【緊急公開】医療機関を襲った8月12日の大規模サイバー攻撃｜医療法人鳳應会グループ Medi Face社がデジタルフォレンジック解析および証拠保全を完了（2026-08-12 19:33:27発生）

News / 2026.08.14

Webシェル侵入からGSC奪取、Cloudflareでのブランド詐称まで。医療法人を標的とした高度なSEOポイズニングと、APIジオクローキングによる隠蔽工作を組み合わせた組織的なサイバー攻撃への対応

Medi Face,
Ltd.

医療機関を襲った大規模サイバー攻撃

デジタルフォレンジック解析および
証拠保全を完了（2026-08-12 19:33:27発生）

医療法人鳳應会グループ
株式会社Medi Face

医療法人鳳應会グループおよび株式会社Medi Faceは、2026年8月12日 19:33:27（JST）、当社グループのWebインフラを狙った高度な組織的サイバー攻撃を検知いたしました。

医療情報サービスを展開する株式会社Medi Face（医療法人鳳應会グループ / 理事長：近澤徹）は、2026年8月12日 19:33（JST）より現在も断続的に続く、当社グループWebインフラを狙った高度な組織的サイバー攻撃に対し、迅速型デジタルフォレンジック解析および全証拠の保全を完了いたしました。 攻撃の主導者と思われる人物の接続元IPを東京都内で特定しており、現在、刑事告訴を含む厳格な法的措置への移行準備を進めております。 本攻撃は医療機関の社会的信用を標的とした極めて悪質かつ高度な手口であるため、同様の被害を未然に防ぐための公益的観点から、本攻撃の全技術的解析結果およびIoC（侵害の痕跡）を緊急公開いたします。

本攻撃は、海外IP（182.10.98.57：インドネシア等）を何重にも経由したPHP Webシェルの直接起動を起点として、Google Search Console（GSC）権限の所有権奪取、Cloudflare Pagesを用いたブランド詐称、さらには検知を回避する三重APIジオクローキングに至るまで、事前に緻密に設計された多段階のキルチェーン（Kill Chain）で構成されています。

単なる金銭目的のランサムウェアやランダムな脆弱性スキャンとは一線を画し、医

療機関の社会的信用と検索インフラの資産価値を標的とした約4ヶ月間に及ぶ中長期計画に基づく構造的な攻撃であることが判明いたしました。

当社グループでは、同様の被害を未然に防ぐための脅威インテリジェンスの共有と医療業界全体のセキュリティ水準向上（公益的観点）を目指し、本攻撃の全技術的解析結果を緊急公開いたします。なお、既にデジタルフォレンジック解析によりすべての証拠保全は完了し、防弾ホスティングによって秘匿されている攻撃主体の特定に至るサーバーログ、IPアドレス等を含むインターネット上の痕跡をすでに確保しております。今後は保全した証拠に基づき、刑事告訴ならびに損害賠償請求を含む法的措置を進めて参ります。

■ 速報 ｜ 証拠保全の完了と、首謀者特定の進捗（2026年8月14日時点）

1. デジタルフォレンジック完了：ファイル削除による証拠隠滅を無効化

攻撃者はすでに侵入に用いたバックドアファイル（fgh.php、yomanx498.php等）を削除し、証拠隠滅を図ったとみられます。しかし、当社法務チームおよびセキュリティ担当者は、削除ファイルのキャッシュ断片・ファイルシステムメタデータ・タイムスタンプ、および223,701行に及ぶサーバーアクセスログの迅速なデジタルフォレンジックを完了し、すべての証拠を保全済みです。ファイルの削除行為そのものが、証拠隠滅の故意を示す付加的証拠となります。

2. 首謀者接続元IPを国内（東京都内）で特定

決済関連IPアドレスやトークン等の解析により、組織的なサイバー攻撃の実質的な主導者（首謀者）と思われる人物の接続元IPアドレスが、インドネシアを経由した防弾ホスティングの背後に、国内（東京都内・永田町～六本木付近）から検出されております。

3. 刑事訴訟および国際捜査共助の準備

当社弁護団は現在、特定された首謀者に対し、不正アクセス禁止法・電子計算機損壊等業務妨害罪・名誉毀損罪等の適用を視野に入れた刑事訴訟の提起を検討中です。また、インドネシア側の実行犯グループに対しては、国際刑事司法共助条約（MLAT）を通じた国際捜査共助の申請も並行して準備を進めています。

■ 本レポート公開の意義

本攻撃の標的は、国民の健康と医療情報を担う医療法人・クリニックです。医療分野のウェブサイトは、Googleが「YMYL（Your Money or Your Life）」として最高水準の信頼性を要求する分野です。攻撃者はその高い「ドメイン権威」を意図的に悪用し、患者が医療情報を検索した際に違法賭博サイトへ誘導されるよう仕向けました。本件は、**医療機関の社会的信頼を意図的に悪用した極めて悪質な組織的な高度標的型サイバー犯罪（APT）**であり、国民の公衆衛生インフラの根幹そのものを脅かす重大な攻撃です。

本解析レポートを一般公開する最大の目的は、医療業界および社会全体における連鎖的な被害を未然に防ぐという公益的使命にあります。当法人は、攻撃者の特定や法的追及という次元にとどまらず、本稿で詳（つまび）らかにする攻撃の技術的構造が、広く皆様の「脅威インテリジェンス（防衛ナレッジ）」として共有され、医療機関ひいては社会全体のサイバーレジリエンス向上の一助となることを期しております。

■ 攻撃の全体像と技術的特異性（解析レポート抄録）

本攻撃は、単発的なスキャンではなく、120日以上前から計画された「高度標的型組織犯罪」です。当社に対する事前の情報収集、Cloudflare Pagesを用いた偽サイトの構築、Google Search Consoleの権限奪取などが周到に行われました。

【攻撃者が採用した高度な隠蔽技術（一部抜粋）】

三重API地理的クローキング（Geo-Cloaking）： インドネシアのモバイル端末からアクセスした場合のみ違法ギャンブルサイトへ誘導し、日本のIPやPC端末（捜査機関やセキュリティ研究者を含む）からのアクセスは「無害なループ」へ転送し証拠を隠滅する高度な判定機構を実装。

ブランド詐称とAMPの悪用： Cloudflare Pagesの無料サービスを悪用し、当社のブランド名（medi-face / fraise-clinic）を冠した偽ページを作成。Google公式のAMPフォーマットを使用することで、検索エンジンからの信頼性を偽装。

Telegramを用いたC2（指揮統制）： 実行犯グループはTelegramのプライベートチャンネルを利用し、暗号化された環境下で作業分担や進捗を共有しながら協調攻撃を展開。

※攻撃インフラの5段階構造（防弾設計）、クローキングエンジンの完全コード解析、ゲーム理論的分析（デュアルレバレッジ支配戦略）など、詳細な技術レポート

全文およびIoC一覧は、有識者向けにGitHubにて公開しております。

■ エンジニア・ホワイトハッカーの皆様へ

本攻撃の手口は極めて計画的であり、同一犯罪グループが日本・アジア圏の他の医療法人・企業に対しても同様の攻撃を現在進行形で展開している可能性が高いと考えております。当社内の解析にとどまらず、巧妙化するサイバー犯罪の実態をより深く解明するため、世界中のセキュリティ有識者の皆様からのご意見を広く承りたいと考えております。本レポートに対するフィードバックや、以下のテーマに関するご意見や知見の提供を歓迎いたします。

- 同一手口による他の被害医療機関・企業の発見
- 本稿の解析内容（クローキング機構等）へのフィードバック・盲点のご指摘
- インドネシア国内からのアクセス確認（モバイル端末による証拠コンテンツの表示テスト）
- 攻撃者インフラのOSINT調査（未発見の犯罪インフラの特定）
- アフィリエイトID・決済経路の追跡調査
- 首謀者と思われる人物の接続元IPアドレス（東京都内・永田町～六本木付近タワーマンション）

【情報提供窓口】
メールアドレス： info@medi-face.co.jp
参照番号： MF-2026-0812 ※本文書に含まれるIoCの防御・研究・教育目的への利用、および転載・引用を歓迎いたします（出典の明記をお願いいたします）。

■ 会社概要・お問い合わせ先

組織名：医療法人鳳應会グループ / 株式会社Medi Face（理事長：近澤 徹）
事業内容：医療情報サービスの提供、オンラインクリニックの運営等

公式サイト： https://medi-face.co.jp/

本文書に含まれるIoCの防御・研究・教育目的への利用を自由に許可する。転載・引用歓迎（出典明記を要請）。

© 2026 Medi Face, Ltd. — Released for public benefit under defensive security principles.

Medi Face, Ltd.

CONTACT

企業概要
Medi Face Journal
医療サイトのWebセキュリティ
お知らせ
イベント
Mente for Biz [メンテ]
Z産業医事務所
キャリア・インターン
個人情報保護方針
情報セキュリティ基本方針
特定商取引法に基づく表記

Copyright© 2023 Medi Face, Ltd. All Right Reserved.