

ファイルサーバ等への不正アクセスに関するご報告

2024年4月28日に発生した東急株式会社(以下、東急)の連結子会社(東急ストア子会社)である東光食品株式会社(以下、東光食品)のファイルサーバ等(情報保管機器)への不正アクセスにより、データの一部が不正に読み出された件(以下、本件)に関し、多大なるご心配とご迷惑をおかけいたしましたこと深くお詫び申し上げますとともに、再発防止に努めてまいります。

詳細は下記のとおりです。

記

1. 本件の概要と調査経緯

- 2024年4月28日に東急が構築中の社内で利用する新たなネットワーク基盤の検証用環境(以下、検証用環境)が第三者からの不正アクセスを受け、検証用環境を経由して東急の既存ネットワーク環境(以下、既存ネットワーク環境)へ不正な接続が行われ、既存ネットワーク環境にあった東光食品が管理しているファイルサーバからお客さま等の個人情報が外部へ流出した可能性があることが判明しました。
- 不正アクセス発見後、ログ等により発生原因を突き止め、直ちに拡大防止の措置を行いました。東光食品が管理するファイルサーバからデータの一部が持ち出された形跡を確認しました。
- 持ち出されたデータの特定ができなかったことから、東光食品が管理するファイルサーバに含まれる全てのデータが持ち出されたことを想定し、全ファイルに含まれるすべての個人データの調査を行い、流出した可能性のある個人データの特定を行いました。

※個人情報保護委員会に報告済みです。

※東光食品が管理しているファイルサーバ以外の機器から、個人データの持ち出しがないことは確認しています。

※現時点において、お客さまの個人情報等の不正利用などの事実は確認されておりません。

※検証用環境と既存ネットワーク環境の接続は切断済み、かつ東光食品が管理しているファイルサーバは別の仕組みに変更が完了しているとともに、ランサムウェア等による暗号化やマルウェア等がないことを確認しています。

2. 流出した可能性がある個人データ

属性	主な情報	件数
個人のお客さまに関するもの	氏名、住所、電話番号、メールアドレス	901件
お取引事業者さまに関するもの	氏名、所属(会社、部署)、住所、電話番号、メールアドレス	9,942件
従業員に関するもの (退職者情報含む)	氏名、住所、電話番号、メールアドレス	5,802件

※マイナンバーカード、クレジットカード情報は含まれておりません

3. 本件の発生原因

- ・検証用環境が脆弱な状態となっていたこと
- ・既存ネットワーク環境にあった東光食品が管理しているファイルサーバが脆弱な設定となっていたこと
- ・個人データの削除を含む、管理ルールが徹底されていなかったこと

4. 再発防止策

- ・東急は、検証用環境を含め、ネットワーク全体のセキュリティ管理強化を行いました。
- ・東光食品は、発生原因となったファイルサーバの入れ替えを完了し、原因となった設定の改善を完了しております。また、個人情報に関する管理体制を強化し、改めて個人情報の管理ルールについて、従業員へ徹底してまいります。

5. コールセンターの設置およびお客さまへのご案内について、

本件に関し、流出した可能性のある個人データに該当する方々へは個別にお詫びとお知らせをお送りさせていただくとともに、本件について以下の専用お問い合わせ窓口を設置いたしました。

東光食品 専用お問い合わせ窓口(受付時間: 平日9:00~18:00)
電話番号 0120-367-192

以 上