Pマークニュース ＜２０１８年爽秋号＞　Vol.　２５	（株）トムソンネット Pマークコンサルティンググループ

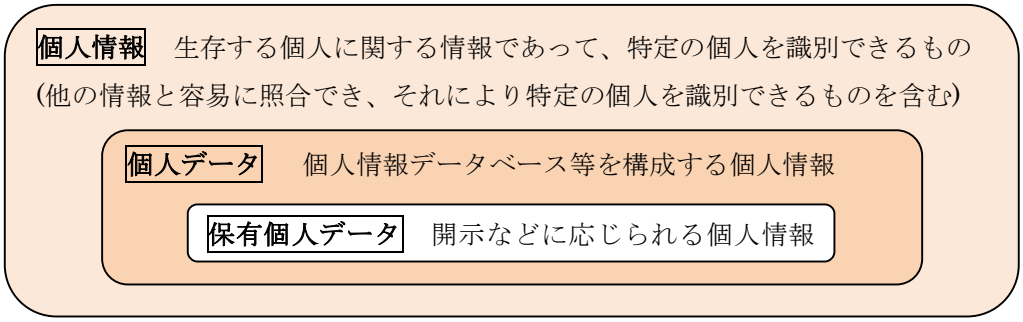
１．改訂 JIS(JIS Q 15001:2017)の運用

改訂 JIS(JIS Q 15001:2017)の「実践ガイドブック」が、漸く 2018.9.14 に発行されました。

改訂 JIS に基づいて運用をしようと思うといくつか「・・・個人情報保護法による」「・・・法令の定める手続きに基づき・・・」という規格に当たります。詳細な規格文はないため、個人情報保護法を理解していないと具体的にどのように運用するか分かりません。こうした悩みを解決すべく期待されていた「実践ガイドブック」ですが、やや期待外れのようです。そこで、いくつか、個人情報保護法（含むそのガイドライン）を参照しながら改訂 JIS の補完をできればと思います。（「実践ガイドブック」とは「JIS Q 15001:2017 対応　個人情報保護マネジメントシステム導入・実践ガイドブック」日本規格協会刊）

（１）「個人情報」と「個人データ」の取扱い

個人情報保護法（以下「法」という）では、「個人情報」「個人データ」「保有個人データ」について下記としています。「個人情報」は全般を規定する概念規定であり、その中に「個人データ」と「保有個人データ」があると定義されています。法でいうと「個人データ」は、「個人情報データベース」を構成する個人情報であるとしています。「保有個人データベース」とは、端的に言うと、個人情報取扱い事業者が開示等の請求に応じることができる「個人データ」です。



この定義に従い、法はその取扱いについて差を設けて規定しています。「個人情報」については、取扱い規制（義務）が軽く、「保有個人データ」については取扱い規制（義務）が重くなっています。図示すれば下表（次ページ）の通りです。

取り扱い項目	個人情報	個人データ	保有個人データ
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		○	○
本人からの開示請求等			○

一方 JIS の 2006 年版では、全てを「個人情報」として定義し、その取扱いを規定していました。JIS の 2017 年版では、「法に準拠することを原則」としつつ、「改正に当たっては，この規格が民間部門の個人情報保護の促進及び消費者保護に重要な役割を果たしていることから、要求事項の基本的な考え方を変更せず、旧規格に基づいて構築された個人情報保護マネジメントシステムがこの規格の改正によって不適合を生じないことに配慮した。」ため、「個人情報」と「個人データ」の取扱いについて、一見整合性が取れない運用となるのではないかと懸念されました。
今迄で必須事項として運用してきた「安全管理」「提供の取扱い」規程は「個人データ」のみ適用で、「個人情報」には適用しなくとも良いのではないか？ 運用の混乱が生じかねません。

そこで、JIS の 2017 年版では、「特定した個人情報については、個人データと同様に取扱わなければならない。」（A.3.3.1）と規定しました。これにより、運用では、従来どおり「個人情報」と「個人データ」の区別は意識せずに済むこととなりました。

しかしながらこの規定はやや大胆かも知れません。法のガイドラインには「・・・『個人情報』には該当するが『個人データ』には該当しない情報の場合」には、「提供者及び受領者に提供の確認・記録義務が適用されない」との解説があります。（法のガイドライン「第三者提供時の確認・記録義務編」）JIS の 2017 年版では、「『「法に準拠することを原則』としていますので、このガイドラインには従わねばなりません。一方で A.3.3.1 では「特定した個人情報については、個人データと同様に取扱わなければならない。」としていますから、特定していると提供の適用除外ガイドラインは意味が無くなりそうでもあります。

JIS の 2017 年版、A.3.3.1 は、「・・・特定した個人情報については、**リスクアセスメントの結果及びマネジメントレビューの結果によって**、個人データと同様に取り扱う。」という規定が適切なのかも知れません。基本は、個人情報保護リスクの低減でありその管理策が有効に働くことです。「木に竹を接いだ」感のある今回の JIS 改訂のようですが、運用上は、JIS の 2006 年版を踏襲でき歓迎する面もあります。

(2)要配慮個人情報の取扱い

JIS の 2006 年版では、「指紋や虹彩など一生変わらない身体の一部の情報は、『特定の機微な個人情報』と同等に取扱うことが望ましい」とされていました。一方。法は要配慮個人情報に含めていません。この結果、JIS の 2017 年版では、要配慮個人情報の規格(A.3.4.2.3)で、「個人識別符号」は、要配慮個人情報には、該当しないと解釈でき、今まで　特定していた運用上の変更が必要です。

更に、「労働組合」「性的嗜好」などの情報について、これを要配慮個人情報の「補完的ルール」として年内にも施行することを個人情報保護委員会は、公表しています。EU の GDPR(一般データ保護規則)と整合させ、EU の欧州委員会が認める「十分性認定」の発効に合わせるためです。

早晩、「労働組合」「性的嗜好」などの情報を反映させた JIS の変更も考えられます。

２．事例に学ぶ：「認識」に漏れはないか　～日本年金機構入力ミス事案～

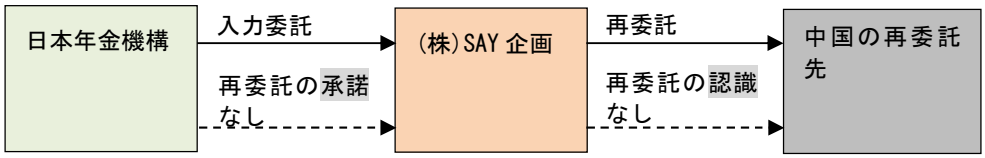
前号に引き続き、事例を元に情報セキュリティの維持・向上のお役に立ちそうなことを述べさせていただきます。今回は 2018 年の春に発覚した日本年金機構（以下「機構」）に関わる事象です。又かと思われるかも知れませんが。

今春、機構が入力委託したマイナンバー等のデータに漏れやミスが大量に見つかり、然るべき時期に源泉徴収税額を反映できなかったことがありました。機構の発表によると、「入力委託先・(株)SAY 企画の入力漏れで、2 月 15 日の支払い時に正しい源泉徴収税額を反映できなかった。2 月 14 日に入力漏れが判明した約 6.7 万人については日本年金機構が入力作業を行い、3 月 15 日の支払い時に還付した。また、2 月 15 日以降に判明した約 1.7 万人の入力漏れは、4 月 13 日の支払い時に正しく反映する」としています。併せて、「入力誤りは約 31.8 万人を見込んでいる。日本年金機構が点検した約 528 万人のうち、源泉徴収税額に影響があった場合も 4 月 13 日の支払い時に正しく反映する」との報道もありました。

どうしてこのようなことが起き、更に問題を大きくしてしまったのか検討してみようと思います。

（１）なにが問題か

本事案は、受託した(株)SAY 企画（以下「SAY 企画」）の業務の質(Q)と納期(D)がずさんだったのが問題と見えますが、機構のチェックの過程でそれ以上に重大な指摘を受けたのは〝再委託〟、それも外国の会社に発注していたことで、国民の不安も煽りました。



機構は、契約上 SAY 企画に再委託は承諾をしておらず、SAY 企画も再委託の承諾申請も行っていませんでした。それに、個人情報保護法の第 24 条（外国にある第三者への提供の制限）では「外国にある第三者に個人データを提供する場合には、あらかじめ外国にある第三者への提供を認める旨の本人の同意を得なければならない」と定めています（例外あり）。この場合、SAY 企画が年金加入者の同意を得るのは現実的ではありませんので機構が行うべきですが、再委託を禁じているため機構はその必要性を認識していません。

そのため、問題のテーマが Q・D から〝委託先の監督〟に移って行きました。SAY 企画は再委託禁止の契約条項に違反したと言うことです。

（2）原因はなにか

事象は 2 点あります。1 点目は発端となった Q・D のこと、2 点目は委託のことです。個人情報の取扱いの視点で考察すると D は除外するとして、1 点目の Q については情報の正確性の原則にもとりますが、ミスが多発したのは実は中国会社ではなく SAY 企画本体だったとの報道も見受けられますので、一般性に欠ける事象と考えこの稿では省略します。

2 点目の委託について、他社の教訓になるのが〝再委託〟です。代表者は「再委託先の業者は中国・大連にあり、5 年前に設立し資本関係はないもののグループ会社のような感覚で再委託の認識はなかった」と発言しています（産経新聞 2018.3.21）。〝グループ会社であれば再委託先に該当しない、しかも外国であっても個人情報を提供できる〟との認識であったようで、これが社会問題になった大元の原因と言えます。

（3）顛末は倒産に

機構は委託業者側の Q・D に問題があり、契約違反を侵し社会不安を呼んだとして SAY 企画に対し向こう 3 年間の競争入札への参加資格を停止しました。主力ユーザからの受注が途絶えた同社の社長は 2018 年 4 月に閉鎖を公表し、同年 6 月 5 日開催の株主総会の決議で解散しました。個人情報の取扱いに関する不祥事で倒産にまで至ったのは希有なケースです。

なお、SAY 企画はプライバシーマーク事業者でしたので、総会に先立つ 6 月 1 日付けで JIPDEC から〝プライバシーマーク付与一時停止措置〟の処分を受けています。

（4）まとめ

今回の問題は、SAY 企画の仕事の質と納期において機構が満足できるレベルでは到底なかったこと、及び業務遂行の過程で承諾されていない再委託を行ったことにあります。再委託先が国外であったことも火に油を注ぐことになりました。

問題を大きくした原因を突き詰めると、代表者に（担当者もか）再委託の認識が欠如していたことにあるのではないでしょうか。〝グループ会社のような感覚〟は確かにその通りだったのでしょう。ではグループ会社なら個人情報を提供していいのか、と言えばそんなことはありません。純然たる委託先です。

社内では極く当たり前のこととして、従前通りになんの疑問も持たず業務を進めていることが多くあります。暗黙知を形式知にしようとの活動は盛んに行われていることと思いますが、そもそも意識にない事柄はその網に掛かりません。ある一方だけからのアプローチ（点検）では〝漏れ〟が出て当然です。

従って、委託先の洗い出しにおいては、業務の流れから攻めるのも一手（こちらが本線）ではありますが、経理部門で把握している支払先を一度洗ってみてはいかがでしょうか。同様のことが「個人情報の特定」でも言えます。業務フローを元に個人情報を抽出したのであれば、机の引き出しやキャビネットの棚卸をする、或いはその逆を是非とも実施されるよう提案します。以て〝認識の漏れ〟をなんとしても防ぎたいものです。

３．Ｐマーク取得事業者における個人情報漏えい事故状況（2017 年）

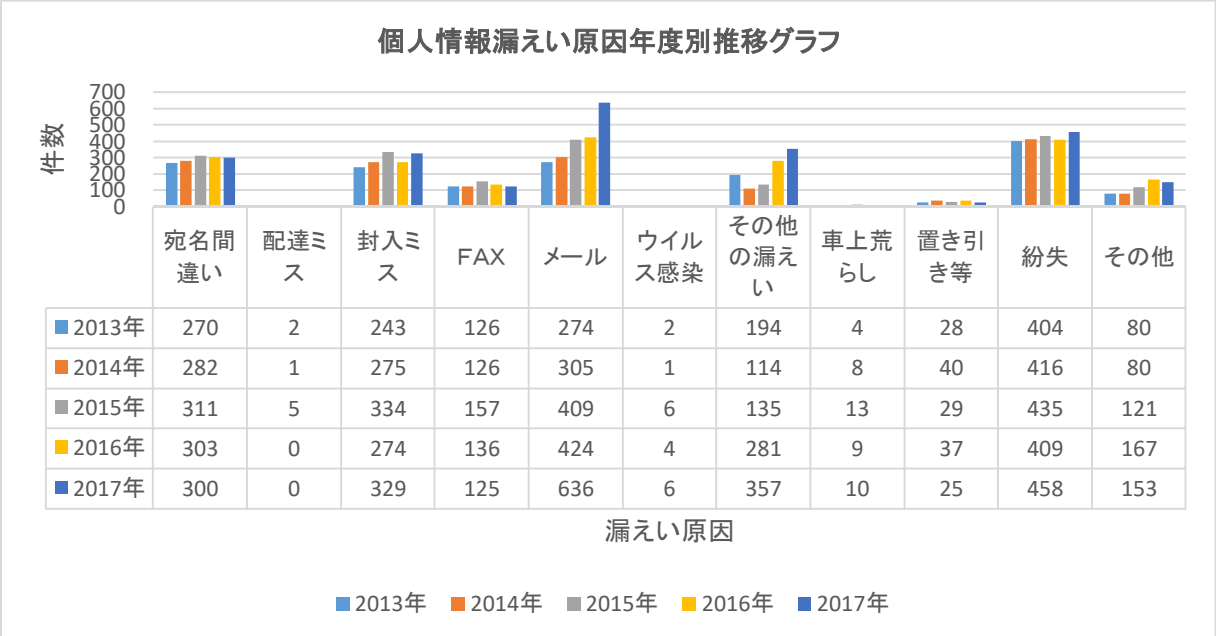
毎年 JIPDEC では、Ｐマーク取得事業者における「個人情報漏えいに係る事故」報告に関する集計結果を公表しています。2017 年度（含む直近 5 年間）の状況は下表の通りです。

（1）Ｐマーク事業者数と個人情報漏えい事故発生件数推移

年度	Ｐマーク取得事業者数（A）	事業者からの個人情報漏洩事故報告			発生割合（A／B）
		報告事業者数	事故報告件数（B）	1 事業者当たり件数	
2013 年	13,591 社	736 社	1,627 件	2.2 件	5.4%
2014 年	14,044 社	768 社	1,646 件	2.1 件	5.5%
2015 年	14,755 社	796 社	1,947 件	2.4 件	5.4%
2016 年	15,297 社	843 社	2,044 件	2.4 件	5.5%
2017 年	15,788 社	911 社	2,399 件	2.6 件	5.8%

2017 年のＰマーク取得事業者における個人情報漏えい事故は、「発生割合」および「1 事業者当たりの報告件数」がともに、ここ数年では最も高くなりました。日頃厳格な個人情報保護に取り組んでいるＰマーク取得事業者でも、年間ベース発生割合では約 20 社に 1 社（5%）が漏えい事故を起こしており、この事実は社会全般の個人情報保護に対する警鐘といえます。

（2）漏えい原因別の年度推移



	宛名間違い	配達ミス	封入ミス	FAX	メール	ウイルス感染	その他の漏えい	車上荒らし	置き引き等	紛失	その他
2013年	270	2	243	126	274	2	194	4	28	404	80
2014年	282	1	275	126	305	1	114	8	40	416	80
2015年	311	5	334	157	409	6	135	13	29	435	121
2016年	303	0	274	136	424	4	281	9	37	409	167
2017年	300	0	329	125	636	6	357	10	25	458	153

上表から、漏えい事故の原因は、「メール（誤送信）」「紛失」「封入ミス」「宛名間違い」が多いことが分かります。特に目につくのが、「メール（誤送信）」の青い棒（2017 年）です。
メールの誤送信が急増した背景には、メール利用がビジネスコミュニケーションの手段として定着化してきたことがあると思われ、利用の拡大に比例して誤送信による漏えい事故が増加したということになります。なお、JIPDEC 資料によればメールの誤送信の内容は、「メール宛先間違い」「ファイルの添付ミス」「BCC と TO/CC の誤り」が 3 大要因になっています。

４．お知らせ

お気づきになられましたか？

今回号から、Pマークニュースの文字のフォントサイズを若干大きくしました。

これは、ある読者の方から「P マークニュースは字が小さ～い！」とのお声を戴いたため、さっそく対応することにしたものです。

Pマークニュースは今回で25号と号を重ねて参りましたが、これからもみなさまに寄り添った形での記事内容や編集方法を目指して行きたいと考えております。

就きましては、P マークニュースに対するご要望やお気づきの点がございましたら、下記にお気軽にご連絡ください。

また、現在、保険代理店様の個人情報保護への取り組みを「代理店様の現場の声」として随時、掲載させて戴いておりますが、個人情報保護、P マーク、情報セキュリティ等々に関するご意見や読者のみなさまにご紹介戴ける事項がございましたら、併せご連絡戴きたくお願い申し上げます。

以上

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）