Qilin は韓国での活動が急増したのは、IT サービス供給業者に侵入し、その業者が管理する複数の資産管理会社を同時に攻撃するサプライチェーン攻撃を仕掛けたことが要因だ。これに続く Kill_Security はインドに強い偏重を示した。

2025年のアジア圏ランサムウェア攻撃は▲被害件数の増加▲攻撃対象の移動（日本→インド）▲国別脅威グループの集中度の差に要約できる。

韓国、インド、日本を含むアジア諸国では多様な攻撃が継続しており、持続的なモニタリングと強化されたセキュリティ体制が求められる。また、RansomHub 解体後に再編された Qilin、Kill_Security などの主要攻撃グループの戦術変化を迅速に反映し、対応策を策定する必要がある。



[図] アジア主要国におけるランサムウェアグループ別攻撃状況 (2024年10月～2025年9月、連続画像P33-P34)

2025年のサイバー脅威動向

主要脅威の動向 - マルウェア Top 9

2025年、多様なタイプのマルウェアが報告され、通信・金融・Linux インフラを標的とした攻撃が顕著となった。 ランサムウェアや認証構造を悪用したマルウェアが活発に拡散され、USB ベースの拡散や SNS 広告を通じた情報窃取など手法も多様化した。
北朝鮮 APT グループ関連の新たなマルウェアが発見され、既存マルウェアも継続的に拡散されている。

1. BPFDoor マルウェア 通信事業者を狙った密かな侵入者

BPFDoor は、Linux システムを対象に動作するバックドア型マルウェアである。ネットワークフィルタリング技術 BPF を悪用し、セキュリティ機器の監視を回避してシステム内部に密かに侵入する。

このマルウェアは特定のパケット受信時のみに活性化される。多様な通信プロトコルを活用して外部コマンドを受信し、内部情報を流出させる。実行過程では正常なシステムプロセスに偽装し、ファイルを複製した後、原本を削除して痕跡を最小化する。/dev/shm パスでメモリベースの実行を試みる。

2025年、韓国通信会社ハッキング事件で当該マルウェアが使用された。特に、加入者認証サーバーを狙った攻撃が報告され、産業全体のセキュリティ点検の必要性が提起された。

2. Qilin ランサムウェア 資産運用会社を標的とした二重脅迫者

Qilin は、RaaS 方式で運営されるランサムウェアである。大半が C 言語で記述される既存ランサムウェアとは異なり、**Rust 言語で開発され、Windows と Linux 環境の両方をサポートする。**一般的なランサムウェアが通常ファイルを一度だけ暗号化するのに対し、Qilin は Linux 環境で同一ファイルを三度暗号化する。バックアップ削除及び復旧妨害機能も含まれる。攻撃者に法律・広報支援まで提供する組織的な運営構造を備えている。

2025年、韓国の資産運用会社を攻撃した。複数の資産運用会社が共有していたシステム管理会社のクラウドサーバーが感染し、顧客情報と内部文書がダークウェブに流出された。

3. Gunra ランサムウェア 交渉なしに復旧した事例

Gunra ランサムウェアも RaaS 形態で運営される。Conti ランサムウェアのソースコードを基に制作されたとされている。Windows と Linux 環境の両方をサポートし、OS に影響を与えるファイルを除外した上で企業の核心資産のみを選択的に暗号化する方式で被害を最大化する特徴がある。

2025年、**金融機関や製造企業を相次いで攻撃した。**被害企業の内部文書や顧客情報がダークウェブに流出することで、産業全体に不安が広がった。ただし、Linux 版では暗号化キー生成方式に構造的な欠陥が発見された。これにより、復号化キーを抽出してデータを復旧した。

主要内容

- BPFDoor、韓国通信会社ハッキングに使用 – 特定パケット受信時のみ活性化し内部情報流出
- Qilin ランサムウェア、Rust言語で開発され Windows と Linux 環境をサポート – 韓国資産運用会社を攻撃
- Gunra ランサムウェア、複数企業を攻撃 – Linux 版暗号化キーの構造的欠陥により復号化可能

2025年のサイバー脅威動向

主要脅威の動向 - マルウェア Top 9

4. Plague マルウェア Linux 認証構造を狙う

Plague マルウェアは、**Linux システムのログイン手順を傍受し、ユーザーアカウント情報を窃取する。**システム起動時に自動実行され、ユーザーが SSH やターミナル経由でログイン時に入力する ID とパスワードを収集する。

Linux は PAM という認証モジュールを通じてログイン情報を確認するが、Plague マルウェアは LD_PRELOAD 手法を活用し、システムが本来実行すべき認証機能の代わりに自身が先に動作するよう設定する。

つまり、ユーザーがログインする際に Plague マルウェアが密かに割り込み、情報を傍受する方式である。ログイン記録を削除し、システム設定を変更して再起動後も動作し続けるよう構成されている。最近では、検知回避と隠蔽機能が強化された形態に進化している。

5. USB 経由で拡散するマイニングマルウェア

USB を介したマルウェア拡散は、物理的アクセスが可能な環境において依然として効果的な手段として活用されている。**最近も USB を媒介に仮想通貨マイニングマルウェアが拡散された事例があった。**

攻撃者は感染した USB にショートカット(.lnk)ファイルを隠し、ユーザーがこれを実行すると PowerShell スクリプトを通じてマイニングプログラムである XMRig をインストールする。単純なインストールに留まらず、PostgreSQL データベースと直接接続され、コマンドを送受信する方式で動作する。 一般的なマルウェアよりも精巧な通信構造を備えており、外部からマイニング活動を制御したり状態を監視できるようにしている。また、GitHub を通じて悪意のあるファイルをダウンロードし、Windows レジストリの Run キーを利用して再起動後も自動実行されるように設計されている。これにより、持続的なマイニングが可能となる。

6. 偽取引所広告で拡散されるインフォスティーラー

攻撃者は Binance などの**有名取引所を装った Facebook 広告を表示し、ユーザーがこれをクリックすると偽の取引所サイトへ誘導した後、installer.msi ファイルのダウンロードを促す。**ファイルは実行直後に悪意のある動作を開始せず、被害者が仮想環境ではなく攻撃者が設定した条件に該当する場合にのみ、悪意のあるスケジューラを登録し、その後インフォスティーラーマルウェアをダウンロードして実行する。

単純なマルウェア配布アドレスへのアクセスだけでは感染せず、非対象ユーザーの場合は正常なサイトへリダイレクトされ検知を回避する。マルウェアは PowerShell を通じて追加ペイロードを取得し、システム情報、ブラウザ保存データ、画面キャプチャ、Telegram アカウントなどの機密情報を収集する。

主要内容

- Plague マルウェア、Linux システムのログイン手順を傍受しユーザーアカウント情報を窃取
- 韓国で USB を介した暗号通貨マイニングマルウェアが拡散した事例が発生
- 偽取引所広告 - 有名取引所を装った Facebook 広告 > 偽取引所サイトへ誘導 > 悪性ファイルダウンロード

2025年のサイバー脅威動向

主要脅威の動向 - マルウェア Top 9

7. プロキシウェアマルウェアの密かな侵入自分の PC が知らないうちに帯域幅を共有していたら？

Proxyware は、ユーザーが自身のインターネット帯域幅を外部と共有し収益を得る合法的なプログラムである。最近ではこれを悪用したマルウェアがセキュリティ脅威となっている。

攻撃者はユーザーの同意なく Proxyware をインストールし、ネットワークリソースを不正に共有させる。これにより金銭的利益を得る Proxyjacking が多数確認されている。Mimo コインマイナーと共に拡散されるか、フリーウェアのインストール過程で広告ページを通じて自動インストールされる方式が用いられる。被害者はシステム性能とネットワーク速度の低下を経験する。

Proxyware は外部サーバーと継続的に通信し、攻撃者が設定した方式に従ってリソースを活用するため、感染事実を認識しにくい。
Cryptojacking と類似するが、CPU ではなくネットワーク帯域幅を活用する点で差別化され、アンチウイルス検知を回避する方式で密かに動作する。

8. BeaverTail & Tropidoor マルウェア ラザルスの採用メール攻撃

BeaverTail と Tropidoor は、北朝鮮の支援を受けているとされる「ラザルス（Lazarus）」が使用するマルウェアで、採用を装ったフィッシングメールを通じて拡散される。攻撃者は実際の企業名を偽装し、開発者や IT 従事者を狙う。**悪意のあるプロジェクトを含むBitbucket リンクをメールに添付して拡散する方式で感染を試みる。**

マルウェア BeaverTail は、ブラウザに保存されたログイン情報と暗号通貨ウォレットデータを収集する情報窃取機能を備えている。Tropidoor はメモリベースのバックドアとして、システム情報収集、コマンド実行、画面キャプチャなど多様な機能を通じて長期的な侵入を可能にする。

9. EndRAT、Kimsukyの 新たなマルウェア

EndRAT は、北朝鮮の支援を受けているとされる 「Kimsuky」 が2025年7月から活用を開始した AutoIt ベースの新たな RAT（リモートアクセストロイ）マルウェアである。

EndRAT はサーバーとの通信に使用される固有文字列「endServer9688」および 「endClient9688」 を含んでおり、これらの識別子に基づいて命名された。一般的に LNK ファイルの実行を誘導する方式で拡散される。
2025年9月には 「ストレスクリア」 というプログラムを装った MSI インストーラーを通じて配布された事例も確認されている。 AutoIt スクリプトを基盤に制作された点、実行条件及び通信構造に特定文字列を使用する方式は既存のマルウェアと差別化される。ㅋ

主要内容

- ユーザーの同意なく Proxyware をインストールし、ネットワークリソースを不正に共有する攻撃手法
- Lazarus、開発者や IT 従事者を狙って BeaverTail および Tropidoor マルウェアを配布
- Kimsuky グループ、新たな RAT（Remote Access Trojan）マルウェア「EndRAT」の使用を開始

2025年のサイバー脅威動向

主要脅威の動向 - 攻撃手法 Top 10

1. ソフトウェアサプライチェーン攻撃

2025年に入り、ソフトウェアサプライチェーン攻撃の規模と精巧さが拡大した。**攻撃者はオープンソースパッケージリポジトリ（npm、PyPIなど）に直接侵入するか、人気ライブラリや開発ツールを改ざんし、正規の更新や依存関係インストールプロセスを通じてマルウェアを広く拡散させた。**これらの攻撃は開発およびCI/CD環境を感染させ、ソースコード窃取、バックドア挿入、認証情報収集などにつながった。その結果、金融、暗号通貨、クラウド、公共機関など様々な産業が連鎖的な被害を受けた。特に2025年には、正規署名および自動配布システムを悪用したサプライチェーン攻撃が多数確認された。

2. 盗難資格情報および MFA 回避 (T1078)

2024年下半期以降、スピアフィッシングや情報漏洩による資格情報の窃取が急増した。攻撃者は**有効なアカウントを確保し、VPN、SSO、クラウド環境に侵入。MFA 回避のため EvilProxy などのプロキシベース認証中間者攻撃ツール**を使用したり、ユーザー端末に多数の認証要求を繰り返し送信し、誤認による承認を誘導する手法も活用する。 APT29 や Scattered Spider などはこの手法で長期潜伏と内部ネットワーク拠点の拡大に成功している。

3. クラウド環境侵害及びリパトリエーション

クラウド・リパトリエーション（Cloud Repatriation）は、コスト最適化、パフォーマンス改善、規制対応のために、中核データやワークロードをオンプレミスに移行する戦略である。ただし、CSP のセキュリティ機能不足により、セキュリティ設定の欠落や構成エラーなどのリスクが伴う可能性がある。特にクラウド環境では、OAuth トークンの窃取、資格情報の悪用による横移動、権限拡張などを通じた侵害が増加している。これに対し、認証、権限、可視性の強化とともに、リパトリエーション時のセキュリティポリシーの再構築が求められる。

4. AI/LLM ベースの攻撃高度化

攻撃者はAIと大規模言語モデル（LLM）を活用し、マルウェアの自動生成、検知回避、精巧なフィッシング文案やディープフェイクコンテンツ制作などを自動化している。その結果、攻撃の効率性と精巧さが向上し、従来の脅威検知手法だけでは遮断が難しくなっている。また、自動化されたツールを通じて大規模な標的型攻撃を迅速に設計・展開し、防御者が対応できる時間を短縮している。 今後、AI ベースの攻撃は多様化と高度化を繰り返し続けると予測される。

2025年攻撃手法 Top 10

1. ソフトウェアサプライチェーン攻撃
2. 盗難資格情報及び MFA 回避
3. クラウド環境侵害及びリパトリエーション
4. AI/LLM ベース攻撃の高度化
5. リモートアクセス及び境界セキュリティの突破
6. MoTW 回避及び圧縮フォーマット悪用
7. ウェブサービスおよびクラウドの悪用
8. スピアフィッシング添付ファイル悪用
9. DLL 検索順序ハイジャック
10. OS 内蔵ツールの悪用 – LOTL

2025年のサイバー脅威動向

主要脅威の動向 - 攻撃手法 Top 10

5. リモートアクセスおよび境界セキュリティの侵害 (T1133)

RDP、VPN、VDI などの外部リモートアクセスサービスを利用した侵入試行が増加している。特に、ネットワーク境界に位置するファイアウォールや VPN などの脆弱性は主要な侵入経路となる。攻撃者は公開ポート、脆弱な認証情報および認証構成を通じて初期侵入を行う。その後、SSOセッションの乗っ取りや認証バイパスにより内部ネットワークへ横移動する。 Ivanti、Fortinet、Cisco ASA、Palo Alto Networks 機器のゼロデイ脆弱性は APT 攻撃の主要な攻撃ベクトルとして利用され、認証バイパス及び内部ネットワーク侵入事例が多数報告されている。

6. MoTW 回避及び圧縮フォーマット悪用 (T1553.005)

攻撃者は**Windowsのセキュリティ機能 MoTW（Mark of the Web）を回避する攻撃を継続**している。MoTW はインターネットからダウンロードされたファイルに Zone.Identifier メタデータを付与し、SmartScreen と Office 保護機能で検証する。 攻撃者は ISO やZIP などの圧縮形式を活用して MoTW が内部ファイルに伝達されないようにしたり、LNK ファイル構造の操作や 7-ZIP の脆弱性（CVE-2025-0411）を利用して MoTW を削除し、警告なしに悪意のあるファイルを実行させる。

7. ウェブサービス及びクラウドの悪用 (T1071.001)

攻撃者は**検知回避のため、C2 通信にGitHub、Dropbox、Google Drive、Telegram などの正常なウェブサービスやクラウドプラットフォームを利用**する。ネットワークトラフィックを一般ユーザー活動のように偽装するため、ファイアウォールや IDS では識別が困難である。2024年にはCloudSorcerer という攻撃グループが GitHub に暗号化されたコマンドを隠し、Microsoft Graph API と Yandex Cloud を介して被害システムと通信した事例があった。 Gamaredon、Kimsuky、PteroBox などの APT 組織もこの手法を活用している。

8. スピアフィッシング添付ファイル悪用 (T1566.001)

2024年下半期以降、攻撃者は**ソーシャルエンジニアリング手法に基づくスピアフィッシングを主要な侵入手段として活用**している。 LNK、CHM、ZIP/RAR ファイルなどが継続的に使用されている。最近では添付ファイルの代わりに悪性 URL や QR コードを活用する手法も利用される。その他、クリックフィックス（ClickFix）手法を通じてユーザーのクリック、認証情報入力、悪性ファイルのインストールを誘導することもある。CrowdStrike および Microsoft の事例によると、このような ClickFix タイプの攻撃は内部ネットワークへのアクセスと資格情報の窃取の主要な経路として活用される

9. DLL Search Order Hijacking (T1574.001) DLL Side Loading (T1574.002)

DLL Search Order Hijacking は、**プログラムがDLLをロードする際にWindows の検索順序を操作し、攻撃者が作成した悪意のあるDLL を正規の DLL の代わりにロードさせる攻撃手法**である。権限昇格、リモートコード実行、および持続性の確保に悪用される。実際、ShadowPad 関連ランサムウェアキャンペーンや NI LabVIEW の制御されていない検索パス脆弱性（CVE-2025-2630）などで利用された。 一般的に、攻撃者は脆弱なパスに悪意のある DLL を配置したり、インストール・更新プロセスの動作を操作したりして、長期間検知を回避しながら権限を維持する。

10. OS 内蔵ツールの悪用 – LOTL (T1059)

攻撃者は**マルウェア痕跡の最小化のため、PowerShell、WMI、rundll32、mshta などの Windows 正規ファイルを利用する LOTL（Living Off The Land）手法**を用いる。この手法はアンチウイルスや EDR などの防御体系を回避し、正規プロセスに悪意ある動作を隠蔽する。 Microsoft の調査によると、Volt Typhoon などの中国系APT グループは、米国防・通信・エネルギーインフラへの侵入において、wmic、netsh、PowerShell を使用して権限取得、資格情報の収集、内部ネットワークの偵察を実施した。

2025年のサイバー脅威動向

主要脅威の動向 – 脆弱性 Top 10

1. Ivanti Connect Secure VPN (CVE-2024-21887, CVE-2025-22457)

APT グループが最初の侵入にファイアウォール、SSL VPN などのネットワークセキュリティ製品の脆弱性を悪用する事例が増加している。特に Ivanti Connect Secure VPN の認証バイパス脆弱性(CVE-2023-46805)とコマンドインジェクション脆弱性(CVE-2024-21887)は、今年に至るまで攻撃者の主要な標的となった。 2025年4月に公開されたバッファオーバーフローによるリモートコード実行脆弱性(CVE-2025-22457)は、中国政府と関連があるとされる APT グループUNC5221が使用した。脆弱性を通じてウェブシェル及びバックドアを配布し、政府機関や金融機関に侵入したことが確認されている。

2. FortiOS & FortiProxy (CVE-2025-24472)

2025年初頭、FortiOS および FortiProxy の認証バイパス脆弱性（CVE-2025-24472）が公開された。**攻撃者はこの脆弱性を悪用し、最高管理者（Super Admin）権限を取得してネットワーク全体を制御できるようになった。**初期侵入段階でこの脆弱性を悪用した事例が報告され、大企業や金融機関が深刻な被害を受けた。脆弱性の PoC が公開されて以降、攻撃の試みが急増した。

3. PAN-OS & GlobalProtect (CVE-2024-0012)

Palo Alto Networks の PAN-OS 管理 Web UI 認証バイパス(CVE-2024-0012, CVE-2025-0108)を足掛かりに、権限昇格(CVE-2024-9474)と認証後のファイル読み取り(CVE-2025-0111)が**連携され、管理者またはルート権限の掌握、構成改ざん、機密情報へのアクセスにつながる脆弱性悪用事例があった。**
GlobalProtect に関しては、CVE-2024-3400 のゼロデイが代表的な脆弱性事例である。リモートシェル確立と内部ネットワーク横断移動が確認された。これに関連し、米国保健福祉省（HHS）のセキュリティチーム（HC3）は、ヘルスケア産業を主要標的産業として指定した。

4. Cisco ASA & Firepower (CVE-2025-20333, CVE-2025-20362)

Cisco ASA および Firepower 機器において、ArcaneDoor 関連の活動に関連するゼロデイおよび N デイ脆弱性が発見された。CVE-2025-20333 は、VPN ウェブサーバーの脆弱性を通じてリモートコード実行を可能にする。CVE-2025-20362 は認証なしで制限された URL へのアクセスを許可する。 両脆弱性は実際の攻撃で連鎖的に悪用された。米国 CISA は連邦機関に対し、資産の特定、フォレンジック収集、迅速な緩和策とパッチ適用を求めた。Cisco は ROMMON とブートチェーン操作による持続性確保戦術も確認した。

2025年の脆弱性 Top 10

1. Ivanti Connect Secure VPN
2. Fortinet – FortiOS/FortiProxy
3. Palo Alto – ファイアウォール/GlobalProtect
4. Cisco ASA/Firepower
5. ファイル転送ソリューション（MOVEit、Cleo など）
6. Sitecore RCE
7. ウェブブラウザのゼロデイ
8. Android 権限昇格
9. 圧縮プログラム
10. オープンソースソフトウェアのサプライチェーン

2025年のサイバー脅威動向

主要脅威の動向 – 脆弱性 Top 10

5. ファイル転送ソリューションの脆弱性 (MOVEit, Cleoなど)

Cleo Harmony、VLTrader などの MFT 製品において、リモートコード実行と認証バイパス脆弱性が確認された。 CLOP ランサムウェアがこれを悪用し、複数の組織に被害を与えた。CVE-2024-50623 は無制限のファイルアップロード・ダウンロードを悪用し、リモートでコードを実行する。CVE-2024-55956 は Autorun ディレクトリ設定を悪用し、認証なしでコマンド実行を許可した。MOVEit Transfer の CVE-2024-5806 は SFTP 認証処理の問題により認証バイパスが可能だった。Safe Wallet フロントエンド資産が侵害され資金窃取が発生した。FBI はこれを北朝鮮攻撃グループ TraderTraitor の活動と特定した。

6. Sitecore RCE (CVE-2025-534690)

Sitecore の ViewState 逆シリアライズ脆弱性(CVE-2025-534690)は、事前認証なしでリモートコード実行を可能にする。古い配布ガイドで提供されたサンプル machineKey の再利用が攻撃の起点と指摘された。 2024年末から悪用状況が観測され、2025年9月に公式勧告が出された。攻撃者はインターネットに公開された Sitecore インスタンスを通じて初期アクセスを確保した後、リモートシェルをインストールし、システムおよびドメイン偵察、資格情報の収集、内部横移動を実行した。その後、設定ファイルや秘密鍵などの機密情報を窃取した。

7. ブラウザのゼロデイ脆弱性 (Chrome: CVE-2024-4947, Firefox CVE-2024-9680)

ウェブブラウザで発見されたゼロデイ脆弱性が実際の攻撃に悪用された。Chrome V8 エンジンの脆弱性（CVE-2024-4947）は、**細工されたウェブページへのアクセスだけでコード実行が可能であり、ラザルス系攻撃グループが金融分野を攻撃する際に利用した。** Firefox のUse-After-Free 脆弱性(CVE-2024-9680)は、ロシアの APT グループ RomCom が欧州と北米でのスパイ活動においてバックドアをインストールするために利用した。これらの脆弱性は、資格情報の窃取、ペイロードの実行、持続性の確保へとつながる攻撃フローが特徴である。

主要内容

- Cleo Harmony、VLTrader などの MFT 製品において、リモートコード実行と認証バイパス脆弱性が確認
- Sitecore の ViewState 逆シリアライズ脆弱性(CVE-2025-534690)は、古い machineKey の再利用が原因
- Chrome V8 エンジンの脆弱性(CVE-2024-4947)は、ウェブページへのアクセスだけでコード実行が可能であり、Lazarus が攻撃に利用

2025年のサイバー脅威動向

主要脅威の動向 – 脆弱性 Top 10

8. Android 権限昇格脆弱性 (Android CVE-2025-38352)

Android CVE-2025-38352 は、ローカル権限昇格を通じて悪意のあるアプリがデバイスの権限を拡大するために使用された。特に、攻撃フロー全体において、ウェブブラウザのゼロデイ脆弱性と組み合わせて、初期のデバイス掌握後に資格情報の窃取、追加ペイロードの実行につながる事例が観察された。 悪意のあるアプリは権限を拡張することで、システム設定の変更、機密データへのアクセス、セキュリティ機能の無効化まで可能となる。モバイルユーザーを標的とした攻撃では、金融情報の窃取やスパイ活動につながるリスクがある。

9. 圧縮プログラムの脆弱性 (CVE-2025-0411, CVE-2025-8088)

攻撃者は圧縮プログラムも攻撃手段として活用している。これに関連し、**個人および企業環境で広く使用される 7-Zip と WinRAR の脆弱性を悪用した攻撃事例**が確認された。7-Zip の MoTW 回避脆弱性(CVE-2025-0411)は、ロシアの攻撃グループがウクライナ政府機関と民間組織を対象に SmokeLoader を配布するために使用された。 WinRAR ではパス探索脆弱性（CVE-2025-6128、CVE-2025-8088）が発見された。特 にCVE-2025-8088 は、RomCom が欧州とカナダの物流、製造、金融、防衛産業企業を攻撃する際に利用したとされている。

10. オープンソースソフトウェアのサプライチェーン脆弱性 (ex: npm package)

JavaScript の npm パッケージなど**広く利用されるオープンソースライブラリにおいて、保守担当者のアカウント乗っ取りとマルウェア注入を組み合わせたサプライチェーン攻撃が相次いだ。**2025年9月にはnpm で保守担当者へのフィッシングとトークン窃取により人気パッケージの多数が汚染された。 同時期に PyPI は開発者向けメールフィッシングキャンペーンを公式に警告し、アカウント乗っ取りリスクを告知した。コンテナ領域では XZ バックドアを含む Docker Hub イメージが多数残存している事実が確認され、サプライチェーンの脆弱性が露呈した。このほか、Rust エコシステムでもウォレットキーを窃取する悪性クレートが発見され、即時削除された。

主要内容

- Android CVE-2025-38352 は、ローカル権限昇格を通じて悪意のあるアプリがデバイスの権限を拡大するために使用
- 攻撃者が 7-Zip と WinRAR の脆弱性を悪用した攻撃事例が確認
- 主要なオープンソースライブラリで、アカウント乗っ取りとマルウェア注入を組み合わせたサプライチェーン攻撃が相次いで発生

2025年のサイバー脅威動向

主要脅威の動向 - モバイル Top 6

1. ソーシャルエンジニアリング手法に基づくモバイル犯罪の高度化

2025年には、ソーシャルエンジニアリング手法を活用したモバイル犯罪がさらに高度化した。主に拡散時点の社会的課題を反映して制作・配布された点が特徴である。**通信会社、AI アプリ、公共機関などを装い、被害者の関心を引く偽装アプリが使用される。**また、急騰株、公募株投資や恋人関係を装い、内面的親密感を形成した後、投資へ誘導する詐欺アプリも多数発見された。これらのアプリは高収益を保証する名目で被害者を惑わせ、悪性アプリのインストールを要求する。

被害者は投資金を入金後、アプリを通じてリアルタイムで操作された収益率を確認することになる。出金要求時には様々な理由を挙げて投資金を返還せず、姿を消す事例が多数発生している。この他にも、秘密の会話ができるという名目でアプリインストールを誘導した後、被害者の連絡先や写真などを奪取し、これを基に拡散を脅迫して資金を要求するボディカムフィッシング事例も継続的に発見されている。

2. 新たな攻撃機能を搭載した悪質アプリ

Android の HCE（Host Card Emulation）を利用して NFC 通信を傍受する手法を活用した悪性アプリが高度化している。Ngate と呼ばれるこのアプリは、NFC 通信を傍受する機能に加え、偽の画面を表示してユーザーの認証情報を窃取する機能も備えている。

これらのアプリは、NFC ベースの機器と接触した際に発生する通信情報を攻撃者に送信する。 攻撃者は NFC 通信情報を基に ATM 不正引き出しなどを実行する。暗号資産情報を窃取するため OCR（光学式文字認識）ライブラリを活用した悪質アプリも新たに発見された。このアプリはユーザーが暗号資産ウォレットのバックアップに使用するニーモニック（Mnemonic）関連情報を画像として保存する点を悪用した。攻撃者は OCR 技術を活用し、画像内に含まれるニーモニックフレーズと暗号資産関連情報を自動分析・抽出・窃取する。

3. 公式ストアにおける悪質アプリの多様化

公式アプリストアにおいても、様々なタイプの悪性アプリが継続的に発見されている。最近では、金融情報窃取（Banker）、高金利ローン（SpyLoan）、暗号通貨情報窃取（SparkCat、SparkKitty）、隠蔽広告実行（HiddenAds）、投資詐欺（ScamFX）など多様なアプリが確認されている。

特に Banker タイプは、悪性機能を含む場合、アプリストアのセキュリティ検査で検出される可能性が高いため、**正常なアプリに偽装して登録した後、インストールされてから外部から悪性ペイロードをダウンロードして実行する方式に進化した。**一部の悪性アプリは、ユーザー環境に応じて悪性機能を条件付きで有効化したり、特定の国や言語設定でのみ悪性行為を実行するなど、知能的に動作するケースが多い。

主要内容

- モバイルソーシャルエンジニアリング手法、通信会社、AI アプリ、公共機関などを装い被害者の関心を引く偽装アプリの利用
- Android の HCE（Host Card Emulation）を利用して NFC 通信を傍受する悪意のあるアプリの登場
- アプリストアに正規アプリとして登録した後、外部から悪意のあるペイロードをダウンロードして実行する方式へ進化

2025年のサイバー脅威動向

主要脅威の動向 - モバイル Top 6

4. 様々な脆弱性を悪用した攻撃

RCE（リモートコード実行）、権限昇格（EoP）**など公開された CVE に加え、未登録の未公開脆弱性を悪用した攻撃が継続的に発見されている。**これらの脆弱性は報告されるまで知られていないため、攻撃者はこれを「ゼロデイ（Zero-Day）」として悪用し、悪意のあるアプリを作成・拡散する。被害者はセキュリティパッチが適用されるまで無防備な状態に晒される可能性がある。

代表的な例として Pixnapping 脆弱性がある。この脆弱性を悪用すると、Android 13～16バージョンの特定端末において、半透明オーバーレイと精密なタイミングを利用してピクセルデータを抽出できる。これによりMFA認証コードなどの機密情報を窃取する。 CVE-2024-43093 脆弱性は、ContactsDirectory を悪用し、ユーザーの操作なしにアプリを自動実行できる権限昇格脆弱性である。ユーザーの知らないうちに悪意のあるアプリを実行したり、バックグラウンドで悪意のある機能を有効化したりできる。実際にこうした機能を行う悪意のあるアプリが発見された事例もある。

5. 北朝鮮関連サイバー攻撃グループの活動

北朝鮮関連攻撃グループが韓国を対象に機密情報を窃取するためのスパイアプリを継続的に拡散している。**主にファイルマネージャー、ソフトウェア更新、セキュリティ文書ビューアなどのユーティリティアプリに**偽装し、ユーザーの疑念を回避するとともに、正常なアプリのように見えるようUIと機能を精巧に設計した。

また、分析を妨害するため、コード難読化、暗号化、動的ロード、条件付き実行など様々な技法を適用した。C2 サーバーを通じて命令を受信し、窃取した情報を外部へ送信する機能も含まれていた。一部の悪意のあるアプリの C2 サーバーではコインフィッシングサイトも存在した。これは暗号資産関連の資産窃取まで範囲を拡大していることを示している。

6. マルウェアプリインストール機器の流通

最近、Android OS ベースのスマートフォンやセットトップボックス（STB）**など、一部の機器がメーカー出荷前からマルウェアが組み込まれた状態で流通している事例が確認された。**これらの機器は正規品より安い価格を掲げて消費者を誘惑する。機器内部には、DDoS 攻撃やクレデンシャルスタッフィング攻撃を実行する Mirai マルウェア、広告収益を狙う HiddenAds タイプのマルウェアが含まれている。 マルウェアはユーザーが気付かない状態で長期間動作する。ネットワークトラフィックの増加、バッテリー消耗、個人情報流出などの被害につながる可能性がある。

また、USB ケーブルを介したハッキング事例も継続的に報告されている。内部にデータ転送機能を悪用した悪性チップセットが含まれており、接続機器からのファイルアクセス、コマンド実行、情報窃取などが可能となるよう設計されている。

主要内容

- 公開された CVE 以外にも、未登録の未公開脆弱性を悪用したモバイル攻撃が継続的に発見されている
- 北朝鮮関連グループ - 主にファイルマネージャー、セキュリティ文書ビューアなどのユーティリティアプリに偽装
- スマートフォン、セットトップボックスなど一部の機器が、メーカー出荷前からマルウェア入りの状態で流通する事例が確認

2025年のサイバー脅威動向

攻撃タイプの統計

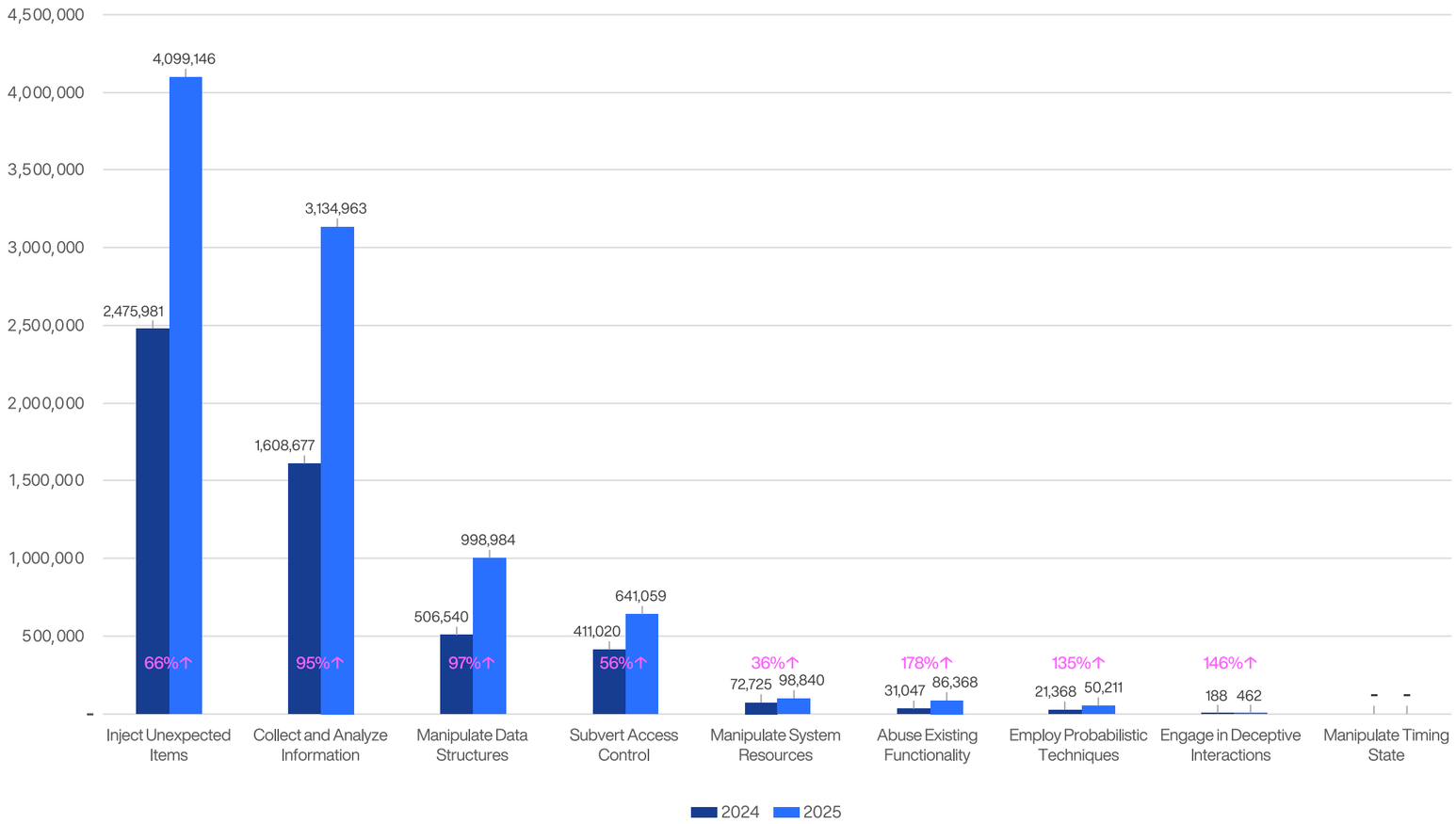
アンラボの侵害対応専門組織「CERT（Computer Emergency Response Team）」は、毎月サイバー脅威の推移を分析した「CERT月次レポート」を発行している。当該レポートをもとにm2025年のサイバー攻撃タイプ統計を公開した。

2025年、**全体の攻撃検知件数は前年比78%増加した。**すべてのタイプが前年比で二桁以上増加し、一部は100%を超える伸びを記録した。

AI ベースの攻撃高度化、クラウド環境の拡大、サプライチェーン脆弱性の悪用など、様々な要因が複合的に作用した結果と分析される。

最も多く発生した攻撃タイプは「予期せぬデータ注入（Inject Unexpected Items）」で、2024年に続き1位を記録した。情報収集・分析（Collect and Analyze Information）、データ構造改変（Manipulate Data Structures）、アクセス制御操作（Subvert Access Control）、システムリソース改変（Manipulate System Resources）が続いた。

2025年攻撃タイプの順位



2025年のサイバー脅威動向

攻撃タイプの統計 – 説明

1. 予期せぬデータの注入

予期せぬデータ注入（Inject Unexpected Items）は、**攻撃者がシステムのデータ入力インターフェースを通じて異常または例外的なデータを注入し、動作を制御または妨害する手法である。**入力値の検証が不十分な場合、入力処理ロジックが脆弱な場合などに発生する。システムは注入された値に応じて、異常動作、セキュリティポリシーの回避、情報漏洩などの問題に直面する可能性がある。

2. 情報の収集と分析

データ情報の収集と分析（Collect and Analyze Information）は、**攻撃者が能動的な問い合わせや受動的な観察を通じて対象システムの情報を確保し分析する攻撃手法である。**攻撃者はシステム構成、ユーザーアカウントなどの詳細情報を収集し、今後の攻撃経路を設計したり潜在的な脆弱性を特定する。この過程は初期侵入のための準備段階として活用される。

3. データ構造の操作

攻撃者が**システム内部のデータ構造を意図的に変更し、正常なデータ処理フローを破壊する**攻撃手法である。これにより、システムの内部データフローを妨害または改ざんし、異常な結果を誘導する。このような操作は予期せぬエラーを引き起こすだけでなく、データの信頼性まで損なう。

4. アクセス制御の回避

アクセス制御の回避（Subvert Access Control）は、**攻撃者がアクセス制御メカニズムを回避または無効化し、許可されていない権限を取得してシステムに不適切にアクセスする**攻撃手法である。これにより、管理者権限や高度なユーザー権限を確保し、機密データへのアクセスや特定機能の操作が可能となる。

5. システムリソースの操作

被害者の CPU、メモリなどのシステムリソースを過剰に消費させ、性能を低下させたり資源を枯渇させる方式である。システムは正常なサービス提供が困難になり、ユーザーは応答速度の低下やシステム停止を経験する。資源枯渇は長期的にサービス拒否（DoS）攻撃と同様の被害をもたらし、システムの可用性を阻害する。

6. 既存機能の悪用

攻撃者がシステムやアプリケーションの正常な機能を利用して被害を引き起こす攻撃手法である。新しいコードを追加せず、既存の機能を悪用することが特徴である。例えば、カスタマーサービスのファイルアップロード機能を悪意のあるファイルの伝達に利用したり、検索機能を通じて内部情報を暴露させる方式がある。

7. 確率的手法の採用

攻撃者が**確率的アプローチを通じてシステムの脆弱性を探索したり、攻撃成功の可能性を段階的に高める手法である。**代表的なものとして、ブルートフォース攻撃とタイミング攻撃がある。パスワード推測などを通じて、時間の経過とともに成功確率を高める。暗号化システムや認証手順が脆弱なシステムに効果的であり、ユーザーが気付かないうちに侵入する。

8. 欺瞞的相互作用の遂行

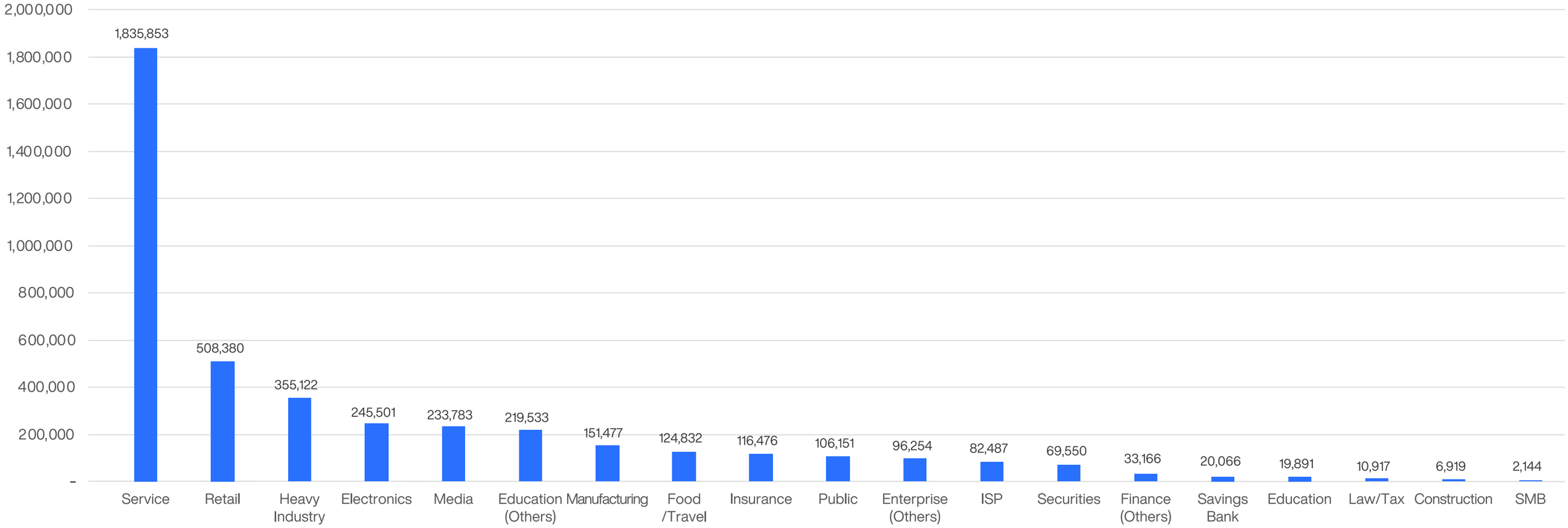
攻撃者がシステムやユーザーと相互作用する際、身元や意図を隠蔽し、誤った情報を伝達して目的の結果を得る攻撃手法である。代表的なものとして、フィッシング、ソーシャルエンジニアリング手法、偽のウェブサイトや電子メールを利用した詐欺がある。これらの手法は、ユーザーを欺いて信頼を得た後、機密情報の入力や悪意のあるファイルのダウンロードを誘導する。

2025年のサイバー脅威動向

攻撃タイプの統計 – 産業別攻撃回数

2025年下半期の産業別攻撃件数を見ると、サービス業が1,835,853件で最も多かった。小売業（508,380件）、重工業（355,122件）、電子・半導体（245,501件）が続いた。

2025年下半期 産業別攻撃回数



2025年のサイバー脅威動向

攻撃タイプの統計 – 産業別攻撃タイプ

2025年下半期 - 産業別攻撃タイプ別比率

	Inject Unexpected Items	Collect and Analyze Information	Manipulate Data Structures	Subvert Access Control	Manipulate System Resource
Service	43%	33%	12%	9%	1%
Retail	37%	50%	7%	3%	1%
Heavy Industry	51%	34%	8%	3%	1%
Electronics	48%	14%	20%	12%	1%
Media	38%	40%	9%	10%	2%
Education (Others)	28%	62%	6%	3%	1%
Manufacturing	48%	37%	11%	2%	1%
Food/Travel	41%	48%	6%	5%	0%
Insurance	30%	62%	4%	4%	0%
Public	40%	45%	7%	5%	1%
Enterprise (Others)	50%	41%	6%	2%	0%
ISP	38%	53%	6%	3%	0%
Securities	53%	30%	9%	3%	4%
Finance (Others)	44%	39%	12%	3%	1%
Savings Bank	41%	36%	10%	8%	0%
Education	49%	42%	6%	3%	1%
Law/Tax	50%	29%	13%	6%	0%
Construction	35%	51%	8%	4%	1%
SMB	80%	1%	9%	3%	0.0%

2026年の展望

→ 2026年展望 Top 5

1. AI を活用したサイバー攻撃の急速な拡大
2. ランサムウェア攻撃の増加と被害の深刻化
3. オープンソースを悪用したサプライチェーン攻撃
4. 国家重要インフラへの脅威が拡大
5. Linux 関連の脅威が増加

2026年の展望

1. AI を活用したサイバー攻撃の急速な拡大

→ アンラボの AI セキュリティ戦略の詳細はこちら

AI を活用した「カスタマイズ型」攻撃

2026年には、AI がリアルタイムで被害者の環境を分析し、標的を的確に狙う攻撃が可能となるマルウェアを生成・実行する適応型攻撃が拡大する。特にAIは、検知回避のための多様なコード変種を生成できるため、既存のセキュリティシステムを回避できる。これにより、静的検知中心のセキュリティでは対応が困難となり、動的分析と行動ベース検知の重要性がさらに高まると予測される。

また、ディープフェイク技術の高度化により、実在人物の音声や顔を精密に模倣したリアルタイムフィッシングが、ビデオ会議や電話通話で悪用される可能性が高い。ディープフェイク技術の品質が向上するにつれ、特定人物の声を悪用して金融情報などの機密データを窃取するディープフェイク攻撃は、被害者が識別困難なレベルまで進化すると見られる。

AI を活用した詐欺の自動化にも注目すべきだ。偽の投資サイト、チャットボット、ショッピングモールなどを大量生成し、被害者と自然に相互作用させる見込みである。既に攻撃者はAIを基盤に肉眼で区別が困難なレベルのフィッシングウェブサイトやメールを制作しており、こうした自動化及び大量生産能力は、攻撃キャンペーンの爆発的な増加につながるだろう。

このほか、AI は攻撃者が新たなハッキング手法を開発する上でも大きく貢献するだろう。脆弱性検知とパターン分析を通じて未知のセキュリティ脆弱性を見つけ出し、ゼロデイ攻撃に活用することも可能だ。結局、攻撃者の AI 活用はハッキングの参入障壁を下げつつ、攻撃頻度と正確性を高めることになる。

AI を狙った攻撃の拡大

AI モデル自体を攻撃対象とする攻撃手法もさらに発展するだろう。 攻撃手法は大きく、プロンプト注入及びデータポイズニング、プロンプト漏洩、モデル逆分析などに分類される。まず、攻撃者はチャットボット、自動分析システム、セキュリティAIなどに悪意のある入力を注入したり、学習データを操作して意図的な誤動作や情報漏洩を引き起こす。これは AI を利用するシステムや AI ベースのセキュリティソリューションなどの信頼性と完全性を根本から脅かす。

攻撃者はプロンプト漏洩を通じてAIに対するプロンプトを窃取することもできる。プロンプトがGitHubなどのコード共有プラットフォームを通じて漏洩すると、攻撃者がこれを悪用して AI を不正に操作する。最近 AI モデルの使用が増えるにつれ、プロンプト漏洩とこれを防御するデータセキュリティにも格段の注意が求められる見通しだ。

また、攻撃者はAIモデルに反復的なクエリを実行してモデルの動作方式を分析し、学習データを奪取するモデル逆解析を実行できる。モデルの応答に基づいて学習データと内部構造を把握し、機密情報を流出させる方式である。攻撃者はセキュリティ脆弱性のある AI モデルに対して逆分析を実行し、攻撃を拡大していくと見られる。

主要内容

- AI ベースのマルウェア、ディープフェイク、詐欺自動化、ゼロデイ脆弱性発見など、ターゲット特化型攻撃の増加
- AI モデルの利用が広がるにつれ、プロンプトインジェクション、プロンプト漏洩、モデル逆解析など AI を狙った攻撃手法も高度化

2026年の展望

2. ランサムウェア攻撃の増加と被害の深刻化

→ アンラボのランサムウェア統合セキュリティ戦略の詳細はこちら

ランサムウェア組織の分断化とカルテル化の加速

2025年、ロックビット（LockBit）、ランサムハブ（RansomHub）などの大型ランサムウェアグループの勢力が弱体化し、活動を停止した。しかし、ランサムウェア生態系自体が弱体化したわけではない。大型グループの弱体化への反動として、アキラ（Akira）、キリン（Qilin）、プレイ（Play）、ガンラ（Gunra）など数多くの小型・新興グループが大量に登場した。 先に、2025年の動向で見たように、新興グループは活発に攻撃を実行しており、このように再編されたランサムウェア生態系は2026年も同様の傾向が予想される。

APT グループとランサムウェア組織間の協力、および RaaS（Ransomware as a Service）基盤の 「ランサムウェアのカルテル化」 は、2026年にさらに深化すると見られる。 中央プラットフォームが攻撃に必要なインフラとツールを提供し、系列会社が攻撃を実行した後、「80対20」で収益を分配するモデルは、ランサムウェア生態系である程度定着したようだ。また、2025年に一部確認された APT グループとランサムウェア組織間の協力は、2026年に国家間の地政学的対立が激化する中で、より活発に進展すると見られる。

防御側の立場では、攻撃者がハッキングの参入障壁が低下した状況でより多様かつ多数の攻撃を実行できるため、セキュリティの難易度が上昇する。特に、ランサムウェアの生態系が細分化され連携も頻繁化することで、攻撃グループを特定することがより困難になると予想される。

中小企業を狙った攻撃の増加

2025年のランサムウェア動向の主な特徴は、参入障壁の低下と攻撃の多様化である。金銭的利益が最優先目的である攻撃者にとって、一度の攻撃でより大きな収益を得られる大企業を標的とするのは合理的であり、2026年も大企業はランサムウェアグループの主要な標的となるだろう。

ただし、多様な攻撃をより容易に実行できる現状では、相対的にセキュリティ態勢が脆弱な中小企業を狙った攻撃がより急速に増加すると予測される。特に、攻撃者はランサムウェアの新種や亜種を作成して攻撃を継続できるため、体系的なマルチレイヤーセキュリティの構築が困難な中小企業を対象とした攻撃は成功率が高まる可能性がある。

実際、2025年にも攻撃者が大企業ではなく中堅企業を主要ターゲットとする戦略へ転換する動きが確認されている。規模の小さい企業ほど、精密な標的型攻撃、内部者買収、ソーシャルエンジニアリング技法に特に注意を払う必要がある。また、同様の攻撃がいつでも再発する可能性がある
可能性があることを認識し、脅威を事前に識別して予防できるセキュリティ体制を整える必要がある。

主要内容

- ランサムウェア産業は犯罪者の収益モデルとして定着し、ランサムウェアの名前が変わるだけで攻撃は持続的に増加すると予想
- システム内のファイル暗号化を超え、データベース、バックアップソリューション、仮想化環境などに対するランサムウェア攻撃が増加
- ランサムウェア攻撃の参入障壁が低下した分、セキュリティ態勢が脆弱な中小企業を対象とした攻撃が増加する見込み

2026年の展望

3. オープンソースを悪用したサプライチェーン攻撃

→ XDR と ZTNA を活用したAhnLabのサプライチェーンセキュリティ戦略の詳細はこちら

オープンソース環境の脅威拡大

2025年、オープンソースパッケージレジストリを狙ったサプライチェーン攻撃が急増した。悪意のあるパッケージが大規模に拡散し、開発者及び CI/CD 環境のパスワードやトークンが流出する事例が多数確認されている。現代のソフトウェア開発の90%以上がオープンソースコンポーネントに依存していることを考慮すると、単一パッケージの侵害は数千の関連プロジェクトにまで連鎖被害を引き起こす可能性がある。

2026年においても、こうした脅威はさらに深刻化する見込みだ。特に、**攻撃者がインストール時点や CI パイプラインで機密情報を収集し、連鎖感染を引き起こす攻撃がより巧妙化すると予想される。**タイポスクワッティング、正規パッケージのメンテナンス担当者アカウント乗っ取り、依存関係混乱攻撃など、多様な手法が複合的に活用される可能性が高い。

こうしたサプライチェーン攻撃の対象となる企業にとっては、**オープンソースの使用状況と全体的なデータフローをリアルタイムで監視し、オープンソースパイプライン全体にわたる可視性を確保することが最も重要な課題となる。**これにより、脆弱性発生時に即時対応が可能となり、被害を最小化しながら回復力を備えることができる。

ソフトウェアからクラウド、ハードウェアまで

2025年のサプライチェーン攻撃は、ソフトウェアを超えクラウドサービス、MSP、セキュリティソリューションプロバイダーにまで拡大する傾向が見られた。例えば、攻撃グループ DragonForceとScattered Spider はクラウド MSP を攻撃し、数十の顧客企業に同時に被害を与える「連鎖サプライチェーン攻撃」を実現したことがある。

また、サプライチェーン攻撃においてソフトウェアを超えハードウェアまで活用される事例も確認された。2025年にはAndroid OS ベースのスマートフォンやセットトップボックス (set-top box) など、一部の機器がメーカー出荷前からマルウェアを含んだ状態で流通する事例があった。こうした機器が感染した状態で大規模に流通すれば、被害規模は計り知れないほど大きくなる。

2026年においても、攻撃者は被害規模拡大のため、ソフトウェア、クラウド、ハードウェアなどドメインを問わず攻撃を敢行すると予測される。そして、サプライチェーン攻撃は今や国境を越えた問題であるため、2026年には国家間協力に基づくサプライチェーンセキュリティフレームワークの必要性が過去に比べ強調される見込みだ。

Key Takeaways

- オープンソースは現代ソフトウェア開発の核心であるが、その開放性と広範な依存関係のため攻撃者にとって魅力的な標的
- オープンソースを安全に使用するためには、オープンソースパイプライン全体にわたる可視性と制御力の確保が必要
- 2026年にはソフトウェア、クラウド、ハードウェアなどドメインを問わずサプライチェーン攻撃が実行されると予測される

2026年の展望

4. 国家重要インフラへの脅威が拡大

→ アンラボの CPS 統合セキュリティ戦略の詳細はこちら

国家基盤施設への攻撃拡大

2025年、全ランサムウェア攻撃の半数が製造、医療、エネルギーなどの重要インフラを標的としたことが明らかになった。重要インフラが集中攻撃を受ける理由は、操業停止懸念による支払い可能性、高価値データ、相対的に不足するセキュリティ投資など多岐にわたる。

今年の産業別被害を見ると、サービス産業はデジタル変革の加速化により最も大きな被害を受けた。製造業はスマートファクトリーの拡大に伴い攻撃が急増した。従来は避けられていた医療分野への攻撃も継続的に発生しており、患者の生命に直結する医療機関は攻撃者にとって高収益を狙える標的となった。こうした基盤施設攻撃の傾向は2026年も継続すると予測される。

また、来年攻撃が増加すると予測される分野は、鉄道、海上、航空輸送ネットワークと通信網などである。該当施設のデジタル化が進むにつれ、港湾と船舶管理システム、航空機管制システム、空港保安システムなどが攻撃対象となり得る。通信網は政府、企業、個人の全データを結ぶ核心インフラとして攻撃頻度が高まっており、2026年には攻撃拡大が予想される。

大半の攻撃者の動機は金銭的利益だが、**2026年には一部国家が支援する脅威グループが地政学的対立を理由に攻撃を敢行すると見られる。**国家間の対立が続く中、社会基盤施設に対するサイバー攻撃もさらに巧妙化していく見通しだ。

産業のデジタル化、攻撃者の標的となる

国家基盤施設の攻撃を貫くキーワードはまさに「デジタル化」である。従来アナログ形態で運用されていたり、外部と断絶された OT ネットワーク環境で運用されていた産業システムは、外部ネットワークに比べて安全であるという認識があった。しかし、こうした環境のデジタル化が加速するにつれ、外部接点が拡大し攻撃対象領域が増加している。そして攻撃者は、こうした攻撃対象領域を狙って攻撃を実行する。

産業施設のデジタル化により最も顕著な変化は、従来の OT から OT と IT を包括する「CPS（Cyber-Physical System）」への概念転換である。**閉鎖された OT 環境の外部接点が増えるにつれ、IT、IoT、クラウド接続まで包括するセキュリティが必要となった。**実際、最近のスマート製造環境ではIoTを含む様々な最新デバイスが適用されているのが確認できる。

CPS 環境を標的とした攻撃手法も高度化している。OT ネットワークが IT 環境と接続される特性を狙い、まずIT 環境を侵害した後、OT ネットワーク内部へ侵入する方法が多く用いられている。OT 環境を標的にして作成されたマルウェアやランサムウェアも発見されている。こうした CPS 環境を狙った攻撃は、2026年を過ぎた未来においても拡大し続けると予想される。

Key Takeaways

- インフラのデジタル化、地政学的紛争、技術の武器化いより、 CPS 環境における国家インフラの脅威
- 国家基盤施設が攻撃を受けた際に迅速に復旧するため、バックアップ体制、復旧プロセスなどサイバー回復力強化が必須

2026年の展望

5. Linux 関連の脅威が増加

→ アンラボの Linux セキュリティ戦略の詳細はこちら

増加する脆弱性、高度化する攻撃

アンラボのデータによると、2025年6月の1か月間だけで176の Linux システムを対象に、1万2千件を超える攻撃が発生した。月ごとに差はあるものの、毎月平均的に100以上のシステムが攻撃を受け、数千件から多い場合は1万件以上の攻撃が発生している。 攻撃の種類も▲DDoSボット▲コインマイナー▲バックドア▲ランサムウェアなど多岐にわたる。Linux の脆弱性も数千件に上り、Linux 環境を標的とした新規マルウェアも2025年上半期だけで6万件以上発見された。 **Linux 環境に対する攻撃頻度、脆弱性数、マルウェア数は2026増加傾向が続くと予想される。**

2025年、国内通信会社の Linux サーバーが侵害され、約2,300万人の顧客個人情報が流出する事件が発生した。攻撃には Linux ベースの BPFDoor バックドアが使用された。攻撃者は Web シェル及びリモートコード実行（RCE）脆弱性を通じて内部システムに侵入した後、HSS サーバーに BPFDoor をインストールし、SIM 情報を窃取した。 **先に、2026年には国家基盤施設の攻撃拡大が予測されていたが、その延長線上として Linux サーバーに対する攻撃も増加すると予想される。**

Linux サーバーへの攻撃が増加する理由は単純である。多数のクライアントPCに接続されており、多様なビジネス重要データが保存されているためだ。**特に、クラウドインフラの大半が Linux ベースで運用されるにつれ、攻撃対象領域が急速に広がっている。** AWS、Microsoft Azure、Google Cloud などの主要クラウド環境や、Docker、Kubernetes のようなコンテナプラットフォームはすべて Linux を基盤としている。Linux システム1台が侵害されると、数百の仮想マシンとコンテナが同時に脅威に晒される可能性がある。

また、**攻撃者はゲスト OS ではなくハイパーバイザー層を直接狙う戦略へ移行している。**2025年6月、Akira ランサムウェアは VMware ESXi や Hyper-V を超え、Nutanix AHV（Acropolis Hypervisor）の仮想マシンディスクファイルの暗号化に成功した。仮想化プラットフォームの多様化が攻撃対象領域の拡大につながっている。 一度の侵害で数百台の仮想マシンを数時間以内に無力化できるため、攻撃効率が最大化される。ランサムウェアをはじめ、Linux ベースのシステムを狙ったマルウェアが増加しており、ビジネス中断など深刻な被害につながる可能性がある。

高度化した Linux 攻撃は、断片的なセキュリティアプローチでは対応が困難である。攻撃がエンドポイント、メールなど多様な区間で開始され、新種・亜種のマルウェアが頻繁に出現するためだ。**したがって、アンラボのセキュリティアーキテクチャのように複数の区間にわたり最適なセキュリティ機能を実行する統合セキュリティシステムの重要性が高まるだろう。**

主要内容

- 運用および性能効率のため、サーバー環境における Linux の使用が増加しているが、セキュリティ管理は不十分な傾向にある
- 仮想化環境と Linux を狙った攻撃が増加する見込み – 1回の攻撃で数百台の仮想マシンを侵害可能
- 複数のセグメントにわたり最適なセキュリティ機能を実行する統合セキュリティシステムの重要性が高まる

AhnLab

AhnLab, Japan
〒 108-0014東京都港区芝 4丁目 13-2田町フロントビル 3階
Tel: +81 3 6453 8315 | Fax: +81 3 6453 8316 | Email: jp.sales@ahnlab.com
Website: www.ahnlab.com/jp | Facebook: www.facebook.com/AhnLabSP | YouTube: www.youtube.com/OfficialAhnLab