ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●冷凍食品大手にサイバー攻撃、取引先各社への出荷に影響

https://www.itmedia.co.jp/news/articles/2607/17/news099.html
https://www.nichirei.co.jp/news/2026/512.html
https://www.nichirei.co.jp/news/2026/513.html
https://www.nichirei.co.jp/news/2026/514.html
https://piyolog.hatenadiary.jp/entry/2026/07/16/022032

このニュースをザックリ言うと･･･

- 7月13日(日本時間)、冷凍食品大手のニチレイより、同社グループのシステムが不正アクセスを受け、障害が発生していると発表されました。

- 障害により、ニチレイロジグループ各社冷蔵倉庫の入出庫業務・ニチレイフーズ冷凍食品出荷業務に影響が生じており、大手外食チェーンや小売店等、低温物流業務における5,000社近くの取引先において商品の欠品が発生する事態となっています。

- また個人情報・顧客データの流出は未確認ながら、被害を受けたサーバーの一部に個人情報が保管されていたことから、個人情報保護委員会へ漏洩の可能性がある事案として報告したとのことです。

- 17日には冷蔵倉庫・食品工場の部分稼働による一部業務を再開、翌週中を目途に正常化を目指すとしています。

AUS便りからの所感等

- 大手企業へのサイバー攻撃で取引先にも物流面での影響が及ぶケースは、昨年9月にアサヒホールディングス、10月にアスクルで発生しています。

- 前述の事例と同様のランサムウェアによる攻撃だったのか等、今回の事案における侵入経路や被害規模等は未発表ですが、それらの事例と比べても一週間以内に一部業務の再開までこぎつけた点は、如何なる防衛体制の構築によるものかという発表があるかについても注目されます。

- ともあれ一連のサイバー攻撃で多く使われる侵入経路である「VPN機器からの侵入」「リモートデスクトップからの侵入」等の呼び水となる未修正の脆弱性の悪用・脆弱なアカウントへの不正ログイン・マルウェア感染等への対策を、各サーバー・クライアント・ネットワーク機器に至るまで実施し、それでも感染や侵入が発生した箇所からの攻撃の展開を遮断すべく、UTM等を組み合わせた適切なネットワークの分割・隔離、およびシステム・データの早期復旧のためのバックアップ実施等を行うのが望まれるところです。

ITmedia NEWS

ニチレイ、システム障害の業務を順次再開　全面復旧は来週中めど

2026年07月17日 16時21分 公開　[林裕也，ITmedia]

ニチレイ（東京都中央区）は7月17日、サイバー攻撃の影響を受けていた業務を、同日から順次再開したと発表した。顧客や取引先からの受発注を一部制限した上で、冷蔵倉庫と食品工場の部分稼働を始めている。

2026年7月17日

各位

株式会社ニチレイ

当社グループでのシステム障害発生について（第3報）

株式会社ニチレイ（本社：東京都中央区、代表取締役社長(CEO)：嶋本和訓）は、サイバー攻撃により発生したシステム障害の影響を受けていた業務について、本日より順次開始しました。
現在、お客さまおよびお取引先さまからの受発注を、一部制限したうえで、冷蔵倉庫及び食品工場の部分稼働を行っています。
なお、来週中を目指し全拠点での通常稼働に向けた準備を進めています。

＜今回影響を受けた業務＞
・ニチレイロジグループ各社 冷蔵倉庫の入出庫業務
・ニチレイフーズ 冷凍食品出荷業務

当社は、発生当日よりシステムの遮断措置を講じ、緊急対策本部を設置のうえ、外部のセキュリティ専門会社支援のもと、調査および対応を進めてまいりました。
本日より、冷蔵倉庫全拠点の入出庫業務および冷凍食品出荷業務について順次、開始しています。

なお、本件に関する原因および影響範囲については引き続き調査を進めております。

お客さまおよびお取引先の皆さまにご迷惑をおかけしておりますことを、お詫び申し上げます。

＜報道関係者問い合わせ窓口＞
株式会社ニチレイ　広報部
MAIL：N1000X036@nichirei.co.jp
TEL：03-3248-2235

以上

ニチレイの発表（出典：プレスリリースより）

障害の影響を受けていたのは、物流子会社ニチレイロジグループ各社による冷蔵倉庫の入出庫業務と、ニチレイフーズの冷凍食品出荷業務。冷蔵倉庫は全拠点で入出庫を順次再開しており、来週中に全拠点での通常稼働再開を目指す。

●2か月連続で過去最多規模の修正…MS、7月の月例セキュリティアップデート

https://forest.watch.impress.co.jp/docs/news/2125154.html
https://www.microsoft.com/en-us/msrc/blog/2026/07/202607-security-update
https://forest.watch.impress.co.jp/docs/news/2125160.html
https://forest.watch.impress.co.jp/docs/news/2125161.html

このニュースをザックリ言うと・・・

- 7月15日(日本時間)、マイクロソフト(以下・MS)より、Windows・Office等同社製品に対する月例のセキュリティアップデートがリリースされています。
- Windowsの最新バージョンはWindows 11 24H2・25H2 KB5101650(ビルド 26100.8875・26200.8875)および11 26H1(一部機種で使用) KB5101649(ビルド 28000.2525)等となります。
- 修正された脆弱点は622件とされ、過去最多とされた6月の208件の3倍近くとなっています。

AUS便りからの所感

- MS製品で修正された脆弱点のうち、Active Directory フェデレーションサービス(AD FS)とSharePoint Serverに関する計2件が既に悪用を確認、BitLockerのセキュリティ機能バイパスの問題についてが攻撃手法公開済み、Windows・Office・SharePoint・Copilot等計62件について、危険度が4段階中最高の「Critical」と評価されています。
- 同日にはAdobe社からも月例のセキュリティアップデート、この他翌週22日にはOracle社からJava等について四半期毎のアップデートリリースが予定されており、このような定期的アップデートのスケジュールについて、特にシステム管理者においては忘れず意識し、OS・機器のファームウェアから各種アプリケーションに至るまで脆弱性への根本的対策としてのアップデートの適用を必須とし、加えてアンチウイルス・UTM等による多重防御策により、適用前の脆弱性への攻撃に備えるようにしてください。
- またChrome 150.0.7871.124/.125、Firefox 152.0.6のように各ブラウザーもほぼ毎週セキュリティ修正を含むアップデートが行われていますが、6月には数百件に上る脆弱点が一度に修正されたこともあり、日々ブラウザーを起動した直後に「Chromeについて」等を開いて確認するぐらいの頻度でアップデートを適用する習慣をとることを強く推奨致します。

Impress Watch


Microsoft、2026年7月の「Windows Update」 ～脆弱性は過去最多の約3倍で622件、「緊急」だけでも62件
悪用されているものも存在、OSやOffice、SharePoint、Exchange、Copilotなどに影響
楠井 秀人　2026年7月15日 09:08
Windows Update
再起動が必要です
お使いのデバイスは、アクティブ時間外に再起動されます。
悪意のあるソフトウェアの削除ツール x64 - v5.143 (KB890830)
2026-07 .NET Framework セキュリティ パッチ (KB5100998)
2026-07 .NET 9.0.18 Security Update for x64 Client (KB5104033)
2026-07 セキュリティ パッチ (KB5101650) (26200.8875)
Microsoft Defender Antivirus のセキュリティ インテリジェンス更新プログラム - KB2267602
Microsoft、2026年7月の「Windows Update」「Microsoft Update」を実施
米Microsoftは7月14日（現地時間）、すべてのサポート中バージョンのWindowsに対し月例のセキュリティ更新プログラムをリリースした（パッチチューズデー）。現在、「Windows Update」や「Microsoft Update カタログ」などから入手可能。

●県の防災メール配信サービス悪用か、迷惑メール13,000件以上が発信

https://www.yomiuri.co.jp/national/20260702-GYT1T00416/
https://www.pref.wakayama.lg.jp/prefg/011400/important_news.html

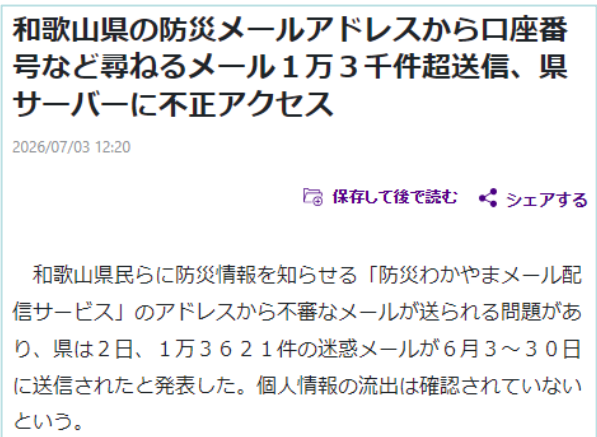
このニュースをザックリ言うと・・・

- 7月2日(日本時間)、和歌山県防災企画課より、同課が運営する「防災わかやまメール配信サービス」のメールアドレスから迷惑メールが外部に送信されていたと発表されました。
- 6月30日に外部からの情報提供により、登録受付用メールアドレスを送信元とした迷惑メールの発信が発覚したとしており、個人情報の流出はなかったとしています。
- 読売新聞では、県のサーバーが不正アクセスを受け、6月3日から30日において、13,621件の不審なメールが発信されたと報じています。

AUS便りからの所感

- 不審なメールの内容として「個人のLINE QRコードの送付依頼」「銀行口座情報の入力・返信依頼」が挙げられており、同県では、誤って送信したQRコードは更新・無効化すること等を呼び掛けています。
- 外部へのメール配信システムが攻撃されたと推測され、具体的な侵入の原因は不明ですが、配信システムからサーバー上のOS・その他アプリケーションまで常時最新バージョンに保つよう管理することが重要です。
- また過去には地方組織や大学等でメール送受信用サーバーが不正アクセスを受け、サーバーに保存されているメールを読み取られたりしたケースも度々報告されており、全てのメールアカウントについて簡単なパスワードを設定していないか、既に在籍していない従業員等のアカウントに依然ログイン可能な状態でないか等の確認を怠りなく実施すべきです。

YOL 讀賣新聞 オンライン


和歌山県の防災メールアドレスから口座番号など尋ねるメール１万３千件超送信、県サーバーに不正アクセス
2026/07/03 12:20
保存して後で読む　シェアする
和歌山県民らに防災情報を知らせる「防災わかやまメール配信サービス」のアドレスから不審なメールが送られる問題があり、県は２日、１万３６２１件の迷惑メールが６月３～３０日に送信されたと発表した。個人情報の流出は確認されていないという。