

クラウドサービス利用者による委託先の監督について

第 1 これまでの経緯

- 1 株式会社エムケイシステム（以下「エムケイ社」という。）が提供する社会保険・人事労務業務支援システム（以下「本件システム」という。）が、令和 5 年 6 月、ランサムウェア攻撃を受け、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。本件では、多くの社会保険労務士事務所や企業等（以下「委託元事業者等」という。）が、本件システムを利用することにより、個人データの取扱いをエムケイ社に委託していた。
- 2 個人情報保護委員会（以下「当委員会」という。）は、令和 6 年 3 月 25 日、エムケイ社に対し、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を行い、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報告を求めた。当委員会は、令和 6 年 7 月 17 日、エムケイ社から報告のあった技術的安全管理措置（アクセス者の識別と認証及び外部からの不正アクセス等の防止）に関する再発防止策の実施状況について、当委員会の指導事項を踏まえた一定の取組が認められたとの結論に至った。
- 3 他方、委託元事業者等におけるエムケイ社に対する監督状況については、調査を実施の上、権限行使を含めた必要な対応を検討することとなっていたため、ランサムウェア攻撃の直前 6 か月に当たる令和 5 年上半期に期間を限定し、実際にエムケイ社に個人情報授受確認書（以下「確認書」という。）を根拠に直接個人データを取り扱わせていた個人情報取扱事業者を選定の上、調査を実施した。

第 2 委託元事業者等への調査について

1 調査対象の委託元事業者等及び調査項目について

令和 5 年上半期に、確認書を根拠にエムケイ社に直接個人データを取り扱わせていた個人情報取扱事業者 3 事業者に対し、以下の事項等に関する調査を実施した。

- ① 本件により漏えいのおそれが生じた本人数
- ② 本件システムを選定した理由・基準
- ③ 本件システムの利用がエムケイ社への個人データの取扱いの委託に該当するとの認識の有無及びその理由
- ④ エムケイ社への監督の実施状況
- ⑤ 確認書を根拠とした個人データの調査等が個人データの取扱いの委託に該当するとの認識の有無（有の場合：エムケイ社に対する監督状況、無の場合：そのような認識を持った理由）

2 回答内容

(1) A 事業者

- ① 漏えいのおそれが生じた本人数
約 1,400 人
 - ② 選定した理由・基準
特に基準は設定しておらず、専ら、機能性、操作性、サポート体制、価格を重視して選定した。セキュリティ対策も選定基準であったが、エムケイ社のパンフレットの記載内容を信用するしかなく、ユーザー側で裏付けをとることもできないので、パンフレット記載内容を信用した。
 - ③ 委託の認識の有無
有。本件システムがクラウドに移行する以前は、委託との認識はなかったが、クラウド移行後は個人情報の取扱いを委託しているとの認識を持った。
 - ④ エムケイ社に対する監督
個人情報の漏えいに注意するよう、エムケイ社の営業やシステム担当者に、3 か月ごとに口頭で注意を発していた。
 - ⑤ 確認書を根拠とする調査が委託であるとの認識の有無及び監督状況
有。エムケイ社の担当者による作業に当たり、作業の進め方の報告を求めた。
- (2) B事業者
- ① 漏えいのおそれが生じた本人数
約 12,000 人
 - ② 選定した理由・基準
社会保険・雇用保険 API¹に対応したサービスを検討していたなかで、本件システムは労災給付 API にも対応しており、多機能であった。当社の情報セキュリティ対策基準においても問題がなかった。
 - ③ 委託の認識の有無
無。エムケイ社による個人データの取扱いは生じないと認識していた。
 - ④ エムケイ社に対する監督
契約時及びシステム構成変更時にセキュリティ対策の確認を実施していた。
 - ⑤ 確認書を根拠とする調査が委託であるとの認識の有無及び監督状況
無。エムケイ社に依頼した作業は、ログの調査であり、個人データ自体の調査ではなかったため。
- (3) C事業者
- ① 漏えいのおそれが生じた本人数
約 72,000 人
 - ② 選定した理由・基準

¹ API(Application Programming Interface)とは、情報システムが提供するデータや機能を外部のソフトウェアから呼び出して利用するための手順やデータ形式などを定めた規約のことである。本文脈では、社会保険や人事労務に関する行政手続きにおいて、本件システムが e-Gov 電子申請用の API に対応しているということを意味している。一般的に、e-Gov 電子申請の API 対応のシステムを利用することにより、事業者にとって申請や届出業務の効率的・簡素化が可能となる。

利用開始時に、当社のセキュリティ基準に基づくチェックリストで、エムケイ社の組織的セキュリティ対策状況及び本件システムの技術的セキュリティ対策状況をチェックし、当社のセキュリティ基準を充足していることを確認した。これらと同様のチェック及び確認は、本件システムの新機能追加時にも実施している。

③ 委託の認識の有無

無。通常の業務フローにおいて、エムケイ社が当社の個人データを取り扱う運用がなされていなかったことから、個人データの取扱いの委託に該当するとの認識はなかった。

④ エムケイ社に対する監督

個人データの取扱いの委託との認識はなかったが、本件システムに個人データを格納していることを認識していたため、安全管理措置としてセキュリティチェック等を実施していた。また、令和4年5月に「個人情報の漏えい等発生時の対応に関する確認書」を締結していた。

⑤ 確認書を根拠とする調査が委託であるとの認識の有無及び監督状況

無。依頼した作業は、個人データの取扱いの委託ではなく、障害対応と認識していた。本件作業に特化した形式での監督はしていなかったが、前述のとおり、当社セキュリティ基準に基づくセキュリティチェックは実施していた。

第3 当委員会の対応（案）

委託元事業者等においては、「エムケイ社への個人データの取扱いの委託」との認識の有無にかかわらず、2事業者にあつては、利用開始時及びシステム変更時にセキュリティ対策に関するチェックが行われており、1事業者にあつては、口頭ベースでエムケイ社の担当者に対しセキュリティ対策に関する注意喚起が頻繁に実施されていた。委託元事業者等の規模に応じて監督の実施方法や範囲に差異はあるものの、委託元事業者等はエムケイ社に対し、セキュリティ対策のチェックや注意喚起による一定程度の監督を実施していたものと認められるため、指導等の権限は行使しない。

しかし、委託元事業者等において、本件システムの利用が個人データの取扱いの委託に該当するにもかかわらず、委託の認識がなかったあるいは認識が薄かった現状が明らかになった。クラウドサービスを利用する場合には、個人データの取扱いの委託に該当するか否かを十分に調査・検討の上、委託に該当する場合には、個人データの安全管理のため、委託先に対し、セキュリティ対策を含めた安全管理措置の状況について定期的に報告を求めるなど、委託先であるクラウドサービス提供事業者に対する必要かつ適切な監督を行うことが重要であり、当委員会が令和6年3月25日に発した「クラウドサービス提供事業者が個人情報保護法上の個人情報取扱事業者に該当する場合の留意点について」の内容を改めて注意喚起したい。

以 上