資料３－２

情報信託機能の認定スキームの在り方に関する検討会
認定・運用ワーキンググループ
とりまとめ（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
認定・運用ワーキンググループ

令和３年〇月

ワーキンググループ検討概要

- 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。
- 一方、認定・運用の過程で課題が生じており、追加の議論が必要とされたことを踏まえ、令和2年11月より、検討会のもとに認定・運用ワーキンググループを設置し、以下の項目について整理を行った。
- 本とりとまとめには、整理した内容を中心に指針Ver2.0改訂案を添付する。

➢ 整理を行った項目

1. 提供先第三者の選定について

   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

   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. 統制環境に問題のある事業者の扱いについて

3. 再提供禁止の例外の事例について

4. 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

認定・運用ワーキンググループ構成員

■ 構成員 （敬称略、五十音順、令和3年3月15日現在）

	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　准教授
	小林　慎太郎	株式会社野村総合研究所　ICTメディア・サービス産業コンサルティング部　上級コンサルタント
	長田　三紀	情報通信消費者ネットワーク
	野村　洋治	富士通株式会社　DXプラットフォーム事業本部　データテクノロジー事業部　シニアディレクター
	花谷　昌弘	株式会社NTTデータ　金融事業推進部　デジタル戦略推進部
	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	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

■ 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、一般財団法人日本情報経済社会推進協会（JIPDEC）

■ 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

1. 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

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

- 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。

- 提供先がPマークまたはISMS認証を取得していないが、ガス・水道・電気・通信などライフラインに関わる規制業種であって、所轄官庁の監督下にある規制業務の範囲内において個人情報保護のための措置が確保されている場合には、Pマークまたは ISMS認証の取得に相当する条件をもつといえる。
  なお、FISC安全対策基準に基づく第三者による監査証明については、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。

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

- 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WGにおいては、以下を新たな第三者認証等の候補として提案し、この内、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が決定した。

	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

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

- 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。

1－②　提供先第三者の選定に係る記載の明確化について

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。

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。

  ✓ 特定の個人を識別することができる記述等としては、「匿名加工情報の適正な加工の方法に関する報告書」※に記載の以下の項目（(a)～(e)は組み合わせによって、(f)は単体で、特定の個人を識別可能。同報告書にて「特定対象項目」と呼ばれる。）を参照する。

  ※　2017年2月21日版　国立情報学研究所「匿名加工情報に関する技術検討ワーキンググループ」作成

  (a)氏名以外の基本4情報（住所、生年月日、性別）
  (b)現在所属するまたは過去に所属した会社、学校等の団体、職歴および学歴であって、具体的な会社名、団体名を含むもの
  (c)本人到達性のあるメールアドレス、SNSのID
  (d)本人到達性のある電話番号（スマートフォン、自宅の電話番号、職場等の電話番号）
  (e)クレジットカード番号
  (f)単体で特定の個人を識別することができるもの（氏名、顔画像）
  ※(a)のうち、住所については市区町村、生年月日については年までとする。性別はそのまま残してよい。

  ✓ 同報告書では、規則1号の措置の対象となる情報については、「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）」を求めている。

- 提供しても安全といえるような処理としては、①上記に加えて、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。

- 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

1－②　提供先第三者の選定に係る記載の明確化について

（参考）仮名加工情報、匿名加工情報との差異について

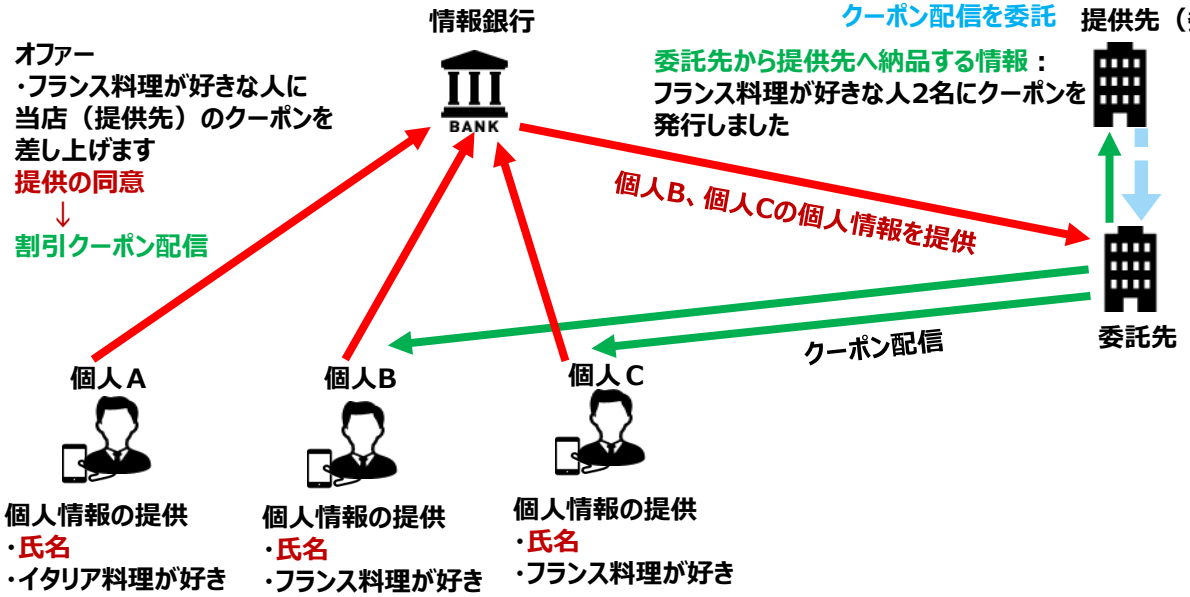
※参照：個人情報保護委員会　改正法に関連する政令・規則等の整備に向けた論点について（仮名加工情報）令和2年11月27日

	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（規則19条1号の加工）** (a)氏名以外の基本4情報（住所、生年月日、性別） (b)現在所属するまたは過去に所属した会社、学校等の団体、職歴および学歴であって、具体的な会社名、団体名を含むもの (c)本人到達性のあるメールアドレス、SNSのID (d)本人到達性のある電話番号（スマートフォン、自宅の電話番号、職場等の電話番号） (f)単体で特定の個人を識別することができるもの(氏名、顔画像) ※(a)のうち、**住所については市区町村、生年月日については年までとする。性別はそのまま残してよい。**	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
	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（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）	－	－
	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（規則第19条第4号）**	「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ものと考えられます。」 （一問一答　令和2年改正個人情報保護法）
	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（規則19条5号の加工）** 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。	市区町村では長寿番付を公表している場合があり、市区町村と生年で、当該年齢該当者が１名の場合もある。 ［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 －
	※クレジットカード番号は、通常、1号又は5号の基準に基づき 削除されると考えられる。	**(e)クレジットカード番号** を削除	不正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の削除又は置換

1－②　提供先第三者の選定に係る記載の明確化について

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
  - ✓ 情報銀行事業者が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

1－②　提供先第三者の選定に係る記載の明確化について

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

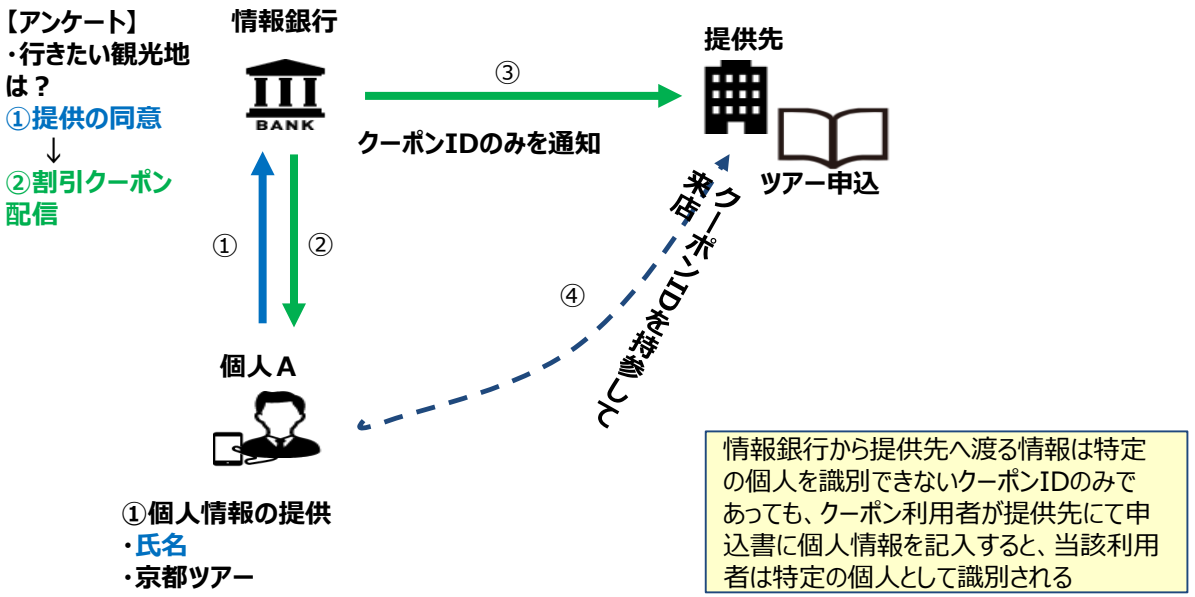
- 委託先が委託元（提供先）に渡す情報は、①（提供先は閲覧のみ）又は②（提供先が個人を識別できないよう加工）の条件を満たす必要がある。

- 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**

1－②　提供先第三者の選定に係る記載の明確化について

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



2. 統制環境に問題のある事業者の扱いについて

- 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。**

3. 再提供禁止の例外の事例について

- 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。

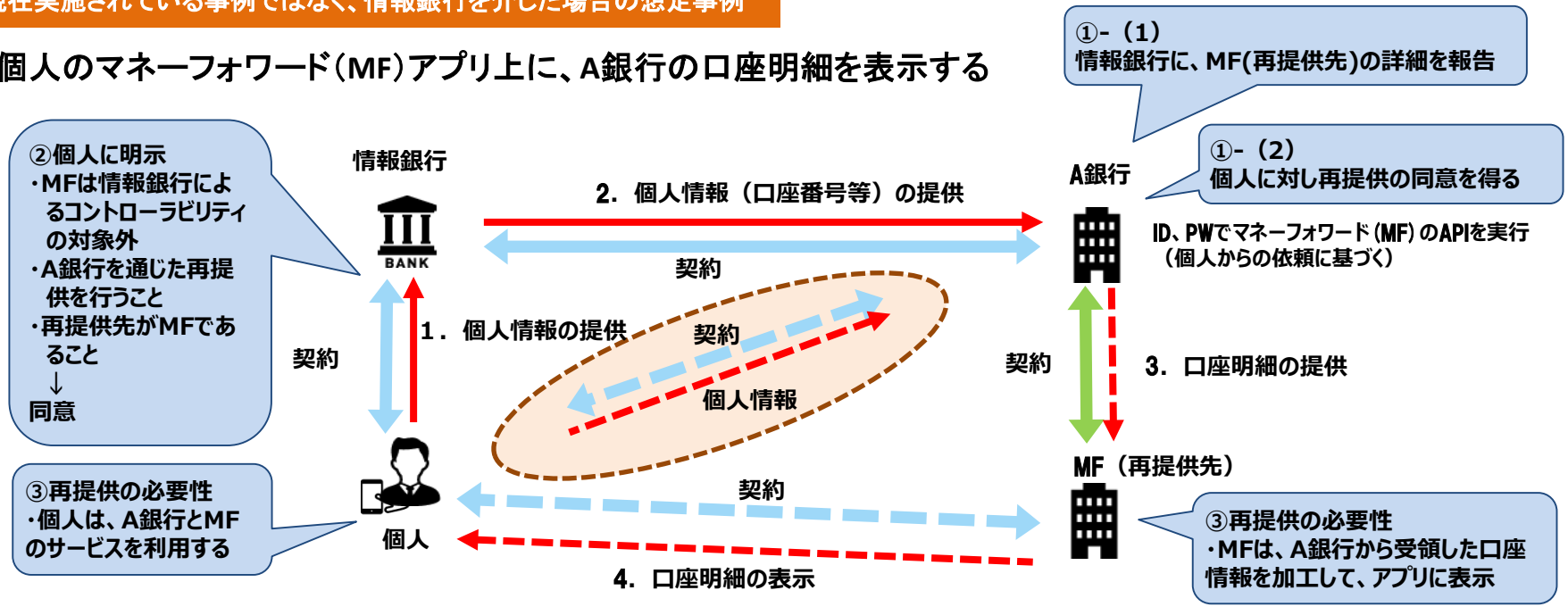
- マネーフォワードのようなアグリゲーションサービスについては、再提供禁止の例外を認めることが本人の利益になることが明らかであり、特に公的なガイドラインまたは業法の整備がされている分野においては、再提供先としての安全性も確保されているといえる。この類型の再提供禁止の例外の要件を以下のとおりとしたい。
  - ✓ 個人は提供先のサービスと再提供先のサービスの双方を利用すること
  - ✓ 再提供先のサービスはいわゆるアグリゲーションサービスであり、提供先のサービスを前提とするものであること
  - ✓ 再提供先の事業は公的なガイドラインもしくまたは業法の整備がされている分野であること

- 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」の意思に基づく再提供であり、提供元と提供元のサービスは同一のものであること
  - ✓ 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

3. 再提供禁止の例外の事例について

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）
・A銀行の口座情報がMFに提供されることは、個人にとって明確な利便性がある。

4. 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。

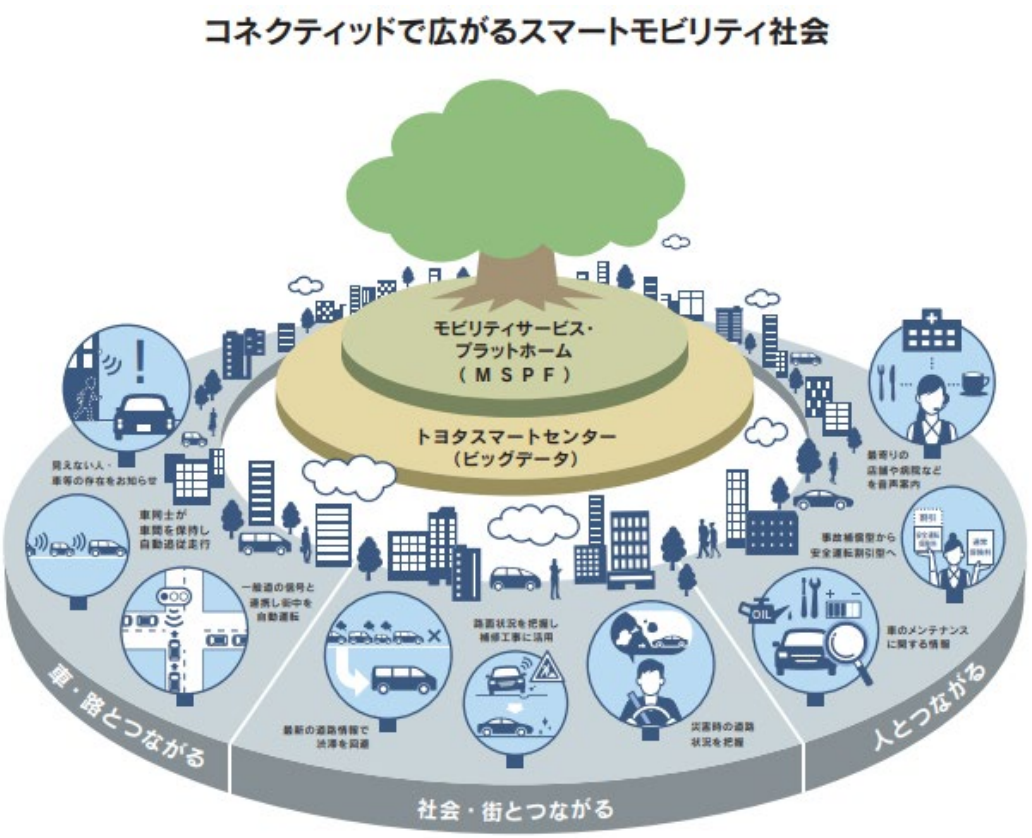
- **運用にあたっては、契約者等が誰であるかを明らかにすること自体、手間がかかることが想定されるほか、情報銀行として各世帯構成員の意思を尊重する観点から、全員の同意が確認される形が望ましい。**
  - ✓ **情報銀行への提供の「同意」は、世帯等構成員情報を利用する場合は、世帯等構成員のいずれか1名（通常は情報銀行契約者）の同意を得る必要がある。**
  - ✓ **提供者（個人）が世帯等構成員全員に対し、世帯等構成員情報が情報銀行によって取得され利用されることを周知し、全員の同意を得たことを確認すべき。また、情報銀行における利用の停止については、世帯等構成員全員からの利用停止の求めを広く認めるべき。**
- **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。**

4. 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。

4. 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

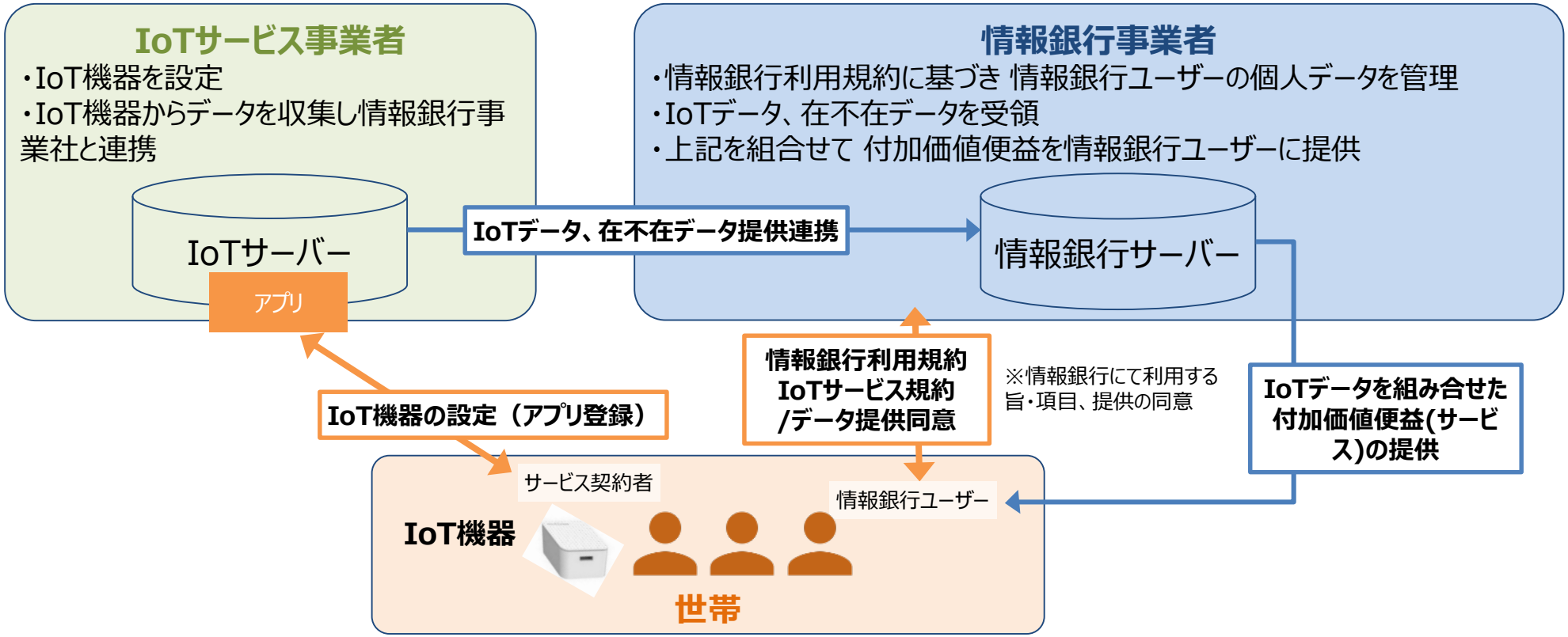
・契約データ（契約者の氏名、生年月日、電話番号、メールアドレスおよび性別等）
・車両データ（車名、車体番号、自動車登録番号、登録年月日、車載器の種類等）
・走行状況に関するデータ（エンジン回転数、アクセス/ブレークの捜査状況、車速、シフトポジション、走行距離及び位置情報）
・ヘルプネット利用時に送信されるデータ（利用者の氏名などならびに緊急事態の内容、通知発進時の位置情報、自動発信/手動発信の別ならびに通報発信時刻等）
・エージェント利用時に送信されるデータ（対話機能を通じて送信されるデータ）

○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

4. 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



4. 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

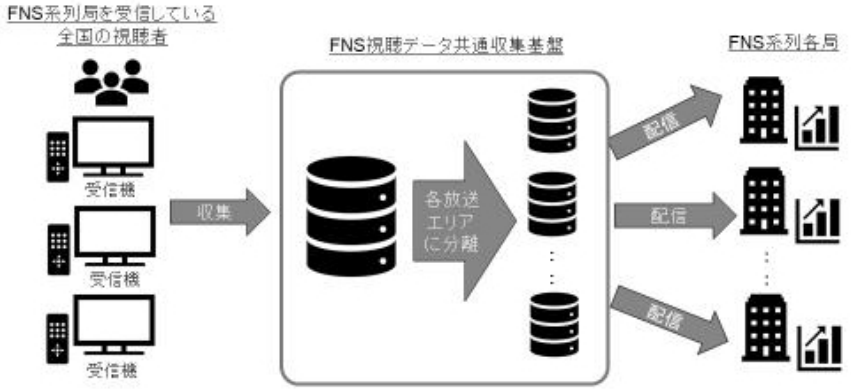
- インフルエンザや熱中症の危険度を知ることができる
- 換気のタイミングを知らせてもらえる、自動で換気モードに切り替わる
- 遠隔でのペットの見守りができる
- 遠く離れて暮らす家族の暮らしぶりを知ることができる
- 同居の家族が帰宅したという情報を得ることができる
- 電気の適切な消費の方法がわかる　等

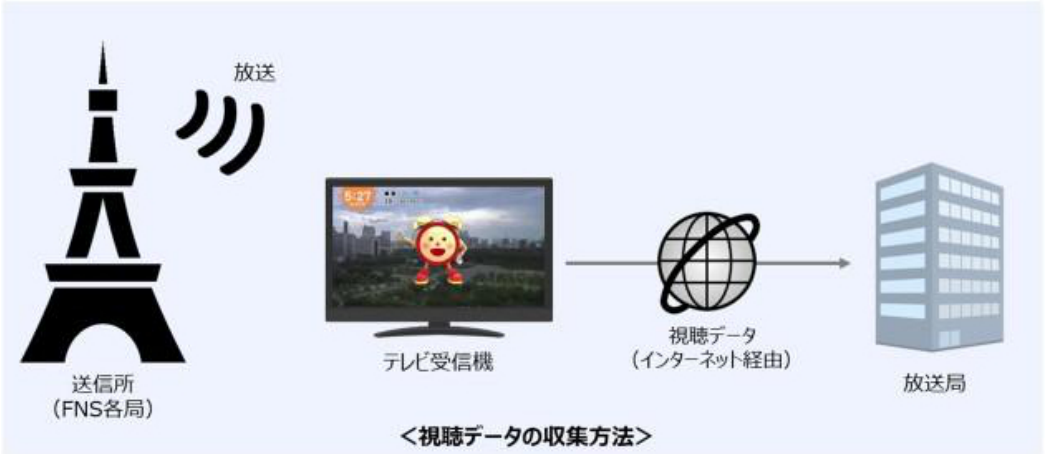
4. 世帯の複数の構成員が利用する機器等から取得される情報の利用について

ユースケース③　放送

FNSデータ視聴利活用プロジェクトの場合

インターネットに接続されているテレビを対象として、視聴データ（番組の視聴時刻情報、IPアドレス、受信機を識別するために発行する情報、受信機に設定されている郵便番号、および放送局を識別する情報）の収集・分析を行う。





<視聴データの収集方法>

■視聴データの利用目的：

収集した視聴データは以下の目的で利用します。

・視聴者の利便性向上

・放送サービスの向上およびより良い番組の制作、番組広報・宣伝

・広告配信やマーケティング活動の参考

■視聴データの利用方法：

収集した視聴データは、放送局や調査会社等が持つ個人情報を含まないデータと組み合わせて分析し、前項の目的のために利用する場合があります。また、その分析結果を用いて、テレビ視聴した方が保有していると推定されるスマートフォンやPCなどに、番組のおしらせや広告を表示する場合があります。これら一連の過程において、特定の個人を識別することがないようにする措置を取っています。

FNSデータ視聴利活用プロジェクト
https://www.fujitv.co.jp/company/news/200519.html

4. 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

- 番組の視聴時刻情報
- 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
- 対象機器に設定されている郵便番号
- 放送局を識別する情報　等

○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Ver2.0」改訂案
（「情報信託機能の認定基準」を抜粋）

情報信託機能の認定スキームの在り方に関する検討会
認定・運用ワーキンググループ

令和3年〇月

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・FISC安全対策基準などの第三者認証等（以下「第三者認証等」という。）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

（※）提供先が、ガス・水道・電気・通信などライフラインに関わる規制業種であって、所轄官庁の監督下にある規制業務の範囲内において個人情報保護のための措置が確保されている場合、当該提供先は第三者認証等を取得した者に準ずる者といえる。

また、情報銀行は、提供先が~~PマークまたはISMS認証~~第三者認証等を取得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

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　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

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、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。

・　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再提供がサービス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、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

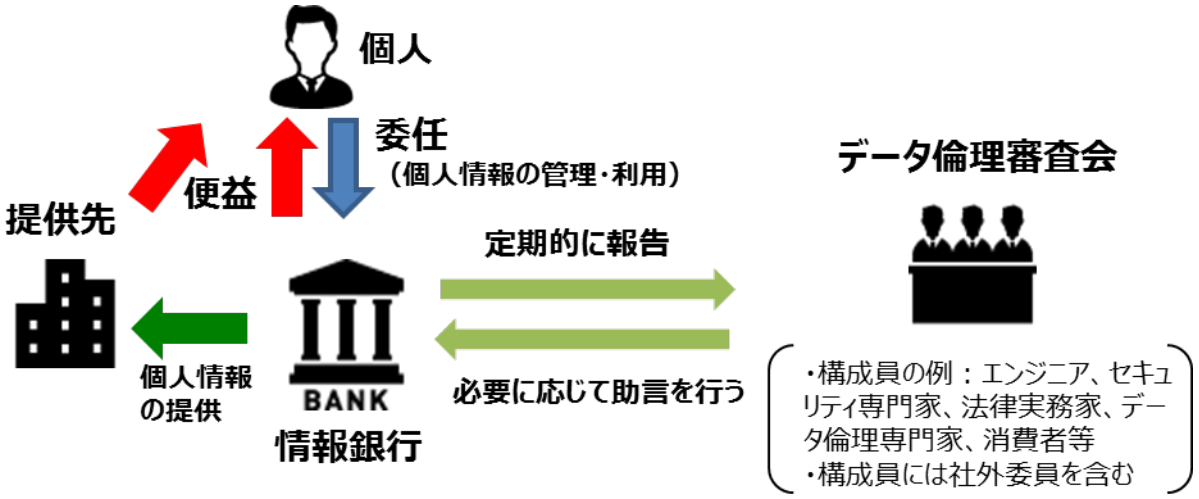
項目	内容
⑤個人のコントローラビリティを確保するための機能について	①情報銀行に委任した個人情報の第三者提供に係る条件の指定及び変更 ・提供先・利用目的・データ範囲について、個人が選択できる選択肢を用意すること(※1) ・選択を実効的なものとするために適切なユーザーインターフェイス（操作が容易なダッシュボードなど）を提供すること ・選択肢及びユーザーインターフェイスが適切に設定されているか、定期的にデータ倫理審査会などの諮問体制に説明し助言を受けること ・利用者が個別の提供先、データ項目等を指定できる機能を提供する場合には、その旨を明示すること
	②情報銀行に委任した個人情報の提供履歴の閲覧（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