キーマンズネット

第 10 回：システムが止まった　その 1 週間、情シスは何をしていたのか？

2026 年、複数の企業でシステムが遮断され、冷凍食品の出荷もタクシーの配車も止まった。復旧まで 1 週間を要したケースもある。2025 年の重大インシデント 12 事例と照らし合わせると、繰り返される障害に共通する構造が浮かび上がる。シリーズの締めとして、最悪の事態を想定して読む 1 冊。

2025 年のインシデントを振り返る

2025 年、国内セキュリティ事件 12 事例を全検証 なぜあの企業の防御は突破されたのか？

2025 年はアスクルやアサヒへの攻撃をはじめ、幅広い業種で深刻なサイバー被害が相次いだ。主な原因は脆弱性の放置や海外拠点の管理不備、多要素認証の未導入にあり、サプライチェーンを介した二次被害も深刻化した。脆弱性管理の徹底や特権 ID の厳格化など、包括的な防御体制の構築が急務だ。

2025 年は、アスクルやアサヒホールディングス（以下、アサヒ）への大規模なランサムウェア攻撃をはじめ、企業の事業継続を脅かすサイバーインシデントが相次いだ 1 年だった。被害は単一の企業にとどまらず、取引先や顧客へと波及し、サイバーリスクが経営上の重要課題であることを改めて浮き彫りにした。本稿では、2025 年に国内で発生した 12 件のセキュリティインシデントとその被害状況を整理し、そこから見えてきた課題を解説する。

国内 12 事例の失敗学、なぜあの企業の防御は破られたのか？

2025 年 9 月以降に発生したアスクルとアサヒのセキュリティインシデントは大きな注目を集めたが、企業を狙ったサイバー攻撃はそれだけではない。被害は多様な業界に広がっている。本稿では注目事例以外のインシデントについても掘り下げ、2025 年に起きたセキュリティ事故の詳細と原因について、金融業や製造業、小売業、食品業界など業界別に整理する。

以下では業種別に被害が大きかった事例を中心に紹介する。まずは金融業だ。金融庁の監督があること、2014 年には金融 ISAC が設立されており、サイバーセキュリティ脅威に関する情報を 400 社以上が共有・分析できていることなどから金融業はサイバーセキュリティにおいて最も先進的だと言われている。

それにもかかわらず事件は起きてしまった。

証券 10 社の顧客口座が侵害

2025 年 1〜5 月には主要な証券会社のうち 10 社程度の顧客口座が相次いで侵害されて、巨額の不正取引が起きてしまった。2025 年 6 月になって金融庁が被害状況を公開している。

被害の規模は最大級だ。不正取引の総額は約 5240 億円で、被害件数は約 5958 件と巨大で、社会的信用の低下はもちろん、証券会社各社は多額の補償対応を迫られた。

この事例ではクレデンシャルスタッフィングとフィッシングを使って、顧客がログイン時に使う認証情報を得た。他の Web サイトで漏えいした ID やパスワードの使い回しが、今回の悪用につながった。証券会社側は顧客用フロントエンドシステムに侵入され、社内の基幹システムへの侵入はないが、顧客の資産が不正な売買や送金に悪用されたことが大きい。

この事例から分かることは対顧客でWebによる取り引きを進めている企業は認証プロセスを強化しなければならないということだ。証券会社各社も顧客への多要素認証を義務化した他、普段と異なるIPやWebブラウザを使った不自然なログインの検知やブロックを強化した。

個人情報が大量流出した損害保険ジャパン

個人情報の大量流出を招いた事例としては損害保険ジャパンの事例が挙がる。

2025年4月に同社が被害に遭ったことを公開し、2025年6月に被害範囲の拡大を公表した。被害の規模は極めて大きく、氏名と連絡先、証券番号がそろった個人情報約337万件以上が外部から閲覧可能だった可能性があった。この他を含めると最大1700万件以上が漏えいした可能性がある。このため金融庁の行政指導の対象となり、社会的信用が大幅に低下したと言われている。

サイバー攻撃の種類は標的型攻撃だ。外部に公開されているサーバの脆弱（ぜいじゃく）性、または不正に入手された管理者の認証情報が狙われた。特定の業務サーバから、本来アクセス権限がないはずのバックアップデータが格納されたストレージ領域まで攻撃が進行したことで情報漏えいを招いた。

この事例から分かることは、計画的な脆弱性診断とパッチ適用が欠かせないことと、情報漏えいに備えてデータを暗号化すること、特権IDをいつどこで使ったのかをリアルタイムで監視したり、制御したりしなければならないことだ。

金融機関が使う機器へサプライチェーン攻撃

少し毛色が違う攻撃もあった。金融機関を狙ったサプライチェーン攻撃だ。金融機関では紙幣や硬貨の計数、選別、収納などのために高さ1m程度の専用機器を利用している。この分野では企業としてローレルバンクマシンのシェアが最も高く、数万台が窓口やバックオフィスで使われている。ここを狙われた。

2025年9月にローレルバンクマシンのデータ保存用サーバが狙われた。クラウドサービス「Jijilla」の脆弱性を突いた不正アクセスだった。このとき、身代金も要求されている。この攻撃で委託先のデータが流出して二次被害が広がり、2025年11月以降、同社のAI-OCRサービスなどを利用していたみずほ証券や丸三証券、第一フロンティア生命保険など多数の金融機関の顧客情報が漏えいした。

この事例から分かることは自社のセキュリティだけでなく、委託先のセキュリティを監査しなければならないこと、もう一つ、クラウドサービスの設定ミスを検知するCSPM（クラウドセキュリティ体制管理）を導入しなければならないことだ。

「製造ラインが止まる」では済まない、国内メーカー2社の流出事案

次は製造業だ。ものづくり日本を支える製造業は全国に34万社もある。攻撃側としては製造ラインを1つ止めるだけで損失が発生するため身代金を要求しやすく、設計図や技術データを盗み出すことでも金銭を獲得できる。また、ITと比べてOT（運用技術）システムのセキュリティ対策が遅れており、レガシーシステムが多数残っているにもかかわらず、不用意なDXでITとOTの連携が増えて攻撃面が拡大していることだ。アサヒの事例もここに含まれる。

Tier1 の矢崎総業が狙われた

日本の製造業の 2 割を占めるのが自動車産業だ。機密データを狙う攻撃は自動車産業も狙ってきた。

被害に遭ったのは矢崎総業だ。同社は自動車産業で Tier1 サプライヤーの位置にあり、自動車メーカーにワイヤーハーネスや計器などを直接供給している。

同社を狙った二重脅迫型のランサムウェア攻撃は 2025 年 7 月ごろに始まり、身代金 1000 万ドルが要求されたという。2025 年 12 月には攻撃者がダーク Web で 350GB の機密データを盗み出したと宣言した。このデータには設計図や取引先情報、契約書などが含まれると攻撃者は主張しており、自動車メーカーへの部品供給遅延があるのではないかと不安を呼んでいる。

この攻撃では公式には不正な第三者がネットワークにアクセスしたとされている。ただし、攻撃者（INC Ransom）の過去の攻撃パターンから、同社の海外拠点の VPN 機器の脆弱性が悪用されたか、または流出した認証情報が使われたと考えられている。攻撃は海外拠点から始まり、国内の基幹システムへ侵入して、一部のファイルサーバを暗号化した他、全社的なバックオフィス業務にまで影響が広がった。

この事例から分かることは損害保険ジャパンの事例と同様に、計画的な脆弱性診断とパッチ適用が必要なこと、海外を含む全拠点で多要素認証を義務化しなければならないこと、拠点間ネットワークを分離してマイクロセグメンテーション化しなければならないことだ。

エンジン部品の美濃工業も狙われた

Tier1 メーカーに部品を納入する Tier2 メーカーも狙われている。エンジンなどに使うアルミダイカスト部品に強みがある美濃工業が大規模なランサムウェア攻撃を受けた。

2025 年 10 月 4 日に攻撃に遭ったことが公開された。全体像が徐々に明らかになる中で、300GB 以上のデータが流出し、ダーク Web に顧客情報が掲載されてしまった。同時に出荷や受発注業務が遅延した。

この攻撃では社員用の VPN アカウントを悪用して、正規の ID とパスワードで突破した。侵入からわずか 1 時間で管理者権限を奪取されてしまい、その後数日かけて社内を横展開して、サーバを初期化したりファイルを暗号化したりした。

この攻撃から分かることは、多要素認証の導入が欠かせないこと、不審なログインを監視しなければならないことだ。

なぜ EDR は止められ、バックアップは消されたのか？　小売業の被害事例

日本で最も企業の数が多いのは小売業だ。全企業の 7 社に 1 社が小売業だ。小売業でもサイバー攻撃が目立った。

アスクルへの攻撃は他社にも波及した

アスクルへのサイバー攻撃は日本の物流インフラを揺るがす甚大な被害をもたらした。同社は全国に翌日配送が可能な物流網に強みがある。これが物流インフラに多大な影響を与える下地になった。

ランサムウェア攻撃が起きたことが分かったのは2025年10月19日だ。2025年12月時点でも完全な復旧には至っていない。このため2025年11月度の売上高は、法人向けサービスで前年同月比95%減という大打撃を受けた。加えて合計で約73万9000件の情報漏えいが確認されている。漏えい内容は顧客からの問い合わせ内容が中心だ。同社への攻撃の影響が大きくなったのは他社の物流を受託していたからだ。無印良品やロフト、そごう、西武百貨店、ネスレ日本などに影響が波及した。他社のオンライン注文や出荷の遅延や停止を招いた。

アスクルへの攻撃は、業務委託先の管理アカウント奪取から始まった。多要素認証が導入されていなかった業務委託先の管理者アカウントが突破口となった。IDとパスワードが何らかの形で漏えい、悪用されたことが侵入の原因だと推定されている。その後ランサムウェア攻撃が始まった。単一のマルウェアではなく、検知を逃れるために複数種類が組み合わされて使用された。侵入後、攻撃者はネットワーク内を横移動して、より高い権限を奪取した。その後、管理者権限を悪用して同社で導入されていたEDRなどのセキュリティソフトを強制的に停止させた。システム復旧を困難にするために、ネットワーク接続されていたバックアップデータも削除・暗号化された。データを暗号化するだけでなく、情報を盗み出して公開すると脅す二重脅迫が実行されて攻撃グループが犯行声明を出している。

つまりアスクルへの攻撃は今回取り上げたさまざまな事例の中でも特に悪質だったことになる。この攻撃から分かることは、多要素認証を導入するときに例外を設けてはいけないということだ。EDRの抜け漏れも怖い。バックアップを取る場合にイミュータブル（不変）でなければならないということだ。攻撃者が削除できない隔離された環境や、書き換え不能な形式でバックアップを保存する必要がある。加えて特権IDの管理を強化して使用を厳格に制限し、常用させない運用が求められる。

駿河屋のECサイトが改ざんされた

小売業を狙う特徴的な攻撃手法はECサイトの改ざんだ。偽のECサイトを立ち上げ、購入者が自分の情報を入力することを狙う。

＊IPAが2025年6月に公開した「情報セキュリティ10大脅威2025個人編」でも「ウェブスキミング　ECサイト（ショッピングサイト）の脆弱性を悪用し正規Webサイトの決済画面を改ざんする。利用者が改ざんされた決済画面にクレジットカード情報を入力してしまうと攻撃者にその情報を詐取される」と解説している。
https://www.ipa.go.jp/security/10threats/eid2eo0000005231-att/kaisetsu_2025_kojin.pdf

この手法で被害を受けたのが全国で140店舗以上を展開し、中古品の買い取り、販売に強みがある駿河屋だ。

同社は2025年7月23日に侵害を検知後、同年8月4日に決済ページの改ざんが発覚、同日中に決済システムを修正した。2万9932人分の個人情報と3万431件のクレジットカード情報が漏えいした可能性がある。約4カ月にわたってカード決済機能が停止したため、売上が減少し、社会的信用が低下した。

攻撃の手法はJavaScript改ざんによるWebスキミングだ。同社の監視ツールには脆弱性があった。社外からサーバを管理・監視するための監視ツールに残っていた欠陥を突かれた。この監視ツール経由でWebサーバに侵入されて、決済画面のプログラムが書き換えられて、購入者のクレジットカード情報などの入力データが外部に自動送信される設定になっていた。

この攻撃では検知から対策完了まで数週間のタイムラグがあり、その間も情報が盗まれ続けた。対策としてはこのような監視ツールを含む管理用ソフトウェアを最新の状態に保つこと、Web サイト向けのファイル改ざん検知システムを導入すること、WAF（Web アプリケーションファイアウォール）を導入することだ。

スーパー全店舗が臨時休業に

EC サイトとは無関係に、小売店が狙われた事例もある。大分県内で 23 店舗を構える中規模スーパーのトキハインダストリーだ。

2025 年 3 月 31 日にランサムウェア攻撃が発覚し、全店舗が臨時休業に追い込まれた。幸いにも 2025 年 4 月 1 日には営業を再開できた。

この攻撃では同社グループ共通のサーバの脆弱性を悪用されたか、または認証情報を窃取されたことでサイバー攻撃を招いた。店舗のレジと連携するシステムがダウンしてしまい、決済システムが動かず店舗の営業ができなくなった。

この攻撃から分かることは、バックアップのオフライン保管（加えてイミュータブルバックアップを導入すること）が欠かせないこと、店舗ネットワークと基幹ネットワークを論理的に分離すること、BCP（事業継続計画）にランサムウェア攻撃を含めることだ。

アサヒビールが店頭から消えた

食料品業界の事例では、アサヒへのサイバー攻撃が 2025 年では最大だ。国内の飲料・食品インフラに極めて大きな影響を及ぼした。アサヒスーパードライなどの出荷が止まり、店頭在庫がなくなって「アサヒの××の入荷は未定です」という張り紙があちこちで目立ったほどだ。完全な正常化は 2026 年 2 月を予定している。

2025 年 9 月 29 日ごろ、まず同社でシステム障害が発生した。調査する中でファイルが暗号化されていることを確認したため、同日に被害拡大防止のためネットワークを遮断した。なお、攻撃者は侵入直後に暗号化を実行せずに約 10 日間潜伏していたことも分かっている。

攻撃された原因はグループ拠点のネットワーク機器の脆弱性にあった。攻撃者はここからグループのデータセンターのネットワークへ入り込み、脆弱な認証情報を悪用して管理者権限を奪取したと分析されている。その後、認証サーバからランサムウェアを配信して、稼働中の複数のサーバと PC を一斉に暗号化した。これによって受注や出荷、在庫管理、メール、コールセンターなどの業務が全面的に停止した。国内の主要なビール工場・飲料工場での生産・出荷システムも停止した。

この他、約 150 万件の個人情報が流出した可能性があると発表された。

この事例から分かることは、ネットワーク機器の脆弱性管理が重要だということだ。本社だけでなく、拠点の機器を含めて計画的な脆弱性管理とパッチ適用が必要であり、サポートが終了した機器を使い続けないことも必要だ。多要素認証の全面導入も必要だ。それも操作の各段階で有効にしておく必要がある。ネットワークのセグメンテーションも有効だ。

止まない医療機関への攻撃　7 割が CISO 設置も被害止まらず

厚生労働省が全国の医療機関 8117 施設を調査した結果によれば、医療機関のセキュリティ意識は高い。CISO を設置している病院は有効回答のうち、73%に達している。JAHIS（保健医療福祉情報システム工業会）と JIRA（日本画像医療システム工業会）が策定したドキュメント「MDS」「SDS」に基づいてベンダーのセキュリティを評価していた率も 85%と高い。ただし、電子カルテシステムのバックアップも進んでいる。

＊「病院における医療情報システムのサイバーセキュリティ調査」、5842 施設から回答があった。
https://www.mhlw.go.jp/content/10808000/001522779.pdf

それでも、2025 年に複数の医療機関がサイバー攻撃を受けた。

徳島大学病院が狙われた

徳島大学病院は 2025 年 10 月 19 日ごろに外部からの不正アクセスを受けたことを確認し、同年 12 月 22 日に公表した。

患者 1 万 6945 名と職員約 2000 人の個人情報が漏えいした可能性がある。氏名だけでなく、医療検査結果や看護キャリア支援システムのデータも含まれていた。

攻撃対象になったのは管理サーバの脆弱性か、または認証情報の不正利用だ。外部から業務システムにアクセスされて、内部データを閲覧された。

この事例から分かることは、インターネット公開資産の管理（ASM）を導入、強化しなければならないことと、特権 ID の管理の厳格化だ。最後のとりでとして異常なデータエクスポートの監視も必要だ。

宇都宮では 30 万人分の個人情報が漏えいか

2025 年 2 月 10 日、栃木県の宇都宮セントラルクリニックがランサムウェア攻撃を受けたことが発覚した。同 2 月 18 日に情報漏えいの可能性を公表、2025 年 5 月 14 日には通常業務を再開できた。

最大約 30 万件の個人情報漏えい（氏名、生年月日、診療情報など）があった他、IT システムの停止によって、診察や健康診断業務が大幅に制限された。

ランサムウェアは VPN 機器か、外部接続アカウントの脆弱性を狙ったと考えられている。侵入された後、院内ネットワーク全体に拡大して、診療・検査系サーバが暗号化された。電子カルテを含むシステムが広範囲に停止した他、二次被害として連携する健康保険組合へも影響が波及してしまった。

この事例から分かることは、外部接続点に多要素認証を導入すること、不審な挙動を検知するために EDR を導入すること、ネットワークのセグメンテーションが必要だということだ。

広島市では私用 PC が原因の被害も

職員の私用 PC（BYOD）が原因になった不正アクセスの事例もある。2025 年 2 月に公表された広島市立北部医療センター安佐市民病院の事例だ。

この PC は院内ネットワークに接続されていた。ところがリモートアクセスツールが不明な人物によって仕込まれており、その結果、患者の情報約 5000 件が漏えいした可能性がある。なお、事件自体は 2024 年 10 月 9 日に発覚していた。

この事例から分かることは、私物デバイスの持ち込み制限を厳格化しなければならないこと、EDR などを用いたエンドポイントの可視化が必要なことだ。USB ポートの無効化も役立つだろう。

以上、12 の国内事例から、発生したサイバー攻撃の詳細と、防ぐための方法を紹介した。

複数の事例を横串にして考える際には、米国国立標準技術研究所（NIST）が公開した「サイバーセキュリティフレームワーク 2.0」（CSF）が役立つ。

・統治　サイバーセキュリティを事業戦略に統合

・識別　資産とリスクの把握、優先順位の決定

・防御　アクセス制御、データ保護、教育

・検知　異常の継続的監視

・対応　インシデント処理とコミュニケーション

・復旧　復旧計画と改善活動

アスクルの事例では特定、防御、検知に課題があり、アサヒでは特定、防御だった。

ソリューションとしては脆弱性対応や多要素認証、特権 ID 管理、EDR、ネットワーク分離、イミュータブルバックアップの導入があてはまる。2026 年に自社が多大な影響を受けないためにも、自社の弱点を把握して強化しなければならない。

初出	2025 年 12 月 26 日
執筆者	畑陽一郎（キーマンズネット）
連載	2025 年のインシデントを振り返る
URL	https://kn.itmedia.co.jp/kn/articles/2512/26/news088.html

キーマンズネット

ニチレイや日本交通でシステム遮断　冷凍食品の出荷もタクシーの配車も止まった 1 週間

7 月 13 日週は、サイバー攻撃を受けて冷凍食品の出荷やタクシーの配車受付が停止する事案が発生した。被害拡大を防ぐにはシステムの遮断が必要だが、その影響で業務を継続できなくなることもある。攻撃を防ぐだけでなく、システムを止めた後の業務継続についても備えが必要だ。

本稿では、2026 年 7 月 13 日〜7 月 17 日までに公表または更新された、国内の主なセキュリティインシデント情報を整理する。この期間には、サイバー攻撃によって物流や配車などの業務に影響が及んだ事案や、ランサムウェアへの感染が疑われる事案が相次いだ。

複数の事案では、被害拡大を防ぐためにサーバやネットワークを遮断している。サイバー攻撃による直接的な被害だけでなく、安全を確保するための遮断措置が業務停止につながる点にも注意が必要だ。

1. ニチレイ、サイバー攻撃で冷凍食品の出荷や冷蔵倉庫の入出庫に影響

食品大手のニチレイは 2026 年 7 月 13 日、同社グループで不正アクセスによるシステム障害が発生したと公表した。7 月 15 日には、調査の結果、同社のサーバがサイバー攻撃を受けたことを確認したと発表した。

同社は発生当日に緊急対策本部を設置し、顧客や取引先の個人情報、顧客データなどを保護するため、グループで使用するシステムを遮断した。この影響で、ニチレイロジグループ各社の冷蔵倉庫における入出庫業務と、ニチレイフーズの冷凍食品出荷業務に影響が生じた。

7 月 15 日の発表時点では、外部のセキュリティ専門会社と安全対策を講じた上で、7 月 17 日から順次、業務を再開する予定としていた。サイバー攻撃の詳しい内容については、さらなる被害の拡大を防ぐためとして公表していない。

調査では、被害を受けたサーバの一部に個人情報が保管されていたことも判明した。同社は「漏えいの可能性がある事案」として個人情報保護委員会に報告した。情報が実際に漏えいしたかどうかは調査中で、漏えいが判明した場合には関係各所に報告するとしている。

出典：当社グループでのシステム障害発生について（第 2 報）（ニチレイ）　https://www.nichirei.co.jp/news/2026/513.html

2. 日本交通、マルウェア感染で電話によるタクシー配車を停止

タクシー・ハイヤー事業を手掛ける日本交通は 2026 年 7 月 13 日、社内システムが外部から不正アクセスを受け、マルウェアに感染したと公表した。不正アクセスが発生したのは 7 月 11 日未明だという。

同社は不正アクセスの検知後、被害拡大を防ぐためにシステムを遮断した。この影響で、ハイヤーの Web 受注・予約管理システム、電話によるタクシー配車サービス、一部の社内向けシステムなどが一時的に利用できなくなった。

電話による配車を停止している間、同社は利用者に対し、タクシー配車アプリ「GO」やタクシー乗り場、流しの車両を利用するよう案内した。陣痛タクシーに関する Web フォームからの登録も一時停止した。

日本交通は社内ネットワークを隔離し、外部のセキュリティ専門機関と影響範囲の特定、原因究明、ログの解析を進めている。7 月 13 日時点で情報漏えいの事実は確認されていないが、データ流出の有無やその範囲について調査を継続している。

出典：弊社システムへの不正アクセスによるシステム停止に関するお詫びとご報告（日本交通）　https://www.nihon-kotsu.co.jp/news/20260713-3334/

3. ファイブフォックス、本社サーバにランサムウェア感染の可能性

アパレル事業を手掛けるファイブフォックスは 2026 年 7 月 14 日、本社サーバの一部がランサムウェアに感染した可能性があると公表した。

同社は 7 月 8 日、通常のセキュリティ調査の過程でランサムウェアに感染した可能性を確認した。被害の拡大を防ぐため、直ちにサーバを停止し、インターネットやメール機能なども停止した。

同日中に対策本部を設置し、個人情報保護委員会に報告した。外部調査機関に被害状況の確認と調査を依頼し、警察にも協力を求めている。

顧客情報の流出を含む影響範囲は調査中としている。店舗は通常通り営業しており、オンラインストアについても別のシステムで運営しているため、本件による影響はないという。

出典：ランサムウェア感染の可能性に関するお知らせとお詫び（ファイブフォックス）
https://www.fivefoxes.co.jp/2026/07/post-20.html

4. 日産化学、システムへの不正アクセスを確認

化学メーカーの日産化学は 2026 年 7 月 16 日、同社システムに対する不正アクセス事案が発生したと公表した。

同社は 7 月 1 日にシステム上の不審な活動を検知した。調査を実施した結果、第三者による不正アクセスが行われていた可能性があることを確認した。

日産化学は事案の判明後、被害拡大と再発を防ぐため、対象システムに必要な対策を実施するとともに、監視体制を強化した。外部の専門家と原因や影響範囲の調査を続けている。

7 月 16 日時点では、顧客や取引先への影響は確認されていない。ただし、被害の全容把握には時間を要する見込みとしており、新たに公表すべき事実が判明した場合には速やかに知らせるとしている。

出典：当社システムに対する不正アクセスについて（日産化学）
https://www.nissanchem.co.jp/news_release/news/n2026_07_16.pdf

システムを遮断しても業務を続けられるか

今回取り上げた事案では、攻撃やマルウェア感染を確認した後、被害拡大を防ぐためにサーバやネットワークを遮断した例があった。その結果、ニチレイでは冷蔵倉庫の入出庫や冷凍食品の出荷、日本交通ではタクシーの電話配車やハイヤーの予約管理に影響が及んだ。

インシデント発生時にシステムを速やかに隔離することは、被害を抑えるために欠かせない。一方、基幹システムや業務システムを遮断すれば、攻撃を受けていない機能も含めて利用できなくなる場合がある。

情シス部門では、どのシステムを遮断すると、どの業務が停止するのかを事前に確認しておきたい。電話や紙、代替サービスなどを利用した暫定的な業務手順に加え、取引先や顧客への案内方法、業務を再開する際の判断基準も整理する必要がある。

また、システムを復旧できたとしても、安全性を確認しないままネットワークへ戻せば、攻撃者が残した侵入経路やマルウェアを通じて再び被害を受ける恐れがある。復旧の速さだけでなく、ログの調査や侵入経路の特定、認証情報の変更、ネットワークへ戻す前の安全確認まで含めた手順が必要だ。

初出	2026 年 7 月 24 日
執筆者	中村篤志（キーマンズネット）
URL	https://kn.itmedia.co.jp/kn/articles/2607/24/news004.html