

不正アクセスの経過と当社の対処について

2026年10月19日

株式会社アルカディア

代表取締役社長 天白成一

このたびの不正アクセスにより多大なるご迷惑とご心配をおかけしておりますことを、深くお詫び申し上げます。これまで公式ブログや管理者様向けメールなどを通じて随時情報更新に努めてまいりました。さらに、今回の不正アクセスの経過と今後の対応についてより詳細なご説明を行う必要があると判断いたしました。現時点で判明している事実、影響範囲、対応状況、および今後の対応方針について、お伝えできる範囲で、以下の通りご説明いたします。

今回の不正アクセスの経過と今後の対応について

2026-10-11

06:26 アクセス開始

06:54 JS 取得 `/html/js/user-login.js`

07:31 モバイルに気づく `/m/` `/m/php/\*` 以下を探索

09:23 `/api2/login` に気づいてログイン試行

10:52 ディレクトリトラバーサルチェック

11:04 `/register` `/register3` でセッション固定攻撃のチェック

11:10 `/fs119-bk` に気づく

15:49 SQL インジェクションのチェック

15:51 `/html/js/app.js` など JS を大量取得、`/api2/login` で大量のログイン試行

16:00 `/register` `/register3` 以下を探索し `/api2/login` で大量のログイン試行

16:16 `/register?aid=int` 以下のパス総当り探索

16:26 `/register?aid=int` 以下のパス総当り探索

16:32 `/fs1190bk` へ狙いを変更?

16:33 `/media` 以下のトラバーサルチェック

16:39 config.ini を取得に成功

23:40 社内のシステム監視により、DB の異常な負荷を覚知しました。この時点で不正アクセスを検知しました。

【不正アクセス】添付ファイルを公開しているメディアサーバーにおいて、内部の URL にアクセスできるディレクトリパストラバーサルが存在していました。内部ソースファイルが取得されたことで、設定ファイル内のサービス間ログイン用シークレットキーが取得されました。シークレットキーを利用し、アカウント ID に対して総当たり攻撃が実施されました。ログインされたセッションから内部情報が取得されました。

2026-10-12

03:00 不正アクセスの経路を遮断 (raidens3 の owner ページからサービスを作成された、ファイルサーバーの脆弱性を修正、内部 API のログインテストを停止)

09:30 DB の PW を変更

13:03 S 町の消防情報の外部連携が失敗していたことが発覚 (DB の PW 変更の影響が原因)

13:46 DB の PW 変更以降、電話発信に失敗していることが発覚

13:58 電話発信の不具合を修正し、正常に動作することを確認

15:20 個人情報保護委員会へ速報を報告

17:05 WordPress のプラグインが追加されていることが発覚

18:30 owner 画面と support の PW 変更

2026-10-13

00:10 メール送信の試験 (DKIM, DMARC など)

01:17 少しずつメール送信開始 (5 件ずつなど、最終的に 1000 件ずつ)

04:10 大量に配信されていることによりバックドアの設置が発覚

04:25 不正なメール配信を検知

04:48 一部のメールの配信速度を変更 (メールの流量制限)

07:16 不正なメール配信の停止

10:20 全サービス対象に公式ブログ公開 (SpeeCAN RAIDEN への不正アクセスによる個人情報漏洩の可能性について)

10:35 raidens3, s2 対象に公式ブログ公開 (不正アクセスに伴う一部サービスの緊急停止について)

10:48 raidens3, s2 の契約情報へ一部サービス緊急停止の案内メール送信

11:00 raidens3, s2 を緊急停止

11:10 アルカディア HP 公開 (SpeeCAN RAIDEN への不正アクセスによる個人情報漏洩の可能性について)

11:10 社内関係者で今後の対応を相談し、すべてのサーバーの検査を順次実施
11:40 所管警察署へ相談
13:54 JPCERT コーディネーションセンターへメールで相談
14:12 raiden・raiden2・s・raiden2XL の契約情報へ不正アクセスの案内メール送信
14:30 社内関係者ですべてサーバーの検査状況を共有
16:10 raiden3, s2 対象に公式ブログ追記 (不正アクセスに伴う一部サービスの緊急停止について)
17:00 不正アクセスのアクセス元 IP アドレスを接続できないように遮断
17:00 13 日の作業内容をブログに公開
18:00 NET119 の DB に不正アクセスの痕跡を発見
18:28 docomo エリアメール担当より、不審なアクセスを検知した旨の連絡あり

2026-10-14

08:30 旧 119RAIDEN・NET119 と社内会計サブシステムの DB に不正アクセスの痕跡を発見
10:00 社内問い合わせ回答例として全サービスが漏洩の可能性の対象である旨を周知
11:30 自動応答が停止していることが発覚 (IVR には問題ないことを確認済み)
15:00 NET119 と旧 119RAIDEN が対象に含まれることを公式ブログへ公開
17:12 旧 119RAIDEN の〇市で電話 1 件が遅かった (17:12 発信で 17:35 架電された)
18:38 S 県道路の空メール登録画面でエラーが表示されていることが判明 (DB の PW 変更が原因で raiden_custom_https の DB 情報を持っているものが失敗している)
19:05 raiden3, s2 のリバースプロキシを無効化し、隔離していたWEBサーバーをネットに接続し、侵害されていないことを確認
19:50 自動応答が復旧 (DB の PW を変更が原因と判明)
22:50 raiden3 の DB で書き換えされている箇所を複数発見

2026-10-15

09:30 raiden3 の DB の改竄されたデータを手作業で修正完了
09:43 raiden3 の外部連携メールの受付再開、受け付けたメールは破棄する状態
11:38 raiden3 を最速で 13 時ごろに復旧できる見込み (→社長に報告)
13:30 raiden3 のソースコードの改竄がないことを確認
13:50 raiden3、s2 に 15 時復旧予定の公式ブログ公開・案内メールを送信
raiden3, s2 のリバースプロキシを有効化
15:10 raiden3, s2 復旧 (→すべてのサービスの復旧完了)

17:50 raiden3, s2 復旧について公式ブログ更新

2026-10-16

15:30 個人情報保護委員会への代行報告を検討・公式ブログ更新

18:10 NET119・119RAIDEN の漏洩の可能性のうち、NET119 の件数確定（9,020 件のメールアドレスに紐づく上記個人情報）

NET119・119RAIDEN の漏洩の可能性についてブログ更新

【安全性の確認】ディレクトリパストラバーサルの解消を確認しています。不正なソースコードが存在しないことを確認しています。データベースが健全であることを確認しています。諸々の設定ファイル及び cron などの設定に問題がないことを確認しています。これらによって、現在、社内調査では、安全性が確認できていると考えていますが、より詳細な調査と対策をセキュリティ専門の第三者機関に依頼し、調査手続きを進めてまいります。

【今後の対応について】

- (1) すべてのサービスに対して、社内で立ち上げた L L M を活用した脆弱性診断及びコードレビューを実施、適宜、対応を行いました。また、今後、外部の会社に委託して脆弱性診断を受けます。
- (2) 社内からデータベースへのアクセスする方法を見直しました。PW をサービスごと個別に設定しました。今後は 2 段階認証を必要とするなど対策を強化します。
- (3) 各サービス、各プロセスの自動監視を強化します。今後に備えて、SOC (Security Operation Center) の導入についても検討していきます。
- (4) X、F a c e b o o k、L I N E、Y a h o o 防災アプリ、緊急速報メール（エリアメール）との連携については、順次、設定ファイルを見直していきます。また、防災行政無線等への連携に関してもメーカー等と協調して動作検証を実施していきます。
- (5) 不正なプログラムによって、外部にメール配信された状況など詳細な調査を継続しています。現時点では、その総数が 1,423,428 であることがわかりました。多くは、クレジットカード会社からの残高確認のような内容でフィッシング詐欺が疑われます。
- (6) 個人情報保護委員会・一般財団法人日本情報経済社会推進協会（JIPDEC）プライバシーマーク推進センター・総務省 近畿総合通信局・ISMS 日本能率協会へ報告済で

す。また、箕面市警察、大阪府警とも協議しています。アクセスログなどを元に被害届を提出予定です。

個人情報漏洩の可能性についての調査、及び具体的な数値等の特定にはなお時間を要する見通しですが、引き続き慎重に調査を継続し、判明次第ご報告できるよう努めてまいります。

引き続き、何卒よろしくお願い申し上げます。