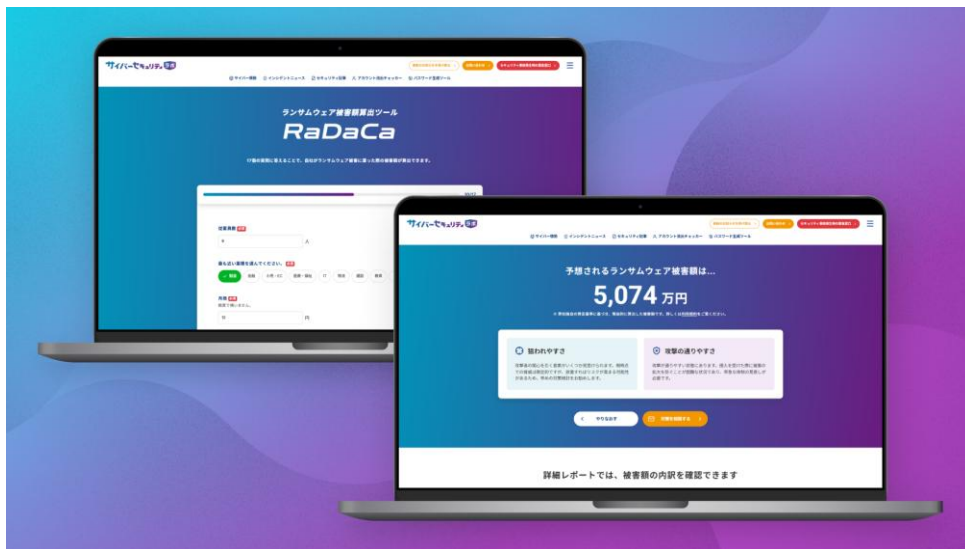


【実態調査公開】セキュリティ対策費用の説明に悩む企業が8割 ～投資判断を後押しするランサムウェア被害額算出ツール「RaDaCa」提供開始～

USEN & U-NEXT GROUPの株式会社USEN ICT Solutions（本社：東京都品川区、代表取締役社長：高橋 領一、以下、当社）は、当社が運営するメディアサイト「[サイバーセキュリティラボ](#)」にて、ランサムウェア被害額算出ツール「[RaDaCa（ラダカ）](#)」の提供を、本日10月1日（木）より開始します。

本ツールは、自社がランサムウェア攻撃を受けた際の想定被害額を具体的な金額で客観的に提示することで、現場担当者と経営層の認識ギャップを解消し、適切なセキュリティ投資の実現を支援するものです。

また、「RaDaCa」の公開に先んじて20社にトライアル導入いただき、セキュリティ対策や予算に関する現状・課題を把握するため、実態調査を行いました。



■ 背景

企業がランサムウェア攻撃による被害額を想定する際、損害賠償やフォレンジック調査、システム復旧など、直接的な対応にかかる費用のみを算出するケースが多く、業務停止に伴う損失は見落とされがちです。しかし、実際の被害額には、業務停止によって生じる逸失利益や機会損失も含まれます。業務が長期にわたって停止することも珍しくありません。

当社では2025年1月より、中堅・中小企業向けにサイバーセキュリティに関する情報発信を行う取り組みとして「サイバーセキュリティラボ」を展開し、情報セキュリティ事故の事例紹介や専門家によるセミナーなどを通じて、実務に資する情報提供を行ってきました。今回、「サイバーセキュリティラボ」上に公開する「RaDaCa」では、被害額の想定から抜け落ちやすい逸失利益や機会損失も含め、被害総額を算出できます。当社は「RaDaCa」の提供を通じて、企業の適切なセキュリティ投資を支援します。

■ ランサムウェア被害額算出ツール「RaDaCa」について

「RaDaCa」は、当社が運営する「サイバーセキュリティラボ」上で提供する、ランサムウェア攻撃の想定被害額を算出できるツールです。いくつかの質問に回答するだけで、見落とされがちな逸失利益や機会損失を含め、ランサムウェア攻撃を受けた際に想定される被害額を具体的な数値として可視化できます。

ランサムウェア攻撃によるリスクを具体的な金額に置き換えることで、経営層に対してセキュリティ対策の必要性や費用対効果を論理的に説明しやすくなります。また、算出された想定被害額と現在のセキュリティ対策予算を比較することで、投資金額が妥当か、あるいは不足しているかを判断する際の基準として活用できます。

ランサムウェア被害額算出ツール「RaDaCa」：<https://www.gate02.ne.jp/lab/radaca/>

「サイバーセキュリティラボ」：<https://www.gate02.ne.jp/lab/>

■ 先行トライアルとアンケート調査で明らかになった課題

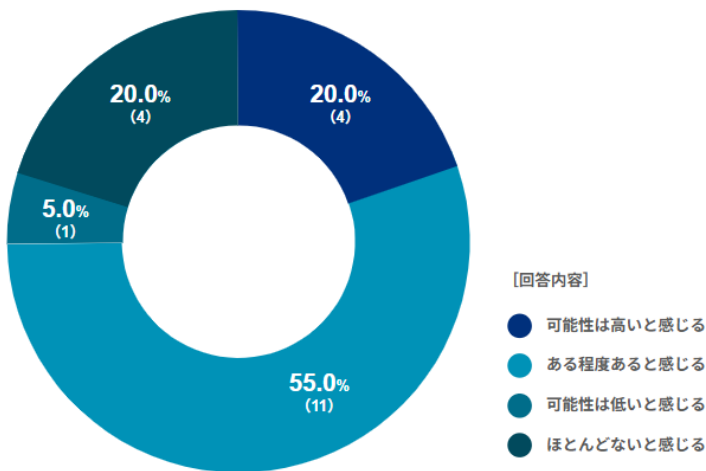
当社が20社に対して実施したアンケート調査では、サイバーセキュリティへの危機感はあるものの、現場担当者の多くが「経営層に被害の具体的な金額イメージを伝えるのが難しい」「費用対効果を説明しづらい」という共通の課題を抱えていることが明らかになりました。

75%以上は「狙われるかもしれない」と思っている

「自社がランサムウェア攻撃の標的になるかもしれないと感じるかどうか」という問いに対して、75%の企業が「標的になるかもしれないと感じている」という旨の回答をしました。この結果から、多くの企業がランサムウェア攻撃を自社にも起こり得る身近なリスクとして捉えていることが分かります。

Q. 自社がランサムウェア攻撃の標的になるかもしれないと感じますか？

* 回答者数 20名



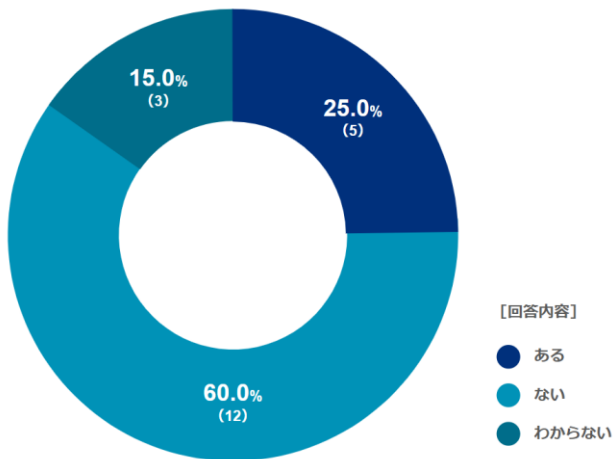
© 2025 USEN ICT Solutions CORPORATION

経営層との議論不足がもたらす予算確保の壁

一方で、サイバー攻撃対策について経営層と具体的な金額をもとに議論したことが「ない」「わからない」と回答した企業は75%となりました。

Q. ランサムウェア対策について経営層と具体的な金額を挙げて議論したことがありますか。

* 回答者数 20名

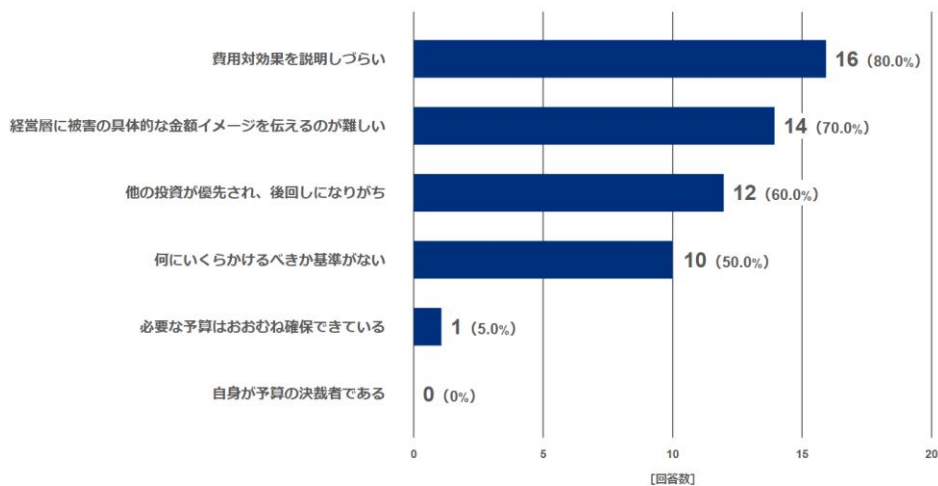


© 2026 USEN ICT Solutions CORPORATION

また、現場担当者はセキュリティ予算の確保について以下のような課題を感じていることが分かりました。

Q. セキュリティ予算の確保について当てはまるものをすべてお選びください。

* 回答者数 20名



© 2026 USEN ICT Solutions CORPORATION

セキュリティ予算の確保についての問いでは、経営層への具体的な金額をもとにした議論の不足や、セキュリティ予算の確保に関する課題が浮かび上がりました。

バックアップの保管・復旧体制に課題

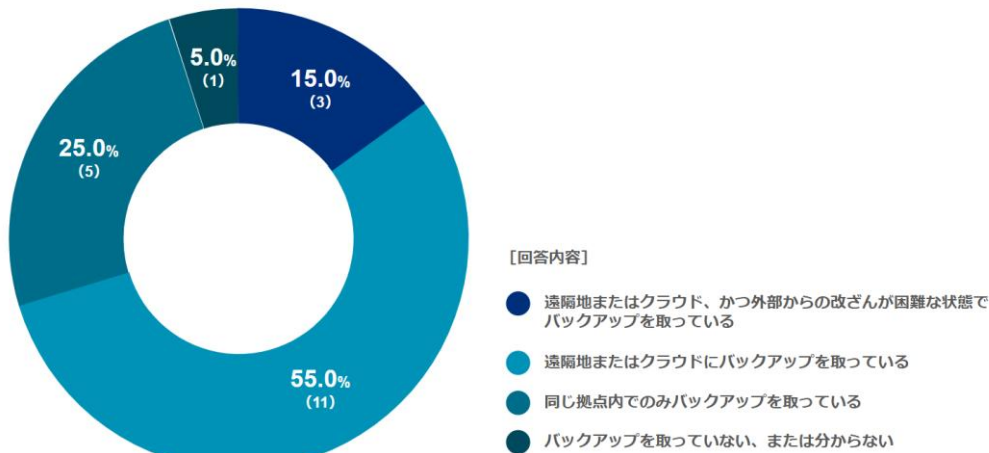
「ランサムウェアの被害にあう可能性はあるものの、どの程度のセキュリティ投資が妥当なのか判断できない」という状況から、データのバックアップの取得にとどまっている企業もあると考えられます。しかし、バックアップは取得するだけで十分とは限らず、その運用方法によっては新たなリスクにつながる可能性があります。

調査に協力した企業の95%がバックアップを取得している一方、外部からの改ざんが困難な環境で安全に保管している企業は15%にとどまりました。

近年のランサムウェア攻撃では、本番データだけでなく、バックアップデータも暗号化や削除の対象となるケースがあります。特に、本番環境と同じネットワーク上にあり、同じ認証情報でアクセスできるバックアップは、攻撃者の侵入によって本番データと同時に被害を受ける可能性があります。そのため、バックアップを取得するだけでなく、本番環境から切り離された場所に保管するなど、攻撃を受けた際にもデータを保護できる状態を整えておくことが重要です。

Q. システムやデータのバックアップ体制を教えてください。

* 回答者数 20名



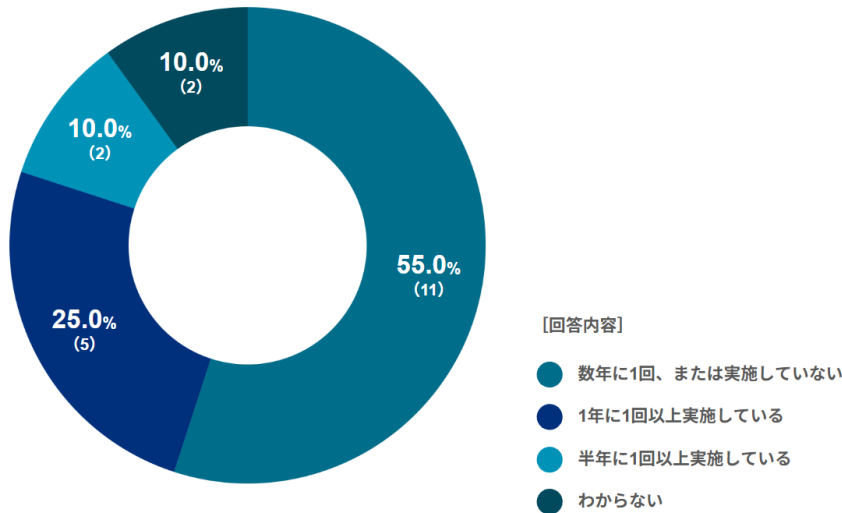
© 2026 USEN ICT Solutions CORPORATION

バックアップデータを保管するだけでなく、セキュリティインシデントの発生時に、そのデータを用いて正常かつ迅速に復旧できる体制を整えておくことも重要です。復旧作業に時間を要すると、業務停止期間が長期化し、ランサムウェアによる被害額の拡大につながる可能性があるためです。

そのため、バックアップについてはデータの取得や保管に加え、実際に本番環境へ復元できるかを定期的に確認し、円滑に復旧できる状態を維持する必要があります。しかし、今回の調査では、セキュリティインシデントの発生を想定した復旧訓練を定期的に行っている企業は、約35%にとどまりました。

Q. セキュリティインシデントの復旧訓練は実施していますか？

* 回答者数 20名



© 2026 USEN ICT Solutions CORPORATION

「RaDaCa」の監修を務めた、東京大学先端科学技術研究センター 客員研究員の西尾 素己氏は、開発の背景や意図について、以下のようにコメントしています。

■ 監修者コメント

東京大学先端科学技術研究センター 客員研究員：西尾 素己氏

昨今のサイバー攻撃は、AIを悪用した無差別攻撃が激化しており、事業規模に関わらず「攻撃を受けること」を大前提とした対策が不可欠です。

対策費用を捻出する際に重要なのは、自社が被害にあった場合の損失を金額ベースで把握することです。最大の被害額をもとに、そのリスクを回避するための費用として、ロジカルに予算を算定すべきだと考えます。

これらの課題意識から、私はランサムウェア被害額算出ツール「RaDaCa」の監修をお引き受けしました。「RaDaCa」は専門家の知見に基づき、企業環境や攻撃の受けやすさを踏まえて、確実な数値を出すことよりも、想定される最大の被害額を試算できるロジックを優先して設計しています。

被害は復旧費用だけではなく、事業停止の損失や信用の毀損など無形資産にも及びます。「RaDaCa」がこうしたリスクまで見据えた、ランサムウェア被害対策における見直しの一助となれば幸いです。

■ まとめ

日本情報経済社会推進協会（JIPDEC）の「企業IT利活用動向調査2026」によると、回答企業の約2社に1社がランサムウェアによる被害を経験しており、被害額が数千万円から億円規模に及ぶケースも報告されています。こうした調査結果からも、ランサムウェア攻撃は企業の事業継続を脅かす、極めて現実的なリスクといえます。

一方、現場担当者が日々の報道などを通じて危機感を高めていても、自社で想定される被害額を具体的に数値化・可視化できなければ、経営層に対してセキュリティ投資の必要性や妥当性を十分に説明することは容易ではありません。

こうした課題に対し、「RaDaCa」はランサムウェア攻撃による想定被害額を具体的な金額で可視化することで、経営層と現場担当者の共通認識の形成を支援します。

当社は「RaDaCa」の提供を通じて、企業の適切なセキュリティ投資を後押しするとともに、今後も社会課題の解決につながるソリューションの提供と情報発信に取り組み、企業の安全な事業継続に貢献してまいります。

（参考：2026年4月発行「企業IT利活用動向調査2026」から見る日本企業のDX、AI活用、ランサムウェア被害の実態）

■調査概要

調査名称：「ランサムウェア対策に関する実態調査」

調査期間：2026年7月21日～2026年8月7日

調査対象：20社（20名）

調査方法：Webアンケート

先行トライアルやアンケート調査結果の詳細は、以下のフォームよりお申し込みください。

「ランサムウェア被害額算出ツール「RaDaCa」で導くリスクの金額化と対策ガイド」

URL：<https://www.gate02.ne.jp/document/risk-visualization-and-countermeasures-by-radaca/>

ランサムウェア被害額算出ツール「RaDaCa」はこちら

URL：<https://www.gate02.ne.jp/lab/radaca/>

*本調査結果を引用いただく際には、以下出典元の明記をお願いいたします。

記載例／データ提供：株式会社USEN ICT Solutions（U-NEXT.HD）「ランサムウェア対策に関する実態調査」（2026年10月発表）

■会社概要

会社名：株式会社USEN ICT Solutions

所在地：東京都品川区上大崎三丁目1番1号 目黒セントラルスクエア

代表者：代表取締役社長 高橋 領一

設立：2017年6月16日

事業内容：電気通信事業法に基づく電気通信事業（届出番号/A-29-16072）、ICT サービス等に関わる事業

URL：<https://usen-ict.co.jp>

法人向けICTソリューション「USEN GATE 02」：<https://www.gate02.ne.jp>

サイバーセキュリティラボ：<https://www.gate02.ne.jp/lab/>

AI-Clutch：<https://ai.gate02.ne.jp>

【報道関係者からのお問い合わせ先】

株式会社U-NEXT HOLDINGS 広報部

TEL：03-6823-2010／MAIL：unhdpr@unext-hd.jp

お問い合わせフォーム：[こちら](#)

【お客様からのお問い合わせ先】

株式会社USEN ICT Solutions

お問い合わせフォーム：[こちら](#)