

『不正アクセスによる個人情報漏洩の 可能性に関して』

株式会社 アルカディア
代表取締役社長 天白成一

2026年10月23日

今回の事案に関するお詫びとご報告

この度は、弊社において発生しました不正アクセスによる個人情報情報が漏洩した可能性のある事案につきまして、関係者の皆様には、多大なるご迷惑とご心配をおかけしましたことを、深くお詫び申し上げます。

また、一連の対応において、サービスの一部を停止せざるを得ない状況になりました。このことは、弊社が提供するサービスが災害情報など、人命や財産に深く関わることを考えれば、弊社として、今回の事態を重く受け止め、企業としての社会的責任と信頼を損ねたことを深く反省しております。

発生した原因を厳密に調査し、影響を受けた皆様に対して誠心誠意の対応を進めてまいります

弊社が提供しているすべてのサービスの運用保守体制を見直すとともに、今後、同様の事態が二度と発生しないよう、社員総力をあげて再発防止を徹底致します。

当社サービスの導入状況及び対応状況

【導入状況(契約数):2026年9月末現在】

官公庁	875件
自治体	715件
消防署	312件
警察署	22件
企業他	242件
学校	584校

【自治体などへの対応状況】

個人情報保護委員会への代行報告を取りまとめ中です。

※代行報告を行う場合、自治体からの同意が必要になります。

※住民の方へのご案内については、個人情報保護法の目的外利用になるため、当社から直接のメール配信は、行っておりません。

10月13日 18時47分更新【第2報】より

漏洩した可能性がある情報は、SpeeCAN RAIDENで扱っている以下となります。

連絡先の名前、メールアドレス、電話・FAX番号
担当者、契約情報
履歴として保存されている本文に記載されている内容

なお、SpeeCAN RAIDENでクレジットカードなどの決済情報の取り扱いはありませんので漏洩対象ではありません。

漏洩の可能性がある個人情報の最大件数

メールアドレス：約3,136,000件
電話番号：約105,000件
FAX 番号：約15,000件

本件数は、あくまでも推定値であり、継続して調査を進めております。対象のサービスは、SpeeCAN RAIDEN(アルカディア社)のメディアサーバーが不正アクセスを受け、内部情報が取得された

- 2026/10/11、SpeeCAN RAIDEN(アルカディア社)のメディアサーバーが不正アクセスを受け、内部情報が取得された
- 10/15 15:10 に全サービス復旧済。侵入経路は遮断済で、社内調査では安全性を確認
- 漏えいした可能性のある個人情報の件数は**調査継続中**(そのうちNET119は9,020件)

項目	内容	不正メール配信総数
発生日時	2026/10/11 06:26 攻撃者がアクセス開始	1,423,428通 フィッシング詐欺メールなど
検知	2026/10/11 23:40 社内システム監視がDB※1の異常負荷を覚知し、不正アクセスを検知	
原因	メディアサーバーの ディレクトリパストラバーサル脆弱性※2 から設定ファイル※3を取得され、サービス間ログイン用シークレットキー※4が流出。アカウントIDへの総当たり※5でログインされ、内部情報を取得された	NET119関連 9,020件 メールアドレスに紐づく個人情報のみ(既往歴などはなし)
影響範囲	全サービスが漏えい可能性の対象 (NET119・119RAIDEN・社内会計サブシステムのDBにも痕跡)。raidен3のDBで一部データ改ざん(10/15修正済)	
二次被害	設置されたバックドア※6から 不正メール 1,423,428通 を外部配信(フィッシング詐欺※7の疑い)。10/13 07:16 当社にて配信停止措置	raidен3・s2 緊急停止 約52時間 10/13 11:00～10/15 15:10
サービス影響	raidен3・s2を緊急停止(10/13 11:00～10/15 15:10)。DBパスワード変更の影響で外部連携・電話発信・自動応答に一時不具合(復旧済)	
現在の状況	全サービス復旧済。セキュリティ専門の第三者機関に詳細調査を依頼し、社内でのセキュリティ強化対策を策定中	

※1 DB(データベース):顧客情報やサービス情報などを整理して保存するシステム
※2 ディレクトリパストラバーサル脆弱性:Webサーバー内の、本来は閲覧できないファイルに不正アクセスできてしまう弱点
※3 設定ファイル:システムの接続先や認証情報など、動作に必要な設定が記録されたファイル
※4 シークレットキー:システム同士が正規の接続相手であることを確認するための秘密情報
※5 総当たり:多数のIDやパスワード等を機械的に試し、ログインを突破しようとする攻撃
※6 バックドア:攻撃者が後から再び侵入・操作できるよう、不正に設置する裏口
※7 フィッシング詐欺:実在する企業等を装い、偽サイトなどへ誘導して情報を盗み取る手口

10月19日 10時00分更新【第12報】より

不正アクセス事案の時系列(10/11～10/16)

日付	時刻	区分	事象
10/11	06:26	攻撃	アクセス開始。ログイン画面・API※1・ファイルサーバー等を探索し、ログイン試行・脆弱性チェックを繰り返す
	16:39	攻撃	ディレクトリパストラバーサルにより設定ファイル(config.ini)の取得に成功
	23:40	検知	社内システム監視でDBの異常負荷を覚知し、不正アクセスを検知
10/12	03:00	対応	不正アクセス経路を遮断(ファイルサーバーの脆弱性修正 等)
	09:30	影響	DBパスワード変更 → 消防情報の外部連携・電話発信に不具合(電話発信は13:58修正)
	15:20	報告	個人情報保護委員会へ速報
	17:05	被害	WordPressへの不正プラグイン※2追加が発覚(18:30 owner・support画面のPW変更)
10/13	01:17～	被害	バックドア経由で不正メールを大量配信(04:10 発覚、07:16 配信停止措置)
	10:20	公表	公式ブログで個人情報漏えいの可能性を公表
	11:00	対応	raidен3・s2 を緊急停止。全サーバーの検査を順次実施
	11:40～	報告	所管警察署・JPCERT/CC※3へ相談、17:00 アクセス元IP※4を遮断
	18:00	被害	NET119のDBに不正アクセスの痕跡を発見
10/14	08:30	被害	旧119RAIDEN・NET119・社内会計サブシステムのDBに痕跡を発見
	11:30	影響	自動応答の停止が発覚(DBのPW変更が原因、19:50 復旧)
	22:50	被害	raidен3のDBで改ざん箇所を複数発見
10/15	09:30	対応	raidен3の改ざんデータを手作業で修正完了。13:30 ソースコード改ざんなしを確認
	15:10	復旧	raidен3・s2 復旧(全サービス復旧完了)
10/16	18:10	公表	NET119の漏えい可能性件数を確定(9,020件)、公式ブログ更新

※1 API:異なるシステムやサービス間で、データや機能を連携するための仕組み

※2 不正プラグイン:システムへ不正な機能を追加するために、攻撃者が組み込んだプログラム

※3 JPCERT/CC:国内のサイバー攻撃やセキュリティ事故について、調整・支援を行う専門機関

※4 IP(IPアドレス):ネットワーク上で通信元や通信先を識別するための番号

10月19日 10時00分更新【第12報】より

■安全性の確認(社内調査) <サービス復旧判断の根拠>

✓ ディレクトリパストラバーサルの解消を確認

✓ 不正なソースコードが存在しないことを確認

✓ データベースが健全であることを確認

✓ 設定ファイル・cron※1等に関係がないことを確認

■再発防止策・今後の対応

#	項目	実施済み	今後の対応
(1)	脆弱性診断※2	全サービスでプライベートLLM※3を活用した脆弱性診断・コードレビュー※4を実施し、対応	外部会社に委託して脆弱性診断を受ける
(2)	DBアクセス管理	社内からのDBアクセス方法を見直し、PWをサービスごとに個別設定	2段階認証※5 など対策を強化予定
(3)	監視強化	各サービス・各プロセスの自動監視を強化中	SOC(Security Operation Center)※6導入を検討中
(4)	外部連携	—	X・Facebook・LINE・Yahoo防災アプリ・エリアメール連携の設定ファイルを順次見直し。防災行政無線等はメーカーと協調し動作検証
(5)	不正メール調査	不正な外部配信の総数 1,423,428通を把握(多くはカード会社を装うフィッシング疑い)	配信状況の詳細調査を継続
(6)	関係機関対応	個人情報保護委員会・JIPDEC・総務省 近畿総合通信局・日本能率協会(ISMS認証機関)へ報告済。箕面市警察・大阪府警と協議	アクセスログ等を基に被害届を提出予定

※1 cron: サーバー上で、決められた時刻に処理を自動実行するための設定

※2 脆弱性診断: システムに攻撃へ悪用される弱点がないかを確認する検査

※3 LLM(Large Language Model: 大規模言語モデル)、ただし、社内利用のみに限定

※4 コードレビュー: プログラムの内容を確認し、不具合やセキュリティ上の問題を点検する作業

※5 2段階認証: パスワードに加え、確認コードなど別の方法でも本人確認を行う仕組み

※6 SOC: サイバー攻撃の監視、分析、対応を専門的に行う組織・機能

10月21日 17時20分更新【第17報】より

不正アクセスにより、多大なるご迷惑とご心配をおかけいたしますことを深くお詫び申し上げます。

2026年10月13日 01:17から2026年10月13日 7:16までのあいだ、不正なプログラムによって、弊社システムから外部に不正なメールが配信されました。その調査経過についてご報告致します。

配信内容:フィッシング詐欺

(実在する企業等を装い、偽サイトなどへ誘導して情報を盗み取る手口)

配信総数:1,423,428通

うち、少なくとも869,575通については、

当社内に保有するメールアドレスへの配信ではないことが明らかになりました。

今後、外部機関でダークウェブ調査を行い、結果について後日ご報告いたします。

※2026年10月13日 07:16時点で不正なメール配信を停止しています。