個人データの本人管理に基づく自律分散協調ヘルスケア

Autonomous Distributed and Collaborative Healthcare Based on Self-Management of Personal Data

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**

PROFILE 1986 年より 2001 年まで電子技術総合研究所。その間 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 年から現職。専門は自然言語処理、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。

hasida.koiti@i.u-tokyo.ac.jp

1 個人データの集中管理と分散管理

ほとんどの B2C サービスにおいては事業者が多数の個人のデータを集中管理している。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、多数の個人のデータをまとめて管理しているとまとめて漏洩するリスクが高い。また、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るので、本人による自己情報コントロール（特に、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 B2C サービスの価値が高まりにくい。

これらの問題を解決するには、個人データの管理をなるべく個人に分散させることによってリスクを低減するとともに、各個人（代理人）が自らの意思に基づいて本人のデータを他者と共有して活用できる必要がある。そのための仕組みを PDS（personal data store）[2,6] と言い、PDS のうち特定の事業者の集中管理に依存しないものを分散 PDS（decentralized PDS）[1,3,4] と言う。

2 PLR

PLR（personal life repository）[3,4] は分散 PDS の一種であり、下図のように、データ共有のための中継サーバとして Google ドライブや Dropbox 等の基本無料のパブリッククラウドストレージをそのまま用いて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。またクラウド上でも端末内でも個人データを暗号化し、復号のための鍵は、原則として Google や Dropbox には開示せず、本人が指定する他者のみに開示する。さらに、法規や契約だけでなく、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、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、自己情報コン

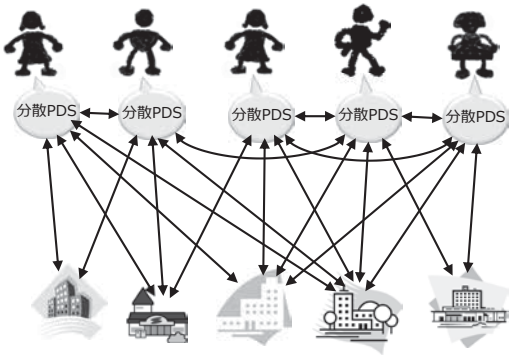

図 1　分散管理（上）と集中管理（下）との組合せ

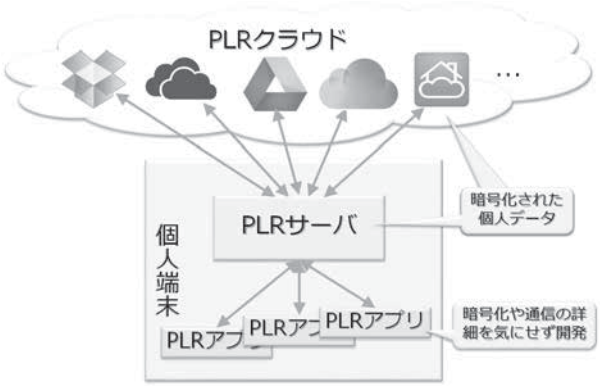

図 2　PLR のアーキテクチャ

トロールを実現する。

集中型サービス同士が直接相互連携するのは一般にきわめて困難であり、不可能な場合も多い。したがって、下図のように、あらゆるサービスを連携させるにはPLRのような分散PDSが必要である。たとえば下図では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個人データを融通し合うなどということは考えられない。したがって、たとえば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、PLRのような仕組みを使って個人が本人のデータを名寄せするしかない。

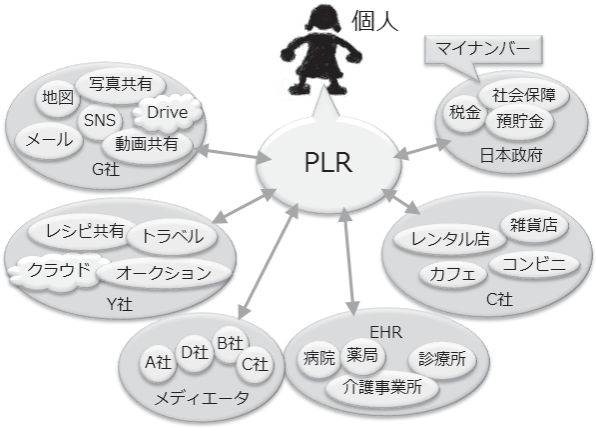

図3　集中型サービス同士のPLRによる間接的連携

3 自律分散協調ヘルスケア

PLRは介護記録を作成し共有するアプリの基盤としてすでに介護の現場で運用されている[5]。2015年8月には、図4のように、被介護者の家族が本人のデータを管理して事業者等と共有する運用を始めた。

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年末には図5のように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。

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個人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

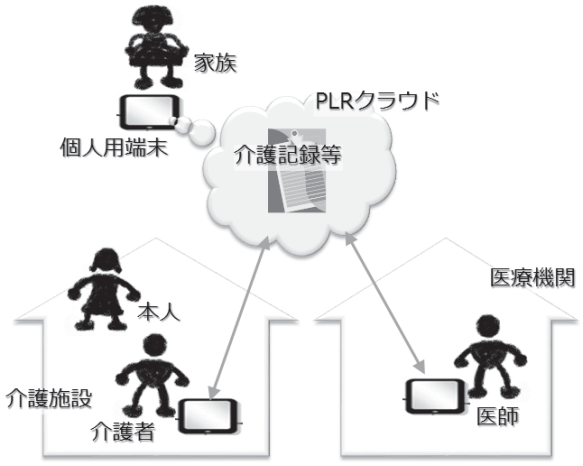

図4　PLRに基づく介護記録等のデータの個人管理による事業者等の間接的な連携

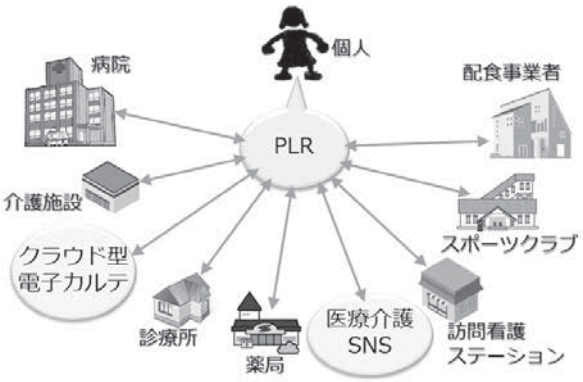

図5　自律分散協調ヘルスケア

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（electronic health record）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PLRのような仕組みが必須である。

4 ヘルスアビッグデータ

PLRによって、個人は本人のデータの共有先での利用形態をDRMで技術的に制限できるので、ヘルスケア等に関連する機微なデータでも安心して開示できるようになり、パーソナルビッグデータの利活用が進むと期待される。

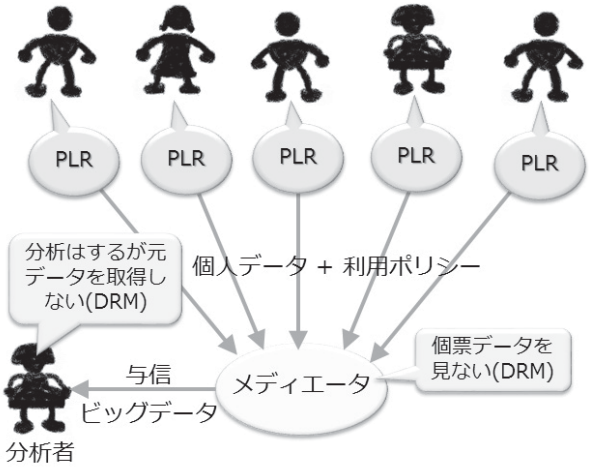

図６　ビッグデータの利活用

上図のように、個人は自分のデータに何らかの利用ポリシーを付与してメディエータ（ビッグデータの流通を仲介する事業者）に開示し、メディエータおよびメディエータがビッグデータの利用を許諾した者は DRM によりその利用ポリシーの範囲内でデータを活用する。データの二次利用においては、「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」というような利用ポリシーがほとんどの場合に妥当であろう。

参考文献

[1] 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 . 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、2015;249-255.

[2] Gordon Bell. A Personal Digital Store. Communications of the ACM, 2001;44: 86-91.

[3] 橋田 浩一 . 分散 PDS による個人データの自己管理 . 人工知能学会誌、2013;28(6): 872-878.

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

[5] 橋田 浩一、和田 典子、藤島 寿智、上沼亜希子 . 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― . デジタルプラクティス、2015;6(1):29-34.

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