2024 年 12 月 25 日
株式会社フジクラ

当社ネットワークへの不正アクセスについて

このたび、当社が管理するサーバに対し、第三者による不正なアクセス及び情報流出の痕跡があったことが確認されました。対象のサーバの一部には個人情報も含まれておりました。

関係する皆さまに多大なるご迷惑とご心配をおかけすることになり、深くおわび申し上げます。

本件につきましては、すでに個人情報保護委員会に必要な報告を行い、外部のセキュリティ専門会社の協力を得ながら関係機関と連携し、事実の確認及び必要な対応に努めております。

引き続き調査その他の対応を続けているところではございますが、このたび、調査も一定程度進捗いたしましたので現時点で判明している事実及び当社の対応につき以下の通りご報告いたします。

１．本件の概要

2024 年 7 月 2 日、当社がネットワークの保守運用を委託している NTT コミュニケーションズ株式会社（以下「保守委託先」）が管理するネットワーク保守・監視用 VPN 装置を通じて、当社の情報ネットワークが外部からの不正なアクセスを受けたことが判明しました。

本事象を確認後、当社は保守委託先と協力して、ただちに侵入経路を特定し、不正使用されたアカウントの無効化、アカウント全保持者のパスワード初期化と利用制限、ネットワーク機器の交換及び認証の強化などの緊急対策を行いました。7 月 19 日から、保守委託先ほか外部セキュリティベンダーとともに、影響範囲を特定するためのフォレンジック調査※を開始いたしました。

※フォレンジック調査：不正アクセスやランサムウェア等のサイバー攻撃被害を受けた際に、原因や犯人の特定などを目的として、サーバ等のデバイスや記憶媒体等のデータを収集し、分析する専門的な調査手法。

フォレンジック調査を進める中で、当社佐倉事業所の複数のサーバに外部からのアクセス及びデータ流出の痕跡があったことが確認されました。流出したデータは各サーバのデータ保存量の一部に留まりますが、対象のサーバには個人情報が保存されていたものも含まれておりましたので、個人情報の漏えいのおそれは否定できないものと考えております。

２．原因と対策

保守委託先による原因分析調査の結果によると、本件の事案の原因は、保守委託先によるネットワーク保守・監視用 VPN 装置の管理に不備があり、その結果同装置に残っていた脆弱性が利用されたことによります。

不正アクセスの発覚後は、上記の通り緊急対策を実施しネットワークの安全を確保したほか、保守委託先に対して再発防止策の検討と実施を指示し、同社が保守運用サービスの運用体制の強化、運用ルールの改訂等を実施した旨を確認しております。当社においても、保

守委託先の管理体制を強化し、機器のログ等の情報収集体制を強化するなど、不正アクセスに対してより迅速に対応可能な体制を構築しました。

３．漏えいのおそれが生じた個人情報

本件により漏えいのおそれが生じた個人情報は、お取引先従業員、大学関係者その他の社外の方、並びに当社及びグループ会社の従業員・元従業員（ともに契約社員、派遣社員、アルバイト等含む）及びその家族等の個人情報で、氏名、住所、電話番号、メールアドレス、生年月日、性別等の連絡先情報・属性情報が中心であり、その他の従業員情報（当社が従業員から受領した情報も含む）や、人事関連情報、インボイス番号、銀行口座番号（暗証番号は含みません）等も一部含まれておりましたが、現時点においてクレジットカード情報やマイナンバーは確認されておりません。

４．今後の対応

現在、本件の対象となったご本人様を正確に特定するための調査を継続しておりますが、調査及びご連絡のための情報の整理が完了後、順次個別にご連絡差し上げることを予定しております。

５．二次被害又はそのおそれの有無及びその内容

現時点で、当社から流出したデータがインターネット上で公開されたなどの事実は確認されておらず、その不正利用などの二次被害も確認されておりません。もし、不審なメールを受け取られたなど、本件による被害が疑われる事例がございましたら、下記問い合わせ先までご連絡をいただきたくよろしくお願いいたします。

６．当社生産活動への影響等

本件による当社生産活動への影響はございません。また、現時点において、流出が問題となるような業務上の秘密の流出も確認されておりません。

当社では、今回の事態を真摯に受け止め、委託先との協働体制の強化を含め、情報セキュリティの一層の強化及び再発防止に全力で取り組んでまいります。

＜本件に関するお問い合わせ先＞

fjk.personalinfo@jp.fujikura.com