平成27年度
集めないビッグデータコンソーシアム
成果報告書
―パーソナルデータエコシステムの実現―

2015年10月5日

集めないビッグデータコンソーシアム

目次

第1章　はじめに

これまでパーソナルデータ(個人に関するデータ)は専ら企業や政府が集めて管理してきた。顧客の連絡先や契約書は企業がまとめて管理せざるを得ないという意味でパーソナルデータの集中管理は必須だが、集中管理だけでは、個人による自己情報コントロールが困難だという倫理的問題が生じ、集中管理されたパーソナルデータがまとめて漏洩する事件が頻発して企業の経営を脅かしている。また企業が管理しているパーソナルデータが本人のために活用されにくく、企業にとっても他社に由来するデータを自社のために活用しにくいので、多くの事業機会が失われている。

一方、各個人も本人のデータを電子的に保有し、自分の利益を高めるようにそのデータを自由に流通させること(A病院の診療録をB病院に開示する、Amazonや楽天での購買履歴を地元の商店に開示するなど)ができれば、生活の質とB2Cサービスの価値が高まり、産業全体が活性化するだろう。また、個人が本人のデータを総合的に管理していれば、パーソナルデータを収集したい企業等は個人から本人同意に基づいてデータを直接取得すれば良いから、パーソナルデータの第三者提供が不要になり、パーソナルデータの共有と管理が容易になる。さらに、個人主導のDRM (Digital Rights Management)等でパーソナルデータの不正使用を技術的に防止できれば、本人同意に基づくパーソナルデータの収集・活用が一層促進され、産業や学術の振興につながる。

東京大学では、このような個人ごとのデータの分散管理を通じてパーソナルデータを効率的に流通させ効果的に活用する仕組みをICTで構築するための研究を進めてきた。それは、この仕組みの中核となる分散PDS (Decentralized Personal Data Store; 個人が特定の事業者に依存せずに本人のデータをパブリッククラウド等で自ら蓄積・管理して他者と共有し活用するためのツール)としてのPLR (Personal Life Repository)の設計・開発、それに基づいて多様な現場での協調作業を支援するICT基盤に関する検討、これらを普及させるための状況分析や戦略の策定等に及ぶ。

たとえば、2025年を目標として進められている医療制度改革は、上記のような自律分散協調的な社会システムを構築するための契機になるだろう。病院が急性期、回復期、療養期等に分類され、診療所や介護事業者も含むヘルスケア事業者の間での相互連携が事業者の経営において不可欠になることにより、これら事業者の間でのデータ共有も必須になる。従来の集中管理によるデータ共有よりも個人分散管理により個人を介したデータ共有の方が安全で安価で利便性も高いので、病院の分類が完了する2017年末ごろには個人に分散したヘルスケアデータの管理が普及し始めるだろう。また、2016年の電力小売の自由化によって電力取引の市場が十全に機能するには、各需要家が自らの電力消費の仕方に合った料金プラン(を提供する小売事業者)をデータに基づいて正しく選択できる必要があるが、電力消費の情報はパーソナルデータであるから本人(家庭)が管理すべきである。欧米の動向に鑑みても、パーソナルデータの本人管理が多様なB2Cサービスにわたって普及する可能性が高い。課題は、それに伴う破壊的イノベーションを世界に先駆けて推進し、パーソナル

データの安全な流通の促進により社会の学習・創造能力を高めることである。

東京大学は、「集めないビッグデータ(Distributed Big Data)」コンソーシアムを設立してこのような構想の実現を目指している。2014年10月に始まった本コンソーシアムの活動においては、パーソナルデータエコシステムを実現するために、分散PDSのあるべき技術仕様を明らかにしつつ、その社会受容性について検討してきた。分散PDSの技術仕様に関しては、個人が本人のデータを自らの意思で他者と共有し活用するための要件を反映した基本的な設計を得た。分散PDSの社会受容性に関しては、スマートタウンやスマートライフに関連する分散PDSのユースケースについて考察し、分散PDSの普及につながるビジネスモデルを検討した。以下ではそれらの成果を報告し、今後の展望を示す。

これらの検討や考察において特に重要な論点は個人と事業者の役割である。個人が担い得る役割は、顧客、生活者、消費者、生産者、従業員、経営者、投資家、データ主体(識別された又は識別され得る自然人)、管理者、代理人、PDS利用者など多岐にわたることが想定される。以下では、これらの役割のうちいずれかを特定すべき文脈においては「顧客」や「生活者」などの用語を用いるが、そうでない場合にはこれらの役割のうち複数を同時に担い得る主体という意味で「個人」と書く。一方、そのように多様な役割を担う個人に対し商品・サービスの提供者や雇用者としての事業者が担うべき役割も多様である。特に、個人の自己情報コントロールを極端に追求しようとすると、個人が判断すべき事項が増えすぎて人間の認知限界や個人端末の能力を越えてしまうので、その判断をある程度まで事業者や市場に委ねる必要があるだろう。以上のような事項に関する検討の多くは今後の課題であるが、以下の報告は個人と事業者の関係についてさらに検討を進める際に有用な手がかりとなろう。

第2章　パーソナルデータの利活用に関する環境変化

2.1　個人を取り巻く環境変化

1980年代以前、すなわちインターネットが大衆化する以前にはプライバシーとは人々が密集して生活している都市のような空間において「一人にしておいてもらう権利」という概念で捉えられていた。

インターネットが大衆化した後、パーソナルデータは旧来の(氏名、性別、生年月日、住所)を超えて多様化の一途を辿った。例えば、Webであれば検索履歴のログ、あるいはネット上での購買履歴、あるいはSNSによる継続的な発信など、その種類を数えきれず、以前とは質的にも量的にも比べものにならないほど拡大した。結果としてプライバシーの焦点はインターネット上を流通するデータ主体のパーソナルデータに移ってきた。「独りにしておいてもらう権利」はインターネットにおける個人という文脈では、「忘れられる権利(the right to be forgotten)」 あるいは「追跡拒否権(Do Not Track: DNT)」という考え方に変容する。

「忘れられる権利」は、過去の自己の情報を保有する事業者に対して、それが現在の自己と一致していない場合に、その情報を削除することを求める権利である。たとえば、検索エンジンに対して、現在の時点では不正確となっている個人情報へのリンクを検索結果として表示しないよう求めることも、忘れられる権利の行使ということになる。

「追跡拒否権」は、インターネットの利用者が、閲覧・訪問先サイトの運営者に対して、オンライン上の行動に関する情報を収集しないよう求める権利である。例えば、cookieを送り込んで個人のアクセス履歴を収集し、ターゲット広告を行なうような操作を拒否することである。DNTはGoogleの裁判で問題になったプロファイリングに関していえば、プロファイル拒否権という見方ができる。

しかし、もう少し抽象化して適用範囲を拡げようとすると、データ主体である個人が自身に関するパーソナルデータのコントロールをできる「自己情報コントロール」をプライバシーとする考え方になる[1]。これを権利として見た「自己情報コントロール権」は具体的には、自己に関する情報を誰に開示するかを本人が決定し、どのような目的で利用させるか、また、どのような第三者に提供するかを本人が許可あるいは拒否する権利であり、またその前提として、事業者が保有する自己情報の開示、訂正、削除を要求する権利、さらに、自己情報がどのような目的に使われるかを知る権利である。もし、これらの要求に応じられない場合は、その正当な理由を本人に知らせなければならない。これらの権利は個人からデータ収集しているWeb事業者にとっては重荷であり、その実効的な実施は遅々として進んでいない[2]ものの、徐々に自己情報コントロールの考え方が浸透し始めている。こ

[1] 自己情報とはデータ主体である当該個人に係わるパーソナルデータと考えられる。

[2] 例外としては、Googleに対して忘れられる権利によって過去の債務に関する検索結果の削除を命じた2013年のEU司法裁判所の判決などがある。日本でも、類似の事件について、人格権に基づき検索結果の非表示を命じる決定が2014年に出された。

のような事情から、個人がWebサービスと引き換えに大量の自身のパーソナルデータをWeb事業者に収集、利用をさせるビジネスモデルも万能ではなくなりつつある。本報告書の文脈でいえば、自分の情報を誰に渡すかを自分自身で決定する権利も含まれる。

2.2　事業環境の変化

2013年6月、政府のIT総合戦略本部は、「世界最先端IT国家創造宣言」を決議し、パーソナルデータの取扱いについて、その利活用を進めるための事業環境整備を進めることとし、「パーソナルデータに関する検討会」(以下「パーソナルデータ検討会」)を設置した。

当初は個人情報保護法の改正にまで踏み込むかどうかは明らかではなかったが、2013年秋には、「パーソナルデータ検討会」で個人情報保護法の改正が目標として掲げられ、2015年9月に国会で改正案が成立した。個人情報保護法は、個人情報の収集制限に関する規定を含むものの、基本的には、事業者が提供しているサービスの利用者から収集したパーソナルデータの利活用を規律する法律である。つまり、基本的には「集めたビッグデータ」を対象にする法律である。事業者が集めたビッグデータに関しては、個人が自分のパーソナルデータに対して行使できる権利は極めて限定的であり、個人情報保護法は、この状況においてパーソナルデータの濫用を避けることが目的である。ただし、パーソナルデータの利用に関しては、個人が利用目的の記述された利用規約あるいは契約に同意していさえすれば企業側は同意された条件に沿う利用は自由にできる。したがって、実態は個人の側にとってはかなり自由度が少ない状況である。

「ビッグデータの正体」[Schoenberger and Cukier, 2013]の著者であるショーンベルガーがIAPP[3]の2013年の基調講演で事業者の提供するソフトウェアやWebサービスにおけるプライバシー情報収集に関する利用規約への利用者の同意の形骸化について述べている[Schoenberger, 2013]。

彼によれば、Webサービスに参加、あるいはWebアプリやソフトのダウンロード 時に、「同意します」を儀式的にクリックするが、契約文書を読んだ人は非常に少数である。しかし、契約文書をまともに読んだらどのくらいの負担になるのだろうか。例えば、少し古いデータだが2008年の調査では、このような契約文書(プライバシーポリシー)を読み通すと、年間244時間(＝30日間のフル仕事) になってしまう。現在の状況ではこの負荷はもっと増えているだろう。儀式的なクリックをクリックトレーニングと呼ぶことが一般化するほどである。契約は当事者双方が契約文書を十分理解した上で合意して成立するものであると言われるから、同意の儀式的なクリックは法律的には、契約が成立しているか疑義がある。

さらにショーンベルガー[Schoenberger, 2013]によれば、事業者の提示するプライバシーポリシーはサービスやアプリの利用者に自己情報の開示の度合いを選ぶ権利を与えていない。さらに第3者への利用者データの転移の状況も教えないという。そして、「同意」しな

[3] The International Association of Privacy Professionals

ければサービスやアプリは使えないというある意味非常に不平等な契約になっている[4]。

ショーンベルガー[Schoenberger and Cukier, 2013]は、ビッグデータの本質として、収集したデータの有効な利用法が収集以前には分からず、収集してみてはじめて思いつくことが多いことを述べている。ということは、個人からデータ収集するときに提示する契約には具体的な利用法が列挙しきれないため、1) 新規の利用法が見つかったときには同意を取り直す、あるいは2)利用法を抽象的に記述し[5]、できるだけ包括的な利用法、すなわち曖昧な記述の契約文書にする、という方法がある。実際の手間を考えると、2)が多いだろうが、そうなるとただでさえ理解しにくい契約文書が曖昧になってしまい、利用者はますますまじめに読まなくなる。

「通知と同意」[6]は本来、有効なサービスやアプリの利用者であるデータ主体のプライバシー保護を与えるという枠組みであるはずだった。しかし、このように形骸化してしまった現状では全く非効率になっていて、実質的に機能していない。この状況はデータ主体である利用者が提供するパーソナルデータの利用権をサービスやアプリの利用と引き替えに全て手放しているような状況を生みがちで、利用者にとってプライバシー保護の観点からみて非常に不利なものである。プライバシー保護が本来の目的だったとすると、形骸化した同意ではないアプローチが必要である。ショーンベルガーは、事業者が収集し利用するパーソナルデータのプライバシー保護は契約文書の同意によるのではなく、事業者の説明責任[7]によるべきだと主張している。

事業者の説明責任を実効性のあるものにするためには次の2点が必要である。

(1)法令による保証
(2)利用者への分かり易い説明

法令による保証を執行できるのは、独立したプライバシー保護の監督機関であり、日本であれば個人情報保護委員会が相当することになるだろう。米国の場合は当然、連邦取引委員会（FTC)であろう。

利用者への分かり易い説明の内容としてまず考えられるのは、利用者のパーソナルデータが実際どのように利用されたかの説明である。処理プロセスを調査してパーソナルデータの利用履歴を洗い出すのは、事業者にとっても非常に手間がかかることである。むしろ、パーソナルデータ取得時にどのような使い方をするかを説明しておくことが肝要である。この説明がきちんとされていれば、パーソナルデータを提供したデータ主体がその利用法

[4] このように、契約内容を一方当事者があらかじめ定め（約款規制）、他方当事者にはその契約を締結するかどうかの選択肢しかない契約のことを、「附合契約」という。契約当事者間の不平等を避けるために、行政による約款規制がなされる場合が多い。
[5] 多くの場合は分かりにくく記述されることになる。
[6] notice and consent
[7] accountability

に対して疑念をいだいた場合に説明を求めることも容易である。その場合は、論点が明確になって事業者側にとっても調査も説明もやりやすい。もちろん、法令に準拠するなら自己情報の開示請求になる。結着が付かない場合は監督機関、日本であれば個人情報保護委員会の規制権限に委ねられるのが望ましく、これによって説明責任の法令による保証を行う。

そこで、(2)の論点が浮上してくる。すなわち、個人情報の取得時にデータ提供を行うデータ主体にデータ収集を行う事業者がどのような説明をし、データ提供の同意を取り付けるかが重要なインタフェースとなる。

パーソナルデータ収集においてデータ主体の自発的入力を念頭においた場合のインタフェース設計の方策が情報処理学会のデジタルプラクティス2015年1月号にいくつか提案されている[佐藤, 2015; 中村 他, 2015; 佐藤 他, 2015]。佐藤[2015]では、データ収集した事業者が収集元の個人に製品宣伝などの連絡をするために、連絡先情報を顧客情報管理データベースに格納して運用する場合のデータプライバシー対策を紹介している。データ主体本人からの訂正や削除の要求、同意の取り下げ要求、などに対応できるように、データベースにおいては個人から得た同意内容や利用履歴を個人毎に管理しておく必要がある。さらに、宣伝や本人へのお知らせを行うメディア毎に同意の内容を別個管理するような肌理の細かさも推奨されている。

しかし、同意の仕方にも注意が必要である。これには少なくとも明示的と暗黙的の2種類が存在する。

明示的同意取得とは、事業者がデータ主体の個人に同意を表明するための行為を求め、その行為をした場合に同意取得したとすることである。Webであれば、同意のチェックボックスのクリックした場合などである。行為がされなければ同意取得は失敗したことになる。明示的不同意取得は、データ主体は不同意を表明する行為をすることになる。

暗黙的同意取得とは、データ主体が行為をしなかった場合に同意取得したとすることである。たとえば、デフォールトを同意にしておき、不同意の場合は何らかの意思表示行為を要求する場合において、データ主体の行為がなかった場合が相当する。デフォールトが不同意であり、データ主体がそれを覆す行為をしなければ暗黙的不同意取得になる。

明示的にせよ暗黙的にせよ同意／不同意を取り消すためにはデータ主体は取り消しのための行為をする必要がある。暗黙的同意／不同意は取り消す行為がない場合は継続する。ただし、ややこしいケースとして暗黙的同意／不同意を暗黙的不同意／同意で覆せるかという問題がある。次のような例を考えてみよう。遺伝子検査事業者に対する個人の遺伝子情報鑑定の申込みで

- あなたの遺伝子情報を研究目的以外に使ってよい場合はチェックしてください

という項目があり、チェックしなかったとすると、この時点では暗黙的不同意となる。しばらくして、この業者がポリシーを変更し、

- あなたの遺伝子情報を研究目的以外に使ってはいけない場合はチェックしてください

という項目が提示されたとしよう。これにチェックしなかった場合は暗黙的同意になってしまう。この場合、遺伝子情報を研究以外の目的、例えば提携保険会社の料率に反映させることが適法かどうかというケースが考えられる。判断が困難であるが、そもそもこのような暗黙的な同意／不同意の入れ替えをするような同意インタフェース自体、極めてデータ主体の個人に不親切であり、利用者への分かり易い説明に反している。

このようにショーンベルガーの説明責任の考え方は、パーソナルデータの保護と利活用における考え方の一方の極を与えているが、十分ではないことがうかがわれる。

2.3　パーソナルデータエコシステム

ショーンベルガーの事業者の説明責任にプライバシー保護の重点をおくべきだという主張は、形骸化している同意は軽く見るという点が問題であるとして、プライバシーバイデザインの提唱者のカブキアン等はこれに異を唱えた[Cavoukian, Dix, Eman and O'Connor, 2014]。つまり、1) 事業者の善意に期待するのは危険、2) プライバシー侵害の大部分は隠蔽されており、発見されることは氷山の一角、3) 業務に多忙を極める監督者ないし監督機関にさらなる負荷を追わせることは物理的にも困難、だと主張している。

1)の論点はまじめな業者には当てはまらないと期待している。しかし、これはあくまでも善意への期待である。2)の論点はおおいにありそうだと思われる。3)の論点は監督機関、日本でいえば個人情報保護委員会の事務体制を十分に整備することが困難視されている状況を考えればさもありなんと思われる。

以下で述べるカブキアンのパーソナルデータエコシステムの主張はショーンバーガーの説明責任の対極に位置するものと捉えられる。カブキアンの主張は、プライバシー保護の全体的仕組みの中にデータ主体である個人を参加させ、中心的役割を与えるべきだというものである。この主張はショーンベルガーの言い分、すなわちデータ主体が唯一自身のパーソナルデータの収集さらに利用に対して権利行使をできる「同意」を軽視ないし無視していることへのカブキアンのアンチテーゼとして位置づけられる。上の1)、2)、3)の論点を踏まえてカブキアンの主張を見直すと、ビッグデータにおいてプライバシー保護に役立つことは、パーソナルデータは常にデータ主体である個人の管理下におき、これによって事業者のパーソナルデータの収集を最小に押さえることとしている。カブキアンは、この考え方をパーソナルデータエコシステム(Personal Data Ecosystem; 以下PDEと略記)という概念で具体化した。

パーソナルデータエコシステム(PDE) [Cavoukian, 2013; 佐古, 2015]

PDEとは、個人、および事業者や組織が、新たなツール、技術を用い、データ主体である個人が自身のパーソナルデータの管理を行うことによって、パーソナルデータを活用する仕組みと考えられる。PDEの構成要素になり得るのは以下のものである。ただし、ここで提案している分散PDSに含まれていない要素がはいっていることにはご留意いただきたい。

(1) PDS (Personal Data Store)

PDV (Personal Data Vault)等とも呼ばれる。データ主体のパーソナルデータをパブリッククラウド等で自ら蓄積・管理し活用するためのツールである。利用者から見ればDropboxやGoogleドライブのようなイメージである。ただし、DropboxやGoogleドライブの利用規約はDropbox社やGoogle社によって一方的に決められている。一方、PDSの基本的な利用規約は、PDE全体で決められている。複数のPDSがPDEに参加している場合は、データ主体が自身のパーソナルデータをPDSの間で移転することもできなければならない。場合によっては利用者個人のスマホやPCの中にデータを置くタイプのPDSも可能であろう。

PDSへのデータ入力はデータ主体の個人あるいはPDEのポリシーに則らなければならず、データ主体と契約した事業者に限られる。データはデータ主体の鍵で暗号化されていると安全である。

PDSへのデータ入力、あるいはデータ利用は、データの主体の個人あるいは、その個人と契約したトラストフレームワーク（後述）の参加メンバーでなければならない。また、データ主体である個人は、事業者からPDEのポリシーを遵守することが要求される。また、データ主体である個人はそのような事業者からパーソナルデータ利用の要請があったときは、個人の判断で諾否を決めることができる。すなわち「同意」原則に則っているわけである。

以下の諸項目は、このようなパーソナルデータの動きを支援、管理するための仕掛けである。

(2)意味的データ交換(semantic data exchange ）

パーソナルデータをPDEに参加している事業者が使用するためにはPDSからデータを読み出す必要がある。この読み出しを実現する取り決めがXDI意味的データ交換プロトコルである。XDIはOASIS (Organization for the Advancement of Structured Information Standards)[8]において、2004年に設立されたXDI技術委員会によって開発されてきている。

データは単なるビット列のデータとして読み出しても利用できない。データを利用するためには、データとその属性を記述するメタデータが組み合わせになっていなければならない。データとメタデータのペア自体は目新しいものではないが、メタデータとして、特定の状況[9]において当該データ集合に適用される権利と許可条件を記載できることが重要である。これはXDIリンクコントラクトと呼ばれ、OASIS [2014]に詳述されている。リンクコントラクトの雛形となるリンクコントラクトテンプレートに記述されるのは以下のような要素である。

[8] OASISは、国際的な非営利目的の協会で、情報社会におけるオープンな標準規格の 開発、合意形成、採択を推進している。

[9] XDIではコンテクスト(context)と呼ぶ。

- リンクコントラクトテンプレートの責任者
- データ利用要求元(データ利用したい事業者)
- データの所有者であるデータ主体。要求を許可／却下できる
- データが利用される状況
- データ利用における操作：読み出し、変更、共有、消去、コピー、移動、など
- 操作が適用されるXDIの要素群。グラフ構造で表現されている。

最後の要素に書いたようにXDIでは全てのデータ要素がグラフ構造で記述されている。例えば以下のような構造である。例えば、太郎と花子の関係が友だちというのは以下のようになる。リンクコントラクト自体もグラフの要素となる。

（太郎）——友達———（花子）

リンクコントラクトの特徴は機械可読な契約として機能することである。したがって、データ主体が記述したリンクコントラクトにしたがった操作(共有、変更など)が機械的に実行される。つまり、データ主体の意志がリンクコントラクトに反映される。特定の事業者の利用に同意したくなければ、一度、リンクコントラクトにその事業者にはデータ利用を許可しないと記述しておけばよい。

さらにデータはリンクコントラクトとペアになって読み出されるので、読み出し先においてもリンクコントラクトの記述内容は遵守される。これは、パーソナルデータが第三者に共有されるとき、同時にリンクコントラクトも付随してくるので、パーソナルデータの第三者共有におけるプライバシー保護の有力な技術となっている。つまり、PDE参加者間での共有はPDEの規約によってプライバシー保護がリンクコントラクト記載の方法で執行されるわけである。また、データの有効期間についても、消去すべき日時をリンクコントラクトに記載しておくことができる。有効期間が過ぎたら自動的に消去できる実装にしておけばよい。

翻って、日本の個人情報保護法では事業者が当初に示した利用目的にデータ主体が同意する形で行われる。これに対して、PDEでは利用条件自体をリンクコントラクトにおいてデータ主体が関与して決められるので、データ主体のパワーが大幅に向上していると言えよう。

(3)トラストフレームワーク(trust framework)

上記(1)(2)の技術的要件に対して、トラストフレームワークはポリシーおよび法的な観点に立つ枠組みであり、以下の2要素からなる。

- ツール：ネットワーク上の相互運用を実現するために、PDE参加者によって実装される技術標準とプロトコル

- 規則：セキュリティ、プライバシーおよびその他の信頼性のレベルを達成するためのビジネス的、法的および運用上のポリシー

トラストフレームワークは上記のツールと規則を記述するオンライン文書、およびそれらを運用するための査定と執行の仕掛けである。

PDEの観点から見て重要なポイントは利用者中心型のトラストフレームワークである点である。利用者中心型トラストフレームワークでは、利用者であるデータ主体は事業者からのデータ使用要求のたびにいちいち自らのデータ利用の状況について気にしなくてもよい。なぜなら、トラストフレームワークの規則にデータ利用に関する取り決めが書かれていて、事業者はその取り決めに従うことが要請されているからである。

利用者中心型トラストフレームワークとして有名なのはMydex社のトラストフレームワーク[10]やRespect Network社のトラストフレームワーク[11]である。両者とも、利用者のセキュリティとプライバシーを尊重する事業者、政府機関などの信頼できる参加者に対してPDSのデータを共有できるように設計されている。

(4)個人IDとデータポータビリティ

データ主体がパーソナルデータを現在格納しているPDSから別の事業者が運営するPDSに乗り換えられること、すなわちデータポータビリティが必要である。例えば、素人でも簡単にGoogleドライブ上のデータをDropboxに移転できるような状況[12]を想定すればよい。

しかし、データポータビリティというからには、パーソナルデータの意味が保持されなければならない。意味とは、具体的には例えば、あるデータは氏名、あるデータは日時、品目、場所、価格などからなる購買履歴、などである。意味の保持は(2)で述べたXDI意味的データ交換プロトコルによって実現される。リンクコントラクトも同時に移転されなければならない。さらに、データポータビリティを確保するためにデータ主体の永続的な識別が行える個人IDが必要である。

(5) 参照によるパーソナルデータ使用

事業者がパーソナルデータあるいはそのコピーを保持して事業を行う場合には、ア) データが古くなること、イ) 法制度が要求するプライバシー保護の遵守、ウ) 漏洩などによる潜在的リスクに常に悩まされる。

そこで、PDEでは、事業者がパーソナルデータのコピーを保持せず、必要なときは参照しにいくという方法を採ることもできる。参照とは読み出すだけで利用後にコピーを保持

---

[10] http://openidentityexchange.org/trust-frameworks/mydex-trust-framework

[11] 佐古[2015]において詳しく説明されている。

[12] 現在は、GoogleとDropboxは別会社なので、データ移転は自分で苦労して行う必要がある。これではデータポータビリティがあるとは言えない。

しないことを意味する。参照の可否はデータ主体の個人の同意すなわちリンクコントラクトによるが、一度「可」とされれば、リンクコントラクトが変更されない限りは参照し続けることができる。参照によるパーソナルデータ使用の利点を以下に列挙する。

- 事業者はパーソナルデータ管理コストを減らせる。
- 常に最新のパーソナルデータが使える。つまり、参照するパーソナルデータはデータ主体の個人がPDSに格納し、継続的に更新している最新のデータだからである。
- データ主体はPDSに格納されている自身のパーソナルデータを直接にコントロールできる。
- 事業者はパーソナルデータのコピーを保管しないので、漏洩のリスクは軽減する。特に膨大な人数のパーソナルデータが一度に漏洩するリスクは非常に低い。
- 事業者が顧客のPDSへの継続的アクセスを許可されれば、顧客が長期間にわたって事業者にとって高い価値を持ち続けることになる[13]。
- 事業者に対してアクセスを許可することによって、データ主体は経済的その他の利益を得る。

なお、事業者はパーソナルデータを必要に応じてPDSに参照に行くのではなく、コピーを事業者自身が保管する方法も可能である。上記のメリットのいくつかは失われるが、データ参照に伴う手間と時間、すなわち暗号化されたデータの復号、データの通信のコストを低減できる。この場合でも、パーソナルデータの利用はトラストフレームワークを遵守しなければならない。

(6)説明責任のある仮名化

PDE内においてもデータ主体に直接結びつく個人IDや実名を使うよりは、仮名を使うほうが個人識別されるリスクに関しては安全である。ただし、裁判など法令によって当局の要求に応えられるように、仮名と個人IDの対応表は保存しておき、必要に応じてデータ主体と仮名化されたパーソナルデータを結びつけられるようにしておかなければならない。

(7) 新技術やリンクコントラクトによる匿名化の強化

個人IDと仮名の対応表を削除してあっても、いかなるパーソナルデータに対してもデータ主体を識別できない、いわゆる完全な匿名化の技術は存在しない。しかし、技術の進展あるいはデータの状況によって匿名化の強度は高まる。たとえば、滞在位置情報に関しては、ア)　仮名化において仮名を5分毎に変更して前後のデータと切り離すこと、イ) 位置を500メートル四方のブロックにまとめること、ウ) 位置情報に雑音を加算して位置をずらすこと、などの処理が考えられる。これらの処理をPDSに格納されている個人の滞在位置データに施すことよって、匿名化の強度を大きく向上でき、安全性が高まる。

[13] 筆者は、顧客にとって継続的な良いサービスが受けられること、事業者にとってサービスを継続できる上客となることの両者を意味すると解釈した。

一方、意味的データ交換におけるリンクコントラクトによって匿名化を行う方法も採れる。これはリンクコントラクトという契約による匿名化である。いずれにせよ、匿名化は利用者であるデータ主体に権限の元で行われる。

以上、説明してきたように、PDEはプライバシー保護というよりは、プライバシー保護をデフォールトにし、使いたい事業者がいればリンクコントラクトに則って利用を許可するという随時的なオプトインのシステムと見なすことができる。データ主体は非常に強い自己情報コントロールを実現できるので、カブキアンの提案したプライバシーバイデザイン(PbD)に関係が深い。そこで、PDEとPbDの関係を概観してみよう。

まず、PbDの7原則を再掲しておく。

原則1. プライバシー保護に関しては、事後の対策ではなく、事前に予防措置をとるべし
原則2. プライバシー保護はデフォールトであるべし
原則3. プライバシー保護の仕組みは制度やシステムの設計時に組み込むべし
原則4. プライバシー保護はゼロサムではなくポジティブサムである。
原則5. プライバシー保護はパーソナルデータの生成から廃棄までの全期間において実施すべし
原則6. プライバシー保護の仕組みを可視化、透明化すべし
原則7. プライバシーは利用者中心の仕組みにすべし

PbDの各々の原則とPDEの関係を考えてみよう。この関係を知ることによって、PbDの理想的な実装システムとしてのPDEの性格が明らかになる。同時にPDE以外のシステムでパーソナルデータを扱う場合においてPbDを取り入れるとすれば、制度や実装の参考例となる。

原則１の事前措置に関しては、パーソナルデータをPDSで個人毎に分散管理する方法自体が、プライバシー保護のための事前の対策として効果的であることが対応する。従来から行われてきたように事業者が中央集権的に膨大な人数のパーソナルデータを収集管理する場合は、プライバシー保護はデータ主体である個人の手を離れて、事業者に一任される。したがって、事業者によってはいい加減な保護しか行われないかもしれないし、漏洩した場合も膨大な人数が一度に漏洩する危険性が高い。分散PDSの場合、パーソナルデータは個人ごとに分散して管理されているため、漏洩のリスクは小さい。

原則2のデフォールト性に関しては、PDEの場合、リンクコントラクトが重要な役割を担う。すなわち、データ主体のプライバシーは、ひとたびリンクコントラクトを決めれば、新規の事業者を相手にする場合もリンクコントラクトに則ってプライバシー保護がデフォールトとして適用されることになる。このため、データ主体の負担は小さい。事業者においても、リンクコントラクトに機械的に従うしかないので、人的労力としての負担増は抑えられる。

原則3の設計時組み込みもリンクコントラクトで実現されている。つまり、パーソナルデ

ータを格納するPDSは言うに及ばず、これを利用する事業者によってシステム設計を行うに際しても、リンクコントラクトを解釈し実行するシステム設計を行うことになるため、設計時組み込みは必然的に行われることになる。

原則4のデータ主体と事業者のポジティブサムあるいはwin-winの関係については既に各所で述べてきた。技術的に重要な点は、事業者にとっては、上記(5) 参照によるパーソナルデータ使用で書いたように最新のデータが入手できること、漏洩やデータ管理およびセキュリティ対策コストが低減すること、などが挙げられる。データ主体にとっては、リンクコントラクトによって自己情報コントロールができていることによる安心感、ひいては事業者への組織的な信頼を持てることがうれしい。結果として、データ主体のパーソナルデータの流通が促進されれば、事業者の事業の拡大にもつながる。なお、(6)説明責任ある仮名化によれば、監督機関や警察などにとっても必用に応じて調査あるいは監査が確実に行えるという利点もある。

現在のように事業者がパーソナルデータを可能な限り囲い込もうという方法は、同業他社への一時の競争力向上にはなるかもしれない。しかし、長期的に見て有効かどうかは冷静に考える必要があるのではないか。

原則5の生成から廃棄までの保護は、(5) 参照によるパーソナルデータ使用によって実現されている。すなわち、事業者は基本的にはパーソナルデータのコピーを持たず、必要なときは常に参照して利用するので、パーソナルデータが利用できるのはPDSで生成されてから廃棄されるまでの間である。その間の保護はリンクコントラクトの内容によって担保される。廃棄後はパーソナルデータ自体が理論上は世界から消滅するので、保護が破れる心配はない[14]。

原則6の可視化、透明化については、a) データ主体は自身のパーソナルデータがPDSにおいて論理的には自らによって管理されること、b) その使用についてはトラストフレームワークに則りリンクコントラクトに記載された方法で行われることによって保証されている。このため、事業者がパーソナルデータを囲い込む現在のパーソナルデータ集中管理に比べて、可視化、透明化のレベルははるかに高い。加えて、間接的ではあるが、PDS間でパーソナルデータを移動できるデータポータビリティも可視化、透明化を支援しているといえよう。

原則7の利用者中心の仕組みに関しては、データ主体の意図にしたがったリンクコントラクトによって利用がなされることで実現している。PDEにおいてプライバシーバイデザインを実現する本質的ツールとしては、PDSに基礎を置くリンクコントラクトと仮名化および参照による利用が重要な役割を果たす。制度的な仕組みとしては、トラストフレームワークに賛同する参加事業者によって運営されている共同体であることが本質的である。

---

[14] ただし、監督機関などの調査や監査のためにオフラインでデータを蓄積しておく場合は、暗号化も含めて厳重な管理が必用である。

以上述べてきたようにPDEは全て参加企業間の契約をベースにするので、「同意」があるわけだから、契約の範囲でパーソナルデータを利用している限りは法律的な問題もないし、パーソナルデータの越境もデータ主体が同意していれば可能であろう。しかし、だからといって法律に基づくプライバシー保護対策がなくてよいとは言えない。例えば、データ主体とPDE参加企業間でのトラブルもありえる。これはリンクコントラクトの解釈の相違、あるいはリンクコントラクトに違反した場合に起こりうる。したがって、トラブル処理を裁定する監督機関がやはり必要になる。米国であればFTC、日本であれば個人情報保護委員会がその候補であろう。逆にいえば、データ主体と事業者のトラブルの裁定機関としていきなり裁判所ではなく、パーソナルデータの監督機関を想定することができる。PDEの規約作りもこの点を留意する必要があるだろう。

PDEの応用としては多くの分野があるが、利益が大きく、同時にハードルが高いのが医療分野である。医療分野では従来までの個人情報の扱いに関する蓄積、あるいは慣性があること、人間の生命に関する事柄という特殊性のため、新規のシステム導入は難しいところである。それ以外の分野では、事業者の経済的判断でPDEが良いとなれば、大いに進展する可能性が高い。

2.4 VRM

事業者が顧客を選別してダイレクトマーケティングするような方法、すなわち事業者が自らの意図によって顧客をマネージメントするようなことをCRM (Customer Relationship Management)と呼ぶ。行動ターゲット広告もその範ちゅうに入るであろう。従来から行われている方法、すなわち事業者が顧客から収集したビッグデータを分析して、その結果を基に行われる顧客へのダイレクトマーケティングはほとんどがCRMの形態である。

しかし、CRMにおいてはデータ主体でもある顧客の意図はほとんど反映されない。顧客はたかだか、サービス開始時に行われる事業者からの契約文書に書かれた条件に承諾するだけである。承諾しなければサービスは利用できないという一方的な関係である。また、契約文書には、利用目的などを非常に広く解釈できるように書かれているころが多い。未知の第三者が利用することを妨げないという場合まである。

そこで、パーソナルデータの本来の持ち主(データ主体)である顧客が自身のパーソナルデータを管理する仕組みがありうる。そこでは顧客のパーソナルデータを使いたい事業者は顧客に利用申請し、顧客が同意した場合にはじめて顧客のパーソナルデータを利用できる。これをVRM (Vendor Relationship Management)と呼ぶ。VRMに関しては提案者のサールズの著書[Searls, 2012]に背景も含めた解説があるほか、パーソナルデータの利活用の視点からの解説書[城田, 2015]も参考になる。

VRMは前節で紹介したカブキアンのPDEを使うと容易に実現できる。サールズはVRMの考え方を実現するプロジェクトVRMにおいて以下の7つの目的を提案している。

(1)サービス事業者との関係を個人が管理するツールを提供する

(2)個人を自分のデータ収集の中心とする

(3)個人がデータをシェアさせる相手を選択できる

(4)個人が自己データを他人が使える期限を設定できる

(5)個人のデータを用いた事業者のサービスの条件を個人の裁量で決定できる

(6)個人がオープンな市場で需要を主張できる

(7)サービス事業者との関係管理ツールの標準、API、コードのオープン化

以上のうち、(2)はPDEのPDS、(3)と(4)はPDEにおいてリンクコントラクトの内容として記述できるものである。プロジェクトVRMはサールズが率いるプロジェクトであるだけに(1)や(7)のようなソフトウエアツールの目的や性格にも言及している。(7)のオープン化はVRMのツール開発事業者による顧客の囲い込みを防ぐことを意図している。PDEではXDIという標準を設けることによって、利用者である個人はPDSの乗り換えができたし、個人はサービス事業者の選択ができた。VRMでは抽象的にコードのオープン化で事業者の選択ができることを担保しようとしているが、PDEに比べると具体性が低い。

ただし、以下に説明する第四者はPDEでは直接触れられていないが、VRMで明示された具体的な概念である。

第四者[15]

ビジネスでは自分、相手、仲介者である第三者が存在することが多い。例えば、カード決済による物品の購入においては、自分＝消費者である顧客、相手＝販売者、第三者＝カード会社、となる。

ところが、どの顧客が販売者にとってよい顧客であるかは販売者にとってはなかなか掴めない。したがって、販売者は種々のデータから顧客のプロファイリングをして、そのプロファイルに基づいて行動ターゲティング広告を購入意欲の高そうな顧客に送りつけることになる。これが従来からのCRMのやり方である。ただし、販売者は顧客のプロファイルを推測しているわけで、必ずしもその精度は高くない。したがって、販売者は大量のデータを囲い込もうとする[16]。

VRMでは顧客は自分自身の行動データ、購買データなどのパーソナルデータを自分で管理している。ただし、それだけでは、無数にある販売者の中から自分の嗜好にマッチした販売者を見つけることは難しい。そこで、自分のパーソナルデータを代理人に預け、代理人はこれを使って多数の事業者との接点を作り出す。代理人は多数の消費者のパーソナルデータを預かってもよい。この消費者の代理人をVRMでは第四者という。

販売者からみれば、代理人のパーソナルデータベースを検索して見込みのある顧客を高い精度で見つけることができる。なぜなら、代理人の持っているデータは販売者が収集した不十分なデータからの推測結果ではなく、顧客本人の管理する正しいパーソナルデータだからである。

---

[15] fourth party

[16] これがビッグデータの一つの側面である。

第四者が上記の例では販売者、さらに一般にはサービス提供事業者にとって役立つことを述べたが、これは本来的には顧客の利益を代表し、その代理人として機能する存在である。このことは、第四者が持つ以下の特性から分かる。

(1)顧客は別の第四者に乗り換えることができる。
(2)別の第四者は同じサービスを提供できる。
(3)別の第四者に乗り換えたとき、パーソナルデータは以前契約していた第四者から移転できる。
(4)第四者はサービス事業者や販売者から独立している。
(5)第四者はその行動について消費者に対する説明責任を負う。

だが、(4)独立性や(5)説明責任に関しては顧客との間でトラブルが起こる可能性もある部分である。よって、独立した監督機関[17]が監査することを考えておく必要があろう。

VRMの実現をめざすベンチャー企業であるパーソナル・ドットコムは2011年に所有者データ契約という概念を打ち出した。

所有者データ契約
(1)データ主体の個人が自分のパーソナルデータの所有権を持つ
(2)データ主体の個人が他者のデータへのアクセスをコントロールできる
(3)データ主体の個人が承認した形でだけ事業者はデータ利用が可能である
(4)データ主体の個人の要求によってパーソナルデータを削除する

これはほぼ完全な自己情報コントロールになっていると考えられ、企業側からの提案としては非常にラディカルである。 ただし、当然、既存の事業者にとっては負担が大きく反対も強い。だが、PbDの立場からすれば、既存の事業者がPbDの第1原則：プライバシー保護は事後ではなく事前の予防措置、第2原則：プライバシー保護はデフォールト、第3原則：プライバシー保護は設計時に組み込む、という諸原則を無視したシステム設計をしてきたからだということになる。今後、どのようなプライバシー保護の方向に進むかを予見できないが、確実なことはデータ主体である個人が信頼できないシステムは淘汰されるということであろう。

2.5　将来の課題

プライバシーバイデザイン(PbD)はプライバシー保護における基本的性質を述べているため、米国やEUの法制度の改正にむけて積極的に取り入れられてきている。一方、日本の改正個人情報保護法も、実質的なプライバシー保護という目的を示さず、個人情報の概念

[17] 日本では個人情報保護委員会。

を中心とする規制枠組みを維持したこともあり、PbDの考え方を明示的に採用していない。

では、日本においてPbDの考え方は全く不要なのかというとそうでもない。PbDの普遍性から、社会、制度、産業のいろいろな場面で意識せざるをえない。

日本版の利用者中心トラストフレームワーク

カブキアンが提案したPDEやサールズが企画したVRMと同じようなアイデアに基づくプロジェクトが日本でも動き始めている。情報銀行コンソーシアム[Information Bank Consortium, 2014]、本報告書の主体である「集めないビッグデータコンソーシアム」[東京大学産学連携本部, 2014]などが活動を開始している。このような利用者中心のトラストフレームワークは利用者であるデータ主体と事業者という参加メンバーが契約に則って活動するので、参加メンバーの同意が基礎になる。契約に準じて問題なく活動が進んでいる間は、法制度の介入はない。だが、参加メンバーからの苦情は発生する余地があるし、場合によってはトラストフレームワーク外部からのクレームもありえる。そのような場合には、個人情報保護法がまず対応する法律になる。逆にいえば、トラストフレームワークの契約設計において個人情報保護法を意識しておかなければならい。

個人情報保護の独立監督機関である個人情報保護委員会は、個人情報等に関する苦情処理を自ら行わず、苦情の申出についての必要なあっせん及びその処理を行う事業者への協力を行うにとどまる。実際に考えても、多数になると予想されるトラストフレームワークの運用における苦情やクレームをいちいち独立監督機関まで持ち込むことは現実的ではない。そこで、トラストフレームワークの内側、あるいは外側に苦情、クレームに関する裁定者を必要とするだろう。裁定者の判断の基準となる規定はトラストフレームワークの契約に含める必要がある。個人情報保護の独立監督機関の役割はむしろこの契約自体の妥当性を判断することであろう。

以上、パーソナルデータの利活用についてショーンバーガーの事業者説明責任、カブキアンのパーソナルデータエコシステムの両極を対比しながら説明してきた。しかし、実際上は、どちらかの極に偏り過ぎるのではなく、個人の情報は個人が管理するという最近聞かれるようになった方向性にそって、この両極の間で最適なシステム設計を行うことが現実的である。

第3章　分散PDS

3.1　PDS

ほとんどのB2Cサービスにおいては事業者が多数の顧客のデータをまとめて集中管理している。顧客の連絡先や顧客との契約書についてはそのような集中管理が必須だが、集中管理されているデータは管理者の都合によって運用されがちであり、自己情報コントロール(とりわけ、自分のメリットを高めるように自分のデータを自由に活用すること)が難しく、ゆえに生活やB2Cサービスの価値が高まりにくい。また、ビッグデータと言われ始めて久しいが、大きな成果があまり出ていないのは、自社のデータしか使えないことが多いからだろう。たとえば新規顧客の開拓には既存の顧客以外のデータ(特に競合他社に由来するデータ)が必要だが、自社由来でないデータを収集するのは非常に難しい。

これらの問題を解決するには、事業者がパーソナルデータを集中管理するだけでなく、下図のように、個人も本人の(事業者との相互作用等に関する)データを管理することにより各個人(または家族や後見人などの代理人)が本人の意思に基づいて本人のデータを他者(他の個人や事業者)と共有して活用できる必要がある。そのための仕組みが前述のPDS (Personal Data Store) [Bell 2001; Searls 2012]である。

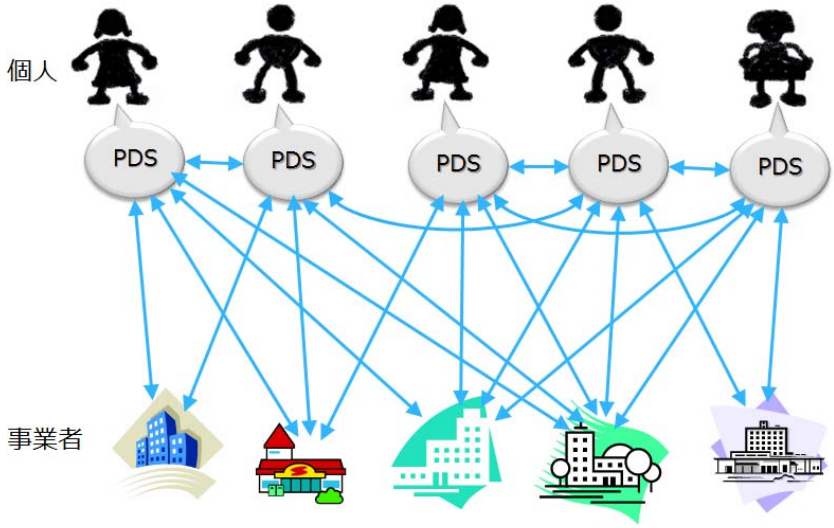

図3-1: パーソナルデータの本人による管理(分散管理)と事業者による管理(集中管理)の組合せ

PDSは、何らかのトラストフレームワークに従って運用され、個人による自己情報コントロールを担保する仕組みである。

PDSにも集中型のものと分散型のものがある。極端に言えば、集中PDS (centralized PDS)では、多数の個人のデータを集中管理する事業者が存在し、その事業者がデータ主体たる本人の意思を個別に確認せずにそのデータを利用できる。これは前章で紹介したショーンベルガーの考え方に近いと考えられる。一方、同じく極端に言えば、分散PDS (decentralized PDS) [青木 他, 2015; 橋田, 2013; 橋田, 2014]では多数の個人のデータを独断で利用でき

る管理者が存在せず、パーソナルデータの利用には本人(または家族等の代理人)の同意が必須である。これは同じく前章で述べたカブキアンやサールズの考え方に近い。実際のPDSはこれら両端極の間に位置付けられるが、前記のような問題の解決には十分に分散的な(つまり自己情報コントロールを十分に担保する) PDSおよびそれを含むパーソナルデータエコシステムが必要と考えられる。また、分散的であるということは1人の管理者が管理するデータが少ない(典型的には1人分に過ぎない)ということであり、そのデータを詐取するコストがメリットを上回るので、たとえば数万人分のデータの集中管理よりも圧倒的に安全であることに注意されたい。

3.2 集中PDS

ヘルスケアに関する集中PDSとして、EHR (Electronic Health Record; 医療機関同士が患者のデータを共有する仕組み)の他に、Google HealthやMS HealthVaultやPicnicHealthや日本の「どこでもMY病院」構想の下で開発されたシステム[厚生労働省, 2013]などのPHR (personal health record; 個人が本人の医療データを管理しヘルスケア事業者と共有して活用する仕組み)が挙げられる。これらはヘルスケアのための民間のPDSだが、デンマークのBorgerなどは、ヘルスケアに限らない多様なパーソナルデータを政府が集中管理して本人の役に立てたり企業等に提供したりするための仕組みである。米国政府が運用するBlue ButtonとGreen Buttonはそれぞれヘルスケアと電力に関する集中PDSと言えるだろう。日本の情報銀行コンソーシアムで検討されているインフメーションバンク[Information Bank Consortium, 2014]や代理機関[IT総合戦略室, 2015]も集中PDSに分類できる。

3.3 分散PDS

分散PDSには、個人端末同士のP2P通信によって利用者間での直接的なデータ共有を実現するものと、中継サーバを用いてデータを共有するものとがある。

前者のP2P型分散PDSとしてはPersonal Server [Want, 2002]などが提案されている。しかし、その後はいまのところ実験的にでも稼働しているものはなさそうである。スマートフォン等の個人用端末によるP2P型の分散PDSの実装は、端末の通信量や電力消費量に関する制約により当面は難しいだろう。

データ共有に中継サーバを用いる分散PDSでは、事業者の悪意や過失によるパーソナルデータの利用を技術的に防止するため、事業者による中継サーバの中のデータへのアクセスを制約する必要がある。そのためにホームサーバや特別な仕様の仮想計算機を用いるような分散PDSとして、Persona [Baden, 2009]、VIS [Cáceres, 2009]、PDV [Mun, 2010]、PrPl [Seon, 2010]、openPDS [deMontjoye, 2014]がある。これらのうちPersonaは個人ごとのデータの暗号化によって、VISとPDVとPrPlとopenPDSは各個人専用の仮想計算機等を用いて分散管理を実現する。

PLR (personal life repository; 個人生活録) [橋田, 2013; Hasida, 2014]は、下図のように、Googleドライブ やDropbox等の基本無料の出来合いのパブリッククラウドストレージをそ

のまま中継サーバとし、それをスマートフォン等の個人端末のアプリ(PLRサーバ)で操作する方式の分散PDSである。専用のサーバを必要としない個人端末用アプリに基づく仕組みなので、導入も運用もきわめて安価である。

PLRでは、クラウド運営事業者が独断でデータを利用したり本人を含む利用者のミスでデータが洩れたりすることを防ぐため、クラウド上でも端末内でもパーソナルデータを暗号化し、復号のための鍵は、原則としてGoogleやDropboxには開示せず、本人および本人が指定する他者のみに開示する。また、そのデータにアクセスするアプリを技術的に限定すること(DRM; digital rights management)で、本人および開示先の他者によるデータの利用法を制限することにより、本人を含む利用者の悪意や過失によるデータ漏洩等をなくすとともに、さらに柔軟な自己情報コントロールを実現する予定である。Android版のPLRサーバおよびそれと連携して具体的なサービスを提供するPLRアプリがすでに開発され、後述のように実務において運用されている。

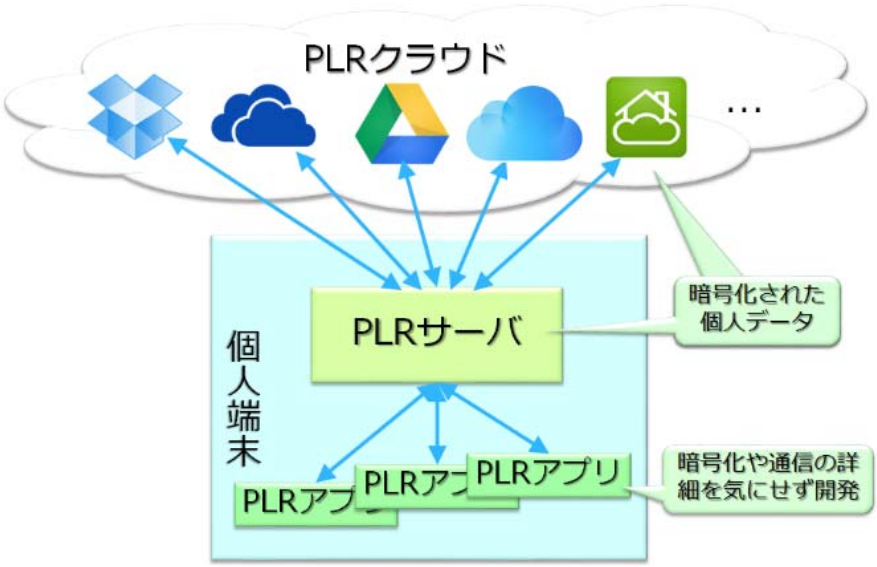

図3-2: PLRのアーキテクチャ

3.4　集中型サービスの間接的連携

集中型サービス(もちろん集中PDSも含む)同士の直接相互連携は通常はきわめて高価かつ困難であり、一般には不可能である。たとえば複数の銀行が合併する際にシステムを統合しようとして失敗するというようなことは珍しくない。また、競合する事業者同士が直接連携するのはほぼ無理だろう。複数のEHR同士の連携はそれらが標準的な仕様に基づいて実装されていれば可能であり、複数のインフォメーションバンクや複数の代理機関についても同様だろうが、EHRやインフォメーションバンクや代理機関を含むさまざまな集中型サービス同士を直接的に相互連携させることはできない。したがって、下図のように、あらゆるサービスを現実的なコストで連携させるには分散PDSが必要である。

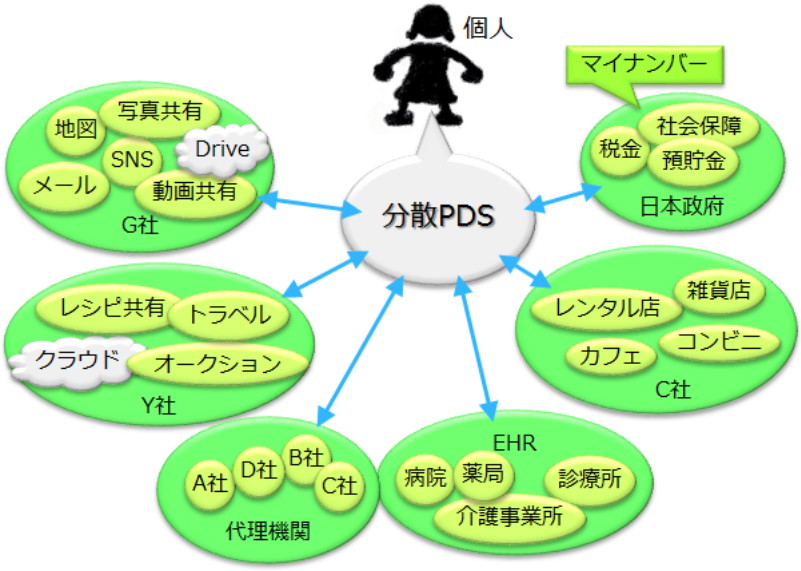

図3-3: 集中型サービスの間での間接的連携

この図ではたとえばG社やY社や日本政府がそれぞれ集中型サービスを提供しているが、これらが相互連携してパーソナルデータを融通し合うなどということは考えられない。日本政府がマイナンバーで管理する私の社会保証のデータとY社が管理する私の購買データを統合して分析するとか、そのように名寄せされたデータを多数の個人にわたって収集して分析するためには、分散PDSを使って個人が本人のデータを名寄せしたり、名寄せされたデータを本人同意に基づいて提供したりするしかない。

分散PDSによって多様な集中型サービスを連携させるための取り組みが前述のPLRに基づいて進められている。介護記録を作成し共有するアプリの基盤として介護の現場でPLRが実際に運用されている[橋田・和田・藤島・上沼, 2015]が、下図のように、介護施設のある入居者の介護記録のデータをその家族が管理して簡単に他者と共有して活用できる体制がPLRに基づいて構築され、2015年8月にその試験運用が始まっている。既存の介護情報システムにも介護記録等に家族がアクセスできるものがあるが、PLRを用いるメリットは、本人(家族)がそのデータを自由に他者(親類縁者、医療機関、他の介護施設、配食事業者、自治体、成年後見人など)と共有して活用できる点にある。

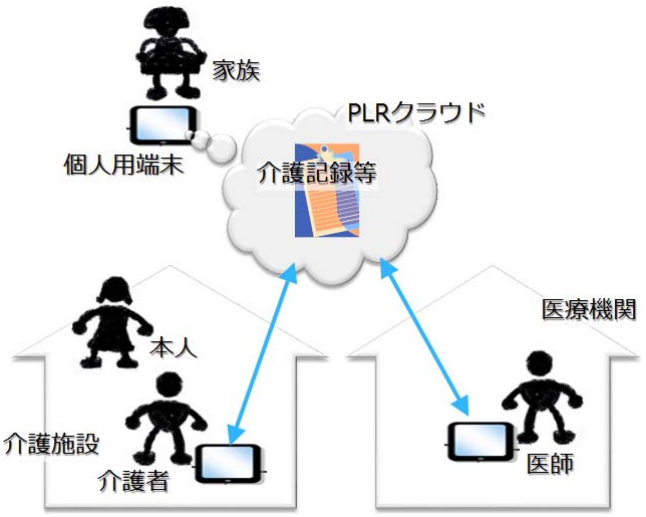

図3-4: PLRに基づく介護記録等のデータの個人管理による事業者等の間接的な連携

また、既存の医療情報システムとPLRとの連携も進めており、2015年末には下図のような自律分散協調的な地域包括ケアを目指したPLRの運用に入る予定である。

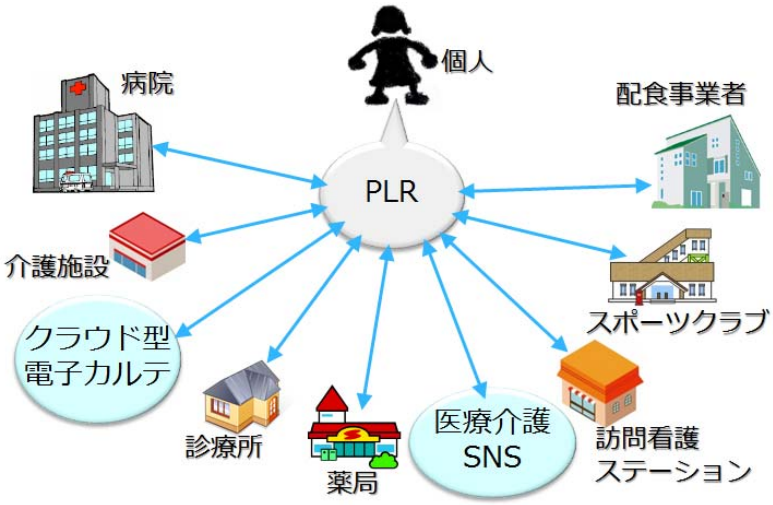

図3-5: 自律分散協調ヘルスケア

医療制度改革や地域包括ケアを実現するには多数のヘルスケア関連事業者がパーソナルデータを共有して相互連携せねばならない。しかし、前述のように集中型サービスを提供する事業者同士が直接連携するのは一般には不可能だから、PLRのような分散PDSを利用する個人が事業者の間の相互連携を仲介する必要がある。EHRや医療介護SNSなど、複数の事業者を連携させるサービスもいくつかあるが、図3-3のように、そのような連携サービス同士を相互連携させるにも分散PDSが必須である。

3.5　取引条件

一般にPDSとは、個人が他者(他の個人や事業者)との関係(サービスの授受など)を管理するためのツールである。その関係の管理は、関係の存在そのものや内容に関するデータの

管理を必然的に伴う。したがって、個人がPDSによって他者との関係を結んだり変えたり解いたりする際には、必ずそれに関連するデータの授受を管理することになる。

自分が相手に提供(開示または共有)するデータに関しては、相手による当該データの利用法に何らかの(空かも知れない)条件が課される。たとえば、自分の医療記録を医療機関に提供する際は「このデータに追記しても良いがデータの一部または全部を消去したり書き換えたりしてはならない」のような条件を課することになろう。自分の住所や電話番号を店舗等に提供する場合は「このデータは私への連絡のみに使って良い」というような条件が想定される。また、自分のデータを二次利用のために提供する場合、「私のデータはN≧1,000の統計分析に含めてその結果を自由に使って良いが、個票データを人間やロボットに見せてはならない」などの条件が考えられる。

データ提供に関する同意は、このような条件だけでなく、データの利用者や利用目的や対価にもよる。つまり、利用者が医師か弁護士か会計士か、提供者が利用者を好きか嫌いか、利用目的がデータ提供者へのサービスか他の営利事業か学術研究か、あるいはサービスを受ける対価はいくらか、そのサービスの質はどうか、または他の目的のためにデータを提供することでいくらもらえるか、等々に依存する。

これらの要因をすべて含む条件を取引条件(trade condition)と呼ぼう。サービスを受けようとする(または財を入手しようとする)個人が提示する取引条件をパーソナルRFP(personal Request For Proposal)と言う。たとえば、「〇月〇日に家族で京都に行くんだけど、2万円以内のおすすめプランを教えて。ちなみにうちの家族構成は…で食事の好みは～だけど、家族構成は他に漏らさないでね」のようなパーソナルRFPが考えられる。一方、財・サービスを提供しようとする者が提示する条件は提案(proposal)ということになる。実際に取引が行なわれるのは、パーソナルRFPと提案が両立する(両者の連言が充足可能な)場合である。パーソナルRFPは個人が提供するデータを提供先が利用する方法に関する条件(「家族構成は他に漏らさないでね」など)を含むが、その条件はデータ提供ポリシー(data provision policy)と呼ぶのが適当だろう。一方で提案は、そのデータの利用者である財・サービスの提供者が想定するデータの利用法に関する条件を含むが、その条件はデータ利用ポリシー(data usage policy)と呼ぶのが良いと考えられる。

取引条件のうちサービスの質等を評価したり担保したりする厳格な方法はないと思われる。一方、データ提供ポリシーを厳格に適用するには、データ所有者が管理するサーバの中にそのデータの利用を限定する方法と、DRMが考えられるが、前者は一般には難しいだろう。既述のようにPLRは、データの所有者がデータ提供ポリシーをDRMによって技術的に強制できることを目指している。これにより、ヘルスケア等に関連する機微なデータでも安心して提供できるようになり、パーソナルビッグデータの利活用が進むと期待される。

3.6　メディエータ

前述のVRMの典型的なユースケースにおいて、個人は、分散PDSで管理するデータを用いて、自分に適した商品やサービスに関する情報を個人端末のアプリによって取得する。

しかし、それらの商品やサービスは数百万・数千万に及ぶので、各個人がそれらすべてをウォッチし続けることは不可能である。したがって、多くの個人と多くの事業者(が提供する商品やサービス)の間の仲介が必要である。その役割を担う者をここではメディエータ(mediator)と呼ぶ。メディエータは個人かも知れないし、事業者かも知れないし、あるいは自然人格も法人格もない市場のような仕組みかも知れない。サールズ[Searls, 2012]の言う第四者もメディエータと考えられる。上述のインフォメーションバンクや代理機関[IT総合戦略室, 2015]のような集中PDSもメディエータとも言えるだろう。

メディエータの主な機能は個人と事業者(の商品やサービス)との間のマッチングであるが、それに伴って、個人や事業者を認証する機能やPDS用のクラウドストレージを提供する機能もあるかも知れない。マッチングとは需要と供給、消費と生産を結び付けること、つまり間接業務であり、これをまとめて自動化することによって社会全体の生産性が飛躍的に高まると期待される。

メディエータの正確な定義やその機能の詳細を解明することは今後の課題である。しかし、分散PDSの普及とそれによる生産性の向上においてメディエータが必須であることは上記の議論から明らかであり、以下本報告書でもしばしばメディエータに言及する。

今後の検討の叩き台として、想定されるメディエータの機能の概略を下の図3-6および表3-1にまとめておく。インフォメーションバンクや代理機関の機能もほぼ同様と考えられる。

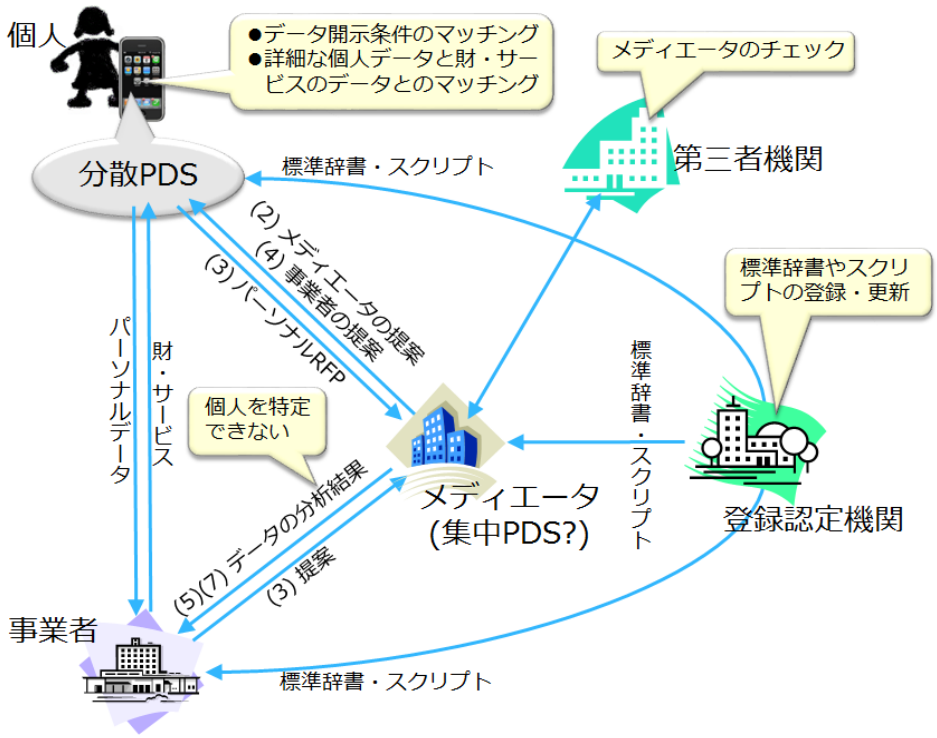

図3-6: メディエータの機能および他のプレーヤとの関係

表3-1: メディエータの担いうる機能

	機能	必須	対価
(1)	個人と事業者向けに分散PDS用のクラウドサービスを提供し、分散PDSの処理効率を高めるとともに、データ収集を高速かつ容易にする。		個人? 事業者
(2)	自らの取引条件(個人への提案)を公開する。	○	
(3)	パーソナルRFPおよび事業者からの提案を集め、それらをマッチング(統合分析)する。	○	個人にポイントを付与?
(4)	(3)に基づき、各個人に合った財やサービスや事業者に関するデータを当該個人に提供する。	○	個人?
(5)	(3)に基づき、財やサービスへの個人のニーズに関するデータを事業者に提供する。このデータは(3)における分析の結果であり、他のデータと組み合わせても個人を特定するのが十分難しいものとする。		事業者
(6)	(4)に応じた個人からの求めにより、個人と事業者の間での取引を仲介する。その一環として決済サービスを提供することも考えられる。		事業者
(7)	多数の個人のデータを分析してその結果を取得する機会を事業者に提供する。(5)と同じく、この結果も個人の特定が十分困難とする。		事業者

第4章　分散PDSのシステム概要

各所で生成されるパーソナルデータを、分散PDSを用いて個人を軸に管理し利活用しようとする場合、そのシステムにはどのような機能と構成要件を備えておく必要があるだろうか。ここでは、第3章で示された分散PDSを実装するためのシステムアーキテクチャを検討したので、報告する。まず、ユースケースの検討を通じて、分散PDSに必要な機能を洗い出す。次に、分散PDSに実装すべき必要最低限の機能要件を単純化して提示する。さらに、暗号技術を使うことによって、クラウドストレージ業者にデータ内容を読まれない工夫を施すことができること等を示す。なお、システム実現に向けた課題については、第6章で述べる。

4.1　ユースケース

「個人が管理するPDS」の機能とアーキテクチャを検討するために, 個人が自身の購買情報を収集/管理/第三者への共有を行い、第三者が生活者の食生活をサポートするサービスをユースケースとして, これらの機能によって実現可能なものであるかを検討する。

4.1.1 ユースケースの目的

生活者の購買情報は、独自のFSP (Frequent Shoppers Program)などのポイントカード/顧客カードを導入している小売事業者や、昨今会員獲得競争が激化している異業種提携による共通ポイントサービス事業者などの場合、CRM (Customer Relationship Management; 顧客関係管理)システムなどで管理・分析され、当該購入店舗/チェーン/グループ/提携事業者内でのクーポンやレコメンドサービスなどに利用される。しかし、事業者は顧客の自社以外での購買情報や顧客の健康状態/食生活を知り得るための情報を保有していないため、分析対象となる情報は顧客の生活全体における極一部に限られる。そこから分析して割り出された顧客の生活者像は断片的なものであり、顧客へ提供されるクーポンやレコメンドによるサービスの質/精度は決して高いものではないのが現状だ。また、適切なサービスを顧客に提供するためには、今後もしくは今その顧客が求めているニーズ/ウォンツを知るためのコミュニケーションが必要である。

もし、各事業者にサイロ化され管理されている生活者個人の情報を個人が管理するPDSへ収集し、どの事業者も保有しない自身で記録する情報などと合わせて管理することができれば、当該個人の全ての購買情報・健康/食生活に関する情報が紐付き、情報自体の質が高まる。そして個人が信頼する事業者に対して、それら情報とともに個人のニーズ/ウォンツを合わせて事業者に伝えることができれば、事業者は顧客へ最適なサービスを提供可能になることが期待できる。

また、PDSによって個人が自身の情報を管理し、同意のもとに第三者へ自身の情報を提供できるようになれば、現行個人情報保護法および改正案で度々議論されている事業者間での個人情報の第三者提供時の本人同意や匿名化の問題を解決することができる。

個人だけでなく、事業者がその情報を活用したサービスを当該個人に提供するためには、

各事業者保有データの個人への還元とともに、個人のニーズおよび情報開示条件と、事業者の提供サービス(提供価値)とサービス利用規約のマッチング、そして個人保有情報の詳細なアクセスコントロールができなければならないが、それが達成できれば生活者と事業者がお互いに信頼した情報共有/活用する社会の実現が期待できる。

4.1.2 ユースケースシナリオの概要

個人は自身が未保有の情報を、データ閲覧/ダウンロードサービスをオンラインサイトやAPIで顧客へ提供している事業者から取得し、それ以外の事業者が保有する情報(特にオフライン店舗での購買情報)は個人が家計簿サービスなどで電子化/登録しているレシートデータや手入力情報を合わせてPDSへ取り込み、管理する。また,医療情報などの機微なものはPDSへ取り込まず,外部に格納されている情報へのリンクを管理する.

個人へサービスを提供するサービスプロバイダ(SP; Service Provider)は、サービス利用条件や個人からどのような情報を開示されればどのようなサービスを提供可能かといったサービスカタログを作成する。

個人がサービスプロバイダのサービスを受けるには、自身が保有している情報から受けられるサービスをサービスカタログから選択するか、 自身が保有する情報、データ提供ポリシーなどを含むパーソナルRFP (Personal Request for Proposal)をサービスプロバイダに開示し、サービスプロバイダからそれに合ったサービスの提案を受ける。もしくは、既に自身が過去にサービスプロバイダから提案を受けたサービス一覧からサービスを検索して利用する。

個人とサービスプロバイダの間での取引開始後、個人は認証代行事業者(IdP; Identity Provider)との認証により、許可(Opt-In)を受けたサービスプロバイダへサービス提供に必要な個人の基本情報と共に、購買・健康情報などを開示する。サービスプロバイダは個人からその情報を受けて、サービスを提供する。この際、どの情報をどのサービスプロバイダにいつ開示したのかをPDS側で記録し、サービス提供後に情報開示は停止される。

4.2　機能とアーキテクチャ

4.1章のユースケースを受けて、本人(USER)のみならず、サービスプロバイダ(SP)、他人、デバイスなどがPDSにアクセスする際に「個人が管理するPDS」の以下の要件を満たす機能及びアーキテクチャを検討した。

1. 利用者がPDSを使用する際は、外部の認証代行事業者（IdP)による認証を用いることもできる。
2. 認証代行事業者を使用することで、本人の確からしさを確保することができ、より品質の良いサービスを受けることも可能となる。
3. サービスプロバイダ、外部のデバイス、利用者本人などからパーソナルデータを取り込んで管理することができる。
4. 利用者は、自分のパーソナルデータを活用することで、アプリケーションやサービス

プロバイダからサービスを受けることができる。

5. パーソナルデータのポータビリティを確保することで、他PDSとの連携や他PDSへのデータ移行などができるようになる。

アーキテクチャの概観を図4-1に、図中の機能一覧を表4-1にまとめる。

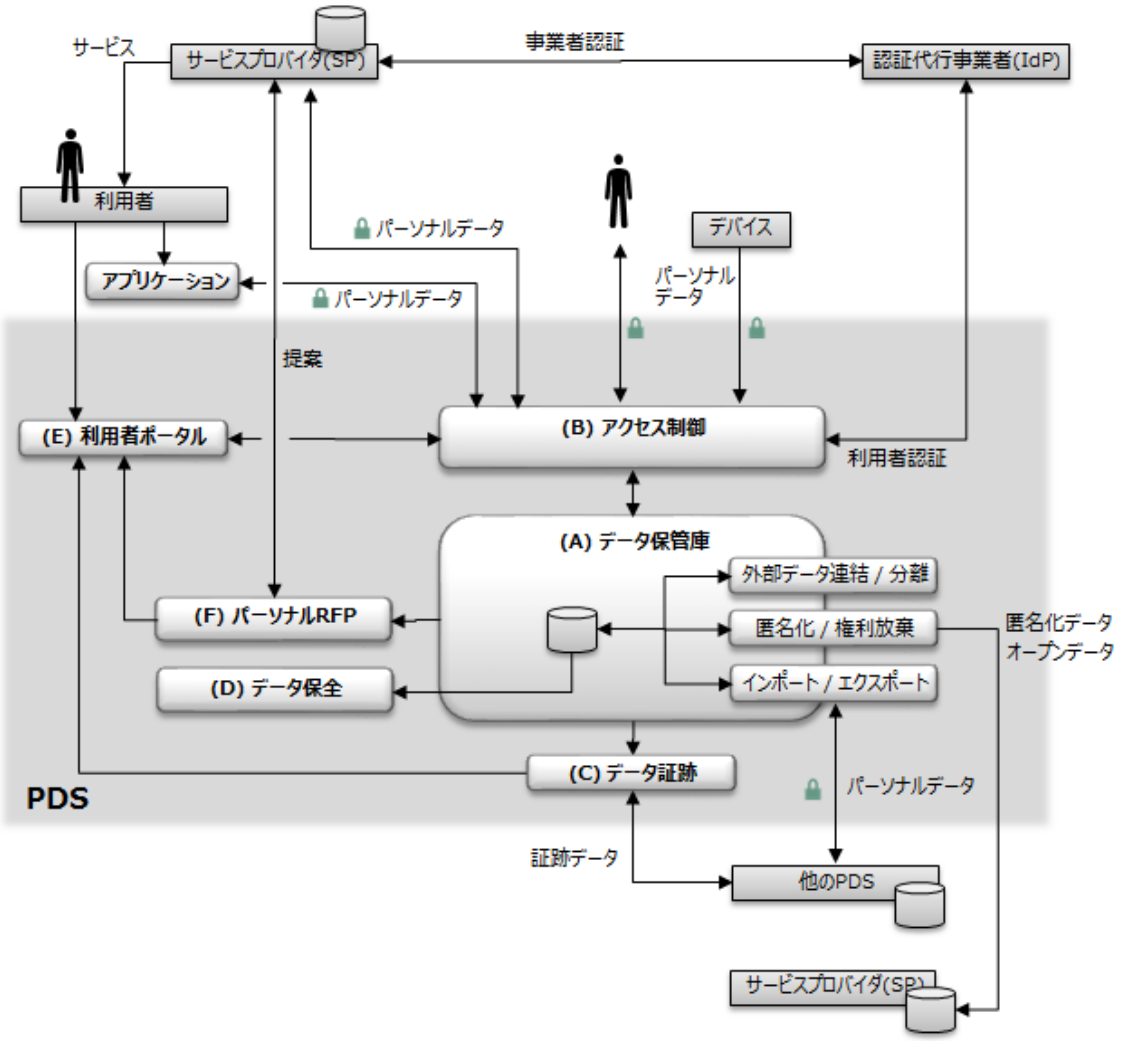

図4-1：PDSのアーキテクチャ

表4-1: PDSの機能一覧

	名称	概要
A	データ保管庫 Data Vault	✓本人に関するパーソナルデータを、本人が管理できる形で保管する ✓PLRではGoogleドライブ等のストレージサービスと個人端末によって実現している
	外部データ連結/分離 Attach/Detach	✓データ保管庫ではなく外部に保管されている個人に紐付けされたデータのマスターインデックスへの登録およびその解除 ✓PLRでは未実装
	インポート/エクスポート Import/Export	✓本人に関するパーソナルデータを本人が利用しやすい形で保管/出力する ✓データは提供先である本人のみが復号できるように暗号化する ✓PLRでは未実装
	匿名化 Anonymize	✓保管しているパーソナルデータを匿名化されたデータに加工する ✓PLRでは未実装
	権利放棄 Waive	✓保管しているパーソナルデータの一部を本人の意思により他システムで自由に利用できる形で公開する ✓PLRでは未実装
B	アクセス制御 Access Control	✓保管されているパーソナルデータについて、本人以外のアクセス権限を設定する ✓アクセス権の設定を受ける本人以外の利用者は、個人が一意に特定できる形で管理できる ✓PLRではストレージサービスのアクセス制御機能と暗号化との組合せによって実現しており、将来はDRMを実装する予定
C	データ証跡 Tracking	✓PDSに保管されているパーソナルデータに関する全ての操作(CRUD,Import,Export)のログを記録する ✓他PDSにエクスポートしたデータの利用状況を取得する ✓他PDSからインポートしたデータを利用する場合に、その利用状況を当該の他PDSに通知する ✓PLRではDRMによって実現する予定
D	データ保全 Data Integrity	✓外部バックアップ等によるデータ保全 ✓PLRではストレージサービスでの多重化によるバックアップを実装の予定
E	利用者ポータル User Portal	✓本人のパーソナルデータの他者による利用を承諾/拒否するための統合的な利用者インタフェース ✓PLRではPersonaryアプリが提供
F	パーソナルRFP Personal RFP	✓本人の保有しているデータや本人の意思に適合するサービス等に関する提案の募集 ✓当初はメニュー化されたサービス対応のみだが、将来はサービスプロバイダが個人の様々な提案要求に対応することを目指す ✓PLRではPersonaryアプリによってパーソナルRFPを作成し開示する予定
外部	サービスプロバイダ SP (Service Provider)	✓サービスを本人に提供する主体
外部	認証代行事業者 IdP (Identity Provider)	✓本人および事業者を認証する主体
外部	アプリケーション APL	✓PDSを利用するアプリケーション
外部	デバイス Device	✓PDSに情報を提供する各種デバイス

4.2.1 機能概要

このアーキテクチャは次に挙げる6つのコンポーネントから構成される。

(A) データ保管庫 (Data Vault)

保管されるデータは主に2種類あり、氏名、生年月日等の個人の変動性の少ない属性データおよび変動性のある体重記録、レシート情報等の実データといった内部で持つデータと本PDSシステムで直接保持しない外部データの所在情報であるマスターインデックスのデータがある。例えば、PDS利用者本人、あるいはその利用者が書き込み権限を与えた別利用者がPDS内にデータを作成したりインポートしたりする場合は実データに相当する。書き込みの仕方としては、PDSへ直接ファイルをコピーしたり、アプリ経由でのデータ作成等が考えられる。また、PDSシステム外部に存在するIoTシステムや他のPDSの個人に紐付く既存実データに外部データを連結(Attach)することもできる。この連結は、データ自体を外部で利用する場合はマスターインデックスで実現される。連結されたデータをマスターインデックスから個人の意思により分離(Detach)する機能もある。更にデータを個人情報保護の面でより円滑に利活用できる為にデータを匿名化(Anonymize)する機能やパーソナルデータに対する権利のオープン化を宣言する権利放棄(Waive)の機能も考えられる。

(B) アクセス制御 (Access Control)

第三者へ権限を与える事により、情報へのアクセス制御を任意に設定する事ができ、どの情報を誰に開示するかをコントロールできる。第三者となるサービスプロバイダとしては個人、事業者、自治体や医療機関等の組織だけでなくデバイス自身も考えられる。いずれも前提として認証局の役割を果たす認証代行事業者にてサービスプロバイダ自身の認証が事前に完了している必要がある。情報開示に対しての様々な個人的なスタンス(マインド)に柔軟に対応する為に開示レベル設定の機能も考えられる。一例としてパーソナルデータの項目名(例：「生年月日」)と項目の値(例：「x年y月z日」)をそれぞれ別に管理する機能も可能である。例として項目名を開示するが値自体は開示したくない人が考えられる。第三者への開示は避けて自分の情報を厳守したい人もいれば、便利なサービスを受けられるのであれば情報開示に対してオープンな人、中間に当たる人それぞれにたいしてカスタマイズできる機能が考えられる。更にXACML(eXtensible Access Control Markup Language)の様なアクセスポリシーを記述するXMLベースのスタンダードを導入する事によってアクセス制御をより汎用的で互換性の高い機能として実装できる。従って複数のサービスプロバイダのアクセス制御に関する用語とポリシーの記述方法の統一化を想定する。

(C) データ証跡 (Tracking)

利用者のPDSに保管されているデータの変更・更新・情報開示等の様々な履歴を取得する。インポート/エクスポートされたデータはインポート元、エクスポート先へデータ履歴を通知する事ができる。例として個人がデータの削除を依頼した場合、そのデータが確か

に消された証拠となる。

(D) データ保全 (Data Integrity)

データ紛失・破損および改ざんのリスク回避の為、外部バックアップ等のデータ保全ができる。本機能は無駄なデータの増幅を防ぐ為の変更差分でのデータ保全、および複数世代のデータ保全・管理機能がある。

(E) 利用者ポータル (User Portal)

PDSの各種機能を可視化した利用者インタフェースを提供する。各種機能の一例として、[(B)アクセス制御]の「誰に何のデータを開示しているか」、[(C)データ証跡]によるデータの利用情報などを表示する、[(F)パーソナルRFP]のサービスカタログなどの機能がある。ポータルへのログインは、より高いレベルでの個人の確からしさを保証する認証代行事業者経由の認証で行うことも考えられる。

(F) パーソナルRFP (Personal Request For Proposal)

利用者の要求情報(受けたいサービスなどのニーズ)と共に利用者のデータ開示情報をサービスプロバイダに送る事によって、受けられるサービスやサービスプロバイダからの提案を閲覧する事ができる。これらの要求情報はサービスプロバイダにて個人が自らの意志で開示したPDSの個人情報をもとに質の高い分析ができ、また個人利用者においてはよりニーズに合うサービスとマッチングされる。複数の個人と複数のサービスプロバイダを結びつける仲介役(メディエータ)が、パーソナルRFPをサービスプロバイダが扱えるように加工したり、複数のサービスプロバイダからの提案を個人に最適化してまとめて提供したりすることも考えられる。このパーソナルRFP機能には何段階かの実装レベルがあり、個人がサービスを選択できるようにサービス内容およびサービスを提供に必要な情報をカタログ化したサービスカタログ機能から始まり、最終的には個人のパーソナルRFPと事業者の提供を市場メカニズムによって調整する機能が想定される。

4.2.2 シナリオと機能要求

4.2章で定義した機能を、ユースケースシナリオから抽出した機能要求に当てはめる。

機能要求①：データ閲覧/ダウンロード対応サービス(例えば食材デリバリーサービスやヘルスケアアプリ)から登録する

1. 利用者は[(E)利用者ポータル]からログインし、ダウンロードに対応しているサービスプロバイダのサービスをサービス一覧から選択する。
2. 認証代行事業者経由でサービスプロバイダへ本人認証した後、選択したサービスのデータが[(A)データ保管庫]へ取り込まれる。取り込んだ履歴は[(C)証跡]で記録される。

機能要求②：機械判読可能な形式のデータ（例えば家計簿サービスからダウンロードしたファイル）を登録する

1. 利用者は[(E)利用者ポータル]からログインし、[(A)データ保管庫]に登録対象データとデータフォーマット(csv、xmlなど)を選択する。
2. [(A)データ保管庫]へデータが取り込まれる。取り込んだ履歴は[(C)データ証跡]で記録される。

機能要求③：自身しか保有していない情報（例えばレシピ情報と料理写真）を手動で登録する」

1. 利用者は[(E)利用者ポータル]からログインし、[(A)データ保管庫]に登録するデータの種類からレシピ情報 を選ぶ。
2. 各項目を手動で入力や画像を指定し、[(A)データ保管庫]に登録する。登録した履歴は[(C)データ証跡]で記録される。

機能要求④：PDSに取り込まれていない外部にあるデータ（例えば医療記録）の所在情報を登録する

1. 利用者は[(E)利用者ポータル]からログインし、[(B)アクセス制御]経由で[(A)データ保管庫]の外部データ連結機能を使って情報のメタデータと所在情報を登録する。
2. 登録された情報のメタデータと所在情報は[(A)データ保管庫]のマスターインデックスに登録される。登録された履歴は[(C)データ証跡]で記録される。

機能要求⑤：保有情報から受けられるサービスの提案をサービスプロバイダへ要求し、サービスプロバイダからサービス提案を受け、サービスを利用する

1. 利用者は[(E)利用者ポータル]からログインし、[(F)パーソナルRFP]で自身が保有する情報項目から享受可能なサービスの提案をサービスプロバイダへ要求する。
2. サービスプロバイダは、受領したパーソナルRFPの情報から最適なサービスを利用者に提案する。そのサービスは、[(E)利用者ポータル]のサービスカタログに登録される。
3. 利用者は、サービスプロバイダから提案されたサービスの内容と利用条件を確認し、当該サービスを利用する場合は、[(B)アクセス制御]からサービスプロバイダへサービス利用に必要な情報項目のデータを開示する。開示した先と開示情報の履歴は[(C)データ証跡]で記録される。
4. サービスプロバイダは認証代行事業者経由で個人を認証し、サービス提供に必要な基本情報と情報項目の開示を受ける。サービスプロバイダが情報を参照した履歴は[(C)データ証跡]で記録される。
5. サービス提供は、サービス提供者側のUIなどPDS外で行われる。
6. 取引終了後、利用者はサービスプロバイダへの情報開示を[(B)アクセス制御]から(もし

くは一定期間後に自動的に)取り消し、[(C)データ証跡]へ記録される。

機能要求⑥：受けたいサービスをサービス一覧から検索し、サービスを利用する

1. 利用者は[(E)利用者ポータル]からログインし、[(F)パーソナルRFP]に登録されているサービスプロバイダのサービスカタログ一覧から、自身が保有する情報項目から享受可能なサービスを検索し、選択する。
2. 利用者は、[(B)アクセス制御]からサービスプロバイダにサービス利用に必要な情報項目を開示する。 開示した先と開示情報の履歴は[(C)データ証跡]で記録される。
3. サービスプロバイダは認証代行事業者経由で個人を認証し、サービス提供に必要な基本情報と情報項目のデータの開示を受ける。サービスプロバイダが情報を参照した履歴は[(C)データ証跡]で記録される。
4. サービス提供は、サービス提供者側のUIなどPDS外で行われる。
5. 取引終了後、利用者はサービスプロバイダへの情報開示を[(B)アクセス制御]から(もしくは一定期間後に自動的に)取り消し、[(C)データ証跡]に記録する。

機能要求⑦：パーソナルRFPを公開し、サービスプロバイダからの提案を待つ

1. 利用者は[(E)利用者ポータル]からログインし、[(F)パーソナルRFP]で自身が保有する情報項目や享受したいサービスの内容を公開する。
2. サービスプロバイダは提供可能なサービスに該当する利用者の出現を検出すると、当該利用者へサービスを提案する。
3. 利用者は、サービスプロバイダから提案されたサービスの内容と利用条件を確認し、当該サービスを利用する場合は、[(B)アクセス制御]からサービスプロバイダへサービス利用に必要な情報項目のデータを開示する。開示した先と開示情報の履歴は[(C)データ証跡]で記録される。
4. サービス提供は、サービス提供者側のUIなどPDS外で行われる。
5. 取引終了後、利用者はサービスプロバイダへの情報開示を[(B)アクセス制御]から(もしくは一定期間後に自動的に)取り消し、[(C)データ証跡]へ記録される。

4.3 PLRにおける安全なデータ共有の実現方法

本節では、分散PDSにおける安全なデータ共有を実現するため、PLR (Personal Life Repository)において、どのような暗号の仕組みが使われているかを報告する。PLRでは、実際のデータはパブリッククラウド(現在ではGoogleドライブ)に置かれているが、基本的には、クラウド事業者にも内容がわからないように暗号化されている。

たとえば、Aさんの住所は、PLRが規定するGoogleドライブ中のフォルダ(profileフォルダと呼ぶ)の中に暗号化されて置かれる。鍵の運用の方法を図4-2に示す。このprofileフォルダには、共通鍵kで暗号化された住所データと、Aさんの公開鍵で暗号化された鍵kのデータ(このデータのファイルはAさんのPLR-IDを所定のハッシュ関数で変換した結果を名前に含む)

が格納されている。このようにデータを配置しておくことによって、Aさんは、自分の秘密鍵で鍵kを復元し、kで住所データを復元できる。自分の公開鍵で住所データを暗号化しておく方法もあるが、住所データ以外の長いデータも同一手順で高速に処理できるよう、高速な共通鍵暗号と低速な公開鍵暗号を組み合わせた本方式を用いている。各自の公開鍵は暗号化せずに格納されている。この公開鍵は、Googleドライブのアクセス制御によって、本人しか更新できないようになっている。

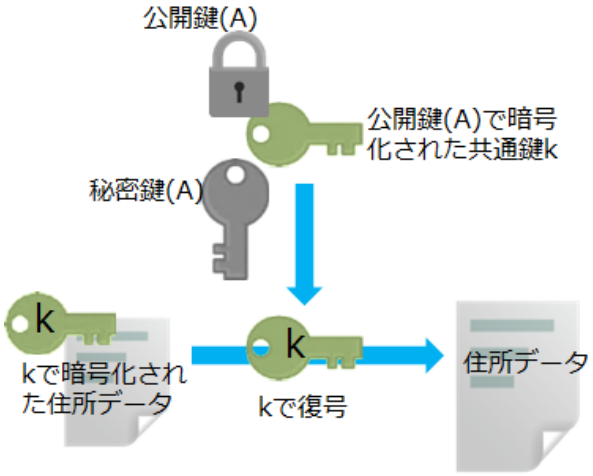

図4-2: 鍵の運用

ここで、BさんがAさんの住所を教えてもらうという名簿管理アプリ(Personary)のユースケースを考える。Bさんはあらかじめ AさんのPLR-ID (PLRにおけるAさんの識別子。現在はメールアドレスを利用)をなんらかの方法で入手しているものとする。Bさんは、名簿管理アプリのインタフェースより、AさんのPLR-IDを入力し、Aさんに「友達」申請をする。このとき、Aさんが自分の公開鍵を参照できるように、公開鍵を含むGoogleドライブ中のファイルのURLをGoogleドライブによってAさんに開示する。AさんのPLRサーバはBさんからの友達申請を自動的に了承し、自分の公開鍵を含むGoogleドライブ中のファイルのURLをGoogleドライブによってBさんに開示する。こうしてAさんとBさんは互いの公開鍵を取得する。

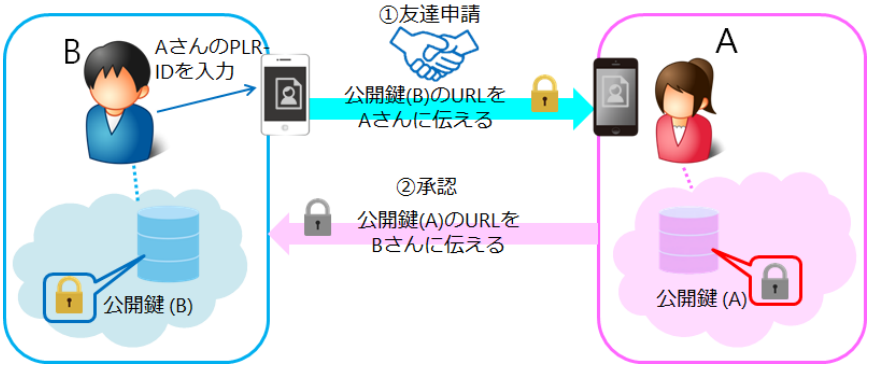

図4-3: 名簿管理アプリによる友達申請

次に、Bさんが名簿管理アプリを使ってAさんに住所が欲しいとのリクエストを送ると、Aさんの名簿管理アプリにBさんからのリクエストが表示される。Aさんがこれを了承すると、Aさんの名簿管理アプリは、BさんがAさんの住所を読めるように、kをBさんの公開鍵で暗号化したデータをAさんのprofileフォルダに格納する。

Aさんからの許可がおりると、Bさんの名簿管理アプリは、Aさんのprofileフォルダから、暗号化された住所データと、自分用に暗号化された鍵データを入手し、これらを用いて住所データを復元する。

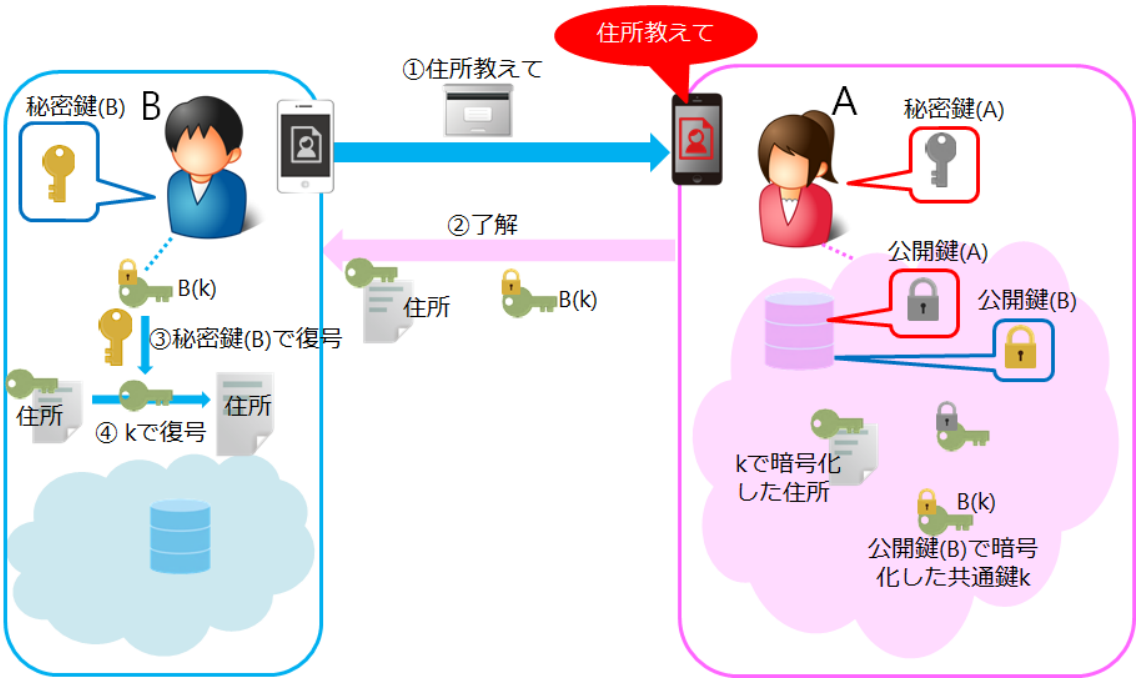

図4-4: 名簿管理アプリによる住所データへのアクセス

第5章　分散PDSのサービスモデル

5.1　スマートタウン

5.1.1 スマートタウンの定義

分散PDSの特徴を活かせるユースケースの一つとして、スマートタウンにおけるPDSの活用について、ビジネスモデルの視点も含めて考察する。一般的にスマートタウンやスマートシティというと、先端技術を活用して街全体の電力の効率的な利用を図るように設計された、環境に配慮した街や都市という意味合いで使われ、HEMS (Home Energy Management System)機器やスマートメーターまたはそれらで扱う電力使用量などと一緒に語られることが多いが、ここでは、ICT技術を駆使して、そのエリアに住まう人が、安心・安全に快適・便利な暮らしを送り、その個人を顧客とする事業者側も事業が活性するように考慮された街や都市と定義し、そのエリア内で発生するデータも電力使用量データのみならず、それ以外のイエナカや購買に纏わるデータ、そこに住まう個人の属性情報などのデータも含め、PDSでの利活用について検討した。なお、本ユースケースにおいては、そのエリアに住んでいることが確認された個人がPDSを使用し、そのメリットを享受できる想定で考えている。

5.1.2 イエナカの暮らしとプライバシー

まず、スマートタウンにおけるイエナカの暮らしに目を向けてみる。前述のHEMS機器やスマートメーターなどで扱われる電力使用量以外に、スマート家電と呼ばれる電化製品では、家電ごとの電力使用量が分かるだけでなく、料理や洗濯をしている時間帯も分かるようである。また、最近のマンションでは、オートロック機能によって鍵の開錠・施錠が管理され、在宅しているかいないかも分かるらしい。ここまでイエナカにICT技術が入り込んでくると、そこに住まう人の暮らしが便利になる反面、個人の暮らしぶりが知らぬ間に事業者に対してオープンになっているのではないかという、所謂プライバシーの懸念が付きまとう。そこで、イエナカで発生するデータをコントロールする権利を個人に与え、個人が意思を持ってパーソナルデータの利活用を事業者に許諾することができるようになれば、個人にとって、より便利で付加価値の高いサービスを受けることが期待できるだろうし、新たなビジネスが生まれる可能性もあると考える。それを実現するための仕組みとして、第3章・第4章で述べた分散PDSが有効であると考えられる。次項では、PDSを使用して個人が自分のデータをコントロールすることによって期待できる利活用ケースを述べる。

5.1.3 電力使用量データの利活用

HEMS機器やスマートメーターで扱われる電力使用量データの活用という意味では、個宅や部屋単位、家電単位での使用量の見える化や家電等の制御が容易に想像される。この電力使用量データをコントロールする権利を個人が持ち、他の事業者に開示し、利用許諾することが可能になれば、別サービスでのパーソナルデータの利活用が促進されよう。

例えば、独り暮らしの老人世帯における電力使用量を読み取り、その状況を監視することで、ある一定期間、電力使用量に変化が見られない場合に、予め個人の指定した第三者にアラートを挙げるようなサービス、所謂見守りサービスに活用できるだろう。また、電力供給の逼迫時には、近隣のスーパーなど流通業者からリアルタイム性のあるクーポンやタイムセールの案内を送り外出を促したり、電力使用量だけでなく、家族構成や趣味・嗜好を開示しておくと、それらを加味した、時間限定のグルメ情報が配信されるなどのサービスも考えられるだろう。

5.1.4 リフォームデータ・設置機器データの利活用

業者にリフォームを依頼した際に行われる間取りの調査や採寸などによって得られるデータも、宅内の様子を伺い知ることができるパーソナルデータと考えられる。間取りの情報だけでなく、施工時期、壁や床に使用している部材、その耐用年数、あるいは設置した機器やそのメーカーなどの情報も有効に利活用ができるデータになり得るだろう。現状、それらの情報は、リフォーム業者で管理されたり、依頼者個人の手元に紙の形で残るのが通常と思われるが、個人が容易に取扱えるデジタル形式で管理する前提で利活用を想定してみる。

例えば、購入または設置した機器の修理や消耗品の補充などを行う場合、メーカーへの問い合わせや修理の依頼など、個別に自分自身で対応するのは面倒で骨が折れることである。

設置機器に関する保証期間や型番、購入店舗などの情報をPDSで管理し、メーカーやメンテナンス業者に予め開示しておくことができれば、適切なタイミングでオファーを受けることが期待できる。メーカーやメンテナンス業者にとっても、機器の保証期間や状態を把握することで、買換えやアフターメンテナンスの提案もできるようになるだろう。また、修理や消耗品のケースだけでなく、該当する機器にリコールが発覚した場合も、個人、メーカー双方にとって、特にメーカーから該当機器の所有者に連絡する手段としてPDSが有益なツールになり得るのではないかと思われる。

5.1.5 パート・アルバイトにおけるマッチング

5.1.3、5.1.4では、個人の所有する機器等で発生するデータや機器そのものに関する情報の利活用について記述した。この項では、一つの行政区など比較的範囲の限られたエリア内で、個人が職探しのために通常必要とされる情報を利活用するケースについて考察してみる。

通常、個人がパートやアルバイトに応募する場合、氏名・住所・電話番号等の連絡先以外に、応募先によっては保有資格や略歴の提示を求められることがある。これらのパーソナルデータをPDSで一元的に管理しておき、これらの情報を応募先の事業者に開示するケースを考えてみる。この場合、応募する個人と募集する事業者とが、PDSを通じて直接繋がることも可能であろうが、事業者の数が増えてくると、個人と事業者とを仲介する第三

者の存在が必要になってくる。この仲介役が3.6で述べたメディエータの一つの機能である。このケースにおいてメディエータは、個人から示された条件(データ提供ポリシー)と事業者から示された条件(データ利用ポリシー)との刷り合わせを行い、マッチングする役割を有する。限られたエリア内で過去の経験や時間を有効活用したいというニーズを満たすことができるようになれば、専業主婦や会社をリタイアしたシルバー人材の再雇用を促進し、地域を活性化するための仕掛けとしても期待できるのではないかと考える。

5.1.6 サービスフロー・収益モデルの仮説

繰り返しになるが、今回のスマートタウンのユースケースでは、何らかの方法でそのエリアに住んでいることが確認された個人がPDSを使用することを前提においている。また、個人が自分のパーソナルデータを開示する相手も、別の機関等から客観的に認定されている事業者である方が、個人にとっても安心感があると考えられ、それら個人や事業者間の信頼関係に基づく枠組み(トラストフレームワーク)や個人の認証を行う機関もしくは機能(IdP：認証代行事業者)も必要であるが、個別の説明は割愛する。本項では、トラストフレームワークをベースとしたPDS使用時のサービスフローと、それを前提とした収益モデルの仮説について以下に述べる。

【基本フロー】

(1)その地域に住む生活者個人は、地域ポータルサイトの提示する利用規約に同意し必要事項を登録することで、地域ポータルサイトにサービス提供者として参加する事業者のサービスを利用する権限を得る。ここでは、地域ポータルサイトがIdPの機能を担うと仮定する。

(2)登録時の個人情報(氏名、住所、性別、生年月日)は、IdPにて集中的に管理される。

(3)IdPに登録した個人は、PDSの機能を使うことができる。

(4)個人はPDSにおいて、IdPで集中管理される個人情報以外の属性情報(職業、年収、家族構成、保有資格など)やサービス事業者が保有する様々な利用履歴も一元的に管理・制御し、指定した相手に開示することができる。

(5)個人が開示する情報によって、受けることができるサービス事業者のサービスが一覧表示される。

(6)個人は、サービス事業者の提示する利用規約に同意し、PDSで管理されている個人情報をサービス事業者に開示する。

(7)サービス事業者は、個人から開示された情報に基づき、個人に対して直接サービスを提供する。

【コンシェルジュ】

個人と事業者双方の開示条件をマッチングする役割として記述した。(3.5 取引条件、3.6 メディエータ)

(8)個人がサービス事業者から個別に提案を受けたい場合は、PDSの機能を使用してサービス事業者に提案を要求する。

(9)サービス事業者は、個人から受け付けた提案要求に対してサービスの提案を行う。

【データブローカ】

今までは各サービス事業者が自ら、個人情報の取得・利用目的、第三者への開示・提供などについて、そのサービス使用者たる個人から同意を取得し、その範囲内でパーソナルデータの利活用を模索しているが、個人から明示的にパーソナルデータ利活用の許諾を受け、その範囲で、専らパーソナルデータを取扱う事業者があっても良いだろう。広義ではメディエータと呼べるかもしれない。このデータブローカは、基本的には個人が特定できないように統計処理されたデータを扱うことを想定するが、パーソナルデータの売買も議論の余地があるだろう

(10)個人は、データブローカに対しパーソナルデータの利活用を許諾する。

(11)個人が開示に同意したパーソナルデータがデータブローカに渡される。

(12)データブローカは、個人から許諾を受けた範囲で、パーソナルデータを必要とする別事業者に利用許諾ないしは販売する。

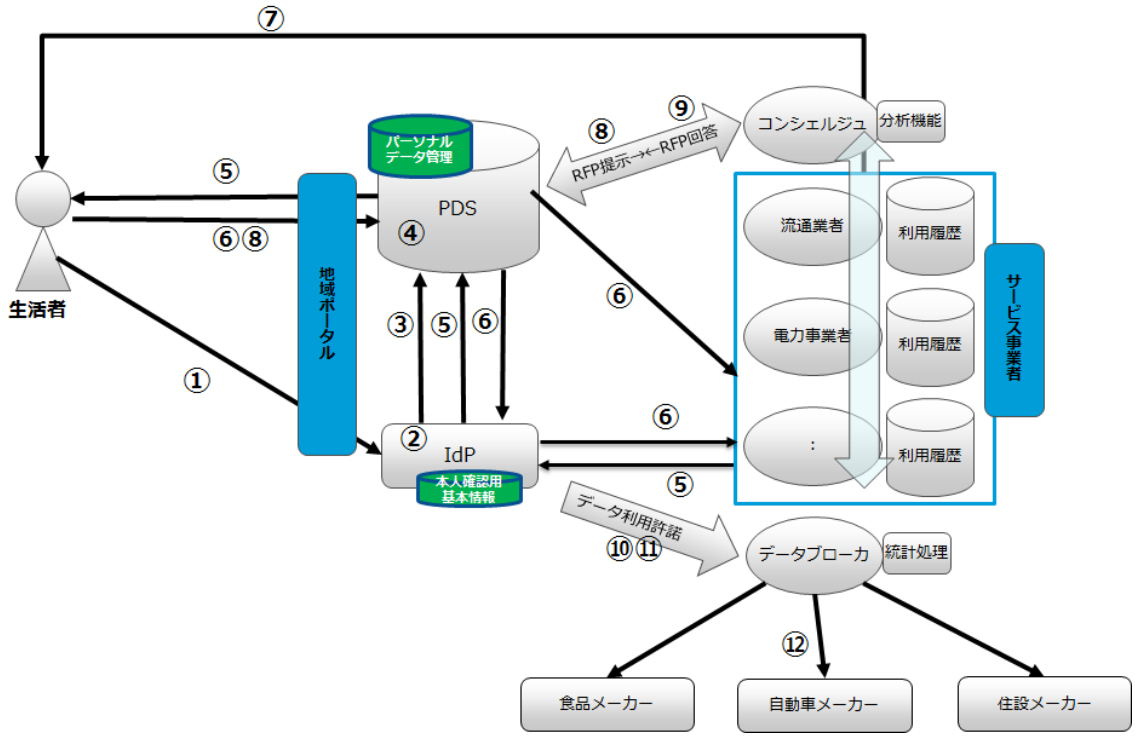

図5-1：サービスフロー

上記のサービスフローを前提とした場合の地域ポータルから見た収益モデルとして、例えば以下が考えられる。但し、個人個人が持つPDSが中心軸になるビジネスモデルにおいては、制度・ルール設計やビジネスモデル実証の議論が必要だろう。また、PDSを使用する生活者個人のITリテラシーの向上や、教育も含めたプライバシー・パーソナルデータに対する意識向上も、今後の課題として考えられよう。

⑴地域ポータルサイト(PDS機能の提供も含む)の利用による個人からの利用料収入
⑵各サービス事業者からのシステム利用料収入
⑶サービス事業者間の送客またはデータ共有による成果に応じたアフィリエート収入
⑷データブローカ経由のデータ販売・利用料収入

5.2　スマートライフ

2025年には高齢化のピークを迎え、医療、介護のリソース不足が予想されており、高品質な医療・介護サービスを受けることのできる社会インフラの整備が急がれている。国や自治体による社会実装に向けた実証実験が各地域で同時進行しているが、個人の医療情報は個々の医療機関で個別に管理されており、その機微な医療情報をいかに個人単位にまとめて管理し、医療圏を超えた運用を実現できるかということが課題となっている。[総務省, 2014]

これらの課題を解決した時、ヘルスケア領域にはICT (Information and Communication Technology)の活用によりライフログの一部としてバイタル、メンタル、医療データ、ゲノム情報等のPHR(Personal Health Records)の情報を蓄積したビッグデータが構築され、個々に適した治療、介護サービス等を享受できる新しいビジネス開発の可能性を秘めている。

個人の疾病発症時に支払う医療費を、疾病予防のための消費にかえることで、医療費削減と新規市場の創出といった効果がもたらされる可能性がある。

社会保障費の多くを占めると言われる65歳以上の医療費、生活習慣病の医療費の増加をおさえるためには、健康維持のための適切な運動、食餌(食事)管理を行うことが必要であるが、そのためには多くの人が健康を意識しはじめる中年期以降からではなく、少年期からの健康リテラシーの向上が求められる。生涯を通じて健康を意識して生活するためにも、個人の健康関連ライフログが誕生時から連続して把握できる仕組みが必要である。

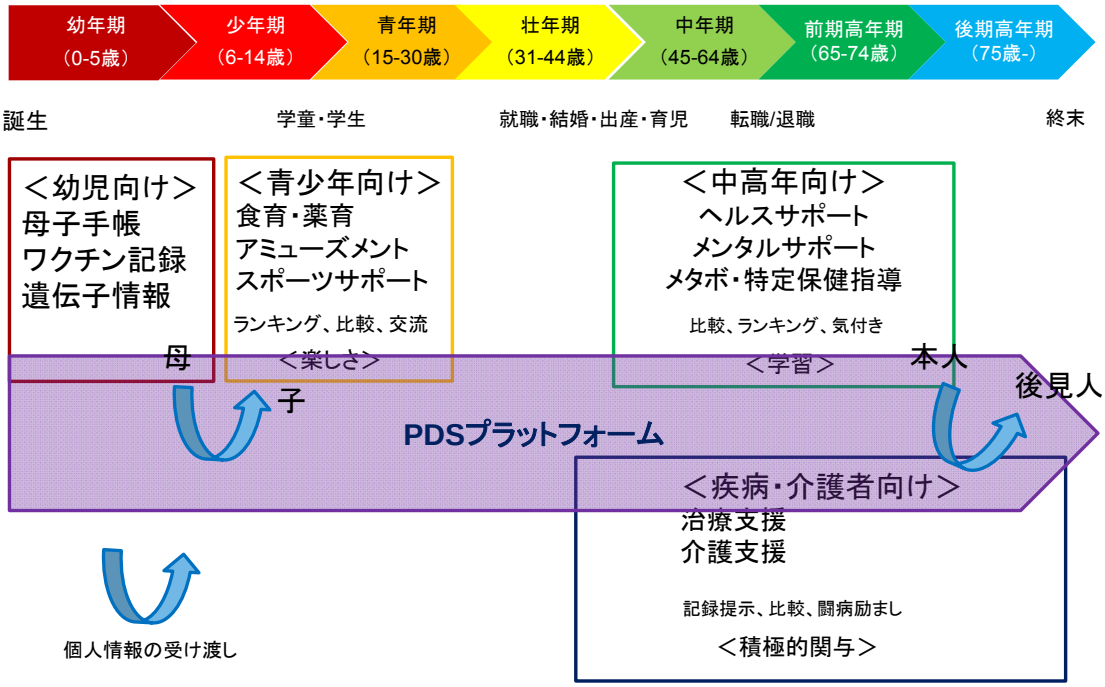

図5-2：スマートライフにおけるライフステージと想定アプリ

所属する組織・地域(学校、企業、自治体など)や医療機関などに分散して管理されている

健診・医療データなどは個人が自ら集める以外に方法はない。

国が進めるスマートライフや健康日本21は、生活改善や予防による健康寿命の延伸であるが、生活者自身が分散PDSアプリで医療情報などをコントロールすることができるようになると、次のような未来が見えてくるであろう。

5.2.1 疾病管理手帳

旅先で具合が悪くなり診療所・病院を受診した際、診療所や病院で既往症や服薬状況などを医師から質問されるが、いまはこれらを体調が悪い中で思い出しながら伝えることになる。

分散PDSの疾病管理手帳があれば、過去の受診歴をもとに、医療情報、調剤(処方)情報、健診データ、バイタルデータなどを提示することができる。

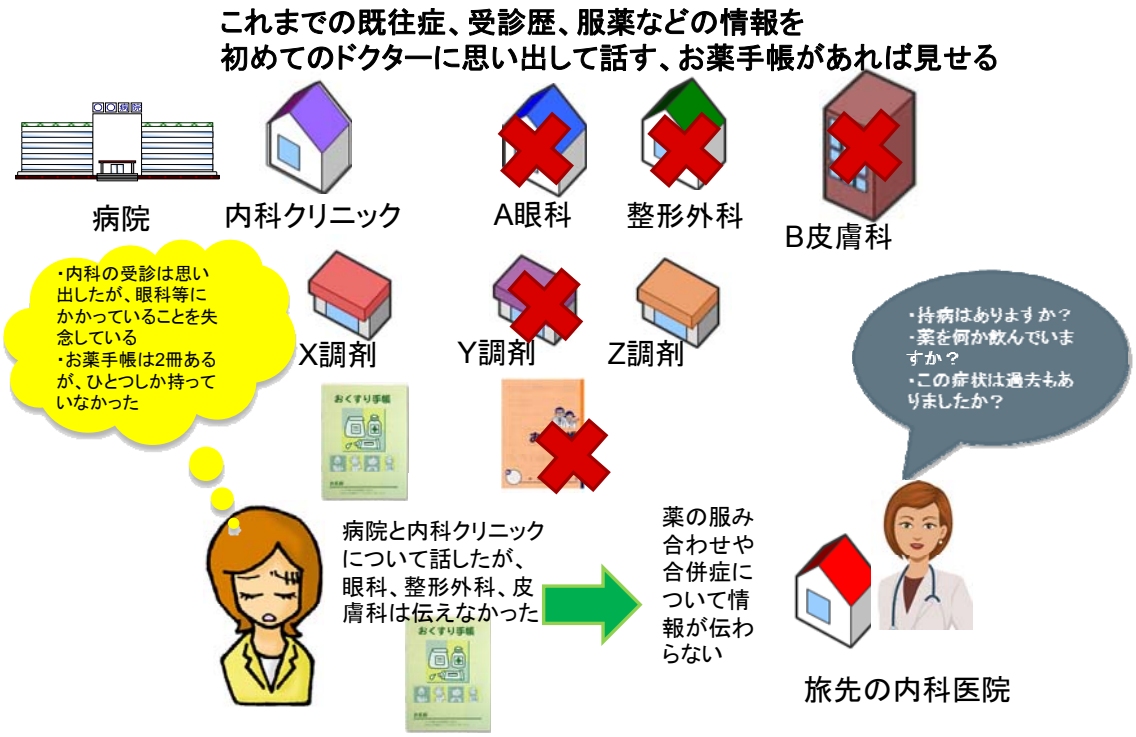

図5-3：旅行先で具合が悪くなった時　Before

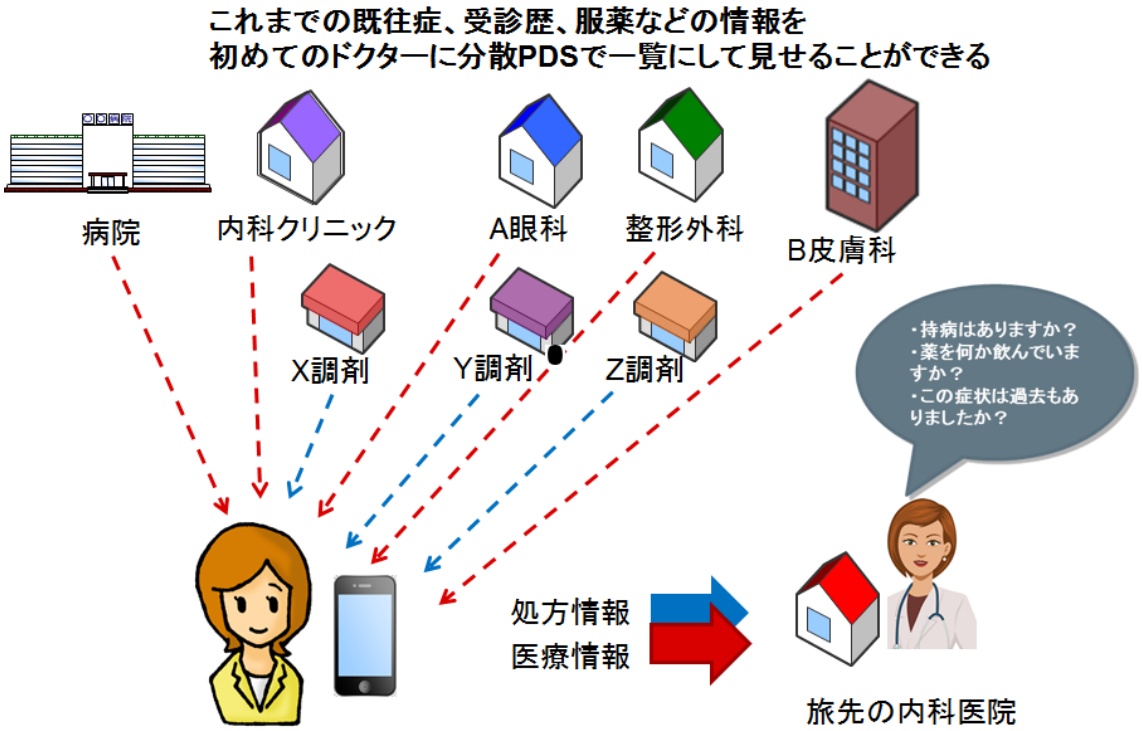

図5-4：旅行先で具合が悪くなった時　After

疾病管理手帳は、2015年7月に4つの臨床学会(日本糖尿病学会、日本高血圧学会、日本動脈硬化学会、日本腎臓学会)と日本医療情報学会のそれぞれの理事会で承認されているミニマム項目セット[日本医療情報学会, 2014]をベースとして作成する。生活習慣病をはじめとした多くの疾病で活用することができ、分散PDSの特徴である情報ポータビリティにより二次医療圏を超えた医療連携が可能となる。

5.2.2 透析患者サポート

透析治療を受けている患者が透析記録を診療所から受けている割合は10%にすぎない。人工透析(血液透析)は通常週3回行われており、旅行や急な出張あるいは冠婚葬祭の訪問先で透析施設や宿泊施設を探すのは困難である。

分散PDSが普及すれば個人が自らの透析情報をメディエータに開示することで、メディエータを通じて、受け入れ先施設や透析食を提供できる宿泊施設、交通機関の予約などを容易に行うことができるようになる

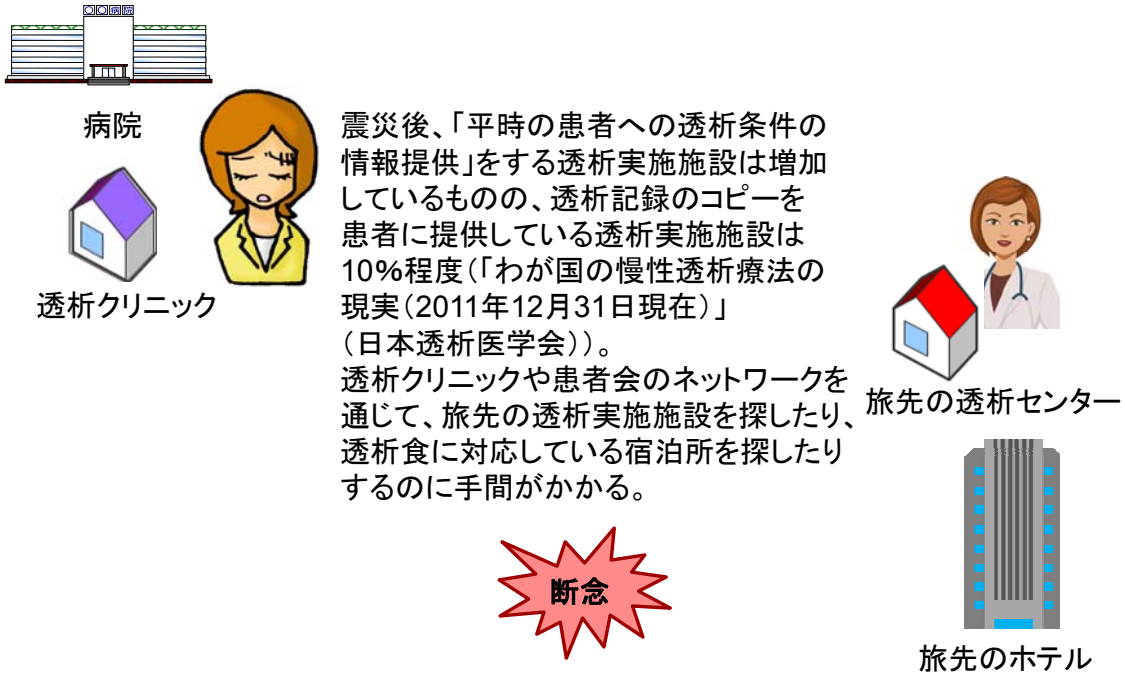

図5-5：持病がある(透析患者)が旅行したい場合　Before

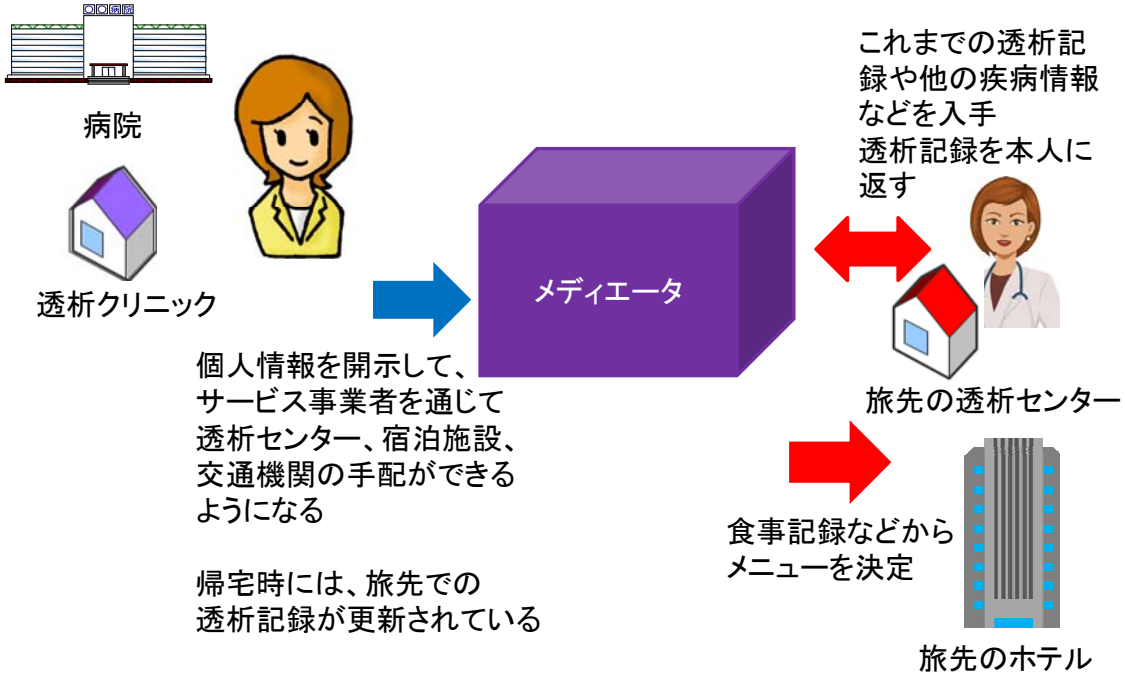

図5-6：持病がある(透析患者)が旅行したい場合　After

5.2.3 個人健診データ

我が国では人は生まれた時から母子保健法、学校保健安全法、労働安全衛生法、高齢者の医療の確保に関する法律などに基づき、生涯を通じて何らかの健康診断を受ける機会を

持っている。

しかしそれぞれの場面で健診データはあるものの、ほとんどは紙ベースのものであり、経年変化を見られるような仕組みにはなっていない。そのため転校、転職、退職などでは健診データは継承されていない。

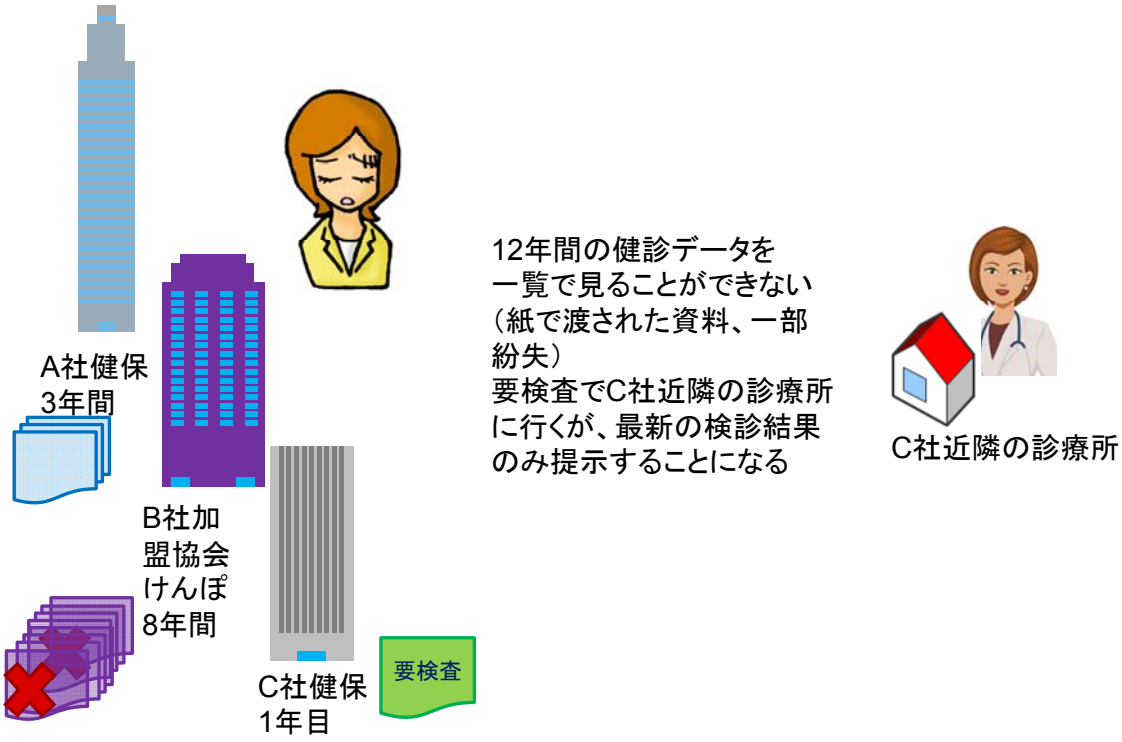

図5-7：3回目の転職先での健康診断　Before

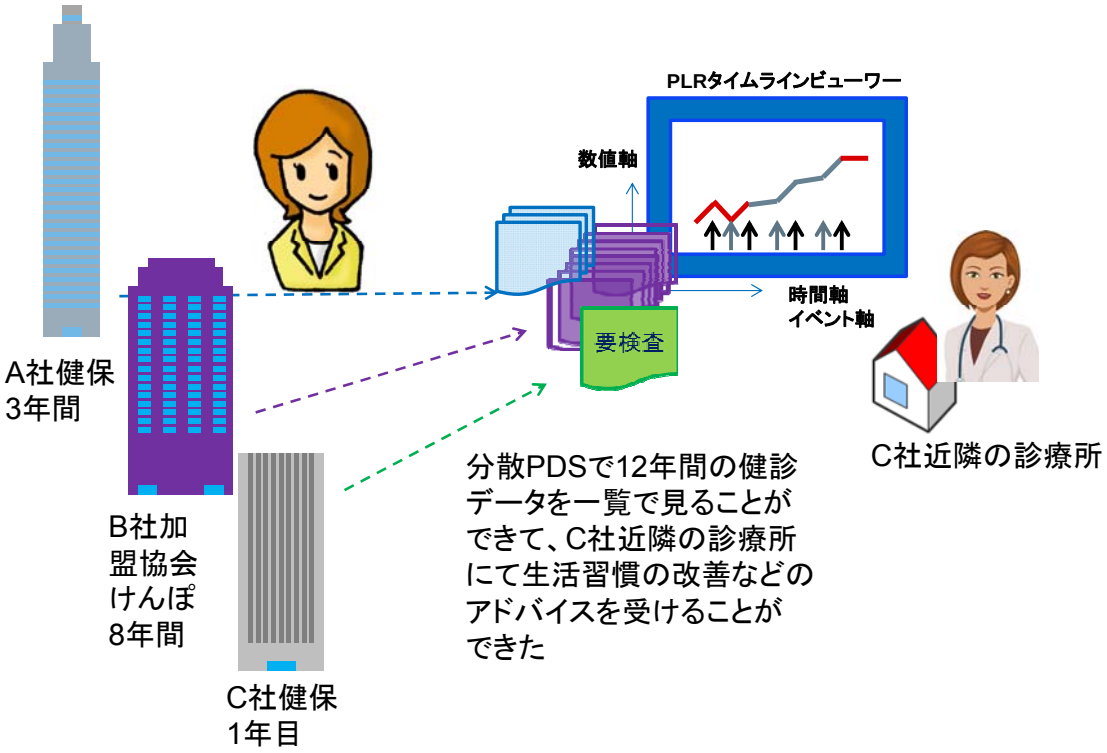

図5-8：3回目の転職先での健康診断　After

分散PDSがこれらの散乱している自己の健診データを管理できる仕組みを持つことで、例えば少年期からの健康に関する教育プログラム、青年期における体力増進などゲーミフィケーションを組み込んだプログラム、社会人向けの健診受診の有無や未病段階での生活改善とその成果に対するインセンティブ(生命保険料か健保組合保険料の逓減策)を与える施策などが考えられる。

5.2.4 患者会アプリ

病と闘うためには患者自身の努力だけでなく患者間あるいは専門医、専門職とのコミュニケーションも大きなサポートになる。

患者会を運営するにあたって会員の個人情報は、サークルや同窓会の名簿管理以上にセキュリティ面での注意が必要である。またインターネット上には様々な情報が氾濫しているため、どの情報がエビデンスのある情報であるか一般人では判断することができない。

分散PDSを使うことで、患者会事務局での安全な名簿管理、連絡や専門医、専門家を含んだ知識の共有などを行うことができる。また匿名性が維持された診療情報や患者のQOL情報を知ることができれば、医薬品開発や医療、看護、介護の改善策にも役立つ可能性がある。

自分の症状と同じ人はどのようなことで対応しているのだろうか知りたい、、、
匿名性を維持して、患者同士の話をしたい、、、
本当の情報について知りたい、、、
専門医や専門職のアドバイスを受けたい、、、
患者会があるようだが、敷居が高い、、、

専門医や
専門職

図5-9：同じ病気の患者同士のコミュニケーション　Before

病名、自分の症状などを開示することで、
なりすましでない患者同士のコミュニティ
に入ることができる(匿名も可能)
問診票や自分の医療データ、ライフログを
開示することで、専門医、専門職から自分に
合ったアドバイスを受けることができたり、
希少疾患研究者とつながることができる

専門医や
専門職

図5-10：同じ病気の患者同士のコミュニケーション　After

5.2.5 サービスフロー・収益モデルの仮説

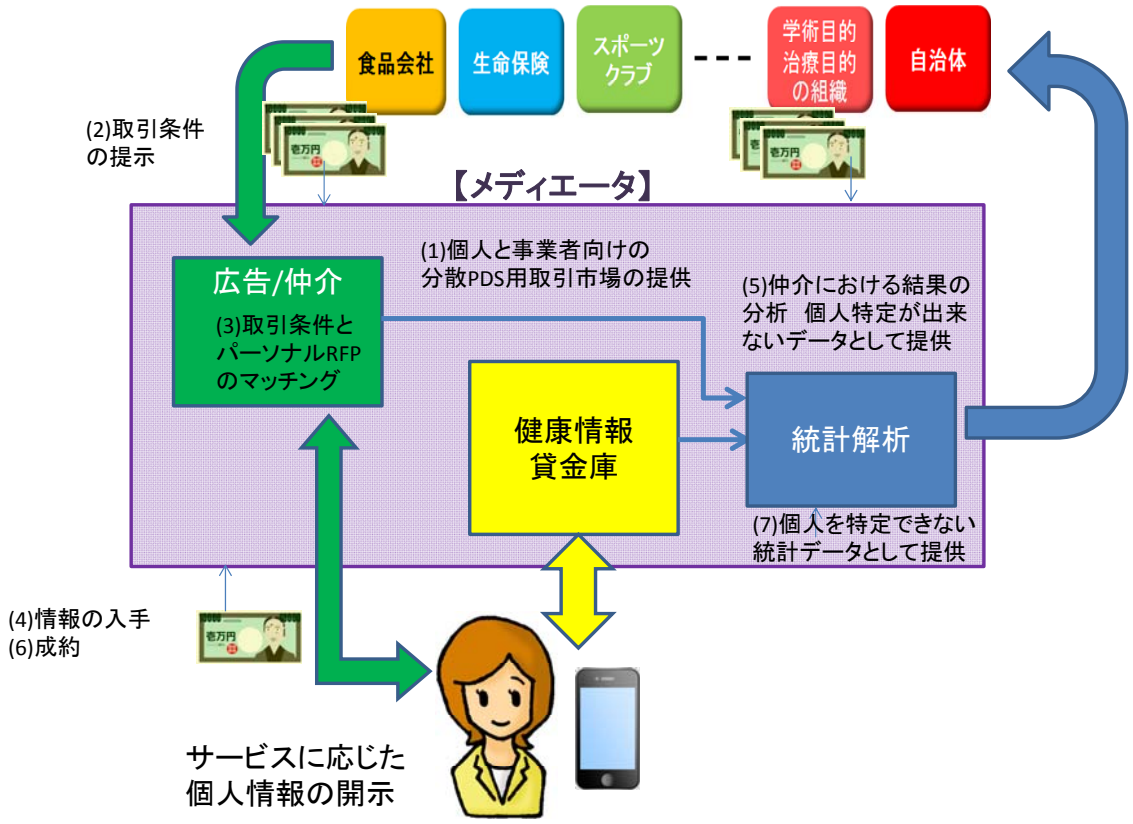

図5-11：健康情報を取り扱うメディエータのサービスフロー

メディエータと呼ばれる個人と多くのサービス提供事業者をマッチングする取引市場を開設すること(1)で、これまでサービス化が難しかった機微な健康情報に効率的、効果的にアクセス可能なサービスが誕生することになる。

また、このケースでは、メディエータは個人の受診履歴などの健康情報を暗号化して「貸金庫」で預かるということも想定している。

個人は、サービス内容によって開示する情報をコントロールでき、サービス事業者も取引条件を明示すること(2)で、アクセスにあたっては個人の機微情報を取り扱う必要がない。メディエータの仲介(3)によって、個人はサービス情報を入手でき(4)、サービス事業者との間で取引が成立(6)すれば、サービス事業者と個人はメディエータに仲介手数料を支払う。

メディエータは、仲介(3)で得られた成約過程を分析してこれをサービス事業者へ提供する(5)事業や個人から預かっている健康情報を個人の了承を得た上で、統計解析された情報としてサービス事業者へ提供する(7)事業を行う。いずれの事業においても、個人を特定できない形で提供される。(なお、(1)~(7)は3.6表3-1:メディエータの担いうる機能に対応)

このような機能を持つメディエータは、公益性の高い運営主体が想定され、ここで得ら

れた利益の一部は、地域医療・介護情報連携を運営、維持する原資となり得る。

　これまで述べてきたスマートライフの実現には、健診データ、医療情報、介護情報そしてバイタルデータなどの情報は、100年カルテ[吉原・荒木, 2015]やどこでもMY病院[医療情報化に関するタスクフォース, 2011]といった考え方が示されているように、一生涯を通じて集めることのできるライフログの仕組み(プラットフォーム)として設計する必要がある。

第6章　今後の検討事項

分散PDSの利活用を普及させていくために今後検討すべき事項を以下に挙げる。

6.1　システムの実現

分散PDSのシステムを構築する上で考慮すべき技術的な事項を以下に改めて列挙する。これらは標準化の対象を特定するための参考にもなるだろう。少なくとも、PDSの間でデータを共有するための方法(データ構造や暗号鍵の扱い)は標準化の必要があると思われるが、これは下記5つの事項のすべてに関係する。

6.1.1 汎用性: 多種のパーソナルデータを統合的に扱える

ある事業者等が個人から集めたデータを他の事業者等に提供(第三者提供)しようとすると、契約上の手続きが煩雑で、契約関係が不透明で、匿名化の規準が不明確であるなどの問題が生ずる。また、そもそも競合する事業者同士は通常は連携しない。分散PDSでは、すべてのパーソナルデータが個人を経由し、本人同意に基づいて流通するので、個人が設定した範囲であれば、事業者間で当該個人に係るデータを間接的に共有できる。様々な業界の事業者等が保有しているパーソナルデータを個人が管理できるようになれば、より多くの種類のパーソナルデータを統合して活用することが可能になる。

6.1.2 継続性: 個人の一生および複数の世代にわたり継続的に利用できる

パーソナルデータは、本人が一生利用できることが望ましい。ゲノムのデータ等は子々孫々にわたり利用できる必要があるだろう。ゆえに分散PDSは100年以上の継続性を確保する必要がある。その間にネットワークやデバイスは確実に進化するから、ハードウエア・ファームウエア改版の際に対応する手立てを考慮せねばならない。個々の分散PDSシステムをこの進化に対応させるのが困難ならば、分散PDSの間でのパーソナルデータのポータビリティを確保することが必須であろう。

6.1.3 互換性: 多くの事業者が参画できる

分散PDSを普及させるためには、様々な業界の事業者が分散PDSと連携し、利用者が享受できるサービスが豊富であることが求められる。多くの事業者を巻き込むためには、新しいサービスを提供しやすいオープンな環境が望ましく、様々なプラットフォームで分散PDSを運用できることが望ましい。

6.1.4 信頼確保: 個人(利用者)による自己情報コントロールが可能である

従来は、個人が本人のデータにアクセスできても、データそのものは事業者等の権限において集中的に管理・運用されており、本人の許可なくパーソナルデータが利用されてしまう可能性があった。個人の気付かぬところで本人のデータが使われるのではなく、個人の意思に基づいてデータが利用されるという自己情報コントロールの原則を満たすことが重要である。自己情報コントロールは、個人が他者に利用を許可したデータの実際の使わ

れ方に関する証跡を残して本人が視認できることなども含む。自己情報コントロールに基づいて、サービスや商品を個人の意思とデータに基づいて個人主導で選択すること、すなわちVRMが実現できる。

6.1.5 安全性: パーソナルデータの漏洩や不正な利用を防げる

個人が安心してデータをやりとりできるように、セキュリティを確保する必要がある。それにはまず、個人が本当に当該個人であり、事業者も同様に当該事業者であることの認証が必要である。次に、本人や他者が自分に都合の良いようにパーソナルデータを改竄する恐れがある場合には、その改竄を検知することによりデータの真正性を担保することも必要となる。また、悪意者からのアクセスを排除するためにサイバー攻撃への耐性を担保することも重要である。本人の過失等によるデータ漏洩を防ぐには暗号技術やその応用としてのDRMが有効だろう。暗号技術の発展に追従してセキュアな状態を確保し続けていくことも求められる。

6.2 ビジネスモデル

医療制度改革はヘルスケア関連事業者の間での分散PDSによる図3-5のようなパーソナルデータの共有を促すと考えられる。しかし、それを推進するためのビジネスモデルの構築は今後の課題である。

たとえば、ほとんどの介護事業者において介護記録は電子化されていないので、3章で述べたような分散PDSに基づく介護記録アプリを普及させる戦略は有望と思われる。保険請求事務は目的が明確なので多くの介護施設において電子化されているのに対して、介護記録があまり電子化されていないのはその目的が明確でないからだが、地域包括ケア等における多職種連携という目的が今後次第に明確化されることは期待できる。ところが、介護記録アプリは単価が低いので、代理店による拡販を図るには単価を上げて代理店の手数料を高める必要があるが、介護施設の負担を増すわけには行かないから、被介護者の家族に対するサービスを付加し、家族が支払うサービス利用料を介護施設や代理店に分配する必要があるだろう。そのサービスは分散PDSの特長を生かしたものでなくてはなるまい。地域包括ケアのための多職種間のデータ共有もそのようなサービスに含まれるだろうが、これに対しては、地域連携診療計画管理料等と同様の趣旨で保険を適用するのが望ましい。見守りやホームセキュリティや映像通話とその履歴データの利用権限を分散PDSによって他者に安全に付与できるというようなサービスも考えられる。

一方、診療所においても診療録の電子化はあまり進んでいないが、診療所用の電子カルテシステム(特に導入コスト)は介護記録アプリよりかなり高い。したがって、販売代理店の利益を確保できる範囲で価格を低く設定することにより、在宅医療等に対応するためにデータ共有が必須であることの理解の広がりに応じて、分散PDSに基づく診療所用電子カルテシステムを代理店経由で普及させることができると考えられる。病院に関しても、医療制度改革に対応するためにデータ共有が必須であることの理解が広がるにつれて、医療デ

ータの本人管理が普及するのではないだろうか。特に自治体や大学が運営する基幹病院がその流れを先導するものと期待される。ちなみに、既存の医療情報システムと分散PDSを連携させる開発作業の実費はシステムの種類ごとに100万円程度以下であり、EHRの導入等に比べてはるかに安価である。

一方、ヘルスケア以外の産業においては、パーソナルデータの共有を促すような法制度的な背景がない。たとえば購買のデータを社会的に流通させられれば、さまざまな財・サービスに関するニーズの情報が共有されることによって財やサービスの新規開発や改善が起こりやすくなるだろう。しかし、購買データを事業者の間で共有するのは困難な場合が多いので、消費者を経由して流通させるしかないだろう。ECサイト等におけるオンラインの購買についてはそのデータを消費者が電子的に取得可能だが、オフラインの購買のデータは紙のレシートで消費者に手渡される場合がほとんどであり、消費者が電子的に蓄積して活用することが難しい。

オフラインの購買データを消費者に電子的に渡すには、オーダエントリーシステムやPOSレジの導入拡大と機能拡張が必要であり、大きなコストがかかる。また、事業者は他の事業者の購買データは欲しいだろうが自分の購買データが他の事業者に流れるのは望まないだろうから、購買データを消費者に電子的に渡すための投資はなされにくいだろう。

しかし一般に、オンラインショッピングやモバイル端末やウェアラブルセンサの普及に伴って個人が電子的に扱えるデータの種類と量が増大し続けることは確実であり、そのデータを自ら蓄積して活用する個人が増えるだろう。事業者は個人からそのようなデータを取得してマーケティングに活用したいに違いない。それには、個人によるデータの蓄積・活用を拡大し、そのような個人との信頼関係を構築する必要がある。信頼関係を築くには、事業者は、個人からデータの提供を受ける際に明確な本人同意を得るだけでなく、自らが保有するデータを電子的に使いやすい形で個人に提供する必要があるだろう。分散PDSによる個人の自己情報コントロールを普及させるため、以上のような個人のエンパワメントのトレンドを加速するようなビジネスモデルの開発が求められる。また、これに関連する制度面での課題については6.3.4節で触れる。

6.3 制度的側面

6.3.1 運用ルールの策定と実効性の担保

分散PDSは、本人の同意に基づく新たなデータ流通の枠組みを構築するものであるがゆえに、顧客とサービス事業者、メディエータ等の関係性を規律する運用ルールの設計が、法制度への対応と同等以上に重要な作業となる。たとえばサービス事業者が取得したデータの消去に関わる時期や条件、事業者間でのデータ共有の制限、メディエータがサービス事業者に提供しうる情報の範囲等については、法による定めが存在しない論点も含め、分散PDSに参加する全ての主体に共有された運用ルールを策定する必要がある。ユースケースのさらなる具体化を進める中で、同意取得手続の標準化や、ルールの実効性を担保する

手段を備えたトラストフレームワークを構築することが、今後の最大の検討課題となる。

今般の個人情報保護法改正に向けた作業の中においても、分野ごとの特性を適切に反映した産業界の自主的なルール策定の重要性は繰り返し指摘されており、改正個人情報保護法の中でも、認定個人情報保護団体制度に関して、個人情報保護指針の策定に際して消費者の代表からの意見を聞き、個人情報保護委員会への届出を行うことが義務付けられる他、同委員会による指針の公表等の規定が整備されている。分散PDSは産業分野を横断した枠組みであるため、認定個人情報保護団体制度の直接的な活用が可能であるかは定かではないが、法令順守や運用ルールの実効性を保証する意味でも、それに準じた形で、個人情報保護委員会等の一定の関与を受けることを検討する余地がある。

6.3.2 同意取得のあり方と事業者間共有

個人情報保護法においては、個人情報の目的外利用や第三者提供を行うにあたり、原則として本人の同意を得ることが義務付けられている。特に改正個人情報保護法によって新たに規定される、人種、信条、社会的身分、病歴、犯罪被害を受けた事実、前科・前歴等を含む要配慮個人情報に関しては本人同意による取得が原則義務化され、さらに本人同意によらない第三者提供の特例(オプトアウト規定)から除外されるなど、パーソナルデータの利用に関わる同意取得のあり方は、今後さらに重要性を増していくものと考えられる。

分散PDSにおいては、事業者がパーソナルデータを利用する都度に本人の同意を得ることを前提としており、新たな事業者が当該データを利用するにあたっては、事業者間でのデータ共有を行わずとも、本人の同意を得た上で直接PDSからデータ取得を行うことが容易となる。このようなデータ利用形式の普及は、特に5.2でサービスモデルとして示した健康情報のような機微性の高いデータを多く含み得る分野において、本人の意思を正確に反映したデータ流通を拡大させることが期待される。

さらに本報告書で示したサービスモデルでは、分散PDSから取得されたデータは主として一つのサービス事業者の中で完結して利用されることを想定しているが、たとえばデータ取得時に明示した範囲での事業者間共有や、匿名化・統計化されたデータ、あるいは改正個人情報保護法により新設される匿名加工情報等の事業者間共有をどのような条件で規律するかなどは、運用ルールを策定する際の論点となるだろう。

6.3.3 顧客の認知限界の緩和

分散PDSにおいて顧客がデータ利用の同意を行うにあたっては、実質的には顧客自身の認知限界への対応が最大の焦点となると考えられる。サービス提供事業者からの同意要請が過度に頻繁であったり、利用目的や提供先の記述が複雑なものであった場合には、内容をよく理解せず同意を行うことが常態化し、本人の実質的な意思決定を尊重する分散PDSの本義を損なうことになりかねない。そのような事態を避けるために、分散PDSのフレームワークを策定する上では、ISO等における通知・同意手段の国際的な標準化や、情報共有標準ラベルの策定等の取り組みを参照しつつ、標準化された、理解しやすいインタフェー

スと手続を運用ルールによって規定することが求められる。

3.6節等で言及したメディエータは、顧客の意思決定を支援する上で主要な役割を担うことが求められる。特にメディエータの機能として主に想定されるサービス事業者と顧客のマッチングサービス等は、顧客の意思決定に関わる負担を軽減し、実質的な本人意思に基づくデータ流通を促進することが期待されよう。さらに将来的には、メディエータが顧客から情報の管理委託を受け、情報提供に関わる意思決定を一定の範囲で代行する役割を果たすなどの可能性をも考慮する必要がある。その場合には、メディエータと顧客の間での包括契約や利用目的変更への規律、メディエータに対する認定制度等を含めた制度設計の検討が必要になると考えられる。

6.3.4 顧客へのデータ還元に関わる制度枠組

分散PDSが普及するためには、個々の顧客が自らのパーソナルデータを利活用可能な形で保有していることが必要となる。特に改正個人情報保護法において開示の求めの請求権性が明確化されることなどを受け、顧客が自己のデータを手にする機会は今後徐々に拡大していくと考えられる。しかし紙媒体などの形式で開示されたデータを、顧客自身がPDSへの登録を行うことは容易ではない。立法課題として、機械判読可能な標準化された形式でのデータ還元を、何らかの形で制度化することを検討する余地が存在しよう。

国際的に高い関心を集める英国のmidataの取り組みは、現状において事業者の対応が法的に義務付けられているわけではないが、自主的な取り組みが十分でない場合には、2013年企業・規制改革法に基づき、特定の形式で顧客のデータを開示することを事業者に義務付ける可能性を示した上で関連の施策を進めている背景がある。同様の施策は、EU一般データ保護規則の制定に向けた作業の中でも「データポータビリティの権利」としての制度的導入が検討されており、データ対象者はデータ管理者から、「構造化された一般的に用いられる機械判読可能な形式」により自らのデータを受け取ると共に、当該データを他のデータ管理者に受け渡すことができる権利を有すると規定されている。

全てのパーソナルデータに関して、このような標準化されたデータ開示を義務付けることには慎重な検討を要するが、特に公的機関の保有するデータや、米国のグリーンボタン(エネルギー)やブルーボタン(ヘルスケア)の施策で対象とされるような、公共性の高い一定の分野に対して、PDSへの登録が容易な、標準化された形式でのデータ提供を求めることには検討の余地があるだろう。6.2で示唆したように、地域包括ケア等のためにヘルスケア事業者が個人やその家族に本人の医療データ等を提供することに対して公的保険を適用することも考えられる。分散PDSの枠組みは、このようなより幅広い、スマートディスクロージャー環境におけるデータ流通を牽引する役割を果たすことが期待される。

参考文献

青木 孝裕, 秋山 智宏, 飯山 裕, 伊藤 直之, 小熊 康之, 織田 朝美, 加藤 綾子, 木虎 直樹, 黒木 信彦, 佐古 和恵, 竹之内 隆夫, 中川 裕志, 橋田 浩一, 藤井 絵美子, 松山 錬, 宮田 智博, 安松 健 (2015) 個人情報を本人が管理するPDSシステムモデル —「集めないビッグデータコンソーシアム」における検討報告—. マルチメディア、分散、協調とモバイル(DICOMO2015)シンポジウム, 249-255.

Randy Baden, Adam Bender, Neil Spring, Bobby Bhattacharjee, and Daniel Starin (2009) Persona: an online social network with user-defined privacy. ACM SIGCOMM Computer Communication Review, Vol.39, pp.135-146.

Gordon Bell (2001) A Personal Digital Store. *Communications of the ACM*, 44: 86-91.

Ramon Cáceres, Landon Cox, Harold Lim, Amre Shakimov, and Alexander Varshavsky (2009) Virtual individual servers as privacy preserving proxies for mobile devices. Proceedings of the 1st ACM workshop on Networking, systems, and applications for mobile handhelds. ACM, pp.37-42.

Ann Cavoukian (2011) Privacy by Design The 7 Foundational Principles. https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

Ann Cavoukian and Reed Drummond (2013). Big Privacy:Bridging Big Data and the Personal Data Ecosystem Through Privacy by Design. https://www.ipc.on.ca/images/Resources/pbd-big_privacy.pdf

Ann Cavoukian, Alexander Dix, Khaled El Emam, Nuala O'Connor (2014) WEBINAR: Big Data Calls for Big Privacy - Not Only Big Promises. 参照日: 2015年4月30日, 参照先: PbD: https://www.privacybydesign.ca/index.php/webinar-big-data-calls-big-privacy-big-promises/

Yves-Alexandre de Montjoye, Erez Shmueli, Samuel S. Wang, and Alex Sandy Pentland (2014) openPDS: Protecting the Privacy of Metadata through SafeAnswers. *PROS ONE*, 9(7) e98790 doi:10.1371/journal.pone.0098790.

橋田 浩一 (2013) 分散PDSによるパーソナルデータの自己管理. 人工知能学会誌, 28(6) 872-878.

橋田 浩一 (2014) 分散PDSと集めないビッグデータ. 人工知能学会誌, 29(6) 614-621.

橋田 浩一, 和田 典子, 藤島 寿智, 上沼亜希子 (2015).自律分散協調ヘルスケアを目指して —PLRに基づく介護支援システムの開発—. 情報処理学会デジタルプラクティス, 6(1) 29-34.

Information Bank Consortium (2014) http://www.information-bank.net/index.html

IT総合戦略室 (2015) IT利活用促進に向けた取組について. http://www.kantei.go.jp/jp/singi/it2/senmon_bunka/number/dai9/siryou5.pdf

厚生労働省 (2013) シームレスな健康情報活用基盤実証事業(国庫債務負担行為に係るもの)平成24年度事業成果報告書. http://www.mhlw.go.jp/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/johokatsuyou/dl/houkokusho08.pdf

Min Mun, Shuai Hao, Nilesh Mishra, Katie Shilton, Jeff Burke, Deborah Estrin, Mark Hansen, and Ramesh Govindan (2010) Personal data vaults: a locus of control for personal data streams. *Proceedings of the 6th International Conference*. ACM.

中村 徹, 渡辺 龍, 清本 晋作, 高崎 晴夫, 三宅 優 (2015) プライバシーに配慮したパーソナルデータ連携実現に向けたプロトコルデザイン—OpenID Connect 設計におけるプラクティス—. 情報処理学会デジタルプラクティス, 6(1) 13-20.

OASIS (2014年12月) LinkContractPattern. OASIS XDI wiki: https://wiki.oasis-open.org/xdi/LinkContractPattern

佐古 和恵 (2015) パーソナルデータエコシステム構築に向けて—自己情報コントロール権の実現—. 情報処理, 55(12) 1361-1367.

佐藤 慶浩 (2015) データプライバシー対策をグローバル対応するための顧客情報管理データベースの設計と運用のプラクティス—連絡先情報をプロモーション連絡に利用する事例—. 情報処理学会デジタルプラクティス, 6(1) 5-12.

佐藤 慶浩, 高崎 晴夫, 中村 徹, 村田 潔, 折田明子, 佐古 和恵, 福島俊一 (2015) 座談会「プライバシーフレンドリーな社会に向けて」. 情報処理学会デジタルプラクティス, 6(1) 43-52.

Viktor Mayer-Schoenberger (2013) IAPP Data Protection Congress in Brussels Keynote: Responsible Use of Data. YouTube: https://www.youtube.com/watch?v=40fSCZaLv_A

Viktor Mayer-Schonberger and Kenneth Cukier (2013) Big Data: A Revolution That Will Transform How We Live, Work and Think. John Murray. (邦訳 斎藤英一郎 (2013) ビッグデータの正体: 情報の産業革命が世界のすべてを変える. 講談社.)

Doc Searls (2012) *The Intention Economy: When Customers Take Charge*. Harvard Business Review Press. (邦訳 栗原 潔 (2013) インテンション・エコノミー —顧客が支配する経済—. 翔泳社)

Seok-Won Seong, Jiwon Seo, Matthew Nasielski, Debangsu Sengupta, Sudheendra Hangal, Seng Keat Teh, Ruven Chu, Ben Dodson, and Monica S. Lam (2010) PrPl: A Decentralized Social Networking Infrastructure. *ACM Workshop on Mobile Cloud Computing and Services: Social Networks and Beyond.*

城田 真琴 (2015) パーソナルデータの衝撃. ダイヤモンド社.

東京大学 産学連携本部 (2014) 集めないビッグデータコンソーシアム. http://www.ducr.u-tokyo.ac.jp/jp/research/dbd-conso/index.html

Roy Want, Trevor Pering, Gunner Danneels, Muthu Kumar, Murali Sundar, and John Light

(2002) The personal server: Changing the way we think about ubiquitous computing. *Ubicomp 2002*, 223-230.

総務省 (2014) スマートプラチナ社会推進会議報告書.
http://www.soumu.go.jp/main_content/000303235.pdf

日本医療情報学会,日本糖尿病学会,日本高血圧学会,日本動脈硬化学会,日本腎臓学会(2014) 4疾病の「ミニマム項目セット」および「どこでもMY病院疾病記録セット」の策定.
http://jami.jp/medicalFields/create-set.pdf

吉原博幸, 荒木賢二 (2015) global EHR Project(100年カルテ)の構想とマイルストーン
http://www.seagaia.org/~sg2015/_src/sc243/150516yoshihara.pdf

医療情報化に関するタスクフォース (2011) 「どこでもＭＹ病院」構想の実現について(自己医療・健康情報活用サービス)
http://www.kantei.go.jp/jp/singi/it2/iryoujyouhou/pdf/siryou1.pdf

補足資料

① 活動記録

日時	名称	場所	内容
2014/10/15 15：00 ～17：20	キックオフ シンポジウム	東京大学大学院 情報学環学術研 究棟大和ハウス 石橋信夫記念ホ ール	【講演】 東京大学：坂井教授 東京大学：須藤教授 東京大学：柴崎教授 東京大学：橋田教授
2014/10/27 10：30 ～13：30	第一回全体会議	東京大学産学連 携プラザ 2AB会議室	【講演】 東京大学：橋田教授 東京大学：生貝特任講師 【特別講演】 東京大学：中川教授
2014/11/19 10：30 ～13：25	第二回全体会議	東京大学工学部 2号館31A会議 室	【議論】 東京大学：橋田教授、生貝特任講師
2014/12/11 15：00 ～18：30	第三回全体会議	東京大学工学部 2号館92B会議 室	【議論】 東京大学：宍戸教授、須藤教授
2015/1/19 13：00 ～16：10	第四回全体会議	東京大学工学部 2号館92B会議 室	【議論】 東京大学：中川教授、橋田教授
2015/2/18 13：00～ 15：10	第五回全体会議	東京大学工学部 2号館92B会議 室	【議論】 東京大学：橋田教授 WG1.2別検討
2015/3/11 13：00 ～16：10	第六回全体会議	東京大学工学部 2号館92B会議 室	【議論】 東京大学：原辰徳准教授 WG1.2別検討
2015/4/21 13：00 ～16：00	第七回全体会議	東京大学工学部 2号館92B会議 室	【議論】 井堀幹夫様 WG1.2別検討
2015/5/14 14：00 ～17：00	第八回全体会議	東京大学工学部 2号館92B会議 室	【議論】 東京大学：橋元教授 WG1.2別検討

2015/6/9 16：00 ～16：30	第九回全体会議	東京大学工学部 2号館111B2	【議論】 東京大学：橋田教授 WG1.2別検討
2015/7/14 13：30 ～14：40	第十回全体会議	東京大学産学連携プラザ 2AB会議室	【議論】 WG1.2別検討
2015/8/18 13：30 ～17：00	第十一回全体会議	東京大学産学連携プラザ 2AB会議室	【議論】 分散PDSの普及戦略
2015/9/4 13：00 ～22：00 9/5 7：00 ～12：00	集中討論会	八王子セミナーハウス	【議論】 報告書の執筆方針検討
2015/9/18 10:30～ 13:00	第十二回全体会議	東京大学工学部 2号館電気系会議室2	【議論】 報告内容に関する検討
2015/10/5	報告会		

WG1

日時	名称	場所	内容
2015/2/5 15：00 ～17：20	第1回WG1	東京大学産学連携プラザ 2AB会議室	【議論】 WG1で議論するテーマについて
2015/3/2 15：30 ～17：30	第2回WG1	東京大学産学連携プラザ 2AB会議室	【議論】 学会発表先について､橋田先生のPLRについての説明と質疑
2015/3/23 15：30 ～17：30	第3回WG1	東京大学　工学部2号館31A会議室	DICOMO 発表申し込み内容について、ユースケースについて、システムアーキテクチャについて
2015/4/13 15：30 ～17：30	第4回WG1	東京大学産学連携プラザ 2AB会議室	ユースケースについて、論文目次について

2015/4/21 10：30 ～12：00	第5回WG1	東京大学 工学部 2号館 3F 33B1	DICOMO発表論文執筆の割り当てについて、掲載ユースケースの絞り込み
2015/5/8 15：30 ～17：30	第6回WG1	東京大学 産学連携プラザ 2AB 会議室	【議論】 持ち寄った論文記述について
2015/6/9 10：00 ～12：00	第7回WG1	東京大学 産学連携プラザ 2AB 会議室	【議論】 DICOMO論文まとめ中に議論した課題の見直し、標準化要件の検討、進捗状況の確認
2015/7/2 14：00 ～16：00	第8回WG1	東京大学 産学連携プラザ 2AB 会議室	【議論】 DICOMOプレゼン資料について、電子母子手帳　柏市のヒアリング、提案システムアーキテクチャとPLRの対応について
2015/7/14 10：30 ～12：30	第9回WG1	東京大学 産学連携プラザ 2AB 会議室	【議論】 DICOMOプレゼンについての報告、PLRにおけるID管理とデータ共有方法について
2015/7/29 10：30 ～12：30	第10回WG1	東京大学工学部2号館 3階 電気系会議室 1C 33A	【議論】 成果のまとめ方について、今後明確にしたいことの持ち寄り
2015/8/17 15：00 ～17：00	第11回WG1	東京大学 産学連携プラザ 2AB 会議室	【議論】 名簿管理アプリとPLRにおける安全なデータ共有方法について、標準化へのアプローチについて、分散PDSの標準化を考えるにあたって、検討すべき要件の整理
2015/8/28 15：00 ～17：00	第12回WG1	東京大学 産学連携プラザ 2AB 会議室	【議論】 報告書執筆項目と分担について

WG2

日時	名称	場所	内容
2015/2/23 10：00 ～12：20	第1回WG2	東京大学産学連携プラザ201会議室	【議論】 今後の進め方の認識合わせ
2015/3/3 13：00 ～15：00	第2回WG2	東京大学産学連携プラザ206会議室	【議論】 各社モデルケース案の共有と見える化
2015/3/23 13：00 ～15：00	第3回WG2	東京大学産学連携プラザ2AB会議室	【議論】 スマートタウン・スマートライフのモデルケースの見える化
2015/4/13 13：00 ～15：00	第4回WG2	東京大学産学連携プラザ2AB会議室	【議論】 メディエータの役割・機能の説明および議論
2015/5/8 13：00 ～16：10	第5回WG2	東京大学産学連携プラザ2AB会議室	【議論】 メディエータの役割、管理するラベル、情報のレベルについて
2015/5/26 13：00 ～15：00	第6回WG2	東京大学産学連携プラザ2AB会議室	【議論】 メディエータの役割について
2015/6/19 13：00 ～14：30	第7回WG2	東京大学産学連携プラザ2AB会議室	【議論】 インテージ様スマートライフの説明、WG2のまとめに向けて
2015/6/29 10：00 ～11：40	第8回WG2	東京大学産学連携プラザ2AB会議室	【議論】 報告書の章立てについて
2015/7/7 16：00 ～17：50	第9回WG2	東京大学産学連携プラザ2AB会議室	【議論】 提案書のイメージ､広報戦略について
2015/7/23 15：00 ～17：00	第10回WG2	東京大学産学連携プラザ2AB会議室	【議論】 WG2議論のまとめについて、コンソーシアム期間内のスコープについて
2015/9/7 14：00 ～15：20	第11回WG2	ワールドインポートマートビル8階	【議論】 報告書のまとめについて､報告会プレゼン資料について

② メンバー

Ⅰ：大学側メンバー	
東京大学　大学院情報理工学系研究科 ソーシャルICT研究センター	教授　橋田浩一
東京大学　大学院情報学環	教授　須藤修
東京大学　空間情報科学研究センター	教授　柴崎亮介
東京大学　先端科学技術研究センター	教授　森川博之
東京大学　情報基盤センター	教授　中川裕志
東京大学　総合教育センター	中山隆弘
東京大学　大学院工学系研究科	特任准教授　美馬秀樹
東京大学　大学院情報学環	教授　橋元良明
東京大学　大学院法学政治学研究科	教授　宍戸常寿
東京大学　大学院情報学環	特任講師　生貝直人
文教大学　情報学部	専任講師　加藤綾子
東京大学 大学院情報理工学系研究科 ソーシャルICT研究センター	特任研究員 森田瑞樹
Ⅱ：法人メンバー	
日本電気株式会社	若目田光生、佐古和恵、森拓也、 竹之内隆夫
日本アイビーエム株式会社	黒木信彦、青木孝裕、宮田智博、篠 崎朋子
アンリツ株式会社	小熊康之、秋山智宏、安嶌裕之、 吉田諒
シナジーマーケティング株式会社	織田朝美、木虎直樹、藤井絵美子、 安松健
大日本印刷株式会社	井上貴雄、勝島史恵、岡本高明、 土屋秀男、栃原聖一、松山錬、 今井哲之
株式会社インテージホールディングス	橋本勝、栗原勝、小森谷祥明、 伊藤直之
アセンブローグ株式会社	青井正三、片野毅
Ⅲ：特別メンバー	
一般財団法人日本情報経済社会推進協会	坂下哲也、保木野昌稔、金子剛哲
地方公共団体情報システム機構	井堀幹夫
名古屋大学	服部亮

中日本高速道路株式会社	高橋秀喜、東晋一郎、小林寛
株式会社ゼンショーホールディングス	高塩仁愛
株式会社ルネサンス	高崎尚樹
埼玉県立総合教育センター	大沼潤一
社会福祉法人恵信福祉会	和田典子
川崎市役所	奥貫賢太郎
株式会社ジェイアール東日本スポーツ	高藤慎介
Ⅳ：事務局	
東京大学産学連携本部	飯山裕、筧一彦
Ⅴ：ご講演	
名古屋大学	教授　岩尾聡士