Ｐマークニュース

＜２０２０年爽秋号＞　Vol. ３３

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

改正個人情報保護法(2020.6.12 公布)の施行については、その多くの改正条文の施行が「公布の日から起算して 2 年を超えない範囲内において政令で定める日」とされており、2022 年春と想定されていますが、法定刑については、2020.12.12 から引き上げとすることが、個人情報保護委員会から公表(2020.10.01 付)されました。その概要と関連する「漏えい等報告・本人通知の義務化」に関する改正法案を概観します。2020 年改正法の最初の施行規定は、法令順守の徹底であり、そのためには個人情報保護の基本ルールの従業者への教育・研修が重要になります。

ゼロトラストとは、「何も信頼せず常に検査する」とのコンセプトの元で情報セキュリティを保つ考え方で、2010 年に米国の調査会社に所属するエンジニアが提唱したものです。最近の情報セキュリティにおけるログチェックの再評価と重視等をゼロトラストに絡めて説明しています。
働き方改革で話題になったテレワークやリモート(サテライト)勤務が新型コロナウィルスによって一挙に常態化しようとしています。それに伴う情報セキュリティに関しては、ゼロトラスト的発想で、今まで採られていた個別の対策を連携させて複合的な観点で見直す好機でもあります

Ｐマーク制度が始まって以来約 20 年、この間Ｐマーク取得事業者数は、ここ 10 年ほどは毎年 500 社前後順調に増え続けて来ました。それが、2020/10 に前月比マイナスという恐らく初めての異常事態に陥ったのです。

Ｐマーク取得事業者数の伸び悩みは、新 JIS 対応への遅れや新型コロナ感染による一時的なものと考えがちですが、他の要因も懸念されます。この機会に、Ｐマーク制度の見直しを含め、今後我が国における個人情報保護の中心的制度として、国家的観点からもＰマーク取得事業者を拡大させることの必要性を説いています。

以上

１．改正個人情報保護法罰則の引き上げ施行は 2020.12.12 から

改正個人情報保護法(2020.6.12 公布)の施行については、その多くの改正条文の施行が「公布の日から起算して 2 年を超えない範囲内において政令で定める日」とされており、2022 年春と想定されていますが、**法定刑については、2020.12.12 から引き上げ**とすることが、個人情報保護委員会から公表(2020.10.01 付)されました。その概要と関連する**「漏えい等報告・本人通知の義務化」**に関する改正法案を概観します。

（１）改正され施行される法定刑について

2020 年 12 月 12 日から個人情報の保護に関する法律（個人情報保護法）の法定刑が下記のように引上げとなります。なお、施行日以前の行為に対する罰則の適用については、改正前の個人情報保護法の規定が適用されます。主な変更点は下記です。

・委員会による命令違反・委員会に対する虚偽報告等の法定刑を引き上げる。
・命令違反等の罰金について、法人に対しては行為者よりも罰金刑の最高額を引き上げる（法人重科）。

改正前後の法定刑の比較は下記です。

懲罰事由区分		懲役刑		罰金刑	
		改正前	改正後	改正前	改正後
個人情報保護委員会からの命令への違反（法 84 条）	行為者	6 か月以下	1 年以下	30 万円以下	100 万円以下
	法人等	―	―	30 万円以下	1 億円以下
個人情報データベース等の不正提供など（いわゆる「個人情報データベースなど不正提供罪」 法 83 条）	行為者	1 年以下	1 年以下	50 万円以下	50 万円以下
	法人等	―	―	50 万円以下	1 億円以下
個人情報保護委員会への虚偽報告（法 85 条）	行為者	―	―	30 万円以下	50 万円以下
	法人等	―	―	30 万円以下	50 万円以下

（個人情報保護委員会資料から）

（２）適用される事案

対象となる事案は「個人情報保護委員会からの命令への違反」ですが、その適用は**「非直罰制」**で、委員会から「勧告」があり**「勧告に従わない」**時(法 43 条－2 項)、あるいは**「緊急に措置をとる必要がある**と認められ、**当該違反行為の中止その他違反を是正するために必要な措置を取る時」**(法 43 条－3 項）です。このように、**非常に要件が厳格で罰則の適用は難しいものとなっており、刑事罰は謙抑的システムとなっています。**

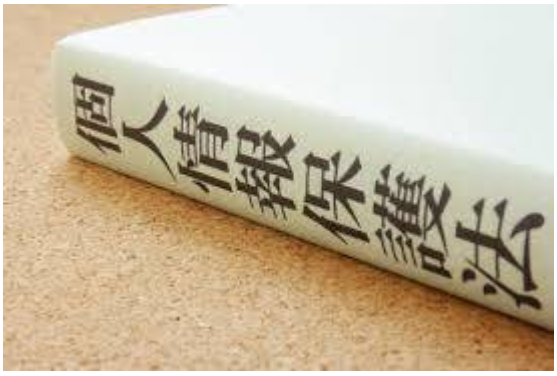
命令への違反に該当するのは、次の項目の違反です。

個人情報保護の基本ルールである事業者の**安全管理措置、 従業者の監督、 委託先の監督**であり、**個人情報の取扱を規定した次の各項目**です。即ち、利用目的による制限、 適正取得、要配慮個人情報の取得、利用目的の通知又は公表、直接書面等による取得、第三者提供の制限の原則、オプトアウトによる第三者提供、第三者提供に係る記録の作成等、第三者提供を受ける際の確認等、保有個人データの開示等、匿名加工情報の作成・第三者提供・識別行為の禁止を規定した各条文の違反についてです。

とりわけ緊急に措置を必要とする項目に、次の各条文の違反をあげています。**安全管理措置、従業者の監督、委託先の監督、利用目的による制限、適正取得、第三者提供の制限の原則、外国にある第三者への提供の制限、匿名加工情報取扱事業者等の義務です**。

この法定刑の引き上げは、2020.12.12 からの施行であり、現行法の各条文も、2022 年春に施行予定の 2020 年改正個人情報保護法で新たに規定される条文も適用されることになります。2022 年施行の改正条文の詳細は、2021.1 から 2021.2 に公表される政令・規則・ガイドラインで明らかになり、現在は具体的にどのような行為が命令違反あるいは緊急措置対象の違反是正対象になるかは不明です。

例えば**クッキー情報などの「提供先において個人データとなる情報の取扱い」**について「提供元では個人データに該当しないものの、提供先において個人データとなることが想定される情報の第三者提供について、**本人同意がが得られていること等の確認**を義務付ける」としていますが、その第三者提供を行う際の確認や記録作成の方法等については今後「委員会規則」で定めることとしています。あるいは**「不適正な方法による利用の禁止」**について「違法又は不当な行為を助長する等の不適正な方法により個人情報を利用してはならない旨を明確化する」としていますが、



「特に、違法又は不当な行為を助長し、又は誘発するおそれがある方法」についても今後「ガイドライン・Q&A」で定めることとしています。

（3）法人への重科の経過・背景

法人への罰則規定を現行「50 万円以下」から「１億円以下」に引き上げている。制度改正大綱(2019. 11. 29)によれば、「経済界からは、事業者は個人情報保護法を遵守しており、ペナルティの引上げに慎重であるべきとの意見が多くありました。しかし、委員会が漏えい等報告を受けた事案や報告徴収・立入検査を行った事案の数は増加傾向にあり、本年８月、委員会が勧告を行った重大な違反事例事件の発生したことを踏まえて」の対応であるとしています。

個人情報委員会へ報告のあった漏洩件数が、2017 年は 3,338 件、2018 年は 4,380 件、そして 2019 年は 4,520 件と増加している事実と「(株) リクルートキャリアに対する勧告及び指導」(2019. 8. 26)を指しています。「リクルートキャリアに対する勧告及び指導」は、

「リクルートキャリアが**安全管理措置**を適切に講じず、個人データを第三者に提供する際に**必要な同意**を得ずに第三者に提供していた」ことに起因する委員会のはじめての勧告及び指導でした。

（4）漏えい等報告・本人通知の義務化

また、2020 年改正では、漏えい等が発生し、個人の権利利益を害するおそれがある場合（即ち、個人データの性質や漏えい等の態様に着目して、要配慮個人情報や財産的被害に至るおそれのある情報の漏えい等や不正アクセスによる漏えい等、これらは件数の多寡は問わない、また、安全管理措置について懸念される一定数以上の大規模漏えい等）に、委員会への報告及び本人への通知を義務化することとしています。なお、「個人データの安全の確保に係る事態であって個人の権利利益を害するおそれが大きいもの」の内容や委員会への報告方法、期限等については今後委員会規則として、規定することとしています。

また、報告先には、**権限委託官庁を現行どおり含みますが、認定個人情報保護団体への報告を変更し不可**とし、個人情報保護委員会への報告として義務化します。**漏洩事実の全容を把握する目的で個人情報取扱事業者に個人情報保護委員会への報告（確定報告）を求めたものと推定されます。**

（5）「罰則の強化」と「漏えい等報告・本人通知の義務化」の意味

2020 年改正では、「個人の権利利益の保護」と「個人情報や個人に関連する情報を巡る技術革新の成果の経済成長等への利活用」の両面で促進されるよう多くの改正がなされています。保護と利用のバランスです。

「個人の権利利益の保護」の実効性確保の観点から、漏洩などの発生を迅速・適格にとらえるための「**漏えい等報告・本人通知の義務化**」とその違反行為に対する最終的な実効性確保の手段としての「**罰則の強化**」の改正がなされているのです。

一方、「個人情報や個人に関連する情報を巡る技術革新の成果の経済成長等への利活用」として、仮名加工情報の創設、個人関連情報の在り方、提供先において個人データとなる情報の取扱いなどが規定されていますが、これら項目については後日詳述する予定です。

2020 年改正法の最初の施行規定は、法令順守の徹底であり、その違反行為に対する最終的な実効性確保の手段の強化です。事業者が個人情報保護の基本ルールを遵守し、漏えいなどを起こさないことがまず要請されました。そのためには個人情報保護の基本ルールの従業者への教育・研修が重要になります。改めて、再度、上述の個人情報保護の基本ルールの周知が要請されています。

２．事例に学ぶ：ゼロトラストのこと

事例シリーズの第10弾になります。本稿では、この所話題に上り始めた「ゼロトラスト」について考えてみたいと思います。

ゼロトラストとは、「何も信頼せず常に検査する」とのコンセプトの元で情報セキュリティを保つ考え方で、2010年に米国の調査会社に所属するエンジニアが提唱したものです。従来の「社内と社外のネットワークの境界に防御戦を張る」方式とは出発点が大きく異なります。クラウドの利用やテレワーク環境を俯瞰すると、どこまでが〝社内〟でどこからが〝社外〟なのか判別が難しく、従って全ての情報流通過程について疑いを持たざるを得なくなっているとの視点です。内部の不正(またはミス)が元になる事案もないとは言えず、従業員が無意識の内に社内に危険要素を撒き散らす可能性もあります。

重要なことは被害に遭っても最小限に食い止めることです。

テレワークが一般的なワークスタイルになりつつある現下において、技術的措置として〝ログ監視〟、人的措置として〝自制〟〝牽制〟等が予防や被害最小化の胆になりますが、おのおのの対策に連携が必要と考えつつ以下検討を進めてみます。

（１）新しい危険

標的型攻撃等の被害が益々甚大になっており、犯罪者が益々インテリジェンスを高めていることを示しています。以前は〝メールの添付ファイルを安易に開かない〟〝怪しげな日本語のメールには返信しない〟等、比較的分かりやすい判断基準で防御できていましたが、今はAmazon、Apple、三井住友銀行等の著名会社を名乗って不正メールを送りつけてきます。本文もきれいな日本語で、「アカウントが凍結されました」「注文がキャンセルされました」「荷物を届けにきましたが不在でしたのでご都合のいい日時をご連絡ください」等と、いかにも自分に関係がありそうなものになっています。ウィルスに限らず、不正なサーバに誘導されるフィッシングメールも前出のような会社名使っています。

また「Emotet」については、巣窟と名指しされたWordの添付ファイルから、圧縮・暗号化に使われるzipファイルにも及んでいます。通信の安全対策の切り札と信じられていた「VPN」も危険にさらされており、実際我が国では2018年にあるゲーム会社が侵入されサーバ内のデータが全部削除される事件が起こりました。大手企業からも被害が報道されています。

VPNの脆弱性(弱点)は、VPN機器内の制御ソフトに内包されているものです。言わば「IoT機器への攻撃」になります。IoT機器に対する攻撃ではネットワークカメラが有名です。都内に設置されている何台かが(世界的には10万台以上のケースもあります)侵入されて、最終的なターゲットへの攻撃の踏み台(中継)に使われました。

加えて、テレワークに使用する自宅の環境は会社よりもセキュリティレベルは当然低くならざるを得ません。特に無線LAN(Wi-Fi)環境です。無線ルータもIoT機器の一種で、中に組み込まれたソフトが攻撃の対象になります。初期設定のままにしないこと、メーカ情報を参照して適宜アップデートすることが求められます。

（2）内部不正の状況

IPA(独法情報処理推進機構)が毎年公表している「情報セキュリティ 10 大脅威」の 2020 年版で〝内部不正による情報漏えい〟が第 2 位にランクされました。2018 年版では第 8 位、2019 年版では第 5 位でしたから急伸しています。

■「情報セキュリティ10大脅威 2020」　NEW：初めてランクインした脅威

昨年順位	個人	順位	組織	昨年順位
NEW	スマホ決済の不正利用	1位	標的型攻撃による機密情報の窃取	1位
2位	フィッシングによる個人情報の詐取	2位	内部不正による情報漏えい	5位
1位	クレジットカード情報の不正利用	3位	ビジネスメール詐欺による金銭被害	2位
7位	インターネットバンキングの不正利用	4位	サプライチェーンの弱点を悪用した攻撃	4位
4位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	5位	ランサムウェアによる被害	3位
3位	不正アプリによるスマートフォン利用者への被害	6位	予期せぬIT基盤の障害に伴う業務停止	16位
5位	ネット上の誹謗・中傷・デマ	7位	不注意による情報漏えい（規則は遵守）	10位
8位	インターネット上のサービスへの不正ログイン	8位	インターネット上のサービスからの個人情報の窃取	7位
6位	偽警告によるインターネット詐欺	9位	IoT機器の不正利用	8位
12位	インターネット上のサービスからの個人情報の窃取	10位	サービス妨害攻撃によるサービスの停止	6位

2019 年に、神奈川県庁からハードディスクの廃棄を引き受けた業者で、データを消去する前に従業員が持ち出してオークションで転売し、購入者した人からの通報で個人情報の情報流出事件として発覚しました。犯人は情報そのものの価値は認識しておらず、ハードディスクが売れるとの軽い気持ちからだったように報道されています。

また、ベネッセの 2,900 万件の個人情報漏洩事件では、スマートフォンを充電しようと PC の USB ポートに差し込んだ所、USB メモリと同じ扱いになることが分かってデータの取り出しに繋がりました。両事案ともある期間に亘って犯行が行われています。その間どうして誰も気づかなかったのか、不思議です。

私物の USB メモリが感染しているのを認識しておらず、そのまま会社の PC に差し込んで不正ソフトを呼び込み他の PC にも感染させたケースも後を絶ちません。

〝ちょっとこれくらいなら〟〝あれっ、こんなことができる〟から始まり次第に大胆になっていく……、ここで思い出すのが〝1 つの重大事故の背後には 29 の軽微な事故があり、その背景には 300 の異常(ヒヤリ・ハット)が存在する〟という「ハインリッヒの法則」です。

犯行の芽をいかにして早く摘むか、またそれ以前にいかにして自制する意識を醸成するかが課題です。

私物の機器を会社の LAN または PC に接続する際には、ウィルスチェックをするように定めても、装填した途端にマルウェアが作動しチェックをする間がない PC もあると思われます(OS の設定変更で作動しないようにもできますが) 。社内ルールとして先ずは PC に許可された機器以外は接続禁止にすることでしょう。PC の USB ポートを塞いだり、共有の外部ストレージを契約するのが現実的です。外部ストレージには安価なサービスもあります。

(3)「ログ」や記録の重要性

社内と社外の境界を通過する電文・メッセージに重きを置いていたセキュリティ対策が、視点を広げて考えざるを得なくなり、業界各社は〝ゼロトラストセキュリティ〟製品を相次いで発表しています。それらの製品は当然ながら技術的措置に限られ、ポイントを〝(複合的な)ログ監視〟に置いています。他に、USB メモリ等の可搬記憶媒体のセキュリティ強化等も含みますが、運用の便宜性等管理機能面を除けばその要素技術は、以前から活用されていたものと変わりはないと言ってもいいでしょう。また、必ずしも安価と言う訳にも行きません。

〝ログ〟については PC やサーバに OS の標準機能として装備されています。最低 6 ヶ月分の領域は持ちたいものです。取り敢えず提案したいのは「サーバのアクセスのチェック」です。ログファイルには夥しい数のログデータが記録されていますが、その中で着目すべき一つは〝エラー〟です。データの改竄や流出に際し、犯人は当初アクセスするためのパスワードを知りませんので色々と変えては何度もアクセスを試みます。都度エラーログが発生しますので後から発見できます。二つ目は人的措置とも被りますが、〝時間外のアクセス〟です。深夜早朝のアクセス、或いは入退記録と照合して全員退社後にサーバにアクセスがある、も疑って然るべきです。その意味で社員の入退記録も重要性を増していると言えます。

人的措置は主として内部犯行の予防を目的としたものが多いのですが、「性弱説」に則るとうっかりや無意識による事案も考えなくてはなりません。「組織における内部不正防止ガイドライン」(IPA)では教育研修、誓約書の取り交わし等と共に〝社内のコミュニケーション〟が力説されています。例えうっかりであっても社内のルール違反に該当するケースを見つけた場合には注意をし合う風土が今こそ必要で、プライバシーマーク事業者で必須事項になっている「運用の確認」、つまり自己点検も〝自制〟〝気づき〟の観点で大変有効と考えます。

(4)終わりに

働き方改革で話題になったテレワークやリモート(サテライト)勤務が、新型コロナウィルスによって一挙に常態化しようとしています。それに伴う情報セキュリティに関しては、今まで採られていた個別の対策を連携させて複合的な観点で見直す好機でもあります。

加えて、見逃し勝ちだった一部の社内ルールをより厳密に運用を始めるいい機会とも言えます。情報セキュリティを維持しつつ柔軟な勤務方式やクラウド等のより安全なシステムアーキテクチャを活用したいものです。

３．Ｐマーク再考！

昨今のコロナ状況は、様々な分野で従来とは異なる企業行動を表面化させ、そこに新たな発見があります。プライバシーマーク（以下Ｐマーク）の動向においてもその一端を見ることが出来ます。

10 月中旬に日本情報経済社会推進協会（JIPEDEC）が公表したＰマーク事業者数は 2020 年 9 月末で 16,485 社となっています。この 2 年間における半期ごとのＰマーク取得事業者数の推移は下表の通りです。

時期	2019/03	2019/09	2020/03	2020/09	2020/10
Ｐマーク取得事業者数	16,275	16,346	16,477	16,485	16,455
半期増減事業者数	306	71	131	8	△30

2020 年 9 月と 10 月の事業者数が問題です。Ｐマーク制度が始まって以来約 20 年Ｐマーク取得事業者数は、ここ 10 年ほどは毎年 500 社前後順調に増え続けていました。それが、今回、前月比マイナスという恐らく初めての異常事態に陥ったのです。

2020 年の 10 月は、新たにＰマークを取得した事業者の数を、2 年毎のＰマーク認証の更新継続を見送った事業者の数が 30 社も上回るという事態が発生したのです。これまでＰマーク制度は、我が国における個人情報取扱い事業者が、個人情報を保護するには最も有効な制度であり、着実に裾野を広げていただけに、この異変はショッキングな出来事となりました。

上記の要因が、新 JIS 対応の遅れや、中々収まらない新型コロナ感染拡大の影響による一時的なものであれば、コロナの収束や時間の経過とともに、再び着実な増加に転ずることが期待されますが、Ｐマークの拡大鈍化の背景には、必ずしも楽観視出来ない問題点も含まれているように思われます。以下においてその懸念される点を探ってみたいと思います。

（１）Ｐマーク制度について

個人情報保護法に則った JIS 規格である JIS Q 15001 の運用に対する第三者認証制度であるＰマーク制度は、

・民間部門の自主的な取り組みの促進
・第三者認証の認証基準とすることにより取り組みへのインセンティブを確保
・認証基準の明確化により認証制度に対する社会的信頼性の確保
・JIS 化することによる業種業態を超えた対応の確保

を狙いとして 1998 年に創設された。以降、現在まで約 20 年間に亘って、JIPDEC が推進母体となり運営されてきました。

我が国における個人情報保護意識の高まりとともに、Ｐマーク制度発足以来、これまでＰマーク取得事業者数は、常に右肩上がりでコンスタントに増加を続けておりました。その結果、現在では 16,000 社を超える事業者において、Ｐマーク制度に基づいた個人情報保護マネジメントシステムの運用が行われています。我が国の個人情報保護の水準は、Ｐマーク取得事業者によって支えられていると言っても過言ではありません。

即ち、Ｐマーク制度発足以来、個人情報を扱う事業者は、Ｐマークを取得し、JIS 規格である JIS Q 15001 によって個人情報保護の運用を行うことが望ましいと考えられてきました。

斯かる観点から、P マーク制度は日本独自の制度ではありますが、制度発足以来、我が国の個人情報保護を支える制度的な柱として、極めて重要な役割を果たすとともに、その役割は今後も変わることなく継続するものと思われます。

（2） Pマーク制度が抱える課題について

P マークの新規取得の伸び悩みと、継続更新の取止め事業者の増加は、コロナ以前から少しずつ一部業種（保険業等）で兆候を示しているようです。その要因を探ってみます。

①Pマーク取得事業者が共通して最も期待する効果は、個人情報漏えいの予防です。
JIS 規格が求める厳格な個人情報の取扱いを遵守することで、個人情報に関する事故を発生させない管理体制と組織作りが可能になります。ところがマイナンバー制度の出現もあって個人情報の取扱ルール等の情報がネット上でも容易に手に入るようになり、P マークを取得しなくてもある程度の水準で個人情報の保護・管理が可能となり、P マーク運用への依存度が、従前にくらべ薄れつつあると思われます。

②次に、Pマークを取得するメリットとしては、「営業上の外部要因に対応できる」といった実利的な面を挙げることが出来ます。システム関連事業や印刷業等、特定の業種においてはPマーク取得事業者の拡大の要因となっています。しかしながら、Pマークによって実利が得られるのは、必ずしも全業種には当てはまるものではなく、全体的に観ると実利面がもたらすPマーク取得事業者の拡大効果が乏しくなっているようです。

③P マーク取得事業者は、P マークの使用（表示）によって自社が個人情報を安全に取扱う事業者であること示し、企業間取引を行なう際の信用拡大に繋がります。この「信用拡大」のPマーク効果を発揮するためには、Pマークの意味するところが、十分社会的に浸透していることが前提になります。しかしながら、現状におけるPマークの認知度はまだまだ不十分で、「知る人ぞ知る」状態であることが気になります。因みにある新聞社の記事検索に「Pマーク」を入力したところ、「該当なし」が返ってきました

（3）今後に期待するもの

以上、Pマークの期待される効果と問題点を挙げてみましたが、Pマークが対象とする個人情報に関しては、「保護」と「利用」の両面から事件や事象を通して、社会的な関心が従来以上に高まっています。今後さらに複雑化する個人情報の取扱いにおいて、法律に基づく取扱ルールの実践を旨とする、P マーク制度の更なる拡大は不可欠であり、その拡大に当たっては、国をも巻き込んだPマーク制度の見直し時期を迎えていると考えます。

先年、内閣府に「個人情報保護委員会」が設置されたことは、我が国の個人情報保護の確立のためには極めて評価すべき事柄でした。P マーク取得事業者の拡大は、JIPDEC のような機関が単独で地道に行うという問題ではなく、国家的な見地から個人情報保護政策の中に組み込まれ、位置づけられるべき問題思われます。

今後、様々な形でPマーク拡大策が検討されると思いますが、ポイントはPマークの認知度のアップとPマーク事業者全体に及ぶインセンティブ付(税制の優遇措置等の政策的支援)にあると考えます。これからもPマーク動向を引き続き注視して行きたいと思っています。

４．お知らせ（トピックス）

（１）JIPDEC が「プライバシーマーク（P マーク）制度普及キャンペーン」を行っています。

P マークの元締めである日本情報経済社会推進協会（DIPDEC）では、P マーク制度の普及・認知度向上を目的として、9 月中旬より、

・「P マーク制度ステッカー」の P マーク取得事業者への配布

・P マークロゴ等の活用事例の募集と紹介

・アンケートの実施

を行っています。

このキャンペーンによって、P マークがより広く知れわたることが期待されます。

（２）マイナンバーカードの交付率が 20%に達しました。

政府はマイナンバーカードの普及に力を入れておりますが、2020 年 10 月 1 日現在で 20.5%となり、漸く 20%台に到達しました。

なお、交付率が 10%に達したのは 2017 年 12 月であり、約 3 年を要して 10%のアップしたことになります。

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）