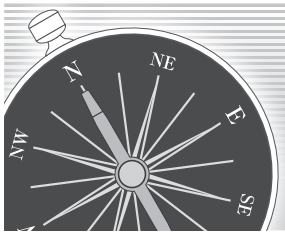

リーガル コンパス

LEGAL COMPASS

弁護士法人神戸シティ法律事務所
弁護士　中馬　康貴
（兵庫県弁護士会所属）

第131回　再委託先に対する「定期的な監査」とは

1　「定期的な監査」とは？

前回（第130回）において、個人情報取扱事業者は、再委託先に対して「委託先を通じて又は必要に応じて自らが、定期的に監査を実施すること等により、委託先が再委託先に対して委託先の監督を適切に果たすこと」が必要であると述べましたが、具体的にどのような手段を講じるべきでしょうか。本稿では、再委託先に対し、「定期的な監査」として講ずべき手段について検討します。

2　前提

「定期的な監査」の内容として、ガイドライン（通則編）では、「取扱いを委託する個人データの内容や規模に応じて適切な方法をとる必要があるが、例えば、必要に応じて個人データを取り扱う場所に赴く又はこれに代わる合理的な方法（口頭による確認を含む）により確認することが考えられる」と言及するにとどまり、「委託先に対して再委託に関する報告を求めるなどの必要な措置を行わない」場合が、委託を受けた者に対して必要かつ適切な監督を行っていない事例として挙げられています。

3　何をどのようにすればよいか

（1）総論

個人情報の取扱い状況を確認する方法について、ガイドラインでは「必要に応じて個人データを取り扱う場所に赴く」とあるものの、現実には現地調査をすることが難しい場合が少なくありません。そこで、委託先から、あるいは再委託先から直接、個人情報の取扱い状況に関する報告書を定期的に（半年ないし1年に1回程度が目安）提出させることが現実的です。

（2）確認内容

委託先を通じて（あるいは再委託先から直接）確認すべき事項は、以下とおりです。

①再委託の有無

前提として、委託元が再委託はされていないと認識している場合は、「再委託をしていない」ことを、委託先から定期的に確認しておくことが必要です。また、再委託をしている場合であっても、委託元が把握している再委託先以外への再委託を実施していないかどうかも定期的に確認しておくべきです。

②再委託先における安全管理措置の状況

再委託がなされている場合には、再委託先における個人情報の取扱い状況、すなわち安全管理措置の実施状況を確認する必要があります。再委託先において講じる安全管理措置は一様ではありませんが、具体的には以下のとおりです。

ア　基本方針・取扱規程等の策定の有無
イ　組織的安全管理措置の内容（組織体制の整備の内容、取扱状況を確認する手段の整備内容、情報漏えい等事案に対応する体制の内容等）
ウ　人的安全管理措置の内容（事務取扱担当者の監督及び教育）
エ　物理的安全管理措置の内容（個人情報等を取り扱う区域の管理、機器及び電子媒体等の盗難等の防止、電子媒体等の取扱いにおける漏えい等の防止措置等）
オ　技術的安全管理措置の内容（アクセス制御措置の実施の有無、アクセス者の識別・認証の実施の有無、不正アクセスや情報漏えいの防止措置の有無）

③再々委託の有無

そして、再委託先が再々委託をしていないかどうかも確認しておくことによって、個人情報を取り扱う事業者の終着点を把握しておくことが重要です。

（3）確認方法

確認方法については、再委託先で講じている安全管理措置について、個別の対応状況を○×形式で回答させ、×である場合はその理由や今後の対応予定を記載させる（あるいは聴取を行う）ことが考えられます。

しかし、この方法は簡便である一方、再委託先において実態を確認しないまま、あるいは管理内容に変更があったにもかかわらずその内容を報告しないまま、単に「○」とだけ記載して回答してくるデメリットが残ります。それを委託元が黙認して放置してしまうと、杜撰な管理を容認することになり、漏えい事故のリスクも高まります。そこで、少なくとも、初回や、数年に1回のタイミングで、○×形式ではなく委託先に対して具体的な実施内容を記載させる等、○×方式以外の方法を併用する必要があります。