参考資料２－２

情報信託機能の認定スキームに関する検討会
認定・運用ワーキンググループ（第１回）　議事概要

日時：2020 年 11 月 30 日（月）16 時 00 分～18 時 00 分
場所：Web 開催
構成員）森主査、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、
長田構成員、野村構成員、花谷構成員、美馬構成員、森田構成員、山本構成員、
湯淺構成員
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事務局、一般社団法人日本 IT 団体連盟、
一般財団法人日本情報経済社会推進協会（JIPDEC）
事務局）総務省、経済産業省

資料１－１「開催要綱」について総務省より説明。
資料１－２「認定・運用 WG における検討事項」について総務省より説明。
資料１－３－１「提供先第三者への提供方法」について太田構成員より説明。
資料１－３－２「情報銀行ビジネス参画事業者を増加させるための検討策」について花谷構成員より説明。
資料１－３－３「提供先第三者に係る情報銀行の認定・運用上の課題について」について IT 連　野津氏より説明。
資料１－４「統制環境に問題のある事業者の扱いについて」について、IT 連　野津氏より説明。
資料１－５「IoT 機器から取得されるデータの利用について」について IT 連　野津氏より説明。

□意見交換
＜提供先第三者に係る情報銀行の認定・運用上の課題について＞
―資料１－３－１について
●どのユーザーにレコメンドを出すかというのは提供先第三者の注文を受けて paspit が考えることになる。そうすると paspit からは何も提供されないことになり、ID のやりとりもいらないのではないか。
●レコメンドでは、提供先第三者のオファーに基づき、ID と性別、年代、趣味、嗜好といった情報を paspit から提供先第三者に渡した情報を利用している。この際、特異な記述は削除している。
●ウェブサイトを審査するとあるが、提供先第三者で個人情報を収集するような仕組みをツールで調査するものかと思う。一方、paspit を通じて個人が自ら提供先のウェブサイトにアクセスし個人情報を提供する仕組みが想定され、このような事後的に個人情報が結びつく仕組みもこの審査に引っかかるように思われるが、システム上どう対処しているのか。
●提供先が最初は個人情報を持っていなかったが、paspit のレコメンドを受けて個人が提

供先に個人情報を提供することによって、提供先で個人を紐づけられる場合があることは課題。提供先第三者の選定に係る記載の①オンサイトで見せるパターンも、②匿名化して渡すパターンも、③委託先に全部預けておいてちょっとしか使わせないというパターンも、全部同様の点が問題になるので、２回目以降の検討させていただきたい。

―資料１－３－２について

●秘密計算の説明があったが、情報提供先で個人からどのように同意をとるのか。トランザクションが発生する場合には、秘密分散や秘密計算を使う必然性はあまりなく、固有の ID データでやりとりすればよいのではないか。

●P12 では、事業者Ｂから暗号化した自社データを②の情報銀行側のデータベースに渡すことになる。ここでは、事業者Ｂ側が顧客との間で事業者 B の情報を情報銀行側に提示することがあることを同意取得してもらいたい。できない場合は、個別に目的を伝えて、同意を取り直していただく必要があると思う。暗号化されたデータが情報銀行側に回って、情報銀行の中でいろいろな分析がされることを想定しており、事業者 B が持ち込んだデータと情報銀行にあるデータをマッチングさせてみて何か気づきが得られるとか、そういったようなものを情報銀行側の秘密計算をする場所において暗号化されたまま分析してもらい、答えを出してもらうとよい。

●１つ１つのデータだと秘密計算するメリットはないが、事業者 B が情報銀行のような存在で、情報銀行と事業者 B の両方が本人から同意を取っていれば、安全に秘密計算してその結果を両者でシェアして活用することができると思う。

●P4 で審査のたびに証跡を揃えるのは負担が大きいとはどういうことか。

●情報提供先企業が複数の情報銀行に接続をしてデータをもらいたい場合、２つ以上の複数の情報銀行に対して提供先になるために、それぞれの情報銀行が定めた内容の審査を受けなければならない。全く同じ審査であれば１つの証跡で複数回使えるので、統一の中身で引用できるような形があるとよいと考えたもの。

―資料１－３－３について

●P13 の提供先が契約を結んでいる委託先に対して情報銀行からデータを提供していくというパターンは、実際の事例として幾つもある。この際、提供先と委託先の契約で、提供先が委託先に預けているデータを見ることが可能となる契約を結んでいるケースも多い。このように P14 のｅ）やｆ）といった情報銀行側の監督義務を超越した契約が既になされているケースがあるが、情報銀行が提供した個人情報と提供先が委託先に委託している個人情報については、いくら契約があったとしてもリスクがあると思う。何らかの厳格なルールをもう少し決めていったほうがよい。

●そこの縛りをどうするかというのも今回決めなければいけない。③の問題と②の問題をくっつけて考えて、提供先に渡せる情報とは何かということを突き詰めていくべきなのかと思う。

●②について、もともと GDPR32 条などで仮名化又は暗号化という対策が定められていた

例があったのでそのように記載したと記憶している。当時は個人情報保護法において仮名化という用語がなかったが、現時点では、法改正に基づいて個人情報保護委員会で仮名加工情報の基準が議論されているので、それに合わせて議論していくとよい。暗号化については日本ではあまり取り扱っていないが、どうとらえるか、その方法として秘密計算というのもあるのかと思う。独自基準を作らなくていいところは合わせていけばよい。

●仮名加工情報については、個人情報保護委員会の公表資料以外に情報がないが、若干緩い原則も出てきているので懸念がある。秘密計算については、情報銀行が提供するという機能に着目していて、第三者から情報をもらって紐づけることは考えていないが、その第三者から同じ個人の情報をもらってきた場合に、果たして個人の意思に基づく情報銀行の在り方と合っているのかといった話も議論させていただきたい。

●各法令や基準間の差分はわかりやすくすべきなので、仮名加工情報の定義は参照しつつ、さらに加重するのであれば、さらに何らかの要件を満たすことが必要、という形にするとよいのではないか。

＜統制環境に問題のある事業者の課題について＞

●例えば、プライバシーマークは個人情報のマネジメントを見ている第三者が見ているものなので、要求されるマネジメントが回っているのであれば、付与される。一方、社会信用を失墜するようなことを行っている場合などケースによっては、一時停止をすることや、欠格にすることもある。

●一般的な契約の場合だと信用失墜行為を条文に含めることはわかるが、法令上の登録等の場合は何となく書き難いと思う。一般的な契約と法令上の登録等の間にあるのが情報銀行の制度だと思うが、契約より厳密な要件とすべきと思われるので、「信頼性に重大な影響を及ぼすおそれがあるようなことがあれば」という抽象的な書き方で取消し事由にしてしまうのはよくないのではないか。ガバナンスの体制の構築、維持等を要件に書いておいて、個人情報と直接的に関係がない場合でも、個人情報における管理体制に問題がありそうという状況があれば、その際はガバナンス体制の違反で認定を取り消すという運用をすればよい。

●プライバシーマークでも類似の事例があるので、情報銀行でやってはいけないということはないと思う。やはり組織防衛論というものもあり、認証のブランド維持ということもある。

●認定の基準とは別に、総合的に評価する範囲として記載されている方が、これから申請する事業者もしっかりしてくるのではないかと思う。

＜IoT 機器から取得される情報の利用について＞

●情報銀行のユーザーから情報銀行が同意を取る上で、家族全員の了解を取ったか、その中には契約者も含まれているか、という点の確認を取る必要はあるのか。

●通常は利用目的などの説明事項があった上で同意を取るため、その中で、家族全員の了解を取ってくださいということを明示事項に加えるものと思う。

●IoT 機器から取得されるデータとあるが、世帯プライバシーの保護についてということだと思う。IoT 機器から取得されるデータであっても、一人一人のデータであればこの議論にはならないため、誤解のないような見出しにしてほしい。また、世帯構成員から同意を得て注意喚起するというのは、放送分野の場合にはイメージしやすいが、例えばセンシングするデータが音声や画像である場合には、個人が特定できるデータも入ってきてしまうので、対象データを限定的にするべきと思う。
●情報銀行ならではというよりも、IoT 機器から取得されるデータの合意の取り方ということで、もっと上位で整理する方がよい。また、仮に IoT 機器に登録をした方と違う世帯構成員が情報銀行に対して何か同意したとしても、IoT 機器のサーバーからデータを呼び出す際に、ID やパスワードが必要になるため、契約主体と話をして情報を取得するという流れにならざるを得ないか、もしくは同一人物が処理をするしかないのではないか。ネットワークで渡されるのであれば、結局、認証をどのように行うのかによると思う。
●ケーブルテレビの視聴履歴であれば、ケーブルテレビ契約者が個人情報の本人となり、家電製品の会員契約、メンバーシップ契約をしていれば、その人が個人情報の本人となるしかない。
●情報銀行が IoT サーバーから取るデータについて在不在データと書かれているが、どのようなデータを受け取ろうとしているのか。便益はその IoT 機器を契約している世帯にだけ戻すことになるのか。
●在不在データというのは、不在の際には電源を落とすであろう機器の情報から得た推定値になる。便益としては、IoT 機器のサービスの一環だが、離れて暮らしている人の在不在、電気をつけているかどうかといった遠隔監視サービスに用いることができる。
●制限された状況でのことをイメージしていると思うが、もっと幅広いデータ収集ができる場合もこの条件になってしまうとなるとどうかと思う。どういう情報の場合なのか、もう少し具体的に書く必要がある。
●ユースケースを想定して論点を表面に出す形で記載したい。また、本来は世帯混在プライバシーと書くべき。
●一番抽象的なレベルで考えると、例えば写真に何人かの顔が写っている場合も同じ構造になっている。テレビの視聴履歴の場合だと基本的には契約者個人の情報なので、その人に了解を取ってもらえばよいと思うが、顔写真のようにそれぞれの人の情報が分かるような場合には、明確に同意を取ってくださいと言うべきではないか。指針には詳細は書き過ぎないようにして、別のところで切り分けを記載しておくとよいと思う。
●具体的には、写真、音声、ビデオで顔認証が取れる場合については世帯混在プライバシーから外す方向で進めていくのかと思う。

以上