

Atlas Support

CYBER RISK REPORT

相次ぐ個人情報流出、 AI時代のセキュリティを問い直す

公表資料40項目から考えるAI時代のセキュリティ



INCIDENT DIRECTORY / 選定10事例＋関連30事例

公表対象規模の延べ値 約5,770万件相当（単位混在）

インターネット企業をはじめ、幅広い業種で情報漏えい

CASE 08

10/5 公表・更新

GMOリサーチ & AI (infoQ) 最大約94.8万件

ソフトの脆弱性を悪用され、最大94万8,498件が対象となった。

ポイント不正交換611件・約287万円を確認し、交換機能を停止した。

CASE 02

10/13 第2報

ブックオフ 638万3,279人

会員データ642万7,735件が流出。対象者は638万3,279人。

ハッシュ化パスワードも対象。決済情報・本人確認画像は対象外。経路は未公表。

CASE 10

10/1 公表・更新

タイムズカー 約660万アカウント

約660万アカウントが流出し、約160万件には本人確認画像も含まれた。

退会者らにも通知し、専用窓口を設けた。

その他37項目

R29 可	<u>ヤマト運輸</u> 10/9 規模未公表	R25 可	<u>ニッポンレンタカー</u> 10/1 41人／別事案55人	R22 可	<u>LEGOLAND Japan</u> 9/25 参考 ホテル予約1,557件
R27 可	<u>佐川急便</u> 10/9 規模調査中	R24 可	<u>チケプラ</u> 10/1 最大107人	R14 確	<u>井筒まい泉</u> 9/25 参考 件数未公表
03 可	<u>手間いらず</u> 10/9 最大約445万人	R16 可	<u>OZmall</u> 10/1 最大44万2,779人	R12 確	<u>キューサイ</u> 9/25 参考 484人
01 確	<u>アドベンチャー / skyticket</u> 10/9 約1,464万件	R18 可	<u>Gポイント</u> 9/30 最大約7万件	R01 確	<u>Gyazo</u> 9/25 参考 約2,362万件
05 確	<u>ローソン</u> 10/8 215万5,345件（Lawson ID）	R09 確	<u>吉野家・はなまる</u> 9/30 応募4,998件／368件	R06 確	<u>ニチレイ</u> 9/18 参考 5万3,866件
04 可	<u>第一興商</u> 10/8 約872.4万件（対象範囲）	R08 確	<u>ベネフィット・ワン</u> 9/30 1万3,460人	R21 可	<u>@cosme</u> 9/16 参考 1万997人
07 確	<u>ミスターマックス</u> 10/6 最大173万5,154人	R13 確	<u>郵便局アプリ</u> 9/29 19人・69件	R28 可	<u>ロート製薬</u> 9/15 参考 規模調査中
06 確	<u>楽天ドライブ</u> 10/6 15,382アカウント	R11 確	<u>イープラス</u> 9/29 返金1,463件	R05 確	<u>LEAN BODY</u> 9/15 参考 約44万アカウント
R04 確	<u>セイコーマート</u> 10/5 57万4,647人	R03 確	<u>タイムズカー</u> 9/29 約660万アカウント	R02 確	<u>ムラウチドットコム</u> 9/15 参考 771万6,811件
09 確	<u>物語コーポレーション</u> 10/5 1,078万8,963件	R23 可	<u>あいの風とやま鉄道</u> 9/28 参考 1,409人	R15 確	<u>Unni 〈カンナムオンニ〉</u> 9/10 参考 人数未記載
R30 可	<u>日本経済新聞社</u> 10/4 1,646人が対象	R20 可	<u>三井不動産</u> 9/28 参考 最大5.5万件	R07 確	<u>京都サンガ</u> 9/8 参考 1万5,612人
R17 可	<u>第一生命</u> 10/2 約12万人	R10 確	<u>集英社「ハピコミュ」</u> 9/28 参考 ブロガー2,835人		
R26 可	<u>らんぽん</u> 10/1 規模未公表	R19 可	<u>東京メトロ</u> 9/27 参考 メール約5.9万件		

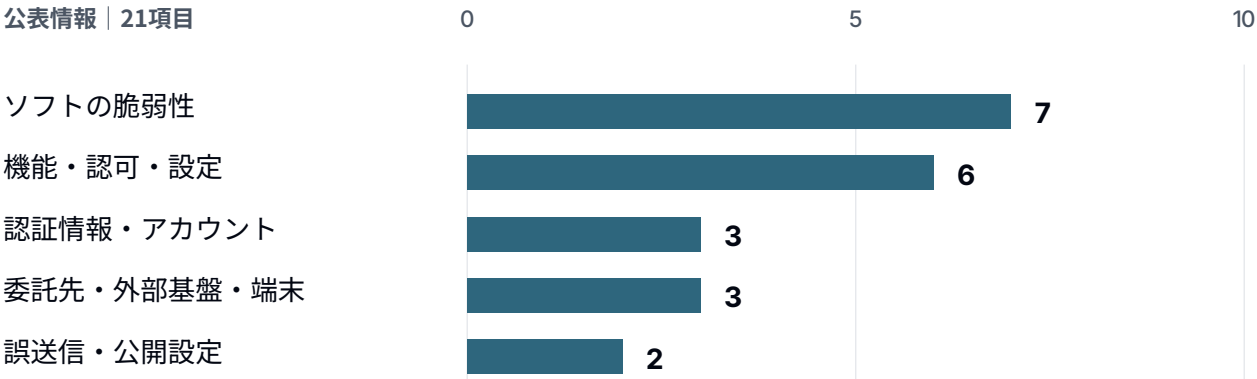
2026年9月29日～10月12日の数値のある21項目を便宜的に延べ合算し、重複1項目を除いた。人・件・アカウントが混在し、最大値や漏えいの可能性も含むため、実際の漏えい総件数ではない。ブックオフ第2報（10/13）は合算に未反映。

CAUSE ANALYSIS / Atlas Supportの独自分析

侵入の入口と、被害を拡げた条件を読み解く

図1 インシデントの要因分類

公表情報 | 21項目



手法未公表19項目 | Atlas Supportによる暫定分類



灰色の3分類はAtlas Supportの独自仮説で、各社が確認した侵入経路ではない。40掲載項目は続報等を含み、独立事故数や全国の発生比率ではない。

侵入経路の分析：狙われた3つの入口

侵入の入口	公表された事例	Atlas Supportの分析
公開Web・API	ムラウチ [R02] はWebの脆弱性を起点に複数システムへ侵入された。Unni [R15] は相談履歴APIへの不正アクセスを公表し、遮断翌日には同じ攻撃者による別経路からの再アクセスも確認した。	NICTは10月13日、公開Androidアプリの解析結果で接続先サーバを狙うA2B攻撃を確認した [O] 。アプリ側に欠陥がなくても、APIの認可不備が被害につながる。これは左記2社の侵入経路を認定するものではない。被害範囲はAPIの権限・取得量と遮断前後のログから絞る。
管理用ID・クラウド	楽天ドライブ [06] は管理用IDの認証情報を盗まれ、15,382アカウント分の保存ファイル閲覧・取得された。事象の期間は1月29日～9月17日だった。	管理用IDの権限が広いほど、閲覧され得るデータも増える。利用元・認証履歴とファイルの閲覧・取得ログを時系列で突き合わせ、被害が及んだ保存領域を絞り込む。認証情報の入手経路は未公表で、端末侵害やキー漏えいは判断できない。
委託先端末・分析ツール	第一興商 [04] の委託先PCはマルウェアに感染し、一時保管データに漏えいのおそれがある（流出は未確認）。LEAN BODY [R05] は分析ツールの脆弱性悪用を公表した。	端末の一時保管データと分析ツールの集約データでは、調査すべき記録が異なる。端末側は保存・削除履歴と外向き通信、ツール側は更新履歴・接続先DB・クエリログを追う。委託先へ渡した元データと残存する複製の差も調べ、保管量・期間と参照権限から漏えい範囲を見積もる。

AI THREAT LANDSCAPE / 攻撃能力の更新

AIのサイバー能力は向上 評価条件と実環境の違いを読む

国内掲載事例でのAI使用は未確認。評価研究と個別事故の原因は区別する。

AIのサイバー攻撃能力の成長

4.7か月

自律タスクの長さが倍増

英国AISIが隔離されたサイバー課題で、AIが80%の確率で終わらせる仕事の長さを推計した。[A]

50/410

既知の弱点で攻撃コード
完成

AnthropicがGLM-5.3を隔離環境で評価した数字で、実際の侵害成功率ではない。[B]

常時

弱点探索・検証を継続

AnthropicはAIを用いた継続的な研究・並列作業の悪用事例を報告した。[C]

急速な成長の背景には、モデルと実行環境の進歩がある

AIがこなせる作業は長くなった。英国AISIは、AIが8割の確率で終わられる課題を、専門家の所要時間で測った。対象としたのは隔離環境でのリバースエンジニアリングやWebの弱点検証で、2026年2月時点の推計では、この所要時間が2024年末以降、約4.7か月ごとに倍増していた。その後に評価したClaude Mythos PreviewとGPT-5.5は、従来の増加ペースから予想されるより長い作業を終えた。ただし、この差が続くかは分からない。別の模擬試験では、更新版のClaude Mythos Previewが、それまで成功例のない課題を10回中3回達成した。いずれも実際の企業への侵入成功率を示す数字ではない。[A]

使える計算量が結果を左右する。AISIは条件をそろえるため、1課題あたりの処理量を250万トークンに制限した。上限を外すと最新モデルの成功率はさらに上がり、用意した課題群だけでは「8割成功できる仕事の長さ」を推計できなくなった。この比較で示される能力は、制限がない場合より控えめだとAISIは説明している。[A]

少人数でも多くの標的を追える。Anthropicが把握した悪用事例では、指揮役のAIが偵察・侵入後の作業と脆弱性調査・ツール開発を分担させ、標的と進捗を次のセッションに引き継いだ。同社は侵入が2～3時間で終わった例に加え、一人で数十の被害先を同時に扱ったと報告する。ただし標的選定と結果確認には人が関わった。[C] NICTもAIによるアプリ解析・弱点探索の効率化を懸念するが、確認されたA2B攻撃でのAI使用は示していない。[O]

AI時代の企業防御を 権限・データ・対応手順から見直す

防御へのAI活用と、人の判断を組み合わせる。

検知から対処までの手順を設計する

Atlas Supportの提案：AIを使う攻撃では、試行の速さと規模が変わる。防御側も検知から封じ込めまでの時間を縮め、自動化の範囲と人の承認が必要な操作をあらかじめ決めておく。 [D] [E]

5つの設計原則

- | | |
|-------------------|--|
| 01 防御にもAIを用いる | 操作記録をAIで分析して不審な指示やデータ取得を捉え、担当者が通知を判断する。 [G] |
| 02 閲覧と実行の権限を分ける | 検索・要約と外部送信・削除を別権限にし、大量出力は人の承認を通す。 |
| 03 不必要なデータを保持しない | 原本・録音・要約・検索用データの期限を定め、委託先の不要な複製も削除する。 [F] |
| 04 不審な操作を速やかに止める | 大量取得などを検知したら、関係するアカウントやAPIキーを無効化して被害の拡大を防ぐ。 |
| 05 AI機能に安全対策を組み込む | Webページや添付資料に紛れた指示をAIが実行しないよう制御し、情報の外部送信が起きないか検証する。 [H] |

侵入後も、被害を最小限に抑える

BUSINESS CONTINUITY

停止時間を抑えるセキュリティBCP

継続すべき業務を定め、隔離したバックアップ、代替システム、手動手順を用意する。切替と復元を演習し、復旧判断から業務再開までの流れと所要時間を確かめる。 [I] [J]

DATA PROTECTION

漏れても悪用されにくいデータ

原本・録音・要約などの保有期間を見直し、不要な複製は削除する。残す情報には仮名加工や暗号化を施し、対応表と鍵をデータ本体と分けて管理することで、漏れい時の本人特定や復号を難しくする。 [K] [L]

Atlas SupportのAIセキュリティ脆弱性診断から改善まで

IPA・NICTの注意喚起を踏まえた、3つの診断領域

IPA・NICTが示した確認事項	Atlas Supportの確認・改善
公開アプリ・API	公開アプリと接続先APIを旧版・検証環境まで棚卸しする。未適用パッチや認証・認可の不備、入力値検証の弱点を調べ、ログで不審な大量取得を追う。[M] [O]
外部サービスとID	クラウドやVPNの利用状況を部署ごとに整理する。ログイン失敗の記録とアクセス元IP・時刻をたどり、見覚えのないアカウントや再有効化されたIDを探す。
保有データ	原本とAI用の派生データについて、保存先とアクセス状況を把握し、保有の必要性を見直して不要な複製を削除する。

不審な大量取得や権限外の閲覧が疑われる場合は、被害範囲を調べ、必要に応じてAPIの停止・アクセス制限や認証情報の再発行を急ぐ。[M] [O]

改善の優先順位と進め方

診断結果を踏まえ、事業への影響が大きい課題から対応の優先順位を定めることが、最初のステップとなる。その後、多要素認証とアクセス権限の見直し、異常検知と操作ログの整備、設定変更時の確認を進める。改善後は生成AI機能をOWASP LLM Top 10 [H]、WebアプリをASVS 5.0.0 [N]に照らして再検証する。

図2 Atlas Supportの支援：診断→改善案の策定→改善・再検証

01 診断

資産・権限・ログを調べ、弱点を洗い出す。

→

02 改善案の策定

課題ごとに修正方法と優先順位を定める。

→

03 改善・再検証

対策を実施し、問題が解消したか再検証する。

NEXT STEP / 診断のご相談

診断の進め方をご相談ください。

気になる領域と現状をお知らせください。診断の対象と改善の進め方を整理します。

診断について問い合わせる

[支援内容を見る](#)

参考文献

[01] ~ [10] 直近の選定事例 / [R01] ~ [R30] 関連事例 / 英字：分析・指針・研究

[01] アドベンチャー
2026/10/9

[02] ブックオフグループホールディングス
2026/10/9 / 第2報 10/13

[03] 手間いらず
2026/10/9

[04] 第一興商
2026/10/8

[05] ローソン
2026/10/8

[06] 楽天モバイル
2026/10/6

[07] ミスターマックス
2026/10/6

[08] GMOリサーチ & AI
2026/10/5

[09] 物語コーポレーション
2026/10/5

[10] タイムズモビリティ（パーク24グループ）
2026/10/1 / 第2報

[A] UK AISI：自律的AIのサイバー能力の進歩
2026/5/13

[B] Anthropic：GLM-5.3の攻撃コード評価
2026/9/29

[C] Anthropic：AI悪用脅威情報 2026年9月
2026/9/10

[D] a16z：AIエージェントの安全をどう守るか
2026/9/26

[E] NCSC：Managing the cyber risk of agentic AI
2026/8/20

[F] 株式会社Elith：件数では測れない漏えいAIが変えた「念のための記録」の価値
2026/10/9

[G] Li et al.：ADR: An Agentic Detection System for Enterprise Agentic AI Security
2026/5/17

[H] OWASP：Top 10 for LLM Applications 2025
閲覧 2026/10/6

[I] IPA：インシデント時の事業継続・復旧
2026/4/28

[J] IPA：バックアップと多層防御
2026/4/28

[K] PPC：高度暗号化と漏えい等報告の例外
閲覧 2026/10/12

[L] PPC：仮名加工情報ガイドライン
閲覧 2026/10/12

[M] IPA：漏えい事案を踏まえた緊急点検
2026/10/9

[N] OWASP：Application Security Verification Standard 5.0.0
閲覧 2026/10/6

[O] NICT IETICE：A2B攻撃への注意喚起
2026/10/13

[R01] Helpfeel | Gvazo 第2報
2026/9/25

[R02] ムラウチドットコム | 第2報
2026/9/15

[R03] パーク24 | タイムズカー
2026/9/29

[R04] セイコーマート | 第4報
2026/10/5

[R05] IFAN BODY | お知らせ
2026/9/15

[R06] ニチレイ | お知らせ
2026/9/18

[R07] 京都サンガF.C. | お知らせ
2026/9/8

[R08] ベネフィット・ワン | お知らせ
2026/9/30

[R09] 吉野家HD | ApplyNow事案
2026/9/30

[R10] 集英社 | ハピコミュ
2026/9/28

[R11] イープラス | 返金情報
2026/9/29

[R12] キューサイ | 企業サイトのお知らせ
2026/9/25

[R13] 日本郵政 | 郵便局アプリ
2026/9/29

[R14] 井筒まい泉 | ApplyNow事案
2026/9/25

[R15] Unni | 企業発表
2026/9/10

[R16] スターツ出版 | OZmall
2026/10/1

[R17] 第一生命 | お知らせ
2026/10/2

[R18] ジー・プラン | Gポイント
2026/9/30

[R19] 東京メトロ | お知らせ
2026/9/27

[R20] 三井不動産 | お知らせ
2026/9/28

[R21] アイススタイル | @cosme
2026/9/16

[R22] LEGOLAND Japan | ホテル予約
2026/9/25

[R23] あいの風とやま鉄道 | お知らせ
2026/9/28

[R24] チケプラ | お知らせ
2026/10/1

[R25] ニッポンレンタカー | 2事案
2026/10/1 / 別事案

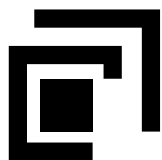
[R26] らしんばん | お知らせ
2026/10/1

[R27] 佐川急便 | 第4報
2026/10/9

[R28] ロート製薬 | お知らせ
2026/9/15

[R29] ヤマトHD | 第3報
2026/10/9

[R30] 日本経済新聞社 | お知らせ
2026/10/4



Atlas Support

株式会社Atlas Support

〒600-8223

京都府京都市下京区七条通油小路東入
大黒町227番地 第2キョートビル402

<https://atlassupportai.com/ja>

© 2026 Atlas Support Inc. All rights reserved.

