SOPHOS

日本におけるランサムウェアの現状 2026 年版

過去 1 年間にランサムウェア攻撃を受けた日本の 152 の組織を対象とした、ベンダーに依存しない独自調査の結果。

ソフォスホワイトペーパー - 2026 年 7 月

レポートの概要

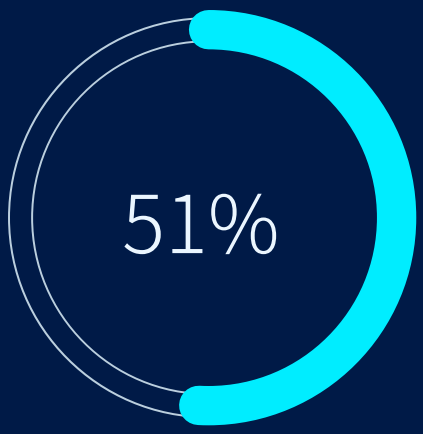
今年で 7 年目を迎える本レポートは、ソフォスが委託した、特定のベンダーに依存しない立場から、ランサムウェアに関する組織の経験についての調査した結果に基づいています。本レポートは、過去 1 年間にランサムウェア攻撃を受けた組織に所属する 2,158 人の IT/サイバーセキュリティリーダー (うち 152 人は日本の回答者) を対象とした調査の結果に基づいています。

本調査は 2026 年 1 月から 3 月にかけて実施されました。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。財務データはすべて米ドルで表示されています。このデータからは、4,000 万ドル以上の異常な身代金が削除されています。

回答者数

152

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。

日本の身代金支払額の中央値。

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として最も多かったのはフィッシングで、**26.3% の攻撃で使用され、次に多かったのは悪意のあるメール (25.7%)、認証情報の侵害 (25%) でした。脆弱性の悪用は、2025 年のレポートの 26% から 14% に大幅に減少しました。
- **運用面の根本原因は、専門知識の不足 (39%) が最も多く、**認識していなかったセキュリティギャップと既知のセキュリティギャップがそれぞれ 37% で続いています。
- **(NEW) メールやフィッシング以外の根本原因**で最も多かったのは、外部に公開されたアプリケーションとシステム (38%) であり、次に多かったのはファイアウォール (25%)、ユーザーデバイス (16%) でした。
- **(NEW) 74% の組織が、過去 1 年間の最も重大なランサムウェアインシデントが、その組織で最も重大だったアイデンティティ攻撃と同一のインシデントだったと回答しています。**

データへの影響

- **攻撃を受けた日本の回答者のうち 51% がデータを暗号化されたと回答しました。**この暗号化率は世界平均の 56% を下回っていますが、2025 年のレポートで日本の回答者が報告した 34% から増加しています。
- **データが暗号化された攻撃の 36% でデータも窃取されており、**この数値は 2025 年の 21% から上昇しています。
- データが暗号化された日本の組織の 96% 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 51% が身代金を支払ってデータを取り戻しています。**この数値は 2025 年のレポートの 70% から大幅に減少しています。
- **日本の組織の 58% 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 2025 年のレポートの 59% からわずかに減少しています。

身代金：要求額と支払額

- **日本の身代金要求額の中央値は 175 万ドルで、**2025 年のレポートで報告された 100 万ドルから 75% 増加しました。

日本の身代金要求額の中央値。

- **身代金要求額の 61% は 100 万ドル以上で、**2025 年のレポートの 53% から増加しています。
- **日本の身代金要求額の中央値は 300 万ドルで、**2025 年の調査で報告された 525,000 ドルから大幅な増加となりました。
- **日本の組織では、身代金要求額に対して中央値で 100% の金額を支払う傾向が見られました。**これは、2025 年のレポートの 68% から増加しています。

ランサムウェアによるビジネスへの影響

- 身代金支払額を除いた、**日本の組織におけるランサムウェア攻撃後の平均復旧コストは 188 万ドルでした。**これは、2025 年のレポートで報告された 67 万ドルから大幅に増加しています。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 52% は、ランサムウェア攻撃から 1 週間以内に復旧しました。**これは、2025 年のレポートの 50% からわずかに増加しています。復旧に 1 ～ 6 か月を要した組織は 23% であり、2025 年のレポートの 16% から顕著な増加が見られました。

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へのランサムウェアの人的影響

42% が、攻撃以降、継続的な業務量の増加を報告しています。この割合は、2025 年の 31% から上昇しました。

41% 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。

38% がストレスやメンタルヘルス問題によるスタッフの欠勤を経験しています。

32% が、シニアリーダーからのプレッシャーの増加を報告しています。

23% が、チームリーダーの交代を報告しています。

ソフォスの提言

ランサムウェア対策としてアイデンティティセキュリティを強化してください。日本のランサムウェア被害者の 4 分の 3 以上が、ランサムウェアインシデントが、その組織で最も重大だったアイデンティティ攻撃と同一のインシデントだったと回答しています。組織は、ITDR (アイデンティティ脅威の検知と対応) を優先し、すべてのアクセスポイントに多要素認証を適用し、人間と人間以外の両方のアイデンティティ認証情報を定期的に監査する必要があります。

最先端の AI モデル悪用した攻撃に備え、エンドポイント保護を強化してください。最先端の AI は、脆弱性の発見や悪用を加速させています。エクスプロイトを利用した攻撃を自動的にブロックできる強力なエンドポイント防御を備えることが不可欠です。

メールセキュリティに優先的に取り組んでください。日本では、フィッシングや悪意のあるメールがランサムウェア攻撃の根本原因の半数近くを占めています。そのため、組織は高度なメールフィルタリングを導入し、DMARC、DKIM、SPF プロトコルを実装するとともに、定期的なフィッシング対策トレーニングに投資することが重要です。

バックアップと復旧インフラに投資してください。堅牢なバックアップ体制を維持していた組織では、暗号化されたデータの復旧率が、過去最高に迫る水準となりました。バックアップは定期的にテストし、オフラインまたはイミュータブル (改ざん不可) な形式で保管するとともに、緊急時にも実行可能な文書化されたインシデント対応計画に組み込むべきです。

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/ransomware2026**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。

2026-07-28 JP-WP (TA) CRE-6011