Vol.2015-SPT-16 No.3
Vol.2015-EIP-70 No.3
2015/11/20

国際連携情報共有プラットフォームにおける情報主体のプライバシー保護に関する一考察

加藤尚徳† 高崎晴夫† 村上陽亮†

概要：iKaaS(intelligent Knowledge-as-a-Service)は総務省平成 26 年度の戦略的情報通信研究開発推進事業（SCOPE、国際連携型研究開発）として採択された、プライバシーに配慮した情報提供を可能にする高度知識集約プラットフォームである。本研究プロジェクトにおいては、日本と欧州の相互のデータ活用が目標として掲げられているが、情報主体のプライバシー保護に配慮したデータ活用が行えるかが大きな課題となっている。プロジェクトにでは DPEC(Data Protection and Ethical Community) が内部のプライバシー問題をガバナンスする機関として設けられ、この課題に対応している。本稿においては、日本と欧州の法制度比較から、越境データ流通における現状の課題一般について考察するとともに、その考察結果を踏まえた DPEC のガバナンス体制について紹介する。その上で、今後の越境データ流通において、検討すべき課題を明らかにする。

キーワード：個人情報保護法，KaaS，プライバシー，越境データ流通，ビックデータ，データ保護

An analysis of privacy protection for the data subject on the International cooperation information sharing platform

Naonori KATO† Haruo TAKASAKI†
Yosuke MURAKAMI†

Abstract: iKaaS(intelligent Knowledge-as-a-Service) was adapted as a Strategic Information and Communications R&D Promotion Programme (SCOPE) which is one of the projects funded by Ministry of Internal Affairs and Communications. That is an advanced knowledge-intensive platform that enables the information provided in consideration for privacy. The cross-border data distribution between EU and Japan is one of the goals of the project, and to protect privacy of the data subject is a major issue. DPEC(Data Protection and Ethical Community) was established as a unit to governance the privacy issue inside. In this paper, we consider issues on the cross-border data distribution from the viewpoint of the legal system comparison between EU and Japan. As a result of the consideration, we introduce the governance framework of DPEC. Moreover, we clarify the issues to be discussed in the future cross-border data distribution.

Keywords: Act on the Protection of Personal Information, KaaS, Privacy, Cross-border data distribution, Big data, Data protection

1. はじめに

ビックデータあるいは IoT（Internet of Things）という言葉が世間を賑わせている。これらの言葉に象徴されるように、活用されるデータあるいはそのデータの利用方法について、ビジネスにおいても研究においても様々なアプローチが試みられている。既存の枠組みを超えたデータの利活用と新たな知見の検討が進められている。一方で、そのうちのいくつかの事例については、いわゆる炎上、あるいは明確に法律に違反すると見受けられるケースも散見される。例えば、NICT（国立研究開発法人情報通信研究機構）が行おうとした実験では、監視カメラの適正な利用について問題提起がなされた1し、JR 東日本による Suica の乗車履歴提供の事例においては、現行法の解釈を誤ったと思われる運用がなされたことが社会問題化した2。

他方で、世界に目を向けてみると、データ活用が民間を中心として推し進められる一方で、やはりデータ保護に関する懸念が散見される。「プライバシー外交3」という言葉に代表されるように、データ保護は世界各国の外交のための重要な手段となっている。2015 年 10 月、EU の欧州司法裁判所は、個人情報の移転に関する EU・米国間の取り決めである「セーフハーバー協定」について、米当局の監視によって EU 市民の個人情報が十分に保護されておらず、同協定が無効であるという判断を下した4。このような判断が各国の経済活動と密接にリンクしていることは想像に難くなく、我が国の事業者がサービスを提供する上で障壁となることは非現実的なことではない。

データの利活用が推進されていく中で、どのように複数の主体間で適正にデータを共有し、国際的なデータ流通が

†1 (株)KDDI 総研
KDDI Research Institute Ltd.

進展する中で、越境データ流通における問題をどのように解決するかは喫緊の課題である。我が国における個人情報保護法、欧州におけるデータ保護指令の双方において見直しの議論が進展しており、課題は山積している。そこで、本稿では､総務省平成 26 年度の戦略的情報通信研究開発推進事業（SCOPE、国際連携型研究開発）として採択された iKaaS(intelligent Knowledge-as-a-Service)について取り上げるとともに、この研究開発の中で検討されている、複数の事業者間における適正なデータ利活用と、日欧間の越境データ流通を実現するプラットフォーム作りについて、その内容を紹介する。その上で、今後益々進展していくであろうデータ利活用について、議論と提案を行いたい。

2. iKaaS(intelligent Knowledge-as-a-Service)

2.1 iKaaS プロジェクト概要

本プロジェクトは、日本側からは総務省平成 26 年度の戦略的情報通信研究開発推進事業（SCOPE、国際連携型研究開発)、欧州側からはホライズン 2020 に参加する事業者が中心となって進めている。これらの事業者は図 1 のとおりである。本プロジェクトは 3 カ年にわたる内容が計画されており、その概要は図 1 の通りである。計画の中では、プラットフォームの設計、実装、試験運用が予定されている。また、プラットフォーム上で活用するデータについては、各種アプリケーションから、環境センシングデータ、空間情報データ､健康管理情報等が共有される予定である。日本、欧州の双方でのデータ取得が予定されており、日本側は宮城県仙台市の田子西地区、グリーン・コミュニティ田子西から、欧州はスペイン、マドリッド市に設置されたセンサーからデータが共有される予定である。これらのデータは、iKaaS プロジェクトに参加している全ての事業者が技術的には利用可能なかたちになる予定で、各事業者のデータ活用によって生み出された新しいサービスの登場が期待されている。これらの各種課題および実行のスケジュールについては、図２のとおりである。

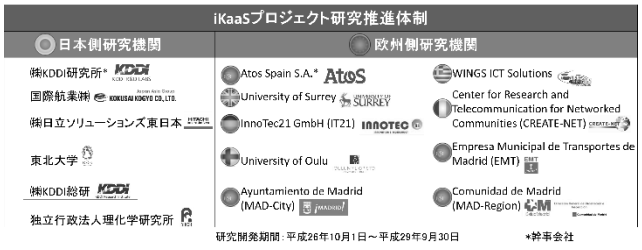

図１．プロジェクト参加事業者一覧

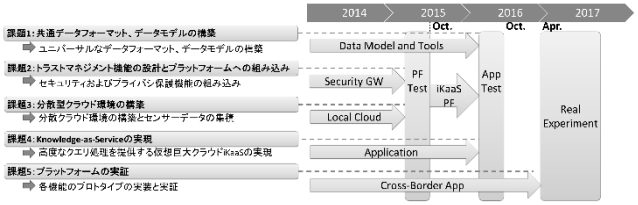

図２．iKaaS プロジェクトにおける課題とスケジュール

2.2 iKaaS プラットフォーム概要

昨今の情報技術およびセンシング技術の発展に伴い、環境、エネルギー、都市空間及び健康に関する様々な情報がインターネット上に膨大に蓄積されてきている。現代社会においては、いわゆるビッグデータと呼ばれるこれらの集合データを利活用して新たなサービスやビジネスを創出していくことが求められており、現在、様々な背景を持ったデータの関連づけから抽出された付加価値データ（知識）をサービスとして提供・還元するビジネスモデル、すなわち Knowledge as a Service（KaaS）モデルが提案されている。しかし､KaaS モデルを実現させるためにはセンシングデータの移送方式やデータの蓄積・管理・提供を担うプラットフォームの構築などの実装面に関する問題、さらに、帰属が異なるデータの所有権やアクセス権などを含むプライバシーポリシー（個人情報保護方針）の問題、また、KaaS モデルによるアプリケーションやサービスモデルの実現など、数多くの問題が存在する。本プロジェクトでは、これまで概念として提案されてきた KaaS モデルを実現させるため、プライバシーに配慮した情報提供を可能にする高度知識集約プラットフォーム〔intelligent Knowledge-as-a-Service; iKaaS〕を開発することを目的に研究を実施されている。

本プロジェクトでは、これまで関連づけられてこなかった異なる文脈（業界）のデータ（例：室内環境×3D 都市モデルデータ×健康状態など）を組み合わせることで新たな知識を生み出し、それをサービスとして提供可能なプラットフォームを作成することを目指している。そして、このプラットフォームを利用した新たなアプリケーションやサービスモデルの提案を行うことを目的としている。

iKaaS プラットフォームは、グローバルクラウドとローカルクラウドで構成され、グローバルクラウドがデータの保管を、ローカルクラウドが各種アプリケーションの役割を果たす。グローバルクラウドはセキュリティゲートウェイの機能を有しており、ローカルクラウド側の要求に対して、データの提供の可否とその方法についてセキュリティゲートウェイが判断する。セキュリティゲートウェイは基本的なプライバシーに関するポリシーを有しており、データの提供の可否とその方法はこのポリシーに基づいて判断

される。このような機能は、データ主体の権利に配慮しつつも、複数の事業者、あるいは国境を越えたデータ流通を円滑にするために設けられている。

2.3 iKaas プラットフォームの特徴

iKaaS プラットフォームの特徴は、大きく分けて二点ある。第一に、これまで関連づけられてこなかった異なる文脈（業界）のデータを組み合わせるために、既存の事業者間の協力の枠組みを超えたプラットフォーム作りがなされるということがある。第二に、本研究プロジェクトには、日本と欧州それぞれの事業者が参加しており、相互のデータ活用が目標として掲げられている。このような試みは、実証研究レベルのものとしては他に例がない。他方で、このような新しい試みゆえの課題も多い。これまで関連づけてこなかった異なる文脈のデータを組み合わせるということは、従来は個人情報あるいはプライバシー情報のような取り扱いをされてこなかった情報についても、組み合わせによって、新たに個人情報性あるいはプライバシー性を帯びる可能性がある。また、複数の事業者間で情報共有がなされる場合のデータ主体との間の同意取得はどのように行っていくべきなのか、その同意取得の形式と範囲については明確なソリューションがない。加えて、欧州との越境データ流通に関しては、EU データ保護指令5において、十分な保護水準と EU が認めた国へのみ越境データ流通が認められることなっている（いわゆる「十分性認定」）。我が国は EU からのこの十分性認定を受けておらず、例外事項に該当しない場合には原則として EU からの越境データ流通が認められない。本研究においては、法制度の観点からのこれらの三つの課題を解決した上で、データ流通の実証研究を行うことが目指されている。

3. 情報共有プラットフォームにおける課題

情報共有プラットフォームにおける課題は、主に技術的課題と制度的課題に大別できる。本稿においては、このうちの制度的課題を取り扱い、特に、コンテクスト（文脈）による情報の性質の変化に関する課題、日欧間の情報流通を行う上での越境流通における課題と、複数の事業者間における情報共有に関する課題について検討する。

3.1 コンテクスト（文脈）による情報の性質の変化

本プロジェクトにおいては、これまで組み合わせが検討されてこなかった異業種間のデータを組み合わせて、新たな知識を生み出してサービスとすることを目的としている。このような様々なデータを組み合わせる試みは、データ利活用の新たな可能性を有している。一方で、従来は単なるセンシングデータや統計データとして扱われていたデータが、組み合わせによって個人情報性あるいはプライバシー性が生じる可能性を同時に有している。

仮にこのようなデータを仮名化データ（連結可能匿名化データを含む）や匿名化データとして取り扱ったとしても万全とは言えない。コンテクスト複雑になればなるほど、上記のデータの個人情報性あるいはプライバシー性については増加する傾向にあると考えた方が良い。例えば、JR 東日本の Suica の事例においては、JR 東日本は SuicaID 等を番号変換したことにより、不可逆なものになっているという説明をしている6。しかしながら、このような場合であっても、再識別化可能であることが指摘されており7、単に仮名化あるいは匿名化しただけでは、個人情報あるいはプライバシーに関するインパクトが取り除かれたと言い切ることはできない。

諸外国の議論を見ると、このようなプライバシー性に配慮した議論が今後深化していくことは明らかである。EU データ保護規則案8では、パーソナルデータ（Personal Data）は「'personal data' means any information relating to a data subject（データ主体）」と定義されている。また、米国消費者プライバシー権利章典法案9においては、パーソナルデータは、「In General.—“Personal data” means any data that are under the control of a covered entity, not otherwise generally available to the public through lawful means, and are linked, or as a practical matter linkable by the covered entity, to a specific individual, or linked to a device that is associated with or routinely used by an individual, including but not limited to— ..」と定義されており、いずれにおいても、パーソナルデータは日本の個人情報に比べて幅の広いものであるといえる。つまり、本プロジェクトで取り扱う情報についても、個人情報保護法の個人情報の定義に縛られることなく、広くパーソナルデータとしての保護を検討する必要性がある。

3.2 情報共有に関する課題

情報の利活用が単一の事業者に閉じる場合、情報の利活用の範囲を定義することはそれほど難しい事ではない。データ主体から同意を得る場合であっても、明確な説明のもとでデータの提供を受け、利用が可能である。一方で、情報共有が複数の事業者にわたって行われる場合には、この定義は 2 つの点で非常に困難になる。1 つ目は、情報の共有事業者の定義の問題である。当該情報共有にどのような事業者が含まれており、また今後含まれる可能性があるかについて、定義可能であるかという問題である。我が国の個人情報保護法を見ると、情報の取得時の同意を得る必要性については特段の定めがない。他方で、共有の範囲について、不明瞭な説明を行うことは、適正な取得についての定め（法 17 条）の観点から問題があるばかりか、欧州データ保護指令を見た場合には、明確な同意（データ保護指令 7 条）の観点から問題がある。2 つ目は、情報の利用目的の特定である。複数の事業者が参画したサービスにおいて、そもそも事前に、今後予定される全ての利用目的を提示することは困難であるといえる。異業種間のデータを組み合

わせて、新たな知識を生み出してサービスを行うといった場合、この新たな知識がどのように創出され、またそれがどのようなサービスにつながってくるかいうことは、容易に予測できることではない。むしろ、従来では想像もしかなったような、知識あるいはサービスが生じるほうが、期待されているというべきである。

このような情報共有においては、我が国の法制度からは二つの解決方法が検討可能である。第一には、利用に際して個別の同意を取得するという方法である。我が国の場合には、この利用目的の変更については、オプトアウト方式での同意も認められており、必ずしもオプトインで同意を得る必要はない（法 18 条)。第二には、共同利用（法 23 条 4 項 3 号)方式をとるということも考えられる。これは、すでにいくつかのサービスにおいて、実際に共同利用方式を採用しているものもある。しかし、この共同利用方式は、かねてから利用方法についての課題が挙げられていた10。共同利用については、法 23 条に定めのある通りであるが、①共同利用の目的、②共同利用する個人データの項目、③共同利用者の範囲、④責任を有する者の氏名・名称、の 4 項目を、ホームページ等で事前に公表することにより、本人の同意を得ることなく個人データを複数の事業者間で共同して利用できる制度である。この共同利用者の範囲を「提携企業」とだけ標記して、個々の企業名を特定しないで共同利用を進める問題は以前から指摘されていた。昨今では、この問題が共通ポイントカードのようなかたちで表出化してきており11、課題の多い制度といえる。

本プロジェクトにおいては、参加する事業者が特定されており、また、それらが重要事項説明書等で適切にデータ主体に対して説明されているため、共同利用形式による情報共有を適法に行える可能性が高い。また、利用目的に関しても、サービスの拡充に応じてオプトアウト形式で同意を得る方が、迅速なサービス展開という意味では有力な選択肢となる。しかしながら、このようなオプトアウトを前提とした同意取得が国際的なコンセンサスを得ているとは言いがたい。EU データ保護指令12を見ると、第 7 条には明確な同意の取得が必要であることが述べられている。この明確な同意にオプトアウトが含まれるかどうかは条文の文言上は明らかでないが、EU Cookie Directive の 2002 年から 2009 年の変更の過程を参照すると、同意取得形式のオプトアウトを許容する形式からオプトイン形式に転換が見られているように、オプトアウトが許容される範囲は狭く解されるようになってきていると考えるのが妥当である。

このように、情報の共有にあたっては、明確なオプトイン型の同意を得ることが望ましく、この同意を前提とした仕組み作りが求められているといえる。

3.3 越境流通における課題

EU データ保護指令を見ると、25 条において「構成国は、取り扱われている又は移転後に取扱いが予定されている個人データの第三国への移転は、この指令に従って採択された国内規定の遵守に実体的な効果を持つことなく、当該第三国が十分なレベルの保護措置を確保している場合に限って、行うことができることを定めなければならない」と定めている。これは、いわゆる「十分性」の認定と呼ばれるもので、EU が十分性を認定した国家に対してのみ、EU 域外のデータ移転を認めている。

十分性の審査は 29 条に定めのある「個人データの取扱いに係る個人の保護に関する作業部会（いわゆる、29 条作業部会)」が 30 条に「共同体域内および第三国における保護レベルに関する意見を委員会に提出すること」と定めているとおりに行うこととされている。この審査基準は図 3 のとおりである。我が国は、この十分性について現在のところ審査を受けておらず、今後、審査を受ける見通しもたっていない。また、審査に当たっては一定程度の期間を要し、今日、明日にでもすぐに有効となるような制度ではない。十分性を満たさない場合には、米国が EU と結んでいるようなセーフハーバー協定を締結するか、事業者単位で、欧州委員会が策定した標準契約条項（SCC）を採用することや拘束的企業準則(BCR)を策定することが考えられるが、これも容易ではない。一方で、26 条には、「データ主体が、予定されている移転に対して明確な同意を与えている場合」の定めがある。そこで、明確な同意のもと、データ移転が行われるようなモデルを設計する必要がある。

内容の諸原則	
目的制限原則	データは、特定の目的のために取り扱われ、その後の利用又はさらなるやり取りは、移転の目的と矛盾しない限りにおいて行われるべき。
データの質及び均衡の原則	データは正確であり、かつ、必要な場合には最新のものとすべき。データは、移転され又はさらに取り扱われるための目的との関連で、適切かつ関連すべきであり、過度であってはならない。
透明性の原則	個人は、取扱目的及び第三国のデータ管理者の身元に関する情報、並びに、公正性を確保するために必要なその他の情報を提供されるべき。
安全性の原則	取扱がもたらすリスクに対応するための技術的かつ組織的安全管理措置を実施すべき。
アクセス・訂正・異議申立ての権利	データ主体は、自らに関して取扱われるすべてのデータの写しを取得する権利、不正確なデータの訂正権、自らに関するデータの取扱に関する異議申立権を有するべき。
転送の制限	最初のデータ移転の受領者による個人データのさらなる移転は、第二の受領者もまた、十分な保護レベルを提供する諸原則にしたがっている場合に限るべき。
追加的原則の例	
センシティブ・データ	センシティブな種類のデータが関係する場合には、データ主体の明示的同意のような追加的安全保護措置を実施すべき。
ダイレクト・マーケティング	データがダイレクト・マーケティングの目的のために移転される場合において、データ主体に「オプト・アウト」を認めるべき。
個人に関する自己決定権	個人は、自動的決定に関する倫理を知る権利を与えられるべきであり、個人の適法な利益を保護するためにほかの措置を講じるべき。

図３．十分性の審査基準

4. 課題解決の指針

4.1 プロセスとステークホルダーの定義

法令遵守の観点からは、国内の情報の利活用においては、一般に個人情報保護法が参照される。我が国の個人情報保護法は、データ主体への利用目的の通知を定めているが(法 18 条)、取得に際しては適正な取得についての定めがあるのみで（法 17 条)、取得に関する通知及び同意は法定義務ではない。このような視点から、多くの情報利活用のシー

ンにおいては、データ主体に対して単に利用目的が通知されるのみであって、利用主体はこのような利用目的に対してオプトインあるいはオプトアウト型の同意が行われるのみである。

一方で、個人情報を含んだデータの移転・利活用のスキームは、取得、保管、利用、開示（第三者提供）と定義可能であり、これは EU においても同様といえる。この取得、保管、利用、開示の四つのプロセスに対して、取得から利用の三つ、あるいは四つのプロセスについて同時に同意を得る構図になっている。しかし、ながら、本プロジェクトで想定するプラットフォームにおいては、各プロセスを一つないしそれ以上の事業者が担当し、各プロセスの主体となる事業者が異なる構図となりえる。そこで、このような複雑なステークホルダー関係について、類型化し、定義すると下記のような定義となる。

「幹事事業者」:本事業における本プロジェクトの取りまとめを行う事業者を指す。

「情報管理事業者」: iKaaS プラットフォームの設計・開発・保守・運用を行う事業者を指す。

「データ管理事業者」:本事業におけるセンサー等の情報収集機器を設置し、情報主体から収集したデータを iKaaS プラットフォームに集約し、流通させる事業者を指す。

「データ利活用事業者」: iKaaS プラットフォームから取得できるデータを活用したアプリを提供する事業者を指す。

「情報主体」: 本プロジェクトに協力することに同意し、情報提供をする者をさす。

上記のステークホルダーの関係性と、責任分解に関する考え方は、図４（図中に明示した事業者は実際のサービスシーンに基づいている）のように整理できる。また、この定義上での同意取得のプロセスは下記のように説明できる。

① 取得するデータを個別に特定する（データの種類及びデータの粒度）
② 個別のデータを取得することについて、データ主体から明確な同意を得る
③ どのデータをどのような利用目的のために組み合わせるのか定義する
④ 利用目的について、データ主体から明確な同意を得る

このような同意取得のプロセスにおいて、明確なオプトイン型の同意を得る

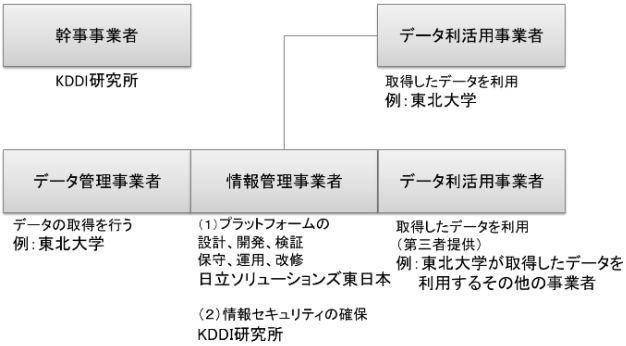

図４．ステークホルダーの責任分解の定義

4.2 DPEC(Data Protection and Ethical Community)の設置

前述のような検討を踏まえて、iKaaS プロジェクトでは、iKaaS プラットフォーム上の必要なデータ保護及び倫理的な問題について審議するための機関（iKaaS データ保護及び倫理委員会、Data Protection and Ethical Community、以下 DPEC）を設置した。DPEC の構成は図５の通りで、幹事会社である KDDI 研究所から責任者を、内外のポリシー検討の担当会社である KDDI 総研から CPO を選んでいる。また、参加事業者のうち、システム構築や情報取得への関与の大きな事業者を中心として委員が選出されている。日本側の情報管理の問題について検討をするという意味合いから、委員は日本人から選ばれているが、プロジェクトのカウンターパートである EU 側からもリエゾンオフィサーが選ばれており、議論に参加する。

DEPC は過半数の議決をもって、プロジェクト内の情報保護に関する問題を判断する内部監査機関であるといえる。データの取得、保管、利用、開示に当たっては、事前に DPEC がその内容について審議することになっている。また、DPEC の体制及びその審議結果については、原則としてプラットフォームの利用者に開示されることとなっている。これによって、データ利活用の適正性と透明性を確保することとしている。

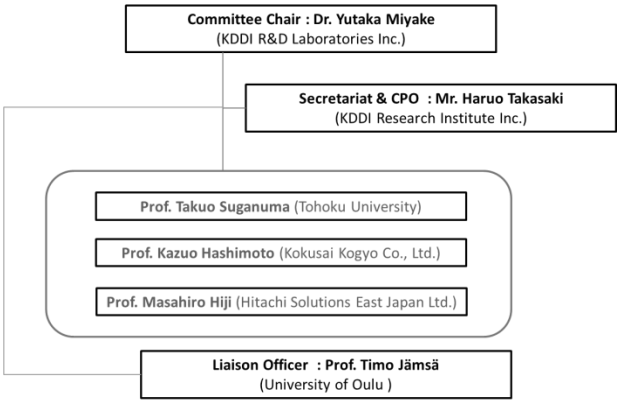

図５．DPEC の構成

4.3 DPEC における審査

DEPC ではあらかじめ、情報共有規則（事業者間の合意事項）、個人情報等保護規則、事業者間の責任分界に関する規程、個人情報等に関する事故発生時の対応規程、プライバシーポリシー、利用規約、審査申込用紙書式、利用者への iKaaS プロジェクト説明図、のようなドキュメントを作成している。これらに基づいて、情報の取得、利用、開示を新たに行うあるいは受けようとする事業者は、申し込み用紙の所定事項を記載の上、DPEC に申し出る。DPEC と当該事業者は協議の上、事業者の行うサービスの特性を踏まえた重要事項説明書を作成する。このプロセスは、図６の通りである。

利用者には、DPEC の審査プロセスを経たサービスのみが提示される。本プロジェクト内で、共通の基準においてプライバシーポリシーが作成され､重要事項説明が行われ、同意が得られることが望ましい。この点においては、プロジェクト全体として、共通のドキュメントを作成すれば足りる。他方で、複数の事業者によって提供される各々の取得の方法、あるいは利活用の方法は、多様なものが予想され、事前にこれらの全てを踏まえたドキュメントを作成することは困難である。かりに、このようなドキュメントが作成可能だったとしても、それは包括的な内容とならざるを得ず、利用者に対して明示的な説明と、その上での明確な同意を求めることができなくなる。本プロジェクトにおいては､これらの課題を解決するために､DPEC を設置し、審査のプロセスを設けることになった。

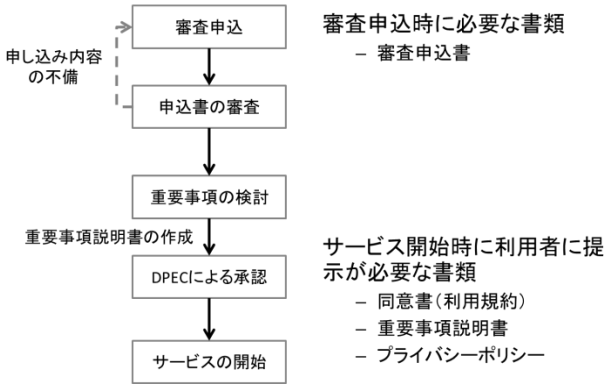

図６．DPEC の審査プロセス

5. 今後の課題

以上のように、研究プロジェクトとして、実験的ではあるものの国際的な情報共有プラットフォームが設計、試験的に実用されようとしている。これまで活用が困難であった情報について、利活用が進めば、我々の社会に寄与する点が大きいことは予測できる。一方で、利活用される情報が増えれば増えるほど、またそれらの情報が一か所に集約されれば集約されるほど、プライバシーをはじめとしたパーソナルデータの問題が顕在化してくることも予想される。既存の制度との整合性ももちろんであるが、今後の制度の方向性、あるいは、さらに進んだ利用者への配慮を含んだ検討と実装が求められている。

今後は、実際にプラットフォームの運用を進めた上で、さらなる課題が生じてくることが予想される。他方で、我が国における個人情報保護法の改正をはじめとして、EU におけるデータ保護規則制定の議論、米国における消費者プライバシー権利章典法案の議論など、パーソナルデータを取り巻く環境は新たな局面に向かっている。こういった議論の中で、制度や法令を遵守すべく検討を進めていくことはもちろん、他方で、このような議論が机上の空論に終始することもあってはならない。実際のユースケースを想定して、現実的な利用の可能性を踏まえた上で、パーソナルデータ保護の議論を展開していく必要がある。本プロジェクトに関しても、既存法制との整合性を検討する上で生じた課題に関しては、しっかりと意見の発信を行い、このような大きな議論に寄与していきたいと考える。

参考文献

1 映像センサー使用大規模実証実験検討委員会調査報告書
http://www.nict.go.jp/nrh/iinkai/report.pdf
2 Suica に関するデータの社外への提供について中間とりまとめ
http://www.jreast.co.jp/chukantorimatome/20140320.pdf
3 石井夏生利「「プライバシー外交」のためのプライバシー」
http://www.soumu.go.jp/iicp/chousakenkyu/data/research/icp_review/08/08-4ishii2014.pdf 「プライバシー外交」ということは、現特定個人情報保護委員会の堀部政男委員長が最初に用いたとされている。
4 同判決文
http://curia.europa.eu/juris/document/document.jsf?text&docid=169195&pageIndex=0&doclang=EN&mode=req&dir&occ=first&part=1&cid=82310
5 同指令日本語訳
http://www.soumu.go.jp/main_content/000196313.pdf
6 Suica に関するデータの社外への提供について
https://www.jreast.co.jp/press/2013/20130716.pdf
7 菊地浩明「k-匿名が使えない事例 Suica 乗降履歴はなぜ匿名化できないのか？」情報ネットワーク法学会 2013 年学会大会分科会１資料
http://in-law.jp/archive/taikai/2013/bunkakai1-Kikuchi.pdf
8
http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52012PC0011
9
https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf
10 経済産業省・パーソナル情報研究会「個人と連結可能な情報の保護と利用のために」
http://www.meti.go.jp/report/downloadfiles/g81110a02j.pdf
11 鈴木正朝他『ニッポンの個人情報』（翔泳社・2015 年）36 頁
12 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data、本指令の日本語訳は、堀部政男研究室仮訳による。
http://www.soumu.go.jp/main_content/000196313.pdf