Ｐマークニュース

＜２０２１年爽秋号＞　Vol. ３７

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

2020 改正個人情報保護法の施行が 2022 年 4 月 1 日となりました(政令第 55 号)。
今回は、主な改正点のうち「漏洩などの報告」ついて、明らかになった留意点を中心に概説します。記事では、
①漏えい等事案の「漏洩」「滅失」「毀損」に該当するケースとしないケース
②漏えい等事案が発覚した場合に講ずべき措置
③委員会報告の「速報」「確報」について
を、具体例を示しながら分かりやすく説明しています。

〝うっかりミス〟の再発防止策として真っ先に挙げられるのが、「ダブルチェックの励行」です。ところが、ある医療機関の報告によれば、「医療事故事例 20,127 件の中で 555 件（2.7%）がダブルチェックを行っていた」とのことです。
　このことから業種や業務には無関係で、ダブルチェックが事故防止の完全な切り札とはならないことが実証されました。
　記事では「ダブルチェック」をより有効にするための方策を提案しています。
　方策の中には「なるほど！」と、頷いて戴ける事項も多いのではないかと思いますので、今回もじっくりお読みください。

　Ｐマークの継続更新のハードルが、近時上がっているようです。
その要因としては、個人情報保護法の改正および、それに伴う JIS Q 15001 規格等の改訂で、個人情報の取扱いの厳正化が求められていることが、挙げられます。
　斯かる状況下でＰマークの更新を安定的に継続するために必要な事項として、
・Ｐマーク担当者（事務局）の複数名制／・個人情報保護マネジメントシステム（PMS）の運用情報（計画・作業状況等）の社内共有化／・定例作業である「個人情報管理台帳」、「リスク分析表」見直し作業の業務担当者全員参加による実施
等を挙げて、PMS 運用の活性化を説いています。

以上

１．事業者に追加して課せられる規制(続)　　改正法のポイント

2020 改正個人情報保護法の施行が 2022 年 4 月 1 日となりました(政令第 55 号)。

今回は、主な改正点のうち、「漏洩などの報告」ついて、明らかになった留意点を中心に概説します。

法ガイドライン及びそのパブコメとして、はじめて「漏洩等の報告・本人通知」の章を設け、事例を含め具体的に記載されています。

なお、このガイドラインが基本となると思われますが、金融機関向けガイドラインの改訂版、JIS 規格改定版は、まだ公表されておりません。

（1）漏えい等事案の「漏洩」「滅失」「毀損」って、どういうこと？

「漏洩」とは、「個人データが外部に流出すること」で、誤送付、誤送信、システムの設定ミス等によるインターネット上で個人データの閲覧が可能、書類・媒体等の盗難による場合、不正アクセス等により第三者に個人データを含む情報が窃取された場合などを指します。

個人データを第三者に閲覧されないうちに全てを回収した場合は、漏えいに該当しません。

次の事例は留意を要します。(パブコメの集約(2021.09.27)から転載)

①フィッシング詐欺等によって、本人が悪意ある第三者にパスワード等の情報を渡した事例は、個人情報取扱事業者から個人データが流出していないことから、「漏えい」に該当しません。

②当該第三者が事業者のデータベースに本人になりすまして、不正アクセスをした場合については、当該第三者が個人データを閲覧した場合には、「漏えい」に該当すると考えられます。

③守秘義務を課した委託先、または共同利用先（以下「委託先 等」）が複数存在する中で、委託先等 A に送るべき個人データを含むメール等を委託先等 B に誤送信した場合について、委託先等 B には守秘義務を課している上に委託または共同利用の相手方であって「外部」とは言えないことから、この場合は「漏えい」にはあたらないと解することでよいか。(損保協会)

⇒　委託先や共同利用先であっても、当該委託・共同利用において対象となる個人データ以外の個人データを誤送信した場合には、「漏えい」に該当し得ます。

④郵便事業者等が「誤配達」した場合も漏えいに該当するのか。この場合、漏えい等事案が発覚した場合に講ずべき措置を行うのは誰になるのか。

⇒　郵便事業者等は、通常、郵送する文書の中身の詳細については関知しないことから、「個人データが記載された書類」に関しては、個人データの取扱いの委託を受けていないものと考えられます。他方、郵便事業者等を利用する個人情報取扱事業者は、

「個人データが記載された書類」を取り扱っており、安全管理措置を講じる義務があることから、郵便事業者等が誤配達をした場合も含め、漏えい等事案が発覚した場合には、必要な措置を講じなければなりません。

「滅失」とは、「個人データの内容が失われること」で、誤って廃棄、紛失した場合などを指します。その内容と同じデータが他に保管されている場合は、滅失に該当しません。

「毀損」とは、「個人データの内容が意図しない形で変更されることや、内容を保ちつつも利用不能な状態となること」を指し、改ざん、暗号化処理された個人データの復元キーを喪失し復元できない場合、ランサムウェア等により個人データが暗号化され、復元できない場合を指します。その内容と同じデータが他に保管されている場合は毀損に該当しません。

（2）漏えい等事案が発覚した場合に講ずべき措置

JIS 規格でも規定されている下記の措置を講ずることがガイドラインでも明記されました。

a）事業者内部における報告及び被害の拡大防止
b）事実関係の調査及び原因の究明
c）影響範囲の特定
d）再発防止策の検討及び実施
e）個人情報保護委員会への報告及び本人への通知
f）事実関係及び再発防止策等についての速やかな公表

どのような「漏洩」「滅失」「毀損」を個人情報保護委員会へ報告しなくはならないか？

個人情報取扱事業者は、次の①から④までに掲げる事態を知ったときは、個人情報保護委員会に報告しなければなりません。

①要配慮個人情報が含まれる個人データの漏えい等が発生し、又は発生したおそれがある事態。

事例 1）病院における患者の診療情報や調剤情報を含む個人データを記録した USB メモリーを紛失した場合

事例 2）従業員の健康診断等の結果を含む個人データが漏えいした場合

②不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態。財産的被害が生じるおそれについては、対象となった個人データの性質・内容等を踏まえ、財産的被害が発生する蓋然性を考慮して判断する。

事例 1）EC サイトからクレジットカード番号を含む個人データが漏えいした場合

事例 2）送金や決済機能のあるウェブサービスのログイン ID とパスワードの組み合わせを含む個人データが漏えいした場合

なお下記の事例については対象ではないとしています。

(パブコメの集約(2021.09.27)から転載)

・銀行口座情報のみが漏えいした場合
・クレジットカード番号の下４桁のみが漏えいした場合
・購買履歴のみが漏えいした場合

・個人データである給与情報や口座番号のみが漏えいした場合
・保険証券に記載された証券番号、保険契約書、保険契約に関する告知書、顧客リスト（顧客の氏名・住所が記載されたリスト）が漏洩等した場合

③不正の目的をもって行われたおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態。（「不正の目的をもって」漏えい等を発生させた主体には、第三者のみならず、従業者も含まれる）

事例 1）不正アクセスにより個人データが漏えいした場合
事例 2）ランサムウェア等により個人データが暗号化され、復元できなくなった場合
事例 3）個人データが記載又は記録された書類・媒体等が盗難された場合
事例 4）従業者が顧客の個人データを不正に持ち出して第三者に提供した場合

なお、漏えい等が発生し、又は発生したおそれがある個人データについて、高度な暗号化等の秘匿化がされている場合等、「高度な暗号化その他の個人の権利利益を保護するために必要な措置」が講じられている場合については、報告を要しない。

「高度な暗号化その他の個人の権利利益を保護するために必要な措置」の具体例は、Ｑ＆Ａで後日示す。

④個人データに係る本人の数が千人を超える漏えい等が発生し、又は発生したおそれがある事態。

事例）システムの設定ミス等によりインターネット上で個人データの閲覧が可能な状態となり、当該個人データに係る本人の数が 1,000 人を超える場合、更に、下記の記述があり、留意すべきです。

・個人データの漏えい等の事案が発生した場合等の対応について（平成 29 年個人情報保護委員会告示第１号）」は廃止することとしており、改正後の法第 22 条の２第１項の報告の要否を判断に当たっては、同告示の「３．」(2)　報告を要しない場合」は考慮されません。
・個人情報保護委員会が報告を受理する権限を事業所管大臣に委任している場合には、当該事業所管大臣に報告する。
・改正後の法第 22 条の２第１項に基づく報告について、認定個人情報保護団体経由の報告は予定されていません。なお、漏えい等報告の義務を負う個人情報取扱事業者以外の者が、当該個人情報取扱事業者の代わりに報告を行う場合には、行政書士法を含む他法令を遵守する必要があります。また、個人情報取扱事業者が、漏えい等事案について、改正後の法第 22 条の２第 1 項に基づく個人情報保護委員会等への報告に加えて、認定個人情報保護団体に対しても報告を行うことは、認定個人情報保護団体による自主的取組の一環として有効と考えられる。としています。なお、JIPDEC の「プライバシーマークにおける個人情報保護マネジメントシステム構築・構築運用指針」(2021.08.30)では、「事実関係、発生原因および対応を関係機関に報告すること」と規定し、「その関係機関とは、報告すべき利害関係を有している機関（本人、委託元/委託先、企業グループ各社、プライバシーマークの審査を受けた機関（プライバシーマーク付与事業者の場合）、個人情報保護委員会、認定個人情報保護団体（所属している場合）など）を指す。」としており、報告は、

従来どおりプライバシーマーク付与事業者への報告も必要で保護委員会報告にも必要なのか、現在は明確でありません。

（3）委員会報告の「速報」「確報」について

①誰がどのように報告しなければならないか?

漏えい等報告の義務を負う主体は、漏えい等が発生し、又は発生したおそれがある個人データを取り扱う個人情報取扱事業者である。

委託の場合・・・個人データの取扱いを委託している場合においては、委託元と委託先の双方が個人データを取り扱っていることになるため、報告対象事態に該当する場合には、原則として委託元と委託先の双方が報告する義務を負う。この場合、委託元及び委託先の連名で報告することができる。なお、委託先が、報告義務を負っている委託元に当該事態が発生したことを通知したときは、委託先は報告義務を免除される。と規定しています。

②「速報」の報告について

下記の項目を、個人情報保護委員会のホームページの報告フォームに入力する方法によって、個人情報取扱事業者が当該事態を知った時点から概ね 3～5 日以内に報告すること。

・概要
・漏えいなどが発生し、又は発生したおそれがある個人データの項目
・漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数
・原因
・二次被害又はそのおそれの有無及びその内容
・本人への対応の実施状況
・公表の実施状況
・再発防止のための措置
・その他参考となる事項

③「確報」の報告について

個人情報取扱事業者は、報告対象事態を知ったときは速報に加え原則 30 日以内に、報告のこと。

（4）「漏洩等の報告・本人通知」について詳細ガイドラインが規定された意味

このほかに、本人への通知に関連して、通知の時間的制限、通知の内容、通知の方法などが更に、詳細に規定されています。（詳細は省略）こうした具体的で詳細なガイドラインの狙いは、事業者にとって、分かりやすく便利であることですが、その対応遵守を強く求めてもいるのです。

守られなかった場合の罰則が強化されました。

金融機関向けガイドラインの改訂版、JIS 規格改定版は、まだ公表されておらず、詳細が流動的でもありますが、このガイドラインが基本となると思われます。

２．事例に学ぶ：「ダブルチェック」をより有効に

事例シリーズの第13弾です。本稿では〝ダブルチェック〟について考察してみようと思います。以前採り上げた「〝うっかりミス〟は予防できないのか」の続編に当たります。

背景は、プライバシーマーク審査機関から耳にしたことですが、事故報告書の中で従業者の不注意を原因としている比率が非常に高く、再発防止策として金科玉条のように再教育・徹底とダブルチェックを挙げている例が大半とのことです。ところが、ダブルチェックをしていたにも拘わらず、すり抜けたケースが中には見受けられるようです。

医療関係でも、厚生省の平成30年度医療安全セミナーで京大付属病院の先生が発表されている内容に「(事故DB上の)20,127件の医療事故事例中555件でダブルチェックを行っていた」とあります。業種や業務と無関係でダブルチェックが事故防止の完全な切り札とはならないことが実証されています。

著名な「稲盛哲学」(稲盛和夫 OFFICIAL SITE)でもダブルチェックの重要性について述べられているように、その有効性については論を俟ちませんが、ダブルチェックを行っても何故すり抜けや見逃しなどが発生するのでしょう。より精度を上げるためにひと工夫が必要なのではないでしょうか。

（1）ダブルチェックの落とし穴

言葉の定義になりますが、〝**ダブルチェック**〟とは「一度点検したことを、もう一度、またはもう一人が確かめること」(広辞苑)とされており、必ずしも複数の人でチェックすることではありません。ルールとして二人でチェックすることが定められていない限り、一人で行ってもいい訳ですが、稲盛哲学では「あらゆる伝票処理や入金処理を複数の人間で行うこと」としています。一方、異なった観点や方法で検査・確認することを〝**クロスチェック**〟と説明されている(同)ように、方法さえ変えれば一人で行っても十分チェックになります。

注意を要するのは、各種の機関(次項参照)から公表されているようにダブルチェックで間違いを犯す率は〝シングル〟チェックの間違い率の乗算(掛け算)にならないことです。「自分が間違いを見逃しても、相方(第二作業者)が見つけてくれるだろう」や「前の人(第一作業者)がチェックしているのだから間違いはないのではないか」等々のバイアス（思い込み等＝**【確証バイアス】**）が掛かるのが原因の一つです。また、第二作業者にとって第一作業者の粗探しになるのではないか、との別のバイアス(気遣い、忖度)が働く場合もあるでしょう。

（2）「ダブルチェックの原則」とクロスチェック

上記のように複数人によるダブルチェックが必ずしも万全の策ではないにしても、それに替わる方法が今すぐは手に入りません。

では、ダブルチェックの精度を上げるにはどうしたらいいのでしょうか。

稲盛哲学では「ダブルチェックの原則」として以下のように述べています。

『ダブルチェックの原則を貫くことは、間違いの発見やその防止のために有効ですが、このような原則を厳格に守るもう一つの目的は、人を大切にする職場をつくることにあります。人間はふとしたはずみで過ちを犯してしまうという弱い一面を持っています。この「人の心」が持つ弱さから社員を守り、人が罪をつくることを未然に防ぐシステムとして有効なのです。そうした経営者の優しい**思いやりの心**が、この原則の根底にはあります』

ここでは〝経営者〟の思いやりとしていますが、〝チェッカー(第二作業者)〟に置き換えてみたらいいと思います。チェッカーの第一作業者への思いやりです。応援する気持ちでし

ょうか。第一作業者を必要以上に疑いの眼で見たり悪意を持ったりせず、リスペクトはしても忖度はしないことです。

片や、クロスチェックは**一回目とは異なる方法**でチェックする訳ですから一回目と二回目（それ以降も）何かを変えることになります。例として、画面に入力した情報をチェックする際に以下の方法(動作)が考えられます。(単に入力した画面を眺め直す等は該当しません)

・画面に向かって指さし確認を行う(電車のホームでよく見かけます)
・声を出して読む(第三者的な立場になります)
・印刷する(外面よりも広い視野に立てます)
・英字や数字の照合を逆読みする(単語や塊で見ない)

〝逆読み〟については、単語や文字の塊で見ると例えば〝Amazon〟がパターンで頭に入っていると確証バイアスでAmzon、Anazon、Amason等が全部正しく見える可能性があります。

最後の文字(この例では〝n〟)から遡ってチェックすることで単語ではなく1文字ずつの確認になります。

（3）「社会的手抜き」

端的に言えば、一人で行った仕事のパフォーマンスよりも**複数で行った場合の一人当たりのパフォーマンスが落ちる**ということです。ウィキペディア（Wikipedia）では、社会的手抜きを『集団で共同作業を行う時に一人当たりの生産性が人数の増加に伴って低下する現象。リンゲルマン効果、フリーライダー（ただ乗り）現象、社会的怠惰とも呼ばれる』と説明されています。マクシミリアン・リンゲルマン(20世紀初頭のフランスの農学者)の実験結果で、「一人で行った時の仕事量(力)を100とすると、二人ですると一人当たりの力は93%に、三人ですると85%・・・のように低下する」との指摘があります。

更に、「二人一組のチアリーダーを、衝立を挟んで座らせ、単独での条件とペアでの条件で大声を出してもらい騒音計で音量を計測する実験をしたところ、ペア条件での音量は単独条件の94%の音量しか出ず手抜きをしていた。しかし、実験後の被験者たちはどちらの条件でも全力を尽くしたと思っていた」とのラタネとハーディ(1968年・米国)の実験も報告されています。

（4）終わりに

各種のバイアスに加え、社会的手抜きが人間には避けられないことから間違いをゼロにすることはできそうにありません。間違い率を下げることが現実的な命題です。

ダブルチェックやクロスチェックは一人による(または一回の)チェックよりも間違い率を下げる効用があるのは明らかではあっても、期待通りの効果を得るためには取り組む時のマインドの持ち方やチェックの動作にもうひと味足すことが望まれます。二人でダブルチェックをする際には相互に応援する気持ちになる、一人でクロスチェックする場面では対象（画面等）を凝視するだけではなく指さしや小さな声で読み上げるような動作を入れる等、すぐにできそうなことから始められるよう提案します。

３．Ｐマーク更新を確実にするための PMS 運用について

Ｐマークを継続更新するハードルが最近徐々に上がっているように思われます。

その要因としては、個人情報保護法が、大型漏洩事故等や EU の動き等に対応するために、個人情報の取扱いが厳正化される方向にあり、加えて「マイナンバー」の取扱いも PMS 運用管理の範疇に加わってきたこと等によります。

以前のように個人情報保護法の改訂が殆どなく、また、それに伴って JIS 規格の変更のない時代は、一度Ｐマークを取得すれば、規程等の変更対応等がないため、個人情報保護マネジメントシステム(PMS)の運用は、比較的容易であり、Ｐマークの継続更新は、あまり問題なく出来ていたようです。

ところが、前回（2015 年）の個人情報保護法改定以降、法の「3 年ごとの見直し」等によって、規程の改訂の頻度が上がることが予定されています。法のこのような動きは、頻繁な JIS 規格の改訂に繋がるものであり、日頃の PMS 運用はもとより、Ｐマークの継続更新に際しても、その対応が求められます。

即ち、Ｐマークの運用・更新には従来以上のマンパワーを投入が必要になってきています。

このような状況の変化は、一部のＰマーク取得事業者においては、PMS 規程の更新や、それに伴う諸規程への対応が出来ないために、折角取得したＰマークにも拘わらず、その更新を断念するといった　残念な事態の発生も稀ではありません。

下表は、保険代理店におけるＰマーク取得事業者と取止め事業者の年度推移を表したものですが、更新取止め代理店数の推移が如実にそのことを表していると思われます。（2017 年改訂施行の影響は、経過措置もあり 2018 年以降に顕在化したといえます）

注：2021 年は 9 月現在

項目	2015 年	2016 年	2017 年	2018 年	2019 年	2020 年	2021 年
新規取得代理店数	16	15	11	7	3	3	7
更新取止め代理店数	5	4	2	13	7	6	3

Ｐマークの更新の取止めは、2018 年から 2020 年が目立っています。この時期は、前回の個人情報保護法の改正（2017 年施行）の影響を受けた時期に当たり、JIS 規格の改定対応が伴い、従前以上にＰマークを継続更新するに対するハードルが上がった時期といえます。

前述の通り法改正や JIS 規格改訂の頻度は、今後、従来以上に高まることが想定されます。

斯かる状況下で、安定的にＰマークの運用・更新を続けて行くためには、日頃からの PMS が求める「全社的」な取り組みが不可欠といえます。

以下では、今後求められる PMS 運用の全社的な取り組みの具体例を示しながら、Ｐマークの安定的な運用・更新を図るための方策を検討してみたいと思います。

（１）安定的なＰマーク運用には複数のＰマーク担当者（事務局）の養成が不可欠です

多くのＰマーク取得事業者において、Ｐマーク取得時の担当者が事務局となり、一人で PMS 運用の旗を振り続けているケースがみられます。この状況で直ちに問題が出る訳では

ありませんが、この担当者が、業務異動や退職すると一気に問題が噴出し、PMS 運用が機能しなくなるといったケースが珍しくありません。PMS 担当者は一朝一夕には育ちませんので、ベテラン・新人等の組み合わせである程度時間を掛けながら、担当者を養成して行くことが肝要です。PMS の推進を一部（一人）の担当者に任せず、世代交代も図りながら常に複数の担当者を養成することは、P マークの安定的な運用・更新を図るための第一歩と言えます

（2）円滑な PMS の全社運用には情報の共有化と、部門管理者の参加・協力が必要です

P マークの更新のベースとなる PMS 運用については、定められた作業項目とスケジュールを示した資料（PMS 運用計画書等）を社内に掲示して、PMS 関連情報を共有化することが、社内の多くの人に PMS 運用の全体を知って貰うもらう上で効果的です。

また、PMS 推進のキーマンは一義的には事務局ですが、部門管理者の PMS 運用への理解と協力は、円滑な運用に不可欠です。部門管理者の協力を得る方法としては、部門管理者が出席する PMS の運用推進のための関係部署会議を、年に 3、4 回開催することが有効です。この会議で、PMS 運用の全社的進捗状況の確認や PMS 運用の改善点について協議することが出来れば、全社を挙げて P マークの推進に取り組む雰囲気も醸成され、P マーク運用の事務局孤軍奮闘状態からの脱出が期待されます。

（3）個人情報の特定とリスク分析の見直し作業は、業務担当者全員の参加で実施します

PMS 運用の中には、「規程文書の見直し」「委託先の見直し」等々いくつかの見直し作業がありますが、見直し作業の中で最も大切なのが、「個人情報の特定（個人情報管理台帳）」と「リスク分析表」の見直しです。

この作業に、業務担当者全員の参加を得ることは中々難しいかも知れませんが、大変重要な作業です。台帳等の見直しの機会に、既に作成されている自部門の「個人情報管理台帳」や「リスク分析表」を前に、「自分の周りにまだ管理されていない個人情報はないか」や「台帳に記載されている個人情報の事項に更新の必要はないか」、さらにリスクに関しても、「個人情報に対するリスクは網羅されているか」や「さらに有効なリスク対策はないか」等々を部署ごとに議論しながら見直すことが出来れば、「個人情報管理台帳」と「リスク分析表」の精度が高まり、また、多くの業務担当者に PMS 運用に対する参加意識を植えつけます。このような台帳とリスク見直しが実際に出来るかどうかは、部門管理者のリーダーシップにかかっていることも付け加えます。

以上、やや偏った見解になっているかも知れませんが、P マークの更新を安定的に継続するために、P マーク事務局だけが必死に頑張る形骸化された PMS 運用を排除し、全社員、全部門を対象とする PMS 運用の原点に近づくための方策を挙げてみました。

PMS 運用の年度締め括りの、マネジメントレビューにおいてはトップマネジメントを交えて自社の「PMS 運用への全員参加度」評価を行ってみては如何でしょうか。

４．お知らせ（トピックス）

（１）P マークを取得するなら「今！」がチャンスです

既に本誌でご案内の通り、改正個人情報保護法が 2022 年（4 月）に施行されます。

この法改正を受けて P マークの準拠規格である JIS Q 15001 も改定される見込であり、再び「新 JIS 対応」が不可避となります。

この「2020 年度版新 JIS 対応」を伴った P マークの取得は、現状以上に負荷の多いものになることが予想されます。

P マーク取得を検討されている保険代理店様にとって、今が取得のチャンスです。

是非、お気軽に下記にご連絡ください。

（２）マイナンバーカードの交付率が３９％に達しました。

政府のマイナンバーカード普及への努力もあって、2021 年 11 月 1 日現在のカード交付率は全国レベルで 39%（発行枚数約 5,000 万枚）と、もう一息で４割に達します。

昨年 10 月に 20%越えをして、約１年で倍増したことになります。

マイナンバーカードの健康保険証利用も始まりました。まだカード発行未済の方はもそろそろマイナンバーカードの取得をご検討ください。

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）