S&J

インシデント0に、本気。

サイバー攻撃後、早期復旧

できる企業

できない企業

その違いとは？

ー早期復旧を実現する3つの準備ー

サイバー攻撃対策のゴールは「攻撃を防ぐこと」だけではありません

多くの企業では、EDRの導入やバックアップの取得など、サイバー攻撃に備えた対策を進めています。

一方で、実際に被害を受けた場合にどのような対応が必要になるのか、どの程度の期間で復旧できるのか、事業を継続しながら対応できるのかまで確認できている企業は多くありません。

サイバー攻撃による被害は、攻撃そのものだけでなく、その後の復旧対応によって事業への影響が大きく変わります。

本資料では、実際の事例をもとに、サイバー攻撃後の早期復旧を実現するために必要な考え方や備えについて解説します。

目次

＜掲載内容について＞
本資料は、2026 年 8 月時点の自社調査情報に基づいて作成しています。
記載内容は予告なく変更される場合があります。※表紙画像は生成 AI を活用して制作しています。

約10日で業務再開を実現した事例として大きな注目を集めた

2026年7月、大手食品・物流企業はサイバー攻撃によるシステム障害を公表しました。物流や出荷業務に影響が発生し、多数の取引先へ波及する事態となりましたが、安全性を確認しながら**約10日で業務再開へと移行**しました。

タイムライン

第１報　7月13日

不正アクセスによるシステム障害が発生し、食品出荷業務等に影響が生じていると発表
(後に複数のメディアにより、障害は06:50頃に社内システム部門が異常を検知し、同日中にシステムの遮断措置を実施したと報じられている)

第２報　7月15日

個人情報漏洩の可能性があること、食品出荷業務などは7月17日より再開予定と発表

第３報　7月17日

受発注を一部制限したうえで、冷蔵倉庫及び食品工場の部分稼働再開

犯行声明　7月21日

ランサムウェア攻撃グループRansomHouseが犯行声明を公開

第４報　7月22日

システム障害の影響を受けていた入出庫業務および冷凍食品出荷業務について、今週中に全拠点が通常稼働に移行する予定と発表

第５報　7月24日

顧客および取引先各社からの受発注制限を解除し、全拠点で平常時の通常稼働に移行したことを発表

なぜ、約10日で復旧することができたのか？

注目されたのは攻撃ではなく「復旧の速さ」

サイバー攻撃の被害を受けた企業の中には、復旧まで数週間から数か月を要するケースもあります。そうした中で、この事例が注目を集めた理由は、約10日という比較的短期間で業務再開に至った点にあります。

公表情報や各種報道によると、バックアップの活用や迅速な初動対応、影響範囲を見極めながらの段階的な業務再開に向けた取り組みが行われていた可能性がうかがえます。

一方で、一般的にこうした早期復旧はバックアップだけで実現できるものではありません。実際には、**データを復元できる環境や迅速に判断できる体制、関係部署との連携、平時からの準備があって初めて実現できるものです。**

つまり、この事例が示しているのは「バックアップの重要性」だけではありません。
重要なのは、攻撃を受けても早期復旧できる状態を平時から整えておくことです。

本編は以下のお役立ち資料ページから
ダウンロードいただけます。

https://www.sandj.co.jp/download/