

データ倫理審査会 審査員のための教本

2021年7月1日
情報銀行推進委員会
認定分科会 認定事務局

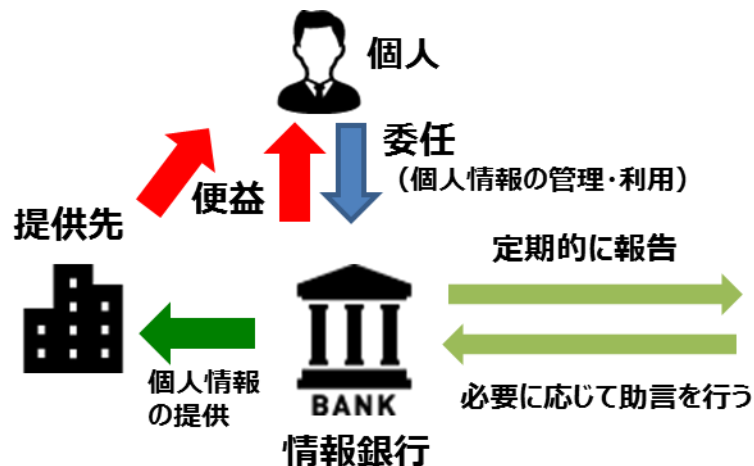


1 データ倫理審査会の役割

- 情報銀行は、個人情報に対する個人によるコントロール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、それぞれが適切に機能するには、データ倫理審査会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い。データ倫理審査会において審議す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。このため、利用者たる個人の視点に立ち、適切な運営が確保される必要がある。
- ・ 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ルビリティを確保するための機能が誤解のないU Iで提供されているか
・個人の同意している提供先の条件について、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



データ倫理審査会



- ・構成員の例：エンジニア、セキュリティ専門家、法律実務家、データ倫理専門家、消費者等
- ・構成員には社外委員を含む

- 情報銀行事業について、以下の事項についてその適切性を審議し、必要に応じて助言を行う
 - ・個人と情報銀行の間の契約の内容
 - ・情報銀行の委任した個人情報の利用目的
 - ・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（U I）
 - ・提供先第三者の選定方法
 - ・委任を受けた個人情報の提供の判断
- 運営方法
 - ・構成員及び（必要な範囲の）議事録は公開する
 - ・必要に応じ情報銀行に調査・報告を求めることができる

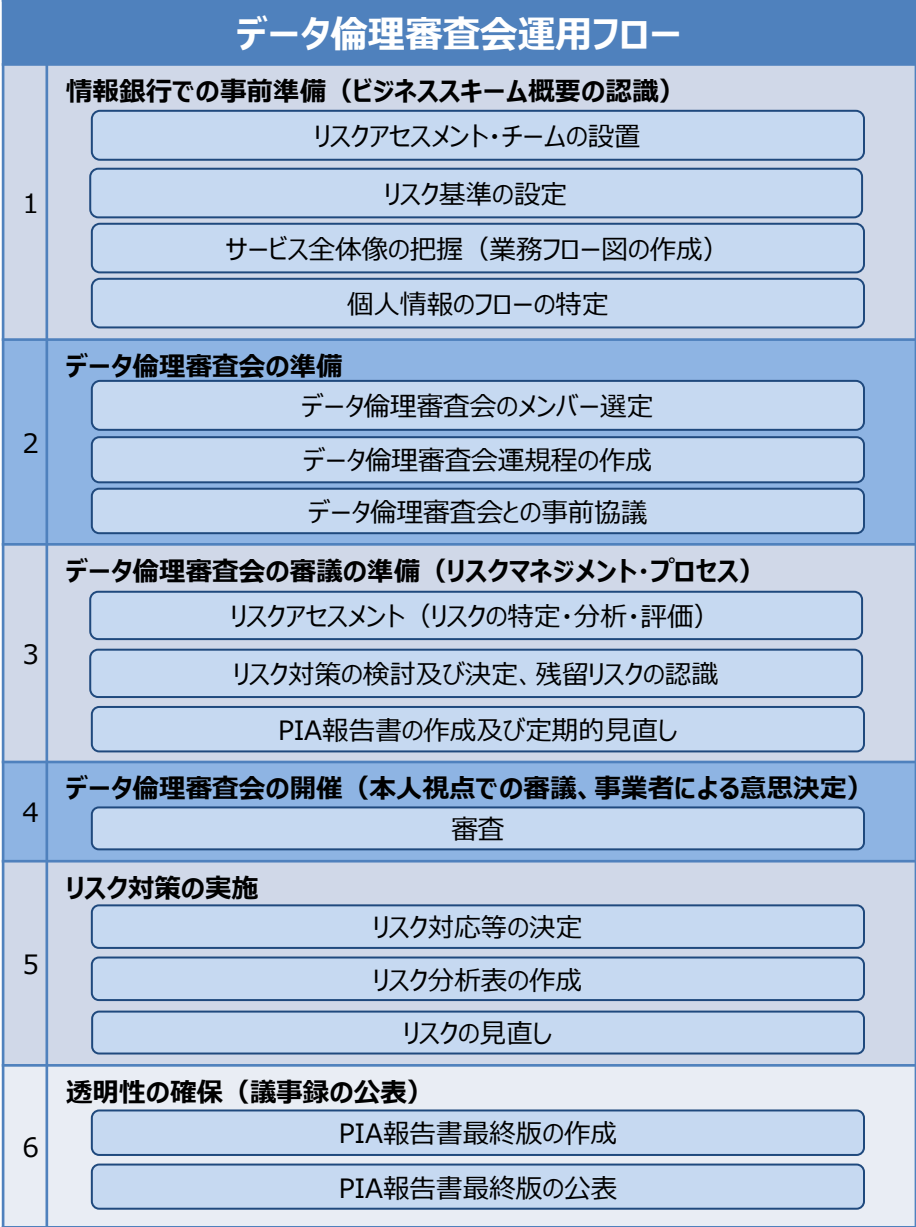
1.1 データ倫理審査会の審査基準

データ倫理審査会の事前協議（ビジネススキームの妥当性協議）		
2.2	ビジネススキームの妥当性	ビジネス詳細設計を進めるにあたっての留意点を助言する
2.3	個人と情報銀行の間の契約内容の妥当性	モデル約款の記載事項を満たしたビジネススキームとなっているか確認する
2.4	情報銀行に委任した個人情報の利用目的の妥当性	利用目的は、できる限り特定されているか確認する 全ての委任者が直接的又は間接的に便益を受け取ることができるか確認する
2.5	情報銀行に委任した個人情報の項目の妥当性	利用目的と取得する個人情報の項目の関係について確認する 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を確認する
2.6	提供先第三者の選定方法の妥当性	当該提供先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
2.7	委任を受けた個人情報の提供の判断	提供先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
データ倫理審査会の開催（委任者視点での協議）		
3.2	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などを確認する。
3.3	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。
3.4	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。
3.5	個人情報の第三者提供条件の指定・変更方法（U I） （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しているかを確認する。
3.6	リスク対策の適切性	想定リスクへの対策として合理的説明ができていないか確認する

医療倫理4原則「善行原則」「正義原則」「無危害原則」「自律尊重原則」
Beauchamp TL, et al: Principles of Biomedical Ethics. 5th ed. Oxford University Press, 2001(生命医学倫理. 第5版. 立木教夫, 他, 監訳. 麗澤大学出版会, 2009

1.2 データ倫理審査会の役割

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



- ビジネススキームの妥当性協議
- ・個人と情報銀行の間の契約内容の妥当性
 - ・個人情報の利用目的及び個人情報の項目の妥当性
 - ・提供先第三者の選定方法の妥当性
 - ・提供データの妥当性
 - ・提供先第三者の個人情報の利用目的の妥当性

- 委任者視点での協議
- ・ユーザビリティの確認（わかり易い・使い易い）
 - ・コントローラビリティの確認（本人による追跡や関与が可能）

議事録を作成し、公開する

1.3 リスクアセスメント・チームの設置

データ倫理審査会へのインプット情報としてリスク分析情報を提供する

データ倫理審査会運用フロー

情報銀行での事前準備（ビジネススキーム概要の認識）

リスクアセスメント・チームの設置

1

リスク基準の設定

サービス全体像の把握（業務フロー図の作成）

個人情報のフローの特定

データ倫理審査会の準備

2

データ倫理審査会のメンバー選定

データ倫理審査会運規程の作成

データ倫理審査会との事前協議

データ倫理審査会の審議の準備（リスクマネジメント・プロセス）

3

リスクアセスメント（リスクの特定・分析・評価）

リスク対策の検討及び決定、残留リスクの認識

PIA報告書の作成及び定期的見直し

データ倫理審査会の開催（本人視点での審議、事業者による意思決定）

4

審査

リスク対策の実施

5

リスク対応等の決定

リスク分析表の作成

リスクの見直し

透明性の確保（議事録の公表）

6

PIA報告書最終版の作成

PIA報告書最終版の公表

ビジネススキーム概要をまとめる
ビジネススキーム詳細設計に先立ち
ビジネススキームの妥当性を協議するための資料を作る

リスクマネジメント・プロセス
委任者の観点と事業継続の観点からリスクを個別に検討
リスク対策案を検討する

リスク分析表の作成
データ倫理審査会の審議を受けてリスク対策を決定する

議事録を作成し、公開する

1.3.1 リスクアセスメント・チームの設置

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。

2. データ倫理審査会 事前協議（提供先の妥当性、ビジネススキームにおけるリスク）

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

データ倫理審査会運用フロー

情報銀行での事前準備（ビジネススキーム概要の認識）

1

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（業務フロー図の作成）

個人情報のフローの特定

データ倫理審査会の準備

2

データ倫理審査会のメンバー選定

データ倫理審査会運規程の作成

データ倫理審査会との事前協議

ビジネススキームの妥当性協議

- ・個人と情報銀行の間の契約内容の妥当性
- ・個人情報の利用目的及び個人情報の項目の妥当性
- ・提供先第三者の選定方法の妥当性
- ・提供データの妥当性
- ・提供先第三者の個人情報の利用目的の妥当性

データ倫理審査会の審議の準備（リスクマネジメント・プロセス）

3

リスクアセスメント（リスクの特定・分析・評価）

リスク対策の検討及び決定、残留リスクの認識

PIA報告書の作成及び定期的見直し

データ倫理審査会の開催（本人視点での審議、事業者による意思決定）

4

審査

リスク対策の実施

5

リスク対応等の決定

リスク分析表の作成

リスクの見直し

透明性の確保（議事録の公表）

6

PIA報告書最終版の作成

PIA報告書最終版の公表

委任者視点での協議

- ・ユーザビリティの確認（わかり易い・使い易い）
- ・コントローラビリティの確認（本人による追跡や関与が可能）

議事録を作成し、公開する

2.1 データ倫理審査会構成メンバー

データ倫理審査会は、委任者を含む利害関係者の視点でのリスク認識を行い、リスク対策に対して助言を与えることを目的とする ISO/IEC 29134:2017 6.3.4.1 Identify stakeholders

メンバー（利害関係者）		担うべき役割及び審査の観点
任意	本人	世論調査、ワークショップ、フォーカスグループ、公聴会、オンライン・アンケート等での意見聴取も有効
必須	個人の代表者	委任者本人の視点で、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。（必須社外委員）
任意	外部のセキュリティの専門家、法律実務家	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、法令遵守）
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（委任者視点での個人情報保護リスクに関連する適切な懸念を持っている他の組織の人々）	委任者本人の視点で、個人情報保護のリスク対策が適切か等。（必須社外委員）

2.2 データ倫理審査会 事前協議（提供先の妥当性、ビジネススキームにおけるリスク）

事前協議はビジネス詳細設計の前における確認である
ビジネス詳細設計を進めるにあたっての留意点を助言する

ビジネススキームの妥当性を事前協議

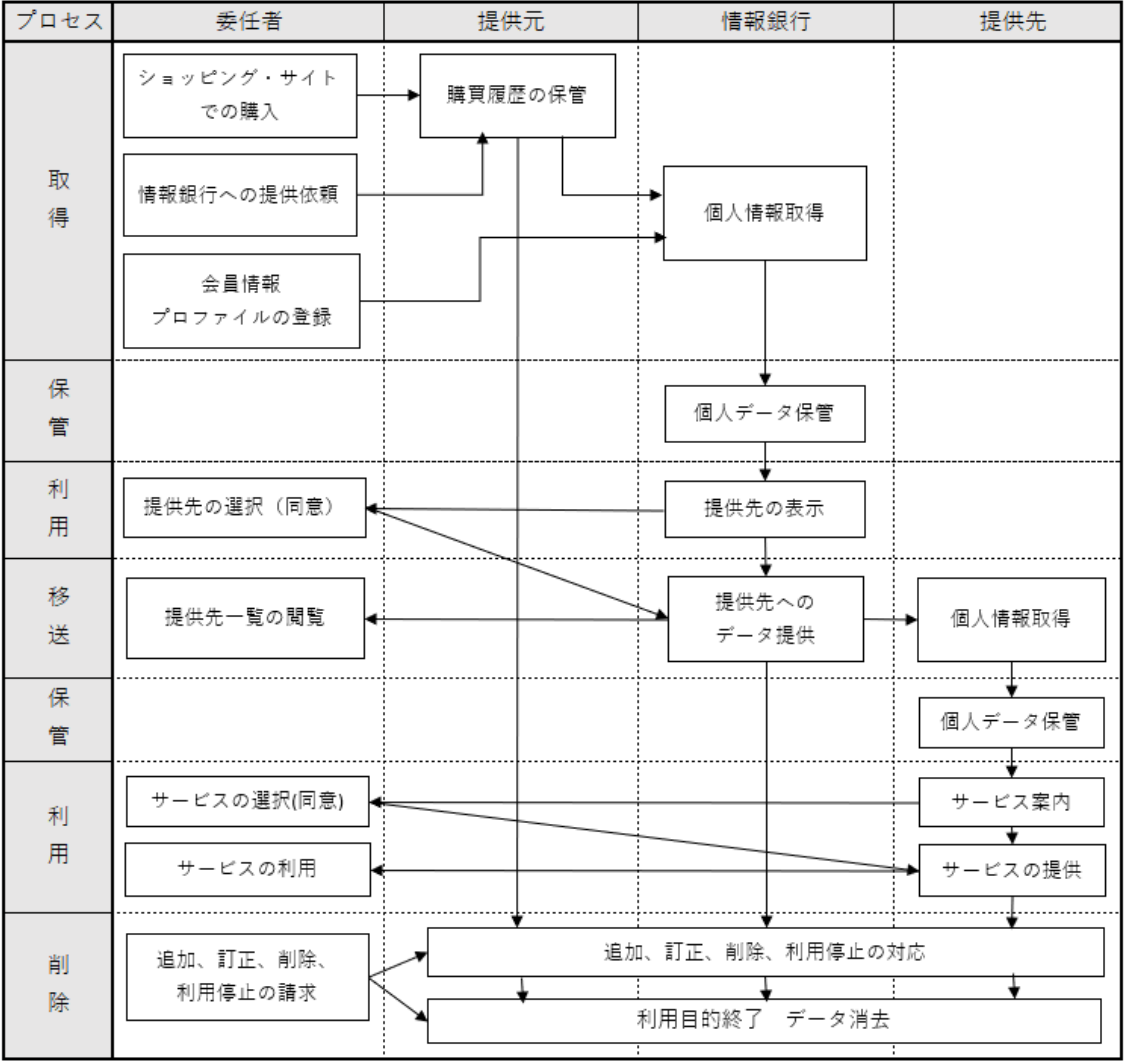
事前協議は、会議開催の他、必要資料を回付し、審議し助言を受ける方法でも良い

①	個人と情報銀行の間の契約内容の妥当性
②	情報銀行に委任した個人情報の利用目的及び個人情報の項目の妥当性
③	提供先第三者の選定方法の妥当性
④	委任を受けた個人情報の提供の判断（提供データの妥当性）
⑤	提供先第三者の個人情報の利用目的（個人にとって不利益となる利用がなされていないか）の妥当性

2.3 ビジネススキーム概要の確認

(1) 個人情報を取り扱う業務の洗い出し	
①	評価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が識別できる情報の取扱いの有無のチェックすることを要請する。 チェック項目は、個人情報の項目、利用目的、保管場所、保管方法、アクセス権を有する者、利用期限、保管期限などである。
②	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。
③	各部門では該当業務を一覧化する。
④	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委任者、提供元、提供先、委託先の役割を洗い出し、組織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特定し、関係部門に結果を周知する。	

2.3.1 業務フロー図の確認



この作業により、委任者、提供元と情報銀行の各部門、提供先、委託先の間で、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、委託先とのやりとりや支店間の輸送において外部に依頼する場合もある

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）のか、後工程が受信（取りに行く）のかなど責任の所在を確認する必要がある

2.3.2 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

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を明らかにする

委任者がアクセスする画面遷移図を作成する。画面には、以下の要件が含まれる

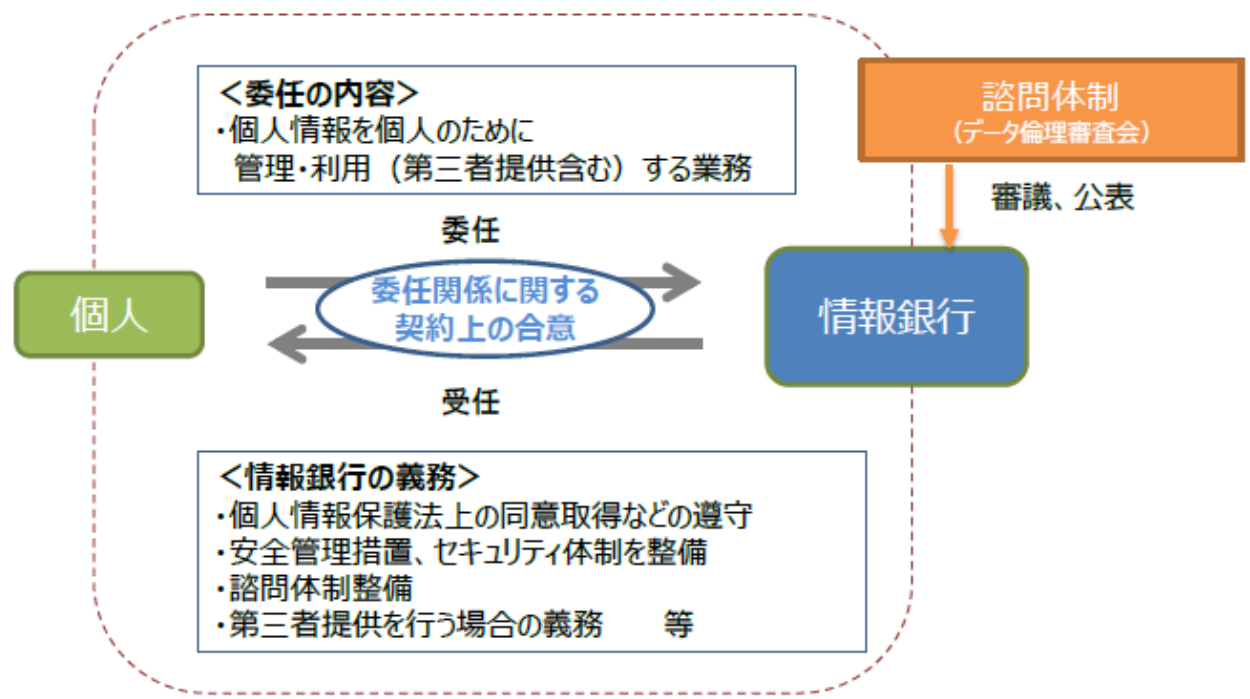
1	個人と情報銀行間の契約の内容、情報銀行サービス利用規約などの説明
2	個人情報の取扱いに関する明示事項
3	会員登録の手続き
4	個人情報の取得画面及び取得した個人情報の閲覧
5	提供先の説明及び個人情報を提供した提供先の一覧
6	第三者提供に係る条件の指定及び同意の取得
7	個人情報の取扱いに関する変更手続き（追加、訂正、削除、利用停止、提供の停止）
8	苦情および相談への対応

画面遷移図は、委任者（本人の権利への対応）の観点から個人情報保護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

2.3.3 個人と情報銀行の間の契約内容の妥当性

モデル約款の記載事項を満たしたビジネススキームとなっているか確認する

〔個人情報の提供に関する契約上の合意の整理〕



※個人情報保護法上の第三者提供・利用目的の変更の同意を満たすことが必要

【参考：未成年等の制限行為能力者が情報銀行を利用する場合】
情報銀行が対象とする個人が未成年者等の制限行為能力者である場合には、契約の締結と、情報銀行との間の同意等の手続きについては、それぞれ法令に照らし、適切な者が行う必要がある。
✓ ①の同意については、個人情報保護法上の「本人の同意」として同意を得るべき者が行う。
✓ ②の契約については、制限行為能力者に関する法律の規定に従い、同意権者の同意に基づいて本人が契約を締結することや、法定代理人が本人に代わって契約を締結することが必要となる。

2.4 情報銀行に委任した個人情報の利用目的の妥当性

利用目的は、できる限り特定されているか確認する

利用目的の特定（個人情報保護法第 15 条第 1 項関係）

個人情報取扱事業者は、個人情報を取り扱うに当たっては、利用目的をできる限り具体的に特定しなければならないが、利用目的の特定に当たっては、利用目的を単に抽象的、一般的に特定するのではなく、個人情報が個人情報取扱事業者において、最終的にどのような事業の用に供され、どのような目的で個人情報を利用されるのかが、**本人にとって一般的かつ合理的に想定できる程度に具体的に特定する**ことが望ましい。

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）

全ての委任者が直接的又は間接的に便益を受け取ることができるか確認する

「情報銀行」の機能は、個人からの委任を受けて、当該個人に関する個人情報を含むデータを管理するとともに、当該データを第三者（データを利活用する事業者）に提供することであり、個人は直接的又は間接的な便益を受け取る。

情報信託機能の認定に係る指針ver2.0

当該利用目的において、情報銀行からの個人情報の提供の提案を受けない委任者が発生しないか確認する

※個人のデータ管理のみを行い、当該データを第三者に提供もしくは、情報銀行からの個人情報の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の助言を行う

全ての委任者は、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確認する

なお、個人データの提供に関し、委任者がサービス紹介を受けた提供先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（全ての委任者に対して情報銀行からの個人情報の提供の提案がなされなければならない）

2.5 情報銀行に委任した個人情報の項目の妥当性

個人情報項目の妥当性	
利用目的と取得する個人情報の項目の関係について確認する	
利用目的との関係が不明瞭な個人情報があれば取得しない（データ最小化の原則）	
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を確認する	
個人情報の取扱いにあたっては、必要最小限の項目をもって利用目的を達成し、利用目的を超えた意味情報（行動の観測、プロファイリング情報等）の抽出を行わないこと（データ最小化の原則）	
取得した個人情報を利用目的の範囲内でプロファイリングし提供先を選別し、本人に提供先サービスを提案する際の留意事項	
【本人のリスク】 プロファイリングのプロセスは不明瞭であるかもしれない。個人はプロファイル化されることを知らず、又は何が関係しているかを理解していないかもしれない	
(GDPRに関するガイドライン) 自動化された個人に対する意思決定とプロファイリング に関するガイドライン	
「自分がどのように評価されているか」が、わからないと不安	対策（「わからない」ことがリスクのため、これを解決する） 情報銀行からの個人情報の提供の提案に選別の条件がある場合、その条件を明示する 例）〇〇地区にお住まいと推測される方に紹介するサービス
「なぜ、自分が、このような評価なのか」理解できないと不満	
「自分の知らないところで自分が評価される」のは不快	
評価によって差別が助長される	
「プロファイリング」とは、自然人と関連する一定の個人的側面を評価するための、特に、当該自然人の 業務遂行能力、経済状態、健康、個人的嗜好、興味関心、信頼性、行動、位置及び移動に関する側面を分析又は予測するための、個人データの利用によって構成される、あらゆる形式の、個人データの自動的な取扱いを 意味する。	
GDPR 第4条（4）	

2.6 提供先第三者の選定方法の妥当性

提供先は個人情報の取り扱いについて適切な監督が可能であるか確認する

個人と情報銀行間の契約において「提供先第三者に帰責事由があり個人に損害が発生した場合は、情報銀行が個人に対し損害賠償責任を負う」としている
情報銀行は提供先を監督しなければならない

監督とは、提供先における個人データ取扱状況の把握を含み、提供先における提供された個人データの取扱状況を把握するために、定期的に監査を行う等により、契約で盛り込んだ内容の実施の程度を調査した上で、提供の内容等の見直しを検討することを含め、適切に評価すること

情報提供先にも、情報銀行と同様、認定基準に準じた扱い（セキュリティ基準、ガバナンス体制、事業内容等）を求め、自らが講ずべき安全管理措置と同等の措置が講じられるよう、監督を行うものとする

情報銀行が認定基準が求める水準を超える高い水準の安全管理措置を講じている場合に、提供先に対してもこれと同等の措置を求める趣旨ではなく、**提供先は個人情報の取扱いのリスクに応じて情報銀行が要求するリスク対策を講じれば足りる**

提供先は、原則として P マークまたは I S M S 認証の取得を要する

提供先が P マークまたは I S M S 認証を取得していない場合、情報銀行認定ガイドブックに則り、情報銀行が当該提供先におけるデータの安全性を確保するための具体的な対策を講じ、提供先における体制と合わせて総合的に「認定基準に準じた扱い」を実現する

委任者が直接的又は間接的に便益を受け取ることができる提供先であるかを確認する

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を確認する

社会的信頼性、苦情が多い事業者ではないことを確認する

2.7 委任を受けた個人情報の提供の判断

提供先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

個人の同意している提供先の条件について、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確認

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確認

提供先がPマークまたはI S M S 認証を取得していない場合、情報銀行認定ガイドブックに則り、情報銀行が当該提供先におけるデータの安全性を確保するための具体的な対策を講じ、提供先における体制と合わせて総合的に「認定基準に準じた扱い」を実現するために、提供する個人情報の限定及び取扱いの限定を行う

「包括同意」においては、提供先の範囲をできる限り特定する

d) 個人情報を第三者に提供することが予定される場合の事項
(中略)

ー 当該情報の提供を受ける者又は提供を受ける者の組織の**種類**、及び**属性**

JIS Q 15001:2017 A.3.4.2.5 A.3.4.2.4 のうち本人から直接書面によって取得する場合の措置

“組織の**種類**、及び**属性**”とは、個人情報の提供を受ける組織（企業）の業種と提供元である組織（企業）との関係（関連会社、持株会社など）をいう

JIS Q 15001:2017 B.3.4.2.5 A.3.4.2.4 のうち本人から直接書面によって取得する場合の措置

(第三者提供の制限の原則)

Q 5－9 第三者提供の同意を得るに当たり、提供先の氏名又は名称を本人に明示する 必要はありますか。

A 5－9 提供先を個別に明示することまでが求められるわけではありません。もっとも、想定される提供先の範囲や属性を示すことは望ましいと考えられます。

「個人情報の保護に関する法律についてのガイドライン」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関するQ & Aより（抜粋）

2.7.1 提供先がPマークまたはISMS認証を取得していない場合①

①情報は情報銀行が管理し、提供先は決められた方法で、必要な情報の閲覧のみができることとする

課題・論点 どのような情報・手法であれば提供先が閲覧しても問題ないか？（転記、複写等の目的外利用を排除）

解決案：転記、複写等の目的外利用を排除するリスク対応が必要

組織的対策	転記、複写を行わない契約を締結する
技術的対策	一覧での閲覧は不可とする技術的対策を講じる（転記、複写リスク）
	一人分のみ閲覧とする技術的対策を講じる
	任意検索不可とする＊（本人が提示したアクセスキーで検索。このアクセスキーは提供先が事前に知り得ないもの）
	複写ができないよう技術的対策を講じることが望ましい
物理的対策	提供先のサービスモデルに応じて、必要な情報のみ閲覧ができるよう表示項目を限定することが望ましい

- ＊プロフィール等の条件を指定して、該当者複数名を一覧検索する「任意検索」は不可とする
- ＊プロフィール等の条件を指定して検索する場合、該当者人数等の個人データに該当しないよう統計情報のみを閲覧可とする。
- ＊対面での対応に対して、本人からの申し出により、本人が提示するアクセスキーを用いて本人確認する場合であって、氏名、生年月日など2要素を聞いて検索することとする（類似例：コールセンターでの応対システム）

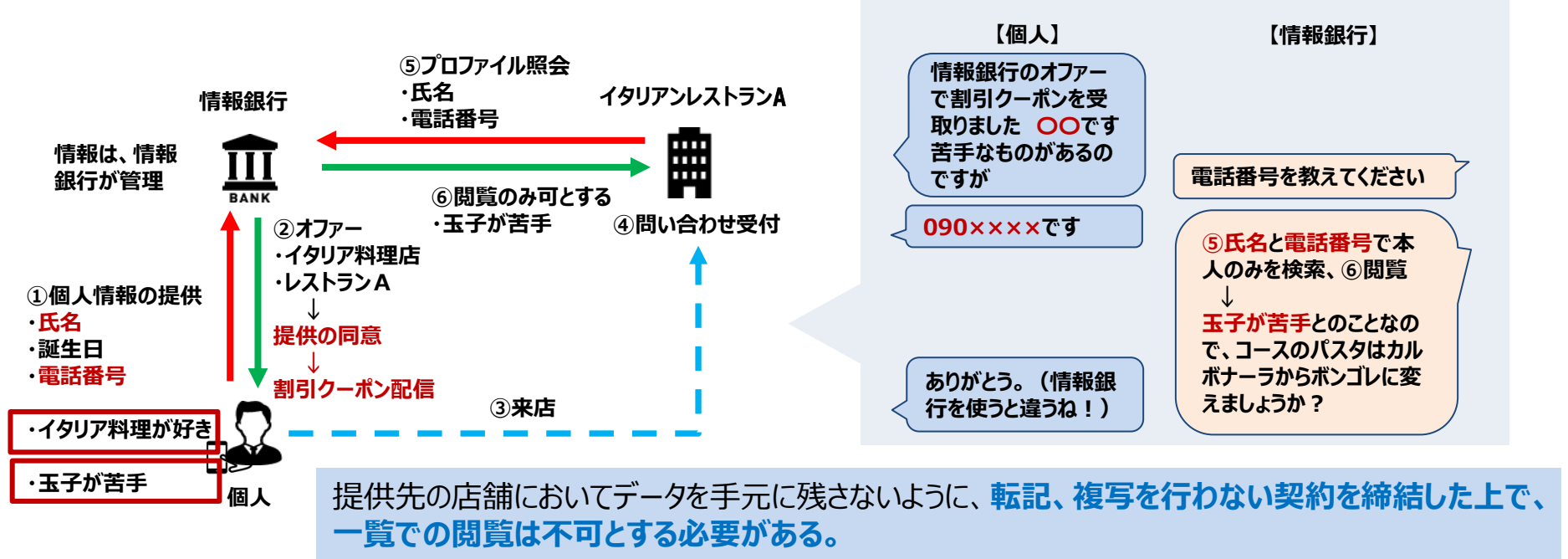
2.7.1 提供先がPマークまたはISMS認証を取得していない場合① 事例1

①情報は情報銀行が管理し、提供先は決められた方法で、必要な情報の閲覧のみができることとする

課題・論点 どのような情報・手法であれば提供先が閲覧しても問題ないか？（転記、複写等の目的外利用を排除）

①事例 1（提供先の店舗で 個人のプロフィールを確認する場合）

提供先の店舗において、本人からの申し出により、**本人が提示するアクセスキーを用いて本人確認**する場合。提供先は、直接本人から取得した個人情報を用いて、情報銀行に保管してある本人の個人情報を閲覧する。
（提供先に本人が、直接問い合わせを行い、本人の登録情報を確認する場合など、以下図解参照）



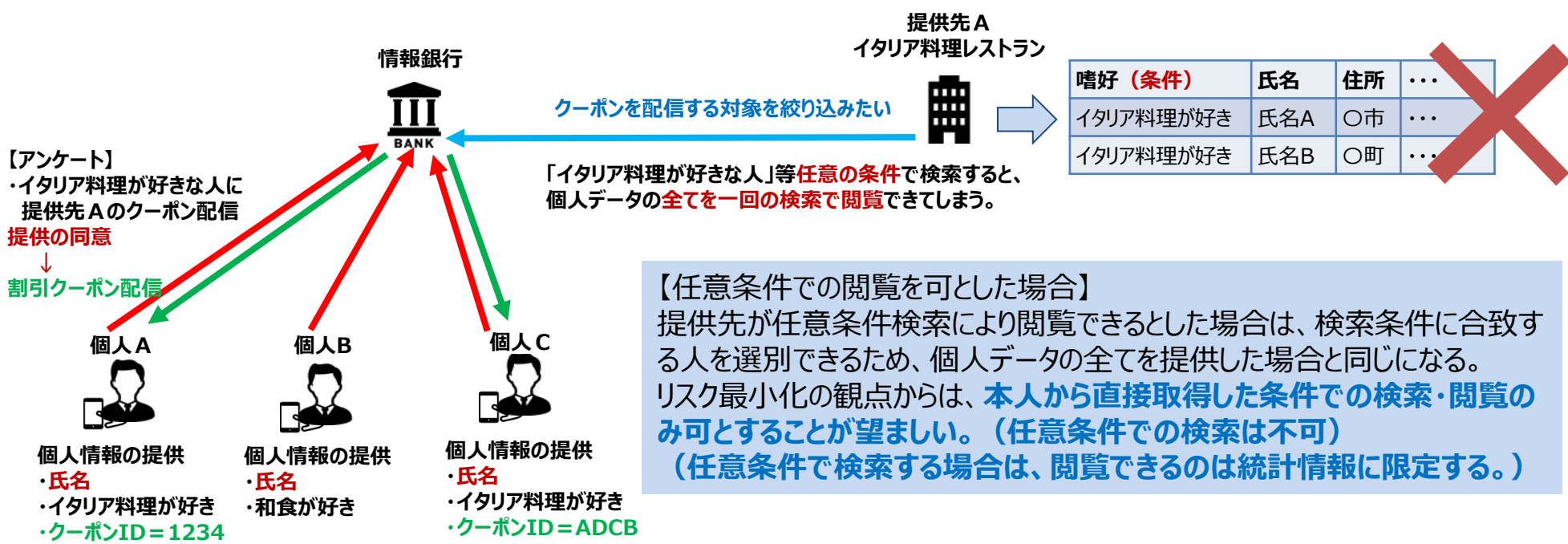
2.7.1 提供先がPマークまたはISMS認証を取得していない場合① 認められない事例1

①情報は情報銀行が管理し、提供先は決められた方法で、必要な情報の閲覧のみができることとする

課題・論点 どのような情報・手法であれば提供先が閲覧しても問題ないか？

①認められない事例1 任意条件での検索を可とした場合

任意条件での検索を可とした場合、以下の事例のように対象者の個人データを「提供」した結果と同じになる。
転記・複写禁止を契約条項に含めても、違反時の罰則は適用できるが、違反を止めることはできないためリスク対策が必要



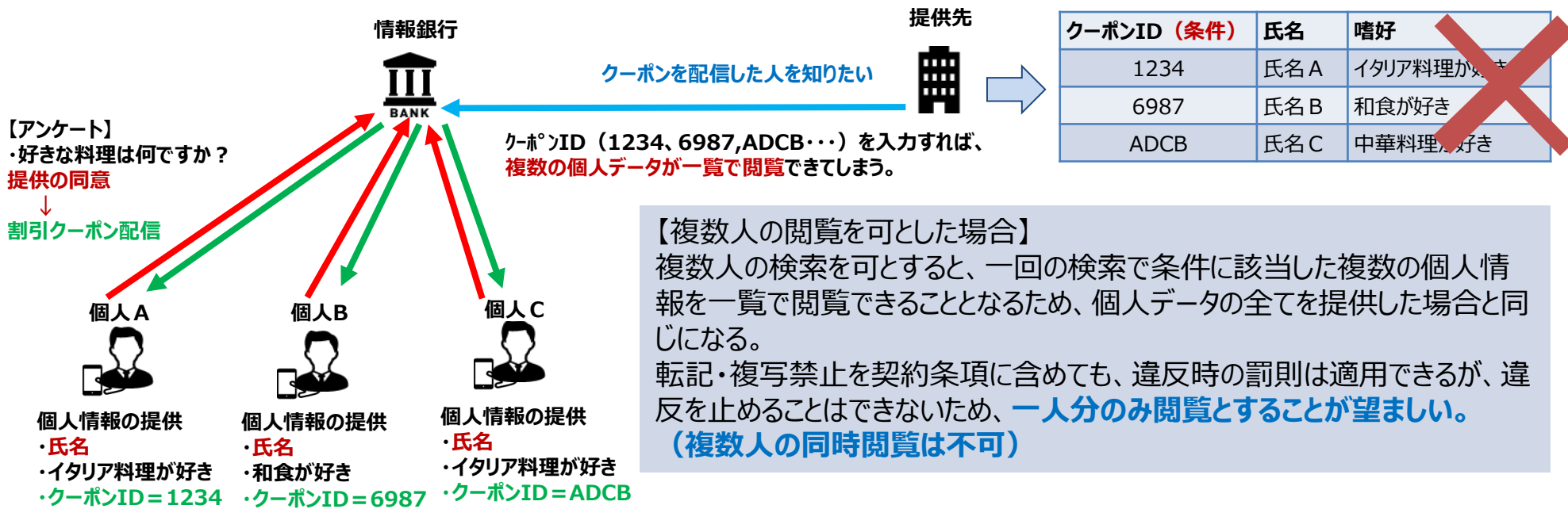
2.7.1 提供先がPマークまたはISMS認証を取得していない場合① 認められない事例2

①情報は情報銀行が管理し、提供先は決められた方法で、必要な情報の閲覧のみができることとする

課題・論点 どのような情報・手法であれば提供先が閲覧しても問題ないか？

①認められない事例2 一度に複数人の検索を可とした場合

一度に複数人の閲覧を可とした場合、以下の事例のように対象者の個人データを「提供」した結果と同じになる。
転記・複写禁止を契約条項に含めても、違反時の罰則は適用できるが、違反を止めることはできないためリスク対策が必要



2.7.2 提供先がPマークまたはISMS認証を取得していない場合②

②提供先において特定の個人を識別できないよう、個人情報の一部の置き換え等の処理を行い、復元に必要な情報を除いた形で提供先に提供する

課題・論点	「特定の個人を識別できない」ための要件とは何か
-------	-------------------------



特定の個人を識別する情報を除くこと（規則19条1号の加工）

「匿名加工情報の適正な加工の方法に関する報告書」（2017年2月21日版 国立情報学研究所「匿名加工情報に関する技術検討ワーキンググループ」）を参照すると、組み合わせによって特定の個人を識別することができる記述等となる項目を以下のとおり、限定的に考えることが望ましい。

- (a)氏名以外の基本4情報（住所、生年月日、性別）
- (b)現在所属するまたは過去に所属した会社、学校等の団体、職歴および学歴であって、具体的な会社名、団体名を含むもの
- (c)本人到達性のあるメールアドレス、SNSのID
- (d)本人到達性のある電話番号（スマートフォン、自宅の電話番号、職場等の電話番号）
- (e)クレジットカード番号

これらに(f)単体で特定の個人を識別することができるもの(氏名、顔画像)を合わせた特定の個人を識別することができる記述等を構成する項目を、以下「特定対象項目」という。

※(a)のうち、住所については市区町村、生年月日については年までとする。性別はそのまま残してよい。

同報告書では、個人情報保護委員会規則第19条第1号の措置の対象となる情報については、「全部又は一部を削除すること（当該全部又は一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む）」を求めている。

提供先で個人情報と照合ができない状態にすること（規則19条5号の加工）

情報又はその組み合わせが一意で、その情報と氏名等が紐づく情報が提供先等にとって入手可能な場合、そのような情報又はその組み合わせは、提供先等で個人情報になる。たとえば、アプリベンダーAが保有するユーザーのGPS移動履歴は多くの場合一意である。アプリベンダーAはユーザーの氏名等を保有しないが、アプリベンダーBはGPS移動履歴と氏名を保有しているとき、アプリベンダーAの保有するGPS移動履歴は、アプリベンダーBにとって個人情報である。

2.7.2 提供先がPマークまたはISMS認証を取得していない場合②

② 提供先において特定の個人を識別できないよう、個人情報の一部の置き換え等の処理を行い、復元に必要な情報を除いた形で提供先に提供する

課題・論点	「特定の個人を識別できない」ための要件とは何か
-------	-------------------------



解決案：提供しても安全といえる処理（１） or （２）

- （１）匿名加工情報相当のものとする
1号加工から5号加工までのすべてを行うが、匿名加工情報作成の意図がないため作成時公表義務等の対象にはならない。
- （２）「匿名加工情報の適正な加工の方法に関する報告書」（2017年2月21日版 国立情報学研究所「匿名加工情報に関する技術検討ワーキンググループ」）を参考に、1号加工、2号加工（個人識別符号の削除等）、4号加工（一般的に特異な情報の削除等）を行うが、履歴は原則としてそのままとする。
特定の個人を識別する可能性がないとは言えないが、現在の履歴には要配慮個人情報が含まれていないことから、個人識別のリスクは許容される範囲である

個人データの再提供の制限への該当性について

「提供先第三者において個人情報を統計情報等個人情報ではないデータに加工し、別の第三者に提供する」場合には、指針2.0によって再提供禁止が緩和されている。（１）の場合は情報銀行によって匿名加工情報相当の加工が行われているため、特定の個人を識別するおそれはなく、再提供は認められる。（２）の場合、特定の個人を識別するおそれがないとはいえないことに加えて、提供先が通常の要件を満たしておらず、再提供先との契約等について不備があるおそれがあるため、再提供は禁止とする。

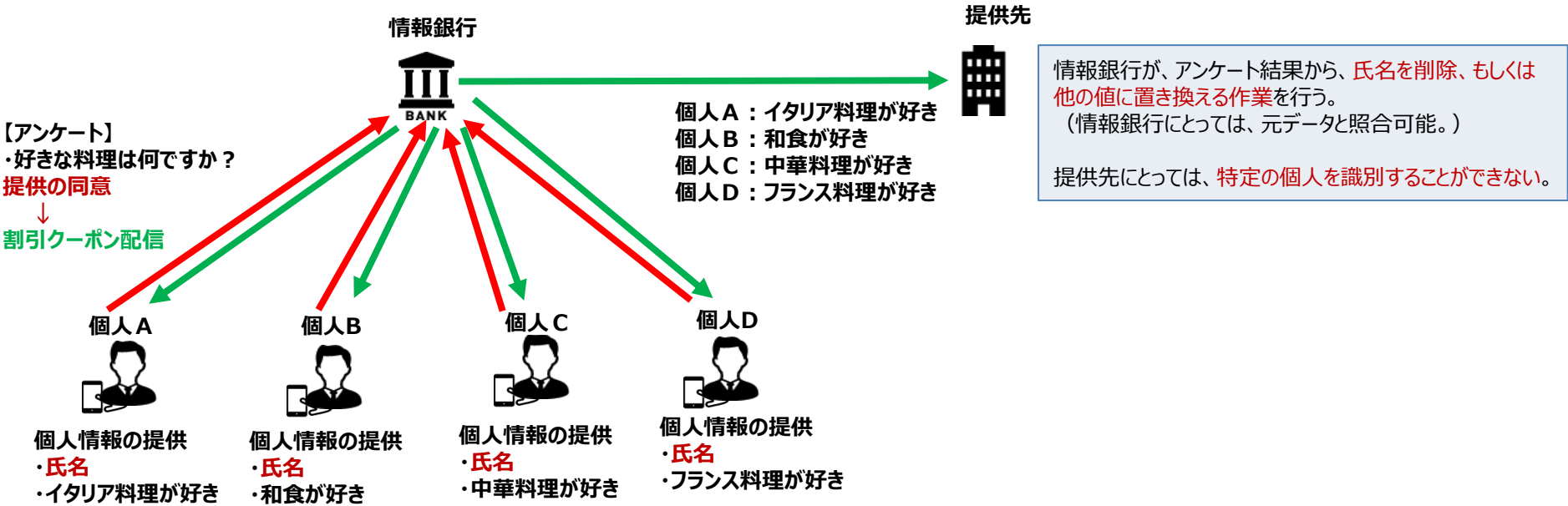
2.7.2 提供先がPマークまたはISMS認証を取得していない場合② 事例1

②提供先において特定の個人を識別できないよう、個人情報の一部の置き換え等の処理を行い、復元に必要な情報を除いた形で提供先に提供する

課題・論点 提供しても安全といえるような処理はどのようなものか、議論が必要ではないか？

②事例 1（記名アンケートの情報を提供する場合）

情報銀行が、アンケート調査対象者の属性情報、アンケート回答内容、ウェブサイトへのアクセスログ等、**当該情報のみでは直接特定の個人を識別することができない情報**を、提供先に提供する場合。



2.7.2 個人情報の定義（提供元基準）

「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）（案）」に関する意見募集結果
<https://search.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000151056>

N o 19

ある情報を第三者に提供する場合、当該情報が「他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなる」かどうかは、当該情報の**提供元である事業者**において「他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなる」かどうかで判断します。

個人情報保護法等の改正に伴う研究倫理指針の改正について
文科省、厚労省、経産省

<https://www.mhlw.go.jp/file/06-Seisakujouhou-10600000-Daijinkanboukouseikagakuka/0000170955.pdf>

P 33

改正後の指針では、提供先の事情において本人同意の要否が左右されとなると、本人保護の観点から安定性を欠くことから、提供先機関における照合性の状況の如何にかかわらず、提供元機関で個人情報とみなされる場合は個人情報の提供とみなすこととする（いわゆる「**提供元基準**」を明確化）

識別非特定情報（パーソナルデータ）も、容易照合性があれば、個人情報になる。

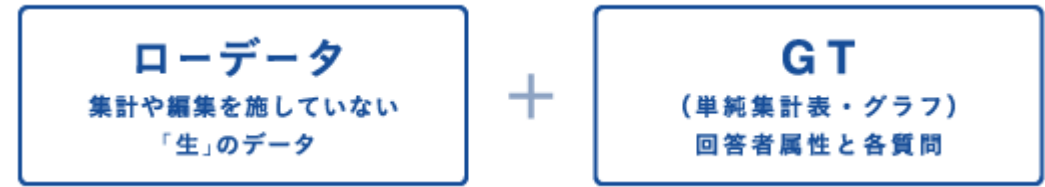
2.7.2 提供先がPマークまたはISMS認証を取得していない場合 事例2

提供先において特定の個人を識別できないよう、個人情報の一部の置き換え等の処理を行い、復元に必要な情報を除いた形で提供先に提供する

提供データのイメージ
特定する情報を除く（氏名、メールアドレス等の削除）
提供先で個人情報と照合ができない状態

事例 アンケート収集代行 株式会社 マクロミル

提供データ



株式会社 マクロミルは、情報銀行認定事業者ではないため
認定指針の全てを満たしているものではありません。
※クライアント等から第三者への再提供は、情報銀行では禁止

本件類似のデータ提供形態の事例として紹介するものです

調査対象者の属性情報、アンケート回答内容、ウェブサイトへのアクセスログ等、当該情報のみでは直接特定の個人を識別することができない情報を提供（クライアント等から第三者への再提供を含みます。）することがあります。

クライアント等は、当社が提供する情報を利用し、また、マーケティング・リサーチ等関連目的のために当該情報とクライアント等が保有する情報を組み合わせて利用する場合があります。

なお、当社が提供する情報とクライアント等が保有する情報を組み合わせることによって特定の個人を識別することができる場合がありますが、当社はこれらの場合、

- (i) 当社が提供する情報をマーケティング・リサーチ等関連目的の範囲内で利用すること、
- (ii) クライアント等が保有する氏名や住所、電話番号、メールアドレス等の直接特定の個人を識別できる情報と当社から提供する情報を紐づけるなどして個人を再特定しないこと
- (iii) クライアント等から再提供を行う場合には再提供可能な者の範囲および再提供先に対して許諾する利用目的等を当該クライアント等と取り決めるものとします。

2.7.3 提供先がPマークまたはISMS認証を取得していない場合③

③情報銀行の監督下で、提供先からPマークまたは ISMS認証を取得している者に個人情報の取扱いを全て委託させる

課題・論点 提供先（委託元）と委託先のスキームと情報銀行の役割を具体化する必要があるのではないか？

解決案：委託元(提供先)と委託先のスキームの整理

リスク対応として、**提供先(委託元)には、それ単体で個人情報となる情報へのアクセス権限を付与しない**

本人に対するオファーや提供先で利用するクーポン発行は、**提供先(委託元)の個人情報の利用目的の中で委託を受ける**

提供先(委託元)には、提供元で個人情報となる情報を納品しなくても、提供先の利用目的で個人情報を扱う場合には、提個人情報の提供に該当する

情報銀行事業者が委託を受けても良い（情報銀行サービスとは別サービスとする）

解決案：情報銀行の役割を具体化

「情報銀行の監督下で、委託させる」場合の具体的条件を提供先の委託契約に規定する

例1) 情報銀行、提供先、提供先の委託先間での三社契約

例2) 提供先が委託先と締結する委託契約に情報銀行の監督が及ぶように規定する

- a) 委託者及び受託者の責任の明確化
- b) 個人データの安全管理に関する事項
- c) 再委託に関する事項
- d) 個人データの取扱い状況に関する委託者への報告の内容及び頻度
- e) 契約内容が遵守されていることを委託者が、定期的に、及び適宜に確認できる事項
- f) 契約内容が遵守されなかった場合の措置
- g) 事件・事故が発生した場合の報告・連絡に関する事項
- h) 契約終了後の措置

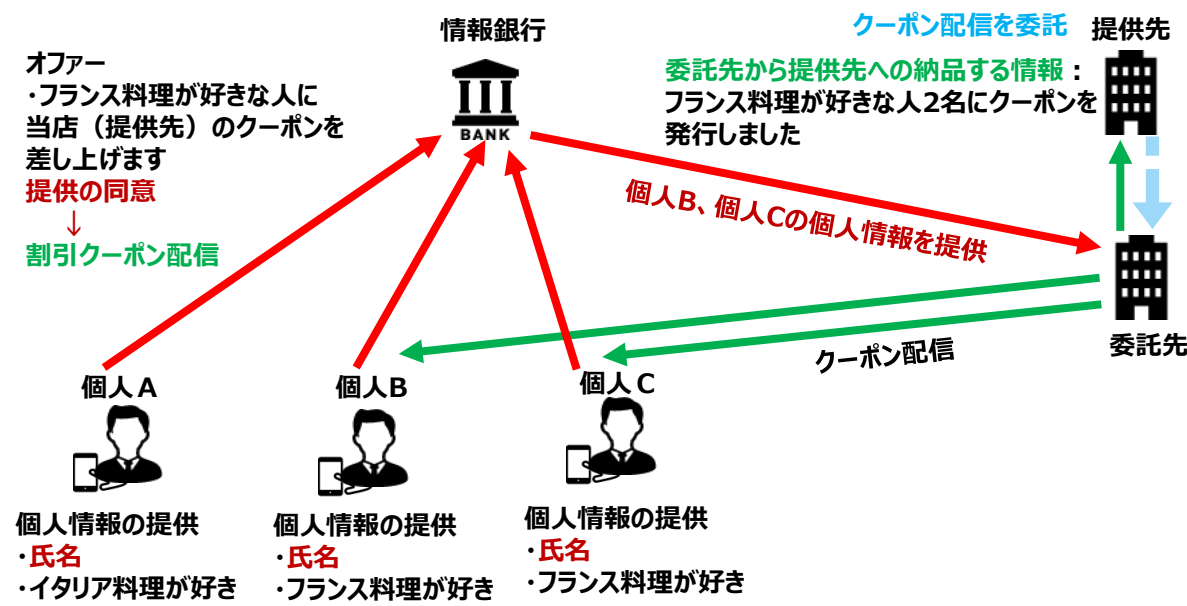
2.7.3 提供先がPマークまたはISMS認証を取得していない場合③ 事例1

③情報銀行の監督下で、提供先からPマークまたは ISMS認証を取得している者に個人情報の取扱いを全て委託させる

課題・論点 提供先（委託元）と委託先のスキームと情報銀行の役割を具体化する必要があるのではないか？

③事例 1 （委託先にクーポン配信を委託する場合）

提供先が、委託先に個人情報の取扱いの全てを委託しているケース（委託先にクーポン配信を委託）
・提供先(委託元)は、委託先に個人データの取扱いを委託するため、提供先に個人データへのアクセス権限は付与しなくて良い。



・提供先はクーポンIDのみを受取る
「提供先において特定の個人を識別できないよう、個人情報の一部の置き換え等の処理を行い、復元に必要な情報を除いた形で提供先に提供する」に該当する

※提供先がクーポンIDすら受取らない場合、委託先は提供先に個人情報を納品しないことになるが、情報銀行は個人情報を提供したといえる（提供元基準）

・Pマークまたは ISMS認証を取得している者に個人情報の取扱いを全て委託させる
情報銀行で委託を受けても良い

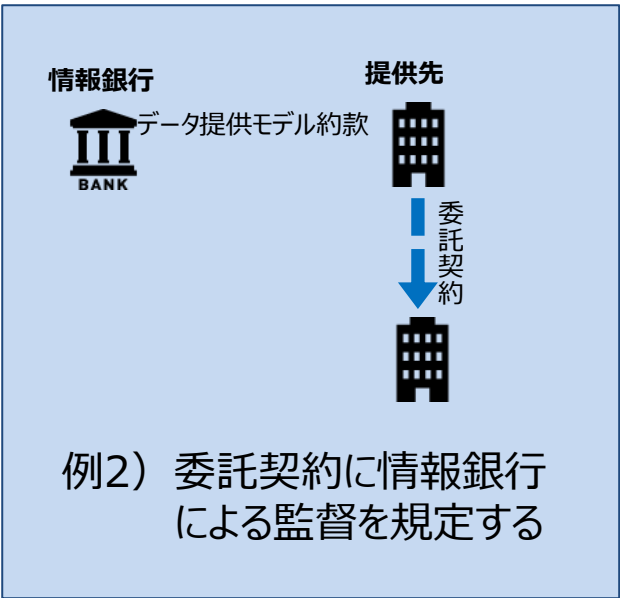
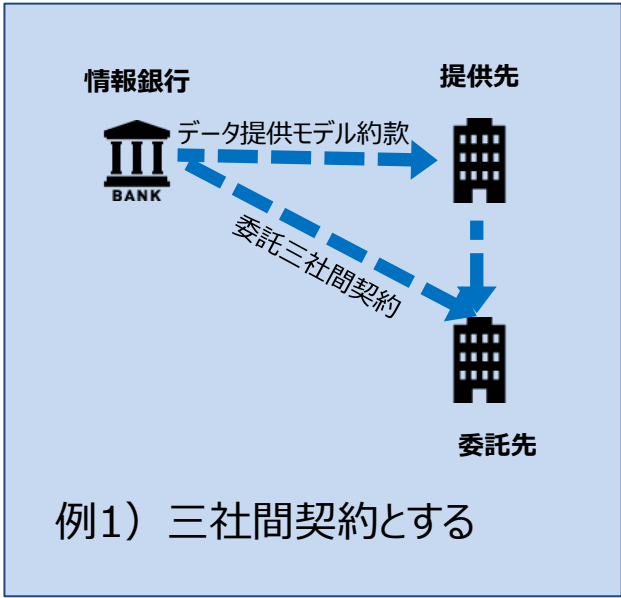
2.7.3 提供先がPマークまたはISMS認証を取得していない場合③ 事例1

③情報銀行の監督下で、提供先からPマークまたは ISMS認証を取得している者に個人情報の取扱いを全て委託させる

課題・論点 「情報銀行の監督下で委託させる」とは、どのような契約が必要か

③事例 1 （委託先にクーポン配信を委託する場合）

三社間契約または、委託契約にて「情報銀行の監督下」とする場合



- 情報銀行の監督が及ぶために委託契約に盛り込むべき要件
- b) 個人データの安全管理に関する事項
 - d) 個人データの取扱い状況に関する情報銀行への報告の内容及び頻度
 - e) 契約内容が遵守されていることを情報銀行が、定期的に、及び適宜に確認できる事項
 - f) 契約内容が遵守されなかった場合の措置
 - g) 事件・事故が発生した場合の報告・連絡に関する事項

2.7.3 提供とは

「提供」とは、個人データ、保有個人データ又は匿名加工情報（以下この項において「個人データ等」という。）を、自己以外の者が**利用可能な状態**に置くことをいう。個人データ等が、物理的に提供されていない場合であっても、ネットワーク等を利用することにより、個人データ等を利用できる状態にあれば（**利用する権限**が与えられていれば）、「提供」に当たる。

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）

「提供」とは、上記のとおり、利用する権限が与えられることである。

委託モデルにおいては、提供先に利用権限が与えられるが、提供先は全面的にそれを行行使することなく、提供を受けた個人情報の管理を委託先に委ねて限定的なアクセスのみを行う。提供を受けた個人情報について、提供先がこのような取扱いをすることについては、情報銀行との間の契約によって義務付けられることになる。

2.8 提供先第三者の個人情報の利用目的の妥当性

提供先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

個人の同意している提供先の条件について、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確認

個人にとって不利益となる利用がされていないか

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を確認する

不適切なインターネット異性紹介事業者の条件

「インターネット異性紹介事業を利用して児童を誘引する行為の規制等に関する法律（平成15年6月13日法律第83号）に規定する「インターネット異性紹介事業者」のうち、次のいずれか一つでも満たすことができない者は、不適切

基本情報の開示	次に掲げる事項をホームページにより、登録希望者又は登録者（以下「顧客」という。）が閲覧できるようにしていること。 ①事業者の概要（事業者名、代表者名、住所、電話番号） ②提供サービスの内容と価格 ③顧客相談の専用窓口の連絡先
サービス提供の対象	18歳以上の独身者のみを対象としていること
サービス内容及び提供条件の明確化	顧客にサービスを提供するに当たっては、提供サービスごとの名称とその内容、対応する価格、提供する条件等を明記していること。 「特定商取引に関する法律」（昭和51年6月4日法律第57号）の適用を受ける場合は、同法の規定に従って、適正に実施していること。
公安委員会への届出	「インターネット異性紹介事業を利用して児童を誘引する行為の規制等に関する法律」第7条の規定に基づき、管轄する都道府県の公安委員会に届け出ていること。
本人確認	登録希望者が本人であり、かつ、18歳以上であることを、公的な証明書を用いて確認し、その写しを記録として保管していること
独身者である旨の確認又はそれに代わる措置	登録希望者が独身者であることを、公的な証明書を用いて確認し、その写しを記録として保管していること。 ① 会員制のサービスであること ② 独身である旨を宣誓させていること（入会申し込みの際に必ず独身である旨を回答させること） ③ 会員規約に、もし既婚者であることが発覚した場合、体かいはもちろんのこと、損害賠償を求めることがある旨を規定していること ④ 有料サービスであること（男女双方とも有料） ⑤ 交際に合意するまでは、事業者のシステムを介して本人同士が連絡をとりあう仕組みであること ⑥ 事業者のシステムを介して本人同士が連絡をとりあう場合において、その内容に公序良俗に反するものが含まれていないか確認し、必要に応じて会員資格の停止又は退会の措置を講じていること

3. データ倫理審査会の開催

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

データ倫理審査会運用フロー

1	情報銀行での事前準備（ビジネススキーム概要の認識）	
	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（業務フロー図の作成）	
2	データ倫理審査会の準備	
	データ倫理審査会のメンバー選定	
	データ倫理審査会運規程の作成	
	データ倫理審査会との事前協議	
3	データ倫理審査会の審議の準備（リスクマネジメント・プロセス）	
	リスクアセスメント（リスクの特定・分析・評価）	
	リスク対策の検討及び決定、残留リスクの認識	
	PIA報告書の作成及び定期的見直し	
4	データ倫理審査会の開催（本人視点での審議、事業者による意思決定）	
	審査	
5	リスク対策の実施	
	リスク対応等の決定	
	リスク分析表の作成	
	リスクの見直し	
6	透明性の確保（議事録の公表）	
	PIA報告書最終版の作成	
	PIA報告書最終版の公表	

ビジネススキームの妥当性協議

- ・個人と情報銀行の間の契約内容の妥当性
- ・個人情報の利用目的及び個人情報の項目の妥当性
- ・提供先第三者の選定方法の妥当性
- ・提供データの妥当性
- ・提供先第三者の個人情報の利用目的の妥当性

委任者視点での協議

- ・ユーザビリティの確認（わかり易い・使い易い）
- ・コントロールビリティの確認（本人による追跡や関与が可能）

議事録を作成し、公開する

3.1 データ倫理審査会（委任者視点での協議／ユーザビリティの確認、コントローラビリティの確認）

個人情報保護リスクアセスメント結果について、委任者の利益に反していないかという観点からリスクを捉えるために、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、以下の事項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）及び個人情報保護管理者を含む会議体で審議し、情報銀行としてリスク対策の決定をする

決定したリスク対策は「安全対策手順書」として別途まとめる

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。

データ倫理審査会が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、同じ第三者によって行われるべきではない

3.2 個人と情報銀行間の利益相反等（善行原則 beneficence）

善行原則（beneficence）とは、他人の幸福を促進する行動を指し、委任者が直接的又は間接的な便益を受け取るサービスを提供することをいう

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などを確認する。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など

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

3.2.1 「同意」取得の妥当性の確認

個人情報の取扱いを許可するか否かの選択の機会について、任意に、具体的に、わかりやすく本人に示していること

「情報銀行」認定申請ガイドブック（TPDMS-1000）_ver2.0

GDPR 第7条 同意の条件（要約）

別の事項とも関係する書面上の宣言の中で本人の同意が与えられる場合、その同意の要求は、別の事項と明確に区別でき、理解しやすく容易にアクセスできる方法で、明確かつ平易な文言を用いて、表示されなければならない
そのような書面上の宣言中の本規則の違反行為を構成する部分は、いかなる部分についても拘束力がない

本人は、自己の同意を、いつでも、撤回する権利を有する
同意の撤回は、その撤回前の同意に基づく取扱いの適法性に影響を与えない
同意の撤回は、同意を与えるのと同じように、容易なものでなければならない

サービスの提供を含め、当該契約の履行に必要な個人データの取扱いの同意を契約の履行の条件としているか否かについて、最大限の考慮が払われなければならない

有効な同意の要素 GDPR 同意に関するガイドライン（要約）

本人が真の選択をせず、同意を強制されたと感じる、又は、同意しなければネガティブな結果に直面すると感じるならば、同意は有効ではない

契約条件の承諾と同意を「抱き合わせる」状況、又は、契約の履行又はサービスの提供に必要とされない個人データを取扱うための同意と契約又はサービスの提供とを「結びつけること」が極めて望ましくない

厳密に必要な事柄以外に個人データの利用を承諾するように強制することも、本人の選択を制限し自由な同意を阻む

同意は、本人が不利益を被らずに 同意を拒否し又は撤回できない場合には、自由であるとはみなされない

ここで「自由」とは「任意」と解釈して良い34

3.3 本人のメリット等（正義原則 justice/equality）

正義原則（justice/equality）とは、公平原則ともいい、根拠のない差別をなくすこと、及び、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

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

3.3.1 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を確認する

取得した個人情報の項目をプロファイリングしサービスを提案する際の留意事項

本人のリスク	「自分がどのように評価されているか」が、わからないと不安	要件	本人はプロファイリングに従わない権利を有する
	「なぜ、自分が、このような評価なのか」理解できないと不満		
	「自分の知らないところで自分が評価される」のは不快	対策	保護を確保するための適切な措置を実装する
	評価によって差別が助長される		

閲覧履歴、購読履歴からのプロファイリング

あなたにオススメのブックツリー

プロファイリングの手順を示している

本の専門家であるブックキュレーターが独自のテーマで集めた数千の本を、あなたの「関心・興味」や「読んでみたい気分」に沿ってご紹介。



オススメから興味のない商品を消したい

プロファイリングに従わない権利の実装

興味のない商品は、下記の手順で消すことができます。

1. 「Myページ」→「あなたにオススメ」を表示。
2. 消したい商品の「この作品に興味はありません」「この著者に興味はありません」いずれかをチェック。
3. 「チェックした評価でおすすめの商品を更新する」を選択。

「この著者に興味はありません」にチェックをすると、当該著者の別の作品もオススメされなくなりますのでご注意ください。

第22条 プロファイリングを含む個人に対する自動化された意思決定

1. データ主体は、当該データ主体に関する法的効果を生じさせる、又は、当該データ主体に対して同様の重大 な影響を及ぼす**プロファイリングを含むもっぱら自動化された取扱いに基づいた決定の対象とされない権利**を有する。
3. （中略）データの管理者は、データ主体の権利及び自由並びに正 当な利益、少なくとも、管理者の側での人間の関与を得る権利、データ主体の見解を表明する権利及びその決 定を争う権利の**保護を確保するための適切な措置を実装する**ものとする。

GDPR 第22条 プロファイリングを含む個人に対する自動化された意思決定

3.3.2 情報銀行に委任した個人情報の項目の妥当性

個人情報の項目の妥当性

利用目的と取得する個人情報の項目の関係について確認する

利用目的との関係が不明瞭な個人情報があれば取得しない（データ最小化の原則）

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を確認する

個人情報の取扱いにあたっては、必要最小限の項目をもって利用目的を達成し、利用目的を超えた意味情報（行動の観測、プロファイリング情報等）の抽出を行わないこと（データ最小化の原則）

取得した個人情報の項目をプロファイリングし提供先を選別し、本人に提供先サービスを提案する際の留意事項

【本人のリスク】 プロファイリングのプロセスは不明瞭であるかもしれない。個人はプロファイル化されることを知らず、又は何が関係しているかを理解していないかもしれない

（GDPRに関するガイドライン） 自動化された個人に対する意思決定とプロファイリング に関するガイドライン

「プロファイリング」とは、自然人と関連する一定の個人的側面を評価するための、特に、当該自然人の 業務遂行能力、経済状態、健康、個人的嗜好、興味関心、信頼性、行動、位置及び移動に関する側面を分析又は予測するための、個人データの利用によって構成される、あらゆる形式の、個人データの自動的な取扱いを意味する。

GDPR 第4条（4）

3.4 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）

無危害原則（non-maleficence）とは、「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、リスク認識そのものである

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

3.4.1 想定リスクの妥当性

事業継続（情報資産保護）の観点からのリスク認識

補助資産	リスク源	リスク	脅威の例（同じ誤用や乱用、あるいは技術的又は環境的な障害を含むシナリオも、潜在的な脅威と見なす）
ハードウェア	異常使用	滅失	個人ファイルの保管：個人利用
ハードウェア	異常使用	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。
ハードウェア	ダメージ	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
ハードウェア	スパイ活動	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
ハードウェア	滅失	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
ハードウェア	滅失	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
ハードウェア	変更	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
ハードウェア	変更	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
ハードウェア	変更	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
ハードウェア	オーバーロード	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
ハードウェア	破損	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
ソフトウェア	異常使用	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
ソフトウェア	異常使用	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
ソフトウェア	異常使用	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
ソフトウェア	ダメージ	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
ソフトウェア	スパイ活動	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
ソフトウェア	スパイ活動	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
ソフトウェア	滅失	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

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。

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。

提供元、提供先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、提供先に確認する。

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。

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。

組織は、個人情報の取扱いに関する法令、国が定める指針その他の規範（以下，“法令等”という。）を特定し参照できる手順を確立し、かつ、維持しなければならない。

A.3.3.2 法令、国が定める指針その他の規範 個人情報保護マネジメントシステム－要求事項 JIS Q 15001：2017

3.5 個人情報の第三者提供条件の指定・変更の方法（U I）（自律尊重原則 autonomy）

自律尊重原則（autonomy）とは、個人情報に関する自己コントロール権をいう

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（U I）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、「提供先が誰か」、「提供先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

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、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

データ主体の「同意」とは、自由に与えられ、特定され、事前に説明を受けた上での、不明瞭ではない、データ主体の意思の表示を意味し、それによって、データ主体が、その陳述又は明確な積極的行為により、自身に関連する個人データの取扱いの同意を表明するものを意味する

GDPR第4条（11）

「自由」の要素は、データ主体に真の選択と支配権限があることを意味している。一般的なルールとして、GDPR は、データ主体が真の選択をせず、同意を強制されたと感じる、又は、同意しなければネガティブな結果に直面すると感じるならば、同意は有効ではないと規定している。

同意が契約条件の交渉できない部分としてまとめられている場合、それは自由に与えられたものとはみなされない。

したがって、同意は、データ主体が不利益を被らずに 同意を拒否し又は撤回できない場合には、自由であるとはみなされない。

GDPR 同意に関するガイドライン 3.1

3.6 リスク対策の適切性

想定リスクへの対策として合理的説明ができているか確認する

リスクへの対策として合理的な説明となっているかを確認する。最低限、日本語としてリスクと対策がかみ合い、かつその対策によってリスクを防止できることを、一般人が納得できること

リスク対策によって、想定したリスクが解消しているか確認する

「人間は間違える」ことを前提としたリスク対策となっているか確認する
間違えても影響を最小限におさえる機能を持っているか確認する
入力した結果、本人に与える影響を逐次説明することが望ましい

「〇〇が正しいことを確認する」というリスク対策は、慢性化の中で見落としや妥協が生じ易い
「〇〇が間違っているものを発見する（間違い探し）」というリスク対策が望ましい
入力エラーは、その理由が本人にわかり易いことが必要

リスクレベルに応じた対策か確認する

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
入力した際に、ポップアップで再確認するなどの配慮を行う

リスク対策が現在の水準と合致しているか確認する

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

3.6.1 委任者（本人の権利への対応）の観点からのリスク特定

委任者にとっては、自らが提供したデータが個別には把握していない第三者に渡ることにつき、漠然とした不安があり、データを提供することによる便益も把握しづらいことから、概して、データの提供には消極的な姿勢が示される。

以下についてコントローラビリティ及びユーザビリティの工夫で解決する

個人情報に関する本人の権利 JIS Q 15001 : 2017 （抜粋）	
個人情報に関する権利	組織は、保有個人情報に関して、本人から開示等の請求等を受け付けた場合は、遅滞なくこれに応じなければならない
開示等の請求等に応じる手続	組織は、開示等の請求等に応じる手続を定めなければならない
保有個人情報に関する事項の周知など	組織は、当該保有個人情報に関し、本人の知り得る状態に置かなければならない
保有個人情報の利用目的の通知	組織は、本人から、当該本人が識別される保有個人情報について、利用目的の通知を求められた場合には、遅滞なくこれに応じなければならない
保有個人情報の開示	組織は、本人から、当該本人が識別される保有個人情報の内容が事実でないという理由によって当該保有個人情報の訂正、追加又は削除の請求を受けた場合は、遅滞なく必要な調査を行い、その結果に基づいて、当該保有個人情報の訂正等を行わなければならない
保有個人情報の利用又は提供の拒否権	組織が、本人から当該本人が識別される保有個人情報の利用の停止、消去又は第三者への提供の停止の請求を受けた場合は、これに応じなければならない

委任者の観点からのリスクの例
その個人情報の第三者提供に同意した覚えが無い
提供された個人情報が何に使われているか十分に理解できない
第三者提供をやめさせる方法がわからない

3.6.2 委任者（本人の権利への対応）の利用場面の影響からのリスク認識

サービス別及びユーザインタフェース（UI）別の画面遷移図からのリスク認識

委任者が情報銀行に委任する又は委任した個人情報の項目や利用状況を認識できるのは、利用画面の表示や操作ボタンである

どのように説明文が表示されているか、表示文がわかり易いか、また、個人情報を委任する及びサービスを利用する前に同意しているかについて、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を確認するため画面遷移図を作成する

委任者の利用場面のタイプ、特に、彼らの個人情報保護リスクを識別するためのデジタルデバイスの使用におけるリスクを特定する

意図せぬ結果をもたらす可能性のある潜在的な委任者の行動の例

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）

3.6.3 委任者（本人の権利への対応）の観点からのリスク認識

ウェブサイト上で個人情報を取得する場合

サービス等の申込手続のなかで、個人情報の登録フォームを表示する前に、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）を表示し、「同意する」ボタンを押してから個人情報の登録フォームに移るようにする

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
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

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

3.6.3.1 誤って「同意する」ボタンを押してしまうリスク認識

視線や操作の流れは「上から下へ」「左から右へ」流れるようにする

必要事項は、読んでから「同意」等の操作ができるようにする

「同意」ボタンや「送信」ボタンの下に必要事項が記載すると、必要事項を読んでから操作ボタンを押すためには逆スクロールが必要となり、これを読むことを前提にしていけないことになる

画面遷移も基本的な流れは、前方向に進むこと、画面内は「上から下へ」「左から右へ」流れるようにして、戻ったりしないよう工夫する

お客様のお立場	☐ 自社での導入を検討する立場 ☐ お客様に提案・販売する立場 ☐ その他
メールマガジンの配信について 必須	グループのセミナー・キャンペーン・新サービス等のお知らせをメールマガジンでお届けします。 メールマガジンの配信を希望されますか? ☒ 希望する ☐ 希望しない
個人情報取扱いについての同意 必須	☐ 末尾に記載する弊社の個人情報の取り扱いに関する事項に同意する

送信
(クリックで完了)

当社が個人情報を取得するにあたって示すべき事項

当社は、JISQ15001の規格に準拠した個人情報保護マネジメントシステムを構築、運用し、プライバシーマークを取得しております。以下に掲げる事項は、同規格の要求事項に基づき、問い合わせ者に関する個人情報を取得するにあたり、当社がご本人に対して明示すべきものを列挙しています。

事業者の名称

「送信」ボタンの下に必要事項が記載してある
内容を確認後、逆スクロールをして戻らなければならず不便
「読み飛ばし」の「本人のリスク」がある

3.6.3.2 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

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利用目的を表示する場合

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

個人識別可能情報利用に係る通知	
サービス概要	移動履歴地図サービス
利用主体	Example 株式会社
提供する個人情報	メールアドレス 位置情報
取得方法	記録ボタンをおした時
利用目的	移動履歴を地図にしてあなたに提供するため
第三者提供	いたしません
保存期間・廃棄	半年間保存の後廃棄
本人による関与	以下から、保存されている情報の参照、訂正他ができます。
問い合わせ先	http://example.com/maps/
	Tel: 03-0000-0000
	email: info@example.com https://example.com/info/

例：項目名を省略する場合

●●●● Telco 4G 12:09 83%

alice@example.org として：
移動履歴地図サービス▼
(Example 株式会社)は、以下の情報を参照しようとしています：

■ メールアドレス >

■ 位置情報 >

(記録ボタンをおした時に取得。)
これは、移動履歴を地図にしてあなたに提供するためです。
第三者提供はいたしません。
半年間保存の後廃棄します
以下から、保存されている情報の参照、訂正他ができます。
<http://example.com/maps/>
お問い合わせは：Tel: 03-0000-0000, email: info@example.com, <https://example.com/info/>

Cancel

Accept

<

>

📄

📖

📋

経済産業省「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」

3.6.3.3 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

SIMなし 16:21 100%

利用規約

新規登録(本人)

ID

test

Eメールアドレス

test@systema.co.jp

登録

※携帯キャリアのメールアドレスをご利用の場合「ドメイン指定受信・拒否設定」、「迷惑メール設定」によって、メールが届かない場合があります。

携帯キャリアのメールアドレスの設定画面より

ドメイン

を受信できる設定になっているかをご確認ください。

累計800万人が利用するポイントサイト

今すぐ**無料会員登録**しよう!

メールアドレスを入力後、

ドメイン

から無料会員登録のご案内メールが届きます。

メールアドレス

メールアドレスを入力してください。

登録する

※ドメイン指定受信をされている場合、

ドメイン

からのメールを受信できるようご設定ください。

※お使いのメールソフトによっては、メールが「迷惑メール」フォルダに入る場合がございます。メールが届かない場合は、迷惑フォルダもご確認ください。

新規会員登録画面でメールアドレスを入力する場合

入力するメールアドレスの利用目的が明示されている

入力するメールアドレスの利用目的が明示されていない

はじめに利用目的等を明示し同意を得ているが、長文になるので利用者の十分な理解は得られない

データ入力の都度、その利用目的及び本人に及ぼす影響を端的に明示することが望ましい

3.6.3.4 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

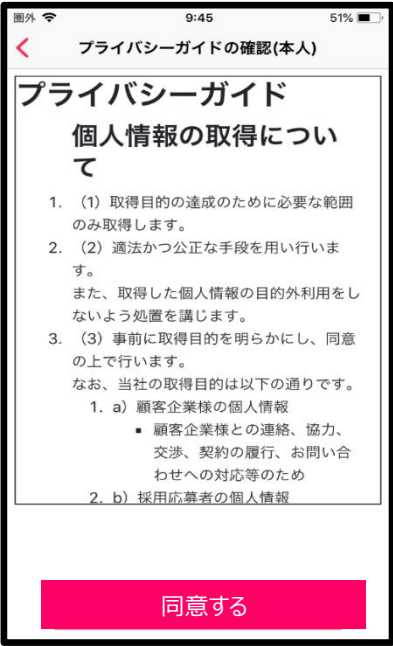
重要な項目は、ファーストビューで見えるようにする

重要な項目がスクロールしないと見えない

情報銀行と個人間のモデル契約やプライバシーポリシー等は、全文を確認できるようにすることが必要だが、スクロールして表示するので、全文を読む読者が多くない可能性がある

それぞれの入力画面で、これを入力するとどうなるのか／本人への影響／利用目的は、その都度短文で明示しないと理解できない

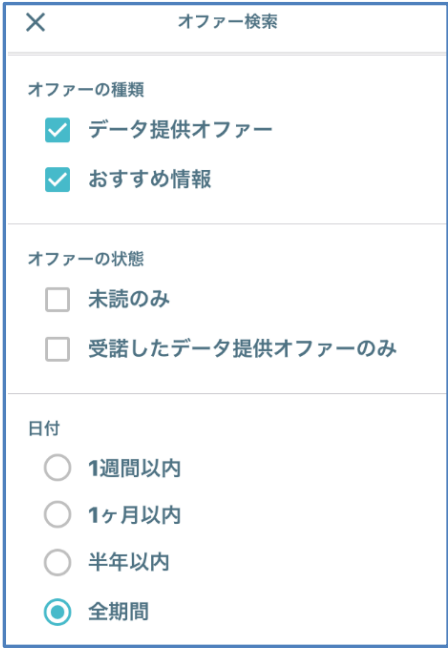
重要な項目がスクロールして最後にあると見逃す



モデル契約やプライバシーポリシー等の全文は、いつでも確認できる状態にすること、あらかじめ同意を得ることが必要

スクロールして表示するので、一般的には誰も読まない

実質的には、各入力画面で必要事項を明示し、都度、同意を得ながら進める



要件のみの表示では、誰に対して情報を提供するのか不明

入力フォームページと誘導元のデザインは統一感をもたせ、同一企業のものであることが直感的にわかる必要がある

ルックアンドフィールがあまりにも異なると、「違うWebサイトに飛ばされた？」と誤解させる恐れがある

それぞれの画面で主体者が誰であるかを明示する
例えば、自社ロゴまたはサービスロゴを表示するなど

3.6.4 委任者（本人の権利への対応）の観点からのリスク認識

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

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

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

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

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 2 3 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 2 3 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

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）

3.6.5 委任者（本人の権利への対応）の観点からのリスク認識

表示量に関する注意事項

消費者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することはできないことが想定される。
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、消費者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

消費者に多量の契約文章を読むように仕向けることは難しい。
これは、消費者が今まさに何らかの処理を行おうとしている時にはなおさらである

経済産業省「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」

3.6.6 委任者（本人の権利への対応）の観点からのリスク認識

具体的値の表示に関する事項

本人が、明示事項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。

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。

例)「電話番号」と通知するのではなく、「電話番号：03-1234-5678」と通知することである。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

取得する個人識別可能情報の項目名が表示されても、消費者にはそれが何を意味するか理解できない可能性がある。
このような状況に対応するために、具体的な値を表示するリンクを各項目に表示することが望ましい。

ある処理を許可することによって新たな個人情報が生成される場合には、同意前に実際の値を表示することは不可能である。
その場合は例示を行うのが望ましい。

例) ショッピングを行った時の購買データを提供するというような場合、消費者が会員にな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、どのようなものが提供されるのかについての消費者の理解を得るのが望ましい

Telco 4G 12:0983%

alice@example.orgとして：
移動履歴地図サービス▼
(Example 株式会社)は、以下の情報を参照しようとしています：
■ メールアドレス >
■ 位置情報 >
(記録ボタンをおした時に取得。)
これは、移動履歴を地図にしてあなたに提供するためにです。
第三者提供はいたしません。
半年間保存の後廃棄します
以下から、保存されている情報の参照、訂正他ができます。
http://example.com/maps/
お問い合わせは：Tel: 03-0000-0000,
email: info@example.com,
https://example.com/info/
CancelAccept

Telco 4G 12:0983%

メールアドレス▼
alice@example.com ?
あなたのアカウントに登録されたメールアドレスです。

例：例示を行う場合

お客様にご提供いただくのは、お客様が購入された物品のレシート情報です。
以下の様な情報が弊社に送られます。

Example Pharmacy		
Date:2014-08-27 15:04:01		
Store ID: 1234		
Customer ID: 989814501		
Item	Qty	Prs

Rose Soap	10	58.00
SleepNow	1	24.50
Subtotal		82.50
Tax (18%)		14.85
Total		97.35

3.6.7 委任者（本人の権利への対応）の観点からのリスク認識

表示形式に関する注意事項

電子的に表示する場合は、表示を担当するソフトウェアが当該条件を読み込んで、消費者の好みに最適化して表示をしたり、消費者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。これを消費者が理解できる形で表示するにあたっては、画像・アイコン等を援用してわかりやすさを求めることも可とする。

経済産業省「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」

差分通知の方法

同意を取得しようとした場合には、前回取得した同意の内容に消費者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。

経済産業省「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」

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。

3.6.8 委任者（本人の権利への対応）の観点からのリスク認識

同意するものの識別状態の表示

本人が個人情報を入力する前に、明示事項を読んで同意する仕組みにする

意思確認をする場合には、具体的に誰又はどのID に対して意思確認をしようとしているのか表示すること。
※ 昨今のシステムでは、多くの場合、複数のアカウントを使い分けることが多くなってきている。
どのアカウントでの同意かというのは非常に重要な事で、これを混同させることによって、不当な同意を取得するような攻撃も考えられる。したがって、「どの立場として」同意しようとしているのかを明示すべきである。

消費者がどの立場で、誰に対して同意しようとしているのかを、分かりやすい形で明示的に表示するのは重要である

同意の行為

表示した項目に関する明示的許可の取得にあたっては、消費者の能動的な行動によること

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

能動的な行為とは、消費者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、スライダーをスライドする、などのユーザーインターフェイスが考えられる

これらの行為を行う画面と、表示が別れてしまうと、消費者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

同意をする対象条件は、同一画面に出すのが望ましい

3.6.8.1 消費者がどの立場で、誰に対して同意しようとしているのかを、分かりやすい形で明示的に表示する

表示量を少なくすることで、情報取得主体者が不明瞭になることがある

情報銀行スマホ・アプリのサービス提案画面に表示

株式会社

提供済み

アンケート

好きな番組情報を教えてください

ベネフィット

今年の冬オススメ情報のご案内と100円相当進呈（請求額より差引／モニターP付与）

提供するマイデータ

性別

男性

取得目的

好きな番組ジャンルとどのようなことに関心があるかを把握し、コンテンツ開発に活用いたします。頂いた情報は、のみで利用し、第三者には提供しません。

過去事例

「好きな番組を教えてください」の情報取得主体者は誰か？

提供するマイデータとは、情報取得主体者が提供する記載になっているが、実際には情報銀行から情報取得主体者に提供される個人データであり、提供主体者は情報銀行

このサービス提案画面は、本人に語り掛けているのは
情報取得主体者なのか
情報銀行なのか
不明瞭

3.6.8.2 消費者がどの立場で、誰に対して同意しようとしているのかを、分かりやすい形で明示的に表示する

表示量を少なくすることで、情報取得主体者が不明瞭になることがある

カーライフアンケートに
答えると
**もれなく
進呈!**



私は
カーシェア。

私は
マイカー。

あなたはマイカー派？カーシェア派？

クルマは所有するもの。そんな価値観も変わりつつあるようです。あなたはクルマをどのように利用していますか？
カーライフについての簡単なアンケートにご協力ください。
本アンケートに参加いただくと、もれなく30ポイントプレゼントいたします。

オファー期間 2019年10月23日～2019年12月8日

データ提供先企業

リワード ポイント

- ポイントとは、データ提供日から14日間は付与予定ポイント、その後獲得ポイントとして付与されます。

提供するマイデータ

- カーライフについての調査内容
- 登録基本情報（名前、住所、性別、生年月日、メールアドレス、携帯電話番号）

データ利用目的

- クルマの利用状況を分析し、サービス向上や商品・コンテンツ開発のヒントを得るため。
- 投稿された内容を個人を特定しない形で 内のコンテンツとして活用するため。

データ利用期間 2019年10月23日～2020年12月31日

データ提供オファーの詳細

本データ提供オファー（以下「オファー」）にご参加いただく前に、本ページに記載の内容、ならびに本規約をよくお読みいただき、内容に同意いただいた上でご参加ください。

データ提供オファー規約

参加方法

本規約に同意の上、下記「参加する」ボタンから必要事項をご記入の上、オファー期間中にご参加ください。

※本データ提供オファーに参加しない内容の表示やお問い合わせ窓口は2週間です。質問を返すことはできませんのでご注意ください。

アンケート募集事業者が不明瞭

このキャンペーンで「アンケート」募集しているのは、情報銀行／提供先事業者か不明瞭

情報銀行が「アンケート」を募集しているのであれば、アンケートの回答は、事後であっても情報銀行の個人情報の取得履歴で検索できなければならない（情報銀行が取得したことが明示されなければならない）

提供先事業者が「アンケート」を募集しているのであれば、アンケートの回答は情報銀行が取得してはならない

本文に記載の「データ提供先企業」の明示があるが、アンケート主体者が誰であるか不明瞭

左記本文のデータ利用目的は、誰の利用目的ですか？情報銀行の利用目的か／提供先の利用目的か不明瞭

提供先の個人データの利用目的を明示する必要がある

このキャンペーンの主体者（個人情報の取得者）を明確に認識できるような工夫が必要

過去事例

同意の独立性

表示した項目に関する同意は、他と独立した行為を通じて取得する

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係る同意を紛らせて同意を取得しようとする攻撃は十分想定しうる
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

同意内容の事後的参照

消費者が同意した内容に希望時に参照できるように、任意の時に参照できるような適切な手段で消費者に通知する

この際に使う手段は、消費者が、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

経済産業省「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」

Article 7 Conditions for consent 第7条 同意の要件

4. 同意が自由に与えられたか否かを判断する場合、特に、サービスの提供を含め、当該契約の履行に必要な個人データの取扱いの同意を契約の履行の条件としているか否かについて、最大限の考慮が払われなければならない

GDPR は、同意が求められる個人データの取扱いが直接的又は間接的に契約に関する反対給付になりえないことを確保している個人データの適法な取扱いの二つの法的根拠、すなわち、**同意と契約は融合させて曖昧にできるものでもない**

3.6.10 過剰紐づけへのリスク対策

データの最小化の原則（「情報銀行」認定申請ガイドブック）

個人情報の取扱いにあたっては、必要最小限の項目をもって利用目的を達成し、利用目的を超えた意味情報（行動の観測、プロファイリング情報等）の抽出を行わないこと

目的を超えた紐づけ、事務に必要な情報との紐づけが行われないよう、どのような対策を講じるか

個人情報が増え集約・使用されてしまうと、対象者について、業務に必要な範囲を超えて情報を得ることができ、人のプライバシーを不正に暴いてしまう恐れがある

個人情報が、使用目的を超えて取り扱われないよう、また、業務に必要な情報と併せて取り扱われないよう、合理的な対策が講じられるか、システムと人の操作の両面から検討

システム間ではさまざまな接続／連携がなされており、適切な制御をしなければ、別々のシステムで保有されている個人情報全てを紐づけ・参照等することもできてしまう

特に、さまざまな事務で共通基盤として用いられているようなシステムでは、一つの事務に必要な情報以外のさまざまな範囲の情報を保有することが考えられる

共通システムではない個別システムであっても、過剰紐づけ・参照等のリスクがある

システム上で適切な制御がなされていても、運用者がさまざまな権限を悪用して、業務と無関係な個人情報を手動で集めてしまうリスクもある

以上のリスクを防止するためのリスク対策を検討

3.6.10.1 過剰紐づけの事例

プロファイリングの結果、既知の個人情報から要配慮個人情報など本人の望まない個人情報が推測され過剰紐づけされた事例

米国のスーパーマーケットTarget社

「無香料性ローション・特定サプリメント・大きめのバック」の購買履歴等から妊娠している可能性が高いと推測した顧客に、ベビー服等のオファーを提供した。ティーンエイジャーの娘に対して、一緒に住む彼女の父親が妊娠の事実を知る前に、妊娠に関連する広告が送られてきてしまった。

（出典：山本龍彦「ビッグデータ社会とプロファイリング」（『論究ジュリスト』2016年夏号所収））

Facebookの「いいね！」を用いた研究

ある研究では、Facebookの「いいね！」の履歴と他の情報を組合せることで、男性利用者の性的指向の88%、利用者の民族的素性の95%、利用者がキリスト教徒かイスラム教徒かの82%を正確に予測することができた。また民主党支持か共和党支持かの85%、アルコール・ドラッグ・煙草を使用しているかの65～75%を正確に推測することができた。

（出典：Federal Trade Commission（FTC）「Big Data: A Tool for Inclusion or Exclusion?」（2016年1月））

出典 水町雅子「パーソナルデータを巡る現状の問題点」平成25年10月
<http://www.kantei.go.jp/jp/singi/it2/pd/dai3/siryou6.pdf>

3.7 リスク対応

リスク低減

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。

リスクの保有

リスクのレベルがリスク基準を満たしている場合は、追加の管理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

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。

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。

3.8 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

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。

セキュリティリスクと違いプライバシーリスクは本人のリスクであるため、事業者の判断で残留リスクとして保有することはできず、常に改善の対象となる。

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

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