SOPHOS

日本の
ランサムウェアの
現状 2023年版

日本の中規模組織の IT プロフェッショナル 300人を対象とした、ベンダーに依存しない独自調査の結果をお届けします。

ソフォス ホワイトペーパー2023 年 5月

調査について

ソフォスは、14 か国の中規模組織 (従業員数 100～5,000 人) に所属する 3,000人の IT/サイバーセキュリティリーダーを対象として、ベンダーに依存しない独立した調査を実施しました。調査は 2023 年 1月から 3月にかけて実施され、回答者には過去 12カ月の経験に基づいて回答するよう依頼しました。

主な調査結果

- **日本の組織の 58% が、昨年ランサムウェアの被害を受け**、2022年に被害報告を受けた 61% から若干減少しました。一方、全世界では、過去 12か月間に組織がランサムウェア攻撃を受けたと答えた回答者は 66% でした。
- **日本の組織における攻撃の根本原因は、「悪用された脆弱性」が最も多く、**インシデントの 37%で使用されています。侵害された認証情報は、2番目に多い攻撃ベクトルで、攻撃の 26% で使用されていました。
- **攻撃を受けた日本の回答者のうち 72% がデータを暗号化されました。**これは、世界平均である 76% よりもわずかに低いですが、日本の回答者が昨年報告した 69% よりもわずかに高い結果となっています。
- **また、データが暗号化された攻撃の 34% でデータが盗まれており、**これは世界平均の 30% をわずかに上回っています。
- **データが暗号化された日本の組織の 95% がデータを取り戻しており、**これは世界平均の 97% をわずかに下回っています。
- **バックアップは依然としてデータの復元に使用される最も一般的な方法であり、**日本の回答者の 60% がこのアプローチでデータを復元しました。これは、2022年の調査でバックアップを使用した 72% に比べて大幅な減少です。
- **日本ではデータを暗号化された企業のうち 52% が身代金を支払っており**、これは昨年の 50% からわずかに増加しています。2022年の調査と同様、日本の回答者は身代金を支払う傾向が平均以上であると報告されています (世界平均 2023年：47%、2022年：46%)
- **データが暗号化された日本の組織の 22% は、複数の復旧方法**を平行して使用していました。
- 身代金を支払った日本の組織の 20人の回答者は正確な金額を共有しています。身代金の支払額の平均値、中央値ともに**世界平均を大幅に下回っています。**
  - 身代金の支払いの平均値：日本平均 113,048 ドル / 世界平均 1,542,330 ドル
  - 身代金の支払いの中央値：日本平均 45,038 ドル / 世界平均 400,000 ドル

  55% が 5,000ドルから 99,999ドルの間で支払い、35% は 100,000ドルから 499,999ドルの間で支払いました。
- 身代金の支払いを除くと、**ランサムウェア攻撃から回復するために支払った日本の組織が負担した平均 (平均値) 請求額は、131万ドルと報告されており**、この中にはダウンタイム、人件費、デバイスのコスト、ネットワークコスト、逸失利益などのコストが含まれます。これは、世界平均コストの 182万ドルを下回っています。
- **ランサムウェアの被害を受けた日本の民間企業の 91% が、攻撃によりビジネスや収益が失われたと回答しており**、これは世界平均の 84% を上回っています。
- **日本の組織の 49% は、攻撃から回復するのに平均 1週間かかっています。**24% が 1か月かかり、28% が 1 ～ 6か月かかりました。

- **日本の組織の 82% が何らかの形のサイバー保険に加入していると回答しており**、47% が単独のサイバー保険、34% がより広範なビジネス保険の一部としてサイバー保険に加入していると回答しています。一方、世界的には、91% がサイバー保険に加入しており、47% が単独のサイバー保険、43% がより広範なビジネス保険の一部としてサイバー保険に加入していると回答しています。
- 昨年サイバー保険に加入した**日本の回答者の 93%** が、**防衛力が保険の内容に直接影響を与えたと答えています。**
  - 62% が、保険の補償範囲のコストに影響を与えたと回答
  - 58% が、保険加入能力に影響を与えたと回答
  - 29% が、保険の補償範囲の総額やサブリミットなどのポリシーの条件に影響を与えたと回答

まとめ

ランサムウェアは、引き続き日本の組織が直面する大きな脅威となっています。RaaS（Ransomware as a Service）のビジネスモデルが成長しているため、来年は攻撃が減少するとは予測していません。この観点から、組織は次のことに注力してください。

- 以下を使用して防御シールドをさらに強化すること
  - 脆弱性の悪用を防ぐ強力なエクスプロイト対策機能を備えたエンドポイント保護、侵害された認証情報の悪用を阻止する ZTNA (Zero Trust Network Access) など、最も一般的な攻撃ベクトルから防御するセキュリティツール
  - 攻撃への自動対応、攻撃者の妨害を行い、防御側が対応時間を稼ぐ適応型テクノロジー
  - 社内での提供、もしくは専門の MDR (Managed Detection and Response) サービスプロバイダーと連携しての提供に関わらず、24時間年中無休の脅威検出、調査、対応
- 定期的なバックアップの作成、バックアップからのデータの復元の練習、最新のインシデント対応計画の維持など、攻撃の準備を最適化すること
- タイムリーなパッチ適用やセキュリティツールの構成の定期的なレビューなど、適切なセキュリティ予防策の維持すること

詳細情報

ランサムウェアの現状 2023年版 レポートで、世界全体の調査結果や分野別のデータをご覧ください。

ランサムウェアの詳細と、ソフォス製品がお客様の企業の防御にどのように役立つかをご覧ください。

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。

2023-05-09 (WP-PC)