

【重要なお知らせ】ランサムウェアによる不正アクセスに関するご報告（第六報）

2026年6月4日

株式会社東北新社 代表取締役社長 小坂恵一
株式会社オムニバス・ジャパン 代表取締役社長 丸井庸男

平素は格別のご高配を賜り、厚く御礼申し上げます。

2025年12月9日に発覚いたしました、株式会社オムニバス・ジャパン（以下「オムニバス・ジャパン」といいます。）に対するランサムウェア攻撃による不正アクセス事案（以下「本件」といいます。）に関し、株式会社東北新社（以下「弊社」といいます。）およびオムニバス・ジャパンが外部専門機関と連携して実施した調査において確認された内容を踏まえ、以下のとおりご報告いたします。

2025年12月17日付けの第一報、同月26日付けの第二報、2026年1月22日付けの第三報、同年2月13日付の第四報および同年3月12日付の第五報の内容は[こちら](#)です。

1. 本件の概要

外部の攻撃者（以下「攻撃者」といいます。）からのサイバー攻撃により、オムニバス・ジャパンが運用するサーバーにおいて不正アクセス事案が発生したことが、2025年12月9日に発覚いたしました。攻撃者によって、当該サーバーに保管されていた一部の情報が暗号化されるとともに、その一部が、専用のブラウザ等を利用しなければアクセスできないダークウェブ上の攻撃者のリークサイト（以下「リークサイト」といいます。）に公開される事象を確認いたしました。

フォレンジック調査の結果、不正アクセスの対象となったサーバーのうち1台について、ファイルが外部に持ち出された形跡は確認されなかったものの、当該サーバーに保存されていたファイルと同一のファイルがリークサイト上に公開されていることを確認いたしました。このため、当該1台のサーバーに保存されていた情報については流出した可能性を否定できない一方、それ以外のサーバーについては、持ち出しの痕跡や新たな情報公開がいずれも確認されていないことから、流出の可能性は極めて低いものと考えております。

2. 漏えい等の原因

本件の直接の原因は、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でも特定に至りませんでした。パスワードの運用や監視体制に不足があったこと、およびネットワーク機器の設定不備が本件の原因であると推測しております。

3. 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、本件に起因する情報の不正利用等の二次被害については、確認されておりません。

万が一、弊社またはオムニバス・ジャパンを騙り、または攻撃者を自称する等の不審なメール等を受信された場合は、開封せず、また当該メッセージに記載された URL 等へのアクセスはなさないようお願い申し上げます。

4. オムニバス・ジャパンのサーバーから漏えい等した可能性のあるデータ

現時点で、オムニバス・ジャパンにて制作された映像作品の出演者および制作スタッフ（計 800 名。弊社グループ社員・元社員を含みます）の氏名、所属先情報、連絡先情報および一部の顔画像等の個人情報が、漏えい等した可能性のあるデータに含まれております。

※ 上記の方々のうち、弊社が連絡先情報を保有しているの方々に対しては、順次、個別にご連絡を差し上げております。

5. 今後の公表の実施状況

今後、新たな事実が判明した場合には、速やかにオムニバス・ジャパン及び弊社ホームページにおける公表等でご報告いたします。

6. 再発防止策

弊社およびオムニバス・ジャパンは、事案発覚後、速やかに対策本部を設置し、外部専門機関と連携のうえ、オムニバス・ジャパンにおいて、該当システムのネットワーク切り離し、端末・サーバーの安全性確認、ファイアウォールの新規導入、監視体制の新規構築等の再発防止措置を実施済みです。

これに加え、オムニバス・ジャパンにおいて、制作物の運用ルールの策定、従業員に対する教育の実施、定期的な IT 監査の実施等のセキュリティ体制の強化を行ってまいります。

7. 今後の対応

今後も、外部セキュリティ専門機関および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。

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。

< 本件に関するお問い合わせ先 >

株式会社東北新社

toiawase_security@tfc.co.jp