2026年 情報漏洩・不正アクセス事案の傾向と対策

Webアプリケーション・APIを中心とした攻撃の変化



株式会社神戸デジタル・ラボ

アジェンダ

1. 2026年の情報漏洩動向
2. 侵入経路の実態と公開情報の限界
3. Web/API攻撃の変化
4. 優先すべき対策と結論

Copyright © Kobe Digital Labo , Inc. All rights Reserved

エグゼクティブサマリー

2026年、Webシステムへの攻撃が重要なセキュリティ課題として顕在化

主要な調査結果

1. 国内のWebシステムを経由した情報漏洩事案が**増加**している
2. 侵入経路はWebアプリ・API、第三者製コンポーネント、VPNなど**多岐にわたる**
3. APIの**認証・認可やビジネスロジックの不備**を探索する攻撃が確認されている
4. AIエージェントのように試行錯誤する**適応型自動攻撃**が観測されている
5. 脆弱性管理やWAFに加え、**アプリケーション固有の設計・実装・運用**を守る必要がある

結論

WebアプリとAPIそのものの防御力が、情報漏洩リスクを左右する重要な要素になっている

※公開情報では侵入原因が特定できない事案も多く、「自社開発Webアプリの脆弱性が最多」とまでは断定できない

Copyright © Kobe Digital Labo , Inc. All rights Reserved

PART 1

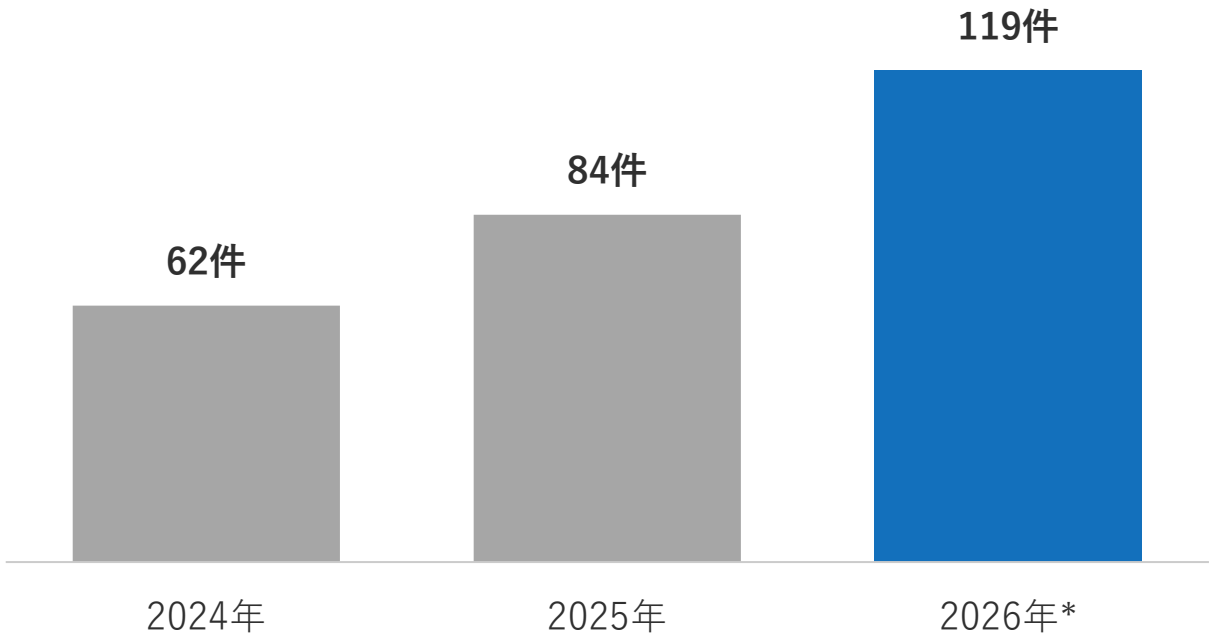
2026年の情報漏洩動向

Copyright © Kobe Digital Labo , Inc. All rights Reserved

Web経由の漏洩事案は10月時点で119件、前年通年を42%上回る

2026年の119件のうち81件（約68%）が7月以降に公表された

Webシステム経由の個人情報漏洩事案（公表ベース）



注目点

- 2026年は10月6日時点で、2025年通年を**約42%**上回る
- 119件のうち**81件が7月以降**に公表
- 81件は年間集計の**約68%**に相当し、後半に集中

解釈上の注意

- マクニカ独自の集計で、全インシデントは網羅しない
- ランサムウェアやリスト型攻撃は集計対象外
- 公表ベースの件数で、攻撃発生日とは異なり得る

* 2026年は10月6日時点。出典：マクニカ セキュリティ研究センター「相次ぐWEBシステムからの情報漏洩事案について」（2026年10月7日）

Copyright © Kobe Digital Labo , Inc. All rights Reserved

PART 2

侵入経路の実態と公開情報の限界

Copyright © Kobe Digital Labo , Inc. All rights Reserved

攻撃の入口は一つではなく、5つの経路に分類できる

「Webで漏洩」と「自社開発Webアプリが原因」は同義ではない

分類	主な攻撃対象	代表的な問題
A. 自社Webアプリ・API	独自開発システム、業務API	認証・認可不備、アクセス制御、ロジック欠陥
B. 第三者製Webコンポーネント	CMS、BI、フレームワーク、ミドルウェア	既知・未知の製品脆弱性
C. ネットワーク機器	VPN、境界機器	機器の脆弱性、設定不備
D. 認証情報・秘密情報	ID、パスワード、APIキー	漏洩した資格情報の悪用
E. 原因非公表	侵入経路を特定できない事案	分類不能

重要な考え方

Webサービスでの漏洩でも、実際の侵入経路は**第三者製ソフトウェア**や**認証情報の悪用**の可能性がある

分析方針

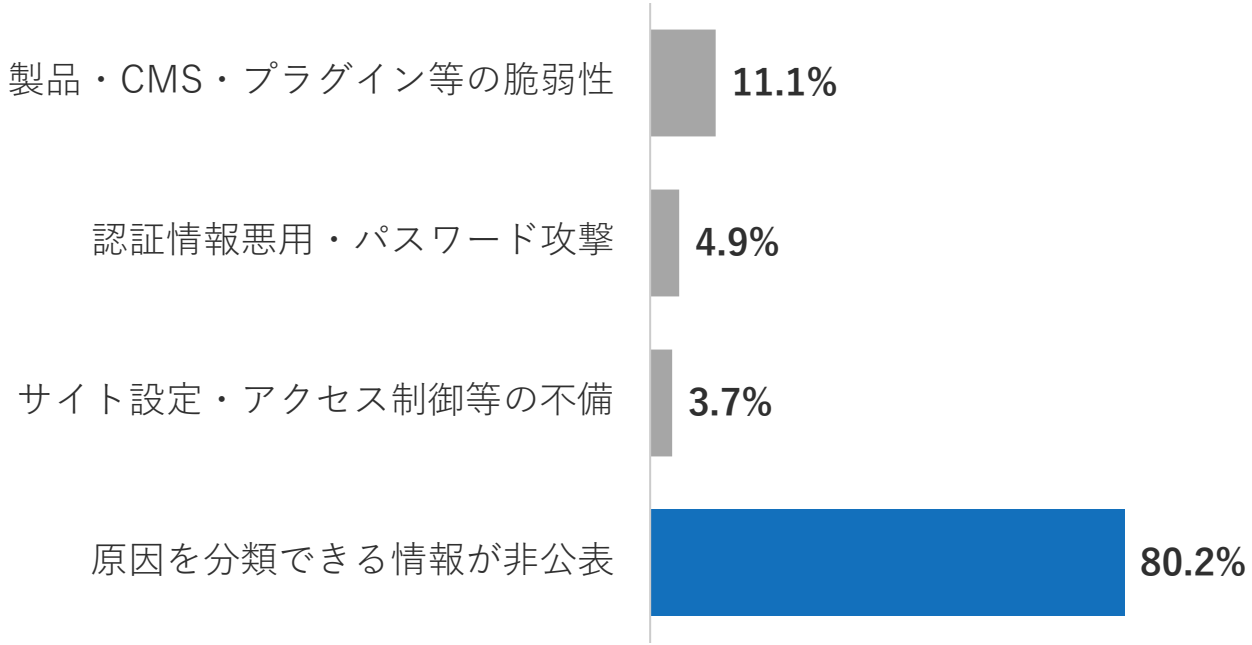
- 公表された事実を優先する
- 侵入経路が不明な場合は「原因非公表」とする
- 推測を事実として扱わない
- 複数経路がある場合、単一原因に無理に分類しない

Copyright © Kobe Digital Labo , Inc. All rights Reserved

公表事案の約8割は、侵入原因を詳細に分類できない

2026年7月以降の81事案のうち65件（80.2%）は原因が非公表

2026年7月以降の81事案の原因内訳（公開情報から分類）



この数字から言えること

- 製品の脆弱性が確認された事案は存在する
- 認証情報悪用やアクセス制御不備も確認されている
- ただし原因非公表の事案が**大半**を占める

この数字からは言えないこと

- 自社開発Webアプリの脆弱性が全体の何割を占めるか
- 最も多い侵入経路が何か
- 非公表事案の原因が特定カテゴリに集中しているか

侵入経路の「件数ランキング」を断定するより、**実際に確認された攻撃手法と防御上の弱点**を分析することが重要

出典：マクニカ セキュリティ研究センター「相次ぐWEBシステムからの情報漏洩事案について」（2026年10月7日）。

Copyright © Kobe Digital Labo , Inc. All rights Reserved

自社Webアプリ・APIの弱点は、製品のCVEでは捉えられない

利用者・権限・操作対象を組み合わせたテストが必要

代表的な問題

- 未認証の利用者が情報を閲覧できる
- 他人の予約情報や会員情報を取得できる
- APIが必要以上の個人情報を返す
- 一般利用者が管理者機能を実行できる
- 操作の順序や条件判定を悪用できる
- セッションやトークンの管理が不十分

事例：skyticket

2026年10月9日公表

- バス予約サービスで、予約完了ページが**ログインなしで表示**でき、第三者が機械的に閲覧
- 製品のCVEではなく、**サービス固有の認証・アクセス制御設計**の問題
- 別経路では業務管理システムの脆弱性も悪用され、**同じ企業で複数の弱点**が攻撃された

事例：ローソンID

2026年公表

- 約**215万5千件**の個人情報漏洩が公表された
- アプリ上で利用者本人に対し情報を表示するためのセキュリティ機構が第三者に悪用された
- 具体的な脆弱性は非公表のため、**特定の認可欠陥とは断定できない**

出典：株式会社アドベンチャー「不正アクセスによるお客様情報の流出に関するお詫びとお知らせ」（2026年10月9日）、株式会社ローソン「第三者による不正アクセスに伴う個人情報漏えいに関するお詫びとお知らせ」（2026年10月8日）

Copyright © Kobe Digital Labo , Inc. All rights Reserved

第三者製品とネットワーク機器も、主要な侵入経路になる

Web/APIの防御だけでは十分ではない

Metabase（BIツール）

- 脆弱性：**CVE-2026-72898**（SQLインジェクション）
- 認証なしで不正なSQLを実行し、**管理者権限を得る**可能性
- 製品側の公開前から悪用された事例も確認

示唆

一般公開を想定しない管理系システムの露出状況も点検する

KDDI（メール基盤）

- 対象：ISP向けメールシステム
- 経路：組み込まれた**第三者製ソフトウェアの脆弱性**
- 漏洩したメールアドレス：**12,231,954名**
- 漏洩したパスワード：**7,616,173名**

示唆

自社開発部分に問題がなくても、組み込んだソフトウェアが侵入経路になる

デジタル庁 GSS

- 経路：**VPN機器の脆弱性**
- 約**24.6万件**の個人情報を含むファイルが漏洩した可能性
- 悪用された脆弱性の評価は**CVSS Medium**

示唆

CVSSだけで優先度を決めず、外部公開状況と侵害時の影響も評価する

出典：JPCERT/CC「MetabaseのSQLインジェクションの脆弱性（CVE-2026-72898）に関する注意喚起」（2026年8月14日）、KDDI「ISP事業者向けメールシステムに対する不正アクセスについてのお詫びとご報告」（2026年7月6日、7月21日更新）、デジタル庁「ガバメントソリューションサービスへの不正アクセスによる職員等の個人情報の漏えいの可能性について」（2026年9月11日）

Copyright © Kobe Digital Labo , Inc. All rights Reserved

PART 3

Web/API攻撃の変化

Copyright © Kobe Digital Labo , Inc. All rights Reserved

JPCERT/CCは、正規画面を経由しないAPI直接操作を警告

APIサーバー側で権限を確認しなければ、画面での制限は防御にならない

報告された主な攻撃手法（2026年10月8日 注意喚起）

1. 公開スマートフォンアプリを解析する
2. APIエンドポイントやAPIキーを抽出する
3. 画面操作では実行できない**内部APIを直接呼び出す**
4. 認証トークンやHTTPヘッダーを変え、応答の違いを調べる
5. **ユーザー権限変更**や不正アカウント作成を試みる
6. NoSQLインジェクション等でデータアクセスを探索する
7. 他システムから**窃取したAPIキー**を悪用する

防御上のポイント

- APIごとに**認証・認可**を確認する
- **オブジェクト単位**のアクセス権を検証する
- 管理者機能へのアクセスを厳格に制限する
- APIキーを**唯一の認証根拠としない**
- すべてのAPIを棚卸しする
- 非公開APIや旧バージョンAPIも点検する

出典：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」（2026年10月8日）

Copyright © Kobe Digital Labo , Inc. All rights Reserved

認証済みであることと、データを取得する権限は別問題

「誰が、何を、どの条件で操作できるか」をAPIごとに守る

従来の対策で注目されやすいもの	2026年の事例から重視すべきもの
• SQLインジェクション	• **オブジェクト単位**の認可不備
• XSS	• **機能単位**の認可不備
• コマンドインジェクション	• 認証の不備
• 既知のCVE	• 過剰なデータ返却
	• ビジネスロジックの悪用
	• APIの過剰公開
	• 管理用エンドポイントの露出
	• APIキー・トークンの管理不備

例：予約情報API

```
GET /api/reservations/12345
```

正常な動作
予約番号12345の**所有者だけ**が情報を取得できる

危険な実装
ログイン済みかだけを確認し、**所有者かを確認しない**

結果
別の番号を指定すると、**他人の予約情報**を取得できる

設計原則
認証済みであることと、データを取得する権限は**別問題**。OWASP API Security Top 10でも認可不備は重要リスク

出典：OWASP「OWASP Top 10 API Security Risks – 2023」、OWASP「REST Security Cheat Sheet」

Copyright © Kobe Digital Labo , Inc. All rights Reserved

AIエージェントのような適応型自動攻撃が、国内で観測された

攻撃は「大量試行」から「応答に応じた試行錯誤」へ

約40分	326	1,200件超
継続時間	使用IP数	アクセス数

観測された攻撃の流れ

- SQLインジェクションで**認証回避**を試行
- 失敗すると**通常アカウントでログイン**
- ポイント機能など**サイト固有の仕組み**を探索
- 対象に応じて通信手法やツールを使い分け
- 同様の攻撃を複数回観測

観点	単純な自動攻撃	観測された適応型攻撃
試行内容	固定パターン中心	**応答を見ながら変更**
攻撃対象	一般的な既知脆弱性	**サイト固有機能も探索**
攻撃の流れ	大量の同種リクエスト	**複数の手法を段階的に試行**
通信元	少数IPに集中しがち	**多数IPに分散**
防御の難しさ	パターン検知で対応可	**行動全体の分析が必要**

重要な留保
AIの使用を直接証明する証拠はない。「**AIエージェントのような適応型自動攻撃**」と表現し、断定を避ける

出典：株式会社サイバーセキュリティクラウド「国内で相次ぐ不正アクセス、AIエージェントによる攻撃の可能性」（2026年10月9日）

Copyright © Kobe Digital Labo , Inc. All rights Reserved

PART 4

優先すべき対策と結論

Copyright © Kobe Digital Labo , Inc. All rights Reserved

WAFは重要だが、アプリケーションの認可設計を代替しない

WAF・パッチ管理に加え、4層の多層防御でアプリ固有の弱点を守る

WAFが有効な領域

- 既知の攻撃パターンの遮断
- SQLインジェクション等の一般的な攻撃の検知
- 悪意あるリクエストの制限
- Bot対策やアクセス制御の一部

WAFだけでは防ぎ切れない領域

- **正規APIの認可不備**
- 他人のデータを取得できるロジック
- 過剰な権限を持つAPI
- 正規機能を悪用した情報収集
- ビジネスロジックの欠陥
- 分散IPを使った低頻度の探索

必要な多層防御

第1層 攻撃面の把握	公開Webサイト／API／モバイルアプリ連携 ／管理画面／BIツール／旧システム／VPN
第2層 設計・実装の安全性	**サーバー側認証・認可**／最小権限／入力検証 ／データ返却の最小化／セッション管理
第3層 攻撃の抑制	WAF／APIレート制限／Bot対策／ 高リスク操作への追加制御
第4層 検知・対応	APIログ監視／異常アクセスパターンの分析 ／認可エラーの監視／インシデント対応体制

出典：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」（2026年10月8日）、OWASP「REST Security Cheat Sheet」

Copyright © Kobe Digital Labo , Inc. All rights Reserved

最優先はWeb/APIの棚卸しとAPI認可の点検

10の対策を3段階の優先度で整理する

優先度	対策	具体的な実施内容
最優先	Web/APIの棚卸し	公開・非公開・旧API・管理画面を洗い出す
最優先	API認可の点検	利用者・対象データ・操作ごとの権限確認
最優先	外部公開資産の管理	VPN、BI、管理機能の露出状況を確認
高	Webセキュリティテスト	認証後機能、API、ロジックまで診断
高	API自動化対策	レート制限、Bot対策、異常操作検知
高	第三者製品管理	コンポーネント棚卸しと脆弱性対応
高	ログ監視	API操作、異常応答、権限変更を監視
中	秘密情報管理	APIキーの最小権限・短寿命化・失効
中	被害拡大防止	MFA、ネットワーク分離、EDR
中	データ最小化	不要データ削除、API返却項目の削減

Copyright © Kobe Digital Labo , Inc. All rights Reserved

結論

WebアプリとAPIそのものの防御力が、情報漏洩リスクを左右する

1. **Webシステム経由の情報漏洩が増加**
   2026年は10月6日時点で119件と、前年通年を上回る

2. **侵入経路は多様**
   自社Web/API、第三者製品、VPN、認証情報の悪用を確認

3. **Web/API固有の弱点が攻撃対象**
   認証・認可不備、過剰権限、ロジック、管理機能を探索

4. **攻撃の自動化が高度化**
   応答を評価しながら手法を変える適応型攻撃を観測

5. **防御の重点を広げる必要**
   WAF・パッチ管理に加え、API認可・継続テスト・監視を強化

今後の取り組み

公開画面だけでなく、API、管理機能、モバイルアプリ連携、BI、旧エンドポイントまでを**一つの攻撃面**として管理する

そのうえで、**認可・最小権限・自動化耐性・継続監視**を強化する

Copyright © Kobe Digital Labo , Inc. All rights Reserved

APPENDIX

参考資料

Copyright © Kobe Digital Labo , Inc. All rights Reserved

Appendix A｜主な事例の比較

公表された侵入経路から分類し、原因非公表は推測で補わない

事例	攻撃対象	公表された侵入経路・問題	分類	注意点
skyticket	予約サービス	ログインなしで予約完了ページを閲覧可能	Webアプリのアクセス制御	別の侵入経路も存在
ローソンID	アプリ関連システム	セキュリティ機構を含む仕組みの不正利用	詳細原因非公表	認可欠陥と断定不可
Gyazo	画像アップロードサーバー	サーバーの脆弱性を悪用しコマンド実行	Webサーバー脆弱性	自社実装か第三者製品か不明
Metabase	BIツール	CVE-2026-72898、SQLインジェクション	第三者製Webコンポーネント	製品脆弱性
KDDI	メール基盤	第三者製ソフトウェアの脆弱性	第三者製コンポーネント	大規模な情報漏洩
デジタル庁 GSS	VPN機器	VPN機器の脆弱性	ネットワーク機器	CVSS Mediumでも重大な影響

出典：各社公表資料（Appendix C参照）、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）

Copyright © Kobe Digital Labo , Inc. All rights Reserved

Appendix B｜調査上の留意事項

数字とAI攻撃の扱いは、公表情報で支持できる範囲にとどめる

数字の取り扱い

- 事案件数は集計元の定義に依存する
- 公表日と実際の侵害発生日は異なる場合がある
- 「漏洩」と「漏洩のおそれ」は区別する
- 個人情報件数とアカウント件数は単純合算しない
- 同一人物・同一アカウントの重複があり得る
- 原因非公表の事案を推測で分類しない

AI攻撃の取り扱い

- AIエージェントのような挙動が観測されている
- ただし、AI使用そのものが**立証されたわけではない**
- AIを使った攻撃件数の増加を示す統計とは区別する

結論の範囲

支持できる結論

「Webアプリケーション・APIの防御が重要性を増している」

断定できない結論

「情報漏洩の最大原因は自社開発Webアプリの脆弱性である」

Copyright © Kobe Digital Labo , Inc. All rights Reserved

Appendix C｜参考資料

本資料で参照した公開情報（2026年10月15日時点）

1 **マクニカ セキュリティ研究センター（2026年10月7日）**
「相次ぐWEBシステムからの情報漏洩事案について」
https://security.macnica.co.jp/blog/2026/10/web-incidents2026.html

2 **JPCERT/CC（2026年10月8日）**
「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」
https://www.jpcert.or.jp/at/2026/at260030.html

3 **サイバーセキュリティクラウド（2026年10月9日）**
「国内で相次ぐ不正アクセス、AIエージェントによる攻撃の可能性」
https://www.cscloud.co.jp/news/report/202610099351/

4 **OWASP（2023年版）**
「OWASP Top 10 API Security Risks – 2023」
https://owasp.org/API-Security/editions/2023/en/0x11-t10/

5 **OWASP Cheat Sheet Series**
「REST Security Cheat Sheet」
https://cheatsheetseries.owasp.org/cheatsheets/REST_Security_Cheat_Sheet.html

6 **株式会社アドベンチャー（2026年10月9日）**
「不正アクセスによるお客様情報の流出に関するお詫びとお知らせ」
https://jp.adventurekk.com/news/apology-notice-unauthorized-access-data-leak/

7 **株式会社ローソン（2026年10月8日）**
「第三者による不正アクセスに伴う個人情報漏えいに関するお詫びとお知らせ」
https://www.lawson.co.jp/contents/cont07/1533174_3310.html

8 **株式会社Helpfeel（2026年9月16日）**
「『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」
https://corp.helpfeel.com/news/news-20260916-1

9 **JPCERT/CC（2026年8月14日）**
「MetabaseのSQLインジェクションの脆弱性（CVE-2026-72898）に関する注意喚起」
https://www.jpcert.or.jp/at/2026/at260023.html

10 **KDDI株式会社（2026年7月6日、7月21日訂正）**
「ISP事業者向けメールシステムに対する不正アクセスについてのお詫びとご報告」
https://newsroom.kddi.com/news/assets/2026/kddi_nr_s-73_4619/kddi_nr_s-73_4619_pdf_01.pdf

11 **デジタル庁（2026年9月11日）**
「ガバメントソリューションサービスへの不正アクセスによる職員等の個人情報の漏えいの可能性について」
https://www.digital.go.jp/news/2026-0911-01
https://www.digital.go.jp/press/5fc99139-a4e2-4b7b-8b0c-d475e926143f

Copyright © Kobe Digital Labo , Inc. All rights Reserved