2026 年 3 月 11 日

# 弊社サーバーへの不正アクセスに関する調査結果と今後の対応について（第 3 報）

この度、弊社が受けたサイバー攻撃および個人情報の漏えいにつきまして、お客様ならびに関係者の皆様に多大なるご心配とご迷惑をおかけしておりますことを、深くお詫び申し上げます。

外部専門機関によるフォレンジック調査の完了に伴い、弊社として把握した事案の実態および今後の対応状況について、以下の通りご報告いたします。

記

1. 調査により確認された事象および原因
   外部専門機関による調査報告を受け、弊社において以下の実態を確認いたしました。

   - 不正侵入の経緯
     攻撃者による不正アクセスが行われ、弊社のファイアウォールが突破されたことにより、ネットワーク内部への侵入を許す結果となりました。
   - 発生原因
     業務遂行上の必要性から維持していた特定のアカウント設定が存在しており、攻撃者によってその脆弱性が悪用されたことが主因です。
   - 攻撃の性質
     特定の組織を狙った標的型攻撃ではなく、攻撃者が IP アドレス順に無差別な攻撃を試みる中で、弊社の旧環境が標的となった可能性が高いとの見解を得ております。
   - 攻撃者および手法
     外部の悪意ある第三者（ランサムウェアグループ）による攻撃であることを確認いたしました。侵入後、弊社内のウイルス対策ソフトを強制停止・削除する隠蔽工作を行った上で、情報の窃取とデータの暗号化が実行されました。

2. 情報漏えいの範囲と現在の安全性
   - 被害範囲の限定
     攻撃を受けた範囲は、既に利用を終了していた「旧来の社内ネットワーク内」のサーバーに限定されていることを確認しております。
   - 現行システムの安全性
     現在稼働している新社内ネットワーク環境、およびショッピングモール等の外部システムでの侵害や感染の事実は一切ございません 。弊社が提供していた過去のサービスを含むシステム全般について、現在は安全な状態であることを確認いたしました。

- 情報漏えいの詳細
  クレジットカード情報やマイナンバーなど、二次被害の可能性が高い情報の流出は確認されておりません。

3. 今後の対応および個人情報の精査について
   弊社では、流出した恐れのある全ての情報について、現在も継続して精査を行っております。
   - 継続的なデータ精査
     ダークウェブ上に公開された約 36,000 ファイルの内容を確認しており、規則性のない複雑なデータについても外部機関と連携した精査（データクレンジング）を進めております。
   - 個人通知の実施状況
     精査により判明した対象の方々には順次個別の通知とお詫びを実施しており、本日までに約 8,000 名への通知を完了いたしました。残る対象の方につきましても、情報が特定され次第、弊社より速やかに個別通知を継続してまいります。
   - 監視体制の延長
     不測の事態に備え、専門機関による監視調査についても期間を延長して継続実施いたします。

4. 実施済みの再発防止策
   弊社では本事態を重く受け止め、外部専門家の指導のもと、以下の対策を完了いたしました。
   - 侵入口の完全な遮断とシステムの刷新
     不正アクセスの起点となった古い接続装置（VPN）やサーバーは、すべて物理的に撤去・廃止いたしました。現在は、被害を受けた環境とは論理的に切り離された、安全な新システムへの移行を完了しております。
   - 不審な挙動の検知・ブロック機能の強化
     システム内での不審な動きを即座に検知し、自動的に遮断する最新のセキュリティ対策を導入いたしました。これにより、外部からの不正な試みを早期に発見し、被害を未然に防ぐ体制を整えております。
   - 多要素認証の導入とアクセス権限の厳格化
     第三者による不正ログインを防ぐため、原則すべての業務システムにおいて「多要素認証（二段階認証）」を導入いたしました。あわせて、システムを利用できる権限を業務上の必要最小限に絞り込むなど、社内の管理ルールを刷新し、運用の厳格化を図っております。

本件に関するお問い合わせにつきましては、下記窓口までご連絡いただけますようお願い申し上げます。

【本件に関するお問い合わせ窓口】
株式会社 47CLUB 個人情報お問い合わせ窓口
メールアドレス：pi@47club.jp

以上