

対象となる情報主体(ご本人)様、及び保護者の皆様

2025年4月23日

齋藤コロタイプ印刷株式会社

代表取締役 齋藤 裕子



弊社工場システムへの不正侵入被害に関するお詫びとお知らせ

謹啓 皆様ますますご繁栄のこととお慶び申し上げます。

弊社、齋藤コロタイプ印刷(株)は、皆様の卒業アルバム作成に携わりました会社でございます。

先般、弊社工場のシステムが悪意のある第三者によってランサムウェアによる攻撃を受けたことが特定されました。「ランサムウェア」とは、不正侵入先のデータの取得を主目的とするものではなく、暗号化することでファイルを利用不可能な状態にした上で、そのファイルを元に戻すことと引き換えに身代金を要求する不正プログラムを指します。専門業者による調査の結果、情報の外部流出は確認されておりませんが、可能性としては否定出来ないということから、対象となる皆様へご報告させていただき次第となり、学校様へご報告、及び弊社ホームページにて情報公開を行うと共に、学校様の要請に基づき本書面を皆様へ送付させて頂いた次第でございます。

この度は、弊社工場のシステムに第三者の侵入を許してしまったこと、及び、皆様の卒業アルバムへ掲載されている情報の外部流出の可能性を否定出来ない状況であること、そして今回のサイバー攻撃に関しての情報の解析、分析や調査に時間を要したこと、及び弊社の対応不備等の不手際からご報告が遅くなってしまいましたこと、心よりお詫び申し上げます。

弊社に於きましてはこれまでも、複数のセキュリティ機能を集約したネットワークセキュリティ機器の設置、及びウイルス対策ソフトの導入等を行うと共に個人情報保護法に基づいた個人情報の適切な取扱いに関する対応を定め運用を行ってまいりました。その上で、今回の専門業者による調査結果や警察機関からのご助言から再発防止に向けた対策を既に実施しており、今後も、常に安全性の向上に努めて参る所存でございます。

改めまして、衷心より深く陳謝申し上げますとともに、今後の推移のご報告と対応につきましては、適宜誠実に取り組んで参りたく存じ上げます。

尚、経緯詳細、ならびに対策につきましては以下のようにご報告させていただきます。

敬白

記

【概要】

2024年7月に弊社工場においてネットワーク接続異常が発生したことから、関連システムを停止し関連業者様の協力を受け内部調査を行ったところ、外部からの不正侵入によるトラブルの可能性が高いと思われることから、担当行政機関である個人情報保護委員会、及びプライバシーマークの審査機関である日本印刷産業連合会へ報告を行うと共に専門業者へ相談し、情報の解析や分析、調査を進めたところ、2024年11月末の結果報告にて「ランサムウェア」によるサイバー攻撃を受けたものと特定されました。

「ランサムウェア」とは、暗号化することでファイルを利用不可能な状態にした上で、そのファイルを元に戻すことと引き換えに身代金を要求する不正プログラムを指します。

今回サイバー攻撃を受けたサーバーには弊社が作成しました2023年度卒業・卒園アルバムのデータを保管しており、その内、データ全体の2.5%のデータが暗号化による被害を及ぼした状況にあります。暗号化されたデータ、及び、同サーバー内の他のデータにつきましても、外部流出(ダウンロードによる情報の抜き取り)の事実は確認されておきませんが、「ランサムウェア」によるサイバー攻撃を受けた際、サーバー上の個人情報を一時的に第三者に閲覧されたり、一部を抜き取ったりされた可能性を否定できないため、本件の被害状況は「個人情報漏洩のおそれ」となっております。

また、今回の攻撃を受けたサーバーにつきましては運用を停止し、バックアップデータにて新たなサーバを設置し、外部への通信を遮断する等の対策を施し暫定的運用を行っておりましたが、現在は専門業者からのアドバイス等を参考に、システムに新たな安全対策を施した上で運用を開始している状況でございます。

【漏えい等が発生したおそれがある個人情報データ】

2023年度卒業アルバム掲載データ(氏名・写真)

※文集は対象外でございます

【原因】

調査により、第三者がVPN接続(インターネット上に仮想的な専用線を作成し、データを暗号化して送受信する通信方法)機器を経由し不正アクセスをした為と判明致しました。

【二次被害又はそのおそれの有無及びその内容】

現時点におきまして、本件による被害報告はございません。

【データの滅失】

弊社におきましては、アルバム制作に利用したデータの全てを、内部規定で定めた期間について、普段は起動しない状態で別の保存媒体にバックアップデータを保存しておりますので、本件によるデータの滅失は

ございません。

【対策】

弊社では、従前より個人情報保護に係る規程等を整備し、プライバシーマークを取得した上で、個人情報の安全な運用を心がけており、ウィルス対策ソフトの導入や UTM と呼ばれる複数のセキュリティ機能を集約したネットワークセキュリティシステムの導入により不正侵入検知等の機能を実装しておりましたが、調査会社及び警察機関からのアドバイスをもとに、改めて以下の再発防止策を実施いたしました。

- ・原因となりましたネットワークに対し外部から接続する通信手段 (VPN 接続) を廃止致しました。
- ・全従業員のアカウントに対して、より複雑で推測されにくいパスワードへ変更しました。
(今回の攻撃で万が一従業員のパスワードが知られてしまった場合、その情報をもとに不正にアクセスされてしまうことを防ぐ為)
- ・外部からのネットワークに接続する際に使用される、インターネットの「住所」であるグローバル IP アドレスの変更を行いました。
(攻撃を受けた時のアドレスから変更を行うことで、以前の情報をもとにした不正アクセスを防ぐ為)
- ・ネットワークセキュリティシステム自体に存在していた、外部からの攻撃に対して弱点となる箇所がないか詳細に調べ、アップデートを行うなどの対策を実施しました。(脆弱性対策)
- ・ネットワークセキュリティシステムへの外部からのアクセス履歴について、システム本体とは別にクラウドサービスへ保存体制を構築しました。(システム本体とは異なる場所にアクセス履歴の情報を保存することで、第三者によって不正アクセスの侵入履歴を改ざんされるのを防ぐ為)
- ・今回の原因となったネットワーク以外において、テスト的に運用を行っているリモート通信環境のセキュリティを強化する為、2 段階認証を適用致しました。

また、弊社におきましては、従業員に対して個人情報の取り扱いを含む個人情報保護マネジメントシステム規定の年次教育を継続して実施しておりますが、更に本事案を受け、教育内容を改めて刷新し、鋭意社員教育の徹底に努めて参ります。

【お問合せ先】

斎藤コロタイプ印刷株式会社

個人情報窓口

〒980-0811 宮城県仙台市青葉区一番町 2-7-10

E メール soumu@saicollo.co.jp

電話 022-222-5481 (平日 8:30～16:30)

FAX 022-222-5416