資料１

EUの状況：
データポータビリティの権利を中心に

2016年11月11日　生貝直人
東京大学大学院情報学環客員准教授
科学技術振興機構さきがけ研究員（ビッグデータ基盤領域）

EU一般データ保護規則
（General Data Protection Regulation, GDPR）

- 2012年に欧州委員会から当初案が公表されてから4年を経て2016年4月に採択、2018年5月から施行。1995年データ保護指令を置き換え、EUのデータ保護法制を一本化。
- EU市民を標的としたサービスを提供する域外企業にも適用されることを明確化、全世界年間売上高の4%または2,000万ユーロのいずれか高い方等を上限とした高額な制裁金を導入。
- 全体としてデータ保護指令の内容を踏襲しているが、データ保護責任者の設置やデータ保護影響評価の実施等に関わる新たな規律が導入される。

- →中でもPDS・情報銀行に関わりが深いと考えられるのが、データ主体の権利として新しく導入された「データポータビリティの権利（The Right to Data Portability）」。

GDPR20条：データポータビリティの権利
（The Right to Data Portability）

1. データ主体は、以下の場合には、彼または彼女が管理者に提供した、彼または彼女に関わる個人データを、構造化された、一般的に用いられる機械可読なフォーマット（structured, commonly used, machine-readable format）で受け取る権利を有すると共に、それらのデータを妨害されることなく、当該個人データが提供された管理者から、他の管理者に移転する権利を有する。
   (a)第6条第1項(a)もしくは第9条第2項(a)に従った同意、あるいは第6条第1項(b)に従った契約に基づき、当該処理が行われており、かつ、
   (b)当該処理が自動的な方法によって実行されている場合。
2. 第1項に従って彼または彼女がデータポータビリティの権利を行使するにあたり、技術的に可能な場合には、データ主体は当該個人データをある管理者から別の管理者に、直接的に移転する権利を有する。
3. 本条第1項に規定される権利の行使は、第17条（※訳注：消去される権利（忘れられる権利））に影響を与えない。同権利は、公共の利益や、当該管理者に委ねられた公的権限の行使に関わる任務の遂行に不可欠な処理には、適用されないものとする。
4. 第1項に規定される権利は、他者の権利や自由に対して不利な影響を与えてはならない。

- ①データ管理者から本人が自らのデータを扱いやすい電子的な形式で取り戻し、それを他のデータ管理者に移転する権利と、②あるデータ管理者から別のデータ管理者に直接移転する権利の2つの権利から構成される。
- ただし、技術的に互換性のあるデータ処理システムの導入や維持までをも義務付けているわけではない（前文68）。

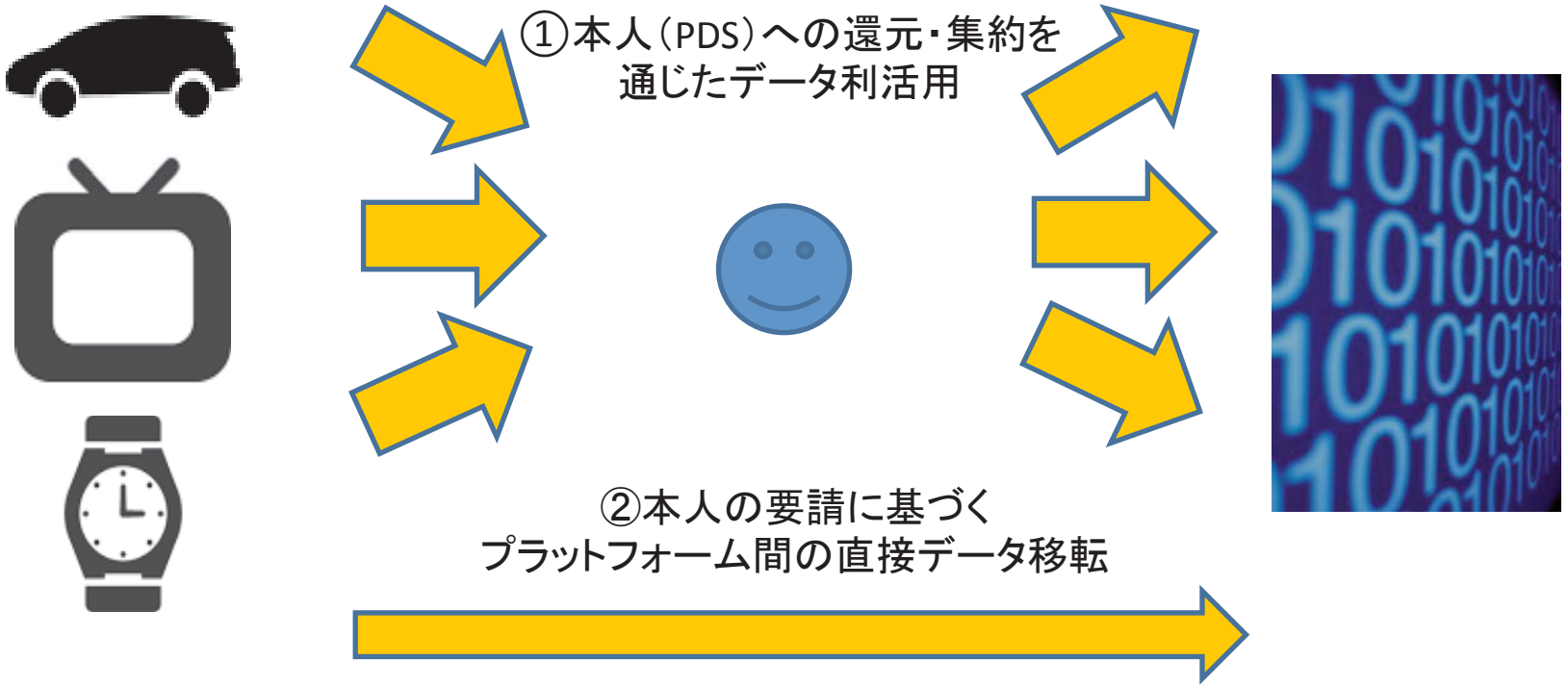
欧州委員会によるデータポータビリティ権の解説（2015/12）

- **個人はより多くのコントロールを手にする。それはいかにしてビジネスを支援するか？：** 新しいデータポータビリティの権利は、個人が自らの個人データを、あるサービスプロバイダーから別のサービスプロバイダーに移動させることを可能とする。スタートアップや小規模企業たちは、デジタルジャイアンツに支配されたデータ市場にアクセスし、プライバシー親和的なソリューションによってより多くの消費者を惹きつけることができるようになる。
  - **例：個人にとっての利益、ビジネスにとっての利益**：ある新しい小規模企業が、ウェブサイトをシェアするオンラインソーシャルメディアを提供する市場への参入を望むとする。現在のルールの下では、個々の新しい消費者は、彼らがそこに参加するために提供したいと望む個人データを、新しいウェブサイト上においてもう一度はじめから入力し直さなければならない。それは人々が新しいビジネスにスイッチする上での障壁となりえる。
- **データ保護の改革によって**：データポータビリティの権利は、潜在的な消費者が、サービスプロバイダー間で彼らの個人データを移転することを容易にする。それは自らのパーソナルデータに対するコントロールを消費者が行使可能となることを促すと同時に、競争と市場における新しいビジネス活動の推進を促すことになる。

European Commission - Fact Sheet
Questions and Answers - Data protection reform (2015/12)より

GDPR20条におけるデータポータビリティの権利

- 企業サイドの困難：人々のパーソナルデータは様々な事業者やデータベースに散逸しており統合的な利活用ができず、一部のプラットフォーム企業へのデータ集中が進む。
- 個人サイドの困難：個々人のデータはさまざまなプラットフォームに囲い込まれており、プラットフォームを移行する際には多くの過去データを諦めなければならない。
- こうした状況を改善し、個人による自己データ利用機会を拡大することで、個人データの利活用と保護を両立しようとするのが、データポータビリティの権利。



2012年欧州委員会当初提案時の条文

2012年に欧州委員会から公表されたGDPR当初案と最終可決版の主な変更点：

1. 適用対象データとして、当初案には存在しなかった「彼または彼女が管理者に提供した」という限定が最終可決版には明記。
2. 当初案には存在しなかった「技術的に可能な場合」の「直接的な移転」という規定が追加。
3. フォーマットや技術標準を欧州委員会が特定可能であるという規定を削除。
4. 他者の権利との調整が明記。

2012年1月GDPR欧州委員会当初提案（当初案条文番号は18条）

1. データ主体は、電子的手段により、構造化された一般的に用いられるフォーマットで個人データが処理される場合、処理されているデータの複製を、一般的に用いられ、データ主体がその後も利用できる、電子的で体系化されたフォーマットで、管理者から取得する権利を有する。
2. データ主体が個人データを提供し、かつその処理が同意あるいは契約に基づいている場合、データ主体が提供し自動的処理システムに保持されている個人データおよびその他の情報を、個人データを取り下げたデータ管理者の妨害を受けることなく、一般的に用いられる電子的フォーマットで、他の自動的処理システムに移転する権利を有する。
3. 欧州委員会は、第1項に規定する電子的なフォーマット、および第2項に従って行われる個人データ移転のための技術標準、様式および手続を特定することができる。それに関する実施法令は、第87条第2項に規定する審査手続に従って採択されるものとする。

立法過程での主な議論

【肯定的見解】

●EU市民：6割以上が自らの個人データへのコントロール能力不足を感じており、特にクラウドサービス等におけるポータビリティの必要性を認識（ユーロバロメーター）。
●欧州データ保護監察官（EDPS）：同意・契約に基づくデータのみを適用対象とすべきかという問題がある。データ主体が提供したデータだけではなく、より広い適用範囲を持つようにするべきではないか。
●ドイツBfDI（連邦データ保護当局）：一般的に用いられるフォーマットで個人データが処理されている場合という表現については、その形式で管理者がデータ処理を行っている場合に同権利の適用が限定されるように解されるべきではなく、データ処理一般に適用される必要があるのではないか。

【否定的見解】

●ebay：ebayでの他ユーザーへの評価コメントや、paypalでの取引履歴など、第三者のプライバシーに関わるデータを含んでしまうリスクがある。人的資源管理システムや顧客管理システムに登録された情報は企業にとって大きな商業的価値を持つため、これらをも全体的に対象にすることは競争上の問題を惹起する。
●ニュージャージー工科大学ピーター・スワイア教授：広範なデータポータビリティの導入は、競争政策と矛盾すると共に、スタートアップを含む中小企業に過度な負担を押し付け、消費者利益をも低下させることになりかねない。

欧州の議論状況につき、佐々木勉「欧州におけるデータ・ポータビリティの在り方を巡る議論の動向」、総務省AIネットワーク化検討会議提出資料（2016年4月）も参照。

GDPRにおけるデータポータビリティの権利の具体化に関わる主な論点

- 対象となる「彼または彼女が管理者に提供した」データとはどのようなデータを指すか？
  - データ主体が直接入力した個人データが含まれることは間違いないが、IoTデバイスから生成されたセンサーデータ等はどこまで対象に含まれうるか？
- 「一般的に用いられる機械可読なフォーマット」とはどのようなフォーマットを指すか？
  - 行動規範（GDPR40条）の活用等が指摘される
- ポータビリティにかかるコストを誰が負担するか？

EUにおける今後の具体化プロセスと主要プレイヤー

- データポータビリティ権の具体化に関わる主なプレイヤーとしては、①各国データ保護当局により構成される29条作業部会の運用ガイダンス策定、②加盟国政府の国内的対応、③欧州委員会による実施法令等の策定、④各種業界団体の行動規範策定（GDPR施行後は欧州委の認定を取得可能）、⑤EU・各国裁判所の法解釈等がある。
- この他2016年末には、EUデジタル単一市場政策の一環として、⑥データ流通促進のための「技術標準、オンラインプラットフォームやクラウドコンピューティングサービス間のスイッチング・ポータビリティ促進」を含む「データの自由な流通（Free Flow of Data）イニシアティブ」を公表予定。

29条作業部会におけるガイダンス策定

- 29条作業部会は2016年2月、GDPR施行に向けた2016年の行動計画を公表し、2016年末までに「データポータビリティの権利」「データ保護影響評価」「認証」「データ保護責任者」についてのガイダンス策定を行うとする。
- さらに2018年に向け、部会内に「プライバシーの未来」「重要条項」「技術」「国際移転」「国境・移動・法執行」「電子政府」「金融問題」「協働」という9つのサブワーキンググループ（SWG）を設置。特に技術SWGは、データポータビリティの基盤となるデータ標準化の他、IoTを含む各種情報技術へのGDPR適用を主導すると考えられる。
  - 技術SWGの主要検討テーマ：追跡拒否（Do Not Track）、データポータビリティ、Wi-Fi位置情報やブルートゥースビーコン、最低限の技術的基準、電子投票、雇用者の電子的監視、スマートデバイスの適切な情報提供・同意取得方法、電子通信プライバシー指令、スマートメーター・グリッド等

29条作業部会：データ保護指令29条に規定される、EUデータ保護法制の統一的運用の担保と、EUおよび各国のデータ保護政策に対する独立の助言を行う機関。各国のデータ保護当局と、EU機関のデータ保護を担当する欧州データ保護監察官等から構成。GDPRの施行に伴い、欧州データ保護会議に改組・機能強化予定。
GDPRによりEU全体のデータ保護が一本化された後も、運用は原則として各国データ保護当局が行うため、GDPRの各種規定具体化に強い影響力を有する。

個人データ流通促進に対する EUのアプローチ

- 個人データ保護を人権として捉え（欧州連合基本権憲章8条）、データ保護指令・GDPRによる強固なデータ保護法制を前提とする。
- 各種取引データを機械可読な形で本人に還元し利活用を行う英midataや仏MesInfos等は、そうした制度的環境の中で、本人の意思に基づく形でのデータ流通を進める施策と位置付けられる。
  - 近年のPDSやMyDataに対する関心の高まりも、GDPRの各種規定（データ主体の権利、管理者の義務）に対するコンプライアンス手段としての側面が大きい。
- データポータビリティの権利は、それら本人中心型データ流通促進策を制度的に後押しする役割を有する。

いくつかの英国の組織は、個人の消費や取引に関わるデータを、本人がポータブルかつ安全な形で確認・アクセス・利用することを可能とするmidataや類似する施策を通じて、すでにデータポータビリティを提供している。それは消費者がより良い取引を発見したり、自身の支出行動に対する理解の補助となるようなアプリケーションやサービスを活用するためにデータを活用することを支援している。

英情報コミッショナー庁によるGDPRデータポータビリティ権の解説（2016）より

各国の関連状況

■ 英国midataに関する立法

midataの取り組みは現状で法的強制力は存在していないが、2013年規制・企業改革法では、政府が「エネルギー、モバイル、金融、小売」の4分野につき、消費者の求めに応じて特定の形式で取引データを提供する義務を課す権限を設けている（未施行）。産業界の自主的な施策が十分でない場合には、同法を実際に施行する可能性を示すことで、midataの取り組みを後押ししている。

■ フランス・デジタル共和国法案

英国midataと類似したMesInfosの取り組みが進められるほか、2016年10月に採択されたデジタル共和国法では、「データのポータビリティと回収（Portabilité et récupération des données）」として、消費法典（code de la consommation）を改正する形で、一定規模以上のオンラインサービスプロバイダーを対象とした法制が導入される。対象データに「利用者がアップロードしたすべてのファイル」が含まれるなど、個人データに限られないより幅広い規定として位置付けられる。

■ 米国Green Buttonの制度的背景

2007年のエネルギー自立・安全保障法において、電力購入者が、各過程に設置されるスマートグリッド情報（時間ごとのホールセール・小売価格、使用量、電力発生源等）に、①書面か電子的・機械可読な形式で直接アクセス可能とすること、②アプリケーション利用のためにインターネット等からいつでも自らの情報にアクセス可能とすることを求めている。

■ ニュージーランド

EUでのGDPR可決を受け、2016年、プライバシー・コミッショナーが同国民にデータポータビリティ制度導入必要性についてアンケート調査を実施。回答者の56%がオンラインサービス間での個人データ移転を「きわめて重要」「重要」と回答。GDPR施行に向けた動向を注視しつつ、近く予定される同国個人情報保護法改正において、データポータビリティ権を導入すべきかの議論を始めるべきとする。

参考：わが国におけるデータポータビリティ制度導入の選択肢（COCN提言より）

- ①EUデータ保護規則案のような、個人情報保護法の改正等による、個人データ全般のポータビリティ
  - 例外要件などは緻密に検討する必要
  - グローバル・プラットフォームへの対応を行うための「実効的な」域外適用強化の可否
- ②英国midataや米国Green Buttonのような、代替性の低い重要データを保有する特定分野への適用
- ③補助金や税制等を通じたインセンティブ型導入

産業競争力懇談会（COCN）「IoT時代のプライバシーとイノベーションの両立」2015年度報告書 p.79-80

参考：GDPR17条
消去の権利（忘れられる権利）

1. データ主体は、当該データ主体に関わる個人データについて管理者に不当な遅滞なく消去させる権利を持つものとする。管理者は、次に掲げる根拠のいずれかが適用される場合、個人データを不当な遅滞なく消去する義務を負うものとする。
   - (a) 個人データが収集された、又はその他の処理目的に照らして、当該個人データがもはや必要ない場合。
   - (b) データ主体が、第 6 条第 1 項(a)又は第9条第2項(a)による処理の同意を撤回し、かつ当該処理に関して他の法的根拠がない場合。
   - (c) データ主体が、第21条第1項により不服を申立て、かつ処理に関して優先する法的根拠がない場合。又はデータ主体が第21条第2項により不服を申し立てる場合。
   - (d) 個人データが不法に処理された場合。
   - (e) 個人データが、管理者が従うべき EU 法又は加盟国の国内法における法的義務の遵守のために消去されなければならない場合。
2. 管理者が個人データを公開しており、第1項による個人データを消去する義務を負う場合、その管理者は、利用可能な技術及び実施の費用を考慮した上で、当該個人データを処理している管理者たちにデータ主体が当該個人データのあらゆるリンク又はコピー若しくは複製の消去を要求している旨を通知するために、技術的措置を含む合理的手段をとらなければならない。
3. 第 1 項及び第 2 項は、取扱いが次に掲げるいずれかに必要な場合、適用されない。
   - （※省略：表現の自由、法的義務・公的任務、公衆衛生、研究等）

プロファイリングとPDS・情報銀行

- 高度な人工知能・アルゴリズムを利用したパーソナルデータの解析による「プロファイリング」は多大なポテンシャルを有する。
  - マーケティング、与信評価、保険料率の決定、採用活動、人事評価、潜在的な犯罪者の特定、、、
- 特にPDSに蓄積されたパーソナルデータ（ディープデータ）に基づく精度の高いプロファイリングは事業者のみならず個人にも好機をもたらし、PDSや情報銀行の主要機能となることも期待できるが、一定のルールを考慮する必要はないか？
  - どのようなルールが、プロファイリングの価値とリスクをバランスできるか？

GDPRのプロファイリング関連規定

- プロファイリングの定義
  - 「`プロファイリング`とは、特に自然人の業務実績、経済的状況、健康、個人的嗜好、関心、信頼性、行動、位置あるいは移動を分析あるいは予測するような、自然人に関する一定の個人的側面を評価するための個人データの利用から構成される、あらゆるデータ処理の形態を意味する。（第4条(4)）」
  - プロファイリングがデータ処理に含まれることを明示（前文72）
- プロファイリングに異議を申し立てる権利
  - データ主体は一定の根拠に基づくプロファイリングに異議を申し立てることができる（第21条）
- 適切なプロファイリングに求められる要件
  - 使用される論理（logic）、データ主体にとっての意義と予測される帰結についての意味のある情報へのアクセス（前文63）
  - 適切な数学的・統計的処理を用いること、不正確さの訂正や誤りのリスクを最小化するための技術的・組織的措置の実施、個人の利益や権利へのリスクに比例した安全措置と差別的影響の抑止（前文71）

22条：プロファイリングを含む自動的な個人に関する意思決定
（Automated individual decision-making, including profiling）

- １．データ主体は、プロファイリングを含む自動的処理のみに基づいて行われた、彼または彼女に法的な影響をもたらす、あるいはそれと類似する重要な影響をもたらす決定に服さない権利を有する。
- ２．第1項の規定は、以下で挙げる決定には適用しない。
  - (a)データ主体とデータ管理者の間で契約を締結する、あるいは契約を実施するために必要な決定。
  - (b)データ主体の権利や自由、合法的利益に対する十分な保護が担保された、当該データ管理者に適用される、欧州連合あるいは加盟国の法によって認められている場合。あるいは、
  - (c)データ主体の明確な同意に基づいている場合。
- ３．第2項(a)および(c)に言及される場合においては、データ管理者は最低限、管理者の側での人的介入を得たり、彼や彼女の見解を述べたり、決定に異議を唱えたりする権利を含む、データ主体の権利や自由、合法的利益を保護する適切な措置を実施しなければならない。
- ４．第2項で規定される決定は、第9条第2項(a)か(g)（※データ主体の明確な同意か実質的な公共の利益）に該当すると共に、データ主体の権利や自由、合法的利益を保護するための適切な措置が整えられていない限りは、第9条第1項で規定する特別な種類の個人データに基づいてはならない。

22条に関連する規定

- データ主体が情報を得る権利
  - 「第22条(1)および(4)が規定するプロファイリングを含む自動的な個人に関する意思決定の存在、少なくともそのような場合には、使用される論理についての意味のある情報、ならびにその処理のデータ主体にとっての意義および予測される帰結。」（第13条第2項(f)、第14条第2項(g)、第15条第1項(h)）
- データ保護影響評価の実施
  - 大規模な機微情報処理の他、プロファイリングを含む自動的な意思決定を行う場合には特に実施が求められると明記（第35条第3項）

プロファイリングに関わる論点

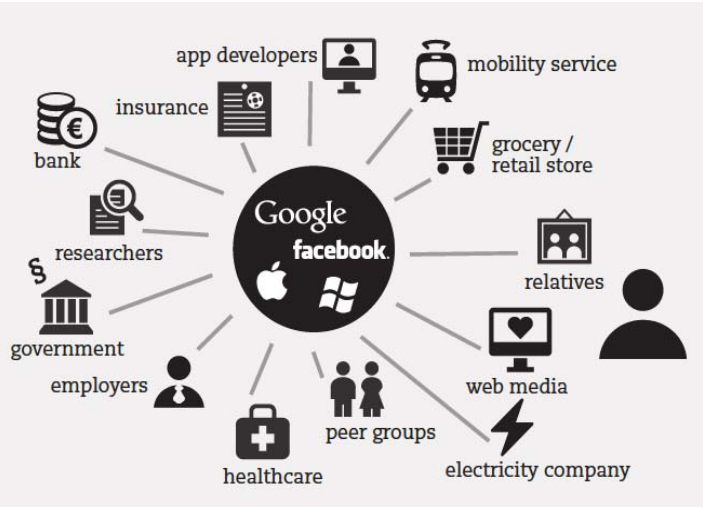
- 「法的な影響をもたらす、あるいはそれと類似する重要な影響をもたらす決定」とは、いかなる決定か？
  - GDPRでは「いかなる人的介在も経ない、オンラインのクレジット申請の自動的な拒否や電子的採用活動」を例示（前文71）
- 「使用される論理についての意味のある情報、ならびにその処理のデータ主体にとっての意義および予測される帰結」とはどのような情報を指すか？
- 「管理者の側での人的介入」とは、どの程度の人的介入であれば十分か？

- →欧州データ保護会議（29条データ保護作業部会から改組）がガイダンスを策定（前文72）

「集中型」「分散型」データ流通エコシステムの相互関係

- データポータビリティ権は、事実上本人が関与しえない集中型パーソナルデータ流通エコシステムと対置されるべき、本人主導型の新たな「分散型」エコシステムを生み出しうる。
- しかし、技術的・ビジネス的な限界、さらには消費者の認知限界（自らデータを管理することの限界）などの要素により、本人主導型エコシステムにも限界がある。分野やデータの性質、消費者の選好などにより、二つのエコシステムは並存・競争・協調すると考えるべきである。

現在の集中型データ流通エコシステム



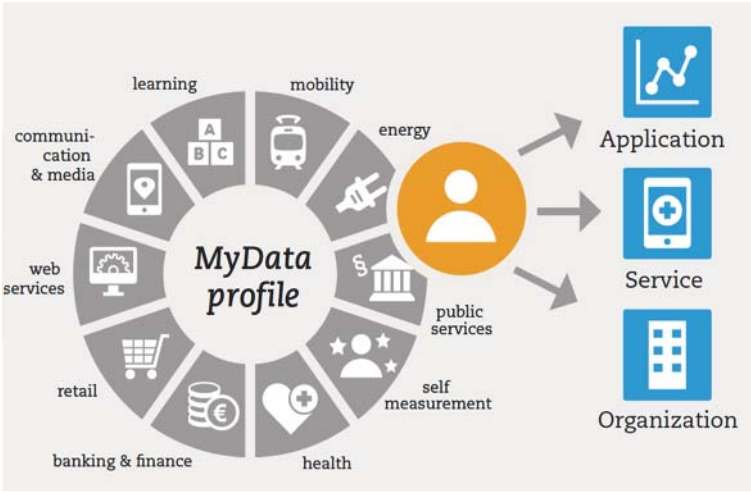
従来のオプトアウト型第三者提供や、匿名加工情報等のラフデータを利用すれば十分に実現可能であり、かつ消費者が自己管理を重視しないデータのサービス領域

本人同意

ポータビリティ権

医療情報のように、従来の第三者提供での利用が困難であったり、長期に名寄せされたディープデータが必要で、かつ消費者が自己管理を重視するデータ領域

データポータビリティに基づく分散型データ流通エコシステム



図：Antti Poikola, Kai Kuikkaniemi, Harri Honko “MyData: A Nordic Model for human-centered personal data management and processing”, 2015, CC-BY 4.0.