参考１

情報信託機能の認定に係る指針

（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 30 年６月策定（Ver. 1. 0）

令和元年 10 月改定（Ver. 2. 0）

令和３年８月改定（Ver. 2. 1）

令和４年６月改定（Ver. 2. 2）

令和５年＊月改定（Ver. 3. 0）

目次

Ⅰ　はじめに

個人情報を含むパーソナルデータの適切な利活用を推進する観点から、これまで政府では様々な議論がなされてきた。

2016 年には「官民データ活用推進基本法」（平成 28 年法律第 103 号）が成立し、「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」（同法第 12 条）について定められた。

高度情報通信ネットワーク社会推進戦略本部（IT 総合戦略本部）の下で開催された「データ流通環境整備検討会」では、個人の関与の下でデータの流通・活用を進める仕組みである情報銀行等について議論が行われた。2017 年 2 月には、同検討会下の「AI、IoT 時代におけるデータ活用ワーキンググループ」中間とりまとめにて、「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、情報銀行等の仕組みが有効であるとされ、官民連携して情報銀行の社会実装に向けた積極的な取組を推進する必要性が示された。

2017 年 7 月に取りまとめられた総務省情報通信審議会「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」第四次中間答申では、情報銀行について、「信頼性を確保するための社会的な仕組み」として、当面は「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ていくことが望ましい」とされた。

これを受け、認定制度を有効に機能させるため、2017 年 11 月より総務省及び経済産業省において「情報信託機能の認定スキームの在り方に関する検討会」（以下「指針検討会」という。）が開催され、2018 年 6 月、本指針の初版となる「情報信託機能の認定に係る指針 Ver1.0」が公表された。

その後、総務省における実証事業、各企業における事業の検討等による事業の具体化や指針に基づく認定の開始等を踏まえ、情報銀行に関する基本的な考え方やデータ倫理審査会の役割等について指針検討会にて議論の上、指針の記載の見直しを行い、2019 年 10 月に「情報信託機能の認定に係る指針 Ver2.0」を公表した。

2021 年 8 月には、制度運用の過程において顕在化した課題である健康・医療分野の情報の取扱いや提供先第三者の選定等について指針検討会に議論の上、記載の見直しを行い、「情報信託機能の認定に係る指針 Ver2.1」を公表した。

2022 年 6 月には~~今般~~、指針検討会におけるプロファイリングや令和２年・３年改正個人情報保護法への対応に関する議論を踏まえた改定を行うと共に、指針の体裁を全体的に整理することとし、「情報信託機能の認定に係る指針 Ver2.2」として公表することとなった。

今般、利用者個人や社会のために活用するニーズが高く、継続して検討を進めてきた健康・医療分野の要配慮個人情報の取扱いについて整理し、指針の記載の見直しを行い、「情報信託機能の認定に係る指針 Ver3.0」として公表することとなった。

情報銀行は、パーソナルデータの本人のデータに対する権利利益を確保し、本人のコントローラビリティを高め、パーソナルデータの流通・活用を促進するという目的を有している。かかる目的のもと、今後も実証事業を実施し、サービスの展開や関連制度の運用状況等を踏まえ、指針検討会において継続して議論を行い、指針の見直しを行っていく。

Ⅱ　適用範囲

１　本指針の基本的な運用について

（１）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情報銀行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・運用に必要な事項は、各認定団体において決定する。

（２）認定の対象

- 認定は、事業者単位[1]・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、利用者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。

（３）本指針の対象とする事業における個人情報の範囲

- 本指針では、情報銀行が利用者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、要配慮個人情報を含む事業は、認定の対象としない（要件を満たした上で取り扱うことができる健康・医療分野の要配慮個人情報[2]を含む事業を除く。）。

（４）用語の定義

「本指針」・・・情報信託機能の認定に係る指針 Ver3.0~~2.2~~
「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

（５）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、当該認定によって利用者個人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。

---

[1] 本指針の記載は、個人情報の保護に関する法律における「個人情報取扱事業者」の認定を想定したものとなっているが、同法における「行政機関等」~~や地方公共団体~~が申請する場合には、「個人情報取扱事業者」を想定した認定要件は、適用される法規範を踏まえ適切に読み替える必要がある。

[2] 情報銀行において取り扱うことが可能な健康・医療分野の要配慮個人情報は、Ⅱ３（２）「事業で扱うデータの種類」参照。

- 一定の水準を満たした上でのレベル分けを行うことは想定しないが、認定団体において認定基準の一部を独立した認定の対象とすることは想定される。
- 提供する機能をわかりやすく開示するなど、利用者個人を起点としたデータの流通、利用者個人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。

（６）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、利用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、いずれも利用者個人が安心して当該サービスを利用するためのものであり、モデル約款の内容と事業内容に係る認定基準は多くの共通要素を有するため、認定要件に準拠する形でモデル約款の記載事項を作成している。
- 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。

2　本指針における情報銀行の定義・考え方

（1）定義

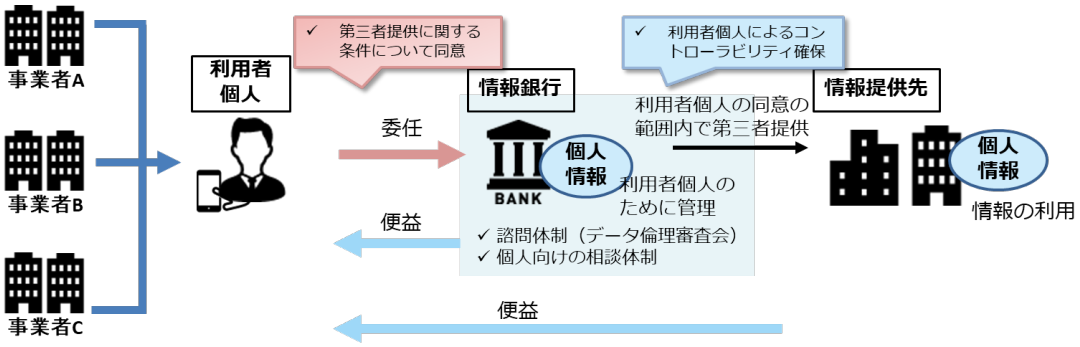
- 「情報銀行」は、実効的な本人関与（コントローラビリティ）を高めて、パーソナルデータの流通・活用を促進するという目的の下、利用者個人が同意した一定の範囲において、利用者個人が、信頼できる主体に個人情報の第三者提供を委任するというもの。

（2）機能

- 「情報銀行」の機能は、利用者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、利用者個人は直接的又は間接的な便益を受け取る。
- 利用者個人の同意は、使いやすいユーザーインターフェイスを用いて、情報銀行から提案された第三者提供の可否を個別に判断する方法、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。

（3）利用者個人との関係

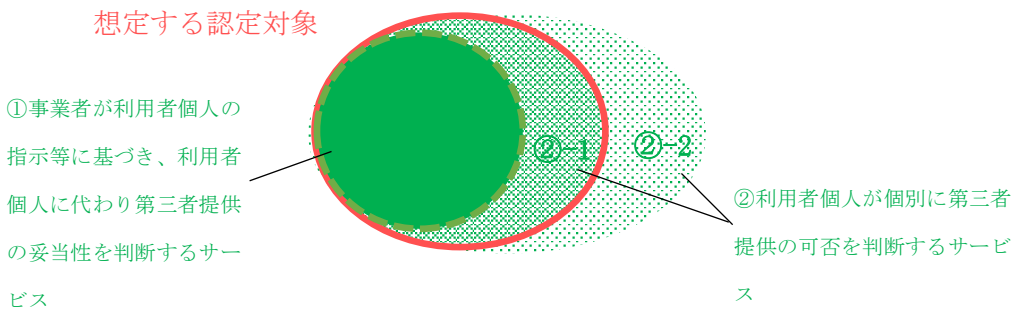
- 情報銀行が利用者個人に提供するサービス内容（情報銀行が扱うデータの種類、提供先第三者となる事業者の条件、提供先第三者における利用条件）については、情報銀行が利用者個人に対して適切に提示し、利用者個人が同意するとともに、契約等により当該サービス内容について情報銀行の責任を担保する。



3　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

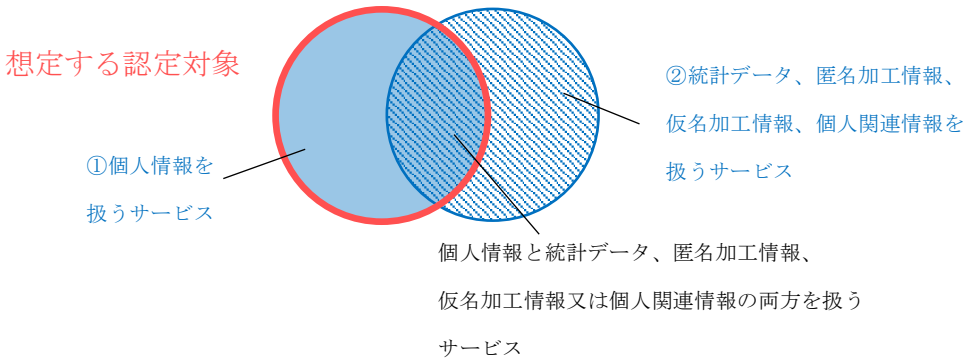
- 認定の対象は、①事業者が個人情報の第三者提供を利用者個人が同意した一定の範囲において利用者個人の指示等に基づき行い、その際利用者個人に代わり第三者提供の妥当性を判断するサービスと、②利用者個人が個別に第三者提供の可否を判断するサービスのうち、情報銀行が比較的大きな役割を果たすものとする。
- ②利用者個人が個別に第三者提供の可否を判断するサービスのうち、提供事業者が情報の提供先を選定して利用者個人に提案する場合など、提供事業者が比較的大きな役割を果たす（責任をもつ）ケース（②-1）を想定。他方、純粋な PDS などデータの管理や提供に関し利用者個人の主体性が強いサービス（②-2）は認定の対象として想定していない（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・安全で信頼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利用者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利用者個人への便益（便益の有無を含む）について、必要な情報を利用者個人に対して開示することが必要。

・ 仮名加工情報・個人関連情報[3]については、利用者個人のコントローラビリティを高める観点から本指針にて付加される規律を遵守することが必要。なお、これらの情報に関する情報銀行における規律については、令和２年改正個人情報保護法の施行後現れるユースケースの内容等も踏まえ、引き続き検討する。



・ 要配慮個人情報については、「民間 PHR 事業者による健診等情報の取扱いに関する基本的指針」（総務省・厚生労働省・経済産業省。以下「PHR 指針」という。）に定める「健診等情報」[4]に該当するものであり、利用者個人に明示的に開示・説明され、利用者個人が十分に理解することができる健康・医療分野の要配慮個人情報に限り、その要件[5]を満たした上で、取り扱うことができる。これ以外の要配慮個人情報は、本指針が認定の対象とする事業において取扱可能である個人情報には~~、要配慮個人情報は~~含まない。

・

・ なお、次に記載する健康・医療分野の個人情報~~のうち、次に記載する情報~~は、要配慮個人情報に該当しないことから、要配慮個人情報の取扱いに係る要件に関わらず、取扱可能である。[6]

・

・ 利用者個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等ではなく、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

[3] 情報銀行において、個人関連情報は利用者個人の指示のもと情報銀行に預けられる。そのため、情報銀行は、通常、個人関連情報を個人データとして取得する形で取り扱うこととなる。

[4] PHR 指針において「健診等情報」とは、個人が自らの健康管理に利用可能な個人情報保護法上の要配慮個人情報で次に掲げるもの、及び予防接種歴とされている。
・個人がマイナポータル API 等を活用して入手可能な健康診断等の情報
・医療機関等から個人に提供され、個人が自ら入力する情報
・個人が自ら測定又は記録を行うものであって、医療機関等に提供する情報

[5] 健康・医療分野の要配慮個人情報を取り扱う場合における要件は、「（５）健康・医療分野の要配慮個人情報を取り扱うサービスに係る要件」に記載されるものの他、各章に定める基準等を参照。

[6] 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、既述のとおり、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。

であって、例えば以下のもの（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。また、検診機関や医療機関等において医療専門職が管理する情報を除く。）。

	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

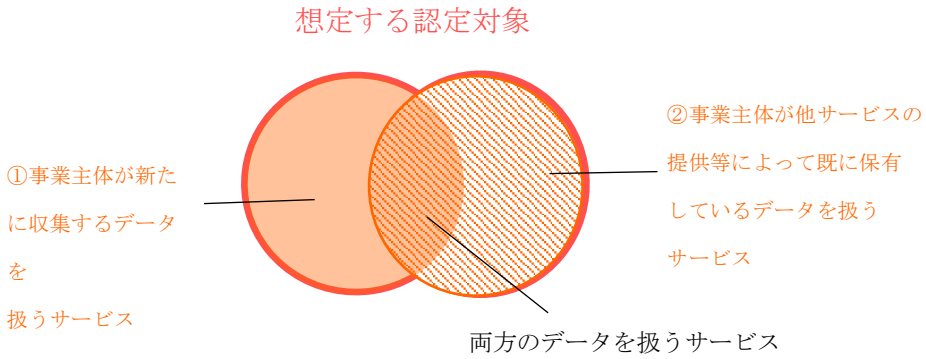
（３）データの収集方法

- 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、新たに利用者個人との間で情報銀行としての契約が必要となる。
- 健康・医療分野の要配慮個人情報を新たに取り扱う際、PHR 指針に定める健診等情報のうち、「医療機関等から個人に提供され、個人が自ら入力する情報」若しくは「個人が自ら測定又は記録を行うものであって、医療機関等に提供する情報」に該当する場合には、当該情報が取り扱うことが可能なもの[7]であることをデータ倫理審査会において確認すること[8]。
- 健康・医療分野の要配慮個人情報は、収集されることのメリットやリスクについて利用者個人が正しく理解した上で提供されるべきであることから、情報銀行が利用

[7] 情報銀行において取り扱うことが可能な健康・医療分野の要配慮個人情報は、Ⅱ３（２）「事業で扱うデータの種類」参照。

[8] 個人がマイナポータル API 等を活用して入手可能な健康診断等の情報は、第三者への提供が想定されているものであるため、確認不要とするが、今後の取得可能な情報の追加等により見直すことがあり得る。

者個人から同意を得る際には、明示的に開示・説明することはもとより、かかりつけ医等医療専門職からの助言を得るよう促すこと。また、情報銀行は、かかりつけ医等から求められた場合には、追加の情報提供等に努めなければならない。



（4）商号等に関する注意事項

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）

（5）健康・医療分野の要配慮個人情報を取り扱うサービスに係る要件

- （2）で述べた健康・医療分野の要配慮個人情報を取り扱う場合は、利用者個人にとって明確な便益があり、かつ、不利益が生じるおそれがないことを要する。
- 明確な便益があることは、利用者個人に提供される便益について、その便益がもたらされると認めるに足る根拠が示されなければならない。
- この場合、「利用者個人に提供される便益」は、利用者個人の健康増進や適切な医療の提供といった健康に係る便益をもたらすものを原則とするが、介護保険外サービス、子育てサービス、保険関連サービスなどの健康・医療に関連する便益についても、根拠があることを前提に容認する。
- 「その便益がもたらされると認めるに足る根拠」とは、医療専門職による診断・助言のほか、学会等におけるコンセンサスなど、データ提供時点において一定の合理性が認められる知見・見解のことを指す。
- その根拠の妥当性の判断に当たっては、医療専門職の参加するデータ倫理審査会への諮問を要する。

・　利用者個人が間接的な便益を受けるもの（すなわち利用者個人以外のための利用）については、利用者個人が直接的に便益を受けるものがある場合であって、かつ、当該利用用途に公益性[9]がある場合に限り容認する[10]。

・　利用者個人から同意を得る際に、利用者個人以外のために利用することについて、明示的に説明を行う必要がある。

「公益性」があることとは

- 例えば、健康・医療分野であれば障害者の支援、公衆衛生の向上を目的とする事業など、行政分野であれば地域社会の健全な発展を目的とする事業など、教育・スポーツ分野では児童又は青少年の健全な育成、国民の心身の健全な発達への寄与のために利用する用途を想定。
- **公益社団法人及び公益財団法人の認定等に関する法律（平成18年法律第49号）の別表に定める「公益に関する事業」を参考に判断する**。

[9] 公益社団法人及び公益財団法人の認定等に関する法律（平成 18 年法律第 49 号）の別表に定める「公益に関する事業」を参考として、それに類する事業であれば「公益性」があると類推する。

[10] 例えば、生活習慣改善に向けた運動プログラム開発や車椅子、歩行器等の性能改善といった健康・医療分野の製品・サービスの開発・改善は、利用者個人が間接的な便益を受けるものであって「公益性」があると類推できる。

Ⅲ　情報信託機能の認定基準

１　事業者の適格性

（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でき、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

・ 提供先第三者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、提供先第三者の管理体制を把握するなど適切な監督をすること、提供先第三者にも、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

・ 提供先第三者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

・ 提供先第三者が第三者認証等の取得等をしていない場合であっても、情報銀行が次のⅰ～ⅲ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第三者が遵守していると認められる場合には、情報を提供することができる

ⅰ　情報は情報銀行が管理し、提供先第三者には転記・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、必要な情報の閲覧のみができることとする

ⅱ　提供先第三者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、提供先第三者に提供する

iii　情報銀行の監督下で、提供先第三者から第三者認証等の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、提供先第三者の委託先に対して情報銀行の監督が及ぶよう提供先第三者と委託先間の委託契約に規定し、提供先第三者に渡る情報は上記ⅰ又はⅱの条件を満たすものとする

- 情報銀行は、上記のⅰからⅲまでにおいて、自らのサービスと関連して提供先第三者が利用者個人から直接書面（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

ⅰ　提供先第三者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

ⅱ　利用者個人との契約時及び利用者個人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第三者が独自に提供するサービスとの区別を利用者個人が認識できるような表示を行う

- 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・プライバシー保護

（１）基本原則及び遵守基準

①　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保護対策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・提供先第三者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[11]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

②　遵守基準

- 個人情報の取扱い、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）をしていること（認定申請時にプライバシーマーク又は ISMS 認証を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）
- 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
- 個人情報保護法における安全管理措置として同法の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[12]

---

[11]（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/210101_guidlines01.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
- 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 27001：2013Information 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 27002：2013Information 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
  https://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Management_Standard_H28.pdf
- 総務省情報セキュリティサイト
  http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/

[12] 特に、健康・医療分野の要配慮個人情報を取り扱う場合は、本指針に定める遵守基準の他、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」（総務省・経済産業省）に基づくリスクマネジメント及び制度上の要求事項に対応すること。

・ 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

（2）情報セキュリティの具体的基準

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・システムなどを準備し、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かつ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り、マネジメントの改善などを行うこと

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、更新をすること

⑤ 情報セキュリティ組織

・ 責任者を明確化し、組織体制を構築すること
・ 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

・ 経営層は従業員へセキュリティ方針及び手順を遵守させ、個人情報を扱う担当者を明確化すること
・ 情報セキュリティの意識向上、教育及び訓練を実施すること

⑦　資産の管理

- 情報及び情報処理施設に関連する資産を洗い出し、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適切な取扱いが担保されていることを示すこと[13]
  （例）JIS Q 27017「JIS Q 27002 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・廃棄すること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

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の対応をすること

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適切な取扱いが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

[13] 外部クラウドなどを活用する場合や、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。

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の操作手順書・管理策を策定、実施すること
- マルウェアからの保護のための検出、予防、回復の管理策を策定、実施すること
- 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を行うこと

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、制御を実施すること
- 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を特定すること
- 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すること
- 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を実施すること（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し、合意のうえ、定期的に監視すること（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、手順の明確化を行い、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

・ 漏えい等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 関係法令等の遵守
・ 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すること
・ プライバシー及び個人情報保護について、関連する法令及び規制を確実に遵守すること
・ 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に定期的なレビューを実施すること

（3）プライバシー保護対策

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。

（プライバシー保護対策等に関し参考とするべき事項等）
■JIS Q 15001 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[14]
■ISO/IEC 29151:2017

[14] 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）

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

（プロファイリングに関する情報銀行の対応）

いわゆるプロファイリング（パーソナルデータとアルゴリズムを用いて、特定個人の趣味嗜好、能力、信用力、知性、振舞いなどを分析又は予測すること[15]）については、情報銀行が自らこれを行う場合のほか、プロファイリング結果を受け取る場合、提供先第三者へ元データを提供する等の形で関与する場合を含め、関係する各主体において利用目的の特定、透明性、データの最小化等の点で必要な配慮がなされるよう、情報銀行において対応すべきである。また、データの処理過程、結果の利用方法等の適切性をデータ倫理審査会において審査することが推奨される。

特に、要配慮個人情報等を推知することにより利用者個人に重大な不利益を与える可能性のあるプロファイリングについては、当該プロファイリングを「要配慮プロファイリング」として、要配慮プロファイリングを取り扱うことのみならず、分析・予測に含まれるロジック（実施する場合）や、利用者個人への影響・リスクに関する有意な情報について明示し、本人同意を得ることが望ましい。また、この際、利用者個人への説明内容、説明方法について、情報銀行における本人関与の実効性を高めるための工夫がなされることが望ましい。

なお、本指針において情報銀行における要配慮個人情報の取扱いは、健康・医療分野の要配慮個人情報について取扱要件を満たした場合のみ認めているが~~られていないことから~~、提供される要配慮個人情報を超えて、新たに要配慮個人情報の項目に相当する情報を生成~~情報銀行において、要配慮個人情報であるプロファイルを取得又は推知~~することのないよう注意する必要がある。

[15] パーソナルデータ+α 研究会「プロファイリングに関する最終提言案」（NBL1211 号 6 頁）

3　ガバナンス体制

（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）相談体制

- 利用者個人や事業者から、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）諮問体制

以下を満たす、社外委員を含む諮問体制（データ倫理審査会）を設置していること

- 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が参加していること
- 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えること
- 情報銀行は定期的に諮問体制に報告を行い、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こと（情報銀行は当該求めに応じて、適切に対応すること）
- 健康・医療分野の要配慮個人情報を取り扱う場合には、要配慮個人情報の取得に当たっての確認、提供先第三者における利用用途の適切性の判断等のため、医療専門職が参加していること

（5）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利用者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
- 利用者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利用者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）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）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（利用者個人との間、必要に応じて情報提供元・提供先第三者との間）

（２）利用者個人への明示及び対応

以下について、利用者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利用・提供する場合はその旨、仮名加工情報に加工して利用する場合はその旨、個人関連情報を取り扱う場合はその旨と取り扱う情報の概要、取得元
・　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、利用者個人がそれを利用するための手続き
・　利用者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[16]

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、利用者個人の合意を得ること

（事業全体）

・　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

[16] 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。

（個人情報等の取扱い）

- 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
- 利用者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
- 個人情報の取扱いの委託を行う場合には、必要な監督を行うこと
- 仮名加工情報を取り扱う場合、その旨を明示し、共同利用は行わず、漏えい等が生じた場合はその事実を公表すること
- 個人関連情報を取り扱う場合、その旨と取り扱う情報の概要、取得元を明示すること
- 健康・医療分野の要配慮個人情報を取り扱う場合、その旨と取り扱う情報の概要、情報の取得・提供に係る判断プロセス等の当該情報の取扱いに当たって特に定めている事項を明示すること

（提供先第三者との関係）

- 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
- 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される
- 例外的に、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ⅰ～ⅲの条件をいずれも満たす場合には、情報銀行は再提供を行う提供先第三者に対して個人情報を提供でき、提供先第三者は当該個人情報を再提供できる

  ⅰ　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

  （ⅰ）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

  （ⅱ）利用者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、提供先第三者が利用者個人から同意取得すること

（ⅲ）再提供先からの更なる第三者提供は認められないこと

ⅱ　提供元（情報銀行）は、利用者個人に対して、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、例えば「金融分野のアグリゲーションサービス」）　を明示すること。再提供については利用者個人により選択可能とし、かつデフォルトオフにすること。利用者個人が提供元（情報銀行）側のユーザーインターフェイス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）が利用者個人から同意を取得する必要はない。

ⅲ　再提供の必要性、すなわち、利用者個人の利便性と、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再提供が利用者個人の指示のもと、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。

・　提供先第三者が認定事業者である場合において、上記ⅰ～ⅲ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」と読み替えて適用する。この場合、利用者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。

・　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。

・　健康・医療分野の要配慮個人情報を提供する場合は、提供先第三者における利用用途の適切性、利用者個人にとって直接的に明確な便益をもたらすものであることの根拠の妥当性等を確認すること。

（４）利用者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

・　提供先第三者・利用目的・データ範囲について、利用者個人が選択できる選択肢を用意すること[17]

・　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、定期的に諮問体

[17] 選択肢の設定については、利用者個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。

制（データ倫理審査会）に説明し助言を受けること
・ 利用者個人が個別の提供先第三者、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）
・ どのデータがどこから提供され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、提供先第三者での利用状況など、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）
・ 利用者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第三者に提供せず、利用しないこと
・ 指示を受けた以降、既に提供先第三者に提供されたデータの利用が当該提供先第三者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、あらかじめ利用者個人に明示すること

④ 情報銀行に委任した個人情報の開示等
・ 簡易迅速で利用者個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及び利用者個人が請求した方法による開示を可能とする仕組みを提供すること[18]
・ 開示されるデータのフォーマットは、可能な限り他の事業者でも使い易い形式とすること
・ 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

（5）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、利用者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利用者個人に損害が発生した場合は、情報銀行は当該個人に対し損害賠償責任を負う

[18] 例えば、情報銀行を営む事業者が、利用者個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。

５　諮問体制（データ倫理審査会）に関する事項

（１）データ倫理審査会における審議の考え方

・　情報銀行は、利用者個人の代理として、利用者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利用者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）

・　利用者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ユーザーインターフェイスで提供されているか

・　利用者個人の同意している提供先第三者の条件について、利用者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

・　利用者個人にとって不利益となる利用がされていないか、利用者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

・　利用者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

（２）審議事項

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

・　利用者個人と情報銀行の間の契約の内容

・　情報銀行に委任した個人情報の利用目的（提供先第三者におけるものを含む）

・　利用者個人により情報銀行に委任され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（ユーザーインターフェイス）

・　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

健康・医療分野の要配慮個人情報を取り扱う場合、上記に加え、以下の事項について助言を行う

・　情報銀行において取り扱うことが可能な健康・医療分野の要配慮個人情報であるか

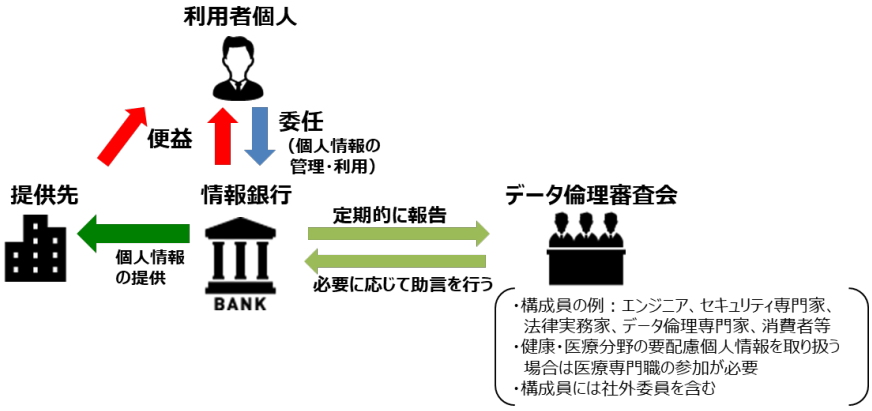
・　提供先における利用用途の適切性

・　利用者個人にとって直接的に明確な便益をもたらすものであることの根拠の妥当性

（３）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

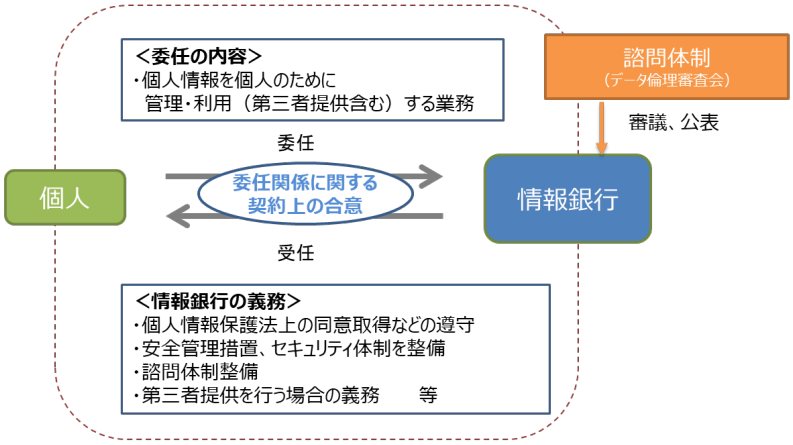

利用者個人
便益
委任
（個人情報の
管理・利用）
提供先
情報銀行
BANK
個人情報
の提供
定期的に報告
必要に応じて助言を行う
データ倫理審査会
・構成員の例：エンジニア、セキュリティ専門家、
法律実務家、データ倫理専門家、消費者等
・健康・医療分野の要配慮個人情報を取り扱う
場合は医療専門職の参加が必要
・構成員には社外委員を含む

Ⅳ　情報信託機能のモデル約款の記載事項

1　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、利用者個人と情報銀行の間の合意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、利用者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、利用者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、より利用者個人のコントローラビリティを確保した、利用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、利用者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利用者個人が未成年者等の制限行為能力者である場合には、①契約の締結と、②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利用者個人が契約を締結することや、法定代理人が利用者個人に代わって契約を締結することが必要となる。

- ②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　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）利用者個人と情報銀行の間

①　目的

・　利用者個人からの委任にもとづき、個人情報を含む利用者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」[19]は含まない~~

・　別段の定めのない限り、用いる用語の定義は個人情報の保護に関する法律に定めるところに従う。

③　情報銀行の行う業務範囲

・　情報銀行は、利用者個人に代わって当該個人の個人情報について、当該個人の合理的利益が得られるような活用手法、提供先第三者の選定、第三者提供、個人情報の維持・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利用者個人に不利益が生じないよう配慮すること）

・　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（要件を満たした上で取り扱うことができる健康・医療分野の要配慮個人情報[20]を除く。）

・

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

---

[19] ~~本指針Ⅱ３（２）に記載の健康・医療分野の情報は、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。~~

[20] 情報銀行において取り扱うことが可能な健康・医療分野の要配慮個人情報は、Ⅱ３（２）「事業で扱うデータの種類」参照。

（個人情報等の取扱い）

- 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第三者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
- 利用者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、具体的事業内容に照らした便益を含む）の明示
- 個人情報の取扱いの委託を行う場合には、必要な監督を行うこと
- 情報漏えい等発生の場合、法令の定めに従い個人情報保護委員会への報告、利用者個人への通知を行うこと
- 仮名加工情報を取り扱う場合、その旨を明示し、共同利用は行わず、仮名加工情報の漏えい等の際は、個人情報保護委員会への報告・利用者個人への通知ではなく、漏えい等の事実の公表を行うこと
- 個人関連情報を取り扱う場合、その旨と取り扱う情報の概要、取得元を明示すること
- 健康・医療分野の要配慮個人情報を取り扱う場合、その旨と取り扱う情報の概要、情報の取得・提供に係る判断プロセス等の当該情報の取扱いに当たって特に定めている事項を明示すること
-

（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、当該提供先第三者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、提供先第三者にも、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、提供先第三者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

利用者個人が情報銀行に委任した情報の取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（仮名加工情報である個人情報の場合、開示請求の対象とならないことを明示すること）

⑦　利用者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、利用者個人は、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（利用者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　利用者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の求め（過剰な内容とならないよう留意すること）があった場合には適切な対応につとめること

⑨　相談窓口

・　情報銀行は利用者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、利用者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利用者個人に損害が発生した場合は、情報銀行は当該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際、当該情報提供元から取得する場合や利用者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

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（利用者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、利用者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　情報漏えい等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）情報銀行と提供先第三者との間

①　提供されるデータの「形式」「提供方法」等に関する規定

②　提供先第三者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（利用者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）特に、健康・医療分野の要配慮個人情報を取り扱う場合には、Ⅱ３（５）の健康・医療分野の要配慮個人情報を取り扱うサービスに係る要件に関する規定

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、提供先第三者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　提供先第三者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　情報漏えい等の際の原因究明に向けた、提供先第三者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

Ⅴ　情報信託機能の認定スキーム

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

・　申請の対象となる事業が健康・医療分野の要配慮個人情報を取り扱うものである場合は、医療専門職が有識者として参加する認定委員会による、データ倫理審査会において利用用途が適切であると判断していることの確認（更新時においては、認定以降、データ倫理審査会が利用用途や提供先の確認を適切に行っていたかどうかの確認）

・

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　認定基準違反、個人情報漏えい等の場合の対応

・　認定基準に違反した場合、個人情報漏えい等の場合は、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、判断する

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・報告徴収などを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