資料3－3

第3回情報信託機能の認定スキームの在り方に関する検討会

論点整理（案）について

（認定基準案、モデル約款案）

2018/2/23

検討会　事務局

認定基準　基本原則（案）

【「認定」に関する基本原則】

○ 消費者を起点とした、民間団体等による「任意の認定制度」（社会的な仕組み）。
　事業を行うために認定が必須とはならない。
○ 消費者に向けた認定基準。一定の要件を満たす者を認定するもので、レベル分けは想定しない。
　データの信頼性、ビジネス競争領域は含まない。

＜経営面／セキュリティ面の要件案＞
①事業主体の経営的安定性が担保されている
②事業実施や、個人情報取り扱いの知識・経験があり社会的信用がある
③データセンター・セキュリティ体制の保有、セキュリティ対策の実施、セキュリティ対策団体への参加

＜ガバナンス体制＞
①「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」という趣旨を実現するための、ガバナンス体制の構築
②相談体制の設置（例 「データ倫理審査委員会」の設置（社内外委員））

＜情報銀行に求められる義務＞
情報銀行による公正な事業運営を確保するために求められる善管注意義務、忠実性、公平性など

認定基準　具体的基準（案）

１）事業者の適格性

項目	内容
①経営面の要件	・法人格を持つこと
	・業務を健全に遂行するに足りる財産的基礎を有していること
	・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（又は賠償責任保険に加入するなど担保すること）
②業務能力など	・データや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、社会的信用を有していること（実施体制が整っていること）
	・プライバシーポリシーが策定されていること
	・認定団体が定めるモデル約款に準じた契約約款を作成・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）
	・情報提供先の管理体制などを把握できること
	・個人にわかりやすい説明、形式などにつとめること
	・法令を遵守すること
③機能の明示について	・個人が、自らの情報の利用履歴を閲覧、コントロールできる機能（例：データポータビリティ機能）の有無を明示すること
	・約款に違反した場合や、提供先第三者に起因して個人に損害が発生した場合の損害賠償責任に関する事項を明示すること

2）セキュリティ基準 十分なデータを管理するセキュリティ体制や施設を確保できるよう、下記基準を満たすこと

項目	内容
①運用基準（人的体制や遵守ルールなど）	・セキュリティ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、データ量が増加した場合でも十分な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 （十分なセキュリティ対策の例） ・外部アタックテストなどの定期的セキュリティチェックを実施すること ・セキュリティ対策のための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 ・セキュリティ情報を収集・交換するための制度的枠組みに加盟すること
	・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、個人情報の取り扱いについて、Pマークなど必要となる事項を担保していること
	・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）又は以下の基準を満たしていること（又は、中小企業における組織的な情報セキュリティガイドラインを遵守していること）
	・個人情報を扱う担当者が明確であること、扱う場合の認証基準、アクセス制限などが整備されていること
	・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
	・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
	・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

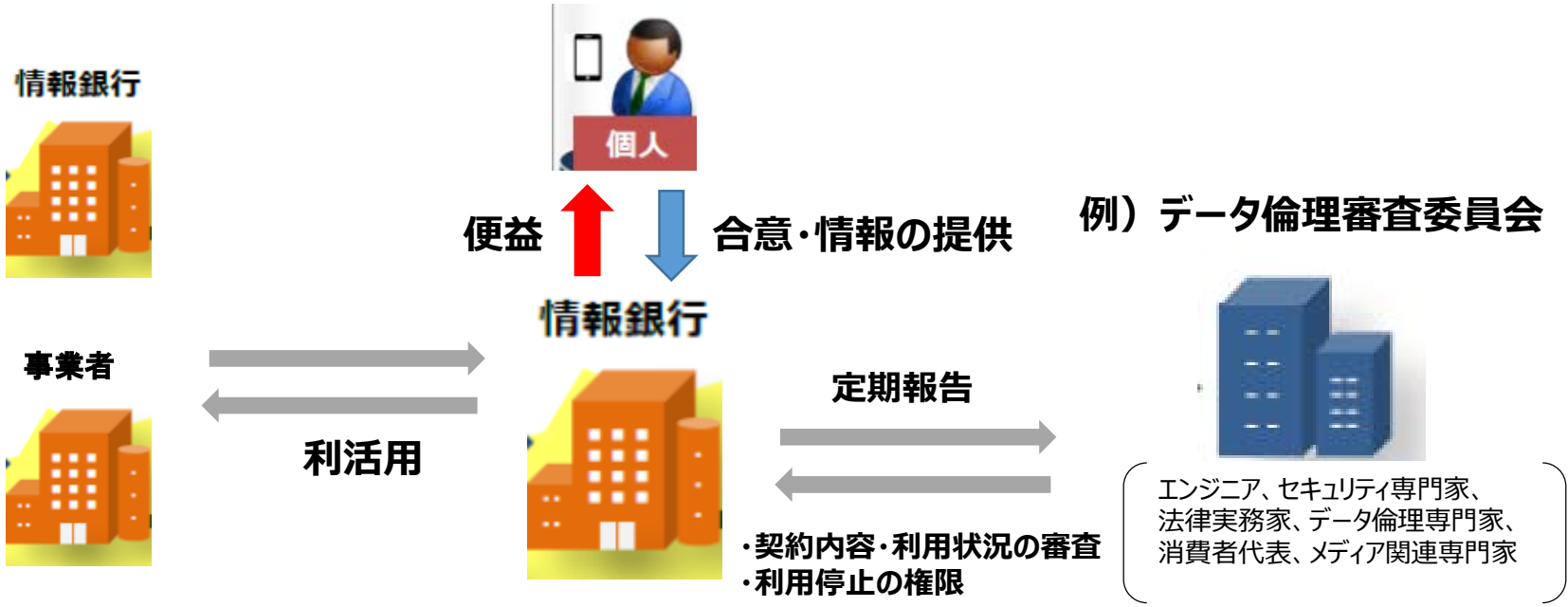
2）セキュリティ基準（つづき）

項目	内容
②技術基準（施設・設備などの基準）	・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
	・データセンターへの入室管理、情報を扱う区域の管理、定期的な検査を行うこと
	・情報を取り扱う機器等かデータを削除・廃棄した場合には責任者が確認すること
	・情報を取り扱う機器等のソフトウェア、ハードウェアなど最新の状態に保持すること、セキュリティ対策ソフトウェアなどを導入すること
	・ログ等の定期的分析により、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
	・通信経路又は内容の暗号化などの対応を行うこと

３）ガバナンス体制

項目	内容
①基本理念	「データは、個人がその成果を享受し、個人の豊かな生活実現のために使うこと」の趣旨を企業理念に活用し、その理念の実現のためのガバナンス体制の構築を定め経営責任を明確化していること
②相談体制	・個人や事業者から、電話や電子メール等による問い合わせ、連絡、相談等を受け付けるための窓口を設けること
③第三者委員会（監査委員会）	以下を満たす相談体制を設置していること（例「データ倫理審査委員会」） ・データ解析を専門とするエンジニア、集積技術を専門とするエンジニア、セキュリティの専門家、法律実務家、データ倫理の専門化、消費者代表、メディア関連の専門家を構成員に含む ・データ利用に関する契約や利用方法などについて適切性を審議する
④透明性（定期的な報告・公表）	・提供先第三者、利用目的、契約約款に関する重要事項の変更などを個人にわかりやすく開示できる体制が整っていること、透明性を確保すること
⑤認定団体との間の契約	・認定団体との間で契約を締結すること（認定基準を遵守すること、更新手続き、認定基準に違反した場合などの内容）

第三者委員会（データ倫理審査委員会）のイメージ



モデル約款の具体的記載事項（案）

・認定団体において、モデル約款を策定

・認定を受ける情報銀行は、当該モデル約款を準拠の上、それぞれの約款を作成

1　個人と情報銀行の間

１）目的

利用者からの委任にもとづき、利用者の個人情報を利用者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

情報銀行は、個人および社会への便益の還元を行うこと

２）定義

今回のモデル約款の対象となる個人情報には「要配慮個人情報」「クレジットカード決済に必要な情報」「銀行口座情報」は含まない

３）情報銀行の行う業務範囲

民間の認定団体から認定をうけた情報銀行は、個人に代わって当該個人情報について、当該個人の合理的利益が得られるような活用手法、情報提供先の選定を行うことができる

４）情報銀行が担う義務

・認定団体からの認定を受けた者であり、認定団体の定める認定要件を遵守する

・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

・個人情報の取得の方法、利用目的の公表

４）情報銀行が担う義務（つづき）

・個人情報の第三者提供を行う場合の判断基準（認定基準に準じて判断）の明示

・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：データ倫理審査委員会の審査・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公表

・個人からの求めがあれば、提供先第三者への個人情報の提供を行わない

・個人が自らの情報の撤回（オプトアウト）を求めた場合は、対応すること

（提供先第三者との関係）

・個人情報の第三者提供を行う場合、当該提供先からの再提供は禁止する

・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
（提供契約には、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、内容などを盛り込むこと）

５）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同意／契約をすること

６）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

７）情報銀行の機能の明示について

・個人が、自らの情報の利用履歴を閲覧、コントロールできる機能（例：データポータビリティ機能）の有無を明示すること

８）相談窓口

・個人からの相談への対応体制を設けること、その旨を明示すること

９）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

10）損害賠償責任

・情報銀行は、約款に違反して損害が発生した場合や、提供先第三者に起因して個人に損害が発生した場合の損害賠償責任に関する事項を明示すること

（提供先第三者起因の場合）

①情報銀行に提供先第三者の選任・監督に過失があった場合

②情報銀行に提供先第三者の選任・監督に過失はないが、

→第三者提供先に過失があった場合

→第三者提供先に過失がなかった場合

→不可抗力だった場合

2　情報銀行と情報提供元（情報提供先）との間

１）複数の情報提供元（情報提供先）事業者毎の事情を勘案し、提供されるデータの「形式」「提供方法」等に関する規定

２）情報提供元（情報提供先）事業者と情報の利用範囲や取扱条件の制限に関する規定

３）情報漏えいの際の原因究明に向けた、情報銀行と情報提供元（情報提供先）事業者の協力体制などに関する規定

４）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