会　議　録

<table>
<tr><td colspan="2">会議の名称</td><td colspan="3">第６回つくば市プライバシー影響評価制度検討懇話会</td></tr>
<tr><td colspan="2">開催日時</td><td colspan="3">令和６年(2024年)８月21日　開会15：00　閉会17：00</td></tr>
<tr><td colspan="2">開催場所</td><td colspan="3">つくば市役所コミュニティ棟１階　会議室１
（オンライン併用）</td></tr>
<tr><td colspan="2">事務局（担当課）</td><td colspan="3">政策イノベーション部　科学技術戦略課</td></tr>
<tr><td rowspan="3">出席者</td><td>委員</td><td colspan="3">坂下座長、落合座員、鯉沼座員、鈴木座員、冨田座員、平山座員、髙橋座員、水町座員</td></tr>
<tr><td>その他</td><td colspan="3">（オブザーバー）
内閣府地方創生推進事務局 牟田企画調整官、畠中研修員
デロイトトーマツサイバー合同会社　三谷氏、林氏</td></tr>
<tr><td>事務局</td><td colspan="3">政策イノベーション部
稲葉次長
政策イノベーション部　科学技術戦略課
中山課長、大垣課長補佐、高橋課長補佐、工藤データ連携推進監、金塚係長、金山係長、東泉係長、六笠主任、藏内主事、松好研修員</td></tr>
<tr><td colspan="2">公開・非公開の別</td><td>■公開　□非公開　□一部公開</td><td>傍聴者数</td><td>０名</td></tr>
<tr><td colspan="2">非公開の場合はその理由</td><td colspan="3">－</td></tr>
<tr><td colspan="2">議題</td><td colspan="3">(1)　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
(2)前年度からの継続論点の整理について</td></tr>
<tr><td>会議次第</td><td colspan="4">１　開会
２　議事
(1)　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
(2)　前年度からの継続論点の整理について
３　その他
４　閉会</td></tr>
</table>

１　開会

事務局（中山課長）：それでは定刻となりましたので、ただいまから第６回つくば市プライバシー影響評価制度検討懇話会を開会いたします。会議に入る前に、４月の人事異動に伴い、新たに政策イノベーション部長の髙橋が座員として懇話会に参加しますので、よろしくお願いいたします。

髙橋座員：政策イノベーション部長の髙橋でございます。４月に着任しております。今回からPIAの懇話会の座員として参加させていただきます。どうぞよろしくお願いいたします。

事務局（中山課長）：申し遅れましたが私、本日事務局の進行を行う、科学技術戦略課長の中山です。どうぞよろしくお願いいたします。本日の座員の皆様のご出席については、現地５名、オンライン２名となっております。鈴木先生については、遅れて出席される予定です。また本日は内閣府地方創生推進事務局から、牟田様も御参加いただいております。牟田様、一言お願いいたします。

牟田調整官：内閣府地方創生推進事務局でスーパーシティ担当しております牟田です。よろしくお願いいたします。前回第５回に続いて出席をさせていただいております。前回も申し上げましたけれども、このスーパーシティという取組にとって、データ連携基盤の利活用というのはいわば中心的な取組になってございます。今年はつくばがスーパーシティに指定されて３年目であり、つくばスーパーサイエンスシティ構想の中において、データ連携基盤の具体的な利活用をしっかりと進めていきたいタイミングになっているかと市と認識を合わせているところです。内閣府としてもPIAの検討を含め、データ連携基盤の利活用について、つくば市と連携して取組を進めていくこととしておりますので、内閣府の事業という形で、デロイトトーマツにも参加をいただきながら市とともに今年度利活用も検討させていただいています。本日の懇話会は昨年度皆様でやっていただいた中間取りまとめをもとに、主として制度化に当たり更に検討を深めるとお聞きをしていますので、安全安心のもとでデータ連携基盤の利活用が進むように、内閣府としてもぜひ市民委員の方々にも活発に御意見をいただけるとよいと考えておりますので、どう

ぞよろしくお願いします。

事務局（中山課長）：ありがとうございました。今牟田様からご紹介にありました通り、今年度のPIAへの制度検討について連携させていただいているデロイトトーマツサイバー合同会社様からは、三谷様と林様が出席されています。それでは早速ではございますが、ここからはつくば市プライバシー影響評価制度検討懇話会設置要項の規定に基づき、座長に進行をお願いしたいと思います。坂下座長、よろしくお願いいたします。

坂下座長：では本日もよろしくお願いします。本日の予定を申し上げます。本日の議事は２件になります。また会議の公開、非公開についてですが、つくば市附属機関会議及び懇談会等の公開に関する条例によって、法令又は条例で定めがある場合を除いて原則公開となります。本日の懇話会は非公開事由に該当しませんので、公開で進めます。また会議の記録のために、事務局においてZoomの録画及び写真撮影をしますので御了解ください。次に本日の配付資料の確認です。次第に配付資料一覧がありますので御覧いただき過不足ある場合は、事務局までお知らせください。それでは議事に入る前に令和６年度における懇話会の進め方について、事務局から御説明お願いいたします。

〔資料１について事務局から説明〕

坂下座長：どうもありがとうございました。今年度は今回を含め３回の会議を行い、最終取りまとめをまとめるということで進めます。本日も言い残しがないように御意見いただきたいと思います。

２　議事

(1) 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

坂下座長：それでは議題に入ります。「議事(1)　民間サービスのユースケースを用いたPIA等の検討について、事務局から説明をお願いいたします。

〔議事(1)について事務局から説明〕

坂下座長：どうもありがとうございました。御苦労されてまとめられていると思います。それでは事務局から説明がありました民間サービスのユースケースを用いたPIA制度の検討結果につきまして、各委員の方々から御質問お願いしたいと思います。オンラインの方は挙手機能で、会場の方は挙手をお願いいたします。いかがでしょうか。

鯉沼座員：先ほどa病院・b病院・c病院では、オンラインでの受診歴の使用を前提としているというお話でしたが、この親子は受診する際にはこのオンライン診察サービスは、おそらく念頭にないかと思うのですが、この親子がa病院・b病院・c病院を受診した際に問診票等で、例えば「今後オンラインサービスで使用することに同意する」といった対応をした上でこのサービスを使用するという考えでよろしいですか。つまり、アプリの利用のタイミングでオプトインはされているのですが、それ以前にa病院・b病院・c病院を受診した時に、データ連携基盤でこのデータが使用されることに対する何か同意をとる想定なのでしょうか。

事務局（高橋補佐）：今の御指摘あった部分ですが当然ながらリアルに病院にかかっているタイミングでは、その方はこのオンライン診療については想定していないと思っております。子どもの保護者というところから、吹き出しで伸びている部分ですが、アプリを利用するタイミングに２段階で同意を取ろうと思っています。まず１段階目が、このアプリ自体を利用するための同意です。それとは別に２段階目として、今まさに御指摘あった部分の病院でたまっている情報についても活用し、診療情報としてデータ連携基盤を活用して提供、A社で利用する部分の同意をこのタイミングで取ろうと思っています。リアルな病院の中で取れれば一番いいのかもしれないですが、実際には突発的に発生して、この診療サービスを使うことになると思いますので、このアプリの中での２段階での同意の所得で、その部分についてはクリアしようと思っているところです。

坂下座長：ありがとうございます。水町先生お願いします。

水町座員：今の点でもちょっと関連しますが、評価基準が少し甘いというと言い過ぎですが、緩やかな感じを受けました。今のサービスの場合、お子さん

のオンライン診療だからいいような気もしなくはないですけれども、やっぱりいつもかかる病院のカルテを取り寄せるとか、いつもかかってない病院のカルテを取り寄せてお医者さんに診てもらうとか、いつもかかっている病院にオンラインで別の病院受診をしているとか、b 病院を受診しているとかということがわかってしまうわけです。内科、小児科、皮膚科であればそんなに気にする方はいないのかもしれないですけど、小児科は行きたいけれど、他の病気の情報は伏せたいという人もいるような気もします。それはちょっと小児の場合は少ないかもしれないですが、例えば、メンタル系の病院に行っている時に歯医者にそれを知らせる必要があるのかというと、薬の飲み合わせが駄目という場合はよくないですけど、別にそういうことないのであれば、そこまで全部健康状態をつまびらかに明らかにする必要があるのかという考えはあると思います。同意を取るということだと思いますが、２段階の同意と言っても結局段階を踏んでいればいいかというとそうではなくて、結局もういざ今すぐやるとなった時に、「b 病院からカルテ取り寄せます」「c 病院にこの結果行きます」と画面が出て、そんなサービスだったのかと思ったとしても、とりあえず他のサービスを探すのが面倒くさい時に、「もうやり直すの面倒くさいから致し方ない」と同意するけど、「何となく嫌だな」ということもあるのではないかと思います。また、同意の取り方がとてもわかりづらいなど、利用規約に書いてあっても読まない人は多いと思いますけど、利用規約と分けて２段階でやると言っても、どういう結末になるのかがよく分からないような書きぶりだとなんかよく分からないけど、とりあえず書いちゃうというような、理解が不十分で同意する場合もあると思います。だから評価項目を見ると、例えば、資料２の８ページの＃7、ここは第三者提供する前に同意取得すればいいという文章だから起こりやすさ「１」になっていますが、同意する前の適切な説明があるかとか、そういうことも評価しないといけないのではないかなとか、逆に言うと＃のある評価項目は同意取っているかではなく同意取ってなくても提供できる場合は、法律上適法な場合はありますから、その意味では何かちょっと厳し過ぎるけど緩すぎるという感じを受けました。あと＃９や＃８も同意取得しているのかということが、結局、＃８は法律上同意までいらないと思うので、そういう意味で

厳しすぎるけれど、アプリでプライバシーポリシーに書いてあればいいだけなら誰でもそれはやるのではないかなとそれがわかりやすいかとかが、評価項目になるのではないのかなと思いました。あと＃９も利用者がどういうふうに情報選択したり削除したりできるかというのが、結局本件だったらその診療情報とか診療を受けたことってことが大事な気がします。ユーザー情報をアプリで削除したところで病院側にこういう受診しましたとかいう情報が残っちゃうので、結局ユーザー情報と問診情報が削除されることに意味があるのかとか、もう少し評価項目の細かい点を検討された方がいいかと思います。あと＃15でいえば過剰収集発生じゃないかに対して、限定していると書いてありますけど、そのa病院b病院分のカルテ情報まで収集することが過剰じゃないのか、特に診療に必要ないのに、全範囲全期間取得したら、そこまでいるんですか等の論点があるのではないでしょうか。あと＃22の目的外利用については、病院側で研究利用とかしないのか。発生しないと書いてあってもそれはA社が言っているだけで、c病院は実は研究に利用している可能性もあるから、そういえるのか。評価項目と回答の当てはめがちょっとずれている気がしました。本件でのプライバシーリスクを考えると、同意のところとか、病院データのやりとりっていうところのような気がするので、そういうことを踏まえた評価になるといいかと思います。あとちょっと違う観点から意見として、資料２の６ページで範囲について御説明いただいてありがとうございます。概ねよくわかったのですが、Aのパーソナルデータ連携基盤は対象外っていうのはちょっとどうなのかと思います。やっぱりそれこそがそのスーパーシティの大きな機能であれば、パーソナルデータ連携基盤は別途PIAをやるべきではないのかなと思って、結局土管で通しているだけだからいいとはいえ、それが市民にわかるかってことですよね。ただ単にこれだけ見ると、あらゆる病院のデータが連携基盤に溜まるって思う市民もいるかもしれないのに、対象外とか言われちゃうと、市役所がなぜ病院データを持っていていいのかと誤解される可能性もあるから、データ連携基盤にPIAは、必要じゃないのかなと思いました。あと最後もう１点ですが、資料の10ページで、次の論点にもなるかもしれませんが、市役所が民間サービスにお墨付きを与えるのではないかみたいな論点を書いていただいてい

ますが、11 ページを見ると、やっぱり主語が「つくば市は、本事業の評価をリスク小としました」となっていて、起こりやすさは大体１になるはずの基準になって、基準が結構ゆるいので３とか４は多分つかない評価になっていて、結局総合評価はAかBにしかならないと思って、そういう判断を市が下すところまで市が責任を負えるのかと思うので、もうちょっと書きぶりを考えた方がいいのではないかと思います。

坂下座長：ありがとうございます。まず今４点いただきましたが、最初の１点目については、まず子どもの話でこれはやっているので、大人の場合のこともあるのでしょうが、一旦そこは外して考えていった方がいいと思います。２つ目の評価については、市役所の方々が、自身が民間事業者になったつもりで今回評価していますが、ただ実際に出てきた時には、さっきの同意規定の部分も見なければいけないということを水町先生は指摘しているので、これは出てきた時にこれは考えなきゃいけないだろうと思います。３つ目のデータ連携基盤自身の PIA はどちらかと言えばセキュリティの方だと思いますが、当然必要だと思います。これはまた別途議論はしたいと思います。最後のところについては次の議論の方に移る話になりますから、ここはまた次のところで意見を聞きたいと思います。では他に御意見がありましたらお願いします。落合先生お願いします。

落合座員：どうもありがとうございます。実際に試してみていただいて、イメージが共有された部分は十分あるかと思っています。１点目が、多分 PIA への対象自体どのように考えるかというところです。今回は実験ですが、さっき水町先生おっしゃられていましたが、全体を見ていくこと自体は大事だと思います。今回はサンプルで検討しているだけだと思いますのでとりあえずいいと思いますが、最終的には全体的にどうなっているのか、評価される形になっていた方がいいのではないかと思います。様々な情報連携において、対策をすると言っても、そのテーマにあったような対策がされているかどうかを改めて振り返ってみるということは、悪いことではないように思います。もちろん１回評価した内容を流用して、組み合わせた場合にどう変わるかだけでもいいとは思いますので、それは今後、運用の際に御検討いただければと思いました。２点目が、先ほど水町先生がおっしゃっていた点があっ

て、ケース自体がどうこう言っても仕方がないというか、あくまで設例だと理解していますので、このケース自体をどう改善してくださいというよりも、どちらかというとこの評価項目でどう書いておくといいのかがあると思います。つまり先ほどお話されていた内容が、多分、同意の任意性、つまり急迫的な場合に言われると、そこでのその同意に対して任意性があるのかという話になるかと思います。また、明確性と言うべきなのかはありますが、わかりやすさと言うべきなのか迷いますが、同意をするだけの項目であれば多分、この評価でいいかと思っています。一方で、一旦そういう項目を立てたからそれにはめ込めば終わりという場面というよりは、実際には留意をするべきポイントが任意性や、明確性ないしは説明が十分であるかといった点であり、仮に考慮していくのであれば評価項目自体にそういう注意を書いておいていただいた方がいいと思います。単に「同意」と書いた時に、そこまでいろいろな同意の方式や内容を、精査しに行くのは、必ずしも継続的に実施されるかはわからないと思いますし、書く方の個人的な知見に頼ることになるかと思います。先ほど御議論あったような点は、単純に同意と書いておくだけがいいのかどうかという点で、見ていくといいと思いました。第３点としましては、これはスキームの整理自体ではありますが、仮に病院との関係としては、ドクターの業務として、実施していた病院、病院内診療所の業務として実施しているという場合であれば、第三者提供ではなく委託のようにも思います。もちろん他の病院の情報を見ることがあれば、そこは委託ではあるのだがさらに同意がとられているという処理になるとは思います。結果として、他の病院の情報を見るということがあれば、委託ではあるが、同意が必要となるかもしれませんので、もう少し整理の余地があるかとは思いました。ただ、あまりこのケース自体を言っても仕方がないことはあるかと思いますが、委託をしているのかどうかは実際には誰が最終的な管理をしているのかで、その管理義務が明示的にかかっているかに関わります。一応第三者提供の場合でも、外部に情報が適法に出されたことで終わりではないので、一応気にしてくださいと市の安全管理ガイドライン等には書いてあったように思います。ただそのルールはやや弱い話ではありますので、どういう関係性になっているかで言うと、委託であるのかどうかは１つポイントにな

るかと思いました。第４点としまして、これが起こりやすいのかどうかという評価について、どういう場合に１をつけるべきなのか、２がどういう場合にくるのかが、やはり１ケースだけですと、どういう相場感で運営するのが良いのかが若干わからない気はします。今後他のものなども企画していく中で、相場感が１ということが正しいのかどうかですが、結果として全部１になってしまうとあまりマッピングしている意味がなくなってくるので、そこはまた今後、見ていただければと思いました。テクニカルなところを申し上げて恐縮ですが、以上です。

坂下座長：ありがとうございます。４点御指摘がありましたので、１つはフィードバックをちゃんと入れたほうがいいという話。また同意の部分についてはもうちょっと細かく整理した方がいいのではないかという話。更にユースケースの部分については委託と第三者提供の話がありますけど、これは今回、市の提案は第三者提供で整理されていますから、実際これを出してくる事業者は違うのかもしれませんが、その時はそういう観点で見なきゃいけないだろうということ。また、起こりやすさを詰めていくと、例えばプライバシーマーク等第三者認証を受ける時の審査の時の書類等を出さなくてはいけなくなってしまいます。それでは厳しすぎて対応できる事業者も少なくなりますから、相場感はどこかで決めた方がいいと思います。その他御意見ございますか。大丈夫でしょうか。それでは次の議題に進みたいと思います。

（２）前年度からの継続論点の整理について

坂下座長：続いて「議事（2）前年度からの継続論点の整理」につきまして事務局から説明お願いします。

〔議題２について事務局から説明〕

坂下座長：どうもありがとうございました。今事務局から御説明がありました評価項目と評価基準と、評価体制について、順番に時間を取って、各委員の御意見も伺って、議論したいと思います。まずは評価項目について、各委員から御意見御質問をいただきたいと思います。では、平山座員お願いしま

す。

平山座員：説明ありがとうございました。今回議論になっている起こりやすさの部分で、特に今回システムのところ、データセンターがISMAPに対応しているということで全部１になっているということだと思いますが、私も詳しいわけではないのですが、ちょっと調べると、認証等に何千万もかかるシステムらしく、実際ここの検討されているようなスタートアップが、そんなシステムを構築するとは思えないということを前提にすると、ここがそうじゃなかった場合に、ここの数字がどう変わっていくのかは結構具体的なテーマになるのかと思いました。市役所が事業としてやる場合においては、概ね大企業が契約主体になっていくことが多いと思うので、割としっかりしたシステムでやられているところが多いと思うのですが、民間がもう少しそうではない市の事業ではないようなものになって、より動きやすいような民間のサービスだった場合は、そこまで多分そうじゃないので結果的には数字が変わってきてしまうのだろうというところが１つのポイントになるのかと思っているので、あまり却って難しくしすぎてしまうと、それで首を絞めることにもなりきれない。つくばはスタートアップの都市なので、スタートアップの方々ができる限り参加しやすいような枠組みでないと、それはそれでまた使い勝手が悪くなってしまうのではないかというのが私の意見でしょうか。

坂下座長：ありがとうございます。ちょっとISMAPは確かに多いのですが、経産省、総務省でクラウドサービスチェックリストを出しています。ISMAPではない場合は、多分それでチェックをするのかとちょっと思います。評価項目の部分などほか御意見いかがでしょうか。落合先生お願いします。

落合座員：ISMAPの点ですが、ISMAPはある程度の規模のIT事業者でも場合によっては自治体向け営業をしていないと取っていないことがあると思っています。大手の会社でITシステム系でも最近とろうかと思ったけれど大変ですよねと言われているところがあるくらいでした。ISMAPの点は決めておかないと、そういう前提になってしまって、かなり多くの場合をはじくことになってしまうかと思います。先ほど座長がおっしゃられたような、何かを参照してこう評価しておくと決めておいた方が、いいかなと思います。そこでどう評価していいか自分で考えてくださいと急に検討を求められてしまう

と、またそれも大変なのかもしれないので、そこはある程度事前に整備しておけると、いいのではないかと思いました。

坂下座長：ありがとうございます。続きまして、水町先生お願いします。

水町座員：ISMAPの件ですけども、私も詳しいわけではないのですがGoogleやAmazon等を使えばいいという気もするので、スタートアップでサーバーをクラウドにすれば、できなくはないと思います。自社のデータセンターをISMAP対応するのは当然大変だと思うのですが、そこは事業者に広く聞いていただければいいのかと思いました。あとISMAPは結局基盤のところだけなので、ISMAPにあるサーバーを操作上操作するのは、事業者の事業所から端末たたいて等であって、そこの管理が重要で。ISMAPのセンターに侵入してセンターから漏えいさせるというのは、きっとできなくはないけど難しいと思います。事業者のPCを感染させてという方がインシデントとして多いように思いますので、評価基準では対応されているとは思うのですけれど、要約のところだとISMAPがあれば、ISMAPをメインに書いていただいている感じでISMAPさえ取れば、ISMAPを取ってなければどうなのですかという感じなので、そういう事業者運用面も含めて要約に書いていただきたいのかなと思いました。

坂下座長：ここは事務局である程度選択肢が取れるように、整理をしていただければと思います。他によろしいでしょうか。では、次に評価基準の方について、御意見ございましたらお願いします。落合先生お願いします。

落合座員：先程の点とも関わるかと思いますが、同意という項目がある場合には、同意があること自体で良く、同意で処理しているのかどうかというレベルでの議論になり、まず形式的に同意があるかどうか自体になるとも思われます。それに対して、同意の方式として、さらに、どういった点を説明し、取得のプロセスでどのようにしておくかが議論になっていると思っています。その意味では、例えば具体例としては、わかりやすい説明になっているか、といった点が１つあると思います。規約の中に同意を完全に埋め込んでいくだけではないという方向かと思いますので、こういう形で使われますということを、全体としてもわかりやすくしておこうという話があったと思います。理解ができるような内容で同意を取得しようとしているか、最終的に

は緊急で差し迫っている時に、同意を取らないと駄目だという話になってしまうと、緊急時に使えなくなってしまうことはあるとは思います。一方で、できるならばそういうことではなく、選択肢があった方がいいということでもあろうかと思います。事前に同意を取らなかった場合にサービスができないとまでなると、かなりサービスとしては厳しい場合もあると思います。そうすると、事前に準備できるのであればなるべくそういう形にしていただいている等の事前の努力を評価しておくという点が論点と思いますので、少し踏み込んで見ていくとしたら、評価基準の中にプラスして書き込んでいただくのがいいかと思いました。

坂下座長：ありがとうございます。非常に重要な指摘だと思います。他に御意見ございましたらお願いします。この場は「定規」を作っている場なので、実際に物が出てこないと当ててみてどうかはわかりませんから、今の助言を得て、中をちょっと見直してバリエーションが取れるようにしていくということでまずは良いと思います。続きまして評価体制につきまして御意見ありましたらお願いいたします。冨田座員お願いします。

冨田座員：４ページの起こりやすさの評価をするときに、今までだと１か４かとなってしまうものを、別添の４の必須か推奨という項目を加えて、そういう極端な評価にはならないようにしたっていうことですよね。それは１か２かになるってことですか。例えば１項目しかなくて、推奨だったり必須だったりしてそれができていたら１、できなかったら２という感じでしょうか。

事務局（高橋補佐）：事務局から御説明しますと、例えば、その観点が１つしかなく、その観点が推奨のものであれば、冨田座員がおっしゃった通り、プラス１点は加点されるので、２になるということです。この観点が例えば２つ３つあって、全部推奨でそれが全部対応されてなければそこにさらに加点、加点とされるので、４になる可能性もありますし、そこはこの評価項目に対してどれだけの観点が用意されているか、それが必須なのか推奨なのかの違いによって、その評価項目に対しての最大４が発生するのか３が発生するのが決まってくるという形です。

冨田座員：評価してしまうということですね。いやそこが単純に、何で４段階あるのに、２段階までしかいかない項目があるのだろうというのが疑問で

す。

坂下座長：もうちょっとわかりやすい方がいいかもしれませんね。ありがとうございます。他いかがでしょうか。鯉沼座員お願いします。

鯉沼座員：評価の体制についてPIA評価委員会というか、今後このテーマについて評価するような委員会が作られると思うのですが、その委員会で実際にすることと言ったら、影響度や起こりやすさについては、今その定規にあたる部分を詰めているので、これに則ってほぼ機械的に行われるのかという印象受けたのですが、そうなるとこのPIA評価委員会で議論すべき内容は、このグラフの「C(orB)」や「B(orA)」等の評価をどうしようかということをするような内容になるのでしょうか。つまり、PIA評価委員会ができたときにどういったことを議論するのかは、この定規の部分をきっちり決めているのでこの後は「orA」か「orB」かだけ決めるようなそういった委員会になるのがちょっと怖いと思います。実は私が伺いたいのはこちらの評価体制としてPIA評価委員が今後発足してこれらを議論する上で、総合評価の他に、「orA」「orC」以外の結論となるようなことも今後あり得るのですか。

事務局（高橋補佐）：評価委員会については、懇話会の中でもなかなか十分な議論ができていないというのが正直なところです。そういったところもありまして、今の御指摘の点については前回の懇話会の中でも、市民委員がどういった役割を求められているのかがそもそもわからないといった御意見をいただいております。我々として今PIA評価委員会に期待していることとしては、事務局で一次評価（案）を作らせていただいて、起こりやすさと影響度についてはこういう評価になり、それを当てはめた場合の総合評価についてはこういう形になりましたけれども、この評価についてどう思われますかという妥当性の部分を皆様から御意見をいただきたいと思っています。ですので、総合評価として「Bでした」「Cでした」といった案を作りますけれども、その評価自体が本当に妥当なものなのかどうかについて、御意見を賜りたいと思っているというところが、今の評価委員会に期待するところです。ただ一方で、やはり市民の目線でその評価について御意見をいただく際に、むしろどういったところについて気になるのかとか、どういった点について評価した方がいいのかといったところについては、我々としても率直に知り

たいところなので、もし今のこの場で御意見等いただければ、そういった観点についても評価委員会の役割として持たせたいなと思うのでぜひコメント等いただければと思っております。

鯉沼座員：もちろんいろんなサービスを使用するにあたって、おそらくこの財産の影響や身体の影響で起こりやすくなったところでほとんどの評価すべき項目は、一通り網羅しているような感じはするのですが、それとは違う市民はあまりそのシステムのことをわかってないから出てくるような不安といったところが今後こういったPIA評価委員会で汲み上げ、ここで計り知れないようなところをちょっと吸い上げられるような仕組みとか、市民の本音で話せるようなことをこの委員会で引き上げられれば、非常に市民として使いやすいかなというような気がします。

坂下座長：そうですね。鯉沼委員の意見は的を得ていると思います。受容性や社会基盤として使われる時の受け入れのご指摘になっているのですが、その観点は我々のような専門でやっている人たちはどうしても、見えないところがあって、やはり市民の委員の方が自由に御意見いただくというのは非常にいいことだと思いました。では水町座員よろしくお願いします。

水町座員：２点ありまして、今の点に関してですけれども、評価基準がしっかり定まっていないと、案件やその評価委員によってぶれが結構出ると思うので、評価基準をしっかりと準備していることはとても評価できると思います。ただ今おっしゃったような面もありますので、評価基準以外で懸念、リスクはないかという評価基準が、評価項目を１個追加しておいて、バスケットクローズ的に、そこで評価基準にないものを吸い上げるような、仕組みにしたらどうかと思いました。あとは評価委員会で評価基準もやっぱり定期的に見直さないといけないかと思いますので、個別評価の他に評価基準の見直しも評価委員会の業務としてあればよいと思います。あと２点目ですけれども、協定書や利用規約について、利用規約に含める要件として、追加した方がいいと思う点をこれから述べたいと思います。大幅な変更が生じた場合は再申請を申し出るなどと入れていただいていますが、再申請を申し出なかった場合とか、要は利用規約に定めている事業者側の義務に違反した場合の措置について追加すべきではないか。虚偽があった場合はデータ連携基盤の利用を

停止するという制裁しかなく、措置がそれぐらいしかないのですけども、それ以外の、何かこういうことしましょう、例えばPIAを実施しましょうとか、改善しましょうとか、再申請しましょうとか、そういう義務があるはずで、この義務違反時の措置を規定しておく必要があるかなと思います。あとはPIA を公表されることと、PIA の結果によってはデータ連携基盤を利用できない可能性があるというのを事前に了解してもらった上で、PIA に取り組んでもらうというようにしないと、例えばリスク大と出てしまったときに、公表しないでくれともめる可能性もあるかと思いますので、そういう規定は入れるといいかと思いました。あとちょっと細かい点になりますが、再評価の場合の重要な変更について、別添３の１ページ目＃４、＃５のところにインプットアウトプットで変更があれば大規模なシステム改修です、と書いてありますが、インプットアウトプットって結構よく変わると思います。入力項目がちょっと変わるとか、もらうデータがちょっと１項目増えるとか、アウトプットも１項目増える程度で、大規模システム改修となるとしょっちゅう再評価するので、年間で再評価件数が多くなるような気もするので、ここはもうちょっと絞ってもいいかと思いました。

坂下座長：他の御意見いかがでしょうか。座長が質問してはいけないですけど、資料３の最後のページのところの①と②のそれぞれで、最後に市がPIAを実施するっていうことと、②はつくば市のPIAを受けるという言葉になっているのですが、このPIA評価書は事業者が書くということで、事業者が行ったものを市がPIAを評価しますというケースと、また②の場合だったら、つくば市の基準でやるPIAをやってきてくださいという見方でよろしいですか。評価書は誰が書くのかという質問です。

事務局（高橋補佐）：一時的な入力自体は、もちろん事業者に回答いただくのですけれども、その回答いただいた情報に基づいてPIAを実施するのはあくまで市になるので、つくば市が、情報が不足してれば、情報を入手しますし、追加のヒアリングをかけて、それを完成させることがつくば市の行う作業になってくるかと思っています。

坂下座長：市が評論する。でも評価書を出すのは事業者が出す。

事務局（高橋補佐）：そうです。

坂下座長：落合座員、お願いします。

落合座員：まずPIAの方の起こりやすさですけれど、最終的に１の場合が「無視できる」と書いておくことがいいのかどうかもあるように思っております。１が「無視」となっていますけれど、「必ずしも高くない」くらいにしておいた方が、あまり対策しなくてもいい、ようには見えなくもないと思いました。また、割と１に寄ってくる場合も多いのではないかという気もいたしましたので、何か無視という言い方よりは、少し可能性としてはあまり高くないというように言いつつ、ただ２よりは、もう少し起こりにくいような形で表現を少し工夫していただいた方がいいかと思いました。この基準の運用の点で、この起こりやすさの判定の中で、今回は特に１という評価になっていたかと思いましたが、例えば、管理の話を大目に議論していたところはございましたが、いろいろな主体との間で連携をするという作業があるときは、情報連携に関するつなぎ込みの部分で、リスクが生じる場合もあるとは思います。改めて見直してみたところ、その前のページの物理的観点、技術的観点、管理的観点でこういう対策をしていますということが主に書かれてはいましたが、こういうふうに広げて使っていきますという部分でも、多少は起こりやすさは増えるはずではあるとは思います。あまり完全に１になりすぎないようにということで広めに使っていくという部分については、少し評価をする要素を入れておいていただいた方がいいかと思いました。協定書や利用規約について、実効性担保で利用規約や協定書の中に、こういったことを定めておくということの中に、できるだけわかりやすく説明をするなど、利用者にとって、あまり不都合を感じる形にならないように、できるだけプロセスを設計してくださいというあたりは、合意する内容の中に入れておいていただいてもいいかと思います。ただ個別具体的な手法を書きすぎると、いろいろなケースがありすぎますので一般的に提供する契約書の内容としてむしろ協定書等の内容として不適切なると思います。抽象的な概念としては、わかりやすいこと等本人のためになることと、本人にとって不都合な判断を強いるものではないということは重要なポイントだと思いますので、それを合意していく内容の中にも若干入れておいてはと思いました。

坂下座長：ありがとうございます。細かく書くといいかもしれませんね。他御

意見いかがでしょうか。

平山座員：特段はないのですが、体制のところで、やはり民間サービスのところで難しいのが、民間がサービスをしますので民間のデータを使いますというときに、一般論で言うとなかなかこのデータ連携基盤を使わずにやるっていうケースが多くなると思います。あえてデータ連携基盤を使うという場合にのみ、今回PIAが使われるということになるわけですけど、そういうケースが、どこまであるのかがなかなか難しいなと思って今聞いていました。どこまでが実際には今後起こりうるので一番多いのは市役所の事業なのか、何かそういったデータを民間事業者が使う際にこのデータ連携基盤を使っていくというそのハイブリッドのような形が一番実際には多いのだろうと思うので、そういったところの、観点での議論をもう少し進められるといいと体制のところを読んで思いました。こう書かないと民間が民間でやるものなのに、何で市がPIAをやるのかという論点になってしまうのでそうならないためには、ここのデータ連携を使う場合はと書かないといけないということだと思いますが、それを言った時に、さっきの資料で言うところのデータ連携基盤は対象から外れていたので、そうするとやっぱり余計わかりにくくなると感じるところではありました。ただ、今回の論点ではあんまりないと思います。

坂下座長：現在はサービスがまだない状態で「定規」だけ作っている段階なので、実際にサービスが具体的に見えてこないと議論ができないところもあります。

鈴木座員：すいません。途中で少し抜けましたが、資料を見させていただいて継続論点のところと、議題１を御議論いただきましてありがとうございます。今ちょっとあった中で、ちょっと平山座員の発言でしたが私もちょっとデータ連携基盤を我々簡単に使い過ぎだなと少し反省しました。確かに、水町先生もおっしゃっていたように一般の人は、データ連携基盤にデータが溜まっていくと思ってしまうと私も思ったので、むしろ、データ連携基盤を使うサービスでやるというようなことは前提として我々やっているのですが、データ連携基盤の意味がわからなくて、むしろデータ連携基盤という単語を使うことが最ものリスクになって、それが分からないから怖いとなっちゃわ

ないかを、今日ちょっと聞いて思いました。あと１個目の「ABCD」のところで、説明を受けてみて、その時はわかりやすいかなと思ったのですが、「C(orB)」というのはもう少し書き方があってよかったかなと思います。色分けの問題で、例えば「D」と「D(orC)」のそのぐらいはいいと思いますが、「C」は例えばもう黄色にしちゃって「C(orB)」が薄い黄色で、要するに、ざっくりとした色分けは「DCBA」でちゃんと分かれている形がよいと思います。「B」が黄色と青になっていて「C」が赤とオレンジになっているのがちょっと気になりました。色を変えたらだいぶわかりやすくなると思っています。発言のまとめとしては、「DCBA」っていうのは、いろいろそれぞれ「D(orC)」と「D」は色のグループ同じにして、「C」と「C(orB)」のグループも色のグループ同じにして、「B」と「B(orA)」も色のグループ同じにして、「B」だけれど、条件満たしているから「A」とし、「C」だけれど条件を満たしているから「B」とするというのがわかりやすくなるといいと思いました。やっぱり基本的には「ABCD」でしか出さないというのは良いかと思うので、何もなかったら「C」だけどちゃんと満たしているから安全ですとリスク下げるということで、わかりやすくなると良いと議論１のときに思いました。

坂下座長：ありがとうございます。非常によくわかりました。

鈴木座員：左側がわかりやすいですよね。従来のリスクマップは、リスクの大きさで色のグループが同じだからわかりやすいのですが、今回それを真ん中で割ったので、何かうまく色合いのグループをかけると良いと思いました。

坂下座長：これはこれでやっぱり１つのアウトリーチの姿だと思いますので、例えば「C(orB)」のようなところは、完全に要協議いう区分になってくと思いますから、今後、ユースケースを当てはめたときにまた改善していくという流れで良いのかと思います。ありがとうございます。時間もだんだん差し迫って参りましたが、何か言い残したことがありましたらぜひお願いします。次回12月になりますので、今日できる限り御意見をいただきたいと思います。

事務局（高橋補佐）：追加で事務局から御意見を求めてよろしいでしょうか。議題１のところで水町座員からも御指摘いただいていた部分で評価報告書概

要版の件ですけれども、今「つくば市が」というような主語のもと総合評価等々について、公表するような形をとらせていただきます。PIA については市の責任のもと行うことになりますので、ある程度市の責任のもとこうやって公表する形になるのかなと思っているのですけども、一方で民間事業者に対するお墨付きの話ですとか、何らかの懸念点等はございまして、どこまでつくば市という名義のもとで、総合評価を含めた評価を公表するべきなのかという点についてちょっと御意見いただければと思っております。

坂下座長：公表のレベルをどこまで考えたらいいかということなので、すべての座員の方からご意見いただきたいと思うのですが、平山座員からお願いします。

平山座員：今のお話において、基本的にデータ連携基盤を活用した事業というのは、市役所の事業であることが多いと思っていますので、民間事業のデータも活用される際に、リスクがないかどうかを確認して公表する。これは市役所が市民の方々に安全性などいろんなものを説明するための情報として公表していくっていうことが、１つだと思います。今回のケースのように、民間と民間でやる場合のものは、基本的には先ほど申し上げた通り、民間は別にデータ連携基盤使う必要は本来ないので、民間同士で勝手にやればいいものをあえて使うということは、お客様サービスの対象に対して、あえて地域を限定した事業であり、かつ民間同士でやってしまうと情報がどう使えるかわからないというような不安があるかもしれないわけですけど、あえてその市のデータ連携も活用することによって、正しくこういったものが公表されるとすれば、自分たちにとってのレピュテーションリスクの低下やその信用補完みたいな部分に繋がっていくことが起こる価値なのだろうと思います。そういった観点で、公表していくととらえていくと、説明がつきやすいのではないかと思います。市が主語で、ある意味市のサービスとしてやっていく際の説明のものと、先ほどから議論があった例えばリスク小でこれはリスク小と書くのではなく、リスクが制限されている等の文言でうまく調整していくのがよいと思います。リスクゼロということは絶対ないわけですけど、ある程度限定されているものだとか、そういったような部分が、より説明されることで、やはり新しいテクノロジーを使う際は、みんな怖いので、その怖

い部分に対して、こういったリスクはあるかもしれないけれども、こういった価値があるのだから、できる限り安心安全に使っていこう、私達も可能な限りチェックはしていますというメッセージを正しく市民に伝えることで、他の自治体に比べて、より先端的な技術が使われるような街になっているというところを目指していくと考えると、公表するところの意味合いっていうのは、２つあるのではないかと考えました。

冨田座員：私は、つくば市のサービスだったらつくば市を前面に出してほしいなと逆に思うし、民間の企業だったら、新しいサービスを使う時はおっしゃった通り怖いと思うのですが、時代的に新しいサービスがどんどん出てくるので人々って結構慣れてはきていると思います。それはあるよねとみんなわかって、でもそれ以上の価値を求めるからやるという部分ももちろんあると思うので、そこをもうちょっと後押ししてくれる一歩が、このつくば市がある程度のリスクはあるけど、これぐらいですよ、だから使ってみてくださいみたいな後押しをしてくれると、使いやすいかなというのが私の感覚なので、主語はつくば市にしてほしいなと思います。

坂下座長：ありがとうございます。鯉沼座員いかがですか。

鯉沼座員：私もつくば市が主体となってそのデータ連携基盤を使って行うサービスなのであればつくば市の主語でやるのは妥当かなと考えています。あとこういった情報を民間同士でやりとりすると、民間としてそういったサービスをしているような業者とかもあると思うのですが、そこにあえて市のサービスを行うことによって市民としては、例えばこの提示いただいた、例えばオンライン診療サービスとかで、その情報が市のデータ連携基盤を通して活用されるって話ですが、市民としてはこういった情報が活用されるのはさらに何かプラスアルファで、この情報をさらに活用した何かサービスとかそういった何か展開とかもちょっと期待するようなこともあるので「つくば市は」とした方が、そういった所を活用されてさらにサービスができるのではないかっていうのも込めてちょっと使用してみたいという希望も込めて、やりたいという人は結構いるのかなと感じております。

坂下座長：ありがとうございます。落合先生いかがですか。

落合座員：公表の仕方について、行われている内容とそれが意味のある新しい

ものであるかが、わかるような形であることが大事だと思います。一方で全体の仕組やサービスの中身をもう少しわかるような形にすると、字が多くなってしまいます。専門家的には端的にまとまってわかりやすいと思うのですが、読む人の大半は専門家ではないため、無味乾燥な書かれ方と感じてしまう側面もあると思います。言葉だけではなく、例えば図面をつけるなどどういうイメージを持つべき取組なのかをわかるようなものの打ち出しができた方が良いと思いました。

坂下座長：ありがとうございます。水町先生お願いします。

水町座員：主語がつくば市という点について、つくば市が民間サービスについて評価できるという御判断であれば良いと思います。しかし、例えば内閣官房だったら、「本事業の総合評価をBとしました」、民間企業の事業を「リスク小」とは書かず、国が認定することはしないと思います。これは公務員的な考え方にもよるとは思いますが、国や自治体が他人の事業の評価をどこまで断言できるのかという問題があるからです。他にマイナス面としては、評価基準について細かく作ってはいますが、起こりやすさが１以外にはほとんどならないはずですよね。評価基準を満たしている中でインシデントが起こっているのがこの世の中です。事業者があまり情報を出さない、出しても全然返ってこないこともあり得る中で、どれだけの情報をもとに見きれるかという問題もあり、ここは市の判断になりますが、市民に与える影響やどれだけの情報を持って確固たる判断ができるかをお考えいただきたいと思います。

鈴木座員：前提として、民間のサービスで市のデータ連携基盤をわざわざ使ってやることがあるのかと思っています。やっぱりメリットがあるのは、つくば市がデータ連携基盤を持っていて、市が保有するデータを使う場合になるだろうと思っていました。そのため民間と民間でこれを使う方が実はレアケースで、しかし市民からすれば、「一部でもつくば市が保有するデータを使うなら市がちゃんと確認してほしい」と思いますし、まさしく国レベルでは確認できないけど、行政単位で直接住民にリーチするから責任を持てるということが、現実的に可能かをチャレンジしているのがこのPIAかと思いました。現行の方針で頑張っていくのが良いのではということと、やはりユース

スタディーやケーススタディの例として、つくば市が、市が保有するデータを扱うケースを考えていくのが、このPIAが事実的に意味を持つのではないかと思いました。

坂下座長：ありがとうございます。髙橋部長お願いします。

髙橋座員：まず本日皆さん本当にありがとうございます。私の立場で意見を言うと非常におこがましいような気がしますので、皆さんの御意見を踏まえて、ちょっと考えたことは、やはり民間事業者が民間のデータを使う時に、データ連携基盤を使うというのを想定するのは非常に難しい。今回お示しさせていただいた民間ユースケースも、これはどうなのかという御意見もあり難しかったと思っています。また民間同士のやり取りであるということに起因して、評価の主体がつくば市でいいのかという御意見がありました。そこで一点、弁護士の先生方にお伺いしたいのは、例えば主語をつくば市にして、リスクがAやBであるとされたがインシデントが起こってしまった場合に、つくば市側にどれぐらい責任が降ってくるのか。参考となるような過去の事例をご存じでしょうか。

坂下座長：水町先生いかがですか。

水町座員：そのような事例は存じ上げないですが、法律的に考えると、国家賠償請求がされるということですよね。事業者を訴えかつ市役所も訴えるとした際に、市役所は監督義務違反を主張されると思います。本件は純粋民間だから、自治体が関係している部分は、データ連携基盤の接続を許可して使わせた部分とPIAの実施なので、訴えるとしたらそこくらいしかない。市がリスクを判断したからサービスを使ったのに、判断に過失があったから損害が発生したという構成ができる可能性はあります。メディアとか市民感情の観点からは、主語をつくば市にするかの問題ではない。PIAをやっていなくて、データ連携基盤に接続させたというだけでも、こんな不十分なサービスをデータ連携基盤に接続させた市に過失があるという法的構成が取れるわけですから、メディアや議会対応で、市がこう言っているがどうしてこういうことが起きたのかということを総合的に吟味した方がいいと私は思います。落合先生、補足があればお願いしたいと思います。

落合座員：最終的には評価をしたことが、どこまで意思決定に直接働きかけて

いるかではあると思いますが、そういう意味では直接的なものではなく、間接的に判断に影響を及ぼす可能性があるという程度のものであると思います。このため、直ちに責任が生じうるということではないだろうと思います。どちらかというと何か言われるとすれば、データ連携基盤を使っている中での審査の方があり得ると思います。ただこれも実際に利用許可をする水準かどうかということにかかってくる部分が大きいとは思うので、PIA での全体的な評価が直ちに法的責任の有無に繋がるようなものではないと思います。ただ一方で責任が０とは言えないので、こういった説明を行うことについてのディスクレーマーなどは、書いておいても良いと思います。ディスクレーマーがあるから決定的だと言えないですが、書いてあった方があくまで参考資料と示すことができると思います。決して保障するものではないと理解しているので、そういう位置付けのものであるということ自体は示した方がいいと思いました。

髙橋座員：今の御意見を踏まえて、鈴木先生からも、そういったこともありながらつくば市としてやるということが PIA であるというような力強いお言葉をいただきましたので改めて内容を練り 12 月にはもう少し良いものをお示しするように頑張っていきたいと思います。どうもありがとうございます。

坂下座長：本日予定しておりました案件はすべて終了いたしました。進行を事務局に戻したいと思います。お願いいたします。

事務局（中山課長）：長時間にわたり御議論いただきありがとうございました。次回の懇話会は、12 月頃の開催を予定しております。次回は本日いただいた御意見を踏まえまして、最終取りまとめに関する協議として御議論をいただきたいと考えております。以上をもちまして、第６回つくば市プライバシー影響評価制度検討懇話会を閉会といたします。ありがとうございました。

第６回つくば市プライバシー影響評価制度検討懇話会

日時：令和６年(2024年)８月21日（水）15時～
場所：つくば市役所コミュニティ棟１階　会議室１
（オンライン併用）

次　　第

１　開会

２　議事
(1) 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
- ➢ 検討結果の説明　（20分）
- ➢ 検討結果に関する質疑　（20分）

(2) 前年度からの継続論点の整理について
- ➢ 整理結果の説明　（15分）
- ➢ 評価項目に関する議論　（10分）
- ➢ 評価基準に関する議論　（20分）
- ➢ 評価体制に関する議論　（25分）

３　その他

４　閉会

○ 配付資料
資料１　令和６年度における懇話会の進め方について
資料２　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
資料３　前年度からの継続論点の整理について

○ 参考資料
別添１　PIA調査シート
別添２　PIA評価報告書（概要版）
別添３　継続論点の整理一覧表
別添４　評価項目　新旧対象表

資料１

令和６年度における懇話会の進め方について

＜経緯＞

- **これまでに５回の懇話会**を通じてPIA制度の構築に向けて制度の骨格について議論を進め、**中間とりまとめ**を行った。
- 令和５年度は、**行政が行政保有のデータを活用するユースケースによって議論**を行ったが、つくばスーパーサイエンスシティ構想の取組をさらに進める上では、**データ連携基盤を活用して、民間事業者を含めた多様な主体が、行政･民間の様々なデータを用いて新たなサービス実装を行うことが想定**される。
- このような点を踏まえ、中間とりまとめをベースとし、令和５年度とは**異なるユースケース（民間ユースケース）をもとに議論を継続**し、評価体制･評価基準等について**さらに検討を深める**こととした。

＜今年度の進め方＞

- 中間とりまとめをベースとし、 新たな**ユースケースに基づきPIA制度案の検討を深め**、つくば市におけるPIA制度の確立に向けて「**最終とりまとめ**」**をとりまとめる。**

＜実施概要＞

協議事項		概要
①	民間ユースケースを用いたPIA制度の検討	前年度の懇話会で議論･とりまとめた評価体制･評価基準等をもとに、民間ユースケースを用いて検討･確認を行い、PIA制度の確立に向けて、各論点の検討を深める。
②	前年度からの継続論点の整理	中間とりまとめにおいてさらに検討が必要な論点（継続論点）とされた民間サービスの特性を踏まえた検討等について議論を行い、PIA制度に反映･更新する 今回
③	「最終取りまとめ」の作成	上記①ユースケースを用いたPIA制度の検討結果及び②継続論点の整理を踏まえ、懇話会として、つくば市におけるPIA制度の確立に向けた「最終とりまとめ」をとりまとめる

＜スケジュール＞

今回

令和6年(2024年) 8月

第6回

①民間ユースケースを用いたPIA制度の検討

②前年度からの継続論点の整理

令和6年(2024年) 12月

第7回

③「最終取りまとめ」に関する協議

※第６回で協議し切れなかった論点があれば協議

令和7年(2025年) 2月

第8回

とりまとめ

資料2

議題１　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

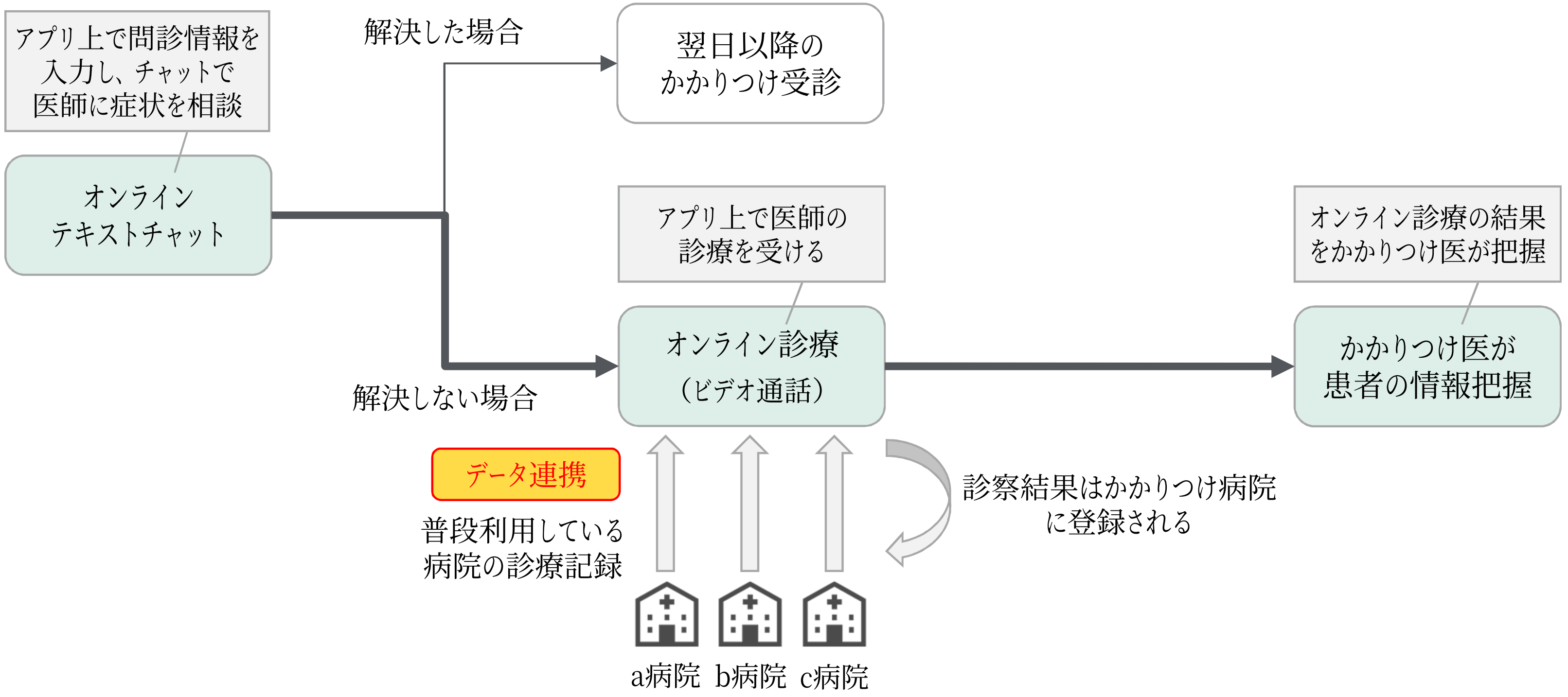
民間サービスのユースケースとして、「小児向けオンライン診療サービス（仮）」を事例に制度案を検討する。

＜ユースケースのサービス概要＞

概要

- ■ かかりつけ医の診療時間外である休日・夜間でも、自分の診療情報を使って、安心・安全なオンライン診療が受けられる医療サービス
- ■ データ連携基盤を活用し、アプリに入力した問診情報のほかに、普段利用している病院に保管されている診療記録を医師が参照しながらオンライン診療を行える仕組みを構築
- ■ 「民間事業者」が提供するサービスであり、行政はサービス運営に関与しておらず、行政データの取扱いもない

サービスイメージ※



※　民間事業者が検討するサービスを参考に、懇話会での議論用に市がサービス内容を設定したもので、実際の事業者のサービスを示すものではありません。

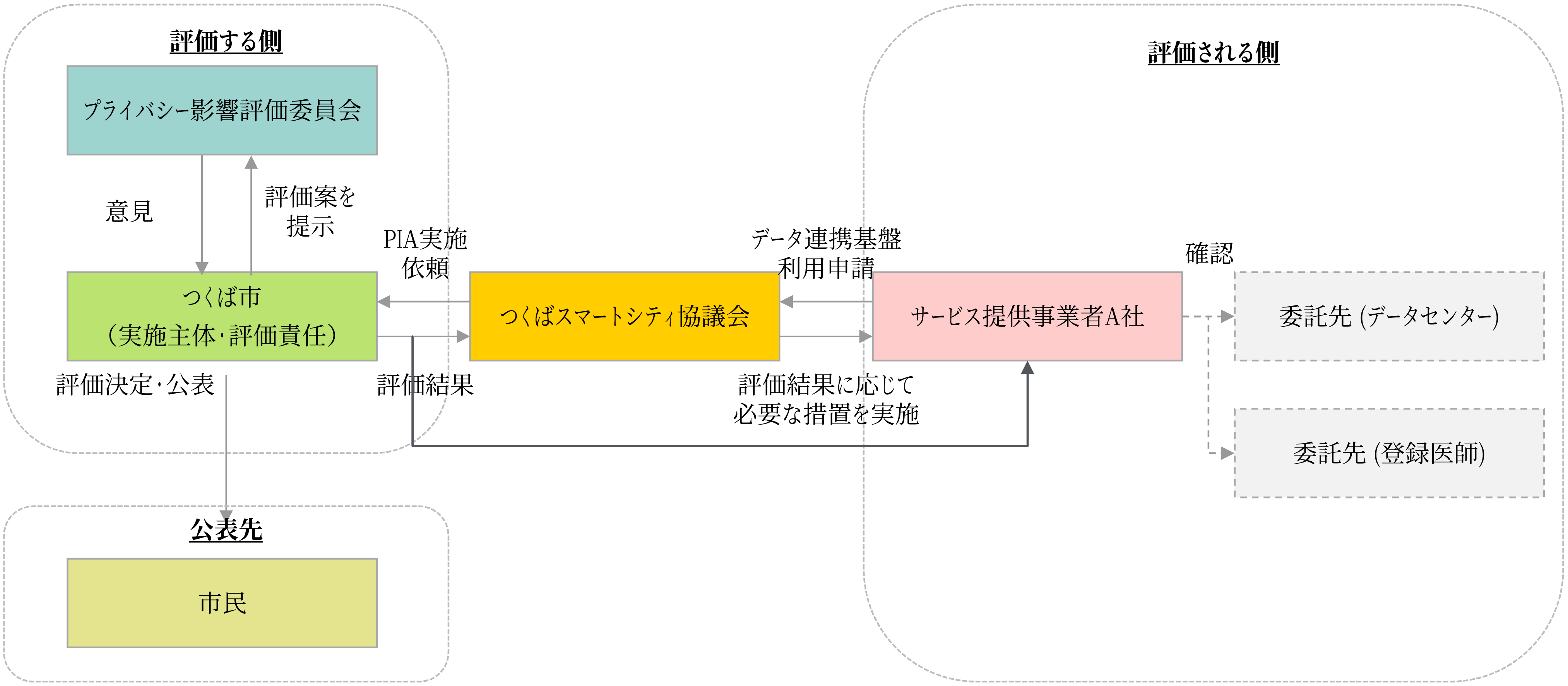
※　懇話会での議論用に市でサービス内容を簡素化、一部加工しています。実際の事業実施にあたっては関係法令を踏まえ事業が実施されます。

議題１　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

資料2

＜本サービスのPIA実施に係る評価体制について＞

- 本ユースケースでは、A社が提供するデータ連携基盤を活用したサービス（小児向けオンライン診療サービス（仮））を対象にPIAを実施。A社がサービス提供のためにデータ連携基盤の利用申請を行うに当たって、PIAもあわせて実施。
- 本ユースケースを用いて、民間事業者がサービス主体となって、データ連携基盤を活用してプライバシーデータを用いたサービスを提供するケースについて、これまで検討してきた評価の考え方等で問題なくPIAを実施することが可能か検討を行った。

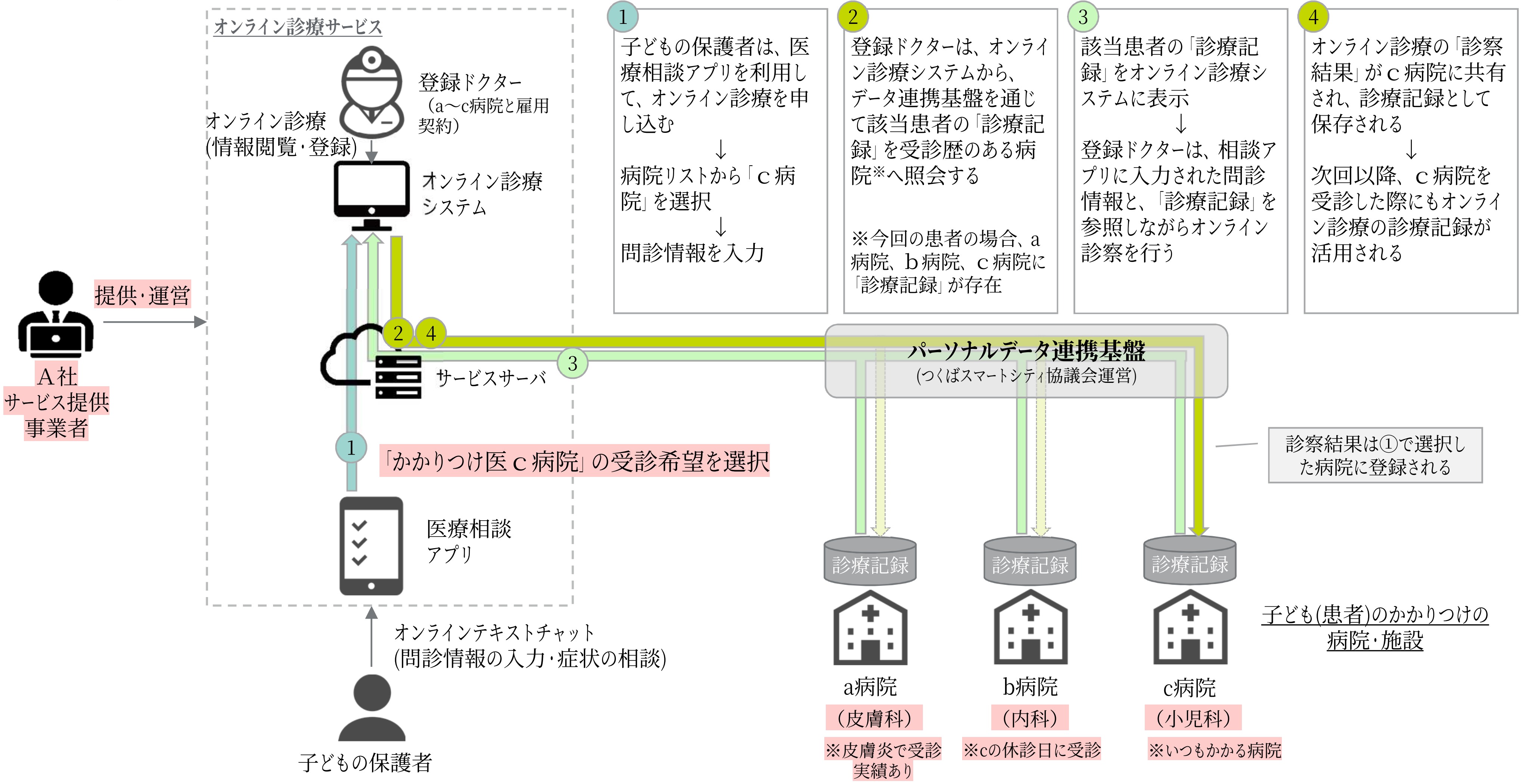


議題１　民間サービスのユースケースを用いたPIA制度の検討について

資料2

【今回議論する想定利用ケース】
- サービスの利用者は体調を崩した子どもを抱える保護者
- 普段は小児科のｃ病院（かかりつけ医）を主に受診している。その他、症状に応じて皮膚科のａ病院、内科のｂ病院も受診している。
- 今回、子どもが夜間に39.0℃の発熱、発疹の症状が発生し、サービスを利用。
- ３日前にかかりつけ医のｃ病院（小児科）が休診だったため、別のｂ病院（内科）を受診した。

＜サービス利用の流れ＞



1
子どもの保護者は、医療相談アプリを利用して、オンライン診療を申し込む
↓
病院リストから「ｃ病院」を選択
↓
問診情報を入力

2
登録ドクターは、オンライン診療システムから、データ連携基盤を通じて該当患者の「診療記録」を受診歴のある病院※へ照会する

※今回の患者の場合、ａ病院、ｂ病院、ｃ病院に「診療記録」が存在

3
該当患者の「診療記録」をオンライン診療システムに表示
↓
登録ドクターは、相談アプリに入力された問診情報と、「診療記録」を参照しながらオンライン診察を行う

4
オンライン診療の「診察結果」がｃ病院に共有され、診療記録として保存される
↓
次回以降、ｃ病院を受診した際にもオンライン診療の診療記録が活用される

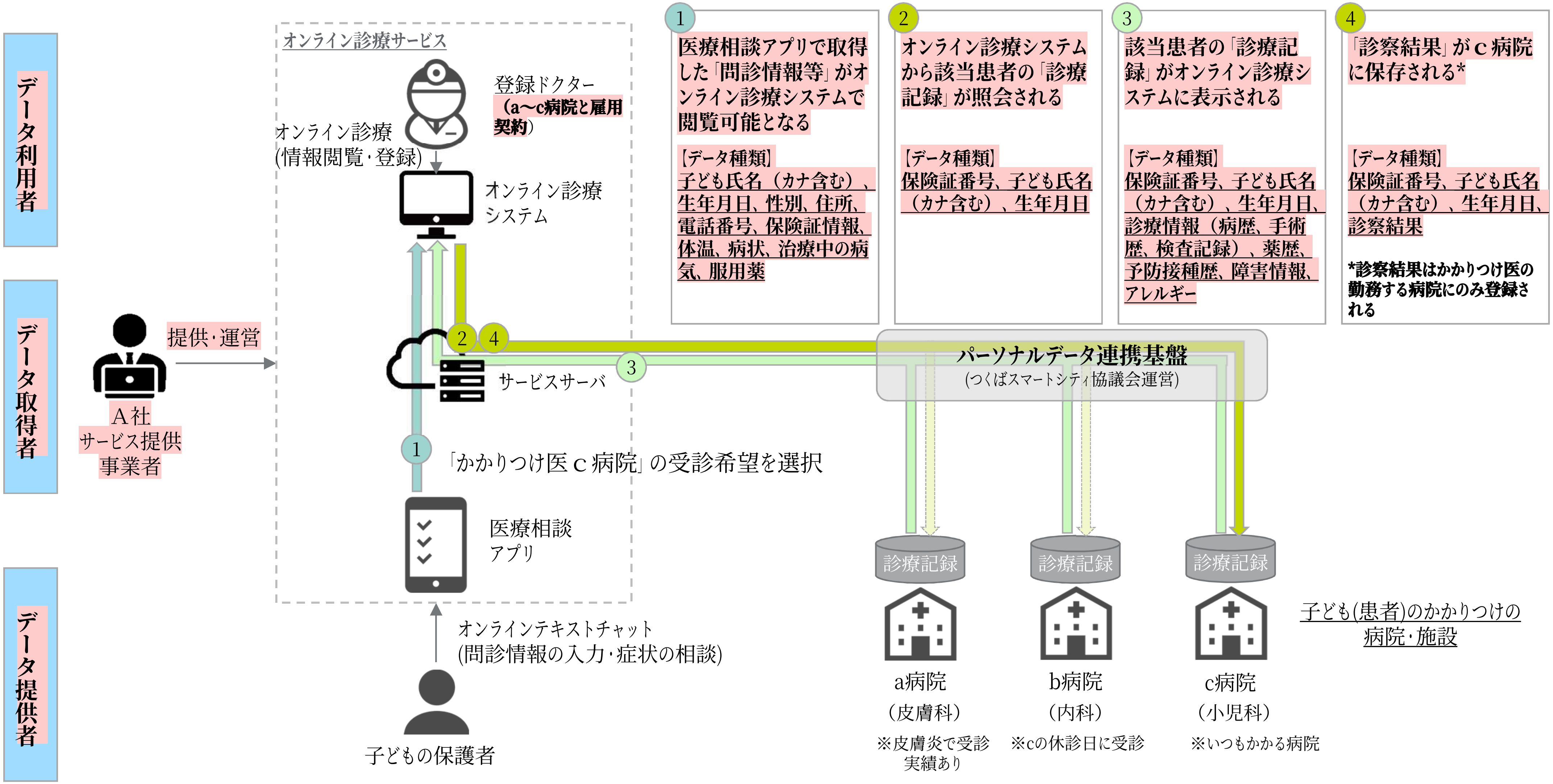
※　民間事業者が検討するサービスを参考に、懇話会での議論用に市がサービス内容を設定したもので、実際の事業者のサービスを示すものではありません。
※　懇話会での議論用に市でサービス内容を簡素化、一部加工しています。実際の事業実施にあたっては関係法令を踏まえ事業が実施されます。

議題１　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

資料2

＜サービスの関係者、使用するプライバシーデータの種類とデータ利用の流れ＞

- 子どもの保護者を「データ提供者」として、オンライン診療サービスを提供・運営するＡ社にデータを提供（Ａ社がデータ取得者）。提供されたデータをもとに、登録ドクターが「データ利用者」としてオンライン診療を実施。
- サービスの各段階で使用されるプライバシーデータの種類は下図のとおり



データ利用者

データ取得者

データ提供者

オンライン診療サービス

登録ドクター
（a〜c病院と雇用契約）

オンライン診療
(情報閲覧・登録)

オンライン診療
システム

提供・運営

Ａ社
サービス提供
事業者

② ④

③

サービスサーバ

①

「かかりつけ医ｃ病院」の受診希望を選択

医療相談
アプリ

オンラインテキストチャット
(問診情報の入力・症状の相談)

子どもの保護者

パーソナルデータ連携基盤
(つくばスマートシティ協議会運営)

診療記録

診療記録

診療記録

a病院
（皮膚科）
※皮膚炎で受診実績あり

b病院
（内科）
※cの休診日に受診

c病院
（小児科）
※いつもかかる病院

子ども(患者)のかかりつけの病院・施設

①

医療相談アプリで取得した「問診情報等」がオンライン診療システムで閲覧可能となる

【データ種類】
子ども氏名（カナ含む）、生年月日、性別、住所、電話番号、保険証情報、体温、病状、治療中の病気、服用薬

②

オンライン診療システムから該当患者の「診療記録」が照会される

【データ種類】
保険証番号、子ども氏名（カナ含む）、生年月日

③

該当患者の「診療記録」がオンライン診療システムに表示される

【データ種類】
保険証番号、子ども氏名（カナ含む）、生年月日、診療情報（病歴、手術歴、検査記録）、薬歴、予防接種種歴、障害情報、アレルギー

④

「診察結果」がｃ病院に保存される*

【データ種類】
保険証番号、子ども氏名（カナ含む）、生年月日、診察結果

***診察結果はかかりつけ医の勤務する病院にのみ登録される**

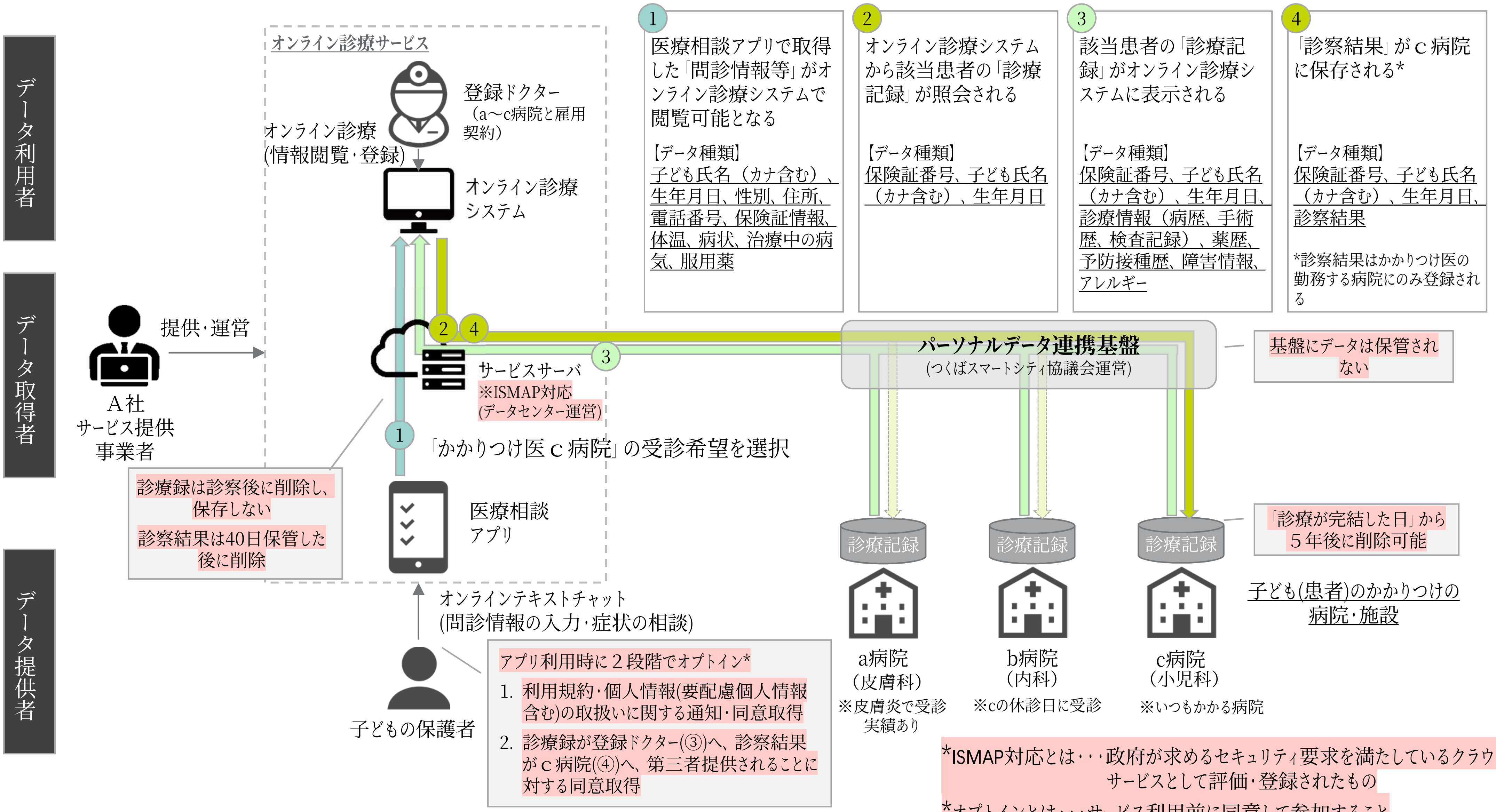
※　民間事業者が検討するサービスを参考に、懇話会での議論用に市がサービス内容を設定したもので、実際の事業者のサービスを示すものではありません。
※　懇話会での議論用に市でサービス内容を簡素化、一部加工しています。実際の事業実施にあたっては関係法令を踏まえ事業が実施されます。

議題１　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

資料2

＜PIAの主な確認ポイント＞

- プライバシーデータの取得･利用･保管･廃棄の一連の流れにおける対応はどうなっているか
- セキュリティ対策は十分か
- プライバシーデータの利用にあたって同意が取られているか



データ利用者

データ取得者

データ提供者

オンライン診療サービス

登録ドクター
（a～c病院と雇用契約）

オンライン診療
(情報閲覧･登録)

オンライン診療システム

サービスサーバ
※ISMAP対応
(データセンター運営)

A社
サービス提供事業者

提供･運営

診療録は診察後に削除し、保存しない

診察結果は40日保管した後に削除

1 「かかりつけ医ｃ病院」の受診希望を選択

医療相談アプリ

オンラインテキストチャット
(問診情報の入力･症状の相談)

子どもの保護者

アプリ利用時に２段階でオプトイン*

1. 利用規約･個人情報(要配慮個人情報含む)の取扱いに関する通知･同意取得
2. 診療録が登録ドクター(③)へ、診察結果がｃ病院(④)へ、第三者提供されることに対する同意取得

1	2	3	4
医療相談アプリで取得した「問診情報等」がオンライン診療システムで閲覧可能となる	オンライン診療システムから該当患者の「診療記録」が照会される	該当患者の「診療記録」がオンライン診療システムに表示される	「診察結果」がｃ病院に保存される*
【データ種類】 子ども氏名（カナ含む）、生年月日、性別、住所、電話番号、保険証情報、体温、病状、治療中の病気、服用薬	【データ種類】 保険証番号、子ども氏名（カナ含む）、生年月日	【データ種類】 保険証番号、子ども氏名（カナ含む）、生年月日、診療情報（病歴、手術歴、検査記録）、薬歴、予防接種歴、障害情報、アレルギー	【データ種類】 保険証番号、子ども氏名（カナ含む）、生年月日、診察結果 *診察結果はかかりつけ医の勤務する病院にのみ登録される

パーソナルデータ連携基盤
(つくばスマートシティ協議会運営)

基盤にデータは保管されない

診療記録

a病院
（皮膚科）
※皮膚炎で受診実績あり

b病院
（内科）
※cの休診日に受診

c病院
（小児科）
※いつもかかる病院

「診療が完結した日」から５年後に削除可能

子ども(患者)のかかりつけの病院･施設

*ISMAP対応とは･･･政府が求めるセキュリティ要求を満たしているクラウドサービスとして評価･登録されたもの

*オプトインとは･･･サービス利用前に同意して参加すること

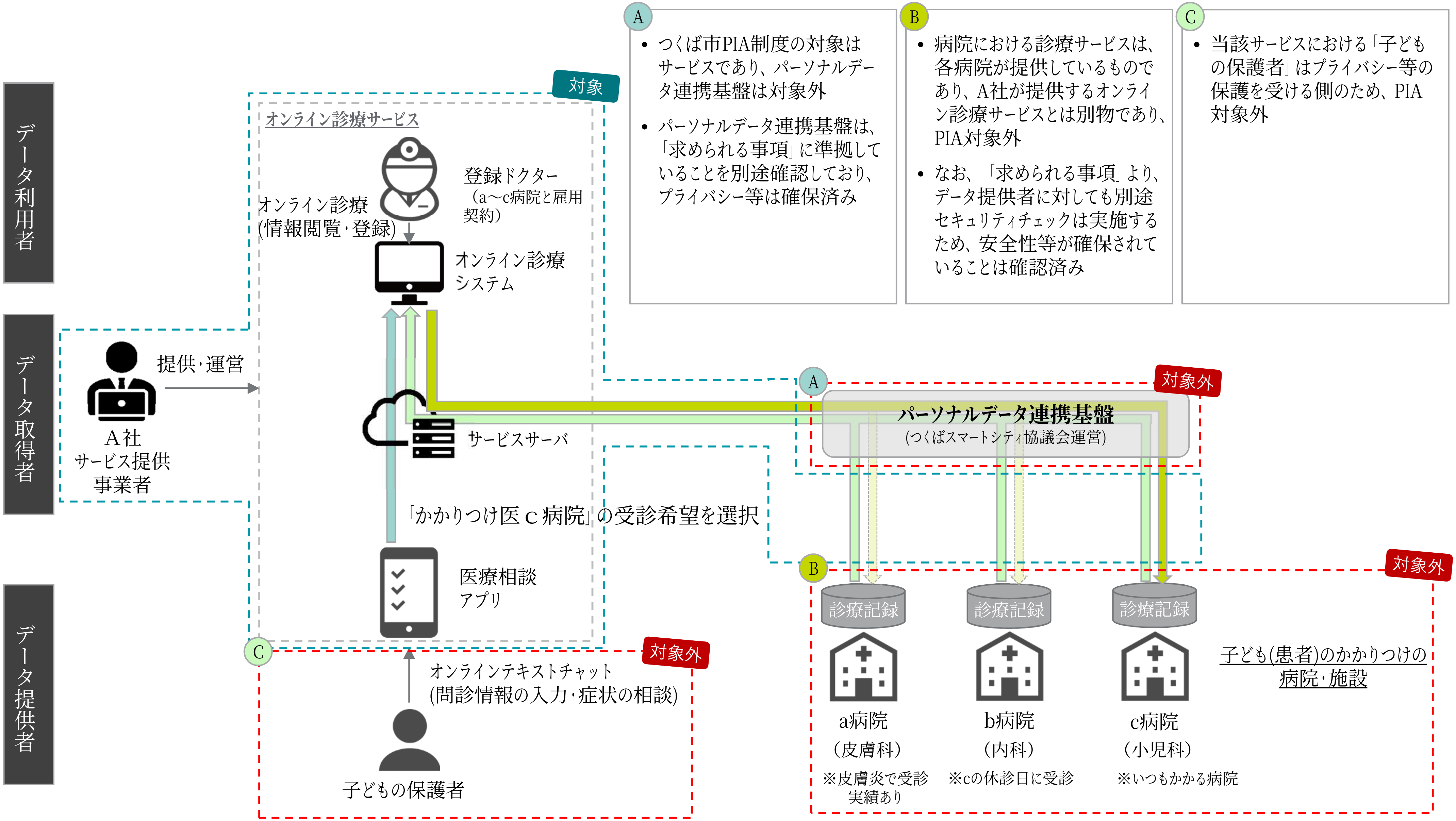
※ 民間事業者が検討するサービスを参考に、懇話会での議論用に市がサービス内容を設定したもので、実際の事業者のサービスを示すものではありません。
※ 懇話会での議論用に市でサービス内容を簡素化、一部加工しています。実際の事業実施にあたっては関係法令を踏まえ事業が実施されます。

議題１　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

資料2

＜PIAの評価対象範囲＞

- オンライン診療サービス及び、サービスを提供している事業者A社
- オンライン診療サービスと各病院間のデータ連携



A
- つくば市PIA制度の対象はサービスであり、パーソナルデータ連携基盤は対象外
- パーソナルデータ連携基盤は、「求められる事項」に準拠していることを別途確認しており、プライバシー等は確保済み

B
- 病院における診療サービスは、各病院が提供しているものであり、A社が提供するオンライン診療サービスとは別物であり、PIA対象外
- なお、「求められる事項」より、データ提供者に対しても別途セキュリティチェックは実施するため、安全性等が確保されていることは確認済み

C
- 当該サービスにおける「子どもの保護者」はプライバシー等の保護を受ける側のため、PIA対象外

※　民間事業者が検討するサービスを参考に、懇話会での議論用に市がサービス内容を設定したもので、実際の事業者のサービスを示すものではありません。
※　懇話会での議論用に市でサービス内容を簡素化、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を踏まえ事業が実施されます。

議題１　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

資料2

＜PIA実施結果（影響度）＞

- 今回のサービスで使用するプライバシーデータを「影響度」の判定表に当てはめた結果は下表のとおり
- 「アレルギー情報」といった身体に直接影響を及ぼす可能性がある情報や、「病歴」といった配慮を要する情報など、機微度の高い情報を取り扱うことから、影響度としては「４」と評価された

影響度の評価	4	• オンライン診療にあたり、利用者(患者)にとって情報漏洩等した場合に、心身への影響が甚大な個人に関する情報を取扱う

「財産への影響」　高い ↑ ↓ 低い

レベル	取扱情報の詳細			
4				
3				
2		住所、生年月日、性別、電話番号、健康保険証番号、健康保険証情報	健康診断結果、病歴、手術歴、看護記録、身体検査記録、レセプト情報、身体／知的障害情報、薬歴、予防接種歴	持病、保有感染症、カルテ（エックス線写真も含む）、精神障害情報、アレルギー
1		体温		
	1	2	3	4

低い ←→ 高い

「心身への影響」

参考：JNSA「JOモデル」、JISX9251（ISO/IEC29134）

議題１　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

資料2

＜PIA実施結果（起こりやすさ）＞

- 今回のサービス内容について「PIA調査シート」（別添１）により確認した結果は下表のとおり
- プライバシーデータの「取得・利用・保管・廃棄」の過程において、想定されるリスクに対して取り得る措置が講じられていることが確認できたことから、起こりやすさとしては「１」と評価した

起こりやすさの評価	1	・個人情報の取扱いは国内に限定されており、日本の個人情報保護法に準拠している ・サービス提供事業者はPマークの取得、委託先であるサービスサーバはISMAP対応しており、十分に安全管理措置を講じている ・同意の取得、不正利用の防止、問合せ窓口の設置など、利用者保護の措置が十分とられている

#	評価項目	事業者の回答	評価	起こりやすさ
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	提供・共有する。第三者へ提供する前に同意取得する	実施している	1
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	アプリ上で、サービス利用開始前に本人へ通知し、同意取得する	実施している	1
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	ユーザ情報・問診情報はアプリ上で本人にて削除可能である	実施している	1
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。	プライバシーポリシーに窓口を公表しており、電話・メールによる問合せが可能である	実施している	1
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	クラウドサーバはISMAPの要求事項を満たしており、対策は十分に講じている	実施している	1
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。	クラウドサーバはISMAPの要求事項を満たしており、対策は十分に講じている。医師・サービス提供事業者は盗難対策・入退室管理・外部デバイスの接続制限など情報漏洩対策を徹底している	実施している	1
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	クラウドサーバはISMAPの要求事項を満たしており、対策は十分に講じている。オンライン診療システム・アプリはログオン時の二要素認証の導入・複数回認証失敗時のロックアウト・適切なアサイン権限管理など不正アクセス対策を徹底している	実施している	1
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。	オンライン診療システム・アプリは、個人情報の編集可能なアクセス権者を最小限に設定した上で、変更時に変更用パスワードを必須としている	実施している	1

資料2

＜PIA実施結果（起こりやすさ）＞

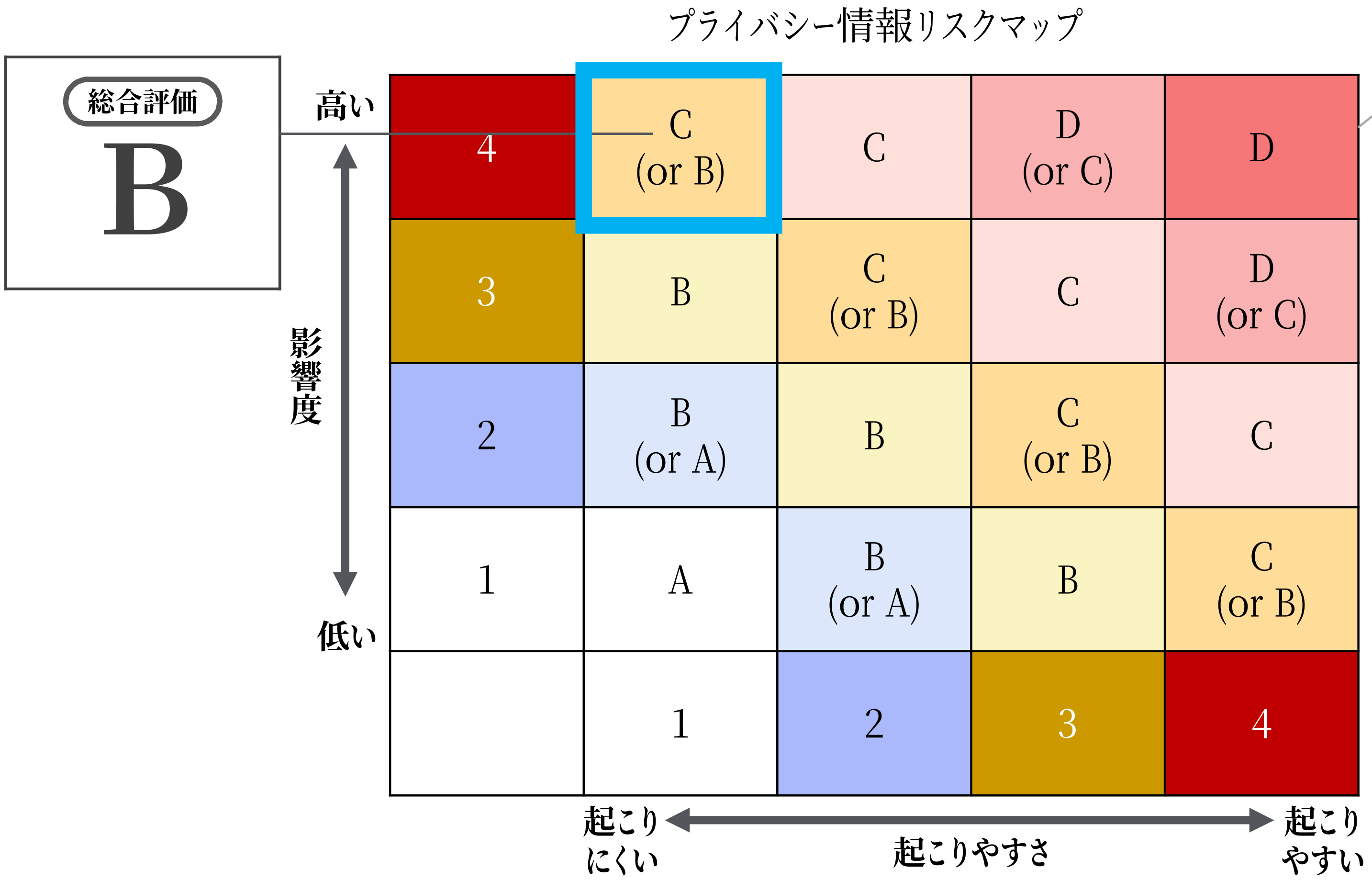
#	評価項目	事業者の回答	評価	起こりやすさ
15	個人に関する情報の過剰収集が発生しないか	オンライン診療・決済に必要な情報に限定し、収集している	実施している	1
16	個人に関する情報の処理目的に関する情報が不十分でないか。利用者にわかりやすく説明しているか	オンライン診療アプリのメニューから処理目的に関する情報ページを呼び出し、表示することが可能である	実施している	1
17	個人に関する情報の不必要な長期保有が発生しないか。	データの保管期間を定めた上で、適切な方法で廃棄している	実施している	1
18	サービスを提供することにより不利益を被る住民がいないか、不当な扱いを受けることがないか	本サービスにより、不利益を被る・不当な扱いを受ける住民はいない	実施している	1
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。	クラウドサーバはISMAPの要求事項を満たしており、対策は十分に講じている。サービス提供事業者はファイアウォール、アンチウイルスソフトの導入に加え、セキュリティパッチの即時適用、24時間365日の保守運用体制の導入など、予防・被害を最小化する対策を講じている	実施している	1
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	クラウドサーバはISMAPの要求事項を満たしており、対策は十分に講じている。サービス提供事業者は24時間365日の保守運用体制の導入、情報システム・セキュリティに関する内部監査を年１回以上実施している	実施している	1
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。	医師は「オンライン診療の適切な実施に関する指針」より、厚生労働省が指定する研修を受けている。サービス提供事業者は社内の研修計画に基づき、教育を実施している	実施している	1
22	目的外利用が発生しないか	目的外利用は発生しない • サービス提供事業者は利用目的を明確にした上で、個人情報を取扱っている。データの持ち出し制限に加え、イベントログの監視等しており、不正な操作が行われないように取り組んでいる • 委託先の契約・医師との雇用契約にて、個人情報の種類・利用目的等は明記し、目的外の利用・第三者への無断提供をしない旨を定め、締結している • クラウドサーバ：利用契約において秘密の保持を定めている。ISMAPの要求事項を満たした安全管理対策が取られている。	実施している	1

議題１　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

資料2

＜本サービスに対するPIAの総合評価＞

- オンライン医療サービスの提供にあたり、個人に関するセンシティブな情報を取扱うため、影響度は「４」となる一方、十分なプライバシー対策が講じられているため、起こりやすさは「１」の評価
- 影響度と起こりやすさの評価結果を「プライバシー情報リスクマップ」に当てはめると「C (or B)」となるが、今回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：リスク小**」と評価しました



プライバシー情報リスクマップ

総合評価

B

影響度				
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

前年度のリスクマップから見直しを実施しております。

議題１では当該ユースケースに対する評価結果としての妥当性について、リスクマップの妥当性については議題２でご説明の上、ご意見頂戴できればと存じます

【凡例】

A：リスク微小
（想定されるリスクは極めて少ないが、ゼロリスクではないことを理解のうえ判断）

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）

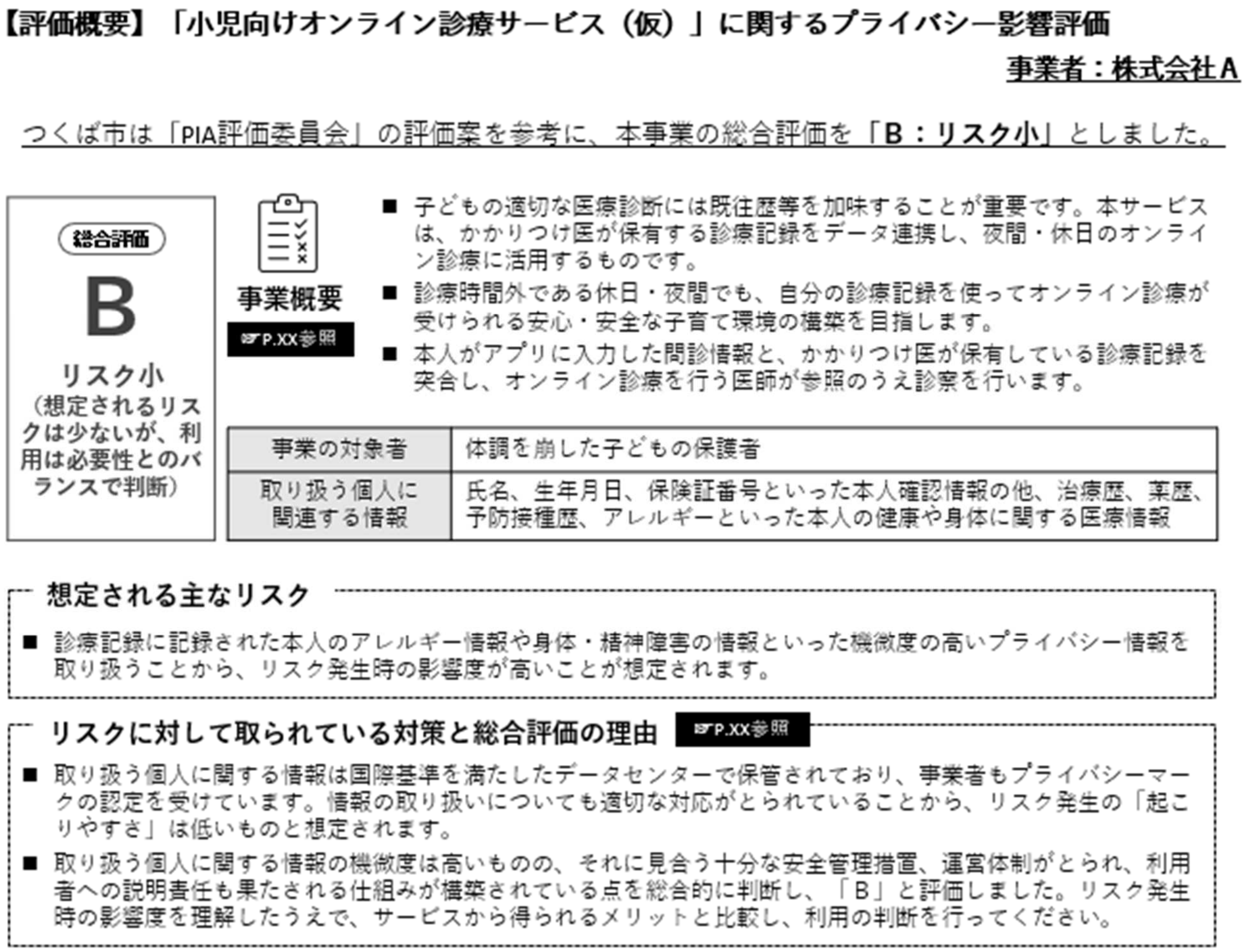
C：リスク中
（中程度のリスクがあることを十分理解のうえ、利用を慎重に判断）

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）

議題１　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

資料2

＜本サービスに対するPIA評価報告書（概要版）のイメージ＞　別添２参照



【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

☞P.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　☞P.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。

資料３

議題２　前年度からの継続論点の整理について

- 「中間とりまとめ」で示した主要論点における「今後整理すべき事項と整理に当たってのポイント」（以下、「継続論点」という）について、事務局で16項目に分類し方向性を検討した。　（別添３）
- 16の継続論点のうち、特に「評価項目」・「評価基準」・「評価体制」について、行政／民間サービスの別で違いが生じるか否か議論が必要

#	分類	継続論点	本日の協議対象
1	用語の定義	個人関連情報のうちどこまでを対象とするのか	－
2		個人情報保護法の定義と「センシティブ情報」・「プライバシー情報」との関係性の精査の上、含むべき事項がないか	－
3		PIAを適用する対象(初期評価基準)をどのように定めるか	－
4	実施のタイミング	再評価実施のタイミングはどの段階が適切か	－
5		「大幅なシステム改修」はどの程度で必要と見なすのか	－
6	評価項目	民間ユースケースにおけるチェック項目の違い	対象
7	評価基準	市民にとって安心を得られる基準かどうか	対象
8		民間ユースケースの場合に当該基準を使うことの齟齬がないかどうか	対象
9	評価体制	民間サービスを対象とした場合のPIAの実効性を担保するために体制構築に当たり留意すべき点	対象
10		PIAはあくまでリスクを可視化し、可能な限り是正を求める手段であり、漏洩の責任は事業者にあると整理するかどうか	－
11		PIA制度の実効性を担保するため、運用面で協定・規約を整備する形でよいか。法的拘束力を有する条例ではなく、内規であるつくば市の要綱により制度化し、つくばスマートシティ協議会との協定の下、データ連携基盤利用規約でPIAの実効体制を確保する	－
12		評価を踏まえた対応をどのレベルまで行うべきか(各評価結果の評価後の対応はどうすべきか、D評価でもサービスリリースできるようにするのか、D評価の場合は基盤に接続させないのか 等)	－
13		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どう対処するか	－
14		PIA制度の適切な運用をモニタリングするため、年に１度程度つくば市から(仮)評価委員会に制度の運用状況を報告するとともに、個人情報保護法の改正等のタイミングに合わせて必要な見直しを行う形でよいか	－
15		制度的にはパブコメの対象ではなく、パブコメには時間を要し、サービスリリースが大幅に遅れることになるため、評価委員会において市民が参画することで市民の意見を反映させる形でよいか	－
16	公表	市民にわかりやすく伝えるための公表様式、公表方法	－

議題２　前年度からの継続論点の整理について（＃６評価項目）

＜論点＞ 民間ユースケースにおけるチェック項目の違い

＜PIA実施結果＞

- 今回、民間事業者が民間データを活用してサービス提供を行うユースケース[*1]に基づきPIAを実施した結果、現行の評価項目にて項目の過不足や回答できない等の問題はなく、民間特有の論点・懸念[*2]は見つからなかった
- 一方、具体的なユースケースに基づき、評価項目を記入した過程で、「評価項目」の使い勝手・構成等において見直した方がよい点が見つかった

＜評価項目の見直し＞

- 今回の見直しでは、内容に関する大幅な変更はしておらず、申請者の目線で回答しやすい、負荷のかからない評価項目へと見直しを実施　（別添４「評価項目　新旧対照表」）

Ⅰ. 現行の評価項目の記載では不十分であり、事業者が回答する際に迷う点が見つかったため、評価項目の追記・修正を実施（No.3, 13-④, 17, 19-①[*3]）

Ⅱ. ルールの運用に関する観点から、評価項目の修正を実施（No.11-⑤, 12-⑥⑦⑧⑨, 13-⑥, 14-③, 18-③[*3]）

Ⅲ. 確認の必要がないと考えられる項目が含まれていたため、項目の削除を実施（No.18-④[*3]）

Ⅳ. 評価項目間で要件が重複していたため、項目の統廃合を実施（No.13-①②, 14-①②, 16-①②, 17-③④[*3]）

[*1] サービス提供にあたり、行政の関与及び、行政が取得したデータ活用はない、民間事業者のみで構成され、民間事業者が取得したデータのみを活用したユースケース

[*2] 前年度の懇話会において、行政・民間における第三者提供・同意取得等における差異に関するご意見を頂戴し、評価項目への反映は実施済み。今回のユースケースにおいて反映版の評価項目を用いてPIA実施したが、民間特有の懸念は見つからなかった

[*3] 修正前の番号を記載

資料３

議題２　前年度からの継続論点の整理について（＃７、８評価基準）

＜論点＞
- 市民にとって安心を得られる基準かどうか
- 民間ユースケースの場合に当該基準を使うことの齟齬がないかどうか

＜PIA実施結果＞

- 評価項目同様、民間事業者が民間データを活用してサービス提供を行うユースケースに基づきPIAを実施した結果、現行の評価基準にて問題なく、評価結果を導くことができ、民間特有の論点・懸念は見つからなかった
- 一方、具体的なユースケースに基づき、評価した結果、評価項目の内容を考慮せず、機械的にリスク算出している点やリスクマップの考え方・文言に改善点が見つかった

＜評価基準の見直し＞

Ⅰ. 「個人情報の取扱い」に関する項目が評価対象外となっていたが、評価対象に変更（No.07-10）

Ⅱ. すべての評価項目を一律判定し、リスクを算出しているが、必須・推奨を振り分けた上で、リスクの算出方法を見直し

Ⅲ. 自由記述の項目がリスク算出に影響しない仕組みになっているが、代替措置を講じている場合はリスク算出に組み込むように見直し

Ⅳ. 事業者による努力により、起こりやすさは低減できるため、従前のリスクマップの基準より柔軟に評価できるよう見直し

＜協議ポイント＞

1.　見直しⅡについて、以下見直しを行ったが、妥当か
    - 「個人情報保護法*4」を参考に「必須/推奨」の観点を追加し、
        - ✓ 必須は従前どおり、１つでも実施できていない場合は「４」
        - ✓ 推奨はリスクの積み上げとし、１つ実施していない毎に「＋１」

No.	評価項目	対応状況の判定	必須/推奨	起こりやすさ
x	xxxx	－	－	2
	xxxx	実施している	必須	
	xxxx	実施している	必須	
	xxxx	実施している	必須	
	xxxx	実施している	推奨	
	xxxx	実施していない	推奨	
	xxxx	－	－	

↑ 新規追加　　↑ 算出方法見直し

---

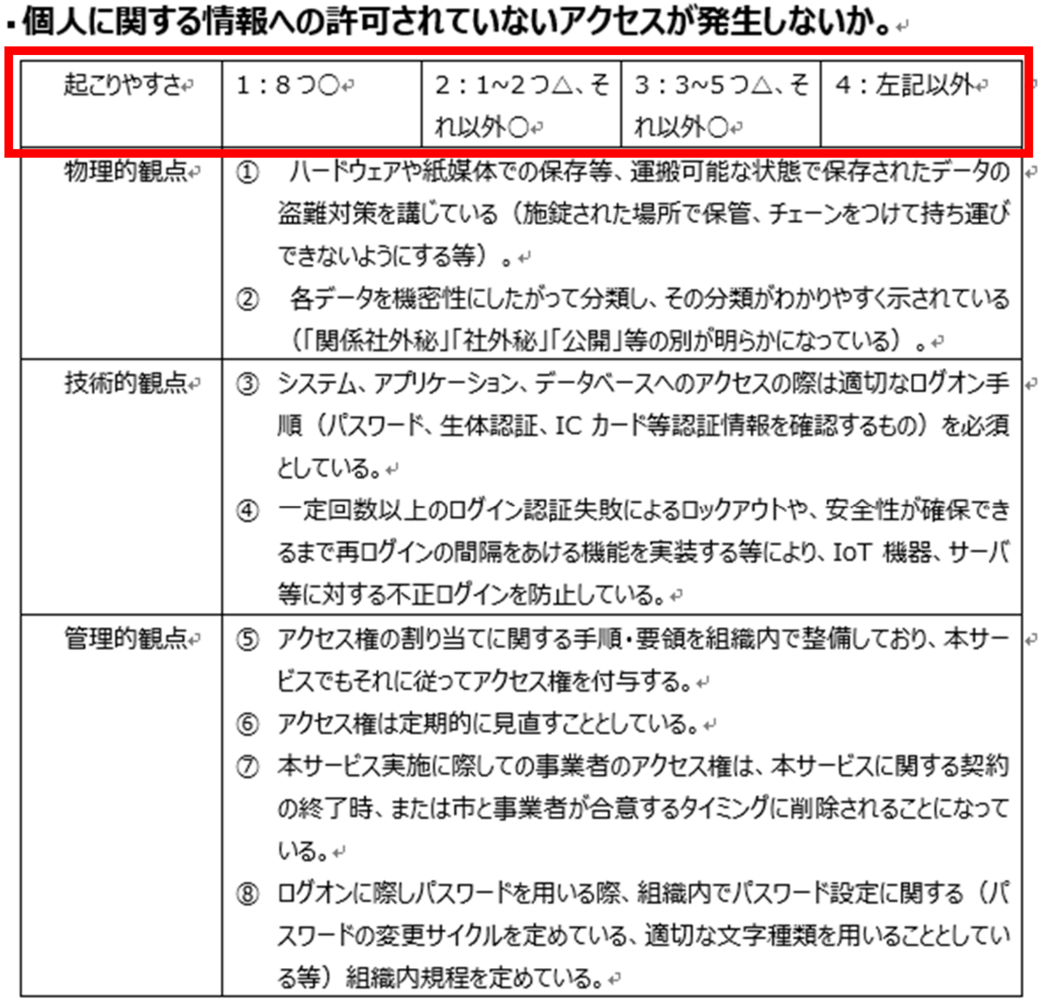
*4 厳密には、「個人情報の保護に関する法律についてのガイドライン(通則編)」も参考にし、必須/推奨を振り分け

資料３

【問題点】　「起こりやすさ」の評価を対応割合に応じて機械的に判定する仕組み

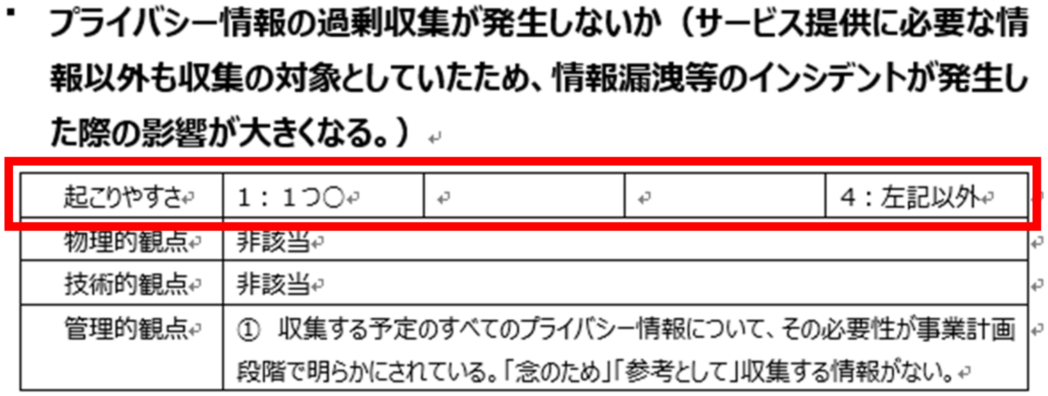
- 「起こりやすさ」の評価が、評価項目別に確認すべき物理的･技術的･管理的観点への対応割合に応じて機械的に判定される仕組みだが、この場合、確認すべき観点の数に左右されやすく、極端な評価になるケースがある

＜具体的なケース＞



▪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。

起こりやすさ	1：8つ○	2：1~2つ△、それ以外○	3：3~5つ△、それ以外○	4：左記以外
物理的観点	①　ハードウェアや紙媒体での保存等、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）。 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）。			
技術的観点	③ 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。 ④ 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。			
管理的観点	⑤ 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。 ⑥ アクセス権は定期的に見直すこととしている。 ⑦ 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。 ⑧ 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）組織内規程を定めている。			



▪　プライバシー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。）

起こりやすさ	1：１つ○			4：左記以外
物理的観点	非該当			
技術的観点	非該当			
管理的観点	①　収集する予定のすべてのプライバシー情報について、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。			

左の評価項目の場合は、確認すべき観点が８個あるのに対して、
右の評価項目の場合では、確認すべき観点が１個しかなく、
対応しているか否かで「起こりやすさ」の評価が「１」もしくは
「４」かの両極端な評価となってしまう

資料３

議題２　前年度からの継続論点の整理について（＃７、８評価基準）

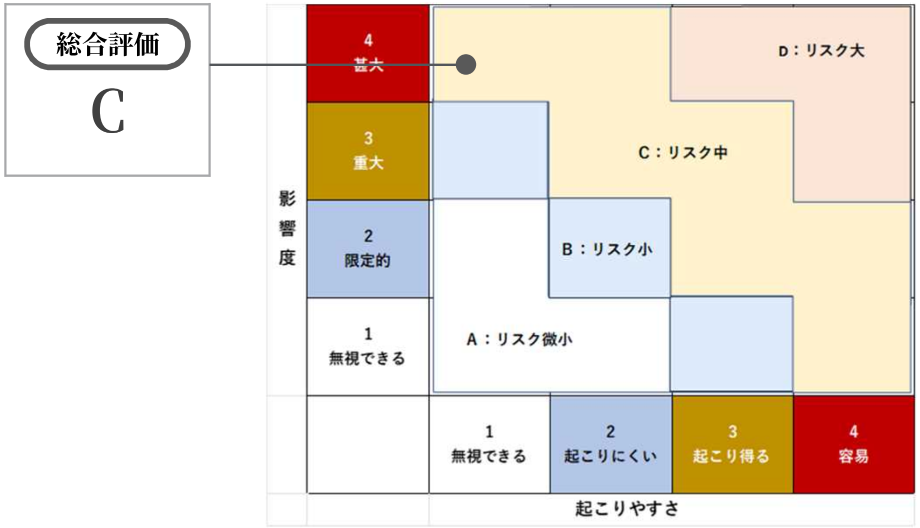
＜論点＞
- 市民にとって安心を得られる基準かどうか
- 民間ユースケースの場合に当該基準を使うことの齟齬がないかどうか

＜協議ポイント＞

2. 従前の４段階のリスクマップから、７段階のリスクマップに見直しを行ったが、妥当か
   - 事業者が努力してもリスク低減できないと、「事業者の参入障壁」・「サービス利用を敬遠する市民が出てくる」可能性を懸念
   - 当該リスクマップを策定する際に参考にした、JISX9251のリスクマップの考え方は段階設定に幅を持たせることを許容
   - 従前のリスクマップの基準を基本線にしつつ、例外的にリスクを上げ下げできる余地を残すことで柔軟な基準へと見直し

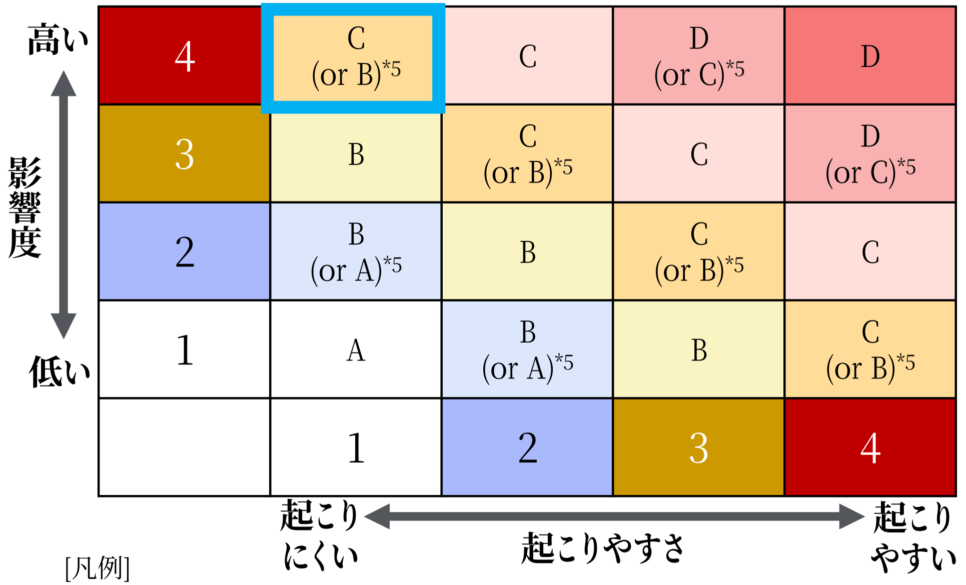
＜ユースケースの評価結果＞

従前のリスクマップ



見直し後のリスクマップ

[*5] 原則は表記のリスクとなるが、十分な対策を講じている場合、市の判断のもと括弧内のリスクに下げる余地あり



影響度					
高い	4	C (or B)[*5]	C	D (or C)[*5]	D
	3	B	C (or B)[*5]	C	D (or C)[*5]
	2	B (or A)[*5]	B	C (or B)[*5]	C
低い	1	A	B (or A)[*5]	B	C (or B)[*5]
		1	2	3	4
		起こりにくい	起こりやすさ		起こりやすい

[凡例]
A：リスク微小（想定されるリスクは極めて少ないが、ゼロリスクではないことを理解のうえ判断）
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）
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）
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）

資料３

議題２　前年度からの継続論点の整理について（＃９評価体制）

＜**論点**＞　民間サービスを対象とした場合のPIAの実効性を担保するために体制構築に当たり留意すべき点

＜PIA実施結果＞

- 民間事業者が民間データを活用してサービス提供を行うユースケースに基づきPIA実施した結果、民間特有の懸念として、市が民間事業者・民間サービスに対して、例えば、起こりやすさは「無視できる」とお墨付きを与えてしまうことは事業者に悪用される、市民に誤解を与えるリスクがあるため、評価結果の見せ方は気を付ける必要がある
- また、PIA実効性を阻害するリスクとして想定されるのは、「評価される側」である“サービス提供事業者”と考えられる
- サービス提供事業者に実効性を阻害されないために、①市と協議会の間で締結する「協定書」と、②協議会が定めるデータ連携基盤の利用規約上に必要な措置を規定し、遵守させる対応策が考えられる

＜対応案＞

- 評価結果の見せ方として、前述のリスクマップでも触れたが、「影響度」・「起こりやすさ」の文言について誤解を与えないように、それぞれ「影響度：高い⇔低い」「起こりやすさ：起こりやすい⇔起こりにくい」という程度を示すにとどめ、「１　無視できる」、「４　甚大」といった各段階ごとの評価を示す用語はつけない形に見直し
- 「PIA評価報告書概要版」の記載においても、上記を踏まえ、リスクが無いように見えないように書きぶりを修正

資料３

議題２　前年度からの継続論点の整理について（＃９評価体制）

＜**論点**＞　民間サービスを対象とした場合のPIAの実効性を担保するために体制構築に当たり留意すべき点

＜対応案＞

①市と協議会の間で締結する協定書に含める内容（案）

- 市が定める要綱に基づき、サービス提供事業者に対し、市がPIAを実施する。
- 協議会は、プライバシーデータ連携基盤の利用申請があった場合は、速やかに市に通知する。
- 市は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。
- 協議会は、市が実施するPIAの結果、その他の両者の協議により定める基準に基づき、パーソナルデータ連携基盤の利用の可否を決定する。　等

②サービス提供事業者向けの利用規約に含める要件（案）

- つくば市が定める要綱に基づき、つくば市のPIAを受ける。
- サービス提供事業者はPIAの結果に応じてプライバシー情報の適正な取扱い等の改善策を講じる。
- 協議会はPIAの実施にあたってサービス事業提供者から提供された情報に虚偽が含まれていたことが判明した場合は、データ連携基盤の利用を停止する。
- PIAを受けたサービスに大幅な変更が生じた場合は、サービス提供事業者はPIA評価の再申請を申し出る。　等

＜協議ポイント＞

- 評価結果についてリスクがないような誤解を与えないためにも、リスクマップの文言を修正するとともに、公表物であるPIA評価報告書において書きぶりを見直したが、内容について懸念等ないかご意見頂戴したい
- PIAの実効性を阻害されない観点から、市と協議会の間で締結する「協定書」と、協議会が定める利用規約に含める事項案を整理したが、内容について懸念等ないかご意見頂戴したい

別添１

様式第６号（A4横）

提出日：令和●年（20**年）●月●日
サービス提供事業者名：株式会社Ａ

（仮）プライバシー影響評価委員会　御中

つくば市

PIA事務局一次評価シート

つくば市は、株式会社Ａが申請した「小児向けオンライン診療サービス（仮）」事業について、PIA一次評価を以下のとおり実施しました。

※ 当該ユースケースは、民間事業者が検討するサービスを参考に、懇話会での議論用に市がサービス内容を設定したもので、実際の事業者のサービスを示すものではありません。

※ 懇話会での議論用に市でサービス内容を簡素化、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を踏まえ事業が実施されます。

■一次評価結果（自動算出のため入力不要）

影響度	起こりやすさ
4	1

■影響度

影響度（運用マニュアル別紙2を参照し、判定すること）	取り扱う個人に関する情報の種類と具体的な内容
4	別紙のとおり

■起こりやすさ

No.	調査項目概要（概要、及び盛り込むべき要素や詳細）	事業者による回答、及びヒアリング結果	関連する添付書類名・ページ番号	事業者による自己評価	つくば市による起こりやすさ各観点の判定	実施の必須/推奨	起こりやすさ※自動判定につき入力不要	つくば市から（仮）プライバシー影響評価委員会への申し送り事項
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）	入力不要	入力不要	入力不要	入力不要	ー	入力不要	
	①本サービスの目的及び内容	かかりつけ医の診療時間外である休日・夜間でも、自分の診療情報を使って、安心・安全なオンライン診療が受けられる医療サービス		入力不要	入力不要	ー	入力不要	
	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	（利用者）オンライン診療アプリ、（医師）オンライン診療システム、（医療機関）電子カルテ、（データセンター）ISMAP対応サービスサーバー		入力不要	入力不要	ー	入力不要	
	③本サービスで期待される効果	子どもの適切な診断には既往歴等を加味することが重要だが、現状の夜間・休日のオンライン診療では問診のみの情報で診察している。本サービスによりかかりつけ医が保有する診療録をデータ連携することで、安心・安全な夜間・休日のオンライン診療サービスを提供する。		入力不要	入力不要	ー	入力不要	

No.	調査項目概要（概要、及び盛り込むべき要素や詳細）	事業者による回答、及びヒアリング結果	関連する添付書類名・ページ番号	事業者による自己評価	つくば市による起こりやすさ各観点の判定	実施の必須/推奨	起こりやすさ※自動判定につき入力不要	つくば市から（仮）プライバシー影響評価委員会への申し送り事項
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）	入力不要	入力不要	入力不要	入力不要	－	入力不要	
	①サービス提供事業者の概要	サービス提供事業者Ａ社		入力不要	入力不要	－	入力不要	
	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	Ｐマーク取得		入力不要	入力不要	－	入力不要	
	③本サービスの責任者及び従事者			入力不要	入力不要	－	入力不要	
	④リスク管理責任者、セキュリティ責任者			入力不要	入力不要	－	入力不要	
	⑤委託先	データセンター		入力不要	入力不要	－	入力不要	
	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）	医師、病院		入力不要	入力不要	－	入力不要	
	⑦サービスを提供される主体	休日・夜間に体調を崩した利用者（患者）及び保護者		入力不要	入力不要	－	入力不要	
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、	オンライン診療の適切な実施に関する指針（厚生労働省）		入力不要	入力不要	－	入力不要	
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）	別紙のとおり		入力不要	入力不要	－	入力不要	
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。）	入力不要	入力不要	入力不要	入力不要	－	入力不要	
	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	別紙のとおり		入力不要	入力不要	－	入力不要	
	②処理担当者			入力不要	入力不要	－	入力不要	
	③各段階において取り扱うデータの内容	別紙のとおり		入力不要	入力不要	－	入力不要	
	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。）	別紙のとおり		入力不要	入力不要	－	入力不要	
	⑤データを用い作業する場所	・サービス提供事業者A社においてセキュリティポリシーに基づき安全管理対策が取られた場所で作業を実施している。 ・医師がオンライン診療を行う場所は「物理的に外部から隔離される空間」で行うことがガイドラインに定められている		入力不要	入力不要	－	入力不要	
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。）	入力不要	入力不要	入力不要	入力不要	－	入力不要	
	①住所	日本国内		入力不要	入力不要	－	入力不要	
	②当該部屋の階			入力不要	入力不要	－	入力不要	
	③当該建物の構造	免震構造		入力不要	入力不要	－	入力不要	
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。※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）。	病院（かかりつけ医）が保有する診療録を、データ連携基盤を通じてサービス提供事業者Ａ社で参照可能にする部分及びオンライン診療の結果をサービス提供事業者Ａ社から病院へ提供する部分が該当 同意取得の有無：診療前相談（医師）のタイミングで、患者側で選択		○：実施している	○：実施している	必須	1	

別添1

No.	調査項目概要（概要、及び盛り込むべき要素や詳細）	事業者による回答、及びヒアリング結果	関連する添付書類名・ページ番号	事業者による自己評価	つくば市による起こりやすさ各観点の判定	実施の必須/推奨	起こりやすさ※自動判定につき入力不要	つくば市から（仮）プライバシー影響評価委員会への申し送り事項
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。 ※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）。	サービス利用開始時：入力した問診情報の利用について、アプリ側で説明表示、同意取得 診療前相談時：かかりつけ医側の診療録の利用について医師が診療前相談時に同意取得		○：実施している	○：実施している	必須	1	
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。）	アプリサービスのユーザー登録情報、問診情報の削除申請はアプリ上で実施可能（サービスの利用停止） 診療結果については５年保存の法定義務があり不可		○：実施している	○：実施している	必須	1	
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。	サービス提供事業者Ａ社が定めるプライバシーポリシーに窓口情報を掲載している。電話及びメールで問合せが可能		○：実施している	○：実施している	必須	1	
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。）	入力不要	入力不要	入力不要	入力不要	－	1	
	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）。	データセンター：ISMAPの要求事項を満たしている		○：実施している	○：実施している	推奨		
	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。	データセンター：ISMAPの要求事項を満たしている		○：実施している	○：実施している	推奨		
	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。	データセンター：ISMAPの要求事項を満たしている		○：実施している	○：実施している	必須		
	④重要な機器やネットワークを冗長化している。	データセンター：ISMAPの要求事項を満たしている		○：実施している	○：実施している	推奨		
	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。	・サービス提供事業者A社で社内規程を定めており、対策を講じている。 ・オンライン診療を行う医師との雇用契約に定めており、対策を講じていることを確認している		○：実施している	○：実施している	推奨		
	その他、対策している内容（自由記述）			入力不要	入力不要	－		

No.	調査項目概要（概要、及び盛り込むべき要素や詳細）	事業者による回答、及びヒアリング結果	関連する添付書類名・ページ番号	事業者による自己評価	つくば市による起こりやすさ各観点の判定	実施の必須/推奨	起こりやすさ※自動判定につき入力不要	つくば市から（仮）プライバシー影響評価委員会への申し送り事項
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。	入力不要	入力不要	入力不要	入力不要	—	1	
	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）。	データセンター：ISMAPの要求事項を満たしている オンライン診療システム：オンライン診療システムを利用するPCはワイヤーロックで固定している。診療結果を紙出力した場合は、個人別ファイルに収納し、施錠されたロッカーで保管している 医療相談アプリ：使用時にユーザー認証を必要とする 保守管理事業者：事業者が定めるセキュリティポリシーに基づき必要な安全管理対策が取られている		○：実施している	○：実施している	必須		
	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）。	データの機密性に基づいて分類のうえ、個人情報の該当有無を表示している				推奨		
	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。	データセンター：ISMAPの要求事項を満たしている 保守管理事業者：入館証によって入退室管理がされている 医師：勤務先の病院からの場合は病院側で管理されている。自宅からの場合は入退室管理は行っていないが、ガイドラインに従い自宅等「物理的に外部から隔離される空間」で実施している		○：実施している	○：実施している	必須		
	④デバイスや記録媒体の接続制限がある。	サービス提供事業者A社：社内規程で制限されており、実施していることを確認している データセンター：ISMAPの要求事項を満たしている 医師：オンライン診療システムへのデバイスや記憶媒体の接続は原則禁止されている		○：実施している	○：実施している	推奨		
	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。	サービス提供事業者A社：社内規程に基づき管理されており、実施していることを確認している データセンター：ISMAPの要求事項を満たしている 医師：オンライン診療の場所は「物理的に外部から隔離される空間」で行うことがガイドラインに定められている		○：実施している	○：実施している	推奨		
	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。	サービス提供事業者A社：社内規程に基づき管理されており、実施していることを確認している データセンター：ISMAPの要求事項を満たしている 医師：医師は基本的に貸与PCを使用するが、BYODでのオンライン診療システムの使用は禁止していない。		○：実施している	○：実施している	推奨		
	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）。	サービス提供事業者A社：社内規程に定めがあり、遵守されている データセンター：ISMAPの要求事項を満たしている 医師：雇用契約に定めがあり、遵守されている		○：実施している	○：実施している	必須		
	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。	サービス提供事業者A社：社内規程に定めがあり、遵守されている データセンター：ISMAPの要求事項を満たしている 医師：雇用契約に定めがあり、遵守されている		○：実施している	○：実施している	推奨		
	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。	サービス提供事業者A社：社内規程に定めがあり、遵守されている データセンター：ISMAPの要求事項を満たしている 医師：雇用契約に定めがあり、遵守されている		○：実施している	○：実施している	必須		
	その他、対策している内容（自由記述）			入力不要	入力不要	—		

No.	調査項目概要（概要、及び盛り込むべき要素や詳細）	事業者による回答、及びヒアリング結果	関連する添付書類名・ページ番号	事業者による自己評価	つくば市による起こりやすさ各観点の判定	実施の必須/推奨	起こりやすさ※自動判定につき入力不要	つくば市から（仮）プライバシー影響評価委員会への申し送り事項
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。	入力不要	入力不要	入力不要	入力不要	－	1	
	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。	データセンター：ISMAPの要求事項を満たしている オンライン診療システム：ログオンはID、パスワード及びSMSへ送付するワンタイムコードを必要とする二要素認証を採用している。 医療相談アプリ：使用時にユーザー認証を必要とする		○：実施している	○：実施している	必須		
	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。	オンライン診療システム：５回以上のログイン認証失敗で一定時間の再ログインを禁止している。 医療相談アプリ：５回以上のログイン認証失敗でロックがかかり、解除手続きが必要となる		○：実施している	○：実施している	推奨		
	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。	サービス提供事業者Ａ社：医師、サービス責任者、セキュリティ責任者等の職責に応じたアクセス権が定められており、付与されている 保守管理事業者：事業者の社内規程に基づきアクセス権が付与されている				必須		
	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。	サービス提供事業者Ａ社、保守管理事業者：異動・退職等のタイミングでアクセス権の見直しを行っている		○：実施している	○：実施している	推奨		
	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。	契約終了時点でデータ連携基盤へのアクセス権が削除され、サービスから遮断される				推奨		
	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。	サービス提供事業者Ａ社：社内規程に基づきパスワードの変更サイクルを定め、遵守している		○：実施している	○：実施している	推奨		
	その他、対策している内容（自由記述）			入力不要	入力不要	－		
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。	入力不要	入力不要	入力不要	入力不要	－	1	
	①イベントログを取得・保持するようになっている。	データセンター：ISMAPの要求事項を満たしている オンライン診療システム：イベントログ（アクセス、操作等）を記録している 医療相談アプリ：イベントログ（アクセス、操作等）を記録している		○：実施している	○：実施している	必須		
	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。	オンライン診療システム：記録済みの診療結果を変更する場合には変更パスワードを必要とする。また、変更権限を有するアクセス権者を限定している。		○：実施している	○：実施している	推奨		
	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。	サービス提供事業者Ａ社：サービス責任者の承認・確認プロセスが定められており、遵守されている 保守管理事業者：事業者の社内規程に基づき定められており、遵守されている				推奨		
	その他、対策している内容（自由記述）			入力不要	入力不要	－		

No.	調査項目概要（概要、及び盛り込むべき要素や詳細）	事業者による回答、及びヒアリング結果	関連する添付書類名・ページ番号	事業者による自己評価	つくば市による起こりやすさ各観点の判定	実施の必須/推奨	起こりやすさ※自動判定につき入力不要	つくば市から（仮）プライバシー影響評価委員会への申し送り事項
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。）	入力不要	入力不要	入力不要	入力不要	―	1	
	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。	収集する情報は、オンライン診療に必要な情報、決済に必要な情報に限定されている		○：実施している	○：実施している	推奨		
	その他、対策している内容（自由記述）			入力不要	入力不要	―		
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。	入力不要	入力不要	入力不要	入力不要	―	1	
	①HP等で本サービスに関する情報をいつでも閲覧できる。	アプリ上のメニューから常時呼び出し、表示することができる		○：実施している	○：実施している	必須		
	②利用者向けの説明資料が用意されている。	アプリ上のメニューから常時呼び出し、表示することができる		○：実施している	○：実施している	推奨		
	その他、対策している内容（自由記述）			入力不要	入力不要	―		
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。	入力不要	入力不要	入力不要	入力不要	―	1	
	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。	サービス提供事業者Ａ社：オンライン診療システムから紙出力した診療結果は、法定保管期限を迎えた後、溶解処理で廃棄する。使用期限を迎えた業務PCについては専門業者による廃棄を行う。 病院：法定保管期限を迎えた後、病院側で不要と判断した診療録については溶解処理で廃棄する。		○：実施している	○：実施している	必須		
	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。	データセンター：ISMAPの要求事項を満たしている		○：実施している	○：実施している	必須		
	③データの廃棄期限等を明確に定めており、適切に廃棄している。	サービス提供事業者Ａ社：医療相談アプリを通じて入手した情報及び診療結果は40日後に廃棄、データ連携基盤を通じて入手した診療録については診療後に廃棄することを明記している。 病院：診療結果の保存期間は法定義務で５年間と定められているが、病状によっては後年度の再発リスク等に備える理由から、法定期間を超えて保存する必要から明確な廃棄期限は明記していない。		○：実施している	○：実施している	推奨		
	その他、対策している内容（自由記述）			入力不要	入力不要	―		
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。）	入力不要	入力不要	入力不要	入力不要	―	1	
	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。	サービス提供により不利益を被る住民はいない		○：実施している	○：実施している	必須		
	その他、対策している内容（自由記述）			入力不要	入力不要	―		

No.	調査項目概要（概要、及び盛り込むべき要素や詳細）	事業者による回答、及びヒアリング結果	関連する添付書類名・ページ番号	事業者による自己評価	つくば市による起こりやすさ各観点の判定	実施の必須/推奨	起こりやすさ※自動判定につき入力不要	つくば市から（仮）プライバシー影響評価委員会への申し送り事項
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。	入力不要	入力不要	入力不要	入力不要	－	1	
	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。	データセンター：ISMAPの要求事項を満たしている サービス提供事業者A社：ファイアウォール、セキュリティ対策ソフトを導入している		○：実施している	○：実施している	必須		
	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。	自動で適用される		○：実施している	○：実施している	必須		
	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。	サービス提供事業者A社：24時間365日対応できる体制を整えている データセンター：ISMAPの要求事項を満たしている				必須		
	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。	対応手順書が定められている		○：実施している	○：実施している	推奨		
	その他、対策している内容（自由記述）			入力不要	入力不要	－		
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。）	入力不要	入力不要	入力不要	入力不要	－	1	
	①外部との通信を常時モニタリングしている。	サービス提供事業者A社：24時間365日対応できる体制を整えている データセンター：ISMAPの要求事項を満たしている		○：実施している	○：実施している	推奨		
	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。	サービス提供事業者A社：必要なログを取得し、一定期間保存している データセンター：ISMAPの要求事項を満たしている		○：実施している	○：実施している	必須		
	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）	サービス提供事業者A社：情報の正確性は担保している データセンター：ISMAPの要求事項を満たしている		○：実施している	○：実施している	必須		
	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。	データセンター：ISMAPの要求事項を満たしている サービス提供事業者A社：年1回の監査を実施している		○：実施している	○：実施している	推奨		
	その他、対策している内容（自由記述）			入力不要	入力不要	－		
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。	入力不要	入力不要	入力不要	入力不要	－	1	
	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。	サービス提供事業者A社：社内で研修計画を定めて実施している 医師：「オンライン診療の適切な実施に関する指針（厚生労働省）」において、2020年4月以降、オンライン診療を実施する医師は厚生労働省が指定する研修を受講しなければならないことが定められている		○：実施している	○：実施している	必須		
	その他、対策している内容（自由記述）			入力不要	入力不要	－		

No.	調査項目概要（概要、及び盛り込むべき要素や詳細）	事業者による回答、及びヒアリング結果	関連する添付書類名・ページ番号	事業者による自己評価	つくば市による起こりやすさ各観点の判定	実施の必須/推奨	起こりやすさ※自動判定につき入力不要	つくば市から（仮）プライバシー影響評価委員会への申し送り事項
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）	入力不要	入力不要	入力不要	入力不要	―	1	
	①目的外利用は発生しない。	本サービス内での目的外利用は発生しない。 ・サービス提供事業者Ａ社：利用規約において取り扱う個人情報の種類と利用目的を明記し、規約の範囲外での利用・第三者への無断提供をしないことを定めている ・医師：雇用契約において秘密の保持を定めている。アクセス権を限定している。必要な研修を実施している。 ・データセンター：利用契約において秘密の保持を定めている。 ISMAPの要求事項を満たした安全管理対策が取られている。		○：実施している	○：実施している	必須		

その他、つくば市から（仮）プライバシー影響評価委員会への申し送り事項	
想定されるリスクの概要　※「影響度」「起こりやすさ」それぞれで最も高い値のついた項目について、生じる可能性のあるリスクシナリオを記載する。	

以上

別添２

【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

☞P.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

☞P.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、民間事業者が検討するサービスを参考に、懇話会での議論用に市がサービス内容を設定したもので、実際の事業者のサービスを示すものではありません。
※　懇話会での議論用に市でサービス内容を簡素化、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を踏まえ事業が実施されます。

別添２

１．評価対象となる事業の概要

事業の概要

- ■ 今回PIAの対象となったのは、かかりつけ医が保有する本人の診療記録データを活用した「（仮）小児向けオンライン診療サービス」（以降「本サービス」）です。
- ■ 本サービスは、子どものかかりつけ医の診療時間外である休日・夜間でも、子どもの診療情報を使ってオンライン診療が受けられる安心・安全な子育て環境を構築することを目的としています。

期待される効果と本事業による市民への不利益がないことの説明

- ■ 子どもの適切な診断には既往歴等を加味することが重要ですが、現状の夜間・休日のオンライン診療サービスは問診のみの情報で診察しているケースがほとんどです。
- ■ 本サービスは、子どもが普段かかっている医療機関が保有する診療記録をデータ連携させ参照可能とすることで、急な体調不良時でも安心して夜間・休日のオンライン診療が受けられるようになります。
- ■ 利用するプライバシーデータは医師がオンライン診療を行う目的のみに利用され、目的外利用はなく、不利益を受けることはありません。

本事業の関係者

- ■ 本サービスを運用するのは、株式会社Ａです。
- ■ Ａ社との利用契約に基づき、データ管理を行うのは、株式会社Ｂ（データセンター）です。
- ■ 本サービスは上記２社で運営されており、つくば市の関与、データ提供はありません。

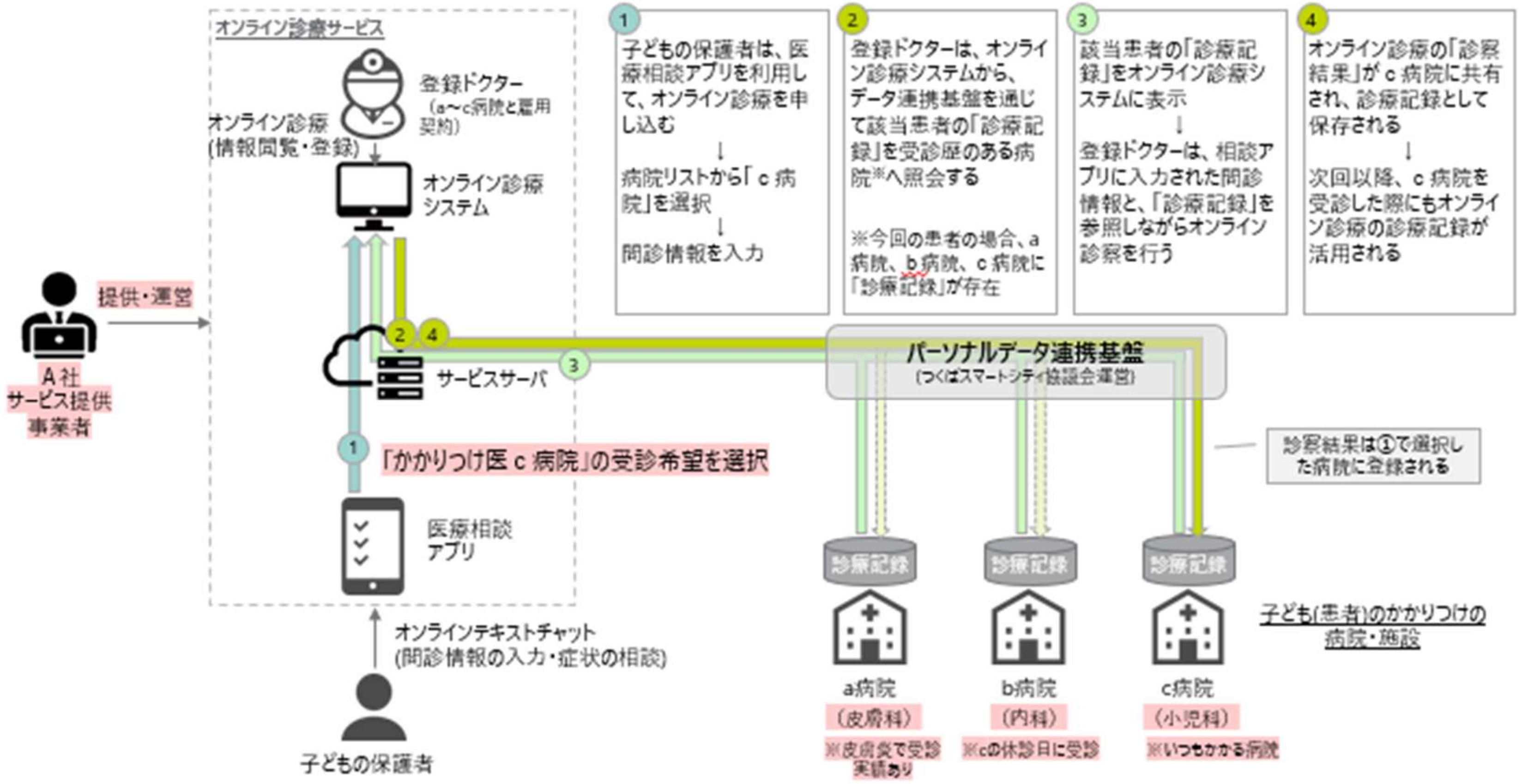
※　民間事業者が検討するサービスを参考に、懇話会での議論用に市がサービス内容を設定したもので、実際の事業者のサービスを示すものではありません。
※　懇話会での議論用に市でサービス内容を簡素化、一部加工しています。実際の事業実施にあたっては関係法令を踏まえ事業が実施されます。

発行：つくば市科学技術戦略課
サービス提供事業者：株式会社Ａ

別添２

１．評価対象となる事業の概要

業務の流れ



1
子どもの保護者は、医療相談アプリを利用して、オンライン診療を申し込む
↓
病院リストから「ｃ病院」を選択
↓
問診情報を入力

2
登録ドクターは、オンライン診療システムから、データ連携基盤を通じて該当患者の「診療記録」を受診歴のある病院※へ照会する

※今回の患者の場合、a病院、b病院、ｃ病院に「診療記録」が存在

3
該当患者の「診療記録」をオンライン診療システムに表示
↓
登録ドクターは、相談アプリに入力された問診情報と、「診療記録」を参照しながらオンライン診察を行う

4
オンライン診療の「診察結果」がｃ病院に共有され、診療記録として保存される
↓
次回以降、ｃ病院を受診した際にもオンライン診療の診療記録が活用される

※　民間事業者が検討するサービスを参考に、懇話会での議論用に市がサービス内容を設定したもので、実際の事業者のサービスを示すものではありません。
※　懇話会での議論用に市でサービス内容を簡素化、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を踏まえ事業が実施されます。

発行：つくば市科学技術戦略課
サービス提供事業者：株式会社Ａ

別添２

２．本事業におけるプライバシー情報の取扱いと安全性

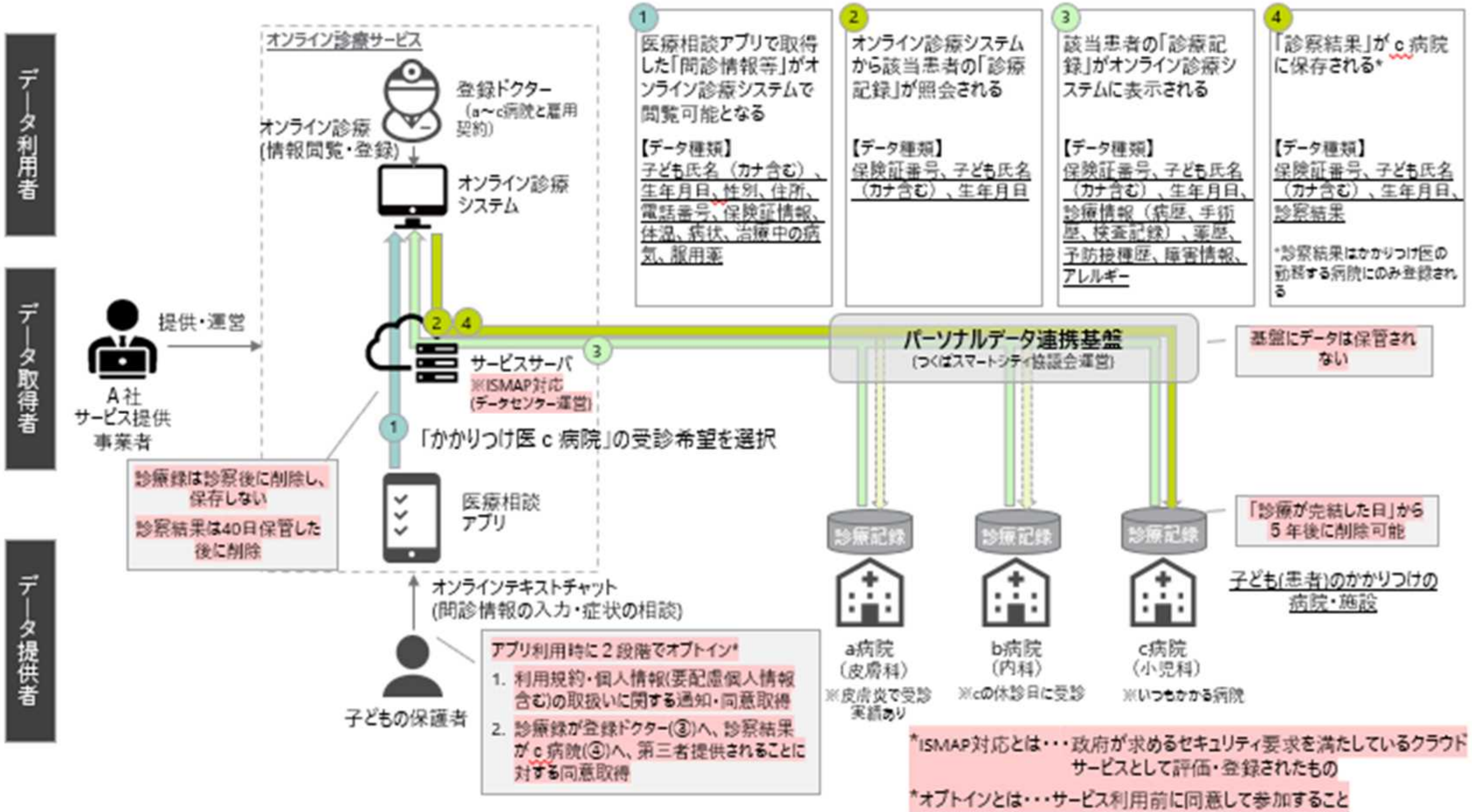
取り扱う情報

本事業で取り扱うプライバシー情報は次のとおりです。

□ 本人確認に用いる情報：子ども氏名、生年月日、保険証情報、住所、電話番号

□ 診察に用いる医療情報：診察記録、薬歴、予防接種歴、体温、病状、アレルギー、診察結果

情報の収集、利用、保管、廃棄の方法



① 医療相談アプリで取得した「問診情報等」がオンライン診療システムで閲覧可能となる
【データ種類】
子ども氏名（カナ含む）、生年月日、性別、住所、電話番号、保険証情報、体温、病状、治療中の病気、服用薬

② オンライン診療システムから該当患者の「診療記録」が照会される
【データ種類】
保険証番号、子ども氏名（カナ含む）、生年月日

③ 該当患者の「診療記録」がオンライン診療システムに表示される
【データ種類】
保険証番号、子ども氏名（カナ含む）、生年月日、診療情報（病歴、手術歴、検査記録）、薬歴、予防接種歴、障害情報、アレルギー

④ 「診察結果」が c 病院に保存される*
【データ種類】
保険証番号、子ども氏名（カナ含む）、生年月日、診察結果
*診察結果はかかりつけ医の勤務する病院にのみ登録される

診療録は診察後に削除し、保存しない
診察結果は40日保管した後に削除

基盤にデータは保管されない

「診療が完結した日」から５年後に削除可能

アプリ利用時に２段階でオプトイン*
1. 利用規約・個人情報(要配慮個人情報含む)の取扱いに関する通知・同意取得
2. 診療録が登録ドクター(③)へ、診察結果が c 病院(④)へ、第三者提供されることに対する同意取得

*ISMAP対応とは・・・政府が求めるセキュリティ要求を満たしているクラウドサービスとして評価・登録されたもの

*オプトインとは・・・サービス利用前に同意して参加すること

※　民間事業者が検討するサービスを参考に、懇話会での議論用に市がサービス内容を設定したもので、実際の事業者のサービスを示すものではありません。
※　懇話会での議論用に市でサービス内容を簡素化、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を踏まえ事業が実施されます。

２．本事業におけるプライバシー情報の取扱いと安全性

第三者提供・目的外利用の有無と、ある場合の概要

■ 第三者提供の有無

　病院（かかりつけ医）が保有する診療記録を、データ連携基盤を通じてサービス提供事業者Ａ社で参照可能にする部分及びオンライン診療の結果をサービス提供事業者Ａ社から病院へ提供する部分が該当します

■ 目的外利用の有無

　目的外利用は発生しません

※　民間事業者が検討するサービスを参考に、懇話会での議論用に市がサービス内容を設定したもので、実際の事業者のサービスを示すものではありません。
※　懇話会での議論用に市でサービス内容を簡素化、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を踏まえ事業が実施されます。

別添２

２．本事業におけるプライバシー情報の取扱いと安全性

プライバシー影響評価の結果

■ 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、総合評価は「Ｂ：リスク小」と判定しました。

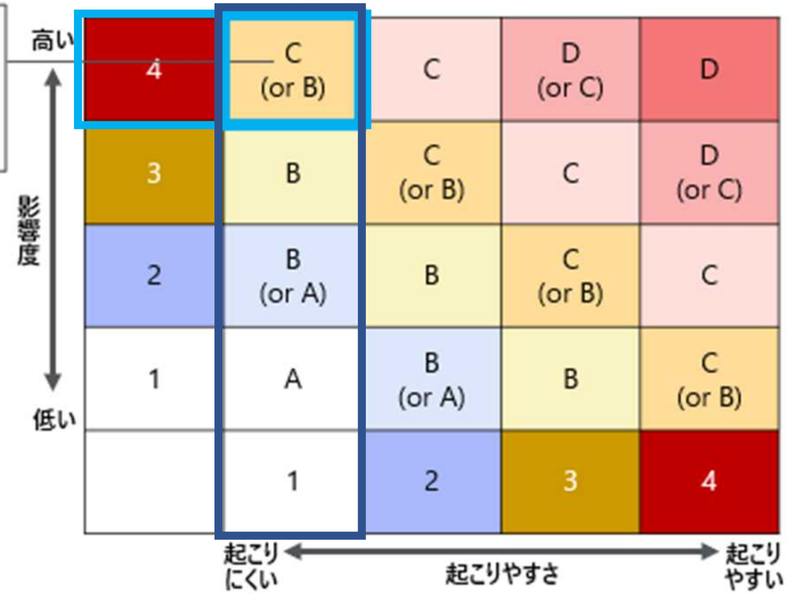
【主なリスクと対策状況】

取り扱うプライバシー情報の機微度の高さ

- 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から、影響度は「４」と評価しました。
- 一方で、データ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。データの取扱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「１」と評価しました。

プライバシー情報リスクマップ

総合評価
B



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

【凡例】
A：リスク微小
（想定されるリスクは極めて少ないが、ゼロリスクではないことを理解のうえ判断）
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）
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）
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）

※ 民間事業者が検討するサービスを参考に、懇話会での議論用に市がサービス内容を設定したもので、実際の事業者のサービスを示すものではありません。
※ 懇話会での議論用に市でサービス内容を簡素化、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を踏まえ事業が実施されます。

別添３

議題２　前年度からの継続論点の整理について

前年度の残論点の方向性について下表のとおり整理いたしました

#	分類	論点	方向性案
1	用語の定義	個人関連情報のうちどこまでを対象とするのか	• 個人関連情報は、下記定義案に記載のとおり – [定義案] 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)を指す
2		個人情報保護法の定義と「センシティブ情報」・「プライバシー情報」との関係性の精査の上、含むべき事項がないか	• センシティブ情報 – 個人情報保護法で定める「要配慮個人情報」が該当 • プライバシー情報 – #1に記載の「定義案」が該当
3		PIAを適用する対象(初期評価基準)をどのように定めるか	• 適用対象 – プライバシー情報を取扱っており、データ連携基盤に接続しているシステム又は、データ連携基盤に関係する事務/業務
4	実施のタイミング	再評価実施のタイミングはどの段階が適切か	• 大規模なシステム改修や新技術開発に伴う大幅な仕様変更がある場合は、再評価を実施する – 大規模なシステム改修時とはインプットと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とする
5		「大幅なシステム改修」はどの程度で必要と見なすのか	
6	評価項目	民間ユースケースにおけるチェック項目の違い	• PIA制度の評価項目案を提示する – データ連携基盤のあるべきを見据え、民間・行政でチェック項目に差異は設けず、一律とする – ただし、法令の定める事務又は業務の遂行に必要な範囲内で、行政機関が個人データを取扱う場合は、同意取得等は必ずしも求めない
7	評価基準	市民にとって安心を得られる基準かどうか	• 制度運用する中で適時にアップデートすることで安心を得られる基準を目指す
8		民間ユースケースの場合に当該基準を使うことの齟齬がないかどうか	

別添３

議題２　前年度からの継続論点の整理について

前年度の残論点の方向性について下表のとおり整理いたしました

#	分類	論点	方向性案
9	評価体制	民間サービスを対象とした場合のPIAの実効性を担保するために体制構築に当たり留意すべき点	• 民間特有の留意点は想定されない
10		PIAはあくまでリスクを可視化し、可能な限り是正を求める手段であり、漏洩の責任は事業者にあると整理するかどうか	• PIAの評価結果に関する説明責任は評価者であるつくば市が負う。万一の情報漏洩の責任は、サービス提供事業者等主たる原因者が負う
11		PIA制度の実効性を担保するため、運用面で協定・規約を整備する形でよいか。法的拘束力を有する条例ではなく、内規であるつくば市の要綱により制度化し、つくばスマートシティ協議会との協定の下、データ連携基盤利用規約でPIAの実効体制を確保する	• つくば市要綱で整理し、協定及び規約で実効性を担保する
12		評価を踏まえた対応をどのレベルまで行うべきか(各評価結果の評価後の対応はどうすべきか、D評価でもサービスリリースできるようにするのか、D評価の場合は基盤に接続させないのか 等)	• サービス提供事業者向けの利用規約にて、高リスクの判定結果だったサービスにおいては「つくばスマートシティ協議会」の判断の下、データ連携基盤への接続をお断りする可能性がある旨を定める
13		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どう対処するか	• データ連携基盤利用規約においてPIAの実施を前提とすることで十分な資料提供が得られない場合は、評価不能となり、基盤に接続できない運用とする
14		PIA制度の適切な運用をモニタリングするため、年に１度程度つくば市から(仮)評価委員会に制度の運用状況を報告するとともに、個人情報保護法の改正等のタイミングに合わせて必要な見直しを行う形でよいか	• 年に１度(仮)評価委員会に対象外通知の実績等を含む制度運用状況の報告を行い、適切な制度運用に必要な見直しを行う仕組みとする
15		制度的にはパブコメの対象ではなく、パブコメには時間を要し、サービスリリースが大幅に遅れることになるため、評価委員会において市民が参画することで市民の意見を反映させる形でよいか	• 評価委員会に市民委員が参画することで市民の意見を反映させた評価とする
16	公表	市民にわかりやすく伝えるための公表様式、公表方法	• 公表様式：詳細に公表する場合、攻撃者に内部情報・リスクを提供することに繋がるため、開示する情報量を制限し、粒度を粗くする • 公表方法：市のHPにおいて公開する

別添 4

■PIA事務局一次評価シート_新旧対応表

修正前		修正後			
No.	調査項目概要（概要、及び盛り込むべき要素や詳細）	No.	調査項目概要（概要、及び盛り込むべき要素や詳細）※追加/変更/削除箇所を青字で記載	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
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）	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		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		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		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）	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		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		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		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		④リスク管理責任者、セキュリティ責任者	－	－
	⑤委託先		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）		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		⑦サービスを提供される主体	－	－
03	サービスが適合する法令・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）	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）	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。）	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。）	－	－

No.	調査項目概要（概要、及び盛り込むべき要素や詳細）	No.	調査項目概要（概要、及び盛り込むべき要素や詳細）※追加/変更/削除箇所を青字で記載	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
	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		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		②処理担当者	－	－
	③各段階において取り扱うデータの内容		③各段階において取り扱うデータの内容	－	－
	④処理手順		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処理場所		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。）	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		①住所	－	－
	②当該部屋の階		②当該部屋の階	－	－
	③当該建物の構造		③当該建物の構造	－	－
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。※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）。	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。※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）。	必須	個人情報保護法 第27条、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。 ※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	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。 ※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	必須	個人情報保護法 第21条、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。）	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。）	必須	個人情報保護法 第34条、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。	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
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。）	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）。		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。		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。		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。		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

No.	調査項目概要（概要、及び盛り込むべき要素や詳細）	No.	調査項目概要（概要、及び盛り込むべき要素や詳細）※追加/変更/削除箇所を青字で記載	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
	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ている。		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）		その他、対策している内容（自由記述）	–	–
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。	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）。		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）。		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。		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。		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。		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ている。		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）。		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ている。		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で明記している。		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）		その他、対策している内容（自由記述）	–	–
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。	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ハードウェアや紙媒体での保存等、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。※調08と同様		~~①ハードウェアや紙媒体での保存等、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。※調08と同様~~	–	–
	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）。※調08と同様		~~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）。※調08と同様~~	–	–
	③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。		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)
	④一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。		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

No.	調査項目概要（概要、及び盛り込むべき要素や詳細）	No.	調査項目概要（概要、及び盛り込むべき要素や詳細）※追加/変更/削除箇所を青字で記載	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
	⑤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。		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)
	⑥アクセス権は定期的に見直すこととしている。		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
	⑦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。		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
	⑧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）組織内規程を定めている。		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）		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。	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ハードウェアや紙媒体での保存等、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。※調08と同様		~~①ハードウェアや紙媒体での保存等、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。※調08と同様~~	－	－
	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）。※調08と同様		~~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）。※調08と同様~~	－	－
	③イベントログを取得・保持するようになっている。		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)
	④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。		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
	⑤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、社内規程を定めている。		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）		その他、対策している内容（自由記述）	－	－
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。）	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。		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）		その他、対策している内容（自由記述）	－	－
16	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。（興味本位での紐づけや本来は別々で管理している個人に関する情報を統合し保持することがないことを説明すること。）	~~16~~	~~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。（興味本位での紐づけや本来は別々で管理している個人に関する情報を統合し保持することがないことを説明すること。）~~	－	－
	①APIなど、当該システムやDBに接続する手段が公開されていない。		~~①APIなど、当該システムやDBに接続する手段が公開されていない。~~	－	－
	②不適切な紐づけの防止につながる規程（事業Aで得た個人に関する情報を他事業に転用しない等）が定められている。または、案件ごとに担当者を分離し不適切な紐づけが発生しないようにしている。		~~②不適切な紐づけの防止につながる規程（事業Aで得た個人に関する情報を他事業に転用しない等）が定められている。または、案件ごとに担当者を分離し不適切な紐づけが発生しないようにしている。~~	－	－

No.	調査項目概要（概要、及び盛り込むべき要素や詳細）	No.	調査項目概要（概要、及び盛り込むべき要素や詳細）※追加/変更/削除箇所を青字で記載	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
	その他、対策している内容（自由記述）		~~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処理目的に関する情報が不十分でないか。利用者にわかりやすく説明しているか。（利用開始時の説明が十分であり、利用者が処理目的及び範囲について理解できていることを説明すること。）	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。~~が不十分でないか。利用者にわかりやすく説明しているか。（利用開始時の説明が十分であり、利用者が処理目的及び範囲について理解できていることを説明すること。）~~	－	－
	①HP等で本サービスに関する情報をいつでも閲覧できる。		①HP等で本サービスに関する情報をいつでも閲覧できる。	必須	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。		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
	③（該当する場合）アプリ上等で処理目的を説明する場合、利用者の理解を確認する工程を必須としている（「理解しました」等のメッセージにチェックを入れる等）。		~~③（該当する場合）アプリ上等で処理目的を説明する場合、利用者の理解を確認する工程を必須としている（「理解しました」等のメッセージにチェックを入れる等）。~~	－	－
	④利用者向けの相談窓口を設置している。		~~④利用者向けの相談窓口を設置している。~~	－	－
	その他、対策している内容（自由記述）		その他、対策している内容（自由記述）	－	－
18	個人に関する情報の不必要な長期保有が発生しないか。	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。	－	－
	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。		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。		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データの廃棄期限等を契約段階で明記することとしている。		③データの廃棄期限等を明確に定めており、適切に廃棄している。~~を契約段階で明記することとしている。~~	推奨	該当なし
	④廃棄実施時には、その旨を市と確認することとしている。		~~④廃棄実施時には、その旨を市と確認することとしている。~~	－	－
	その他、対策している内容（自由記述）		その他、対策している内容（自由記述）	－	－
19	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。）	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。）	－	－
	①本サービスが住民に与える影響について、コンプライアンス担当部門などが確認する体制がある。		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）		その他、対策している内容（自由記述）	－	－
20	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。	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。		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)

No.	調査項目概要（概要、及び盛り込むべき要素や詳細）	No.	調査項目概要（概要、及び盛り込むべき要素や詳細）※追加/変更/削除箇所を青字で記載	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
	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。		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。		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。		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）		その他、対策している内容（自由記述）	－	－
21	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。）	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。		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。		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）		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。		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）		その他、対策している内容（自由記述）	－	－
22	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。	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。		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）		その他、対策している内容（自由記述）	－	－
23	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。）※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。	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。		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

令和6年(2024年)4月1日

つくば市プライバシー影響評価制度検討懇話会
座員名簿（案）

（五十音順）

	氏名	役職等	備考
1	おちあい　たかふみ 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	
2	こいぬま　てつや 鯉沼　哲矢	市民委員	
3	さかした　てつや 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	
4	すずき　けんじ 鈴木　健嗣	国立大学法人筑波大学システム情報系 系長・教授	
5	たかはし　やすひろ 髙橋　安大	つくば市政策イノベーション部 部長	
6	とみた　るみこ 冨田　留美子	市民委員	
7	はしもと　なおみ 橋本　尚美	市民委員	
8	ひらやま　ゆうた 平山　雄太	IDEAPOST株式会社　代表取締役社長	
9	みずまち　まさこ 水町　雅子	宮内・水町ＩＴ法律事務所　弁護士	

会　議　録

<table>
<tr><td colspan="2">会議の名称</td><td colspan="3">第７回つくば市プライバシー影響評価制度検討懇話会</td></tr>
<tr><td colspan="2">開催日時</td><td colspan="3">令和６年(2024 年)12 月 20 日　開会 17:00　閉会 19:00</td></tr>
<tr><td colspan="2">開催場所</td><td colspan="3">つくば市役所コミュニティ棟１階　会議室１
（オンライン併用）</td></tr>
<tr><td colspan="2">事務局（担当課）</td><td colspan="3">政策イノベーション部　科学技術戦略課</td></tr>
<tr><td rowspan="3">出席者</td><td>委員</td><td colspan="3">坂下座長、落合座員、鈴木座員、冨田座員、平山座員、髙橋座員、水町座員</td></tr>
<tr><td>その他</td><td colspan="3">（オブザーバー）
内閣府地方創生推進事務局 牟田企画調整官
デロイトトーマツサイバー合同会社　三谷氏、林氏</td></tr>
<tr><td>事務局</td><td colspan="3">政策イノベーション部　科学技術戦略課
　中山課長、高橋課長補佐、金山係長、東泉係長、六笠主任、藏内主事、松好研修員</td></tr>
<tr><td colspan="2">公開・非公開の別</td><td>■公開　□非公開　□一部公開</td><td>傍聴者数</td><td>１名</td></tr>
<tr><td colspan="2">非公開の場合はその理由</td><td colspan="3">－</td></tr>
<tr><td colspan="2">議題</td><td colspan="3">(1) 最終とりまとめ（案）について
(2) 最終とりまとめに向けた残論点について</td></tr>
<tr><td>会議次第</td><td colspan="4">１　開会
２　議事
(1) 最終とりまとめ（案）について
(2) 最終とりまとめに向けた残論点について
３　その他
４　閉会</td></tr>
</table>

１　開会

事務局（中山課長）：定刻となりましたので、ただいまから第７回プライバシー影響評価制度検討懇話会を開会いたします。本日の座員の皆様のご出席は

現地が６名、オンライン１名となっております。なお、本日鯉沼座員・橋本座員はご欠席とのことでございます。また本日はオンラインで内閣府地方創生推進事務局から牟田様にもご参加いただいております。牟田様一言お願いできますでしょうか。

牟田調整官：オンラインから失礼します。内閣府の牟田です。本日もどうぞよろしくお願いいたします。スーパーシティの取り組みは、つくばで様々な実証やチャレンジをしていただいてかなり進んできていると思います。改めて住民中心、住民とともにつくばスーパーサイエンスシティ構想を進めていこうという中で、やはりPIAが重要だなという風に感じているところでもございますので、改めて市民目線で、いろんなご意見いただきながら、次回で取りまとめていくとお聞きをしておりますので、ご議論いただければなと内閣府としても思っております。本日もどうぞよろしくお願いいたします。

事務局（中山課長）：ありがとうございました。また今年度のPIA制度の検討につきまして、連携させていただいているデロイトトーマツサイバー合同会社様からは三谷様、林様にご出席いただいております。それではここからはつくば市プライバシー影響評価制度検討懇話会設置要綱の規定に基づきまして、座長に進行をお願いしたいと思います。坂下座長よろしくお願いいたします。

坂下座長：では本日もよろしくお願いします。予定を申し上げます。本日は議事が２件です。よろしくお願いします。ここで会議の公開、非公開ですが、つくば市附属機関の会議及び懇談会等の公開に関する条例により、法令または条例で定めがある場合を除いて原則公開となります。本日の懇話会は非公開事由に該当しないので、公開で進めて参ります。また会議の記録のために事務局においてZOOM録画及び写真撮影等をさせていただきます。そこはご承知おきください。

２　議事

(1) 最終とりまとめ（案）について

坂下座長：それでは議題に入ります。「議事(1)　最終とりまとめ（案）について、事務局から説明をお願いいたします。

〔議事(1)について事務局から説明〕

坂下座長：どうもありがとうございました。全体の構成についてと 23 ページより前の部分で御意見ありましたらお願いいたします。平山座員からよろしいですか。

平山座員：非常によくまとまっていましたし、これまで懇話会で議論してきた内容が概ね細かい形で反映されていると思います。特に個別のポイントで気になる点はなかったです。特にチーフプライバシーオフィサーをしっかりと作るということが明記されていてかなり踏み込んだものになっていると思います。

坂下座長：ありがとうございます。冨田座員お願いします。

冨田座員：私も特に気になる点はなかったです。

坂下座長：ありがとうございます。落合座員お願いします。

落合座員：よい形でまとめていただいていると思っています。基本的にはこれまで議論してきたものを積み重ねていただいたものだと思うので、これをつくば市として取りまとめることもそうですし、内閣府の方々にもこれをどう他にも広げていくのかということも合わせて、今後取り組んでいかれるといいと思います。

坂下座長：ありがとうございます。鈴木座員お願いします。

鈴木座員：私も拝見しまして、しっかりと内容が詰められていて、これまで議論してきた内容が入ってよかったなと思いました。1 つだけ、14 ページの「本評価制度はサービスを対象に PIA を行うというもの」がまさしく原則だと思います。しかし、例えば同じサービスでも全く似ているサービスが A 社 B 社と出てきた場合、今だとそれを分ける仕組みがもちろんないなっていう。それを分けていいのか、いけないのかはありますけれども、例えばちゃんとデータの管理ができる、できそうだと。そういったところの区別が今のところなかなか難しいなと。そこについて記載している内容や、関連する内容の記載がなかったのですが、例えば医療費であれば、医療機器製造業、製造販売業がそれを担保できるとか、もちろんちゃんとやりますということで

ISOを要件につけることもありますが。プライバシーインパクトの評価の中で、A社B社と同じサービスが出てきたときに、信頼のおけるA社がプライバシー評価を行って〇が出て、信用できなさそうなB社が同じサービスだった場合には通さざるを得なくなったりするのかなというのを不安に思いましたので、発言させていただきました。

坂下座長：今のご意見について事務局から意見はありますか。

事務局（高橋補佐）：サービスを対象にPIAを行うという前提条件を書かせていただいていますが、仮にそのサービス内容が同じだったとしても、背景にあるデータの処理の仕方や管理体制などの違いが、おそらくサービスごとにあるかと思います。仮にそういったA社B社が出てきた場合は、背景となる部分をしっかり評価し区別して、A社は〇で、B社は×という評価の違いが出てくるのはあり得るのではないかと思っております。

鈴木座員：原則としてサービス提供事業者の評価を行わないということからすると、サービス提供者の信頼性を評価することがこのシステムでできるのかなっていうのが気になったところでして。しないというふうに決めるのも手だと思いますが、現行でそこに関わるものはありますでしょうか。

事務局（高橋補佐）：現在の項目の中で、事業者自体の信頼性を評価する項目はありません。

坂下座長：法人番号やプライバシーマークで見るなど、いろいろやり方がありますが、そこのところは先々のことかもしれません。ただそういった部分もあるということをお示しいただいたのだと思います。

鈴木座員：特に起こりやすさがそれに関連するだろうと思い、気になったところです。

平山座員：スタートアップを対象にしていくと思うと、どこまで厳しくするかは悩ましい部分でもあると思いますし、この辺りは今後運用の中で整理していくことだと思います。

鈴木座員：市民目線から見れば、つくば市がやっているなら大丈夫かなっていうのがあります。例えばナンバーワンスタートアップ会社のようなところに行って、個人情報をちゃんと扱えますよっていうふうに言っているのと、他の個人情報を扱うのに長けている会社とサービスは同じ場合がある。その時

に適切に扱われれば、このぐらいのプライバシーインパクトということを守れば、サービス事業者の信頼性とは分離するというのは実は正しい方向なのかなと。

落合座員：まず信頼性を何で測ったことにするかが最初にあると思っていました。いろいろな制度でいうと ISMS やプライバシーマークなどのやり方もなくはないと思いますが、ただしかしながら、金融では ISMS を持っていないところもたくさんありますが、セキュリティが低いわけではありません。その際何をもって見ているのかというと、取り扱いに対する体制や組織的安全管理措置、人的安全管理措置などですが、その他にも物理面、技術面もあるとは思います。その観点で、概要版４ページ No.21 が人的体制に対する措置の一部かなと思います。要するに教育研修が中心的なものを構成し、管理責任者の設置などは実務的に評価しておくことによって、責任者と教育研修体制、また目的外利用というところで、例えばアクセス権限管理などがありますが、No.12 で人的な部分はみていくことだと思います。また組織については No.20 で、監査によりセキュリティ体制が適切に管理されているかということで、ここはスリーラインディフェンスまでは言ってない内容だと思いますが、内的なリスク管理や監査のためのフレームワークがあるのかどうかを見ています。また、全般的に規定を整備して、それに基づいてという内容を明示的に書かれてはいませんが、そういったことを意識してみていくことで、結局は規定の中で行っていくのは、No.11-17 に書かれているような情報についての情報収集であっても、必要十分な範囲でのみ利用するようにしている形だと思います。その中で実質的には見ている側面があると思いますので、マークや認証とは言っていないと思いますが、実態的には要求される内容には入ってはいると思います。プロセスや組織として管理できる体制があるのかどうかは、起こりやすさなどにつながってくるので、少なくとも個人情報の取扱いに関する限りにおいては、評価側でも理解していただいて、今後運用していただくことで解消していくことがあると思います。見てないというと心配ですが、内容を実務的に整理してみていけば概ね必要な組織や人的なプロセスはみていると言える項目が入っていると思います。

鈴木座員：非常に明確でした。No.20 がほぼ組織、No.21 が人的な内容だとして、

組織的に管理される体制があるのかをみるのと、またそれを扱う人々に対する教育研修だとどんな教育研修をしているのかのレギュレーションがあるから、大卒、高卒、中卒も基本的には教育内容が決まっているというかというと、別にここにプライバシーマークとかを定めなかったとしてもしっかりとサービス事業者側がちゃんとした体制であるのかどうかを確認するメカニズムがすでに入っているという理解でよいかなと思いました。

高橋座員：まさに座員の皆さんもおっしゃっていただいた通り、全体としては議論が網羅されているかなと思いますし、また今後運用するという観点においても、あまりにも厳し過ぎないといいますか、実際の運用の中でいろいろ出てくるだろうというところまで先を見通してですね、記載させていただいていると思いますので、あくまでも基本的な考え方だと思いますので、この心を忘れずに運用していくことによって初めてPIA制度が意味をなしてくると思います。よくまとまっていると思います。

坂下座長：ありがとうございます。水町座員お願いします。

水町座員：文書としてしっかりと書かれていてわかりやすく綺麗にまとまっていると思います。細かい点を申し上げますが、今の話に関しては物理対策がないかもしれないですね。考えていただいた方がいいかもしれません。また4ページ1段落目「不安感が蔓延している～」という書きぶりだと、データ利活用を促進するためには、PIA が必要と読めなくもないので、2 段落目では、いわば両輪の関係ということが言いたいのだと思うので、「市民に安心していただくために」のような言い方がいいかなと思いました。また2段落目「片手落ち」は違う用語の方がいいかもしれません。また9ページの評価委員会について15ページ4段落目の内容が9ページには記載がない。15ページが具体的なので、そこをリファーする形にした方が評価委員会の機能として過不足がないと思いました。あと10ページ3段落目で「セキュリティ評価とPIAの大きな違いが時期」といった記載がありますが、基本的に事前評価なのでこのままでいいとは思いますが、もし事後評価が出てくる場合、このような記載にしない方がいいかもしれないかなと。最も大きな違いと書くと、事後評価が出てきた場合に備えて少しトーンを落としてもいいのかなと。特に強い意見ではありません。次が11ページ図3で脚注と図のリンクがわ

かりづらいので、コンサルの方に直していただくといいのかなと思いました。また13ページの「個人関連情報の定義」の記載は直した方がよくて、このままだと仮名加工情報のような定義ぶりになっているので、「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ので膨大」と書いた方がよいと思います。個人情報保護委員会のガイドラインとかだとそこまではっきりは書いてないようにも思います。その辺ご検討いただいた方がいいと思います。あとは17ページ「影響度判定表」は評価委員会で細かい部分を別途検討したほうがいいのかなと思っていました。あと18ページのNo.7が「必須」というのはどういう意味でしたでしょうか。

事務局（高橋補佐）：評価項目としては第三者提供を評価することになっておりますので、仮にそのサービスの中で第三者に対してデータを提供するような仕組みが、管理サービスの中に含まれている場合は、それに対して同意を取られているかを評価する。この項目に関しては第三者提供にあたるので、それに対しては法的には同意をとることが必須と考えられるというふうに我々としては考えています。

水町座員：役所の場合は第三者提供じゃなくて目的外提供か目的内提供かの規制になっているので、まず第三者という概念がない。民間の場合は第三者提供であっても一応オプトアウト可能とか、法令に基づく場合とか、公衆衛生向上とかで例外がなくはないと思います。

事務局（高橋補佐）：水町先生おっしゃる通りこの22項目については官民問わずということで評価項目に入れていますが、やはり目的外なのか、第三者提供なのかが官民で違うと思うので、どちらかに当てはまらないというものの整理が必要かもしれません。

水町座員：また民間でも要配慮じゃなければオプトアウトで適法に第三者提供できますし、公衆衛生向上ために同意困難な場合とかは第三者提供できるので、同意がなくてもできる場合があります。必須という書きぶりは良くて、評価基準の説明のところに詳細を書いたほうがいいのではないかと。運用段階でそこも考えていただければいいかなとは思います。ご質問ですが23ページの「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」はどういう方を想定されているのでしょうか。

事務局（高橋補佐）：スーパーシティに関してはアーキテクトという役割が位置付けとしてございまして、現在は鈴木先生です。アーキテクトを想定した書きぶりとご理解いただければと思います。

水町座員：「PIA 制度を運用している民間事業者の代表者」というのはつくばと関係なく実施している人という意味ですか。

事務局（高橋補佐）：具体的な会社が頭にあるわけではないですが、民間としてすでに PIA を運用していらっしゃる会社がいくつかあると思うので、先行事例的にやっていらっしゃるところの代表の方も入っていただければ、有意義な意見をいただけるのではないかと思い書かせていただきました。

水町座員：セキュリティ専門の方は箇条書きに入らないでよいでしょうか。データ連携分野がそれを含んでいる感じですか。

事務局（高橋補佐）：セキュリティの分野で全面に出てくる方は含まれていないです。

水町座員：入れたほうがいいかもしれないですね。セキュリティ情報技術に関する有識者とかでもいいのかもしれないです。

事務局（高橋補佐）：あくまで 1 例なので、この内容でフィックスするわけではないです。御意見参考にしたいと思います。

水町座員：あと 25 ページ 1.2.7 の 11 行目で句読点の位置を修正したほうがいいと思いました。

坂下座長：細かく見ていただきありがとうございます。

落合座員：個人情報の安全管理措置の中で物理の話がありましたが、項目の詳細が手元にないのですぐに思い出せないことが無きにしも非ずですが、例えば No.6 の「データ保管場所に関する情報」は物理的安全管理措置については、取り扱い管理区域、機器電子媒体等の盗難防止、持ち運びの際の漏洩防止、廃棄の 4 点で整理されていると思います。No.11、No.12 としてはおそらく盗難防止、漏洩防止、廃棄等に関して一部処理されている部分もあると思います。No.17 における長期保有も含めて詳細基準に書いていないところがあれば付け足していただいた方がいいかもしれませんが、項目としては足りないわけではないと思いました。運用のときにチェックするポイントを押さえる形にすればいいのではと思います。No. 7 と No.8 の個所で No.8 で同意

を得ない場合はその根拠という場合があると思いますので、No.８で別の正当な理由を考慮する形になると思いますが、念のため No.７ の関係で形式的には同意を取っている形になっているので、同意が必要だというふうに思われる場合も多いが、ここは適法に処理してるかというくらいで、読んでいただくのがいいのではと思います。No.７に No.８の内容を一言足しておいていただくといいのではないか。ただここを指摘すると全部を言わないといけなくなるので、全体として頭書きのところに同意など特定の手段を設けているところでは、実質的に適法であればそれは手法として基本的には認めます、と記載する形がいいのではと思います。セキュリティなどに、大体最初にリスクベースアプローチですと記載すると、その後適切な手法であれば読んで良いということになると思います。それを明確に書いていただいく形でというのはいかがでしょうか。

事務局（高橋補佐）：御意見いただきありがとうございます。反映させていただきたいと思います。資料に出している項目は見出しのみなので、項目の細かい内容を踏まえて直していければと思います。

坂下座長：最終とりまとめは誰に読んでもらいたい資料ですか。

事務局（高橋補佐）：位置付けとしては懇話会から市に対しての提言書となります。市はこれをもってして正式制度化を図るという位置付けになります。提言書はもちろん市民の方々にも公開します。

坂下座長：市への意見表明であれば、あまり難しくなってしまうと、きっと１ページ目で終わっちゃうと思います。そこの部分は事務局の方々で考えていただいて、プライバシーに対して、市が考えていますということをアピールする文書だと思うので、そこがちゃんと伝わるようにしてください。

（２）最終とりまとめに向けた残論点について

坂下座長：続いて「議事（2）最終とりまとめに向けた残論点」につきまして事務局から説明お願いします。

〔議題２について事務局から説明〕

坂下座長：ありがとうございました。責任分界点についてご意見・ご質問がありましたら、挙手をお願いします。平山座員からお願いします。

平山座員：私はこの事務局案に賛成で、明記しないでいいと思います。その根拠は、これが起こりうるときは個人情報が漏洩したということだと思いますが、それはPIAの問題なのか、セキュリティインシデントの結果としてプライバシーにも影響があったというケースの方が実際には多いのではと思いまして、それはケースによって違うのですが、結論は書いてある通りでPIAの範囲の中だけで終わらない気がするので、今回のこの制度の中に、そこまで書き込まないで、あくまで情報漏洩や、インシデントが起きた際に別で動くものの中で整備した方が綺麗なんじゃないかなという意見です。

坂下座長：ありがとうございました。水町座員お願いします。

水町座員：私はおまとめいただいた通りでいいと思います。2点意見がありまして、本文24ページ「責任分界点の考え方②」で、いわゆる優良誤認、不適切な記載のような、虚偽までいかないが、あえて黙っていたものも責任を負ってもらったほうがいいと思います。しかも不利益を生じさせたかどうかは関係ないと思います。実損害はなくても虚偽申告はよくないので、ここの記載の責任範囲が狭すぎるかなと。やはり誤認、誤導はよくない。今の要約版だと、申請内容全体に責任を負うとなっているからPIAの内容自体にも責任を負ってもらわないといけないのかなっていうふうに思いました。もう1点は要約版8ページ「プライバシーインシデント」の説明はいいと思うのですが、例の「炎上事例」が「不適切な目的外利用」などの記載にした方がいいと思います。適法で炎上することもあると思うので。私の意見は以上です。

事務局（高橋補佐）：ありがとうございます。ご指摘の通り必要な修正をかけていきたいと思います。

落合座員：スマートシティ協議会は作業としては何をしているのでしょうか。

事務局（高橋補佐）：つくば市の今後の体制の話になるのですが、現時点でつくば市としては、プライバシーデータ連携基盤をつくばスマートシティ協議会が整備をして持っていただくといった前提で考えております。そのためサービス提供事業者は市ではなくて、協議会との間でデータ連携基盤の使用可

否が決まることになります。ですので、サービス提供事業者は協議会に対して利用申請をし、それに基づいて、協議会が市に対してこのサービスを運用していきたいので、PIAをお願いしますといった流れを考えています。協議会はこのような機能・役割を担っている形を想定しております。

落合座員：接続先に対して、テクニカルなテスト等はしないということですか。

事務局（高橋補佐）：しないという想定です。

落合座員：わかりました。データ連携をする画面のところで問題が発生することがあり得なくはないと思うので、示していた仕様通りの基盤を提供するところは責任がありそうですが、今回のPIAに関して受けさせるだけということですね。

坂下座長：市があって、サービス提供事業者がいて、データ連携基盤整備主体がある体制は、スマホでいうところのアプリストアが協議会、中にあるアプリが提供事業者というように考えられます。ただつくばの場合、市がスーパーサイエンスシティ構想で特別特区になって PIA を行っているので、一番大きいフレームは市である。その上で協議会というストアが頑張っていて、そこにサービス提供事業者がアプリを提供していくのに PIA をどうするかという話になりますから、最後の責任は PIA は市がやりますとなると思います。

続きまして、再評価の基準についてご意見がある方がおられましたらお願いします。

鈴木座員：再評価について正確に把握したいのですが、再評価と普通の評価は何が違うという位置付けで書いているのでしょうか。

事務局（高橋補佐）：こちらで想定している再評価は、すでに提供済みのサービスは基本的には１回はPIAを受けている前提になっていますが、再度PIAを受けなければいけない状況になった場合の、再評価の基準はどのように考えればいいのかを今回議論させていただきたいと思っています。

鈴木座員：結局もう１回全部同じことやるのだったら再評価というよりも評価のやり直しとかがいい気がします。再評価するという場合に、例えば変更した部分だけの評価をするから再評価にするということができるのかなと。実際にはそういった変更があった場合には、再度PIAの評価を受けるというシ

ンプルな形でも良いのかなと。再評価という新しい枠組みを作ってしまうと、PIA 評価と PIA 再評価っていう２つの規則がなんかできちゃうような気がしました。日本語の問題でもありますが、再評価の意味をまず明らかにしたいと思って質問させていただきました。

事務局（高橋補佐）：事務局としても、例えば安全管理に資する変更であれば、簡易的な再評価に限定するといった方針が定まっていない状況でして、なのでどういった状況になったら再評価を行うという点を決めたいということと、実施する場合にどこまで行えばいいのかを考えていかなければいけないなというのが現状でして、厳密にはそこについて定めきれていないところが正直なところです。

鈴木座員：そしたら、例えばシステムの変更に対する再評価っていうふうな形の位置付けなのですね。システムが変更に当たると判断されるレベルがこの大幅な仕様変更、それを超えて全く別なシステムとなった場合には再評価じゃなくて、再び１からの評価の実施。変更の場合には再評価で簡易な評価をするという位置付けなのでしょうか。

落合座員：全然違うという場合は、１からということはあり得るのでしょうか。ただシステムの構成がある程度変わるだけだとか、システムだけでもなくてサービスそのものに大きな変更があった場合でも評価するべき場合があると思っています。例えば情報を使ったサービスであって、情報の提供範囲が広くなり、管理できているのかということがあるかもしれませんが、わざわざ再評価というシステムを入れておくのであれば、マイナーな変化の場合には、簡易審査になるような形で設計しておいた方が良いのだろうと思います。そうでなければ１から見直すことになりますが、基本的には差分をある程度比較して変わっているところを見ていくことが合理的に想定されるのではないかと思います。変更点に関しては、新しくヒアリングしたり調査したりする方法がいいのではと思います。

坂下座長：水町先生ご意見お願いします。

水町座員：そうしますと再評価というのは、変更点に対する簡易な再評価ということ。ここで気になるのが大幅な仕様変更というもので、個人的には大幅な変更は変更申請ではなく再度評価するしかない。例えば取扱情報のレベル

が変わることが変更申請と我々が言うことはほとんどない。例えば対象者が100人のシステムだったのが、1万人になりますというのは、対象人数の変更なので軽微な変更ですよね。例えばこれまでは散歩に行く日を調べていたのが、何か病院に行く日を調べることになりました。外出の頻度を調べているから同じですと言われると困るし。AIのアルゴリズムが変わったら私の中ではとてもセンシティブなので、これは変更でいいのかなという。ここに書いてある大幅な仕様変更っていうようなことは再度1から評価でいいのかなと。むしろそうじゃない変更のときのために簡易評価を残すのは、運用上としては良いなと思いました。

1回PIAやればいいというのをやめてくださいというのがここの論点で、ただ軽微な変更の場合は直さないでいいことを前提にして、1回PIAやってももう一度やってくださいというのをここでは再評価って言っていて、その再評価に1からやり直しと、変更点だけ見ればいいというものがあるという分岐になると思いました。実際問題、特定個人情報保護評価では、再評価を結構やっていますが、基本的には差分を見ています。しかし例えば国民健康保険のシステムなんかで、マイナ保険証が出てきたりすると仕様変更。また新しいシステムとくっつけますとか、そういうもので再評価をやっています。基本的には保険証の部分しか見ていませんけれども、ただ委員の構成が変わったりすると、該当箇所だけではなくて、もともとの部分も再評価されるみたいな感じで、一度PIAをやったらずっと通用するわけじゃなくて、運用の中でどの程度だったら軽くて、どの程度だったらちゃんとやるというのは、評価委員会のメンバーとかそのご判断とかにもよってくるのかなと思いました。話は変わりますが、私の意見としては、基本的に事務局の案で問題ないと思います。ただ追加すると、丸で囲ってある部分がその通りなので、データの種類に変更が生じるとやり直す必要があるから、そこが今はサービスに変更等が生じた場合の例示にない。特定個人情報保護評価と違っていいところは、粒度が粗い。JNSA基準で影響度が違うデータを取り扱うことになった場合とかを例で入れていたらいいかなっていうのが1点。2点目は評価項目が変わる場合が、つくばの場合は後から権限管理しているかどうかのレベル感だから、権限管理をいきなりしなくなるとかそういうことがあった

らやり直さなきゃいけないけど多分そういうことはない。そう考えると、結局サービスに変更等が生じた場合の例示として、体制変更がある場合の他に評価項目の細則を満たさなくなったような場合とかの記載を足しておけばいいのではという気はします。以上です。

坂下座長：どうもありがとうございます。事務局からなにかありますか？

事務局（高橋補佐）：いただいた御意見参考に修正していきたいと思います。ありがとうございます。

坂下座長：あんまり基準を細かく決めないほうがいいと思います。私の当協会では大きな自治体の特定個人情報評価をやっております。5 年ごとの見直しがきていまして、水町先生がおっしゃったように、マイナ保健証の部分があれば、その部分だけの評価しかしていません。ただ私たちはそうではなくて、業務フローを全部作りまして、業務フローが変わったら全部やり直します。本当にやるのだったらそういうことになってしまうのですね。あと再評価っていうのは基本的にはもう動いているという前提で、評価を行ってその上で差分を見るっていうのが、現場で私たちがやっている PIA。それを言い出すときりがなくなってしまうから、PIA はつくばスーパーサイエンスシティ構想の中で取り入れてくということの宣言文ですから、あまりここは細かく落とし込まない方がよろしいと思って、実際に運用してから調整すべき部分じゃないかというふうに座長としては考えます。高橋座員お願いします。

高橋座員：本文 29 ページで、再評価についても基本的にはサービスの変更の前に認識をしています。中を見ていくと「変更した場合」というように過去形で出て来ていて変わった後に申請をしてもいいように読めてしまうかなと思いましたので、そこについては再評価を変える前にやるということを明記しておいた方が安心かなと思いました。

落合座員：どのタイミングで気づくかということですが、変更がある場合に届け出をもらうのであれば、報告書ではなくて基盤の規約などで、「変更する予定がある場合は届け出てほしいこと」の明記が必要だと思いました。報告書の変更は必要ないと思います。

坂下座長：今出ましたご意見につきまして事務局の方で必要な個所は修正をお願いしたいと思います。次の議事に移ります。その他としまして、最終とり

まとめの流れについて事務局よりご説明お願いします。

事務局（高橋補佐）：今後のスケジュールに関して、本日ご意見多々いただきましたので、それを踏まえ事務局の方で最終取りまとめ案の修正をかけさせていただきます。修正作業を年明けにかけて行いまして、次回2月14日に第8回PIA懇話会ということで、最終回の予定になっておりますが、今回の修正を加えた最終とりまとめ案についてご確認いただいて、最終的には内容についての合意を取り付けたいと考えております。第8回で合意まで取り付けられた場合は、最終調整を行いまして、年度内の3月中に懇話会としての最終取りまとめとして公表をさせていただきたいと考えております。この公表をもって令和7年に入りましたら、早期に実際の正式な制度として、市として制度化を図りたいと考えております。今後の流れとしてこのような形で進めてまいりたいと思っております。

坂下座長：第8回懇話会もご多忙と思いますが、ご参加いただければと思います。それでは本日予定しておりました案件はすべて終了いたしました。長時間ありがとうございました。進行を事務局に戻したいと思います。

事務局（中山課長）：長時間に渡りご議論いただきましてありがとうございました。次回の懇話会は2月14日を予定しております。以上をもちまして第7回つくば市プライバシー影響評価制度検討懇話会を終了いたします。どうもありがとうございました。

第７回つくば市プライバシー影響評価制度検討懇話会

日時：令和６年(2024年)12月20日（金）17時～
場所：つくば市役所コミュニティ棟１階　会議室１
（オンライン併用）

次　第

１　開会

２　議事

(1) 最終とりまとめ（案）について
- 事務局からの説明
- 内容、方向性等に関する質疑

(2) 最終とりまとめに向けた残論点について
- 事務局からの説明
- 責任分界点に関する議論
- 再評価の実施基準に関する議論

３　その他

４　閉会

○ 配付資料

資料１　最終とりまとめ（案）　詳細版
資料２　最終とりまとめ（案）　概要版
資料３　残論点に関する資料

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
目次（案）

今回ご確認いただきたい範囲
（今回懇話会での協議対象）

0　はじめに

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

1.2　各論

今回対象外
（次回懇話会での協議対象）

2　検討の経緯
  2.1　委員の主な意見
    2.1.1　評価対象
    2.1.2　評価基準
    2.1.3　評価項目
    2.1.4　評価体制
    2.1.5　実効性の担保
    2.2.6　公表

3　懇話会の概要
  3.1　構成員
  3.2　検討事項
  3.3　懇話会開催状況

4　総括

別表
1　評価項目一覧（案）
2　評価結果報告書（概要版）様式（案）

別添資料
1　懇話会資料、議事録
2　懇話会設置要項

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、●機関が参画（2024年●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。

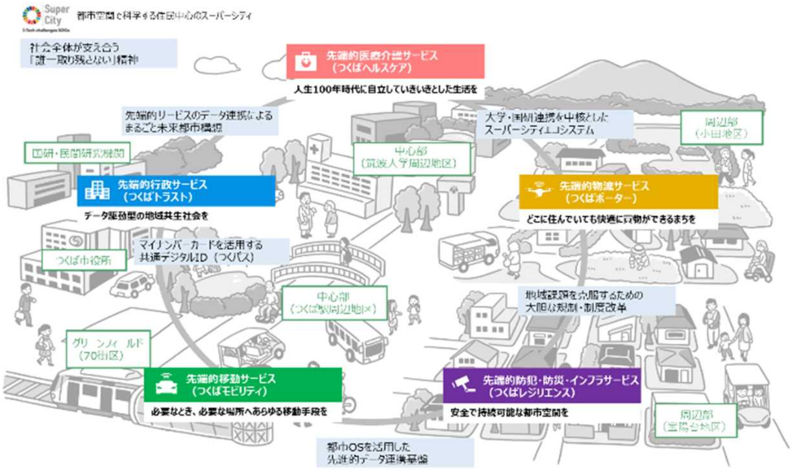


図１　つくばスーパーサイエンスシティ構想

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。こういった不安感が蔓延している環境下では、市民はデータの提供を拒み、利活用を図りたいデータが収集されないという事態に陥りかねない。

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片手落ちであり、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、構想を成功裡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。

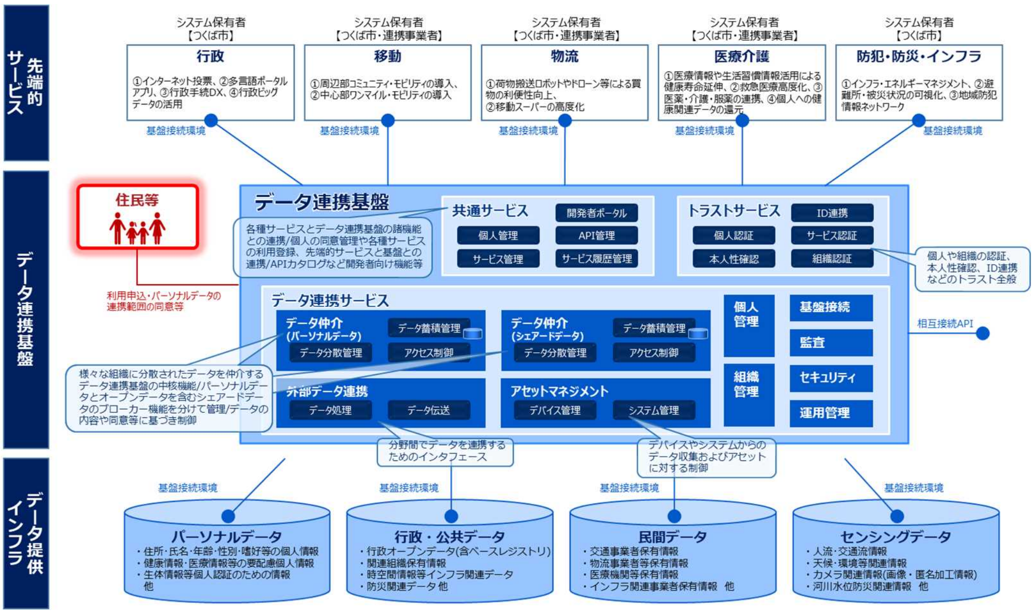


図２　データ連携基盤の活用イメージ

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

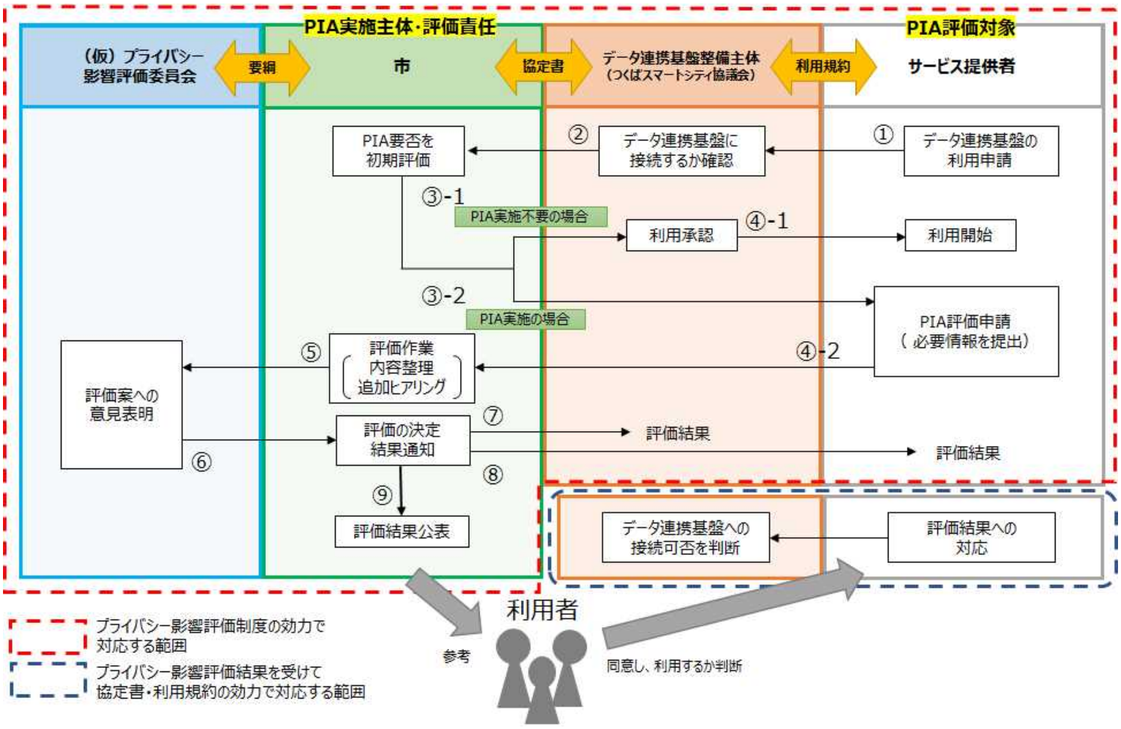


図２　PIA 実施体制（全体像）

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。

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、両者の最も大きな違いは、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。

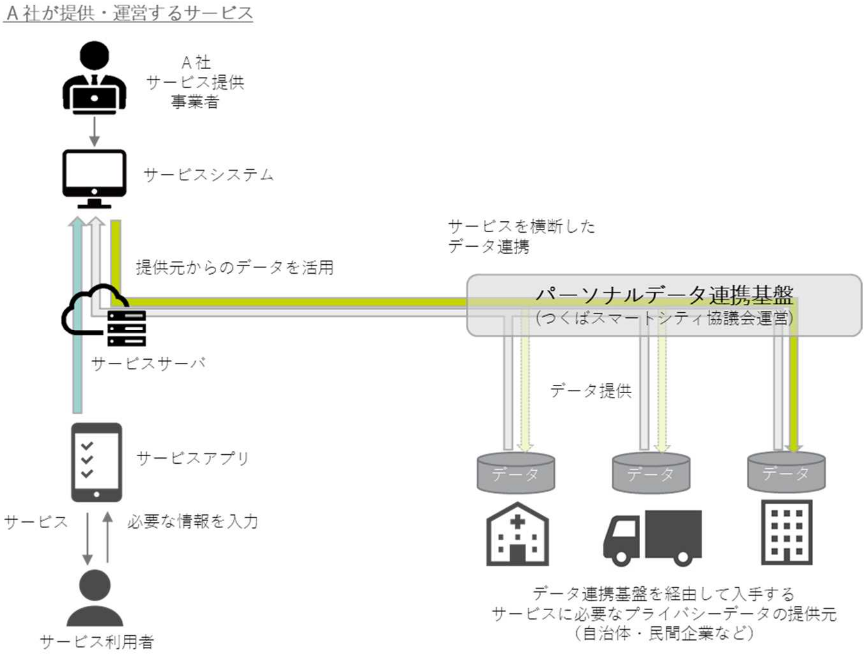


図３　PIA 評価の対象範囲のイメージ [5]

1.2.2　初期評価

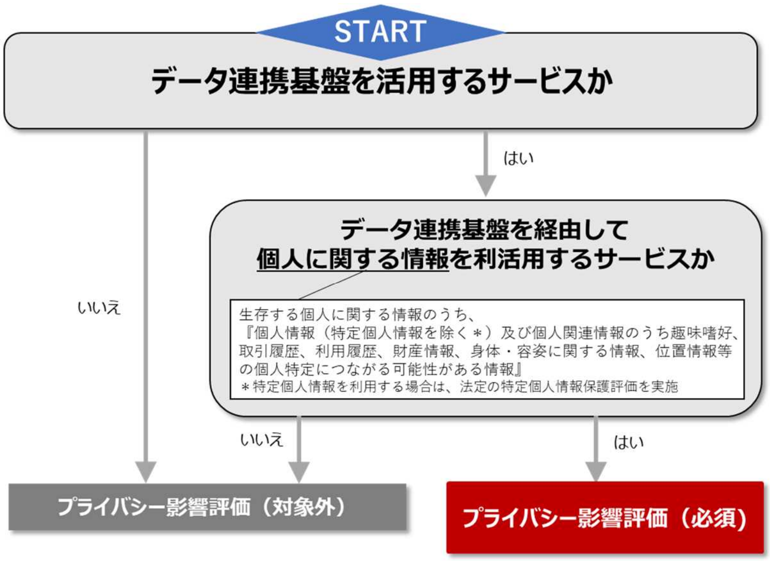


図４　PIA 要否を判断する初期評価の流れ

---

[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「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、その仕組み全体を評価するのではなく、当該サービスに関係するデータのやり取り、取り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」はその情報そのものだけでは個人の特定に繋がりづらいものの、他の情報と紐づくことで個人の特定が可能な情報が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」を特定の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」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●「評価項目一覧」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・財産・精神の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「JO モデル」[6]を参考にした。JO 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。

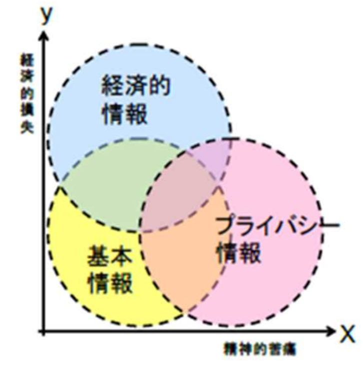
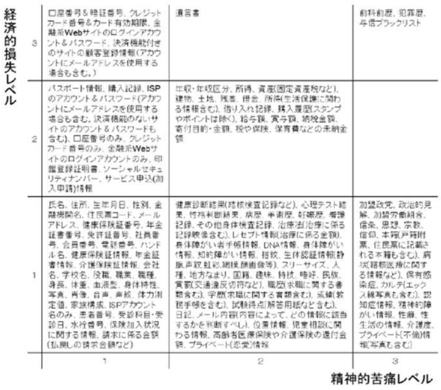


図 5-2：EP 図（Economic-Privacy Map）



経済的損失レベル

3	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（アカウントにメールアドレスを使用する場合も含む。）	遺言書	前科前歴、犯罪歴、与信ブラックリスト
2	パスポート情報、購入記録、ISPのアカウント＆パスワード(アカウントにメールアドレスを使用する場合も含む。決済機能のないサイトのアカウント＆パスワードも含む)、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、ソーシャルセキュリティナンバー、サービス申込(加入申請)情報	年収・年収区分、所得、資産(固定資産税など)、建物、土地、残高、借金、所得(生活保護に関わる情報含む)、借り入れ記録、購入履歴(スタンプやポイントは除く)、給与額、賞与額、納税金額、寄付目的・金額、税や保険、保育費などの未納金額	
1	氏名、住所、生年月日、性別、金融機関名、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、社員番号、会員番号、電話番号、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、会社名、学校名、役職、職業、職種、身長、体重、血液型、身体特性、写真、肖像、音声、声紋、体力測定値、家族構成、ISPアカウント名のみ、患者番号、受診科目・受診日、水栓番号、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)	健康診断結果(結核検査記録など)、心理テスト結果、性格判断結果、病歴、手術歴、妊娠歴、看護記録、その他身体検査記録、治療法(治療に係る記録映像含む)、レセプト情報(治療に係る金額)、身体障がい者手帳情報、DNA情報、身体障がい情報、知的障がい情報、指紋、生体認証情報(静脈声紋虹彩網膜顔画像等)、スリーサイズ、人種、地方なまり、国籍、趣味、特技、嗜好、民族、賞罰(交通違反切符など)、職歴(求職に関する書類含む)、学歴(求職に関する書類含む)、成績(教務手帳を含む)、試験得点(解答用紙など含む)、日記、メール内容(内容によって、どの情報に該当するかを判断すべし)、位置情報、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	加盟政党、政治的見解、加盟労働組合、信条、思想、宗教、信仰、本籍(戸籍附票、住民票に記載される本籍も含む)、病状(結核医療に関する情報など)、保有感染症、カルテ(エックス線写真も含む)、認知症情報、精神的障がい情報、性癖、性生活の情報、介護度、プライベート(不倫)情報(写真も含む)
	1	2	3

精神的苦痛レベル

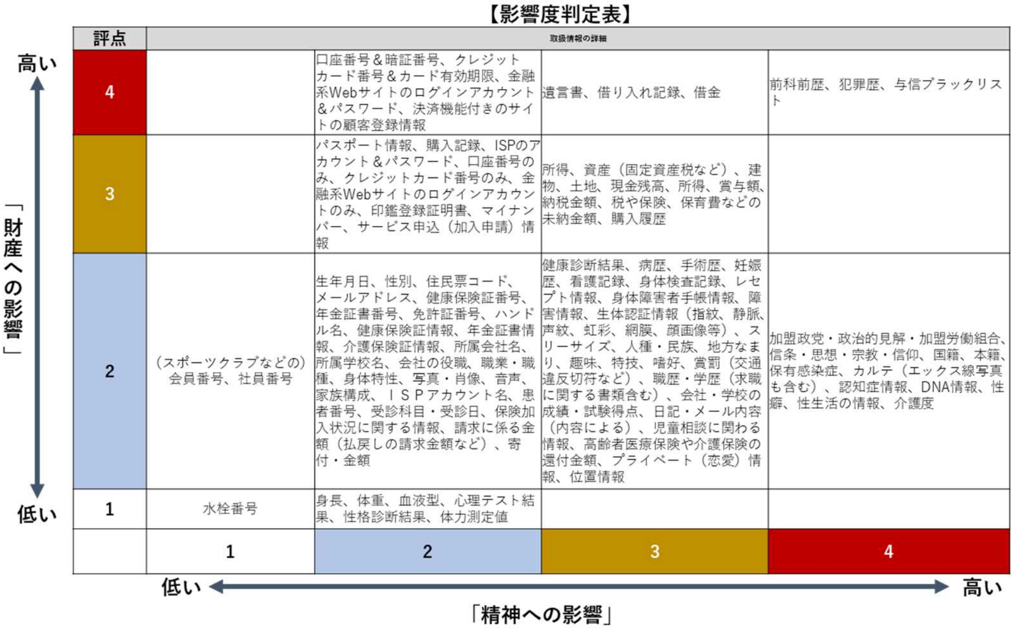
図 5-3：シンプル EP 図

【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」

---

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

J0 モデルを参考に、本懇話会で検討したものが別表●「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】

評点	取扱情報の詳細			
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		
	1	2	3	4

＋

「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●「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●「評価項目一覧」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	

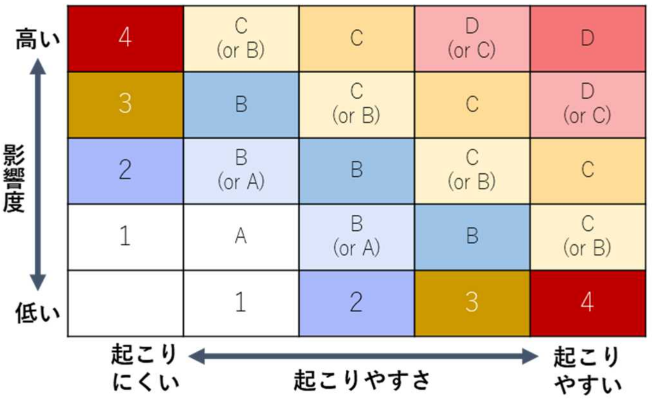
⇒ 「必須」についてはすべて対応済である一方で、「推奨」の２項目（⑤と⑥）が未対応のため、評価項目 No.13 の起こりやすさの評価は、ベースラインとなる１に、未対応で加点となる＋２を加えて「３」

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。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。



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

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●『「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●　「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、より上位（査定としては悪い）の評価とすることを原則としつつも、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て、実情に応じて総合的に判断することを評価委員会で議論のもと可能にするなど、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
- サービス利用者の代表（市民）

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

---

[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

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）及び利用者の、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、虚偽の申告に端を発して他者に不利益を生じさせた場合は、それに対する一切の責任を負う。

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

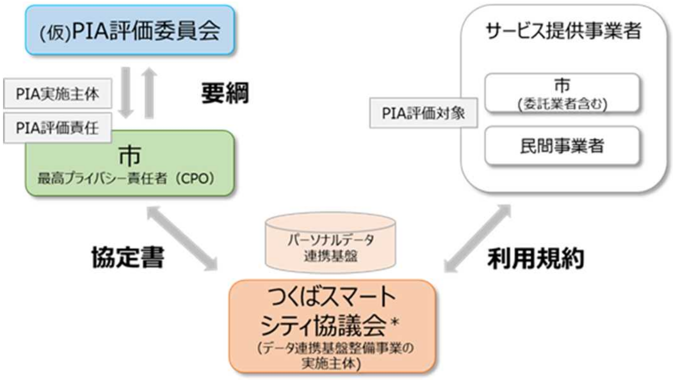
ーインシデント発生時の責任範囲については、PIA 評価の有無に関わらず、プライバシーインシデントを原因として発生した損害に応じて、法的根拠に基づき判断されるものである。

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●　PIA 制度の実効性を担保する仕組み

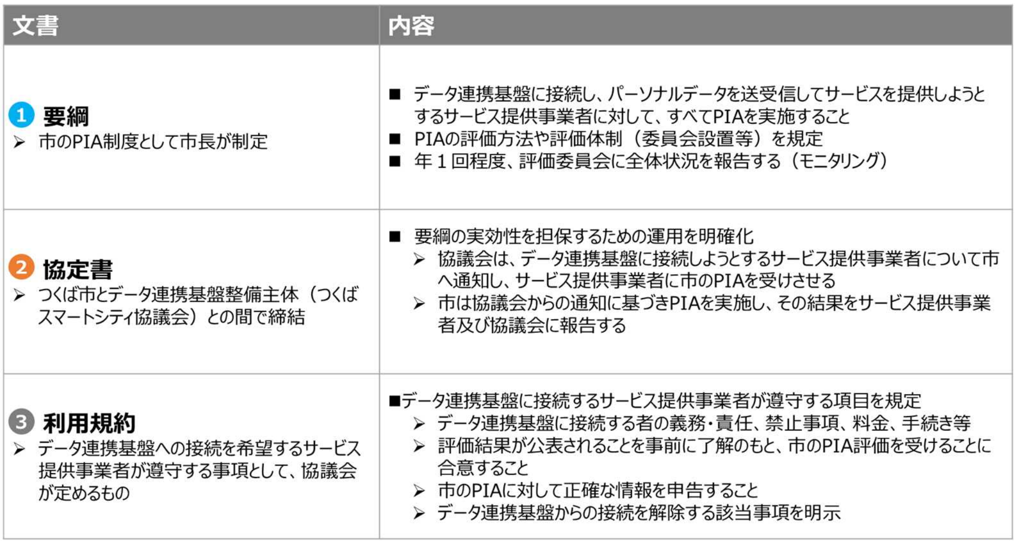
「要綱」「協定」「利用規約」が規定する具体的な条文内容については、市の責任において具体化を図るものと承知しており、本懇話会では実効性を担保するために、これらにどのような事項を規定するべきかという範囲で議論を行った。

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。

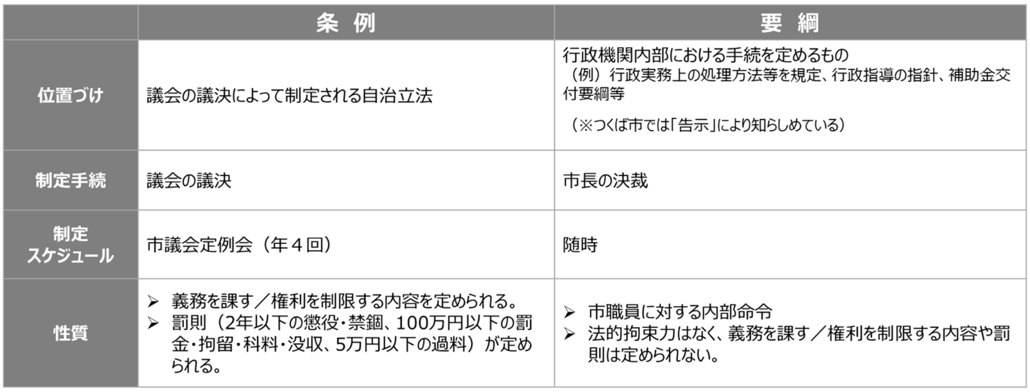
本件については PIA 制度の外側の、市と協議会間の整理の問題であり、本懇話会としては一定の結論を纏めることはせず、最終的な考え方の整理は市の判断に委ねるが、検討に当たっては様々な意見があるということを念頭に置きつつ、PIA 制度の実効性を担保するために、要綱・協定・利用規約にどのような規定を盛り込むかについて慎重に検討されたい、という点を本懇話会として申し送りたい。



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

【表●】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。

表●　「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。

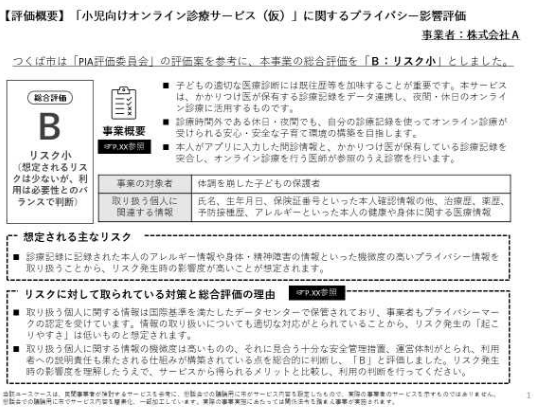
また、総合評価の結果については評価書の形で対外的に公表する。公表にあたって最も重要なことは PIA 評価の内容を市民に理解してもらうことであり、評価書では専門用語や難解な表現を避け、市民に分かりやすい言葉を使用することが重要であることが懇話会においても繰り返し議論された。

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
☞P.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

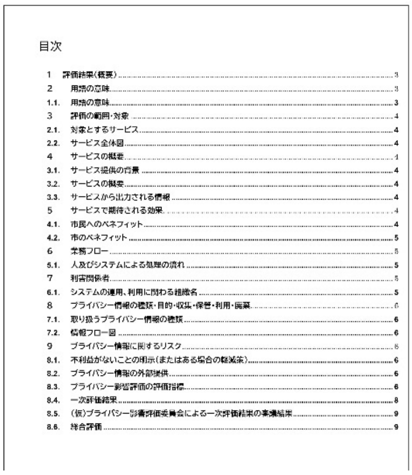
想定される主なリスク

■ 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 ☞P.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。

1



目次

【図●】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た場合であり、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

修が生じた場合、サービスを提供・運営する体制変更が生じた場合、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った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のレベルが変わ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等が想定される。

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

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

---

[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

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。

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（案）概要版　目次

0　はじめに

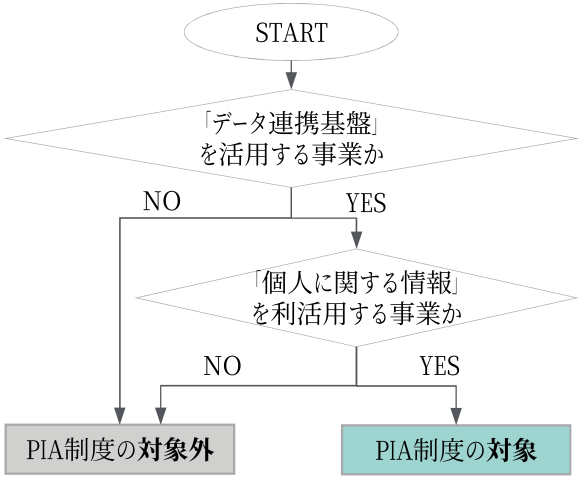
- 本書は「つくば市プライバシー影響評価制度検討懇話会」にて協議・検討した事項を踏まえ、つくば市が確立すべき「プライバシー影響評価制度(以下、PIA制度)」の方向性について一定の整理を行い、取りまとめた概要書である

- なお、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

- また、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

1　初期評価／評価対象／実施のタイミング

初期評価


START

「データ連携基盤」
を活用する事業か

NO

YES

「個人に関する情報」
を利活用する事業か

NO

YES

PIA制度の**対象外**

PIA制度の**対象**

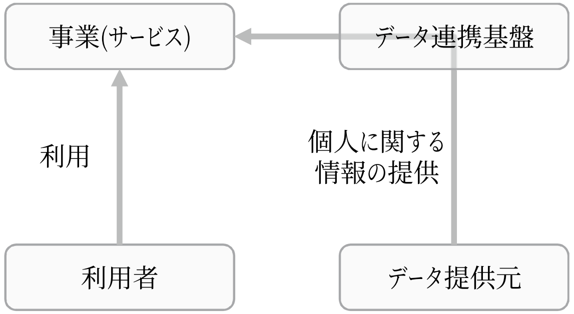
図1 PIA要否を判断する初期評価の流れ

- 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


事業(サービス)

データ連携基盤

利用

個人に関する
情報の提供

利用者

データ提供元

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**

なお、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「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、その仕組み全体を評価するのではなく、当該サービスに関係するデータのやり取り、取り扱いに関する部分が評価対象

タイミング

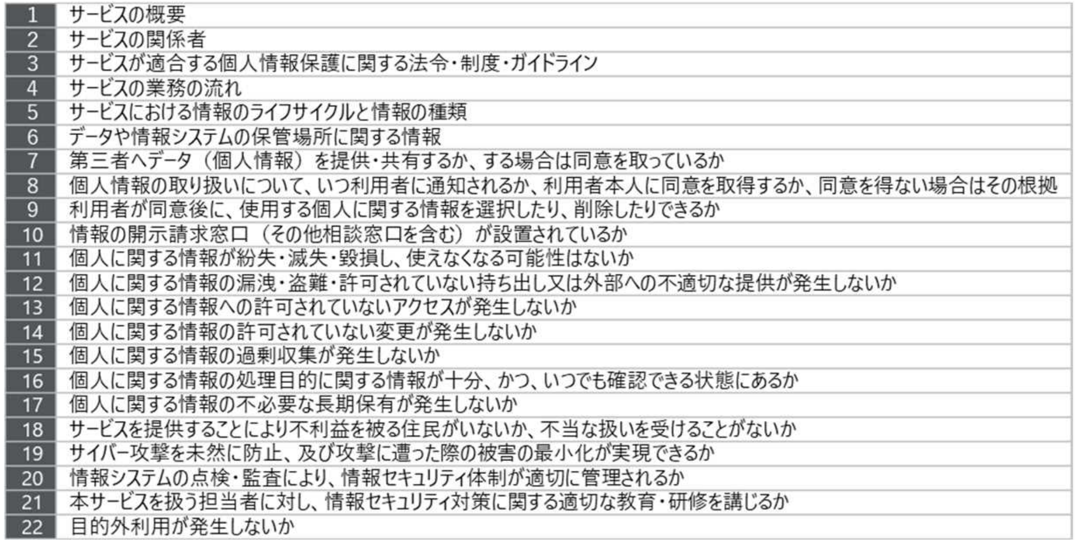
- PIAを実施するタイミングについて、「**初回**」･「**再評価**」の２点について検討
  - ➢ 「初回」は、評価の結果次第で措置を講じる必要が出てくるため、詳細な設計･開発に取りかかる前が費用対効果等の観点から推奨
  - ➢ 「再評価」は、提供中のサービスに大幅な仕様変更等、PIA制度に大幅な見直しが生じた場合が該当 (詳細は「４運用」にて後述)

2　評価項目／評価基準①

評価項目

- 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に実施する

[1] JIS X 9251, GSCA PIAモデルポリシー, 特定個人情報保護評価 等



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

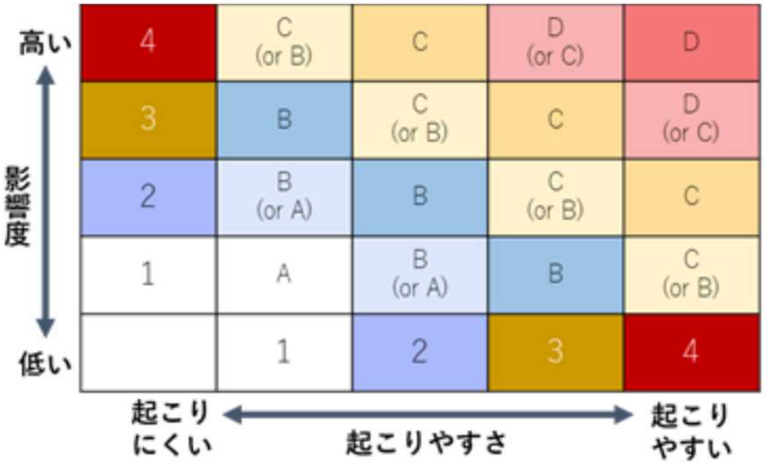
評価基準

- 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

影響度（1～4） ✖ 起こりやすさ（1～4） ➡ 総合評価（A～D）

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）



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

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

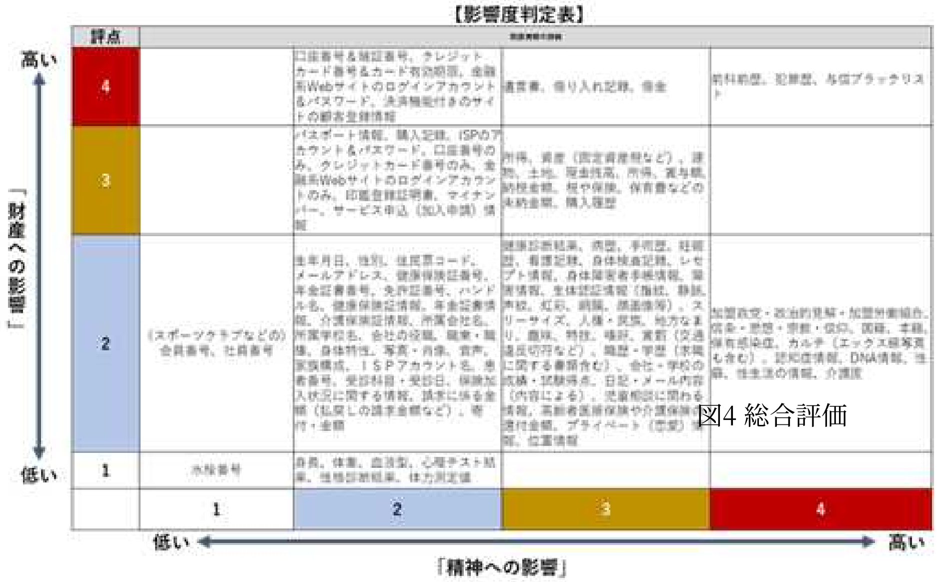
評価基準

【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



評点				
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	請求書、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、貰与額、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給付金額、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	[illegible]	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		
	1	2	3	4

図4 総合評価

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

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

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

【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点加点し、３つ以上対応できていない場合は最大４点

3　評価体制における役割･責任／実効性の担保

評価体制における役割・責任

- 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

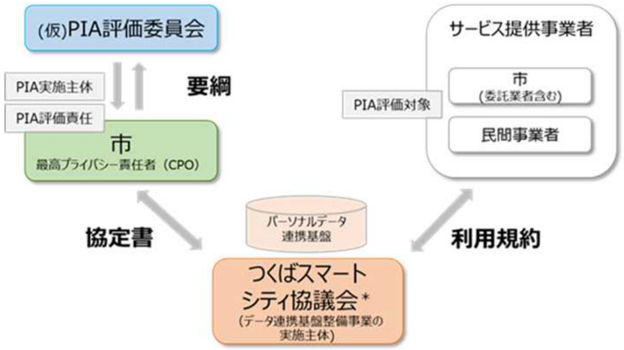


図8 評価体制のイメージ

図9「PIA制度」における責任分界点

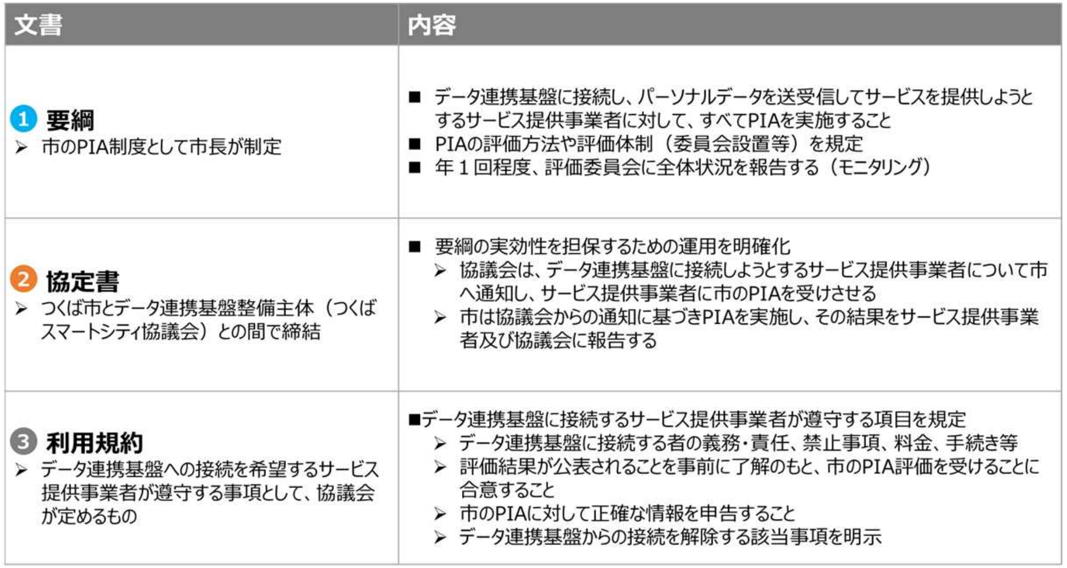
市	• PIA評価結果及び、制度運用にかかる<u>**説明責任を負う**</u>
サービス提供事業者	• PIA申請内容に関する<u>**責任を負う**</u>
データ連携基盤整備主体（協議会）	• サービス提供事業者に対してPIA評価を実施させる<u>**責任を負う**</u> ※なお、再評価の実施要否においてはサービス提供事業者の責任が問われる場合もあるため、この限りではない
利用者	• ―（なし）

※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

別途協議(論点①)

実効性の担保

- 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
  - 市ー協議会：「**協定**」
  - 協議会ー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



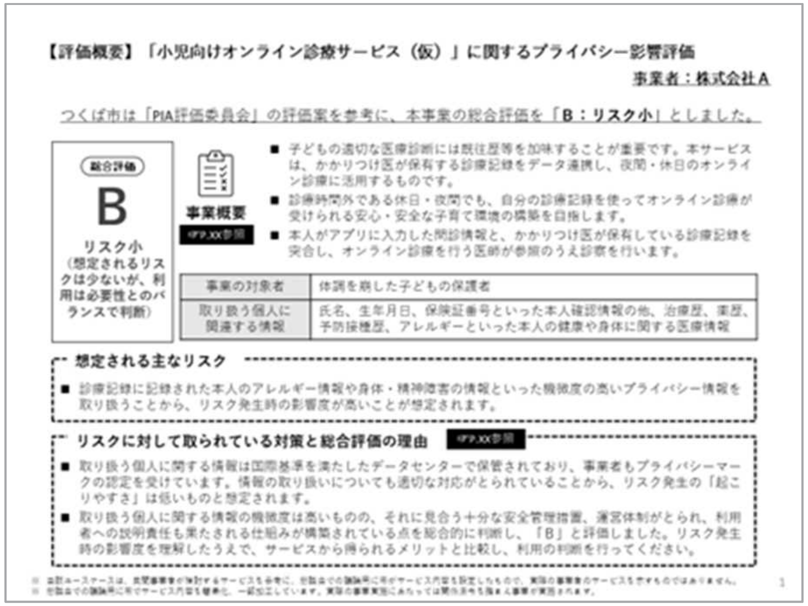
文書	内容
① **要綱** ➢ 市のPIA制度として市長が制定	■ データ連携基盤に接続し、パーソナルデータを送受信してサービスを提供しようとするサービス提供事業者に対して、すべてPIAを実施すること ■ PIAの評価方法や評価体制（委員会設置等）を規定 ■ 年１回程度、評価委員会に全体状況を報告する（モニタリング）
② **協定書** ➢ つくば市とデータ連携基盤整備主体（つくばスマートシティ協議会）との間で締結	■ 要綱の実効性を担保するための運用を明確化 ➢ 協議会は、データ連携基盤に接続しようとするサービス提供事業者について市へ通知し、サービス提供事業者に市のPIAを受けさせる ➢ 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

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

結果の通知と公表

- 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、利用は必要性とのバランスで判断）

事業概要
→P.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　→P.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。

図11 評価報告書（概要版）のイメージ

別途協議(論点②)

運用

- 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**」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、サービス提供者に体制変更がある場合

有効期間	制度運用において発見される課題
• 将来的には、時代の変化とともに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

参考情報

- 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：プライバシーに関する炎上事例、個人情報漏洩 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

資料３

３　残論点について（①責任分界点）

＜これまで＞

- 前回の懇話会では、評価結果の公表にあたり、PIA評価報告書の書きぶりを気を付けないと、「市」がサービスに対する安全性を保証しているように映りかねない点についてコメントいただき、**責任分界点**について従前の懇話会において十分に協議・検討できていない認識である

＜考察＞

- 本懇話会で明確にすべき責任分界点は「PIA制度」であるため、以下の切り口から分けて整理

A)「PIA制度」における責任分界点

B)「PIA制度“外”」における責任分界点（具体的には、プライバシーインシデント原因として発生した損害における責任分界点 等）

＜論点＞

- 以下の**考え方・整理に違和感ないか**、また、今後公表を予定している内容となるが、**市・協議会のスタンスについて対外的な見え方として懸念等ないか**等、意見頂戴できればと考える
- なお、責任分界点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ため、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）」として明示すること等を検討する

	A.「PIA制度」における責任分界点	B.「PIA制度“外”」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**	• 明記しない（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と考えられるため）
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	• ー（なし）	

資料3

3　残論点について（②再評価の実施基準）

＜これまで＞

- 前回の懇話会では、「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)や新技術開発に伴う大幅な仕様変更がある場合は、再評価を実施」を基準案として提示

＜考察＞

- 前回案の書きぶりでは多くのシステム改修が再評価を求められるのではないかとのご指摘を受け、**例示等を追記することで基準を明確化**するとともに、再評価の実施基準について**網羅性の観点から再検討**

【網羅性の観点】

- 再評価が必要となるケースとは、PIAの総合評価（A～D）が変わる可能性が見込まれる場合が想定
  - ✓ 影響度：「データの種類」に変更が生じる場合
  - ✓ 起こりやすさ：「調査項目」への回答に変更が生じる場合
- 上記に変更が生じる場合として、以下２パターンが想定
  1. 「**サービス**」に変更等が生じた場合
  2. 「**PIA制度**」に変更等が生じた場合

＜論点＞

- 考察を踏まえ見直した、以下案について、**内容の網羅性や例示の妥当性**、サービス提供事業者が当該内容を確認し、**再評価の申請を過不足なく行えるか否か**について意見を頂戴できればと考える
- また、ポジティブな変更時（ex. 強固な安全管理策を追加的に講じる等）は運用を考慮し、簡易的な再評価に留める方向にて検討中
- なお、現断面では「運用」を検討し尽すことは難しいものの、将来的には、定期評価する「更新性」への移行を含めて継続検討する

i.　「サービス」に変更等が生じた場合[*1]	ii.　「PIA制度」に変更等が生じた場合[*1]
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、サービス提供者に体制変更がある場合は、再評価を実施 例えば、「大規模なシステム改修」とは、取扱情報のレベルが変わるデータを収集開始する場合やオンプレからクラウドへサーバ移行する場合、「サービス提供者に体制変更」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、等が該当する	法令・ガイドラインの改訂や社会の動き等により、PIA制度の大幅な見直し（評価項目や評価基準等に変更）が必要となった場合は、市として十分に検討した上で、再評価を実施する場合がある 例えば、「法令・ガイドラインの改訂」とは、個人情報保護法の改正等により、新たに考慮すべきプライバシー要件が追加となった場合、「社会の動き」とは、新技術の開発等により現行の評価項目・基準では評価が難しいケースが生じた場合、等が該当する

[*1] 青字は第６回懇話会にて提示した実施基準（案）からの加筆・修正箇所

会　議　録

<table>
<tr><td colspan="2">会議の名称</td><td colspan="3">第８回つくば市プライバシー影響評価制度検討懇話会</td></tr>
<tr><td colspan="2">開催日時</td><td colspan="3">令和７年(2025年)２月14日　開会17：00　閉会18：00</td></tr>
<tr><td colspan="2">開催場所</td><td colspan="3">つくば市役所　本庁舎５階　庁議室
（オンライン併用）</td></tr>
<tr><td colspan="2">事務局（担当課）</td><td colspan="3">政策イノベーション部　科学技術戦略課</td></tr>
<tr><td rowspan="3">出席者</td><td>委員</td><td colspan="3">坂下座長、落合座員、鯉沼座員、鈴木座員、平山座員、髙橋座員、水町座員</td></tr>
<tr><td>その他</td><td colspan="3">つくば市　五十嵐市長
（オブザーバー）
内閣府地方創生推進事務局 牟田企画調整官、畠中研修員
デロイトトーマツサイバー合同会社　三谷氏、林氏</td></tr>
<tr><td>事務局</td><td colspan="3">政策イノベーション部
　稲葉次長
政策イノベーション部　科学技術戦略課
　中山課長、大垣課長補佐、高橋課長補佐、工藤データ連携推進監、金塚係長、金山係長、東泉係長、藏内主事、松好研修員</td></tr>
<tr><td colspan="2">公開・非公開の別</td><td>■公開　□非公開　□一部公開</td><td>傍聴者数</td><td>０名</td></tr>
<tr><td colspan="2">非公開の場合はその理由</td><td colspan="3">ー</td></tr>
<tr><td colspan="2">議題</td><td colspan="3">(1) 最終とりまとめ（案）について</td></tr>
<tr><td>会議次第</td><td colspan="4">１　開会
２　議事
(1) 最終とりまとめ（案）について
３　その他
４　閉会</td></tr>
</table>

１　開会

事務局（中山課長）：それでは定刻となりましたので、ただいまから第８回つくば市プライバシー影響評価制度検討懇話会を開会いたします。本日の座員の皆様のご出席は、現地が５名、オンラインが２名（落合座員、水町座員）となっております。なお、本日冨田様、橋本様はご都合によりご欠席でございます。また、内閣府地方創生推進事務局から牟田様、畠中様、今年度のPIAの制度検討について連携しているデロイトトーマツサイバー合同会社からは、三谷様、林様が出席されております。そして本日は市長の五十嵐が出席しておりますので、一言ご挨拶申し上げます。よろしくお願いいたします。

市長：この度は、素晴らしいまとめをしていただきまして本当にありがとうございます。もちろん、これまでのすべての会議録もすべて読ませていただいていました。間違いなく前例がないPIAの仕組みとして、今後の各自治体のよすがになるのではないかと思っていますし、私がすごく感銘を受けたのは、専門家ではなくとも、見て直感的にもわかりやすいということだと思っています。当然、市民がその判断をする際に、何のことかわからないような仕組みであってはいけませんから、こうやって縦軸横軸をとって、ここではこういうものなのだな、自分がこういう判断をするのだなということが見えることはすごく大きいと思いますし、その意味で、専門家の皆様と市民の皆様が議論をしてよかったとありがたく思っています。実は先日、デジタル大臣の平さんとちょっと会うことがあって、その時に、個人情報の話をいろいろしたので、実は今こういう仕組みをつくば市で作っていて、国の会議に入るような専門家の先生方と市民が一緒になって議論をしていると話をし、一度オンラインで中間の取りまとめ内容を簡単にレクさせてもらいました。そうしたところ、良いねということで、4月にデジタル行財政改革会議で、このPIAを私から簡単に説明させていただくことになりました。すでに国としてこういうものがあるということは、価値があると思いますし、デジ庁や国全体、当然その先に自治体もありますし、そういう場所でデータの取り扱いについての大きな羅針盤になっていくのではないかと思っていますので大変感謝をしています。これだけ素晴らしいものを作ってくださいましたので、

ここから制度化をして、運用していくというのが役所側の責任であり、大変だからこそやる価値があると思いますし、どうやって実効性のあるものにしていくか進めていければと思っています。本当に良いきっかけと良い内容のものを作ってくださったことを改めてお礼申し上げます。本当は最後までいて皆様と議論したいのですが、今日もうすでに始まっている別の会合がありまして、そこに遅刻してでも、１秒でも早く来いと言われているので、冒頭のみで大変残念ですけれども、ぜひこれから今日の最後の議論を経て、また取りまとめをしていただければと思っております。本当に今までのご尽力に感謝申し上げます。ありがとうございました。

事務局（中山課長）：ありがとうございました。市長はこちらで退席させていただきます。それでは、早速ですがここからは、つくば市プライバシー影響評価制度検討懇話会設置要項の規定に基づき、座長に進行をお願いしたいと思います。坂下座長、よろしくお願いします。

坂下座長：今日が最終回となりますので、よろしくお願いいたします。本日の議事は１件です。ここで、会議の公開・非公開についてですが、「つくば市附属機関の会議及び懇談会等の公開に関する条例」により法令又は条例で定めがある場合を除き、原則公開となります。本日の懇話会は非公開事由に該当しないため、公開で進めてまいります。また、会議記録のため事務局でzoom録画及び写真撮影をさせていただいておりますことご理解ください。

２　議事

(1) 最終とりまとめ（案）について

坂下座長：それでは、議題に入りたいと思います。「議事(1)　最終とりまとめ（案）」について、事務局から説明をお願いします。

〔議事(1)について事務局から説明〕

坂下座長：ご説明どうもありがとうございました。最終回ですので、一通り取りまとめられておりますし、挙手方式で15分程度時間を取って皆様から意見をいただきたいと思います。ご意見のある方は挙手をお願いします。オン

ラインの方も挙手機能でお願いします。いかがでしょうか。平山座員お願います。

平山座員：まずは事務局、本当にお疲れ様でした。取りまとめ大変だったと思います。先ほど市長もお話しされていましたけど、これ自体は今後も変わり行くものだと思いますし、どういう事例が出てきてどういうふうにPIAをやって、それがどういうふうにPDCAで正しく変わっていくか、みんなが使いやすいようにしていくかというところも含めてやっていく必要があると思います。そういった意味では、これで終わりというよりはスタートだと思います。一方で、データ連携基盤を活用したところで、本当にそれで良いのかという議論も後々出てくるでしょうし、少なくともデータ連携基盤を活用した事業というものが、今後どういうものが出てくるかによっても変わってくると思います。ここはしっかりとやっていく必要があると思います。全体としては、私は異論なく、やっとですねという感じがしています。

坂下座長：ありがとうございます。他ご意見いかがでしょうか。オンラインの先生方いかがですか。水町座員お願いします。

水町座員：まず、このとりまとめ案を拝見しましたが、とてもしっかりした文章で丁寧に書いてあって、文章力が高いと思いました。大変だったと思いますが、きれいにまとめていただいてありがとうございます。私からは、とりまとめ案の「2.1　座員の主な意見」のところで追加していただきたいところが２点あります。まず、別表１の影響度について、JNSAのモデルも書いていただいておりますが、これ自体そもそも多くの人のコンセンサスを得て４とか３とか決まっているものでもないので、別表１の影響度判定表も、フレキシブルに評価委員会で見直していただきたいというのが１点。あともう１点は、起こりやすさについての意見ですが、今の案ですと、通常やるであろう対策ができていれば発生しにくいという評価になるので、その是非であるとか、対策項目等についても、評価委員会できちんとレビューいただきたいというのを意見として追加いただきたいと思います。あと何点か細かい点をお伝えしたいのですが、別添１の評価項目一覧について、※で書いていただいたのでそれで基本的に問題ないと思うのですが、No.09も※が必要だと思います。というのも、同意後に使用する個人に関する情報を選択したり削

除したりできるかということは、そういうサービスはけっこう難しく、あまりユーザーが直せないもので、プロフィール等しか直せないものが多いです。だから、全部の情報を削除とか選びなおすとかはなかなか難しいので、これが必須になると満たせない事由がけっこう多いのではないかということです。同意後だったら、1回同意した後にまた直すとなるとシステム作りに影響が出てしまうというところです。法律上は第34条、第35条になっていますが、法律はもっとゆるく、このNo.09の文に書いてあるようなことまでは要求されていないので、※表記等で工夫していただいたほうが良いのかなということです。あと、No.16の①について、第32条であれば備え置きとかでも良いはずで、法律上の要求よりちょっと柱書きが厳しい可能性があって、本人の求めに応じて回答しても良いはずです。「等」と書いてあるが、いつでも閲覧できなくても、その本人が求めればすぐ出すという状態でも適法なので、必須だと少し厳し過ぎるかもしれない。そのあたりの表記を調整いただければと思います。細かくて恐縮でした。私からは以上です。

坂下座長：ありがとうございます。影響度や安全管理措置のところは意見として追加することは特に問題ないと思いますし、あと今のところの２つもつくば市の想い次第ですけど、我々が厳しくやるんだとなれば必須で頑張るということもありますが、これからサービスを作っていく話なので、必須でなくても良いかなとは思います。他ご意見ございますか。落合座員お願いします。

落合座員：今回まで丁寧に議論をまとめていただき、とりまとめも本文だけではなく、中間的な概要と、1枚ものと、しっかり作っていただき、見た方に1枚だけでもわかってもらえる形でしっかり完結していただきました。皆様に改めて、ご尽力に感謝申し上げたいと思います。私は、とりまとめの内容そのものについては、細かい意見はないですが、今後の運用に関してコメントさせていただきます。先ほど水町座員にお話いただいたような、比較的細かいけれど、若干法令の内容と違うところについて、実際に運用して、あまり現実的ではないものが出てくる可能性も否定できないと思います。ですので、これをメンテしていくこと自体も必要だと思います。その時に毎回このレベルの会議を開催されていると辛すぎる気もするので、特に技術的な事項

等については、どこまでいくと技術的なのかは若干判断が入るところがあると思いますが、運用状況を見て見直しをしていただくと良いと思います。その時にあまり重過ぎる手続きを踏まずに実施いただくことも、現実的な運用としては大事だと思いますので、ぜひ、そういった視点でお願いいたします。一度定めてしまったから変えられないというわけではなく、運用しながら良いものにしていただきたいと思います。もう１点、先ほどの点は細かい話でしたが、もう少し大きい意味で言いますと、個人情報保護法等については、本年改正されるかどうかはともかく、今後改正されることがあると思いますし、その中でルール自体が変わっていくこともあるでしょう。また、昨今の生成AIによってもいろいろ変わってくると思います。先ほど、法技術的な事項は申し上げたのですが、ルールや社会環境も変わる可能性がありますし、AI事業者ガイドライン等の中でも入れているようなアジャイルガバナンスでも、運用を回すだけではなく、ルール自体の妥当性も見直し続けることが大事だというコンセプトであります。それも大きい意味でのルール変更ということで大事になってくると思いますので、必要に応じて実施していただきたいと思います。最後に、運用にあたって、個別の案件の審査や評価が今後出てくると思いますが、もうすでにフォーマットができていて、わかりやすい形になっていますが、特に見やすさやどういうふうにアクセスできると良いかということは、ここで議論している委員の言葉以上に、直接ユーザーになる市民のご意見を聞いたり、接したりする中で出てきて、よりこういう方法があるのではないか、こういう情報は公開していくと良いのではないかというものをぜひ見つけて、市民の対話のきっかけになるような形で、わかりやすい運用を心がけていただけると良いと思います。

坂下座長：ありがとうございます。鈴木座員お願いします。

鈴木座員：水町座員にお伺いしたいのですが、確かにこのNo.09は課題になるところですが、削除ができる、同意を撤回する、同意しないという要件がどこに書かれているかお伺いしたいと思いました。実運用としては我々のところでも、大体最低でも15日とか30日とか日付を決めて、その期間までは同意撤回ができますと明示して、それで運用しているのが現状です。水町座員がおっしゃる通り、ある一定期間以上そのシステムに入れてしまったらもう

動かせないということもあるし、かと言って、同意したらもう撤回できないということで、一定期間おいて同意撤回はできると、ただそのあと同意撤回できませんということをしても、このNo.9というのは、そういう理解で満たされるということになりますでしょうか。水町座員に対するご質問です。

水町座員：大学の研究では、同意撤回についてきちんと書いていただいて、それ自体とても良いことです。けれども、個人情報保護法では、同意撤回については規定がなく、同意を得て第三者提供したり目的外利用したりすることはできると書いてありますが、その撤回がいつでもできるような権利を保障しなさいということは法律には入っていません。したがって、法律の要求事項ではないです。ただ、法律というのは守らなければいけない最低ルールで、そこから上乗せしていくことはいくらでもできて、例えばPマークは法律より上乗せしていることと理解しています。だから研究でも、同意撤回についてきちんと説明文章の中にも入れ込んでいるのだと思います。ここのNo.09で柱書いただいているのも、プロフィールの変更やSNSでの投稿修正ができるものをイメージして書いていると思いますが、極論言うと、全部撤回できるかはなかなか難しい。1回同意して提供しているデータを取り戻すことはけっこう難しく、すでに匿名加工していると思うので、誰の情報かわからない状態で、同意撤回されてもそこからは戻せないと思います。やはり、そういう疑義がないように柱書をする必要があると思います。だから鈴木座員がおっしゃった通りです。現実的に不可能で、非常に困難な場合もありますが、同意撤回を認めるべきという、本人の権利に配慮してやっていらっしゃること自体はすごく良いことですので、ぜひPIAでもやるのであれば、ここまでやらなくても当てはまる程度にしておいた方が、PIAとしてはきれいなのかなと思います。あまりにも要求レベルが高く、「推奨」であれば良いが「必須」となると、きついと考えております。

鈴木座員：よくわかりました。大学もきちんとやっていることがわかって良かったです。わかりやすい具体例ですと、データを取ってそれをAIに学習させたら、その人のデータを使わなかったと言えなくなるので、一旦同意撤回の期限を設けて、ここから先は消せないところに入りますよという感じで、30日とか期日を決めてやっている現実運用があるので、そういう知見も含

めていけるようにしたいです。私も水町座員の意見に全く同意で、今回フレームワークはしっかりできましたが、この評価項目一覧等は、それぞれの法律が変わるとか、時代によって要求が変わるということも含んだ上で進められるのが良いなと。審査ではなく評価という言葉の言い回しですが、審査をして合格不合格というものではなく、あくまでも評価をするものということで、議論にもありましたが、Dでもやらなければいけないことが世の中にあるということがわかります。明示しなくても良いですが、普通の人からしたら信じるしかないレベルの量が書いてあるわけです。それをどうやって信じるのかというと、通常は最後のページを見るわけで、誰がこれをやったのかと。座員のメンバーは、市民、専門家、大学等も入っている、その上でつくば市が実施するのであれば、信頼できるだろうということ程度しかわかりません。しかしこれは本当に大事なことで、これを課していくことで我々がステークホルダーである市民との信頼関係を築くためにやっているかが伝わるような、結果の公表だけではなく、これは単に事業者を縛るものでもなく、Bだからやって良いとかCだからやって良いというような法律的なものでもなく、サービスに対して客観的にどういうリスクがあるかを示せるものです。一番の目的は、市民との信頼関係を築くためにやっていることが伝わることだと思いながら見ておりました。ただ、分野によっては、評価することが信頼になる分野もあるので、審査ではないということが通じない場合もありますが、あくまでも合格不合格のためではないということは伝えていく必要があると思います。

坂下座長：ありがとうございます。以上の皆様からの意見について、事務局で反映を検討していただき、最終的に座長の私に一任いただく形でよろしいでしょうか。ありがとうございます。それでは私の方で最終確認の上、「最終とりまとめ」とします。本日で本懇話会は最後となりますので、これまでご議論いただいた内容を踏まえた最終とりまとめを市へ提出いたします。そこで全８回の懇話会を振り返り、市への期待・要望・感想等お一人ずつご意見を伺いたいと思います。構成員名簿の順番にご指名いたしますので、落合座員から順番にいきたいと思います。

落合座員：先ほど最後に言うべきことを言ってしまったので、なかなか難しい

ところがありますが、先ほど申し上げた通り、フレームは良いものができていると思います。今後は、フレーム自体の運用を充実させていくことも大事です。これまで、個別のケースを念頭に置いた議論もしてきましたし、様々な視点での議論があったと思いますが、実際につくば市で運用していく中で、運用する方の経験が蓄積されていくことも改めて大事だと思います。運用の経験についても、どこかの機会で振り返っていただければと思います。フレームを運用するのは人なので、能力の向上や経験の蓄積も非常に大事で、今後担当になる方にしっかり引き継いでいただきたいと、つくば市にはお願いしたいです。改めて、8回の議論どうもありがとうございました。

坂下座長：ありがとうございました。続きまして鯉沼座員お願いします。

鯉沼座員：私は市民委員として2年ほど参加させていただきました。参加しようと思い立った経緯としましては、自宅に市民委員に興味ありますかというハガキが来て、当時は何も考えずチェックをつけたのですが、大きいプロジェクトに携わることができて、今となれば、あの時チェックしておいてよかったと感じております。私自身あまり専門的な分野ではなかったこともあり、正直、前半のディスカッションについては概念的な話がメインだったので、とんでもない会議に私なんかが参加してしまっているという印象でしたが、回を重ねるごとに具体的な話になり、市民としてサービスを利用するにあたり、どんなことが怖いのか、私だったらこういうことを考えるなと、具体的に考えることができたので、よかったと考えています。今後どのようなサービスが出てきて、どのような評価がされて、市民としてそのサービスを活用するかしないかを検討することが楽しみです。皆様ありがとうございました。

坂下座長：ありがとうございました。鈴木座員お願いします。

鈴木座員：あそこに、つくば市の「世界の明日が見える」というフレーズが書かれています。今回のPIAはGDPRに沿っていると思っており、私は法律の専門家ではありませんが、「データ最小化」も入っているなと思いながら見ていました。スマートシティは日本だけでなく世界中で取組が進められています。GDPRも一般データ保護なので、スマートシティはこういうことでうまくいったということを世界にも発信する形で運用できたら、世界に誇れる

と思います。海外の企業がつくば市のスマートシティでサービスを始める時にも適用できると思いまして、広い視野を持ってグローバルな視点で、このPIAは海外から輸入し日本の方法に合わせて実施しましたが、それをもう一度海外に返せるように発展したら良いと思いました。ありがとうございました。

坂下座長：ありがとうございました。平山座員お願いします。

平山座員：私も最初に話してしまいましたので、特に追加する内容はないのですが、私の場合はつくばスマートシティ協議会の代表という立場もございますので、しっかりと見ていきたいと思います。

坂下座長：ありがとうございました。水町座員お願いします。

水町座員：私はもともとプライバシー影響評価を日本に導入することをやっていたので、1年間毎日PIAの仕事しかしていないような状況で、作業としては長いことやっていて非常に思い入れがある仕組みでした。いろいろと話してしまい、皆様にはご迷惑をおかけしたと思っています。様々な意見が出た中で、運用ができるようにきれいに制度化できたことは、つくば市の実力がとても高いのだと思います。また、私は個人情報保護が好きなのですが、そのような人の意見ばかりですと、世間から離れてしまう部分もあるので、皆様が様々な背景や知識を持たれた上でお話いただいて、とても良い成果が出たのではないかと思っています。コロナ以降、世の中がDXに走る状況で、自治体や国もDXだから、という進め方が多いように感じているのですが、DXの意識が行き過ぎると個人情報が疎かになってしまい、利活用だけすれば良いという場面も散見され、見ていてヒヤリとすることがあります。一方で、住民意識として個人情報保護は必須ですから、スマートシティを進めるにあたって、個人情報も忘れてはいけないので、こういう仕組みがあること、その意識が制度に根づいていることはとても良いことだと思います。お世話になり、ありがとうございました。

坂下座長：ありがとうございました。髙橋座員お願いします。

髙橋座員：つくば市の職員という立場として、2年間このようなもの作っていただき、感謝の気持ちでいっぱいです。私は、中間とりまとめができた後にこの議論に参加させていただいたので、初めからきれいな形でまとまってい

て、まとめるまでのご苦労は議事録で察するしかないですが、それ以降の議論においても先生方から有意義なご指摘をいただき、結果としてこのような形になったのだと思います。日本ではまだこれからのPIAについて、つくばというまちから日本全体に横展開できるような最先端の取組ができ、また、このような形で外に出しても恥ずかしくないものが作れたことを本当に嬉しく思いますし、誇りに思うところです。今後の運用面では、市が責任を持って進める立場ですので、これがゴールではなく、我々にとってはスタートとなる気持ちで、非常に身が引き締まる思いです。議論でもありましたが、ここで決めるというより運用の中で判断していく部分があると思いますし、個人情報保護をしながら、一方で、市民が使いやすい良いサービスは使ってもらえるような形にするという、アクセルとブレーキのちょうど良い具合を見極めながら、根拠のある評価を今後進めていきたいと思います。

坂下座長：ありがとうございました。本日内閣府もご出席ですので、牟田調整官からもご発言お願いします。

牟田調整官：発言の機会をいただきありがとうございます。まず2年間8回にわたる懇話会で、すばらしい形でとりまとめていただきまして、スーパーシティを進める内閣府としても、市民の方々と有識者の先生方に感謝申し上げたいと思います。先ほど、つくば市の実力という話もありましたが、事務局とは今年度入ってから毎週このPIA懇話会に向けて打ち合わせを実施していて、一番そばで見てきましたけれども、事務局にもお疲れ様でしたとお伝えしたいと思います。なぜこれをつくば市が検討しているのかに立ち返ると、平成30年頃にこのスーパーシティの話が出始めた時に、スーパーシティのもとで個人情報が勝手に使われてしまうのではないかという不安が大きな声として上がった中で、スーパーシティのもとでも、当然個人情報保護法を順守し、個人情報を扱うサービスをする時には、市民の理解を得ながらPIAも必要だという議論が国でもあり、制度設計がされてきました。令和4年につくば市がスーパーシティに指定されましたが、つくば市がその思いをしっかり酌んで、このような形で実施していることは非常に重要なことだと思います。全国どこにもない先駆けた検討で、本当にチャレンジングなことをつくば市という一つの地域発でやっていただいたことが非常に重要だと思ってお

りますので、内閣府としても連携して進めていきたいです。せっかくなので2点だけ簡単にお話させていただきます。昨年度末、内閣府からスーパーシティとして検討を進める上では、民間活用のユースケースを検討いただきたいということは申し上げていて、それを踏まえて前々回の第6回の懇話会では、民間活用のユースケースをご提示の上で議論いただきました。これまでの懇話会の中で、現実的にそういうユースケースを実現することは難しいのではないかと厳しいご意見もいただきましたが、確かに今年来年というスケジュール感ですぐ実現することは難しいかもしれません。しかし、市が掲げているスーパーサイエンスシティー構想の中では、民間も含めて多様なデータ活用を行い、サービスを実現していくことを目指していますので、難しい部分もあるという課題も含めてご議論いただき、将来の姿を見据えて、今後の発展にも対応できる形でPIAの仕組みをご検討いただきとりまとめていただきました。これをスタートとして、アジャイルで進めていただきたいと思います。難しいお願いをしっかり受けとめてご議論いただきまして、改めてありがとうございました。また、つくば市で実施したものとしてこの成果を広げていくべきと多々ご指摘をいただいております。この点は、内閣府に対する宿題と受けとめておりますので、国の各種会議でも、データ利活用と個人情報の関係が議論になることが考えられますので、全国に先駆けた検討を受けとめた上で、他の地域でも様々な場面で活用できるように、スーパーシティの使命として実施して参りたいと思います。本当にありがとうございました。

坂下座長：では最後に、私から一言だけ総括をします。皆様がおっしゃったことは、フレームはしっかりできて、これから中身を詰める必要がある部分は共通しております。ただ、これは定規を作っただけで、測るものはまだ何もなく、そこをしっかりやる必要があります。八潮で陥没事故がありましたが、サービスは道路で走る車で、道路自体が駄目だと、車が落ちてしまいます。ですので、その基盤のPIAを実施することと、PIAを実施するのが協議会であるならば、協議会の組織のガバナンスが効くかどうかを今後チェックしなければいけません。国会では村上総務相が、自治体は1700もいらない、400で良いと大騒ぎしています。日本の場合、35年で4割人が減ります

が、今つくば市は、26万人のはずで、4割減ったら16万です。16万人というのは、現在の釧路市と同じ人口規模で、それが35年後の姿です。その時に、今の生活インフラはすべて維持できるかどうかを考えると、官民がデータ連携しなければ生き残れないでしょう。それを解決するために先駆けて定規を作ったわけです。今後、委員の方々にお願いしたいことは、市民委員の方々は、これからスーパーシティのサービスがリリースされた時に、PIAを実施してこのサービスがリリースされていることを、周囲の市民の方にも、お話していただきたい。また、有識者の先生方には、他の自治体に同じことやらせては駄目で、つくば市のこのまとまっているものを、より具体的にしたもので展開できるよう、啓発してほしい。更に、つくば市には、生活に密着している自治体でも中央官庁と同じように人事異動がありますから、人が変わると急に萎むということがないように、今回の考え方を後継の方にバトンを渡し、必要に応じて英語に翻訳して発信すると良いと思います。英語に翻訳すれば、海外からの直接投資がつくば市に来る可能性があります。そういうことを実施することが一つの産業活性化政策になります。今回、皆様のご尽力が非常に良いことをやっていて、人口が減る中で、地方自治をどうやって発展させるかの一つのトリガーになると思うので、この成果を展開していただきたいと思っています。私からの総括は以上です。2年間どうもありがとうございました。それでは次の議事に移ります。その他として、事務局からこれからの流れについてご説明をお願いします。

事務局（高橋補佐）：今後の流れにつきまして簡単にご説明いたします。今回ご議論いただきまして座長にご一任いただいたということで、この後、座長と相談をし、本日いただいたご意見を踏まえて、最終的な修正を加えた形で、3月中をめどに正式な最終とりまとめとして、つくば市から公表したいと思います。令和7年度に入りましたら、しかるべきタイミングでこの最終とりまとめの内容を踏まえて、つくば市として正式なPIA制度を施行したいと考えています。最後に事務局からも御礼させていただければと思います。2年間にわたる議論を踏まえて、このような最終とりまとめに行き着くことができまして、ありがとうございました。最後なので正直申し上げまして、PIAチームは私を含め4人おりまして、あと昨年度、卒業した1名を加えて

5名いたのですが、5人とも本当に大変でした。ここに至ったのも、皆様が我々に寄り添って親身にご助言いただいたことが励みになり、本当に参考になりまして、その結果としてこのような最終とりまとめに行き着くことができました。本当にありがとうございました。また、今年度は内閣府さんからも1年通してかなり手厚いサポートをいただき、デロイトさんにもサポート入っていただきまして、本当にこのような形でまとめることができました。昨年度は東京海上日動さんにもご協力いただき、総力を結集してここまでまとめることができたと思いますので、我々としましてもこの成果を次につなげて運用し、施行していきたいと思っておりますので、引き続きご指導をいただければと思います。事務局から以上です。

坂下座長：座員の皆様、事務局から説明があった点につきましてご質問やご意見等ございますか。それでは、本日予定しておりました案件はすべて終了いたしましたので、ここでマイクを事務局に戻します。

事務局（中山課長）：長時間にわたりご議論いただきありがとうございました。令和5年3月から、座員の皆様にご検討いただいた集大成である「最終とりまとめ」に基づき、今後つくば市ではPIAの制度化を進めてまいります。約2年間の長きに渡り、ご議論、ご助言を賜り、誠にありがとうございました。以上で、第8回つくば市プライバシー影響評価制度検討懇話会を閉会とします。ありがとうございました。

第８回つくば市プライバシー影響評価制度検討懇話会

日時：令和７年(2025年)2月14日（金）17時～
場所：つくば市役所本庁舎５階　庁議室
（オンライン併用）

次　第

１　開会

２　議事
（１）最終とりまとめ（案）について

３　その他

４　閉会

○　配付資料
資料１　最終とりまとめ　詳細版（案）
資料２　最終とりまとめ　概要版（案）
資料３　最終とりまとめ　ポイント説明資料（案）

資料１

「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（案）

令和７年（2025 年）　　月

つくば市プライバシー影響評価制度検討懇話会

目次

別添

（別冊）参考資料編

１　懇話会議事録、資料

２　懇話会設置要項

省略

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。

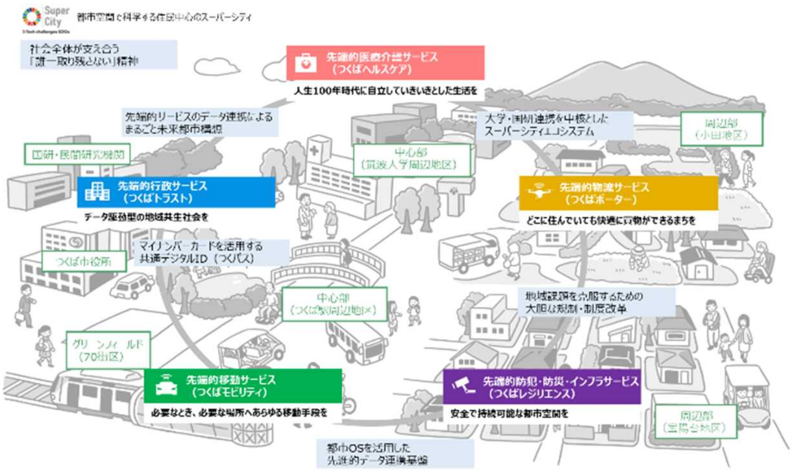


図１　つくばスーパーサイエンスシティ構想

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、構想を成功裡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。

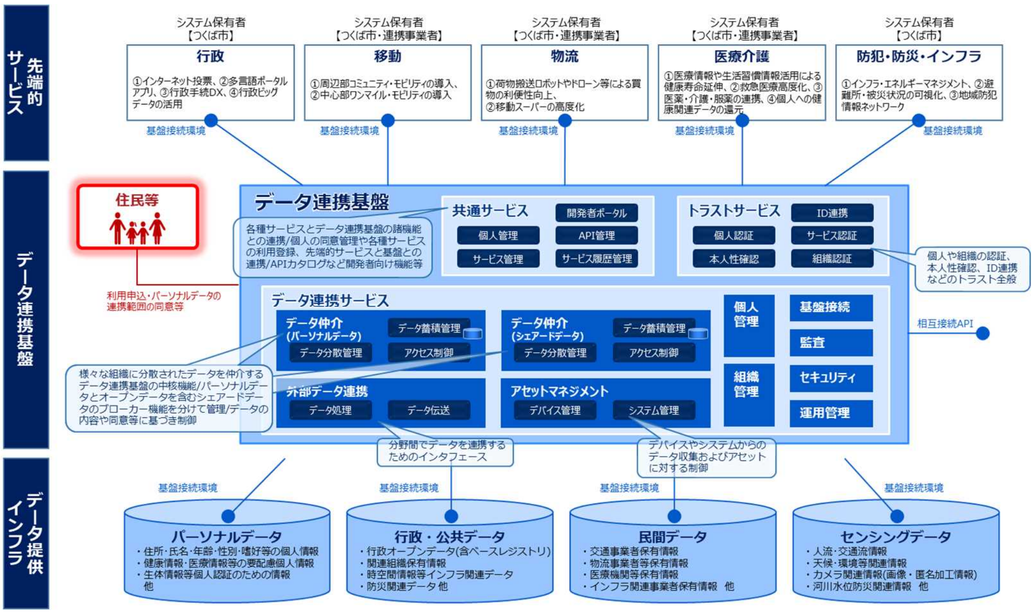


図２　データ連携基盤の活用イメージ

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

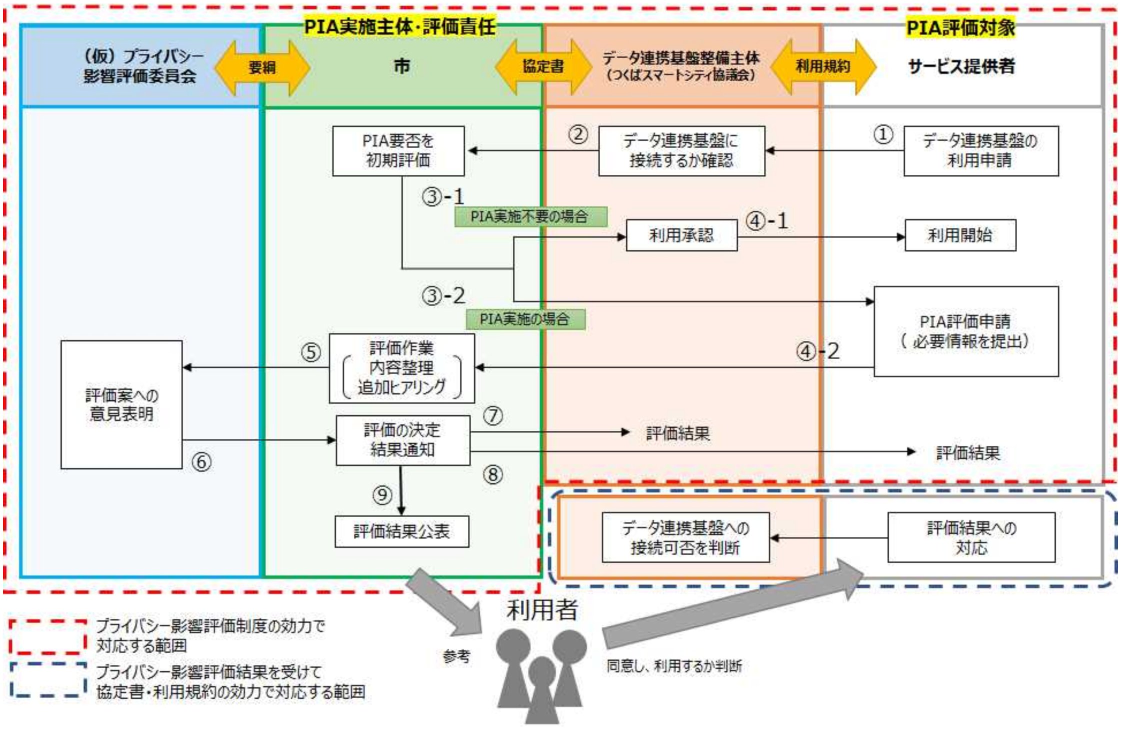


図３　PIA 実施体制（全体像）

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。

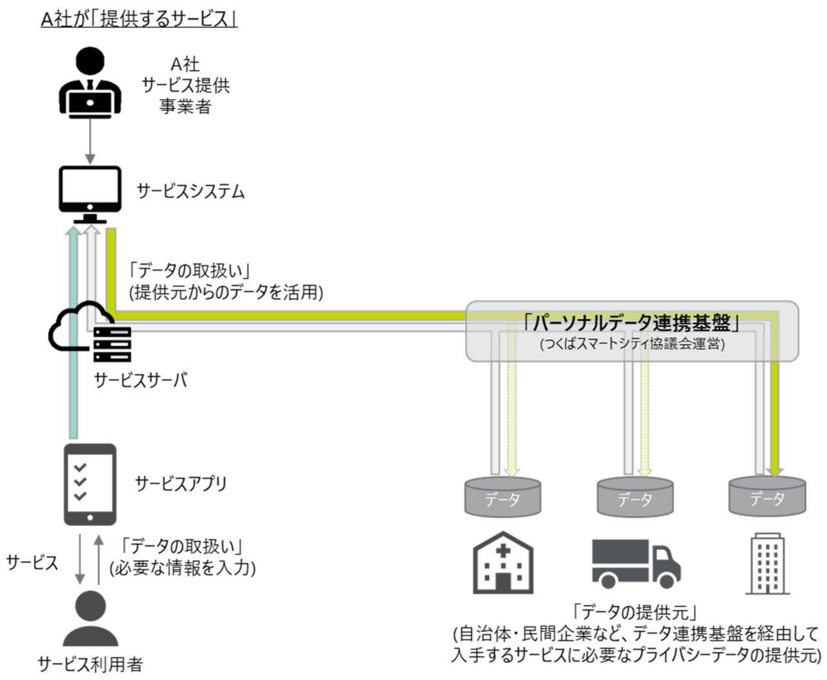


図４　PIA 評価の対象範囲のイメージ [5]

1.2.2　初期評価

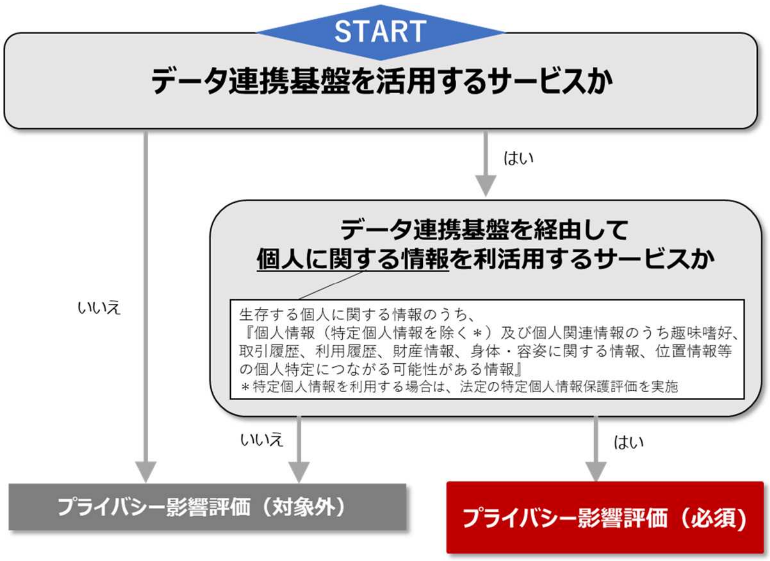


図５　PIA 要否を判断する初期評価の流れ

---

[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」を特定の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」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・財産・精神の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「JO モデル」[6]を参考にした。JO 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。

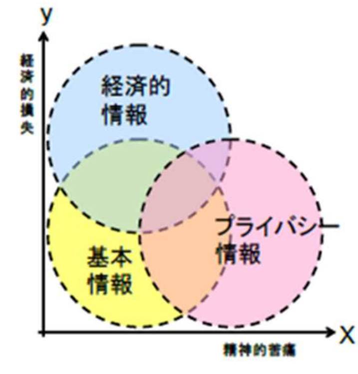
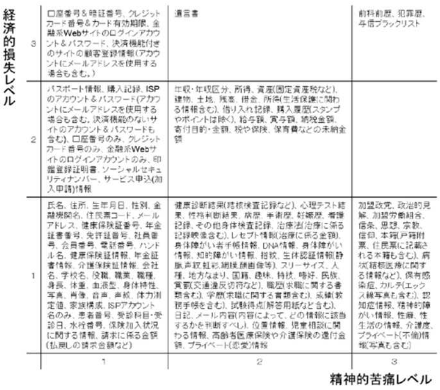


図 5-2：EP 図（Economic-Privacy Map）



経済的損失レベル

3	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(アカウントにメールアドレスを使用する場合も含む。)	遺言書	前科前歴、犯罪歴、与信ブラックリスト
2	パスポート情報、購入記録、ISPのアカウント＆パスワード(アカウントにメールアドレスを使用する場合も含む。決済機能のないサイトのアカウント＆パスワードも含む)、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、ソーシャルセキュリティナンバー、サービス申込(加入申請)情報	年収・年収区分、所得、資産(固定資産税など)、建物、土地、残高、借金、所得(生活保護に関わる情報含む)、借り入れ記録、購入履歴(スタンプやポイントは除く)、給与額、賞与額、納税金額、寄付目的・金額、税や保険、保育費などの未納金額	
1	氏名、住所、生年月日、性別、金融機関名、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、社員番号、会員番号、電話番号、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、会社名、学校名、役職、職業、職種、身長、体重、血液型、身体特性、写真、肖像、音声、声紋、体力測定値、家族構成、ISPアカウント名のみ、患者番号、受診科目・受診日、水栓番号、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)	健康診断結果(結核検査記録など)、心理テスト結果、性格判断結果、病歴、手術歴、妊娠歴、看護記録、その他身体検査記録、治療法(治療に係る記録映像含む)、レセプト情報(治療に係る金額)、身体障がい者手帳情報、DNA情報、身体障がい情報、知的障がい情報、指紋、生体認証情報(静脈,声紋,虹彩,網膜,顔画像等)、スリーサイズ、人種、地方なまり、国籍、趣味、特技、嗜好、民族、賞罰(交通違反切符など)、職歴(求職に関する書類含む)、学歴(求職に関する書類含む)、成績(教務手帳を含む)、試験得点(解答用紙など含む)、日記、メール内容(内容によって、どの情報に該当するかを判断すべし)、位置情報、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	加盟政党、政治的見解、加盟労働組合、信条、思想、宗教、信仰、本籍(戸籍附票、住民票に記載される本籍も含む)、病状(結核医療に関する情報など)、保有感染症、カルテ(エックス線写真も含む)、認知症情報、精神的障がい情報、性癖、性生活の情報、介護度、プライベート(不倫)情報(写真も含む)
	1	2	3

精神的苦痛レベル

図 5-3：シンプル EP 図

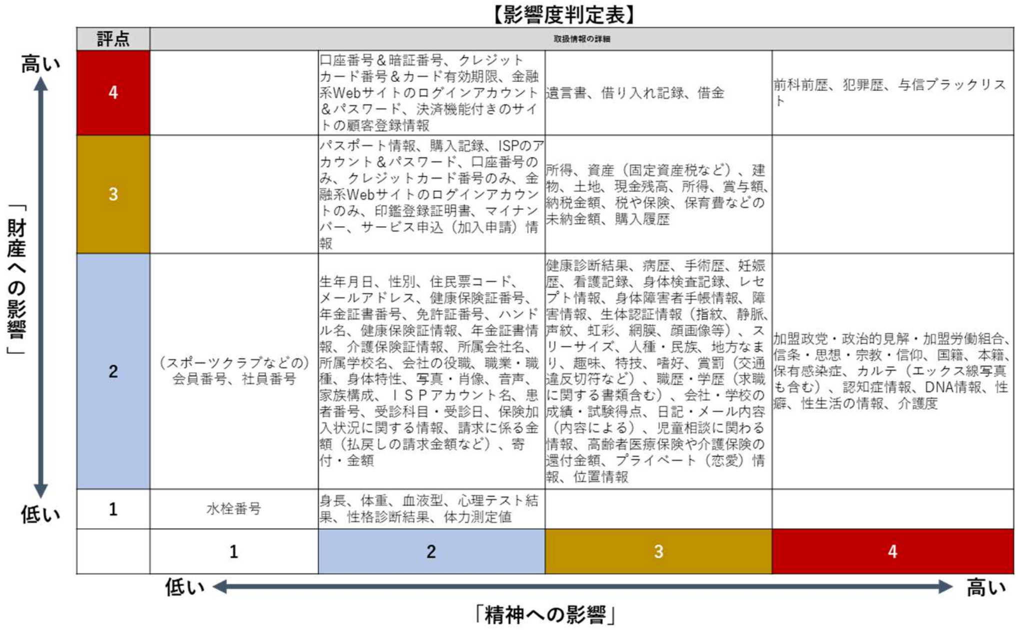
【引用】JNSA「情報セキュリティインシデントに関する調査報告書」

JO 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】

評点	取扱情報の詳細			
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		
	1	2	3	4

＋

「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」

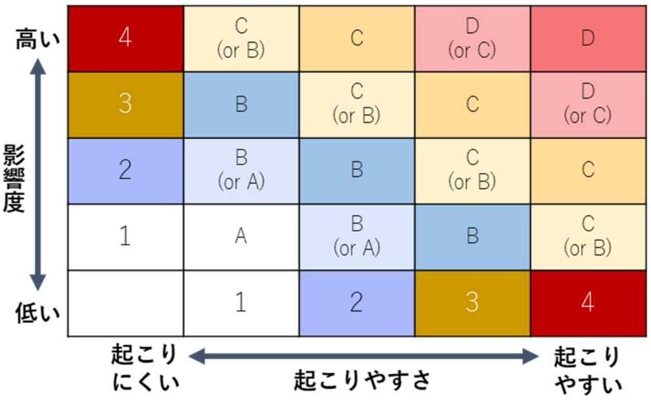
上記の考え方に基づき評価項目について一通り評価し、その中で最も高い評点を当該サービスの「起こりやすさ」の評価として採用する。また、「起こりやすさ」の評価作業の過程で、評価項目一覧で示した 22 項目以外の観点による懸念、リスクが見つかった場合は、評価委員会で議論の上、判定するのがよいだろう。

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。



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

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。

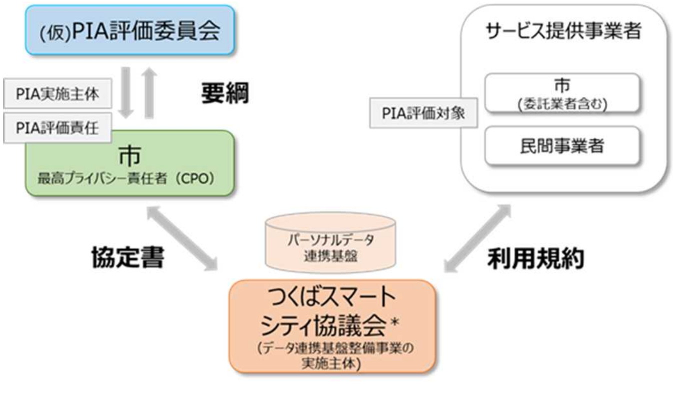


図６　PIA制度の実効性を担保する仕組み

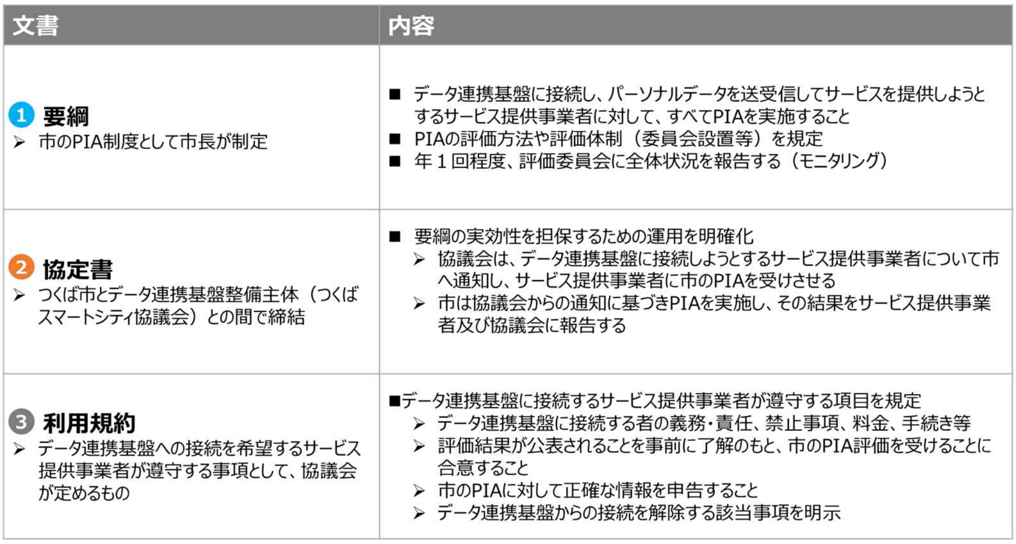
「要綱」「協定」「利用規約」が規定する具体的な条文内容については、市の責任において具体化を図るものと承知しており、本懇話会では実効性を担保するために、これらにどのような事項を規定するべきかという範囲で議論を行った。

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。

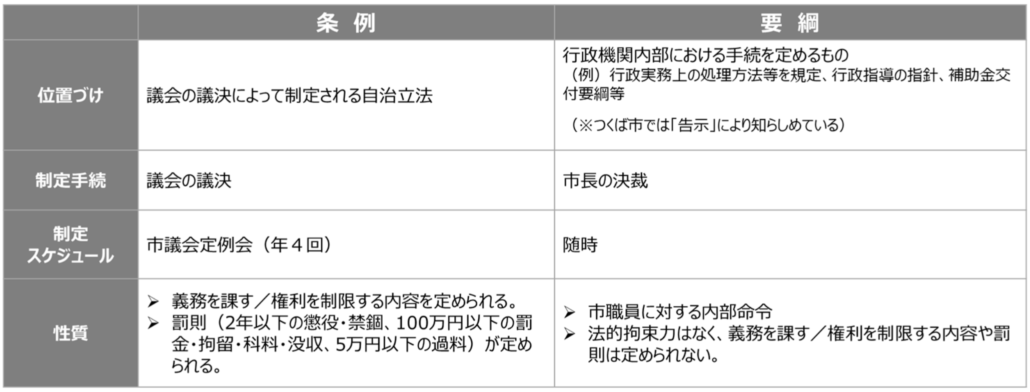
本件については PIA 制度の外側の、市と協議会間の整理の問題であり、本懇話会としては一定の結論を纏めることはせず、最終的な考え方の整理は市の判断に委ねるが、検討に当たっては様々な意見があるということを念頭に置きつつ、PIA 制度の実効性を担保するために、要綱・協定・利用規約にどのような規定を盛り込むかについて慎重に検討されたい、という点を本懇話会として申し送りたい。



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。

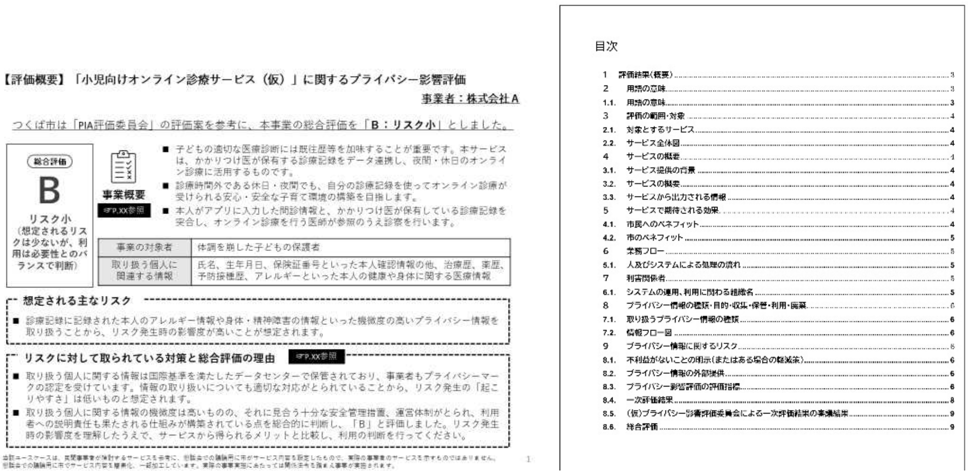
また、総合評価の結果については評価書の形で対外的に公表する。公表にあたって最も重要なことはPIA評価の内容を市民に理解してもらうことであり、評価書では専門用語や難解な表現を避け、市民に分かりやすい言葉を使用することが重要であることが懇話会においても繰り返し議論された。

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
☞P.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 ☞P.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。

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。

≪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　直美	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	民間事業者が実施主体となり、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	民間事業者が実施主体となり、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。）	必須	個人情報保護法 第34条、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。	必須	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データの廃棄期限等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	－

資料２

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（案）概要版　目次

資料２

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サービス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

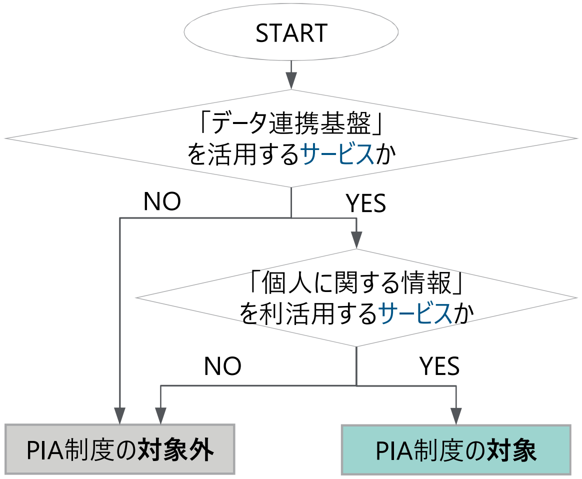


図1 PIA要否を判断する初期評価の流れ

- 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**」を活用するサービスか
  - ➢ 「**個人に関する情報**」を利活用するサービスか

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こと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

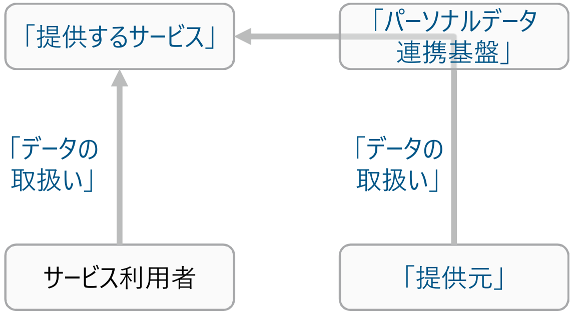


図2 サービス構成の全体イメージ

- 「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、当該サービスに関係する「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)

資料２

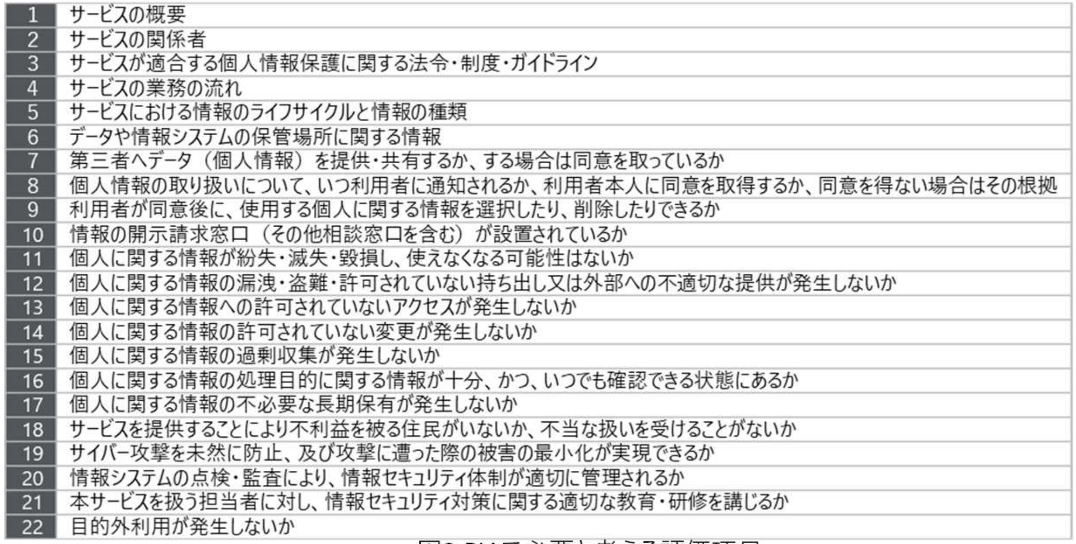
2　評価項目／評価基準①

評価項目

- 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に実施する

[*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

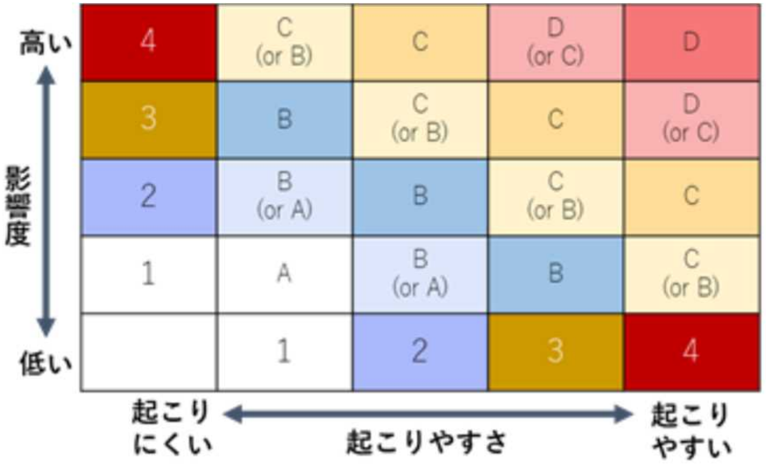
評価基準

- 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

影響度（１～４） × 起こりやすさ（１～４） → 総合評価（A～D）

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）



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

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、原則としては上位の評価を採用する方針とすることとしつつも、総合的に評価した上で下位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

評価基準

【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

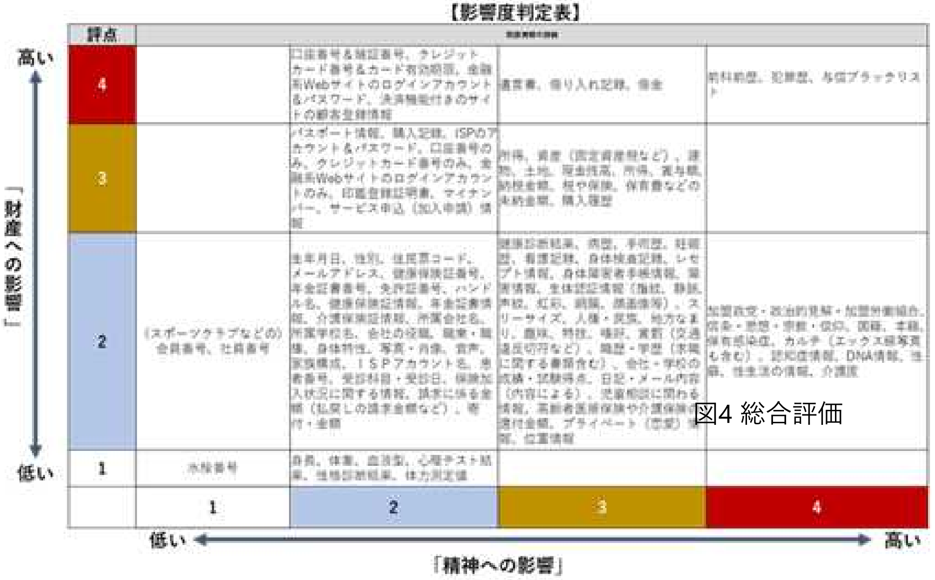


図6 影響度判定表

「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

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

【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点加点し、
  ３つ以上対応できていない場合は最大４点

3　評価体制における役割・責任／実効性の担保

評価体制における役割・責任

- 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

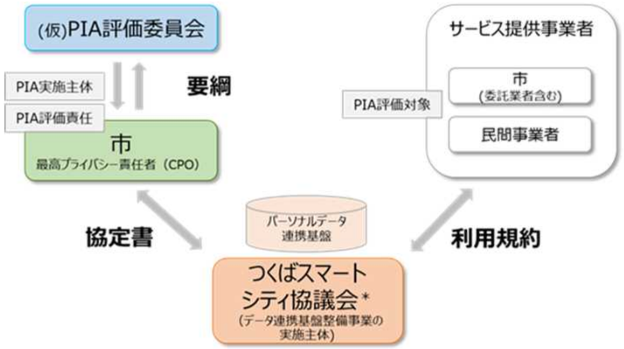


図8 評価体制のイメージ

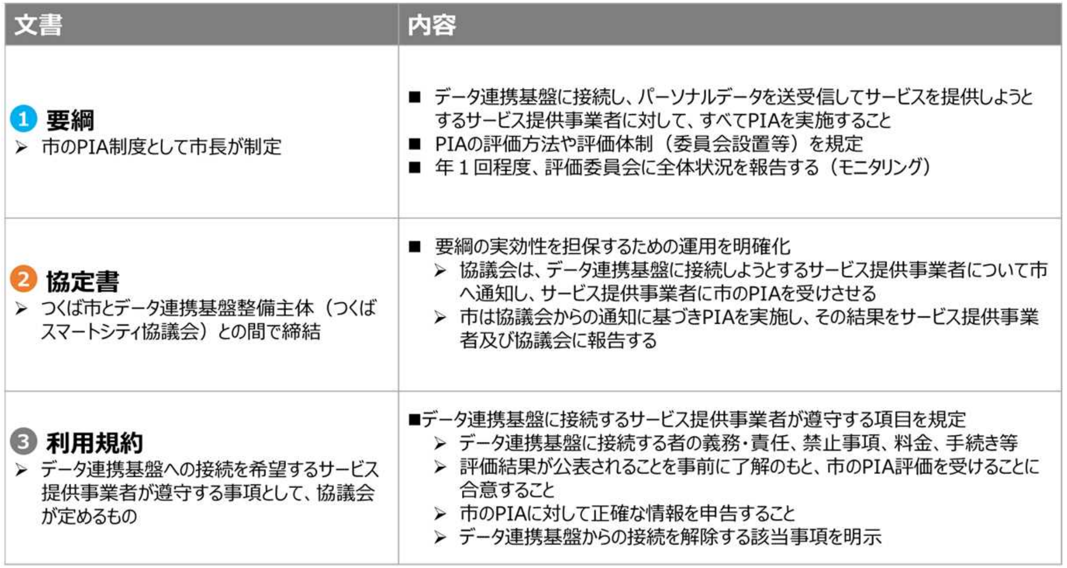
図9 「PIA制度」における責任分界点

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

実効性の担保

- 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



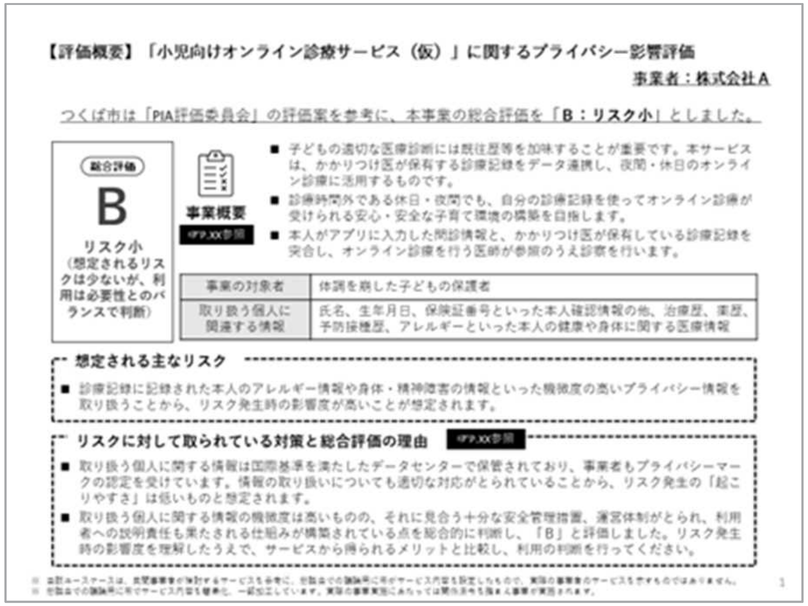
文書	内容
① **要綱** ➢ 市のPIA制度として市長が制定	■ データ連携基盤に接続し、パーソナルデータを送受信してサービスを提供しようとするサービス提供事業者に対して、すべてPIAを実施すること ■ PIAの評価方法や評価体制（委員会設置等）を規定 ■ 年１回程度、評価委員会に全体状況を報告する（モニタリング）
② **協定書** ➢ つくば市とデータ連携基盤整備主体（つくばスマートシティ協議会）との間で締結	■ 要綱の実効性を担保するための運用を明確化 ➢ 協議会は、データ連携基盤に接続しようとするサービス提供事業者について市へ通知し、サービス提供事業者に市のPIAを受けさせる ➢ 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

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

結果の通知と公表

- 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、利用は必要性とのバランスで判断）

事業概要
※P.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 ※P.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。

図11 評価報告書（概要版）のイメージ

運用

- 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	制度運用において発見される課題
• 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、現時点では明確な基準は設けず、「都度」判断する	• 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
- 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：個人情報の漏えい、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

資料３

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

- つくば市は、**人々の生活の利便性向上を目指し**、先端的な技術・サービスの社会実装に向けて、「つくばスーパーサイエンスシティ構想」を推進している
- 本構想の特徴として、都市の持つデータの連携が挙げられるが、**個人に関する情報を利活用**することで、より先進性の高いサービスの実装が可能となる
- 個人に関する情報の利活用にあたっては、安心・安全なサービスであることは欠かせず、**プライバシーへの影響を適切に評価するPIA制度の検討**を行った

何がPIA評価の対象で、いつ実施すべきか？

■ 初期評価

- 「データ連携基盤」を活用し、「個人に関する情報」を利活用するサービスが対象

■ 評価対象

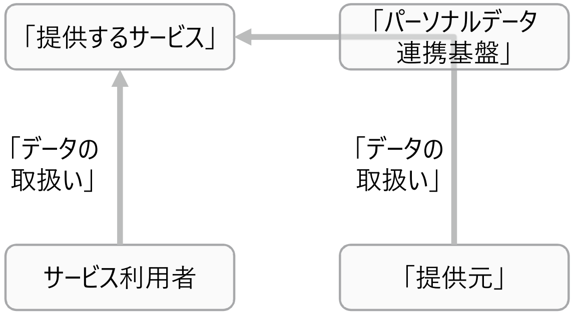
- 「提供するサービス」及び、サービスに関係する「データの取扱い」が本PIAの評価対象 *図1参照

  ※具体的には、「提供するサービス」にて「データの取扱い」に関する本人への通知や安全管理措置が十分に講じられているか等の観点より評価を行う

■ タイミング

- 「初回」はサービス開始前に実施要

  ※詳細設計・開発に取り掛かる前に実施推奨



「提供するサービス」

「パーソナルデータ連携基盤」

「データの取扱い」

「データの取扱い」

サービス利用者

「提供元」

図1 サービス構成の全体イメージ

どのようにPIA評価は行われるか？

■ 評価体制における役割・責任

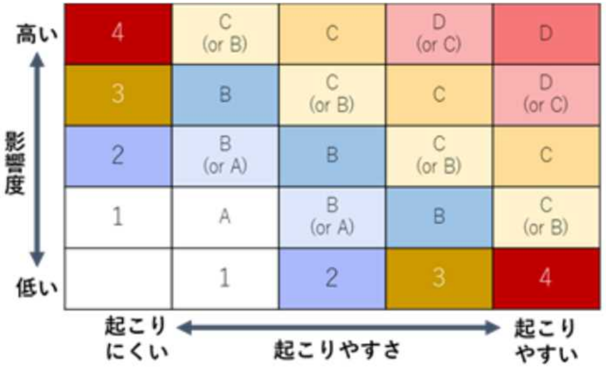
- 「市」が有識者等を構成員とした「プライバシー影響評価委員会」の助言を踏まえ、「サービス提供事業者」に対して、PIAを実施する

■ 評価項目

- データの取扱い・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に関する評価項目(全22項目64質問)にて構成

■ 評価基準

- 個人に関する情報において財産／精神の観点からプライバシーに及ぼす「影響度」と、評価項目の観点からリスクの「起こりやすさ」を導出し、「総合評価」を4段階で判定 *図2参照



高い	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)
低い		1	2	3	4

図2 総合評価

PIAの実効性はどう担保し、実施後は？

■ 実効性の担保

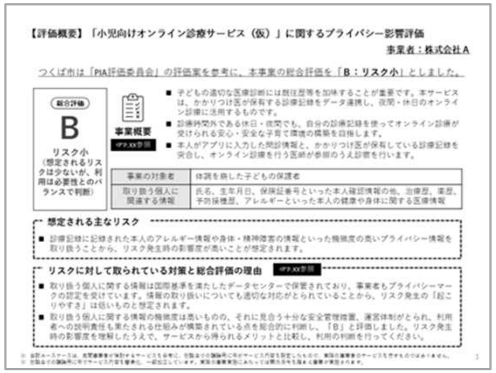
- 市はPIA制度を「要綱」、市－データ連携基盤整備主体間は「協定書」、データ連携基盤整備主体－サービス提供事業者間は「利用規約」にて取り決めを行い、実効性を担保する

■ 結果の通知と公表

- 市はPIAの結果をデータ連携基盤整備主体・サービス提供事業者に「通知」するとともに、市のHP等で「公表」する *図3参照

■ 運用

- PIA評価結果が変わる可能性が見込まれる場合は「再評価」が必要となるが、評価実績を有していない現時点では都度判断とする



【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、利用は必要性とのバランスで判断）

事業概要

- 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

- 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。

図3 評価報告(概要版)のイメージ