不正アクセスの発生に関する個人情報保護法に基づくご報告（第２報・最終報）

Report Based on the Act on the Protection of Personal Information Regarding the Unauthorized Access (the 2nd and final report)

2025年5月7日
株式会社フジクラ
May 7th, 2025
Fujikura Ltd.

2024年12月25日に当社のホームページ上で公表しておりますとおり、2024年7月2日に、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り、対象となったサーバ（以下「対象サーバ」）の一部に個人情報が含まれていたことが確認されました。関係者の皆様に多大なご迷惑とご心配をおかけしましたことを深くお詫び申し上げます。

As published on our website on December 25, 2024, we have acknowledged traces of unauthorized access and information leakage by a third party on servers managed by our company on July 2, 2024, and confirmed that some of the affected servers (the "Affected Servers") contained personal information. We deeply apologize for any inconvenience and concern this may have caused for all those involved.

当社では、その後も対象サーバに含まれていた個人情報について調査を継続し、この度調査が完了いたしました。前回の公表内容から著変ないところではございますが、以下のとおりご報告いたします。

We have continued to investigate the personal information contained in the Affected Servers, and the investigation is now complete. While there are no substantial changes from the information previously disclosed, we would like to report the following.

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。

1. Overview of the incident

On July 2, 2024, it was discovered that our information network had been accessed unauthorizedly from the outside through a network maintenance and monitoring VPN device managed by NTT Communications Corporation (the "Maintainance Vendor "), to whom we have outsourced network maintenance operations.

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。そして、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。

After acknowledging this incident, we immediately cooperated with the Maintenance Vendor to identify the intrusion route, deactivate the abused accounts, reset passwords and restrict usage for all account holders, replace network equipment, and strengthen authentication measures. Additionally, starting from July 19, we initiated a forensic investigation* with the Maintenance Vendor and another external security vendor to determine the extent of the impact by this incident.

* Forensic Investigation: A specialized investigation method that collects and analyzes data from storage media and devices such as servers, to identify the cause and culprits of cyber-attacks, including unauthorized access and ransomware incidents.

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、対象サーバには個人情報が保存されていたものも含まれていたため、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。

In the course of the forensic investigation, traces of external access and data leakage on multiple servers at our Sakura Works were discovered. Although the leaked data constitutes only a portion of the data stored on each server, some of the Affected Servers contained personal information, leading us to believe that there is a potential risk of personal information leakage.

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。

2. Cause and countermeasures

According to the results of the cause analysis conducted by the Maintenance Vendor, the incident was caused by deficiencies in the management of the network maintenance and monitoring VPN device by the Maintenance Vendor, resulting in vulnerabilities that remained in the device being exploited.

不正アクセスの発覚後は、上記のとおり緊急対策を実施して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。
After the discovery of unauthorized access, we implemented emergency countermeasures as described above to ensure network security.　Additionally, we instructed the Maintenance Vendor to examine and implement measures to prevent recurrence.　We have confirmed that the Maintenance Vendor has strengthened their operational framework for maintenance services and revised their operational rules. We have also reinforced our management system for the Maintenance Vendor and enhanced our information collection system, including equipment logs, to respond more swiftly to an unauthorized access.

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、お取引先従業員様、大学関係者様その他社外の方、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、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。
3. Personal information at risk of leakage
The personal information at risk of leakage due to this incident included that of employees of our business partners, university affiliates, and other external parties, as well as the employees and former employees (including contract employees, temporary staffs, part-time workers, etc.) of our company and group companies, and their families. This primarily consisted of contact and attribute information such as names, addresses, phone numbers, email addresses, dates of birth, and genders.　Additionally, certain employee information (including information we have received from employees), HR information, invoice numbers, and bank account numbers (excluding PINs) were also included.　However, no credit card information or My Number (Individual Number) has been detected.

4. 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。

4. Possibility of secondary damage or the risk thereof and its content

At present, we have not acknowledged any facts indicating that the data leaked from our company has been published on the internet, nor have we acknowledged any secondary damages such as unauthorized use thereof.　Should you receive any suspicious emails or encounter any cases that may indicate damage related to this incident, please contact us at the inquiry address below.

5. 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、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。

5. Impact on our production activities

There is no impact on our production activities due to this incident.　Additionally, no leakage of business secrets that could cause issues has been detected.

6. お問い合わせ

　本通知に関するお問い合わせは、下記の連絡先までお願いいたします。

　fjk.personalinfo@jp.fujikura.com

6. Inquiries

For inquiries about this notice, please contact us at the address below.

fjk.personalinfo@jp.fujikura.com

　皆様には多大なご迷惑とご心配をおかけしましたことを改めて深くお詫び申し上げます。本件について個人情報の漏洩のおそれがあることが判明したご本人様については、当社が把握しているご連絡先に対して順次個別のご通知を差し上げます。

　当社は、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。

We sincerely apologize again for any inconvenience and concern this may have caused. For those individuals whose personal information is at risk of leakage, we are going to send an individual notification to the contact information we have on record.

We take this incident very seriously and are committed to strengthening our information security measures and preventing recurrence, including enhancing our collaboration with subcontractors.

以上

End