2024 年 11 月 29 日

関係者様各位

ライクキッズ株式会社
代表取締役　岡本 泰彦

サイバー攻撃被害の可能性について(第３報)

2024 年 10 月 1 日に公表しました「サイバー攻撃被害の可能性について（第１報）」のとおり、当社システムが外部よりランサムウェアによる攻撃を受けました（以下、「本件」といいます)。関係者の皆様にはご迷惑とご心配をおかけする事態となりましたこと、深くお詫び申し上げます。

当社では本件が発生して以降、緊急対策本部を立ち上げるとともに、外部専門家の支援を受けながら、不正アクセスの原因や情報漏洩の可能性、および影響を及ぼす可能性のある情報の範囲を把握するための調査を鋭意進めてまいりました。このたび現時点での調査結果として判明しました内容をご報告申し上げます。また、個人情報保護委員会にも、本内容を報告しております。

1. 経緯と対応状況

2024 年 9 月 30 日早朝（日本時間）にシステム障害が発生しました。調査の結果、当社の複数のサーバがランサムウェアに感染し、データが暗号化されていることを確認しました。感染が確認されたシステム環境は外部とのネットワークを遮断しており、被害の拡大を防ぐための対応を実施しております。

現在、主要業務につきましては、手動での対応を行うとともに、既存環境とは分離し、隔離されていたシステムを利用することにより継続しております。システムの復旧につきましては、被害を受けたネットワーク環境は再利用せず、新しい環境を構築した上で、システムの完全な復旧を予定しております。外部専門家の助言及びチェックを受けながら、新しい環境の構築を進めてまいります。

2. 不正アクセスの原因

本件は、インターネットとの接続口の脆弱性を攻撃者に悪用され、当社の環境へ侵入されていたことが判明しております。当社ではこの事態を重く受け止め、再発を防止すべく外部専門家による助言及びチェックを受けながらさらなる対策を講じてまいります。

3. 個人情報の漏洩について

本件により暗号化されたサーバには、下記の個人情報を含むデータが保存されておりました。これらの個人情報の漏洩の有無に関して、外部専門家による調査を実施し、その結果、サーバ内の個人情報を閲覧された可能性はございますが、個人情報データを持ち出された形跡は確認されませんでした。現時点において、本件に起因する個人情報を用いた不正利用等の二次

被害については、確認されておりません。引き続き、お取引先様名や当社名を騙る不審な電話やメール等による勧誘や詐欺には十分にご注意いただき、不審に思われた場合は、下記フリーダイヤルまでご連絡いただきますようお願い申し上げます。

【保存されていた個人情報】

合計　：　158,410 件

内容　：　お預かりしている園児・児童（卒園者を含む）の個人情報

－氏名、生年月日、アレルギー情報等の要配慮個人情報

お預かりしている園児・児童（卒園者を含む）の保護者の個人情報

－氏名、生年月日、住所、電話番号、メールアドレス、口座情報

従業員（退職者を含む）の個人情報

－氏名、生年月日、住所、電話番号、メールアドレス、口座情報、マイナンバー情報、性別・学歴等の属性情報、勤務場所などの人事情報

外部講師、嘱託医、施設貸主の個人情報

－氏名、住所、電話番号、口座情報

【相談窓口】

ライクキッズサポートセンター

TEL ： 0120-230-513　　受付時間：平日 10：00～18：00

4. 公表の経緯について

2024 年 10 月 1 日に当社ホームページにて「サイバー攻撃被害の可能性について（第１報）」ご案内し、その後 2024 年 10 月 31 日に「サイバー攻撃被害の可能性について（第２報）」をご案内いたしました。その後、本調査結果の公表に至るまで時間を要したことを深くお詫び申し上げます。

5. 再発防止策について

当社はこのたびの事態を厳粛に受け止め、調査結果を踏まえてシステムのセキュリティ対策および監視体制の強化を行い、再発防止に努めてまいります。

本件により、関係者の皆様には多大なご迷惑とご心配をおかけしたことを重ねて深くお詫び申し上げます。再発防止に向けて、全社を挙げて情報セキュリティ体制の構築と強化徹底を図り、信頼回復に努めてまいります。

以上