株式会社エムケイシステムにおける再発防止策の実施状況及び今後の対応について

資料２
公表資料

- 株式会社エムケイシステム（以下「エムケイ社」という。）が社会保険労務士事務所等を対象に提供する社会保険／人事労務業務支援システム（以下「本件システム」という。）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事案について、個人情報保護委員会（以下「当委員会」という。）はエムケイ社に対し、令和６年３月25日、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条の規定により指導を行い、同法第146条第１項の規定により再発防止策の実施状況を報告するよう求めていた。
- エムケイ社から報告のあった再発防止策の実施状況に関して確認したところ、現時点にお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。当委員会としては、エムケイ社が再発防止策を確実に実施すること等を引き続き注視していく。
- 一方、ユーザ等のエムケイ社に対する監督の実施状況等については調査中であり、今後、権限行使を含めた必要な対応を検討する。エムケイ社においては、本件システムにおける個人データの取扱いを継続するか否かを検討中であるとのことであり、かかる検討結果についても引き続き注視していく。

指導の原因となる事実	指導の内容	策定した再発防止策の実施状況
【アクセス者の識別と認証】 エムケイ社においては、本件システムのユーザのパスワードルールが脆弱であり、また、管理者権限のパスワードも脆弱であり類推可能なものであった。	1. 法第23条及び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）に基づき、必要かつ適切な措置を講ずること。 2. エムケイ社において策定された再発防止策を確実に実施すること。	① 令和５年６月、パスワードポリシーを強化した。 ② 令和５年６～７月、全ユーザが新ルールに基づくパスワードを設定した。 ③ 令和５年６月、不要アカウントの削除を実施し、削除ルールを整備した。 • 社内の未使用アカウントを削除した。 • 契約解除したユーザ及びトライアル利用期間が終了したユーザについては、解約及び終了の翌営業日にアカウントを削除する運用に変更した。 ④ 令和６年２月、デバイス認証を導入した。 • ID及びパスワード認証に加え、電子証明書導入済のデバイスからのみ本件システムの利用を許可するデバイス認証を導入した。
【外部からの不正アクセス等の防止】 エムケイ社においては、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していただけでなく、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できなかった。		セキュアなプラットフォーム上で本件システムを再構築の上、以下を実施した。 ① 安全な環境における長期のログ保管 • 令和５年６月、ログの発生源と保管先を分離し、安全な環境で１年間以上のログが保管できるようにした。 ② ペネトレーションテストの定期的実施 • 令和５年６月以降、外部機関により年２回実施する。直近では令和６年５月に実施。 ③ 令和５年７月、ふるまい検知EDR(※1)の導入と外部のSOC(※2)による常時監視を開始した。 ④ ソフトウェアの更新・管理の徹底 • 令和５年７月、パッチ適用ツールの利用により、漏れなく迅速にソフトウェアを更新する仕組みを導入し、適用結果を日次で確認している。 ⑤ WAF(※3)ルールの最適化ツールの導入 • 令和５年８月、ビッグデータとAIを活用した最適なWAFルールを自動適用するツールを導入した。 ⑥ その他 • 令和５年７月、セキュリティ専門会社とアドバイザリー契約を締結。 • 令和６年４月、社内のセキュリティ啓発活動の強化と拡充。

※1 EDR(Endpoint Detection and Response:PC等のエンドポイントの不審な挙動を検知・防御する仕組み)
※2 SOC(Security Operation Center:セキュリティ・サービス及び監視を提供する組織)
※3 WAF(Web Application Firewall:Webサイトへのアクセス内容を監視し、攻撃パターンを検知・遮断する仕組み)