PRESS RELEASE

報道関係者各位

2025 年 11 月 25 日
株式会社オーケーウェブ

【独自調査】なぜ防げない？ランサムウェア侵入経路、企業と個人の「認識ギャップ」が浮き彫りに

世界中のありがとうの物語を蓄積し可視化する」をパーパスとし、法人・個人向けコミュニティサービスを展開する株式会社オーケーウェブ（東京都港区、代表取締役：杉浦元、以下「オーケーウェブ」）は、深刻化するランサムウェア攻撃の脅威に対し、その侵入経路の実態と一般ユーザーの防衛意識に関する調査（n=500 人）を実施しました。

調査結果を詳しく見る

■OKWAVE の投稿から読み解く、セキュリティ対策への意識の高まり

近年、ランサムウェアの被害件数は高止まりしており、企業活動に甚大な影響を与えています。同時に、**国内最大級の Q&A コミュニティ「OKWAVE」においても、「ウイルスに感染したかもしれない」「身に覚えのない請求が来た」「セキュリティソフトはどれがい**

いか」といったセキュリティ対策に関する悩みや相談が近年増加傾向にあり、一般ユーザーの不安も高まっていることが伺えます。

こうした背景から、本調査では**「企業の被害実態」**と**「個人の防衛意識」**という 2 つの側面から脅威の実態を分析しました。調査は、近年の国内外における企業のランサムウェア被害事例（※1）の分析と、一般ユーザー500 名を対象としたセキュリティ意識に関するアンケート調査（※2）の二部構成で行いました。

その結果、**企業が最も警戒すべき侵入経路と、一般ユーザーが「危険」と認識している経路との間に、深刻な「認識のギャップ」が存在**することが明らかになりました。

（※1）IPA（情報処理推進機構）、警察庁、JPCERT/CC、海外 CERT 機関などが公開しているインシデントレポートを基に分析。

（※2）調査期間：2025 年 11 月 1 日～11 月 21 日、調査対象：全国のインターネット利用者 500 名、調査方法：Web アンケート調査

■調査結果サマリー

- **企業への最大の脅威は「VPN・RDP」**
  近年の国内・海外のランサムウェア被害事例を分析した結果、攻撃の主要な侵入経路（初期アクセス）は、**「VPN 機器の脆弱性」（約 45%）**と**「リモートデスクトップ（RDP）」（約 30%）を合わせて 75%**を占めました。これらはテレワーク普及に伴い外部に公開された IT インフラであり、攻撃者にとって格好の標的となっています。

- **一般ユーザーの認識は「メール」に集中**
  一般ユーザー500 名に「コンピューターウイルスの感染経路（複数選択可）」を尋ねたところ、**「メールの添付ファイル・URL リンク」（約 90%）**が突出し、次いで**「不正サイトや広告」（約 80%）**となりました。**企業への侵入経路として深刻な「VPN」や「RDP」は、ほとんど認識されていませんでした。**

- **ランサムウェア認知度「知っている」8 割、「仕組みも理解」は 2 割**
  「ランサムウェア」という言葉自体は約 80%（「よく知っている」約 20%、「聞いたことはある」約 60%）が認知していました。しかし、**その仕組みまで理解し**

ている層は 2 割に留まり、脅威の具体的な内容が浸透していない可能性が示唆されました。

- **8 割が「不安」だが、基本的な防御策が手薄**
  現状のセキュリティ対策について、**全体の約 80%が「不安を感じている」**と回答しました。しかし、具体的な対策（複数回答）を見ると、**「ウイルス対策ソフトの利用」は約 60%、「定期的なバックアップ」はわずか約 30%**に留まりました。**「不審なメールを開かない」（約 80%）といった意識面の対策に比べ、技術的な防御策の実施率が著しく低い結果**となりました。

■調査結果ハイライト

1. 企業への主な侵入経路：「外部公開機器の脆弱性」が 7 割超
近年のランサムウェア攻撃グループ（RaaS など）による企業・組織への侵入事例を分析した結果、最も多く利用されている侵入経路は以下の通りです。

1. **VPN 機器の脆弱性を悪用した侵入（約 45%）**テレワークの普及で増加した VPN 機器の、修正パッチが未適用の脆弱性を突き、不正アクセスを行う手口が主流となっています。
2. **リモートデスクトップ（RDP）経由の侵入（約 30%）**外部に公開された RDP に対し、推測しやすいパスワードや流出した認証情報を用いたブルートフォース攻撃（総当たり攻撃）による侵入が後を絶ちません。
3. **フィッシングメール（約 20%）**従来型の手口である、不正な添付ファイルやリンクを含むメールを従業員に送り付け、マルウェアに感染させる経路も依然として高い割合を占めています。
4. **その他（サプライチェーン攻撃など）（約 5%）**

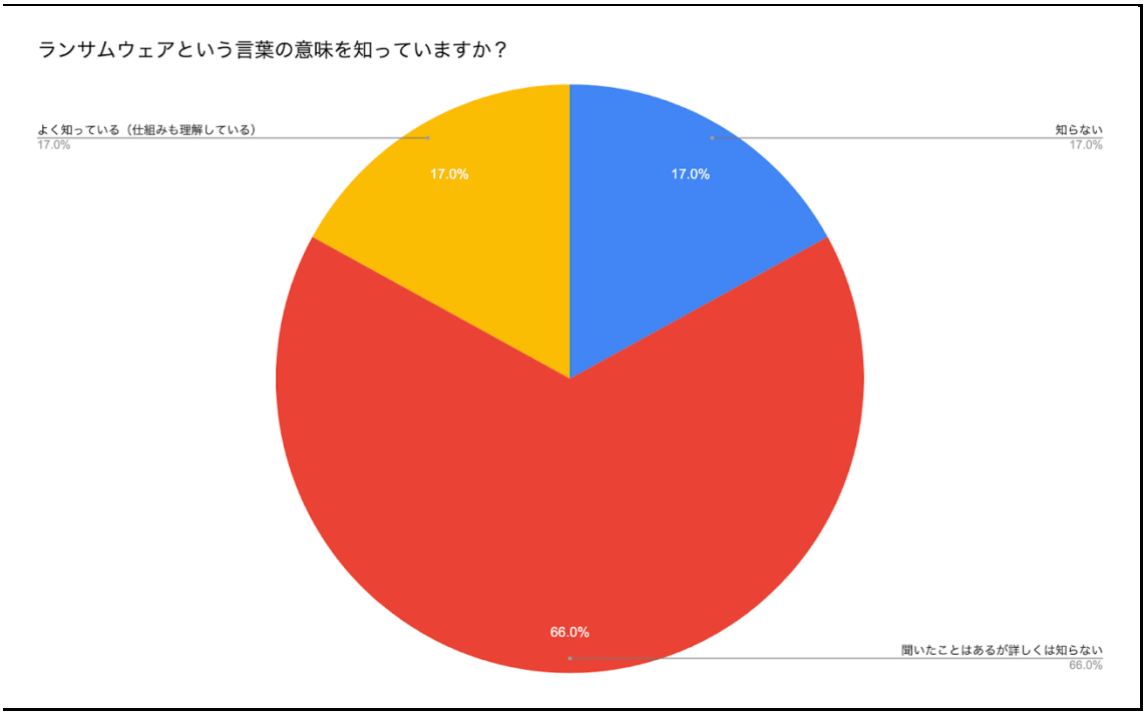
多くの企業が『従業員のメール開封』を最大の脅威と捉えがちですが、実態は異なることがわかりました。近年の高度な攻撃グループは、まず企業の『入口』である VPN や RDP といった外部公開サーバーの脆弱性を執拗に狙います。ここを突破されれば、フィッシングメールを介さずとも、一気にネットワーク内部へ侵入されてしまいます。防御の焦点は『人』だけでなく『システム』にも当てる必要があるようです。

2. 一般ユーザーの意識調査：「メール」への警戒が突出、セキュリティ対策に「不安」と「穴」

一般ユーザー500 名へのアンケート結果からは、企業の被害実態とは異なる傾向が見られました。

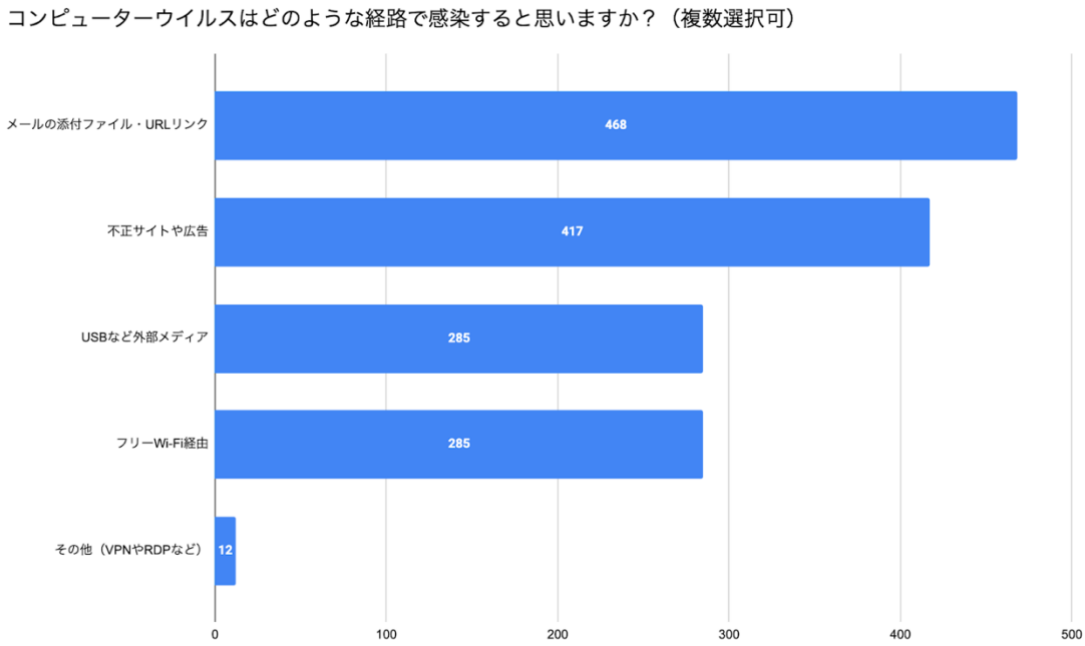
●ランサムウェア認知度「知っている」8 割、「仕組みも理解」は 2 割

「ランサムウェア」という言葉自体は約 80%（「よく知っている」約 20%、「聞いたことはある」約 60%）が認知していました。しかし、その仕組みまで理解している層は 2 割に留まり、**脅威の具体的な内容が浸透していない可能性**が示唆されました。



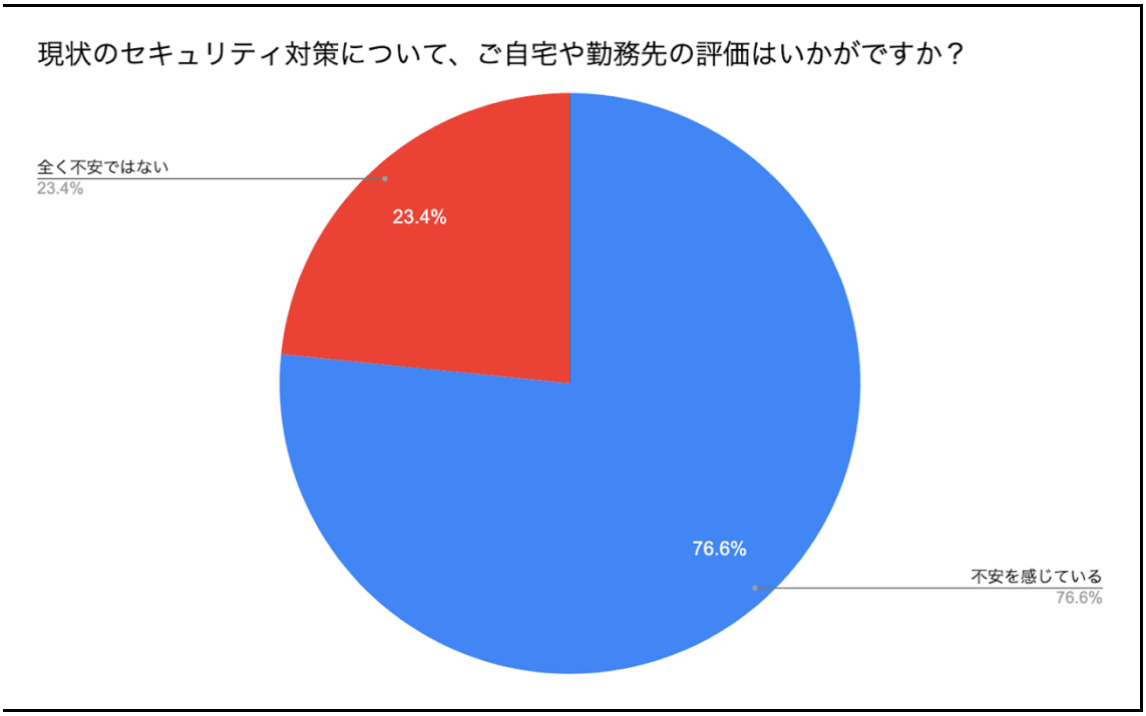
●感染経路の認識「メール」が 9 割、VPN/RDP は認識外

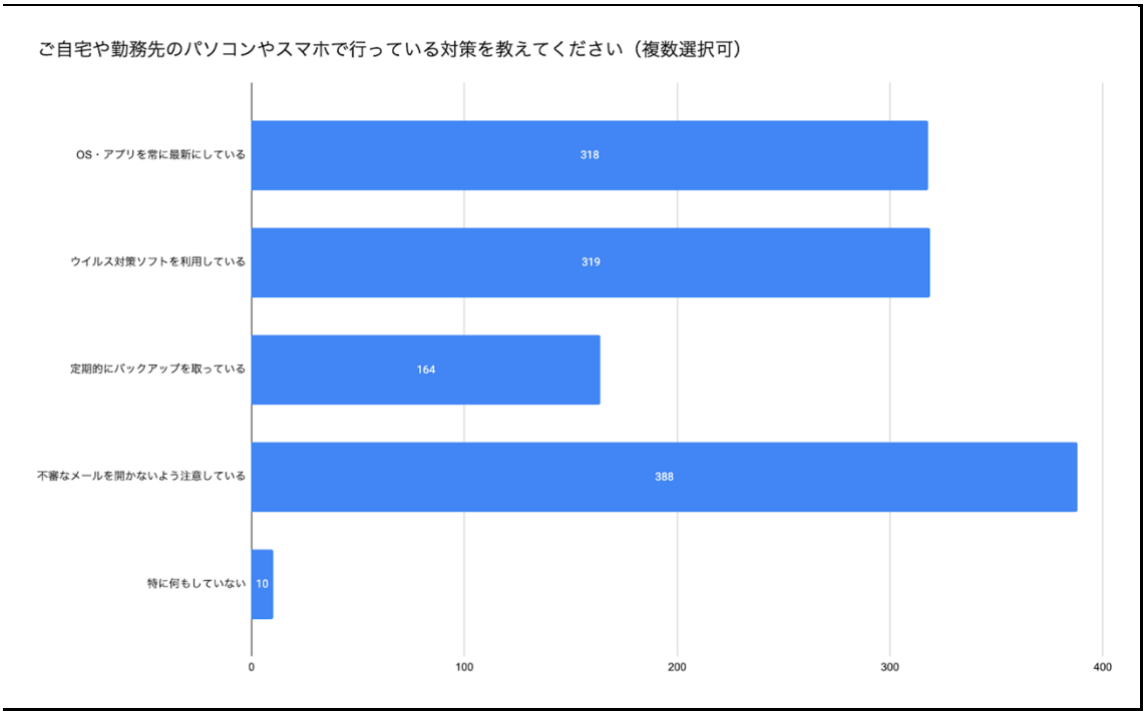
一般ユーザー500 名に「コンピューターウイルスの感染経路（複数選択可）」を尋ねたところ、「メールの添付ファイル・URL リンク」（約 90%）が突出し、次いで「不正サイトや広告」（約 80%）となりました。**企業への侵入経路として深刻な「VPN」や「RDP」は、ほとんど認識されていない**ことがわかりました。



●セキュリティ対策の実態：8 割が「不安」、しかし「バックアップ」実施率は 3 割

現状のセキュリティ対策について、全体の約 80%が「不安を感じている」と回答しました。しかし、具体的な対策（複数回答）を見ると、「ウイルス対策ソフトの利用」は約 60%、「定期的なバックアップ」はわずか約 30%に留まりました。「不審なメールを開かない」（約 80%）といった意識面の対策に比べ、**技術的な防御策の実施率が著しく低い結果となり、多くのユーザーが基本的な防御網を持たないままインターネットを利用している危険な実態**が明らかになりました。





■狙われる「入口」と「意識」のギャップ

今回の調査で、ランサムウェア攻撃の「実際（企業の侵入経路）」と「一般の認識（アンケート結果）」には大きなギャップがあることが明らかになりました。

- **ギャップ 1：【経路】 企業は「機器の脆弱性」、個人は「メール」を警戒**
  実際の企業被害は、VPN や RDP など外部公開機器の脆弱性や設定不備を突かれるケースが最多（約 75%）です。しかし、**一般ユーザーの意識は「メール（約 90%）」に集中**しており、**システム的な脆弱性への認識が低い**ことが示唆されました。

- **ギャップ 2：【対策】 8 割が「不安」なのに、最も重要な「バックアップ」は 3 割**
  多くの人がセキュリティに不安を感じている一方で、**ランサムウェア被害からの「最終防衛策」であるバックアップの実施率は約 30%と極めて低水準**です。これは、攻撃を受けた際、身代金を支払うか、データを全て諦めるかの二択を迫られる企業・個人が多いことを示しており、非常に危険な状態です。

■今すぐ取り組むべき「鉄壁の 4 防衛ライン」とは？
ランサムウェア攻撃は「たまたまメールを開いた一人の従業員」だけが原因ではありません。**システム的な脆弱性と、従業員の意識の両面から対策を講じる必要**があります。そこで、今すぐ取り組むべきセキュリティ対策の鉄壁の 4 防衛ラインをご紹介します。

第 1 の防衛ライン：【入口対策】外部からの侵入を徹底的に防ぐ
攻撃者が最初に狙う「入口」を固めます。テレワークの普及により、VPN 機器やリモートデスクトップ（RDP）が最大の標的となっています。
脆弱性管理の徹底（使用している VPN 機器やサーバーのセキュリティパッチを常に最新の状態に保ち、不要なポートは閉鎖する）や、**多要素認証（MFA）の必須化**（VPN、RDP、クラウドサービスなど、外部からアクセスする全てのアカウントに多要素認証を導入する）などを実施しましょう。

第 2 の防衛ライン：【端末対策】マルウェアの実行を阻止する
万が一、メールや Web サイト経由でマルウェアが侵入しても、実行させないための対策です。
まずは、**信頼できるセキュリティソフト（アンチウイルス/EDR）の導入**をしましょう。アンケート結果では導入率が低い結果でしたが、これは**必須の対策**です。既知のウイルスを検知する従来型アンチウイルス（EPP）に加え、未知の脅威や侵入後の不審な挙動を検知・隔離する EDR（Endpoint Detection and Response）の導入が、現代の企業防衛には

不可欠です。さらに、**OS・ソフトウェアの最新化**も実施するようにしましょう。これは全従業員・全端末で 100%実施されるべき基本中の基本施策です。

第 3 の防衛ライン：【人的対策】「うっかり」を組織で防ぐ
従業員のセキュリティ意識は、依然として重要な防衛ラインです。「不審なメールを開かない」という意識は高いものの、攻撃は巧妙化しています。怪しいメールを見分ける訓練を定期的に行い、IT 部門へ即時報告する体制を構築するといいでしょう。

第 4 の防衛ライン：【復旧対策】被害を最小限に抑える
どれだけ防御しても、100%防ぎきることは不可能です。攻撃されることを前提とした「復旧」の準備が、事業継続の鍵となります。**バックアップを正しく、定期的に実施しましょう。アンケートで実施率が低かったこのバックアップこそが、ランサムウェア攻撃を受けた際の「最後の砦」**となります。

まずは、基本的な防御の徹底が最重要
今回の調査で、**ランサムウェア攻撃の「実際（企業の侵入経路）」と「一般の認識（アンケート結果）」には大きなギャップがあることが明らか**になりました。
さらに深刻なのは、多くのユーザーが不安を感じながらも、**ランサムウェア被害の「最後の砦」であるはずのバックアップや、基本的な防御であるウイルス対策ソフトが徹底されていない実態**です。 この「意識」と「実行」のギャップが、ランサムウェア攻撃成功の隙を与えていると考えられます。**企業は、基本的な防御策を最優先するとともに、従業員教育、そして万が一の事態に備えた「オフライン・バックアップ」の徹底が必要**でしょう。

今回は、国内最大級の Q&A コミュニティ「OKWAVE」において近年増加傾向にある「セキュリティ対策に関する悩み」をテーマに調査いたしました。株式会社オーケーウェブは、今後も人々の疑問や不安に寄り添い、より実態に即した情報提供に努めてまいります。

■アンケート調査概要
調査主体：株式会社オーケーウェブ
調査名：セキュリティ対策に関する意識調査
調査対象：一般ユーザー
調査期間：2025 年 11 月
調査方法：インターネット調査

有効回答数：500 名

本調査リリースの内容に加え、さらなる詳細については、弊社運営メディア『OKWAVE セレクト』内にて詳しくご紹介しています。

セキュリティ対策に関する詳細はこちら

・セキュリティソフト関連記事
MetaDefender Core
MetaDefender Kiosk
Sophos Firewall XGS
u.trust LAN Crypt
Webroot
Carbonite® Endpoint

・セキュリティ関連記事
バックアップ戦略のよくある失敗と対策事例
【2025 年版】最新サイバー攻撃の手口と対策
暗号化ソフト導入の注意点と運用のコツ
UTM とは？ファイアウォールとの違いとメリット
MetaDefender Core の仕組みと導入メリット
【2025 年版】マルウェア被害の動向と企業対策

■株式会社オーケーウェブの取り組みと今後の展望
株式会社オーケーウェブは、「互い助け合う社会の実現」を理念に掲げ、世界を『ありがとう』で満たすことを目指しています。

現代社会は、分断や対立といった課題が語られることが多くあります。しかし、その一方で、私たちの日常には数えきれないほどの『ありがとう』が存在しています。オフィスや学校、家庭、街中や旅先など、日々のあらゆる場面で人と人とが支え合い、小さな『ありがとう』が自然に生まれています。

オーケーウェブは、こうした日常の『ありがとう』に光を当て、その背景にある物語を可視化することを通じて、人々がより優しさや温かさを実感できる社会をつくりたいと考えています。

一人ひとりがこの一か月に交わした『ありがとう』
組織やコミュニティの中で積み重なった『ありがとう』
世界中で今この瞬間に生まれている無数の『ありがとう』

これらを共有・循環させることで、世界はよりやさしく、温かく、そして豊かな場所になっていくはずです。

今後も株式会社オーケーウェブは、「ありがとう」を核とした事業やサービスを進化させ、利用者や社会全体の信頼と共感を育む取り組みを展開してまいります。そして、世界中の『ありがとう』をつなぎ、その可能性を最大化するプラットフォームとして、新たな価値を創造し続けてまいります。

【記事等へのデータ引用・転載時のお願い】
本リリースの調査結果・画像をご利用いただく際は、必ず株式会社オーケーウェブ公式サイト（ https://okwave.co.jp/ ）へのリンク設置をお願い致します。

■株式会社オーケーウェブについて
株式会社オーケーウェブ（証券コード：3808）は、「世界中のありがとうの物語を蓄積し可視化する」ことをパーパスに掲げ、お互いを助け合う（互助）プラットフォームの運営と、互助の絆や関係性を作るサービスを提供。

Q&A 形式のコミュニティサイト『OKWAVE』の運営を軸に、ユーザー参加型のサポートコミュニティ『OKWAVE Plus』を企業や地方自治体向けに提供するほか、700 社以上の導入実績のあるクラウドサンクスカード『GRATICA』を展開しています。
また、メディアサービスでは『OKWAVE media』を中心に、強いドメインパワーを活かした記事制作・配信を展開し、企業や団体の広報・PR 活動を支援しています。

代表者：代表取締役社長　杉浦 元
本社所在地：東京都港区新橋 3 丁目 11-8　オーイズミ新橋第 2 ビル 702
URL： https://www.okwave.co.jp/

■本件に関するお問い合わせ先

株式会社オーケーウェブ
事業推進グループ
E-mail：sales_okwaveplus@ml.okwave.co.jp

当社は、今後も互い助け合いをベースとしたコミュニティの DX 化を通じて、様々な社会課題の解決や地域の発展に寄与するサービスを提供してまいります。

※ここに掲載されている情報は、発表日現在の情報です。最新の情報と異なる場合がありますので、あらかじめご了承ください。