

分散型台帳技術とパーソナルデータストアによる在宅ケア情報の共有

加藤 綾子†

文教大学情報学部†

1. はじめに

分散型台帳技術 (Distributed Ledger Technology: DLT) は、中央管理機構を必ずしも必要としないことや、金融等の取引システムの維持管理コストを削減する手段となり得る可能性などが注目され、多分野への応用が期待されている。一方で、情報が全ノードによって保有される点や、データの真正性が参加ノードの多数決で承認される点など、いくつかの部分で応用可能性が疑問視される側面もある。

特定の組織や政府などに拠らない脱中心的な取引やデータ流通の在り方は、このほかにも、パーソナルデータストア (Personal Data Store: PDS) を用いた個人本人の同意に基づく方法が考案されている。

本稿は、社会的要請の高い在宅ケアのデータの共有について、パーソナルデータストアの使用を想定しつつ分散型台帳技術を組み合わせた場合に成し得ることの一案を検討・提示する。

2. 分散型台帳技術の特徴

分散型台帳技術は次の5つの技術要素から構成される。すなわち、(1) 台帳を管理するデータベース技術、(2) 暗号学的ハッシュ関数、(3) 公開鍵暗号技術、(4) P2P 通信技術、(5) コンセンサスアルゴリズムである [1]。Satoshi Nakamoto [2] などによると、分散型台帳技術の取引手順の概要は次の通りである。すなわち、ある取引主体 (ノード) は、1つ前の取引内容と次の取引主体の公開鍵の情報などから生成されたハッシュ値に電子署名をして、取引情報を P2P ネットワークに流す。その取引情報は台帳に記録される。次の取引主体が取引する際も同様の行為が行われる。

複数の取引はまとめられてブロック化され、ブロックのハッシュ値が生成される。ハッシュ関数は生成元のデータが少しでも異なると異なるハッシュ値を生成する。分散型台帳技術ではこの特性を活かしてデータの改ざんの有無が確認される。このブロックは時系列に連結されて、ブロックチェーンとなる。

分散型台帳技術は、中央管理機構のない P2P における二重取引問題を解決するため、Proof-of-Work という負荷を課している [2]。分散型台帳システムのポイントは、信用を担保する機関が存在せず、かつ、参加者が誰であったとしても、適切な取引の行為がなされることで生成されたデータだけが選択され続ける方法によって、データの真正性を担保しよ

Sharing Home-Care Data Using Distributed Ledger Technology and Personal Data Store

†Ayako Kato, Faculty of Information and Communications,

Bunkyo University

うとする点である。Proof-of-Work では最も長いチェーンが採用される。最も長いチェーンは、ネットワーク参加者の大多数が支持したチェーンであることを表している [2]。

つまり、このシステムは多数決主義を採用している。これは参加者の大多数は悪意が無いという性善説に則っており、悪意ある参加者が多数を占める場合には成立しない。

悪意あるノードをできるだけ参加させない方法の一つは、ネットワークへの参加制限を設けることである。分散型台帳技術は、パブリック型とコンソーシアム型ないしプライベート型 (以下クローズド型と呼ぶ) に大分される [1]。前者では、各ノードのネットワークへの参加は自由であり、ネットワークの中央管理機関が不在となる。後者はネットワークへの参加に承認が必要となるため、厳密には脱中心型であるとはいえない。その代わり、後者は前者に比べて緩やかなコンセンサスアルゴリズムの採用が可能であり、ネットワーク参加者の約3分の2以上の合意をもってデータの真正性が承認されることが多いという [1]。

分散型台帳技術では、ネットワークの参加者全員が全取引情報の記録を保有することになる。公的機関に登録され公開されているような情報であれば、情報が全ノードによって共有されても差し支えないが (例えば土地の登記簿など)、機微情報については全ノードによる共有が必ずしも適さないことがある。

分散型台帳技術で扱うことのできる対象は、まだ模索段階であるが、全ノードが同じプロトコルで情報を追記しそれを全ノードで共有するシステムである訳だから、通貨など一つの規格化された情報が扱いやすいだろう。全ノードが同じ情報を共有すべきケースは、実はさほど多くないかもしれない。ただし全ノードによって同じ情報が共有されるべきユースケースを見出すことができれば、分散型台帳技術の特徴を活かすことができるかもしれない。

3. パーソナルデータストアの役割および分散型台帳技術との組み合わせ

地域包括ケアでは医療・介護・予防・住まい・生活支援の一体的提供が目指されているが [3]、一人のケア対象者に対して複数の事業者が関与するため、複数事業者による当該個人に係る情報の共有・連携が重要な課題となる。この課題に対応するために、情報連携システムの導入が試みられている [4]。また、医療介護分野の一部ではパーソナルデータスト

ア(PDS)の導入が検討され始めている[5]。長年日本の医療介護分野では事業者間のデータ共有・連携が困難であったが、PDSは事業者間のデータ共有に個人を介在させることでこの問題を解決しようとしている。PDSは個人が所有するものと想定されるが、事業者のデータストア(以下、事業者PDS)があっても構わない。ただし、事業者PDSは従来の事業者のデータベースとさほど変わらない位置づけとなる。

個人の介在により、複数事業者のデータが個人のPDSに集約されたとして(事業者が保有するパーソナルデータの扱いに関して個人の管理権限が及ぶようになったとして)、次に問題となるのは、異なる事業者間のデータ共有方法とデータ連携方法だろう。

事業者間のデータ共有・連携に個人を介在させることで、確かに従来に比べて遥かにパーソナルデータの利活用が促進されるだろうけれども、例えば少なくとも次のような懸念事項が考えられる。

(a)事業者間のデータ共有・連携に個人を介在させた場合、個人が不都合なデータを書き換えたり秘匿したりする恐れがある。この問題への対処策として、PDSの実現方法の一つであるPLRではDRMの使用が想定されているが、専門家としての事業者にとって個人は素人であり、素人の手を介したデータを必ずしも信用し切れないという心理的障壁は払拭できないかもしれない。ただし、個人の管理権限のもと、事業者間でデータが直接移管される場合はこの限りではない。

(b)複数の事業者が一人のケア対象者についてそれぞれ別個に同一種類のデータを測定している場合、それらのデータを結合させるのに手間を要する。事業者間でデータが直接移管される場合であってもこの手間は省けない。事後、統計分析等にデータを使用するならば、データ整形の時間を要しても差し支えないが、在宅ケアで人の生命が掛かっている場合や、測定の都度これまでの履歴を確認する必要がある場合などは、複数の異なる事業者がそれぞれ取得したデータが速やかに共有・連携されると良い。

例えば、医師、看護師、薬剤師、配膳業者、見守りサービス業者、家族がそれぞれ別個にケア対象者の血圧を測定しているとする。その場合、複数事業者による測定結果は、1つのシークエンス・データとして時系列に連結されると有用であるだろう。なおかつ、これまでのデータに改ざんが無いことが即時に確認できると良い。一事業者では測定頻度が低い場合でも、複数事業者による測定結果が時系列に連結されれば、高頻度データ化する。

クローズド型の分散型台帳技術を用いて、例えば血圧データなど、同一種類のデータでそれぞれのブロックチェーンを形成することができれば(図1)、(a)の懸念に対しては、データが改ざんされていないことが関係事業者間で相互承認される。(b)の課題に対しては、分散型台帳技術では時系列に取引情

報が連結される訳だから、ほぼ自動的にケア対象者についての同一種類のデータのシークエンスが生成されることになる。

分散型台帳技術は、Proof-of-Workの採用によって過去の取引情報がほぼ変更不可能となるため、取引情報の修正・訂正が頻繁に発生するような分野には不向きであるとの指摘がある[1]。しかしながらこの特徴は、情報そのものやその記録の厳密さが求められる医療介護分野には適している可能性がある。修正・訂正に関する情報も含めて全ての記録が保存されていれば、データの遡及可能性も高まる。

今回のケースでは参加ノードを制限するクローズド型の採用が想定される。参加承認には個人のPDSを利用して、当該種類のデータの測定者に参加許可を与える方法が考えられる。ただ、本稿の案は結局、本人同意に基づく分散的なデータ流通を実現しようとするPDSの在り方と相同する。しいて言えば、複数事業者によって同一種類のデータの測定がなされる場合に、当該ノード同士のデータの連結と同期の方法として、分散型台帳技術に利点を見出すことができるのではないだろうか。

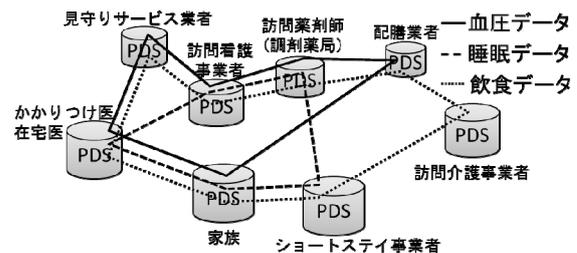


図1. 複数事業者による同一種類のデータ連結・共有のイメージ

4. まとめと課題

本稿は、在宅ケアのデータの共有においてPDSの使用を想定しつつ、クローズド型の分散型台帳技術を組み合わせた場合、複数事業者による同一種類のデータの連結や同期において利点を見出せるのではないかと指摘した。ただし、これらはPDSによっても実現され得る可能性があるため、分散型台帳技術を組み合わせるといふ本案の必然性には課題が残る。

主要参考文献

- [1]山藤敦史, 箕輪郁雄, 保坂豪ら(2016)「金融市場インフラに対する分散型台帳技術の適用可能性について」『JPX ワーキング・ペーパー』, Vol. 15, 日本取引所グループ。
- [2]Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," <https://bitcoin.org/bitcoin.pdf>
- [3]厚生労働省, http://www.mhlw.go.jp/stf/seisakunitsuite/bunya/hukushi_kaigo/kaigo_koureisha/chiiki-houkatsu/
- [4]武藤真祐(2015)「地方における地域包括ケアを推進するための情報連携 ICT システムの展開について」地方創成 IT 利活用推進会議 第2回政策企画ワーキンググループ, http://www.kantei.go.jp/jp/singi/it2/region/sewg_dai2/siryou6.pdf
- [5]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(2015)「地域包括ケア等の基盤となるヘルスケアデータの本人管理に関する実証を開始: 自身のヘルスケアデータを自ら管理・活用出来る世界初の仕組み」, http://www.sict.i.u-tokyo.ac.jp/news/pr_20150909_hasida.pdf