連載（41）

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41回「役に立つPマークのポイントご紹介します」の1回目

平松　徹

1. 形だけのPマークだから返上することになる

Pマークを取得する会社が増えています。取引先からの要請があり、取得を決めたというところが多いようですが、一方せっかく取得したのに、返上する会社もまたあるようです。その返上の理由は、個人情報の取り扱いについてかなりの手数がかかり、なかなか実行できない。形だけのPマークになっている。ならば返上しようということのようです。

個人情報を大切に取り扱うことは良いことですから、簡単に返上ということももったいない。実行して成果が上がる取組みであれば良いわけです。

どのようなシステムを作り、文書化し、実行するかがポイントになります。そのあたりについて、3回ほどにわたり、実際の取得についてのポイントや文書のモデルなどご紹介したいと思います。

今回はプライバシーマネジメントシステムでもっとも基本になる、個人情報の洗い出しと、リスク管理について書きます。

2. 文書体系の確認です

まず文書関連の確認から。

Pマークの要求事項であるJIS Q 15001に次のようにあります。

> **3.5.1 文書の範囲**
> 事業者は、次の個人情報保護マネジメントの基本となる要素を書面で記述しなければならない。
> a)個人情報保護方針
> b)内部規程
> c)計画書
> d)この規格が要求する記録及び事業者が個人情報保護マネジメントシステムを実施する上で必要と判断した記録

これが文書作成として要求されているものです。このうち内部規程は15個必要ですし、計画書は「教育」と「内部監査」の2つを作成しなければなりません。また、この他にプライバシーマネジメントシステム（以下PMS）について全体像を表現した「個人情報基本規程」も必要です。これは会社の個人情報についての取組みの全体像がわかる文書です（**表1**）。今回載せる私のモデルはかなり個性的ですが、分かりやすく作っているので参考にしていただければと思います（表1参照）。

その全体像に対して詳細なルールなどを書いたものとしての各種手順書や規程、そして実際にPMSを運用していくときに必要な記録を残すための帳票フォーマットも必要です。つまりPMSは文書体系としては次の3つのからなります。この枠組みが大切です。

> **PMSの文書体系**
> 1. 個人情報基本規程
> 2. 各種規定、手順書類
> 3. 運用のための帳票フォーマット

表1 「個人情報基本規程」モデル

3.3 計画

3.3.1 個人情報の特定

15001	責任者	当社の具体的取組	規程・記録
「個人情報」特定の手順の確立と維持	個人情報保護管理者	・当社の事業運営で取り扱うすべての個人情報を洗い出し、特定する。 ・「個人情報運用マニュアル」「個人情報特定規程」に基づいて個人情報を洗い出し、「個人情報洗い出し台帳」に記入する。 ・保護すべき個人情報について「個人情報管理台帳」に登録し管理する。 ・「個人情報管理台帳」は新規の個人情報の取り扱いが発生したとき、及びMRで見直しを実施する。個人情報の特定の手順について問題点が発生したときは「個人情報運用マニュアル」「個人情報特定規程」についても見直しを実施する。	「個人情報運用マニュアル」 「個人情報特定規程」 「個人情報洗い出し台帳」 「個人情報管理台帳」

3.3.2 リスクなどの認識、分析及び対策

15001	責任者	当社の具体的取組	規程・記録
目的外利用の防止の手順の確立、維持 リスクの認識、分析及び対策の実施	個人情報保護管理者	・目的外利用を防止するために必要な対策などについて「個人情報運用マニュアル」「個人リスク管理規程」で明確にし、目的外利用がないよう取り組みを実施する。 ・個人情報を取り扱う各局面でのリスクを認識し、分析し、対策を講じる。対策の実行と効果についてMRで評価し、改善を図る。 ・「個人情報運用マニュアル」「個人リスク管理規程」「リスクマネジメント表」については、MRで見直しをする。	「個人情報運用マニュアル」 「個人リスク管理規程」 「リスクマネジメント表」

3. 二重構造のPマーク

この中ではやはり目を引くのは内部規定の多さです。

規程は運用ルールなどを文書化したものですから守られなければ意味がありません。ただこれだけ規程類があると現場でこの通り実行しなさいといってもなかなかできるものではありません。

そこで私は「二重構造のPマーク」ということで指導をします。会社全体としての構築はきめ細かく、重箱の隅を突つくくらいに作り上げ、一方、現場では大事なことを確実に実行するために極力ポイントを絞り込んで運用します。

そのための文書として全体版が「個人情報基本規程」と「各種規程類」、現場運用版が「個人情報運用マニュアル」になります。「個人情報基本規程」と「各種規程類」を要約したものが個人情報運用マニュアルといっても良いですね。

とにかく現場でしっかり運用することが最大のポイントになる。実行することの意味が分かり、自覚した上でPMSを実行するためには教育も必要です。その教材として「個人情報運用マニュアル」がある。新入社員が入ってきたときも「個人情報運用マニュアル」を渡して教育する。それを続けていくとプライバシーについての自覚も深まり、PMSの本来の目的である人をいたわり配慮するということもできてきます。

なんといっても個人情報保護法にしてもPマーク制度にしても、その根本は個人情報がプライバシーにかかわり、触ると痛いという痛みを伴う場合があることの理解と配慮です。

4. JIS Q 15001の「解説」が大切

それでは、さっそく個人情報の洗い出しから始めます。業務ごとにどのような個人情報を取り扱っているか、業務の流れに沿って洗い出しを実施します。

15001規格に次のようにあります。

> **3.3.1 個人情報の特定**
> 事業者は、自らの事業の用に供するすべての個人情報を特定するための手順を確立し、かつ、維持しなければならない。

ここで大切なのは、「手順を確立」「維持」という言葉です。手順の確立とは単に仕組みを作ればよいのではなく、確実に文書化するということ、また維持というのは状況が変わればその文書も変え、常にPMSと整合性を持つように維持をしなければいけないということです。

Pマークの要求事項であるJIS Q 15001には「解説」がついています。この解説が大切です。ここを読んでPMSを組み立てることをお勧めします。Pマーク審査を受けると分かるのですが、審査員

表2 「個人情報管理台帳」(個人情報洗い出し台帳)モデル

業務	個人情報	入手先	利用目的	管理者	件数	保管場所	保管期間	廃棄方法
採用	履歴書	応募者	採用管理	人事課長	50件/年	人事キャビネット	採用 → 退職後 10年	シュレッダー
							不採用 → 10日以内に返却	返却

の審査はかなり硬直的との印象があります。建前で押してくる。柔軟性に乏しい。それに対しこの「解説」は少し柔軟です。

解説で次のように述べられています。

- ●個人情報をもれなく特定できる手順をルールとして確立する。
- ●特定した個人情報については、「個人情報の項目、利用目的、保管場所、保管方法、アクセス権限を有するもの、利用期限等」を記載した「個人情報管理台帳」を整備し、その台帳を定期的に確認し、最新の状態で維持する。
- ●台帳整備については、全ての個人情報ではなく、利用目的の範囲内で個々の従業者にゆだねるなど、柔軟な取り扱いで良い場合もある。

5. 保護不要の個人情報は管理しない

個人情報の特定では、個人情報がどのような場合に取り扱われるのかを業務ごとに洗い出して「個人情報洗い出し表」に記録していきます。この作業では「請求書」や「見積書」などはとりあえず「個人情報洗い出し表」には載せますが、その後の「個人情報管理台帳」には載せません。

請求書には個人名が載りますが、それだけで請求書について個人情報保護を図るというのは現実的ではありません。解説で「柔軟な取り扱いでよい場合もある」とあります。台帳で管理するのは保護すべき個人情報に限定すべきということです。だから、個人情報特定手順のポイントになる文章は次のようになります。

1. 個人情報とは個人に関する情報で、氏名、生年月日その他の記述などによって特定の個人と識別できるものである。
2. 業務の中で取り扱われている個人情報を部門ごとに業務を振り返りながら洗い出し、「個人情報洗い出し台帳」に記録する。
3. 「請求書」や「見積書」など単に氏名のみが出てくる書類については、保護が必要ないものとして保護不要個人情報として、管理対象の個人情報から除外する。
4. 管理対象の個人情報を「個人情報管理台帳」に記録する。

ここでは個人情報管理台帳しっかり作成し、管理することが大切です(**表2**)。

6. リスクにはプロセス上のリスクと結果としてのリスクがある

次に「リスクの認識、分析、対策」です。「解説」に次のようにあります。

- ●リスク認識とは、特定した個人情報の「取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄」の流れの各局面において、適正な保護措置を講じない場合のリスクを洗い出すこと。
- ●リスク分析とは、洗い出したリスクを定性的な評価などをすること。
- ●洗い出したリスクに対して、合理的な対策を講じる。合理的な対策とは、事業者の事業内容や規模に応じ、経済的に実行可能な最良技術の適用に配慮することである。
- ●対策を打っても残る「残存リスク」を把握し、管理する。
- ●講じた対策が十分であるかを検証し、定期的に見直さなければならない。

リスクとは次のようにまとめることができます。

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

これらはプロセスリスク。

表3 「リスクマネジメント表」モデル

業務	個人情報	ライフサイクル	業務手順	リスク	影響	発生	評価	リスク対応	残存リスク
採用	履歴書（住所、氏名、生年月日など）	取得入力	本人などからの送付	漏えい、紛失、盗難。	A	中	8	手順を決め守る。教育する。	ヒューマンエラーによる漏えい、紛失。盗難。
		移送送信	必要に応じて持ち運ぶ。	漏えい、紛失、盗難。	A	中	8	手順を決め守る。教育する。	ヒューマンエラーによる漏えい。
		利用加工	採用についての判断をする。	漏えい（関係のない人が見てしまう）	A	中	8	手順を決め守る。教育する。	ヒューマンエラーによる漏えい。
		保管ＢＵ	履歴書用ファイルに入れ、キャビネットの所定の場所に保管。	紛失、盗難。	A	中	8	施錠管理。手順を決め守る。教育する。	ヒューマンエラーによる紛失。盗難。
		消去廃棄	保管期限後にシュレッダー処理。	間違ってシュレッダー処理をする。	A	中	8	手順を決め守る。教育する。	ヒューマンエラーによる紛失。盗難。

そしてその結果が「本人」に悪影響を及ぼす次の危険性につながる。

- 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。ここで「本人」というのは個人情報の本人をいいます。「Aさん」という個人情報の「本人」はA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使え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。プロセス上のリスクと結果のリスクです。

今の例でいうと、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。

一方、プロセス上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。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度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大したことありません。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。

リスク認識、分析、対策で大切なのは、業務の一連の流れの中で各局面での作業が必要になるということです。「リスクマネジメント表」のモデルを載せておきますので参考にしてください(表3)。次回はリスクマネジメントについてもう少し踏み込んで話しを進めます。

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