

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（概要版） 目次

0	はじめに	P 2
1	初期評価／評価対象／実施のタイミング	P 3
2	評価項目／評価基準	P 4 – 5
3	評価体制における役割・責任／実効性の担保	P 6
4	結果の通知と公表／運用	P 7
5	参考情報	P 8

0 はじめに

- 本書は「つくば市プライバシー影響評価制度検討懇話会」にて協議・検討した事項を踏まえ、つくば市が確立すべき「プライバシー影響評価制度(以下、PIA制度)」の方向性について一定の整理を行い、取りまとめた概要書である
- つくば市は、人々の生活の利便性を向上させるスマートシティの取組の1つである、「つくばスーパーサイエンスシティ構想」の実現に向けて、先端的サービスの社会実装を推進するとともに、パーソナルデータを連携・利活用することでサービスがもたらすプライバシーへの影響を適切に評価するPIA制度の確立を目指している
- なお、PIAの評価を行うことによって、個人に関する情報を利活用する事業のプライバシーにおけるゼロリスクを保証するものではない点については留意いただきたい
- また、評価実績を有していない現時点では合理的な根拠をもって全ての考え方を整理することは難しく、またプライバシーに関する社会の動向は変化が激しく、PIA制度のあり方も常に変化するため、本書の内容が未来永劫正しいとは限らず、継続的に見直しを図っていくものである

1 初期評価／評価対象／実施のタイミング

初期評価

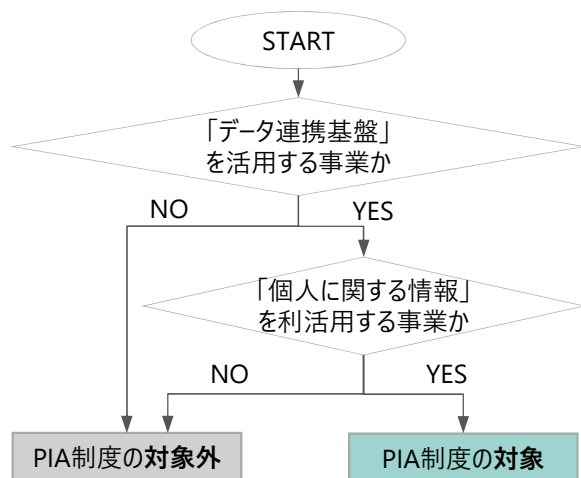


図1 PIA可否を判断する初期評価の流れ

- ・ プライバシー影響評価を必要とするか否かについて、2つの基準より初期評価を実施する
 - 「データ連携基盤」を活用する事業か
 - 「個人に関する情報」を利活用する事業か

なお、「個人に関する情報」の定義について、個人情報、仮名加工情報、匿名加工情報、個人関連情報の4つを適用範囲とするのが分かりやすい一方、評価対象となる情報が膨大なものになってしまい、実効性が低下する懸念があるため、当面の間は以下のとおり最低限必要な範囲に限定した形で制度運用を開始する

- － 生存する個人に関する情報のうち、個人情報(マイナンバーを除く)及び特定の個人関連情報(趣味嗜好、取引履歴、利用履歴、財産情報、身体・容姿に関する情報、位置情報等)

評価対象

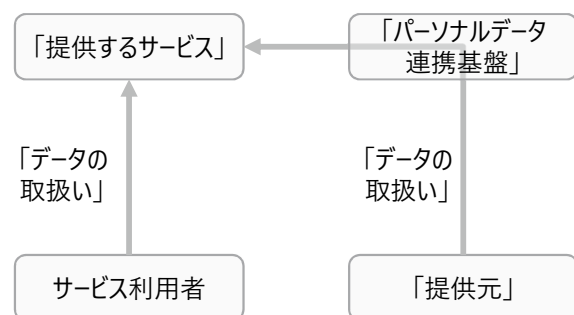


図2 サービス構成の全体イメージ

- ・ 「データ連携基盤」に接続し、「個人に関する情報」を利活用するサービスが取り扱う情報の処理の流れ、関係者、実施体制、本人同意の有無といった、**サービス構成全体が対象**

「提供するサービス」を評価するというPIA制度の趣旨に鑑みると、様々なデータを仲介し、サービスに繋ぐ土管の役割を担う「パーソナルデータ連携基盤」や、基盤を通じて連携させる「データの提供元」は、「提供するサービス」からは独立して運営されているものであることから、当該サービス及び、当該サービスに関する「データの取扱い」に関する部分が評価対象となる。

タイミング

- ・ PIAを実施するタイミングについて、「初回」・「再評価」の2点について検討
 - 「初回」は、評価の結果次第で措置を講じる必要が出てくるため、詳細な設計・開発に取りかかる前が費用対効果等の観点から推奨
 - 「再評価」は、提供中のサービスに大幅な仕様変更等、PIA制度に大幅な見直しが生じる場合が該当(詳細は「4 運用」にて後述)

2 評価項目／評価基準①

- PIAに関する複数の規格・基準^{*1}から共通項目を考慮し、必要十分な評価項目を作成 (右表はイメージ)
- 全22項目(64の質問)で構成^{*2}されており、内訳としては、
 - サービスの概要及びデータの取り扱い
 - 情報の通知・同意の取得などプライバシーへの配慮
 - 個人に関する情報に対する安全管理措置 等
- なお、今後評価を行う過程で明らかになった課題や、時代の変化に応じて評価項目の見直しは定期的実施する

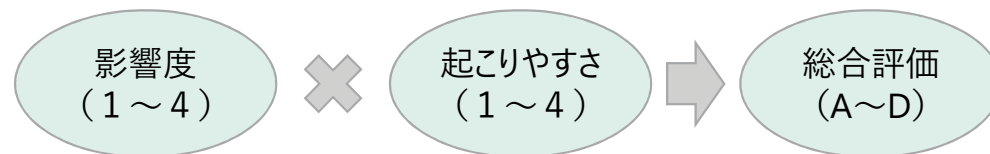
^{*1} JIS X 9251, GSCA PIAモデルポリシー, 特定個人情報保護評価 等

^{*2} サービス提供事業者が行政・民間の違いで差を設けることはなく、同一の尺度にて構成

1	サービスの概要
2	サービスの関係者
3	サービスが適合する個人情報保護に関する法令・制度・ガイドライン
4	サービスの業務の流れ
5	サービスにおける情報のライフサイクルと情報の種類
6	データや情報システムの保管場所に関する情報
7	第三者へデータ（個人情報）を提供・共有するか、する場合は同意を取っているか
8	個人情報の取り扱いについて、いつ利用者に通知されるか、利用者本人に同意を取得するか、同意を得ない場合はその根拠
9	利用者が同意後に、使用する個人に関する情報を選択したり、削除したりできるか
10	情報の開示請求窓口（その他相談窓口を含む）が設置されているか
11	個人に関する情報が紛失・滅失・毀損し、使えなくなる可能性はないか
12	個人に関する情報の漏洩・盗難・許可されていない持ち出し又は外部への不適切な提供が発生しないか
13	個人に関する情報への許可されていないアクセスが発生しないか
14	個人に関する情報の許可されていない変更が発生しないか
15	個人に関する情報の過剰収集が発生しないか
16	個人に関する情報の処理目的に関する情報が十分、かつ、いつでも確認できる状態にあるか
17	個人に関する情報の不必要な長期保有が発生しないか
18	サービスを提供することにより不利益を被る住民がいないか、不当な扱いを受けることがないか
19	サイバー攻撃を未然に防止、及び攻撃に遭った際の被害の最小化が実現できるか
20	情報システムの点検・監査により、情報セキュリティ体制が適切に管理されるか
21	本サービスを扱う担当者に対し、情報セキュリティ対策に関する適切な教育・研修を講じるか
22	目的外利用が発生しないか

図3 PIAで必要と考える評価項目

- サービスで利活用する個人に関する情報がプライバシーに及ぼす「影響度」と、リスクの「起こりやすさ」の2つの評価を掛け合わせて「総合評価」を導出する



評価	残存リスク	判断の目安
A	微小	想定されるリスクは極めて少ないと推定されるが、ゼロリスクではないことを理解のうえ判断することを推奨
B	小	想定されるリスクは少ないと推定されるが、利用は必要性和とのバランスで判断することを推奨
C	中	中程度のリスクがあることを十分理解のうえ、利用を慎重に判断することを推奨
D	大	利用には重大なリスクを伴うことを理解のうえ判断することを推奨

図5 総合評価（凡例）

影響度 ↑ 高い ↓ 低い	4	C (or B)	C	D (or C)	D
	3	B	C (or B)	C	D (or C)
	2	B (or A)	B	C (or B)	C
	1	A	B (or A)	B	C (or B)
		1	2	3	4
	起こりにくい ← 起こりやすさ → 起こりやすい				

図4 総合評価

A-B、B-C、C-Dの評価の狭間に位置する座標は、機械的な基準の適用により事業者側の努力を反映せず、結果的に制度の有効性を損ねるおそれがあるため、総合的に評価した上でどちらの評価にも倒せる余地(or)を残している

2 評価項目／評価基準②

【影響度】

- 個人に関する情報が漏洩した際に本人に与える影響を「精神への影響」・「財産への影響」の2軸で定義
- 利活用する情報の種類より、1～4の評点で判定し、影響度の高い方を当該サービスの「影響度」として評価

【起こりやすさ】

- 評価項目のうち、個人情報保護法等で対応が必須か否かで「必須」・「推奨」を分類
- 「必須」「推奨」で評点方式に差があり、評価項目の中で、最も高い評点を当該サービスの「起こりやすさ」として評価

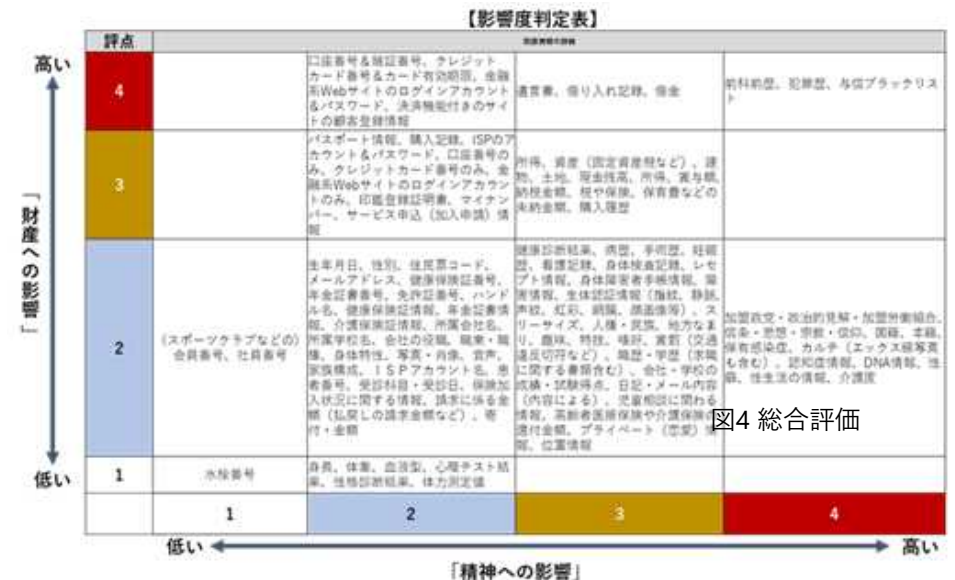


図6 影響度判定表

「身体への影響」についてはサービスの内容によって異なるため、都度、評価委員会で議論のうえ、影響度の評価に加味する

【左表の説明】

- No.7：評価項目が「必須」のみで、対応済のケース
- No.8：評価項目が「必須」のみで、未対応のケース
- No.13：評価項目に「必須」「推奨」が混在しているケース

【評点方式の補足】

評価項目の64の質問に対する回答を踏まえ評点を実施

- 「必須」：1つでも対応できていない場合は4点
- 「推奨」：1つ対応できていない場合は1点加算し、3つ以上対応できていない場合は最大4点

No	評価項目	必須/推奨	対応状況	評価
7	第三者へデータ（個人情報）を提供・共有するか、する場合は同意を取っているか。 ※個人情報保護法に基づき適切に対応している場合は要件を満たしているとする	必須	対応済	1
No	評価項目	必須/推奨	対応状況	評価
8	個人情報の取り扱いについて、いつ利用者に通知されるか。利用者本人に同意を取得するか。同意を得ない場合はその根拠を明示。	必須	未対応	4
No	評価項目	必須/推奨	対応状況	評価
13	個人に関する情報への許可されていないアクセスが発生しないか。			3
	(省略)			
	③アクセス権の割り当てに関する手順・要領を組織内で整備しており、本サービスでもそれに従ってアクセス権を付与する。	必須	対応済	
	④アクセス権者を必要最低限となるよう定期的に見直すこととしている。	推奨	対応済	
	⑤本サービス実施に際しての事業者のアクセス権は、本サービスに関する契約の終了時、または市と事業者が合意するタイミングに削除されることになっている。	推奨	未対応(+1)	
	⑥ログオンに際しパスワードを用いる際、組織内でパスワード設定に関する（パスワードの変更サイクルを定めている、適切な文字種類を用いることとしている等）組織内規程を定めた上で、対策を実施している。	推奨	未対応(+1)	

図7 評点方式のケース

3 評価体制における役割・責任／実効性の担保

- PIA制度の運用に当たって、
 - 評価にかかる実施体制の監督及び、評価結果・制度運用に関する説明責任を果たす「**最高プライバシー責任者(CPO)**」を庁内に設置する
 - 評価結果の妥当性・制度運用に関して第三者の助言を期待し、市民・有識者等を構成員とした「**プライバシー影響評価委員会**」を設置する
 - PIA制度及び、プライバシーインシデント発生時にサービスが及ぼす損害に関して、**責任分界点**は下表のとおり整理した

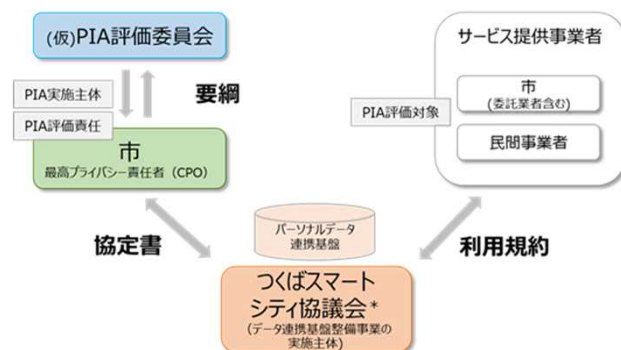


図8 評価体制のイメージ

図9「PIA制度」における責任分界点

市	・ PIA評価結果及び、制度運用にかかる 説明責任を負う
サービス提供事業者	・ PIA申請内容に関する 責任を負う
データ連携基盤整備主体（協議会）	・ サービス提供事業者に対してPIA評価を実施させる 責任を負う ※なお、再評価の実施要否においてはサービス提供事業者の責任が問われる場合もあるため、この限りではない
利用者	・ - （なし）

※なお、プライバシーインシデントを原因として発生した損害の責任分界点は、PIA制度の責任分界点とは異なり、PIA評価の有無に関わらず、法的根拠に基づき判断されるものと考えられる

- 市におけるPIA制度の実効性を担保する方法として、今回の制度の主旨と照らし、「条例」ではなく、「**要綱**」を用いる
- また、関係者間で以下取り決めをすることで、規律を保ち、PIA制度全体の実効性を担保する
 - 市－協議会：「**協定**」
 - 協議会－サービス提供事業者：「**利用規約**」
- 評価結果を踏まえた、サービスのデータ連携基盤への接続可否について、「協定」・「利用規約」で規定するか否かは本懇話会で結論は出さず、今後の判断に委ねることとなった

文書	内容
1 要綱 市におけるPIA制度として市長が制定	■ データ連携基盤に接続し、パーソナルデータを送受信してサービスを提供しようとするサービス提供事業者に対して、すべてPIAを実施すること ■ PIAの評価方法や評価体制（委員会設置等）を規定 ■ 年1回程度、評価委員会に全体状況を報告する（モニタリング）
2 協定書 つくば市とデータ連携基盤整備主体（つくばスマートシティ協議会）との間で締結	■ 要綱の実効性を担保するための運用を明確化 協議会は、データ連携基盤に接続しようとするサービス提供事業者について市へ通知し、サービス提供事業者が市のPIAを受けさせる 市は協議会からの通知に基づきPIAを実施し、その結果をサービス提供事業者及び協議会に報告する
3 利用規約 データ連携基盤への接続を希望するサービス提供事業者が遵守する事項として、協議会が定めるもの	■ データ連携基盤に接続するサービス提供事業者が遵守する項目を規定 データ連携基盤に接続する者の義務・責任、禁止事項、料金、手続き等 評価結果が公表されることを事前に了解のもと、市のPIA評価を受けることに合意すること 市のPIAに対して正確な情報を申告すること データ連携基盤からの接続を解除する該当事項を明示

図10 要綱・協定・利用規約の関係性

4 結果の通知と公表／運用

- 市は決定した総合評価の結果を、
 - ① 協議会・サービス提供事業者に速やかに「通知」する
 - ② 評価書の形で対外的に「公表」する
 - － 評価書は「詳細版」と「概要版」を用意する
 - － 利用者がプライバシーの観点より、サービスを利用するか否かを判断するための材料として、評価結果とサービスの概要を記載したものとする
- また、評価結果の通知を受けた協議会・サービス提供事業者が改善措置を講じた場合、その措置の内容をPIA評価とともに公表する仕組みを検討・導入する
 - － 例えば、総合評価「C」であったものの、サービス提供事業者の自助努力で「B」相当に改善が図られた場合等が該当する

【評価概要】「小児向けオンライン診療サービス（仮）」に関するプライバシー影響評価
事業者：株式会社A

つくば市は「PIA評価委員会」の評価案を参考に、本事業の総合評価を「B：リスク小」としました。

総合評価 B リスク小 (想定されるリスクは少ないが、利用は必要性和のバランスで判断)	事業概要 09.000000	■ 子どもの適切な医療診断には既往歴等を加味することが重要です。本サービスは、かかりつけ医が保有する診療記録をデータ連携し、夜間・休日のオンライン診療に活用するものです。 ■ 診療時間外である休日・夜間でも、自分の診療記録を使ってオンライン診療が受けられる安心・安全な子育て環境の構築を目指します。 ■ 本人がアプリに入力した問診情報と、かかりつけ医が保有している診療記録を突合し、オンライン診療を行う医師が参照のうえ診療を行います。
事業の対象者 取り扱う個人に関連する情報	体調を崩した子どもの保護者 氏名、生年月日、保険証番号といった本人確認情報の他、治療歴、薬歴、予防接種歴、アレルギーといった本人の健康や身体に関する医療情報	

想定される主なリスク

- 診療記録に記録された本人のアレルギー情報や身体・精神障害の情報といった機微度の高いプライバシー情報を取り扱うことから、リスク発生時の影響度が高いことが想定されます。

リスクに対して取られている対策と総合評価の理由

- 取り扱う個人に関する情報は国際基準を満たしたデータセンターで保管されており、事業者もプライバシーマークの認定を受けています。情報の取り扱いについても適切な対応がとられていることから、リスク発生の「起こりやすさ」は低いものと想定されます。
- 取り扱う個人に関する情報の機微度は高いものの、それに見合う十分な安全管理措置、運営体制がとられ、利用者への説明責任も果たされる仕組みが構築されている点を総合的に判断し、「B」と評価しました。リスク発生時の影響度を理解したうえで、サービスから得られるメリットと比較し、利用の判断を行ってください。

※ 本評価書は、事業者が提供するサービスと併せて、当該サービスの利用に必要と認められる範囲で公表するものとします。実際の事業実施にあたっては関係法令も踏まえ事業が実施されます。

図11 評価報告書（概要版）のイメージ

- サービス提供開始時に受けた総合評価(A~D)が変わる可能性が見込まれる場合は「再評価*1」が必要となる
 - i. 「PIA制度」に大幅な見直しが生じた場合
 - － 法令・ガイドラインの改正や社会の動き等により、PIA制度の大幅な見直しが必要となった場合
 - ii. 「サービス」に大規模な変更が生じる場合
 - － 大規模なシステム改修や新技術開発等に伴う大幅な仕様変更、取り扱う個人に関する情報が変わり影響度判定に変更がある、サービス提供者に体制変更がある場合

有効期間
・ 時代の変化、技術の変化とともにPIA制度の見直しを行う可能性がある ・ PIA制度に見直しがあった場合の再評価及び、過去に受けた評価結果の有効期間について、評価実績を有していない現時点においては適切な判断が難しいため、明確な基準は設けず、「都度」判断することとする

制度運用において発見される課題
・ 制度運用過程で明らかになった課題に対する対応はCPOの権限・責任のもと、評価委員会に諮ったうえで、市が対応方針を決定し、必要な措置を講じる

*1 再評価の程度について、1 から評価をやり直すべきものと、変更による差分だけを評価すれば足りるものとに分けられることが想定されるが、現時点で基準を細かく決めることはせず、今後の運用の中で調整する

参考情報

- つくばスーパーサイエンスシティ構想（P2）：個人に関する情報を含む都市の様々なデータを「データ連携基盤」を活用して、新たな先端的服务として官民を問わず社会実装し、人々の生活の利便性を向上させるスマートシティの取組の1つ
- 影響度（P5, 6）：プライバシーインシデント発生時にサービスで利活用する個人に関する情報がプライバシーに及ぼす「影響度」
- 起こりやすさ（P5, 6）：プライバシーインシデントの発生リスクの「起こりやすさ」
- プライバシーインシデント（P7）：プライバシーにかかわる不適切な事案（例：個人情報漏えい、滅失、毀損等）
- 条例（P7）：市民の代表である議会の議決を経て制度化する方法。法的拘束力を持って義務や罰則を定めることができる
- 要綱（P7）：市長の権限で適時に制度化することができる方法。法的拘束力を持った形で義務や罰則を科すことはできない