2026 年 9 月 17 日

各　位

会 社 名　株式会社シンカ
代表者名　代表取締役社長　江尻　高宏
（コード：149A　東証グロース市場）
問合せ先　執行役員ＣＦＯ　飯田　裕樹

（開示事項の経過）弊社運営サービス紹介サイトへの不正アクセスに関する調査結果のお知らせ

2026 年 8 月 28 日付「弊社運営サービス紹介サイトへの不正アクセスに関するお知らせ」および 2026 年 9 月 1 日付「（開示事項の経過）弊社運営サイトの再開に関するお知らせ」にて公表いたしました弊社サービス紹介サイトへの不正アクセスの件につきまして、外部専門調査機関による調査が完了いたしましたので、その結果および再発防止策について、下記のとおりお知らせいたします。

調査の結果、外部からアクセス可能な状態にあった個人情報について、外部への持ち出し（漏えい）は確認されませんでした。

お客様ならびに関係者の皆さまには、多大なるご心配とご迷惑をおかけいたしましたことを、改めて深くお詫び申し上げます。

記

１．経緯

2026 年 8 月 24 日	弊社サービス紹介サイト（ https://kaiwa.cloud/ ）（以下「本サイト」といいます。）に対し、複数の不正プログラムが設置されていることを検知
2026 年 8 月 25 日	社内調査により、不正プログラムのうち 1 件が、当該サイトが設置されているサーバー（以下、「本サーバー」といいます。）からの情報取得を技術的に可能とするものであることを確認
2026 年 8 月 26 日	リスク拡大の回避および調査のため、本サイト及び関連サイトを含む 4 サイト（以下、「本 4 サイト」といいます。）へのアクセスを一時停止
2026 年 8 月 28 日	第一報として 2026 年 8 月 28 日付リリースを公表。あわせて、個人情報の保護に関する法律第 26 条第 1 項に基づき、個人情報保護委員会へ速報を提出

2026年8月28日～9月1日　安全性を確認したサーバー環境への移設を完了し、各サイトの公開を順次再開
2026年9月2日　所轄警察署への相談を実施
2026年9月14日　外部専門調査機関による調査が完了し、個人情報の漏えいを示す痕跡はなかった旨の調査報告書を受領
2026年9月17日　個人情報保護委員会へ確報を提出

2．調査の結果

（1）調査の概要

・調査機関　：外部専門調査機関（デジタルフォレンジック専門事業者）
・調査期間　：2026年8月27日 ～ 2026年9月7日
・調査対象　：本サーバーおよび本4サイトのアクセスログ、データベース、構成情報（プロセス、利用者情報、定期実行設定、ディレクトリ構成）、検出した不正プログラム検体、および稼働中のプラグインのソースコード
・調査手法　：アクセスログ、データベースおよび構成情報の解析、不正プログラム検体の解析、対象プラグインの実装コードの検証、ならびに各証跡の相互照合

（2）個人情報の漏えいの有無

調査の結果、検出された不正プログラムが実行され、サーバー内のデータを外部へ送信した形跡は確認されませんでした。

したがいまして、2026年8月28日付リリース「2．外部からアクセスされた可能性のある個人情報」に記載いたしました情報（弊社のセミナー・ウェビナーへのお申込みまたはお問い合わせをいただいた方の氏名、会社名、メールアドレス、電話番号等）につきまして、外部への漏えいの事実は確認されませんでした。

（3）侵入経路および原因

外部専門調査機関の調査の結果、本件は、本サイトで使用していたCMSのプラグインの脆弱性を悪用され、第三者がサーバーへ侵入し、不正プログラムを設置したことによるものと判明いたしました。

（4）弊社サービス「カイクラ」への影響

カイクラは、ネットワーク、クラウド環境、データストア、認証基盤のいずれも本サイトとは分離された構成であり、今回の事象によるサービスへの影響はありません。サイト

停止期間中を含め、通常どおりご利用いただいております。
　カイクラと本サイトは、以下の点で技術的に異なる構成であり、サービス紹介サイトへの攻撃がカイクラに影響を及ぼすことはございません。

①環境および運用体制の分離
　カイクラと本サイトは、全く異なるクラウドサービスを利用しております。両者のサーバー間に接続は一切なく、それぞれ独立した環境で運用しております。また、社内の運用管理者も異なるグループが担当しております。
②アプリケーションの非共通
　本サイトで不正プログラムが確認されたアプリケーションは、カイクラでは使用しておりません。
③認証方式の分離
　カイクラと本サイトでは、サーバーへの接続方法および認証方法が全く異なります。
　あわせて、平常時より以下のセキュリティ施策を実施しております。
・サーバー上でアンチウイルスソフトおよび侵入検知システムを稼働させ、二重の防御を行っております。
・年に一度、第三者によるペネトレーションテスト（侵入テスト）を実施し、検出された改善点については順次改修を行っております。

３．二次被害の状況
　本件における、個人情報の外部への漏えいの事実は確認されておらず、本日現在、本件に起因する二次被害の発生は確認されておりません。

４．お客様・関係者の皆さまへのお願い
　上記のとおり個人情報の漏えいは確認されておりませんが、念のため、弊社または関係者を装った不審なメール、SMS、電話等にご注意いただきますようお願い申し上げます。
・不審なリンクを開かない
・添付ファイルを開かない
・個人情報、パスワード、認証コード等を求められても回答しない
　不審なご連絡を受け取られた場合、下記８．のお問い合わせ窓口までご相談ください。

５．再発防止策
　本件を厳粛に受け止め、外部専門調査機関の助言も踏まえ、以下の再発防止策を実施し

ております。

（１）即時実施した対策

①サーバー環境の再構築

不正プログラムを除去したうえで、安全性を確認した新たなサーバー環境へ全サイトを移設し、クリーンな状態で再構築いたしました。

②認証情報の刷新およびアクセス制御の強化

移設先サーバーおよび管理画面に係る認証情報を全面的に刷新するとともに、管理画面へのアクセスについて追加の認証を設定いたしました。

③防御・検知機構の導入

サーバーに、より堅牢なセキュリティソフトを導入し、不正なプログラムの検出および駆除を行う体制を整備いたしました。あわせて、ファイルの改ざんを検知し担当部門へ即時に通知する仕組みを導入いたしました。

④保有する個人情報の非保有

Web サイトを通じて取得した個人情報について、サーバー上より、保有するデータすべて削除いたしました。あわせて、サーバー上にデータを保存しない設定に変更いたしました。

⑤社内の運用管理組織の変更

本件サービス紹介サイトの運用管理組織を、マーケティング部門から情報システム部門に変更し、明確化いたしました。

（２）今後実施する対策

①Web サイト基盤の刷新

サーバーおよびソフトウェアの管理を要しない SaaS 型の CMS へ移行し、脆弱性管理をサービス提供事業者の責任範囲といたします。あわせてサイトごとに独立した環境とし、万一の際の影響範囲を限定できる構成といたします。

②旧環境の廃止

移行の完了後、旧 CMS および関連する環境をすべて停止・削除いたします。

③アカウント管理の運用整備

Web サイト管理システムのアカウントについて、付与権限の基準を定めるとともに、定期的な棚卸を運用として継続的に実施いたします。

④役職員教育の再徹底

本件を教訓とした情報セキュリティ教育を全役職員を対象に実施するとともに、標的型攻撃訓練を含む実践的な教育の実施を継続してまいります。

実施予定の恒久対策を速やかに実施するとともに、全社を挙げて再発防止に取り組んでまいります。

６．監督官庁等への報告

・個人情報保護委員会：2026 年 8 月 28 日に個人情報の保護に関する法律第 26 条第 1 項に基づく速報を提出し、本調査結果を踏まえ、2026 年 9 月 17 日に確報を提出いたしました。

・警察当局：2026 年 9 月 2 日、所轄警察署へ相談および被害の申告を行っております。

７．弊社業績に及ぼす影響

弊社サービス「カイクラ」等の運営継続に問題はなく、本件が 2026 年度の弊社業績に及ぼす影響は軽微である見込みであります。今後、開示すべき事項が生じた場合には、速やかにお知らせいたします。

８．お問い合わせ窓口

本件に関するお問い合わせ窓口は下記のとおりです。

問合せメールアドレス：incident@thinca.co.jp

以　上