サイバーセキュリティ総研｜月次まとめ

# 2026年10月のサイバー攻撃・情報漏えい事案まとめ――国内130件を一覧化、目立ったのは「アプリ会員」「委託先経由」「盗まれた認証情報」

2026年11月2日版　／　発行：サイバーセキュリティ総研（cybersecurity-info.com）
Web版：https://cybersecurity-info.com/column/cyber-incidents-2026-10-summary/

**お断り：**本記事は2026年11月2日時点で確認できた公表情報と報道をもとにしています（11月2日に外務省とGMOグローバルサインの2件を追加）。対象は、2026年10月に公表された事案と、9月以前に公表され10月に続報（件数の確定や原因の判明など）があった事案です。件数は各組織の公表値で、重複の有無や数え方が異なるため合算していません。報道のみで確認したものは出典欄に「報道」と記しました。公表されたものに限られ、すべての事案を網羅しているわけではありません。

**この記事の要点**

- 2026年10月に公表された国内のサイバー攻撃・不正アクセスの事案を**130件**確認した。100万件を超える個人情報の漏えい（可能性を含む）を公表した組織は20を超える
- 手口別では、Webサイトやアプリへの不正アクセスが75件と最も多い。外食やECの公式アプリの会員情報が、数百万〜1,000万件単位で漏えいした
- 委託先・SaaS・クラウドを経由した被害が29件。1社への侵入が数十〜数千の利用組織に波及する例が続いた
- 盗まれたIDやパスワード、クラウドの認証情報が悪用された事案が17件。正規のアカウントで入られると、侵入として気づきにくい
- ランサムウェアや恐喝では、決算発表の延期や受注・出荷の停止など、業務そのものへの影響が目立った。GMO事件では攻撃者が注目を武器にした
- 11月にまずやるべきことは、委託先とSaaSの棚卸し、外部に公開しているアプリやAPIの点検、管理者とクラウドのアカウントの多要素認証、古いデータの削除

2026年10月は、国内で情報漏えいの公表が途切れなく続いた1か月でした。ブックオフ、スカイチケット、カプコン、焼肉きんぐ、バーガーキングなど、身近なサービスの会員情報が数百万件単位で漏えいしたほか、防災メールの配信サービスやクラウド事業者への攻撃が、自治体や警察、数百の企業に波及しました。月末にはGMOインターネットグループのクラウドサービスを狙った恐喝事件が続き、21日にはPHPの重大な脆弱性への対応で、国内外の多くのサイトが一斉に止まりました。

この記事では、当サイトが報じた34件に、各組織の公表資料などで確認した事案を加えた国内130件を一覧にし、どのような攻撃や事案が多かったのかを整理します。記事の末尾に、全件の一覧表を載せています。

## 数字で見る10月

個人情報保護委員会が10月28日の委員会で示した資料によると、不正アクセスによる個人データの漏えい等の報告は、**10月1日から16日までの半月だけで830件**にのぼりました。9月1か月分（303件）の約2.7倍です。このうち、漏えい等した本人数が1,000万人を超える報告が4件、100万人超1,000万人以下が18件ありました。4月1日から10月16日までに漏えい等した延べ本人数は約2億6,000万人とされています（速報時点の数字で、金融業や電気通信業など委任先の省庁を経由した報告や、行政機関の報告は含みません）。

以下は、当サイトの報道と各組織の公表資料などで確認した事案を、主な手口で分けたものです。

| 主な手口 | 件数 | 代表的な事案 |
|---|---|---|
| Webサイト・アプリへの不正アクセス | 75件 | 良品計画（MUJIアプリ）、ブックオフ、スカイチケット、カプコン、焼肉きんぐ、バーガーキング、花キュービット、リクルート、ローソン、So-net、松屋 |
| 委託先・SaaS・クラウド経由 | 29件 | IDCFクラウド、アルカディア、ユミルリンク、Studio、ショップサーブ、コミューン、NECの委託先、アマデウス（JAL・ANA）、NTTデータの委託先 |
| 認証情報・アカウントの悪用 | 17件 | 日本経済新聞社、デジタルアーツ、楽天ドライブ、日本郵政、富士急ハイランド、大学のメールアカウント |
| ランサムウェア・恐喝 | 9件 | GMOインターネット、大阪公立大学、小池酸素工業、佐賀大学、丸木医科器械 |

分類は、公表資料から読み取れる主な手口で1つに決めたもので、厳密なものではありません。たとえばIDCFクラウドや釧路市、小平市の事案はランサムウェアによるものですが、被害が委託先や利用組織に広がった点を重視して「委託先・SaaS・クラウド経由」に入れています。ランサムウェアがかかわる事案は、表の分類以上に多いと考えてください。

100万件を超える個人情報の漏えい（可能性を含む）を公表した主な組織は次のとおりです。佐川急便（最大約5,323万件、重複を含む）やユミルリンク（延べ約5,163万件）、良品計画（MUJIアプリ、最大約2,726万件）、ソースネクスト（最大約2,252万件）、ショップサーブ（約2,335万人）のように、さらに大きな規模の事案もありました。

| 組織 | 公表された規模 |
|---|---|
| アドベンチャー（skyticket） | 約1,464万件 |
| カプコン（CAPCOM ID） | 1,177万4,247件 |
| バーガーキング公式アプリ | 約1,118万件 |
| 焼肉きんぐ公式アプリ | 1,078万8,963件 |
| 第一興商 | 最大約872万件 |
| ライドオンエクスプレスHD | 最大約650万件（可能性） |
| ブックオフ | 638万3,279人 |
| ふるさとチョイス | 445万4,097件 |

| 組織 | 公表された規模 |
| --- | --- |
| 手間いらず（宿泊予約） | 最大約445万人分 |
| ディップ（バイトル） | 最大388万件 |
| リクルート（カーセンサー） | 最大370万9,551件 |
| 松屋 | 237万7,127件ほか |
| アンドエスティHD | 約250万件ほか |
| ローソン（ローソンID） | 215万5,345件 |
| So-net | 214万1,986件ほか |
| 日本経済新聞社 | 約183万件 |
| ミスターマックス | 最大173万人 |
| ファインズ（予約システム） | 153万6,322件 |
| H2Oリテイリング | 約126万件 |
| 花キューピット | 423万8,242件 |

## 傾向1：アプリとECの「会員情報」が、100万件単位で漏れた

最も多かったのは、Webサイトやスマートフォンアプリへの不正アクセスで、75件にのぼります。特徴的なのは、外食チェーンや小売、チケット販売などの**公式アプリの会員情報**が、まとめて取得された事案が多いことです。焼肉きんぐのアプリでは約1,081万件の登録のうち1,079万件が、バーガーキングのアプリでは約1,118万件が対象になりました。月末には、松屋のモバイルオーダーなどの利用者約237万件、花キューピットの会員約424万件の漏えいが公表され、10月30日には良品計画が「MUJIアプリ」の最大約2,726万件（メールアドレス、生年月日、性別）の流出の可能性を公表しました。10月に公表されたアプリの会員情報の事案では、最大の規模です。

原因の詳細は多くが調査中か非公表ですが、公表された範囲では、アプリやWebの**正規の機能を悪用された**例が目立ちます。ローソンは利用者本人に情報を表示する仕組みを突破され、ネットプロテクションズ（NP後払い）やアエナでは機械的な連続アクセスで情報が取得されました。ニモカでは利用履歴を送る自動送信の機能が悪用されています。NICTは、公開されたアプリを解析して裏側のサーバーを狙う手口を「A2B攻撃」と名付けて注意を呼びかけています（関連記事）。

もう一つの共通点は、**持たなくてよいデータ、消し忘れたデータ**が被害を広げたことです。スカイチケットは、不要になった後も削除せずにクラウドに残していたデータベースのバックアップから、返金先の口座情報などが読み取られました。ソースネクストは、パスワードを復号できる形で保管していたため、復号された状態で流出しました。

## 傾向2：委託先・SaaSを経由した「連鎖」

委託先やSaaS、クラウドへの攻撃が、その利用組織に波及した事案は29件ありました。1社への侵入で影響が広がる規模は、ほかの手口とは桁が違います。

- **IDCFクラウド**：ランサムウェアの被害が495の企業・自治体に及んだ。原因は認証システムのOSSの脆弱性で、修正版を適用する前に侵入された
- **アルカディア「SpeeCAN RAIDEN」**：自治体の防災メールの配信基盤が狙われ、22府県警の職員情報にも波及。配信基盤から142万通を超えるフィッシングメールが送られた
- **ユミルリンク「Cuenote」**：メール配信サービスを通じて、50システム、延べ約5,163万件が対象に
- **Studio、コミューン、ショップサーブ**：サイト制作、コミュニティ、ECの基盤が狙われ、デジタル庁を含む約100の組織や、7,858の店舗に影響が出た
- **スカラコミュニケーションズ、トレードワークス**：フォームや証券システムの委託先への攻撃で、大和証券、シチズン時計、岩井コスモ証券などが影響を公表
- **NECの再委託先**：再委託先の正規アカウントが盗まれ、大阪公立大学など複数の顧客のシステムに被害が及んだ
- **月末にも連鎖が続いた**：予約システムを提供するアマデウスへの不正アクセスで日本航空・JTA（約9万2,000人分）と全日本空輸が、NTTデータの委託先の「デジタル証券プラットフォーム」への不正アクセスで近鉄グループHDの社債購入者の情報が、ライフネット生命の連携システムの脆弱性でKDDIの顧客情報（最大2万2,541件）が、それぞれ漏えいの可能性を公表した

利用組織から見ると、自社のシステムは何も変えていないのに、ある日「委託先が攻撃を受けた」と連絡が来る形です。第一興商（約872万件）やライドオンエクスプレス（最大約650万件）のように、自社のデータを預けていた委託先の被害で、大規模な漏えいの可能性を公表せざるを得なかった例もありました。

## 傾向3：盗まれた認証情報で「正面から」入られる

IDやパスワード、クラウドの認証情報を盗まれ、正規のアカウントで入られた事案は17件でした。日本経済新聞社は開発用クラウドの認証情報を窃取され、約183万件が漏えいしました。デジタルアーツはクラウド運用用の認証情報を盗まれ、痕跡は1年以上前までさかのぼるとしています。楽天ドライブでは管理用アカウントの認証情報が悪用されました。

メールアカウントの乗っ取りも続きました。日本経済新聞社の社員のアカウントから約9,000件のなりすましメールが送られ、それをきっかけに日経BPの社員も認証情報を盗まれています。大学ではフィッシングで乗っ取られたアカウントから迷惑メールが大量に送られました。日本郵政や富士急ハイランドでは、ほかのサービスから流出したIDとパスワードを使う「リスト型攻撃」で不正ログインされています。

正規のアカウントによるアクセスは、外から見ると普段の業務と区別がつきにくく、発見が遅れがちです。逆に、アンドエスティHDは侵入から約2時間半で不正な操作を検知し、サーバーを隔離しました。**入られた後に早く気づけるかどうか**が、被害の大きさを分けています。

## 傾向4：ランサムウェアと恐喝は「業務停止」と「注目」を武器に

ランサムウェアや恐喝の被害では、情報の漏えいだけでなく、業務が止まる影響が目立ちました。小池酸素工業はシステム障害で決算業務が遅れ、中間決算の発表を延期しました（法定期限を超える見込み）。医療

機器卸の丸木医科器械は基幹システムが止まり、受注と出荷ができなくなりました。大阪公立大学はサーバー約500台が停止し、約1週間休講しています。

GMOインターネットグループのクラウドサービスをめぐる事件では、攻撃者が約80億円を要求し、情報を少しずつ公開すると予告して注目を集め続けました。SNSでの盛り上がりそのものが恐喝の圧力になる構図は、当サイトのコラムで詳しく考察しています。

## 10月のそのほかの動き

- **PHPの重大な脆弱性と一斉停止**：10月21日に修正版が公開されたPHPの脆弱性では、高市総理が対応を呼びかけ、国内外で多くの組織がサイトやサービスを予防的に止めた（関連記事）
- **国の注意喚起と相談窓口**：相次ぐ不正アクセスを受け、国家サイバー統括室とIPAが注意喚起を出し、IPAは「不正アクセス特別相談窓口」を開設した（関連記事）
- **AIを使った攻撃の観測**：国内サイトでAIエージェントによるとみられる攻撃が観測された（関連記事）。韓国の金融機関を狙った攻撃では、AIで作成した履歴書が容疑者の手掛かりになった（関連記事）。攻撃の速さと量が増す前提で備える必要がある
- **海外では暗号資産取引所の巨額被害**：Binanceが10月30日、推定約63億ドル規模の不正出金を公表した。開発・運用担当者のノートPCが侵害され、そこからサービスを動かすシステムに入り込まれた可能性があるという（ITmedia NEWS）

## 11月に企業がまずやるべきこと

10月の事案から見えるのは、特別な攻撃よりも、**委託先、認証情報、公開しているアプリ、古いデータ**という基本的な部分の弱さを突かれた例が多いことです。次の点から点検することをおすすめします。

| 点検すること | 10月の事案との関係 |
| --- | --- |
| 委託先とSaaSの棚卸し | どの委託先・SaaSに、どの個人情報を預けているか。再委託先まで含めて、誰が自社のシステムに入れるアカウントを持っているか |
| 公開しているアプリ・APIの点検 | 本人確認や表示の仕組み、自動送信の機能、連続アクセスへの制限が、悪用に耐えられるか |
| 管理者・クラウドのアカウント | 多要素認証の徹底、使っていないアカウントの削除、クラウドの認証情報やアクセスキーの定期的な更新 |
| 古いデータとバックアップ | 不要になったデータやバックアップ、変更履歴のログが残っていないか。パスワードは復元できない方式で保管しているか |
| 脆弱性への対応の速さ | 修正版が出てから適用するまでの日数。すぐに適用できない場合の代わりの手段（停止、アクセス制限） |
| 入られた後に気づく仕組み | 通常と異なる大量のデータアクセスや、深夜の管理操作を検知して、すぐに止められるか |

## 2026年10月の事案一覧（国内130件）

公表日の順に並べています。公表日が複数あるものは、主な公表の期間を記しました。「当サイト記事」のリンク先では、続報を含めて詳しく伝えています。表は横にスクロールできます。

| 公表日 | 組織（業種） | 主な手口 | 規模・影響 | 原因・経路 | 出典 |
|---|---|---|---|---|---|
| 10/1〜10/23 | 佐川急便<br>物流 | Webサイト・アプリへの不正アクセス | 最大約5,323万件（重複含む）の個人情報が流出の可能性（第5報） | Webサイト「お荷物問い合わせサービス」への不正アクセス | 当サイト記事 |
| 10/01 | 日本原子力研究開発機構（JAEA）<br>研究機関 | Webサイト・アプリへの不正アクセス | 研究支援サイトのファイル2,419件が不正ダウンロード。個人情報を含むファイル367件・175人（マイナンバーを含む人6名）。10/30の追記で369件・7名に更新 | クラウド上の研究支援サイトへの外部からの不正アクセス（手口は非公表） | 公表資料 |
| 10/01 | スターツ出版「オズモール」第2報（初報9/27）<br>出版・Web | Webサイト・アプリへの不正アクセス | 最大442,779名分（メールアドレス、一部は氏名・都道府県） | 海外からの大量アクセス。脆弱性は特定・対策済みだが詳細は非公表 | 公表資料 |
| 10/01 | ニッポンレンタカーサービス アプリ 第2報（初報9/26）<br>レンタカー | Webサイト・アプリへの不正アクセス | 会員55名。カード登録会員は免許証情報・カード番号下4桁も対象 | 9/19〜21の外部攻撃（手法は非公表） | 公表資料 |
| 10/01 | ローソン（メールサーバの不正利用）<br>小売 | 認証情報・アカウントの悪用 | 9/25〜27に英文の不審メール約70万通（推計）を送信。情報漏えいは確認されていない | 第三者によるメールサーバの不正利用。原因は調査中 | 公表資料 |
| 10/01 | らしんばん<br>中古品販売 | Webサイト・アプリへの不正アクセス | 個別に連絡した顧客（件数は非公表）。氏名・住所・身分証の番号・買取時の口座など | 9/14〜16の第三者による不正アクセス。経路は調査中 | 公表資料 |
| 10/2 | 日本エネルギー経済研究所<br>研究機関 | 認証情報・アカウントの悪用 | パスポート情報13件の漏えいを確認 | フィッシングで所員6名のM365アカウントが侵害 | 当サイト記事 |
| 10/2 | 池上通信機<br>製造 | ランサムウェア・恐喝 | 攻撃者のリークサイトで同社の情報の公開を確認（第3報） | ランサムウェア集団がデータ窃取を主張 | 当サイト記事 |
| 10/2〜10/21 | 大阪公立大学<br>大学 | ランサムウェア・恐喝 | サーバー約500台が停止、約13万件に流出の可能性。NECのクラウドストレージからも情報漏えい | 保守委託先NECの再委託先の正規アカウントが悪用された | 当サイト記事 |
| 10/02 | 第一ライフグループ・第一生命保険<br>保険 | Webサイト・アプリへの不正アクセス | 約12万名（従業員・退職者など）。顧客情報へのアクセスは確認されていない | 第三者による不正アクセス（9/24検知） | 公表資料 |
| 10/02 | エネルギー・金属鉱物資源機構（JOGMEC）<br>独立行政法人 | Webサイト・アプリへの不正アクセス | メールアドレス約8,500件（役職員約1,100、外部約7,400） | 外部からの不正アクセス。9/9に外部機関からの情報提供で判明 | 公表資料 |
| 10/02 | ジャパンタイムズ（グループ会社）<br>新聞・出版 | Webサイト・アプリへの不正アクセス | グループ会社のサーバの一部。漏えいの有無は調査中。電子版・購読者DBへの影響なし | 不明 | 公表資料 |

| 公表日 | 組織（業種） | 主な手口 | 規模・影響 | 原因・経路 | 出典 |
|---|---|---|---|---|---|
| 10/02 | サミーネットワークス「777CON-PASS」<br>オンライン抽選（遊技関連） | Webサイト・アプリへの不正アクセス | 件数は調査中（電話番号の一部・生年月日・ユーザーIDなど） | 9/25・9/30の不正リクエスト。経路は調査中 | 公表資料 |
| 10/02 | セーファーインターネット協会<br>一般社団法人 | 委託先・SaaS・クラウド経由 | 件数は不明（氏名・メールアドレス・通報内容など） | さくらのレンタルサーバでの事案に起因 | 公表資料 |
| 10/02 | 講談社BECK<br>出版 | 認証情報・アカウントの悪用 | 9/14に不審メール50件を送信 | 認証情報の窃取とみられる（報道） | 報道 |
| 10/03（10/09に続報） | アバハウスインターナショナル<br>アパレル（EC） | 認証情報・アカウントの悪用 | 会員・受注情報。件数は不明。なりすまし返金メールを確認 | 社内システムへの不正ログインを起点に不正プログラムを設置し、DBが侵害された | 公表資料 |
| 10/03 | エスケーロジ 第2報（初報9/24）<br>物流 | ランサムウェア・恐喝 | 社内情報の一部が漏えい。件数は不明 | 不明 | 公表資料 |
| 10/04 | 日本経済新聞社（M365）<br>報道 | 認証情報・アカウントの悪用 | 9/30になりすましメール約9,000件を送信 | 社員のM365アカウントに不正ログイン | 公表資料 |
| 10/04 | 日経BP<br>出版 | 認証情報・アカウントの悪用 | 26人の氏名・メールアドレス | 日経社員を装ったフィッシングで認証情報を窃取された | 公表資料 |
| 10/05 | 物語コーポレーション「焼肉きんぐ」公式アプリ<br>外食 | Webサイト・アプリへの不正アクセス | 10,808,784件中10,788,963件（会員番号・氏名・メール・電話） | 10/2からの断続的な外部アクセス。経緯は調査中 | 公表資料 |
| 10/05 | 大和証券（委託先スカラコミュニケーションズ）<br>証券 | 委託先・SaaS・クラウド経由 | 約11万名、合計約22万件。自社システムへの侵害はなし | 委託先サーバへの不正アクセス（10/2夜〜10/3朝） | 公表資料 |
| 10/05 | 大起水産 公式アプリ<br>外食（回転ずし） | Webサイト・アプリへの不正アクセス | 174,933人（退会者を含む） | 第三者による不正アクセス（9/15判明）。経路は非公表 | 公表資料 |
| 10/05 | セイコーマートアプリ 第4報（初報9/29）<br>小売 | Webサイト・アプリへの不正アクセス | 対象を574,647人に確定 | アプリサーバ経由で会員情報サーバへ不正アクセス | 公表資料 |
| 10/05（10/14に第2報） | GMOリサーチ＆AI「infoQ」<br>アンケートサイト | Webサイト・アプリへの不正アクセス | 第1報は最大948,498件、第2報で894,082件の持ち出しを確定。ポイント不正交換611件・2,869,500円分 | ソフトウェアの脆弱性を悪用（名称は非公表） | 公表資料 |
| 10/05（10/13に調査結果） | くふうカンパニー「くふう まちトークβ版」<br>Webサービス | Webサイト・アプリへの不正アクセス | 308人の生年月日・性別が閲覧できる状態（うち1人はメールアドレスも取得された） | システムの脆弱性の悪用 | 公表資料 |
| 10/6 | 関西国際大学<br>大学 | Webサイト・アプリへの不正アクセス | 学修記録の複数ファイルが外部に流出した可能性 | 不正アクセス（経路は非公表） | 当サイト記事 |

| 公表日 | 組織（業種） | 主な手口 | 規模・影響 | 原因・経路 | 出典 |
|---|---|---|---|---|---|
| 10/6 | ミスターマックス<br>小売 | Webサイト・アプリへの不正アクセス | 最大173万人分の会員情報 | 不正アクセス | 当サイト記事 |
| 10/6〜10/21 | 小池酸素工業<br>製造 | ランサムウェア・恐喝 | 流出の疑いがあるファイルがネット上に公開。中間決算の発表を延期 | サイバー攻撃によるシステム障害 | 当サイト記事 |
| 10/06 | 旭化成セラピューティクス（医療関係者向けサイト）<br>医薬品 | 委託先・SaaS・クラウド経由 | 医療従事者 最大約51.4万人（うち約4.4万人はメールアドレスあり）、従業員約700人。公式の数字（報道では約55.8万人） | 委託先・医薬情報ネットの会員DBへのサイバー攻撃 | 公表資料 |
| 10/06 | シチズン時計<br>精密機器 | 委託先・SaaS・クラウド経由 | 約10万人（問い合わせフォームに入力された情報） | フォーム提供元スカラコミュニケーションズのサーバへの不正アクセス（大和証券と同じ委託先） | 公表資料 |
| 10/06（10/08更新） | 楽天ドライブ（楽天モバイル）<br>通信・クラウドストレージ | 認証情報・アカウントの悪用 | 687件と313件のアカウント情報、15,382アカウントで保存ファイルが閲覧された | 管理用アカウントの認証情報を不正に取得・悪用された | 公表資料 |
| 10/06（PDFの日付） | ニモカ（nimoca）<br>交通系IC | Webサイト・アプリへの不正アクセス | 521件（カード番号・生年月日・メールアドレス）。10/15に再開 | 利用履歴照会サービスの自動送信機能が悪用された | 公表資料 |
| 10/07 | エイチ・アイ・エス（タイ子会社）<br>旅行 | Webサイト・アプリへの不正アクセス | 最大627人分のパスポート情報 | 経路は不明。検知は2025/12/11で、公表まで約10か月 | 公表資料 |
| 10/07 | 戸田建設<br>建設 | Webサイト・アプリへの不正アクセス | 取引先メールアドレス最大7,200件、取引データ最大6,000件、従業員4,778人分（件数は報道による） | 支払管理システムへの外部からの侵入（10/1〜5） | 報道 |
| 10/07（10/8・10/13に続報） | ライドオンエクスプレスHD（銀のさら・釜寅等）<br>外食（宅配） | 委託先・SaaS・クラウド経由 | 最大約650万件。流出の痕跡は未確認で、データは復旧不能 | サーバ運営会社（名称非公表）へのランサムウェア攻撃 | 公表資料 |
| 10/07（10/09に適時開示） | 手間いらず「TEMAIRAZU」（サイトコントローラー）<br>宿泊向けSaaS | 委託先・SaaS・クラウド経由 | 最大約445万人分の宿泊予約情報 | 旧インストール型サービスの一部機能にあったセキュリティ上の問題 | 公表資料 |
| 10/8 | 第一興商<br>エンタメ | 委託先・SaaS・クラウド経由 | 顧客・従業員の最大約872万件 | 委託先の従業員端末がマルウェアに感染 | 当サイト記事 |
| 10/08 | ローソン（ローソンID）<br>小売 | Webサイト・アプリへの不正アクセス | ローソンID 2,155,345件、アプリ予約26件（カード番号の一部を含む）。10/24の訂正でメールアドレスは対象外に | 本人情報を表示する仕組みを突破された（9/12〜14、9/17） | 公表資料 |
| 10/08 | 修道学園 第2報（初報9/30）<br>教育 | Webサイト・アプリへの不正アクセス | 取引先の口座情報、教職員・外部講師の個人情報（件数は不明）。学生の情報は含まれない | 管理サーバへの不正アクセス。原因は調査中 | 公表資料 |

| 公表日 | 組織（業種） | 主な手口 | 規模・影響 | 原因・経路 | 出典 |
|---|---|---|---|---|---|
| 10/9〜10/23 | ブックオフグループHD<br>小売 | Webサイト・アプリへの不正アクセス | 会員638万3,279人（会員データ642万7,735件） | 会員管理システムへの不正アクセス | 当サイト記事 |
| 10/9〜10/28 | アドベンチャー（skyticket）<br>旅行 | Webサイト・アプリへの不正アクセス | 約1,464万件。その後、カード情報や返金先口座32,341件の流出も判明 | 削除せずに残していたDBのバックアップなどが読み取られた | 当サイト記事 |
| 10/9〜10/21 | コミューン<br>SaaS | 委託先・SaaS・クラウド経由 | 延べ16万6,505人。ヤマハ、スズキなど導入企業のコミュニティに波及 | 招待リンクの不正入手と署名鍵の悪用 | 当サイト記事 |
| 10/9 | ディップ（バイトル）<br>人材 | Webサイト・アプリへの不正アクセス | 最大388万件のメールアドレス | 不正アクセス | 当サイト記事 |
| 10/9 | 穴吹ハウジングサービス<br>不動産 | ランサムウェア・恐喝 | オーナーズサイトを一時停止 | ランサムウェア | 当サイト記事 |
| 10/09 | リゾートトラスト<br>会員制リゾート | Webサイト・アプリへの不正アクセス | 会員情報 約2万6,000件 | Webサイトのシステムで異常動作（10/5）。経路は不明 | 公表資料 |
| 10/09 | ココナラ（スキルマーケット）<br>オンラインサービス | Webサイト・アプリへの不正アクセス | 履歴書449件、職務経歴書関連書類1,845件を持ち出された | 10/8に不正アクセス。同日、脆弱性を修正（詳細は非公表） | 公表資料 |
| 10/13 | Fivot（IDARE）<br>決済 | Webサイト・アプリへの不正アクセス | 12万9,659人。残高・取引履歴も対象 | 業務用の外部ソフトウェアの脆弱性 | 当サイト記事 |
| 10/13 | NEXT STAGE<br>建設関連 | Webサイト・アプリへの不正アクセス | 取引先など最大約4万件 | 業務用BIツール（Metabase）のアカウントの不正利用 | 当サイト記事 |
| 10/13〜10/30 | アルカディア（SpeeCAN RAIDEN）<br>防災配信SaaS | 委託先・SaaS・クラウド経由 | メールアドレス最大約313万件（推定）。22府県警にも波及。142万通の不正メール配信 | 配信サービスへの不正アクセス | 当サイト記事 |
| 10/14 | アエナ ECアプリ<br>小売 | Webサイト・アプリへの不正アクセス | 最大817,215人（カード名義・下4桁・有効期限を含む） | 機械的な連続アクセス。詳細は調査中 | 公表資料 |
| 10/14 | 東産業 公式サイト（初報9/14）<br>製造 | Webサイト・アプリへの不正アクセス | 問い合わせフォームの顧客情報（件数の記載なし） | WordPressとサーバ側の脆弱性（報道ではwp2shell） | 公表資料 |
| 10/14 | トイポ「トイポアプリ」<br>アプリ運営 | Webサイト・アプリへの不正アクセス | 697,209名の登録情報 | 他ユーザーの情報を取得できる脆弱性 | 公表資料 |
| 10/14 | 札幌国際大学<br>教育 | 認証情報・アカウントの悪用 | 複数のアカウントが乗っ取られ、フィッシングメールを大量に送信 | 7/9以降のフィッシングで偽サイトに認証情報を入力した | 公表資料 |
| 10/14 | スズキ二輪「スズキワールド」<br>二輪販売 | Webサイト・アプリへの不正アクセス | 問い合わせフォームの個人情報 約4,400件 | 不明（7/29に検知） | 公表資料 |

| 公表日 | 組織（業種） | 主な手口 | 規模・影響 | 原因・経路 | 出典 |
|---|---|---|---|---|---|
| 10/15 | ACCESS（台湾子会社CROS）<br>IT | Webサイト・アプリへの不正アクセス | 越境EC利用者15万件超。セキュリティコードを含むカード情報も流出 | 不正アクセス | 当サイト記事 |
| 10/15 | ビーケー・ジャパン（バーガーキング）<br>外食 | Webサイト・アプリへの不正アクセス | 公式アプリの会員情報約1,118万件 | 不正アクセス | 当サイト記事 |
| 10/15 | ビューティガレージ<br>EC | Webサイト・アプリへの不正アクセス | 顧客情報77万5,725件の外部流出を確認 | ECサーバーへの不正アクセス | 当サイト記事 |
| 10/15 | ソースネクスト<br>ソフトウェア | Webサイト・アプリへの不正アクセス | 最大2,251万9,960件。パスワードが復号された状態で流出 | 復号鍵にアクセスできるAPIへの不正アクセス | 当サイト記事 |
| 10/15 | 釧路市<br>自治体 | 委託先・SaaS・クラウド経由 | 児童生徒・教職員のアカウント情報や全39校の管理用パスワード | 学習用端末の委託先がランサムウェア被害 | 当サイト記事 |
| 10/15 | エムスリー「MR君」<br>医療IT | Webサイト・アプリへの不正アクセス | 医師会員の1割未満と製薬企業担当者数百名 | 不明 | 公表資料 |
| 10/15 | 丸木医科器械<br>医療機器卸 | ランサムウェア・恐喝 | 基幹システムが停止し、受注・出荷も停止 | 不明 | 公表資料 |
| 10/15〜18（第1〜3報） | NTTソルマーレ「コミックシーモア」<br>電子書籍 | Webサイト・アプリへの不正アクセス | 会員情報の流出を確認（件数は精査中） | 原因は特定済みとするが非公表 | 公表資料 |
| 10/16 | ヤマト運輸<br>物流 | Webサイト・アプリへの不正アクセス | クロネコ代金後払いサービスの購入者情報など計約531万件 | 後払いサービスへの不正アクセス | 当サイト記事 |
| 10/16 | 小平市<br>自治体 | 委託先・SaaS・クラウド経由 | 公式サイトが閲覧不能。フォーム入力情報に漏えいのおそれ | 保守委託先が使うクラウド基盤がランサムウェア被害 | 当サイト記事 |
| 10/16 | Eストアー（ショップサーブ）<br>EC基盤 | 委託先・SaaS・クラウド経由 | 最終報で約2,335万人・7,858店舗。カード情報の一部は約209万人分 | EC構築サービスへの不正アクセス | 当サイト記事 |
| 10/16 | ファンケル／アテニア<br>化粧品通販 | Webサイト・アプリへの不正アクセス | ファンケル会員368,184名、アテニア会員417,312名 | ECサイトの特定機能の悪用（10/3〜10） | 公表資料 |
| 10/16 | ゴルフダイジェスト・オンライン<br>EC・メディア | Webサイト・アプリへの不正アクセス | 従業員・委託先等1,789件の流出を確認、顧客55件が照会された可能性 | 侵害された別サーバを経由した照会 | 公表資料 |
| 10/16（10/20に第2報） | 岩井コスモ証券（委託先トレードワークス）<br>証券 | 委託先・SaaS・クラウド経由 | 4,975名（第2報で364名追加）。7口座で意図しない注文があり、5口座で約定（原状回復済み） | 委託先のシステムへの不正アクセス | 公表資料 |
| 10/16 | 三井住友DSアセットマネジメント「投信直販ネット」<br>資産運用 | 委託先・SaaS・クラウド経由 | マイページが停止。口座・取引への影響は確認されていない | 取引委託業者のシステムへの不正アクセス | 公表資料 |

| 公表日 | 組織（業種） | 主な手口 | 規模・影響 | 原因・経路 | 出典 |
|---|---|---|---|---|---|
| 10/16・10/19 | 日本郵政（ゆうゆうポイントサイト／ゆうID）<br>郵政 | 認証情報・アカウントの悪用 | 10/16にサイトを緊急停止。10/19公表でゆうID 249アカウント・住所録83件 | 外部で入手されたID・パスワードの利用 | 公表資料 |
| 10/16・10/19・10/29追記 | ファインズ（予約システム、初報9/25）<br>IT | 委託先・SaaS・クラウド経由 | 予約者情報1,536,322件 | 入力処理の不備を悪用され、不正な管理者アカウントで取得された（原因を10月に初めて開示） | 報道 |
| 10/16 | 日本経済新聞社（開発用クラウド）<br>報道 | 認証情報・アカウントの悪用 | 約183万件（個人情報約15万件、識別子のみ約168万件） | 開発用クラウドの認証情報を窃取された（10/7） | 公表資料 |
| 10/17（10/19に第2報） | セカンドリテイリング<br>リユース小売 | Webサイト・アプリへの不正アクセス | 外部への漏えいは確認されていない | 社内システムへの侵入（10/15確認） | 公表資料 |
| 10/19 | ニフティ<br>ISP | Webサイト・アプリへの不正アクセス | 最大542,513件 | 回線申込・受付管理システムへの外部からのアクセス | 公表資料 |
| 10/19 | Z会「Z-IDシステム」<br>教育 | 認証情報・アカウントの悪用 | 13アカウント | パスワードリセット機能を短時間に連続操作された | 公表資料 |
| 10/19 | パピレス「Renta!」<br>電子書籍 | Webサイト・アプリへの不正アクセス | サービスを一時停止。件数は不明 | 調査中 | 公表資料 |
| 10/19 | エンタッチ（東邦HD子会社）<br>医療DX | ランサムウェア・恐喝 | 医療従事者等の氏名・メール・予約情報など。件数は調査中 | DBへの不正アクセス（10/9）。経路は不明 | 公表資料 |
| 10/19 | エイチ・ツー・オーリテイリング（阪急・阪神百貨店予約サイト）<br>百貨店 | Webサイト・アプリへの不正アクセス | H2O ID 約126万件 | 予約サイトを経由して顧客管理システムへ侵入 | 公表資料 |
| 10/19（10/20に第2報） | リンクステーション「GETTIIS」<br>チケット販売 | Webサイト・アプリへの不正アクセス | 会員ID 317,971件、ハッシュ化パスワード311,451件、カード関連情報（一部・暗号化）29,515件 | 主催者向け「Gettii-Lite」の脆弱性の悪用 | 公表資料 |
| 10/19〜10/30 | クリプトン（SONICWIRE、D2R）<br>音楽ソフト販売 | Webサイト・アプリへの不正アクセス | 36万2,137件（氏名、メールアドレス、ハッシュ化パスワード）ほか | 第三者による不正アクセス | 公表資料 |
| 10/20 | トラストバンク（ふるさとチョイス）<br>Webサービス | Webサイト・アプリへの不正アクセス | 会員情報445万4,097件。寄附控除の試算額も | 不正アクセス | 当サイト記事 |
| 10/20 | NEC（委託先へのサイバー攻撃）<br>ITサービス | 委託先・SaaS・クラウド経由 | 複数の顧客でシステム障害と個人情報の流出。件数は非公表 | 委託先の正規アカウントの認証情報を窃取された（9月下旬） | 公表資料 |
| 10/20 | フジテレビジョン<br>放送 | Webサイト・アプリへの不正アクセス | メディア関係者 最大730件 | 番組宣伝システムへの不正アクセス（10/19夜） | 公表資料 |

| 公表日 | 組織（業種） | 主な手口 | 規模・影響 | 原因・経路 | 出典 |
|---|---|---|---|---|---|
| 10/20 | 国土交通省・経済産業省・環境省（住宅省エネキャンペーン事務局、運営は博報堂）<br>官公庁（委託） | 委託先・SaaS・クラウド経由 | 16,950事業者・23,918名（速報値） | 委託先システムでの外部からの不正操作 | 公表資料 |
| 10/20 | 富士急ハイランド「CLUB フジQ」<br>レジャー | 認証情報・アカウントの悪用 | 159名（一部はカード番号の一部を含む） | 外部で入手されたID・パスワードの組み合わせ（9/4〜7） | 公表資料 |
| 10/20 | メドレー「@link」<br>医療IT | Webサイト・アプリへの不正アクセス | サービスを一時停止。個人情報への影響は調査中 | 不明 | 公表資料 |
| 10/21〜 | GMOインターネット（お名前.com デスクトップクラウド）<br>クラウド | ランサムウェア・恐喝 | 情報の持ち出しを確認。攻撃者が約80億円を要求し、情報を公開 | 不正アクセス（侵入経路は非公表） | 当サイト記事 |
| 10/21 | リクルート「カーセンサーnet」「C-MATCH」<br>情報サービス | Webサイト・アプリへの不正アクセス | 最大3,709,551件（カーセンサーnetの問い合わせ利用者3,210,421件など） | 第三者による不正アクセス。経路は調査中 | 公表資料 |
| 10/21 | ラクスライトクラウド「ブラストメール」（＋石油資源開発が影響を公表）<br>メール配信SaaS | 委託先・SaaS・クラウド経由 | 全契約者の情報と、一部顧客の配信先リスト | API用サーバ2台に侵入してコマンドを実行された | 公表資料 |
| 10/21 | デジタルアーツ<br>セキュリティ製品・SaaS | 認証情報・アカウントの悪用 | クラウド6サービスの一部顧客情報。件数は非公表 | クラウド運用用の認証情報を窃取された。痕跡は2025年7月頃まで遡る | 公表資料 |
| 10/21 | JFEケミカル（第一報）<br>化学 | Webサイト・アプリへの不正アクセス | 規模は調査中 | 不明（10/14に認識） | 公表資料 |
| 10/22〜10/23 | カプコン<br>ゲーム | Webサイト・アプリへの不正アクセス | CAPCOM ID 1,177万4,247件のメールアドレスなど | CAPCOM IDへの不正アクセス | 当サイト記事 |
| 10/22 | Studio（ノーコードサイト制作）<br>SaaS | 委託先・SaaS・クラウド経由 | デジタル庁（最大1万3,323件）など100近い組織が影響を公表 | サービスへの不正アクセス | 当サイト記事 |
| 10/22 | ネットプロテクションズ「NP後払い」<br>決済 | Webサイト・アプリへの不正アクセス | 取引28,884件分の氏名・住所 | 請求書再発行システムへの機械的な連続リクエスト | 公表資料 |
| 10/22 | 厚生労働省（委託先テクノヒル）<br>行政（委託） | 委託先・SaaS・クラウド経由 | 6名分のID・パスワードが漏えいし、不正ログインも確認。受講者最大595名 | 第三者によるサイバー攻撃 | 公表資料 |
| 10/23 | アンドエスティHD<br>アパレル | Webサイト・アプリへの不正アクセス | 顧客約250万件・取引先約1万件 | 業務サーバーへの不正アクセス。約2時間半で検知・隔離 | 当サイト記事 |

| 公表日 | 組織（業種） | 主な手口 | 規模・影響 | 原因・経路 | 出典 |
|---|---|---|---|---|---|
| 10/23〜10/30 | グッドスマイルカンパニー<br>EC | Webサイト・アプリへの不正アクセス | カード番号全桁など最大2,800名分。下4桁などは40万枚超 | 脆弱性を悪用され管理者権限を奪取、決済ページに不正プログラム | 当サイト記事 |
| 10/23 | ヤマダデンキ「ヤマダビデオ」「スマホゴールド会員」<br>家電小売 | Webサイト・アプリへの不正アクセス | サービスを一時停止。影響は調査中 | 外部からの不正アクセス | 公表資料 |
| 10/26 | ユミルリンク（Cuenote）<br>メール配信SaaS | 委託先・SaaS・クラウド経由 | 延べ5,162万8,280件、50システムに影響 | メール配信サービスへの不正アクセス | 当サイト記事 |
| 10/26 | 古河電工パワーシステムズ<br>製造 | Webサイト・アプリへの不正アクセス | 発注者・製品送付先の個人情報が閲覧された可能性 | 出荷管理Webシステムへの不正アクセスの疑い | 当サイト記事 |
| 10/26 | バンダイロジパル（バンダイナムコHD・BANDAI SPIRITS連名）<br>物流 | 認証情報・アカウントの悪用 | 「一番くじONLINE」の配送情報。件数は調査中 | 物流サーバの侵害、アカウントの不正利用（10/21発見） | 公表資料 |
| 10/26 | ドトールコーヒー<br>外食 | Webサイト・アプリへの不正アクセス | 都内4店舗の従業員・退職者951名（銀行口座番号を含む） | 外部の第三者による不正アクセス（10/20検知） | 公表資料 |
| 10/26 | Gunosy<br>ITメディア | 認証情報・アカウントの悪用 | 取引先25名、役職員・退職者107名 | 不正に入手された社内アカウントのID・パスワード | 公表資料 |
| 10/26 | 楽天グループ（Rakuten Travel Xchange／楽天トラベル多言語サイト）<br>旅行予約 | Webサイト・アプリへの不正アクセス | 海外サイトは予約者最大約4万件（うち支払い情報約3.6万件）、ログイン利用者最大約260万件 | 不明（9/10検知、多言語サイトは10/20検知） | 報道 |
| 10/26 | ギフティ（グループ子会社）<br>eギフト | Webサイト・アプリへの不正アクセス | 損失見込み約5.5億円。利用者への被害は確認されていない | システムの脆弱性の悪用 | 報道 |
| 10/27 | ソニーネットワークコミュニケーションズ「So-net」<br>ISP | Webサイト・アプリへの不正アクセス | So-net会員情報2,141,986件、plala（Sコース）会員情報443,495件、メールアドレスとパスワード54,401件ほか | 外部からの不正アクセス（10/19発生）。経路は調査中 | 公表資料 |
| 10/27 | 日本大学 更新版（初報9/14）<br>教育 | 認証情報・アカウントの悪用 | 教職員6名、不審メール計3,977件 | フィッシング等でID・パスワードを窃取されたとみられる | 公表資料 |
| 10/28 | 経済産業省（電力・ガス取引監視等委員会「デントリネット」）<br>行政 | Webサイト・アプリへの不正アクセス | サイトを停止。流出の有無は調査中 | 不明（10/27未明に発生） | 報道 |
| 10/28 | 花キューピット<br>生花EC | Webサイト・アプリへの不正アクセス | 会員423万8,242件（ユーザーID、メールアドレス、ハッシュ化パスワード） | 管理システムへの不正アクセス（10/14〜15） | 公表資料 |
| 10/28 | ソニー生命保険<br>保険 | Webサイト・アプリへの不正アクセス | 代理店として扱ったメディケア生命の契約情報 約38.5万件 | 契約者向けサイトなどへの不正アクセス | 公表資料 |

| 公表日 | 組織（業種） | 主な手口 | 規模・影響 | 原因・経路 | 出典 |
|---|---|---|---|---|---|
| 10/28〜10/29 | 日本航空・日本トランスオーシャン航空・全日本空輸<br>航空 | 委託先・SaaS・クラウド経由 | JAL・JTAは約9万2,000人分の予約情報（一部はパスポート番号も）。ANAは調査中 | 予約システムを提供するアマデウスへの不正アクセス | 報道 |
| 10/28 | ベネフィット・ワン（トク買）<br>福利厚生 | 委託先・SaaS・クラウド経由 | クレディセゾン会員向けサービスの2万9,465人 | 委託先フォレステックのシステムへの不正アクセス | 公表資料 |
| 10/28 | モイ（ツイキャス）<br>ライブ配信 | Webサイト・アプリへの不正アクセス | サービスとコーポレートサイトを緊急停止 | サーバーへの不正アクセスの痕跡を検知 | 公表資料 |
| 10/29 | 鹿児島銀行など4行庫（Payどん）<br>金融 | 委託先・SaaS・クラウド経由 | メール通知システムが保有する個人情報の一部に漏えいの可能性 | メール送信の委託先アララへの不正アクセス | 公表資料 |
| 10/29 | NEL（osina）<br>マーケティング | Webサイト・アプリへの不正アクセス | 23万5,329人。銀行口座情報やSNS連携用の認証情報も | 利用していたデータ分析ツールの脆弱性 | 公表資料 |
| 10/29 | クラブネッツ（CNポイント）<br>ポイントサービス | Webサイト・アプリへの不正アクセス | 会員IDと氏名1万6,936件、住所などを含む2,857件 | サテライトシステムへの不正アクセス | 公表資料 |
| 10/29 | 料理王国<br>出版 | Webサイト・アプリへの不正アクセス | 会員情報など約8,000件（延べ） | サーバー内のデータが外部から取得できる状態に | 公表資料 |
| 10/30 | 松屋フーズHD<br>外食 | Webサイト・アプリへの不正アクセス | 松弁ネットなどの利用者237万7,127件、アプリ会員最大3,000件 | 公式アプリの管理システムへの不正アクセス | 当サイト記事 |
| 10/30 | 佐賀大学（事務用NAS、前回9/28）<br>教育・附属病院 | ランサムウェア・恐喝 | 約8万人分の個人情報が流出した可能性。患者情報は調査中 | 9/24に被害を確認。経路は調査中 | 公表資料 |
| 10/30 | 日本交通（第6報）<br>交通 | Webサイト・アプリへの不正アクセス | 6区分で計約29万人（タクシー利用者の情報は含まない） | 7月11日の不正アクセス | 公表資料 |
| 10/30 | 良品計画（MUJIアプリ）<br>小売 | Webサイト・アプリへの不正アクセス | 最大約2,726万件（メールアドレス、生年月日、性別） | 公式アプリへの外部からの不正アクセス | 公表資料 |
| 10/30 | KDDI・ライフネット生命<br>通信・保険 | 委託先・SaaS・クラウド経由 | KDDIの顧客情報 最大2万2,541件 | ライフネット生命の連携システムの脆弱性 | 公表資料 |
| 10/30 | 東急不動産<br>不動産 | Webサイト・アプリへの不正アクセス | 自社管理サイトで4,082件、Studio利用サイトで25件 | WordPressなどの脆弱性とアクセス権限の設定不備。別にStudioへの不正アクセスの影響 | 公表資料 |
| 10/30 | コアデ（はにくじランド）<br>EC | Webサイト・アプリへの不正アクセス | 最大7,622名 | 不正なコマンド実行と認証情報の不正利用 | 公表資料 |
| 10/30 | 大都開発（かたしな高原）<br>レジャー | 認証情報・アカウントの悪用 | 253人の情報が閲覧されたおそれ。約3万800件にフィッシングメール | メール配信の委託先イグレックスの管理用アカウント情報で不正ログイン | 公表資料 |

| 公表日 | 組織（業種） | 主な手口 | 規模・影響 | 原因・経路 | 出典 |
|---|---|---|---|---|---|
| 10/30 | 日本製薬団体連合会など4団体<br>業界団体 | 委託先・SaaS・クラウド経由 | メールアドレス3万750件 | メール配信の委託先ユミルリンク（Cuenote）への不正アクセス | 公表資料 |
| 10/30 | 外務省<br>行政 | Webサイト・アプリへの不正アクセス | メールアドレスや氏名など約3,600件（うち約900件は省員以外）。機密性の高い情報が含まれていたことは確認されなかったとしている | 外部とやり取りできるネットワークへの不正アクセス（7月27日に検知） | 報道 |
| 10/30（第三報） | GMOグローバルサイン（GMOトラスト・ログイン）<br>認証SaaS | 委託先・SaaS・クラウド経由 | 利用企業2,492社・4万5,030人分の氏名やメールアドレスなど | ロゴ画像用の公開領域に顧客情報を含むファイルも保存する設計で、約9年間外部から取得できる状態だった | 報道 |
| 10月（第5〜7報） | IDCフロンティア（IDCFクラウド）<br>クラウド | 委託先・SaaS・クラウド経由 | 495の企業・自治体に影響。委託元のJR東海などにも波及 | ランサムウェア。認証システムのOSSの脆弱性を修正版の適用前に悪用 | 当サイト記事 |
| 10/31 | 近鉄グループホールディングス<br>鉄道 | 委託先・SaaS・クラウド経由 | 社債の購入者2,678件（氏名、購入金額） | NTTデータの委託先「デジタル証券プラットフォーム」への不正アクセス | 公表資料 |

## 海外の主な事案（10件）

| 公表日 | 組織（業種） | 規模・影響 | 原因・経路 | 出典 |
|---|---|---|---|---|
| 10/2 | Bitget（暗号資産取引所）<br>暗号資産 | 3億8,750万ドルが流出 | 第三者のセキュリティ製品のゼロデイ脆弱性 | 当サイト記事 |
| 10/7 | デンマーク 中央個人登録簿（CPR）<br>政府 | 約880万人分の氏名・住所・個人番号など | パスワード「123456」の民間IT企業経由で侵入か | 当サイト記事 |
| 10/14（テキサス州への届出） | CenterPoint Energy（米）<br>電力・ガス（重要インフラ） | テキサス州の届出で1,062,060人（全社の総数ではない）。攻撃者は約749万件と主張しているが、同社は確認していない | 外部公開システムの一つ（初報は9/14の8-K） | 報道 |
| 10/16 | フロリダ州 高速道路安全・自動車局（FLHSMV、米）<br>州政府（運転免許） | 現行の免許・IDの保有者に通知を開始。影響人数は非公表（攻撃側は20万件超と主張、未検証） | 地元警察署の利用者1名の認証情報が悪用された（9/4） | 公表資料 |
| 10/16頃 | ETS（Educational Testing Service、米）／カリフォルニア州教育省<br>教育（試験委託先） | 州内の在籍生 約570万人規模。2006年以降の記録を含み、総数は未公表 | 侵害された認証情報でSFTPに約4か月にわたり繰り返し侵入 | 報道 |
| 10/23頃 | Quest Diagnostics（米）<br>臨床検査 | 患者記録の一部（規模は調査中） | 顧客向けの「Quanum Lab Services Manager」への不正アクセス（10/21） | 報道 |

| 公表日 | 組織（業種） | 規模・影響 | 原因・経路 | 出典 |
|---|---|---|---|---|
| 10/27 | LiteLLM（OSS）<br>AI基盤 | 1.107.0に不正プログラムが混入 | ソフトウェアサプライチェーン攻撃 | 当サイト記事 |
| 10/30 | Binance（暗号資産取引所）<br>暗号資産 | 推定約63億ドル。約30億ドル分を凍結 | 開発・運用担当者のノートPCが侵害され、不正出金か | 報道 |
| 10月中旬 | 英国 法律扶助庁（Legal Aid Agency）<br>政府機関 | 盗まれた記録が1978年まで遡ると判明。件数は非公表 | 2025年4月の攻撃 | 報道 |
| 10月 | 韓国の金融機関<br>金融 | 16社・約10万件に拡大 | AIエージェント使用の可能性も | 当サイト記事 |

## よくある質問

### Q. 10月に公表された事案は、本当にこれですべてですか？

いいえ。本記事は、当サイトの報道と、各組織の公表資料やセキュリティ専門メディアで確認できたものをまとめたもので、自社サイトだけで告知された小規模な事案などは含まれていない可能性があります。メールの誤送信や記憶媒体の紛失などの事故も、今回の一覧からは除いています。

### Q. 件数を合計すると、何件の個人情報が漏えいしたことになりますか？

合計はしていません。各組織が公表する件数は、重複を含むもの、延べ人数のもの、漏えいの「可能性」の最大値などが混在しており、足し合わせると実態とかけ離れた数字になるためです。

### Q. 自分の情報が含まれているかは、どう確かめればよいですか？

多くの組織は、対象者にメールやSMSで個別に連絡するか、会員サイトに照会の仕組みを設けています。ただし、お詫びや補償を装ったフィッシングも増えます。メールやSMSのリンクからではなく、自分で開いた公式サイトや公式アプリで確認してください。

### Q. 中小企業も同じような被害に遭いますか？

遭います。今回の一覧でも、委託先やSaaSの被害に巻き込まれた組織の多くは、自社で特別なミスをしたわけではありません。自社がどのサービスに、どの情報を預けているかを把握しておくことが、被害を受けたときの初動の速さにつながります。

## まとめ

2026年10月は、国内で130件のサイバー攻撃・不正アクセスの事案が公表され、100万件を超える個人情報の漏えいが相次ぎました。手口としては、アプリやWebの仕組みを悪用した会員情報の取得、委託先やSaaSを経由した連鎖、盗まれた認証情報による正規アカウントでの侵入が中心で、ランサムウェアや恐喝は業務の停止という形で企業を追い込みました。

どの手口も、攻撃者にとって「最も手間のかからない入口」を狙っている点で共通しています。**委託先と預けている情報を把握する、アカウントを守る、使わないデータを持たない、入られたらすぐ気づく**。11月は、この基本をあらためて点検する月にしたいところです。


## 自社の「入口」と「預け先」を、外から点検してみませんか

サイバーセキュリティ総研では、外部から狙われやすい弱点を洗い出す脆弱性診断や、端末の24時間監視と初動対応を担うMDRを提供しています。「何から備えればよいか分からない」という段階からご相談いただけます。

**診断メニューを見る**　**無料で相談する（お問い合わせ）**


各事案の出典は、一覧表の「出典」欄に記しています。

参照：個人情報保護委員会「最近の不正アクセスによる個人データの漏えい等の傾向」（2026年10月28日参考資料2）／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」（当サイト記事）／国家サイバー統括室の注意喚起（当サイト記事）／Security NEXT／ScanNetSecurity

---


本資料は、上記Web版記事の2026年11月2日時点の内容をPDFにしたものです。最新の情報や訂正はWeb版をご確認ください。
© サイバーセキュリティ総研