2024 年４月１日
各位

会社名 株式会社山田製作所
代表者名 代表取締役社長 佐藤 賢
問い合わせ先 取締役 事業管理本部長 宮嶋 俊幸
電話 0270-40-9111

ランサムウェア被害に関する調査結果のご報告(第３報)

当社は、第三者によるランサムウェアを用いた標的型攻撃を受け、当社サーバ保存情報の暗号化やアクセスログ抹消等の被害が発生したこと（以下「本インシデント」といいます。）を 2024 年２月７日及び８日に公表いたしました。

この度、外部の専門企業の協力のもと進めてまいりました本インシデントの調査が完了いたしましたので、調査結果及び再発防止に向けた取り組み等についてご報告を申し上げます。お客様はじめ多くのご関係先にご迷惑と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とともに、当社の本インシデントへの対応について多くのご支援を賜りましたことについて深く感謝申し上げます。

記

１．調査結果

（１）被害の原因

2024 年１月、当社保有のリモートアクセス装置が攻撃者からのサイバー攻撃を受け、当該リモートアクセス装置を通じて攻撃者が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ました。また、2024 年２月、クラウドサービス上に当社が構築していた当社サーバに不正侵入され、当該サーバからその他のドメイン配下のサーバにも不正侵入されていたことも確認されました。

（２）被害の拡大

2024 年２月６日の深夜に不正侵入されたサーバ上で EDR※1 機能を無効化した上でランサムウェア「LockBit」が展開され、社内ネットワーク上の複数のサーバに保存されていたデータが暗号化されました。併せまして、ランサムウェアの展開を実行したサーバのイベントログの消去を実施し、証拠の隠滅を図った痕跡も確認されております。

※1 Endpoint Detection and Response の略。パソコンやサーバ等の機器に不審な挙動を検知するソフトウェアを導入し、迅速な対応を支援する仕組み

２．再発防止に向けた取り組み

本インシデントにおいて侵入経路となった脆弱性への対策は完了しておりますが、より高度な情報セキュリティレベルを実現するために、外部の専門機関による脆弱性診断の結果やアドバイスに基づき、継続的な改善及びセキュリティ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。

３．マイナンバー情報及び個人情報の流出可能性について

本インシデントの調査を通じて、マイナンバー情報や個人情報が外部に持ち出された痕跡については現時点で確認できておりません。

しかしながら、外部流出の可能性を完全に否定することは難しいことから、万一、情報流出があった場合の二次被害の防止を最優先と考え、流出可能性のある情報について以下のとおりお知らせします。

なお、2024 年２月９日及び 2024 年３月 29 日に個人情報保護委員会への報告を実施しております。

（１）マイナンバー情報

①2016 年３月時点で、当社従業員であった方

（２）個人情報

①お客様及びご関係先のご担当者様

→氏名及び役職を含む、業務上の連絡先情報が主となります。

②当社株主様

③採用候補者様

④当社従業員及び過去当社従業員であった方

４．マイナンバー情報の流出可能性がある方に向けた当社対応

現時点では二次被害は確認されておりませんが、マイナンバー情報の流出の可能性がある方に対しては、情報の性質を鑑みた対応について順次個別にご連絡を実施いたします。

５．個人情報の流出可能性がある方に向けた当社対応

現時点では二次被害は確認されておりませんが、今後個人情報が流出した可能性がある方に対し、当社関係者になりすました不審メールやご連絡があるおそれがございますのでご注意いただけますようお願い申し上げます。

【二次被害等に関するお問い合わせ窓口】

当社　事業管理本部　人事部

電話: 0270-40-9254

皆様には、多大なるご迷惑とご心配をおかけしておりますことをあらためてお詫び申し上げます。

当社では、今回の事態を真摯に受け止め、警察及び関係当局の要請や指示には迅速かつ適正に対応するとともに、より一層の管理体制の強化に向けて努力してまいりますので、何卒ご理解とご協力を賜りますようお願い申し上げます。

以上