Ｐマークニュース

＜２０１７年爽秋号＞　Vol.　２１

（株）トムソンネット

Ｐマークコンサルティンググループ

１．Ｐマークの遵守規格 JIS Q15001 の改訂

改正個人情報保護法が 2017.5.30 に施行されたことに伴って、個人情報保護に関する JIS Q 15001 が改訂されます。前回の制定が 2006 年ですから、11 年ぶりの改訂です。この規格はＰマークの遵守規格ですから、Ｐマーク取得事業者の遵守規程も変わってきます。改訂の骨子について、2017.8 に示された JIS Q15001 原案をもとに解説します。

（１）改正 JIS の基本としている考え方

①改正 JIS Q15001 は改正個人情報保護法に対応したものであるとともに、国際基準である ISO/IEC 専門業務用指針「附属書 SL」との整合性をとったものにしているといわれています。

ISO/IEC 専門業務用指針「附属書 SL」では、今後制定・改正される全ての ISO マネジメントシステム規格について、その構成、分野共通の要求事項及び用語定義を共通化することが定められています。

既に ISO9001（品質）、ISO14001（環境）、ISO/IEC27001（情報セキュリティ）は、付属書 SL に適合した規格構成に改訂されています。

これに伴いやや違和感を覚える定義もあります。「事業体」は「組織」と言い換えられ、「教育」は「認識」、「点検・監査」は「パフォーマンス評価」として規定されているなどです。

②改正個人情報保護法と整合させ、その定義も同一にしています。

例えば、法の定義との大きな違いのひとつに「個人情報」「個人データ」「保有個人データ」があります。法は「個人情報」「個人データ」を使い分け、個人情報の取扱いルールを下表のように規定しています。

	保有個人データ	個人データ	個人情報	匿名加工情報
利用目的の特定・通知等	○	○	○	
目的外利用の禁止	○	○	○	
適正取得	○	○	○	
安全管理措置	○	○		△
第三者提供の制限	○	○		
事業者名等の公表	○			△
本人からの開示請求等	○			

一方、JIS Q15001 では「個人情報」「個人データ」「保有個人データ」を区別せずに全てを一括して「個人情報」としていました。今回、法に合わせて定義したことによって、「保有個人データ」を「電子計算機を用いて検索することができるように体系的に構成した情報の集合物又は一定の規則に従って整理、分類し、目次、索引、符合などを付すことによって特定の個人情報を容易に検索できる

ように体系的に構成した情報の集合物を構成する個人情報であって、本人から求められる開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止の求めの全てに応じることができる権限を有するもの」(3.4.4.1 での定義)と定義することはなく、法の定義に従った「保有個人データ」として明確になっています。

しかしながら、「個人情報」「個人データ」については、改訂 JIS では注意が必要です。

改訂 **JIS Q15001** では「組織は、特定した個人情報については、個人データと同様に取り組まなければならない」(A.3.3.1)という規程を入れています。「個人情報」も特定した以上は「個人データ」として扱うのです。例をあげると、法ガイドライン(第三者提供時の確認・記録義務編)の、ただし書きに、「個人データ」でない「個人情報」については「義務がない」とされている項がありますが、その但し書きは意味がなく、そのただし書きは規定されていません。法よりも広い範囲の「第三者提供時の確認・記録」の「義務が生ずる」こととなります。個人情報と特定すれば、法がきめ細かくガイドラインで配慮していた取扱いはなく、改訂 **JIS Q15001** では、法が新たに追加した「第三者提供時の確認・記録義務」を広く適用することが求められています。

この他にもいくつかの改訂点があり、P マーク事業者の規程類には多くの改訂が必要になっています。

（２）公表されている今後のスケジュールについて

①改正 JIS のパブコメの締め切り・・・2017.9.17
②改正 JIS の公表・・・2017. 11 月の予定
③改正 JIS による P マーク新規審査・・・公表後 6 か月後から
④改正 JIS の実施ガイドラインの出版・・・ 2018 の春頃
⑤改正 JIS による P マーク審査移行期間・・公表後 6 か月後から 2 年間
⑥更新審査の改正 JIS による審査・・公表後 6 か月後から 2 年間は現行基準による審査も可

JIS 改正案目次の一部

Q 15001 : 9999

目　次

２．保険代理店様における個人情報保護への取り組み（２）
ー　Ｐマーク運用における PMS 事務局としての留意点　ー

前号に続き、保険代理店様の個人情報保護への取り組みをご紹介します。

今回は、丸紅セーフネット株式会社様で P マークの事務局をご担当されている経営管理部の高野様に P マーク運用のポイント等を伺いました。

（１）P マークを取得する「前」と「後」では、社内のみなさんの個人情報の取扱いに対する「意識」の変化はありましたか。

⇒　弊社が P マークを取得したのは 2015 年 7 月でした。そして今年（2017 年）の 5 月に最初の更新審査を受け、無事更新を済ませることが出来ました。

個人情報保護については、P マーク取得以前から弊社では社内規定の整備やシステム強化を図り、その対応に努めてきましたが、P マークの JIS 規格に基づく PMS 体制における PDCA の確立は、安易な妥協を許さない体系的なものであり、最初は全社に浸透させるため戸惑いました。P マーク取得後は、社内の雰囲気も徐々に「P マークを取得しているのだから・・・」ということで、定着化に向け良い方向に進み、現在では概ね順調に PMS を回すことが出来ているように感じます。

これを P マークの取得前後という観点で比較しますと、P マーク取得前は個別の対応策による「点」の管理だったものが、現在では全社での PMS の PDCA 展開によって、次第に「面」による個人情報保護体制が出来上がりつつあると評価しています。

（２）P マークの日常の運用で注力されている点や大切だと思われる事柄は何ですか。

⇒　PMS を運用する上で一番力を注いでいることは、個人情報保護の管理レベルを、支店を含めて全場所、全従業者において同レベルで PMS 運用を進めることです。

この方針を実現するために、個人情報管理台帳の作成およびリスク分析は、全部署（本社各部署および全支店）毎、個別に行って管理しています。また、PMS 監査においても全社同一レベルということを意識して監査・指導を行っています。このような全社同一性確保のアプローチについては、先般の P マーク更新審査の際にも、審査員の方から「PMS 運用の網羅性が高い」との評価を戴きました。

次に P マーク事務局担当者として心掛けていることは、日常の PMS 運用における記録類の整備・管理です。事務局の役目として運用状況の把握がありますが、日頃キチンとした運用記録等の整理によって、状況を容易に把握できるといった効果があります。

さらに PMS の運用記録で電子化できるものは、サーバー管理しています。サーバーで管理することで、支店等の担当者に確認連絡することなく、事務局で一括管理できるのはメリットです。

（３）最近の保険会社各社からの個人情報保護に関する指導・要請は如何ですか。

⇒　P マークを取得した時には、これで保険会社からの個人情報保護に関するヒアリングが簡単になるのではと期待しましたが、P マーク取得以降の各保険会社からヒアリング状況を振り返ると、期待した通りにはなっておらず、従前とあまり変わってはいません。

今年の保険会社のヒアリングにおいても、一部の保険会社から弊社が PMS 規程で定めている「委託先評価シート」について評価項目の不足を指摘されました。

こうした保険会社の指摘が各社一律であればよいのですが、現状は一部の保険会社の指導・要請が厳しい等、各社足並みが揃っておらずその対応に苦慮しています。

今後、情報セキュリティや個人情報保護に関する保険会社の指導が、PMS 規程を踏まえた各社統一的なものになって行くことを期待しています。

３．「やさしい情報セキュリティ」その１１：「自己点検」について

今回は「自己点検」について述べてみたいと思います。プライバシーマーク事業者の中ではお馴染みの“運用の確認”として JIS Q 15001 に掲げられていますが、大変重要な活動にも拘わらず“予備監査”と位置づけ、監査の前にしか実施されていない企業を多く見かけるからです。

JIS の解説編にも書かれているよう、自己点検は“日常業務において気付いた点があればそれを是正及び予防していくためのもの”です。退社時の戸締まりや消灯など、言わずもがなのことから決められた日（月）のパスワード変更や情報廃棄等々・・沢山のことが思い浮かぶことでしょう。監査が年に１回（標準的に）なのに対し、自己点検は項目によって毎日～半年と実施サイクルを柔軟に考えることができることから、運用がし易くしかも効果が高いとされています。

以下、自己点検を実際に運用するに当たってのヒントとなりそうなことを挙げてみます。

（１）“自己”点検は意味があるのか？

代表者の方にインタビューすると、よく「ウチの会社に悪い社員はいない」と仰られます。つまり「性善説」です。社員の中に“悪人”がいると思えば経営どころではない訳ですから当然です。

ここで、提案したいのは「性弱説」に立ちましょう、です。人は良かれと思ってルールと違うことをしたのが裏目に出たり、1 回くらいは・・とか、急いでいるから・・などと魔が差すこともあります。つまり“人間は弱いものだ”との認識からスタートしませんか？

自己点検は“自分への牽制”になります。もし虚偽の記入や報告をされた場合、後で発覚した際には罰則が適用されます。自己申告がベースとは言え、従業者にとって決して軽いものではないことを理解してもらえる筈です。

（２）本業に差し支えるのではないか？

自己点検は“タイムリーに”と良く言われますが、闇雲に従業者に押し付けると本業に差し支えることも出てきます。JIS のガイドラインには“日常的な運用の確認を実施するために業務に支障が出るというのでは本末転倒である”とはっきり記されています。

上述したように、毎日の最終退出時の記録がきちんと付けられているか（安全管理者）、などは月に 1 回でいいでしょうし、アクセスログの異常チェック（情報システム管理者）は毎週必要になるかもしれません。全従業者が対象になる、パスワードの変更は 3～6 ヶ月ごと、不要情報の定期的廃棄は年末の大掃除の時や年度末が適しているのではないでしょうか。いずれもリスク分析結果や社内規程にルール化されていることを確実に実施したか、の観点でチェックします。

一般的には 10～20 の点検項目を挙げ、各々の項目についていつ実施するかを年間計画表にまとめている会社を多く見受けます。毎回全項目を全従業者に強いる必要はありません。必要な時間も高々5 分程度とすることで十分効果を発揮できるものと考えます。

（３）やり方は？

やり方（実施の方法）には大別して、①全従業者に 1 年を通した点検表を配布し記入を求める、②グループ単位に 1 年を通した点検表を配布し記入を求める（リーダがメンバーに聴取したり実施記録を点検）、③事務局から都度点検項目を全従業者又はグループ責任者にメールで送り、それに回答を求める（その後事務局が集約）、の三通り（或いはその組み合わせ）があります。

中央省庁や行政法人などにおいては今や自己点検が義務化されており、誠にキメの細かい指針が示されていますが、各社では現実的に可能な運用を考えられたらいいと思います。点検項目も全社で同じとするのではなく、共通項目に加え実施対象者に独自に“率先して気を付ける”項目を追加してもらうことで味付けし、自主性を高めるのも有意義です。

自己点検自体も PDCA サイクルを回さなければなりませんので、監査やマネジメントレビューの時、発覚した問題の是正・改善状況や運用の改善、点検項目について代表者の意見聴取などを行うべきです。

（４）明日から

実行は早いに越したことはありません。実施中であれば、これを機会に点検項目や実施時期、実施対象者の再検討をされることをお勧めします。繰り返しますが、決して高見を狙わず定着度を睨みつつ年々精度を上げることを念頭に置き、着実に実施することが肝要です。

４．Ｐマークの審査機関と費用について

現在Ｐマークの審査機関は、一般財団法人日本情報経済社会推進協会（JIPDEC）によって指定された下表の18民間事業者団体とJIPDECが申請の受付・審査と付与可否の認定等を行っています。
（下表の取扱件数や審査費用等はJIPDEC公表資料に基づく集計および費用です）

（１）審査機関一覧と審査（新規取得＋更新）における取扱状況（2017年／10月）

（＊）審査件数は直近約2年間の新規・更新審査の合計、カッコ内は新規審査数を示します。

機関ｺｰﾄﾞ	Ｐマーク審査機関名	審査件数（＊）
11	一般社団法人情報サービス産業協会(JISA)	463(18)
12	一般社団法人日本マーケティング・リサーチ協会(JMRA)	106(3)
13	社団法人全国学習塾協会(JJA)	13(1)
14	一般財団法人医療情報システム開発センター(MEDIS-DC)（医療・福祉関連業種の申請先）	361(55)
15	一般財団法人全日本冠婚葬祭互助協会(全互協)	50(2)
16	社団法人日本グラフィックサービス工業会(JaGra)	198(17)
17	一般社団法人日本情報システム・ユーザー協会(JUAS)	3,090(708)
18	財団法人くまもとテクノ産業財団(KPJC)（九州・沖縄地方に本社のある会社の申請先）	731(114)
19	一般社団法人中部産業連盟(中産連)（愛知県、岐阜県、三重県、富山県、石川県に本社のある会社の申請先）	915(135)
20	一般財団法人関西情報センター(KIIS)（大阪府、京都府、福井県、滋賀県、兵庫県、奈良県、和歌山県に本社のある会社の申請先）	1,658(254)
21	一般財団法人日本データ通信協会(JADAC)	1,159(354)
22	一般社団法人コンピュータソフトウェア協会(CSAJ)	212(72)
23	特定非営利活動法人みちのく情報セキュリティ推進機構(TPJC)（東北地方に本社のある会社の申請先）	231(29)
24	社団法人日本印刷産業連合会（日印産連）	452(18)
25	財団法人放送セキュリティセンター(SARC)	169(19)
26	一般社団法人北海道IT推進協会(DPJC)（北海道に本社のある会社の申請先）	151(20)
27	特定非営利活動法人中四国マネジメントシステム推進機構（中四国MS機構）（中国・四国地方に本社のある会社の申請先）	349(47)
28	一般社団法人モバイル・コンテンツ・フォーラム(MCF)	32(7)
	一般財団法人日本情報経済社会推進協会(JIPDEC)	5,114(568)

（２）Ｐマークの新規取得および更新時の審査費用について

単位：円

区分	新規取得のとき			更新のとき		
種別(企業規模)	小規模	中規模	大規模	小規模	中規模	大規模
申請料	51,429	51,429	51,429	51,429	51,429	51,429
審査料	205,715	462,857	977,142	123,428	308,572	668,571
付与登録料	51,429	102,858	205,715	51,429	102,858	205,715
合計	308,573	617,144	1,234,286	226,286	462,859	925,715

企業規模は事業者の資本金および従業員数で決まります。
業種によって異なりますが、保険代理店が該当する「製造業・その他」の場合は、以下となります。

小規模	中規模	大規模
従業員2～20人	資本金3億円以下 または従業員21人から300人	資本金3億円超 且つ従業員301人～

５．お知らせ

（１）「Bad Rabbit」（ランサムウェアの一種）に関する緊急のお知らせ

「WannaCry」に続き、目下ランサムウェアの一種「Bad Rabbit」の感染が拡大中で、IPA（情報処理推進機構）から緊急警告が出されています。

https://www.ipa.go.jp/security/ciadr/vul/20171026-ransomware.html

感染すると PC が使えなくなり、ハードディスクからデータを取り出しても暗号化されているため開くことができません。開こうとすると金銭を要求されます。対策としては、

①不審なインストーラ等のプログラムを実行しない（特に Adobe Flash（筆者注））

②不審なメールの添付ファイルの開封やリンクへのアクセスをしない

③ウイルス対策ソフトの定義ファイルを更新する（OS のセキュリティ更新も。（筆者注））

④定期的なバックアップをする

とされています。万一感染した場合には、以下の窓口へご相談ください。

- IPA　情報セキュリティ安心相談窓口

https://www.ipa.go.jp/security/anshin/

Ｐマークについてのご相談は下記で承っています。ご気軽にどうぞ！

連絡先　　**株式会社トムソンネット**（http://www.tmsn.net/）

〒101-0062 東京都千代田区内神田駿河台４－６　御茶ノ水ソラシティ１３階

電話　03-3527-1666　　FAX03-5298-2556

担当:　岩原 秀雄（Mail：iwaharahi1017@tmsn.net）　　平泉 哲史（Mail：s.hiraizumi@tmsn.net）

本間 晋吾（Mail: s.honma@tmsn.net）

以上