

Pマークニュース

<2016年爽秋号> Vol. 17

(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. 金融庁の対応はどうか？

— 個人情報保護に関する法律施行規則が公示されました —

2. 近時（直近3年間）Pマークを取得した保険代理店について

3. 「やさしい情報セキュリティ」その8：情報セキュリティが重要な経営課題に

4. マイナンバーこぼれ話、ご存知でしたか？

5. トムソンネットからのお知らせ

1. 金融庁の対応はどうか？

— 個人情報保護に関する法律施行規則が公示されました —

改正個人情報保護法が、法令の整備、ガイドラインの整備を着々とすすめ、2017年春頃(改正法(2015.5.27 法律第57号)の公布から2年以内)に施行されようとしています。

2016.9.30に改正「個人情報保護の法律についてのガイドライン」(第19回個人情報保護委員会以下今回ガイドラインという)が提案され、2016.10.5付で「個人情報保護に関する法律施行規則」が公示されました。

個人情報保護法の10年ぶりの改正であり、内容的に大きく変わっていることから、事業者の対応が注目されます。

とりわけ、今回ガイドラインで別途の規律が必要と考えられるとされた「金融関連(信用等含む)」についての金融庁の対応が注目されます。

また、Pマーク取得事業者は、改訂が必要となりますが、取得しておいて「良かった!!」ということでしょうか。一方未取得事業者は、規制ルールの多さと難しさに茫然でしょうか？

いずれにしても全事業者の遵守すべき法律が改正施行される来春までには、その理解が必須となります。

主な改正点は下記ですが、詳細は順次に今後このニュースで採り上げていくことにします。



(1) 個人情報の定義の追加と関連規定の整備

- ① 「個人識別符号」を個人情報と明記。
- ② 「要配慮個人情報」定義の新設と関連規定の整備
- ③ 「匿名加工情報」定義の新設と関連規定の整備
- ④ 「個人情報取扱い事業者」定義の改正
- ⑤ 「匿名加工情報取扱い事業者」の明記

(2) 利用目的制限の緩和

- ① 「合理的な」関連を有さずとも利用目的の変更可
- ② 市販の電話帳を規制対象外に

(3) 「提供」に関する規定の改訂

① 第三者提供時の確認・記録義務の新設

- ・ 確認・記録の適用対象 適用対象外の明定
- ・ 確認義務 確認方法、複数回にわたる提供の際の確認方法
- ・ 記録義務 記録の作成方法、記録事項(提供者、受領者)、保存期間(1年、3年)

② オプトアウト規定の見直し

③ 提供罪の新設

(4) 匿名加工情報の取扱いについて

① 匿名加工情報の適正な加工

② 匿名加工情報等の安全管理措置

③ 匿名加工情報の作成時・第三者提供時の義務

④ 識別行為の禁止

(5) 開示等請求権の明確化

(6) 個人情報保護委員会の新設とその権限規定の整備

(7) 個人情報の取扱いグローバル化への対応

今回ガイドラインは、全ての分野に共通の汎用的なガイドラインとして、個人情報保護委員会が作成したものであり、「従来の各分野別のガイドラインを一元化したもの」と位置付けています。

ただし、一部の分野(医療関係、金融関係、情報通信関連など)については、「このガイドラインを基礎として、当該分野において必要となる別途の規律を定める。」としています。

現在の金融分野ガイドラインには、いくつかの他のガイドラインにない定めがあります。

例えば、「本人同意の形式は原則として文書による」(「金融分野に関する個人情報保護に関するガイドライン」第4条 2015.7.2 金融庁)としています。今回ガイドラインの本人同意の形式例示にある「口頭による」ことを排除しており、異なっています。この金融分野の特則を今後とも踏襲するか否か、事業者にとっては、実務への影響は「大」です。

また、「個人データ管理責任者は、株式会社組織であれば取締役又は執行役員等の業務執行に責任のあるものでなければならない。」「(「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」2-1 2015.7.2 金融庁)等の実務指針の取扱いも注目されます。

更に、今回ガイドラインでは、安全管理措置については、番号法ガイドラインに準ずるとしており、金融分野事業者は安全管理措置の中小企業特例が認められないことが、改めて明記されたことも注目されます。

改正個人情報保護法では、今までは JIS 規格であったものが、法令として明文化され、具体的に詳細に規定されました。例えば、「要配慮個人情報」として 11 項の定義を解説しており、「提供」については、例外対象の具体的な明示をしつつ、新たに、提供時の確認・記録義務を(申請様式を含め)詳細に定めています。

従って、JIS Q15001:2006 も改訂されることになりませんが、かなり大幅な改訂が予想されます。法令等として、かなり具体的で詳細に規定しているだけに、改訂 JIS への移行には、時間を要すると思われませんが、P マーク取得事業者であっても、かなりの大幅な改訂対応が必要となると考えられます。

P マーク未取得事業者は、大変です。JIS Q 15001:2006 に近い内容の規定も多く、JIS を理解していない事業者が法律として遵守していくには、かなりハードルが高いものとなります。更に保険代理店が金融分野事業者であることを考えると、金融分野の特則の定めへの対応を当局がどうするのか、またその検査や違反への罰則適用にどう対応するのかも注目されるどころです。

2. 近時（直近3年間）Pマークを取得した保険代理店について

弊社では、保険代理店業におけるPマーク取得事業者数推移を、JIPDECの公表資料からフォローしていますが、よくこんな質問を受けます「ところで、どんな保険代理店さんがPマークを取得していますか」といったものです。

この点に関しては、Pマークニュースでもかつて「2013年爽秋号」で採り上げ、Pマークを取得している保険代理店の「地域」、「資本金」、「従業員数」、「兼業・専業の別」、「専属・乗合の別」等を調査し、記事にしていました。

当時(2013年9月)のPマーク取得保険代理店数は93社でしたが、概況は以下の通りです。

- ①地域（事業所の本社所在地）は、東京が57%と他を圧倒し、東京集中の感が強いものでした。
- ②資本金区分では、1,000万円～3,000万円の中堅事業者が38%と多く、1000万円以下は7%でした。
- ③従業員数では100名以上の大型代理店が36%と多く、大型代理店からPマーク取得が進みました。
- ④兼業・専業の別では、専業が73%と兼業を大きく上回っていましたが、兼業がまだ27%もありました。
- ⑤専属・乗合の別では、乗合が68%と増えつつありました。専属の殆どはアフラック専属でした。

そこで、前回（2013年9月）の調査以降の直近約3年間に、新たにPマークを取得した保険代理店（49社）の傾向を追ってみました。

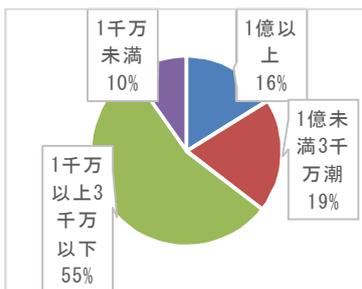
- ①地域性については、相変わらず**東京中心（51%）**と言えますが、これまでPマーク取得保険代理店が存在しなかった、宮城県、長野県、新潟県、和歌山県の各県でPマーク取得代理店が出現して、**全国各地への拡大傾向**がみられます。
- ②資本金区分については、前回の調査と同傾向で、**1,000万円～3,000万円の事業者が35%**と最も多く、1,000万円未満は3件（6%）になっています。
- ③従業員数をHP上で公表している事業者は、49社中20社に留まっているため、状況を断言することは難しいのですが、従業員数が100名以上の事業者が20社中12社（60%）と**大型代理店中心**の傾向です。
- ④兼業・専業の別についてみると、**専業が88%**を占めて、前回調査時の73%より、一層保険代理店の専業化が進んでいることが窺えます。
- ⑤専属・乗合の別では、78%が乗合でしたが、アフラックの専属代理店が10社（20%）と健闘しています。但し、昨年（2015年）の3月以降、アフラックの専属代理店で新たにPマークを取得した保険代理店はありません。

また、乗合で特筆されるのは、生保の乗合で半数以上が10社以上の生命保険会社との乗合になっており、**来店型の店舗を構えている事業者**でのPマーク取得が増えています。

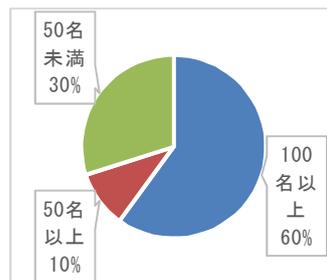
- ⑥さらに今回は、会社設立時期（昭和以前／平成1ケタ／平成10～19年／平成20年以降）との関係も調べてみました。

結果、平成10年以降設立の**新しい保険代理店が63%**（平成10～19年：16社／平成20年以降：15社）と多数を占めました。

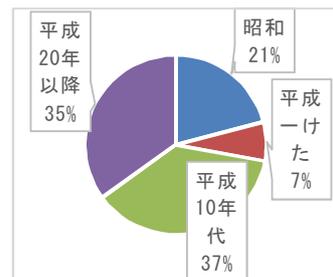
規模別割合（資本金）



規模別割合（従業員数）



設立時期別割合



3. 「やさしい情報セキュリティ」その8：情報セキュリティが重要な経営課題に

大手企業やセキュリティ分野の企業が会員に名を連ねる NPO 法人日本ネットワークセキュリティ協会（以下、JNSA）が毎年作成している「情報セキュリティインシデントに関する調査報告書」の2015年版が6月に公表されました。それによれば、2015年の情報漏えいによる想定損害賠償額が2,541億円になったそうです。同年のインシデント（事故）は799件としており、1件当たりの平均損害賠償額は約3億2千万円に上ります。

米国では情報セキュリティ強化を怠ったことで株主訴訟の対象になるケースが出ています。情報セキュリティが重要な「経営問題」ないしは「経営課題」となって来ました。

(1) 社内で誰が“被害者”になり易いか

興味深いデータがあります。情報セキュリティ分野の老舗であるNRIセキュアテクノロジーズ（株）が発表した調査レポート「サイバーセキュリティ傾向分析レポート 2015」に、開いてはいけない標的型攻撃メールを実験として送信した際の開封率を調査した結果、役員の開封率が従業員の約1.6倍だった旨が記述されています。

従業員では約20%だったのに対し、役員では約30%にもなり、上のクラスの人ほど改善の余地が大きくあると警告を発しています。年代との相関関係の可能性もあります。

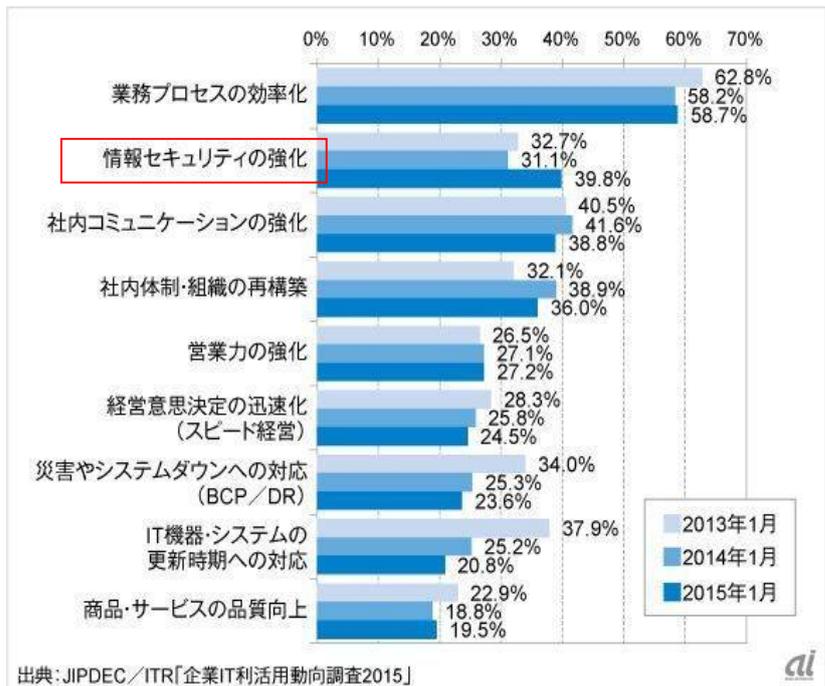
また、各社にはそそっかしい性格の社員が必ず存在し、インシデントを繰り返し起こす傾向があります。繰り返し注意を喚起したいものです。

(2) なぜ“無防備”なのか

昨年(2015年)社会的な大問題になった日本年金機構の100万人以上の個人情報漏えい事件について、各種の報告書が出されていますが、そもそものキッカケは“まさか自分たちの組織が攻撃されるとは”との意識があったとされています。前回(第7回)で述べた調査では34.8%の人が“自分の会社が攻撃されるとは思っていない”と答えています。今や、全ての企業が攻撃に晒されていると考えないといけない時代です。決して大企業や著名な機関だけが攻撃者のターゲットになるとは限らなくなっています。最終ターゲットに到達する前に、取引先の担当者のメールアドレスを不正に入手しようとする手口があります。

(3) IoT (Internet of Things (モノのインターネット)) 時代に向けて

クルマのカーナビに代表されるように、家電品・事務機器等、所謂コンピュータ以外の製品がネットに繋がる時代になりました。それは即ち、サイバー（インターネットを使った）攻撃の対象となることを意味します。情報セキュリティをIT部門に任せっぱなしではいられません。IoT時代において



は、情報漏えいと共に業務の停止による被害額も問題になりそうです。

東京海上日動火災保険(株)では「サイバーリスク保険」を用意しています。

単に損害賠償金のみならず、お詫び状作成・送付費用やアフターケアのためのコールセンター委託費用等も含んでおり、情報（特に個人情報）漏えいが起こるといかに多様な対応が求められるかが垣間見えます。

(4) 損害賠償額はいくらに

前述のJNSAは「2003年度情報セキュリティインシデントに関する調査報告書」の中で、個人情報の想定“損害賠償額”の算出式（J0モデル）を公表しています。IPA（(独法)情報処理推進機構）でもモデルを出していますが、こちらは想定“被害額”です。

J0モデルでは基礎情報価値500円をベースとし、機微情報度や本人特定容易度、情報漏えい元組織の社会責任度、事後対応評価の要素を掛け算して賠償額を求めます。一度算出してみたいかでしょうか。

(5) “自主点検と報告”の重要性について

インシデントをゼロにすることはできませんが、人的・組織的な対策を講ずることにより被害を極小化できる余地があります。日本年金機構の件も、組織的にすぐに対応を取っていれば、被害が極く小さなもので済んだはずですが。監視を委託している専門機関から警告が通報されていたにも拘わらず、然るべき職制に報告が上がらなかったことから甚大な被害になりました。“不適合”“ヒヤリハット”があった場合にはすぐに報告を上げる風土が重要です。

有名なトヨタ生産方式の「あんどん」では、点けた当人を叱責することはありません。“原因と対策”の方にチームの智恵と労力を結集することにより、品質において世界に確たる地位を築いています。

プライバシーマーク付与事業者においては、監査や代表者による見直し等が義務付けられていますが、“効果のある”自主点検（運用の確認）をより重視するようになってきました。発表時期から80年以上経ったハインリッヒの「1:29:300の法則」は未だに説得力を持っています。体制として「CSIRT」を編成し、重大なインシデントに対応することも考えなくてはなりません。

中央官庁から、“有効な自主点検の運用に関する提案”を求められることが目立って来ました。監査（通常年1回）よりも回数を多く手間をさほど掛けず、つまり自主的な点検を行いたい、が趣旨です。自己申告ではありますが、そのチェックリストに目を通すことによるリマインド（念押しのための確認）と報告の習慣化効果は確実に期待できます。

4. マイナンバーこぼれ話、ご存知でしたか？

早いもので、昨年マイナンバーの通知カードの交付から既に1年以上が経過しようとしています。そこで、マイナンバーに纏わるちょっと興味のある話題を拾ってみました。

(1) 2016年度上半期、マイナンバー漏洩事故は66件 - 「重大事態」2件

個人情報保護委員会が、2016年4月から9月までの2016年度上半期に関する活動状況を取りまとめ、マイナンバー漏えい事故等についての状況を発表しています。

特定個人情報の漏洩や紛失といった事故は、同期間中に49機関から66件の報告を受け、そのうち2件は「重大な事態」だったということです。

66件の内訳を見ると、行政機関が2機関より3件、地方公共団体が30機関で37件、民間事業者が17機関で26件でした。また立入検査の実施件数は4件で、マイナンバー法違反のおそれがあるとして5件に対して文書による指導を実施しています。

また66件のうち、2件に関しては紛失した特定個人情報100人を超えており、委員会規則が定める「重大な事態」に当たります。

①従業員約400人分のマイナンバーが記載された扶養控除等申告書を郵便局へ運ぶ途中、車両の窓ガラスを割られ持ち去られた。

②再委託先の担当者が情報システムに記録されていた特定個人情報含む従業員情報約400人分を、誤って削除した。

また、同期間中にマイナンバー苦情あつせん相談窓口が受け付けた苦情や相談は545件ありました。内容を見ると、「提供の求め、本人確認」に関するものが202件と最も多く、次いで「管理体制」が121件で、「漏洩、紛失など」が64件で続き、「通知カード、マイナンバーカードの取扱い(39件)」「個人情報保護法(34件)」といった相談も寄せられています。

(2) 個人番号法違反として摘発されたのはこんな事件

今年3月に、マイナンバー法違反で全国初の逮捕がありました。事件の内容は、

- ☞ 香川県高松市在住の男性会社員をマイナンバー法違反の容疑で逮捕
- ☞ 勤務先のパート従業員に好意を寄せ、自宅に侵入してマイナンバーを撮影
- ☞ 住居侵入罪の容疑で逮捕されていたところ、マイナンバー法違反で追送検

住居侵入罪の容疑で逮捕されていたところ、スマートフォンを調べたらマイナンバーの写真が出てきたことからマイナンバー法違反で追送検されたという経緯です。

今回逮捕の理由となったマイナンバー法違反は、マイナンバーの不正取得行為を理由とするものです。暴行、脅迫、不正侵入などの違法な行為によってマイナンバーを不正に取得した場合には、3年以下の懲役、または、150万円以下の罰金という刑事罰となります。

マイナンバー法の条文には次のように定められています。

マイナンバー法 51 条 1 項…人を欺き、人に暴行を加え、若しくは人を脅迫する行為により、又は財物の窃取、施設への侵入、不正アクセス行為その他の個人番号を保有する者の管理を害する行為により、個人番号を取得した者は、3年以下の懲役又は150万円以下の罰金に処する。

マイナンバー法は、個人情報保護法の特別法として制定されており、マイナンバーを個人情報の中でも特に保護すべきものとして厳重な定めを規定しています。そのため、マイナンバーを流出させたり、不正取得したりした行為に対しては、厳しい刑事罰が科されていますので、注意が必要です。

(3) 個人番号カードの発行はまだ全体の1割にも達していません

総務省によるとマイナンバーカードの申請件数は、10月の上旬時点では1,143万件で、内850万件がカード交付済みとのことです。これは日本の人口に占める申請率は約9%に当たり、まだ10人に一人しか申請していないこととなります。

マイポータル制度など個人番号カードを使った各種サービスの拡充が、来年(平成29年)にはいろいろ予定されています。まだカード申請をなさっていない方は、そろそろ申請をご検討ください。

5. トムソンネットからのお知らせ

弊社のホームページが以下のように見易くリニューアルされました。

The screenshot shows the TMSN.net website homepage. At the top, there is a navigation bar with links for Home, Seminars, Consulting Support, Publications, Consultant Introduction, Company Information, and Personal Information Protection. A main message box states that TMSN.net is a collection of experts with years of experience in insurance business, offering original seminars and consulting to support clients. Below this, there are sections for 'Introduction of Company Services' (divided into Seminars, Consulting/Support, and Publications), 'Business Concepts', 'Consultants', and 'Public Lectures' (with a list of dates for seminars and P-mark news).

(1) **コンサルタント紹介**では、現役時代にそれぞれの会社で**保険業務を経験した30余名のメンバー**を紹介しています。

みな様からの各種ご相談をお待ちしておりますので、お気軽に声をお掛け下さい。

(2) 弊社が定時開催している**損保／生保の公開講座**の**内容や日程**を分かり易く掲載しております。

是非とも、新入社員の研修や中堅社員のスキルアップにご活用ください。

(3) **Pマークニュース欄**からは、**バックナンバー**も参照出来ますので、ご利用ください。

Pマークについてのご相談は下記で承っています。お気軽にどうぞ！

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