2026 年 5 月 13 日

各　位

会社名　　フィーチャ株式会社
代表者名　代表取締役社長 CEO 兼 CTO 曹　暉
（コード番号：4052 東証グロース）
問合せ先　取締役 CFO　　立花　嵩大
（TEL.03-6907-0312）

ランサムウェア被害に関する調査結果および再発防止策のご報告（最終報）

2026 年 2 月に公表いたしました当社サーバーにおけるランサムウェア被害（以下「本件」）につき、外部専門家の支援のもと実施した調査が完了しましたので、調査結果および再発防止策の概要を下記のとおりご報告いたします。

株主・投資家の皆様をはじめ関係者の皆様には、ご心配とご迷惑をおかけしておりますことを、改めて深くお詫び申し上げます。

（記）

1．調査結果の概要（確認事実と制約）

（1）確認された事実

- 不正アクセスおよびランサムウェア感染が発生していたことを確認しました。
- 不正アクセスが確認されたサーバー等は合計 32 台で、そのうち 13 台はランサムウェアに感染しました。
- 攻撃者が、当社の 1 台のサーバー上に集約したファイルを、ファイル転送ツールを用いて攻撃者管理のクラウドストレージ（OneDrive）へ送信したことが確認されています。
- また、当社の GitHub サーバーから、144 個の GitHub リポジトリが外部にコピーされたことが確認されています。
- 窃取された可能性のある情報の一部について、複数の一般サービスサイト上での掲載が確認されています。（URL 等の詳細は二次被害防止および捜査・封じ込めの観点から公表しておりません。なお、当社データに関連する情報および外部ストレージへのリンクが、一般のウェブブラウザからも閲覧可能なフォーラム上に掲載されていることが確認されています。）
- 当社が把握していたものとは異なる外部ストレージへのリンクが、第三者により公開されていたことが確認されています。当該ファイルについてはパスワードにより保護されており、現時点で内容の確認や第三者による実質的な取得事実は確認されておりません。

（2）調査上の制約（断定できない点）

- 調査の結果、本件における最初の痕跡は、2025 年 7 月 9 日、ファイアウォールを介した当社サーバーへの不正アクセスであることが確認されていますが、当該不正アクセスの具体的な原

因・手法については、関連ログがランサムウェアによって暗号化されていたこと等から特定には至っておりません。

- 外部送信されたファイルについては、集約されたファイルの痕跡が残存しておらず、個別ファイルの特定には至っておりません。
- 攻撃者によるログの消去・ランサムウェアによるログの暗号化等の制約により、窃取されたファイルの全容を断定することは困難であると判断しております。

2. 復旧状況

当社は、被害拡大防止措置および復旧対応を進め、現在は通常業務を再開しております。 また、外部公開状況の確認およびダークウェブ監視を含む継続的なモニタリングを実施しております。

3. 再発防止策

当社は、本件を重大なセキュリティインシデントとして厳粛に受け止め、侵入防止・社内拡散防止・権限管理・端末対策・監視体制の各段階において、多層的な対策を実装・強化しております。

主な取り組みは以下のとおりです。

- 外部接続基盤の刷新、多要素認証の導入、不審ログイン監視
- ネットワーク分離等による社内拡散防止
- 管理者権限分離等のアカウント管理強化（継続的な見直しを含みます）
- EDR（Endpoint Detection and Response） 等の端末セキュリティ対策の導入
- 外部 SOC（Security Operation Center） を含む監視体制の強化

加えて、インシデント対応プロセスおよび社内ルールの整備・見直しを継続し、再発防止と継続的改善を図ってまいります。

4. 今後の対応

当社は、情報セキュリティを経営上の重要課題として位置づけ、再発防止策の実効性確保と継続的改善に取り組んでまいります。また、引き続き事実関係の確認および影響範囲の監視を継続し、新たにお知らせすべき事項が判明した場合には、適切なタイミングで情報を開示いたします。

５．業績への影響

現時点で、本件による業績予想の修正はありません。今後開示すべき事項が発生した場合には速やかにお知らせいたします。

以　上