



滋賀県警察

サイバーセキュリティ海賀

サイバー犯罪からあなたを守るセキュリティ情報をお届けします。

R8年度 No.36

続報 Webサービスを狙った不正アクセス

今すぐ確認したい6つのポイント

国内で、WebサービスやAPI、管理システムを狙った不正アクセスによる情報漏えい等の被害が相次いでいます。自組織の環境を改めて総点検してください。

⚠ 確認すべき主な攻撃の手口

これらの手口により、情報の窃取・改ざん・不正なアカウント作成等が行われています。



既知の脆弱性の探索

OS・ミドルウェア・Webアプリケーションの既知の脆弱性や設定不備を探索し、不正に侵入を試みる。



APIへの不正リクエスト

アプリの解析等からAPIのエンドポイントを特定し、不正なリクエストによりデータの取得や操作を試みる。



盗まれたAPIキー等の悪用

窃取したAPIキーや認証情報を使い、正規の機能を悪用してデータにアクセスしたり、システムを操作する。



Webシェルの設置等

不正に侵入した後、Webシェルを設置し、継続的にシステムへアクセスする。また、アカウントの作成や権限変更の試行も確認されている。



攻撃を防ぐだけでは不十分です。

すでに侵入されていないか、今すぐ確認してください。

✓ 今すぐ確認したい6つのポイント

自組織のWebサービス・API・管理システム等について、以下の項目を点検してください。

1 公開範囲の確認



- ☐ 不要な管理画面やサービスをインターネットに公開していないか。
- ☐ 公開しているサービスの一覧を把握できているか。
- ☐ 利用していない機能・環境を停止しているか。

2 アカウントの確認



- ☐ 身に覚えのないアカウントや、本来不要なアカウントが存在しないか。
- ☐ 退職者・利用停止済みのアカウントが有効になっていないか。
- ☐ 管理者アカウントに多要素認証(MFA)を設定しているか。

3 API・APIキーの確認



- ☐ APIのエンドポイントや公開範囲を把握しているか。
- ☐ APIキーやトークンに必要な以上の権限を与えていないか。
- ☐ 不要なキーを無効化し、有効期限や失効手段を設定しているか。

4 脆弱性対策の確認



- ☐ OS・ミドルウェア・Webアプリケーション等に未適用の更新がないか。
- ☐ サポート終了製品を利用していないか。
- ☐ 設定の不備(デフォルト設定、不要な機能の有効化等)がないか。

5 ログの確認



- ☐ Webサーバ、認証、API、データベース等のログを確認しているか。
- ☐ 直近1か月のログを確認し、可能であれば3か月程度に範囲を広げて確認する。
- ☐ 不審なログイン、アクセス元IP、大量アクセス、権限変更等の痕跡がないか。

6 保有データの確認



- ☐ 利用目的を終えた個人情報等をシステム上に残していないか。
- ☐ 不要なデータへのアクセス権限を見直しているか。
- ☐ 万一に備え、重要なデータのバックアップや暗号化等を実施しているか。



あわせて実施したい対策

- ☒ 多要素認証(MFA)の導入・徹底
- ☒ APIのレート制限やエンドポイントごとのアクセス制御
- ☒ 不要なサービス・アカウント・APIキーの整理
- ☒ 最小権限の原則に基づくアクセス制御
- ☒ ログの適切な取得・保存と定期的な確認
- ☒ インシデント発生時の対応体制・手順の整備



● IPA「不正アクセスによる漏えい等の事案を踏まえ、速やかに実施すべき対策等について」(2026年10月9日) <https://www.ipa.go.jp/security/security-alert/2026/alert20261009.html>
● 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) <https://www.jpccert.or.jp/at/2026/at260030.html>