資料4－3

## 第4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

# 認定基準（案）について

2018/3/23

**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。

**１）事業者の適格性**
**経営面の要件、業務能力などの要件、認定団体が定めるモデル約款に準じた契約約款の策定・公表**

**２）セキュリティ基準**
**運用基準（人的体制、遵守ルール）、技術基準など**

**３）ガバナンス体制**
**相談体制、監査体制、認定団体との契約の締結　など**

**４）事業内容**
**情報銀行の義務、求められる機能　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<br>（例）直近（数年）の財務諸表の提示　等 |
| | ・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）<br>（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 |
| 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）<br>（例）類似の業務経験を有する　等<br>・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 |
| | ・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）<br>（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<br>（例）十分な人的体制が整備されている、従前より取引がある　等 |
| | ・個人が理解しうるようわかりやすい説明、形式などにつとめること |

## 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<br>（十分なセキュリティ対策の例）<br>・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<br>・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<br>・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監査体制 | 以下を満たす、社外委員で構成される監査体制を設置していること（例：データ監査審議会）<br>・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<br>・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 |
| 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、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） |

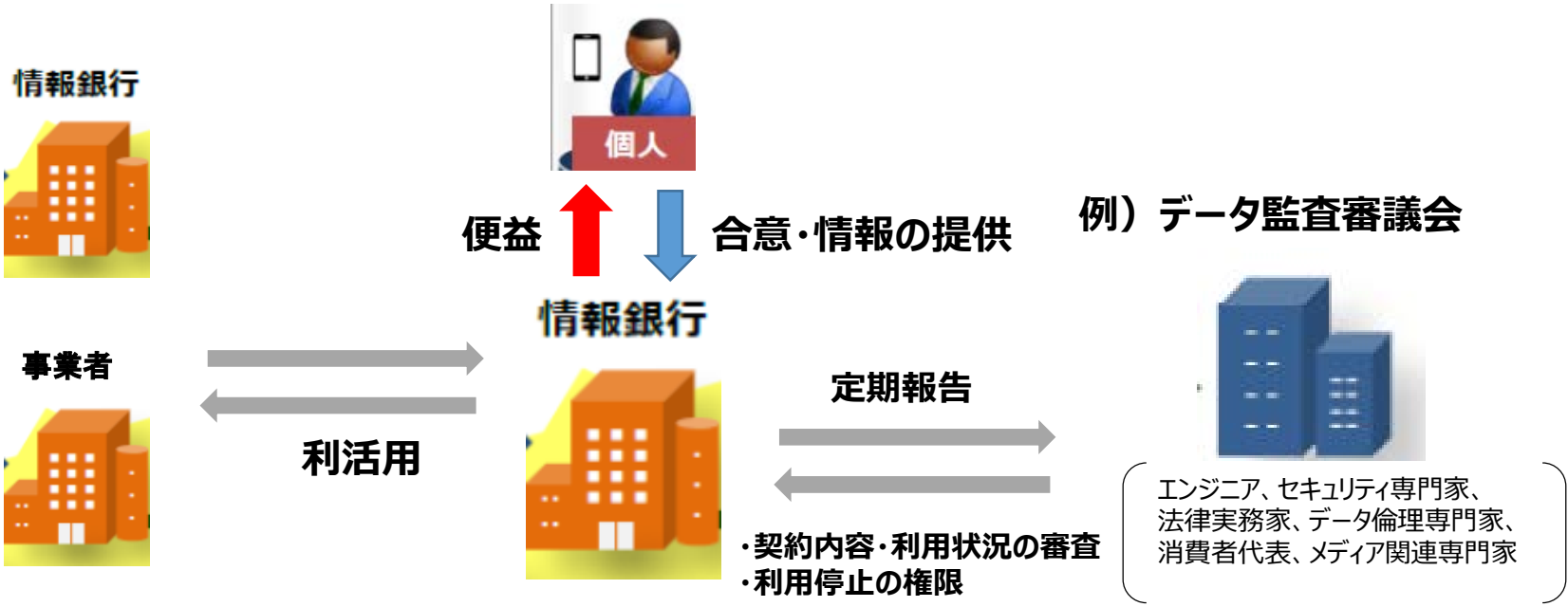
# ４）事業内容について

| 項目 | 内容 |
| --- | --- |
| 個人への明示及び対応 | 以下について、個人に対しわかりやすく示し、必要とされる対応を行うこと<br>・個人情報の取得の方法、利用目的<br>・情報銀行の行う事業及び対象とする個人情報の範囲<br>・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（提供先第三者については認定基準に準じて判断）を示し、個人情報保護法上の同意を取得すること<br>・個人が自らの情報を撤回する場合の手続き<br>・個人が自らの情報を閲覧する場合の手続き<br>・個人が自らの情報の利用履歴を閲覧する場合の手続き<br>・個人が相談窓口を利用する場合の手続き<br>・情報銀行の行う事業による便益 |
| 情報銀行の義務について | 個人情報の第三者提供及び利用目的について、個人情報保護法上の同意を取得すること<br>以下を遵守するとともに、モデル約款に準じて約款等に明記し、個人の合意を得ること<br>・個人情報保護法上の同意の取得をはじめ、法令を遵守すること<br>・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<br>・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<br>・個人情報の第三者提供を行う場合の適切な判断基準（認定基準に準じて判断）の設定・明示<br>・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：データ監査審議会の審査・承認など）<br>・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<br>・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<br>・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<br>（提供先第三者との関係）<br>・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<br>・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<br>（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、損害賠償責任等規定すること） |

# ４）事業内容について

| 項目 | 内容 |
| --- | --- |
| 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下記の機能を有すること<br>その他の機能（例：データポータビリティ機能など）があれば、それを示すこと<br>・自らの情報がどこに提供されたのかの履歴を閲覧する機能<br>・個人が情報銀行へ情報提供をしない旨の意思表示又は自らの情報の撤回をする機能 |
| 責任の範囲について | ・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<br>・情報銀行と提供先第三者の契約に、提供先第三者に帰責事由があり損害発生した場合には提供先第三者が損害賠償責任を負うということを明記する（情報銀行は損害賠償を含む提供先第三者に関する相談も受け付ける）<br>・（上記契約をしなかった場合）個人と情報銀行の約款に、第三者提供先に帰責事由があった場合には、情報銀行が損害賠償を負うということを明記する。（情報銀行は第三者提供先に求償する。） |

# 監査体制（例：データ監査審議会）のイメージ




・第三者提供先の
審査、判断
・利用目的・契約内容などの
審査、判断
・議事録の公開