参考資料８－３

「情報信託機能の認定に係る指針ver1.0」

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

（はじめに）

- 個人情報を含むパーソナルデータの円滑な流通を実現するため、これまで内閣官房等で議論されてきた個人の関与の下での新たなサービスを早期に立ち上げることが期待される。
- その一つである情報信託機能を提供する「情報銀行」については、一定の要件を満たした者を社会的に認知するため、民間の団体等による任意の認定の仕組みが望ましいとの提言がなされている。
- この認定の仕組みを有効に機能させるためには、個人情報保護法の趣旨も踏まえた、また、本人の関与という要素を十分に取り込んだ「認定基準」や「モデル約款」が非常に重要となる。
- 本検討会では以下の認識の下、認定基準等について検討を行ってきた。
    - 新しいサービスを普及させるためには、利用者や社会の信頼を得ることが大切であり、一定の信頼性を満たす者を認定するとともに、個人のコントローラビリティを確保する必要がある。
    - 他方、このようなサービスは現時点では存在せず、今後、その出現が期待される分野であるため、サービスの内容やビジネスモデルを限定することは望ましくなく、様々なタイプのサービスが提供され、事業者の競争を促すような認定基準とすることが必要である。
- 本検討会では平成29年11月～平成30年4月までの計６回に及ぶ議論を踏まえ、認定基準等を「情報信託機能の認定に係る指針ver1.0」（案）としてとりまとめた。
- 今後、総務省による実証、これからのサービスの展開や関連制度の運用状況等を踏まえ、継続して議論・見直しを行っていくことが求められる。その際、ver1.0では対象外とした要配慮個人情報等の扱いについても検討を行うべきである。（※）

＜認定に係る「指針」＞

- 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、認定を行う団体は、本指針に基づき、認定制度を構築・運用する
- 将来的には、認定基準及び認定スキームについては、本検討会及び認定団体において継続的に見直しを行う（モデル約款は民間企業における多様な活動をサポートするため、例えば認定団体によって分野別に複数作られるなどに多様な進化をしていくもの）

※見直した場合には、認定事業の適切な更新の仕組みが必要となる。

情報信託機能に関する検討の概要

情報信託機能に関する検討の経緯

● **データ流通環境整備検討会（内閣官房ＩＴ総合戦略室）**
「AI、IoT時代におけるデータ活用WG 中間とりまとめ」（平成29年2月）

（ポイント）

・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には、個人の関与の下でデータ流通・活用を進める仕組み（情報銀行等）が有効。

・情報銀行等については、分野横断的なデータ活用に向けた動きが出始めており、今後、事業者、政府等の連携により、その社会実装に向けて積極的に取組を推進する必要がある。

・本検討会で提示した分野横断的かつ基本的な課題、推奨ルール等を参考として、政府や消費者を含めた多様な関係者が参画した実証実験等の取り組みが各分野で進められるとともに、自主ガイドラインを含めたルール作りについての議論が深まることで、国民・消費者の信頼・理解が得られていくことが期待される。

● **情報通信審議会（総務省）**
「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（平成29年7月）

（ポイント）

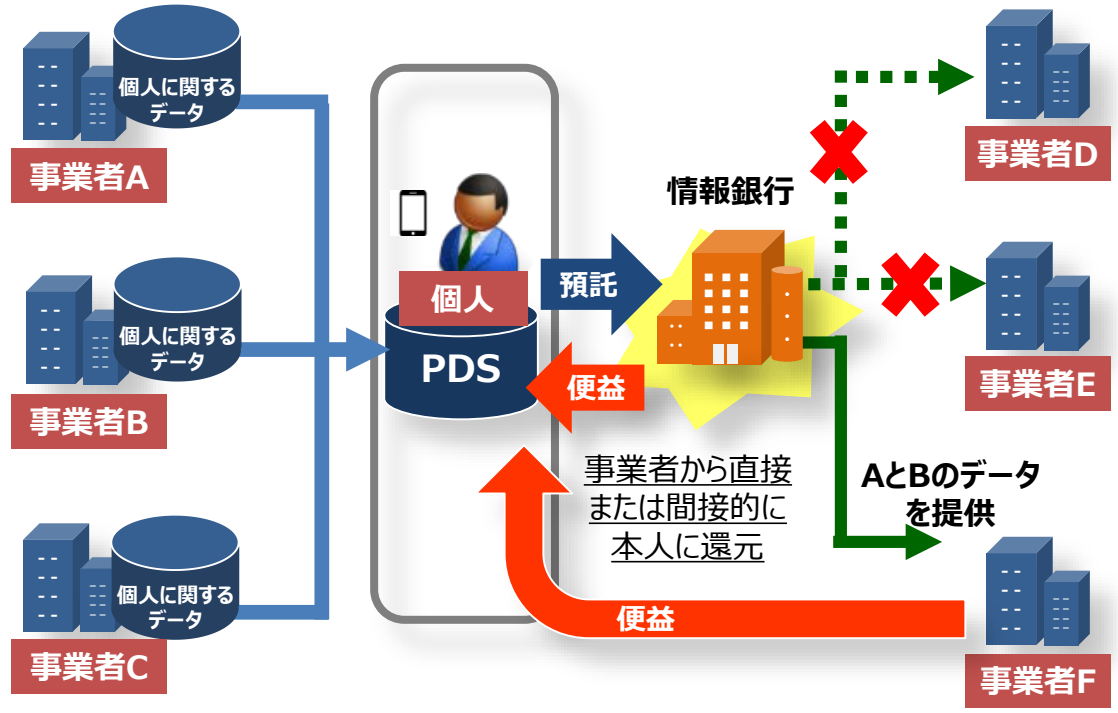
・情報信託機能を担う者について、一定の要件を満たした者を社会的に認知するため、民間の団体等によるルールの下、任意の認定制度が実施されることが望ましい。

・情報信託機能については、2017年夏以降、必要なルールを更に具体化するための実証事業を継続するとともに、2017年中に、産学が連携して推進体制を整備し、任意の認定制度やルールの在り方について検討し、年内に認定業務に着手することを目指す。

「情報銀行」の定義

情報銀行（情報利用信用銀行）とは、個人とのデータ活用に関する契約等に基づき、PDS等のシステムを活用して個人のデータを管理するとともに、個人の指示又は予め指定した条件に基づき個人に代わり妥当性を判断の上、データを第三者（他の事業者）に提供する事業。

情報銀行のイメージ



※　本人には便益が還元されず、社会全体にのみ便益が還元される場合もある。

「AI、IoT時代におけるデータ活用ワーキンググループ　中間とりまとめの概要」（内閣官房IT総合戦略室）より

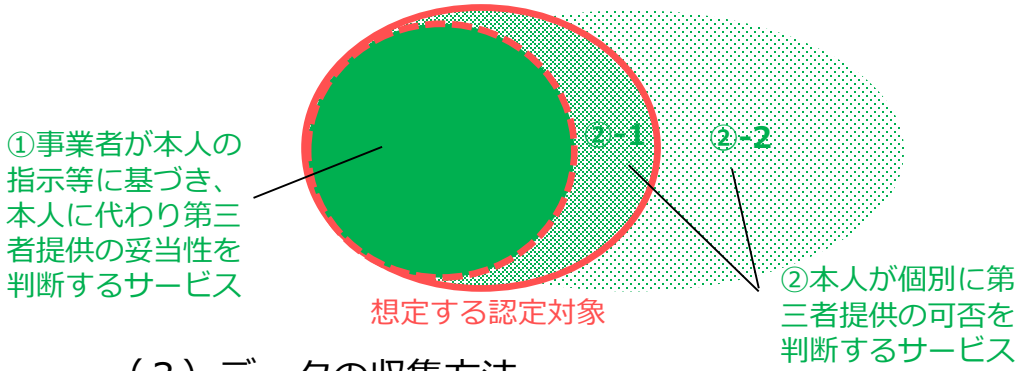
とりまとめの基本的な考え方

（認定の対象について）

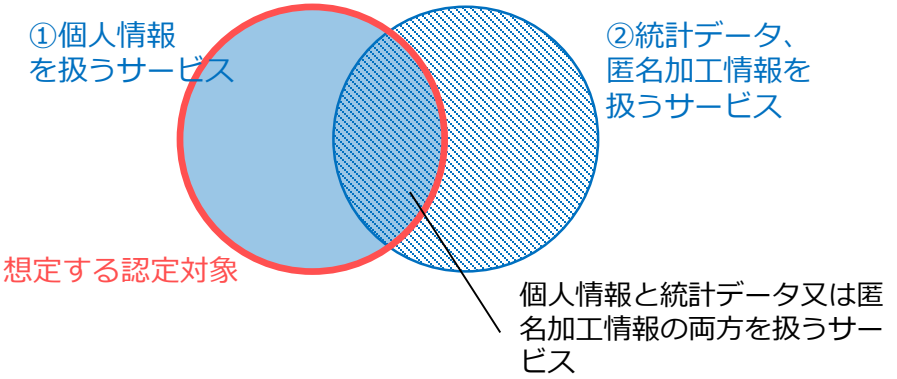
- 「認定」はあくまで任意のものであり、認定を受けることが事業を行うために必須ではない。
- 認定の対象は、①事業者が個人情報の第三者提供を本人が同意した一定の範囲において本人の指示等に基づき本人に代わり第三者提供の妥当性を判断するサービスが基本であるが、様々な形態の事業の出現を想定し、②本人が個別に第三者提供の可否を判断するサービスも含むこととする。（※）

※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。

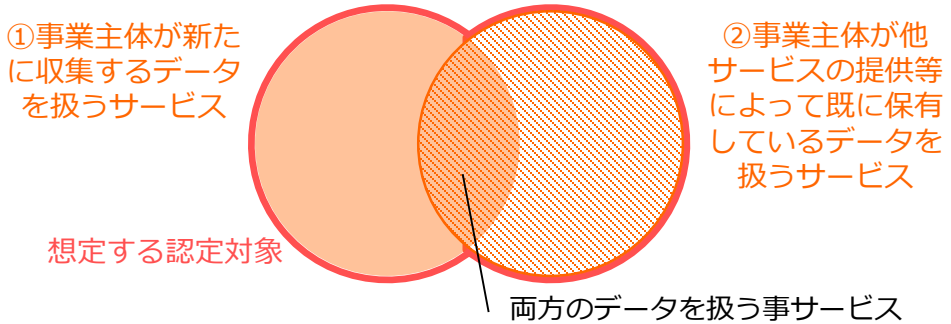
（１）個人情報の提供に関する同意の方法



（２）データの種類



（３）データの収集方法



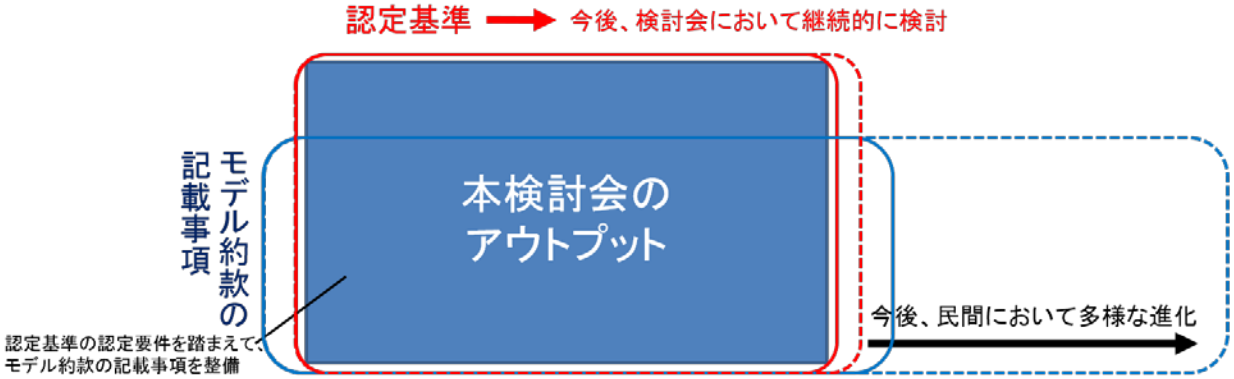
※本検討会で対象とする「個人情報」には、「要配慮個人情報」「クレジットカード番号」「銀行口座番号」は含まない

（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」とは、消費者個人を起点としたサービスとして、また、個人情報の取扱を委任するサービスとして、消費者の便益、委任の内容等について事業者と消費者の間の契約の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。



（個人のコントローラビリティの確保について）

- 「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と活用を促進するという目的の下、本人が、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、信頼できる主体に委任するというもの。
- 他方、現時点において情報銀行は存在しておらず、データの流通促進を進めるという社会的要請を踏まえ、情報銀行が市場に登場し、競争する環境を整備することが急務。
- 認定基準及びモデル約款における、「個人のコントローラビリティを確保するための機能」については、以上のような観点からコントローラビリティとサービスの多様性とのバランスを考慮したもの。

※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スキームの在り方に関する検討会」構成員

【委員】

	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　副本部長
	上原　哲太郎	立命館大学情報理工学部情報システム学科 教授
	加毛　明	東京大学大学院法学政治学研究科　准教授
	越塚　登	東京大学大学院情報学環 ユビキタス情報社会基盤センター長・教授
	小林　慎太郎	株式会社野村総合研究所 ICT・メディア産業コンサルティング部 パブリックポリシーグループマネージャー／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　執行役員
	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	全国地域婦人団体連絡協議会　事務局長
	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　チーフコンサルタント
	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　常任顧問
	森　亮二	英知法律事務所　弁護士
	若目田　光生	一般社団法人日本経済団体連合会 情報通信委員会企画部会 データ戦略WG　主査 日本電気株式会社　データ流通戦略室長

【オブザーバー】

真野　浩	一般社団法人データ流通推進協議会　代表理事
美馬　正司	株式会社日立コンサルティング 公共コンサルティング本部ディレクター
石原　遥平	一般社団法人シェアリングエコノミー協会
山本　龍彦	慶應義塾大学法務研究科教授
太田　祐一	株式会社Data Sign代表取締役社長

【関係省庁（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

【事務局】

一般社団法人日本IT団体連盟

株式会社富士通総研（※調査協力のみ）

« 開催実績 »

・第１回　２９年１１月７日（火）
・第２回　３０年１月１０日（水）
・第３回　　２月２３日（金）
・第４回　　３月２３日（金）
・第５回　　４月１９日（木）
・第６回　　４月２４日（火）

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
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）類似の業務経験を有する、プライバシーマーク・ISMS認証などの認証を有している　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

2）情報セキュリティ等①

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。 ・次頁の「情報セキュリティ②③具体的基準」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）情報セキュリティ等②　具体的基準

項目	内容
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
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
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
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
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
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
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
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③　具体的基準

項目	内容
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
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
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）
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
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
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
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
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）参考：プライバシー保護対策等について

前述の、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十分に整備・遵守していくことが必要である。

また、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。

なお、参考まで個人情報保護法ガイドラインに定められている措置の項目を掲載する。

※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なる事項等）

■JISQ15001個人情報保護マネジメントシステム（要求事項）

■ISO/IEC 29100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

Table 3 – The privacy principles of ISO/IEC 29100

1. Consent and choice
2. Purpose legitimacy and specification
3. Collection limitation
4. Data minimization
5. Use, retention and disclosure limitation
6. Accuracy and quality
7. Openness, transparency and notice
8. Individual participation and access
9. Accountability
10. Information security
11. 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
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（仮称）） ・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
④透明性（定期的な報告・公表）	・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
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①

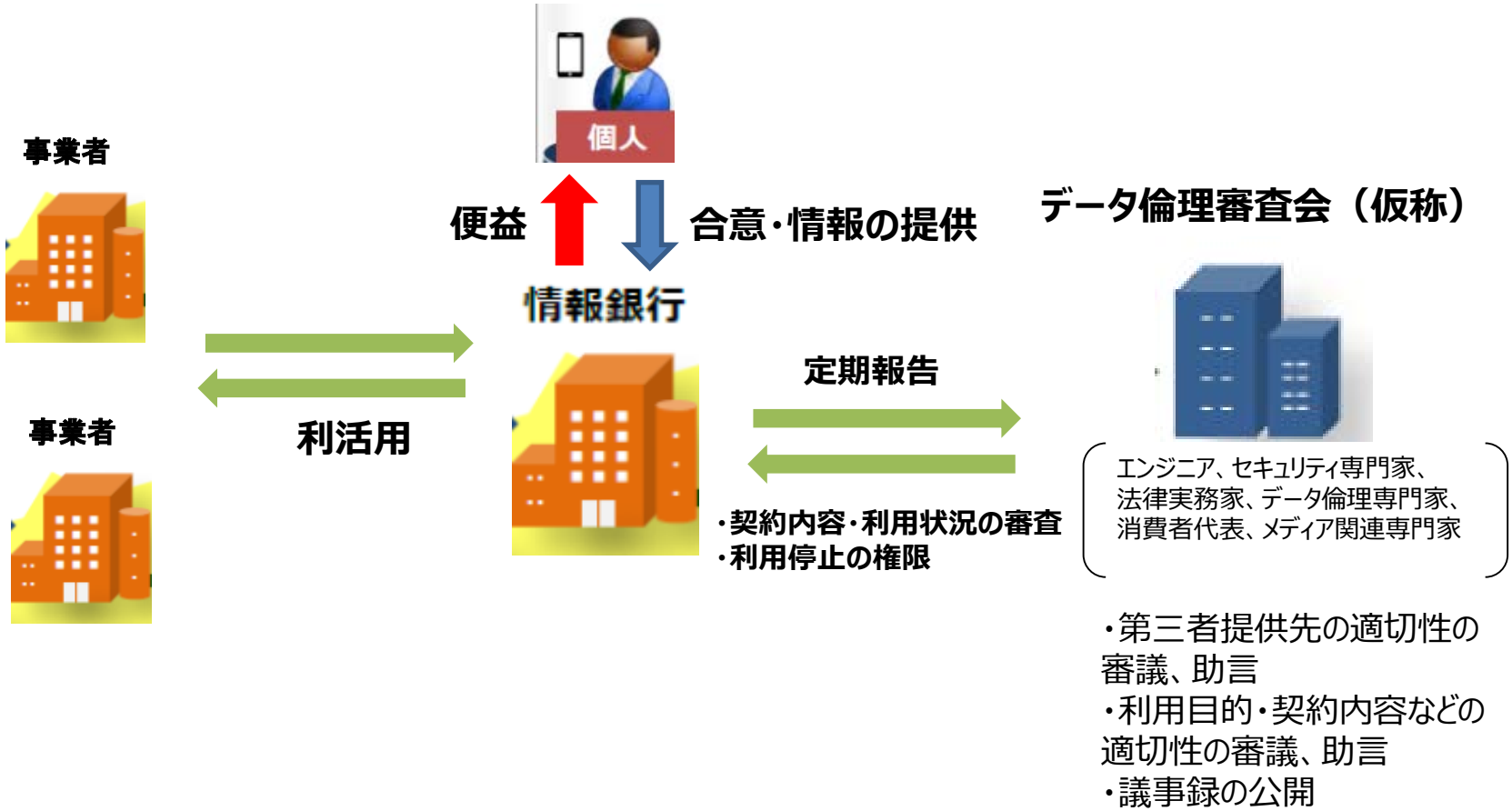
項目	内容
契約約款の策定	・モデル約款の記載事項に準じ、認定団体が定めるモデル約款を踏まえた契約約款を作成・公表していること（又は認定後速やかに公表すること）　（個人との間、（必要に応じて）情報提供元・情報提供先事業者との間）
個人への明示及び対応	以下について、個人に対しわかりやすく示すとともに個人情報の利用目的及び第三者提供について個人情報保護法上の同意を取得すること（同意取得の例：包括的同意、個別同意など） ・情報銀行の行う事業及び対象とする個人情報の範囲、事業による便益 ・対象となる個人情報とその取得の方法、利用目的 ・個人情報の第三者提供を行う場合の提供先第三者及び利用目的に関する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
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（同意の取得を含む）をはじめ、関係する法令を遵守すること ・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(仮称) 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 （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再提供の禁止 ・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 ・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について規定すること

４）事業内容②

項目	内容
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(仮称)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、他の事業者へのデータの移行等いわゆるデータポータビリティ機能を提供する場合には、その旨を明示すること
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（仮称））のイメージ



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

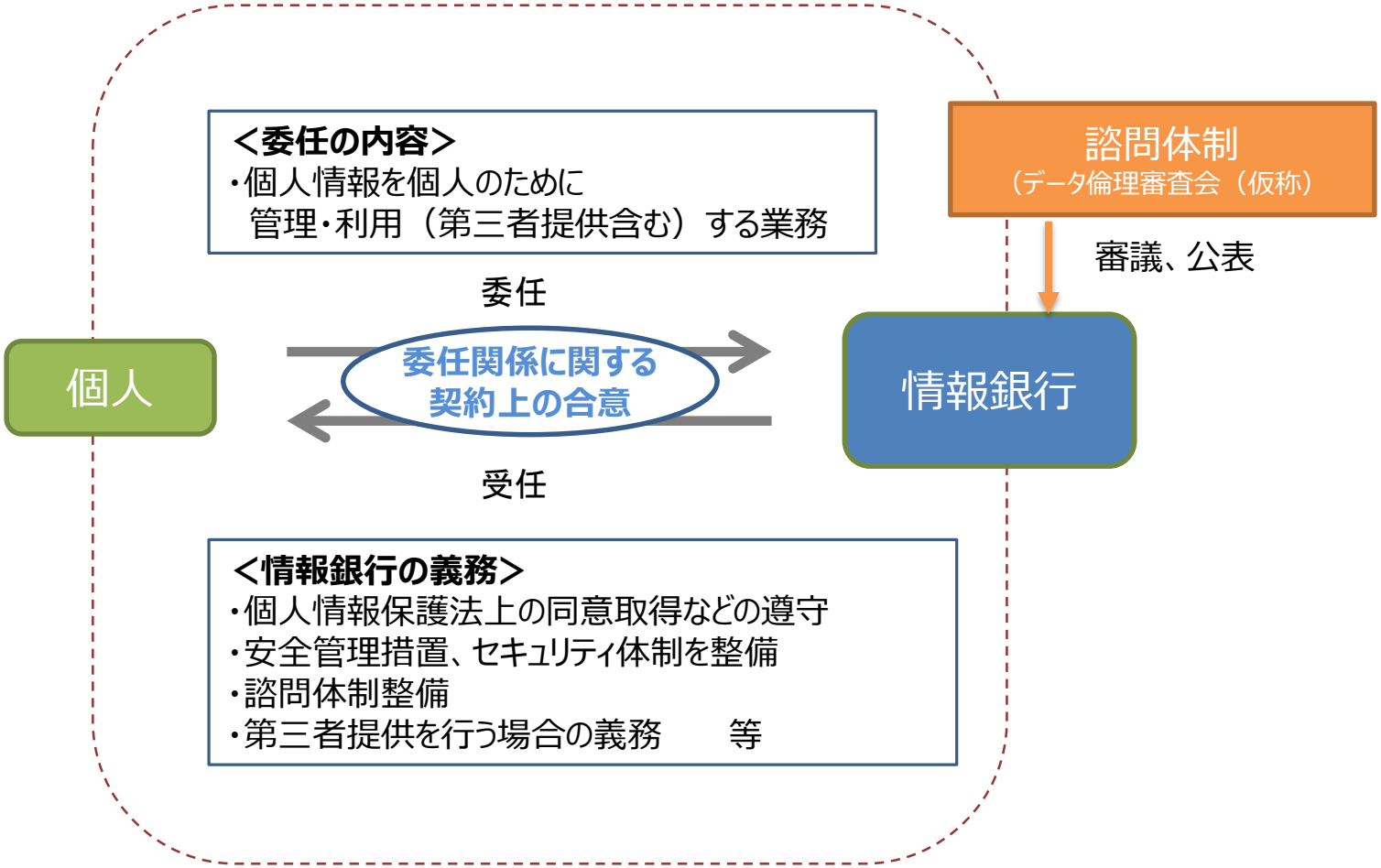
■　情報信託機能を提供する「情報銀行」のサービスについて、債権債務の内容や情報銀行の責任範囲を明確化するため、**個人と情報銀行の間を委任関係に関する契約上の合意**と整理する。

■　「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

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」「クレジットカード番号」「銀行口座番号」は含まない

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(仮称)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

（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再提供は禁止する
・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
・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、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、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等）

３）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

４）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

５）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

６）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