2026 年 10 月 30 日

株式会社ビジュアルアーツ

不正アクセスによる社内情報および個人情報漏えいの可能性に関するお知らせとお詫び（第 3 報　最終報）

平素より弊社事業にご理解とご支援を賜り、誠にありがとうございます。

2026 年 6 月 4 日および 7 月 31 日にお知らせいたしました「不正アクセスによる社内情報および個人情報漏えいの可能性に関するお知らせとお詫び」につきまして、外部専門機関によるフォレンジック調査の報告書を 2026 年 10 月 21 日に受領いたしました。その調査結果および現在の対応状況をご報告申し上げます。

改めまして、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、心より深くお詫び申し上げます。

なお、個人情報保護委員会に対しては、2026 年 5 月 11 日に速報を提出した後、2026 年 6 月 29 日付で確報を提出いたしました。

1. 外部専門機関による調査結果について

弊社では、本件において、クラウドサービスへのアクセスに用いる認証情報が窃取された経路を調べるため、外部専門機関による調査を実施いたしましたが、その経路の特定には至りませんでした。

調査では、当該認証情報が保存されていた可能性のある開発用端末および開発関連の処理を実行する端末を対象に、端末に残された記録などを解析するフォレンジック調査を実施いたしました。調査期間は、2026 年 9 月 15 日から 10 月 21 日までです。

今回の調査で確認できた範囲では、対象端末に、本件に関連する不正アクセスやマルウェア感染などの侵害を示す明確な痕跡は確認されませんでした。ただし、一部の記録には本件の発生当時の情報が残っていないなど、調査上の制約がありました。このため、今回の調査結果をもって、対象端末への不正アクセスや、当該端末を通じた認証情報の窃取がなかったと判断することはできません。

2. 漏えいした可能性がある個人情報の範囲

2026 年 6 月 4 日付のお知らせでご案内した範囲について、現時点で新たに対象となる情報は確認されておりません。

3. 現時点での被害状況

現時点において、「anemoi」のマスターデータ以外の情報が外部サイト等で公開・拡散されている事実は確認されておりません。また、漏えいした可能性のある情報を利用した二次被害も確認されておりません。引き続き監視を継続してまいります。

4. 再発防止策の進捗状況

弊社では、外部専門機関の協力を得ながら、再発防止策の実施を継続しております。

- 監視体制の強化：社内システムに対する 24 時間体制の監視サービス（MDR）の全社導入が完了いたしました。
- 認証基盤・アクセス権限の点検：外部専門家の支援のもと、社内で利用するクラウド・ID 基盤のセキュリティ設定について点検を実施しており、認証方式・アクセス権限の見直しを進めております。
- ネットワーク・境界防御の強化：社内ネットワークの構成やファイアウォール等の境界防御について、外部専門業者と協議のうえ、強化策を検討し、一部の施策については実施を進めております。
- 経営層への報告体制の強化：本件を踏まえ、セキュリティガバナンスに関する経営層への定期報告体制を強化し、対策の実施状況を継続的にモニタリングする体制を整えております。
- セキュリティ教育の実施：予定しておりました全従業員対象の情報セキュリティ教育を実施いたしました。
- 全社的なロードマップに基づく実施：以上の取り組みは、外部専門家の助言を踏まえた包括的な改善計画に沿って、引き続き優先順位をつけながら順次実施しております。

なお、本件に関する定期的なご報告は今回をもって終了いたしますが、今後、新たにお知らせすべき事項が判明した場合には、速やかに公表いたします。

5. お問い合わせ窓口

本件に関するご照会は、下記の担当窓口にてお受けしております。

株式会社ビジュアルアーツ　特別対応窓口

メールアドレス：contact.privacy@visual-arts.jp

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、改めて深くお詫び申し上げます。再発防止と信頼回復に向け、全社一丸となって取り組んでまいります。

以　上