

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）

【サマリー】

攻撃を受けたのは、いずれも**事業の中核となるサービス**を支えるシステムです。両社ともサービスの提供は続けていますが、サービスを利用する会員の情報が大規模に外部へ持ち出されました。

原因を公表した同時期の事案の中には、**Webシステムやそこで使われるソフトウェアの脆弱性**を起点としたものがあります。そして攻撃する側では、AIの高度化によって、脆弱性を見つけて悪用するまでの**量・速さ・能力**が変わりつつあります。

2026年10月9日には**内閣官房国家サイバー統括室**も、ウェブシステムに係る脆弱性の悪用などによる不正アクセス事案を複数確認しているとして、「**定期的に脆弱性診断等を実施する**」ことを含む対策の徹底を、速やかに検討するよう求めています。^{※3}

本資料は、公表された事実と公的な資料をもとに、**事業の要となるシステムを、いま、どのように点検し直すべきか**を整理したものです。

※1 株式会社物語コーポレーション 「『焼肉きんぐ』公式アプリ 会員管理システムへの第三者からの不正アクセスによる個人情報漏えいに関するお詫び」（2026年10月5日）

※2 タイムズモビリティ株式会社 「『タイムズカーWebサイト』への不正アクセスによる個人情報漏えいの可能性について（第1報）」（2026年9月25日）、同 「『タイムズカーWebシステム』への不正アクセスに関する調査結果および今後の対応について（第2報）」（2026年9月28日、10月1日更新）、同（第3報）（2026年9月29日、10月1日更新）

※3 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）

押さえておきたいセキュリティニュース&トレンド解説

① 公表された事案に見る、Webシステムの脆弱性という入口

外部に公開されたWebシステムは、事業の窓口であると同時に、攻撃の入口にもなります。

JPCERT/CC（JPCERTコーディネーションセンター）は2026年10月8日、直近の2026年9月前後に国内組織で不正アクセスによる個人情報等の漏えい被害が相次いでいるとして、注意喚起を公表しました。寄せられた被害の情報をもとに、攻撃者が標的ごとにさまざまな既知の脆弱性を探索し、悪用を試みている可能性などを指摘しています。^{※4}

同じ時期に、各社が自ら原因を公表した事案の中には、次のようにWebシステムやそこで使われるソフトウェア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	公表された影響
GMOリサーチ & AI株式会社 アンケートサイト「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	最大94万8,498件 （同社が保有する全件）。一部会員のポイントが本人の意思によらず交換され、サービスを停止 ^{※5}
株式会社ムラウチドットコム ECサイト「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、その後、複数のシステムへ不正アクセス	個人情報7,716,811件 （2026年7月に判明、9月15日の第二報で件数を確定） ^{※6}
株式会社Helpfeel 画像共有サービス「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、システム上で任意のコマンドを実行された	ユーザーに関するデータ約2,362万件、画像に関するメタデータ約4.9億件など 。サービスを一時停止（9月27日に再開） ^{※7}

これらの事案では、入口となった脆弱性から、会員情報や、サービスの提供そのものにまで影響が広がっています。

事業の要となるシステムほど、外部とつながる入口が多く、守るべき情報も集まっています。

注記

※4 一般社団法人JPCERTコーディネーションセンター「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 GMOリサーチ & AI株式会社「当社が運営するアンケートサイト『infoQ』への不正アクセスによる個人情報漏えいに関するお詫びとお知らせ」（2026年10月5日）

※6 株式会社ムラウチドットコム「弊社における不正アクセスによるお客様情報漏えいに関するお詫びとご報告（第二報）」（2026年9月15日）

※7 株式会社Helpfeel「『Gyazo』への不正アクセスによる情報漏えいに関するお知らせとお詫び」（2026年9月16日）、同（第二報）（2026年9月25日）、同「『Gyazo』サービス再開のお知らせ」（2026年9月26日）

② なぜ今なのか：AIの高度化で、攻撃の「量・速さ・能力」が変わった

「これまで問題なかった」は、これからも問題ないことを意味しません。

「毎年、脆弱性診断を実施している」。その積み重ねは、確かに事業を守ってきました。個々の事案の攻撃手法は公表されていませんが、攻撃する側の条件は確実に変わっています。

量 月ごとに公表される脆弱性が、2026年1月から8月で倍増

5,045件 → **10,740件**

月ごとに公表される脆弱性は、2026年1月の5,045件から8月の10,740件へと倍増しました（採番の自動化による増加分を含む）。悪用が確認された脆弱性も、1～8月だけで2025年の1年分を上回っています。Googleの脅威インテリジェンスグループは、AIが脆弱性の発見と悪用のペースを変えつつあるとしています。^{※8}



速 約2週間の作業が、10時間未満に

約2週間 → **10時間未満**

Palo Alto Networks Unit 42が調査した1件の侵入事例では、複数の人のチームが連携しても通常は約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時間未満で終えています。^{※9}

人 約2週間

AI 10時間未満

能 AIが、侵入の最初から最後までをやり通せる水準に

平均34% → **全段階**

英国AIセキュリティ研究所による32段階の模擬企業ネットワーク攻撃では、2025年末のAIモデルは平均34%しか完了できませんでしたが、最新のモデルは全段階を完了できるようになったと報告されています。^{※10}誰でも入手できる形で公開されるAIモデルも、米国NISTの評価機関が「これまでに公開された中で最もサイバー能力の高いオープンウェイトモデル」と評価する水準に達しています（Z.ai社のGLM-5.3）。^{※11}

2025年末のモデル
平均34%

最新のモデル
全32段階を完了

「攻撃には手間とコストがかかる」という前提で点検の範囲や頻度を決めてきたのであれば、いまはその前提を確かめ直す時期にあたります。

では、何を確かめ直せばよいのでしょうか。

注記

※8 Google Threat Intelligence Group "Vulnerability Discovery and Exploitation Trends in the AI Era" (2026年10月1日)

※9 Palo Alto Networks Unit 42 "An AI-Assisted Cyber Attack: Inside a Unit 42 Investigation" (2026年9月2日)

※10 欧州システミックリスク理事会 (ESRB) "Addressing frontier AI models with cyber capabilities from a financial stability perspective" (2026年7月)

※11 NIST CAISI "CAISI's Assessment of Z.ai's GLM-5.3 Cyber Capabilities" (2026年9月17日)

③ 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）。※3その確かめ方には、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さない

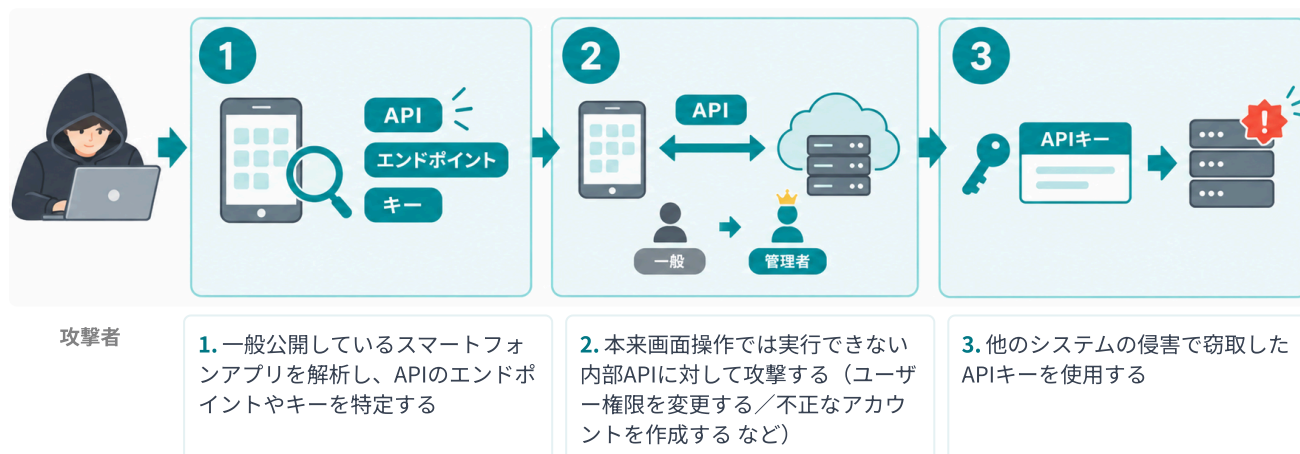
● 専門家による手動診断

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。次の2つは、その例です。

ツールで見つけにくい入口①：画面の裏側にある「API」

JPCERT/CCは、「アプリの管理用APIへの不正なリクエストによって、情報の不正な書き換え等が発生しているものがあります」と注意を呼びかけています。※4API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（権限の変更など）ができてしまいます（アクセス制御の不備）。要求が通っても、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は、すべての事案で同一の攻撃手法が使われていることを示すものではないとしています。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）

注記

※3 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）

※4 一般社団法人JPCERTコーディネーションセンター「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）

ツールで見つけにくい入口②：管理画面で動き出す命令
（典型的な例）

お問い合わせフォームなどに書き込まれた命令（スクリプト）が、後日、担当者が管理画面を開いたときに動き出す。「クロスサイト・スクリプティング（XSS）」と呼ばれる脆弱性を悪用した攻撃で、管理者の権限を奪われると、会員全体の情報やサービスそのものに手が届きます。**命令を書き込む画面と、命令が動く画面は別です。管理画面の表示まで、複数の画面をまたいでツールで確かめるのは難しいのです。**



検証でも、ツールでは見つけきれなかった

「誰が、どの操作をしてよいか」「入力した内容が、どの画面に表示されるか」は、サービスの仕様で決まります。ツールはその仕様を知りません。

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。同ガイドは「ビジネスロジックに深く依存する脆弱性（状態遷移の不整合など）や複雑な認証・権限管理の問題については自動検出が難しく、そういった脆弱性の発見には、ビジネスロジックの理解にもとづく手動診断が不可欠となる。」と記しています。^{※12}

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	×	×	×	×	×
クロスサイト・スクリプティング（XSS）	△	△	△	△	△
SQLインジェクション	△	△	△	△	△

△＝部分的に検出　×＝検出なし（同ガイド 付録A.4「手動診断とツール診断の比較結果」から5項目を抜粋。製品名は同ガイドの表記のまま）

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。

注記

※12 IPA 産業サイバーセキュリティセンター 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作成プロジェクト「脆弱性診断内製化ガイド」（2025年7月31日初版、8月29日改訂）。本文10ページ、56～57ページ。

対策のポイント

内閣官房国家サイバー統括室は2026年10月9日、特に大量の個人情報や機微な情報を取り扱う事業者等に対し、インターネットに公開されているシステムは「いつ攻撃を受けてもおかしくない」という前提で対策を講じることが重要だとし、委託先を含むサプライチェーン全体で安全性を確保することなどを求めました。^{※3}**事業の要となるシステムから、次の3点で確かめ直すことをお勧めします。**

① 何を：事業の中核となるサービスを支えるシステムから

会員管理、予約、ポイント、本人確認など、事業の中核となる情報と機能を扱うWebシステムやAPIを、優先して点検します。JPCERT/CCは、一般利用者向けのアプリのほか、「BIツールや従業員向け管理システムなど、管理・運用側で不特定多数の利用者からのアクセスを想定していないシステム」が被害に遭うケースもあるとして、こうしたシステムの点検も求めています。^{※4}

② どのように：仕様を理解したうえでの手動診断で

Webアプリケーションは、認可制御や業務ロジックの不備を、仕様を踏まえて確認します。JPCERT/CCも、対策として「非公開APIを含む各APIエンドポイントでアクセス制御を実施し、許可された利用者やHTTPメソッドからのアクセスのみを受け付ける」ことを推奨しています。^{※4}サーバーやネットワーク機器は、設定や構成を確認します。

③ どこまで：委託先が運用する部分も含めて

事業の要となるサービスには、外部の事業者が運用・保守している部分も含まれます。

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、どんな個人情報をどれだけ保有し、どのシステムと連携しているかを把握しているか
- ☐ 会員管理・ポイント・本人確認など、事業の要となる機能を、ツールによる診断だけで済ませていないか
- ☐ 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
- ☐ 従業員向けの管理システムやBIツールなど、社内向けのシステムも点検の対象に入っているか
- ☐ 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
- ☐ 配布しているアプリに埋め込んだAPIのキーは、取り出されうる前提で、サーバー側で利用者の権限を確かめているか
- ☐ APIのキーやトークンに有効期限を設け、漏えいが疑われるときにすぐ無効にできるか

範囲から外れていた場合、それが意図的な判断だったのか、何となく外れていたのかは、確認する価値があります。

注記

※3 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）

※4 一般社団法人JPCERTコーディネーションセンター「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）

当社の支援アプローチ（ご支援可能な具体的な対策案）

事業の要となるシステムを、専門エンジニアが確かめます。

● Webアプリケーション脆弱性診断（専門エンジニアによる手動診断）

自社内での自動チェックでは見抜けない「認可制御の不備」や「業務ロジックの欠陥」を、専門エンジニアが精密に洗い出します。ツール診断だけで終わらず、ビジネスロジックまで踏み込んで検証する点が特徴で、外部公開システムや重要データの保護に最適です。

● プラットフォーム診断

OSやミドルウェアなど、Webサービスを支える基盤を診断ツールで調べ、バージョンを含めて、既知の脆弱性が残っていないかを確認します。

● スマホアプリ診断 / ペネトレーションテスト / LLM脆弱性診断 / AWS設定監査サービス

会員アプリとその裏側でつながるAPI、実際の攻撃を想定した侵入経路、生成AIを組み込んだサービス、クラウド（AWS）の設定まで、高い専門性を持つエンジニアが精緻な検証を実施します。

● SiteGuardシリーズ（WAF／脆弱性スキャナー／プラグイン）

WAF

導入実績150万サイト以上、国内WAF市場シェアNo.1※13。
攻撃をリアルタイムに検知・遮断します。

SiteGuard Scanner for WordPress

WordPressサイトの脆弱性を、外部からだけでなく内部からも、定期的に自動で診断します。月額980円（年払い）で始められます。

SiteGuard WP Plugin

2014年の提供開始から10年以上、世界で60万以上ダウンロードされてきたプラグインです。

こんなときは、ご相談ください

事業の要となる機能を、専門家の目で確かめたい	Webアプリケーション脆弱性診断
会員アプリと、その裏側のAPIの安全性を確かめたい	スマートフォンアプリ脆弱性診断／Webアプリケーション脆弱性診断
OSやミドルウェアなど基盤のバージョンに、既知の脆弱性が残っていないか確かめたい	プラットフォーム診断
クラウドの設定や、不要な管理機能・ファイルの公開状況を確認したい	AWS設定監査サービス
生成AIを組み込んだサービスの安全性を確かめたい	LLM脆弱性診断
実際の攻撃者の視点で、侵入の経路と影響の広がりを確かめたい	ペネトレーションテスト
診断や改修が終わるまでの間も、公開中のサービスを守りたい	SiteGuardシリーズ（WAF）
何を点検すべきか、まだ決まっていない	まずはご相談ください（範囲の整理から）

➡ ▶ 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。何を点検すべきか決まっていない段階でも構いません。範囲の整理からご相談ください（お問い合わせは巻末へ）。

脆弱性診断・テスト

- Webアプリケーション脆弱性診断
- プラットフォーム診断
- スマートフォンアプリ脆弱性診断
- LLM脆弱性診断
- ペネトレーションテスト
- AWS設定監査サービス

コンサルティング・体制構築

- リスクアセスメント
- Webセキュリティコンサルティング／セキュリティ顧問
- セキュア開発プロセス構築支援／セキュア開発ガイドライン策定支援／ASPM環境構築支援

防御・検知（WAF等）

- マネージドWAF「SiteGuard Cloud Edition」
- ソフトウェア型WAF「SiteGuard」
- SiteGuard Scanner for WordPress（2026年10月サービス開始）

教育・訓練

- Security Campus（集合研修）
- Security Campus（一般従業員向け／エンジニア向け／Web担当者向け）

EGセキュアソリューションズ株式会社は、2008年の創業以来、**Webアプリケーションセキュリティに特化**して研究・開発・サービス提供を行う「Webセキュリティ専門家集団」です。

- ▶ 純国産WAF「SiteGuard」シリーズ——官公庁・金融・学校法人・医療機関をはじめ導入実績多数
- ▶ Webアプリケーション脆弱性診断は『情報セキュリティサービス基準』適合
- ▶ イー・ガーディアン株式会社（東証プライム／証券コード：6050）100%子会社

〒105-0001 東京都港区虎ノ門1-2-8 虎ノ門琴平タワー8F

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

各種サービスに関するお問い合わせはこちらまで

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

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。

セミナーのご案内

【11月17日開催 | 弊社も登壇します（無料）】

相次ぐインシデントへのセキュリティ防御戦略をテーマに、プロが「今、強化すべき要所」を伝えるカンファレンス。情報漏洩・サイバーセキュリティが気になる方はぜひ。登録者にはアーカイブも。

詳細：https://www.eg-secure.co.jp/seminar/20261117_event

