■「情報銀行」認定審査サーベイランスチェックシート（ver.2.01）

「情報銀行」認定審査チェックシート（Ver.2.01） より抜粋加筆修正

一般社団法人 日本IT団体連盟 情報銀行推進委員会
2021年2月1日制定 2021年7月1日改訂

項目	「情報銀行」認定申請ガイドブック ver.2.01 （2021年7月1日改訂）			確認方法（引用： JIS Q 15001:2017, JIS Q 27001 :2014, JIS X 9250:2017）	認定基準に対応する 申請者の書類、規定類の名称と項番
	項目	認定基準	提出書類		
5.2 情報セキュリティ・プライバシー					
43	5.2.2⑪ 通信の情報セキュリティ	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）	【2-16】27001「A.13.2 情報の転送」に記載されている措置を講じていることが確認できる書類	以下に関する規定及び実施記録を確認（規定の内容、承認印、制定日、改定日を確認） ・(A.13.2.1)あらゆる形式の通信設備を利用した情報転送を保護するために，正式な転送方針，手順及び管理策を備えなければならない。 ・(A.13.2.3)電子的メッセージ通信に含まれた情報は，適切に保護しなければならない。	
44		提供元から個人データ受領するサーバ又はパソコンを特定し、それ以外のサーバ又はパソコン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 ※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。	【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	当該技術的対策を示す書類及び実施記録を確認	
45		提供先が個人データの提供を受けるサーバ又はパソコンを特定し、それ以外のサーバ又はパソコンで受領できないようにする技術的対策（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 ※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。	【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	当該技術的対策を示す書類及び実施記録を確認	
52	5.2.2⑭ 情報セキュリティインシデント管理	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	【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	・システムに対する脆弱性診断の実施及び実施記録を確認 ・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の規定を確認	

■「情報銀行」認定審査サーベイランスチェックシート（ver.2.01）

「情報銀行」認定審査チェックシート（Ver.2.01） より抜粋加筆修正

一般社団法人 日本IT団体連盟 情報銀行推進委員会
2021年2月1日制定 2021年7月1日改訂

項目	「情報銀行」認定申請ガイドブック ver.2.01 （2021年7月1日改訂） 項目	認定基準	提出書類	確認方法（引用： JIS Q 15001:2017, JIS Q 27001 :2014, JIS X 9250:2017）	認定基準に対応する申請者の書類、規定類の名称と項番
5.3 プライバシー保護対策					
67	5.3.2⑥ 同意及び選択	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。	【3-7】同意の取得の際に本人に示す書類（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】本人への説明文が個人情報保護法の「明示」条件を満たしていることを確認できる書類（画面遷移図）	個人情報の取扱いに関する本人への説明文書と同意の順序を確認 ※「同意の順序」とは、本人への説明文が個人情報保護法の「明示」条件を満たしていることを確認できること。 また説明文は、項目52 の「消費者向けオンラインサービスにおける通知と同意・選択に関するガイドライン」を考慮のこと。 「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	
70	5.3.2⑥ 同意及び選択（2）	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。	【3-9】15001「A.3.4.2.4 個人情報を取得した場合の措置」に記載されている措置を講じていることが確認できる書類	以下に関する規定及び実施記録を確認（規定の承認印、制定日、改定日を確認） ・A.3.4.2.4 個人情報を取得した場合の措置 ①個人情報を取得する場合、個人情報の取得の場面に応じて、あらかじめ，その利用目的を公表している，又は取得後速やかにその利用目的を本人に通知又は公表していること。 ・通知又は公表の記録 ②本人への利用目的の通知又は公表を要しないのは，a)～d)の場合に限定していること。 a)利用目的を本人に通知するか，又は公表することによって本人又は第三者の生命，身体，財産その他の権利利益を害するおそれがある場合 b)利用目的を本人に通知するか，又は公表することによって当該組織の権利又は正当な利益を害するおそれがある場合 c)国の機関又は地方公共団体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，利用目的を本人に通知するか，又は公表することによって当該事務の遂行に支障を及ぼすおそれがある場合 d)取得の状況からみて利用目的が明らかであると認められる場合 ・本人に通知又は公表せずに取得した個人情報が有る場合，A.3.4.2.4のただし書きに該当することの記録	
71			【3-9】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」に記載されている措置を講じていることが確認できる書類	以下に関する規定及び実施記録を確認（規定の承認印、制定日、改定日を確認） 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 ・本人に明示した書面 ・個人情報の特定に関する記録 ・本人に明示し，本人の同意を得ずに取得した個人情報が有る場合，当該A.3.4.2.5のただし書きに該当することの説明 A.3.4.2.4ただし書きとは 人の生命，身体若しくは財産の保護のために緊急に必要がある場合，又はただし書きA.3.4.2.4のa)～d)のいずれかに該当する場合は，本人に明示し，本人の同意を得ることを要しない。 ・本人に明示した書面(A.3.4.2.5) ・個人情報の特定に関する記録(A.3.5.3a)) ・本人に明示し，本人の同意を得ずに取得した個人情報が有る場合，当該A.3.4.2.5のただし書きに該当することの記録	
72			【3-9】15001「A.3.4.2.7 本人に連絡又は接触する場合の措置」に記載されている措置を講じていることが確認できる書類	以下に関する規定及び実施記録を確認（規定の承認印、制定日、改定日を確認） ・A.3.4.2.7 本人に連絡又は接触する場合の措置 ①個人情報を利用して本人に連絡又は接触する場合には，本人に対して，A.3.4.2.5のa)～f)に示す事項又はそれと同等以上の内容の事項，及び取得方法を通知し，本人の同意を得ていること。 ②本人に通知し，本人の同意を得ることを要しない場合は，a)～f)の場合に限定していること。 ③共同して利用する者から個人情報を取得する場合であって，共同して利用する者がA.3.4.2.7d)の措置を講じない場合，本人に対して，A.3.4.2.5のa)～f)に示す事項又はそれと同等以上の内容の事項，及び取得方法を通知し，本人の同意を得ていること。 ・本人への通知書面(A.3.4.2.7) ・本人の同意書面 ・個人情報の特定に関する記録(A.3.5.3a)) ・同意を得ずに本人に連絡又は接触している場合，当該連絡又は接触がA.3.4.2.7のただし書きに該当することの記録	

■「情報銀行」認定審査サーベイランスチェックシート（ver.2.01）

「情報銀行」認定審査チェックシート（Ver.2.01） より抜粋加筆修正

一般社団法人 日本IT団体連盟 情報銀行推進委員会

2021年2月1日制定 2021年7月1日改訂

項目	「情報銀行」認定申請ガイドブック ver.2.01 （2021年7月1日改訂）			確認方法（引用： JIS Q 15001:2017, JIS Q 27001 :2014, JIS X 9250:2017）	認定基準に対応する 申請者の書類、規定類の名称と項番
	項目	認定基準	提出書類		
73			【3-9】15001「A.3.4.2.8 個人データの提供に関する措置」に記載されている措置を講じていることが確認できる書類	以下に関する規定及び実施記録を確認（規定の承認印、制定日、改定日を確認） ・A.3.4.2.8 個人データの提供に関する措置 ①個人データを第三者に提供する場合には，あらかじめ，本人に対して，A.3.4.2.5のa)～d)に示す事項又はそれと同等以上の内容の事項，及び取得方法を通知し，本人の同意を得ていること。 ②本人に通知し，本人の同意を得ることを要しない場合は，a)～g)の場合に限定していること。 ③個人データを共同利用している場合，共同して利用する者の間で，A.3.4.2.7に規定する共同利用について契約によって定めていること。 ・本人への通知書面(A.3.4.2.8) ・本人の同意書面 ・個人情報の特定に関する記録(A.3.5.3a)) ・同意を得ずに第三者に提供している場合，当該提供がA.3.4.2.8のただし書きに該当することの説明 ・共同利用についての契約(A.3.4.2.8f))	
75		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	【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）	同意の取得画面を確認	

■「情報銀行」認定審査サーベイランスチェックシート（ver.2.01）

「情報銀行」認定審査チェックシート（Ver.2.01） より抜粋加筆修正

一般社団法人 日本IT団体連盟 情報銀行推進委員会
2021年2月1日制定 2021年7月1日改訂

項目	「情報銀行」認定申請ガイドブック ver.2.01 （2021年7月1日改訂）			確認方法（引用： JIS Q 15001:2017, JIS Q 27001 :2014, JIS X 9250:2017）	認定基準に対応する申請者の書類、規定類の名称と項番
	項目	認定基準	提出書類		
87	5.3.2⑨ データの最小化	・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	【3-12】9250「5.5 データの最小化」に記載されている措置を講じていることが確認できる書類	以下に関する規定及び実施記録を確認（規定の承認印、制定日、改定日を確認） ・利用期限を過ぎたら個人データを確実に廃棄または匿名化することの規定を確認。 ※「利用期限を過ぎたら個人データを確実に廃棄または匿名化することの規定を確認。」は、JIS X 9250 による要求事項である。JIS Q 15001 では、利用期限を過ぎた個人データの廃棄は努力義務であるが、JIS X 9250 では必須である	
95	5.3.2⑩ 利用，保持及び開示の制限（2）	（委託） 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	【3-14】15001「A.3.4.3.4 委託先の監督」に記載されている措置を講じていることが確認できる書類	以下に関する規定及び実施記録を確認（規定の承認印、制定日、改定日を確認） ・委託先選定基準に基づいて委託先を評価した結果、委託する業務のリスク対策として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するための規定を確認及び評価した結果を確認 ・委託先一覧を確認 ・委託先選定基準、評価結果の書類を確認	
97		（委託） 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	【3-14】15001「A.3.4.3.4 委託先の監督」に記載されている措置を講じていることが確認できる書類	委託先の契約書（または、雛形）の項目を確認 委託先点検結果を確認	
104	5.3.2⑩ 利用，保持及び開示の制限（4）	（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	【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	提供先の利用目的に関する公開または明示に関する文書及び説明画面を確認 情報提供先との契約に、該当項目が規定されていることを確認	
105		（情報提供先） 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（※） 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。	【3-14】15001「A.3.4.3.2 安全管理措置」に記載されている措置を講じていることが確認できる書類	提供先選定基準及び選定結果を確認	
106		（情報提供先） 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	【3-14】15001「A.3.4.3.2 安全管理措置」に記載されている措置を講じていることが確認できる書類	提供先選定基準に基づいて提供先を評価した結果、提供する業務のリスク対策として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するための規定及び実施記録を確認 提供先一覧及び選定基準、評価結果の書類を確認 ※情報銀行認定審査チェックシートVer2.01項目94と同じ観点で行うこと	
107	5.3.2⑩ 利用，保持及び開示の制限（5）	（情報提供先） 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	【3-14】15001「A.3.4.3.2 安全管理措置」に記載されている措置を講じていることが確認できる書類	提供先の監督に関する規定 監督実施記録を確認	

■「情報銀行」認定審査サーベイランスチェックシート（ver.2.01）

「情報銀行」認定審査チェックシート（Ver.2.01） より抜粋加筆修正

一般社団法人 日本IT団体連盟 情報銀行推進委員会
2021年2月1日制定 2021年7月1日改訂

項目	「情報銀行」認定申請ガイドブック ver.2.01 （2021年7月1日改訂）			確認方法（引用： JIS Q 15001:2017, JIS Q 27001 :2014, JIS X 9250:2017）	認定基準に対応する 申請者の書類、規定類の名称と項番
	項目	認定基準	提出書類		
5.4 ガバナンス体制					
125	5.4.1② 相談体制	個人や事業者から、電話や電子メール等による問い合わせ、連絡、相談等を受け付けるための窓口を設けており、相談があった場合の対応プロセスを定めていること	【4-2】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」に記載されている措置を講じていることが確認できる書類	以下に関する規定及び実施記録を確認（規定の承認印、制定日、改定日を確認） ①個人情報の取扱い及び個人情報保護マネジメントシステムに関して，本人からの苦情及び相談を受け付けて，適切かつ迅速な対応を行う手順が内部規程として文書化されていること。 ②苦情及び相談への対応を実施していること ③苦情の申立て先が，本人にとって明確であること。 ④認定個人情報保護団体の対象事業者となっている場合は，当該団体の苦情解決の申し出先も明示していること。 ⑤本人からの苦情及び相談を受け付けて，適切かつ迅速な対応を行うための体制の整備を行っていること。	
126	5.4.1③ 諮問体制[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 ） ・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 ※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）	【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） （データ倫理審査会運用ガイドラインを参照すること）	・構成員の所属、経歴、専門等を記載した書類（構成員名簿等） ・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） を確認	
127		・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。	【4-5】データ倫理審査会で何を審査するかの規定（左記事項を規定した書類） （データ倫理審査会運用ガイドラインを参照すること）	・データ倫理審査会からの助言と助言に対する対応方法（リスク対策、リスク受容）を確認 ・データ倫理審査会からの助言をリスク受容する場合は、その理由を確認 ※データ倫理審査会の審査項目は、少なくとも以下の項目を含めている必要がある。 ・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い、承認する。 ・当該承認に係る議事録の要旨を開示する。	
128		・構成員及び（必要な範囲の）議事録を公開する（※1、※2）。 ※1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。 ※2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。	【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を参照すること）	・データ倫理審査会　議事録を確認 ・データ倫理審査会からの助言と助言に対する対応方法（リスク対策、リスク受容）を確認 ・データ倫理審査会からの助言をリスク受容する場合は、その理由を確認 ※データ倫理審査会の審査項目は、少なくとも以下の項目を含めている必要がある。 ・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い、承認する。 ・当該承認に係る議事録の要旨を開示する。	

■「情報銀行」認定審査サーベイランスチェックシート（ver.2.01）

「情報銀行」認定審査チェックシート（Ver.2.01） より抜粋加筆修正

一般社団法人 日本IT団体連盟 情報銀行推進委員会
2021年2月1日制定 2021年7月1日改訂

項目	「情報銀行」認定申請ガイドブック ver.2.01 （2021年7月1日改訂）			確認方法（引用： JIS Q 15001:2017, JIS Q 27001 :2014, JIS X 9250:2017）	認定基準に対応する 申請者の書類、規定類の名称と項番
	項目	認定基準	提出書類		
129	5.4.1③ 諮問体制[設置](2)	・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。	【4-5】データ倫理審査会で何を審査するかの規定（左記事項を規定した書類） 【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を参照すること）	・データ倫理審査会からの助言と助言に対する対応方法（リスク対策、リスク受容）を確認 ・データ倫理審査会からの助言をリスク受容する場合は、その理由を確認 ※データ倫理審査会の審査項目は、少なくとも以下の項目を含めている必要がある。 ・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い、承認する。 ・当該承認に係る議事録の要旨を開示する。	
130		・「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 ※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	【4-5】データ倫理審査会で何を審査するかの規定（左記事項を規定した書類） （データ倫理審査会運用ガイドラインを参照すること）	・「情報銀行」は定期的に諮問体制に報告を行う。 ・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。	
131	5.4.1③ 諮問体制[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）	【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（左記事項を審議した議事録） （データ倫理審査会運用ガイドラインを参照すること）	・データ倫理審査会　議事録を確認 ・データ倫理審査会からの助言と助言に対する対応方法（リスク対策、リスク受容）を確認 ・データ倫理審査会からの助言をリスク受容する場合は、その理由を確認 ※データ倫理審査会の審査項目は、少なくとも以下の項目を含めている必要がある。 ・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い、承認する。 ・当該承認に係る議事録の要旨を開示する。 ・「情報銀行」は定期的に諮問体制に報告を行う。 ・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。	
132		・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）	【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（左記事項を審議した議事録） （データ倫理審査会運用ガイドラインを参照すること）	・データ倫理審査会　議事録を確認 ・データ倫理審査会からの助言と助言に対する対応方法（リスク対策、リスク受容）を確認 ・データ倫理審査会からの助言をリスク受容する場合は、その理由を確認 ※データ倫理審査会の審査項目は、少なくとも以下の項目を含めている必要がある。 ・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い、承認する。 ・当該承認に係る議事録の要旨を開示する。 ・「情報銀行」は定期的に諮問体制に報告を行う。 ・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。	
133		・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 −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	【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（左記事項を審議した議事録） （データ倫理審査会運用ガイドラインを参照すること）	・データ倫理審査会　議事録を確認 ・データ倫理審査会からの助言と助言に対する対応方法（リスク対策、リスク受容）を確認 ・データ倫理審査会からの助言をリスク受容する場合は、その理由を確認 ※データ倫理審査会の審査項目は、少なくとも以下の項目を含めている必要がある。 ・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い、承認する。 ・当該承認に係る議事録の要旨を開示する。 ・「情報銀行」は定期的に諮問体制に報告を行う。 ・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。	
134		・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	【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を参照すること）	・構成員の所属、経歴、専門等を記載した書類（構成員名簿等） ・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） を確認 ・データ倫理審査会　議事録を確認 ・データ倫理審査会からの助言と助言に対する対応方法（リスク対策、リスク受容）を確認 ・データ倫理審査会からの助言をリスク受容する場合は、その理由を確認 ※データ倫理審査会の審査項目は、少なくとも以下の項目を含めている必要がある。 ・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い、承認する。 ・当該承認に係る議事録の要旨を開示する。 ・「情報銀行」は定期的に諮問体制に報告を行う。 ・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。	

■「情報銀行」認定審査サーベイランスチェックシート（ver.2.01）

「情報銀行」認定審査チェックシート（Ver.2.01） より抜粋加筆修正

一般社団法人 日本IT団体連盟 情報銀行推進委員会

2021年2月1日制定　2021年7月1日改訂

項目	「情報銀行」認定申請ガイドブック ver.2.01 （2021年7月1日改訂）			確認方法（引用： JIS Q 15001:2017, JIS Q 27001 :2014, JIS X 9250:2017）	認定基準に対応する 申請者の書類、規定類の名称と項番
	項目	認定基準	提出書類		
135	5.4.1③ 諮問体制[実施](2)	・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	【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（左記事項を審議した議事録） （データ倫理審査会運用ガイドラインを参照すること）	・データ倫理審査会　議事録を確認 ・データ倫理審査会からの助言と助言に対する対応方法（リスク対策、リスク受容）を確認 ・データ倫理審査会からの助言をリスク受容する場合は、その理由を確認 ※データ倫理審査会の審査項目は、少なくとも以下の項目を含めている必要がある。 ・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い、承認する。 ・当該承認に係る議事録の要旨を開示する。 ・「情報銀行」は定期的に諮問体制に報告を行う。 ・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。	

■「情報銀行」認定審査サーベイランスチェックシート（ver.2.01）

「情報銀行」認定審査チェックシート（Ver.2.01） より抜粋加筆修正

一般社団法人 日本IT団体連盟 情報銀行推進委員会
2021年2月1日制定 2021年7月1日改訂

項目	「情報銀行」認定申請ガイドブック ver.2.01 （2021年7月1日改訂） 項目	認定基準	提出書類	確認方法（引用： JIS Q 15001:2017, JIS Q 27001 :2014, JIS X 9250:2017）	認定基準に対応する申請者の書類、規定類の名称と項番
5.5 事業内容					
140	5.5.1① 契約約款の策定	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）	【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）	・個人との約款の公開を確認できる画面確認 ・情報提供元及び情報提供先との契約を確認	
144	5.5.1④ 個人のコントローラビリティを確保するための機能について	①「情報銀行」に委任した個人情報の第三者提供に係る条件の指定及び変更 ・提供先・利用目的・データ範囲について、個人が選択できる選択肢を用意すること(※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 ・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 ・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	【6-1】機能の提供を示す書類（実サービスの画面のキャプチャ等）（左記事項を示すこと）	当該機能の提供を示す書類（実サービスの画面のキャプチャ等）を確認	
145		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	【6-1】機能の提供を示す書類（実サービスの画面のキャプチャ等）（左記事項を示すこと）	当該機能の提供を示す書類（実サービスの画面のキャプチャ等）を確認	
146		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	【6-1】機能の提供を示す書類（実サービスの画面のキャプチャ等）（左記事項を示すこと）	当該機能の提供を示す書類（実サービスの画面のキャプチャ等）を確認	
147		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	【6-1】機能の提供を示す書類（実サービスの画面のキャプチャ等）（左記事項を示すこと）	当該機能の提供を示す書類（実サービスの画面のキャプチャ等）を確認	
※	継続的改善事項・留意事項への対応状況（別紙）			直近の認定付与に係る審査で指摘した継続的改善事項・留意事項への確認（別紙）	

※一般財団法人日本情報経済社会推進協会（JIPDEC）の「プライバシーマーク付与適格性審査基準」を一部引用

■「情報銀行」認定審査チェックシート（Ver1.0）

審査チェックシートの記入例

一般社団法人 日本IT団体連盟 情報銀行推進委員会

2019年7月1日策定

項目	「情報銀行」認定申請ガイドブック ver 1.0			確認方法（引用： JIS Q 15001:2017, JIS Q 27001 :2014, JIS X 9250:2017）	認定基準に対応する申請者の書類、規定類の名称と項番
	項目	認定基準	提出書類		
5.1 事業者の適格性					
1	経営面の要件	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）	【1-1】事業者の登記簿謄本	国内に活動拠点を持つ法人格であることを確認 ・法人の名称、事業概要、所在地、法人番号な	01_現在事項全部証明書
2		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、債務超過がないこと）等	【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）	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）等確認	02_第2期計算書類（201403） 02_第3期計算書類（201503） 02_第4期計算書類（201603） 02_第5期計算書類（201703） 02_第6期計算書類（201803）
3		損害賠償請求があった場合に対応できる能力があること （例）一定の資産規模がある、賠償責任保険に加入している 等	【1-3】損害保険証書（ない場合は、賠償責任に関する説明資料）	賠償責任に関する説明としては、賠償額の算定根拠と資金計画の整合性を確認	03_損害賠償に関する説明資料
4	業務能力など	個人情報保護法を含む必要となる法令を遵守していること	【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	「特定した関連法令の一覧表」を確認 項目51,52の確認方法で確認	04_特定した関連法令の一覧表
			・・・・・・・・		
12	情報セキュリティマネジメントの運用・監視・レビュー	情報セキュリティマネジメントに必要な人・資源・資産・システムなど準備、割り当て、確定すること	【2-2】27001「5.3 組織の役割、責任及び権限」、27001「7 支援」	以下に関する規定を確認（規定の内容、承認印、制定日、改定日を確認） ・情報セキュリティの役割及び責任に関する規	【2-1】ISMSマニュアル 5.3 組織の役割、責任及び権限 7 支援
13		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	【2-3】27001「6.1.2 情報セキュリティリスクアセスメント」	以下に関する規定を確認（規定の内容、承認 ・リスクアセスメント及びリスク対策に関する規 ・定期的及び適宜に実施することの定め ・リスクを洗い出しに漏れがおきないよう規定し するなど） ・リスク対策として定めたルールは、残留リスクを	【2-1】ISMSマニュアル 6.1.2 情報セキュリティリスクアセスメント
14			【2-2】27001「9.2 内部監査」	以下に関する規定を確認（規定の内容、承認印、制定日、改定日を確認） ・情報セキュリティの内部監査に関する規定 ・継続的改善に関する規定	【2-1】ISMSマニュアル 9.2 内部監査
15			【2-2】27001「10.2 継続的改善」に対応する書類	以下に関する規定を確認（規定の内容、承認印、制定日、改定日を確認） ・情報セキュリティの内部監査に関する規定 ・継続的改善に関する規定	【2-1】ISMSマニュアル 10.2 継続的改善

該当する書類のファイル名を記入する

ファイルの中の何章に記載されいているかを記載する

※一般財団法人日本情報経済社会推進協会（JIPDEC）の「プライバシーマーク付与適格性審査基準」を一部引用