2023 年 8 月 1 日
株式会社エムプラス

過去に弊社に在職されていた皆様へ

このたび、弊社の委託先である RSM 汐留パートナーズ社会保険労務士法人が利用する「社労夢」（以下、「本件システム」といいます）のサーバーがランサムウェアによる第三者からの不正アクセスを受けたことが判明いたしました。
現時点で情報漏えいの事実は確認されておりませんが、個人情報の漏えいの可能性を考慮し、個人情報保護委員会に対する報告を行っております。過去に弊社に在職されていた皆さまにおかれましては、以下の内容をご確認くださいますようお願い申し上げます。

**1. 概要**

弊社は、給与計算・社会保険手続き等の業務を社外の専門家である RSM 汐留パートナーズ社会保険労務士法人に委託しており、当該社会保険労務士法人においては、委託業務遂行のために本件システムを利用しておりました。
このたび、本件システムを提供している株式会社エムケイシステムより、同社のサーバーがランサムウェアによる第三者からの不正アクセスを受けた旨が公表され、本件システムに保存されていた個人情報が漏えいしたおそれがある旨が判明しました。
なお、2023 年 7 月 19 日付の同社公表にて、外部専門機関による調査結果として、何らかのデータが攻撃者によって窃取された可能性は完全には否定できないものの、情報窃取及びデータの外部転送等に関する痕跡がない等、現時点において情報漏洩の事実は確認されておらず、また、マイナンバーについては高度な暗号化処理を施しており、今回の流出の恐れがある情報範囲には含まれていない旨報告されております。
株式会社エムケイシステム 2023 年 7 月 19 日発表
「当社サーバへの不正アクセスに関する調査結果のご報告（第 3 報）」

**2. 個人情報が漏えいしたおそれがある対象者**

(1) 現在在籍している従業員
(2) 過去在籍していた従業員のうち、2017 年 3 月以降に退社した、雇用保険又は社会保険に加入していた従業員

**3. 漏えいしたおそれのある個人情報の項目**

(1) 氏名（本人および扶養家族）
(2) 生年月日（本人および扶養家族）

(3) 住所
(4) 性別
(5) 電話番号
(6) 本人の給与及び賞与金額
(7) 口座情報

**4. 漏えいのおそれが生じた原因**

株式会社エムケイシステムのサーバーに対するランサムウェアによる第三者からの不正アクセス

**5. ご留意いただきたい事項**

現時点で、漏えいの事実や情報の悪用等による二次被害は確認されていませんが、漏えいしたおそれのある個人情報の項目の重要性から、念のため、不審な連絡や訪問者等にはご注意いただきますようお願いいたします。

**6. 今後の対応**

今回の事案について弊社としても重く受け止め、再発防止に向けて、委託先と連携の上、利用システムの見直し等、必要なセキュリティ対策を十分検討し進めてまいります。

**7. お問い合わせ先**

本件に関する弊社へのお問い合わせは以下までご連絡ください。

株式会社エムプラス　お問い合わせ窓口

privacy@kenkyuukai.jp