TOKIO MARINE

リスクマネジメント最前線

2025| No.7

自治体のデジタル実装における PIA の役割・あり方

ビジネスリスク本部　青島　健二　上級主席研究員（専門分野：経営管理、業務改革、ERM）
ビジネスリスク本部第五ユニット　渡邉　彩恵香　主任研究員（専門分野：リスクマネジメント）

スマートシティに関しては、本リスクマネジメント最前線において過去 3 回[1]にわたり寄稿をしてきたが、その間に国の政策や自治体の目指すデジタル実装の姿が相当に鮮明になってきている。特に、2022 年以降は「デジタル田園都市国家構想」に合致し採択されたデジタル実装事業には国からの補助金が拠出されるようになったため、自治体はその取り組みを一層加熱させ医療や介護の分野にも実装の対象を拡大させている。一方で、デジタル化されるデータに含まれる市民のプライバシーデータの「ガバナンス」、特に「プライバシー保護」は自治体にとって極めて重要な課題であるはずだが、それへの取り組みがデジタル実装の事業計画に十分に落とし込まれているとは言い難い。したがって本稿では、自治体のデジタル実装における PIA(プライバシー影響評価)の役割とそのあり方について言及するものである。

1. 政府（内閣府）の PIA 制度化に関するガイドライン

(1) 自治体におけるデータ連携基盤の活用に向けて

スーパーシティやスマートシティにおけるデータ利活用にあたって、「データ連携基盤」は不可欠な中核的基盤と位置付けられる。「データ連携基盤」とは、さまざまな主体（自治体、企業、市民等）が保有するデータを収集・整理し、異なる組織・サービスの間でそれらのデータを連携・共有することを目的とする基盤である。

内閣府は、スーパーシティやスマートシティの取り組み、およびそこにおけるデータ連携基盤活用を推進するため、2023 年に「**データ連携基盤に求められる互換性・安全性・プライバシーに関する事項**」の初版を公表した。当資料では、互換性・安全性・プライバシーの各観点に関してデータ連携基盤の整備主体が実施することが望まれる 118 の事項が列挙され、その中に「PIA の実施」が盛り込まれている。PIA とはプライバシー影響評価（Privacy Impact Assessment）の略で、市民のデータが多様な組織・サービス間で共有されることから生じるプライバシーの懸念に対し、データ連携基盤に接続する組織・サービスがどのような対策を講じているのかを評価・宣言する取り組みを指す。

2025 年 3 月、内閣府は「データ連携基盤に求められる互換性・安全性・プライバシーに関する事項」の関連資料として、「**データの利活用に当たって PIA をルール・仕組み化する際の検討ポイント**」（以下、「検討ポイント」）を新たに公表した。次項では、「検討ポイント」の要点を抜粋する。なお、「検討ポイント」の参考情報として「つくば市プライバシー影響評価制度検討懇話会 最終とりまとめ（令和 7 年 3 月）」が挙げられているが、これは令和 5 年度

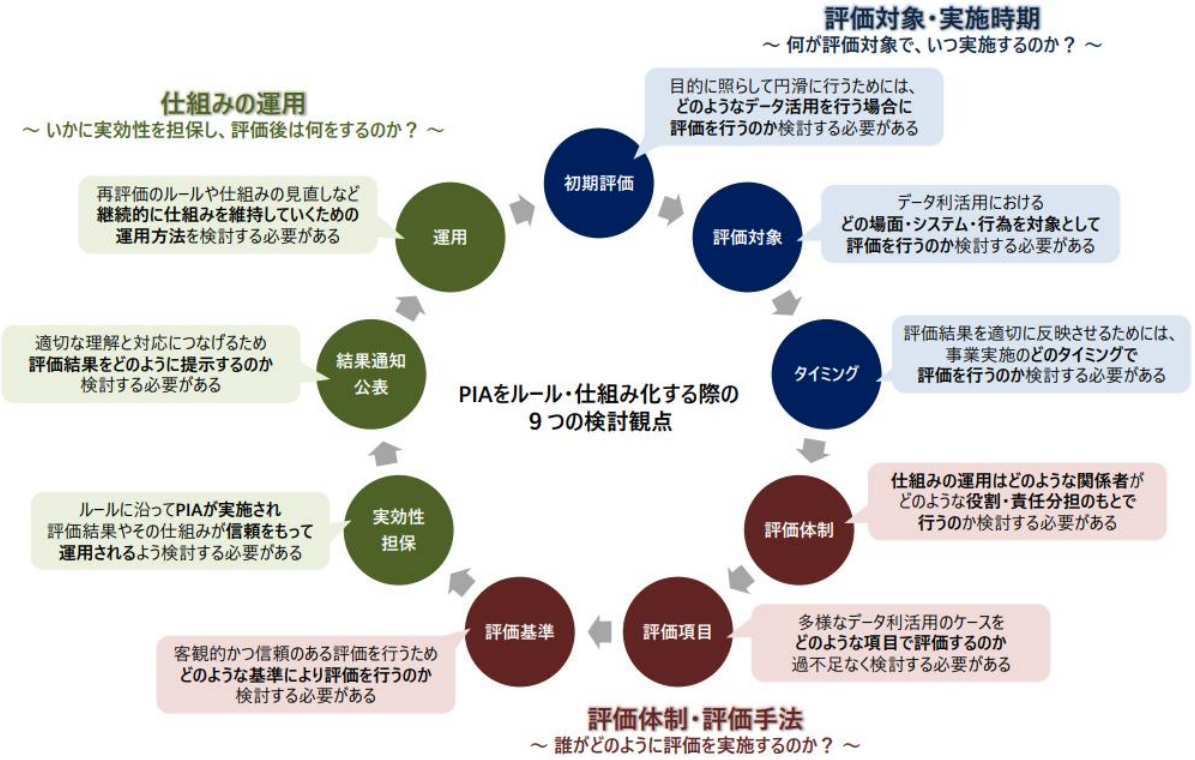
[1] 2020 No.20「スマートシティにおけるリスクマネジメント」、2021 | No.8「スマートシティにおける DX の重要性」、2024 | No.7「PIA（プライバシー影響評価）の現在地と課題」

にかけて東京海上日動火災保険株式会社および東京海上ディーアール株式会社（以下、弊社）が参画した公募事業「つくば市プライバシー影響評価制度策定支援業務」をベースとしたものである[2]。

(2) PIA 制度構築にあたってのポイント

PIA の制度を構築するにあたり、内閣府の「検討ポイント」は「評価対象・実施時期」「評価体制・評価手法」「仕組みの運用」の観点を重視している。特にスーパーシティ・スマートシティの取り組みを推進する自治体であれば、パーソナルデータを扱うサービスが複数・継続的に提供されることもあり、1 回限りの PIA 実施は望ましくない。将来提供されるサービスに対する PIA 実施、また既存サービスに対する定期的な PIA 実施等も念頭に置き、PIA を仕組みとして確立・運用することが求められる。

■ 図表 1 「PIA をルール・仕組み化する際の検討観点とその必要性」



出典：内閣府「データの利活用に当たってPIAをルール・仕組み化する際の検討ポイント」（2025年3月） P2より引用

弊社として、特に自治体ごとの事情を踏まえた検討を要する要素は「評価体制」および「運用」であると考える。

まず「評価体制」については、各自治体で PIA を所掌する部署以外に、自治体が任意で設置している諮問機関等を組み入れることもあり得る。こういった機関が存在する場合、PIA スキームのどこに・どの程度の関与度合いで組み込むのか、個々の事情に応じた体制構築が必要となる。また、自治体の職員には PIA 対象となるサービスのリスクを特定・評価するスキルも求められるが、仮に専門人材が不足する場合には外部機関への業務委託等により PIA の品質を担保することが一案となる。

「運用」についても上記の観点と関連する検討が必要だ。制度の見直しに際した諮問機関等との連携要領、PIA に携わる職員・機関の繁忙度等を考慮し優先度の高い案件のみ PIA 実施対象とする（「評価対象」の基準の調整も必要）など、検討すべき観点は多岐にわたる。いずれも、「4. 具体的な PIA 事例/イメージ」でも言及する。

[2] 出典：東京海上日動火災保険(株)・東京海上ディーアール(株)プレスリリース「スマートシティの「プライバシー影響評価」コンサルティングサービスの提供開始」

2. データガバナンスにおける PIA の役割

独立行政法人情報処理推進機構（IPA）の「信頼できるパートナーになるためのデータガバナンス読本」では「データガバナンスとは、自社の重要な資産であるデータを戦略的に管理・活用するための仕組みやルール、体制のことを指し、データの品質やセキュリティを保ちつつ、誰がどのように使えるかを明確にすることで、ビジネス価値を最大化し、リスクを最小化する取り組み」と定義されている。これを自治体に置き換えると、下表のように要素を整理することができる。

■ 図表 2 データガバナンスの項目（企業・自治体）

企業におけるデータガバナンス			自治体におけるデータガバナンス		
項目	例		項目	例	
自社の重要な資産であるデータ	a	特許	自治体の重要な資産であるデータ	a	自治体の特色
	b	生産データ		b	主要産品等のデータ
	c	販売地域データ		c	居住地域データ
	d	顧客データ		d	市民の行動データ
	e	上記のクロス分析結果（どこの地域のどういう属性の顧客に、どういう特許を使用したどのような製品が売れているのか）		e	上記のクロス分析結果（どこの地域のどういう属性の市民に、どういうサービスを提供すれば市民がより幸せになるのか）
戦略的に管理・活用するための仕組みやルール、体制	f	各種コードの名寄せ・統一	戦略的に管理・活用するための仕組み	f	マイナンバーカードによる各種コードの統一
	g	データウエアハウスの構築		g	データ連携基盤の構築
	h	CDO（最高データ責任者）の任命		h	CDO（最高データ責任者）の任命
ビジネス価値（指標）	i	売上額	自治体の価値（KPI）	i	人口
	j	利益額		j	地方税収
	k	マーケットシェア		k	住民の平均寿命
リスク	l	売上・利益の減少	リスク	l	人口・税収の減少
	m	評判の悪化		m	評判の悪化
	n	倒産		n	倒産
リスクの最小化（対策）	o	リスクの洗い出し・評価	リスクの最小化（対策）	o	リスクの洗い出し・評価
	p	ロスプリベンション（損失の未然防止）		p	ロスプリベンション（事業中止/未然防止）
	q	ロスミティゲーション（損失の最小化）		q	ロスミティゲーション（損失の最小化）

出典：弊社作成

企業においても自治体においても、リスクを負う上ではリスクを上回る価値を創出することが絶対条件である。企業の場合は、ERM（企業リスクマネジメント）と呼ばれる取り組みの中で、各事業・業務におけるリスク量の計量手法や、計量されたリスク量と期待される効果を比較評価する手法があるが、自治体の場合は今までそのような取り組みが必ずしも一般化していなかった。そこで、自治体にとって最大のステークホルダーである市民への負の影響を最大のリスクと捉え、プライバシーデータを活用した新規事業におけるプライバシーリスクへの影響を評価し公開する手法が PIA（プライバシー影響評価）であると捉えることができる。以下は、プライバシー影響評価に関する国際規格である

「ISO/IEC29134:2017」における標準的なステップと、各ステップにおける実施事項を関連するデータガバナンスの項目に紐づけたものである。

■ 図表 3 PIA の実施項目・実施事項とデータガバナンス関連項目との関係

ISO29134 に準じた PIA の実施ステップ	実施事項	ﾃﾞｰﾀｶﾞﾊﾞﾅﾝｽ項目*
【ステップ 0 】 初期評価	・ 事業実施可否評価 ・ PIA 実施可否評価	p
【ステップ 1】 PIA の必要性の決定	・ 実施責任者の任命	h
【ステップ 2】 PIA の事前準備	・ リスク基準	o
【ステップ 3】 アセスメント対象の説明	・ アセスメント対象のビジネスプロセス、情報システムの説明	a b c d e f g
【ステップ 4】 ステークホルダーのエンゲージメント	・ ステークホルダーの特定	-
	・ 協議およびコミュニケーション計画	p q
	・ ステークホルダーからのフィードバックの共有	
【ステップ 5】 プライバシー安全対策要件の決定	・ PII 情報フロー	g
	・ プライバシー安全対策要件のリスト	p q
【ステップ 6】 プライバシーリスクアセスメント	・ プライバシーリスクの特定	o
	・ プライバシーリスクの分析結果	
	・ プライバシーリスクマップ	
【ステップ 7】 プライバシーリスク対応の準備	・ プライバシーリスクに対する対応措置のリスト	p q
	・ 管理策のリスト、対応措置の実装	
【ステップ 8】 PIA のフォローアップ	・ PIA パブリックサマリ	i j k l m n o p q
	・ PIA 報告書	

*各記号は、【図表2】データガバナンスの項目（企業・自治体）における記号に紐づけている。

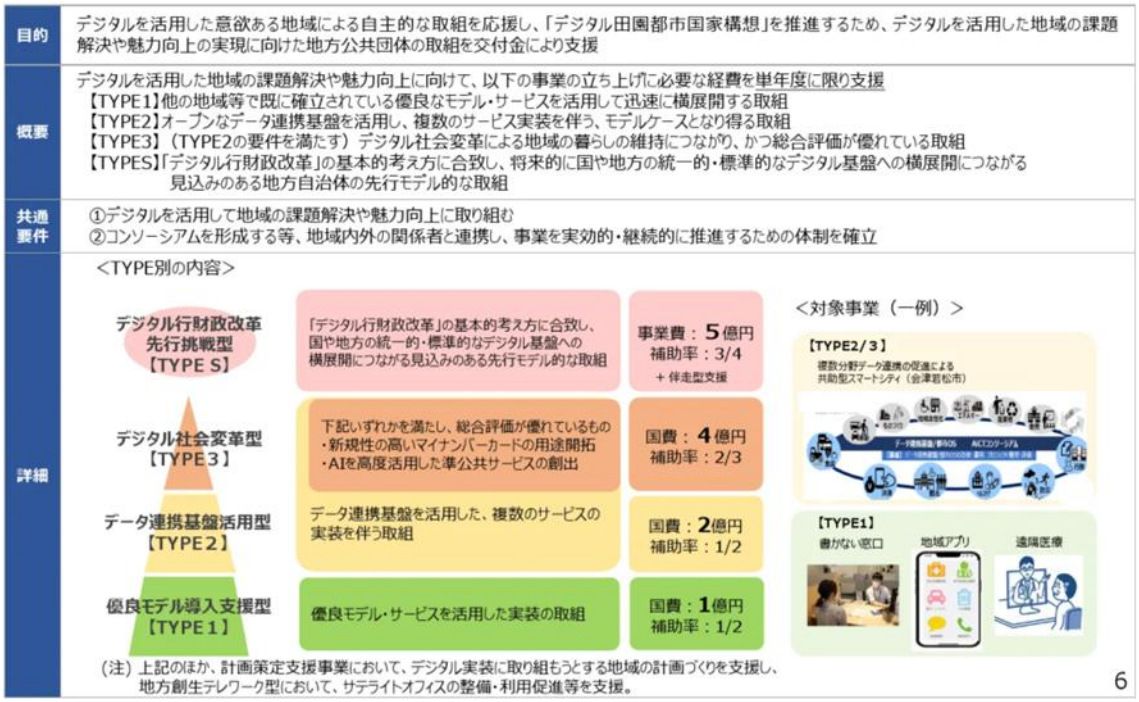
出典：弊社作成

3. デジタル田園都市国家構想（デジタル実装タイプ）における PIA 実施の必要性

デジタル田園都市国家構想とは、「デジタル実装を通じて地方が抱える課題を解決し、誰一人取り残されずすべての人がデジタル化のメリットを享受できる心豊かな暮らしを実現する」という構想であり、2022 年に内閣官房により策定された戦略に基づき、2023 年度から 2027 年度までの 5 ヵ年計画で推進されている。国に「デジタル実装タイプ」の対象事業として採択された場合は、2 分の 1 から 4 分の 3 の補助金が国から交付されることから、多くの自治体はデジタル実装を積極的に検討しており 2024 年度には 781 件の事業が採択された。以下のような分野で、成果が上がりつつある。

- 住民サービスの向上
  - オンライン申請や情報提供の拡充、AI を活用した問い合わせ対応等
- 教育分野の変革
  - オンライン学習の推進、学習教材のデジタル化、遠隔教育の実施等
- 医療・福祉分野の効率化
  - オンライン診療、遠隔医療、健康管理アプリの導入等
- 地域経済の活性化
  - デジタル技術を活用した地域産品の販売促進、観光情報の発信等
- 防災・減災対策の強化
  - 防災アプリの開発、避難情報の発信、ドローンを活用した情報収集等

■ 図表 4 デジタル田園都市国家構想における「デジタル実装タイプ」の制度概要



出典：デジタル田園都市国家構想交付金について（令和６年４月内閣官房、内閣府）

しかしながら、自治体が所管するサービスや情報システムにおいて、住民のプライバシー情報が漏えいするなどのインシデントは毎年複数件が確認されており、2024 年においては下表の通りである。攻撃と防御が「いたちごっこ」の状況

であり完全な防御が困難とされるサイバー攻撃だけでなく、担当者の不注意が原因のインシデントも含まれていることから、自治体におけるデータガバナンスが依然として十分ではない実態が垣間みえる。

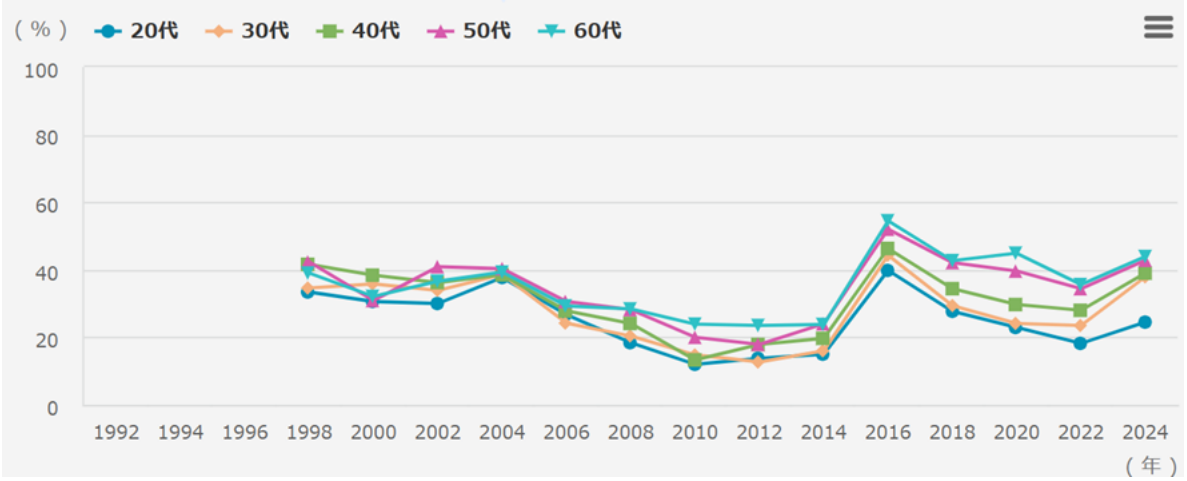
■ 図表 5 2024 年に自治体で発生した情報漏えいインシデントの例

発表時期	自治体	概要
2024 年 2 月	大阪市福祉局	障がい福祉サービス事業所等宛ての事務連絡を行う際に誤って個人情報が記載されたファイル等を添付送信し、7,468 人の個人情報が漏えいした。個人情報には氏名、住所、一部に電話番号や生年月日も含まれていた。
2024 年 2 月	宮崎県東諸県郡綾町役場	2 件の個人情報漏えい事案が発生した。1 件は町民の情報がホームページに不適切に公開され閲覧できる状態になっていた事案、もう 1 件は介護情報を誤った FAX 番号へ送信してしまった事案であった。
2024 年 2 月	鹿児島県出水市	市が管理するメール中継サーバが不正アクセスされ、特定のメールアカウントを不正利用し市の教育機関宛にスパムメールを送信した事案が発生した。この不正アクセスは 2 日間にわたり行われ、結果として 129,975 件のスパムメールが送信された。
2024 年 3 月	淀川河川公園管理センター	管理センター運営のホームページでサーバへの不正アクセスが発覚。システム改修時に発生し、約 3 万 4000 名の利用者情報流出の可能性がある。影響を受ける情報には氏名、生年月日、性別、住所、電話番号、メールアドレス、銀行口座、ログイン情報が含まれ、メールアドレスと銀行口座は暗号化されているものの、他の情報は非暗号化の状態であった。

出典：株式会社アクト社ホームページ

市民は、自身のプライバシー情報をどのように取り扱われるか不安を覚えており、ひとたび情報漏えいのインシデントが発生するとその不安が不信となって顕在化する。例えば 2015 年に日本年金機構への標的型サイバー攻撃で、125 万件の年金個人情報が流出したインシデント発生時は、「国民総背番号制（現在のマイナンバーカード制度）は個人のプライバシーが守られないと思う」と回答する市民が 20 代から 60 代にわたる全ての年代で 4 割を超えた。特に、年代が高くなるほどそう思う市民の割合が増加する傾向にあり、60 代においては 6 割に迫る結果であった。高齢化が都市部よりも進行する地方においては、「デジタル実装」が市民に受け入れられる鍵の一つは、プライバシーデータのガバナンスにあるといっても過言ではない。

■ 図表 6 生活定点調査「国民総背番号制は個人のプライバシーが守られないと思う」



出典：生活総研「生活定点調査」

以上のことから、自治体におけるデジタル実装は「地方が抱える課題を解決し、誰一人取り残されずすべての人がデジタル化のメリットを享受できる心豊かな暮らしを実現する」上で必要であるものの、データガバナンスの不備が原因で個人データ流出等のインシデントがひとたび起きてしまうと、市民が自身のデータ提供を拒否するような事態が想定される。そして、自治体が市民のプライバシーデータを収集・活用できなくなると、デジタル実装の目的が十分に達成できなくなってしまう。そのような事態を防ぐために必要な取り組みが、PIA であると考えることができる。

4. 具体的な PIA 事例/イメージ

弊社はこれまで、東京海上日動火災保険株式会社と連携の上、茨城県つくば市（2022 年 4 月、スーパーシティに指定）および長野県茅野市[3]（同、デジタル田園健康特区に指定）に対し、PIA 制度構築支援ならびに PIA 実施支援を提供してきた。それらの実績を踏まえ、自治体における PIA 制度の具体的なあり方・考え方を紹介する。

(1) 内閣府「データの利活用に当たって PIA をルール・仕組み化する際の検討ポイント」と具体的実践

内閣府の「検討ポイント」では PIA 制度構築に際する 9 つの観点が挙げられている。各観点について、弊社が重要と考える点を整理した。内閣府の「検討ポイント」内の解説と重なる部分もあるが、一部ではより実務に近い要点も記載している。

■ 図表 7 内閣府の「検討ポイント」と弊社の PIA 支援における基本的考え方

内閣府の「検討ポイント」が示す観点		弊社の PIA 支援における基本的考え方（※一部、内閣府ガイドラインと重なる部分あり）
1. 評価対象・実施時期		
	初期評価（PIA 実施要否の判定条件設定）	• 欧米の**先行する PIA 事例**等を踏まえ、PIA 対象／対象外を定める基準を協議・決定。 • 結果的に対象となる事業数が、PIA **運用に支障をきたさず**、かつ真に **PIA 実施が求められる事業が抜け落ちない**よう考慮。
	評価対象（PIA 対象とする場面・システム・行為の設定）	• PIA 対象の事業・サービスについて、**データのライフサイクル等**を明らかにした上で PIA 対象とする範囲を明確化。（例）PIA 対象サービスの事業者の委託先のうち、ISMS（情報セキュリティマネジメントシステム）認証取得済みの企業が提供するプラットフォームは PIA の対象から除外
	評価実施タイミング	• サービスイン前の事業に対する PIA の場合、サービスの設計・開発・実証等計画への影響をなるべく抑えたタイミングで実施。 • サービスイン後の事業に対する PIA の場合、サービス提供時の状況を詳細に把握の上評価。評価の結果、事業者が実施可能な範囲で効果の高いリスク対策を検討・実施することが重要。
2. 評価体制・評価手法		
	評価体制（PIA 運用に際しての関係者、責任の所在、役割分担）	• 各自治体の PIA 所管部署の他、諮問機関等の関与の程度・あり方を決定。 • PIA を行うことと、対象となったサービスの安全性が完全に担保されることは**イコールとはならず**、PIA 実施主体ではなくサービス提供事業者が引き続き安全性の確保に努めるとすることを推奨。

[3] 東京海上ディーアール(株)・長野県茅野市「茅野市における「プライバシー影響評価」に関する制度策定」

内閣府の「検討ポイント」が示す観点		弊社の PIA 支援における基本的考え方 （※一部、内閣府ガイドラインと重なる部分あり）
	評価項目（多様なデータ利活用のケースへの適用を前提）	• 前述の ISO/IEC29134:2017 やこれに対応する JIS X 9250、そのほか複数の基準等を参照しながら、様々な事業を一律の基準で評価するための評価項目一覧を作成。
	評価基準	• （個別評価）上記の各項目について、リスクが顕在化した際の「影響度」および「起こりやすさ」を判定する基準を設定。 • （総合評価）各評価項目の結果全体を踏まえ、PIA 対象のサービスが安心して利用可能なのか、またはリスク軽減措置の実施が求められるのか等を判定する基準を策定。
3．仕組みの運用		
	実効性担保（ルールに沿った PIA 実施、評価結果に対する信頼性確保のあり方）	• 評価結果に対する信頼性確保にあたっては、PIA フローに、第三者による評価結果のレビューを組み込むことを推奨。
	結果通知・公表	• PIA 対象サービスの事業者に対する結果通知とあわせて、どのようなリスク対策を求めるのか（何を・いつまでに）、対象サービスは実施可能なのか等を明らかにする。 • PIA 結果を誰に、どのような方法で公表するかを検討。市民向けに広く公表する場合は、簡潔かつ平易にサマライズした内容を公表すること等が有効（次項でも解説）。
	PIA 制度の運用	• 定めた PIA 制度（運用ガイドライン、評価項目、評価用各種フォーマット等）が実施できるよう、定期的（年に一度等）な制度の点検・見直しの実施を推奨。

出典：「内閣府の『検討ポイント』が示す観点」については内閣府「データの利活用に当たって PIA をルール・仕組み化する際の検討ポイント」（2025 年 3 月）より引用。他の部分は弊社作成。

(2) 弊社が考える PIA ツールキット

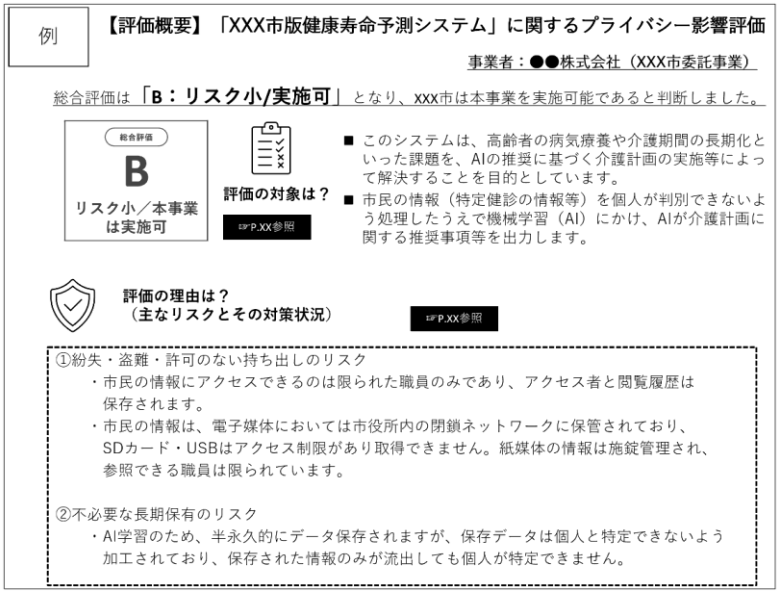
最後に、PIA の仕組み化・制度化にあたって、各自治体において弊社が必要と考えるツールを紹介する。上記「PIA 制度の運用」の考え方でも触れているが、当該自治体が定める PIA の意義や手順・基準等を記載した「運用ガイドライン」（仮称）や、PIA の要否判定から最終的な結果通知までの一連の手続きで用いるフォーマットの他、PIA 報告書のひな型も揃えられるとよい。なお、制度上の建付けは各自治体が整理する必要がある。

■ 図表 8 弊社が考える PIA ツールキット

名称（仮称）	位置付け、主な内容
運用ガイドライン	PIA の実務手順等を記載する文書。 • PIA の意義や狙う効果 • 初期評価（＝あるサービスに対する PIA 実施要否の判定）の基準、要領 • PIA 実施体制ならびに手順の総論 • PIA 実施手順の各論（事業者へのヒアリング、リスク評価、評価結果の審議・確定、事業者への通知、結果の公表等） • 事業者に提出・開示を求める情報の一覧（対象サービスのシステム構成図、取り扱われるプライバシー情報の内容、データ処理の方法等） • リスク評価項目および基準（各項目の個別評価ならびに総合評価の尺度） • PIA 評価結果ごとの事業者への要求事項
PIA フォーマット	PIA を実施する際に用いるフォーマット（様式）。 • PIA 初期評価書・・・対象サービスが該当する PIA 実施要件を明らかにする。 • PIA 調査シート・・・リスク評価項目を羅列。事業者が、対象サービスのリスク対策状況等について回答するための調査票。 • PIA 一次評価シート・・・調査シートの回答内容を受け、PIA 実施主体（一義的には自治体の PIA 所管部署）が対象サービスのリスクの程度を判定するための様式。 • PIA 評価結果審議シート・・・自治体が実施した一次評価結果の妥当性を、第三者機関ないし会議体が審議する際に用いる様式。場合により一次評価結果の修正が提案される。
PIA 評価報告書のひな型	事業者・PIA 関係者向け／市民（サービス利用者）向けたそれぞれのひな型。 • 事業者・PIA 関係者向け報告書・・・PIA 実施概要、システム構成図、データのライフサイクル、評価結果の詳細、リスク改善要求の詳細等を記載。 • 市民（サービス利用者）向け報告書・・・総合評価結果（A 評価、B 評価等）をわかりやすく記載するとともに、サービスの概要・主なリスクとその対策状況等を中心に平易に記載。万が一リスクが比較的高いと判断された場合は、事業者によるリスク対策実施によりリスクが軽減されたと確認できたのちに作成・公表することも一案である。

出典：弊社作成

■ 図表 9 PIA の評価報告書（市民（サービス利用者）向け）のイメージ



出典：弊社作成

5. おわりに

PIA の実施は 2025 年 7 月時点の国内において法的に義務付けられておらず、したがって“これさえ実施すればよい”という拠り所が存在しないのが実態だ。自治体の PIA 導入にあたっては何よりも PIA の仕組み化に労力を要するため、本稿で取り上げた先行的事例やポイントを踏まえつつ、最低限必要な環境・ツールを整備することから始めることを提案したい。特にツールや具体的な実施要領は、現に存在するサービスを対象とした PIA を実施する中で改善を図り、各自治体の実状に見合ったものとしていくことが望ましい。

[2025 年 8 月 18 日発行]

東京海上ディーアール株式会社

ビジネスリスク本部
上級主席研究員　青島　健二（専門分野：経営管理、業務改革、ERM）
主任研究員　渡邉　彩恵香（専門分野：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