PIA の取組の促進について

―PIA の意義と実施手順に沿った留意点―

2021 年 6 月 30 日

個人情報保護委員会

目次

はじめに

デジタル社会の進展により、個人情報を含む個人に関する情報[1]（以下「個人情報等」という。）の利活用が著しく拡大している。個人情報等を利活用した新たな事業・サービスは、消費者に様々な利便性を提供する一方で、その利活用の手法が複雑化、多様化していることに伴い、事業者が個人情報等を適正に取り扱っているかについて、消費者の不安感が高まっている。事業者においては、個人情報等を取り扱うに際し、個人の権利利益の保護の重要性を十分に認識し、自らの事業が個人の権利利益にどのように影響を与えるかを的確に理解した上で、個人情報等を適正に利活用することが求められている。

個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）に規定する義務は、あらゆる分野を対象とする法の性格上、必要最小限度の規律であることから、事業者においては、個人情報保護法の遵守の範囲にとどまらず、自身が取り扱う個人情報等の性質、利用方法、取扱いの実態等に即した個人の権利利益の保護についての自主的な取組が期待されている。

また、個人情報保護法は、利用目的の通知・公表、安全管理措置の実施、第三者提供時の同意取得、本人からの開示等の請求等への対応等、主に手続面から規定が設けられているが、個人の権利利益の保護を実体面からも担保すべく、個人情報の保護に関する法律等の一部を改正する法律（令和２年法律第 44 号。以下「令和２年改正法」という。）において不適正利用の禁止規定が新設され、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よる個人情報の利用が禁止されたところである。このことからも、事業者においては、形式的な法令遵守を超えて、個人情報等の取扱いの性質等に着目した実質的な個人の権利利益の保護を行った上での、適正な利活用が求められている。

事業者における個人情報等の取扱いについては、違法又は不当な事案が発生した場合の事後的な対応コストが大きいことが特徴として挙げられる。一般的に、システムの稼働後にリスクが顕現化した場合には、機器の交換やシステムの改修などが必要となるため、設計時に対策を行った場合に比べて、多大なコストや手間がかかることが指摘されている。また、一度漏えい等した個人情報等を回収するなど、事故等が発生する前の状態に消費者との関係を戻すことは不可能であり、個人情報等の取扱いに係る事案によって失墜した消費者からの信頼を回復することは容易ではない。

このような観点から、個人情報等を取り扱うにあたっては、事後における対処療法的な対応ではなく、個人情報等の保護を含む個人の権利利益の保護を事業の設計段階で組み込

[1] 個人に関する情報には、個人情報保護法で規定されているものに限定されるわけではなく、情報通信技術の高度化などの環境の変化を受けて、個人情報保護法の外縁部分にあるものも含めた、より幅広い、個人に関するあらゆるデータに対する配慮が求められるようになっている。本稿が説明する PIA においては、法令遵守にとどまらない範囲を自主的に対応することも重要であり、個人情報保護法上の個人情報を含む個人に関する情報という形で説明を行うこととする。

み、上記のような事後の改修費用の増嵩や信用毀損等の事態を事前に予防することが肝要である。こうした事前の対策を重視し、事業全体を通じて計画的にプライバシー保護の取組を実施する考えは「プライバシー・バイ・デザイン（Privacy by Design)」と呼ばれ、国際的にも重視されている。この「プライバシー・バイ・デザイン」の考えを実践する手法の一つがPIA（Privacy Impact Assessment、個人情報保護評価）である。

「個人情報保護法 いわゆる３年ごと見直し 制度改正大綱」（以下「制度改正大綱」という。）においては、PIAについて、「個人データの管理や従業員への教育効果等も含め、事業者自身にとって、効率的かつ効果的に必要十分な取組を進めるための有用な手段である」と評価している。また、個人情報等に係る本人を含む利害関係者の関心が増大する中、PIAは、事業者が個人情報等の取扱いに関する説明責任や透明性を確保するために有用な手法であると考えられる。

もっとも、現状、我が国の事業者においては、PIAが十分に浸透しているとは言い難い。その背景として、PIA の意義や必要性が多くの事業者において理解されていないことや、あるいは必要性を感じている事業者においても、PIA の実施手順・方法が分からない場合も少なくないことが挙げられる。

本稿は、制度改正大綱において、PIAについて、「民間の動向を踏まえつつ、民間の自主的な取組を促進することが望ましい」とされていることも踏まえ、PIAを促進する上で、事業者、消費者、認定個人情報保護団体をはじめとする関係団体等の関係者に、PIAの意義や手順を知っていただく必要があるため、お示しするものである。

なお、PIAの実施方法は、事業の規模、性質や取り扱われる個人情報等の内容等によって様々であると考えられる。したがって、本稿で示した実施手順によりPIAの手法が限定されるわけではなく、既に自主的にPIAを実施している事業者においては、その取組による蓄積を土台にしつつ、本稿で示した留意点等も参考にして更なる優良な取組が行われることが期待される。

Ⅰ．PIA の意義

１．PIA の考え方

PIA は、個人情報等の収集を伴う事業の開始や変更の際に、プライバシー等の個人の権利利益の侵害リスクを低減・回避するために、事前に影響を評価するリスク管理手法である[2]。

PIA の具体的な手順等については後述するが、PIA は、事業の企画・設計段階から個人情報等保護の観点を考慮するプロセスを、事業のライフサイクルの中に組み込むこととともいえる。こうした企画・設計段階からプライバシー対策をとることについて、よりポジティブにとらえる考え方として、「プライバシー対策をコストとしてではなく、むしろ商品やサービスの品質を高めることとして捉えるべきである」といった指摘も存在する[3]。確かに、PIA を実施するには、人的リソース等の一定のコスト負担を要するが、事後的に消費者から批判に晒されたり、関係当局による是正指導等の対象となるなどして、事業自体を断念するような例もある中、個人情報等を取り扱う事業を円滑に行っていくために、消費者の信頼を得ることは不可欠であり、そのためにも PIA は有効な手法である。

なお、PIA は基本的には企画・設計段階での実施が想定されているが、その後の段階で必要性を認識する等により実施する場合でも、具体の権利利益の侵害が発生する前にリスクを認識し、必要な対応策を講じることができる場合もあるため、設計を終えた後の段階における PIA の実施にも一定の意義が認められる。また、PIA は、システム構築の関連で語られることが多いが、個人情報等を取り扱う事業であれば、システムの構築等を行わない場合であっても有用である。さらに、PIA は、事業の新規実施時のみならず、既存事業の見直しにも有効である。

PIA の対象範囲については事業の規模や性質等によっても異なるが、最終的に消費者本人の個人情報等の保護を含む権利利益の保護にどれだけ資するかということが重要である。したがって、消費者本人から個人情報等を取得する場面やその個人情報等を利用して当該本人にサービスの提供を行う場面等、個人情報等の取扱いにより影響を受ける消費者との関係を整理し、場面ごとに個人情報等のリスクを適切に評価することが不可欠である。また、事業を主体的に実施する事業者本体のみならず、個人情報等にアクセスして取り扱う可能性がある委託先など、事業に関わる利害関係者を含めて実施することが望ましい。

さらに、PIA の対象として、個人情報保護法の規律のみならず、消費者の不安や懸念を払拭するために、個人情報保護法の遵守にとどまらない範囲も含めて対応することが重

---

[2] JISX9251:2021（情報技術－セキュリティ技術－プライバシー影響評価のためのガイドライン）では、PIA について、「個人識別可能情報の処理に関する潜在的なプライバシー影響の、特定、分析、評価、協議、伝達及び対応の計画を立てるための全体的なプロセスであって、組織のより広範なリスクマネジメントの枠組みに組み込まれたもの。」と定義している（同規格 3.7）。

[3] 総務省・経済産業省「DX 時代における企業のプライバシーガバナンスガイドブック ver1.0」（2020 年８月）（https://www.meti.go.jp/press/2020/08/20200828012/20200828012-1.pdf）P9。

要である。例えば、PIA の対象事業が個人関連情報[4]を取り扱う場合において、その影響を評価し、個人の権利利益保護のための対策を講じるといった取組は、消費者との関係で望ましいものと考えられる。

PIA の実施範囲や取り組む視点については、事業分野毎に共通している部分もあると考えられ、その意味で、認定個人情報保護団体をはじめとした業界団体等が、その事業分野における PIA を実施するための基準や対象範囲、評価項目等を整理して、必要に応じてその構成員に共有していくことは有効である[5]。また、当該団体等が、事業者が実施した PIA の妥当性を第三者の立場から評価することは、PIA の信頼性を高める上で非常に有効である。

上述のとおり、PIA は、個人情報等の取り扱いに係る影響を評価し、評価結果を基に対策を講じることで、個人の権利利益の保護の実現と事後的な問題発生の防止を図るものであるが、PIA を実施することによる主な効果としては、以下が挙げられる。

① 消費者をはじめとする利害関係者からの信頼性の獲得
② 事業のトータルコストの削減
③ 従業者の教育を含む事業者の個人情報等の取扱いに関するガバナンスの向上

①の消費者をはじめとする利害関係者からの信頼性の獲得については、個人情報等の取扱いに係るリスクが顕在化したり、事故が発生した場合、消費者等の不安や不満が高まり、場合によっては事業の継続が困難となる場合も考えられる。PIA は、個人情報保護法等の法令を遵守していることや、個人の権利利益を侵害するリスクを低減するために適切な対応を実施した旨の証明となり、消費者等の不安や不満を軽減し、レピュテーションリスクを低減する手段として有効であり、事業の実施にあたり、事業者が個人情報等を保護する取組を行っているという社会的な信用を得ることに資する。

後述するが、PIA の実施結果を公表する等して、消費者をはじめとする利害関係者とリスク対策等を共有することにより、説明責任を果たし透明性を高めることができ、消費者・事業者間の情報の非対称性の解消に資することになる。

②の事業のトータルコストの削減については、事業の企画・設計の段階で PIA を実施し、個人情報等の取扱いに係るリスクを把握した場合、多額のシステム投資をする前に、必要な軌道修正を行うことが可能となる。一度事業が開始された後に実際に消費者の権利利益の侵害が発生すると、当該消費者への補償や、システムの修正に多大なコストがかかることにもなり、場合によっては、やむなくその事業を中止せざるを得なくなり、

---

[4] 個人関連情報は、令和２年改正法により新設され、条文上、「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」と定義しており、例えば、氏名と結びついていないインターネットの閲覧履歴、位置情報、クッキー等が含まれ得る。

[5] 第 164 回 個人情報保護委員会「改正法に関連するガイドライン等の整備に向けた論点について（認定個人情報保護団体制度）」（https://www.ppc.go.jp/files/pdf/210126_shiryou-2.pdf）p10。

これまでの投資が全て無駄になることにもなりかねない。PIA は、こうした事態を未然に防止するための有効な手段であり、結果として事業のトータルでのコスト負担を抑えることが可能となる。

実際に PIA を実施している事業者からは、「システム完成後にシステムを作り直すのではなく、システムの設計段階でリスク評価しておくことで、コスト削減につながっている」といった評価が聞かれている。

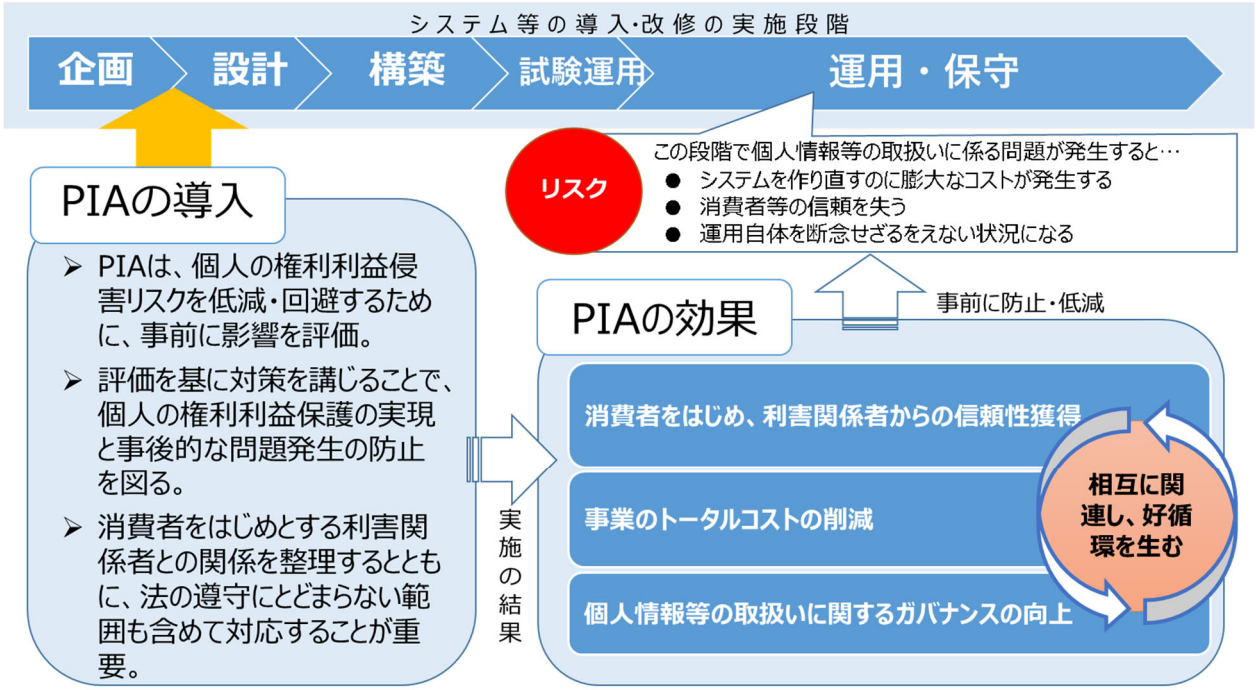
③の従業者の教育を含む事業者の個人情報等の取扱いに関するガバナンスの向上については、実際に事業に取り組む従業者が事業の企画段階で PIA に携わることで、個人情報等の適正な取り扱いの必要性について自覚を持つのみならず、その過程で法令の内容の確認等を行うことを通じて、教育効果ももたらされると考えられる。

経営層にとっても、PIA の実施により、自社の個人情報等の取扱状況とそのリスクを把握することができるため、組織としての個人情報等の取扱いに関するガバナンスの向上に資することとなる。事業者においては、個人情報等の保護などへの対応を有効に機能させるために、PIA の実施を総務部署や法務・コンプライアンス部署、システム部署、業務運営部署などの担当部署任せにするのではなく、経営層も関与する形で行うことが肝要である。

実際に PIA を実施している事業者からは、「社内における個人情報等の利活用実態を把握できるようになり、個別の案件においてチェック機能が働くようになった」、あるいは「業務に携わる社員のデータ活用におけるプライバシー保護意識が向上するとともに、個別案件について、部門を横断して助言ができるようになった」といった効果が確認されている。

なお、これらの効果は相互に関連する。例えば、PIA の実施が結果的にコストの削減につながるとともに、消費者をはじめとする利害関係者の信頼を醸成する。こうした効果は経営層・従業者の更なる意識付けにつながり、個人情報等の取扱いに関するガバナンスの向上に資する。ガバナンスが向上すれば、更に PIA の取組が進み、それが新たなコスト削減や更なる信頼性の向上を生む。このように、PIA の実施により、様々な効果が創出されるとともに、その効果の好循環が生まれることが期待される。

図表１　PIA の意義・効果



２．国内外の動向

PIA はこれまで欧米を中心に先行して実施されている状況であり、デジタル化の進展やそれに伴う個人情報等の取扱いに係る問題が顕在化する中で、1990 年代以降、米国、カナダ、ニュージーランド、オーストラリア、韓国等で導入されている[6]。これらのうち、米国や韓国など法令に基づき PIA の実施を求めている国もあるが、その対象は行政機関となっている。

こうした中、EU の GDPR（General Data Protection Regulation、一般データ保護規則）において、法制度としては初めて民間事業者に対して PIA の実施が義務付けられている[7]。

また、国際規格の分野では、2008 年には金融機関向けに開発された PIA に関する国際規格 ISO 22307：2008（Financial services - Privacy Impact Assessment）、2017 年には民間企業、政府機関、非営利団体など、あらゆる種類及び規模の組織向けに開発された国際規格 ISO/IEC 29134：2017（Information technology - Security techniqu

[6] 瀬戸洋一編著『ISO/IEC 対応　プライバシー影響評価実施マニュアル』（日科技連出版社、2020 年）P3。

[7] GDPR では、DPIA（Data Protection Impact Assessment）と呼称され、「取扱いの性質、範囲、過程及び目的を考慮に入れた上で、特に新たな技術を用いるような種類の取扱いが、自然人の権利及び自由に対する高いリスクを発生させるおそれがある場合、管理者は、その取扱いの開始前に、予定している取扱業務の個人データの保護に対する影響についての評価を行わなければならない」とされている。

es – Guidelines for privacy impact assessment）が発行され、実施手順や報告書の構成等の推奨事項が示されている。

なお、これらの法令や国際規格に基づいて実施するケースのみならず、海外においては、データ保護の取組による消費者の信頼確保が不可欠であるとの認識の下、実施手順を自ら構築する等して、自主的にPIAを実施している事業者も存在する。

我が国では、公的部門において、特定個人情報保護評価の実施が法定されている[8]。一方、民間部門においては、PIAについて法令による規定はなく、制度改正大綱においても、現時点において、評価の項目や手法等を規定して義務化することは、民間部門における自主的な取組を阻害するおそれもあり、まずは自主的な取組によって行われることが重要であるとの考え方を示したところである。

こうした中、国内では、2021年1月に上記の国際規格ISO/IEC 29134：2017を翻訳したJISX 9251：2021（情報技術－セキュリティ技術－プライバシー影響評価のためのガイドライン）が発行されている。

国内では一部の事業者がPIAを実施しているものの、社会に十分に浸透しているとはいえない。上述のとおり、PIAの意義や実施方法が十分に理解されていないことが一因と考えられるが、今後、JISX 9251：2021の発行等も契機に、PIAの取組が広がっていくことが期待される[9]。

[8] 国の行政機関や地方公共団体等がマイナンバーを保有する前に自ら情報漏えい等のリスクを評価し、その対策について書面に記載して公表する制度であり、行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）第28条に規定されている。

[9] ISO 22307：2008、ISO/IEC 29134：2017やJISX 9251：2021は、主に個人情報等を処理するシステムの設計時等におけるリスク評価に関する規格であるが、別途、個人情報等の保護について、ISO/IEC 29100：2011（Information technology－Security techniques－Privacy framework）、ISO/IEC 27001：2013（Information technology-Security techniques-Information security management systems-Requirements）、JIS Q 27001:2014（情報技術―セキュリティ技術－情報セキュリティマネジメントシステム－要求事項）、JIS Q 15001：2017（個人情報保護マネジメントシステム－要求事項）といったマネジメントに関する規格がある。

Ⅱ．PIA の実施手順に沿った留意点

事業者の PIA についての理解促進等に資するように、PIA の実施手順と各段階における基本的な留意点を、以下において示すこととする。

ここで示す実施手順等は、JISX 9251：2021 の内容も参考に一例として記載したものであるが、上述のとおり、対象となる事業の規模、性質や取り扱われる個人情報等の内容等によっても変わってくる。

既に、独自にリスク評価のためのフォーマットを作成し、サービスの設計段階からリスク評価を行うことができる体制を整備するなど、自主的に PIA の手法を検討し、実施している事業者も存在する。PIA は、あくまで個人情報等の取扱いを伴う新規事業等における個人の権利利益の侵害リスクについて、事前の影響評価を行うことにより、必要な対策に繋げていくことが目的であるから、その実施手法は、事業者のリソース等も踏まえ、最終的には事業者自身において、最適な手法を考慮していくことが重要であり、画一的なものではない。

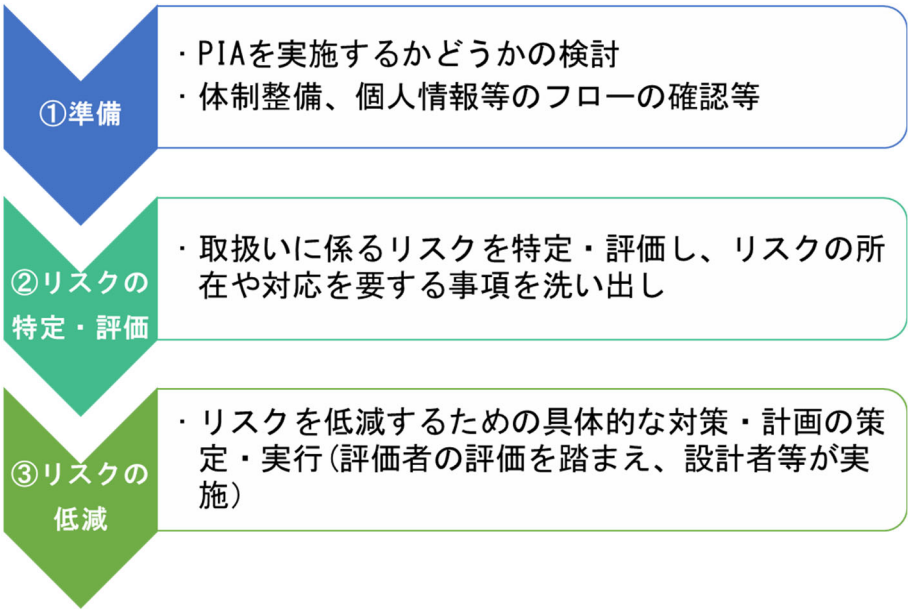
その上で、PIA の一般的なプロセスを大別すると、①準備、②リスクの特定・評価、③リスクの低減に分けることができる（図表２参照）。

①の準備については、PIA を実施するかどうかを検討した後、PIA を実施するための体制の整備や、個人情報等を取り扱う事業における当該個人情報等のフローを確認する等の多角的かつ幅広い情報収集・整理を行うプロセスである（下記１及び２）。

②のリスクの特定・評価については、①の準備をもとに、評価者が個人情報等の取扱いに係るリスクを具体的に特定・評価し、重大なリスクの所在や、リスクを低減するための対応を要する事項を洗い出すプロセスである（下記３及び４）。

③のリスクの低減については、②で評価者が特定・評価したリスクを低減するための具体的な対策・計画を、設計者等が策定し実行するプロセスである（下記５）。

図表２　一般的な PIA のプロセス



１．PIA の実施要否の検討

個人情報等を取り扱う業務の実施もしくは見直し等に際して、幅広く、PIA を実施する必要があるのか否かを検討する。

PIA を実施する過程で想定していなかったリスクが発見される可能性もあり、様々な事業で実施されることが重要である。例えば、要配慮個人情報や生体認証データ等機微な情報を取り扱う場合、取得した個人情報等から本人の行動・関心等の分析を行ういわゆる「プロファイリング」の結果を利用する場合、委託・共同利用により他の事業者とともに個人情報等を取り扱う場合などに、PIA を実施することが有効と考えられる。

その他、例えば、JISX 9251：2021 においては、個人情報等の取扱いに関する規定・業務フロー・データフロー等の変更、事業の拡大又は買収といった場合に、PIA の実施が推奨されている。

また、GDPR においては、「特に新たな技術を用いるような種類の取扱いが、自然人の権利及び自由に対する高いリスクを発生させるおそれがある場合」に PIA を実施することとなっている（第 35 条）[10]。

---

[10] とりわけ、以下の場合に求められるとされている。なお、「データ保護影響評価（DPIA）及び取扱いが 2016/679 規則の適用上、「高いリスクをもたらすことが予想される」か否かの判断に関するガイドライン」において、事例も含めて実施基準の解説がなされている。

（a）プロファイリングを含め、自動的な取扱いに基づくものであり、かつ、それに基づく判断が自然人に関して法的効果を発生させ、又は、自然人に対して同様の重大な影響を及ぼす、自然人に関する人格的側面の体系的かつ広範囲な評価の場合

（b）第 9 条第 1 項に規定する特別な種類のデータ又は第 10 条に規定する有罪判決及び犯罪行為と関連する個人データの大規模な取扱いの場合

（c）公衆がアクセス可能な場所の、システムによる監視が大規模に行われる場合

しかしながら、どのような場合に PIA を実施するかについては、事業者及び実施する事業の内容によって様々である。例えば、既に PIA を実施している事業者においては、新規案件や新サービスを開始する際には必ず PIA を実施することとしていたり、独自のチェックリストを作成し、一定の基準に該当した場合に実施することとしているなどの取決めをしている例もみられる。このように、あらかじめ事業者において、PIA の実施基準を定めておくことも有効である。

２．PIA の準備

（１）体制の整備

PIA を実施することを決定した場合は、PIA を実施するための体制を整備する必要がある。具体的には、実施責任者の任命、投入人員数などリソース計画、スケジュールの策定が挙げられる。

こうした準備にあたり、経営層が PIA の必要性等を理解・認識した上で、必要なリソースを割り当てることにコミットすることが重要である。

実施責任者については、事業者によって責任者の職位等のレベルは様々考えられるが、PIA の対象とする業務プロセスについての理解力とリスクの評価、対策の検討等に際しての適切な判断力を有する者である必要がある。

投入人員について、PIA は法令、システム面等様々な視点から評価を行う必要があるため、事業を実施する部門のみならず、法務部門やシステム部門等の人材も組み込みながら、責任者も含めて、評価者として数人程度のチームを組成することが考えられる。

なお、外部有識者も含む第三者機関を設置して、事案に応じて、チームが実施した評価及び検討した対応策について当該第三者機関が審議を行うといった方法も有効である。

所要期間については、最終的な事業の開始時期等を考慮する必要があるが、数週間から数か月程度での実施が考えられる。

事業の性質等によって適切な投入人数や所要期間が異なってくる点には留意が必要である。

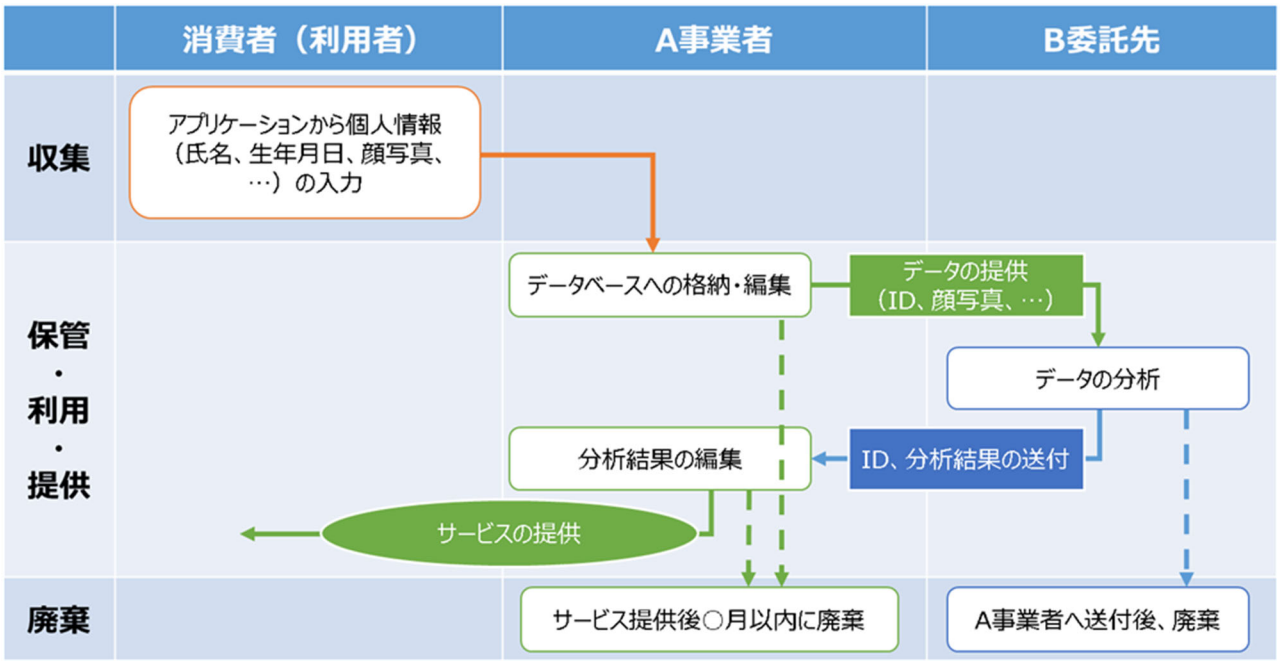
（２）個人情報等のフローの整理

個人情報等の取扱いに係るリスクを評価する前提として、個人情報等がどのように取り扱われるかを関係者間で適切に共有して確認できるように、個人情報等のフローを整理しておく必要がある。この整理にあたっては、個人情報等の収集・保管・移転・利用・廃棄といったプロセスごとに整理し、フローを可視化・詳細化しておくことが有効である（図表３参照）。

フローを整理するにあたっては、個人情報等の取扱いに係る利害関係者を明確にフロー図の中に組み込むこと、換言すれば関係主体として示しておくことが重要である。利害関係者として、個人情報等を取得・利用する事業者、個人情報等の取扱いにより影響を受ける消費者等の個人、委託先等が挙げられる。PIA は、導入するシステム等のオペレーション主体である事業者等に限定した分析ではなく、消費者との関係性を明確にした分析であることが求められる。

個人情報等の収集方法や利用の目的、処理の方法等を明確に分かるように整理しておくことが重要である。

図表３　フロー図のイメージ



（３）関係法令等の整理

個人情報等の取扱いに係る消費者等の権利利益の侵害リスクを評価するために、評価の根拠・要件を漏れなく洗い出して整理しておくことが必要である。

法令に違反する事項がないか等の確認は、リスク評価において当然に必要であるため、個人情報保護法をはじめとする関係法令を整理しておく必要がある。

次に、PIA においては、法令の遵守にとどまらず、消費者等の不安や懸念を払拭するための評価も求められるため、当該事業分野に関して公的機関が示した指針や、認定個人情報保護団体の個人情報保護指針等の業界自主ルール、自社の規程・契約・関連するセキュリティ管理策等を洗い出して整理しておく必要がある。

３．リスクの特定

個人情報等の取扱いに係るリスクの特定においては、上記２（２）において整理したフローの段階ごとに、上記２（３）で整理した根拠・要件に基づいた消費者等の個人の権利利益がリスクに晒されていることはないかといった観点のほか、事業者側のオペレーションなどに伴い想定されるリスク要因、消費者・利用者側の利用方法などに伴うリスク要因なども踏まえて、これを洗い出し、整理することが求められる。

事業者側のリスク要因として、以下の着眼点が考えられる[11]。なお、これらはあくまで例示であり、リスク要因は、事業の性質等によって変わり得ることに留意が必要である。

- 利用目的の通知や同意の取得が本人に分かりやすい形で行われるか。
- 本人が、自らの個人情報等がどのように取り扱われることとなるか、利用目的から合理的に予測・想定できるか。
- 個人情報等が過剰に収集される可能性がないか。
- 本人からの各種請求への対応は滞りなく行われるか。
- 権限のない者が個人情報等に不正にアクセスする可能性がないか。
- 個人情報等の紛失、盗難又は不正に持ち出される可能性がないか。
- 不適正な個人情報等の編集、紐づけ、分析等の利用が行われる可能性がないか。
- 不必要に保有し続ける情報がないか。

消費者等側のリスク要因については、事業者側で想定している利用方法として意図していた行動とは異なる行動（デバイスの誤操作・誤設定、機器の紛失等）があり得ることも踏まえて、リスクを特定していく必要がある。

以上を踏まえたリスクの洗い出しを行い、図表４のようなリスク整理表を作成することが有効である。リスク整理表においては、個人情報保護法等の法令により求められること、公的機関の指針や業界ルールにより求められること、それ以外に事業の性質上求めることが望ましいと考えられること等の区別を明確にしていくことが望ましい。

---

[11] JISX9251:2021 においては、プライバシーリスクを特定する観点として以下を上げている。
— PII（個人識別可能情報）への認可されていないアクセス（機密性の喪失）
— PII への許可されない変更（完全性の喪失）
— PII の紛失、盗難又は許可されていない持ち出し（可用性の喪失）
— PII の過剰収集（運用管理の喪失）
— PII の処理目的に関する情報提供不十分（透明性の欠如）
— PII 主体の権利への考慮の欠如（例：アクセス権の喪失）　　等

図表４　リスク整理表のイメージ

	個人情報保護法	○○事業ガイドブック	その他
収集	・利用目的が通知・公表されているか ・不正な取得がなされていないか …	・同意の取得や通知が本人に分かりやすい形で行われているか。 …	・事業に不要な情報まで収集していないか …
保管	・内容の正確性が確保されているか ・必要かつ適切な安全管理措置が講じられているか …	・示されているセキュリティ対策がなされているか。 …	・各種請求対応は円滑に行われるか。 ・消費者による機器の紛失等の際の処理が適切になされるか。 …
利用	・目的外の利用がないか ・不適正な利用がなされていないか …	・推奨されている手順に沿って利用がなされているか …	・処理のログが取られているか ・不適切な編集・分析が行われる可能性はないか …
提供	・第三者提供時にあたり同意を取得することとされているか …	移転先が本人に明示されているか …	・移転する情報は必要かつ最小限なものとなっているか …
廃棄	・必要ない情報は廃棄されているか …	・保存期間が設定されているか …	・廃棄時に複数人で確認されるか …

４．リスクの評価

上記３で特定したリスクについて、「影響度」及び「発生可能性」の観点で評価を行う。リスク評価の基準は、定量的な基準を設定することは困難と考えられるため、図表５のような数段階（無視できる、限定的、重大、甚大等）の基準を設定することが考えられる。

図表５　評価基準の例

（影響度）

レベル		基準
4	甚大	・利用者に回復不可能な多大な不利益が生じ、これに伴い、企業の信用失墜や経済的損失が生じる （心理的・身体的疾患、口座番号、暗証番号の流出等）
3	重大	・利用者に一定の不利益が生じるものの、回復可能であり、企業の信用等への影響はそれほど大きくない （迷惑メールの受信、アカウントの乗っ取り等）
2	限定的	・一部の利用者に不安感を与え、企業の信頼等に影響が及ぶ可能性があるが、その範囲は限定的 （サービスへのアクセス拒否、利用方法に関する説明不足等）
1	無視可	・利用者への不利益の程度は極めて小さく、企業への影響は無視できるレベル （同意取得時にアプリケーション上にチェックを入れる煩わしさ等）

（発生可能性）

頻度		基準
4	非常に高い	・安全管理等に不備があるため、リスク発生が容易に想定される （セキュリティ対策の不備で情報漏えい等が発生する等）
3	ある程度高い	・安全管理の一部に不備があるため、リスク発生の可能性がある （ノートPCや携帯電話などのモバイルの紛失等）
2	一定の可能性	・安全管理措置により、リスク発生の可能性は低い （注意喚起のメッセージが表示される中でのメール誤送信等）
1	非常に低い	・リスク発生の可能性は極めて低い （入館証読取機でセキュリティ対応の採られた室内の書類の紛失等）

（出典）美馬正司「民間における PIA の取組（企業におけるプライバシー保護の勘所）」（https://www.jipdec.or.jp/library/report/20210225-3.html）p20 を一部加工

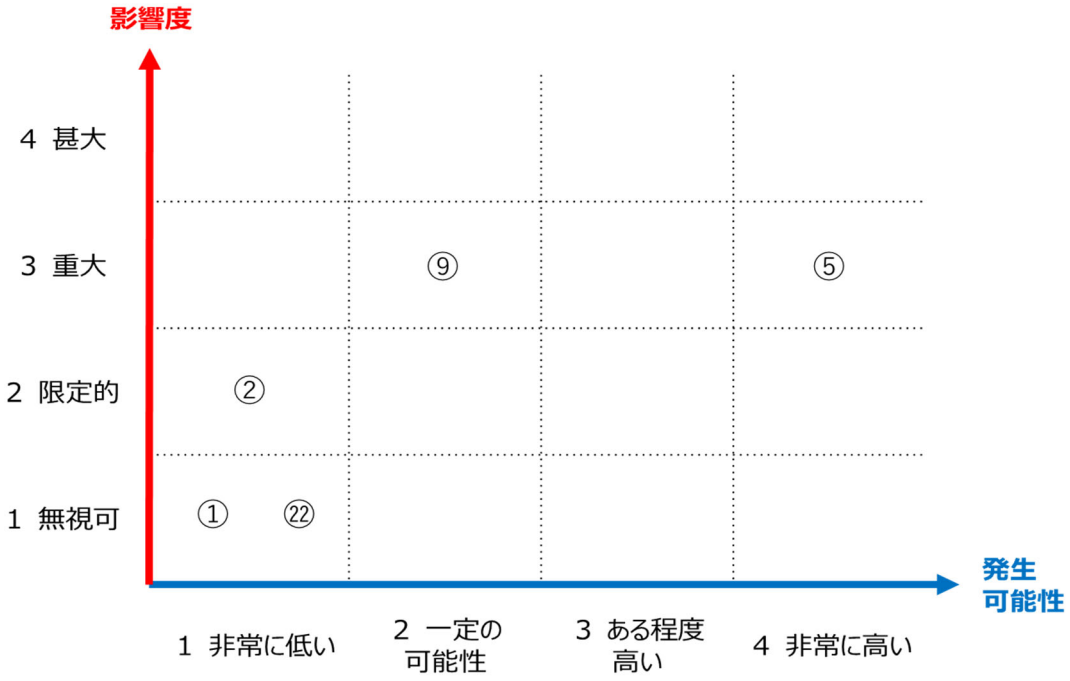
上記のような基準に従い、特定した各リスクについて、想定されている個人情報等の取扱内容等に照らし、影響度及び発生可能性を評価していく（図表６参照）。

図表６　評価表のイメージ

	特定したリスク	取扱状況、措置等	影響度	発生可能性
収集	①利用目的の通知や同意の取得が本人に分かりやすい形で行われるか	図も含めてアプリケーション上に内容を表示し、チェックを入れる設計となっている	1	1
	②事業に不要な情報まで収集されていないか	一部、利用目的と関連のない情報を取得する設計となっている	2	1
	…	…	…	…
保管	⑤○○事業ガイドブックに示されているセキュリティ対策がなされているか	一部、実施できていないセキュリティ対策がある	3	4
	…	…	…	…
利用	⑨処理のログが取られているか	ログは取るようにしているが、容易に編集・削除できるようになっている	3	2
	…	…	…	…
…	…	…	…	…
廃棄	㉒必要ない情報は廃棄されているか	サービス提供後、○月以内に廃棄されることとしている	1	1
	…	…	…	…

上記の作業実施後、各リスクの分布を総覧的に把握し、対策を講じる優先度等の検討を行いやすくするため、影響度と発生可能性の二軸のリスクマップを作成することが考えられる（図表７参照）。

図表７　リスクマップのイメージ



５．リスクへの対応

上記４で評価者が評価したリスクについて、まずは設計者等が対応方針[12]を決定していくことが考えられる（図表８参照）。

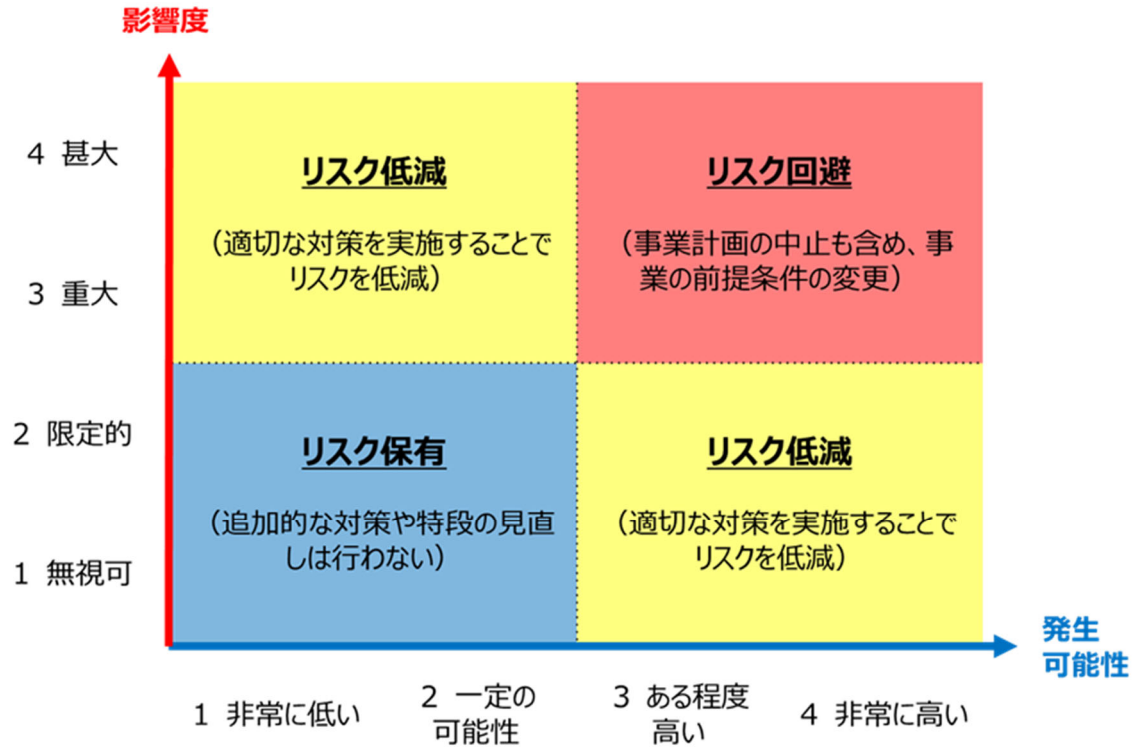
影響度が高く、発生可能性も高い場合は、事業者は事業計画の中止も含め、事業の前提条件の変更などリスク回避行動を取ることが考えられる。

影響度は低いものの、発生可能性が高い場合、もしくは影響度は高いものの、発生可能性が低い場合は、適切な対策を実施することでリスクを低減させることが考えられる。

影響度が低く、発生可能性も低い場合は、追加的な対策や特段の見直しは行わず、そのままリスクを保有するといった選択肢もあり得る。

[12] JISX9251:2021 には、対応方針の選択肢として、リスク回避、リスク保有、リスク低減の他に、リスク移転が挙げられている。これは、特定のリスクを委託先などの外部の当事者に移転するような意思決定であるが、移転先で適切なリスク低減策が講じられなければ、事業全体として同様のリスクが残存していることに変わりないことに留意が必要である。

図表８　対応方針の例



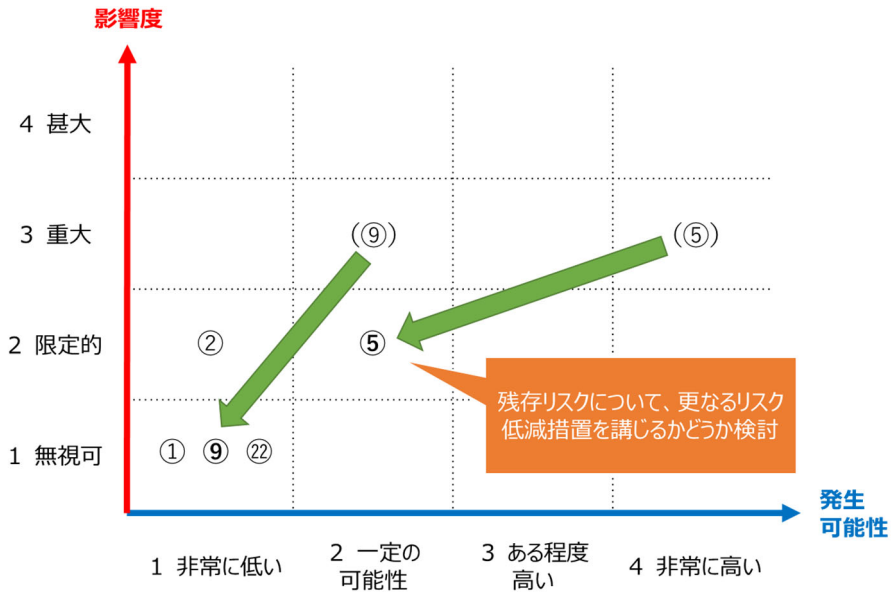
上記の対応方針を踏まえて、リスク保有部分を除き、設計者等は具体的な対応策を検討する。特定したリスクによって、対応策は様々であるが、例えば、ログを容易に編集・削除できるといったリスクが特定された場合、対応策としては、ログにアクセスできる者を限定し、また監査部門がシステム監査を行うこと等が考えられる（図表９参照）。

図表９　対応策の例

特定したリスク	想定していた取扱状況、措置等	対応策
…	…	…
⑤○○事業ガイドブックに示されているセキュリティ対策がなされているか。	一部、実施できていないセキュリティ対策がある	・推奨されているセキュリティ対策を実施 ・ …
…	…	…
⑨処理のログが取られているか	ログは取るようにしているが、容易に編集・削除できるようになっている	・ログにアクセスできる者を限定し、また監査部門がシステム監査を行う ・ …
…	…	…

これらの対応策を踏まえて、影響度、発生可能性を再評価した上でリスクマップを修正し（図表 10 参照）、残存するリスクについて、さらに低減等する必要があると判断した場合は、更なる対応策を検討することも考えられる。

図表 10　修正後のリスクマップのイメージ



6．PIA 報告書のとりまとめ等

PIA の実施結果等について、報告書としてとりまとめ、経営層への報告を行うことにとどまらず、対外公表することは、消費者をはじめとするステークホルダーへの説明責任と透明性の観点から有効である。

もっとも、対外公表に際して、実施結果等の詳細まで提供する必要性は乏しく、むしろ、報告書のサマリーを作成し、簡潔でより分かりやすい形で公表することが有効である。

報告書には、上記のプロセスで整理した個人情報等の取扱いのフロー、当該フローのうち PIA の実施範囲、実施方法、特定したリスク、当該リスクの評価結果、対応策等について記載することが考えられる。

事案に応じて、報告書の内容について、第三者機関のチェックを経て、信頼性を高めることも有効である[13]。その際、特に消費者団体などの消費者を代表する立場にある者からの確認を得ることが重要である。

[13] この第三者機関の役割を、認定個人情報保護団体をはじめとする民間団体が担うことも考えられる。

おわりに

PIA は、個人情報保護法等の法令遵守に限定した画一的なチェックリストにより形式的に実施するだけでは、十分な効果は期待できない。本稿に記載している PIA の意義や実施手順の各段階での留意点・着眼点を踏まえて、多角的観点を持ってきめ細かく実施していくことにより、個人の権利利益の侵害リスクを遺漏なく洗い出して、そのリスクを適切に低減・解消し、消費者をはじめとする利害関係者からの信頼を得ることができると考えられる。

こうした有効かつ実効的な PIA の手法等は、それぞれの事業の内容、個人情報等の取扱いの方法によって様々であり、特定の手法に限定できるものではない。PIA にはそのための人員と実施期間などコスト負担が伴うものであり、投入できるリソースに制約がある以上、リスクベースでの効果的な実施が期待されるといった側面もある。各事業者においては、本稿を参考にしつつ、自身にとって最適な PIA の手法を検討して効果的にリスク対策をとっていくことに期待したい。

本稿が、PIA の実施に関心を持つ事業者や、業界内の PIA 実施の支援を検討している認定個人情報保護団体をはじめとする民間団体にとって有益なものとなるとともに、これまで PIA に関心を持っていなかった事業者等にも、自身の個人情報等の取扱いについて見直す契機となることを期待する。

参考文献

【 報告書等 】

- 個人情報保護委員会「個人情報保護法 いわゆる３年ごと見直し 制度改正大綱」(2019年)(https://www.ppc.go.jp/files/pdf/200110_seidokaiseitaiko.pdf)
- 総務省・経済産業省「DX 時代における企業のプライバシーガバナンスガイドブック ver1.0」(2020 年)(https://www.meti.go.jp/press/2020/08/20200828012/20200828012-1.pdf)

【 標準 】

- 「Financial services - Privacy Impact Assessment」(ISO 22307：2008)
- 「Information technology - Security techniques - Guidelines for privacy impact assessment」(ISO/IEC 29134：2017)
- 「情報技術－セキュリティ技術－プライバシー影響評価のためのガイドライン」(JISX 9251：2021)
- 「Information technology－Security techniques－Privacy framework」(ISO/IEC 29100:2011)
- 「Information technology－Security techniques－Information security management systems-Requirements」(ISO/IEC 27001:2013)
- 「情報技術－セキュリティ技術－技術セキュリティマネジメントシステム－要求事項」(JISQ27001：2014)
- 「個人情報保護マネジメントシステム－要求事項」(JISQ 15001：2017)

【 書籍 】

- 瀬戸洋一編著「ISO/IEC 対応　プライバシー影響評価実施マニュアル」(日科技連出版社、2020 年)

【 その他 】

- 第 164 回 個人情報保護委員会「改正法に関連するガイドライン等の整備に向けた論点について（認定個人情報保護団体制度)」(https://www.ppc.go.jp/files/pdf/210126_shiryou-2.pdf)
- European Data Protection Board「Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679」(https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47711)
- 美馬正司「民間における PIA の取組（企業におけるプライバシー保護の勘所)」(https://www.jipdec.or.jp/library/report/20210225-3.html)