

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

最終更新: 2026-10-08

JPCERT-AT-2026-0030

JPCERT/CC

2026-10-08

I. 概要

各被害公表や報道のとおり、直近2026年9月前後で国内組織における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ます。

複数の製品やサービスで被害が発生している中、技術的な情報の共有が不足しており、把握している情報は限定的かつ断片的であるものの、攻撃被害の拡大等の状況に鑑み、下記のとおり注意を促す次第です。また、本注意喚起は、普段から断続的、散発的に発生しているランサムウェア攻撃等の不正アクセス事案とは別に、大量の個人情報等の漏えいにつながっている、特に増加している恐れのある攻撃類型について取り上げるものです。

一般利用者向けのアプリのほか、BI（ビジネスインテリジェンス）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い、内部に保存していた情報が漏えいするケースもあります。こうしたシステムについても下記のような点検などを行う必要があります。

侵害原因や攻撃手法などに関する新たな情報が判明した場合、本ページを更新していきます。

II. 確認されている攻撃手法や攻撃の痕跡

※本項の情報は、JPCERT/CCに寄せられた情報などに基づくものです。すべての事案で同一の攻撃手法が使用されていることを示すものではありません。また、今後の状況などを踏まえて情報を追加する可能性があります。

ケースA：さまざまなソフトウェアの既知の脆弱性を探索し攻撃試行するもの

一連の攻撃については、一つの共通するソフトウェアの脆弱性を悪用しているのではなく、標的ごとにさまざまな既知の脆弱性有無についてスキャンし、脆弱性を探索して悪用を試行したり、脆弱性ではないものの、機器の管理不備等を悪用した攻撃（環境設定ファイルやバックアップファイルの窃取など）を試みている可能性があります。

ケースB：API経由での不正な操作

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。JPCERT/CCでは、次のような攻撃手口に関する複数の報告を受けています。

- (a) 一般公開しているスマートフォンアプリを解析しAPIのエンドポイントやキーを特定する
- (b) 本来画面操作では実行できない内部APIに対する攻撃
 - ユーザー権限を変更する
 - 不正なアカウントを作成する
 - ヘッダーの有無の切り替えや不正な形式の認証トークンの付与による応答の違いを確認する
 - NoSQLインジェクションによるブラインド探索によってアカウント情報を特定する
- (c) 他のシステムの侵害で窃取したAPIキーを使用する

なお、現時点までに次の不審なアクセス元が確認されています。

※下記IPアドレスは9月ごろに悪用されていたものです。調査時点では正規利用されている可能性もあります。

不審な送信元IPアドレス

- 3.112.252[.]14
- 54.95.112[.]6
- 69.10.51[.]162
- 172.86.91[.]7
- 210.149.87[.]120

User-Agentの例

- curl/7.88.1
- python-requests/2.34.2
- Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0 Safari/537.36

ケースC：MetabaseのSQLインジェクションの脆弱性（CVE-2026-72898）

本脆弱性も、APIへの不正なリクエストを通じて悪用されるものです。JPCERT/CCでは、2026年8月14日に本脆弱性に関する注意喚起を公表しています。影響を受ける製品や対策などの詳細については、次の注意喚起をご確認ください。

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

<https://www.jpcert.or.jp/at/2026/at260023.html>

なお、現時点までに次の不審なアクセス元からのアクセスが確認されています。

※下記IPアドレスは8月上旬から9月上旬までの間に悪用されていたものです。調査時点では正規利用されている可能性もあります。

不審な送信元IPアドレス

- 213.163.202[.]171
- 221.216.140[.]49
- 221.216.140[.]129

User-Agentの例

- python-requests/2.33.1
- Metabase-GHSA-vwf4/2.0

III. 対策

JPCERT/CCに報告されている攻撃手口に基づいて、次の対策の実施を推奨します。API経由のアクセスへの対策の詳細は、OWASPのガイドライン等を参考にしてください。

API経由のアクセスへの対策：

- APIへのアクセスには単位時間あたりのリクエスト件数を制限し、短時間に繰り返されるアクセスや大量実行を防止する
- ログイン、パスワードリセット、SMS送信、検索処理などの負荷や悪用のリスクが高い機能には個別にレート制限や利用回数制限を設定する
- 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
- API利用者やAPIトークンには必要最小限の権限のみを付与する
- APIトークンには適切な有効期限を設定し、長期間有効なトークンの使用を避ける
- 不要となった、または漏えいが疑われるAPIトークンは速やかに無効化できるようにする

上記の他、汎用的な対策：

- サービスの利用地域が限定される場合は、アクセス元の地域を制限する
- 既知の脆弱性の影響を受けるバージョンで運用している場合は、修正済みのアップデートを適用する
- Webサーバー等が侵害された後の横展開対策を見直す
- 不正アクセス検知体制の点検と検知時の初動対応を見直す
- 漏えい発生時を想定した、平時からの顧客への二次被害防止等の呼びかけ（多要素認証など）
- 業務上必要のないサービスや機能（管理機能など）がインターネットに公開されている場合、公開を停止する
- 法令や契約等で定められた保存期間を過ぎたデータや利用目的を終えたデータを残さない

繰り返しになりますが、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（従業員向け、BIツールなど）が被害に遭うケースもあります。こうしたシステムについても上記のような点検などを推奨します。

IV. 参考情報

OWASP API Security Project team

OWASP Top 10 API Security Risks 2023

<https://api-security.owasp.org/editions/2023/en/0x11-t10/>

OWASP Cheat Sheets Series

REST Security Cheat Sheet

https://cheatsheetseries.owasp.org/cheatsheets/REST_Security_Cheat_Sheet.html

株式会社マクニカ 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

<https://security.macnica.co.jp/blog/2026/10/web-incidents2026.html>

V. 調査依頼、情報提供等

今回の事案に関連して、不審なアクセスや侵害が疑われる事象、攻撃手法、侵害原因などに関する具体的な情報がございましたら、JPCERT/CCまで情報提供いただけますと幸いです。また、インシデント対応に関するご相談についても、JPCERT/CCまでご連絡ください。

注意喚起に関する問い合わせ先：

一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）
サイバーセキュリティコーディネーショングループ
Email：ew-info@jpcert.or.jp

インシデント対応相談の連絡先
<https://www.jpcert.or.jp/form/>

調査ベンダー等からの相談対応
<https://www.jpcert.or.jp/ir/consult.html>

一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）
サイバーセキュリティコーディネーショングループ
Email：ew-info@jpcert.or.jp



一般社団法人JPCERTコーディネーションセンター
〒103-0023
東京都中央区日本橋本町4-4-2 東山ビルディング8階
TEL: 03-6271-8901 FAX 03-6271-8908

© 1996-2026 JPCERT/CC