情報信託機能の認定スキームに関する検討会（第 17 回）議事概要

日時：2021 年 5 月 17 日（月）16 時 00 分～18 時 00 分
場所：Web 開催
構成員）宍戸座長、生貝構成員、石原構成員、伊藤構成員、井上構成員、太田構成員、
落合構成員、高口構成員、小林構成員、立谷構成員、田中構成員、長田構成員、
日諸構成員、藤本構成員、古谷構成員、真野構成員、美馬構成員、森構成員、
森下構成員、森田構成員、山本構成員、若目田構成員
説明員）大日本印刷（株）
オブザーバー）内閣官房情報通信技術（ＩＴ）総合戦略室、個人情報保護委員会、
一般社団法人日本ＩＴ団体連盟
事務局）総務省、経済産業省

□資料１７－１「情報信託機能の普及促進に向けた課題解決に係る調査 報告資料」について大日本印刷（株）より説明。
□資料１７―２「検討会（第 16 回）における主な意見とその考え方」について事務局より説明。
□資料１７－３「「情報信託機能の認定に係る指針 Ver2.0」改定案」について事務局より説明。

□意見交換
＜情報信託機能の普及促進に向けた課題解決に係る調査＞
●情報銀行を運営する上で認証を厳格にすることも重要だが、本人確認のレベルもキーになると思う。この点について検討したのか。また、P10 の図は、個人の情報銀行Ａでの同意に基づき情報銀行Ｂやそのデータ提供先にもデータが提供されるというものか、それとも、情報銀行 A での同意は情報銀行Ｂの認証まで及ぶのみで、そこから先は個人が情報銀行 B にアクセスして開示制御をするのか。
●本人確認という観点では、「犯罪による収益の移転防止に関する法律施行規則第 6 条」に準拠した方法で本人確認を実施したか否かでレベル分けするのが良いのではないかなどを検討したが、実証では認証の要求レベルについて特に検討した。例えば ID・パスワードのアカウント登録のみの低い認証のサービスと、生体認証も行っているサービスが同じ連携の中でデータ提供されないようにするなど検討を行った。また、情報銀行の連携のモデルは、ワンストップでサービスが利用できることを想定したので、情報銀行 A から情報銀行 B の提供先を利用するような形で検討した。
●P11 の検討内容⑤について、データ提供先事業者としての適格性を判断するのに必要十分であり、提供元となる情報銀行が適切な監督を実施できる基準とあるが、具体的に教えていただきたい。
●報告書の 3.5.6.1 にあるが、特に認定を取得していない事業者に関しては基準が必要になるといったことを挙げている。

●各認定情報銀行におけるセキュリティには様々な側面があり、認証だけには依存しないと思うが、認証のレベルを中・高という曖昧なもので考えてよいのか。かかる認証のレベルを測る基準は情報銀行の認定基準において定義されているのか、それともこれから考えていくのか。クラス分けされた異なる情報銀行が存在し得るということが前提なのか。同じレベルの認証・セキュリティでも、取り扱う情報が機微なのか否か、情報の性質に応じて類型化することが次のステップと思う。

●レベル低・中・高で定義するのは、現実には時代とともにセキュリティのレベル感に変化が起こるので難しいと思い、実証の中では明確に規定をしなかった。現行の認定制度を含めて特に情報銀行のクラス分けはされておらず、異なるレベルの情報銀行が存在するということは意図していない。

●P5 の２の同意について３つに整理したとあるが、何かポイントがあれば教えてほしい。また、P11 に消費者によるコントローラビリティの確保とあるが、コントローラビリティのしやすさや、多様な消費者を想定して検討したのか。

●利用者は、サービスを利用する各段階で求められる同意につき、それぞれの意味がわからなくなりがちであるから、情報銀行を最初に使う際の利用規約への同意、これから ID 連携することに対する同意、ID 連携した後にサービスを利用する際にデータを第三者提供すること対する同意を区分けして必要な要素をまとめた。また、コントローラビリティに関して、例えばドコモや KDDI の設定のような、ユーザーが多いため広く使われる中でスタンダードになるようなものも意識して検討の要素に加えており、大勢のユーザーに対して、情報弱者やスキルが低い方も含め、消費者が自分のデータに対して主権を発揮できるよう、機能、役割を考えた。

●P10 の６つの観点は報告書 P69 の様々なユースケースを洗い出して出てきたものと思うが、P10 の図では消費者から情報銀行 A と B にそれぞれインタラクションがなく、これは何かの観点にかかってきているものなのか。

●報告書の図は情報銀行の役割や位置づけを明確に表している図で、P10 の図は情報銀行を介してデータが転々としていくことを示している。

●本人確認のレベルの話は IAL への配慮が必要になってくると思う。また、情報銀行の認証レベルの話は、エンティティーの認証レベルと情報銀行の認証レベルの話を分けて考える必要がある。その際、情報銀行同士の認証が重要であり、例えば資格の失効や、認定状態がリアルタイムで分かるようなレジストリ基盤の必要性も考えられる。

＜検討会（第 16 回）における主な意見とその考え方＞

●番号４について、情報銀行のコンセプトは消費者に明示して判断してもらうというよりも、情報銀行が消費者のデータを適切に取扱い、提供先より先にデータ提供をしないというものだった。健康・医療データはより丁寧な取扱いが必要だと思うが、第三者提供後の取扱いについて、あらかじめ本人に明示する前提の情報銀行サービスを今後設計していくことは、情報銀行のコンセプトと整合しないのではないかと懸念する。

●番号９について、複数の世帯構成員から利用されるデータのオプトアウトについて、放送

セキュリティセンターの指針では、必ずしも契約主体でない世帯構成員からのオプトアウトを前提とするものではなかったのではないか。
●放送セキュリティセンターの指針でも、オプトアウトを求めるのは広く世帯構成員である。ただ、基本的に契約者の家族が世帯構成員となる視聴履歴と異なり、今回の場合は同乗者なども世帯等構成員に含むことから本人確認が難しい。それでも、本人確認ができた限りという条件付でならばオプトアウトさせていいのではないかと考えた。このような意味では、放送セキュリティセンターの指針と整合しているといえる。
●番号８については、何か起きたら必ず取消しをするという意味合いではなく、ガバナンスに関連する問題があると判断される場合に適用されるもので、仮に何かあったとしても、適切に直ちに是正した場合にはディスクロージャーも考慮して取消しがされない場合があるというような要件であると思う。

＜「情報信託機能の認定に係る指針 Ver2.0」改定案＞
●要配慮個人情報に該当しない情報の例について、例えば、今後、医師発ベンチャーによる AI 問診サービス等、医療機関でない民間事業者が行うサービスがあった場合、その中で、実質的には医療機関による問診と同様の質問があったり、既往歴や過去の治療歴に関する質問があったり、遺伝子や遺伝を推察するような情報が質問項目として含まれている場合、当該情報は個人が入力して個人が管理している情報となるが、要配慮情報ではないとしてよいのか、追々考えていく必要がある。
●レベル２情報、レベル３情報を整理していくに当たり、どういった条件を課すのか引き続き検討させていただきたい。
●「本人又はその家族が本人の健康管理のために取得・管理する」という表現は、医療機関で検査して、その情報を本人たちで取得・管理している場合も含んでいるように読めるため、書きぶりを修正すべき。
●取り扱える情報を組み合わせれば、例えば鬱状態にあるかどうかを推知できると思うが、従来、要配慮個人情報を推知する場合は、その情報は要配慮個人情報には当たらないという整理だったと思う。データを積み重ねてプロファイリング・解析すると、要配慮個人情報と同等の情報が得られると思うがどのように考えていくのか。今回の個人情報保護法の改正では、不適切な利用の禁止や、プロファイリングを含む利活用における利用目的の特定をする等の方向性が示されていると思うが、情報銀行の場合には、説明責任や透明性が求められるのではないか。
●情報の組合せによる影響については重要な指摘であるため、引き続き検討課題とさせていただきたい。
●IT 連のガイドブックでは、「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」とされている。また、不当な差別を生ずる可能性があるプロファイリングの可能性についてはデータ倫理審査会でも審議することになっている。
●医師とベンチャーが共同開発した民間サービスでも、鬱症状を高精度で判定する民間サービスがある。

●令和元年 10 月のとりまとめでは、信用スコアの取扱いについて一定の整理を行った。今後、不適正利用禁止などについて指針を見直す際、前提として考え方を整理し直す作業が必要になると思うので、プロファイリングに関する指摘については、今後の課題として引き続き検討することとしたい。
●要配慮個人情報の取扱いに係る実証事業では、血圧や心拍数、身長、体重等に関して項目の抽出によっては機微な情報が明らかになってしまうのではないかという議論はあった。鬱病の話はなかったが、AI 等を使って将来的には組合せによって色々なことがわかるのではないかという点はチェックしていた。
●一定の推知を人工知能で行うサービスにおいて、病名を判定するものになると、規制上は薬機法でプログラム医療機器になるため、医療機関で行うべきサービスになる。一方、もう少し抽象的な形でリスク評価を行って受診勧奨する程度であれば、規制上は民間事業者でもサービスを行うことができる場合もある。規制も踏まえた上で整理してほしい。なお、医療行為の範囲などは全部に明確な線引きが難しく、定義し切れないまま議論されてきているものであり、指針に記載するのであれば、この点も踏まえて書きぶりを検討してほしい。
●再提供禁止の例外のサービスの乗換えについて、同様または類似のサービスというのは、かなり幅のある考え方と思う。例えばフェイスブック、インスタグラム等は類似なのかというと、様々な捉え方が出てくると思うが、これをどのような方向で具体化していくのか。
●考え方としては、再提供の必要性があって、再提供禁止の例外の濫用を避けるよう定めているため、一定の制限はかかってくると思うが、具体的にどのような基準で整理していくかまでは議論が進んでいない。
●再提供禁止の例外については、「サービスの乗換え」は本人の権利であるため、情報銀行がこれを禁止することはできないという観点から出てきたもの。
●情報の組合せによる影響について、どのような行為によって何が推論できるかで行為規制などをすることは、現実的に難しいし、事業者の創造性に蓋をするもので妥当でないと思う。情報を何のためにどう使うのか、何をするかについての説明を徹底すればよい話で、プロファイリングをやるという場合には、情報銀行には徹底した開示説明が義務づけられるというにとどまる。また、乗換えについては、「個人の指示の下に」という一言を入れると良いのではないか。
●サービスの乗換えが、あくまで本人の意思の発信であるということは重要だと思うが、サービスの類似性と本人の意思は少し別の論点と思うので、サービスの類似性を議論していくのであれば、何が類似で、何が類似でないか考える必要があり、そこは問わないということであれば、あくまで本人の意思ということを重視することになる。この点の切り分けが必要。
●情報銀行の廃業、合併など、事業者の都合により移転せざるを得ない場合も考えられると思う。
●プロファイリングについては、情報銀行が絡むプロファイリング一般の問題を議論しているのか、ヘルスケアデータなどを取り扱うという観点から検討会の議論で気をつけなければならないのか。また、情報銀行は高度な信頼が求められるという観点から、より徹底し

た透明性などを求めるのか、さらに進んで、一定の規制として、IT 連のガイドラインで示されているようなデータ倫理審査会で議論をすることも含めての手続的な統制がかかるのか、今後、一体的な統制を議論していくのか。論点自体は整理しておく必要があり、これを次以降の検討に送ることが必要だと思う。次回までに事務局に整理していただきたい。

以上