

被害に遭った企業	被害内容と原因
日揮ユニバーサル株式会社	2024年12月、同社の一部サーバー内のデータが暗号化し、個人データを含む情報漏洩の可能性を確認した旨を発表。調査の結果、同社で管理する一部のサーバーがランサムウェアに感染していることを確認。原因については、インターネットとの接続口から社内環境へ侵入されたとしている。
カシオ計算機株式会社	2025年1月、同社が2024年10月に公表した自社サーバーに対するランサムウェア感染問題について、社内外関係者や取引先、ユーザーなど合計8478名の個人情報流出を確認したと発表。原因については、フィッシングメール対策および海外拠点を含むグローバルでのネットワークセキュリティの不備としている。
日本海建設電気株式会社	2025年1月、サーバーが外部からの不正アクセスを受けランサムウェアに感染した結果、保有する一部の個人情報データがウェブに公開された旨を発表。個人情報の漏洩については、警察からの連絡で判明した。原因については、導入していたVPN機器に関連したセキュリティ機器のシステムが更新されていなかったためとしている。
株式会社オートメ技研	2025年2月、サーバーが外部からの不正アクセスにともない、ランサムウェアに感染したと発表。原因については、同社が利用するVPNの脆弱性を利用し不正アクセスが行われた可能性が確認されている。

その影響は同社に物流業務を委託していた(株)良品計画や(株)ロフトにもおよんだ。

ランサムウェア被害の傾向が、表に示したように「暗号化」から「情報流出・公開」へと変わってきていることにも注目したい。しかも、その多くが当初はシステム障害と認識されていたのに、調査の過程でランサムウェア感染が原因であることが判明したというケースであることも見過ごせない。つまり、知らず知らずのうちにランサムウェアに感染し、情報流出につながるケースが拡大しているのだ。

では、拡大するランサムウェア被害にどのように対応すればよいのか。その点について、セキュリティ会社の(株)ブロード(東京都千代田区)は「ランサムウェアを含む不正アクセスの主な経路はVPN(仮想専用通信網)などの脆弱性や不適切な設定であることが多い」と指摘。社内ネットワークおよびWEBシステムで横断的に脆弱性を把

握し、さらに実際に侵害可能なポイントでAIが自動検証する「RidgeBot」などの導入がオススメだ、と。ただし「実際にはそこにいきなり侵入するわけではなく、多数の段階を経て攻撃している」とも。だからこそ「日常的にユーザーが使用しているパソコンでのメールやインターネット閲覧のリスクを100%に隔離するエンドポイント対策『HP SCE』を導入する」と強調する。さらに内部からの漏洩を防ぐためには、特権アクセスを制御し、侵害のシステム間展開や誤操作・内部不正を防ぐ「BeyondTrust」製品群を導入するのも一案だとアドバイスする。

ブロードはセキュリティ分野では業界のトップリーダー、自社にマッチしたソリューションをアドバイスしてもらうのはどうか。サイバー対策にはやはり転ばぬ先の杖が効果的だ。

大手企業でも被害が拡大中!!

ランサムウェア被害をどう防ぐか

警察庁の発表によると、2025年上期の国内ランサムウェア被害報告件数は116件に達し、前年から微増という結果になった。また本誌の調査によると、国内で企業・団体が公表したサイバーインシデント事例は150件に達しており、なかでもランサムウェア被害が目立っていた。そこで、今号では昨今のランサムウェア被害の傾向と対策について紹介したい。

攻撃は最大の防御なり

Ridge Security - RidgeBot®

高度な知識を要するセキュリティ検証を AI で自動化！
進化を続ける攻撃の手口をいち早くシミュレーション！
実在するセキュリティの弱点を継続的に発見！

詳細は [Broad Security Square] で <https://bs-square.jp/columbus>

株式会社ブロード

〒100-0014 東京都千代田区永田町1-11-30 サウスビル永田町 7F
TEL: 03-6205-7463 (代表)