

日本の不正アクセス・情報漏洩の統計と企業一覧

2026年10月2日に確認した公開資料に基づく初回統計版。

「最近、漏洩事故が増えた」と一括りにすると、件数の増加、1件の被害規模、委託先から複数企業への波及を混同する。公表統計では、2025年の上場企業等の漏洩・紛失事故は前年より減った一方、公表された延べ対象人数は約1.93倍に増えた。警察が把握したランサムウェア被害は2026年上半期123件で、前年同期116件から6.0%増えている。ただし、この2つの統計は対象が異なる。東京商工リサーチの2025年調査、警察庁の2026年上半期資料・本文9頁

引用に登場した企業・組織はすべて確認表に収録した。追加事案を含む台帳は32行・31の企業／組織表記からなり、漏洩または不正閲覧を確認した15行、漏洩の可能性14行、侵害確認・漏洩未確認2行、侵害確認・漏洩確定範囲不明1行に分けた。これは抽出事例の記述統計であり、日本全体の漏洩率や攻撃成功率の推計には使えない。1行が複数グループ会社や複数環境を含む場合もある。

資料は事案台帳、出典台帳、波及先・追加確認候補、調査履歴、集計用データに分けて保存した。出典の原文、取得日時、SHA256、検索・閲覧結果はevidenceに残した。

1. 全国の規模は、母集団を分けて読む

指標	対象期間	集計値	対象と限界
上場企業と子会社が公表した漏洩・紛失事故	2025年	180件・158社	非上場企業を網羅しない。可能性・紛失も含む
同調査の公表された延べ対象人数	2025年	30,636,910人分	同一人物の重複を除去した人数ではない。人数非開示70件を含む全件の総被害人数でもない
民間事業者等の漏洩等報告の処理	2025年度	17,139件	2025年4月～2026年3月。漏洩だけでなく滅失・毀損等を含む。サイバー攻撃件数ではない
警察へのランサムウェア被害報告	2025年	226件	警察が把握した企業・団体等の被害。漏洩確認件数とは異なる
警察へのランサムウェア被害報告	2026年上半期	123件	半期の集計開始以降最多。2026年通年へ単純に倍増換算しない

出典は東京商工リサーチ、個人情報保護委員会の令和7年度年次報告・第2章第4節と付表2、警察庁2025年資料・本文13頁、警察庁2026年上半期資料・本文9頁。

件数は微減でも、延べ対象規模は増えた

同じ調査内の比較	2024年	2025年	増減（本調査で計算）
公表事故件数	189件	180件	－4.8%
ウイルス感染・不正アクセスによる事故	114件	116件	＋1.8%
公表された延べ対象人数	15,865,611人分	30,636,910人分	＋93.1%

小数第1位に丸めた計算値を記載した。東京商工リサーチの公表文は事故件数の減少を4.7%と表記しているため、原文の表記と再計算値を混同しない。2025年調査

ランサムウェアの半期系列は、2024年上期114件・下期108件、2025年上期116件・下期110件、2026年上期123件である。直近の増加は確認できるが、2026年9月のニュースの多さだけから国内の全漏洩件数が何倍になったかは判断できない。警察庁・図表4

2. 「不正アクセスが何割か」も、母集団で変わる

東京商工リサーチの2025年公表事故180件では、ウイルス感染・不正アクセス116件、誤表示・誤送信37件、紛失・誤廃棄18件、不正持ち出し・盗難7件、不明・その他2件だった。ウイルス感染・不正アクセスは64.4%を占める。東京商工リサーチ・原因別図表

一方、個人情報保護委員会への直接報告13,345件の原因表では、不正アクセスは「報告者」533件、「委託先」328件、「不明」395件で計1,256件、9.4%となる。紙媒体のみの事案は10,263件、76.9%だった。どちらもこの13,345件が分母であり、委任先省庁分を含む17,139件を分母に置かない。年次報告・付表2（2）④⑤

この差は矛盾ではない。新聞や企業の公表を通じて見つけやすい大規模事案と、医療機関等の書類の誤交付まで含む行政への報告では、集まる事故が違う。年次報告の「不正の目的をもって行われたおそれ」22.3%も報告義務上の類型であり、上の原因別9.4%と同じ指標ではない。分類の意味を変えずに引用する必要がある。個人情報保護委員会・報告の処理状況と付表

3. どの業種が漏洩を公表したか

業種	2025年の公表企業数	158社に占める割合（再計算）
製造業	50社	31.6%
サービス業	23社	14.6%
情報通信業	21社	13.3%
金融・保険業	20社	12.7%
小売業	15社	9.5%
その他	29社	18.4%

東京商工リサーチの件数から再計算した。各業種の全企業数を分母にした被害率ではないため、「製造業が最も侵入されやすい」とは結論できない。大企業の顧客規模や公表慣行も観測件数に影響し得る。東京商工リサーチ・産業別

今回の事案台帳には、小売、交通・移動、物流、保険、出版、エンターテインメント、行政、クラウド・予約・採用管理などが入った。特に、利用者情報を多数の企業から預かるシステム提供会社の侵害を、利用企業自身への侵入と混同しないことが重要になる。

4. 引用された説明で修正する点

引用文の読み方	今回の確認結果
Gyazoの約2,362万件を利用者人数と読む	匿名ユーザー関連データを含む「件」。画像メタデータ約4.9億件等は別のデータ型。画像ファイルの流出件数とは異なる
ショップサーブの約885万件を885万人と読む	8,853,839件。複数登録を含み得るため、人数ではないと明記
セイコーマートを57万アカウントの可能性のまま扱う	保存した9月30日の第三報本文は572,022人分の不正閲覧確認。古い検索要約とは状態が異なる
ニチレイを障害・漏洩未確認のまま扱う	9月18日の第7報で漏洩を確認。配送先3,308件、取引先6,849件、従業員等43,709件
ベネフィット・ワンを不正アクセス被害に入れる	原因はプログラムの条件設定不備。他社担当者への情報提供を確認した事案で、攻撃ではない
KDDIを既知脆弱性の放置と扱う	侵入確認時点でベンダーも未認識だった脆弱性と公式説明
VOISINGの原因をMetabaseのCVEまで確定する	公式はBIツールの既知脆弱性を説明。製品名・CVEの対応付けはpiyologの推定として分離
ニッポンレンタカーを1件・96人とする	41名と55名は公式に別手法の事象と説明。対象者重複が不明なので合算しない

根拠はGyazo第二報、ショップサーブ第二報、セイコーマート第三報、ニチレイ第7報、ベネフィット・ワン公式PDF、KDDI訂正済み調査結果、VOISING第四報、piyologのVOISING分析、ニッポンレンタカー別事象の公表。

追加で調べたEPARKリラク&エステも、初報の約3,300万レコードを第二報で精査後約2,218万レコードに更新し、正確な人数への換算は困難と説明していた。続報を追うと、漏洩の確認状況だけでなく数値やデータ型も変わる。EPARK第二報

5. 原因の説明は、分かっている段階を分ける

今回の32行のうち、ソフトウェア脆弱性を企業・行政の一次資料で確認できたものは5行だった。対象はGyazo、GSS、VOISING、KDDI、ApplyNowである。「脆弱性が原因」と「攻撃前に修正できる既知脆弱性を放置」は同じではない。前者の5行から、後者の全国での割合は計算できない。

原因として確認した内容	台帳行数	判断できる範囲
ソフトウェア脆弱性	5	既知・未認識・公開時期不明をさらに区別する
アクセス制御・監視の課題	1	アフラックが説明した取得制限・検知の課題。初期侵入手順を確定する分類ではない
設定・認証情報の問題	1	集英社によるCMS設定とAPI認証情報の原因推定
ネットワーク機器経由・詳細未公表	1	日本テレネットの公表。VPN脆弱性と断定しない
プログラム不備・攻撃ではない	1	ベネフィット・ワン
侵入方法未公表／本調査で未検証	23	分からない原因をVPN・従業員端末・AIに割り当てない

この分類は「根本原因の相互排他的な学術分類」ではなく、公表された説明の粒度を残した手動分類である。原文の説明、分類理由、出典を台帳の各行に置いた。キーワード照合で原因判定した行は0行。

AIについても、今回の台帳から攻撃にAIを使った割合は計算できない。警察庁の資料には生成AIを悪用した国内事件の記述があるため、「公式確認がない」「AI攻撃は0件」とは書かない。ただし、それを今回の各社事案の攻撃者の手法へ転用する根拠はない。警察庁2025年資料・特集Ⅰ

追加分析：どこまで原因を説明できるか

「原因」は、攻撃者が最初に入った箇所、侵入を可能にした技術的な不備、大量取得や横展開を止められなかった条件に分けて読む。VPN経由、パスワード利用、ランサムウェア感染、委託先への侵害は、それぞれ別の段階・関係を示す。これらを1つの原因ランキングへ混ぜると、どの対策が必要かを判断できない。

原因の詳細台帳は全32行に入口、技術的成立要因、管理・運用、脆弱性の事前公開、認証・権限、原因説明の到達段階を記録した。「未確認」は、問題がなかったという意味ではない。原文の説明と手動判断を残し、推測で穴を埋めていない。原因集計データ

公表資料から説明できる段階	行数	32行に占める割合
技術的原因を公式が説明	6	18.8%
技術的原因を公式が推定	1	3.1%
制御・監視の弱点を公式が説明	1	3.1%
入口の機器種別まで公式が説明	1	3.1%
具体的原因の一次説明なし	21	65.6%
一次本文の追加検証が必要	2	6.3%

最初の6行は、脆弱性5行とベネフィット・ワンのプログラム不備1行。集英社は企業自身が原因を「考えます」と説明しているため推定に分けた。アフラックは大量照会の制御・監視不足を説明しているが、具体的な認証突破手順は明らかではな

い。日本テレネットはネットワーク機器経由と説明しているが、機種・脆弱性は非公表。対策の公表を、攻撃前に同じ対策が欠けていた証拠へ自動的に変換していない。

攻撃事案だけを分母にした比較

攻撃ではないベネフィット・ワンを除く31行では、脆弱性5行（16.1%）、設定・認証情報の問題の企業推定1行（3.2%）、制御・監視の課題1行（3.2%）、入口の機器種別のみ1行（3.2%）、具体的侵入方法の非公表・一次未検証23行（74.2%）となる。これは今回集めた公表事例内の構成であり、全国の原因割合ではない。原因の説明の粒度も異なるため、相互排他的な根本原因の推計として使わない。

漏洩・不正閲覧確認済みの攻撃14行だけに絞ると、脆弱性4行、設定・認証情報の企業推定1行、制御・監視の課題1行、非公表・一次未検証8行（57.1%）となる。漏洩確認済みに限定しても半数超の具体的侵入方法が分からず、「漏洩した企業は主に何を怠ったか」を全国へ一般化する材料には足りない。

脆弱性を悪用された5行の内訳

攻撃前に分かっていた範囲	行数	脆弱性5行に占める割合	対象
攻撃前に公開され、修正適用前に悪用	2	40.0%	GSS、VOISING
発覚時点でベンダー未認識	1	20.0%	KDDI
攻撃前の公開時期が不明	2	40.0%	Gyazo、ApplyNow

追加で確認したGSSのQ&Aは、攻撃前に脆弱性が公表され、修正プログラム適用前に悪用されたと説明している。当初の深刻度はMediumだったとも説明している。したがって、GSSは事前公開の有無が分からない分類から更新した。ただし、修正が間に合わなかった期間の日数や、管理者が意図的に放置したかは公表資料から判定していない。デジタル庁Q&A・原因について

VOISINGの修正適用の時間的課題と、KDDIのベンダー未認識の脆弱性は、同じ対策で事前に防げたと断定できない。40.0%は確認した脆弱性5行の内訳であり、「国内攻撃の40%がパッチ放置」とは読めない。VOISING第四報、KDDI調査結果

この台帳で分析できることと、追加データが必要なこと

公表事例内での原因別件数、漏洩確認状況とのクロス集計、原因情報が未確認である割合、脆弱性の事前公開の有無は分析できる。一方、「どの対策をすれば漏洩確率が何%下がるか」「どの業種が侵入されやすいか」「AIが攻撃成功率を上げたか」は、この事案台帳だけでは推定できない。被害を受けなかった企業の対策状況、対象企業数、観測期間、統一した技術調査結果が必要になる。

非公表の原因をすべて明らかにするには、企業や調査会社が保持するログ、構成、フォレンジック報告などの非公開資料が必要になる場合がある。まず公開された続報・調査結果で空欄を減らし、公開情報で解消できない欄はそのまま残す。

6. 委託先・共通システムから複数組織へ波及する

ショッピングサービスの事案では、PFUとキングジムが過去にそのサービスを利用していた顧客データの漏洩の可能性を公表した。現在のECサイトのシステムとは別であり、「現在もその企業の通販システムへ侵入された」とは読めない。PFUは最大169,355件の注文データを対象候補とし、人数ではないと説明している。PFU公表、キングジム公表

ApplyNowでは、吉野家4,998件、はなまる368件、両社の採用担当者等418件の公表を確認した。契約終了後に残っていた応募者情報も対象になっている。これらはApplyNow侵害の影響範囲であり、吉野家やはなまるのシステムが侵害されたという公表ではない。両社連名の公式PDF

宿泊予約のTEMAIRAZUでは、複数ホテルが予約情報を使った不審メッセージを告知した。提供元は不正アクセスを確認しているが、宿泊者情報の取得範囲と不審メッセージとの関係は調査中としている。漏洩確認済みのホテル総数や被害者人数は

置かない。手間いらず公式PDF

別表には、一次資料で本文を確認した波及先と、piyologから発見したホテル・自治体等の追加確認候補を収録した。候補行は「一次本文未照合」と明示し、漏洩確認済み企業数へ加算しない。施設名・ブランド名と法人名も同一単位として合計しない。波及先・候補一覧

7. 網羅性と解釈の限界

初回の網羅対象は、引用文に挙げた22の直接事案の企業・組織と、ショップサーブの波及先PFU・キングジムの計24表記である。全24表記を収録した。デジタル庁は企業ではなく行政として区別した。追加調査は公表統計、piyologの2026年7～9月アーカイブ、月別一覧、各社続報から実施した。

日本国内のすべての漏洩事件を1社ずつ網羅した台帳ではない。非公表・未発見の事故は数えられず、行政への報告は匿名集計で、公開ニュースの名寄せとは別の母集団である。本調査の32行を月ごとに分けても全国の増加率にはならない。公表日と侵入日も異なり、2026年9月の公表に数年前からの不正アクセスが含まれる場合がある。

ムラウチドットコム の件数は公式第二報PDFを直接取得できなかったため、公式案内の漏洩確認と、公式第二報を報じるINTERNET Watchの数値を組み合わせた。佐川急便の第三報は公式URLを確認したが動的ページの本文を取得できず、報道に基づく暫定行とした。これら2行は原因の一次検証済み事案へ含めない。古い検索要約と現在の公式本文が食い違った場合は、それぞれの取得結果を残し、採用した本文を明示した。

この初回版で確実に言えるのは、公開事案の件数だけでなく、対象データの量、個人を特定する情報の種類、共通システムから波及した企業数を分けて追う必要があるという点である。原因の説明まで追う際は、「不正アクセス」とだけ書かれた発表を、脆弱性管理・設定・認証・監視の具体的な問題へ勝手に翻訳しない。

8. 「Uncensoredなローカルモデルが漏洩増加の原因か」を検証する

2026年10月2日に追加調査した範囲では、AIの悪用と制限の少ないモデルの利用実態を示す一次研究・調査はある。しかし、日本の今回の漏洩事案や全国の増加分をUncensoredなローカルモデルへ帰属させる割合・因果効果は確認できない。「悪用の存在」と「国内の被害増加の原因」を区別する。

分けて確認する4項目

ローカル実行は攻撃者の手元の計算機等でモデルを動かす形態、オープンウェイトはモデルの重みが公開されていること、Uncensoredは拒否・内容制限が少ない特性を指す。3つは別の属性であり、同じ意味ではない。公開モデルをクラウド上で動かす場合もある。Uncensoredの定義や評価も研究によって異なるため、名称だけで犯罪利用を判定しない。

確認したい主張	必要な証拠	今回の確認結果
攻撃者がAIを使った	会話・ツール実行ログ、捜査・運営者の調査結果	海外の一次調査で観測あり
特定のUncensoredモデルを使った	モデル名・版・設定と攻撃活動との対応	利用サービスの研究あり。国内台帳の各事件への対応は未取得
ローカルで動かした	実行機器・配備形態の証拠	国内台帳の各事件について未取得
そのために被害が増えた	利用有無・時期・成功率を比較できる被害／非被害データ	全国の因果効果を示すデータは今回未取得

公開されている数値は何を数えているか

一次資料	数値	数えている対象	この数値だけでは言えないこと
Uncensoredモデルの生態系研究（2025年arXiv原稿）	調査した52のWebアプリのうち10が攻撃支援・悪意あるコード生成カテゴリ	特定の探索手順で見つけたWebサービス。用途は重複あり	10件の実被害、国内の利用率、攻撃者の手元でのローカル実行
Anthropicの悪用観測（2025年3月～2026年3月）	832の停止アカウント、13,873の行動観測。574／832（約69％）で攻撃能力開発を観測	Claudeで検知・停止したアカウントとモデルへ求めた行動	全攻撃者の69%、832の漏洩事件、Uncensoredローカルモデルの利用率
MicrosoftのEvilTokens調査（2026年9月）	12,000超の侵害されたメール受信箱、10,000超の組織との関連を報告	1つのAI利用犯罪サービスに関連した世界の被害	国内全体の割合、AIがなければ発生しなかった件数、モデルのローカル実行の確定

出典はUncensoredモデル研究・5.1節、Anthropicのデータセットと観測結果、MicrosoftのEvilTokens調査。

Uncensoredモデル研究は、モデルやサービスを発見する研究で、漏洩被害の統計ではない。モデル数には量子化版等の派生が含まれ、機能分類には著者によるメタデータのキーワード照合も使われている。論文の分類をそのまま「犯罪に使われた実証済みモデル数」とは扱わない。一般の成人向け会話、医療相談、セキュリティ検証を含む著者の広いカテゴリも、日本の漏洩犯罪件数へ換算しない。

Anthropicの調査は商用サービス側の観測であり、ローカルモデル全体を見渡すデータではない。停止対象を選んだ標本なので、一般利用者や全攻撃者へ割合を広げられない。行動の観測は攻撃成功の確認と同義ではなく、同社のリスクスコアも攻撃成功確率ではない。Microsoftの調査はAI利用と実際の侵害の関連を報告しているが、AIの寄与分を推定する比較群は示していない。

国内台帳の集計では未確認をゼロにしない

今回の国内台帳は企業等の被害公表を起点にしており、攻撃者側のモデル名、制限設定、配備形態、会話・実行ログは事件ごとに取得できていない。したがって「AIを使わなかった」「Uncensoredモデルによる被害は0%」とも判定できない。今回取得した資料だけでは利用率を算出できない、という結果を残す。

原因欄で確認した脆弱性や認証・設定の問題は、被害側で侵入を可能にした条件を示す。AIは攻撃者の調査、コード作成、標的選定、取得情報の分析などを助ける可能性があり、両者は同時に成立し得る。脆弱性が判明したという理由でAI利用を否定せず、逆に自動化や大量アクセスだけを見てAI利用を断定しない。

因果効果を統計的に確認するためのデータ

事件ごとにAI利用の確認状態、モデル名・版、拒否制限の設定、ローカル／クラウドの配備形態、利用工程、証拠の種類、攻撃の成否を記録する。未確認を非利用へ変換しない。被害の出た事件だけでなく失敗した攻撃も集め、標的の規模、業種、脆弱性公開時期、修正状況、観測方法の違いをそろえて比較する。

モデル公開前後の漏洩件数とダウンロード数が同時に増えたという相関だけでは、因果は証明できない。証拠のある攻撃群での成功率・所要時間・試行数の比較や、同じ条件でAI利用の有無を変えた実験なら寄与の一部を評価できる。ただし、実験で攻撃能力が上がったことと、日本の実被害増加への寄与率は別の結果である。

参考文献と追跡方法

全出典台帳はURL、資料区分、取得日時、HTTP状態、原文SHA256を記録している。全国統計の根拠は東京商工リサーチ、個人情報保護委員会、警察庁。個別事案の判断は企業・行政の公式本文を優先した。piyologは時系列・関連組織・一次資料を探索入口として用い、推定部分を企業公表と分離した。piyolog

更新時は、既存の原文を上書きせず、新しい続報を別の出典として保存し、事案管理番号を維持して台帳の状態・規模・原因を更新する。集計の再現手順と取得失敗は調査履歴に記載した。

企業・組織の事案一覧（32行）

JP001 Helpfeel／Gyazo

業種：情報通信

漏洩の確認状況：漏洩・不正閲覧確認

公表規模：23620000

原文の単位：ユーザー関連データ件

規模を読む際の条件：約数・匿名利用を含む。人数ではない

原因の分類：ソフトウェア脆弱性

公表された原因と留保：アップロードサーバーで任意コマンド実行。既知か未公表かは不明

分類した理由：初報と第二報でデータの外部流出を確認。画像メタデータと画像ファイルは区別

採用資料の公表・更新日：2026-09-25

出典番号：S04;S60

出典URL：<https://corp.helpfeel.com/news/news-20260925-01>;<https://corp.helpfeel.com/news/news-20260916-1>

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

JP002 Eストアー／ショップサーブ

業種：情報通信

漏洩の確認状況：漏洩・不正閲覧確認

公表規模：8853839

原文の単位：データ件

規模を読む際の条件：同一顧客の複数データを含み得る。人数ではない

原因の分類：侵入方法未公表

公表された原因と留保：サーバー上の不正プログラムで外部送信。具体的な侵入方法は調査中

分類した理由：第二報で外部送信を確認。利用店舗の公表を別の侵害に数えない

採用資料の公表・更新日：2026-08-02

出典番号：S18

出典URL：<https://estore.jp/press/20260802/>

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

JP003 タイムズモビリティ／パーク24／タイムズカー

業種：移動サービス

漏洩の確認状況：漏洩・不正閲覧確認

公表規模：6600000

原文の単位：アカウント

規模を読む際の条件：約数。本人確認書類約160万件は内数

原因の分類：侵入方法未公表

公表された原因と留保：Webサイトへの不正アクセス。侵入に用いた脆弱性等は未公表

分類した理由：第二報で約660万アカウントを公表。書類画像を別人数として加算しない

採用資料の公表・更新日：2026-09-29

出典番号：S05;S06

出典URL：<https://share.timescar.jp/news/2026/0928/1815.html>;<https://www.park24.co.jp/news/2026/09/20260929-1.html>

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

JP004 ムラウチドットコム／通販・顧客管理

業種：小売

漏洩の確認状況：漏洩・不正閲覧確認

公表規模：7716811

原文の単位：顧客情報件

規模を読む際の条件：規模の数値は第二報を報じた記事で照合

原因の分類：侵入方法未検証

公表された原因と留保：Webシステム脆弱性との報道あり。公式第二報PDF本文未取得のため原因集計では未検証

分類した理由：公式案内で持ち出しを確認。数値のみINTERNET Watchを補助根拠として採用

採用資料の公表・更新日：2026-09-15

出典番号：S30;S71

出典URL：<https://murauchi.com/static-pages/privacy/pressrelease.html>;<https://internet.watch.impress.co.jp/docs/news/2141530.html>

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

JP005 セイコーマート／セイコーマートアプリ

業種：小売

漏洩の確認状況：漏洩・不正閲覧確認

公表規模：572022

原文の単位：人分

規模を読む際の条件：公式本文では会員情報を閲覧確認

原因の分類：侵入方法未公表

公表された原因と留保：手法の詳細は公表を差し控えると説明

分類した理由：第三報の見出しは可能性だが本文は不正閲覧確認。本文を優先

採用資料の公表・更新日：2026-09-30

出典番号：S08

出典URL：https://online.seicomart.co.jp/delivery/cms/preview.php?pre_no=121

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

JP006 デジタル庁／GSS

業種：行政

漏洩の確認状況：漏洩の可能性

公表規模：246000

原文の単位：個人情報件

規模を読む際の条件：約数。職員等18.9万件、関係事業者等5.7万件。一般市民を含まない

原因の分類：ソフトウェア脆弱性

公表された原因と留保：VPN機器の既知脆弱性を利用した侵入。修正適用前に悪用。その後に保守担当アカウントを利用

分類した理由：公表本文は外部漏洩の可能性。アカウント利用と初期侵入経路を分離

採用資料の公表・更新日：2026-09-12

出典番号：S16;S72

出典URL：<https://www.digital.go.jp/news/2026-0911-01>;<https://www.digital.go.jp/press/5fc99139-a4e2-4b7b-8b0c-d475e926143f>

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

JP007 VOISING／BIツール

業種：エンターテインメント

漏洩の確認状況：漏洩・不正閲覧確認

公表規模：170000

原文の単位：情報件

規模を読む際の条件：約数。ツール製品名とCVEは公式に特定されていない

原因の分類：ソフトウェア脆弱性

公表された原因と留保：既知脆弱性への修正適用が攻撃までに間に合わなかったと公式説明

分類した理由：第四報で原因・約17万件を確認。Metabaseとの対応付けはpiyologの推定

採用資料の公表・更新日：2026-09-30

出典番号：S07;S40;S41

出典URL：<https://voising-official.com/news/1015>;<https://piyolog.hatenadiary.jp/entry/2026/10/01/112213>;<https://github.com/metabase/metabase/security/advisories/GHSA-vwf4-m7j8-wcjf>

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

JP008 アフラック生命保険／よりそうネット等

業種：金融保険

漏洩の確認状況：漏洩・不正閲覧確認

公表規模：4400000

原文の単位：人

規模を読む際の条件：約数。銀行口座情報約22万人は内数

原因の分類：アクセス制御・監視の課題

公表された原因と留保：通常アクセスに見える通信による大量取得。公式FAQが制限と監視の不足を説明

分類した理由：公式FAQで漏洩を確認。詳細な侵入手順と運用上の課題は同一視しない

採用資料の公表・更新日：2026-10-01

出典番号：S19

出典URL：https://www.aflac.co.jp/info/yorisou_faq.html

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

JP009 KDDI／ISP向けメールシステム

業種：情報通信

漏洩の確認状況：漏洩・不正閲覧確認

公表規模：12231954

原文の単位：名（公式表記）

規模を読む際の条件：メール情報の対象。パスワード7,616,173名は内数。独自に人の名寄せはしていない

原因の分類：ソフトウェア脆弱性

公表された原因と留保：第三者製ソフトウェアの脆弱性。6月17日の発覚時点でベンダーも未認識

分類した理由：7月21日訂正後の漏洩確認人数を採用。初報の可能性件数を上書きしない

採用資料の公表・更新日：2026-07-21

出典番号：S52;S20

出典URL：https://newsroom.kddi.com/news/assets/2026/kddi_nr_s-73_4619/kddi_nr_s-73_4619_pdf_01.pdf;
https://newsroom.kddi.com/news/assets/2026/kddi_nr_s-71_4593/kddi_nr_s-71_4593_pdf_01.pdf

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

JP010 東京メトロ／メトポ

業種：交通

漏洩の確認状況：漏洩の可能性

公表規模：59000

原文の単位：メールアドレス件

規模を読む際の条件：約数・メール情報のみ

原因の分類：侵入方法未公表

公表された原因と留保：会員向けWebサービスへの不正アクセス

分類した理由：公式PDFは漏洩の可能性と記載

採用資料の公表・更新日：2026-09-27

出典番号：S13

出典URL：<https://www.tokyometro.jp/info/files/9172e2efa7222d15f8d4f601b6385457.pdf>

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

JP011 イープラス／払戻し情報管理

業種：チケット

漏洩の確認状況：漏洩・不正閲覧確認

公表規模：1463

原文の単位：払戻し情報件

規模を読む際の条件：銀行口座情報751件は内数。一般会員データベースと別

原因の分類：侵入方法未公表

公表された原因と留保：払戻し用Webシステムへの不正アクセス

分類した理由：公式案内で1463件の漏洩を確認。全会員が対象とは読まない

採用資料の公表・更新日：2026-09-29

出典番号：S11

出典URL：<https://support-qa.eplus.jp/hc/ja/articles/62711500727961>

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

JP012 集英社／HAPPY PLUS COMMUNITY

業種：出版

漏洩の確認状況：漏洩・不正閲覧確認

公表規模：2835

原文の単位：ブロガー名

規模を読む際の条件：メール11,237件、取引先10,780件、案件630件は別のデータ型

原因の分類：設定・認証情報の問題

公表された原因と留保：CMS設定不備に起因するAPI認証情報攻撃、特権アカウント作成を原因と推定

分類した理由：公式PDFが漏洩を明記。原因は企業による推定として保持

採用資料の公表・更新日：2026-09-28

出典番号：S38

出典URL：<https://www.shueisha.co.jp/wp-content/uploads/2026/09/Shueisha20260928-1.pdf>

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

JP013 ベネフィット・ワン／ベネワン・プラットフォーム

業種：福利厚生

漏洩の確認状況：漏洩・不正閲覧確認

公表規模：13460

原文の単位：名

規模を読む際の条件：2,322企業・団体の従業員情報。ダウンロードした側は1社1名

原因の分類：プログラム不備（攻撃ではない）

公表された原因と留保：アンケート結果ダウンロード機能の条件設定不備。認知後の解消作業未実施

分類した理由：第三者の攻撃ではなく他社担当者への誤表示・提供。攻撃統計から除外

採用資料の公表・更新日：2026-09-30

出典番号：S31

出典URL：<https://corp.benefit-one.co.jp/company/news/news/2026/20260930/20260930.pdf>

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

JP014 ヤマト運輸／クロネコ代金後払い

業種：物流

漏洩の確認状況：漏洩の可能性

公表規模：

原文の単位：未公表

規模を読む際の条件：対象人数・件数は公表されていない

原因の分類：侵入方法未公表

公表された原因と留保：後払いサービスへの不正アクセス

分類した理由：10月2日の第二報で購入者情報等の漏洩可能性を公表

採用資料の公表・更新日：2026-10-02

出典番号：S09

出典URL：https://www.yamato-hd.co.jp/important/info_260929_1.html

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

JP015 佐川急便／お荷物問い合わせ等

業種：物流

漏洩の確認状況：漏洩の可能性

公表規模：

原文の単位：未公表

規模を読む際の条件：公式第三報はURLのみ確認。本文の根拠は報道

原因の分類：侵入方法未検証

公表された原因と留保：サービスへの不正アクセスとの報道。具体的な侵入方法は未検証

分類した理由：INTERNET Watchの第三報報道を暫定採用。公式ページは動的表示で本文未取得

採用資料の公表・更新日：2026-10-02

出典番号：S42;S59

出典URL：<https://internet.watch.impress.co.jp/docs/news/2145343.html>;<https://www2.sagawa-exp.co.jp/information/detail/421/>

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

JP016 京王電鉄グループ／グループシステム

業種：交通

漏洩の確認状況：侵害確認・漏洩未確認

公表規模：

原文の単位：未公表

規模を読む際の条件：漏洩人数をゼロとは扱わない

原因の分類：侵入方法未公表

公表された原因と留保：ランサムウェア感染を確認。初期侵入経路は未公表

分類した理由：公式初報はシステム障害とランサムウェアを確認。漏洩確定とは書かない

採用資料の公表・更新日：2026-09-26

出典番号：S14;S25

出典URL：<https://www.keio.co.jp/news/update/announce/nr260926v13404/>;<https://piyolog.hatenadiary.jp/entry/2026/09/30/021814>

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

JP017 ニッポンレンタカー／NRアプリ・第一事象

業種：移動サービス

漏洩の確認状況：漏洩の可能性

公表規模：41

原文の単位：名

規模を読む際の条件：会員情報が閲覧された可能性

原因の分類：侵入方法未公表

公表された原因と留保：アプリへの不正アクセス。詳細未公表

分類した理由：41名の事象を、10月1日公表の55名の別手法の事象と分離

採用資料の公表・更新日：2026-09-26

出典番号：S35

出典URL：<https://www.nipponrentacar.co.jp/info/202609.html>

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

JP018 ニッポンレンタカー／NRアプリ・第二事象

業種：移動サービス

漏洩の確認状況：漏洩の可能性

公表規模：55

原文の単位：名

規模を読む際の条件：第一事象との対象者重複は不明。41名と合算しない

原因の分類：侵入方法未公表

公表された原因と留保：9月19～21日の攻撃。第一事象と異なる手法と公式説明

分類した理由：別の不正アクセスと明記しているため別行にした

採用資料の公表・更新日：2026-10-01

出典番号：S36

出典URL：https://www.nipponrentacar.co.jp/info/202610_2.html

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

JP019 クオカード／LINEキャンペーンシステム

業種：決済関連

漏洩の確認状況：漏洩の可能性

公表規模：

原文の単位：未公表

規模を読む際の条件：LINE表示名・当選情報。決済システムは別

原因の分類：侵入方法未公表

公表された原因と留保：キャンペーン専用システムへの不正アクセス

分類した理由：一部情報の閲覧または流出可能性。QUOカード決済情報の漏洩とは書かない

採用資料の公表・更新日：2026-09-29

出典番号：S32

出典URL：<https://www.quocard.com/newsroom/important/20260929/>

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

JP020 手間いらず／TEMAIRAZU

業種：情報通信

漏洩の確認状況：漏洩の可能性

公表規模：

原文の単位：未公表

規模を読む際の条件：宿泊予約情報。被害施設総数と人数は未公表

原因の分類：侵入方法未公表

公表された原因と留保：原因は特定・対策済みだが手法の詳細を公表しない

分類した理由：宿泊者情報の閲覧・取得可能性は否定できず、フィッシングとの因果も調査中

採用資料の公表・更新日：2026-09-28

出典番号：S37;S22

出典URL：<https://www.temairazu.co.jp/pdf/1206/news-update;https://piyolog.hatenadiary.jp/entry/2026/09/30/013735>

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

JP021 らしんばん／通販・買取サービス

業種：小売

漏洩の確認状況：漏洩の可能性

公表規模：

原文の単位：未公表

規模を読む際の条件：口座情報、本人確認情報、買取同意書画像等を含み得る

原因の分類：侵入方法未公表

公表された原因と留保：9月14～16日の不正アクセス

分類した理由：公式初報は漏洩した可能性。件数がないためゼロを置かない

採用資料の公表・更新日：2026-10-01

出典番号：S33

出典URL：<https://www.lashinbang.com/info/26357>

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

JP022 スターツ出版／OZmall

業種：情報サービス

漏洩の確認状況：漏洩の可能性

公表規模：447610

原文の単位：名分

規模を読む際の条件：最大値・メールアドレス。一部は氏名と都道府県

原因の分類：侵入方法未公表

公表された原因と留保：9月26日に大量の不正アクセスを検知

分類した理由：公式本文の最大対象範囲を採用。全情報の漏洩確認とはしない

採用資料の公表・更新日：2026-09-27

出典番号：S12

出典URL：<https://starts-pub.jp/info20260927>

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

JP023 ニチレイグループ／グループサーバー

業種：食品・物流

漏洩の確認状況：漏洩・不正閲覧確認

公表規模：53866

原文の単位：情報件

規模を読む際の条件：配送先3,308件、取引先6,849件、従業員等43,709件の算術合計。ユニーク人数ではない

原因の分類：侵入方法未公表

公表された原因と留保：サイバー攻撃を受けたサーバー。具体的侵入経路は未公表

分類した理由：9月18日第7報で漏洩を確認。初報の漏洩未確認状態から更新

採用資料の公表・更新日：2026-09-18

出典番号：S51;S34

出典URL：<https://www.nichirei.co.jp/news/2026/524.html>;<https://www.nichirei.co.jp/news/2026/512.html>

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

JP024 さくらインターネット／レンタルサーバー・販売管理

業種：情報通信

漏洩の確認状況：漏洩の可能性

公表規模：1360563

原文の単位：アカウント

規模を読む際の条件：レンタルサーバー951アカウントはこの対象範囲に含まれる

原因の分類：侵入方法未公表

公表された原因と留保：複数環境への不正アクセス。環境間の関連と具体的手法は未確定・未公表

分類した理由：公式第三報は閲覧・取得の可能性。明確な外部持ち出し事実は未確認

採用資料の公表・更新日：2026-09-10

出典番号：S17

出典URL：<https://www.sakura.ad.jp/corporate/information/newsreleases/2026/09/10/1968225692/>

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

JP025 ファインズ／予約システム

業種：情報通信

漏洩の確認状況：侵害確認・漏洩確定範囲不明

公表規模：1536322

原文の単位：予約情報件

規模を読む際の条件：公表した対象件数。人数ではない

原因の分類：侵入方法未公表

公表された原因と留保：9月22日に異常検知・不正アクセス確認

分類した理由：題名は情報漏えいだが本文は不正アクセスと対象件数を記載。実際の持ち出しの断定を保留

採用資料の公表・更新日：2026-09-25

出典番号：S15

出典URL：<https://e-tenki.co.jp/news/弊社システムへの不正アクセスによる情報漏えい/>

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

JP026 日本郵政／日本郵便／郵便局アプリ・ゆうID

業種：物流

漏洩の確認状況：漏洩・不正閲覧確認

公表規模：19

原文の単位：名分

規模を読む際の条件：不正取得データ69件。19名分と69件を分ける

原因の分類：侵入方法未公表

公表された原因と留保：郵便局アプリへの不正アクセス

分類した理由：公式発表で69件・19名分の不正取得を確認

採用資料の公表・更新日：2026-09-29

出典番号：S10

出典URL：https://files.japanpost.jp/assets/34d9d11432734cfaa759e78fe395b688/18239b871f714763aa7eb15c25e7b30b/20260929_01.pdf

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

JP027 イエローハット／会員情報管理

業種：小売

漏洩の確認状況：漏洩の可能性

公表規模：1801499

原文の単位：名

規模を読む際の条件：最大値。別ブランドのシステムには影響なしと説明

原因の分類：侵入方法未公表

公表された原因と留保：会員システムへの不正アクセス

分類した理由：8月28日の公表本文は漏洩の可能性。2りんかんの別件と混同しない

採用資料の公表・更新日：2026-08-28

出典番号：S44

出典URL：<https://www.yellowhat.jp/information/yellowhat/202608.html>

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

JP028 EPARKリラク & エステ／PeakManager

業種：情報通信

漏洩の確認状況：漏洩・不正閲覧確認

公表規模：22180000

原文の単位：レコード

規模を読む際の条件：約数。名寄せ後も人数への置き換えは困難と公式説明

原因の分類：侵入方法未公表

公表された原因と留保：データベース情報の外部転送後に削除。手法の詳細は非公表

分類した理由：9月24日の第二報で漏洩確認。初報約3,300万から精査後約2,218万へ更新

採用資料の公表・更新日：2026-09-24

出典番号：S70;S65

出典URL：<https://www.epark-relax.co.jp/news/231>;<https://www.epark-relax.co.jp/news/225>

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

JP029 ApplyNow／きちりホールディングス／採用管理・電子雇用契約

業種：情報通信

漏洩の確認状況：漏洩・不正閲覧確認

公表規模：

原文の単位：全体件数未公表

規模を読む際の条件：委託元の確認済み件数を全体件数へ置き換えない

原因の分類：ソフトウェア脆弱性

公表された原因と留保：データ分析ツールの脆弱性。公式は製品名・CVE・攻撃前の公開時期を特定しない

分類した理由：親会社初報は可能性。吉野家等の公式公表で同じ侵害からの漏洩を確認

採用資料の公表・更新日：2026-09-30

出典番号：S69;S54;S55;S56

出典URL：<https://www.kichiri.co.jp/wp-content/uploads/2026/09/2609091111.pdf>;<https://biz.applynow.jp/support/>;https://www.yoshinoya.com/wp-content/uploads/2026/09/30185541/news_2026093004.pdf;<https://mai-sen.com/news/2026/post-459.html>

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

JP030 GMOインターネット／ConoHa WING

業種：情報通信

漏洩の確認状況：侵害確認・漏洩未確認

公表規模：426

原文の単位：侵害対象アカウント

規模を読む際の条件：侵害範囲。漏洩人数・件数ではない

原因の分類：侵入方法未公表

公表された原因と留保：一部Webサーバー領域に不正プログラム。会員情報管理は別環境

分類した理由：公式告知で侵害を確認。会員・契約・支払情報の漏洩はないと説明

採用資料の公表・更新日：2026-09-20

出典番号：S66

出典URL：https://www.conoha.jp/wing/news/?ap=2015054834&btn_id=news--news_wing-news

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

JP031 ロート製薬／通信販売の通話・顧客管理

業種：製薬

漏洩の確認状況：漏洩の可能性

公表規模：

原文の単位：未公表

規模を読む際の条件：通話音声データ等と顧客管理情報

原因の分類：侵入方法未公表

公表された原因と留保：通信販売関連システムで不正取得の可能性

分類した理由：9月15日の続報を採用。取得範囲・件数は調査中

採用資料の公表・更新日：2026-09-15

出典番号：S67

出典URL：https://www-sc10-cd.rohto.com/news/whatsnew/2026/0915_01/

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

JP032 日本テレネット／受託・顧客管理等

業種：情報通信

漏洩の確認状況：漏洩の可能性

公表規模：

原文の単位：区分別件数のみ

規模を読む際の条件：60.2万件・40.4万件・3.3万件等を公表。集計対象の重複不明のため総数は置かない

原因の分類：ネットワーク機器経由（詳細未公表）

公表された原因と留保：ネットワーク機器から侵入しマルウェアで暗号化。具体的機器・脆弱性は未公表

分類した理由：公式調査結果は外部転送痕跡なし。ただし区分別に漏洩のおそれの情報を記載

採用資料の公表・更新日：2026-06-12

出典番号：S68

出典URL：https://www.nippon-tele.net/release/20260612_4659/

判定方法：原文本文・続報を読んだ手動判断（機械的分類なし）

参考文献一覧

S01 東京商工リサーチ・2025年上場企業調査

https://www.tsr-net.co.jp/data/detail/1202348_1527.html

S02 個人情報保護委員会・2025年度年次報告

https://www.ppc.go.jp/aboutus/report/annual_report_2025/

S03 警察庁・2025年サイバー脅威情勢

https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7/R07_cyber_jousei.pdf

S04 Helpfeel・Gyazo第二報

<https://corp.helpfeel.com/news/news-20260925-01>

S05 タイムズカー・第二報

<https://share.timescar.jp/news/2026/0928/1815.html>

S06 パーク24・タイムズカー第三報

<https://www.park24.co.jp/news/2026/09/20260929-1.html>

S07 VOISING・第四報

<https://voising-official.com/news/1015>

S08 セイコーマート・第三報

https://online.seicomart.co.jp/delivery/cms/preview.php?pre_no=121

S09 ヤマト運輸・10月2日第二報

https://www.yamato-hd.co.jp/important/info_260929_1.html

S10 日本郵便・郵便局アプリ

https://files.japanpost.jp/assets/34d9d11432734cfaa759e78fe395b688/18239b871f714763aa7eb15c25e7b30b/20260929_01.pdf

S11 イープラス・スマチケ

<https://support-qa.eplus.jp/hc/ja/articles/62711500727961>

S12 スターツ出版・OZmall第二報

<https://starts-pub.jp/info20260927>

S13 東京メトロ・メトポ

<https://www.tokyometro.jp/info/files/9172e2efa7222d15f8d4f601b6385457.pdf>

S14 京王電鉄・ランサムウェア

<https://www.keio.co.jp/news/update/announce/nr260926v13404/>

S15 ファインズ・予約システム

<https://e-tenki.co.jp/news/弊社システムへの不正アクセスによる情報漏えい/>

S16 デジタル庁・GSS

<https://www.digital.go.jp/news/2026-0911-01>

S17 さくらインターネット・第三報

<https://www.sakura.ad.jp/corporate/information/newsreleases/2026/09/10/1968225692/>

S18 Eストーリー・ショップサーブ第二報

<https://estore.jp/press/20260802/>

S19 アフラック・FAQ

https://www.aflac.co.jp/info/yorisou_faq.html

S20 KDDI・メールシステム第一報

https://newsroom.kddi.com/news/assets/2026/kddi_nr_s-71_4593/kddi_nr_s-71_4593_pdf_01.pdf

S21 piyolog・2026年9月記事一覧

<https://piyolog.hatenadiary.jp/archive/2026/09>

S22 piyolog・TEMAIRAZU

<https://piyolog.hatenadiary.jp/entry/2026/09/30/013735>

S23 piyolog・Gyazo

<https://piyolog.hatenadiary.jp/entry/2026/09/17/032044>

S24 piyolog・GSS

<https://piyolog.hatenadiary.jp/entry/2026/09/11/220855>

S25 piyolog・京王

<https://piyolog.hatenadiary.jp/entry/2026/09/30/021814>

S26 セキュリティ対策Lab・9月事例

<https://rocket-boys.co.jp/security-measures-lab/2026-09-latest-cyber-attack-cases/>

S27 セキュリティ対策Lab・2026年大規模16事例

<https://rocket-boys.co.jp/security-measures-lab/2026-japan-major-security-incidents-17-gyazo-epark-fines-times/>

S28 サイバーセキュリティラボ・9月16事例

<https://gate02.ne.jp/lab/security-article/incident-news-summary-202609-extra-edition/>

S29 東京商工リサーチ・2024年上場企業調査

https://www.tsr-net.co.jp/data/detail/1200872_1527.html

S30 ムラウチドットコム・調査報告

<https://murauchi.com/static-pages/privacy/pressrelease.html>

S31 ベネフィット・ワン・9月30日発表

<https://corp.benefit-one.co.jp/company/news/news/2026/20260930/20260930.pdf>

S32 クオカード・LINEキャンペーン

<https://www.quocard.com/newsroom/important/20260929/>

S33 らしんばん・10月1日発表

<https://www.lashinbang.com/info/26357>

S34 ニチレイ・第一報

<https://www.nichirei.co.jp/news/2026/512.html>

S35 ニッポンレンタカー・NRアプリ第一事象

<https://www.nipponrentacar.co.jp/info/202609.html>

S36 ニッポンレンタカー・NRアプリ別事象

https://www.nipponrentacar.co.jp/info/202610_2.html

S37 手間いらず・9月28日発表

<https://www.temairazu.co.jp/pdf/1206/news-update>

S38 集英社・HAPPY PLUS COMMUNITY

<https://www.shueisha.co.jp/wp-content/uploads/2026/09/Shueisha20260928-1.pdf>

S39 JCOM・KDDI共通基盤の続報

https://newsreleases.jcom.co.jp/news/20260706_21698.html

S40 piyolog・VOISING

<https://piyolog.hatenadiary.jp/entry/2026/10/01/112213>

S41 Metabase・脆弱性勧告

<https://github.com/metabase/metabase/security/advisories/GHSA-vwf4-m7j8-wcjf>

S42 佐川急便の続報紹介・INTERNET Watch

<https://internet.watch.impress.co.jp/docs/news/2145343.html>

S43 KDDIの続報紹介・NEXSIGHT

<https://cyber.nexsight.co/articles/2026/08/11/kddi-isp-mail-system-breach-soumu-guidance/>

S44 イエローハット・予約システム

<https://www.yellowhat.jp/information/yellowhat/202608.html>

S45 piyolog・ApplyNow

<https://piyolog.hatenadiary.jp/entry/2026/10/02/174228>

S46 piyolog・2026年8月記事一覧

<https://piyolog.hatenadiary.jp/archive/2026/08>

S47 piyolog・2026年7月記事一覧

<https://piyolog.hatenadiary.jp/archive/2026/07>

S48 サイバーセキュリティ.com・漏洩一覧

<https://cybersecurity-jp.com/leakage-of-personal-information>

S49 セキュリティ対策Lab・8月漏洩一覧

<https://rocket-boys.co.jp/security-measures-lab/2026-08-data-breach-cases-summary/>

S50 piyolog・タイムズカー

<https://piyolog.hatenadiary.jp/entry/2026/09/28/214857>

S51 ニチレイ第7報

<https://www.nichirei.co.jp/news/2026/524.html>

S52 KDDI調査結果

https://newsroom.kddi.com/news/assets/2026/kddi_nr_s-73_4619/kddi_nr_s-73_4619_pdf_01.pdf

S53 ApplyNow初報

<https://applynow.co.jp/news/20260909>

S54 ApplyNow対象者案内

<https://biz.applynow.jp/support/>

S55 吉野家・はなまる

https://www.yoshinoya.com/wp-content/uploads/2026/09/30185541/news_2026093004.pdf

S56 井筒まい泉

<https://mai-sen.com/news/2026/post-459.html>

S57 警察庁統計一覧

<https://www.npa.go.jp/publications/statistics/cybersecurity/>

S58 IPA届出状況

<https://www.ipa.go.jp/security/todokede/crack-virus/about.html>

S59 佐川急便第三報

<https://www2.sagawa-exp.co.jp/information/detail/421/>

S60 Gyazo初報

<https://corp.helpfeel.com/news/news-20260916-1>

S61 警察庁2026上半期

https://www.npa.go.jp/publications/statistics/cybersecurity/data/R8kami/R08_kami_cyber_jousei.pdf

S62 PFU漏洩公表

<https://www.pfu.ricoh.com/news/2026/news260918-2.html>

S63 きちりApplyNow初報

<https://www.kichiri.co.jp/news/2026/ir/4180/>

S64 キングジム

<https://www.kingjim.co.jp/news/detail/858.html>

S65 EPARK第一報

<https://www.epark-relax.co.jp/news/225>

S66 ConoHa

https://www.conoha.jp/wing/news/?ap=2015054834&btn_id=news--news_wing-news

S67 ロート製薬

https://www-sc10-cd.rohto.com/news/whatsnew/2026/0915_01/

S68 日本テレネット

https://www.nippon-tele.net/release/20260612_4659/

S69 ApplyNow親会社添付

<https://www.kichiri.co.jp/wp-content/uploads/2026/09/2609091111.pdf>

S70 EPARK第二報

<https://www.epark-relax.co.jp/news/231>

S71 ムラウチ第二報の件数報道

<https://internet.watch.impress.co.jp/docs/news/2141530.html>

S72 デジタル庁GSS不正アクセスQ&A（2026年9月12日更新）

<https://www.digital.go.jp/press/5fc99139-a4e2-4b7b-8b0c-d475e926143f>

S73 Consiglieres in the Shadow（arXiv v1、2025年8月18日）

<https://arxiv.org/html/2508.12622v1>

S74 Anthropic Mapping AI-enabled cyber threats（2026年6月3日）

<https://www.anthropic.com/research/attack-navigator>

S75 Microsoft Disrupting EvilTokens（2026年9月22日）

<https://blogs.microsoft.com/on-the-issues/2026/09/22/disrupting-eviltokens-the-ai-chatbot-built-for-cybercrime/>