

相次ぐWebサービスへの不正アクセスとAIが変えた攻撃の前提

～事業の根幹を担うサービスの安全性点検のすすめ～

2026年9月以降、私たちの生活に身近なWebサービスで、不正アクセスによる情報漏えいの公表が相次いでいます。

会員情報

約 **1,079万** 件が漏えい

「焼肉きんぐ」公式アプリの会員管理システムから、会員情報が漏えいしました。^{※1}

運転免許証画像などの本人確認書類

約 **160万** 件が漏えい

タイムズカーWebシステムから、退会済みを含む約660万アカウントの情報が漏えいしました。^{※2}

9/15



ムラウチドットコム
調査結果を公表

9/16



Gyazo
公表

9/25



タイムズカー
公表

10/5



焼肉きんぐ公式アプリ
infoQ (GMOリサーチ
& AI)
公表

10/8



JPCERT/CC
注意喚起

10/9



国家サイバー統括室
対策の徹底を要請

○ 被害の公表 ● 公的機関の発信 | 各社・各機関の公表資料より。日付は最初の公表日（ムラウチドットコムは調査結果〔第二報〕の公表日）

原因を公表した事案の中には、Webシステムの脆弱性を起点としたものがあります

（各社の公表資料より）

運営会社（サービス）

公表された侵入の起点

GMOリサーチ & AI (infoQ)

「当社サイトで使用していたソフトウェアの脆弱性」を悪用して侵入された^{※3}

ムラウチドットコム（ムラウチドットコム）

「Webシステムの一部に存在していた脆弱性」を悪用されたことを起点に、複数のシステムへ不正アクセス^{※4}

Helpfeel（Gyazo）

「画像アップロードサーバーに存在した脆弱性」を悪用され、任意のコマンドを実行された^{※5}

なぜ今？ AIの高度化で、攻撃の「量・速さ・能力」が変わった

量 5,045件 → **10,740件**



月ごとに公表される脆弱性が、2026年1月から8月で倍増（採番の自動化による増加分を含む）^{※6}

速 約2週間 → **10時間未満**

人 約2週間

AI 10時間未満

複数の人のチームで約2週間かかる規模の作業を、AIエージェントを使った攻撃者が10時間未満で（1件の侵入事例）^{※7}

能 平均34% → **全段階**

2025年末のモデル
平均34%

最新のモデル
全32段階を完了

32段階の模擬企業ネットワーク攻撃を、最新のAIモデルは全段階完了できるように^{※8}

何を確かめ直すのか：攻撃の入口となる脆弱性が残っていないか

国も「定期的に脆弱性診断等を実施する」ことを求めています（内閣官房国家サイバー統括室、2026年10月9日）。※9確かめ方には、大きく2つの手段があります。

● ツールによる自動診断

広い範囲を短時間で確認できる。定期的な点検に欠かせない

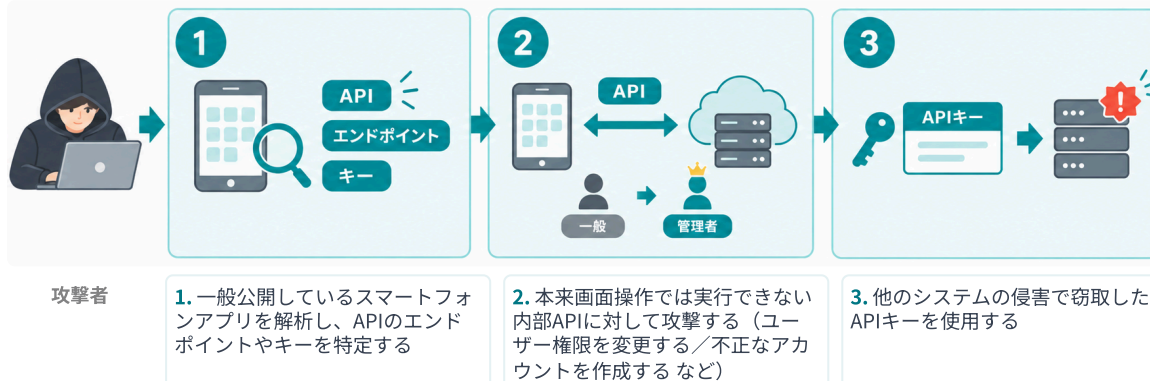
● 専門家による手動診断

サービスの仕様や業務の流れを理解したうえで確認できる

ただし、ツールだけでは見つけきれない入口があります。

例：画面の裏側にある「API」

APIは、アプリの画面の裏側でサーバーとデータをやりとりする窓口です。この窓口が「この利用者に許された操作か」を確かめずに要求を受け付けると、権限のない利用者でも、画面にはない操作ができてしまいます。それが許されない操作かどうかは、サービスの仕様を知らないツールには判断できません。



（JPCERT/CCに報告されている手口です。※10本資料で取り上げた個別の事案の原因を示すものではありません）

検証でも、ツールでは見つけきれなかった

IPAの中核人材育成プログラムのプロジェクトとして公開された「脆弱性診断内製化ガイド」では、手動診断で見つかった脆弱性を、5製品の診断ツールで検出できるか確かめています。※11

脆弱性の種類	製品D	製品E	製品F	製品G	製品H
アクセス制御や認可制御の欠落	×	×	×	×	×
クロスサイト・リクエスト・フォージェリ（CSRF）	×	×	×	×	×
メールヘッダ・インジェクション	×	×	×	×	×

×＝検出なし（同ガイド 付録A.4から3項目を抜粋）

ツール診断をやめましょう、という話ではありません。広い範囲はツールで定期的に確かめ、事業の要となる部分は、仕様を理解した専門家の目で確かめる。この組み合わせが大切です。

技術に詳しくなくても、いま確認できること

自社で確認すること

- 自社が公開しているWebシステムやスマートフォンアプリが、どんな個人情報をごだけ保有し、どのシステムと連携しているかを把握しているか
- 前回、専門家による手動診断を受けたのはいつで、どの範囲だったか
- 業務上必要のない管理機能やファイルが、インターネットに公開されたままになっていないか

委託先に確認すること

- 委託先が開発・運用・保守している部分は、誰が、いつ、どのような方法で点検しているか
- 事業の要となる機能について、専門家による手動診断を行っているか。ツールによる診断だけで済ませていないか
- 診断の範囲から外れている部分と、そこに残るリスクについて、説明を受けているか

EGSSにできること

▶ まず初めの一步に：

まずは**Webアプリケーション脆弱性診断**で、事業の要となる機能から、専門家の目で確かめることをお勧めします。何を点検すべきが決まっていな段階でも構いません。範囲の整理からご相談ください。

事例・出典の詳細は、完全版（8ページ）をご覧ください。

EG Secure Solutions

<https://www.eg-secure.co.jp/>

お問い合わせ

dl-sales-hq@eg-secure.co.jp

出典

※1 物語コーポレーション（2026年10月5日） ※2 タイムズモビリティ 第1～3報（2026年9月25日～10月1日） ※3 GMOリサーチ & AI（2026年10月5日） ※4 ムラウドットコム 第二報（2026年9月15日） ※5 Helpfeel（2026年9月16日） ※6 Google Threat Intelligence Group（2026年10月1日） ※7 Palo Alto Networks Unit 42（2026年9月2日） ※8 欧州システミックリスク理事会（ESRB）報告書（2026年7月。英国AIセキュリティ研究所の評価） ※9 内閣官房国家サイバー統括室（2026年10月9日） ※10 JPCERT/CC 注意喚起 JPCERT-AT-2026-0030（2026年10月8日） ※11 IPA 中核人材育成プログラム8期生「脆弱性診断内製化ガイド」（2025年8月29日改訂）

免責事項：本書に記載されている情報は、作成時点（あるいは発行日時点）のものであり、事前の予告なく変更される場合があります。当社は、本書の内容の正確性、完全性、最新性についていかなる保証も行うものではありません。また、お客様が本書の情報を利用したことによって生じたいかなるトラブルや損害についても、当社は一切の責任を負いかねますので、あらかじめご了承ください。