

2023年6月28日

2020年7月以降に当社を退職された皆様へ

社会保険業務で利用する外部システムへの不正アクセスに伴う個人情報漏えい懸念について

この度、星光ビル管理株式会社（以下「当社」）が社会保険業務で利用する外部システム【社労夢 Company Edition】（株式会社エムケイシステム(以下「M社」)社製の製品）がランサムウェア（身代金要求型コンピュータウイルス）に感染し、第三者からの不正なアクセスがあったことが判明しました。（6月5日システム停止、6月8日ランサムウェア感染が判明）

6月20日にM社から発表された「中間報告書」によれば、「個人情報が外部に送信された形跡について発見されていない」とのことではありますが、現時点でマイナンバーを含む個人情報の漏えいを完全に否定できる状況にはないため、引き続き不審な照会電話や郵便物等にご注意いただきますようお願い申し上げます。

1.概要

当社では、2020年10月より社会保険業務にてM社のクラウドサービスを利用開始しています。このサービスは、社会保険申請業務において、2700を超える社会保険労務士事務所、管理者数826万名と、極めて多くの顧客において利用されているサービスであり、当社でも社会保険関係の電子申請には必要不可欠のシステムであるとの判断から導入したものです。

M社の概況（ホームページより）

- 社労士事務所 2,754（2023年4月1日現在）
- 年間累計電子申請 366万件以上（2022年4月～2023年3月）
- 管理事務所 約57万事業所（2023年4月1日現在）
- 社労夢で管理する在籍者数 約826万名（2023年4月1日現在）

M社では6月5日にシステムサーバがランサムウェアに感染し、第三者から不正アクセスがあったことが確認されています。ただし6月20日に発表された「中間報告書」によれば、個人情報が外部に送信された形跡は発見されておらず、また二次被害について現時点では確認されていません。とりわけマイナンバーについては、M社製品とは切り離れた環境で完全に暗号化されており、流用や悪用ができない仕組みとなっています（M社ホームページより）。

しかしながら、M社のシステムに保存されている当社従業員の個人情報が漏えいしている可能性が完全に否定できる状況でないため、この段階で情報連携するものです。

2.情報漏えいが懸念される対象者

当所在籍者及び 2020 年 7 月以降の退職者（出向者含む。派遣社員含まず。）

3.情報漏えいが懸念される個人情報の項目

氏名、生年月日、住所、個人番号(マイナンバー)、性別、電話番号

4.二次被害、そのおそれの有無及びご留意いただきたい事項

現時点では、情報漏えいの事実や情報の悪用による二次被害は確認されていませんが、漏えいが懸念される個人情報項目の重要性等から、マイナンバーに関する不審な照会電話や郵便物、市役所等の職員を装った訪問等にはご注意ください。くれぐれも、安易にマイナンバーカードを渡したり、暗証番号を伝えたりすることがないようにしてください。

<デジタル庁 HP の Q&A より抜粋>

Q：日本のマイナンバー制度で、なりすまし被害が生じる恐れはありませんか。

A：マイナンバーの利用範囲を法律や条例で制限し、マイナンバーを利用する際の厳格な本人確認も義務付けています。万が一、マイナンバーが漏えいした場合でも、マイナンバーだけでは手続はできませんので、それだけでは悪用されません。

（参考）【株式会社エムケイシステム発表情報】

第三者によるランサムウェア感染被害への対応状況のお知らせ

HP：<https://www.mks.jp/company/topics/>

5.お問い合わせ

お問い合わせについては、極力メールにてお願いします。

■本件への対応全体について

星光ビル管理(株) リスク・コンプライアンス統括部 メール：0152compliance@saycogroup.co.jp

Tel: 06-6201-2859

■本件への該当有無確認や個人情報項目について

星光ビル管理(株) 財務・経理部 給与・社会保険 G メール：sayco.kyuyo@saycogroup.co.jp

Tel: 06-6201-3598

以 上