プライバシー影響評価（PIA・DPIA）の重要性と実務

～顔認証・情報銀行等の先端サービスから日常業務まで～

弁護士　水町雅子

旬刊経理情報 2022 年 5 月 1 日号通巻 No.1643 掲載の「個人情報を保護しつつビジネスに活用するプライバシー影響評価の重要性と実務ポイント」の元原稿となります。

この記事のエッセンス

- 個人情報を保護しながらビジネスを実施する際に有用となるスキームが、プライバシー影響評価である。「顔認証を利用した顔パスイベント入場」や、EBPM 実現に向けた「行政情報分析基盤」に関するプライバシー影響評価について具体的に紹介する。
- ・プライバシー影響評価により、個人情報の取扱いを透明化して消費者の信頼を得ること、ビジネスの設計・実装に個人情報保護を予め埋め込むこと、従業者・委託先にとって業務従事中の具体的なガイドとなること、個人情報に対する競業他社との差別化に資することが考えられる。

本文

昨今のビジネス遂行では、個人情報の取扱いを避けて通ることのできないものも多い。個人情報を保護しながらビジネスを実施する際に有用となるスキームが、プライバシー影響評価（Privacy Impact Assessment、頭文字を取って PIA と呼ばれる）である。英米法系の国では PIA と呼ばれるが、GDPR（一般データ保護規則）では、DPIA（データ保護影響評価、Data Protection Impact Assessment）と呼ばれ、義務付けもされている（以下、これらを総称して、単にプライバシー影響評価又は PIA と呼ぶ）。本稿ではプライバシー影響評価（PIA）の意義・プロセスについて解説するとともに、顔認証サービス等に対して実際に実施されたプライバシー影響評価についても紹介していきたい。

１．プライバシー影響評価（PIA）の意義

（１）プライバシー権保護とビジネスの成功の両立

プライバシー影響評価とは、例えるなら環境影響評価のような事前評価を個人情報に対して実施するものである。環境影響評価とは、大規模な開発事業などを実施する際に、事業者が、あらかじめその事業が環境に与える影響を予測・評価し、住民や関係自治体などの意見を聴くとともに、それらを踏まえてより良い事業計画を作ることにより、適正な環境配慮がなされるようにするための手続をいう（環境影響評価法 1 条参照）。プライバシー影響評価では、個人情報を取り扱うビジネス・施策などを実施する際に、一般人やステークホルダ

ー、専門家の意見を聴きながら、あらかじめプライバシーに与える影響を予測し、かかる影響を排除又は十分に軽減するための対策を検討・実装することにより、プライバシー権保護とビジネスの成功との両立を図ることとなる。

プライバシー・バイ・デザイン（Privacy by Design）、データ保護・バイ・デザイン（Data Protection by Design）、データ保護・バイ・デフォルト（Data Protection by Default）の重要性が叫ばれてから久しいが、プライバシー権保護とビジネスの成功を相反するものと捉えて、ビジネスの企画・設計が終わった後からプライバシー保護を検討しても、時すでに遅しと言える。ビジネスの企画・設計・実装が完了し、サービス開始間近になって、個人情報保護上の問題が判明したとしても、そこから設計・実装を変更するには多大な時間とコストを要する可能性がある。初期段階からビジネスの設計・実装に個人情報保護を予め埋め込んでおくことが重要である。このプライバシー・バイ・デザイン、データ保護・バイ・デザインを実際に実行するためのスキームが、プライバシー影響評価である。

（2）消費者などの様々な目線を取り入れられる

また、プライバシー影響評価を実施することで、社内のビジネス関係者以外に、広く、消費者、専門家などの様々な観点からの意見を聴取することができる。昨今、個人情報保護に対する国民意識が非常に高く、個人情報に関する失敗事例では、消費者、SNS、メディアその他さまざまな方面から強い非難を受けることも多い。社内だけで個人情報保護を検討していると、どうしてもビジネス寄りの視線になってしまい、消費者目線に欠ける場合もある。また個人情報や要配慮個人情報は法律上確立された定義・解釈がある一方で、プライバシーは多義的概念である。社内の限られた人数だけでの検討では、多様な視点を取り入れられない可能性もあるが、この点、プライバシー影響評価を実施することで、多種多様な様々な立場の者から意見を聴取することも可能となる。

（3）競合他社との差別化

さらに別の角度からプライバシー影響評価を説明すると、個人情報保護に対する優良企業にとっても、このスキームは有意義であると言える。多くの企業は日々個人情報保護に努め、様々な取組みを行っている。しかし、個人情報をずさんに取り扱っている企業との差別化を、目に見える形で実行するのは実は難しい。プライバシーマーク、ISMS の取得などで個人情報保護の取組を対外的にアピールできるが、多くの企業がすでにこれらの認定を得ており、差別化材料にはならない場合も多々存在する。この点、プライバシー影響評価を実施すれば、自社の個人情報保護の取組を具体的に説明し対外的にもアピールできるため、個人情報に対する競業他社との差別化材料としての役割も期待できる。

（4）従業者・委託先への教育効果

また従業者や委託先に対する教育的効果も考えられる。事業者は、従業者に個人情報保護

のための教育を行うべきであるものの、個人情報保護法の研修を実施しても、従業者にとっては具体的に気を付けるべきポイントがわかりづらい場合もある。この点、プライバシー影響評価では、自分が実施している業務中にどのようなプライバシーリスクがあり、それを排除又は十分に軽減するためにはどのような対策が有効かを検討するため、従業者・委託先にとって具体的な気づき・ガイドとなりうることが考えられる。

（5）個人情報の取扱いをブラックボックス化しない

個人情報を取り扱われる側から見れば、今まではブラックボックスともいえる個人情報の取扱いについて、具体的な説明を受けられるという意義もある。この点、プライバシーポリシーや個人情報保護基本方針等が、本来はこのような役割を担うべきかもしれないが、消費者目線で見ると、難しく抽象的な文章となっている場合もある。「自分の個人情報は誰にどのように取り扱われているのか」「自分の個人情報は何に使われるのか」「自分の個人情報は誰に提供されていくのか」「自分の個人情報はどのように管理されているのか」「自分の個人情報はちゃんと守られているのか」、このような消費者の疑問にプライバシー影響評価は回答することができる。プライバシー影響評価では、「どのように個人情報を取り扱うのか」「どのようなリスク対策を講じるのか」「プライバシー権保護/個人情報保護にどのように取り組んでいるのか」を明らかにするからである。

2．プライバシー影響評価（PIA）の実践例

（1）顔認証 PIA

プライバシー影響評価の実践例として、筆者が日本電気株式会社協力の下作成した、「顔認証を利用した顔パスイベント入場に関する個人情報リスク評価 DPIA・PIA」（図表 1　顔認証 PIA）[1]を紹介したい。顔認証により、来場者は手ぶら（チケットレス）かつ短時間、接触レスでスムーズにイベントに参加することができる。他方で、重要な個人情報である顔画像が万一悪用されたり流出してしまえば、プライバシーに与える影響は非常に大きく、また様々な場所での監視につながる懸念や、顔認証の精度の問題等も存在する。顔認証の活用といった比較的新しい取組みはイノベーションに欠かせないものではあるが、個人情報やプライバシー権の保護が大前提であり、プライバシーに与える悪影響を防止・軽減する対策を事前に十分講じた上で、適法・適正に技術が活用されていくことが重要であり、プライバシー影響評価が実施された。

---

[1] https://www.miyauchi-law.com/f/210812necpia.pdf

図表 1　顔認証 PIA からの抜粋

1.1　顔パス入場の概要

①申込時

利用者

・Webから申込み
・氏名、生年月日、住所、電話番号、メールアドレス、パスワードを入力する
・**「顔パス入場 」を利用したい場合に限り** 、顔写真データの登録の同意を行い 、顔写真データをアップロード する
・いったん登録した後に 、顔写真登録の取消も可能

②入場時

顔パス利用者

※顔パス入場者以外は、 通常ゲートから通常通り入場

・顔パス入場者 は、 顔パス 入場ゲートのカメラで 撮影した顔写真データをアップロードして識別 ・認証することの同意を行う 。同意された場合のみウォークスルー用のゲートに進む
・ゲートのカメラで顔写真を撮影
・認証できた場合は、 入場ゲートが自動的に開く
・認証できなかった場合は 、通常ゲートから通常通り入場するか 、係員に問い合わせる

5

3　顔パス入場の個人情報保護のポイント（対策まとめ）

顔写真データは、大変重要な個人情報です。また、顔認証が悪用等されると、なりすましや監視等につながる懸念もあります。顔認証技術を利用・提供する企業にはこれらのリスクその他のプライバシー権侵害や不正行為を防止するため、様々な対策を応じる必要があります。 NECでは本評価記載の通りの措置を講じており、その主なポイントは以下の通りです。

主なポイント

① **顔写真データ自体はすぐに削除**
・顔写真データを利用者が登録後、速やかに顔認証システムでは「特徴量抽出 *」を行います。特徴量抽出後は、速やかに登録された顔写真データ自体を削除します。
・来場時にゲートで撮影した顔写真データも、速やかに特徴量抽出を行い、撮影データを削除します。
*特徴量抽出：まず、画像中から顔を検出した後、顔のなかから目や鼻、口端、顔の輪郭、配置の特徴などの特徴的な点を数値化した顔特徴量を抽出します。顔識別・顔認証は、この特徴量を用いて実施します。

② **希望者だけが、顔パス入場**
・顔パス入場希望者以外は、通常ゲートから通常通り入場できます。

③ **NECが提供する顔認証機能では、氏名・住所等の情報は保持しません**
・ID・顔写真データ、顔写真データから抽出した特徴量のみを保持します。このうち、顔写真データは上記の通り特徴量抽出後速やかに削除するため、 ID及び特徴量のみ保存しています。
・但し、Y社の催事管理システムでは、申込者情報として氏名・住所・電話番号・メールアドレス・ IDなどの情報を保存しています。

④ **セキュリティ**
・様々なセキュリティ対策を履践しています。 NECではPマーク付与認定及びISMS認証を取得しています。

10

5.3　入場するために顔画像を登録しなければならないのか

某イベントに参加したいです。
でも、そのために顔画像を登録したり顔認証をするのは嫌です。

希望者だけ、顔画像による顔パス。通常ゲートからチケット提示でも入場できます
- 顔認証による顔パス入場は、あくまで希望者だけが対象。
- 顔パス入場以外に、通常ゲートからチケットを提示し、通常の方法で入場することができます。顔パス入場が通常入場とは自由に選択可能です。通常入場を選択した場合にも来場者に不利益はありません（もっとも、通常入場の際は、入場待ちリスク、係員との接触リスク等はあり）

取消可能
- 一度顔パス入場を申し込んだ方でも、顔パス入場する前までであれば取消が可能。
- 取消を希望された場合は、顔写真、特徴量その他の個人情報を速やかに削除します（但し、問合せ対応のためIDだけは取消済のIDとして記録し保持しておく）。

残存リスク
- 取消時については、 NECだけでなく、X社・Y社においても確実に削除されることを確認する必要があります。

15

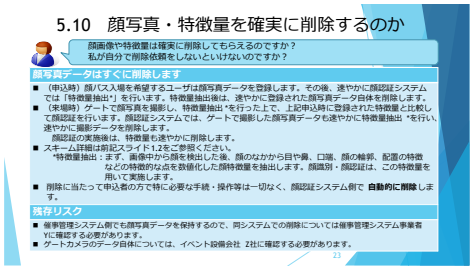
5.8　知らない間に顔画像が撮影されないのか

知らない間に顔画像を撮影したり、顔認証したりしないですか？

知らない間に顔認証することはありません
- **顔パス入場ゲートでのみ** 顔認証を行います。顔パス入場ゲートは通常ゲートと異なる**外観** になっており、顔認証を実施することを立看板で **周知**しています。
- なお、顔パス入場ゲートで顔画像を撮影した場合であっても、 **事前に顔写真を登録していない場合は**認証エラーとなります。そして顔パス入場ゲートで撮影された顔画像・特徴量データは速やかに削除されます。
- 顔パス入場ゲート以外では、顔認証を実施しません。

残存リスク
- ゲートカメラの運営はイベント設備会社 Z社に委ねられています。ゲートカメラで常時撮影しているか、人がカメラ前に立った時だけ撮影しているのかは、 Z社に確認する必要があります。

21



本件における個人情報保護の主なポイントは、次の 3 点である（図表 1　顔認証 PIA）。
①顔写真データ自体はすぐ削除すること
②希望者だけが顔パス入場となること
③NEC が提供する顔認証機能では氏名・住所等の情報は保持しないこと

顔パス入場を希望する者が自身で顔写真データを登録するが、顔認証システムでは速やかに「特徴量抽出」を行う。特徴量抽出とは、画像中から顔を検出した後、顔のなかから目や鼻、口端、顔の輪郭、配置の特徴などの特徴的な点を数値化した顔特徴量を抽出することをいう。顔識別・顔認証は、この特徴量を用いて実施するため、特徴量抽出後は、速やかに登録された顔写真データ自体を削除する。入場時に入場ゲートで撮影した顔写真データも、速やかに特徴量抽出を行い、撮影データを削除する。さらに、NEC では氏名・住所等の情報は保持せず、速やかに消去する顔写真データ以外は、特徴量と ID のみを保持する。

「顔認証を利用した顔パスイベント入場に関する個人情報リスク評価 DPIA･PIA」では、このほか、「なりすまして別人が入場することはないのか」「誤認証・誤認識で入場できないことはないのか」「顔認証・顔画像が不正利用されないのか」「もし特徴量が漏えいしたらどうなるのか」「漏えい対策」「知らない間に顔画像が撮影されないのか」「顔画像や特徴量を他人に提供することはないのか」「顔写真・特徴量を確実に削除するのか」「監視につながらないのか」などの検討を行った。

（2）姫路市 PIA

プライバシー影響評価の実例として、次に、筆者が姫路市協力の下作成した、「総務省実証事業における姫路市行政情報分析基盤個人情報リスク評価 PIA」（図表 2 図表 1　顔認証 PIA）[2]を紹介したい。姫路市では、市の持つ業務データを活用して、エビデンスに基づくより良い政策立案（EBPM
）を行うために、データ分析基盤システムを開発した。本事業は、総務省が平成２９年度に実施した「地域におけるビッグデータ利活用の推進に関する実証」事業としても採用されている。姫路市では、前例や職員の経験・勘などに依存しない、第三者による検証が可能で透

[2] https://www.miyauchi-law.com/f/180628PIAhimeji.pdf

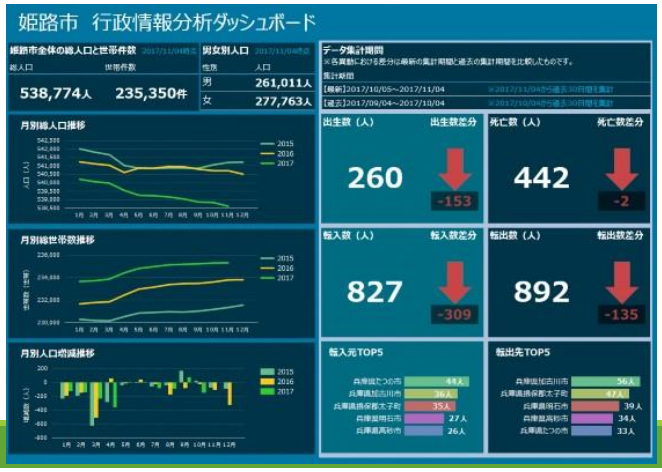
明性の高いエビデンスベースの政策立案を推進するために分析基盤を構築したが、分析対象データには個人情報が多く含まれ、プライバシー権侵害や不正行為を防止するため、プライバシー影響評価が実施された。

図表 2　姫路市 PIA からの抜粋

2　姫路市分析基盤は、どのようなものか

分析画面のイメージ

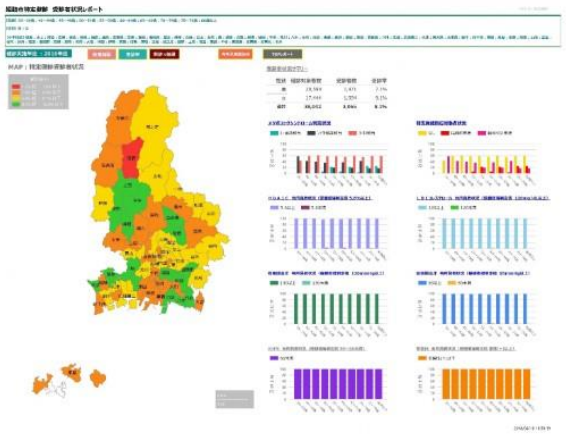
- 分析基盤は、姫路市職員のみ操作できます。分析基盤を通じて作成した統計結果は会議資料や市ホームページ等で利用することがあります。
- 住民基本台帳データを分析し図示等することで、人口推移、出生数推移、転出入状況、経年変化等をとらえ、将来予測も可能となります。
- 正確な情報を精緻に分析することで、市の今後の政策検討の基礎データとし、より良い行政政策を検討・実行していきます。
- 右の数値等はダミーです。



2　姫路市分析基盤は、どのようなものか

分析画面のイメージ

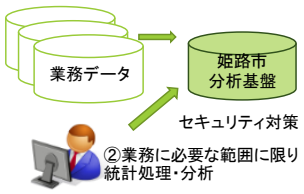
- 分析基盤は、姫路市職員のみ操作できます。分析基盤を通じて作成した統計結果は会議資料や市ホームページ等で利用することがあります。
- 特定健診データを分析し地図情報と重ねる等することで、地域ごとの受診率などをわかりやすく図示できます。
- 現状を分析することで、特定健診の受診率向上、ひいては住民の健康状況の向上をめざします。
- 右の数値等はダミーです。



２　姫路市分析基盤は、どのようなものか

自治体の持つ業務データをもとに分野横断的な分析を行い、より良い行政・政策を目指す仕組み

業務データには個人情報が多く含まれます。
プライバシー権侵害や不正行為を防止するため、本評価記載の通りの厳格な措置を講じます 。

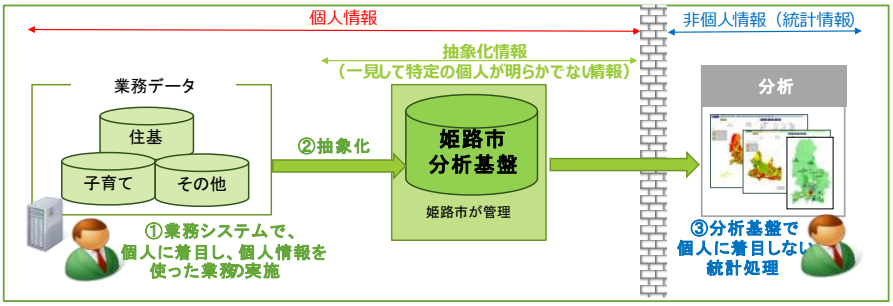


主なポイント

① 子育て、住民基本台帳等の業務データ（個人情報）から、**氏名等を削除**して、**誰の個人情報か一見してわからない状態に加工**（抽象化）します
② **市役所職員が**自身の**業務に必要な範囲に限り**①の情報を元に、市の現状などを**統計処理**します。市職員が閲覧できるのは統計情報のみで、①情報は閲覧することはできません。
③ 分析結果を元に政策立案、課題解決、住民サービス向上等を検討して 、**より良い行政**を目指します
④ 分析・統計作成作業は、地方公務員法上、守秘義務を 負う市職員が行います。守秘義務違反等には刑罰 や懲戒処分を科せます。
⑤ 姫路市分析基盤は、インターネットと切り離された環境にあり 、姫路市が厳重に管理している端末から操作します。セキュリティ対策を厳重に講じています 。

3

４　姫路市分析基盤の全体像



① 市では、行政サービス・業務を実施するために、住基情報、子育て情報その他の業務データ（個人情報を含む）を収集・利用・保管等しています。市職員は原則として自分の担当業務に必要な個人情報のみを取り扱っています。
② 業務データから氏名等を削除して、一見して誰の情報かわからないデータに加工します（抽象化）。抽象化した情報を分析基盤に取り込みます。分析基盤上のデータを、職員等は直接閲覧・ダウンロード・印刷等することはできません
③ 市職員は分析基盤を利用して、統計処理を行います。統計情報は非個人情報であり、個人に着目しない統計処理のみを行います。

11

姫路市分析基盤の個人情報保護対策の主なポイントは、次の５点である。

①市の持つ業務データから、氏名等を削除して、誰の個人情報か一見してわからない状態に加工（抽象化）すること

②市職員が自身の業務に必要な範囲に限り、①の情報を元に市の現状などを統計処理し、市職員が閲覧できるのは統計情報のみであること

③分析結果を元に政策立案、課題解決、住民サービス向上等を検討して、より良い行政を目指すこと

④ 分析・統計作成作業は、地方公務員法上、守秘義務を負う市職員が行い、守秘義務違反等には刑罰や懲戒処分を科せられること
⑤姫路市分析基盤は、インターネットと切り離された環境にあり、姫路市が厳重に管理している端末から操作するなど、セキュリティ対策を厳重に講じていること

このほかにも、「姫路市分析基盤がどのような効果を有するのか」、「姫路市分析基盤で誰のどのような個人情報がどのような者にどのような利用目的でどのように利用・保管するのか」、「住民等に不利益処分等がなされることはないか」、「個人情報を不正にのぞき見・外部提供等されないか」、「個人情報が漏えいしないか」、「統計情報のための適切な加工がなされるか」などの検討を行った。

（3）情報銀行

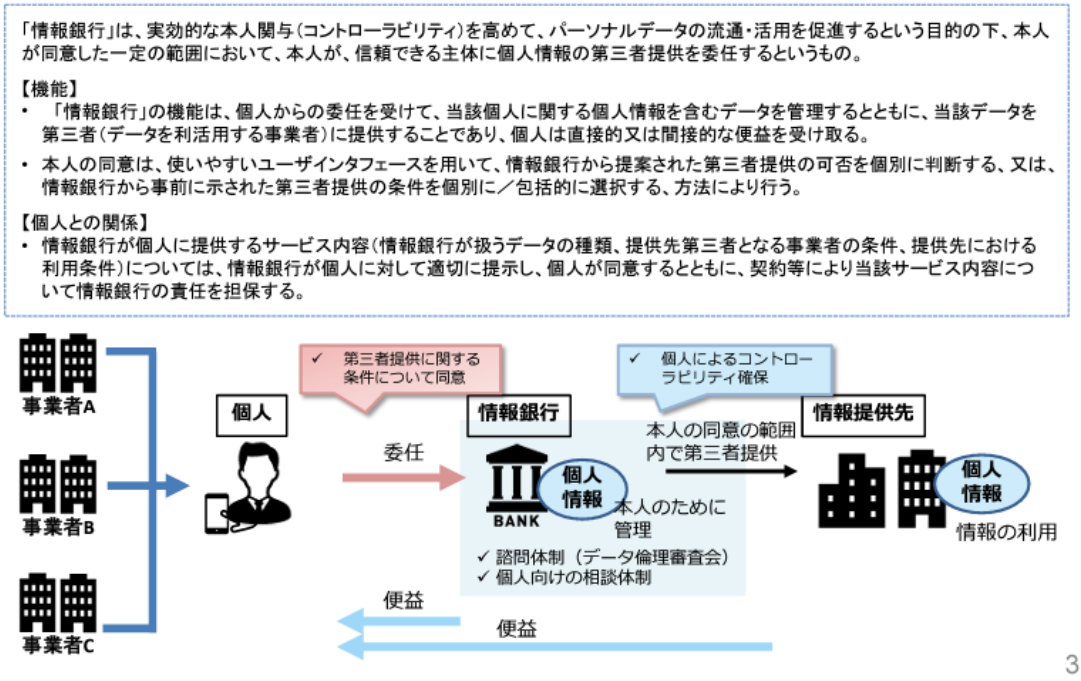
本人関与の下でデータ流通・活用を進める仕組みである情報銀行でも、認定時にプライバシー影響評価に相当するスキームが用いられている。情報銀行では、本人の同意（委任）により本人の個人データを管理して第三者に提供し、それによって当該本人は便益を受け取るというスキーム（図表 3）がとられるが、情報銀行事業が本人の利益に反していないかという観点から適切性について審議する「データ倫理審査会」が設置される（総務省及び経済産業省「情報信託機能の認定に係る指針 Ver2.1」[3]P13④）。そのデータ倫理審査会の運営の際に、PIA を参考にすると良いと考えられ、『「情報銀行」認定制度 データ倫理審査会 運用ガイドライン』[4]ではプライバシー影響評価を中心とした記載がなされている。

---

[3] https://www.meti.go.jp/press/2021/08/20210825001/20210825001-3.pdf

[4] https://www.tpdms.jp/file/TPDMS-1140.pdf。同ガイドラインは筆者のほか、森亮二弁護士、崎村夏彦氏による監修。

図表 3　情報銀行イメージ



出典：総務省及び経済産業省「情報信託機能の認定に係る指針 Ver2.1」P3

3．プライバシー影響評価の実践方法

プライバシー影響評価は、民間企業か公的機関かの別を問わず、また先端的なサービスか日常的業務かの別を問わず、実施可能である。

（1）関連法令・ガイドライン等

データ保護影響評価（DPIA）は、GDPR で実施義務が課せられており（GDPR35 条）、『データ保護影響評価（DPIA）及び取扱が 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』[5]も公表されている。

日本でもプライバシー影響評価は、マイナンバー関連では「特定個人情報保護評価」としてマイナンバー法（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）で実施義務が課せられており（同法 28 条）、特定個人情報保護評価指針も公布されている。他方で、マイナンバー以外に関するプライバシー影響評価自体は、日本ではまだ実施義務が法律上定められていないため、何を対象にどのようなプロセスで実施しなければならないといった基準はないが、ISO/IEC 29134：2017 Information technology — Security techniques — Guidelines for privacy impact assessment や JIS X 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といった規格も発行されてお

---

[5] 個人情報保護委員会による日本語仮訳→
https://www.ppc.go.jp/files/pdf/dpia_guideline.pdf

り、これらを参照することが考えられる。『「情報銀行」認定制度 データ倫理審査会 運用ガイドライン』も上記 ISO や JIS 規格を元にプライバシー影響評価について記載されているので、参考にするとよいだろう。

（2）プライバシー影響評価の主な実施プロセス

プライバシー影響評価の主な実施プロセスは、①実態把握、②リスク特定、③対策検討である。①実態把握では、プライバシー影響評価を実施するビジネスや施策の全体像、目的、効果、取り扱われる個人情報の詳細、個人情報のフロー等を把握・特定する。②リスク特定では、①で把握された実態に対してどのようなプライバシーリスクが考えられるか特定し、影響度と発生可能性の組み合わせで評価する。③対策検討では、②で特定されたリスクを排除又は十分に軽減するための対策を検討し評価する。

①実態把握のためには、プライバシー影響評価を実施するビジネスや施策に関する既存ドキュメントの確認や関係者ヒアリングを行う等の方法が考えられ、さほど難しいものではないと考えられる。③対策検討も、斬新な対策や高度な対策が求められるわけではなく、さほど難しいものではない。例えば、個人情報が誤入力されるリスクがあるなら、ダブルチェックする、チェックデジットをつける等の対策が考えられるし、個人情報が不正持出しされるリスクがあるなら、施錠管理する、データの書き出しを制御する等の対策が考えられる。

難しいのは、②リスク特定である。個人情報保護やプライバシーの観点から類型的に想定されるリスクはあり、それは特定個人情報保護評価書等を参照すれば把握可能であるが、対象ビジネスや対象施策特有のリスクをどう特定するかが難しい。そのため、関係者によるブレインストーミング、有識者へのヒアリング、一般消費者へのヒアリング等、複数の方法を組み合わせて実施すると良いだろう。

なお、プライバシー影響評価は「評価」とあるため、第三者による評価との誤解も多いが、海外では自らの気づきが重要として、自己評価とされている。日本では自己評価だけだと受容性に乏しい可能性があるため、自己評価と第三者評価を融合させることも考えられる。例えば、自社で有識者とともに評価を実施したり、自己が実施した評価について第三者の点検を受ける等の方法が考えられる。また第三者評価としても、自社自らがプライバシーリスクを十分認識し、リスク対策を的確に実践していくスキームを採用できれば、それも良いだろう。

（3）終わりに

プライバシー影響評価と聞くと、難しいものと捉える向きもあるが、実際には、個人情報の実態を把握し、プライバシーリスクを特定の上、リスク対策を検討するという、ある意味オーソドックスな取組みである。個人情報保護に資する仕組みであるため、興味を持たれた方はぜひ取り組んでみられると良いだろう。