情報信託機能の認定スキームに関する検討会（第 6 回）議事概要

日時：2018 年 4 月 24 日（火）10 時 00 分～12 時 00 分
場所：総務省 10 階第一会議室
構成員）宍戸座長、井上構成員、上原構成員、小林構成員、田中構成員、日諸構成員、若目田構成員
オブザーバー）一般社団法人データ流通推進協議会、日立コンサルティング、一般社団法人シェアリングエコノミー協会、株式会社データサイン
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
事務局）総務省、経産省、一般社団法人日本 IT 団体連盟

□資料６－１「検討会とりまとめ（案）について」事務局より説明。
□資料６－２「検討会とりまとめ（案）についての確認事項」総務省より説明。
□意見交換
＜セキュリティ基準について＞
●基本原則としては、セキュリティ、プライバシー双方配慮すると記載されているのでよい。
●具体的基準について、例えばアクセス制御の部分で最も重要なのは、アクセス権がある者がアクセス権のある資産にしかアクセスできないことが担保されていること。
●最近は、技術で守るより、運用で守る方が費用対効果が高いことあるため、「常時、サイバー空間の情勢に応じたアップデートが行われていること。」などの追記が必要。
●インシデント検知後の対策について、体制など記載が弱いので追記すべき。また、「セキュリティ基準」か「ガバナンス体制」のどちらかに「セキュリティ監査」を追記すべき。
●特にプライバシーについて、昨年度規格化された JISX9250 が、プライバシーの最も基本的フレームワークであることから原則に追加した。ただ具体的な行動プラクティスをまとめた ISO29151 などについては、まだ発行されて間もないため、今後の議論。ここではアクセス制御の部分などセキュリティ基準に上乗せできる部分を追記いただいている。
●アイデンティティ管理システムの部分について、認証にも踏み込み LOE のレベル 3 程度を求めていくというのもあるが、ここに記載するのは、かなり具体的すぎるかもしれない。
●アクセス制御と暗号の項目の記載は、もう一段階概略化して良い。「技術的セキュリティ」として「アクセス制御と暗号」と整理してはどうか。
●このセキュリティ基準は原案で公開されていくのでよいが、現在の記載はセキュリティポリシーの上位概念であり、今後実装に際してはガイドライン的なものが必要。

－データの国内制限について
●資産の管理の箇所で「固有のデータセンター、それと同等の委託先･･･」のところで、国外でのデータ管理は厳しい問題があり、国内限定という要件を検討してはどうか。
●総務省が出している医療分野の ASP・SaaS のガイドラインでは、国内法の適用範囲が及ぶ、と記載されているので、国内限定の議論で参照してはどうか。

●約款で海外法人であることを根拠にサーバの設置場所でもめてしまう場合もあるので、国内に設置するというのもあるのではないか。
●全て国内に設置ということではなく、主要なデータを保管する場所は国内、など幅が必要ではないか。
●国内に限定すべきかについて、一つは、事業者にとって不便なので、外資系クラウドが使えないとはすべきではない。一方、利用者の便益の観点で、いつのまにか国外にデータが流出する、ということ徹底的に排除されるべき。海外にデータが行ってしまうと、国内法が通用しない可能性もある。そこで、「国内法に則って事業を行う」ということを明確にすべき。
●係争が起こった時、日本法ではないから責任を持たないとならないよう準拠法を日本法とするのが重要。

－P マーク、ISMS 認証について

●P マーク又は ISMS 認証が必須ということだが、これから認証を取得していく場合、申請中で、仮で認証を受けている部分でも OK としてほしい。
●P マークと ISMS 認証は「or」か「and」か。
●P マークと ISMS は違うものであり、両方とると二重のガバナンスになるのを嫌ってとって片方しか取らない例はかなりある。
●今回の案では、民間の認定スキームであり、安全安心を担保しつつも、民間の認定団体の負担を軽減できる部分も考慮。P マーク又は ISMS 認証のどちらかを取得していれば、客観的に何等か認証制度を受けていることがわかる。それに上乗せする部分など具体的基準で確認。
●消費者から見て、P マークへの認知が非常に高いので、P マークの場合は、具体的基準 12、13 ページを合わせ技で、遵守していると提示すれば対応可能ではないか。
●いずれにせよ、マネジメントシステムをしっかり回している経験がありそれを継続的に取得している事業者であるというのが、認定の入り口にあるということが重要。

＜認定の対象範囲について＞

－認定の対象と責任範囲について

●損害賠償との兼ね合いで、認定対象に、今回「PDS 的に情報提供者本人が個別の提供に係る判断をする場合」も含むとなると、本人が判断したのに、その結果損害が生じた場合にまで、情報銀行が責任を負うというのは重いのではないか。
●今回の認定対象の変更案は、ベン図左の情報信託機能の範囲を右側（PDS 的機能）にも広げるということ。その範囲変更によっても、責任は分解できず、情報銀行が一旦責任を負うということが、前提であると思う。
●個人に理解して有効な同意を得ていただくのが重要であり、ダッシュボードなどで個別同意に近い形もご検討されているところ。本検討会が、包括的な同意を取得するということを主眼に検討されてきたのは理解しているが、既に高い信頼を得ている企業だけではなくスタートアップ企業も含めて考えた場合には、包括的同意だけでなく個別同意も想定され、

多様な主体が認定を受けられるようにしていただきたい。なお、個別同意であっても、この認定を受けた場合には、責任は情報銀行が負う、ということではないか。
●認定を受けなければ良いというのはそれでよいが、認定を受けない行為が、自分たちが安心安全ではないということを示していることになりかねず、最初から認定を受けられないというのは不利益にあたる。
●仮に認定申請しない事業は、安心安全なものではないということを証明してしまうということになる、などの議論があるのであれば、対象はもとの①のほうがシンプルではないか。
●そもそも、認定を受ける、受けないは自由であり、認定を受けなくても損だということではない。自前で情報開示や、監査委員会などもまわして安心してもらうことも本来できる。それを P マーク同様、簡便にわかりやすい徴表として民間の認定スキームを作っている。認定制度の存在によって、直ちに情報銀行以外の PDS、データ取引市場にまでデグレデーション（degradation）の問題がおこるとは思わない。PDS については、個々の情報提供時に、ユーザーインターフェースを提供して個人にわかり易く示すこともあるので、重たい義務も受けてもやりたいという事業者が希望するのであれば認定対象としてはどうか。
●PDS 機能も、誰にでも第三者提供してもよいという形、PDS 事業者が第三者提供先を事前に選別しておく形など、様々なものが考えられる。損害賠償請求について、PDS だからといって個人に全部責任を負わせるといった、一つの方向にはならないと考える。
●この認定を受けないとデグレデーションしてしまう、という心配の声は、本認定に対する期待度を示しているのだろう。認定は任意のものであり、認定を受けないで事業をすることも問題はない。一方、認定を受けたい人が受けられるという視点も重要であるように思う。

－データ取引市場について

●今回の対象として、昨年の情報通信審議会答申にもあるデータ取引市場運営事業者は対象ではないという理解でよいか。データ取引市場はデータを売買しない、徹底した透明性が求められており、情報銀行で求められている機能と異なる。
●データ取引市場、情報銀行、PDS の機能を全部兼ね備えた事業もありうるので、取引市場だけが対象外というのは難しいのではないか。データ取引市場だけを単独でやる事業者は、この検討からは対象外。
●情報銀行兼データ取引市場は、まだ存在しておらず、わかりにくい上に相当な競争上の問題がありそう。本来であれば情報銀行兼データ取引市場にも何かのマークがあったほうが良いが、現時点ではそこまで基準を広げて考えるのは難しい。そのような兼業業者が出てきた際に追加のガイドラインを整理してはどうか。

＜経営条件について＞

●経営面の要件について、スタートアップ企業では「経常赤字 2 年」はハードルが高い。「財産的基礎」の要件として、財産的基礎のある会社から出資を受けているなどはどうか。
●民泊関連で同様の議論があり、ベンチャー企業は基本的に資金を成長につぎ込むため赤字が多い。そのため、キャッシュフローなど支払い不能に陥っていないということにしたの

で、それも参考すれば、多様な事業者の参加が可能となり盛り上がるのではないか。
●重要なのは、生活者にとって不利益を被ることにならないよう、何かあったときに保障ができ、事業が継続できること。損害賠償請求の対応は保険でカバーできる。事業の継続性の裏づけの判断は難しくキャッシュフローの観点もあるかもだが客観的に判断できることが重要。
●事業継続性が失われたときに、顧客の個人情報がしっかりした扱いを担保できるような観点がより重要。

＜確認事項について＞
●モデル約款の定義部分で「クレジットカード番号、銀行口座番号」を含めるかだが、この場で議論が詰まっているわけではなく、セキュリティ要件をもう一度考えることになる。今回は Ver1.0 としてとりまとめ、速やかにその先の検討を行いたい。
●「監査委員会」という言い方について第三者監査は、相当な対価・位置づけとなるが、ここではデータの扱い方（第三者提供や利用目的）を審査するものではないか。
●情報銀行の「データ監査審査会」は仮称なので、その趣旨がわかるような表現にしたい。

＜認定団体の認定スキームについて＞
●認定団体の認定スキームについて、仮に認定団体が複数出現した場合「モデル約款に準じた」ではなく、「モデル約款の記載事項に準じた」扱いになるのではないか。
●認定団体の独立性、中立性、公平性が担保されていることが必要。今後このとりまとめを受けて、認定団体ができるときには認定責任なども検討すべき。
●認定団体が中立性を担保するというのは必須の条件だとおもう。
●認定要件、監査体制についてマルチステークホルダプロセスだということがはっきりするような記載を設けることでよいのではないか。

以上