

日本企業を対象としたランサムウェアの 被害状況報告書 (2017～2025)

AhnLab SEcurity intelligence Center (ASEC)

2025年 3月 17日

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、対象者外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)	該当の業種などでは自由に使用でき、出典を明記する場合は内部教育、同業種、セキュリティ担当者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には厳しく制限
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2次的著作物の作成を許可

バージョン履歴

バージョン	日付	内容
1.0	2025-03-17	新規作成

目次

序論.....	5
1) データ概要	5
被害状況の分析	6
1) 年度別被害件数の増加	6
2) 月別の被害件数	7
3) 業種別の被害状況	8
主要なランサムウェア攻撃グループ.....	10
ランサムウェア対応戦略	12



本報告書には現在までに確認された内容をベースに、セキュリティアナリストの意見が多く含まれています。アナリストごとに意見が異なる場合があります、新たな根拠が確認される場合、報告書の内容が事前告知なしに変更される可能性があります。

序論

日本のランサムウェアの被害件数はアジアで 2 位を記録しており、グローバル経済および主要産業分野で影響力を持つ企業が多数位置しているため、攻撃者の主要な標的となっている。特に 2023 年以降、日本を対象とする攻撃が急激に増加しており、製造業、情報通信業、建設業など、主要産業が集中攻撃を受けている。これは、日本企業が保有している膨大なデータ、サプライチェーン内の影響力、そして一部の産業分野でのセキュリティの脆弱性が攻撃者に経済的利益を狙う機会を提供しているものと分析される。

本報告書は、このような流れを反映し、アンラボの収集データと Ransomware.live に記録された日本の被害企業データを比較分析し、2017 年から 2025 年まで日本の企業を対象としたランサムウェア被害事例を統計分析して、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、プライマリ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もとにする。収集されたデータは、攻撃発生時点、DLS 掲示タイトル、ランサムウェアグループ名、被害企業名、産業分野大分類で構成されており、これをもとに日本企業を対象に実行されたランサムウェア攻撃の推移および産業分野別の被害状況を分析した。

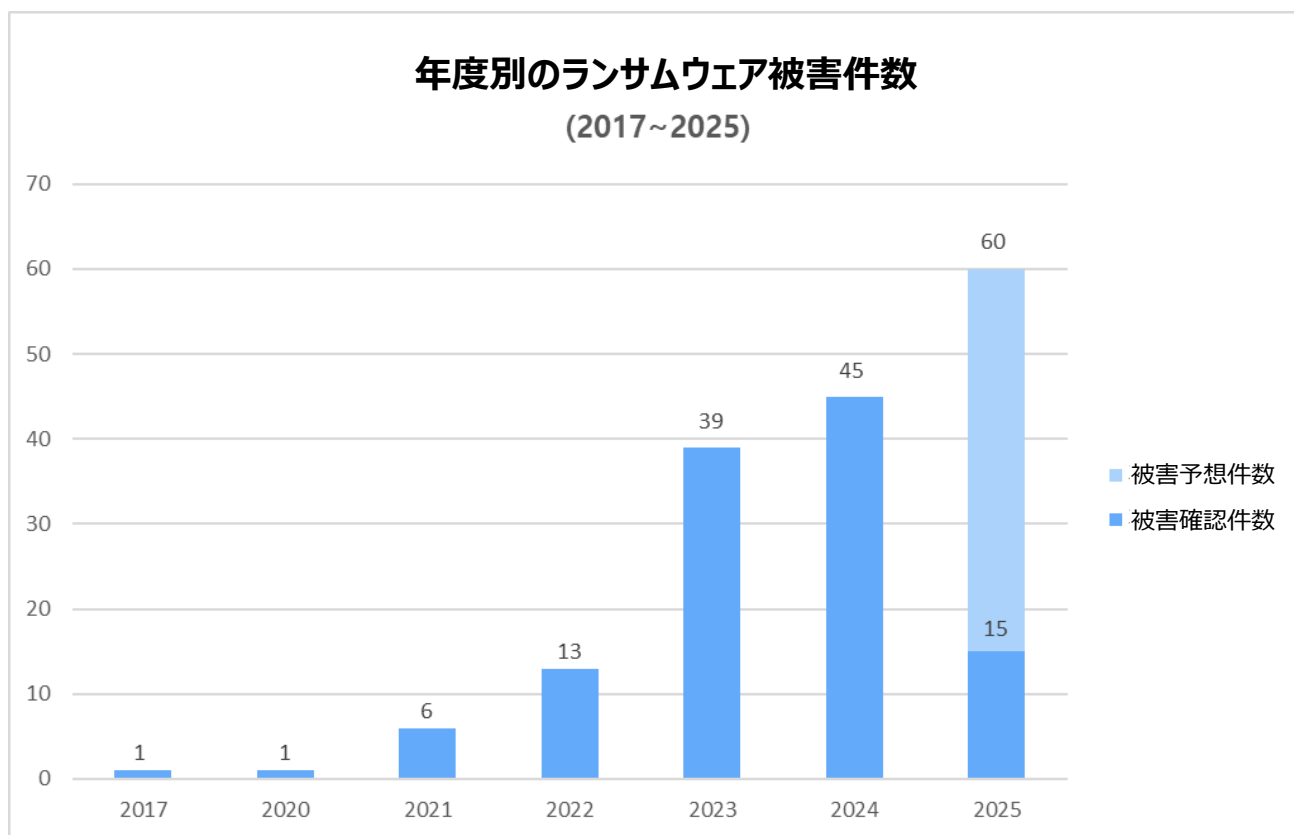
データ収集プロセスは、次のような基準を適用した。第一に、日本企業の範囲は、日本に本社を置く企業の海外法人を含む。これは、海外法人が本社と緊密に連携しており、その法人に対する攻撃が実質的に日本企業の被害に繋がるという判断に基づく。第二に、攻撃発生時点は、DLS に初めて掲示された日付を基準に設定する。第三に、産業の大分類は、日本標準産業分類 (JSIC) を基準に区分する。

今回の報告書は、プライマリデータと外部公開データを結合して、日本国内のランサムウェア攻撃動向をより定量的に分析し、ランサムウェアの脅威の特性と主要ターゲットとなる産業をよりよく理解することに焦点を当てた。これをもとに、今後日本企業がランサムウェアの攻撃に備えられるよう、セキュリティ戦略立案の基礎資料を提供していく。

被害状況の分析

1) 年度別被害件数の増加

日本企業を対象とするランサムウェアの被害件数は、2017年から 2024年まで持続的に増加する傾向を示している。特に 2023年から攻撃件数が急増しており、特定の産業分野と時期に集中して発生する傾向が確認された。



[図1] 年度別のランサムウェア被害件数

2017年から 2021年まではランサムウェアの被害事例が比較的に低いレベルを維持しており、攻撃が散発的に発生する傾向を示した。しかし、2021年から徐々に増加傾向が現れ始め、以降本格的な拡散の兆しが見え始めた。

2022年にはランサムウェアの被害事例が合計 13件発生しており、これは前年（2021年、6件）に比べて2倍以上増加した数値である。一年中攻撃が続いていたが、特定の時期に集中して発生するのではなく、徐々に増加する様相を見せた。これは、2023年以降本格的な攻撃の拡散の前兆現象と解釈できる。

2023年には第2四半期 (Q2) から攻撃の頻度が増加し始め、年末までに計 39件の被害が報告された。これは前年比で 3倍近く増加した数値であり、ランサムウェアグループが日本のマーケットをより積極的に標的にしていることを示唆している。特に、2023年以降に攻撃が急増した背景には、法執行機関の取り締まりを回避しようとするランサムウェアグループの機会主義的戦略が影響を与えているものと分析される。大規模なグループはこの戦略により小規模・分散型の組織運営に移行し、既存のヨーロッパと北米からアジア地域および中小企業まで主要対象として攻撃を拡大する傾向を示した。

2024年には攻撃件数が 45件に達し、前年度よりも増加傾向が続いた。攻撃が特定の時期に集中する傾向がより顕著になり、主要な産業分野を対象とした精密な攻撃が確認された。

2025年の第1四半期 (Q1) には 15件の被害事例が報告され、これは前年度 (6件) の約 150%増加した数値である。現在までの増加傾向を考慮すると、2025年末までに 60件以上のランサムウェア被害が発生すると予測される。

このような傾向を考慮すると、日本企業を対象としたランサムウェア攻撃は一時的な現象ではなく、長期的なセキュリティ脅威として定着していることを示している。特に、攻撃者は制裁を回避しながらも高い経済的利益を狙える企業や組織を集中して狙う傾向を示しており、今後の被害規模はさらに拡大する可能性がある。そのため、日本企業は既存のセキュリティポリシーを再点検し、能動的な脅威検知および対応体系を整備することが必須である。

2) 月別の被害件数

2021年にはランサムウェア攻撃が断続的に発生し、特定の時期に集中するなどの明確なパターンは確認されなかった。2022年には前年比攻撃頻度が増加し、さまざまな時点で攻撃が発生しており、徐々に増加傾向が現れた。

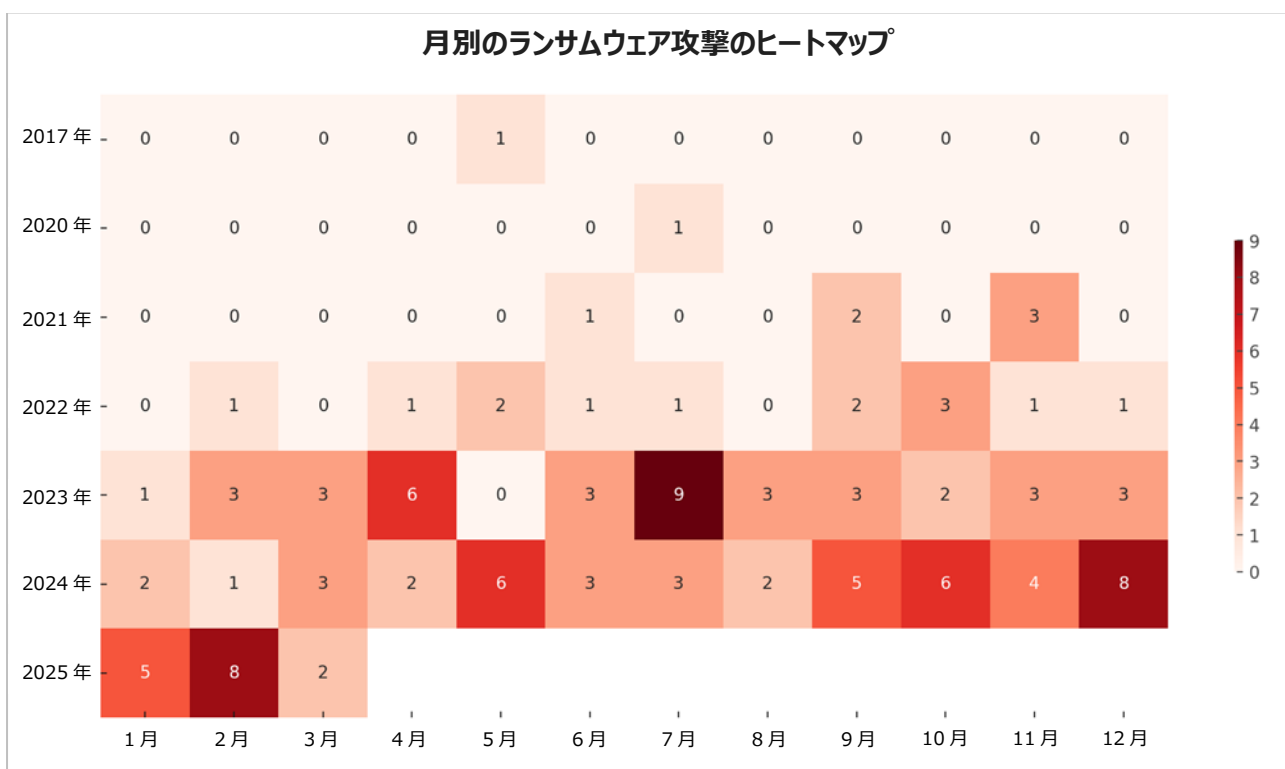
2023年にはランサムウェア攻撃が全体的に増加し、特に 4月と 7月に攻撃頻度が比較的高く現れた。前年度と比べると攻撃件数が大幅に増加したが、特定の産業分野や時期に集中するような一貫したパターンは確認されなかった。

2024年にはランサムウェア攻撃が大幅に増加し、第4四半期 (Q4) に集中して発生する傾向が確認され

た。これは、特定の時期にランサムウェア攻撃が集中する傾向がある可能性を示唆する。企業の決算シーズン、連休期間中のセキュリティ対応の空白、主要な産業分野のビジネス日程などを考慮すると、攻撃者はセキュリティが脆弱になる時点を分析して標的にした可能性が高い。

2025年の第1四半期（Q1）にも前年同期に対して比較的高い攻撃件数が報告されており、これは2024年の第4四半期に集中していた攻撃が新しい年にも続く可能性があることを示している。ランサムウェア攻撃が単発ではなく持続的なキャンペーン形式で行われ、特定の時期に集中して攻撃が発生するパターンが繰り返される可能性がある。ただし、このような現象が一時的な流れなのか、産業別の特性や経済的要因と関連があるかは、さらなる分析が必要だ。

今後、特定の産業分野が年末や特定の四半期ごとにセキュリティリスクが高まる時期があるかを分析し、これに応じた対応戦略を策定することが重要だ。



[図2] 月別のランサムウェア攻撃のヒートマップ

3) 業種別の被害状況

被害を受けた産業分野の中では製造業が全体の攻撃件数の中で最も高い割合（69件）を占め、ランサ

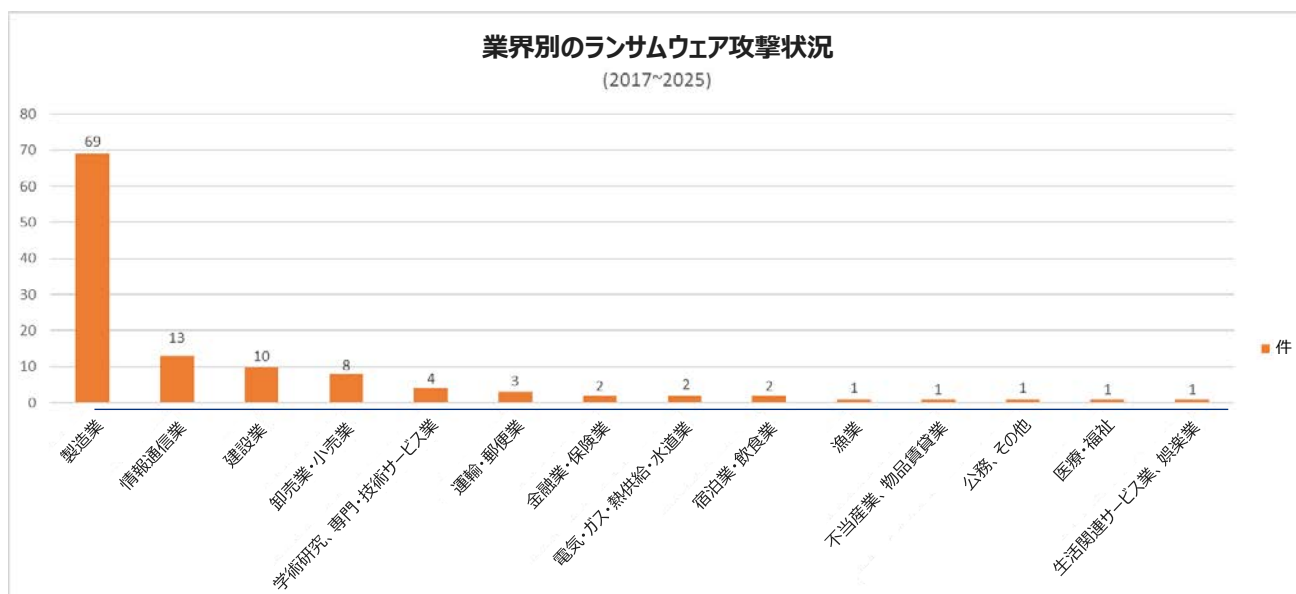
ムウェア攻撃の主要ターゲットとなった。製造産業分野は、大規模生産システムとグローバルサプライチェーンを運営する特性上、運用技術（OT）および情報技術（IT）システムが複雑に絡み合っており、システム障害が発生した場合は生産の遅延による損失が大きいため、攻撃者に優先的に標的にされる可能性が高い。

情報通信業（13件）および卸売業・小売業（8件）も比較的多くの攻撃を受けており、これは大量のデータ、またはサプライチェーンを活用したサプライチェーン攻撃が可能であるためと見られる。

建設業（10件）および専門・技術サービス業（4件）もまた、主要なターゲットに含まれる傾向を示した。これらの産業分野は、プロジェクトベースの業務が多く、契約情報、図面などの重要データが保存されたシステムを運用する特性があるため、ランサムウェア攻撃者の標的になる可能性がある。

宿泊業・飲食業、医療・福祉、運輸・郵便業など、さまざまな産業分野（各 3件以下）も攻撃対象となっており、特定の産業分野だけでなく、全産業分野にわたってセキュリティ強化が必要であることを示唆している。

日本の産業の被害状況は、製造業が主要なターゲットである韓国企業のランサムウェア被害傾向と類似しており、主要な基盤産業が持続的に攻撃対象となっていることを示している。



[図3] 業界別のランサムウェア攻撃状況

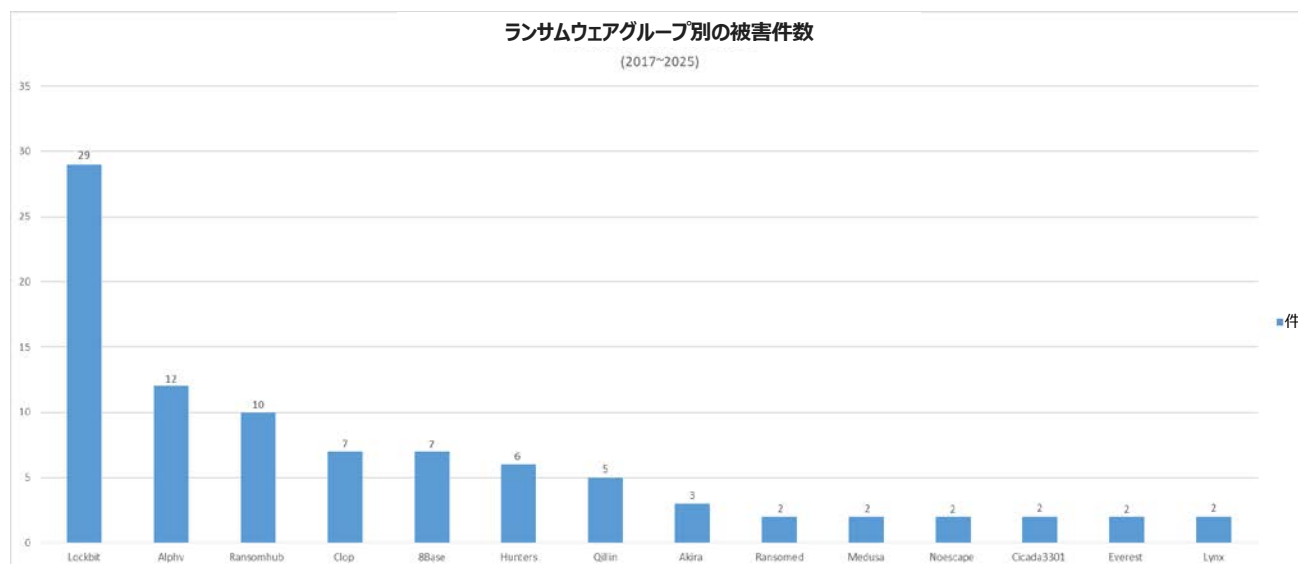
主要なランサムウェア攻撃グループ

2017年から 2025年までの間に日本企業を対象に攻撃したランサムウェアグループのうち、最も活発に攻撃を実行したグループは LockBit (29件)、Alphv (BlackCat) (12件)、RansomHub (10件)、Clon (7件)、8Base (7件) などが確認された。

上位のランサムウェアグループ (LockBit、Alphv、RansomHub、Clon など) は、攻撃全体の多くを占め、攻撃手法を持続的に発展させながらも、既存の Ransomware-as-a-Service (RaaS) モデルを維持しながら活動する特徴が見られる。

特に、2024年以降にランサムウェアグループの再編が行われており、一部のグループの活動が急減または中断され、新しいグループが急速に台頭する現象が確認された。LockBit は 2021年から攻撃を続け最も多くの被害事例を記録しているが、法執行機関の取り締まりがあった 2024年 2月からは活動頻度が急減する流れを見せた。Alphv (BlackCat) と 8Base もまた、DLS の閉鎖と運営中止により活動が中止になった。一方、RansomHub は 2024年 2月以降に登場し、現在までに 10件の攻撃を実行しながら急速に勢力を拡大している。LockBit、Alphv、8Base などの取り締まり後、これらのグループの RaaS 系列会社を使用していた攻撃者たちが RansomHub に大挙移動した状況が確認されており、これによって今後 RansomHub および類似した新しいグループの攻撃が増加する可能性が高い。

ランサムウェアのエコシステムでは既存のグループのコードを活用したり、活動中止後のリブランディング (Rebranding) による新規グループの出現が増加する傾向を示しており、今後は攻撃グループ間の相関分析と継続的な活動監視が必要であると判断される。



[図4] ランサムウェアグループ別の被害件数

ランサムウェア対応戦略

ランサムウェア攻撃が徐々に精巧化し、被害規模が拡大していることに伴い、日本企業はより強力なセキュリティ戦略を確立する必要がある。以下は、最近のランサムウェアの動向と主なセキュリティ推奨事項をもとにまとめた対応戦略である。

1. ダークウェブおよび脅威インテリジェンスモニタリング

- ダークウェブおよびハッキングフォーラムを持続的にモニタリングし、企業関連データの漏洩有無を確認する。
- OSINT (Open Source Intelligence) をベースに、脅威インテリジェンスを取集して予防措置を強化する。
- 攻撃グループの戦術 (TTPs) の変化を追跡して最新の脅威情報とセキュリティポリシーを連携させて、セキュリティレベルを持続的に改善する。

2. 脆弱性管理およびパッチの適用

- 最新のセキュリティパッチを迅速に適用し、既知の脆弱性の悪用を遮断する必要がある。
- 定期的な脆弱性評価とペネトレーションテストを実施し、セキュリティホールを事前に検出して補完する必要がある。

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: ランサムウェアの内部拡散を防ぐために、ネットワークを複数のセキュリティゾーンに分離して管理する。
- アクセス権限の最小化: ユーザーが不要なシステムまたはデータにアクセスできないように、最小権限の原則を適用する。
- ログおよび振る舞いベースのモニタリング: エンドポイントとネットワークで疑わしい活動 (例: 大量のファイル暗号化、異常なホスト間の通信) を検知し、迅速に対応できるようにする。

4. データのバックアップおよび復旧計画の策定

- 3-2-1 バックアップ戦略を遵守し、データの 3つのコピーを 2種類のストレージに保管し、1つはオフライン状態 (またはクラウドに保存) で維持する。
- バックアップデータの整合性を定期的に検証し、実戦対応のための復旧訓練を実施する。

5. 攻撃の検知と対応の自動化

- 侵入検知・遮断システム (IDS・IPS) と、エンドポイント検知・対応 (EDR) ソリューションを活用し、リアルタイムで攻撃を検知して遮断する。
- ランサムウェア感染が疑われる場合、すぐに隔離措置を講じて被害の拡散を防ぐ。

6. 情報セキュリティ教育および内部プロセスの強化

- フィッシング対応教育: ランサムウェアの主な流入経路であるフィッシング攻撃を防ぐために、定期的な教育と模擬訓練を行う。
- 社内セキュリティポリシーの改善: 重要なデータへのアクセス手順を強化し、多要素認証 (MFA) を導入して不正アクセスを遮断する。

7. Ransomware-as-a-Service (RaaS) に対応

- LockBit、Alphv (BlackCat)、8Base などの主要なランサムウェアグループが壊滅していく中、これらの RaaS 系列会社が RansomHub に移動している。これにより、今後 RansomHub のような新規ランサムウェアグループの攻撃頻度が増加する可能性が高く、日本の企業は新たな脅威グループの動向を綿密にモニタリングする必要がある。

ランサムウェア攻撃は、技術的防御だけでは完全に遮断できない脅威であり、企業は全体的なセキュリティポリシーを見直し、多層防御戦略を確立して対応能力を強化する必要がある。これにより、ランサムウェアの脅威を効果的に緩和し、長期的なセキュリティシステムを構築することができるだろう。

More security, More freedom

株式会社アンラボ (AhnLab, Inc.)

〒108-0014 東京都港区芝 4丁目 13-2田町フロントビル 3階

Tel: 03-6453-8315 (代) | Fax: 03-6453-8316

www.ahnlab.com/jp

この報告書は著作権法によって保護される著作物であり、営利目的の無断転載と無断複製を禁じます。

この報告書の内容を全部または一部の引用、加工する際は、アンラボが刊行した報告書であることを明らかにしてください。

* この報告書に収録されている内容または配布に関するすべての問い合わせは、
アンラボ (031-722-8000) までお願いいたします。

この報告書は <https://atip.ahnlab.com> を通して利用できます。

© 2025 AhnLab, Inc. All rights reserved.