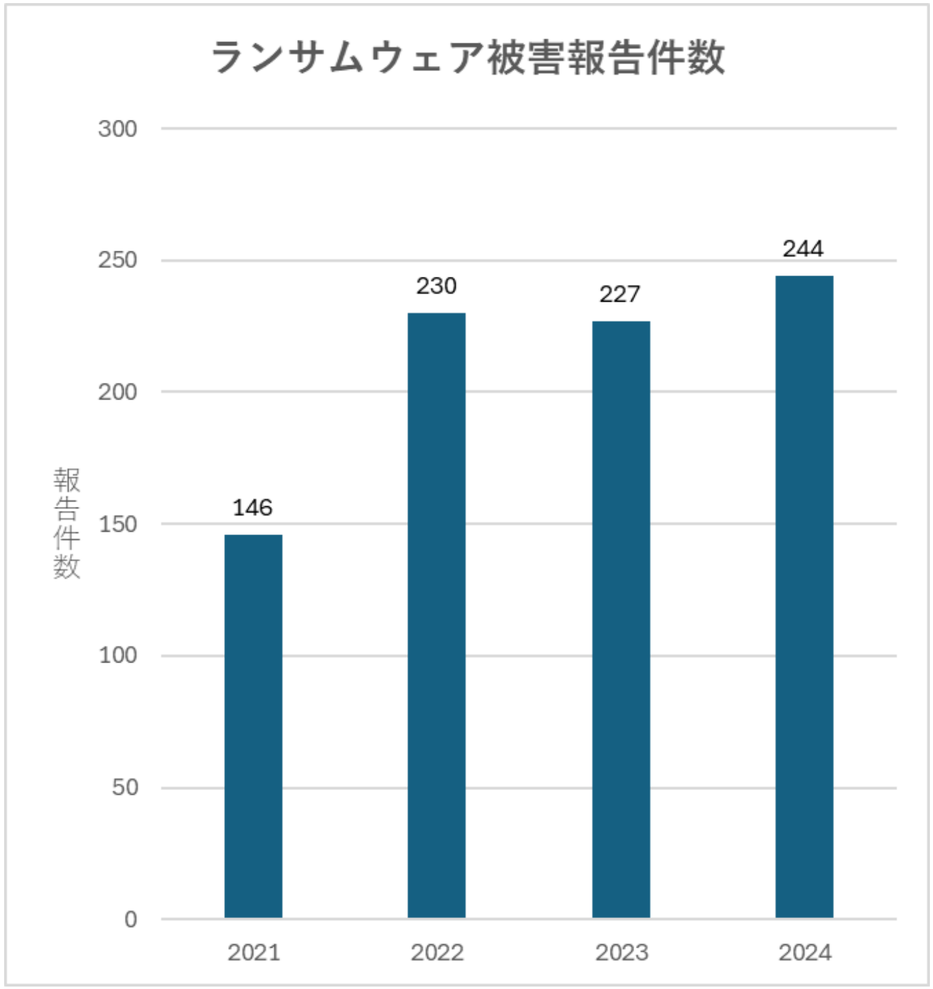
ランサムウェア攻撃の被害事例と求められる対策

2026年4月20日
インフォテック株式会社

本資料は、2026年2月時点での情報をもとに作成をしております。

近年におけるランサムウェア被害



- ランサムウェア攻撃による被害は、現在においても情報セキュリティ上の最も重大な脅威の一つであり、IPAが公表した「情報セキュリティ10大脅威［組織編］(2026年)」でも1位に位置付けられています。(1)
- 2022年以降、ランサムウェア被害の報告件数は、1年あたり200件を超える高い水準で推移していることが、左の表からわかります。(2)
- 本資料では、実際の被害事例を紹介しつつ、日本国内におけるランサムウェア被害の現状と、組織として求められる対策について整理します。

ランサムウェア攻撃の被害事例

- 2024年にA社が運営する複数のサービスが停止する事態が発生しました。
- 後にランサムウェアを含む大規模なサイバー攻撃を受けていたことが判明しました。
- 最長2か月にわたる動画配信サービス・受注システムなどの停止や、約25万人分の個人情報や企業情報の漏えいといった被害が確認されています。(3)
- 攻撃者は、フィッシングにより従業員アカウント情報を窃取し、窃取されたアカウントにを利用して社内ネットワークに侵入したものと考えられています。

ランサムウェア攻撃の被害事例

- サイバー攻撃の影響によって、A社には以下の金銭的な影響が生じました。

業績への影響	金額（通期見通し）
売上高の減少	84億円
営業利益の減益	64億円
特別損失	36億円

- 身代金の支払いについては公式な発表はされていません。

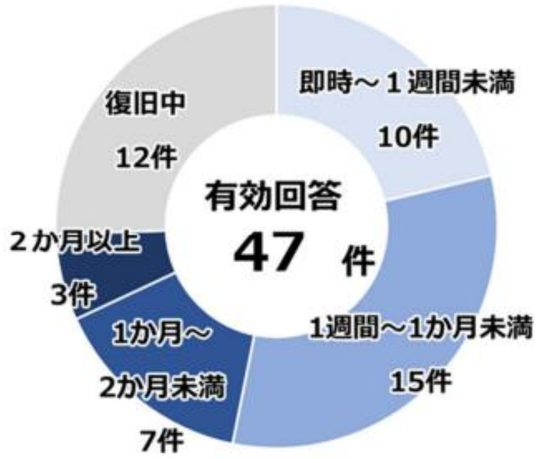
日本国内におけるランサムウェア被害の現状

日本国内におけるランサムウェア被害の現状について、以下の4つの観点から説明します。

- 調査・復旧にかかる期間と費用
- 感染経路
- 身代金の支払い
- 求められる対策

調査・復旧にかかる期間と費用

期間



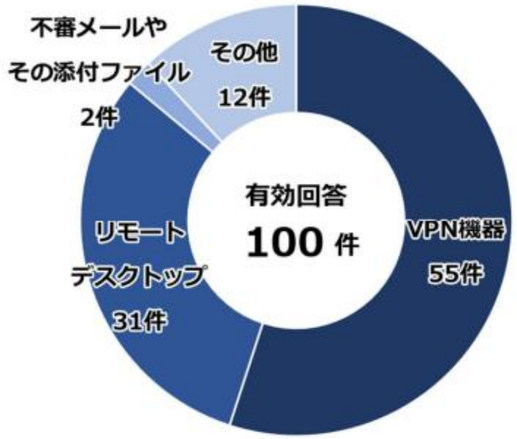
復旧まで1週間以上を要する組織が半数以上です。(2)

費用

復旧に1,000万円以上を要する組織が約60%です。(2)

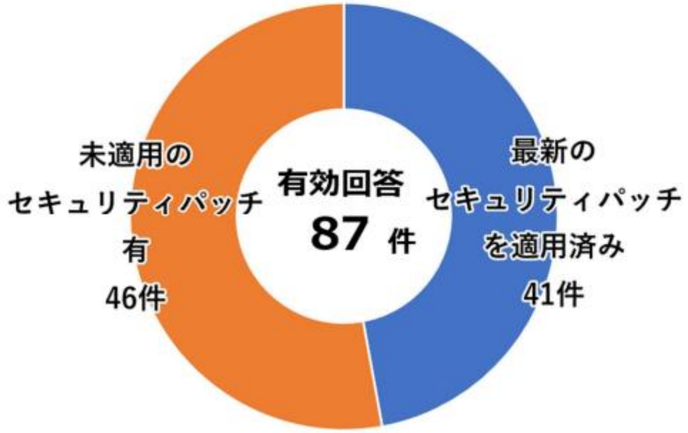
感染経路

感染経路



VPN機器とリモートデスクトップからの侵入が80%以上を占めます。(2)

侵入経路とされる機器のセキュリティパッチの適用状況



侵入経路の機器の半数以上が、最新のセキュリティパッチを適用していませんでした。(2)

身代金の支払い

- 原則として、身代金の支払いは復旧の手段にはなりません。
  - 1回目の支払い後に復旧できた割合は17%しかありません。(4)
  - 追加の支払いを含めた場合も、復旧率は67%にとどまります。(4)
  - 支払いを行ったという情報が広まると、他の攻撃グループから更なる攻撃を受ける可能性が増えます。
  - 国からの制裁金を科される場合もあります。
- 身代金の支払いは犯罪組織への資金提供とみなされ制裁を受ける可能性があります。
  - ただし、身代金の支払いを直接禁じる法律はありません。(5)（2026年2月現在）
- 2023年の日本の身代金の支払い率は32%と、国際平均の54%より低い数値です。(4)

求められる対策

- ランサムウェア攻撃は、複数の手段を用いて組織への侵入を行い、内部で暗号化に向けた準備を行う攻撃のため、単一の対策では不十分です。
- そのため、複数の対策を絡めた**多層防御**を構築することが求められます。
- 特にVPN機器やリモートデスクトップが侵入経路として悪用されることが多いため、それらの機器への**最新のセキュリティパッチの適用**を最優先で行うことを推奨します。
- 侵入後の内部での不審な動きを検知するため、EDRやNDR等の不審なふるまいを検知する仕組みの導入も効果的です。

セキュリティは後付けでは守れない

セキュリティ対策は、システム開発の設計段階から対策することが重要です。

インフォテックが提供するセキュリティソリューションは
Security By Design x DevSecOpsをベースに構築、確かな安心をお届けします。

Security By Design

システム設計段階からセキュリティを組み込んで開発を行います

CIS Benchmarks® (*1)やCIS Controls® (*2)を活用し、設計・開発・保守におけるセキュリティの標準化と継続的な評価改善を可能とします

DevSecOps

保守フェーズではDevSecOpsに基づき、PDCAサイクルにWebアプリケーション脆弱性診断(*3)やクラウド／SaaSのセキュリティ態勢管理（CSPM(*4)・SSPM(*5)）を組み込むことで、運用の継続的な改善をご支援します

お問い合わせ・資料請求はこちらから

インフォテック株式会社HP 問い合わせ窓口
https://www.iftc.co.jp/contact/form/?kind=2

お電話でのお問い合わせ
03-3348-0360　※【受付時間】土日祝日を除く平日の9:00～17:30

(*1) OSやクラウドなどのITシステムに対する安全な設定方法をまとめたガイドラインで、セキュリティ強化や監査対応に活用
(*2) サイバー攻撃から組織を守るための18の優先度付きセキュリティ対策で、実践的かつ段階的な導入が可能なベストプラクティス集
(*3) スリーシェイク社の「Securify」を用いた自動診断
(*4) クラウド環境の設定ミスや脆弱性を検出・修正し、セキュリティとコンプライアンスを維持する管理ツール
(*5) SaaSアプリのセキュリティ設定を監視・管理し、データ漏洩や権限の過剰付与などのリスクを防ぐための管理ツール

参考文献

(1) 独立行政法人情報処理推進機構（IPA）．「 情報セキュリティ10大脅威」．
https://www.ipa.go.jp/security/10threats/index.html, (2026/2/9).

(2) JCIC.「サイバーリスクの数値化モデル」.
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/003_04_00.pdf, (2026/2/9).

(3) piyolog. 「 KADOKAWAグループへのサイバー攻撃や悪質な情報拡散についてまとめてみた」．
https://piyolog.hatenadiary.jp/entry/2024/08/19/074417, (2026/2/9).

(4) Proofpoint. 「身代金支払率15か国調査 2024」. https://www.proofpoint.com/jp/blog/threat-insight/japan-ransomware-payment-result-2024, (2026/2/9).

(5) 東洋経済. 「知っておきたいランサムウェア「身代金」の法規制」. https://toyokeizai.net/articles/-/794272, (2026/2/9).