資料３－１

公 表 資 料

株式会社エムケイシステムに対する個人情報の保護に関する法律に基づく行政上の対応について

令和６年●月●日
個人情報保護委員会

個人情報保護委員会（以下「当委員会」という。）は、令和６年●月●日、株式会社エムケイシステム（以下「エムケイ社」という。）における個人情報等の取扱いについて、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「法」という。）第 147 条の規定による指導等を行った。

１．事案の概要

エムケイ社は、社会保険/人事労務業務支援システム（以下「本件システム」という。）を、社会保険労務士（以下「社労士」という。）の事務所等のユーザ（以下「ユーザ」という。）に対し、SaaS 環境[1]においてサービス提供していたところ、令和５年６月、エムケイ社のサーバが不正アクセスを受け、ランサムウェアにより、本件システム上で管理されていた個人データが暗号化され、漏えい等のおそれが発生した。

本件システムは、主に社労士向けの業務システムであり、社会保険申請、給与計算及び人事労務管理等の業務のために利用するものである。同システムで取り扱われていた個人データは、社労士の顧客である企業や事業所等（以下「クライアント」という。）の従業員等の氏名、生年月日、性別、住所、基礎年金番号、雇用保険被保険者番号及びマイナンバー等である。

エムケイ社の報告によれば、現時点において、個人データの悪用などの二次被害は確認されていない。

２．事案の規模

(1) エムケイ社からの情報による本件システムの利用実績

社労士事務所：2,754 事業所、管理事業所：約 57 万事業所　（令和５年４月１日時点）
本件システムで管理する本人数：最大約 2,242 万人　（令和５年６月 5 日時点）

(2) 当委員会が受領した漏えい等報告件数

令和５年６月６日から現在までに受領した漏えい等報告件数は、報告者ベースで 3,067 件（本人数計 7,496,080 人）である[2]。大部分は社労士事務所からの提出であり、顧問先事業者との連名報告の形での報告が多かった。内訳は、社労士事務所等が 2,459 件（本人数計 6,724,609 人）、顧問先事業者が 404 件（本人数計 392,125 人）、企業等が

[1] Software as a Service の略。一般的には、事業者がソフトウェアをクラウド上で稼働し、ユーザはインターネット経由でアクセスすることにより、当該ソフトウェアを利用できる仕組みとなっている。
[2] エムケイ社からの報告を除く。

204 件（本人数計 379,346 人）である[3]。

３．エムケイ社が本件において個人データを取り扱っていたこと

(1) ガイドラインＱ＆Ａ7-53 について

「個人情報の保護に関する法律についてのガイドライン」に関するＱ＆Ａ（以下「ガイドラインＱ＆Ａ」という。）7-53 には、「クラウドサービス提供事業者が、当該個人データを取り扱わないこととなっている場合とは、契約条項によって当該外部事業者がサーバに保存された個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合等」と記載されている。

(2) エムケイ社とユーザとの間の利用規約

本件システムの利用に当たり、エムケイ社は、ユーザに利用規約（以下「本件利用規約」という。）の同意を求めていた。

(3) エムケイ社における実際の個人データの取扱いの状況

- エムケイ社は、ユーザから本件システムの利用に関する調査・支援要請があった場合、両者の間で「個人情報授受確認書」（以下「授受確認書」という。）を取り交わした後、個人データを取り扱っていた。なお、令和５年上半期における、授受確認書によるエムケイ社の個人データ取扱い実績は、合計 20 件であった。
- 授受確認書には、「個人情報保護法を遵守し、下記目的達成の為に個人情報を授受します。」「媒体　お客様の委託データ」「授受の形態　保守用 ID によるデータ調査」などの記載がある。
- エムケイ社は、保守用 ID を有しており、これを用いて、本件システム上の個人データにアクセスすることが可能であった。

(4) 検討

ア　利用規約

本件利用規約においては、エムケイ社がサービスに関して保守運用上又は技術上必要であると判断した場合、ユーザがサービスにおいて提供、伝送するデータ等について、監視、分析、調査等、必要な行為を行うことができる旨が規定されていた。また、本件利用規約において、エムケイ社は、ユーザの顧問先に係るデータを、一定の場合を除き、ユーザの許可なく使用し、又は第三者に開示してはならないという旨が規定されており、エムケイ社は、当該利用規約に規定された特定の場合には、社労士等のユーザの顧問先に係る個人データを使用等できることとなっていた。

イ　アクセス制御

エムケイ社は、保守用 ID を有しており、それを利用して本件システム内の個人

[3] 漏えい等報告において、現時点で本人数不明として報告されているものを除く。また、本人数については社労士事務所等と顧問先事業者とで重複して報告している可能性がある。

データにアクセス可能な状態であり、エムケイ社の取扱いを防止するための技術的なアクセス制御等の措置は講じられていなかった。

ウ　エムケイ社がユーザに提供するサービスの性質

ソフトウェアをインターネット経由で利用できるタイプのクラウドサービスにおいては、様々なアプリケーションやソフトウェアの提供があり得るところ、本件システムは、ユーザである社労士事務所や企業等が社会保険及び雇用保険の申請手続や給与計算等をオールインワンで行うことができるというものである。すなわち、本件においてエムケイ社がクラウドサービス上で提供するアプリケーションは、ユーザである社労士事務所や企業等が、個人の氏名、生年月日、性別、住所及び電話番号などの個人データを記録して管理することが予定されているものであり、実際に大量の個人データが管理されていた。

エ　エムケイ社による個人データの取扱いの状況

本件では、エムケイ社が、ユーザと授受確認書を取り交わした上で、実際にユーザの個人データを取り扱っていた実績がある。

オ　小括

以上の事実関係を考慮すると、本件において、クラウドサービス提供事業者であるエムケイ社がガイドラインＱ＆Ａ7-53 の「個人データを取り扱わないこととなっている場合」とはいえず、また、個人データの取扱いを防止するための適切なアクセス制御は行われていなかったことが認められる。したがって、本件において、エムケイ社は、個人情報取扱事業者としてユーザから個人データの取扱いの委託[4]を受けて個人データを取り扱っていたといえる。

(5) 補足

ガイドラインＱ＆Ａ7-55 では、「単純なハードウェア・ソフトウェア保守サービスのみを行う場合で、契約条項によって当該保守サービス事業者が個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合等には、個人データの提供に該当」しないこととされている。ここでは、例として、「保守サービスの作業中に個人データが閲覧可能となる場合であっても、個人データの取得（閲覧するにとどまらず、これを記録・印刷等すること等をいう。）を防止するための措置が講じられている場合」等が挙げられており、「取扱いを防止するためのアクセス制御等の措置」が講じられているか否かが重要である。

本件において、エムケイ社が有する保守用 ID については、個人データの取得を防止するための技術的な措置は講じられていないことから、個人データの提供に該当し、委託に基づき個人データを取り扱っているものと認められる。

---

[4] 個人情報の保護に関する法律についてのガイドライン（通則編）3-4-4 において、「『個人データの取扱いの委託』とは、契約の形態・種類を問わず、個人情報取扱事業者が他の者に個人データの取扱いを行わせることをいう。具体的には、個人データの入力（本人からの取得を含む。）、編集、分析、出力等の処理を行うことを委託すること等が想定される。」ものとされている。

４．法律上の問題点

(1) エムケイ社について－安全管理措置（法第 23 条）の不備

法第 23 条において、「個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は毀損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない」と規定している。個人情報の保護に関する法律についてのガイドライン（通則編）（以下「ガイドライン」という。）「10（別添）講ずべき安全管理措置の内容」において、個人情報取扱事業者は、技術的安全管理措置として、「個人データを取り扱う情報システムを使用する従業者が正当なアクセス権を有する者であることを、識別した結果に基づき認証しなければならない。」（10-6(2)アクセス者の識別と認証）とされ、また、「個人データを取り扱う情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用しなければならない。」（10-6(3)外部からの不正アクセス等の防止）とされている。

しかしながら、エムケイ社においては、ユーザのパスワードルールが脆弱であったこと、また、管理者権限のパスワードも脆弱であり類推可能であったことから、アクセス者の識別と認証に問題があった。また、ソフトウェアのセキュリティ更新が適切に行われておらず、深刻な脆弱性が残存されていただけでなく、ログの保管、管理及び監視が適切に実施されておらず、不正アクセスを迅速に検知するには至らなかったことから、外部からの不正アクセス等の防止のための措置についても問題があった。

したがって、エムケイ社においては、技術的安全管理措置に不備が認められる。

(2) ユーザ（エムケイ社の委託元）について

本件では、エムケイ社の技術的安全管理措置の不備が原因となり、ランサムウェアの侵入を許し、個人データの漏えい等のおそれが生じた。したがって、本件漏えい等事態は、クラウドサービス事業者であるエムケイ社側の責任の範囲において生じた事態であり、ユーザには、法第 23 条が求める安全管理措置のうちエムケイ社のような技術的安全管理措置の不備は認められない。

他方、法第 25 条において、「個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない」と規定している。法第 25 条に関するガイドライン 3-4-4 では、委託元である個人情報取扱事業者は、取扱いを委託する個人データの内容を踏まえ、個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、委託する事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）等に起因するリスクに応じて、適切な委託先の選定、委託契約の締結及び委託先における個人データ取扱状況の把握について、必要かつ適切な措置を講じなければならないことが規定されている。

本件漏えい等事態発覚当時のエムケイ社のウェブサイトにおいては、本件サービスに関し、万全のデータセンターとセキュリティ管理をしている旨が記載され、また、漏

えい対策についても万全の体制である等と記載されていた。本件において、ユーザの多くは、エムケイ社に対する個人データの取扱いの委託を行っていたとの認識が薄く、委託先の監督が結果的に不十分となっていた可能性がある。

(3) クライアント（ユーザの委託元）について

本件システムのユーザである社労士事務所に対して個人データの取扱いを委託していたクライアントも、個人情報取扱事業者として従業者の個人データを取り扱っていたところ、自らも法第 23 条が求める安全管理措置を講ずる義務を負うとともに、委託先である社労士事務所に対し、法第 25 条が求める委託先の監督義務を負う。

しかしながら、本件において、クライアントの多くは、社労士事務所に対して個人データの取扱いの委託及びエムケイ社に対する再委託を行っていたとの認識が薄く、委託先等への監督が結果的に不十分となっていた可能性がある。

(4) 行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号。以下「番号法」という。）上の問題点について

本件システムにおいてはマイナンバーも取り扱われていたが、電子申請時等にマイナンバーを入力しても、原則的にマイナンバーは保管されない仕組みであった。また、ユーザが、オプションサービスを利用する場合にマイナンバーが管理されることがあったが、その場合は、高度な暗号化による秘匿化がされた状態で保管されていたものと認められた。

したがって、エムケイ社に対し、番号法の規定による指導は行わないこととする。

５．当委員会の対応

(1) エムケイ社

エムケイ社は、本件を機にデータセンターにおける本件システムの提供を停止し、よりセキュリティが強化されている環境で本件システムを再構築し、サービスを再開した。しかしながら、本件システムのユーザである社労士事務所や企業等から大量の個人データの取扱いの委託を受けていること及びエムケイ社の安全管理措置の不備が認められたことに鑑み、以下の対応を行う。

ア　法第 147 条の規定による指導

- 法第 23 条及びガイドラインに基づき、必要かつ適切な措置を講ずること。
- 再発防止策を確実に実施するとともに、爾後、適切に運用し、継続的に個人データの漏えい等の防止その他の個人データの安全管理のために必要かつ適切な措置を講ずること。

イ　法第 146 条第１項の規定による報告徴収

- 法第 146 条第１項の規定により、再発防止策の実施状況について、関係資料を提出の上、令和６年４月 26 日までに報告するよう求める。

(2) ユーザ及びクライアントについて

本件において、ユーザは、クライアントの従業員等の多数の個人データを取り扱っているところ、前述のとおり、ユーザ及びクライアントにおいて本件が個人データの取扱いの委託又は再委託を行っているとの認識が薄く、委託先等の監督が結果的に不十分となっていた可能性がある。

ユーザ及びクライアントの安全管理措置並びにエムケイ社に対する監督の実施状況は、個々のユーザ及びクライアントによって異なり得るため、実際にエムケイ社による個人データの取扱いがあったユーザ及びクライアントを中心に今後も継続して調査し、権限行使を含めた必要な対応を検討する。

(3) 注意喚起

今回、各事業者において、クラウドサービスの利用が委託等に該当する場合があることの理解が不足していたと考えられることから、クラウドサービスを利用して個人データを取り扱う場合及び個人データの取扱いの委託先がクラウドサービスを利用している場合に関し、①クラウドサービスの利用が、法第 27 条第 5 項第 1 号に規定される「個人データの取扱いの全部又は一部を委託することに伴って当該個人データが提供される場合」に該当する場合があること及び②①に該当する場合には、委託元は委託先に対する監督義務があることについて、注意喚起を実施することとする。

以　上