

不正アクセスに関するお知らせ 第4報・続報 (2026/08/17)

2026.08.17

お知らせ

お客様各位

平素より弊社サービスをご利用いただき、誠にありがとうございます。
株式会社ロジックベインでございます。

弊社では、2025年12月8日付「不正アクセス発生に関するお知らせ」、2026年1月30日付「不正アクセスに関するお知らせ 第2報」および同年2月27日付「不正アクセスに関するお知らせ 第3報・最終報告」により、弊社ネットワーク環境への不正アクセスおよびこれに伴うファイル暗号化被害（以下「本件」といいます。）についてご報告を申し上げてまいりました。

2026年2月27日付の第3報においては、本件事案に関する弊社からの定期的なお知らせを最終報告とさせていただき旨をご案内しておりましたが、その後も、弊社にて、必要な確認および精査を進めておりましたところ、本件に関して追加でお知らせすべき事実が判明いたしましたので、本第4報・続報において追加でご報告申し上げます。本件により、お客様、お取引先の皆様その他関係者の皆様には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。

1. 本件の概要

攻撃者からのランサムウェア攻撃により、本件が発生したことが2025年12月8日に発覚いたしました。弊社は、本件が発覚した後、直ちに被害拡大防止措置を講じるとともに、外部専門機関と連携してフォレンジック調査を実施し、上記各公表を通じて、その状況をご報告してまいりました。

第3報の後も、弊社は、外部専門機関による調査を引き続き実施していたところ、その調査により、後記

2. のとおり、弊社が保有していた情報の一部がダークウェブ上のリークサイト（専用のブラウザ等を利用しなければアクセスできないウェブサイトです。）に掲載されていることを新たに確認いたしました。

なお、後記4. のとおり、現時点において、当該リークサイト以外での当該掲載情報の公開・拡散、掲載された情報の不正利用による二次被害は確認されております。

2. 漏えい等が発生し、または発生したおそれがある個人情報の項目及び本人の数

現時点において、本件によって漏えいが発生し、または発生した可能性があるデータは、以下のとおりです。

＜ダークウェブ上のリークサイトへの掲載が確認された情報項目＞

・お客様、お取引先の方および展示会等でご来場いただいた方等の氏名、所属先情報（会社名、部署名）、連絡先情報（メールアドレス、住所、電話番号）等

＜ダークウェブ上のリークサイトへの掲載は確認されていないものの、漏えいのおそれがある情報項目＞

・上記のほか、弊社とのメールでのやり取りに記載された個人情報、お客様との販売履歴に関連する個人情報、弊社製品の評価版ダウンロードの際にご入力いただいた個人情報、展示会において取得した個人情報、弊社がデータとして管理していた契約書に記載された個人情報等

※なお、クレジットカード情報やマイナンバーが含まれていた事実は確認されております。

本件によって漏えいが発生し、または発生した可能性のある方の数は、約97,338名です。このうち、実際にダークウェブ上のリークサイトへの情報の公開が確認されている方の数は、17,559名です。

3. 本件の原因

これまでの公表文書においてもご報告してまいりましたとおり、弊社がフォレンジック調査を依頼した外部専門機関による調査の結果、本件は、攻撃者が弊社のVPN接続を経由して社内ネットワークに不正にアクセスし、ランサムウェアを実行したことにより発生したものと推測されます。そして、今回のダークウェブ上への情報のリークも、当該不正アクセスによって情報を窃取されたことが原因であると考えられます。弊社は、本件を重く受け止め、本件発覚後速やかに、全端末のインターネット接続を遮断するとともに、後記6. の再発防止策を実施しつつ、現在も継続してセキュリティ対策の強化に取り組んでおります。

4. 二次被害またはそのおそれの有無および内容

現時点で、リークサイト以外での情報公開や、SNS等を通じた情報の拡散、本件に起因するお客様の個人情報を用いた不正利用等の二次被害については、確認されております。

カテゴリ

お知らせ

ご案内

ご報告

アップデート

イベント

ニュースリリース

メディア情報

新着情報

社長コラム

5. 不正アクセスの発生と関係機関への対応状況

弊社は、本件の発覚後、個人情報保護委員会に対し、個人情報保護法に基づく報告を速やかに実施し、その後も調査の進展に応じて複数回にわたり追加の報告を行っております。また、警察に対しても被害の相談を行っております。さらに、外部専門機関に対してフォレンジック調査を依頼し、本件の原因および影響範囲の調査を実施いたしました。

本人通知の対象となる方に対しましては、電子メール、書面その他の個別の通知に向けて準備を進めており、順次ご案内をお送りしております。なお、連絡先の確認ができず個別の通知が困難な方に対しましては、本公表をもって代替的にお知らせいたします。

6. 再発防止策

弊社は、本件発覚後、速やかに全端末のインターネット接続を遮断するとともに、外部専門機関と連携のうえ、フォレンジック調査の実施、不正な挙動を検知・防御する仕組みであるEDR（Endpoint Detection and Response）の導入、アクセス権限管理の再設計および認証強度の引き上げ等の再発防止措置を実施しました。

これに加え、ISO27001の早期取得、ログ管理体制の強化、セキュリティ担当部署の設立等のセキュリティ体制の強化に引き続き取り組んでおります。

今後も、外部セキュリティ専門機関、外部弁護士と相談しながら再発防止に向けた取り組みを継続し、より安心・信頼いただける環境の構築に尽力させていただきます。

7. 今後の見通し

引き続き、関係各所および外部専門機関と連携して、本件の全容解明、被害の拡大防止および実効性の高い再発防止策の策定に向けて全力で取り組んでまいります。今後、新たな事実が判明した場合には、速やかに個別のご連絡または弊社ホームページにおける公表等でご報告いたします。

皆様には、多大なるご心配をおかけいたしますことを深くお詫び申し上げます。

8. お問い合わせ窓口

本件に関するご質問等がございましたら、以下の窓口までお問い合わせください。

株式会社ロジックベイン セキュリティ対応窓口

Email：privacy@lvi.co.jp

受付時間：平日 9:00-17:30

お客様に安心してサービスをご利用いただけるよう、引き続き全社を挙げて対応してまいります。

何卒ご理解賜りますようお願い申し上げます。

■過去掲載内容については、こちらから参照できます。

- ・[不正アクセスに関するお知らせ 第3報・最終報告 \(2026/02/27\)](#)
- ・[不正アクセスに関するお知らせ 第2報 \(2026/01/30\)](#)
- ・[不正アクセス発生に関するお知らせ \(2025/12/8\)](#)



[記事一覧へ](#)

無料ダウンロード（30日間）

[お問い合わせ](#)



