参考資料１－１

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

令和元年10月８日

（はじめに）

- 個人情報を含むパーソナルデータの円滑な流通を実現するため、個人の関与の下での新たなサービスを早期に立ち上げることが期待されるとの考えのもと、その一つである情報信託機能を提供する「情報銀行」については、一定の要件を満たした者を社会的に認知するため、民間の団体等による任意の認定の仕組みが望ましいとの提言が、平成２９年６月の情報通信審議会においてなされた。
- この認定の仕組みを有効に機能させるためには、個人情報保護法の趣旨も踏まえた、また、本人の関与という要素を十分に取り込んだ認定基準を作成することが重要であった。
- 総務省及び経済産業省で開催した本検討会では、以下の認識の下、平成29年11月～平成30年4月までの計６回に及ぶ議論を行い、平成30年6月に**「情報信託機能の認定に係る指針ver1.0」**（以下「認定指針」）をとりまとめた。
  - 新しいサービスを普及させるためには、利用者や社会の信頼を得ることが大切であり、一定の信頼性を満たす者を認定するとともに、個人のコントローラビリティを確保する必要がある。
  - 他方、このようなサービスは現時点では存在せず、今後、その出現が期待される分野であるため、サービスの内容やビジネスモデルを限定することは望ましくなく、様々なタイプのサービスが提供され、事業者の競争を促すような認定基準とすることが必要である。
  - なお、「個人のコントローラビリティを確保するための機能」については、コントローラビリティとサービスの多様性とのバランスを考慮する必要がある。
- 認定指針の策定に関する検討は、情報銀行のサービスが未だ開始されていない中で行われたが、その後、総務省による情報銀行の実証事業、その他各企業における情報銀行事業の検討、さらには認定指針に基づく一般社団法人日本ＩＴ団体連盟による認定事業の開始等の動きがあった。
- 本とりまとめは、これらの状況変化の中で顕在化した課題に対応するとともに、今後の情報銀行事業の発展を見据え、認定指針について見直しが必要か検討を行うため、検討会を平成31年1月～6月までに計7回開催し、以下の認識の下、とりまとめたものである。
  - 新しいサービスを普及させるためには、実際に検討されている事業内容に応じて、必要と認められる点については認定制度を柔軟に見直すことが必要である。
  - より柔軟かつ事業の普及に合わせた対応を確保するため、認定指針に定める内容の他にも、認定団体をはじめとした関係者における、普及に向けた独自の取り組みも期待される。

＜本検討会の今後の運用方法＞

・ 情報銀行事業及びその認定についてはまだ開始後間もないため、本検討会は当面継続し、定期的に開催して認定指針の運用状況について点検する。

・ 情報銀行事業の展開や関連制度の動向等を踏まえて認定指針を改定する必要が生じた場合には、総務省・経済産業省または認定団体からの提案を受け、本検討会において審議し、本指針の改訂を行うことができる。

＜認定指針の見直しと認定制度の関係＞

・ 認定指針が改訂された場合、改訂に伴う認定制度の運用や見直しの時期については、認定団体において決定する。

情報信託機能の認定スキームに関する検討会（第7回～第13回）

【委員】

（敬称略、五十音順、肩書きは令和元年6月6日現在）

	石原　遥平	一般社団法人シェアリングエコノミー協会
	伊藤　直之	株式会社インテージ　開発本部　事業開発室 エバンジェリスト
	井上　貴雄	大日本印刷株式会社 ABセンター コミュニケーション開発本部　本部長
	太田　祐一	株式会社Data Sign　代表取締役社長
	落合　孝文	渥美坂井法律事務所・外国法共同事業　弁護士
	加毛　明	東京大学大学院法学政治学研究科　准教授
	高口　鉄平	静岡大学学術院情報学領域　准教授
	小林　慎太郎	株式会社野村総合研究所 ICT・メディア産業コンサルティング部　パブリックポリシーグループマネージャー／上級コンサルタント
○	宍戸　常寿	東京大学大学院法学政治学研究科　教授
	立谷　光太郎	株式会社博報堂　顧問
	田中　邦裕	さくらインターネット株式会社　代表取締役社長
	長田　三紀	情報通信消費者ネットワーク
	藤本　洋史	情報信託機能普及協議会
	古谷　由紀子	公益社団法人日本消費生活アドバイザー・コンサルタント・相談員協会　監事
	真野　浩	一般社団法人データ流通推進協議会　代表理事
	美馬　正司	株式会社日立コンサルティング スマート社会基盤コンサルティング第2本部　ディレクター
	森　亮二	英知法律事務所　弁護士
	森下　哲朗	上智大学法科大学院　教授
	森田　弘昭	株式会社マイデータ・インテリジェンス　取締役
	山本　龍彦	慶應義塾大学大学院法務研究科　教授
	湯淺　墾道	情報セキュリティ大学院大学 学長補佐／情報セキュリティ研究科　教授
	吉澤　陽子	みずほ銀行　データソリューション開発部 ソリューション企画チーム　次長
	若目田　光生	一般社団法人日本経済団体連合会 デジタルエコノミー推進委員会企画部会 データ戦略WG　主査／ 株式会社日本総合研究所 リサーチ・コンサルティング部門　上席主任研究員

【関係省庁（オブザーバー）】

内閣官房 情報通信技術（IT）総合戦略室

個人情報保護委員会事務局

［事務局］ 一般社団法人日本IT団体連盟（※平成31年3月31日まで）

［主催］ 総務省、経済産業省

（参考）「情報銀行」に関する検討の経緯

●官民データ活用推進基本法（平成28年12月　公布・施行）
個人の関与の下での多様な主体による官民データの適正な活用（第12条）

- 国は、個人に関する官民データの円滑な流通を促進するため、事業者の競争上の地位その他正当な利益の保護に配慮しつつ、多様な主体が個人に関する官民データを当該個人の関与の下で適正に活用することができるようにするための基盤の整備その他の必要な措置を講ずるものとする。

● データ流通環境整備検討会（内閣官房ＩＴ総合戦略室）
「AI、IoT時代におけるデータ活用WG 中間とりまとめ」（平成29年2月）

- パーソナルデータを含めた多種多様かつ大量のデータの円滑な流通を実現するためには、**個人の関与の下でデータ流通・活用を進める仕組み（PDS、情報銀行、データ取引市場）が有効**。
- 情報銀行等については、分野横断的なデータ活用に向けた動きが出始めており、今後、事業者、政府等の連携により、その社会実装に向けて積極的に取組を推進する必要がある。

● 情報通信審議会（総務省）
「IoT／ビッグデータ時代に向けた新たな情報通信政策の在り方」第四次中間答申（平成29年7月）

- データ取引市場及び情報信託機能を担う者について、一定の要件を満たした者を社会的に認知するため、**民間の団体等によるルールの下、任意の認定制度が実施されることが望ましい**。
- 情報信託機能については、2017年夏以降、必要なルールを更に具体化するための実証事業を継続するとともに、2017年中に、産学が連携して推進体制を整備し、任意の認定制度やルールの在り方について検討し、年内に認定業務に着手することを目指す。

とりまとめの概要

- 本検討会では、以下の項目について、情報銀行及び認定指針に基づく認定の考え方に関し、整理を行った。
- 整理した内容を中心に、指針ver1.0を見直した指針ver2.0について添付する。

1. 情報銀行認定の基本的な考え方
   - ①情報銀行の定義・考え方
   - ②情報銀行の提供するサービス例
   - ③未成年等の制限行為能力者が情報銀行を利用する場合
   - ④情報銀行における個人情報の加工
   - ⑤行政機関／独立行政法人等の認定について
   - ⑥複数者が共同で情報銀行事業を行う場合の認定
   - ⑦提供先第三者の選定
   - ⑧認定の対象とする個人情報の範囲

2. 個人による情報銀行の選択等
   - ①個人情報提供の対価
   - ②情報銀行に関する透明性の確保
   - ③データ倫理審査会

3. プレイヤー間の連携
   - ①情報銀行間の連携
   - ②情報銀行とデータ取引市場の連携
   - ③提供先第三者からの「再提供」禁止に関する考え方

4. 信用スコアの取扱い

5. 今後の情報銀行の展開に向けたその他の取組み

1．情報銀行認定の基本的な考え方

【検討会での議論及び基本的な考え方】

- 情報銀行については、個人情報の活用に関して社会的な不安がある中で、個人の関与の下でデータの流通・活用を進める仕組みとして議論が始められた。情報銀行が、個人から委任を受けた個人の代理として、個人が安心して自らに関する情報を預けられる存在として機能することにより、情報の流通・活用が促進されることが期待される。
- 指針ver1.0では情報銀行について、情報銀行が備えるべき機能を中心に定義されていたところ、こうした情報銀行の目的も踏まえて、情報銀行の定義を再度整理が必要との意見があった。
- また、今後情報銀行事業が実サービスとして展開されていく場合、情報銀行の基本的な機能である、個人情報の管理及び第三者提供の機能以外にも、付随するサービス提供が行われていくと考えられる。情報銀行の果たしていく役割を明確化するため、こうした付随するサービスの例についても示す必要があるとの意見があった。
- 以上を踏まえ、情報銀行の定義及び情報銀行の提供するサービスについて整理した。
- 加えて、情報銀行事業の具体化や、日本IT団体連盟による認定制度の運用開始に伴い、認定の考え方についても明確化が必要な点が出てきたため、認定する事業者の単位や、対象とするデータの範囲等について、認定指針における考え方の整理を行った。認定指針に基づく認定は、本とりまとめで整理した解釈に基づいて行われるべきである。

■「情報銀行」の定義について

- 指針ver1.0では、内閣官房IT総合戦略室「データ流通環境整備検討会中間とりまとめ」（平成29年2月）における情報銀行の定義を基本としたが、本定義で定義された、包括的な同意を取得するケースに加え、個別的な同意を取得するケースのうち情報銀行が比較的大きな役割を果たすものについても認定の対象とした。

> 【指針ver1.0における「情報銀行」の定義】
> 情報銀行（情報利用信用銀行）とは、個人とのデータ活用に関する契約等に基づき、PDS等のシステムを活用して個人のデータを管理するとともに、個人の指示又は予め指定した条件に基づき個人に代わり妥当性を判断の上、データを第三者（他の事業者）に提供する事業。

- 情報銀行の機能に加え、基本となる考え方や目的を含めて、認定指針の対象となる情報銀行の定義・考え方を次項のとおり整理した。

1－①　情報銀行の定義・考え方

指針に追記

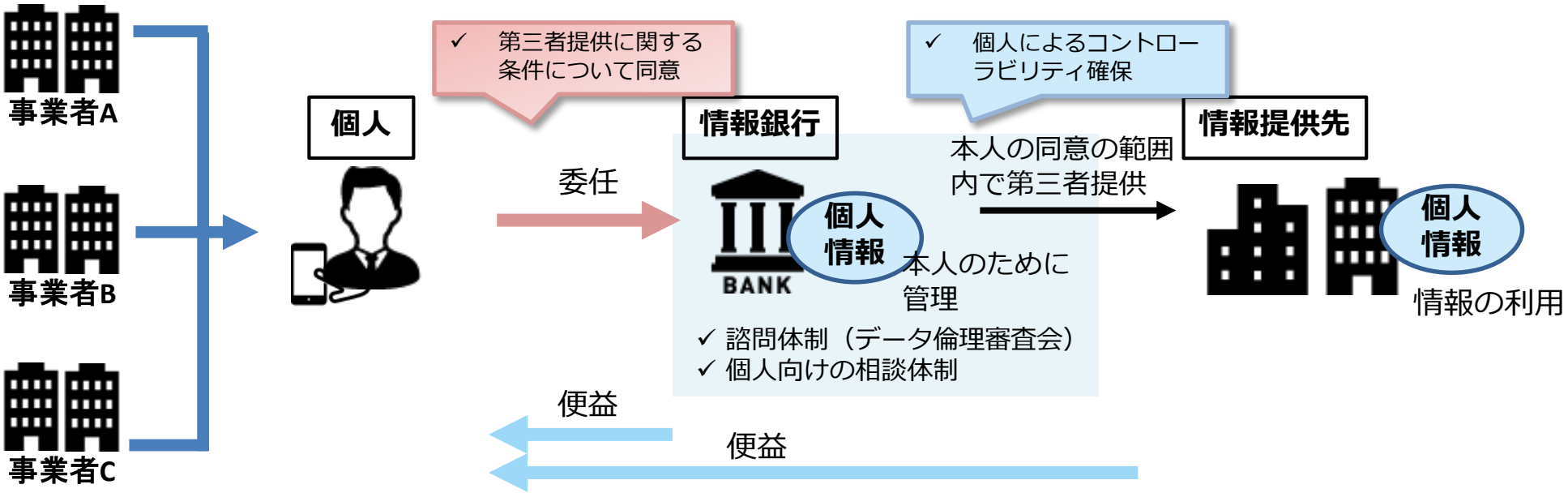
「情報銀行」は、実効的な本人関与（コントローラビリティ）を高めて、パーソナルデータの流通・活用を促進するという目的の下、本人が同意した一定の範囲において、本人が、信頼できる主体に個人情報の第三者提供を委任するというもの。

【機能】

- 「情報銀行」の機能は、個人からの委任を受けて、当該個人に関する個人情報を含むデータを管理するとともに、当該データを第三者（データを利活用する事業者）に提供することであり、個人は直接的又は間接的な便益を受け取る。
- 本人の同意は、使いやすいユーザーインターフェイスを用いて、情報銀行から提案された第三者提供の可否を個別に判断する、又は、情報銀行から事前に示された第三者提供の条件を個別に／包括的に選択する方法により行う。

【個人と情報銀行の関係】

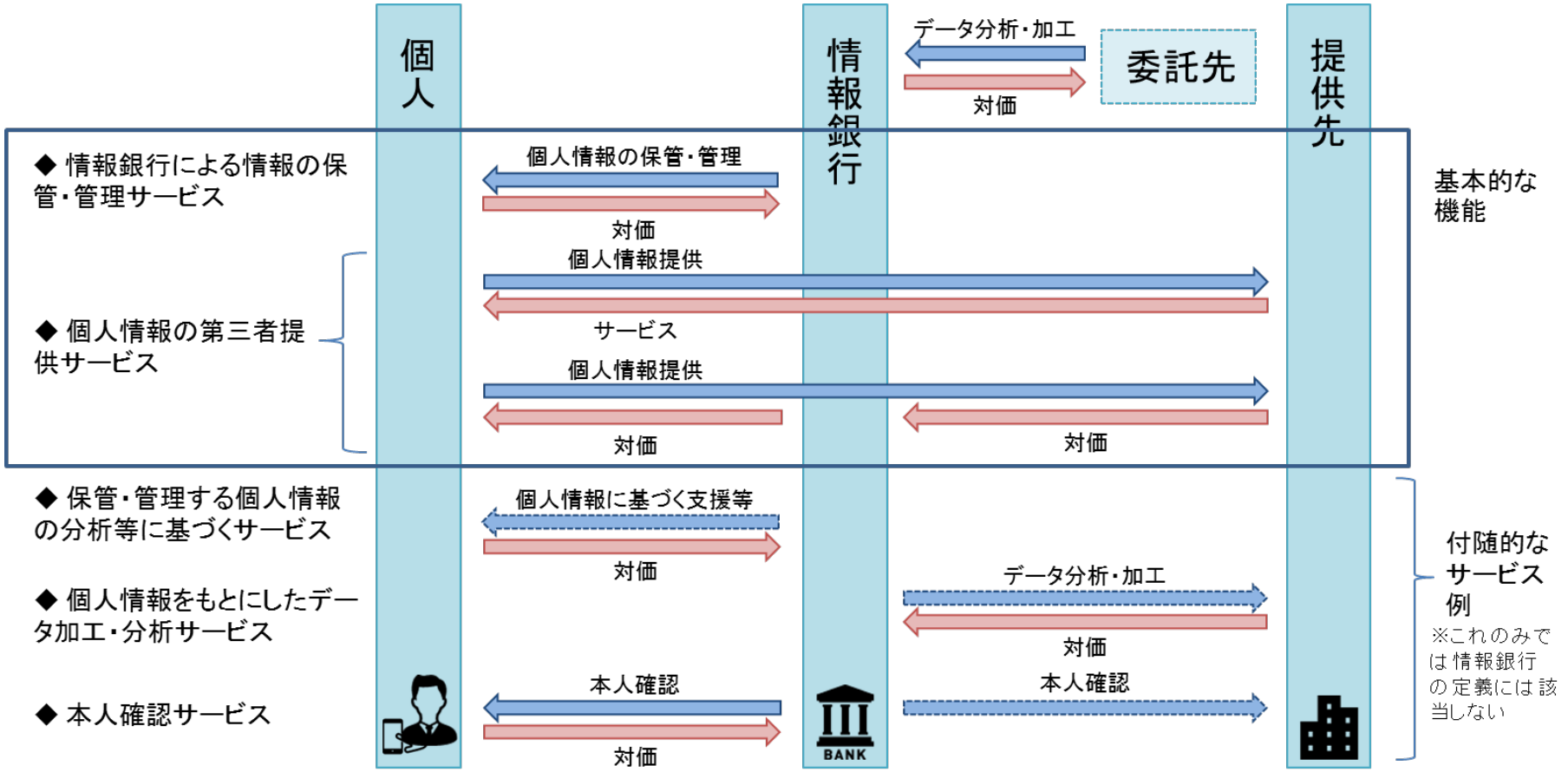
- 情報銀行が個人に提供するサービス内容（情報銀行が扱うデータの種類、提供先第三者となる事業者の条件、提供先における利用条件）については、情報銀行が個人に対して適切に提示し、個人が同意するとともに、契約等により当該サービス内容について情報銀行の責任を担保する。



1－②　情報銀行の提供するサービス例

- 情報銀行の基本的な機能は個人情報の管理及び第三者提供であるが、情報銀行事業においてはこれらに付随して他のサービスを提供することも考えられ、サービスの提供や対価についてもその形態によって様々な形を取りうる。以下にこうしたサービスの例を示すが、情報銀行の提供サービスについては今後多様な展開を見せることが望まれるため、このサービス例に限られるものではない。
- 情報銀行事業については、基本的な機能を核としつつ、このように付随して様々なサービスが提供されることで、今後広がりを見せていくことが期待される。

■ **情報銀行の提供するサービス例**



1－③　未成年等の制限行為能力者が情報銀行を利用する場合

指針に追記

- 情報銀行は将来的には、例えば未成年者向けのインターフェイスを提供するなど、判断能力の不十分な者の判断を補完する役割を担うことが想定されることも踏まえ、これらの者に対する法的な保護についても留意する必要がある。
- 認定指針では、情報銀行は①個人情報の第三者提供等に関し個人の同意を取得することに加え、②個人との契約により責任関係を明確にすることとなっている 。
- 基本的に、①同意を行う者と②契約を行う者は同一の主体を想定しているが、未成年者等の制限行為能力者については、これらの行為を行う主体が異なる場合もあり得る。
- 情報銀行が対象とする個人が未成年者等の制限行為能力者である場合には、契約の締結と、情報銀行との間の同意等の手続きについては、それぞれ法令に照らし、適切な者が行う必要がある。
  - ✓　①の同意については、個人情報保護法上の「本人の同意」として同意を得るべき者が行う。
  - ✓　②の契約については、制限行為能力者に関する法律の規定に従い、同意権者の同意に基づいて本人が契約を締結することや、法定代理人が本人に代わって契約を締結することが必要となる。

■ 個人情報保護法との関係（①）

- 個人情報保護法においては、利用目的（16条1項、2項、3項2号-4号）、要配慮個人情報の取得（17条2項）、第三者提供（23条1項、24条）において、「本人の同意」に関する規定が存在する。
- 「本人の同意」については、「個人情報の取扱いに関して同意したことによって生ずる結果について、未成年者、成年被後見人、被保佐人及び被補助人が判断できる能力を有していないなどの場合は、親権者や法定代理人等から同意を得る必要がある」とされている。（「個人情報の保護に関する法律についてのガイドライン（通則編）」より。）未成年者については、個別の事案ごとに判断されるべきであるが、個人情報保護法上、本人が判断できる能力を有していると認められる場合がある。
- なお、開示等の請求（32条1項）は、「未成年者又は成年被後見人の法定代理人」によってすることができる。

【参考：　情報銀行における手続き等】
個人情報の利用／第三者提供に関する条件の指定、UIを用いたその他の手続き（同意の撤回、開示請求、履歴の閲覧）
個人情報の提供による便益の受け取り

■ 契約（民法）との関係（②）

- 認定指針においては、個人と情報銀行の間で契約を締結することが前提となっている。
- 未成年者等の制限行為能力者は、法律の規定に従い、同意権者の同意に基づいて本人が契約を締結したり、法定代理人が本人に代わって契約を締結したりすることが必要となる。

【参考：　情報銀行における手続き等】
情報銀行／個人間の契約の締結

1－④　情報銀行における個人情報の加工

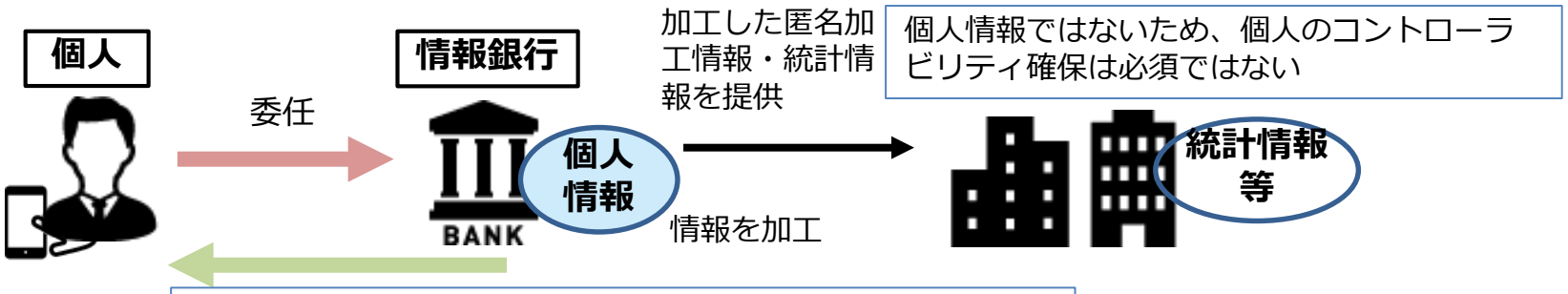
指針に追記

- 認定指針では、個人情報保護法の遵守や、個人のコントローラビリティ確保の観点から、情報銀行における個人情報の取扱いについて、認定基準の中で取扱いの条件を定めている。

（個人情報の取扱いの条件の例）
・個人情報の取扱い（第三者提供、利用目的に係る判断基準等）を個人に示し、適切な同意取得を行うこと
・提供先からの再提供を禁止するとともに、提供先での利用目的を適切に制限すること
・個人情報提供の条件の選択・変更、トレーサビリティ、同意の撤回、開示の請求についての機能が提供されること

- 情報銀行において、個人から取扱いを委任された個人情報を、統計データや匿名加工情報に加工した場合には、当該データは個人情報の取扱いに関する条件の対象外である。（情報銀行において個人情報の加工を行った場合でも、当該データが個人情報にあたる場合は条件の対象となる。）
- 情報銀行が個人情報を匿名加工情報や統計情報として加工し、当該データを他者に提供することについては、個人情報保護法上の利用目的の特定や第三者提供に係る規定は適用されず、認定指針においてもこのことについて個人から事前に同意を得ることは必須ではないが、個人情報の提供による便益を個人が受け取るという情報銀行の考え方を踏まえると、加工して提供するという旨やこれによる個人の便益について、個人に対して明らかにすることが必要である。
- なお、提供先における、情報銀行から提供された個人情報の取扱い（加工を含む）については、（個人からの委任の範囲内で）提供先と情報銀行との間のデータの取扱い条件の中で取り決める必要があると考えられる。提供先において個人情報を他の個人情報と合わせて加工する場合を含め、提供先における個人情報の利用目的について個人から同意を得ることが認定指針で求められる。

■ **情報銀行において加工した統計情報、匿名加工情報の扱い**



1－⑤　行政機関／独立行政法人等の認定について

指針に追記

- 指針ver1.0では、個人情報の保護に関する法律の適用される者が情報銀行として認定を受けることが想定されているが、行政機関の保有する個人情報の保護に関する法律、独立行政法人の保有する個人情報の保護に関する法律または各地方自治体の制定する個人情報保護条例の対象となる者が事業に関わる場合もあると考えられる。
- 指針ver1.0では、本人同意の取得等に関し「個人情報保護法に基づき」行うものと記載しているが、個人情報の利用や第三者提供に関する本人同意の取得に関してはそれぞれの法令で規定されており、他の法令が適用される者が情報銀行の認定を申請する場合には、当該法律または条例を踏まえ適切に読み替える必要がある。
- なお、当然ながら、指針に定める要件の他にも、それぞれの主体において適用される法令を遵守する必要がある。

■ 第三者提供に関する本人の同意等に関連する条文

- 個人から「個人情報の管理及び第三者提供」について委任を受けることを事業の基本とする情報銀行においては、個人情報の第三者提供や提供先での利用目的について、個人の同意を得ることが必要となっている。民間企業、行政機関、独立行政法人いずれについても、法令により、利用目的の変更や提供について本人の同意を得ることが必要とされている。

	行政機関 〇行政機関の保有する個人情報の保護に関する法律（平成15年法律第58号）	独立行政法人 〇独立行政法人等の保有する個人情報の保護に関する法律（平成15年法律第59号）	民間企業 〇個人情報の保護に関する法律（平成15年法律第57号）
利用目的及び第三者提供の制限	（利用及び提供の制限） 第8条　行政機関の長は、法令に基づく場合を除き、利用目的以外の目的のために保有個人情報を自ら利用し、又は提供してはならない。 2　前項の規定にかかわらず、行政機関の長は、次の各号のいずれかに該当すると認めるときは、利用目的以外の目的のために保有個人情報を自ら利用し、又は提供することができる。（略） 一　本人の同意があるとき、又は本人に提供するとき。 二～四　（略）	（利用及び提供の制限） 第9条　独立行政法人等は、法令に基づく場合を除き、利用目的以外の目的のために保有個人情報を自ら利用し、又は提供してはならない。 2　前項の規定にかかわらず、独立行政法人等は、次の各号のいずれかに該当すると認めるときは、利用目的以外の目的のために保有個人情報を自ら利用し、又は提供することができる。（略） 一　本人の同意があるとき、又は本人に提供するとき。 二～四　（略）	（利用目的による制限） 第16条　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、前条の規定により特定された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。 2･3　（略） （第三者提供の制限） 第23条　個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。 一～四　（略）

- なお、利用目的や第三者への提供について同意が必要な場合の例外については各法令において差異があるが、情報銀行事業においては指針に従い、個人に対して必要な事項を明確にし、同意を取得する必要がある。

1－⑥　複数者が共同で情報銀行事業を行う場合の認定

指針に追記

- 指針ver1.0では、情報銀行は単独の事業者が運営することを前提としているが、検討会で報告された情報銀行の実証事業では、複数者が共同で情報銀行を運営する例もあった。今後、情報銀行の運営形態が多様化し、複数者が共同で事業を行い、認定を申請することも想定される。
- 認定指針においては認定の申請を事業者単位／事業単位いずれでも受け付けることとされており、事業単位の申請については、複数者が共同で行う事業を認定することも想定されるべきである。この場合、複数者の間で役割分担を合理的に定め、全ての認定要件を満たすことが必要であるとともに、利用者に対する説明・損害賠償の責任は、全ての者が連帯して負うべきである。
- また、複数者が共同で事業を行う場合には、複数者のうちどの者が個人情報を取り扱うのかについて明確にする必要がある。
- なお、将来的には、認定団体において認定要件を満たすために必要な一部の機能の提供について独自に審査するなど、認定の取得を促進するような取組みを行うことも考えられる。

■ 参考：認定基準と事業／事業者との関係

複数者が共同で事業を行う場合、認定要件の考え方によって、情報銀行としてどのように満たすべきかは異なると考えられる。

（例）

- ✓ 事業者の適格性に関する要件　→　原則として全ての者が満たす必要
- ✓ 情報セキュリティ等に関する要件　→　個人情報を実際に取り扱う者が満たす必要
- ✓ ガバナンス体制　→　事業として満たす必要（基本理念については、原則として全ての者が満たす必要）
- ✓ 事業内容　→　事業として満たす必要（個人情報の取扱いに関しては、要件を満たす者を明確にする必要）

■ 個人情報を取り扱う者の明確化の必要性

- 複数者が共同で情報銀行事業を行う場合、個人情報を取得する者及び個人情報を取り扱う者を明確にする必要がある。
- 複数者が個人情報を取り扱う者となる場合は、複数者が共同して取得する場合及び、一部の者のみが取得する場合がある。
- 共同で事業を行う個人情報取扱事業者の間で個人情報の授受（共同して取得した者の間の授受または取得した者から他の者への受け渡し）がある場合には、個人情報保護法上の共同利用として整理することも考えられる。この場合、当然ながら、共同利用に関し法律上求められる事項について、情報銀行は適切に対応することが必要である。

1－⑦　提供先第三者の選定

指針に追記

- 指針ver1.0では、情報銀行は個人情報を提供する提供先第三者に対して、「情報銀行と同様、認定基準に準じた扱い」を求めることとされている。認定基準では、個人情報を安心して預けられるかという観点から、セキュリティ基準やガバナンス体制等に関し情報銀行に一定の水準を求めており、提供先にも同様の扱いを求めることで、情報銀行を利用する個人の安心を確保することとしている。
- 提供先がPマークまたはISMS認証を取得していない場合は、情報銀行が当該提供先におけるデータの安全性を確保するための具体的な対策を講じ、提供先における体制と合わせて総合的に「認定基準に準じた扱い」を実現することも考えられる。
- 提供先第三者の選定に関し、認定の具体的な考え方については以下のとおりである。

■ 認定の具体的な考え方

認定指針

［指針ver1.0の認定基準における記載］
・情報提供先にも、情報銀行と同様、認定基準に準じた扱い（セキュリティ基準、ガバナンス体制、事業内容等）を求めること
・個人情報の第三者提供を行う場合の提供先第三者及び利用目的に関する適切な判断基準（認定基準に準じて判断）の設定・明示

- 情報銀行は、個人情報の第三者提供にあたり、個人が予め同意した条件の下で提供の可否について一定の判断を行う。このため、まず、情報銀行は適切な判断基準を設定することが求められる。
- 個人が安心して利用できる情報銀行を認定するという観点から、この判断基準において、情報銀行は提供先にも「認定基準に準じた扱い」を求めることが求められている。
- 提供先がPマークまたはISMS認証を取得していない場合、提供先における「認定基準に準じた扱い」の確保について、次のとおり指針に限定的に補足を記載する。

指針の補足

情報銀行は、提供先がPマークまたはISMS認証を取得していない場合であっても、
- 情報は情報銀行が管理し、提供先は決められた方法で、必要な情報の閲覧のみができることとする
- 提供先において特定の個人を識別できないよう、個人情報の暗号化処理または個人情報の一部の置き換え等の処理を行い、復元に必要な情報を除いた形で提供先に提供する
- 情報銀行の監督下で、提供先からPマークまたはISMS認証を取得している者に個人情報の取扱いを全て委託させる

のいずれかの対策を講じた上で、それぞれのケースにおいて求められる情報セキュリティ・プライバシーに関する具体的基準を提供先が遵守していると認められる場合には、「認定基準に準じた扱い」であるとすることができる。

1－⑦　提供先第三者の選定

情報銀行

判断基準の作成

- 認定指針に従い、個々の情報銀行において、提供先第三者を選定するための判断基準を設定する。同基準の中で、「情報銀行と同様、認定基準に準じた扱い」をどのように確保するのかについて定める必要がある。
- 提供先がPマークまたはISMS認証を取得しておらず、指針の補足にある具体的な対策を講ずる場合には、情報銀行は、これによって「認定基準に準じた扱い」が実現することの説明を認定の申請にあたり明確にすることが必要である。

認定団体

認定

- 認定団体は、認定にあたり、個々の情報銀行において設定した判断基準及びこれに基づく選定体制について、提供先における「認定基準に準じた扱い」の確保を満たすものであるか審査する。（※判断基準等の適切性を審査するものであり、個々の提供先の選定自体を審査するものではない。）
- 提供先がPマークまたはISMS認証を取得しておらず、情報銀行が指針の補足にある具体的な対策を講ずることによって「認定基準に準じた扱い」であるとする場合には、認定団体は、その適切性についても確認することが必要である。

情報銀行

認定後の運用

- 提供先第三者を選定するための判断基準及び判断プロセスは、個人に対しわかりやすく示すことが求められる。この際、提供先がPマークまたはISMS認証を取得しておらず、指針の補足にある具体的な対策を講ずる場合には、情報銀行は、このことを個人に対しても明らかにする必要がある。
- 個々の提供先第三者の選定の可否については判断基準に基づき情報銀行が判断し、加えて当該判断基準及び選定のプロセスや結果が適切であるかについては、データ倫理審査会においても審議することとなる。

1－⑧　認定の対象とする個人情報の範囲

指針に追記

- 指針ver1.0では、「要配慮個人情報、クレジットカード番号、銀行口座番号」に関する個人情報を認定の対象外としている。
- このうち、要配慮個人情報については、引き続き対象外として、継続検討とした。
- クレジットカード番号及び銀行口座番号に関する個人情報については、情報銀行を利用する個人と提供先との間で費用や対価の支払いが発生する場合に、個人から情報銀行に委任する情報として第三者提供を行うニーズがあることから、対象に追加することとする。
- なお、クレジットカード番号を保有する場合は業界ルール（PCI DSS）が存在し、クレジットカードの加盟店においてもクレジットカード番号の非保持化が求められるなど、適切な取扱いが求められることから、情報銀行においても当然これらを遵守する必要がある。

■ **指針ver1.0で認定対象外となっており、認定対象に追加するもの**

	概要	考え方の整理
クレジットカード番号に関する個人情報	・加盟店においてはクレジットカード番号の非保持化またはPCI DSS準拠が求められている ・流出により、不正利用の恐れ	・個人が提供先第三者から受けたサービスに対し支払を行う際に、支払情報としてクレジットカード番号を使用する可能性があるとの意見があったことから、認定の対象に追加する
銀行口座番号に関する個人情報	・個人と銀行口座を結びつける情報 ・銀行口座番号のみでは、当該口座からの振り込みはできない	・提供先第三者が個人情報を提供した個人に対して対価を渡す際に、支払情報として銀行口座番号を使用する可能性があるとの意見があったことから、認定の対象に追加する

■ **指針ver1.0で認定対象外となっており、今後の取扱いは継続検討とするもの**

	概要	考え方の整理
要配慮個人情報	・個人情報保護法において定義 　－本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報	・健康・医療分野の要配慮個人情報を取り扱う「情報銀行」を認定することについて健康・医療データWGで検討した結果、賛否両論の様々な意見が寄せられ、引き続き展開を注視していくこととされた（※） ・教育分野における個人情報の取り扱いについても、今後、情報銀行の仕組みを活用したいとの要望があったことから、情報銀行を活用するにあたっての要配慮個人情報の取り扱いについて、ニーズの具体化を踏まえた対応を行う方向で引き続き検討する

（※）第10回検討会資料10-2「健康・医療データWG報告」（平成31年3月15日）参照

2. 個人による情報銀行の選択等

【検討会での議論及び基本的な考え方】

- 情報銀行は、個人情報に対する個人のコントローラビリティを高めることを基本的な考え方としており、情報銀行はデータを個人のために活用し、個人にとって信頼できる存在であることが期待される。
- 情報銀行は、例えば「信託」のようなかたちで個人にとっての利益を最大化するとともに、情報提供元・情報提供先等他の関係者の利益についても考慮する場合がある。情報銀行が事業を行う場合には、個人に対し、提供する機能や第三者提供によるメリットなど一定の条件を示して契約を結ぶことで、個人にとってメリットを担保する。
- こうしたことを踏まえ、個人が情報銀行を比較し、より条件のよい情報銀行を選択することが可能となるよう、情報銀行に関する必要な情報について透明性を高めることが必要との意見があった。
- また、各情報銀行が設置するデータ倫理審査委員会についても、個人のコントローラビリティを高めるという観点から重要であり、その役割の明確化が必要であるとの意見があった。

■ 個人が情報銀行を選択する際のポイント

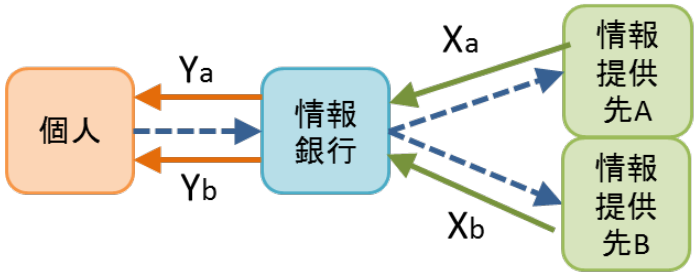
情報銀行を選択する際のポイント	認定基準における位置づけ
1）事業内容について ・個人にとってどのような便益／リスクがあるか	※情報銀行から個人に説明する
2）情報銀行の業務能力、セキュリティ	※認定により一定水準を担保
3）委任する個人情報についての条件（第三者提供の判断基準） ・個人情報の範囲 ・個人情報の提供先 ・個人情報の利用目的 ・第三者提供によるリスク・便益	※適切なUIにより個人に対し第三者提供に関する選択肢を提示する ※提供先のセキュリティ水準等については、認定により一定水準を担保 ※個人にとって不利益の生じる利用がなされないよう、データ倫理審査会において審査
4）コントローラビリティの機能の有無 ・個人情報の提供についてどこまで細かく指定できるか ・どこまで細かく履歴をトレースできるか ・一度提供されたデータの利用を停止できるか ・情報銀行から他にデータを移せるか	※どのような機能を提供するかについて、情報銀行から個人に対し条件を明示
5）その他の条件 ・事業終了時、契約終了時の対応 ・相談窓口	※契約書に記載 ※適切な相談窓口の設置について、認定により担保

2－①　個人情報提供の対価

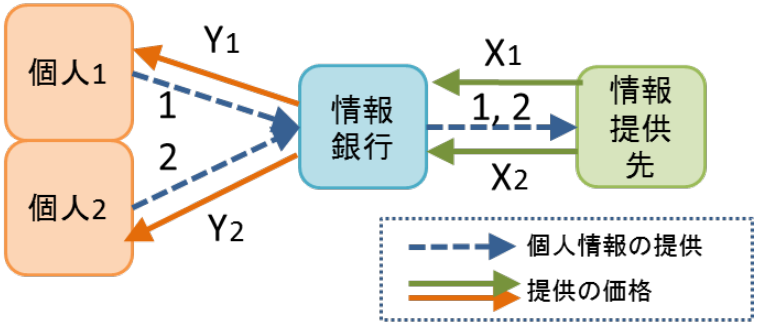
- 情報銀行は、個人情報を提供先第三者に提供することが事業の核となっており、これにより個人に何らかの便益が提供される。事業の形態によっては、情報銀行と提供先及び個人との間で個人情報提供の対価の授受が発生することも考えられる。
- 個人情報提供の対価設定に決まった方法はなく、個人情報の紐付く個人によって、或いは個人情報が提供される提供先によって、この個人情報提供の対価が異なるものになることもあり得る。
- 情報銀行は営利事業として運営されることが多いと想定されることから、個人情報提供の対価は、基本的に情報銀行において自由に設定されるものと考えられる。
- この場合、各情報銀行において、責任をもって、一定の考え方のもと、対価設定を行うべきである。例えばフリークエントユーザーを優遇することや、キャンペーンによる時期によって対価を変えるなど、条件の変化に応じた顧客による対応の差別化はあり得るが、合理的な理由付けができる範囲において行われるべきである。
- また、個人情報の提供により個人が便益を得るという情報銀行の目的に照らし、個人がより条件のよい情報銀行を選択できるよう、対価の設定についての必要な情報が利用者及び利用者となる可能性のある個人に対して開示されることが必要である。

■ 関係者間で生じうる対価設定の違い

【ケース1】
同じ個人の情報を提供する場合でも、提供先（A、B）によって対価（Xa、Xb）が異なる場合。



【ケース2】
同じ提供先に情報を提供する場合でも、情報の属する個人（1,2）によって提供先における対価（X1、X2）が異なる場合。



2－②．情報銀行に関する透明性の確保

指針に追記

- 情報銀行事業の健全な発展のためには、透明性の確保が重要であり、指針ver1.0では、情報銀行サービスの利用者である個人による自身に関する情報に対するコントローラビリティの確保、及び、情報銀行のガバナンスを確保するための事業報告という観点から、明示／公表の必要な内容について定めている。
- 情報銀行サービスの利用者である個人に伝えるべきものとして、提供先第三者や利用目的の内容に応じたリスクについて追加する。今後の事例の積み重ねにより、将来的には、明示が必要なリスクを類型化していくことも考えられる。
- これらに加えて、個人が自身にとってよりメリットのある情報銀行を選択することができるようにするため、一定の情報公開が必要と考えられる。このため、個人の受ける便益の考え方、他の情報銀行や事業者にデータを移転する機能の有無等、個人による情報銀行の選択に資する内容を、利用者となる可能性のある個人に対して公表することを、認定要件に追加する。
- さらに、認定団体において、認定した情報銀行について、個人にとってのメリットやリスクを整理して公表することにより、個人の注意を促し、適切な選択を後押しすることも考えられる。

	考え方	認定指針における記述（案） ※赤字部分を追加
個人（利用者）への明示	個人（利用者）が自身に関する情報に対してコントローラビリティを確保するために必要な情報	・提供先第三者、利用目的、契約約款に関する重要事項の変更などを個人にわかりやすく開示できる体制が整っていること ・個人のコントローラビリティを確保するための機能の提供について（※個人が自身に関する情報に対してコントローラビリティを確保するための各種機能の有無について） ・提供先第三者や利用目的に応じたリスク（注意点）
定期的な事業報告の（一般への）公表	個人（利用者）、取引事業者を含めた、関係者によるガバナンスの確保	・透明性を確保（事業に関する定期的な報告の公表など）すること
利用者となる可能性のある個人への公表	利用者となる可能性のある個人が自身にとってよりメリットのある情報銀行を選択するために必要な情報	・個人による情報銀行の選択に資する情報（当該情報銀行による個人への便益の考え方、他の情報銀行や事業者にデータを移転する機能の有無など）を公表すること

2－③. データ倫理審査会

指針に追記

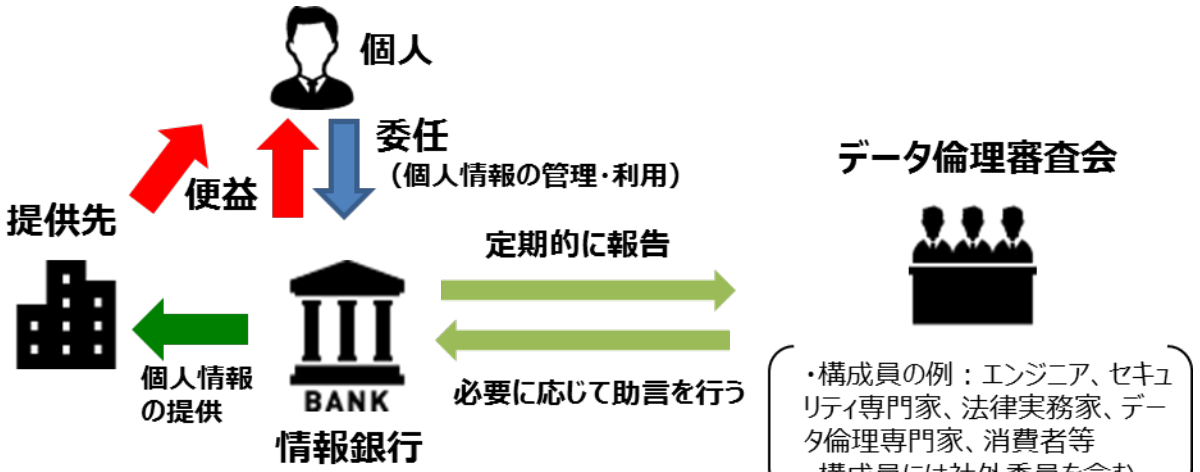
- 情報銀行は、個人情報に対する個人によるコントローラビリティを高めることを基本的な目的としており、これを適切に担保するには、各情報銀行に設置される諮問体制であるデータ倫理審査会の役割が重要となる。
- データ倫理審査会は各情報銀行で個別に組織するものであるが、それぞれが適切に機能するには、データ倫理審査会の役割について一定の共通認識が持たれることが望ましい。データ倫理審査会において審議するべき基本的な内容等については以下のとおりである。なお、運営の適切性を担保するため、構成員及び（必要な範囲の）議事録は公表されるべきである。
- これに加えて、認定団体等において、このような共通認識の醸成を行い、個人のコントローラビリティを適切に担保するため、データ倫理審査会の構成員に対する研修等の啓発活動を行うことも考えられる。

■ データ倫理審査会における審議の考え方

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

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

（例）・個人によるコントローラビリティを確保するための機能が誤解のないUIで提供されているか
・個人の同意している提供先の条件について、個人の予測できる範囲内で解釈されて運用されているか
・個人にとって不利益となる利用がされていないか／個人に対し個人情報の利用によるリスクが伝えられているか
・個人にとって高いリスクを発生させる恐れがある場合には、GDPRで義務づけられているDPIA（データ保護影響評価）を参考にすることも考えられる



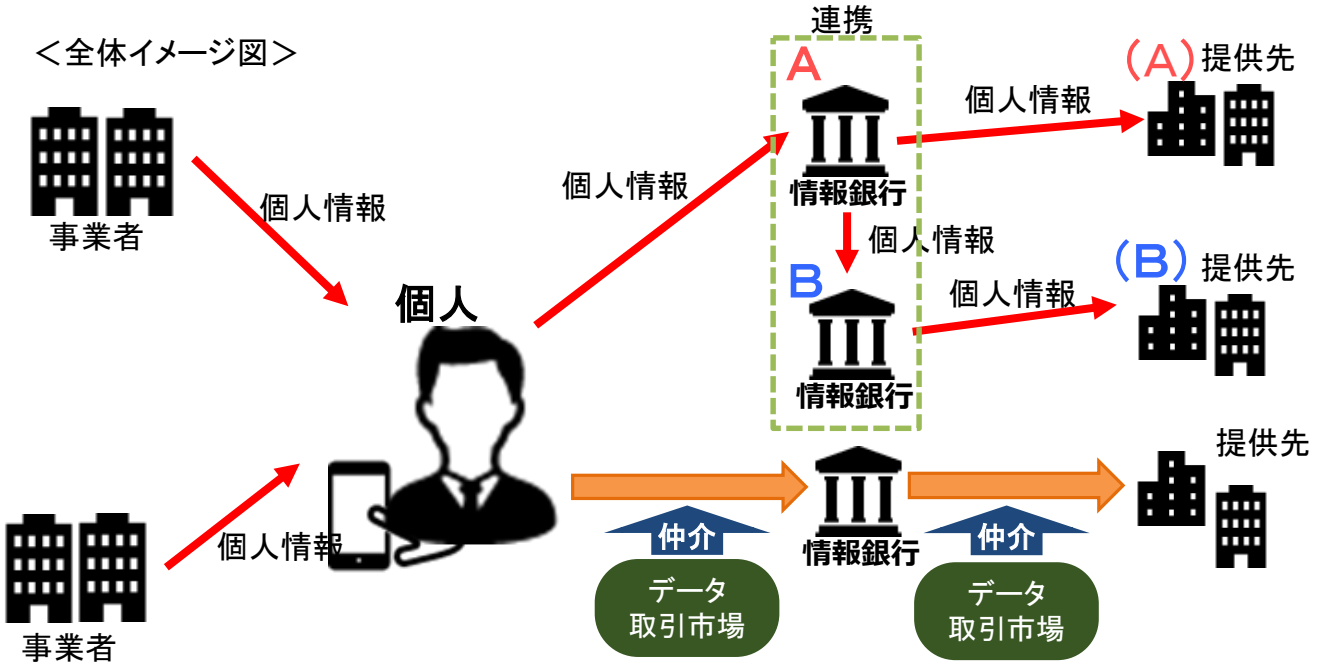
●情報銀行事業について、以下の事項についてその適切性を審議し、必要に応じて助言を行う
- ・個人と情報銀行の間の契約の内容
- ・情報銀行の委任した個人情報の利用目的
- ・個人による情報銀行に委任した個人情報の第三者提供に係る条件の指定及び変更の方法（UI）
- ・提供先第三者の選定方法
- ・委任を受けた個人情報の提供の判断

●運営方法
- ・構成員及び（必要な範囲の）議事録は公開する
- ・必要に応じ情報銀行に調査・報告を求めることができる

3. プレイヤー間の連携

【検討会での議論及び基本的な考え方】

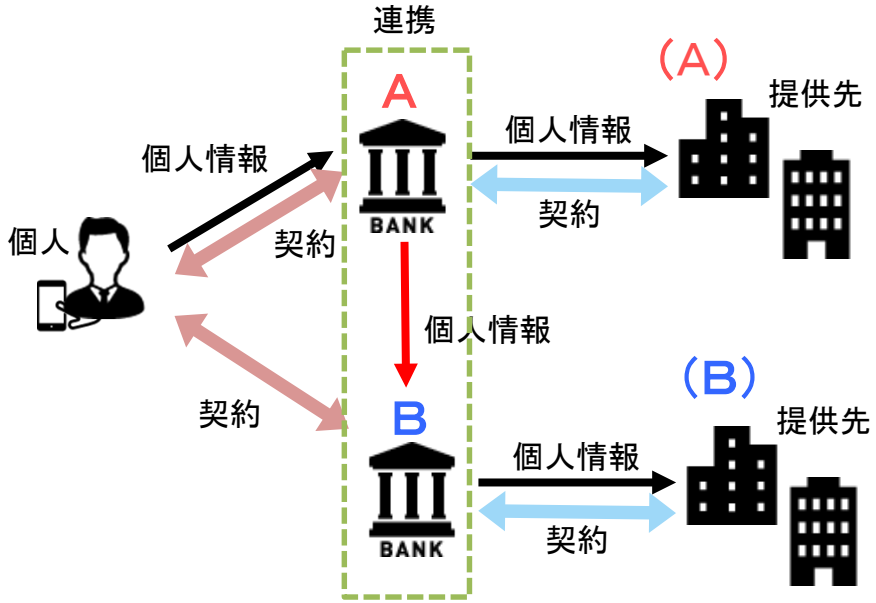
- 情報銀行に関する議論の出発点である、データ流通の促進という観点からは、情報銀行と、情報提供元及び情報提供先、さらには他の情報銀行やデータ取引市場等他のプレイヤーとの間の円滑なデータ流通が望まれるとの意見があった。
- また、例えば金融分野では個人の銀行口座残高や利用履歴等の情報を銀行から取得する電子決済代行業に関して法整備が行われるなど、個人の情報を取得・集計して活用するようなサービスが今後増えることが考えられることから、情報銀行から提供を受けた個人情報をさらに他の事業者に提供して活用する場合の考え方についても明確にするべきとの意見があった。
- このため、今後情報銀行の普及が更に進んだ場合における、情報銀行間の連携、情報銀行とデータ取引市場との連携、情報銀行からの直接の提供先からの二次提供について、認定指針に照らした考え方の整理を行った。
- なお、プレイヤー間の連携を進めるにあたっては、引き続き、個人によるコントローラビリティを確保した流通の実現に留意することが必要である。
- また、他の分野を含めてデータポータビリティに関する議論が行われており、情報銀行においてもこうした動きに留意し、データポータビリティについても尊重していくことが必要である。



3－①　情報銀行間の連携

- 情報銀行が複数存在し、それぞれが別々の情報提供先と連携している場合、個人が複数の情報銀行を通じて個人情報の提供を行うことにより、より多くの提供先に個人情報が提供され、便益を得る機会が増えることも期待される。
- さらに、情報銀行間でデータを移転する機能が確保される場合や、情報銀行間の連携が進んだ場合、個人はより簡易に複数の情報銀行を利用することで、データを個人のコントローラビリティの下におきつつ、個人にとっての利便性が高まることも期待される。
- 今後、情報銀行の普及が更に進んだ場合には、こうした情報銀行の連携が期待されるところであり、特に、情報銀行間のデータの移行に関する「プラットフォーム」の検討や、データ形式や伝送方式の標準化についても、国や認定団体などにおいて取り組むことが期待される。

■ 情報銀行間の連携イメージ

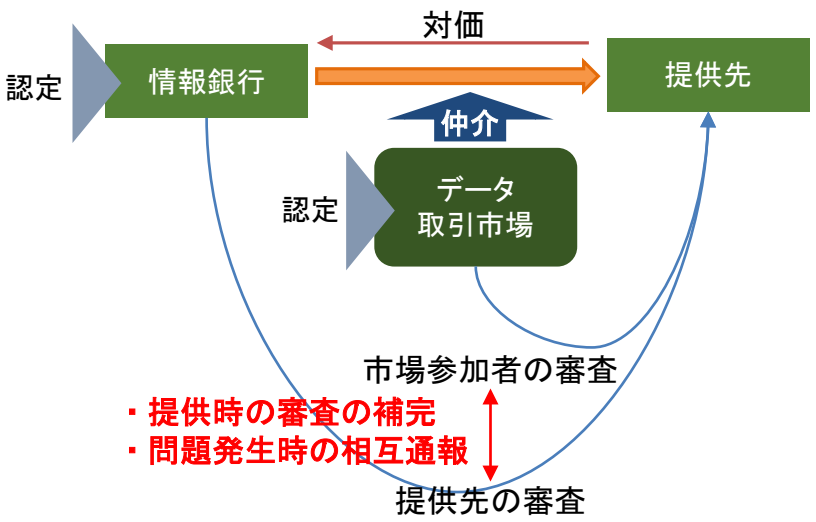


情報銀行Aが個人と情報銀行Bの契約を代行して個人の負担を減らすなど、
個人にとって利便性の高い形での連携が進むことが期待される。

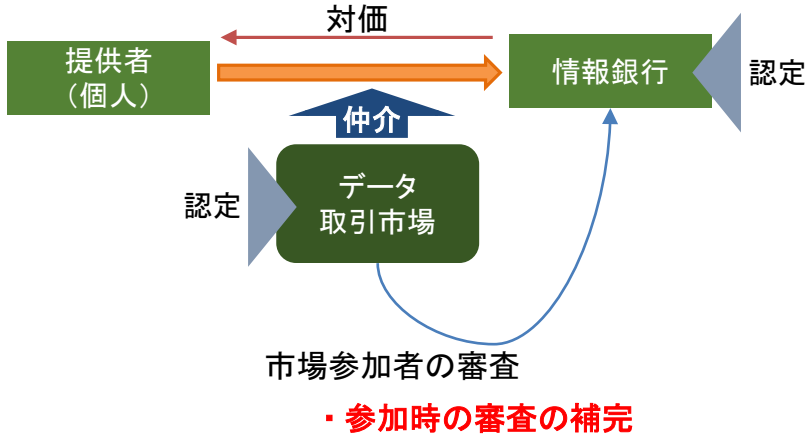
3－②　情報銀行とデータ取引市場の連携

- データ取引市場は、「データ保有者と当該データの活用を希望する者を仲介し、売買等による取引を可能とする仕組み（市場）」で、情報銀行がデータ取引市場に参加し、情報提供元又は情報提供先となる事業者との仲介を受けることも考えられる。この場合に、情報銀行とデータ取引市場が連携することで、データの流通が進むことが期待される。
- 認定指針では、情報銀行は提供先第三者に対し、セキュリティ基準・ガバナンス体制・事業内容等について、認定基準に準じた扱いを求めることとされている一方、データ取引市場においても、市場参加者に一定の参加要件を求めている。このため、情報銀行とデータ取引市場が提供先第三者に共通して求める要件については、一方の審査において当該要件を満たしている場合にはそれをもってもう一方の審査を満たしていることとして審査内容の一部を補完することが考えられる。加えて、このような連携が行われた場合、提供先において問題が発生した際に相互に通報するなどにより、ガバナンスを高めることも考えられる。
- また、認定を受けた情報銀行は一定の要件を満たすことを認定団体により確認を受けていることから、情報銀行がデータ取引市場に参加するにあたり、データ取引市場による市場参加者の審査の一部を補完することも考えられる。
- データ取引市場についても、一定の水準を満たしたものについて民間団体による認定が予定されていることから、認定を受けた情報銀行とデータ取引市場との間で連携が行われることにより、情報銀行によるデータ取引市場を介したデータの流通がより活発となり、データの利活用が更に進展することが期待される。

■ 情報銀行事業者がデータ取引市場運営事業者を介してデータを提供するケース



■ 情報銀行事業者がデータ取引市場運営事業者を介して個人から情報を収集するケース



3－③　提供先第三者からの「再提供」禁止に関する考え方

指針に追記

- 指針ver1.0においては、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、情報銀行は提供先第三者に対し、当該第三者に提供される個人情報の再提供を禁止することとされている。
- 他方で、情報銀行の提供先第三者から別の第三者への上記個人情報の提供については「再提供」にあたらなければ禁止されない。再提供にあたらないケースを以下①～③のとおり明確化する。
- また、プレイヤー間の円滑なデータ流通を促進していくに当たっては、情報の再提供を行うニーズも想定されることから、提供先第三者からの再提供について、一定の条件を満たした場合にのみ限定的に認めることとし、以下④のとおり条件を定める。
- 一方、①～④のいずれにも当てはまらない場合は、本指針においては禁止されることとなる。

［指針ver1.0の認定基準における記載］
・個人情報の第三者提供を行う場合、当該提供先からの個人情報の再提供の禁止

【考え方】指針ver1.0では、以下のことを確保するため、再提供を認めないこととしている。

（A）個人のコントローラビリティ確保のため、提供先第三者及び利用目的に関し、個人の同意が適切に取得されること

（B）情報銀行が提供先第三者での個人情報の適切な取扱いについて監督し、提供先第三者における問題発生時の責任も負うこと

3－③　提供先第三者からの「再提供」禁止に関する考え方

■ 再提供にあたらないケース

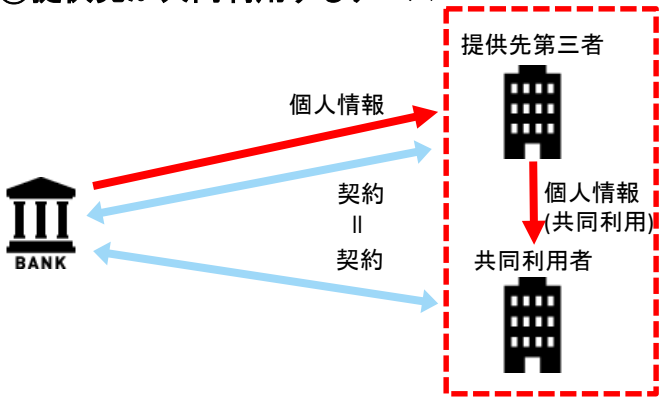
①提供先第三者において個人情報ではないデータに加工するケース

- 提供先第三者において個人情報を統計情報等個人情報ではないデータに加工し、別の第三者に提供することは、個人情報保護法において制限されない。
- ただし、情報銀行の理念を踏まえ、【考え方】(A)を満たすため、加工して利用することについて、予め利用目的として本人に示すことが必要。

②個人情報の取扱いを委託するケース

- 提供先第三者から委託に伴って提供する場合は、個人情報保護法において本人の同意が必要となる「第三者への提供」にあたらない。
- 提供先第三者と委託先の間には業務委託契約が締結され、(A)及び(B)については満たされると考えられる。

③提供先が共同利用するケース



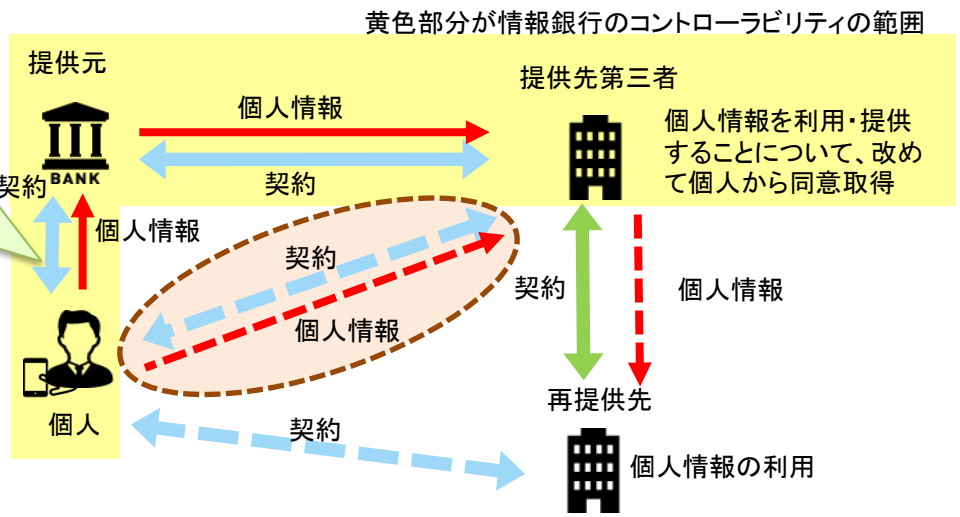
- 共同利用にともなって個人情報が提供される場合は、個人情報保護法において本人の同意が必要となる「第三者への提供」にあたらない。
- この場合、【考え方】(A)を満たすため、共同利用が行われる事業者の範囲について、個人が正しく把握できるようにした形で、提供先の条件について個人に提示する必要がある。
- また、【考え方】(B)を満たすため、情報銀行が共同利用を行う全ての事業者と契約することが必要である。

3－③　提供先第三者からの「再提供」禁止に関する考え方

■④「再提供」が一定の条件により認められるケース

・再提供先における個人情報の取扱いが、提供元（情報銀行）を介した個人のコントローラビリティの範囲外であるところ、個人情報の提供先第三者から再提供先へ当該個人情報の第三者提供を行うこと及び当該再提供先（業種や事業分類でも可）について、予め情報銀行のUIの中（※）で個人に明示すること。
例）決済代行業者Aから、委託・共同利用に該当しない外部の〇〇サービス事業者に提供　等

※　再提供についてはデフォルトオフだが、上記のような個人情報の流れを明示し、これについて利用者がオンにするようなＵＩを備える等



情報銀行は、個人起点のデータ利活用を推進するために、個人が信頼できる情報銀行に個人情報の取り扱いを委任することで、個人の情報に対するコントローラビリティを高めることを目的とするものであることから、情報銀行から個人情報を提供された第三者による当該情報の再提供は禁止される（情報銀行は、個人の同意があっても、再提供を行う事業者に個人情報を提供してはならない）のが原則である。ただし、次のような条件を満たす場合には、個人のコントローラビリティが確保され、情報信託機能の認定制度の趣旨を損なうものではないものとして、例外的に提供先第三者による再提供を認める（情報銀行は、以下の条件を満たす場合に限り、再提供を行う第三者に対して個人情報を提供することができる）ものとする。

- 提供元（情報銀行）は、提供先第三者との契約の中で、再提供について以下の条件を求めること。

（1）提供先第三者は、再提供先への提供について、再提供先の業種や事業分類（または個社名）と、その利用目的、提供する個人情報の項目、再提供先に対する個人情報の開示等の請求等の窓口を提供元（情報銀行）に報告すること

（2）個人と提供先第三者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、個人情報保護法第23条第1項に基づき、提供先第三者が個人から同意取得すること

（3）再提供先からの更なる第三者提供は認められないこと

- 再提供先における個人情報の取扱いが、提供元（情報銀行）を介した個人のコントローラビリティの範囲外であるところ、提供元（情報銀行）は、個人に対して、提供先第三者から再提供先へ当該個人情報の第三者提供を行うこと及び当該再提供先（業種や事業分類でも可、例：「金融分野のアグリゲーションサービス」）を明示すること。再提供については個人により選択可能とし、かつデフォルトオフにすることが望ましい。個人が提供元（情報銀行）側のUIで再提供を可とする場合、個々の再提供先への提供については、提供元（情報銀行）が個人から同意を取得する必要はない。
- 再提供の必要性、すなわち、個人が提供先第三者及び再提供先のサービスを利用すること及び提供先第三者において情報銀行から受け取った個人情報について付加や加工をすることにより再提供先のサービスが可能・有効となるものであることを前提とする。（例：金融分野のアグリゲーションサービス等）

※　認定団体は、提供先第三者の基準が実質的に遵守されるよう（再提供先のセキュリティ、プライバシーに係る体制を確認する等）確認することが望ましい。

3－③　提供先第三者からの「再提供」禁止に関する考え方

■ ①～④に該当せず禁止されるケース

⑤　①～④に当てはまらないケース

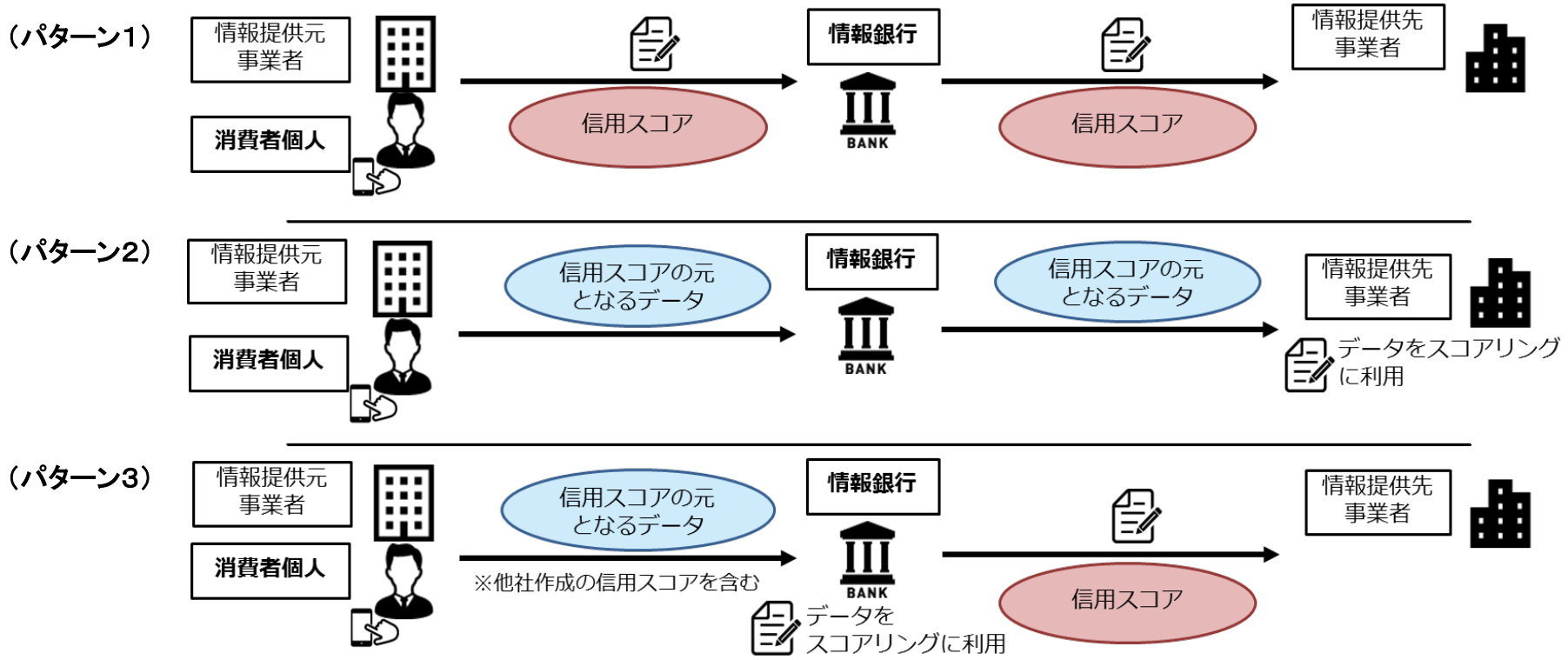
- このケースでは、個人のコントローラビリティが十分に確保されていない。

例：個人に再提供先が明示されず、再提供先において個人の意図しない利用がなされている場合

4.「信用スコア」の取扱い

- 情報銀行の普及が進めば、個人に関する様々なデータの収集が進み、いわゆる「信用スコア」の作成や流通が促進される可能性がある。
- 「信用スコア」については明確な定義がなく、個人に一定のスコアを付与するものでは、例えば与信能力に関する評価や、英語の試験の点数も一種のスコアといえる。こうした広義のスコアは現在でも広く一般的に利用されているものであり、情報銀行を通じた流通によって利便性が向上することが期待される。
- 他方で、個人の部分的な能力等に止まらず、個人の社会的な評価に関する信用スコアについては、その利用方法如何によっては、スコアに迎合する者が増え社会の多様性が損なわれたり、結婚や就職などに利用され、人間の差別や選別につながりかねない危険も孕んでいるとの意見があった。
- こうしたことを見据え、情報銀行での活用を通じて差別に繋がりうる信用スコアの扱いについて、一定の取扱い方針を示す。

■ **情報銀行が「信用スコア」を取り扱う場合のパターン**



4.「信用スコア」の取扱い

- 情報銀行は、「個人のためにデータを活用する」ことを目的の基本としており、いわゆる「信用スコア」を扱う場合は、個人にとって不利益な利用とならないよう、留意する必要がある。
- 特に、個人の部分的な能力等に止まらず、個人の社会的な評価に関する信用スコアを想定し、情報銀行が参考にするべき留意点について以下のことが考えられる。

■ 情報銀行において「信用スコア」を取り扱う場合の留意点

① 同意取得
（パターン1及び3） 情報銀行は、個人に対し、信用スコアが提供先においてどのように利用されるのか及びそれによるリスクについて、明示的に説明すること。
（パターン2及び3） 情報銀行は、個人に対し、取得又は第三者提供される個人情報が信用スコアの算定に利用されること及びそれによるリスクについて、明示的に説明すること。

② 信用スコアの利活用
（パターン1及び3） 情報銀行は、「個人のためにデータを活用する」ことが原則となることから、提供することによって、個人にとって不利益となる恐れがある場合は提供しない、または個人に対しリスクを示すなど、個人の利益を踏まえた利活用を行うこと。

③ 非提携企業による信用スコアの二次利用
（パターン2） 情報銀行は、他者が作成したスコアを作成者又はスコアの対象となる個人から取得し、他の第三者に提供する場合で、作成者が二次利用に対し制限を設けている場合には、制限に反しない範囲で提供を行うこと。

④ 信用スコアの基礎データ
（パターン2） 情報銀行は、「個人のためにデータを活用する」ことが原則となることから、遺伝情報や、差別に繋がる過去の情報を信用スコアを算定する者に対し提供しないこと。
（パターン3） 情報銀行は、「個人のためにデータを活用する」ことが原則となることから、遺伝情報や、差別に繋がる過去の情報を基礎データとして用いないこと。

⑤ 説明責任・透明性
（パターン3） 情報銀行は、スコアに用いたデータ及びスコアの算出方法について、アカウンタビリティを持つこと。

⑥ 人間の関与
（パターン3） 信用スコアを機械化された処理により数値化する場合において、人間の関与を本人が求めることを認めるという対応を行うかについても検討すること。

5. 今後の情報銀行の展開に向けたその他の取組み

- 指針に定める一定の水準を満たす情報銀行を認定することで、認定を受けた情報銀行の選択・普及を促し、消費者が安心して利用できる情報銀行の普及が進むことが期待される。
- その他にも、今後情報銀行の普及を図っていくために、関係者において必要と考えられる取り組みやその他の論点について、以下のような意見があった。

■ 消費者への普及啓発及び支援

情報銀行が個人の豊かな生活の実現に貢献するためには、個人が自身のパーソナルデータに関与を及ぼし、リスクを適切に把握した上でデータの活用によるメリットを享受できるよう、情報銀行を通じたデータの活用に関する正しい理解が進むことが必要であり、行政、認定団体、情報銀行事業者などの関係者それぞれにおいて、普及啓発や必要な支援を行うことが期待される。

■ デジタルプラットフォーマーに関する議論との関係

「デジタル・プラットフォーマーを巡る取引環境整備に関する検討会」の下で、デジタル・プラットフォーマーにおいて集積された利用者のデータの移転・開放に関する議論も行われているところであるが、今後、安心・安全にこうした移転・開放を進めるため、情報銀行が利用者に戻されたデータを安全に受け取る主体として活用されることも期待される。

■ モデル契約約款の充実

認定指針では、認定基準を満たすとした場合に必要なモデル約款の記載事項について記載しているが、情報銀行事業の普及を見据えるとモデル契約約款はこれらに限らず盛り込むべき事項について示されることが期待され、経済産業省「AI・データの利用に関する契約ガイドライン」等関連するガイドラインを参考に、認定団体において今後さらに充実させていくことが期待される。

■ 情報銀行の国際展開

今後の情報銀行事業の拡大に向けて、関係者で協力し、情報銀行の国際展開にも取り組むことが期待される。

別添

赤字：ver1.0からの変更点

「情報信託機能の認定に係る指針ver2.0」（案）

情報信託機能の認定スキームの在り方に関する検討会

令和元年●月

1．本指針の基本的な運用について

基本的な運用について
再整理

＜本指針の位置づけ＞

・　本指針は、①認定基準・②モデル約款の記載事項・③認定スキームから構成され、認定団体は、本指針に基づき、認定制度を構築・運用する。

・　認定は任意のものであり、認定を受けることが事業を行うために必須ではない。

・　本指針に定めるもののほか、認定制度の構築・運用に必要なことは、各認定団体において決定する。

＜認定の対象＞

・　認定は、事業者単位・事業単位いずれについても行うことができる。

・　複数の法人等が共同して行う事業を事業単位で認定する場合には、責任分担を明確にするとともに、個人に対して各者が連帯して責任を負うことが求められる。

＜本指針の対象とする個人情報の範囲＞

・　本指針では、情報銀行が個人から委任を受けて管理及び第三者提供を行う個人情報として、要配慮個人情報を認定の対象としない。

（※）本指針の記載は、個人情報の保護に関する法律の適用される者の認定を想定したものとなっているが、行政機関の保有する個人情報の保護に関する法律、独立行政法人の保有する個人情報の保護に関する法律又は地方自治体の定める個人情報保護条例が適用される者が申請する場合には、個人情報保護法を引用した認定要件は、当該適用される法令を踏まえ適切に読み替える必要がある。

注）用語の定義
「本指針」・・・情報信託機能の認定に係る指針ver2.0
「認定団体」・・・本指針に基づき、情報銀行の認定を行う団体、　「認定」・・・認定団体が本指針に基づき行う情報銀行の認定

（認定基準について）

- 「認定基準」は、一定の水準を満たす「情報銀行」を民間団体等が認定するという仕組みのためのものであり、当該認定によって消費者が安心してサービスを利用するための判断基準を示すもの。レベル分けは想定しない。
- 提供する機能を消費者にわかりやすく開示するなど、消費者個人を起点としたデータの流通、消費者からの信頼性確保に主眼を置き、事業者の満たすべき一定の要件を整理。データの信頼性などビジネス上のサービス品質を担保するためのものではない。
- 今後事業化が進む分野であるため、サービスの具体的内容や手法（データフォーマット等）はできるだけ限定しない。

（モデル約款の記載事項について）

- モデル約款の記載事項は、消費者個人を起点としたサービスとして、また、個人情報の取扱いを委任するサービスとして、認定基準の目的を達成する観点から契約において最低限、定めることが必要な事項として、標準的な内容を示すもの。
- 認定基準とモデル約款は本来別物ではあるが、消費者が安心して当該サービスを利用するためのものという点で、モデル約款の内容と認定基準のうち事業内容に係る要件は多くの共通の要素を有するものとなり、認定要件に準拠する形でモデル約款の記載事項を作成。
- 本記載事項に定める事項以外にも、認定団体において、情報銀行事業の実態に応じたモデル約款を定め、データの利用に関する関連する他のガイドライン等も参考にしつつ、多様な観点から改善が検討されることが期待される。

本指針における情報銀行の定義・考え方

定義の再整理

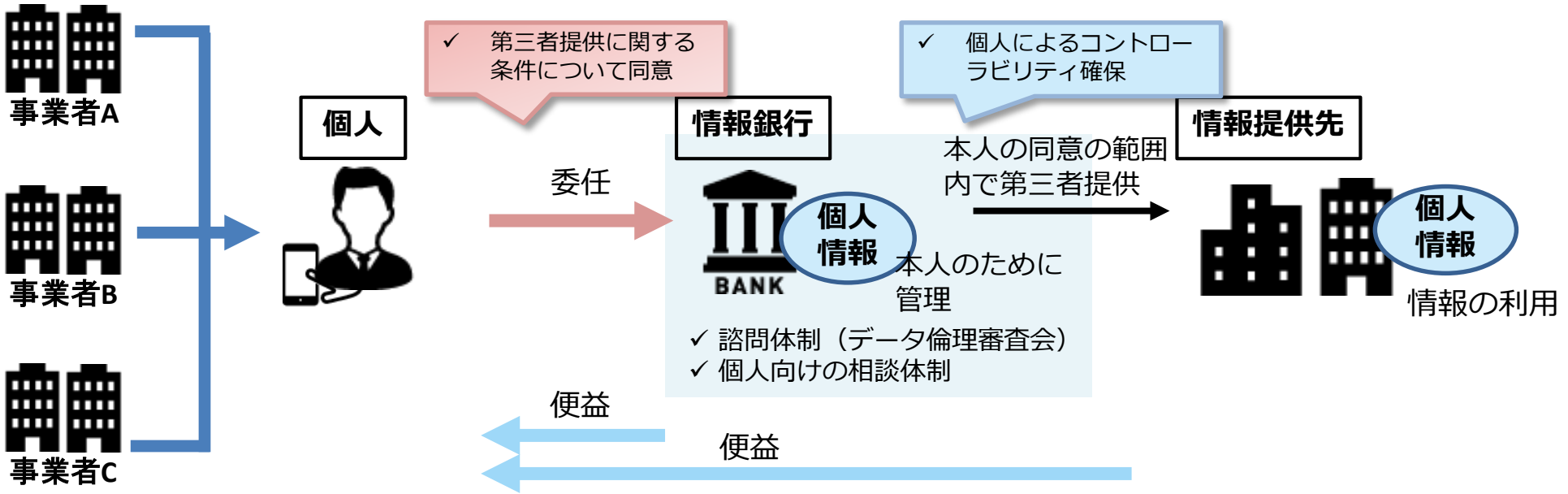
「情報銀行」は、実効的な本人関与（コントローラビリティ）を高めて、パーソナルデータの流通・活用を促進するという目的の下、本人が同意した一定の範囲において、本人が、信頼できる主体に個人情報の第三者提供を委任するというもの。

【機能】

- 「情報銀行」の機能は、個人からの委任を受けて、当該個人に関する個人情報を含むデータを管理するとともに、当該データを第三者（データを利活用する事業者）に提供することであり、個人は直接的又は間接的な便益を受け取る。
- 本人の同意は、使いやすいユーザーインタフェイスを用いて、情報銀行から提案された第三者提供の可否を個別に判断する、又は、情報銀行から事前に示された第三者提供の条件を個別に／包括的に選択する方法により行う。

【個人との関係】

- 情報銀行が個人に提供するサービス内容（情報銀行が扱うデータの種類、提供先第三者となる事業者の条件、提供先における利用条件）については、情報銀行が個人に対して適切に提示し、個人が同意するとともに、契約等により当該サービス内容について情報銀行の責任を担保する。

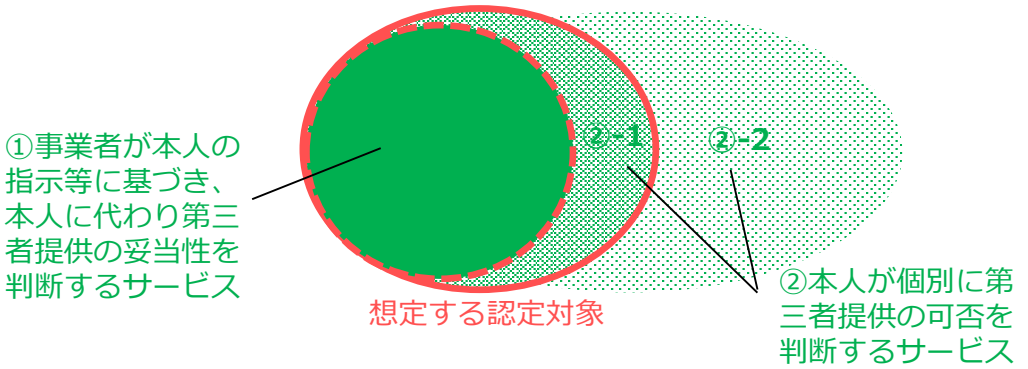


本指針の対象とするサービス

（１）個人情報の提供に関する同意の方法

- 認定の対象は、①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と、②本人が個別に第三者提供の可否を判断するサービスのうち、情報銀行が比較的大きな役割を果たすもの（※）とする。

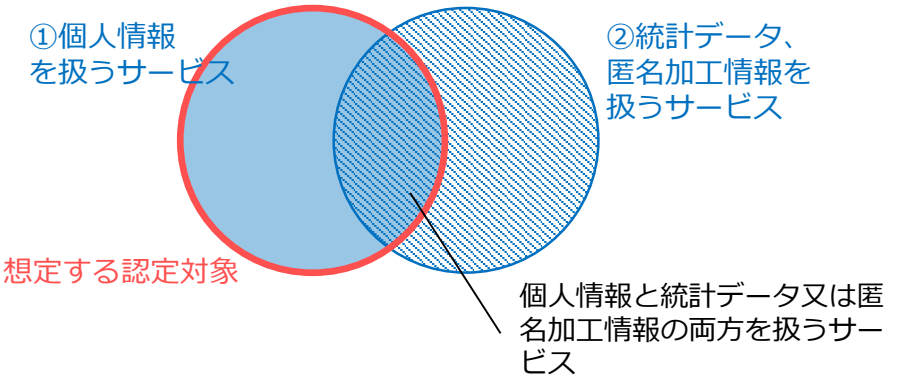
※②本人が個別に第三者提供の可否を判断するサービスのうち、提供事業者が情報の提供先を選定して個人に提案する場合など、提供事業者が比較的大きな役割を果たす（責任をもつ）ケース（②-1）を想定。他方、純粋なＰＤＳなどデータの管理や提供に関し個人の主体性が強いサービス（②-2）まで認定の対象として想定している訳ではない（認定がないことをもって信頼性が低いと評価されるべきものではない）。
※なお、データ保有者と当該データの活用を希望する者を仲介し、売買等による取引を可能とする仕組み（市場）である「データ取引市場」については認定の対象外。



（２）事業で扱うデータの種類

- 本指針は、個人情報を扱う事業を対象に、安心して利用出来る情報銀行という観点から認定要件を定めており、個人情報を全く扱わない事業は対象としない。

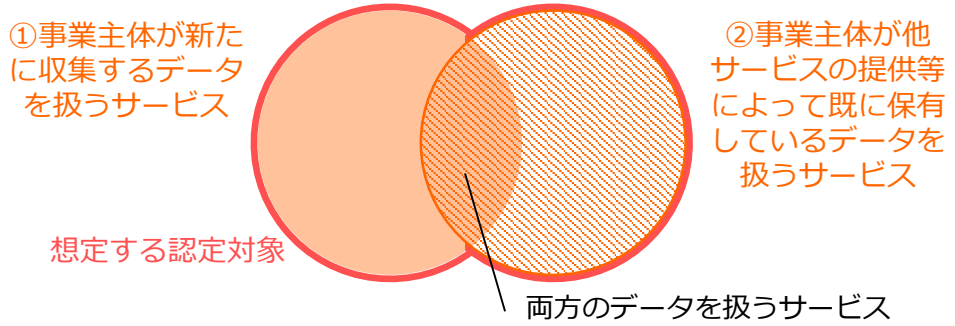
※本指針において、「個人情報」に関して設けている取扱上の制限等については、統計データ・匿名加工情報については適用されない。（統計データ・匿名加工情報に対する個人のコントローラビリティの及ぶ程度については、情報銀行ごとに判断されるべきである。）
※ただし、個人情報の加工及び加工した情報の提供を行う場合には、その旨や当該提供による個人への便益（便益の有無を含む）について、必要な情報を個人に対して開示することが必要。



※本検討会で対象とする「個人情報」には、「要配慮個人情報」は含まない

（３）データの収集方法

- 本指針に基づき認定する事業主体としては、情報銀行事業以外の他サービスを提供している者も想定されるため、情報銀行として扱うデータは、新たに収集するデータと、事業主体が既に保有しているデータのいずれもが考えられる。
- 既に保有しているデータを情報銀行として扱う場合には、新たに個人との間で情報銀行としての契約が必要となる。



※情報銀行を新たに営もうとする者は、以下について注意すること

- 銀行法上の「銀行」以外の者が商号又は名称に銀行であることを示す文字を使用することは禁止されていること。（銀行法第6条第２項）
- 信託業法上の「信託会社」等以外の者が商号又は名称に信託会社であると誤認されるおそれのある文字を用いることは禁止されていること。（信託業法第14条第２項）

情報信託機能の認定基準

認定基準

1）事業者の適格性

項目	内容
①経営面の要件	・法人格を持つこと
	・業務を健全に遂行し、情報セキュリティなど認定基準を担保するに足りる財産的基礎を有していること （例）直近（数年）の財務諸表の提示（支払不能に陥っていないこと、債務超過がないこと）等
	・損害賠償請求があった場合に対応できる能力があること （例）一定の資産規模がある、賠償責任保険に加入している　等
②業務能力など	・個人情報保護法を含む必要となる法令を遵守していること ・プライバシーポリシー、セキュリティポリシーが策定されていること
	・個人情報の取り扱いの業務を的確に遂行することができる知識及び経験を有し、社会的信用を有するよう実施・ガバナンス体制が整っていること （例）類似の業務経験を有する、プライバシーマーク・ISMS認証などの認証を有している　等
	・情報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、情報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、情報提供先にも、情報銀行と同様、認定基準に準じた扱い（セキュリティ基準、ガバナンス体制、事業内容等）を求めること（※）　等
	・認定の対象となる事業が限定される場合、事業者は申請の対象となる事業の部分を明確化すること

（※）情報銀行は、提供先がPマークまたはISMS認証を取得していない場合であっても、
- 情報は情報銀行が管理し、提供先は決められた方法で、必要な情報の閲覧のみができることとする
- 提供先において特定の個人を識別できないよう、個人情報の暗号化処理または個人情報の一部の置き換え等の処理を行い、復元に必要な情報を除いた形で提供先に提供する
- 情報銀行の監督下で、提供先からPマークまたはISMS認証を取得している者に個人情報の取扱いを全て委託させる

のいずれかの対策を講じた上で、それぞれのケースにおいて求められる情報セキュリティ・プライバシーに関する具体的基準を提供先が遵守していると認められる場合には、「認定基準に準じた扱い」であるとすることができる。

2）情報セキュリティ・~~プライバシー等①~~

項目	内容
基本原則	・リスクマネジメントにもとづき、情報セキュリティ及びプライバシーに関する十分な人的体制（組織体制含む）を確保していること、対象個人、データ量、提供先が増加した場合でも十分な情報セキュリティ体制を講じることができる体制を有すること。 ・国際標準・国内規格の考え方も参考に、情報セキュリティ及びプライバシー保護対策を徹底すること（例：JISQ15001個人情報保護マネジメントシステム（要求事項）、ISO/IEC29100（JIS X 9250）プライバシーフレームワーク）
遵守基準	・個人情報の取り扱い、安全管理基準について、プライバシーマーク又はISMS認証の取得（業務に必要な範囲の取得を行っていること）をしていること ・定期的にプライバシーマーク又はISMS認証の更新を受けること （※認定申請時に、プライバシーマーク又はISMS認証申請中である場合は、事業を開始するまでの間に当該認証を取得すること） ・個人情報保護法の安全管理措置として保護法ガイドラインに示されている基準を満たしていること、また、業法や業種別ガイドラインなどで安全管理措置が義務付けられている場合にはそれを遵守していることを示すこと。 ・~~次頁の「情報セキュリティ②③具体的基準」~~次項以降に示す具体的基準を遵守して業務を実施すること、認定申請時に当該基準を遵守していることを示すこと

（参考基準等）
・個人情報の保護に関する法律ついてガイドライン（通則編） https://www.ppc.go.jp/files/pdf/guidelines01.pdf
・プライバシーマーク制度審査基準 https://privacymark.jp/system/guideline/pdf/pm_shinsakijun.pdf
https://privacymark.jp/system/guideline/pdf/guideline_V2_180410.pdf
・ISMS認証 https://isms.jp/isms.html
・JIS Q 27001：2014 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項
（ISO/IEC 27001：2013 Information technology - Security techniques - Information security management systems - Requirements）
・JIS Q 27002：2014 情報技術－セキュリティ技術－情報セキュリティ管理策の実践のための規範
（ISO/IEC 27002：2013 Information technology - Security techniques - Code of practice for information security controls）
・経済産業省 情報セキュリティ管理基準参照 http://www.meti.go.jp/press/2015/03/20160301001/20160301001-1.pdf
・総務省セキュリティURL http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/

2）情報セキュリティ等② 具体的基準

項目	内容
①情報セキュリティマネジメントの確立	・経営層（トップマネジメント）は情報セキュリティマネジメントに関してリーダーシップ、コミットメントを発揮すること ・情報セキュリティマネジメントの境界及び適用可能性を明確にし、適用範囲を決定すること ・情報セキュリティリスクアセスメントのプロセスを定め、適用すること、リスク分析、評価、対応を行うこと
②情報セキュリティマネジメントの運用・監視・レビュー	・情報セキュリティマネジメントに必要な人・資源・資産・システムなど準備、割り当て、確定すること ・定期的なリスクアセスメントや、内部監査などを実施することで、情報セキュリティマネジメントの適切性、妥当性及び有効性を継続的に改善すること
③情報セキュリティマネジメントの維持・改善	・情報セキュリティマネジメントを適切・継続的に維持していくこと ・不適合が発生した場合、不適合の是正のための処置を取ること、マネジメントの改善など行うこと
④情報セキュリティ方針策定	・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
⑤情報セキュリティ組織	・責任者の明確化、組織体制を構築 ・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に加盟すること
⑥人的資源の情報セキュリティ	・経営層は従業員へのセキュリティ方針及び手順に従った適用の遵守、個人情報を扱う担当者の明確化 ・情報セキュリティの意識向上，教育及び訓練の実施
⑦資産の管理	・情報及び情報処理施設に関連する資産の洗い出し、特定し、適切な保護の責任を定めること ・固有のデータセンターを保有していること、又はそれと同等の管理が可能な委託先データセンターを確保していること 外部クラウドを活用する場合には当該クラウド利用契約上の情報セキュリティ要件などで担保されていることを示すこと（例：JIS Q 27017「JIS Q27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範」） ・情報を取り扱う媒体等から情報を削除・廃棄が必要となった場合にそれが可能な体制もしくは仕組みを有すること ・対象となる事業で扱う情報が他事業と明確に区分され管理されていること ※なお、外部クラウドなど活用する場合や、委託を行う場合に相手方事業者との間で、裁判管轄を日本の裁判所とすること、準拠法を日本法とすることを合意しておくこと
⑧技術的セキュリティ	（アクセス制御） ・アクセス制御に関する規定を策定し、対応すること（例：アイデンティティ管理システムの構築、アクセス制御方針の実装） ・情報にアクセス権を持つ者を確定し、それ以外のアクセスの制限を適切に行うこと （暗号） ・情報の機密性、真正性、完全性を保護するため暗号の適切で有効な利用をすること ・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など対応すること

2）情報セキュリティ③ 具体的基準

項目	内容
⑨物理的及び環境的情報セキュリティ	・自然災害，悪意のある攻撃又は事故に対する物理的な保護を設計、適用すること ・情報及び情報処理施設への入退室管理、情報を扱う区域の管理、定期的な検査を行うこと 外部クラウドを活用する場合には当該クラウド利用契約上の情報セキュリティ要件などで担保されていることを示すこと ・情報を取り扱う機器等のソフトウェア、ハードウェアなど最新の状態に保持すること、セキュリティ対策ソフトウェアなどを導入すること
⑩運用の情報セキュリティ	・情報処理設備の正確かつ情報セキュリティを保った運用を確実にするため操作手順書・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り、不正アクセスの検知に関する対策を行うこと、情報漏えい防止措置を施すこと ・技術的ぜい弱性管理、平時のログ管理や攻撃監視などに関する基準が整備されていること ・サイバー空間の情勢を把握し、それに応じた運用上のアップデートなどが行われること
⑪通信の情報セキュリティ	・システム及びアプリケーション内情報保護のためのネットワーク管理策、制御の実施 ・自ら提供するか外部委託しているかを問わず、全てのネットワークサービスについて、情報セキュリティ機能、サービスレベル及び管理上の要求事項の特定 ・情報サービス，利用者及び情報システムは、ネットワーク上でグループごとに分離 ・組織の内部及び外部での伝送される情報のセキュリティを維持するための対策の実施（通信経路又は内容の暗号化などの対応を行うこと）
⑫システムの取得・開発・保守	・情報システム全般にわたり情報セキュリティを確実にするため、新しいシステムの取得時および既存システムの改善時要求事項としても情報セキュリティ要求事項を必須とすること ・開発環境及びサポートプロセス（外部委託など）においても情報セキュリティの管理策を策定、実施すること
⑬供給者関係	・供給者との間で、関連する全ての情報セキュリティ要求事項を確立、合意、定期的監視 ・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要求事項を含む
⑭情報セキュリティインシデント管理	・情報セキュリティインシデントに対する迅速、効果的な対応のため責任体制の整備、手順の明確化、事故発生時は、速やかに責任体制への報告、対応（復旧・改善）、認定団体への報告などを実施すること ・漏洩など事故発生時の対応体制、報告・公表などに関する基準が整備されていること ・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が整備されていること ・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を定期的に実施すること
⑮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	・情報セキュリティ継続を組織の事業継続マネジメントシステムに組み込むこと
⑯遵守	・情報システム及び組織について、全ての関連する法令、規制及び契約上の要求事項などを遵守 ・プライバシー及び 個人データの保護は、関連する法令及び規制の確実な遵守 ・定めた方針及び手順に従って情報セキュリティが実施・運用されることを確実にするための定期的なレビューの実施

2）~~参考：~~プライバシー保護対策~~等について~~

基本原則において、「リスクマネジメントにもとづき、情報セキュリティ及びプライバシーに関する十分な人的体制（組織体制含む）を確保していること」「国際標準・国内規格の考え方も参考に、情報セキュリティ及びプライバシー保護対策を徹底すること」としており、プライバシー保護対策についても、以下の事項等を参考に、十分に整備・遵守していく~~ことが~~必要~~がで~~ある。

~~なおまた~~、2017年にISO/IEC 29100プライバシーフレームワークに基づく行動規範の国際規格（ISO/IEC 29151※）が発行されたところであり、本認定基準への採否については、継続的に検討していくことが重要である。

~~なお、参考まで個人情報保護法ガイドラインに定められている措置の項目を掲載する。~~

※29151の正式名称："Code of practice for privacy personally identifiable information protection"

（プライバシー保護対策等に関し参考とするべきなる事項等）

■JISQ15001個人情報保護マネジメントシステム（要求事項）

■~~ISO/IEC 29100~~ JIS X 9250:2017プライバシーフレームワークで定義されているプライバシー原則

表3－この規格におけるプライバシー原則
1. 同意及び選択（Consent and choice） 2. 目的の正当性及び明確化（Purpose legitimacy and specification） 3. 収集制限（Collection limitation） 4. データの最小化（Data minimization） 5. 利用，保持，及び開示の制限（Use, retention and disclosure limitation） 6. 正確性及び品質（Accuracy and quality） 7. 公開性，透明性，及び通知（Openness, transparency and notice） 8. 個人参加及びアクセス（Individual participation and access） 9. 責任（Accountability） 10. 情報セキュリティ（Information security） 11. プライバシーコンプライアンス（Privacy compliance）

■（参考）個人情報保護法ガイドライン（通則編）86頁以降抜粋

講じなければならない措置	項目
基本方針の策定	・事業者名称、関係法令・ガイドライン等の遵守、安全管理措置に関する事項、質問及び苦情処理窓口等
組織的安全管理措置	・組織体制の整備、個人データの取扱いに係る規律に従った運用、個人データの取り扱い状況を確認する手段の整備、漏えい等の事案に対応する体制整備、取扱状況の把握及び安全管理措置の見直し等
人的安全管理措置	・従業者の教育
物理的安全管理措置	・個人データを取り扱う区域の管理、機器及び電子媒体等の盗難等の防止、電子媒体等を持ち運ぶ場合の漏えい等の防止、個人データの削除及び機器、電子媒体等の廃棄
技術的安全管理措置	・アクセス制御、アクセス者の識別と認証、外部からの不正アクセス等の防止、情報システムの使用に伴う漏えい等の防止

３）ガバナンス体制

項目	内容
①基本理念	「データは、個人がその成果を享受し、個人の豊かな生活実現のために使うこと」及び「顧客本位の業務運営体制」の趣旨を企業理念・行動原則等に含み、その実現のためのガバナンス体制の構築を定め経営責任を明確化していること
②相談体制	・個人や事業者から、電話や電子メール等による問い合わせ、連絡、相談等を受け付けるための窓口を設けており、相談があった場合の対応プロセスを定めていること
③諮問体制	以下を満たす、社外委員を含む諮問体制を設置していること（データ倫理審査会~~（仮称）~~） ・構成員の構成例：エンジニア（データ解析や集積技術など）、セキュリティの専門家、法律実務家、データ倫理の専門家、消費者等多様な視点でのチェックを可能とする多様な主体の参加 ・データ利用に関する契約や利用方法、提供先第三者などについて適切性を審議し、必要に応じて助言を行う ・情報銀行は定期的に諮問体制に報告を行うこと、諮問体制は、必要に応じて情報銀行に調査・報告を求めることができる、情報銀行は当該求めに応じて、適切に対応すること
④透明性（定期的な報告・公表等）	・提供先第三者、利用目的、契約約款に関する重要事項の変更などを個人にわかりやすく開示できる体制が整っていること、透明性を確保（事業に関する定期的な報告の公表など）すること ・個人による情報銀行の選択に資する情報（当該情報銀行による個人への便益の考え方、他の情報銀行や事業者にデータを移転する機能の有無など）を公表すること
⑤認定団体との間の契約	・認定団体との間で契約を締結すること（認定基準を遵守すること、更新手続き、認定基準に違反した場合などの内容、認定内容に大きな変更があった場合は認定団体に届け出ることなど） ・誤認を防ぐため、認定の対象を明確化して認定について表示すること

４）事業内容~~①~~

項目	内容
①契約約款の策定	・モデル約款の記載事項に準じ、認定団体が定めるモデル約款を踏まえた契約約款を作成・公表していること（又は認定後速やかに公表すること）　（個人との間、（必要に応じて）情報提供元・情報提供先事業者との間）
②個人への明示及び対応	以下について、個人に対しわかりやすく示すとともに個人情報の利用目的及び第三者提供について個人情報保護法上の同意を取得すること（同意取得の例：包括的同意、個別同意など） ・情報銀行の行う事業及び対象とする個人情報の範囲、事業による便益、提供先第三者や利用目的に応じたリスク（注意点） ・対象となる個人情報とその取得の方法、利用目的、統計情報・匿名加工情報に加工して提供する場合はその旨 ・個人情報の第三者提供を行う場合の提供先第三者及び利用目的に関する判断基準及び判断プロセス ・情報銀行が提供する機能と、個人がそれを利用するための手続き ・個人が相談窓口を利用するための手続き
③情報銀行の義務について	以下の要件を満たすとともに、モデル約款の記載事項に準じて約款等に明記し、個人の合意を得ること ・個人情報保護法をはじめ、関係する法令等を遵守すること（取り扱う情報の属する個別分野に関するガイドラインを含む） ・個人情報について認定基準のセキュリティ基準にもとづき、安全管理措置を講じ、セキュリティ体制を整備した上で維持・管理を行うこと ・善管注意義務にもとづき、個人情報の管理・利用を行うこと ・対象とする個人情報及びその取得の方法、利用目的の明示 ・個人情報の第三者提供を行う場合の提供先第三者及び利用目的に関する適切な判断基準（認定基準に準じて判断）の設定・明示 ・個人情報の第三者提供を行う場合の適切な判断プロセスの設定・明示（例：データ倫理審査会~~（仮称）~~ の審査・承認など） ・個人情報の提供先第三者及び当該提供先第三者の利用目的の明示 ・個人が自らの情報の提供に関する同意の撤回（オプトアウト）を求めた場合は、対応すること ・個人情報の取り扱いの委託を行う場合には、個人情報保護法第22条に照らして必要な監督を行うこと （提供先第三者との関係）

４）事業内容~~①（つづき）~~

項目	内容
④情報銀行の義務について	・個人情報の第三者提供を行う場合、当該提供先からの個人情報の他の第三者への再提供の原則禁止（※） ~~・個人情報の取り扱いの委託を行う場合には、個人情報保護法第22条に照らして必要な監督を行うこと~~ ・個人情報の提供先第三者との間での提供契約を締結すること ・当該契約において、必要に応じて提供先第三者に対する調査・報告の徴収ができること、損害賠償責任、提供したデータの取扱いや利用条件（認定基準に準じた扱いを求めること）について規定すること

※ 情報銀行は、個人起点のデータ利活用を推進するために、個人が信頼できる情報銀行に個人情報の取り扱いを委任することで、個人の情報に対するコントローラビリティを高めることを目的とするものであることから、情報銀行から個人情報を提供された第三者による当該情報の再提供は禁止される（情報銀行は、個人の同意があっても、再提供を行う事業者に個人情報を提供してはならない）のが原則である。ただし、次のような条件を満たす場合には、個人のコントローラビリティが確保され、情報信託機能の認定制度の趣旨を損なうものではないものとして、例外的に提供先第三者による再提供を認める（情報銀行は、以下の条件を満たす場合に限り、再提供を行う第三者に対して個人情報を提供することができる）ものとする。

- 提供元（情報銀行）は、提供先第三者との契約の中で、再提供について以下の条件を求めること。

（1）提供先第三者は、再提供先への提供について、再提供先の業種や事業分類（または個社名）と、その利用目的、提供する個人情報の項目、再提供先に対する個人情報の開示等の請求等の窓口を提供元（情報銀行）に報告すること

（2）個人と提供先第三者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、個人情報保護法第23条第1項に基づき、提供先第三者が個人から同意取得すること

（3）再提供先からの更なる第三者提供は認められないこと

- 再提供先における個人情報の取扱いが、提供元（情報銀行）を介した個人のコントローラビリティの範囲外であるところ、提供元（情報銀行）は、個人に対して、提供先第三者から再提供先へ当該個人情報の第三者提供を行うこと及び当該再提供先（業種や事業分類でも可、例：「金融分野のアグリゲーションサービス」）を明示すること。再提供については個人により選択可能とし、かつデフォルトオフにすることが望ましい。個人が提供元（情報銀行）側のUIで再提供を可とする場合、個々の再提供先への提供については、提供元（情報銀行）が個人から同意を取得する必要はない。
- 再提供の必要性、すなわち、個人が提供先第三者及び再提供先のサービスを利用すること及び提供先第三者において情報銀行から受け取った個人情報について付加や加工をすることにより再提供先のサービスが可能・有効となるものであることを前提とする。（例：金融分野のアグリゲーションサービス等）

なお、認定団体は、提供先第三者の基準が実質的に遵守されるよう（再提供先のセキュリティ、プライバシーに係る体制を確認する等）確認することが望ましい。

４）事業内容~~②~~

項目	内容
⑤個人のコントローラビリティを確保するための機能について	①情報銀行に委任した個人情報の第三者提供に係る条件の指定及び変更 ・提供先・利用目的・データ範囲について、個人が選択できる選択肢を用意すること(※1) ・選択を実効的なものとするために適切なユーザーインターフェイス（操作が容易なダッシュボードなど）を提供すること ・選択肢及びユーザーインターフェイスが適切に設定されているか、定期的にデータ倫理審査会~~(仮称)~~などの諮問体制に説明し助言を受けること ・利用者が個別の提供先、データ項目等を指定できる機能を提供する場合には、その旨を明示すること
	②情報銀行に委任した個人情報の提供履歴の閲覧（トレーサビリティ） ・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イスを提供すること ・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
	③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） ・個人から第三者提供・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 ・指示を受けた以降、既に提供先に提供されたデータの利用が当該データの提供を受けた提供先で制限されるか否か、制限される場合にはどの範囲で制限されるかを、あらかじめ本人に明示すること
	④情報銀行に委任した個人情報の開示等 ・簡易迅速で本人の負担のないユーザーインターフェイスにより、保有個人データの開示の請求（個人情報保護法第28条に基づく請求）を可能とする仕組みを提供すること(※2) ・その他、~~他の事業者へのデータの移行等いわゆるデータポータビリティ機能を提供する場合には、その旨~~他の情報銀行や事業者にデータを移転する機能の有無を明示すること
⑥責任の範囲について	・消費者契約法など法令を遵守した適切な対応をすること ・情報銀行は、個人との間で苦情相談窓口を設置し、一義的な説明責任を負う ・提供先第三者に帰責事由があり個人に損害が発生した場合は、情報銀行が個人に対し損害賠償責任を負う

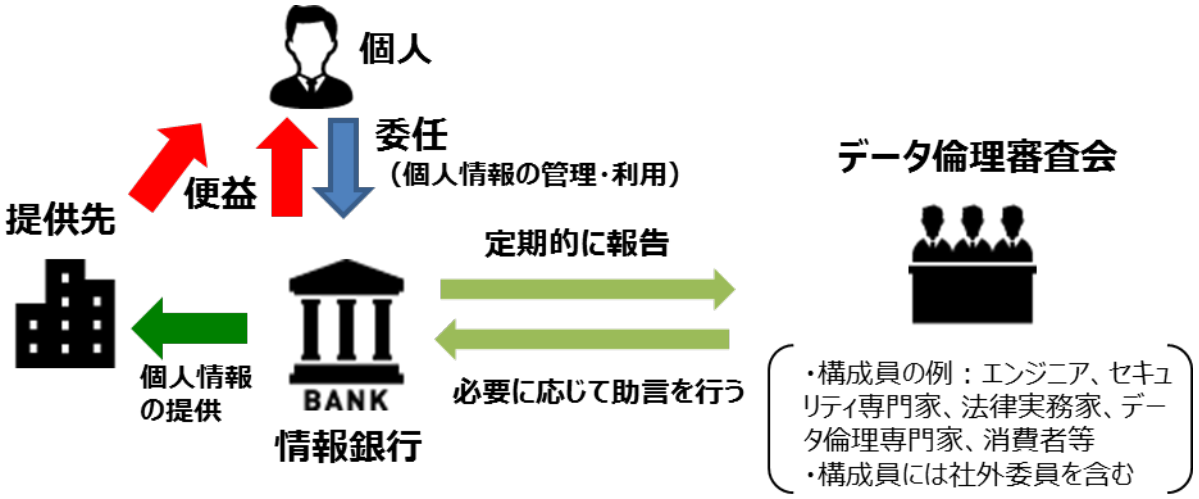
（※1）選択肢の設定については、本人が第三者提供について判断できる情報を提供する必要があり、例えば、「上場企業／その他含む」「観光目的／公共目的」のように数の少ない分類方法から、より個別具体的で数の多い分類方法までが考えられる。
（※2）例えば、情報銀行を営む事業者が、本人から提供された情報で情報銀行として取り扱う範囲のデータについては、本人確認によりログインしたサイト上で、一括して閲覧・ダウンロードできる仕組みが考えられる。

諮問体制（データ倫理審査会）に関する事項

説明の追加

■ データ倫理審査会における審議の考え方
- 情報銀行は、個人の代理として、個人が安心して自らに関する情報を預けられる存在であることが期待される。このため、利用者たる個人の視点に立ち、適切な運営が確保される必要がある。
- このため、データ倫理審査会は、情報銀行の事業内容が個人の利益に反していないかという観点から審議を行う。

（例）・個人によるコントローラビリティを確保するための機能が誤解のないUIで提供されているか
・個人の同意している提供先の条件について、個人の予測できる範囲内で解釈されて運用されているか
・個人にとって不利益となる利用がされていないか／個人に対し個人情報の利用によるリスクが伝えられているか
・個人にとって高いリスクを発生させる恐れがある場合には、GDPRで義務づけられているDPIA（データ保護影響評価）を参考にすることも考えられる



●情報銀行事業について、以下の事項についてその適切性を審議し、必要に応じて助言を行う
- ・個人と情報銀行の間の契約の内容
- ・情報銀行の委任した個人情報の利用目的
- ・個人による情報銀行に委任した個人情報の第三者提供に係る条件の指定及び変更の方法（ＵＩ）
- ・提供先第三者の選定方法
- ・委任を受けた個人情報の提供の判断

●運営方法
- ・構成員及び（必要な範囲の）議事録は公開する
- ・必要に応じ情報銀行に調査・報告を求めることができる

情報信託機能のモデル約款の記載事項

個人情報の提供に関する契約上の合意の整理

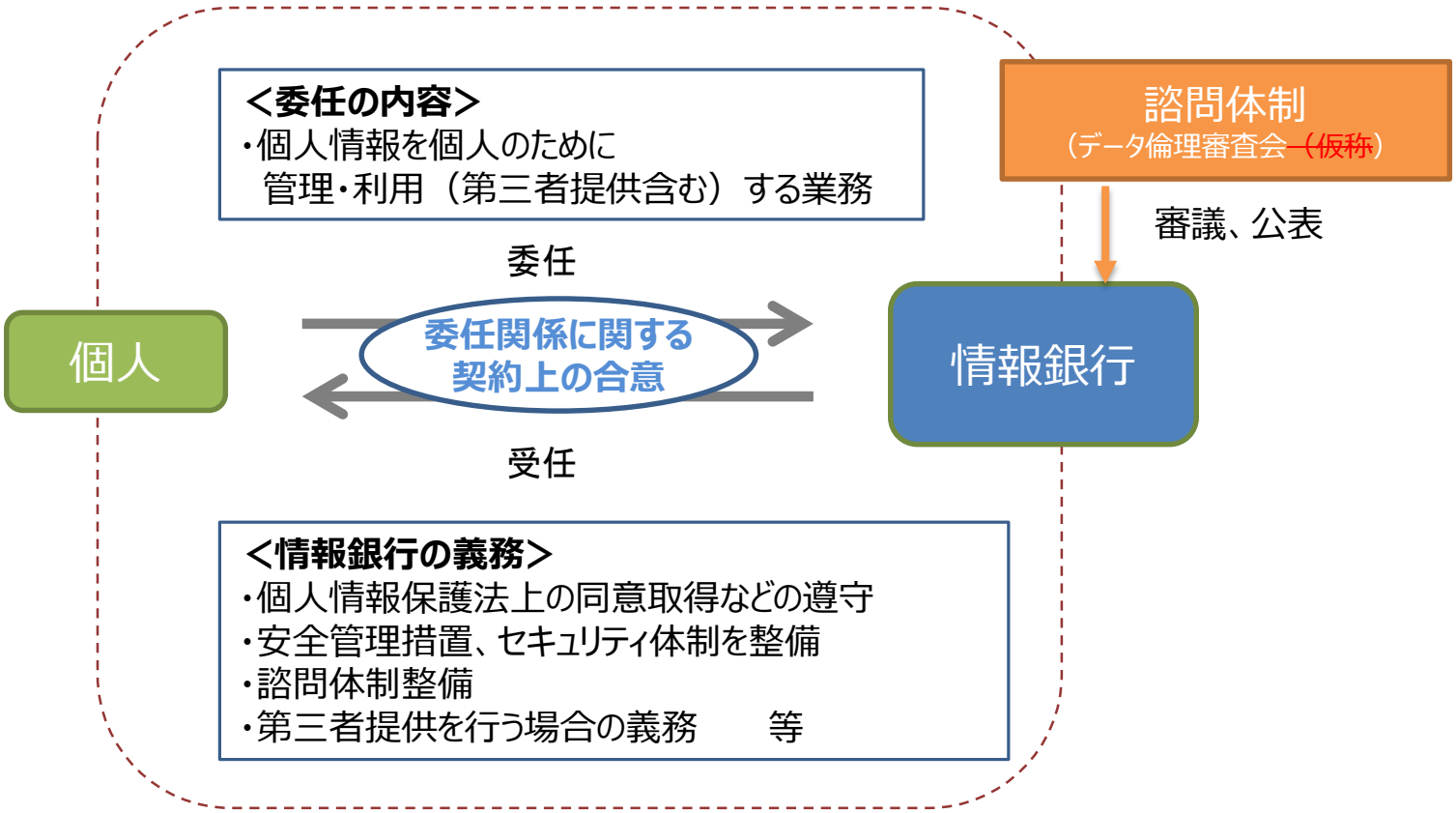
■　情報信託機能を提供する「情報銀行」のサービスについて、債権債務の内容や情報銀行の責任範囲を明確化するため、**個人と情報銀行の間を委任関係に関する契約上の合意**と整理する。

■　「委任関係」とは、個人に代わって妥当性を判断の上、個人情報を適正に管理･利用（第三者提供含む）することについて、個人が情報銀行に委任する関係とする。

■　このような委任関係を、より個人のコントローラビリティを確保した、消費者個人を起点としたサービスの実現に資するものとするため、個人への便益や委任の内容などの具体的合意条件を契約関係として整理する標準的な契約条項を「モデル約款の記載事項」として示す。

■　その際、委任関係の内容を契約等でわかりやすく整理し、個人情報保護法上の第三者提供においても有効な包括的同意(又は個別的同意)が取得できるよう整理することが重要。

〔個人情報の提供に関する契約上の合意の整理〕



※個人情報保護法上の第三者提供・利用目的の変更の同意を満たすことが必要

【参考：未成年等の制限行為能力者が情報銀行を利用する場合】

情報銀行が対象とする個人が未成年者等の制限行為能力者である場合には、契約の締結と、情報銀行との間の同意等の手続きについては、それぞれ法令に照らし、適切な者が行う必要がある。

✓ ①の同意については、個人情報保護法上の「本人の同意」として同意を得るべき者が行う。

✓ ②の契約については、制限行為能力者に関する法律の規定に従い、同意権者の同意に基づいて本人が契約を締結することや、法定代理人が本人に代わって契約を締結することが必要となる。

モデル約款の記載事項

・モデル約款の記載事項を踏まえ、認定団体において、モデル約款を策定
・認定を受ける情報銀行は、当該モデル約款の記載事項に準じ、認定団体が策定するモデル約款を踏まえた契約約款を作成すること

1　個人と情報銀行の間

1）目的
　個人からの委任にもとづき、個人情報を含む個人のデータを当該個人の利益を図るために適正に管理・利用（第三者提供を含む）する「情報銀行」の事業について定めること

2）定義
　本委任契約の対象となる「個人情報」には「要配慮個人情報」~~「クレジットカード番号」「銀行口座番号」~~は含まない

3）情報銀行の行う業務範囲
　情報銀行は、個人に代わって当該個人データについて、当該個人の合理的利益が得られるような活用手法、情報提供先の選定、第三者提供、個人データの維持・管理、業務の適切な提供・改善のための利用などを行う。（情報銀行は、それぞれが行う業務の内容、便益、データ範囲などを明記。またその活用によって個人に不利益が生じないよう配慮すること）

4）情報銀行が担う義務
（事業全体）
・個人情報保護法に定める義務を遵守すること
・個人情報について安全管理措置を講じ、セキュリティ体制を整備した上で維持・管理を行うこと
・善管注意義務にもとづき、個人情報の管理・利用を行うこと

４）情報銀行が担う義務（つづき）

（個人情報の取扱い）

・対象とする個人情報及びその取得の方法、利用目的の明示

・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（認定基準に準じて判断）の明示（提供後に適切なセキュリティの下でデータ管理が行われることを判断基準に含める）

・個人情報の第三者提供を行う場合の判断プロセスの明示（例：データ倫理審査会~~(仮称)~~による審査・承認）

・個人情報の第三者提供に関する同意の取得方法の明示

・個人情報の提供先第三者及び当該提供先第三者の利用目的の明示

・個人が自らの情報の提供に関する同意の撤回（オプトアウト）を求めた場合は、対応すること

・情報銀行の行う事業による便益（一般的便益に加え、具体的事業内容にてらした便益を含む）の明示

・個人情報の取り扱いの委託を行う場合には、個人情報保護法第22条に照らして必要な監督を行うこと

（提供先第三者との関係）

・個人情報の第三者提供を行う場合、当該提供先からの個人情報の他の第三者への再提供は原則禁止する

~~・個人情報の取り扱いの委託を行う場合には、個人情報保護法第22条に照らして必要な監督を行うこと~~

・個人情報の提供先第三者との間での提供契約を締結すること

・当該契約において、情報提供先にも、認定基準に準じた扱い（セキュリティ基準、事業内容等）を求めること

・当該契約において、必要に応じて提供先第三者に対する調査・報告の徴収ができることを記載すること

・当該契約において、提供先は適切な情報管理体制を構築していることを要求すること

５）プライバシーポリシーの適用

・情報銀行は当該情報銀行が定め公表しているプライバシーポリシーで定める内容を遵守すること

６）情報銀行の機能について

個人が情報銀行に委任した情報の取り扱いについてコントロールできる機能の明示（下記の機能に加え、その他の機能があれば、それを示すこと）

・情報銀行に委任した個人情報の第三者提供に係る条件の指定及び変更

・情報銀行に委任した個人情報の提供履歴の閲覧（トレーサビリティ）

・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）

・情報銀行に委任した個人情報の開示等

7）個人の指示に基づいて、個人情報を情報提供元事業者から情報銀行に移行する場合は、個人は、情報提供元事業者との間で、事前に情報の移行に関する了承を得ること（個人からの依頼に基づき、情報銀行が情報提供元事業者に情報の移行に関する了承を得ることを含む）

8）個人は情報銀行が委任内容を適切に運営できるよう、情報銀行から必要に応じて確認など求めがあった場合（※）には適切に対応につとめること　※過剰な内容の求めとならないよう留意すること

9）相談窓口
・情報銀行は個人からの相談への対応体制を設けること

10）重要事項の変更
・個人情報の取得・提供などに関する約款内容に重要事項に変更がある場合には、事前通知を行うこと、同意を得ること

11）損害賠償責任
・消費者契約法など法令を遵守した適切な対応をすること
・情報銀行は、個人との間で苦情相談窓口を設置し、一義的な説明責任を負う
・提供先第三者に帰責事由があり個人に損害が発生した場合は、情報銀行が個人に対し損害賠償責任を負う

12）事業終了時、事業譲渡時、契約解除時の扱いについて
・情報銀行に関する事業を終了、譲渡する又は、契約解除を行う場合の対応、個人情報の取り扱いについて規定すること

13）準拠法など
・裁判管轄を日本の裁判所とし、準拠法を日本法とする

2　情報銀行と情報提供元との間

１）提供されるデータの「形式」「提供方法」等に関する規定（例：情報提供元が保有する個人情報を情報銀行が取得する場合は、当該情報提供元から取得する場合や個人が情報提供元からダウンロードし情報銀行に提供する場合などにおける仕組みや手法などを含む）

２）情報銀行側における情報の利用範囲や取扱条件の制限に関する規定（個人と情報提供元との間に事前に情報の移行に関する了承がある場合、又は、個人からの依頼に基づき情報銀行が情報提供元に情報の移行に関する了承を得る場合の規定）

３）情報銀行は情報漏えい等のインシデント発生時には、速やかに情報提供元へ通知すること

４）情報漏えいの際の原因究明に向けた、情報提供元と情報銀行との協力体制などに関する規定、損害賠償責任に関する規定

５）情報提供環境のセキュリティ要件(ネットワーク経由でデータ提供する場合のVPNの設定等)に関する規定

3　情報銀行と情報提供先との間

１）提供されるデータの「形式」「提供方法」等に関する規定

２）情報提供先における情報の利用範囲や取扱条件の制限に関する規定（個人から同意を得ている利用目的の範囲内での活用、認定基準に準じたセキュリティ体制、他の第三者への再提供の禁止、加工した情報の取扱い等）

３）情報銀行から提供する情報が匿名加工情報である場合には、情報提供先に対しこの旨を明示すること

４）２）の履行に関する情報銀行の確認・調査への協力に関する規定

５）情報提供先は情報漏えい等のインシデント発生時には、速やかに情報銀行へ通知すること

６）情報漏えいの際の原因究明に向けた、情報提供先と情報銀行との間の協力体制などに関する規定、損害賠償責任に関する規定

７）情報提供環境のセキュリティ要件(ネットワーク経由でデータ提供する場合のVPNの設定等)に関する規定

情報信託機能の認定スキーム

認定団体における認定スキーム

１）認定団体の適格性
・独立性、中立性、公平性などが担保されていること

２）認定する際の審査の手法
・認定を申請する情報銀行（申請事業者）による申請フォーマットの入力（なお、認定は、事業者単位／事業単位いずれでも申請を受け付けることとし、申請の対象となる事業の範囲は申請事業者側が定義する）
・申請フォーマットにもとづいた、事務局によるヒアリング、有識者を構成員とする認定委員会による審査
・認定料の設定　・認定の有効期間（２年間）、更新手続きの設定

３）認定証について
・認定団体が情報銀行を認定した場合、認定団体名が明記された認定証を交付する
・認定を受けた情報銀行（認定事業者）は当該認定証をHPなどで提示する（認定申請時に、認定を受ける業務範囲を限定した事業者は、認定証の提示は当該認定を得た事業範囲のみとする）
・認定団体は、認定事業者リストをHPなど含めて掲示する
・認定団体は認定を受けていない事業者（認定を取り消された事業者、更新期限を超過した事業者を含む）が認定証を無断で使用していることが判明した場合は、適切な対応をすること

４）認定事業者が認定内容に違反した場合、個人情報漏洩が起こった場合の対応
・認定基準に違反した場合は、認定の留保、一時停止、停止、認定の取り消し、事業者名の公表などを含めて検討し、第三者委員会（監査（諮問）委員会）に諮問、判断

５）認定団体と認定事業者との間の契約
・認定団体と認定事業者との間で契約を締結する
・当該契約には、認定基準を遵守すること、更新手続き、認定基準違反時の対応、認定団体が認定事業者に対して、認定などに必要となる検査、報告徴収などできるようにすることなどが含まれる

６）認定団体の運用体制
・認定団体が責任ある認定を行うことができるよう、以下の体制を備える
・事務局　・認定委員会　・苦情等窓口
・第三者組織（監査諮問委員会）（有識者、消費者、セキュリティ専門家などを含む構成とする）

認定団体の運用スキーム