「情報銀行」認定申請ガイドブック

ver. 2.01

一般社団法人　日本IT団体連盟
情報銀行推進委員会

2021 年 7 月 1 日

（制改訂履歴）

版	制改訂年月日	内容
1.0 版	2018 年 12 月 21 日	新規制定、施行
2.0 版	2020 年 7 月 1 日	指針 ver2.0 への対応ほか（巻末別添「変更履歴表」参照）
2.01 版	2021 年 7 月 1 日	・サーベイランス審査及び認定付与の更新に関する説明を追加 ・参考基準等の名称・URL を更新 ・提出書類（例）及び脚注を加筆修正 （巻末別添「変更履歴表」参照。認定基準の変更は無し。）

目次

1　はじめに ..... - 1 -
1.1　はじめに ..... - 1 -
1.2　本書の概説 ..... - 4 -
1.2.1　「情報銀行」認定の意義 ..... - 4 -
1.2.2　「情報銀行」認定審査について ..... - 4 -
1.2.3　認定の種別 ..... - 4 -
1.2.4　本資料の構成・見方 ..... - 4 -
1.2.5　著作権の取り扱い ..... - 5 -
1.2.6　改訂について ..... - 5 -
2　認定の対象となる「情報銀行」の範囲 ..... - 6 -
3　運用スキーム ..... - 11 -
4　申請・認定フロー ..... - 14 -
4.1　全体フロー ..... - 14 -
4.2　事前申請フロー ..... - 15 -
4.2.1　事前申請の目的 ..... - 16 -
4.2.2　事前申請のエントリー ..... - 16 -
4.2.3　事前申請必要書類の作成～提出 ..... - 16 -
4.2.4　事前申請の受領、確認 ..... - 16 -
4.2.5　事前申請ミーティングの実施 ..... - 16 -
4.2.6　審査計画書の提示～本申請の検討 ..... - 17 -
4.3　本申請フロー ..... - 18 -
4.3.1　本申請書の提出 ..... - 20 -
4.3.2　本申請の受領と審査料の請求処理～入金 ..... - 20 -
4.3.3　秘密保持契約の締結 ..... - 20 -
4.3.4　キックオフミーティング ..... - 20 -
4.3.5　審査書類の提出 ..... - 20 -
4.3.6　書類審査 ..... - 21 -
4.3.7　回答期限と取り下げの判断 ..... - 21 -
4.3.8　書類審査の終了 ..... - 21 -
4.4　認定決定フロー ..... - 22 -
4.4.1　適合性評価・認定判定 ..... - 23 -
4.4.2　契約書の締結及び認定料の請求～入金 ..... - 23 -
4.4.3　認定の付与 ..... - 23 -
4.4.4　認定の公表 ..... - 23 -
4.4.5　サーベイランス審査 ..... - 23 -
4.4.6　認定の取消し等 ..... - 24 -
4.4.7　認定付与の更新 ..... - 24 -
5　認定基準と提出書類 ..... - 25 -

5.1 事業者の適格性 - 25 -
5.1.1 事業者の適格性の具体的基準 - 25 -
5.2 情報セキュリティ・プライバシー - 28 -
5.2.1 基本原則及び遵守基準 - 28 -
5.2.2 情報セキュリティの具体的基準 - 29 -
5.3 プライバシー保護対策 - 35 -
5.3.1 基本原則 - 35 -
5.3.2 プライバシー保護対策の具体的基準 - 35 -
5.4 ガバナンス体制 - 45 -
5.4.1 ガバナンス体制の具体的基準 - 45 -
5.5 事業内容 - 50 -
5.5.1 事業内容の具体的基準 - 50 -
6 モデル契約約款 - 55 -
6.1 個人情報の提供に関する契約上の合意の整理 - 55 -
6.2 モデル契約約款 - 56 -
① 個人と「情報銀行」の間 - 56 -
② 「情報銀行」と情報提供元との間 - 58 -
③ 「情報銀行」と情報提供先との間 - 58 -

1 はじめに

1.1 はじめに

消費者個人が各種サービスを利用する際、当該個人のプロフィール、位置情報、購買履歴、検索履歴等を含む個人情報が当該サービスを提供する企業によって収集され、それらの個人情報の一部は第三者に提供されている場合がある。

この点、消費者個人においては、その個人情報の第三者提供に同意した覚えが無い、提供された個人情報が何に使われているか十分に理解していない、第三者提供をやめさせる方法がわからない等の不安、そして、企業側においては、消費者が同意内容を正確に理解しているか懸念している、レピュテーションリスクが心配である等の個人情報の利活用にあたっての躊躇が見られるのが現状である。

「個人情報の保護に関する法律」（平成 15 年法律第 57 号。以下「個人情報保護法」。）第 23 条第 1 項等[1]においては、個人情報の「第三者提供の制限」について、原則として本人の同意を必要と規定されており、同法に基づき企業が消費者個人の同意を取得してはいるものの、実態としては、以上のとおり事業者の同意の取り方又は消費者個人の意識が十分ではない等のケースがあり、そのギャップを埋めるための取組が求められている。

個人情報を含むパーソナルデータの円滑な流通について、政府による様々な取組みが進められてきている。

2016 年に「官民データ活用推進基本法」（平成 28 年法律第 103 号）[2]が成立し、同法第 12 条において、「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」として、「国は、個人に関する官民データの円滑な流通を促進するため、事業者の競争上の地位その他正当な利益の保護に配慮しつつ、多様な主体が個人に関する官民データを当該個人の関与の下で適正に活用

---

[1] 第二十三条　個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。
一　法令に基づく場合
二　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。
三　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。
四　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。
また、「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）」（平成 28 年 11 月（平成 29 年 3 月一部改正）個人情報保護委員会）では次のとおり規定されている。
個人情報取扱事業者は、個人データの第三者への提供に当たり、あらかじめ本人の同意（略）を得ないで提供してはならない（略）。同意の取得に当たっては、事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）等に応じ、本人が同意に係る判断を行うために必要と考えられる合理的かつ適切な範囲の内容を明確に示さなければならない。
なお、あらかじめ、個人情報を第三者に提供することを想定している場合には、利用目的において、その旨を特定しなければならない（略）。
以上を含む個人情報保護関連法令・ガイドライン等については、個人情報保護委員会ウェブページ（http://www.ppc.go.jp/personalinfo/legal/）参照。

[2] IT 総合戦略本部ウェブページ（https://www.kantei.go.jp/jp/singi/it2/hourei/deta_katsuyosuishin.html）参照。

することができるようにするための基盤の整備その他の必要な措置を講ずる」と規定された。

2017 年 2 月には、「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）の下に設置された「データ流通環境整備検討会 AI、IoT 時代におけるデータ活用ワーキンググループ」（以下「データ活用 WG」。）[3]において「中間とりまとめ」が行われ、「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の流通・活用を進める仕組みである PDS、情報銀行、データ取引市場が有効」とされ、「情報銀行（情報利用信託銀行）」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きた段階であり、今後、事業者、政府等が連携してその社会実装に向けて積極的に取り組みを推進する必要。」とされた。

上記中間とりまとめでは、特に「情報銀行の意義」として、消費者個人「自らが示した一定の範囲内で第三者（他の事業者）へデータ提供するよう信頼できる者に委託することで、自ら個別に判断する必要なく、データ活用の便益を享受でき（略）、また、信頼に足る情報銀行が関与することで、データホルダーから個人へデータを戻しやすくなるとともに、個人にとって第三者へのデータ提供の障壁が低くなるなど、より多くのデータの流通・活用が進むことが期待される」とされた。

また、「情報銀行と個人情報保護法との関係」について、「自らの指示又は予め指定した条件（例えば、第三者におけるデータの活用目的・公益性、本人又は社会に還元される便益、情報の機微性等を勘案したもの）の範囲で情報銀行が個別の第三者提供を行うことに本人が同意している場合には、本人同意に基づく第三者提供と整理することができる」とされた。そのため、「情報銀行は、第三者提供に係る有効な本人同意を確保する観点から、パーソナルデータの第三者提供の条件等についてあらかじめ分かりやすく明確に説明するほか、第三者提供の状況について定期的に本人に報告・対話するなど本人の意向の把握・確認・反映に努め、本人が希望する場合には第三者提供を停止するといった措置を講ずることが望ましい」とされている。

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[4]においては、「情報銀行」について、「今後、情報信託の機能を提供する事業者が現れ、実際に事業を遂行する場合において、当該事業が適切に運営されるためには、情報信託機能の信頼性を確保するための社会的な仕組みが必要」とされた。具体的には、「本人にとっては、自らが提供したデータが個別には把握していない第三者に渡ることにつき、漠然とした不安があり、データを提供することによる便益も把握しづらいことから、概して、データの提供には消極的な姿勢が示される」ことから、「このような消極的姿勢を解消し、情報信託機能を提供する事業が適切に認知されるためには、パーソナルデータを提供する明確なメリットを提示するだけでなく、本人の不安を軽減し、安心・安全にデータを預けることを可能とするため（略）、一定の要件を満たした事業者については、第三者による認定・公表を含め、客観的な基準の下に社会的に認知する仕組み」として、「当面は、（略）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。

「情報銀行」に関する認定制度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

[3] IT 総合戦略本部ウェブページ（https://www.kantei.go.jp/jp/singi/it2/senmon_bunka/data_ryutsuseibi/kentokai.html）参照。
[4] 総務省ウェブページ（https://www.soumu.go.jp/menu_news/s-news/01tsushin01_02000227.html）参照。

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「契約約款」が重要となる。そこで、これらを検討するため、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「情報信託機能検討会」。）[5]が開催され、2018 年 6 月、「認定基準」、「モデル約款」及び「認定スキーム」について「情報信託機能の認定に係る指針 ver1.0」（以下「指針 ver1.0」。）が策定された。

一般社団法人日本IT団体連盟（以下「IT 連盟」。）においては、「情報銀行」に関する以上の政府の取組みと積極的に連携・協力してきた。2017 年 4 月には、上記中間答申における「データ取引市場等サブワーキンググループ」の取りまとめ[6]において、「情報銀行」制度についての政策提言を発表[7]し、また、上記検討会においては事務局としても参画したところである。

そこで、IT 連盟として、「情報銀行」に関する以上の経験や知見等を活かしつつ、指針 ver1.0 に準拠する形で、2018 年 8 月に「情報銀行推進委員会」を設置した。そして、企業が消費者個人から同意のもと、個人情報を含むパーソナルデータを預かり、消費者個人の代わりに妥当性を判断の上、第三者の事業者にパーソナルデータを提供する「情報銀行」事業を審査・認定する「情報銀行認定」事業を行うこととし、同 9 月に公表[8]、同 10 月には説明会[9]を開催した。

2018 年 12 月に、「情報銀行」認定申請ガイドブック（本書）の ver1.0 を公開すると伴に、「情報銀行」の認定申請受付を開始し、2019 年 6 月から「情報銀行」サービス事業の認定付与が開始されところである[10]。「情報銀行」の認定を受けようとする事業者にとっては、認定を受けることにより、IT 連盟により認定マークの使用が許諾される。

なお、IT 連盟による認定はあくまで任意のものであり、認定を受けることが「情報銀行」に関する事業を行うために必須ではない点に留意が必要である。

本書は、IT 連盟による「情報銀行」認定を受ける場合のガイドブックとして活用願いたい。

なお、政府において、「官民データ活用推進戦略会議」に設置された「官民データ活用推進基本計画実行委員会データ流通・活用ワーキンググループ」[11]による上記データ活用 WG による中間とりまとめのフォローアップ等について検討や、情報信託機能検討会では指針の見直しに向けた検討等が行われ、2019 年 10 月に指針 ver2.0[12]が策定されたところである。本書については、これら政府や行政の検討結果等をふまえつつ、今後も見直しが行われる場合があるため、ご留意頂ければ幸いである。

---

[5] 総務省ウェブページ（https://www.soumu.go.jp/main_sosiki/kenkyu/information_trust_function/index.html）参照。
[6] 総務省ウェブページ（本文については https://www.soumu.go.jp/main_content/000501157.pdf、概要については https://www.soumu.go.jp/main_content/000501156.pdf）参照。
[7] IT 連盟ウェブページ（概要については https://www.itrenmei.jp/files/johoginkokoso.pdf、詳細版については https://www.itrenmei.jp/files/johoginko.pdf）参照。
[8] 2018 年 9 月 12日。IT 連盟ウェブページ（https://www.itrenmei.jp/registration/）参照。
[9] 2018 年 10 月 16日「情報銀行認定」に関する説明会。資料は、IT 連盟ウェブページ（https://www.itrenmei.jp/registration/）参照。
[10] IT 連盟ウェブページ（https://www.itrenmei.jp/topics/2018/3639/）
[11] IT 総合戦略本部ウェブページ（https://www.kantei.go.jp/jp/singi/it2/detakatuyo_wg/index.html）参照。
[12] 総務省ウェブページ（https://www.soumu.go.jp/menu_news/s-news/01tsushin01_02000290.html）

1.2 本書の概説

1.2.1 「情報銀行」認定の意義

「情報銀行」認定の意義は二点あげられる。認定団体により、認定基準に適合した事業を認定することで、事業者にとっては、国際水準のプライバシー保護対策や情報セキュリティ対策等に関する認定基準に適合している、安心・安全な「情報銀行」として、消費者個人に対し、消費者自身の情報を信頼して託せられる事業者であることをアピールすることが可能となる。また、消費者個人にとっては、消費者が自らの情報資産を主体的に活用することを通じて、豊かな暮らしを享受することができる社会を実現する。

1.2.2 「情報銀行」認定審査について

「情報銀行」の認定申請にあたっては、プライバシーマーク又は ISMS 認証（これらが無い場合は 第三者監査による同等の認証）を取得していることが必要である。

また、「情報銀行」の認定は、そのサービス・事業運営の中で PDCA を回して継続的改善を図る、『マネジメントの実施状態』に対する認定である。よって、通常認定の申請をするためには、「情報銀行」事業・サービスを開始し、計画～実行～点検～改善・マネジメントレビューの「PDCA 運営実施記録」を整えることが必要となる。

審査は、書類およびヒアリングによる審査が原則である。ただし、取得している第三者認証及び利用するデータセンター等の安全性が、不十分であると判断された場合は、現地審査を実施する場合がある。

1.2.3 認定の種別

「情報銀行」の認定には、サービス・事業の開始後の PDCA 運営実施記録の確認を必要とする『通常認定』と、サービス・事業開始前であっても 一定の安全性を備えた「情報銀行」を認定対象とした、「情報銀行」の運営計画がサービス・事業開始可能な状態を満たしていること（プライバシー・バイ・デザイン／セキュリティ・バイ・デザイン）を認定する『P 認定』[13]がある。

P認定は、サービス・事業開始前に認定を取得することが可能であるが、「P認定取得後に、サービスを開始して PDCA 実施記録を整え、通常の認定を取得することが前提であること」や、「P 認定の更新、再申請は出来ないこと」、「認定マークは、P認定マークを使用すること」等の制約がある。

1.2.4 本資料の構成・見方

- 1章（はじめに）：「情報銀行」認定の開始にあたっての、背景・経緯等と本書の概説を記載。
- 2章（認定の対象となる「情報銀行」の範囲）：「情報信託機能の認定に係る指針」にて定められ

[13] IT連盟ウェブページ（ https://www.tpdms.jp/file/20190320-1News.pdf ）参照

た、「情報銀行」の定義・考え方、取り扱うデータの同意方法・種類・収集方法、対象となる事業者・サービス事業を記載。事前申請において、IT連盟が確認する。

・3章（運用スキーム）：IT連盟における、「情報銀行」認定に関する運用スキームやガバナンス体制について記載。

・4章（申請・認定フロー）：申請から認定までのフローを記載。認定交付後の契約・規程類については本書とは別に提示する。[14]

・5章（認定基準と提出書類）：項目毎に、認定基準と、その適合性を確認するために必要となる書類（例）を記載。書類の審査基準は、別途定め、申請事業者に提示する「『情報銀行』認定審査チェックシート」（以下、「認定審査チェックシート」という。）を参照のこと。

・6章（モデル契約約款）：①個人と「情報銀行」との間（モデル約款）、②「情報銀行」と情報提供元との間（モデル契約）、③「情報銀行」と情報提供先との間（モデル契約）の 3 種を策定（別添）。認定を受ける「情報銀行」サービス・事業を行う場合には、少なくとも「モデル契約約款」を盛り込んだ契約約款を作成することが必要となる。

1.2.5 著作権の取り扱い

本「情報銀行」認定申請ガイドブックの著作権は、IT連盟に帰属し、無断転載は禁止する。

1.2.6 改訂について

2018 年 12 月に公開した IT 連盟発行の「情報銀行」認定ガイドブック ver.1.0 を、総務省・経済産業省の情報信託機能検討会策定の「情報信託機能の認定に係る指針 ver2.0」に合わせて改訂を実施した。なお、主な改訂内容は、「変更履歴表」を参照のこと。（別添）

なお、本資料（以下、ver.2.0）の認定基準による審査の運用開始は本資料の公開日からとするが、ver.2.0 の公開日から 6 ヶ月間は「併用期間」として、旧資料（以下、ver.1.0）、ver.2.0 何れかの基準を選択して認定申請をすることができる。また併用期間の終了から 2 年間を「移行期間」とし、移行期間の終了日をもって ver.1.0 の適用が廃止となり付与された認定が無効になるため、終了日までに ver2.0 での更新認定取得が必要となる。（ver.1.0 で申請した審査の継続中に併用期間を過ぎた場合であっても、ver.2.0 への変更はできない。この場合は、ver.1.0 で認定を取得した後、移行期間内に ver.2.0 での更新審査を受けて ver.2.0 への移行を完了する必要がある。）[15]

[14] IT連盟ウェブページ（ https://www.tpdms.jp/application/index.html ） 参照資料：「情報銀行認定マーク付与に関する規約他一式」のダウンロード［ZIP］ 参照

[15] IT連盟ウェブページ（ https://www.tpdms.jp/file/verup_accreditation_criteria.pdf ）参照

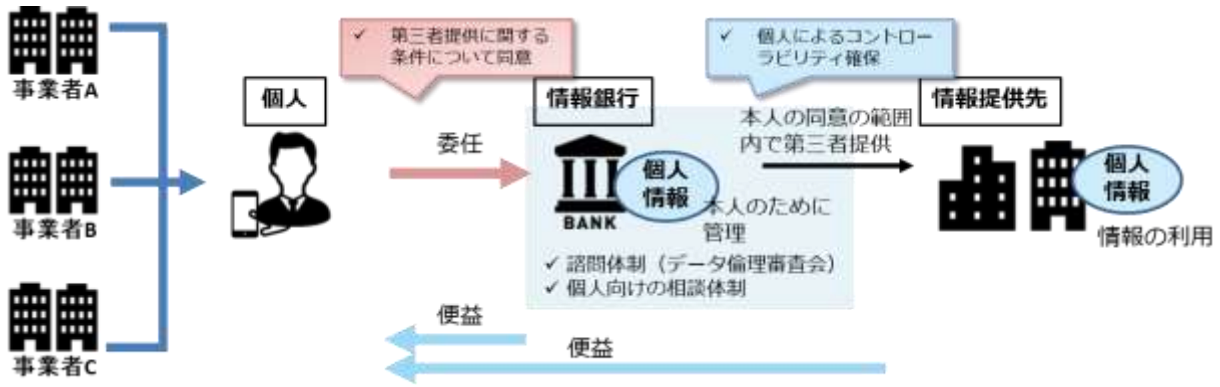
2 認定の対象となる「情報銀行」の範囲

「情報銀行」[16]は、「指針 ver2.0」において、「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」と定義されている。

【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、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。

【個人と情報銀行の関係】
- 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。

【「情報銀行」のイメージ】



【出典】情報信託機能の認定に係る指針 ver2.0（総務省/経済産業省）

[16] 「情報銀行」という名称については、
・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）
により、銀行という文字を使うことは禁止されている。そのため本ガイドブックでは通称として利用しており、「」付きの情報銀行という表現にしている。

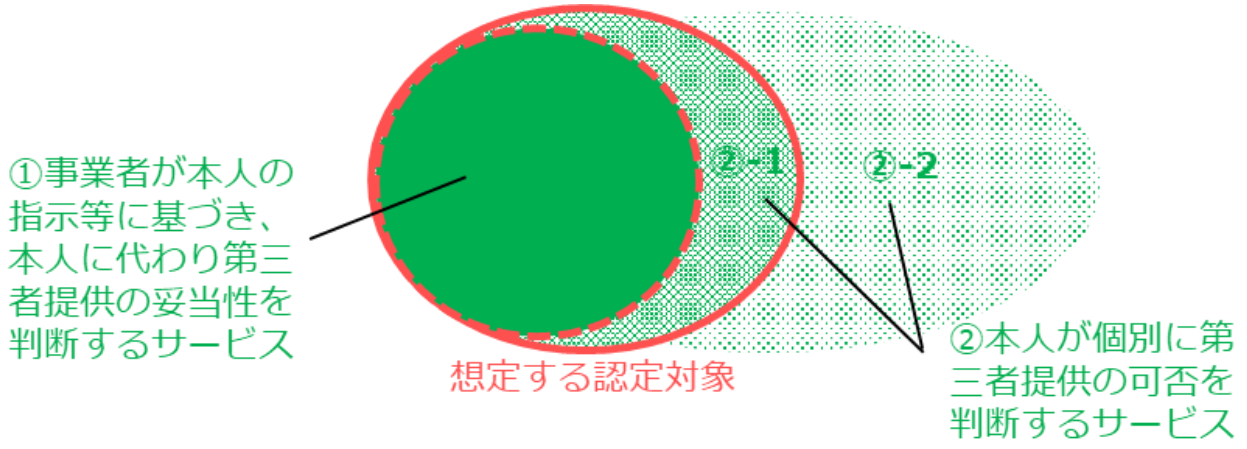
IT 連盟による認定の対象となる「情報銀行」については、情報信託機能検討会の指針 ver2.0 を踏まえ、具体的には次のものとする。

（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の部分）を想定[17]。他方、純粋なPDS[18]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。



【出典】指針 ver2.0

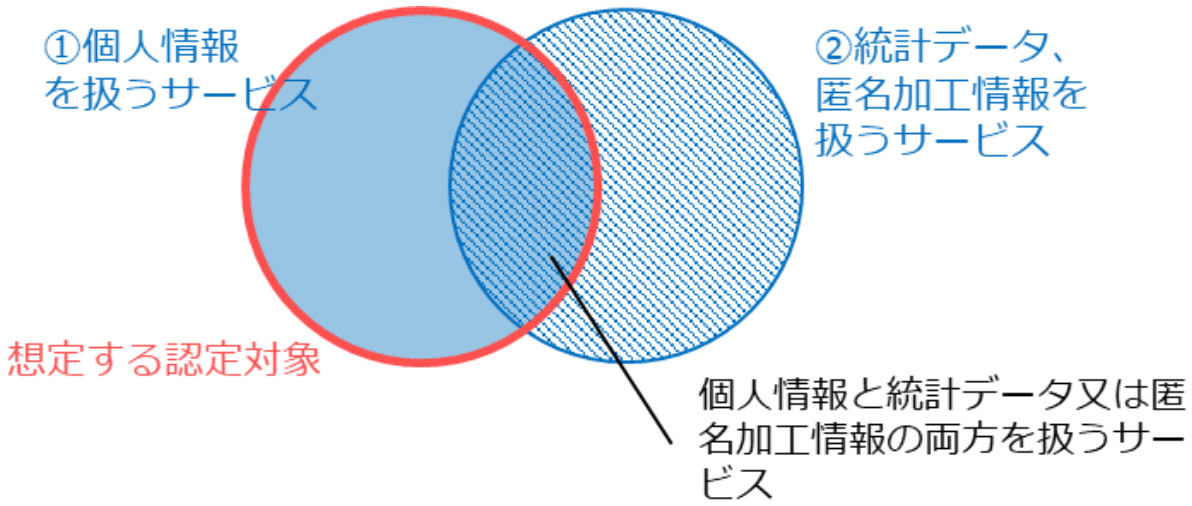
[17] （②－１）の部分を対象とすることで、認定の範囲は、データ活用 WG 中間とりまとめにおける「情報銀行」の定義よりも広くなっている。

[18] データ活用 WG 中間とりまとめによると、PDS（Personal Data Store）とは、「他者保有データの集約を含め、個人が自らの意思で自らのデータを蓄積・管理するための仕組み（システム）であって、第三者への提供に係る制御機能（移管を含む）を有するもの。」とされている。また、PDS 及び「情報銀行」等の定義については、「民間企業や諸外国等の先行する取り組みや提案を踏まえ、現時点では以下のように整理するが、今後ビジネスの動向を踏まえ適宜見直す可能性がある。なお、それぞれは排他的なものではなく、同一の者が複数の機能を担うことも想定される。」とされている。

（２）事業で扱うデータの種類

個人情報[19]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。

※対象とする「個人情報」には、「要配慮個人情報」[20]は含まない
※「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。
※ただし、情報銀行が個人情報を匿名加工情報や統計情報として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。
※個人の部分的な能力等に止まらない、個人の社会的な評価に関する指標（所謂「信用スコア」等）の取り扱いについては、個人にとって不利益な利用とならないよう留意する必要がある。[21]
※信用スコアが個人情報である場合は、認定の対象となる。



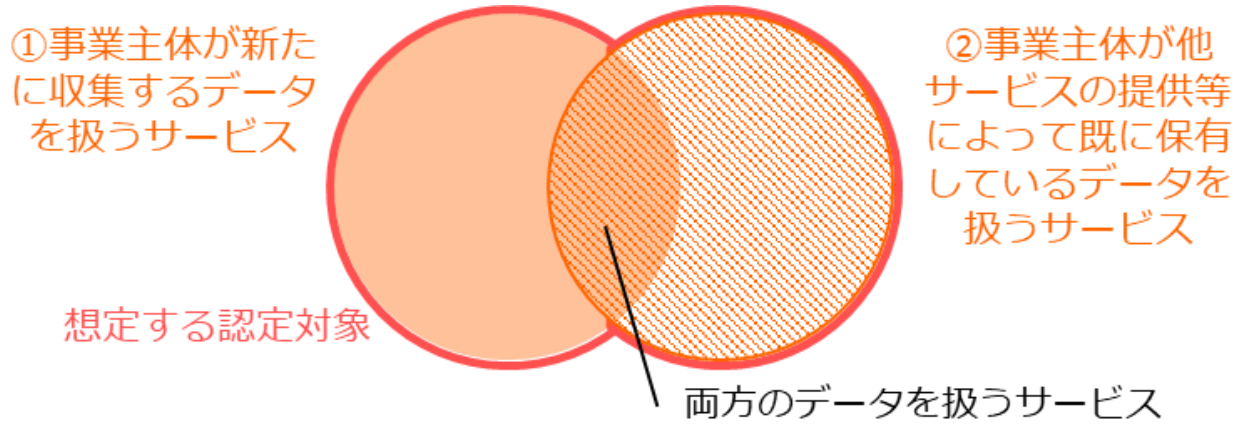
【出典】指針 ver2.0

[19] 個人情報保護法第2条第1項に規定する「個人情報」を意味する。
[20] 個人情報保護法第2条第3項に規定する「要配慮個人情報」を意味する。
[21] 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　4.「信用スコア」の取扱い　参照。

（３）個人情報の収集方法

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。



【出典】指針 ver2.0

（４）認定の対象となる事業者

・認定の対象となる事業者は、個人情報の保護に関する法律の適用される者である。
・行政機関、独立行政法人または地方自治体が認定を申請することが想定される場合には、別途認定基準等を公表する。

（５）認定の単位及び種類

・認定は、事業者（法人）単位、サービス・事業単位の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サービス・事業を認定する場合には、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。尚、個人情報を取り扱う者を明確にする必要がある。[22]
・共同で事業を行う場合、個人情報の取り扱いを行う事業者は審査の対象となる。

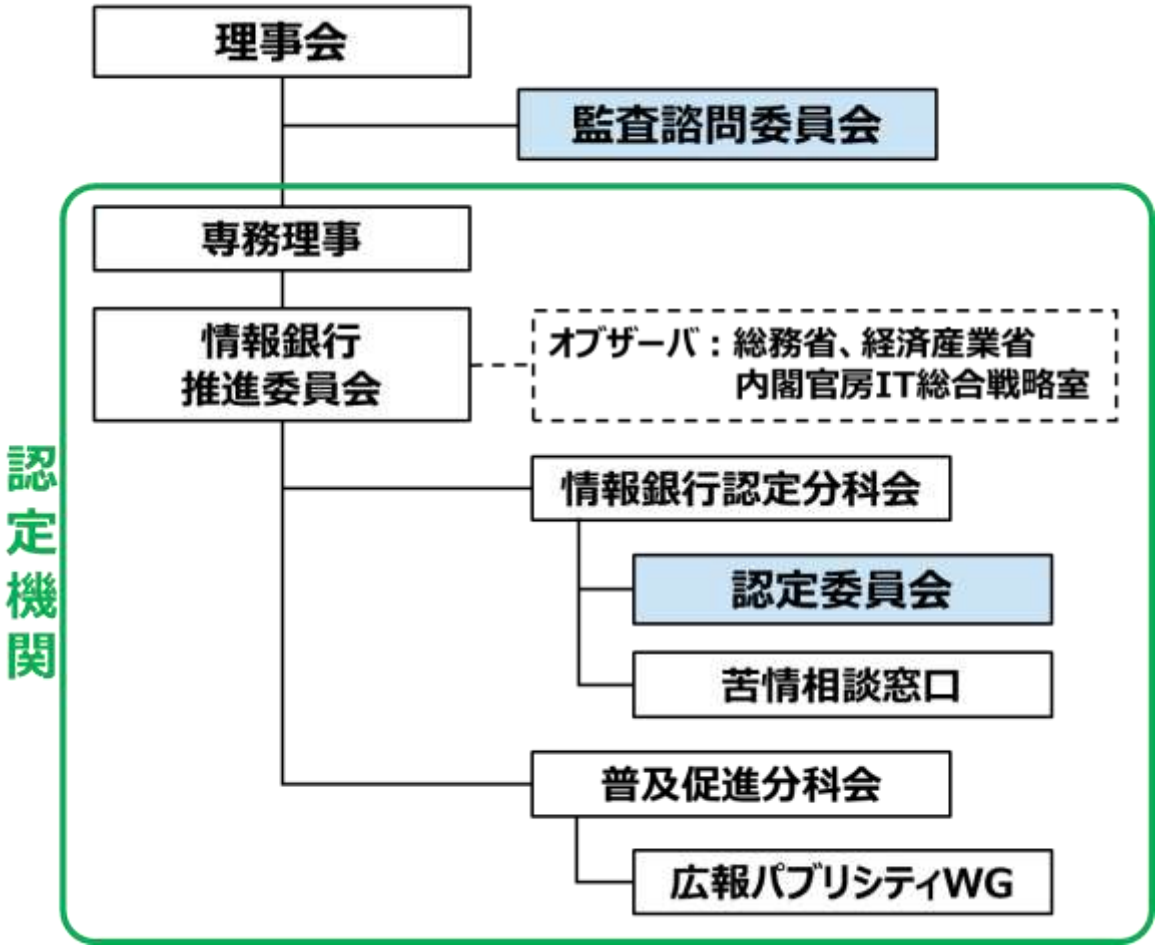
■個人情報を取り扱う者の明確化の必要性
・複数者が共同で情報銀行事業を行う場合、個人情報を取得する者及び個人情報を取り扱う者を明確にする必要がある。
・複数者が個人情報を取り扱う者となる場合は、複数者が共同して取得する場合及び、一部の者のみが取得する場合がある。
・共同で事業を行う個人情報取扱事業者の間で個人情報の授受（共同して取得した者の間の授受または取得した者から他の者への受け渡し）がある場合には、個人情報保護法上の共同利用として整理することも考えられる。この場合、当然ながら、共同利用に関し法律上求められる事項について、情報銀行は適切に対応することが必要である。

【出典】指針 ver2.0

[22] 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（https://www.soumu.go.jp/main_content/000648745.pdf）
１－⑥複数者が共同で情報銀行事業を行う場合の認定　参照

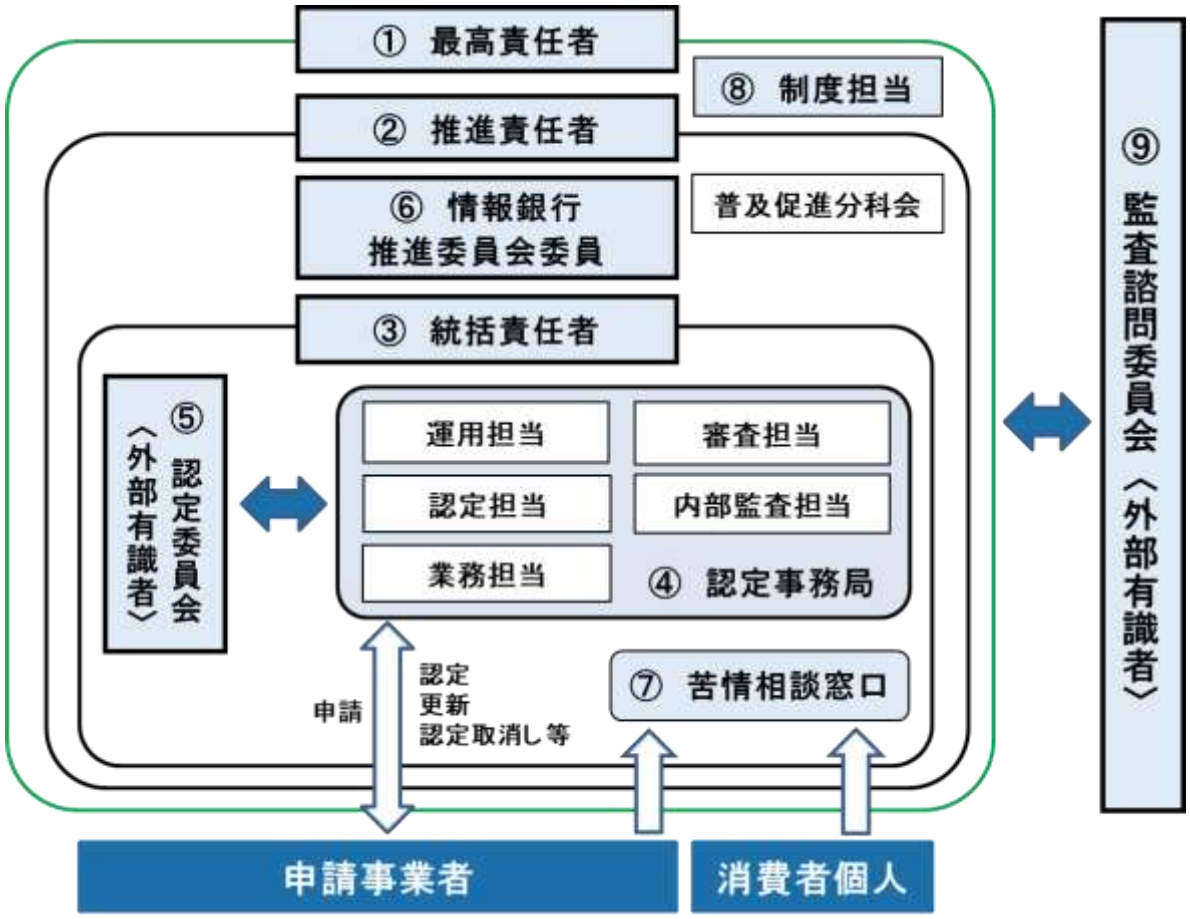
3 運用スキーム

IT連盟における「情報銀行」認定に関する運用スキームについては、情報信託機能検討会の指針を踏まえ、「情報銀行」認定における独立性、中立性、公平性などを担保しつつ、責任ある認定を行うことができるよう、以下のガバナンス体制で運用する。



以上のうち、「情報銀行」に関する認定機関については、具体的には次の責任体制としている。

【認定機関全体図】



① 最高責任者（専務理事）：認定機関を代表し、認定制度の企画立案及び認定業務等による「情報銀行」推進等認定機関の運営に関する責任を有する。

② 推進責任者（情報銀行推進委員会委員長）：認定業務、問合せ・苦情等対応業務及び普及促進業務等「情報銀行」推進に関する責任を有する。

③ 総括責任者（情報銀行認定分科会分科会長）：認定業務並びに申請事業者及び消費者個人等からの問合せ・苦情等対応業務を総括し、執行の責任を有する。

④ 認定事務局：下記担当者で構成され、認定業務を実施する。
・運用担当：認定業務運営における品質維持等を行う。
・業務担当：申請受付、認定証発行等を行う。
・認定担当：認定判定用報告書の作成等を行う。
・審査担当：書類審査等、審査計画書及び審査報告書の作成等を行う。
・内部監査担当：認定業務運営について内部監査を実施する。

⑤ 認定委員会：上記④の認定判定用報告書等により認定基準への適合性評価、認定判定を行う。

⑥ 情報銀行推進委員会委員：上記⑤の結果を踏まえ、認定決議、認定判定を行う。

⑦ 苦情等相談窓口：申請事業者及び消費者個人等からの問合せ・苦情等対応を行う。

⑧ 制度担当：指針の見直し等を踏まえた認定制度の企画立案等の検討を行う。

⑨ 監査諮問委員会：認定機関の運営に関する公平性等の監査諮問を行う。

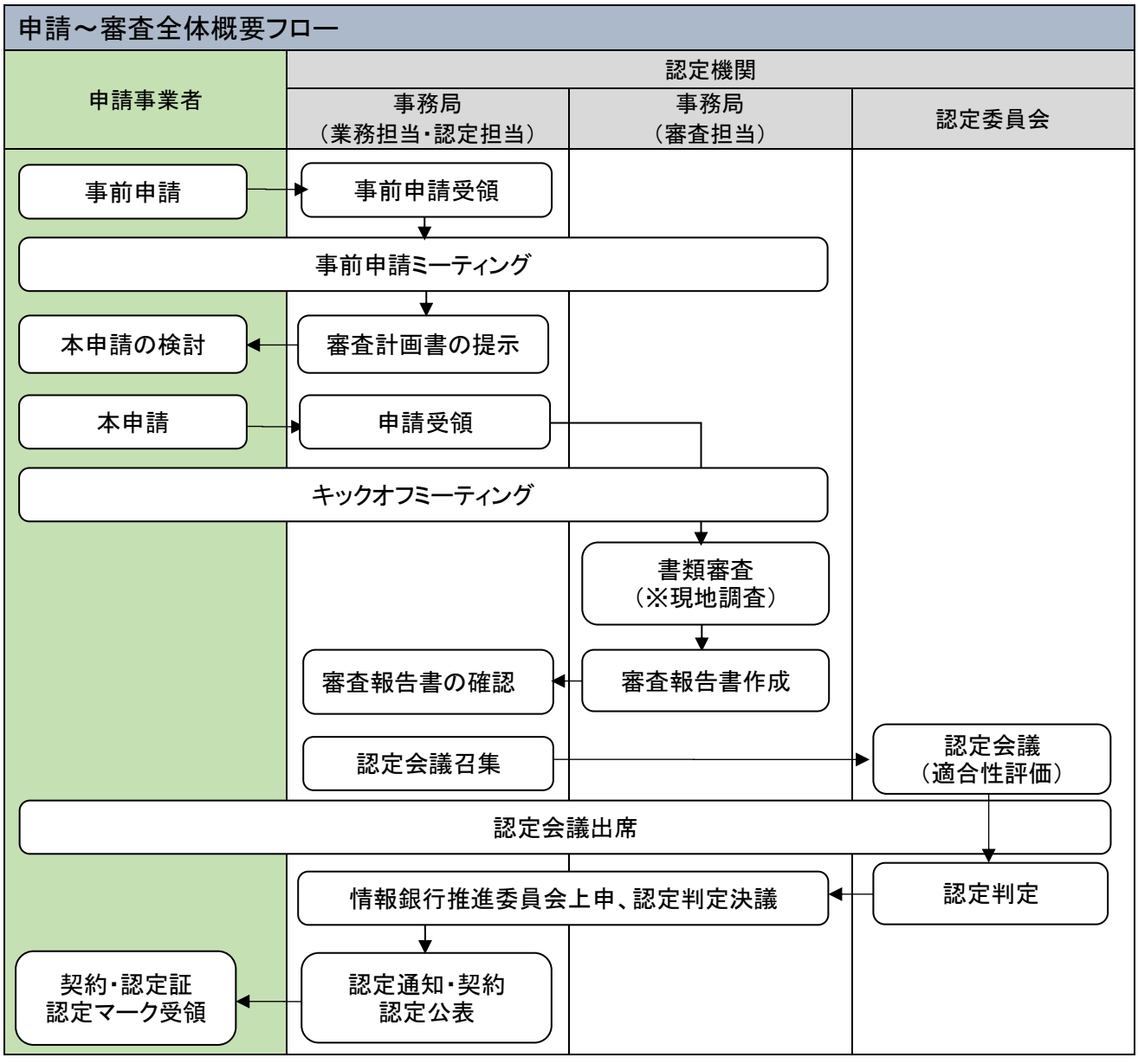
4 申請・認定フロー

認定について、申請から認定までの流れ、そして、それぞれの段階で必要な提出書類等は次のとおりである。

4.1 全体フロー

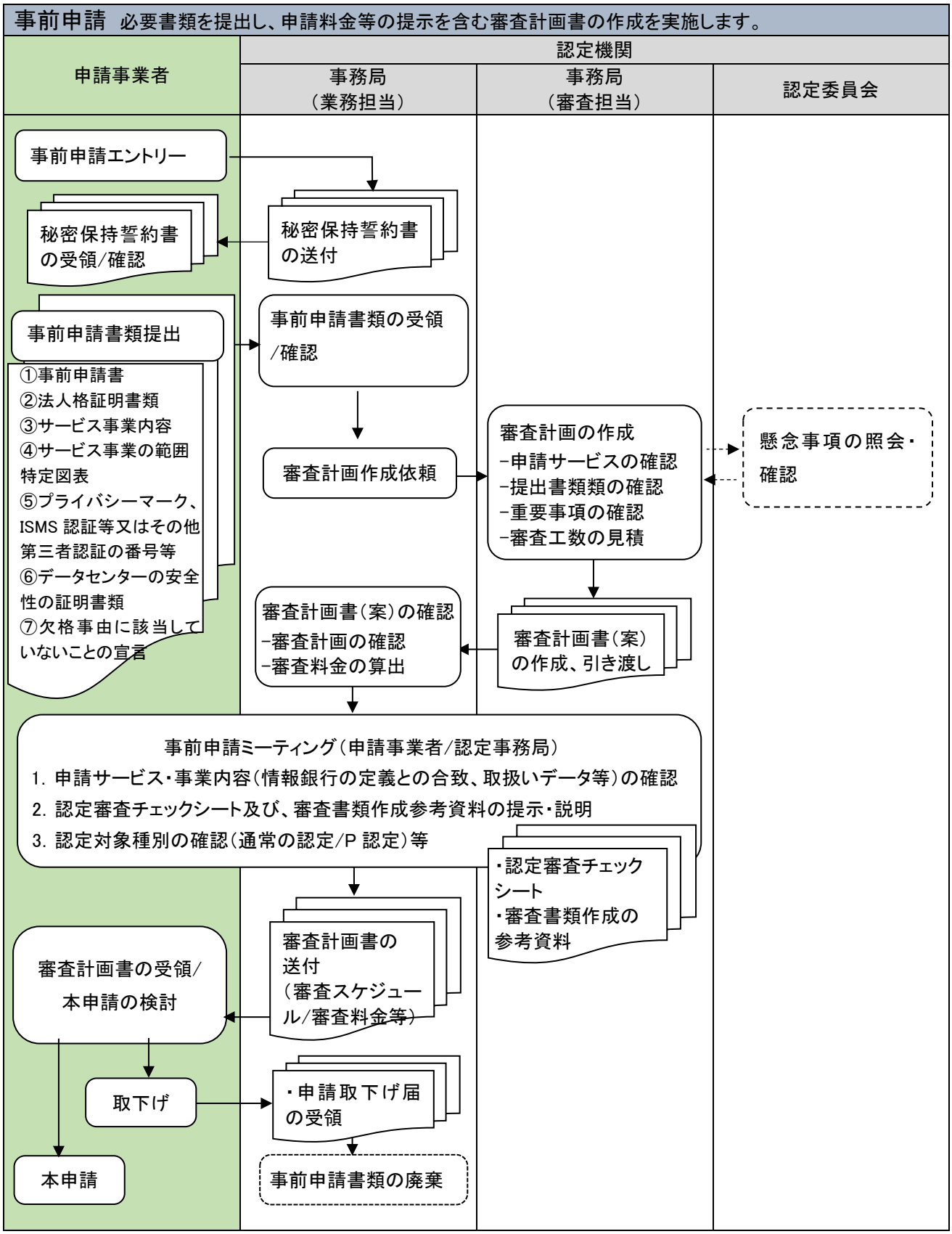
申請事業者においては、はじめに事前申請を行う。事前申請における提出書類等を踏まえ、IT連盟において審査料金、審査工数を算出し、審査計画を作成する。

申請事業者においては、IT 連盟から提示される審査料金等を踏まえ、本申請を行う。本申請後は、事務局（審査担当）が書類審査を行い、詳細の内容確認を行い、審査報告書を作成する。この審査報告書をもとに、事務局（認定担当）が認定判定用報告書を作成し、認定委員会で適合性評価・認定判定を行う。



4.2 事前申請フロー

下記は認定申請の具体的な手順となる。事前申請の方法や申請に必要な書類などについて説明する。



4.2.1 事前申請の目的

事前申請に必要な書類の取得方法および提出窓口等について説明する。事前申請においては、申請事業者のサービス・事業が「情報銀行」の定義にあてはまっているか、個人情報の取扱いが適切か等、本申請に進む上での基本事項の確認と審査スケジュールや審査料金の見積を行う。

4.2.2 事前申請のエントリー

申請事業者は、認定事務局に対し、申請事業者名、サービス・事業名称等を記載したメールを、以下窓口に送信して事前申請のエントリーをする。

認定事務局は、エントリー受付番号及び、事前申請書類の情報開示に対する「秘密保持誓約書」、「事前申請書」のフォーマットを、申請事業者に提出する。

※認定申請に関する 各種書類の提出・お問い合わせ窓口

情報銀行推進委員会 情報銀行認定分科会 認定事務局【 tpdms_info@itrenmei.jp 】

4.2.3 事前申請必要書類の作成～提出

申請事業者は、事前申請に必要な以下の書類を用意し、IT 連盟の指定する方法で提出する。

①事前申請書（含む認定対象種別）
②法人格を証明できる書類（複写データ可）
③サービス事業内容を記載した書類
④サービス事業の範囲が特定できる図表等
⑤プライバシーマーク（以下「P マーク」という。）、ISMS 認証又はそれらと同等の第三者認証に関する番号又はこれら認証を示す書類（第三者認証によっては、現地審査を行なうことがある）
⑥データセンターの安全性を証明する書類（SLA、SOC 等。第三者監査等による安全性が不十分であると判断される場合は、現地審査を行なうことがある）
⑦「TPDMS-2210 欠格事由及び判断基準」 の欠格事由に該当していないことの宣言

※要件を満たしていれば、書類②～⑦の書式は特に定めない。また書類③④はまとめても良い。

4.2.4 事前申請の受領、 確認

認定事務局は、提出書類に基づき事前申請の受付を行い、内容の確認を実施する。事前申請の書類から本申請が可能であるかどうか否かの初期確認を行う。

4.2.5 事前申請ミーティングの実施

事前申請書類内容の確認完了の連絡をした後に、本申請が可能であるかの最終判断を行うために申請事業者と認定事務局による「事前申請ミーティング」を実施する。「事前申請ミーティング」では、次の①～③を主に確認する。

①申請サービス・事業内容（情報銀行の定義、取扱いデータ等）の確認
②「認定審査チェックシート（審査基準）」の説明、本申請書類作成時の留意事項等の説明
③認定対象種別の確認（通常の認定/P 認定）、その他懸念事項の相互確認

認定事務局は、本申請に進むことの可否を判断し、可能な場合は「審査計画書」を作成する。

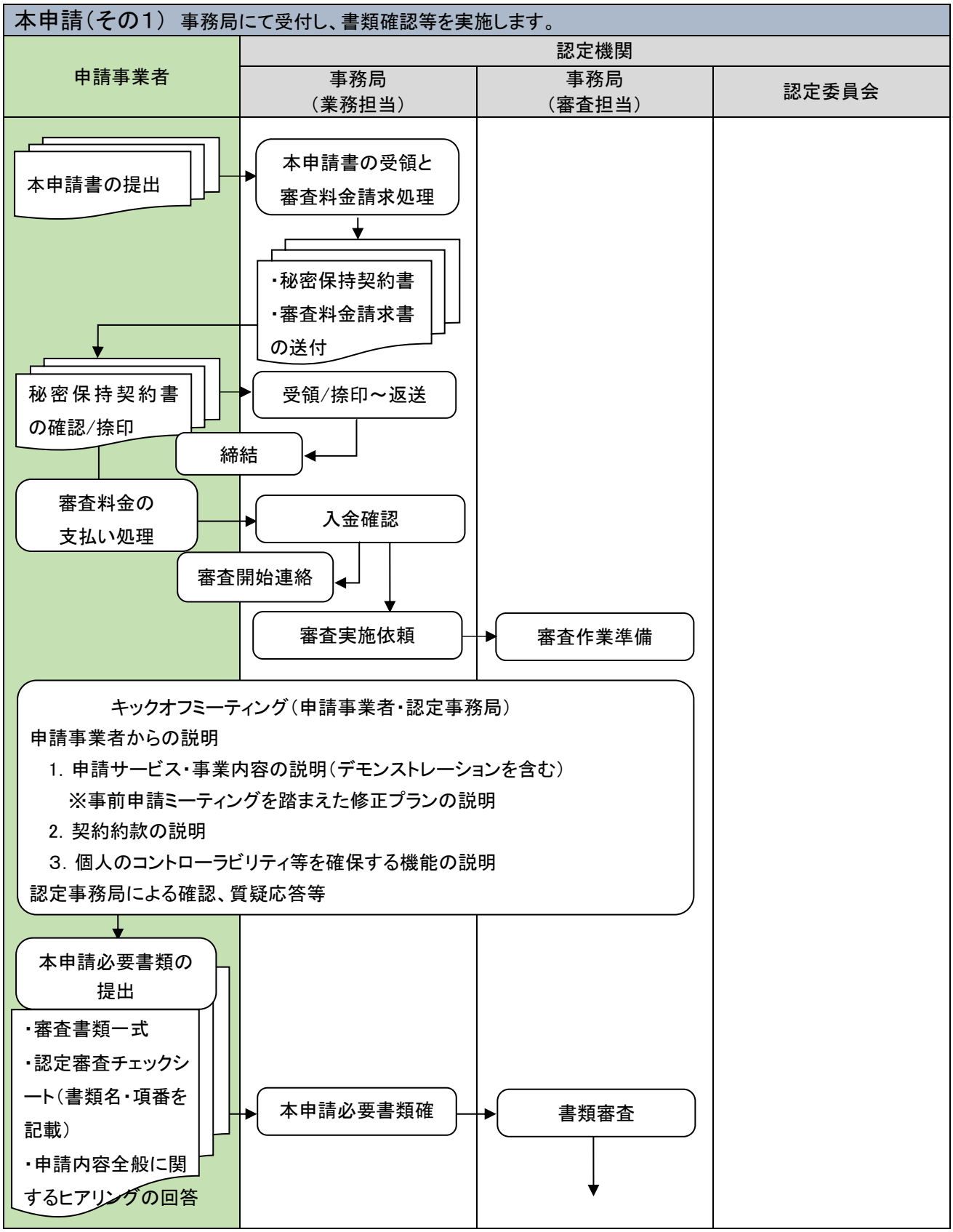
4.2.6 審査計画書の提示～本申請の検討

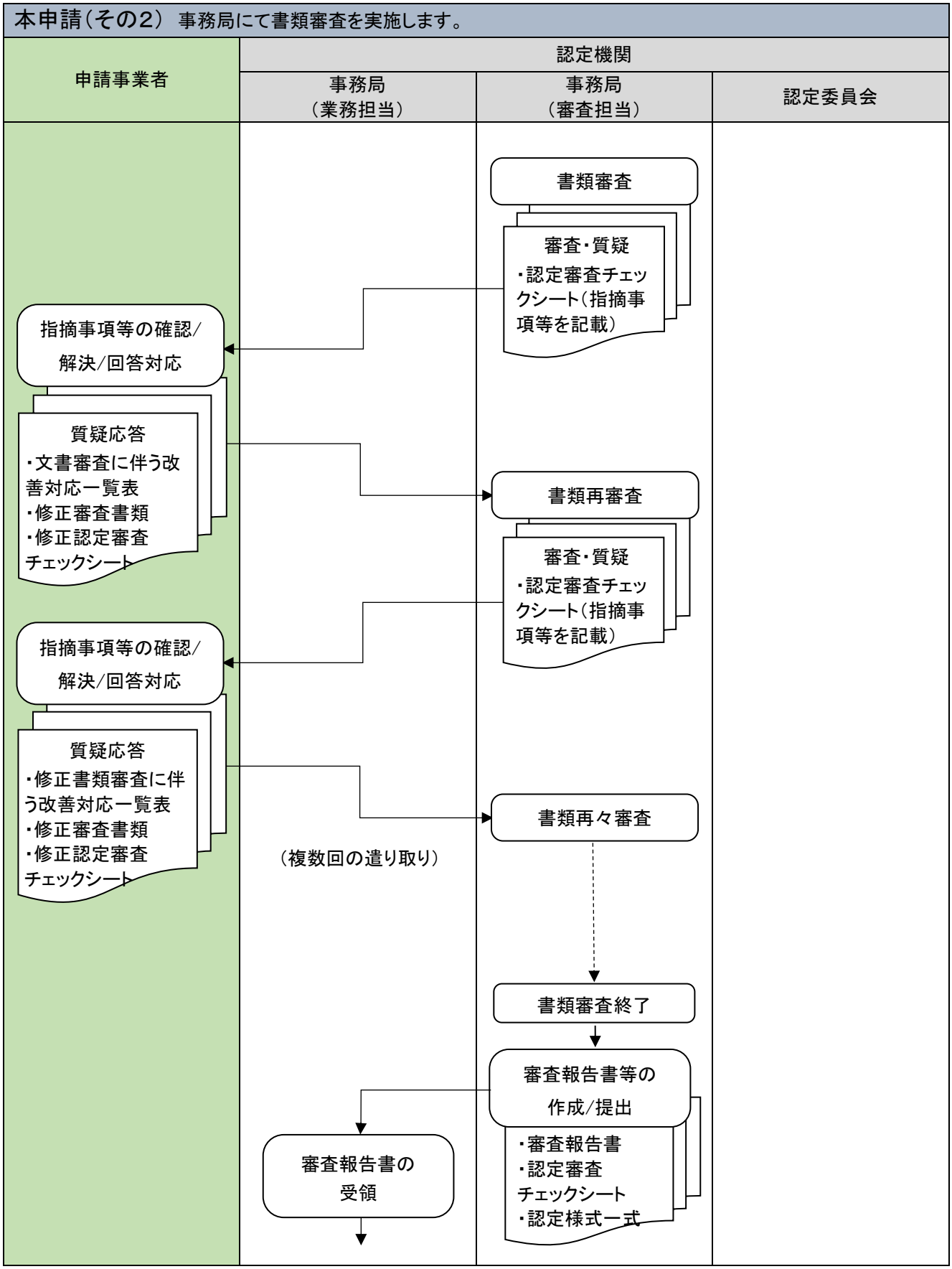
認定事務局より、申請事業者に、審査料金の見積、審査体制、審査スケジュール等の記載された「審査計画書」を送付する。申請事業者は「審査計画書」を元に、本申請に進むかを検討する。

なお、本申請に進まず、申請を取り下げる場合は、申請事業者は、1 ヶ月を目途に「申請取下げ届」に必要事項を記入の上、認定事務局に提出する。認定事務局は、申請事業者からの受領書類一式を廃棄する。

4.3 本申請フロー

本申請の具体的な手順は以下の通りである。





4.3.1 本申請書の提出

申請事業者は、「本申請書」を作成し、認定事務局に提出する。

4.3.2 本申請の受領と審査料の請求処理～入金

認定事務局は、「本申請書」に基づき、本申請の受付を行い、「本申請書」に不備がないことを確認する。確認後、申請事業者に「秘密保持契約書」（別紙様式）及び、審査料金の提示された「請求書」を送付する。（複数事業者が共同で情報銀行事業を行い、複数者が個人情報を取り扱う場合、その事業者数に応じて、審査費用が必要となる。）

申請事業者は請求書に記載の期日までに指定の口座へ審査料金を入金する。

※一旦支払われた審査料金は、本申請を取り下げた場合であっても返金されない。

4.3.3 秘密保持契約の締結

申請事業者とIT 連は、秘密情報の取扱に関して、秘密保持契約締結の手続を行う。

申請事業者は、認定事務局から提示された「秘密保持契約書」を確認し、捺印の上、2通を認定事務局に送付する。認定事務局は、うち1通に捺印をして申請事業者に返送する。

「秘密保持契約書」の締結と「審査料金の入金」をもって本申請手続きが完了し、認定審査が開始可能な状態となる。認定事務局は、本申請手続きが完了した旨を連絡する。

4.3.4 キックオフミーティング

認定審査の開始にあたり、申請事業者・認定事務局による「キックオフミーティング」を実施する。申請事業者が以下①～③の説明を行ない、認定事務局が確認し、質疑応答等を行なう。

申請事業者は、キックオフミーティングにて受けた認定事務局からの疑問・指摘等を踏まえて、審査書類を修正・作成すると伴に、回答を用意する。

【申請事業者】

①申請サービス・事業内容の説明

事前申請ミーティングを踏まえた修正プラン（デモンストレーションを含む）を説明

※P 認定の場合は、デモンストレーションの代わりに画面遷移図の説明でも可

②契約約款の説明（後述する「6. モデル契約約款」に基づき作成した契約約款）

③個人のコントローラビリティ等を確保する機能の説明

【認定事務局】

上記①～③に関して確認し、質疑応答を行なう

4.3.5 審査書類の提出

申請事業者は、審査に必要な下記書類を用意し、認定事務局に提出する。

① 審査書類一式（後述する「5. 認定基準と提出書類の提出資料（例）」参照）

② 「認定審査チェックシート」

※各々の認定基準に対応する「書類・規定類の名称と項番」を、例示に倣って記載し提出する

③ キックオフミーティング時に指摘された事項に対する回答

4.3.6 書類審査

必要書類の提出確認が完了後、認定事務局は書類審査を開始する。

認定事務局は、書類審査作業中に、確認事項、問題、指摘事項（以下、指摘等という。）が生じた場合は、申請事業者に対して、「認定審査チェックシート」の「不備及び確認事項」欄にて指摘等をする。申請事業者は、指摘等を受け取り次第、速やかに指摘等への回答や解決を図り、審査書類の修正、再提出を行うものとする。

申請事業者は、審査書類の修正、再提出を行う場合は、認定事務局からの指摘等を転記し、その対応状況（対応日時、内容、回答）を記載した「文書審査に伴う改善対応一覧表」及び、修正した審査書類、「認定審査チェックシート」を提出する。また、申請事業者から認定事務局への質問等も行うことができる。

これらの遣り取りを繰り返して、書類審査を進める。

4.3.7 回答期限と取り下げの判断

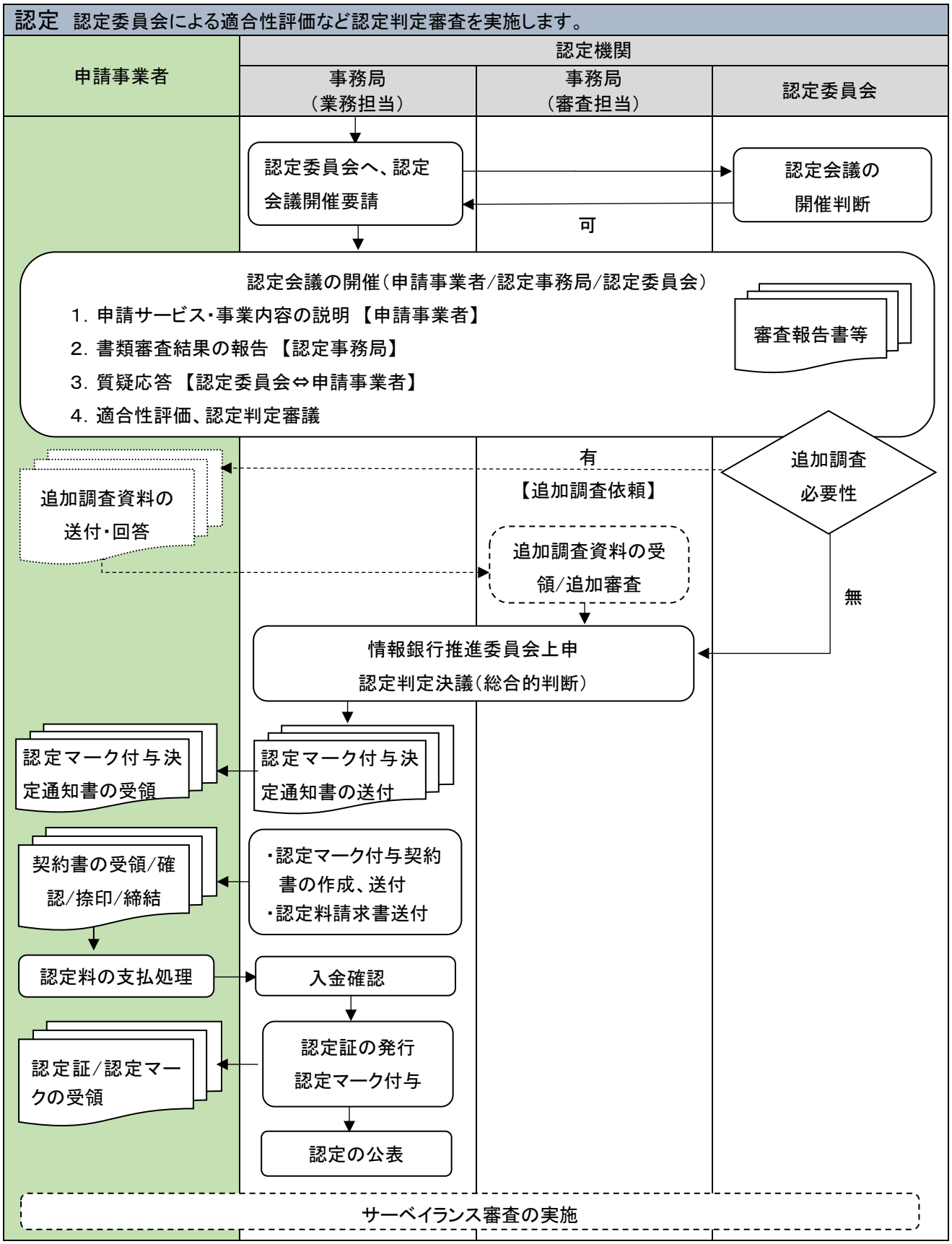
書類の提出及び質疑応答では、基本的に要請から1ヶ月以内に回答することが必要である。期間内に回答がない場合、回答不備が複数回連続する場合は、申請の取り下げとみなす事がある。

4.3.8 書類審査の終了

認定事務局による書類審査において、指摘等が無くなった時点で書類審査が終了する。認定事務局は、審査結果に基づき 認定委員会による認定会議用の「審査報告書等」を作成する。

4.4 認定決定フロー

認定手続きの手順は以下の通りである。



4.4.1 適合性評価・認定判定

事務局において作成した「審査報告書」等に基づき、申請事業者の同席の元、認定委員会による、適合性評価、認定判定を行う「認定会議」を開催する。その際、認定委員会の判断により、追加資料の提出や追加調査が必要になる場合がある。また、追加資料や追加調査の結果次第で、条件付きで認定する場合や、再度「認定会議」が開催される場合がある。

なお、申請事業者は、追加資料の提出や追加調査には速やかに応じることが必要である。

認定会議の結果を踏まえ、IT連盟情報銀行推進委員会による総合的判断による認定決議が行なわれ、認定判定が下される。認定事務局は「認定マーク付与決定通知書」を申請事業者送付し、結果を通知する。

4.4.2 契約書の締結及び認定料の請求～入金

認定判定を受けた申請事業者（以下「認定事業者」という。）とIT 連盟との間で、「情報銀行認定マーク付与契約」等を締結する。当該契約には、認定基準の遵守義務、更新手続き、認定基準違反時の対応、認定事業者に対する検査や報告徴収等が含まれる（別紙）。

また、認定事務局から認定事業者に、認定料の提示された「請求書」が送付される。認定事業者は、請求書に記載の期日までに指定の口座へ認定料相当額を入金する。なお、一旦支払われた認定料は、認定を辞退した場合であっても返金されない。

4.4.3 認定の付与

認定事業者には、IT 連盟より「認定証/認定マーク」が付与される。

当該認定事業者は、当該認定マークをウェブページ等で提示することができる。なお、サービス事業について認定を受けた場合については、認定マークの提示は当該認定を得たサービス事業の範囲のみで提示することとする。

認定マークの使用については、「情報銀行認定マーク使用ガイドライン」（別紙）に定めるものとする。また申請事業者は、「問合せ窓口」を設置し、個人（個人情報委任者）からの問合せ等への適切な対応に努めなければならない。

なお、認定付与の有効期間は、認定付与契約にて定めた期日から2年間とし、認定期間中は、1 年ごとのサーベイランス審査を実施する。

4.4.4 認定の公表

認定事業者（サービス事業について認定を受けた場合は当該サービス事業を含む。）については、IT連盟情報銀行推進委員会のウェブページ【https://www.tpdms.jp/】に掲示する。

4.4.5 サーベイランス審査

認定事業者のマネジメントシステムが、認定基準の要求事項に対し引き続き適合し、且つ有効に機能していることを確認するため、PDCA のサイクルが正しく機能しているかを確認することを目的に、1 年ごとにサーベイランス審査を実施する。サーベイランス審査の実施に関する通知は認定事務局から行う。

認定事務局から、「サーベイランス審査実施通知 兼 審査書類提出依頼」 を認定事業者へ発

行する。認定事業者は、サーベイランス審査に必要な以下の書類を用意し、IT 連盟の指定する方法で提出する。
①「サーベイランス審査実施通知 兼 審査書類提出依頼」 ※認定事務局から送付
②「サーベイランス審査 提出書類チェックリスト」 ※認定事務局から送付
③審査書類
書類の提出を受け、審査員が審査を開始する。審査完了後、認定維持の判定～決議が行われ、認定維持が決定される。
なお、付与された認定が P 認定の場合は、P 認定取得後は以下の流れとなる。
①認定事業者は、「情報銀行」サービス事業の開始前に、実行、点検、改善・マネジメントレビューの「PDCA運営計画」を、認定事務局に提出し、認定事務局はこれを確認する。
②認定事務局は、サービス・事業の開始後 3 ヶ月～6 ヶ月を目途にサーベイランス審査を実施し、P 認定取得時の計画に準拠しているかを確認する。
③認定事業者は、サービス・事業の開始後半年を目途にPDCA を一巡させ、運営実施記録を整えて、通常認定を申請する。

4.4.6 認定の取消し等

認定事業者において、IT連盟に認定事業者の利用者から苦情相談等があり、且つIT連盟より認定事業者に問題解決を求めたにも係わらず当該認定事業者による対応に問題があった場合もしくは、個人情報の漏えいの発生等認定基準に違反した場合は、認定委員会において、認定の一時停止、停止、取り消し、当該事業者名の公表等の措置を検討し、監査諮問委員会に諮問の上、対応する。
また、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等を含む）が認定マークを無断で使用していることが判明した場合は、IT 連盟は適切な対応を行う。

4.4.7 認定付与の更新

認定事業者は、付与契約の有効期間の満了に際し、付与契約の更新を受けることができる。更新を受けようとする認定事業者は、付与契約の有効期間の満了の 8 ヶ月前の前日から 4 ヶ月前の前日までに、更新審査の申請をすることが原則である。また、P 認定事業者が通常認定を取得する場合も、付与契約の更新手続きと同様の扱いとする。
※TPDMS-2200_情報銀行認定マーク付与に関する規約 参照
【 https://www.tpdms.jp/file/TPDMS-2200.pdf 】

5 認定基準と提出書類

「認定基準」については、情報信託機能検討会の指針 ver2.0 において、次のとおり規定されているところである。

- 「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。

以上を踏まえ、IT 連盟において策定した認定基準及びその適合性を確認するために申請事業者において提出が必要となる書類については、以下のとおりである。

5.1 事業者の適格性

5.1.1 事業者の適格性の具体的基準

項目	認定基準及びその適合性を確認するために必要な提出書類
①経営面の要件	■認定基準 〇法人格を持つこと ※「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） ■提出書類（例） 【1-1】事業者の登記簿謄本
	■認定基準 〇業務を健全に遂行し、情報セキュリティなど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

項目	認定基準及びその適合性を確認するために必要な提出書類
	超過がないこと）等 ■提出書類（例） 【1-2】財務内容の確認資料（決算書、財務諸表又はこれらに準ずる書類）
	■認定基準 〇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 ■提出書類（例） 【1-3】損害保険証書（ない場合は、賠償責任に関する説明資料）
②業務能力など	■認定基準 〇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 〇個人情報保護方針が策定されていること（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、トップマネジメントの氏名等を含む方針） 〇セキュリティポリシー（情報セキュリティ方針）が策定されていること ■提出書類（例） 【1-4】「情報銀行」事業を行う上で遵守が必要となる関連法令を示す書類 【3-1】15001「A.3.2.2 外部向け個人情報保護方針」 【1-5】15001[23]「A.3.2.2 外部向け個人情報保護方針」の公開先を示す書類（URL 等） 【1-6】27001[24]「5.2 方針」の公開先を示す書類（URL 等）
	■認定基準 〇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 ■提出書類（例） 【1-7】プライバシーマーク又はISMS認証の取得を示す書類（これらがない場合は、これらに準ずる第三者認証又は監査に関する認証取得証明書又は監査報告書）

[23] 15001 は、「JIS Q 15001：2017 情個人情報保護マネジメントシステム－要求事項」を指す
[24] 27001 は、「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」を指す。

項目	認定基準及びその適合性を確認するために必要な提出書類
	■認定基準 〇情報提供先との間でモデル契約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 （※）指針 ver2.0 の記載事項をもとに IT 連盟として以下を定める。 情報銀行は、提供先がPマークまたはISMS認証等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、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、個人情報の一部の削除または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[25] 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。 ■提出書類（例） 【1-8】情報提供先との契約関係書類
	■認定基準 〇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 ■提出書類（例） 【1-9】当該サービス事業の内容と範囲を示す書類

[25] 提供先は、「提供先において特定の個人を識別できないよう、個人情報の一部の削除または置き換え等の処理を行い、復元に必要な情報を除いた形」の、情報銀行にとって個人情報に該当するデータへのアクセス権限を持つことが許容される。

5.2 情報セキュリティ・プライバシー

5.2.1 基本原則及び遵守基準

情報セキュリティ等に関する基本原則及び遵守基準については、情報信託機能検討会の指針ver2.0 において、次のとおり規定されているところである。

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）

②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 認証等の取得（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、認定取得までに当該認証を取得）

■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

・「JIS Q 15001:2017 対応個人情報保護マネジメントシステム導入・実践ガイドブック」（JIPDEC 編）
https://webdesk.jsa.or.jp/books/W11M0100/index/?syohin_cd=330546

・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）

・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

・総務省スマートフォン プライバシー イニシアティブⅢ
https://www.soumu.go.jp/main_content/000495608.pdf

5.2.2 情報セキュリティの具体的基準

以上を踏まえ、IT 連盟において策定した具体的基準及びその適合性を確認するために申請事業者において提出が必要となる書類については、以下のとおりである。提出書類については、該当する措置を講じていることが確認できる書類を提出すること。

なお、以下の認定基準については、「情報銀行」事業に関する事項に対して「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」（以下「27001」という。）の要求事項を満たすものとしている。

項目	認定基準及びその適合性を確認するために必要な提出書類
①情報セキュリティマネジメントの確立	■認定基準 〇経営層（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 〇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 〇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 ■提出書類（例） 【2-1】27001「5.2 方針」に対応する書類 【2-2】27001「4.3 情報セキュリティマネジメントシステムの適用範囲の決定」に対応する書類 【2-3】27001「6.1 リスク及び機会に対処する活動」に対応する書類（下記書類を必ず含むこと） ・業務フローの各プロセスにおけるリスクを洗い出し、分析し、評価し、リスク対策を決定した結果の書類（リスク分析表） ・リスク分析表で決定したリスク対策を文書化した書類
②情報セキュリティマネジメントの運用・監視・レビュー	■認定基準 〇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 〇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 ■提出書類（例） 【2-2】27001「5.3 組織の役割、責任及び権限」、27001「7 支援」に対応する書類 【2-3】27001「6.1.2 情報セキュリティリスクアセスメント」に対応する書類 【2-2】27001「9.2 内部監査」及び 27001「10.2 継続的改善」に対応する書類
③情報セキュリティマネジメントの維持・改善	■認定基準 〇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 〇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

項目	認定基準及びその適合性を確認するために必要な提出書類
	■提出書類（例） 【2-2】27001「4.4 情報セキュリティマネジメントシステム」及び 27001「10.1 不適合及び是正措置」に対応する書類
④情報セキュリティ方針策定	■認定基準 〇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 ■提出書類(例) 【2-1】27001「5.2 方針」に対応する書類 【2-4】27001「A.5 情報セキュリティのための方針群」に対応する書類
⑤情報セキュリティ組織	■認定基準 〇責任者の明確化、組織体制を構築 〇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 ■提出書類（例） 【2-5】27001「5.3 組織の役割、責任及び権限」、27001「A6.1.1 情報セキュリティの役割及び責任」に対応する書類 【2-6】加盟団体名及び活動概要を示す書類
⑥人的資源の情報セキュリティ	■認定基準 〇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 〇情報セキュリティの意識向上、教育及び訓練の実施 ■提出書類（例） 【2-7】27001「7.2 力量」、27001「7.3 認識」に対応する書類 【2-8】情報セキュリティに関する教育の実施サマリー
⑦資産の管理	■認定基準 〇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 〇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」） 〇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 〇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

項目	認定基準及びその適合性を確認するために必要な提出書類
	※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 ■提出書類（例） 【2-9】270001「A.8.1.1　資産目録」、27001「A.8.1.2　資産の管理責任」、27001「A.8.2　情報の分類」、27001「A.8.1　資産に対する責任」、2700127001「A.8.3.1「取外し可能な媒体の管理」及び「A.8.3.2　媒体の処分」に対応する書類 【2-10】固有のデータセンターを保有していることを示す書類又は委託先データセンターに関する契約書 【2-11】データセンターの設置場所が国内にあること（但し、緊急事態に対応するために必要な場合を除く）を示す書類、27001「A.8.1.4　資産の返却」に対応する書類 【2-12】外部クラウドサービスの利用に関する契約書（利用する場合）
⑧技術的セキュリティ	■認定基準 （アクセス制御） 〇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） 〇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） 〇情報の機密性、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 〇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 ■提出書類（例） 【2-13】27001「A.9　アクセス制御」、27001「A.9.2　利用者アクセスの管理」及び 27001「A.10　暗号」に対応する書類
⑨物理的及び環境的情報セキュリティ	■認定基準 〇自然災害、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 〇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 〇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 ■提出書類（例） 【2-14】27001「A.11　物理的及び環境的セキュリティ」に対応する書類

項目	認定基準及びその適合性を確認するために必要な提出書類
⑩運用の情報セキュリティ	■認定基準 〇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 〇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 〇情報、ソフトウェア及びシステムイメージのバックアップは、合意されたバックアップ方針に従って定期的に取得し、検査すること 〇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 〇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 〇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 ■提出書類（例） 【2-15】27001「12.1 運用の手順及び責任」、27001「A.12.1.1 操作手順書」、27001「A.12.2 マルウェアからの保護」、27001「A.12.3.1 情報のバックアップ」、27001「A.12.4 ログ取得及び監視」及び 27001「A.12.6 技術的ぜい弱性管理」に対応する書類
⑪通信の情報セキュリティ	■認定基準 〇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 〇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 〇情報サービス、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 〇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） 〇提供元から個人データ受領するまたは機器（サーバ又はパソコン等。以下「機器」という。）を特定し、それ以外の「機器」で受領できないようにする技術的対策（ネットワーク認証や電子証明書による相互認証、もしくはトークンを用いる場合は、トークンの受け渡し管理等）及びセキュリティの保たれた物理的区域にて取り扱うこと[26] 〇提供先が個人データの提供を受ける「機器」を特定し、それ以外の「機器」で受領できないようにする技術的対策（例として、ネットワークや電子証明書による相互認証、もしくはトークンを用いる場合は、トークンの受け渡し管理等）及びセキュリティの保たれた物理的区域にて取り扱うこと[26] ■提出書類（例） 【2-16】27001「A.13.1.1 ネットワーク管理策」、27001「A.13.1.2 ネットワークサービスのセキュリティ」、27001「A.13.1.3 ネットワークの分離」及び

[26] 提供元からの個人データの受領、提供先への個人データの提供を、インターネット等を経由して行う場合は、ID、パスワードだけでの認証では不足である。ID、パスワードは、本人以外が知らないことが保証されない。例えば、サイバー攻撃等で他国から同じID、パスワードでアクセスされることを排除できない。また、提供先従業員が自宅で私的にデータを受領することも排除できない。

項目	認定基準及びその適合性を確認するために必要な提出書類
	27001「A.13.2　情報の転送」に対応する書類 【2-16】提供元から個人データ受領する「機器」を特定し、それ以外の「機器」で受領できないようにする技術的対策を記載した書類 【2-16】提供先が個人データの提供を受ける「機器」を特定し、それ以外の「機器」で受領できないようにする技術的対策を記載した書類
⑫システムの取得・開発・保守	■認定基準 〇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における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 〇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 ■提出書類（例） 【2-17】27001「A.14.1　情報システムのセキュリティ要求事項」及び 27001「A.14.2　開発及びサポートプロセスにおけるセキュリティ」に対応する書類
⑬供給者関係	■認定基準 〇供給者との間で、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 〇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 ■提出書類(例) 【2-18】27001「A.15　供給者関係」に対応する書類
⑭情報セキュリティインシデント管理	■認定基準 〇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 〇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 〇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 〇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 ■提出資料（例） 【2-19】27001「A.16.1　情報セキュリティインシデントの管理及びその改善」に対応する書類 【2-20】システムに対する脆弱性診断の実施内容を示す書類
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	■認定基準 〇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 ■提出書類（例） 【2-21】27001「A.17.1　情報セキュリティ継続」に対応する書類

項目	認定基準及びその適合性を確認するために必要な提出書類
⑯遵守	■認定基準 〇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 〇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 〇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 ■提出書類（例） 【1-4】27001「A.18.1　法的及び契約上の要求事項の順守」、15001「A.3.3.2 法令、国が定める指針その他の規範」に対応する書類 【2-22】27001「A.18.2　情報セキュリティのレビュー」に対応する書類

5.3 プライバシー保護対策

5.3.1 基本原則

プライバシー保護対策等については、情報信託機能検討会の指針 ver2.0 において、前述「5.2 情報セキュリティ等」と同様、次の基本原則を十分に整備・遵守していく必要がある。

■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）

5.3.2 プライバシー保護対策の具体的基準

以上を踏まえ、IT 連盟において策定した具体的基準及びその適合性を確認するために申請事業者において提出が必要となる書類については、以下のとおりである。

なお、以下の認定基準については、「情報銀行」事業に関する事項に対して、「JIS Q 15001：2017 個人情報保護マネジメントシステム－要求事項」（以下「15001」という。）及び「JIS X 9250：2017 情報技術―セキュリティ技術―プライバシーフレームワーク（プライバシー保護の枠組み及び原則）（ISO/IEC 29100:2011 Information technology -- Security techniques -- Privacy framework）」（以下「9250」という。）の要求事項を満たすものとしている。

項目	認定基準及びその適合性を確認するために必要な提出書類
①基本方針の策定	5.1.1 事業者の適格性の具体的基準 ②業務能力など を参照
②組織的安全管理措置	■認定基準 〇組織体制の整備、個人データの取扱に係る規律に従った運用、個人データの取扱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を実施していること ■提出書類（例） 【3-2】15001「A.3.3.4 資源、役割、責任及び権限」、15001「A.3.3.5 内部規定[27]」、15001「A.3.3.6 計画策定」、15001「A.3.7.1 運用の確認」、15001「A.3.3.7 緊急事態への準備」及び 15001「A.3.7.3 マネジメントレビュー」に

[27] 内部規程には、手順書レベルの規定も含む。手順書レベルの規定とは、A.3.3.3 によって実施した個人情報保護リスクの特定・分析を踏まえて策定した対策を講じる手順を文書化したものをいう。また、本規定は JIS Q 15001:2014 に準拠すること

項目	認定基準及びその適合性を確認するために必要な提出書類
	対応する書類
③人的安全管理措置	■認定基準 〇従業者の教育を実施していること ■提出書類（例） 【3-3】15001「7.3　認識」及び 15001「A.3.4.5　認識」に対応する書類 【3-4】プライバシー保護に関する教育実施サマリー
④物理的安全管理措置	5.2.2 情報セキュリティの具体的基準　⑨物理的及び環境的情報セキュリティを参照
⑤技術的安全管理措置	5.2.2 情報セキュリティの具体的基準　⑧技術的セキュリティを参照
⑥同意及び選択	■認定基準 〇個人情報の取扱を許可するか否かの選択の機会について、任意に、具体的に、わかりやすく本人に示していること。ただし、適用される法令が個人の同意なしに個人情報の取扱うことを明確に認める場合を除く。 〇9250「5.9　個人参加及びアクセス」に定める「個人参加及びアクセスの原則」の下における権利について、同意を得る前に本人に明示すること 〇9250「5.8 公開性、透明性及び通知」に定める「公開性、透明性及び通知の原則」によって示される情報について、同意を得る前に本人に提供すること 〇本人から直接個人情報を取得する場合は、同意を与えるか又は同意を保留するかによる影響について、少なくとも次に示す事項を本人に明示し、本人の同意を得なければならないこと[28] a）「情報銀行」を運営する申請事業者の名称又は氏名 b）個人情報保護管理者（若しくはその代理人）の氏名又は役職名、所属及び連絡先 c）利用目的（本人が理解できるよう具体的に記載すること） d）第三者提供 ・第三者提供に係る条件（提供先第三者、その利用目的及び第三者提供の対象となる個人情報の項目等についての判断基準及び

[28] 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下記が必要となる。
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。
個人情報の第三者提供等に関する個人の同意については、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。
個人との契約については、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。

項目	認定基準及びその適合性を確認するために必要な提出書類
	判断プロセス） ・ 第三者に提供する目的 ・ 提供する個人情報の項目 ・ 提供の手段又は方法 ・ 第三者の業種及び申請事業者との関係 ・ 個人情報の訂正等を行った場合に当該個人情報を第三者に提供する場合はその旨 ・ 個人情報の提供に関する第三者との契約がある場合はその旨 e）個人情報の取扱いの委託を行うことが予定される場合にはその旨 f） 開示等の請求等に応じる旨及び問合せ窓口 g）本人が個人情報を与えることの任意性及び当該情報を与えなかった場合に本人に生じる結果 h）本人が容易に知覚できない方法によって個人情報を取得する場合（クッキー情報の取得等やスマートフォンのアプリ経由で自動的に取得する位置情報、端末情報等）には、その旨 〇情報提供元から個人情報の提供を受ける場合は次のとおり。 ・情報提供元にて本人の意思を確認することを契約で定めること ・情報提供元から利用者の個人情報の提供を受けた場合、あらかじめ利用目的を公表している場合を除き、速やかに本人に利用目的を通知し、又は公表すること 〇同意の取得の方法について、デフォルトオンになっていないこと ■提出資料（例） 【3-7】同意の取得の際に本人を示す書類（情報提供先選定基準、同意画面のキャプチャや画面フロー等） 【3-7】本人への説明文が 15001 A.3.4.2.5 の「明示」[29]条件を満たしていることを確認できる書類（画面遷移図） 【3-8】情報提供元との契約関係書類 【1-8】情報提供先との契約関係書類

[29] 「明示」とは、本人に対し、その利用目的を明確に示すことをいい、事業の性質及び個人情報の取扱状況に応じ、内容が本人に認識される合理的かつ適切な方法によらなければならない。「明示」する事例としては下記がある。
・契約書その他の書面を相手方である本人に手渡し又は送付する
・本人がアクセスした自社のウェブ画面上に明示すべき事項を明記する
・スマートフォン等での小さい画面での同意画面の工夫
スマートフォン等の小さな画面で個人情報の取扱いについての同意画面を表示する場合は、以下の2点に留意する必要がある。
① 表示量を押さえる関係上、当該画面には全てを表示できないことが想定される。その場合には、要約表示をまず行う。
② 表示が分かれてしまうと、何に対して同意をしているのかが分からなくなるおそれがある。したがって、同一画面に表示することが望ましい。
「ISO/IEC 29184:2020 情報技術－オンラインにおけるプライバシーに関する通知及び同意」についても併せて参照のこと

項目	認定基準及びその適合性を確認するために必要な提出書類
	【3-9】9250「5.2 同意及び選択」、15001「A.3.4.2.4 個人情報を取得した場合の措置」に対応する文書、15001「A3.4.2.5 A.3.4.2.4 のうち本人から直接書面によって取得する場合の措置」、15001「A.3.4.2.7 本人に連絡又は接触する場合の措置」及び15001「A.3.4.2.8 個人データの提供に関する措置」に対応する書類
⑦利用目的の正当性及び明確化	■認定基準 〇利用目的が適用される法令を遵守していること及び適法な根拠に依拠していることを確実にすること 〇新しい利用目的のために初めて個人情報が収集される前に、又は、個人情報が使用される前に、本人にその目的を明示すること 〇利用目的の記載について、明確かつ状況に適応した適切な表現を使用すること ■提出資料（例） 【3-10】9250「5.3 目的の正当性及び明確化」及び 15001「A.3.4.2.1 利用目的の特定」に対応する書類
⑧収集制限	■認定基準 〇適用される法令の範囲内及び特定された目的のために最低限必要であるものに制限すること 〇個人情報をみだりに収集せず、収集する個人情報の量及び種類の両方について、利用目的を達成するのに必要なものに制限すること 〇個人情報の収集を始める前に、利用目的を実現するためにどの個人情報が必要かを慎重に考慮すること 〇個人情報取扱いのポリシー及び実践の一部として、収集する個人情報の種類及びそれを収集する正当な理由を明確にすること 〇本人によって要求された特定のサービス提供以外の目的のために、追加の個人情報を収集する場合、可能な限り、本人がそのような個人情報を提供するか否か選択できること 〇本人に、以上のような追加の情報の要求に応じる回答は任意であるという旨を明確に知らせること ■提出資料（例） 【3-11】9250「5.4 収集制限」及び 15001「A.3.3.1 個人情報の特定」に対応する書類
⑨データの最小化	■認定基準 〇次に示すような方法で、データ処理手順及びICTシステムを設計及び実装すること ・処理される個人データを最小限にするとともに、プライバシー利害関

項目	認定基準及びその適合性を確認するために必要な提出書類
	係者及び個人データが開示されるか又は個人データにアクセスする者の数を最低限に抑えること ・“知る必要性（need to know）”の原則を確実に採用すること、すなわち、個人データの処理の正当な目的の中で、その者の職務の遂行に必要な個人データだけにアクセス権が与えること ・個人情報の取扱いにあたっては、必要最小限の項目をもって利用目的を達成し、利用目的を超えた意味情報（行動の観測、プロファイリング情報等）の抽出を行わないこと ・個人データの処理の目的が終了している場合で、個人データを保存するという法的要求事項がなく、そうすることが現実的な場合には個人データを確実に破棄又は匿名化すること[30] ■提出資料（例） 【3-12】9250「5.5　データの最小化」に対応する書類
⑩利用、保持及び開示の制限	■認定基準 〇個人データの利用、保持及び開示（提供を含む。）は、具体的、明示的かつ正当な利用目的を達成するために必要な範囲に限定すること 〇適用される法令によって、異なる目的が明示的に要求されていない限り、収集の前に特定した利用目的に個人データの利用を限定すること 〇定められた利用目的を達成するのに必要な期間だけ個人データを保持し、かつ、必要な期間を経過した後は個人データを確実に破棄又は匿名化すること 〇定められた利用目的が無効になったが、適用される法令が保持を要求している場合は、全ての個人データをアーカイブに保管し、安全を確保し、かつ、それ以上処理されないようにすること （委託） 〇個人データの取扱いの全部又は一部を委託する場合、特定した利用目的の範囲内で委託契約を締結しなければならないこと 〇委託先は、十分な個人データの保護水準を満たしている者を選定しなければならないこと 〇情報銀行で行うリスク分析と同等以上のリスク分析に基づき、選定基準を定めていること 〇委託先を選定する基準を確立しなければならないこと、当該基準には、少なくとも委託する当該業務に関しては、自社と同等以上の個人情報保護の水準にあることを客観的に確認できることを含めなければ

[30] 15001 では、利用期限を過ぎた個人データの廃棄は努力義務だが、9250 では必須である

項目	認定基準及びその適合性を確認するために必要な提出書類
	ならないこと 〇個人データの取扱いの全部又は一部を委託する場合は、委託する個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならないこと 〇委託先に対し、次に示す事項を契約によって規定し、十分な個人データの保護水準を担保しなければならないこと a）委託先との責任の明確化 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定期的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 〇当該契約書などの書面を少なくとも個人データの保有期間にわたって保存しなければならないこと （共同利用） 〇情報提供先における当該個人データの共同利用が行われないよう情報提供先と契約すること 〇情報提供元との間における共同利用をしないこと 〇共同事業等において共同利用により情報信託サービスを提供する場合は、次に示す事項又はそれと同等以上の内容の事項を、あらかじめ、本人に通知するか、又は本人が容易に知り得る状態に置いていること a）共同して利用すること b）共同して利用される個人情報の項目 c）共同して利用する者の範囲 d）共同して利用する者の利用目的 e）共同して利用する個人情報の管理について責任を有する者の氏名又は名称 f）取得方法 〇共同して利用する者の間で、上記事項について契約によって定めること 〇当該契約書などの書面を少なくとも個人データの保有期間にわたって保存しなければならないこと

項目	認定基準及びその適合性を確認するために必要な提出書類
	（情報提供先） 〇情報提供先は、当該個人データを当初又はその後提供を受ける際に特定された利用目的の範囲内で利用目的を特定し、その範囲内で当該個人データを利用することとし、情報提供先と当該利用目的の範囲内で契約を締結すること 〇情報提供先は、十分な個人データの保護水準を満たしている者を選定しなければならないこと。具体的には、第三者認証を取得していることである（プライバシーマークまたは、ISMS認証等）。 ただし、情報銀行は、提供先がPマークまたはISMS認証等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、個人情報の一部の削除または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[31] 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。 〇情報提供先を選定する基準を確立しなければならないこと、当該基準には、少なくとも情報提供先における個人データの取扱に関しては、自社と同様の個人情報保護の水準にあることを客観的に確認できることを含めなければならないこと 〇提供する個人データの安全管理が図られるよう、情報提供先に対する必要かつ適切な監督を行わなければならないこと 〇情報提供先に対し、次に示す事項を契約によって規定し、十分な個人データの保護水準を担保しなければならないこと a）情報提供先との責任の明確化 b）個人データの安全管理に関する事項 c）情報提供先における委託に関する事項 d）個人データの取扱状況に関する報告の内容 e）契約内容が遵守されていることを定期的及び適宜に確認できる事項

[31] 提供先は、「提供先において特定の個人を識別できないよう、個人情報の一部の削除または置き換え等の処理を行い、復元に必要な情報を除いた形」の、情報銀行にとって個人情報に該当するデータへのアクセス権限を持つことが許容される。

項目	認定基準及びその適合性を確認するために必要な提出書類
	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 〇当該契約書などの書面を少なくとも個人データの保有期間にわたって保存しなければならないこと ■提出資料（例） 【3-11】15001「A.3.3.1 個人情報の特定」に対応する書類 【3-12】9250「5.5 データの最小化」に対応する書類 【3-13】9250「5.6 利用、保持及び開示の制限」、15001「A.3.4.3.2 安全管理措置」及び 15001「A.3.4.3.1 正確性の確保」に対応する書類 【3-14】15001「A.3.4.3.4 委託先の監督」（情報銀行で行うリスク分析と同等以上のリスク分析に基づき、選定基準を定めていることを確認できること）及び 15001「A3.4.3.2 安全管理措置」に対応する書類 【3-15】15001「A.3.4.2.8 f） 個人データを共同利用している場合」に対応する書類 【3-16】同意の取得の際に本人を示す書類（情報提供先選定基準、同意画面のキャプチャや画面フロー等） 【1-8】情報提供先との契約関係書類【3-8】情報提供元との契約関係書類
⑪正確性及び品質	■認定基準 〇処理された個人データが、利用目的に照らして、正確、完全、最新（古いデータを保存する正当な根拠がある場合を除く）、十分かつ適切であることを確実にすること 〇本人以外（情報提供元等）から収集した個人データの信頼性を当該個人データが処理される前に確保すること 〇本人による個人データの変更（訂正等）の請求があった場合、本人確認の上、対応すること 〇正確性及び品質を確保するのに役立つ個人データ収集手順を確立すること 〇収集及び保管している個人データの正確性及び品質を定期的に点検するための管理の仕組みを確立すること ■提出書類（例） 【3-8】情報提供元との契約関係書類 【3-17】9250「5.7 正確性及び品質」、15001「A.3.4.3.1 正確性の確保」、15001「A.3.4.2.2 適正な取得」、15001「A.3.4.4 個人情報に関する本人の権利」及び 15001「A.3.7.1 運用の確認」に対応する書類

項目	認定基準及びその適合性を確認するために必要な提出書類
⑫公開性、透明性及び通知	■認定基準 〇個人データ処理に関する個人情報保護方針、個人データの取扱手順及び実践について、明確かつ入手が容易な方法で本人に提供すること 〇個人データが処理されるという旨、利用目的、個人データが開示される可能性があるプライバシー利害関係者（情報提供先、委託先等）の種類及び連絡先を含む個人情報保護管理者の氏名又は職名及び所属を明示又は通知すること 〇本人が自分の個人情報の処理を制限するため、並びに、当該情報にアクセス、修正及び削除することができるようにするため、本人に対して提供する選択肢及び手段を開示すること 〇個人データ取扱手順に大きな変更があった場合には、本人に通知すること 〇個人情報を匿名加工情報や統計情報として加工し、当該データを他者に提供する場合、加工して提供するという旨やこれによる個人の便益について、個人に対して明らかにすること ■提出書類（例） 【3-18】9250「5.8 公開性、透明性及び通知」、15001「A.3.2.2 外部向け個人情報保護方針」及び 15001「A.3.4.2.5 A.3.4.2.4 のうち本人から直接書面によって取得する場合の措置」に対応する書類 【3-19】本人が自分の個人情報にアクセス、修正及び削除することができるユーザインターフェイス画面のキャプチャ 【3-20】個人データ取扱手順に大きな変更があった場合の通知内容及び方法を定めた書類
⑬個人参加及びアクセス	■認定基準 〇事前に適切なレベルの本人確認が可能であり、かつ法令上許容される場合には、個人データに本人がアクセス及び確認できるようにすること 〇本人がその特定の状況で適切及び可能であれば、個人データの正確性及び完全性に異議申立てができ、個人データを修正、訂正又は削除することができるようにすること 〇情報提供先には、修正、訂正又は削除を連絡すること 〇過度な遅延又はコストを伴わず、単純、迅速かつ効率的な方法で本人がこれらの権利を行使することができる手順を確立すること ■提出書類（例） 【3-21】9250「5.9 個人参加及びアクセス」及び 15001「A.3.4.4 個人情報

項目	認定基準及びその適合性を確認するために必要な提出書類
	に関する本人の権利」に対応する書類 【3-22】本人が自分の個人データにアクセス及び確認することができる画面のキャプチャ 【3-23】情報提供先への修正、訂正又は削除を連絡する手順に対応する書類

5.4 ガバナンス体制

5.4.1 ガバナンス体制の具体的基準

項目	認定基準及びその適合性を確認するために必要な提出書類
①基本理念	■認定基準 〇「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 ■提出書類（例） 【4-1】15001「A.3.2.2 外部向け個人情報保護方針」に対応する書類
②相談体制	■認定基準 〇個人や事業者から、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 ■提出書類（例） 【4-2】苦情相談窓口が示されているHPなどの表示内容を示す書類 【4-3】15001「A.3.6 苦情及び相談への対応」に対応する書類
③諮問体制	■認定基準 〇諮問体制の［設置］。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[32]） ・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

[32] IT連盟は、データ倫理審査会の運用を、ISO/IEC 29134 Information technology — Security techniques — Guidelines for privacy impact assessment （情報技術－セキュリティ技術－プライバシー影響評価のためのガイドライン）を基本として認定基準を定める。この他、以下の規格を参照する。
・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 15001：2017 個人情報保護マネジメントシステム－要求事項」
・JIS X 9250：2017 情報技術―セキュリティ技術―プライバシーフレームワーク（プライバシー保護の枠組み及び原則）（ISO/IEC 29100:2011 Information technology -- Security techniques -- Privacy framework）
・JIS Q 31010：2012 リスクマネジメント－リスクアセスメント技法
・ISO/IEC 29184 Information technology － Online privacy notices and consent 情報技術 － オンラインにおけるプライバシーに関する通知及び同意
・Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 （データ保護影響評価（DPIA）及び取り扱いが 2016/679 規則の運用上、「高いリスクをもたらすことが予想される」か否かの判断に関するガイドライン）
・ISO26000 Guidance on social responsibility 社会的責任に関する手引
またデータ倫理審査会においては、その運用を支援する具体的な指針として解説した「データ倫理審査会運用ガイドライン（TPDMS-1140）」についても参照すること。

項目	認定基準及びその適合性を確認するために必要な提出書類
	※構成員（例）は、消費者を含む利害関係者で構成される必要がある。以下の視点で審査をする。 −エンジニア：事業者の視点で、漏えい等リスク分析・リスク対策が十分か、他の構成員からの指摘が実現可能か、システム構築の視点から漏えい等リスク分析・リスク対策が十分か、等。（社内委員） −セキュリティ専門家：事業者の視点で、ハードウェア・ソフトウェアのリスク対策が適切か等。（社外委員限定は求めない社内委員） −法律実務家：事業者や提供先の視点で、法令を遵守しているか等。（社外委員限定は求めない） −データ倫理専門家：個人の視点で、個人情報保護のリスク対策が適切か等。（社外委員） −消費者：個人の視点で、コントローラビリティが確保されているか。提供先の条件が個人の予測できる範囲内で運用されているか等。（社外委員） （少なくとも社外委員には、データ倫理の専門家及び消費者の代表者を含むことを求める） ・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。 ・構成員及び（必要な範囲の）議事録を公開[33]する。 ※議事録の公開については、以下を満たすこと −公開する議事録は、必ずしも議事録全体である必要はない。特に、議事録にデータ管理者のセキュリティリスクにかかわる特定情報や事業上の秘密情報が記載されている場合は、残留リスクの暴露に相当することになる。そのような場合には、データ倫理審査会議事録に記載されている機密性の高い情報を削除し、個人に関連する重要な項目と構成員を記述した公開要約版の公開であっても構わない。 ・情報提供先の選択肢及びユーザインターフェイスの適切性について、助言を行う。

[33] データ倫理審査会の開催は、サービス事業の企画前及びサービス事業の開始前に、提供先の妥当性や個人に還元する便益等を協議する「ビジネススキームの妥当性協議」と、開始後に ユーザビリティや残留リスクの受容性を審議する「個人視点でのデータ倫理審議」が必要である。少なくとも年1回、ビジネスの変更の発生時等 必要に応じて適宜開催することを求める。

項目	認定基準及びその適合性を確認するために必要な提出書類
	・「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[34]、「情報銀行」は当該求めに応じて、適切に対応すること 〇諮問体制の［実施］。以下を満たす、審議事項を実施していること ・個人と情報銀行の間の契約の内容 ※「個人と情報銀行の間の契約の内容」において、適切性を審議すべきものとして、以下が挙げられる。 −ビジネススキームの妥当性（個人情報を委任する個人に不利益が及ばないか） −残留リスクの妥当性（リスク対策を施してもなお残るリスクは受容可能か） −個人へ還元する便益の妥当性（個人の全てが、直接的又は間接的な便益を受け取ることができるか） ・情報銀行に委任した個人情報の利用目的 ※「情報銀行に委任した個人情報の利用目的」において、適切性を審議すべきものとして、以下が挙げられる。 −利用目的の妥当性（わかり易いか、個人が誤解するような説明がなされていないか、個人に便益が提供できない個人情報の取り扱いがなされていないか） −取得する個人情報の項目（利用目的の達成のために必要最小限の項目となっているか）、便益との関連（個人に便益を還元するために必要最小限の項目となっているか） −利用目的の説明の妥当性（わかり易いか、個人が誤解するような説明がなされていないか） ・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） ※「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）」において、適切性を審議すべきものとして、以下が挙げられる。 −個人の同意を得る様々な場面（個人情報の取得時、サービス利用開始時、サービス利用中等）において、情報銀行から個人に提示すべき情報が、個人に分かり易く提示できているか

[34] データ倫理審査会は以下の項目についての調査・報告を求めることができる。
−データ倫理審査会の運用ルールが定められ文書化されているか
−データ倫理審査会の運用ルールに「情報銀行に調査・報告を求めることができる」旨の規定があるか

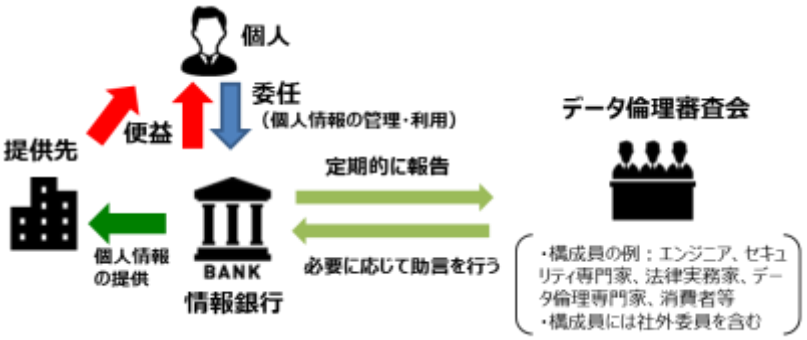
項目	認定基準及びその適合性を確認するために必要な提出書類
	−提供先の選択・同意、提供履歴の閲覧、訂正、利用停止、問合せ対応等、個人のコントローラビリティが確保されているか ・提供先第三者の選定方法 ※「提供先第三者の選定方法」において、適切性を審議すべきものとして、以下が挙げられる。 −提供先がプライバシーマーク又はISMSを取得していない場合の代替措置の妥当性 −提供先第三者の個人情報の利用目的の妥当性（個人にとって不利益となる利用がなされていないか） −安全管理措置のレベルの妥当性（個人情報の取り扱いプロセスにおいて、リスク対策が十分になされているか） −情報銀行による提供先第三者の監督方法の妥当性（提供先第三者を監督する方法は十分か、契約のみではなく、実地監査などの手段が講じられているか）、提供先第三者からの再提供の有無、及びその管理方法の妥当性 ・委任を受けた個人情報の提供の判断 ※「委任を受けた個人情報の提供の判断」において、適切性を審議すべきものとして、以下が挙げられる。 −提供する個人情報の項目の妥当性（提供先の利用目的を達成するために必要最小限の項目になっているか） −選定された提供先第三者が、提供先としてふさわしいか。提供先選定の判断プロセスの妥当性 ■提出書類（例） 【4-4】構成員の所属、経歴、専門等を記載した書類（構成員名簿等） 【4-5】設置の目的・審議事項等を規定した書類（設置要綱、設置規則等） 【4-5】データ倫理審査会で何を審査するかの規定と、規定に基づき審査した議事録 【4-5】構成員及び（必要な範囲の）議事録が公開された URL 等 データ倫理審査会運用ガイドライン(TPDMS-1140)を参照すること
④透明性（定期的な報告・公表等）	■認定基準 〇提供先第三者、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

項目	認定基準及びその適合性を確認するために必要な提出書類
	○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 ■提出書類（例） 【3-20】個人データ取扱手順に大きな変更があった場合の通知内容及び方法を定めた書類 【4-7】透明性確保を示す書類（開示項目一覧、開示先URL等） 【4-7】個人による情報銀行の選択に資する情報を示す書類
⑤認定団体との間の契約	■認定基準 ○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 ■提出書類（例） 【4-8】認定団体との契約関係書類 【4-9】認定マークの表示箇所を示す書類（画面キャプチャ等）

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

【出典】指針 ver2.0

5.5 事業内容

5.5.1 事業内容の具体的基準

項目	認定基準及びその適合性を確認するために必要な提出書類
①契約約款の策定	■認定基準 〇モデル契約約款の記載事項に準じ、認定団体が定めるモデル契約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） ■提出書類（例） 【5-1】個人との契約関係書類 【3-8】情報提供元との契約関係書類 【1-8】情報提供先との契約関係書類 【5-2】契約約款の公表状況を示す書類（実サービスの画面キャプチャ等）
②個人への明示及び対応	■認定基準 〇以下について、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 ・個人が相談窓口を利用するための手続 ■提出書類（例） 【5-3】15001「A.3.4.2.5　A.3.4.2.4 のうち本人から直接書面によって取得する場合の措置」及び 15001「A.3.4.4 個人情報に関する本人の権利」に対応する書類 【5-3】「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）を示した書類 【5-3】統計情報・匿名加工情報に加工して提供していることを示す書類（提供する場合）

項目	認定基準及びその適合性を確認するために必要な提出書類
③「情報銀行」の義務について	■認定基準 〇以下の要件を満たすとともに、モデル契約約款の記載事項に準じて契約約款等に明記し、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） ・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」（https://www.soumu.go.jp/main_content/000648745.pdf）3-③提供先第三者からの「再提供」禁止に関する考え方（P.23～26）参照 これを踏まえ、IT連盟としては、再提供が一定の条件により認められるケース　について、実質的な遵守基準の考え方を、以下に定める。 ・情報銀行が取得した個人データについては、個人データの取り扱いの各プロセスにおいて情報銀行のリスクアセスメントによって認識した脆弱性があってはならず、これは再提供先といえども同様である。 ・この結果、再提供先は、十分な個人データの保護水準を満たしている

項目	認定基準及びその適合性を確認するために必要な提出書類
	者を選定しなければならない。具体的には、第三者認証を取得していることである（プライバシーマークまたは、ISMS認証、等）。 ・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情報銀行に報告すること ・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 ・再提供先からの更なる第三者提供は認められない。 ・再提供先における個人情報の取扱いが、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、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、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） ■提出書類（例） 【5-1】個人との契約関係書類 【1-8】情報提供先との契約関係書類
④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	■認定基準 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(※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。） ・選択を実効的なものとするために適切なユーザインターフェイス（UI、操作が容易なダッシュボードなど）を提供すること

項目	認定基準及びその適合性を確認するために必要な提出書類
	・選択肢及びユーザインターフェイス（UI）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インターフェイス（UI）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インターフェイス（UI）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（※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。） ・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 ■提出資料（例） 【6-1】上記①から④の機能の提供を示す書類（実サービスの画面キャプチャ、Web モック画面のキャプチャ、イメージ図等）
⑤責任の範囲について	■認定基準 〇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 〇「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

項目	認定基準及びその適合性を確認するために必要な提出書類
	責任を負うこと 〇「情報銀行」は、利用者からIT連盟の苦情相談窓口への苦情相談等に適切に対応すること 〇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こと ■提出資料（例） 【1-4】15001「A.3.3.2 法令、国が定める指針その他の規範」に対応する書類 【6-2】15001「A.3.6 苦情及び相談への対応」に対応する書類 【1-8】情報提供先との契約関係書類

6 モデル契約約款

6.1 個人情報の提供に関する契約上の合意の整理

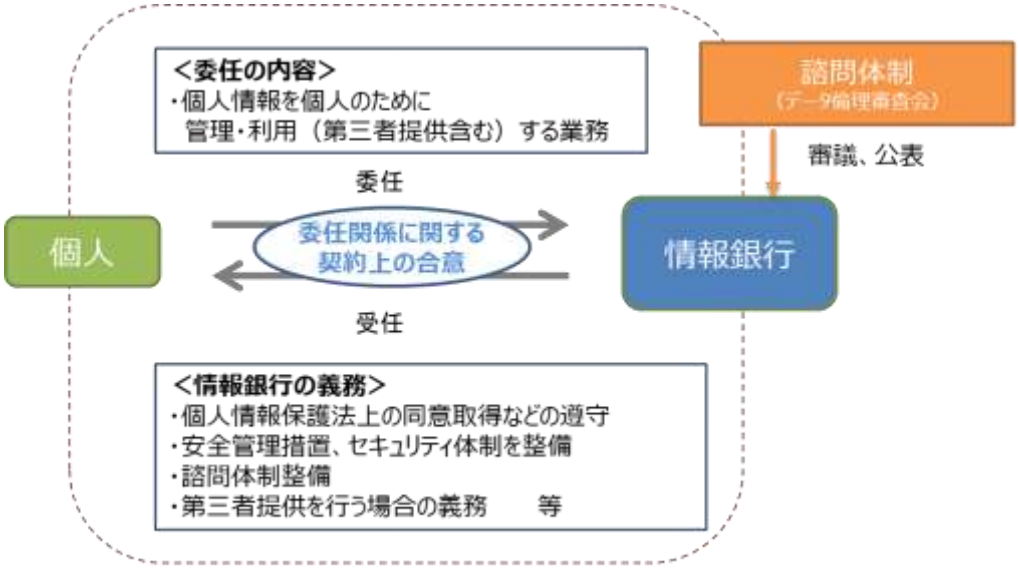
情報信託機能検討会の指針 ver2.0 において、「個人情報の提供に関する契約上の合意の整理」については、次のとおりとされている。

■ 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

【出典】指針 ver2.0

【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。

6.2 モデル契約約款

IT 連盟において、前述 6.1 の整理及び指針 ver2.0 における「モデル約款の記載事項」を踏まえ、認定にあたって最低限盛り込む必要がある規定を記載した「モデル契約約款」（別添）を策定した。

申請事業者において、認定を受ける「情報銀行」事業を行う場合は、少なくとも「モデル契約約款」を盛り込んだ契約約款を作成することが必要となる。

個人と「情報銀行」の間は、モデル約款。「情報銀行」と情報提供元との間および「情報銀行」と情報提供先との間は、モデル契約とした。

＜参考＞指針 ver2.0 における「モデル約款の記載事項」

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

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

（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、「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） 個人情報を情報提供元事業者から「情報銀行」に移行する場合
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）「情報銀行」から確認など求めがあった場合
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、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

別添）変更履歴表

【2020 年 7 月 1 日 改訂（ver.2.0）】

ページ	項番	ガイドブック ver.2.0
1～5	1. はじめに	情報の追記 本書の概説の追加
6	2. 認定の対象となる「情報銀行」の範囲	指針 ver2.0 に合わせて変更
7～10	2. 認定の対象となる「情報銀行」の範囲	（1）個人情報の提供に関する同意の方法 （2）事業で扱うデータの種類 （3）個人情報の収集方法 以上、指針 ver2.0 に合わせて変更 （4）認定の対象となる事業者 （5）認定の単位及び種類 以上、追加
12～13	3. 運用スキーム	認定機関全体図に情報銀行推進委員会委員を追加し、その説明を記載
14	4.1 全体フロー	情報銀行推進委員会による認定判定決議を追加
15～16	4.2 事前申請フロー	事前申請エントリー～事前申請ミーティングの追加等、事前申請フローの見直し修正
17～20	4.3 本申請フロー	キックオフミーティングの実施要領、書類審査の手順の追記等、本申請フローの見直し修正
21～23	4.4 認定決定フロー	認定会議、情報銀行推進委員会の開催、認定付与に係る条件、P 認定の場合の付与後の流れ等、認定決定フローの見直し修正
26	5.1.1 事業者の適格性の具体的基準	②業務能力など の認定基準の捕捉説明追記
28、30、31	5.2.2 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 の提出書類（例）追加 ⑩運用の情報セキュリティ の認定基準及び提出書類（例）追加 ⑪通信の情報セキュリティ の認定基準及び提出書類（例）追加
33～39	5.3.2 プライバシー保護対策の具体的基準	①基本方針の策定 の認定基準及び提出書類（例）は 5.1.1 の該当箇所参照 ②組織的安全管理措置 の提出書類（例）の内部規定に関する補足として、脚注を追記 ④物理的安全管理措置及び⑤技術的安全管理措置 の認定基準及び提出書類（例）は 4 章の該当箇所参照 ⑥同意及び選択 の認定基準の補足説明追記及び提出書類（例）追加 ⑨データの最小化 の認定基準の捕捉説明追記 ⑩利用、保持及び開示の制限 の認定基準及び提出書類（例）の捕捉説明追加

43～47	5.4.1 ガバナンス体制の具体的基準	③諮問体制　の解説、認定基準及び提出書類（例）追加及び指針 ver2.0 の記載内容を引用追記 ④透明性（定期的な報告・公表等）　の認定基準及び提出書類（例）追加
48～51	5.5.1 事業内容の具体的基準	②個人への明示及び対応　の認定基準及び提出書類（例）追記 ③「情報銀行」の義務について　の認定基準追加及び提出書類（例）追記 ④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　の認定基準追記
53	6.1 個人情報の提供に関する合意の整理	未成年等の制限行為能力者が情報銀行を利用する場合について追記
54～57	6.2 モデル契約約款	指針 ver2.0 に合わせて修正

【2021 年 7 月 1 日　改訂（ver.2.01）】

ページ	項番	ガイドブック ver.2.01
15、16	4.2.3　事前申請必要書類の作成～提出	「TPDMS-2210 欠格事由及び判断基準」の欠格事由に該当していないことの宣言　を必要書類⑦として追加
23	4.4.5　サーベイランス審査	サーベイランス審査に関する説明を追加
24	4.4.7　認定付与の更新	認定付与の更新に関する説明を追加
25～27	5.1.1　事業者の適格性の具体的基準	②の、提出書類（例）を加筆修正
28	5.2.1 基本原則及び遵守基準	参考基準等　の参照先名称、URL を更新
29～55	5.2.1、5.3.2、5.4.1、5.5.1	提出書類（例）　に、「に対応する書類」という文言を追記　※必要該当箇所に追記
29～34	5.2.2　情報セキュリティの具体的基準	④、⑤、⑥、⑦、⑧、⑩、⑮、⑯の、提出書類（例）を加筆修正
35～44	5.3.2 プライバシー保護対策の具体的基準	⑥、⑩の、提出書類（例）及び脚注を加筆修正
45～49	5.4.1 ガバナンス体制の具体的基準	③、④の、提出書類（例）及び脚注を加筆修正
48	5.4.1 ガバナンス体制の具体的基準	③諮問体制の参照基準として、データ倫理審査会運用ガイドライン（TPDMS-1140）を追加
50～54	5.5.1 事業内容の具体的基準	①、④の、提出書類（例）を加筆修正