資料12－1

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（案）

平成31年4月26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「指針ver1.0」）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したもの。
- 指針ver1.0の策定に関する検討は、情報銀行のサービスが存在し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、さらには本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、指針ver1.0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～●月までに計●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、定期的に開催して指針の運用状況について点検することとする。

・ 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。

＜指針の見直しと認定制度の関係＞

・ 本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

（敬称略、五十音順、平成31年4月1日現在）

【委員】

	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 ITイノベーション部　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　副本部長
	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 情報通信委員会企画部会 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

（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、情報銀行及び本指針に基づく認定の考え方について整理を行った。
- 整理した内容を中心に、指針ver1.0を見直した指針ver2.0について最後に添付する。

1. 情報銀行認定の基本的な考え方
   - ①情報銀行の定義
   - ②情報銀行の提供するサービス例
   - ③情報銀行と契約を行う者が異なる場合
   - ④統計データ、匿名加工情報の扱い
   - ⑤行政機関／独立行政法人等
   - ⑥複数者が共同で行う場合の選定
   - ⑦提供先第三者の選定
   - ⑧認定の対象とする個人情報

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情報提供先からの再提供

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

【概要】

- 情報銀行については、個人情報の活用に関して社会的に不安がある中で、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では情報銀行の定義について、情報銀行が備えるべき機能を中心に記載されていたところ、こうした情報銀行の目的も踏まえ、再度整理を行った。
- 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として定義され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。
- 加えて、各社における情報銀行事業の具体化や、認定制度の運用開始に伴い、認定の考え方についても精査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、考え方の整理を行った。

■ 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。

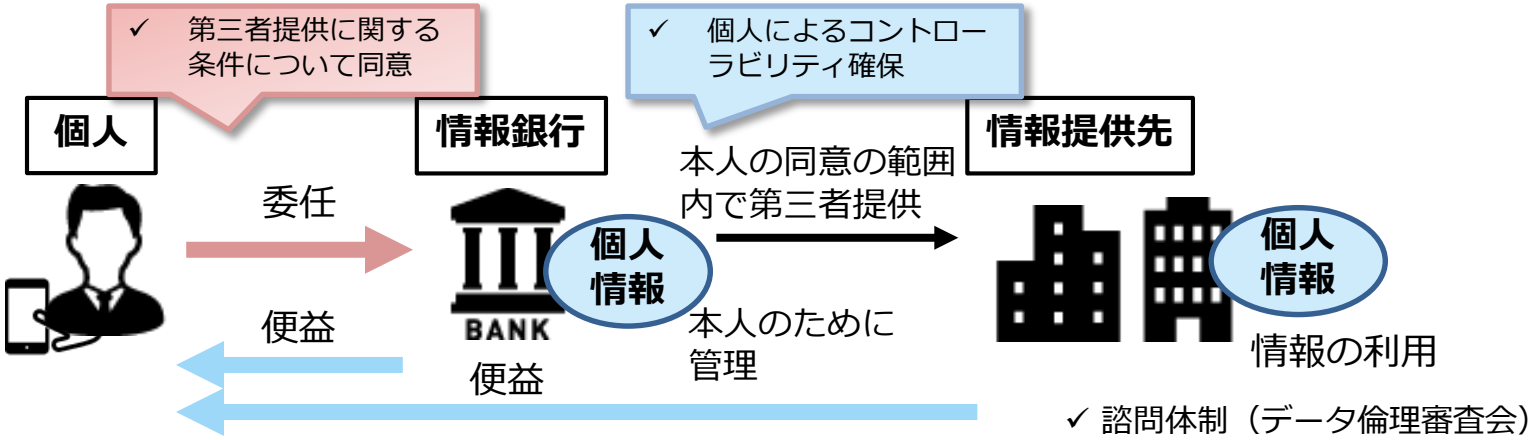
同意取得のパターン	概要	本指針に基づく認定との関係
①　包括的な同意	・事業者が個人情報の第三者提供を本人が同意した一定の範囲において本人の指示等に基づき本人に代わり第三者提供の妥当性を判断するサービス	・認定の対象
②－１　個別的な同意（情報銀行の関与が強い場合）	・提供事業者が情報の提供先を選定して個人に提案する場合など、提供事業者が比較的大きな役割を果たす（責任をもつ）ケース	・情報銀行が比較的大きな役割を果たすため、認定の対象
②－２　個別的な同意（個人の主体性が強い場合）	・純粋なPDSなどデータの管理や提供に関し個人の主体性が強いサービス	・純粋なPDSについては、認定の対象外（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

1－①　情報銀行の定義

【目的】
- 「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、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、使いやすいユーザインタフェースを用いて、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。

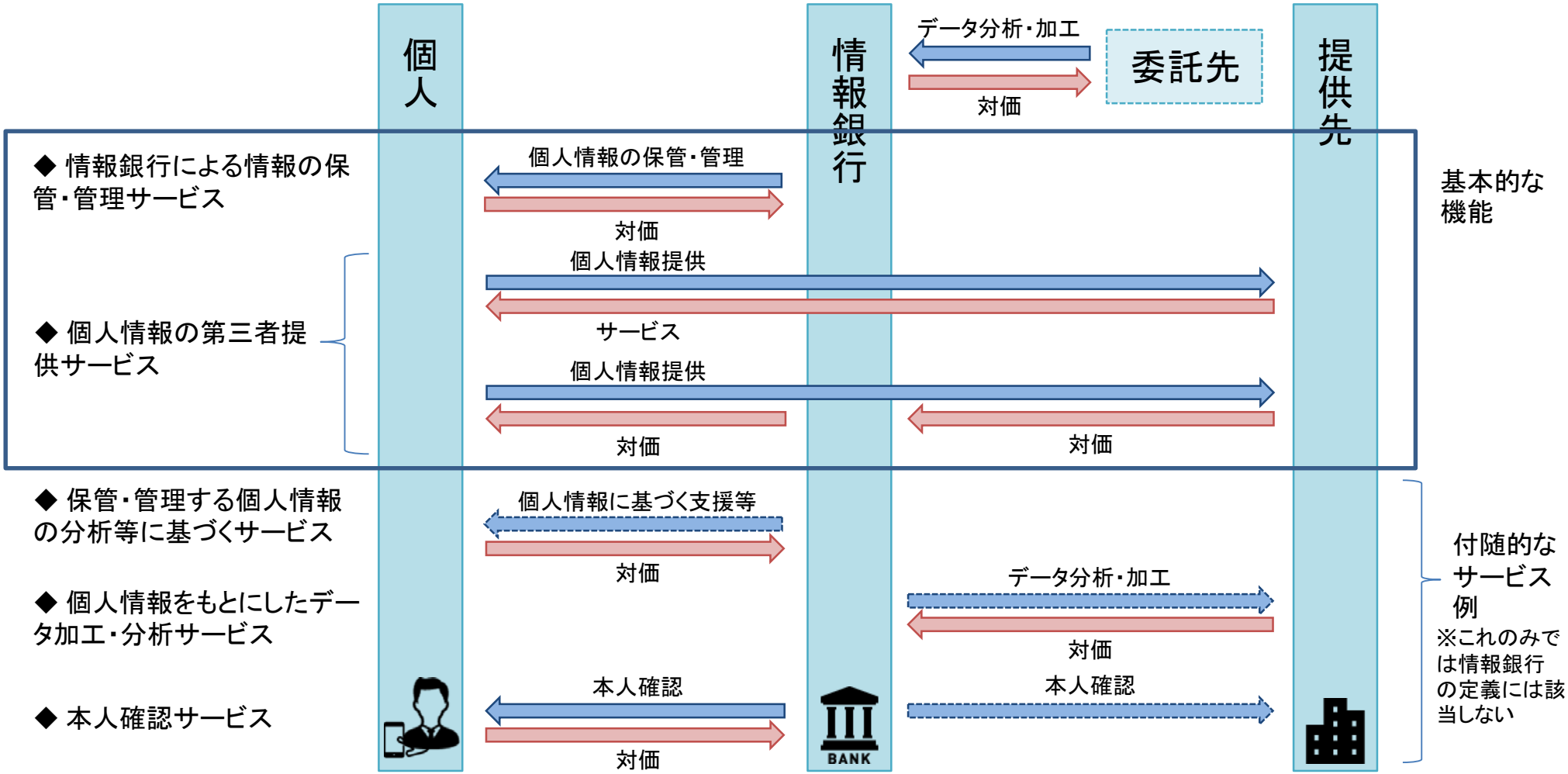
【個人と情報銀行の関係】
- 情報銀行が個人に提供するサービス内容（情報銀行が扱うデータの種類、第三者提供先となる事業者の条件、提供先における利用条件）については、情報銀行が個人に対して適切に提示し、個人が同意するとともに、契約等により当該サービス内容について情報銀行の責任を担保する。



- **指針の「情報銀行の定義」を修正**

1－②　情報銀行の提供するサービス例

- 情報銀行を定義する機能は、個人情報の管理及び第三者提供であると考えられるが、情報銀行事業においてはこれらに付随して、他の様々な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の方向についてもその形態によって様々な形を取りうると考えられる。なお、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、必ずしもここに示したサービスに限られるものではない。
- このように、基本的な機能を核としつつ、様々な機能が提供されることで、情報銀行事業が広がることが期待される。



1－③　情報銀行と契約を行う者が異なる場合

- 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、判断力の低い者の判断を補完する役割を担うことも想定されることから、情報銀行との間の手続きを行う者の考え方について整理する。
- 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得ることに加え、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人物として想定しているが、以下の通り、両者が異なる場合もあり得ることから、情報銀行が対象とする者によっては、留意する必要がある。
  - ✓　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、未成年・成年被後見人等であれば親権者・法定代理人等の確認が必要となる。

- **指針に考え方を記載**

● 個人情報保護法との関係

- 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。

● 契約（民法）との関係

- 認定指針においては、個人と情報銀行の間で契約関係を持つことが前提となっている。
- 未成年者及び成年被後見人については、契約は法定代理人が行うことができるとされている。
- なお、民法においても、主体により制限が生じる行為は場合により異なるが、この場合は契約をする者が行う。

	個人が情報銀行に対して行う手続き	手続きを行う者
契約	・情報銀行／個人間の契約の締結	・本人（法定代理人が確認）
個人情報の提供に関する手続き	・個人情報の利用／第三者提供に関する同意（条件の指定）	・「本人の同意」を行う者
	・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）	・「本人の同意」を行う者
その他	・相談窓口の利用	・本人または法定代理人
	・個人情報の提供による便益の受け取り	・本人（本人及び法定代理人）

1－④　統計データ、匿名加工情報の扱い

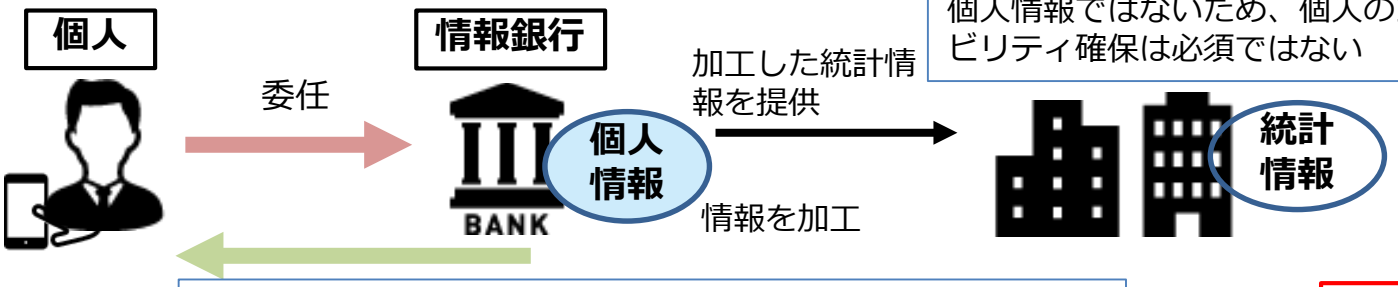
- 認定指針では、個人情報保護法の遵守や、個人のコントローラビリティ確保の観点から、情報銀行における個人情報の取扱いについて、認定基準の中で取扱いの条件を定めている。
- これらの取扱いの条件は個人情報を念頭においており、個人情報に当たらない統計データや匿名加工情報の取扱いについては、条件の対象外である。

※情報銀行や提供先第三者において個人情報の加工を行った場合でも、個人情報にあたる場合は条件の対象となる。

- 他方で、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、情報銀行が取り扱う個人情報について、統計情報や匿名加工情報として加工して活用することが想定される場合には、これによる個人への便益の有無を含め、個人に対し明示する必要がある。

● 情報銀行の取り扱う個人情報に関する主なルール

	主な項目	概要
4. 事業内容	①業務に関する個人への明示・説明	・情報銀行における個人情報の取扱い（第三者提供、利用目的）、情報銀行が個人に提供する機能とその利用について、個人に対しわかりやすく示すこと
	②情報銀行の業務（個人情報の適切な取扱い等）	・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
	③個人による情報のコントローラビリティを確保するための機能の提供	・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



- **指針に考え方を記載**

1－⑤　行政機関／独立行政法人等

- 指針ver1.0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／情報提供元／情報提供先となることを想定して整理されているが、「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関係する場合においては、同様の基準により運用されることが適当と考えられる。（ただし、指針において「個人情報保護法に基づき同意を取得する」とある箇所については、適用される法律または条例に読み替える必要がある。）
- 当然ながら、指針に定める以外にも、適用される法令を遵守する必要がある。

- **指針に記載を補足**

● 第三者提供に関する本人の同意取得に関連する法令間の差異について

- 行政機関個人情報保護法及び独立行政法人個人情報保護法では、個人情報の第三者提供の制限について、制限の外となる条件について差異があり、指針による情報銀行への要求は、法令による要求よりも範囲が広い場合がある。

項目	行政機関	独立行政法人	民間企業
第三者提供の制限	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。次に掲げる場合を除く。 一　本人の同意があるとき、又は本人に提供するとき。 二　行政機関が法令の定める所掌事務の遂行に必要な限度で保有個人情報を内部で利用する場合であって、当該保有個人情報を利用することについて相当な理由のあるとき。 三　他の行政機関、独立行政法人等、地方公共団体又は地方独立行政法人に保有個人情報を提供する場合において、保有個人情報の提供を受ける者が、法令の定める事務又は業務の遂行に必要な限度で提供に係る個人情報を利用し、かつ、当該個人情報を利用することについて相当な理由のあるとき。 四　前三号に掲げる場合のほか、専ら統計の作成又は学術研究の目的のために保有個人情報を提供するとき、本人以外の者に提供することが明らかに本人の利益になるとき、その他保有個人情報を提供することについて特別の理由のあるとき。	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。次に掲げる場合を除く。 一　本人の同意があるとき、又は本人に提供するとき。 二　独立行政法人等が法令の定める業務の遂行に必要な限度で保有個人情報を内部で利用する場合であって、当該保有個人情報を利用することについて相当な理由のあるとき。 三　行政機関（行政機関の保有する個人情報の保護に関する法律（平成十五年法律第五十八号。以下「行政機関個人情報保護法」という。）第二条第一項に規定する行政機関をいう。以下同じ。）、他の独立行政法人等、地方公共団体又は地方独立行政法人に保有個人情報を提供する場合において、保有個人情報の提供を受ける者が、法令の定める事務又は業務の遂行に必要な限度で提供に係る個人情報を利用し、かつ、当該個人情報を利用することについて相当な理由のあるとき。 四　前三号に掲げる場合のほか、専ら統計の作成又は学術研究の目的のために保有個人情報を提供するとき、本人以外の者に提供することが明らかに本人の利益になるとき、その他保有個人情報を提供することについて特別の理由のあるとき。	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。次に掲げる場合を除く。 一　法令に基づく場合 二　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。 三　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。 四　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

- 個人情報の取得にあたっての利用目的の通知・公表／明示や、開示請求に関する制限の特例に関する規定にも差異があるが、これに係わらず、情報銀行における利用目的については指針に従い、個人に対して明確にする必要がある。
- 開示請求に関する規定にも差異があるが、個人が開示の請求を行えるという規定は存在している。

1－⑥　複数者が共同で行う場合の認定

- 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、複数者が共同して情報銀行事業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、複数者が共同して運営することも考えられることから、情報銀行事業の多様な展開を見据え、複数者による認定も想定されるべきである。
- 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、複数者で運営する事業を認定することが想定される。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とともに、利用者に対する説明・損害賠償等の責任は、全ての者が連帯して負うべきである。
- なお、将来的には、認定団体において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対応も考えられる。

- **共同での申請／認定があり得る旨を指針に記載**

■ **参考：認定基準と事業／事業者との関係**

	認定項目	概要	考え方（例）
1. 事業者の適格性	①必要な経営能力	・法人格をもつこと ・業務を健全に遂行し損害賠償にも対応しうる財産的基礎を有すること	・事業者が満たす必要
	②必要な業務能力	・関係法令を遵守すること ・個人情報の取扱いに関する知識・経験及び実施・ガバナンス体制を有すること ・情報提供先の適切な監督を行うこと	・事業者が満たす必要
2. 情報セキュリティ等		・情報セキュリティ及びプライバシーに関する基準の遵守　等	・個人情報を実際に扱う事業者が満たす必要
3. ガバナンス体制	①基本理念	・情報銀行の目的に沿った企業理念、行動原則と経営責任の明確化がされていること	・事業者が満たす必要
	②相談体制	・個人や事業者からの相談に対応する体制を設けていること	・事業として満たす必要
	③諮問体制	・個人情報の第三者提供や利用について、適切性を審議するため、社外委員や専門家を含む体制を設けていること	・事業として満たす必要
	④透明性の確保	・事業に関する定期的な報告の公表など、透明性が確保されていること	・事業として満たす必要

	認定項目	概要	考え方（例）
4. 事業内容	①契約約款の策定	・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	・事業として満たす必要
	②業務に関する個人への明示・説明	・情報銀行における個人情報の取扱い（第三者提供、利用目的）、情報銀行が個人に提供する機能とその利用について、個人に対しわかりやすく示すこと	・担う者を明確にする必要
	③情報銀行の業務（個人情報の適切な取扱い等）	・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	・担う者を明確にする必要
	④個人による情報のコントローラビリティを確保するための機能の提供	・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	・事業として満たす必要
	⑤責任の範囲（損害賠償等）	・相談窓口を設置し、個人に対し一義的な説明責任を負うこと ・提供先第三者に帰責事由があり損害が発生した場合は、個人に対し賠償責任を負うこと（必要に応じ提供先第三者に求償）	・担う者を明確にする必要

※この他、個人情報を取得し、個人情報保護法上の個人情報取扱事業者となる者を明確にする必要。
※また、共同で運営する者の間で個人情報の授受がある場合には、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。（法律に沿った対応が必要。）

1－⑦　提供先第三者の選定

- 指針ver1.0では、情報銀行は個人情報を提供する情報提供先に対して、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。
- 情報銀行の利用者の安心を担保するには情報提供先は一定の水準を満たすべきであると同時に、情報銀行を通じたデータの利活用の裾野を広げることで、情報銀行の活用が広がることも期待される。
- 「情報提供先に対して認定基準に準じた扱いを求める」という原則は変わらないが、例えば情報は決められたサイトでの閲覧のみとする、物理的に渡す場合にはトークン化するなどの追加的な措置を情報銀行側が講じたり、提供先において個人情報の取扱いをよりセキュリティ水準の高い主体に委託するなどの、リスク低減を目的とした対応により、提供先の能力を補完することにより、情報銀行の安全な運用の確保と、提供先の広がりが両立されることが考えられる。
- ただし、情報銀行において提供先第三者についての判断基準を定める必要があり、これが「認定基準に準じた扱い」として認定基準を満たすことについては、どのような補完措置により同水準の安全性を実現できるかについての客観的な検証が必要である。

■「認定基準に準じて」情報提供先に求められると考えられる主な要件

	主な項目	概要
1. 事業者の適格性	①必要な経営能力	・法人格をもつこと ・業務を健全に遂行し損害賠償にも対応しうる財産的基礎を有すること
	②必要な業務能力	・関係法令を遵守すること ・個人情報の取扱いに関する知識・経験及び実施・ガバナンス体制を有すること
2. 情報セキュリティ等		・情報セキュリティ及びプライバシーに関する基準の遵守　等
3. ガバナンス体制	①基本理念	・情報銀行の目的に沿った企業理念、行動原則と経営責任の明確化がされていること
	④透明性の確保	・事業に関する定期的な報告の公表など、透明性が確保されていること
4. 事業内容	①契約約款の策定	・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
	③情報銀行の業務（個人情報の適切な取扱い等）	・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
	④個人による情報のコントローラビリティを確保するための機能の提供	・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
	⑤責任の範囲（損害賠償等）	・提供先第三者に帰責事由があり損害が発生した場合は、個人に対し賠償責任を負うこと（必要に応じ提供先第三者に求償）

※情報銀行を念頭に置いた要件のため、必ずしも全てそのまま提供先に遵守させる必要はない。

■ 情報銀行が情報提供先に求める事項

情報銀行は、以下について確実に担保できるかという基準により、情報提供先を選定するべきと考えられる。（モデル約款の記載事項より）

- 情報の利用範囲（個人から同意を得ている利用目的の範囲内での活用）
- 取扱条件の制限（セキュリティ体制）
- 情報銀行による確認、調査への協力
- インシデント発生時の対応、損害賠償

- **指針の記載を変更**

1－⑧　認定の対象とする個人情報の範囲

- 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」を認定の対象外としているが、このうち要配慮個人情報については継続検討とし、クレジットカード番号及び銀行口座番号については認定対象に加えることとした。
- 要配慮個人情報については、医療・健康分野及び教育分野について検討し、特に今後情報銀行の活用が期待される教育分野についてはニーズの具体化も踏まえて継続的に検討することとした。
- クレジットカード番号及び銀行口座番号については、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との意見があったことから、対象に追加することとした。
- 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、情報銀行において扱う場合においても当然これらを遵守する必要がある。

	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されている（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、偏見等） ・不当な差別や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される	・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、継続検討とした。 ・教育分野の要配慮個人情報の取扱いについても、今後情報銀行における活用の可能性を確認したことから、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。
クレジットカード番号	・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PCIDSS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考えられ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	・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、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考えられるとの意見があったことから、認定の対象に追加する

- **指針の記載を変更**

2. 個人による情報銀行の選択等

- 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することが期待される。
- 情報銀行が事業を行う場合、それぞれが個人に対し、情報銀行の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、契約を結ぶことで、個人にとってメリットを担保するが、例えば「信託」のように個人にとって利益を最大化することが義務づけられているわけではなく、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。
- このため、個人が情報銀行を比較し、自らにとってより有利な情報銀行を選択することが可能となることも重要であると考えられる。
- また、各情報銀行に設置が求められ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な役割を果たすと考えられる。

● 個人が情報銀行を選択する際のポイント

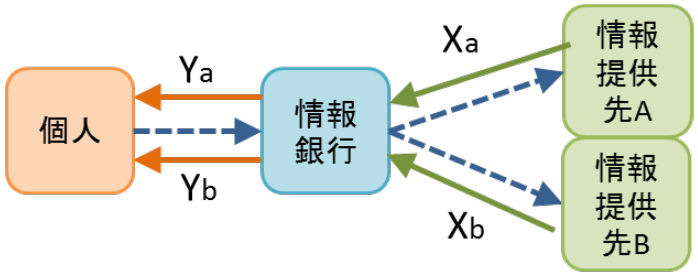
情報銀行を選択する際のポイント	認定との関係
1）事業内容について ・どのような便益を得られるか	※情報銀行から個人に説明する
2）情報銀行の業務能力、セキュリティ	※認定により一定水準を担保
3）委任する個人情報についての条件 ・個人情報の範囲 ・個人情報の提供先 ・個人情報の利用目的 ・第三者提供によるリスク・便益	※適切なUIにより個人に対し選択肢を定時する ※提供先のセキュリティ水準等については、認定により一定水準を担保 ※個人にとって著しく不利益の生じる利用については、データ倫理審査会において審査
4）コントローラビリティの機能の有無 ・個人情報の提供についてどこまで細かく指定できるか ・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

3－①　個人情報提供の対価

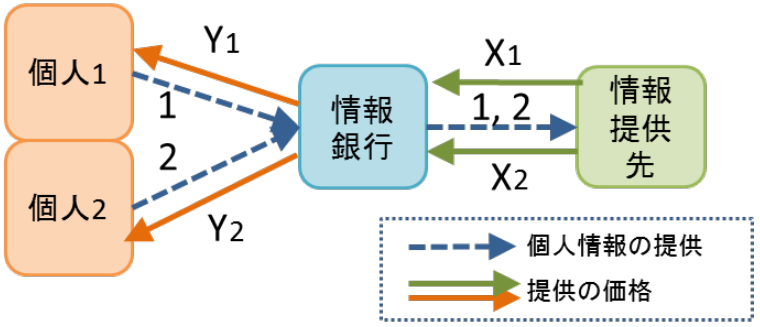
- 情報銀行は、個人情報を提供先第三者に提供することが事業の核となっており、これにより個人に何らかの便益が提供される必要がある。事業の形態によっては、情報提供先及び個人との間で個人情報提供の対価の授受が発生することも考えられる。この際には、個人情報に対する対価の設定が行われることから、その考え方を整理した。
- 個人情報に対価設定に決まった方法はなく、個人情報の紐付く個人によって、或いは提供される提供先によって、この個人情報の対価が異なるものになることもあり得る。
- 情報銀行は営利事業として運営される場合が多いと想定されることから、個人情報の対価は、基本的に情報銀行において自由に設定されるものと考えられる。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、価格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の、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、消費者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消費者に対して開示されることが必要。

● 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。



3－2. 情報銀行に関する透明性の確保

- 情報銀行事業の健全な発展のためには、透明性の確保が必要であり、指針ver1.0では、情報銀行サービスを利用する個人に対する、自らの情報へのコントローラビリティの確保のために必要な情報開示及び、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、開示／公表の必要な内容について定めている。
- これに加えて、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にも、一定の情報公開が必要と考えられ、情報銀行の公表するべき内容として、個人の受ける便益の考え方、データポータビリティ機能の有無等、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こととする。
- さらに、認定団体において、認定した情報銀行について、個人のメリットを整理して公表することにより、個人による適切な選択を後押しすることも考えられる。

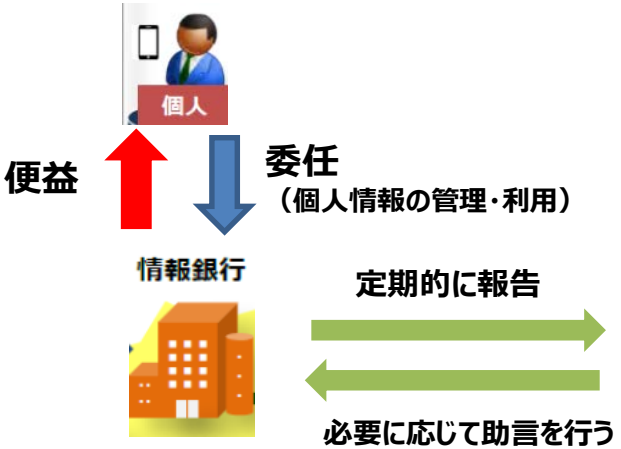
	考え方	認定指針における記述（案）
個人（利用者）への明示	個人（利用者）が自身に関する個人情報に対してコントローラビリティを確保するために必要な情報	・提供先第三者、利用目的、契約約款に関する重要事項の変更などを個人にわかりやすく開示できる体制が整っていること ・個人のコントローラビリティを確保するための機能の提供について ・提供先第三者や利用目的の内容に応じ、必要な場合には個人に対するリスクを情報銀行は適切に伝える必要がある
定期的な事業報告の（一般への）公表	個人（利用者）、取引事業者を含めた、関係者によるガバナンスの確保	・透明性を確保（事業に関する定期的な報告の公表など）すること
利用者となる可能性のある個人への公表	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内容（当該情報銀行による個人への便益の考え方、データポータビリティ機能の有無など）を公表すること

- **指針に記載を追記**

3－3. データ倫理審査会

- 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目的とすることを基本的な考え方としており、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成するものだが、それぞれが適切に機能するためには、一定の共通認識が持たれることが望ましい。このため、データ倫理審査会において審議するべき基本的な内容について整理する。
- 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、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。

- **指針の記載を変更**



データ倫理審査会（仮称）

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

●情報銀行事業について、以下の事項についてその適切性を審議し、必要に応じて助言を行う
・個人と情報銀行の間の契約の内容
・情報銀行の委任した個人情報の利用目的
・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）
・第三者提供先の選定方法

●運営方法
・構成員及び議事録は公開する
・必要に応じ情報銀行から調査・報告を求めることができる

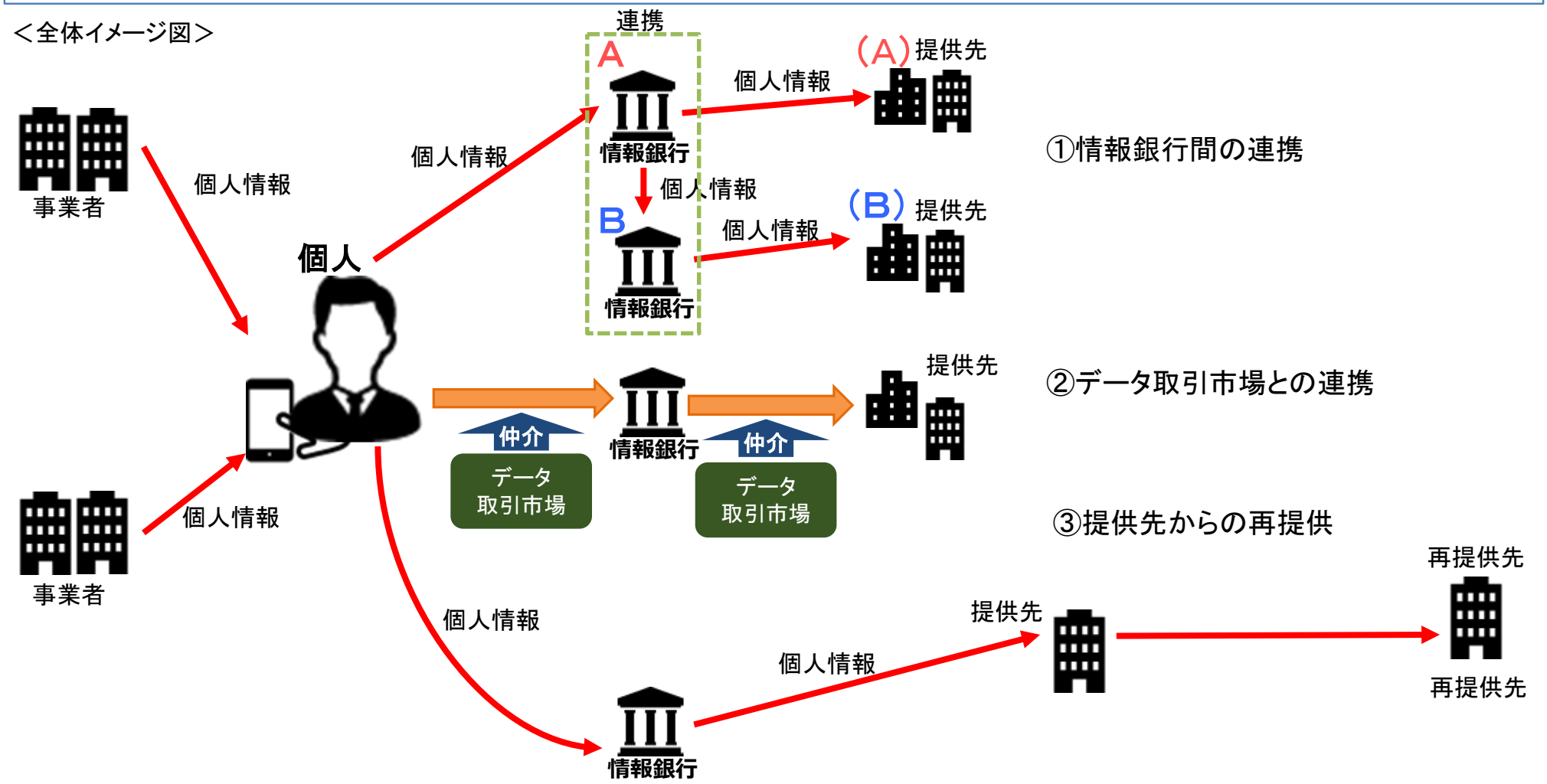
■ データ倫理審査会における審議の考え方
- 情報銀行は、個人のために個人情報の管理・第三者提供を行うということが基本的な考え方となる。このため、利用者たる個人の視点に立ち、適切な運営が行われているかという視点から審議することが必要である。
- このため、情報銀行の事業内容が個人の利益に著しく反していないかという観点から、審議する必要があると考えられる。

（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
・個人にとって著しく不利益となる利用がされていないか／個人に対しこれ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

3. プレイヤー間の連携

- 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目的を達成するという観点からは、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のプレイヤーとの間の円滑なデータ流通が重要であり、このためには、プレイヤー間の連携が進むことが望まれる。
- このため、情報銀行の普及が更に進んだ場合における、情報銀行同士の連携、情報銀行とデータ取引市場との連携、情報提供先からの再提供について、現状の認定指針に照らした考え方の整理を行った。

＜全体イメージ図＞

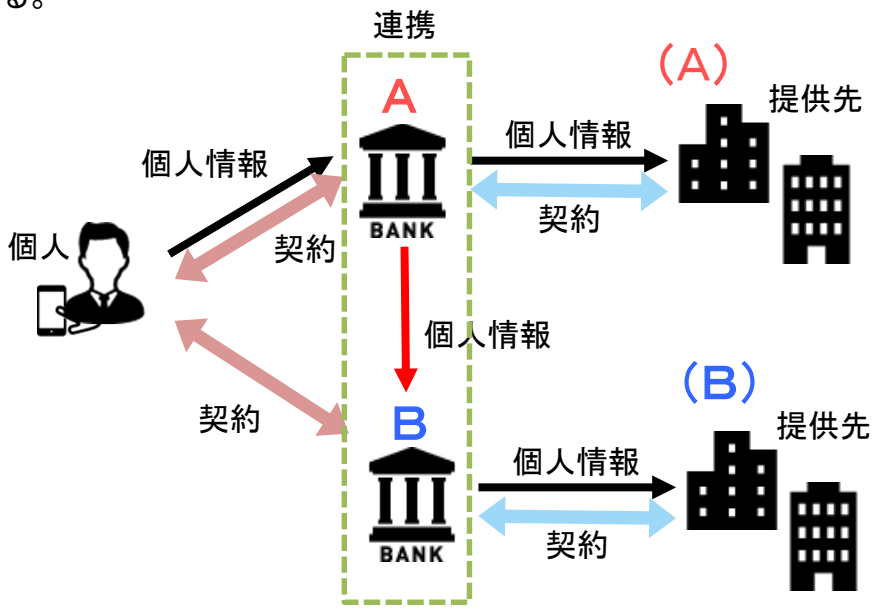


3－①　情報銀行間の連携

- 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できる。
- さらに、情報銀行間のデータポータビリティ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、情報銀行の展開が進んだ場合には、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データ形式や伝送方式の標準化についても必要である。

● 情報銀行間の連携

- 情報銀行間の連携が進むことで、個人はより容易に、複数の情報銀行を利用することができる。
- 情報銀行間の連携を促進するためには、データの移行と利活用を容易にするために、データ形式や伝送方式の標準化の検討も必要となる。

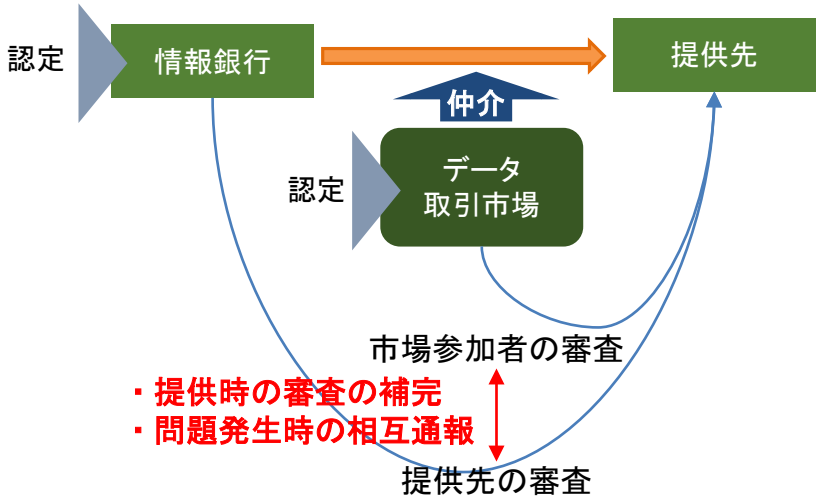


情報銀行Aが個人と情報銀行Bの契約を代行して個人の負担を減らすなど、
個人にとって利便性の高い形での連携が進むことが期待される。

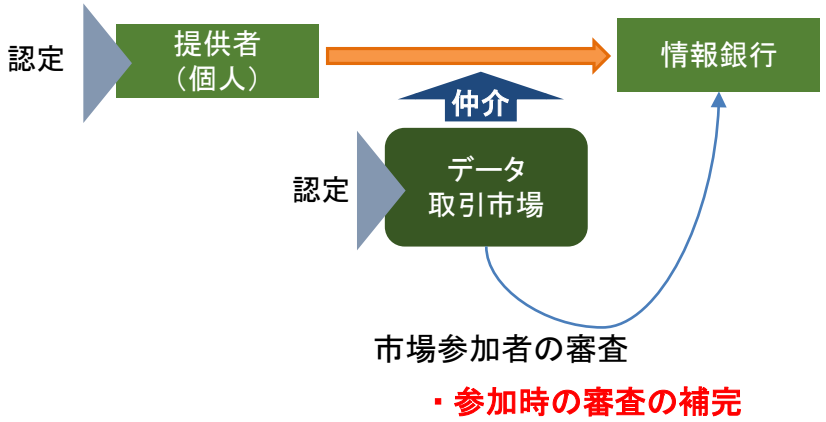
3－②　情報銀行とデータ取引市場の連携

- 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、売買と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。
- 指針では、情報銀行は情報提供先に対し、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している。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おり、満たすべき事項に共通点がある場合、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場合、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、データの利活用の更なる進展が期待される。

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



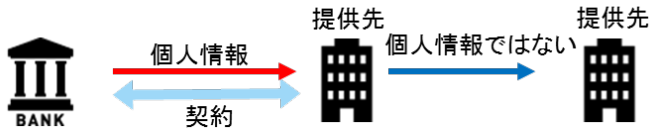
3－③　情報提供先からの再提供

- 指針の記載を変更

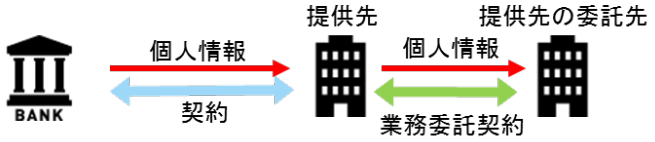
- 指針ver1.0においては、情報提供先からの再提供を禁止しているが、情報銀行から提供先に提供されたデータの別の第三者への提供が全く認められない場合、活用の範囲が相当程度狭まると考えられる。以下の考え方の下、提供先から別の第三者への提供が認められる場合について整理した。

【考え方】指針ver1.0では、以下について確実に満たすため、再提供を認めないこととしている。
①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
②情報銀行が提供先での個人情報の適切な取扱いについて監督し、提供先における問題発生時の責任も負うこと

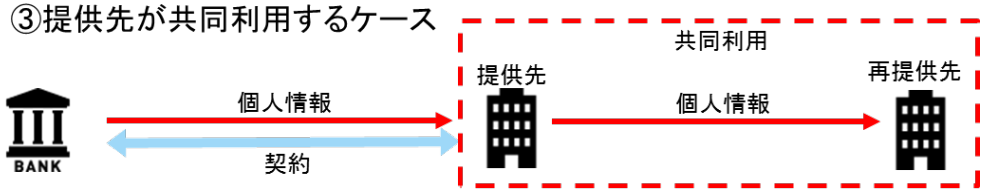
①提供先において加工するケース（個人情報でない）



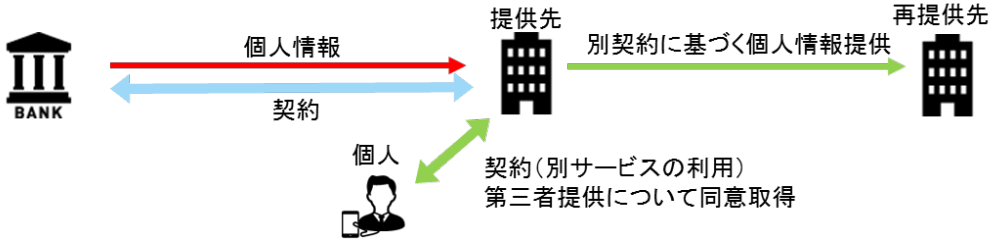
②個人情報を委託するケース



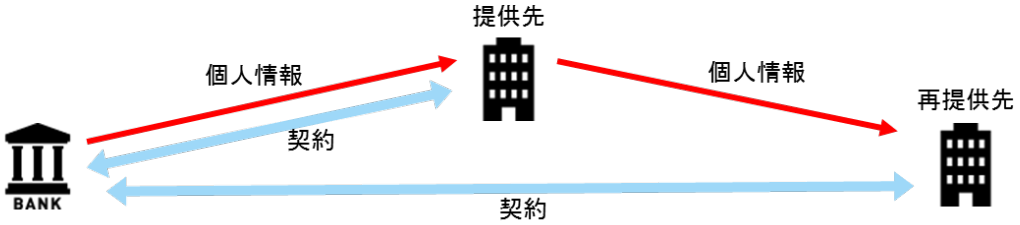
③提供先が共同利用するケース



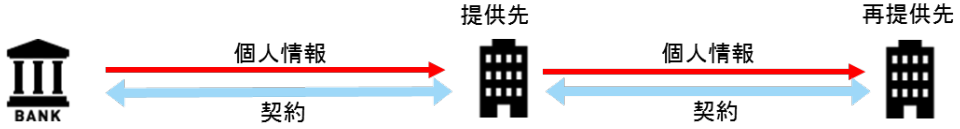
④個人が提供先のサービスを利用し、直接契約を結ぶケース



⑤情報銀行が再提供先と新たに契約を締結するケース



⑥①～⑤に当てはまらない再提供のケース



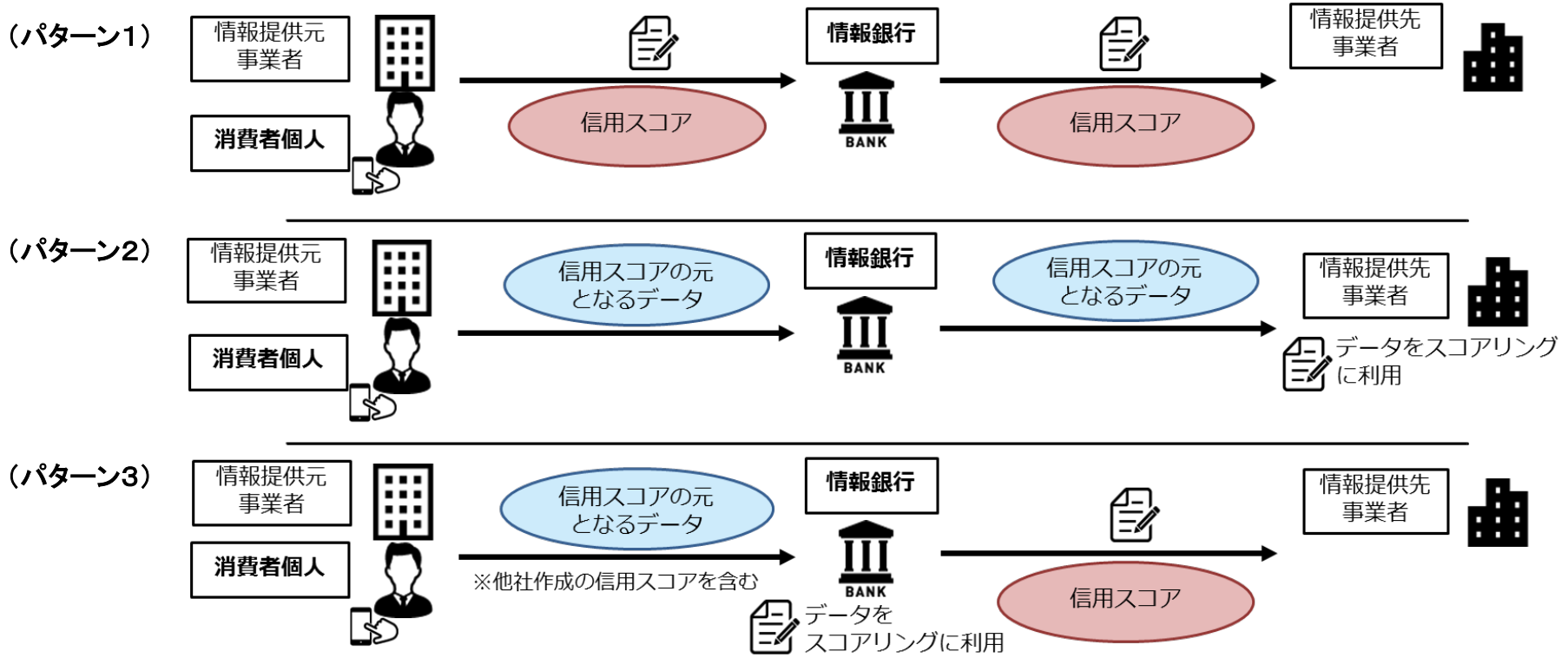
3－③　情報提供先からの再提供

「再提供」等のパターン	考え方
①提供先で情報を加工したことにより、提供される情報が個人情報ではない場合	• 個人情報の再提供を禁止しているため、個人情報にあたらない情報であれば、再提供は制限されない。 • ただし、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。 →認められる
②委託にともなって個人情報を提供する場合	• 提供先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。 →認められる
③提供先での共同利用にともなって提供する場合	• 共同利用にともなってデータ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。またこの場合、予め一定の情報について本人に通知することが求められる。 • ①を満たすため、個人が共同利用が行われる事業者の範囲を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。 • ②を満たすには、情報銀行と再提供先の間には直接の契約がなされる必要がある。 →提供先が個人と直接契約を結ぶ場合（④に該当）または情報銀行が共同利用を行う全ての者と契約する場合（⑤に該当）に限り、認められる
④個人が提供先のサービスを利用し、直接契約を結ぶ場合	• 個人と提供先が別にサービス提供に関する契約を結び、当該サービスに関するデータを再提供する場合であれば、情報銀行の責任が及ぶ範囲の外であると整理できる。 • 再提供については、提供先の責任において、個人から適切に同意を取得する必要があり、情報銀行の監督の範囲外であることを明らかにする必要がある。 →認められる
⑤情報銀行が再提供先と新たに契約を締結する	• ①を満たすため、提供先からさらに再提供先に提供することについて、事前に同意を取得する必要がある。 • ②を満たすことに関しては、情報銀行が再提供先と新たに契約を締結することで、情報銀行から直接提供する場合と同じ条件が確保されると整理できる。 →認められる
⑥再提供先について、事前に同意を取得する	• 情報銀行と再提供先の間には直接の契約がなされないため、②情報銀行が再提供先の監督を行うことはできない。 →認められない

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、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スコアや、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「ソーシャルスコア」いついては、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。
- 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

● 情報銀行において信用スコアを取り扱う場合の留意点

- 情報銀行は、「個人のために情報を活用する」ことを目的の基本としており、信用スコアを扱う場合は、個人にとって不利な利用とならないよう、特に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「ソーシャルスコア」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。

① 同意取得

（パターン1） 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が必要である。

（パターン2） 情報銀行は、個人に対し、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が必要である。

② 信用スコアの利活用

（パターン1） 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、提供先において、個人にとって不利益となる利用がなされ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が望ましい。

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が望ましい。

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、遺伝情報など、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することについては慎重に行動するべきである。

（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、遺伝情報など、差別に繋がる過去の情報を基礎データとして用いることについては慎重に行動するべきである。

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必要がある。

⑥ 人間の関与

（パターン3） 信用スコアの数値化において、機械化された処理の場合に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が必要である。

5. 今後の情報銀行の展開に向けたその他の取組み

- 指針に基づく認定の普及により、認定を受けた情報銀行について信頼性を確保し、消費者が安心してできるようにするとともに、認定された情報銀行の選択・普及を促すことで、一定の水準を保った情報銀行の普及を促すことが期待される。
- その他にも、今後情報銀行の社会的な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

情報銀行によるメリットを個人がより享受できるようにするためには、個人が自身のパーソナルデータに関与を及ぼし、利活用することに関する意識の向上と、情報銀行に対する正しい理解が進むよう、関係者において普及啓発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。（P）

● 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望まれる。

別添

4/26の検討会を受けて追記予定

「情報信託機能の認定に係る指針ver●」（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

平成31年●月

１．本指針の基本的な運用について

＜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、認定を行う団体は、本指針に基づき、認定制度を構築・運用する

・　「認定」はあくまで任意のものであり、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＞

・　本指針に基づく認定は、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の委任を受け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。

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情報銀行に行う認定

（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、多様な進化がされることが期待される。

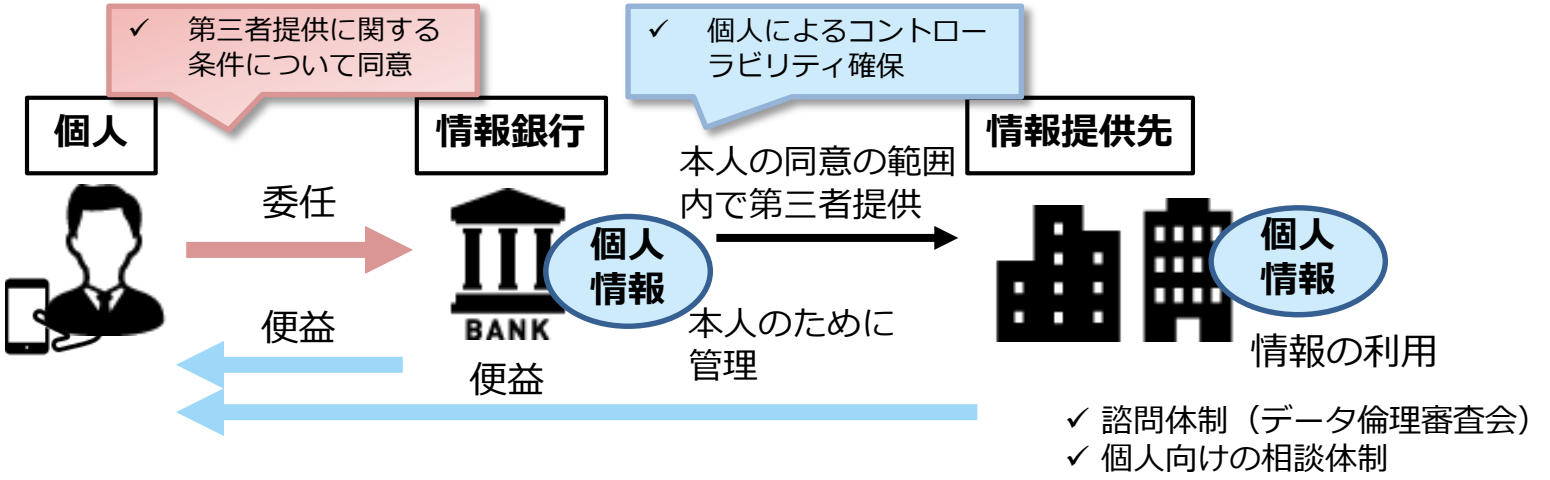
本指針における情報銀行の定義

定義の再整理

【目的】
- 「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、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、使いやすいユーザインタフェースを用いて、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、第三者提供先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。

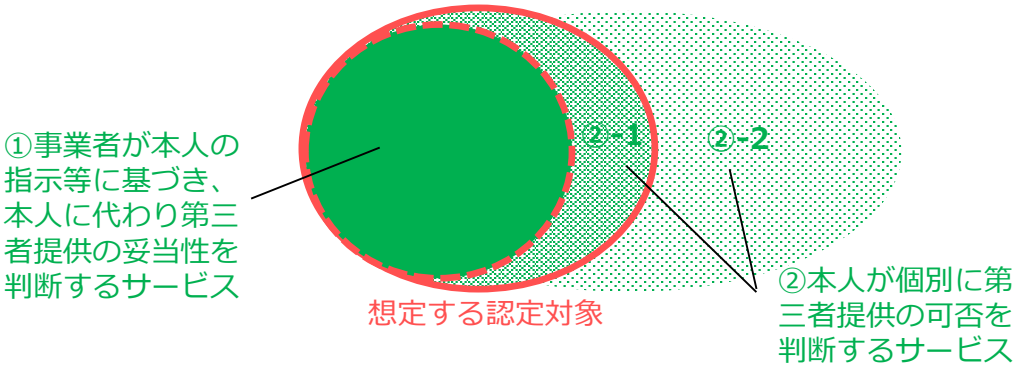


本指針の対象とするサービス

（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が基本であるが、様々な形態の事業の出現を想定し、②本人が個別に第三者提供の可否を判断するサービスも含むこととする。（※）

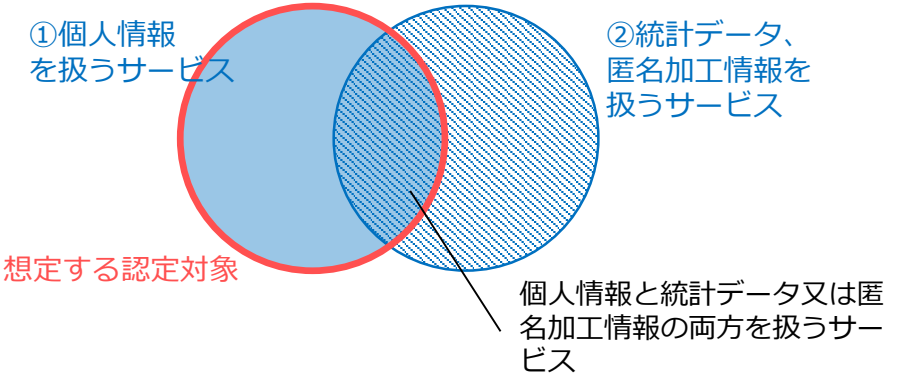
※②本人が個別に第三者提供の可否を判断するサービスのうち、提供事業者が情報の提供先を選定して個人に提案する場合など、提供事業者が比較的大きな役割を果たす（責任をもつ）ケース（②-1）を想定。他方、純粋なＰＤＳなどデータの管理や提供に関し個人の主体性が強いサービス（②-2）まで認定の対象として想定している訳ではない（認定がないことをもって信頼性が低いと評価されるべきものではない）。
※なお、データ保有者と当該データの活用を希望する者を仲介し、売買等による取引を可能とする仕組み（市場）である「データ取引市場」については認定の対象外。



（２）事業で扱うデータの種類

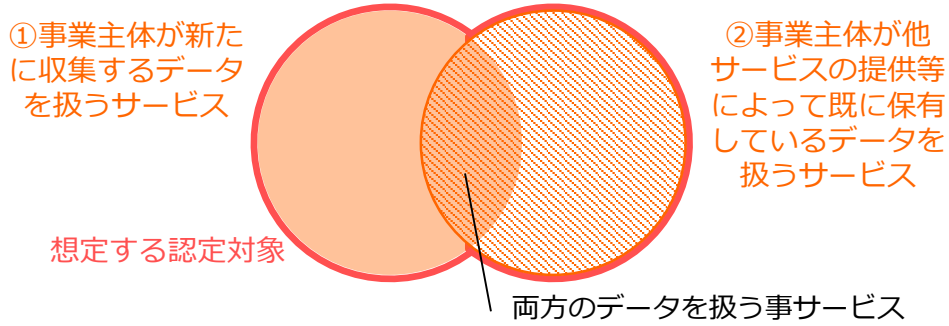
- 本指針は、個人情報を扱う事業を対象に、安心して利用出来る情報銀行という観点から認定要件を定めており、個人情報を全く扱わない事業は対象としない。

※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。（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情報の提供（情報銀行における個人の利用目的）やこれ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。



（３）データの収集方法

- 本指針に基づき認定する事業者としては、情報銀行事業以外の事業を行う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おいても、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（情報銀行と同水準の安全・適切な個人情報の扱いの確保）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

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」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①

項目	内容
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
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
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
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
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
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
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
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②

項目	内容
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
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
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）
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
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
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
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
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

プライバシー保護対策についても遵守するべき旨を明確化

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

Table 3 – The privacy principles of ISO/IEC 29100

1. Consent and choice
2. Purpose legitimacy and specification
3. Collection limitation
4. Data minimization
5. Use, retention and disclosure limitation
6. Accuracy and quality
7. Openness, transparency and notice
8. Individual participation and access
9. Accountability
10. Information security
11. 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適切な選択に資する内容（当該情報銀行による個人への便益の考え方、データポータビリティ機能の有無など）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
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）
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）（※１） ・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 ・対象となる個人情報とその取得の方法、利用目的 ・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
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（同意の取得を含む）をはじめ、関係する法令を遵守すること ・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、統計情報等への加工について ・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 （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再提供（※２）の禁止 ・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 ・個人情報を加工した匿名加工情報を提供する場合には、提供先第三者に対し匿名加工情報である旨を明示すること ・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について規定すること

（※1）行政機関個人情報保護法、独立行政法人個人情報保護法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は、当該法令に基づく同意を取得する。
（※2）「再提供」に該当するか否かは、個人情報に対する個人のコントローラビリティ（第三者提供の同意の適切な取得を含む）の確保と情報銀行による提供先の監督について、担保されるか否かによって判断されるべきである。

４）事業内容②

項目	内容
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、その旨を明示すること
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（仮称））の基本的な概要

説明の追加

便益

委任
（個人情報の管理・利用）

情報銀行

定期的に報告

必要に応じて助言を行う

データ倫理審査会（仮称）

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

●情報銀行事業について、以下の事項についてその適切性を審議し、必要に応じて助言を行う
・個人と情報銀行の間の契約の内容
・情報銀行の委任した個人情報の利用目的
・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
・第三者提供先の選定方法

●運営方法
・構成員及び議事録は公開する
・必要に応じ情報銀行から調査・報告を求めることができる

■ データ倫理審査会における審議の考え方
- 情報銀行は、個人のために個人情報の管理・第三者提供を行うということが基本的な考え方となる。このため、利用者たる個人の視点に立ち、適切な運営が行われているかという視点から審議することが必要である。
- このため、情報銀行の事業内容が個人の利益に著しく反していないかという観点から、審議する必要があると考えられる。

（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
・個人にとって著しく不利益となる利用がされていないか／個人に対しこれによるリスクが伝えられているか

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

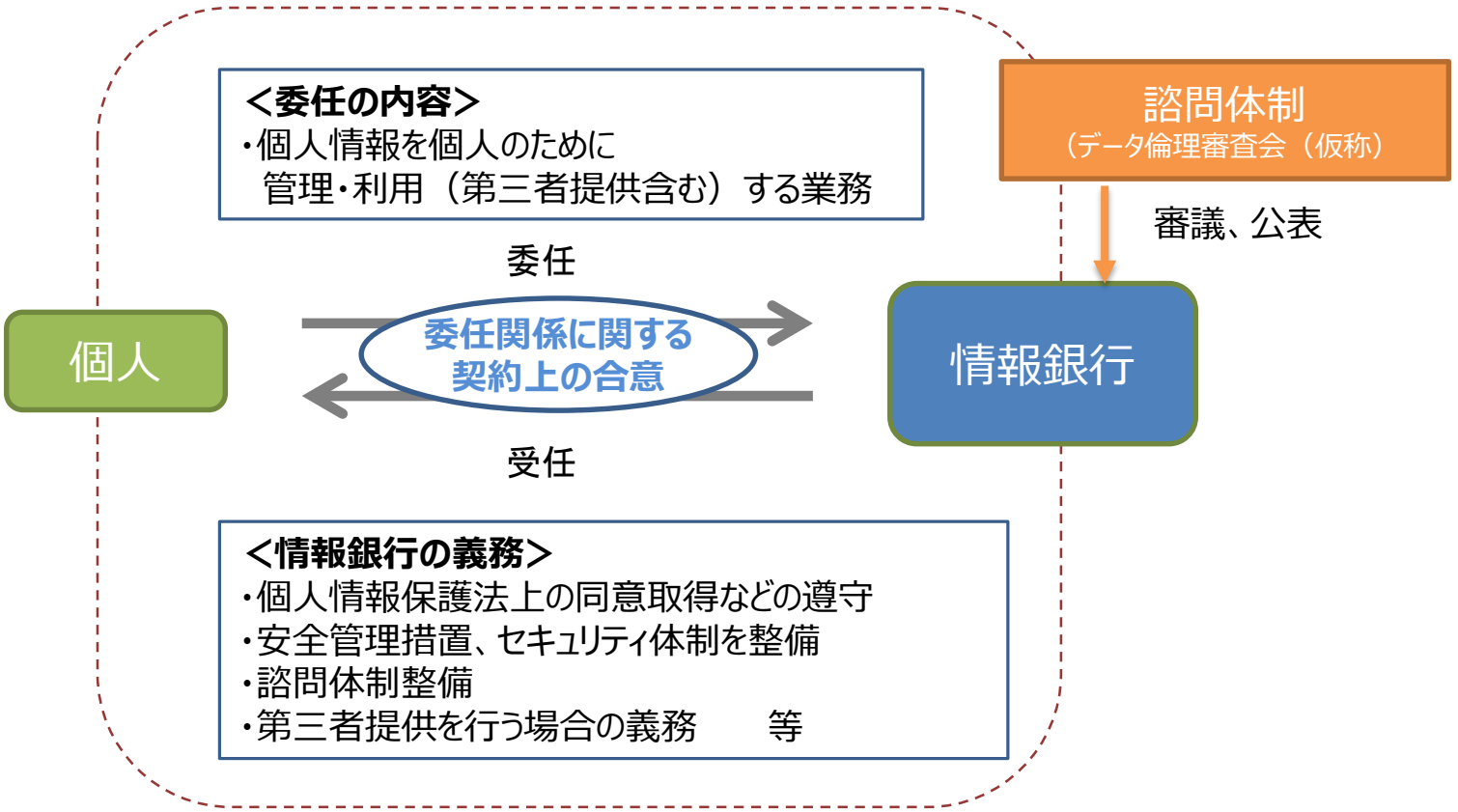
■　情報信託機能を提供する「情報銀行」のサービスについて、債権債務の内容や情報銀行の責任範囲を明確化するため、**個人と情報銀行の間を委任関係に関する契約上の合意**と整理する。

■　「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：個人が未成年者・成年被後見人の場合】

本指針では、①同意を行う者と②契約を行う者は、同一の人物として想定しているが、個人が未成年者や成年被後見人の場合など、両者が異なる場合は、両者が異なる場合もある。

✓①の同意については、個人情報保護法上の「本人の同意」を行う「本人」が行う。（個人が情報銀行との間で行う手続きのうち、「本人の同意」に係わるものについては、「本人」が行う。）

✓②の契約については、未成年・成年被後見人等であれば親権者・法定代理人等の確認が必要となる。

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

（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再提供は禁止する
・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（情報銀行と同水準の安全・適切な個人情報の扱いの確保）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等）

３）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

４）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

５）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

６）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