連載

使いこなして何ぼ!!のISO

…ＩＳＯコンサルティングの現場から…

第44回「役に立つPマークのポイントご紹介します」の3回目

㈱ソフィア　平松　徹

前回は、経済産業省のガイドラインの中の4つの安全管理措置についてご紹介しました。今回はさらに「従業者の監督」と「委託先の監督」についてご紹介します。

1. 従業者の監督

「従業者の監督」は組織的安全管理措置、人的安全措置に関連します。この二つの安全管理措置を実効あるものにするための要求事項です。決めたことをきちんと実行してもらうべく従業者の監督をしなければいけないということ。ガイドラインに次のようにあります。

> 個人情報取扱事業者は、法第20条に基づく安全管理措置を遵守させるよう、従業者に対し必要かつ適切な監督をしなければならない。
> その際、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、必要かつ適切な措置を講じるものとする。

ガイドラインには従業者への監督ができていない場合の例示が記載されています。

> **従業者に対して必要かつ適切な監督を行っていない事例**
> ・安全管理の規程等に従って業務を行っていることを定期的に確認しない結果、個人データが漏えいした場合。
> ・内部規程等に違反して個人データが入ったノート型パソコン、メモリーなどを繰り返し持ち出していたにもかかわらず、その行為を放置した結果、紛失し、個人データが漏えいした場合。

なお従業者とはガイドラインでは次のようになっています。

> 「従業者」とは、個人情報取扱事業者の組織内にあって直接間接に事業者の指揮監督を受けて事業者の業務に従事している者をいい、雇用関係にある従業員（正社員、契約社員、嘱託社員、パート社員、アルバイト社員等）のみならず、取締役、執行役、理事、監査役、監事、派遣社員等も含まれる。

教育訓練などについて審査されるときは、従業者全員について漏れなく実施されているかどうかが問われます。アルバイトでも業務に携われば個人情報を漏らしてはいけません。アルバイトについてもきちんと監督するということ、改めて確認しておく必要があります。

2. 委託先の監督

次に委託先の監督です。個人情報を委託先に預けて業務を実施してもらうときに必要になります。個人情報が委託先から漏れることが多い。だからここは重要です。ガイドラインに次のようにあります。

> 個人データの取扱いの全部又は一部を委託する場合、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。
> 「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。
> 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、少なくとも安全管理措置と同等

表1 「雇用に管理に関する個人情報の適正な取り扱いを確保するために事業者が講ずべき措置に関する指針について」(厚生労働省ガイドライン)

	項目	内容
1	利用目的の特定について	労働者が合理的に想定できるように、具体的、個別的に利用目的を特定する。
2	本人の同意について	労働者本人に通知などしたうえで、本人が口頭や書面などで承諾する意思表示を行うことが望ましい。
3	従業者の監督などについて	①扱う者の権限を明確にする。 ②権限を与えられた者のみが業務を実施する。 ③みだりに第三者に知らせたり、不当な目的に使用しない。 ④管理責任者を選任する。 ⑤必要な教育及び研修を行う。
4	委託先の監督について	1) 委託先選定のための基準を設ける。 2) 講ずべき措置は・・・ ①個人情報を漏らさない、盗用しない。 ②再委託するときは委託元へ文書で報告する。 ③委託契約期間を明記する。 ④利用後の破棄、削除を適切、確実にする。 ⑤改ざんなどを禁止、又は制限する。
5	第三者提供で留意すること	①提供先で、個人情報を漏らしたり、盗用しない。 ②再提供するときはあらかじめ文書を持って事業者の了承を得る。 ③提供先での保管期間を明確にする。 ④利用後の破棄もしくは削除を適切、確実にする。 ⑤複製などを禁止する。
6	保有個人データの開示について	開示することで業務の実施に著しい支障を及ぼす恐れがある保有個人データについて開示に関する事項を定め、労働者に周知する。
7	個人データについての閲覧の場所、時間について	個人データの閲覧など円滑に行われるように十分に留意する。
8	苦情処理について	苦情、相談を受け付けるための窓口を明確にするなど、必要な体制整備に努める
9	その他配慮事項	①個人情報の取り扱いに関する重要事項を定めるときはあらかじめ労働組合などに通知し、必要に応じ協議する。 ②重要事項を定めたら、労働者等に周知する。

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。

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。

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。

また、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。

委託を受けたものに対して必要かつ適切に監督を行っていない事例として次のようにガイドラインにあります。

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

①安全管理措置の状況を契約締結時、それ以後も適宜把握せず、委託先が個人データを漏えいした場合。

②安全管理措置の内容を委託先に指示しなかった結果、委託先が個人データを漏えいした場合。

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た結果、再委託先が個人データを漏えいした場合

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。

以上が、経済産業省のガイドラインではポイントになる、「安全管理措置」「従業者の監督」「委託先の監督」です。

3. 厚生労働省のガイドラインも重要

厚生労働省のガイドラインも重要です。人事情報に個人情報はふんだんに含まれています。ポイントをまとめましたので参考にしてください(表1)。

4. 労働者の健康情報の取り扱いについての留意事項としてのガイドラインもある

また厚生労働省は、特に労働者の健康情報の取り扱いについて留意事項として次のようにも定めています。労働安全衛生法で会社に義務付けられている健康診断などでは社員の健康情報について嫌でも会社は取り扱わねばなりません。

「雇用管理に関する個人情報にうち健康情報を取り扱うに当たっての留意事項」(厚生労働省ガイドライン)

①労働者から提出された診断書の内容以外に医療機関から健康情報を収集する必要があるときは、労働者に承諾を得る。ただできれば、これらの情報は労働

者本人から提出を受けることが望ましい。
②健康保険組合などに対して労働者の健康情報の提供を求めるときは、労働者の承諾を得る。ただ、できればこれらの情報は労働者本人から提出を受けることが望ましい。
③「利用目的」「安全管理体制」「健康情報を取り扱う者の権限、取り扱う範囲」「開示、訂正、追加、削除の方法」「苦情処理」については規定などで定め、労働者に通知する。また、それを規定などにする際には、労働組合等にも通知し、必要に応じて協議を行うことが望ましい。

表2 「個人情報に関する基本方針」(消費者庁ガイドライン)

	項目	内容
1	行う措置を対外的に明確にする	①考え方や方針を策定公表する。 ②利用目的の通知・公表、開示等の諸手続きについてあらかじめ対外的にわかりやすく説明などする。
2	消費者等の権利利益の一層の保護	①保有個人データについて本人からの求めがあったときはDMの発送停止など自主的に利用停止等に応じる。 ② 委託処理の透明化を進める。 ③本人にとって利用目的が明確になるようにする。 ④個人情報の取得元、取得方法を具体的に明記する。 ⑤漏洩などしたときは、可能な限り事実関係を公表する。
3	責任体制の確保	①外部からの不正アクセスの防御対策、管理者の設置、内部関係者のアクセス管理、持ち出し防止策などの安全管理の責任体制確保のための仕組みを整備する。 ②委託元、委託先のそれぞれの責任等を明確に定めることにより、再委託の場合も含め実効的な監督体制を確保する。
4	従業者の啓発	教育研修などを通じて従業者の個人情報保護意識を徹底する。
5	安全管理措置	本人が被る権利利益の侵害の大きさを考慮し、事業の性質などに起因するリスクに応じ、必要かつ適切な措置を講じる。
6	苦情処理の制度	苦情受付窓口の設置、苦情処理手順の策定等を実施する。

5. 特定の機微な個人情報

JISQ15001では、健康情報の取り扱いについては「特定の機微な個人情報」のひとつとして次のように規定されています。

3.4.2.3 特定の機微な個人情報の取得、利用及び提供の制限
事業者は、次に示す内容を含む個人情報の取得、利用又は提供は、行ってはならない。
ただし、これらの取得、利用又は提供について、明示的な本人の同意がある場合及び3.4.2.6のただし書きA)～D)のいずれかに該当する場合は、この限りではない。
A)思想、信条又は宗教に関する事項
B)人種、民族、門地、本籍地(所在都道府県に関する情報を除く。)、身体・精神障害、犯罪歴その他社会的差別の原因となる事項
C)勤労者の団結権、団体交渉その他団体行動の行為に関する事項
D)集団示威行為への参加、請願権の行使その他の政治的権利の行使に関する事項
E)保健医療又は性生活に関する事項

E)項が健康情報についての規定です。「保健医療」に関する個人情報は、原則取得してはいけないとまず禁止をしておいて、ただし、法令に基づく場合はOKとの但し書きで会社として取り扱いができることになります。

この「特定の機微な個人情報」の部分は、Pマークと個人情報保護法の違いということで、しっかりと確認しておく必要があります。機微情報についての規定は個人情報保護法ではありません。Pマークではしっかりと規定されています。

これは例えば採用などでは、思想や信条など原則として聞いてはいけないということです。といっても現実にはどのような考えを持っているというのは採用情報としては、採用の有無を決める重要な判断基準のひとつになるものです。だから、聞かざるをえません。ここでは、本人が嫌がることを聞かないということで、しつこく聞いたりしなければ問題ないと判断すべきです。常識の範囲内という考え方が重要です。

6. 消費者庁のガイドライン

最後にもともと内閣府が出している指針を取り上げます(表2)。

以上が行政の出している代表的なガイドラインです。この3つくらいはPマークを取得する会社であれば、何らかの意味で関連してきますので、「法令、国が定める指針その他の規範」として特定し、いつでも参照できる手順にしておく必要があります。

この3つのガイドライン一様に読みにくいのが難点です。といって、守らなくて良いわけではありません。参考にしていただければと思います。

I

筆 者
平松 徹(ひらまつ とおる)
(株)ソフィア 代表取締役
JRCA ISO9001主任審査員
CEAR ISO14001主任審査員
社会保険労務士、中小企業診断士、行政書士
TEL:047-308-2256 FAX:047-308-2257
E-mail:to@iso-hiramatsu.jp