参考資料１７－２

総務省　情報流通行政局　デジタル企業行動室　御中

令和２年度
情報信託機能の普及促進に向けた
課題解決に係る調査

報告書

（抜粋版）

2021 年 3 月 31 日

大日本印刷株式会社

目次

第1章　はじめに

政府では、令和元年 6 月 21 日に閣議決定された「成長戦略フォローアップ」のもと、パーソナルデータの第三者提供を可能にする「情報銀行」について認定を加速させることが掲げられており、データ主導社会の実現に向け、強力に取り組んでいくこととされている。特に、パーソナルデータの適切な利活用推進の観点から、平成 29 年 3 月に開催された「データ流通環境整備検討会」では、PDS や情報銀行の意義・有効性やデータ流通環境整備の必要性等が採り上げられ、官民連携で社会実装に向けて積極的な取組みを推進する必要があるとの提言があった。

これを受け同年 7 月、総務省情報通信審議会において情報信託機能についての議論が行われ、その後、総務省及び経済産業省が開催する「情報信託機能の認定スキームに関する検討会」において、任意の認定スキームについて検討を重ね、平成 30 年 6 月に「情報信託機能の認定に係る指針 Ver1.0」が策定された。

また、総務省では、平成 30 年度に具体的なユースケースの実証を通じて認定スキームの検証を行い、令和元年度には、情報信託機能を活用したサービス等の提供にあたっての運用上の課題等の抽出、解決策の検討及びモデルケースの創出を行った。

一方、平成 30 年度から令和元年度にかけて総務省及び経済産業省が開催した検討会では、要配慮個人情報の情報銀行における活用については、引き続き展開を注視していくこととされ、また、令和元年 10 月に公表された検討会のとりまとめにおいては、情報銀行間の連携、データ倫理審査会の構成員に対する人材育成が今後の課題とされた。

したがって本調査事業では、情報信託機能の普及促進のため、総務省及び経済産業省によって執り行われた検討会で取り纏められた内容を踏まえ、以下 3 テーマについて調査を実施することでユースケースの実証および検証による課題抽出等を図り、報告書として纏めるものとする。

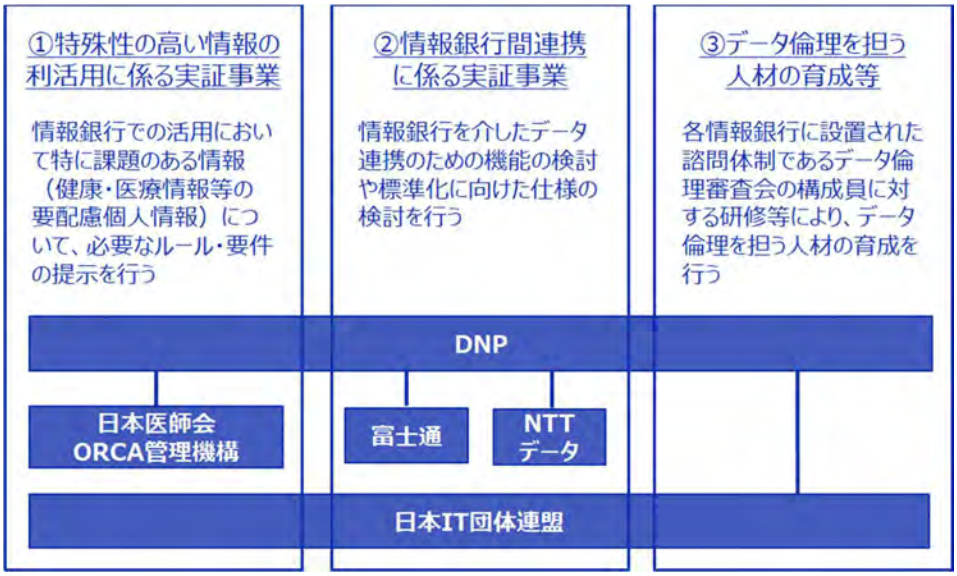


図 1　調査概要・実施体制

第2章 特殊性の高い情報の利活用に係る実証事業

第3章 情報銀行間連携に係る実証事業

3.1. 背景・目的

2019 年度に実施された「戦略的イノベーション創造プログラム（SIP）第 2 期／ビッグデータ・AI を活用したサイバー空間基盤技術」において、図 3-1 のような情報銀行間連携における主な課題が提起された。そして現在、情報銀行サービスを提供する事業者が既に複数立ち上がっている。

これら状況を踏まえると、情報銀行間連携時における特定の情報銀行プラットフォームに依存しないオープンな共通仕様の策定が急務になっていた。そのため、消費者が複数の情報銀行を通じてパーソナルデータをより多くのデータ提供先事業者に流通させ、それにより便益を得る機会が増すエコシステムの形成に必要な情報銀行間連携を実現すべく、その共通仕様について検討した。

戦略的イノベーション創造プログラム（SIP）第 2 期で提起された情報銀行間連携における主な課題

① 消費者が複数の情報銀行サービスを利用する際の「認証方式」
② 情報銀行間のデータ連携時における「データ形式」
③ 情報銀行サービスの提供に関わる事業者に求められるデータ連携時に必要な「機能・ルール」

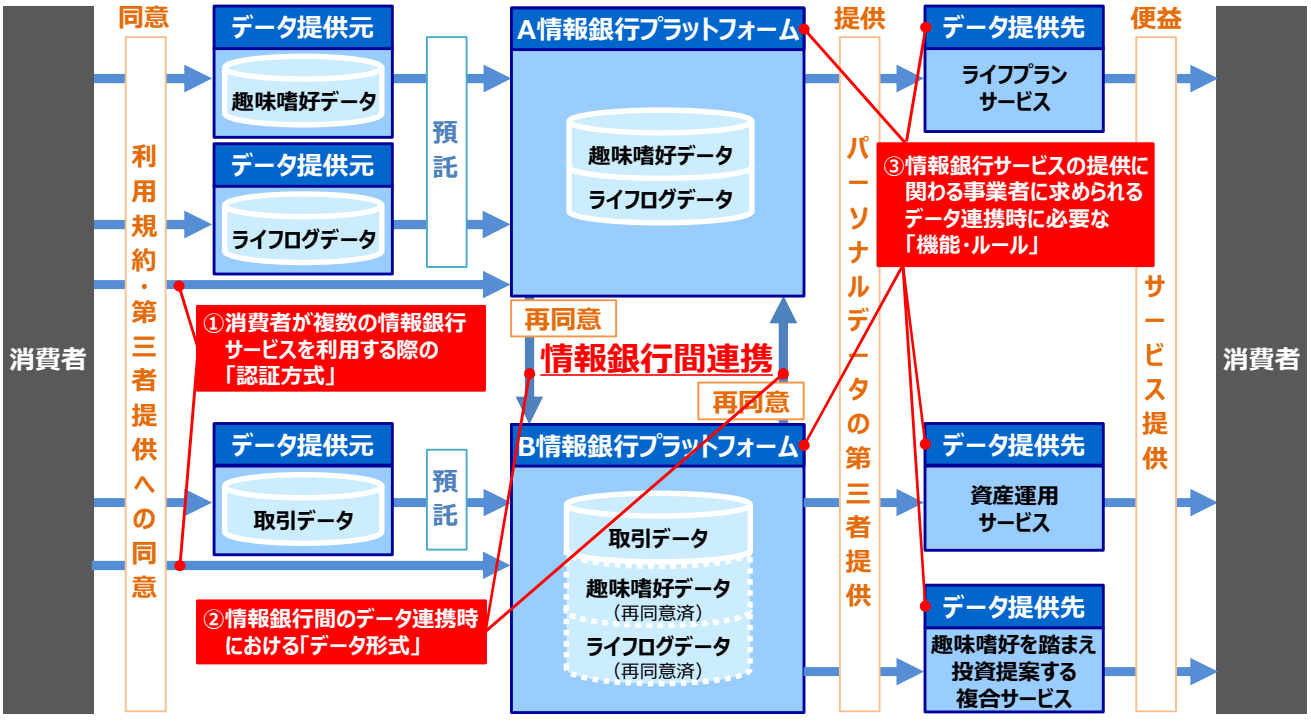


図 3-1 情報銀行間連携モデルのイメージと主な課題との対応

3.2. 実施概要

消費者が複数の情報銀行を利用する際の利便性向上や便益を得る機会の増加を主な狙いとした「認証方式」「データ形式」といった共通仕様の策定、及び消費者にとって安心感があるデータ流通の実現に必要な「機能・ルール」の規定に取り組んだ。

また、共通仕様となる「認証方式」と「データ形式」を検討する際、特定の情報銀行プラットフォームに依存しないオープンな情報銀行間連携仕様にするため、一般社団法人日本 IT 団体連盟の情報銀行認定を取得済かつ本実証事業の趣旨に賛同頂けた情報銀行サービス事業者にオブザーバーとしてアンケート調査にご協力頂き、見識を備えた事業者の意見をより多く取り入れるようにした。

3.2.1. 検討方針

課題を踏まえた情報銀行間連携時における共通仕様（認証仕様、データ定義）、及び必要な「機能・ルール」に関する検討方針は、以下の通りである。

表 3-1 課題を踏まえた検討方針

課題	検討方針	対応する節
① 消費者が、複数の情報銀行サービスを利用する際の**「認証方式」**	認証はセキュリティに関わる要素のため、**利便性だけではなく、セキュリティとの両立**を目指した「認証方式」を検討する。 具体的には、消費者が複数の情報銀行サービスを利用する際に、**必要以上に認証を繰り返すことなくサービスを利用できる方式**、かつ**必要十分なセキュリティ強度の認証方法を提供できる方式**を検討し、情報銀行間で連携する際の認証仕様を策定する。	3.3.
② 情報銀行間のデータ連携時における**「データ形式」**	異なる情報銀行事業者間でデータ連携することを踏まえ、**データフォーマットの標準化だけではなく、データが持つ信頼性や秘匿性といった情報の質的側面も考慮**した「データ形式」を検討する。 具体的には、消費者が多くの事業者に対して情報登録等の対応を個別にすることなく、より多くのサービスを利用できる環境を整備するために、事業者間でデータ連携する際の**標準化フォーマット**を定義する。また、**連携されるデータが持つ情報の信頼性や秘匿性の度合いを連携先事業者でも把握できるようにする方策**についても検討し、情報銀行間における連携データの定義に反映する。	3.4.
③ 情報銀行サービスの提供に関わる事業者に求められるデータ連携時に必要な**「機能・ルール」**	データ流通の普及・促進を妨げる要因の一つになっている消費者不安を低減するため、**消費者によるコントローラビリティの確保**、及び消費者が**安心してパーソナルデータを預託できる信頼性の高い事業者として認識されるため**に必要な「機能・ルール」を検討する。検討は、消費者本人が**パーソナルデータに関する利活用状況の把握や制御**するために必要な機能・ルールの観点で行い、サービス提供に関わる各事業者の役割を意識して整理する。	3.5.

3.2.2. オブザーバーの意見を取り入れた共通仕様検討の進め方

本実証事業では、見識を備えた事業者の意見をより多く取り入れるべく、情報銀行認定を取得済かつ本実証事業の趣旨に賛同頂けた情報銀行サービス事業者にオブザーバーとしてご協力頂きつつ、共通仕様の検討を進めた。

オブザーバーへの意見収集は 2 回実施しており、共通仕様検討前の第 1 回目では「共通仕様検討時における観点・考慮点」、ドラフト版共通仕様作成後の第 2 回目では「検討したドラフト版共通仕様に対する改善点・要望」の観点でアンケート調査を実施した。

第 1 回目の「共通仕様検討時における観点・考慮点」に関するオブザーバーからの意見を踏まえ、ドラフト版の共通仕様を作成した。また、作成したドラフト版の共通仕様をオブザーバーに開示した上で、第 2 回目の「検討したドラフト版の共通仕様に対する改善点・要望」に関する意見を踏まえ、仕様をブラッシュアップしつつ、今後に向けた改善点・要望について整理するといった進め方で共通仕様を策定した。

なお、オブザーバーとしてご協力頂いた具体的な事業者や意見については、本書の「3.6.情報銀行間連携仕様に関するアンケート調査」をご参照頂きたい。

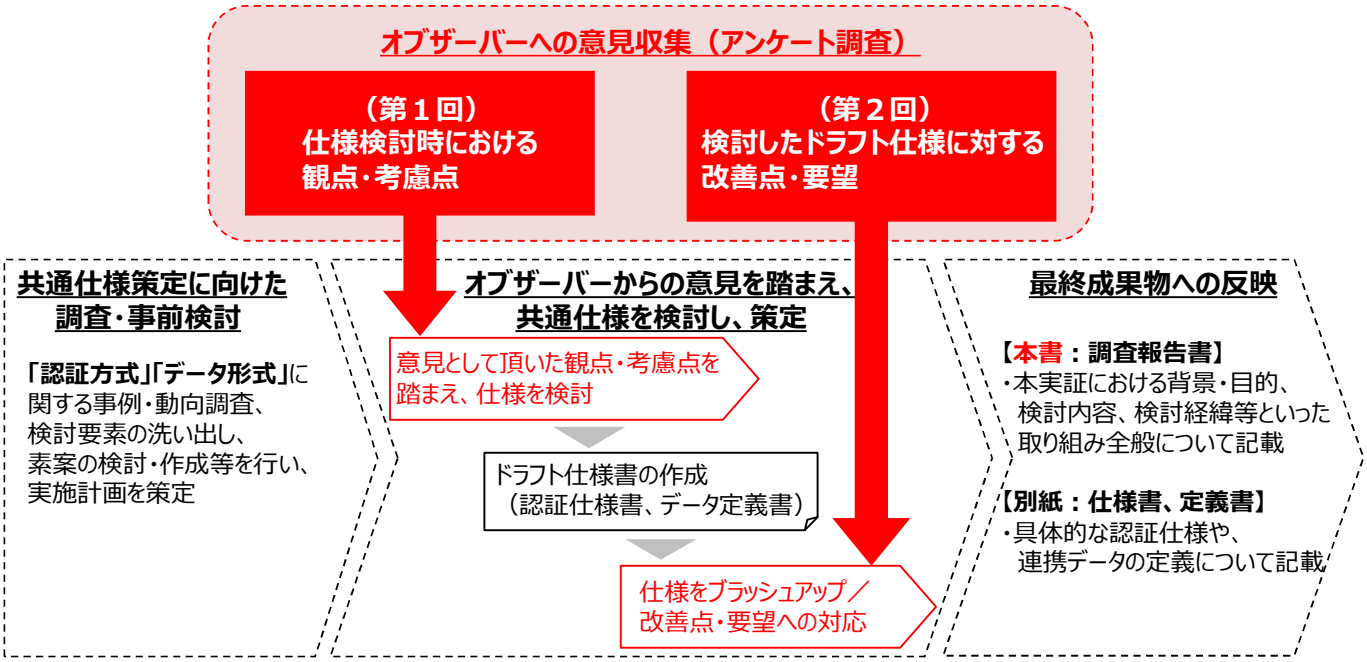


図 3-2 オブザーバーの意見を取り入れた検討の進め方

3.2.3. 策定した情報銀行間連携仕様に関する資料構成

本書では、本実証事業における背景・目的、検討内容、検討経緯等といった取り組み内容全般について記載しており、検討結果となる具体的な情報銀行間連携時における共通仕様は別紙としている。そのため、情報銀行システムの開発等を行う際に、具体的な情報銀行間連携時における認証仕様や連携データの定義を確認したい場合は別紙をご参照頂きたい。

なお、別紙は、情報銀行間で連携する際の認証仕様を定めた「認証仕様編」と、連携するデータを定義した「データ定義編」の２つに大別され、各編には概要説明書が各々付属している。別紙を参照される際はこれらを最初にご一読頂きたい。

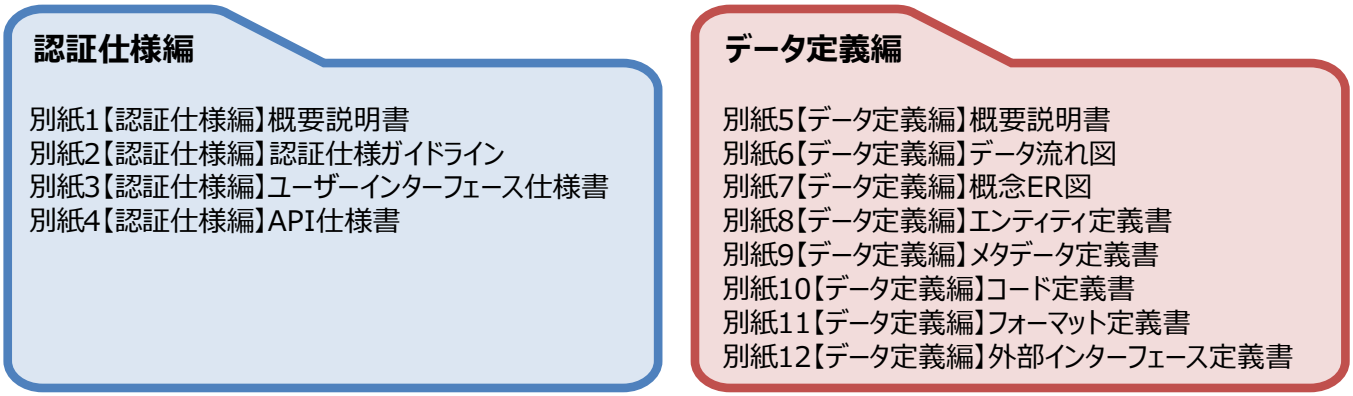


図 3-3 別紙の資料構成

3.3. 消費者が複数の情報銀行サービスを利用する際の「認証方式」

消費者が複数の情報銀行を利用する際の認証に関するユーザビリティの向上と、セキュリティの確保を両立させる「認証方式」について検討した。（図 3-4 参照）

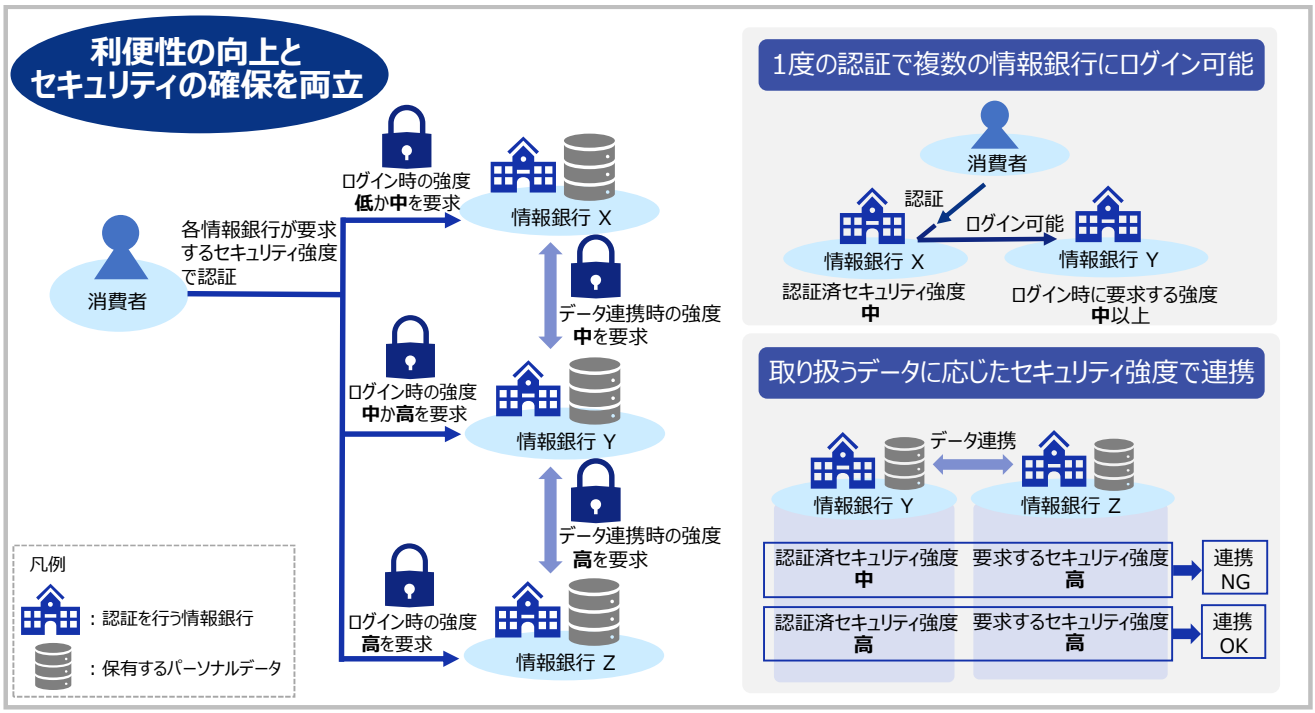


図 3-4 情報銀行間連携における認証方式の検討ポイント

本実証事業で検討した「情報銀行間連携における認証方式」に関する概要を以下に示す（表 3-2 参照）。

表 3-2 情報銀行間連携における認証方式の検討項目

No	実施項目	検討内容・方法	検討結果・成果物
1	情報銀行間連携に適した認証方式	• 複数の標準的な 4 種類の認証方式を、消費者の利便性、セキュリティ、情報銀行の負荷という 3 つの観点で比較評価 • 更に、評価点が高かった 2 案について、実現性、経済性、将来性の観点で追加評価し、情報銀行間連携に適した方式を選定	• 連携し合う情報銀行が、互いの情報銀行 ID を用いた認証を可能にする OIDC 認証方式となるコミュニティ型（ソーシャルログイン方式）を採用
2	情報銀行間連携における考慮すべき特有の仕様	• 情報銀行間連携における ID 連携やデータ連携について、必要となる同意の種別をユースケースから抽出して整理	• ユースケースを基に認証に関連する同意をサービスの利用規約に関する同意、ID 連携に関する同意、第三者提供に関する同意、の 3 つに整理

No	実施項目	検討内容・方法	検討結果・成果物
3	認証仕様への Financial-grade API（FAPI）採用	• 認証方式に、セキュアな仕様である Financial-grade API（FAPI）を採用する妥当性について評価	• FAPI が適していると判断し、採用 • 但し、取り扱うデータの秘匿性を踏まえた上で、連携し合う情報銀行間で合意することを前提に、情報銀行間連携の運用について OIDC による ID 連携と、OAuth によるデータ連携で開始することを許容
4	連携時における認証セキュリティ強度の制御	• 認証に関する国際標準とされている NIST Special Publication 800-63B（NIST SP 800-63B）を基に、認証仕様を具体化	• ID 連携時において、情報銀行が対応する認証レベルと要求する認証レベルにより、連携可否を判断する仕様 • データ連携において、取り扱うデータの秘匿レベルと認証レベルの組み合わせによって、連携可否を判断する仕様
5	ユーザーインターフェース仕様の策定	• 情報銀行間連携時における認証関連のユーザーインターフェース仕様を検討し、ドラフト版を作成 • 更に、ドラフト版に対応したモックアップを作成し、実機によるユーザビリティ検証を行うことで、ユーザーインターフェース仕様をブラッシュアップ	• 各要件に対する要求レベルを整理したユーザーインターフェース仕様 （別紙 3【認証仕様編】ユーザーインターフェース仕様書参照） • 消費者の混乱・誤操作等を防止するための対策を反映
6	API 仕様の策定	• 認証時やデータ連携時に情報銀行が担う役割を整理した上で、API 仕様を具体化 • データ連携時に情報銀行が利用する、OpenID Connect（OIDC）の RP, OP, RS の役割毎に API 仕様を検討	• 情報銀行間連携時における認証関連の API 仕様 （別紙 4【認証仕様編】API 仕様書参照）

3.3.1. 情報銀行間連携に適した認証方式

情報銀行間でデータを連携するにはデータを保有する情報銀行への認証が必要となり、かつ第三者にデータを提供する際には消費者から同意を得る必要もある。しかしながら、消費者にとって情報銀行間のデータ連携の度に各情報銀行への認証と同意を求められることは煩雑であり、ユーザビリティが低下する可能性が高い。

また、認証方式を検討するという点においてはユーザビリティの低下を避けようとするあまりに認証のセキュリティ強度を下げ過ぎないようすべきことや、認証機能を提供する情報銀行の開発コストや運用費といった負担に配慮すべきことも考慮する必要がある。

そのため、「消費者の利便性」、「セキュリティ」、及び「情報銀行への負荷」の 3 つの観点から、最適と思われる認証方式を検討した。

3.3.1.1. 認証方式の比較検討

以下の標準的な認証方式（4 案）について、「消費者の利便性」、「セキュリティ」、及び「情報銀行への負荷」の観点で比較検討した。

- 案 1:認証基盤で認証、共通 ID を利用（OIDC）
- 案 2:情報銀行が認証、情報銀行の ID を利用（OIDC）
- 案 3:認証基盤で認証、共通 ID を利用（SAML）
- 案 4:情報銀行が認証、情報銀行の ID を利用（スクレイピング）

表 3-3 認証方式の比較検討（4 案）

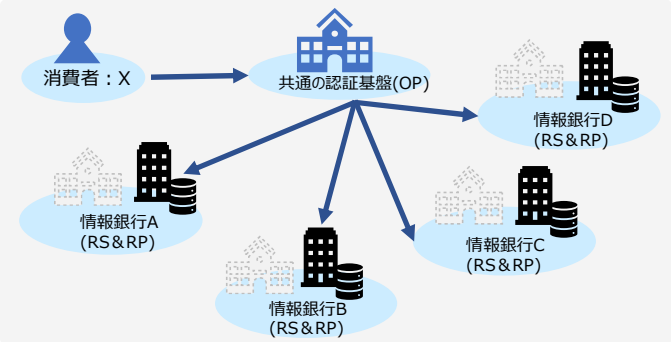
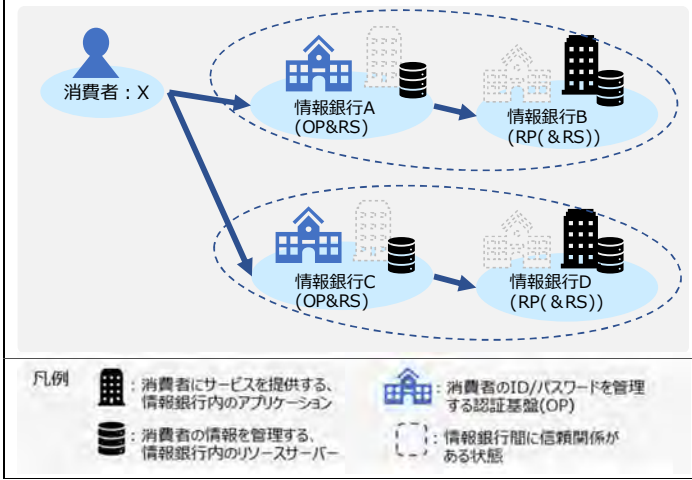
案:認証方式	評価	消費者の利便性	セキュリティ	情報銀行への負荷
案 1: 認証基盤で認証、共通 ID を利用（OIDC）	結果	○	○	△
	評価内容	・共通 ID によるシングルサインオンができる。（常に同じ ID/パスワードでログイン可能）	・OIDC によりセキュアな認証方式を提供できる。 ・データの特性に応じて、認証画面のセキュリティ強度を変更できる。	・利用する認証基盤に対応した開発・運用が必要になる。（RP、RS） ・情報銀行が OP を作成する必要がない。
案 2: 情報銀行が認証、情報銀行の ID を利用（OIDC）	結果	○	○	△
	評価内容	・データ連携先の ID でログインでき、データ連携ごとの認証を省略することができる。	・OIDC によりセキュアな認証方式を提供できる。 ・データの特性に応じて、認証画面のセキュリティ強度を変更できる。	・認証基盤を利用するため、開発・運用が必要になる。（OP、RP、RS）
案 3: 認証基盤で認証、共通 ID を利用（SAML）	結果	○	△	×
	評価内容	・組織で統一した ID を利用し、常に同じ ID/パスワードでログインできる。	・認証基盤が全情報銀行の ID を管理する必要がある。	・SAML による認証を利用するため、開発・運用が必要になる。（SAML の SP）

案:認証方式	評価	消費者の利便性	セキュリティ	情報銀行への負荷
			・データの特性に応じて、認証画面のセキュリティ強度を変更できない。	・すべての情報銀行の ID/パスワードを認証基盤にフェデレーションする必要がある。
案 4: 情報銀行が認証、情報銀行の ID を利用 （スクレイピング）	結果	×	×	△
	評価内容	・データ連携する情報銀行ごとに ID/パスワードを登録する必要がある。	・情報銀行に他の情報銀行の ID とパスワードを保管しなければならない。	・他の情報銀行の ID を登録する画面を作成し、ID/パスワード管理する負荷がある。

4 案の比較検討から、案 1 と案 2 は、セキュアな仕組みの構築が可能であり、データの特性に応じたセキュリティ強度の変更にも対応可能であると判断できた。よって、認証方式には、案 1 または案 2 の採用を基本方針とした。

次に、認証方式に選出した 2 案を情報銀行間連携に適用した場合の構成について検討した。

表 3-4 認証方式の適用検討

案 1 中央集権型（シングルサインオン方式）の ID 管理 	共通の認証基盤の ID/パスワードを入力して、複数の情報銀行のアプリケーションにログインする仕組み。データ連携する全ての情報銀行のログイン（認証）を省略できる。 左の図では、認証基盤の共通 ID/パスワードを使用することで、情報銀行 A、B、C、D のログインを省略できる。
案 2 コミュニティ型（ソーシャルログイン方式）の ID 管理 	他の情報銀行（OP）が提供する ID/パスワードを入力して、情報銀行のアプリケーションにログインする仕組み。データ連携するために信頼関係を結んだ他の情報銀行のアカウントを利用してログインするため、データ連携元と連携先の情報銀行へのログインが 1 回にできる。 左の図では、情報銀行 A の ID/パスワードを入力して、情報銀行 B にログインできる。（情報銀行 C、D の信頼関係は、A、B の信頼関係と同様。なお、情報銀行 A、C の間には信頼関係はないため、ソーシャルログインはできない）

更に、認証方式の案 1 と案 2 について、実現性、経済性、将来性の点で比較評価した。

表 3-5 認証方式の比較評価（2 案）

案:認証方式	評価	実現性	経済性	将来性
案 1: 認証基盤で認証、共通 ID を利用 （OIDC）	結果	×	△	○
	評価内容	早期実現（例えば来年度からのサービス化など）は難しい。共通の認証基盤構築、運営組織の設立には、リソースと期間を要する。また、認証基盤を担う組織には公共性が求められる可能性もあり、制度面での整備も必要となる。	共通の認証基盤を構築する必要はあるが、各情報銀行は OP を作成する必要がない。	情報銀行数に依存しない構成のため、将来、情報銀行数が増加したときには、理想的な構成になり得る。
案 2: 情報銀行が認証、情報銀行の ID を利用 (OIDC)	結果	○	×	△
	評価内容	情報銀行数が少ない段階では、各情報銀行が OP を作成することで、早期実現しやすい。	各情報銀行が、個別に OP を作成する必要があるため、連携する情報銀行が増える度に追加対応が必要になる。	案 1 と同じ OIDC の仕様を採用しているため、将来、案 1 へ移行（※）できる可能性が高い。但し、移行時に各情報銀行の個別 ID への対応などを検討する必要がある。

※:案 2 から案 1 への移行イメージ

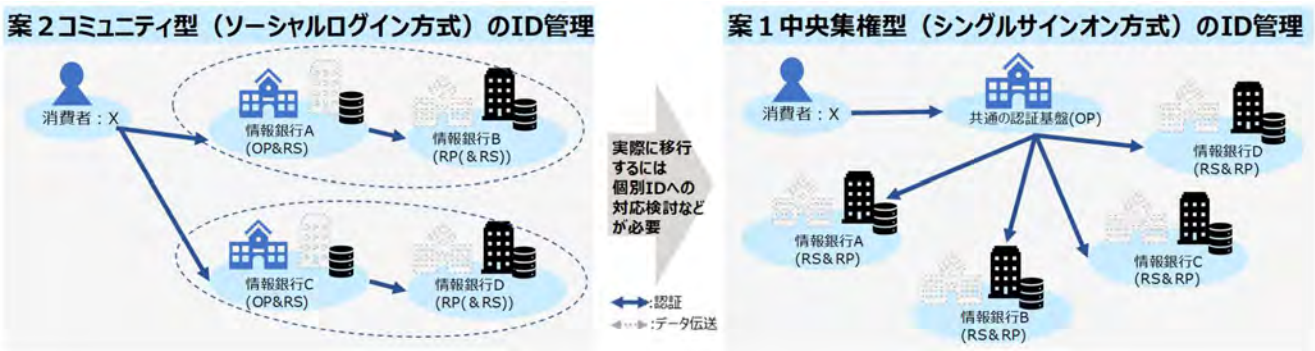


図 3-5 案 2 から案 1 への移行イメージ

3.3.1.2. 結論

案 1 は経済性や将来的の面で選択肢になり得るが、認証を共通の認証基盤に委ねる方式になるため、信頼性と安全性を兼ね備えた共通の認証基盤の実現及び運営組織の設立が前提となることから、早期実現は難しい。

一方、案 2 は多くの情報銀行が連携し合う状況では経済性の面で案 1 に劣るが、早期に実現しやすいという点や将来的に案 1 への移行も可能な点を踏まえて今年度に検討する方式として妥当と評価した。

そのため、案 2 のコミュニティ型（ソーシャルログイン方式:連携し合う情報銀行が、互いの情報銀行 ID を用いた認証を可能にする OIDC 認証方式）を採用した。

3.3.2. 情報銀行間連携における考慮すべき特有の仕様

情報銀行を利用する際にはサービスの利用規約などについて消費者から同意を得る必要がある。また、情報銀行が保有するデータはその多くがパーソナルデータであり、第三者への提供時にはデータを所有する消費者の同意が必要になる。これは情報銀行間の連携時においても考慮すべき仕様となる。

よって、情報銀行間連携に伴う ID 連携時とデータ連携時の 2 つのタイミングについて、必要になる消費者からの同意とその際の同意内容を整理して処理フローに組み入れた。

3.3.2.1. ID 連携のユースケース抽出

情報銀行間連携における ID 連携のユースケースを抽出した上で、各ユースケースで必要となる消費者への同意の種類を洗い出した。

表 3-6 ID 連携のユースケースに関する情報銀行の状態パターン整理

ユースケース	情報銀行の状態		説明
	ID 連携元情報銀行（情報銀行 B）	ID 連携先情報銀行（情報銀行 A）	
新規登録	ID 登録済み	ID 未登録済み	ID 連携元情報銀行で ID が登録済で、ID 連携先情報銀行で新規登録する場合
初回 ID 連携	ID 登録済み	ID 登録済み	ID 連携元情報銀行、ID 連携先情報銀行双方の ID が登録済で、双方の情報銀行の既存 ID を ID 連携により紐づけする場合
ログイン	ID 連携済み		双方の情報銀行が ID 連携済みの状態にて、ログインする場合

表 3-7 ID 連携のユースケースと同意の関係

ユースケース	ユースケースでの流れ	同意の有無
新規登録	①情報銀行 A のアカウント新規登録（情報銀行 B のアカウントで新規登録）を開始	
	②情報銀行 A の**利用規約への同意**	○
	③情報銀行 B のセッションなしなら、情報銀行 B の認証 情報銀行 B のセッションありなら④へ	

ユースケース	ユースケースでの流れ	同意の有無
	④情報銀行 B の **ID 連携に関する同意**	○
	⑤情報銀行 A のアカウント新規作成完了	
初回 ID 連携	①情報銀行 A と情報銀行 B との ID 紐づけを開始	
	②情報銀行 B のセッションなしなら、情報銀行 B の認証 情報銀行 B のセッションありなら③へ	
	③情報銀行 B の **ID 連携に関する同意**	○
	④情報銀行 A と情報銀行 B との ID 紐づけ完了	
ログイン	①情報銀行 B の ID で情報銀行 A にログインを開始	
	②情報銀行 B のセッションなしなら、情報銀行 B の認証 情報銀行 B のセッションありなら③へ	
	③情報銀行 B の ID 連携の確認	
	④情報銀行 B の ID で情報銀行 A にログイン完了	

3.3.2.2. **データ連携のユースケース抽出**

情報銀行間連携におけるデータ連携のユースケースを抽出した上で、各ユースケースで必要となる消費者への同意の種類を洗い出した。

表 3-8 データ連携のユースケースに関する情報銀行の状態パターン整理

ユースケース		情報銀行の状態		説明
		情報銀行 A	情報銀行 B	
データ連携	データ取得	データ取得側	データ提供側	情報銀行 A が情報銀行 B からデータを取得する場合
	データ提供	データ提供側	データ取得側	情報銀行 A が情報銀行 B にデータを提供する場合
データ連携の停止		データ取得側（取得済み）	データ提供側	情報銀行 A が、情報銀行 B のデータを取得している状態で、情報銀行とのデータ連携を停止する場合
		データ提供側	データ取得側（取得済み）	情報銀行 A が、情報銀行 B にデータを提供している状態で、情報銀行とのデータ連携を停止する場合
		データ取得側、かつ、データ提供	データ提供側	情報銀行 A が、情報銀行 B から取得したデータを、別の情報銀行（例 情報銀行 C）に提供している状態で、情報銀行とのデータ連携を停止する場合

表 3-9 データ連携でのユースケースと同意の関係

ユースケース	ユースケースでの流れ	同意の有無
データの取得	①情報銀行 A が情報銀行 B からのデータ取得を開始	
	②情報銀行 B のセッションなしなら、情報銀行 B の認証（認証レベル別） 情報銀行 B のセッションありなら③へ	
	③情報銀行 B での**第三者提供に関する同意**	○
	④情報銀行 A が情報銀行 B とのデータ連携完了	
データの提供	①情報銀行 B が情報銀行 A からデータ提供を開始	
	②情報銀行 A のセッションなしなら、情報銀行 A の認証（認証レベル別） 情報銀行 A のセッションありなら③へ	
	③情報銀行 A での**第三者提供に関する同意**	○
	④情報銀行 B が情報銀行 A からデータ提供完了	
データ連携の停止	①データ連携停止を開始	
	②データ連携停止完了	

3.3.2.3. 情報銀行間連携の認証での同意

ユースケース抽出とその処理の検討結果から、情報銀行間連携の認証での同意は、以下と定義した。

表 3-10 情報銀行間連携の認証における同意の種類

同意のカテゴリ	同意の種類	図 3-6 との対応
利用規約に関する同意	消費者が情報銀行を利用する際に提示され、情報銀行サービスの利用規約や利用目的などについて消費者が行う同意。	①
	データ連携先情報銀行（RP）がパーソナルデータを特定の目的で利用することについて、消費者が行う同意。	④
ID 連携に関する同意	消費者が ID 連携によるログインを選択した際に、ID 連携元情報銀行（OP）から ID 連携先情報銀行（RP）に ID が提供されることについて、消費者が行う同意。（消費者が ID 連携を選択済みのため、提供する情報の通知である。）	②
第三者提供に関する同意	データ連携元情報銀行からデータ連携先情報銀行にパーソナルデータを提供することについて、消費者が行う同意。	③
	データ連携先情報銀行がパーソナルデータを再提供することについて、消費者が行う同意。	⑤

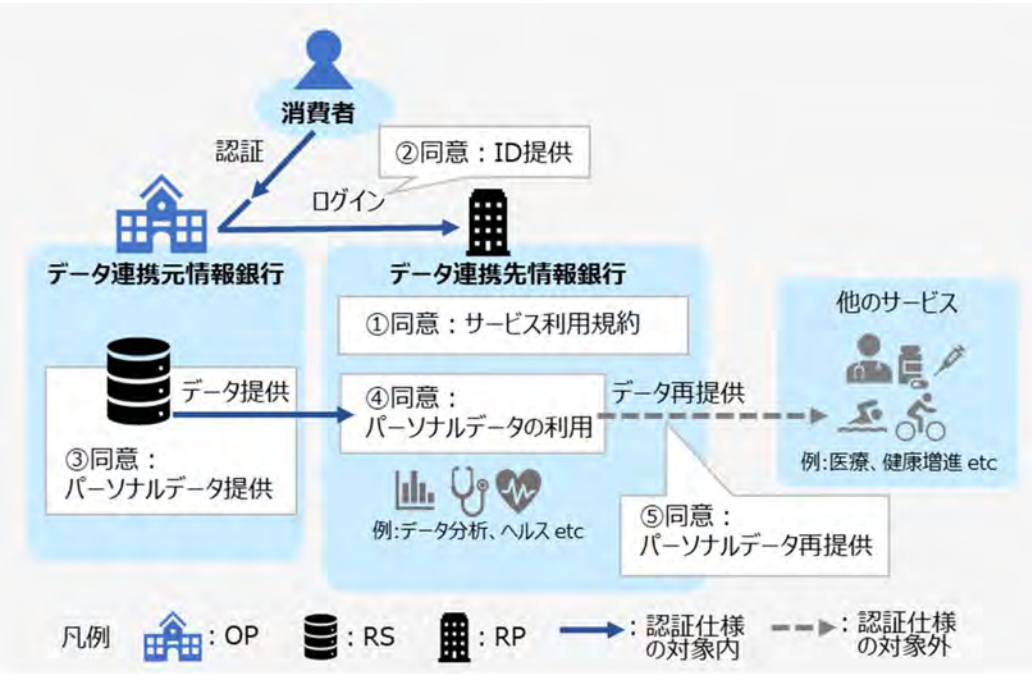


図 3-6 同意の種類

「同意した」と判断する行為について

消費者から得る同意について、消費者に何をどのように画面上で通知し、それに対して消費者がどのような操作をしたかによって「同意が得られた」と判断するかを検討した。

情報銀行が消費者から同意を得る場合、消費者による明確な同意の操作が必要であり、「消費者が操作をしなかった」ことを「同意した」と判断することがないよう認証仕様に記載した。

例えば、「第三者提供に同意しない場合は、チェックボックスにチェックを入れてください。」という表示を出し、消費者がチェックボックスにチェックしなかったとき、「同意しないという操作をしなかった」ことを「同意した」と見做すことはできず、「第三者提供に同意する場合は、チェックボックスにチェックを入れて下さい。」という表示を出し、消費者がチェックボックスにチェックすることではじめて「同意した」と見做すことができる、とした。

3.3.3. 認証仕様への Financial-grade API（FAPI）採用

現在、企業間の情報連携において HTTP による API が多く利用されている。その連携においてセキュアに認可を実施する仕様としては OAuth 2.0 が多く利用されている。OIDC は、OAuth 2.0 の拡張仕様である。近年、この OAuth 2.0 及び OIDC を基に、更にセキュリティを強化した FAPI の利用が国際的に活性化してきている。

3.3.3.1. 情報銀行間連携の認証仕様に求められる要件

情報銀行間連携の認証仕様に求められる要件には以下がある。

- 資本関係を結んでいない企業間の認証連携には、公平な国際標準のプロトコルの採用が必要である。
  情報銀行においても、国際標準のプロトコルを採用し、公平性を保つこと、かつ、グローバル化に対応できることは重要である。
- 情報銀行では、パーソナルデータを取り扱うことから、高いセキュリティ強度が求められるため、ハイグレードなセキュリティ対策が必要である。

3.3.3.2. FAPI の採用理由

要件を踏まえて情報銀行間連携における認証仕様を検討した結果、以下の理由で FAPI を採用した。

- OIDC は、認証連携での知名度が高く、インターネットにおけるデータ連携の標準規格であり、公平性が高い。
  FAPI は、その OIDC を基にして、OpenID Foundation が金融業界向けに策定した仕様であり、世界的なオープンバンキングで利用されている。
- 一般的な OAuth や OIDC では、トークンを盗まれるとそれを利用されてしまう恐れがあった。
  FAPI の Advanced Security Profile ではクライアント証明書による相互認証と、クライアント証明書へのトークンのバインドを必須にしてこれを防ぐなど、セキュリティを大幅に強化している。

高いセキュリティ強度を求めると、それに伴い開発コストは高くなるが、標準化された FAPI を適用し、データ連携だけではなく ID 連携についても FAPI をベースとした仕様に統一し、一般的なフローである Authorization code flow を採用することによって、コストを抑えつつ品質的にも十分な実装が可能になるのではないかと考えた。

3.3.3.3. 結論

FAPI は国内外を問わず金融関連での実績が豊富で、情報銀行間連携の認証仕様に求められる要件にも適合する。今後、情報銀行は秘匿性の高いデータを取り扱うことが予想されるため、高いセキュリティ要件に応えられる必要があり、FAPI の採用が妥当と考える。

なお、現行の各情報銀行の状況を考慮し、取り扱うデータの秘匿性を踏まえた上で、連携し合う情報銀行間で合意することを前提に、準備期間として、情報銀行間連携の運用を OIDC による ID 連携と OAuth によるデータ連携で開始することを認める。

3.3.4. 連携時における認証セキュリティ強度の制御

データの重要度、秘匿性は、各情報銀行によって、また、データの内容によっても異なる。そのため、情報銀行間で連携する際の認証では、連携する情報銀行や扱うデータの重要度等に応じて、複数のセキュリティ強度を設定し、使い分けるべきである。

このような背景から、情報銀行間連携におけるセキュリティ強度の制御について検討した。

3.3.4.1. 検討内容・方法

調査

認証におけるセキュリティ強度の考え方について、認証に関するガイドラインとして国際標準とされている NIST SP 800-63B を基に調査した。

NIST SP 800-63B は、米国国立標準技術研究所（NIST）の認証に関するガイドライン:NIST SP 800-63-3 の一部であり、Authenticator Assurance Level（AAL）として、登録済みアカウントのログイン時の認証プロセスへの強度が述べられている。情報銀行間連携の認証レベルには、NIST SP 800-63B の AAL のレベルを使用した。

検討

セキュリティ強度の要件や、扱うデータの秘匿性は情報銀行ごとに異なる。また、情報銀行内でも、扱うデータによって秘匿性が異なる。

ID 連携及びデータ連携について、以下の条件を可能にして、かつ、情報銀行間で連携できる制御を検討した。

- 情報銀行ごとに認証を設定できること
- データの秘匿性に応じてレベルを設定できること
- 連携において、各情報銀行に大きな負担とならない仕組みにすること

3.3.4.2. ID 連携の制御

ID 連携の認証には、ログインする際のセキュリティ強度を示す、「NIST SP 800-63B」の「Authenticator Assurance Level」である AAL を認証レベルとして用いることとした。

- 認証レベル 1:例 ID とパスワードを用いた認証
- 認証レベル 2:例 2 段階認証（認証レベル 1 の認証後、追加でワンタイムパスワードを用いた認証を実施）
- 認証レベル 3:例 2 段階認証（認証レベル 1 の認証後、追加で暗号デバイスを用いた認証を実施）

認証レベルを用いた制御を検討した結果、以下を比較することで、ID 連携の可否を判定する仕様とした。

- ID 連携元情報銀行の提供可能な認証方式の認証レベル
- ID 連携先情報銀行が要求する認証レベル

本実証事業における認証仕様では、認証レベル 1 と 2 の 2 種類の認証レベルを想定して検討を進めた。その場合の ID 連携での制御の例を以下に示す。

表 3-11 ID 連携時の制御の例

① ID 連携元情報銀行が提供する認証方式の認証レベル	②ID 連携先情報銀行が ID 連携元情報銀行に求める認証方式の認証レベル	ID 連携の可否（①≧②で連携可）
認証レベル=1	要求する認証レベル=1	○連携可
認証レベル=1	要求する認証レベル=2	×連携不可
認証レベル=2	要求する認証レベル=1	○連携可
認証レベル=2	要求する認証レベル=2	○連携可
認証レベル=1、2	要求する認証レベル=1	○連携可
認証レベル=1、2	要求する認証レベル=2	○連携可（※）

※ID 連携元情報銀行（①）が認証レベル＝2 の認証をしたときのみ連携できる。

上の例では、ID 連携先情報銀行が求めている認証レベル「2」の認証方式を、ID 連携元情報銀行が提供していない（ID 連携元情報銀行が提供しているのは、認証レベル「1」のみである）ため、連携ができない状態となる。

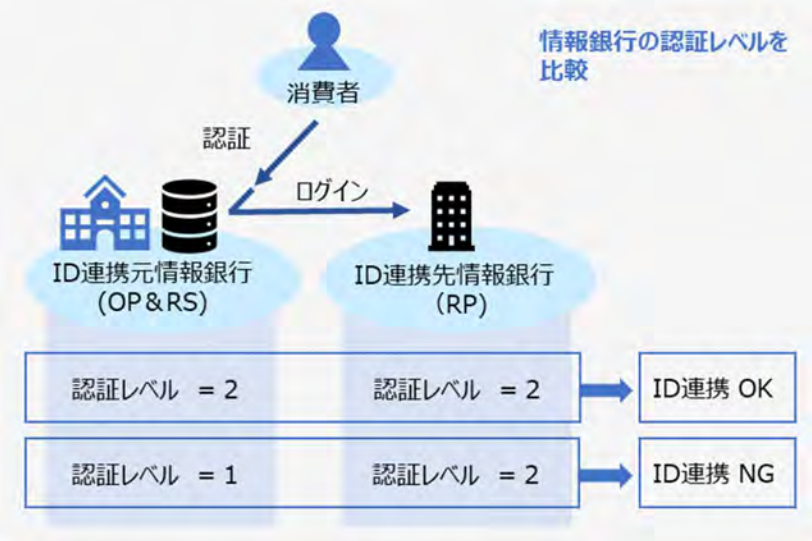


図 3-7 ID 連携の可否判断の例

3.3.4.3. データ連携の制御

データ連携の認証では、情報銀行間で連携するパーソナルデータの秘匿性が反映される制御を検討した。それぞれのデータの秘匿性を「秘匿レベル」として数値化した。

また、秘匿レベルは、認可プロトコル OAuth 2.0 の「スコープ」単位で設定する仕様とした。スコープは、アクセス権の範囲を定義するものであり、データ連携元情報銀行の扱うサービスやデータなど、業務の単位で任意に設定される。

データを保有するデータ連携元情報銀行では、データの秘匿レベルに対応する認証レベルの認証方式を用意する。セッションの認証レベルによっては、データ連携のために追加の認証が必要になる場合がある。

「データ連携元情報銀行の現在のセッションの認証方式の認証レベル」と「データ連携先情報銀行が要求する認証レベル」を比較することで、データ連携の可否を判定する。

表 3-12 データ連携時の制御の例

データ連携元情報銀行の要求データの秘匿レベル	① データ連携元情報銀行のセッションの認証レベル	② データ連携先情報銀行がデータ連携元情報銀行に求める認証方式の認証レベル	データ連携の可否（①≧②で連携可）
秘匿レベル＝1	認証レベル=1	要求する認証レベル=1	○連携可
秘匿レベル＝2	認証レベル=1	要求する認証レベル=2	×連携不可（※）
秘匿レベル＝1	認証レベル=2	要求する認証レベル=1	○連携可
秘匿レベル＝2	認証レベル=2	要求する認証レベル=2	○連携可

※ID 連携元情報銀行にて、認証レベル 2 の追加認証を行うことで、連携が可能となる。

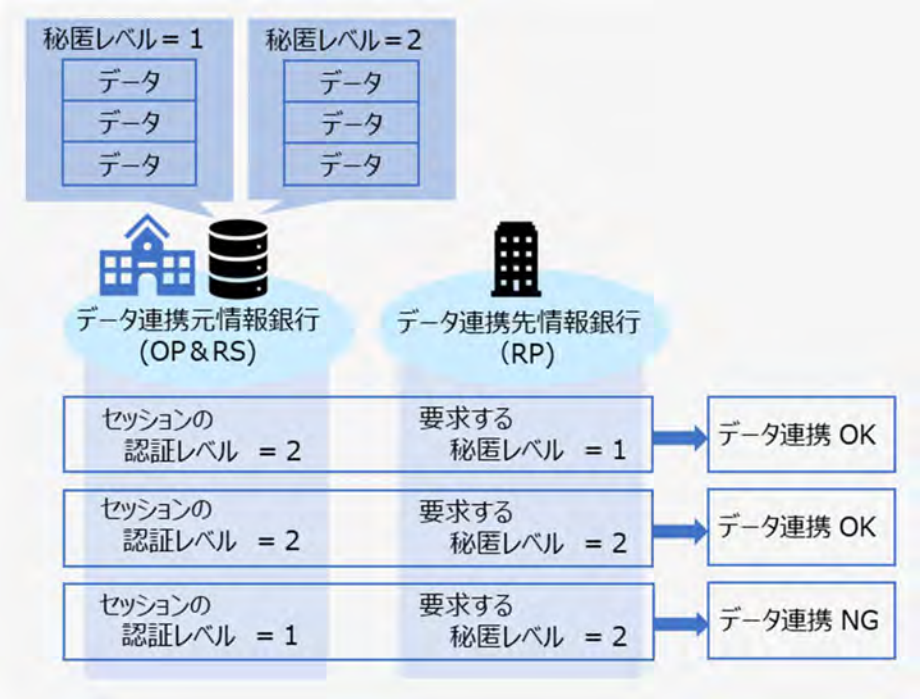


図 3-8 データ連携の可否判断の例

3.3.4.4. 結論

各情報銀行単位に認証レベルを設定し、データ属性単位に秘匿レベルを設定した。これらのレベルの組み合わせ単位に制御することで、情報銀行間で合意しやすいデータのやりとりが可能となる。これにより、各情報銀行に大きな負担とならない仕組みを実現することができた。

3.3.5. ユーザーインターフェース仕様の策定

ID 連携およびデータ連携におけるユーザーインターフェースの仕様について検討した。

3.3.5.1. 検討理由

情報銀行間で連携する場合、消費者は連携する情報銀行の数に応じた認証をすることになる。そのため前項までの検討において、ソーシャルログイン方式を採用して 1 つの情報銀行が他の情報銀行の認証を担うことで、消費者の認証の回数を減らすことを提案した。ソーシャルログイン方式では、連携元と連携先の画面が交互に切り替わりながら消費者に認証や同意の操作を求めることになる。そのため、消費者が混乱しないようなユーザーインターフェースを提供する必要がある。

3.3.5.2. 検討内容

消費者の混乱を招く可能性がある懸念事項を洗い出し、その対策を実施した。

消費者の混乱を招く可能性がある懸念事項

情報銀行間連携を行う際に生じうる懸念事項として以下を挙げた。

- 既に認証済みの場合は、認証時のパスワード入力画面などがスキップされるため、それにより混乱する可能性がある。
- 今、どちらの情報銀行の画面を表示しているのかが分からなくなり、混乱する可能性がある。
- 今、どの情報銀行の ID でログインしているかを把握できずに、混乱する可能性がある。
- 今、どの情報銀行の認証で担保されているかを把握できずに、混乱する可能性がある。
- 今、どの程度のセキュリティ強度で認証しているのかを把握できずに、混乱する可能性がある。
- どの情報銀行から、どの情報銀行へパーソナルデータを連携しようとしているのか分からなくなり、混乱する混乱する可能性がある。

求められるユーザーインターフェース

ボタンを押すなどの操作をする際に消費者が混乱しないように、操作前に現在どのような状態にあり、何をする操作なのかが分かる画面表示をする。また、一目で理解や把握ができるように必要な情報は 1 画面で表示する。

施策

以下のような項目などを挙げ、ユーザーインターフェース仕様書の該当画面に説明を記載した。

記載例

- 「どこの情報銀行の何を許諾したのか」を消費者が誤解しないよう、操作前後の画面に説明を表示する。
- 用語や表示内容を統一する。
- 認証画面の場合、「認証」という用語を表示する。
- 2 段階認証の画面の場合、2 段階認証が求められていることを消費者が明確に認識できるように、「2 段階認証」をタイトル行に入れる。

また、以下の推奨事項等を定めることで、視覚的なわかりやすさの向上を試みた。

- 消費者が承諾する内容を誤解させない表示
- 現在のログイン済み情報銀行の表示（アイコンなど）
- 認証レベルの表示（今の自分の認証レベル）
- データ連携のデータの流れる方向の表示（アイコンなどでの「情報銀行 A→情報銀行 B」）

3.3.5.3. 結論

消費者の混乱を招く可能性のある操作について、画面に説明を表示するなどの対策を実施した。これにより、消費者の混乱・誤操作を防止することが期待できる。また、今後の更なる改善として、全体プロセスのうち、現在どのステップまで進んでいるかなど、現在の状況を把握できるようなユーザーインターフェースにするなども考えられる。こうした継続的なユーザーインターフェースの改善を通じて消費者のユーザビリティ向上に努める必要がある。

3.3.6. API 仕様の策定

情報銀行間連携の認証仕様のための API について、FAPI の仕様を開発する各情報銀行の負担を軽減しつつ、高いセキュリティ強度を保持できるような仕様を検討し、API 仕様を策定した。

3.3.6.1. 検討内容

API の仕様を決定するにあたり、以下の事項を調査・検討した。

- API 仕様の基となる FAPI プロトコルの要求事項は、OIDC プロトコルのどの要求事項が選定されているかを確認し、整理した。
- API のセキュリティを強化するために適用されるリクエストヘッダ・レスポンスヘッダについて、公的機関の情報を調査し、検討した。

3.3.6.2. 検討結果

- API 基盤上で実現可能なパターンを試みた結果、FAPI プロトコルの要求事項内で、現時点で、実装に向けた開発技術の難易度が低く、頻繁に利用されるパターン「Authorization code flow」を選択した。
- 独立行政法人 情報処理推進機構（IPA）により Web アプリケーションで推奨されているリクエストヘッダ・レスポンスヘッダを付加した。（IPA は、日本の IT 国家戦略を技術面・人材面から支えるために設立された独立行政法人であり、国内の IT 情報実施機関として最も信頼される団体である。）また、Web アプリケーションで推奨されているリクエストヘッダ・レスポンスヘッダを付加したことでセキュリティが担保できているかについて、脆弱性に関する Web 検証ツールを用いて検証し、問題ないことを確認した。
- FAPI は、高いセキュリティ強度を保持し、グローバルでの適用もあるが、クライアント証明書を要するクライアント認証などは、証明書の管理などの課題もまだ残されている。そのため、取り扱うデータの秘匿性を考慮（すべて

秘匿レベル 1 など）した上で、連携し合う情報銀行間で合意すれば、情報銀行間連携の運用を OIDC による ID 連携と OAuth によるデータ連携で開始することを認める仕様とした。

調査・検討の結果、認証仕様として以下の API の仕様を策定した。

表 3-13　API の一覧

API 名	説明	RP	OP	RS
認可リクエスト	認証・認可を要求する API	利用	提供	—
認可レスポンス	認可リクエストの結果を受け取る API	提供	利用	—
トークンリクエスト（発行）	トークンを発行する API	利用	提供	—
リソースアクセス	RS のデータにアクセスする API	利用	Token Introspection を提供	提供
トークンリクエスト（再発行）	トークンを再発行する API	利用	提供	—
トークン無効化	発行したトークンを無効化する API	利用	提供	—
OpenID Provider Configuration Document	OpenID プロバイダーについての情報	利用	提供	—
JWKS	ID トークンの署名検証に必要な公開鍵情報を JSON 形式で返す API	利用	提供	—
Token Introspection	アクセストークンに関する情報を返す API	—	提供	利用
同意状況取得	RP に対する同意一覧を返す API	利用	提供	—
同意取り消し	RP に対する同意を取り消す API	利用	提供	—

考察

情報銀行間連携の認証仕様における API の標準仕様を提供したことで、情報銀行の API 開発への負担が軽減されることを期待するが、本仕様は認証認可が中心となっており、今後もリソースアクセス用の API 仕様なども順次拡張していくことで、より高い負担軽減効果が期待できる。

3.3.7. 認証方式に関する今後の課題と対応

情報銀行間連携における認証方式ついて、今後の更なる普及、促進に必要と思われる検討・取り組みとして下記が挙げられる。

高い認証レベルに対応した認証方法の導入・推進

昨今、企業間連携において本人確認の脆弱性に起因した問題が発生したこともあり、今後は本人確認・本人認証の確からしさがより重要になる。そのため、生体認証や暗号デバイスを用いた認証等といった高い認証レベルに対応した認証方法を消費者に提供することが求められる。機器コスト、機器の本人への確実な送付など、導入における課題もあるが、パソコンやスマートフォンなど消費者本人が保有する端末を活用する方法も可能なため、今後の普及に期待したい。

データ連携元情報銀行からデータ連携を強制的に打ち切れる手段の仕様化

本仕様では、消費者からのデータ連携の取り消し要求は、サービスを提供するデータ連携先情報銀行で受け付ける前提になっている。基本的にはこの仕様で問題ないが、消費者に不利益を与えるような不適切なデータ連携先情報銀行であることが事後的に判明した場合等に、消費者がデータ連携元情報銀行にデータ連携の取り消し要求をすることで、強制的にデータ連携を打ち切れる手段についても仕様化すべきではないかと考える。今後、その必要性自体も含めて検討する必要がある。

ユーザビリティ向上のための更なる仕様改善

情報銀行間連携時に、複数の情報銀行の画面切り替えが連続して発生すると、消費者は自分が今、どの情報銀行に対して、何の操作しているのかが分からなくなってしまう可能性が高い。そのため、情報銀行間連携における全体プロセスをステップ表示した上で、現在はどのステップにあるかなどについて、言語的にではなく、視覚的に把握できるようにアイコンを用いたり、ハイライトしたり、といった工夫が必要になる。このようなユーザビリティ向上のための更なる仕様改善が今後も必要と考える。

開発の効率や品質を高める開発プロセスや成果物の標準化

本実証事業では、情報銀行間連携における認証仕様を策定したが、加えて、開発の効率や品質を高めるため、開発プロセスや成果物に関する開発標準を整備する必要がある。例えば、テスト手法を標準化したり、開発ツールを整備したり、開発チュートリアルや開発ガイドラインを作成したり、といったことが求められる。こうした開発全体を標準化する取り組みを行うことが、本実証事業で策定した認証仕様の普及、促進にも繋がると考える。

3.4. 情報銀行間のデータ連携時における「データ形式」

「情報銀行間のデータ連携時のデータ形式」として、特定プラットフォームに依存しない連携データの在り方を検討し、同一・類似分野だけでなく、異分野間においてもデータ流通可能な連携データモデル、データ形式等について、共通仕様を検討した（図 3-9 参照）。

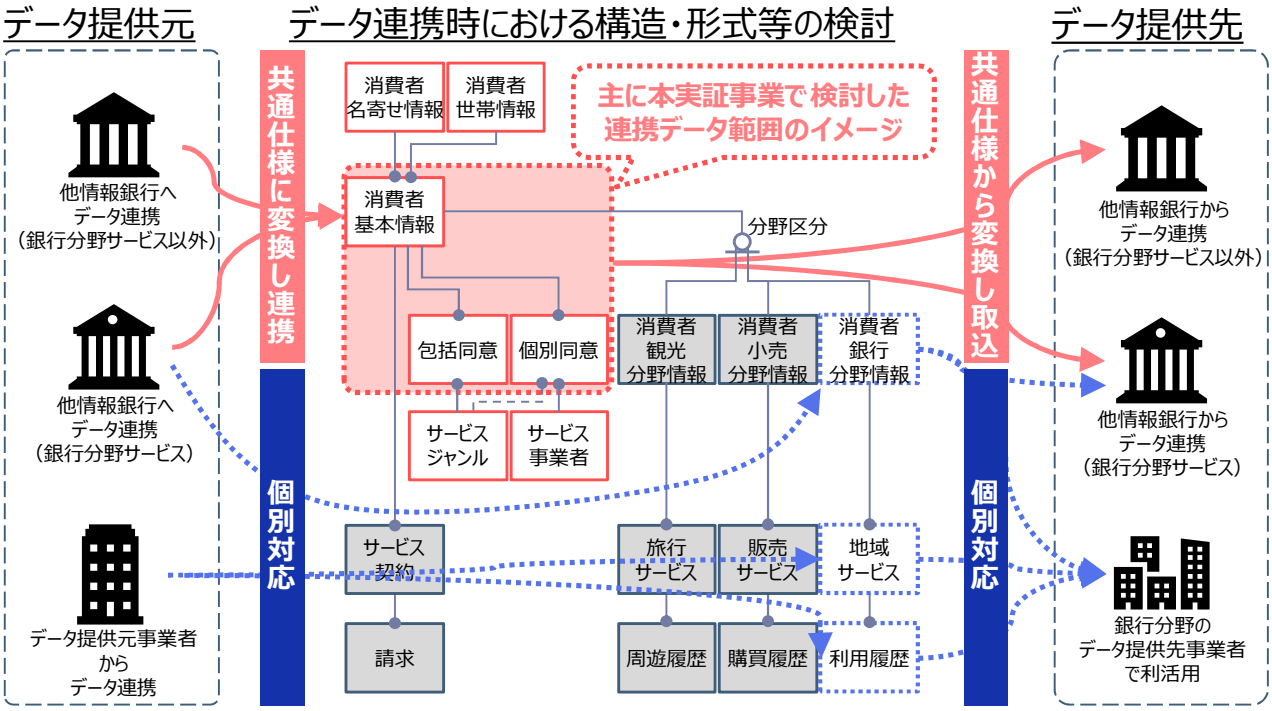


図 3-9 データ連携時における構造・形式等の検討イメージ

本実証事業で検討した「情報銀行間のデータ連携時におけるデータ形式」の概要を以下に示す（表 3-14 参照）。

表 3-14 共通仕様概要

No	実施項目	検討内容・方法	検討結果・成果物
1	データ項目の定義・名称標準化	• 基本情報、同意管理情報、履歴情報について、データ項目の定義・名称標準化を実施 • 基本情報のデータ項目定義にあたっては、業界トップ 17 社やオーストラリア政府により作成された消費者データに関する標準である CDS (Consumer Data Standards)の「Common」のパートを参考に検討	• 情報銀行間データ連携する際の共通データ項目を定義 （別紙 8【データ定義編】エンティティ定義書、別紙 10【データ定義編】コード定義書、別紙 11【データ定義編】フォーマット定義書参照）

2	情報銀行間データ連携に付与するメタデータ	• 情報銀行間データ連携時に付与する「データの説明」と情報銀行が保有しているデータを示す「データカタログ」の 2 種類のメタデータを検討	• メタデータの共通仕様や、各項目の説明や型を定義 （別紙 9【データ定義編】メタデータ定義書参照）
3	基本情報、同意管理情報、履歴情報に関するデータ構造	• データ項目間の関係性を整理分類した上で、データ構造を検討 • また、4 種類の同意（個別同意、包括同意、包括同意と個別同意拒否、包括同意と個別同意）を設定できるように、企業マスタを用意し、個別同意と包括同意を関連付けるデータ構造を検討	• 基本情報、同意管理情報、履歴情報に関するデータ構造を定義 （別紙 7【データ定義編】概念 ER 図参照）
4	伝送時におけるデータフォーマット	• データ連携元、データ連携先におけるフォーマット変換等の負担を削減するため、XML 等の一般的な伝送時におけるデータフォーマットについて調査・評価を実施した上で選定し、具体的な記述方法を検討	• 情報銀行間データ連携する際の JSON 形式を定義 （別紙 12【データ定義編】外部インターフェース定義書参照）
5	情報銀行に求められる匿名加工技術、トレーサビリティ提供に必要な提供履歴データ	• 匿名加工データの活用事例を調査し、情報銀行の介在可能性が考えられる事例を抽出の上、主なユースケースとして、収集データ、活用内容、及び情報銀行に求められる役割や機能、強みについて整理 • また、匿名加工以外のデータ変換・加工技術についても、事例調査の上、情報銀行が介在する場合に想定されるユースケースを整理	• 情報銀行におけるデータ変換・加工に関するユースケースの整理結果
6	データカタログ・履歴の共有方法	• データカタログについて、一般的なデータ共有技術・サービスを比較・評価し、情報銀行間で共有する仕組みの実装方法を検討 • 履歴情報について、消費者に包括的なトレーサビリティを提供するために適した共有の仕組みの実装方法を検討し、3 種類のデータ管理方式を比較評価	• データカタログのデータ共有技術・サービス評価結果 • 履歴情報を共有するデータ管理方式の評価結果

3.4.1. 基本情報、同意管理情報、履歴情報に関するデータ項目の定義、及び名称標準化

情報銀行間でデータ連携するにあたって、連携するデータ項目の定義や名称が情報銀行によってばらばらであると、データ連携先においてデータクレンジングなどの作業が必要となり、相互でのデータ利活用が阻害される要因となると考える。データクレンジングなどの作業なしにデータ連携を行うには、連携データを予め標準化しておく必要がある。

本実証事業においては、連携データのうち、連携頻度が高い氏名、住所等の個人情報の基本情報、データ取得やデータの第三者提供等における消費者からの同意取得に関する同意管理情報、履歴情報を対象とし、データ項目の定義、名称の標準化を実施した。

3.4.1.1. 基本情報の定義における検討内容・方法

まずは、下記の業界のトップ企業 17 社のウェブサイト等の公知情報を確認し、各社が収集している個人情報を調査した。

- 飲料製造業
- 教育、学習支援
- 医療、福祉
- ホテル
- 不動産賃貸・管理業
- 銀行業
- 郵便業
- 通信業
- 電子計算機・同附属装置製造業
- 電気業
- 衣服・その他の繊維製品製造業
- 小売業
- 自動車、自動車車体・附随車製造業
- 情報サービス業
- 農業
- 民生用電気機械器具製造業
- 家具・装備品製造業

調査により得られた個人情報のうち、企業特有の情報（アンケート、パスワード、ログイン ID 等）や、業界特有の情報（出身学校、年収（信用調査）、世帯情報等）を除く、氏名、生年月日、性別、住所、電話番号、メールアドレスを基本情報の項目とした。なお、世帯情報を対象外とした理由は以下の通りである。

- 調査の結果、世帯情報を扱っている企業が少なく 17 企業中 2 企業（ホテル業、不動産賃貸・管理業）のみであった。

- 業界によって適した世帯の定義（住基世帯、扶養関係に基づく税世帯、福祉等の実態世帯など）が異なることから、各業界に適した個別定義を行う必要があり、全業種横断的な共通定義は適さない。

次に、基本情報の項目に対して、CDS（Consumer Data Standards)の「Common」のパートでの定義情報やマイナンバー等の日本のデータ流通仕様や RFC を参考に、基本情報の項目の細分化や定義付けを行った。CDS はオーストラリア政府により消費者データ権法（企業が保有する個人情報へ安全にアクセスする権利を消費者に付与するもの）の導入の一環として開発されたものであり、消費者主権の個人情報流通に適したデータ標準仕様を定めている。

金融業界以外で保有する個人情報も含めたものとなっている点で、本取組である情報銀行間のデータ連携との共通点が多いことから、本実証事業における定義書の参考とした。

CDS を参考にした 1 例として「メールアドレス」をあげると、「Common」において、メールアドレスは用途別に複数保有している。そのため、本定義においてもメールアドレスは用途別に複数保有できるようにし、優先するメールアドレスか否かなども設定できるようにした。本実証事業で定義した基本情報「メールアドレス」の定義例を表 3-15 に示す。

また、日本国内におけるパーソナルデータの流通に適した項目にするため、マイナンバーのデータ流通仕様を参考に定義をカスタマイズした。具体的には、日本人や日本の地域に適した氏名や住所の項目定義、生年月日が正確にわからない人への対応として、“2014 年春生まれ”等の特定の生年月日以外の表現ができる生年月日の項目定義などのカスタマイズをした。

表 3-15 基本情報「メールアドレス」の定義例（別紙 8【データ定義編】エンティティ定義書一部抜粋）

項目分類			項目名	説明
大分類	中分類	小分類		
識別子	-	-	ユーザー識別子	基本個人情報の所有者のユーザー識別子。
識別子	-	-	メールアドレス ID	メールアドレスを一意に識別するキー。
名称	-	-	優先	優先するメールアドレスか表す。 省略時の場合は false とみなす。 ・true:優先する ・false:優先しない
区分	-	-	用途	E メールアドレスの用途を表わす。
名称	メールアドレス	-	メールアドレス	E メールアドレス。フォーマットは RFC 5322 に準拠する。

3.4.1.2. 同意管理情報の定義における検討内容・方法

ある情報銀行を既に使っている消費者が、別の情報銀行を新たに使い始める場合、第三者提供に関する同意の設定を最初からやり直すのは煩雑である。そのため、消費者の負担を軽減する目的で、既に利用している情報銀行から新たに使い始める情報銀行に同意条件も引き継ぎ、初期表示できることが望ましいと考えた。本検討では、この際に連携する同意条件などの同意管理情報について定義した。なお、同意は連携元の情報銀行と消費者の間の同意であるため、連携先の情報銀行で改めて同意の意思表示が必要になる（個人情報保護法 第二十三条）ことを踏ま

えて検討した。例えば、連携した同意条件を連携先の情報銀行で消費者に再提示し、「同意」ボタンを押した時点で初めて有効な同意とするといった前提なども併せて検討した。

情報銀行において消費者より取得する消費者のデータの第三者提供に関する同意は、「情報信託機能の認定に係る指針 ver1.0」（以下、認定指針 ver1.0）における認定の範囲（図 3-10 参照）において、包括同意と個別同意の２種類の同意取得パターンが想定されている。また、消費者の意思表示には、第三者提供を同意する条件を示す場合と、第三者提供を拒否する条件を示す場合の 2 パターンがある。

■ **参考：情報銀行による同意取得のパターンと認定の範囲（指針ver1.0より）**

指針ver1.0では、情報銀行による同意の取り方について、以下のとおり整理し、認定の対象について定義している。

同意取得のパターン	概要	本指針に基づく認定との関係
① 包括的な同意	・事業者が個人情報の第三者提供を本人が同意した一定の範囲において本人の指示等に基づき本人に代わり第三者提供の妥当性を判断するサービス	・認定の対象
②－1 個別的な同意（情報銀行の関与が強い場合）	・提供事業者が情報の提供先を選定して個人に提案する場合など、提供事業者が比較的大きな役割を果たす（責任をもつ）ケース	・情報銀行が比較的大きな役割を果たすため、認定の対象
②－2 個別的な同意（個人の主体性が強い場合）	・純粋なPDSなどデータの管理や提供に関し個人の主体性が強いサービス	・純粋なPDSについては、認定の対象外（情報銀行が付随的なサービスとしてPDS機能を提供することはあり得る）

図 3-10 情報銀行による同意の取り方

(出典:「情報信託機能の認定スキームの在り方に関する検討会 取りまとめ（案）」平成 30 年 4 月)

以上より、次の表 3-16 に示す、個別同意や包括同意を単独で設定する場合の 2 パターンと、包括同意と個別同意を組み合わせて設定する 2 パターン（包括同意と個別同意拒否、包括同意と個別同意）の 4 パターンに整理し、データ項目を定義した。なお、下記 3 つの箇条書きに示した何れの提供形態であっても第三者提供の同意が必要になるという点では同じとなる。加えて同意した条件の中に利用期間の定めがあった場合は、利用期間内においてのみデータ提供できるということにも注意が必要になる。

- 同意したデータ項目について、内容が更新される都度、継続的に同意した第三者にデータ提供する（継続的なデータ提供に関する権限を情報銀行に付与）
- 同意したデータ項目について、同意時点の内容を同意した第三者に一度だけデータ提供する（情報銀行はデータ提供する都度、消費者から同意を得る）
- 同意したデータ項目について、同意時点の内容を同意した第三者はデータの保有はせず参照のみで利用する（第三者の環境にダウンロードすることが出来ない対策・制限あり）

表 3-16 第三者提供に関する同意のパターン

第三者提供同意のパターン	内容
(a)個別同意（特定の企業を個別同意する）	個別同意とは、情報銀行に対して、消費者が指定した事業者にパーソナルデータの提供を同意すること。

(b)包括同意（特定の業界を包括同意する）	包括的同意とは、情報銀行に対して、消費者が指定した条件を満たした事業者にパーソナルデータの提供を同意すること。
(c)包括同意と個別同意拒否（特定の業界で包括同意し、特定の企業を個別同意拒否する）	個別同意拒否とは、情報銀行に対して、消費者が指定した事業者へのパーソナルデータの提供を拒否すること。個別同意されていないことと、個別同意拒否は近しい意味合いになるが、包括同意の条件を満たしていても、特定の企業を拒否したい場合等に個別同意拒否を使うことがある。
(d)包括同意と個別同意(特定の業界で包括同意し、それとは別の特定の企業を個別同意する)	(a)(b)を合わせたもの。

※包括と個別それぞれの同意/同意拒否が存在する場合は、包括よりも個別の方が消費者による意思がより明確に示されていることが想定されるため、個別の同意/同意拒否が優先されることとした

以下の図 3-11 は、データ提供先 A、B のみ個別同意している例で、その二つのみにデータが連携される。

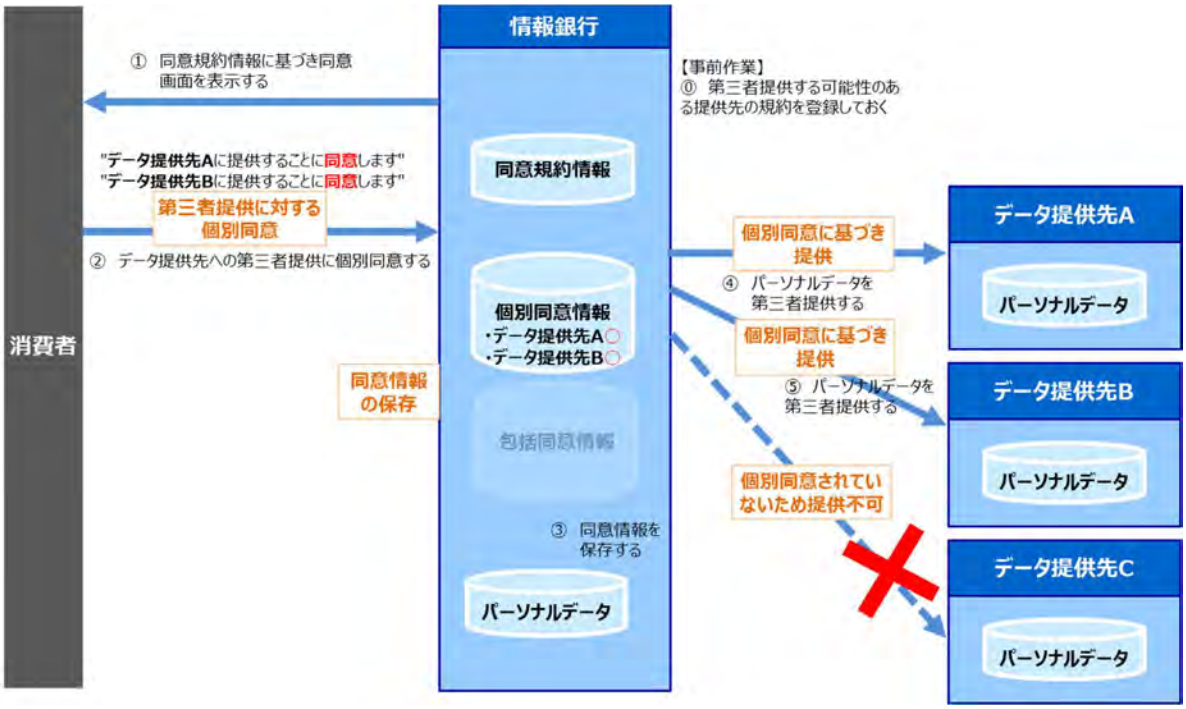


図 3-11 (a)個別同意（特定の企業を個別同意する）イメージ

以下の図 3-12 は、運輸業のみ包括同意している例で、運輸業のデータ提供先 A,B のみにデータが連携される。

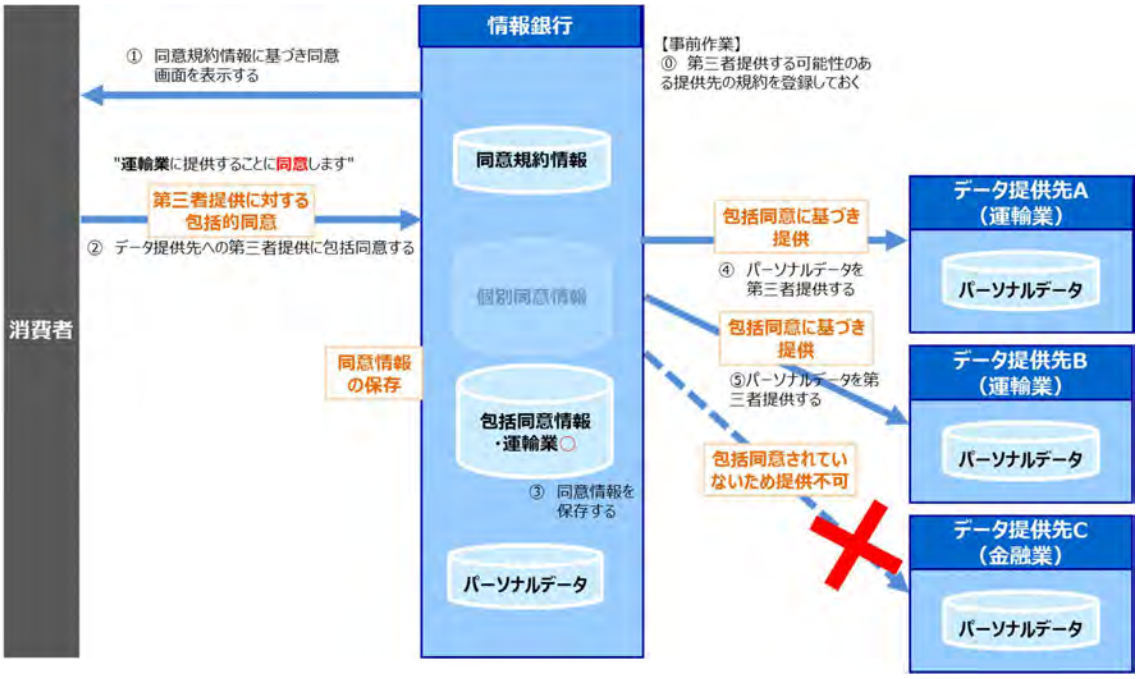


図 3-12 (b)包括同意（特定の業界のみを包括同意する）イメージ

以下の図 3-13 は、運輸業に包括同意しているが、運輸業のデータ提供先 C にはデータ提供個別同意拒否をしているため、データ提供先 A、B のみデータが連携される。

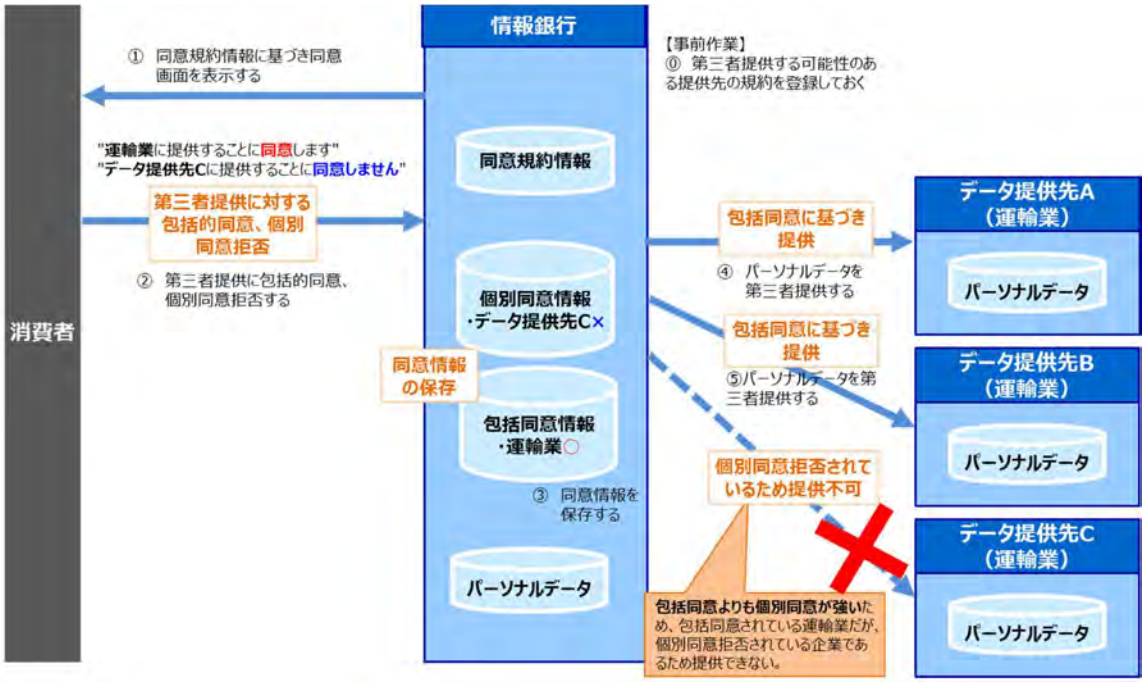


図 3-13 (c)包括同意と個別同意拒否（特定の業界で包括同意し、特定の企業を個別同意拒否しているケース）イメージ

以下の図 3-14 は、運輸業に包括同意しており、金融業のデータ提供先 C にもデータ提供個別同意をしているため、データ提供先 A、B、C にデータが連携される。

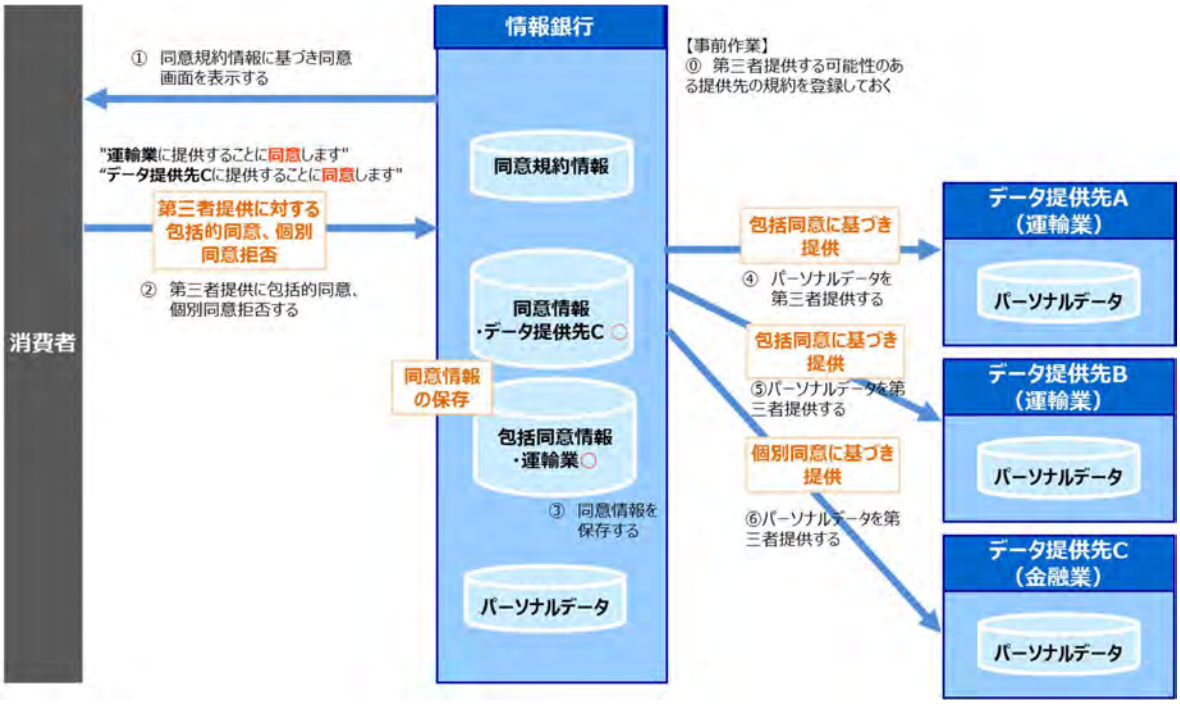


図 3-14 (d)包括同意と個別同意（特定の業界で包括同意し、それとは別の特定の企業を個別同意する）イメージ

同意管理情報には、提供するデータや提供先など、どういった条件に対して消費者より同意を取得したかといった同意条件を含める必要がある。

情報銀行の認定制度に関する指針として公表された「情報信託機能の認定に係る指針 ver2.0」（以下、認定指針 ver2.0）において、情報銀行は、同意条件として提供先・利用目的・データ範囲についての選択肢を消費者に対して用意する必要がある旨記載されている。

そこで、個別同意、包括同意における同意条件として表 3-17 及び表 3-18 のような条件を指定できるように定めた。

表 3-17 個別同意における消費者が選択できる選択肢（同意条件）

提供先	利用目的	データ範囲
具体的な企業名	具体的なサービス、利用目的	具体的なデータ項目（補足情報として、秘匿レベルの最大値）

表 3-18 包括同意における消費者が選択できる選択肢（同意条件）

提供先	利用目的	データ範囲
• 業界別での分類 • 会社規模での分類（従業員数、売上高等の分類） • 民間かそれ以外かでの分類 • 情報セキュリティマネジメントシステム（ISMS）適合性評価制度の認証を受けた事業者やプライバシーマーク付与事業者での分類	• 観光目的、公共目的等の数の少ない分類 • 個別具体的で数の多い分類	• データ項目別の分類（属性データ、購買データ、資産データ等）

条件で指定できる選択肢について、認定指針 ver2.0 では「本人が第三者提供について判断できる情報を提供する必要があり、例えば、『上場企業／その他含む』『観光目的 ／公共目的』のように数の少ない分類方法から、より個別具体的で数の多い分類方法までが考えられる。」と定めており、それらの具体的な分類方法については各情報銀行の裁量に委ねられている。

提供先については、後述の「3.5.2.消費者が同意した利活用目的に必要なデータのみを選択提供・連携する機能・ルール」にて検討したルールに則り、第三者提供時の同意の際の提供先の選択肢を表すためのデータ項目を定義した（表 3-19 参照）。

表 3-19 提供先に関する条件設定のためのマスタとデータ項目定義

マスタ名称	データ項目	データ項目の定義方法
業種分類マスタ	業種 ID（大分類）、業種名（大分類）、業種 ID（中分類）、業種名（中分類）、業種 ID（小分類）、業種名（細分類）	総務省の日本標準産業分類の定義を使用した。
会社規模分類マスタ	会社規模分類 ID、会社規模分類名	会社規模分類は「大企業」、「中小企業」、「小規模企業」に分類した。 大企業は中小企業、小規模企業以外の企業とし、中小企業、小規模企業は、中小企業基本法で規定する定義とした。
民間分類マスタ	民間分類 ID、民間分類名	民間分類は、「民間企業」、「民間企業以外」に分類した。 民間企業とは、公的機関に属さない民間が出資及び経営を行う企業とし、民間企業以外とは、国

		（中央政府）や地方公共団体が保有する企業（公企業）や、行政機関などとした。
認定分類マスタ	認定分類 ID、認定分類名	一般社団法人日本 IT 団体連盟による「情報銀行」の認定事業者、プライバシーマーク又は ISMS 認証取得事業者（「情報銀行」の認定事業者以外）、その他事業者での分類とした。

一方、利用目的、データ範囲は汎用的にすることで各情報銀行の色や提供可能サービスが変わってくるため、本検討ではデータ項目の定義対象からは除外し、提供の際の共通ルールについて定義付けを行い、URL 形式の ID で各情報銀行がマスタ（利用制限マスタ及びスコープマスタ）を作成し、それを参照することで連携できるようにした。

利用制限マスタのデータ項目は表 3-20 のとおり定義した。表 3-20 で ID は、利用制限を一意に識別するために URL の形式としており、特定のアドレスを指す目的の項目ではない。利用制限マスタでは、情報銀行が第三者提供する際に消費者に提示する利用目的に関する条件を表すためのデータ項目を保有している。

表 3-20 利用制限マスタの定義例

No	データ項目		説明
1	利用制限		包括同意、個別同意の利用制限を表す。
2		利用制限 ID	利用制限を一意に識別する ID を表す。 具体的な ID としては情報銀行が自由に決定してよいが、全ての情報銀行間でユニークな形式になるように設定する必要がある。
3		タイトル	利用制限のタイトルを表す。 利用制限を一言で表す内容を記載する。
4		説明文	利用制限を詳細に説明するための文章となる。 利用制限の特徴を第三者へ説明するために必要となる。
5		スコープ	利用制限に含まれるスコープを表す。 スコープマスタと紐づく ID となる。

スコープマスタのデータ項目は表 3-21 のとおり定義した。スコープマスタでは、情報銀行が第三者提供する際に消費者に提示する利用範囲に関する条件を表すためのデータ項目を保有している。

表 3-21 スコープマスタの定義例

No	データ項目		説明
1	スコープ		包括同意、個別同意の許諾するデータ項目と可能な操作の範囲を表す。
2		スコープ ID	基本個人情報・同意情報の提供が可能な項目や操作の範囲を一意に表す URL。 具体的な ID としては情報銀行が自由に決定してよいが、全ての情報銀行間でユニークな形式になるように設定する必要がある。
3		秘匿レベル	秘匿レベルコードを表す

4		タイトル	スコープのタイトルを表す。 スコープを一言で表す内容を記載する。
5		説明	スコープを詳細に説明するための文章となる。 スコープの特徴を第三者へ説明するために必要となる。
6	属性情報		スコープに含まれる、データ項目と操作の集合を表す。 許諾するデータ項目と可能な操作を一意に表す。 情報銀行が自由に決定してよいが、全ての情報銀行間でユニークな形式になるよう設定する必要がある。
7		操作	属性に対する操作を表す。 read:読込 write:書き込み delete:削除
8		属性	属性の名前を表す。 データカタログの基本個人情報属性情報で定義されている属性が設定される。

3.4.1.3. 履歴情報の定義における検討内容・方法

情報銀行間でデータ連携する際、当該データがこれまでどのように流通されてきたかを示す履歴情報（流通履歴）を連携することで、情報銀行は、消費者の求めに応じて、情報銀行間でのデータの流通履歴を一元的に開示することが可能となる。そのため、データが流通された日時、その際の流通元の情報銀行と流通先の情報銀行等、必要となる項目について定義付けを行った。なお、これらの定義は、3.5.5.にて検討した包括的なトレーサビリティ実現に向けた機能・ルールを踏まえたものとなっている。

表 3-22 履歴情報の定義例（別紙 8【データ定義編】エンティティ定義書一部抜粋）

項目分類	項目名	説明
識別子	流通元情報銀行識別子	基本個人情報・同意情報の流通元の情報銀行の識別子を表す。 識別子は、連携元情報銀行における OpenID Connect の Issuer Identifier である。
名称	流通元情報銀行名	基本個人情報・同意情報の流通元の情報銀行の名称を表す。
識別子	流通先情報銀行識別子	基本個人情報・同意情報の流通先の情報銀行の識別子を表す。 識別子は、連携先情報銀行における OpenID Connect の Client ID である。
名称	流通先情報銀行名	基本個人情報・同意情報の流通先の情報銀行の名称を表す。
日付	流通日時	基本個人情報・同意情報が流通された日時を表す。
区分	概要	基本個人情報・同意情報の流通の概要を表す。
区分	目的	基本個人情報・同意情報の流通の目的を表す。

区分	利用状況	流通された基本個人情報・同意情報の利用状況を表す。

また、情報銀行は、消費者との間で、利用規約の締結やパーソナルデータの第三者提供等に関する同意を得ている。これらの同意に関する履歴情報については、どの情報銀行においても保有するものと想定し、消費者が情報銀行に対して行った全ての同意に関する、同意した日時や同意を取った情報銀行の情報等の履歴情報（同意管理履歴）について定義付けを行った。

なお、履歴情報として管理する同意の種類と定義は以下（表 3-23 参照）としている。

表 3-23 履歴情報として管理する消費者による同意の種類

消費者による「同意」の種類	定義
利用規約に関する同意	情報銀行やサービス事業者が消費者とサービスに関する契約を締結するにあたっての規約の内容に関する同意のこと。
情報取得に関する同意	情報銀行に消費者が個人情報を預託する際の同意のこと。 但し、情報銀行が消費者から利用規約の同意を得る際に消費者から個人情報の預託を同時に受ける場合、利用規約に関する同意に含めても良い。
第三者提供※に関する同意 ※再提供（データ提供先による他の第三者へのデータ提供）も第三者提供に含めるものとする。	情報銀行が消費者から預託された個人情報を第三者に提供することに関する同意のこと。 第三者提供に関する同意の中に、以下が含まれる。 ・個別同意 ・包括同意 ・包括同意と個別同意拒否 ・包括同意と個別同意

3.4.2. 情報銀行間データ連携に付与するメタデータ

情報銀行がデータを連携する際に、いつどこで取得されたものかといったデータ自身の付加的な説明を提供する必要がある。また、情報銀行間でのデータ連携にあたり、情報銀行が消費者からどのようなパーソナルデータの預託を受けているかを示すデータを他の情報銀行に提供することで、データを受け渡すか否かの判断が可能になる。本実証事業においては、情報銀行間でのデータ連携時において、これらの必要となるデータをメタデータとし、メタデータ項目の定義付けを行った。

3.4.2.1. メタデータ項目の定義における検討内容・方法

まず、情報銀行のデータ連携時のユースケースをベースに、必要なメタデータを検討した結果、以下の 2 種類を軸に整理した（表 3-24 参照）。

表 3-24 メタデータの種類

No	メタデータの種類	概要	例
1	データの説明	そのデータが、いつどこでどのように取得されたものなのか、などを示す。	作成日時、データ提供元情報銀行情報、情報銀行間連携の同意情報
2	データカタログ	その情報銀行で扱っているパーソナルデータや同意情報が、どのような情報なのかを示す。	パーソナルデータ・同意情報に定義されている項目、本人確認されているか否か、住所はどの住所を表しているか

また、情報銀行のデータ連携時のユースケースとしては、以下の 2 つを想定した。

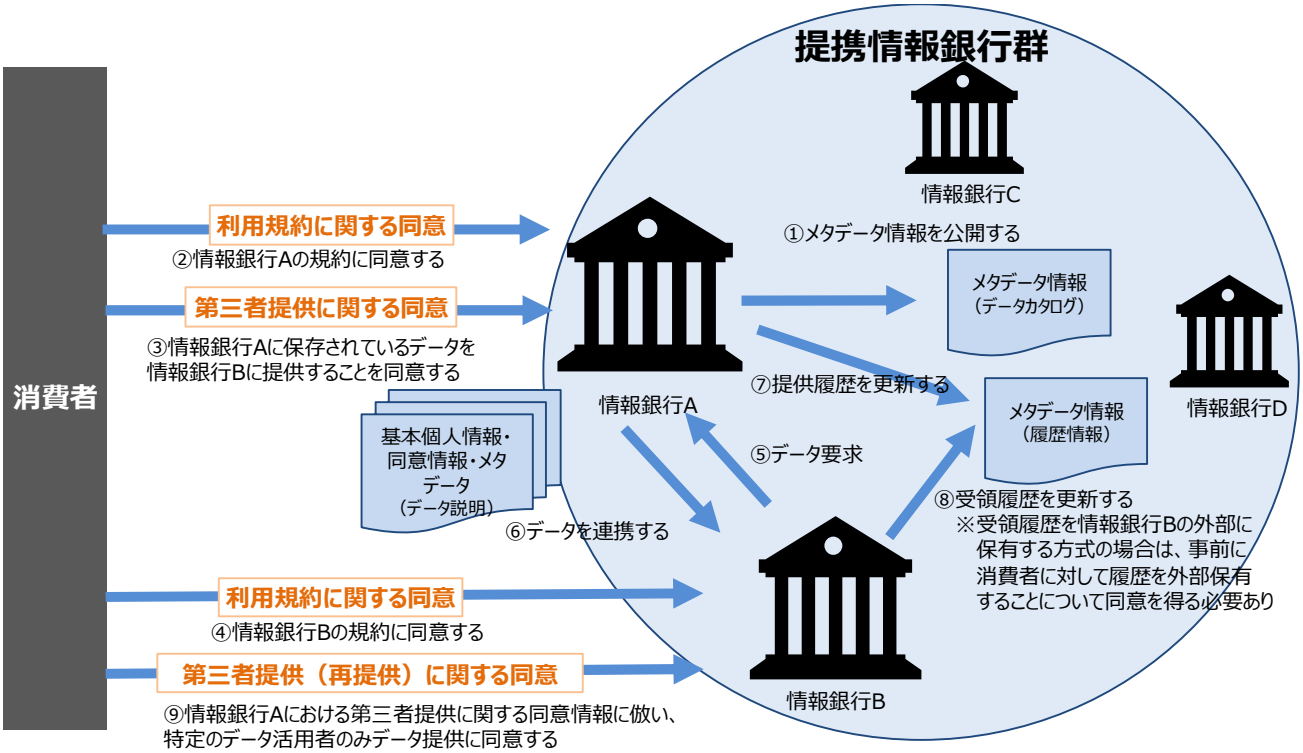


図 3-15 メタデータの流れの例:情報銀行 A と契約後、情報銀行 A から情報銀行 B にデータ連携する場合

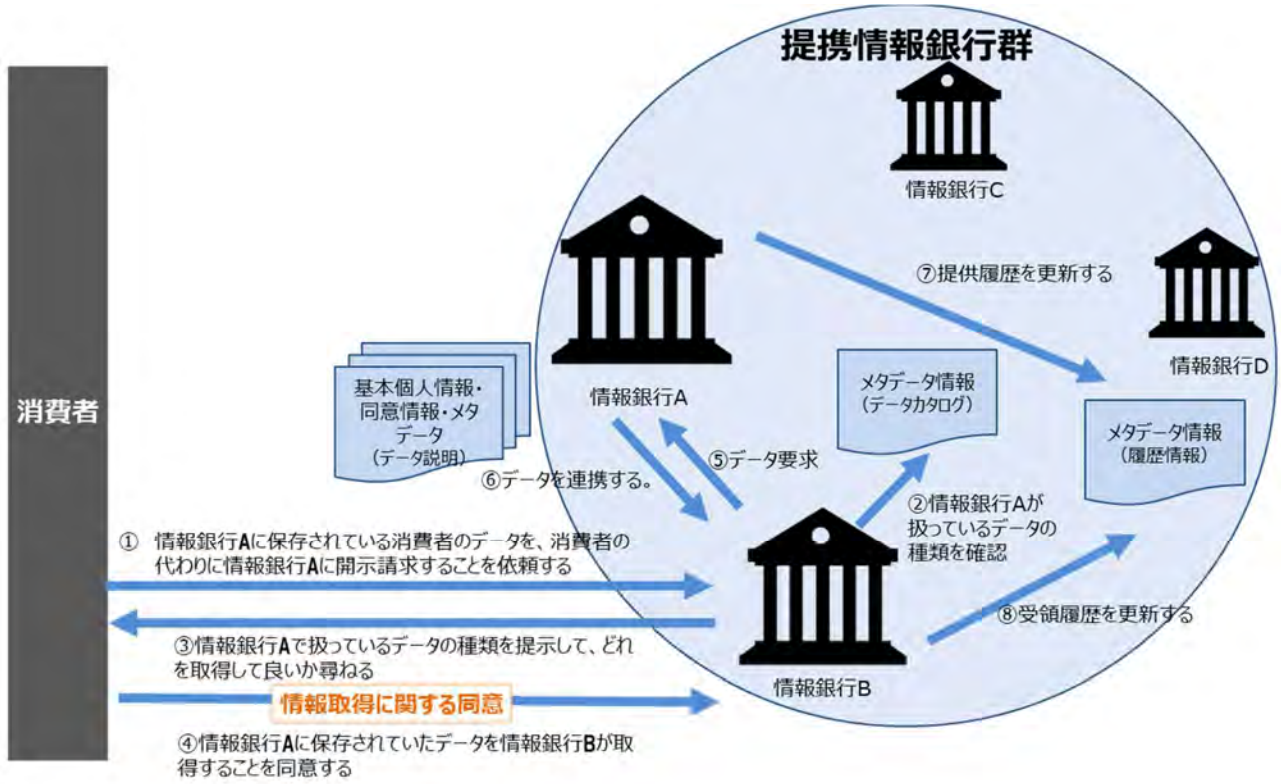


図 3-16 メタデータの流れの例:契約済の情報銀行 B に対して、契約済の情報銀行 A へのデータ開示の代理請求を依頼した上で、開示されたデータを情報銀行 B に提供場合

次に、上記の 2 種類のメタデータに必要な項目を洗い出した。その際参考として、プラットフォーム間の連携のために最低限共通化することが必要な事項を総務省・経産省等で 2017 年に取りまとめた「データ流通プラットフォーム間の連携を実現するための基本的事項」を利用した。また、メタデータの作成方法については、データカタログ項目を策定する業界団体やグループ企業等向けに業界内外でのデータ提供・利用を円滑化することを目指して策定された「データカタログ作成ガイドライン V1.1 （中間とりまとめ） 概説」等を参考にした。

最後に、上記で挙がった項目に対して、以下の観点（表 3-25 参照）で見た上で、更なるメタデータ項目の精査を行った。

表 3-25 メタデータ項目の精査の観点

	メタデータの種類	メタデータ項目の精査の観点
1	データの説明	基本個人情報や同意情報が、いつ、どこで、どのように取得されたか、どのように利用して良いデータなのかが分かる項目があること。
2	データカタログ	その情報銀行がどのようなデータが扱っているかが分かる項目があること。

メタデータ項目の精査後、「データカタログ作成ガイドライン V1.1 （中間とりまとめ）」のうち、情報銀行間連携で必要な項目を参考に、メタデータの項目の分類分けや詳細化を行った。その際、情報銀行間連携に必須ではない項目についての除外（データカタログの「カタログの対象地域」など）や、センサーを用いて観測しデータ収集を想定しているような項目（収集元情報銀行、センサー種類等）は情報銀行の流れに合わせた項目（情報収集期間、情報収集方法）に変換した。また、データカタログでは一つのデータカタログで複数のレコードを管理できるようになっているが、本定義におけるメタデータでは一つのパーソナルデータに対し一つのメタデータを管理することとし、データセット（複数のデータのまとまり）の概念を除外した。

3.4.2.2. メタデータ項目の構造化における検討内容・方法

以下の 8 つのメタデータの構成（表 3-26 参照）とし、それぞれメタデータが保有する項目について定義付けを行った（別紙 9【データ定義編】メタデータ定義書参照）。

表 3-26 メタデータ一覧

メタデータ名	説明
連携メタデータ	連携するデータのメタデータ情報（連携メタデータ）に関する基本情報を保有する。
連携メタデータ-情報銀行間同意情報	連携するデータのメタデータ情報（連携メタデータ）の情報銀行間同意情報を保有する。
連携メタデータ-個別同意提供先	連携するデータがどのような同意に基づいて連携しているのかを表す情報銀行間同意情報のうち、個別同意に関する情報を保有する。
連携メタデータ-個別同意済み利用制限	連携するデータがどのような同意に基づいて連携しているのかを表す情報銀行間同意情報のうち、個別同意の利用制約に関する情報を保有する。
連携メタデータ-包括同意提供先	連携するデータがどのような同意に基づいて連携しているのかを表す情報銀行間同意情報のうち、包括同意に関する情報を保有する。
連携メタデータ-包括同意済み利用制限	連携するデータがどのような同意に基づいて連携しているのかを表す情報銀行間同意情報のうち、包括同意の利用制約に関する情報を保有する。
データカタログ	情報銀行が保有するデータの情報（データカタログ）に関する基本情報を保有する。
データカタログ-基本個人情報属性情報	情報銀行が保有するデータの情報（データカタログ）のうち、基本個人情報の型などの情報を保有する。

連携メタデータ

連携メタデータは、消費者の同意の上、パーソナルデータとともに情報銀行間で連携されるデータであり、その構造は、図 3-17 に示すとおり、連携メタデータの詳細部には、連携されるパーソナルデータの真正性（パーソナルデータに電子署名が付与されているかを表す）や、本人確認レベル（本人確認をどのように実施した上で取得したのかを表し、厳格度合いに応じてレベル分けを実施。表 3-27 に定義を記載）を表す本人性を保有する。また、連携メタデータには利用条件部として、消費者が同意した提供期間（第三者に提供して良い期間）と利用期間（第三者が利用して良い期間）を設けている。

また、連携メタデータは消費者による同意に関する情報も保有し、同意内容の概要や同意したデータの秘匿レベル（扱うデータの秘匿性の高さに応じてレベル分けを実施。表 3-28 に定義を記載）を表すデータ秘匿レベル分類等を保有する。

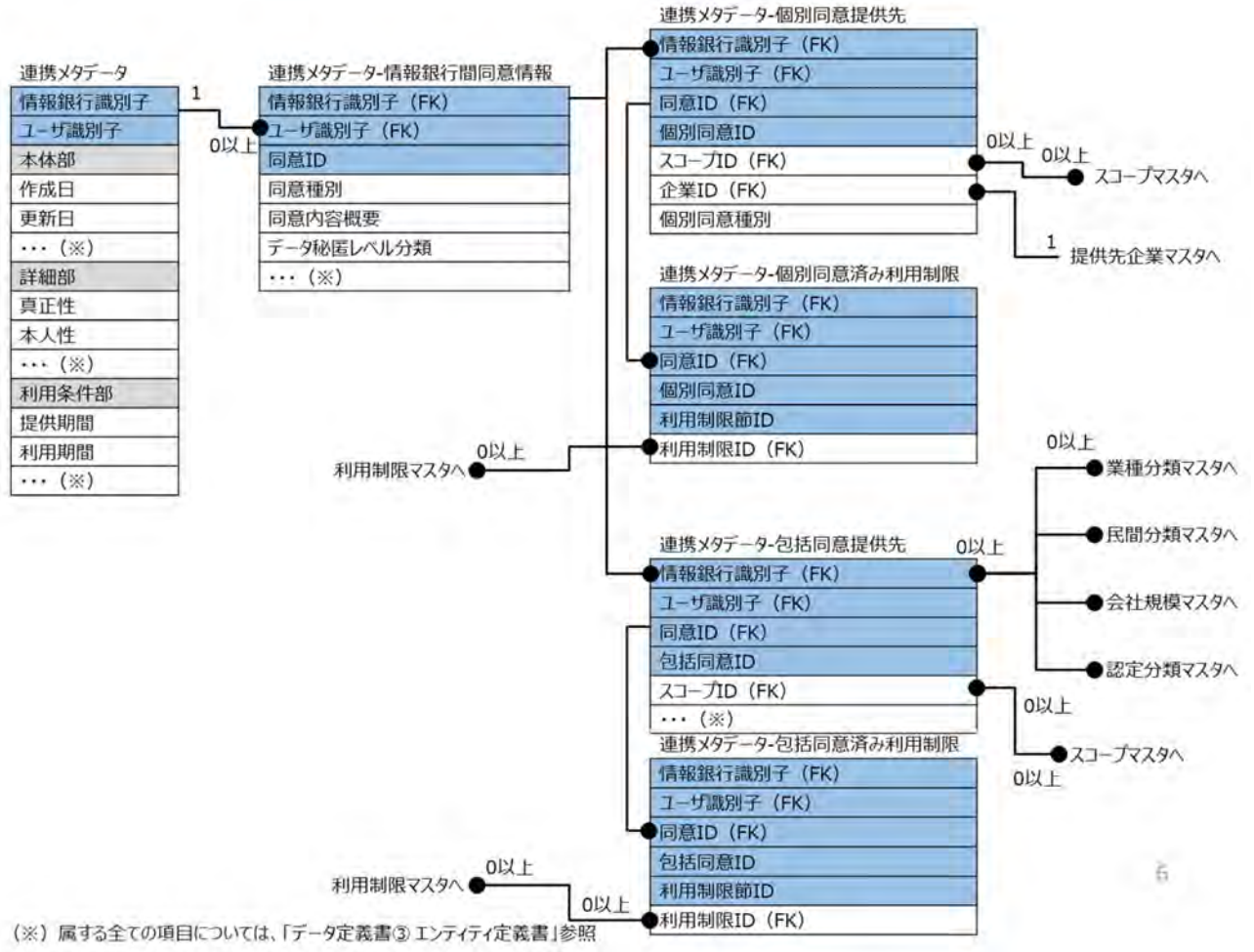


図 3-17 連携データに関するメタデータ構造（別紙 7【データ定義編】概念 ER 図より一部抜粋）

表 3-27 本人確認レベルの定義

レベル	対応する本人確認方法	具体的な本人確認方法の例
身元保証レベル 1	本人確認を実施していない、もしくは、「犯罪による収益の移転防止に関する法律施行規則第６条」に準拠しない各情報銀行独自の方法で本人確認を実施	情報銀行側で本人確認をしていない（本人の自己申告のみ） など
身元保証レベル 2	「犯罪による収益の移転防止に関する法律施行規則第６条」に準拠した方法で本人確認を実施	顔写真付きの公的確認書類を確認 顔写真なしの公的確認書類 2 点を確認 マイナンバーカードの JPKI を使った確認 オンラインで本人の顔と本人確認書類の顔写真などの送信を受けて確認 など
身元保証レベル 3	（任意定義）	追加定義する場合の例としては、「犯罪による収益の移転防止に関する法律施行規則第 6 条」に準拠した方法で**本人確認書類の検証担当者が情報銀行の定めた有資格者によって行う** など

表 3-28 秘匿レベルの定義

レベル	対象となる情報定義	具体的なデータ項目の例
秘匿レベル 1	本人の同意に基づいて情報銀行が取得・提供可能な情報	生年月日、趣味、家族構成、購買履歴、移動履歴、本人又はその家族が本人の健康管理のために取得・管理する健康情報 等
秘匿レベル 2 秘匿レベル 3	業界団体、有識者等の情報銀行における取扱いに関する検討が必要な秘匿性が高い情報（レベルの数値が高いほど慎重な取扱いが必要） • 秘匿レベル 2、3 については、要配慮個人情報を取り扱う可能性があるため、有識者等の意見を踏まえて定義する必要がある。 • 今後の業界団体、有識者等の情報銀行における取扱いに関する検討結果に従い、順次定義するものとする。 （2021 年 3 月現在で検討されている情報は、保険医療に関するもの）	以下は、保険医療情報における項目の例。 **本人に開示されている医療情報** • 特定健診項目、血液・尿等の検査結果、診療明細書、処方せん、調剤明細書 等 （詳細については本書第 2 章を参照）

データカタログ

データカタログは、情報銀行間のデータ連携に先立ち、データ連携元の情報銀行がどのようなデータを保有しているかを示すものである。データカタログにはパーソナルデータは含まれていないため、情報銀行間で共有する際に、消費者から同意を得る必要はない。データカタログにも、連携メタデータと同様に、詳細部に本人性や真正性を保有し、利用条件部に提供期間、利用期間を保有する定義としたが、これは個々の消費者のパーソナルデータに関する本人性や真正性を表すものではなく、情報銀行が保有するデータに対する本人性や真正性についてのポリシーを表している（図 3-18 参照）。

図 3-18 データカタログ構造（別紙 7【データ定義編】概念 ER 図より一部抜粋）

3.4.3. 基本情報、同意管理情報、履歴情報に関するデータ構造

データ項目の定義・名称標準化を実施した後、基本情報、同意管理情報、履歴情報（流通履歴）、履歴情報（同意管理情報）について、データ項目間の関係性を整理分類した上で、データ構造の定義を実施した。

3.4.3.1. 基本情報に関するデータ構造における検討内容・方法

基本情報としてデータ項目を定義した氏名、生年月日、性別、住所、電話番号、メールアドレスのうち、3.4.1.で示した業界のトップ企業 17 社の調査や CDS 等を踏まえ、メールアドレス、電話番号、住所については、用途によって複数保有できることとした。そのため、以下の図に示す通り、1 つの氏名と性別に対して、メールアドレス、電話番号、住所がそれぞれ複数紐づく構造としている（図 3-19 参照）。

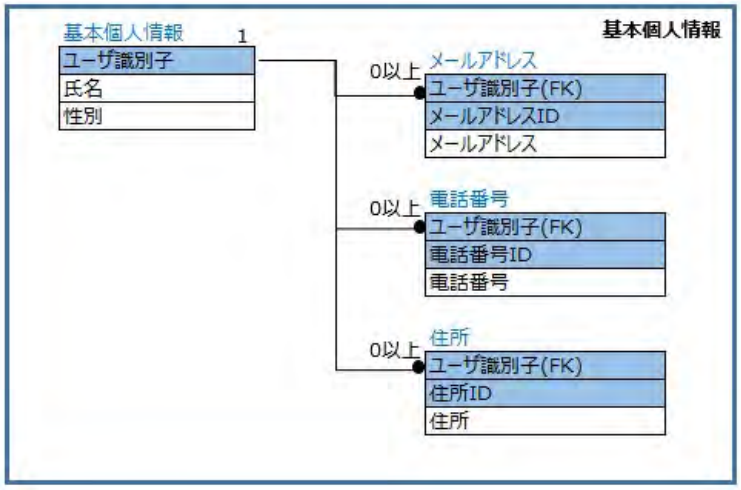


図 3-19 基本情報におけるデータ構造（別紙 7【データ定義編】概念 ER 図より一部抜粋）

3.4.3.2. 同意管理情報に関するデータ構造における検討内容・方法

3.4.1.で第三者提供に関する同意の種類を 4 種類（個別同意、包括同意、包括同意と個別同意拒否、包括同意と個別同意）示した。この包括同意と個別同意拒否のような、包括同意したがこの企業だけには拒否といったきめ細かな同意設定をできるようにするために、企業マスタを用意し、個別同意と包括同意を関連付けられるようなデータ構造とした。図 3-20 がそのイメージとなる。

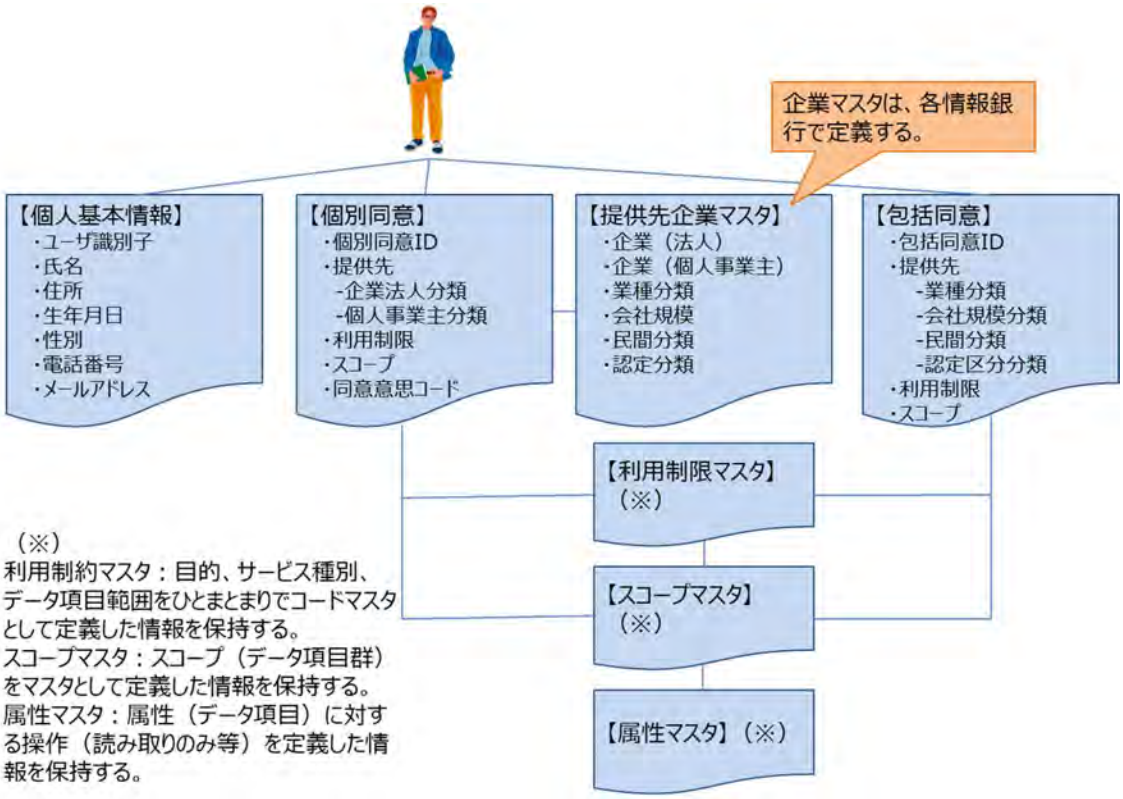


図 3-20 同意管理情報におけるデータ構造イメージ（詳細は別紙 7【データ定義編】概念 ER 図参照）

4 種類の同意ごとに、消費者が同意する際のイメージとそれによって情報銀行が保有する同意管理情報の例を以下に示す。

個別同意の場合、消費者 A が図 3-21 の左図（利用目的から企業を選ぶパターン（上）、企業から利用目的を選ぶパターン（下））の 2 つの同意画面のパターンが想定されるが、いずれのパターンにおいても、情報銀行に同意した場合、図 3-21 の右図の通りのデータで表現できる。

情報銀行Aの第三者個別同意画面（利用目的から企業を選ぶパターン）

利用目的	データ範囲	提供先	同意	同意拒否
市場調査、ならびにデータ分析やアンケートの実施等による金融商品やサービスの研究や開発のため	氏名 住所 生年月日 性別	○○株式会社	☑	☐
		××株式会社	☐	☐
ダイレクトメールの発送・電話によるご案内等、金融商品やサービスに関する各種ご提案のため	氏名 住所 生年月日 性別 Eメールアドレス 電話番号	○○株式会社	☑	☐
		××株式会社	☐	☑
	職業	○○株式会社	☐	☐
	家族構成	××株式会社	☐	☐

情報銀行Aの第三者個別同意画面（企業から利用目的を選ぶパターン）

提供先	利用目的	データ範囲	同意	同意拒否
○○株式会社	市場調査、ならびにデータ分析やアンケートの実施等による金融商品やサービスの研究や開発のため	氏名 住所 生年月日 性別	☑	☐
	ダイレクトメールの発送・電話によるご案内等、金融商品やサービスに関する各種ご提案のため	氏名 住所 生年月日 性別 Eメールアドレス 電話番号	☑	☐
		職業 家族構成	☐	☑
××株式会社	関連会社・提携会社を含む各種商品・サービスのご案内	氏名 住所 性別	☐	☐

以下の二つの個別同意に対して同意したことになる。

個別同意データのレコードイメージ

ユーザ	提供先	利用目的	データ範囲	同意意思
A	○○株式会社	市場調査、ならびにデータ分析やアンケートの実施等による金融商品やサービスの研究や開発のため	氏名 住所 生年月日 性別	同意
A	○○株式会社	ダイレクトメールの発送・電話によるご案内等、金融商品やサービスに関する各種ご提案のため	氏名 住所 生年月日 性別 Eメールアドレス 電話番号	同意
A	○○株式会社	ダイレクトメールの発送・電話によるご案内等、金融商品やサービスに関する各種ご提案のため	氏名 住所 性別	同意拒否

図 3-21 個別同意の場合の消費者が同意する際のイメージと同意管理情報の例

包括同意の場合、図 3-22 の左図の包括同意画面の通り消費者 A が情報銀行に同意すると、図 3-22 の右図の通りのデータで表現できる。

情報銀行Aの第三者包括同意画面

利用目的	データ範囲	提供先	同意
市場調査、ならびにデータ分析やアンケートの実施等による金融商品やサービスの研究や開発のため	基本情報	金融業界	☑
		製造業界	□
ダイレクトメールの発送・電話によるご案内等、金融商品やサービスに関する各種ご提案のため	購買情報 基本情報 ヘススケア情報	金融業界	☑
		製造業界	□
	購買情報 基本情報	金融業界	□
		製造業界	□
関連会社・提携会社を含む各種商品・サービスのご案内	基本情報	金融業界	□
		製造業界	□

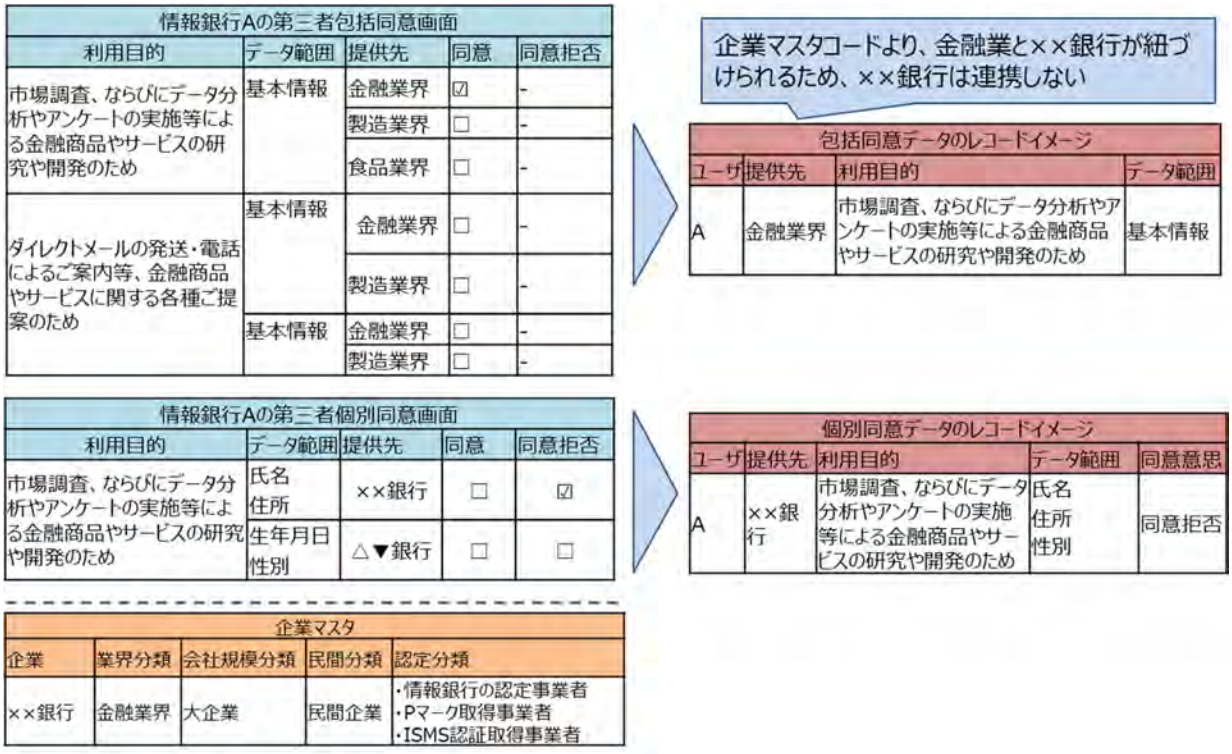
以下の二つの包括同意に対して同意したことになる。
※包括同意はレコードがあることで、同意したことになる。

包括同意データのレコードイメージ

ユーザ	提供先	利用目的	データ範囲
A	金融業界	市場調査、ならびにデータ分析やアンケートの実施等による金融商品やサービスの研究や開発のため	基本情報
A	金融業界	ダイレクトメールの発送・電話によるご案内等、金融商品やサービスに関する各種ご提案のため	購買情報 基本情報 ヘルスケア情報

図 3-22 包括同意の場合の消費者が同意する際のイメージと同意管理情報の例

包括同意をして一部個別同意拒否する場合、消費者 A が図 3-23 の左図の上段と下段の画面の通り情報銀行に同意・同意拒否すると、包括同意データのレコードとしては、金融業界に対する包括同意として表現されるが、金融業界である XX 銀行（図 3-23 の左図下の企業マスタにより判断）については個別に同意拒否していることから、個別同意データのレコードとして、XX 銀行が同意拒否であることが表現される。



情報銀行Aの第三者包括同意画面

利用目的	データ範囲	提供先	同意	同意拒否
市場調査、ならびにデータ分析やアンケートの実施等による金融商品やサービスの研究や開発のため	基本情報	金融業界	☑	-
		製造業界	□	-
		食品業界	□	-
ダイレクトメールの発送・電話によるご案内等、金融商品やサービスに関する各種ご提案のため	基本情報	金融業界	□	-
		製造業界	□	-
	基本情報	金融業界	□	-
		製造業界	□	-

企業マスタコードより、金融業と××銀行が紐づけられるため、××銀行は連携しない

包括同意データのレコードイメージ

ユーザ	提供先	利用目的	データ範囲
A	金融業界	市場調査、ならびにデータ分析やアンケートの実施等による金融商品やサービスの研究や開発のため	基本情報

情報銀行Aの第三者個別同意画面

利用目的	データ範囲	提供先	同意	同意拒否
市場調査、ならびにデータ分析やアンケートの実施等による金融商品やサービスの研究や開発のため	氏名 住所	××銀行	□	☑
	生年月日 性別	△▼銀行	□	□

個別同意データのレコードイメージ

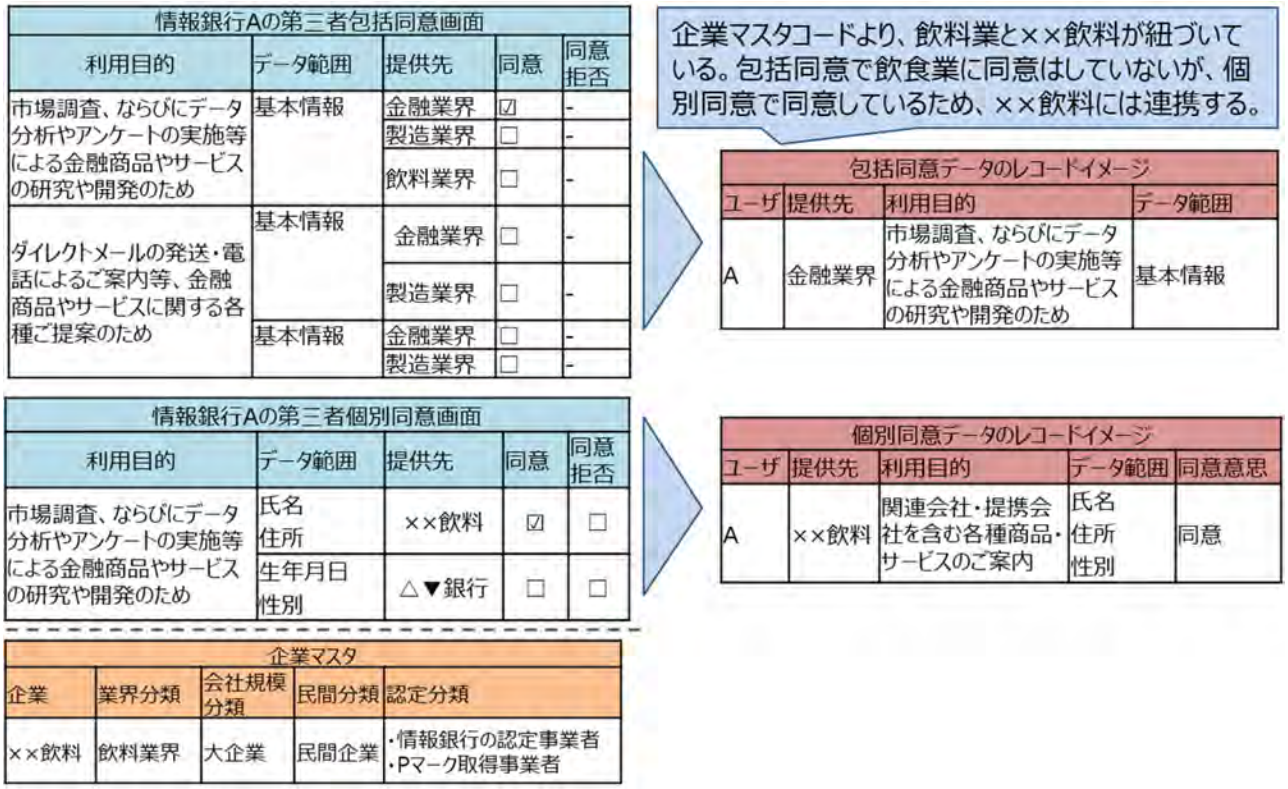
ユーザ	提供先	利用目的	データ範囲	同意意思
A	××銀行	市場調査、ならびにデータ分析やアンケートの実施等による金融商品やサービスの研究や開発のため	氏名 住所 性別	同意拒否

企業マスタ

企業	業界分類	会社規模分類	民間分類	認定分類
××銀行	金融業界	大企業	民間企業	・情報銀行の認定事業者 ・Pマーク取得事業者 ・ISMS認証取得事業者

図 3-23 包括同意をして一部個別同意拒否の場合の消費者が同意する際のイメージと同意管理情報の例

包括同意していない業界の企業に対して個別同意する場合、消費者 A が図 3-24 の左図の上段と下段の画面の通り情報銀行に同意すると、包括同意データのレコードとしては、金融業界に対する包括同意として表現されるとともに、個別同意データのレコードとして、XX 飲料を同意したことが表現される。



情報銀行Aの第三者包括同意画面

利用目的	データ範囲	提供先	同意	同意拒否
市場調査、ならびにデータ分析やアンケートの実施等による金融商品やサービスの研究や開発のため	基本情報	金融業界	☑	-
		製造業界	□	-
		飲料業界	□	-
ダイレクトメールの発送・電話によるご案内等、金融商品やサービスに関する各種ご提案のため	基本情報	金融業界	□	-
		製造業界	□	-
	基本情報	金融業界	□	-
		製造業界	□	-

企業マスタコードより、飲料業と××飲料が紐づいている。包括同意で飲食業に同意はしていないが、個別同意で同意しているため、××飲料には連携する。

包括同意データのレコードイメージ

ユーザ	提供先	利用目的	データ範囲
A	金融業界	市場調査、ならびにデータ分析やアンケートの実施等による金融商品やサービスの研究や開発のため	基本情報

情報銀行Aの第三者個別同意画面

利用目的	データ範囲	提供先	同意	同意拒否
市場調査、ならびにデータ分析やアンケートの実施等による金融商品やサービスの研究や開発のため	氏名 住所	××飲料	☑	□
	生年月日 性別	△▼銀行	□	□

個別同意データのレコードイメージ

ユーザ	提供先	利用目的	データ範囲	同意意思
A	××飲料	関連会社・提携会社を含む各種商品・サービスのご案内	氏名 住所 性別	同意

企業マスタ

企業	業界分類	会社規模分類	民間分類	認定分類
××飲料	飲料業界	大企業	民間企業	・情報銀行の認定事業者 ・Pマーク取得事業者

図 3-24 包括同意していない業界の企業に対して個別同意する場合の消費者が同意する際のイメージと同意管理情報の例

3.4.3.3. 履歴情報に関するデータ構造における検討内容・方法

消費者が複数の情報銀行を利用している場合、それぞれの情報銀行において、いつ何を同意したか、いつどんなデータがどこに提供されたかといった履歴をそれぞれの情報銀行で確認することは消費者の負担が大きい。そこで、1 つの情報銀行で包括的なトレーサビリティが確認できる仕組みを提供するために必要なデータ項目・データ構造を定義した（図 3-25 参照）。なお、これらの定義は、3.5.5.にて検討した包括的なトレーサビリティ実現に向けた機能・ルールを踏まえたものとなっている。

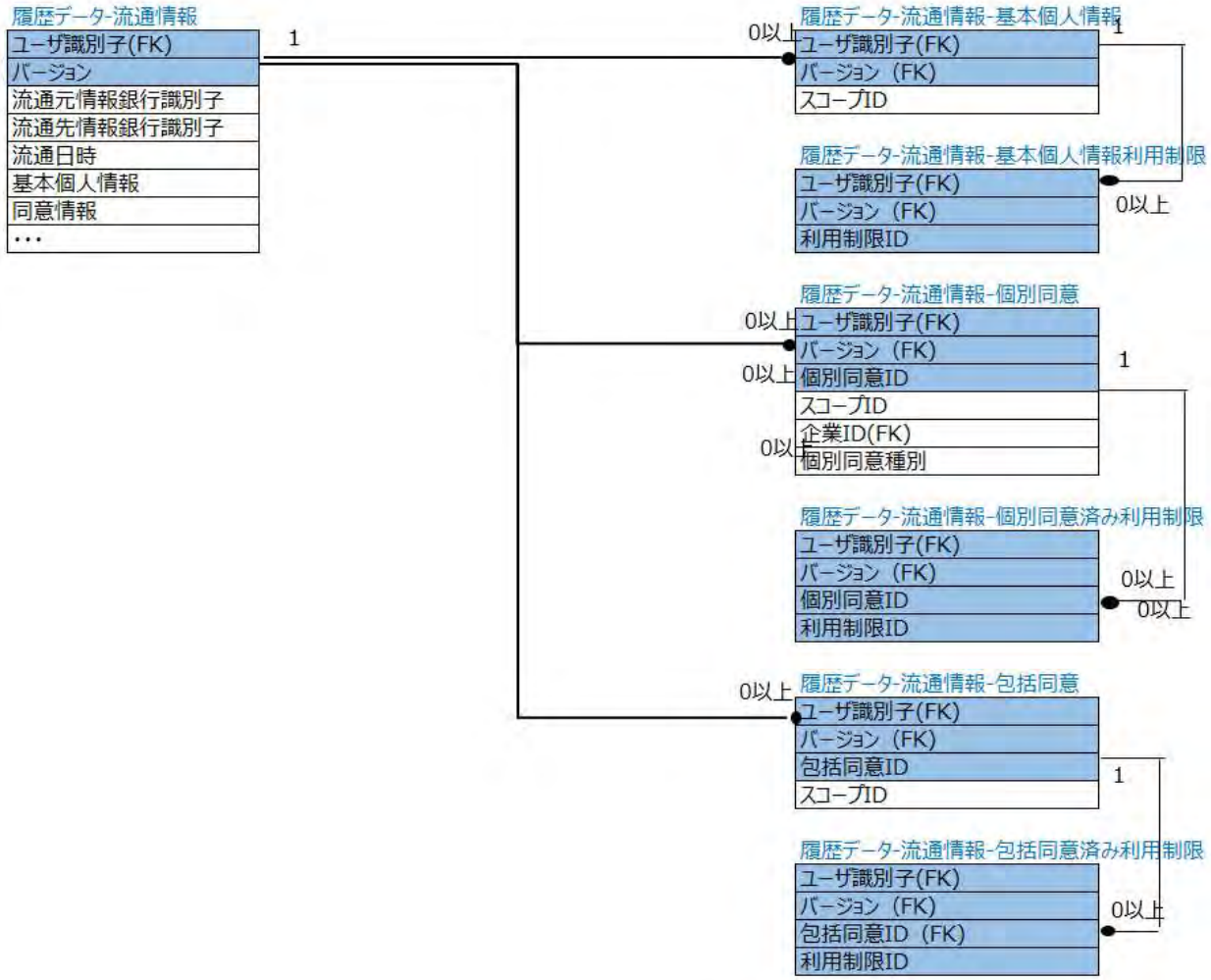


図 3-25 履歴情報（流通履歴）におけるデータ構造（別紙 7【データ定義編】概念 ER 図より一部抜粋）

履歴情報（同意管理情報）については、1 人の消費者に対して複数の同意情報が紐づく構造としている。例えば、消費者が利用規約の同意を行った後、利用規約の改定があった場合において、どのバージョンの利用規約に対して同意したかを管理できるようにしている（図 3-26 参照）。

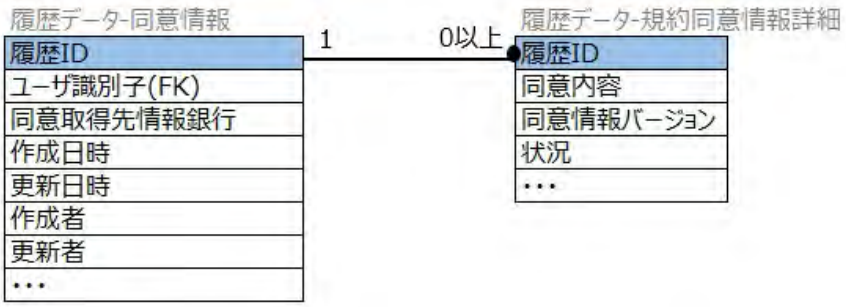


図 3-26 履歴情報（同意管理情報）におけるデータ構造
（別紙 7【データ定義編】概念 ER 図より一部抜粋）

3.4.4. 伝送時におけるデータフォーマット

一般に伝送時におけるデータフォーマットはCSVやXML等、様々なものが用いられている。本実証事業においては、データ連携元やデータ連携先におけるフォーマット変換等の負担を削減するため、データフォーマットについて調査・評価を実施した上で選定し、更にその詳細な記載方法を定義した。

3.4.4.1. データフォーマット候補の抽出

伝送時におけるデータフォーマットを選定するため、一般的なデータ連携で利用されるデータ形式である、固定長・CSV・TSV・XML・JSON・キーバリュー方式を候補として挙げた（表 3-29 参照）。

表 3-29 データ連携時の一般的なデータ形式

データ形式	特徴	メリット	デメリット
固定長	• 表構造/階層構造 • バイナリ/テキスト	• データサイズが小さくなる傾向がある（基本的にデータそのものを格納しデータ名を格納しないため） • データの処理速度が速い傾向がある（基本的に先頭から順にアクセスするため）	• データの構造の変更が難しい（構造が変わるとデータのオフセットが変わるためデータへのアクセス方法の変更が必要となり関連システムへのインパクトが大きい） • データを保護・保障する仕組みが用意されていない（独自に対応が必要） • データにメタ情報を付与しづらい（データの構造の変更が難しいためメタデータのような可変の情報を付与しづらい）
CSV、TSV	• 表構造 • テキスト	同上	同上
XML	• 階層構造 • テキスト	• データの構造の変更がしやすい（階層構造のため新たな階層を増やしても既存の階層に影響が出にくい） • データにメタ情報を付与しやすい（データの構造の変更がしやすいためメタデータのような可変の情報を付与しやすい） • データを保護・保障する仕組みが用意されている（XML電子署名、XML暗号化）	• データサイズが大きくなる傾向がある（データに加えてデータ名や名前空間などデータを識別する情報を多く格納するため） • データの処理速度が遅い傾向がある（データへのアクセスが階層をたどる方式のため。またメモリ使用量が多くなる傾向があるため）
JSON	• 階層構造 • テキスト	• データの構造の変更がしやすい（階層構造のため新たな階層を増やしても既存の階層に影響が出にくい） • データにメタ情報を付与しやすい（データの構造の変更がしやすいためメタデータのような可変の情報を付与しやすい） • データを保護・保障する仕組みが用意されている（JWS、JWE）	• データサイズがやや大きくなる傾向がある（データに加えてデータ名を格納するため） • データの処理速度が遅い傾向がある（データへのアクセスが階層をたどる方式のため。またメモリ使用量がやや多くなる傾向があるため）

キーバリュー	• キーバリュー構造 • テキスト	• データの構造の変更がしやすい（キー名でデータアクセスするため新たなデータを増やしても既存のデータに影響がでにくい） • データにメタ情報をやや付与しやすい（データの構造の変更がしやすいためメタデータのような可変の情報を付与しやすい）	• データサイズがやや大きくなる傾向がある（データに加えてデータ名を格納するため） • データを保護・保障する仕組みが用意されていない • データの処理速度がやや遅い傾向がある（データへのアクセスがマップ方式のため。またメモリ使用量がやや多くなる傾向があるため）

3.4.4.2. データフォーマット評価・選定

それぞれのデータ形式の特徴と、以下を主な評価観点としてデータ連携におけるデータ形式の評価を実施したところ、JSON 形式の評価結果が最も高くなった（表 3-30、表 3-31 参照）。

- データの処理速度
- データサイズ
- データの構造変更への影響
- データを保護・保障する仕組み
- データのメタ情報の付与のしやすさ

表 3-30 データ連携時の一般的なデータ形式の評価

データ形式	データ連携における評価の観点									ポイント
	構造変更	メタ情報	保護・保障	技術者の数	作り込みやすさ	プラットフォームへの依存	最新の Web 技術との親和性	処理速度	データサイズ	
固定長	難しい	付与しづらい	なし	少ない	難しい	高い	低い	速い	小	2
CSV、TSV	難しい	付与しづらい	なし	多い	容易	高い	低い	速い	小	4
XML	容易	付与しやすい	あり	多い	難しい	低い	やや低い	遅い	大	4.5
JSON	容易	付与しやすい	あり	多い	容易	やや低い	高い	やや遅い	中	7.5
キーバリュー	やや容易	やや付与しやすい	あり	多い	容易	高い	高い	やや遅い	中	5

表 3-31 データ連携時の一般的なデータ形式の評価にあたってのポイント付与基準

ポイント付与基準								
構造変更	メタ情報	保護・保障	技術者の数	作り込みやすさ	プラットフォームへの依存	最新の Web 技術との親和性	処理速度	データサイズ
難しい:0 やや容易:0.5 容易:1	付与しづらい:0 やや付与しやすい:0.5 付与しやすい:1	なし:0 あり:1	少ない:0 多い:1	難しい:0 容易:1	高い:0 やや低い:0.5 低い:1	低い:0 やや低い:0.5 高い:1	遅い:0 やや遅い:0.5 速い:1	大:0 中:0.5 小:1

つまり、JSON の階層構造は CSV などの表構造と比べてデータ構造の変更による影響が少ない点や、JSON は XML と比べてタグを挟む必要がないのでデータ量が少なくなり、処理のパフォーマンスが高い点などが、情報銀行におけるデータ連携に適しているため、高い評価に繋がった。また、2018 年から 2020 年に構築されたシステムでは、データ連携時におけるファイルフォーマットとして、JSON が XML の 5 倍以上採用されているとのデータ[1]があり、近年のシステムでは一般的なデータ形式として流通している。利用しているシステムが多いことから技術者の数が多く、サードパーティー製のライブラリが数多く存在することや資料が多いことによる作り込みやすさもメリットとして挙げられる。

加えて、実際に、3.4.1.で検討した基本情報や同意管理情報に即して考えてみると、次のような利点がある。

① 階層構造の表現のしやすさ

基本情報や同意管理情報は階層構造で項目を表している。階層構造とすることでわかりやすい構造になり、名前など同じ定義の要素を複数の場所で使用することが可能になる。

例えば基本情報では【住所】と【メールアドレス】に同じ用途(purpose)という項目名をつけているが、JSON であれば以下のように区別ができる。

【住所】

```
"addresses": [
  {
   "purpose": "本籍",
     "combined": {
       "address": "○○県○○市..."
     }
     ...
  },
```

[1] 出典:programmableweb.com「JSON is Clearly the King of API Data Formats in 2020」（2020 年 4 月 3 日 記事）<https://www.programmableweb.com/news/json-clearly-king-api-data-formats-2020/research/2020/04/03>（参照日 2021 年 2 月 17 日）

```
    …
  ]

  【メールアドレス】
  "emailAddresses": [
    {
      "purpose": "勤務先",
      "address": "example@example.org",
      …
    },
    …
  ]
```

② 保守性、拡張性

JSON や XML といった階層構造は将来的に別の階層が追加される際に、既存のデータ項目名との重複を気にする必要が無いため、既存の階層に影響が出にくく、保守性や拡張性が高い。

例えば本実証事業で定義した【氏名】や【住所】に加えて将来【クレジットカード】を追加する場合、そのクレジットカードの用途やカード名義などといったデータ項目を定義する際に他の項目の定義を気にせずに設定できる。

```
  【氏名】
  "name": [
    …
  ]

  【住所】
  "addresses": [
    {
     "purpose": "本籍",
      …
    },
    …
  ]

  【クレジットカード】
  "creditCards": [
    {
      "purpose": "社用決済",
```

```
      "name": "HANAKO  YAMADA",
     ...
    },
    ...
  ]
```

③ 配列の表現のしやすさ

基本情報や同意情報は複数の住所や電話番号の設定を行う必要がある。JSON はデフォルトで配列の表現が可能なため、他のデータ形式と比べて複数の住所や電話番号をシンプルに表現できる。

例えば電話番号を配列表現する際には、【JSON】であれば以下のようにシンプルに表現できるが、【XML】は配列とするキー名（下記例では telephone というキー名）が一致している必要がある。

【JSON】

```
{
  "name": "○○",
  "telephones": ["0120-444-444", "0120-555-555"],
  ...
}
```

【XML】

```
<personalData>
  <name>○○</name>
  <telephone>0120-444-444</telephone>
  <telephone>0120-555-555</telephone>
</personalData>
```

なお、本実証事業においては JSON を推奨するものの、データ連携を行う情報銀行間での調整が行われていれば、JSON 以外の形式でも問題ない。また、連携フォーマットについて情報銀行間での調整負荷を軽減するため、連携元と連携先との間にフォーマット変換を行うプラットフォームを介すことも想定される。

3.4.5. 情報銀行に求められる匿名加工等のデータ変換・加工技術

パーソナルデータについて特定の個人を識別及び復元できないようにするための技術として、匿名加工等のデータ変換・加工技術が存在する。情報銀行にてパーソナルデータを流通させるにあたり、これらの技術が適用可能と推測されるが、どのようなケースで有効活用できる可能性があるのかが明確になっていない。そこで、匿名加工データの活用事例を調査し、情報銀行の介在可能性が想定される事例を抽出の上、主なユースケースとして、収集データ、活用内容、及び情報銀行に求められる役割や機能、強みを具体化した。

また、匿名加工以外のデータ変換・加工技術についても、事例調査の上、情報銀行が介在する場合に想定されるユースケースを取りまとめた。

3.4.5.1. 匿名加工データの活用事例に関する調査内容・方法

匿名加工データの活用事例について公知情報を基に調査し、抽出された事例をカテゴライズ後、活用データ・スキーム・活用内容をまとめた（表 3-32 参照）。

表 3-32 匿名加工データの事例一覧

No	カテゴリ	タイトル	活用データ	スキーム	データ活用内容
1	購買データ	ID-POS データの活用[2]	属性情報、購買履歴（購買日時、購買店舗、購買商品等）	小売事業者が収集したポイントカード等の ID-POS データを匿名加工し、商品の仕入れ元のメーカーや卸業者に販売。メーカーや卸業者は、自社の商品をエンドユーザーが購入している状況を詳細に分析。	よりターゲットを絞った効果的なマーケティング
2		クレジットカード利用情報の活用 [2]	属性情報、クレジットカード利用履歴（購買日、購買金額、購買店舗等）	クレジットカード事業者が収集した利用者の属性や利用履歴について、匿名加工を行った上で研究機関に提供し、マーケティングや商品開発に関する分析等を依頼。	今後の事業計画の参考や新たな事業に関する示唆を得る
3		クレジットカード情報の利活用事例[3]	属性情報、クレジットカード利用履歴（購買日、購買金額、購買店舗等）	カード会社が保有するクレジットカードユーザーのカード利用情報について、匿名加工を行った上で、分析会社に提供。分析会社は、匿名加工情報から消費指数を作成し、統計閲覧会員向けに指数を提供するサービスを提供。	消費指数の作成

[2] 出典:三菱総合研究所「匿名加工情報・個人情報の適正な利活用の在り方に関する動向調査 調査報告書（平成 30 年 3 月）」<https://www.ppc.go.jp/files/pdf/tokumeikakou_report.pdf>（参照日 2021 年 2 月 17 日）

[3] 出典:株式会社野村総合研究所「パーソナルデータの適正な利活用の在り方に関する動向調査（平成 30 年度）報告書＜別添資料＞事例集」<https://www.ppc.go.jp/files/pdf/jireisyu_201903.pdf>（参照日 2021 年 2 月 17 日）

4		不動産開発事業者によるポイントカードデータの利活用事例[4]	属性情報、利用履歴（商業施設名、店舗名、購入金額、日時）	不動産開発事業者が地域限定で発行しているポイントカードの登録情報や利用履歴データを匿名加工し、研究機関に提供し、データ分析を委託。不動産開発事業者は、研究機関からポイントカードの匿名加工情報と、大手 SNS における、ポイントカードが利用されているエリアに関する不特定多数の投稿データを組み合わせた分析結果を取得。	SNS を用いたキャンペーンによる販促効果の分析
5	位置データ	Wi-Fi 位置情報の利活用事例 [3]	Wi-Fi 利用者情報（MAC アドレス、言語情報）、位置情報（MAC アドレス、取得時刻、地点名）	通信会社が保有する位置情報（通信の秘密に該当しない、フリーWi-Fi のアクセスポイントの位置情報）及び Wi-Fi 接続時に選んだ言語情報について、匿名加工を行った上で、研究機関に提供。研究機関は、どこの観光施設に行ったのか、行かなかったのか、あるいは、どういう順番で施設を訪問したのか、等の分析を実施。	言語圏ごとの観光施設の訪問や訪問順序等の分析
6		観光客情報の利活用事例 [3]	属性情報、履歴情報（移動情報、決済・購買情報、サービス利用情報、閲覧情報）	ローカルプラットフォーム事業者が訪日外国人から取得したデータの匿名加工を「おもてなしプラットフォーム」の運営事業者に委託。ローカルプラットフォーム事業者は、匿名加工されたデータをおもてなしプラットフォーム運営事業者に提供。おもてなしプラットフォーム運営事業者はデータを分析し、分析結果をローカルプラットフォーム事業者に提供。	国籍ごとの観光施設の訪問や訪問順序、購買行動等の分析
7	医療データ	生命保険会社による健康データ等の利活用事例 [4]	属性情報、保険種類、払込保険料、健診情報 ライフログ（歩数、運動時心拍数等）	生命保険会社が収集した健康データ等を活用した共同研究のため、委託先が匿名加工したデータを外部研究機関に提供。生命保険会社と外部研究機関が共同でデータを活用し共同研究を実施。	健康増進型保険の提供にあたり、健康データ等を用いて健診結果数値の予測等を行うための研究

[4] 出典:株式会社野村総合研究所「パーソナルデータの適正な利活用の在り方に関する実態調査（令和元年度）報告書＜別添資料＞事例集」<https://www.ppc.go.jp/files/pdf/personal_date_cases2019.pdf>（参照日 2021 年 2 月 17 日）

8		第一生命保険[5]	（詳細不明） 属性情報、医療情報（社内、社外）	（詳細不明） 保険会社が、社内で保有する医療情報と社外から取得した匿名加工した医療情報を掛け合わせて分析。	疾病による入院・死亡のリスク分析による生命保険の引受基準適正化
9		医療 DB 事業者による医療データの利活用事例 [4]	属性情報、医療情報（傷病名、処置情報、薬剤名）属性情報	医療機関が保有する薬剤の処方実態データ（レセプトデータの一部）を入退院に係るデータ（DPC データの一部）を匿名加工し、医療 DB 事業者に提供。医療 DB 事業者は薬剤の効用や副作用の分析し、製薬会社に提供。	薬剤の効用や副作用の分析
10		製薬企業による医療データの利活用事例 [4]	属性情報、医療情報（傷病名、処置情報、薬剤名、臨床検査結果データ）	医療 DB 事業者が保有する匿名加工情報を製薬企業に提供。製薬会社は匿名加工情報をデータ分析業者に提供し、データ分析を委託し、分析結果を取得。	薬剤の効用や副作用の分析
11		アステラス製薬 医療・健康データの活用 [5]	属性情報、医療情報（傷病名、処置情報、薬剤名）	（詳細不明） 製薬会社が、匿名加工したレセプトデータ等を医薬品等の安全対策の向上等に活用。	医薬品等の安全対策の向上等に活用
12		レセプトデータの活用 [2]	レセプトデータ	健康保険組合が保有するレセプトデータについて、匿名加工を行った上で、医療 DB 事業者に提供。医療 DB 事業者は健康保険組合や研究機関や製薬会社等に対して、データ提供やコンサルティングなどのサービスを提供。 医療データベース事業者:レセプトデータ等のデータベース化及び分析を行い、健康保険組合、研究機関、製薬会社等に提供。	組合員に対する保健事業の効果増大や効率化を図るために検討する際、自らが保有するレセプトデータ等と医療 DB 事業者の保有する他組合のデータの比較・分析結果を参考（健康保険組合） 匿名加工された医療ビッグデータを用いて新薬・新サービス開発や学術的研究を実施（研究機関・製薬会社）

[5] 出典:日本経済団体連合会「Society 5.0 の実現に向けた個人データ保護と活用のあり方 提言付属資料～個人データ活用事例～（2019 年 10 月 15 日）」<
https://www.keidanren.or.jp/policy/2019/083_honbun.pdf>（参照日 2021 年 2 月 17 日）

13		医療健康情報の利活用事例 [3]	属性情報、レセプトデータ、健診情報	健康保険組合が保有する健診情報、レセプトデータについて、匿名加工を行った上で、医療健康情報サービス事業者に提供。医療健康情報サービス事業者は分析を行い、分析結果を健康保険組合に提供。	組合員の生活習慣の改善につながる、企業の健康経営に向けた様々なサービスの開発
14		健康診断情報の利活用事例 [3]	属性情報、健診情報	ヘルスケア事業者が保有する健診データについて、匿名加工を行った上で、研究機関に提供。研究機関は、「このような状況にあった個人は、このような運動をしたら、検査数値がこのように変わる可能性が高い」、「今後このままでは検査数値はこのように変化していく可能性が高い」といった検査数値の予測のための分析を行い、分析結果をヘルスケア事業者に提供。	検査数値の予測
15		処方箋記載事項の活用 [2]	患者情報（年齢・性別）、調剤情報（薬局、調剤年月日、薬剤名）	調剤薬局が取り扱う処方箋に含まれる患者情報及び調剤情報について、匿名加工を行った上で、専門シンクタンクに提供。シンクタンクは、処方箋情報等の分析を行い、製薬会社、研究機関等にデータベースやコンサルティングのサービスを提供。	自社・他社の薬がどのように販売・利用されているかを把握（製薬会社） 薬の服用等に関する研究（研究機関）
16	人材データ	役員報酬・従業員賃金等情報の活用 [2]	企業データ（企業情報、役員情報（役職、年齢、報酬、退職金等）、従業員の賃金指標等）	税理士事務所・公認会計士事務所が保有する企業データについて、匿名加工を行った上でシステム事業者に提供。システム事業者はデータベースを作成し、自社サービスの会員（税理士事務所・公認会計士事務所）等に提供。	取引先企業に対するアドバイス（主に税務に関するもの）を行う際に取引先企業と類似した企業に関するデータを参考
17	物流データ	物流ドライバーの運行・生体情報の利活用事例 [3]	生体情報（性別、生年月日、体温等）、運行情報（時間、距離、速度等）、ドライブレコーダーによる動画	物流事業者は、ドライバーの同意の上でグループ会社から提供を受けたドライバーの運行情報および生体情報について、匿名加工を行った上で、研究機関に提供。研究機関はドライバーの安全運行管理システムの開発のためのデータ分析を行い、分析結果を物流会社に提供。	ドライバーの安全運行管理システムの開発のための分析
18	電力データ	住宅事業者による電力データの提供事例 [4]	属性情報、履歴情報（消費電力量、売電量、買電量、発電量）	住宅事業者が自社の契約住宅から取得したHEMS(Home Energy Management System)データを匿名加工し、データ分析会社等の第三者に販売提供。データ分析会社等は、受領データに含まれる消費電力	消費電力の予測等の分析

				等の電力に関するデータから、消費電力の予測等の分析を実施。	
19	閲覧データ	凸版印刷電子チラシ「Shufoo!」の取組み [5]	属性情報、チラシの閲覧状況等	電子チラシサービス「Shufoo!」を通じて取得したチラシの閲覧状況等のデータを匿名加工し、事業者に提供。	消費者に対するタイムリーで最適な情報提供に活用
20	介護データ	介護サービス利用情報の活用 [2]	介護データ（ケアプラン、アセスメント情報等）	介護事業者が保有する介護データについて、匿名加工を行った上でケアプラン分析・提案事業者に提供。ケアプラン分析・提案事業者は、AI 開発事業者との業務提携により、AI を用いて、利用者の体調や症状に合った、より効果的なケアプランをケアマネージャーに提案するシステムを開発中。	利用者の体調や症状に合った、より効果的なケアプランをケアマネージャーに提案するシステムの開発

3.4.5.2. 匿名加工技術において情報銀行に求められるユースケース

上記事例について情報銀行の介在可能性を検討し、介在可能性が有る事例を基に、匿名加工技術において情報銀行に求められるユースケースとして 5 つのケースを想定した（図 3-27、表 3-33 参照）。

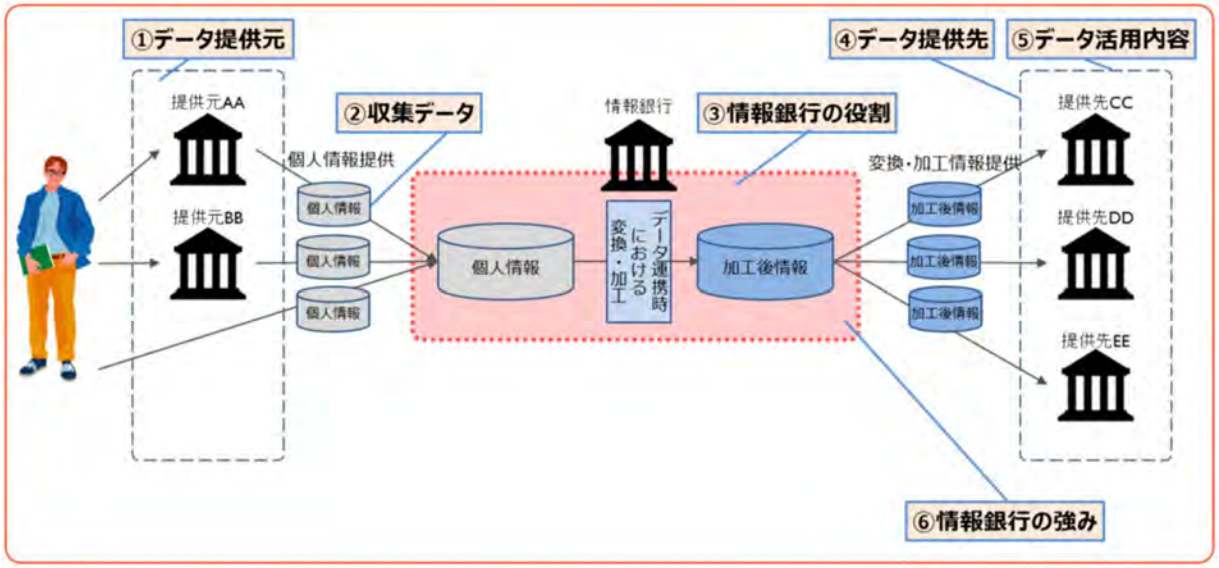


図 3-27 情報銀行によるデータ変換・加工に関するユースケース全体イメージ

表 3-33 情報銀行によるデータ変換・加工に関するユースケース一覧（匿名加工）

No	ケース	①データ提供元	②収集データ	③情報銀行の役割	④データ提供先	⑤データ活用内容	⑥情報銀行の強み
1	購買データの活用	小売業者 クレジットカード会社 ポイントカード会社 各種 EC サイト 等	ポイントカード利用購買履歴 クレジットカード利用履歴	パーソナルデータの収集 匿名加工情報の作成 匿名加工情報の提供	メーカー 卸業者 小売業者	商品開発 マーケティング戦略 販促効果分析 事業計画立案	同一人物の様々なポイントカードやクレジットカードでの購買データを紐づけた上で匿名加工することで、分析精度向上が期待できる。
2	位置データの活用	通信会社 ローカルプラットフォーム事業者(各地域で訪日外国人からデータを取得した事業者)	位置データ（GPS データ等の移動履歴） 属性情報	同上	観光施設 店舗 等	属性ごとの店舗や観光施設の訪問行動の分析による観光施策立案	情報銀行が広く一般に浸透すれば、位置データを豊富に収集することができる可能性がある。
3	医療データの活用	健康保険組合 調剤薬局	健診データ レセプトデータ 処方箋に関する情報 ライフログ	同上	生命保険会社 研究機関 健康保険組合	健診結果数値の予測 生活習慣の改善アドバイス 等	同意が得られれば、匿名加工情報だけでなく、匿名加工されていない情報と合わせての分析や、医療データ以外の情報銀行に蓄積された様々なデータと掛け合わせた分析により、分析精度向上が期待できる。
4	人材データの活用	税理士事務所 公認会計士事務所	人材データ 企業データ	同上	税理士事務所 公認会計士事務所 転職エージェント	取引先企業に対する税務に関するアドバイス	情報銀行が、税理士事務所・公認会計士事務所が保有していない企業の従業員データを補完することができれば、活用の幅が広がる。
5	物流データの活用	物流会社	ドライバーの運行情報 ドライバーの生体情報	パーソナルデータの収集 パーソナルデータの提供 匿名加工情報の作成 匿名加工情報の提供	研究機関（匿名加工情報） 物流会社（個人情報）	ドライバーの安全運行管理システムの開発のための分析	生体情報を安全に管理し、ドライバーにデータ流通を制御・見える化させるユーザー起点のデータ流通を実現することで、不安感の払しょくに寄与できる。

3.4.5.3. その他データ変換・加工技術において情報銀行に求められるユースケース

その他、匿名加工以外のデータ流通において求められるデータ変換・加工技術として、「秘密計算」、「クレンジング」、及び「仮名加工」が想定されるため、それぞれにおける情報銀行の強みや、想定されるユースケースを取りまとめた（表 3-34 参照）。

表 3-34 情報銀行によるデータ変換・加工に関するユースケース一覧（匿名加工以外）

No	ケース	①データ提供元	②収集データ	③情報銀行の役割	④データ提供先	⑤データ活用内容	⑥情報銀行の強み
1	秘密計算	医療機関 調剤薬局	医療データ 健診データ レセプトデータ 処方箋に関する情報	秘密計算	研究機関 製薬会社	新薬・新サービスの開発 学術的研究　等	秘匿された情報のみ取得し、秘密計算による分析結果のみをデータ提供先企業に提供することにより、消費者がより安心できるモデルとなる。
2	クレンジング	小売業者 クレジットカード会社 ポイントカード会社 各種 EC サイト　等	ポイントカード利用購買履歴 クレジットカード利用履歴	クレンジング	メーカー 卸業者 小売業者	消費者に対するタイムリーで最適な情報提供	複数のクレジットカード会社、ポイントカード会社、各種 EC サイト等からデータを収集できても、購買情報に格納されている企業名、顧客氏名、住所、商品名等に表記ゆれが生じていた場合、情報の一元管理ができない。そのため、クレンジングにて表記ゆれを訂正することにより、購買行動が整理された状態でのデータ提供が可能となる。
3	仮名加工	同上	同上	仮名加工 仮名加工情報の分析	―	―	仮名加工情報は第三者提供できないが、仮名加工情報を基に、情報銀行自体の改善、新サービス開発のための分析を行うことは可能である。

3.4.6. データカタログ・履歴情報の共有方法

3.4.2.にて述べた 2 種類のメタデータのうち、データの説明はパーソナルデータに付与して情報銀行間で連携される一方、データカタログはパーソナルデータに付与されるものではなく、単独で情報銀行間で連携されるメタデータとなる。このデータカタログに関する情報銀行間で共有する仕組みについて検討した。

また、3.4.1 や 3.4.3 でデータ項目や構造について定義した履歴情報について、消費者に包括的なトレーサビリティを提供するために適した共有の仕組みの実装方法を検討した。

3.4.6.1. データカタログの共有における検討内容・方法

データカタログを情報銀行間で共有することによって、お互いの情報銀行が取り扱う基本個人情報等を確認することができる。情報銀行間でのデータカタログの共有が必要となるケースとしては以下等が想定される。

① 共有先情報銀行の選定時
情報銀行が、データ共有先として他の情報銀行を選定するにあたって、他のそれぞれの情報銀行が取り扱うデータに取得したいデータがあるか等を確認する。

② 情報銀行Ａから情報銀行Ｂへの開示請求時
消費者からのデータ開示請求の委任を受けた情報銀行Ａが情報銀行Ｂに対して開示請求を行う際に、情報銀行Ａは情報銀行Ｂのデータカタログを確認した上で、消費者に情報銀行Ｂが保有するデータ項目のうち、開示を依頼する項目を選択させる。

情報銀行は、情報銀行事業の運営を開始するにあたり、取り扱う基本個人情報や同意情報に定義されている項目等をメタデータとしてデータカタログに記録する。その更新は、情報銀行にて取り扱う基本個人情報や同意情報に定義されている項目が変更された場合等に行うと想定される。そのため、更新頻度はそれ程高くはないと想定される。

これらを踏まえ、データカタログの共有の仕組みを実装する方法について、検討を行った。

企業間などで情報を共有するためのサービス・技術として一般的なものを調査し、それぞれの採用にあたってのフィージビリティを整理した。

一般的なデータ共有技術・サービスとしては、以下のクラウドストレージ(法人向け）、バージョン管理サービス、ファイル検索システム、ブロックチェーンを利用したシステムが挙げられる（表 3-35 参照）。

表 3-35 各種データ共有技術・サービスの特徴、メリット、デメリット

データ共有技術・サービス	特徴	具体的なサービス	メリット	デメリット
クラウドストレージ（法人向け）	・オンラインで利用可能なファイル共有サービス ・主に有償。個人向けのクラウドストレージと比べ容量が大きく履歴管理等の機能を有する。	・Box ・OneDrive ・AmazonS3 等	・インターネットがつながればマルチプラットフォームで利用可能。 ・2 段階認証等のセキュリティに関する機能を具備。 ・サポート体制を有している。 ・利用可能な容量や人数が多い（プランによる）。	容量や利用人数、利用したい機能によってコストが高くなる。

バージョン管理システム	• Git 等のバージョン管理システム • 変更履歴を管理する分散型のシステム	• GitHub 等	• インターネットがつながればマルチプラットフォームで利用可能。 • 複数のリポジトリを簡単に作成可能。 • データの変更点がわかりやすく共有可能。	Git の予備知識が必要
データカタログ検索システム	• データ検索システム • データに対応するメタ情報（作成日時、カテゴリなどのタグ、説明文等）を紐づけメタ情報での検索可能。	■オープンソース • CKAN • Fess ■クラウドサービス • Google Cloud Data Catalog • Azure Data Catalog	紐づけられたメタ情報でデータの検索が可能。	• オープンソースの CKAN や Fess であれば、構築作業が必要。 • クラウドサービスの Google Cloud Data Catalog や Azure Data Catalog であれば有料。
ブロックチェーンを利用したデータ管理システム	• 分散型台帳技術 • データの改竄に強いデータ構造でセキュリティ性が高い。	Hyperledger Fabric 等	• 改竄が困難であり、改竄されたときに検知も容易。 • 分散型なので一部の機器が故障してもサービスの継続が可能。	• 記録したデータを削除することはできない。 • ブロックチェーンの構築が必要。

これらのデータ共有技術・サービスについての、データカタログを共有する際のフィージビリティ評価にあたっては、データカタログを情報銀行が検索しやすいかといった検索性、データ連携を行う情報銀行のみがデータカタログが共有できるようにするためのデータ公開権限設定のしやすさ、更新頻度はそれ程高くないことが想定されるデータカタログについて、コストを抑えて共有の仕組みが構築できるかといった、3 つの観点で評価した（表 3-36 参照）。

表 3-36 データ共有技術・サービスのデータカタログの共有に関するフィージビリティ評価

データ共有技術・サービス	データカタログの共有とのフィージビリティ評価			評価結果※
	検索性	データ公開権限設定	コスト	
クラウドストレージ（法人向け）	× 検索性を高めるための機能を実装する必要がある。	○ ファイルごとの公開設定の仕組みが用意されている。	△ クラウド利用料が必要	8 点
バージョン管理	× 検索性を高めるための機能を実装する必要がある。	○ ファイルごとの公開設定の仕組みが用意されている。	○ オープンソースであり、安価な構築・運用可	10 点
データカタログ検索システム	○	○ ファイルごとの公開設定の仕組みが用意されている。	○ オープンソースであり、安価な構築・運用可	15 点

	紐づけられたメタ情報でデータの検索が可能であり検索性が高い。			
ブロックチェーンを利用したデータ管理システム	× 検索性を高めるための機能を実装する必要がある。	× 秘密鍵・公開鍵を用いた権限設定を構築する必要がある。	× 構築・運用コストが高い。	0 点

※評価結果:〇5 点、△3 点、×0 点にて算出

これらのフィージビリティ評価の結果、データカタログの共有の仕組みを実装する方法として、データカタログの項目で検索することができ、情報銀行が取得したいデータカタログの検索が行うことが可能な「データカタログ検索システム」を採用することを推奨する。

さらに、「データカタログ検索システム」には「CKAN」、「Fess」、「Google Cloud Data Catalog」、「Azure Data Catalog」といったソリューションがあるが、その中でも「CKAN」の利用を下記の理由で推奨する。

- 自治体の公共データを公開している実績がある。
- オープンソースである。
- データに対応する「メタ情報」（作成日時、カテゴリなどのタグ、説明文など）を紐づけ、メタ情報で検索することが可能。
- 「CKAN」は公開したいデータ（データセットという）に複数のファイル、メタデータを紐づけることが可能。

3.4.6.2. 履歴情報の共有における検討内容・方法

消費者によるトレーサビリティを確保するため、どの情報がどの情報銀行にいつ連携されたかを消費者が確認できる手段が必要である。

消費者本人が複数の情報銀行で自身のパーソナルデータがどのように利活用されているかを確認できるようにする方法の 1 つとして、各情報銀行がパーソナルデータを第三者提供した際の履歴を保有した上で、その履歴を情報銀行間で共有し合い、消費者に開示する方式が想定される。

また、履歴情報は、消費者ごとにデータの取得や提供といったアクションが発生する都度追加されるため、登録される頻度は高いが、一度登録した情報は変更されることはない、といったデータとしての特徴を踏まえて管理及び共有方法を検討する必要がある。

消費者本人が履歴を確認する手段を情報銀行が提供できるように、どのような仕組みが必要か、各情報銀行が保有する履歴データをどのように管理すべきか、について検討した。

データの管理方式としては、以下の 3 つが想定される。

① 中央集中管理方式

一か所に履歴を集めて管理する方式。消費者は、集中管理された履歴データを確認する（図 3-28 参照）。

② 分散管理方式 1（連携し合う各情報銀行が個別管理）

各情報銀行が互いに履歴データを連携し合い、各情報銀行が独自に管理する方式。消費者は、必要に応じて、自身が利用する情報銀行で履歴を確認する（その情報銀行が直接関わったデータ連携に関する履歴データの確認が可能）（図 3-29 参照）。

③ 分散管理方式 2（連携し合う情報銀行で共同管理）

ブロックチェーンなどを使って履歴を連携し合う情報銀行で共同管理する方式。消費者は、必要に応じて、自身が利用する情報銀行で履歴を確認する（どの情報銀行からでも同一の履歴データの確認が可能）（図 3-30 参照）。

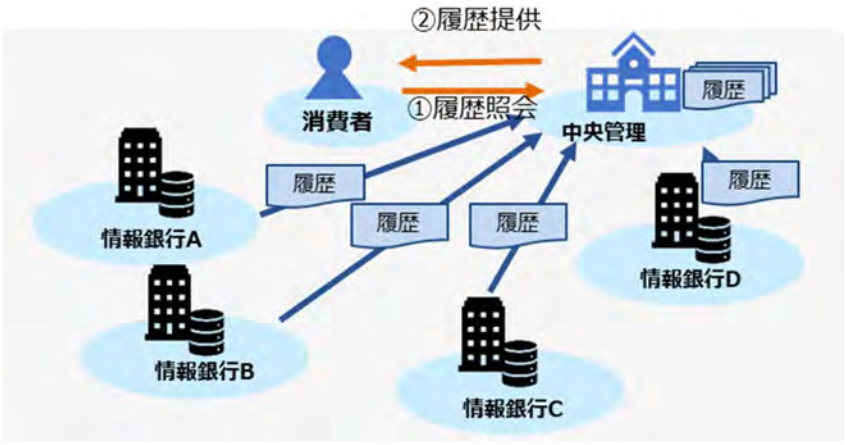


図 3-28 ①中央集中管理方式イメージ

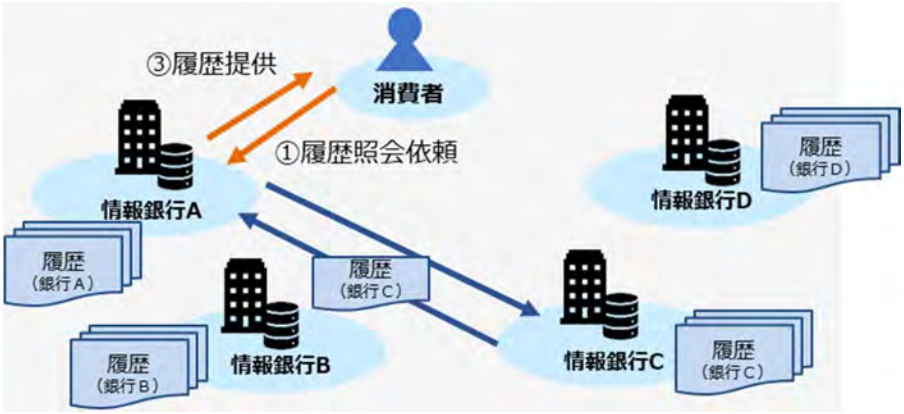


図 3-29 ②分散管理方式 1（連携し合う各情報銀行が個別管理）イメージ

図 3-30 ③分散管理方式 2（連携し合う情報銀行で共同管理）イメージ

これらのデータ管理方式について、様々な観点で評価した結果を以下の表 3-37 に示す。

表 3-37 履歴データの管理方式に関する評価

履歴データの管理方式	評価基準							評価結果※
	消費者の利便性（包括的トレーサビリティ実現）	改竄防止	漏洩防止		情報銀行の運用負担		早期実現性	
			漏洩対策のしやすさ	漏洩時の影響度	連携する情報銀行が一定時	連携する情報銀行の増加時		
①中央集中管理方式	○ 情報銀行とは別のサイトを見る必要があるものの包括的に履歴確認可能。	△ 第三者からの改竄リスクあり（暗号化など改竄防止策を別途講じる必要あり）。内部の改竄リスクは低い。	○ 特定機関 1 か所での対策となり対策しやすい。	× 管理情報を集中しているため、漏洩時の被害は大きい。	○ 特定機関が情報銀行に代わって運用するため負担少。	△ 特定期間において中央での履歴の追加等、負担が大きくなるものの情報銀行における負担は大きくない。	△ 特定の機関の設立にあたっての調整に時間を要するものの、共通基盤となるソリューションは既に登場してきている。	25 点
②分散管理方式 1（連携し合う各情報銀行が個別管理）	△ 自情報銀行以外の履歴は報銀行間で消費者の ID を紐づけたもののみ表示。	△ 第三者からの改竄リスクは高くないが自情報銀行内の改竄リスクあり。	△ 対策が各情報銀行に分散され統制が難しい。	△ 管理情報が分散しているため、漏洩時の被害は限られる。	× 各情報銀行が実施するため、運用負担は大きい。	○ 連携する情報銀行が増加した場合であっても負担はあまり変わらない。	○ 情報銀行間でのインターフェース仕様の調整の他は大きな開発は不要なため早期に実現可。	23 点

③分散管理方式 2（連携し合う情報銀行で共同管理）	△ 同上	○ 改竄することが困難であり、もし改竄されたときに検知が容易。	○ 秘密鍵・公開鍵の仕組みにより漏洩を防止。	× 秘密鍵の漏洩等により復元された場合の被害は大きい。	△ 改竄防止、漏洩防止に係る安全管理対策等の運用負担が②よりも少ない。	○ 連携する情報銀行が増加した場合であっても負担はあまり変わらない。	△ 構築の難易度が高く、各情報銀行間での調整、設計、開発にやや時間を要する。	25 点

※評価結果:○5 点、△3 点、×0 点にて算出

3 つのデータ管理方式は、評価観点によって一長一短あるが、評価結果としては大きな差はなく、①中央集中管理方式と③分散管理方式 2（連携し合う情報銀行で共同管理）がやや高い結果となった。

①中央集中管理方式を目指す場合、早期実現性を重視するのであれば、特定機関の設立を待たず、既に提供されている共通基盤となるソリューションの活用も有効であると考える。

また、③分散管理方式 2（連携し合う情報銀行で共同管理）を目指す場合は、まずは②分散管理方式 1（連携し合う各情報銀行が個別管理）を早期に実現した上で、連携し合う情報銀行での共同管理に向けた各情報銀行間での調整等の準備を進めていくことが良いと考える。分散管理方式 2（連携し合う情報銀行で共同管理）の実現のさらに将来は、履歴データだけでなく、消費者の ID についても特定の情報銀行が発行するのではなく、分散して管理することで、消費者が自身のデータを自身でコントロールすることがより可能となる。

但し、履歴データは消費者がいつ、どこにデータを提供したかといった履歴に関する情報であり、提供したパーソナルデータそのものは含まれないが、多くのデータの提供履歴を読み解くことで個人を特定できる可能性もあるため、情報漏洩防止などの安全管理対策は十分に実施すべきと考える。また、本実証事業では、履歴情報の実現方式として 3 種類を挙げ、簡易な評価は行ったものの、履歴情報の改竄による影響度、技術の陳腐化等の可能性、情報銀行ビジネス上の観点等も加味し、より深く検討した上で選択することが望ましいと考える。

3.4.7. データ形式に関する今後の課題と対応

情報銀行間連携におけるデータ定義ついて、今後の更なる普及、促進に必要と思われる検討・取り組みとして下記が挙げられる。

共通データ項目の定義対象・範囲の拡充

本実証事業では、17 の業界のトップ企業のウェブサイト等の公知情報を確認し、各社が収集している個人情報を調査した上で、基本情報のデータ項目を定義した。今後は、基本情報のデータ項目の拡充はもちろん、健康に関するデータなど、サービス事業者からのデータ活用ニーズが高いデータ項目について、共通データ項目として定義していくことが必要である。

複数要素を連結して保有しているデータへの対応

基本情報のデータ項目の 1 つとして定義した氏名について、外国人も想定し、項目としてミドルネームを設定・定義したが、ミドルネームへの対応は各企業によって様々であり、姓や名に連結して保有されていることが多い。また、住所においても、丁目番地に建物名を連結して保有している企業などもある。

本定義では氏名や住所に関する分割項目は必須としていないが、既に各企業が保有しているデータを流通させ、利活用しやすくする目的で分割項目にも対応しようとすると、切り分け処理等の変換が必要になるため、実態に即した対応方法の検討が必要になる。

各情報銀行で保有するマスタ情報の紐づけ負荷の軽減

各情報銀行において保有する利用制限マスタやスコープマスタ等の各種マスタ内の情報は、情報銀行によって定義が異なるため、情報銀行間でデータ連携するには、事前にデータ連携元とデータ連携先のマスタ内の情報を紐づけておく必要がある。

現状、これらのマスタ情報の紐づけはデータ連携元とデータ連携先で個別調整する必要がある。今後、情報銀行が増加した際や、マスタ情報の種類や内容のバリエーションが増えた際に、対応負荷の増大が予想される。そのため、そもそも紐づけが不要になるように連携し合う情報銀行間でマスタ情報を共通化したり、データ連携時に共通プラットフォームを利用したり、といったマスタ情報の紐づけ負荷を軽減する対策が必要になる。

情報銀行間で不変な共通ユーザー識別子を保有する是非

本実証事業では、各情報銀行が管理する固有のユーザー識別子を基本情報に保有する仕様となる。その上で、情報銀行間でデータ連携する際は、消費者の同意の元、同一人として各行固有のユーザー識別子を紐づける仕様にしており、不変な共通ユーザー識別子を保有する仕様にはしていない。そのため、誤った紐づけがなされたり、各行に分散して保有された情報が個別に更新されたり、情報の鮮度の違いよって差異が発生したり、といったことが度重なることで、情報の真偽が判別できなくなったり、不整合が生じたり、といったリスクがある。そのリスク軽減策として、情報銀行間で不変の共通ユーザー識別子を基本情報に保有し、消費者個人を一意に識別できるようにする管理方法が考えられる。例えば、公的個人認証サービスの電子証明書に紐づく共通ユーザー識別子を採用すれば、不整合リスクが抑えられることはもちろん、特定企業による囲い込み防止や、行政手続きと民間手続きとの連携・ワンストップ化の実現など、サービス品質向上への道が開かれる可能性もある。但し、消費者個人の多様な情報を不整合なく統合し、トレースしやすくなるということは、プライバシー上の懸念もあるため、慎重に検討する必要がある。

3.5. 情報銀行サービスの提供に関わる事業者に求められるデータ連携時に必要な「機能・ルール」

情報銀行間でデータ連携を行う主なユースケースを検討・想定した上で、必要となる基本的な機能・ルールについて検討を行った。

また、検討に際して、データ流通の普及・促進を妨げる大きな要因の一つになっている消費者不安を低減する対策として、消費者が連携データに関する利活用状況の把握や制御に必要な機能・ルールに着目し、以下に示す 6 つの観点（表 3-38、表 3-39、表 3-40、表 3-41、表 3-42、表 3-44 参照）で検討した。

なお、それぞれの機能・ルールに関する詳細については、3.5.1～3.5.7 にて記載している。

表 3-38 連携データの目的外利用を抑止するために、連携データ利活用状況をチェックする機能・ルール

	課題	対応	
		機能/ルール	対応内容
1	情報銀行、データ提供先、再提供先が取得したデータの利用履歴に関する消費者開示	機能・ルール	情報銀行、データ提供先、再提供先が取得したデータの利用履歴についての消費者への開示の必要性について検討を行った結果、単純に利用履歴を開示するのではなく、事業者が目的外利用を行わないために、どのような対策を行っているかを、消費者に対して開示するルールを設けることとした。 また、第三者提供の同意時に、利用期間を明示して合わせて同意することで、消費者により安心感を与えることができると考え、利用期限に関する機能・ルールを定めた。
2	データ提供先が利用目的を明示する際の利用目的の明確化	ルール	データ提供先が利用目的を明示する際の利用目的の明確化について指針がないことから、利用目的は消費者が容易に理解できるようにすることをルールとして定めた。
3	情報銀行によるデータ提供先・再提供先に対する適切なデータ利用の確認・監督	ルール	データ提供先・再提供先の目的外利用を抑止するための対策を行うとともに、それらを情報銀行が確認・監督を行うためのルールを定めた。

表 3-39 消費者が同意した利活用目的に必要なデータのみを選択提供・連携する機能・ルール

	課題	対応	
		機能/ルール	対応内容
1	利用目的に応じた第三者提供先へのデータの選択提供	機能	情報銀行が消費者より第三者提供先へのデータ提供の個別同意を得る際は、情報銀行は、提供先、利用目的ごとに必要となるデータ範囲を提供条件として提示し、選択できる機能の具備を定めた。

		ルール	情報銀行が消費者よりデータを取得する際、利用規約等に利用目的ごとに必要となるデータ項目を記載し、消費者に提示することをルールとして定めた。
2	データの秘匿性の度合いを可視化した提供方法	機能	個人情報の提供に関して、情報銀行が消費者から個別に同意を得る際、情報銀行が、提供先名称、その利用目的、提供するデータ項目を明示、選択する画面に、提供するデータ項目の秘匿レベルも併せて明示することを定めた。
3	取得データが利用目的の達成に必要であることの消費者説明	ルール	消費者からのデータ取得や、第三者へのデータ提供（再提供含む）にあたって、消費者からその同意を得る際は、当該データが利用目的の達成に必要であることの説明（どういった場合に、何のために、どの様に利用するか）を明示するルールを定めた。

表 3-40 消費者が同意撤回、利用停止・消去の申し出をした場合の各事業者における対応ルール

	課題	対応	
		機能/ルール	対応内容
1	データ提供先におけるデータ利用状況の消費者開示	機能	情報銀行が消費者に対して、データ提供先における保有データや保有データの利用状況を一覧表示することができる機能と、消費者が一度行った同意の撤回を行うことができる機能の具備を定めた。
		ルール	データ提供先が情報銀行を通じて、データの利用状況に関する情報を消費者に開示することと、消費者からの同意の撤回の申請に対して適切な対応をすることをルールとして定めた。
2	データ提供先から情報銀行へのデータ利用状況の報告	機能	データ提供先が、情報銀行に対して保有データや保有データの利用状況に関する報告を行う機能を具備することを定めた。
		ルール	データ提供先が情報銀行に対して保有データや保有データの利用状況に関して行う報告に関するルールと、紛争防止のために情報銀行とデータ提供先間で定めるべき契約条項に関するルール、匿名化・統計化、仮名化されたデータに対する消費者からの同意撤回の申請への対応に関するルール、契約に関する各事業者の負担を軽減するために各事業者の仲介機関となるプラットフォームを利用することを定めた。

表 3-41 信頼性の高い包括的なトレーサビリティを消費者へ提供するために必要な機能・ルール

	課題	対応	
		機能/ルール	対応内容
1	情報銀行が取得・提供したデータに関する包括的な閲覧履歴の消費者開示	機能	消費者が自己のデータの提供先・提供履歴を容易に確認できるよう、情報銀行が取得・提供したデータについて、包括的に項目を検索・一覧表示できる機能の具備を定めた。
		ルール	情報銀行が取得・提供したデータの包括的な消費者向け閲覧履歴の開示に向けて、以下をルールとして定めた。 ・ 消費者に対して、情報銀行が取得・提供したデータを包括的に検索・一覧表示できる機能を提供する者は、認定指針 ver2.0 にて「情報信託機能の認定基準」に定められている条件を満たす者であること。 ・ 情報銀行に預託されたデータについて、情報銀行間を跨って包括的に以下項目を検索・一覧表示できる機能を消費者に提供すること。 ・ 情報銀行及び情報銀行から第三者提供を受ける者は、取得・提供した消費者のデータにアクセスがあった場合、上記項目のデータを保存すること。

表 3-42 データ提供先事業者への情報提供に伴うリスク対策に必要な機能・ルール

	課題	対応	
		機能/ルール	対応内容
1	情報銀行のデータ提供先事業者としての適格性を判断するのに必要十分であり、かつ提供元となる情報銀行が適切な監督を実施できる基準	ルール	情報銀行から第三者提供を行う場合のデータ提供先事業者として必要十分であり、かつ提供元の情報銀行が適切な監督を実施できる基準（提供先が情報銀行ではない場合）を検討するにあたり、プライバシーマークの基準を中心として、改正個人情報保護法等の新たな規制への対応等も踏まえ、追加・変更等が必要と想定されるルールを定めた。 なお、本ルールは、データ提供先事業者が複数の情報銀行から認定を受ける際の共通の認定基準となることが望ましいと考える。

表 3-43 データポータビリティ、及び付随して必要になる改竄防止策、盗聴防止策に関する機能・ルール

	課題	対応	
		機能/ルール	対応内容
1	情報銀行を介したデータの移転に関する電子的な請求	機能	消費者がデータの移転を情報銀行に対して電子的に請求できる機能、消費者からのデータ移転の請求をデータ提供元に連携する機能、消費者が指定したデータ提供先に電子的なデータの移転を行う機能、データの移転の状況（移転中・移転完了等）を消費者に連携する機能の具備を定めた。
		ルール	情報銀行とデータ提供元事業者間、及び情報銀行間で、提供データの提供方法等に関するデータ移転に関する契約を締結することをルールとして定めた。
2	データの移転に関する請求を行う者が当該個人であることの確認	機能	データの移転請求の際に、第三者による不正な請求を防止するために、サービス利用者に対するオンラインでの本人確認機能とともに、情報銀行がデータの移転請求を行う者が消費者本人であることを確認するための本人認証機能を具備することを定めた。
		ルール	消費者によるデータ移転の請求依頼を受け付けるにあたって、要配慮個人情報等の秘匿レベルの高い情報を収集する可能性を考慮し、犯罪収益移転防止法規定の本人確認を行うことと、本人認証の必要性・厳格性について検討し、採用の要否の判断をすることを推奨ルールとして定めた。
3	データの移転時における盗聴防止	機能	データ移転時の第三者による盗聴を防止するための通信データの暗号化を行う機能の具備を定めた。
		ルール	情報銀行及びデータ提供元/データ提供先間で、データの盗聴があった場合に備え、責任及び損害等の負担に関する項目（責任や損害賠償を負担する/しない条件等を明記）を契約に盛り込むこと、API を通じてデータを移転する場合は OAuth 2.0 等によって、API セキュリティを担保することを推奨ルールとして定めた。
4	データの移転時における改竄防止	機能	データの改竄を防止するために、通信データの暗号化を行う機能と、電子署名技術等を用いた改ざん防止機能、消費者がデータ提供元に対して訂正の申請を実施できる機能、情報銀行等がデータクレンジングや結合を行うことができる機能の具備を定めた。

		ルール	本人及び代理人によるデータの訂正を禁止し、データの作成者（データ提供元）のみが正しいデータ等へデータを修正できるものとすることと、情報銀行によるデータ加工（クレンジング・結合）後のデータ提供方法に関する契約を締結することを定めた。

3.5.1. 情報銀行間連携のユースケースと必要な機能・ルール

情報銀行間のデータ連携時に必要な機能・ルールを検討するにあたり、消費者の同意の元、情報銀行間でデータを連携する主なユースケースにおける手続きやデータの流れを検討した。

検討したユースケースは、以下の消費者同意に基づく情報銀行による第三者提供パターンの 2 つと、開示請求（データポータビリティ）パターンの 1 つとなる。

第三者提供パターン

- ユースケース①:消費者の同意に基づき情報銀行 A が情報銀行 B からデータ取得する
  消費者が新たに情報銀行 A を契約・利用するにあたり、契約済の情報銀行 B が保有している消費者のデータを、消費者の同意に基づき情報銀行 A が情報銀行 B から取得する。
- ユースケース②:消費者の同意に基づき情報銀行 A が情報銀行 B からデータ提供を受ける
  消費者が契約済の情報銀行 B 対して、同じく契約済の情報銀行 A へのデータ提供に同意し、情報銀行 A が情報銀行 B からデータ提供を受ける。

開示請求（データポータビリティ）パターン

- ユースケース③:消費者の代理となり情報銀行 A が情報銀行 B からデータ開示を受ける
  消費者が新たに情報銀行 A を契約・利用するにあたり、情報銀行 A に対して、既に契約済の情報銀行 B へのデータ開示の代理請求を依頼し、情報銀行 A は開示請求先の情報銀行 B からデータ開示を受ける。

なお、いずれのユースケースにおいても、データ提供先となる情報銀行 A に対して、データ提供元となる情報銀行 B からデータを提供する形態を前提とする。これを踏まえ、本書の以下の説明文中では、消費者が元々情報信託したデータ提供元となる情報銀行 B から直接的にデータ連携する事業者を「提供先」とし、情報銀行 B のデータ提供先の一つになる情報銀行 A を介して間接的にデータ連携する事業者を「再提供先」とした。

3.5.1.1. ユースケース①:消費者の同意に基づき情報銀行 A が情報銀行 B よりデータ取得する

消費者が新たに情報銀行 A を契約・利用するにあたり、既に契約済の情報銀行 B の保有している消費者のデータを情報銀行 A へデータ提供することを消費者が指示し、情報銀行 A がデータ取得する。本ユースケースは、消費者が新たに情報銀行 A を契約・利用するにあたり、既に情報銀行 B で登録した情報（消費者が預託したデータや、第三者提供に関する同意条件等）を極力引き継いだかたちで情報銀行 A に登録するような流れとした。
以下（図 3-31 参照）を推奨フローとする。

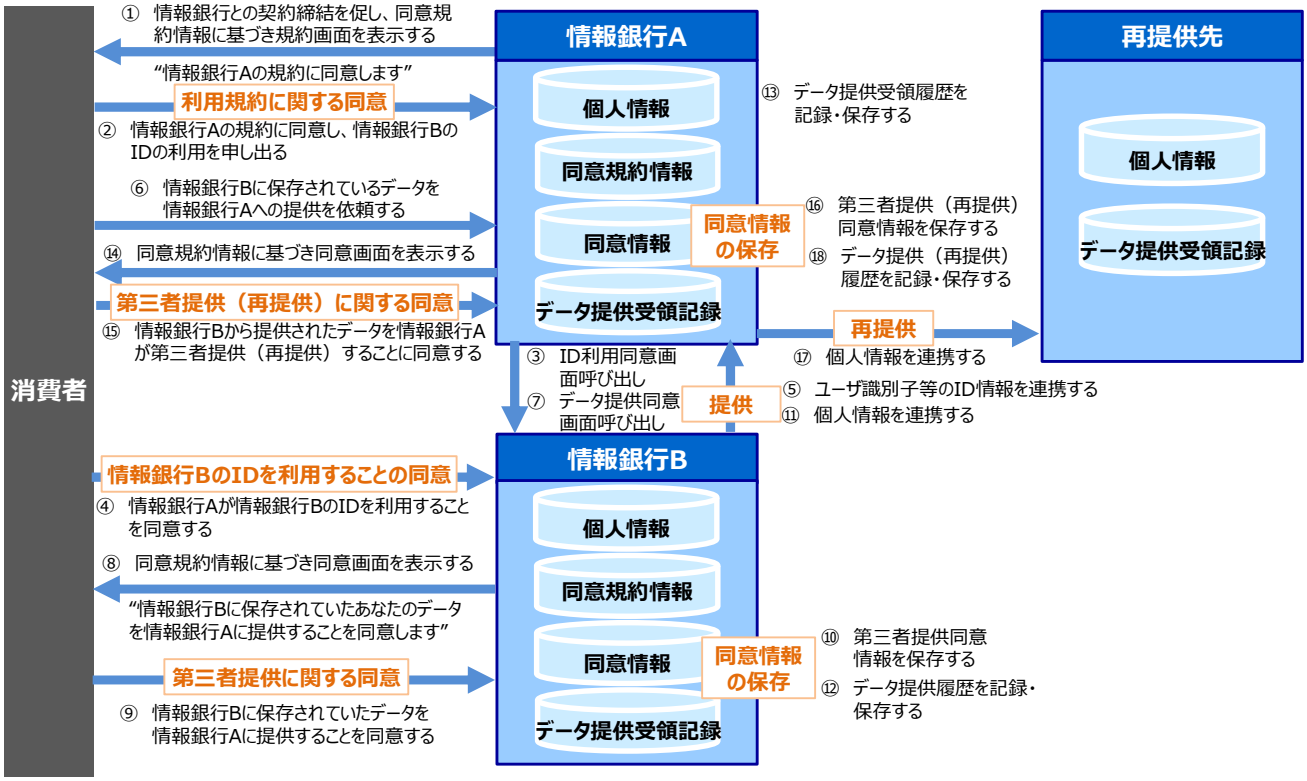


図 3-31 ユースケース①:消費者の同意に基づき情報銀行 A が情報銀行 B よりデータを取得する際の推奨フロー

3.5.1.2. ユースケース②:消費者の同意に基づき情報銀行 A が情報銀行 B よりデータ提供を受ける

消費者が契約済の情報銀行 B に対して、契約済の情報銀行 A へのデータ提供を同意した上で、情報銀行 B は情報銀行 B へデータ提供する。本ユースケースは、消費者が情報銀行 B に預託済のデータの第三者提供先の 1 つが情報銀行 A であることを想定したものとなる。以下（図 3-32 参照）は、個別同意によるデータ提供の場合における推奨フローとなる。

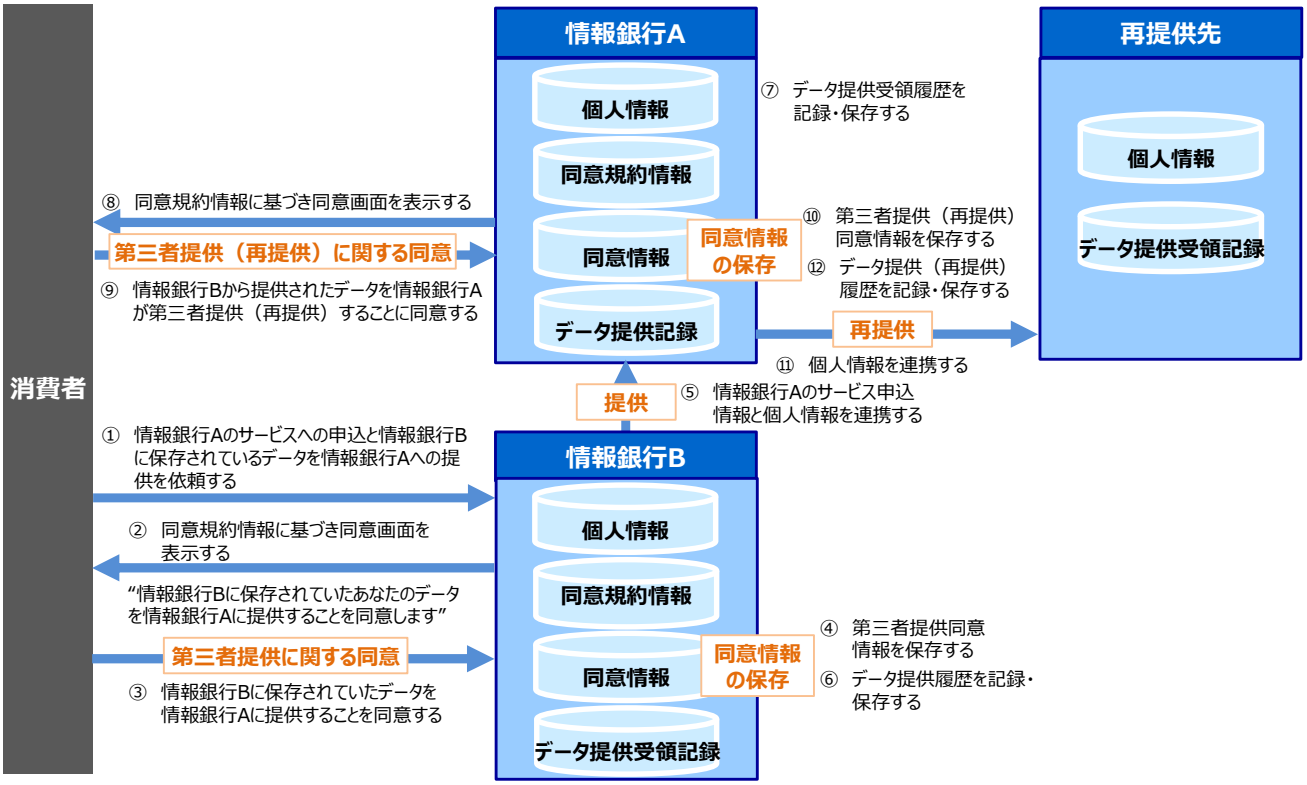


図 3-32 ユースケース②:消費者の同意に基づき情報銀行 A が情報銀行 B よりデータ提供を受ける際の推奨フロー

3.5.1.3. ユースケース③:消費者の代理となり情報銀行 A が情報銀行 B よりデータ開示を受ける

消費者が新たに情報銀行 A を契約・利用するにあたり、情報銀行 A に対して、既に契約済の情報銀行 B へのデータ開示の代理請求を依頼し、情報銀行 A は開示請求先の情報銀行 B よりデータ開示を受ける。本ユースケースは、改正個人情報保護法によって、事業者が保有している個人データの開示方法について、電磁的記録の提供を含め、消費者が指示できるようになることを想定し、情報銀行 A が消費者の代理となって、情報銀行 B の保有しているデータを紙媒体ではなく電子データとして開示を求めるものとなる。その際の推奨フローは以下（図 3-33 参照）となる。

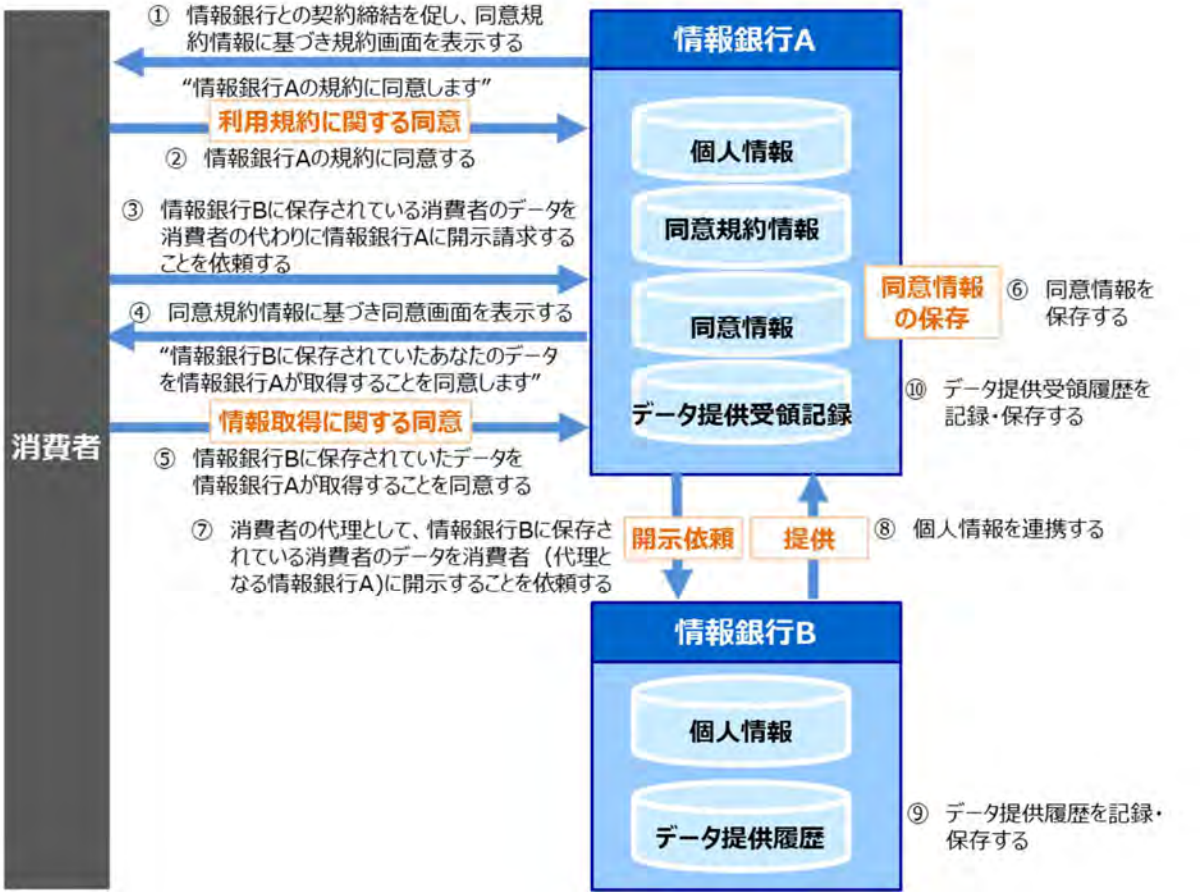


図 3-33 ユースケース③:消費者の代理の情報銀行 A が情報銀行 B よりデータの開示を受ける際の推奨フロー

3.5.1.4. 情報銀行間連携のユースケースにおける機能・ルール

情報銀行間でのデータ連携の際は、以下のルール（表 3-44 参照）を推奨する。

表 3-44 情報銀行間でのデータ連携に関するルール

区分（推奨/必須）	対象	ルール
推奨	情報銀行	第三者提供に関する同意 • 情報銀行は、他の情報銀行に個人情報を提供する場合であっても、消費者の同意を得ること。（オプトアウト方式の禁止） • 個人情報の提供元となる情報銀行は、上記の同意を得るにあたって、提供先となる情報銀行名、提供する個人情報の項目、提供先となる情報銀行における利用目的を消費者に明示すること。 • 他の情報銀行に提供する個人情報については、消費者がその範囲を選定できるようにすること。 • 認定指針 ver2.0 では、情報銀行から個人情報の提供を受けた事業者が第三者に当該個人情報を提供する場合、再提供とみなされ、原則禁止となっている。但し、個人情報の提供先は情報銀行であることから、再提供することが前提となると想定されるため、情報銀行は、認定指針 ver2.0 に記載された再提供の原則禁止の例外条件を満たすこと。 • 上記例外条件には、再提供先への第三者提供について、消費者の同意を得ることとなっているが、同意を得る際は、再提供先の利用目的を消費者に明示するとともに、利用目的は消費者が容易に理解できるようにすること。 • 消費者が契約済の情報銀行（情報銀行 B）で同意した第三者提供に関する条件に関する情報について、消費者が他の情報銀行（情報銀行 A）への提供を同意した場合は、次の通りとする。 情報提供を受ける情報銀行（情報銀行 A）は、消費者との契約締結後に初めて消費者から第三者提供に関する同意を得る際、情報銀行（情報銀行 B）より受領した第三者提供に関する条件を初期表示させるとともに、条件の変更が可能な仕組みを提供すること。 • 上記の第三者提供に関する条件の初期表示にあたって、本実証事業で定義する共通仕様に則った上で、予め連携し合う情報銀行間で条件の選択肢の対応付けルールを定めておくこと。必ずしも連携し合う情報銀行間で条件の選択肢を完全に一致させておく必要はない。

推奨	情報銀行	利用規約に関する同意 • 情報銀行は、サービスに関する規約について消費者の同意を得ること（情報銀行から個人情報の提供を受けた情報銀行も同様）。 • 利用規約には、情報銀行間で連携を行うために必要となる消費者固有のユーザー識別子を連携先の情報銀行に対して提供することを記載し、あわせて同意を得ること。また、予め連携を行う情報銀行間で連携に関する取り決めについての契約を締結するにあたり、ユーザー識別子の連携元の情報銀行以外の情報銀行から取得したデータと組み合わせて個人を識別してはならないことを契約書に明記しておくこと。 • 利用規約に関する同意の際に、合わせて個人情報を取得する場合は、情報銀行は、取得する個人情報の項目、利用目的を明示し同意を得ること。これらは、サービスに関する規約の中に含めても良い。 • 他の情報銀行から個人情報の提供を受ける場合、提供を受ける前に、情報銀行は、サービスに関する規約について消費者の同意を得て、契約を締結すること。

3.5.2. 連携データの目的外利用を抑止するために、連携データの利活用状況をチェックする機能・ルール

個人情報保護法によって、本人同意なしでの連携データの目的外利用は認められていないものの、消費者にとっては、提供した自身のデータが目的外利用されているのではないか、目的外利用によって何らかの不利益が生じるのではないか、といった不安があるものである。連携データの目的外利用を抑止し、消費者の不安を解消するため、データ提供先におけるデータ利活用状況を消費者や情報銀行がチェックする仕組み等が求められる。以下（図 3-34 参照）の通り、それらの仕組みの実現にあたって必要となる機能・ルールの検討を行う。

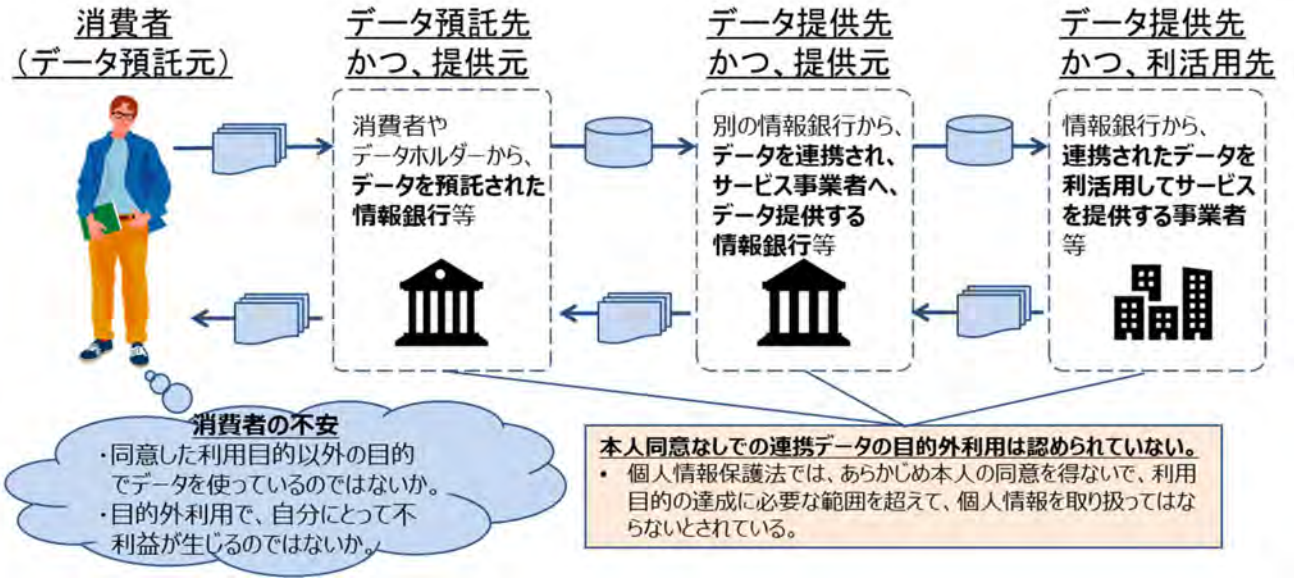


図 3-34 連携データの目的外利用に関する消費者の不安

3.5.2.1. リスクの可視化・深掘り

データ利活用状況の把握や制御に必要な機能・ルールが整備されていない環境下における、連携データの目的外利用に関するリスクをステークホルダーごとに洗い出し、それらのリスクに対する現状の機能・ルールを調査した上で、今後あるべきルールや機能提供を行うにあたっての課題についての検討を行った。

また、連携データの目的外利用については、「情報銀行に提供したデータの目的外利用」、「情報銀行が第三者提供したデータの目的外利用」、「データ提供先が再提供したデータの目的外利用」の 3 つの観点でそれぞれ整理した。

なお、再提供（データ提供先がさらに別の第三者にそのデータを提供すること）については、認定指針 ver2.0 では、原則禁止ではあるが、一定の条件を満たす場合可能となっている。

＜連携データの目的外利用に関するリスクと課題（情報銀行に提供したデータの目的外利用）＞

ステークホルダーごとのリスク

消費者:

- 情報銀行に提供したデータの目的外利用、及びそれらの不安を抱えること

情報銀行:

- 消費者が情報銀行によるデータの目的外利用について不安を抱えることによる利用の抑制
- 目的外利用発覚時の信頼低下
- 損害賠償

データ提供先:

- (特になし)

リスクに対する現状の機能・ルール

取得タイミング:

- 情報銀行が消費者からデータを取得する際、取得するデータ項目、利用目的を約款等で明示し、消費者の同意を得ることとなっている（認定指針 ver2.0）。
- 情報銀行によるデータ取得の際の利用目的の明示の際、利用目的が具体的であることが求められている（個人情報保護法）。

利用タイミング:

- 個人情報取扱事業者は、あらかじめ本人の同意を得ないで、利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならないとなっている（個人情報保護法　第十六条）。
- 情報銀行が取得したデータの情報銀行による利用についての記録作成に関するルールはない。
- 情報銀行が取得したデータの情報銀行による利用記録についての消費者への開示ルールはない。

ルール化・機能提供に関する課題

取得タイミング:

- (特になし)

利用タイミング:

- 情報銀行が取得したデータの情報銀行による利用履歴についての消費者への開示

＜連携データの目的外利用に関するリスクと課題（情報銀行が第三者提供したデータの目的外利用）＞

ステークホルダーごとのリスク

消費者:

- 情報銀行が第三者提供したデータの目的外利用、及びそれらの不安を抱えること

情報銀行:

- 消費者がデータ提供先によるデータの目的外利用について不安を抱えることによる利用の抑制
- 情報銀行が第三者提供したデータの目的外利用が発覚した際の信頼低下
- 個人に対する説明責任、損害賠償

データ提供先:

- 目的外利用発覚時の信頼低下
- 消費者又は情報銀行に対する損害賠償

リスクに対する現状の機能・ルール

取得タイミング:

- 情報銀行が第三者提供に係る条件について、提供先第三者、その利用目的及び第三者提供の対象となる本個人情報の項目または、それらについての判断基準及び判断プロセス、のいずれかについて、消費者に通知の上、消費者から予め同意を取得するものとなっている（認定指針 ver2.0）。
- データ提供先へのデータ提供時の利用目的の明示の際の、利用目的の明確化について定めたルールがない。

利用タイミング:

- データ提供先が取得したデータのデータ提供先による利用についての記録作成に関するルールはない。
- データ提供先が取得したデータのデータ提供先による利用記録についての消費者への開示ルールはない。
- 情報銀行によるデータ提供先のデータ利用状況の確認に関するルールはない（但し、認定指針 ver2.0 では、情報銀行に対して、「どのデータがどこに提供されたのかという履歴を閲覧できるユーザーインターフェースを提供すること」、「提供の日時、提供されたデータ項目、提供先での利用状況など、履歴の詳細を提供する場合は、その旨を明示すること」とのルールはある。）。

ルール化・機能提供に関する課題

取得タイミング:

- データ提供先による利用目的の明示の際の、利用目的の明確化

利用タイミング:

- データ提供先による利用履歴についての消費者への開示
- 情報銀行によるデータ提供先のデータ利用の確認・監督

＜連携データの目的外利用に関するリスクと課題（データ提供先が再提供したデータの目的外利用）＞

ステークホルダーごとのリスク

消費者:

- 情報銀行が第三者提供したデータをデータ提供先が再提供した場合の目的外利用、及びそれらの不安を抱えること

情報銀行:

- 消費者がデータ再提供先によるデータの目的外利用について不安を抱えることによる利用の抑制
- データ提供先が再提供したデータの目的外利用が発覚した際の信頼低下
- 消費者に対する説明責任、損害賠償

データ提供先:

- 再提供したデータの目的外利用が発覚した際の信頼低下
- 消費者又は情報銀行に対する損害賠償

再提供先:

- 目的外利用が発覚した際の信頼低下

- 消費者又はデータ提供先、情報銀行に対する損害賠償

リスクに対する現状の機能・ルール

取得タイミング:

- 消費者とデータ提供先との間に契約が締結され、再提供先への第三者提供については、オプトインでの同意（個人情報保護法 第二十三条第一項）に基づき、提供先第三者が消費者から同意取得することとなっている（認定指針 ver2.0）。
- データ再提供先へのデータ再提供時の利用目的の明示の際の、利用目的の明確化について定めたルールがない。

利用タイミング:

- データ再提供先が取得したデータのデータ再提供先による利用についての記録作成に関するルールはない。
- データ再提供先が取得したデータのデータ再提供先による利用記録についての消費者への開示ルールはない。
- 情報銀行によるデータ再提供先のデータ利用状況の確認に関するルールはない。

ルール化・機能提供に関する課題

取得タイミング:

- データ提供先による利用目的の明示の際の、利用目的の明確化

利用タイミング:

- データ再提供先による利用履歴についての消費者への開示
- 情報銀行やデータ提供先によるデータ再提供先のデータ利用の確認・監督

これらの整理によって、洗い出した課題を整理すると、以下の 3 つに大別される。

- 課題①情報銀行、データ提供先、再提供先が取得したデータの利用履歴に関する消費者開示
- 課題②データ提供先が利用目的を明示する際の利用目的の明確化
- 課題③情報銀行によるデータ提供先・再提供先に対する適切なデータ利用の確認・監督

これらの課題に関する検討を行った。

3.5.2.2. 「課題①情報銀行、データ提供先、再提供先が取得したデータの利用履歴に関する消費者開示」に関する検討

情報銀行、データ提供先、再提供先が取得したデータについて、消費者が、情報銀行、データ提供先、再提供先においてデータをどのように利用したかを確認できる機能を提供することで、連携データの目的外利用の抑止につながるものである。

データ連携についての消費者向けの開示機能が充実している事例として、内閣府が市民向けに提供しているマイナポータル（行政手続の検索やオンライン申請や、行政からのお知らせを受け取ることができる専用サイト）が挙げられる。マイナポータルでは、行政機関間での市民の個人情報のやり取りについて、いつ、どういった目的で行われたか、を市民

自身が確認できる仕組みとなっている。但し、どういった事務手続きにおいて個人情報がやりとりされたかは確認できる（表 3-45 参照）ものの、実際の利用履歴を開示する仕組みではない。

表 3-45 マイナポータルのやりとり履歴詳細で表示される項目[6]

	項目	説明
1	整理番号	整理番号が表示されます。
2	状況	提供状況が表示されます。
3	やりとり履歴受信日時	やりとり履歴の提供決定を受信した日時が表示されます。
4	照会日時	行政機関等が、あなたの情報を照会した日時が表示されます。
5	照会機関	やりとり履歴を照会した行政機関等名が表示されます。
6	情報照会者部署名	あなたの情報を照会した部署名が表示されます。
7	提供日時	行政機関等が、あなたの情報を提供した日時が表示されます。
8	提供機関	あなたの情報を提供した行政機関等名が表示されます。
9	事務	あなたの情報がやりとりされた事務名が表示されます。
10	事務手続	あなたの情報がやりとりされた事務手続名が表示されます。
11	やりとりされた情報の名称	あなたの情報がやりとりされた情報の名称が表示されます。やりとりされた情報の名称を選択すると、特定個人情報等の項目表示が表示され、やりとりされた情報に含まれるすべての項目を確認できます。

利用履歴を開示する仕組みの実現にあたっては、データ提供を受けた事業者が、当該データを利用するごとに記録を行う必要があるが、記録にはかなりの負担がかかる。データ利用履歴の代替として、システムを介して当該データを参照した場合の、参照履歴を消費者に開示する方法も想定されるが、消費者が理解できるかたちに参照履歴を加工するなどの対応が必要となり、この場合も事業者の負担が大きくなる。

そのため、実効的な方法としては、利用履歴を開示するのではなく、事業者が目的外利用を行わないために、どのような対策を行っているかについて、消費者に対して開示することが望ましい。

但し、消費者にとっては、上記の対策の公表によって目的外利用への不安は軽減させるものの、消費者が自主的に対策について定期的に確認する負担が生じる。そのため、データ提供を同意する時点で、利用期間を設定し、当該期間を超えた際はデータ消去を行い、利用停止するといった方法により、消費者の負担なく目的外利用への不安を大幅に軽減することが可能となる。

[6] 出典:内閣府大臣官房番号制度担当室「マイナポータル」の「やりとり履歴詳細説明」
＜https://img.myna.go.jp/manual/03-02/k0057.htm＞（参照日 2021 年 2 月 17 日）

これらを踏まえ、目的外利用を行わないための対策に関する機能・ルールを以下のとおり定めた（表 3-46、表 3-47 参照）。

表 3-46 目的外利用を行わないための対策に関する機能

区分（推奨/必須）	対象	機能
推奨	情報銀行	消費者がデータ提供を同意する画面において、当該データの利用期間を示した上で同意する機能を具備すること。

表 3-47 目的外利用を行わないための対策に関するルール

区分（推奨/必須）	対象	ルール
推奨	データ提供を受けた事業者（情報銀行を含む）	ホームページやサービスアプリ等にてデータの目的外利用を行わないための対策を公表すること。 消費者が同意した利用期間を超えた際は、速やかにデータ消去を行い、利用を停止すること。

3.5.2.3. 「課題②データ提供先が利用目的を明示する際の利用目的の明確化」に関する検討

現在、情報銀行がデータ提供先にデータ提供するにあたって、消費者にデータ提供先におけるデータの利用目的を明示した上で、同意を得ているが、その際明示される利用目的の明確化について定めたルールが必要である。

2019 年 12 月に公正取引委員会が公表した「デジタル・プラットフォーム事業者と個人情報等を提供する消費者との取引における優越的地位の濫用に関する独占禁止法上の考え方」（2019 年 12 月 17 日公正取引委員会）において、優越的地位の濫用となる行為類型として、デジタル・プラットフォーム事業者が「利用目的を消費者に知らせずに個人情報を取得すること」を挙げている。その中で、消費者に利用目的を知らせるにあたっての、利用目的の記載内容や記載場所について、一般的な消費者が利用目的を理解することが困難な状況として、利用目的を消費者に知らせずに個人情報を取得したと判断される場合があるとし、具体的な例として、以下が挙げられている。

- 利用目的の説明が曖昧である、難解な専門用語によるものである。
- 利用目的の説明文の掲載場所が容易に認識できない。
- 利用目的の説明文が分散している。
- 利用目的の説明文が他のサービスの利用に関する説明と明確に区別されていない。

「デジタル・プラットフォーム事業者と個人情報等を提供する消費者との取引における優越的地位の濫用に関する独占禁止法上の考え方」は、デジタル・プラットフォーム事業者に向けた考え方ではあるが、情報銀行において、データ提供先による利用目的を明確に示すためのルール策定において参考になる。

これらを踏まえ、データ提供先による利用目的を明確に示すためのルールを以下のとおり定めた（表 3-48 参照）。

表 3-48 データ提供先による利用目的を明確に示すためのルール

区分（推奨/必須）	対象	ルール
推奨	情報銀行	利用目的は消費者が容易に理解できるようにすること （例） • 利用目的の説明は曖昧にならないようにすること。 • 利用目的の説明に難解な専門用語を用いないこと。 • 利用目的の説明文は他のサービスの利用に関する説明と明確に区別すること。
推奨	情報銀行（データ提供先が第三者にデータを再提供するにあたり情報銀行がデータ提供先に代わって消費者に同意を得る場合）	再提供に関する同意を得る際は、再提供先の利用目的を消費者に明示するとともに、利用目的は消費者が容易に理解できるようにすること （例） • 利用目的の説明は曖昧にならないようにすること。 • 利用目的の説明に難解な専門用語を用いないこと。 • 利用目的の説明文は他のサービスの利用に関する説明と明確に区別すること。

3.5.2.4. 「課題③情報銀行によるデータ提供先・再提供先に対する適切なデータ利用の確認・監督」に関する検討

連携データの目的外利用を抑止するために、情報銀行がデータ提供先・再提供先に対する適切なデータ利用の確認・監督を行うためのルール・機能を整備する。

プライバシーマーク制度（事業者が個人情報の取扱いを適切に行う体制等を整備していることを評価し、その証として「プライバシーマーク」の使用を認める制度）におけるプライバシーマーク付与適格性審査基準では、個人情報の目的外利用を行わないことやそのための措置を講じることなどが求められている。また、情報セキュリティマネジメントシステム（ISMS）適合性評価制度（国際的に整合性のとれた情報セキュリティマネジメントシステムに対する第三者適合性評価制度）の評価基準においても、組織がどのような情報をどのように取り扱うかを特定し、情報の適切な保護・管理が求められている。そのため、データ提供先・再提供先がプライバシーマーク付与事業者や情報セキュリティマネジメントシステム（ISMS）適合性評価制度の認証を受けた事業者である場合、情報銀行から提供を受けたデータの目的外利用を防止するための対策は十分になされているものと判断し、追加的なルールは設けないこととする。

なお、データ提供先・再提供先がプライバシーマーク付与事業者又は情報セキュリティマネジメントシステム（ISMS）適合性評価制度の認証を受けた事業者ではない場合は、以下のルールを設ける（表 3-49 参照）。

表 3-49 提供先・再提供先が講ずべき対策に関するルール

区分（推奨/必須）	対象	ルール
推奨	データ提供先・再提供先事業者	内部向け個人情報保護方針を文書化し、以下に定める事項を含めること。 • 事業の内容及び規模を考慮した適切な個人情報の取得、及び提供に関すること（特定された利用目的の達成に必要な範囲を超えた個人情報の取扱いを行わないこと及びそのための措置を講じることを含む）。 個人情報を管理するための台帳を整備していること。台帳に少なくとも以下の項目が含まれていること。 • 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
推奨	情報銀行	データ提供先に対して、特定した利用目的の達成に必要な範囲内で個人情報を利用していること、及び上記の対策を講じているか、を定期的（1 年に一度程度を推奨）に確認すること。 また、データ提供先がデータの再提供を行う場合は、データ提供先が再提供先に対して、特定した利用目的の達成に必要な範囲内で個人情報を利用していること、及び上記の対策を講じているか、を定期的（1 年に一度程度を推奨）に確認した結果についてデータ提供先から報告を受け、その内容を確認すること。
推奨	データ提供先	データ提供先がデータの再提供を行う場合は、データ提供先が再提供先に対して、特定した利用目的の達成に必要な範囲内で個人情報を利用していること、及び上記の対策を講じているか、を定期的（1 年に一度程度を推奨）に確認し、確認結果を情報銀行に報告すること。

3.5.2.5. 今後の課題・改善点

本実証事業において、消費者との間で連携データの利用目的について同意を得る際に、利用目的の曖昧性を排除し、明確に消費者に示すとともに、目的外利用を抑止するための対策を消費者に伝えることという推奨ルールを挙げた。このルールにより消費者の目的外利用に対する不安感が緩和されることが期待できる。しかし、同意の際の条件として、提供先、利用目的、提供する情報については消費者に提示されるものの、一度の提供同意で継続的に同意した情報が第三者に提供されるものなのか、といった第三者への具体的な提供形態までは示されず不明確であることが多い。利用目的の明確化と同様に、具体的な以下のような提供形態を消費者に示すルールの検討が必要である。

- 同意したデータ項目について、内容が更新される都度、継続的に同意した第三者にデータ提供する
- 同意したデータ項目について、同意時点の内容を同意した第三者に一度だけデータ提供する
- 同意したデータ項目について、同意時点の内容を同意した第三者はデータの保有はせず参照のみで利用する

3.5.3. 消費者が同意した利活用目的に必要なデータのみを選択提供・連携する機能・ルール

消費者がデータ提供に同意する際、利活用目的が複数ある場合において、個々の利活用目的ごとに必要なデータとの対応が提示されない場合がある。利活用目的 1 つ 1 つに対して、それぞれ必要となるデータであるか否かを消費者が確認した上で、利活用目的単位でデータを選択・提供同意できる仕組みが望ましい。以下（図 3-35 参照）の通り、それらの仕組みを実現するための機能・ルールの検討を行う。

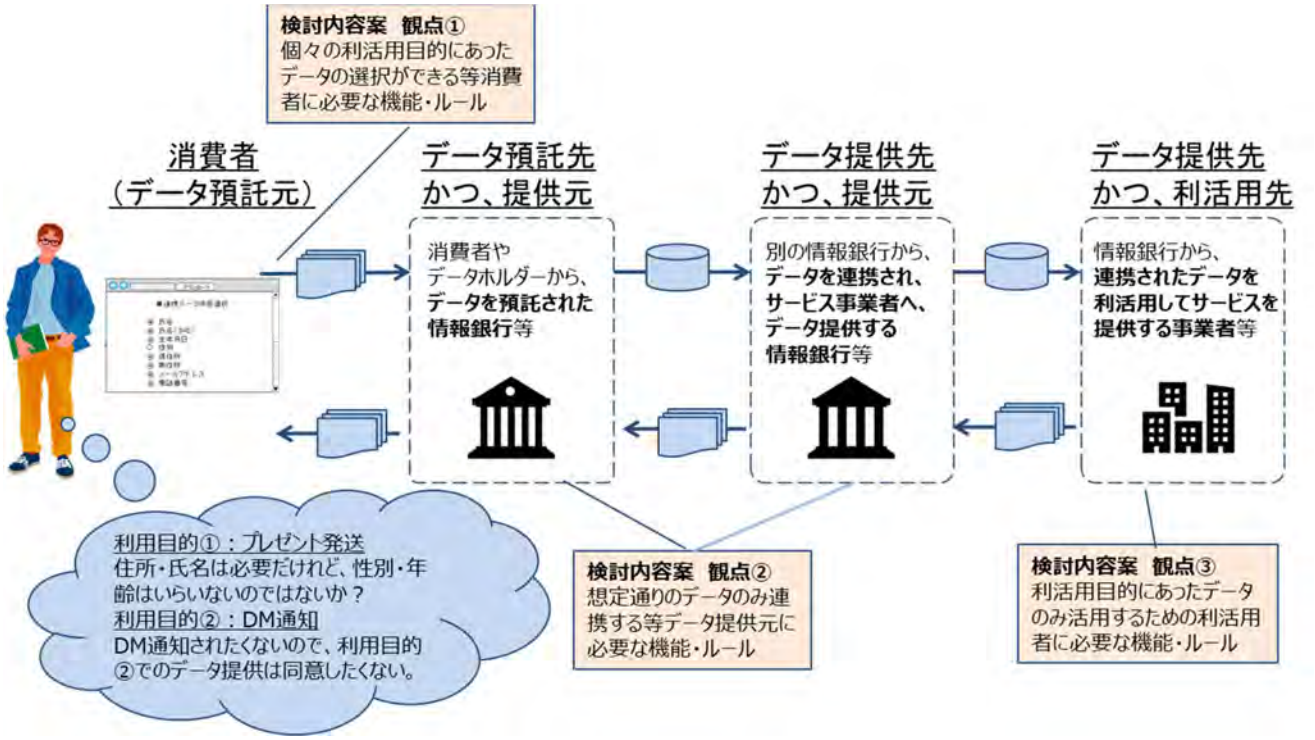


図 3-35 消費者による利活用目的に必要なデータのみの選択提供に係る不安

3.5.3.1. リスクの可視化・深掘り

消費者が同意した利活用目的に必要なデータのみを連携するにあたって、データ利活用状況の把握や制御に必要な機能・ルールが整備されていない環境下を想定し、その際のリスクをステークホルダーごとに洗い出した上で、それらのリスクに対して現状整備されている機能・ルールを調査、今後あるべきルールや機能提供を行うにあたっての課題についての検討を行った。

また、消費者がデータ提供を同意するパターンとして、「情報銀行に対する利活用目的に必要ないデータの提供」、「データ提供先に対する利活用目的に必要ないデータの提供」、「再提供先に対する利活用目的に必要ないデータの提供」、の 3 つを想定した。

なお、再提供（データ提供先がさらに別の第三者にそのデータを提供すること）については、認定指針 ver2.0 では原則禁止ではあるが、一定の条件を満たす場合可能となっている。

＜データ利活用状況の把握や制御に必要な機能・ルールが整備されていない環境下におけるリスクと課題（情報銀行に対する利活用目的に必要ないデータの提供に関するリスク）＞

ステークホルダーごとのリスク

消費者:

- 利活用目的に必要ないデータの提供

情報銀行:

- 利活用目的に必要ないデータの提供リスクがあることによる消費者の利用の抑制

データ提供先:

- (特になし)

リスクに対する現状の機能・ルール

取得タイミング:

- 情報銀行が消費者からデータを取得する際、取得するデータ項目、利用目的を約款等で明示し、消費者の同意を得ることとなっている（認定指針 ver2.0）。
- 上記のルールにおいても、個人情報保護法においても、利用目的が複数あった場合、個々の利用目的ごとに必要となるデータ項目を提示する必要はない。
- 利用目的の達成に必要なデータであるかどうか、理由を消費者に明示するといったルールはない。

ルール化・機能提供に関する課題

取得タイミング:

- 個々の利用目的ごとの情報銀行へのデータ提供の選択
- データの秘匿レベルに応じた情報銀行へのデータ提供方法変更
- 情報銀行による取得データが利用目的の達成に必要であることの消費者への説明

＜データ利活用状況の把握や制御に必要な機能・ルールが整備されていない環境下におけるリスクと課題（データ提供先に対する利活用目的に必要ないデータの提供のリスク）＞

ステークホルダーごとのリスク

消費者:

- 利活用目的に必要ないデータの提供

情報銀行:

- 利活用目的に必要ないデータの提供リスクがあることによる消費者の利用の抑制

データ提供先:

- 利活用目的に必要ないデータの提供リスクがあることによる消費者の利用の抑制

リスクに対する現状の機能・ルール

取得タイミング:

- 情報銀行が第三者提供に係る条件について、提供先第三者、その利用目的及び第三者提供の対象となる本個人情報の項目または、それらについての判断基準及び判断プロセス、のいずれかについて、消費者に通知の上、消費者から予め同意を取得するものとなっている（認定指針 ver2.0）。
- 上記のルールにて、個人情報保護法においても利用目的が複数あった場合、個々の利用目的ごとに必要となるデータ項目を提示する必要はない。
- 利用目的の達成に必要なデータであるかどうか、理由を消費者に明示するといったルールはない。

ルール化・機能提供に関する課題

取得タイミング:

- 個々の利用目的ごとの第三者へのデータ提供の選択
- データの秘匿レベルに応じた第三者提供方法の変更

＜データ利活用状況の把握や制御に必要な機能・ルールが整備されていない環境下におけるリスクと課題（再提供先に対する利活用目的に必要ないデータの提供に関するリスク）＞

ステークホルダーごとのリスク

消費者:

- 利活用目的に必要ないデータの再提供

情報銀行:

- 利活用目的に必要ないデータの再提供リスクがあることによる消費者の利用の抑制

データ提供先:

- 利活用目的に必要ないデータの再提供リスクがあることによる消費者の利用の抑制

リスクに対する現状の機能・ルール

取得タイミング:

- 個人とデータ提供先との間に契約が締結され、再提供先への第三者提供については、オプトインでの同意（個人情報保護法　第二十三条第一項）に基づき、提供先第三者が消費者から同意取得することとなっている（認定指針 ver2.0）。
- 個人情報保護法において利用目的が複数あった場合、個々の利用目的ごとに必要となるデータ項目を提示する必要はない。
- 利用目的の達成に必要なデータであるかどうか、理由を消費者に明示するといったルールはない。

ルール化・機能提供に関する課題

取得タイミング:

- 個々の利用目的ごとの再提供先へのデータ提供の選択
- データの秘匿レベルに応じたデータ再提供方法変更
- 再提供先による取得データが利用目的の達成に必要であることを消費者への説明

これらの整理によって、洗い出した課題を整理すると、以下の 3 つに大別される。

- 課題①利用目的に応じた第三者提供先へのデータの選択提供
- 課題②データの秘匿性の度合いを可視化した提供方法
- 課題③取得データが利用目的の達成に必要であることの消費者説明

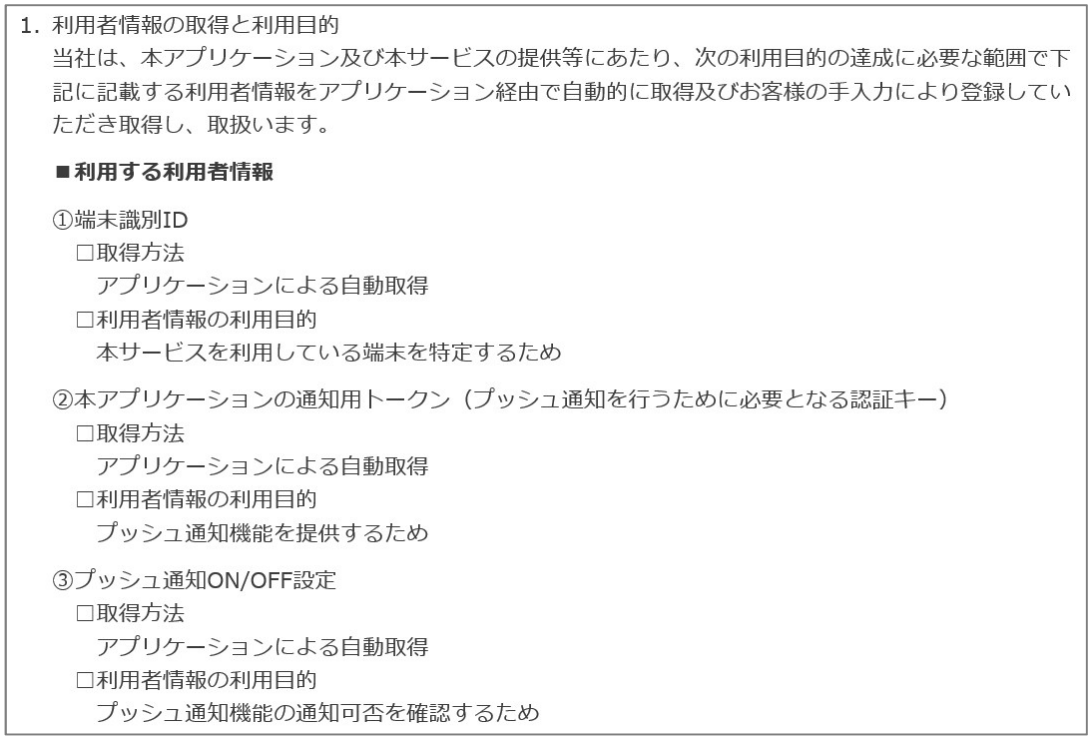
これらの課題に関する検討を行った。

3.5.3.2. 「課題①利用目的に応じた第三者提供先へのデータの選択提供」に関する検討

消費者が事業者に自身のデータを提供する際、利用目的に必要ないデータが提供されるかも知れないといった不安を解消するには、利用目的が複数ある場合において、個々の利用目的ごとに必要なデータとの対応が提示され、消費者が理解した上で同意することが望ましい。

そのため、情報銀行が、消費者からデータを取得する際、データ提供先にデータを提供する際、データ提供先がデータを再提供する際に、消費者に対して事前に個々の利用目的ごとに必要なデータとの対応を開示し、同意を得るためのルール・機能について検討を行った。

多くの事業者では、消費者からデータを取得、データ提供先にデータ提供するにあたり、プライバシーポリシー等で利用目的と取得・提供するデータを公表している。その中でも、個々の利用目的ごとに必要なデータとの対応までを公表している事業者の事例を以下（図 3-36、図 3-37 参照）に示す。



1．利用者情報の取得と利用目的
当社は、本アプリケーション及び本サービスの提供等にあたり、次の利用目的の達成に必要な範囲で下記に記載する利用者情報をアプリケーション経由で自動的に取得及びお客様の手入力により登録していただき取得し、取扱います。

■利用する利用者情報

①端末識別ID
□取得方法
アプリケーションによる自動取得
□利用者情報の利用目的
本サービスを利用している端末を特定するため

②本アプリケーションの通知用トークン（プッシュ通知を行うために必要となる認証キー）
□取得方法
アプリケーションによる自動取得
□利用者情報の利用目的
プッシュ通知機能を提供するため

③プッシュ通知ON/OFF設定
□取得方法
アプリケーションによる自動取得
□利用者情報の利用目的
プッシュ通知機能の通知可否を確認するため

図 3-36 プライバシーポリシーにおける個人情報とその利用目的に関する記載事例
（NTT ドコモ・スマートフォン用アプリケーション「d 払いアプリ」プライバシーポリシー（2021 年 1 月時点））

2. 利用者情報の端末外部へのデータ送信及び第三者提供等

(1) 当社は、前条において自動もしくはお客様に登録いただき取得した情報を、本アプリケーション内に組み込まれた情報収集モジュールにて取得・蓄積・転送し、次の利用目的の達成に必要な範囲で下記に記載する利用者情報を第三者へ提供することがあります。

■利用する利用者情報

本アプリケーションの通知用トークン（プッシュ通知を行うために必要となる認証キー）
お客様の本アプリケーション上での利用・操作・設定情報
□利用者情報の利用目的
本サービスの品質改善、各種分析・調査を実施するため
□情報収集モジュール名
Google Analytics
□モジュール作成会社
Google Inc.
□第三者提供の有無
有（Google Inc.への提供）

■利用する利用者情報

端末の位置情報（GPS位置情報、Wi-Fi位置情報、基地局の情報を用いて推測される位置情報、Bluetooth位置情報）
□利用者情報の利用目的
お客様の近くにある本サービスが利用できるお店情報の表示やクーポンを配信するため
□情報収集モジュール名
本アプリケーション本体
□モジュール作成会社
株式会社ＮＴＴドコモ
□第三者提供の有無
有（Google Inc.への提供）

図 3-37 プライバシーポリシーにおける個第三者に提供する個人情報と提供先での利用目的に関する記載事例（NTT ドコモ・スマートフォン用アプリケーション「d 払いアプリ」プライバシーポリシー（2021 年 1 月時点））

本事例では、プライバシーポリシーに個々の利用目的ごとに必要なデータとの対応が記載されたものとなるが、情報銀行が消費者よりデータ提供の個別同意を得る際は、以下（表 3-50 参照）のような提供条件を提示し、提供先、利用目的、データ範囲をそれぞれ選択できるような機能を設けることが望ましい。

表 3-50 個人情報の提供に関する条件の例

個人情報の提供に関する条件の例					
提供先		利用目的		データ範囲	
☑	株式会社 AAA 銀行	☑	市場調査、ならびにデータ分析やアンケートの実施等による金融商品やサービスの研究や開発のため	☑	氏名 住所 生年月日 性別
		☑		☑	氏名 住所

			ダイレクトメールの発送・電話によるご案内等、金融商品やサービスに関する各種ご提案のため		生年月日 性別 E メールアドレス 電話番号
				☑	職業 家族構成
				□	世帯収入 預貯金額 取引金融機関名称
□	株式会社 BBB 生命	□	関連会社・提携会社を含む各種商品・サービスのご案内	□	氏名 住所 生年月日 性別
				□	職業 家族構成

情報銀行が消費者よりデータ提供の包括同意を得る際は、提供条件の利用目的を選択した際に、利用目的に合致するデータ範囲のみ表示するルール及び機能（表 3-51、表 3-52 参照）を追加することが想定される。

表 3-51 情報銀行・提供先・再提供先が講ずべき対策に関する機能

区分（推奨/必須）	対象	機能
推奨	情報銀行	情報銀行が消費者より第三者提供先へのデータ提供の個別同意を得る際は、情報銀行は、提供先、利用目的ごとに必要となるデータ範囲を提供条件として提示し、それぞれ選択できるような機能を具備すること。
推奨	情報銀行、第三者提供先	第三者提供先が消費者より情報銀行から提供を受けたデータの再提供の個別同意を得る際は、情報銀行又は第三者提供先は、再提供先、利用目的ごとに必要となるデータ範囲を提供条件として提示し、それぞれ選択できるような機能を具備すること。

表 3-52 情報銀行・提供先・再提供先が講ずべき対策に関するルール

区分（推奨/必須）	対象	ルール
推奨	情報銀行	情報銀行が消費者よりデータを取得する際、利用規約等に利用目的ごとに必要となるデータ項目を記載し、消費者に提示すること。

3.5.3.3. 「課題②データの秘匿性の度合いを可視化した提供方法」に関する検討

情報銀行が消費者から第三者提供先へのデータ提供について個別に同意を得る際、情報銀行が、提供先名称、その利用目的、提供するデータ項目を明示するにあたり、提供するデータ項目の秘匿レベル（扱うデータの秘匿性の高さに応じて分けられたレベル。3.4.2.にて定義を記載）を併せて明示することで、消費者は秘匿レベルに応じて同意すべきか否かの判断をし、納得した上でデータ提供を同意することができる（表 3-53 参照）。秘匿レベルが高いほど、より強固な認証手段や、暗号化等のデータの機密性や完全性を高めた技術を用いてデータ提供することが望ましい。

表 3-53 個人情報の提供に関する条件の例

個人情報の提供に関する条件の例						提供するデータの秘匿レベル
提供先		利用目的		データ範囲		
☑	株式会社 AAA 銀行	☑	市場調査、ならびにデータ分析やアンケートの実施等による金融商品やサービスの研究や開発のため	☑	氏名 住所 生年月日 性別	レベル 1
		☑	ダイレクトメールの発送・電話によるご案内等、金融商品やサービスに関する各種ご提案のため	☑	氏名 住所 生年月日 性別 E メールアドレス 電話番号	レベル 1
				☑	既往症	レベル 2
				□	世帯収入 預貯金額 取引金融機関名称	レベル 1
□	株式会社 BBB 生命	□	関連会社・提携会社を含む各種商品・サービスのご案内	□	氏名 住所 生年月日 性別	レベル 1
				□	既往症	レベル 2

なお、秘匿レベルは、個人情報を取り扱うレベル毎（レベルが上がるほど慎重な取扱いが必要）に整理が必要となる。秘匿レベル 1 は、本人の同意に基づいて情報銀行が取得・提供可能な情報と定義し、レベル 2 以上については、要配慮個人情報を含む可能性があるため、今後の情報銀行における取扱いに関する検討結果に従い、順次定義することとした。

情報銀行による秘匿レベルの明示に関する機能として、以下（表 3-54 参照）を推奨する。

表 3-54 秘匿レベルの明示に関する機能

区分（推奨/必須）	対象	機能
推奨	情報銀行	• 個人情報の提供に関して、情報銀行が消費者から個別に同意を得る際、情報銀行が、提供先名称、その利用目的、提供するデータ項目を明示、選択する画面に、提供するデータ項目の秘匿レベルを合わせて明示すること。 • 提供するデータ項目の秘匿レベルの設定にあたっては、複数のデータ項目をまとめて明示する場合は、そのデータ項目の中で、最も秘匿レベルが高いものを記載すること。
推奨	情報銀行、第三者提供先	• 第三者提供先が消費者より情報銀行から提供を受けたデータの再提供の個別同意を得る際は、情報銀行又は第三者提供先は、提供先名称、その利用目的、提供するデータ項目を明示、選択する画面に、提供するデータ項目の秘匿レベルを合わせて明示すること。 • 提供するデータ項目の秘匿レベルの設定にあたっては、複数のデータ項目をまとめて明示する場合は、そのデータ項目の中で、最も秘匿レベルが高いものを記載すること。

3.5.3.4. 「課題③取得データが利用目的の達成に必要であることの消費者説明」に関する検討

情報銀行が消費者からデータを取得する際や、データを第三者に提供・再提供する際、当該データが本当に利用目的の達成に必要であるかどうかを消費者が判断することは難しい。そのため、情報銀行は、取得するデータが利用目的の達成に必要であることの理由を消費者に説明することが望ましい。

事業者によっては、プライバシーポリシー等において、取得するデータの利用目的を説明する文章を工夫し、当該データをどういった場合に何のためにどの様に利用するかを詳細に記載している。情報銀行においても、消費者からデータ取得や提供に関する同意を得る際に、説明文書を分かりやすいかたちで閲覧できるような工夫が必要である（表 3-55 参照）。

表 3-55 情報銀行・提供先・再提供先が講ずべき対策に関するルール

区分（推奨/必須）	対象	ルール
推奨	情報銀行	• 消費者からのデータ取得や、第三者へのデータ提供にあたって、消費者からその同意を得る際は、当該データが利用目的の達成に必要であることの説明（どういった場合に、何のために、どの様に利用するか）を明示すること。 • 上記説明の明示にあたっては、同意を得る画面等から説明文書へのリンクを設けるなど、煩雑にならないよう工夫すること。
推奨	情報銀行、第三者提供先	• 第三者提供先が消費者より情報銀行から提供を受けたデータの再提供の個別同意を得る際は、情報銀行又は第三者提供先は、提供先名称、その利用目的、提供するデータ項目を明示、選択する画面に、当該データが利用目的の達成に必要であることの説明（どういった場合に、何のために、どの様に利用するか）を明示すること。 • 上記説明の明示にあたっては、同意を得る画面等から説明文書へのリンクを設けるなど、煩雑にならないよう工夫すること。

3.5.3.5. 今後の課題・改善点

秘匿性が高い要配慮個人情報等を含む可能性がある秘匿レベル 2 以上について、情報銀行で取り扱う情報に関する専門家や有識者を交えた検討結果に従い、順次定義を見直す必要がある。なお、2021 年 3 月現在で検討されている情報分野としては、保険医療情報がある。また、秘匿レベル 1 についても、実用的な定義となるように細分化するなどの改善が必要と考える。

3.5.4. 消費者が同意撤回、利用停止・消去の申し出をした際に、各事業者に求められる機能・ルール

改正個人情報保護法によって消費者本人は、条件付き（個人データの当該本人の権利や利益が害される等）で個人情報取扱事業者に対して個人データの利用停止や第三者への提供の停止の請求が可能になっている。また、認定指針 ver2.0 によって、情報信託機能の認定基準となる事業内容における「個人のコントローラビリティを確保するための機能」の一つとして、「情報銀行に委任した個人情報の第三者提供・利用の停止（同意の撤回）」が要求されている。同意に対する消費者の不安を軽減し、個人データの流通・利活用をより一層、普及・促進させるためには、消費者が一度同意した個人データを取り扱う情報銀行等の個人情報取扱事業者に対して、同意の撤回、利用停止・消去の請求が円滑に行える仕組みが必要である。それらの仕組みの実現にあたって必要となる機能・ルールの検討を行う。

3.5.4.1. リスクの可視化・深掘り

消費者からの同意撤回への対応に必要な機能・ルールが整備されていない環境下におけるリスクをステークホルダーごとに洗い出し、それらのリスクに対する現状の機能・ルールを調査した上で、今後あるべきルールや機能提供を行うにあたっての課題についての検討を行った。

また、リスクについては、「第三者へのデータの提供停止」、「データ提供先による利用停止」、「データ提供先におけるデータの消去」の 3 つの観点でそれぞれ整理した。

＜同意の撤回、利用停止、消去に関するリスクと課題（第三者へのデータの提供停止）＞

ステークホルダーごとのリスク

消費者:

- データが継続してデータ提供先に提供されてしまうこと

情報銀行:

- 利活用目的に必要ないデータの提供リスクがあることによる消費者の利用の抑制

データ提供先:

- (特になし)

リスクに対する現状の機能・ルール

請求時/処理後タイミング:

- 消費者から、第三者提供・利用停止の指示を受けた場合、情報銀行はそれ以降そのデータを提供先に提供しないことが義務付けられている（認定指針 ver2.0）。

ルール化・機能提供に関する課題

請求時/処理後タイミング:

- (特になし)

＜同意の撤回、利用停止、消去に関するリスクと課題（データ提供先によるデータの利用停止）＞

ステークホルダーごとのリスク

消費者:

- データ提供先に継続して利用されてしまうこと

情報銀行:

- データ提供先におけるデータの利用停止を正しく確認できない可能性がある
- データ提供先によるデータの継続利用が発覚した際の信頼低下

データ提供先:

・データの継続利用が発覚した際の信頼低下

リスクに対する現状の機能・ルール

請求時/処理後タイミング:

- 消費者は、個人情報取扱事業者に対し、個人データが第 16 条の規定（利用目的）に違反して取り扱われているとき又は第 17 条の規定（同意の取得）に違反して取得されたものであるときは、当該個人データの利用の停止又は消去を請求することができる（個人情報保護法 第三十条）。
- データ提供先による取得したデータの利用に関する記録を消費者へ開示するルールはない。
- 情報銀行によるデータ提供先のデータ利用状況の確認に関するルールはない。

ルール化・機能提供に関する課題

請求時/処理後タイミング:

- データ提供先によるデータ利用状況の消費者への開示
- 情報銀行によるデータ提供先のデータ利用状況の確認

＜同意の撤回、利用停止、消去に関するリスクと課題（データ提供先におけるデータの消去）＞

ステークホルダーごとのリスク

消費者:

- データ提供先から消去されないこと

情報銀行:

- データ提供先におけるデータの消去を正しく確認できない可能性がある
- データ提供先によるデータの継続所有が発覚した際の信頼低下

データ提供先:

- データの所有が発覚した際の信頼低下

リスクに対する現状の機能・ルール

請求時/処理後タイミング:

- データ提供先による取得したデータの消去に関する記録を消費者へ開示するルールはない。
- 情報銀行によるデータ提供先のデータの消去の状況の確認に関するルールはない。

ルール化・機能提供に関する課題

請求時/処理後タイミング:

- データ提供先による保有データの消費者への開示
- 情報銀行によるデータ提供先の保有データの確認

上記の整理によって、洗い出した課題を整理すると、以下の 2 つに大別される。

- 課題①データ提供先におけるデータ利用状況の消費者開示
- 課題②データ提供先から情報銀行へのデータ利用状況の報告

これらの課題に関する検討を行った。

3.5.4.2. 「課題①データ提供先におけるデータ利用状況の消費者開示」に関する検討

データ提供先によるデータの利活用等に対して消費者が一度同意を行ったデータについて、データ提供先が保有しているデータ及びそのデータの利用状況を確認できる機能（ダッシュボード機能等）とともに、状況に応じて同意の撤回等を申請できる機能を提供することによって、消費者が容易に同意の撤回を行うことが可能になる（表 3-56 参照）。

表 3-56 データの利用状況の開示に関する消費者向け機能

区分（推奨/必須）	対象	機能
必須	情報銀行	【消費者に対して、データ提供先による保有データや保有データの利用状況を一覧表示する機能】 ・「データの利用状況の開示に関するルール」（表 3-57参照）に定められた情報項目を、本機能を通じて消費者に提供することが望ましい。 理由:同意の撤回に際し、消費者が自己のデータの提供先・提供履歴・提供先の利用状況をいつでも容易に確認できることにより、同意の撤回の判断を支援するため。
	情報銀行	【同意の撤回等を申請できる機能】 ・ 消費者が一度同意を行った自己のデータの提供や提供先によるデータの利用を撤回できる機能である。 理由:消費者が同意の撤回を行うたに必要な機能であるため。

データの利用状況の開示機能及び同意の撤回等の申請機能の事例として、株式会社 NTT ドコモの「パーソナルダッシュボード」[7]（図 3-38 参照）、KDDI 株式会社の「プライバシーポータル」[8]（図 3-39 参照）が挙げられる。前者の「パーソナルデータダッシュボード」では、データの提供先と提供しているデータの確認と、同意の撤回（データ提供の停止）を行うことが可能である。また、後者の「プライバシーポータル」では、個別の同意内容の確認と同意の撤回、規約の同意状況の確認が可能である。

データの利用状況の開示機能及び同意の撤回等の申請機能に関して、以下のルール（表 3-57、表 3-58 参照）を設ける。

表 3-57 データの利用状況の開示に関するルール

区分（推奨/必須）	対象	ルール
必須	情報銀行/データ提供先事業者	データ提供先は、情報銀行を通じて消費者に対して以下の情報(※)を開示すること ・ 保有しているデータ及びデータごとの利用目的 ・ 保有しているデータの利用状況 （利用中または利用停止中の状況） (※)最新情報を表示すべきである為、前営業日以降の情報を推奨するが、具体的な情報の鮮度は、情報銀行間の契約で定めること

表 3-58 消費者による同意の撤回等への対応に関するルール

区分（推奨/必須）	対象	ルール
必須	情報銀行/データ提供先事業者	消費者が電子的に容易に同意を撤回できる機能を用意し、期限内(※)に申請に対して適切な対応をすること ＜期限に関するルール＞ ・ 情報銀行は消費者からの申請を 1 営業日以内にデータ提供先に連携すること ・ データ提供先は、申請の連携後 1 営業日以内に、申請に対する適切な対応を行い、その結果を情報銀行に連携すること

[7] 出典:株式会社 NTT ドコモ「パーソナルダッシュボード」
＜https://datadashboard.front.smt.docomo.ne.jp/＞（参照日 2021 年 2 月 17 日）

[8] 出典:KDDI 株式会社「プライバシーポータル」
＜https://www.kddi.com/corporate/kddi/public/privacy-portal/＞（参照日 2021 年 2 月 17 日）

		(※)可能な限り消費者からの申請に対応すべきであるため、上記の期限を推奨とするが、具体的な期限は情報銀行間の契約で定めること

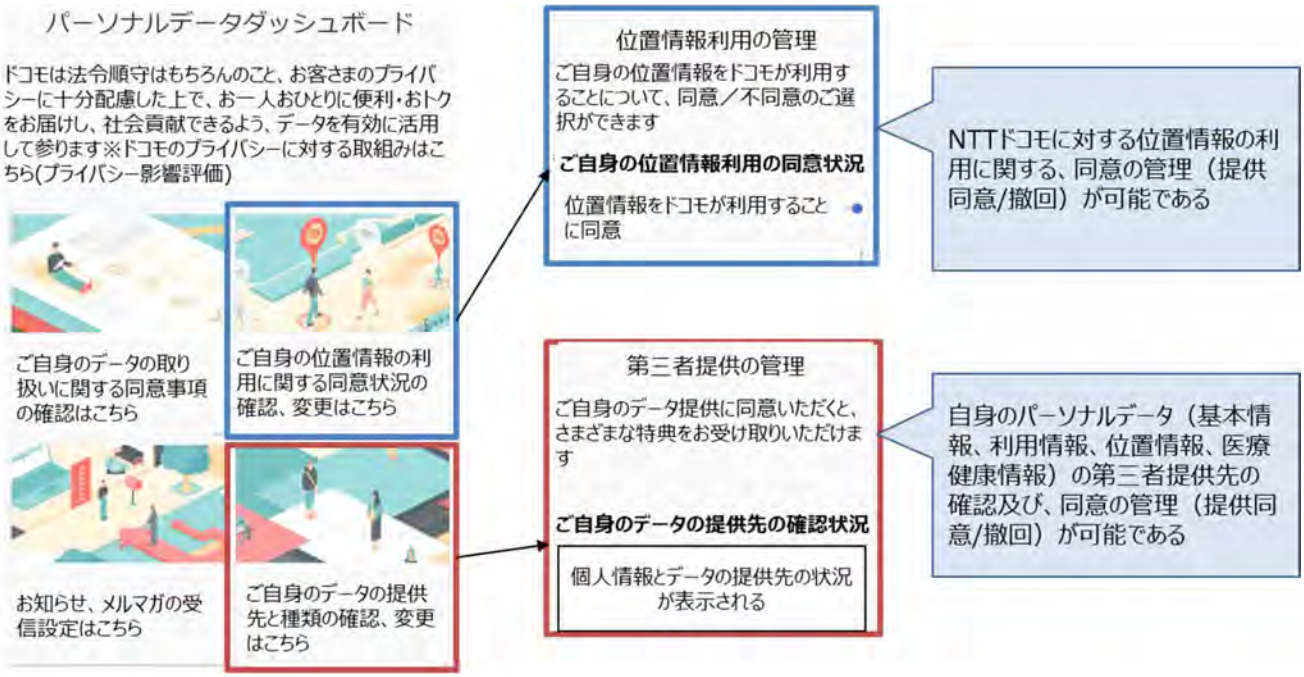


図 3-38 パーソナルダッシュボードのイメージ

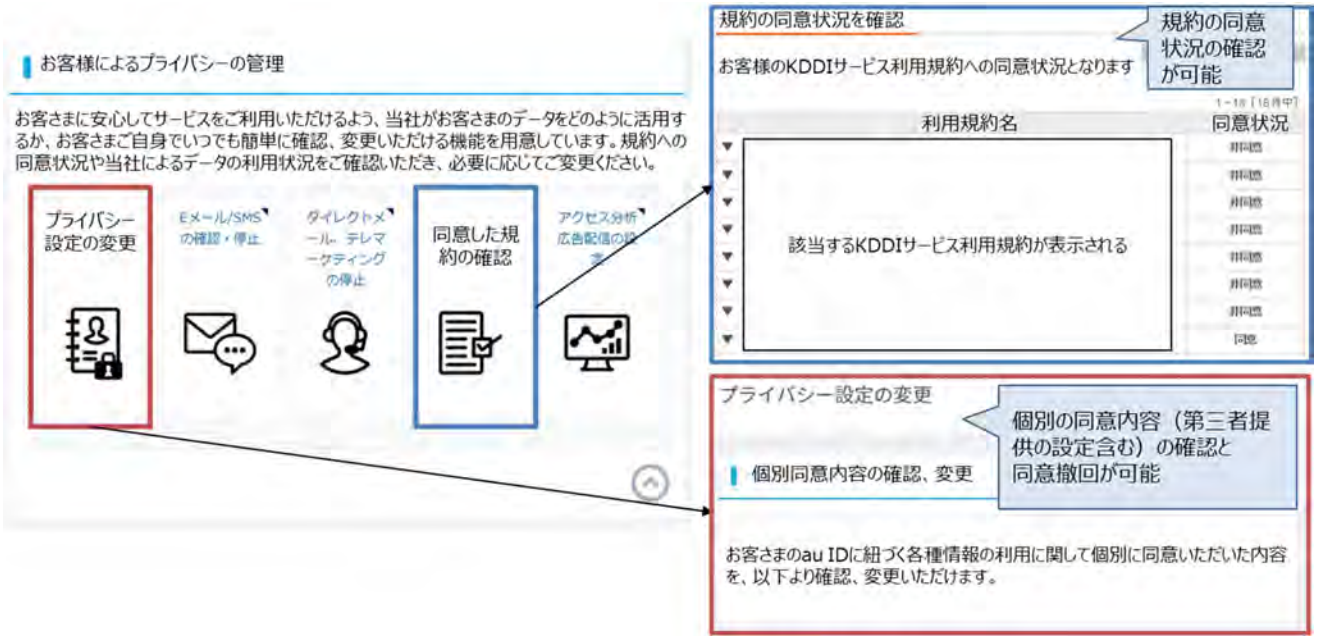


図 3-39 プライバシーポータルのイメージ

3.5.4.3. 「課題②データ提供先から情報銀行へのデータ利用状況の報告」に関する検討

課題①で記載したデータの利用状況の開示機能及び同意の撤回等の申請機能を実現するために、データ提供先が情報銀行に対して保有データやその利用状況に関する報告を行う機能が必要である。情報銀行がデータ提供先の保有データや保有データの利用状況を直接確認できる機能が望ましいが、業務負担の大きさやセキュリティの観点から、実効的な方法として、以下（表 3-59 参照）の通り、データの提供先が情報銀行に報告を行う形式を推奨する。

表 3-59 データ提供先のデータ利用状況の確認機能

区分（推奨/必須）	対象	機能
推奨	情報銀行/データ提供先事業者	【データ提供先のデータ利用状況を確認する機能】 「データの利用状況の開示に関するルール」（表 3-57 参照）に則り、データ提供先が情報銀行に対して保有データや保有データの利用状況に関する報告を行う機能。 理由:情報銀行が消費者に対して、自己のデータの利用状況等を表示するために、情報銀行自体がデータ提供先の状況を確認する必要があるため。

また、以下（表 3-60 参照）に、情報銀行によるデータ提供先の利用状況の報告に関するルールを設ける。

表 3-60 提供先による情報銀行への報告に関するルール

区分（推奨/必須）	対象	ルール
必須	情報銀行/データ提供先事業者	情報銀行は、データ提供先に対して、保有データや保有データの利用状況に関する報告を定期的に求めること。また、データ提供先は、情報銀行から報告が求められた際に、速やかに報告必要事項を報告するための環境を整備すること ＜報告必要事項に関するルール＞ 消費者ごとに整理された、保有しているデータの内容及び保有しているデータごとの利用状況を報告すること ＜報告方法に関するルール＞ 電子的に報告を行うこと(報告の際は必要事項がまとめられた資料（管理台帳等）を提出すること) ＜報告頻度に関するルール＞ 営業日毎(※)または、情報銀行から報告を求められた際、データ提供先は報告を実施すること (※)最新の情報を消費者に表示するべきであるため、推奨頻度として記載しているが、具体的な期限は情報銀行間の契約で定めること

推奨	情報銀行/データ提供先事業者	情報銀行はデータ提供先との業務提携の契約に、紛争防止（以下に例を記載）のための契約条項を盛り込むこと ＜最低限必要な条項の例＞ ・ 報告義務(データの利用状況の報告が必要であるため) ・ 契約の解除(不正等があった場合の契約の解除のため) ・ 違約金、損害賠償(不正等があった場合、情報銀行がデータ提供先に損害賠償請求や違約金の請求をすることが想定されるため)
推奨	情報銀行/データ提供先事業者	匿名化・統計化、仮名化されたデータに対する、利用停止及び消去の消費者からの申請に対して、以下の対応をすること ＜匿名化・統計化データ＞ ・ 利用停止:利用停止の申請があった時点以降では、匿名化及び統計化は停止すること。なお、申請以前に匿名化・統計化されていたデータの継続的な内部利用に加え、消費者からの同意取得がない第三者提供も可とする ・ 消去:加工前の提供されたデータは削除すること。しかし、既に匿名化・統計化されたデータは削除しなくてもよい ＜仮名化データ＞ ・ 利用停止:利用停止の申請があった時点以降では、仮名化は停止すること。なお、申請以前に仮名化されていたデータについて、継続的な利用に加え、消費者からの同意の取得無しの第三者提供は不可とする ※仮名化データの第三者提供は改正個人情報保護法で禁止されているため、消費者から同意を取得しなければならない ・ 消去:加工前の提供されたデータ及び既に仮名化されたデータは削除すること

3.5.4.4. 今後の課題・改善点

上記の機能の実装及びルールの導入によって、消費者が情報銀行等の個人情報取扱事業者に対して、一度同意を行ったデータに対する同意の撤回や利用停止、消去を容易に請求することができる環境の整備が可能になる。これによって、一度同意したデータに対して、いつでも同意の撤回等の請求が可能になるため、同意に対する消費者の心理的障壁が下がり、個人データの流通・利活用の普及に期待ができる。

但し、消費者が同意撤回等の請求をした際に消費者が不利益を被ることを防ぐために、当該請求への対応に関する契約内容（紛争防止の観点も含む）について、情報銀行とデータ提供先間で詳細に定めていくことが今後の課題である。

3.5.5. 信頼性の高い包括的なトレーサビリティを消費者へ提供するために必要な機能・ルール

情報銀行が個人情報流通基盤を介した情報提供を行う場合、様々な情報銀行が林立し、消費者本人が自分の提供データを把握・管理することが困難となる可能性があるため、情報銀行が包括的なトレーサビリティ機能を持つことが期待される。そこで、以下（図 3-40 参照）の通り、情報銀行に委任した個人情報について、信頼性が高い包括的なトレーサビリティ機能を消費者に提供するため、現時点で想定されるリスクの可視化・深掘りにて課題を抽出後、必要な機能（全体スキーム、個人情報提供履歴内容、確認手順等）及びルールの検討を行う。

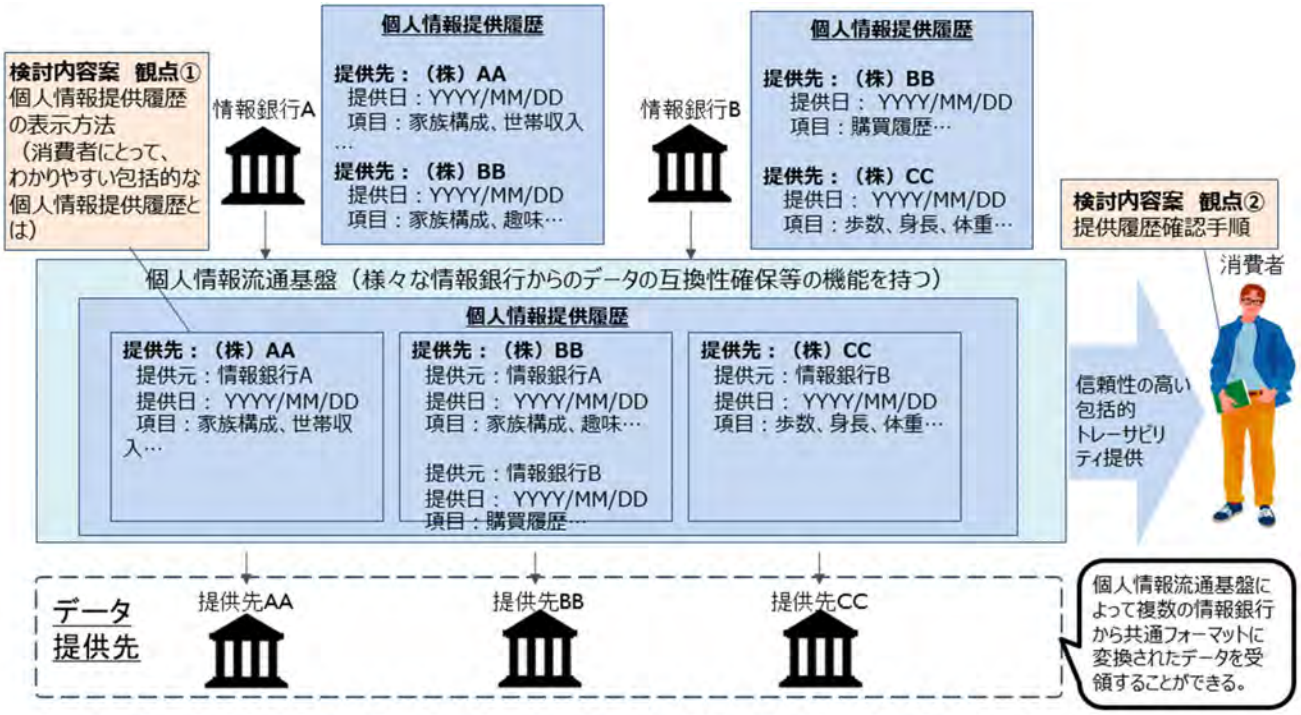


図 3-40 信頼性の高い包括的なトレーサビリティのイメージ

3.5.5.1. リスクの可視化・深掘り

データ連携時の包括的なトレーサビリティに関する機能・ルールが整備されていない環境下にて、消費者本人によるデータ管理について想定されるリスクをステークホルダーごとに洗い出した。また、それらのリスクに対する現状の機能・ルールを調査した上で、今後あるべきルールや機能提供を行うにあたっての課題についての検討を行った。

＜情報銀行が林立した場合の消費者本人によるデータ管理に関するリスクと課題＞

ステークホルダーごとのリスク

消費者:

- 情報銀行が第三者提供したデータを把握できない可能性について不安を抱えること
- 情報銀行が第三者提供したデータを把握できない可能性について不安を抱えることにより、消費者が第三者提供の同意を抑制すること

情報銀行:

- 情報銀行が第三者提供したデータを把握できない可能性について不安を抱えることにより、消費者が第三者提供の同意を抑制すること

データ提供先:

- 情報銀行が第三者提供したデータを把握できない可能性について不安を抱えることにより、消費者が第三者提供の同意を抑制すること

リスクに対する現状の機能・ルール

取得～消去までのタイミング:

- 情報銀行に委任した個人情報の提供履歴に関する包括的な閲覧（トレーサビリティ）機能について定められたルールはない。
- 認定指針 ver2.0 では、情報銀行に対して、「どのデータがどこに提供されたのかという履歴を閲覧できるユーザーインターフェースを提供すること」、「提供の日時、提供されたデータ項目、提供先での利用状況など、履歴の詳細を提供する場合は、その旨を明示すること」とのルールがある。
- 個人情報保護法では、個人情報取扱事業者に対して、個人データを第三者に提供した場合は当該個人データを提供した年月日、当該第三者の氏名又は名称等の記録、第三者から個人データの提供を受ける場合は当該個人データの提供を受けた年月日、当該確認に係る事項等に関する記録を作成しなければならない旨のルールがある。

ルール化・機能提供に関する課題

取得～消去までのタイミング:

- 情報銀行が取得・提供したデータの包括的な消費者向け閲覧機能に関するルール、機能

これらの整理によって、洗い出した課題を整理すると、以下に集約される。

- 課題①情報銀行が取得・提供したデータに関する包括的な閲覧履歴の消費者開示

この課題に関する検討を行った。

3.5.5.2. 「課題①情報銀行が取得・提供したデータに関する包括的な閲覧履歴の消費者開示」に関する検討

情報銀行が取得・提供したデータの包括的な消費者向け閲覧履歴の開示を実現するためには、該当機能を提供する者、該当機能として求められる機能、及び該当機能を提供可能とするために必要な履歴データの保存についてルールを設ける必要がある。

現状では情報銀行に委任した個人情報の提供履歴に関する包括的な閲覧（トレーサビリティ）機能について定められたルールはないが、認定指針 ver2.0、及び個人情報保護法にてデータ提供履歴の記録・閲覧に関するルールが定められていることも踏まえ、必要なルール（表 3-61 参照）を検討した。

表 3-61 情報銀行が取得・提供したデータの包括的な消費者向け閲覧履歴の開示に向けて必要なルール

区分（推奨/必須）	対象	ルール
必須	消費者に対して、情報銀行が取得・提供したデータを包括的に検索・一覧表示できる機能を提供可能とする者（情報銀行、または当該プラットフォームを提供する第三者を想定）	消費者に対して、情報銀行が取得・提供したデータを包括的に検索・一覧表示できる機能を提供する者は、認定指針 ver2.0 にて「情報信託機能の認定基準」に定められている条件を満たす者であること。 理由:厳格な情報管理を実施できる者でなければ、情報漏洩・改竄等が発生し、消費者に被害が及んでしまう可能性があるため。
必須 ※具体的な項目については、実現可能性に応じて検討の余地あり	（同上）	情報銀行に預託されたデータについて、情報銀行間を跨って包括的に以下項目を検索・一覧表示できる機能を消費者に提供すること。 ・日時 ・データ提供元 ・データ提供先 ・アクション内容（データ預託、データ提供、第三者提供に関する同意、更新、第三者提供の同意撤回請求、利用停止、消去等） ・提供データ項目 ・利用目的 ・同意情報 理由:消費者が自己のデータの提供先・提供履歴をいつでも容易に確認できることにより、自己のデータのコントローラビリティ確保を実現するため。

必須	（同上）	情報銀行、及び情報銀行から第三者提供を受ける者は、取得・提供した消費者のデータについて動きがあった場合、上記項目のデータを保存すること。 理由:情報銀行に預託されたデータについて、情報銀行間を跨って包括的に検索・一覧表示できる機能を消費者に提供するため。

情報銀行が取得・提供したデータの包括的な消費者向け閲覧履歴の開示を実現するため、必要となる機能について検討するにあたり、内閣府のマイナポータルの事例を参考にした。

- マイナポータルでは、行政機関間での市民の個人情報のやり取りについて、いつ、どういった目的で行われたか、を市民自身が確認できる仕組みとなっている。
- マイナポータルのやり取り履歴確認の画面の流れ、画面の構成要素は以下（図 3-41、図 3-42、図 3-43 参照）の通りである。まず、やりとり履歴について「提供の要求」を行い、行政側で処理された結果、「閲覧可能」または「閲覧済」となった場合のみ、履歴の照会が可能となる。なお、タイムラグが出ないようであれば、要求と照会を分離することは不要である。

提供状況	説明
受付済	やりとり履歴の提供要求が受け付けられ、処理中
閲覧可能	すべての情報が提供され、閲覧可能
閲覧済	該当期間のやりとり履歴の要求結果は閲覧済み（閲覧可能）
閲覧済(削除)	当該期間の要求結果は閲覧済みであり、且つ削除済み（閲覧不可）
要求件数超過	要求結果件数が上限数(100件)を超えたため、マイナポータルでの要求結果の受け取り不可。要求期間を変更して再度、提供要求する必要がある
閲覧対象なし	指定された要求期間に、閲覧できる情報がない
空き容量不足	やりとり履歴を取得するための利用者フォルダーの空き容量不足。不要なお知らせ等を削除して、空き容量を確保してから再度、提供要求する必要がある
要求失敗	ネットワーク障害等が発生したため、提供要求が受け付けられなかった。再度、提供要求する必要がある
要再実行	提供要求が集中したため、提供要求が受け付けられなかった。再度、提供要求する必要がある

図 3-41 内閣府のマイナポータルの事例:全体の流れ[9]

[9] 出典:内閣府大臣官房番号制度担当室「マイナポータル」の「やりとり履歴を確認する」
＜https://img.myna.go.jp/manual/03-02/0048.html＞（参照日 2021 年 2 月 17 日）

	項目	説明
絞込条件	①照会日	照会日で絞込みしたい場合に入力
	②照会機関	照会した行政機関等で絞込みしたい場合に選択
	③提供日	提供日で絞込みしたい場合に入力
	④提供機関	提供した行政機関等で絞込みしたい場合に選択
	⑤やりとりされた情報の名称	やりとりされた特定個人情報で絞込みしたい場合に選択
	⑥詳細な絞込条件を設定する/詳細な絞込条件を隠す	詳細な絞込条件画面と一覧画面を切替したい場合に選択
	⑦クリアボタン	絞込条件を消去したい場合に選択
	⑧絞込ボタン	指定した条件で絞込みして一覧に表示したい場合に選択
一覧	⑨受信日時	やりとり履歴の提供決定を受信した日時
	⑩照会日時	行政機関等があなたの情報を照会した日時
	⑪照会機関	あなたの情報を照会した行政機関等名
	⑫提供日時	行政機関等があなたの情報を提供した日時
	⑬提供機関	あなたの情報を提供した行政機関等名
	⑭やりとりされた情報の名称	選択することにより、履歴詳細を表示
	⑮状況	提供状況
ー	⑯ダウンロードボタン	履歴一覧データを保存
ー	⑰前の画面へボタン	ひとつ前の画面へ戻る

図 3-42 内閣府のマイナポータルの事例:やりとり履歴一覧[10]

情報銀行が取得・提供したデータの包括的な消費者向け閲覧機能では、「データ提供元」「データ提供先」に関する情報に置き換わるが、同様の機能が必要になる。アクション（取得・提供・同意・同意撤回請求・利用停止・消去等）、検索キー、表示項目としてどこまで対象とすべきかについては、事業者の負担等を勘案して検討する必要がある。

[10] 出典:内閣府大臣官房番号制度担当室「マイナポータル」の「やりとり履歴一覧」
＜https://img.myna.go.jp/manual/03-02/k0056.html＞（参照日 2021 年 2 月 17 日）

項目	説明
①整理番号	整理番号
②状況	提供状況
③やりとり履歴受信日時	やりとり履歴の提供決定を受信した日時
④照会日時	行政機関等が、あなたの情報を照会した日時
⑤照会機関	やり取り履歴を照会した行政機関等名
⑥情報照会者部署名	あなたの情報を照会した部署名
⑦提供日時	行政機関等が、あなたの情報を提供した日時
⑤やりとりされた情報の名称	やりとりされた特定個人情報で絞込みしたい場合に選択
⑥詳細な絞込条件を設定する/詳細な絞込条件を隠す	詳細な絞込条件画面と一覧画面を切替したい場合に選択
⑦提供日時	行政機関等が、あなたの情報を提供した日時
⑧提供機関	あなたの情報を提供した行政機関等名
⑨事務	あなたの情報がやりとりされた事務名
⑩事務手続	あなたの情報がやりとりされた事務名
⑪やりとりされた情報の名称	あなたの情報がやりとりされた情報の名称。やりとりされた情報の名称を選択すると、やりとりされた情報に含まれるすべての項目を確認可能
⑫法第21条第2項各号の該当	通常は「非該当」と表示。マイナンバー法に適合しないため、情報のやりとりが行われなかった場合は、「第1号該当」「第2号該当(提供者)」「第2号該当(照会者)」のいずれかが表示される
⑬あなたの情報を確認ボタン	やりとりされたあなたの情報の詳細を確認。確認メッセージが表示される
⑭前の画面へボタン	一つ前の画面へ戻りたい場合に選択
⑮状況	提供状況
⑯ダウンロードボタン	履歴一覧データを保存
⑰前の画面へボタン	ひとつ前の画面へ戻る

図 3-43 内閣府のマイナポータルの事例:やりとり履歴詳細[11]

内閣府のマイナポータルの事例も踏まえ、情報銀行が取得・提供したデータの包括的な消費者向け閲覧機能として、消費者が自分の提供データを把握・管理しやすい閲覧機能とはどのようなものかを検討した。（表 3-62 参照）

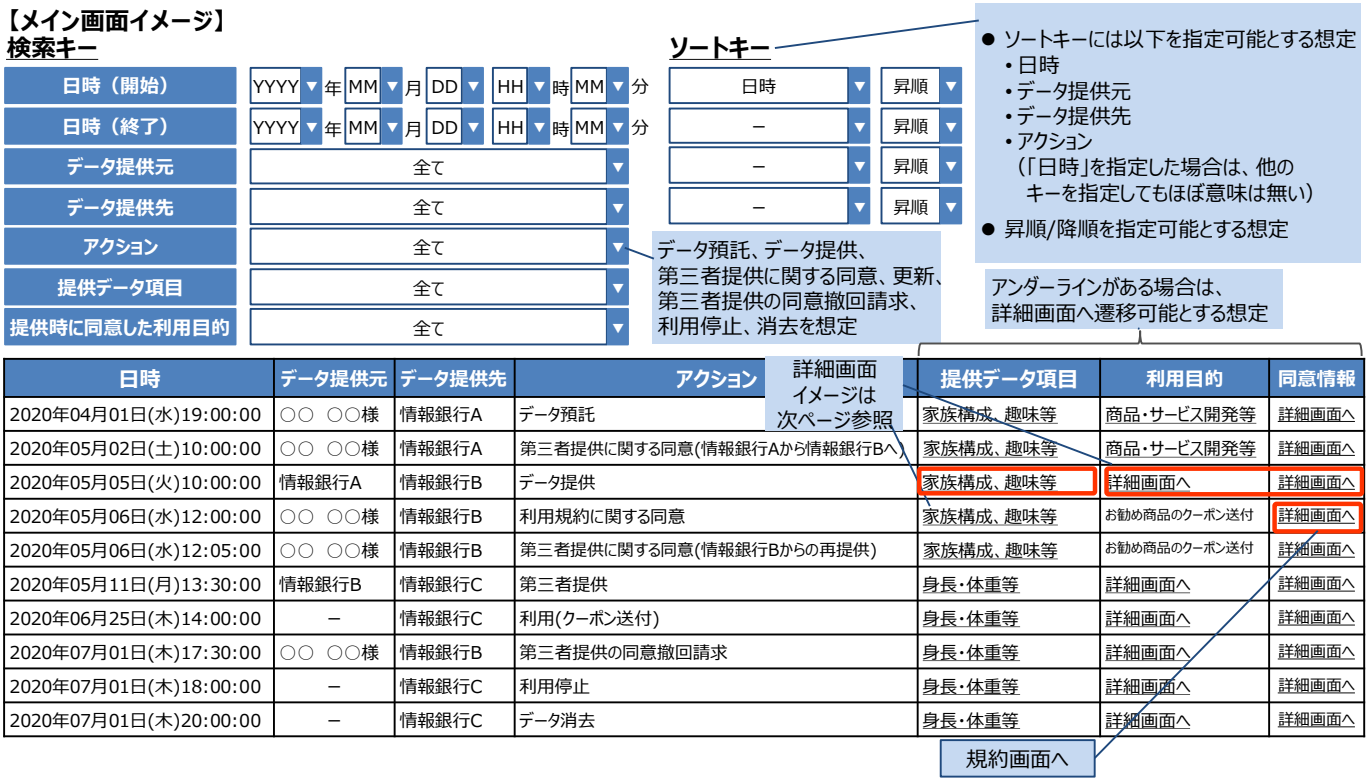
表 3-62 情報銀行が取得・提供したデータの包括的な消費者向け閲覧機能

区分（推奨/必須）	対象	機能
必須 ※具体的な項目については、実現可能性に応じて検討の余地あり	消費者に対して、情報銀行が取得・提供したデータを包括的に検索・一覧表示できる機能を提供可能とする者（情報銀行、または当該プラットフォームを提供する第三者を想定）	情報銀行に預託されたデータについて、情報銀行間を跨って包括的に以下項目を検索・一覧表示できる機能であること。 ・日時 ・データ提供元 ・データ提供先 ・アクション内容（データ預託、データ提供、第三者提供に関する同意、更新、第三者提供の同意撤回請求、利用停止、消去等） ・提供データ項目 ・利用目的 ・同意情報

[11] 出典:内閣府大臣官房番号制度担当室「マイナポータル」の「やりとり履歴詳細」
<https://img.myna.go.jp/manual/03-02/k0057.html>（参照日 2021 年 2 月 17 日）

		理由:消費者が自己のデータの提供先・提供履歴をいつでも容易に確認できることにより、自己のデータのコントローラビリティ確保を実現するため。
推奨	（同上）	参照したいデータに到達し易くなるよう、検索キー、ソートキーの設定が可能であることが望ましい。 理由:提供データの件数、データ項目数が膨大な量に及ぶケースも想定されるため。

具体的な画面イメージを以下（図 3-44 参照）に示す。



日時	データ提供元	データ提供先	アクション	提供データ項目	利用目的	同意情報
2020年04月01日(水)19:00:00	○○ ○○様	情報銀行A	データ預託	家族構成、趣味等	商品・サービス開発等	詳細画面へ
2020年05月02日(土)10:00:00	○○ ○○様	情報銀行A	第三者提供に関する同意(情報銀行Aから情報銀行Bへ)	家族構成、趣味等	商品・サービス開発等	詳細画面へ
2020年05月05日(火)10:00:00	情報銀行A	情報銀行B	データ提供	家族構成、趣味等	詳細画面へ	詳細画面へ
2020年05月06日(水)12:00:00	○○ ○○様	情報銀行B	利用規約に関する同意	家族構成、趣味等	お勧め商品のクーポン送付	詳細画面へ
2020年05月06日(水)12:05:00	○○ ○○様	情報銀行B	第三者提供に関する同意(情報銀行Bからの再提供)	家族構成、趣味等	お勧め商品のクーポン送付	詳細画面へ
2020年05月11日(月)13:30:00	情報銀行B	情報銀行C	第三者提供	身長・体重等	詳細画面へ	詳細画面へ
2020年06月25日(木)14:00:00	－	情報銀行C	利用(クーポン送付)	身長・体重等	詳細画面へ	詳細画面へ
2020年07月01日(木)17:30:00	○○ ○○様	情報銀行B	第三者提供の同意撤回請求	身長・体重等	詳細画面へ	詳細画面へ
2020年07月01日(木)18:00:00	－	情報銀行C	利用停止	身長・体重等	詳細画面へ	詳細画面へ
2020年07月01日(木)20:00:00	－	情報銀行C	データ消去	身長・体重等	詳細画面へ	詳細画面へ

図 3-44 情報銀行が取得・提供したデータの包括的な消費者向け閲覧機能のメイン画面イメージ

閲覧機能利用時の目的に応じて、「検索キー」「ソートキー」をどのように指定すれば閲覧できるかの例を以下（図 3-45 参照）に示す。

<例1>
「趣味」の情報がどこから提供されたものか辿って確認したい場合

検索キー		ソートキー	
日時（開始）	YYYY 年 MM 月 DD HH 時 MM 分	日時	降順
日時（終了）	YYYY 年 MM 月 DD HH 時 MM 分	－	昇順
データ提供元	全て	－	昇順
データ提供先	全て	－	昇順
アクション	データ提供		
提供データ項目	趣味		
提供時に同意した利用目的	全て		

<例2>
情報銀行Aから提供された履歴をデータ提供先ごとに確認したい場合

検索キー		ソートキー	
日時（開始）	YYYY 年 MM 月 DD HH 時 MM 分	データ提供先	昇順
日時（終了）	YYYY 年 MM 月 DD HH 時 MM 分	－	昇順
データ提供元	情報銀行A	－	昇順
データ提供先	全て	－	昇順
アクション	全て		
提供データ項目	全て		
提供時に同意した利用目的	全て		

<例3>
「第三者提供の同意撤回請求」を行った「既往歴」について「利用停止」されているか確認したい場合

検索キー		ソートキー	
日時（開始）	YYYY 年 MM 月 DD HH 時 MM 分	日時	昇順
日時（終了）	YYYY 年 MM 月 DD HH 時 MM 分	－	昇順
データ提供元	全て	－	昇順
データ提供先	全て	－	昇順
アクション	利用停止		
提供データ項目	既往歴		
提供時に同意した利用目的	全て		

<例4>
「身長・体重」データに関する「お勧め商品のクーポン送付」の履歴を直近のものから順に確認したい場合

検索キー		ソートキー	
日時（開始）	YYYY 年 MM 月 DD HH 時 MM 分	日時	降順
日時（終了）	YYYY 年 MM 月 DD HH 時 MM 分	－	昇順
データ提供元	全て	－	昇順
データ提供先	全て	－	昇順
アクション	全て		
提供データ項目	身長・体重		
提供時に同意した利用目的	お勧め商品のクーポン送付		

図 3-45 情報銀行が取得・提供したデータの包括的な消費者向け閲覧機能の検索条件設定例

情報銀行が取得・提供したデータの包括的な消費者向け閲覧機能の詳細画面イメージを以下（図 3-46 参照）に示す。なお、例示する内容は、消費者が契約済の情報銀行 A に対して、契約していない情報銀行 B へのデータ提供を同意した上でデータ提供する包括同意のケースとなる。

提供データ項目	秘匿レベル	秘匿レベルの説明
• 家族構成 • 趣味 • 住所 • 生年月日 • 性別 • 身長 • 体重 • 購買履歴 ・・・	秘匿レベル1	本人の同意に基づいて情報銀行が取得・提供可能な情報
• 特定健診項目 • 処方せん • 検査結果項目 • 調剤明細項目 ・・・ • 診療明細項目	秘匿レベル2	情報銀行における取り扱いに関する議論が必要な要配慮個人情報を含む可能性がある秘匿性の高い情報（2021年3月現在で検討されている情報は、保険医療に関するもの）

※ 本画面は秘匿レベルの説明画面です。提供項目を確認したい場合は「提供データ項目」の詳細画面をご確認ください

「提供先」「利用目的」の詳細画面イメージ

情報銀行Aにおける第三者提供に関する条件

提供先	利用目的	データ範囲
☑ 金融業、保険業	☑ 商品・サービス開発	☑ 秘匿レベル1
		☑ 秘匿レベル2
	☑ 最適な商品の提案（DM通知）	☑ 秘匿レベル1
		☐ 秘匿レベル2
☐ 不動産業，物品賃貸業	☐ 商品・サービス開発	☐ 秘匿レベル1
		☐ 秘匿レベル2
	☐ 最適な商品の提案（DM通知）	☐ 秘匿レベル1
		☐ 秘匿レベル2
☑ 学術研究，専門・技術サービス業	☑ 商品・サービス開発	☑ 秘匿レベル1
		☐ 秘匿レベル2
☐ 宿泊業，飲食サービス業	☐ 商品・サービス開発	☐ 秘匿レベル1
		☐ 秘匿レベル2
・・・	・・・	

情報銀行Bにおける第三者提供に関する条件

提供先	利用目的	データ範囲
☑ 銀行業	☑ 商品・サービス開発	☑ 秘匿レベル1
		☑ 秘匿レベル2
	☐ お勧め商品のクーポン送付	☐ 秘匿レベル1
		☐ 秘匿レベル2
☑ 協同組織金融業	☐ 商品・サービス開発	☐ 秘匿レベル1
		☐ 秘匿レベル2
	☑ 最適な商品の提案（電話）	☑ 秘匿レベル1
		☐ 秘匿レベル2
☑ 貸金業，クレジットカード業等非預金信用機関	☐ 商品・サービス開発	☐ 秘匿レベル1
		☐ 秘匿レベル2
	☑ 最適な商品の提案（電話）	☑ 秘匿レベル1
		☐ 秘匿レベル2
	・・・	・・・

秘匿レベル	秘匿レベルの説明	秘匿レベルの情報項目例
秘匿レベル1	本人の同意に基づいて情報銀行が取得・提供可能な情報	• 生年月日 • 趣味 • 家族構成 • 購買履歴 • 移動履歴 など
秘匿レベル2	情報銀行における取り扱いに関する議論が必要な要配慮個人情報を含む可能性がある秘匿性の高い情報	• 特定健診項目 • 検査結果項目 • 診療明細項目 • 処方せん • 調剤明細項目 など

図 3-46 情報銀行が取得・提供したデータの包括的な消費者向け閲覧機能の詳細画面イメージ

3.5.5.3. 今後の課題・改善点

データ項目に着目した場合、消費者目線としては、複数の履歴を辿らなくても、「現在データを保有している情報銀行・提供先事業者」と「データ連携された経路（例:情報銀行 A→情報銀行 B→企業 X→企業 Z）」が一目でわかる機能が具備されていることが望ましいため、今後の改善点として挙げられる。

また、包括的なトレーサビリティを提供するために、情報銀行間でユーザー識別子や履歴情報を共有する必要があるが、その共有について消費者に予め同意を得ておく必要がある。例えば、利用規約に消費者のユーザー識別子や履歴情報を連携先情報銀行に対して提供することを記載し、同意を得ておく等の対応が必要になる。さらに、予め連携を行う情報銀行間で連携に関する取り決めの契約を締結するにあたり、ユーザー識別子を利用して他の情報銀行から

取得したデータと組み合わせる等して、消費者本人の同意を得ずにトラッキングする行為を禁止することを契約書に明記するといった対策も必要と考える。

3.5.6. データ提供先事業者への情報提供に伴うリスク対策に必要な機能・ルール

情報信託機能の認定基準では、データ提供先についても情報銀行と同様に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）を求める旨が挙げられている。しかし、多くの事業者にとって、情報銀行と同レベルの基準に適合することは困難であるため、「データ提供先事業者」が増えない可能性が想定される。その場合、消費者にとってのメリットも広がらないため、結果的に活用する消費者も増えず、情報銀行事業の発展は厳しいものとなることが予想される。また、情報銀行が林立し、事業者が複数の情報銀行から認定を受けなければならない場合、事業者の負担は更に重いものとなる。そのため、共通の認定基準を設定し、その基準に適合すれば複数の情報銀行との接続可能が認められることが望ましい。そこで、以下（図 3-47 参照）の通り、「データ提供先事業者」に特化した適切な基準を整備することで、情報提供に伴うリスク対策と情報銀行事業の促進を両立する方策について検討する。

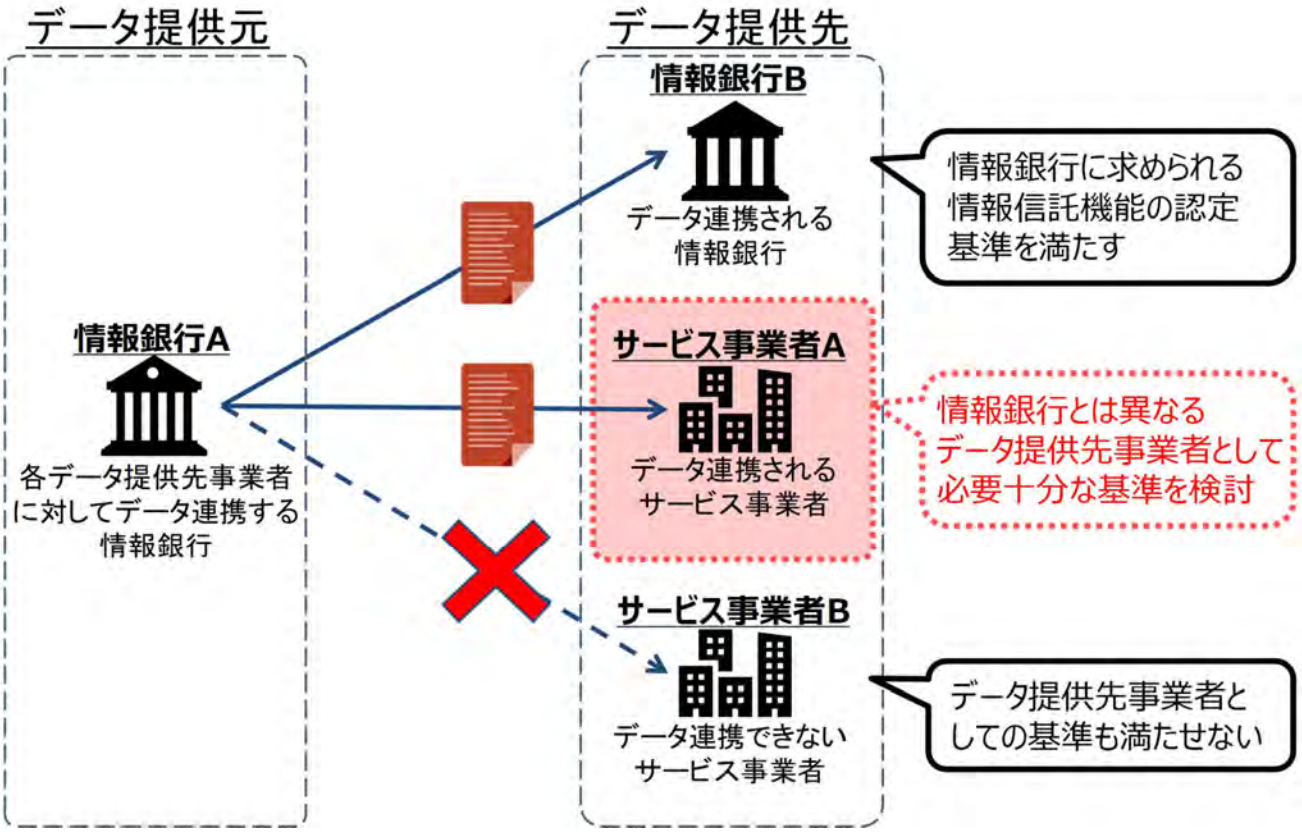


図 3-47 データ提供先事業者への情報提供に伴うリスク対策のイメージ

3.5.6.1. リスクの可視化・深掘り

情報銀行ビジネスにおけるデータ提供先事業者に特化した基準が整備されていない環境下にて、データ提供先事業者へデータ提供を行った場合に想定されるリスクをステークホルダーごとに洗い出した。また、それらのリスクに対する現状の機能・ルールを調査した上で、今後あるべきルールや機能提供を行うにあたっての課題についての検討を行った。

<データ提供先事業者へのデータ提供に伴うリスクと課題>

ステークホルダーごとのリスク

消費者:

- 情報銀行に提供したデータの利活用が期待した程進まないことに対する不満

情報銀行:

- 情報銀行が基準への適合が難しいことによるデータ提供先事業者の僅少化
- 期待した程利活用が進まないことに対する不満よる消費者の利用抑制

データ提供先:

- データ提供先事業者に求められる基準が厳しく、適合することが困難

リスクに対する現状の機能・ルール

提供タイミング:

- 情報信託機能の認定基準として、「データ提供先との間でモデル約款の記載事項に準じた契約を締結することで、データ提供先の管理体制を把握するなど適切な監督をすること、データ提供先にも、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）を求めること等」が挙げられている。

  また、情報銀行が担う義務として、個人情報の第三者提供を行う場合の提供先及び利用目的についての判断基準(認定基準に応じて判断)、判断プロセス、同意の取得方法を明示することが挙げられている（認定指針 ver2.0）。
- 個人情報取扱事業者は、一部例外を除き、あらかじめ本人の同意を得た場合、またはあらかじめ本人に利用目的・提供データ項目・提供方法等を通知するか本人が容易に知り得る状態に置くとともに個人情報保護委員会に届け出たとき以外は、個人データを第三者に提供してはならないとしている（個人情報保護法第二十三条）。

ルール化・機能提供に関する課題

これらを踏まえ、課題として整理すると以下に集約される。

- 課題①情報銀行のデータ提供先事業者としての適格性を判断するのに必要十分であり、かつ提供元となる情報銀行が適切な監督を実施できる基準

この課題について検討を行った。

3.5.6.2. 「課題①情報銀行のデータ提供先事業者としての適格性を判断するのに必要十分であり、かつ提供元となる情報銀行が適切な監督を実施できる基準」に関する検討

情報銀行から第三者提供を行う場合のデータ提供先事業者として必要十分であり、かつ提供元の情報銀行が適切な監督を実施できる基準（提供先が情報銀行ではない場合）を検討するにあたり、プライバシーマークの基準を中心として必要な観点を挙げる。認定指針 ver2.0 の認定基準の遵守基準にて、プライバシーマークまたは ISMS 認証の取得、及び定期的な更新が定められていることから「プライバシーマーク付与適格性審査基準」に着目して観点を検討した（表 3-63 参照）。

表 3-63 提供先・再提供先が講ずべき対策に関するルール

区分（推奨/必須）	対象	ルール
必須	情報銀行ビジネスにおけるデータ提供先事業者	(1)「プライバシーマーク付与適格性審査基準」に定められていない「再提供」に関する追加項目
必須	（同上）	(2)新たな規制への対応項目（改正個人情報保護法等）
必須	（同上）	(3)その他必要と想定される観点の追加項目 ① 認定指針 ver2.0 の認定基準への充足（「情報セキュリティ 具体的基準」の遵守） ② 「プライバシーマーク付与適格性審査基準」の具体化・明確化（安全管理措置） ③ 「プライバシーマーク付与適格性審査基準」について、情報銀行のデータ提供先事業者としては不要となる基準を除外 ④ 上記以外

以下（表 3-64、表 3-65、表 3-66、表 3-67、表 3-68、表 3-69 参照）に、(1)～(3)の詳細を示す。

なお、「対象審査項目」の番号は、JIS Q 15001:2017 附属書 A（(規定)管理目的及び管理策）にて使用されている番号であり、プライバシーマーク付与適格性審査基準の記載もこれに準じている。

表 3-64 (1)プライバシーマーク付与適格性審査基準に定められていない「再提供」に関する追加項目

対象審査項目（追加事項と附属書 A 内の番号）		追加理由
「本人に連絡又は接触する場合の措置」（追加） • 情報銀行から提供された個人情報の本人に対して連絡または接触する場合、法令等で同意が不要とされているときを除き、当該本人に対して情報銀行以外の手段で連絡または接触することに関する同意取得を義務付ける	A.3.4.2.7 の 1	データ提供先事業者が本人に連絡又は接触する場合は、情報銀行が代替して同意取得し、再提供先が本人に接触等する場合は、再提供先で同意取得するものである。 但し、データ提供先事業者が情報銀行から提供された個人情報の本人に対して、情報銀行以外の方法により取得した個人情報を利用して、連絡または接触するときで、情報

		銀行を通じて連絡または接触の同意を得ていないときには、トラブルになる可能性があるため、データ提供先事業者は本人に対して情報銀行以外の手段で連絡または接触の同意を得ることを義務付ける必要がある。
「保有個人データの訂正、追加又は削除」にて、訂正等の請求を受ける経路（変更） • 個人情報保護法では、訂正等の請求を受ける経路が本人からに限定されているが、本人から情報銀行を介した経路についても対象とするよう変更	A.3.4.4.6 の 1～3	基本的には、情報銀行が保有する個人データが正となるため、データ提供先事業者が訂正等を行うことはない。但し、データ提供先事業者が本人の同意を直接得て第三者に再提供している際、情報銀行を経由してデータ提供先事業者が保有個人データの訂正等の事実を認識した場合、第三者の再提供先へ渡っている情報についても訂正等を行うよう義務付ける必要がある。

表 3-65 (2)新たな規制への対応項目（改正個人情報保護法等）

対象審査項目（追加事項と附属書 A 内の番号）		対応理由
「個人データの提供に関する措置」にて、本人同意の取得義務対象ケース（追加） • 第三者提供における本人同意の取得義務について、提供元では個人データに該当しないものの、提供先において個人データとなることが想定されるケース	A.3.4.2.8 の 1	改正個人情報保護法にて追加される予定であり、施行に合わせて対応が必要であるため。
適正な利用義務の明確化に関する禁止事項（新規追加） • 違法又は不当な行為を助長する等の不適正な方法による個人情報の利用の禁止	―	
オプトアウト規制の強化に関する対象範囲の条件（新規追加） • 第三者に提供できる個人データの範囲の限定（不正取得された個人データ、オプトアウト規定により提供された個人データも対象外）	―	
外国にある第三者への提供に係る情報提供の充実（新規追加）	―	

• 当該外国における個人情報の保護に関する制度、当該第三者が講ずる個人情報の保護のための措置、その他当該個人に参考となるべき情報の提供		
仮名加工情報の取扱い（新規追加） • 第三者への提供には本人の同意が必要 • 内部分析に限定する等を条件に、開示・利用停止請求への対応等の義務を緩和	—	
保有個人データに関する公表事項（追加） • 事業者の住所、事業者である法人の代表者の氏名 • 個人データの第三者提供時の記録の閲覧手続 • 利用停止等の手続 • 共同利用時の管理責任者の住所、管理責任者である法人の代表者の氏名	—	改正個人情報保護法にて追加された内容であり、同等のレベルを求められるため。
「個人情報を取得した場合の措置」にて、利用目的の通知又は公表に対する条件（追加） • 利用目的の通知又は公表について、利用目的の通知又は公表が利用者に理解しやすいものであること（説明の具体化、平易に利用できる用語の使用、説明文の記載場所のわかりやすさ、他のサービスの利用に関する説明との明確な区別等）	A.3.4.2.4 の 1	「デジタル・プラットフォーマーと個人情報等を提供する消費者との取引における優越的地位の濫用に関する独占禁止法上の考え方」において、利用目的を消費者に知らせずに個人情報を取得したと判断されるケースとして、一般的な消費者が利用目的を理解することが困難な状況で消費者の個人情報を取得した場合が挙げられているため。
個人情報等の不当な取得に関する禁止事項（新規追加） • 消費者がサービスを利用するための対価として提供している個人情報等とは別に、個人情報等その他の経済上の利益を提供させることの禁止	—	「デジタル・プラットフォーマーと個人情報等を提供する消費者との取引における優越的地位の濫用に関する独占禁止法上の考え方」において、「優越的地位の濫用として問題」としている内容であるため。

表 3-66 (3) その他必要と想定される観点の追加項目

①プライバシーマーク付与適格性審査基準の具体化・明確化（安全管理措置）

対象審査項目（追加事項と附属書 A 内の番号）		追加理由
安全管理措置（追加）	A.3.4.3.2 の 1	プライバシーマーク付与適格性審査基準では、個人情報を特定し、特定した個人情報

• 個人情報を扱う責任者その他の体制整備等を行う「安全管理措置」、個人情報を取り扱う従業員への定期的な研修等を行う「人的安全管理措置」、個人情報を扱う区域・機器の管理等を行う「物理的安全管理措置」、個人情報へのアクセス制御等を行う「技術的安全管理措置」等、安全管理措置の内容をより具体化かつ明確化すること		についてリスクアセスメントを実施、そのリスクに応じた安全管理措置を講じることとなっている。これらの安全管理措置が講じられていることを担保できるよう、項目の具体化・明確化が必要である。

表 3-67 (3) その他必要と想定される観点の追加項目

②認定指針 ver2.0 の認定基準への充足（「情報セキュリティ 具体的基準」の遵守）

対象審査項目（追加事項と附属書 A 内の番号）		追加理由
資産の管理（新規追加） • 情報及び情報処理施設に関連する資産の洗出し、特定、適切な保護の責任設定 • 固有のデータセンター保有、又はそれと同等の管理が可能な委託先データセンターの確保 • 外部クラウドを活用時の契約上の情報セキュリティ要件担保 • 情報を取り扱う媒体等から情報を削除・廃棄可能な体制もしくは仕組みの保有 • 対象となる事業で扱う情報の他事業との明確な区分、及び管理 • 外部クラウド活用時、委託時における相手方事業者との裁判管轄(日本の裁判所)・準拠法(日本法)の合意	—	認定指針 ver2.0 の「情報セキュリティ 具体的基準」にて定められている基準と同等のレベルが求められる。
運用の情報セキュリティ（新規追加） • 情報処理設備の正確かつ情報セキュリティ担保のための操作手順書・管理策の策定・実施 • マルウェアからの保護のための検出、予防、回復の管理策の策定・実施 • ログ等の常時分析による、不正アクセスの検知に関する対策、及び情報漏洩防止措置 • 技術的ぜい弱性管理、平時のログ管理や攻撃監視等に関する基準整備	—	

• サイバー空間の情勢把握、及び運用上のアップデート実施		
システムの取得・開発・保守（新規追加） • 新システム取得時及び既存システム改善時における要求事項への情報セキュリティ要求事項の組込み • 開発環境及びサポートプロセス（外部委託など）における情報セキュリティ管理策の策定・実施	—	
供給者関係（新規追加） • 供給者との間における、関連する全ての情報セキュリティ要求事項の確立、合意、定期的監視 • 要求事項への ICT サービス・製品のサプライチェーンに関連する情報セキュリティリスク対処の包含	—	
事業継続マネジメントにおける情報セキュリティの側面（新規追加） • 組織の事業継続マネジメントシステムへの情報セキュリティ継続の組込み	—	
「内部向け個人情報保護方針」を文書化した情報について、必要に応じた方針の見直し、更新が行われること（追加）	A.3.2.1 の 4	認定指針 ver2.0 の「情報セキュリティ 具体的基準」にて定められている基準(情報セキュリティ方針を策定し、経営層、取り扱う従業員層への周知、必要に応じた方針の見直し、更新)と同等のレベルが求められるため。
「緊急事態への準備」として必要な対応（追加） • 定期的な脆弱性検査に関する基準や脆弱性発見時の対応体制などの整備 • 外部アタックテストなどのセキュリティチェック、インシデント対応訓練やセキュリティ研修などの定期的な実施	A.3.3.7 の 5・6	認定指針 ver2.0 の「情報セキュリティ 具体的基準」にて定められている基準と同等のレベルが求められるため。
「安全管理措置」として必要な対応（追加） • 情報セキュリティに関する情報を収集・交換するための制度的枠組みへの加盟 • アクセス制御に関する規定の策定・対応 • 情報の機密性、真正性、完全性保護のための暗号の適切で有効な利用	A.3.4.3.2 の 2～5	

• 電子政府推奨基準で定められている暗号の採用や、システム設計の確認 • 自然災害に対する物理的な保護の設計・適用 • 外部クラウド活用時の契約上の情報セキュリティ要件担保		

表 3-68 (3) その他必要と想定される観点の追加項目

③プライバシーマーク付与適格性審査基準について、情報銀行としては不要となる基準を除外

対象審査項目（追加事項と附属書 A 内の番号）		追加理由
「個人情報を取得した場合の措置」の例外事項（本人への利用目的の通知または公表を要しない場合に関する項目）	A.3.4.2.4 の 2	データ提供先事業者が個人情報を取得・活用できるのは、情報銀行がデータ提供先事業者による利用目的を公表し、本人の同意を得た場合のみと想定されるため。
「本人に連絡又は接触する場合の措置」に関する例外項目	A.3.4.2.7 の 2・3	データ提供先事業者が本人に連絡又は接触する場合は情報銀行が代替し、その旨同意を得るものとすること、また、再提供先が本人に接触等する場合は再提供先で同意を得るものと想定されるため。
「個人情報に関する権利」の本人から開示等の請求等受け付けた場合の対応にて、「保有個人データに当たらないもの」として対象外を定めた項目	A.3.4.4.1 の 2	情報銀行が扱うのは預託されたデータであり、保有個人データに当たるか当たらないかは関係ないため。
「保有個人データの利用目的の通知」を求められても通知を必要としないケース、及び通知を必要としないケースに該当することを本人へ通知・説明することを定めた項目	A.3.4.4.4 の 2・3	データ提供先事業者が個人情報を取得・活用できるのは、利用目的を公表し、本人の同意を得た場合のみと想定され、利用目的は既に通知済みと想定されるため。

※他の基準の文言にて上記審査項目の番号が指定されている場合は、併せて記述を変更する必要がある。

表 3-69 (3) その他必要と想定される観点の追加項目

④その他

対象審査項目（追加事項と附属書 A 内の番号）		追加理由
「個人情報の特定」の手順に関する文書化対象（変更） • 個人情報保護法では、文書化の対象が自らの事業の用に供している全ての個人情報に限定されているが、情報銀行から提供を受けた個人情報、及び当該個人情報と併せて管理するその他の個人情報を対象とするよう変更	A.3.3.1 の 1	情報銀行から提供される個人情報を扱うにあたり、同等の基準を設定することが必要なため。
「個人情報に関する権利」にて、開示等の請求等を受け付ける経路（変更） • 個人情報保護法では、開示等の請求等を受ける経路が本人からに限定されているが、本人から情報銀行を介した経路についても対象とするよう変更	A.3.4.4.1 の 1	情報銀行から提供される個人情報を扱うにあたり、同等の基準を設定することが必要なため(データ提供先事業者では、主として情報銀行を経由した手続きとなる)。
「保有個人データの利用目的の通知」にて、利用目的の通知を受け取る経路（変更） • 個人情報保護法では、利用目的の通知を受け取る経路が本人からに限定されているが、本人から情報銀行を介した経路についても対象とするよう変更	A.3.4.4.4 の 1	
「保有個人データの開示」にて、開示等の請求等を受け付ける経路（変更） • 個人情報保護法では、開示等の請求等を受け付ける経路が本人からに限定されているが、本人から情報銀行を介した経路についても対象とするよう変更	A.3.4.4.5 の 1	
「保有個人データの利用又は提供の拒否権」にて、利用停止等の請求を受け取る経路（変更） • 個人情報保護法では、利用停止等の請求を受け取る経路が本人からに限定されているが、本人から情報銀行を介した経路についても対象とするよう変更	A.3.4.4.7 の 1	
「保有個人データの利用又は提供の拒否権」にて、利用停止等の請求を受け取る経路（変更）	A.3.4.4.7 の 2	

• 個人情報保護法では、利用停止等の請求を受け取る経路が本人からに限定されているが、本人から情報銀行を介した経路についても対象とするよう変更		
「苦情及び相談への対応」にて、苦情を受け取る経路（変更） • 個人情報保護法では、苦情を受け取る経路が本人からに限定されているが、本人から情報銀行を介した経路についても対象とするよう変更	A.3.6 の 5	

3.5.6.3. 今後の課題・改善点

情報銀行事業の推進・発展を目指すためには、個人情報を適切に取り扱うことができるセキュリティ基準・ガバナンス体制等の維持を前提としつつ、様々な事業者の意見・要望を踏まえ、適切に基準を見直していくことが必要である。

総務省の「情報信託機能の認定スキームの在り方に関する検討会」では様々な有識者や事業者で構成された「認定・運用ワーキンググループ」が設置され、提供先第三者に係る情報銀行の認定・運用上の課題や選定条件について議論が行われている。今後、提供先第三者の選定について取りまとめがなされる予定であるため、その結果を踏まえ、整合性を取りつつ、適切に見直しを行う必要がある。

3.5.7. データポータビリティ、及び付随して必要になる改竄防止策、盗聴防止策に関する機能・ルール

改正個人情報保護法によって、データ提供元企業等の個人情報取扱事業者が保有する個人データに対して、消費者本人が電磁的記録形式のデータの開示請求を行うことができるようになった。法改正を踏まえ、情報銀行が消費者の代理となり、様々なデータ提供元企業に対して、電磁的記録形式での個人情報開示請求を行うことによって、データポータビリティが推進される。そのため、下記想定フロー（図 3-48 参照）の実現に必要な方法及びその際の改竄・盗聴防止策について検討した。

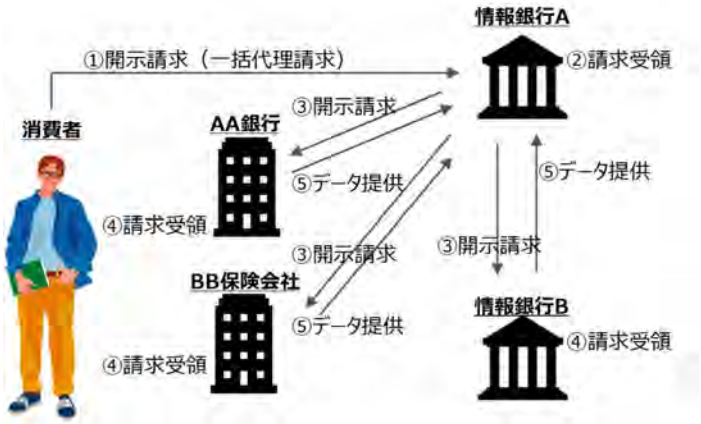


図 3-48 消費者による電磁的記録形式での開示請求のフロー

3.5.7.1. リスクの可視化・深掘り

データポータビリティ、データ流通時の改竄・盗聴の防止に必要な機能・ルールが整備されていない環境下におけるリスクをステークホルダーごとに洗い出し、それらのリスクに対する現状の機能・ルールを調査した上で、今後あるべきルールや機能提供を行うにあたっての課題についての検討を行った。

また、リスクについては、以下の通り、「データポータビリティの権利の確保」、「第三者による不正請求」、「第三者による盗聴」、「消費者本人や代理人によるデータ改竄」の 4 つの観点でそれぞれ整理した。

＜データポータビリティに関するリスクと課題（データポータビリティの権利の確保）＞

ステークホルダーごとのリスク

消費者:

- データポータビリティの権利が確保されない可能性がある

情報銀行:

- (特になし)

データ提供先:

- 電磁的記録の提供への環境整備ができない（書面での交付しかできない）

リスクに対する現状の機能・ルール

請求タイミング:

- 保有個人データの開示方法について、電磁的記録の提供を含め、本人が指示できるように定められている。（改正個人情報保護法　第二十八条）

ルール化・機能提供に関する課題

請求タイミング:

- 情報銀行を介した電子的な情報開示のための機能及びそのルールの策定

＜データポータビリティに関するリスクと課題（第三者による不正請求）＞

ステークホルダーごとのリスク

消費者:

- 自分のデータが第三者によって開示請求されてしまう可能性がある

情報銀行:

- 開示請求が、データの所有者本人ではない第三者によって行われる可能性がある
- 本人に委任されていない代理人による請求に対応してしまう可能性がある

データ提供先:

- 情報銀行からの開示請求がデータ所有者本人によるものではなく、不正な請求に基づくものである可能性がある

リスクに対する現状の機能・ルール

請求タイミング:

- 開示請求等は本人が委任した代理人によって実施することができる。（個人情報保護法 第三十二条第三項、同法施行令 第十一条）
- 個人情報取扱事業者は、開示等の請求を受け付ける方法として、以下 4 点を定めることができる。（個人情報保護法施行令 第十条）
  - 開示等の請求等の申出先
  - 開示等の請求等に際して提出すべき書面等の請求等の方式
  - 開示等の請求等をする者が本人又は代理人であることの確認の方法
  - 手数料の徴収方法

ルール化・機能提供に関する課題

請求タイミング:

- データの移転の請求を行う者が当該個人であることを確認する機能の導入及びそのルールの策定

＜データポータビリティに関するリスクと課題（第三者による盗聴）＞

ステークホルダーごとのリスク

消費者、情報銀行、データ提供先:

- データ流通の際に第三者にデータを盗み取られる可能性がある

リスクに対する現状の機能・ルール

請求タイミング:

- 個人情報の漏洩や滅失、破棄損防止のための安全管理措置を講じる必要がある。（個人情報保護法第二十条）

ルール化・機能提供に関する課題

請求タイミング:

- 盗聴を防止するための機能及びそのルールの策定

＜データポータビリティに関するリスクと課題（消費者本人や代理人によるデータ改竄）＞

ステークホルダーごとのリスク

消費者:

- (特になし)

情報銀行:

- 消費者や代理人によって改竄された不正なデータを提供してしまうこと

データ提供先:

- 消費者や代理人によって改竄されたデータを活用することにより、損害を受ける可能性がある

リスクに対する現状の機能・ルール

受領タイミング:

- 消費者や代理人によるデータの改竄を防止するためのルールはない。

ルール化・機能提供に関する課題

受領タイミング:

- データの改竄を防止するための機能の導入及びそのルールの策定

上記の整理によって、洗い出した課題を整理すると、以下の 4 つに大別される。

- 課題①情報銀行を介したデータの移転に関する電子的な請求
- 課題②データの移転に関する請求を行う者が当該個人であることの確認
- 課題③データの移転時における盗聴防止
- 課題④データの移転時における改竄防止

これらの課題に関する検討を行った。

3.5.7.2. 「課題①情報銀行を介したデータの移転に関する電子的な請求」に関する検討

情報銀行（情報銀行が委託するプラットフォームを含む）を介した電子的な情報開示を実現するために、まず、データ提供元からデータを受領するデータ提供先の情報銀行が具備すべき主な機能は以下の 4 つが考えられる。

① 消費者がデータの移転を情報銀行に対して電子的に請求できる機能
② 消費者からのデータ移転の請求をデータ提供元に連携する機能
③ 消費者が指定したデータ提供先に電子的なデータの移転を行う機能
④ データの移転の状況（移転中・移転完了等）を消費者に連携する機能（及び移転が完了した際に報告や通知を行う機能）

さらに、①の機能については、情報銀行に接続しているデータ提供元の一覧を表示する機能、各データ提供元が保有しているデータを一覧表示する機能、消費者が移転させたいデータを選択（申請）し、そのデータの移転を代理人（情報銀行）に委任する機能の 3 つの機能で構成される。

次に、移転の請求を受け、移転先のデータ提供先にデータを提供することになるデータ提供元（情報銀行含む）が具備すべき主な機能は、保有している消費者のデータの形式や項目をデータ提供先となる情報銀行に連携する機能である。

以下（表 3-70 参照）に具備すべき主な機能をまとめる。

表 3-70 情報銀行を介した電子的な情報開示のための機能

区分（推奨/必須）	対象	機能
必須	情報銀行	【消費者がデータの移転を情報銀行に対して電子的に請求できる機能】 データポータビリティを実現するために、情報銀行と接続しているデータ提供元に対して、消費者が自己のデータの移転を情報銀行に対して請求できる。本機能は、以下の 3 機能で構成される。 ・ 情報銀行に接続しているデータ提供元の一覧を表示する機能 ・ 各データ提供元が保有しているデータを一覧表示する機能 ・ 消費者が移転させたいデータを選択（申請）し、そのデータの移転を代理人（情報銀行）に委任する機能 理由:消費者にとって利便性の高いデータポータビリティを実現するため
		【消費者からのデータ移転の請求をデータ提供元に連携する機能】 消費者が情報銀行に行った、データの移転の請求の内容を、請求に関連するデータ提供元に連携する。 理由:情報銀行が窓口となって、消費者からのデータの移転の請求をとりまとめており、その内容をデータ提供元に連携する必要があるため
		【消費者が指定したデータ提供先に電子的なデータの移転を行う機能】 消費者の同意に基づいて、消費者が指定したデータ提供先に等がデータを移転させる。 理由:電子的に実施することにより、消費者負担が少ないデータポータビリティを実現するため

		【データの移転の状況（移転中・移転完了等）を消費者に連携する機能（及び移転が完了した際に報告や通知を行う機能）】 消費者が実施したデータの移転請求後のステータスを表示する。 理由:消費者が自己のデータの移転請求後のステータスを確認できるようにするため
	データ提供元事業者（情報銀行含む）	【保有している消費者のデータの形式や項目をデータ提供先とる情報銀行に連携する機能】 データ提供元事業者（情報銀行含む）が、保有している消費者のデータの形式や項目をデータ提供先となる情報銀行に連携する。 理由:情報銀行が消費者に対して、データ提供元が保有しているデータに関する情報を開示するため

上記の情報銀行を介した電子的な情報開示のために必要な機能に関して、データポータビリティの実現に向けた利害関係者間の契約に対するルールを以下（表 3-71 参照）のように設ける。なお、必ずしも情報銀行同士が直接契約を締結する必要はないが、利害関係者がルールを遵守する枠組みが必要になる。

表 3-71 データポータビリティの実現に向けた利害関係者間の契約に関するルール

区分（推奨/必須）	対象	ルール
推奨	情報銀行/データ提供元事業者（情報銀行含む）	データ移転に関する契約を締結すること。契約で定めるべき主な項目を以下に記載する。 ＜提供データの提供方法＞ ・ データの形式（PDF、Excel 等の電子形式） ・ データの提供手段（API 等） ・ データの項目（粒度、表記） ※粒度の例:住所のデータとして、「東京都港区」としてまとめて扱っているのか、市区町村ごとに区別して扱っているのか等 ※表記の例:生年月日を西暦で扱っているか、和暦で扱っているか等 ＜データ移転の期限に関するルール＞ ・ 情報銀行が消費者からの申請をデータ提供元に連携する期限

		・ データ提供元が、情報銀行からの申請の連携後に当該データを情報銀行に提供する期限 ・ 情報銀行が、データ提供元から当該データの受領後に指定されたデータ提供先にデータを移転する期限 ※いずれの期限も推奨期限として 1 営業日以内とする
推奨	情報銀行	データ移転に関する契約を締結すること。契約で定めるべき主な項目を以下に記載する。なお、便宜的に、データ提供先となる情報銀行を情報銀行 A、データ提供元となる情報銀行を情報銀行 B とする。 ※基本的に、上記の項目と同様であるが、留意点を記載する ＜提供データの提供方法＞ データの形式や項目については、情報銀行 B がデータクレンジングや結合の加工を実施したうえで、情報銀行 A に提供するかどうかを契約で定めること ＜データ移転の期限に関するルール＞ 情報銀行 B が、既に所有している情報を情報銀行 A に連携する期限 ※推奨期限として 1 営業日以内とする

上記に記載されていない契約に関する規則やルールについては、経済産業省の「AI・データの利用に関する契約ガイドライン[12]」等を参照すること。また、ルールの設計にあたり、データ提供先となる情報銀行とデータ提供元（情報銀行を除く）間、及びデータ提供元となる情報銀行間で API 等を活用したデータ連携の仕組みの整備が必要になることにも留意すること。

[12] 出典:経済産業省「AI・データの利用に関する契約ガイドライン」
＜https://www.meti.go.jp/press/2018/06/20180615001/20180615001-1.pdf＞（参照日 20201 年 2 月 17 日）

3.5.7.3. 「課題②データの移転に関する請求を行う者が当該個人であることの確認」に関する検討

データの移転請求の際に、第三者による不正な請求を防止するために、サービス利用者に対するオンラインでの本人確認機能とともに、データの移転請求を行う者が消費者本人であることを情報銀行が確認するための本人認証機能（表 3-72 参照）が必要である。これらの機能によって、情報銀行は、データ提供元に対して、データの移転請求が当該データの所有者本人の意思に基づいていることを担保することができる。

表 3-72 データの移転の請求を行う者が当該個人であることを確認する機能

区分（推奨/必須）	対象	機能
推奨	情報銀行	【本人確認機能】 消費者がサービス利用開始時に、消費者に対して本人確認を行う。本人確認のレベルは下表のルールに従う。 理由:データの移転請求を念頭に、サービス利用者が、当該データの保有者本人であることを確認するため
推奨		【本人認証機能】 消費者によるデータの移転請求時に、当該請求が消費者本人によって行われていることを確認する。本人認証の手段は下表のルールに従う。 理由:データの移転請求を行う者が、当該データの所有者本人であることを確認するため

また、データの移転請求を行う者が当該個人であることを確認する機能に関して、以下（表 3-73、表 3-74 参照）のルールを設ける。

表 3-73 データ移転の請求者に対する本人確認に関するルール

区分（推奨/必須）	対象	ルール
推奨	情報銀行	消費者によるデータ移転の請求依頼を受け付けるにあたって、データ提供元事業者から要配慮個人情報等の秘匿レベルの高い情報（秘匿レベル 2 以上を想定）を収集する場合は、事前に犯罪収益移転防止法規定の本人確認を行うこと
推奨	データ提供元事業者（情報銀行含む）	当該データ提供元の事業や取り扱うサービスに応じて、データ移転の代理請求元（データ提供先）となる情報銀行との契約において本人確認の実施の必要性・厳格性について定めること

表 3-74 データ移転の請求者に対する本人認証に関するルール

区分（推奨/必須）	対象	ルール
推奨	情報銀行	情報銀行は、データの移転請求を行う者が、本人確認を行ったデータの保有者本人であることを確認するために、本人認証の厳格性と採用の必要性を判断すること。なお、本人認証を採用する場合は、知識要素・所有要素・生体要素の認証要素を複数組み合わせた多要素認証を採用することを推奨する ・（知識要素の例）ID／パスワード、秘密の質問等 ・（所有要素の例）SMS 認証やアプリ認証、IC カード等 ・（生体要素の例）顔や指紋、虹彩、声紋、静脈認証等

3.5.7.4. 「課題③データ移転時における盗聴防止」に関する検討

データ移転の際に想定される盗聴インシデントとして、①意図しない事業者へのデータの提供と、②データの盗み取りがある。盗聴インシデント①については、情報銀行が、ネットワークの改竄等を起因として、意図していないデータ提供先に、データを提供してしまう（正規のデータ提供先にデータが提供されない）ケースが想定される。また、盗聴インシデント②については、第三者が、情報銀行とデータ提供先を接続する通信ネットワークに仮想的な迂回経路を作成し、データを盗み取る（正規のデータ提供先にもデータは提供される）ケースが想定される。

これら盗聴インシデントに対応するため、情報銀行は、SSL/TLS 等を採用した、データ移転時の盗聴を防止するための通信データの暗号化を行う機能（表 3-75 参照）を具備する必要がある。

表 3-75 データの移転時における盗聴防止に関する機能

区分（推奨/必須）	対象	機能
必須	情報銀行	【通信データの暗号化を行う機能】 SSL/TLS 等を採用し、移転されるデータの暗号化を行う。 理由:データ移転時の第三者による盗聴を防止するため

また、データの移転時における盗聴を防ぐための対応ルールとして、以下（表 3-76 参照）を設ける。

表 3-76 データの移転時における盗聴防止に関するルール

区分（推奨/必須）	対象	ルール
推奨	情報銀行/データ提供先事業者/データ提供元事業者	情報銀行及びデータ提供元/データ提供先間で、データの盗聴があった場合に備え、責任及び損害等の負担に関する項目（責任や損害賠償を負担する/しない条件等を明記）を契約に盛り込むこと。

推奨	情報銀行/データ提供先事業者/データ提供元事業者	API を通じてデータを移転する場合、金融 API 向けのセキュリティ標準である FAPI（Financial-grade API）の基盤となる OAuth 2.0 等によって、API セキュリティを担保すること。

3.5.7.5. 「課題④データの移転時における改竄防止」に関する検討

データ移転の際に想定される改竄インシデントとして、①悪意のあるデータの変更、②データの一部の削除（秘匿）、③データの捏造が想定される。改竄インシデント①については、例えば、ローンの契約時に、源泉徴収票を所属会社から金融機関へ共有する際に、融資条件を良くするために、所得金額を 100 万円上積みして変更する等のケースが想定される。また、改竄インシデント②については、健康診断のデータを病院から生命保険会社に共有する際に、保険料金を下げるために、既往症のデータ等のデータの一部を故意に削除（秘匿）する等のケースが想定される。最後に、改竄インシデント③については、現在所属している企業から転職先へ業務経歴のデータを共有する際に、事実ではない過去の経歴を捏造して追加する等のケースが想定される。これら改竄インシデントに対応するため、情報銀行は、「第三者からのデータ移転時の改竄を防止するための通信データの暗号化を行う機能（SSL/TLS を採用する等）」や、「本人及び代理人によるデータの改竄を防止するための機能（電子署名の技術等）」を具備する必要がある。

また、改竄インシデントに該当しない適切なケースとして、訂正ケース④データ提供元に対するデータの誤りの訂正依頼・再取得や、適切な加工ケース⑤データクレンジング・結合が想定される。訂正ケース④については、健康診断のデータを病院から生命保険会社に共有する際に、消費者本人がデータの誤りを発見し、再度病院に訪れ、誤りを修正してもらう等のケースが想定される。また、加工ケース⑤については、情報銀行が、データ提供先がデータをそのまま活用できるように、データの正規化等のデータの品質向上のための加工（データクレンジング）や、必要に応じて結合を行う等のケースが想定される。本書では、データを編集するが適切なケース④、⑤については共にデータの改竄には該当しないものとする。なお、訂正ケース④に対応するために情報銀行が具備すべき機能として、「誤ったデータを訂正するために消費者がデータ提供元に対して訂正の申請を実施できる機能」や、「データ提供元が消費者からの申請に基づいて、データの誤りを電子的に訂正する機能」がある。また、加工ケース⑤においては、「データ提供元から連携されたデータに対して、データクレンジングや結合を行う機能」を情報銀行が具備する必要がある。

上記インシデントへの対策等として、情報銀行やデータ提供元事業者などのステークホルダーが具備すべき機能を以下（表 3-77 参照）にまとめる。

表 3-77 データの移転時における改竄防止に関する機能

区分（推奨/必須）	対象	機能
改竄インシデント①悪意のあるデータの変更 改竄インシデント②データの一部の削除（秘匿） 改善インシデント③データの捏造		
必須	情報銀行	【通信データの暗号化を行う機能】 SSL/TLS 等を採用し、移転されるデータの暗号化を行う。 理由:第三者からのデータ移転時の改竄を防止するため

		【データの改竄を防止するための機能】 電子署名技術等を使用し、移転されるデータの改竄を検知する。 理由:本人及び代理人によるデータの改竄を防止するため
適切な訂正ケース④データの誤りの訂正依頼・再取得		
必須	情報銀行	【消費者がデータ提供元に対して訂正の申請を実施できる機能】 データに不備があった場合、消費者がデータ提供元に対して、データの訂正申請をできる。 理由:消費者は自身でデータの変更（修正等）を実施することができないため、データ提供元に変更の申請をする必要がある。また、消費者による改竄を防止するため
	データ提供元事業者（情報銀行含む）	【データの誤りを訂正する機能】 データ提供元事業者（情報銀行含む）が、上記の消費者による申請に基づいて、保有している消費者のデータを訂正する。 理由:改竄防止の観点から、消費者本人による訂正ができないため
適切な加工ケース⑤データクレンジング・結合		
推奨	情報銀行	【データクレンジングや結合を行う機能】 データ提供元から連携されたデータに対して、データクレンジングや結合を行う。 理由:データ提供先事業者に対して、情報銀行が付加価値を提供するため

上記に記載した、データ移転時のデータの改竄を防止するための機能及びデータクレンジング・結合のための機能に関して、以下（表 3-78、表 3-79 参照）のルールを設ける。

表 3-78 データの移転時における改竄防止に関するルール

区分（推奨/必須）	対象	ルール
必須	情報銀行/データ提供元事業者（情報銀行含む）	本人及び代理人によるデータの訂正を禁止し、データの作成者（データ提供元）のみが正しいデータ等へデータを修正できるものとすること。

表 3-79 データクレンジング・結合に関するルール

区分（推奨/必須）	対象	ルール
必須	情報銀行/データ提供先事業者（情報銀行含む）/情報銀行プラットフォームを提供する第三者	情報銀行とデータ提供先間で、情報銀行によるデータ加工（クレンジング・結合）後のデータ提供方法に関する契約を締結すること。 <データの提供方法> ・データの形式（PDF、Excel 等の電子形式) ・データの提供手段（API 等） ・データの加工方法（データクレンジング・結合) ・ 加工前のデータの提供の要否 ・データの項目（粒度、表記） また、データ提供元の同意がある場合、情報銀行プラットフォームを提供する第三者によるデータ加工（クレンジング・結合等）は可能であるものとする。

3.5.7.6. **今後の課題・改善点**

上記の機能の実装及びルールの導入によって、データポータビリティを実現する環境の整備と、データポータビリティに伴う改竄や盗聴の脅威への対策の実行が可能になる。但し、サイバー攻撃は日進月歩で多様化・巧妙化していくことから、これらの脅威に対応するために有効なサイバーセキュリティ対策を更新・実行していく必要がある。また、有効な対策を講じていたにも関わらず、多様化・巧妙化したサイバー攻撃によって、データの改竄や盗聴を含めたインシデントが発生してしまった場合における利害関係者間の責任について、当事者間の契約をもって詳細に定めていくことが今後の課題である。なお、データ提供元事業者とデータ提供先事業者の当事者間で契約を行う場合、接続する事業者の数だけ契約数が増えてしまうことが想定される。そのため、各事業者の仲介機関となるプラットフォーム等を活用することによって、契約に関する事業者の負担を軽減するなどの対策の検討も必要と考える。

3.6. 情報銀行間連携仕様に関するアンケート調査

3.6.1. ご協力頂いた情報銀行サービス事業者（五十音順・敬称略）

オープンな情報銀行間連携仕様を策定するため、2021 年 2 月時点で一般社団法人日本 IT 団体連盟の情報銀行認定を取得済かつ本実証事業の趣旨に賛同頂けた情報銀行サービス事業者にオブザーバーとしてアンケート調査にご協力頂いた。

- 株式会社 J.Score（ジェイスコア）
- 中部電力株式会社
- 株式会社 DataSign（データサイン）
- フェリカポケットマーケティング株式会社
- 株式会社マイデータ・インテリジェンス

3.6.2. 実施概要

実施したアンケート調査の概要は以下の通りである。

【調査目的】本実証事業で策定する情報銀行間連携仕様の品質向上
【調査対象】情報銀行サービス事業者（5 社）
【調査内容】第 1 回:情報銀行間連携時おける共通仕様を検討する上での観点・考慮点
第 2 回:情報銀行間連携時におけるドラフト版の共通仕様に対する改善点・要望
【調査手法】アンケート形式
【調査時期】第 1 回:2020 年 8~9 月
第 2 回:2020 年 12 月

第 1 回アンケートでは、情報銀行間連携時における共通仕様となる「認証仕様」と「データ定義」を検討する上での観点・考慮点についてご意見を頂いた。

第 2 回アンケートでは、第 1 回アンケートで頂いた意見を踏まえて作成した情報銀行間連携時におけるドラフト版の共通仕様に対して、情報銀行サービスを利用する立場になって消費者目線で認証時やデータ連携時の「ユーザーインターフェース」に関する改善点・要望についてご意見を頂くと共に、情報銀行サービスを提供する立場から事業者目線で「認証仕様」と「データ定義」に対する改善点・要望についてご意見を頂いた。

なお、第 1 回と第 2 回アンケートの際に「情報銀行やデータ流通に関する普及、促進」についてのご意見も頂いたため、併せて本節でまとめる。

3.6.3. アンケート結果

各事業者から頂いた具体的な意見、及び意見に対する考察を以下にまとめる。

3.6.3.1. 【第 1 回アンケート】認証仕様の検討について頂いたご意見

観点 1. 検討する認証方式の採用方針

本実証事業では認証基盤のアーキテクチャについて、「独立した認証基盤（認証局等）を利用する方式」と「信頼関係を結び、データ連携し合う情報銀行が、認証機能も担う方式」の 2 案を比較検討し、その結果現時点における実現性の高さを評価して後者の「情報銀行が、認証基盤も担う方式」を採用する方針とした。この方針について各事業者からご意見を頂いた。

回答結果

各社が選択した回答状況は以下の通りである。

- ✓ 方針に違和感なく、支持する ・・・ 2 社
- ✓ 方針は支持するが、仕様策定において、提案したい考慮点・観点がある ・・・ 2 社
- ✓ 方針の見直しを提案する ・・・ 0 社

考察

回答が得られた全 4 社から、方針についての支持は得られた。その際に、仕様策定において提案したい考慮点・観点として、以下のようなご意見を頂いた。

- ✓ 認証のあり方を検討する上で、認証は各情報銀行で行うものの、認証を高度化する機能については、いち早く関連省庁または推進団体のリーダーシップのもと「共通システム」の整備を進め、情報銀行がそれぞれに行う認証を“迅速かつ安価に高度化”できるようにしてほしい。
- ✓ 採用すべき認証方式については、今後の情報銀行がどのようなビジネスモデルとして発展していくのか、あるいは発展させていくべきなのか、によって現時点における実現性だけでなく、異なる観点での評価が必要になる可能性もあり、仕様の固定化が、新たなビジネスモデルの創造を妨げないように留意する必要がある。
- ✓ 現行の各情報銀行におけるユーザー認証の仕組みが標準化されていない状況下において、情報銀行間連携時における認証仕様のみの標準化を推し進めることには違和感があるため、フロントの情報銀行サービスの認証方式を踏まえた連携仕様を検討すべきではないか。

これらのご意見を踏まえ、各情報銀行が、新たに創造するビジネスモデルに適した柔軟な対応や、現行のユーザー認証の仕組み等の状況を踏まえた対応をしやすいように、本認証仕様において要となる必須部分は必要最低限に留め、推奨部分や、各情報銀行に裁量を委ねる任意部分などを明確にして、認証仕様を策定した。

観点 2. 検討する認証仕様において、参考にする規格・ガイドライン

本実証事業で、認証・認可、伝送等に関する通信仕様を検討する際、参考にする想定の規格・ガイドライン（下記 3 つ）が適切か等について各事業者からご意見を頂いた。

- ➢ FAPI（Financial-grade API） ・・・ 全銀協 API ガイドラインでも推奨されている標準仕様

- SP 800-63-3 ・・・ 電子的認証に関するガイドライン
- RFC 8485 - Vectors of Trust ・・・ 認証レベルなどの情報を簡潔に表現するための規格

回答結果

各社が選択した回答状況は以下の通りである。

- ✓ 適切と考える、若しくは問題ない ・・・ 4 社
- ✓ 問題ないと考えるが、他にも参考にすべき規格・ガイドラインを提案したい ・・・ 0 社
- ✓ 別に参考とすべき規格・ガイドラインがあり、見直しを提案したい ・・・ 1 社

考察

回答が得られた全 5 社中 4 社から、認証仕様の検討時に参考にする想定の規格・ガイドラインについて、適切、若しくは問題ない、との回答を得た。但し、注意喚起や見直しの提案として、以下のようなご意見も頂いた。

- ✓ 現段階で適切と言えるが、ベンチマークとなる内閣府の動向を確認しつつ平仄を合わせる必要がある。
- ✓ 現行当社の認証・認可・伝送手段は、FAPI に対応しておらず、取り扱うデータに対してオーバースペックであると考える。そのため、取り扱うデータ、連係データレベルに応じた方式の採用を望む。例えば、データレベルによっては、OpenID Connect Core 1.0 の準拠が望ましいと考える。また、基本的な共通属性のみの連携を想定した OpenID Connect Core 1.0 の Aggregated and Distributed Claims 方式で十分の可能性も視野に入れて頂きたい。

本仕様の検討においては、通信標準化に高い見識を持つ専門家から「国際的な通信標準化の流れを踏まえると、日本の情報銀行業界においても、FAPI ベースの仕様を策定すべきと考える」とのアドバイスを頂いていることや、5 社中 4 社から理解が得られたことを踏まえ、FAPI をベースとした。但し、取り扱う連携データレベルによっては、OpenID Connect Core 1.0 等の FAPI 以外の仕様を許容するかについても検討した。

観点 3. 通信方式に関するニーズ

本仕様を検討する上で、情報銀行サービス事業者が求める通信方式に関するニーズについて各事業者からご意見を頂いた。

回答結果

各社が選択した回答状況は以下の通りである。

- ✓ 取り扱うデータ(要配慮を含むなど)に応じて認証レベルを変える仕様があれば利用を検討したい ・・・ 5 社
- ✓ 消費者からの認証に、多要素認証(知識、所有物、生体などの組合せ認証)を提供したい ・・・ 5 社
- ✓ 他情報銀行と連携したサービスを提供する場合、消費者に認証が 1 回で済む仕組みを提供したい ・・・ 4 社
- ✓ 将来、FIDO2 による生体認証などを用いたパスワードレス認証に移行したい ・・・ 4 社
- ✓ 自社 ID 認証に加え、ソーシャルログイン(他情報銀行 ID を用いたログインなど)も提供したい ・・・ 3 社
- ✓ 情報銀行間でデータ連携する場合、OAuth によるデータ連携を標準としたい ・・・ 3 社
- ✓ サービス事業者からの認証に、多要素認証(知識、所有物、生体などの組合せ認証)を提供したい ・・・ 3 社

- ✓ 他社 ID などを用いた第三者認証をする場合でも、認可（消費者からの許諾）は自社で行いたい ・・・ 3 社
- ✓ 電話対応などでユーザー所有のスマホへ認証認可要求をプッシュ通知するユースケースに対応したい ・・・ 2 社
- ✓ 将来、共通の認証基盤が構築され、共通 ID 認証が実現されれば、自社 ID 認証は廃止したい ・・・ 2 社
- ✓ 将来、共通の認証基盤が構築され、共通 ID 認証が実現されても、自社 ID 認証を併存させたい ・・・ 2 社

考察

全 5 社で利用意向を確認できた「取り扱うデータに応じて認証レベルを変える仕様」や、5 社中 4 社と高いニーズがあった「連携サービス提供時における消費者認証が 1 回で済む仕組み」は、本仕様を策定する上での主要な目的でもあるため、検討の方向性が概ね適切であることを確認できた。また、同様に高いニーズが確認できた「消費者への多要素認証の提供」や「生体認証などを用いたパスワードレス認証への移行」から、シンプルに情報銀行として、より高いセキュリティの認証方式を消費者に提供したいという考えも伺えるため、将来に向けて、情報銀行業界における認証方法自体の高度化、標準化に向けた取り組みが重要になると考えられる。

3.6.3.2. 【第 1 回アンケート】データ定義の検討について頂いたご意見

観点 1．標準化データ項目を拡充する方向性

本実証事業における標準化データ項目は、消費者の基本情報データ項目（氏名、性別、生年月日など）が中心となるが、本検討による仕様策定後も継続して標準化データ項目を拡充していくことを想定し、実現したいユースケース、標準化すべきと考える事業分野や、データ種類（本人確認情報、行動ログなど）などといったデータの標準化が求められる対象について各事業者からご意見を頂いた。

回答結果

各社が選択した回答状況は以下の通りである。

- ✓ 情報銀行間でデータ連携して実現したいと考えるユースケースがある ・・・ 1 社
- ✓ ユースケースはないが、標準化すべきと考える分野やデータ種類がある ・・・ 3 社
- ✓ 現時点では、情報銀行間でデータ連携して実現したいと考えるユースケースはない ・・・ 1 社

考察

実現したいユースケースがあると回答した事業者からは以下のようなご意見を頂いた。

- ✓ 基本情報データ項目に加え、ヘルスケア分野等で取得する、健康に関するデータ（体組成計での測定記録、血圧や体温等日々の記録等）は、データ項目を統一し、情報銀行間連携がスムーズに行われるよう、事前に項目が統一されていた方が良い。

また、標準化すべきと考える分野やデータ種類があると回答した事業者からは以下のようなご意見を頂いた。

- ✓ 現状、情報銀行を運営している事業者が取得している情報はアンケートデータがメインになっているケースが多く、消費者目線からすると各情報銀行を利用する際に同じようなアンケートに回答することになってしまっている。
  そのため、基本情報データ項目も基本的にはアンケートベースで取得していると考えられ、アンケートデータの

フォーマットを標準化することで、広範囲の情報を対象とすることもでき、情報銀行を利用する際の消費者の利便性を向上させ、情報銀行の利用を活性化させることにもつながると考える。

- ✓ 情報銀行は「情報インフラ」であることから、「個人に関わる基本的な情報」については標準化すべき領域と考える。具体的には、国勢調査にあるような「家族・住まい」「仕事・資格、スキル」に関する情報や、「からだ・健康」「QR を含む金融決済手段、口座情報」「公的証明書番号」に関する情報も標準化すべきではないかと考える。これら情報が流通できる状況を整備することで、育児・介護支援やセカンドキャリア支援を目的としたスキルマッチングなどの人生 100 年時代を健康に生き抜くために必要な健康サービスの多様化や、情報漏洩を防止しつつ入力の手間や負担を減らすことや、公的個人認証サービスの電子証明書に紐づいたユーザー識別子と連携することで行政手続きの簡略化・迅速化などが実現できるようになるのではないかと考える。
- ✓ 標準化すべきデータ種類としては、情報銀行における本人確認方法についてのガイドライン等がない本人確認情報や、データの持ち方が多岐にわたる位置情報などが挙げられる。また、標準化すべき分野としては、取扱いが難しくなかなか参入しにくいヘルスケア分野について、活用ルールも含め、標準化することで活用シーンを拡大する事が可能になるのではないかと考える。

これらのご意見を踏まえると、本人確認情報なども含む個人に関する基本的な情報の拡充、形式などが統一されていないことで活用が難しくなっているアンケートデータや位置情報の標準化、事業分野としてニーズが高かったヘルスケア分野における活用ルールも含めた標準化が求められていることが分かった。各事業分野で定められた標準が既に存在、もしくは検討されている場合は、整合を保ちつつ標準化に取り組む必要もあるが、情報銀行業界として、これらデータ種類や事業分野について、今後も継続してデータ項目の標準化に取り組み、拡充していくことが必要と考える。

観点 2. 検討するデータ定義において、準拠、または参考にする規格・ガイドライン

本実証事業で情報銀行間連携におけるデータ定義を検討する際、参考にする想定の規格・ガイドライン（下記 3 つ）が適切か等について各事業者からご意見を頂いた。

- ➢ IMI 共通語彙基盤 ・・・ データに用いる文字、用語を共通化し、情報の共有や活用を円滑に行うための基盤
- ➢ データカタログ作成ガイドライン ・・・ データカタログの項目定義の考え方、項目策定の手順等に関する文書
- ➢ Consent Receipt Specification ・・・ GDPR 等の各種レギュレーションに準拠している同意管理仕様

回答結果

各社が選択した回答状況は以下の通りである。

- ✓ 適切と考える、若しくは問題ない ・・・ 4 社
- ✓ 問題ないと考えるが、他にも参考にすべき規格・ガイドラインを提案したい ・・・ 1 社
- ✓ 別に参考とすべき規格・ガイドラインがあり、見直しを提案したい ・・・ 0 社

考察

全 5 社から、情報銀行間連携におけるデータ定義の検討時に参考にする想定の規格・ガイドラインについて、適切、若しくは問題ない、との回答が得られた。但し、注意喚起として、以下のようなご意見も頂いた。

- ✓ 基本的に問題ないが、欧州のデジタル広告業界団体である IAB Europe が出している Transparency & Consent Framework 2.0 といった規格や、産業データ流通推進協議会で検討された内容など、主要な業界団体などで策定された規格との整合性確保や、検討内容の重複がないように意識して取り組むべきと考える。

これら回答結果、ご意見を踏まえると、情報銀行間連携におけるデータ定義の検討時に参考にする想定の規格・ガイドラインに関する方針について、概ね適切であることを確認できたが、主要な業界団体などで策定された規格、検討内容についても意識しつつ、情報銀行間連携におけるデータ定義を検討した。

3.6.3.3. 【第 2 回アンケート】消費者目線でユーザーインターフェースに関する改善点・要望

観点 1. 他情報銀行 ID を用いた認証が可能なソーシャルログイン方式に関する改善点・要望

本実証事業では、消費者の利便性向上を意図し、新たに利用開始したい情報銀行に対して、既に利用している他情報銀行 ID を用いた認証を可能にしたり、既に利用している複数の情報銀行 ID を消費者本人が認証時に使用したい情報銀行 ID に紐づけることで、複数の情報銀行に対して同一 ID での認証を可能にしたりすることができるソーシャルログイン方式に関して、消費者目線で、便利さ・使い易さ・理解し易さなどの観点から、良いと感じた点、及び改善が必要と感じた点について各事業者からご意見を頂いた。

回答結果

各社からコメント頂いた回答内容は以下の通りである。

［良い点］

- ✓ 認証済みの連携元情報銀行から連携先情報銀行へ、認証情報が引き継がれることで、認証の手間（ID/パスワードの入力、画面遷移等）が省かれる点は、消費者にとって便利で使い易いと思う。
- ✓ 世界的規模でサービスを展開している大規模プラットフォーマー等でも提供しているソーシャルログインは、馴染みのある認証仕様のため分かり易く、特に引っ掛かるポイントもなく、スムーズに操作を進めることが出来た。
- ✓ 「第三者提供に関する同意」の画面で、提供されるデータ項目を明示していることは良いと感じた。
- ✓ 連携に際しての情報が、ユーザーインターフェースに明示され、文字として説明されている点が良いと感じた。
- ✓ 今後、様々な情報銀行間連携が実現される場合、基準としてユーザーインターフェースが揃っていると、消費者が混乱し難いなど、安心感がある。

［改善が必要と感じた点］

- ✓ 新規登録のケースにおいても、ログイン（サインイン）する認証画面から始まる遷移になっているため、消費者にとって動線が分かり難いと感じた。別途、新規登録（サインアップ）する画面を用意した上で、表示順は、①新規利用する情報銀行の新規登録画面、②新規利用する情報銀行の利用規約表示、③既に利用している情報銀行のアカウントで登録するための認証画面、④既に利用している情報銀行の第三者提供に関する同意表示、⑤新規利用する情報銀行の登録完了通知画面にするのが望ましいと考える。
- ✓ 新規登録のケースにおいて、新規利用する情報銀行の利用規約よりも先に、既に利用している情報銀行のアカウントで登録するために、既に利用している情報銀行の第三者提供に関する同意を表示する遷移になっている。第三者提供に関する同意をした後に、利用規約に同意しないこともできるが、その場合、既に同意してしまった第三者提供に関する同意はどうなるのかなど、消費者に不安を与えてしまう可能性もあるため、順番を①新

規利用する情報銀行の利用規約、②第三者提供に関する同意とするか、同時に表示すべきではないかと思う。認証仕様ガイドラインなどに、ID 連携時における利用規約や第三者提供に関する同意をどのタイミングで取得するかについて参考として記載すべきと考える。

- ✓ 新規利用する情報銀行に、既に利用している情報銀行から ID 情報を連携することが、既に利用している情報銀行の第三者提供にあたるか、疑問に感じた。消費者本人が新規利用する情報銀行に対して、既に利用している情報銀行へのアクセスを認可済みであれば、既に利用している情報銀行の意志で（消費者同意のもと）第三者提供することとは異なると思う。そのため、ID 情報の連携に必要なのは、第三者提供に関する同意ではなく、認可の再確認になるのではないかと思う。
- ✓ ID プロバイダーとしての利用規約と、情報銀行サービスとしての利用規約を明確に分けた方が良いと思う。
- ✓ 現在どの情報銀行 ID でログインしている状態なのかを画面上に表示した方が、消費者にとって、認証済みで認証が省略された場合に安心感があると思う。また、認証済みの場合は、認証が省略されることについて予め消費者に分かるようにしておくべきだと思う。
- ✓ 認証レベルによって認証方法が変わる仕様のため、現在認証済みの認証レベルを統一アイコンなどで分かり易く画面に表示した方が良いと思う。また、どの認証レベルの場合に、どのような認証方法になるかについて予め消費者に分かるようにしておくべきだと思う。
- ✓ 基本的に「連携し慣れている人」ではなく、「連携し慣れていない人」を基準にする必要があるため、連携先情報銀行と連携元情報銀行で共通化された連携ステップを表示した上で、現在どのステップにいるかを、情報銀行ごとのアイコンを表示したり、ハイライトしたりするなど、言語的な表現ではなく視覚的な表現で把握できるようにしておくべきと思う。また、連携先情報銀行と連携元情報銀行を跨る画面遷移を繰り返すことで、現在どのステップにいるかを見失い易くなるため、全画面遷移するのではなく、画面中の小窓で連携元のログイン画面を表示する等、分かり易い画面遷移方法についても検討すると、より良くなると思う。
- ✓ ログインの際に、ID/パスワードだけでなく、端末の生体認証などで本人確認を徹底した方が消費者に安心して使って頂けるのではないかと思う。

考察

良い点として、消費者に対する利便性や分かり易さ、基準があることによる安心感など、期待通りのご意見を頂いた。

一方で、改善が必要と感じた点として、新規登録時における分かり易さ、各種同意の趣旨を踏まえた取得順序、認証レベルや情報銀行間連携ステップなどの消費者にとって馴染みのない部分を分かり易く伝える表現についてご意見を頂いた。改善が必要と感じた点として頂いたご意見は、どれもユーザーインターフェースの改善に繋がる内容であったため、基本的に「ユーザーインターフェース仕様書」に反映し、具体的な仕様に落とし込むには更なる検討が必要な一部内容についても、今後の課題として、本書に記載した。

観点 2．取り扱うデータの秘匿性に応じて認証レベルを切り替えるデータ連携方式に関する改善点・要望

本実証事業では、消費者の利便性向上とセキュリティの両立を目指し、情報銀行間でデータ連携する目的で消費者に対して第三者提供の同意を求める際に、データの利用目的と連携する具体的なデータ項目を明示した上で、取り扱うデータの秘匿性に応じた認証レベルで認証する方式を採用した。

また、データ連携に関係する仕様として、消費者がデータ連携の停止を希望した際に、速やかに停止できるように、消費者に対して提供中の全サービスを、利用目的毎に連携している具体的なデータ項目を明示した上で、個別にデータ連携の停止を依頼できるユーザーインターフェースを提供することも盛り込んだ。

これら方式、仕様に関して、消費者目線で、便利さ・使い易さ・理解し易さなどの観点から、良いと感じた点、及び改善が必要と感じた点について各事業者からご意見を頂いた。

回答結果

各社からコメント頂いた回答内容は以下の通りである。

［良い点］

- ✓ 情報銀行が提供するサービスに対して、利用目的毎に連携するデータ項目が明示された上で、利用目的単位にデータ連携の可否を選択できるため、消費者が利用したいサービスを使うために必要なデータ項目だけの連携で済み、情報銀行間で過剰に連携する必要がなくなる点が良いと感じた。
- ✓ 連携するデータ項目を、「ユーザー属性」や「健康情報」等のカテゴリに分けて消費者に明示するのは良いと感じた。
- ✓ 消費者に提供中のデータ連携を伴うサービスについて、すべての利用目的とそれに関連するデータ項目が明示された上で、すべての利用目的を一括選択したり、特定の利用目的を個別選択したりして、消費者がデータ連携停止をスムーズに指示できる画面を提供するのは良いと感じた。

［改善が必要と感じた点］

- ✓ 消費者が希望する利用目的を単一選択した上で、その利用目的で取り扱う連携データの秘匿性に応じた認証レベルで認証する方式になっているが、将来的に多くの利用目的でデータ連携される状態を想定すると、利用目的の単一選択を繰り返し、より高い認証レベルでの認証が必要になれば追加で認証も行うというのは、ユーザビリティとして良くない。そのため、一度に複数の利用目的を選択できるようにし、選択された利用目的の中で最も高い認証レベルの認証を 1 回すれば済む方式にした方が良いと思う。
- ✓ 「第三者提供に関する同意」画面において、提供されるデータ項目を明示しているが、そのデータ自体が何なのかも明示して欲しいと感じた。例えば、「氏名」と項目だけを表示するのではなく、「氏名 － 田中一郎 － 本人確認に利用」等、項目毎に具体的に提供されるデータと、提供先での利用目的を表示した方が良いと思う。
- ✓ 消費者が混乱しないように、どちらの情報銀行から、どちらの情報銀行へデータを連携するのかを視覚的に把握できるようにすると良いと感じた。例えば、データ連携元とデータ連携先の情報銀行名称を表示し、その名称の間にデータが流れる方向を矢印で示すなど方法が考えられる。
- ✓ 「データ連携」を行うと、結果としてどうなるのかが分からなかったため、説明した方が良いと感じた。例えば、「連携先にデータ自体を渡して、連携先にデータが保持される」のか、それとも「連携先はデータを参照するだけで、連携先ではデータを保持しない」のかや、「第三者提供に関する同意をした後は、データが更新される度に随時データ連携される」のか、それとも「第三者提供に関する同意をした時点のデータが一度だけ連携される」のかといったことが予め消費者に分かるように説明しておくと良いと思う。
- ✓ 「データ連携停止」を行うと、結果としてどうなるのかが分からなかったため、説明した方が良いと感じた。例えば、「連携停止するだけで、連携先に連携済みのデータは残り、連携先のサービスは利用できる状態が維持される」

のか、それとも「連携停止に伴い、連携先に連携済みだったデータも削除され、連携先のサービスは利用できなくなるのか」といったことが予め消費者に分かるように説明しておくと良いと思う。

- ✓ ユーザーインターフェース上、「サービス利用停止」と「データ連携停止」が同じようなフローになっており、分かり難く感じた。言葉の定義やユーザーインターフェースで分かり易い表現にすると良いと思う。また、「データ連携停止」ができるのであれば、「いつでもこちらからデータ連携を停止できます」等のリンクがあると、より分かり易いと思う。

考察

良い点として、利用目的毎に連携するデータ項目をカテゴライズして表示することで分かり易くしている点、同意を利用目的毎に選択できるようにすることで結果的に必要なデータのみを連携する制御ができるようにしている点、消費者がデータ連携停止をスムーズに指示できる画面を提供するようにしている点が挙がった。これら消費者のコントローラビリティを確保する目的で仕様化した点について、多くの賛同、支持が得られたと思う。

一方で、改善が必要と感じた点として、多様なデータ連携サービスが実現される未来を見据えた選択方法や、消費者に誤解を与えないようにデータ連携内容（データ連携方向、具体的なデータ値、動作結果など）をどのように伝えるべきかなどについて、予め説明しておく事項も含めご意見を頂いた。これら改善点を参考に認証仕様をブラッシュアップした。

3.6.3.4. 【第 2 回アンケート】事業者目線で情報銀行間連携時におけるドラフト版の共通仕様に対する改善点・要望

観点 1. ドラフト版の認証仕様に対する改善点・要望

本実証事業では、情報銀行サービスを提供する立場から、事業者目線で情報銀行間連携時におけるドラフト版の共通仕様となる「認証仕様」に対して改善を望む点や、今後の普及促進、活動など関する要望・期待について各事業者からご意見を頂いた。

回答結果

各社からコメント頂いた回答内容は以下の通りである。

- ✓ 情報銀行間連携で取り扱うデータの秘匿レベルが低い場合などは、FAPI に対応していなくても、OIDC での ID 連携や、OAuth でのデータ連携を認める仕様にした方が、実態に即しているのではないかと思う。
  また、ID 連携における OIDC と FAPI との違いや、データ連携における OAuth と FAPI との違いについて仕様書等に明記しておくのが良いと思う。
- ✓ 情報銀行間連携で取り扱うデータの秘匿レベルと、連携元と連携先の情報銀行が対応している認証レベルにより連携の可否を判断する仕様になっているが、連携有無とは無関係に認証レベルの低い情報銀行が秘匿レベルの高いデータを取り扱うことは消費者にとってリスクがあるため、各情報銀行に対して、秘匿レベルに応じた認証レベルを要求し、その要求を満たす事業者同士以外の連携は不可とするなど対応が必要ではないかと思う。
- ✓ ユーザー認証画面や許諾画面等において、消費者にとって意図しない動作を防ぐために、「戻る」「進む」「Negative」「Positive」等のボタン配置に関しても、ユーザーインターフェース仕様書にオプトイン方式を前提とした推奨仕様を記載した方が良いと思う。

- ✓ スコープは、消費者からの同意を利用目的毎に個別に取得すべきことや、利便性を踏まえて同意の取り消しを一括で行うこともできるようにしておいた方が良いことを考えると、利用目的（サービスではない）と、データ項目グループの組み合わせで設定することを推奨する仕様が良いと思う。
- ✓ 認証仕様として、要求レベルが「必須」となっているものは、情報銀行間で接続する場合に強く求められる要求になると思うが、今後、情報銀行以外のサービスと接続する場合の対応などの整理も必要になると思う。

考察

情報銀行サービスを提供している事業者の実態に即した仕様にするには、今後採用事例が増加すると考えられる高セキュリティの FAPI を見据えつつも、取り扱うデータの秘匿レベル次第では既に現時点で広く普及している素の OIDC や OAuth も認めるべきではないか、といったご意見や、取り扱うデータの秘匿レベルに応じた認証レベルを各情報銀行に対して要求すべきではないか、といったご意見があり、各情報銀行に求める要求レベルについては、慎重にバランスを取る必要があることが分かった。本実証事業で策定した仕様としては、FAPI をベースとし、取り扱うデータの秘匿レベルに応じた認証レベルで認証することを推奨とするが、取り扱うデータの秘匿性を考慮（すべて秘匿レベル 1 など）した上で、連携し合う情報銀行間で合意すれば、情報銀行間連携の運用を OIDC による ID 連携と OAuth によるデータ連携で開始することを認める仕様とした。

また、オプトイン方式を前提としたボタン配置や、消費者の利便性とシステム制御を踏まえた最適なスコープ設計に関するご意見を頂いた。これらは、認証仕様をより実用的なものにするために有意義な提案であったため、そのまま仕様に反映した。

観点 2. ドラフト版のデータ定義に対する改善点・要望

本実証事業では、情報銀行サービスを提供する立場から、事業者目線で情報銀行間連携時におけるドラフト版の共通仕様となる「データ定義」に対して改善を望む点や、今後の普及促進、活動など関する要望・期待について各事業者からご意見を頂いた。

回答結果

各社からコメント頂いた回答内容は以下の通りである。

- ✓ 消費者本人の意志でデータ連携を指示する場合（データポータビリティ観点）と、消費者の同意に基づき情報銀行がデータ連携する場合（第三者提供観点）との違いを明確にし、主体等について整理することを希望する。例えば、認証レベルの低い情報銀行から、認証レベルの高い情報銀行へデータ連携するケースにおいて、消費者の意志によりセキュリティの高い情報銀行へデータ移行することと、セキュリティの問題ではなく偶々高い認証レベルを採用している別情報銀行のサービスも利用できるように、消費者の同意に基づき情報銀行がデータ連携することではまったく異なると思う。
- ✓ 消費者の第三者提供に関する同意情報は、各情報銀行がそれぞれのサービスで利用・管理することを想定しており、情報銀行間連携の範囲外の認識でいた。そのため、個別同意情報や包括同意情報もパーソナルデータとして情報銀行間連携するのであれば、その意義や扱いなどを整理する必要があると思う。また、同意管理をデータ項目毎に利用目的や提供先事業者との組み合わせで行うなども必要になると思う。

- ✓ 情報銀行間連携で必要になる同意情報について、連携し合う情報銀行の両方で両行分を保有するか、共通のストレージに互いに保存するか、各情報銀行で自行分のみを保有して API を介して互いに参照し合うか、といった共有方法を検討する必要がある。また、その共有方法は、同意や同意撤回などの状況をスムーズに参照でき、連携し合う情報銀行以外を排除するアクセス管理もし易い方法が適していると考える。
- ✓ 氏名、メールアドレス、電話番号などの基本個人情報は更新される可能性があるデータのため、データ連携等により分散管理された場合に論理的な不整合が発生し、同一人か否かの判別ができなくなる等のリスクがある。そのため、今後に備えて基本個人情報の中に不変の識別子 ID などを任意入力できる項目を設けておくことが望ましいと考える。
- ✓ 氏名や住所などについて分割項目と単一項目が設定されているため、連携インターフェースは目的の項目のみを抽出できる形式（XML や JSON など）が適していると思う。なお、住所の分割項目として「市区郡町村名」の項目に、町域・字名までを含む仕様であれば、その旨を仕様に明記した方が良いと思う。

考察

消費者本人の意志でデータ連携を指示する場合（データポータビリティ観点）と、消費者の同意に基づき情報銀行がデータ連携する場合（第三者提供観点）との違いや、個別同意情報や包括同意情報をパーソナルデータとして扱うことについては、ご理解頂けるように整理した上で、本書に説明等を記載した。

また、同意情報に関する共有方法、今後に備えた任意項目追加、採用するインターフェース形式等については、仕様にどのように反映すべきかを検討した上で、具体的な対応を決定した。

3.6.3.5. 【アンケート共通】情報銀行やデータ流通に関する普及、促進について頂いたご意見

観点 1．情報銀行やデータ流通に関する普及、促進

本実証事業を通じて、情報銀行やデータ流通の普及、促進に必要な活動、取り組みなどについて各事業者からご意見を頂いた。

回答結果

各社からコメント頂いた回答内容は以下の通りである。

- ✓ 消費者が特定の情報銀行にロックインされないようにする意味でも、情報銀行間連携におけるデータ仕様を策定することに対して賛同する。また、情報銀行間連携を確実なものにし、個人中心のデータ流通を実現するためには、認定された情報銀行の必須機能として提供されるべきと考える。本実証事業の連携仕様策定において、必須・推奨の範囲についても検討されることを期待する。
- ✓ 本実証事業でデータ定義した基本個人情報は、比較的共通化しやすい分野であったと考える。高いデータ共通化のメリットを享受できるのは、具体的な特定業種分野、位置情報やインターネット上での行動履歴など、データの持ち方が既に多岐にわたっている上に、ユースケース毎に個別最適化されている分野ではないかと考える。そのため、今後、これら分野における利用方法やデータ仕様の共通化が進むことで、参入障壁が下がり、市場が活性化することを期待する。

- ✓ 情報銀行間連携によりカタログ化されるデータの持ち方について、基本的なアーキテクチャを整理する必要があると考える。世界的規模でサービスを展開している大規模プラットフォーマーは、データを一元管理しているからこそ、データ活用の機動性が生まれ、強みとなっている。極論、情報銀行も、ネットワーク化することで、“仮想的な大規模プラットフォーマー”となれるかが普及の成否を握っていると言える。どこまでを「共通データ」として、どのように「安全に保存」されていて、同意に基づいてリクエストがあった場合、いかに「流通して、利用」できる状態にするか。初期のシステムデザインとして非常に重要な観点と考える。また、「データの改ざん防止」の観点では、「共通データ」の部分は協調領域として情報銀行間でコンソーシアムを形成し、データベースを繋ぐことで“疑似的なブロックチェーン”を構築し、相互にデータの補完とバックアップを行い、個人同意の基でアクセスできるような生態系が有効と考える。この形態は、万一どこかの情報銀行がサーバーダウンなど、危機的な状況に陥ったとしても、相互補完できるという「耐障害性」の観点でも有効ではないかと考えている。当然ながら、「セキュリティ」と「利便性」はトレードオフの関係にあり、分散化すると、技術的なハードルは高まるものの、ここの設計が情報銀行の成否を握ると考える。
- ✓ 情報銀行が社会・ユーザー・事業法人など多くのステークホルダーに認められ、ビジネスとして発展していくためには、情報銀行間でのデータ連携に加え、種々の課題に対応していく必要あると考える。とりわけ、情報銀行間におけるデータ連携では、インシデント発生時の責任分界の標準化や、前提となるデータ連携に伴う収益・コスト分配の考え方に関して、事業者による十分な論点の洗い出しと議論が有効かつ必要と考える。
- ✓ 内閣府から発表されている認証仕様に関する動向や、デジタル庁設立に伴い、様々な分野のデータ定義が策定される可能性に注意を払いつつ、それらと平仄を合わせて今後も継続して改善や検討する必要があると思う。
- ✓ 今後、様々な分野の情報銀行事業者が現れ、新たなビジネスモデルやユースケースを実現できる環境を作るために、提供先に対する要件緩和や情報銀行自体の認知度向上など、情報銀行事業者が増えるような取り組みを望む。

考察

これらのご意見を踏まえると、情報銀行が広く一般的に認知され、データ流通を普及、促進するには、「個人中心のデータ流通を支える情報銀行間連携の実現」や「大規模プラットフォーマーに負けないサービスを消費者へ提供するために、情報銀行間連携による“仮想的な大規模プラットフォーマー”の実現」といった消費者に対するサービス品質の向上に役立つ情報インフラに成長していくことが必要となり、そのためには、実際に情報銀行サービスを提供する事業者が集まり、「情報銀行間連携を実現するために必要な責任分界や収益・コスト分配といった事業者間における取り決め」について十分に議論した上で、決めていくことが重要と考える。

また、今後の更なる普及、促進には、内閣府やデジタル庁等といった政府系の取り組みと足並みを揃えることはもちろん、情報銀行事業者が様々な分野で新たなビジネスモデルやユースケースを実現できる環境作りが必要不可欠となる。

3.7. 情報銀行間連携の普及・促進に向けた今後の取り組み

情報銀行間連携の普及・促進のため、情報銀行認定を行う日本 IT 団体連盟への働きかけや、情報銀行のビジネスセミナー等の情報銀行に関係する業界の協調の場を通じて、情報銀行間連携を模索する事業者とのコネクションを形成しながら、実現に向けた取り組みを重ねることで、本実証事業の成果となる共通仕様を積極的に展開し、データ流通社会の実現に貢献することを目指す。

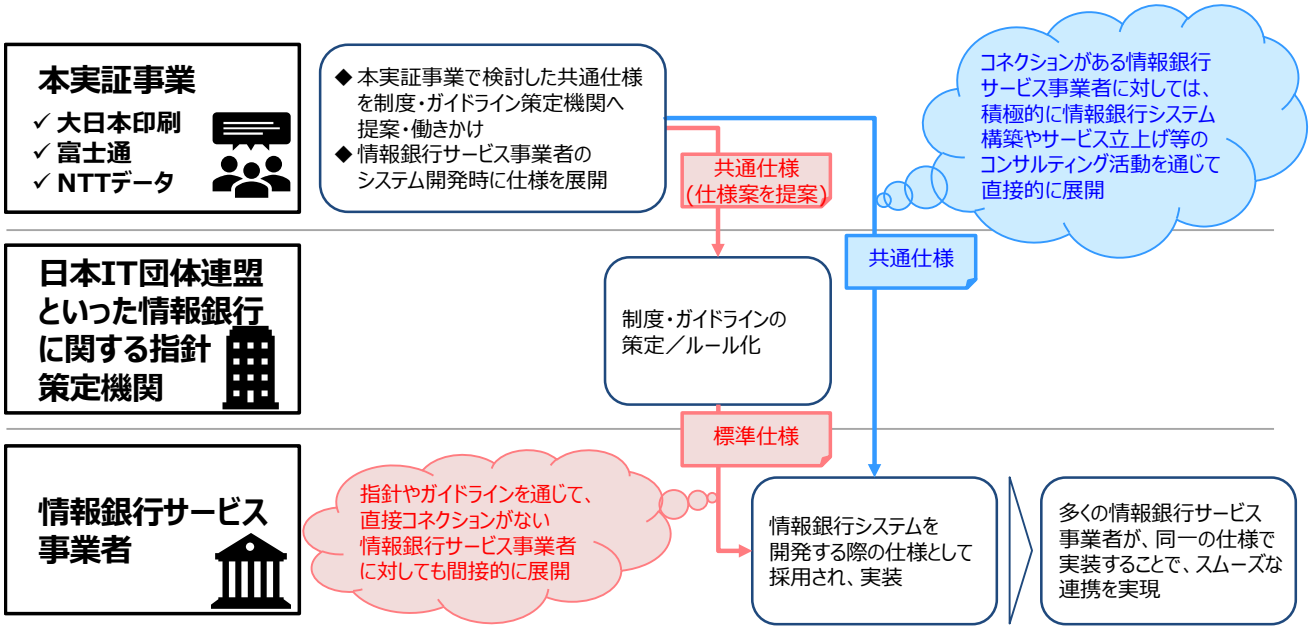


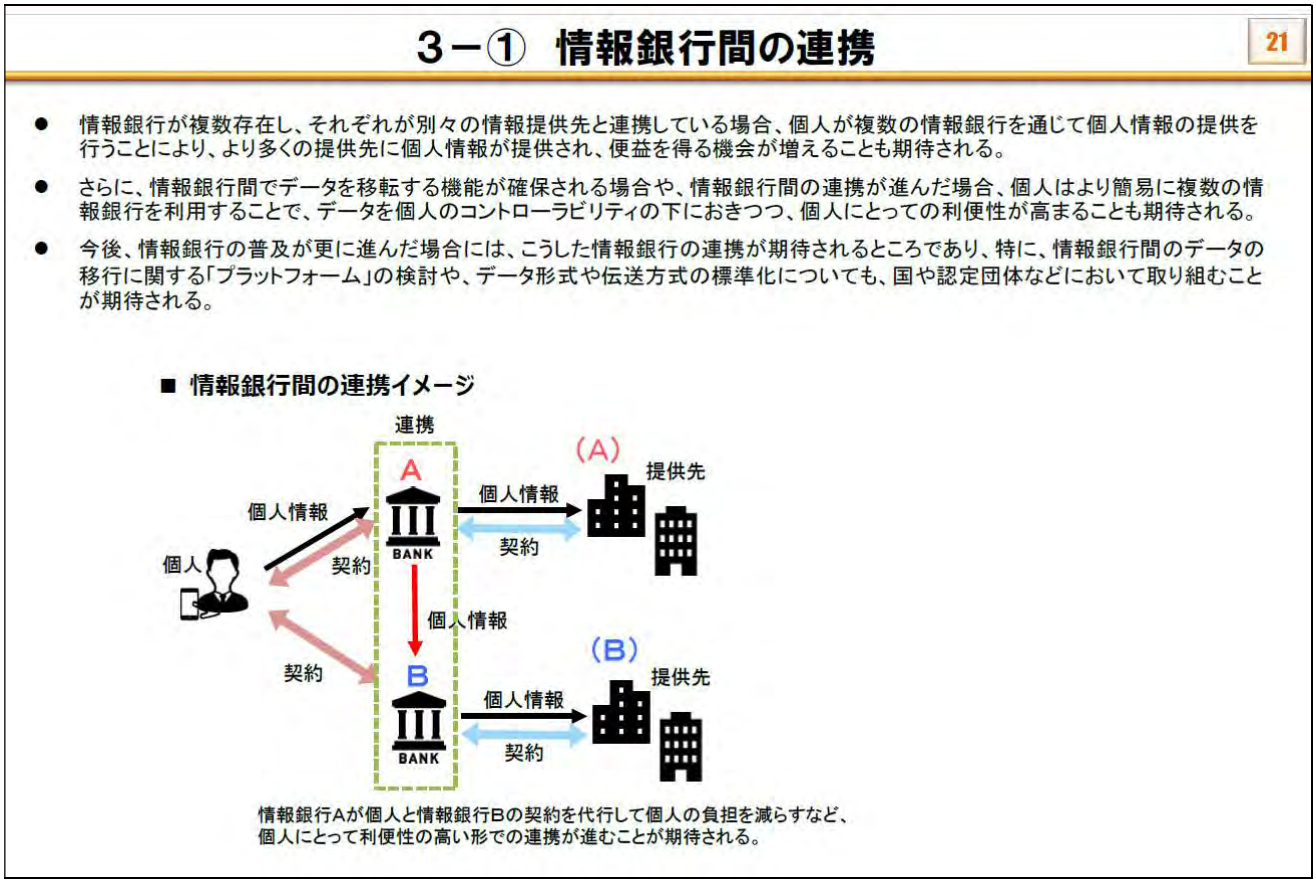
図 3-49 普及・促進に向けた今後の取り組み

【補足】第三者提供先からの再提供の禁止事項に関して

個人情報に対する個人のコントローラビリティの確保と、情報銀行の監督による提供先での適切な取扱いの確保という考え方から、情報銀行には提供先第三者を監督する義務がある。
認定基準における再提供禁止の条項は、再提供先は情報銀行の監督下から逸脱してしまい情報銀行に求められる義務を果たせないので、これ禁止すべきであるという考え方に基づいて規定されているものと理解している。

今回の情報銀行間連携に関しては、連携する情報銀行はいずれも認定を取得した情報銀行の想定である。
情報銀行Ａから見た時に連携先の情報銀行Ｂは、提供先にあたり、情報銀行Ｂの提供先（情報銀行Ａから見た時の再提供先）には、情報銀行Ａの監督が及ばないが、情報銀行Ｂの監督下にあり、個人によるコントローラビリティと、提供先での適切な取り扱いの確保は、いずれも問題ない。

これに加えてこれまでの議論も踏まえ、認定を受けた情報銀行を提供先とした場合、この情報銀行からの更なる提供は再提供の禁止に該当しない旨を指針に記載するなど明確化することが望まれる。



引用：令和元年 10 月 8 日付け 情報信託機能の認定スキームの在り方に関する検討会とりまとめ資料より

3.8. 謝辞

本実証事業では、データを新たな資源として捉え、消費者が便益を実感できるデータ利活用の実現を目指す Society 5.0 時代に相応しいデジタル化に貢献するため、データ流通網の構築に不可欠な「情報銀行」の社会実装を促進することを目的に、情報銀行間連携仕様を策定した。

本実証事業の実施に当たり、認証仕様の検討において、国際標準化の取り組みに精通している有識者として、富士通の長谷川一知氏及び同社の榊原宏紀氏に有益な助言を頂いた。また、認証認可技術に造詣が深い専門家として、富士通研究所の新崎卓氏及び同研究所の野田敏達氏に専門的な助言を頂いた。ここに感謝の意を表する。

また、データ定義、必要な機能・ルールの検討において、情報銀行、データ流通、個人情報保護に関する制度等に関する有識者として、NTT データの花谷昌弘氏及び同社の山田英二氏に実用的な助言を頂いた。ここに感謝の意を表する。

情報銀行間連携仕様の検討にご協力頂いた有識者、専門家のプロフィール紹介

国際標準化の取り組みに精通している有識者
氏名:**長谷川 一知**（はせがわ かずとも） 所属:富士通株式会社 法務・知財・内部統制推進本部 知的財産戦略統括部 役職:シニアマネージャー 【主な著作物等】 ・エディタとして、ネットワーク技術等の国際標準 ITU-T G.986、ITU-T Y.4409 などを出版 【主な活動、実績等】 ・ITU-T SG13, SG15, SG20 等にて国際標準化活動に 20 年従事 ・現在は富士通のスタンダード推進・活動支援として DSA(データ社会推進協議会)等で活動
氏名:**榊原 宏紀**（さかきはら ひろのり） 所属:富士通株式会社 法務・知財・内部統制推進本部 知的財産戦略統括部 【主な著作物等】 ・プロジェクトリーダとして、無線給電技術の国際標準 IEC 62827-1、IEC 62827-3 などを出版 【主な活動、実績等】 ・IEC/TC100 傘下の Technical Area の国際幹事、国際議長に 10 年従事 ・現在は ISO/TC159/SC1/WG5 人間工学 Expert

認証認可技術に造詣が深い専門家
名前:**新崎　卓**（しんざき　たかし） 所属:株式会社富士通研究所　デジタル革新コア・ユニット 役職:プリンシパルエキスパート 【主な著作物等】 ・解説論文、生体認証と改正個人情報保護法をめぐる動き、IEICE Fundamental Review Vol.11 No.2 PP108-112、2017 年 7 月 ・バイオメトリックセキュリティ・ハンドブック、オーム社、2006 年 11 月出版、編集幹事及び執筆者 ・IEEE Biometric Council Newsletter Vol.33, 2020, 個人 Interview の掲載 ・Encyclopedia of Biometrics、Springer; 2nd ed. 2015 版、静脈認証関連の執筆者 ・“Mobile Iris Recognition” (Chapter 19), Iris and Periocular Biometric Recognition IET Book, PP435-438, 2017, Akira Yonenaga and Takashi Shinzaki ・“Use Case of Palm Vein Authentication” (Chapter 5), Handbook of Vascular Biometrics, PP145-158, Springer, 2019/5, Takashi Shinzaki 【主な活動、実績等】 ・生体認証も含めて認証認可技術とそのシステムに関する研究開発に 30 年以上従事 ・現在は認証ソリューション戦略を担当 ・SC 37 専門委員会（バイオメトリクス）: 国内委員長 ・SC 27/WG 5 小委員会（アイデンティティ管理とプライバシー技術）: エキスパート ・SC 17/WG 3 小委員会（機械可読渡航文書）:委員 ・FIDO Alliance: WG メンバー（FIDO Security & Privacy Requirements Working Group 等） ・ISO/TC68（金融サービス）:委員 ・SC 37 to TC68 国内リエゾン ・ISO/IEC JTC1/SC37 to ISO/TC68/SC8:国際リエゾン ・情報ネットワーク法学会:会員 ・IEEE BIOSIG プログラム:委員
名前:**野田　敏達**（のだ　びんたつ） 所属:株式会社富士通研究所　セキュリティ研究所　サイバーセキュリティ P J 【主な著作物等】 ・富士通社内のセキュリティガイドラインの執筆者 ・日銀金融研究所の論文「OAuth 2.0 に対する脅威と対策:金融オープン API の一段の有効活用に向けて」（著者:中村啓佑 https://www.imes.boj.or.jp/research/papers/japanese/kk37-3-4.pdf）の作成に貢献

情報銀行、データ流通、個人情報保護に関する制度等に関する有識者
氏名:**花谷　昌弘**（はなたに　まさひろ） 所属:株式会社エヌ・ティ・ティ・データ　金融事業推進部　デジタル戦略推進部 役職:部長 【主な著作物等】 ・「情報銀行のすべて」（ダイヤモンド社） 【主な活動、実績等】 ・総務省　情報信託機能の認定スキームの在り方に関する検討会　認定・運用 WG　委員（2020 年度） ・内閣府　総合科学技術・イノベーション会議　データ連携基盤サブ WG　委員（2017 年度） ・MyData Global　個人会員（2018 年～）
氏名:**山田　英二**（やまだ　えいじ） 所属:株式会社エヌ・ティ・ティ・データ　公共・社会基盤事業推進部　社会デザイン推進室 役職:ソーシャル・プロデューサー 【主な著作物等】 ・「ｅデモクラシーという地域戦略」小学館スクウェア（2002）（共著） ・「金融機関のためのマイナンバーへの義務的対応＆利活用ガイド」きんざい（2015）（共著） ・「新社会基盤　マイナンバーの全貌」日経 BP 社（2015）（共著） 【主な活動、実績等】 ・入社以来、エヌ・ティ・ティ・データの社内シンクタンク部門にて、電子政府やビッグデータによるマーケティング等に関する研究に従事 ・現在、デジタル・ガバメントの将来ビジョンや政策提言に従事 ・同志社大学大学院、九州大学、法政大学等で非常勤講師に就任

3.9. 第 3 章別添資料一覧

別紙 1【認証仕様編】概要説明書
別紙 2【認証仕様編】認証仕様ガイドライン
別紙 3【認証仕様編】ユーザーインターフェース仕様書
別紙 4【認証仕様編】API 仕様書
別紙 5【データ定義編】概要説明書
別紙 6【データ定義編】データ流れ図
別紙 7【データ定義編】概念 ER 図
別紙 8【データ定義編】エンティティ定義書
別紙 9【データ定義編】メタデータ定義書
別紙 10【データ定義編】コード定義書
別紙 11【データ定義編】フォーマット定義書
別紙 12【データ定義編】外部インターフェース定義書

第5章　全体まとめ

本報告書の冒頭で述べた背景を踏まえ、本事業では大きく 3 つのテーマにおいて調査を行った。

まず、「特殊性の高い情報の利活用に係る実証事業」において取扱う対象とした要配慮個人情報は、定期健康診断結果情報とし、情報銀行において他の個人情報（今回は当該消費者の趣味趣向情報）と組み合わせることによって、一定程度の有用性を確認できる結果となった。これは、例えばアレルギーやお薬手帳といった他の要配慮個人情報のみならず、購買履歴情報や IoT 機器等で生成される様々なパーソナルデータを、情報銀行を通じて利活用することにより、消費者課題や事業者課題、社会課題の解決にも貢献できる結果であったといえる。

また、「情報銀行間連携に係る実証事業」では、情報銀行同士が連携しデータ交換する際に望まれる仕様等を策定し、連携において考慮すべき機能やルールについて検討した。今回のように消費者視点を考慮した仕様や機能を整理し、情報銀行同士が連携し易い環境やルールを事前に整えておくことは重要と考える。更に消費者の視点という意味では、「データ倫理を担う人材の育成等」において、データ倫理についての共通認識を醸成するための審査基準に加え、消費者視点でリスク分析を行える人材を育成するためのプログラムやその内容を審査する構成員を育成するプログラムを作成し、研修も実施した。

これらの本事業における調査内容を踏まえた上で、今後も継続的に、積み残した課題や新たな課題を解決していくことができれば、情報銀行を中心としたデータ流通の更なる促進が期待できるだろう。

用語集

（50 音順・アルファベット順）

No	用語	用語解説
1	オープンソース	Open Source Initiative が定めた“The Open Source Definition”に適合したソフトウェアのこと。利用や再配布に制限を加えないこと、ソースコードを配布すること、プログラムの変更やその配布を許可することなどの条件を満たす。
2	オプトイン	ユーザーに対して事前に許可や同意を求めること。
3	コントローラビリティ	制御可能性のこと。消費者が自身のパーソナルデータを思い通りに管理・制御できること。
4	サービス事業者	消費者に対してサービスを提供する事業者のこと。データ提供元やデータ提供先となり得る。
5	シングルサインオン	一度認証してログインすれば、登録されている他のサービス（アプリケーション）へログインする際の認証を省略できる認証方式のこと。 情報銀行間連携においては、ある情報銀行で特定の認証レベルでログイン済みの場合、同じ認証レベル以下の要求をする別の情報銀行に対しては、認証を省略してログインできる方式のこと。
6	スクレイピング	Web サイトから情報を抽出する方式のことで、認証方式としては第三者（中間的業者）が利用者の ID とパスワードを預かり、管理されたデータなどにアクセスする方式のこと。
7	ステークホルダー	利害関係者のこと。
8	ソーシャルログイン	Facebook、Twitter、LINE といった既に使用している SNS 等 のアカウントを利用して、Web サイトやサービスに新規登録したり、ログインしたりできる認証方式のこと。 情報銀行間連携においては、消費者が既にアカウントを登録済みの情報銀行の ID を利用して、他の情報銀行にログインできる方式のこと。
9	ダッシュボード	各種のデータを視覚化して、一目で容易に理解することを支援するツールのこと。
10	データポータビリティ	本人が提供した各種サービスが保有するデータを再利用しやすい形で本人に還元又は他者に移管できること。
11	データ移転	消費者が特定の事業者から消費者本人のパーソナルデータを取得し、他の事業者に対して取得したパーソナルデータを預託すること。また、消費者が事業者の保有する消費者本人のパーソナルデータについて、事業者に対して開示請求を行った際に、事業者からデータを消費者に提供（開示）すること、若しくは消費者が情報銀行に委託し、情報銀行が委託された消費者のパーソナルデータについて、

		事業者に対して開示請求を行った際に、事業者から消費者の代理である情報銀行にデータを提供（開示）すること、もこれに含む。
12	データ提供	データを第三者に渡すこと。
13	データ提供元事業者	消費者のパーソナルデータを保有し、サービス事業者等のデータ提供先事業者に当該パーソナルデータを提供する事業者のこと。
14	データ提供先事業者	消費者のパーソナルデータを保有するデータ提供元事業者から、データを受領する事業者のこと。
15	データ連携	異なるアプリケーションやシステムをまたいでデータを渡すことや、そのプロセスのこと。 情報銀行間連携においては、消費者の第三者提供に関する合意に基づき、情報銀行が管理する消費者のパーソナルデータを、他の情報銀行に提供すること。
16	データ連携元情報銀行	消費者の第三者提供に関する同意に基づき、情報銀行間においてデータ連携する際、他の情報銀行にパーソナルデータを渡す側の情報銀行のこと。 なお、本書では ID 連携のみを指す場合は、「ID 連携元情報銀行」とした。
19	データ連携先	情報銀行間においてデータ連携する際の、データを受け取る側の情報銀行のこと
20	データ連携先情報銀行	消費者の第三者提供に関する同意に基づき、情報銀行間においてデータ連携する際、他の情報銀行からパーソナルデータを受け取る側の情報銀行のこと。 なお、本書では ID 連携のみを指す場合は、「ID 連携先情報銀行」とした。
21	トレーサビリティ	一般的には、物品の流通経路を生産段階から最終消費段階または廃棄段階までを追跡可能な状態を意味するが、本書ではデータの流通経路の追跡可能性を意味する。
22	プライバシーマーク	日本産業規格「JIS Q 15001 個人情報保護マネジメントシステム－要求事項」に適合し、個人情報について適切な保護措置を講ずる体制を整備していることを証明するマークのこと。一般財団法人日本情報経済社会推進協会（JIPDEC）が付与する。
23	プラットフォーム	個人情報利用に関する同意・流通履歴などを管理する情報銀行の仕組みを支える技術基盤のこと。
24	ユーザーインターフェース	利用者と製品やサービスとのインターフェース（接点）のこと。
23	情報セキュリティマネジメントシステム（ISMS）適合性評価制度	国際的に整合性のとれた情報セキュリティマネジメントシステムに対する第三者適合性評価制度のこと。
24	情報信託機能の認定に係る指針	総務省及び経済産業省が、「情報信託機能の認定スキームの在り方に関する検討会」にて取りまとめた民間団体等による情報銀行の任意の認定の仕組みに

		関する指針のこと。2018 年 6 月に ver1.0 が公開され、2019 年 10 月に ver2.0 が公開された。
25	身元保証レベル	取得した身元保証情報の信頼性の高さを示す指標のこと。複数の情報銀行間でデータを流通させる際に、流通先で情報の信頼性を把握するために用いられる。身元保証レベルは、1 以上の整数値であり、数値が高いほど、情報の信頼性が高いことを意味する。
26	認証レベル	情報銀行の認証におけるセキュリティ強度を示す指標のこと。提供するサービスや扱うデータの秘匿性を踏まえて各情報銀行が設定する。認証レベルは、1 以上の整数値であり、数値が高いほど、セキュリティ強度が高いことを意味する。
27	秘匿レベル	情報銀行で取り扱うデータの秘匿性の高さを示す指標のこと。秘匿レベルは、1 以上の整数値であり、数値が高いほど、秘匿性が高いことを意味する。 なお、秘匿レベル 1 は、「本人の同意に基づいて情報銀行が取得・提供可能な情報」となるが、秘匿レベル 2 以上については、要配慮個人情報を取り扱う可能性があるため、今後の業界団体、有識者等の情報銀行における取扱いに関する検討結果に従い、順次定義するものとなる。2021 年 3 月現在で検討されている情報分野は、保険医療情報となる。
28	Consumer Data Standards （略称:CDS）	FAPI を参考に、オーストラリア政府により消費者データ権法の導入の一環として開発されたもので、オーストラリア人がデータをより適切に管理できるようにした標準仕様のこと。
29	Financial-grade API （略称:FAPI）	金融業界などの高度なセキュリティが求められる環境での使用を想定した API の技術仕様のこと。OAuth 2.0、OIDC を基にしており、国際標準化団体の OpenID Foundation のワーキンググループによって策定が進められている。
30	ID 連携	ある情報銀行に消費者が新規登録やログインする際に、既に利用している別の情報銀行の認証結果を利用すること。
31	National Institute of Standards and Technology （略称:NIST）	米国国立標準技術研究所のこと。NIST SP 800 シリーズなど、世界的なデファクトスタンダートとなる情報セキュリティ関連文書を発行している。
32	OAuth 2.0	API（Application Program Interface）を利用し、複数の Web サービスを連携して動作させる際に、アクセスする操作やデータの範囲を限定するためのアクセス認可に関する技術仕様のこと。標準化団体 IETF によって策定された。
33	OpenID Connect （略称:OIDC）	ユーザー認証に使用される ID トークンを発行するための技術仕様のこと。 OAuth 2.0 を基にしており、標準化団体 OpenID Foundation によって策定された。

34	OpenID Provider （略称:OP）	消費者のアカウントを管理し、トークンを発行（アクセス権を付与する認可）する役割のこと。
35	Relying Party （略称:RP）	OP に対してトークンを要求し、消費者のパーソナルデータを活用して消費者にサービスを提供する役割のこと。
36	Resource Server （略称:RS）	消費者のパーソナルデータを管理・蓄積する役割のこと。
37	Request for Comments （略称:RFC）	インターネット技術を議論し標準化を進める任意団体「IETF」が作成したインターネット技術の標準的な仕様等を記した文書のこと。
38	Security Assertion Markup Language （略称:SAML）	異なるインターネットドメイン間でユーザー認証を行うための標準仕様のこと。標準化団体 OASIS Open によって策定された。
39	Secure Sockets Layer/Transport Layer Security （略称:SSL/TLS）	インターネット接続を安全に保つため、2 つのシステム間で送信されるデータを暗号化し、第三者による盗み見や改竄を防止する技術のこと。

参考文献

（50 音順・アルファベット順）

No	参考文献
1	一般社団法人データ流通推進協議会，データカタログ作成ガイドライン V1.1（中間とりまとめ），2019 年 1 月 25 日.
2	経済産業省、総務省、IoT 推進コンソーシアム，データ流通プラットフォーム間の連携を実現するための基本的事項，平成 29 年 4 月 .
3	個人情報の保護に関する法律.
4	個人情報の保護に関する法律等の一部を改正する法律，令和 2 年 6 月公布.
5	公正取引委員会，デジタル・プラットフォーム事業者と個人情報等を提供する消費者との取引における優越的地位の濫用に関する独占禁止法上の考え方，2019 年 12 月 17 日.
6	情報信託機能の認定スキームの在り方に関する検討会，情報信託機能の認定に係る指針 ver1.0，平成 30 年 6 月.
7	情報信託機能の認定スキームの在り方に関する検討会，情報信託機能の認定に係る指針 ver2.0，令和元年 10 月.
8	Dick Hardt（編）「The OAuth 2.0 Authorization Framework」＜ https://tools.ietf.org/html/rfc6749＞（参照日 2021 年 2 月 24 日）.
9	Nat Sakimura, et al.「Financial-grade API - Part 1: Read-Only API Security Profile」＜ https://openid.net/specs/openid-financial-api-part-1-ID2.html＞（参照日 2021 年 2 月 24 日）.
10	Nat Sakimura, et al.「Financial-grade API - Part 2: Advanced Security Profile」＜ https://openid.net/specs/openid-financial-api-part-2.html＞（参照日 2021 年 2 月 24 日）.
11	Nat Sakimura, et al.「OpenID Connect Core 1.0 incorporating errata set 1」＜ https://openid.net/specs/openid-financial-api-part-1-ID2.html＞（参照日 2021 年 2 月 24 日）.
12	OpenID Foundation「FAPI 2 0 Baseline Profile」＜ https://bitbucket.org/openid/fapi/src/master/FAPI_2_0_Baseline_Profile.md＞（参照日 2021 年 2 月 24 日）.
13	Paul A. Grassi, et al.「NIST Special Publication 800-63 Revision 3 Digital Identity Guidelines」<https://pages.nist.gov/800-63-3/sp800-63-3.html>（参照日 2021 年 2 月 24 日）.

14	Paul A. Grassi, et al.「NIST Special Publication 800-63B Digital Identity Guidelines Authentication and Lifecycle Managemente」<https://pages.nist.gov/800-63-3/sp800-63b.html>（参照日 2021 年 2 月 24 日）.