資料18－2

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）

令和3年〇月〇日

情報信託機能の認定スキームの在り方に関する検討会（第15回～第18回）

■ 構成員 （敬称略、五十音順、令和3年6月14日現在）

	生貝　直人 （第16回～）	一橋大学大学院法学研究科　准教授
	石原　遥平	一般社団法人シェアリングエコノミー協会 シェアリングエコノミー認証制度統括　ディレクター・弁護士
	伊藤　直之	株式会社インテージ　事業開発本部　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　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
	高口　鉄平	静岡大学学術院情報学領域　教授
	小林　慎太郎	株式会社野村総合研究所 ICTメディアコンサルティング部 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
	日諸　恵利	みずほ情報総研株式会社　社会政策コンサルティング部 医療政策チーム　医療産業課　チーフコンサルタント
	藤本　洋史	情報信託機能普及協議会　理事
	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 サステナビリティ消費者会議　代表
	真野　浩	一般社団法人データ社会推進協議会　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 慶應義塾大学　政策・メディア研究科　特任教授
	森　亮二	英知法律事務所　弁護士
	森下　哲朗	上智大学法学部　教授
	森田　弘昭	株式会社マイデータ・インテリジェンス 取締役執行役員COO
	山本　龍彦	慶應義塾大学法務研究科　教授
	湯淺　墾道	明治大学公共政策大学院ガバナンス研究科　教授
	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

■ 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

一般社団法人日本IT団体連盟

■ 事務局

総務省情報流通行政局情報流通振興課デジタル企業行動室

経済産業省商務情報政策局情報経済課

とりまとめの概要

- 令和元年10月、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及び「情報信託機能の認定に係る指針Ver2.0」を公表。とりまとめにおいては、情報銀行に関する基本的な考え方や、提供先第三者の選定、データ倫理審査会、情報銀行間の連携等に関して整理・明確化を行った。
- その後、情報銀行の認定が進み、認定・運用の過程において顕在化した課題に対して追加の議論が必要とされたことを踏まえ、令和2年7月～令和3年6月に検討会及び検討会のもとに設置した認定・運用ワーキンググループを開催した。
- 本とりまとめは、検討会において整理した以下の項目について、とりまとめたものである。また、整理した内容を中心に、指針Ver2.0を見直した指針Ver2.1を添付する。

➢ **整理を行った項目**

1. 健康・医療分野の情報の取扱い
2. 提供先第三者の選定について
   - 2－① PマークとISMS認証に加えて許容される第三者認証等
   - 2－② 提供先第三者の選定に係る記載の明確化
3. 統制環境に問題のある事業者の扱い
4. 再提供禁止の例外について
   - 4－① 情報銀行間連携の考え方
   - 4－② 再提供禁止の例外の具体例
5. 世帯の複数の構成員が利用する機器等から取得される情報の利用について

1．健康・医療分野の情報の取扱い

- 指針ver2.0では、要配慮個人情報は認定対象外であり、今後の取扱いは継続検討とされた。
- 一方、要配慮個人情報のうち、健康・医療分野の情報については、安全に配慮した上で、本人や社会のために情報銀行において活用するニーズは高いとの意見が多く出ている。
- 健康・医療分野の情報は、本人が情報自体の意味や、その情報から推定され得るリスク、本人以外への影響等を十分に理解していないことが多く、その特殊性から、情報銀行で取扱う情報については、本人に明示的に開示・説明されており、本人が十分に理解している情報であることが必要である。
- この観点から、情報銀行で取扱う情報の検討にあたり、健康・医療分野の情報のレベル区分を行い、その考え方を整理した。

■ **情報銀行で取扱う健康・医療分野の情報のレベル区分（レベルが上がるほど慎重な取扱いが必要）**

	情報区分	考え方、情報項目例
レベル0	本人の同意を必要とせずに取得・提供可能な、個人情報に該当しない情報	・統計データ ・匿名加工情報
レベル1	本人の同意に基づいて取得・提供可能な、要配慮個人情報に該当しない健康・医療分野の個人情報	・本人に対して医師その他医療に関連する職務に従事する者により行われた疾病の予防及び早期発見のための健康診断その他の検査の結果ではなく、健康診断、診療等の事業及びそれに関する業務とは関係ない方法により知り得た個人情報※ ※例えば、本人の病歴や個人情報の保護に関する法律施行令第2条第1号から第3号までの事項を内容とする記述等は含まれない 【例】歩数、体重、体脂肪、体温、血圧、脈拍　等のバイタルデータ
レベル2	本人同意と医療専門職（医師、歯科医師、薬剤師、保健師等）の助言に基づいて情報銀行が取得し、データ倫理審査会において医療専門職の助言と承認に基づいて提供可能な、健康・医療分野の要配慮個人情報	・本人に明示的に開示・説明されており、本人が十分に理解している医療情報 【例】法定健診項目（既往歴含む）、アレルギー、お薬手帳、OTC医薬品　等
レベル3	レベル2において取り扱いを保留する情報	・レベル2情報に含まれない情報 【例】レベル2情報に含まれない検査結果、腸内細菌、口腔内細菌、遺伝子情報　等

1．健康・医療分野の情報の取扱い

- 認定指針においては、レベル区分に基づき、第１段階として、指針ver2.0で取扱い可能な統計データ・匿名加工情報（レベル0情報）及び要配慮個人情報に該当しない健康・医療分野の個人情報（レベル１情報）の取扱いについて追記を行う。
- 今後は、PHRの検討状況と整合を図りながら、第２段階として、要配慮個人情報に該当する情報（レベル2情報）の取扱いについて、対象情報や同意・審査要件等を継続的に検討し、認定指針の改定を行うことが望ましい。

【参考】レベル１情報（健康・医療分野の個人情報のうち、要配慮個人情報に該当しないもの※）の内容

※本人の病歴や個人情報の保護に関する法律施行令第2条第1号から第3号までの事項を内容とする記述等は含まれない。

・本人に対して医師その他医療に関連する職務に従事する者により行われた疾病の予防及び早期発見のための健康診断その他の検査の結果ではなく、健康診断、診療等の事業及びそれに関する業務とは関係ない方法により知り得た個人情報であって、例えば以下のもの。

	項目
1	歩行測定（歩数・歩幅・ピッチ・接地角度・離地角度・外回し距離）
2	体重
3	体脂肪
4	体温
5	血圧
6	脈拍
7	心拍数
8	消費カロリー
9	摂取カロリー
10	睡眠時間
11	月経日

	項目
12	内臓脂肪レベル
13	水分量
14	筋肉量
15	骨量
16	タンパク質
17	基礎代謝
18	皮下脂肪
19	呼吸数
20	酸素飽和度（取り込まれた酸素のレベル）
21	ストレスチェック
22	肌の状態
23	視力

2. 提供先第三者の選定について

- 提供先第三者の選定に係る以下の指針Ver2.0の記載について、PマークとISMS認証に加えて許容される第三者認証等を明確化すべき、第三者認証等を取得していない例外ケースではどのような情報・手法が認められるのか明確化すべきといった課題が生じたことから、整理が必要である。

1）事業者の適格性
②業務能力など

・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（※）**

1－①　PマークとISMS認証に加えて許容される第三者認証等について

（※）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。

1－②　提供先第三者の選定に係る記載の明確化について

２－①　PマークとISMS認証に加えて許容される第三者認証等

- 指針および認定基準の「提供先第三者の選定基準」が厳しく、提供先が限られてしまうことが、認定取得および認定情報銀行の普及拡大の妨げになっていることから、PマークとISMS認証に加えて許容される第三者認証等について、明確化することが必要である。

  なお、FISC安全対策基準に基づく安全管理措置がなされている事業者については、既に運用上許容しているため、指針に明示することとしたい。

- 提供先がPマークまたはISMS認証を取得していないが、以下の業種別ガイドラインにおける安全管理措置を遵守している事業者※の場合には、既存の第三者認証等の取得に相当するものとみなす。
  ※遵守しているか否かは認定団体により審査される

  ・電気通信事業における個人情報保護に関するガイドライン（「電気通信事業者」（同第２条１号））
  ・放送受信者等の個人情報保護に関するガイドライン（「受信者情報取扱事業者」（同第３条３号））
  ・金融分野における個人情報保護に関するガイドライン（「金融分野における個人情報取扱事業者」）

- 上記に加え、例えば以下のような業法や業種別ガイドラインなどに従い安全管理措置が確保されていると認められる事業者の場合も、同様に提供先とすることが考えられる。

  ・電気事業法（「認定電気使用者情報利用者等協会（同改正法（2022.4施行）第３７条の４）の認める提供先」）
  ・空港分野における情報セキュリティ確保に係る安全ガイドライン（「空港分野の重要インフラ事業者」）
  ・ MaaS 関連データの連携に関する ガイドライン Ver.1.0（「プラットフォーム運営者」、「データ利用者」）

2－①　PマークとISMS認証に加えて許容される第三者認証等

- 一方、提供先第三者は、Pマーク等第三者による認証（信用）を取得する動機が低く、また、提供先第三者には、大企業の“一店舗・一部門”や “中小企業(店舗)”が一定数存在するが、企業の“一店舗・一部門”単位では、原則Pマークを取得できない。そのため、大企業の“一店舗・一部門” を想定した、Pマーク、ISMS認証に加えて許容される新たな“プライバシー保護認証”を、提供先選定条件に加えることが考えられる。

- 本検討会及びその下のWGでの議論を踏まえ以下の新たな第三者認証等の候補の内、Pマークの部門認証の例外措置を適用し、情報銀行の特性を見定めて安全管理措置を選択した、「Pマーク情報銀行版（仮称）」について、認定団体を中心に検討を進めていくこととする。

	基準	認証機関
Pマーク情報銀行版(仮称)	JIS Q 15001:2017 （ISMSを参照）	JIPDEC
既存の部門 JIS Q 15001	JIS Q 15001:2017 （ISMSを参照）	ア 日本規格協会ソリューションズ
		イ BSIグループジャパン
		ウ 日本品質保証機構（JQA）
		エ SGSジャパン
ISO 27701	ISMS （ISO 29100を参照）	未定
独自基準	JIS Q 15001ベース	未定

２－①　PマークとISMS認証に加えて許容される第三者認証等

- 今後、WGおよび検討会親会にて採用が決定された認証等※については、その名称を指針に追加する。
  ※「等」には、一定の基準を満たすことが客観的に担保されるものが該当する。

- 指針に明示された認証等に加え、認定の運用上、認定団体が許容すべきと判断する認証等が生じた場合には、当該認証等を認めることが、提供先につき「情報銀行と同様、認定基準に準じた扱い」をするものといえるかを認定団体において判断できるものとする。

- 認定団体が指針に明示された以外の認証等を採用した場合、指針において当該認証等を明示するかにつき検討会等の場において有識者の意見を聞くこととする。

2－② 提供先第三者の選定に係る記載の明確化

①提供先は閲覧のみの場合

- 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場合、転記、複写等の目的外利用を排除するため以下の対応が必要となる。

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

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

- 情報は情報銀行が管理し、**提供先とは転記・複写禁止の契約を締結し、一覧での閲覧や任意検索ができない方法で、一人分のみ検索できる技術的対策を施した上で、**必要な情報の閲覧のみができることとする。

2－②　提供先第三者の選定に係る記載の明確化

②提供先が個人を識別できないよう加工する場合

- 提供先で特定の個人を識別できないようにするためには、提供データ自体に個人情報が含まれないようにする必要があるため、特定の個人を識別する記述等を除くこと（規則1号の加工※）および個人識別符号を除くこと（規則2号の加工）が必要である。

※　以下「規則〇号の加工」という場合、個人情報の保護に関する法律施行規則第19条各号の加工をいう。

✓ 規則1号の加工における特定の個人を識別することができる記述等としては、個人情報保護委員会事務局レポート※に記載のある、以下の項目を参照する。

※　2017年2月「匿名加工情報　パーソナルデータの利活用促進と消費者の信頼性確保の両立に向けて」

(1) 本人の氏名
(2) 生年月日、連絡先（住所・居所・電話番号・メールアドレス）、会社における職位又は所属に関する情報について、それらと本人の氏名を組み合わせた情報
(3) 防犯カメラに記録された情報等本人が判別できる映像情報
(4) 本人の氏名が含まれる等の理由により、特定の個人を識別できる音声録音情報
(5) 特定の個人を識別できるメールアドレス
(6) 個人情報を取得後に当該情報に付加された個人に関する情報
(7) 官報、電話帳、職員録、法定開示書類（有価証券報告書等）、新聞、ホームページ、SNS等で公にされている特定の個人を識別できる情報

※住所であれば「〇〇市」まで（人口の多い都心部であれば、「〇〇区」まで）、生年月日であれば「生年月」まで、あるいは「生年」までといったように、情報の項目それぞれについて一定程度曖昧化されるように部分的な削除や置換えを行う考え方が想定される。また、住所・生年月日・性別等の複数の項目の組合せで一意にならないように各項目の加工レベルを調整する考え方も想定される。
携帯電話番号や電子メールアドレス、SNS 等のID、クレジットカード番号等は、多数の事業者においてそれぞれユーザーから取得されていることを踏まえると、他の事業者が保有している個人情報との間で識別子的な機能も有することから、部分的な削除だけでは、残った情報を起点として個人の特定につながる可能性も高くなると思われるため、基本的には、全部削除することが望ましい。

✓ 同レポートでは、講ずるべき措置として、「記述等の全部又は一部を削除すること（当該全部又は一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）」が求められている。

2－②　提供先第三者の選定に係る記載の明確化

- 提供しても安全といえるような処理としては、①前頁に加えて、規則4号の加工（一般的に特異な情報の削除等）および5号の加工（提供先で個人情報と照合できないようにすること）を行うことが必要と考えられる。もっとも、履歴は原則として※そのままでよいものとする。また、②匿名加工情報相当のものにして提供することも可能である。

  ※　移動履歴等の個人特定性の高い履歴データを除く。

- 提供先において特定の個人を識別できないよう、**当該個人情報に含まれる記述等の一部の削除処理（当該一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）を行い、**提供先に提供する

- 本検討会下のWGにおいては、上記の結論が示されたものの、
  - 提供先で特定の個人を識別できないようにする加工として、匿名加工情報に求める加工基準に近い加工を求めることは、データ倫理審査委員会による審査等、安全な提供先の選定のための他の規律を有する認定情報銀行においては過剰な制限である
  - 各社の事業に応じた独自の安全管理措置の余地がなくなる

  といった理由から、今後の情報銀行事業の拡大の妨げとなる旨の意見があった。
  このことから、加工基準については、今後も運用の拡大に伴い見直しを検討することが望ましい。

2－② 提供先第三者の選定に係る記載の明確化

（参考）仮名加工情報、匿名加工情報との差異について

	匿名加工情報	本案（指針）	仮名加工情報※
定義	特定の個人を識別することができず、加工元の個 人情報を復元することができないように加工された個人に関する情報	提供先において特定の個人を識別できないよう、個人情報の一部の置き換え等の処理を行い、復元に必要な情報を除いた情報	他の情報と照合しない限り特定の個人を識別す ることができないように加工された個人に関する情報
加工基準	特定の個人を識別することができる記述等の 全部又は一部の削除又は置換（規則第19条第１号）	**特定の個人を識別する情報を除くこと** (1) 本人の氏名 (2) 生年月日、連絡先（住所・居所・電話番号・メールアドレス）、会社における職位又は所属に関する情報について、それらと本人の氏名を組み合わせた情報 (3) 防犯カメラに記録された情報等本人が判別できる映像情報 (4) 本人の氏名が含まれる等の理由により、特定の個人を識別できる音声録音情報 (5) 特定の個人を識別できるメールアドレス (6) 個人情報を取得後に当該情報に付加された個人に関する情報 (7) 官報、電話帳、職員録、法定開示書類（有価証券報告書等）、新聞、ホームページ、SNS等で公にされている特定の個人を識別できる情報	特定の個人を識別することができる記述等の全部又は一部の削除又は置換 「氏名のほか、住所や生年月日など、これらの記述等を組み合わせることによって特定の個人を識別することができる場合にも、その組合せが特定の個人を識別することができる記述にならないように、記述等の全部又は一部を削除する必要がある」 （一問一答　令和2年改正個人情報保護法）
	個人識別符号の全部の削除又は置換（規則第19条第２号）	**個人識別符号の全部の削除又は置換**	個人識別符号の全部の削除又は置換
	個人情報と当該個人情報に措置を講じて得られる情報を連結する符号の削除又は置換（規則第19条第３号）	※広く普及し提供先で連結可能な符号については、規則第19条第５号による加工が必要。	－
	特異な記述等の削除又は置換（規則第19条第４号）	**特異な記述等の削除又は置換**	－
	その他の個人情報データベース等の性質を勘案した適切な措置（規則第19条第５号）	**提供先等で個人情報と照合ができない状態にすること** ・情報又はその組み合わせが一意で、その情報と氏名等が紐づく情報が提供先等にとって入手可能な場合、そのような情報又はその組み合わせは、提供先等で個人情報になる。当該個人情報データベース等の性質を勘案し、その結果を踏まえて適切な措置を講ずること。 ・電話番号やメールアドレス、SNS 等のID、クレジットカード番号、広告ID等の符号であって、他の事業者が保有している個人情報との間で識別子的な機能を有することが想定される場合の当該符号の削除又は置換。	－
	－	－	不正に利用されることにより財産的被害が生じるおそれのある記述等

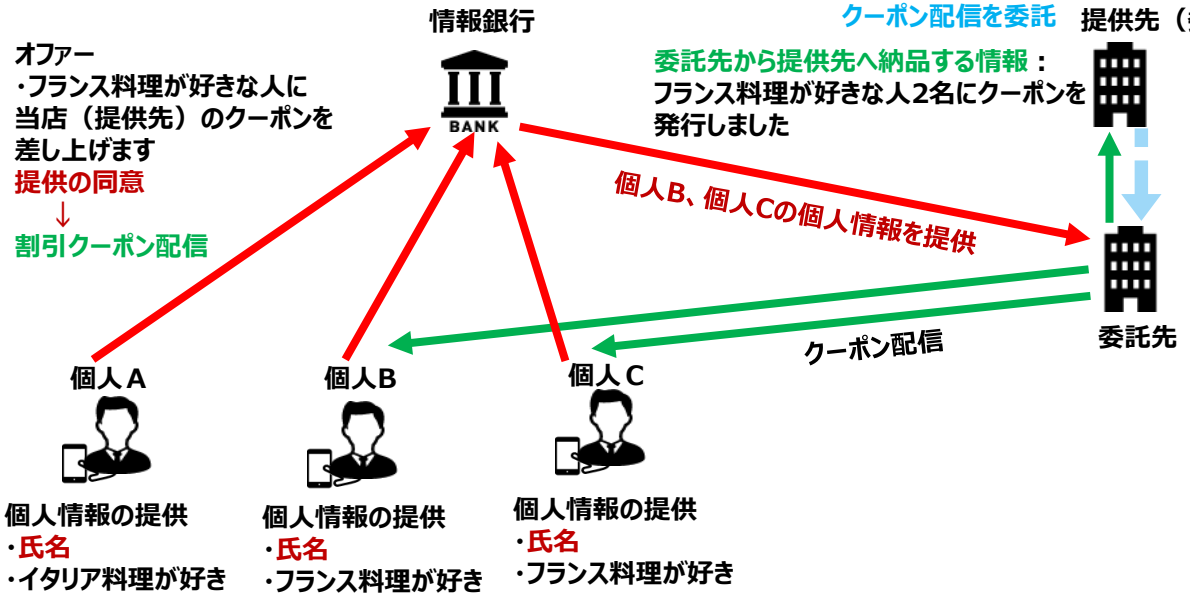
長寿番付を公表している市区町村においては、市区町村と生年で、個人が識別される場合もある。
［例］飯田市長寿番付では105歳は１名のみ
https://www.city.iida.lg.jp/uploaded/attachment/46613.pdf

※仮名加工情報の第三者への提供は禁止されている。

2－②　提供先第三者の選定に係る記載の明確化

③提供先が情報の取扱いを委託する場合

- 提供先(委託元)と委託先の関係については、以下のように整理される。
  - ✓ 委託先は、提供先(委託元)に対し、それ単体で個人情報となる情報へのアクセス権限を付与してはならない
  - ✓ 委託先が、本人に対するオファーや提供先（委託元）で利用するクーポンの発行を行う場合、これらの行為が提供先(委託元)の個人情報の利用目的の範囲内で委託を受けたものである必要がある
  - ✓ 委託先が提供先（委託元）の利用目的のために個人情報を扱う場合、委託先から提供先(委託元)に対して個人情報が提供されなくとも、情報銀行は提供先に対して個人情報を提供したことになる
  - ✓ 情報銀行事業者は、情報銀行として得た情報と委託先として得た情報を混在しないよう措置を講じた上で、自ら委託を受けてもよい（情報銀行サービスとは別サービスとする）



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

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

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

2－②　提供先第三者の選定に係る記載の明確化

③提供先が情報の取扱いを委託する場合

- 情報銀行の役割を具体化するため、情報銀行の監督下で委託させる場合の具体的条件を提供先と委託先間の委託契約に規定する必要がある。
  例1）情報銀行、提供先、提供先の委託先間での三社契約
  例2）提供先が委託先と締結する委託契約に情報銀行の監督が及ぶように規定する
    a) 委託者及び受託者の責任の明確化
    b) 個人データの安全管理に関する事項
    c) 再委託に関する事項
    d) 個人データの取扱状況に関する委託者への報告の内容及び頻度
    e) 契約内容が遵守されていることを委託者が，定期的に，及び適宜に確認できる事項
    f) 契約内容が遵守されなかった場合の措置
    g) 事件・事故が発生した場合の報告・連絡に関する事項
    h) 契約終了後の措置

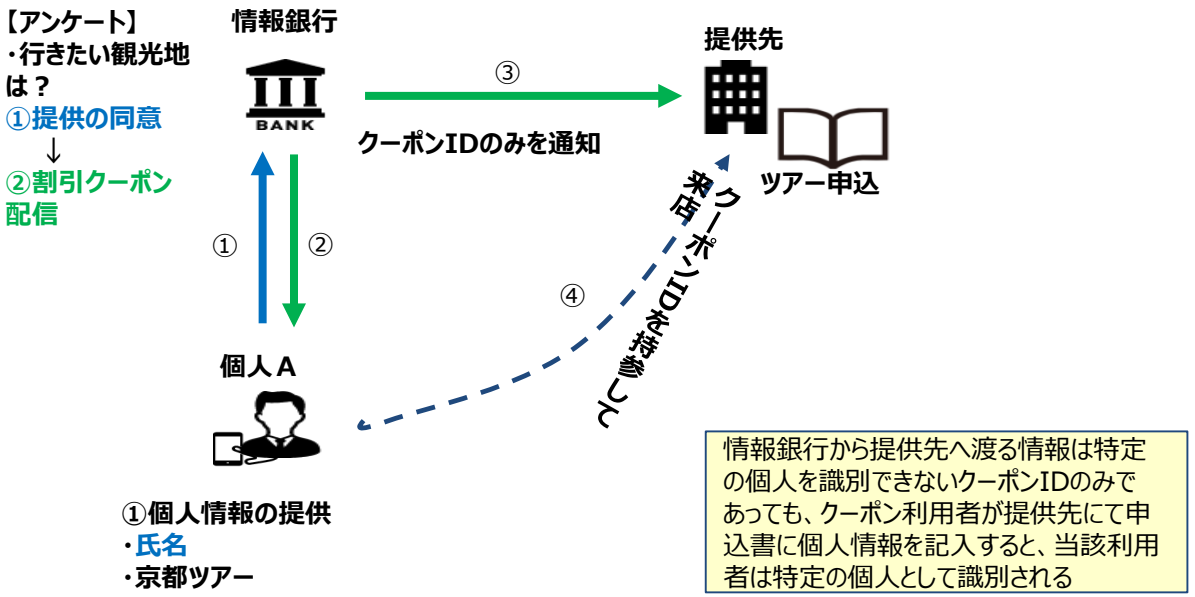
- 委託先が委託元（提供先）に渡す情報は、①（提供先は閲覧のみ）又は②（提供先が個人を識別できないよう加工）の条件を満たす必要がある。

- 情報銀行の監督下で、提供先から第三者認証等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。**また、提供先の委託先に対して情報銀行の監督が及ぶよう提供先と委託先間の委託契約に規定し、提供先に渡る情報は①又は②の条件を満たすものとする**

2－② 提供先第三者の選定に係る記載の明確化

①～③全てについて

- 情報銀行から提供先に対し、閲覧のみ、提供先において個人を識別できない方法、あるいは委託先に処理を委ねる形で情報が提供されても、個人が提供先のサービスを使う際に個人情報を登録する等して提供先に個人データが渡り、また個人が識別される場合がある。
- 個人は、情報銀行が選択した提供先であるがゆえに当該提供先を信頼して個人情報を提供することが想定されるため、かかる信頼を保護する必要がある。
- そこで、情報銀行は、自らのサービスと関連して提供先第三者が利用者から直接書面（電磁的方法を含む）により個人情報を取得することを許容する場合、以下のいずれかの措置を講ずるべき。
  - ✓ 提供先におけるコンプライアンス体制の構築及びその実施（監査の実施等）を客観的かつ検証可能な方法で確認する
  - ✓ 利用者との契約時及び利用者への提供先第三者に関する情報提供時に、情報銀行の提供するサービスと提供先が独自に提供するサービスとの区別を利用者が認識できるような表示を行う



3．統制環境に問題のある事業者の扱い

- 情報銀行には、個人情報の取り扱いの業務を的確に遂行できることに加え、社会的信用を有するよう実施することや、認定制度の趣旨を実現するためのガバナンス体制の構築が求められる。

- 統制環境(ガバナンス体制)に課題のある事業者は、情報銀行の認定制度全体の信頼性に影響を及ぼす可能性があるため、ガバナンス体制が不十分である情報銀行事業者への認定付与に関する考え方を、認定指針に追加することを検討すべき。

- 形式的には認定基準を満たしていても、「認定制度全体の信頼性に重大な影響を与える恐れがある事案」が発生している事業者を認定することは、認定制度の信頼性維持の観点から好ましくない。

- 事業者が認定を付与されない、または制裁措置をうける場合には、その根拠が認定指針の記載から明らかになる必要がある。

- 一方、登録事項と関係ない事故での取消しについては、認定指針に明示的に記載すべきではなく、ガバナンス体制の要件を記載した上で、個人情報保護と直接関係ない事項を含め、管理体制に問題がある場合に取り消すという運用がよい。

- **事業者による社会的信頼性を損なう行為の存在を認定において考慮するため、ガバナンス体制の要件において、社会的信頼維持のための体制を求めることとし、情報銀行認定事業者としての社会的信頼を確保するために必要なコンプライアンスを損なわないための体制が整っており、それを維持していることを要件とすべき。**

4. 再提供禁止の例外について

- 再提供禁止は指針ver2.0における重要なルールであり、その例外について、どのような事例が例外として許容され、どのような事例が許容されないかといった具体的な検討も含めた議論の深化が必要である。個人の利便性と例外要件の濫用を防ぐ観点から、マネーフォワードのようなアグリゲーションサービスと乗り換えの場合を例外とすることが適当である。

- マネーフォワードのようなアグリゲーションサービスについては、再提供禁止の例外を認めることが本人の利益になることが明らかであり、特に公的なガイドラインまたは業法の整備がされている分野においては、再提供先としての安全性も確保されているといえる。この類型の再提供禁止の例外の要件を以下のとおりとしたい。
  - ✓ 個人は提供先のサービスと再提供先のサービスの双方を利用すること
  - ✓ 再提供先のサービスはいわゆるアグリゲーションサービスであり、提供先のサービスを前提とするものであること
  - ✓ 再提供先の事業は公的なガイドラインもしくまたは業法の整備がされている分野であること

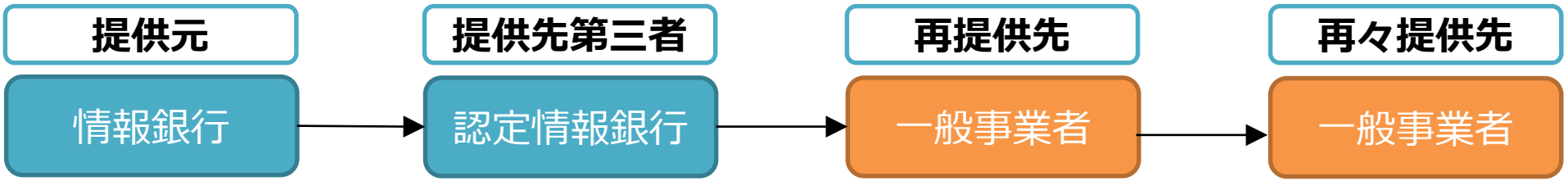
- 個人がサービスを乗り換えるために提供先から再提供先にデータを提供させる場合、個人の同意は明確であり、再提供禁止の例外を認めることが本人の利益になることが明らかであるが、個人が提供先サービスの解約を行う可能性が高いことから、以下を要件として再提供の例外としたい。
  - ✓ 個人による提供先のサービスと再提供先のサービスの双方の利用は、再提供時においてなされていれば足りるとすること
  - ✓ 個人の「乗り換え」の意思に基づき個人の指示のもとなされる再提供であり、提供先のサービスと再提供先のサービスは同様ないし類似の内容のものであること
  - ✓ 個人が提供先のサービスを解約する場合、提供先と再提供先の一定の関係を保つため、情報銀行と再提供先が契約を交わす等、解約の影響を回避する措置を講じること

4－①. 情報銀行間連携の考え方

- また、令和2年度総務省予算事業の一つである情報銀行間連携にかかる実証事業は、再提供禁止との関係でみれば、提供先第三者が認定を受けた情報銀行（以下「認定事業者」という。）である場合となる。
再提供先となる一般事業者には、提供元となる情報銀行の監督が直接には及ばないが、提供先第三者である認定情報銀行の監督下にあり、個人のコントローラビリティと、各提供先における情報の適切な取り扱いは確保されている。
そこで、かかる情報銀行間連携の場合についても、再提供禁止の例外として認めることが適当である。
ただし、個人のコントローラビリティやトレーサビリティ確保のため、実証事業で示された情報銀行間のデータ連携時に必要な機能・ルールを基に、認定団体により作成される標準仕様に準拠することが推奨される。

- 指針の記載としては、提供先第三者が認定事業者である場合と所定の条件を満たす場合にのみ再提供を認めることとし、当該情報銀行が、通常の（提供先が認定事業者でない場合の）再提供禁止の例外に関するルールにおける提供元（情報銀行）と同様の立場の者とみて、以降の提供先である各主体を含め規律がなされるよう、読み替え規定を置くこととしたい。

【提供先が認定事業者である場合】



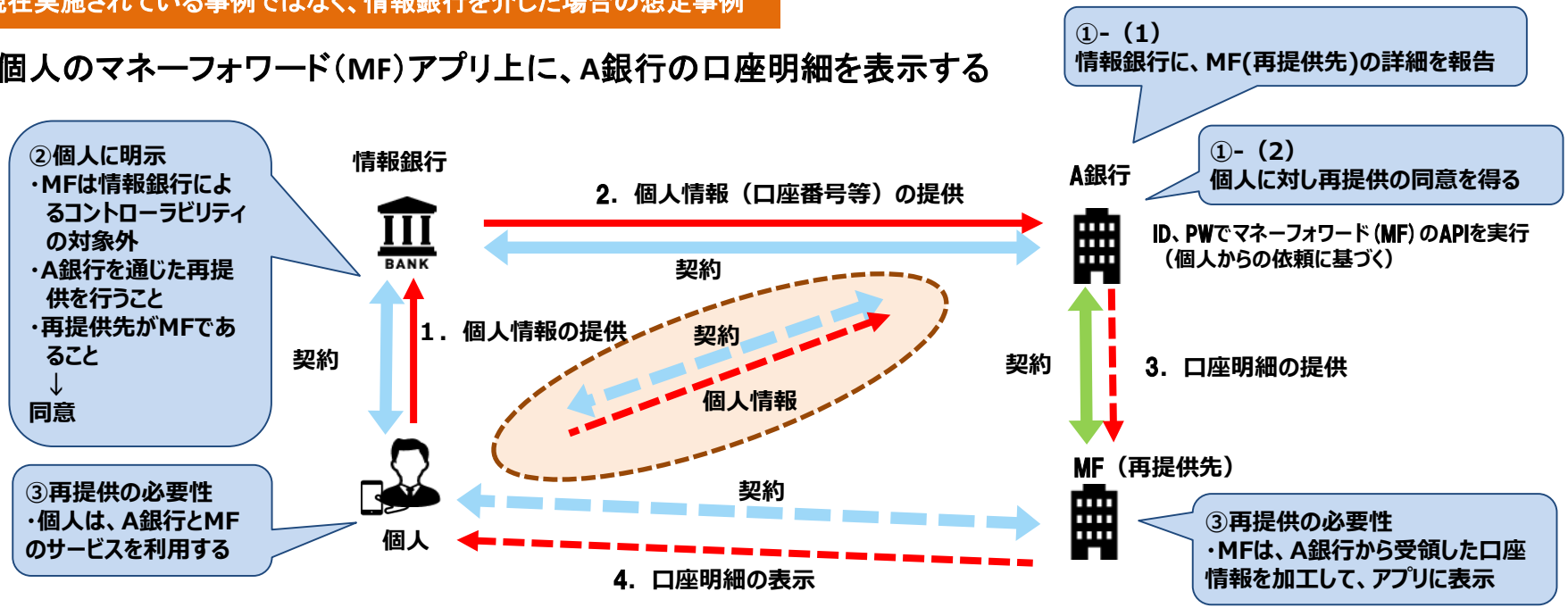
①アグリゲーションサービス
②サービスの乗り換え

- 上記実証事業においては、提供先第三者が認定を受けた情報銀行である場合のみ検討されており、再提供先や再々提供先が情報銀行となって、情報銀行間で情報が流通する場合の個人のコントローラビリティやトレーサビリティについては整理がなされていない。そのため、この点は今後の検討課題となる。

4－②．再提供禁止の例外の具体例

例外の具体例）　金融アグリゲーションサービス
※現在実施されている事例ではなく、情報銀行を介した場合の想定事例

・個人のマネーフォワード（MF）アプリ上に、A銀行の口座明細を表示する



前提：個人は「情報銀行」と契約を締結済み。また「A銀行」に口座開設済み。
①情報銀行はA銀行に対して、再提供の条件（1）～（3）を求める
（1）再提供先であるMFの業種・事業分類・利用目的・項目・相談窓口を、情報銀行に報告する
（2）A銀行が、再提供の同意を得る　（3）更なる第三者提供はしない

②情報銀行は個人に対し、「MFは情報銀行によるコントローラビリティの対象外」「A銀行を通じた再提供を行うこと」「再提供先がMFであること」を明示する。⇒個人が同意

③再提供の必要性があること　が前提である
・個人はA銀行(提供先) びMF(再提供先)のサービスを利用している
・MFの家計簿管理サービスは A銀行の金融サービスを前提とするものである（A銀行の口座情報をMFのアプリ上に表示する）
・再提供先の事業は公的なガイドラインもしくまたは業法の整備がされている分野である。

5. 世帯の複数の構成員が利用する機器等から取得される情報の利用について

- テレマティクス機器、IoT機器等の世帯等※の複数の構成員が利用する情報収集機器等から取得されるデータを利用する場合には、世帯等の複数の構成員の個人情報が混在することが想定されるため、それらの構成員の同意が得られていることの確認や利用停止の求めの取扱いについて配慮する必要がある。
  ※世帯等とは、IoTセンサー等で一次的にパーソナルデータを把握できる範囲の社会的集団を指す。

- 当該データを「世帯等構成員情報」とし、「特定の日時における世帯等の生活状況（在宅の有無、移動履歴等）を特定できる個人情報（ただし、情報収集機器等の契約者情報等に紐付くことにより特定の情報収集機器等利用者等※が識別されれば個人情報となる。）を指し、実際に当該機器等を利用した者が個別に特定されるものを除くもの」と整理する。
  ※ 情報収集機器利用契約の契約者、情報取集機器の利用者、情報収集機器利用料金の支払者等

- 世帯等構成員情報には、情報収集機器等利用サービスの契約者及びその世帯構成員についての在宅の有無等の防犯上重要な情報、移動履歴や視聴履歴等の重要なプライバシーを構成しうる情報が含まれる。
  ※スマートウォッチ等、取得したデータが世帯の特定の構成員のものと特定される場合や、写真、音声、ビデオ等で個人が識別できる場合は、取得されたデータは各個人の個人データとなるため、世帯等構成員情報から除く。

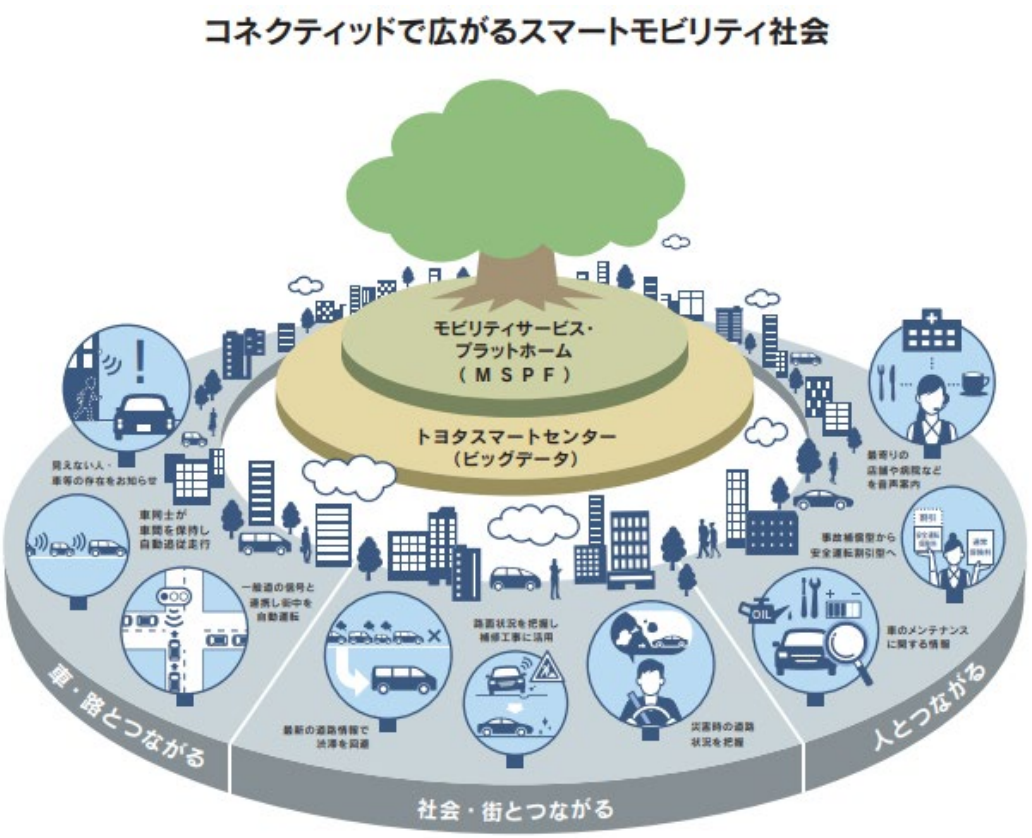
- **運用にあたっては、契約者等が誰であるかを明らかにすること自体、手間がかかることが想定されるほか、情報銀行として各世帯等構成員の意思を尊重する観点から、全員の同意が確認される形が望ましい。**
  - ✓ **情報銀行への提供の「同意」は、世帯等構成員情報を利用する場合は、世帯等構成員のいずれか1名（通常は情報銀行契約者）の同意を得る必要がある。**
  - ✓ **提供者（個人）は、世帯等構成員全員に対し、世帯等構成員情報が情報銀行によって取得され利用されることを周知し、全員の了解を得た上で同意すべき。また、情報銀行における利用の停止については、情報銀行は、停止を求める世帯等構成員の世帯等構成員情報であることを確認できる限りにおいて、各世帯等構成員からの利用停止の求めを広く認めるべき。**
- **その詳細な方法については、認定団体が定める基準を遵守すること。認定団体の基準の設定に際しては、関連するIoT機器分野にかかる認定個人情報保護団体（特に一般社団法人放送セキュリティセンター）の個人情報保護指針等を参考とすることが望ましい。**

5. 世帯の複数の構成員が利用する機器等から取得される情報の利用について

ユースケース① テレマティクスサービス

トヨタ自動車「コネクティッドカーから取得するデータの利活用・保護の取組みについて」

contents/tconnectservice/contents/pdf/toyota_datapolicy.pdf



情報銀行と軌を一にする構想だが、
トヨタ自動車はISMSもしくはプライバシーマークを取得していない

コネクティッドカーからの車両データの取得と利活用は、コネクティッドサービス（T-Connect/G-link）に申込、利用規約に同意ののち、サービスの利用を開始することによって可能となる。
クルマの制御ネットワークに接続する車載通信機(Data Communication Module)により車両データを取得、トヨタスマートセンター（クラウドサービス）に蓄積する。取得・蓄積した車両データをお客様のモニリティライフを充実させるコネクティッドサービスの各サービスに利用したり、「もっといいクルマ」づくりのための開発に活用したりする。

T-Connect利用規約（抜粋）
第14条（契約データおよび車両データの第三者提供）
(1)提供先：契約者が利用車両を購入したまたは利用者が指定した販売店
(2)提供先：協業事業者。ただし、協業事業者に協業サービスの利用を申込んだ場合に限ります。
(3)提供先：共同開発・研究先（車両・商品・サービス等の企画・開発・研究・改良等を行う企業・ 機関等）
(4)提供先：取引先（車両・商品・サービス等に含まれる部品・製品の企画・開発・製造・改良等を 行う企業等）
(5)提供先：提携機関および企業（社会・交通・生活インフラの提供・整備を行う企業等）
(6)提供先：医療機関および関係機関
(7)提供先：国土交通省。ただし、2016 年 12 月 1 日以降に T-Connect の利用を開始した場合に限ります。
(8)提供先：KDDI

位置情報などクルマを利用する個人の行動を表す内容が含まれているセンシティブな情報です。お客様の同意をいただいたうえで、慎重にとりあつかいます。ルールや世論、技術の動向を注視し、車両データを正しく取り扱っているかチェックします。

5. 世帯の複数の構成員が利用する機器等から取得される情報の利用について

ユースケース① テレマティクスサービス

○テレマティクスデータから得られる情報

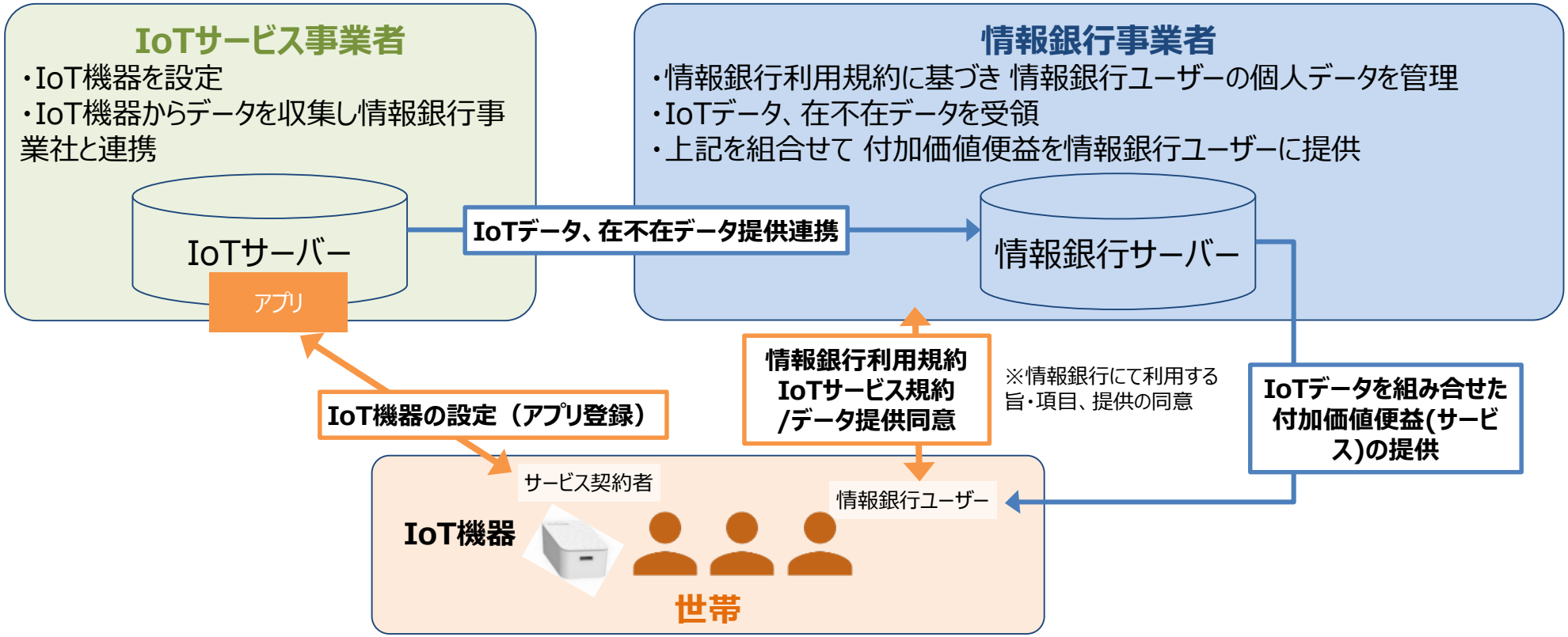
・契約データ（契約者の氏名、生年月日、電話番号、メールアドレスおよび性別等）
・車両データ（車名、車体番号、自動車登録番号、登録年月日、車載器の種類等）
・走行状況に関するデータ（エンジン回転数、アクセル/ブレーキの操作状況、車速、シフトポジション、走行距離及び位置情報等）
・ヘルプネット利用時に送信されるデータ（利用者の氏名、緊急事態の内容、通知発進時の位置情報、自動発信/手動発信の別、通報発信時刻等）
・エージェント利用時に送信されるデータ（対話機能を通じて送信されるデータ） 等

○テレマティクスデータを使うとできること

・車両位置を把握し、事故や故障の際速やかなサポートを受けられる
・通行止めや事故情報を踏まえた最適なルートを選択できる
・車体に異常があるときに検知・通知でき、部品の交換にも速やかに対応してもらえる
・車両の盗難防止し、追跡が可能になる
・安全や燃費の観点から運転内容を評価できる
・事故リスクを的確に把握し、自動車保険商品の開発に役立てられる
・運転の特徴から自動車保険の割引が適用される 等

5. 世帯の複数の構成員が利用する機器等から取得される情報の利用について

ユースケース② エアコン等のIoT機器



5. 世帯の複数の構成員が利用する機器等から取得される情報の利用について

ユースケース②　エアコン等のIoT機器

○エアコン等の居室内IoT機器データから得られる情報

・室温、湿度、照度
・二酸化炭素、揮発性有機化合物
・機器使用の時間帯
・在宅の有無　等

○エアコン等の居室内IoT機器データを使うとできること

・インフルエンザや熱中症の危険度を知ることができる
・換気のタイミングを知らせてもらえる、自動で換気モードに切り替わる
・遠隔でのペットの見守りができる
・遠く離れて暮らす家族の暮らしぶりを知ることができる
・同居の家族が帰宅したという情報を得ることができる
・電気の適切な消費の方法がわかる　等

5. 世帯の複数の構成員が利用する機器等から取得される情報の利用について

ユースケース③ 放送

視聴履歴に合わせて、様々な作品をおすすめする

視聴傾向に合わせたおすすめや、J:COMからのおすすめ番組などを表示する。

※セットトップボックスの略。セットトップボックスを通じて視聴履歴を収集。

Smart J:COM Box 利用規約　抜粋

第 10 条（個人情報の取扱い）

当社は、個人情報の保護に関する法律（平成 15 年法律第 57 号）、個人情報の保護に関する基本方針（平成 16 年 4 月 2 日閣議決定）、
放送受信者等の個人情報の保護に関するガイドライン（平成 29 年4月27日総務省告示第 159号）および
電気通信事業における個人情報保護に関するガイドライン（平成 29 年4月18日総務省告示第 152 号）に基づくほか、当社が別途掲示する個人情報保護ポリシーおよび
本規約の規定に基づいて、契約者の個人情報を適切に取扱うものとします。

2 当社は、契約者の個人情報（別記 2）を次に掲げる目的のために利用するものとします。

（1）契約者の確認や利便性の提供・向上、並びにサービスを提供するための工事の施工等の業務、サービスのメンテナンス、アフターサービス、
変更・解約等に関する諸手続き、番組誌等の送付、および料金請求や収納業務等のため。

（2）アンケート調査およびその分析を行い、設備の保守および新規サービスの開発やサービスレベルの維持・向上を図り、
あるいは集計・分析を行い、統計資料または匿名加工情報を作成するため。

＜中略＞

（6）契約者世帯のテレビの視聴日時、チャンネル、および番組内容(以下総称して「**視聴履歴**」といいます。)、
Smart J: COM Boxの双方向通信サービスまたはインターネットの使用状況（法の趣旨に則り法律上保護されるべきものは除きます）、
並びにSmart J: COM Boxの操作に関する記録を利用し、営業・販売活動の促進やプロモーションを行い、またはお勧め情報の表示を行うため。

＜中略＞

6 当社は、視聴履歴の取得から最大7年間の保存期間の経過後、当該情報を削除するものとします。ただし、当該保存期間の経過を待たずに当社が不要と判断した場合は、
直ちに削除するものとします。

7 当社は、契約者がSmart J:COM Box上で所定の設定を行った場合には、本条第 2 項第 6 号に規定する目的で視聴履歴を利用しないものとします。

5. 世帯の複数の構成員が利用する機器等から取得される情報の利用について

ユースケース③　放送

○視聴データから得られる情報

- 視聴履歴（視聴日時、チャンネル、および番組内容）
- 双方向通信サービスまたはインターネットの使用状況
- STB※の操作に関する情報
- テレビ受信機IPアドレス、対象機器を識別するために発行する情報
- 放送局・番組を識別する情報　等

※放送信号を受信して、一般のテレビで視聴可能な信号に変換する装置

○視聴データを使うとできること

- 視聴者の利便性向上につなげる
- 放送サービスの向上および、より良い番組制作に活かす
- おすすめの番組の情報を得ることができる
- 広告配信やマーケティング活動の参考　等

別添

赤字：ver2.0からの変更点

「情報信託機能の認定に係る指針Ver2.1」（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３年〇月

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）

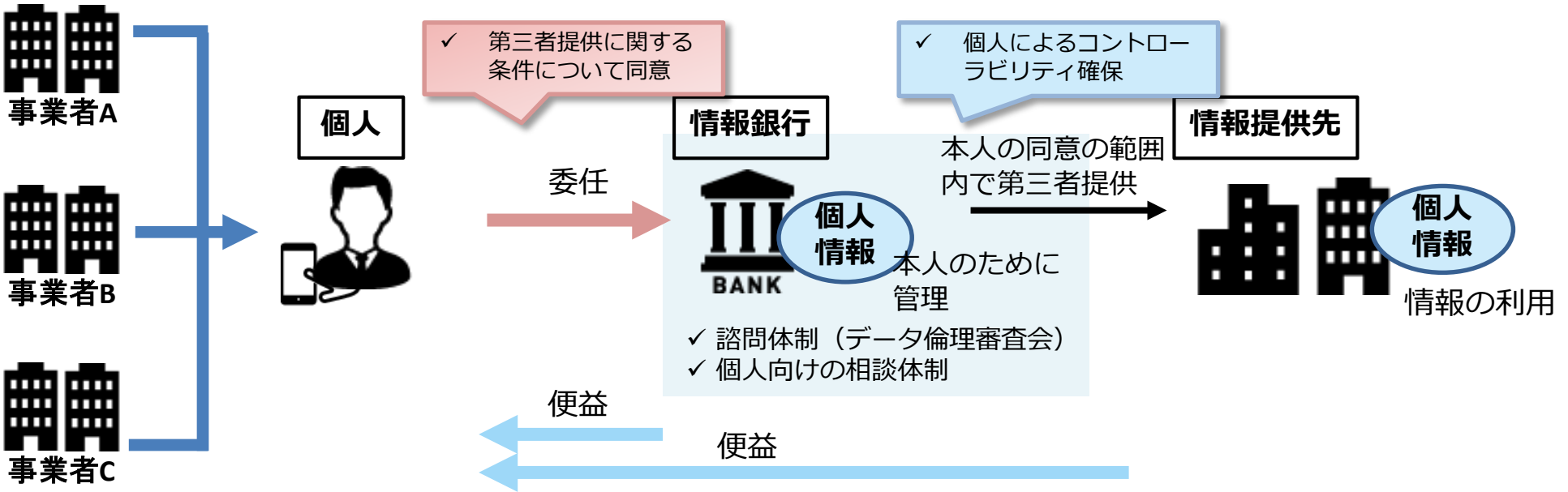
- モデル約款の記載事項は、消費者個人を起点としたサービスとして、また、個人情報の取扱いを委任するサービスとして、認定基準の目的を達成する観点から契約において最低限、定めることが必要な事項として、標準的な内容を示すもの。
- 認定基準とモデル約款は本来別物ではあるが、消費者が安心して当該サービスを利用するためのものという点で、モデル約款の内容と認定基準のうち事業内容に係る要件は多くの共通の要素を有するものとなり、認定要件に準拠する形でモデル約款の記載事項を作成。
- 本記載事項に定める事項以外にも、認定団体において、情報銀行事業の実態に応じたモデル約款を定め、データの利用に関する関連する他のガ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

「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。

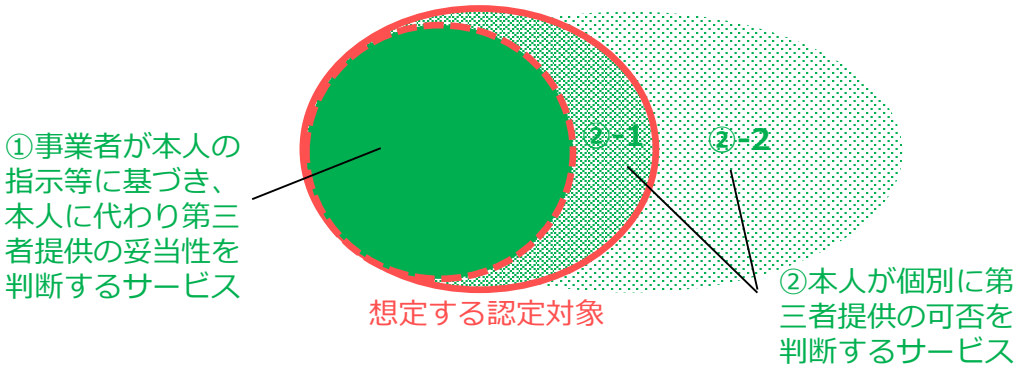


本指針の対象とするサービス

（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。

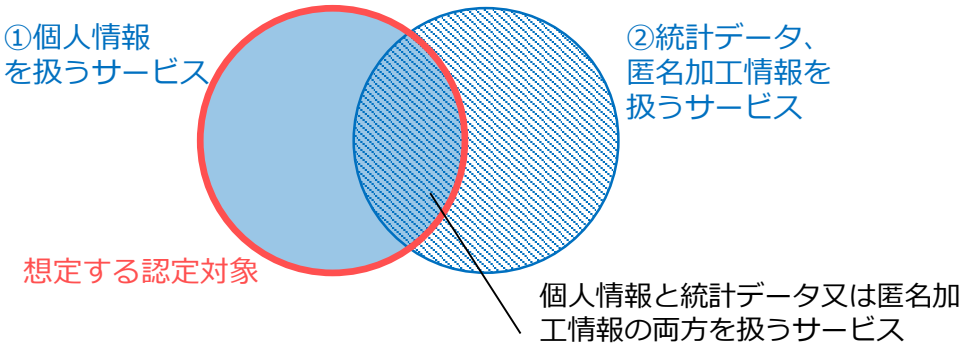
※②本人が個別に第三者提供の可否を判断するサービスのうち、提供事業者が情報の提供先を選定して個人に提案する場合など、提供事業者が比較的大きな役割を果たす（責任をもつ）ケース（②-1）を想定。他方、純粋なＰＤＳなどデータの管理や提供に関し個人の主体性が強いサービス（②-2）まで認定の対象として想定している訳ではない（認定がないことをもって信頼性が低いと評価されるべきものではない）。
※なお、データ保有者と当該データの活用を希望する者を仲介し、売買等による取引を可能とする仕組み（市場）である「データ取引市場」については認定の対象外。



（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~~検討会指針~~で対象とする「個人情報」には、「要配慮個人情報」は含まない。なお、健康・医療分野の個人情報のうち、次頁に記載する情報は、要配慮個人情報に該当しないことから本指針の対象となる。

健康・医療分野の個人情報のうち、要配慮個人情報に該当しないもの（※）

※例えば、本人の病歴や個人情報の保護に関する法律施行令第2条第1号から第3号までの事項を内容とする記述等は含まない。

- 本人に対して医師その他医療に関連する職務に従事する者により行われた疾病の予防及び早期発見のための健康診断その他の検査の結果ではなく、健康診断、診療等の事業及びそれに関する業務とは関係ない方法により知り得た個人情報であって、例えば以下のもの。

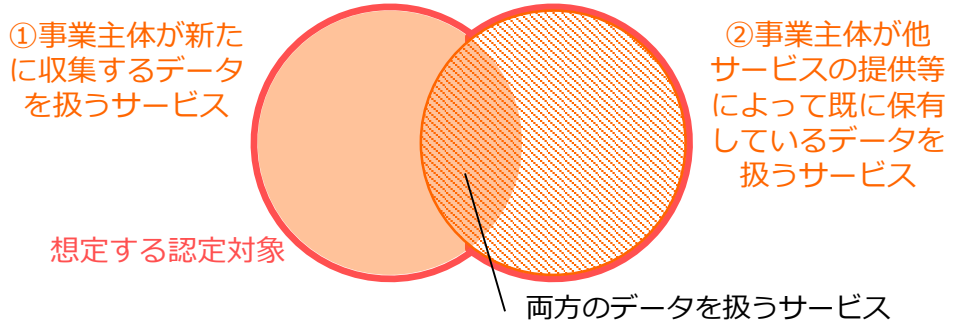
	項目
1	歩行測定（歩数・歩幅・ピッチ・接地角度・離地角度・外回し距離）
2	体重
3	体脂肪
4	体温
5	血圧
6	脈拍
7	心拍数
8	消費カロリー
9	摂取カロリー
10	睡眠時間
11	月経日

	項目
12	内臓脂肪レベル
13	水分量
14	筋肉量
15	骨量
16	タンパク質
17	基礎代謝
18	皮下脂肪
19	呼吸数
20	酸素飽和度（取り込まれた酸素のレベル）
21	ストレスチェック
22	肌の状態
23	視力

なお、個人情報でない健康・医療分野の情報（統計データ、匿名加工情報）については、前頁に記載のとおり、本指針にて個人情報に関し設けられている取扱上の制限等は適用されない。

（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

認定基準

1）事業者の適格性

項目	内容
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）類似の業務知識及び経験を有する。プライバシーマーク・ISMS認証などの第三者認証を有する、FISC安全対策基準に基づく安全管理措置を講じている（以下「第三者認証等の取得等」という。）　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

（※）提供先が第三者認証等の取得等をしていないが、認定団体が認める業種別ガイドラインにおける安全管理措置を遵守している事業者であると認定団体が認める場合には、既存の第三者認証等の取得等に相当するものとみなす。

また、情報銀行は、提供先が~~PマークまたはISMS認証~~第三者認証等の~~を~~取得等をしていない場合であっても、

① 情報は情報銀行が管理し、提供先には転記・複写禁止の契約を締結し、一覧での閲覧や任意検索ができない方法で、一人分のみ検索できる技術的対策を施した上で、~~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

② 提供先において特定の個人を識別できないよう、当該個人情報に含まれる記述等の一部の削除処理（当該一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）を行い、~~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

③ 情報銀行の監督下で、提供先から~~PマークまたはISMS認証~~第三者認証等の~~を~~取得等をしている者に個人情報の取扱いを全て委託させる。また、提供先の委託先に対して情報銀行の監督が及ぶよう提供先と委託先間の委託契約に規定し、提供先に渡る情報は①又は②の条件を満たすものとする

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。

ただし、情報銀行は、自らのサービスと関連して提供先第三者が利用者から直接書面（電磁的方法を含む）による個人情報を取得することを許容する場合、以下のいずれかの措置を講ずる必要がある。

・提供先におけるコンプライアンス体制の構築及びその実施（監査の実施等）を客観的かつ検証可能な方法で確認する。

・利用者との契約時及び利用者への提供先第三者に関する情報提供時に、情報銀行の提供するサービスと提供先が独自に提供するサービスとの区別を利用者が認識できるような表示を行う。

2）情報セキュリティ・プライバシー

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についてのガイドライン（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　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　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）プライバシー保護対策

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・遵守していく必要がある。

~~なお、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。~~

~~※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事項等）

■JISQ15001個人情報保護マネジメントシステム（要求事項）

■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

■ISO/IEC 29151:2017

Information technology -- Security techniques -- Code of practice for personally identifiable information protection

JIS X 9250及びISO/IEC 29151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）

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社会的信頼維持のための体制	・情報銀行認定事業者としての社会的信頼を確保するために必要なコンプライアンスを損なわないための体制が整っており、それを維持していること
③~~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
④~~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） ・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
⑤~~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
⑥~~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

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）

（※）世帯等（IoTセンサー等で一次的にパーソナルデータを把握できる範囲の社会的集団）の複数の構成員が利用する情報収集機器等から取得されるデータを利用する場合には、世帯等の複数の構成員の個人情報が混在することが想定されるため、それらの構成員の同意が得られていることの確認や利用停止の求めの取扱いについて配慮すること。その詳細な方法については、認定団体が定める基準を遵守すること。認定団体の基準の設定に際しては、関連するIoT機器分野にかかる認定個人情報保護団体（特に一般社団法人放送セキュリティセンター）の個人情報保護指針等を参考とすることが望ましい。

４）事業内容

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、提供先第三者が情報銀行認定を受けた事業者（以下「認定事業者」という。）である場合又は次の~~ような~~1～3の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、認定事業者のほか、以下の1～3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。

1　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
2　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~~べきであることが望ましい~~。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。
3　再提供の必要性、すなわち、個人の利便性と、再提供の例外の濫用の防止の観点から、再提供の例外は①再提供先が公的なガイドラインまたは業法の整備がされている分野におけるいわゆるアグリゲーションサービスである場合と②再提供が個人の指示のもと、同様ないし類似の内容のサービスへの乗り換えとして行われる場合を前提とすること。~~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、提供先第三者が認定事業者である場合において、上記1～3の条件は、「提供元（情報銀行）」とあるのは「提供先第三者」、「提供先第三者」とあるのは「再提供先」、「再提供」とあるのは「再々提供」と読み替えて適用されるものとする。また、この場合、個人のデータコントローラビリティ確保等の観点から、認定団体の作成する、情報銀行間におけるデータ連携時に必要な機能・ルールに係る標準仕様に準拠することが推奨される。

~~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

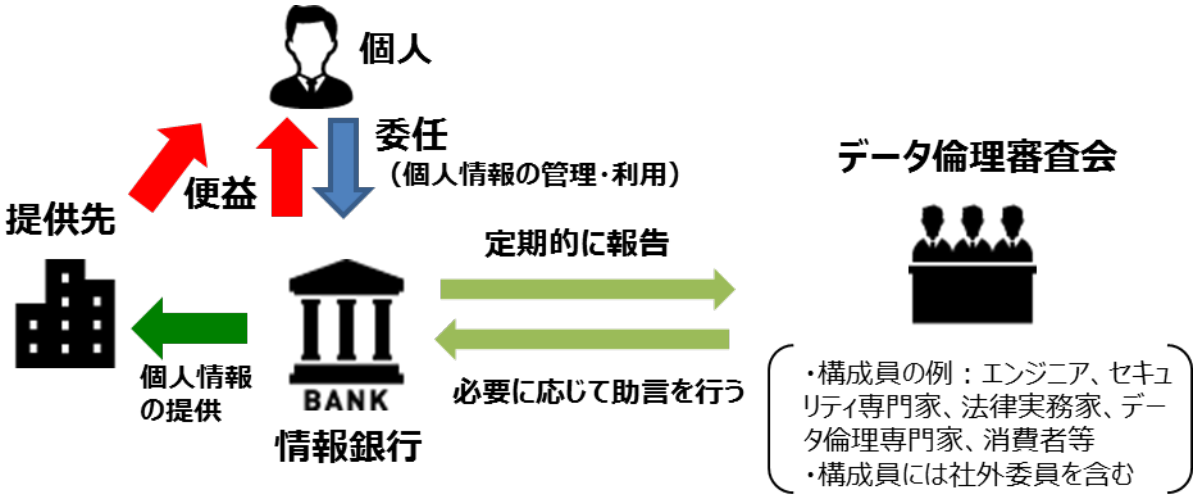
項目	内容
⑤個人のコントローラビリティを確保するための機能について	①情報銀行に委任した個人情報の第三者提供に係る条件の指定及び変更 ・提供先・利用目的・データ範囲について、個人が選択できる選択肢を用意すること(※1) ・選択を実効的なものとするために適切なユーザーインターフェイス（操作が容易なダッシュボードなど）を提供すること ・選択肢及びユーザーインターフェイスが適切に設定されているか、定期的にデータ倫理審査会などの諮問体制に説明し助言を受けること ・利用者が個別の提供先、データ項目等を指定できる機能を提供する場合には、その旨を明示すること
	②情報銀行に委任した個人情報の提供履歴の閲覧（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

■ 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

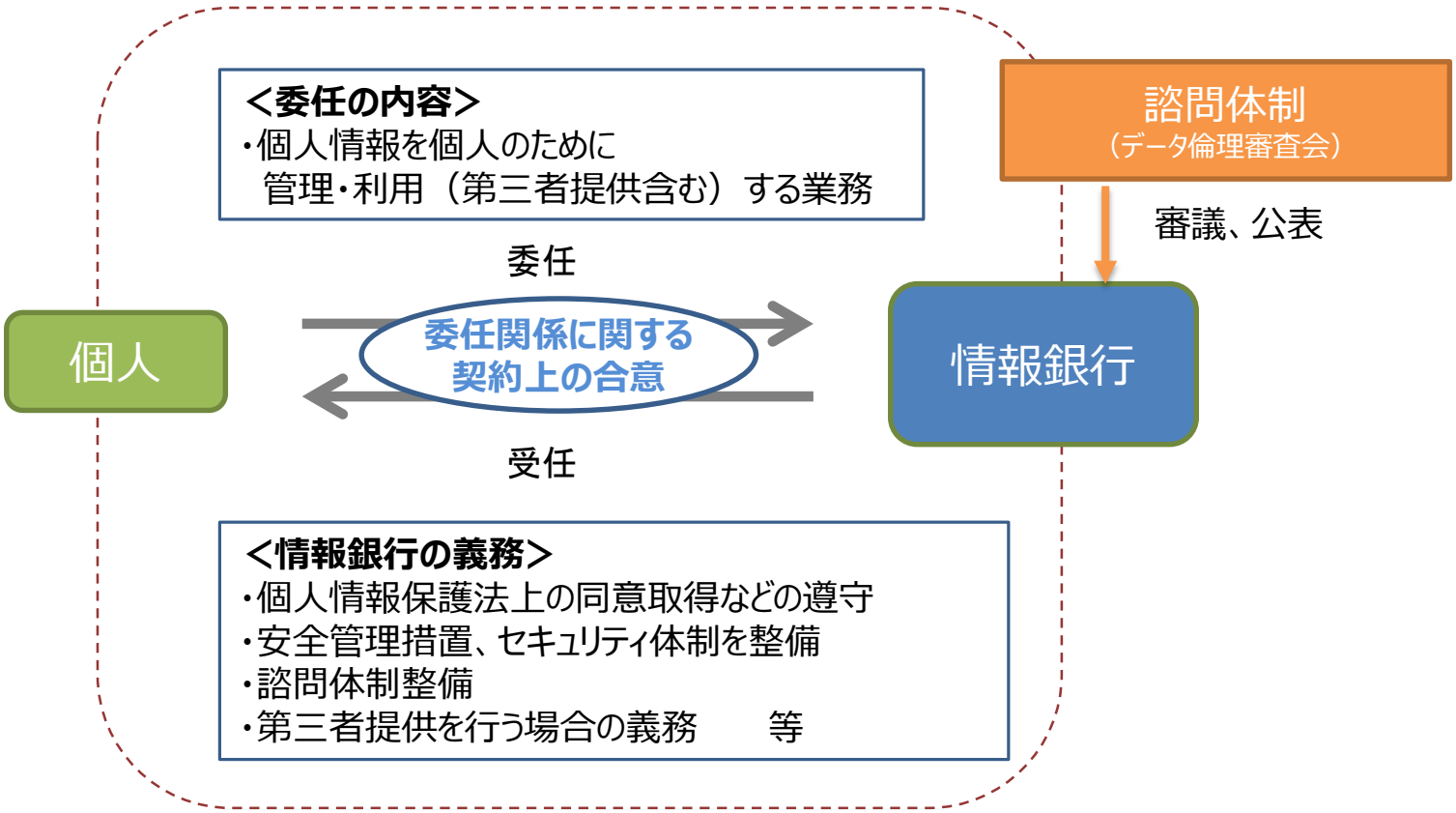
■　情報信託機能を提供する「情報銀行」のサービスについて、債権債務の内容や情報銀行の責任範囲を明確化するため、**個人と情報銀行の間を委任関係に関する契約上の合意**と整理する。

■　「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」（※）は含まない
　※本指針５頁に記載する情報は、要配慮個人情報に該当しないことから、本委任契約の対象となる

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