

## 災害時利用を想定した Personal Data Store を基盤とした電子母子手帳の開発 Development of Electronic Mother and Child Handbook on Personal Data Store Assuming Disaster Use

永山 大輔<sup>†</sup> 住友 貴広<sup>†</sup> 越塚 登<sup>†</sup>  
Daisuke Nagayama Takahiro Sumitomo Noboru Koshizuka

### 1. 背景

パーソナルデータの適切な共有は、様々な場面で重要性を増している。例えば、東日本大震災では産科医療機関の機能が低下した一方、母体搬送要請が平時の 5 倍に増加し、0 歳児の致死率は 277 倍となった。背景には小児周産期医療リソースの不足、災害時医療計画の整備不足に加え、情報共有機構の機能不全が挙げられる。処置が必要な妊産婦の抽出や医療情報アクセシビリティの低下により、妊産婦に適切な処置を施すことが困難だった。

本研究では災害時の情報共有及び医療支援を円滑にするため、Personal Data Store<sup>1</sup>(以下 PDS) 機能を有した電子母子手帳を開発し、収集した医療・位置データを関係機関と適切に共有する機構を構築することを目的とする。

平時には電子母子手帳として使用し、医療データ、及び位置データを収集する。災害時には、救助計画立案時における救助が必要な母子を地図上にマッピングする機能を提供する。ユーザの事前承諾のもと、平時の診察で蓄えられた医療データ、及び現在の位置データを事前に登録された病院、保健所、NPO などの災害救助関連機関と共有し、地図上でどの地点にどのような状態の要救護者が存在するかを可視化(図 1)、救助計画立案の一助とする。

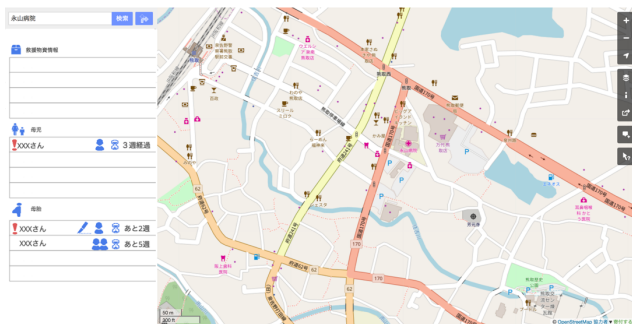


図 1 要救護者を確認する web アプリ  
イメージ図

### 2. 課題

本提案の電子母子手帳を実現するために、主に 2 つの技

<sup>†</sup> 東京大学 The University of Tokyo

<sup>1</sup> ユーザーの活動によって作り出されたデータ、及び個人に関する情報を主体的に保存・管理・提供することを可能とするシステムの総称

術的な課題を解決する必要がある。

#### 2.1 簡便なアクセスコントロールの設定

本システムでは被災時のみ医療情報や位置情報を関連機関と共有するため、アクセスコントロールを設定する必要がある。しかし、現実世界のイベントを考慮して行うアクセスコントロールの設定は、かなり煩雑である。どんな非常事態が(震災時、ミサイル発射時など)、どこで起こった時(自宅近辺、現在地付近、予め登録した地域など)、誰に(NPO、保健師、病院など)、どの情報を(医療データ、位置データなど)共有するかを設定する必要がある。全ての組み合わせについて一つ一つ手動で設定するのは非常に困難であると考えられるため、アクセスコントロールの設定をできる限り簡便にする機構が必要となる。

複雑なアクセスコントロールへの対応策としては、本人のデータの運用を代理人が行う情報銀行[1]があるが、情報銀行は、特定のサービスで生じたデータを他の事業者へ販売する際の意思決定を代替するものであり、今回のように一つのシステム内で完結したアクセスコントロールに対しては有効でない。

#### 2.2 ユーザ自身によるデータ管理の実現

今回扱う位置データ及び医療データのようなプライバシー情報を扱う場合、富士通が開発するオープンソース PDS プラットフォーム Personium[2]や Microsoft が提供する健康情報管理 PDS の Microsoft HealthVault[3]ではデータを特定事業者が集中管理していた。しかし集中管理方式は、全データにアクセス可能な運用者がセキュリティにおける単一障害点なる点や、各事業者のデータフォーマットや情報公開手段の整備不足によりデータの可用性が低下してしまう点で課題を残している。[4]

そのため、は Personal Life Repository[5]では、個人の電子カルテデータや購入履歴、預貯金と言った各種データを暗号化して、Google Drive などの無料クラウドへ保存する手法を提案している。この手法であれば個人のデータは個人が運用可能で、任意のサービスにデータ本体を配置することによりデータの持続性と可用性を担保できる。一方この手法では、ファイルシステムを利用してデータ構造を構築する必要が生じる。そのため、大量のリクエストの処理や、複雑なクエリを発

行してデータを取得することが難しいという課題がある。

### 3. 提案方式

2. で明らかにした課題に対し、本研究では以下のアプローチで解決を試みる。

#### 3.1 機械学習のリアクティブな値提案による、簡便なアクセスコントロールの設定

本研究では煩雑なアクセスコントロールの設定を、機械学習とリアクティブなインターフェースによって支援する方式を提案する。

ユーザがプライバシーポリシーに関する幾つかの質問に回答すると、そのユーザと似通ったポリシーを持つユーザのアクセスコントロールポリシーを参照し、仮のアクセスコントロールの設定を提示する。ユーザは仮の値を見て、自分の考えて異なっている点が存在すれば、その都度値を変更する。こうして変更された値により再度機械学習によるマッチングが行われ、仮の値が入力されていた項目に対し、更新が適用される。ここで、ユーザが手動で設定した値のみでなく、自動的に提案された値で、かつユーザの目に写ったがユーザが、アクションを起こさなかったものについても入力値が確定されたと判断する。

以上のシステムにより、ユーザは最低限の操作によってアクセスコントロールを設定することが可能になる。

#### 3.2 個人向けクラウドストレージサービスを利用した、ユーザ自身によるデータ管理

Google 社が提供するアプリケーション、Fusion Table [6] という RDB ライクなサービスを利用して、データがユーザによって運用管理される PDS を実現する。2.1 で述べたようなアクセスコントロールに必要なポリシー及び、現実のイベントを参照するためのシステム内変数と、Fusion Table の使用に必要な Credential 情報のみ本システムの API サーバによって管理し、実際のデータはすべて Fusion Table 上で管理する。(図 2)

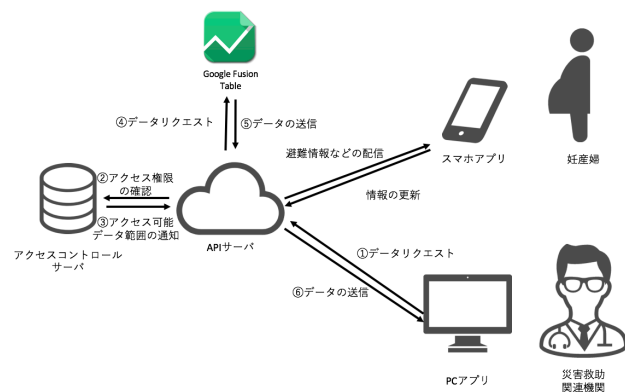


図 2 Google Fusion Table を用いたデータ参照の流れ

ユーザは本システムのアカウント作成時に Google のアカウントを紐づけ、OAuth 認証により特定の Fusion Table への接続を許可する。診察で得られたデータを書き込む際には、本システムが提供するサーバを仲介し、ユーザの Fusion Table に書き込まれる。

被災時などにデータ所有者でないユーザにより医療データが参照される際は、アクセスコントロールに必要な情報を持っている API サーバがブローカの役割を担い、情報をリクエストしたユーザのアクセス権限を確認し、データを返却する。救助関連機関がデータを本システムの API サーバにリクエストすると、API サーバはリクエストを発行したユーザに閲覧権限が認められるかどうかを、アクセスコントロールサーバに確認する。アクセス権限が認められなかった場合は、リクエストを棄却する。アクセス権限が認められた場合は、API サーバが該当ユーザの Fusion Table にデータのリクエストを SQL 形式で発行する。Fusion Table が SQL を処理し生成したデータを受け取った API サーバ、同データを関連機関の PC アプリに返却する。

### 4. 今後の展望

提案システムを構築し実際の医療現場で利用されることにより、そのフィードバックを元にアクセスコントロールやユーザによるデータ管理の手法についての運用上の課題を洗い出す。最終的には複数の医療圏で採用され、従来の紙の母子手帳を代替することを目指す。一方で妊産婦という特定の疾患領域にとどまらず、お薬手帳や電子カルテの仕組みの中に本提案システムのような情報共有機能が付随されることで、より被災時のレジリエンスが高い社会の実現が期待される。

#### 参考文献

- [1] 総務省 平成 29 年度版情報通信白書 [http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/pdf/n2200\\_000.pdf](http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/pdf/n2200_000.pdf)
- [2] Personium <https://personium.io/>
- [3] Microsoft HealthVault <https://international.healthvault.com/>
- [4] 橋田 浩一, 分散 PDS と情報銀行: 集めないビッグデータによる生活と産業の全体最適化, 情報管理, 公開日 2017/07/01, Online ISSN 1347-1597, Print ISSN 0021-7298, <https://doi.org/10.1241/johokanri.60.251>, [https://www.jstage.jst.go.jp/article/johokanri/60/4/60\\_251/article-char/ja](https://www.jstage.jst.go.jp/article/johokanri/60/4/60_251/article-char/ja)
- [5] Hasida.K. 2014. Personal life repository as a Distributed PDS and its dissemination strategy for healthcare services. Big Data Becomes Personal: Knowledge into Meaning.
- [6] Gonzalez, Hector, et al. "Google fusion tables: data management, integration and collaboration in the cloud." *Proceedings of the 1st ACM symposium on Cloud computing*. ACM, 2010.