

# 「情報銀行」認定 申請ガイドブック

ver 0.9

(素案)

一般社団法人 日本IT団体連盟  
情報銀行推進委員会  
201x年〇月〇日

1	はじめに.....	1
2	認定の対象となる「情報銀行」の範囲.....	4
3	運用スキーム.....	7
4	申請・認定フロー.....	10
4.1	全体フロー.....	10
4.2	事前申請フロー.....	11
4.2.1	事前申請書類の入手と提出.....	12
4.2.2	事前申請必要書類の入手.....	12
4.2.3	事前申請書類の書類提出.....	12
4.2.4	秘密保持契約の締結.....	12
4.2.5	各種書類の提出・お問い合わせ窓口.....	12
4.2.6	事前申請の受理.....	12
4.2.7	申請スケジュール、料金等の提示.....	12
4.2.8	申請の取下げ.....	12
4.3	本申請フロー.....	13
4.3.1	本申請必要書類の提出.....	15
4.3.2	秘密保持契約の締結.....	15
4.3.3	本申請の受理と請求処理.....	15
4.3.4	キックオフミーティング.....	15
4.3.5	認定対応書類の提出.....	15
4.3.6	質疑応答.....	16
4.3.7	現地調査.....	16
4.3.8	質疑応答.....	16
4.3.9	回答期限と取り下げの判断.....	16
4.4	認定決定フロー.....	17
4.4.1	適合性評価・認定判定.....	19
4.4.2	追加調査.....	19
4.4.3	契約書の締結及び請求.....	19
4.4.4	認定の付与.....	19
4.4.5	認定の公表.....	19
4.4.6	認定の取消し等.....	19
5	認定基準と提出書類.....	20
5.1	事業者の適格性.....	20
5.2	情報セキュリティ等.....	23
5.2.1	基本原則及び遵守基準.....	23
5.2.2	具体的基準.....	24
5.3	プライバシー保護対策等.....	29
5.3.1	基本原則.....	29
5.3.2	具体的基準.....	29

5.4	ガバナンス体制.....	38
5.5	事業内容.....	40
6	モデル約款.....	47
6.1	個人情報の提供に関する契約上の合意の整理.....	47
6.2	モデル約款.....	48
①	個人と「情報銀行」の間.....	48
②	「情報銀行」と情報提供元との間.....	50
③	「情報銀行」と情報提供先との間.....	50

# 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<sup>1</sup>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)<sup>2</sup>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。

<sup>1</sup> 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(<https://www.ppc.go.jp/personal/legal/>)参照。

<sup>2</sup> 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](https://www.kantei.go.jp/jp/singi/it2/hourei/deta_katsuyosuishin.html))参照。

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」。) <sup>3</sup>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)へデータ提供でき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 <sup>4</sup>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」が重要となる。

<sup>3</sup> 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](https://www.kantei.go.jp/jp/singi/it2/senmon_bunka/data_ryutsuseibi/kentokai.html))参照。

<sup>4</sup> 総務省ウェブページ([http://www.soumu.go.jp/menu\\_news/s-news/01tsushin01\\_02000227.html](http://www.soumu.go.jp/menu_news/s-news/01tsushin01_02000227.html))参照。

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」)<sup>5</sup>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<sup>6</sup>において、「情報銀行」制度についての政策提言を発表<sup>7</sup>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、第三者の事業者にも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<sup>8</sup>、同10月には説明会<sup>9</sup>を開催したところである。

「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利用が許諾される。認定マークについては、ver1.0 及びそれを踏まえて IT 連盟として策定した情報セキュリティやプライバシー保護対策等に関する認定基準に適合している事業を行うことを示すものであり、当該事業者が安心・安全な「情報銀行」として、消費者個人がその個人情報を信頼して託せる事業者であることをアピールすることが可能となる。

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、現在、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」<sup>10</sup>が上記データ活用 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するとともに、情報信託機能検討会では指針 ver1.0 の見直しに向けた検討等が行われている。従って、本書については、これらの検討結果等をふまえて、今後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。

<sup>5</sup> 総務省ウェブページ([http://www.soumu.go.jp/main\\_sosiki/kenkyu/information\\_trust\\_function/index.html](http://www.soumu.go.jp/main_sosiki/kenkyu/information_trust_function/index.html))参照。

<sup>6</sup> 総務省ウェブページ(本文については [http://www.soumu.go.jp/main\\_content/000501157.pdf](http://www.soumu.go.jp/main_content/000501157.pdf)、概要については [http://www.soumu.go.jp/main\\_content/000501156.pdf](http://www.soumu.go.jp/main_content/000501156.pdf))参照。

<sup>7</sup> 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。

<sup>8</sup> 2018年9月12日。IT 連盟ウェブページ(<https://www.itrenmei.jp/registration/>)参照。

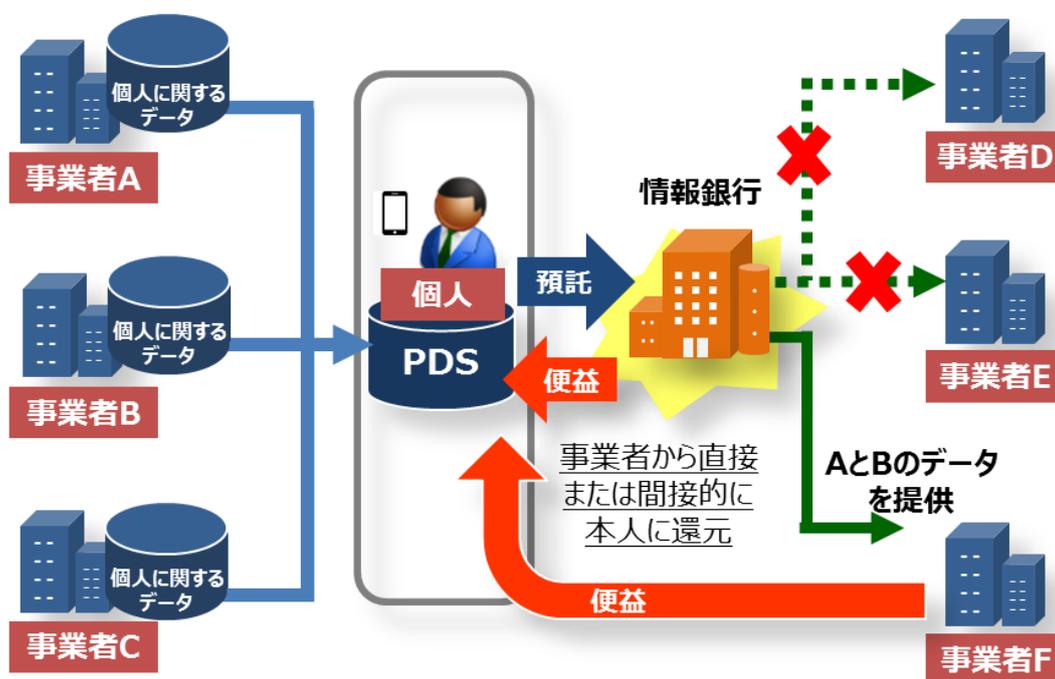
<sup>9</sup> 2018年10月16日「情報銀行認定」に関する説明会。資料は、IT 連盟ウェブページ(<https://www.itrenmei.jp/registration/>)参照。

<sup>10</sup> 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](https://www.kantei.go.jp/jp/singi/it2/detakatuyo_wg/index.html))参照。

## 2 認定の対象となる「情報銀行」の範囲

「情報銀行」<sup>11</sup>とは、データ活用 WG 中間とりまとめにおいて、「個人とのデータ活用に関する契約等に基づき、PDS<sup>12</sup>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。(データの提供・活用に関する便益は、データ受領事業者から直接的又は間接的に本人に還元される。)」と定義されている。

【「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。

【出典】データ活用 WG 中間とりまとめ

<sup>11</sup> 「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)  
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。

<sup>12</sup> 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。

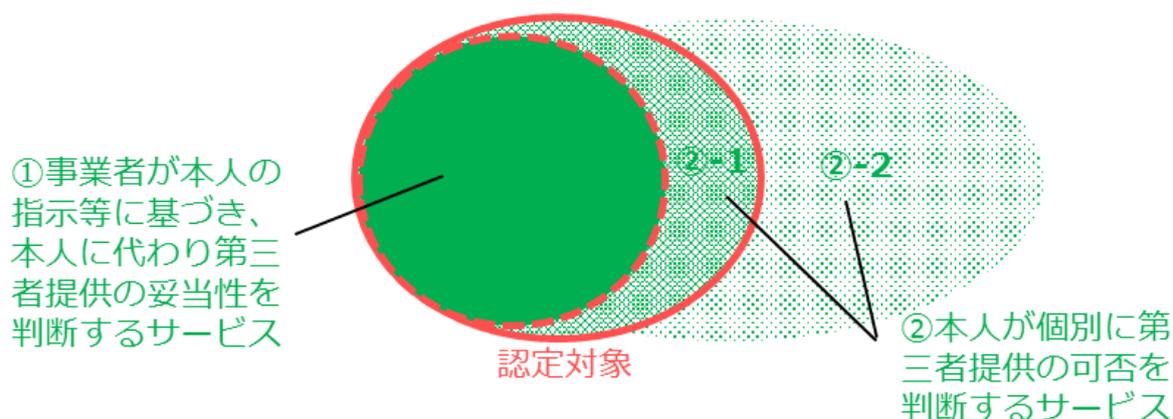
IT 連盟による認定の対象となる「情報銀行」については、情報信託機能検討会の指針 ver1.0 を踏まえ、具体的には次のものとする。

### (1) 個人情報の提供に関する同意の方法

認定の対象としては、「情報銀行」認定を申請する事業者(以下「申請事業者」という。)が、個人情報の第三者提供について、消費者個人本人が同意した一定の範囲において、当該本人の指示等に基づき当該本人に代わり第三者提供の妥当性を判断するサービスを提供する場合(以下①の部分)を基本とする。

また、今後の様々な形態の事業の出現を想定し、当該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、申請事業者が個人情報の提供先を選定して当該本人に提案する場合など、申請事業者が比較的大きな役割を果たす(責任をもつ)場合(以下②-1の部分)も認定の対象として含むこととする<sup>13</sup>。

他方、純粋なPDSなどデータの管理や提供に関し消費者個人の主体性が強いサービスを提供する場合(以下②-2の部分)は認定の対象には含まれない。



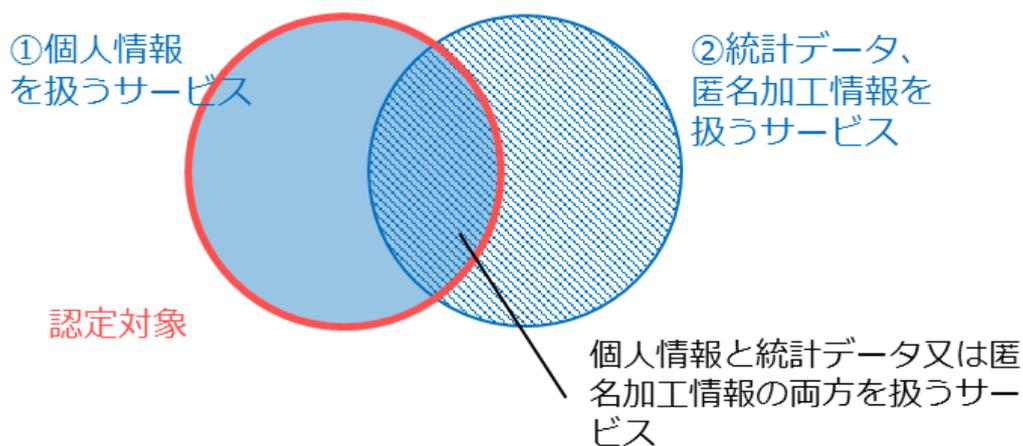
【出典】指針 ver1.0

<sup>13</sup> (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」の定義よりも広がっている。

## (2) 個人情報の種類

認定の対象としては、「個人情報」<sup>14</sup>(ただし、「要配慮個人情報」<sup>15</sup>、クレジットカード番号及び銀行口座番号を除く。以下「対象個人情報」という。)を扱うサービスを提供する場合を基本とする。なお、以上の場合においては、対象個人情報とともに、統計データ又は匿名加工情報も扱うサービスを提供する場合も含まれる。

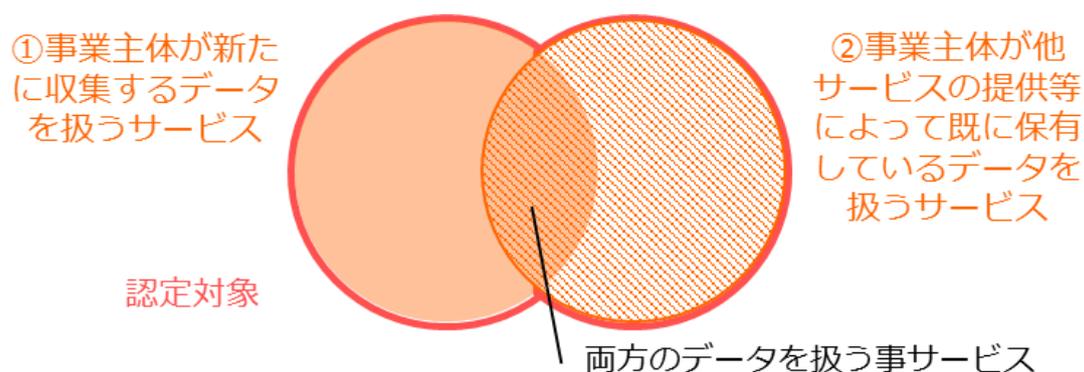
他方、統計データ又は匿名加工情報のみを扱うサービスを提供する場合は認定の対象ではない。



【出典】指針 ver1.0

## (3) 個人情報の収集方法

認定の対象としては、申請事業者が新たに収集する個人情報を扱うサービスを提供する場合のみならず、当該事業者が他サービスの提供等によって既に保有している個人情報を扱うサービスを提供する場合も含まれる。



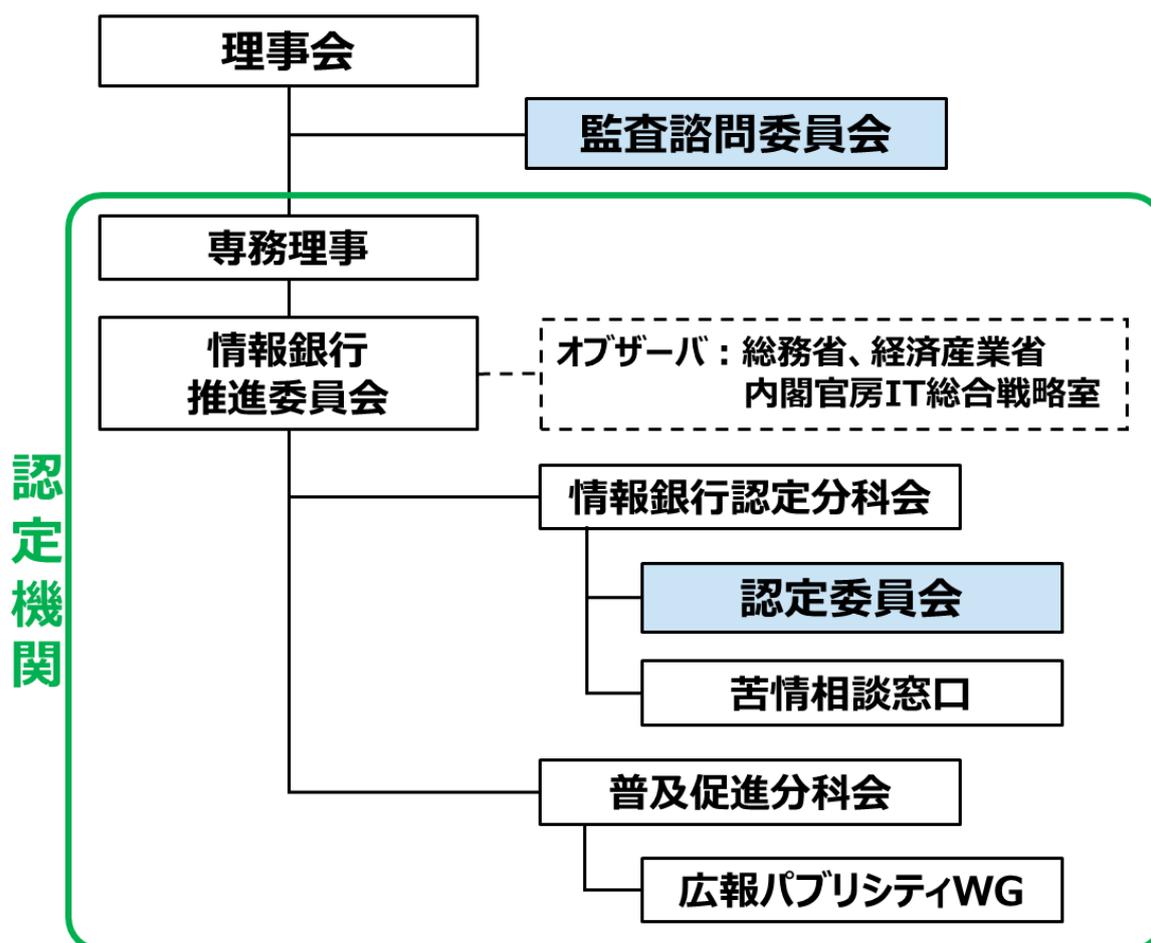
【出典】指針 ver1.0

<sup>14</sup> 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。

<sup>15</sup> 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。

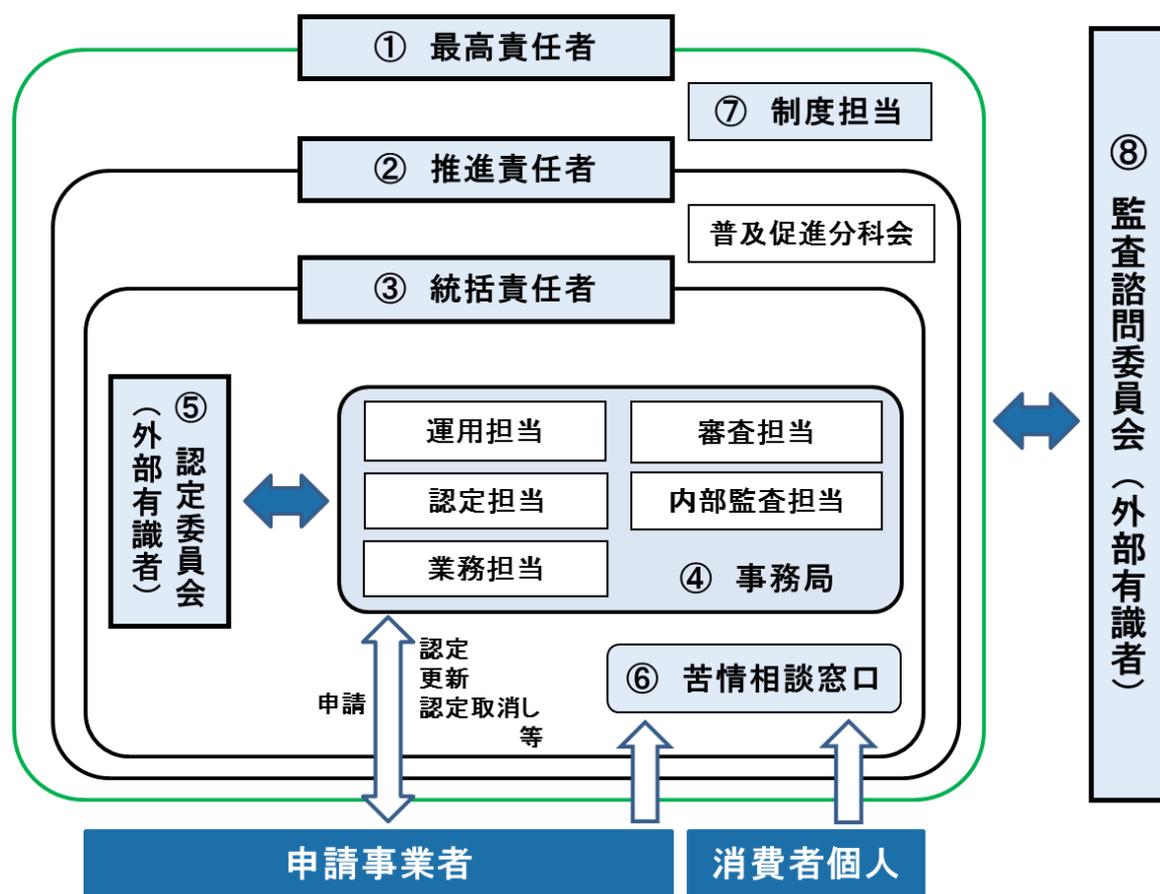
### 3 運用スキーム

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 ver1.0 及び JIS Q 17065 (ISO/IEC17065)「適合性評価-製品、プロセス及びサービスの認証を行う機関に対する要求事項」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 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。
- ⑦ 制度担当：指針 ver1.0 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。
- ⑧ 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。

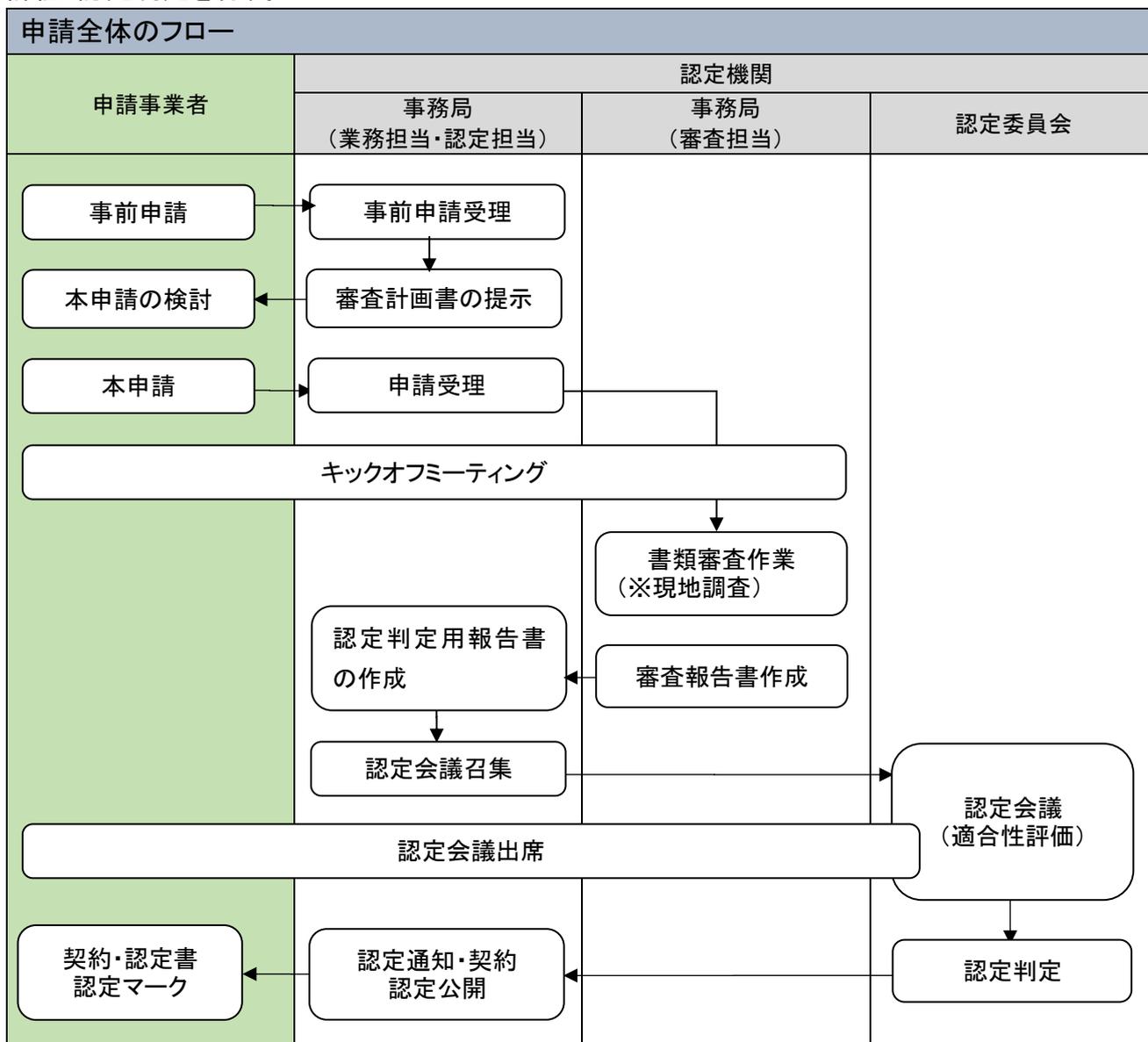
## 4 申請・認定フロー

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

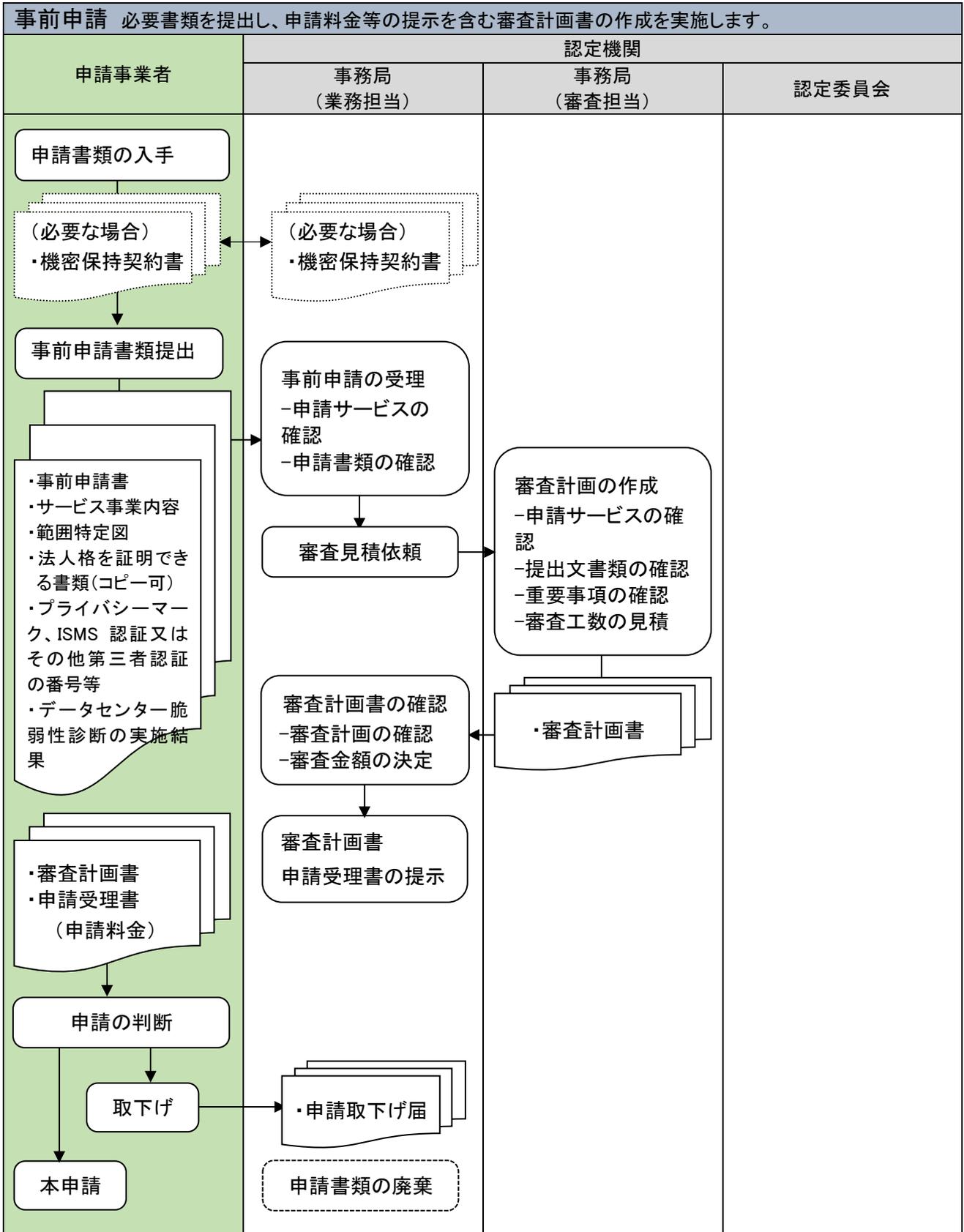
申請事業者においては、はじめに事前申請を行う。事前申請における提出書類等を踏まえ、IT 連盟において審査料金を算出し、審査計画を作成する。

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 事前申請書類の入手と提出

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。

#### 4.2.2 事前申請必要書類の入手

事前申請に必要な書類等はIT連盟のウェブページ(【※URLを記載予定】)よりダウンロード可能である。

#### 4.2.3 事前申請書類の書類提出

申請者は、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にて提出する。

- ① 事前申請書
- ② サービス事業内容
- ③ サービス事業の範囲が特定できる図表等
- ④ 法人格を証明できる書類(コピー可)
- 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
- ⑥ データセンターの脆弱性診断の実施記録

#### 4.2.4 秘密保持契約の締結

事前申請書類の情報開示において、秘密保持契約の取り交わしが必要な場合は、「秘密保持契約書」(別紙様式)を提出する。

#### 4.2.5 各種書類の提出・お問い合わせ窓口

一般社団法人日本IT団体連盟

情報銀行推進委員会 情報銀行認定分科会 認定事務局

【※URLを記載予定】

#### 4.2.6 事前申請の受理

事務局は、提出書類などに基づき、事前申請の受付を行い、書類一式に不備がなくすべてが揃っていることを確認する。

#### 4.2.7 申請スケジュール、料金等の提示

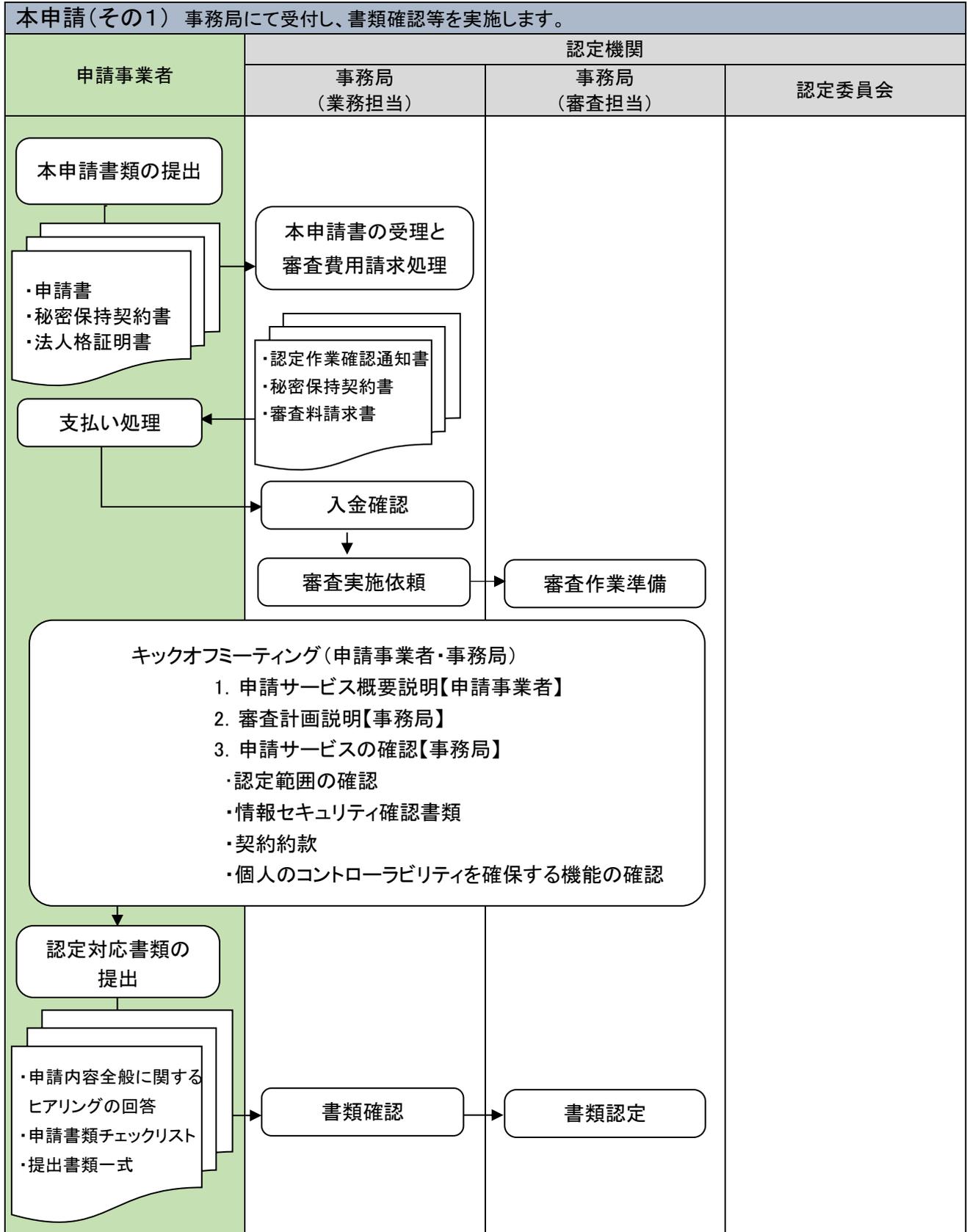
事務局より、申請者に、審査スケジュール、審査担当等の記載された「審査計画書」、申請料金等の提示された「申請受理書」を送付する。申請者は本申請に進むかを検討する。

#### 4.2.8 申請の取下げ

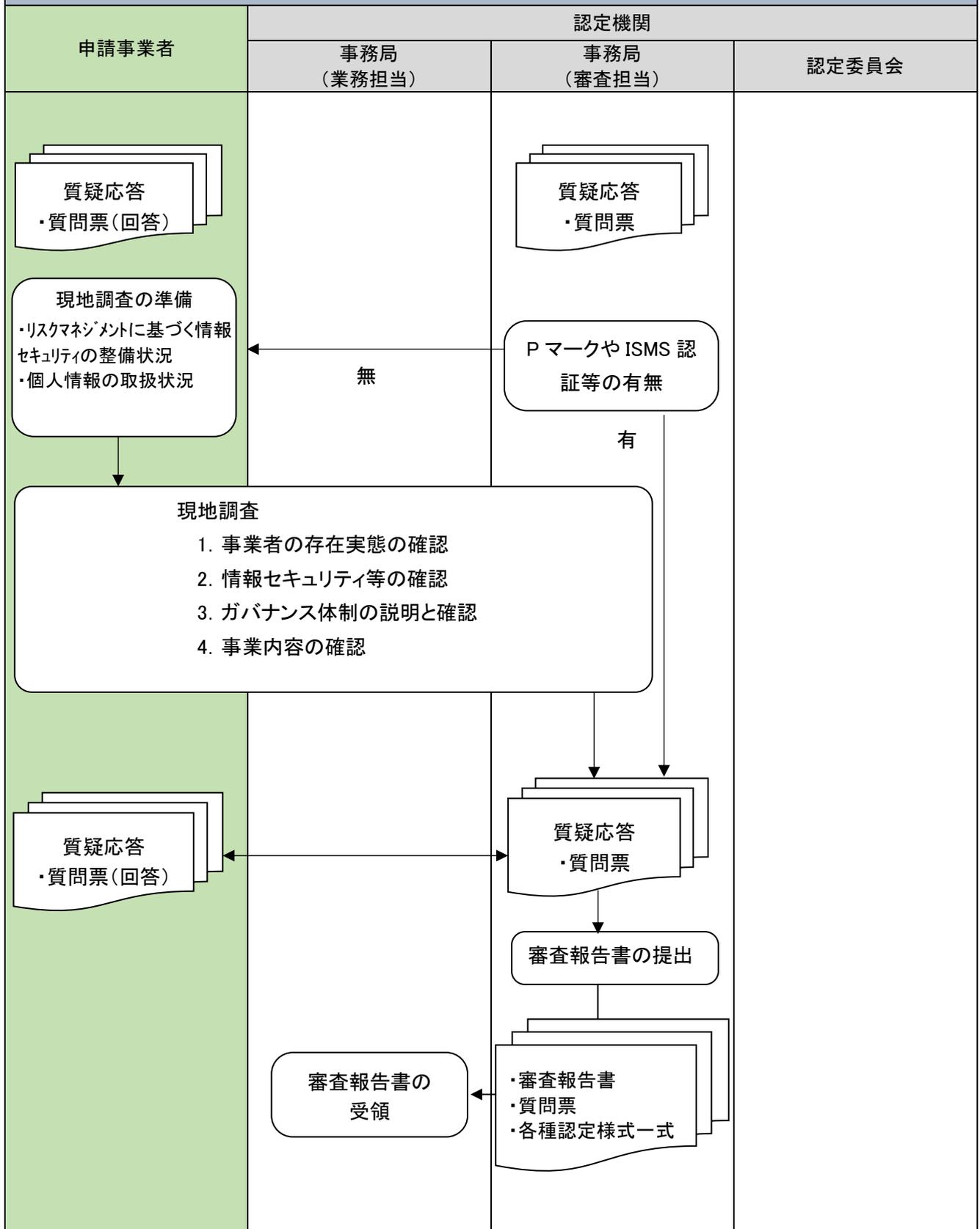
本申請に進まず、申請を取り下げる場合は、1週間を目途に「申請取下げ届」に必要事項を記入の上、事務局に提出する。事務局は、申請者からの受領書類一式を廃棄する。

### 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。



本申請(その2) 事務局にて審査を実施します。



#### 4.3.1 本申請必要書類の提出

申請事業者は、申請に必要な以下の書類を用意し、事務局に提出する。

- ① 申請書
- ② 秘密保持契約書(別紙様式)
- ③ 法人格証明書

#### 4.3.2 秘密保持契約の締結

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

#### 4.3.3 本申請の受理と請求処理

事務局は、提出書類などに基づき、本申請の受付を行い、書類一式に不備がなくすべてが揃っていることを確認する。確認後、申請事業者に「認定作業確認通知書」、「秘密保持契約書」及び審査料金の提示された「請求書」が送付される。

申請事業者は請求書に記載の期日までに指定の口座へ手数料を入金する。

※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。

#### 4.3.4 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・事務局(審査担当等)による「キックオフミーティング」を次の通り実施する。

##### ① 申請サービス事業の概要説明【申請事業者】

申請サービス事業の概要(デモンストレーションを含む)を説明する。

##### ② 審査計画説明【事務局】

審査計画書をもとに認定作業のスケジュール、認定作業の内容等を説明する。

##### ③ 申請サービス事業の確認【事務局】

申請サービス事業に関して、以下の内容を確認する。

- ・認定範囲の確認
- ・情報セキュリティ確認書類
- ・契約約款(後述する「6. モデル約款」参照)
- ・個人のコントローラビリティを確保する機能の確認

#### 4.3.5 認定対応書類の提出

申請事業者は、認定に必要な下記書類を用意し、事務局に提出する。なお、必要書類の作成については、「キックオフミーティング」時に、事務局より説明する。

- ① 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
- ② 申請書類チェックリスト
- ③ 「提出書類」(第5章参照)一式

#### 4.3.6 質疑応答

必要書類の提出確認が完了後、事務局による確認作業が開始される。

事務局が確認作業中に確認事項があった場合や問題を発見した場合、事務局は申請事業者に対して「質問票」を発行する。

申請事業者は、「質問票」を受け取り次第、速やかに確認事項の回答や問題の解決を図る。また、申請事業者から事務局への連絡も行うことができる。

#### 4.3.7 現地調査

Pマーク、ISMS認証、又は、それらと同等の第三者認証を受けていない事業者及びサービス事業の場合、申請内容の確認、文書の整理状況や管理体制等の確認を目的に、現地調査を行う。

以下の項目について、現地調査を行う。

- ① 申請事業者の存在実態の確認
- ② 情報セキュリティ等の確認
- ③ ガバナンス体制の説明と確認
- ④ 事業内容の確認

#### 4.3.8 質疑応答

事務局が現地確認作業中に確認事項があった場合や問題を発見した場合、申請事業者に対して「質問票」を発行する。

申請事業者は、「質問票」を受け取り次第速やかに確認事項の回答や問題の解決を図る。また、申請者から事務局への連絡も行うことができる。

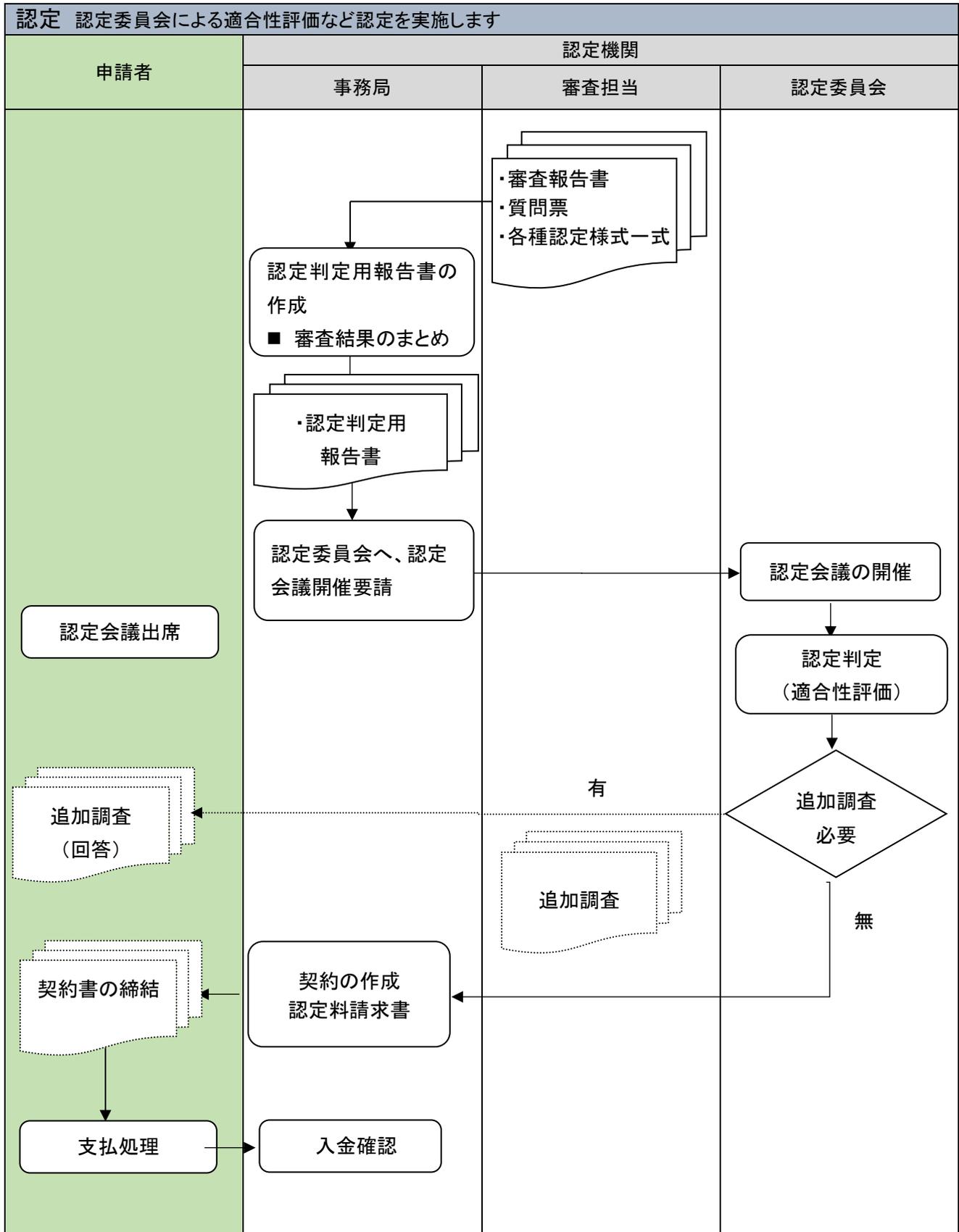
#### 4.3.9 回答期限と取り下げの判断

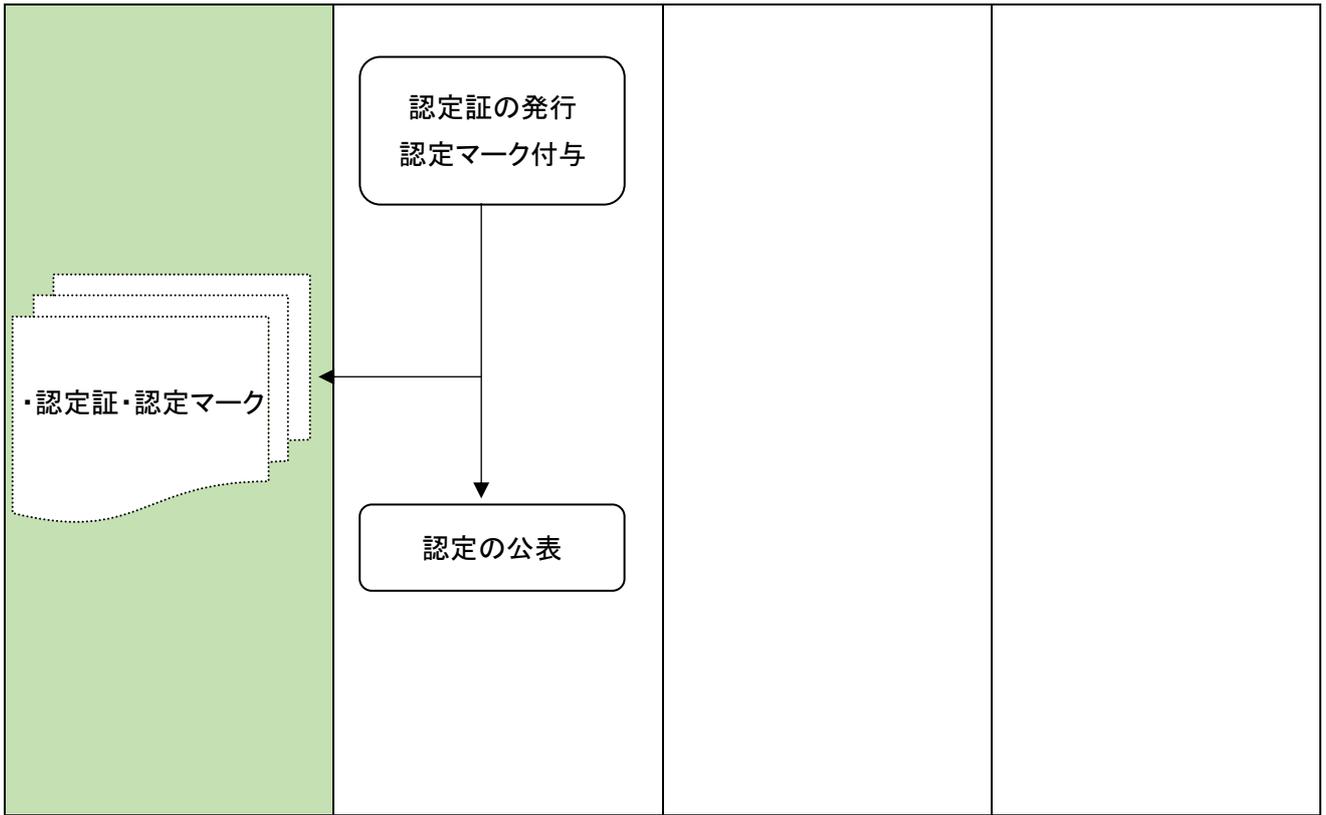
書類の提出及び質疑応答では、基本的に要請から1ヶ月以内に回答することが必要である。

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。

#### 4.4 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、審査結果に関する「審査報告書」等に基づき「認定用報告書」を作成し、「認定委員会」にて、適合性評価、認定判定が実施される。その際、認定委員会の判断により、追加資料の提出や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は、再度認定会議が開催される場合がある。

#### 4.4.2 追加調査

適合性評価・認定判定の際に、追加資料の提出や追加調査の条件付きで認定する場合がある。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。

#### 4.4.3 契約書の締結及び請求

認定を受けた申請事業者（以下「認定事業者」という。）について、申請事業者と IT 連盟との間で契約書を締結する。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。

また、契約締結後、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手数料を入金する。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。

#### 4.4.4 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 Web サイト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る場合については、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ができる。

#### 4.4.5 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連盟のウェブページに掲示する。

#### 4.4.6 認定の取消し等

認定事業者において、IT連盟に消費者から苦情相談等があり、IT連盟より認定事業者に問題解決を求めたにもかかわらず当該認定事業者による対応に問題があった場合及び個人情報の漏えいの発生など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、認定の取り消し、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。

## 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 ver1.0 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

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	<p>■ 認定基準</p> <p>○法人格を持つこと</p> <p>※「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</p> <ul style="list-style-type: none"> <li>・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)</li> <li>・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)</li> </ul> <p>■ 提出書類(例)</p> <p>【1-X】事業者の登記簿謄本</p> <hr/> <p>■ 認定基準</p> <p>○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る財産的基礎を有していること</p> <p>(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</p>

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
	<p>■ 提出書類(例) 【1-X】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)</p> <hr/> <p>■ 認定基準 ○ 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</p> <p>■ 提出書類(例) 【1-X】損害保険証書(ない場合は、【1-X】の提出書類)</p>
②業務能力など	<p>■ 認定基準 ○ 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(個人情報保護方針)、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</p> <p>■ 提出書類(例) 【1-X】「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(関連行政機関への届出、許認可等) 【1-X】15001「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-X】27001「5.2 方針」の公開先を示す書類(URL 等)</p> <hr/> <p>■ 認定基準 ○ 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</p> <p>■ 提出書類(例) 【1-X】プライバシーマーク又はISMS認証の取得を示す書類(これらが無い場合は、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)</p> <hr/> <p>■ 認定基準 ○ 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</p>

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
	<p>■ 提出書類(例) 【1-X】情報提供先との契約関係書類</p> <hr/> <p>■ 認定基準 ○ 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</p> <p>■ 提出書類(例) 【1-X】当該サービス事業の内容と範囲を示す書類</p>

## 5.2 情報セキュリティ等

### 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 ver1.0 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）
- 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についてガイドラン（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/pm_shinsakijun.pdf)  
[https://privacymark.jp/system/guideline/pdf/guideline\\_V2\\_180410.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/](http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/)

### 5.2.2 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 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。)及び「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」(以下「27002」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
情報セキュリティマネジメントの確立	<p>■認定基準</p> <ul style="list-style-type: none"> <li>○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</li> <li>○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</li> <li>○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</li> </ul> <p>■提出書類(例)</p> <p>【2-X】27001「5.2 方針」、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」及び 27001「6.1 リスク及び機会に対処する活動」に対応する書類</p>
情報セキュリティマネジメントの運用・監視・レビュー	<p>■認定基準</p> <ul style="list-style-type: none"> <li>○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</li> <li>○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</li> </ul> <p>■提出書類(例)</p> <p>【2-X】27001「5.3 組織の役割、責任及び権限」、27001「7 支援」、27001「6.1.2 情報セキュリティリスクアセスメント」、27001「9.2 内部監査」及び 27001「10.2 継続的改善」に対応する書類</p>
情報セキュリティマネジメントの維持・改善	<p>■認定基準</p> <ul style="list-style-type: none"> <li>○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</li> <li>○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</li> </ul>

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
	<p>■提出書類(例) 【2-X】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</p>
情報セキュリティ方針策定	<p>■認定基準 ○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</p> <p>■提出書類(例) 【2-X】27001「5.2 方針」及び 27002「5 情報セキュリティのための方針群」に対応する書類</p>
情報セキュリティ組織	<p>【認定基準】 ○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</p> <p>■提出書類(例) 【2-X】27001「5.3 組織の役割、責任及び権限」に対応する書類 【2-X】加盟団体名及び活動概要を示す書類</p>
人的資源の情報セキュリティ	<p>■認定基準 ○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</p> <p>■提出書類(例) 【2-X】27001「7.2 力量」に対応する書類 【2-X】情報セキュリティに関する教育の実施サマリー</p>
資産の管理	<p>■認定基準 ○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</p>

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
	<p>■提出書類(例)</p> <p>【2-X】27002「8.1.1 資産目録」、27002「8.1.2 資産の管理責任」、27002「8.3.2 媒体の処分」及び 27002「8.2 情報の分類」に対応する書類</p> <p>【2-X】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</p> <p>【2-X】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</p> <p>【2-X】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)</p>
技術的セキュリティ	<p>■認定基準</p> <p>(アクセス制御)</p> <p>○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)</p> <p>○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> <p>(暗号)</p> <p>○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</p> <p>○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</p> <p>■提出書類(例)</p> <p>【2-X】27002「9 アクセス制御」及び 27002「10 暗号」に対応する書類</p>

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
物理的及び環境的情報セキュリティ	<p>■認定基準</p> <ul style="list-style-type: none"> <li>○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</li> <li>○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</li> <li>○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</li> </ul> <p>■提出書類(例)</p> <p>【2-X】27002「11 物理的及び環境的情報セキュリティ」に対応する書類</p>
運用の情報セキュリティ	<p>■認定基準</p> <ul style="list-style-type: none"> <li>○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</li> <li>○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</li> <li>○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</li> <li>○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</li> <li>○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</li> </ul> <p>■提出書類(例)</p> <p>【2-X】27002「12.2.1 操作手順書」、27002「12.2 マルウェアからの保護」、27002「12.4 ログ取得及び監視」及び 27002「12.6 技術的ぜい弱性管理」に対応する書類</p>
通信の情報セキュリティ	<p>■認定基準</p> <ul style="list-style-type: none"> <li>○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</li> <li>○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</li> <li>○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</li> <li>○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)</li> </ul> <p>■提出書類(例)</p> <p>【2-X】27002「13.1.1 ネットワーク管理策」、27002「13.1.2 ネットワークサービスのセキュリティ」、27002「13.1.3 ネットワークの分離」及び 27002「13.2 情報の転送」に対応する書類</p>
システムの取得・開発・保守	<p>■認定基準</p> <ul style="list-style-type: none"> <li>○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</li> </ul>

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
	<p>○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</p> <p>■提出書類(例) 【2-X】27002「14.1 情報システムのセキュリティ要求事項」及び 27002「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</p>
供給者関係	<p>■認定基準</p> <p>○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</p> <p>○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応の要求事項を含む</p> <p>■提出書類(例) 【2-X】27002「15 供給者関係」に対応する書類</p>
情報セキュリティインシデント管理	<p>■認定基準</p> <p>○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</p> <p>○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</p> <p>○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</p> <p>○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</p> <p>■提出資料(例) 【2-X】27002「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-X】システムに対する脆弱性診断の実施内容を示す書類</p>
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	<p>■認定基準</p> <p>○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</p> <p>■提出書類(例) 【2-X】27002「17.1.1 情報セキュリティ継続の計画」に対応する書類</p>
遵守	<p>■認定基準</p> <p>○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</p> <p>○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</p> <p>○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</p> <p>■提出書類(例) 【2-X】27002「18.1 法的及び契約上の要求事項の順守」及び 27002「18.2 情報セキュリティのレビュー」に対応する書類</p>

## 5.3 プライバシー保護対策等

### 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 ver1.0 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・遵守していくことが必要とされているところである。

- 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 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
基本方針の策定	<ul style="list-style-type: none"><li>■ 認定基準</li><li>○ 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を含む方針を策定していること</li><li>■ 提出書類（例）</li><li>【3-X】15001「A.3.2.2 外部向け個人情報保護方針」に対応する書類</li></ul>
組織的安全管理措置	<ul style="list-style-type: none"><li>■ 認定基準</li><li>○ 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、取扱い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</li><li>■ 提出書類（例）</li></ul>

	<p>【3-X】15001「A.3.3.4 資源、役割、責任及び権限」、15001「A.3.3.5 内部規定」、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」に対応する書類</p>
人的安全管理措置	<p>■認定基準 ○従業員の教育を実施していること</p> <p>■提出書類(例) 【3-X】15001「7.3 認識」及び 15001「A.3.4.5 認識」に対応する書類 【3-X】プライバシー保護に関する教育実施サマリー</p>
物理的安全管理措置	<p>■認定基準 ○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、電子媒体等の廃棄を実施していること</p> <p>■提出書類(例) 【3-X】15001「C.11 物理的及び環境的セキュリティ」に対応する書類</p>
技術的安全管理措置	<p>■認定基準 ○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を実施していること</p> <p>■提出書類(例) 【3-X】15001「C.9 アクセス制御」に対応する書類</p>
同意及び選択	<p>■認定基準 ○個人情報の取扱いを許可するか否かの選択の機会について、制限なく、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いを明確に認める場合を除く。 ○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 ○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 ○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 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)の氏名又は職名, 所</p>

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

○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

○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-X】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-X】情報提供元との契約関係書類

【1-X】情報提供先との契約関係書類

【3-X】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「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」、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

<p>利用目的の正当性及び明確化</p>	<p>■認定基準</p> <ul style="list-style-type: none"> <li>○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</li> <li>○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</li> <li>○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</li> </ul> <p>■提出資料(例)</p> <p>【3-X】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</p>
<p>収集制限</p>	<p>■認定基準</p> <ul style="list-style-type: none"> <li>○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</li> <li>○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</li> <li>○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</li> <li>○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</li> <li>○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</li> <li>○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</li> </ul> <p>■提出資料(例)</p> <p>【3-X】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</p>
<p>データの最小化</p>	<p>■認定基準</p> <ul style="list-style-type: none"> <li>○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 <ul style="list-style-type: none"> <li>・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</li> <li>・“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を与えること</li> <li>・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</li> </ul> </li> </ul>

	<p>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</p> <ul style="list-style-type: none"> <li>・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</li> </ul> <p>■提出資料(例) 【3-X】9250「5.5 データの最小化」に対応する書類</p>
<p>利用、保持及び開示の制限</p>	<p>■認定基準</p> <ul style="list-style-type: none"> <li>○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</li> <li>○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</li> <li>○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</li> <li>○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</li> </ul> <p>(委託)</p> <ul style="list-style-type: none"> <li>○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</li> <li>○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</li> <li>○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ならないこと</li> <li>○提供する個人データの安全管理が図られるよう、委託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</li> <li>○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</li> <li>○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 <ul style="list-style-type: none"> <li>a) 委託先との責任の明確化</li> <li>b) 個人データの安全管理に関する事項</li> <li>c) 再委託に関する事項</li> </ul> </li> </ul>

- 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

○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)

○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う情報提供先と契約すること

○情報提供元との間における共同利用をしないこと○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

○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

○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

(情報提供先)

○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

○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

○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

	<p>○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</p> <p>○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</p> <ul style="list-style-type: none"> <li>a) 情報提供先との責任の明確化</li> <li>b) 個人データの安全管理に関する事項</li> <li>c) 情報提供先における委託に関する事項</li> <li>d) 個人データの取扱状況に関する報告の内容</li> <li>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</li> <li>f) 契約内容が遵守されなかった場合の措置</li> <li>g) 事件・事故が発生した場合の報告・連絡に関する事項</li> <li>h) 契約終了後の措置</li> </ul> <p>○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</p> <p>■提出資料(例)</p> <p>【3-X】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</p> <p>【3-X】15001「A.3.4.3.4 委託先の監督」に対応する書類</p> <p>【3-X】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</p> <p>【3-X】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)</p>
<p>正確性及び品質</p>	<p>■認定基準</p> <p>○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</p> <p>○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</p> <p>○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</p> <p>○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</p> <p>○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</p> <p>■提出書類(例)</p> <p>【3-X】情報提供元との契約関係書類</p>

	<p>【3-X】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</p>
<p>公開性，透明性及び通知</p>	<p>■認定基準</p> <ul style="list-style-type: none"> <li>○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</li> <li>○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</li> <li>○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</li> <li>○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</li> </ul> <p>■提出書類(例)</p> <p>【3-X】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</p> <p>【3-X】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</p> <p>【3-X】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</p>
<p>個人参加及びアクセス</p>	<ul style="list-style-type: none"> <li>○本人の識別要素が適切な保証レベルであらかじめ認証されており，適用される法令によってそのようなアクセスが禁止されていない場合には，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ようにすること</li> <li>○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</li> <li>○情報提供先には，修正，訂正又は削除を連絡すること</li> <li>○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</li> </ul> <p>■提出書類(例)</p> <p>【3-X】9250「5.9 個人参加及びアクセス」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</p> <p>【3-X】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</p>

	面のキャプチャ 【3-X】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

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	<p>■認定基準</p> <p>○「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</p> <p>■提出書類(例)</p> <p>【4-X】15001「A.3.2.2 外部向け個人情報保護方針」に対応する書類</p>
②相談体制	<p>■認定基準</p> <p>○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</p> <p>■提出書類(例)</p> <p>【4-X】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</p> <p>【4-X】15001「A.3.6 苦情及び相談への対応」に対応する書類</p>
③諮問体制	<p>■認定基準</p> <p>○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))</p> <ul style="list-style-type: none"> <li>・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</li> <li>・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い、承認する。また、当該承認に係る議事録の要旨を開示する。</li> <li>・情報提供先の選択肢及びユーザインターフェースの適切性について、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</li> </ul> <p>■提出書類(例)</p> <p>【4-X】構成員の所属、経歴、専門等を記載した書類(構成員名簿等)</p> <p>【4-X】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)</p>

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
④透明性(定期的な報告・公表)	<p>■認定基準</p> <p>○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</p> <p>■提出書類(例)</p> <p>【4-X】開示体制を示す書類</p> <p>【4-X】透明性確保を示す書類(開示項目一覧、開示先URL等)</p>
⑤認定団体との間の契約	<p>■認定基準</p> <p>○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)</p> <p>○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</p> <p>■提出書類(例)</p> <p>【4-X】認定団体との契約関係書類</p> <p>【4-X】認定マークの表示箇所を示す書類(画面キャプチャ等)</p>

## 5.5 事業内容

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
契約約款の策定	<p>■認定基準</p> <p>○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)</p> <p>■提出書類(例)</p> <p>【5-X】個人との契約関係書類  【4-X】情報提供元との契約関係書類  【1-X】情報提供先との契約関係書類  【5-X】契約約款の公表状況を示す書類(画面キャプチャ等)</p>
個人への明示及び対応	<p>■認定基準</p> <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)</p> <ul style="list-style-type: none"> <li>・「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</li> <li>・対象となる個人情報とその取得の方法、利用目的</li> <li>・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</li> <li>・「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</li> <li>・個人が相談窓口を利用するための手続</li> </ul> <p>■提出書類(例)</p> <p>【5-X】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</p>
「情報銀行」の義務について	<p>■認定基準</p> <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"> <li>・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</li> <li>・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</li> </ul>

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
	<ul style="list-style-type: none"> <li>・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</li> <li>・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</li> <li>・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</li> <li>・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)</li> <li>・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</li> <li>・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</li> </ul> <p>(提供先第三者との関係)</p> <ul style="list-style-type: none"> <li>・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</li> <li>・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</li> <li>・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</li> <li>・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</li> </ul> <p>■提出書類(例)</p> <p>【5-X】個人との契約関係書類</p> <p>【1-X】情報提供先との契約関係書類</p>

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
<p>個人のコントロールABILITYを確保するための機能について</p>	<p><b>【認定基準】</b></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"> <li>・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。)</li> <li>・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(操作が容易なダッシュボードなど)を提供すること</li> <li>・選択肢及びユーザ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</li> <li>・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</li> </ul> <p>②「情報銀行」に委任した個人情報の提供履歴の閲覧(トレーサビリティ)</p> <ul style="list-style-type: none"> <li>・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を提供すること</li> <li>・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</li> </ul> <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"> <li>・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</li> </ul> <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"> <li>・簡易迅速で本人の負担のないユーザ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(※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。)</li> </ul>

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
	<p>・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</p> <p>■提出資料(例) 【6-X】上記①から④の機能の提供を示す書類(Web モック画面のキャプチャ、イメージ図等)</p>
責任の範囲について	<p>■認定基準</p> <ul style="list-style-type: none"> <li>○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</li> <li>○「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こと</li> <li>○「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</li> <li>○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</li> </ul> <p>■提出資料(例)</p> <p>【6-X】15001「A.3.3.2 法令、国が定める指針その他の規範」、15001「A.3.6 苦情及び相談への対応」に対応する書類</p> <p>【5-X】個人との契約関係書類</p> <p>【1-X】情報提供先との契約関係書類</p>

【提出書類一覧】

No	提出書類
【1-X】	事業者の登記簿謄本
【1-X】	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)
【1-X】	損害保険証書(ない場合は、【1-X】の提出書類)
【1-X】	「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(関連行政機関への届出、許認可等)
【1-X】	15001「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-X】	プライバシーマーク又はISMS認証の取得を示す書類(これらが無い場合は、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)
【1-X】	情報提供先との契約関係書類
【1-X】	当該サービス事業の内容と範囲を示す書類
【2-X】	27001「5.2 方針」、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」及び 27001「6.1 リスク及び機会に対処する活動」に対応する書類
【2-X】	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
【2-X】	【2-X】27001「5.2 方針」及び 27002「5 情報セキュリティのための方針群」に対応する書類
【2-X】	27001「5.3 組織の役割、責任及び権限」に対応する書類
【2-X】	加盟団体名及び活動概要を示す書類
【2-X】	27001「7.2 力量」に対応する書類
【2-X】	情報セキュリティに関する教育の実施サマリー
【2-X】	27002「8.1.1 資産目録」、27002「8.1.2 資産の管理責任」、27002「8.3.2 媒体の処分」及び 27002「8.2 情報の分類」に対応する書類
【2-X】	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-X】	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
【2-X】	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)
【2-X】	27002「9 アクセス制御」及び 27002「10 暗号」に対応する書類
【2-X】	27002「11 物理的及び環境的セキュリティ」に対応する書類
【2-X】	27002「12.2.1 操作手順書」、27002「12.2 マルウェアからの保護」、27002「12.4 ログ取得及び監視」及び 27002「12.6 技術的ぜい弱性管理」に対応する書類
【2-X】	27002「13.1.1 ネットワーク管理策」、27002「13.1.2 ネットワークサービスのセキュリティ」、27002「13.1.3 ネットワークの分離」及び 27002「13.2 情報の転送」に対応する書類
【2-X】	27002「15 供給者関係」に対応する書類
【2-X】	27002「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-X】	システムに対する脆弱性診断の実施内容を示す書類
【2-X】	27002「18.1 法的及び契約上の要求事項の順守」及び 27002「18.2 情報セキュリティのレビュー」に対応する書類
【3-X】	15001「A.3.2.2 外部向け個人情報保護方針」に対応する書類
【3-X】	15001「A.3.3.4 資源、役割、責任及び権限」、15001「A.3.3.5 内部規定」、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」に対応する書類
【3-X】	15001「7.3 認識」及び 15001「A.3.4.5 認識」に対応する書類
【3-X】	プライバシー保護に関する教育実施サマリー
【3-X】	15001「C.11 物理的及び環境的セキュリティ」に対応する書類
【3-X】	15001「C.9 アクセス制御」に対応する書類
【3-X】	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-X】	情報提供元との契約関係書類
【3-X】	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「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」、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
【3-X】	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
【3-X】	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
【3-X】	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-X】	15001「A.3.4.3.4 委託先の監督」に対応する書類
【3-X】	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-X】	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-X】	情報提供元との契約関係書類
【3-X】	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
【3-X】	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-X】	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-X】	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
【3-X】	9250「5.9 個人参加及びアクセス」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

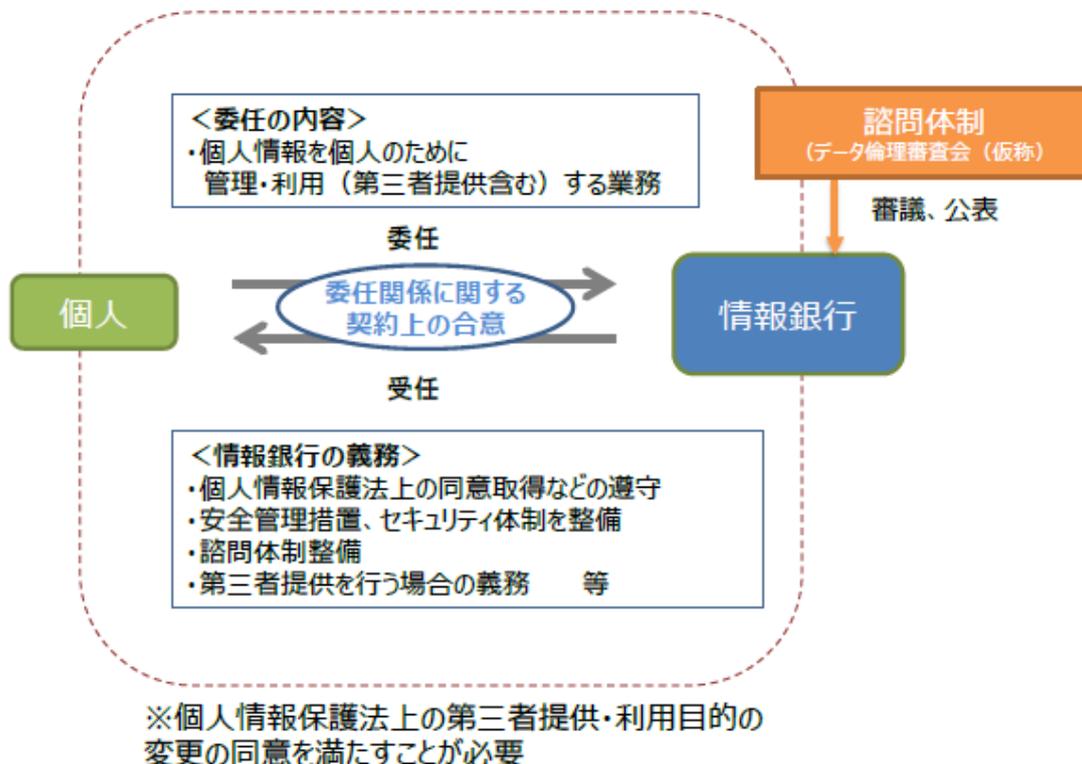
【3-X】	本人が自分の個人データにアクセス及び確認することができる画面のキャプチャ
【3-X】	情報提供先への修正, 訂正又は削除を連絡する手順に対応する書類
【4-X】	苦情相談窓口が示されているHPなどの表示内容を示す書類
【4-X】	15001「A.3.6 苦情及び相談への対応」に対応する書類
【4-X】	構成員の所属、経歴、専門等を記載した書類(構成員名簿等)
【4-X】	設置の目的・審議事項等を規定した書類(設置要綱、設置規則等)
【4-X】	開示体制を示す書類
【4-X】	透明性確保を示す書類(開示項目一覧、開示先URL等)
【4-X】	認定団体との契約関係書類
【4-X】	認定マークの表示箇所を示す書類(画面キャプチャ等)
【5-X】	個人との契約関係書類
【5-X】	契約約款の公表状況を示す書類(画面キャプチャ等)
【5-X】	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-X】	個人との契約関係書類
【6-1】	15001「A.3.3.2 法令、国が定める指針その他の規範」、15001「A.3.6 苦情及び相談への対応」に対応する書類
【7-4】	情報銀行と個人との間の契約約款
【7-5】	情報銀行と情報提供先との間の契約約款
【7-6】	情報銀行と情報提供元との間の契約約款
【8-1】	上記①から④の機能が提供されることがわかる資料、Web モック画面のキャプチャ、イメージ図などの提供

## 6 モデル約款

### 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 ver1.0 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ル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。



【出典】指針 ver1.0

## 6.2 モデル約款

IT連盟において、前述 6.1 の整理及び指針 ver1.0 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。

### <参考>指針 ver1.0 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」「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に配慮すること)

##### 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(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