■「情報銀行」認定審査サーベイランスチェックシート（ver.1.01）

「情報銀行」認定審査チェックシート（ver.1.3） 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 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		
5.2 情報セキュリティ等					
42	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「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及び実施記録	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） ・(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。 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、本人は知っているが、本人以外が知らないことが保証されない。 ・(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。	
49	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	
5.3 プライバシー保護対策等					
64	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、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）	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。	
67	同意及び選択	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	【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及び実施記録	以下に関する規定を確認（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	
69	同意及び選択	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	
84	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及び実施記録	以下に関する規定を確認（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すが、JIS X 9250 では必須である	

■「情報銀行」認定審査サーベイランスチェックシート（ver.1.01）

「情報銀行」認定審査チェックシート（ver.1.3） 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 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		
91	利用，保持及び開示の制限	（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及び実施記録	以下に関する規定を確認（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	
93	利用，保持及び開示の制限	（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	
100	利用，保持及び開示の制限	（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）	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	
101	利用，保持及び開示の制限	（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	【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	提供先選定基準を確認及び選定結果を確認 ・第三者認証を取得していること（プライバシーマークまたは、ISMS、等） 情報銀行は、提供先がPマークまたはISMS認証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、個人情報の暗号化処理または個人情報の一部の置き換え等の処理を行い、復元に必要な情報を除いた形で提供先に提供する ・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。	
102	利用，保持及び開示の制限	（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を確認 提供先一覧及び選定基準、評価結果の書類を確認 ※項目90と同じ観点で行うこと	
103	利用，保持及び開示の制限	（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を確認 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.1.01）

「情報銀行」認定審査チェックシート（ver.1.3） 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 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		
5.4 ガバナンス体制					
120	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及び実施記録	以下に関する規定を確認（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。	
121	諮問体制	以下を満たす、社外委員を含む諮問体制を設置していること（データ倫理審査会（仮称）） ・構成員の構成例：エンジニア（データ解析や集積技術など）、セキュリティの専門家、法律実務家、データ倫理の専門家、消費者等多様な視点でのチェックを可能とする多様な主体の参加 ・データ利用に関する契約や利用方法、提供先第三者などについて適切性を審議し、必要に応じて助言を行い、承認する。また、当該承認に係る議事録の要旨を開示する。 ・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。 ・「情報銀行」は定期的に諮問体制に報告を行うこと、諮問体制は、必要に応じて「情報銀行」に調査・報告を求めることができる、「情報銀行」は当該求めに応じて、適切に対応すること	【4-4】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） ※規程に基づき審査したデータ倫理審査会の実施記録及び議事を確認 （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.1.01）

「情報銀行」認定審査チェックシート（ver.1.3） 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 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		
5.5 事業内容					
125	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	
129	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	「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（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）	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）	
130	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	「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）	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）	
131	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	「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）	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）	
132	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	「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	【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）	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）	
※	継続的改善事項・留意事項への確認（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