

6問 サイバー攻撃に加え、日本では災害リスクも考慮した裁判情報のデータの保管が必要と考えるが、裁判情報の保管の在り方について、法務当局に問う。

- (委員御指摘のとおり、) 指定法人のデータベースが安定的に提供されるためには、サイバー攻撃や災害リスク等も考慮した上で、指定法人において民事裁判情報等を適切に保管する必要がある。
- 本法律案においては、指定法人の保有する民事裁判情報等に関する漏えい、滅失又は毀損の防止その他の安全管理に関する事項を業務規程の必要的記載事項としており、所要の提出書類等により、漏えい、滅失等のリスクへの適切な対策が講じられているかについて、そのデータの保管の在り方も含め、審査することを想定している。
- 具体的なデータの保管先や保管方法等については、必要となるシステムの内容や要する費用等を勘案してまずは指定法人において検討されるべきものではあるが、法務省としても、指定法人において十分な安全管理措置が講じられるように業務規程の認可を適切に行うとともに、各種監督権限の行使を通じて、指定法人における民事裁判情報の適正な保管・管理が徹底されるよう努めてまいりたい。

(参考1) 保有民事裁判情報等の管理(本法律案第6条第1項第3号)

指定法人が仮名加工民事裁判情報等の提供を適切に行うためには、当該情報を提供に適した状態に保つとともに、訴訟関係者の権利利益に配慮して本制度に対する国民の信頼を確保することが必要である。そのために指定法人が行うべき情報の管理としては、仮名加工民事裁判情報に

ついて電子判決書等の内容と齟齬がないように正確性を保つこと、訴訟関係者等の苦情の申出に応じて適切な処理を行って提供に適した状態に保つこと、保有民事裁判情報等の漏えい、滅失、又は毀損の防止その他の安全管理を講ずることが必要になる。

(参考2) 安全管理に関する事項 (民事判決情報データベース化検討会報告書抜粋 (第5・4(3)イ [36ページ]))

本検討会においては…民事裁判情報が「個人データ」に該当するか否かにかかわらず、情報管理機関には、国民の信頼に足りるだけの安全管理措置を講ずることが求められるとの意見があり、このような観点からは、民事裁判情報の漏えい、滅失又は毀損の防止その他の民事裁判情報の安全管理のために必要な安全管理措置として、①業務マニュアルの整備等の組織的安全管理措置、②従業者に対する教育等の人的安全管理措置、③端末の盗難防止等の物理的安全管理措置及び④情報セキュリティ対策等の技術的安全管理措置を講じる必要があるほか、民事裁判情報の漏えい、滅失、毀損等が発生した場合は、監督官庁に報告する必要があると考えられる。

(参考3) 可用性に関する指摘 (民事判決情報データベース化検討会第13回会議 [令和5年12月22日実施] 議事録抜粋)

結論的にはこのような原案について特に結論に異を唱えるものではないのですが、ただ若干書きぶりが気になるところがございまして、このサービス全体の趣旨に鑑みると、もちろん漏えいの防止とか、あるいは仮名加工前の情報が外に漏れてはいけないということはもちろん重要ではあるのですが、このサービスの趣旨を考えると、安定的に利用者の方が利用できるようにすると、いわゆる可用性も非常に大きな要素だと思うのです。したがって、34頁だけではなくてもう少しその前の32頁・33頁辺りの安全管理措置のところの記述ぶりも含めて、漏えいの防止とかそちらだけではなくて、サービスの安定的な提供、可用性ということについても業務委託先にも監督する必要があるし、また、情報管理機関自らもその管理措置を講じる必要があるという、少し書きぶりについて御配慮いただけると有り難いと思います。以上でございます。

(参照条文)

○ 民事裁判情報の活用の促進に関する法律案

(業務規程)

第八条 指定法人は、基本方針に従って、民事裁判情報管理提供業務に関する規程（以下この条及び第十八条第一項第四号において「業務規程」という。）を定め、法務大臣の認可を受けなければならない。これを変更しようとするときも、同様とする。

2 業務規程には、次に掲げる事項を定めておかなければならない。

一・二 (略)

三 保有民事裁判情報等の漏えい、滅失又は毀損の防止その他の保有民事裁判情報等の安全管理に関する事項

四・五 (略)

六 前各号に掲げるもののほか、民事裁判情報管理提供業務の実施に必要な事項として法務省令で定める事項

3 (略)