資料17－1

第17回　情報信託機能の認定スキームの在り方に関する検討会

情報信託機能の普及促進に向けた課題解決に係る調査
－　報告資料　－

情報銀行間連携に係る実証事業

2021年5月17日
大日本印刷株式会社

DNP

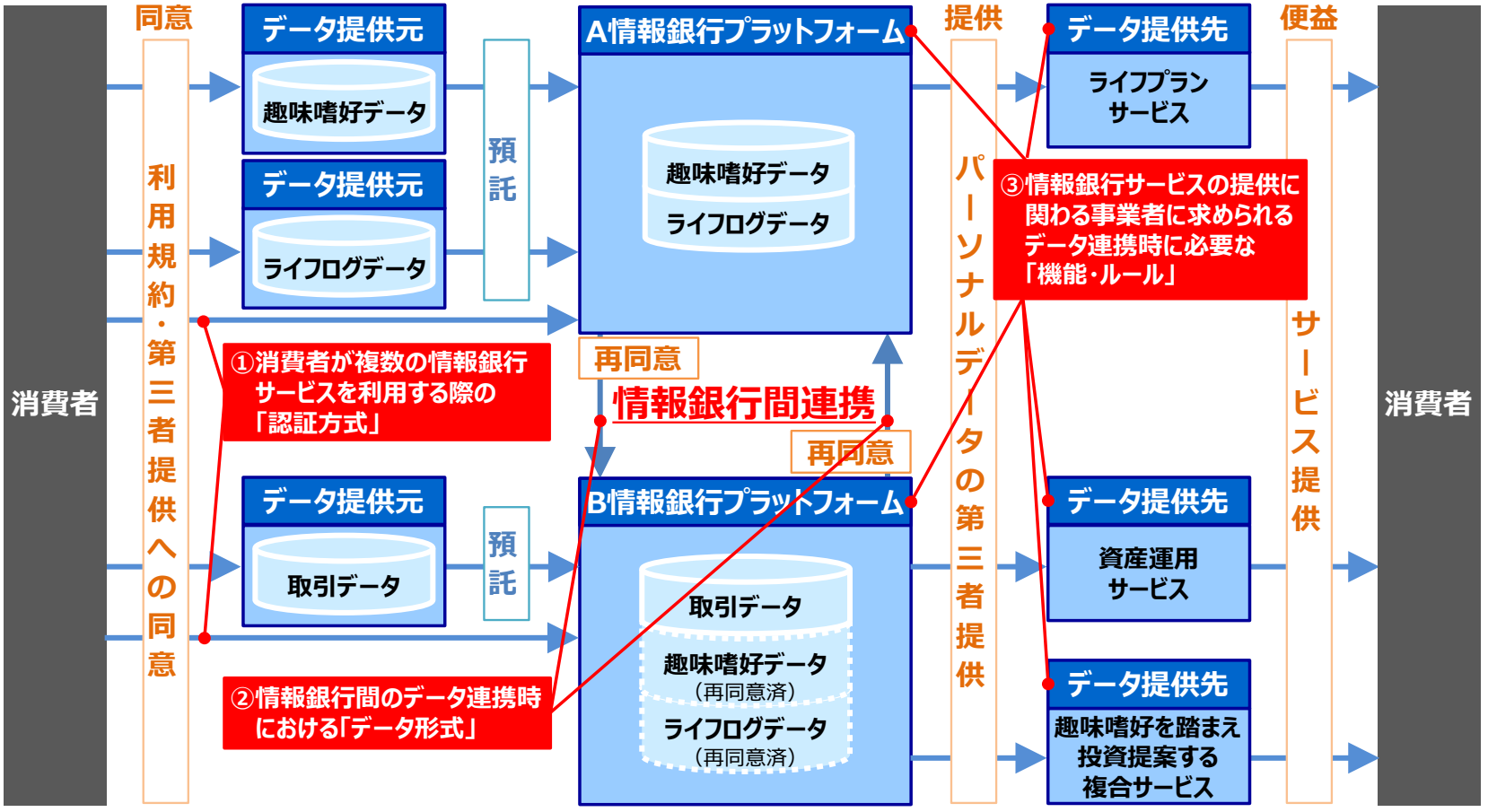
1. 情報銀行間連携に係る実証事業の背景

DNP

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」において提起された主な課題を踏まえ、情報銀行間連携時におけるオープンな共通仕様の策定に取り組んだ。

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」**



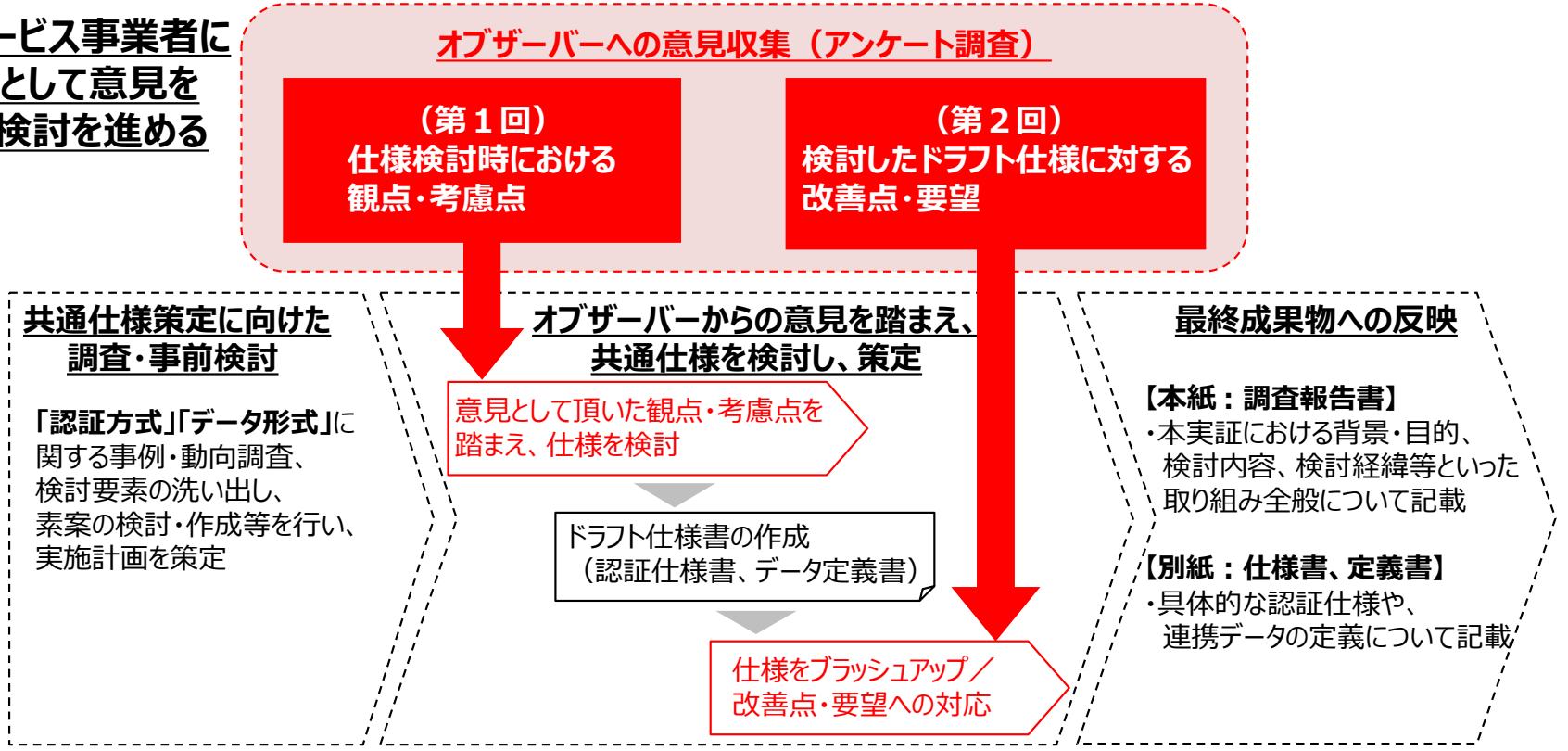
2. 情報銀行間連携に係る実証事業の概要

DNP

主な課題を踏まえた検討方針、及び検討の進め方に関する概要は以下の通りである。

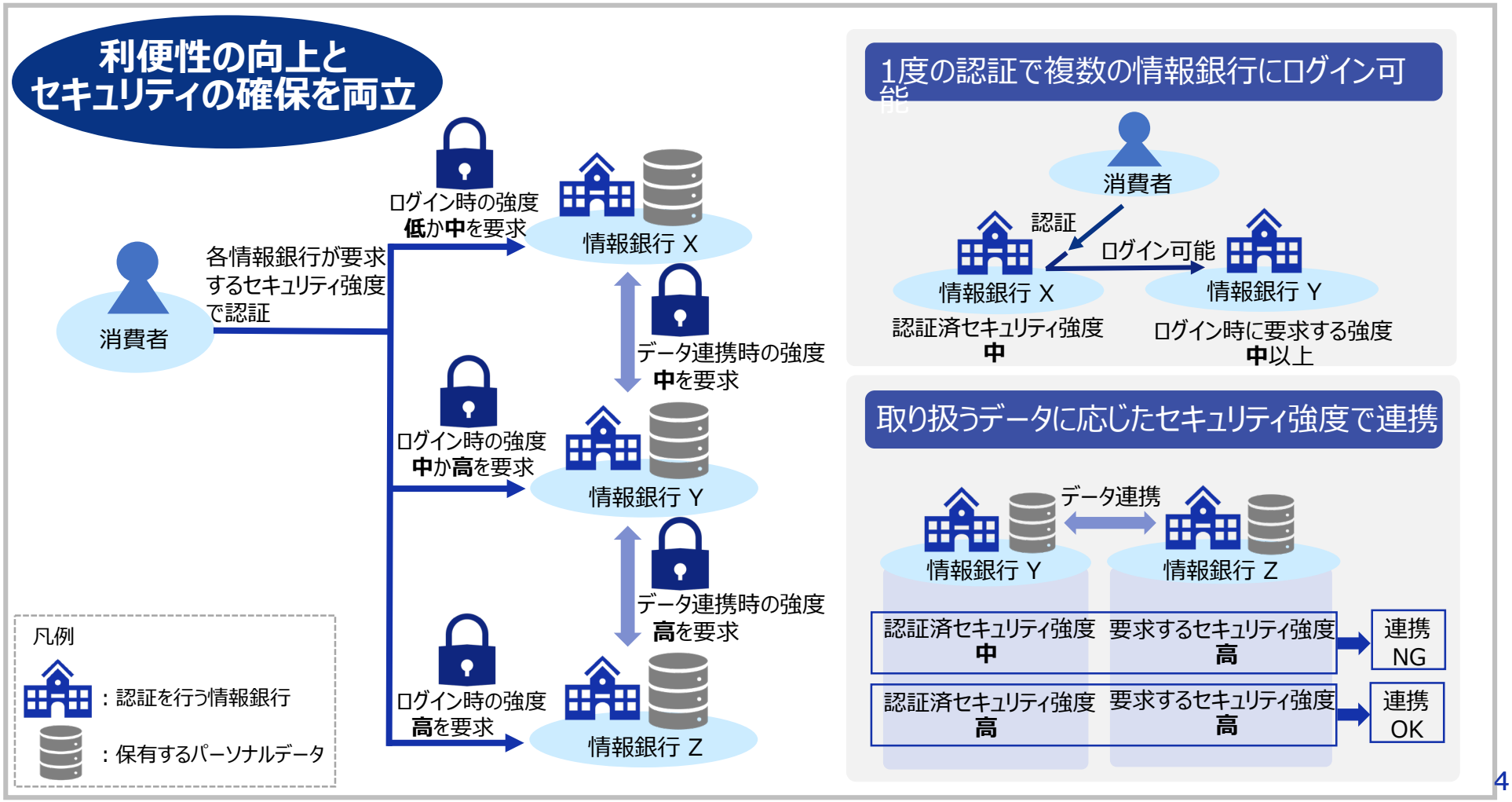
課題	検討方針
①消費者が複数の情報銀行サービスを利用する際の**「認証方式」**	認証はセキュリティに関わる要素のため、利便性だけではなく、セキュリティとの両立を目指した「認証方式」を検討
②情報銀行間のデータ連携時における**「データ形式」**	データフォーマットの標準化だけではなく、データが持つ信頼性や秘匿性といった情報の質的側面も考慮した「データ形式」を検討
③情報銀行サービスの提供に関わる事業者に求められるデータ連携時に必要な**「機能・ルール」**	データ流通の普及・促進を妨げる要因の一つになっている消費者不安を低減するため、消費者によるコントローラビリティの確保、及び消費者が安心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

情報銀行サービス事業者にオブザーバーとして意見を頂きながら、検討を進める方法で実施



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」 DNP
～「認証方式」に関する検討概要～

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た。



4. 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」 DNP
～「認証方式」に関する検討結果・まとめ（1/2）～

検討結果

項番	実施項目	検討内容・方法	検討結果
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、情報銀行への負荷という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
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で、情報銀行間連携の運用についてOIDCによるID連携、OAuthによるデータ連携を許容
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

4. 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」～「認証方式」に関する検討結果・まとめ（2/2）～

DNP

検討結果

項番	実施項目	検討内容・方法	検討結果
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 ✓ 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	✓ 情報銀行間連携時における認証関連のAPI仕様

まとめ

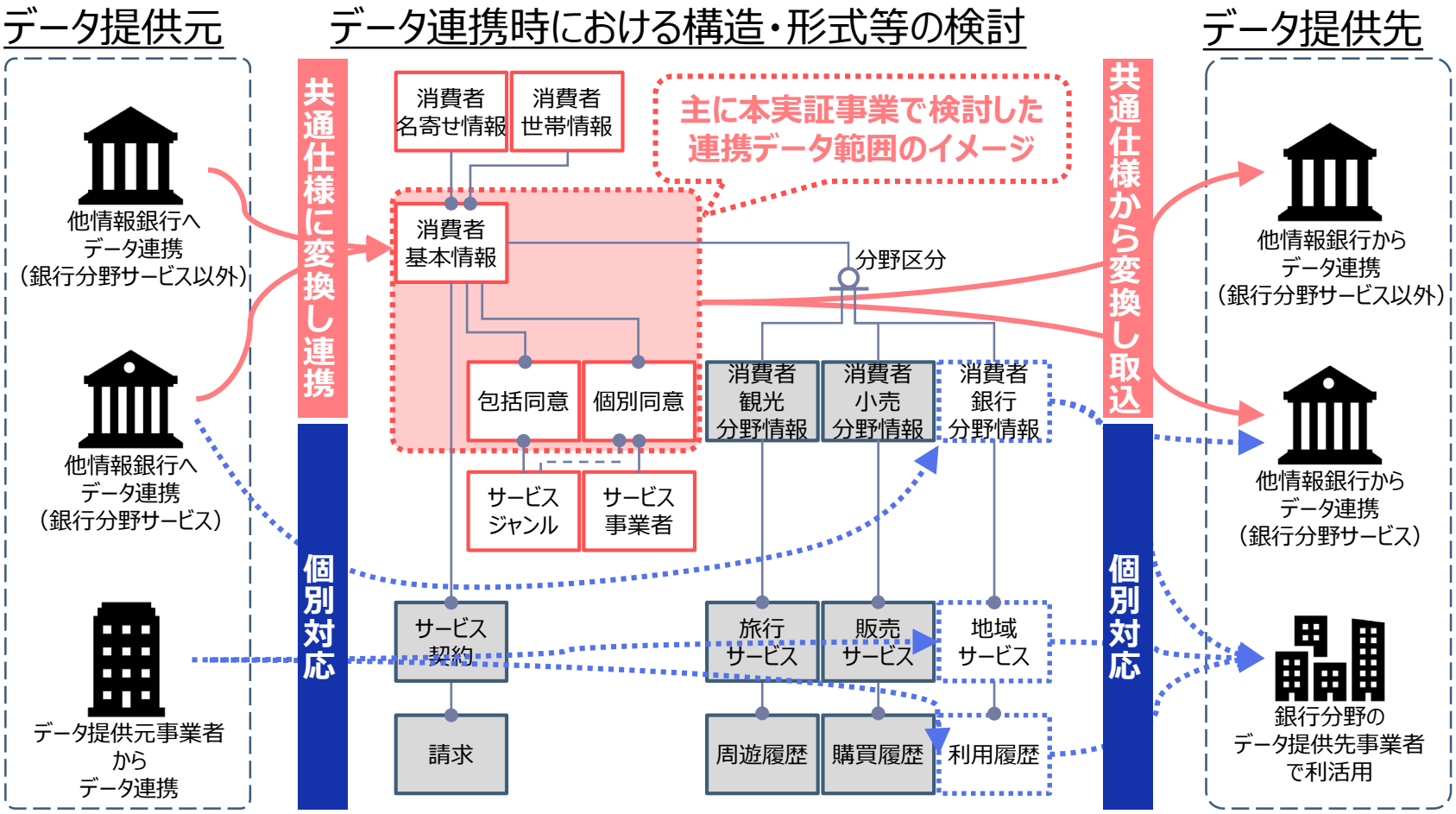
情報銀行間連携における認証方式を、ID連携時、データ連携時に分けて仕様を検討した。
また、消費者に対する必要最低限の認証要求と、取り扱うデータの秘匿性を踏まえた必要十分なセキュリティ強度のバランスを意識して認証方式を検討し、情報銀行間連携における認証仕様としてまとめた。
なお、今後の更なる普及、促進に必要と思われる検討・取り組みとして下記が挙げられる。

- 高い認証レベルに対応した認証方法の導入・推進
  →生体認証、暗号デバイスを用いた認証等の普及
- 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
  →事後的に判明した不適切なデータ連携先情報銀行への対処法
- ユーザビリティ向上のための更なる仕様改善
- 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

5. 情報銀行間のデータ連携時における「データ形式」 ～「データ形式」に関する検討概要～

DNP

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ようにするため、事業者間でデータ連携する際の標準化フォーマットを検討した。
また、連携データが持つ情報の信頼性や秘匿性を連携先事業者が把握する方策も検討した。



6. 情報銀行間のデータ連携時における「データ形式」 ～「データ形式」に関する検討結果・まとめ（1/2）～

DNP

検討結果

項番	実施項目	検討内容・方法	検討結果
1	データ項目の定義・名称標準化	✓ 業界トップ17社や国際的な標準規格等を参考に、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	✓ 情報銀行間データ連携する際の共通データ項目を定義
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
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
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を調査・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

7. 情報銀行間のデータ連携時における「データ形式」 ～「データ形式」に関する検討結果・まとめ（2/2）～

DNP

検討結果

項番	実施項目	検討内容・方法	検討結果
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

まとめ

消費者の基本情報、同意管理情報、履歴情報等に関するデータ項目やデータ構造、伝送時のデータフォーマットについて、海外で利用されている汎用的な仕様をベースに、日本固有の特徴を踏まえたカスタマイズをして定義した。また、連携されるデータの信頼性や秘匿性の度合いなどを把握するために必要なメタデータを含め、情報銀行間連携における連携データについて定義した。
なお、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
- 複数要素を連結して保有しているデータへの対応
  →氏名におけるミドルネームや住所における番地・建物名などへの切り分け処理等の対応
- 各情報銀行で保有するマスタ情報の紐づけ負荷の軽減
- 情報銀行間で不変の共通ユーザー識別子を保有する是非
  →情報の不整合リスクを抑えるのに有効な不変の共通ユーザー識別子について、プライバシー上の懸念も踏まえて要検討

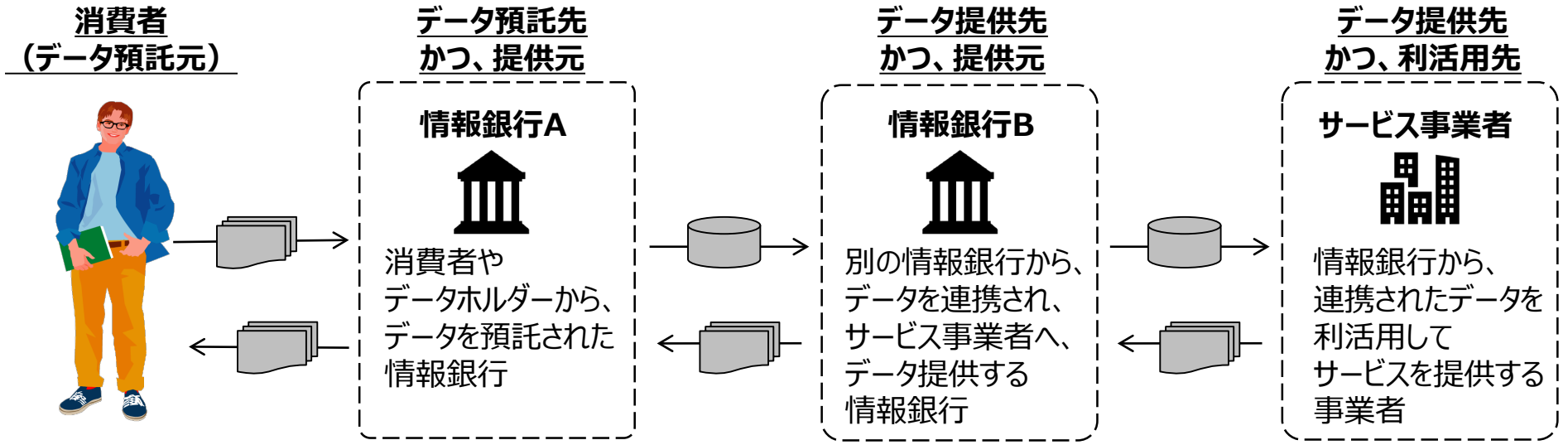
8. 事業者に求められるデータ連携に必要な「機能・ルール」
～「機能・ルール」に関する検討概要～

DNP

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、主に、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を行うために必要な機能・ルールについて、下記6つの観点で検討した。

６つの観点

① 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
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
③ 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
④ 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
⑤ 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
⑥ 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



9. 事業者に求められるデータ連携に必要な「機能・ルール」～「機能・ルール」に関する検討結果・まとめ～

DNP

検討内容

①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

- ✓ 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
- ✓ 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
- ✓ 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

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

- ✓ 利用目的に応じた第三者提供先へのデータの選択提供
- ✓ データの秘匿性の度合いを可視化した提供方法
- ✓ 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

③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

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

④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

⑤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

⑥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

- ✓ 情報銀行を介したデータの移転に関する電子的な請求
- ✓ 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
- ✓ データの移転時における盗聴防止
- ✓ データの移転時における改竄防止

まとめ

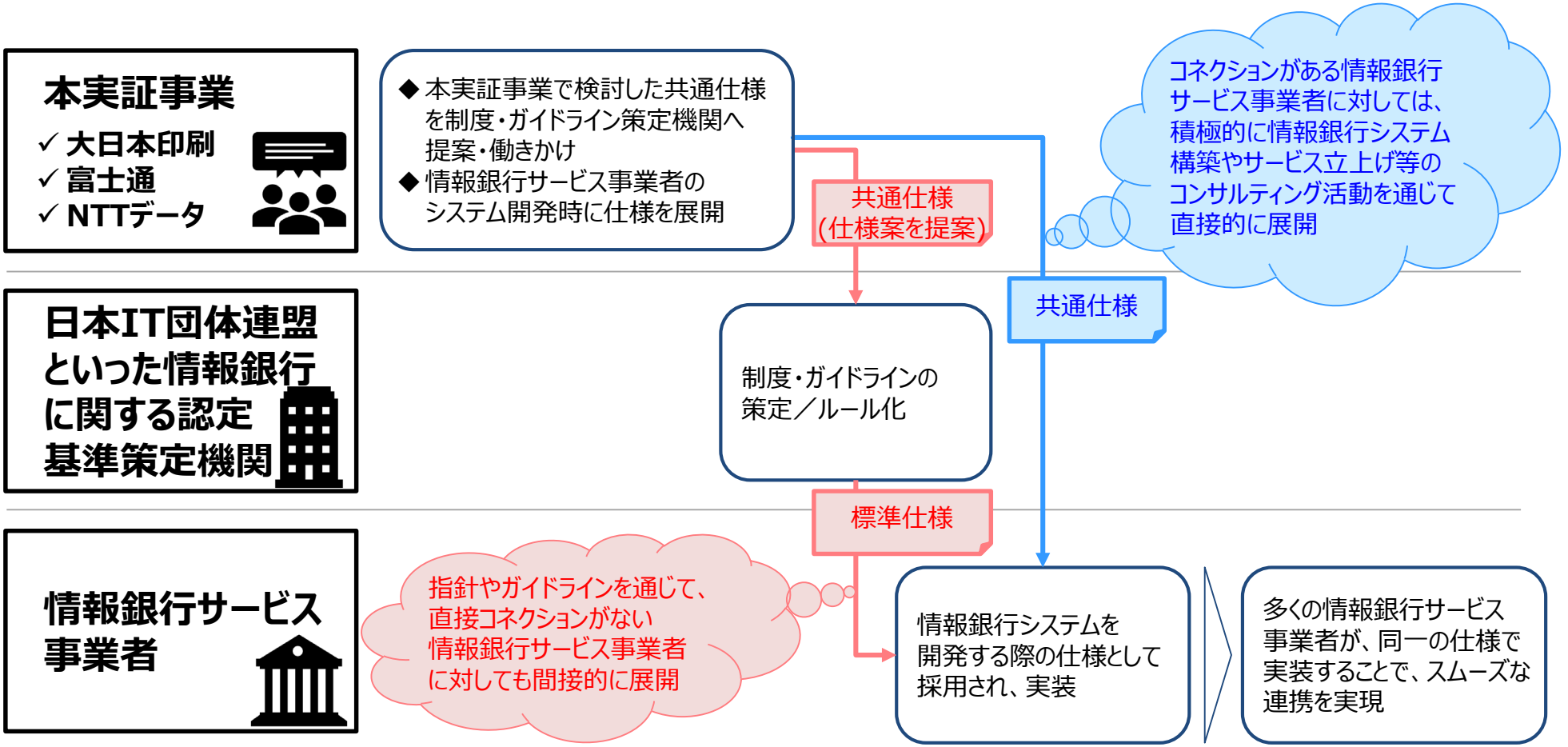
「消費者本人がパーソナルデータに関する利活用状況の把握や制御を行うために必要な機能・ルール」について、具備すべき機能や、運用的なルールなどについて検討・整理した。
本実証事業で得られた結果が浸透し、消費者によるコントローラビリティの確保はもちろん、それに応える事業者への信頼度が増すことで、消費者不安が低減され、データ流通が普及・促進することを期待する。
なお、今後の更なる普及、促進に必要と思われる検討・取り組みとして下記が挙げられる。

- ➢ 秘匿レベル定義のブラッシュアップ
  ➞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、順次定義を見直し
- ➢ 包括的なトレーサビリティを提供するために必要なユーザー識別子や履歴情報の共有に対する消費者理解の獲得
- ➢ 「情報信託機能の認定スキームの在り方に関する検討会」における提供先第三者に係る情報銀行の認定等に関する議論や動向を踏まえた基準の見直し

10. 情報銀行間連携の普及・促進に向けた今後の取り組み

DNP

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。

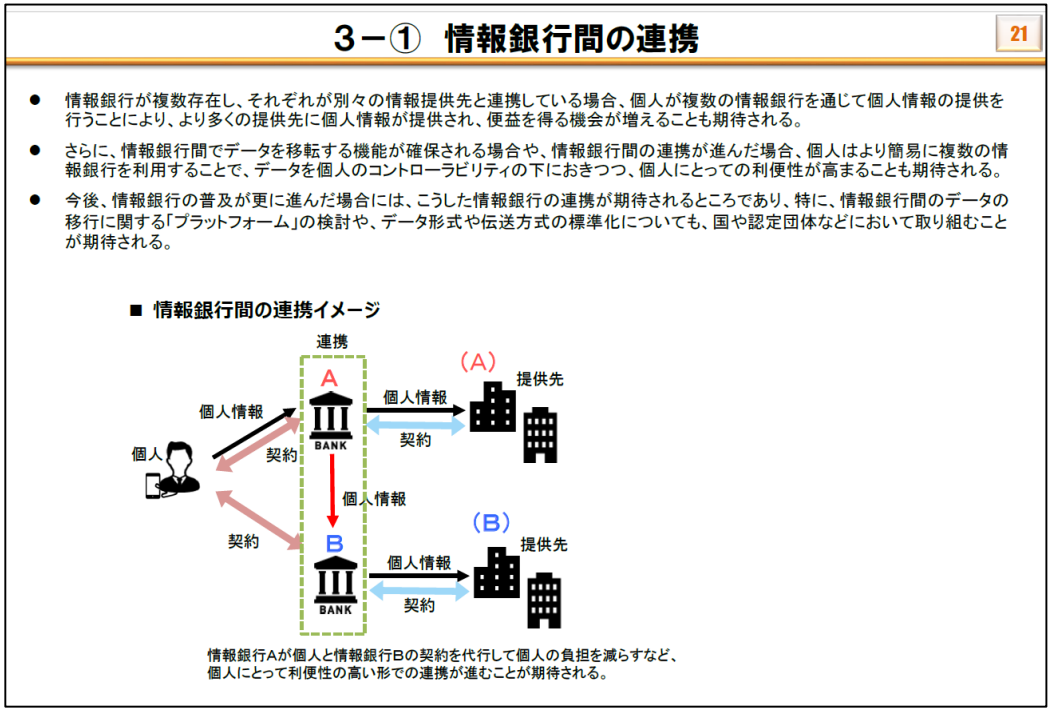


【補足】 第三者提供先からの再提供の禁止事項に関して

DNP

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、これを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