2－2－3－4．委託先の監督（法第22条関連）

法第22条

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。

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、法第20条に基づく安全管理措置を遵守させるよう、委託を受けた者に対し必要かつ適切な監督をしなければならない（2－1－4．「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。その際、委託する業務内容に対して必要のない個人データを提供しないようにすることは当然のこととして、取扱いを委託する個人データの内容を踏まえ、本人の個人データが漏えい、滅失又はき損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、事業の性質及び個人データの取扱状況等に起因するリスクに応じた、必要かつ適切な措置を講じるものとする。

「必要かつ適切な監督」には、委託先を適切に選定すること、委託先に法第20条に基づく安全管理措置を遵守させるために必要な契約を締結すること、委託先における委託された個人データの取扱状況を把握することが含まれる。

①委託先の選定

委託先を適切に選定するためには、委託先において実施される個人データの安全管理措置が、委託する当該業務内容に応じて、少なくとも法第20条で求められる安全管理措置と同等であることを、合理的に確認することが望ましい。また、委託先の評価は適宜実施することが望ましい。

②委託契約の締結

委託契約には、当該個人データの取扱いに関する、必要かつ適切な安全管理措置として、委託元、委託先双方が同意した内容とともに、委託先における委託された個人データの取扱状況を合理的に把握することを盛り込むことが望ましい。

なお、本人からの損害賠償請求に係る責務を、安全管理措置に係る責任分担を無視して一方的に委託先に課すなど、優越的地位にある者が委託元の場合、委託先に不当な負担を課すことがあってはならない。

③委託先における個人データ取扱状況の把握

委託先における委託された個人データの取扱状況を把握するためには、委託契約で盛り込んだ内容の実施の程度を相互に確認することが望ましい。

委託元が委託先について「必要かつ適切な監督」を行っていない場合で、委託先が再委託をした際に、再委託先が適切といえない取扱いを行ったことにより、何らかの問題が生じたときは、元の委託元がその責めを負うことがあり得るので、再委託する場合は注意を要する。

なお、漏えいした場合に二次被害が発生する可能性が高い個人データ（例えば、クレジットカード情報（カード番号、有効期限等）を含む個人データ等）の取扱いを委託する場合は、より高い水準において「必要かつ適切な監督」を行うことが望ましい。

また、消費者等、本人の権利利益保護の観点から、事業内容の特性、規模及び実態に応じ、委託の有無、委託する事務の内容を明らかにする等、委託処理の透明化を進めることが望ましい。

【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場合】

事例1）個人データの安全管理措置の状況を契約締結時及びそれ以後も適宜把握せず外部の事業者に委託した場合で、委託先が個人データを漏えいした場合

事例2）個人データの取扱いに関して定めた安全管理措置の内容を委託先に指示せず、結果、委託先が個人データを漏えいした場合

事例3）再委託の条件に関する指示を委託先に行わず、かつ委託先の個人データの取扱状況の確認を怠り、委託先が個人データの処理を再委託し、結果、再委託先が個人データを漏えいした場合

事例4）契約の中に、委託元は委託先による再委託の実施状況を把握することが盛り込まれているにもかかわらず、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かった結果、委託元の認知しない再委託が行われ、その再委託先が個人データを漏えいした場合

【個人データの取扱いを委託する場合に契約に盛り込むことが望まれる事項】

・委託元及び委託先の責任の明確化
・個人データの安全管理に関する事項
　・個人データの漏えい防止、盗用禁止に関する事項
　・委託契約範囲外の加工、利用の禁止
　・委託契約範囲外の複写、複製の禁止
　・委託契約期間
　・委託契約終了後の個人データの返還・消去・廃棄に関する事項
・再委託に関する事項
　・再委託を行うに当たっての委託元への文書による報告
・個人データの取扱状況に関する委託元への報告の内容及び頻度
・契約内容が遵守されていることの確認（例えば、情報セキュリティ監査なども含まれる。）
・契約内容が遵守されなかった場合の措置
・セキュリティ事件・事故が発生した場合の報告・連絡に関する事項

2－2－4．第三者への提供（法第23条関連）

⑴原則（法第23条第1項関連）

法第23条第1項

個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。

1　法令に基づく場合

2　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

3　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって本人の同意を得ることが困難であるとき。

4　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

個人情報取扱事業者は、あらかじめ※1、本人の同意を得※2ないで、個人データを第三者に提供してはならない（2－1－4．「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。同意の取得に当たっては、事業の性質及び個人情報の取扱状況に応じ、本人が同意に係る判断を行うために必要と考えられる合理的かつ適切な範囲の内容を明確に示すこと。

※1「あらかじめ」とは、「個人データの第三者への提供に当たりあらかじめ」をいう。

※2「本人の同意を得（る）」については、2－1－10．参照。