茅野市プライバシー影響評価
実施手順書

令和７年５月

令和８年６月改定

目次

1. はじめに

1.1. 本手順書の位置づけ

本市では、人口減少や少子高齢化の進展といった課題を背景に「DX 基本構想」（2022 年 6 月）、「「茅野市の DX」のススメ方-茅野市 DX 基本計画-」（2025年 4 月）を策定し、DX（デジタル・トランスフォーメーション）による住民の利便性向上等を目指している。

一方、個人に関する情報[1]の使用に漠然とした不安感を抱く市民もいることから、DX の推進にあたっては情報の利活用に関する透明性を確保することが求められている。

このことから、本市では後述する条件に当てはまるサービスに潜在するリスクを、原則としてサービスの提供前に評価する取り組みとしてプライバシー影響評価（以下「PIA」という。）を推進する。

PIA の推進により、個人に関する情報を活用するサービスに潜在する大きなリスクを低減するとともに、市民が当該サービスのプライバシーに関するリスクを適切に理解して、安心して主体的に利用できるか判断する際の端緒とすることが期待できる。

本書は、上記効果を実現すべく、PIA を実施する際に参照する運用手順書である。

なお、PIA は、被評価者（2.3.3 参照）からの回答に基づき行われるものであり、本市が PIA を実施することは必ずしも PIA 実施対象となったサービスのプライバシーリスクを完全に取り除くことを意味しない。

ついては本市は、PIA の評価結果に関わらず、被評価者に対し、個人に関する情報の厳格な管理を求めるものとする。

1.2. PIA 実施の根拠

本市における PIA は、「「茅野市の DX」のススメ方-茅野市 DX 基本計画-」に基づき実施するものである。

[1] 個人情報、要配慮個人情報、個人識別符号、仮名加工情報、匿名加工情報、個人関連情報のこと。個人情報保護法における個人情報よりも広い範囲を指す。

2. 総論

2.1. 対象サービス

以下に当てはまるサービスに対し PIA を実施する。

- ◆ 都市 OS 及び都市 OS に接続するサービス[2]
- ◆ 都市 OS に接続しないが、茅野市が導入又は推進[3]するサービスのうち、個人に関する情報を扱う等、市が PIA 実施を必要と判断するサービス

2.2. 評価対象者

PIA の評価対象者は、対象サービスの実施にあたり、製品・システム等を提供する事業者（以下「サービス提供事業者」という。）及び対象サービスに関する本市の担当部署を含むサービスの運用に関係する者（これらを総称し、以下「サービス提供関係者」）という。）とする。

2.3. 体制・手順の概要

2.3.1. 実施体制

PIAは茅野市が実施主体となり、DX 推進協議会（合意形成・普及拡大会議、事務局（ワーキンググループ幹事会）、データガバナンス部会、マーケティング・広報部会、その他各部会・ワーキンググループ等）及びサービス提供関係者との連携のもと実施する。

2.3.2. 評価者

PIA の評価者は茅野市とする。なお実際の評価にあたっては、一次評価を DX 推進課、二次評価をデータガバナンス部会が行い、それらを踏まえた最終的な総合評価を茅野市が判定することとする。

2.3.3. 被評価者

PIA の被評価者は、「2.2.評価対象者」に該当する者のうち、本市が必要と認めて PIA 調査協力依頼をした者であって、これに応じた者とする。

2.3.4. 手順の概要

PIAは以下の手順に沿って実施する。

【プロポーザル方式の場合】

① 本市が PIA の実施要否及びサービス提供関係者を明らかにする（実施判

[2] ただし、個人に関する情報を全く扱わない等、茅野市が PIA の実施を不要と判断したサービスを除く。

[3] 茅野市がサービスを導入・所有しないものの、国や民間事業者等が提供する既存サービスを、市の施策として活用・展開すること。

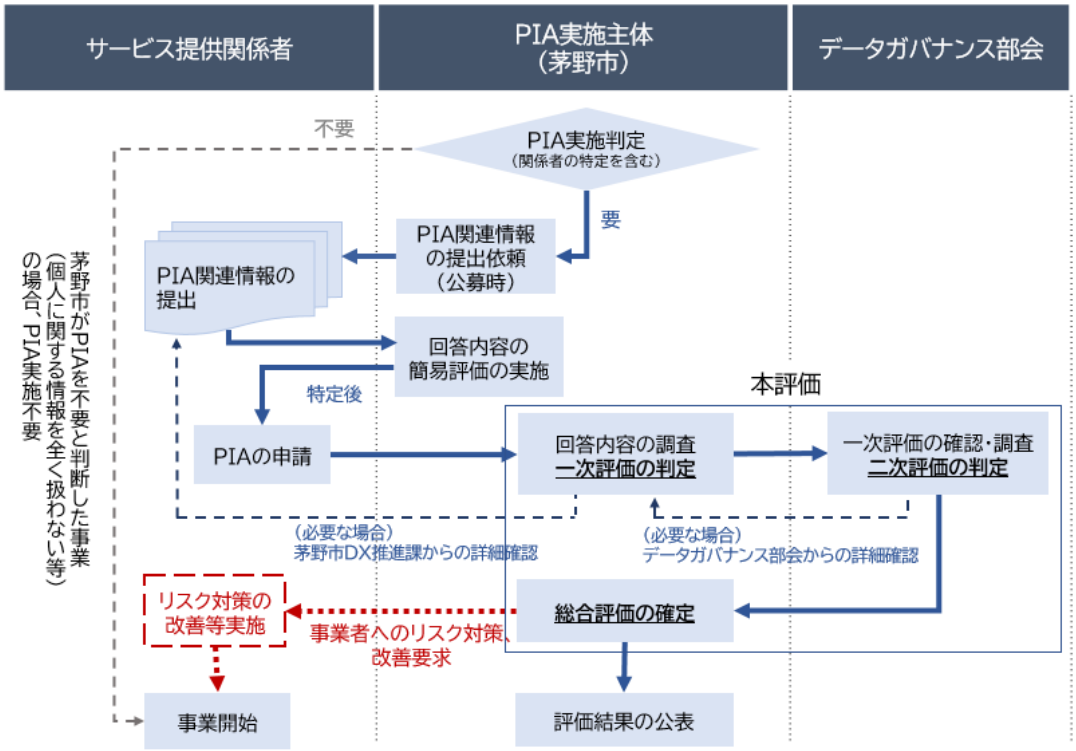
定及び関係者の特定）。
② 実施判定の結果、PIA を要する場合には公募に応じるサービス提供事業者から PIA に必要な情報を取得する。
③ 取得した情報をもとに、本市が簡易評価を実施する。
④ 最も適した提案者（サービス提供事業者）の特定後、サービス提供関係者からの PIA 実施申請により、PIA に必要な情報を取得する。
⑤ 取得した情報をもとに、本市が本評価（一次評価）を実施する。
⑥ 一次評価結果をもとに、データガバナンス部会が本評価（二次評価）を実施する。
⑦ 二次評価結果をもとに、本市が本評価（総合評価）を決定する。
⑧ 総合評価結果をパブリックサマリとして公表する。

【プロポーザル方式以外の場合】
① 本市が PIA の実施要否及びサービス提供関係者を明らかにする（実施判定及び関係者の特定）。
② 実施判定の結果、PIA を要する場合にはサービス提供関係者に協力を要請する。
③ 要請に応じたサービス提供関係者からの PIA 実施申請により、PIA に必要な情報を取得する。
④ 取得した情報をもとに、本市が本評価（一次評価）を実施する。
⑤ 一次評価結果をもとに、データガバナンス部会が本評価（二次評価）を実施する。
⑥ 二次評価結果をもとに、本市が本評価（総合評価）を決定する。
⑦ 総合評価結果をパブリックサマリとして公表する。

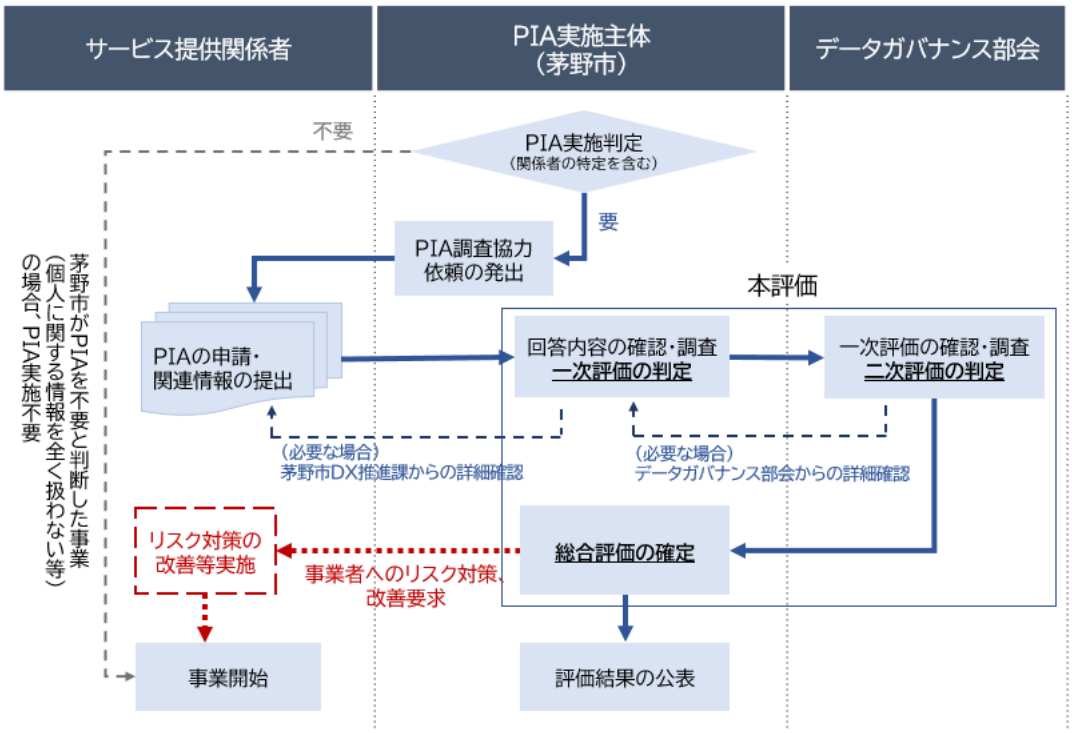
※図示化した実施体制並びに手順の概要は以下のとおり。なお、手順の詳細は4章・5章を参照のこと。

図：茅野市のPIA実施体制・実施手順概要

【プロポーザル方式の場合】



【プロポーザル方式以外の場合】



3. 用語の整理

PIA に関する用語は、以下のとおりである。

□ **プライバシーリスク**[4]

個人情報の「扱い」方に失敗、つまり個人のプライバシーの権利が侵害されたときに顕在化するリスク。

□ **LGWAN**[5]

総合行政ネットワーク（LGWAN）は、地方公共団体を相互に接続する行政専用のネットワーク。

□ **個人情報**[6]

生存する個人に関する情報であって、氏名、生年月日その他の記述等により特定の個人を識別することができるもの、又は個人識別符号が含まれるもの。

□ **要配慮個人情報**[7]

個人に対する不当な差別や偏見が生じないように特に配慮が必要な情報（人種、信条、社会的身分、病歴、犯罪歴等）

□ **個人識別符号**[8]

当該情報単体から特定の個人を識別することができるものとして政令に定められた文字、番号、記号その他の符号。

□ **仮名加工情報**[9]

個人情報を、他の情報と照合しない限り特定の個人を識別することができないように加工して得られる個人に関する情報。個人情報のうち、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別できるものの場合は、当該個人情報に含まれる記述の一部を削除することで、また個人識別符号が含まれる個人情報の場合は、当該符号の全部を削除することで得られる。

□ **匿名加工情報**[10]

個人情報を特定の個人を識別することができないように加工して得られる個人に関する情報であって、復元して特定の個人を再識別できないようにしたもの。

---

[4] 出所： Gartner Japan
[5] 出所：地方公共団体情報システム機構
[6] 個人情報の保護に関する法律第2条をもとに編集。
[7] 個人情報の保護に関する法律第2条第 3 項をもとに編集。
[8] 個人情報の保護に関する法律第2条第 2 項をもとに編集。
[9] 個人情報の保護に関する法律第2条第 6 項をもとに編集。
[10] 個人情報の保護に関する法律第2条第 6 項をもとに編集。

□　**個人関連情報**[11]

生存する個人に関する情報であって、個人情報、仮名加工情報及び匿名加工情報のいずれにも該当しないもの。

□　**住基システム**[12]

住民基本台帳ネットワークシステムのこと。住民の方々の利便性の向上と国及び地方公共団体の行政の合理化に資するため、居住関係を公証する住民基本台帳をネットワーク化し、全国共通の本人確認ができるシステムとして構築するもの。

□　**ISMS（情報セキュリティマネジメントシステム）**[13]

個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源を配分して、システムを運用すること。

□　**マルウェア**[14]

「Malicious Software」（悪意のあるソフトウェア）を略したもので、さまざまな脆弱性や情報を利用して攻撃をするソフトウェア（コード）の総称。

[11] 個人情報の保護に関する法律第2条第 7 項をもとに編集。
[12] 出所：総務省　ホームページ
[13] 出所：情報マネジメントシステム認定センター
[14] 出所：総務省　ホームページ

4. 各手順の詳細

以下のとおり、サービス設計段階から、PIA が完了し結果を市民に公表するまでの手順を示す。

なお、PIA は、原則として対象サービスの開始前（サービス設計段階）に実施するが、実施中のサービスでシステム改修等大幅な変更の必要が生じた場合等、相当の必要が生じた場合においても実施するものとする。

また、本市がプロポーザル方式によりサービス導入を行う場合で、公募時点で PIA の実施を必須と判断した場合は、公募に応じるサービス提供事業者に対して手順 4.2 から PIA のフローを開始し、原則として手順 4.2.2 までを契約締結前に実施する。その他のサービス提供関係者に対しては、手順 4.3.1 以降の PIA のフローをサービス実装完了までに実施する。

4.1. PIA の実施判定等及び実施準備

4.1.1. PIA 実施判定及びサービス提供関係者の特定

本市は、PIA の対象となり得るサービスに対して、個人に関する情報の取り扱いの有無及び内容等を把握し、PIAの実施要否及びサービス提供関係者を明らかにする。

本市は、PIA 実施判定にあたり、サービス提供関係者に対し必要に応じてヒアリングを実施する。

4.1.2. PIA 調査の依頼（PIA 実施時のみ）

実施判定の結果、PIA の実施が必要と判断した場合は、本市は様式第 1 号「PIA 調査協力依頼書」により、サービス提供関係者に対して PIA 調査への協力依頼を行い、これに応じた者に様式第 2 号「PIA 調査シート」及び記入要領を送付し、必要事項の記載を依頼する。[15]

4.2. PIA 調査及び簡易評価の実施（プロポーザル方式の場合のみ）

4.2.1. サービス提供事業者からの PIA 調査シートの提出

本市は、プロポーザル方式によりサービス提供事業者の特定を行う場合は、必要に応じて様式第 2 号「PIA 調査シート」の提出を求める。

この場合において、公募に応じるサービス提供事業者は、必要事項を記入した様式第 2 号「PIA 調査シート」及び関連資料等を本市に提出する。

---

[15] PIA の評価対象には特定の主要サービス提供事業者のみならず、関係するサービス提供関係者（本市の担当部署を含むその他の運用関係者等）を含むことから、評価情報は複数の関係者から提供を受ける場合がある。

4.2.2. 簡易評価の実施[16]

本市は、4.3.2 及び 4.3.3 の手順に準じて、様式 2 号「PIA 調査シート」の記載内容を踏まえた PIA 簡易評価を行う。評価にあたっては、様式第 4 号「PIA 事務局一次評価シート」を準用する。

簡易評価の結果、評価結果が「D」となったサービス提供事業者は、原則契約又は選定の対象から除外するものとし、以降のPIAは実施しない。

4.3. PIA 調査及び本評価（一次評価）の実施

4.3.1. サービス提供関係者からの PIA 実施申請

サービス提供関係者は、必要事項を記入した様式第 2 号「PIA 調査シート」（関連資料等を含む）並びに様式第 3 号「PIA 実施申請書」を本市に提出し、本市に対して PIA の実施申請を行う。（4. 2. 1によりすでに様式第 2 号「PIA 調査シート」を提出している場合は、改めての提出は不要。）

4.3.2. 一次評価シートの作成

本市は、様式第 2 号「PIA 調査シート」における No.01 から 18 の各項目及び想定されるリスク[17]の回答内容並びに関連提出書類の詳細を確認する。詳細確認にあたり不備・不明点がある場合は、サービス提供関係者に対し、関連資料等の追加提供依頼や詳細のヒアリングを実施する。

本確認を踏まえ、本市はその結果や補足情報を様式第 4 号「PIA 事務局一次評価シート」に記載する。とりわけ「影響度」及び「起こりやすさ」の一次評価の整理にあたっては、サービス提供関係者から提出された関連資料及びヒアリングで聴取した内容等を十分考慮する。

4.3.3. 一次評価の確定

本市は、前項で様式第 4 号「PIA 事務局一次評価シート」に記載した「影響度」及び「起こりやすさ」[18]の数値のうち、最も数値の大きいものを一次評価結果として確定する。

---

[16] PIA は本来 4.3 から 4.6 のプロセスを踏まえて実施するが、プロポーザル方式において公募に応じる全てのサービス提供事業者に細かなPIAを実施する必要はないことから、提出資料をもとに簡易的な評価を実施する。簡易評価は、実質的には 4.3.2、4.3.3 に定めるPIA一次評価のプロセスに準じた形で実施する。

[17] 各項目の詳細は「5.PIA 評価要領」を参照。また PIA 調査シートの、対象サービスに関して想定されるリスク（リスクシナリオ）の記載欄については、サービス提供関係者に漏れなく記載させること。

[18] 「影響度」及び「起こりやすさ」から評価する点は、「JISX9251（ISO/IEC 29134：2017）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」における考え方に準拠している。

4.4. データガバナンス部会による本評価（二次評価）の実施

本市は、データガバナンス部会に対し一次評価結果を報告し、本結果に対する二次評価を依頼する。依頼の際には、サービス提供関係者からの申請書類（様式第 3 号「PIA 実施申請書」に記された提出書類）及び一次評価結果（前項で作成した様式第 4 号「PIA 事務局一次評価シート」）を送付する。

データガバナンス部会は、一次評価結果を踏まえた二次評価を実施し、その結果を様式第 5 号「データガバナンス部会二次評価シート」に記入する。

審議の結果、サービス提供関係者への再確認・再検討等が必要になる場合は、4.3.2 から 4.4 の手順を繰り返す。

4.5. 本評価（総合評価）の決定

4.5.1. 総合評価結果の決定

データガバナンス部会は、前項で作成した様式第 5 号「データガバナンス部会二次評価シート」を、PIA 一次評価結果に対する二次評価結果として本市に送付する。

本市は、受領した様式第 5 号「データガバナンス部会二次評価シート」をもとに最終的な総合評価を決定し、その結果を様式第 6 号「PIA 総合評価結果通知書」に記入する。

4.5.2. 総合評価結果に基づく対策の要請・勧告

本市は、決定した評価結果（前項で作成した様式 6 号「PIA 総合評価結果通知書」）をサービス提供関係者に通知し、サービス提供関係者に対して必要な対策の要請又は勧告を行うとともに、対象サービスの実施にあたって適切な対応が取られているかを確認する。

4.6. PIA 評価結果の公表

4.6.1. パブリックサマリの作成

本市は、総合評価結果に基づき、様式第 7 号「PIA パブリックサマリ」を作成する。

4.6.2. パブリックサマリの公開

本市は、作成した様式第 7 号「PIA パブリックサマリ」を茅野市のウェブサイト等で公開する。

5. PIA 評価要領

5.1 基礎情報の確認（調査項目「No.01 から 06」の確認）

PIA の実施にあたっては、まずサービス提供関係者（本市の担当部署を除く）に対し、以下の基礎的な情報の提供を求めるとともに、取り扱うプライバシー情報の有無や概要を把握する。

番号	種類及び盛り込まれるべき事項
01	サービスの概要がわかる資料 • 本サービスの目的及び内容 • 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 • 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 • サービス提供関係者の概要 • サービス提供関係者の認証（P マーク、ISO27001（ISMS）等）取得・遵守状況（わかる範囲で） • 本サービスの責任者及び従事者 • リスク管理責任者、セキュリティ責任者 • 委託先 • 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） • 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及び適合状況（可能な場合）がわかる資料
04	サービスの業務の流れがわかる資料（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 • 処理担当者 • 各段階において取り扱うデータの内容 • 処理手順 • 処理場所
06	データや情報システムの保管場所に関する情報 • 住所 • 当該部屋の階 • 当該建物の構造

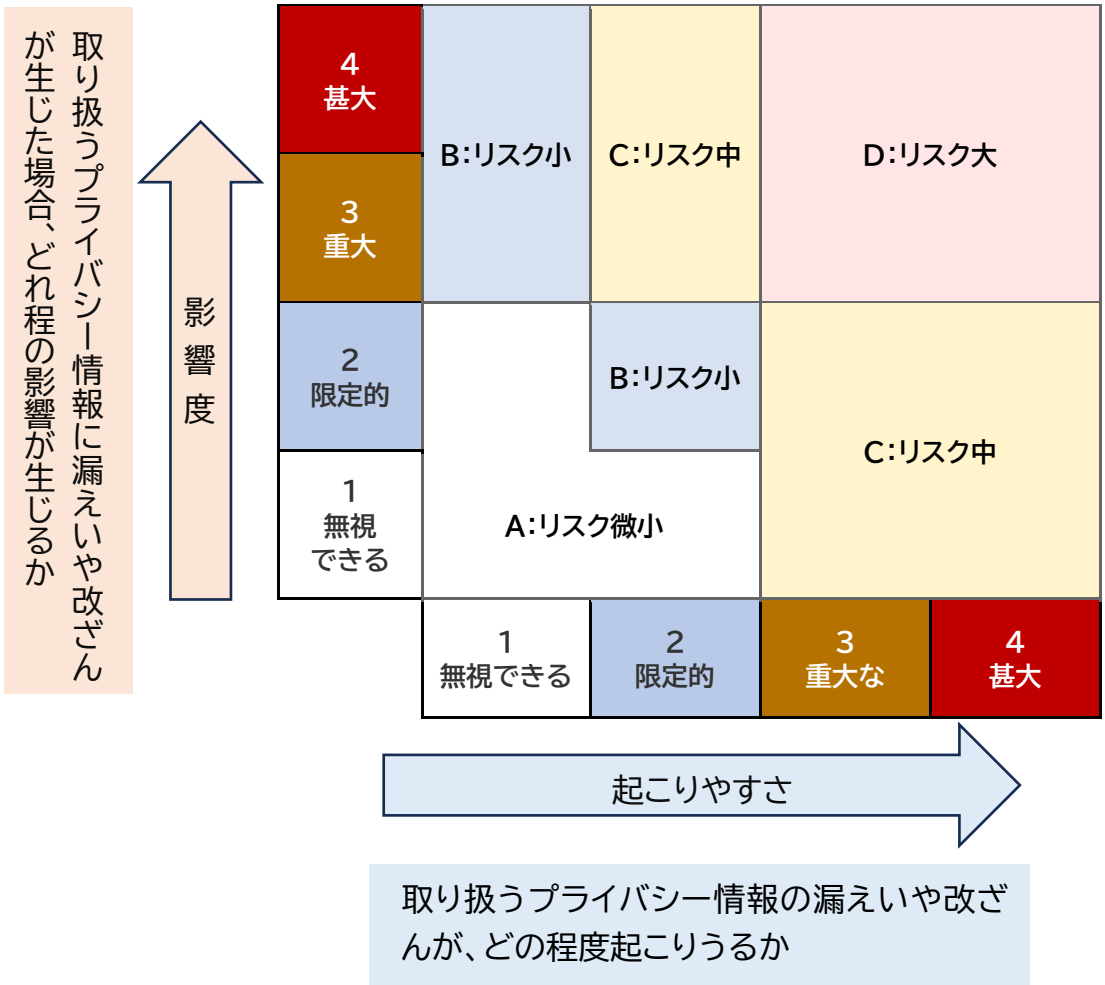
5.2 一次評価（調査項目「No.07 から 18」による評価）

5.2.1. 一次評価の全体像（影響度及び起こりやすさのマトリクス）

① 一次評価は「影響度」と「起こりやすさ」により判定する。
② 「影響度」は、「5.2.2 影響度の判定方法」により判定する。
③ 「起こりやすさ」は、「5.2.3 起こりやすさの判定方法」により判定する。
④ 「影響度」「起こりやすさ」によりそれぞれで行った判定結果を、以下の「プライバシー情報リスクマップ」にプロットし、一次評価案を出す。

※ ②、③の具体的な手順は次項以降のとおり。

【プライバシー情報リスクマップ】[19]



[19] 「影響度」及び「起こりやすさ」それぞれの評価指標についても、「JISX9251（ISO/IEC 29134：2017）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」における考え方に準拠している。

5.2.2. 影響度の判定方法

① 影響度のレベルは、以下の 4 段階で評価する。

レベル	評価項目ごとの評価指標
4 甚大	プライバシー情報の主体が、克服できないことがある重大な又は不可逆的な結果に直面する可能性がある
3 重大	プライバシー情報の主体が、深刻な困難を伴いながらも対処することが可能な重大な結果に直面する可能性がある
2 限定的	プライバシー情報の主体が、幾つかの困難は生じるものの、対処可能な不都合が生じる可能性がある
1 無視できる	プライバシー情報の主体は影響を受けないか、又は何ら問題なく対処できる幾つかの不都合が生じる可能性がある

② ①のレベル区分を判定するにあたっては、評価対象とするサービスで取り扱う情報の漏えい・改ざん等が発生した場合の影響について、「財産への影響」と「心身への影響」[20]の観点から次頁の「影響度判定表（概要版）」を用いて評価する。

③ 「PIA 調査シート」により、評価対象とするサービスが取り扱う情報（氏名以外の情報）を確認する。その情報が次頁の表に存在する場合、その位置する場所の左側に記載の数字を「財産への影響レベル」、下側に記載の数字を「心身への影響レベル」とみなした上で、双方のうち、より高い数字を影響度の一次評価案とする。
（例：評価対象とするサービスが取り扱う情報が「健康診断結果」である場合は、「財産への影響レベルは『2』」、「心身への影響レベルは『3』」となり、影響度の一次評価案は心身への影響レベルをとって「3」となる。）

④ 評価対象とするサービスが取り扱う個人に関する情報が複数存在する場合は、全ての情報について③の評価を行った上で、最も影響レベルが大きいものを一次評価案とする。

⑤ 「影響度判定表（概要版）」に、評価対象とするサービスが取り扱う情報が見当たらない場合は、「影響度判定表（詳細版）」を用いる。「影響度判定表（詳細版）」にも評価対象とするサービスが取り扱う情報が見当たらない場合は、以下の「影響度判定表（概要版及び詳細版）」に記載の「定義」に照らし合わせる等により判断する。

※ 影響度判定表は、「概要版」「詳細版」ともに、氏名とともに該当情報の漏

[20] 財産・心身への具体的な影響例は、JNSA（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）が過去に作成した、個人情報が漏えいした際の影響金額の算定ロジック（JO モデル）を参考としている。

えい・改ざん等が発生した場合の影響を示している。
したがって、PIA の対象とするサービスの性質上、該当情報が氏名とともに漏えい・改ざん等が生じ得ない場合においては、判定表内における記載箇所も変動する可能性があることから、実態に応じて適宜修正も可能であることに留意する。

【影響度判定表(概要版)】

4 甚大	返済不能な債務が発生		口座番号、暗証番号など	借入記録など	犯罪歴など
3 重大	財産が大幅に減少		パスポート情報など	現金残高など	
2 限定的	財産が脅かされる可能性が発生	社員番号など	健康保険証番号など	健康診断結果、障害情報など	DNA 情報など
1 無視できる	いら立ち程度	水栓番号など	身長など		
財産への影響 / **心身への影響**		煩わしい手間が発生(いら立ち程度)	不安、ストレスが発生	心理的な健康状態が悪化	長期にわたる心理的疾患を発症
		1 無視できる	**2 限定的**	**3 重大**	**4 甚大**

【影響度判定表(詳細版)】

4 甚大	返済不能な 債務が 発生		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 重大	財産が 大幅に 減少		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 限定的	財産が 脅かされる 可能性が 発生	(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、動画音声、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、服薬情報、アレルギー	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 無視 できる	いら立ち 程度	水栓番号など	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		
財産への影響		煩わしい手間が発生(いら立ち程度)	不安、ストレスが発生	心理的な健康状態が悪化	長期にわたる心理的疾患を発症
心身への影響		1 無視できる	2 限定的	3 重大	4 甚大

5.2.3. 起こりやすさの判定方法[21]

① 起こりやすさのレベルは、影響度レベルと同様、4段階で評価する。その判定は、【リスク評価項目 No.07～18 と観点の一覧】で設定された項目ごとに、それぞれの観点をどの程度満たすかによって判断する。

② 各リスク評価項目における観点を、以下のとおり〇・△・×の3段階で評価し、〇を2点、△を1点、×を0点とする。
観点のうち、「非該当」の項目があれば、その項目を除いて起こりやすさを判定する[22]。

> 〇（2 点）： 観点を満たす対応が実施されている
> △（1 点）： 対応が実施されているが、一部の観点を満たさない
> ×（0 点）： 対応が実施されていない

③ 「観点」の個数はリスク評価項目ごとに異なることから、項目ごとに満点の数値が変わる[23]ため、以下の起こりやすさ判定表に記載された割合を目安に各項目のレベルを判定する[24]。

レベル	評価項目ごとの評価指標
4 容易に起こり得る	非該当項目を除き、点数が **0 点**（全て「×」）
3 起こり得る	非該当項目を除き、点数が **5 割未満**
2 起こりにくい	非該当項目を除き、点数が **5 割以上**（平均で全て「△」）
1 無視できる	非該当項目を除き、点数が**満点**（全て「〇」）

④ 「起こりやすさ」のレベル判定は、リスク評価項目ごとに判定したレベルのうち、最も高いものを一次評価案とする。（例：評価対象とするサービスが取り扱う情報への対策について、「No.10 が『3』、それ以外のリスク評価項目が『1』」の場合、起こりやすさの一次評価案は『3』となる。）

---

[21]「起こりやすさ」の評価項目は、「JISX9251（ISO/IEC 29134：2017）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」や G20 Global Smart City Alliance による”Privacy Impact Assessment Model Policy”等を参考としている。

[22]（例）リスク評価項目 No.07 は4つの観点から構成されるため、本来は8点満点で評価を行うが、アプリを活用しない事業の場合、観点③は非該当であるため、残る3つの観点をもとに6点満点で評価する。

[23]（例）リスク評価項目 No.07は4つの観点からなる項目のため8点満点で評価するが、リスク評価項目 No.8 は2つの観点からなる項目のため4点満点で評価する。

[24]（例）4つの観点からなるリスク評価項目については、観点が4つとも「〇」の場合の得点は 8/8 点（満点）のため、起こりやすさを「1」と判定する。4つのうち3つ△・1つ〇の場合の得点は 5/8 点（得点率 62.5%＞点数 5 割以上）のため、起こりやすさを「2」と判定する。

【リスク評価項目 No.07～18 と観点の一覧】

■ **07. 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。）**

物理的観点	① 当社は、本サービスに関する情報（特に個人に関する情報の処理目的等）を、市民・利用者がHP等でいつでも閲覧できるようにしている。 ② 当社は、本サービスにおいて、個人に関する情報の処理目的等がわかる市民・利用者向けの説明資料を用意することとしている（利用規約、サービス約款等）。
技術的観点	③ 当社は、本サービスにおいて、アプリケーション上等で個人に関する情報の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）。
管理的観点	④ 当社は、本サービスにおいて、利用者が個人に関する情報の取り扱いについて同意した後に、利用者の認識・意図・希望と異なる情報処理がなされることのないよう、使用する個人に関する情報を選択したり、削除したりできるようにしている。

■ **08. 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。）**

管理的観点	① 当社は、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等が確認する体制を整備している。 ② 当社は、本サービスにおいて、市民・利用者（当市を含む）がアクセス可能な情報の開示請求窓口（その他相談窓口を含む）を設置している。

■ **09. 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。）**

管理的観点	① 当社は、本サービスにおいて、収集予定の全ての個人に関する情報の必要性を事業計画段階で明らかにしており、当社の判断のもと、「念のため」「参考として」等の名目で過剰な情報を収集していない。

■ **10. 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。**

技術的観点	① 当社は、サービスにおいて、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には適切なログオン手順（パスワード等認証情報を確認するもの）を取ることを必須としている。 ② 当社は、本サービスにおいて、IoT 機器、サーバ等に対する不正ログインを防止する対策を講じている（一定回数以上のログイン認証失敗によるロックアウト、安全性が確保できるまでの再ログインの間隔をあける機能の実装等）。
管理的観点	③ 当社は、本サービスにおいて、ログイン時のパスワード設定に関する組織内規程を定めるとともに、規程を適時見直すこととしている。 ④ 当社は、本サービスにおいて、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、それに則ったアクセス権を付与している。また特定の ID やアカウントの共同利用は行っていない（共同利用に起因する権限をもたない人員による不正アクセスを防止している）。 ⑤ 当社は、本サービスにおいて、アクセス権を定期的に見直すこととしている。 ⑥ 当社は、本サービスにおいて、当市や契約相手方との契約終了時又は合意したタイミングで自身のアクセス権を削除することとしている。

■ **11. 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。**

技術的観点	① 当社は、本サービスにおいて、イベントログを取得・保持している。 ② 当社は、本サービスにおいて、許可されていない変更操作を防ぐ仕組みを講じている。
管理的観点	③ 当社は、本サービスにおいて、データの重要な変更の承認・確認等のプロセスに関する社内規程を定めている。

■ **12. 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。（本来は別々で管理している個人に関する情報を、本来の利用目的を超えて紐づけたり、統合し保持することがないか）**

技術的観点	① 当社は、本サービスにおいて、API など、当該システムや DB に接続する手段を非公開としている。

管理的観点	② 当社は、本サービスにおいて、不適切な情報の紐づけ防止のための規程を定めている（取得した個人に関する情報を他事業に転用しない等）。又は、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。

■ **13. 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。**

物理的観点	① 当社は、本サービスにおいて、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）。 ② 当社は、本サービスにおいて、各データを機密性にしたがって分類し、その分類をわかりやすく示している（「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 当社は、本サービスにおいて、データや機器を取り扱う又は保管する場所に立ち入る人員に対し、適切な入退室管理策を講じている（IC カード方式、スマートフォン認証、生体認証等）。 ④ 当社は、本サービスにおいて、使用するデバイスや記録媒体に対し、接続制限の設定をしている（特定の USB メモリのみ利用可能にする等）。
管理的観点	⑤ 当社は、本サービスにおいて、データや機器を取り扱う又は保管する場所に非関係者が入室する際には、適切な管理を行っている（入退室の記録、身分証の携行確認、秘密保持誓約書の記入等）。また入室を許可した場合でも、非関係者を明確に見分けるための措置を講じている（色の異なる入退室カードを貸与する等）。 ⑥ 当社は、本サービスにおいて、個人のパソコンやスマートフォン等端末は原則として業務で用いないこととしている（BYOD としての利用（外出先やテレワーク等）やその他やむを得ない場合を除く）。また、テレワークに関する規程や、必要に応じて執務室内への個人端末の持ち込みを制限する規程等、端末の利用制限に関する必要な組織内規程を定めている。 ⑦ 当社は、本サービスにおいて、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）。 ⑧ 当社は、本サービスにおいて、データを持ち出す際には組織内で許可を得る等の組織内規程を定めている。 ⑨ 当社は、本サービスにおいて、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。 ⑩ 当社は、本サービスにおいて、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。

■ **14. 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。)**

物理的観点	① 当社は、本サービスにおいて、データ保管媒体を自然災害(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している(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)。 ② 当社は、本サービスにおいて、関連するバックアップデータ(クラウドサービスを用いたものを含む)を、元データと物理的に隔離され、かつ①を満たす場所に保管している。 ③ 当社は、本サービスにおいて、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。
技術的観点	④ 当社は、本サービスにおいて、重要な機器やネットワークを冗長化している。

■ **15. 個人に関する情報の不必要な長期保有が発生しないか。**

物理的観点	① 当社は、本サービスにおいて、紙媒体で保存されたデータについて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。 ② 当社は、本サービスにおいて、関連するハード媒体(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。
技術的観点	③ 当社は、本サービスにおいて、サーバ等で保存されたデータについて適切な方法で消去することとしている。
管理的観点	④ 当社は、本サービスにおいて、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。 ⑤ 当社は、本サービスにおいて、データの廃棄が完了した際は廃棄完了の旨を当市や契約相手方に報告することとしている。

■ **16. 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。**

技術的観点	① 当社は、本サービスにおいて、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。 ② 当社は、本サービスにおいて、関連するアプリケーション等に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。
管理的観点	③ 当社は、本サービスにおいて、情報システムの脆弱性に関する情報を適時受け取る体制を構築しており、脆弱性が発見された場合は速やかに対処することができる。 ④ 当社は、本サービスにおいて、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）を組織内規程で定めている。

■ **17. 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。）**

技術的観点	① 当社は、本サービスにおいて、外部との通信を常時モニタリングしている。 ② 当社は、本サービスにおいて、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。 ③ 当社は、①②で取得する情報の完全性を担保している（時刻の正確性等）
管理的観点	④ 当社は、①②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。

■ **18. 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・研修を講じているか。**

管理的観点	① 当社は、本サービスにおいて、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としている。

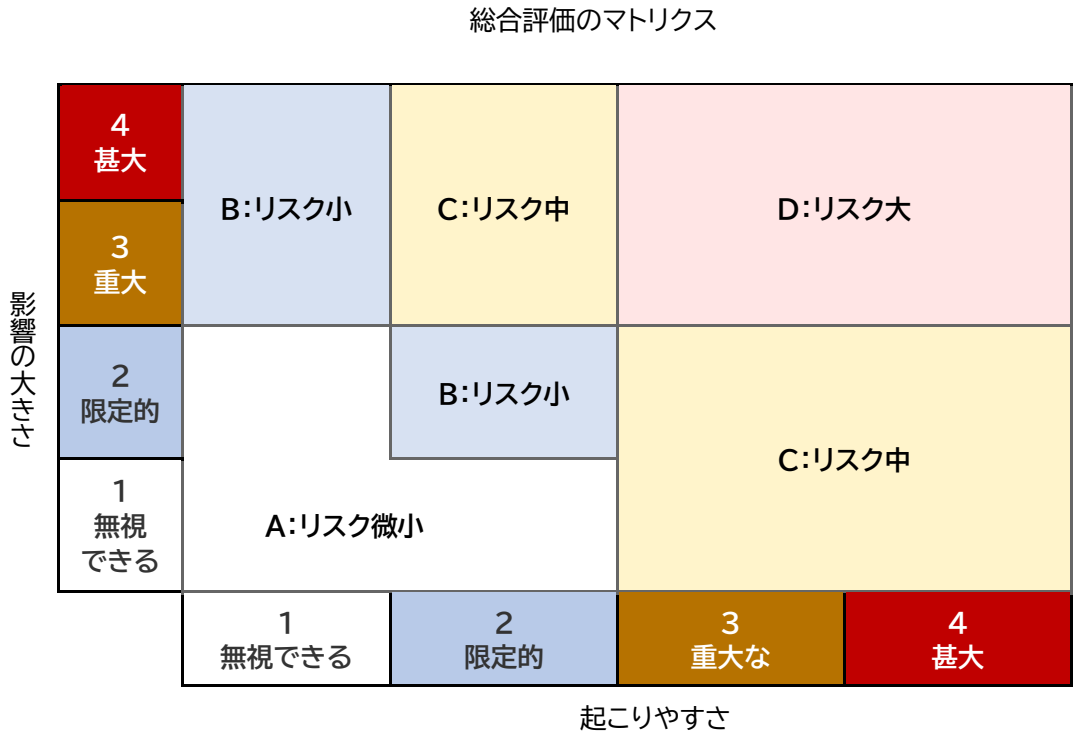
5.3 二次評価

一次評価結果及びサービスの内容を踏まえ、データガバナンス部会において議論し、総合的に判定する。

5.4 総合評価

一次評価及び二次評価を経て、PIA 総合評価を決定する。プライバシー情報リスクマップに基づく総合評価のマトリクスは以下のとおりである。

【プライバシー情報リスクマップ（総合評価）】



総合評価	内容
D:リスク大	サービスは原則実施不可（実施にあたり、事業者による追加的な対策の実施や、改善要求の履行を「必須」とする）
C:リスク中	サービスは実施可（ただし実施に当たり、事業者による追加的な対策の実施や、改善要求の履行を「推奨」する）
B:リスク小	サービスは実施可
A:リスク微小	サービスは実施可

本市は、決定した総合評価をサービス提供関係者に通達するとともに、とりわけ判定が C、D の場合には、必要な対策の要求又は勧告を行う。その後一定期間の後に、対象サービスの実施にあたって適切な対応が取られているかを確認するとともに、総合評価を見直し、サービスの実施について改めて判断する。