CyberCrime Control Project

令和８年10月

広島県警察本部
サイバー犯罪対策課
☎082-228-0110

［続報］相次ぐサイバー攻撃の手口と対策



情報流出を伴うサイバー攻撃が相次ぎ発生。
ソフトウェアやWebサービスの間を繋ぐ接点となる
ＡＰＩ※を悪用した事例も確認されています。

※ アプリケーション・プログラミング・インターフェース

確認されている攻撃の手口

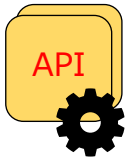
1 既知の脆弱性を悪用

- 標的ごとに既知の脆弱性を探索し、悪用して侵入
- 環境設定ファイルやバックアップなどの情報の窃取も…



2 管理用APIの不正操作

- アプリの解析等から管理用APIの情報（キーなど）を特定
- 権限の変更や不正なアカウント作成を行い、システムを操作



3 BIﾂｰﾙ※へのSQLｲﾝｼﾞｪｸｼｮﾝ

※ ビジネスインテリジェンスツール

- BIﾂｰﾙの脆弱性※を、APIへの不正なリクエストを通じて悪用
  ※ CVE-2026-72898
- 認証なしで不正にデータベースへアクセスし、情報を取得



4 APｻｰﾊﾞ上にWebｼｪﾙ※設置

※ アプリケーション　※ バックドア（裏口）の一種

- 公開Webｻｰﾊﾞからアクセス可能なAPｻｰﾊﾞ上にWARﾌｧｲﾙを設置
- WARﾌｧｲﾙに含まれるJSPﾌｧｲﾙがWebｼｪﾙとして動作し、外部からサーバ上のコマンド実行が可能



ＡＰＩ経由のアクセスへの対応

1 APIへのアクセスを制限

- 単位時間あたりのリクエスト件数を制限
- 負荷や悪用リスクの高い機能には個別にレート制限や利用回数制限を設定
- 非公開APIを含む各APIエンドポイントでアクセス制限

2 APIトークンの権限制御

- API利用者やAPIトークンには必要最小限の権限のみ付与
- 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使用を避ける
- 不要・不審なトークンは速やかに無効化

※ 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」
https://www.jpcert.or.jp/at/2026/at260030.html

サイバー犯罪被害の通報・相談は…

- 警察庁　サイバー事案に関する相談窓口
- 広島県警察本部サイバー犯罪対策課（代表☎０８２－２２８－０１１０）
- 最寄りの警察署

過去のセキュリティ情報は県警ホームページで　https://www.pref.hiroshima.lg.jp/site/police3/cyber-security.html ▶▶▶