情報処理学会論文誌 Vol.57 No.12 2664–2674 (Dec. 2016)

国際連携情報共有プラットフォームにおける情報主体に配慮したプライバシ保護対策の提案

加藤 尚徳[1,a)] 高崎 晴夫[1] 村上 陽亮[1]

受付日 2016年3月10日, 採録日 2016年9月6日

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．このような国際連携情報共有プラットフォームにおいては，プライバシ保護技術にとどまらず，様々なプライバシ保護対策が必要となる．本稿においては，日本，欧州のデータ保護法制が求めるデータ保護水準を考慮しつつ，プライバシ保護対策の原則を明らかにする．そのうえで，実際のデータ流通においてどのようなプライバシ保護対策が必要か，包括的な検討を行う．データ主体の視点を取り入れたマルチステークホルダプロセスをふまえて，継続的なプライバシ保護対策のアセスメントの必要性について言及する．

キーワード：個人情報保護法，プライバシ，プライバシ・バイ・デザイン，ビックデータ，データ保護，マルチステークホルダプロセス

A Proposal of Privacy Protection Scheme Considering Data Subject on the International Cooperation Information Sharing Platform

Naonori Kato[1,a)] Haruo Takasaki[1] Yosuke Murakami[1]

Received: March 10, 2016, Accepted: September 6, 2016

Abstract: iKaaS (intelligent Knowledge-as-a-Service) has been adopted 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 govern 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, privacy, privacy by design, big data, data protection, multi-stakeholder process

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

[1] 株式会社 KDDI 総合研究所
KDDI Research Institute Ltd., Chiyoda, Tokyo 102–8460, Japan
[a)] xan-katou@kddi.com

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．たとえば，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]．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*1」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．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，わが国の事業者がサービスを提供するうえ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．わ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．そのうえで，今後ますます進展していくであろうデータ利活用について，プライバシ保護対策の提案を行う．

2. iKaaS（intelligent Knowledge-as-a-Service）と情報共有プラットフォームにおける課題

2.1 iKaaS プロジェクト概要

iKaaS 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日欧共同の国際連携プロジェクトである．iKaaS プロジェクトは 3 カ年にわたる内容が計画されており，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すべ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．

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ともない，環境，エネルギー，都市空間およ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等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等を含むプライバシポリシ（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等，数多くの問題が存在する．iKaaS 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が実施されている．

iKaaS 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 × 健康状態等）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に関するポリシを有しており，データの提供の可否とその方法はこのポリシに基づいて判断される．

*1 2016 年 7 月 12 日，「セーフハーバー協定」に代わる新たな欧州・米国間の枠組み「プライバシーシールド」の採択にかかる宣言が，欧州委員会によって公表された．

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 2 点ある．第 1 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 2 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．先行する研究 [4]，あるいは同時期の研究 [5], [6], [7] と比較しても，プライバシ保護を念頭においた取り組みとして，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ある．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，組合せによって，新たに個人情報性あるいはプライバシ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になっている（いわゆる「十分性認定」）．わが国は 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．本稿においては，法制度の観点からこれらを 3 つの課題にまとめ，その解決策を提示する．

2.3.1 コンテクスト（文脈）による情報の性質の変化

iKaaS プロジェクトにおいては，これまで組合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，組合せによって個人情報性あるいはプライバシ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いえない．コンテクストが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性については増加する傾向にあると考えた方がよい．たとえば，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．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，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に関するインパクトが取り除かれたといいきることはできない [8]．

諸外国の議論を見ると，このようなプライバシ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[*2]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権利章典法案においては，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，iKaaS 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 [9], [10], [11], [12] 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．

たとえば，本プロジェクトにおいて検討の過程でプライバシ性が生じる可能性があるものとして考慮されたものを以下に紹介する：環境センサ，ウェアラブルセンサ，Home Energy Management System（HEMS）の各センサから収集されたデータの組合せである．環境センサからは大気中の CO_2 の量が，ウェアラブルセンサからは心拍数や血圧が，HEMS からはその家庭における電力使用量が分かる．これらのデータからは，その家庭に現在人がいるかどうか，何人の人がいるか（ウェアラブルセンサを付けていない人についても推定可能），どんな活動をしているか（寝ているか，テレビを見ているか，家事をしているか，風呂に入っているか，運動をしているか）等が推測可能である．このように，単にセンサデータといっても，その組合せを用いて多くの推定が可能であり，コンテクストが複雑になるほど，プライバシ性が増す傾向にある．

2.3.2 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ことではない．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

[*2] 2016 年 4 月 27 日に General Data Protection Regulation（GDPR）は有効となった．本稿は規則案の段階で執筆されており，記述は規則案に基づく．

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．わ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 [13], [14] 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 [15]）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，今後予定されるすべ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，従来では想像もしなかったような，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，わが国の法制度からは 2 つの解決方法が検討可能である．第 1 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．わが国の場合には，この利用目的の変更については，オプトアウト（事後同意）方式での同意も認められており，必ずしもオプトイン（事前同意）で同意を得る必要はない（法 18 条）．第 2 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あげられていた．共同利用については，法 23 条に定めのあるとおりであるが，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 [16]．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，課題の多い制度といえる．

iKaaS 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いいがたい．EU データ保護指令を見ると，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．

2.3.3 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．わが国は，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，審査にあ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．

3. 課題解決の指針

3.1 プライバシ保護要件の定義

プライバシ保護のためには，その要件を定義する必要がある．このような要件を考えるうえで，最も参考になるのは，OECD が定めたプライバシガイドラインにおける 8 原則である．あるいは，アン・カブキアンが提唱しているプライバシー・バイ・デザイン [17] においては，7 つの原則が定められている．これらは，プライバシ保護のための大枠を定義してはいるが，実際のプラットフォーム設計を前提にしたものとはいえない．実際には，これらを，プラッ

トフォームの設計と対比させつつ，原則を分解する必要がある．本稿においては，先の 2 つの原則を参照しつつ，日欧の法制度および現在議論が進められている制度改正の議論もふまえて，14 の判断項目を以下のとおりに定めた．

1．情報保護の範囲
2．開示性と説明責任
3．第三者による処理に関する説明責任
4．データ主体のアクセス権の確保
5．データの正確性の確保
6．セキュリティの確保
7．データ利用目的の明確化と通知
8．目的の制限
9．取得の制限
10．保持の制限
11．利用および開示に関する制限
12．同意の取得
13．優越的地位の乱用
14．その他の手続きとの整合性

特に，後述のプロセスの定義にも共通するが，データの移転プロセスを，取得・保管・利用・開示と定義した．データの移転プロセスが明確化されることによって，情報保護の範囲の定義が行えるようになる．つまり，対象となるデータだけでなく，起こりうるデータの組合せが定義されることによって，情報保護の範囲を定めることができる．また，実際のサービス提供を想定し，優越的地位の乱用についても制限を設けた．これは，データ主体がサービスに同意せざるをえないような状況において，データ主体のパーソナルデータの提供を強制しないようにするものである．さらに，その他の手続き，たとえば大学内における倫理審査のような手続きについても整合性を求めることによって，実際の環境における衝突が生じないように配慮した．

3.2 プロセスの定義

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．わ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），取得に関する通知およ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 4 つのプロセスに対して，取得から利用の 3 つ，あるいは 4 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．

① 取得するデータを個別に特定する（データの種類およびデータの粒度）．
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，得る同意は，明確なオプトイン型の同意でなければならない．

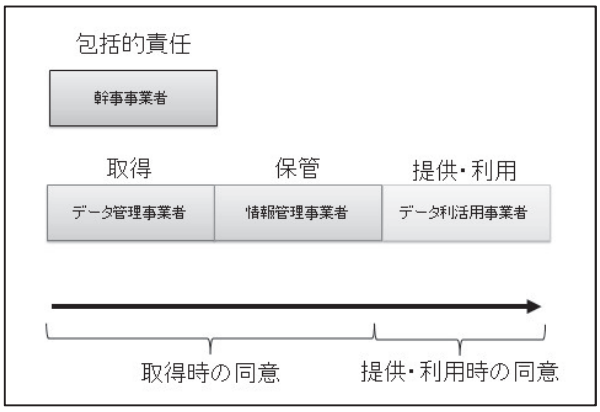

図 1 ステークホルダとプロセスの定義
Fig. 1 Definitions of stakeholders and process.

3.3 ステークホルダの定義

iKaaS 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 1 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うる．そこで，このような複雑なステークホルダ関係について，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 iKaaS プロジェクトのと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」：iKaaS 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指す．

プロセスとステークホルダが明確化されることによって，プラットフォームにおける責任分界を明確化することができる．これらの関係性を図示したものが**図 1** である．

3.4 内部監査機構の設置

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．幹事会社である KDDI 研究所から責任者を，内外のポリシ検討の担当会社である KDDI 総研から CPO（Chief Privacy Officer）を選んでいる．また，各委員は各事業者にアドバイザとして加わっている学術研究機関の研究者で構成されている．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が選ばれており，議論に参加する．

DPEC 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，開示にあたっては，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 の体制およ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．

DPEC は，審査申込書，同意書（利用規約），重要事項説明書，プライバシポリシ等のプロジェクト内外に示す文書を作成している．これによって，内部における事業者間の責任分界を事前に定めており，運用面における責任の所在を明確にしている．規約は，先に示した定義を中心として構成がなされている．DPEC は，特に，データ主体に示す重要事項説明書の作成に対して助言を行う．この助言を通して，iKaaS プロジェクト全体で提供される一般的な利用規約と各事業者が行うサービスとの差分がデータ主体に明確に提示されるような配慮を行っている．また，当該事業者におけるその他の規約と，サービスが抵触しないかについても検討をする．たとえば，健康管理情報等を利用する場合で当該事業者が大学であるような場合には，大学内の倫理規定との抵触がないかどうかについても，必要な書類の提出を求めて，問題がないか審査を行う．

3.5 マルチステークホルダプロセス

内部監査組織を設けて，事前の審査体制を構築したとしても，実際のサービスに至るまでには依然として課題が残っている．情報主体からの同意を得る際に，有効な同意を得ることができるかという問題である．情報主体が，DPEC の定めた内容を正しく理解し，十分に納得したうえで合意を行う必要がある．このような同意でないと，EU データ保護指令の観点からしても，必要な同意を得たとは見なされない．さらに，情報主体の受容性が一定程度確保されているかについても，レピュテーションリスクの観点から考察されることが望ましい．そこで，iKaaS プロジェクトでは，最終的なサービスの開始前にマルチステークホルダプロセス（MSHP）[18], [19], [20], [21] を設けることが予定されている．マルチステークホルダプロセスとは，たとえば内閣府によると「多種多様なステークホルダが対等な立場で参加し，協働して課題解決にあたる合意形成の枠組み」と説明されている．iKaaS プロジェクトでいうならば，プロジェクトの参加事業者と，情報主体，そして DPEC がまずはこれにあたるといえる．

iKaaS プロジェクトにおいては，以下のようなマルチステークホルダプロセスが想定されている．

① 重要事項説明書作成時の合意形成
② 同意取得時の合意形成
③ サービス開始後の合意形成の継続

なお，現段階においては，本研究のマルチステークホルダプロセスは，事業者による自主的な取り組みの一環として行っており，公的な主体はこのプロセスに加わっていない．この点について，2 点付記する．1 点は，2015 年 9 月に成立した改正個人情報保護法において，個人情報保護委員会が設置されたことである．加えて認定個人情報保護団体と当該団体が定める個人情報保護指針についてマルチステークホルダプロセスを用いて検討が進められるべきことが定められた．仮に，今後，このような制度が構築されていくとすると，個人情報保護委員会に事前の相談を行うことや，認定個人情報保護団体において議論を行うという可能性も出てくる．いずれにしても，現状は公的主体を加えた公式な議論ができる環境にはないため，本稿執筆時点においては可能性の 1 つとして付記する．もう 1 点は，欧州側とのマルチステークホルダプロセスの可能性である．本稿は日本側の検討をとりまとめたものであるが，今後，欧州側とも協力して，プライバシ保護の取り組みを行う可能性を検討中である．これが実現すると，欧州のデータ保護を担当する公的機関であるプライバシコミッショナと議論し，SCC（標準契約約款）等の具体的な措置が行える可能性が出てくる．この点については，今後の本研究の課題として取り組む予定である．

4. プロジェクトにおける実践

4.1 DPEC における審査

DPEC 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，プライバシポリシ，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うえ，DPEC に申し出る．DPEC と当該事業者は協議のうえ，事業者の行うサービスの特性をふまえた重要事項説明書を作成する．

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．iKaaS プロジェクト内で，共通の基準にお

いてプライバシポリシが作成され，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，事前にこれらのすべてをふまえたドキュメントを作成することは困難である．仮に，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えず，利用者に対して明示的な説明と，そのうえでの明確な同意を求めることができなくなる．iKaaS 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．

4.2 マルチステークホルダプロセスの実施

前述に想定したマルチステークホルダプロセスに基づいて，どのようなマルチステークホルダプロセスを具体的に実施していくか，iKaaS プロジェクトにおける具体的なあてはめをもとに，現在の実施状況をふまえて解説する．

iKaaS プロジェクトにおいては，取得したセンサデータをもとにしたサービスユースケースがいくつか想定されている．このうち，最も早く具体的な実施が予定されているのが，アンケートによる調査（氏名，年齢，連絡先，住所等）と機器（装着型活動量計，体重計，室内環境センサ）を用いた見守りサービスの検討である．当該エリアの複数の住民から上記のデータを取得し，分析，将来的な見守りサービスに生かすことができないかというサービスユースケースである．

①の段階としては，住民の代表者に対して，同意取得時に提示する書類（同意書，重要事項説明書，プライバシポリシ，同意撤回書類）を見せ，協議を行う．具体的には，分かりにくい箇所はないか，不安に思う箇所はないか，等の修正個所の要望をとりまとめることになる．この要望に基づいて，上記の書類をアップデートする．

②の段階としては，いわゆる説明会のようなものを開催して，同意取得に必要な合意形成を得るというものである．

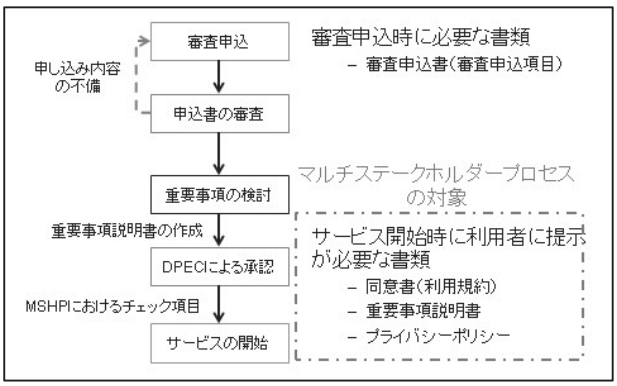

図 2 審査のプロセスと各項目の関係性
Fig. 2 Relationship between review process and items.

同意取得に必要な理解を情報主体に求めるとともに，サービスユースケースそのものを実施するうえでの信頼関係を構築することも目的となる．

③の段階としては，サービス開始後に，情報取得を継続するうえでの疑問，不安等を受け付けるプロセスである．単なる苦情処理ではなく，②の段階で理解ができないサービス内容について，継続的，追加的に合意形成を行っていくことが必要である．

4.3 プロセス全体のアセスメント

プロセスの最終段階においては，DPEC によって審査された内容がデータ主体に適切に理解されているかについての確認作業が設けられている．確認項目は以下のとおりである．

1. どんな情報を提供し，どんな目的で利用されるか．
2. プライバシポリシについて理解できたか．
3. 第三者の関与について．
4. 情報の提供後にどのようなオプションが与えられるか．
5. セキュリティの状況について．
6. 利用目的に不明確・不明瞭なものはなかったか．
7. 保管期間について説明があったか．
8. 同意を強制されなかったか．

データ主体にこれらの項目を確認することによって，データ主体が本来受けるべき説明を適切に受けたかを評価する．仮に，これらの項目について，不十分な点があった場合，不十分な点について再度の説明を試みることや，改善策について検討する．

iKaaS プロジェクトでは，2016 年 1 月に試験的に確認プロセスを実施した．その結果，データ主体から「問題がおこった場合に該当項目を立ち返って確認をすることがある」点が指摘された．これは，サービス開始時の同意においては，同意主体が同意規約やプライバシポリシをよく読まずに同意している可能性を示唆している．この点については，定量的な評価が別途行われることが望ましい．一方で，データ主体の保護の視点からは，データ主体がデータ提供における初期の同意において，同意内容を十分に理解せずに同意しているということを織り込んで，サービスを運営する必要もある．

先の③の段階において，継続的，追加的な合意形成の必要性について触れたが，本節における指摘からも，やはり継続的，追加的な合意形成の必要性について，説明をすることが可能である．つまり，当初の明示的な同意の有効性について考慮することに終始するのではなく，明示的な同意を継続的，追加的な同意形成の中に見いだすということである．また，データ主体にプラットフォーム上の自己のデータに対するアクセス権や削除請求権等の機能を明確化することによって，同意が不十分である点をカバーできる可能性もある．たとえ，明示的なオプトイン型の同意が得

られていたとしても，それだけを理由とした排他的な利用の権利が認められるわけではない．むしろ，明示的なオプトイン型の同意は，プラットフォームを運営する事業者とデータ主体との関係性を構築する，最良のきっかけでしかない．きっかけに終始し，固執することで，当事者間の関係性が悪化する可能性があることを考慮しなければならない．

DPEC の目的は，サービス開始までにデータ主体から明示的なオプトイン型の同意を取得することだけではなく，同意取得後，サービス開始後も継続して，そのサービス実施体制とともにデータ主体への配慮について監査を行っていくことも含まれると結論付けることができる．各事業者が明示的なオプトイン型の同意を取得することの必要性については，社会的な共通認識が広がりつつあるといえる．一方で，iKaaS のような情報共有プラットフォームにおいては，参加する事業者の数も多く，データ主体がこれらの事業者と個々に交渉を行うことは困難であるといえる．データ主体のいわゆる相談窓口が一元化されることによって，よりデータ主体に即したプライバシ保護が可能になると筆者らは考えている．DPEC はそのためのプラットフォームを横断した内部監査組織であり，DPEC がプライバシ保護のフォーカルポイントになることにより，プラットフォーム全体で事業者ごとのばらつきのないプライバシ保護の提供が可能になると考える．

4.4 課題に対する取り組みと評価

本研究においては，コンテクストによる情報性質の変化，情報共有に関する課題，越境流通における課題，の 3 つを解決すべき課題としてとらえ検討をしてきた．検討においては，これらのいずれの課題に対しても，他の解決策との比較検討の結果，有効なオプトイン形式の同意を得ることが唯一の解決策であるという結論を得た．本研究においては，有効なオプトイン形式の同意をより確実なものにするために，iKaaS プラットフォームにおける保護要件の定義，プロセスの定義，ステークホルダの定義を，プライバシ保護をプラットフォームに反映できるよう，その設計段階から行った．加えて，これらを担保する機能として，内部監査機構（DPEC）を設置，データ主体との間にマルチステークホルダプロセスを実施した．以下，個々の課題について，具体的にまとめる．

コンテクストによる情報性質の変化については，情報の取得時の評価だけでは不十分との結論に達した．そのことにより，情報の取得時と情報の利用時の 2 段階に分けたパーソナルデータ該当性の評価およびプライバシ性の評価を行うことにした．これらの評価は，定義されたプロセスごとに，データの取得・保管・利用が生じる際に DPEC への審査が要求されることによって，必ず実施がなされる構成になっている．また，データ主体に対して，取得時，利用時にそれぞれ取得，利用を行う事業者が中心となって同意取得を行うことにより，データ主体の予期しない事態が生じないように配慮した．なお，データの保管に関しては，iKaaS プラットフォームにおいては，データの取得と一体的に取り扱うことが可能であることから，データ主体の同意取得は 3 段階としなかった．仮に，今後，何らかの特徴的な保管を行うプラットフォームが生じ，データ主体への配慮が求められるような場合には，同意プロセスを 3 段階に分割することもありうる．

情報共有に関する課題については，データ主体に情報共有主体にどのような事業者が含まれており，誰が責任をとるのかを明確に提示できることを念頭に解決策を検討した．そのうえで，2 段階に分けた同意を取得することで，データ主体の意思が必要十分に反映できるように配慮した．情報共有型プラットフォームにおいては，複数の事業者がプラットフォームを構成するため，データ主体が予想しないデータ活用が行われる可能性がある．これに対して，一義的に責任を負う事業者を定めるとともに，各プロセスを可視化しデータ主体に提示することで対処した．それぞれのプロセスにおける同意の十分性については，1 つ目の課題と同様に 2 段階同意を行うことで達成された．

越境流通における課題については，欧州における規制において同意取得をオプトイン形式で行うことによって解決されることから，同意取得による解決策を検討した．結果として，2 段階同意を導入することによって，欧州の求める同意の要件を十分に満たした構成となっていると筆者らは考えている．欧州においても，データ主体にとって明確な同意がどのようなものであるかという点は，現在も議論が続いている点である．本研究においては，データ主体に対する説明の徹底とマルチステークホルダプロセスによるデータ主体も参加したルール作りによって，最大限の努力義務を果たせるような構成を設けた．これによって，現状において，情報共有型プラットフォームにおいて十分な同意取得が行えると筆者らは考えている．各種規約や定義についても，同意が十分であったかを立証するための十分な証拠になると考えている．

以上のような解決策について，全体として包括的な評価を行う機能として，DPEC を設けて，さらに自主的なマルチステークホルダプロセスを行うことによって，データ主体の理解を十分なものとするとともに，ルール作りに関与を求めることによって，データ主体に配慮したプライバシ保護対策が達成される体制を構築した．

4.5 本取組の実際の運用状況

パーソナルデータの該当性とプライバシ性の 2 つの評価はそれぞれ異なった基準を持って行われる．パーソナルデータの該当性の評価については，外形的な判断基準が用いられる．収集するデータがデータ主体の ID と紐付いて

管理されている，あるいは紐付く可能性が残っているような場合には，パーソナルデータに該当するという評価を行っている．すなわち，収集するデータに着目して，そのデータの性質から判断を行っている．一方で，プライバシ性については，データの利用目的の中で，個人のプライバシに関わるような利用が行われるかどうかに焦点を当てた評価が行われる．データの利用過程に着目し，利用過程においてプライバシインパクトがどの程度生じるかを判断する．このプライバシインパクトの評価は，一般的なプライバシの枠組み（ISO29100 等）を参照しつつプライバシが問題となるような場合を考慮することに加えて，サービス開始前に先に示したマルチステークホルダプロセスを実施することによって行われる．

これらの 2 つの評価が個別に行われることによって，パーソナルデータ保護とプライバシ保護を同時に，プロジェクトにおいて達成することができる．筆者らは，パーソナルデータ保護とプライバシ保護の文脈が複雑に絡み合ってしまうことが，結果的にそれら 2 つの問題を複雑化しあるいは保護の達成を困難にしてしまう原因であると考えている．2 つの保護をプロセスとして切り分けることによって，十分な保護が達成されると考えている．また，パーソナルデータ保護の文脈は取得されるデータ種別の問題として，プライバシ保護の文脈はデータの利用過程の問題として示されることによって，データ主体にとっても「何が保護されるのか」が分かりやすい状態をつくることができる．

また，実際の同意取得プロセスにおいては，iKaaS プロジェクトに関連したデータの取得およびサービスの利用を受ける際には，3.1 節で示した 14 の項目がデータ主体に示される．データ主体には iKaaS プロジェクト全体において，これらの 14 の項目がどのように取り扱われるかについて「同意書」として示され，同意取得が行われる．個別のサービスが開始される際に，個別のサービスにおいて差分が生じる場合には，「重要事項説明書」において，その差分が示される．具体的には，サービス提供事業者，個別の利用目的，個別のサービスにおいて生じるプライバシインパクト，具体的なデータの収集，保管方法等が含まれている．加えて，iKaaS プロジェクト全体のプライバシ保護の方針を示すものとして「プライバシポリシ」が示される．

「同意書」は共通の基準（14 の項目）に基づいて定められており，「プライバシポリシ」は共通のものが利用される．そのため，すでに同意を得ているサービス以外のサービスが開始されるような場合には，新たな「重要事項説明書」がデータ主体に示されることになる．サービスごとの提供事業者，データの利用目的，プライバシインパクト，サービスごとのデータの収集や保管方法等が差分として示される．データ主体から，これらの差分に関する同意を得たうえで，サービスが開始される．

5. おわりに

本稿を通して，複数の事業者が共同して運営するプラットフォームにおけるデータ活用において，どのようなプライバシ保護要件を考慮すべきか概観した．そのうえで，プライバシ保護の実践的な取り組みとして，どのような施策が可能であるかについて述べた．

筆者らが提案した情報共有プラットフォームにおけるプライバシ保護対策は，日本，欧州，双方の法制度の水準を満たすものであり，本研究を通して情報共有プラットフォームにおけるプライバシ保護の必要十分な要件が提示できたと考えている．本研究を通してみると，情報共有プラットフォームを適正に設計することによって，データ主体の意向をふまえた情報流通が可能になり，結果として現状のデータ流通における課題を解消することができるのではない．筆者らは，現在のプライバシを取り巻く問題の源泉の 1 つが，データ主体の意向から乖離してデータ流通が行われることであると考えており，このような乖離をどのように埋めていくかが問題解消の鍵になると考えている．本研究はそのような問題解消に対して指針を示し，1 つの提案を行うものである．本稿を通して，その目的は達成されたと筆者らは考えている．

プライバシ保護要件については，日本のローカルな個人情報保護法に終始するのではなく，グローバルスタンダードの視点を欠かさずに，検討を進めることが必要である．多くのプラットフォームを運営する事業者にとっては，自国以外の制度を参照することに意味を見いだすことに疑問を感じるかもしれない．しかしながら，国際的なデータ移転が日常的に行われている中で，自国民以外のデータ主体のデータがプラットフォーム上流通しないことが保証されるであろうか．合理的な範囲のグローバルスタンダードを織り込むことは必須であるといえる．その点で，欧州におけるデータ保護の議論を今後も参照していくことは欠かせない．特に，欧州の人権思想に根ざしたプライバシ保護については，設計のできるだけ早い段階で考慮しておくべきである．事後的な対策で対処できる範囲には限界があり，後々に抜本的な見直しを迫られる可能性がある．iKaaS プロジェクトは欧州との共同プロジェクトであることから，欧州側の保護に対する考え方について議論を交わしているが，パーソナルデータの保護について非常に厳密に考えていることが理解できた．そのため，プロジェクトの当初より，欧州水準でのプライバシ保護を念頭に検討を進めてきた経緯がある．一方で，欧州の保護水準を満たす要件について定義，実装することに困難が生じていたことも事実である．データ利活用においては，できるだけ早い段階で欧州の保護水準について配慮すべきである．

プライバシ保護施策としては，一般的なプライバシ保護要件ベースに検討した保護要件をもとに，具体的にどのよ

うな体制づくりが必要であるかを検討した．各種内規の実効性を担保するために，プロセスおよびステークホルダの定義を行った．また，内部監査機関を設けることによって，データの取得，保管，利用，提供のプロセスが始まる前に，規約との整合性を担保できるようにした．さらに，内部監査機関のもう 1 つの役割がマルチステークホルダプロセスである．データ主体との間で対話の場を設けることで，先に定めたプライバシ保護要件が充足されることを確認する．それとともに，データ主体の同意が完全な理解のもとになされていないという前提のもとで，継続的，追加的な合意形成をはかっていく．これらのことから，データ主体との長期的に良好な関係が構築され，データの利活用についてもますます進むのではないかと期待している．いわゆるレピュテーションリスクについても，これらの手順を踏むことで最小化，あるいは事前の抑制を行うことができるのではないかと考えている．

なお，本稿におけるプライバシ保護要件とその具体的施策については，iKaaS プラットフォームの具体的機能実装への反映がなされていることを付け加えたい．本稿においては，紙面の関係上，iKaaS プラットフォームの具体的な技術的施策の紹介ができなかったが，iKaaS プロジェクトは，技術的な検討が本稿で紹介したような検討と並行して行われる計画となっており，実際，そのような進め方がなされている．たとえば，DPEC で審査される内容は，単に規約との整合性を確認するだけでなく，技術開発側にフィードバックされている．iKaaS プラットフォームでは，プライバシに配慮したセキュリティゲートウェイの開発が進められている．このセキュリティゲートウェイの保持するプライバシポリシは，本稿で検討したプライバシ保護要件が反映されるだけでなく，DPEC での審査によって得られた知見がフィードバックされている．また，ユーザのアクセス権や削除請求権等の機能実装の具体的な形態が検討されている．

ビックデータの活用においては，データ主体から継続的なデータの提供を受けることが欠かせない．その際に，最初の同意についての修正をまったく受け付けないということは，データ主体にとっては，約款の細かな文言に固執して，これらの文言を突きつけたうえで，契約の履行を強制することにほかならない．この状態の法的評価については，様々であると思われるが，より良い関係性に着目した場合には，回避すべき事態である．これは，プラットフォームを運営する事業者とデータ主体との社会的な力関係の観点からも，望ましいことではない．規約の単純な履行以上のことに努めることは，当事者間の信頼関係の醸成に効果的であることは，試験的に行ったデータ主体との対話からも明らかであった．プラットフォーマがデータ主体とのより良い関係を構築することで，ビックデータの活用が進んでいくことを望む．

謝辞 iKaaS プロジェクトは総務省平成 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）としての助成を受けている．

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，独立行政法人情報通信研究機構（オンライン），入手先 ⟨http://www.nict.go.jp/nrh/iinkai/report.pdf⟩（参照 2016-08-12）．
[2] Suica に関するデータの社外への提供についての有識者会議：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，JR 東日本（オンライン），入手先 ⟨http://www.jreast.co.jp/chukantorimatome/20140320.pdf⟩（参照 2016-08-12）．
[3] 石井夏生利：「プライバシー外交」のためのプライバシー，情報通信政策レビュー，No.4, pp.54–78 (2013).
[4] iCore（オンライン），入手先 ⟨http://www.iot-icore.eu⟩（参照 2016-08-12）．
[5] SOCIOTAL（オンライン），入手先 ⟨http://sociotal.eu/⟩（参照 2016-08-12）．
[6] OCEAN（オンライン），入手先 ⟨http://www.ocean-project.eu/bin/view/about/Japanese⟩（参照 2016-08-12）．
[7] ClouT（オンライン），入手先 ⟨http://clout-project.eu/jp/⟩（参照 2016-08-12）．
[8] 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（オンライン），入手先 ⟨http://in-law.jp/archive/taikai/2013/bunkakai1-Kikuchi.pdf⟩（参照 2016-08-12）．
[9] 瓜生和久（編著）：一問一答 平成 27 年改正個人情報保護法，商事法務 (2015).
[10] 鈴木正朝，高木浩光，山本一郎：ニッポンの個人情報，翔泳社 (2015).
[11] 第二東京弁護士会情報公開・個人情報保護委員会（編著）：Q&A 改正個人情報保護法—パーソナルデータ保護法制の最前線，新日本法規 (2015).
[12] 日置巴美，板倉陽一郎：平成 27 年改正個人情報保護法のしくみ，商事法務 (2015).
[13] 宇賀克也：個人情報保護法の逐条解説第 4 版，有斐閣 (2013).
[14] 園田逸夫（編著）：個人情報保護法の解説（改訂版），ぎょうせい (2005).
[15] 堀部政男研究室：EU データ保護指令仮訳，総務省（オンライン），入手先 ⟨http://www.soumu.go.jp/main_content/000196313.pdf⟩（参照 2016-08-12）．
[16] 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，経済産業省（オンライン），入手先 ⟨http://www.meti.go.jp/report/downloadfiles/g81110a02j.pdf⟩（参照 2016-08-12）．
[17] アン・カブキアン（著），一般財団法人日本情報経済推進協会（JIPDEC）（訳），堀部政男/JIPDEC（編著）：プライバシー・バイ・デザイン：プライバシー情報を守るための世界的潮流，日経 BP 社 (2012).
[18] 生貝直人：情報社会と共同規制：インターネット政策の国際比較制度研究，勁草書房 (2015).
[19] 株式会社野村総合研究所：平成 26 年度我が国経済社会の情報化・サービス化に係る基盤整備（パーソナルデータ利活用に関するマルチステークホルダープロセスの実施方法等の調査事業）報告書，経済産業省（オンライン），入手先 ⟨http://www.meti.go.jp/meti_lib/report/2015fy/000296.pdf⟩（参照 2016-08-12）．
[20] 情報通信審議会情報通信部会ドメイン名政策委員会マルチステークホルダープロセス検討ワーキンググループ：マル

チステークホルダープロセス検討ワーキンググループ報告書，総務省（オンライン），入手先 ⟨http://www.soumu.go.jp/main_content/000314325.pdf⟩（参照 2016-08-12）．
[21] 総務省：マルチステークホルダーの考え方，総務省（オンライン），入手先 ⟨http://www5.cao.go.jp/npc/sustainability/concept/index.html⟩（参照 2016-08-12）．

加藤 尚徳 （正会員）

（株）KDDI 総研研究主査．2009 年新潟大学法学部卒業．2014 年総合研究大学院大学複合科学研究科情報学専攻博士 5 年一貫課程単位取得満期退学．修士（情報学）．プライバシ・個人情報保護・知的財産法等の調査研究に従事．

高崎 晴夫

（株）KDDI 総研主席研究員．1980 年東北大学法学部卒業．国際電信電話（株）（現，KDDI（株））入社後，2005 年より現職．プライバシ保護関連研究に従事，カナダ・オンタリオ州よりプライバシバイデザインアンバサダの認定を受ける．

村上 陽亮

（株）KDDI 総研調査 1 部長．1998 年東京大学法学部卒業．国際電信電話（株）（現，KDDI（株））入社後，総務省等の官公庁渉外業務等に従事した後，2013 年から現職．海外，特に欧州の情報通信政策および市場動向に関する調査研究に従事．