2025 年 3 月 21 日

光精工株式会社

ランサムウェア被害に関わる調査結果のご報告(第 2 報)

当社は、２０２５年1月１９日にランサムウェア攻撃を受け、サーバー内の情報が暗号化される被害に遭いました。本件については、２０２５年2月４日にホームページ上で初報を公開いたしましたが、このたび、外部の専門企業と協力して進めてきた調査が完了しましたので、調査結果および再発防止に向けた取り組みについてご報告いたします。
お客様をはじめ多くのご関係先にご迷惑、ご心配をおかけいたしましたことを深くお詫び申し上げます。また、対応について多くのご支援を賜り、心より感謝申し上げます。

記

1.調査結果

(1) 被害の原因

弊社のリモートアクセスサービスに対し、委託先システムベンダが管理するユーザ認証情報が不正に利用されたことが確認されました。現在、漏洩の原因、漏洩元、および漏洩が発生した時期について調査を継続しております。

２０２４年1月１１日に攻撃者が漏洩したアカウント情報を利用してリモートアクセスサービスを経由し、弊社社内ネットワークに不正侵入し、探索行為を行っていたことが調査により確認されております。さらに、同月１４日に、侵入経路を利用して弊社ドメインサーバにバックドアプログラムが埋め込まれ、攻撃用の仮想ネットワークが社外および社内に構築されていたことが判明しました。

⑵ 被害の状況

２０２４年1月１４日から１９日にかけて EDR（Endpoint Detection and Response）が無効化され、ユーザ認証情報が不正に取得され、その後データが転送されたことが確認されました。最終的に、1 月 19 日に社内の各システムに暗号化実行ファイルが登録され、ファイルが暗号化されました。

EDR：Endpoint Detection and Response とは、デバイスの状況を監視して、不正なアクセスやマルウェアの感染を検知・対処するソフトウェアです。

2.再発防止に向けた取り組み内容

本件の侵入経路となったリモートアクセスサービスは即日利用を停止し、全システムアカウントのパスワード変更を実施いたしました。また、メールサービスの多要素認証化を行い、なりすまし対策を強化しております。さらに、XDR（Extended Detection and Response）を導入し、セキュリティ強化を図りました。

今後は、外部の専門機関による脆弱性診断を行い、診断結果やアドバイスに基づき、継続的なセキュリティ改善および監視体制の強化を行い、再発防止に取り組んでまいります。

XDR（Extended Detection and Response）とは、EDR の機能を拡張し、エンドポイント以外のレイヤまで一貫して監視するソフトウェアです。

3.個人情報の流出可能性について

調査を通じて、社員をはじめ関係者の個人情報が外部に流出した可能性が高いことが判明しました。万が一、情報が流出した場合の二次被害の拡大防止を最優先に考え、流出可能性のある情報について、以下のとおりお知らせいたします。

本件については、２０２４年２月および３月に個人情報保護委員会への報告を行っております。

(1) マイナンバー情報

２０２２年１月以降当社に直雇用されていた一部の従業員

(2) 個人情報

個人情報は以下の先様の情報になります。

① お客様およびご関係者様
② 当社株主様
③ 採用候補者
④ 当社および関連会社の従業員および従業員であった方
⑤ 技能実習生・特定技能の方

4.マイナンバー情報の流出可能性がある方に向けた対応について

マイナンバー情報が流出した可能性がある方には、本件公表後に個別にご連絡を実施する予定です。

5.個人情報の流出可能性がある方に向けた対応について

個人情報が流出した可能性のある方に対して、後日ご連絡する予定です。なお、当社関係者・警察・行政機関をかたった「なりすましメール」や不審な連絡が届く可能性がありますので、ご注意いただけるようお願い申し上げます。

◆二次被害などに対するお問い合わせ先◆

光精工株式会社　総務部
電話 0594-22-3155　Fax　0594-22-3170

6.最後に

このたびは、皆様に多大なるご迷惑とご心配をおかけし、誠に申し訳ございません。心よりお詫び申し上げます。

当社では今回の事態を受け、警察および関係当局のご指導のもと、迅速かつ適正な対応を進めるとともに、再発防止策を徹底してまいります。なにとぞご理解とご協力を賜りますよう、お願い申しあげます。

以上