2026

ランサムウェア攻撃に関する意識と実態調査

システム担当者・経営層の視点

Arcserve Japan

arcserve®

ランサムウェア攻撃に関する意識と実態調査：システム担当者・経営層の視点

本レポートは、企業のシステム部門関係者および経営層500名を対象に実施された、ランサムウェア攻撃に関するオンラインサーベイの結果をまとめたものです。昨今のサイバー脅威に対する専門家や意思決定者のリアルな不安、実際の被害状況、そして今後の対策強化の方向性を客観的な立場から分析します。

内容

ランサムウェア攻撃に関する意識と実態調査：システム担当者・経営層の視点 1

1. ランサムウェア攻撃に対する不安と経験 3

攻撃に対する不安度 3

実際の被害経験 4

2. 被害実態：暗号化と復旧のハードル 5

バックアップデータの暗号化 5

復旧時間とコスト 6

3. 現在のIT環境とバックアップ体制 8

ITインフラと保存先 8

運用の頻度とテスト 8

4. 懸念事項と今後の対策強化 10

懸念されるポイント（複数回答） 10

現在の課題と「イミュータブル」への期待 10

今後の投資意向（強化したいポイント） 12

5. 結論 13

【調査概要】

調査名称：ランサムウェア攻撃に関する意識と実態調査

調査目的：企業におけるランサムウェア対策の実態と課題を把握する

調査対象：全国の企業に勤務する情報システム担当者および経営層

調査対象属性：従業員規模：

100名未満 35%、100-299名 15%、300-999名 14%、1000-4999名 13%、5000名以上 15%、他 8%

調査方法：インターネットリサーチ（オンラインサーベイ）

調査期間：2025年12月

サンプリング方法：事前登録モニターを対象、調査対象に絞ったモニターを抽出

有効回答数：500名

回答者属性（主な内訳）

業種構成：製造業 22%、情報通信業 17%、サービス業 13% など

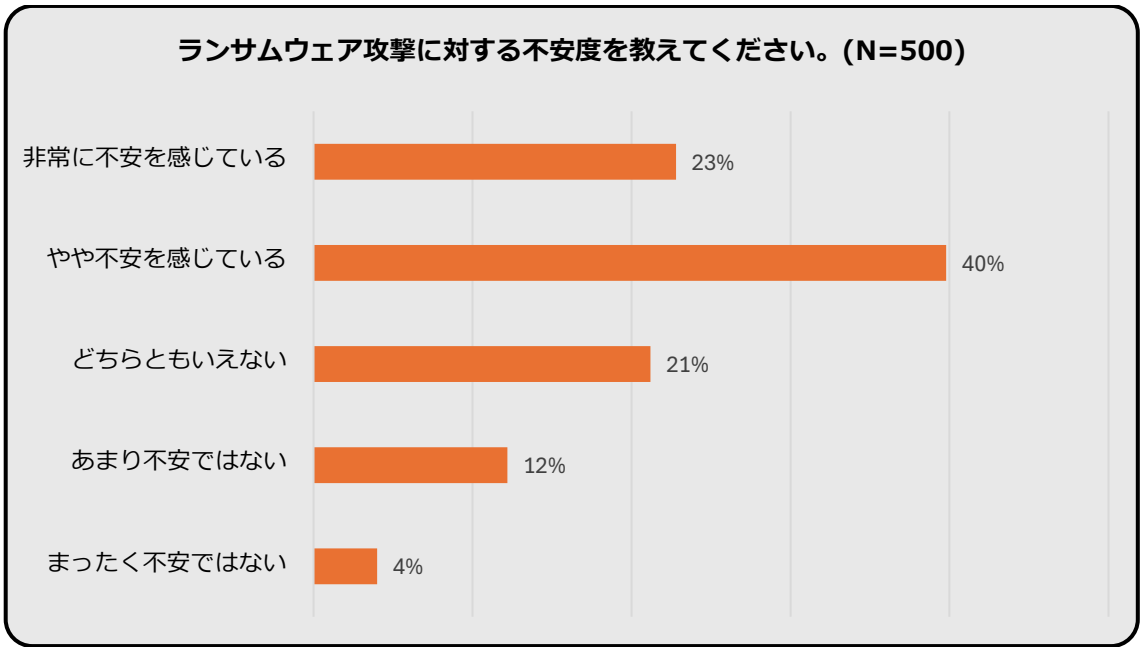
地域構成：全国（東京都 28%、神奈川県 10%、埼玉 7%、千葉 7%、大阪府 7%、愛知県 5% など）

1. ランサムウェア攻撃に対する不安と経験

システム担当者や経営層の多くが、ランサムウェアの脅威を身近なリスクとして捉えています。

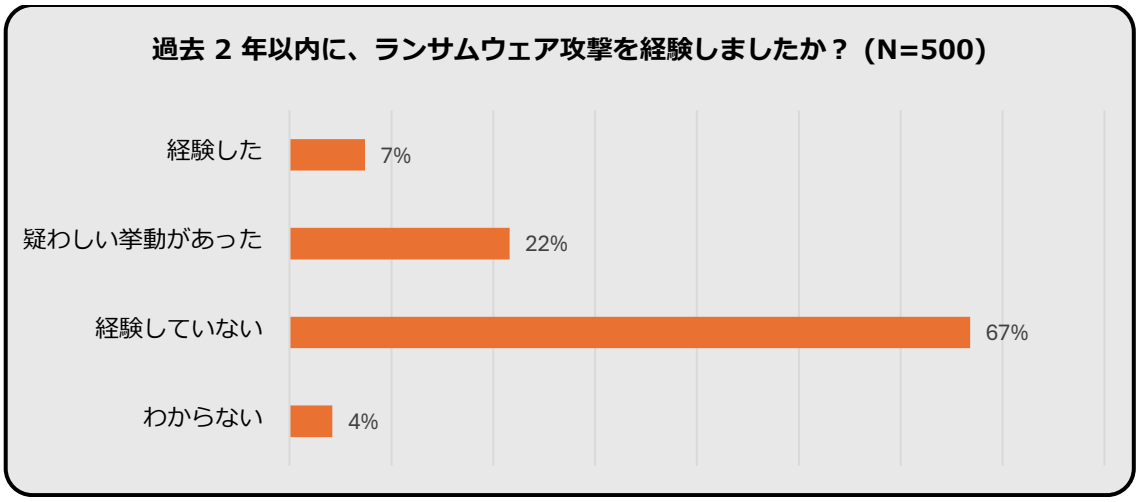
攻撃に対する不安度

アンケートによると、回答者の **63%（「やや不安を感じている」40%＋「非常に不安を感じている」23%）**が攻撃に対して不安を抱いています。「まったく不安ではない」と回答した割合はわずか4%に留まり、組織のリーダー層において危機意識が定着していることが分かります。



実際の被害経験

過去2年以内の被害状況については、以下の通りです。



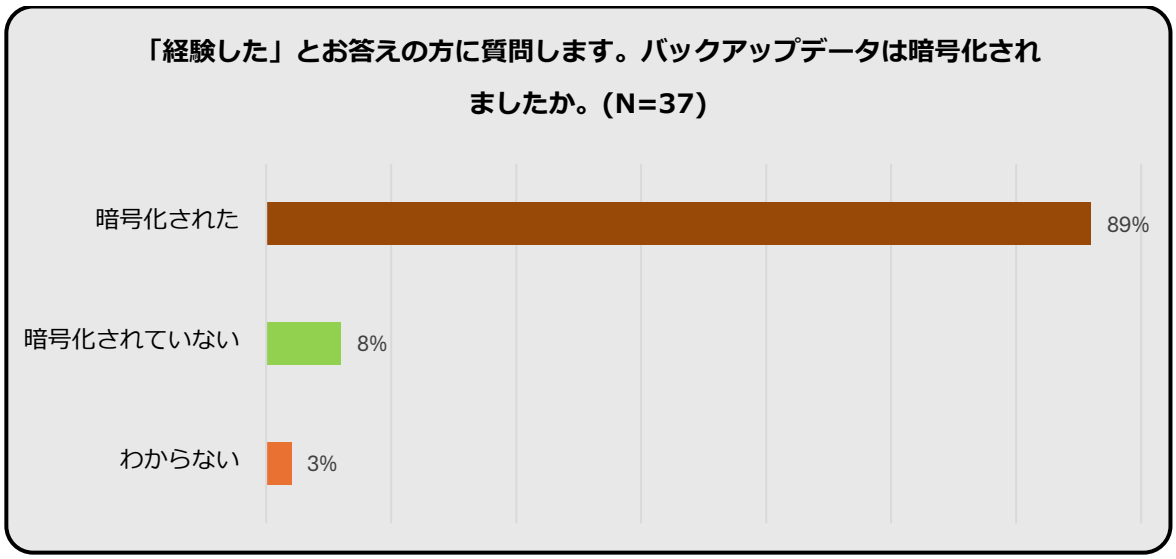
「経験した」および「疑わしい挙動があった」を合わせると、 **約30%** の組織が何らかの影響を受けている可能性があり、攻撃が決して他人事ではない実態が浮き彫りになっています。

2. 被害実態：暗号化と復旧のハードル

実際に被害に遭った組織の回答からは、攻撃の深刻さと復旧における課題が見て取れます。

バックアップデータの暗号化

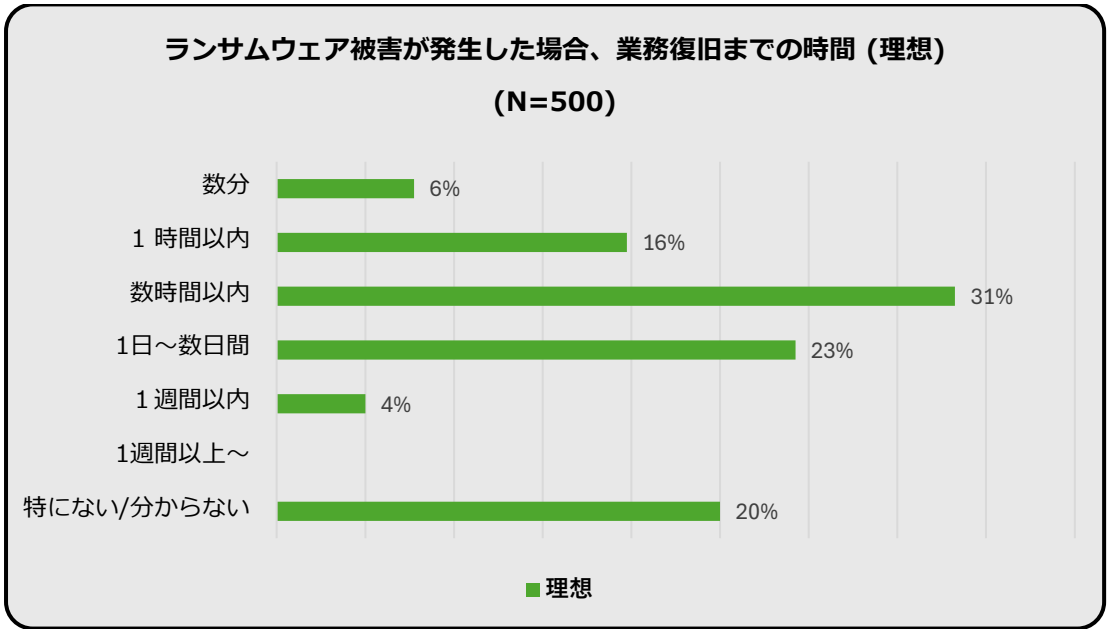
被害経験者のうち、89%という極めて高い割合で「バックアップデータまで暗号化された」と回答しています。これは、単にデータを保存するだけでは不十分であり、攻撃者がバックアップを優先的に狙う傾向を裏付けています。



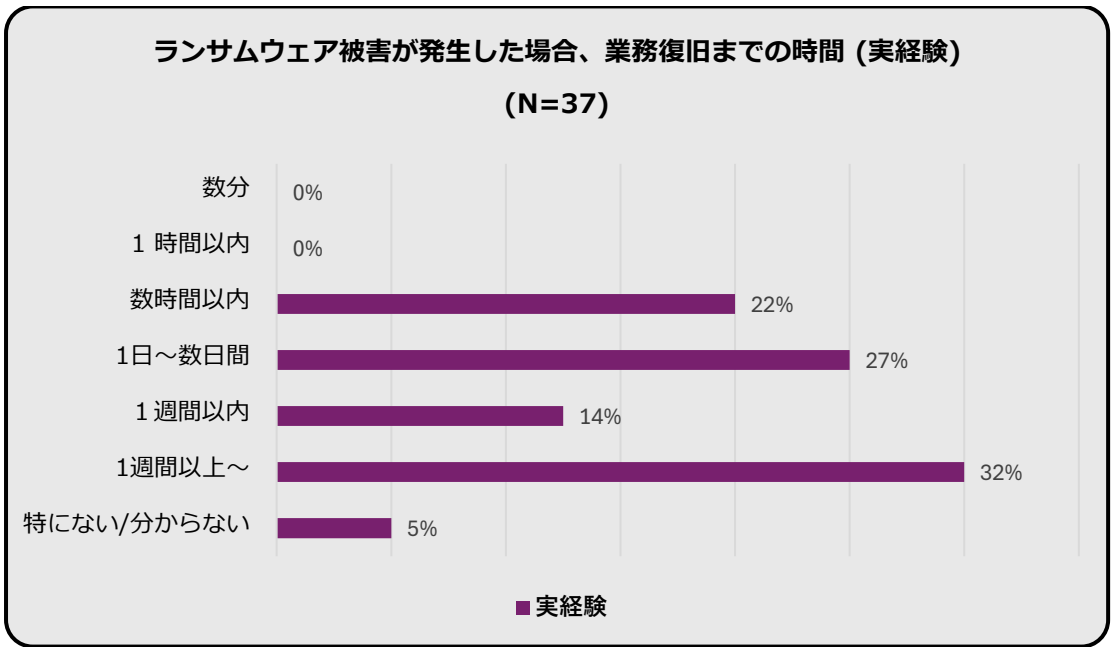
復旧時間とコスト

復旧にかかる時間と費用は、組織によって大きな幅があります。

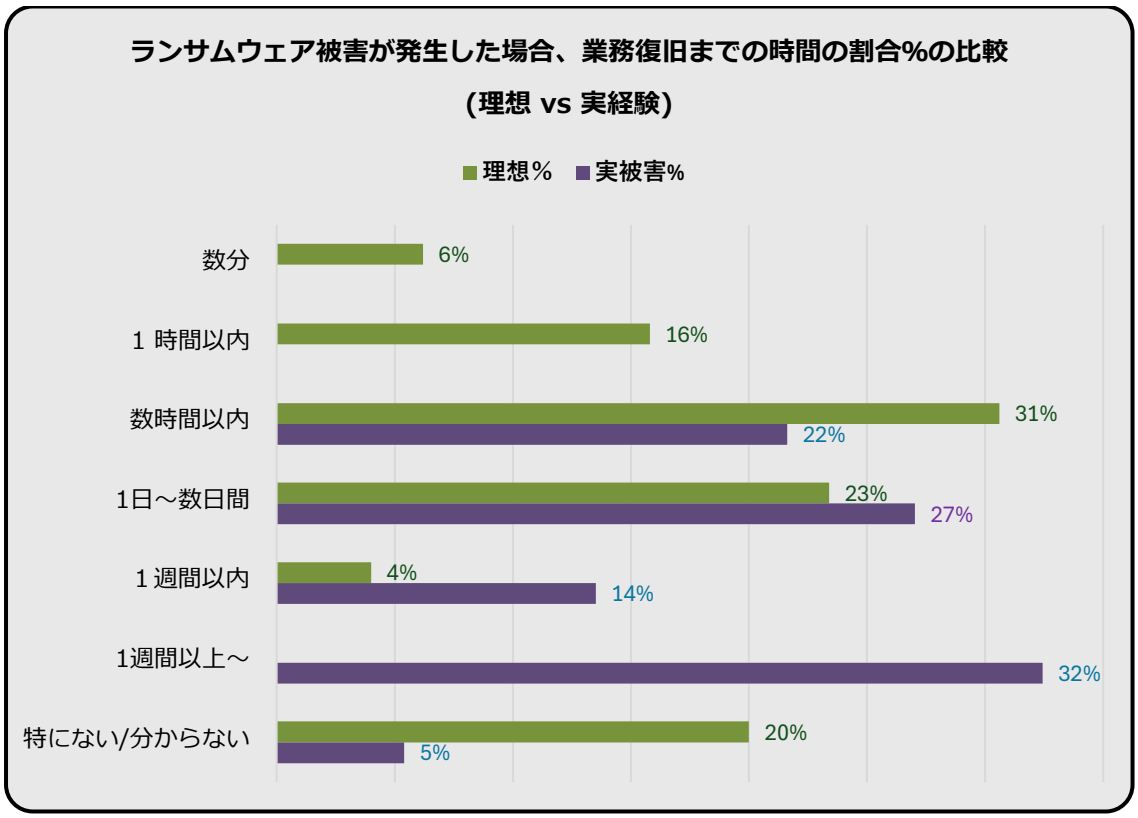
- **理想的な復旧時間:** 理想とする復旧時間は「数分」「１時間以内」「数時間以内」で53%と大半の企業は迅速な業務復旧を理想としています。



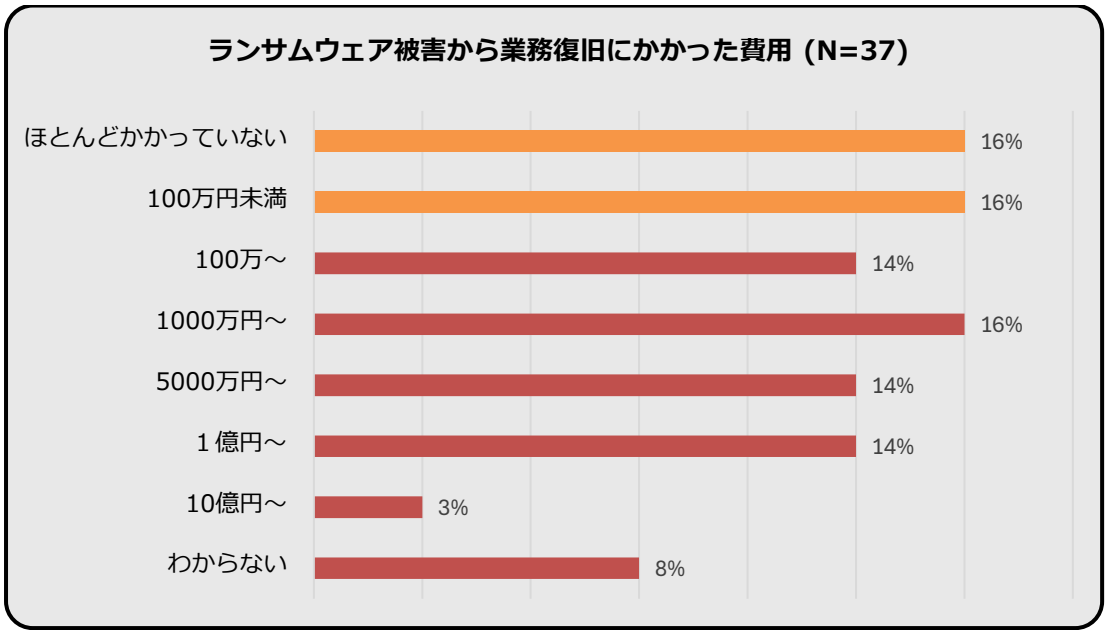
- **実際の復旧時間:** 一方で、実際に被害を受けた際にかかった時間では、「1週間以上～1カ月未満」が30%で最多となっており、ビジネスへの影響が長期化するリスクがあります。



復旧時間の理想と実際の割合 (%) 比較



- **復旧費用:** 100万円未満から10億円以上まで分散していますが、 **約60%** の組織が100万円以上の費用を要しており、中には数千万円から数億円規模の莫大なコストを支払ったケースも確認されました。

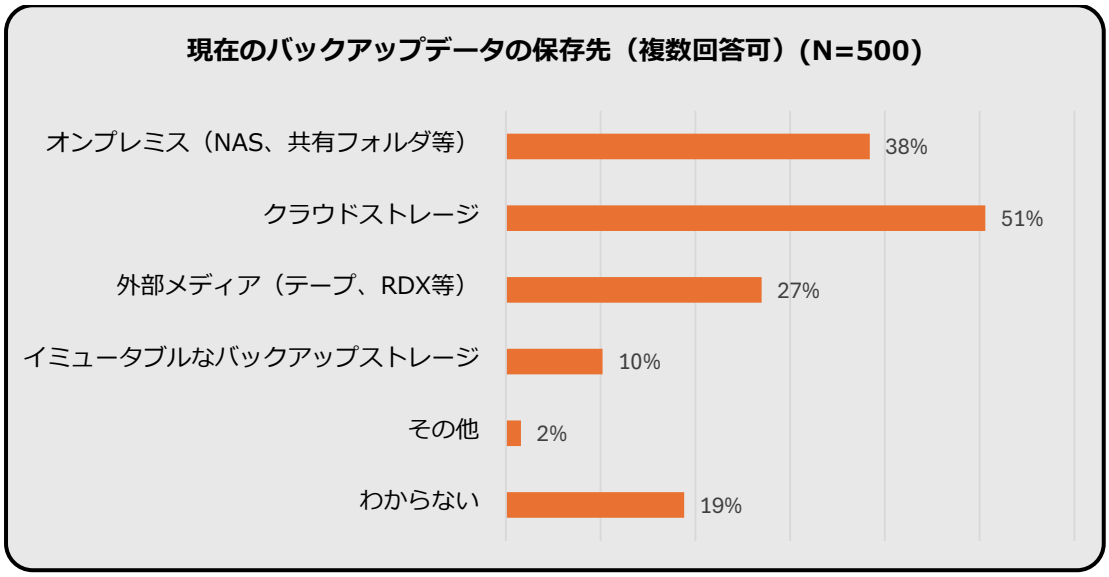


3. 現在のIT環境とバックアップ体制

組織のITインフラが多様化する中で、バックアップの運用状況も変化しています。

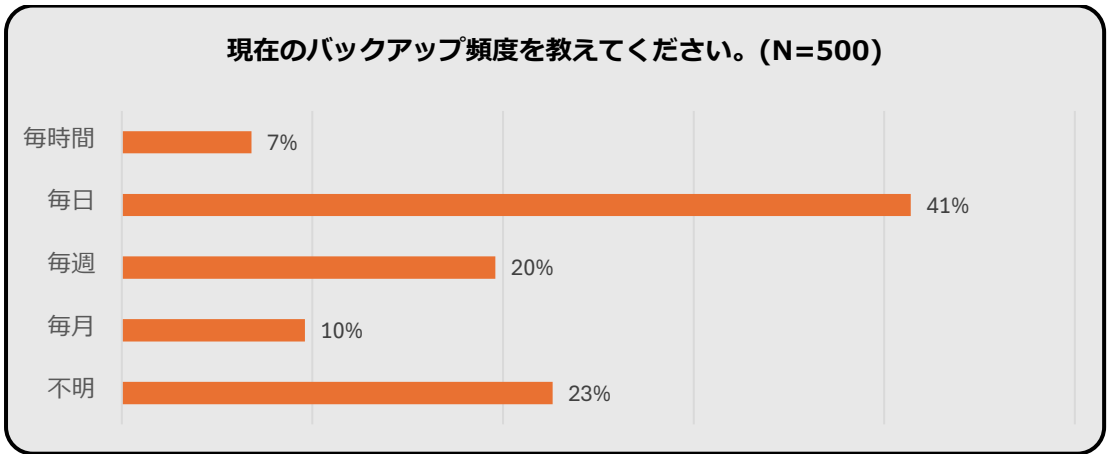
ITインフラと保存先

現在のインフラ環境は「クラウド中心」が37% **で最も多く、バックアップの保存先も「クラウドストレージ」が** 51% **と過半数を超えています。一方で、外部メディア（テープ等）を利用する組織も** 27%存在し、多様な手段が併用されています。

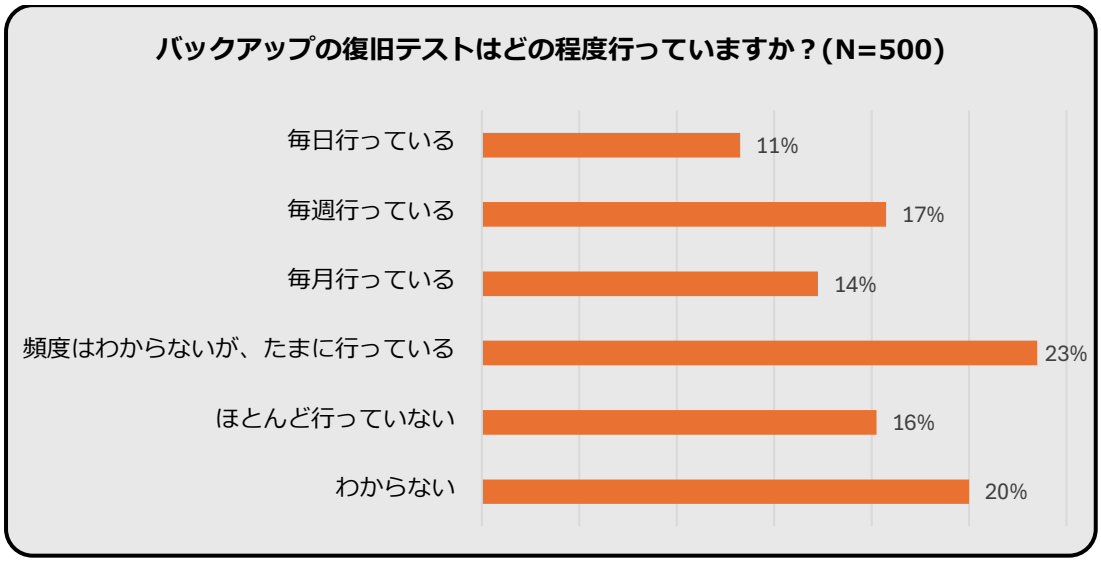


運用の頻度とテスト

- **バックアップ頻度:** 「毎日」行っている組織が41%で最多です。



- **復旧テスト:** 毎日・毎週・毎月と定期的に実施している組織がある一方で、「頻度はわからないがたまに行っている」が **23%** 、「ほとんど行っていない」が16%存在します。有事の際に確実に復旧できる体制の確保が、今後の課題と言えるでしょう。

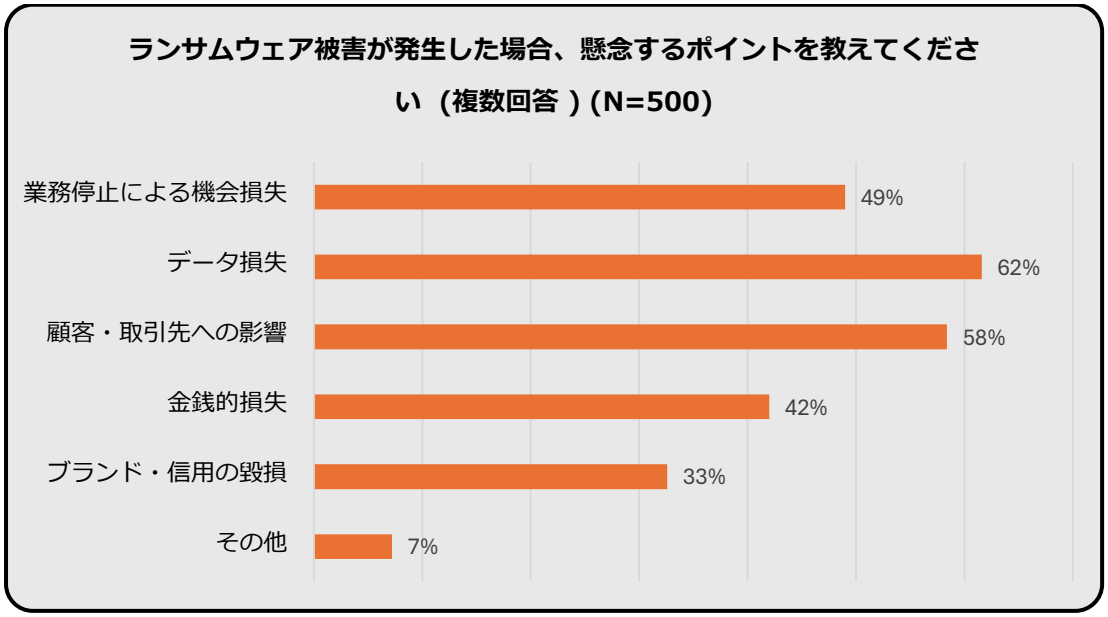


4. 懸念事項と今後の対策強化

組織がどのようなリスクを懸念し、どのような対策を求めているのかを分析します。

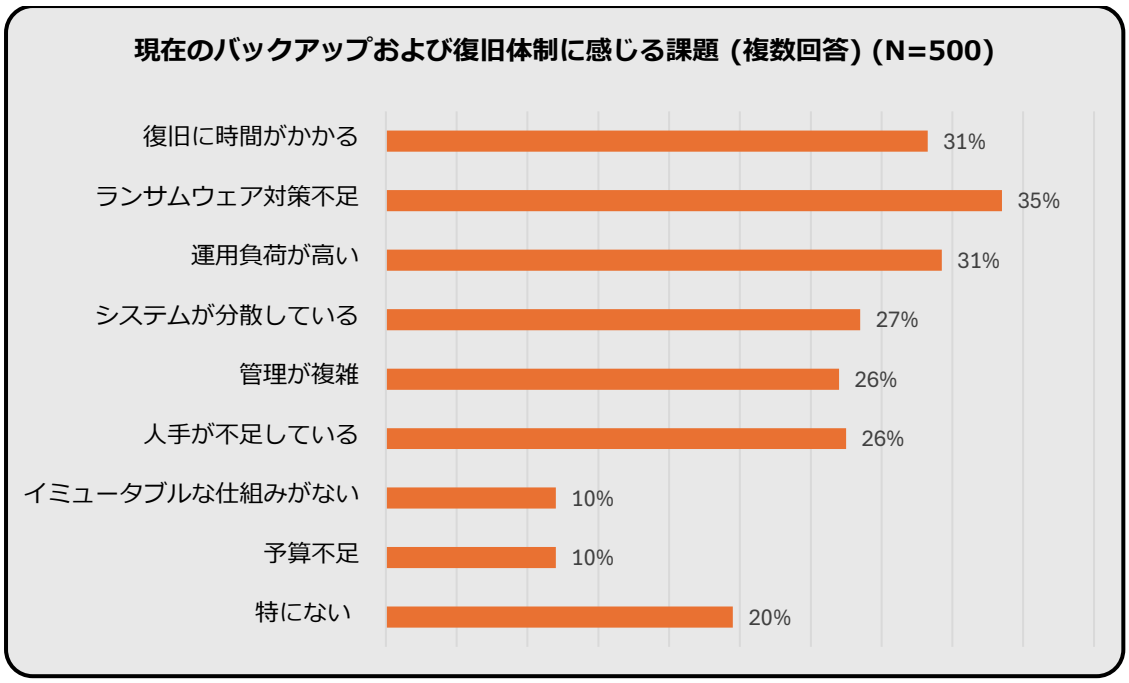
懸念されるポイント（複数回答）

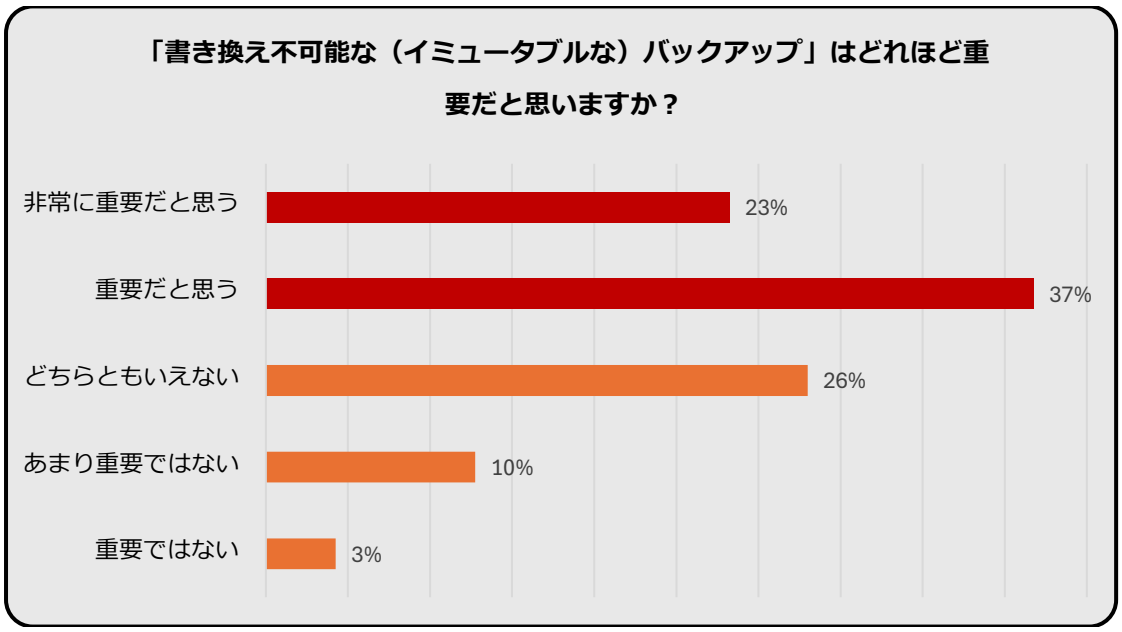
1. **データ損失 (62%)**
2. **顧客・取引先への影響 (58%)**
3. **業務停止による機会損失 (49%)**
4. **金銭的損失 (42%)**



現在の課題と「イミュータブル」への期待

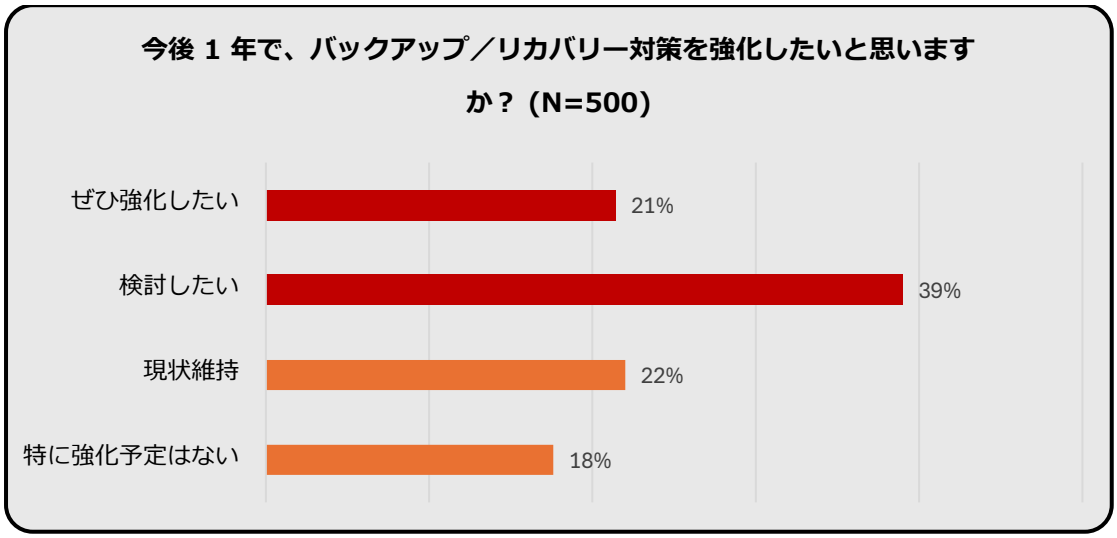
現状の体制に対し、35% **の回答者が「ランサムウェア対策不足」を課題に挙げています。また、攻撃者がデータを書き換えられないようにする** 「イミュータブル（書き換え不可能）なバックアップ」 **については、全体の** 60%が「重要だと思う（37%）」「非常に重要だと思う（23%）」と回答しており、その有効性に高い期待が寄せられています。



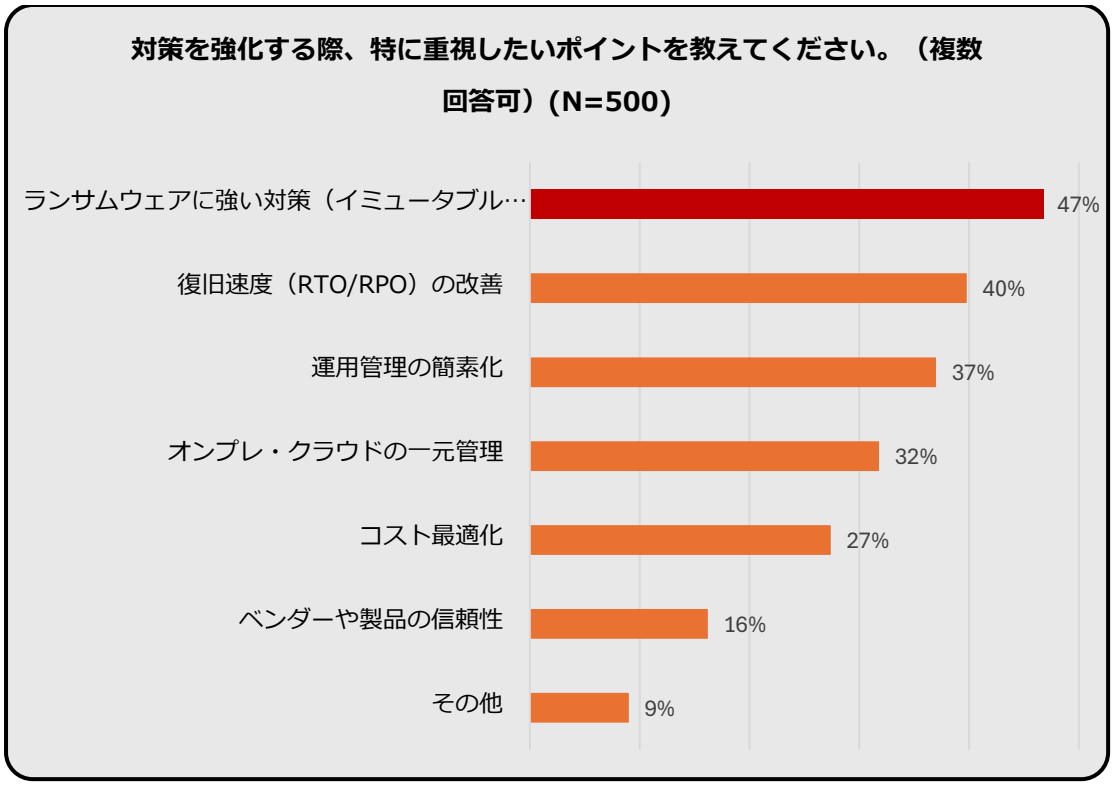


今後の投資意向（強化したいポイント）

今後1年で対策を「強化したい・検討したい」と考える組織は60%に達します。



強化の際に重視されるポイントは以下の通りです。



5. 結論

本調査の結果から、システム担当者や経営層はランサムウェア攻撃を重大な脅威と認識しており、特に「バックアップデータの暗号化」への対策を急務と考えていることが分かりました。

今後の対策においては、単なるデータの保存に留まらず、**「復旧速度の向上」** **「イミュータブル（書き換え不可能）な仕組みの導入」**、そして複雑化する環境における「管理の簡素化」が、組織を守るための鍵となります。ベンダー各社には、これらの高度なニーズに応える信頼性の高いソリューションの提供が期待されています。

arcserve Japan合同会社
東京都千代田区神田神保町1-105
神保町三井ビルディング
Tel: 03-4520-0600