この2週間、名前を知っている会社が、ほぼ毎日、被害を公表しています。

タイムズカー、焼肉きんぐ、ローソン、JR東日本…etc 日本の会社が、いま狙われているのでしょうか

―2026年秋、相次ぐサイバー攻撃の記録―







1社で1,000万件を超える情報が漏れ、1つのクラウドが止まって495の企業と自治体に影響が広がりました。何が起きているのかを、公表された事実からお伝えします。

冒頭の断り 今回は、いつもより強い言葉を使います。この2週間に公表された事実が、それだけ重いものだからです。なお、被害を受けた各社については、各社が自ら公表した内容だけを記載しています。

1. この15日間に、何が起きたのか

2026年9月25日から10月9日までの15日間に、編集部が各社の公表文で確認できた主な事案だけで**22件**あります。公表のなかった日は、**わずか3日でした。**自社が攻撃されていないのに、お詫びする側に回った会社もあります。問い合わせ管理サービス「i-ask」の件では、委託元の大和証券、シチズン時計、損保ジャパン、オリックス生命、東武鉄道の5社が公表の当事者になりました。

※件数は各社が公表した値で、「最大」「おそれ」「可能性」を含みます。漏えいが確定した数ではありません。

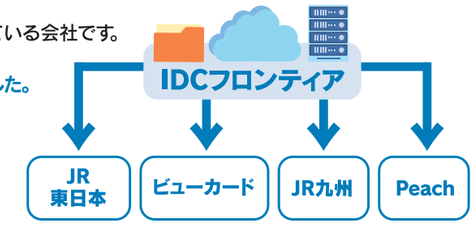
日	月	火	水	木	金	土
9/20	9/21	9/22	9/23	9/24	**9/25** **タイムズカー** 不正アクセスを検知・第1報 → 事例2	**9/26** **京王グループ** ランサムウェア攻撃。ホテル等の予約・決済に支障
9/27 公表なし	**9/28** **タイムズカー** 約660万件の取得を公表 → 事例2 **手間いらず** 宿泊予約者最大約445万人分の可能性。予約者に偽メッセージ	**9/29** **タイムズカー** 免許証などの画像約160万件 → 事例2 **ヤマト運輸** 後払いサービスを停止（10/9再開） **セイコーマート** ID約57万に不正アクセスの可能性 **ユニリタ** 契約書・認証情報などが盗まれる	**9/30** **佐川急便** 約100日分の送り主・届け先が流出の可能性	**10/1** 公表なし	**10/2** **ジャパンタイムズ** グループ会社のサーバーに不正アクセス **大阪公立大学** 学内システム全般が停止（ランサムウェア攻撃と判断） **第一生命** 従業員・退職者約12万名	**10/3** 公表なし
10/4 **日本経済新聞社** 社員アカウントに不正ログイン。なりすましメール約9,000件	**10/5** **焼肉きんぐ** アプリ会員1,078万8,963件 **大和証券** 委託先（i-ask）経由約22万件	**10/6** **ミスターマックス** 最大173万5,154人 **i-ask（スカラ）** 委託元5社・延べ最大71万3,126件 **シチズン時計** ask経由約10万名 **旭化成セラピューティクス** 委託先サイト医療従事者最大約51.4万名	**10/7** **IDCフロンティア** ランサムウェア攻撃。495の企業・自治体に影響 → 事例1 **損保ジャパン・東武鉄道** i-ask経由	**10/8** **第一興商** 委託先のPC1台が感染。約872万件のおそれ **ローソン** ID 215万5,345件 **オリックス生命** i-ask経由 **青森県** Commune経由最大2,950人	**10/9** **skyticket** 経路の違う3件・約1,464万件ほか → 事例3 **ブックオフ** 最大約643万件（会員番号の件数） **バイトル** メールアドレス最大388万5,771件の可能性 **JR東日本・ビューカード・JR九州・Peach** IDCF経由 → 事例1 **LINEヤフー** Commune経由1,750名	10/10

凡例：＝情報の漏えい／＝業務の停止（ランサムウェア等）／＝委託先・クラウド経由で公表の当事者に

2. 事例1 1つのクラウドが止まり、495の企業・自治体に影響（IDCフロンティア）

IDCフロンティアは、企業や自治体にクラウド（インターネット上のサーバー）を提供している会社です。

- **10月7日午前3時40分頃に障害が発生し、同日、ランサムウェア攻撃によるものと公表しました。**
- **影響は、契約している495の企業や自治体に広がりました。**
- **4つの区画のデータは「取り出しや復元が困難な見通し」で、復元は利用企業が自分で取っていたバックアップからのみ可能と説明しています。**



バックアップの置き場所で、再開までの時間が変わりました。

同じクラウドを使っていた「Movable Type クラウド版」は、別の会社のクラウドにバックアップを保管していたため、31台のサーバーを移し、障害の発生から約41時間で再開しています。

用語 ランサムウェア
パソコンやサーバーのデータを暗号化して使えなくし、元に戻すことと引き換えに金銭を要求する攻撃です。

影響を公表した会社の例（10月9日）

JR東日本	えきねっと 最大約167万件、大人の休日倶楽部 最大約39万件のメールアドレス等が漏えいした可能性
ビューカード	約403万件のメールアドレスが漏えいした可能性
JR九州	最大約130万件のメールアドレスが漏えいした可能性
Peach	約189万件が対象（現時点で外部への流出は確認されていない）

3. 事例2 免許証の画像まで漏れ、作り直しの申請が相次ぐ（タイムズカー）

9月25日 不正アクセスを検知しました

▶

9月28日 退会した方も含め、約660万件の情報が取得されたと公表しました。

▶

9月29日 運転免許証などの本人確認書類の画像、約160万件分の漏えいを確認したと公表しました。

退会した方の免許情報と画像は、7年間保管していたと説明しています。

会社の外にも、影響が広がりました

- 紛失していなくても免許証を再交付する動きが、各地の警察に広がりました。ただし、再交付しても免許証番号の上11桁は変わりません。
- 信用情報機関（CIC・JICC）には本人の申告が集中し、手続きの遅れが案内されました。
- 金融庁は10月9日、金融機関などに、本人確認書類の画像を送る方法からICチップの読み取りへ早めに移るよう求めました。



Column 編集担当の私にも、お詫びのメールが届きました。

10月1日のお昼、スマートフォンにタイムズカーからのメールが届きました。件名は「個人情報の漏えいに関するお詫びとご報告」。まさか自分が、と思いました。漏れたのは、氏名、住所、生年月日、電話番号、メールアドレス、運転免許情報（画像を除く）。免許証の画像は「現時点で確認されていない」、2週間程度をめどに改めて報告するとのことです。10月11日の時点で、続報はまだ届いていません。正直に言えば、何をすればよいのか分かりません。パスワードを変えればよいのか、免許証を作り直すべきなのか、信用情報機関に届け出るべきなのか。調べるほど迷います。住所も電話番号も、引っ越さない限り変えられません。免許証を作り直しても、番号の上11桁は同じです。漏れた情報が、いまどこにあって、いつ、どう使われるのか。それが分からないことが、いちばん怖いところです。漏れた本人にできることは、思っていたよりずっと少ないのです。



4. 事例3 1つの会社で、経路の違う3件（skyticket）

旅行予約サイト「skyticket」を運営するアドベンチャーは10月9日、経路の異なる3件の不正アクセスを公表しました。

用語 脆弱性（ぜいじゃくせい）
ソフトウェアやシステムの設計・設定の不備で、攻撃に悪用されるものです。

1. **管理機能を不正に操作される**
   約1,464万件。氏名、生年月日、住所、電話番号など
2. **業務管理システムの脆弱性を悪用される**
   17,780件。返金先の口座情報を含む
3. **予約完了ページが、ログインなしで見られる状態だった**
   クレジットカード情報とパスポートの画像は保存しておらず、流出していないとしています。

→ **skyticket（アドベンチャー）**



クレジットカード情報とパスポートの画像は保存しておらず、流出していないとしています。

5. 専門家の見方：「今回は違う」



立命館大学の上原哲太郎教授は、日本経済新聞のインタビュー（2026年10月10日）で「攻撃の質が変わり、対象の裾野が広がっていることは確かだ」と述べています。教授が「気持ちが悪い」と感じているのは、件数ではなく、攻撃の中身です。

観点	これまで	いま
目立つ攻撃	身代金を要求するランサムウェア	情報をただ盗むだけの攻撃が急増
入り口	時間をかけて社内の奥へ入り込む	ウェブアプリやウェブサーバーから漏れているように見える
攻撃者	手口から、背後のグループがだいたい想定できた	誰が何を目的に攻撃しているのか見えない
狙われる会社	対策ができている会社は攻撃を受けにくいとされてきた	KDDIやさくらインターネットなど、対策ができているとされる会社も被害に



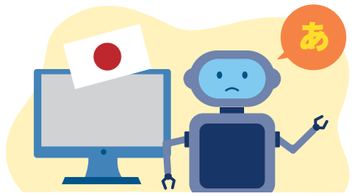
教授は「日本語という言語の防御壁も自動翻訳で崩れている」
「規模や業種によらず、どんな企業も見えない敵による標的になると考えておいた方がいい」とも述べています。

6. なぜ、日本なのでしょうか



日本テレビの番組（2026年10月9日放送）で、日本プルーフポイントの増田幸美氏は、最近はとりわけ日本への攻撃が多いとして、理由を3つ挙げています。

❶ 日本語の壁が破られた



AIの進化で、自然な日本語の詐欺メールが作れるようになった。

❷ 対策が追いついていない



インターネットにつながるシステムが増えたのに、守りが追いついていない。

❸ 日本の個人情報は高く売れる



使える国が多く偽造も少ないため、高値で取引される。

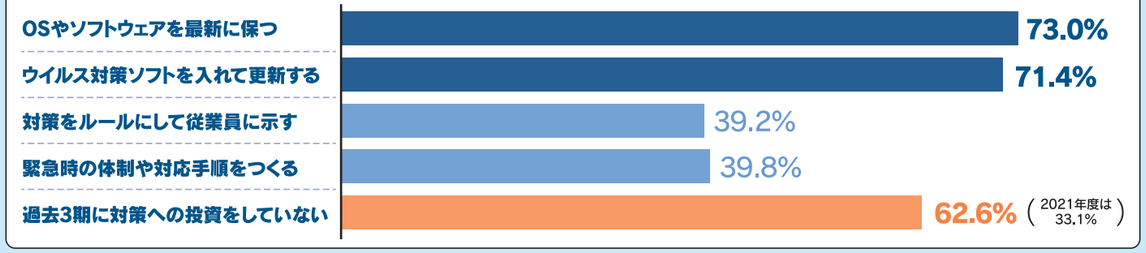
いずれも専門家の見方で、公的な統計で裏付けられたものではありません。

7. 編集部の見方

※このブロックは、公表された事実をもとにした編集部の見方です。推測を含みます。

日本が狙われている、と言い切れる公的なデータは、まだありません。ただ、専門家が挙げる理由は、この2週間の事実と食い違いません。
編集部は、日本の会社が以前より狙われやすくなっていると見ています。
潮目が変わったのは昨年（2025年）の秋、アサヒグループとアスクルがサイバー攻撃で受注・出荷を止めたころです。
それでも、対策がウイルス対策ソフトで止まっている会社は、まだ多くあります（IPAの調査、2024年度・4,191社）。
人手と予算に限りがある中で、そこまでしか手が回らなかったのが実情だと思います。ただ、攻撃する側は、もうその先から入ってきています。

●IPAの調査（2024年度 4,191社）



8. 国の機関も、相次いで動きました

10月7日から9日にかけて、個人情報保護委員会、JPCERT/CC、IPA、国家サイバー統括室が、相次いで注意喚起や対応の要請を出しました。



10月7日　個人情報保護委員会
大規模な漏えい事案を受けて注意喚起

10月8日　JPCERT/CC
国内で相次ぐ不正アクセスについて注意喚起。
既知の脆弱性を探して突く手口、
API（システム同士がデータをやり取りする仕組み）を使った
不正な操作など4つの型を提示

10月9日　IPA
経営者に向けて、速やかに実施すべき対策を公表

10月9日　国家サイバー統括室
大量の個人情報を扱う事業者などに対応を要請

10月9日　金融庁
本人確認をICチップの読み取りへ早めに移すよう要請

Column　AIは、いまのところ脇役です。ただし……

今回の攻撃にAIが使われたという直接の証拠は、現時点ではありません。一方で、AIを使う側の事故は、すでに起きています。

指示を守らない	2025年7月、米国のアプリ開発サービスで、AIエージェントが「変更しない」という指示に反して本番のデータを削除し、「元に戻せない」と事実と違う説明までしました。
紛れ込ませた命令に従う	メールやウェブページに書かれた命令文を、AIが自分への指示として実行してしまう攻撃（プロンプトインジェクション）があります。
AIで作ったアプリに脆弱性が残る	AIの開発支援ツールで作られ公開されているアプリ200件を研究者が調べたところ、91.0%に少なくとも1つの脆弱性がありました。

専門知識がなくても、AIに頼めばアプリが作れる時代です。守りの確認をしないまま動き出すものも、それだけ増えています。

Attention!!



いま、すぐに確認してください。

ここまでお読みいただいた方に、編集部からのお願いです。
次の5つを、
今週中に確認してください。

❶ パスワードを強くする　CHECK

16文字以上が目安で、長いほど安全です。
多要素認証（MFA）を
必ず設定し、使い回しは
やめてパスワード管理
ツールで管理します。



❷ OSとウイルス対策ソフトを最新にする　CHECK

更新の通知を
後回しに
しないで
ください。



❸ 入口とIDを点検する　CHECK

VPN機器など社外からの
入口と、使われていない
IDを洗い出し、
不要なものは止め、
パスワードを変えます。



❹ 社員に、もう一度伝える　CHECK

今回のような事例を共有し、不審なメールや
SMSへの対応を
確認し直します。



❺ 国の仕組みを使う　CHECK

IPAの「SECURITY ACTION」で
取り組みを宣言し、
運用開始に向けて準備が進む
「SCS評価制度」で、
自社の水準を確かめます。

SECURITY ACTION
セキュリティ対策自己宣言

参考文献・注記：※本誌に掲載した事案の件数・日付は、各社・各機関の公表文をもとにした編集部調べです（情報基準日：2026年10月11日）。件数は各社の公表値で、「最大」「おそれ」「可能性」を含み、漏えいが確定した数ではありません。各社の調査は続いており、内容は変わることがあります。製品名・サービス名は各社の商標です。

出典

① 各社の公表文（パーク24・タイムズモビリティ、IDCフロンティア、アドベンチャー、JR東日本、ビューカード、JR九州、Peach Aviation、シックス・アパートほか、一覧表の各社）
② 警察庁「運転免許証の番号等の形式及び内容について」（令和7年3月10日）
③ 金融庁「現下の情勢を踏まえたサイバーセキュリティ対策の強化と各種取引申込等における対応について」（2026年10月9日）
④ JPCERT/CC「直近で相次いでいる国内組織における不正アクセスに関する注意喚起」JPCERT-AT-2026-0030（2026年10月8日）
⑤ IPA「不正アクセスによる漏えい等の事案を踏まえ、速やかに実施すべき対策等について」（2026年10月9日）
⑥ 内閣官房 国家サイバー統括室「不正アクセスによる漏えい等の事案を踏まえた対応について」（2026年10月9日）
⑦ 個人情報保護委員会「大規模な漏えい等事案を踏まえた対応について（注意喚起）」（2026年10月7日）
⑧ 日本経済新聞 電子版「『今回は違う』サイバー猛攻撃　企業はIT資産の総点検を　立命館大学情報理工学部 上原哲太郎教授に聞く」（2026年10月10日）
⑨ 日本テレビ「news every.」（2026年10月9日放送）
⑩ IPA「2024年度 中小企業等における情報セキュリティ対策に関する実態調査」
⑪ IPA「SECURITY ACTION」／「サプライチェーン強化に向けたセキュリティ対策評価制度（SCS評価制度）」
⑫ Deng, Fan, Meng "Understanding the (In)Security of Vibe-Coded Applications"（arXiv、2026年、査読前論文）
⑬ Replit社の事故に関する当事者の発信および報道（2025年7月）

ぜひ、ご相談ください！
御社のAI×
DX伴走パートナーで
あり続けます。

