連載（30）

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30回　今回はPマークコンサルの現場から

～プライバシーリスクとビジネスリスクのバランスをとることがもっとも大切です～

平松　徹

1．リスクとは「確からしさとその結果の組み合わせ」

今回は今指導している企業の、Pマークコンサルの現場をスケッチします。それももっとも大切なリスクマネジメントのところに絞って報告します。

リスクという言葉、あいまいですね。われわれコンサルタント泣かせの言葉です。リスクというと危険という日本語になり、悪いことばかりとの印象なのですが、実は良いほうもリスクです。金融商品などでリターンに対するリスクという場合、リターンは投資の結果得るものであり、リスクはそのいろいろな状況すべてを含んだものになります。良い結果の場合もあるし、悪い結果になることもあります。簡単な言葉でいえばリスクとは「予想がブレた結果のいろいろな組み合わせ」です。

JISにリスクマネジメント規格があります。JIS Q 2001の「リスク」の定義は次のようになっています。

JIS Q 2001から

> d)リスク
> 自体の確からしさとその結果の組み合わせ、又は事態の発生確率とその結果の組み合わせ

> 備考1.ある状況では、リスクは予想との乖離のことである。

「確からしさ、自体の発生確率とその結果の組み合わせ」がリスクですから、将来や未来についてのいろいろな可能性がリスクです。

個人情報で考えてみます。例えば履歴書を取り扱っている採用担当者がいるとします。採用するかどうか履歴書を見て検討していたのですが、チョッとトイレに立ったときにうっかり履歴書をおきっぱなしにして離席をしてしまった。それで他の人に履歴書の内容が丸見えになってしまった。これは個人情報の漏えいです。普段はしっかりしているＡさんなのでこんなことはないのですが、チョッと熱っぽくてついトイレにそのまま立ってしまったのです。

このときのリスクの一つはＡさんがトイレに立って履歴書を裏返しにしなかったから、個人情報が誰の目にも見えてしまったことです。例えば上司が声をかけて、今日は早く帰ったらと進めてＡさんがトイレに立つ前に履歴書をきちんとしまって帰ったなら、個人情報の漏えいはなかったかもしれません。それだと個人情報が漏れることはなかった。これも一つの可能性としてありました。未来で想定されるいろいろな可能性がリスクです。

2．リスクマネジメントはいろいろの可能性を考えて、手を打つこと

リスクマネジメントとは、そのいろいろとある可能性の中から課題を特定し、事前対策を打つことです。簡単にいえば、悪い状況を事前に検討してそれに対処するようにすれば悪いことは未然に防ぐことができます。

個人情報マネジメントシステムもリスクマネジメントを核にしています。個人情報が漏れること、そしてその結果として個人情報の「本人」が迷惑

を被ることがリスクです。

ずいぶんと難しい話を延々としてきましたが、コンサルタントは大事な言葉でブレてはいけません。それではプロフェッショナルの名前が泣きます。だからまずしっかりとリスクという言葉を確認しました。

3．Pマーク委員会でのリスクの説明

PマークもISOの親戚ですので規格要求事項を基にしています。これがPマークではJIS Q 15001規格です。リスクの関連については、次の通り要求しています。

JIS Q 15001:2006規格より

3.3.3 リスクなどの認識、分析及び対策

事業者は3.3.1によって特定した個人情報について、目的外利用を行わないため、必要な対策を講じる手順を確立し、かつ、維持しなければならない。

事業者は、3.3.1によって特定した個人情報について、その取り扱いの各局面におけるリスク(個人情報の漏えい、滅失またはき損、関連する法令、国が定める指針その他の規範に対する違反、想定される経済的な不利益及び社会的な信用の失墜、本人への影響などのおそれ)を認識し、分析し、必要な対策を講じる手順を確立し、かつ、維持しなければならない。

次はPマーク取得に取り組んでいるある会社のPマーク委員会でのリスク説明の場面です。ISOも同じですが、認証取得最初の頃の委員会では、規格要求事項を規格本文を参照しながらの説明が主になります。

「リスク」を説明します。15001を見てください。リスクについてカッコの中に書いています。

リスクとは「個人情報の漏えい、滅失またはき損、関連する法令、国が定める指針その他の規範に対する違反、想定される経済的な不利益及び社会的な信用の失墜、本人への影響などのおそれ」です。

図表1を見てください。

図表1

リスクとは

- 個人情報の漏えい、滅失またはき損
- 関連する法令、国が定める指針その他の規範に対する違反

これらはプロセスリスク。結果として「本人」に悪影響を及ぼす危険性がある。

- 想定される経済的な不利益及び社会的な信用の失墜
- 本人への影響などの、おそれ

これらは結果のリスク。「本人」への影響そのもの。

個人情報が漏れたり、壊れたりしたら「本人」が迷惑を被る可能性が高いですね。ここで「本人」というのは個人情報の本人をいいます。「Bさん」という個人情報の「本人」はBさんです。個人情報が壊れるというと、例えばクレジット情報の中の個人情報が壊れる場合などです。生年月日が間違えているとクレジットが効かなくなってしまうかもしれません。クレジットが使えないのは本人にとっては迷惑です。

リスクには2種類あります。プロセスのリスクと結果のリスクです。

今の例で言うと、生年月日を間違えてクレジット情報として入力することはプロセス上のリスクです。これでは必ずしも個人情報の「本人」が迷惑するとは限りません。しかし、このために個人情報の「本人」がクレジットが利かなくて困ってしまったら、結果としてのリスクになります。この二つを明確に区別して考えることが大切です。

結果としてのリスクが重大であれば、リスクを防ぐ事前の取組みにも質的にも量的にも大きなものが要求されます。

例えば、病院のカルテが漏えいして過去の病気が分かってしまったので、管理職への登用を見送られたというのは、個人情報が漏れてしま

ったことによる結果のリスクです。これはとても影響が大きいので、病院のカルテについては、本当に厳密な管理の仕組みが必要です。ここでは結果としてのリスクの大きさが、リスクが起こらないようにする取組みを決定する大きな要素になることを理解してください。

一方、プロセスのリスクについては「事態の発生の確率」ということに関連してきます。病院のカルテが紛失してしまっても、カルテの個人情報の本人たちにどのような迷惑が及ぶかどうか分かりません。あまり良い気持ちはしないので大なり小なり個人情報の「本人」にとって良くはないのでしょうが、関係ないよっておっしゃる方もいるに違いありません。人それぞれです。

カルテが1枚紛失したら、これはまずプロセス上のリスクです。これで「本人」が平気だったら影響は軽いですね。風邪を引いた履歴しかないようなカルテだってあるでしょう。風邪を引いたので1回行っただけの病院のカルテであれば、そのカルテが漏れてもたいしたことありません。でもだからといってカルテが紛失して良いわけではありません。カルテが紛失するというプロセス上のリスクはぜひ防がなければいけません。

つまり結果としてのリスクとプロセス上のリスクと分けて考えないといけないということです。

4．名刺管理で考えてみます

次に名刺で考えてみます。Pマーク制度では、名刺の取り扱いが一般常識とはかなりかけ離れて取り扱われます。すこし異様なくらいです。

名刺は1枚1枚管理しなさいという審査員が多い。仕事の基本からは名刺1枚をきちんと管理することは大切なのですが、少し過剰の感があります。

例えば名刺1枚を机に上においてCさんがトイレに行ったとします。この名刺の出し放しについて。もうひとつ、名刺をしまうときの施錠管理の問題について少し考えてみましょう。

名刺の出し放しはやはりまずいですね。個人名があるものは原則として個人情報の名前が見えないようにして離席をしないといけない。その通りです。というよりも、書類を机において離席するときは、裏返しするのが仕事の基本ですね。これは個人情報だから裏返すのではありません。個人情報管理ではなく、情報管理として問題なのです。書類は情報の塊です。それが漏れたらまずいのです。

しかし、名刺はどうですか?名刺は誰にも配ります。情報が漏れない情報管理が必要ですか。漏れてもかまわないのだったら、名刺を出し放しにして離席しても良いかもしれません。むしろ皆の目に触れたほうが、名刺の個人情報の「本人」は喜ぶかもしれません。

「ほう、○○さんに合えたのか、良かったな」と上司とのコミュニケションも弾むかもしれない。しかし、かなりのPマーク審査員がこれはダメというようです。個人情報の漏えいはいけないことですから。

15001規格でいうと確かにこれは許されません。ここは15001規格の限界と私は考えています。Pマークを取ろうと思ったら、この点は考えを変えないといけません。チョッと常識からは外れますが、しようがありません。そうしないとPマークは取れません。今のところですが…。

もうひとつ、名刺保管の施錠管理の問題があります。わたしもすべての審査員にお会いしたわけではないので、なんともいえないのですが、よく聞く話では、名刺1枚だって個人情報だから、やはり机の中で保管するのであれば、1枚でも施錠管理が必要なので、鍵のかかるところに入れるのが、多くのPマーク審査員の判断のようです。

Pマーク制度の基本的な考え方について少し考えましょう。

15001規格に次のようにあります。

JIS Q 15001規格より

> **3.1 一般要求事項**
> 事業者は、個人情報保護マネジメントシステムを確立し、実施し、維持し、かつ、改善しなければならない。
>
> **2.7 個人情報マネジメントシステム**
> 事業者が、自らの事業の用に供する個人情報について、その有用性に配慮しつつ、個人の権利利益を保護するための方針、体制、計画、実施、点検及び見直しを含むマネジメントシステム

5・プライバシーリスクとビジネスリスク

Pマーク委員会の場面を続けます。

> 個人情報マネジメントシステムを確立することが大切なのですね。そして、個人情報保護マネジメントとは「個人の権利利益を保護する」ためのマネジメントシステムです。「有用性に配慮しつつ」という表現がとても大切です。有用性とは役に立つということです。マネジメントをしっかりとして、個人が迷惑を被らないようにしないといけないということです。そのためのマネジメントシステムがここでは要求されています。
>
> ここでプライバシーリスクとビジネスリスクについて説明します。
>
> プライバシーリスクとは、個人情報についてのリスクです。ビジネスリスクとは、ビジネス全般を遂行するときに障りになるリスクです。
>
> 名刺1枚でも施錠管理するのはプライバシーリスクを考えると必要です。しかし、鍵のない机に座っている人は会社として鍵を新たにつけないといけなくなります。出費だし、鍵をかけたり、外したりの手間も増えますね。
>
> 確かに名刺ホルダーを使っている名刺ホルダー保管には施錠管理が必要です。個人名がたくさんになるとDMなども打てます。DMをもらう人にしてみればはた迷惑この上ないかもしれません。だから名刺ホルダーは厳重に管理する必要があります。しかし、名刺をほとんどもらわないような人の机も施錠管理が必要なのでしょうか。
>
> これが、プライバシーリスクとビジネスリスクのバランスの問題です。ビジネスリスクを考えたら、名刺をあまりもらわない人の机には施錠管理はもったいない。金銭的にも手数としてもです。このあたりのバランスを間違えるとビジネストとして非常に非効率になります。Pマークを取る以上、プライバシーリスクを優先することは必要です。ただ程度問題です。
>
> 大切なのは、Pマークのマネジメントの目的が、「個人が迷惑を被むらないこと」だったこと。結果としてのリスクをここでは考えるべきなのです。名刺が1枚漏れても誰も迷惑しないのです。ただ、勤めている会社を知られたくないという人もいると思います。いやいや名刺を作らされて、いやいや名刺を渡した。そんな人にとっては自分の名刺が人の目に触れるのが嫌でしょうね。プライバシーリスクはそこまで考えないといけません。いったん考えて、その結果そんな人はごく稀だから今回は考慮しないとすれば良いわけです。検討することが大切です。

6・プライバシーリスクの取り扱いについては企業ごとに違ってよい

15001規格に「安全管理措置」というのがあります。

JIS Q 15001規格より

> **3.4.3.2 安全管理措置**
> 事業者は、その取り扱う個人情報のリスクに応じて、漏えい、滅失またはき損の防止その他の個人情報の安全管理のために必要、かつ、適切な措置を講じなければならない。

そしてその解説が次です。

JIS Q 15001:2006 解説より

3.4.10 安全管理措置(本体の3.4.3.2)

なお、安全管理措置は、個人情報が漏えい等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情報の取り扱い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ことが求められているのであって、すべての個人情報について一律な措置を求めるものではない。

“漏えい、滅失またはき損”とは、個人情報保護法第20条で規定する内容と同義であり、個人情報への不正アクセス、個人情報の紛失、破壊及び改ざんなども含む概念である。

“必要かつ適切”という意味は、経済的に実行可能な最良の技術の適用に配慮することである。“経済的に実行可能な最良の技術”は、事業者の事業内容や規模によって異なる。

またまたPマーク委員会の場面です。

ここで言っているのは、100%の手を打つ必要はないということです。まず、15001規格では「すべての個人情報について一律な措置を求めるものではない」と言っています。「本人が被る権利利益の侵害の大きさを考慮」がやはり最終の基準です。そして、「事業の性質及び個人情報の取り扱い状況等に起因するリスクに応じた必用かつ適切な措置」といっています。

個人がどれくらい迷惑を被るかの程度を基準にして、どんな事業での取扱い、どのような個人情報の取り扱いなのかを考慮して、必要かつ適切な措置をしたら良いということです。

そして大切なのは、「必用かつ適切」というのは「経済的に実行可能な最良の技術の適用に配慮することである」ということ。そして「“経済的に実行可能な最良の技術”は、事業者の事業内容や規模によって異なる」とも言っているのです。

15001規格も事業者の状況を考えてよいと言っています。

「経済的」が判断基準です。当社の「経済的」の基準がここで必要になってきます。それを明確にしておくことが、今後の取組みがブレないために必要です。Pマーク審査員からいろいろと言われたときに、そこを明確にしてたじろがないことが良いPマークにするためにぜひとも必要です。ビジネス上どこまで許容できるかが、ポイントです。経済的に実行可能だからと、会社にあるお金をすべて使ってよいわけではありません。ビジネスに障りが出るのであれば、それと個人情報「本人」への個人利益の保護を天秤にかけて重いほうを取らないといけません。赤字を出してまで、個人情報の保護のほうに大きく力を入れるというのは、部分最適は満たしても必ずしも全体最適を充たしてはいません。

プライバシー保護は図れても、ビジネス全体の利益は図れないとまずいということです。

Pマークを取ろうとしてプライバシーリスクだけを考えると、ビジネスリスクのほうがおろそかになります。Pマーク審査ではプライバシーリスクに重点が置かれすぎる場合が多いようです。

あるISOコンサルタントとお会いしたときのこと。その方はPマークについても10社以上指導されているということでした。「Pマークの審査員はISOと違って審査員要求事項が多すぎますね。過大な要求が多くて本当に困ってしまいます」とポロッとおっしゃっておりました。

ビジネスの障りになったらPマーク制度も生かされません…。

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