

警察庁「令和8年上半期」 ランサムウェア被害の6割が 中小企業だった。 業務データのバックアップ自動化を 進める3つのステップ

警察庁が2026年9月10日に公表した令和8年上半期サイバー脅威情勢で、ランサムウェア被害123件（半期最多）のうち約6割が中小企業。製造業が最多業種。業務データを失わないバックアップ設計と自動化の3ステップを解説します。

警察庁が公表した令和8年上半期の状況

警察庁「令和8年上半期におけるサイバー空間をめぐる脅威の情勢等について」（2026年9月10日公表）によると、上半期のランサムウェア被害届出件数は123件で、統計開始の2020年下半期以降、半期として過去最多となりました。

企業・団体の規模別内訳は、中小企業79件（約64%）、大企業31件、団体等13件。業種別では製造業が37件と最多（全体の約3割）です。

中小企業に関係する3つの論点

論点1：件数では中小企業が多数派

「大企業が狙われる」というイメージがありますが、被害の件数では中小企業が全体の約6割を占めています。攻撃の手口が自動化・大量送信型の場合、企業規模に関係なく感染の機会が生まれます。「自社は小さいから狙われない」という前提は統計と合っていません。

論点2：製造業・物流業は「止まること」で損失が直撃する

ランサムウェアに感染すると、業務データが暗号化され業務システムにアクセスできなくなります。製造業で受注・出荷・在庫情報が使えなくなるとラインが止まり、物流業で配送スケジュールが失われると当日の配送が組めません。製造業が最多業種（37件）であることは、この「止まる業種」での被害が表れています。

論点3：「戻せるかどうか」が被害の規模を決める

バックアップが感染したPCと同じ場所に保存されていたり世代管理されていなかったりすると、バックアップごと暗号化されてしまいます。「感染した後に戻せるか」を事前に確認しておくことが、被害の大小を分ける最大の要因のひとつです。

自社で今日から確認できる5項目

#	確認すること	答えられないときのリスク
1	業務データ（受注・顧客・在庫など）はどこに保存されているか	感染時にどこが影響を受けるか判断できない
2	バックアップを最後に取得したのはいつか。自動か手動か	担当者が変わると止まる。直近の状態に戻せない

#	確認すること	答えられないときのリスク
3	バックアップから実際にデータを復元できるか、過去に試したことがあるか	バックアップが壊れていて戻せないケースがある
4	バックアップは業務PCやサーバーと常時接続されていないストレージに保存されているか	感染端末と同期していると、バックアップも暗号化される
5	バックアップ設定を管理しているのは誰か。その担当者が不在でも確認できる状態か	属人化によりバックアップが止まっていても誰も気づかない

バックアップ自動化を進める3つのステップ

ステップ1：何がどこにあるかを整理する

受注・顧客・経理などの業務データの保存場所を一覧化します。担当者の頭の中だけにある状態では、その人が不在のときに動けません。

ステップ2：バックアップを自動化する

- ・頻度：日中に受注・出荷が動くシステムなら、少なくとも日次の自動バックアップが目安
- ・世代管理：過去7日分など複数世代を保持し、感染に気づかず上書きされるリスクを減らす
- ・保存先の分離：業務PCやサーバーと常時接続されていないクラウドストレージや外部メディアに保存する

ステップ3：定期的に「戻せること」を確認する

四半期に1回など定期的に復元テストを行い、バックアップが正常に完了したかを自動メール通知で確認する手順を決めておきます。

株式会社DnDは、バックアップとセキュリティ対策を標準で組み込んだシステム開発を行うDX/AX（AIによる業務変革）パートナーです。業務データの保存場所整理から、バックアップ自動化・復元確認の仕組み設計まで対応しています。

お問い合わせ・ご相談（無料）：<https://dnd-inc.jp/contact.html>