TOKIO MARINE

リスクマネジメント最前線

2024 | No.7

# PIA（プライバシー影響評価）の現在地と課題

ビジネスリスク本部　上級主席研究員　青島　健二
専門分野：新規事業開発、業務/IT 改革、企業リスク管理、海外現地法人管理
経歴：製造業にて人事労務、経営企画部門の業務に従事後、IT 系シンクタンクにて調査研究、及び各種コンサルティングに従事。2005 年より、東京海上ディーアールに勤務。その間、タイ国東京海上火災保険に 3 年間出向。

ビジネスリスク本部　主任研究員　渡邉　彩恵香
専門分野：企業等のリスクマネジメント
経歴：2021 年に東京海上ディーアール入社。企業等のリスクマネジメント等に従事。

地方都市の多くは人口減少、高齢化に課題を抱えており、その解決の切り札として、デジタル技術を活用した都市構想「スマートシティ」の構築を目指している。一方、スマートシティに対して住民は、自身のプライバシー情報が扱われることに少なからず不安を抱いていることから、情報を預けることに安心してもらうこと、情報を預けることで得られる便益を理解してもらうことが、スマートシティが成功するための鍵となっている。

当社では、実際に国・地方自治体・民間各事業において PIA（Privacy Impact Assessment： プライバシー影響評価）の実施を支援した立場から、PIA のあり方について解説する。

## 1. PIA とは何か

### (1) サービスに潜在するプライバシーリスクを、事前に明確化する枠組み

PIA（Privacy Impact Assessment： プライバシー影響評価）とは、あるサービスにおいて想定される「個人情報及びプライバシーに係るリスク分析、評価、対応検討を行う手法」[1]であり、サービスの導入前に実施することが推奨されている枠組みである。

2024 年 5 月現在、日本において PIA は法規上の定義を得ておらず、事業者等に対する PIA の実施義務も存在しない[2]。すなわち、これまでに日本国内で実施された PIA の各事例は、ISO や JIS といった規格やその他の類似枠組みを参照しながら、それぞれのサービス提供者が自発的に評価要領を設定し、実施したものだと言える。

---

[1] 出典：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 ver1.2」（2022 年 2 月 18 日）
https://www.meti.go.jp/press/2021/02/20220218001/20220218001.html

[2] ただし、日本では番号法第 27 条・第 28 条に基づく「特定個人情報保護評価」が存在し、特定個人情報（マイナンバーを含む個人情報のこと）ファイルを保有する、または保有しようとする行政機関・地方公共団体等に対する、特定個人情報保護評価の実施義務がある。**本稿で定義する PIA には、特定個人情報保護評価は含まない。**

しかしながら、前段で述べたPIAの姿かたちは、国内でみられるPIA実施事例に概ね共通する。当社の考えるPIAの構成要素を「5W1H」（How:どのように実施するか については、本稿第 3 章で記載）に基づき整理する。

### □「なぜ(why)」実施するか

PIA 実施により期待できることの一例として、対外的にはサービス利用者等に対する説明責任を果たすこと、また対内的には、サービス設計段階でのリスク特定により、当該サービスにおけるリスク対策のコストを適正化すること等が挙げられる。

■ 表 1 PIA の実施により期待できること

| 期待できること | 内容 |
|---|---|
| **サービスの透明性向上** | 当該サービスで想定されるリスクや、リスクへの対策状況を事業者自らが公表することにより、当該サービスの利用者等における、より適切な意思決定につながる。 |
| **サービスの信頼性向上** | 当該サービスが、プライバシー保護を念頭に置いて設計されたことを示すことで、ステークホルダーからの信頼が向上する。 |
| **サービスにおけるリスク管理とコストの適正化** | 当該サービスの設計段階でリスクを特定・評価することにより、リスク対策にかけるコストが適正化される。<br>重大なリスクが判明した場合、早期に対策を講じれば人的・財務的コストが抑えられるが、当該サービスのリリース前後に判明した場合は、改修等に多大なコスト投入を要することが想定される。 |

### □「何を(what)」対象とするか

PIA の実施対象として第一に想定されるのは、プライバシーに関する情報を取り扱うサービスである。ここで注意すべきは「プライバシーに関する情報」に関する統一的な定義も、現在のところ存在せず、事業者の判断に委ねられるという点である。少なくとも個人情報保護法で定義される「個人情報」や「個人関連情報」を含み、これより広範な情報を検討の俎上に載せることが望ましいと考えられる。

### □「いつ(when)」実施するか

PIA は、原則としてサービスの設計段階に実施される。前段で引用した「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 ver1.2」では、サービスの仕様や要件を定義する前の段階で、リスク評価とリスク低減対策を実施し、サービスのリリースを判断する段階で、リスク対策の進捗を確認するという進め方を例示している。

あるいは、リリース済みのサービスの仕様等を大きく変更するタイミングで PIA を実施することも有効である。その他、事業者が必要と判断した際の実施も有り得る。

### □「誰が(who)」実施するか

基本的に当該サービス提供元の責任者が、PIA 実施やその結果内容に対する責任を負う。リスク評価の実務は、サービス提供者（単体または複数の事業者）が担うか、外部機関等が関与し、作業を実施する場合もある。サービス提供者自らがリスク評価等の実務を担う場合は、一連の PIA 結果に対し第三者が監査を実施し、その監査結果も含んだ上で PIA を完了するケースも考えられる。

□「どこで(where)」PIA 結果を用いるか

目的次第ではあるが、特にサービスの透明性向上を念頭に置いた場合は、当該サービスの公式ウェブサイトや、サービスについて説明する場等で結果を公表することが一案である。その際は、想定される利用者の属性を考慮した上で、可能な限りわかりやすい資料を用いて公表することが望ましい。

## 2. PIA を巡る制度・取り組みの状況

先に述べたとおり、2024 年 5 月現在、日本においては PIA の実施を定める法規は存在せず、一部の企業や行政機関が、自らの意思決定によって PIA を実施している。一方、欧州や米国では PIA（またはそれに相当する枠組み）が義務付けられている場合もあり、日本からみた先行事例として位置付けられる。それぞれの状況を簡単に紹介する。

### (1) 日本：PIA 実施は「推奨」の段階

これまで述べてきたとおり、マイナンバー制度に基づく特定個人情報保護評価制度を除いて、PIA を義務付けたり、PIA の実施要領を定めたりする法規は現在のところ存在しない。ただし、以下のとおり複数の文書において、PIA の実施が推奨されている。

■ 表 2 日本における PIA 実施の推奨状況

| 出典 | 推奨内容 |
|---|---|
| **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」**[3] | 事業者における自主的な PIA の取り組みを促すことが望ましいとしている。 |
| **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 ver1.2」** | パーソナルデータを利活用する事業に対し、プライバシーガバナンスを機能させ、またプライバシーに関する取り組みに経営資源を投入することを推奨している。 |

このような状況下で、一部の民間企業（特に比較的機微なユーザー等の情報を扱う企業）や行政機関（特にスマートシティの取り組みを推進する自治体等）が PIA の取り組みを推進している。上記の「ガイドブック」では民間企業の PIA 実施事例が紹介されており、企業によってリスク評価の進め方や PIA の位置付け等が様々であることが読み取れる。

### (2) 欧州：GDPR における DPIA の義務付け

一方、欧州では GDPR（General Data Protection Regulation： EU 一般データ保護規則）の第 35 条において、DPIA（Data Protection Impact Assessment： データ保護影響評価）の実施が義務化されるとともに、実施対象となる条件やその実施方法が定められている。

実施対象は業務単位・システム単位で特定されることが多く、例えば「個人の位置情報や行動を追跡する」場合、「人種・民族、政治的意見、宗教・哲学的信条…（以下略）に関するパーソナルデータを使用する」場合等に

[3] 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 12 月 13 日）
https://www.ppc.go.jp/files/pdf/200110_seidokaiseitaiko.pdf

DPIA を実施することとなっている。また、DPIA のアウトプットにはパーソナルデータの処理方法と目的、データ処理の必要性、データ主体の権利・自由に対するリスクの評価結果を含むこととしている。

例えばフランスのデータ保護機関（CNIL; Commission Nationale de l'Informatique et des Libertés）は DPIA に関するガイドラインやツールキットを整備しているほか、フィンランドの首都ヘルシンキにおいても同様の整備が進んでいる。

### (3) 米国：行政機関に対する義務付けと、州法における PIA の義務化検討

米国においては、欧州のように民間事業者に対する統一的な PIA の実施義務等は規定されていないものの、電子政府法や国土安全保障法が、連邦行政機関に対し PIA の実施を義務付けている。PIA の実施対象は個人を特定できる情報を電子的に収集するシステムとされており、情報の取り扱いが各種法令規制に準拠していることを確認・宣言するとともに、当該システムで想定されるリスクと、その軽減策等を含むこととしている。米国国務省のウェブサイト[4]では、2024 年 5 月時点で 100 を超える PIA の実施結果が公表されており、医療データの記録システムからパスポート情報の記録システムまで、多岐にわたる行政サービスが対象となっている。

加えて、一部の州では PIA の実施義務を含む州法の検討が進んでいる。例えば米国・テキサス州では Texas Data Privacy and Security Act (TDPSA)が 2023 年 6 月 16 日に成立し、2024 年 7 月 1 日から施行されることとなっている。TDPSA における PIA では、パーソナルデータの管理者に対し、PIA 対象となるサービスが消費者にもたらす便益とリスクを比較・検討することを求めている[5]。なお、例えばシアトル市はプライバシーデータを扱う市の事業について、PIA を実施しウェブサイトで公開している。

### (4) PIA に関連する規格等

以上でみてきたとおり、一部の国・地域では PIA 実施にあたってのフレームワークが整備されつつあるが、国際的に参照できる枠組みとしては、国際標準化機構（International Organization for Standardization）の発行する ISO/IEC 29134:2023 "Information technology — Security techniques — Guidelines for privacy impact assessment"が挙げられる。また、ISO/IEC 29134:2017 に対応する規格として、日本規格協会が発行する 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」が参照可能である。以下で紹介する当社の PIA 実施支援も、これらを念頭に置き進めている。

## 3. 当社が提案する PIA の姿

PIA（プライバシー影響評価）の本質的な価値は、一般個人が自身の情報を漏えい・暴露・改ざんされる「可能性」と「精神的なダメージの大きさ」を評価するところにある。さらに、その評価結果を踏まえ、一般個人がその事業やサービスに、自身の情報を提供してよいのかを判断する材料となることや、行政や企業がその事業やサービスを、そのままの状態でリリースする、ないしは継続してよいのかを判断する材料となること、さらに、行政・企業・個人といった利用者が、その事業やサービスを利用してよいのかを判断する材料となることにある。

[4] U.S. Department of State, "Privacy Impact Assessments" https://www.state.gov/privacy-impact-assessments-privacy-office/

[5] 参考：Davis Wright Tremaine LLP, "Texas Data Privacy and Security Act – An Overview, " July 6, 2023. https://www.dwt.com/blogs/privacy--security-law-blog/2023/07/texas-data-privacy-and-security-act-overview

■ 表 3 PIA の提供価値

| PIA の読み手 | PIA が読み手に提供する価値 |
|---|---|
| **一般個人** | 自身の情報が漏えい・暴露・改ざんされる「可能性」と「精神的なダメージの大きさ」を踏まえ、その事業やサービスに自身の情報を提供してよいのか、一般個人が判断する材料となること。 |
| **事業やサービスの提供者（行政・企業）** | 一般個人の情報が漏えい・暴露・改ざんされる「可能性」と「精神的なダメージの大きさ」を踏まえ、その事業やサービスをそのままの状態でリリースする、ないしは継続してよいのか、提供者が判断する材料となること。 |
| **利用者（行政・企業・個人）** | 一般個人の情報が漏えい・暴露・改ざんされる「可能性」と「精神的なダメージの大きさ」を踏まえ、その事業やサービスを利用してよいのか、利用者が判断する材料となること。 |

PIA 報告書の様式や目次構成、記載内容については、様々な有識者が様々な持論を展開している状況にあるが、本質を踏まえれば、以下のような取り組みを行うことが PIA に求められる。

■ 表 4 当社が提案する PIA の姿

| PIA が行うべき取り組み | | 具体的な取り組み内容 |
|---|---|---|
| **①PIA 報告書に記載されている内容が、事業やサービスの提供者に寄り添ったものではなく、客観的に判断した結果であることを担保すること。** | □ | PIA の実施者は、事業やサービスの提供者とは別とすること。 |
| | □ | PIA の実施者が事業やサービスの提供者となる場合は、PIA 報告書の公平性を、提供者とは利害関係の無い別の者が担保すること。 |
| **②一般個人の情報が漏えい・暴露・改ざんされる「可能性」は、性善説ではなく性悪説で評価すること。（但し、蓋然性のある範囲内であること。）** | □ | PIA の実施者は、事業やサービスの提供者から説明される対策を鵜呑みにせず、業務フローに沿い、自らがあるべき対策をイメージした上で、実際の対策と比較し評価すること。（最も良い方法は、ウォークスルー調査） |
| | □ | PIA の実施者は、一般個人の情報を窃取しようとする犯人（含：内部犯行）の立場に立って、現在の対策にセキュリティホールが無いか思考すること。 |
| | □ | PIA の実施者は、世の中で起きている情報漏えい事故等のインシデントとその手口を熟知していること。 |
| **③一般個人の情報が漏えい・暴露・改ざんされた場合の「精神的なダメージの大きさ」は、あらゆる立場の個人を想定した最大のもので評価すること。** | □ | PIA の実施者は、その事業やサービスに自身の情報を提供する（または収集される）一般個人がどのような方であるのかを漏れなくイメージすること。（例えば、著名人や著名な組織・地域に所属する者、障がい者、患者等） |

| PIA が行うべき取り組み | 具体的な取り組み内容 | |
|---|---|---|
| | □ | PIA の実施者は、自身の情報が漏えいした場合の精神的なダメージについて、被害者の立場に立ってイメージすること。（例えば、ストーカーに追われている方が自身の GPS 情報が暴露されたことを知ればどうなるか） |
| **④公表される PIA 報告書は、読み手が容易に理解できるものであること。** | □ | PIA 報告書内で専門用語を使用する場合は、別に専門用語の意味を付記すること。 |
| **⑤公表される PIA 報告書は、読み手がアクセスできるかたちで公表されること。** | □ | 公衆の場から一般個人の情報を収集する事業やサービスに関する PIA 報告書の場合は、PIA 報告書を Web サイト上等で公開し、かつ検索サイト等で検索されやすくなるよう、工夫すること。 |
| | □ | 将来的な事業やサービスの利用者（行政・企業・個人）に対しては、その事業やサービスの案内から遷移するかたちで、PIA 報告書を閲覧できるようにすること。 |
| | □ | 事業やサービスの提供者（行政・企業）に対しては、PIA の実施者が電子メールや対面・オンライン会議等の手段により直接的に報告を行うこと。 |
| **⑥PIA の結果、コンプライアンス違反が判明した場合は、是正勧告に類する内容を PIA 報告書内で明記すること。** | □ | PIA の実施者は、PIA の対象となる事業やサービスが遵守すべき法律、条例、行政のガイドライン等を把握すること。（多岐にわたることが予想されるため、予め事業やサービスの提供者からリストの提供を受けることが望ましい） |
| | □ | PIA の結果、コンプライアンス違反が判明した場合、PIA の実施者は是正勧告に類する内容を PIA 報告書内で明記すること。また、どうすれば違反しない事業やサービスになるのか、示唆を与えることが望ましい。 |
| **⑦PIA は、その他読み手が考慮すべき情報を記載すること。** | □ | PIA 報告書は、いつ時点での状態を所与として作成されたものであるのかを明記すること。 |
| | □ | PIA において、調査が十分できなかった事項を明記すること。（例えば、ネットワークで授受する情報が、通信間では暗号化されているという対策について、実際にそうなっていることは確認できず、事業やサービスの提供者が示す電子証明書をもとに評価をしていること等） |

## 4. PIA を実行する上での課題

当社では今まで、行政や民間企業における PIA を実施してきたが、その取り組みにおいて様々な課題を認識するに至っている。下表は、それらの課題と課題に対する対策の方向性について、当社としての見解をまとめたものである。

■ 表 5 PIA を実行する上での課題と対策の方向性

| PIA 実施上の課題 | 課題に対する対策の方向性 | |
|---|---|---|
| ①PIA の対象となる事業や、サービスを構成する情報システムに、行政のデータ連携基盤や汎用クラウドサービス、提供者である企業全体に共通する基盤システム（以降、「基盤」と呼称）が含まれている場合は、基盤としてのセキュリティ上の事由や、基盤を提供する組織の対応ポリシー等により、PIA として調査・評価を行うのが困難となることがある。 | □ | 基盤提供者側には、基盤を使用して提供される事業やサービスが PIA を実施する際に、基盤側として開示できる情報について予め整理しておき、都度の要請に応じる体制を整備することが期待される。 |
| | □ | PIA の実施者には、基盤側に提供を求めたい情報は必要最小限にとどめることとし、基盤側から必要な情報を提供いただけない場合は、過去のインシデント事例等からリスクを類推する取り組みが期待される。 |
| ②（主として行政が該当）PIA とは別に、特定個人情報保護評価を実施する必要がある場合は、調査・評価項目や内容がそれらの間で重複し、情報を提供する事業やサービスの提供者に過剰な対応負荷を与えてしまう可能性がある。 | □ | PIA に先行して特定個人情報保護評価が実施される場合は、特定個人情報保護評価の実施者から評価時に入手した情報を可能な限り得ることとする。逆に PIA が特定個人情報保護評価に先行する場合は、PIA の実施時に得た情報は可能な限り特定個人情報保護評価の実施者に提供することが期待される。 |
| ③PIA とは別に、情報セキュリティ監査やサイバー攻撃対応の状況を調査・評価する取り組みが別に存在する場合は、調査・評価項目や内容が、それらの間で重複し、情報を提供する事業やサービスの提供者に過剰な対応負荷を与えてしまう可能性がある。 | □ | PIA と、情報セキュリティ監査やサイバー攻撃対応の状況を調査・評価する取り組みは、同一の組織または共同体により実施されることが望ましい。 |
| | □ | PIA と、情報セキュリティ監査やサイバー攻撃対応の状況を調査・評価する取り組みが、別の組織により実施される場合は、互いに調査・評価項目や内容を共有し、できる限り取り組みが重複しないようにすることが期待される。 |
| ④PIA の実施を依頼する者が、PIA の実施者に支払うことのできる費用には制約があるため、PIA の実施者は必ずしも徹底的に PIA を行える訳ではない。（例えば、数百万円をかけて情報システム全体の脆弱性テストを行うことはほぼ不可能） | □ | PIA の実施者はその受託に当たり、調査・評価方法を具体的に明示し、当該 PIA における免責について PIA 報告書に明記すること。（免責の例文：「本報告書は、事業者より提供頂いた情報を基に作成いたしました。また、本報告書は、時間的制約およびコスト的制約のもとで作成いたしました。したがって、本報告書は、潜在するその他のリスクの有無や危険の増大要因をすべて網羅したわけではありません。」） |

| PIA 実施上の課題 | 課題に対する対策の方向性 | |
|---|---|---|
| ⑤PIA の実施を依頼する者が事業やサービスの提供者である場合、評価を良くしてもらえないと事業やサービスが売れないため、PIA の実施者に対して何らかの修正圧力がかけられる可能性がある。 | □ | PIA 報告書について、事業やサービスの提供者とは利害関係に無い者がその妥当性・公平性について確認を行うこと。（本当は他の ISO 等と同様に、PIA の認証機関が存在するとよい） |

## 5. まとめ

監視カメラ映像や位置情報、クッキー等の情報を含め、一般個人のプライバシーに関わる情報を容易に入手できるようになった昨今では、個人のプライバシー情報を守る取り組みは、世界共通の課題であると言える。一方で、個人のプライバシー情報を活用する事業やサービスには、市民の安全・安心や生活の質向上、利便性の向上につながるものが数多くある。事業やサービスの「ベネフィット」が「リスク」を上回ることは大前提であるが、どれだけ「リスク」を抑制すべきかという議論をするにあたっては、今後蓄積されるであろう様々な PIA 報告書がその材料となり、徐々に社会の共通認識として収斂されることを期待したい。当社としては、引き続き PIA の実施や PIA の実施支援を通じて、一般個人のプライバシー保護のあり方について考察を進めたいところである。

[2024 年 7 月 1 日発行]



ビジネスリスク本部
上級主席研究員　青島　健二（専門分野：新規事業開発、業務/IT 改革、企業リスク管理、海外現地法人管理）
主任研究員　渡邉　彩恵香（専門分野：企業等のリスクマネジメント）

〒100-0004 東京都千代田区大手町 1-5-1 大手町ファーストスクエア ウエストタワー23F
Tel. 03-5288-6580　Fax. 03-5288-6590 www.tokio-dr.jp