連載（33）

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33回　今回もPマークコンサルの現場から…④

～Pマーク審査あれこれ～

平松　徹

1. 名刺印刷委託先も管理する

今回もPマーク審査について書きます。

ある会社A社の現地審査での指摘事項について少し見てみます。

指摘事項

> **個人情報の委託先評価及び契約について**
> 貴社の個人情報の委託先特定に漏れがあり、評価及び契約も行われていない。再度、個人情報の委託先を見直し評価し契約すること。

もともとA社は3社の個人情報の委託先を評価し、契約していました。現地審査の時にほかに対象となる委託先があるのではないかと質問されて、名刺の印刷先の印刷会社など3社が新たに評価と契約の必要があるとのことになりました。

この名刺の印刷会社との委託先契約について聞いたとき、私は正直少し違和感がありました。A社は社員30人くらいの会社です。名刺発注は前に印刷してもらったものを再発注の依頼をするだけです。個人名と会社の住所、役職などが個人情報になります。それだけの個人情報の委託先です。それで個人情報委託先としての「評価と契約」が必要???

確かに、個人情報が悪用されて個人が迷惑をこうむってはいけません。A社の社員の個人情報が漏れてDMの宛先になったり、電話勧誘の相手先になってしつこく勧誘などされたら問題にもなります。だから委託先が個人情報を漏らさないようにすることは大切です。

しかし程度問題です。ここではバランス感覚が必要です。この会社では、名刺についてはいろいろな角度から検討し、名刺や名刺印刷についてはあまり細かい管理はしないことにしました。リスク評価でリスクが現実になったときの影響の度合いをそれほど大きいものではないとのことで、管理の程度を小さなものにしたわけです。

ただ、Pマークの要求事項が書かれているJISQ15001には

> **3.4.3.4 委託先の監督**
> 事業者は個人情報の取り扱いの全部または一部を委託する場合は、十分な個人情報の保護水準を満たしているものを選定しなければならない…。

とあります。この規格に従えば個人情報を一部でも業務委託すれば委託先の監督が必要となります。審査員は規格どおりに審査しているので問題ないわけです。JISQ15001規格が細かく要求しすぎているのかもしれません。

2. 現地審査の概要

ここで現地審査がどのように行われるのかご紹介します（**表1**参照）。

これが現地審査の概要です。間に1時間昼食休憩がありますので、正味6時間の審査です。ISO審査との違いはコンサルタントなどの外部者の立会いができない点です。私もISOの審査員をしていますが、確かにコンサルタントの立会いがあると少しやりにくいですね。仕組みの不備の状況や、考え方が少し間違っている点など、そのコンサルタントが指導したわけですので、少々指摘がしづ

表1　現地審査のスケジュール

時間帯	項目	内容
9:30 ～ 9:50	・代表者，関係者挨拶 ・代表者へのインタビュー	●個人情報保護に対する取組みや体制、マネジメントレビューなどについて聞く
9:50 ～ 14:00	・個人情報マネジメントシステム(PMS)の整備状況の確認	●個人情報に対する取組み状況の確認、質疑 ●事業内容、個人情報の流れ(収集、利用、保管、外部委託、廃棄・返却など)
14:00 ～ 15:50	・運用確認 ・社内見学	●PMSに基づいて運用されているかの確認 ●記録などの確認と特に安全対策を中心にした運用の確認
15:50 ～ 16:20	書類審査についての確認	●書類審査の結果を受けてPMSを修正、是正していることの確認
16:20 ～ 16:30	総評、終了挨拶	●1日審査した結果についてのコメント、今後のスケジュールなど

表2　審査員についてのアンケート内容

	質問内容
1	全体的に満足か
2	指摘事項、コメントが有益なものだったか
3	審査の進め方が、審査を受けた会社の個人情報の取り扱いの状況にあったものだったか
4	審査員がJISの要求事項を熟知した上での審査になっていたか
5	コミュニケーションが円滑に図られた審査だったか
6	審査員同士のコミュニケーションは円滑だったか
7	審査員の態度は紳士的だったか
8	時間を守っての審査だったか

らいことなどもあります。

ただ、指摘事項についての是正をしてもらう必要があるので、要求事項に詳しいコンサルタントがいらっしゃる方が、その後やりやすい場合もあります。その意味ではコンサルタントの同席は善し悪しです。

おもしろいのはお願い事項です。

> プライバシーマーク付与認定審査という業務の性格上、昼食、お土産などについては、固くお断りしています。

と明言しています。

これは審査を受けた会社から直接聞いた話なので間違いありません。ISOの審査でも多くの審査機関がこのような利益供与については禁止をしていますが、明言している会社はそれほど多くはありません。ただ、審査の公平さ、公正さを確保する意味では必要なことです。

3. Pマークでも審査員に対するアンケートがある

審査員に対するアンケートがここでもあります。質問項目は以下の8点で、「満足、やや満足、普通、やや不満、不満」の5段階評価です(表2参照)。

審査を受けた会社から聞いた内容ですので、アンケート通りの文章ではありませんが、内容はこの8つです。あるべき審査の姿を基準に質問しています。良いアンケートになっていると思います。

このアンケートの有効利用が審査を受ける会社には大切です。審査する方と審査される方はともすれば上下の関係になりがちです。審査が通らなければPマークを名刺につけることはできません。要求されることをすべてクリアーして初めて審査に通ると考えると、審査員のご機嫌を損ねないように、できるだけ甘くみてもらって審査をパスしたいと考えがちです。

ここでよく聞かれる言葉が「○○をしたら良いのですね」です。自分の会社にとって良いかどうかではなく、どのようにしたら審査に通るかの気持ちがにじみ出ている言葉です。アンケートの2番目の内容はそれを明確に否定しています。役立つPマークでなければいけません。

表3　指摘事項に対する改善報告書の内容

	改善報告書の内容での必要事項
1	不適合の原因を書く
2	不適合の原因を除去するための是正処置を書く
3	是正処置の効果(原因が除去されたか)を書く
4	不適合が除去されたこと、是正処置がなされたことを証明するものを添付する

4. 審査員は審査員アンケートをとても気にする

もう10年近く前になりますが、品質ISOのコンサルティング先が審査を受けたときに、社長に対してかなり居丈高で、規格で要求していないことをさも正当な要求のように押し付けていたので思わず「○○社長！ 審査員のアンケートがあるので何かあったらしっかり書くことも良いかもしれませんね」とその審査員に聞こえるように言ったら、その後ピタッとその審査員、おとなしくなりました。

また、これもやはり8年位前ですが、コンサルティング先が品質ISOの審査を受けたときに審査員の一人が夜に私の携帯に電話してきました。ただならぬ様子だったので何ごとかと思ったのですが、アンケートにかなりきついことを書かれたので、審査機関の社長にそうではないと説明して欲しいとの内容でした。かなり青ざめた声の表情でした。悪い評価ですと、次に使ってもらえません。審査員にとっては死活問題なのです。すぐにその審査員が良い審査をしていたことを審査機関の社長に電話しました。アンケートも善し悪しです。答える人の主観でかなり内容が左右されます。

しかし、アンケートを実施する方は注意しないといけません。うまく使わないと今度は審査員が顧客に迎合してしまうことになりかねません。厳しい審査ができなくなってしまいます。まさに両刃の剣です。

このアンケート、アンケート担当に行くようになっています。アンケートの依頼文章の中に「今後の審査業務の改善に生かすためにのみ利用し、これ以外には使用しない、記入された内容で審査上不利な扱いを受けることは決してない」などとも書かれているようです。このあたりの配慮も大切ですね。

5. 改善報告書は仕組みの見直し、再構築がポイント

指摘事項については文書でリーダー、そして審査員の方から審査を受けた会社に文書できます。文書の発行日から3カ月を期限として改善報告を求めます。ついでですが、この改善報告書を出したらまた再指摘事項が送られてきますが、その後

の期限は2カ月です。改善には時間がかかります。審査を受けてから認証まで、半年やそこらはゆうにかかると考えたほうが良いですね。Pマークを取得するのはなかなかやっかいです。

そして、改善報告書の書き方について審査員は注意してきます。その中の一つが対応結果についての報告の書き方、内容です。**表3**に示す4つを要求する場合が多いようです。

ISOでも是正処置については同じように原因の除去を要求します。ただ、原因の除去の要求はあまり有効ではありません。例えば先ほどの委託先についての指摘事項の不適合の原因はPMSを構築した担当者の「委託先管理」についてのJIS Q 15001の要求事項についての理解不足です。

初回登録の審査で出てくる不適合の原因は、ほとんどが審査を受ける会社のPマーク要求事項に対する理解不足、認識不足です。だから原因の除去はPマーク担当者の教育しかありません。あるいはコンサルティング会社の理解不足とそれによる指導ミスといったほうがよいのかもしれません。

ただ、Pマーク審査員の審査内容は審査員により大きく違います。指摘されたことが本当にその通り不適合かどうか疑問になることも少なくありません。良い審査員にあたるか良くない審査員に当たるかが、一番の大きいとの声もあります。それがいい加減な風聞でないことにPマーク制度の今後の大きな課題があります。ひとりのコンサルタントとして私もそこは実感します。コンサルティングするときにはいろいろの雛形を使いますが、同じ雛形で作成したものなのに審査員による指摘に大きなバラツキがあることが少なくありません。

是正は再発防止をすることです。仕組みを見直し改善することで再発防止としての是正はできます。その改善した仕組みの通りに運用していることを記録で証明すれば再発防止ができたことになります。だから、仕組みを見直すことを要求すれば審査を受ける会社も改善報告書を書きやすくなります。原因の除去などと難しい表現を使うのではなく、仕組みを見直し、再構築するよう指導すれば良いと思うのですが…。

6. 再指摘事項の内容

このA社ですが、この指摘に対して委託先3社の評価をし、契約もしました。それで改善報告書で報告しました。その後すぐにまた指摘事項がきました。次のような内容です。

再指摘事項

新たな委託先評価と契約は確認できたが、管理台帳に評価日と締結日が確認できない。日にちが確認できる管理をすること。また評価表と契約書を添付すること。

契約で大切なのは契約日がいつかということです。JIS Q 15001では具体的に要求していませんが、管理項目としては大事です。A社では管理台帳を手直しし、再度の改善報告書を作成提出しました。

7. 個人情報の利用の安全性の確保がポイント

Pマーク審査では「個人情報の利用の安全性の確保」ということにポイントを置いて審査がされます。インターネットでのやりとりで個人情報の暗号化の仕組みができているか、ネットワークに不正侵入されないような仕組みが構築されているか、個人情報に不正にアクセスできないためのアクセス制限はきちんとなされているかなど、かなり重点を置いて審査され、かなり高いレベルのセキュリティの仕組みを要求されます。

過去にトラブルがなかったから良いのではなく、今後トラブルが発生しないように予防処置の意味での取組みが要求されます。リスクマネジメントです。もしも個人情報が漏れたり、壊されたりしたときの影響を考えて、万全の対策を打っておくことが要求されています。

8. 説明責任を果たすことが大切

いまコンプライアンスが問われる時代です。個人情報が漏れた場合に、会社として手を打っておいた場合と管理が杜撰だった場合では世間の受け取り方に大きな違いが出ます。

説明責任は会社がどこまで仕組みを作り取り組んでいたか、どこができてどこができなかったのかなどを事実に基づいて周りに説明し明らかにすることです。説明できるためには仕組みを作って対策として実行できていることが前提です。少し手数がかかっても仕組みを作り取り組むことが大切と考えるべきです。それが会社を守ることになります。Pマークは個人情報の安全性については要求水準が高いと心得ておく必要があります。今後も個人情報が大切に取り扱われることが必要な社会が続きます。個人情報のセキュリティレベルを上げることはぜひとも必要です。

9. 個人情報関連はいろいろと課題が多い

ただ、個人情報保護の取組みについては、法律の内容、コンプライアンスの取組みの仕方など疑問に感じることが少なくありません。これはPマークとは少し離れた議論になりますが、例えば個人情報を扱うプロセスではいたるところで判子を押させられます。「とにかく押してください」と業務のいろいろな場面で要求されます。

会社を訪問してもスンナリ中に入れなくて、まず来訪者リストに書かされて、入館証をつけて初めて入れる会社も増えています。特定の部屋に入るときはセキュリティカードがないとは入れない会社も多いですね。本当に必要ならば良いのですが、余計と思えることも多く、ビジネスがスムーズに進まないもどかしさを感じるのは私だけでしょうか。

これはその仕組みが何のためにあるのかが明確にできていない場合に多く起こります。どのような個人情報があり、それが漏れた場合にどのような影響があるのかをしっかり評価する、「リスク評価」の取組みが弱いとそうなります。

JISQ15001でも、弱いのは要求事項のそもそもの目的や趣旨説明がないこと。また、「3.3.3リスクなどの認識、分析及び対策」が、きわめて簡単にしか記述されていないことも問題です。JIS Q 15001要求事項の解説にもあまり明確に説明されていません。その割に審査ではリスクマネジメントを徹底的に要求してくるのでその落差がかなり大きいですね。JIS Q 15001規格の改定も必要とされていると思います。

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