

防御の限界——防げなかった後で何をするか | サイバー攻撃が示した物流停止と事業継続

Published: 2025-10-21 / Updated: 2026-07-15

Summary

加工食品・低温物流大手のサイバー攻撃事案では、システム遮断が冷蔵倉庫の入出庫と冷凍食品の出荷に影響し、外食・小売へ波及しました。本記事は、完全防御が困難な前提で、検知、遮断、証跡保全、代替運用、安全確認、段階復旧を業務単位で設計する考え方を整理します。データの復元だけではなく、認証、端末、ネットワーク、現場設備、人員、取引先接続が安全に戻る事が業務再開条件です。

Key Points

- サイバー攻撃への防御が破られたとき、最優先は被害拡大の阻止です。しかしシステムを遮断すれば業務も止まります。したがって、侵入防止だけでなく、どこまで止めるか、停止中に何を残すか、誰が再開を判断するかを、WMS・ERP・認証・通信・電源・人員まで含む業務単位で事前に設計します。
- 冷蔵倉庫の入出庫業務と冷凍食品出荷への影響
- サイバー攻撃確認とグループシステム遮断措置

Sources / References

Company-primary-source

加工食品・低温物流大手「システム障害発生について」

URL: <https://www.nichirei.co.jp/news/2026/482.html>

同「システム障害発生について（第2報）」

URL: <https://www.nichirei.co.jp/news/2026/483.html>

Source Article

<https://www.ieee802.co.jp/articles/article-003-antiransom.php>

© Kei Communication Technology Inc.

This document is a summary of the source article. For the latest information, refer to the source URL.