「情報銀行」認定制度
データ倫理審査会
運用ガイドライン
（TPDMS-1140）

一般社団法人日本ＩＴ団体連盟

情報銀行推進委員会

目次

はじめに 1
1. 適用範囲 1
2. 参照規格 1
3. 用語の定義 2
4. データ倫理審査会運用の基礎 4
4.1 データ倫理審査会の全体概要 4
4.2 データ倫理審査会の意義 6
4.2.1 プライバシー・バイ・デザイン／PIA 6
4.2.2 データ倫理審査会の意義 7
4.3 データ倫理審査会運用フロー 8
5. 「情報銀行」での事前準備 9
5.1 リスクアセスメント・チームの設置（参照：ISO / IEC 29134　6.3.1） 9
5.1.1 責任者（評価者）の任命 10
5.1.2 実施担当者（査定者）の任命 10
5.2 リスク基準の設定（参照：ISO / IEC 29134　6.3.1, Annex A） 11
5.2.1 リスク基準の考え方 11
5.2.2 影響度を推定する方法 12
5.2.3 発生の可能性を推定する方法 13
5.3 サービス全体像の把握（業務フロー図の作成） 14
5.3.1 個人情報のインプット・アウトプットの確認 14
5.3.2 サービス別及びユーザインタフェース（UI）別の画面遷移図 15
5.3.3 システム要件情報（参照：ISO / IEC 29134　7.3.1.2） 17
5.3.4 システム設計情報（参照：ISO / IEC 29134　7.3.1.3） 18
5.3.5 運用計画及び手順情報（参照：ISO / IEC 29134　7.3.1.4） 18
5.4 個人情報のフローの特定 18
5.4.1 対象となる個人情報の取扱いを明確化 18
5.4.2 業務の棚卸と個人情報取扱い業務の特定 19
5.4.3 特定した業務毎の個人情報の主要情報整理と集約 20
6. データ倫理審査会の準備 20
6.1. データ倫理審査会のメンバー選定 20
6.2. データ倫理審査会運営規程の作成 21
6.3. データ倫理審査会の事前協議 22
7. プライバシーリスクアセスメント 23
7.1. リスクの特定（参照：ISO / IEC 29134　6.4.4.1、Annex B） 23
7.2. リスク分析（参照：ISO / IEC 29134　6.4.4.2） 26

7.3. リスク評価（参照：ISO / IEC 29134　6.4.4.3、Annex D） 27
7.4. リスク対策の検討（参照：ISO / IEC 29134　6.4. 5、6.4.3） 28
7.4.1 リスク低減・保有・回避・移転 28
7.4.2 リスク対策の考え方 31
7.5. 残留リスクの認識 35
7.6. リスク対策の確認 35
7.7. PIA 報告書（参照：ISO / IEC 29134　6.5.1、6.5.2） 37
8. データ倫理審査会の開催 38
8.1. データ倫理審査会の開催趣旨（参照：ISO / IEC 29134　6.5.4） 38
8.2. データ倫理審査会の審査基準 38
8.2.1. 個人と「情報銀行」間の利益相反等（善行原則　beneficence） 38
8.2.2. 本人のメリット等（正義原則 justice/equality） 39
8.2.3. 想定リスクの妥当性・リスク対策の適切性（無危害原則 non-maleficence） 39
8.2.4. 個人情報の第三者提供条件の指定・変更方法（UI）（自律尊重原則　autonomy） 40
8.2.5. 提供先第三者の選定方法 41
8.2.6. 委任を受けた個人情報の提供の判断 41
9. リスク対策の実施 41
9.1. リスク対応等の決定 41
9.2. リスク分析表 41
9.3. リスクの見直し 42
10. PIA 報告書の公表 43
10.1. PIA 報告書最終版の作成 43
10.2 PIA 報告書最終版の公表 43
附属書A リスクアセスメント・チームの作業手順 45
附属書B データ倫理審査会の審査基準 46

（制定改訂履歴）

版	制改訂年月日	内容
初版	2021 年 7 月 1 日	新規制定

はじめに

データ倫理審査会は、「情報銀行」の事業内容が個人の利益に反していないかという観点から、データ利用に関する契約や利用方法、提供先第三者などについて適切性を審議し、必要に応じて助言を行うことを目的としている。

データ倫理審査会の運用は、リスクマネジメントプロセスを適用することによって個人情報の保護を維持し改善し、かつ、リスクを適切に管理しているという信頼を利害関係者に与える。

データ倫理審査会は、「情報銀行」のサービス設計時点から始まるプロセスであるため、プライバシー・バイ・デザインを保証することができる。データ倫理審査会は、「情報銀行」のサービス開始後も継続して運用される。

本ガイドライン中、「望ましい」と記載されている規定については、個人情報は、個人の人格尊重の理念の下に慎重に取り扱われるべきものであることに配慮して適正な取扱いが図られるべきとする法の基本理念を踏まえ、個人情報保護の推進の観点から、できるだけ取り組むことが望まれるものである。

このガイドラインは、認定基準を満たす「情報銀行」の運用を「情報銀行」内部で評価するためにも、外部関係者が評価するためにも用いることができる。

1. 適用範囲

このガイドラインは、「「情報銀行」認定申請ガイドブック」の認定基準「5.4.1 ガバナンス体制の具体的基準 ③諮問体制」に規定するデータ倫理審査会について、その運用を支援する具体的な指針として解説するものである。

「情報銀行」のサービスの種類又は規模を問わず、全ての「情報銀行」に適用できることを意図している。

なお、本ガイドライン中に事例として記述した部分は、理解を助けることを目的として、該当する事例及び該当しない事例のそれぞれにつき、典型的な例を示すものであり、すべての事案を網羅することを目的とするものではない。実際には個別事案ごとに検討が必要となる。また、幾つかの業種の例を取り上げたもので、すべての業種の例を網羅しているわけではない。

このほか、個人情報の性質及び利用方法又は事業実態の特殊性等に鑑み、特別に個人情報の適正な取扱いを確保する必要がある場合には、「情報銀行」認定において、別途更なる措置を要求することもあり得る。

2. 参照規格

本ガイドラインでは、データ倫理審査会の運用について、 ISO/IEC 29134：2017 Information technology — Security techniques — Guidelines for privacy impact assessment（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）を基本とする。この他、以下の規格を参照する。

・JIS Q 27001：2014 情報技術－セキュリティ技術－情報セキュリティマネジメント

システムー要求事項（ISO/IEC 27001：2013 Information technology - Security techniques - Information security management systems – Requirements）
・JIS Q 27002：2014 情報技術ーセキュリティ技術ー情報セキュリティ管理策の実践のための規範（ISO/IEC 27002：2013 Information technology - Security techniques - Code of practice for information security controls）
・JIS Q 15001：2017 個人情報保護マネジメントシステムー要求事項
・JIS X 9250：2017 情報技術―セキュリティ技術―プライバシーフレームワーク（プライバシー保護の枠組み及び原則）（ISO/IEC 29100:2011 Information technology -- Security techniques -- Privacy framework）
・JIS Q 31010：2012 リスクマネジメントーリスクアセスメント技法
・ISO/IEC 29184 Information technology － Online privacy notices and consent 情報技術 － オンラインにおけるプライバシーに関する通知及び同意
・Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679（データ保護影響評価（DPIA）及び取り扱いが 2016/679 規則の運用上、「高いリスクをもたらすことが予想される」か否かの判断に関するガイドライン）
・ISO26000 Guidance on social responsibility 社会的責任に関する手引

3. 用語の定義

このガイドラインで使用する用語は、このガイドラインで特別の定めがあるもののほか、参照規格及び JIS Q 0073：2010 リスクマネジメントー用語、JIS Q 27000 情報技術ーセキュリティ技術ー情報セキュリティマネジメントシステムー用語、「情報信託機能の認定に係る指針」、「「情報銀行」認定申請ガイドブック」において使用する用語の例による。

(1) プライバシーへの影響／プライバシーリスク
本人又は本人が所属するグループのプライバシーに（悪）影響を与え得るもの。プライバシーへの影響は、個人情報保護法に違反している個人情報の取り扱いだけではなく、適法であっても発生する可能性がある。

(2) 「情報銀行」サービスの利用環境
個人情報が依存する「情報銀行」サービスの利用環境は、通常、以下のものがある。
- スマートフォン、タブレット、家庭用コンピュータ上のインターネットブラウザソフトウェア、インターネットテレビ等のユーザが提供したハードウェア、およびソフトウェア
- ハードウェア：コンピュータ、通信リレー、USB ドライブ、ハードドライブなど
- ソフトウェア：オペレーティングシステム、メッセージング、データベース、ビジネスアプリケーションなど

- コンピュータチャンネル：ケーブル、ワイヤレス、 光ファイバ など
- 個人：ユーザ、管理者、トップマネジメントなど
- 紙媒体：印刷、コピーなど
- 伝送チャネル：メール、ワークフローなど

「情報銀行」サービスの利用環境（リスク源が自主的に行うことができるかどうか）に関するアクションは、通常以下の通り。

- 異常な使用/機能不安：「情報銀行」サービスの利用環境は、変更または破損することなく意図された使用状況から逸脱する
- ダメージ：「情報銀行」サービスの利用環境の一部または全部が破損
- スパイ活動：「情報銀行」サービスの利用環境は破損することなく監視
- 消失：「情報銀行」サービスの利用環境が紛失、盗難、売却、譲渡されたため、財産権を行使することはもはや不可能
- 変更/変化：「情報銀行」サービスの利用環境が変化
- オーバーロード/運用上の限界を超過：「情報銀行」サービスの利用環境は、オーバーロード、過剰使用、または正常に機能しない条件で使用される

(3) 本人又は個人

「情報銀行」に個人情報の取扱いを委任している個人。個人情報保護法上、個人情報によって識別される特定の個人、言い換えれば個人情報の対象者を本人という。

(4) 評価者

「情報銀行」側のリスクアセスメント責任者をいう。詳しくは 5.2.1 参照。

(5) 査定者

「情報銀行」側のリスクアセスメント担当者をいう。査定者は、リスクアセスメントを始めとするデータ倫理審査会運営全般を担当する。

リスクアセスメントは複数の観点から実施しなければならないため、複数の立場の者を任命する必要がある。もっとも、当該者間での意見が異なったり責任が不明確になったりすることを避ける必要があるため、各者の役割分担を明確にし、全般を総括するリーダーを合わせて任命する。詳しくは 5.2.2 参照。

(6) 提供元

本人の指示に基づき、個人情報を「情報銀行」に提供する組織・個人。

(7) 提供先第三者

本人の指示に基づき、「情報銀行」が個人情報を提供する先の組織。

(8) 委託先

「情報銀行」が個人情報の取扱いを委託している組織・個人。

(9) 利害関係者

「情報銀行」におけるある決定事項若しくは活動に影響を与え得るか、その影響を受け得るか、又はその影響を受けると認識している、個人又は組織

例えば、以下の者が挙げられるが、これらに限定されるものではない。

- 本人
- 消費者団体
- 提供元
- 提供先第三者
- 委託先
- 規制当局／認定個人情報保護団体

(10)発生の可能性（likelihood）

何かが起こる可能性。一般的な用語を用いて示すか、又は数学的に示す。

例）発生確率。所定時間内の頻度

(11)脅威（threat）

リスク事象（ペリル peril）とも言われるが、目的に有形の影響を与える事象であり、不正アクセス、盗難、紛失、流出、改ざん、紛失、毀損・滅失、破壊、誤用、誤操作、追跡不能などがある。

例）ドア、窓などの物理的保護の欠如、監査証跡（ログ管理）の欠如、アクセス管理の欠如など

(12)リスク源（risk source）

脅威の発生の可能性を生む事象であり、危害要因（ハザード hazard）ともいわれ、一つの脅威が、つけ込むことができる脆弱性をいい、いわゆるセキュリティ・ホールを指す。

例）ドア、窓などへの物理的保護の欠如、監査証跡（ログ管理）の欠如、アクセス管理の欠如などがある。

(13)多乱（disturbance）

アウトプットを目標値からはずれさせようとするリスク源への影響。

4. データ倫理審査会運用の基礎

4.1 データ倫理審査会の全体概要

「情報銀行」は、個人情報に対する個人によるコントローラビリティを高めること

を基本的な目的としており、これを適切に担保するには、各「情報銀行」に設置される諮問体制であるデータ倫理審査会の役割が重要となる。

データ倫理審査会は各「情報銀行」で個別に組織するものであるが、社外委員を含んでおり、「情報銀行」とは異なる第三者的立場で「情報銀行」における個人情報の取扱いについて、利用者たる個人の視点に立って適切な運営が行われているかという視点からチェックを行う。これにより個人情報の適切な取扱い、そして個人からの信頼獲得と「情報銀行」事業の健全な発展に寄与することが期待される。信頼は透明性に基づいており、データ倫理審査会はオープンなコミュニケーション、共通の理解と透明性を促進する規律あるプロセスである。利害関係者とプライバシーリスクに関する認識を共有し、プライバシーリスクを低減する対策を検討する。

もっとも、データ倫理審査会が適切に機能するには、その役割について一定の共通認識が持たれることが望ましく、本ガイドラインを参照されたい。

データ倫理審査会において審議するべき基本的な内容等については以下のとおりである。なお、運営の適切性を担保するため、構成員及び（必要な範囲の）議事録は公表されるべきである。

■データ倫理審査会における審議の考え方

・「情報銀行」は、個人の代理として、個人が安心して自らに関する情報を預けられる存在であることが期待される。「情報銀行」は利用者たる個人の視点に立ち、適切な運営が確保する必要がある。

・このため、データ倫理審査会は、「情報銀行」の事業内容が個人の利益に反していないかという観点から審議を行う。

（例）

・個人によるコントローラビリティを確保するための機能が誤解のないＵＩで提供されているか／個人情報の第三者提供に係る条件の指定及び変更の方法（ＵＩ）はわかりやすいか

・提供先第三者の選定方法は適切か／提供の判断は適切か

・個人の同意している提供先第三者の条件について、個人の予測できる範囲内で解釈されて運用されているか

・個人にとって不利益となる利用がされていないか／個人に対し個人情報の利用によるリスクが伝えられているか／個人情報の利用目的は適切か

・個人と「情報銀行」の間の契約は適切か

・個人にとって高いリスクを発生させる恐れがある場合には、GDPR で義務づけられている DPIA（データ保護影響評価）を参考にすることも考えられる

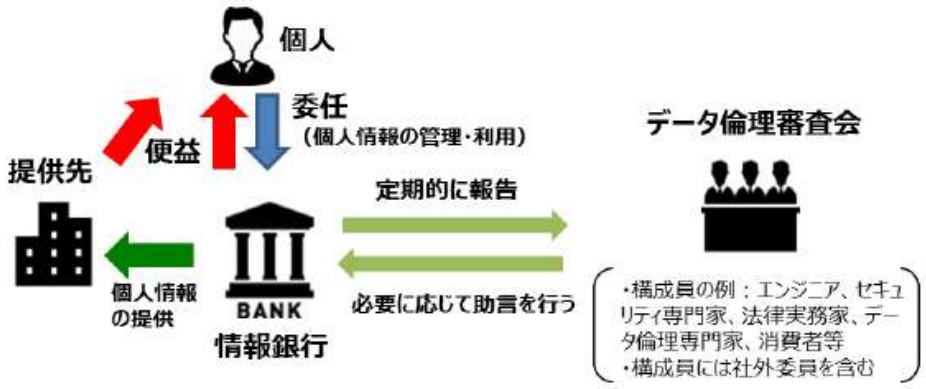


図 1.　諮問体制（データ倫理審査会）に関する事項

「情報信託機能の認定に係る指針 ver2.0

4.2 データ倫理審査会の意義

4.2.1 プライバシー・バイ・デザイン／PIA

世界的なプライバシー権保護に対する潮流として、「プライバシー・バイ・デザイン」「データ保護・バイ・デザイン」がある。事後ではなく事前に、初期設定・デフォルトとして IT システム及びビジネス・プラクティスの設計・構造に組み込まれ、データのライフサイクル全体を通じて透明性をもってプライバシー権を尊重する考え方である。

そして、プライバシー・バイ・デザインの実践方法として国際的にも取り組まれているのが、「プライバシー影響評価（Privacy Impact Assessment、PIA）」「データ保護影響評価（Data Protection Impact Assessment、DPIA）」である。実際の個人情報の取扱いに先立ち、計画段階でプライバシーへの影響に関するアセスメントを行い、事前想定でＰＤＣＡを行い、リスク対応を盛り込んだ実行計画とするものである。個人情報の取扱開始後・事業実施後も、定期的にあるいは必要に応じて継続することが必要である。

プライバシー・バイ・デザイン、そしてプライバシー影響評価は、早期警戒システムとして機能する。個人情報を取り扱う組織が闇雲にあらゆる対策を講じようとすれば多額の投資が必要となる。これに対して、個人情報の取扱いに起因する潜在的なプライバシーリスクを事前に予測することで、リスクを予防したり受容可能なレベルにまで軽減したりするためにどのような対策が必要かについて優先順位を付して検討することができる。プライバシー影響評価を実施せずに、あとから容認できないプライバシーへの影響が判明した場合には、プロジェクトを完全にキャンセルする必要も考えられるし、計画段階でプロジェクトを修正しなければならない場合もある。プライバシー・バイ・デザインやプライバシー影響評価は個人情報取扱い上の問題を早期に識別し、潜在的懸念を早期に考慮し、個人情報取扱い上のミスを避けることと、合理的なスケジュール・コストを両立させるのに役立つ。

4.2.2 データ倫理審査会の意義

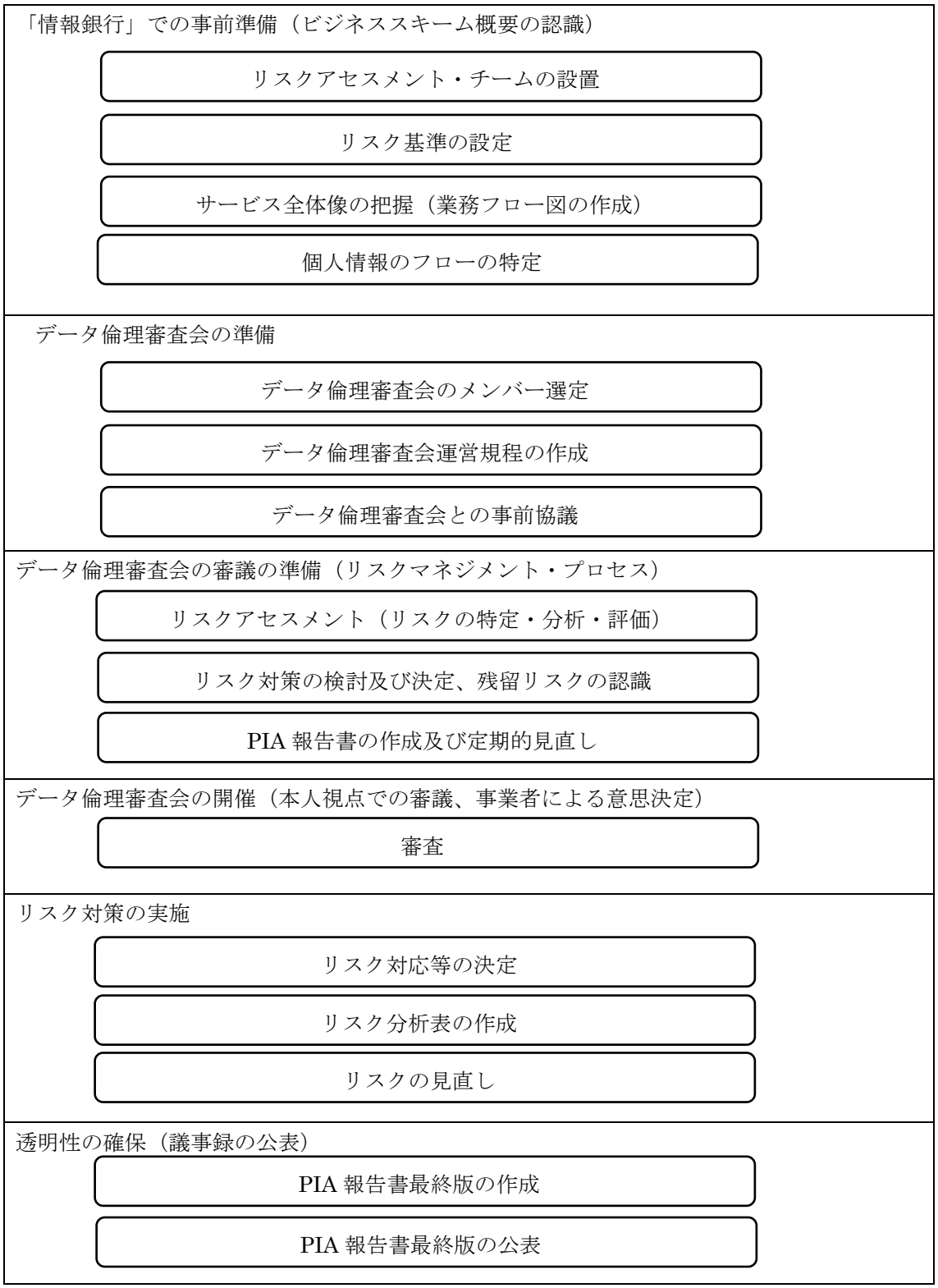
データ倫理審査会は、プライバシー・バイ・デザインを実践し、「情報銀行」が実施したプライバシー影響評価をチェックするスキームであり、データ倫理審査会の目的は、データ倫理審査会での審議結果、リスクアセスメントの結果を利害関係者に伝えることである。データ倫理審査会は、複数の様々な立場の利害関係者（本人、マネジメント層、社外の関係者、官公署等）からの信頼・期待に応えていく必要があるが、データ倫理審査会及びプライバシー影響評価には、例えば次の効果が期待される。

・本人に対して個人情報の権利を尊重し、本人の視点に立ったサービスであることを証明し、「情報銀行」のプロセス、情報システム又はプログラムの設計に、個人情報保護対策が組み込まれているという本人の信頼を得るのに役立つ。
・新しい「情報銀行」サービスのプライバシーリスクをレビューし、その影響と可能性を評価する。
・個人その他の利害関係者とプライバシーリスクに対する認識を共有し、リスクを軽減し、個人情報保護責任を果たしている説明・証跡を提供する。
・マネジメント層にとっては、個人情報リスクを管理し、意識を高め、責任（accountability）を確立するための手段となり、個人情報の取り扱いに関する可視性、及びそれが引き起こす可能性のあるリスクと影響、「情報銀行」サービス戦略へのインプットとなりうる。個人情報の取り扱いに関するリスク要件をよりよく理解し、要件に対する活動を評価する機会として、「情報銀行」サービスの設計及び提供のためのインプットとして、また実施後の変更管理プロセスを通じてレビュー及び修正に用いることができる。
・「情報銀行」が個人情報保護を真剣に受け止めており、従業者、委託先、提供元及び提供先第三者に遵守させるべき事項を体系的に見える化する。提供元、提供先第三者に対して、「情報銀行」や提供先第三者が個人情報をどのように処理しているかを評価する手段にもなる。
・官公署（規制当局）に対しては、法令遵守や個人情報保護の要件を満たしていることの説明に役立つことが考えられる。

データ倫理審査会は、以下の基本的な機能を果たす。

・影響を受ける対象者、影響を受ける個人情報のライフサイクルのプライバシーリスクについて、リスクが残留又は低減されるかにかかわらず確認する。
・プライバシーリスクを改善・是正する対策について確認する。議事録内容については、機密性を明確に評価し、分類する必要がある（非公開、機密、公開など）。

4.3 データ倫理審査会運用フロー



5. 「情報銀行」での事前準備

データ倫理審査会にて審議を受ける前に、「情報銀行」としてのプライバシー影響評価を実施しなければならない。そのための準備として、まずは以下を行う必要がある。

・リスクアセスメント・チームの設置
・リスク基準の設定
・サービス全体像の把握
・個人情報のフローの特定

5.1 リスクアセスメント･チームの設置（参照：ISO / IEC 29134　6.3.1）

「情報銀行」側でリスクアセスメントを行うチームを設置する。チームメンバーは以下を含むものとする。

表 1. リスクアセスメント・チームメンバー

メンバー		担うべき役割
責任者（評価者）		プライバシー影響評価を始めとするデータ倫理審査会運営全般について責任を負う。
実施担当者（査定者）		プライバシー影響評価を始めとするデータ倫理審査会運営全般を担当する。全般を総括する実施担当リーダーを任命するほか、以下の担当者を任命する。
必須	「情報銀行」担当者	「情報銀行」のスキームや実務改善の検討を行う。
必須	個人情報保護管理者	個人情報保護の観点を中心に、プライバシー尊重のための検討を行う。
任意	法務部門	法令遵守・契約実務を中心に、プライバシー尊重のための検討を行う。
必須	情報セキュリティ部門	セキュリティ対策が十分か等の検討を行う。
任意	人事、経理・財務部門、「情報銀行」運営部門、広報部門及び内部監査などの従業者	経営資源の配分の妥当性、事業収益と事業リスクのバランスの妥当性、本人その他の利害関係者とのコミュニケーションの在り方等について検討を行う。
任意	アプリケーション及びデータベース管理者 コンピュータ又はネットワーク管理者	システム構築・管理の視点からリスク分析・リスク対策が十分か、他のメンバーからの指摘が実現可能か等の検討を行う。

任意	アプリケーション運用者 コンピュータ又はネットワーク運用者 保守要員	設計通りの運用が担保できるか、運用上のリスクが考慮されているか等の検討を行う。

5.1.1 責任者(評価者)の任命

「情報銀行」側のリスクアセスメント責任者（評価者）を任命する。評価者は、プライバシー影響評価を始めとするデータ倫理審査会運営全般について責任を負い、データ倫理審査会議事録及び PIA 報告書に署名する。この責任を果たせる立場の者を任命する。

リスクアセスメントには、マネジメントレベルの強力な関与が必要である。評価者はマネジメントレベル（役員相当）であることが望まれる。また評価者は、リスクアセスメントの実施に十分であると判断できるレベルの人員・人数の実施担当者を任命する責任があり、リスクアセスメントの実施に必要なリソースが十分に割り当てられていることを確認する必要がある。

また評価者は、次の観点に対応する必要がある。詳細は 5.2 以下を参照すること。

・本人と「情報銀行」双方への影響レベルを推定するための基準は何か（例えば、識別レベル、個人情報の機微度、影響を受ける本人の人数、「情報銀行」の影響レベル）。
・発生の可能性を推定するために使用される基準・尺度は何か（例えば、「情報銀行」サービスの利用環境の脆弱性とその脆弱性を悪用するリスク源の能力）。
・影響度を推定するための尺度は何か。
・リスクを評価するために使用される各組み合わせ（影響度と発生の可能性のレベル）の重要性は何か。特に、リスク受容の基準は何か。
・影響度と発生の可能性のレベルに対処するために適用可能な戦略は何か。特に、許容できるリスクに対する戦略は何か。
・個人情報処理の利点によって戦略はどのように変更されるか。

5.1.2 実施担当者(査定者)の任命

「情報銀行」側のリスクアセスメント担当者（査定者）を任命する。査定者は、プライバシー影響評価を始めとするデータ倫理審査会運営全般を担当する。

リスクアセスメントは複数の観点から実施しなければならないため、表 X のように、複数の立場の者を任命する必要がある。もっとも、当該者間での意見が異なったり責任が不明確になったりすることを避ける必要があるため、各者の役割分担を明確にし、全般を総括するリーダーを合わせて任命する。

5.2 リスク基準の設定（参照：ISO / IEC 29134　6.3.1, Annex A）

5.2.1　リスク基準の考え方

リスク基準は、リスクの重大性を評価するための目安となる条件である。影響度と発生の可能性に関する評価基準を定める。5.2.2 及び 5.2.3 に示す基準に基づいてもよいし、「情報銀行」によってこれらと異なる基準を定義してもよい。

リスク基準（risk criteria） リスクの重大性を評価するための目安とする条件。 注記1 リスク基準は、「情報銀行」の目的並びに外部状況及び内部状況に基づいたものである。 注記2 リスク基準は、規格、法律、方針及びその他の要求事項から導き出されることがある。 JIS Q 0073：2010 リスクマネジメント－用語

リスク基準は、「情報銀行」の価値、目的、及びリソースを反映する必要がある。リスク基準を定義する際には、以下の要素を考慮する。

- 個人情報保護に影響する法的及び規制上の要因
- 業界ガイドライン、専門的基準、企業方針、顧客契約などの外部要因
- 特定のアプリケーション又は特定の利用場面の文脈で事前に決められた要素
- 情報システムの設計及び関連する個人情報保護要件・安全対策に影響を与える可能性のある他の要因
- 製品、サービス、又はシステムのユーザへの危害。危害には、物理的、経済的、評判の低下、家庭内生活の侵害、身体的、場所と空間、行動的、通信上、データと画像、思考と感情、協同などの様々な種類のプライバシーへの（悪）影響などが含まれる。
- 法的規制要件、契約上の義務
- 利害関係者の期待と認識、及びのれんと評判に対する悪影響
- 個人データの可用性、機密性、整合性の運用上の重要性
- 情報処理の戦略的価値
- 情報処理によってもたらされる現在価値と将来の機会、別名「戦略的価値」

リスク（risk） 目的に対する不確かさの影響。 注記1 影響とは、期待されていることから、好ましい方向及び／又は好ましくない方向にかい（乖）離することをいう。 注記2 目的は、例えば、財務、安全衛生、環境に関する到達目標など、異なった側面があり、戦略、組織全体、プロジェクト、製品、プロセスなど、異なったレベルで設

定されることがある。

注記3 リスクは、起こり得る事象、結果又はこれらの組合せについて述べることによって、その特徴を記述することが多い。

注記4 リスクは、ある事象（周辺状況の変化を含む。）の結果とその発生の可能性との組合せとして表現されることが多い。

注記5 不確かさとは、事象、その結果又はその発生の可能性に関する、情報、理解若しくは知識が、たとえ部分的にでも欠落している状態をいう。

JIS Q 0073：2010 リスクマネジメント－用語

5.2.2 影響度を推定する方法

どのくらいのダメージが発生するのかを推定する。例えば、以下のような指標が考えられる。

但し、ダメージは本人にのみ発生するものではなく、本人を含むグループへの風評被害が発生したり、「情報銀行」やそれ以外の他の事業者等へのダメージ等も発生したりする可能性がある。例えば、個人情報に関する重大な不適切事案が発生すると、本人だけではなく、本人が所属するグループ（居住地域、遺伝を共通にする者など）にも被害を与える可能性がある。また不適切事案を発生させた事業者にダメージが発生するだけではなく、同種業界や同種のシステムなどにも嫌悪感や萎縮効果などのダメージが広がりうる。

さらに影響度は、本人の置かれている立場等によっても変化する可能性がある点に留意する。例えば、平均的な個人であれば家族に住所を知られたとしてもプライバシーに重大な影響を受けない場合が多いと考えられる一方で、DV 被害者の場合は甚大な被害を受けるおそれが高い。

表２．個人情報の性質に基づく影響度の例

影響度	個人情報の性質
1　小	一般に公開等されている情報
2　中	正当な権限を有する者のみアクセスできる情報（限定公開された情報等）
3　大	本人の評判に影響を及ぼす可能性のある情報（所得、刑罰など）
4　甚大	本人の健康、自由、生命等に影響を及ぼす可能性のある情報（人事評価、健康情報、犯罪被害をもたらす情報など）

※それぞれを明確に区分できない可能性に十分留意する（特に３と４、２と３等）

表３．影響度の指標例

影響度の指標	影響の程度
1　小	個人は影響を受けないか、または、不都合（情報の再入力、煩わしさ、苛立ちなど）自体はあるものの問題なく対処することができる。
2　中	個人は、対応に困難（余分なコスト、ビジネスサービスへのアクセス拒否、恐怖、理解の欠如、ストレス、体調不良など）を伴うものの対処することができる、重大な不都合に遭遇することがある。
3　大	個人は、対応に重大な困難（資金面、物的損害、失業、健康状態の悪化など）を伴う、重大な結果に遭遇する可能性がある。
4　甚大	個人は、克服できない重大な、または不可逆的な結果に直面する可能性がある（資金面、就業不能、長期にわたる心理的または身体的疾患、死亡など）。

5.2.3 発生の可能性を推定する方法

5.2.2 では、リスクが発生した際の影響度を推定する方法を記述した。5.2.3 ではリスクが発生する可能性を推定する。「情報銀行」サービスの利用環境（ハードウェア、アプリケーション、情報記録媒体等）の脆弱性とそれを利用するリスク源の能力（スキル、利用可能な時間、財源、情報システムの活用、モチベーションなど）を考慮して、各脅威が悪用される可能性を推定する必要がある。

発生の可能性は、「被害の発生の可能性（発生確率）」ともいわれる。ここでいう確率は、一般的な「客観確率」では測ることができない。「客観確率」は、繰り返し試行（過去の実績）によって発生する頻度として確率を求める。この方法で考えると、例えば「個人情報の保管キャビネットを施錠していない」という「弱点（リスク発生源）」に対して、「盗難」の発生という「脅威（リスク事象）」が、過去に発生したことがないので発生確率は０、即ちリスクは“ない”となるが、これは誤りである。

リスク分析では、過去に発生していない事象について「発生の可能性」を考える。例えば「個人情報の保管キャビネットを施錠していない」は、“常に”「盗難」の可能性があるので発生確率は「いつでも起きる」と考える。この手法を「主観確率」という。

表４．発生の可能性の指標例

発生の可能性の指標	発生の可能性
1　ほとんど起きない	「情報銀行」サービスの利用環境の特性を利用して脅威が起こる可能性は僅少である。 例）十分な技術的、物理的アクセス権限設定を施したデータセンターにおける内部不正など。

2　起きることがある	「情報銀行」サービスの利用環境の特性を利用して脅威が起こることは困難である。 例）通信の入口対策、内部対策、出口対策などの十分な多段防護を施したデータセンターにおけるサイバー攻撃等。
3　しばしば起きる	「情報銀行」サービスの利用環境の特性を利用して脅威が起こる可能性がある。 例）説明が理解しにくいユーザビリティでは、本人が意図しないか、又は理解していない個人情報の取扱いが生じる。
4　いつでも起きる	選択されたリスク要因にとって、「情報銀行」サービスの利用環境の特性を利用して脅威を実施することは極めて容易である。 例）提供先第三者への個人データ移送において、提供先第三者のアクセス認証が不十分な場合、サイバー攻撃を排除できない。

リスク発生の可能性は、インターネットへのアクセス、外部サイトとのデータ交換、他の情報システムとの相互接続、システムの異質性または可変性などによって、変化させることができる。逆に、相互接続がなく、インターネットに接続されていない同質のシステムは、リスク発生の可能性を低減させる可能性がある。

5.3 サービス全体像の把握（業務フロー図の作成）

5.3.1 個人情報のインプット・アウトプットの確認

どのように業務を実施しているかプロセスを明らかにする。提供元、「情報銀行」、提供先第三者、データセンター、委託先等、関連する全ての個人情報の取り扱いについて部門毎に個人情報が自部門に入って来てから他へ出て行く（無くなる）までのプロセスを、取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄の情報のライフサイクルで捉える。情報のライフサイクルとは、特定した情報が社内に入ってから出て行くまでの、「取得・作成」→「処理・加工」→「保管・バックアップ」→「移送・送信」→「返却」→「消去・廃棄」という、情報の取扱の流れを指す。続くリスク認識は、情報のライフサイクルの全ての局面ごとに検討する必要がある。

特に、以下の表５項目について個人情報の流れを識別する。

表５． 個人情報の流れの検討

・組織内で誰が個人情報の取扱いの責任を負うのか（誰が責任者なのか）
・取り扱われる個人情報の内容・種類
・個人情報の取り扱いによって本人にもたらされる主な便益は何か
・本人が自分の個人情報の処理について決定・関与等できるか（通知、同意、拒否、アクセス、修正、削除など）。またその方法・具体的状況について。
・個人情報の収集方法と提供元
・個人情報の利用目的
・個人情報の取扱い方法
・収集された情報が他の情報源からの情報と結合されるか、突合されるか
・個人情報の利用期間及び保管期間
・個人情報の管理及び変更方法、「情報銀行」サービスの利用環境
・個人情報取扱者とアプリケーションが個人情報を保護する方法
・個人情報の提供先第三者。また提供先第三者における個人情報の取扱い方法
・より低いレベルの個人情報保護が適用される提供先第三者に提供された個人情報の取扱い
・個人情報の廃棄時期・廃棄方法

5.3.2 サービス別及びユーザインタフェース(UI)別の画面遷移図

本人が「情報銀行」に委任した個人情報の第三者提供に係る条件の指定及び変更の方法を明らかにする。本人がアクセスする画面遷移図を作成する。画面は、以下の要件を満たさなければならない。

- 個人と「情報銀行」間の契約の内容、「情報銀行」サービス利用規約などの説明
- 個人情報の取扱いに関する明示事項
- 会員登録の手続き
- 個人情報の取得画面及び取得した個人情報の閲覧
- 提供先第三者の説明及び個人情報を提供した提供先第三者の一覧
- 第三者提供に係る条件の指定及び同意の取得
- 個人情報の取扱いに関する変更手続き（追加、訂正、削除、利用停止、提供の停止）
- 苦情および相談への対応

画面遷移図は、本人（本人の権利への対応）の観点からのプライバシーリスクを個別に検討するための基礎資料として有効である。

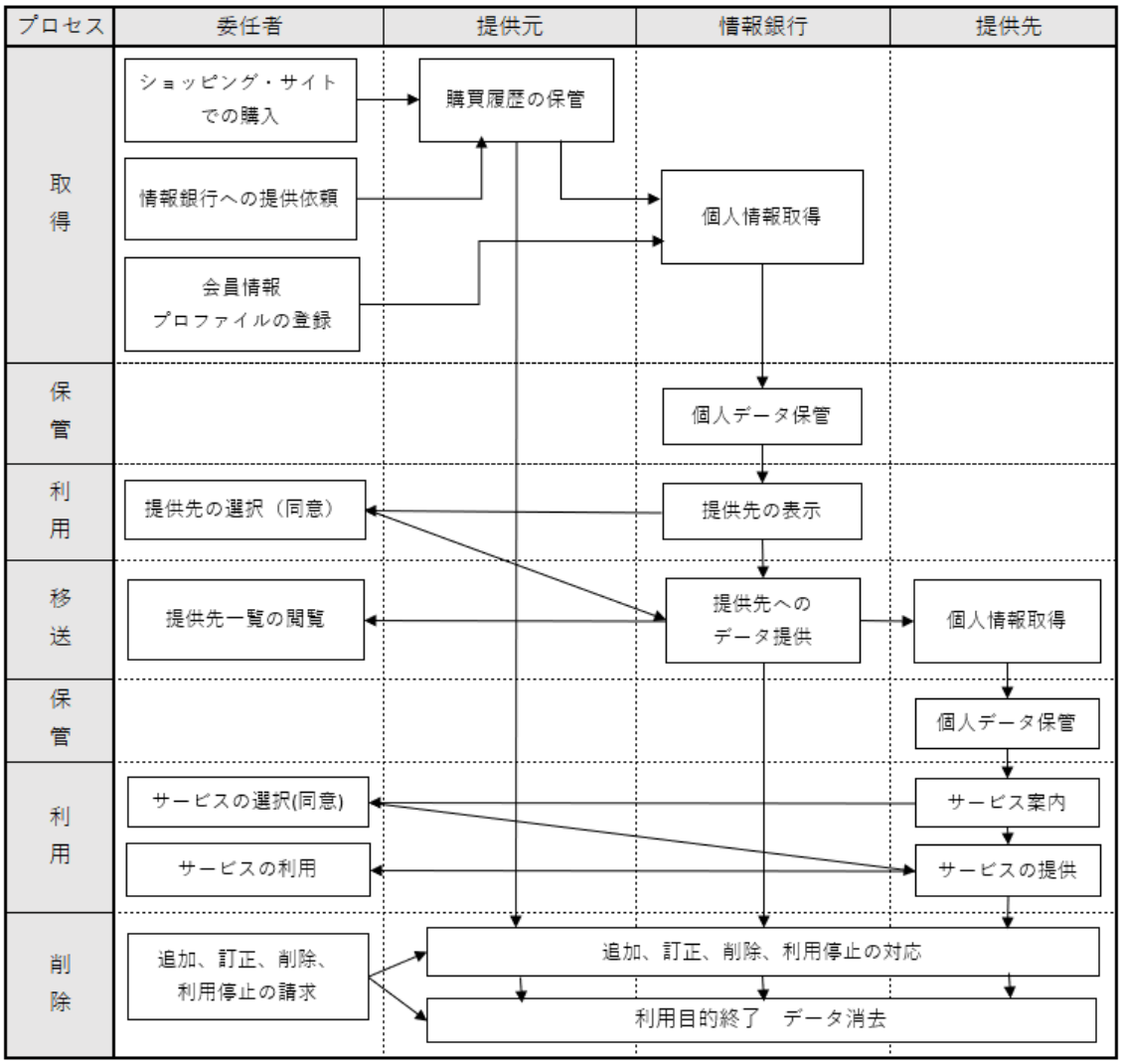


図２．業務フロー図の例

この作業により、本人、提供元と「情報銀行」の各部門、提供先第三者、委託先等の間で、情報の流れを具体的に把握でき、業務の内容と責任範囲を明確にすることができる。

情報の“ライフサイクル”によっては、 委託や提供など社外に渡る場合、倉庫やデータセンターなどロケーションが異なる場合や、委託先や他支店への移送・配送等を外部に依頼する場合もある。

作業工程を経るごとに、管理責任部門が変わることがあるので、工程間の情報の授受については、特に責任を明確にすることが重要なポイントとなる。例えば、情報を移送する場合、前工程が送信（届ける）なのか、後工程が受信（取りに行く）なのかなど、責任の所在を確認する必要がある。

業務フロー図（ワークフロー・ダイアグラム）
フロー図は、情報を取り扱う各局面（プロセス）に対して、情報がどこから来るか（インプット）と、どこへ行くか（アウトプット）を図式化する技法。情報のライフサイクルをフロー図にするためには、一つ一つのプロセスをインプットとアウトプットでつなげて全体像を記述する。

［参考］類似の手法に流れ図（フロー・チャート）がある。フロー・チャートは、プロセス内の処理内容の順序や判断分岐を記述することに特徴を持つ、主にプログラム構造を記述するために使う手法として有効である。

① 業務フロー図のチェック
プロセスとプロセスを矢印でつなぐ。このとき、アウトプットとインプットで情報のデータ形態が一致しているか確認する。例えば、前のプロセスのアウトプットが「応募ハガキ」で次のプロセスのインプットが「宛名データ」となっている場合、「入力」プロセスの記述が欠落していることがわかる。

② 業務フロー図の先頭と最後
業務フロー図の先頭は、どこ（提供元や本人）から「取得（授受）」するかにつながるインプットになる。先頭のインプットの前に「どこ（取得元）」及び「取得するデータ形態」を記述する。
フロー図の最後は、情報が無くなる「納品（移送）」、「返却」または「消去・廃棄」となる。例えば、インプット「応募ハガキ」をアウトプット「宛名データ」にする「入力」プロセスでは、入力したパソコンに残る情報（中間生成物）の「消去・廃棄」プロセスまでつなぐ。

5.3.3　システム要件情報（参照：ISO / IEC 29134　7.3.1.2）

また、サービス全体像を把握するため、システム要件についても記述することが望ましい。システム要件情報には、以下が含まれていることが望ましい。

- 処理の目的
- 情報システムによってサポートをしているか、又はサポートをする予定のビジネスプロセスの説明
- 情報システムに対して定義されている機能要件のリスト、及びそれらの義務又は実装のレベル
- 情報セキュリティ対策方針
- データをどのように集め、誰から、なぜ収集するかについての記述。説明には、誰が個人情報にアクセスできるかを記載する

・ 情報システム又はその個人情報が第三者と共有されることが意図されている場合、その情報システム又は個人情報が誰と共有されるのか、及びその目的
・ この情報システムに関与する個人情報の処理の正当性

5.3.4 システム設計情報（参照：ISO / IEC 29134　7.3.1.3）

サービス全体像を把握するため、システム設計についても記述することが望ましい。システム設計情報には、以下が含まれていることが望ましい。

・機能的（又は論理的）アーキテクチャの概要
・物理的アーキテクチャの概要
・個人情報を含む可能性のある情報システム、データベース、テーブル、及びフィールドの構造とリスト
・本人に通知して同意を得るタイミングを説明する業務フロー図
・接続された当事者と転送されたデータフィールドを定義するインタフェースのリスト
・サーバポート、プロトコル、API、及び暗号化の詳細

5.3.5 運用計画及び手順情報（参照：ISO / IEC 29134　7.3.1.4）

サービス全体像を把握するため、運用計画及び手順についても記述することが望ましい。運用計画及び手順情報には、以下が含まれていることが望ましい。

・情報システムの識別要素とユーザ管理の概念
・運営コンセプト。情報システム又はその一部がオンサイトで運営されているか、外部から運営されているか委託、再委託の有無及び委託の範囲、又はクラウドソースで運営されているかを含む。
・サポートコンセプト、特に、情報システムのサポートに関与する第三者の氏名、個人情報にアクセスできる程度、及び個人情報にアクセスできる場所のリスト
・ログ記録のコンセプト及びログ記録された情報のそれぞれの保存計画
・バックアップ計画と復旧計画
・メタデータの保護と管理
・データ保持と削除計画及びメディア処分
・廃止措置のコンセプト

5.4 個人情報のフローの特定

5.4.1 対象となる個人情報の取扱いを明確化

個人情報を適切に管理するためには、まず管理すべき対象となる個人情報を明確化するところから始める。そのうえで、査定者は少なくとも 5.3 表５の事項に留意する。なお、5.4.1 のプロセスのアウトプットは、5.3.1 から 5.3.5 までのアウトプットと統合することも可能である。

「情報銀行」サービスの利用環境については、例えば以下を検討する。

・ 本人のハードウェアとソフトウェア（本人のスマートフォン上の「情報銀行」が提供するアプリケーションなど）
・ ハードウェアの種類（コンピュータ、ルータ、電子メディアなど）
・ ソフトウェアの種類（オペレーティングシステム、メッセージングシステム、データベース、ビジネスアプリケーションなど）
・ コンピュータ通信ネットワークの種類（ケーブル、Wi－Fi、光ファイバー など）
・ 個人情報を記録する媒体の種類（印刷物、コピー用紙など）
・ 伝送チャネルの種類（アプリ上への表示、メール、郵送など）

「情報銀行」サービスの利用環境について、一般的に使用されている運用計画と手順をその基本概念と照合するのがよい。例えば以下を検討する。

・ 識別要素とユーザ管理の方法
・ 作業が現場又は外部で行われている場合は、委託先の利用、その場所と個人情報へのアクセスの程度
・ メタデータの使用、ロギング、バックアップ及びリカバリ
・ データの保存、削除、メディアの廃棄
・ システムの停止

5.4.2 業務の棚卸と個人情報取扱い業務の特定

(1) 個人情報を取り扱う業務の洗い出し

① 評価者又は査定者は「情報銀行」の各プロセスを所轄する全ての部門に対し、部門毎に通常業務の基点から終点まで個人情報（個人関連情報を含む）の取扱いの有無のチェックすることを要請する。
② チェック項目は、5.3表５記載事項である。
③ 各部門では通常業務を各部門員一人一人の担当業務での個人情報取扱いプロセスを一覧化する。
④ 各部門では該当業務を一覧化する。
⑤ 査定者は、部門単位の一覧化された調査結果を集約する。

(2) 個人情報を取り扱う業務の絞込み

① 査定者は、集約結果を基に部門長とともに個人情報の利用目的と照合し、不要な個人情報を整理（廃棄、消去）する。
② 不要な個人情報と保護の対象とする個人情報の区分けを行い、「情報銀行」としての個人情報取り扱い業務を絞り込んで一覧化する。

(3) 絞込んだ業務毎の全体像の把握

関係者が把握できるよう本人、提供元、提供先第三者、委託先の役割を洗い出し、

「情報銀行」内の他部門や他組織を含めて業務の内容と責任範囲を明確にする。

(4) 「情報銀行」として取り扱う個人情報取扱い業務の特定

査定者は、評価者に集約結果を報告し、評価者の承認を経て、「情報銀行」として取り扱う個人情報取り扱い業務を特定し、関係部門に結果を周知する。

5.4.3 特定した業務毎の個人情報の主要情報整理と集約

新規サービス構築／追加時、サービスの重要な変更時、個人情報の取扱いの新規／追加／重要な変更が発生したとき等には、以下を行う。

(1) 個人情報特定台帳の作成

査定者は、部門単位の調査結果を「個人情報特定台帳」に従って一覧化し個人情報を集約する。

(2) 個人情報の特定の承認

個人情報の特定漏れを発生させないため、定期的に、5.4.2の各号に従い「個人情報特定台帳」に反映し、評価者の承認を得て、最新性を維持する。

(3) 業務の棚卸の実施

少なくとも年１回以上、適宜に全部門を対象に前１項及び第２項を行う。

棚卸の実施月を定めリスクアセスメント手順書に記載する。

個人情報特定台帳

No.	業務名（個人情報分類）	担当部門	個人情報名	個人情報の項目	件数	利用目的	開示	要配慮	媒体	入手経路・方法	保管場所	保管方法	アクセス権を有する者	利用期限	保管期限	委託/提供/共同利用	返却/廃棄方法

図３．個人情報特定台帳の例

6. データ倫理審査会の準備

6.1. データ倫理審査会のメンバー選定

データ倫理審査会は、本人を含む利害関係者の視点でリスク認識を行い、リスク対策に対して助言を与えることを目的とする。

データ倫理審査会のプロセスを透明化し、プライバシーリスクに対処するためのデータ倫理審査会の目標を達成するために、査定者は、リスクアセスメント・チームとは

別に、外部の専門家等から構成されるデータ倫理審査会を組織する必要がある。なお、リスクアセスメント・チームは、データ倫理審査会に対し必要な説明を行ったり、助言を受けて実務改善を実施したり、データ倫理審査会運営を担う事務局となる。

データ倫理審査会は、複数の様々な立場の利害関係者（本人、マネジメント層、社外の関係者、官公署等）からの信頼・期待に応えていく必要があることから、かかる様々な立場の利害関係者をデータ倫理審査会メンバーとして選定するものとする。「情報銀行」に関心を持っているか、又は「情報銀行」によって影響を受ける可能性のある利害関係者（個人又は団体）を選定する。

表６．データ倫理審査構成メンバー

メンバー（利害関係者）		担うべき役割及び審議の観点
任意	本人	世論調査、ワークショップ、オンライン・アンケート等での意見聴取も考えられる （社外委員）
必須	個人の代表者	本人の視点で、コントローラビリティが確保されているか。提供先第三者の条件が個人の予測できる範囲内で運用されているか等。 （社外委員）
任意	外部のセキュリティの専門家	事業者が見落としているリスクの助言（セキュリティ対策）等。 （社外委員）
任意	法律実務家	事業者が見落としているリスクの助言（コンプライアンス、プライバシー尊重）等。 （社外委員）
必須	データ倫理の専門家（本人視点でのプライバシーリスクに関連する適切な懸念を持っている他の組織の者）	本人の視点で、プライバシーリスク対策が適切か等。 （社外委員）

6.2. データ倫理審査会運営規程の作成

データ倫理審査会の組織及び運営に関する規程を定め、当該規程に基づき、データ倫理審査会のメンバー及び事務局に業務を行わせるものとする。規程では、議事運営に関する諸事項や利害関係を有する者が審議に加わらないこと等を定める。

運営規程、メンバー名簿、データ倫理審査会の開催状況及び審議の概要について、公表する。ただし、審議の概要のうち、公表することにより支障が生じるなど、非公開とすべきとデータ倫理審査会が判断したものについては、公開しない。

6.3. データ倫理審査会の事前協議

この段階では、「情報銀行」のプライバシーリスクアセスメントを進めるに先立ち、以下のビジネススキームの妥当性を協議する。協議は、会議開催の他、必要資料を回付し、審議し助言を受ける方法でも良い。

- 個人と「情報銀行」の間の契約の内容
- ビジネススキームの妥当性（個人情報を委任する個人に不利益が及ばないか）
- 個人へ還元する便益の妥当性（個人の全てが、直接的又は間接的な便益を受け取ることができるか）
- 「情報銀行」に委任した個人情報の利用目的
  - 利用目的の妥当性（わかり易いか、個人が誤解するような説明がなされていないか、個人に便益が提供できない個人情報の取り扱いがなされていないか）
  - 取得する個人情報の項目（利用目的の達成のために必要最小限の項目となっているか）、便益との関連（個人に便益を還元するために必要最小限の項目となっているか）
- 個人による「情報銀行」に委任した個人情報の第三者提供に係る条件の指定及び変更の方法（ＵＩ）
  - 個人の同意を得る様々な場面（個人情報の取得時、サービス利用開始時、サービス利用中等）において、「情報銀行」から個人に提示すべき情報が、個人に分かり易く提示できているか
  - 提供先第三者の選択・同意、提供履歴の閲覧、訂正、利用停止、問合せ対応等、個人のコントローラビリティが確保されているか
- 提供先第三者の選定方法
  - 提供先第三者がプライバシーマーク又はＩＳＭＳを取得していない場合の代替措置の妥当性
  - 提供先第三者の個人情報の利用目的の妥当性（個人にとって不利益となる利用がなされていないか）
  - 安全管理措置のレベルの妥当性（個人情報の取り扱いプロセスにおいて、リスク対策が十分になされているか）
  - 「情報銀行」による提供先第三者の監督方法の妥当性（提供先第三者を監督する方法は十分か、契約のみではなく、実地監査などの手段が講じられているか）、提供先第三者からの再提供の有無、及びその管理方法の妥当性
- 委任を受けた個人情報の提供の判断
  - 提供する個人情報の項目の妥当性（提供先第三者の利用目的を達成するために必要最小限の項目になっているか）
  - 選定された提供先第三者が、提供先第三者としてふさわしいか。提供先第三者選定の判断プロセスの妥当性個人と「情報銀行」の間の契約内容（本人へ還元する便益を含む）の妥当性

7.　プライバシーリスクアセスメント

7.1. リスクの特定（参照：ISO / IEC 29134　6.4.4.1、Annex B）

次に「リスク特定」、すなわち、各局面（プロセス）におけるリスク因子（脅威と弱点）を発見し、認識し、記述する。リスク特定の目的は、本人や「情報銀行」に影響を与えるどのような事態が発生するか又はどのような状況が存在するおそれがあるかを特定することである。

リスクアセスメントでは、本人（本人の権利への対応）の観点と事業（情報資産保護）の観点等からのプライバシーリスクを個別に検討する必要があるが、前者の本人の観点を重視しなければならない。

「リスク」とは、目的（PDCA の Plan に相当する）に対する不確かさの影響であり、具体的には、本人への被害や事業活動の損失、好ましくない結果の可能性をいう。

業務フロー図の各局面（インプット、プロセス、アウプット）について影響を与える要素を書き出す。

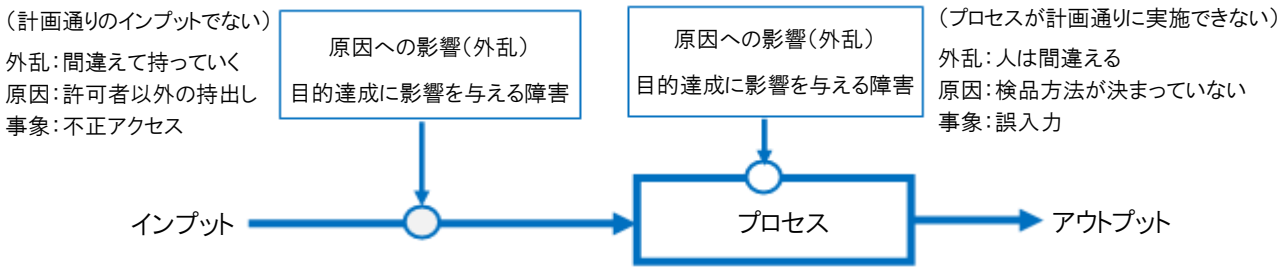


図４．リスク（好ましくない結果の可能性）

(1)　本人（本人の権利への対応）の観点からのリスク認識

本人のプライバシー権を十分保障・尊重することが「情報銀行」事業の根幹であるため、まずは本人にとってのプライバシーリスクを丁寧に検討する。本人の観点からのリスクは、例えば以下が考えられるが、これらに限られるものではなく、サービスの内容・性質等によって異なってくるものである。

・個人情報の利用目的と取扱いが本人の理解と異なる
・本人にとって、自分の個人データがどこに提供されたのかわからない
・個人データの第三者提供に同意した覚えが無い、同意の範囲・条件が曖昧である
・同意した範囲・条件以外に個人情報が取得・利用・提供される
・提供された個人データが何に使われているか十分に理解できない
・提供された個人データがどのように取り扱われるか、保護されるかがわからない
・第三者提供を止める方法がわからない
・収集された情報が他の情報源からの情報と結合されるか、突合されるのかがわからない。利用目的を超えた結合・突合がなされる可能性がある。個人情報の利用・

提供を全体として見たときに、本人が意図しない情報まで把握されたり、プロファイリングされたりしてしまう。

・「情報銀行」や委託先等の内部不正（現従業者のほか、退職者を含む）により個人情報が悪用・提供される
・個人情報が漏えいする
・個人情報が悪用される
・個人情報が適切に安全管理されているかどうかわからない
・保有個人データの開示・訂正・利用停止等が行えない
・個人情報が不必要に長期間保存される

本人が同意した個人情報の内容や利用・提供条件やその状況を十分認識できるように、どのような説明がなされているか、説明がわかりやすいか、画面構成が見やすいか、また、画面表示及び同意の順序が個人情報の取り扱いプロセスと整合しているか等を確認するために、5.3.2 の通り、画面遷移図を作成しなければならない。

(2) 法令・指針・規範違反発生の可能性からのリスク認識

法令・指針等の遵守は当然の要請であり、査定者は、プライバシーリスクを識別するための適切な知識を持つ人を関与させなければならない。

① 現状の確認作業で特定した関係する法令・指針・規範に対し、対応ができているかどうかを洗い出す。不備がないかをチェックする。
② 提供元、提供先第三者が個人情報の取扱いについて守るべきルールがあるか否かを確認し、ある場合は今回の利用がどれに該当するか、また利用する上で他に守らなければならない事項はないかを提供元、提供先第三者に確認する。
③ 過去のプロジェクトから入手可能な関連情報を使用する。
④ 未対応部分が発見され、「情報銀行」としてコントロール可能なものは「即是正」項目、それ以外は出来うる限りの取り組み事項として「要是正」項目として区分する。

(3) 事業（情報資産保護）の観点からのリスク認識

① ライフサイクルの各局面においてのリスク因子（脅威と弱点）を洗い出す。
② 前①で洗い出したリスク因子（脅威と弱点）から引き起こされる個人情報への好ましくない結果をリスクとして捉える。
③ 目的外利用については、特に精査する。

個人情報の誤用や悪用、あるいは技術的・環境的な障害も、潜在的な脅威とみなすべきである。

表７．一般的な脅威の典型的なリスト

	「情報銀行」サービスの利用環境	アクション	個人情報保護リスク	脅威の例
1	ハードウェア	異常使用	個人情報の滅失	個人ファイルの保管：個人利用
2	ハードウェア	異常使用	個人情報への不正アクセス	機微情報を取り扱う用途としては不適切なUSB フラッシュドライブ、またはメモリの使用、個人的な理由で、機微情報を含んだハードウェアの運搬を行う。
3	ハードウェア	ダメージ	個人情報の滅失	データ更新、コンフィギュレーション、保守のエラー マルウェアによる感染、部品の交換等
4	ハードウェア	スパイ活動	個人情報への不正アクセス	相手に気づかれず電車内で行う他人のスクリーン画面の観察。スクリーン等の画面の撮影。ハードウェアの位置情報の収集、電磁信号の遠隔検知 等
5	ハードウェア	滅失	個人情報の滅失	ノート型 PC、　携帯電話の盗難、デバイス、ハードウェアの処分
6	ハードウェア	滅失	個人情報への不正アクセス	ホテルの客室からのノート型 PC の盗難、スリによる携帯電話の紛失、廃棄された保管機器やハードウェアの回収、電子的保管デバイスの紛失
7	ハードウェア	変更	個人情報の滅失	互換性のないハードウェアの追加による故障、システムの適切な稼働に必須の部品の除去等
8	ハードウェア	変更	個人情報への不正アクセス	ハードウェアを基盤としたキーロガーによるトラッキング、ハードウェア部品の除去、デバイスの接続（USB フラッシュドライブ）、OS のインストール、データの回収
9	ハードウェア	変更	個人情報の改ざん	互換性のないハードウェアの追加による故障、アプリソフトの適切な稼働に必須の部品の除去等
10	ハードウェア	オーバーロード	個人情報の滅失	保管ユニットの空き容量なし、停電、処理能力オーバー、オーバーヒート：高温
11	ハードウェア	ハードドライブ破損	個人情報の改ざん	不完全な廃棄、又は保守契約の不備による個人情報への不正アクセス
12	ソフトウェア	異常使用	個人情報の滅失	データ削除、偽造又はコピーされたソフトウェア、オペレーターの人的ミスによるデータ削除
13	ソフトウェア	異常使用	個人情報への不正アクセス	コンテンツのスキャンニング、データの不適切な相互参照。アクセス権限の設定の高度化、利用履歴の削除、電子メールによる大量の迷惑メールの送信、ネットワーク機能の誤用

14	ソフトウェア	異常使用	個人情報の改ざん	データベース上の希望しないデータ変更、ソフトウェアが動作するために必要なファイルの削除、オペレーターの人的ミスによるデータ変更
15	ソフトウェア	ダメージ	個人情報の滅失	稼働している、または実行可能なソースコードの削除、論理爆弾、他
16	ソフトウェア	スパイ活動	個人情報の滅失	ネットワークアドレスとポートのスキャンニング、コンフィギュレーションデータの収集、搾取可能な欠陥の場所を特定するためのソースコードの分析、データベースがどのように、悪意のある質問に対応するかのテストを実施
17	ソフトウェア	スパイ活動	個人情報の改ざん変更	ネットワークアドレスとポートのスキャンニング、音声データにおける攻撃上の脆弱性、分析結果レポート、または業者のポートやサービス
18	ソフトウェア	滅失	個人情報の滅失	データアクセスに使用するソフトウェアライセンスの未更新

(4) 誤操作等の可能性からのリスク認識

誤操作等からのリスクを特定する。例えば以下などが考えられる。

- セキュリティに関する設定を不適切に変更する
- スマートフォン、タブレット端末、IC カード等を紛失する
- 誤操作したり、設定を誤解したりする
- サイバー攻撃（たとえば、マルウェアを埋め込んだ電子メールや、重要な個人情報やセキュリティ情報を引き出すためにWebサイトを偽装するためのトリックリンク、広告に追加された偽の光学コード、本人のスマートフォンの光学式コード認識アプリを偽の Web サイトにルーティングするなど）

7.2. リスク分析（参照：ISO / IEC 29134　6.4.4.2）

リスク分析は、リスクの特質を理解し、リスク基準を決定するプロセスである。7.1 にて洗い出した想定リスクに、①影響度の指標と②発生の可能性の指標を付与する。リスク分析は、状況に応じて、定性的、半定量的もしくは定量的、又はこれらの組み合わせとなりうる。実際には、リスクレベルの一般的な指標を取得し、主要なリスクを明らかにするために、定性分析が最初によく使用される。可能かつ適切な場合、リスクのより具体的かつ定量的な分析も実施することが望ましい。

①影響度は、潜在的な結果とリスク基準で決定された尺度に基づいて推定することが望ましい。5.2.2 を参照のこと。

②発生の可能性については、5.2.3 を参照のこと。5.2.3

プライバシーリスク分析には、プライバリーリスクの原因と根源、そのポジティブな

結果及びネガティブな結果、そしてそのような結果が生じる可能性について考慮する必要がある。査定者は、結果と可能性に影響を及ぼす要素を特定する必要がある。一つのイベントは複数の結果をもたらす可能性があり、複数の目的に影響を与える可能性がある。査定者は、対策とその有効性を考慮する必要がある。

プライバシーリスクとして高い又は非常に高い影響があるか、発生する可能性があるか又は非常に高いと判断された場合、「情報銀行」はそのリスクをその副要素に分解することを検討する必要がある。 この分解により、「情報銀行」はどの副要素が大きな影響又は可能性に寄与しているかを明らかにし、それらを個別に分析することができる。これは、より適切な対策を特定するのに役立つ。

脅威（ISO / IEC 27000：2016、2.83 参照）の可能性を評価するため、「情報銀行」は、リスク源の能力、「情報銀行」サービスの利用環境の脆弱性、リスク対策を考慮することが望ましい。リスクごとに、以下を識別する。

・ 最も可能性が高いリスク源（ISO ガイド 73：2009、3.5.1.2 参照）
・ 最も可能性の高い脅威
・ 本人に対する最も深刻な影響
・ リスク所有者（ISO ガイド 73：2009、3.5.1.5 参照）
・ 既存のリスク対策と、それが対処に役立つリスク

本人に影響がある場合は、「情報銀行」の管理下か否かを問わず、そのリスク源を含める必要がある。「情報銀行」は可能な限り包括的なプライバシーリスクのリストを作成する必要がある。

7.3. リスク評価（参照：ISO / IEC 29134　6.4.4.3、Annex D）

リスク評価は、特定されたプライバシーリスクの優先順位を決定する目的で実施する。リスクは、［影響度］と［発生の可能性］の組み合わせで評価される。このように［影響度］と［発生の可能性］二つを考慮したリスクのランク付けを行い、本人に対するプライバシー影響の重大度を最重視した上で、その他「情報銀行」に対する全体的な影響等も踏まえて、リスクへの対応（必要の有無／優先順位）を決定する。

場合によっては、リスク評価の結果を受けて、さらなる詳細な分析を行うべき場合もある。

発生の可能性と影響度から求めたリスク評価（ランク）についてリスク受容基準を定める。例えば図 5 では、リスク評価値３までとするなどが考えられる。

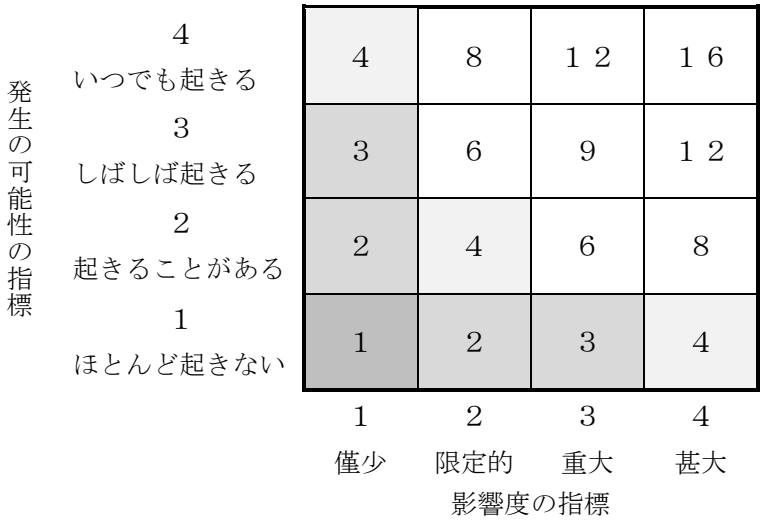


図５．リスクマップの例（太枠内がリスク評価値）

7.4. リスク対策の検討（参照:ISO / IEC 29134　6.4. 5、6.4.3）

上記にて評価されたプライバシーリスクをなくすか、許容可能なレベルまで低減することのできる実効性のある対策について、組織的、人的、物理的、技術的な観点から検討する。

7.4.1 リスク低減･保有･回避･移転

プライバシーリスクの対応措置には、次の 4 つの選択肢がある。

リスク低減、リスク保有、リスク回避及びリスク移転

(1)リスク低減

適切なリスク対策を選択することによって、リスクを低減することができる。リスク対策の選択後に残留リスクが残っている場合、「情報銀行」は残留リスクが許容できないかどうかを判断し、必要に応じ追加のリスク対策によってさらに対処することが求められる。

リスク低減措置を実施することで、利害関係者が得られる利益に影響を及ぼす場合がある。このような状況では、評価者はリスク／ベネフィット分析を実施し、リスクがベネフィットを上回っているかどうか、又はその逆かを判断する。リスクが上回る場合、別のリスク対策を講じなければならない。

リスク低減措置は、例えば以下などが挙げられる。

- 取り扱う個人情報の種類の変更
- 「情報銀行」の構造、方針及び/又は手順の変更
- 個人情報を取り扱う従業者資格の変更（たとえば、許可、研修、認定など）
- 「情報銀行」サービスの利用環境又はアプリケーションの変更（予防措置、検出措置又は是正措置の 3 種類がありうる）

リスク低減のためのアプローチとしては、「影響度」を低減させる、又は「発生の可能性」を低減させることを検討する。

① 「影響度」の低減

影響が発生したとしても、影響が大きくない、アウトプットとして次工程に被害を及ぼさない方法を検討する。例えば、「人は間違える」という可能性を確実に低減することはできない。間違えても被害を及ぼさない対策としては、誤入力が発生しても、二重入力により間違いを発見して次工程に正しいデータを送るようにしたり、紛失が発生しても、データを暗号化したりすることにより拾得者が不正にデータを使えないようにすることなどが考えられる。

被害が発生しても、被害が拡大しない対策を「ダメージ・コントロール」といい、改善活動の一種である。

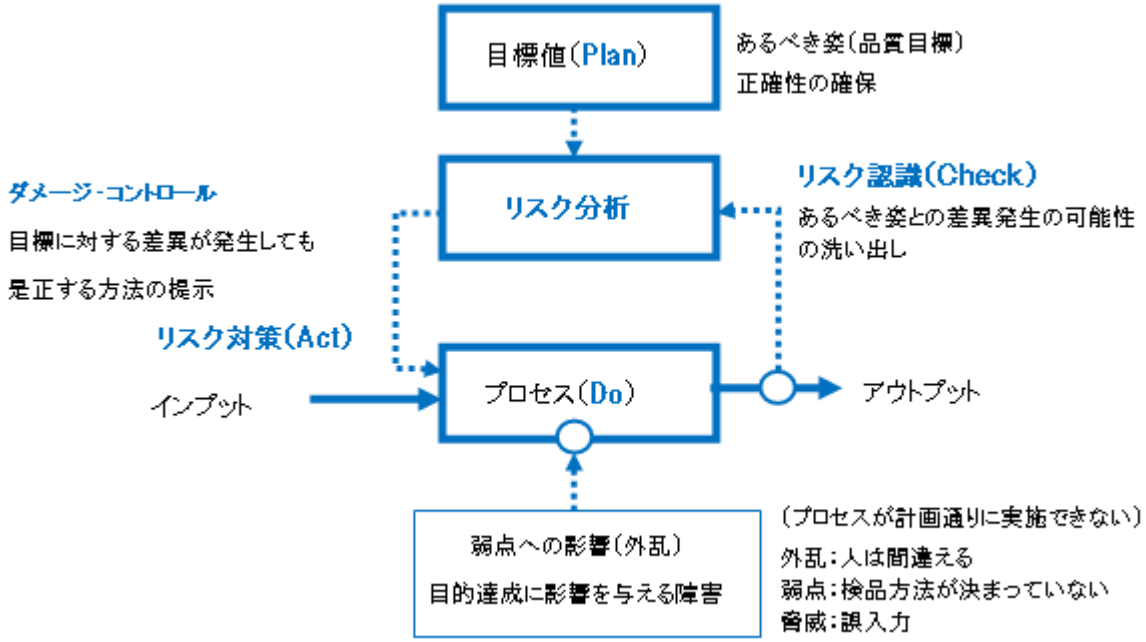


図６．「影響度」の低減

② 「発生の可能性」の低減

リスク発生原因を除去することにより、発生させない（または発生しにくくする）方法を検討する。リスク発生原因を除去する方法としては、例えば、保管キャビネットを常時施錠し、鍵管理することにより不正持ち出しを排除したり、入退出セキュリティ設備を導入し、不正侵入者による盗難を防止したりすることなどが考えられる。

業務フロー図では、「弱点への影響（外乱）」を除去する「フィルター（雑音

除去装置)」を挿入する。

リスク発生原因を除去する対策を「リスク回避」と言い、構造改革の一種である。

対策を講じた後には、フィルターが当初計画していた目標値の機能を果たしているかについて、チェックし、ＰＤＣＡによる改善を続ける。

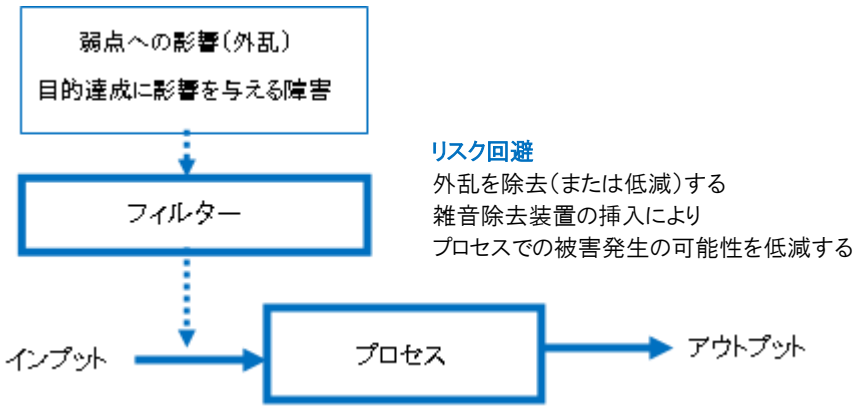


図７．「発生の可能性」の低減

(2) リスクの保有

リスクレベルがリスク基準を満たしている場合は、追加のリスク対策を実施する必要がなく、リスクを保有することができる。

(3) リスク回避

リスクが高すぎるとみなされた場合、「情報銀行」は、撤退するか、又は条件を変更することによって、リスクを完全に回避することを決定する必要がある。

(4) リスク移転

リスク移転には、特定のリスクを外部当事者と共有するという決定を伴う。移転は、結果のサポートをする保険によって、又は情報システムを監視し、定義されたレベルの損害を被る前に攻撃を阻止するために即座の行動を取るパートナーに委託することによって行うことができる。

もっとも、詐欺又は不適切な行動による個人情報の喪失のような重大又は最大のリスクを本人に移転することは適切ではない。リスクの共有は「情報銀行」と他の組織との間で行われるべきであり、重大なリスクは本人に移転するべきではない。

リスク移転は、新しいリスクを生み出すか、既存リスクを変容させる可能性がある。したがって、追加のリスク対策が必要な場合がある。

また、リスク管理の責任を移転しうる場合もありうるが、通常、プライバシーへの悪影響の責任を移転することは不可能である。利害関係者は通常、悪影響が「情報銀行」の過失であるとみなす。

7.4.2 リスク対策の考え方

リスク対応として、アプリケーション又はプロセスの再設計も考えられるが、他の方法で実効性のあるリスク対応が可能であれば、再設計が必須というものではない。

「影響度」は重大・深刻であるが、「発生の可能性」が稀というようなリスクも存在する。経済的観点からこのようなリスクに対応しないという選択をすることは認められない。

「情報銀行」は、リスク対応措置の選択において、データ倫理審査会の意見を聞くことが望ましい。いくつかの対応措置が個々に又は組み合わせて適用され得る。

リスク対応措置自体が、評価、対応、監視、見直しの必要があるプライバシーリスクを導き出す可能性がある。重大なプライバシーリスクは、リスク対策の失敗又は無効であることを示している可能性がある。これらの二次的プライバシーリスクは、新しいプライバシーリスクとして扱われる のではなく、元のプライバシーリスクと同じリスク対応計画に組み込まれ、2 つのプライバシーリスクの関係を特定することが望ましい。

(1) 本人（本人の権利への対応）の観点からのリスク対策

※以下はあくまで例であり、以下の対策を講じてさえいれば良いというものではない。また以下の対策では、7.1 にて特定されたリスク全てに対応できないので、特定の上、評価し、対応要と判断されたリスク全てについて、リスクをなくすか、許容できるレベルまでリスクを低減できるようなリスク対策を講じる必要がある点に十分留意する。

① 個人情報を取得する場合の同意

・本人が個人情報を記入・登録する前に、明示事項を読んで同意する仕組みにする。同意するか判断するに当たり必要な事項や個人情報に関する明示事項（規約がある場合は規約も含む）を、本人にわかりやすく表示する。明示に当たっては⑤⑥⑦を参照する。

・ウェブサイトの場合、本人が「同意する」ボタンを押したあとに個人情報の登録フォームに移るようにする。また、誤って「同意する」ボタンを押してしまうこともありうるので、誤操作を避けるための工夫を施すことが望ましい。

・ウェブサイトの場合、フォームに登録した内容に誤りがないかどうかを確認してから送信するような仕組みにする。

・ウェブサイトの場合、本人がフォームに登録した情報の内容をウェブ画面上で確認・訂正できるようにしておく（トップページからすぐアクセスできるようにする）ことが望ましい。

② スマートフォンなどの小さな画面で個人情報の取扱いについての同意画面を表示する場合

・表示量を押さえる関係上、当該画面には全てを表示することはできないこと

が想定される。その場合には、要約表示をまず行う。

・表示が分かれてしまうと、何に対して同意をしているのかが分からなくなるおそれがある。したがって、同一画面に表示することが望ましい。

③　個人情報取得にあたっての注意事項

・取得する個人情報の項目は適切か。個人情報の利用目的に照らして不要と判断できる個人情報はないか検討する。

・後に、本人から個人情報の開示等の請求等がなされたときに本人確認を行うのに必要な情報を取得する。

・また、必ず記入してもらう項目と、任意で記入する項目を区分する工夫も必要である。

例）　携帯電話への連絡を希望する場合は、携帯電話の番号を記載するなど

個人情報を取得する方法は適切か？偽り等の不正の手段により個人情報を取得してはならない。

個人情報保護委員会「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）」3-2-1

【個人情報取扱事業者が不正の手段により個人情報を取得している事例】

例１）親の同意がなく、十分な判断能力を有していない子どもから、取得状況から考えて関係のない親の収入事情などの家族の個人情報を取得する場合

例２）個人情報保護法第２３条に規定する第三者提供制限違反をするよう強要して個人情報を取得した場合

例３）他の事業者に指示して上記事例１）又は事例２）などの不正の手段で個人情報を取得させ、その事業者から個人情報を取得する場合

例４）本人の同意を得ることなく、かつ、個人情報保護法第２３条の各項各号に定める方法によることなく個人情報が提供されようとしていることを知り、又は容易に知ることができるにもかかわらず、当該個人情報を取得する場合

例５）上記１）又は上記２）などの不正の手段で個人情報が取得されたことを知り、又は容易に知ることができるにもかかわらず、当該個人情報を取得する場合

④　個人情報取得時における安全性は確保されているか

個人情報を取得するまでの過程で個人情報が漏えいする危険がないかどうかリスク分析を行い、必要な対策を講じなければならない。

例えば、はがきや FAX の場合、誤配送や誤送信により他人に見られる危険等が、インターネットの場合はハッキングや電子メールの誤送信などにより個人情報が漏えいする危険等がある。

⑤　表示量に関する注意事項

本人ができるだけ短時間で読むことができる内容を少ない画面数で表示する

ことが望ましい。表示量を押さえる関係上、当該画面には全てを表示できない場合も想定される。その場合は、要約表示をまず行う必要がある。
取得する個人識別可能情報の項目の表示にあたっては、プライバシーへの影響が異なるものについては、本人がその違いを明確に意識できるように、プライバシー影響度グループごとに分けて表示することが望ましい。
当該画面で割愛された情報を含む詳細は、その時点で消費者が希望すれば参照できるようにする必要がある。
例）電子的な通知の場合は、ポップアップ、ドリルダウンするなど 。

⑥ 具体的表示に関する注意事項

本人が、明示事項（利用目的や第三者提供など）があることに気がつかずに個人情報を記入することを避ける。重要な明示事項を目立つように記載する。例えば、以下等が考えられる。

・重要事項については、本人が見落とすことのないよう太字にする、文字を大きくするなど目立たせる工夫をする。
・可能な場合には、取得する個人情報の項目の値を通知時に表示すべきである。取得する個人情報の項目名が表示されても、本人からするとそれが何を意味するか理解できない可能性がある。そのため、具体的な値を表示する。
例えば、「電話番号」と通知するのではなく、「電話番号：03-1234-5678」と通知する。具体的値を表示できない場合には、例示をする必要がある。これらの値の表示は、当該画面からのリンクをたどることによって表示される形にしてもよい。
もっとも、同意前に実際の値を表示することが不可能な場合も考えられる。その場合は例示を行うのが望ましい。例えば、ショッピング時の購買データを提供する場合、本人が会員登録する段階ではショッピングはまだ行っていないので、具体的な購買データは存在しない。そのような場合は、例としての購買データを示し、どのようなデータが提供されるのかに関して、本人が理解できるようにする。

図７の事例に示す方法で必要事項を明示し、本人の同意を得て、個人情報を取得するかについては、トラブル発生のリスク（取得する個人情報の性質・利用目的等により異なる）を勘案して決定する。

図８．具体的に表示する例

出典「オンラインサービスにおける消費者のプライバシーに配慮した情報提供・説明のためのガイドライン」

⑦ 表示形式に関する注意事項

電子的に表示する場合は、本人の好みに最適化して表示をしたり、本人の判断を補佐したりすることができるように、機械可読な形式で提供されることが望ましい。これを本人が理解できる形で表示するにあたっては、画像・アイコン等を使用することもできる。

画像等の解釈は文化的背景によって大きく異なる可能性があることに留意する。混乱を産まないためには、その地域・文化圏における標準を別途定めることが望ましい。このようにすることにより、受け取った機器側で適宜選択して表示することなども可能になる。

⑧ 差分通知の方法

二回目以降の同意取得時には、前回の同意内容に本人がその時点でその画面からアクセスできることを条件として、前回との差分のみを通知することができる。前回と今回で同一の本人に対して差分を通知するために、他人と混同しないよう本人を認証し、これに基づき差分を抽出する必要がある。

⑨ 同意の行為

・同意の取得にあたっては、本人の能動的な行動が必要である。
能動的な行動とは、本人が自らの意志によって起こさなければならない行為を指す。たとえば、チェックボックスをクリックする、ボタンを押す、スライドバーをスライドするなどが考えられる。

・同意を取得する画面は、個人情報の取り扱いに関する事項を明示する画面と同一の画面であるのが望ましい。表示が別れてしまうと、本人は何に対して同意をしているのかが分からなくなるおそれがあるためである。

⑩　同意の独立性

個人情報に関する同意は、他の同意と独立させる。多数の個人情報の取り扱い以外の同意項目の中に、個人情報の取り扱いに関係する同意が混ざっていると、本人にとっては、内容を理解できないまま同意してしまうおそれがある。これを避けるために、個人情報の取り扱い関連の同意は、他の同意とは分けて取得すべきである。

⑪　同意内容の事後的参照

・消費者が同意した内容を希望時に参照できるように、適切な手段で本人に通知する。本人が、事後的に、任意の時に参照できるような手段を使うべきである。

・後から同意が撤回可能な場合は、その手段も合わせて通知すべきである。

⑫　その他

上記に限らず、必要なリスク対策を行う。

(2) 法令・指針・規範違反発生の可能性からのリスク対策

「即是正」項目は、未対応部分を明確にした上で果たすべき義務事項に対し実効性のある具体的施策を検討する。「要是正」については、利害関係者と十分協議を重ね最適な対策の検討を行う。

(3) 事業（情報資産保護）の観点からのリスク対策

リスク分析により“対策を施すべき”とした「弱点」について、組織的、人的、物理的、技術的な観点から実効性のある対策を検討する。実現困難な対策とならないよう、費用、構築の容易さ、運用の容易さ等の観点からも検討する。

すでに計画されている対策又は既存の対策を記述する。

7.5. 残留リスクの認識

対策を施してもなお残るリスクを検討し、把握し、監視し、見直し、残留リスクが顕在化した場合など必要に応じてさらに対応する。監視は、対策が有効であり続けることを内部の利害関係者に保証するために、プライバシーリスク管理計画にとって不可欠である。

7.6. リスク対策の確認

・リスク分析表

リスク分析表を作成する。9.2 を参照のこと。

・リスク対策は、ISO / IEC 29100 原則の要件を満たす必要がある。

ISO / IEC 29100 のプライバシー原則は、同意及び選択（Consent and choice）、目的の正当性及び明確化（Purpose legitimacy and specification）、収集制限（Collection

limitation）、データの最小化（Data minimization）、利用、保持、及び開示の制限（Use、retention and disclosure limitation）、正確性及び品質（Accuracy and quality）、公開性、透明性、及び通知（Openness、transparency and notice）、個人参加及びアクセス（Individual participation and access）、責任（Accountability）、情報セキュリティ（Information security）、プライバシーコンプライアンス（Privacy compliance）。

・リスク対策が、リスクの低減や除去に対応しているかを確認する。
7.1 で特定し、7.3 で評価し、対応要と判断されたリスク全てに対して具体的にどのような対策を取るか検討・確認する。対策によってリスクをなくすことができるか、又はリスクレベルが許容できるとみなされるまで、対策を追加していく。対策は、公認の国際規格で定義されているか、公認の機関によって公表されているものからも選択できるし、これらとは無関係に「情報銀行」によって定義することも可能である。
・「弱点」への影響が発生しても、アウトプットへの「被害」を食い止められるかを確認する。
例えば「人は間違える」と言う弱点に対して「間違えないよう気をつける」と言う対策は、「間違い」（弱点への影響）が発生した場合の「被害」を防止する対策とはならない。
「検査」するという対策について、「間違いがないことを確認する」だけでは不十分である。「確認して間違いを発見した場合は、作業を止めて、前工程に戻す」など具体的手順に落とし込む。
・ルールとして定められている事項についても、リスク対策として報告する。
これによって、どのようなリスクへの対策かが確認できる。ルール通りに実施していないリスクが残れば、実施記録で点検する。
・リスク対策を実施する計画を策定する。
特に、以下の点などについて決定する。
－どのようなリスク対策を行うか。
－そのためにどのようなリソースが必要なのか
－誰が責任者か
－いつまでに行うか
－どのように結果を評価するか
・個人情報リスク
過剰・不正収集、目的外利用、不正利用、不正提供、誤用、漏えい、滅失、毀損、廃棄ミス等のリスクを検出し、防止し、セキュリティを維持する対策は十分か（本人に通知、個人データの最小限の保有、個人データの匿名化など）などを確認する。
・上記が不十分な場合、潜在的な影響を検討する
リスクの発生を防止し、その影響を識別し、制限したり（バックアップ、完全性チェック、プライバシーリスクの管理など）、抑制したりするための対策は十分か。
・上記が不十分な場合、リスク源を検討する

リスク源が行動を起こしたりリスクを現実化したりすることを防ぎ、それらの影響を識別して制限し、又はそれらを無効にするように設計された制御（物理的及び論理的アクセス制御、行動の追跡、第三者の管理、マルウェアに対する保護など)。リスク源の能力が高いほど、強固な管理策が必要になる。

・上記が不十分な場合、「情報銀行」サービスの利用環境を検討する

脆弱性の悪用を防止し、発生する脅威を検出して制限し、通常の動作状態を復元する対策（ソフトウェア、ハードウェア、個人、紙文書などの脆弱性を減らす)。

・説明

評価者は、残留リスクがなぜ受け入れられるのかを説明すべきである。

評価者は、既存の対策及び決定された追加対策を、以下の参照リストと比較し、必要な対策が省略されてないことを確認すべきである。

- ISO / IEC 27001：2013、Annex A の管理策
- ISO / IEC 29151 の管理策
- 国内規格を含む、個人情報保護に関する対策セット
- 外部要因からの対策
- 内部要因からの対策

・再度のリスクアセスメント

許容可能なレベルにリスクを低減するための対策を決定するのに十分な情報が提供されていれば良いが、もし情報が不十分である場合、評価者は、可能な限りリスクアセスメントをもう一度繰り返すべきである。

評価者は、追加対策を考慮に入れることによって、影響のレベル及び残留リスク（すなわち、対策の実施後に残るリスク）の可能性を再推定するべきである。その後、プライバシーリスクマップ上に再配置する。

7.7. PIA 報告書（参照：ISO / IEC 29134　6.5.1、6.5.2）

(1) PIA 報告書の作成

PIA 報告書を作成する。PIA 報告書には、主に、上記 5 及び 7.1 から 7.6 までで検討・決定した内容を記載する。リスクアセスメント・チームその他の「情報銀行」内部の適切な者にレビューを依頼した上で、評価者が PIA 報告書に署名する。

(2) PIA 報告書全文のデータ倫理審査委員会への提出

PIA 報告書は全文をデータ倫理審査会に提示する必要がある。データ倫理審査会の審議後に、データ倫理審査会にとどまらずに一般公表も行う。一般公表に際しては全文又は要約を公表対象とすることができる。要約公表とする場合は、その旨及びその理由をデータ倫理審査会に諮問しなければならない。詳細は 10 を参照のこと。

8. データ倫理審査会の開催

8.1. データ倫理審査会の開催趣旨（参照：ISO / IEC 29134　6.5.4）

プライバシーリスクアセスメント結果について、データ倫理審査会に諮問する。データ倫理審査会は「情報銀行」事業について、その適切性を審議し、必要に応じて助言を行う。

データ倫理審査会からの助言に対して、リスクアセスメントの責任者（評価者）を含むリスクアセスメント・チームで協議し、「情報銀行」としてリスク対策を決定する。データ倫理審査会は、必要があれば「情報銀行」に追加調査・追加報告を求めることができ、「情報銀行」は当該求めに応じて、適切に対応する。

データ倫理審査会の独立した審議は、リスクアセスメントが適切に実施されたこと、推奨事項を実施していない場合はその理由（例えば、残留リスクはメリットよりも小さい等）を説明する手段となりうる。データ倫理審査会という、「情報銀行」以外の第三者によるレビュー又は監査は、リスクアセスメントに信頼性を与え、透明性を向上させ、経験から学び、リスクアセスメントの質を高める方法になる。なお、リスクアセスメント自体が「情報銀行」ではなく第三者によって実施される場合、データ倫理審査会及び監査は、リスクアセスメントを実施した当該第三者によって行われるべきではない。

8.2. データ倫理審査会の審査基準

データ倫理審査会の審議は、主に以下の観点から行うものとするが、これら以外の観点からの審議を妨げるものではない。なお、以下に記載する観点は、6.3 とも重複する点がある。

8.2.1.　個人と「情報銀行」間の利益相反等（善行原則　beneficence）

本人と「情報銀行」間に利益相反がなく、本人にとってリスクよりも便益の方が大きいか等を確認する。なお、データ倫理とは異なるが、「倫理」という意味で共通する部分があるので、医療倫理原則についてもここで触れる。医療倫理 4 原則の１つに「善行原則」があり、患者のために最善を尽くすことをいう。本審議基準は、善行原則に類似するものであるとも考えられる。

- 利用目的と取り扱う個人情報の関係に矛盾がないか。利用目的を想定できない個人情報を取得していないか。個人情報の過剰取得がないか。
- 業務フロー図で定義した個人情報の取扱いについて、その必要性が説明できるか。一般人の視点に立って納得できる程度に合理的か。
  例えば、その範囲の個人情報を取り扱う必要があるか、その個人情報の項目を取り扱う必要があるか、その処理を行う必要があるか等。
- 要配慮個人情報に該当しないが、不当な差別や偏見その他の不利益が生じる可能性がないか。
- 利用目的の達成に不必要・不相当な個人情報を入手しないよう、どのような対策を

講じるか。網羅的・探索的に個人情報を入手する場合や、利用目的や入手経路、対象者の範囲が十分に特定されていない場合に特に問題になるので注意を要する。

- 個人情報の取扱いがプライバシー等へ与える影響度合いはどの程度か。どのようなリスクが考えられるのか。リスク対策は十分か。残留リスクは許容できるレベルか。
- 個人情報の取扱いによって、本人が得られるメリットは何か。どの程度のメリットか。リスクとメリットのバランスとして、メリットが必ず上回っているといえるか。
- 必要性が低かったり影響が大きかったりする場合は、代替策があれば代替策を立て、代替策がない場合は取扱いをやめるか、リスク対策を厚く講じるべき。但し、プライバシーへの影響が大きい場合でも、取扱いをやめたり、代替策を立てたりすることが困難なときもあり、取扱い中止・変更が必須とされるわけではない。そのような場合は、リスク対策を厚く講じる等、個人情報を取り扱う必要性とプライバシーに与える影響とを比較考量し、適切な取扱いを図っていく。

8.2.2. 本人のメリット等（正義原則 justice/equality）

「情報銀行」と契約した個人全てが直接的又は間接的にメリットを享受できること、個人情報の提供の提案を受けない者が発生しないなど、提供した結果などを確認する。医療倫理 4 原則の 1 つに「正義原則」（公平原則ともいう）があり、患者を平等かつ公平に扱うこと、根拠のない差別をなくすことをいう（競合する要求の間に適正なバランスを確立することを含む）。本審議基準は、正義原則に類似するものであるとも考えられる。

- 「情報銀行」と契約した全ての個人は、個人データの提供により直接的又は間接的な便益を受け取ることができるか。
- 個人情報の提供の提案を受けない個人が発生しないか。

※個人データ管理のみを行い、個人データを第三者に提供しないか提供の提案を行わない状態は、当該本人に対し「情報銀行」の機能を履行した（契約を履行した）状態とは言い難く、このような状態が長く続かないよう改善する。

※本人が、サービス紹介を受けた提供先第三者への個人データの提供に同意せず、個人データの第三者提供がなされなかった場合であっても、提供先第三者のサービス紹介によって便益を受けたことになり、「情報銀行」の機能は履行されているといえる。

- 本人が得られるメリットはどのようなものか。

8.2.3. 想定リスクの妥当性・リスク対策の適切性（無危害原則 non-maleficence）

想定リスクの妥当性とリスク対策の適切性を確認する。すなわち、リスクを十分に事前に想定した上で、リスクをなくすか、又は許容できるレベルまで軽減する十分な対策を講じているかを確認する。医療倫理 4 原則の 1 つに「無危害原則」があり、「危害を引き起こすのを避けるという規範」あるいは、「害悪や危害を及ぼす

べきではない」ことであると定義される。本審議基準は、無危害原則に類似するものであるとも考えられる。

・ 起こりうるリスクが、十分想定されているか。他には想定されないか。
「情報銀行」にとっては、日々計画・遂行する業務のことなので、プライバシーリスクを見落とすこともある点に留意する。
専門家でない一般人の視点で見たときに、自分の個人情報が取り扱われることで何が不安なのか、脅威なのかといった観点が十分検討されているか。加えて、専門家の視点から、想定されるリスクが他にないか。
・ 「情報銀行」が評価した、リスクの影響度と発生の可能性は妥当か。
・ プライバシーへの影響・リスクが大きいものは、リスク対策の適切性の観点から十分なチェックを行う。
・ リスクとリスク対策がかみ合っているか。その対策によってリスクを防止・軽減できることを、一般人の視点で見て納得できるか。
・ リスクレベルに応じた対策か。特に、プライバシーへの影響・リスクが大きいものについては、十分な対策がとられているか。
・ リスク対策が現在同種の事業に求められる水準と合致しているか。
・ リスク対策として良い点があれば、その旨を意見するのもよい。

8.2.4. 個人情報の第三者提供条件の指定･変更方法(UI)（自律尊重原則 autonomy）

本人の個人情報の取扱いについて、本人が十分な説明を受けて理解した上で自ら選択できるようになっているかを確認する。利用目的その他に関する十分な説明と、個人情報の第三者提供条件の指定・変更方法（ＵＩ）のわかりやすさが重要となる。医療倫理 4 原則の 1 つに「自律尊重原則」があり、患者が情報を開示され内容を理解した上で、自身の意思に基づき決定することを尊重することをいう。

GDPR でも、「管理者は、データ主体に対し、簡潔で、透明性があり、理解しやすく、容易にアクセスできる方式により、明確かつ平易な文言を用いて」情報提供する義務が課せられており（第 12 条第 1 項）、また第 4 条（11）では「自由に与えられ、特定され、説明を受けた上での、不明瞭ではない、本人の意思の表示」との規定が設けられており、日本だけではなく欧州においても、情報を開示され内容を理解した上で、自身の意思に基づき決定することが尊重されていると考えられる。

・ 一般人の視点で、「提供先第三者が誰か」、「提供先第三者における個人情報の利用目的」、「提供する個人情報の項目」、「提供先第三者から自分に対して連絡または接触があるのか」がわかりやすく、誤解を与えない説明で示されているか
・ 「情報銀行」及び提供先第三者に提供した個人情報に関する変更（追加、訂正、削除、利用停止、提供の停止）の方法がわかりやすく、使い易く示されているか

・ 表７.本人の権利への対応として適切なユーザインターフェイスが確保されているか。なお、適切なユーザインターフェイスとは、7.4.2（1）本人（本人への権利への対応）の観点からのリスク対策を備えていることをいう。

8.2.5. 提供先第三者の選定方法

当該提供先第三者の個人情報の取扱いについて「情報銀行」側の適切な監督が可能であるか確認する。

・ 提供先第三者における個人情報の利用目的は適切か
・ 本人が直接的又は間接的に便益を享受できる提供先第三者であるか
・ 不当な差別や偏見その他の不利益が生じる可能性がないか
・ 社会的信頼性を有する事業者か。深刻な苦情を受けているか、深刻でなくとも苦情が多い事業者ではないか

8.2.6. 委任を受けた個人情報の提供の判断

提供先第三者における個人情報の利用目的に鑑みて、利用目的達成のための必要最小限の項目となっているか確認する。

・ 個人の同意している提供先第三者の条件について、個人の予測できる範囲内で解釈されて運用されているか
・ 個人にとって不利益となる利用がされていないか／個人に対し個人情報の利用によるリスクが伝えられているか

9. リスク対策の実施

9.1. リスク対応等の決定

データ倫理審査会からの助言について、リスクアセスメントの責任者（評価者）及び個人情報保護管理者を含むリスクアセスメント・チームで協議し、データ倫理審査会の助言をどう反映していくか検討する。そのうえで、「情報銀行」として 7.6 で検討したリスク対策を改訂等するなどして、リスク対策を最終決定する。決定したリスク対策は安全対策手順書または業務手順を定めた内部ルールとして別途まとめる。なお、決定したリスク対策は ISO / IEC 29100 原則の要件を満たしている必要がある。

データ倫理審査会の助言のすべてを必ず受け入れなければならないものではないが、「情報銀行」は対応を行った助言、対応を行わなかった助言を分け、対応を行わなかった助言についてはその理由、そして今後の対応計画をデータ倫理審査会に説明、報告する必要がある。

9.2. リスク分析表

リスク対策が決定したら、決定されたルールに従って運用を行っていかなければな

らない。そしてルールに従った運用であることを確認できるようにしておく必要がある。そこで、そのような確認を行うための方法を決定し、リスク分析表の「運用結果の記録」欄に記入する。すなわち、「運用結果の記録」欄に記入してある項目を点検すると、運用がルール通りに実施されていることが確認できるようにする。

例えば「取得」プロセスのリスク対策で、「授受記録を取る」ことを決定し、「個人情報の授受に関する手順」としてルール化した場合には、「運用結果の記録」欄に「授受記録」と記入し、また「関連規程」欄にこのルール名を記入する。定期的な点検では、「授受記録」を確認する。

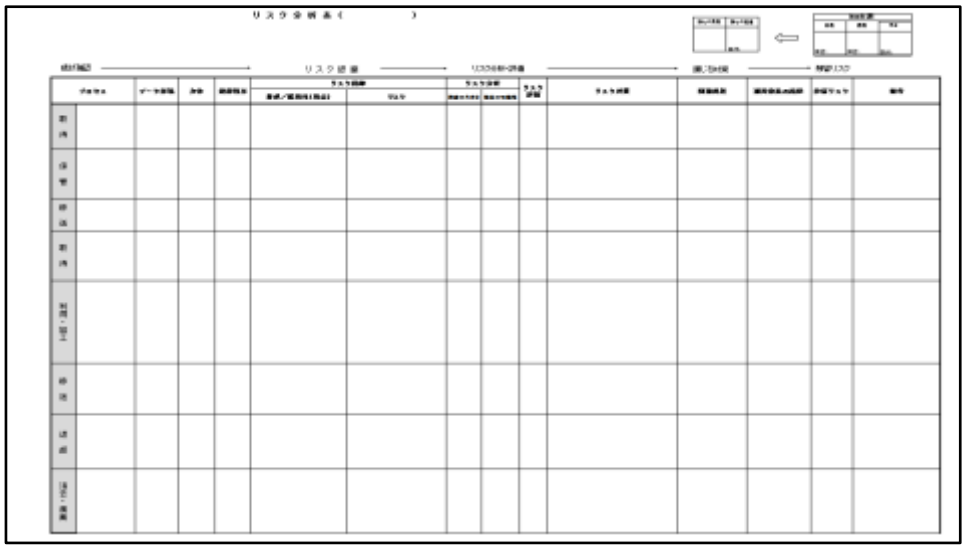


図９．リスク分析表の例

9.3. リスクの見直し

・定期的な見直し

リスクは環境の変化（取扱量の拡大等も含む）や技術の進展等により常に変動する。したがって定期的な見直しは必須であり、また必要に応じて随時見直しを行うこともルール化する。リスクは常に変化することを認識し、少なくとも年１回の見直しを行う。見直しの実施月を定め、文書化する。

・他部門との情報共有

ある部門で顕在化したリスクやヒヤリ・ハットは、他の部門でもあてはまる場合がある。そのような時は、顕在化した部門内での見直しに止まるのではなく、情報を共有化する。

・実施に先立つ計画・ルール化

とりあえず実施（Do）して、点検（Check）の結果、目標との間に差異があったら見直し（Act）するという後追いの活動では、インシデントが多発し、検品・修正に終始することになってしまう。実施に先立ち、十分な計画を検討しルール化しておくことが必須となる。

・リスク対策の再決定

新規の個人情報取扱業務が発生した場合や、既存業務で個人情報の主要情報を変更した場合、又は新たな弱点を発見した場合は、7 に従いリスク対策の検討を行い、8 に従いデータ倫理審査会にて審議を受け、リスク対策の見直しを決定する。 見直したリスク対策は安全対策手順または業務手順を定めた内部ルールに反映する。

・訓練

個人情報の取り扱いを開始する前に、プロジェクトに関わる従業者等に対して適切な訓練を提供しなければならない。個人情報の取扱いに関する従業者との取り決め（就業規則・契約・誓約書等）を保存し、必要に応じて訓練を記録する。

10. PIA 報告書の公表

10.1. PIA 報告書最終版の作成

「情報銀行」は、PIA 報告書の最終版を作成する。7.7 で作成した PIA 報告書を見直し、データ倫理審査会の審議を経て変更した点を PIA 報告書にも反映する。PIA 報告書は全文をデータ倫理審査会に提示する必要があるが、一般公表に際しては全文又は要約を公表対象とすることができる。要約公表とする場合は、その旨及びその理由をデータ倫理審査会に諮問しなければならない。なお、PIA 報告書には「情報銀行」のセキュリティリスクにかかわる特定情報や事業上の秘密情報が記載されている可能性もあり、全文公表することで、かえって残留リスクの暴露に相当することもありうる点にも留意するものとする。

一般公表する PIA 報告書は、要約であっても全文であっても、以下の内容を含むものとする。合わせて、「情報銀行」のプライバシーポリシーや行動規範、利害関係者に対する義務ならびに関連する法令の遵守も参照できるようにすることが望ましい。

・サービス全体像
・個人情報のフロー（特に、収集・提供される個人情報の種類等）
・個人情報の取り扱いが行われる法域
・リスクアセスメントの適用範囲
・リスクアセスメントの概要（特に、「情報銀行」によるリスク対策の概要）
・リスク対応計画
・本人がとるべきであるあらゆる対策
・データ倫理審査会の審査・助言
・利害関係者との協議状況
・問合せ先
・公表日

10.2 PIA 報告書最終版の公表

PIA 報告書最終版を公表する。一般の者、特に本人がウェブサイトに見つけやすいようにして、公開された PIA 報告書最終版をダウンロードできるようにする。

附属書A　リスクアセスメント・チームの作業手順

表 A.1 に規定したリスクアセスメント・チームの作業手順は，理解を助けることを目的として、本ガイドラインの各項の概要を整理したものである。

詳細手順は、該当する各項を参照されたい。

表 A.1　リスクアセスメント・チームの作業手順

5.2	リスク基準	リスク基準は、リスクの重大性を評価するための目安となる条件であり、影響度と発生の可能性に関する評価基準として定める。
5.3	サービス全体像の把握（業務フロー図の作成）	どのような手段で業務を実施しているかプロセスを明らかにする。
5.4	個人情報のフローの特定	管理すべき対象となる個人情報を明確にする。
7.1	リスクの特定	各局面（プロセス）においてのリスク因子（脅威と弱点）を発見し、認識し記述する。
7.2	リスク分析	リスクの特質を理解し、リスク基準を決定する。洗い出したリスクに、影響度の指標と発生の可能性の指標を付与する。
7.3	リスク評価	リスク及び／又はその大きさが、受容可能か又は許容可能かを決定するために、リスク分析の結果をリスク基準と比較する。
7.4	リスク対策の検討	リスク分析により“対策を施すべき”とした「弱点」について、組織的、人的、物理的、技術的な観点から費用、構築の容易さ、運用の容易さ、効果等の観点から実効性のある対策を検討する。
7.5	残留リスクの認識	対策を施しても尚残るリスクを検討し、把握し、監視し、見直し、残留リスクが顕在化した場合など必要に応じてさらに対応する。
7.6	リスク対策の確認	対策を施しても尚残るリスクを検討し、把握し、監視し、見直し、残留リスクが顕在化した場合など必要に応じてさらに対応する。

附属書B **データ倫理審査会の審査基準**

表 B.1 に規定したデータ倫理審査会の審査基準は，理解を助けることを目的として、本ガイドラインの各項の概要を整理したものである。

詳細手順は、該当する各項を参照されたい。

表 B.1　データ倫理審査会の審議基準

8.2.1	個人と「情報銀行」間の利益相反等（善行原則　beneficence）	本人と「情報銀行」間に利益相反がなく、本人にとってリスクよりも便益の方が大きいか等を確認する。
8.2.2	本人のメリット等 （正義原則 justice/equality）	「情報銀行」と契約した個人全てが直接的又は間接的にメリットを享受できること、提供の個人情報の提供の提案を受けない者が発生しないことなどを確認する。
8.2.3	想定リスクの妥当性・リスク対策の妥当性 （無危害原則 non-maleficence）	想定リスクの妥当性とリスク対策の適切性を確認する。すなわち、リスクを十分に事前に想定した上で、リスクをなくすか、又は許容できるレベルまで軽減する十分な対策を講じているかを確認する。
8.2.4	個人情報の第三者提供条件の指定・変更方法（ＵＩ） （自律尊重原則 autonomy）	本人の個人情報の取扱いについて、本人が十分な説明を受けて理解した上で自ら選択できるようになっているかを確認する。
8.2.5	提供先第三者の選定方法	当該提供先第三者は個人情報の取り扱うについて適切な監督が可能であるか確認する。
8.2.6	委任を受けた個人情報の提供の判断	提供先第三者の個人情報の利用目的に対して必要最小限の項目となっているか確認する。

監修　日本 IT 団体連盟　情報銀行推進委員会 認定委員会　委員長
英知法律事務所　弁護士　森 亮二

日本 IT 団体連盟　情報銀行推進委員会 認定委員会　委員
宮内・水町 IT 法律事務所　弁護士　水町 雅子

日本 IT 団体連盟　情報銀行推進委員会 認定分科会　分科会長
NAT コンサルティング合同会社　代表社員　崎村 夏彦

編集　日本 IT 団体連盟　情報銀行推進委員会 認定委員会

日本 IT 団体連盟　情報銀行推進委員会 認定分科会 認定事務局

日本 IT 団体連盟　情報銀行推進委員会 認定分科会 認定事務局
主任審査員　野津 秀穂