Ｐマークニュース

＜２０２０年盛夏号＞　Vol. ３２

株式会社トムソンネット　Ｐマークコンサルティンググループ

目 次 と 記 事 概 要

以上

１．2020 個人情報保護法が改正されました
－「個人の権利利益の保護」と利活用のバランス－

3 年ごと見直しの個人情報保護法が 2020.6.5 に成立し、6.12 公布されました。「個人の権利拡大」「データの利活用」「法執行の強化」などについて、改正し、2022 年春に施行するとしています。

これに伴う P マーク審査基準の改定がいつになるか現在公表はありませんが、2015 年改正では、法改正に基づき JISQ15001、P マークの審査基準が改訂され、改正 JIS による審査は 2018 年 8 月からとなっています。過去の経過から類推すれば 3 年後の審査基準改定が見込まれます。

（1）法改正のポイント

「個人の権利拡大」に関しては、「個人の権利または正当な利益が害される恐れがある場合には、データの利用停止を企業に求める権利の拡大」「クッキーなど個人と照合して使うデータの提供時の本人の同意の義務化」などが法定されました。

「データの利活用」では、「仮名加工情報」の制度を導入しています。事業者が、各店舗から顧客の年齢や性別、来店時間帯などの情報を集め、社内で分析して、売れ筋商品のリサーチ・開発に活かす等の使い方が想定され、「匿名加工情報」より事業者にとって利活用しやすい規定が導入されました。

「法執行の強化」では、「一定以上の個人情報漏洩の報告義務化」「法人への罰金上限を 1 億円に引き上げ」などが法定されました。

	項目	内容
1	**「保有個人データ」範囲の拡大**	**「保有個人データ」の「６か月保持」の条件を廃止する。(改正法案２条７項)**
2	**利用停止・消去権**	**利用停止・消去等の個人の請求権**について、不正取得等の一部の法違反の場合に加えて、**個人の権利または正当な利益が害される恐れがある場合にも認める。(改正法案３０条)**
3	**「仮名化情報」の創設**	他の情報と照合しなければ特定の個人を識別することができないように加工された個人情報の類型として「仮名化情報」を導入する。(改正法案２条９項) ・個人識別符号は全て削除すること。 ・組織内で利用するもので第三者提供は行えない。 ・開示請求に応える必要はない。 ・利用目的の特定と公表が必要である。
4	**「クッキーID 等」情報(「個人関連情報」)の提供制限**	生存する個人に関する情報であって、個人情報、仮名加工情報及び匿名加工情報のいずれにも該当しないもの(クッキーID 等)を**「個人関連情報」という。**(改正法案２６条２項の 1) ・第三者が**「個人関連情報」を個人データとして取得することが想定される時は、当該本人の同意なく提供してはならない。**

	項目	内容
5	**漏えい等報告及び本人通知の義務化**	一定数以上の個人データ漏えい等、一定の類型に該当する場合、速やかに個人情報保護委員会への報告と本人への通知を行うことを個人情報取扱事業者に義務付ける。 (改正法案２２条２項) ・報告先を個人情報保護委員会・権限委任官庁とし、認定個人情報保護団体を不可とする。
6	**ペナルティの強化**	・委員会の命令違反 6 か月以下の懲役又は 30 万円以下の罰金 **⇒　一年以下の懲役又は 100 万円以下の罰金(83 条)** ・個人情報データベースなど不正提供 一年以下の懲役または 50 万円以下の罰金(84 条) ・虚偽の報告・資料提出、立入検査拒否の違反 30 万円以下の罰金⇒**50 万円以下の罰金(８５条)** ・83 条から 85 条の違反行為については、行為者を罰するほか、その法人に対しても罰金刑を科する(**両罰規定であるが法人重科**) ⇒　法人に対する罰金を 83 条・84 条では **1 億円以下に**、85 条は 50 万円以下(行為者と同額)に

（2）改正個人情報保護法が事業者に与える影響

「保有個人データ」範囲の拡大、利用停止・消去の請求権、「仮名化情報」の創設、「クッキーID 等」情報(「個人関連情報」)の提供制限、いずれも、ほとんどの事業者に関係しない事項に映るかもしれません。しかしながら、それは大きな見誤りです。

個人データを利活用し、デジタル化による企業活動をすすめている企業は、「仮名化情報」「クッキーID 等」情報(「個人関連情報」)を利用し、多くのメリットを享受している現実があり、そのルール作りが必要になったのです。更に、個人データの利活用の高度化に伴って、個人の権利が脅かされている現実があり、そのルール作りも必要になっているとみるべきです。「当社は今回の改正には関係ない」と思っている事業者は時代の流れに遅れをとっています。目を覚ましてください。

具体的な事例は、2021 年に、政令、個人情報委員会規則、ガイドラインとして公布されることになっています。こうした具体的な事例を参照して、［目覚めていない］事業者が「個人データの利活用の高度化」に追いつくチャレンジ期間があるとも考えます。各項目についての詳細は、次回以降の P マークニュースでご紹介していきます。

更に注目したいのは、「漏えい等報告及び本人通知の義務化」「ペナルティの強化」です。従来ともすれば、個人情報保護法の罰則は、「あって無きよう」で、罰金適用の事例も多くなかったのですが、2019 年の「リクナビ内定辞退率分析事件」の発生を契機に、個人情報保護委員会の機能を強化し、法違反の行為者でなく法人に対して重科することに改正されたのです。

JIS 規格は個人情報保護法より厳しく規定されてきましたが、2020 個人情報保護法の改正では、全ての事業者が、従来の JIS 規格にない基準をクリアすることが求められています。そして、その遵守は事業者の義務であり、その違反には、行為者でなく**事業者に厳しい罰則**が規定されたのです。法改正はされましたが、事業活動の中で、何をどうしていけばよいのか? その**実践策の基本**が PMS の運用なのでしょうか。

２．事例に学ぶ：無線 LAN・Wi-Fi に伴うリスク対策

事例シリーズの第 9 弾になります。本稿では、目下のところ自宅作業（テレワーク）を強いられている方を念頭に置き、「無線 LAN（Wi-Fi)」について述べてみたいと思います。

2015～16 年に佐賀県で、17 才の少年が学校の傍に受信機を運んで校内無線 LAN の弱点につけ込み、約 15 万件の個人情報を持ち出しました。日本の公教育分野では過去最大規模の情報漏洩事件となっています。本シリーズでも、「やさしい情報セキュリティ」の「その 10：ルータの脆弱性について」と題して筆を執り、要注意点をご紹介しました。今回新たな観点を盛り込んでいるものの、内容が一部重複するかもしれませんがご容赦ください。

この度のテレワーク指向は、コロナ禍で降って湧いたように持ち上がったため、整備すべき事項を十分確認する前に実行に移った会社も多いのではないでしょうか。

その中で目に付きにくい自宅環境内の無線 LAN ルータ(Wi-Fi ルータ)に関する点検・確認を提案させていただこうと思います。

※〝無線 LAN〟は、電波を使って機器間の通信を行う LAN の通称で、各種の規格があります。片や〝Wi-Fi〟は無線 LAN の一種で、規格の一つ「IEEE 802.11」を基に業界団体「Wi-Fi Alliance」が定めた製品認証プログラム及びその仕様を指しますが、現在では実質的に〝無線 LAN〟と同義に使われています。

（１）無線 LAN を安全に使うために

①2 種類の〝パスワード〟

無線 LAN ルータの背面または底面を表にすると、右のような情報が印刷されたり刻印されているのを目にすることでしょう。パスワードと思しきものが 2 箇所あります。いずれも出荷される時点でメーカが初期設定しています。

一つは「Key」で、他方は「パスワード」です。

前者は、〝ユーザ〟の立場でルータを利用する際、PC やスマホなどから接続要求をするために入力する情報です。後者はルータの設定を変更する際に〝管理者〟としてログインするための情報です。いずれも重要情報に違いはありませんが、万一破られたときに被害規模が大きくなるのは後者の方です。盗まれた際にはルータの設定を改竄されて本来と異なるサイトに接続されたり、入力した口座情報を傍受されるなどの事案に発展します。

問題はルータのメーカや機種によって同じ「ユーザー名」と「パスワード」が初期設定されていることです（例えば、〝admin と password〟や〝root と空白〟など)。ユーザー名は変更できませんが、**パスワードはすぐにも変更するべき**です。

手順は、PC またはスマホでブラウザを起動させ、URL の領域に IP Address （この場合 192.168.11.1。その前に〝http:〟などが必要の場合もあり)を入力して Enter を押下するとルータの認証画面が表示され、件のユーザー名とパスワードを入れれば管理者モードでログインできます。後はメニューに従ってパスワードを変更します。

② 暗号化の強度

右の写真は、au(KDDI)が無料配布していた「HOME SPOT CUBE」の底面です。

SSID(アクセスポイント(＝アンテナ)の名前)を 3 種類持っていることが分かります。説明書にも書かれていますが、下 1 桁の文字で暗号化のレベルが示されています。SSID3 の〝A〟は WPA2 方式、SSID2 の〝W〟は WEP 方式です。

SSID1 には書かれていませんが WPA2 の旨が説明書にあります。SSID1 と SSID3 の違いは 2.4G

と 5G の周波数の違いです。ここで〝5G〟と知って「我がルータは 5G(ファイブジー)ができるんだ」と喜んではいけません。ルータの 5G は後ろに〝Hz〟が隠れています。
重要なことは、**WPA2 方式が適用できる機器に WEP 方式を選んではいけない**と言うことです。当今のルータは WPA2 方式一辺倒で、WEP は最早や装備されていないと思いますが、上図のように数年前まで市販されていたものには旧型機との互換性維持のため付加されていました。

③ファームウェアの更新

WEP 方式は、受信機と特別のソフトを使うと数分で暗号鍵が判明することが分かっているのに対して、WPA2 は非常に強力との定評がありましたが、2017 年に「KRACK」と言われる脆弱性が発覚し世界を震撼させました。
無線 LAN ルータにはファームウェア(電子機器に組み込まれたハードウェアを制御するためのソフトウェア)が格納されており、典型的な「IoT 機器」です。KRACK の件を受けて、メーカはいち早く**ファームウェアの更新バージョン**をリリースしています。
ルータの管理者画面でファームウェアの更新履歴を確認できます。最新の更新が 2017 年以降になっていたら一安心と言ったところですが、アップデートの所要時間は数分程度でしょうから、KRACK 対応に限らず最新版にすることをお勧めします。

（2）電波の届く範囲

無線 LAN の電波は障害物がない限り 50～100m の範囲で受信可能とされています。屋内では壁や家具などのため 10m 程度でも不安定になるケースもありますが、佐賀県の事案のように屋外に漏れた電波は、見通しのきく場所であれば少々離れていても盗聴(傍受)できることを心に留めておきたく思います。もし無防備(暗号化なしの平文)で ID・パスワードや口座・暗証番号を無線で飛ばしたことを想定してみていただければ、空恐ろしさが想像できるでしょう。
基本的に無線データはハガキに喩えられます。場所などの条件が揃えば誰にでも見られてしまいます。ハガキの場合はプライバシー保護のシールを貼ったりして情報を目隠しします。或いは封書を利用します。電子データの場合はそれが暗号化になります。

（3）ついでながら

テレワークに付き物なのがメールのやり取りです。ファイルの添付も頻繁に発生していると思われ、zip 形式に圧縮しつつパスワードを付与するのが最も一般的です。所が zip 暗号鍵は定番ソフトの「Lhaplus」で解読できます。Word や Excel ファイルにパスワードを設定する方が安全ですが、zip をお使いの場合は鍵を〝英数字の混合で 10 桁以上〟にして暗号解読の時間を長引かせることを心掛けていただきたく思います。
zip 以外では「アタッシェケース」が高い評価を得ていますが、受信側にも当該のソフトをインストールする必要があります。推奨したいのは外部ストレージを使う方法です。無料サービスも多数ありますが、Google ドライブや OneDrive、Dropbox などは月額料金がコーヒー一杯程度の料金で安心して利用できます。送信者は見て欲しいファイルを収納したフォルダに受信者を〝招待〟することでファイルを届ける(見てもらう)ことができます。

（4）終わりに

情報セキュリティに対する脅威は留まるところを知らない状況にあります。折からの状況下にあってやむにやまれず実施したテレワークで、標的型攻撃の踏み台にされたり、自宅環境の脆弱さが故に会社が責任を取らされる可能性も否定できません。私的な環境とは言え外部、特に取引先に被害を及ぼした際には最悪のことまで考えるべきです。
本稿には部分的に技術的なものも含んでいるとは思いますが、社内で分かる人の支援を以てテレワーク環境の強化を図っていただければ幸いです。

３．Ｐマーク取得の保険代理店について調べました

日本情報経済社会推進協会（DIPDEC）が公表しているＰマーク取得事業者検索によれば、2020年７月末時点で、業種の中分類「保険業」でヒットする事業者は138社あります。

この 138 社の中には、保険の鑑定業務等を行っている事業者も含まれるため、138 社をさらに振り分け保険代理店業に限りますと 116 社が該当します。

今回は、この 116 社の保険代理店について、各社がネット上で公開している企業情報等からその特性等を調べてみました。

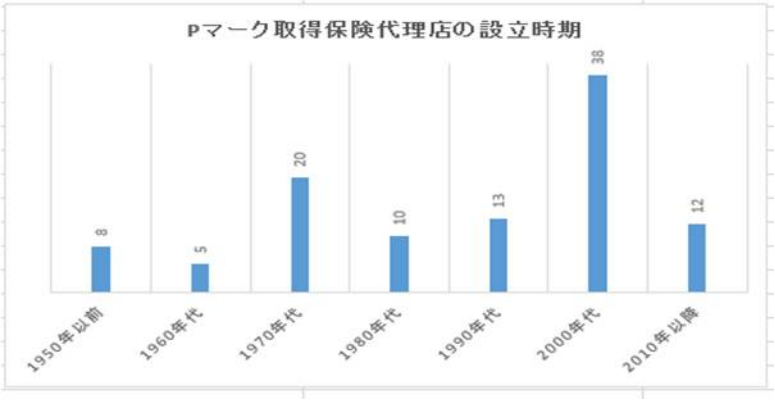
（１）企業属性について

①Ｐマーク取得代理店の本店所在地

順位	所在地	代理店数	順位	所在地	代理店数	順位	所在地	代理店数
1	東京都	６０	7	千葉県	3	12	茨城県	1
2	大阪府	１４	7	新潟県	3	12	岐阜県	1
3	神奈川県	6	7	大分県	3	12	和歌山県	1
3	福岡県	6	10	長野県	2	12	奈良県	1
5	愛知県	5	10	京都府	2	12	島根県	1
5	兵庫県	5	12	宮城県	1	12	香川県」	1

Ｐマーク取得事業者は18都道府県に分布しており、東京に60事業者52%と集中しています。また、上位６都府県の合計は96事業者と83%を占め、Ｐマークの取得が大都市中心であることが窺えます。その一方ではＰマーク取得保険代理店がまだ１社もない道県が「29」と６割を超え存在しており、Ｐマークの取得が全国レベルで浸透していないのは残念です。

②設立時期（116 社中 106 社が設立時期を公表しています）

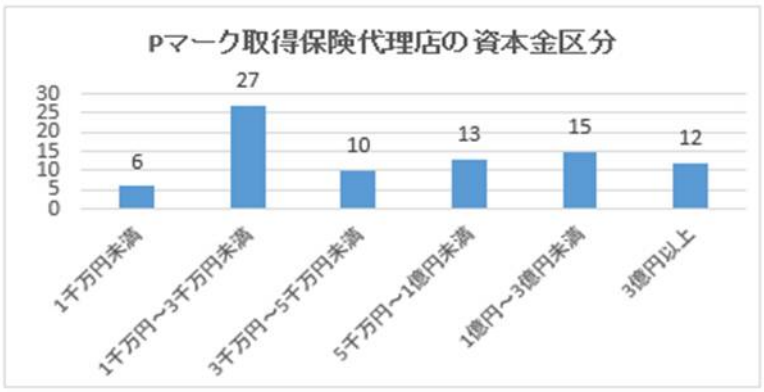


設立時期を 10 年毎に区切って、設立時期の分布をグラフにしました。

一番多かったのは 2000 年（平成 12 年）～2009 年に設立された保険代理店で 38 社を数えます。

また、設立後まだ 10 年に満たないような若い保険代理店で、既に 12 社が Ｐ マークを取得しているのが注目されます。

③資本金（116 社中 83 社が資本金を公表しています）



資本金のレベルで見ますと資本金が１千万円～3 千万円未満の規模の保険代理店における Ｐ マーク取得が 27 社あります。

資本金１億円以上の保険代理店においては、兼業（不動産業等）代理店の割合が多くなっています。

④従業員数

ホームページの企業概要に社員数を公表しているＰマーク保険代理店は、54 社と全体の半分以下に留まっていますが、従業員数を公表している保険代理店業を営む事業者の社員数の分布を示すと下表の通りとなります。

社員数公表の 54 社のうち 24 社（44%）が、社員数 50 名未満の保険代理店です。

この従業員数でも明らかな通り、保険代理店における P マークの取得は、資本金や従業員数といった要素よりも、代理店経営者のガバナンス意識等の反映によることが窺えます。

社員数区分	事業者数	社員数区分	事業者数	社員数区分	事業者数
300 名以上	12	100 名～299 名	12	50 名～99 名	6
30 名～49 名	10	10 名～29 名	12	10 名未満	2

（２）事業形態について

①専業／兼業割合について

Ｐマーク取得事業者の中には、保険代理店事業を営むと同時に他の事業も営むという、所謂兼業代理店も多くあります。今回の調査対象となった 116 社については、専業 76 社（66%）／兼業 40 社(34%)でした。

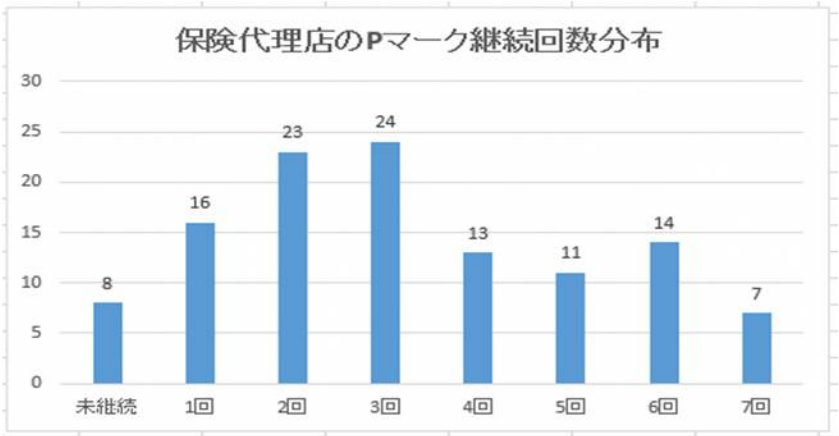
兼業の場合の保険代理店業以外の業務としては、不動産管理業／経営コンサルティング業／財務・金融コンサルティング業／IT 関連等が挙がっています。

②専属代理店／乗合代理店区分について

ホームページ上では取扱い保険会社を公表していない会社も一部あったため、振り分けが可能となったのは 91 社でした。結果は専属代理店 13 社（14%）、乗合代理店 78 社（86%）でした。専属代理店の 13 社はいずれも AFLAC の来店型代理店です。

また、乗合代理店は、その大半が生損保双方について複数社との乗合形態を採っています。

（３）Ｐマーク継続更新について



Ｐマークの更新回数から、当該保険代理店がいつ頃Ｐマークを取得し、継続しているかが、分かります。Ｐ マークの更新審査は 2 年毎に行われますので、「未継続」の区分の会社は、まだＰマークを取得して 2 年が経過していない保険代理店です。

グラフからは継続回数が 2 回、3 回（4～5 年前にＰマークを取得）という保険代理店が多いのが分かります。

その一方で未継続、や継続回数１回の代理店が少ないことは、最近、保険代理店のＰマーク取得が伸び悩んでいることを反映しています。

４．お知らせ（トピックス）

（１）弊社の教育研修（損保公開講座／生保公開講座）は、８月より再開しております。

新型コロナウイルス感染症の影響により、一時実施を見合わせておりました前述の教育研修は８月より従来通り参加者を募集しております。

なお、ZOOM によるオンライン研修も可能ですので、弊社ホームページよりお申し込みください。

以上

Ｐマークをはじめとして各種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　（https://www.tmsn.net/）
〒101-0062 東京都千代田区神田駿河台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）