2026 年 4 月 27 日
アルプスアルパイン株式会社

社内システムアクセス用の個人情報に対する不正アクセスについて

このたび、当社が利用している外部 VPN システムに不正アクセスを受け、個人情報が外部の攻撃者に閲覧された可能性を否定できない事案が発生したことが判明いたしました。
関係する皆様をはじめ、関係各位にご心配をおかけしておりますことをお詫び申し上げます。
本事案につきましては、現在も調査を継続しており、現時点で判明している内容に基づき、ご報告いたします。なお、上記の不正アクセスを受けた可能性のある個人情報以外の当社および当社グループ会社の顧客情報や取引先情報等への不正アクセス事実は確認されておらず、現時点でそれらの情報が外部の者に閲覧された事実や外部に流出した事実は確認されておりません。

1. 事案の概要

2026 年 3 月 18 日、当社が利用している外部 VPN システムにおいて、当社の社内システムの保守管理等を委託している委託先事業者から、外部の者による不正なアクセスが行われた痕跡が確認された旨の連絡を受領しました。
4 月 13 日、その後の委託先事業者が実施した調査の結果、当社のサーバーに対しても、不正アクセスが行われたことが判明し、当社社内システムへアクセスするためにシステムに登録されている方の個人情報が外部から閲覧された可能性を完全には否定できない状況であることが判明いたしました。
なお、上記以外の顧客情報や取引先情報等が当該システムに保存されていた事実は確認されておらず、現時点でそれらの情報が外部の者に閲覧された事実や外部に流出した事実は確認されておりません。

2. 影響を受ける可能性のある情報

現時点で、影響を受けた可能性がある情報は、当社および当社のグループ会社のシステムにアクセスするために登録されている、役員、従業員（退職者を含みます。）等や委託先企業の従業員の一部の方の個人情報であり、以下の情報です。

- ログイン ID（社員番号を一部含む）
- 氏名
- 会社メールアドレス
- 役職
- 部門名

- システム ID

なお、パスワードについては、暗号化された形で管理されており、現時点において、不正アクセスによって当該パスワードを取得された事実は確認されていません。クレジットカード情報、銀行口座情報、マイナンバー等の機微な個人情報については、当該システム上に保存されていないことを確認しております。

3. 原因および調査状況

本事案の原因は、当社が利用している外部 VPN システムへの不正アクセスによるものであることが判明しております。現在、外部専門機関とも連携し、詳細な原因調査を継続いたします。

4. 現在までの対応

当社では、本事案を把握後、速やかに以下の対応を実施しました。

- 当該システムの利用停止およびセキュリティ設定の見直し
- 外部専門機関による技術的調査の実施
- 当社内・グループ会社内等の関係者への状況説明
- 関係機関への相談・報告および必要な対応の検討

5. 再発防止に向けた取り組み

当社は本事案を重く受け止め、調査結果を踏まえたうえで、以下の再発防止策を順次実施してまいります。

- VPN システムを含むシステム全体のセキュリティ対策および監視体制の強化
- 個人情報の取扱いおよび管理ルールの再点検
- 社内システム利用者に対する情報セキュリティ教育の継続的な実施

6. 今後の対応

今後、新たにお知らせすべき事実が判明した場合には、速やかに公表いたします。

現時点では、本件に起因する個人情報の不正利用等による二次被害は確認されておりませんが、今後、当社関係者になりすました不審メールや連絡等にはご注意いただけますようお願い申し上げます。

なお、上記のとおり漏えいした情報は、主として、当社および当社のグループ会社の従業員（退職者を含みます。）に関するものであることに鑑み、当社および当社のグループ会社の従業員には、既に社内システムに関するパスワードを念のため変更するよう通知済みでございます。

7. お問い合わせ窓口

本件に関する問い合わせ先： コーポレートコミュニケーション部
電話 050-3311-0617（広報）
https://www.alpsalpine.com/j/common/inquiry.html