2026年2月16日
東京都板橋区板橋４－２－３
株式会社ソーゴー

弊社ファイルサーバへの不正アクセス事案に関する調査結果のご報告（最終報）

拝啓

平素は格別のご高配を賜り、厚く御礼申し上げます。
2025年2月公表「弊社ファイルサーバへの不正アクセスによるサイバー攻撃に関する調査結果のご報告」にてご報告申し上げました通り、弊社社内にある複数台のファイルサーバが、第三者の不正アクセスによるサイバー攻撃を受けた件につきまして、多大なるご心配とご迷惑をおかけしておりますことを、深くお詫び申し上げます。

当社では本件発生以降、外部専門機関の協力のもと、影響範囲の特定およびセキュリティ対策の強化を進めてまいりました。 この度、長期にわたる影響調査を完了し、あわせて多角的な再発防止策を講じることで、安全な運用体制を構築いたしました。
つきましては、最終的な調査結果と現在のセキュリティ体制について、下記の通りご報告申し上げます。
今後も外部専門機関と協力のもと、全社を挙げて情報セキュリティの強化に取り組み、信頼回復に努めてまいる所存です。何卒ご理解賜りますようお願い申し上げます。

敬具

記

1.事案の概要
2024 年11月11日午前8時頃、弊社社員が社内に設置されているファイルサーバにアクセスできない旨の報告を受け確認を行なったところ、当該ファイルサーバが第三者の不正アクセスによるサイバー攻撃を受けたことが発覚しました。直ちに調査を開始し、警察への被害申告を行い、個人情報の漏洩の有無、および復旧に向けて対応を進めておりました。

2.ダークサイト調査（※1）の経過報告について
専門調査機関により、本件に関連する情報の漏洩・公開の有無を1年間にわたり継続的に調査・監視いたしましたが、現時点において情報の流出事実は確認されておりません。
専門家の見解において、攻撃から1年が経過しても情報が公開されない場合、今後の流出や悪用リスクは極めて低いと判断されます。 つきましては、お客様に安心してご利用いただける安全性が確認されたものとし、本期間の満了をもってモニタリング調査を完了とさせていただきます。

3. 実施した取り組みについて

(1) データ管理環境のクラウド移行および堅牢なバックアップ体制の確立

(2) メールセキュリティ製品の導入による侵入経路対策の強化

(3) 全PC端末およびサーバ端末へEDR製品 **(※2)** の導入および監視体制の整備

(4) セキュリティ専門会社の支援による現状のセキュリティ対策状況の網羅的な確認

(5) 再発防止のためのセキュリティ運用体制の見直しおよび強化

(6) 全社員を対象とした情報セキュリティ教育の徹底

※1.一般的な検索エンジンではアクセスできないダークウェブを対象にした違法活動や情報流出の監視・調査

※2.EDR（Endpoint Detection and Response）：端末の不正な挙動を監視し、ウイルス感染の早期検知を目的とした セキュリティ対策製品

以上