SOPHOS
Cybersecurity delivered.

日本の ランサムウェアの 現状 2022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2022年 4月

調査について

ソフォスが調査会社 Vanson Bourne 社に委託して、31 か国の中規模組織 (従業員数 100～5,000 人) に所属する 5,600 人の IT プロフェッショナルを対象に、ベンダーにとらわれない独立した調査を実施しました。調査は 2022 年 1 月から 2 月にかけて実施され、回答者には前年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 61% が、昨年ランサムウェアの被害を受け**、2020年に被害報告を受けた 15% から大幅に増加しました。これに対して、世界全体では、2021年にランサムウェア攻撃を経験した回答者は 66% でした。
- **攻撃を受けた日本の回答者 69% がデータを暗号化されました。**これは、世界平均の 65% よりやや高く、2020年に日本の回答者が報告した 47% から大幅に増加しています。
- **データを暗号化された日本の回答者の 95% が何らかのデータを取り戻しました。**これは、99% が少なくとも一部のデータを取り戻したと報告している世界的な結果と一致しています。
- **バックアップはデータの復元に使用された一番の方法であり、**日本の回答者の 72% がこのアプローチでデータを復元しました。**日本の回答者の 50% は身代金を支払いました。**複数のリカバリ方法を平行して使用することが、現在では一般的になっていることが分かります。これに対して、世界全体では、回答者の 73% がバックアップを使用し、46% が身代金を支払ってデータを復元しています。
- **身代金を支払った日本の組織は、平均して 54% のデータを取り戻しました。**世界的に見ると、身代金を支払った組織が復元したデータは 61% で、2020年の 65% よりも若干減少しています。
- 日本の回答者の 60人が正確な身代金の額を教えてくれました。**その平均支払額は 4,327,024米ドルになりました。**これは、すべての調査対象国の中で最も高い身代金の平均額です。5% は 10,000米ドル未満、48% は 100万米ドル以上を支払いました。世界的に見ると、身代金の平均支払額は 812,360米ドルで、100万米ドル以上の支払い率はほぼ 3倍に増加しました (2020年の 4% から 2021年の 11% に増加)。
- **2021年にランサムウェア攻撃の影響から復旧するための日本の組織が負担した平均コストは 960,000米ドルでした。**これは、2020年に報告された 1,610,000米ドルから大幅に減少しています。この平均復旧コストと平均身代金支払い額に差があるのは、多くの場合、被害者が身代金額を支払ったのではなく保険会社が支払ったことが反映されています。
- **日本の回答者の 92% が、ランサムウェアの攻撃が業務に支障をきたしたと回答しています。**これは、世界的な数値である 90% とさほど違いはありません。
- **日本の回答者の 89%が、ランサムウェアの攻撃により、自社の取引/収入の損失を招いたと回答しています。**これも、世界的な数値である 86% とさほど違いはありません。
- **日本の組織は、攻撃から回復するのに平均 1ヶ月かかりました。**
- **日本の回答者の 77% が、ランサムウェアが被害を受けた場合にはサイバー保険を利用していると回答しています。**世界全体では、この数値は 83% となっています。
- **97% が、この 1年間でサイバー保険の加入が困難になったと報告しています。**59% が保険の加入に求められるサイバーセキュリティのレベルが高くなったと回答し、50% がサイバーセキュリティのポリシーがより複雑になっていると述べ、44% が以前よりも保険の手続きプロセスに時間がかかると回答、30% が以前よりも高額になったと回答しています。サイバー保険の大幅な値上げが 2021年第 2四半期から第 3四半期にかけて始まったことを考えると、次回の更新時に多くの組織がかなりの値上げを経験する可能性があります。

- **96% は、保険の等級を向上させるために、過去 1年間にわたり、サイバー攻撃対策を変更しています。**世界全体では、97% が変更し、64% が新しいテクノロジー / サービスを導入し、56% が従業員のトレーニングと教育活動を強化し、52% がプロセスと行動を変更しました。
- **日本のランサムウェアの請求の 99% はサイバー保険で支払われました。**ランサムウェアの被害に遭い、ランサムウェアに対するサイバー保険が適用された組織のうち、保険会社は、再稼働させるための費用に 74%、身代金に 51%、その他の費用に 28% を支払ったと報告しています。

まとめ

日本の組織が直面しているランサムウェアの課題は、今後も拡大し続けます。サイバーセキュリティを最適化することは、すべての組織にとって不可欠です。重要な 5つのポイントは次のとおりです。

- 自社のすべてのポイントに高品質なエンドポイント保護製品を導入してください。既存のセキュリティコントロールを見直し、今後もニーズに応えられるようにしてください。
- プロアクティブに脅威を発見し、攻撃が実行される前に攻撃者を阻止します。社内に時間的余裕やスキルがない場合は、MDR のプロバイダーにアウトソーシングしてください
- パッチが適用されていないデバイス、保護されていないマシン、オープンになっている RDP ポートなど、セキュリティギャップを探し出し、塞ぐことでインフラを強化します。XDR はこの目的に最適なソリューションです。
- 最悪の事態に備えます。サイバーインシデントが発生した場合の対応策を把握し、事前に手順を実行する練習をしてください。
- バックアップを作成し、そこからの復元する練習します。目標は、迅速に復旧して稼働させることです。

詳細情報

ランサムウェアの現状 2022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。

それぞれのランサムウェアグループの詳細については、ソフォスランサムウェア脅威インテリジェンスセンターを参照してください。

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。

2022-04-04 (WP-NP)

SOPHOS