■題名：プライバシー保護機能を有したセキュア分散パーソナルデータプラットフォーム
“miParu”PDS
■副題：あらゆる健康データをスマホなどのエッジデバイスに貯めて多用途活用
■著者：南　重信
■所属：株式会社　ミルウス　代表取締役

1. はじめに

データは 21 世紀の石油といわれるほど、その重要性は高まっている。　特に個人に紐づけられたパーソナルデータは、本人の医療・健康だけでなく、匿名化・ビックデータ解析による製薬・治験・マーケティングなど幅広い応用が期待される。

一方、パーソナルデータはプライバシー性の高い情報であるため、その取り扱いには格段の配慮が必要であり、欧州の GDPR(EU 一般データ保護規則) や国内の改正個人情報保護法等を念頭に置いた活用が必要である。

パーソナル・データ・ストア(PDS)は、パーソナルデータを個人が管理する仕組みであり、GDPR や改正個人情報保護法のベースとなる本人承諾と整合性が高く、データを個人が預けて運用を信託する情報銀行も PDS の技術を採用している。

インターネットの世界も中央集権の Web2.0 から対等分散の Web3.0 に向けたパラダイムシフトが、既に始まっているのではとの意見もあり、個人が端末(Edge)で、分散管理する PDS は Web.3.0 時代の核技術となりうる。

株式会社ミルウスは、情報銀行がデータの銀行であるならば、日常生活においてパーソナルデータをプライバシーを保ちながら安全かつ機動的に活用する仕組みも必要ではないかと考え、データの財布の機能を Edge Device であるスマホ等に PDS として保管活用する Edge 型の分散 PDS に着目。　その具体的な実現として、”miParu”　PDS プラットフォームを開発・展開している。

2. PDS の概要

パーソナルデータの保管・活用形態は、サービス提供者がネットを介して取得したデータを自社のクラウドに保管し、サービスに用いるとともに、必要に応じて本人承諾の下、二次利用するのが現在の主流である。PDS でも情報銀行や PLR のようにパーソナルデータをクラウドに保管して個人がデータ運用を信託した銀行や個人がスマホのアプリで管理活用するのが Web2.0 時代の一般的なアプローチである。一方、Edge ベースの分散型 PDS は、個人のスマホに PDS を構築する(図 1)。

個人が管理する PDS もクラウドに集める情報銀行、管理だけスマホで行う PLR、スマホ上に PDS を構築する Edge 型分散 PDS 等のアプローチがあり、各々一長一短ある。

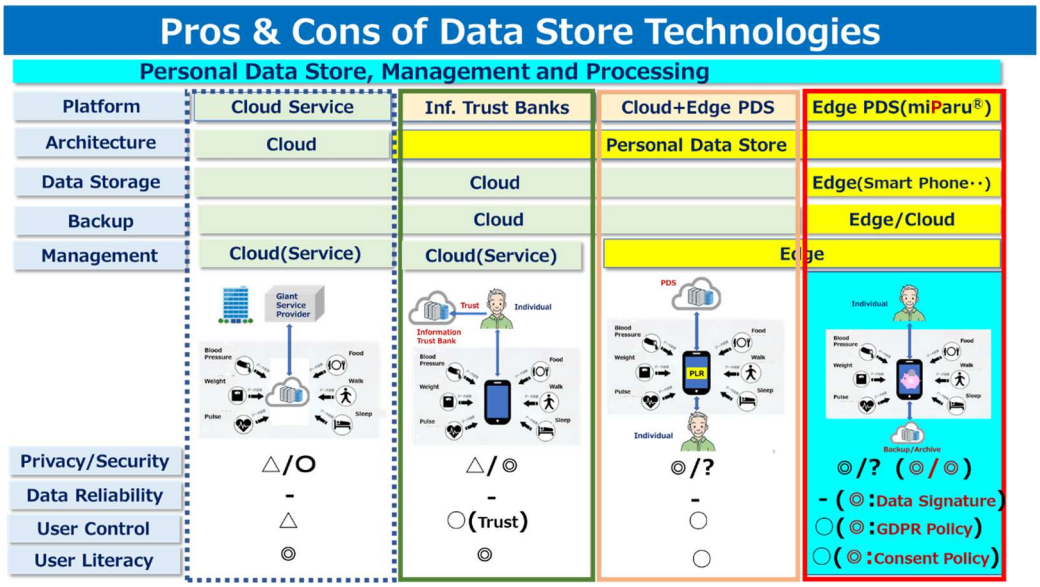


図 1. 従来型クラウドサービスと PDS の分類

情報銀行は多くの人の、パーソナル・データを預けるため、高度の信頼性が求められる、昨今、相次いで発生している情報流出や攻撃の格好のターゲットになる恐れは皆無ではない。また、預けてしまったパーソナルデータのコントロールは銀行に委ねられるため機動的な活用には向かない。一方、個人がいちいち自身のパーソナル・データの活用に関与する必要が無いため、特に IT リテラシの低い高齢者には優しいシステムと考えられる。

管理のみを分散化する PLR は、クラウド上にデータを保管するという意味では、情報銀行と同様の課題があるが、スマホ上で個人が管理するためテータの機動的な活用には適している。ただしデータ活用を虎児に委ねるため面倒さは残る。

データ保管と管理をスマホで行う分散型 PDS は、クラウド型ではないため、大量のデータを同時に流出したり、攻撃されるリスクは低い、また手元にデータがあるため機動的な活用や災害時などネットが使えない場合にもデータにアクセスできる利点がある。さらに、個人の手元に多様なデータを統合できるため、多様なクラウドに分散している本人のデータ統合がクラウド間の個別統合より容易化できる可能性もある。その反面、データと管理の両方が個人の裁量下に置かれるため、個人による改竄が行われたり、スマホを紛失するリスクは無視できない。また、PDS のサイズが大きくなった場合のオーバフロー対策も課題である。

3. セキュア分散 PDS “miParu®”

多くの利点があるデータ・管理分散型 PDS の課題解決を目指して、図 2 に示す、セキュア分散 PDS “miParu®”を開発している。同図に示すように、生活者や患者が取得した医療・健康データはカードやスマホ内で生成する本人固有の秘密鍵を用いたデジタル署名が施され、本人が承諾した閲覧者・データ利用者(ここでは医師と薬剤師)の公開鍵で暗号化され、パーソナル・データの保管期限、匿名再配布許諾などのデータ・コントロール情報を持った”miPari®”コンテナに搭載されて相手先の医師や薬剤師に配布される。

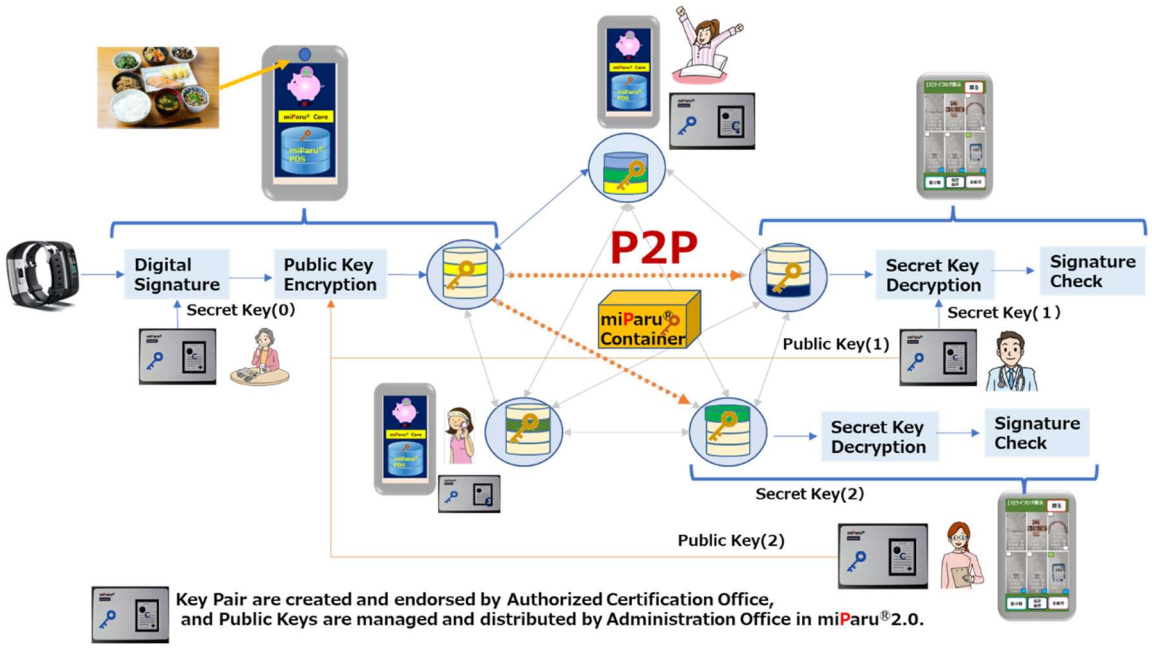


図 2 “miParu®”PDS の基本原理

分散 PDS の課題を解決する”miPari®”PDS の特徴を以下にまとめる。

(1)改竄抑止: 分散 PDS で Edge デバイスであるスマホを個人が所有し、管理が個人に委ねられるために改竄のリスクは避けられず、医療用途や将来のビックデータ用途でのデータ信頼性を損なう恐れがある。この課題に対応するため”miPari®”PDS では、パーソナルデータをスマホで取得した直後に日付・時間が付与されたデータに本人固有の秘密鍵でデジタル署名を付与する。 これにより改竄された場合は受信側で検出し、そのデータを排除することが可能となる。さらに署名によりデータのオーナーシップが明確となり、将来、パーソナルデータに資産価値を付与する事が可能となる。

(2) 流出抑止: 信頼性の高い大手での、個人情報流出事故が多発し、社会問題となっている。分散 PDS では、膨大なデータが同時に流出する危険は少ないが、個人管理となるため個人が穴となり情報流出が発生する恐れがある。クラウド社会においても情報流出は個人の過失や犯罪等に起因するケースが非常に高く、サーバ・クライアント間の機器の防御の上に、個人の責任を明確化して流出抑止することが有効であり、個人ベースの分散 PDS は、そのような視点からは適したシステムであると考えられる。 ”miPari®”PDS では、各個人にカードなどで付与された個人固有の秘密鍵を用いた公開鍵インフラ(PKI)手法を個人間に適用することにより、情報流出の穴を容易に特定可能とした責任明確化により、データ流出抑止を図る。 個人間の PKI を実現する Person to Person(P2P)システムである。

(3) データ制御: サービスと引き換えに複雑な本人同意説明を用いてパーソナルデータを収集する時代は終わりつつあり、丁寧で実効性の高い説明のもとに得られた本人同意の下にパーソナルデータを流通する時代が主流となりつつある。”miPari®”PDS では、GDPR のデータ制御理念を、サービス説明/本人同意説明とリンクしたデータ制御情報をパーソナルデータに付与した”miParu®”コンテナとして流通することにより実現する。本人同意はサービス毎の都度同意とし、パーソナルデータ収集を伴うサービスの目的、サービス期間、提供先での保管期限/消去要求対応、匿名化等の処理後データの再配布条件等を高齢者にも分かりやすく説明した上で、署名付本人同意をデータに付与、コン

テナに収容して配布する(図 3)。

これにより、分散 PDS の課題でもある、IT リテラシの低いユーザでも安全でプライバシー保護性の高いパーソナルデータ活用が可能となる。

図 4 に示す例では、パーソナルデータの秘匿レベルに応じたパーソナルデータの種別に応じたパケットをデータ制御情報を含むサービス定義書パケットに収容し、国際標準化の進んでいる IoT コンテナで配布する案である。

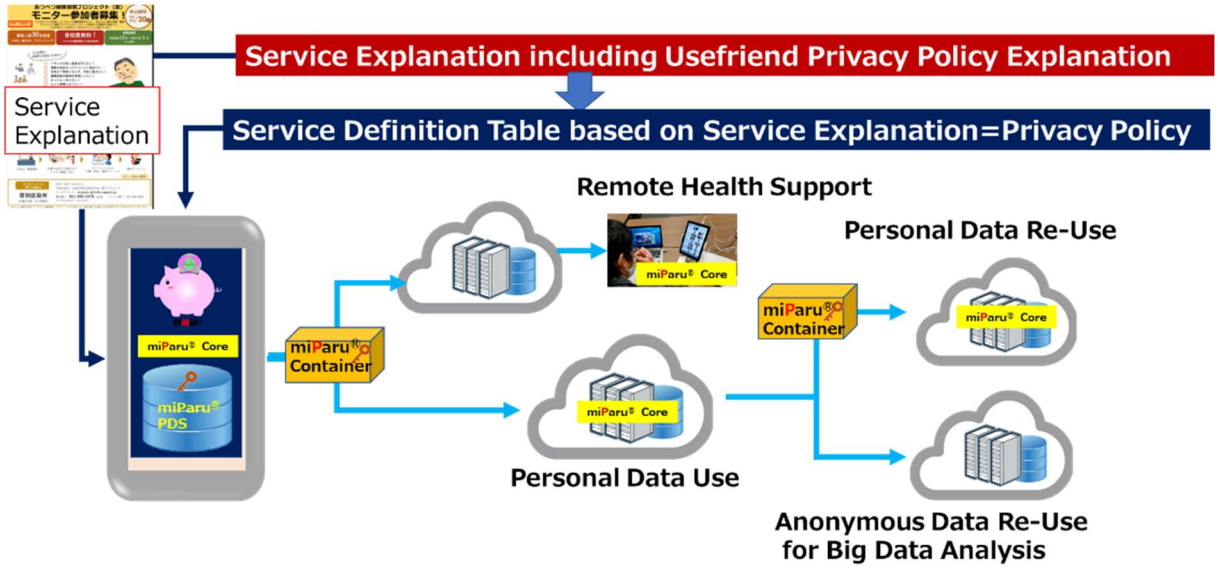


図 3 丁寧な説明とリンクした都度同意に基づいたパーソナルデータ制御の仕組み

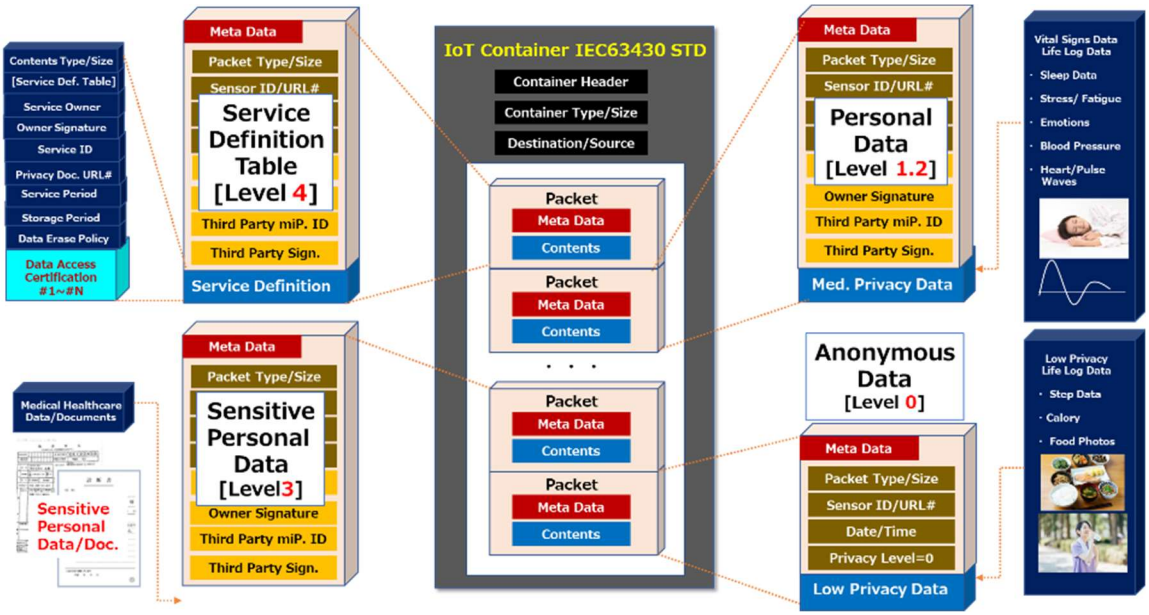


図 4　国際標準コンテナに収容する”miPari®”コンテナ案

(4) バックアップとアーカイブ: スマホの紛失/更新やメモリ容量の制約による PDS オーバフロー対策としてバックアップ/アーカイブ機能を提供する。”miPari®”PDS の特徴は暗号化したデータ保管先は HDD 等の個人の機器や汎用クラウド等、個人の裁量で選択できる点にある。　また、バックアップ/アーカイブ化するデータも選択可能であり、重要度の低いデータはバックアップしないという選択も可能となる。

4. ”miPari®”PDS の応用事例

プライバシーを保護したパーソナルデータを流通する”miPari®”PDS の応用範囲は広いが、コロナ禍の中で、リモート健康支援への期待は高い。　2020 年度に北海道で実施した実証試験では、約 100 名の住民や社員の参加の下、北海道郡部の住民の健康支援や札幌市内の住民や企業従業員を対象に札幌市の専門家がリモート健康支援を行った。

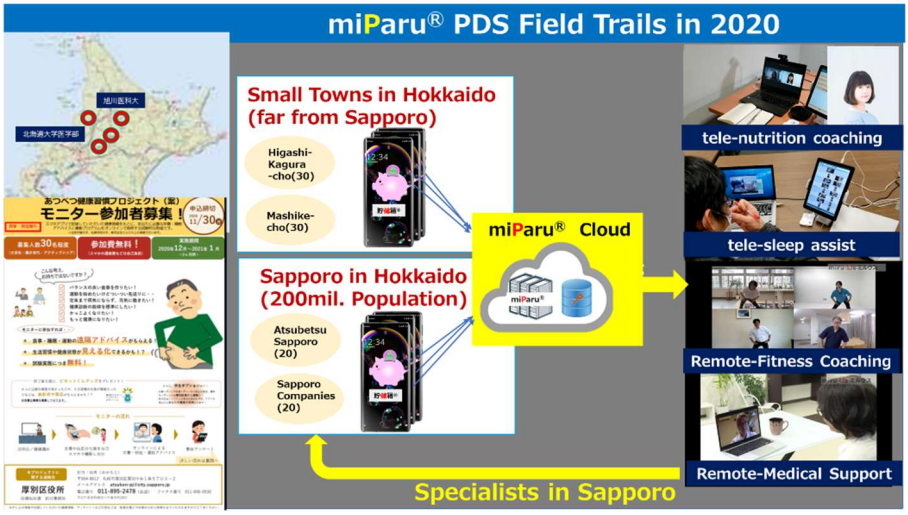


図 5 北海道実証試験の概要

北海道は札幌市・旭川市の専門家の豊富な大都市と広く分散した専門家の非常に少ない小規模自治体の二極構造になっており、また冬の積雪期には移動が困難になるなど、コロナ禍だけでなくリモート健康支援の必要性の高い地域である。

本実証では札幌市在住の管理栄養士、運動トレーナー、北海道大学の睡眠研究者(准教授)が約 1～2 週間の食事写真、行動記録(歩数/位置情報)、睡眠時間、血圧計表示写真、体重計表示写真を用いて、LINE のテレビ電話を用いたリモート食指指導、運動指導、睡眠指導を行った。これらの指導では、各線分野を超えたライフログを用いた指導ができ、指導者からは好評であった。　また、パーソナルデータの秘密鍵を有した専門家個人の閲覧者を限定することによるプライバシー性の高いシステムのため安心してパーソナルデータを低起用していただけた。

本実証では、これらの結果を匿名化し東北医科薬科大の医師が総合的な判断を行った。

被験者 255
血圧の推移

	朝			夕		
	sBP	dBP	P	sBP	dBP	P
10 月 27 日	117.5	76.5	58.5	113.5	66.5	90
28 日	113	71	61.5	122.5	78	65.5
29 日	121.5	77.5	62	119	74	78
30 日	116	75	58.5	112.5	72	73
31 日	111	70.5	79.5	103	63	101
11 月 1 日	119	76	71.5	120	73	80
12 月 7 日	124	81.5	59	121.5	70	61.5
8 日	127	77	61.5	122	75	60
9 日	128	78	65.5	125.5	81.5	60
10 日	122.5	67.5	62.5	121	76	66
11 日	121	77	61	119	63	76.5
12 日	115	72	67	113	70.5	74
13 日	128.5	80.5	62.5	123	64	70.5
平均	120.3077	75.38462	63.88462	118.1154	71.26923	73.53846

表 1. 実証試験に於いて血圧計表示写真から得た血圧値例

医師のコメント例:

・血圧は全て正常値内にあり安定した推移をしています。

・食事は、3 食とも緑黄色野菜、糖質・脂質・タンパク質のバランスが取れています。

・睡眠時間の平均は6 時間です。睡眠時間が4 時間の日があり、疲労回復のために十分な睡眠時間を取るように心がけて下さい

本実証では、パーソナルデータを用いた非匿名支援と、医師による住民全体の傾向を把握する匿名データ活用を実施し、パーソナルデータの、きめ細やかなコントロール補可能に”miPeau®”PDSのメリットを明確化することかできた。

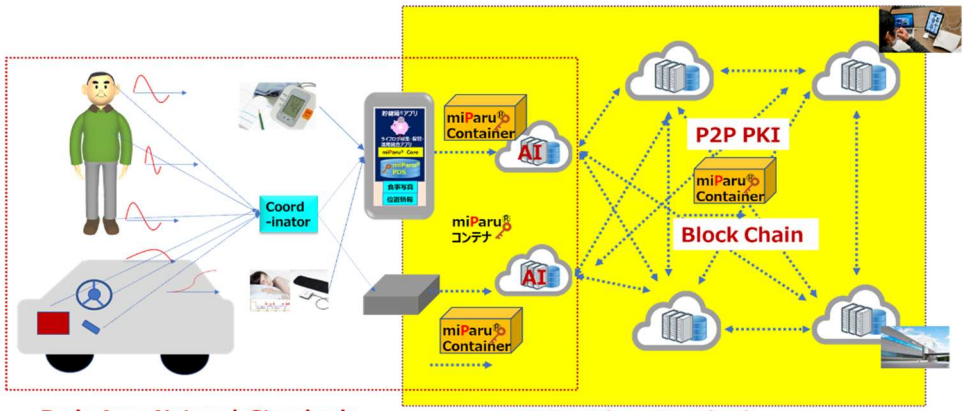
4. 今後の展開

(株)ミルウスが描く Web3.0 時代の平等・フェアで分散化されたパーソナルデータ流通社会では(図 6)、国際標準化が進んでいるボディエリアネットワーク等で得られた、人だけでなく車や家電機器等の多様なボディに装着されたセンサからのデータが有機的に統合され、あたかも一つの仮想バイタルセンサとしてサイバー空間で定義され、人々は特に意識することなくプライバシー保護や流出を抑止して、自身の健康医療に活用するだけでなく、匿名利用を行うサイトに提供しポイントを得る等でメリットを実感できると期待する。また、パーソナルデータの取得提供記録(台帳)である健康情報通帳®も、ブロックチェーン技術により多様なサービス提供者で対等かつ真正性を有して、に分散共有することにより、真に分散・対等なパーソナルデータ流通網が実現すると考える。

このような社会の実現には、オープンなプラットフォームで互換性の高いパーソナルデータの流通が必須であり、BAN や IoT コンテナの国際標準化等とも連携しながら、”miPeau®”PDS の開発・事業展開を推進する。

Final Goal @2024 WEB 3.0 World

miruWs® 3.0: Integrated Vital Signs Sensor for Any BODY
miParu® 3.0: Secure Distributed Personal Data Store Platform



Body Area Network Standards
(BLE/Dependable BAN / Smart BAN等)

IoT Container Standards
(ISO/IEC)