2026 年 4 月 27 日
阿尔卑斯阿尔派株式会社

关于用于访问公司内部系统的个人信息遭到非法访问的说明

本次确认，本公司使用的外部 VPN 系统遭到受非法访问，无法排除个人信息已被外部攻击者浏览的可能性。对此，给相关各位及有关各方带来的忧虑与不安，本公司深表歉意。
有关此事件，本公司目前仍在持续调查中。现将已查明的情况，公告如下。
此外，除上述可能遭到非法访问的个人信息外，未发现本公司及集团公司客户信息、交易方信息等遭到非法访问，目前也未确认该等信息被外部人员浏览或泄露至外部。

1. 事件概要

2026 年 4 月 3 日，本公司所使用的外部 VPN 系统的受托方（负责本公司内部系统的维护管理等业务）通知我司，确认存在外部人员非法访问的痕迹。
4 月 13 日，根据受托方后续进行的调查，查明本公司的服务器也遭到了非法访问，因而无法完全排除以下可能：为访问公司内部系统而注册的人员的个人信息被外部浏览。
此外，已确认上述系统内未保存除上述内容以外的客户信息、交易方信息等，目前未发现这些信息被外部人员浏览或泄露到外部。

2. 可能受到影响的信息

目前，可能受到影响的信息是，为访问本公司及集团公司的系统而注册的董事、员工（含离职人员）以及部分受托方企业员工的个人信息，具体项目如下：

- 登录 ID（部分包含员工编号）
- 姓名
- 公司邮箱地址
- 职务
- 部门名称
- 系统 ID

另外，密码以加密形式管理，目前未确认因本次非法访问导致密码被获取的情况。信用卡信息、银行账户信息、个人专用号码等敏感个人信息，已确认未存储于该系统中。

3. 原因及调查情况

现已确认，此事件系本公司所使用的外部 VPN 系统遭到非法访问所引发。目前正在与外部专业机构合作，就详细原因持续开展调查。

4. 截至目前的主要应对措施

察觉本事件后，本公司立即实施了以下措施：

- 停用相关系统并调整安全设置
- 委托外部专业机构开展技术调查
- 向公司内部及集团内相关人员进行情况说明
- 向有关机构咨询、报告，并就必要应对措施进行研究

5. 防止再次发生的举措

本公司严肃看待本次事件，将根据调查结果，依次落实以下再发防止对策：

- 强化包括 VPN 系统在内的整体系统的安全对策及监控体制
- 重新审视个人信息处理及管理规范
- 持续对内部系统用户实施信息安全教育培训

6. 今后的应对

今后如发现需要另行告知的新情况，将迅速公布。

截至目前，尚未发现因本事件导致个人信息被非法使用等二次受害的情况，但各位如收到冒充本公司相关人员的可疑邮件或联络，请务必留意。

如前所述，本次可能泄露的信息主要涉及本公司及集团公司的员工（含离职人员），因此，我司已通知相关员工，为安全起见及时更改公司内部系统的密码。

7. 咨询窗口

本事件相关咨询方式：Corporate Communication 部

电话：+81-50-3613-1581（公关）

https://www.alpsalpine.com/e/common/inquiry.html