「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（2025 年）３月

つくば市プライバシー影響評価制度検討懇話会

目次

0　はじめに

0.0　制度検討の背景

つくば市は、住民のつながりを力にして、大胆な規制改革とともに先端的な技術とサービスを社会実装することで、科学的根拠をもって人々に新たな選択肢を示し、多様な幸せをもたらすことを目指す、「つくばスーパーサイエンスシティ構想」を推進している。この取組を法的にも後押しすべく、2022 年 4 月 12 日に政府から「スーパーシティ型国家戦略特別区域」として区域指定され、現在様々な取組を進めているところである。

「つくばスーパーサイエンスシティ構想」は、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[1]」を活用して、新たな先端的サービス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つであり、都市の持つデータをいかに有機的に連携させ、有効に活用し、データの利活用なしには実現できないような新たな体験を市民生活に還元していくかが大きな鍵を握る。

こういった目的の下、つくば市においては、官民が連携した本構想の推進役として「一般社団法人つくばスマートシティ協議会[2]」（以下「協議会」という。）を設立し、これを中心に様々な先端的サービスの展開に取り組んでいる。本構想の特徴であるデータ連携については、協議会が整備主体としてデータ連携基盤を整備しており、オープンデータを活用したサービスから段階的に提供を開始しているところである。今後は個人に関する情報、すなわちパーソナルデータを取り扱うパーソナルデータ連携基盤の整備まで活動の領域を広げ、パーソナルデータの活用で実現する、他に類の無い、より先進性の高いサービスを社会実装していくことを目指している。[3]

---

[1] 自治体や事業者、個人等が有する様々なデータを収集・整理・提供することにより、先端的サービスの提供を行うために必要不可欠な中核的な基盤（都市 OS）

[2] つくばスーパーサイエンスシティ構想の推進等を目的に、2024 年４月１日付で一般社団法人として設立。会員機関として、市・大学・研究機関及び民間企業等、53 機関が参画（2025 年２月１日現在）

[3] 現在、国においてデータ連携基盤の構築や積極的活用を後押しすると同時に、類似の機能を有した基盤への重複投資の回避や、データ連携基盤間の円滑な連携を目指すため、各都道府県に対して、データ連携基盤の共同利用ビジョンの策定が依頼されている。本ビジョンの内容如何で、パーソナルデータ連携基盤の整備主体が最終的に決まることになるが、2025 年２月現在において方針が決定していないことから、本懇話会では協議会が整備する前提で議論を行った。

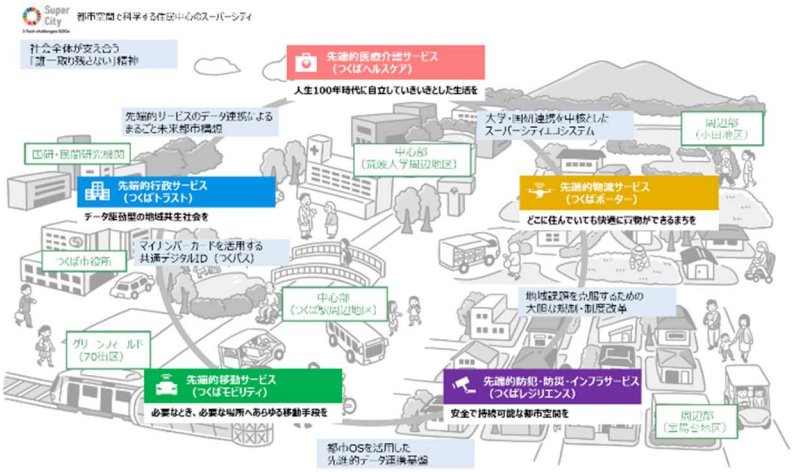


図１　つくばスーパーサイエンスシティ構想

一方で、都市の様々なデータを連携させ、利活用することで高度なサービスを実現していくことについては、カナダ・トロント市のスマートシティ事業の事例においても表出したように、特に自分に関する情報が自分の与り知らないところで使われているのではないかと漠然とした不安感を抱く市民がいることも事実である。

したがって、「つくばスーパーサイエンスシティ構想」を市民の理解のもと前進させていくためには、「先端的サービスの社会実装の推進」を進めることだけでは不十分であり、様々なデータの利活用に対して市民が不安に感じている「プライバシーへの配慮」を市として一緒に進めることが、市民に安心していただきながら、構想を成功裏に進めていく上においては重要であるという、いわば両輪の関係にあると言える。

以上を踏まえ、つくば市は、科学技術とデータを用いて生活全般にわたり先端的サービスの社会実装に係る取組を推進するのと併せて、パーソナルデータを連携させ利活用することで実現する先端的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「プライバシー影響評価制度」を確立するため、「つくば市プライバシー影響評価制度検討懇話会」を設置した。本懇話会は、つくば市がプライバシー影響評価制度を検討するにあたって、市民が先端的サービスを安心して選択できる環境を構築するために求められることは何かを念頭に置きつつ、市民や有識者の意見を聴きながら、適切なプライバシー影響評価制度の在り方を幅広く検討するために開催したものである。

本「最終とりまとめ」は、これまでに懇話会で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の方向性について一定の整理を行い取りまとめたものである。

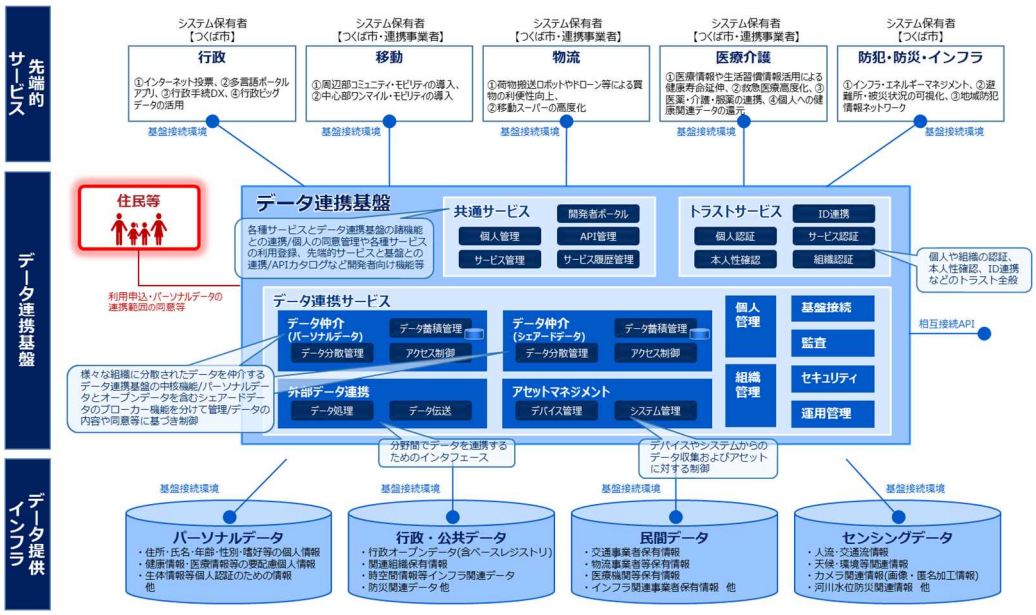


図２　データ連携基盤の活用イメージ

1　つくば市プライバシー影響評価制度の方向性

1.1　総論

1.1.1　基本的な考え方

市が「つくばスーパーサイエンスシティ構想」を推進していくにあたり、プライバシー影響評価（以下「PIA 評価」という。）の仕組みを制度化する目的は、個々の先端的サービスが提供されるごとにその場その場でリスク検討を行うのではなく、あらゆる先端的サービスを網羅的かつ統一の基準で比較・検討することにより、公平・公正な観点で評価される環境を整え、市民にプライバシー保護の観点からも納得のある選択を保障するためである。 その際、先端的サービスが提供される前に、当該サービスを利用する市民に対して、予め考えられるプライバシーに関するリスクを洗い出した上で、対策等を講じてリスクを低減させるとともに、評価結果を公開して、市民が当該サービスの利用から得られる利便性と、利用することにより受け入れることになるプライバシーリスクの可能性を比較・検討したうえで、納得のもとサービスを利用するかどうかを市民それぞれが主体的に選択できるよう、わかりやすく情報公開する。

もっとも、プライバシー影響評価制度（以下「PIA 制度」という。）により予めプライバシーリスクを洗い出し、サービスが及ぼすプライバシーへの影響を評価したからといって、決してリスクがゼロになるものではない。この点については、評価結果の受け手である市民だけでなく、評価される側であるサービス提供事業者に対しても、制度の趣旨を正しく理解してもらう必要があると考えられる。

なお、PIA 評価の結果を受けて、データ連携基盤に接続のうえサービスを展開するのか・しないのかの判断は密接な関係にあり、PIA 制度の範囲をどこまでにするかについては様々な考え方があり、議論が分かれるところである。これに対し本懇話会としては、つくば市の PIA 制度は、サービスの評価と結果の公表までを範囲とすべきと考える。あくまでも第三者の立場からのリスクの比較・検討にとどまることで客観性が担保されるものであり、評価結果に基づくサービスへの是正措置の要求や、データ連携基盤への接続可否の判断といった、サービスの実施可否に関わる部分については、評価結果を踏まえてデータ連携基盤整備主体及びサービス提供事業者の責任のもと主体的に判断されるべきものであり、PIA 制度からは切り離すのが妥当と考えるためである。

1.1.2　PIA 評価の方法

評価方法の設計にあたっては、国内外の先例を参考にして、市独自の要素を加味しながら構築することが望ましい。本懇話会としては、PIA の国際的なガイドラインである ISO/IEC 29134:2017 に基づく JIS 規格である 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」の考え方を参考に制度設計を行うことを提言する。なお、PIA の先行事例として、特定個人情報保護評価制度の取組や、G20 Global Smart City Alliance（GSCA）[4]が国際的な議論のもと作成した「PIA モデルポリシー」についても本懇話会において情報提供が行われた。制度設計にあたってはこれら先行事例についても参考にし、必要十分な評価項目となるよう懇話会として検討し、評価項目のあるべき姿をまとめた。これについては「1.2.4　評価項目」で詳述する。

評価方法の基本的な考え方としては、評価対象となるサービスに想定されるプライバシーリスクについて、リスク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」と、そのリスクの「起こりやすさ」の２軸が重要な要素を占めることから、これらで評価のうえ、サービスに対する総合評価を決定する方法とすることが適していると考える。

また、「つくばスーパーサイエンスシティ構想」の目指す方向性として、データ連携基盤を活用した新たな先端的サービスを官民問わず社会実装していくことを踏まえ、サービスの主体が行政か民間かの違いで評価項目や評価基準に違いが生じるか否かについて本懇話会においてユースケースに基づき検討した。本懇話会の結論としては、官民の違いで評価項目や評価基準に差を設ける必要はなく、同一の尺度で評価すればよいと考える。

[4] 2019 年に日本が G20 の議長国になったことを契機に、テクノロジーの社会実装に必要なルール作りや合意形成に関して、都市や自治体のサポート役となり、スマートシティの実現に貢献するために、世界経済フォーラム（WEF）が事務局として設立された国際コンソーシアム。つくば市は 2019 年６月の設立時より参画。

1.1.3　実施体制

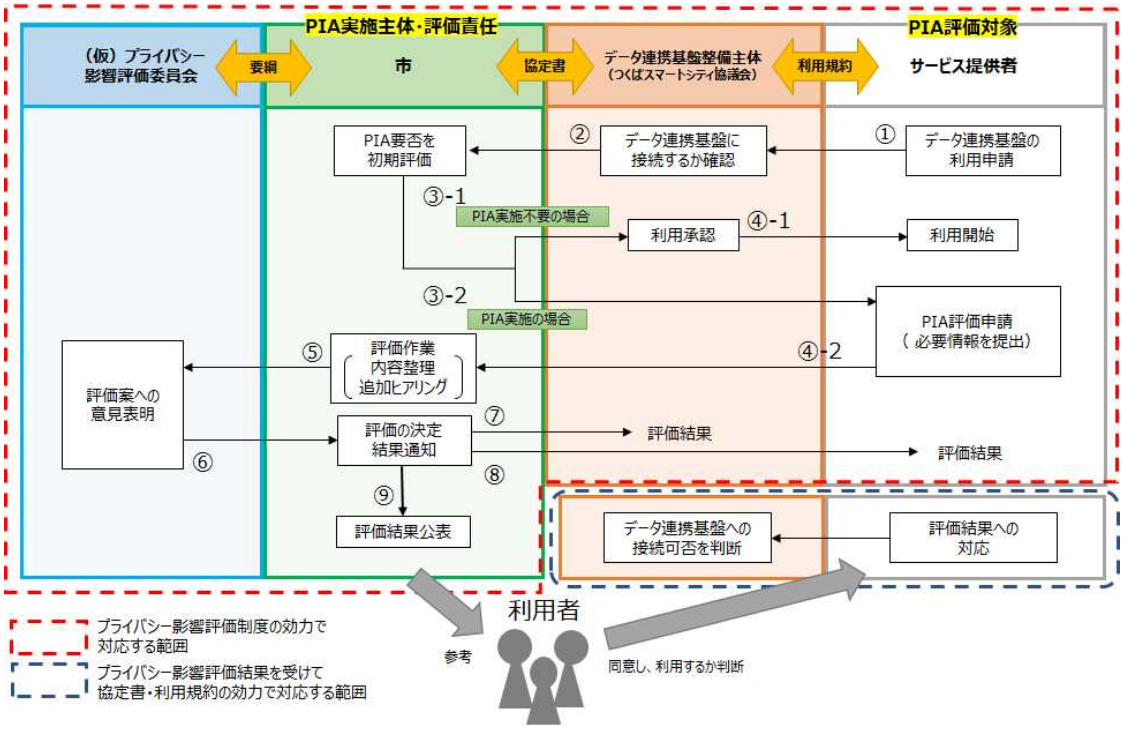


図３　PIA 実施体制（全体像）

PIA 制度を市の責任のもと運用し、評価を実施していくにあたっては、庁内の役割と責任を明確に定めた実施体制を構築する必要がある。組織としてどのように意思決定がなされ、最終的に誰の責任と権限のもと PIA 評価を市として実施するのかについて明らかにするべきである。

これについて、本懇話会としては、庁内の役割と責任を明確にする観点から、庁内に市の PIA 評価に係る実施体制を総理し、PIA 評価を決定する権限を有する「最高プライバシー責任者（Chief Privacy Officer、以下「CPO」という。）」を設置し、CPO の責任と権限のもと評価に係る実施体制を監督し、市として説明責任を果たしていくことが妥当であると考える。

また、市が行った評価が恣意的・独善的な内容にならないよう、その妥当性を第三者の立場から検討し、評価内容の客観性を担保する仕組みが必要と考える。これについては、市民や有識者等を構成員とした「（仮称）プライバシー影響評価委員会」（以下「評価委員会」という。）を設置し、市が行った評価内容に対して意見聴取を行う体制を構築するべきである。これにより市は評価委員会の意見を踏まえ、最終的な評価を決定することで、評価の妥当性や客観性を担保することができる。

なお、評価委員会のもう１つの機能として、市が適切に評価制度を運用

しているかをチェックする役割を評価委員会に持たせることが望ましいと考える。年１回程度、評価委員会から市に対して評価状況等の報告を求めることで、評価制度の適切な運用を確保するための監査的な役割を評価委員会が担うことが期待される。

また、昨今の高度に発達した情報通信社会において、個人情報保護に関する法制度等の動向は目まぐるしく変化していくことが予想されることから、市の評価制度に関しても硬直化することなく、状況の変化に応じて素早く柔軟に対応することが求められる。このことから、評価委員会の有識者には個人情報保護に関する最新の動向を踏まえた助言を期待するとともに、実際の利用者の立場でもある市民委員の意見を踏まえつつ、市は評価制度の見直しを適時適切に行い、制度の改善を図っていくことが求められる。これについては、各論「1.2.4　評価項目」、「1.2.6.1　プライバシー影響評価委員会」にて後述する。

1.2　各論

1.2.1　評価対象

わが国では個人番号制度（マイナンバー）の枠組みの下での制度上の保護措置として、特定個人情報保護評価の仕組みがすでに整備されている。同制度では、個人番号をその内容に含む個人情報ファイル又は個人情報データベース等の「特定個人情報ファイル」を取り扱う事務を対象に評価を行うことが、官（行政）がマイナンバーを事務で取り扱う上での法定義務として定められている。

一方、つくば市が今回制度化を目指すPIA制度は、前述の特定個人情報保護評価のような法律で実施が義務付けられているものではない。しかしながら、市民が個人に関する情報を活用する先端サービスに対して抱いている漠然とした不安への配慮として、今後データ連携基盤整備主体である協議会が整備予定のパーソナル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について、官民を問わず対象として、プライバシーへの影響に関する評価を行うことが適切と考える。

PIA評価は、当該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、サービス構成全体を対象に潜在的なプライバシーリスクを洗い出し、それがプライバシーに及ぼす影響を評価するために実施するものである。いわゆる「セキュリティ評価」と呼ばれる、サービスが用いるサーバの不正アクセスに対する堅牢性を確認するといった、情報システムの安全性や信頼性についての評価とは目的を異にするものである。また、両者の違いとしては、PIA評価は基本的にサービス実施前に評価するのに対し、セキュリティ評価は完成したものに対して評価する点にある。

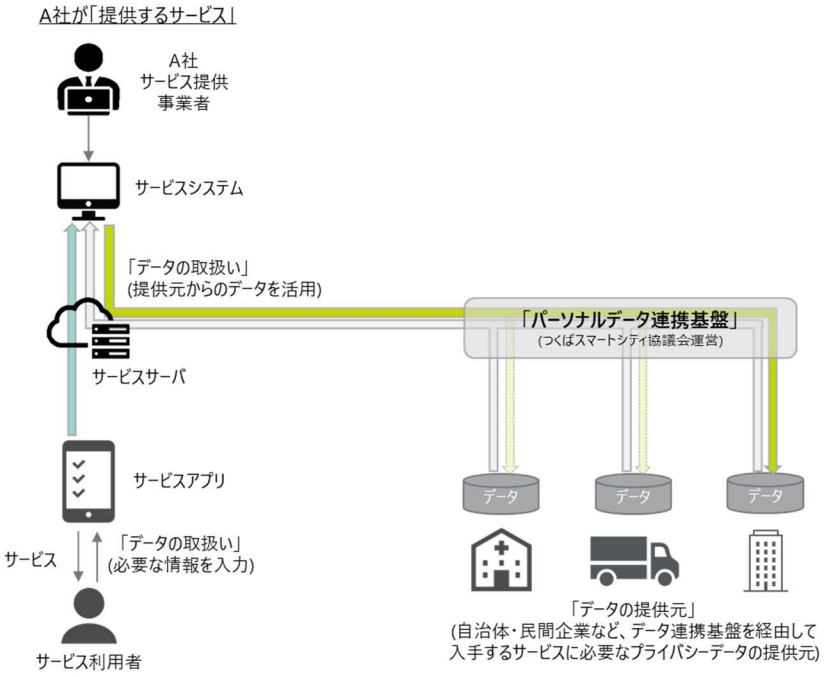


図４　PIA 評価の対象範囲のイメージ [5]

1.2.2　初期評価

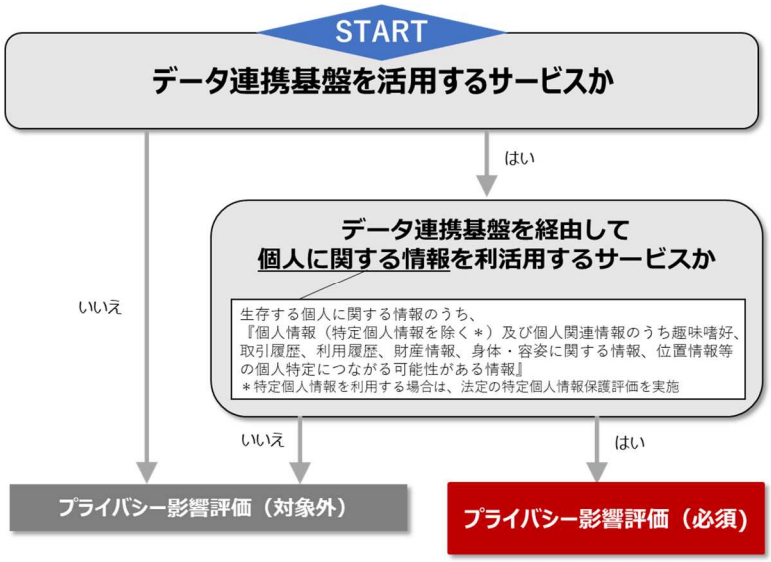


図５　PIA 要否を判断する初期評価の流れ

[5] 「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係する「データの取扱い」に関する部分が評価対象となる。

「つくばスーパーサイエンスシティ構想」においては、様々な先端的サービスの社会実装を目指しており、そのすべてにおいて PIA を実施することが最善であるが、すべてを対象に評価を行おうとした場合、評価に係る作業量が膨大になり、結果的に間に合わせの粗雑な評価に陥る危険性や、費用面での問題といったジレンマを抱えることになる。

これについて本懇話会としては、特定個人情報保護評価が「しきい値判断」の仕組みを採用し、評価の必要性を判断しているように、つくば市の PIA 制度についても重要性判定基準を設け、対象サービスに対する評価を必要とするか否かについて判定する初期評価の仕組みを設けることが適切だと考える。

具体的な初期評価にあたっては、対象となるサービスが、

① データ連携基盤を活用するサービスか
② データ連携基盤を経由して個人に関する情報を利活用するサービスか

の２つの判定基準への該当性を見たうえで、すべて当てはまる場合については PIA 評価を必須とし、いずれかに該当しない場合については対象外とするという初期評価の方法が考えられる。

なお、②の判定基準にある「個人に関する情報」については、個人情報という幅広い概念において、どこまでを範囲に含めるかが重要な問題となることが、本懇話会においても議論となった。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。）においては、生存する個人に関する情報を、個人情報、仮名加工情報、匿名加工情報、個人関連情報の４つに分類しており、市の PIA 制度についても、この法の定義に従って、この４つを適用範囲として決めることが最も分かりやすい一方で、そのまま適用すると却って実効性を阻害することになりかねないという指摘も見られた。

例としては、個人関連情報の定義が「個人に関する情報であって、個人情報・仮名加工情報・匿名加工情報のいずれにも該当しないもの」とされており、具体的に次のようなものが挙げられる。

【個人関連情報の例】

- Cookie
- IP アドレス
- 位置情報
- 購買履歴
- 閲覧履歴　等

上記の例のとおり、「個人関連情報」は識別できなくても個人に関する情報であれば全て該当することになり、その数は膨大なものになる。仮に市の PIA 評価の対象とする「個人に関する情報」の対象を「個人関連情報」のすべてとした場合、評価対象となる情報の範囲が無尽蔵に広がり、結果として評価を行い切れず、実効性が低下するということが懸念される。

以上を踏まえ、本懇話会としては、PIA 制度の実効性低下を防ぐ観点から、当面の間は評価対象とする「個人に関する情報」を最低限必要な範囲に限定した形で制度運用を開始することを推奨する。具体例としては、以下が考えられる。

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)

1.2.3　実施のタイミング

PIA 評価の実施のタイミングについては、当該サービスが新たに提供されようとするサービスが新たに評価を受けるのか、既に評価を受けて提供済みのサービスが再評価を受けるのかの違いを考慮して判断する必要がある。

① 新たに提供されるサービスの場合

初期評価の重要性判定基準に該当する新規サービスについては、サービス提供開始前に、可能な限り早期に評価を実施する必要がある。サービス提供事業者にとっては、評価結果次第で必要な対応をとることを踏まえると、詳細なシステム設計・開発に取り掛かる前に評価を受けることが費用対効果の観点からも望ましい。

② 既に提供済みのサービスの場合

既に PIA 評価を受けて提供済みのサービスについては、当該サービスに大規模なシステム改修(インプットやアウトプットに変更があるとき、AI はアルゴリズムが変わったとき等)や新技術開発等に伴う大幅な仕様変更、サービスを提供・運営する体制変更がある場合、さらに個人情報保護に関する法改正等、社会の動きを踏まえた評価制度自体の変更が生じた場合は、再評価を実施する必要がある。

なお、再評価を必要とする具体的なケースについては、「1.2.9　運用」にて詳述する。

1.2.4　評価項目

本評価制度によってサービスを対象にPIA評価を行うことが、利用者である市民にとって、またサービス提供事業者の双方にとって意味のあるものにするためには、具体的に何について評価するのか、すなわち評価項目をどう設定するかが極めて重要である。これに対して本懇話会では、JIS X 9251における評価項目を基本としつつ、特定個人情報保護評価とGSCA PIAモデルポリシーの評価項目の共通部分を明らかにし、必要十分な評価項目を検討した。

検討の結果として必要と考える評価項目としては、サービスの概要、サービスで利用する個人に関する情報の種類、情報のライフサイクル(収集、利用、保管、廃棄）におけるデータ処理の概要、想定されるプライバシーリスクに対する対応状況など、以下の全22項目について、サービス提供事業者が官か民かによる違いで差を設けることなく同一の尺度で評価することが妥当であると考える。

【PIAで必要と考える評価項目】

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

評価項目のうち、１から６については評価対象となるサービスの全容を把握するための項目、7から 22 については想定される具体的なプライバシーリスクに対しての対応状況について確認するための項目となっている。

また、７から 22 の想定されるプライバシーリスクへの対応状況については、情報セキュリティを確保するための対策としての考え方を参考にし、「物理的・技術的・管理的（人・組織）」の３つの観点から対応状況を評価することが適切と考える。また、それらの観点が「個人情報保護法」及び「個人情報の保護に関する法律についてのガイドライン(通則編)」に照らしたときに法的に求められているものなのか、あれば望ましいものなのかを明らかにし、それぞれを「必須」と「推奨」に分類すると、評価をする際の使い勝手が向上するものと考える。

これらを踏まえ、評価項目及びそれを評価するための観点を含めて、本懇話会として取りまとめたものが別添１「評価項目一覧（案)」となる。実際の制度化に際しては、これを参考に具体的な評価業務への落とし込みをすることが望まれる。

なお、今回検討した評価項目が将来にわたっても常に適切であるとは限らず、評価を繰り返す中で明らかになった課題や、時代の変化に応じて、評価項目の適時見直しを図っていくことが肝要である。評価委員会の機能として、運用状況を踏まえて、定期的に見直しを実施していくことが求められる。

1.2.5　評価基準

評価対象のサービスに想定されるプライバシーリスクに関して、リスク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」と、そのリスクの「起こりやすさ」の２軸で評価し、最終的に２つの評価を掛け合わせた「総合評価」として示すことになる。評価の実施にあたって、尺度を予め明確に示しておくことが必要である。

1.2.5.1　影響度

プライバシーリスク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どの程度の影響を及ぼすか、どのような尺度で評価するべきかについて議論を行った。JIS X 9251 においても影響レベルの推定方法の例が示されているが、本懇話会では影響度を判定する具体的な尺度を設定するためにさらに一歩踏み込んだ議論を行い、独自の尺度として、身体的危険・財産的損失・精神的苦痛の３つの観点からプライバシーにどの程度の影響を及ぼすかについて判定する方法について検討を行った。

具体的な判定方法の検討にあたっては、特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）が、情報漏洩インシデント発生時の損害額を試算するための考え方として提唱する「J0 モデル」[6]を参考にした。J0 モデルは、個人情報が漏洩した際に被害者に与える影響を、「精神的苦痛」と「経済的損失」という２種類の尺度で定量的に表したもので、横軸（ｘ軸）に「精神的苦痛」、縦軸（ｙ軸）に「経済的損失」を置いたグラフを作成し、そのグラフ内に想定される漏洩情報の例を影響の度合いに応じて配置のうえ、グラフの位置により当該情報の影響度の大きさを求めることができる、というものである。

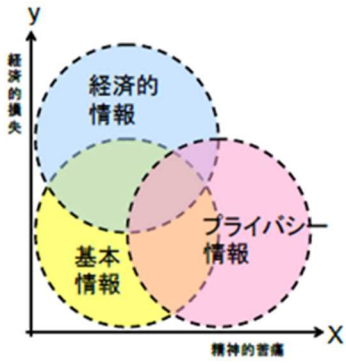


図 5-2：EP 図（Economic-Privacy Map）

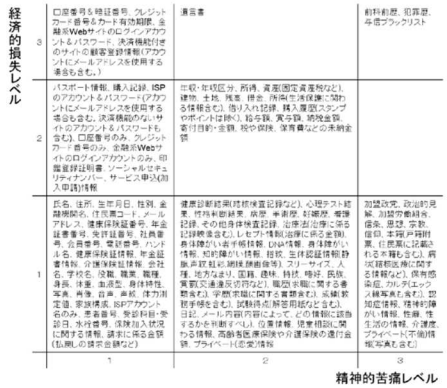


図 5-3：シンプル EP 図

【引用】JNSA「情報セキュリティインシデントに関する調査報告書」

J0 モデルを参考に、本懇話会で検討したものが別表１「影響度判定表」である。横軸に「精神への影響」、縦軸に「財産への影響」を置き、それぞ

[6] JNSA Damage Operation Model for Individual Information Leak
https://www.jnsa.org/result/incident/2019/2019-006.pdf

れを度合いに応じて４段階で表すこととした。「影響度判定表」で例示する情報の位置づけについては、J0 モデルが３段階であったものを、JIS X 9251 の影響度の考え方に合わせて４段階に見直すとともに、一部情報を追加・削除するなど、懇話会での議論を通じて再配置を行った。

【影響度判定表】

「財産への影響」	「精神への影響」 1	2	3	4
4		口座番号＆暗証番号、クレジットカード番号＆カード有効期限、金融系Webサイトのログインアカウント＆パスワード、決済機能付きのサイトの顧客登録情報	遺言書、借り入れ記録、借金	前科前歴、犯罪歴、与信ブラックリスト
3		パスポート情報、購入記録、ISPのアカウント＆パスワード、口座番号のみ、クレジットカード番号のみ、金融系Webサイトのログインアカウントのみ、印鑑登録証明書、マイナンバー、サービス申込（加入申請）情報	所得、資産（固定資産税など）、建物、土地、現金残高、所得、賞与額、納税金額、税や保険、保育費などの未納金額、購入履歴	
2	（スポーツクラブなどの）会員番号、社員番号	生年月日、性別、住民票コード、メールアドレス、健康保険証番号、年金証書番号、免許証番号、ハンドル名、健康保険証情報、年金証書情報、介護保険証情報、所属会社名、所属学校名、会社の役職、職業・職種、身体特性、写真・肖像、音声、家族構成、ＩＳＰアカウント名、患者番号、受診科目・受診日、保険加入状況に関する情報、請求に係る金額（払戻しの請求金額など）、寄付・金額	健康診断結果、病歴、手術歴、妊娠歴、看護記録、身体検査記録、レセプト情報、身体障害者手帳情報、障害情報、生体認証情報（指紋、静脈、声紋、虹彩、網膜、顔画像等）、スリーサイズ、人種・民族、地方なまり、趣味、特技、嗜好、賞罰（交通違反切符など）、職歴・学歴（求職に関する書類含む）、会社・学校の成績・試験得点、日記・メール内容（内容による）、児童相談に関わる情報、高齢者医療保険や介護保険の還付金額、プライベート（恋愛）情報、位置情報	加盟政党・政治的見解・加盟労働組合、信条・思想・宗教・信仰、国籍、本籍、保有感染症、カルテ（エックス線写真も含む）、認知症情報、DNA情報、性癖、性生活の情報、介護度
1	水栓番号	身長、体重、血液型、心理テスト結果、性格診断結果、体力測定値		

高い ↑ 「財産への影響」 ↓ 低い

低い ← 「精神への影響」 → 高い

＋

「身体への影響」を評価委員会で加味して「影響度」を判定

別表１「影響度判定表」

使用方法としては、J0 モデルの考え方を踏襲し、該当する情報の「影響度判定表」における位置に応じて「精神への影響」と「財産への影響」の度合いを１～４の評点で判定し、そのうち影響度の高い方の評点を当該サービスの「影響度」の評価として採用する。なお、該当する情報が及ぼす「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ことが予想され、一律の基準で評価することが難しいことから、サービスごとに評価委員会で議論のうえ、影響度の評価に加味する形をとることが適していると考える。また、「影響度判定表」に位置付けがない情報の利活用ケースが発生した場合についても、評価委員会で議論し判定するのがよいだろう。

なお、影響度を４段階で示す際に、それぞれの段階をどのような表現で示すかについて議論を行った。JIS X 9251 では「１　無視できる」「２　限定的」「３　重大な」「４　甚大な」という用語が程度を表す表現として用いられている。このような表現を用いることのメリットとしては、評点が

示す意味をイメージしやすい点が挙げられる一方で、このイメージを悪用されるおそれがあることがデメリットとなる。具体的には、本制度は民間がサービス提供主体となるものも評価対象であるが、評価の結果「１　無視できる」といった評価がついた民間サービスについて、民間サービス提供者側がこの評価をもって市があらゆるリスクについては無視できると判定した、というように評価結果を都合よく解釈したり、喧伝する恐れが考えられる。これらの両面からの議論を踏まえ、本懇話会としては「１　無視できる」「２　限定的」「３　重大な」「４　甚大な」といった段階ごとの評価を示す用語をつけることはせず、「高い⇔低い」という程度を示すにとどめることが適当と考える。

1.2.5.2　起こりやすさ

評価対象となるサービスに想定されるプライバシーリスクの「起こりやすさ」の判定方法については、1.2.4 で提示した別添１「評価項目一覧(案)」を使って判定する方法を検討した。

具体的な判定方法としては、1.2.4 で提示したとおり、全 22 項目の評価項目のうち、法令上対応が「必須」の観点については、１つでも対応できていない場合は「４」（起こりやすいという評価）と判定する。一方、法令上は対応が必須ではない「推奨」の観点については、１つ未対応ごとに「＋１」を加点し、最終的に当該項目の中の積み上げ点数で最低「１」から最大「４」の４段階で判定することとする。以下に具体的な事例についての評価例を示す。

【ケース１】評価項目が「必須」のみで、対応しているケース

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。	必須	対応済	1

⇒ 必須の評価項目に対応しているので評価項目 No. 7 の起こりやすさの評価は「１」

【ケース２】評価項目が「必須」のみで、未対応のケース

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	必須	未対応	4

	を得ない場合はその根拠を明示。			

⇒ 必須の評価項目に未対応なので評価項目 No.8 の起こりやすさの評価は「４」

【ケース３】評価項目に「必須」「推奨」が混在しているケース

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
	①システム、アプリケーション、データベースへのアクセスの際は適切なログオン手順（パスワード、生体認証、IC カード等認証情報を確認するもの）を必須としている。	必須	対応済	
	②一定回数以上のログイン認証失敗によるロックアウトや、安全性が確保できるまで再ログインの間隔をあける機能を実装する等により、IoT 機器、サーバ等に対する不正ログインを防止している。	推奨	対応済	
	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	

⇒ 「必須」についてはすべて対応済である一方で、「推奨」の２項目（⑤と⑥）が未対応のため、評価項目 No.13 の起こりやすさの評価は、ベースラインとなる１に、未対応で加点となる＋２を加えて「３」

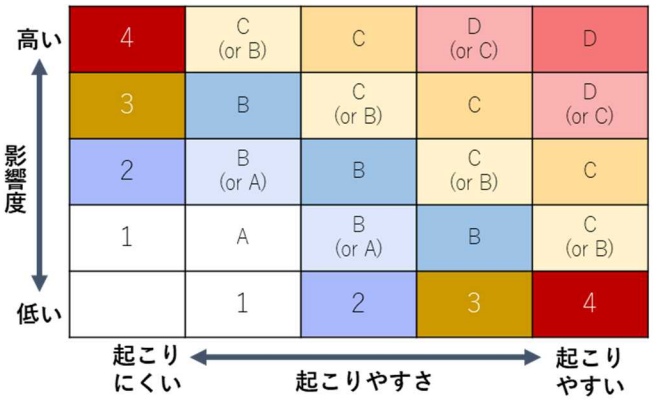
上記の考え方に基づき評価項目について一通り評価し、その中で最も高い評点を当該サービスの「起こりやすさ」の評価として採用する。また、「起こりやすさ」の評価作業の過程で、評価項目一覧で示した 22 項目以外の観点による懸念、リスクが見つかった場合は、評価委員会で議論の上、判定するのがよいだろう。

なお、「起こりやすさ」を示す４段階の評点に対しても、「影響度」と同様に、「１　無視できる」「２　起こりにくい」「３　起こりえる」「４　容易に起こりえる」といった段階ごとの評価を示す用語をつけることはせず、「起こりやすい⇔起こりにくい」という程度を示すにとどめることが適当と考える。

1.2.5.3　総合評価

一連の評価作業の過程により特定されたプライバシーリスクに関する「影響度」と「起こりやすさ」の評価結果に基づき、当該サービスに対する PIA 評価の最終的な結果を、４段階による「総合評価」として示すのがよいと考える。

具体的な「総合評価」の判定方法としては、JIS X 9251 が提案する「プライバシーリスクマップ」の考え方に準拠すると運用しやすいであろう。「プライバシーリスクマップ」は、縦軸に「影響度」、横軸に「起こりやすさ」を置いた座標のようなもので、座標平面の位置で４段階のＡＢＣＤ評価を表したものである。



評価の過程で判定された「影響度」と「起こりやすさ」の各評点をマップに落とし込んだ上で、各評点が座標平面上で交差する場所に位置づくＡＢＣＤで「総合評価」を判定する仕組みである。

総合評価の「ＡＢＣＤ」に持たせる意味についても議論があり、懇話会としてモデル案を検討した。まず、そのサービスが引き続き保有していると推定されるリスクの量（残存リスク）を示すものとして、上から「リス

ク大」「リスク中」「リスク小」「リスク微小」の４段階の意味付けを行った。さらに、利用者がその残存リスクを踏まえてどのような判断をすれば望ましいかの判断の目安を示すこととした。これをまとめたものが別表２『「総合評価」凡例』である。

評価	残存リスク	残存リスクを踏まえた判断の目安
A	リスク微小	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	リスク小	想定されるリスクは少ないと推定されるが、利用は必要性とのバランスで判断することを推奨
C	リスク中	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	リスク大	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

別表２　「総合評価」凡例

また、懇話会において座標平面のＡＢＣＤの位置の妥当性について議論を行った。「影響度」と「起こりやすさ」の評点に従って、必ず一つのＡＢＣＤが機械的に決まる仕組みは明瞭である一方で、例えばサービスで利活用する個人に関する情報の種類で評点が決まる「影響度」については、サービス提供事業者の努力のみでは評価を改善することができない。機械的に基準を適用することが、却って事業者側にとってはサービス体制や運用面でいくら努力しても評価に反映されない仕組みと捉えられ、結果として参入障壁につながり、そのことが本来市民にとって有意義であるはずのサービスが使えないといった不利益を招くおそれが懸念される。

このような懸念を踏まえ、本懇話会としては、座標平面に位置づくＡＢＣＤの一部に、「Ｂ（or Ａ）」「Ｃ（or Ｂ）」のように、選択が可能な「or」を導入することを提案する。考え方としては、一定程度運用上で柔軟に対応できる余地を残す仕組みとして、評価委員会においてサービス内容やプライバシーリスクへの対応状況を踏まえ、原則としてより低い方の評価（悪い評価）を採用することとしつつ、総合的な判断としてより高い方の評価（良い評価）を採用することも一部可能にすることを提案する。

なお検討にあたっては、「1.1.1　基本的な考え方」で示したとおり、本制度を用いて評価をしたからと言って決してリスクがゼロになるわけではない、というメッセージを総合評価に明確に持たせることで、本評価制度に対する市民の誤解を招かないようにすることと、市の総合評価が事業者

等のお墨付きとなり、日々のPDCAサイクルを回すことを止めてしまうなど疎漏が発生しないように留意した。

1.2.6　評価体制における役割・責任

PIA 制度を市が運用していくにあたって必要となる評価体制について懇話会で議論し、以下の通り整理した。

1.2.6.1　プライバシー影響評価委員会

市が行った評価が恣意的・独善的な内容にならないよう、その妥当性を第三者の立場から検討し、評価内容の客観性を担保する仕組みとして、市民や有識者等を構成員とした評価委員会を設置することを「1.1.3　実施体制」で提言したが、評価委員会に期待される機能、権限等については以下が挙げられる。

① 機能

評価委員会に期待される第一の機能としては、市が実施するPIA評価の内容が個人情報保護に関する専門的な観点及び実際に利用する市民の観点から見たときに妥当なものか、第三者の立場から市に対して意見具申を行うことである。

また、第二の機能としては、市が適切に評価制度を運用しているかをチェックするため、年１回程度市に対して PIA 制度の運用状況等を報告することを求めるなどして、PIA制度の適切な運用を確保するためのチェック機能を担うことである。

さらに、第三の機能としては、個人情報保護に関する法改正等、社会の動きを踏まえた助言を市に対して行い、PIA制度が硬直化しないよう適宜見直しを図っていくことを促すことである。

② 権限と責任

評価委員会は市の PIA 評価結果やリスク認定、制度の見直しを決定するための機関ではなく、あくまで PIA 評価内容や制度に客観性を持たせるために、第三者の立場から市に対して意見具申することを目的に設置するものであり、評価委員会自身が何らかの決定権や是正権限、結果に対する責任を持つものではない。

なお、市は評価委員会の意見は最大限尊重の上、評価の決定やPIA制度を運用していくことが求められる。

③ 構成員

評価委員会の構成員については、マルチステークホルダー・プロセス[7]の考え方に基づき、市の責任において実情に応じた形で適切な構成員を選定されたいが、一例として以下のような属性を含む構成が考えられる。

- 認定個人情報保護団体[8]の責任者
- 個人情報保護法制に詳しい法曹関係者
- つくばスーパーサイエンスシティ構想の企画立案に係る責任者
- PIA 制度を運用している民間事業者の代表者
- データ連携分野に関する有識者
- セキュリティ情報技術に関する有識者
- サービス利用者の代表（市民）　　など

なお、評価の公平性を保つため、事前接触の防止の観点から、評価委員会の構成員を誰が担うかについては、事後公開とすることが適切である。

1.2.6.2　最高プライバシー責任者（CPO）

市として PIA 制度を運用していくに当たって、庁内の役割と責任を明確にする観点から、庁内に「最高プライバシー責任者（CPO、Chief Privacy Officer)」を設置することを提言する。CPO は市の評価に係る実施体制を総理し、PIA 評価を決定する権限を有するとともに、PIA 評価結果と PIA 制度の運用に対して説明責任を果たす責務を負う。

なお、CPO は特別職又は幹部職員など庁内の然るべき職位の者が担うべきと考えるが、具体的な人選については庁内で議論の上、決定されるべきものと考える。

1.2.6.3　責任分界点

現代社会においては日々様々な形で個人情報の漏洩や不正利用等のプライバシーに影響を及ぼす不適切な事案が発生しているように、どんなに

[7] ３者以上の社会の様々な立場にある組織や個人が、対等な立場で参加･議論できる会議を通し、単体もしくは２者間では解決の難しい課題解決のために、合意形成などの意思疎通を図るプロセスのこと

[8] 業界・事業分野ごとの民間による個人情報の保護の推進を図るために、自主的な取組を行うことを目的として、個人情報保護委員会の認定を受けた法人のこと

事前に備えたとしても、リスクはゼロになるわけではなく、プライバシーリスクは発生し得ると心得ておくべきであろう。その意味において、PIA 制度は「1.1.1　基本的な考え方」で示したとおり、市がサービスを利用する市民に対してゼロリスクを保証するためのものではなく、また市がサービス提供事業者にサービスのお墨付きを与えるものでもない、という制度の位置づけを改めて明確にしておきたい。

PIA 制度が行うことは、サービス提供に際し起こる可能性のあるプライバシーリスクを評価し、市民がサービスの利用から得られる利便性と、サービスを利用することにより受け入れることになるプライバシーリスクの可能性を比較・検討した上で、納得のもとサービスを利用するかどうかを主体的に選択できるよう、評価結果をわかりやすく情報公開することである。

これを踏まえ、一連の PIA 評価の利害関係者である市、サービス提供事業者、データ連携基盤主体（協議会）の PIA 制度における責任分界点は以下の通り整理される。

【PIA 制度における責任分界点の考え方】

① 市の責任範囲

基本的に市は当該サービスに対する PIA 評価を実施・決定する評価主体として、PIA 評価の完遂と評価結果に対する説明責任を負う。

② サービス提供事業者の責任範囲

サービス提供事業者は、協議会との間で合意するデータ連携基盤の利用規約に基づき市の PIA を受けるにあたって、正確な情報を申告する義務を負うとともに、PIA 再評価に該当するサービス上の変更が生じる場合は速やかに申告し、再評価を受ける義務を負う。また、虚偽の申告のみならず、優良誤認、不適切な記載、あるいは故意に申告しなかった内容に関しても、実損害の有無に関わらず一切の責任を負う。

③ データ連携基盤整備主体（協議会）の責任範囲

協議会は市との協定に基づき、サービス提供事業者に対して市の PIA 評価を受けさせる義務を負う。

これらの責任分界点の考え方については、利害関係者に明確に伝え、理解してもらう必要があることから、最終的に公開する評価書上に「PIA 評価に関するディスクレーマー（免責、留意事項）」として明示するなどの配慮が求められる。

なお、本懇話会ではPIA制度における責任分解点の考え方について整理を行ったもので、PIA 評価を受けたサービスに万が一プライバシーに関わる不適切な事案（以下「プライバシーインシデント」という。）が発生した場合の責任分解点の考え方とは区別することが適当と考える。プライバシーインシデント発生時の責任範囲については、PIA評価の有無に関わらず、プライバシーインシデントを原因として発生した損害に応じて、法的根拠に基づき判断されるものである。

1.2.7　実効性の担保

これまでに評価対象、評価項目、評価基準といったPIA制度の内容についてまとめてきたが、市がPIA制度を運用していく中で最も重要なことは関係者にPIA制度をしっかりと守ってもらえるか、すなわちPIA制度の実効性をいかに担保するか、という点にあり、本懇話会においても議論を行った。

今回本懇話会としては、PIA 制度を市の「要綱」で定め制度化することが望ましいという結論に至った。その上で市が「要綱」として整備したPIA制度をいかに守ってもらうかという部分については、PIA 評価の関係者である３者、すなわち① PIA 評価主体である市、② データ連携基盤整備主体である協議会、③ その基盤を使ってサービスを展開するサービス提供事業者の関係を「要綱」とは別の規程でルール化することで、これら全体でPIAが守られる体制を構築するという形を提案する。

具体的には下図で示すとおり、PIA制度として市が制定する「要綱」、市と協議会との間で締結する「協定」、協議会とサービス提供事業者との間で合意する「利用規約」により規律を保ち、PIA制度全体の実効性を担保する仕組みにすることが考えられる。

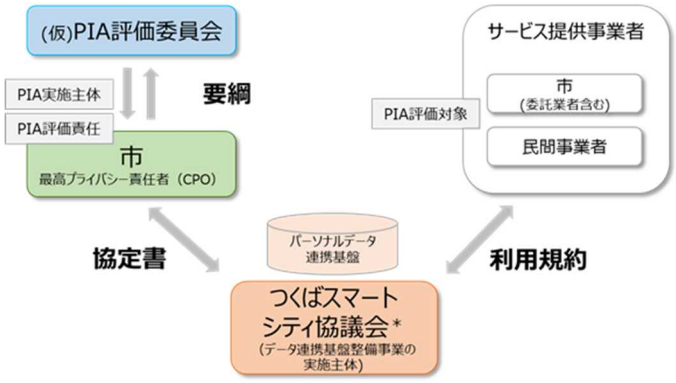


図６　PIA制度の実効性を担保する仕組み

「要綱」「協定」「利用規約」が規定する具体的な条文内容については、市の責任において具体化を図るものと承知しており、本懇話会では実効性を担保するために、これらにどのような事項を規定するべきかという範囲で議論を行った。

この議論の中で特に論点となったのが、PIA 評価結果を受けてからの協議会とサービス提供事業者の行動に対して「協定」「利用規約」で縛りを設けるか、という点であった。「1.1.1　基本的な考え方」で示した通り、PIA 制度からサービスの実施可否の判断は切り離して考えるので、この「協定」「利用規約」で縛りを設けるか、という点は PIA 制度とは別の議論ではある。一方で、今回議論してきた PIA 制度の特徴の１つが「要綱・協定・利用規約という全体の関係性で PIA 制度の実効性が担保される」という点にあり、また利用者にとっても、例えば PIA 評価で「Ｄ評価」となったサービスがその後どのように取り扱われるのか、という点に関しての考え方への関心度は高いと思われることから、本懇話会として議論を行った。

この点に関して、本懇話会においては議論が分かれる結果となった。例えば、「Ｄ評価の場合はデータ連携基盤への接続を許可しない」という規定を「協定」に盛り込むなどして、評価結果をもってサービスの実施可否を縛ることについては、以下のように議論が分かれた。

① 市の協議会に対する行き過ぎた制限ではないか。あくまで利用するか否かの選択は利用者が評価結果を参考に判断されるべきものであり、協定で縛りを設ける必要はないのではないか。
② Ｄ評価は「影響度」も「起こりやすさ」も極めて高いという評価から導出されているものであり、実際に行使するかしないかは別として、サービスを止められる権限を規定しておくことは必要ではないか。

本件については PIA 制度の外側の、市と協議会間の整理の問題であり、本懇話会としては一定の結論を纏めることはせず、最終的な考え方の整理は市の判断に委ねるが、検討に当たっては様々な意見があるということを念頭に置きつつ、PIA 制度の実効性を担保するために、要綱・協定・利用規約にどのような規定を盛り込むかについて慎重に検討されたい、という点を本懇話会として申し送りたい。

文書	内容
① **要綱** ➢ 市の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に市の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

別表３　要綱・協定・利用規約の関係性

なお、一般論として制度の実効性を担保する方法論としては、法的拘束力を持って義務や罰則を定めることができる「条例」を市民の代表である議会の議決を経て定め制度化する方法と、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が、市長の権限で適時定めることが可能な「要綱」として制度化する方法が挙げられる。

	条　例	要　綱
位置づけ	議会の議決によって制定される自治立法	行政機関内部における手続を定めるもの （例）行政実務上の処理方法等を規定、行政指導の指針、補助金交付要綱等 （※つくば市では「告示」により知らしめている）
制定手続	議会の議決	市長の決裁
制定スケジュール	市議会定例会（年４回）	随時
性質	➢ 義務を課す／権利を制限する内容を定められる。 ➢ 罰則（2年以下の懲役・禁錮、100万円以下の罰金・拘留・科料・没収、5万円以下の過料）が定められる。	➢ 市職員に対する内部命令 ➢ 法的拘束力はなく、義務を課す／権利を制限する内容や罰則は定められない。

別表４　「条例」と「要綱」の違い

一見すると法的拘束力を持つ「条例」として制度化した方が義務や罰則といった強制力が生じるため実効性は担保されやすいが、これは同時に対象者に対して何らかの義務を課す、または権利を制限する（イノベーションを阻害する）ことを意味するため、条例以外に実効性を担保するための取り得る手段が無いのか精査するなど、条例化という手段の選択には慎重を期すべきである。

本懇話会が考える市のPIA制度は、「1.1.1　基本的な考え方」で示したとおり、データ連携基盤を活用し、個人に関する特定の情報を利活用するサービスに対してPIA評価を実施し、その結果を公表するための制度として提案している。PIA 制度として、評価結果に基づきサービスへの是正措置を要求したり、データ連携基盤への接続可否を決定したり、何らかのペナルティを科すといった、義務や罰則を含む制度は想定していない。よって、本懇話会としては、市のPIA制度は「条例」ではなく、「要綱」で整備することが適切であると考える。

1.2.8　結果の通知と公表

市は決定した総合評価の結果を協議会及びサービス提供事業者に速やかに通知する。結果を踏まえ、協議会とサービス提供事業者は、必要に応じて改善や対策を施した後、パーソナルデータ連携基盤への接続とサービス提供を開始することになる。

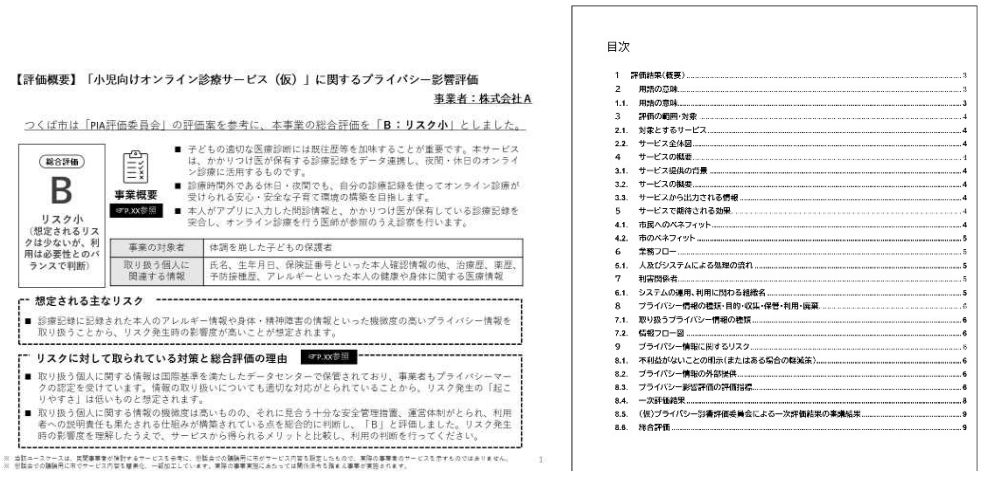
また、総合評価の結果については評価書の形で対外的に公表する。公表にあたって最も重要なことはPIA評価の内容を市民に理解してもらうことであり、評価書では専門用語や難解な表現を避け、市民に分かりやすい言葉を使用することが重要であることが懇話会においても繰り返し議論された。

評価書に含むべき内容としては、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、サービスを利用することで得られる便益と、サービス利用に伴い生じる可能性があるプライバシーに関する不利益の両面について具体的な事例を挙げて透明性をもって説明する、また、評価結果とサービス概要を一つの評価書に統合し、評価結果だけでなく、どのようなサービスが提供されるのかを一つの資料で理解できるようにするといった、市民の理解を助ける配慮への意見が示された。

市民に公開する評価書の形式については、評価内容について詳細に記述した「詳細版」と、要点をまとめた読みやすさと分かりやすさを優先した「概要版」の２種類の形式で作成されることが望ましい。忙しい多くの市民は、詳細に書き込まれた評価書の内容を全て読み込むことは現実的に難しく、サービスの利用の是非を判断するために最低限必要な情報が端的にまとまった形で提供されることを望むと考えられる。よって、概要版と詳細版の２種類を用意することで、当該サービスのPIA評価を理解してもらうための中心資料として概要版を多くの人に読んでもらい、さらにPIA評価の詳細について知りたい、より専門的な観点からPIA評価の全容を把握したいといった要望に応じるための補足資料として詳細版を読んでもらう、

という整理で評価結果を公表することが、市民からの信頼を築くことに繋がると考える。

なお、評価結果の通知を受けて、協議会又はサービス提供事業者が何らかの対応を取った場合、PIA 評価の公表と併せてその対応内容も周知することが望ましい。例えば、総合評価「C」という結果を受けて、サービス提供事業者の自助努力で「B」相当に改善する対策等を取った場合に、市が公表する PIA 結果と一緒に周知しないと、総合評価「C」という結果だけが独り歩きしてしまうことが懸念される。よって、評価結果を受けて協議会又はサービス提供事業者が実施する対応方針についても市が報告を受ける仕組みを併せて導入することが適切である。


【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、利用は必要性とのバランスで判断）

事業概要 <PP.XX参照>

■ 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察を行います。

事業の対象者	体調を崩した子どもの保護者
取り扱う個人に関連する情報	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 <PP.XX参照>

■ 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。

※ 当該ユースケースは、当該事業者が実施するサービスを念頭に、当該会合の議論用に当該サービス内容を設定したもの。実際の事業者のサービスを示すものではありません。
※ 当該会合の議論用に用いるサービス内容も簡素化、一部加工しています。実際の事業実施にあたっては関係法令も踏まえ事業者が実施されます。

1

目次

図７　左：評価報告書（概要版）　右：評価報告書（詳細版）イメージ

1.2.9　運用

これまでに論じてきた PIA 評価の考え方とは別に、PIA 制度を実際に動かしていく中で、PIA 評価後に直面することが想定される運用上の課題について、下記の通り考え方を整理した。

1.2.9.1　PIA 再評価における考え方

PIA 再評価を必要とするケースとは、既存の評価時に判定された「影響度」と「起こりやすさ」が変わる可能性がある何らかの変更がサービス上生じる場合であり、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ということになる。これはすなわち、取り扱う個人に関する情報の種類が変更される（「影響度」が変動）、評価項目への回答が変更される（「起こりやすさ」が変動）場合を指す。

このような事象が生じるケースは、当該サービスに大規模なシステム改

修が生じる場合、サービスを提供・運営する体制変更が生じる場合、またPIA 制度自体が大幅に見直され、新たに評価するべき視点が加わる場合などが考えられる。具体的には、「大規模なシステム改修」とは、取り扱う個人に関する情報について影響度判定に変更が生じるデータを収集開始する場合や、オンプレミス[9] からクラウドへサーバ移行する場合等が当てはまる。また、「サービスを提供・運営する体制変更」とは、サービスの運営を受託している事業者が別の事業者に変更した場合や評価項目の細則を満たさなくなった場合等が想定される。このような変更が生じる場合は、変更前に再評価を実施する整理としたい。

なお、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を図るべきと考える。

1.2.9.2　PIA 評価の有効期間に関する考え方

「1.2.4　評価項目」においても触れたとおり、今回検討したPIA 評価の仕組みが将来にわたっても常に適切であるとは限らず、評価を繰り返す中で明らかになった課題や、時代の変化に応じて、PIA 制度を適宜見直していくことが肝要であるが、この時問題となるのが、既にPIA 評価を受けサービスを提供中の既評価済みサービスの取扱いをどうするかという点である。また、PIA 制度に変更は生じなかったとしても、評価結果が将来にわたって有効なのかという点においては議論が分かれるところである。

この点については、評価実績を有していない現時点においては合理的な根拠をもって考え方を整理することが難しいことから、PIA 制度施行後３年程度が経過した時点の運用状況を踏まえて、必要な措置を講じることを前提に、当面の間は以下の通り整理することが現実的と考える。

① PIA 制度を見直した場合の既評価済みサービスの再評価については、一律の基準は設けず、見直し内容に応じて実施の必要性を判断する
② PIA 評価の有効期間については現時点では特に設けない。PIA 評価の実績を積み重ねる中で、評価委員会での検討を継続する

[9] サービス提供に必要なサーバやソフトウェアを、サービス提供事業者自身で管理する施設内に設置し管理すること

1.2.9.3　制度運用過程で明らかになった課題への対応

今後 PIA 評価の実績を積み重ねていく中で、制度運用上の不具合や、制度が実情にそぐわないといった、現時点で想定しえなかった課題が将来的に明らかになっていくことが予想される。また、「1.1.3　実施体制」においても触れたとおり、市が適切に評価制度を運用しているかを評価委員会がチェックする中で、制度の改善点が明らかになることもあるだろう。

このような制度運用過程で明らかになった課題に対する対応については、原則的には CPO の権限と責任の下、市が対応方針を決定し、必要な措置を講じていくことになるが、対応方針の検討の過程においては、評価と同様に、評価委員会に諮った上で決定することを求めたい。市が決定する対応方針に妥当性と客観性を持たせる段取りとして必要なものと考える。

２　検討の経緯

2.1　座員の主な意見

2.1.1　評価対象

≪個人に関する情報≫

- どのような目的で使うのか、個人に関する情報はどこまでを指すのかをあらかじめ明示してほしい。
- 個人関連情報すべてを義務づけるのは対象範囲が膨大となり現実的ではない。例えば義務付け対象は個人情報・仮名加工情報、プライバシーに影響を与え得る個人関連情報は推奨と対象を分けるとしてもよいのではないか。
- 位置情報はセンシティブ情報であり、購買履歴等は個人情報に該当する可能性はあるので、対象には加える検討をした方がよい。

≪初期評価≫

- 初期評価に関して、全数調査にするよりは重要性判定基準を策定して対象事業をしぼった方がよい。(例えば関係する人数、データ連携基盤を活用するのか等。)

2.1.2　評価基準

≪影響度≫

- データの種類によって個人に与える影響は大きく変わる。発生頻度が低くても主体に与える影響が大きい情報もある。
- 情報も、それぞれ個人の置かれている状況によってリスクの影響度が異なる。
- LGWAN 等の用語の使い方に注意する。リスク評価について、「起こりやすい」「起こりにくい」等分類分けすることが本当にいいのか。リスクを明示して利用者に注意喚起を促す記載にする形でもよいのではないか。
- 「起こりやすさ」「影響度」１～４をどのような基準で判断するのか。一定の基準を策定するのか、議論で決めるのか。
- 影響度の数値のつけ方は、実際に対策をどうしているかから逆算する方法もあるので精査が必要である。
- 影響度・起こりやすさの評価は、細かく数字をつけすぎず、全体として総合的に見て付けていく形がよい。補助ツールとして位置づけてはどうか。
- 影響度判定表における各情報の位置づけについては固定化することなく、評価委員会で継続的に見直しを図ってほしい。

≪起こりやすさ≫
・ 通常実施する対策がなされていれば起こりにくいという評価が導かれる仕組みになっているので、その是非や対策項目の過不足について、評価委員会で継続的に検討してほしい。
≪総合評価≫
・ 総合評価とその理由・根拠を明示したほうがよい。
・ 「絶対心配ない」「こういう心配がある」等簡易な表記にしてもらえるとわかりやすい。
・ 一次評価でリスク「中」だったものが総合評価でリスク「小」になると、意図的にリスクを下げているように感じ得る。

2.1.3 評価項目
≪評価項目≫
・ 評価項目の精査が必要。適法であるものを評価する前提で整理する。また、行政事業向け、民間事業向けの整理が必要である。(項目間の重複、不正提供について問う項目の有無、第三者提供・本人同意・目的外利用は適法になりうる点)
・ 事業者の取得している権限や認証は、評価の判断材料の一つになりうる。
・ 何を防ぎたいかを最初に挙げて、そこから情報提供するとわかりやすい。
・ 起こりやすさ判定基準の項目がセキュリティに偏っている。OECD８原則と関連付ける等により、プライバシーリスクに関わる項目も追加すべきである。
・ 既定の評価項目以外に懸念、リスクはないかという包括的な項目を追加し、バスケットクローズ的にないものを吸い上げるような仕組みにしたらどうか。ユースケースに適用して運用しながら過不足を修正していくことでよい。
・ 市と委託業者が行うサービスであれば、 評価シートは事業者に書いてもらえばよい。

2.1.4 評価体制
≪評価体制≫
・ 責任者 (CPO) を誰にするのか。第三者評価と責任逃れの関係になることは防ぐべき。PIA 実施のタイミングは事業が決まってからでは遅い。
・ PIA 実施対象外も含め、年 1・2 回運用状況を評価委員会にフィードバックした方がよいのでは。実施不要の水準も、状況を見ながら調整していくこともありえるのでは。

・ パブリックコメントの実施を検討。
・ 事業者が納得してPIA実施できるようなコミュニケーションをどのようにとるのかも論点の一つ。
・ 評価委員会に市民が参画しても、市民の視点で評価できる項目はあまりないのでは。十分な対策が取られているかは非常に関心が高いが、市民が評価できるのか。

≪責任分界点≫
・ 個人情報漏洩はセキュリティインシデントの結果であることが多い。情報漏洩やインシデントが発生した場合の責任分解点については PIA 制度とは分けて考えるべきだろう。
・ サービス提供事業者の責任の範囲としては、虚偽でない誤認や不適切な記載についても責任を負うべき

2.1.5　実効性の担保
≪PIAの実効性≫
・ 行政としてリスク保有が許されるのか。どこまでのリスク保有を容認するのか整理が必要である。
・ 権限をどこまで持つか、手続にどう組み込むのか検討が必要。委託先の変更のみですべて評価し直しとなると業務量が膨大となる。同種同様のリスクであればPIA省略可も検討しうる。
・ 「評価」と「是正してサービスを実施する」のは切り離して検討すべき。評価委員会は評価理由を明示して評価を出すものであり、是正はサービスの実施主体で行うものと分けるべき。
・ 組織の価値観とリスク許容度（リスクの軽減・移転・回避・受容等）を踏まえ、特定されたリスクへの市の対応まで市民に明示するべき。評価だけではやや無責任に映りかねない。
・ PIA の実施は市の責任で死守すべき。PIA 実施とその権限が CPO にあることを条例でうたわれると一旦成立するのではないか。
・ 条例かどうかは、定める規律内容による。事業主体が決めることが基本となる。実施の適正を担保するために、必要な情報を提供していない等に対して罰則をかけるとすればありえるのではないか。
・ 事業の最終責任を負うのが、市であれば市長権限。民間事業だとしても市が関与する、もしくは市の情報を利用するのであれば市長権限で、是正措置を講じられる状態は必要ではないか。条例までは不要だが、何らかの形で是正要求ができる根拠は必要。ただ、評価委員会には是正権限

はないものと認識。
・ 是正の進め方で方法は変わる。市が責任を負うべき状況で、市が関与しない民間事業の違反や不正をどうするか、議論していく必要がある。
・ プライバシーリスクがあったとしても、それを上回る便益があればサービスは実施可とする考え方もある。
・ 重要なのはサービスの目的の明確化。「安全」はセキュリティの充実度で測り、「安心」はサービス目的が市民の便益に叶うものかで測る。
・ 規約違反の際の措置も考えるべき。接続タイミングだけではなく幅広く市の権限を確保するのがよい。

2.1.6　公表

≪公表≫

・ 総合評価結果は、文章ではなく、パッと見てわかりやすいマークのようなものがよい。
・ サービスの目的と、データを拠出することによるメリットとデメリットをより強調して説明する必要がある。
・ かみ砕いて、市民にわかりやすい表現を用いるべき。

2.1.7　運用

≪運用≫

・ 再評価が評価のやり直しなのか、変更部分のみの評価なのか、再評価の定義が必要。
・ 1 回 PIA をやれば通用するという考えはやめるべき。
・ 基準を細かく決めすぎない方が良い。

３　懇話会の概要

3.1　構成員

【座員】　　◎：座長

落合　孝文	渥美坂井法律事務所・外国法共同事業　パートナー弁護士
鯉沼　哲矢	市民委員
◎坂下　哲也	一般財団法人日本情報経済社会推進協会（JIPDEC）　常務理事
鈴木　健嗣	国立大学法人筑波大学システム情報系　教授
冨田留美子	市民委員
橋本　尚美	市民委員
平山　雄太	IDEAPOST 株式会社　代表取締役社長 前・世界経済フォーラム第四次産業革命日本センター スマートシティプロジェクト長
水町　雅子	宮内・水町 IT 法律事務所　弁護士
藤光　智香	つくば市政策イノベーション部　部長（第１回～第５回）
髙橋　安大	つくば市政策イノベーション部　部長（第６回～第８回）

（敬称略）

【関係府省】

内閣府地方創生推進事務局　企画調整官

【つくば市】

政策イノベーション部次長
スマートシティ戦略課長（第１回）
スマートシティ戦略課課長補佐（第１回）
スマートシティ戦略課係長（第１回）
スマートシティ戦略監（第２回～第５回）
科学技術戦略課長（第２回～第８回）
科学技術戦略課課長補佐（第２回～第８回）
科学技術戦略課データ連携推進監（第６回～第８回）
科学技術戦略課係長（第２回～第８回）

（令和７年３月１日現在）

3.2　懇話会開催状況

○ 第１回懇話会　　令和５年３月 17 日（金）※一部オンライン出席

（議題）

・　「つくば市プライバシー影響評価制度検討懇話会」の設置について
・　座員紹介・座長選任
・　「つくばスーパーサイエンスシティ構想」について
・　事例紹介
・　論点整理
・　今後のスケジュール

○ 第２回懇話会　　令和５年５月 25 日（木）※一部オンライン出席

（議題）

・　国内のプライバシー影響評価取組事例紹介について
・　つくば市が想定するプライバシー影響評価における目的、用語の定義、適用範囲のイメージについて

○ 第３回懇話会　　令和５年９月 27 日（水）※一部オンライン出席

（議題）

・　ユースケースの紹介、想定されるプライバシーリスクについて
・　つくば市プライバシー影響評価制度案について

○ 第４回懇話会　　令和５年 12 月 20 日（水）※一部オンライン出席

（議題）

・　評価項目と評価基準について
・　評価体制について

○ 第５回懇話会　　令和６年３月 15 日（金）※一部オンライン出席

（議題）

・　評価項目・評価基準について
・　制度化について
・　公表について
・　第５回までの中間とりまとめについて

○ 第６回懇話会　　令和６年８月 21 日（水）※一部オンライン出席

（議題）

・　民間サービスのユースケースを用いた PIA 制度の検討について

・　前年度からの継続論点の整理について

○ 第７回懇話会　　令和６年 12 月 20 日(金) ※一部オンライン出席
（議題）
・　最終とりまとめ（案）について
・　最終とりまとめに向けた残論点について

○ 第８回懇話会　　令和７年２月 14 日（金）※一部オンライン出席
（議題）
・　最終とりまとめ（案）について

４　総括

以上のとおり、これまで本懇話会では、「つくばスーパーサイエンスシティ構想」として、つくば市が先端的サービスの社会実装を推進していく中で、様々なデータが利活用されていくことに対して漠然とした不安を感じている市民がいることへの配慮として、利用を検討しているサービスがプライバシーにどのような影響を及ぼす可能性があるかを評価し、その結果を情報公開する仕組み、すなわちプライバシー影響評価制度をどのように構築するべきかについて検討を重ねてきた。本報告書は、これまで計８回に及ぶ懇話会で積み重ねてきた議論の状況を踏まえ、つくば市のPIA制度の在り方に関する基本的な考え方について、一定の方向性を整理したものである。

今回の整理を行うに当たって特に留意した点は、市民目線の制度構築になっているかという点を常に意識したことである。明確な評価基準となっているか、評価に客観性はあるか、市民に分かりやすいかといった視点に立ち、毎回の懇話会において整理を行った。また、PIA評価をすることが、イコール、サービスのゼロリスクを保証する、といった誤解に繋がらないよう、評価の見せ方についても留意して整理を行った。

今回の整理によって、つくば市の PIA 制度について懇話会として一定の方向性を示すことができたと考える。一方で、報告書内でも触れているとおり、今回の整理の考え方が将来にわたって常に正しいとは限らず、むしろ個人情報保護に関する社会の動向や技術革新は変化が激しく、整理の考え方も常に変化していくと考えるのが正しいだろう。こうしたことを踏まえ、つくば市におかれては、本懇話会による今回の整理を参考にして、PIA制度の施行に繋げてもらいたいが、PIA制度を施行したことで甘んじることなく、今後も市民にとって相応しいPIA制度となるよう不断の見直しを続けていってもらいたい。そのことが市民に寄り添い、市民とともに「つくばスーパーサイエンスシティ構想」を推進していくことに繋がるものと期待する。

別添

評価項目一覧（案）

別添１　評価項目一覧（案）

No.	調査項目概要	対策の必須/推奨	個人情報保護法/個人情報保護法ガイドライン(通則編)における該当箇所	備考
01	サービスの概要がわかる資料（事業企画書、提案書、仕様書等）	–	–	–
	①本サービスの目的及び内容	–	–	–
	②本サービスで使用するハードウェア、ソフトウェア、アプリケーション	–	–	–
	③本サービスで期待される効果	–	–	–
02	サービスの関係者がわかる資料（様式不問だが②以外の項目については一覧表形式で作成し、②で該当する取得済み認証があればその証憑を提出すること）	–	–	–
	①サービス提供事業者の概要	–	–	–
	②サービス提供事業者の認証（Pマーク、ISO27001（ISMS）のいずれか）取得状況	–	–	–
	③本サービスの責任者及び従事者	–	–	–
	④リスク管理責任者、セキュリティ責任者	–	–	–
	⑤委託先	–	–	–
	⑥協業先（ソフトウェア、ネットワーク、データベースの管理者を含む）	–	–	–
	⑦サービスを提供される主体	–	–	–

No.	調査項目概要	対策の必須/推奨	個人情報保護法/個人情報保護法ガイドライン(通則編)における該当箇所	備考
03	サービスが適合する個人情報保護に関する法令・制度・ガイドラインの一覧がわかる資料（事業企画書、提案書、仕様書等で示すか、様式不問にて一覧表形式で作成すること） 【例】 ・個人情報保護法ガイドライン（通則編） ・個人情報保護法ガイドライン（行政機関等編） ・金融分野における個人情報保護に関するガイドライン ・医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス 等	–	–	–
04	サービスの業務の流れがわかる資料（様式不問にて、フロー図に示すこと）	–	–	–
05	サービスにおける情報のライフサイクルと、情報の種類がわかる資料（様式不問にて作成すること。）	–	–	–
	①情報のライフサイクル（収集、利用、保管、廃棄）それぞれにおけるデータ処理の概要	–	–	–
	②処理担当者	–	–	–
	③各段階において取り扱うデータの内容	–	–	–
	④処理手順（①を詳細に説明すること。その際、可能であれば様式３を参考にフロー図形式で示すこと。）	–	–	–
	⑤データを用い作業する場所	–	–	–
06	データや情報システムの保管場所に関する情報（様式不問にて作成すること。下記事項の記載が不可能な場合は、その事由を説明し、可能な限り当該保管場所に関する説明文書の添付等で以て代えること。）	–	–	–
	①住所	–	–	–
	②当該部屋の階	–	–	–
	③当該建物の構造	–	–	–

No.	調査項目概要	対策の必須/推奨	個人情報保護法/個人情報保護法ガイドライン(通則編)における該当箇所	備考
07	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	個人情報保護法 第27条、第69条	民間が実施主体となり、個人情報を利用する事業の場合、一部の場合を除き、個人データを第三者へ提供する際には本人同意を取得する必要がある（個人情報保護法第27条）。 一方、行政機関が実施主体となり、個人情報を利用する事業の場合、当初特定された範囲内で保有個人情報を第三者へ提供する際には本人同意は不要だが、当初特定された目的を超えて第三者へ提供する場合に本人同意が必要となる（個人情報保護法第69条）。
08	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。 ※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	個人情報保護法 第21条、第69条	民間が実施主体となり、個人情報を利用する事業の場合、基本的に取り扱いに関する本人同意は不要だが、利用目的を通知/公表しなければならない。また、本人から直接書面で個人情報を取得する場合、利用目的を明示しなければならない（個人情報保護法第21条）。 行政機関が実施主体となり、個人情報を利用する事業の場合、基本的に取り扱いに関する本人同意は不要だが、当初の目的以外で保有個人情報を利用・提供する場合に本人同意が必要となる（個人情報保護法第69条）。
09	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。（利用者の認識・意図・希望と異なる情報処理がなされないことを説明すること。） ※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	個人情報保護法 第34条、第35条	本人は、個人情報取扱事業者に対し、当該本人が識別される保有個人データの内容が事実でないときは、当該保有個人データの内容の訂正、追加又は削除を請求することができる（個人情報保護法第34条）。 また、本人は、個人情報取扱事業者に対し、当該本人が識別される保有個人データが第18条若しくは第19条の規定に違反して取り扱われているとき、又は第20条の規定に違反して取得されたものであるときは、当該保有個人データの利用の停止又は消去を請求することができる（個人情報保護法第35条）。
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。	必須	個人情報保護法 第40条	–

No.	調査項目概要	対策の必須/推奨	個人情報保護法/個人情報保護法ガイドライン(通則編)における該当箇所	備考
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。（個人に関する情報の保存方法・媒体を問わず、本サービスに用いる個人に関する情報を参照・利用できなくなるリスクを防止できているか。）	–	–	–
	①データ保管媒体は、自然災害（地震・水害・落雷等）及び事故（火災・爆発等）による影響を可能な限り低減した場所で保管する（紙媒体でデータを保管する際は、水害及び火災・爆発について対策が講じられていることが望ましい）。	推奨	該当なし	–
	②データのバックアップ（クラウドサービスを用いたものを含む）は、正データと物理的に隔離されかつ①を満たす場所に保管されている。	推奨	該当なし	–
	③（該当する場合）データを格納した媒体を運搬する際には、データの破損が生じにくい手段を選択している。	必須	個人情報保護法ガイドライン(通則編) 10-5 (3)	–
	④重要な機器やネットワークを冗長化している。	推奨	該当なし	–
	⑤業務外の時間帯における端末やハードウェア、書類等の持ち歩き等を必要最小限とする旨を組織内規程で定めた上で、対策を実施している。	推奨	該当なし	–
	その他、対策している内容（自由記述）	–	–	–

No.	調査項目概要	対策の必須/推奨	個人情報保護法/個人情報保護法ガイドライン(通則編)における該当箇所	備考
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。	–	–	–
	①ハードウェアや紙媒体等、運搬可能な状態で保存されたデータの盗難対策を講じている（施錠された場所で保管、チェーンをつけて持ち運びできないようにする等）。	必須	個人情報保護法ガイドライン(通則編) 10-5 (2)	–
	②各データを機密性にしたがって分類し、その分類がわかりやすく示されている（「関係社外秘」「社外秘」「公開」等の別が明らかになっている）。	推奨	該当なし	–
	③適切な（ICカード方式、スマートフォン認証、生体認証等）入退室管理策を講じている。	必須	個人情報保護法ガイドライン(通則編) 10-5 (1)	–
	④デバイスや記録媒体の接続制限がある。	推奨	該当なし	–
	⑤データや機器を取り扱うまたは保管する場所に非関係者が入室する場合は、入退室の記録を取る・身分証を携行させる等の管理を講じたうえで許可しており、組織内の従事者ではないことが見分けられるような措置（色の違う入退室カードを貸与する等）を講じている。	推奨	該当なし	–
	⑥個人のスマートフォン等端末は原則として業務で用いない（除・BYODとしての利用、その他やむを得ない場合）また、必要な場合は執務室内への個人端末の持ち込みを制限する旨の組織内規程を定めた上で、対策を実施している。	推奨	該当なし	–
	⑦データの不正閲覧防止に関する組織内規程を定めた上で、対策を実施している（離席時の画面ロック、公共の場での組織端末使用の制限等）。	必須	個人情報保護法ガイドライン(通則編) 10-5 (1)	–
	⑧データ持ち出しの際は組織内で許可を得る等の組織内規程を定めた上で、対策を実施している。	推奨	該当なし	–
	⑨従業員の異動・退職後も守秘義務を保持する旨を雇用契約に明記した上で、締結している。	必須	個人情報保護法ガイドライン(通則編) 10-4	–
	その他、対策している内容（自由記述）	–	–	–

No.	調査項目概要	対策の必須/推奨	個人情報保護法/個人情報保護法ガイドライン(通則編)における該当箇所	備考
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。	–	–	–
	①システム、アプリケーション、データベースへのアクセスの際は適切なログオン手順（パスワード、生体認証、ICカード等認証情報を確認するもの）を必須としている。	必須	個人情報保護法ガイドライン(通則編) 10-6 (2)	–
	②一定回数以上のログイン認証失敗によるロックアウトや、安全性が確保できるまで再ログインの間隔をあける機能を実装する等により、IoT機器、サーバ等に対する不正ログインを防止している。	推奨	該当なし	–
	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	個人情報保護法ガイドライン(通則編) 10-6 (1)	–
	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	該当なし	–
	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	該当なし	–
	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	該当なし	–
	その他、対策している内容（自由記述）	推奨	該当なし	–
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。	–	–	–
	①イベントログを取得・保持するようになっている。	必須	個人情報保護法ガイドライン(通則編) 10-6 (3)	–
	②許可されていない、または意図せざる変更操作を防ぐ仕組みがある。	推奨	該当なし	–
	③データの重要な変更に関する承認・確認等のプロセスについて、組織内規程を定めた上で、対策を実施している。	推奨	該当なし	–
	その他、対策している内容（自由記述）	–	–	–

No.	調査項目概要	対策の必須/推奨	個人情報保護法/個人情報保護法ガイドライン(通則編)における該当箇所	備考
15	個人に関する情報の過剰収集が発生しないか（サービス提供に必要な情報以外も収集の対象としていたため、情報漏洩等のインシデントが発生した際の影響が大きくなる。）	–	–	–
	①収集する予定のすべての個人に関する情報について、その必要性が事業計画段階で明らかにされている。「念のため」「参考として」収集する情報がない。	推奨	該当なし	–
	その他、対策している内容（自由記述）	–	–	–
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。	–	–	–
	①HP等で本サービスに関する情報をいつでも閲覧できる。 ※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	個人情報保護法 第32条	個人情報取扱事業者は、保有個人データに関し、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置かなければならない（個人情報保護法第32条）。
	②利用者向けの説明資料が用意されている。	推奨	該当なし	–
	その他、対策している内容（自由記述）	–	–	–
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。	–	–	–
	①紙媒体で保存されたデータについては、定められた期限までに適切な方法（シュレッダー処理、溶解処理等）で廃棄することとしている。また、本サービスでのみ利用するハード媒体（CD等）があれば、業務終了時に物理的に破壊することとしている。	必須	個人情報保護法ガイドライン(通則編) 10-5 (4)	–
	②サーバ等で保存されたデータについては、適切な方法で消去する。	必須	個人情報保護法ガイドライン(通則編) 10-5 (4)	–
	③データの廃棄期限を明確に定めており、適切に廃棄している。	推奨	該当なし	–
	その他、対策している内容（自由記述）	–	–	–

No.	調査項目概要	対策の必須/推奨	個人情報保護法/個人情報保護法ガイドライン(通則編)における該当箇所	備考
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。（サービスが市民の権利と自由に与える潜在的な影響や、社会的弱者への潜在的な差別的影響があるか。ある場合は、どのように考慮・軽減されるかを記述すること。）	–	–	–
	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、または不当な扱いを受けることがない。	必須	個人情報保護法 第19条	–
	その他、対策している内容（自由記述）	–	–	–
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。	–	–	–
	①サイバー攻撃防止のために一般的に必要とされる技術的対策（ファイアウォール、マルウェア及び不正アクセスの検知ソフト、侵入したマルウェア等の駆除ソフトの導入）を講じている。	必須	個人情報保護法ガイドライン(通則編) 10-6 (3)	–
	②本サービスの実施に関連するアプリケーション等について、常に最新のセキュリティパッチを当て、アップデートを実施している。	必須	個人情報保護法ガイドライン(通則編) 10-6 (3)	–
	③（未然防止）利用中のシステム等の脆弱性に関する情報を適時受け取る体制があり、脆弱性が発見された場合は対処することができる。	必須	個人情報保護法ガイドライン(通則編) 10-6 (3)	–
	④（被害最小化）セキュリティインシデントが発生した場合の報告及び対応手順（システム停止、ネットワーク切断の要領を含むこと）が、組織内規程で定められている。	推奨	該当なし	–
	その他、対策している内容（自由記述）	–	–	–

No.	調査項目概要	対策の必須/推奨	個人情報保護法/個人情報保護法ガイドライン(通則編)における該当箇所	備考
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。（例：不正アクセス、不正通信についてのモニタリングは常時監視により行っている。またISMSに基づき、内部監査を年に1回実施している。）	–	–	–
	①外部との通信を常時モニタリングしている。	推奨	該当なし	–
	②情報システムの点検・監査に必要なログ（入退室記録、アクセスログ等）等を取得し、定められた期間保存している。	推奨	該当なし	–
	③①②で取得する情報の正確性を担保している（時刻の正確性等）	推奨	該当なし	–
	④①②で取得した情報等を活用し、情報システム・セキュリティに関する内部監査を年に1回以上実施している。	推奨	該当なし	–
	その他、対策している内容（自由記述）	–	–	–
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。	–	–	–
	①本サービスに従事する者全員に対し、各自の役職に適した情報セキュリティ全般の教育・研修を定期的に講じることになっている。	必須	個人情報保護法ガイドライン(通則編) 10-4	–
	その他、対策している内容（自由記述）	–	–	–
22	目的外利用が発生しないか。（入手した個人に関する情報を当初の目的以外で活用して利用者の意図しない用途で使用されてしまうことが無いことを説明すること。また、個人に関する情報ごとの許可されていない又は不適切な紐づけが発生しないか等、確認すること） ※行政機関が実施主体となり、個人情報を利用する事業の場合、個人情報保護法第69条2項に基づく適切な目的外利用であることを説明すること。	–	–	–
	①目的外利用は発生しない。	必須	個人情報保護法 第18条、第69条	–