拡張データポータビリティとAIのガバナンス

Extended Data Portability and AI Governance

東京大学　大学院情報理工学系研究科教授
国立研究開発法人理化学研究所　革新知能統合研究センター
社会における人工知能研究グループ　グループディレクター
橋田　浩一

1986 年より 2001 年まで電子技術総合研究所。1988 年から 1992 年まで（財）新世代コンピュータ技術開発機構に出向。2001 年から 2013 年まで産業技術総合研究所。2013 年から東京大学。2017 年から理化学研究所を兼任。専門は自然言語処理、人工知能、認知科学、サービス科学など。日本認知科学会会長、言語処理学会会長等を歴任。

Hasida53@gmail.com

1 パーソナル AI

膨大な知識を集約することが大規模言語モデル (LLM) によって可能になった。たとえば ChatGPT が米国の司法試験で上位 10%に入る成績を上げたり医学的質問に対して人間の医師よりも詳細で良質の説明をしたりするとのことなので、AI が多くの知的作業において多くの人間を凌ぐようになったと言えよう。LLM が苦手な定量的評価等には専用の AI を使えば良いので、総合的に見て AI が普通の人間並み以上にできることはかなり多い。現在の AI は新しいアイデアを練るために必要な際限のない仮説検証やメタ認知の能力を欠いており、またリアルな体験から学ぶこともほとんどできず、そのような能力を備えた AI の開発はきわめて困難と考えられるが、現在の AI の能力でも社会を激変させるには十分である。

AI が集約する多様な知識はあらゆるサービスやコンテンツに及ぶ。人間は個別のサービスやコンテンツに直接アクセスする必要がなくなり、AI があらゆるデジタルなサービスやコンテンツの個人用ポータルになるだろう。人間が個別の小売事業者から商品を直接買ったり契約書や論文や法律を直接読んだりする時代は終焉しつつある。各個人に必要な商品やサービスや情報を AI が本人に直接提供する (商品とサービスの場合は本人に代わって購入してくれる) ことになるだろう。

そのような個人用ポータル AI をパーソナル AI (PAI) と呼ぼう。Bill Gates や Yann LeCan らも PAI (パーソナル AI エージェント) の普及を予測している。PAI は利用者のパーソナルデータ (PD; 特定個人に関する情報を含むデータ) をこれまでの AI よりもはるかに多く活用する。したがって、PAI が各利用者のプライバシ等の権利を侵害するリスクは明らかにきわめて大きい。逆に、PAI が利用者の PD を本人に無断で他者に漏らしたりせず、利用者がその点について PAI を信用するならば、利用者は他人に絶対知られたくないような秘密等を含む PD も安心して PAI に託すので、PAI が本人に非常に価値の高いサービスを提供し PAI 開発事業者に巨大な収益をもたらすことができる。PAI 開発事業者は、そのような収益性と社会受容性の高さゆえに、利用者の人権を守るように PAI を設計・運用し、またその点に関して利用者から全幅の信頼を得ることに腐心するだろう。詳細は割愛するが、それがうまく行けば、PAI は GDP の 20% の市場規模を持つ巨大な産業を生み出すことになる。

しかし、PAI 開発事業者が利用者のメリットより自社の収益を重視することが考えられるし、またプログラムのバグや学習データの偏りによって PAI が利用者や社会に大きな不利益をもたらすリスクもある。PAI が従来の AI よりも多くの機微な PD を用いるということは、必然的に PAI が生み出し得る価値もリスクも大きいということである。したがって、PAI に対する強力なガバナンスが求められる。

2 拡張データポータビリティ

生成 AI に関しては、プライバシや著作権やフェイク

に関するリスクが指摘されており、もちろんそれらのリスクには対処する必要がある。しかし、PAI を含む AI のリスクはその他にもさまざまなものがあるはずだが、たとえ AI のプログラムのソースコードが公開されたとしても、リスクを前以て予測し尽くすことはできないだろう。かと言って産業競争力等を考えると AI を使わないわけにも行かない。したがって、AI を活用しながらさまざまなリスクを検出して臨機応変に対処するアジャイルなガバナンスが必須である。

AI に限らないさまざまなサービスのガバナンスのためには、各サービスが利用者と社会にどのようなメリットとデメリットをもたらしているか・もたらしそうかをデータの分析によって検出する必要がある。その分析には、サービスによる利用者への介入とそのアウトカムの両方 (介入とアウトカムがオーバーラップすることもある) に関するデータが必要である。この介入は、サービスによる物理的な介入 (治療や料理の提供) だけでなく情報提供 (検索や ChatGPT の回答など) を含む。PAI があらゆるデジタルなサービスとコンテンツを集約するとすれば、技術的にはそれらの利用に関連する PD は利用者本人に集約できるはずだから、個人向けサービスの介入とアウトカムにわたるデータを多くの個人から本人同意等に基づいて収集・分析することにより、各サービスのメリットとデメリットをアジャイルに検出できると考えられる。

しかし、サービスによる介入のデータを利用者が他者に開示できるためには、データポータビリティの権利を拡張する必要があると思われる。GDPR のデータポータビリティ権は各個人が入力した PD とセンサ等で計測された PD を対象とするが、その PD から AI 等のサービス提供者が導出したデータを対象としていない。たとえば利用者の PD を含む質問に対する ChatGPT の回答はその PD から導出した情報を含むだろうが、それはデータポータビリティ権の範囲外と考えられる。したがって、サービスによる介入のデータをサービスのガバナンスに用いるにはデータポータビリティの概念を拡張する必要があるのではないか。

ただし、データポータビリティの対象に加える必要があるのは、PD から導出した情報ではなく、サービスによる利用者への介入に関するデータである。この介入のデータが利用者の経験を計測した PD と見なせるならば、現在のデータポータビリティの範囲に含まれるので、そもそもデータポータビリティ権を拡張する必要はないかも知れない。たとえそうでなくても、サービスによる介入は利用者が経験することだから、そのデータをポータビリティ権の範囲に加えることに対するサービス事業者の抵抗が少なく、法制化は容易と考えられる。

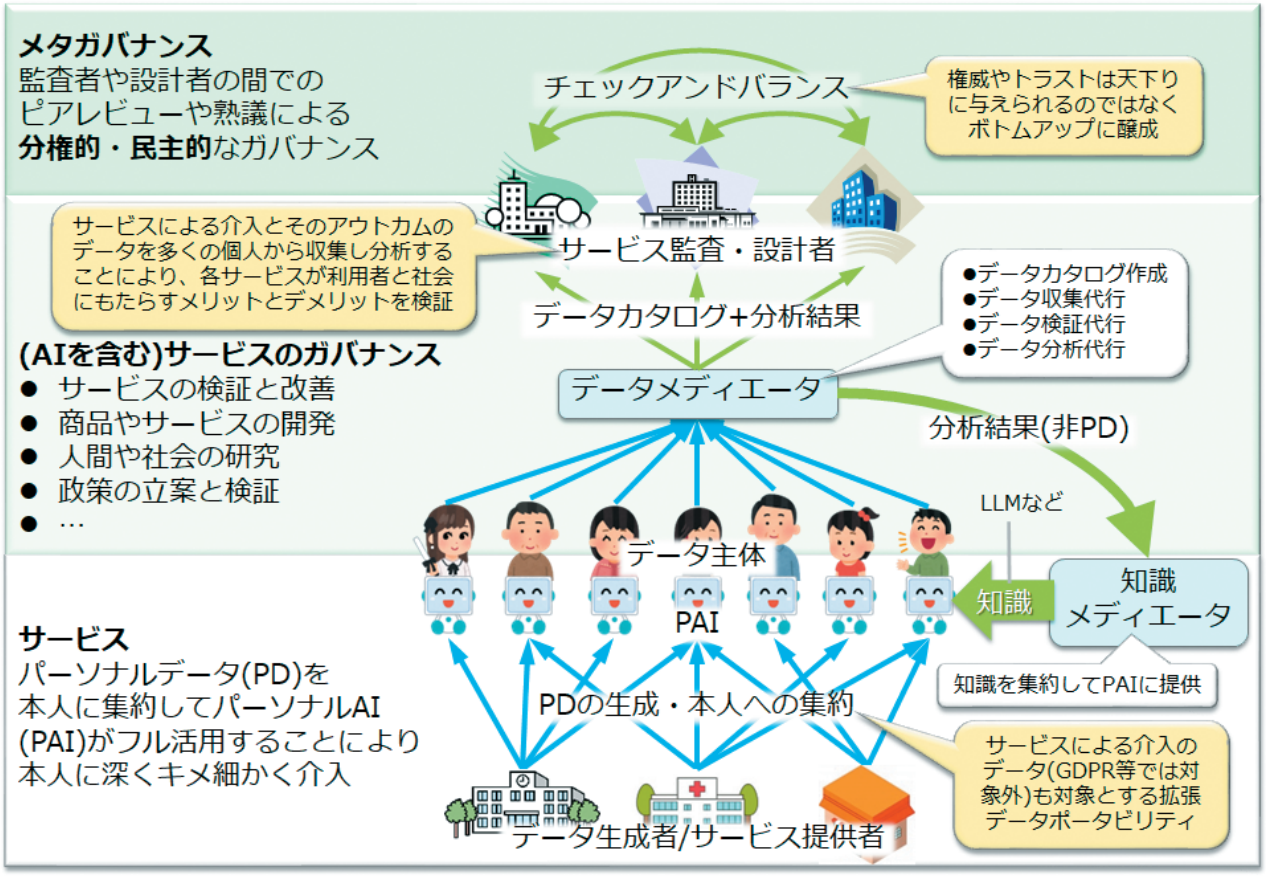
いずれにせよ、データポータビリティ権の範囲がサービスによる介入のデータも含めば、PAI に限らない多様なサービスのアジャイルなガバナンスが PD の収集・分析によって可能である。たとえば、PAI によるどのような介入が利用者の行動をどのように変容させ、それによって利用者の経済的メリットがどのように増減しているかを分析できれば、PAI の改善等に有効だろう。

言うまでもなく、拡張データポータビリティに基づくサービスのガバナンスは完璧ではない。サービスのメリット・デメリットの検証は、サービスの種類等によって難易度が異なり、事実上不可能なこともあるかも知れない。たとえば、リクルートキャリア社が「リクナビ DMP フォロー」というサービスによって得た学生の PD から求めた各学生の内定辞退率のデータを本人に十分に説明せずにトヨタや京セラに販売したといういわゆる「リクナビ事件」について考えると、その内定辞退率のデータが実際に内定の判断を左右したかどうかをデータ分析によって検証するにはかなり大量の PD が必要であり、実際には難しいかも知れない。ガバナンスの徹底にはデータ分析と他の手段を組み合わせる必要があると考えられる。

3 メディエータ

次頁の図の下段の「サービス」の層と中段の「サービスのガバナンス」の層は以上の議論を図式化したものである。いずれの層においても両面市場を仲介する機能としての「メディエータ」が必要である。

「サービス」の層では、さまざまなサービスで用いる PD を含む PD が本人に集約され、それを PAI が多様な知識 (科学や制度の知識、商品やサービスの仕様や価格などの知識、その他) と併せて用いることにより利用者にサービスを提供する。ここで多数の個人の PAI がそれぞれ多様な知識を集約するのは非常に効率が悪いので、知識を集約し多数の個人の PAI に提供する「知識



メディエータ」が必要である。PAI を事業者のサーバで稼働させる場合は PAI と知識メディエータは同一で良いが、いずれにせよ PAI が利用者の PD を (PAI 開発事業者等を含む) 他者に漏らさないことが必要である。

「サービスのガバナンス」の層では、サービスの監査者がサービスの介入とアウトカムの情報を含む PD を多数のデータ主体から収集して分析することにより、利用者と社会に対するサービスのメリットとデメリットを検証し、メリットを増進してデメリットを低減するようにサービスの改善を促す。サービスの設計者も同様に PD を収集・分析して PAI 等のサービスを開発・改良する。同様のデータ収集・分析によって人間や社会に関する学術研究や政策の立案と評価も可能である (サービス設計者は研究者や政策立案者を含む)。

ここでも、多数のデータ主体と多数のデータ利用者 (サービス監査者・設計者) とが直接 PD を授受するのは効率が悪いので、実際には「データメディエータ」が PD の授受を仲介する必要がある。データメディエータは、データ主体が保有する PD のメタデータを収集して PD のカタログを作成し、データ利用者に提供する。データ利用者はそのカタログを参照してデータメディエータに PD の収集・(真正性等の) 検証・分析を発注し、それを受注したデータメディエータは発注仕様に応じて PD を収集・検証・分析し、分析結果をデータ利用者に納入する。上述の知識メディエータもデータ利用者の一種であり、データメディエータによる PD の分析等によって得られる知識を集約する。

この「サービスのガバナンス」の層、とりわけデータメディエータの設計とガバナンスは重要な検討課題であるが、「サービスのガバナンス」とデータメディエータのあるべき姿はデータ利用の目的に応じて異なるだろう。データメディエータは EU のデータガバナンス法におけるデータ利他主義組織またはデータ共有サービス事業者に相当すると考えられる。同法はデータ主体またはデータ保有者が公益目的のため自発的にデータを提供するという「データ利他主義」の概念を規定しており、データ利他主義組織はその際のデータの授受を仲介する (上記のようにデータ分析まで行なうことは同法では想定されていない)。また、同法の下ではデータ共有サービス事業者に当局への届出が義務付けられている。商品・サービスの開発などは非公益目的だが、AI 等のサービスのガバナンスは公益目的と言えるだろう。しかし、このガ

バナンスのため上述のように多数の個人からサービスの介入とアウトカムのデータを収集し分析することにより各種サービスの知識を得るわけだが、その知識を用いて各個人にサービス診断 (各種サービスが本人にもたらしているメリットとデメリットの検証など) のサービスを有料で提供することは公益目的だろうか？ このようなことを明確化するには、データ利他主義等の定義を詳細化する必要があり、それに応じてデータメディエータ等のビジネスモデルが明確になると考えられる。

4 民主的ガバナンス

前図の上段の「メタガバナンス」の層では、多数のサービス監査者・設計者がデータ分析の結果を互いに比較し、チェックアンドバランスにより分権的・ボトムアップにトラストを醸成する。権威もトラストも特定の者に天下りに与えられるわけではなく、複数のデータ利用者へのトラストがデータに基づくピアレビューと熟議によって醸成・維持される。このような分権的・民主的なメタガバナンス (サービスのガバナンスに対するガバナンス) が可能なのは、拡張データポータビリティに基づいて、サービスの介入とアウトカムに関する PD の収集・分析が容易になり、多くのデータ利用者が生まれるからである。このように民主的なメタガバナンスにより、その対象であるサービスのガバナンスの公正性が担保される。

前述のように拡張データポータビリティによるガバナンスはもちろん完璧ではない。しかし拡張データポータビリティは、商品・サービスの開発や人間・社会の研究や政策の立案と評価のみならず民主的なガバナンスの基盤にもなるという意味で、総合的メリットがきわめて大きいと考えられる。