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32回　今回もPマークコンサルの現場から…③

～Pマーク審査では、ISOと違って、ここまで問われる～

平松　徹

Pマーク審査について、いろいろな会社の情報が入ってきます。私もPマークについてはコンサルティングしているので、審査情報については非常に気になります。Pマーク審査は、品質ISOや環境ISOとはかなり違う審査であることは明確な事実です。

そのあたり今回、少し詳しくご報告いたします。以下の指摘の事例は3つのPマーク審査の指摘事項を集めたものです。それも文書審査の結果を拾ってみました。プライバシーマネジメントシステム（以下PMS）の構築の状況を審査したものです。

今回の審査情報については断片的な情報ではありますが、Pマーク審査がISO審査に比べてかなり特色があることに気がつきます。今後もPマークの取得に取り組む会社も多いと思いますので、ぜひ参考にしてください。

1. 個人情報を特定する手順書の中には見直しの仕組みが必要

> 3.3.1　個人情報の特定①
> 個人情報を特定する手順の中に、見直しの手順が入っていない。

これは車の販売会社、A社での審査員の指摘です。Pマークでは保護しなければいけない個人情報を特定しなければいけません。そしてその特定した個人情報について、定期的に見直しをする必要もあります。その手順が抜けているとの指摘です。

15001規格では、個人情報特定の手順についてはその確立と維持しか要求していません。また、Pマーク審査員用のチェックリストでは個人情報を特定した台帳の更新と見直しの手順があるかどうかをチェックするようになっています。

確かに、一度個人情報の洗い出しをし、特定してそれでおしまいでは、チョッと問題です。企業を取り巻く内外の状況は変わるのですから、それに対応して台帳の内容を見直し更新をしなければいけません。それがない規定はやはり不備といわざるを得ません。

また、15001規格の「3.5.2文書管理」のところでは、文書の発行と改訂についての手順を要求しています。その点でも、ここでは見直しに関する手順を文書化する必要があります。

2. 手順書に5W1Hをすべて網羅する必要がある???

> 3.3.1　個人情報の特定②
> 手順はあるが、5W1Hで規定されていない。

この指摘は、ITによる中古車情報提供会社B社でのPマーク審査の事例です。個人情報の特定の手順書の中に5W1Hの要素が網羅されていないということです。

ここは15001規格では個人情報を特定する手順を確立し維持しろといっています。ただ、「3.3.5内部規定」で個人情報を特定する規定は要求されていますので、手順書や規定類が必要になります。

ここの指摘は、少し踏み込んで5W1Hを要求しているところに特徴があります。審査員のチェックリストでは個人情報を特定する手順と承認手順が明確であることを審査するようになっていますが、5W1Hまでは要求していません。審査員独自

の要求事項です。本来不適合の指摘はできません。すべてに5W1Hが必要とはとても思われません。審査員の過剰要求です。

3. リスク管理はポイント中のポイント

> 3.3.3　リスクの認識、分析及び対策
> リスク分析でライフサイクルに応じてリスクを洗い出す手順が明確になっていない。

これはデザイン広告会社C社審査での指摘です。リスク関連のところはPMSではポイント中のポイントになります。15001規格では「3.3.3.3 リスクなどの認識，分析及び対策」でほんの6行しか文章がないのですが、ここをいい加減にしていると審査ではぼろくそに指摘されます。しかし、15001の要求事項が簡単すぎて分かりづらい。15001規格の解説のほうにはかなり詳しく載っていますので、そこを眼を皿のようにして読みこなすことが必要になります。

そしてポイントの一つがこのライフサイクルに応じたリスク分析です。15001規格解説では「リスク認識」について詳細に説明しています。リスクの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･廃棄までのライフサイクルの各局面で考慮されるリスクを洗い出すこととされています。結果としてこれにはかなり細かい作業が必要になります。

解説の冒頭に、この解説書は規格の一部ではない、と明記されているのですが、法的要求事項は法律だけでなく「その他の規範」も入ります。解説もその他の規範ということで要求事項の一部と考えられます。だから結局ライフサイクルの各局面での洗い出しをしなければいけません。

しかし、実際の洗い出しになると本当に大変です。私もコンサルティングで一番苦労するのがこの箇所です。ただ、これをしないと審査には合格できませんのでしっかりと指導します。

審査員用のチェックリストでもライフサイクルに応じてリスクを洗い出す、となっています。要注意のところです。

4. 文章が入っていないからダメとチョッと乱暴な指摘

> 3.3.4　資源、役割、責任及び権限
> 「個人情報保護マネジメントシステムの見直し及び改善の基礎として」が文書の中にない。

これはB社審査での指摘事項です。「　　」の中の文章が手順書の中に書かれていないとの内容です。

この箇所は、個人情報保護管理者が事業者の代表者に、PMSの運用状況を、PMSの見直しと改善の基礎になるものとして報告しないといけないというものです。その文章が文面にないから不適合というものです。文章が入っていなかったから不適合というのは少し乱暴ですね。

ちなみに審査員チェックリストには報告しなければいけない旨を規定しているかどうかをチェックするようになっています。今回の指摘は審査員の過剰要求です。

5. Pマークでは監査責任者は保護管理者から独立している

> 3.3.6　計画書
> 監査計画書の責任者が保護管理者になっている。

これもB社審査での指摘事項です。監査計画は内部監査責任者が作成すべきなのに、保護管理者が作成する仕組みになっているとの指摘です。

15001規格ではPMSを確実に実行するための監査などの計画を文書化しろといっているだけですし、審査員のチェックリストでも事業者の代表者の承認を受けて監査の計画書を作れといっているだけです。

ただ、監査計画を保護管理者が作ってはいけないですね。個人情報保護監査責任者は保護管理者から独立しているわけですから、15001規格などに直接の要求事項がないとしても保護管理者が内部監査計画書を作ってはいけません。ここもISOとの違いです。ISOの場合は内部監査計画書は管

理責任者が作るのが一般的ですから。ここも注意したい点です。

6. 緊急事態が発生したときの公表についての指摘

> 3.3.7　緊急事態への準備①
> 緊急事態が起きたときに事実、発生原因とどのように対応したかを遅れることなく公表する手順がない。

これはA社審査での指摘事項です。緊急事態手順書はあるが、「公表」について漏れているとの指摘です。

ここは審査員のチェックリストでも緊急事態になったら可能な限り事実関係、発生原因、対応策について遅滞なく公表する手順ができているかどうかを審査するようになっています。15001規格も同じ要求事項です。指摘されてしかるべき「指摘」ですね。

7. 緊急事態が起きたらJIPDECに報告しないといけない

> 3.3.7　緊急事態への準備②
> 緊急事態の手順書があるが主務官庁及びJIPDECへの報告手順がない。

これはB社の指摘事項です。緊急事態手順書の中に主務官庁とJIPDECへの報告がないとの指摘です。

ここは審査員のチェックリストでは、規定などの中に緊急事態が発生したら事実関係、発生原因と対応策を「関係機関」に直ちに報告する手順がないといけないとなっています。

15001規格では、やはりチェックリストと同じく、事実関係，発生原因及び対応策を関係機関に直ちに報告するようになっています。関係機関にはJIPDECも入ります。かなり具体的で直接的な要求事項ですね。ISOでは考えられない指摘です。注意したいところです。

8. 経済産業省のガイドラインを参考にしないといけないという指摘

> 3.4.3.2　安全管理措置
> マニュアルに経済産業省のガイドラインを参考とした対策が講じられていない。

これもA社審査での指摘事項です。個人情報保護マニュアルに経済産業省のガイドラインを参考にした対策がないとの指摘です。

審査員のチェックリストでは、安全管理体制が整備されているかどうかを審査するようになっています。また、15001規格でも取り扱う個人情報が漏えい、滅失、毀損しないための安全管理を要求しています。そのときのキーワードは「必要、かつ適切」な安全管理措置ということです。

必要かつ適切な安全管理措置は企業の規模や業種により違いますが、このときの審査員は「経済産業省のガイドラインを参考にした対策が講じられていない」といっています。「参考にした対策」というところがおもしろいところです。

関係省庁からいろいろな個人情報取扱いについてのガイドラインが出ています。15001規格の解説では「行政機関が制定している個人情報の保護に関する指針(ガイドライン)」はこの制度の対象になる法律などであり、それを個人情報保護マネジメントシステムに反映できる手順の確立をしなさいといっています。

経済産業省のガイドラインをシステムに反映できる手順を作っていないので不適合との指摘は的確です。良い指摘と思います。経済産業省のガイドラインは、かなり具体的な指針になっていますので、それを参考にすると良いシステムを構築しての効果的な取組みになります。

9. スクリーンセーバーの起動時間も文書化しないといけないの???

> 3.4.3.2 安全管理措置
> スクリーンセーバーが離席してどのくらいで起動するのか規定がない。

B社審査での指摘です。コンピュータで作業をしていて、トイレなどに立つときにそのままにしておくと画面には個人情報がそのまま露出して漏えいという状況になってしまいます。そこで時間

がたつと自動的にスイッチが切れるスクリーンセーバーを入れて個人情報が漏れるのを防ぐ。その画面が切れる時間を明確に規定するべきだということです。

15001規格では、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るよう要求されているだけです。また、審査員のチェックリストには、盗難防止の措置が規定されていることとあり、「スクリーンセーバーの起動」は例示で上げられているだけです。

経済産業省のガイドラインにはスクリーンセーバーの起動について出ていますので、スクリーンセーバーについて審査員のチェックは良いと思います。ただ、起動時間まで要求するのはちょっと過剰要求なのではないでしょうか。これも審査員要求事項だと思います。細かく決めることに何の意味があるのか審査員は考えないといけません。

10. 教育では理解度確認までしないといけない

> 3.4.5 教育
> マニュアルなどに理解度確認を実施する手順が規定されていない。

A社審査での指摘事項です。教育したときに理解度を確認しないといけないのに、その仕組みが手順書の中に規定されていないという指摘です。

15001規格では事業者は関連する部署、関連する人にPMSについて理解させる手順書を作成することを要求しています。審査員のチェックリストも同じような審査内容になっています。

教育についての15001要求事項は、14001環境ISOに近いものがあります。PMSについて自覚教育を要求している点はうり二つです。ただ、環境ISOでは理解度確認までは要求していません。Pマークでは注意したいところの一つです。

次回は、もう少し文書審査の指摘を拾った上で、さらに現場審査での指摘事項についても取上げます。

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
090-4022-9024