

「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

1) 事業者の適格性

項目	内容
②業務能力など	<ul style="list-style-type: none"> ・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
	<ul style="list-style-type: none"> ・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を有している 等
	<ul style="list-style-type: none"> ・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
	<ul style="list-style-type: none"> ・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

(※) 情報銀行は、提供先がPマークまたはISMS認証、FISC安全対策基準などの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、一覽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必要がある。
 - ・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	<ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・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 <p>※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</p>
⑧技術的セキュリティ	<p>（アクセス制御）</p> <ul style="list-style-type: none"> ・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 <p>（暗号）</p> <ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・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 ・技術的せい弱性管理、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	<ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・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

■(参考)個人情報保護法ガイドライン(通則編)86頁以降抜粋

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)

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	・従業員の教育
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

※修正あり

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・行動原則等を含み、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

※修正あり

項目	内容
①契約約款の策定	<ul style="list-style-type: none">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	<p>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）</p> <ul style="list-style-type: none">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 (※)	<p>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</p> <ul style="list-style-type: none">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べきである。

4) 事業内容

※修正あり

項目	内容
④情報銀行の義務について	<ul style="list-style-type: none">・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ル性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、個人のコントロール性が確保され、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（または会社名）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ル性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）**具体的には、以下の3点を要件とする。**

- (1) 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

- (2) 再提供先のサービスは提供先のサービスを前提とするものであること

- (3) 再提供について、個人にとっての明確な利便性が認められること

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
<p>⑤個人のコントロール性を確保するための機能について</p>	<p>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</p> <ul style="list-style-type: none"> ・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 <p>②情報銀行に委任した個人情報の提供履歴の閲覧（トレサビリティ）</p> <ul style="list-style-type: none"> ・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 <p>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）</p> <ul style="list-style-type: none"> ・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 <p>④情報銀行に委任した個人情報の開示等</p> <ul style="list-style-type: none"> ・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へデータを移転する機能の有無を明示すること
<p>⑥責任の範囲について</p>	<ul style="list-style-type: none"> ・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

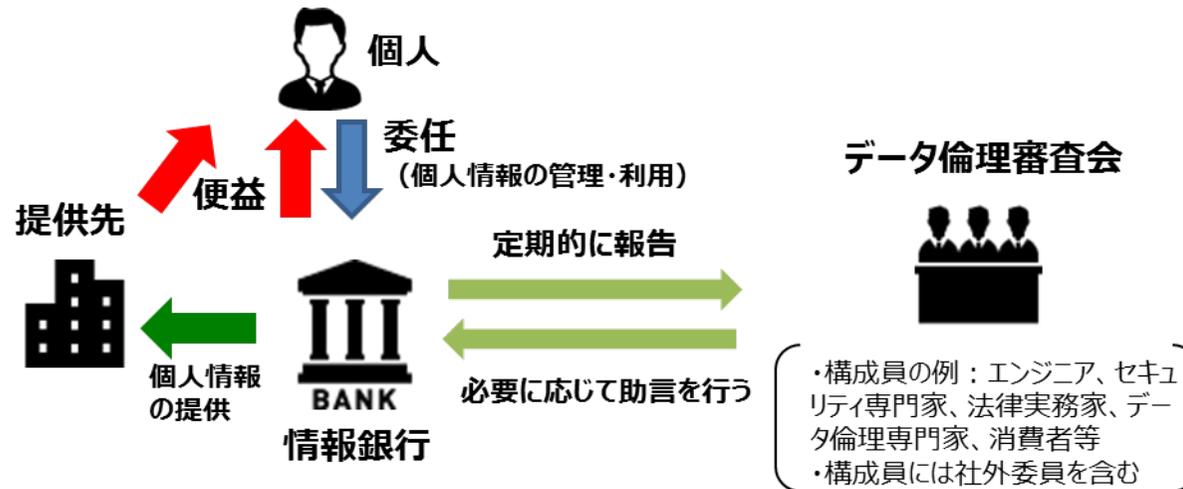
(※1) 選択肢の設定については、本人が第三者提供について判断できる情報を提供する必要があるため、例えば、「上場企業／その他含む」「観光目的／公共目的」のように数の少ない分類方法から、より個別具体的で数の多い分類方法までが考えられる。

(※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ル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