Vol.2018-GN-104 No.13
2018/3/20

パーソナルデータストアを用いたヘルスケアアプリの開発

佐藤優希[†1]　藤井良典[†1]　中村章人[†1]

概要：AI・IoT 技術の進展により，特定可能な個人に関係したパーソナルデータは社会やビジネスで貴重な資源となっている．パーソナルデータの利活用に関する主導権を事業者から個人に移し，本人の意思に基づいて第三者に提供して利活用する VRM（Vendor Relationship Management）という概念とそれを実現する仕組みであるパーソナルデータストア（PDS）が注目されている．しかし，PDS は十分に普及しておらず，アプリケーションも少ない．我々はヘルスケアを事例として PDS の研究・開発を進めており，ユースケースの分析とアプリケーションの開発を通して PDS の機能要件や外部インタフェースを明確にすることを目指している．本論文では，PDS のユースケースを示すとともに，オープンソース PDS Personium を用いたアプリケーションの開発事例を報告する．本アプリケーションはウェアラブルデバイスから取得したヘルスケアデータを PDS で蓄積・管理し，データの可視化やボットによるリマインドなどにより健康づくりへの取り組みを支援する．VRM が要求するパーソナルデータの自己情報コントロールやデータポータビリティは，PDS を用いることで容易に実現できることが確認できた．

キーワード：パーソナルデータ，PDS，VRM，ヘルスケア

Development of Health Care Applications using Personal Data Store

YUKI SATO[†1]　YOSHINORI FUJII[†1]　AKIHITO NAKAMURA[†1]

Abstract: With the rapid advances in AI and IoT technologies, personal data became valuable resources to society and business. Vendor Relationship Management (VRM) is an activity which aims to provide customers with control of personal data and independence from vendors. A software tool called PDS (Personal Data Store) realizes VRM. Although VRM and PDS are factors that are important in personal data utilization, they have not become common. We are proceeding with the research of PDS technology by developing applications in the field of health care. The objectives are definitions of the functional requirements and the external interfaces of PDS. In this paper, we present user cases and applications which utilize health care data and PDS. We use an open source PDS, Personium, for implementation. The base system collects user's health care data via wearable devices and stores them in PDS. The applications assist user's effort to promote good health by visualization of health care data and automatic reminding. The prototype confirmed that PDS facilitates implementation of self-information control rights and data portability requirements demanded by VRM.

Keywords: Personal Data, PDS, VRM, Health Care

1. はじめに

近年の AI・IoT 技術の進展により，特定可能な個人に関係したデータ（パーソナルデータ）は社会やビジネスで貴重な資源となっている[1,2]．例えば，ビジネス分野では新事業・新サービスの創出やマーケティング・広告の材料として個人の行動履歴や購買履歴などのパーソナルデータを利活用している．病院では医療診断の材料として患者のヘルスケアデータの利活用が始まっている．

これまでのパーソナルデータを収集する仕組みは顧客関係管理（Customer Relationship Management: CRM）と呼ばれ，企業が顧客のパーソナルデータを収集・蓄積・管理し，広告・販売促進などのアプローチをしていく［図 1］．CRM では，パーソナルデータ利活用の主導権が企業側に存在し，顧客が自分のパーソナルデータを利活用することはできない．

この CRM の問題に対して，パーソナルデータに関する主導権を個人と企業との間で逆転させた新たな関係構築を目指す事業者関係管理（Vendor Relationship Management: VRM）[2,3]が提案された．顧客は自身のデータをいつでも参照できるだけでなく，どの企業がいつどのように自分のデータを利用するのかを決める権利を有する．このように個人が主導権を持ってパーソナルデータの利用を制御することを自己情報コントロールという．また，顧客はサービスを提供する企業や製品を自分で選択できる権利を有する．サービスや製品の切り替えを行うには，データポータビリティ，すなわちそれまでに蓄積したデータを簡単に移転できる必要がある．

このような VRM の考え方を実現するデータ管理の仕組み（システム）をパーソナルデータストア（Personal Data Store: PDS）[4,5,6,7,8]という．PDS は，パーソナルデータを個人の制御下で蓄積・管理し，本人の意思に基づいて第三者に提供し，利活用するための仕組みである．

†1 会津大学
University of Aizu

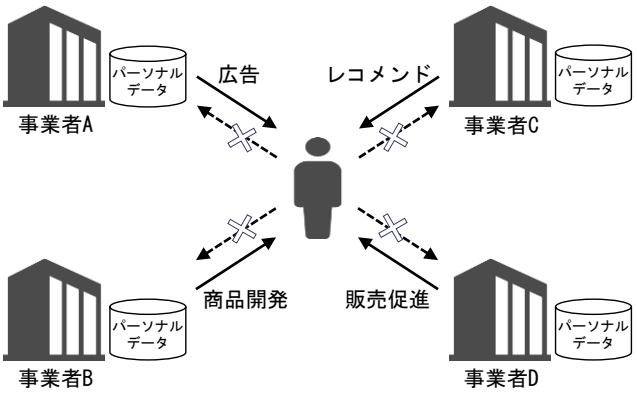

図 1: Customer Relationship Management (CRM)
Figure 1: Customer Relationship Management (CRM)

PDS のソフトウェアやサービスとして，OpenPDS[9]やPLR[10]などがある．しかし，PDS はまだ普及しているとは言えず，PDS を利用したアプリケーションも少ない．したがって，その機能や外部インタフェースは十分検討されていない．特に，PDS 間および他のシステムとの相互運用性や標準プロトコル，アプリケーションの開発に必要なAPI の検討が重要である．

我々は，ウェアラブルデバイスを用いて個人の活動量などのヘルスケアデータを PDS に収集・蓄積し，VRM の考え方に基づいてこのデータを第三者と共有することで健康増進や疾病予防に役立てるヘルスケアアプリケーションを研究・開発している．本論文では，アプリケーションの概要を紹介するとともに，Personium [11]というオープンソースPDS を用いた実装について述べる．

本論文の構成は以下のとおりである．まず２章でヘルスケア分野における PDS のユースケースと, PDS の機能要件を示す．３章では，PDS を用いたヘルスケアアプリケーションの開発事例を報告する．４章では，ヘルスケアへの取り組みを推進するゲームアプリケーションの構想について述べる．

2. PDS のユースケースと機能要件

本章では，PDS のユースケースを示し，機能要件を整理する．我々は個人の活動データや生理データを PDS に収集・蓄積してこれを VRM のモデルに基づいてヘルスケアに利活用するアプリケーションを開発している．ここではPDS の一般的なユースケースではなく我々のアプリケーション設計の基になったものを挙げた．石垣ら[8]によれば，PDS の利用目的はマーケット型，ヘルスケア型，コミュニティ型の三つに分類できる．我々は，個人だけでなく地域やコミュニティのヘルスケアに関する課題解決を図ることも目的としているので，ヘルスケア型でコミュニティ型のアプリケーションといえる．

2.1 ユースケース１：保健指導と疫学研究

個人の活動状況や生理的特徴は，健康増進や疾病予防など，健康管理や保健指導などに利用できる［図 2］．年齢，性別，身長，体重といった基本データに加えて，歩数，ランニング距離やエクササイズ時間，消費エネルギーなどの活動量データ，心拍数や血圧などの生理データを連続的にPDS に蓄積する．データ収集にはウェアラブルデバイスやIoT 機器を利用する．

上記のパーソナルデータを保健師や栄養士に開示することで，適切な保健指導を受けられる．また，血圧などの生理データは，自己申告よりも正確なデータを得られる，心理的な影響をうけない安定状態の測定結果を得られるといったメリットもあり，診断の精度に寄与する．一方，匿名化したライフログデータを大量に集めることができれば，疫学研究に役立てることができる．

従来からインターネットに接続できるデバイス（例えば体重計）を利用したデータ可視化サービスは存在するが，ここで重要なことはデバイスやサービスに分散しているデータを集約できることと，これらのデータをいつだれに提供するかを本人が制御できること（自己情報コントロール）である．

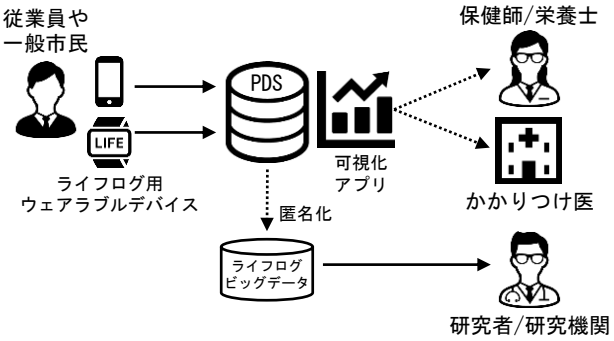

図 2: ユースケース１: VRM に基づく保健指導と疫学研究
Figure 2: Use Case 1: Health Guidance
and Epidemiological Study based on VRM

2.2 ユースケース２：リマインドやアドバイスの自動化

先のユースケースでは，データの提供相手が人であったが，これをプログラムやサービスに置き換えることもできる．我々は，ボットの利用によりリマインドやアドバイスを自動化する機能をアプリケーションに組み込もうとしている．

例えば，活動量の目標値を設定しておくと，一定時刻に過不足の状況を通知し，活動を促すことができる．また，生理データの異常変化に関しては，注意喚起に加えて，家族や医療機関への通知を自動化することができる．

このような自動化サービスは，本人の希望により自由に

切り替えて利用できるべきで，いつ誰にどの情報を開示するかという自己情報コントロールが重要になる．また，ボットなどのプログラムがデータを利用するためには，機械可読な形式で PDS からデータを取り出せねばならない．

2.3 ユースケース３：健康づくりの継続支援

運動や食事は健康管理の重要な要素であるが，継続することが難しい人もいる．この問題に対して，我々はゲーミフィケーション（ゲーム化）[12]の考え方を取り入れて解決を図ろうとしている．具体的には，コミュニティでの情報共有とゲームを考える．

コミュニティ情報共有は，匿名を前提として参加者が自分のヘルスケアデータを公開しあうことである．また，オプトインにより，家族やサークルなど特定の個人と実名でデータを共有する．情報共有することで，他者との比較や自分のレベルを把握して競争心をあおる．

ゲームでは，複数の参加者が順位やポイントを競うことで，健康づくりを楽しみながら継続できる．

2.4 PDS の機能要件

アプリケーションの開発において重要となる PDS の機能要件を以下に述べる. 全要件は文献[1,2]を参照されたい.

2.4.1 自己情報コントロール

自己情報コントロールとは，パーソナルデータを本人の意思に基づいてどのデータを誰に何のためにいつからいつまで提供するかを制御できる仕組みを指す.

例えば，図 2 に示したユースケース１では，自分のヘルスケアデータを保健指導期間中は特定の保健師にすべて開示する．また，ユースケース２のリマインドボットには常にデータアクセスを許可するが，別のボットを利用したくなったら以前のボットのアクセス許可は解除する.

.

2.4.2 データポータビリティ

データポータビリティとは，本人の意思に応じて個人のパーソナルデータを他の事業者に移転できることである. PDS のデータ入出力は当然ながらプログラムで行うため，データは機械可読な形式で取得できねばならない.

PDS のアプリケーションや外部サービスとの連携では，PDS で定められた API を通じてプログラムがデータを操作する．このためデータ形式やプロトコルは，Web で広く用いられている標準化されたものであることが望ましい．また，データには移動履歴や心拍数記録のような構造型のものと，食事写真のような非構造型のものがある．これら２種類のデータを扱えることが求められる.

2.4.3 個人 ID の管理と認証・認可

パーソナルデータを管理する PDS では，個人を識別してデータへのアクセスを制御することが重要である．自己情報コントロールを実現するには，相手の認証と，データの種類別など細粒度での認可が必要である.

ID 管理と認証・認可の機能は，PDS で固有のものを実装する場合と，Web の標準プロトコルである OpenID Connect[13]や OAuth[15]を利用する場合が考えられる．ボットの利用や外部サービスとの連携を考慮すれば，後者の導入が必要である．また，ユースケース１で保健指導をチームで行う場合などは，複数の利用者をまとめて管理するロールベースのアクセス制御ができるとよい.

2.5 オープンソース PDS: Personium

我々は上述の要件を満たす PDS の実装として，オープンソースソフトウェアの Personium[11, 14] を用いる．Personium は以下の特長をもつ.

- **オブジェクト階層**: 複数の PDS サーバ・PDS 事業者間の連携を前提にした設計になっている．サーバを Unit，事業者（テナント）領域を Cell と呼び，一つの Unit に複数の Cell が共存できる．また，アプリケーションごとのデータ格納領域を Box と呼び, 単一 Cell 内に複数の Box を作成できる. それぞれの要素は URI で識別するが，Unit/Cell/Box という階層構造と URI のパス構造がマッチしていて，Web と相性がよい.
- **Web API**: 全機能を HTTP 上の REST スタイル API で提供している．このため，開発者は自由にプラットフォームや実装言語を選択できる．また，既存の Web サービスとの連携も容易になる.
- **認証・認可プロトコル**: PDS ごとにアカウント管理を行わず，Web の標準プロトコルである OAuth 2.0[15] を用いてユーザおよびアプリケーションを認証・認可する．また，各サブジェクトに割り当てたロールに基づくアクセス制御が可能である.
- **データの形式とアクセスプロトコル:** 構造型データは OData，非構造型データは WebDAV を用いてデータ操作を行う. これらは REST スタイル API で定義されたオープンな標準規格である．OData はリレーショナル型, WebDAV は階層ツリー型ディレクトリをデータモデルとしており, 多くのアプリケーションに必要十分なデータ格納機能といえる.

以上の特徴から，Personium は既に述べた PDS の機能要件を満たしているといえる．自己情報コントロールはオブジェクト階層と認証・認可プロトコルにより，データポータビリティは OData と WebDAV のサポートにより，ID 管理と認証・認可は OAuth のサポートとロールベースアクセス制御のサポートにより達成されている.

3. ヘルスケアアプリケーション

本章では，我々が開発するヘルスケアアプリケーションについて述べる．

3.1 データ収集方法とデータ種類

我々は，ヘルスケアデータの取得に iPhone と Apple Watch を用いた．これらのデバイスから取得可能なヘルスケアデータの種類と単位を表 1 に示す．これらのデータは iOS 8.0 および WatchOS 2.0 から導入された HealthKit フレームワーク[16]を利用して取得する．また，表 2 に示す個人の基本データを iPhone から取得して PDS に格納する．

表 1　ヘルスケアデータの種類と単位
Table 1　Kinds of and units of healthcare data

データの種類	単位
歩数†‡	歩
ウォーキング＋ランニングの距離†‡	km
上った階数†[1]	階
アクティブエネルギー‡	kcal
安静時消費エネルギー‡	kcal
スタンド時間‡	時間
エクササイズ時間‡	分
心拍数‡	拍/分
安静時心拍数‡	拍/分
歩行時平均心拍数‡	拍/分
心拍変動‡	ミリ秒

† iPhone で取得可能

‡ Apple Watch で取得可能

表 2　個人の基本属性データ
Table 2　Basic Personal Profile

取得可能なデータ
ID
名前
生年月日
性別
血液型
身長
体重

3.2 PDS へのヘルスケアデータの格納処理

デバイスで取得したヘルスケアデータを Personium に格納するまでの処理手順を示す［図 3］．Apple Watch で取得したデータは，同期している iPhone に自動的に送られ，iPhone 上のアプリから PDS に送信する．この iPhone 上のアプリをヘルスケアクライアントと呼ぶ．

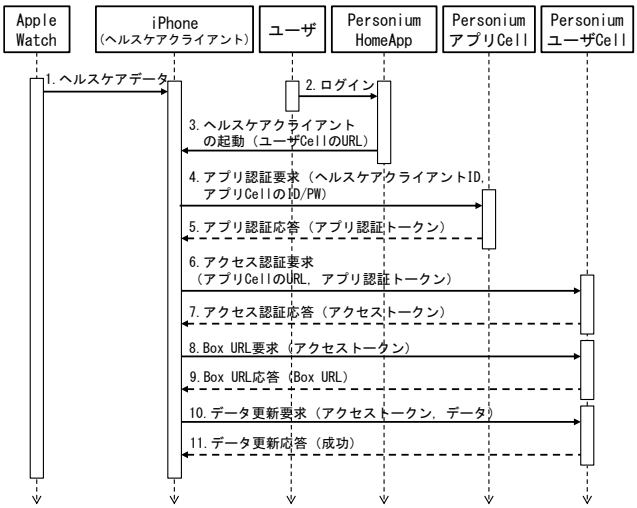

図 3: ヘルスケアデータを PDS に格納する手順
Figure 3: Sequence of storing health care data in PDS

紙幅の都合上，ユーザやアプリケーションの登録，Cell や Box の作成などの事前処理は省略する．

【データ格納手順】

(1) Apple Watch は，取得したヘルスケアデータを定期的に iPhone の iOS ヘルスケアアプリ専用データベース HealthKit に送信する．

(2) ユーザは，iPhone 上のブラウザ（Safari）で Personium の HomeApp にログインする．HomeApp は Personium のユーザアプリケーションを管理する組み込みアプリケーションである．

(3) HomeApp に登録されたヘルスケアサービスがヘルスケアクライアントを起動するとともに，ユーザ Cell の URL を渡す．この iOS アプリ起動処理は Safari を介して行う．このユーザ Cell にヘルスケアデータを格納する Box が配置されている．

(4) ヘルスケアクライアントは，Personium のアプリ認証を要求する．要求先は，アプリ認証を担当するアプリ Cell である．

(5) ヘルスケアクライアントが正当なアプリと認証されれば，アプリ Cell からアプリ認証トークンが返される．

(6) ヘルスケアクライアントは，3 で取得した URL を利用してユーザ Cell にアクセストークンを要求する．この時，5 で取得したアプリ認証トークンを提示することで，Personium の正当なユーザ・アプリからの要求であることが確認される．

(7) 正しいアクセス要求であることが確認できたら，ユーザ Cell セルからアクセストークンが返される．

(8) ヘルスケアクライアントは，ヘルスケアアプリ用 Box の URL を要求する．

1 iPhone の機種によっては取得できない場合もある．

(9) ユーザ Cell から Box の URL が返される.
(10) ヘルスケアクライアントは，Box にヘルスケアデータの格納を要求する. データフォーマットは OData にしたがい JSON 形式を用いる.
(11) データの格納処理が成功すれば，成功応答が返される.

3.3 グラフ化アプリケーション

もっとも基本的なアプリケーションがデータの可視化である．PDS に蓄積されたデータを読み出し，これをグラフ化して可視化する[図 4, 図 5]. 単体で利用する以外に，ユースケース１と２のようなアプリケーションの構成要素としても使える.

個人で利用する場合は，自分のヘルスケアデータの推移，目標値の達成状況などを確認できる［図 5］. コミュニティで利用する場合は，全体平均との差異や自分のランクなども確認できる．また，自己情報コントロールにより，特定の個人と相互にデータを見せ合い，比較する機能も実装予定である.

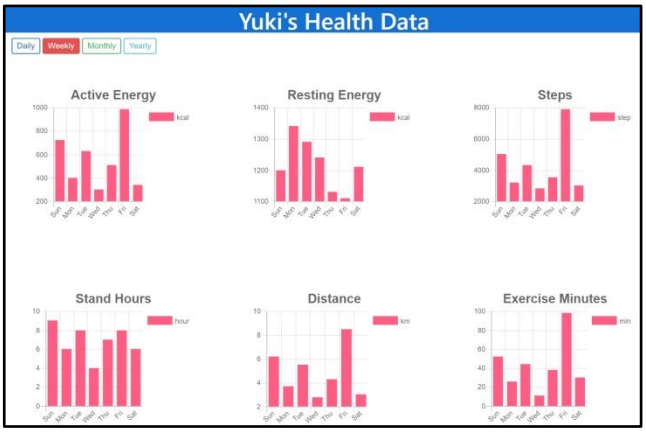

図 4: グラフ化アプリケーション（全体画面）
Figure 4: Grapher application (home view)

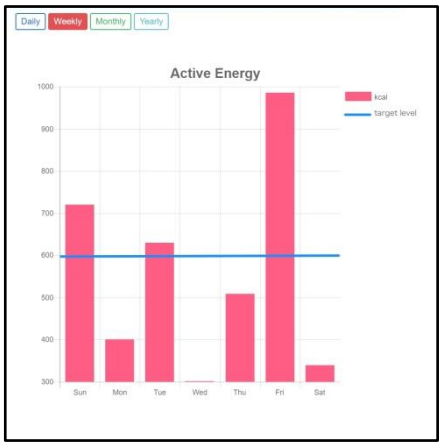

図 5: グラフアプリケーション（拡大画面）
Figure 5: Grapher application (magnified view)

3.4 リマインドボット

ユースケース２で述べたとおり，ボットの利用によりリマインドやアドバイスを自動化するアプリケーションをボットとして開発中である. 普及率の高い LINE と Slack をメッセージングの基盤として用いる.

リマインドボットの主な機能は，活動量の目標値に対する不足状況および目標達成の通知である．一部のデータ種類については iOS ヘルスケアアプリでも目標値設定ができるが，そうでない種類については本アプリケーションで設定する必要がある.

3.5 PDS からのヘルスケアデータの取得処理

先に述べたグラフ化アプリケーションを例に，PDS からのデータ取得手順を示す［図 6］. グラフ化アプリケーションは Web サーバに配備されており，ユーザは Web ブラウザからアプリケーションを利用する.

【データ取得手順】

(1) ユーザは Web ブラウザからグラフ化アプリケーションにログインする.
(2) グラフ化アプリケーションは，Personium の認証情報（ユーザ ID とパスワード）とユーザ Cell の URI を受け取る．続いてユーザ Cell 経由でアプリ Cell にアクセスしてアプリ認証を受ける.
(3) アプリ Cell は，正当なアプリであることを確認する.
(4) アプリ Cell は，ユーザ Cell 内のヘルスケア用 Box へのアクセスを許可し，アクセストークンを発行する.
(5) グラフ化アプリケーションは，アクセストークンを用いて Box にアクセスし，ヘルスケアデータを読み出す.
(6) グラフ化アプリケーションは，取得したデータからグラフを作成し，Web ブラウザでこれを描画する.

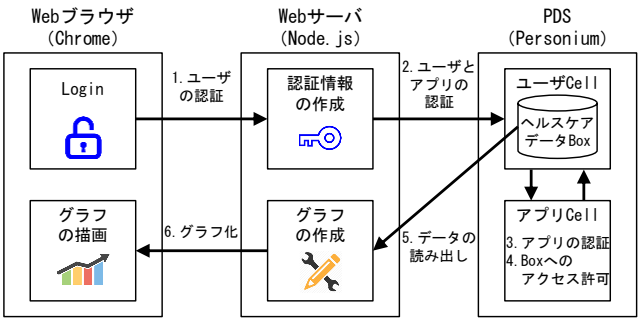

図 6:ヘルスケアデータを PDS から取得する手順
Figure 6: Sequence of fetching health care data from PDS

4. ゲームアプリケーションの構想

健康管理を目的とした運動や食事制限は継続することが難しい人もいる．この問題に対して，我々はゲーミフィケーション[12]の考え方を取り入れて解決を図ろうとしていることはユースケース３で述べた．参加者が健康づくりを楽しみながら継続できるようにすることが目的である．本章では，本研究で今後展開しようとしているヘルスケアのゲーム化について考察する．

4.1 参加者数

ゲームへの参加者数は，以下の２通りが考えられる．

- １人：個人が自分一人でゲームを楽しむ．
- 複数人：他者と順位やポイントを競う．

ここでは特に前者について考える．１人型は，育成ゲームや箱庭ゲームである．例としてたまごっちや SimCity などがある．最近は，ゲームの画面キャプチャを SNS に投稿するという楽しみ方もある．

ヘルスケアデータを共有することへの心理的障壁がある人に対しては，１人型ゲームが有効であろう．実装においては，前に述べたグラフアプリケーションやリマインドボットを組み合わせることができる．Apple Watch のエクササイズデータを利用した NIKE+[17]は，ゲームに加えてトレーナーやパートナーという要素も導入しており，参考になる好例といえる．

4.2 匿名と実名

ゲームに実名で参加するか匿名（ニックネームやハンドル名）で参加するかは，ゲームの種類や個人のポリシーで決められるべきである．家族やサークルなど特定のグループでは，実名での参加が適しているであろう．

我々のシステムでは iPhone から個人の名前などの基本情報を取得し PDS に登録する．Personium は，PDS の識別に URI を用い，PDS 内のデータも個別にアクセス制御できるので，匿名と実名のいずれでもデータ共有を実現するのは容易である．

4.3 参加者の多様性

活動量などは年齢，職業，趣味などによる個人差が大きい．例えば，家族では子供から老人までの年齢層があり，企業ではプログラマーと営業職では行動パターンが異なる．

PDS に蓄積されるヘルスケアデータをゲームに反映させる上で注意すべきことは，絶対値の単純なマッピングでは勝敗が固定化してしまうことである．多様な参加者で一つのゲームを楽しむには，データの正規化などを行い「がんばり」や「継続」を加点するなどの工夫が必要である．また，ボードゲームにおけるサイコロのように，「乱数」や「運」を導入することも有効であろう．

5. おわりに

本論文では，VRM の概念に基づくパーソナルデータの管理ツールである PDS のユースケースを示した．我々はヘルスケアを事例として PDS の研究・開発を進めており，ユースケースの分析とアプリケーションの開発を通して，PDS の機能要件や外部インタフェースの改善を図ることを目指している．

ウェアラブルデバイスから取得したヘルスケアデータを PDS で蓄積・管理し，自己情報コントロールに基づいて人やプログラムにアクセスを認可する．ここでは，Personium というオープンソース PDS を用いて，iPhone および Apple Watch からデータを収集して利用するヘルスケアアプリケーションついて述べた．パーソナルデータの自己情報コントロールやデータポータビリティの必要性と，Personium での実現の容易性を示した．

謝辞 本研究は，富士通研究所からの受託研究の成果である．研究の協力いただいた富士通研究所の石垣一司氏，富士通の下野暁生氏および Dixon Siu 氏に，謹んで感謝の意を表する．

参考文献

[1] 城田: パーソナルデータの衝撃，ダイヤモンド社, ISBN:978-4478064832, 2015.
[2] D. Searls: The Intention Economy: When Customers Take Charge, Harvard Business Review Press, ISBN:978-1422158524, 2012.
[3] Project VRM. http://cyber.harvard.edu/projectvrm/Main_Page
[4] T. Kirkham, S. Winfield, S. Ravet, S. Kellomäki: A personal data store for an Internet of Subjects, IEEE Int'l Conf. on Information Society (i-Society), 2011, pp.92-97.
[5] 下野，今林: 利用者データを中心とする新たな ICT の形, FUJITSU, Vol.64, No.1, 2013, pp.102-110.
[6] T. Kirkham, S. Winfield, S. Ravet, S. Kellomäki: The Personal Data Store Approach to Personal Data Security, IEEE Security and Privacy, Vol.11, No.5, 2013, pp.12-19.
[7] IoT 時代のプライバシーとイノベーションの両立，産業競争力懇談会 2016 年度プロジェクト最終報告, 2017. http://www.cocn.jp/thema95-L.pdf
[8] 石垣，下野: 共助と共創のためのプラットフォームコミュニティ型 PDS/情報銀行の構想，情報処理学会 情報システムと社会環境, Vol.2017-IS-142 No.1, pp.1-6, 2017 年.
[9] Y.-A. Montjoye, S. S. Wang, A. Pentland: On the Trusted Use of Large-Scale Personal Data, IEEE Data Engineering Bulletin, Vol.35, No.4, 2012, pp.5-8.
[10] PLR (Personal Life Repository). http://www.assemblogue.com/
[11] Personium. https://github.com/personium
[12] 井上: ゲーミフィケーション, NHK 出版, ISBN:978-4140815168, 2012.
[13] パーソナルデータを管理「Personium サービス」，富士通. http://jp.fujitsu.com/solutions/cloud/k5/function/paas/personium/
[14] The OAuth 2.0 Authorization Framework, RFC 6749, D. Hardt, Ed., 2012. https://tools.ietf.org/html/rfc6749
[15] Apple HealthKit. https://developer.apple.com/documentation/healthkit
[16] NIKE+. https://www.nike.com/jp/ja_jp/c/nike-plus