「情報信託機能の認定に係る指針Ver2.1」

情報信託機能の認定スキームの在り方に関する検討会

令和３年８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

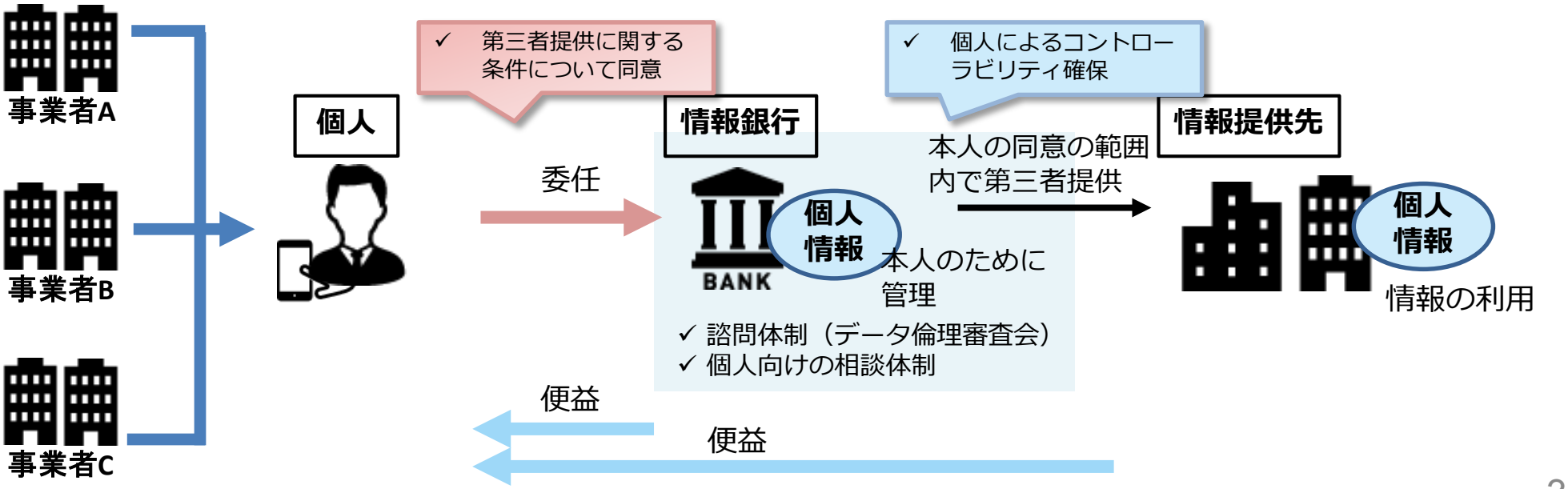
「情報銀行」は、実効的な本人関与（コントローラビリティ）を高めて、パーソナルデータの流通・活用を促進するという目的の下、本人が同意した一定の範囲において、本人が、信頼できる主体に個人情報の第三者提供を委任するというもの。

【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。

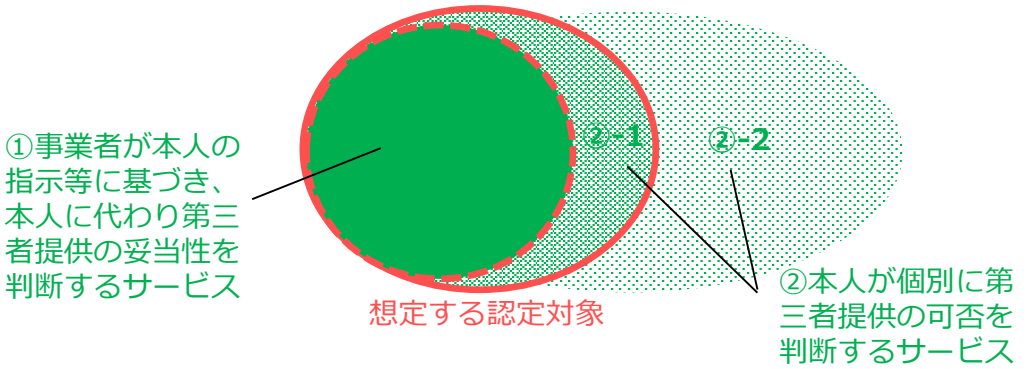


本指針の対象とするサービス

（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。

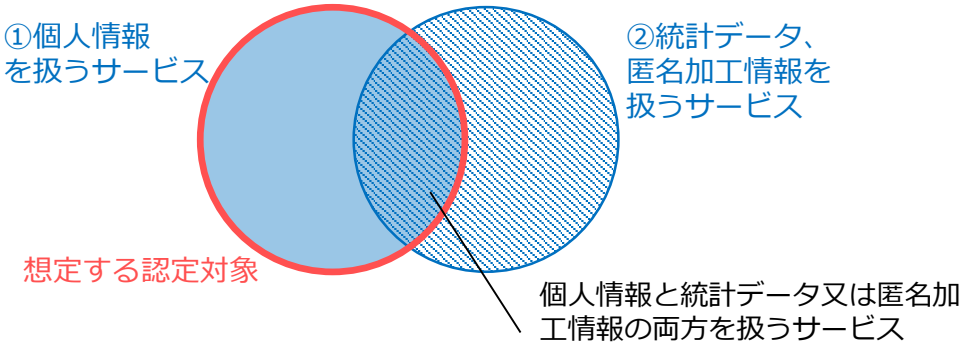
※②本人が個別に第三者提供の可否を判断するサービスのうち、提供事業者が情報の提供先を選定して個人に提案する場合など、提供事業者が比較的大きな役割を果たす（責任をもつ）ケース（②-1）を想定。他方、純粋なＰＤＳなどデータの管理や提供に関し個人の主体性が強いサービス（②-2）まで認定の対象として想定している訳ではない（認定がないことをもって信頼性が低いと評価されるべきものではない）。
※なお、データ保有者と当該データの活用を希望する者を仲介し、売買等による取引を可能とする仕組み（市場）である「データ取引市場」については認定の対象外。



（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。

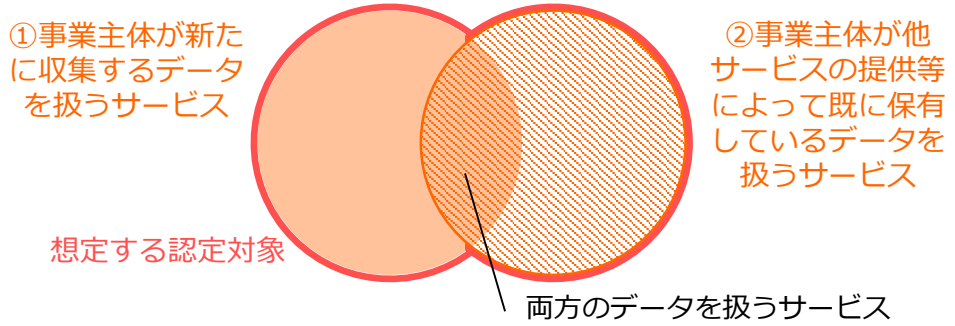
	項目
1	歩行測定（歩数・歩幅・ピッチ・接地角度・離地角度・外回し距離）
2	体重
3	体脂肪
4	体温
5	血圧
6	脈拍
7	心拍数
8	消費カロリー
9	摂取カロリー
10	睡眠時間
11	月経日

	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、提供先が第三者認証等の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、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、提供先に提供する

③ 情報銀行の監督下で、提供先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/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 27001：2013 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 https://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Management_Standard_H28.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。

（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。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。

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。

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

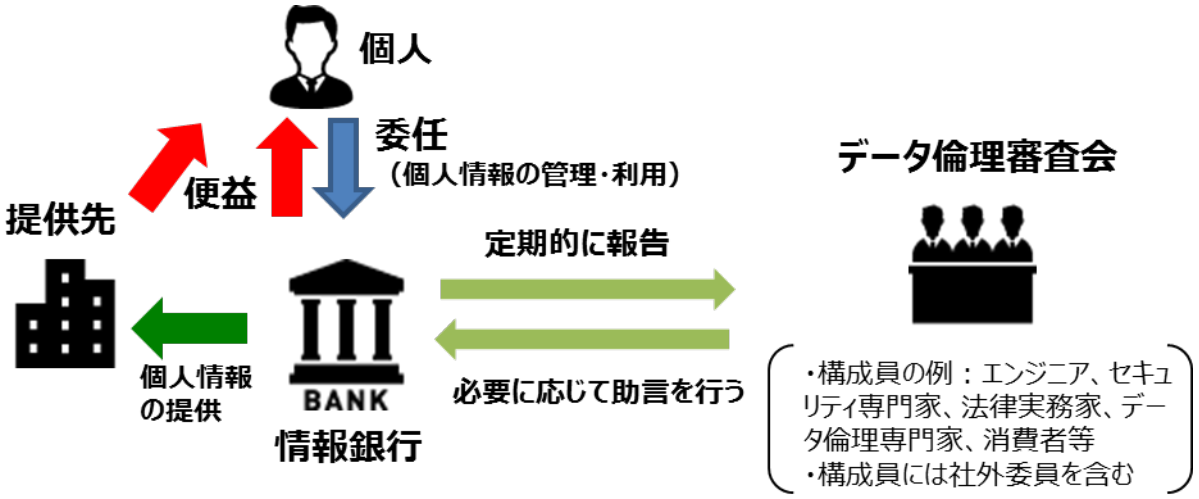
項目	内容
⑤個人のコントローラビリティを確保するための機能について	①情報銀行に委任した個人情報の第三者提供に係る条件の指定及び変更 ・提供先・利用目的・データ範囲について、個人が選択できる選択肢を用意すること(※1) ・選択を実効的なものとするために適切なユーザーインターフェイス（操作が容易なダッシュボードなど）を提供すること ・選択肢及びユーザーインターフェイスが適切に設定されているか、定期的にデータ倫理審査会などの諮問体制に説明し助言を受けること ・利用者が個別の提供先、データ項目等を指定できる機能を提供する場合には、その旨を明示すること
	②情報銀行に委任した個人情報の提供履歴の閲覧（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

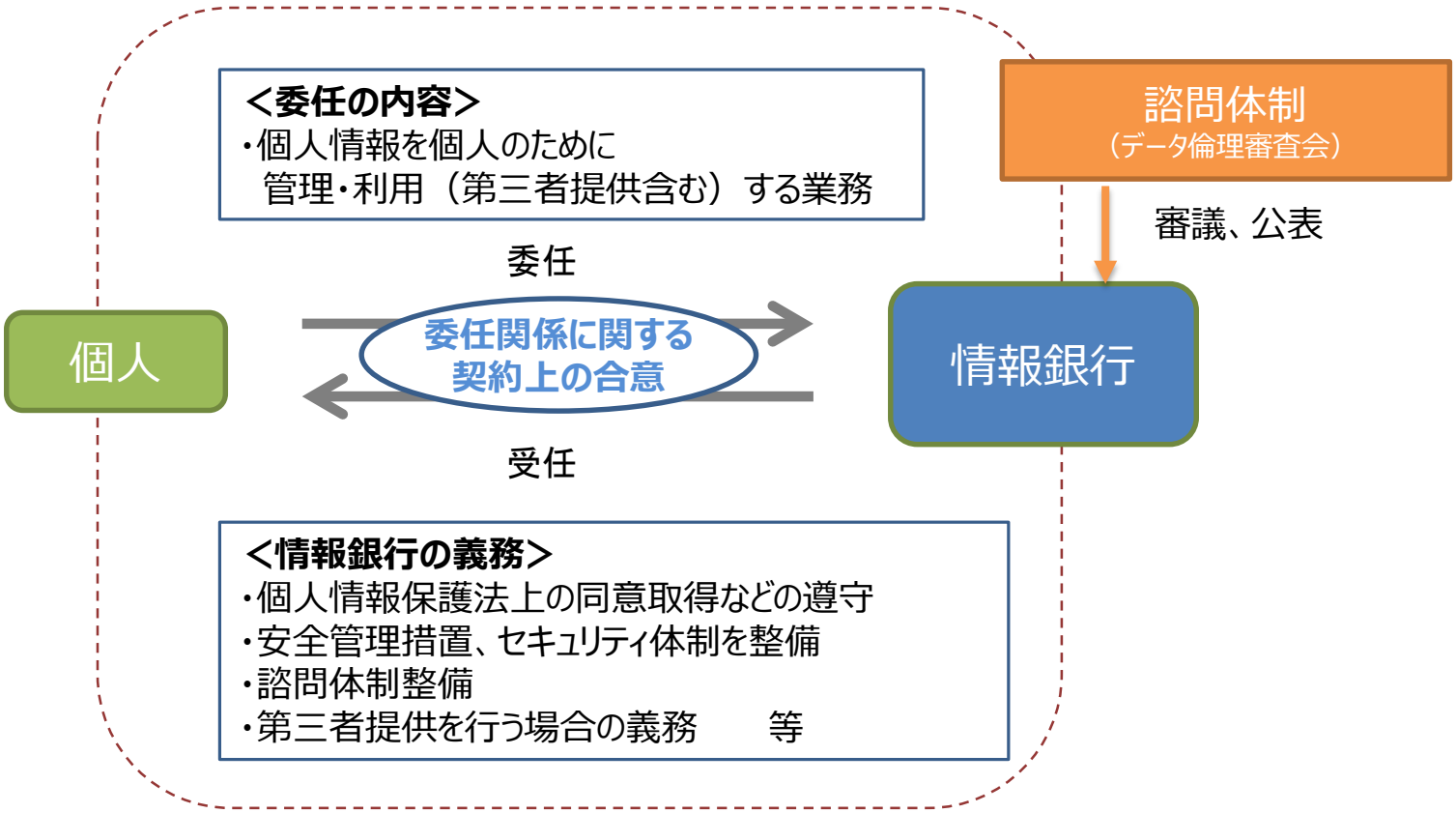
■　情報信託機能を提供する「情報銀行」のサービスについて、債権債務の内容や情報銀行の責任範囲を明確化するため、**個人と情報銀行の間を委任関係に関する契約上の合意**と整理する。

■　「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