Pマークニュース

＜２０２３年陽春号＞　Vol. ４３

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

最新の JIPDEC 編集のガイドブックにおける個人情報保護リスクにかかわる規程ないし審査基準の記述内容・ボリュームは、従来と大きく異なっています。
多くの改定点があり、認定事業者の対応が必要ですが、なかでも大きな追加、改訂に労力を要するのが、個人情報保護リスクへの「認識・対応」、「リスクアセスメント」、「リスク対応」です。これらについて「構築・運用指針」を参照しながら、再検証し、異なる点に焦点を当て、従来の検討をベースに追加検討すべき事項を明らかにして行きます。

今回の「事例に学ぶ」は、IPA の「2023 年版情報セキュリティ 10 大脅威」の「組織編」の第 2 位にランクされている、取引先との関係で発生する『サプライチェーンの弱点を悪用した攻撃のリスク』について「脅威の流れ」「事案の例（3 事案）」「予防措置の考察」といった観点から解説します。
「サプライチェーン」とは商品の企画・開発から、調達、製造、在庫管理、物流、販売までの一連のプロセス、およびこの商流に関わる組織群を指し、情報セキュリティの脅威が取引先(顧客)を巻き込んで実務に重大なトラブルを引き起す事案が多く発生していますので、「サプライチェーン」リスクについて再考しました。

P マーク制度が 2023 年 4 月に創設 25 周年を迎えました。現在 P マーク取得事業者数は 17,400 社に達しています。
この機に、P マークーク取得事業者数の拡大推移を振り返るとともに、直近 5 年間の動向として、業種別に P マーク取得事業者数の増減を、JIPDEC の公表資料からみました。結果、25%と大幅アップした不動産業が目を引きました。
また全体傾向として、ここ数年は P マーク事業者の増加が伸び悩んでいましたが、2022 年からは再び増勢に転じているという、明るい状況も確認できました。

以上

１．個人情報保護リスク　見直しましょう!!　　－ PMS 審査基準も改訂されています －

PMS の審査基準が 2022.4.1 から改訂され、審査されています。その改訂審査基準は、2022.4 からの「改正保護法」の施行の反映に加えて、JIS Q 15001:2017 本文を反映させた「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・運用指針」です。

多くの改定点があり、認定事業者の対応が必要ですが、なかでも大きな追加、改訂に労力を要する「個人情報保護リスク」への認識・対応、リスクアセスメント、リスク対応について、「構築・運用指針」を参照しながら、再検証し、異なる点に焦点を当て、従来の検討に新たに追加検討すべき事項を、明らかにして行きます。

（１）リスクにかかわる審査項目が顕著に増えている。

PMS の審査にかかわるガイドラインは、JIPDEC プライバシーマーク推進センターが編集し、日本規格協会から過去 4 回刊行されています。

過去 2 回(①2007.1.10 発行②2010.8.25 発行)は JIS Q15001:2006 を基準にした「実施のためのガイドライン」として、その後③2018.9.14④2022.6.10 に改訂され発行されました。

後の 2 回は「導入・実践ガイドブック」として、JIS Q15001:2017 を基準にしています。

これらのガイドブックにおける個人情報保護リスクにかかわる規程ないし審査基準の記述の内容・ボリュームは、大きく異なっています。①では 2 頁の記述であったものが、最新の④では 11 頁に亘っています。これは、最新の④では、「P マークにおける PMS 構築・運用指針対応」(以下「構築・運用指針」という)として発行されており、その指針では、従来の JIS Q15001:2017 付属書 A の要求事項に加え、JIS Q15001:2017 本文の要求事項を指針として加えているためです。

関連する要求事項も従来 1 項目(A.3.3.3)だったものが、3 項目(J.3.1.2　J.3.1.3　J.3.1.4)と増えています。

（２）個人情報保護リスクとは?

「リスク」とは、「目的に対する不確かさの影響」(JIS Q15001:2017 の 3.9)ですが、「個人情報保護リスク」とは、下記であり、保険引受リスク、資産運用リスク（市場リスク、信用リスクなど）、オペレーショナル・リスクなどとは、異なるリスクとして、定義されています。(JIS Q15001:2017 の 3.43)

「個人情報の取扱いの各局面(個人情報の取得・入力、移送・送信、利用加工、保管・バックアップ、消去・廃棄に至る個人情報取扱の一連の流れ)における、

①個人情報の漏えい、滅失または毀損、

②関連する法令、国が定める指針その他の規範に対する違反、

③想定される経済的な不利益及び社会的な信用の失墜、

④本人の権利利益の侵害など　好ましくない影響　」

です。

この 4 つの範疇のリスクがしっかり認識・特定されていますか？

①②範疇のリスクにとどまり、最近とみに社会問題化している③④のリスク認識・特定に洩れはないですか？

「構築・運用指針」では、この個人情報保護リスクに対して、3 つの要求事項があります。「リスク及び機会に対処する活動」(J.3.1.2)、「個人情報保護リスクアセスメント」(J.3.1.3)、「個人情報保護リスクへの対応」(J.3.1.4)です。

（3） リスク及び機会への対処(J.3.1.2)

「対処する必要があるリスク及び機会の決定」が必要で、その決定に当たっては、「事業者が営む事業の内容、規模、取扱っている個人情報の種類や量などによって異なること」を考慮し、「必要な体制の構築」、「リスク対策の内容」、「実施する方法」、「リスク対策の効果」を検討すべきとしています。

従来のガイドブックにおいては、前提としていた事項を、一般論として明記した要求事項としています。より具体的には「個人情報保護リスクアセスメント」(リスクの特定、リスクの分析、リスクの評価)及び、「個人情報保護リスクへの対応」(リスク対応策、リスク対応計画、トップの承認、残留リスクの把握)であり、J.3.1.3 及び J.3.1.4 で規定されています。

（4） 個人情報保護リスクアセスメントで要求されること(J.3.1.3)

「構築・運用指針」では個人情報リスクアセスメントとして、下記を要求している。

1. 事業者は、個人情報に関するリスクについて、次の事項を踏まえて、個人情報保護リスクアセスメント（リスクを特定、分析及び評価）をするための手順を定め、かつ実施しなければならない。手順及び実施した内容については、少なくとも年一回及び必要に応じて適宜に見直すこと。

a)次の観点を、個人情報保護の**リスク基準**とする。

1） 本指針に定める事項

2） 法令及び国が定める指針その他の規範に関する事項

3） 個人情報の漏えい、滅失又はき損等に関する事項

b)繰り返し実施した個人情報保護リスクアセスメントに、一貫性及び妥当性があり、かつ、比較可能な結果を生み出すことを確実にする。

c)個人情報保護リスクを特定する。

1)事業者において、事業毎に、個人情報の取扱いを特定する。

2)個人情報の取得、保管、利用及び消去等に至る各局面において、適正な保護措置を講じない場合に想定されるリスクを特定する。

3)上記で特定したリスクの**リスク所有者**を特定する。

d)個人情報保護リスクを分析・評価する。

1)c)で特定したリスクと、a)のリスク基準とを比較する。

2)リスク対応の**優先順位**を明らかにする。

2 事業者は、個人情報保護のリスクを特定、分析及び評価をするための手順を内部規定として文書化しなければならない。

リスクの特定、リスクの分析、リスクの評価についての要求事項です。今回の「構築・運用指針」で明記され、留意すべきは、**「リスク基準」「リスク所有者」「リスク対応優先順位」**に触れていることであり、これらについてその記録への明記が必要と考えられます。

「リスク基準」は、下記の３つの観点とすることを要求事項として追加明記し、特定するリスクごとに、そのリスク基準を明らかにすることが求められています。

①本指針に定める事項(「構築・運用指針」のリスク修正対策に該当するもの)

②法令及び国が定める指針その他の規範に関する事項

(法令及び国が定める指針その他の規範には、事業者が上乗せする基準を含む)

③個人情報の漏えい、滅失又はき損等に関する事項(安全管理措置に関する事項)

「リスク所有者」とは、リスクの特定にあたって、リスクについての責任及び権限を持つ者であり、その特定を要求事項として追記明記しています。特定するリスクごとに、そのリスク基準を明らかにすることが求められています。

また、**「リスク対応優先順位」を**明記する事を要求事項として追加しています。「リスク対応優先順位」の検討に当たっては、「リスクの発生可能性」と「その影響」をマトリックスで表現した「リスクレベル」を考慮することも有用ですが、個人情報保護の分野においては、本人の権利義務の観点から個人情報保護リスクの受容に関しては慎重な対応が必要です。

従って特定した個人情報保護リスクは、リスクレベルを考慮するものの、原則、実施し対応策を検討することが望まれる。とされており、留意を要します。「リスク対応優先順位」として「必須」「中」「低い」などを明記する事が必要になります。

（５）個人情報保護リスク対応で要求されること(J.3.1.4)

1.事業者は、次の事項について、個人情報保護リスクへの対応手順を内部規程として文書化し、かつ実施すること。手順及び実施した内容については、適宜見直さねばならない。

a)個人情報保護リスクへの対応にあたっては、個人情報保護リスクアセスメントの結果を考慮して、必要な対応策（本指針及び事業者が必要であると決定した、個人情報保護に関するリスクを修正する対策を含む）を策定すること。

b) a)を踏まえて、個人情報保護**リスクへの対応計画**を策定し、実施すること。

c)個人情報保護リスクへの対応計画及び実施した内容（現状で実施し得る対策を講じた上で、未対応部分を**残留リスク**として把握し、管理することを含む）について、原則として、**トップマネジメント(代表者)の承認**を得ること。

2.事業者は、a)～c)を実施した記録を保持する。

上記は、「リスク対応策の策定」「リスク対応計画」「リスク対応の結果」「残留リスクの把握」「トップマネジメントの承認」についての要求事項です。

「リスク対応策の策定」については、今回の「構築・運用指針」で新たに追加している事項はありません。従来から実施されている「各リスク管理策を『リスク分析表』に記録し、この際に、選択したリスク管理策を規定している『関連規程』および『その際に使用する様式等』を記録する。」ことが必要です。

「リスク対応計画」「リスク対応の結果」についても、今回の「構築・運用指針」で新たに追加している事項はありません。リスク対応は、リスク対応策の策定とともに、速やかに実施することとし、対応に期間・費用を多く要する時には、「必要に応じて」「リスク対応計画」を作ります。「リスク対応の結果」は、リスク対策の見直し時期に、検証し記録します。現状で実施し得る対策を講じた上で、未対応部分を**「残留リスク」**として把握するものについては、その旨を記録します。

なお、残留リスクとは、リスク対応後に残っているリスクのことであり、受容するリスク（放置していてよいリスク）ではなく、現時点では困難であるが、短期的若しくは中長期的に対応していくリスクを指します。個人情報の不適切な取扱い（不正な取得・利用など)に関するリスクについては、法令遵守の観点から、全て対応する必要があるため、残留リスクとすることは認められません。

「トップマネジメントの承認」については、従来から審査では必須事項であったものの、従来の要求事項(A.3.3.3 など)には、明記されておらず、今回の「構築・運用指針」で新たに明記されています。

（6）まとめ

「構築・運用指針」で求められている要求事項にそって、2022.4 からの PMS 審査が厳密に実施されているか否かについては、とりわけ更新審査対象の事業者にとっての負荷が大きいことから、一部項目については、緩和されているという観測もあります。(定かではありませんが･･･)法改正への対応は、適時に適格に行うとしても、改訂されたリスクマネジメントへの対応は、必要に迫られたらという対応も頷ける一面もあります。

しかしながら、個人情報保護リスクも急激に多様化し変化しています。

テレワーク環境下のリスク、Cookie 情報(位置情報などを含む)の悪用リスク、フェイク電話、フェイクメールなどで個人情報は、日々、新たな危機にあり、大きな社会問題ともなっています。

個人情報保護リスクで言う「想定される経済的な不利益及び社会的な信用の失墜」、「本人の権利利益の侵害など」のリスク認識・特定は、十分でしょうか?

新たな未知のウィルスの発生も多くなっています。最近、これらへのリスク対策が十分でなく、大きな被害が発生しています。

一方、全ての局面で詳細に、リスクアセスメントし、リスク対策をするのは、不可能に近くなっています。**事業特性を考慮して、わが社のリスクを自分の眼で、「構築・運用指針」に従って、特定し、分析し、評価し、対応することが必要です。**

PMS 審査を通過するためのテンプレートから一歩脱することです。日々、各職場が遭遇するであろうリスクを敏感に認識することから一歩を踏み出すことが大切です。

多くのリスクに敏感であることは、「残留リスク」も多くなります。「残留リスク」は未対応リスクであり、少ないことが望まれますが、リスクに敏感であるという意味では好ましいことかもしれません。

２．事例に学ぶ：サプライチェーンリスクについて

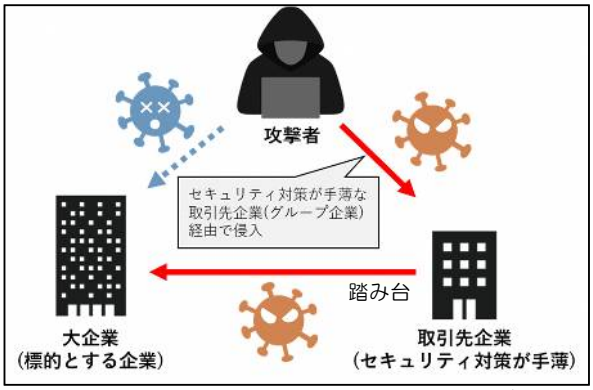
事例シリーズの第 20 弾です。今回は取引先との関係で発生する『サプライチェーンの弱点を悪用した攻撃のリスク』について検討してみたいと思います。

「2023 年版情報セキュリティ 10 大脅威」(以下「IPA 資料」)によると、**『サプライチェーン』とは**商品の企画・開発から、調達、製造、在庫管理、物流、販売までの一連のプロセス、およびこの**商流に関わる組織群**を指します。要は一般に言う“取引先”です。その中で発生するリスクは IPA 資料で「組織」の第 2 位にランクされています。話題になった事案では、部品メーカのランサムウェア被害のため国内 14 工場が稼働停止になったトヨタの例があります。取引先の情報セキュリティへの攻撃が自社の実務に重大なトラブルを引き起こしました。

(１)脅威の流れ

攻撃者は最終的な攻撃目標とする企業や機関(標的)を定めますが、標的の情報セキュリティが堅固で直接攻撃をするのが困難な場合に取引先企業の脆弱な部分を攻撃し、それによって標的の機密情報の窃取や事業継続への重大な支障を図ります。

自社の PR のため Web サイトに主要な顧客名を掲載している企業が多いですが、顧客が標的になった場合にそれを拾われ自社が踏み台になる可能性があります。



参考：株式会社インテリジェント ウェイブ HP

踏み台にされた企業は攻撃を受けたのですから被害者ではありますが、顧客からすると加害者になってしまいます。上流に顧客があり、下流に委託先・仕入先を持つ中間的な立場の企業では**下流企業の事故が上流企業にも波及する可能性があるとの認識が重要**です。

(２)事案の例

ここに 3 つの事案を紹介します。パターンとしては次葉の表のように分類でき、被害企業の機密情報の流出と業務に重大な影響を及ぼした例の両方があります。

①トヨタの例

部品メーカの小島プレス工業がマルウェア攻撃を受けたのをきっかけに(2022 年 2 月 26 日判明)、トヨタは部品の入手が不能となり 2022 年 3 月 1 日に生産を中止しました。小島プレス工業とその子会社とを接続している VPN 装置への不正侵入から、ランサムウェア被害が発生しサーバやパソコン端末の一部でデータが暗号化され業務ができなくなったためです。トヨタでは情報流出の被害はなかったようです。

②JAL の例

やや旧聞に属しますが、2017 年 12 月 20 日、JAL が偽の請求書メールに騙されて約 3 億 8000 万円の詐欺被害に遭った旨を発表しました。委託先のシステムが侵入に遭い、実在する委託先の担当者名で発信されたメールに従って不正な口座に振り込んでしまいました。

「ビジネスメール詐欺」の典型的な例として有名ですが、間違いなく“サプライチェーン”に絡む事案です。余談ですが、同時期にスカイマークも同様の攻撃を受けて振込みを実行した所、既に口座が閉鎖されて実害を免れたとのニュースもありました。

③愛知県公立大学の例

2023 年 3 月 1 日、業務を委託している NTT 西日本の PC が Emotet に感染し、過去のメール履歴として保存されていた NTT 西日本社員、同大学教職員等のメールアドレスが流出しました。翌日そのアドレスを使った第三者からの不審なメールが発信されていることが確認されています。大学では情報システムに被害は及ばなかったものの不審メール受信者からの対応に追われました。**「標的」が大企業に限らない**ことを示しています。

被害企業	事象	業務への支障	被害企業の情報流出
①トヨタ	部品会社への攻撃	1 日間の生産中止	なし
②JAL	委託先でのメールアドレス窃取	3.8 億円の誤送金	社員の氏名、アドレス
③愛知県公立大学	委託先 PC の Emotet 感染	不審メール受信者への対応	職員の氏名、アドレス

（3）予防措置の考察

個人情報保護法では「個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。」とされており、プライバシーマーク事業者に限らず全組織(企業)にとって、取引先(委託先)の業務遂行状況や情報セキュリティについて“監督”する義務があります。

一方、トヨタの事案では個人情報が関わるケースではありませんので、個人情報保護法による義務と言うよりも「内部統制」(リスクの評価と対応)に基づく“点検”になると考えます。

委託先とは基本的に守秘義務契約書(覚書)を交わします。Web サイトに公表しているセキュリティポリシーなどで代替もできますが、問題はその**“契約内容(約束事)”が守られていること**、不祥事や疑念が生じていないことであって、定期的にチェックすることが肝要です。

一つの例として、「**情報セキュリティ診断シート**」(5 分でできる！自社診断&ベンチマーク)が IPA から公開されています。https://www.ipa.go.jp/security/guide/sme/5minutes.html を開けば診断の要領が分かりますが、次頁に診断項目を掲載しました。自社の点検が主目的とは言え、委託先や仕入先での自主点検を促すためのアンケートをする際にも使えると考えます。

巨大なクラウド事業者など“監督”の言葉が馴染まない“委託先”もあります。その場合には各種の報道や公表事項に高いアンテナを張っておきましょう。

（4）まとめ

電子帳簿保存法の施行や電子取引の拡大に伴い、電子情報の授受が益々浸透して行くのは必定です。比例してサプライチェーンリスクに幅広く目を光らせないといけなくなりました。

今回は自社の各種リスク対策に留まらず、取引先に網を広げて考えていただくキッカケにな

ればとの思いで本テーマを取り上げました。P マーク審査では個人情報の取扱いに関する事項の範囲で点検しますが、会社にとっては個人情報よりも重要な情報も多々あるでしょう。自社の情報セキュリティと併せ、“委託先の監督”に関し、内部統制の観点からも会社のマネジメントサイクルのひとコマとして是非毎年(例えば)定期的に実行されるよう祈念します。

［参考］5 分でできる！情報セキュリティ自社診断シート

診断項目	No	診断内容	チェック				点数
			実施している	一部実施している	実施していない	わからない	
Part 1 基本的対策	1	Windows Update※1を行うなどのように、常にOSやソフトウェアを安全な状態にしていますか？	○	○	○	○	
	2	パソコンにはウイルス対策ソフトを入れてウイルス定義ファイル※2を自動更新するなどのように、パソコンをウイルスから守るための対策を行っていますか？	○	○	○	○	
	3	パスワードは自分の名前、電話番号、誕生日など推測されやすいものを避けて複数のウエブサービスで使い回しをしないなどのように、強固なパスワードを設定していますか？	○	○	○	○	
	4	ネットワーク接続の複合機やハードディスクの共有設定を必要な人だけに限定するなどのように、重要情報に対する適切なアクセス制限を行っていますか？	○	○	○	○	
	5	利用中のウェブサービス※3や製品メーカーが発信するセキュリティ注意喚起を確認して社内共有するなどのように、新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？	○	○	○	○	
Part 2 従業員としての対策	6	受信した不審な電子メールの添付ファイルを安易に開いたり本文中のリンクを安易に参照したりしないようにするなど、電子メールを介したウイルス感染に気をつけていますか？	○	○	○	○	
	7	電子メールを送る前に目視にて送信アドレスを確認するなどのように、宛先の送信ミスを防ぐ仕組みを徹底していますか？	○	○	○	○	
	8	重要情報をメールで送る時は重要情報を添付ファイルに書いてパスワード保護するなどのように、重要情報の保護をしていますか？	○	○	○	○	
	9	無線LANを利用する時は強固な暗号化を必ず利用するなどのように、無線LANを安全に使うための対策をしていますか？	○	○	○	○	
	10	業務端末でのウェブサイトの閲覧やSNSへの書き込みに関するルールを決めておくなどのように、インターネットを介したトラブルへの対策をしていますか？	○	○	○	○	
	11	重要情報のバックアップを定期的に行うなどのように、故障や誤操作などに備えて重要情報が消失しないような対策をしていますか？	○	○	○	○	
	12	重要情報を机の上に放置せず書庫に保管し施錠するなどのように、重要情報の紛失や漏えいを防止する対策をしていますか？	○	○	○	○	
	13	重要情報を社外へ持ち出す時はパスワード保護や暗号化して肌身離さないなどのように、盗難や紛失の対策をしていますか？	○	○	○	○	
	14	離席時にコンピュータのロック機能を利用するなどのように、他人に使われないようにしていますか？	○	○	○	○	
	15	事務所で見知らぬ人を見かけたら声をかけるなどのように、無許可の人の立ち入りがないようにしていますか？	○	○	○	○	
	16	退社時に机の上のノートパソコンや備品を引き出しに片付けて施錠するなどのように、盗難防止対策をしていますか？	○	○	○	○	
	17	最終退出者は事務所を施錠し退出の記録(日時、退出者)を残すなどのように、事務所の施錠を管理していますか？	○	○	○	○	
	18	重要情報を廃棄する場合は、書類は細断したり、データは消去ツールを使ったりするなどのように、重要情報が読めなくなるような処分をしていますか？	○	○	○	○	
Part 3 組織としての対策	19	従業員を採用する際に守秘義務や罰則規定があることを知らせるなどのように、従業員に秘密を守らせていますか？	○	○	○	○	
	20	情報管理の大切さなどを定期的に説明するなどのように、従業員に意識付けを行っていますか？	○	○	○	○	
	21	社内外での個人所有のパソコンやスマートフォンの業務利用を許可制にするなどのように、業務で個人所有端末の利用の可否を明確にしていますか？	○	○	○	○	
	22	契約書に秘密保持(守秘義務)の項目を盛り込むなどのように、取引先に秘密を守ることを求めていますか？	○	○	○	○	
	23	クラウドサービスなど外部サービスを利用する時は利用規約やセキュリティ対策を確認するなどのように、サービスの安全・信頼性を把握して選定していますか？	○	○	○	○	
	24	秘密情報の漏えいや紛失、盗難があった場合の対応手順書を作成するなどのように、事故が発生した場合に備えた準備をしていますか？	○	○	○	○	
	25	情報セキュリティ対策(上記1 ～ 24など)を会社のルールにするなどのように、情報セキュリティ対策の内容を明確にしていますか？	○	○	○	○	

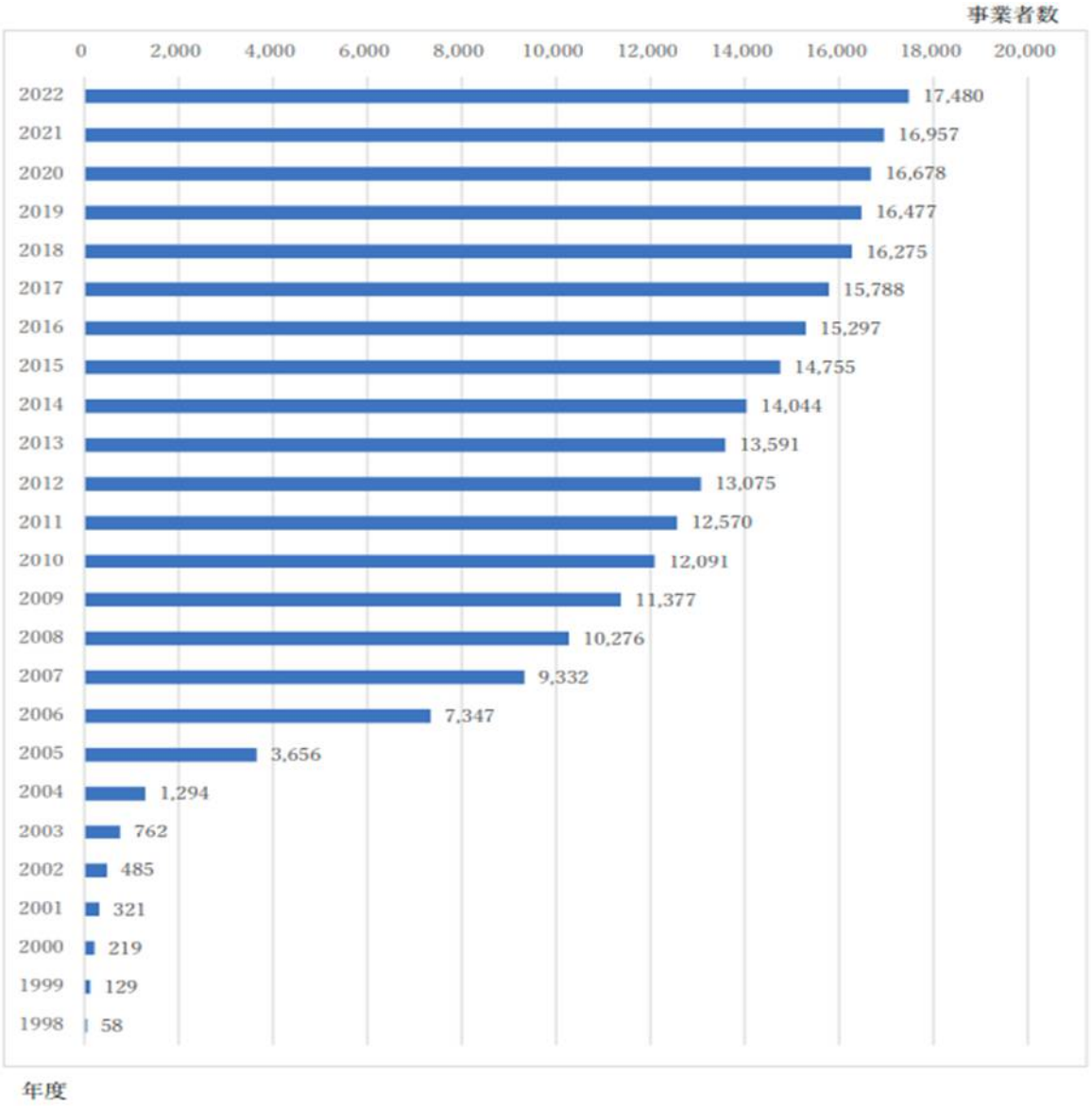
３．Ｐマーク制度が創設 25 周年を迎えました

1998 年 4 月に創設されたプライバシーマーク制度（Ｐマーク制度）は、2023 年 4 月 1 日を以って 25 周年を迎えました。1998 年の制度発足以来、個人情報の保護へ取り組んでいる事業者のインセンティブとなり、社会的に個人情報保護の意識を高めることで、一定の役割を担ってきました。その結果、現在 17,400 社の事業者がＰマークを取得しています。

そこで今回はＰマーク制度 25 年の歩みをＰマーク取得事業者数の推移で振り返ってみます。

（1）Ｐマーク取得事業者の年間増加が 3 年振りに 500 社を超えました

下図はＰマーク制度が始まってからの取得事業者の推移を表しています。



Ｐマークの現在までの増加推移には、以下の時期的な段階がありました。

①1998 年から 2002 年は制度創設の直後で、Ｐマークを取得する事業者は年間 100 社程度と僅かで、マーク制度に対する様子見といった状態が数年続きました。

なお、この時期は個人情報保護法が制定される前であり、P マークを取得した事業者には個人情報保護意識の高さが窺えます。

②2004 年から 2007 年の時期は、個人情報保護法が 2003 年 5 月に制定され、2005 年 4 月に全面施行されたことから、P マーク取得の機運が大いに盛り上がり、その増加は毎年 2000 社を超えており、P マーク取得事業者が急拡大した時期となりました。

③続く 2008 年から 2017 年の約 10 年間は、P マーク制度に対する評価も定まり、P マーク取得事業者の年間増加数は常に 500 社前後を記録するという安定的拡大期が続きました。

④ところが 2018 年から 2021 年の 4 年間は、個人情報保護法改正や JIS15001 規格の改訂があり、こうした法令や規格の変更対応に「コロナ禍」が加わり、年間増加数は従前の半分以下の 200 社前後に止まり、P マーク制度の先行きが不安視されました。

⑤直近の 2022 年から 2023 年をみると、増加数が年間 500 社を超え再び増勢に転じました。2021 年に至る前述④の動向は、P マークに対する事業者の評価・期待が低下しているのではないかとの見方もありましたが、2022 年の動きはそんな不安を払拭するものになりました。ただし、2022 年の増加が一時的なものなのか、上記③と同様の動きを取り戻すのか 2023 年以降の動向が注目されます。

（２）直近 5 年間の業種別Ｐマーク取得動向

下表に業種別の P マークの取得事業者数の動向を直近 5 年間について調べてみました。なお、表にある「増減%」は 2023/3 と 2019/3 を対比したものです。

業種区分	2019/3	2020/3	2021/3	2022/3	2023/3	増減%
建設	299	309	313	320	336	12%
製造業	1,472	1,475	1,459	1,434	1430	▲3%
電気・ガス水道	21	22	22	22	23	5%
運輸・通信	745	753	750	749	777	4%
卸・小売り・飲食	896	903	914	943	977	9%
金融・保険	280	269	259	260	270	▲4%
不動産	**236**	**244**	**263**	**273**	**294**	**25%**
サービス業	12,326	12,520	12,698	12,956	13,373	8 %
合計	16,275	16,477	16,678	16,957	17,480	7 %

①上表に示した 5 年間は、（１）の④の推移説明の通り、P マーク取得事業者の増加は低調期に当たり、全体的に取得事業者数の増加は 2018 年以前に比べて少なくなっています。

②P マーク取得事業者数の増加で目を引く業種が不動産業です。5 年間で 25%アップしています。不動産業界において個人情報保護意識が近時急速に高まっていることが窺えます。

③逆に 5 年間で P マーク取得事業者を減少させたのが、「製造業」と「金融・保険業」です。特に製造業は 2020 年以降毎年減少しているのが気掛かりです。同じ減少組の金融・保険業は、2021 年以降やや持ち直し傾向を示しています。その要因としては P マークを新規取得した保険代理店が 2021 年、2022 年と続けて年間 11 社があったことが挙げられます。

４．お知らせ（トピックス）

業務研修の一環としてご好評を戴いている弊社の損保／生保公開講座について６月から８月の予定をご案内します。

①日程

時期	損保講座基本コース	生保講座基本コース
2023 年 6 月	6 月 15 日（木）	6 月 21 日（水）
2023 年 7 月	7 月 20 日（木）	7 月 19 日（水）
2023 年 8 月	8 月 17 日（木）	8 月 16 日（水）

（注）新型コロナが収束するまでは、研修は原則リモート（ZOOM）形式で行っております。

②講座の内容

【損保講座基本コース】

- 受講対象者：損保関連業の未経験者から経験 3，4 年程度の方
- 講座内容

－損害保険の概要（仕組み、損害保険会社の規模・組織など）

－損害保険商品の種類、自動車保険、火災保険の仕組み

―保険契約の契約業務、保険販売(代理店）の詳細

―損保システムの概要、特色

【生保講座基本コース】

- 受講対象者：生保関連業の未経験者から経験 3，4 年程度の方
- 講座内容

－生命保険の概要（仕組み、生命保険会社の規模・環境など）

―生命保険商品の種類、仕組み

―生命保険の業務

―生保システムの概要、特色

③申し込み方法

弊社ホームページよりエントリーをお願いします。

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。お気軽にどうぞ！

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）