ランサムウェアとは？最新手口・実例・対策を初心者向けにやさしく解説【2025年版】

ランサムウェア詐欺（データ人質ウイルス）とは

ランサムウェアとは、パソコンやスマホのデータを勝手に暗号化して使えなくするウイルスのことです。
犯人は「元に戻したければお金を払え」と要求します。これが「データ人質ウイルス」と呼ばれる理由です。

感染すると写真や仕事の資料など、大切なデータに一切アクセスできなくなります。
企業だけでなく、個人のパソコンやスマホも狙われているため、誰もが注意が必要です。

ランサムウェア詐欺の最新手口（2025年版）

近年のランサムウェアは、より巧妙で見抜きにくくなっています。
ここでは代表的な手口を紹介します。

【不審メールによる感染】
「請求書を確認してください」「荷物の再配達」などのメールに添付されたファイルを開くと感染します。
正規企業を装ったメールでも、送信元アドレスをよく見ると不自然な場合があります。
見慣れない差出人の添付ファイルは開かないようにしましょう。

【偽の警告画面に誘導される詐欺】
「ウイルスに感染しました！」「サポートに連絡してください」といった偽の警告が突然表示され、
電話やリンクをクリックさせようとする手口です。
実際には感染しておらず、電話をすると金銭を要求されるケースもあります。

【ソフトの弱点（脆弱性）を悪用する攻撃】
パソコンやスマホのOS、アプリの更新が止まっていると、その弱点を突かれる可能性があります。
定期的なアップデートを忘れずに行うことが大切です。

【二重恐喝（ダブルエクストーション）】
最近では「データを暗号化する」だけでなく、「盗んだデータを公開すると脅す」二重恐喝も増えています。
支払ってもデータが戻らないケースが多く、非常に危険です。

ランサムウェア被害の実例

実際に発生した被害事例をいくつか紹介します。

【医療機関での事例】
病院では電子カルテを含む患者データが暗号化され、システムが停止しました。

その結果、救急を含む新規受け入れが中断され、地域医療に大きな影響が出ました。
この事件をきっかけに、バックアップ体制の重要性が改めて見直されています。

【企業での事例】
ある企業では、社員が受け取ったメールの添付ファイルを開いたことで感染しました。
社内サーバーが暗号化され、業務が数日間ストップ。復旧に多額のコストと時間がかかりました。

【個人ユーザーの事例】
個人のパソコンでも「無料ソフトのダウンロード」から感染するケースがあります。
データを失ったうえに、身代金を支払っても復旧できなかった例も少なくありません。

ランサムウェア詐欺への対策｜日常でできる予防策

【OSやアプリを常に最新の状態に】
通知が来たらすぐにアップデートしましょう。
これだけで多くの攻撃を未然に防げます。
古いOSを使い続けるのはとても危険です。

【不審メールやリンクを開かない】
知らない差出人のメールは開かず、添付ファイルは絶対に実行しないこと。
また、メール本文のリンクも安易にクリックしないようにしましょう。

【定期的にバックアップを取る】
重要なデータは、外付けハードディスクやクラウドに定期的に保存しましょう。
バックアップを取っていれば、たとえ感染してもデータを取り戻せます。

【セキュリティソフトを導入する】
信頼できるセキュリティソフトを使い、常に最新状態を保つことで感染リスクを大きく減らせます。

被害にあった場合の対応

万が一感染してしまった場合は、次の手順を落ち着いて実行しましょう。

1. ネットワークを切断する。
感染拡大を防ぐため、Wi-FiやLANケーブルを外します。

2. 警察や専門機関に相談する。
自分で解決しようとせず、専門家の指示を受けるのが安全です。

3. 身代金は絶対に支払わない。
支払ってもデータが戻らないケースがほとんどです。

4. バックアップから復旧を試みる。
感染前のデータを保存していれば、そこから復旧できます。

まとめ｜今日からできる小さな対策を続けよう

ランサムウェアの被害は、誰にでも起こり得ます。
しかし、日頃の意識と対策で防げるケースがほとんどです。

・OSやアプリを最新に保つ
・不審メールを開かない
・定期的にバックアップを取る

この3つを習慣にするだけで、被害の可能性は大きく下がります。
今日からできる小さな対策で、あなたの大切なデータを守りましょう。

参考文献

・警察庁「ランサムウェア被害防止のために」

・独立行政法人 情報処理推進機構（IPA）「セキュリティセンター最新情報」

・内閣サイバーセキュリティセンター（NISC）公式サイト

・JPCERT/CC 脅威情報データベース