AhnLab サイバー脅威インテリジェンスレポート

TLP : CLEAR

分析レポート

2025年日本企業を対象としたランサムウェアの被害状況

AhnLab セキュリティインテリジェンスセンター(ASEC)

2026年1月22日

AhnLab

ドキュメントレベルに関するご案内

刊行物や提供されるコンテンツは、以下のようにドキュメントレベルごとに許可された範囲内でのみ使用が可能です。

ドキュメントレベル	配布対象	注意事項
TLP：RED	特定顧客の報告書受信者に限定して提供される報告書	**報告書の受信者または受信部署のみアクセスが許可されたドキュメント** 受信者以外への複製・配布不可
TLP：AMBER+STRICT	特定顧客の内部組織に限定して提供される報告書	**報告書の受信組織（会社）の内部では複製・配布が可能** ただし、組織外での教育目的などで使用する場合はアンラボの許可が必須
TLP：AMBER	特定顧客およびその顧客の顧客に限定して提供される報告書	**報告書の受信組織（会社）の内部およびその組織の顧客には複製・配布が可能** ただし、対象者以外への教育目的などで使用する場合はアンラボの許可が必須
TLP：GREEN	サイバーセキュリティコミュニティに提供される報告書 (業務提携を締結した外部機関を含む)	**該当業種などでは自由に使用でき、出典を明記した上で内部教育、同業種、セキュリティ担当者向けの教育資料として活用可能** ただし、一般人を対象とする発表資料としての使用は厳しく制限
TLP：CLEAN	自由に利用できる報告書	**出典を明記した上で商業性の有無にかかわらず利用可能** 編集や改変などの二次的著作物の作成を許可

目次

CAUTION

本報告書には、現時点で確認された情報を基にした分析者の見解が多数含まれています。分析者ごとに見解が異なる場合があり、新たな事実が確認された際には、事前通知なく内容が変更される可能性があります。

序論

日本はアジア地域においてランサムウェア被害件数で第2位に位置しており、世界経済および主要産業分野で影響力を持つ企業が多数存在することから、攻撃者にとって主な標的となっている。なお、インドはアジア地域で被害件数第1位を記録しており、最も大きな被害を受けている国と分析された。特に2023年以降、日本を標的とした攻撃が急増しており、製造業、情報通信業、建設業などの主要産業に被害が集中している。これは、日本企業が保有する膨大なデータ、サプライチェーン上での影響力、ならびに一部産業におけるセキュリティ脆弱性が攻撃者にとって高い経済的利益を狙える機会を与えているためと考えられる。

本報告書では、アンラボが独自に収集したデータと ransomware.live に記録された日本企業の被害データを統合し、2024年11月から2025年10月までの日本企業を対象としたランサムウェア被害事例を統計分析することで主な示唆を提示することに重点を置く。

1) データ概要

報告書の分析対象データのうち、独自収集データは、ランサムウェアグループが運営する DLS（Dedicated Leak Sites）に公開された情報を基にしている。収集されたデータは、攻撃発生時点、DLS 掲載タイトル、ランサムウェアグループ名、被害企業名、産業大分類で構成されており、これを基に日本企業を対象に行われたランサムウェア攻撃の推移および産業別被害状況を分析した。

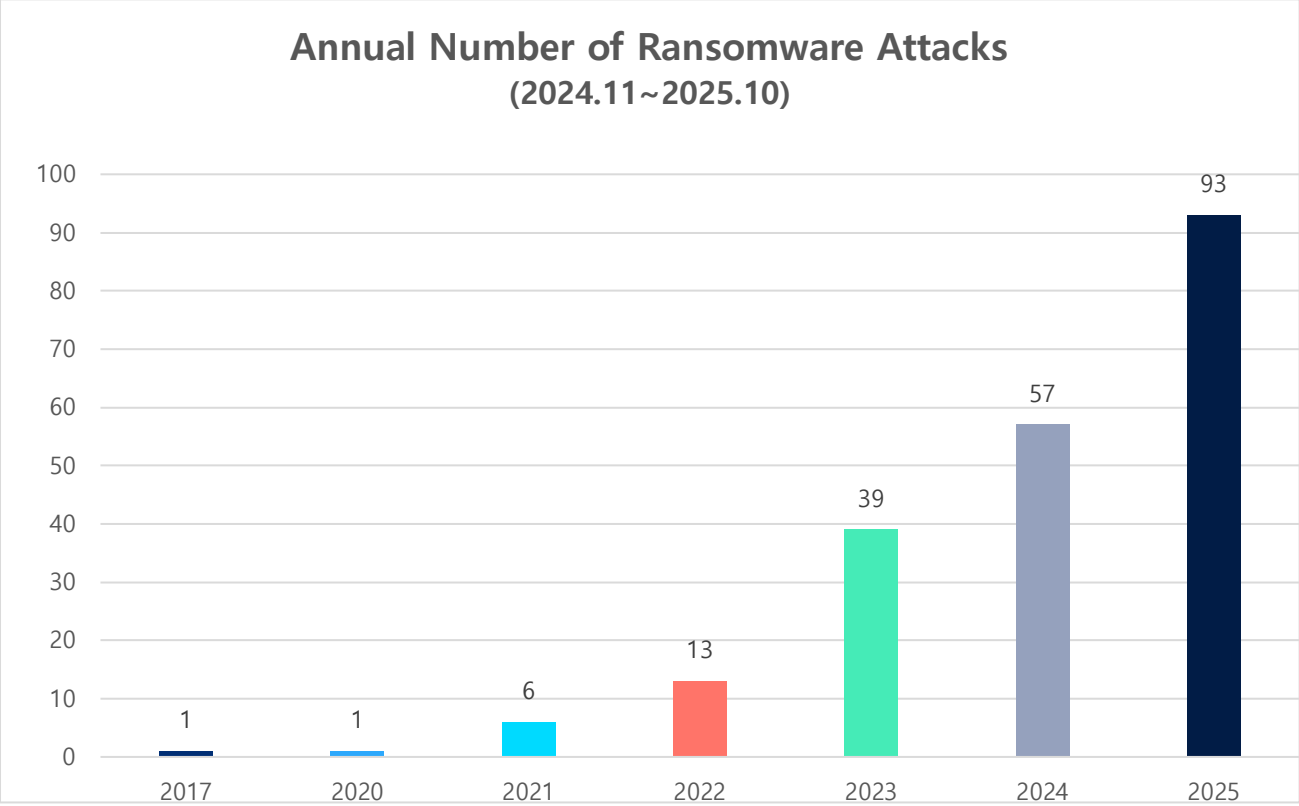
データ収集にあたっては、以下の基準を適用した。第一に、日本企業の範囲には日本に本社を置く企業の海外法人を含む。これは、海外法人が本社と密接に連携しており、海外法人への攻撃が実質的に日本企業の被害につながると判断したためである。第二に、攻撃発生時点は DLS に初めて掲載された日付を基準とする。第三に、産業大分類は日本標準産業分類（JSIC）に基づいて区分する。

本報告書は、独自収集データと外部公開データを組み合わせ、日本国内におけるランサムウェア攻撃の動向をより定量的に分析するとともに、ランサムウェア脅威の特性および主な標的となる産業をより深く理解することに焦点を当てたものである。これらの分析結果を踏まえ、今後日本企業がランサムウェア攻撃に備えるためのセキュリティ戦略策定に資する基礎資料を提供することを目的とする。

被害状況の分析

1）年度別侵害件数の増加

2017年から2025年10月までのデータを分析した結果、日本企業を対象としたランサムウェア侵害事例は継続的な増加傾向を示している。2024年（1～12月）には計57件が報告され、2025年（1～10月）にはすでに93件へと急増した。両期間を補正し、月平均の攻撃件数に換算すると、2024年は約4.75件/月、2025年は約9.3件/月となり、約2倍に増加したと分析される。これは、攻撃の頻度と密度の双方が大幅に高まっていることを意味する。



[図 1] 年度別ランサムウェア侵害件数

2017年から2021年にかけては、侵害件数がそれぞれ1件、1件、6件と低水準で推移しており、攻撃は散発的に発生していた。しかし、2022年（13件）を起点として増加傾向が顕在化し、2023年には前年の約3倍となる39件が記録され、本格的な拡大局面に入った。この時期以降、ランサムウェアグループが日本市場を主な標的として認識し始めたと考えられる。

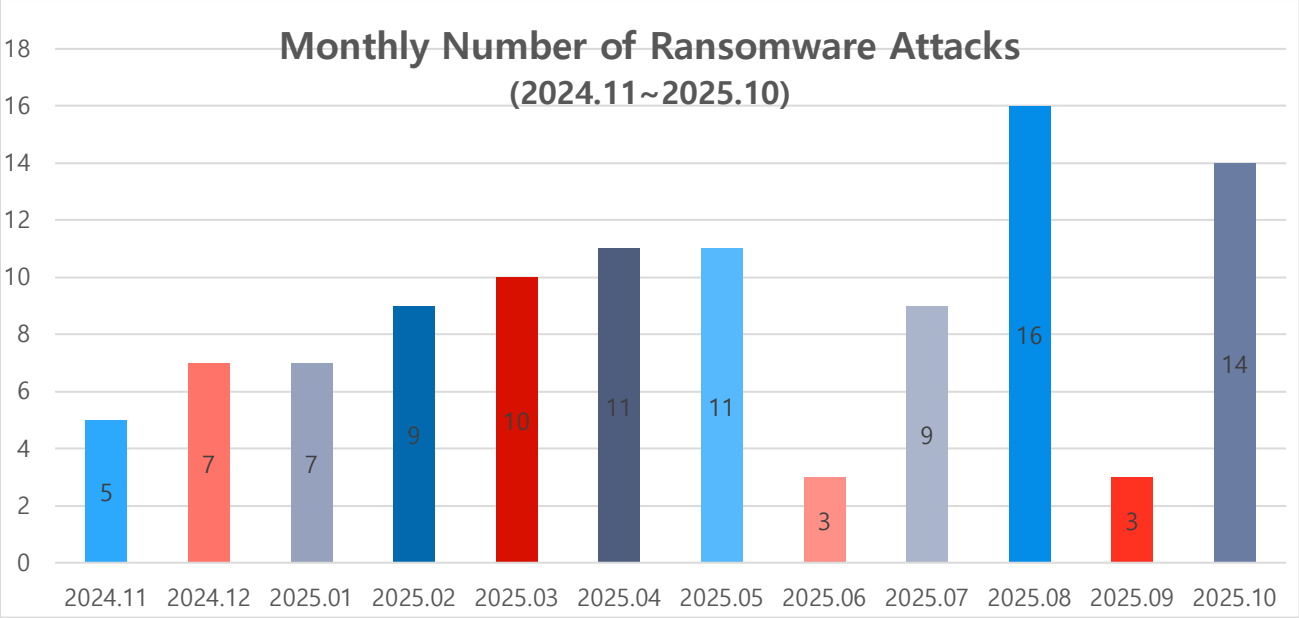
2024年には攻撃件数が57件に達し、増加傾向が継続した。特に、攻撃の時期的な集中度が高まり、主要産業を狙った精緻な侵入試行が多数確認された。さらに2025年は、わずか10か月間で93件が報告されている。これは、攻撃が単発的あるいは季節的な事象を超え、年間を通じた常時的・継続的なキャンペーンへと移行した結果であると解釈される。

攻撃頻度が上昇した主な要因としては、従来の大規模グループ（LockBit、BlackCat など）が法執行機関による摘発を受けた後、新興および中堅グループ（Qilin、SafePay、Hunters International（現 World Leaks）など）が攻撃を拡大したこと、ならびに RaaS（サービスとしてのランサムウェア）におけるアフィリエイトの分散的活動が複合的に作用した点が挙げられる。こうしたエコシステムの再編は攻撃の持続性・連続性を高め、月間攻撃件数の増加につながった。

以上を踏まえると、2025年における攻撃急増は、単なる量的拡大にとどまらず、ランサムウェアのエコシステムが新たな安定段階に移行し、攻撃者が活動戦略を常時・分散型へと再構築した結果であると評価できる。攻撃が特定の時期に限定されず、年間を通じて継続する傾向が強まっていることから、日本企業には既存のセキュリティ方針の見直しおよび継続的な脅威検知、対応体制（CTI に基づくモニタリング）の強化が求められる。

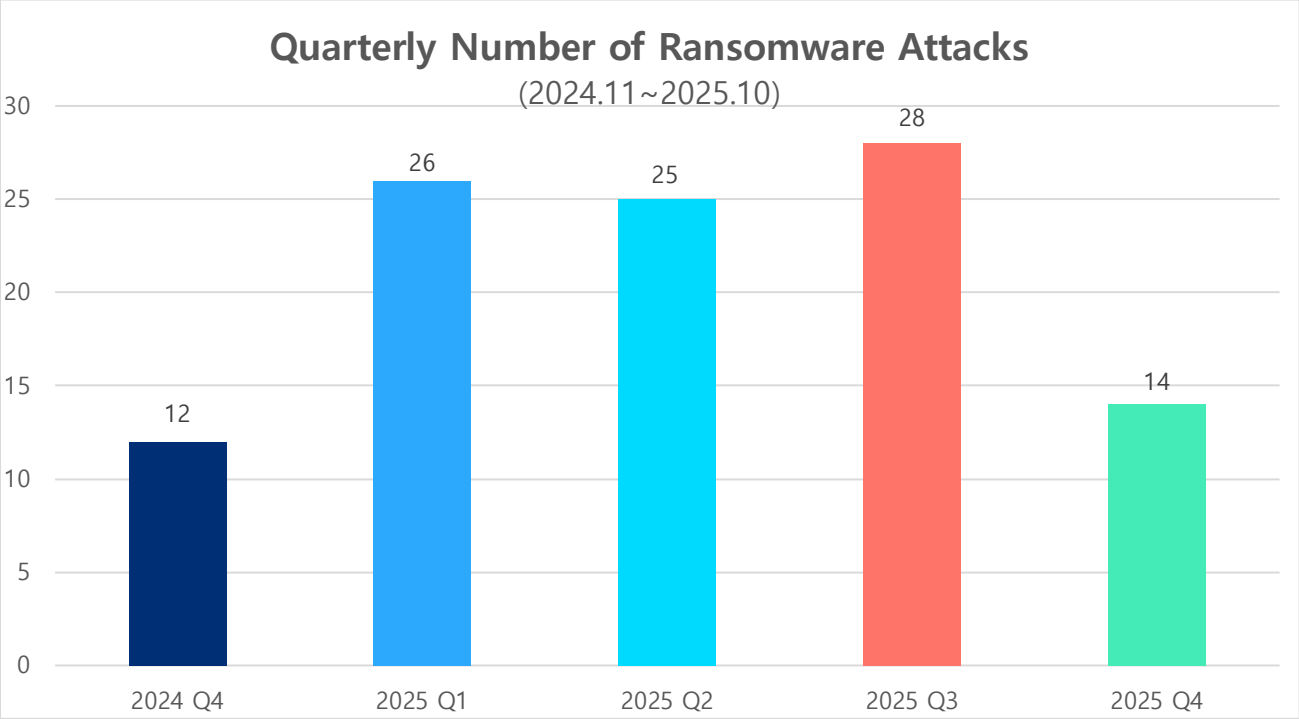
2) 月別侵害件数

2024年11月および12月におけるランサムウェア攻撃は、それぞれ5件、7件と報告されており、特定の時期に集中する明確なパターンは確認されなかった。攻撃は比較的低水準で散発的に発生していたものの、年末に向かうにつれて緩やかな増加傾向が見られた。



[図 2] 月別ランサムウェア侵害件数

2025年に入ると、ランサムウェア攻撃は前年末を上回る水準で推移し、連続的な拡大傾向を示した。1～3月は月7～10件程度の攻撃が継続し、上昇基調を維持した。4月および5月も同程度の水準が続いたが、6月は一時的に3件まで減少した。ただし、これは例外的な動きに近く、7月以降は再び攻撃頻度が上昇し、8月には16件、10月には14件が記録されるなど再び高い脅威水準となった。特に8月は当該期間中で最も多くの侵害事例が集中した月であり、攻撃キャンペーンが積極的に展開された状況を示している。



[図 3] 四半期別ランサムウェア侵害件数

四半期別に見ても同様の傾向が明確に表れている。2024年第4四半期は計12件と比較的低水準であったのに対し、2025年第1四半期から第3四半期にかけてはそれぞれ26件、25件、28件が報告され、全体として高い攻撃密度が維持された。2025年第4四半期についても、10月時点ですでに14件が発生しており、年末にかけて再び増加する可能性が示唆される。

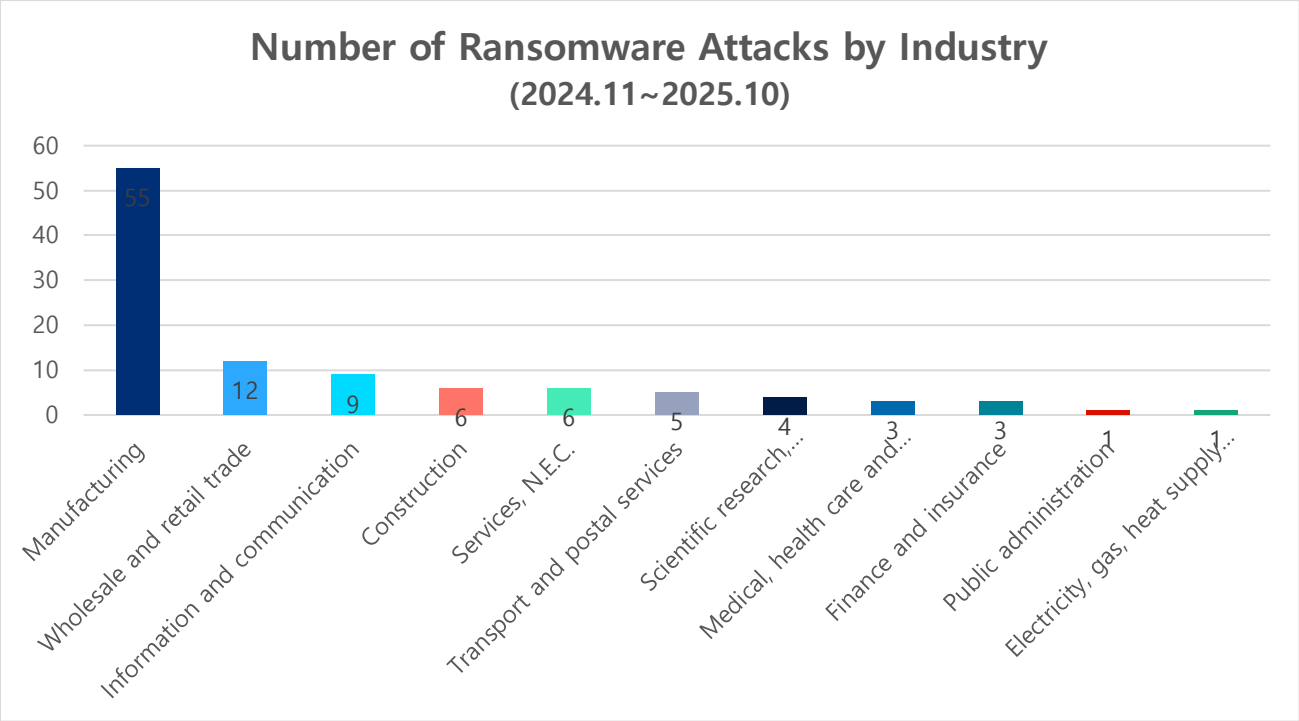
ランサムウェア攻撃は特定の時点に限定された単発的事象ではなく、年間を通じて繰り返されるキャンペーン型攻撃として継続していることが分かる。一見すると特定の四半期や時期に集中しているように見えるものの、実際には年間の大部分において恒常的なリスク状態が続いている。ただし、年末年始や特定産業において業務が集中する時期（決算期、休暇明け、事業再開など）に攻撃が増加する傾向も一部確認されており、こうした外的要因と攻撃時期との相関関係を継続的に分析する必要がある。

今後は、特定産業が相対的に脆弱となる特定の四半期や時点が存在するかについてより精緻な分析を行うとともに、攻撃者が周期的にキャンペーンを展開する特性を踏まえた常時かつ先制的な対応戦略を構築することが重要であると判断される。

3) 産業別被害状況

被害を受けた産業の中では製造業（55件）が全攻撃件数の中で圧倒的な割合を占めており、ランサムウェア攻撃の主要標的であることが確認された。製造業は大規模な生産設備およびグローバルなサプライチェーンを基盤として運営されており、OT（運用技術）と IT システムが複合的につながっている。このような構造的特性から、システム停止が発生した場合の生産遅延や金銭的損失が極めて大きく、攻撃者にとっては交渉圧力をかけやすい産業であると評価される。特に、中堅・中小の製造業を中心にセキュリティインフラが相対的に脆弱な組織が多数確認された。

卸売・小売業（12件）および情報通信業（9件）も高い攻撃頻度を示した。卸売・小売業はサプライチェーン攻撃のリスクが高く、情報通信業は大量の顧客データとネットワークインフラを保有していることから、攻撃が成功した場合の影響範囲が大きい点で主な標的となっている。さらに、建設業（6件）、運輸・郵便業（5件）、学術・専門技術サービス（4件）、医療・福祉（3件）、金融・保険（3件）、行政（1件）、電気・ガス・熱供給業（1件）など、多様な産業分野で被害が報告された。これらの産業はプロジェクトベースの業務や重要データ（設計図、契約書、患者情報など）を扱うケースが多く、攻撃者が金銭的な交渉力を最大化しやすい環境であるという共通点を有している。



[図 4] 産業別ランサムウェア攻撃状況

学術サービス、教育支援サービス、電気・ガス、金融・保険、行政、芸術・エンターテインメントなどの分野においても計 6 件の被害が確認されており、全産業が攻撃対象となっていることが明らかとなった。これは、特定産業に限定した対策では不十分であり、産業全体にわたるセキュリティ強化が必要であることを示唆している。

特に 2025 年の韓国では、例外的に製造業よりも金融業におけるランサムウェア被害が多く報告されたが、これはあくまで特異な事例であり、通常は日本・韓国ともに製造業が最も高い被害割合を示している。したがって、両国においては基幹産業に対する継続的な防御体制の強化が不可欠であり、特定産業のみに注力した対策はかえって新たな脆弱性を生み出す恐れがある。韓国の金融業界における今回の事例が示すように、攻撃者は資金の流れや決済インフラといった高収益構造を狙い戦略を転換する可能性があるため、日本においても金融・通信など非製造分野への備えを怠るべきではない。

主要ランサムウェア攻撃グループ

本統計期間において、日本企業を対象に最も活発に攻撃を行ったグループは Qilin（19件）であり、全体の約18%を占めた。これに続き、Unknown（13件、グループを特定できない場合）、SafePay（5件）、Lynx（4件）、World Leaks（4件）、Akira（3件）、Clop（3件）、Devman 2.0（3件）、Hunters（3件）などが主要な活動グループとして確認された。上位10グループが全体の半数以上を占めており、攻撃が依然として少数の活発なグループに集中している状況がうかがえる。

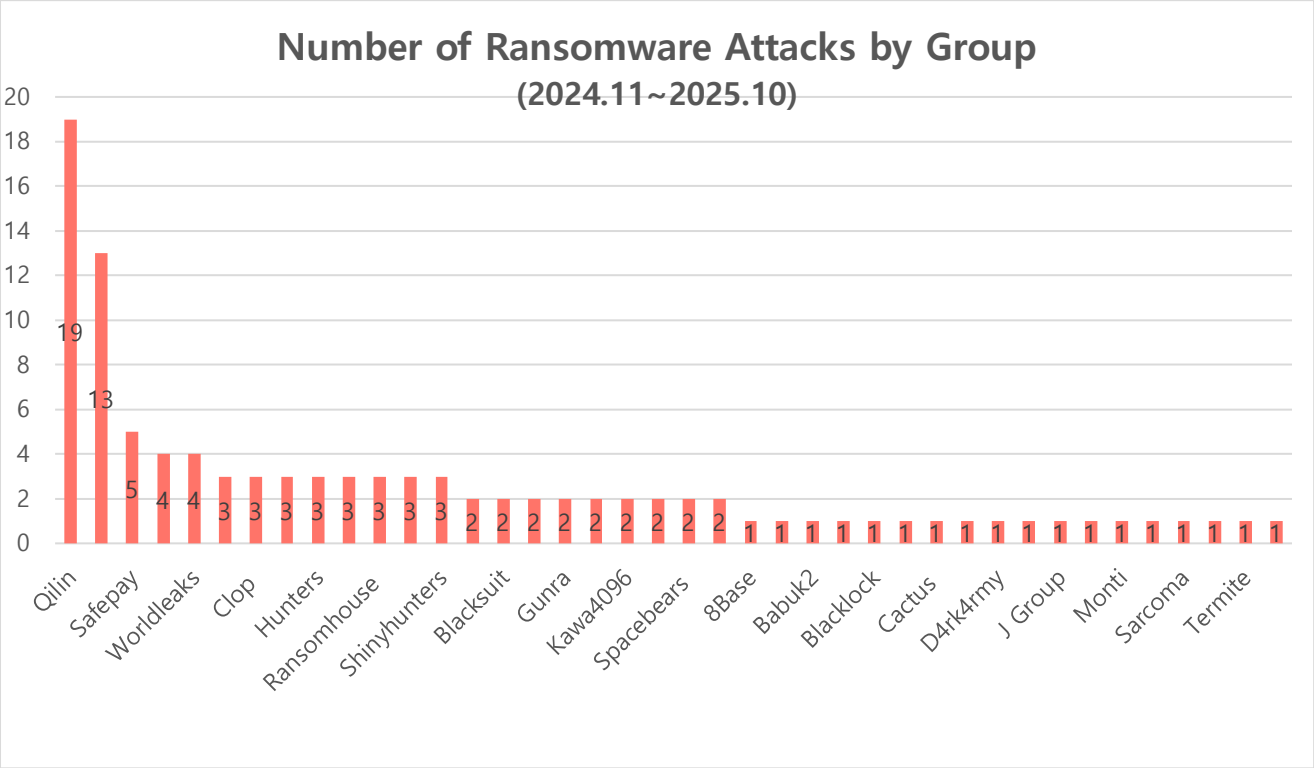
2024年以降、ランサムウェアのエコシステムは中堅・新興グループを中心とした再編が加速している。かつて市場を主導していた LockBit、Alphv（BlackCat）、8Base といった大規模グループは、法執行機関による摘発、内部インフラの崩壊、DLS の閉鎖などの影響を受け、活動が急速に縮小した。その結果として生じた空白を Qilin、SafePay、Hunters International（現 World Leaks）といった中堅勢力が素早く埋める動きが見られた。特に Qilin は、2024年下半期以降継続的な攻撃キャンペーンを展開し、アジア地域における代表的なマルチアフィリエイト型グループとして台頭している。

また、Devman や Lynx などは既存グループからコード・インフラを共有する形で登場した派生型（Rebranding/Spawned）グループであり、技術的連続性を維持しつつ、新たな名称および運営戦略の下で活動を継続している。これらのグループは従来の Ransomware-as-a-Service（RaaS）モデルを踏襲しながらも、小規模組織を中心とした攻撃を多数実行する「分散型攻撃パターン」を示している。

一方で、BlackSuit（現在は活動停止）、RansomHub（2025年3月まで活動後、現在は活動停止）、ThreeAM などは一時的に活発な動きを見せたものの、2025年上半期以降は急速に活動が減少あるいは事実上活動停止している。これらの解体後、アフィリエイトが Qilin、Lynx、Play、Dragonforce などに吸収され、グループ間でのアフィリエイト移動やコードの再利用（Reuse）が顕著となっている。この動向は、ランサムウェアのエコシステムが単純な競争構造から脱却し、共通の技術基盤を軸とした協業的形態へと進化していることを示唆している。

総合すると、日本を標的としたランサムウェア攻撃は、従来の大規模グループ主導型構造から多核化した中堅・分散型エコシステムへと再編されつつある。加えて、攻撃主体の多様化やリブランディングの頻度が高まる中で、特定グループの追跡に依存するのではなく、TTP（戦術・技術・手順）に基づく行動分析型のアプローチが一層重要となっている。統計が示すとおり、日本市場を主要標的とするグループは継続的に増加して

おり、日本のみならず韓国やアジア全域においてもより広範かつ複合的な脅威に備える必要性が高まっている。そのため、脅威インテリジェンスの観点からも、多様化するグループの戦術変化やアフィリエイト間の横断的な活動を精緻に追跡・分析する体系的な対応が不可欠である。



[図 5] ランサムウェアグループ別侵害件数

ランサムウェア対応戦略

近年、日本国内におけるランサムウェア攻撃は、攻撃グループの多様化と戦術の高度化が同時に進行し、産業全体へと拡散している。特に製造業はデジタルトランスフォーメーション（スマートファクトリー、IoT 連携など）の過程において工程・設備システムのセキュリティ脆弱性が顕在化しやすく、最も高い被害件数（55件）を記録した。これを踏まえ、日本企業は技術的防御にとどまらず、脅威インテリジェンス、サプライチェーン、組織的対応体制全般を強化する必要がある。以下は、直近の統計および動向を基に導出した対応戦略である。

1. ダークウェブおよび脅威インテリジェンスのモニタリング
   - ダークウェブ、Telegram、ハッカーフォーラムなどにおいて、企業関連データの流出、脅迫情報、アカウント権限の販売に関する投稿を常時モニタリングする。

- OSINT および CTI（脅威インテリジェンス）分析を通じて新興ランサムウェアグループの戦術(TTPs) を把握し、予防的対策を強化する。
- 攻撃グループの多様化傾向（Qilin、Lynx、Devman など）を考慮し、特定グループ依存ではなく、行動（Behavior）ベースの検知体制を確立し、セキュリティ水準を継続的に向上させる。

2. 脆弱性の管理およびパッチプロセスの高度化
   - 製造業といった OT・IT 融合環境では、運用技術（PLC、MES、HMI など）のパッチ遅延が主な侵入経路となる。
   - 定期的な脆弱性評価（VA）および侵入テスト（Pentest）を実施し、デジタルトランスフォーメーション区間におけるセキュリティ脆弱性を早期に特定する。
   - 特定された脆弱性に対して自動化されたパッチ管理ソリューションを導入し、悪用リスクを最小化する。

3. ネットワークおよびシステムセキュリティの強化
   - ネットワーク分割（Segmentation）により、工程ネットワーク、業務ネットワーク、外部ネットワーク間の lateral movement (内部拡散) を遮断する。
   - Zero Trust ベースのアクセス制御および最小権限の原則（Least Privilege）を適用し、攻撃者の内部移動可能性を最小限に抑制する。
   - ネットワークおよびエンドポイントのログを常時収集・分析し、異常なファイル暗号化や SMB トラフィックを早期に検知する。

4. データのバックアップおよび復旧計画の策定
   - 3-2-1ルール（3 copies、2 storage types、1 offsite）を遵守し、バックアップサーバーをネットワークから分離（air-gap）することで、攻撃時のデータ損失を防止する。
   - 定期的な復旧シミュレーションを実施し RTO・RPO（復旧目標）を検証するとともに、実際の侵害状況に備えた復旧手順を標準化する。

5. 攻撃の検知および対応の自動化
   - 侵入検知・遮断システム（IDS/IPS）およびエンドポイント検知・対応（EDR）ソリューションを活用し、攻撃をリアルタイムで検知し遮断する。
   - ランサムウェア感染が疑われる場合は、即時に隔離措置を講じ、被害拡大を防止する。
   - 専門的なデジタルフォレンジックサービスを活用し、初期侵入経路、内部移動、データ流出経路を

精査し、関係者と透明性をもって共有する。
- 日本の主要産業（製造、通信、金融）に特化した攻撃シナリオベースのプレイブックを整備し、対応速度を向上させる。

6. 情報セキュリティ教育および内部プロセスの強化
- ランサムウェアの主な侵入経路であるフィッシングや悪意のある電子メールの添付ファイルに対処するため、全従業員を対象とした定期的な模擬訓練（Phishing Simulation）を実施する。
- 重要データへのアクセスには多要素認証（MFA）を適用し、管理者権限使用時には特権アクセス管理（Privileged Access Management）を義務化する。
- セキュリティ侵害事故発生時の意思決定および報告フロー（Incident Chain）を明確化し、対応の混乱を最小化する。

7. Ransomware-as-a-Service（RaaS）エコシステムの変化への対応
- 既存の有力グループ（LockBit、Alphv、8Base）の瓦解後、Qilin、RansomHouse、Devman などの新興グループが急速に台頭している。
- 企業は新興グループのリブランディング・協業パターンを継続的に追跡し、RaaS アフィリエイト間のコード再利用や戦術共有に注目する必要がある。
- これらの情報収集には、脅威インテリジェンスサービスを積極的に活用する。

8. サプライチェーンおよび外部委託先のセキュリティ検証
- 日本の製造・流通産業における多層的サプライチェーン構造を背景に、下請・外注企業が迂回侵入経路として悪用される事例が増加している。
- 契約時にセキュリティ遵守条項（Security SLA）を盛り込み、定期的なベンダーリスク評価（Vendor Risk Assessment）を実施する。
- 主要サプライチェーンノードの資産識別およびアクセス制御を通じて、サプライチェーン経由の攻撃を遮断する。

9. 多様な TTP に基づくカスタマイズ対応戦略の策定
- 日本国内のランサムウェアグループが攻撃手法・戦術（TTP）を急速に変化させており、単一の防御体制ではすべての攻撃に対応することは困難である。
- 各グループの侵入ベクター（フィッシング、サプライチェーン、リモートサービスの悪用など）を分析し、攻撃段階別（Initial Access → Execution → Exfiltration）の防御戦略を策定する。
- MITRE ATT&CK フレームワークを基盤として組織内部の防御カバレッジ（Defense Coverag

e) を点検し、新たな TTP に応じた検知ルールおよびポリシーを継続的にアップデートする。

- 攻撃者の戦術の多様化およびリブランディング傾向（Qilin、Lynx、Devman など）を踏まえ、単純なシグネチャ検知から脱却し、ビヘイビアベースかつ脅威インテリジェンス連携型の対応体制を構築する。

日本におけるランサムウェア攻撃環境は、グループの多様化と対象産業の拡大という複合的脅威へと進化している。製造業中心の被害構造は依然として維持されているものの、攻撃者は常に高収益・高データ価値を有する産業（金融、通信など）へと標的を転換する可能性がある。そのため、日本企業には、多様な攻撃者、多様な侵入経路、多様な産業を想定した多層的かつ継続的なセキュリティ戦略の実行が求められる。

また、ランサムウェアは技術的対策のみで完全に防御可能な脅威ではないことから、企業はセキュリティ方針を再整備し、多層的な防御戦略を構築することで先制的対応能力を強化すべきである。これにより、日本企業はランサムウェア脅威を効果的に軽減し、長期的なセキュリティ体制を構築できる。

分析レポート

2025 年日本企業を対象とした ランサムウェアの被害状況

(株)アンラボ

〒108-0014 東京都港区芝 4 丁目 13-2 田町フロントビル 3 階

ホームページ：www.ahnlab.com/jp

Tel： +81 3-6453-8315 | Fax： +81 3-6453-8316

AhnLab