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３回）　議事概要

日時：2021 年３月 15 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３－１「認定・運用WG（第２回）における主な意見」について総務省より説明。
資料３－２「認定・運用WGとりまとめ（案)」について総務省より説明。

□意見交換
＜提供先第三者の選定について＞
●P.8 の国立情報学研究所の資料から引用された「本人到達性のあるメールアドレス」というのは、名前@会社名といった本人が分かるメールアドレスのことか。
●本人到達性のあるメールアドレスというのは、一般的に個人情報として説明されている名前@会社名といったものではなく、単なる英数字の羅列であっても本人到達性のあるメールアドレスは含まれる。本人にサービスとして割り振られているメールアドレスは全て該当すると思う。
●相談窓口のグループメールアドレスなどは、本人到達性があるとは言わないと思う。
●P.9 では、個人を識別する情報を除くため、「生年月日については年まで、住所については市区町村まで」とされており、例えば生年月日を月までにしても個人を識別することは難しいと思うが、ここで指定するべきことなのか。また、クレジットカード番号はなぜ削除されているのか。
●国立情報学研究所の資料では、他の情報との組み合わせや場合分けなどは想定していないため、やや保守的に生年月日については年までといった。クレジットカード番号については、平成 27 年の個情法改正の際に、個人情報は、本人と密接な関連があることや、本人または本人の機器と密接な関連があること、簡単には変えられる情報ではないこと、といった要素で判断すべきではないかという議論があり、クレジットカード番号も本人にとって重要な情報であり、簡単に変えられる情報ではないことから、規則１号の加工で削除されていた。
●クレジットカード番号は、匿名化や仮名化の議論という以上に、安全管理措置として PCIDSS に準拠していない事業者に生のままの情報を渡すのはどうなのかという課題があ

るため、その観点で書いていただくと良い。
●P.4 の「ガス・水道・電気・通信などライフラインに関わる」の「など」には何か別のものも入るのか、それともこの４業種に限っているのか。
●所轄官庁の監督下にあるか、もしくは公的にガイドラインがあって一定の監査の枠組みがあるものが挙げられていると思う。例えば、医療情報の分野では、厚労・経産・総務の３省でガイドラインを作り、その下に自主規制団体をつくって運用することになっており、このような場合もケースに入れることが考えられる。また、MaaS の情報連携などのモビリティーサービスも業規制の範囲内といえ、金融等ほどではないにせよ個情委も入って公的に情報の取扱について整理されているので、医療・ヘルスケアとモビリティーも認めてよい場合があるのではないか。
●医療については現行の認定指針で対象外とされているため、認定指針に追加する際に検討したい。P.4 の「規制業務の範囲内において個人情報保護のための措置が確保されている」というのは、例えば許認可であれば、認可の要件として個人情報に関することが要求されているという場合を想定しているため、モビリティーについては該当しないのではないか。
●４業種以外は要検討のため、ガス・水道・電気・通信にかかる「など」を外すかどうか、外した上で何か追加するのか検討したい。
●電気、通信、金融については、公的な機関が入ってルールを作り、それに基づいて個人情報を活用すると承知しているが、ガス、水道については同様の仕組みがあるのかわからないので、もしあるのであれば、何のガイドラインなのか、またそれはどの分野を意識して作成されたものなのかを記載するとよい。また、P.8 の「履歴は原則としてそのままでよいものとする」という記載は、匿名加工よりも緩和された部分のようである。しかし、移動履歴などの個人特定性のある履歴データは加工が必要で、そのままでよいとする原則の対象から除くものと想像しているが、このままの記載ではどこまでが含まれるのかわからない。
●金融、放送、通信分野では、いわゆる業全体について監督されているが、ガス、水道は特段個人情報保護の議論がされておらず、電気についても一部の情報利用の枠組みに乗っている場合に限ると思うので、ライフラインという言葉は使わない方が良い。その上で、個別に官公庁が入ってルール整備がされており、それに対して何らかの制裁が自主規制団体や業法で担保されている場合に当該範囲を認めることができるのではないか。
●P.8、P.9 について、当初は仮名加工情報に近い形で開示・提供する話だったと思うが、現時点では匿名加工情報と仮名加工情報の中間の形を模索しているようにみられ、わかりづらい。
●仮名加工情報は内部利用を前提とするもので、それを外部提供することは個情法との差分が大きくなってしまう。そのため、提供しても安全な形ということで、匿名加工情報に寄せた形となっている。
●P.8 の匿名加工情報について、国立情報学研究所のレポートを引用しているが、個人情報保護委員会の発行しているレポートの中でも触れている部分があるため、同レポートも含めて引用して欲しい。P.9 は、右肩に個人情報保護委員会の資料参照となっているが、元資料から加工されておりミスリーディングであるため、表記は事務局と相談させていただき

たい。また、仮名加工情報は基本的には第三者に提供しないことを前提とした制度であり、それを踏まえた説明としていただいた方がよいと思う。
●匿名加工情報に寄っていってしまっているところは、事業者としては非常に使いにくい。情報銀行の認定を受けていない事業者は、同意を取っていれば個人情報をそのまま第三者提供できるため、認定を受けた事業者と受けていない事業者の差が広がってしまう。事業者が現在行っている安全管理措置にもできなくなるものが出てくることを危惧している。情報銀行も前提として個人から第三者提供の同意を得ており、個別同意であればどの情報を誰に渡すかを明示した上で、かつ倫理審査委員会も通った上で行っているにも関わらず、匿名加工に近い加工までは必要ないのではないか。
●仮名加工情報側に寄せることは難しいと思うが、安全な形で安全管理措置のできない提供先に渡すとはどういうことなのかということを、もう少し詰めなければいけないと思う。
●例外３類型については、エンドユーザーの目線からすると、例外を積み重ねることによってわかりにくくなっているように感じる。今回の例外３類型に異論はないが、今後どこまで例外を積み重ねていくのか基本的な考え方があるとよい。
●認定指針ではもともとＰマークやISMS認証を取得した提供先のみに提供できるとされていたが、そこから拡大して安全管理措置をできない提供先に情報が提供されてしまう恐れもあるため、ユーザーの利便性だけでは決められないと思う。ある程度具体的な中身が詰まってから例外を抜いていきたい。
●慎重に議論して限界を探っていく方向性は賛成だが、安全性を守るための技術を使えば使うほど複雑化して分かりにくくなるという矛盾もあるので、ある種のカテゴリカルな線引きがどこかで必要になると思う。
●P.10 で情報銀行が委託先になる場合に、他の委託先の情報と混ぜてはいけないことになると思うが、情報銀行で持っている「男性」という情報に対してこのようなクーポンを送って欲しいという同じ要求があった場合に、企業ごとの情報を混ぜてはいけないとなると現実的に難しいと思う。

＜統制環境に問題のある事業者の扱いについて＞
●社会的信頼維持のための体制とは具体的にどのようなものか。
●非常に重大な社会的な問題を起こすような事業者は、社会的信頼維持のための体制ができていないと判断する。これを認定の要件とすることによって、個人情報と関係のないところで社会的信頼を失墜した場合であっても、場合によっては認定を外すことができるというもの。

＜再提供禁止の例外の事例について＞
●P.14 に「サービスは同一のものであること」と記載されているが、同一性はどのようにはかればいいのか。
●再提供禁止の例外はアグリゲーションサービスと乗換えサービスに限ろうとしているので、その乗換えであることが明確になるようにサービスは同一と書いている。

●乗換えに対応して情報銀行からデータをもらう事業者は、情報銀行と何かしら契約をしなければならなくなるが、個人の利便性としてどうか。
●情報銀行の契約が提供先についてくる考え方と、ユーザーの意思のもとでの乗換えなので情報銀行の認めた提供先ではないことをはっきりと示すという考え方があると思うので、検討したい。
●P.14 の「公的ガイドラインまたは業法の整備がされている分野において」というのは、P.34 の方にも加筆していただきたい。
●アグリゲーションサービスと乗換えサービスに限定した経緯は何か。アグリゲーションサービスというのは間口が狭すぎるように思う。
●主査と IT 連、事務局の間で相談する中で、抽象的な書きぶりをせずに類型化しようとしたもの。当面はユースケースで積み上げていくということで、スモールスタートとしたい。

＜世帯の複数の構成員が利用する機器等から取得される情報の利用について＞
●P.16 の枠内に「また、情報銀行における利用の停止については、世帯等構成員全員からの利用停止の求めを広く認めるべき」とあるが、車の同乗者なども含まれるのであれば本人確認などが難しいので、広く認めるべきとしてよいのか。
●世帯構成員全員から広く認めるとなると本人確認の問題が生じてしまうので、本人確認ができる限りにおいて、とするなど検討する。
●P.16 の枠内の「全員の同意を得たことを確認すべき」というのは、契約者本人が行うものと思うが、確認すべきなのは誰なのか分かりづらい。放送セキュリティセンターの指針では、契約者が全員から了解を得ること、そのため、了解を得るように注意喚起すべきという表現になっている。その上で、「世帯等構成員全員からの利用停止の求めを広く認めるべき」の「認めるべき」の相手は誰なのか。情報銀行と契約がない者からの利用停止の求めは技術的に難しいと思う。
●P.21 のユースケース③については、FNS データ視聴利活用プロジェクトを取り上げているが、同プロジェクトでは個人情報に該当しない非特定視聴履歴を扱っているため、個人情報を扱っている有料放送事業者のデータ活用事例などを取り上げてほしい。
●今回は情報の取得場面にフォーカスされていると思うが、例えば、保険や融資などの個人に関する決定に世帯等構成員情報が活用できる場合、個人に関する評価にほかの構成員に関する情報が紛れ込んでしまい、個人への判断がゆがんでくる、あるいは不公平・不公正な形で行われることも想定できるが、利用段階に対する情報銀行としてのスタンスはあるのか。
●認定指針では考えていない部分だが、正確性の観点も取り入れて、IoT データについては不正確なデータを認めないようなことも考えられると思う。

以上