SOPHOS

日本のランサムウェアの現状 2025 年版

過去 1 年間にランサムウェア攻撃を受けた日本の 207 の組織を対象とした、ベンダー中立の独立調査の結果。

ソフォスホワイトペーパー 2025 年 6 月

レポートの概要

本レポートは、過去 1 年間にランサムウェア攻撃を受けた組織に所属する 3,400 人の IT/ サイバーセキュリティリーダー (うち 207 人は日本からの回答者) を対象とした、ベンダー中立の独立調査の結果に基づいています。

この調査は、ソフォスの委託を受けて第三者専門機関が 2025 年 1 月から 3 月にかけて実施しました。

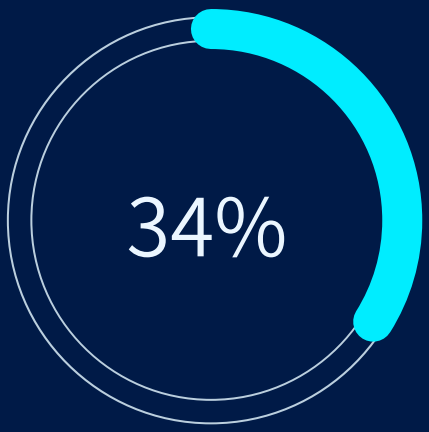
回答者はすべて、従業員数 100 人から 5,000 人の組織に所属しており、過去 12 か月間の経験に基づいて回答しています。

本レポートには、2024 年の調査結果との比較も含まれています。財務データはすべて米ドルで表示されています。

回答者数

207

過去 1 年間にランサムウェア攻撃を受けた組織に勤務する IT/ サイバーセキュリティリーダー



データが暗号化された攻撃の割合

過去 1 年間に日本で支払われた身代金の中央値

ランサムウェア攻撃から復旧するための平均コスト

日本の組織がランサムウェアの被害に遭う理由

- **攻撃の技術的な根本原因で最も多かったのは、脆弱性の悪用と認証情報の漏洩**で、いずれも日本の回答者の 26% が挙げました。続いてフィッシング攻撃が 22% でした。
- **運用面での最も一般的な根本原因は、専門知識の不足**で、日本の回答者の 50% が挙げました。次いで、45% の組織が保護レベルの低さを挙げました。保護レベルの低さがランサムウェアの被害に遭った要因の一つだと回答したのは、44% でした。

データへの影響

- **攻撃を受けた日本の回答者のうち 34% がデータを暗号化されたと回答しました。**この割合は、世界平均の 50% を大幅に下回るだけでなく、2024 年の調査で日本回答者により報告された 76% より低い数値となっています。
- **データが暗号化された攻撃の 21% でデータも窃取されており**、この数値は昨年の 26% を下回っています。
- **データが暗号化された日本の組織の 97% はデータを復元することができました。** この数値は、世界平均と同じです。
- **日本の組織の 70% が身代金を支払ってデータを取り戻しました。**この数値は昨年の 60% から増加しています。
- **日本の組織の 59% がバックアップを使用して暗号化されたデータを復元しました。**この数値は昨年の 68% から減少しています。

身代金：要求額と支払額

- **過去 1 年間における日本の身代金要求額の中央値は 100 万ドル**で、2024 年の調査で報告された 85,200 ドルから大幅な増加となりました。

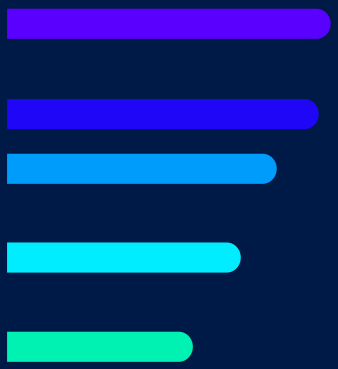
日本で要求された
身代金の中央値

- **身代金要求の 53% が 100 万ドル以上でした。**
- **過去 1 年間に日本で支払われた身代金の中央値は 50 万ドル**で、昨年報告された 99,400 ドルから大幅な増加となりました。
- **日本の組織は通常、身代金要求額の 68% を支払っており**、この数値は世界平均の 85% を下回っています。
  - 67% が**最初の身代金要求額より少ない金額を支払いました** (世界平均：53%)。
  - 25% が**最初の身代金要求額と同額を支払いました** (世界平均：29%)。
  - 8% が**最初の身代金要求額より多い金額を支払いました** (世界平均：18%)。

ランサムウェアによるビジネスへの影響

- 身代金の支払いを除外すると、**過去 1 年間に日本の組織がランサムウェア攻撃からの復旧に要した平均 (中央値) コストはわずか 67 万ドル**で、2024 年に日本の回答者が報告した 293 万ドルから大幅に減少しました。これらのコストには、ダウンタイムコスト、従業員の作業時間、デバイスのコスト、ネットワークのコスト、機会損失などが含まれます。
- **日本の組織のランサムウェア攻撃からの復旧速度は向上しており**、50% が 1 週間以内に完全復旧を達成しています。この割合は昨年の 27% から増加しています。復旧に 1 か月から 6 か月を要した企業はわずか 16% で、昨年の 36% から減少しています。

データが暗号化された組織における IT/ サイバーセキュリティチームに及ぼしたランサムウェアの人的影響



54% が、攻撃を阻止できなかったことへの**罪悪感**を報告しています。

52% が、**チームの優先事項や注力領域の変化**を報告しています。

45% が、経営層からの**プレッシャーが増大** したと報告しています。

39% が、今後の攻撃に対する**不安やストレスの増加**を報告しています。

31% が、**業務量の継続的な増加**を報告しています。

ソフォスの提言

ランサムウェアは、日本の組織にとって依然として大きな脅威です。サイバー攻撃が繰り返され、進化し続ける中で、防御側の組織は自社のサイバー攻撃対策を攻撃の進化に合わせていかなければなりません。本レポートは、2025 年以降重点的に取り組むべき領域を示しています。

- **予防。**ランサムウェア攻撃を受けても、侵入することができず被害が全く発生しなかったということが、企業や組織にとって最も良い結果です。本レポートが指摘している技術的な根本原因と運用面の根本原因の両方を解決するよう努めてください。
- **保護。**基盤となるセキュリティ機能を強化することは必須です。エンドポイントやサーバーは、ランサムウェアの主要な攻撃対象であるため、専用のランサムウェア対策機能を搭載しているエンドポイント保護製品を導入して、悪意のある暗号化を阻止してロールバックできるようエンドポイントの防御を徹底する必要があります。
- **検知と対応。**攻撃をできる限り早期に阻止できれば、影響も軽減することができます。24 時間体制の脅威検出と対応は、今や不可欠な防御層となっています。社内のリソースやスキルが不足している場合は、信頼できる MDR プロバイダーと連携することを検討してください。
- **計画と準備。**インシデント対応計画を策定し、計画をテストしておけば、最悪の事態が発生し、大規模な攻撃を受けた場合でも、攻撃の影響を最小限に抑えることができます。必ず適切なバックアップを取り、バックアップを使用して復旧するテストを定期的に実施してください。

SOPHOS

ソフォスを活用してランサムウェア対策の最適化する方法については、ソフォスのアドバイザーにご相談いただくか、**sophos.com/ransomware2025** をご覧ください。

ソフォスは、業界をリードするサイバーセキュリティソリューションをあらゆる規模の企業に提供し、マルウェア、ランサムウェア、フィッシングなどの高度な脅威をリアルタイムで保護します。実績のある次世代機能により、AI と機械学習を駆使した製品でビジネスデータを効率的に保護できます。

2025-07-11 JA-WP (DD)