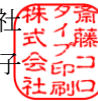


関係山形県立中学校・高等学校 様

2025年4月25日

齋藤コロタイプ印刷株式会社
代表取締役 齋藤裕子



弊社工場へのランサムウェア攻撃に関するお知らせ

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、学校指定の撮影事業者からの委託で貴校の卒業アルバムの作成に携わっている会社でございます。

先般、弊社工場のシステムがランサムウェア※1の攻撃を受けたことが特定されました。また、調査の結果、皆様の卒業アルバムに掲載されている個人情報(お名前・お写真)につきましては漏えいの可能性を完全に否定することが出来ないという結論に至りましたことから、弊社委託元となります写真館をはじめとした撮影業者様及び学校様へご報告、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。

この度は皆様のお名前とお写真のデータを保管しているサーバーに第三者の侵入を許してしまったこと、そしてデジタルフォレンジック※2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。

また、弊社に於きましてはこれまでも、UTM(統合型脅威管理装置)の設置、及びウイルス対策ソフトの導入等を行うと共にJIS Q 15001:2017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おりましたが、今回のデジタルフォレンジック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ます。

尚、経緯詳細に関しましては、次ページ以降にてご報告させていただきます。

敬白

※1 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金銭（身代金）を要求するマルウェアを指します。

※2 デジタルフォレンジックとは

コンピューターやスマートフォンなどのデジタル機器に保存された情報を解析し、証拠を収集・分析する技術です。サイバー犯罪や情報漏洩などの捜査や、訴訟などの法的紛争において用いられます。

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、ランサムウェアによる攻撃の可能性があるとのことから、個人情報保護委員会、及び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デジタルフォレンジック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の攻撃を受けたものと特定されました。

また、当該システムに付きましては外部への通信を遮断する等の暫定的運用を行っておりましたが、フォレンジック調査会社からのアドバイス等を参考にセキュリティ強化対策を実施した上でバックアップデータを用いてサーバ等の再構築を順次行い、1月20日に完全復旧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年度卒業アルバム記載データ(氏名・写真)

【原因】

フォレンジック調査により、第三者がVPN接続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】

現時点において、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の別立てでの保存媒体にアーカイブ(コールドスタンバイ)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 P 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 機器(統合型脅威管理機器)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。

- ・パスワードポリシーをより複雑な条件に変更し全ユーザーにおいて変更を行いました。
- ・UTM 機器(統合型脅威管理機器)の脆弱性対策を実施致しました。
- ・UTM 機器(統合型脅威管理機器)のアクセスログについて、外部への保存体制を構築致しました。(クラウドサービスを利用)
- ・原因となりました業務系ネットワークに対する VPN 接続設定を廃止致しました。
- ・制作系ネットワークにて進めているリモート環境での作業テストに付きましては VPN 接続に Token による2要素認証を適用致しました。
- ・接続回線のグローバル IP アドレスの変更を行いました。

【その他参考となる事項】

弊社工場のネットワーク環境につきまして、メールやインターネット接続による業務を主とした「業務系ネットワーク」、及びアルバム制作業務を行う「制作系ネットワーク」があり、各端末は共通のログイン認証用サーバ(Active Directory サーバ)を経由して当該ネットワークへの接続を行う環境となっております。

【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