Trusted Web の実現に向けたユースケース実証事業
最終報告書　詳細版

下肢運動器疾患患者と医師、研究者間の信用できる
歩行データ認証・流通システム

2024 年 3 月 15 日
株式会社 ORPHE

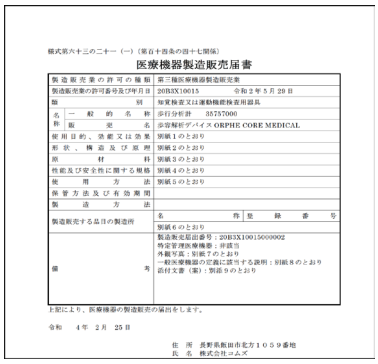
目次

1. 背景と目的

1.1 背景・目的

株式会社 ORPHE（以下、当社）は歩容解析（歩行速度、歩幅、着地角度、着地衝撃といった様々な歩行の特徴値の解析）を可能とする靴型のウェアラブルインタフェース（以下：スマートフットウェア）の研究開発を行っており、近年はスマートフットウェアを変形性膝関節症（以下：膝 OA）などの下肢運動器疾患のアセスメントに応用する研究も行っている。また医療現場での活用を進めるため一般医療機器（医療機器クラス１）にあたる歩行分析計と対応アプリケーションの開発を進めている。

図 1-1-1：ORPHE FOOTWEAR EASYRUN SHIBUYA
（3.0 ソール部に ORPHE CORE センサを内蔵可能）



様式第六十三の二十一（一）（第百十四条の四十七関係）

医療機器製造販売届書

製造販売業の許可の種類		第三種医療機器製造販売業
製造販売業の許可番号及び年月日		20B3X10015　　令和３年５月２９日
類別		知覚検査又は運動機能検査用器具
名称	一般的名称	歩行分析計　　38757000
	販売名	歩容解析デバイス ORPHE CORE MEDICAL
使用目的、効能又は効果		別紙１のとおり
形状、構造及び原理		別紙２のとおり
原材料		別紙３のとおり
性能及び安全性に関する規格		別紙４のとおり
使用方法		別紙５のとおり
保管方法及び有効期間		
製造方法		
製造販売する品目の製造所		名称　　登録番号 別紙６のとおり
備考		製造販売届出番号：20B3X10015000002 特定管理医療機器：非該当 外観写真：別紙７のとおり 一般医療機器の定義に該当する説明：別紙８のとおり 添付文書（案）：別紙９のとおり

上記により、医療機器の製造販売の届出をします。

令和　４年　２月　２５日

住所　長野県飯田市北方１０５９番地
氏名　株式会社ロムズ

図 2-1-2：ORPHE CORE MEDICAL[1]

膝 OA は国内で自覚症状のある人だけでも 1,000 万人以上という非常に多い疾患の一つで、歩行が妨げられるため患者の運動能力や QOL に大きな影響を与える。膝の痛みを恐れて外出することが怖くなり、結果として筋力低下を招き転倒率を上げてしまうといった悪循環は非常に多くみられる。この様な状況でセンサデータとアプリケーションを活用し、自分のデータや他の人のデータに基づいて適切な歩行動作や適切な歩数を AI が提案することで症状が改善することができれば、多くの人の健康寿命を伸ばすことに直結すると考えられる。

[1] 2022 年 12 月より販売開始。歩行分析計として第三種医療機器製造販売業許可を持つ提携企業が独立行政法人医薬品医療機器総合機構（PMDA）に医療機器製造販売届書を申請済。

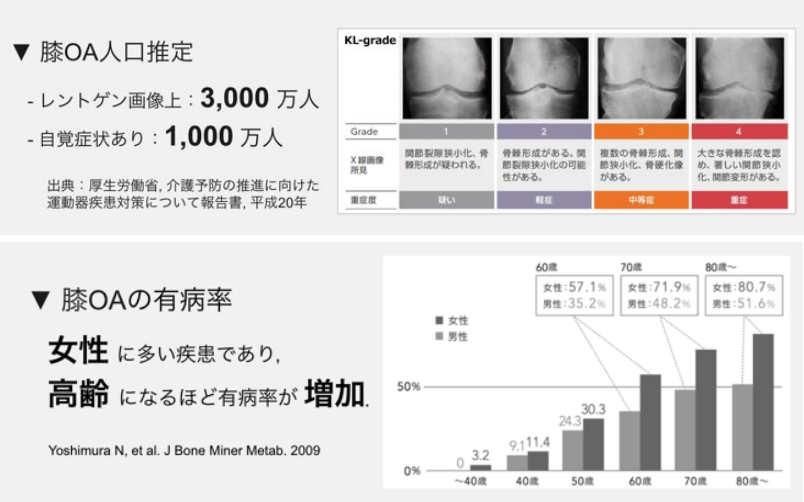


図 1-1-3：膝 OA に関する背景

下肢運動器疾患のアセスメントにおいて歩行分析は重要で、例えば人工膝関節置換術（膝 OA の治療法の 1 つ）では、8 割以上の医療機関において歩行分析を含むリハビリプロトコルが設定されている[2]。一方で現状の臨床現場では目視による定性的な動作分析が多く行われており、ストップウォッチを使ったタイム計測や動画撮影が主に行われていて、歩行についての詳細な分析がデータとして蓄積されていない現状がある。これまでも歩行分析計に区分される医療機器は販売されているものの、ほとんどが 80 万円以上など高価であることと時間が限られるリハビリの現場で使いやすく設計されてないといった問題があり日常的な臨床の現場で用いられている件数は少なかった。この様な背景から患者の歩行データを蓄積する意義は感じられていても、臨床の現場で効率的に蓄積する手段がなかったと言える。またさらには患者の日常生活における実際の歩行については臨床現場からアクセスする手段はなかったと考えられる。

また、データを取得できたとしても、個人情報保護の観点からそのデータを第三者に共有し活用することは難しいという現状がある。当社はこれまでの研究開発の中で様々な研究機関、臨床機関と相談しデータを取得し解析することを行ってきたが、研究目的に応じて同意を取り、データを取得するこの様な研究には非常にリソースがかかっている。もし患者の日常生活におけるデータ、臨床における診察のデータなどが患者のダイナミックな同意に基づいて活用可能であれば、世界中の歩行研究が一気に加速すると考えられる。

この様な背景から、下肢運動器疾患を患う患者の日常的な歩行データ等の生体データとアンケート等の主観的な記録データを、ウェアラブルセンサとスマートフォンアプリを用いて記録可能とし、データの拠出に紐づけてポイント（トークン）を発行するシステムの必要性を感じた。またそのデータを医師や研究者、製薬会社が患者の認証を得た上で活用可能とするシステムの構築を行うことで、歩行研究や歩行に関する治療法の開発を加速するとともに、データ提供者にインセンティブを与えるための費用を拠出する

[2] 飛山 義憲ら, 人工膝関節置換術前後のリハビリテーションプロトコルの実施状況と内容に関する全国調査, 理学療法学, 2021, 48 巻, 4 号

ことができると考えた。

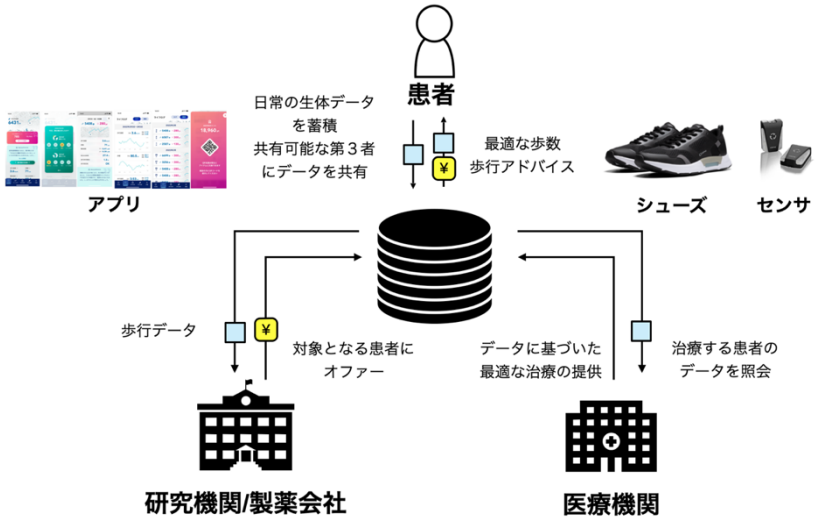


図 1-1-4：事業スキーム

以上の背景から当社は「令和４年度 Trusted Web の実現に向けたユースケース実証事業」に応募し、デジタルウォレットや VC（Verifiable Credential）を活用した下肢運動器疾患患者と医師、研究者間の信用できる歩行データ流通システムのプロトタイプを開発した。

図 1-1-5：事業スキーム開発した患者向けアプリケーションの UI 画像

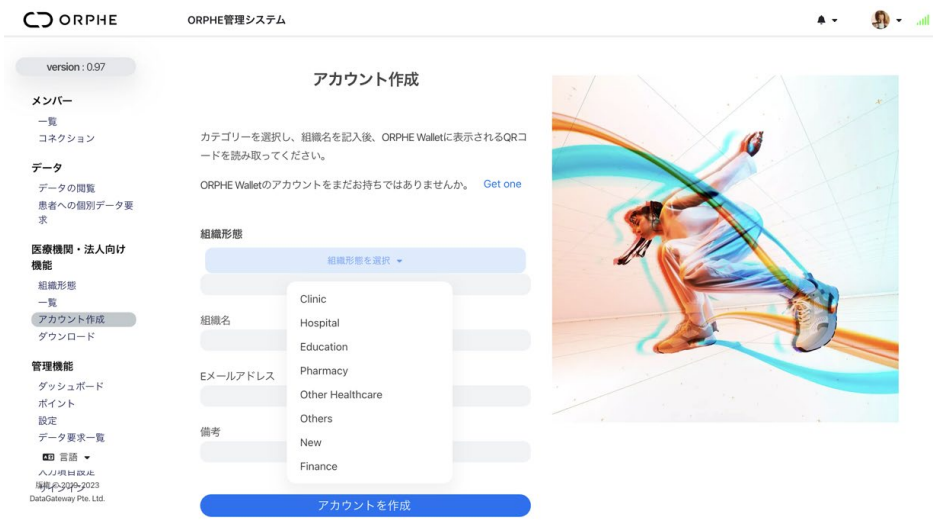


図 1-1-6：開発した医療機関･研究機関向け web アプリケーションのアカウント作成画像

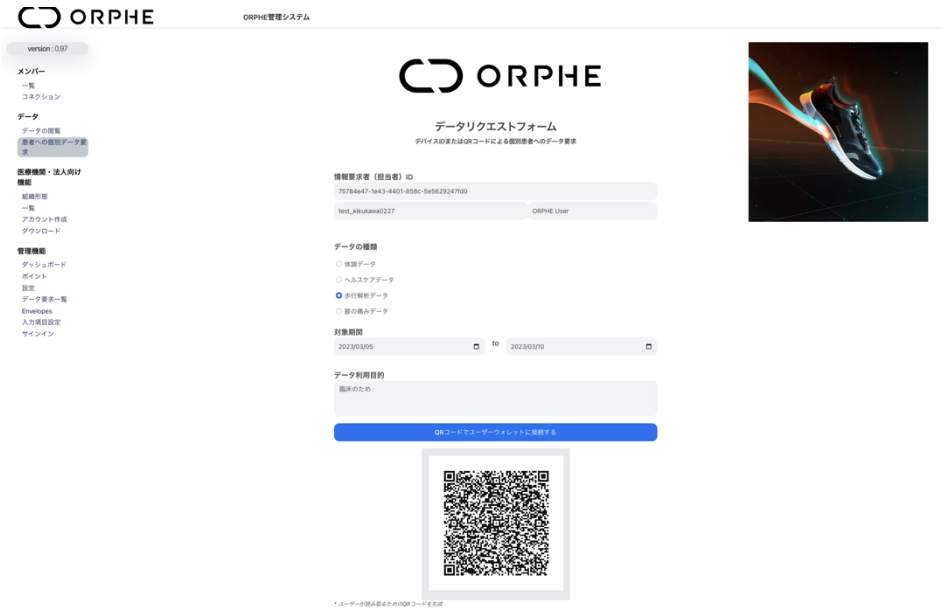


図 1-1-7：開発した医療機関･研究機関向け web アプリケーションの
データリクエストフォーム画像

また、下肢運動器系疾患を患う患者 4 名に対してスマートシューズの貸し出しと開発したプロトタイプシステム（アプリケーション）の配布を行い、それぞれ 10 日間以上アプリを使用してもらう実証実験を行った。またシステムの有用性について医師 2 名、理学療法士 2 名、製薬会社 1 社の新規事業企画担当者 1 名に対してヒアリングを実施した。

令和 4 年度の実証事業を通じて、下肢運動器疾患患者と医師、研究者間の信用できる歩行データ流通システムの基礎的な要素は完成した。以下に、開発したプロトタイプシステムで解決可能な課題を整理した。

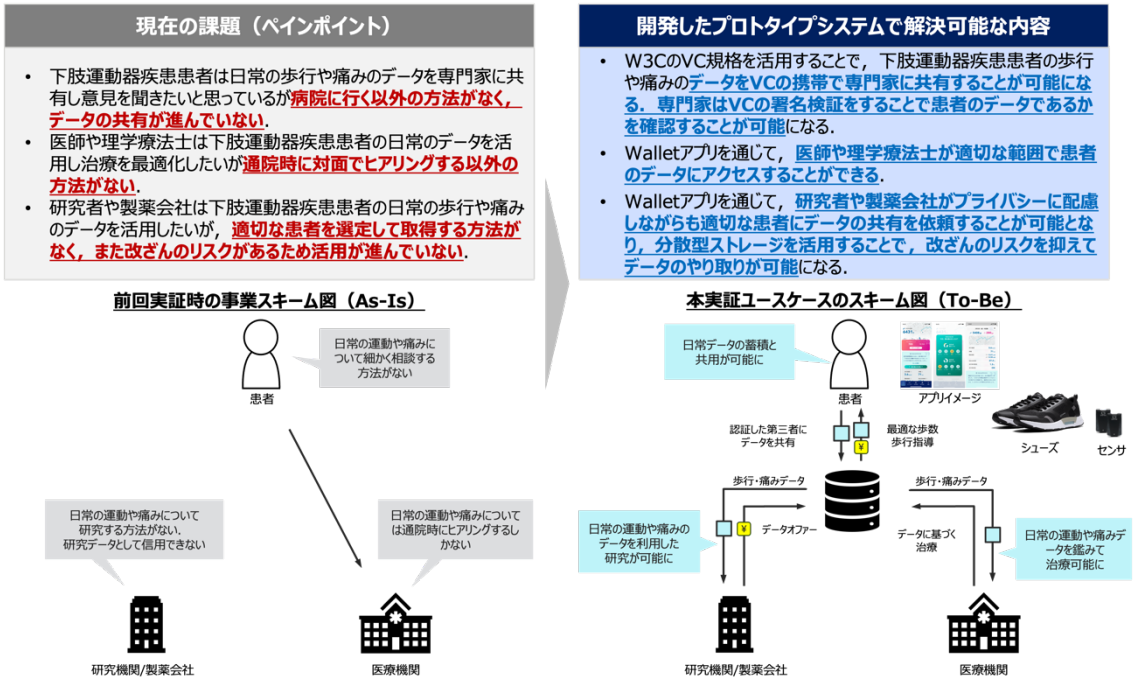


図 1-1-7：事業スキーム図（R4 年度の成果概要を当社にて修正）

開発したシステムを社会実装する上では、以下のような課題が残っていると認識している。

本人のデータであることの証明について、前回の実装では本人のスマートフォンで記録している限り本人のものであるという前提に基づいて実装しているが、実証実験では家族がスマートフォンを使用している間に歩数が記録されたというケースが見られ、本人のデータであることの検証方法に課題があることが確認された。本人のデータであることの証明が不完全のままデータの共有が行われてしまうと、医師や研究機関の診断・治験の精度にも影響し、ビジネスモデルとして機能しなくなる恐れがある。

製薬会社等に対する昨年度のヒアリングからは、提供されるデータの定量的価値まで算定するに至らなかった。社会実装を進めるためには、データの信頼性を担保することの価値を含めたマネタイズモデル（データに基づいて拠出するトークンをベースとしたエコノミクス）を設計する必要がある。

上記の残課題の解決に向けて、本実証事業においては以下の内容を実施する。

データ記録の際に顔認証や歩容認証等の強固な本人確認技術を活用することで、可能な限り本人のデータであることが検証可能なシステムを実装する。

可能な限りユーザによるデータの主体的管理権限を保ちながら、データの共有に対して出資する研究機関/製薬機関の経済的合理性も確保できるような仕組みの検討と実装を行う。特にデータ共有取り消し要求の際のポイント返戻システムの実装と、共有の取り消し要求に対応できる仕組みについて再検討を行い、新たなシステムを実装する。具体的には取り消し要求の期限を設定することが効果的か検証を行いたい。また、ポイント返戻にあたっては、ポイント（トークン）をパブリックチェーン上で扱う場合にはプラットフォーム内でのポイント付与とトークンへの反映タイミングをズラし、ポイント使用直前に付与することで

データの取り消しした際にポイントの返戻可能とすることや、ポイントを使用した時点でデータの取り消し要求をできなくするなどの実例について検証を行う。

プロトタイプシステムを用いたユーザビリティテストを実施し、各ユーザ（患者、医師、研究機関等）のインセンティブを踏まえて事業スキームやシステムの再検討を行うことで、トークンエコノミーの構築およびデータの利用の促進を図る。具体的には、NFT（非代替性トークン）によって歩行の改善や運動の継続を証明するなど、健康やデータの共有による社会的貢献と紐づいたインセンティブ設計を行うことで、実証終了後にできる限りそのまま実社会で活用できるレベルのシステム（アプリケーション）の構築を目指す。

DCT の実用化に求められるセンサデータとしての要件を、同様の取組を推進しているシミック株式会社へのヒアリング等を通じて検討し、ヒアリング結果を踏まえて可能な範囲でシステムに機能実装することでデータの価値を向上させる。

2. 事業の概要

2.1 登場する主体と概要

本事業に登場する主体は開発システムの提供者、患者、医師/理学療法士、研究機関/製薬会社である。各主体間におけるサービスやキャッシュのフローは図 2-1-1 の通りである。

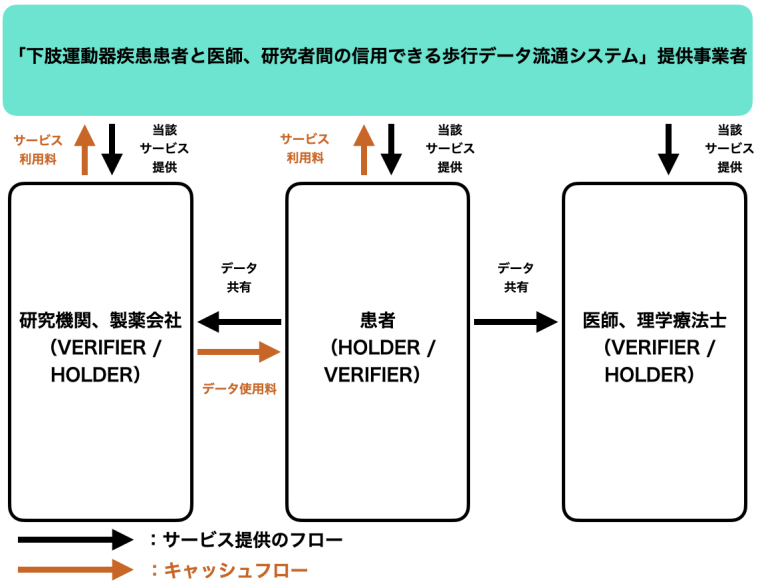


図 2-1-1：登場する主体と概要

各主体の設定と役割および令和 3 年度補正予算 Trusted Web 共同開発支援事業費「Trusted Web の実現に向けたユースケース実証事業」を通して明らかになったものを含む現状の課題を以下の表 2-1-1 に整理した。

表 2-1-1：現状の課題特定①

主体（組織・個人）	設定・役割
患者	**設定：**下肢運動器疾患を持つ患者。日常生活の中で自分に最適な歩数やリハビリを知りたいと考えている。 **役割：**日常生活の中でスマートフットウェアを履いて歩行を行い、記録されたデータを、スマートフォンアプリを通じて蓄積する。また第 3 者からデータ共有のオファーが行われた際に、自分のかかりつけ医であることや、信用できる研究機関、製薬会社であること等を検証し、共有可能な相手であればアプリ上で共有の承認を行う。 **課題：** 1. 日常生活の中で最適な歩数や歩行動作を知りたい。 2. 適切な対象に適切な範囲で自分のデータを共有したい。 3. 継続利用やデータ共有のインセンティブが十分設計されていない。
医療機関	**設定：**整形外科の病院。患者の日常の歩行や主観的な痛みの記録を活用し、最適な治療を提供したいと考えている。

	役割：対象患者のデータを、API を通じて取得し、データに応じた最適な治療を提供する。 **課題：** 1. 患者の日常のデータを把握して治療を最適化させたい。
研究機関/ 製薬会社等	**設定：**下肢運動器疾患の研究や新薬、新医療機器の開発をしたい。 **役割：**研究対象となる患者に問い合わせを行い、取得するデータに応じたポイント（トークン）を購入し、データの取得を行う。 **課題：** 1. 適切な対象の日常の歩行データを集めたい。 2. 無数に集まるデータが研究に扱うデータとして適切か、改ざんされていないか確認できない。 3. センサデータが本人の物であることを確認できない。 4. 共有の取り消しの際のポイントの返戻システムなど、ユーザのデータの主体的管理権限と研究機関/製薬機関にとって魅力的なトークンエコノミーの両立ができていない。

2.2 現状の課題を解決する事業スキーム案

表 2-1-1 に整理した現在の課題、および本実証実験で実現を目指す課題とスキーム図を図 2-2-1 にまとめた。

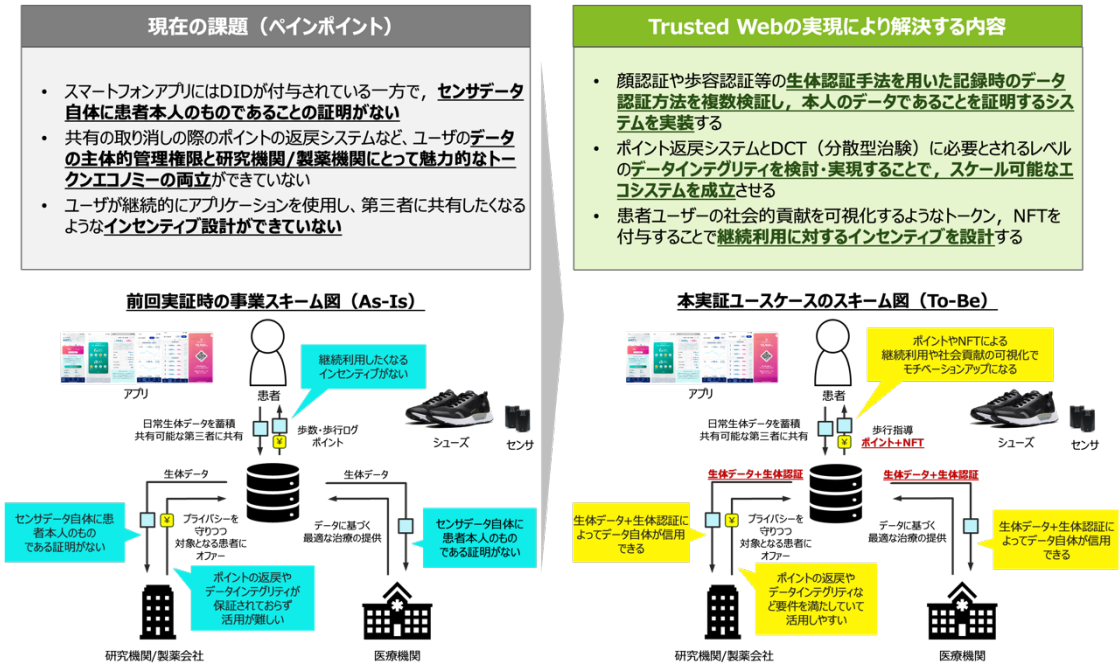


図 2-2-1：事業スキーム図

表 2-2-1：現状の課題特定②

課題の対象	解決すべき課題	Trusted Web システムによって解決できること
患者	日常生活の中で最適な歩数や歩行動作を知りたい	Trusted Web システムを通して多くの患者データが蓄積され機械学習などの解析が進むことで、自分に近い症例における最適な行動が見つかるなど精度の高いレコメンドが可能となる。
	適切な対象に適切な範囲で自分のデータを共有したい	証明されたデータ要求者に承認した範囲のデータ共有を行うことで、属性情報の開示範囲やアクセスをコントロールすることで課題解決に資する。また、提供した属性情報が合意した範囲（期間、提供先）において取り扱われているかを追跡できることで、情報管理をゆだねることなく主体的に行うことが可能。そして自分のデータの開示範囲（データの種類、期間）に伴ってポイントの形でインセンティブを得ることができる。

課題の対象	解決すべき課題	Trusted Web システムによって 解決できること
	継続利用やデータ共有のインセンティブが十分設計されていない	患者ユーザの社会的貢献を可視化するようなトークン、NFT を付与することで**継続利用に対するインセンティブを設計**する。 この様なインセンティブが設計されることでデータの蓄積が進み、それによってデータの共有も増すため、Trusted Web の社会実装が広がることとなる。
医療機関	患者の日常のデータを把握して治療を最適化させたい	Web 上のシステムを通じてデータ共有の要求を行い、承認を得た患者の日常における歩行データや痛みのデータにアクセスし、最適な治療の検討や術前術後の変化等をデータで確認することができる。
研究機関/ 製薬会社等	適切な対象の日常の歩行データを集めたい	Web 上のシステムを通じてデータ共有の要求を行い、承認を得た患者の日常における歩行データや痛みのデータにアクセスし、最適な治療の検討や術前術後の変化等をデータで確認することができる。
	無数に集まるデータが研究に扱うデータとして適切か、改ざんされていないか確認できない	ブロックチェーンを活用したデータの管理や本人確認を組み合わせることで無数に集まるデータに信用が付与され、活用可能となる。
	センサデータが本人のものであることを確認できない	顔認証や歩容認証等の生体認証手法を用いた記録時のデータ認証方法を複数検証し、本人のデータであることを証明するシステムを実装する。これによってデータの信頼できる領域が拡大し、Trusted Web によってデータの価値が向上しエコシステムが構築できる。
	共有の取り消しの際のポイントの返戻システムなど、ユーザのデータの主体的管理権限と研究機関/製薬機関にとって魅力的なトークン	ポイント返戻システムと DCT（分散型治験）に必要とされるレベルのデータインテグリティを検討・実現することで、スケール可能なエコシステムを成立させる。これによって遠隔で取得された生体データも信用することが可能となり、Trusted Web によっ

課題の対象	解決すべき課題	Trusted Web システムによって 解決できること
	エコノミーの両立ができていない	てデータの価値が向上しエコシステムが構築できる。

2.3 社会・経済に与える影響・価値

変形性膝関節症の患者数について、自覚症状を有する者は約 1,000 万人、潜在的な患者（X 線診断による患者数）は約 3,000 万人と推定されている（図 2-2-1）。重症の変形性膝関節症では、関節変形、運動痛および可動域制限等により起立歩行に支障が生じる [3]。

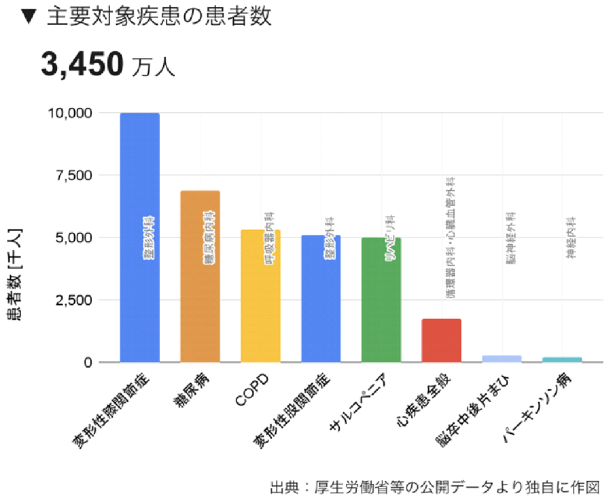


図 2-3-1：主要対象疾患の患者数

変形性関節症治療薬の世界市場規模は 2021 年で 74 ドル、2026 年に 112 億ドル、市場の平均年成長率は 8.6%で推移する見込みであり，高齢者人口の増加、変形性関節症の罹患率の上昇、低侵襲手術の需要の増加が、変形性関節症治療薬市場の成長要因となっている [4]。

本ユースケースは変形性関節症を中心とした下肢運動器疾患に悩む患者の日常生活において適切な歩行を行いたい、医療機関の適切な指導をしたいという要求を叶えつつ、研究機関への情報提供を可能とすることで加速度的に治療法の発見、医療機器の開発、製薬といった活動を進捗させることを可能とする。歩行は変形性関節症に限らず糖尿病、サルコペニア、脳卒中後片麻痺、パーキンソン病など様々な疾患と関連があり（図 2-3-1）、この様なシステムが社会実装されることで多くの疾患への研究開発が進む可能性があり、ほぼ全ての人類の歩行寿命、健康寿命を延ばすことに貢献できると考えている。

[3] 厚生労働省.「介護予防の推進に向けた運動器疾患対策について報告書」.
https://www.mhlw.go.jp/shingi/2008/07/dl/s0701-5a.pdf

[4] BCC Research.「変形性関節症治療：世界市場 2026 年予測」.

また分散型治験（DCT）は新型コロナウイルスの感染拡大を背景に欧米で実施例が増える中、日本でも規制に見直しが行われるなど注目の高まっている技術である。スマートシューズから得られる歩行データが活用可能になった場合の経済的価値について、日本ではまだ DCT の実施例が少ないため経済効果の算定は難しいが、いくつかの側面から経済効果を考察することができる。

- 低コスト化：分散型治験は、従来の臨床試験に比べてコストが低く抑えられることが期待される。これは、物理的な試験施設や人件費の削減、データ収集と管理の効率化、治験参加者へのリクルートメントやフォローアップの簡素化などが要因となる。
- 治験のスピードアップ：DCT はリモート環境で行われるため、治験の開始から結果の取得までの期間を短縮できる可能性がある。これにより、新薬の承認や市場投入までの期間が短縮され、関連産業におけるイノベーションの促進や競争力の向上が期待されます。また当社の提案するシステムでは個人が日常的に蓄積しているデータを共有可能とするため、さらなるスピードアップが期待できる。
- 参加者の多様性の拡大：DCT は地理的な制約が少ないため、幅広い地域や人口層からの参加者を集めやすくなる。これにより、治験の結果の信頼性や適用範囲が向上し、より多くの患者に適切な治療法が提供されることが期待される。
- データ活用の促進：DCT ではリアルタイムで大量のデータが収集されるため、データ解析や AI 技術を活用した新たな治療法や薬物開発の可能性が広がる。

このように DCT の採用が進むことで、製薬業界だけでなく、医療業界全体や関連産業にも大きなインパクトを与えると期待される。現在でも、下肢運動器系疾患の遠隔リハビリの市場規模は、変形性膝関節症に対する人工関節置換術が年間 8.5 万件、前十字靭帯再建術が年間 1.5 万件、半月板損傷術が年間 5 万件程度実施されており、対象となる国内患者数は 142,000 人/年にのぼっている [5]。

[5] 第 7 回 NDB オープンデータ，厚生労働省.
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000177221_00011.html

2.4 ペイン・ゲインの整理（Value Proposition Canvas）

Value Proposition Canvas による顧客セグメント整理と、本事業が顧客に提供できる価値を整理した。

初期的には、患者が取得/入力したデータを主体的に管理しつつ、信頼できる形で、医師や企業に共有できる仕組みと、データ共有に対してインセンティブが発生するシステムを確立する。中長期的には、データの価値の最適化を行い、多くの患者がデータを生み出しつつ、企業/研究者が実際に利活用できるようなエコシステムの確立を目指す。

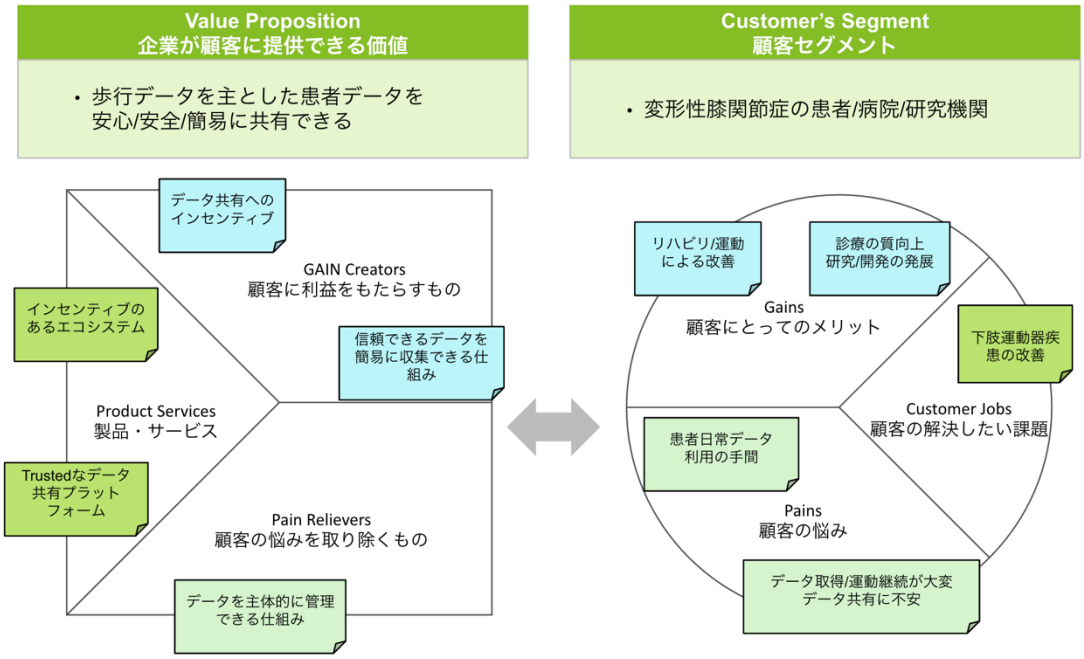


図 2-4-1：Value Proposition Canvas

3. 本実証事業における検証計画

3.1 事業実証で明らかにする論点への導出・経緯

本実証事業で明らかにする論点について、ビジネスモデル、UI/UX、アーキテクチャ、データ保護、ガバナンスの観点で以下のように整理した。

ビジネスモデルについては、1）どのようなビジネスモデルにすべきか、2）データ利用者が必要とするサンプルサイズはどれくらいか、について明らかにすることとした。1）はサービス提供者、患者、医療機関、研究機関/製薬企業と多くのステークホルダが参加するエコシステムにおいて各者の観点で納得できるビジネスモデルであることが必要であるため、患者ユーザへの実証実験後のヒアリング、医療提供者/データ利用企業へのヒアリングを通して検証する。また、海外で成功した PHR を取り扱うサービスモデルケースを選定し、デスクトップ調査を行うこととした。2）は、データ利用企業へのヒアリングを実施した。

UI/UX については、1）生体認証フローをどうすべきか、2）データ共有の同意取得の仕様をどのようにすべきか、3）ポイント返戻/同意撤回のルールはどのようにすべきか、4）ユーザビリティのネックになるポイントはどこか、について検討することとした。1）はデータが本人のものであることの信頼性を高める目的で生体認証を導入するが、繰り返しの実施によってユーザビリティを損なわないデザインが必要であると考え、web wallet の仕様を考慮し、最適なフローについて検討する。2）は患者のユーザビリティとデータ利用者のユーザビリティを両立させるための使用が必要であるため、同意画面に必要な要素の検討と実装を行い、ユーザヒアリングを行うこととした。3）はデータを利用する企業の経済的合理性を担保するためポイント返戻機能を必要とするが、患者観点から同意撤回の仕様について検討する必要があると考え、実現可能な仕組みについて検討する。4）は、開発したアプリの改善点を抽出するため、実際にアプリを利用したユーザにヒアリングを実施することとした。

アーキテクチャについては、１）アカウント復旧のフローをどのようにすべきか、２）顔認証にどのサービス/パッケージを利用すべきか、３）歩容認証の技術選定と実装の検討、４）どのパブリックブロックチェーンを利用するか、を論点とした。１）は、DID・web wallet の利用におけるアカウントの復旧手段のセキュリティとユーザビリティの両立は技術的にも課題と考えているため、今回は生体認証の利用を含めた多要素認証によるパスワードリセットおよびデバイス紛失時のアカウント復旧オプションを複数検討することとした。２）は、生体認証の実装に顔認証を活用することを想定しており、要件の整理と各種候補の比較検討を実施することとした。３）は、スマートシューズから取得された歩行データの認証手段の一つとして歩容認証の導入を検討するが技術的に完成したサービスが存在しないため、調査が必要と考え、本システムに適応可能な技術を選考文献調査から選定し、既存データへの適応結果をもとに実装の有無を決定する。４）は、前回実証からトランザクション速度の低さによる処理待ちが明らかになったため、再度利用するパブリックブロックチェーンについて検討することとした。

データ保護については、１）データ混入に有効な認証方法は何か、診療情報の真正性をどのように保つか、を論点とした。１）は、データの利活用を推進する上で、不適切なデータの混入はサービスの信頼性を損ねることになりうるし、不正なデータ生成による不正なポイント取得はエコシステムの崩壊を招く可能性があるため、不正なデータの混入を防ぐ必要があると考え、データフロー、ステークホルダの整理、企業へのヒアリングを通して、本システムに最適な認証方法について検討することとした。２）はデータを利活用した研究開発時に診療ラベルの真正性が重要になるため、データ登録フロー検討および診療情報取り扱いにかかるルールの調査を実施することとした。

ガバナンスについては、1） PHR を取り扱うサービスにおける規約や技術標準はどのようなものか、2）本システムにおいて必要な各ステークホルダに必要なガバナンスは何か、を論点とした。1）は、個人情報やヘルスケアデータを扱うサービスにおける規約などを参考に本サービスの規約を作成する必要があると考え、パーソナルデータを取り扱う国内外のサービスについて提供会社、サービス開始時期、サービス内容などの調査し、調査したサービスのうち比較的長期間サービス提供を継続できているサービスについて 3 つの論点（ビジネスモデル、サービス環境、トラスト）で深掘り調査・分析を行うことで、それぞれ ORPHE のサービス等と比較をしてユースケースの改善・社会実装に向けて有益となり得る示唆の検討を行うこととした。2）は、本サービスの釈迦実装する上で各ステークホルダにかかるガバナンスを整理する必要があるため、ステークホルダ毎にサービス利用におけるプロセスを整理し、必要な技術および規約について検討を進めることとした。

3.2 本事業におけるスコープ

本事業では患者が取得/入力したデータを自身のコントロールのもとで医療機関/研究機関に共有し、歩行に関するデータの利活用が促進されるシステムを構築する。特に前年度の実証で構築したシステムをもとにさらに以下の点を追加した新規なシステムを開発し、そのフィージビリティについて検証する。

- 生体認証を用いて、取得したデータが本人のものであることの信頼性を向上する仕組みを導入する。
- ポイント返戻機能の実装や臨床試験に活用しやすいようなデータインテグリティやデータやり取りのシステムに調査・検討し、システムへ実装する。
- ポイントや NFT の導入によって、患者が継続利用や健康増進に求められる行動の実施を可視化・促進する機能の開発を行う。

ただし、開発システムのサービス化は次の段階であるため実証実験後のアプリやトークンの一般公開は本事業のスコープ外とする。また分散型臨床試験（DCT）に必要とされるデバイスの要件についても調査し可能な範囲で実装を試みるが、本事業の期間内で実現することが困難なことも見込まれる。特にハードウェアやファームウェアレイヤーの改修についてはスコープ外として、アプリケーションやソフトウェアレベルでの改修を主なスコープとする。

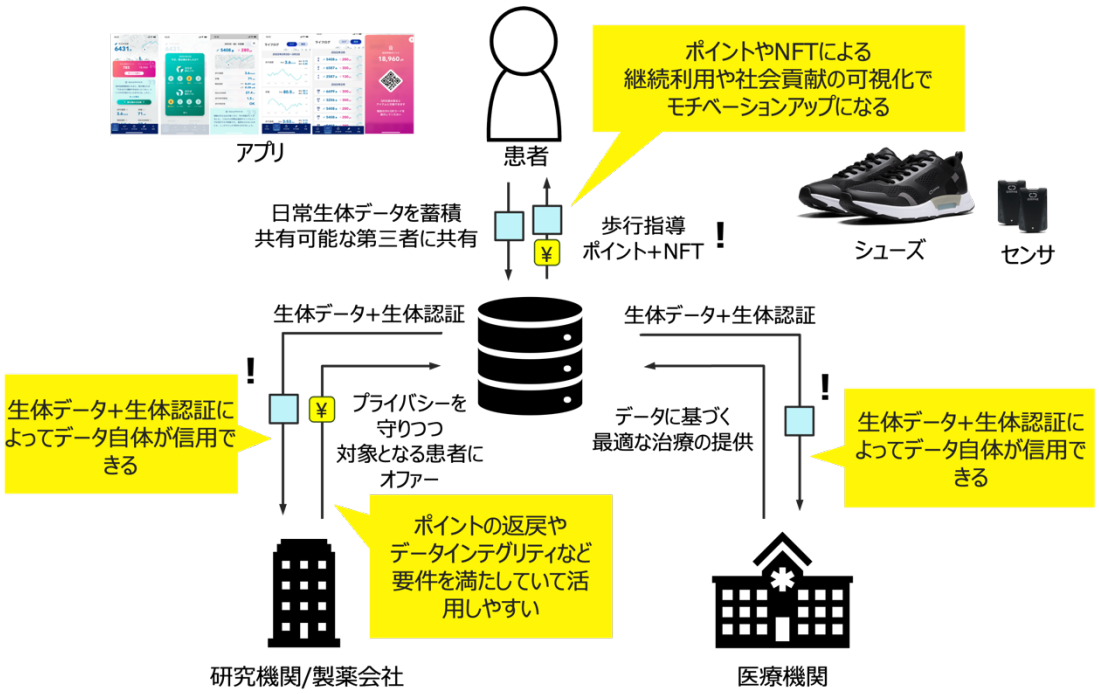


図 3-2-1：本実証ユースケースのスキーム図

3.3 実施事項・成果物一覧

本実証事業での実施事項は大きく 5 つに類型化でき、①実証ユースケースに関わるステークホルダ調整、②プロトタイプシステム開発、③実証実験の実施、④必要なルール・ガバナンス整理、⑤報告書取りまとめとした。

1　実証ユースケースに関わるステークホルダ調整

(1) 実証参加者調整・説明会参加（ORPHE 社）

実証実験実施のために、実証実験協力者（大阪大学大学院医学系研究科：医師・理学療法士）に対して説明会を実施。協力内容について、「説明会資料」を用いて、認識のすり合わせを行う。リクルートされた患者に対して、実証実験趣旨の説明などを行う。

2　プロトタイプシステム開発

(1) 技術調査（歩容認証）・実装

歩容データから歩容認証を行うアルゴリズムについての調査と実装可能性の検証、実装を行う。

(2) 業務・システム要件定義

ユースケースをもとに業務要件・システム要件を定義する。

(3) 開発（アプリ・インフラ）

ORPHE 社がシステム要件をもとにモバイルアプリを開発する。

(4) 開発（ウォレット・web アプリケーション）

システム要件をもとに DataGateway 社が開発を行う。

(5) アプリテスト

テストケースを作成、ORPHE 社がアプリ・システムのテストを実施する。

3　実証実験の実施

(1) 実証実験

下肢運動器疾患患者のユースケースについて医療機関の協力のもと実証実験を実施した。

(2) デモ動画作成

実証実験で利用するアプリの動作をデモ動画として整理する。

(3) 利用者ヒアリング

実証実験に参加した患者ユーザにヒアリングを実施する。

4　必要なルール・がバンス整理

(1) 調査

DCT にセンサデータを活用するための要件やガイドラインについて調査を実施する。

(2) 取りまとめ

(3) ルール・ガバナンス案の提示。

5　報告書の取りまとめ

(1) 実証結果分析

論点について検証を解した結果の分析を実施する。

(2) Trusted web の実現に向けた示唆提言の整理

(3) 最終成果報告書作成

開発アプリ・アンケート・検証結果分析等の取りまとめを行う。

表 3-3-1：成果物一覧

実施項目		具体的な作業内容	担当（会社名）	想定成果物
実施計画書作成・契約締結		実証ユースケース・開発システムの合意・詳細スケジュール・作業スコープの合意・契約金額の合意	ORPHE 社	実施計画書 契約書
実証ユースケースに関わるステークホルダ調整	実証参加者調整・説明会実施	実証協力事業者に対して説明会の実施、協力内容について認識すり合わせを行う	ORPHE 社	説明会資料
	実証参加者との契約・合意	実証協力事業者に対して同意契約を締結	ORPHE 社	協業契約書
	実証マニュアル作成	アプリ利用のマニュアルを作成し、実証参加者に説明	ORPHE 社	実証マニュアル
プロトタイプシステム開発	技術調査（歩容認証）・実	歩容データから歩容認証を行うアルゴリズムについての調査と実装	ORPHE 社	-

	装			
	技術調査（ウォレット）・実装	データ使用の取り消し機能を備えたウォレットについての技術調査と実装	DataGateway 社	-
	業務・システム要件定義	ユースケースをもとにビジネス要件を定義、上記ビジネス要件をもとにシステム要件定義	ORPHE 社	業務フロー 画面遷移図 機能一覧 システム構成図
	開発（アプリ・インフラ）	システム要件定義をもとに開発	ORPHE 社	アプリ・システム
	開発（インフラ・ウォレット）	システム要件定義をもとに開発	DataGateway 社	アプリ・システム
	単体テスト・結合テスト	テストケース策定のもとテスト実施	ORPHE 社	テスト結果
実証実験の実施	実証実験	下肢運動器系疾患患者のユースケースについて医療機関の協力のもと実証実験実施	ORPHE 社 大阪大学大学院医学系研究科スポーツ医学教室	実証実験結果
	動画撮影	実証実験の様子・アプリ利用の様子を動画撮影	ORPHE 社	動画
	利用者アンケート	アプリを利用したステークホルダに対して、アンケートを実施	ORPHE 社	アンケート
必要なルール・ガバナンス整理	調査	DCT（分散型治験）にセンサデータを活用するための要件やガイドラインについて調査	ORPHE 社	調査結果
	取りまとめ、ルール・ガバナンス案の提示	検証論点・調査をインプットにあるべきルール・ガバナンス案の提示	ORPHE 社	あるべきルール・ガバナンス（案）
報告書 取りまとめ	実証結果分析	事前に定義した論点の検証結果分析	ORPHE 社	論点検証結果
	Trusted web の実現に向けた	Trusted web の実現に向けた示唆提言の整理	NTT データ経営研	-

	示唆提言の整理			
	最終報告書作成	開発アプリ・アンケート・調査・検証結果分析等の取りまとめ	NTT データ経営研	最終報告書

3.4 実施スケジュール

3.4.1 全体スケジュール

本事業における各種実施スケジュールは以下の通りである。

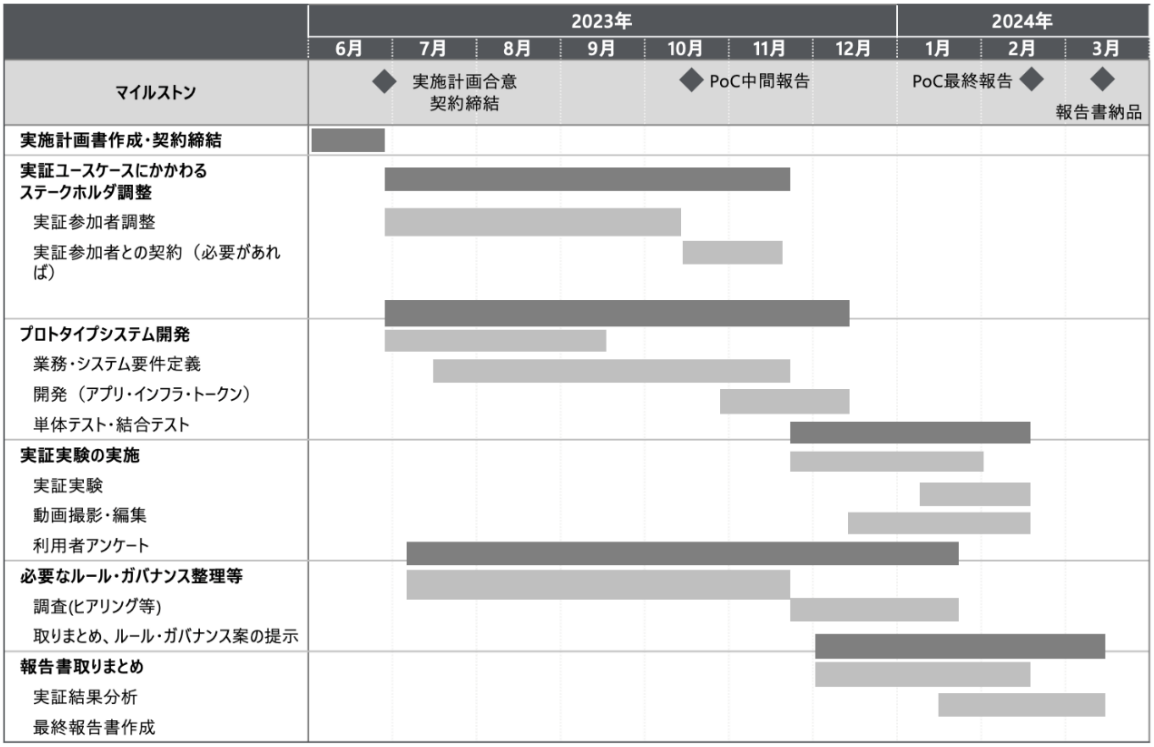


図 3-4-1：全体スケジュール

3.4.2　成果物の作成フロー

本実証事業における各種成果物の作成フローは以下の通りである。

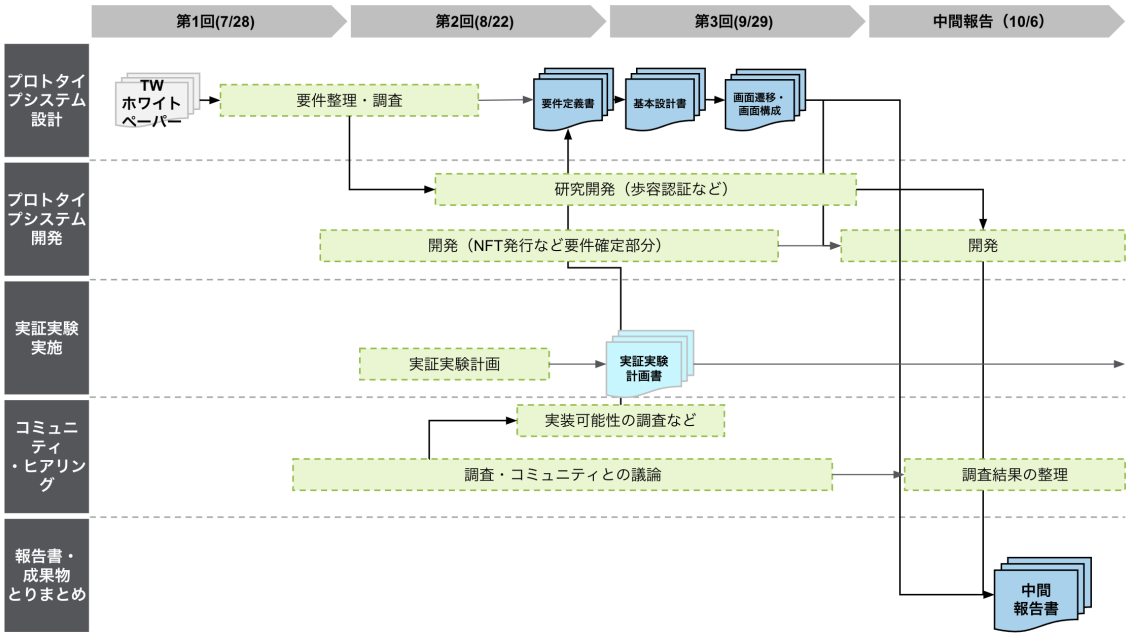


図 3-4-2(a)：成果物作成フロー(前半)

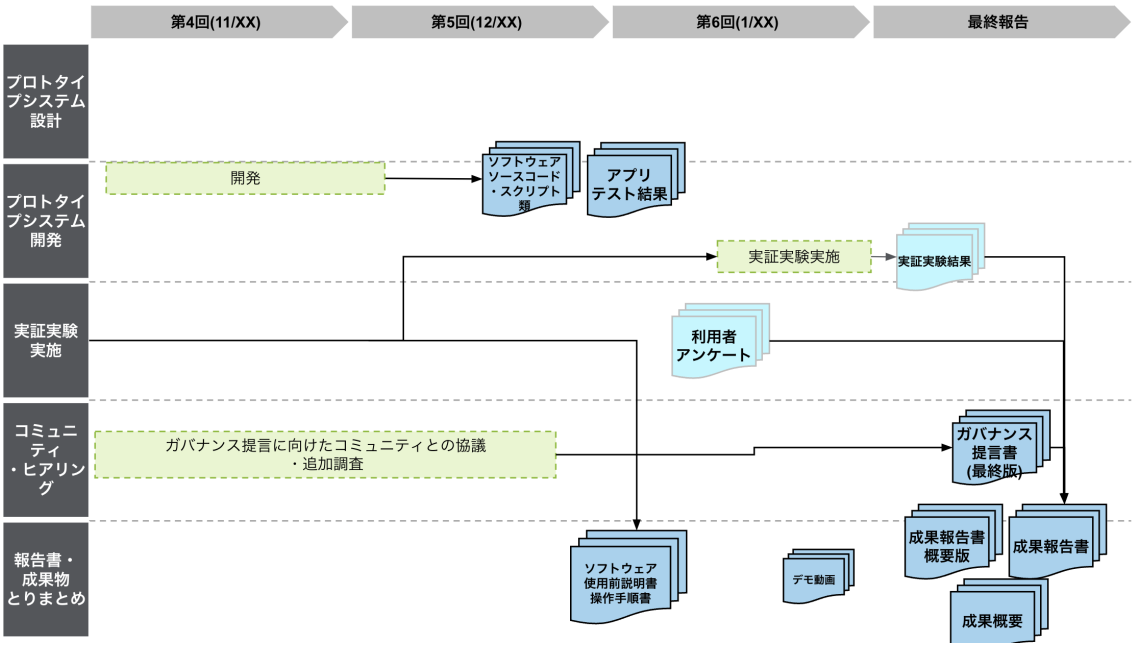


図 3-4-2(b)：成果物作成フロー(後半)

3.5 実施体制

本実証事業は、株式会社 ORPHE、DataGateway Pte. Ltd.、株式会社 NTT データ経営研究所の３社で取り組む。DataGateway Pte. Ltd.は、主にシステムの要件検討やバックエンドの実装の役割を担う。株式会社 NTT データ経営研究所は、主に事例調査および本開発システムの要件やガバナンス設計の検討を担う。

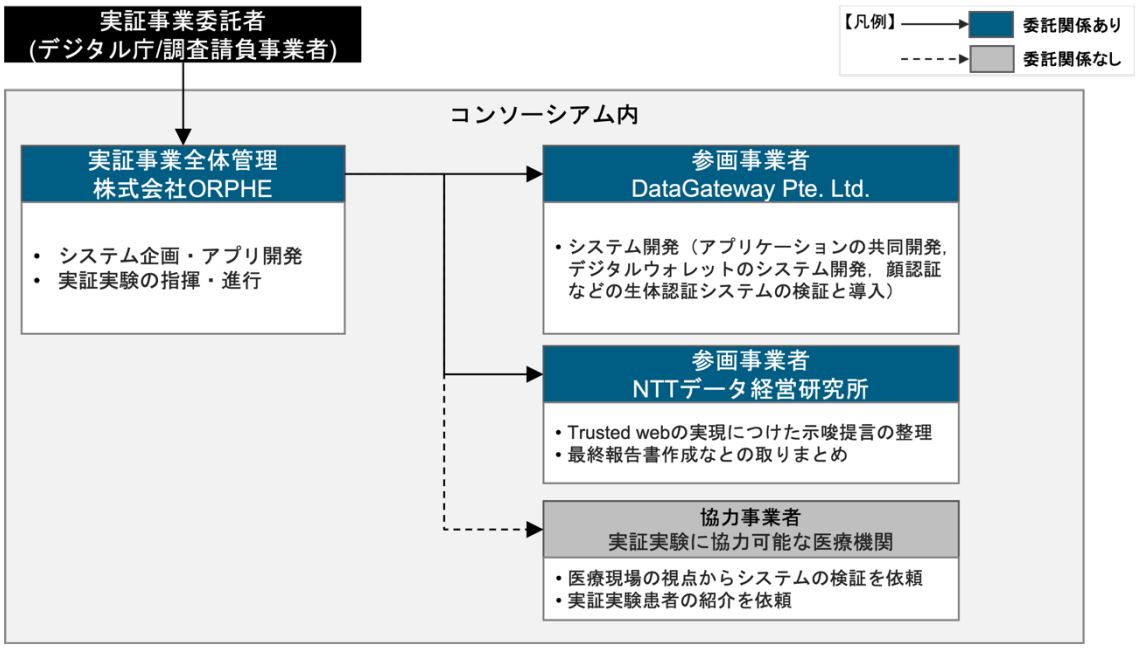


図 3-5-1：実施体制

4. 実証検証（企画・プロトタイプ開発）

4.1 実施概要

4.1.1 企画・プロトタイプ開発で明らかにする論点とその結果

企画・プロトタイプ開発で明らかにする論点としては、1）顔認証パッケージの選定、2）生体認証のフロー、3）歩容認証技術の選定、4）歩容認証のモバイルアプリへの実装の可否、5）本ユースケースにおいて歩容認証機能を実装するか、6）アカウント/パスワード/秘密鍵の復旧手段の検討、7）利用するパブリックブロックチェーン、とした。

1）顔認証パッケージの選定

本システムでは、データがユーザ本人のものであることの信頼性の向上を図るため、生体認証を実装することとした。また、生体認証を活用することで、アカウント復旧時の要素認証の候補となることも期待された。

まず個人の顔特徴量データを用いて個人認証が可能な NEC 社が開発する顔認証サービスについて導入の検討を行った。本サービスは、認証精度が高く、個別の認証が可能であることから秘密鍵復旧のオプションとして活用可能というメリットがあり、ユーザビリティとアプリの操作煩雑性を低減できることが期待された。一方、検討の中で、個人判別可能な特徴量データをどこに保存するべきかという議論が挙がり、秘密鍵復旧時に活用するには外部ストレージに保存しておく必要があるが、アプリ利用をするにあたり顔特徴量を外部ストレージへ保存することを強制する形になるため、データの主体的なコントロールのコンフリクトが生じることが懸念された。実際には、同社の技術の提供時期の問題によって、本実証実験におけるシステムへの実装は見送ることとなった。

上記懸念も含めて個別顔認証の実装が困難であると判断したため、改めて顔認証に求める要件を整理した。アプリ起動時における顔認証による本人の認証は、アプリ利用者の本人性の向上に資するが、当初解決を図っていた他人がデバイスを保持することにカウントされてしまう歩数の混入防止には効果を発揮しないことが明確になった。そのため、特別高い認証精度や個人認証までの機能を必要とせず、標準的な本人認証を行う顔認証技術で要件を満たすとした。候補となる顔認証実装手法として、3rd party 製サービス（Luxand）および OS 標準搭載パッケージの比較検討を行った。3rd party 製サービスは、精度が高いと謳われていることや複数アカウントの作成が可能であったものの、特徴量保存が行バになること、実装コストが比較的高いこと、サービス利用料がかかることなどが確認された。一方、OS 標準の顔認証（iOS の FaceID）でも、十分であると想定される誤認率（100 万分の 1 以下）であり、実装コストが比較的低い、サービス料がかからない、OIDC でのパスキー実装が容易であること、ユーザが慣れ親しんでいるなどのメリットが考えられたため、OS 標準の顔認証メソッド（Face ID）を活用することとした。

2）生体認証のフローをどのようにすべきか

本システムでは、データが本人のものであることをより担保するため、アカウントログインに生体認証（顔認証）を利用することとした。Woollet（web wallet）の認証（woollet auth）に生体認証が実装されるが、データ計測/入力時においても同等の認証・セキュリティレベルが望ましいことから、アプリ起動時（woollet 以外の機能利用時）にも生体認証を必要とした。生体認証を何度も実施すること

は、ユーザビリティの損失につながることが懸念されたため、アプリケーション利用時に要求される認証を全て woollet auth に集約することとし、アプリを起動した時点で woollet auth に遷移し、生体認証によるログインを実施することで、woollet と同等のセキュリティレベルをアプリ全体で担保できるようにした。認証結果は JWT token として発行し、API を経由してアプリ側にも共有することで、認証後一定期間は再度の認証を不要とした。詳細なフローについては以下に示す。

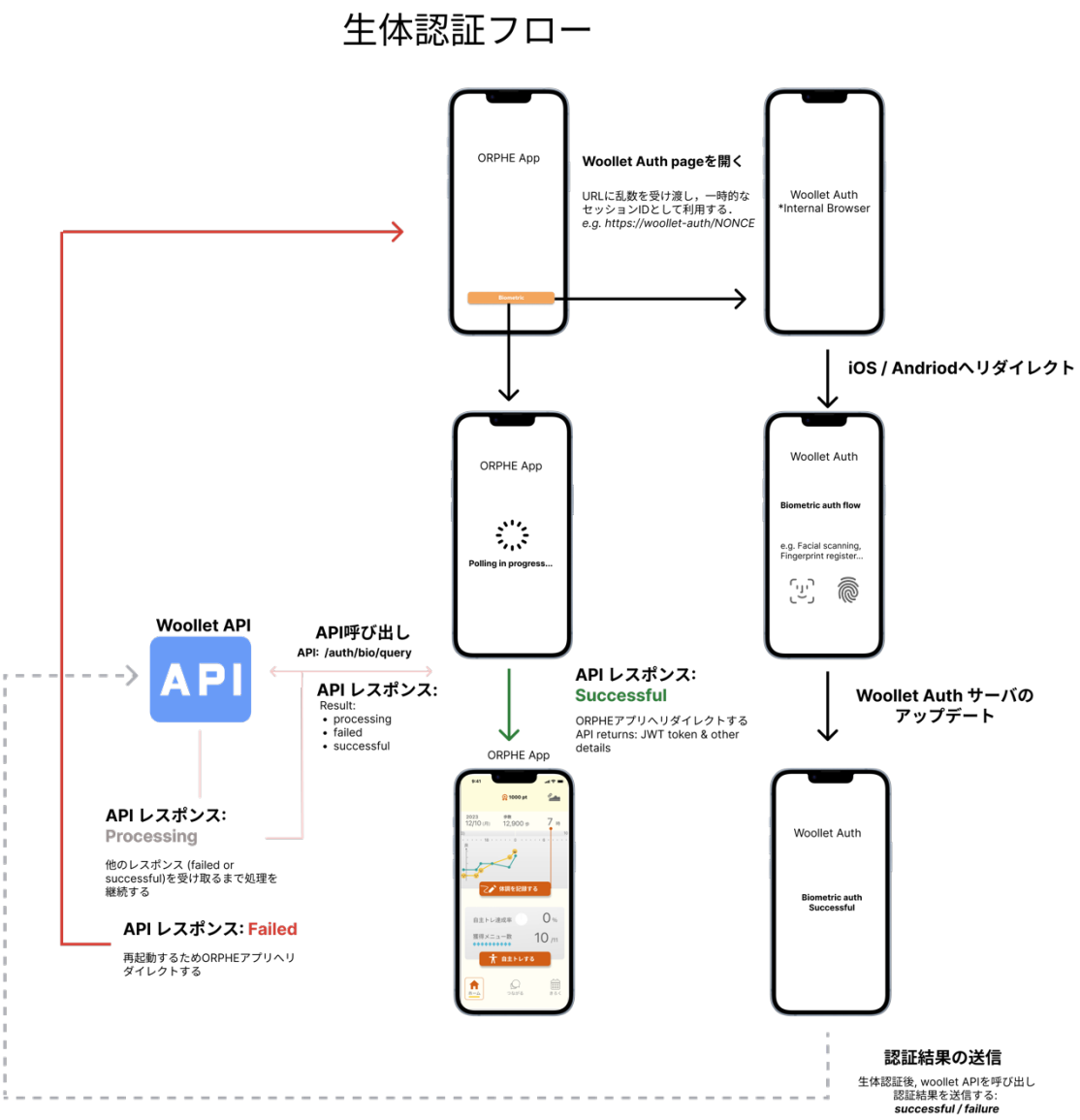


図 4-1-1：生体認証のフロー

3）歩容認証に適応する技術の選定

データ利用者がデータを利用するにあたり、データが患者本人のものであるかを確認できない点に課題があると考え、データの本人性を担保する手段を検討した。データの本人性を認証できる手段として、歩容認証はスマートシューズから歩行データを取得する本システムにおいて、データそのものを対象に登録されたデータとの一致度を評価するものであり、最も適合する手段であると考えた。

まず、開発システムへの応用可能性を考慮し、モーションセンサもしくはスマホ内蔵センサで取得できる情報を用いた技術を対象に調査を行い、以下の代表的な３つの技術を比較した。

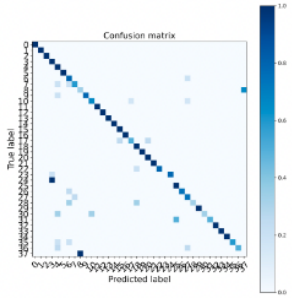
		歩容認証技術		
		技術1 Arshad et al., 2021 IEEE	技術2 Jung et al., 2021 IEEE EMBC	技術3 Choi et al., 2023, Sensors
データ	利用データ種類	足部，加速度	足部，加速度・角速度	スマホ（ポケット内or 手持ち），加速度
	利用データ種類	**特徴量 (Max, min, ave, std)**	**スペクトログラム**	-
	データ周波数	1000 Hz	100 Hz	50 Hz
性能評価	テスト人数・データ数	9 step x 60名	15 step x 69名	10名 x 約90s
	学習データ	80%	80%	10%（？）
	手法	SVM	ResNet18	CNN (12 layers)
	性能評価方法	5-fold CV, 20% test	4-fold CV, 20% test	???
	性能	**98.7 %　(accuracy)**	92.9 %　(accuracy)	0.91 (accuracy) precision, recall, F-score>0.9
コスト	利用ライブラリ	Keras	PyTorch	TensorFlow （TensorFlow Lite）
		⇒ 検証		追加学習，デバイス実装が考慮されている 状況（手持ちorポケット）が限定的 検証人数が限定的

図 4-1-2：歩容技術認証

３ つの技術のうち、中でも学習に用いる特徴量が既存システムと類似しており、識別率も高い技術 1（Arshad et al.、2021 *IEEE*）を選択し、自社の既存データを用いた検証を実施することとした。

上記で選出した技術 1 を自社の既存データに用いてその性能を評価した。

- 対象者：38名（健常者，下肢運動器疾患患者）
- 歩行環境・条件：treadmill上，4分間
- センサスペック：200 Hz
- 解析対象データ：
  右足の連続した20歩，各strideの歩行パラメータ（歩幅など）・統計量（加速度最大値など）
- 解析
  - 手法：SVM
  - train:test = 80:20
- 結果
  - トレーニングデータに対する識別率：0.95
  - テストデータに対する識別率：0.79



- 考察
  - やや先行研究結果よりも低い ⇐ サンプリング周波数，4 km/h，投入特徴量などが理由か
  - limitation
    - トレッドミルの連続した20歩 ⇒ 路上計測は不明
- 展望
  - 精度向上の可能性もありうる（左足データ，特徴量精査，その他手法の検討）
  - 実用過程における精度の低下も考慮しなければならない（路上，日間変化，手法の実装可能性）

図 4-1-3：歩容認証に関する実証の詳細と結果

健常者、下肢運動器疾患患者を含む 38 名のデータを用いた。treadmill 上で歩行した際の右足の連続した 20 歩のデータを解析対象に用いた。各ストライドの歩行パラメータ、およびスマートシューズ内のセンサから取得された 200Hz の加速度、角速度データの統計量（最大値・最小値など）を変数とした。学習データ：検証データ＝80：およびに分割し、サポートベクターマシンによるデータ判別を学習したのちに、識別の性能を評価した。テストデータに対する識別率は 0.79 であった。先行研究結果よりもやや低い結果となったが、両側のデータの使用や特徴量の精査、その他判別手法の検討によって、精度の向上も期待できると考えられる。一方で、実用化においては、路上を歩行すること、日間に変動がありうることなど、精度低下の要因も多く想定できる。また、下肢運動器疾患患者は歩行の改善・変化が比較的短期に起こることがあり、その変化への対応可能性も未知である。

4）歩容認証のモバイルアプリへの実装の可否

先行文献技術は性能の検証を主な目的としているため、社会実装に向けたモバイルアプリへの実装可能性が存在することも必要であるため、調査を行った。

機械学習モデルのアプリケーション実装については、モバイル端末への実装を想定した機械学習パッケージ（TensorFlow lite）がオープンソース化されており、スマホアプリへの機械学習を用いたアルゴリズムの実装は可能であると考えられた。一方で、実際のユースケースを想定したプロセスを考慮すると新規に登録された各ユーザに対して、それぞれ個別の判別モデルを学習させることが必要になるため、より高い認証精度の実現には、ベースとなるモデル構築に多くのサンプル（既存で蓄積しているデータ数よりも多く）が必要になることが考えられた。

5）本ユースケースにおいて歩容認証機能を実装するか

上記の検証により、現状の結果のみでは開発システムで実装するには、課題があると考えられたため、改めて歩容認証の実装の有用性を整理した。

まず、データそのものを対象に認証を行えるため、遠隔で取得されるデータが、登録されたデータと同一の人物から取得されたことを保証するに理想的な認証方法であると考えられる。また、個人の有する特徴をベースにした認証技術は、web wallet の秘密鍵復旧に際しても、オプションとして有効な手段であると考えている。

ポイント発生などのインセンティブが発生する場合には、データの不正な計測が発生する可能性があり、データ自体の本人性を認証することは重要性が高いと考えられる。一方で、臨床試験や医師のアドバイスにデータを使用する場合、患者がデータを不正に取得するインセンティブは低く、データの認証によって本人性を認証することの効果は高くないと考えられる。また、分散型臨床試験（DCT）の実施など実用場面における認証の必要性の観点では、現状では遠隔で取得されるデータの臨床試験利用にあたっては、ID とパスワードによるアプリ利用時ログインまたはデバイスの ID に紐づいた管理以上のことは求められておらず、今後の認証の必要性の見込みも不明であった。よって、総合的に今回の実証実験において、スマホ起動時の顔認証に加えて、アプリ起動時に顔認証を実装することの有用性は大きくないと判断した。

上記の論点を踏まえた結果、歩容認証を実装することに意義は見出せるものの、実用的な認証精度を満たすシステムを実装するには、データ数や判別手法の研究開発およびシステム実装の工数が必要であり、本実証事業においては、医師と患者間のデータ共有をメインな機能と捉えたシステムにおいては不正なデータ取得の発生可能性は低いと考え、更なる開発・実装 は今後の検討事項とした。

6）アカウント/パスワード/秘密鍵の復旧手段の検討

分散型 web システムにおいて、アカウント/デバイス紛失時の秘密鍵復旧手続きは非常に煩雑であり、ユーザビリティとセキュリティを両立する秘密鍵復旧手段の検討も課題であると考える。

個別顔認証および歩容認証の実装を見送ることとした状況から、外部ストレージに保存された特徴量を用いた生体認証による秘密鍵復旧の実装も見送ることとなったが、生体認証（FaceID）を組み合わせた秘密鍵復旧のオプションについて検討・実装を行った。

基本的にはパスワード復旧で事足りるようにしたいため、以下の 3 つの多要素認証によってパスワードリセットを可能とした。

1．Reset password with biometric authentication
2．Reset password with seed phrase
3．Reset password with email one-time password

デバイスを紛失したなどのやむを得ない場合には、2 要素認証によって復旧する手段を実装した。

1．生体認証を実施するデバイスを紛失した場合：
email/password によるサインインとメールアドレスに送信した One-time password を用いた復旧
2．メールアドレスへのアクセスを失った場合：
email/password によるサインインと生体認証を用いた復旧

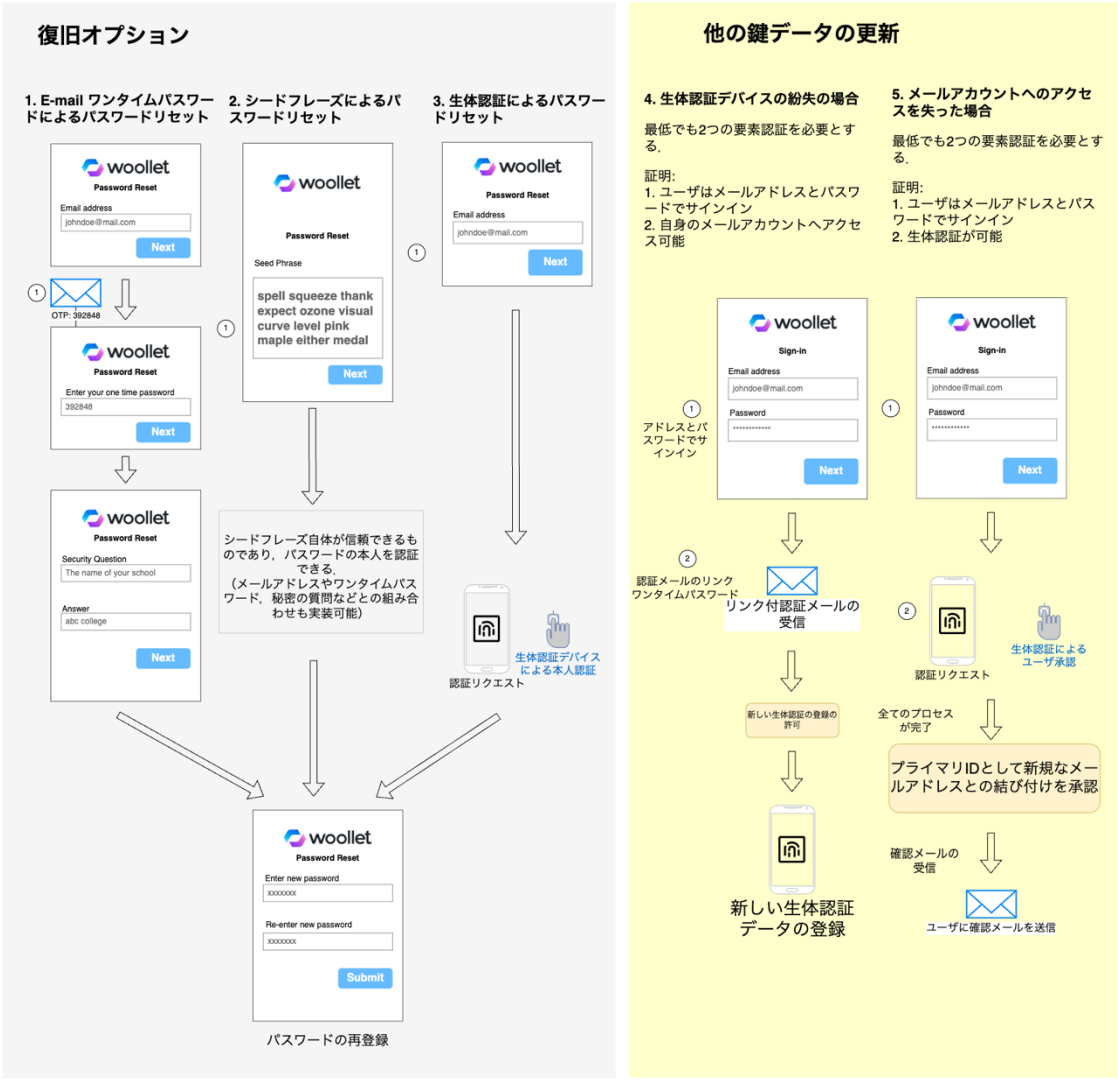


図 4-1-4：アカウント/パスワード/秘密鍵の復旧手段

4.1.2　企画・プロトタイプ開発に用いる技術・標準等を選定した理由および背景

企画・プロトタイプに用いた技術・標準およびその選定の理由は以下の通りである。

1）　Woollet

同意処理、属性の秘密照合が可能な web wallet であることを要件とし、個人情報を活用する際にユーザ同意取得を前提としている点、DataGateway 社独自のプレサイスターゲティング技術を活用した患者情報と検索条件の突合が本実証の条件を満たすため、web wallet として woollet を選定した。

2）　Hyperledger

DID ドキュメントを記録するためのコンソーシアムチェーンには、woollet が元々採用している Hyperledger を使用することとした。これはゼロ知識証明を活用する際に Hyperledger Aries を使用する目的と DID 取り扱い関連のソリューションが豊富に揃っているためである。

3）　**Polygon**

ポイントや NFT の管理を要件とした。トランザクション速度や安全性に課題が確認されたことから、これらの点の改善を求めより良い規格の選定を行い、トランザクション能力の高さに加えて、ガス代の安さ、普及率の高さを鑑みて、パブリックチェーンの Polygon を採用した。

4） **FaceID**

アプリ操作者がアカウント保持者本人であることの信頼性を高めることを主な要件とし、アカウント保持者本人の認証であることを用いてアカウント復旧に利用することも期待された。医療関連情報というプライバシーが必要な情報を取り扱うため、アカウント保持者本人がアクセスしていることを証明する必要性があると考えた。4.1.1 で詳細を述べたように個人認証が可能な顔認証システムは、データ保管など、サービス提供時期の観点から実装を見送り、生体認証によるデータの本人性担保への効力と、実装工数の観点から、実装容易性・相互運用性を考慮し、OS（iOS）標準搭載の FaceID を利用することとした。

5） **IPFS**

データの漏洩、消失への耐性が高いストレージであること、ユーザがデータアクセスを主体的にコントロールできることを要件とした。分散保存することでユーザデータの消失に耐性が高いこと、秘密分散を行うことでデータ保管のセキュリティが高いこと、サービスプロバイダーではなく、ユーザ管理のもとにデータ保存されることから、IPFS を採用した。

6） **Passkey**

パスワード管理の簡易化を要件として passkey を採用したが、セキュリティ向上・UX の向上・多要素認証の導入などの効果も認められる。]

4.2 Verify できる領域を拡大する仕組み

4.2.1 登場主体・要求事項整理

- 下肢運動器疾患患者

【役割】

- 日常生活の中で歩行計測や主観症状入力などによりスマホアプリで（自身のデータであることを可能な限り証明できる形で）データ記録を行う。
- データ共有リクエストに対して、データ利用者・データ利用目的を確認し、アプリ上でデータ共有の承認を行う。

【実証事業において設定した要求事項】

- データ登録時に生体認証を用いて、自身のデータであることを担保する。
- 共有リクエスト者、共有リクエストされたデータ項目を見える形でデータ共有の承認/非承認を決定する。

- 医療機関（医師/理学療法士）

【役割】

- 医療機関の許可のもと、医師/理学療法士などの個人に証明書を発行する。
- 対象患者の診断情報をシステムに登録する。
- 対象患者の日常におけるデータを、システムを通じて確認し、効果的な診療の実施に役立てる。

【実証事業において設定した要求事項】

- 機関の承認のもと、個人に証明書発行が可能。
- 入力した診療情報が書き換え不可能な形で、患者に受け渡される。
- データ共有リクエストは利便性のため、遠隔/対面でやり取りできる。
- 共有されたデータを閲覧できる。

- 研究機関/製薬会社

【役割】

- 研究対象となる患者にデータ共有リクエストおよびリクエスト者の情報を送信し、データ共有許可/データを取得する。

【実証事業において設定した要求事項】

- 対象となる患者に絞ってデータ共有リクエストを送信できる（プレサイスターゲティング）。
- 共有されたデータを閲覧できる。

- サービス提供者（ORPHE）

【役割】

- 医療機関/研究機関などサービス利用機関と契約し、機関の証明書（リレーションシップ VC）を発行する。
- 患者の活動状況およびデータ共有状況に応じて、ポイントを発行する。

【実証事業において設定した要求事項】

- リレーションシップ VC の発行ができる。
- 活動/データ共有に応じたポイントの発行ができる。

4.2.2　企画・プロトタイプシステムの開発におけるペインの解決方法

本実証における企画・プロトタイプシステムの開発におけるペインとその解決方法について、以下のように整理した。

- アプリ利用者の本人認証がなされていないことがペインと考えられ、生体認証を導入することで、部分的にアプリ利用者がスマホ保持者であることの担保ができると考えた。OS 標準搭載の生体認証モジュールが、応用範囲が広く実装が容易なため採用した。
- データ共有リクエストを送信する際に、ユーザ（患者）情報を開示することなく、対象者へリクエストを送る必要性があると考え、プレサイスターゲティングの導入を検討した。ゼロ知識証明、Verifiable credential を用いて実装することで、ユーザプライバシーを守ったまま、医者や研究機関などのデータ利用要件を満たす患者へリクエストの送信ができる。
- シードフレーズを用いた秘密鍵復旧方法の煩雑さはペインの一つと考えており、ID/パスワードや生体認証を組み合わせてユーザの利便性とセキュリティを両立した復旧手法が確立できると考えた。

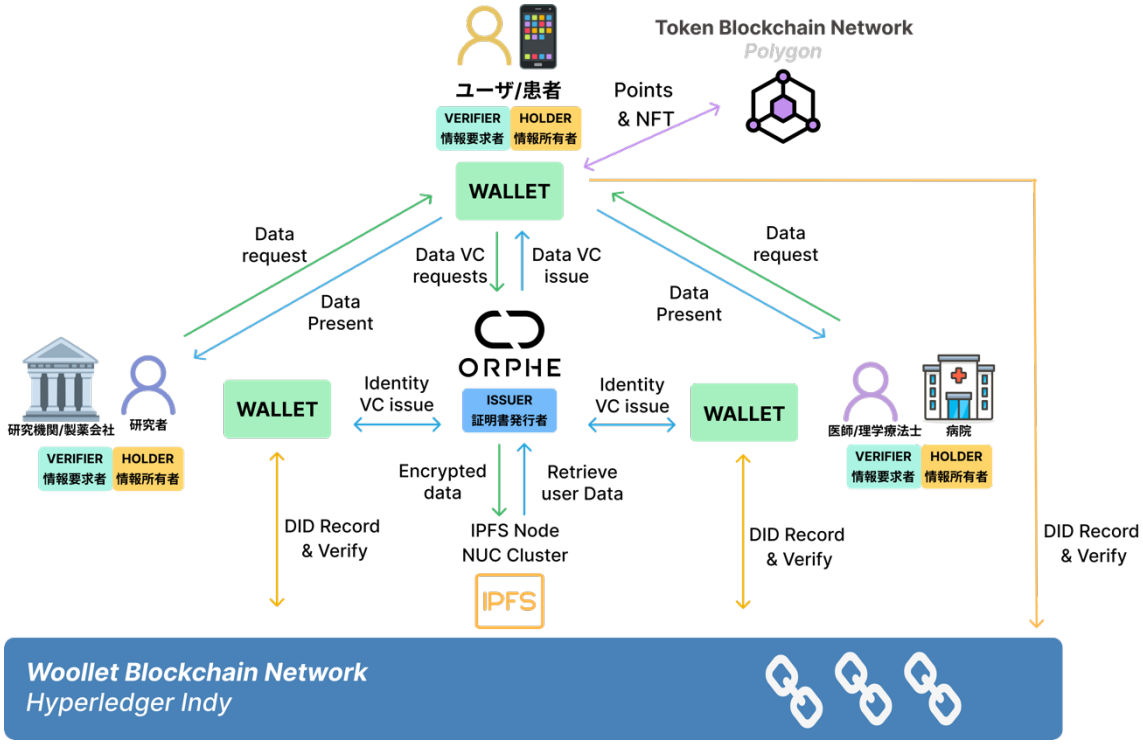


図 4-2-1：本実証事業で開発するシステムにおける各主体の役割と主体間のやりとり

4.2.3 Verify するデータ一覧

各 Verify にかかる課題に対して①Verify の対象、②Verify 方法、③検証者(verifier)、④データ保有者(ownership)、⑤発行者(issuer)、⑥データの置き場所、⑦アクセスコントロール(access control)、⑧成果・留意点の 8 観点で整理した。

- 検証によって解決したい課題：日常生活の中で最適な歩数や歩行動作を知りたい
    - ① Verify の対象：-
    - ② Verify 方法：スマートフォン上の機能による歩数の取得、スマートシューズを利用した歩行動作の計測
    - ③ 検証者：-
    - ④ データの保有者：患者
    - ⑤ 発行者：-
    - ⑥ データの置き場所：患者スマホ、IPFS
    - ⑦ アクセスコントロール：患者本人及びデータ共有許可を受けたものがアクセス可能
    - ⑧ 成果・留意点：個人の歩数や歩行動作を日常的に計測・記録・共有ができる。またデータに基づくコメントフィードバックも可能

- 検証によって解決したい課題：適切な対象に適切な範囲で患者のデータを共有したい
    - ① Verify の対象：医療機関/医師，研究機関/研究者，製薬会社/企業社員
    - ② Verify 方法：データ共有リクエストの受信と医師等の所属証明 VC 及びデータリクエストの許可機能の実装
    - ③ 検証者：患者
    - ④ データの保有者：医師，研究者，企業社員
    - ⑤ 発行者：
        (ア) 法人への発行：ORPHE
        (イ) 所属する個人への発行：リレーションシップ VC を有する法人
    - ⑥ データの置き場所：スマホ，IPFS
    - ⑦ アクセスコントロール：医師/研究者/企業社員が所属証明 VC を患者へ提示することで患者がアクセス可能となる。また、患者がデータリクエスト許可を行った医師/研究者/企業社員のみアクセス可能
    - ⑧ 成果・留意点：リレーションシップ VC の実装によって、サービス提供者（ORPHE）は各法人への証明書発行のみを行い、所属する個人への証明書発行は各法人が実施する。各法人の認証はサービス利用契約の締結を持って行うこととする

- 検証によって解決したい課題：患者の日常のデータを把握して治療を最適化させたい
    - ① Verify の対象：-
    - ② Verify 方法：web システムから医療機関/医師がデータ共有リクエストを患者に送り，許可された場合，データを閲覧できる
    - ③ 検証者：-

④ データの保有者：患者
⑤ 発行者：-
⑥ データの置き場所：スマホ、IPFS
⑦ アクセスコントロールの手法：データ共有許可（合意形成）がない場合、医療機関は IPFS に保存された患者データにアクセスできない
⑧ 成果・留意点：初回登録時の QR コード読み込みによるリレーションシップを確立させることによって、容易に患者個人へのデータ共有リクエストの送信をできる仕組みを実装した

- 検証によって解決したい課題：適切な対象に適切な範囲でリクエスト送信したい
  ① Verify の対象：患者
  ② Verify 方法：プレサイスターゲティング技術を用いて、指定した条件を満たす患者のみにデータリクエスト共有依頼を送信する
  ③ 検証者：医療機関、研究機関/製薬会社
  ④ データの保有者：患者
  ⑤ 発行者：医師、患者
  ⑥ データの置き場所：スマホ、IPFS
  ⑦ アクセスコントロール：プレサイスターゲティングによって、医師等から患者の個人情報にアクセスすることなく、条件を満たす患者にのみデータ共有リクエストが送られる
  ⑧ 成果・留意点：治験を行う際に新たに適切な対象を集めてデータを取得することには大変な労力、資金が必要となる。本システムを通して適切な対象に追加的に同意を取りデータを集めることで、低コストで必要なデータを集められる可能性があることが示唆された。発展的にはポイントを通じたインセンティブ提供を通じて対象に特定の行動を依頼するといった使用方法もあり得る

- 検証によって解決したい課題：センサデータが本人のものであることを確認できない
  ① Verify の対象：患者データ
  ② Verify 方法：顔認証や歩容認証等の生体認証手法を用いた記録時のデータ認証方法を複数検証し、本人のデータであることを証明するシステムを実装
  ③ 検証者：-
  ④ データの保有者：患者
  ⑤ 発行者：患者
  ⑥ データの置き場所：患者スマホ、IPFS
  ⑦ アクセスコントロール：顔認証はスマホ標準搭載のモジュールを利用することため、患者本人以外のアクセスを許容しない
  ⑧ 成果・留意点：顔認証を搭載することで、アプリ利用者がスマホ保持者であることを認証し、データの信頼性の向上ができた。一方で悪意を持ったアプリ登録者本人ではない個人がシューズを利用したり、スマホを持って歩いてもデータ登録時に顔認証ができたりすれば登録がなされてしまうという限界はある。これには歩容認証によるデータそのものの認証

が有効であると考えられるが、技術的ハードルのため実装には至らなかった

- 検証によって解決したい課題：無数に集まるデータが研究に扱うデータとして適切か，改ざんされていないか確認できない
    ① Verify の対象：患者データ
    ② Verify 方法：ブロックチェーンを活用したデータの管理や本人確認を組み合わせることで、無数に集まるデータに信用が付与され活用可能となる
    ③ 検証者：-
    ④ データの保有者：患者
    ⑤ 発行者：-
    ⑥ データの置き場所：患者スマホ、IPFS
    ⑦ アクセスコントロール：患者本人はスマホに保存されたデータにアクセスできる。データ共有許可を受けたもののみ IPFS へのアクセスが可能になる
    ⑧ 成果・留意点：分散型ストレージへの保管によって耐改ざん性を確保したシステムの構築ができた

4.2.4　証明書要件・識別子要件

【証明書】

- 患者情報
  記載情報は、性別、生年月日、身長/体重、疾患名、治療情報など。疾患名や治療情報については診察を担当した医師が、性別など患者の基本情報は患者が入力することでシステムから発行される。データに対して Zk-SNARK による検索を行う必要性があるため、活用する規格は Aries RFC 0036:Issue Credential Protocol 1.0 / Aries RFC 0453:Issue Credential Protocol 2.0 とした。
- 法人間のリレーションシップ VC
  リレーションの内容、権限を記載する。これは、法人のサービス利用契約締結に基づき、ORPHE が承認した際に発行するものとする。プライバシー保護、選択的開示の実装、偽装防止の観点から、SD-JWT、AnonCreds を活用する規格とした。
- 法人に所属することを示す VC（VP）
  記載情報は所属機関、権限、ライセンス有効期限。個人間での P2P データ受け渡しが前提となっているため DIDcomm での通信を行っている。Aries RFC 0023:DID Exchange Protocol 1.0 / Aries RFC 0037:Present Proof Protocol 1.0 / Aries RFC 0454:Present Proof Protocol 2.0 に対応にしている。
- 歩容データ
  センサから取得された歩容データ、スマホから取得された歩行データ、痛みなど患者がアプリで入力したデータを記録する。SD-JWT、AnonCreds を選択的提示が可能であり、EUDIW でも準拠

すべき規格[6]を満たす仕様として指定した。これは、喫緊で公的な規格となることが想定される、Unlinkability も対応、普及が進んでいる、今後 W3C のデータモデル[7]の規格と併せるようバージョンアップが検討される、といった特徴も選定の理由とした。

【識別子】

- 患者 Identifier
  患者を識別するものとする。DID とデータウォレットに関して様々な規格等が統一されていないために、異なるシステム間での相互運用が困難なため、自社でユニバーサルリゾルバを用意する形で対応するために識別子は Hyperledger Indy を用いている。また、Indy では、Opt-in と Opt-out のプロセスを DID ドキュメントと DID メソッドを用いて実装でき、ゼロ知識証明を用いることで、必要最低限の情報のみを開示することができる。これにより、プライバシーが保護され、データの漏洩リスクが軽減される。
- 機関 Identifier
  サービスに関わる機関を識別するものとする。採用規格および採用理由は患者 Identifier と同じ。
- 医師/理学療法士/研究者 Identifier
  医師や理学療法士、研究者を識別するものとする。採用規格および採用理由は患者 Identifier と同じ。

[6] EUDIW は ISO/IEC 18013-5:2021 および Verifiable Credentials Data Model v1.1 のデータモデルに準拠すべきであると定めている。AnonCreds は Verifiable Credentials Data Model v1.1 の規格に準拠している。

[7] Verifiable Credentials Data Model v1.1 のこと。https://www.w3.org/TR/vc-data-model/

4.3 合意形成・トレースの仕組み

本システムで目指す合意形成とその履行のトレースの内容について、①合意の主体、②合意の対象、③合意の条件、④トレースの対象、⑤トレースの手法、⑥合意取り消しの可否について整理を行った。主に合意形成を行うのは、患者と医師/理学療法士間のデータ共有および患者と研究機関/製薬会社間のデータ共有となる。

【患者と医師/理学療法士間のデータ共有】

合意の主体は患者と医師/理学療法士であり、患者情報（基本情報、歩行データ、医療情報）共有が合意の対象となる。合意の条件は、医師/理学療法士の所属が検証されたのちに、患者が医師/理学療法士からのデータ共有リクエスト内容の確認し、共有が許可されることである。履行された合意に関しては、パブリックブロックチェーンレジストリに保存されるため、照会によるトレースが可能な状態である。また、合意の取り消し（データ共有の取り消し）も可能とした。

【患者と研究機関/製薬会社間のデータ共有】

合意の主体は患者と研究機関/製薬機関であり、患者情報（基本情報、歩行データ、医療情報）の共有が合意の対象となる。合意の条件は、研究者/製薬会社社員の所属が検証されたのちに、患者がデータ共有リクエスト内容の確認し、共有が許可されることである。履行された合意に関しては、パブリックブロックチェーンレジストリに保存されるため、紹介によるトレースが可能な状態である。また合意の取り消し（データ共有の取り消し）も可能とした。

上記の合意記録が形成されたタイミングおよび合意取り消しがなされたタイミングは、不正なデータ利用などが行われた際に第三者による確認が必要となる場合があると考えている。第三者がデータリクエスト者とリクエストへ回答したことが分かるため、今回のサービスケースにおいては、ユーザ（患者）が有疾患であることが分かる可能性がある。

4.4 企画・開発物

4.4.1 業務フロー

- プレサイスターゲティングを用いたデータ共有リクエストのフロー

  ユーザ（医療機関や研究機関など）が特定の条件を満たす患者に、データ共有リクエストを送信し患者が承認/非承認し、データ共有がなされるまでのフロー。

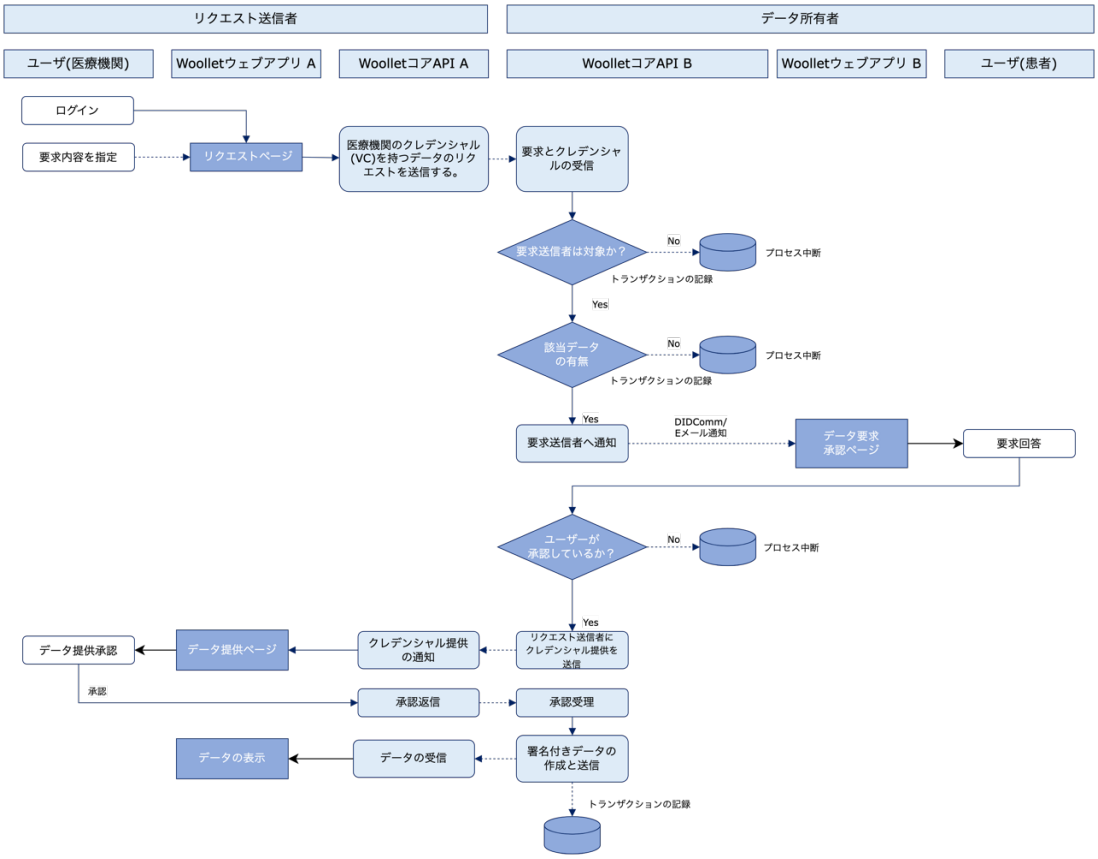


図 4-4-1：データ共有のフロー

4.4.2　ユースケース図

本実証事業におけるユースケース図を以下に示す。主に患者ユーザが利用するモバイルアプリ（ORPHE Mobile App）と、主に医師/医療提供者や研究員などデータ利用者が使うデスクトップアプリが存在する。

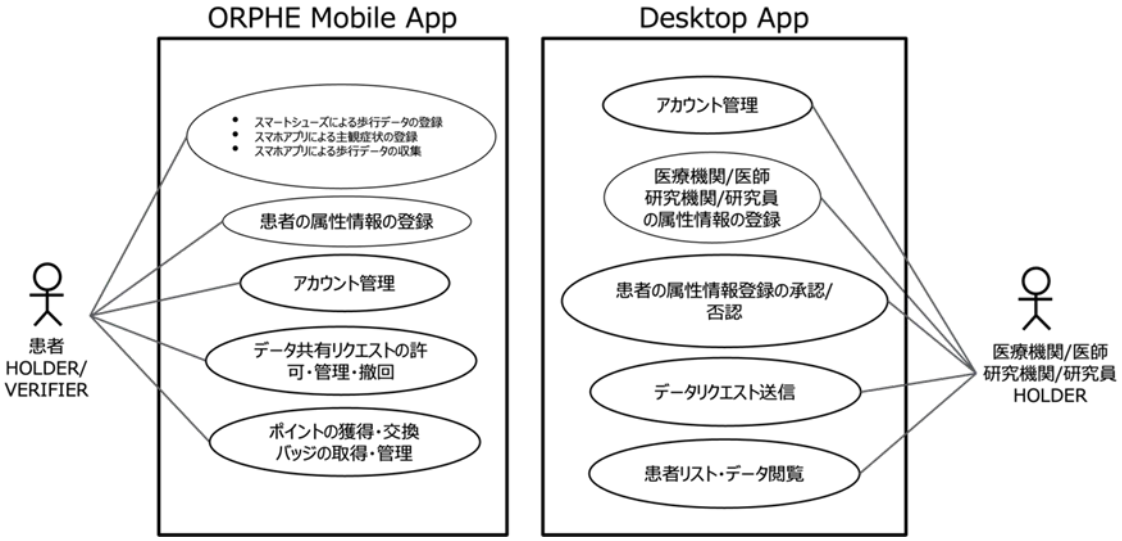


図 4-4-2：ユースケース図

4.4.3　操作画面（UI）

本実証実験にて開発したアプリケーションの主な機能と操作画面について以下で説明する。

①ウォレットのインストール・サービス登録

患者ユーザはまずアプリをダウンロードしたのち、初期画面から新規登録を始めると Woollet（Web ウォレット）登録画面へ移行し、サインイン手続きを行う。医師がアカウント情報を設定する場合には、医師が Desktop アプリで患者診療情報を登録したのちに発行される QR コードを患者アプリで読み込むことで診療情報が引き込まれる。患者は患者基本情報を追加で入力し、登録することでアプリの利用開始ができるようになる。この場合、医師によって入力された信頼性の高い診療情報と共に患者情報が登録されることになる。

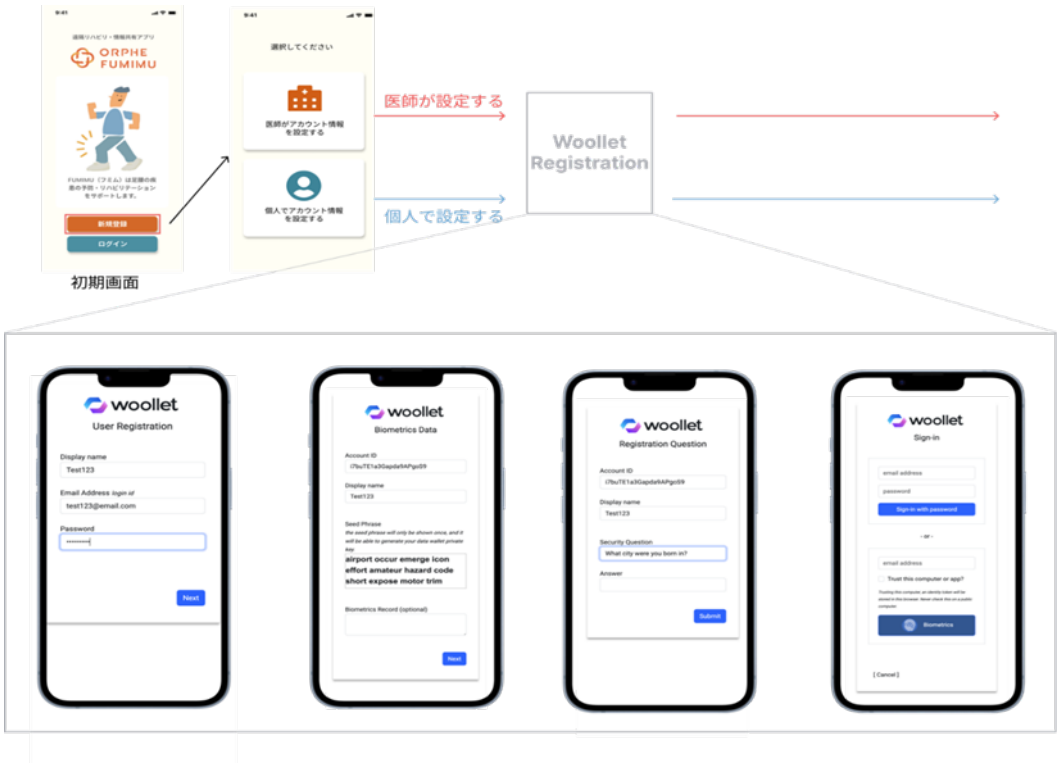


図 4-4-3：モバイルアプリの起動と woollet のサインインフロー（以下へ続く）

図 4-4-4：医師による患者診療情報入力と患者による情報登録

②証明書の発行

体調・痛みの入力を実施すると、データ VC の発行・登録と共にポイントの付与がされる。発行された VC は web wallet（woollet）画面からリストで確認可能となっている。

図 4-4-5：操作画面（UI）–データ VC 発行–

③データ共有

医療機関や研究機関はデスクトップアプリを利用して、患者にデータ共有リクエストを送信する。通知を受け取った患者ユーザは woollet にログインし、データ共有リクエストの内容を確認し、承認/非承認を選択する。承認された場合、データリクエストした側のデスクトップアプリからデータを閲覧できるようになる。患者ユーザはポイントの付与および NFT の発行がされる。

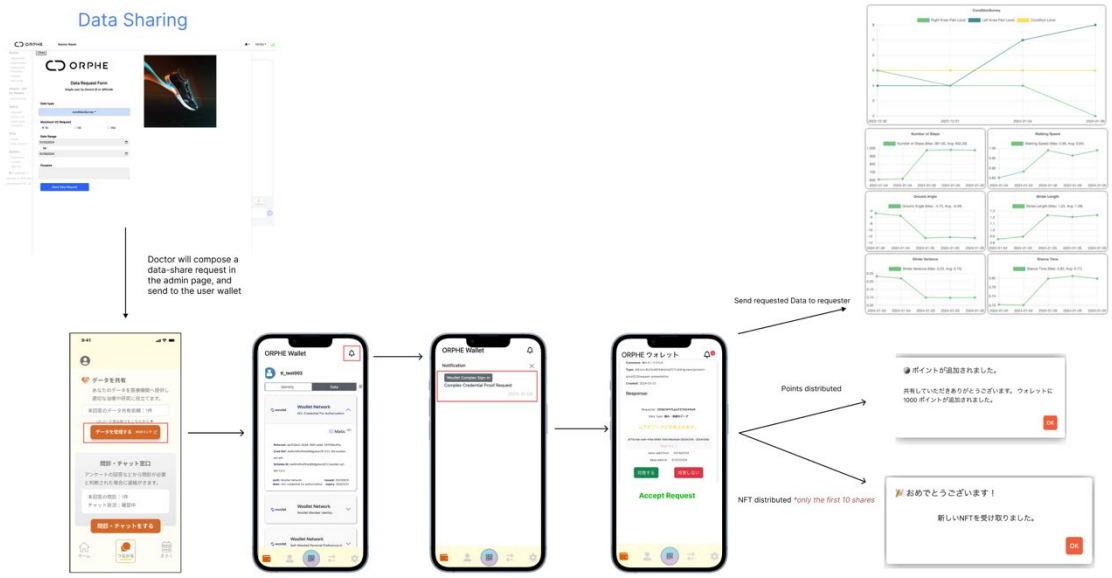


図 4-4-6：操作画面（UI）–データ共有リクエスト–

④ポイントと NFT の管理画面

獲得されたポイントおよび NFT はモバイルアプリの管理画面に表示される。ポイントはシューズやギフト券などと交換が可能である。将来的にはより多くのサービスでの活用を想定している。NFT は歩数やデータ共有の目標基準達成に応じて発行される。例として、3 日連続で 6,000 歩以上の歩数を達成した、データ共有への協力などを設定した。

図 4-4-7：操作画面（UI）–ポイント&NFT–

4.4.4　機能一覧/非機能一覧

本実証実験で開発したシステムの主な機能要件/非機能要件として以下のように定めた。

表 4-4-1：機能/非機能一覧

機能/非機能	機能名	機能概要
機能	歩数、歩行ログの登録	患者がスマホアプリを介して自動的に歩数や簡易の歩行ログが蓄積され、登録を行う機能
機能	主観的情報の入力	患者が、スマホアプリの入力画面で、主観的な情報（膝の痛みや体調など）を入力し、登録を行う機能
機能	歩行分析	患者が、スマホアプリとスマートシューズを使用し、歩行計測を行い、取得データの登録を行う機能
機能	生体認証	アプリ利用者が、登録された本人であることを認証する機能
機能	データの共有依頼	医師、研究者、製薬会社等が、特定の患者に対してデータの共有依頼を行う機能
機能	データ共有の承認	患者が、データ要求者（医師、研究者、製薬会社等）からきた共有依頼を承認する機能
機能	データ共有の撤回	患者が、一度許可したデータ共有を撤回できる機能
機能	共有データの閲覧	医師、研究者、製薬会社等が、共有承認されたユーザ（患者）データを共有され、プラットフォーム内で閲覧する機能
機能	ポイントの蓄積	患者が、スマホアプリ上で歩数の登録、痛みの入力、歩行分析を行うたびにポイントを蓄積できる機能
機能	ポイントの交換	患者が、スマホアプリ上で溜まったポイントを ORPHE に交換することで景品を得られる機能
機能	ポイントの返戻	患者がデータの共有を撤回した際に、定められた分のポイントが研究者/製薬会社等へ返戻される機能
機能	NFT 発行	患者の行動が条件を達成したことを証明する NFT（バッジ）を発行する機能
非機能	改ざんの防止	患者の蓄積されたデータが改ざんされていないことを証明できること
非機能	データ書き込みの速度	外部ストレージへの書き込み処理が課題であるため、可能な限り高速でデータ書き込みができること

機能/非機能	機能名	機能概要
非機能	トランザクションフィー	VC 発行どのトランザクション回数が多くなることが想定されるため、トランザクションフィーができるだけ安価であること
非機能	拡張性	利用者の増加に備えて、スケールアップが可能であること
非機能	運用・保守性	遠隔でのメンテナンスが可能になっている

4.4.4.1 非機能検討（リスク分析とセキュリティ対応方針）

本サービス・アプリを利用するにあたってリスク分析・対応方針の検討を行い、重要な点として個人情報の流出を挙げた。情報を安全に共有するためのシステムであり、個人情報の流出はサービス信頼性を損ねる重大なリスクである。発生ケースとしては、なりすましによるデータ共有リスエストの送信およびデータ閲覧を行うことが考えられる。本リスクについては、医療機関/研究機関はサービス利用にあたって規約を結び、リレーションシップを結ぶこと挙げるため、機関が悪意的な攻撃者に権限を付与することは抑制できると考えられる。また外部の攻撃者に関しては、外部からの直接的な攻撃（ハッキング）は AWS のセキュリティで保護されている。利用者（機関所属者）を狙った攻撃は発生する可能性がある。Desktop アプリのログイン時に生体認証を必要とし、また一定時間操作がなければ自動ログアウトする機能の実装によってリスクの低減を図る。

表 4-4-2：リスク分析とセキュリティ対応方針

サービス（アプリ）利用にかかるリスク			左記リスクへの対応方針・攻撃防止の根拠
	影響度（機密性・完全性・可用性への影響）	**発生可能性**（どのような悪意的な攻撃が考えられるか）	
個人情報の流出	個人情報の流出が生じると、サービス信頼性を損ね、事業への影響が重大である。	なりすましによるデータ共有リクエストの送信、データの閲覧。	医療機関/研究機関はサービス利用にあたって規約を結び、リレーションシップを結ぶことになるため、機関が悪意的な攻撃者に権限を付与することは抑制できると考えられる。

4.4.4.2　非機能検討（大規模・商用・社会実装時の対応方針）

【社会実装時に想定する利用規模】

社会実装する際には、まず参加者数：病院：30 部署、研究機関：10 機関、患者：1,000 人を目指す。データのやり取りについては、1,000 人×150 日利用 x24 回/日データアップロードと 50,000 回のプレサイスターゲティングと見積もり 2TB 程度となる。その後段階的なスケールアップを想定する。

【対応方針】

- Kubernetes を用いて、モジュール化されたシステムを構築しており、必要な処理能力が増大する場合にはノードを増設することで対応できる。
- 多くのストレージが必要になった場合も、ストレージのスケールアップが可能である。
- UI、API、エージェントなどは全て異なるノードにデプロイされるため、それぞれ独立したスケールアウトが可能となっている。
- ピーク時の性能や応答速度に関しても、現状のシステムでも 20 の同時接続が許容できる仕様となっており、1000 人のユーザ利用を想定した場合でも 20 の同時接続が発生する可能性は極めて低いと考えられる。また今後利用人数が増大し、同時接続数の増大が懸念される場合でもサーバの仕様を増強することで対応可能なため拡張性に大きな問題はないと想定している。

以上より想定されるユースケースにおけるスケーラビリティは確保されており、段階的な拡張に対しても対応可能と考えている。

4.4.5　データモデル定義

本開発システムでやりとりを行うデータモデルは以下のように定めた。

表 4-4-3：データモデル

属性値	属性取得元	属性値 （vc 内）
Authority / Organization name	Organization Info	org:name
Department / Branch or Unit		org:unit
Long description		org:desc
Organization logo		org:logo
Data Credential issuance date	Dates	date:issued
Data Credential expiry date		date:expiry
Credentials name	Document Info	doc:name
Credential type		doc:type
Long description		doc:desc
Document logo		doc:logo
Background Color code or image URL		doc:bg
Big file IPFS hash （only used when file need to upload）	Application Data	hash
Meta data of file		meta
Data sub type		type
Data Owner attribute		owner

4.4.6　実験環境

本実証実験の開発システムのバックエンドインフラの説明図（図 4-4-8）および実験環境図（図 4-4-9）を以下に示す。

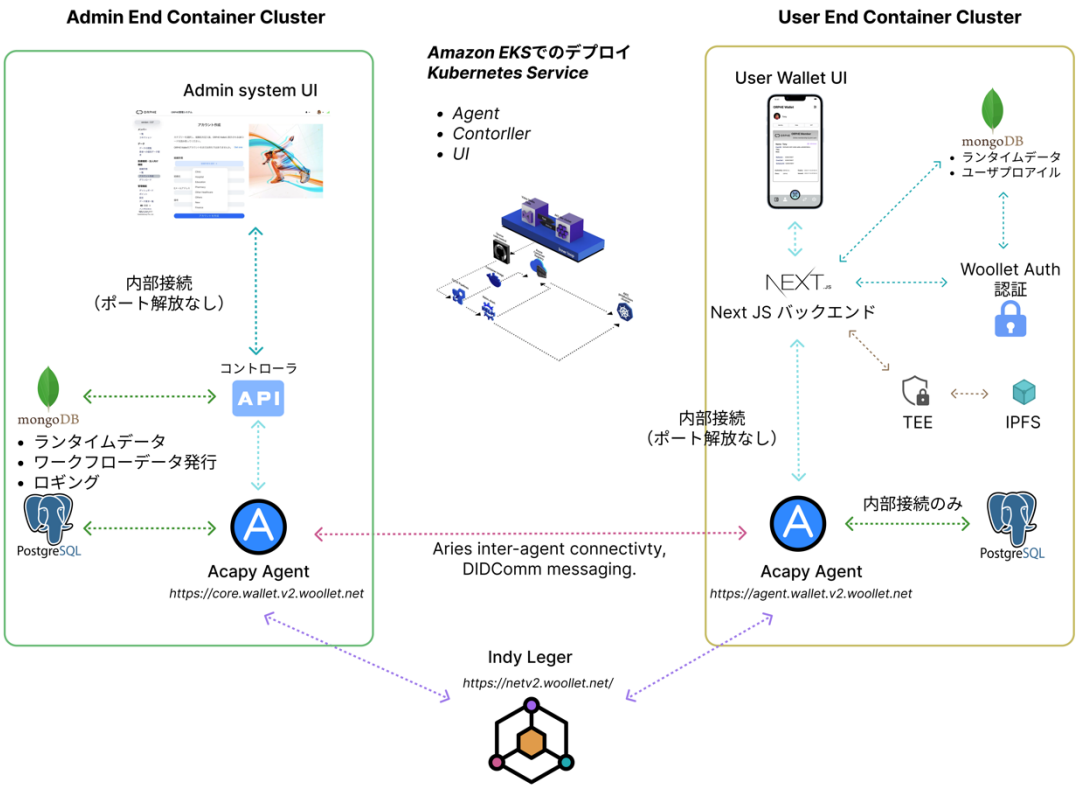


図 4-4-8：バックエンドインフラ

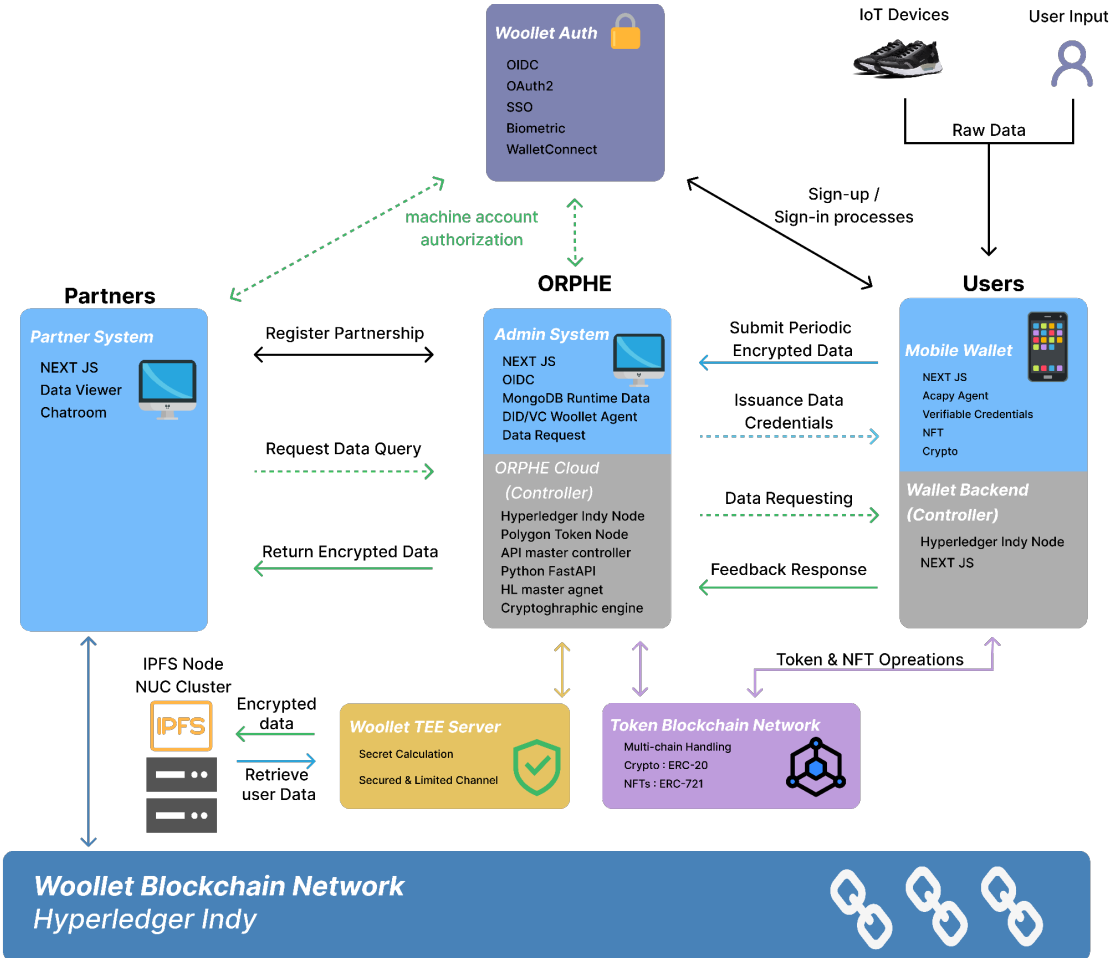

Woollet Auth
OIDC
OAuth2
SSO
Biometric
WalletConnect
IoT Devices
User Input
Raw Data
machine account authorization
Sign-up / Sign-in processes
Partners
ORPHE
Users
Partner System
NEXT JS
Data Viewer
Chatroom
Register Partnership
Request Data Query
Return Encrypted Data
Admin System
NEXT JS
OIDC
MongoDB Runtime Data
DID/VC Woollet Agent
Data Request
ORPHE Cloud (Controller)
Hyperledger Indy Node
Polygon Token Node
API master controller
Python FastAPI
HL master agnet
Cryptoghraphic engine
Submit Periodic Encrypted Data
Issuance Data Credentials
Data Requesting
Feedback Response
Mobile Wallet
NEXT JS
Acapy Agent
Verifiable Credentials
NFT
Crypto
Wallet Backend (Controller)
Hyperledger Indy Node
NEXT JS
IPFS Node
NUC Cluster
IPFS
Encrypted data
Retrieve user Data
Woollet TEE Server
Secret Calculation
Secured & Limited Channel
Token Blockchain Network
Multi-chain Handling
Crypto : ERC-20
NFTs : ERC-721
Token & NFT Opreations
Woollet Blockchain Network
Hyperledger Indy

図 4-4-9：実験環境

4.4.7　システムの構成要素

本実証事業における開発システムの構成要素は以下の通りである。

表 4-4-4：システムの構成要素

コンポーネント名称	システム・ライブラリ名	開 発 区分	開発先/権利の帰属先	型式名・ライセンス名/OSS 名
実証アプリ	Python Fast API	既存	Sebastián Ramírez	MIT, GNU APGL v3.0
	Flutter	既存	Google	BSD 3-Clause
	Next.js	既存	Vercel（以前は Zeit）	MIT
	Node.js	既存	Node.js Foundation	GNU Lesser GPL
サーバホスティング	AWS	既存	Amazon Web Services Inc.	Amazon
ストレージ	IPFS	既存	Protocol Labs	MIT
認証	Hyperledger Aries VC	既存	Linux Foundation	Apache-2.0, PostgreSQL

5. 実証（事業実現に向けたガバナンス・コミュニティ等の検討）

5.1 実施概要

5.1.1 事業実現に向けたガバナンス・コミュニティ等における論点とその結果

事業実現に向けたガバナンス・コミュニティ等における論点とその結果については概要を以下の表にまとめた。

表 5-1-1：ガバナンス・コミュニティの論点・結果

No.	論点	検討結果とその経緯
1	遠隔診療や分散型臨床試験（DCT）におけるウェアラブルデバイスデータの利活用に関するデバイス、システムの技術的要件について	現時点ではシミック社様の開発システムとの連携には、Keychain Core をインストールするため、**デバイスに OS 搭載する必要**であることがわかり、今後の検討項目とした。 開発システムを治験で利用するには、ALOCA などのデータインテグリティの原則に基づいたシステム仕様が必要であることがわかった。
2	臨床研究に活用可能な生体データに必要な要件やデータ数について	**データの信頼性（非改ざん、本人のものであることの担保、患者情報などと統合できること）は必要**である。 治験に関しては、**評価項目としてのエビデンスも重要**であることも明らかとなった。 **必要なデータ数も、数十人～1 万人規模**と用途によりばらつきが見られる。
3	臨床試験に活用可能な生体データに拠出可能な予算、ビジネスモデルについて	**各社利用を想定する用途が異なり拠出可能な予算は 30~500 万/年とばらつきがあった。** サービス利用料として年間利用料を支払うモデルは概ね問題ないと思われる。
4	同意撤回の実装について	同意撤回は、データ利用者の不利益とさせないため、**データ提供同意時に取得したポイント分と交換する（ポイント不足時には撤回できない）**とした。ルールの煩雑化を防ぎ、ユーザも必要分のポイントを取得すれば同意撤回できるものの、**撤回できない状況が発生するため、UC 委員も懸念を示し、一部のユーザからは不安との声**もあった。期間を設定し、段階的にポイント付与するなどの方法が考えられるが、今回は実装に至っていない。また同意撤回時の対処フローの整理も必要であることがわかった。
5	継続利用に対するインセンティブにはどのようなものが考えられる	**データ計測や共有に対するポイントや NFT の発行機能を実装**し、2 週間のユーザ実証実験を実施した。 ポイント獲得のため運動を意識したとの声があり、**一定のモチベー**

	か	**ション効果**はあったと考えられる。また、基準達成に対するバッジの付与は満足感が得られると声もあり、**NFT 付与による可視化もモチベーションアップに効果**が得られると考える。
6	インセンティブ（ポイント・NFT）をどのように設定するか	ポイント率の決定には、エビデンス構築と併せて、データの価値付と並行した更なる調査が必要である。 また**ポイント利用先を設定するなどの課題**もあり、持続可能なエコシステムの実現にはインセンティブ設計を含む参加可能なステークホルダを探索することも必要である。 今回の実装では今後の拡張性を考慮して基準達成のバッジ付与を NFT で実装したが、NFT が第三者に対する運動能力の証明になる機能など、**エコシステムの発展のための NFT の更なる応用方法についても検討していきたい**。
7	ガバナンスとして整理すべき項目にはどのようなものがあるか。（業界のルールには何があるか）	本システムが準拠すべき業界ルールは主に、**個人情報保護法、次世代医療基盤法、医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン、民間事業者の PHR サービスに関わるガイドライン**などが想定される。 データの取り扱いは個人情報保護法に準拠することとなるが、責任の所在やアカウントの管理義務などに関するルールを利用規約として設定する必要がある。

■ビジネスフィージビリティ

ビジネスフィージビリティについては、１）データ活用を促進するために必要なシステム・デバイス・データの要件、２）本サービスに支払うことができるサービス料、３）同意撤回の仕様やインセンティブなどエコシステム確立に関わる要素を論点として取り上げて、詳細に検討を行う。

１）および２）については、シミック社やデータ利用が想定される企業（CRO、製薬企業）を対象にヒアリングや議論を実施し、 本サービスへの反映可能性の検討および今後の社会実装に向けた課題抽出を行う。３）は、他サービスの調査および検討とシステムへの実装、実証実験を通したユーザへのヒアリングによって、実装機能のフィージビリティを検討する。

■ガバナンス・ルール整理

ガバナンス・ルールについては、本サービスを提供するにあたって整理・検討すべき項目の調査を行うこととした。特に本邦でサービス提供する際に準拠すべき法やガイドラインの調査、および海外も含めた PHR を含む情報を取り扱うサービスにおけるガバナンス事例調査（6 章で報告）を行った。

主な検討結果としては、本システムが準拠すべき業界ルールが既に多く存在することがわかり、これらへ対応すること、およびデータ取り扱いに関しては独自に利用規約などで整理すべき項目が生じることが明らかとなった。

■コミュニティ形成

コミュニティの形成については、本事業を通して患者、医療関係者、研究機関/製薬企業などと、医療データを含むデータ流通システムのあり方について議論を進める。特にサービス普及が進むために必要なシステムの機能やビジネスモデルのあり方についてヒアリング、議論から抽出を試みる。

5.1.2 実証ユースケース概要・実施内容・手法

ビジネスフィージビリティに関してデスクトップ調査および以下のステークホルダへのヒアリング結果をもとに論点に関する検討を行った。

表 5-1-2：ステークホルダーへのヒアリング観点

ステークホルダ	ヒアリング観点
企業（CRO、製薬企業; 4 社）	• ソフトウェア・アプリケーションレイヤでの連携の可能性を検討（シミック様） • **臨床試験**や**分散型治験（DCT）**等におけるウェアラブルデバイスデータの利活用に際してデバイス、アプリケーションの要件の確認 • 臨床研究、臨床試験、治験に活用可能な**生体データに必要な要件、**生体データに**拠出可能な予算の確認**
下肢運動器系疾患患者および既往歴を有するユーザ（7 名）	• アプリのユーザビリティについて • **アプリ UI やインセンティブが運動意欲向上につながったか** • データ共有や同意撤回について懸念する点があるか • サービスは利用したいと思えるか
医療従事者（医師、理学療法士）	• デスクトップアプリ（Partner system）のユーザビリティは実用的か • 医療現場でおけるサービスの実用性はあるか

5.2 検証結果

5.2.1 DCT や臨床研究に利活用できるシステム・データの要件

本システムで取得される歩容等のデータを治験データとして利用するには、ALCOA 原則などデータインテグリティを担保するためのシステム要件などが多く存在することがわかった。一方、DCT における生体情報の利用はかなり先進的な例のため確実な要件は世界的にも明確には示されていない状況であることがわかった。

シミック社の開発システムとのデバイスの連携についても検討したが、シミック社の開発システムではデバイス側での処理を行うため、現時点では OS が搭載されたデバイスとの連携を想定しており、今回の実証期間での実装は難しく断念した。今後連携を進めていくためには、デバイスへの OS 搭載または OS を搭載しないファームウェアとの連携を検討する必要がある。一方で調査を進めていくことで我々が想定するような DCT は世界的にも先進的な構想であることがわかり、DCT に生体データを活用するための標準は世界的にも設定されていないと思われる。そこで我々や CMIC のような事業者が生体データの標準化を

進めることで世界の DCT を先導していける可能性が示唆された。今後も連携を図って実現していきたい。

臨床試験におけるデータの利活用については、初期の仮説としてはダイナミックな同意を実装することで治験、臨床研究に活用できると考えていたが、現時点では事前に参加同意を取得する手順が一般的であり、ダイナミックに同意して取得されるデータを直接利用しにくい現状とのフィードバックが得られた。

一方で本サービスの利用者が増えれば、プレサイスターゲティング機能の活用によって条件を満たす研究参加者のリクルートが効率的に行える可能性があり、企業からもポジティブな声が集まったので、今後はこの方向性を重視してエコシステムを構築していきたい。

臨床試験や治験で評価項目とされる歩行関連の指標には、現状 6 分間歩行や Timed up and go テストなどがあるが、日常歩行データは記録可能なデバイスが近年普及し始めたこともあり、臨床評価のエビデンスが少ない。そのため、まずはデータ蓄積およびエビデンスの構築が重要であることがわかった。

5.2.2 継続的な利用・運動実施に資するインセンティブの実現について

ユーザ実証実験への参加者 7 名を対象としたヒアリングおよびデータ利用企業へのヒアリングを実施し、インセンティブ設計について検討を実施した。

本実証実験では本実証事業では持続可能なエコシステムの実装を重視し、データ計測や共有に対するポイントや NFT の発行機能を実装し、2 週間のユーザ実証実験を実施した。

ポイント獲得のためアプリの利用といつもより少し長く歩こうという気持ちになったとの声があり、一定のモチベーション効果があったと考えられる。（ただし、日常的な運動習慣がある参加者は運動量に変化はなかったとの回答もあった。）基準達成に対するバッジの付与は満足感が得られると声もあり、NFT 付与による可視化もモチベーションアップに効果が得られると考える。達成の基準が事前に分かる方がよりモチベーションにつながるとのフィードバックも得られた。

社会実装を行う上で、インセンティブをどのように設定するかについては、ポイント付与の基準・割合はエコシステム全体とのバランスを考慮する必要性があり、企業にサービス利用に拠出できる必要のヒアリングを行った。想定する活用ケースに依存して、必要データ数やデータ項目が異なり、拠出可能予算も 30~500 万/年とばらつくことがわかった。ポイント率の決定には、エビデンス構築と併せてデータの価値付と並行して更なる調査が必要と考えられる。また、今回の実証実験ではポイントの利用先として、自社製品との交換など設定したが、ユーザによって魅力的な利用先を増やす必要があり、持続可能なエコシステムの実現には、インセンティブ設計を含む参加可能なステークホルダを探索する必要がある。

今回の実装では将来的な拡張性を考慮して基準達成の付与バッジを NFT で実装した。NFT が第三者に対する運動能力の証明になる機能など、エコシステム発展のためのさらなる応用方法を探索する必要性が感じられた。

5.2.3 ビジネスモデル・ビジネスフィージビリティについて

本実証を通して、様々なステークホルダの要件を洗い出し、ビジネスモデルをより明確化することができた。患者からは、データが見やすい形で可視化されることは有意義であると感じられるとの意見が多く集まった。また自身の記録した情報が、医師に共有されることでモチベーションが上がったり、アドバイスがもらえれば嬉しいといった声が聞けたりした。下肢の痛みに悩んでいるなどの場合、サービス料として月額料金を支払うことも想定される。患者が払えるサー様々、医師から得られる価値に依存するということがわかった

ので、今後サービスコンテンツを拡充していく必要性が示された。

データの企業提供がマネタイズもとになると仮説立てていたが、ヒアリング結果からかなりまとまった数のデータ/利用者が必要ということ、歩行データの臨床評価におけるエビデンスが少ないことから日常歩行データはすぐにデータ利用に価値と考えづらいことなどがわかった（日常方向データによる、下肢機能の評価に期待は感じられる）。このことから、まずは医師-患もとのサービスから始められるビジネスモデルをとり、サービス利用者・データを増やすことから取り組み、段階的にデータ提供を行う方針とした。

またサービスの信頼性・安全性は、認証取得がなされているかを確認していることも示唆され、海外で長期に継続している類似サービスについても認証取得していることがわかった（6 章で詳細報告）ため、ISMS などの認証取得も重要であると考えられ、今後取得に向けて取り組みを進めることとした。

5.2.4　ガバナンス整理の結果

本ユースケースにおけるシステムにおいては、データの信頼性およびデータ共有範囲を適切にコントロールする仕組みを技術要素のみで実現することが困難であるため、これらに対処するガバナンス設計が必要と考える。本システムが準拠すべき業界ポリシーには、個人情報保護法、次世代医療基盤法、医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン、民間事業者の PHR サービスに関わるガイドライン、景品表示法などが想定される。明確に確立された既存トラストフレームワークはないと考えられるが、医療情報交換のフレームワークである HL7 FHIR がその役割を部分的に有していると考えられる。データ共有の範囲においては、データ共有時になされる同意内容および個人情報保護法によって制限されると考えられる。特にデータの信頼性を担保するため、データ提供者（患者）による不正なデータ計測を禁止するルールが必要となるため、サービス利用規約などによる制約を設ける必要があると考えられた。

6. 調査検証

6.1 実施概要

【調査の背景・目的】

近年多く展開されている、パーソナルデータを取り扱うサービスについて、国内外のユースケースを調査し、調査したサービスの内、比較的長期間サービス提供を継続できているサービスについて 3 つの論点（ビジネスモデル、サービス環境、トラスト）で深掘り調査・分析を行い、それぞれ ORPHE のサービス等と比較をしてユースケースの改善・社会実装に向けて有益となり得る示唆の検討を行う。

【調査方針】

- サービスの概要調査

パーソナルデータを取り扱う国内外のサービスを対象に、サービスを提供する会社、サービスの開始時期、サービス内容、サービスで取り扱われている情報の種類について調査する。

- サービスの抽出

調査をしたサービスから比較的長期間（10 年以上）サービス提供を継続できているものを抽出する。

- 深掘り調査

抽出したサービスについてそれぞれ、ビジネスモデル、サービス環境、トラスト（ガバナンス・テクノロジー）の論点を設定し、それぞれ以下のような内容で深掘り調査を実施する。

  - ビジネスモデル

    各サービスにはどのようなステークホルダがおり、そのステークホルダの間でどのような情報が取り扱われ、どのようなマネタイズ方法・インセンティブ設計でサービスが成立しているのか。

  - サービス環境

    各サービスが普及、かつ長期間継続した理由について、政策面（制度も含む）、社会動向面等の環境的要因としてはどのようなものがあるのか。

  - トラスト(ガバナンス)

    各サービスがトラストを高めるためにどのような法令に準拠し、内部規則を規定し、標準規格を取得しており、また、法令、内部規則、標準規格にはどのような規定があるのか。

  - トラスト(テクノロジー)

    DID/VC 等、Trusted Web に関連した手段の活用の有無およびその他、データの信頼性を高めるために企業がどのような技術を用いているのか。

- 調査結果の比較整理

各論点における深掘り調査結果について、各サービスおよび ORPHE のサービス内容（判明している分）等と比較整理を行い、各論点における共通点、差異やその他特徴等の有無を明らかにする。

- ヒアリング調査

深掘り調査の対象となっているサービスの有識者にヒアリングをし、深掘り調査等の机上調査で明らか

にならなかった点や普及しているサービスのその他の情報等に関して確認をする。

- 結論

深掘り調査およびヒアリング調査の結果を踏まえて、ビジネスモデル、サービス環境、トラストの論点において、サービスが普及した理由や仮説等から ORPHE のユースケースの改善・社会実装に向けて有益となり得る示唆を明らかにする。

6.2 調査結果

6.2.1 サービスの概要調査

6.2.1.1 Dprime

- サービス提供会社

  三菱 UFJ 信託銀行

- サービス開始時期

  2021 年

- サービス内容

  三菱 UFJ 信託銀行が 2021 年から提供を開始した情報銀行と呼ばれるパーソナルデータサービスであり、利用者は個人の明示的な同意に基づいて Dprime に預けたパーソナルデータを企業からのオファー（オファーには提供希望データ、利用目的の説明が記載）に応諾したものに対して提示し、その見返りとして割引クーポン、商品、ポイントを得るサービスである。（図 6-2-1）[8]

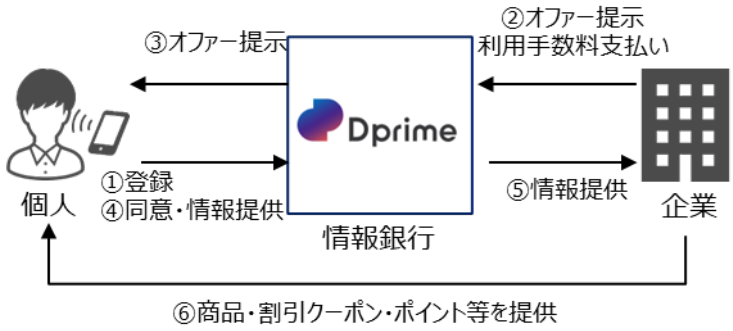


図 6-2-1：Dprime のサービスの流れ

取り扱う情報について、Dprime で取り扱われる情報については以下の通りである。

基本情報：性別、生年月日、住所（郵便番号、都道府県）等
仕事・お金：現在の職業・職種、経験職種、年収、支出等
家族・住まい：配偶者の有無、子供の人数、住居形態、居住年数等
生活・趣味・嗜好：趣味（予算）、利用している SNS、社会貢献活動等
健康・運動：健康についての関心の度合い、使用金額、平均睡眠時間等
食事：平日・休日の自炊頻度、外食の回数、よく飲むお酒等
その他：商品に対するレビュー、インタビュー結果等

6.2.1.2 FitStats

- サービス提供会社

  大日本印刷株式会社

- サービス開始時期

[8] 三菱 UFJ 信託銀行. https://www.dprime-mutb.jp/service/about/

2022 年

- サービス内容

大日本印刷株式会社が提供するパーソナルデータサービスであり、利用者の登録した自身の属性や趣味・趣向に関するデータ、食事・睡眠・運動等のライフログデータ（FiNC と呼ばれるフィットネスアプリと連携して収集）を自ら選んだ企業に提供することで、自分の興味・関心に最適な情報を受け取ることができる。また、利用者は登録したヘルスケアデータをもとに、各人の健康状態を独自のアルゴリズムでスコアリング（スタッツと呼ばれる数値で点数化）して提示し、生活習慣を見直すきっかけを得ることができる。

企業は、利用者の同意のもとで得た 54 分類 500 項目以上のパーソナルデータから利用者を分析し、マーケティングデータとして活用できる。また、利用者を様々なセグメントに分類して、1 人ひとりに最適なコンテンツを配信できる他、アンケート機能を活用して利用者のニーズをより深掘りすることができる。（図 6-2-2）[9]

図 6-2-2：FitStats のサービスの流れ

- 取り扱う情報について

FitStats で取り扱われる情報については以下の通りである。なお、FitStats では提供するデータおよび提供先の企業についても事前に選択をすることが可能となっている。（企業例：エフエム東京、DNP 等）

基本情報：性別、生年月日、住所（郵便番号、都道府県）等
食事：食事習慣（3 食、食事量、早食いか否か等）、飲酒頻度、量等
運動：運動の頻度、片足で立てるか、運動に対する意識等
睡眠：睡眠前の習慣的事項、目覚めた後の状態、夢を見る頻度等
カラダ：喫煙習慣、首・肩の凝りの有無、腰痛の有無、歯の状態等
メンタル：現在のメンタル状況（ひどく疲れた、ヘトヘトだ、憂鬱だ等）
その他：歩数、運動記録、食事記録等（FiNC と呼ばれるフィットネスアプリと連携して収集）

[9] FitStats. https://fitstats.jp/

6.2.1.3　Miles

- サービス提供会社

  Miles Japan 株式会社

- サービス開始時期

  2019 年

- サービス内容

  Miles は米国発祥のサービスであり、日本では Miles Japan 株式会社がサービスを提供している。利用者は自身の歩行、運転等の移動距離に基づいてマイルと呼ばれるポイント（トークン）を付与され、溜まったポイントはオンラインストアの割引クーポン券やギフト券等と交換をすることが可能である。企業は Miles を通して、実店舗への来店促進、ブランド認知や新規顧客の獲得を得ることができる。（図 6-2-3）[10]

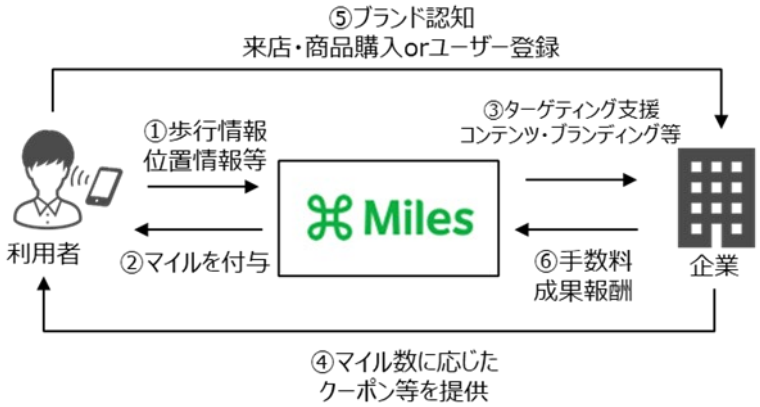


図 6-2-3：Miles のサービスの流れ

- 取り扱う情報について

  Miles では以下のような情報に基づいて、ポイントを付与している。

Miles は利用者が 1 マイル（1,609km）の移動するごとにポイントを提供する。 自動車 1 倍、バス・電車・スキー3 倍、自転車 5 倍、徒歩・ランニング 10 倍と移動手段によってポイントの付与倍率が変動（移動手段については AI で自動的に判定） 移動距離、使用マイル等で利用者のステータスがシルバー、ゴールド、プラチナ、ダイヤに振り分けられる（ステータスに応じて特典有（抽選へのエントリー上限、移動時のボーナスマイル付与、毎月獲得したマイルの内の数%をボーナスとして付与（シルバー 1 %、ダイヤ 4 %））等） ※マイルについては現金に換金することはできない

[10] Miles. https://www.getmiles.com/jp

6.2.1.4　　actcoin

- サービス提供会社

  ソーシャルアクションカンパニー

- サービス開始時期

  2019 年

- サービス内容

  actcoin はソーシャルアクションカンパニーが提供するサービスであり、利用者は社会貢献活動（電気をこまめに消す、駅前清掃に参加する等）を行うことによって actcoin と呼ばれるポイント（トークン）が付与され、溜まった actcoin でミュージカル無料招待への応募、プレゼント抽選への応募に利用することができる。企業としては、actcoin を活用することにより、SDGs や社会貢献活動への取組みについて対外発信、社会貢献活動関連のイベントに関して actcoin を通じて参加者を得ることができる。（図 6-2-4）[11]

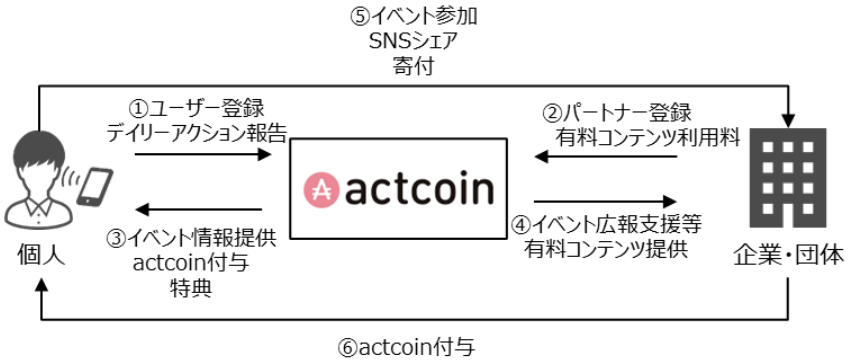


図 6-2-4：actcoin のサービスの流れ

- 取り扱う情報について

  actcoin では以下のような情報に基づいて、ポイントを付与している。

習慣：自ら実施すべき項目（デイリーアクション）を設定し、実施した際に報告をすると actcoin が付与される。（自己申告制（確認等無）、1 アクションで 100actcoin、1 日 17 個上限） イベント参加（渋谷駅前清掃活動、エシカルファッションサンプルモニター等）に参加することで actcoin が付与される。（イベントにより 1000、1500、3000 等 actcoin が付与（渋谷駅前清掃活動：1500、エシカルファッションサンプルモニター：1000）） 寄付：actcoin に記載のある寄付先（ウクライナ支援プロジェクト、社会と子どもを直接つなぐ奨学金等）に寄付をし、領収書を提示することにより寄付額と同額の actcoin が付与される ※　actcoin には換金機能等はなく、あくまでも同コミュニティ内におけるポイントに留まっている

[11] actcoin. https://actcoin.jp/

6.2.1.5　Intuit Mint

- サービス提供会社

  Intuit 社

- サービス開始時期

  2007 年

- サービス内容

  Intuit Mint は Intuit 社が提供する米国の家計簿サービスであり、利用者は自身のオンライン取引口座を登録することにより、Intuit Mint が利用者の取引情報を自動的に収集し、支出額等をカテゴリーごとに自動区分する。また、利用者は Intuit Mint から自身の取引情報をもとに利用者に適合した金融商品等の情報を得ることができる。

  企業は、金融商品の自動紹介機能から新規顧客の獲得および金融商品の情報を利用者に拡散することができる。（図 6-2-5）[12]

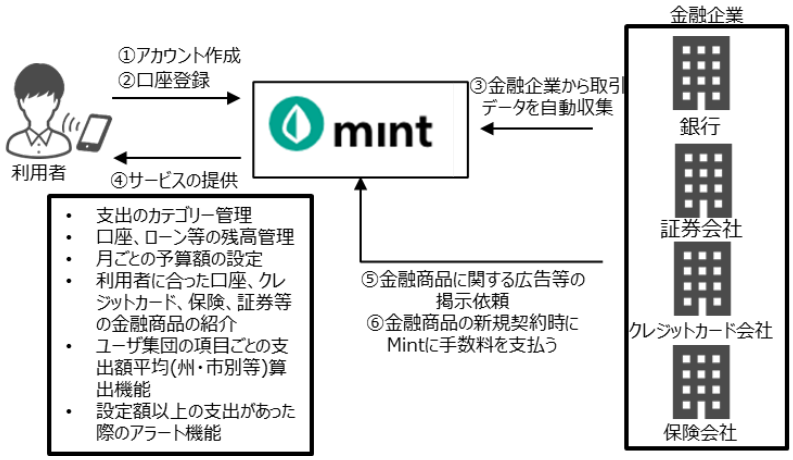


図 6-2-5：Intuit Mint のサービスの流れ

- 取り扱う情報について

  Intuit Mint で取り扱われる情報については以下の通りである。

アカウント作成時：メールアドレス、パスワード、居住国情報（米国・カナダ）、ZIP コード 口座登録時：オンライン口座のアカウント ID、パスワード 自動収集時：金融取引データ、金融資産データ ※利用者がこの他に Intuit 社の提供する納税申告補助アプリケーションである turbotax 等を使用する場合には氏名、住所等の個人情報の入力が必要となる（アカウント作成によって Intuit Mint だけでなく turbotax 等の他のサービスについても利用可能となる）

[12] mint. https://mint.intuit.com/

6.2.1.6　Patients Know Best

- サービス提供会社

  Patients Know Best

- サービス開始時期

  2008 年

- サービス内容

  Patients Know Best は英国の Patients Know Best 社が提供するパーソナルヘルスデータサービスであり、利用者は英国の保険システムである NHS と連携をして自身の診断結果、ウェアラブルデバイスから得られる体重や血糖値等の情報を一元的に管理でき、また、その記録を医療機関、家族等と共有することができる。（連携可能なウェアラブルデバイスは Fitbit、Polar、Withings、Strava 社等のデバイス約 90 種類であり、Apple 社の Apple Health とも連携が可能）

  医療機関はそれらの情報を活用することで、利用者の健康状態の把握、慢性疾患改善のための治療計画・助言を実施することが可能となる他、家族については利用者に対して介護等の必要な支援を行うことができる。（図 6-2-6）[13]

図 6-2-6：Patients Know Best のサービスの流れ

- 取り扱われる情報について

  Patients Know Best では以下のような情報が取り扱われている。

登録時：生年月日、メールアドレス、パスワード、セキュリティの質問、ジェンダー、住所
登録後：利用者の医療情報（検査結果、診断情報、投薬リスト、ケアプラン等）
ウェアラブルデバイス等：血糖値、体重、体温、心臓の測定値等
※ウェアラブルデバイスは Fitbit、Polar、Withings、Strava 社等のデバイス約 90 種類
※Apple 社の AppleHealth とも連携が可能
※PKB のサービスを利用する人全てがウェアラブルデバイスを装着する必要があるわけではない

[13] 医薬産業政策研究所.「グローバルにおける EHR・PHR 環境の特徴」.
https://www.jpma.or.jp/opir/news/068/07.html

6.2.1.7　ivido

- サービス提供会社

  ivido 社

- サービス開始時期

  2016 年

- サービス内容

  ivido は、オランダの ivido 社が提供するパーソナルヘルスデータを取り扱うサービスであり、利用者はかかりつけ医、専門医、薬剤師、その他の種類の医療提供者等の医療提供者から提供された医療情報（診断結果や投薬情報等）を PC、タブレット、スマートフォン等のデバイスで一元的に確認することが可能である。（英国の Patients Know Best と同様にウェアラブルデバイスのデータについても連携可能）

  また、ivido ではスマートフォンのアプリを経由し、患部の画像を医師と共有することで、皮膚疾患等の診断・治療をサポートすることが可能となっている。（図 6-2-7）[14]

図 6-2-7：ivido のサービスの流れ

- 取り扱う情報について

  ivido では以下のような情報が取り扱われている。

登録時：姓名、性別、生年月日、出生地、メールアドレス、住所
医療情報（診断結果、投薬情報等）
ウェアラブルデバイス等：体重、血圧、血糖値等
その他：アプリ経由で撮影した患部の画像等の状況

[14] ivido. “Wat biedt Ivido.” https://ivido.nl/

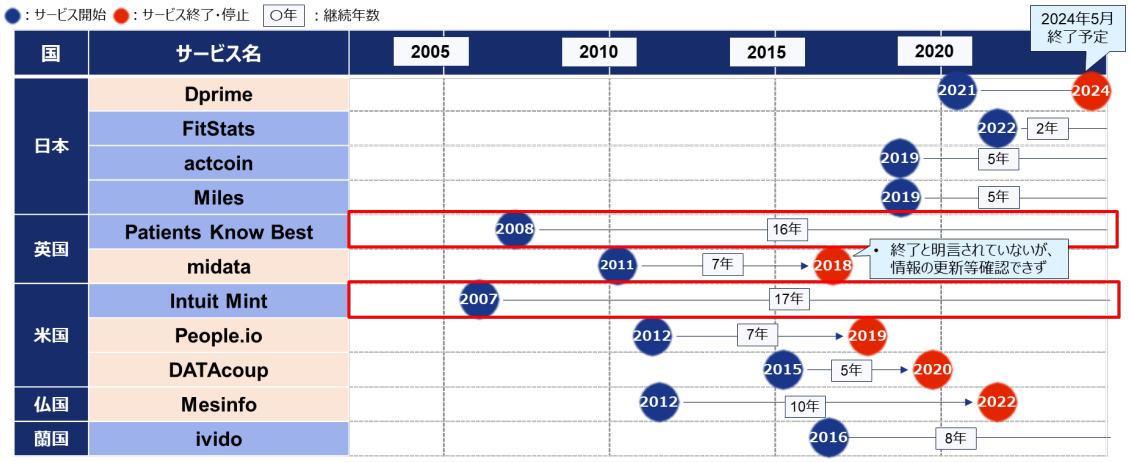
6.2.2　サービスの抽出

国内外のサービスを調査する中で、2010 年代前半に開始したパーソナルデータサービス（米国の DATAcoup、英国の People.io、政府主導の midata、フランスの Mesinfo 等のサービス）については 10 年以内に全てサービスが終了・停止してしまっていることが判明した。継続しているサービスについてもサービス開始から比較的期間が浅い、もしくはサービスが既に終了していることが判明した。

Dprime、FitStats、actcoin、Miles についてはサービス開始が 2020 年前後であり、サービス開始からまだ数年しか経過をしていない。（オランダの ivido についても 8 年）[15]（表 6-2-1）

これらの結果から深掘り調査をするサービスとして比較的長期間（10 年以上）サービスを継続している Patients Know Best（16 年間サービス継続）、Intuit Mint（17 年間サービス継続）を深掘り調査の対象サービスとして抽出した。

表 6-2-1：パーソナルデータサービスのサービス開始・終了（停止）時期



[15] 英国の midata については、明確に終了と明言をされているわけではないが、2018 年以降大きな更新等確認できず、また moneyraters の記事（https://www.moneyraters.com/blog/what-is-midata/ ）では、midata の失敗の要因についての記載がある等サービスとして上手くいかなかった可能性が高い。

6.2.3 深掘り調査結果

6.2.3.1 Patients Know Best

- ビジネスモデル(図 6-2-8)

【ステークホルダ/マネタイズ】

- Patients Know Best は大きく①患者、②介護者（家族等）、③専門家・組織（医療従事者等）という 3 つのステークホルダによってサービスが成立している。
- 患者は専門家・組織からの紹介等で Patients Know Best に登録し、無料でその機能を利用することができる。
- 介護者についても無料で、Patients Know Best の機能を利用することができる。
- 専門家・組織は、Patients Know Best にサービス利用料を支払うことにより、患者の医療情報の共有等の機能を使用することができる。
- Patients Know Best は、専門家・組織からのサービス利用料によって主に収益を得ている。

【インセンティブ】

- 患者については無料で Patients Know Best サービスを利用でき、医療情報の一元的な管理・共有の機能の他、医師からの助言や治療計画の提供、病院の予約等の医療的なサポートを受けることができる。
- 介護者については、Patients Know Best を無料で利用でき、自身の要介護者に関する医療情報が共有されることにより、必要となる介護処置を把握、実施することができる。
- 専門家・組織についてはサービスを利用することにより、アナログ等で大きな負担となっていた慢性疾患患者の経過観察等をオンラインで実施することができ、慢性疾患等の治療・改善に取組みやすくなる。
- また、専門家・組織の内、かかりつけ医（GP）については英国の医療保障制度である NHS の診療報酬システム 16の関係から Patients Know Best のようなサービスを活用することにより、患者の診療所の定着、新規患者の獲得が見込むことが可能となる。

[16] 2.3.1.2 サービス環境参照

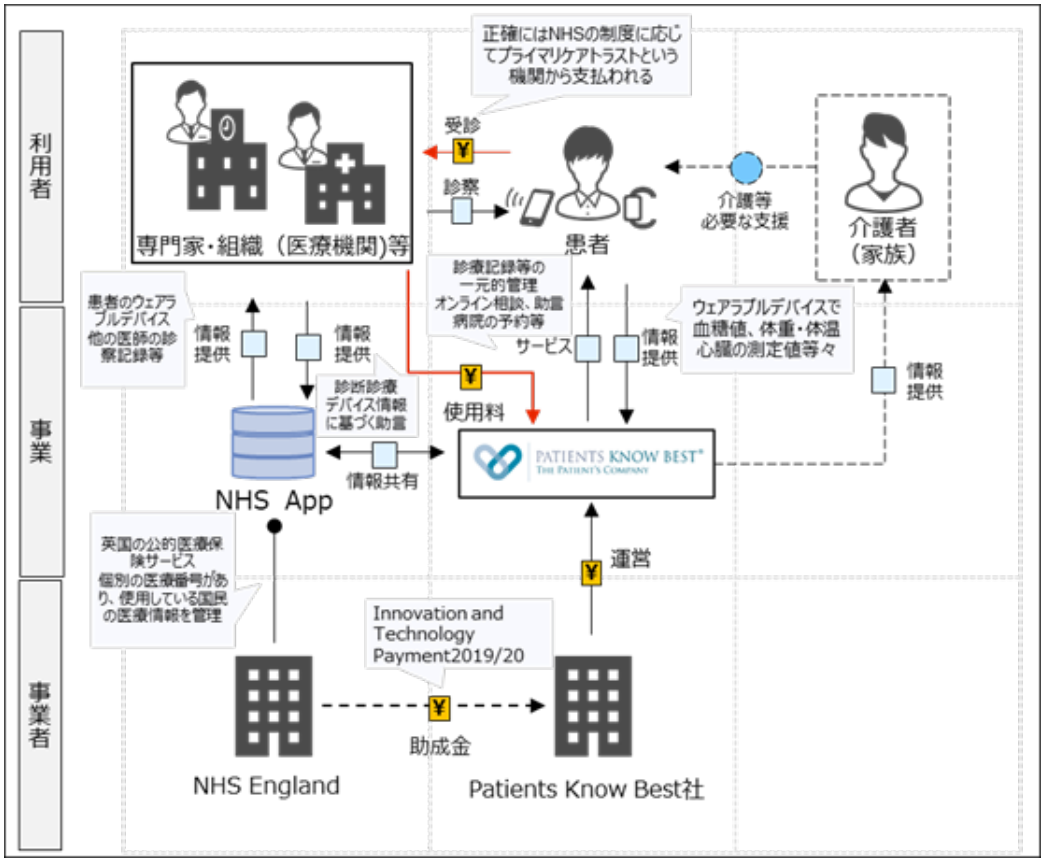


図 6-2-8：iPatients Know Best のビジネスモデル

● サービス環境 [17]

【政策（制度を含む）】

英国の国民保険サービス制度（National Health Service：NHS）では、全ての国民を対象にしている部分や国民に対する医療負担が原則無料である（薬剤費として処方 1 件につき 7.65 ポンドの一部負担あり（60 歳以上、16 歳未満、低所得者世帯等は免除））等では、日本の医療制度（全ての国民を対象で、医療費は無料ではないが少ない負担で受診可能（年齢によって 1～3 割の患者負担が必要）と大きな差異はないが、受診および医者の診療報酬制度に関して大きな差異が確認できる。

まず受診面について、日本では「フリーアクセス制」となっており、個人が保険証を所持していれば、日本全国のどこの医療機関でも医療保険制度の適用を受けつつ、自由な受診が可能となっているが、英国では「登録制」となっており、全ての英国国民は自分のかかりつけの診療所を登録し、救急の場合以外、その診療所の一般医（General Practitioner：GP）の診察を受けなければならない。簡単な治療の場合はかかりつけの診療所で処置を受け、更なる詳しい検査や入院等の高度な医療サービスが必要な場合は病院が紹介される。（かかりつけ診療所の登録はいつでも変更可能である）

診療報酬制度については、日本は出来高払い制度で、診療行為ごとに全国一律の点数（1 点＝

[17] 田畑雄紀.「イギリス医療保障制度の概要 ―日本の制度との違いについて―」.
https://www.kansai-u.ac.jp/Keiseiken/publication/seminar/asset/seminar12/s196_1.pdf

10 円）が定められており、それに基づいて医療費を請求する制度となっているが、英国の診療所については人頭報酬制度となっており、基本的に医療提供者が受け持つ患者の人数に基づいて、資金配分が行われる制度になっている。（出来高払い制度として、かかりつけ医が自身の得意分野を生かし、簡単なケガの治療や慢性病などの治療をすると支払われる追加報酬や、診療所の環境改善、定められた疾病に対するサービスの質の改善を行うと、その成果によって報酬が得られる制度もある）

【社会動向面 [18]】

英国では 1990 年代から医療情報の IT 化に関して注力をし始め、2002 年に「NHS 内の患者情報統合を目的とした国家プログラム（National Programme for IT：NP f IT）」を皮切りに医療情報の IT 化に注力した政策も開始された。NP f IT は、予算の肥大化を理由に 2011 年に廃止されているが 2016 年には「NHS のペーパレス化」インフラと「社会保障改革」を含む NIB の枠組み支援に 42 億ポンドを拠出することを発表する等、国として IT 化への再注力が行われている。

国のそれらに対する資金援助等の支援の結果 2018 年時点で英国の電子カルテ（Electronic Medical Record：EMR）の普及率は 95%以上（日本の普及率は 2020 年時点で約 57%）となっており、ほぼ全てで医療情報の IT 化が完了している。

- トラスト（ガバナンス）

【法令】

Patients Know Best では英国の個人情報保護法令である UK GDPR に準拠している。[19]

【対象事業者】

UK GDPR については、以下の事業者を対象としている。（表 6-2-2）

① 英国内に拠点があり、英国内の管理者または処理者の拠点の活動に関連した個人データの処理を行う事業者
② 英国外に拠点を持ち、英国に所在するデータ主体に対する商品またはサービスの提供に関連して行われる個人データの処理を行う事業者もしくは、英国内で行われるデータ主体の行動のモニタリングに関連して行われる個人データの処理を行う事業者

[18] 厚生労働省.「諸外国における医療情報連携ネットワーク調査」.
https://www.mhlw.go.jp/content/10808000/000685923.pdf

[19] 日本貿易振興機構.「『英国一般データ保護規制（UK GDPR）』実務ハンドブック」
https://www.jetro.go.jp/ext_images/_Reports/01/b0226c404f93f434/20220001rev1.pdf

表 6-2-2：UK GDPR の適用関係

拠点	適用対象となる処理	適用されるケースの例
英国国内に拠点あり	①英国国内の管理者または処理者の拠点の活動に関連した個人データの処理	日本国内の事業者 B が欧州を含めたグローバルな市場に対して EC サイトを展開（当該 EC サイトに関するデータ処理はすべて米国内のサーバ上で実施）、当該事業者 B の兄弟会社 C（EC サイトの運営主体ではない）が、欧州市場に対するマーケティングキャンペーンを主導し、これにより日本国内の事業者 B が欧州市場から収益をあげている。
英国国内に拠点なし	②英国国内に所在するデータ主体に対する商品またはサービスの提供に関連して行われる個人データの処理	■ 日本国内の事業者がゲームアプリを英国国内所在のプレイヤーに配信し、プレイヤーの氏名・課金履歴等を収集 ■ ポンド決済可能で英語表記があり、英国向け配送に言及している EC サイトで顧客の住所・氏名・口座情報等を収集 ■ 日本国内の事業者/非営利団体 A が、英国国内所在の個人に対してメールマガジンを配信するため、氏名・メールアドレス等を管理
	③英国国内で行われるデータ主体の行動のモニタリングに関連して行われる個人データの処理	■ 日本国内の事業者が英国国内に所在する個人から、アプリで位置情報を取得して分析 ■ 日本国内の事業者が Web サイト上からクッキー情報を取得して個人の嗜好等を分析して行動ターゲティング広告を配信 ■ 日本国内の事業者が、ウェアラブル端末（スマートウォッチ等）を通じて英国国内に所在する個人の健康関連情報を取得・管理

【対象となる情報】

UK GDPR では特定された、もしくはされ得る個人に関係する情報を「個人データ」として法令の対象としている。

また、以下のような情報については「特別カテゴリーの個人データ」として分類し、そのデータの処理を原則として禁止するとともに、処理の要件として 10 個の条件を課している等、その管理・処理について通常の個人データ以上の制限を設けている。

(特別カテゴリーの個人データ)
人種・民族的出自、政治的意見、宗教・思想上の信条、労働組合への加入を明らかにする個人データの処理、遺伝子データ、自然人を一意に識別することを目的とする生体データ、健康に関するデータ、自然人の性生活もしくは性的指向に関するデータ等
(特別カテゴリーの個人データの処理のための要件)
①明示的な同意、②雇用、社会保障、社会保護、③重要な利益、④非営利団体、⑤データ主体によって公開されたもの、⑥法的請求または司法行為、⑦実質的な公共の利益の理由、⑧健康または社会的ケア⑨公衆衛生⑩アーカイブ、研究、統計

【同意】

UK GDPR では、原則オプトインを採用しており、個人データの全処理において、データ主体の明示的な同意が必要となる（13 歳未満については親等の同意が必要）。

【本人への情報提供等】

UK GDPR では、個人データを処理するにあたり、データ主体に対して直接収集の場合は収集時点
間接収集の場合は収集後遅くとも 1 か月内に以下の事項について情報提供を行う。

処理目的、処理の適法性の根拠、（間接収集の場合）収集個人データのカテゴリー、受領者（提供先）のカテゴリー、域外移転の有無と根拠、保存予定期間または決定基準、データ主体の権利内容、（間接収集の場合）情報源、自動意思決定の有無と処理ロジック 等

【本人の権利】

個人データのデータ主体である本人には以下のような権利が認められている。

開示請求権（アクセス権）、訂正請求権、消去請求権、処理制限権、データ・ポータビリティの権利、処理禁止権（異議申立権）、完全自動意思決定に服さない権利

【罰則】

また、事業者が遵守しなければならない規制が定められており、違反をすると①1、750 万ポンド以下または事業者である場合は前会計年度の全世界年間売上高の 4%以下のいずれか高い方（83 条 5 項）と、②870 万ポンド以下、または事業者である場合は前会計年度の全世界年間売上高の 2%以下のいずれか高い方（83 条 4 項）の 2 つの上限レベル内で制裁金が課される。（表 6-2-3）

表 6-2-3：UK GDPR の義務および罰則について

UK GDPR 上の諸義務（組織が遵守しなければならない UK GDPR の規制）
①1,750 万ポンド以下または事業者である場合は前会計年度の全世界年間売上高の 4%以下のいずれか高い方
1. データ処理に関する原則を遵守する義務（5 条） 2. 適法に個人データを処理する義務（6 条） 3. 同意の条件を遵守する義務（7 条） 4. 特別カテゴリーの個人データ処理の条件を遵守する義務（9 条） 5. データ主体の権利およびその行使の手順を尊重する義務（12-22 条） 6. 情報通知義務（13、14 条） 7. 個人データの移転の条件に従う義務（44-49 条） 8. ICO の命令に従う義務（58 条 1 項、2 項）
②870 万ポンド以下、または事業者である場合は前会計年度の全世界年間売上高の 2%以下のいずれか高い方
9. 16 歳未満の子どもに対する直接的な情報社会サービスの提供に関する個人データの処理に、子どもの保護責任者による同意または許可を取得する義務（8 条） 10. 適切な技術的・組織的な対策を実施する処理者を利用する義務（28 条） 11. 設計によるデータ保護・デフォルトとしてのデータ保護を確保するために適切な技術的措置および組織的措置を実装する義務（25 条） 12. 該当する場合、英国代理人の選任義務（27 条） 13. 責任に基づいて処理行為の記録を保持する義務（30 条） 14. ICO に協力する義務（31 条） 15. 適切なセキュリティレベルを保証する適切な技術的・組織的な対策を実施する義務（32 条）

16. データ侵害通知義務がある場合、当局への通知義務およびデータ主体への通知義務（33条、34 条）
17. 該当する場合、データ保護影響評価を実施する義務（35 条）
18. 影響評価において緩和できないリスクがあった場合の当局への事前相談義務（36 条）
19. データ保護責任者の選任義務、およびその職や役務を尊重する義務（37 条から 39 条）

● 利用規約

【規約への同意】

Patients Know Best では利用者（患者等）は、サービスの開始時に利用規約に同意をするが、Patients Know Best が規約を変更した場合、サービスの利用を継続することにより、変更後の規約に同意したと見なされる他、規約の変更を通知し、通知後 30 日以内に拒否の申し出がない場合も、利用者が規約の変更を承諾したものを見なされる。

【禁止事項】

利用規約において、以下のような禁止事項が設定されており、Patients Know Best ではこれらの規定違反に対して、直接の規程は定められていないものの、利用規約内に任意の理由で、予告なしに利用者のサービス利用をキャンセル、一時停止できる旨記載があるため、違反行為に対しては、そのような処置をとられる可能性がある。

- **スパムの使用**：未承諾の一括メッセージや商用メッセージ（スパム）からリンクされた宛先としてサービスの一部を使用する行為
- **自動化されたプロセスの使用**：ボット、スパイダー、定期的なキャッシュ、メタ検索などの自動化されたプロセスやサービスを使用してサービスにアクセスする行為
- **サービスの不正変更や迂回**：サービスを変更、迂回する、またはそのような行為を試みる不正な手段の使用する行為
- **サービスへの損害や妨害**：サービスや関連するネットワークに損害を与える、使用不能にする、過度な負担をかける、障害を与える、または他者のサービス利用を妨害する行為
- **再販や再配布**：サービスまたはその一部を再販、再配布する行為
- **ソフトウェアの使用制限**：本サービスに含まれるソフトウェア、コード、スクリプト、またはコンテンツについて、法律で明示的に許可されている範囲を除く行為（①コピー（複製）、②逆アセンブル（分解）、③逆コンパイル（元のソースコードに戻すこと）、④リバースエンジニアリング（逆工学））

【サービス提供者の責任】

Patients Know Best では、利用者の損失に関して、Patients Know Best 側に問題があり、直接的被害が発生した場合にのみ損害賠償をするとの規程が定められており、間接的な理由等での損失については責任を負わないと規定されている。

また、Patients Know Best のサービスについてはサービスを「現状有志」、「すべての欠陥あり」、「利用可能な状態」で提供し、サービスの可用性や情報の正確性、適時性に関して保証をしていない（所

不応の正確性については専門家・組織等の医療情報提供者に依存していると記載）。

- プライバシーポリシー

【収集する情報】

Patients Know Best では、プライバシーポリシーにおいて以下のような情報を収集するとしている。

【基本情報】 名前、メールアドレス、IP アドレス（コンピューターの場所）患者の健康記録 一般的な健康（例：糖尿病等）、性的健康（例:性感染症）、メンタルヘルス（例：うつ病など）、社会的養護に関する情報（例:デイセンター）（これら専門家が PKB レコードを通じて記録し、患者の PKB アカウントで患者と共有した情報をプロバイダー提供データという） 【その他】 患者が自身で PKB アカウントに追加し、利用者のケアを提供する専門家および患者が選択したその他の人に表示されるようにすることを選択した情報

【情報の使用】

Patients Know Best では、サービスの提供および更新や通知等のサービスに関する重要な情報を提供、PKBのメールマガジンを送信するため（受信を選択した場合）、年齢と居住地を特定し、PKBアカウントの基準を満たしているかどうかを判断するために情報が使用される可能性があると規定している。

【情報の共有】

Patients Know Best では、情報の共有について、サポートデスクなどのサービスを当社に代わって提供したり、本サービスに関する問い合わせに回答したりするために、企業と契約する場合があるとの記載があるが、それらの情報提供先には IP アドレスやメールアドレスなど、問い合わせに役立つ最小限の個人情報のみへのアクセスを提供し、暗号化された健康情報にアクセスすることはできない状態にすると規定している。

【データの削除】

Patients Know Best では、取り扱う情報が医療情報であり、記録の削除については、専門家・組織側からの要求に応じてのみ対応すると規定されており、患者が削除を要求できるのは専門家・組織側が閲覧していない患者が追加した情報のみである。

- 標準規格（ISO27001）

【認証内容】

ISO27001 は情報セキュリティマネジメントシステムの規格であり、組織が情報セキュリティリスクを管理し、ビジネスプロセス、情報技術システムおよびデータセキュリティを保護するための枠組みを提供している。ISO27001 の取得企業数は、2022 年の統計で中国（26,301 件）、日本（6,987 件）、英国

（6,084 件）の順で多く、米国については 4 番目（1,980 件）に位置している。[20,21]

ISO は 27001 以外にも ISO9001（品質マネジメントシステム規格）や ISO14001（環境システムマネジメント規格）等多くの規格があり、多くの企業は、特定のマネジメントシステム等に関する組織の体制強化や内外への信頼の獲得の手段として活用している。

【利点】

認証を取得することにより、情報漏えい等の情報リスクの低減や、社員の情報セキュリティ意識・モラルの向上、業務効率の改善や組織体制の強化、組織内外からの信頼獲得等の利点を獲得することができる。

【取得要件】

ISO27001 の認定取得のために、以下のような要件を満たす必要がある。

- 組織的管理策：情報の分類、情報セキュリティインシデント計画策定および準備 等
- 人的管理策：選考時のセキュリティ審査、情報セキュリティの意識向上、教育および訓練 等
- 物理的管理策：物理的セキュリティ対策、装置の物理的保護・管理 等
- 技術的管理策：アクセス制御、暗号化、ネットワークセキュリティ 等

【取得方法】

認証を取得するには、必要な書類や体制等を整備した後、ISO27001 の認証機関（複数あり）に申請を行い、2 度の審査（ファーストステージ審査：文書審査が中心、セカンドステージ審査：マネジメントシステムの実施状況評価等）に合格する必要がある。

また、認定取得後も 1 年に 1～2 回の維持審査、3 年に 1 度の更新審査を受ける必要がある。

【取得費用】

ISO27001 の取得費用は、従業員数、拠点数、業種等によって約 50 万円から約 120 万円程度まで変動をする。（更新審査の際にも数十万の費用がかかる）

● テクノロジー

【DID/VC 等の技術の有無】

Patients Know Best のサービスについて、DID/VC 等の Trusted Web 関連の技術の使用については確認できなかった。

【使用している技術】

Patients Know Best では、情報セキュリティのために以下のようなテクノロジーが使用されている。

---

[20] 一般財団法人.「ISO/IEC 27001（情報セキュリティ）」.
https://www.jqa.jp/service_list/management/service/iso27001/

[21] International Organization for Standardization. “The ISO Survey.”
https://www.iso.org/the-iso-survey.html

- 多要素認証
  - メールアドレス、パスワードの他、ワンタイムパスワードについても使用。また NHS のログイン情報を使用して本人確認を実施
- セキュリティについても NHS App のセキュリティに依拠
- NHS 独自のシステムの使用
  - 患者が自分で家族や医療従事者の中から、自己管理医療記録を共有する相手を決定でき、全データが独自の手法で暗号化され、「Health and Social Care Network (HSCN)」というネットワークに保管されているため、承認された者以外は閲覧することができない
- HSCN
  - インターネットへの単一の接続を持つ代わりに、組織はインターネット接続を提供する多くの HSCN コンシューマーネットワークサービスプロバイダー(CN-SP)の 1 つを介して接続する。その結果、CN-SP を介してより高速で安価なインターネット接続を取得でき、安全性の低い、または監視されていない追加のローカルインターネット接続を取得する必要がなくなる
  - 最も高度なネットワークセキュリティの脅威から組織を保護する NHS セキュアバウンダリーインターネットフィルタリングサービスを作成
  - 次世代ファイアウォール(NGFW)、Web アプリケーション ファイアウォール (WAF)を使用してデジタルおよびクラウドベースの脅威から保護
  - HSCN ネットワーク分析サービス(NAS)による異常動作警告分析
  - HSCN DNS による悪質な Web サイト等のブロック
  - NHS デジタルセキュリティセンターによる悪意ある活動やマルウエアを利用者に通知

6.2.3.2 Intuit Mint

- ビジネスモデル(図 6-2-9)

【ステークホルダ/マネタイズ】

Intuit Mint は大きく①利用者、②関係企業の 2 つのステークホルダによってサービスが成立している。

利用者は無料でアカウントを作成し、自分が利用しているオンライン取引口座等を登録することで Intuit Mint により取引情報等が自動収集され、支出額がカテゴリーごとに自動的に区分される。（現金での支出については手入力が可能）

また、利用者は、関係企業が Intuit Mint に提供する金融商品について、自動収集された取引情報を基に利用者本人に適した金融商品を抽出し、紹介することができる。

Intuit Mint は、関係企業からの金融商品を広告に掲示するための広告料と、利用者がその企業の金融商品を購入した際の紹介料で収益を得ている他、iOS のアプリ限定で、広告削除等のサービスを提供する有料機能により収益を得ている。

【インセンティブ】

利用者については、Intuit Mint を無料で利用でき、1 つのアプリケーションで複数口座の取引情報を一元管理できる他、月ごとの予算額の設定、設定額以上の支出があった際のアラート機能、自分の金

銭状況に適合した金融商品の情報が受け取ることができる。

企業については、Intuit Mint を活用することにより、企業が拡散したい金融商品に関する広告の掲示および各利用者の金銭状況に適した金融商品が紹介される機能により、情報の拡散と新規顧客の獲得が可能となる。

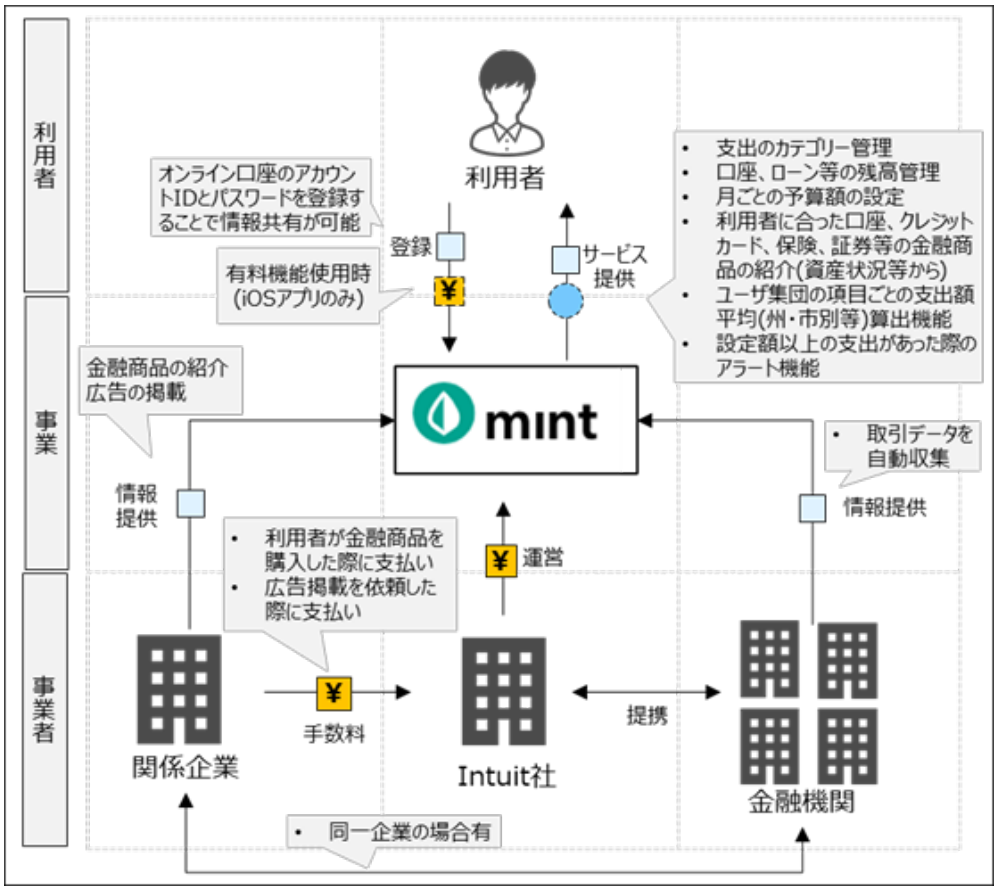


図 6-2-9：Intuit Mint のビジネスモデル

● サービス環境

【政策（制度含む）】

米国における確定申告に関して、日本では、給与取得者の多くは、雇用している会社が年末調整により年間の納税額を見直し、源泉徴収で調整を実施するため、自ら確定申告を行う必要はないが（自営業者を除く）、米国の場合、日本とは異なり、給与取得者、自営業者、投資所得者等、収入があった者は原則として、自ら連邦と州の税務当局の両方に確定申告を行う必要がある。

そのため、日本では自ら確定申告を行う必要がないため、それらにかける時間が少ないのに対して、米国では電子申告（e-file）等を活用しても、確定申告に係る時間は平均して 13 時間とかなりの時間を要する。

【社会動向面】

Intuit Mint が 2007 年にサービスを開始した直後、2008 年 9 月にリーマンショックと呼ばれる経済

危機が発生した。米国内では金融機関の破綻、株価の大幅な下落や失業率の上昇というような状況に陥り、米国において将来に備えた貯蓄や賢い消費方法について、真面目に考えるような倹約施行を持った消費者が増加した。[22]

- トラスト

【ガバナンス】

米国では個人情報保護全般の統一的な法令はなく、分野ごとに制定された個人情報法令もしくは州法で個人情報の保護を行っており、Intuit Mint についてもて金融分野の個人情報保護法令であるグラムリーチブライリー法（Gramm-Leach-Bliley Act：GRBA）および Intuit 社の所在するカリフォルニア州のカリフォルニア州プライバシー権法（California Privacy Rights Act：CPRA）に準拠している。

- 法令（GRBA）

【対象事業者】

GRBA では、以下の事業者を対象としている。

金融機関（銀行、証券会社、保険会社等） その他（**サービスプロバイダー**（金融機関にサービス提供し、顧客情報にアクセスできる企業））

【対象となる情報】

GRBA では個人を特定できる金融情報を「非公開個人情報」として保護の対象としている。「非公開個人情報」には、氏名、住所等の個人情報、銀行口座番号、クレジットカード番号等の財務情報、顧客が金融機関と行った取引情報や信用情報等が該当する。

【同意】

GRBA は、原則としてオプトアウトを採用しており、非公開個人情報を第三者の非関連企業と共有する場合、消費者はこの情報共有から自身を除外する権利、つまりオプトアウトする権利を持つ。金融機関は消費者に対して、そのような情報共有が行われる前に通知を行い、オプトアウトする方法を提供する必要がある。

また、消費者の個人情報がマーケティング目的で金融機関の外部の第三者と情報を共有する場合には消費者に対して事前に積極的な同意を得るオプトインが採用される。

【本人への情報提供等】

GRBA では情報共有にあたり事前および定期的に以下の事項について情報提供をする。

個人情報の収集（目的や範囲等）に関する情報、共有（制限等含む）に関する情報、具体的な保護措置に関する情報、苦情処理の手続きに関する情報等

[22] 小泉雄介.「パーソナルデータ保護の最新動向と利活用に向けた取組み」.
https://www.glocom.ac.jp/wp-content/uploads/2015/03/20150423koizumi.pdf

【本人の権利】

GRBA では消費者に対してプライバシー通知の受け取り権利、オプトアウト・オプトイン権、訂正請求権のような権利が認められている。

【罰則】

グラムリーチブライリー法では不正アクセス等で個人の情報を取得したものまたは取得を試みた者に対して、罰金もしくは 5 年以下の懲役が課され、また米国の他の法律に違反または 12 カ月間に 10 万ドルを超える違法行為の一部として不正アクセス等の行為を行ったものについては25万ドル以下または50万ドル以下の 2 倍の罰金または 10 年以下の懲役またはその両方が課される。

また、Intuit Mint ではグラムリーチブライリー法以外にカリフォルニア州法等を適用しているが、グラムリーチブライリー法と州法の競合については、州法の遵守がグラムリーチブライリー法の要件と矛盾する場合に限り州法を免除し、州法がグラムリーチブライリー法の下で提供される保護よりも大きな保護を個人に提供する場合は、州法は矛盾すると見なされず、州法が適用される。

- 法令（CPRA）[23,24,25]

【対象事業者】

CPRA は、どこを拠点とするかに関わらず、特定の条件（年間の総収入が 2、500 万ドルを超える、10 万件以上の消費者・世帯の個人情報を取り扱う、年間売上高の 50%以上を消費者の個人情報の販売あるいは共有から得ている企業）を満たし、カリフォルニア州の共住者の個人情報を取り扱う企業を対象としている。（単に事業目的で取得しただけの個人情報はカウントされない）

また、上記に該当する事業者を支配し、または支配されており、かつその事業者と共通のブランドを有し、その事業者と個人情報を共有する事業者、その事業者が少なくとも 40%の持分を有する事業者で構成されるジョイントベンチャーやパートナーシップについても CPRA の規制の対象となっている。

【対象となる情報】

CPRA では特定の消費者・世帯に関連付けできる情報を「個人情報」として定義している。また、それらの情報の中でも以下のような情報は、「機微個人情報」として定義され、その情報の使用、開示には消費者の明示的な同意を得なければならない等の取り扱いについて通常の個人情報以上の制限が設けられる。

（機微個人情報）

[23] 杉本武重.「GDPR・CCPA・CPRA の主要論点比較」.
https://www.jetro.go.jp/ext_images/biz/seminar/2021/2e7c9eec1a269310/3.pdf

[24] なおカリフォルニア州プライバシー権法（CPRA）の最終規則に基づく執行を当初の予定である 2023 年 7 月 1 日から 2024 年 3 月 29 日まで延期する判決が出しているため、CPRA が完全に適用されるのは 2024 年 3 月 29 日からとなる

[25] 日本貿易振興機構.「米カリフォルニア消費者プライバシー改正法の最終規則に基づく執行、2024 年 3 月 29 日まで延期」. https://www.jetro.go.jp/biznews/2023/07/cb6458663bddfb07.html

社会保障番号、運転免許証番号、州の身分証明書番号、パスポート番号、消費者のアカウントログイン、財務に関する情報、正確な位置情報、人種、民族的起源、宗教的信念、組合員資格、個人の性生活や性的指向、遺伝的データ等

【同意】

CPRA は、原則としてオプトアウトを採用しており、個人情報の販売・共有について、企業が消費者に対してオプトアウトする権利およびその方法について明示する必要がある。

また、原則的にはオプトアウトであるが、「機微個人情報」や 16 歳未満の消費者の個人情報の販売・共有については必ず、事前に消費者本人からの明示的な同意が必要となる。（13 歳未満については親等からの同意が必要となる）

【本人への情報提供等】

CPRA では、情報の直接収集の場合には収集時および事前通知で、間接収集の場合は事前通知により以下の事項について消費者本人へ情報提供する。

(収集時（もしくは事前）通知】 収集個人情報のカテゴリー、収集・利用目的、販売・共有の有無、保存予定期間・決定基準 (プライバシーポリシー等での公表) 過去 12 ヶ月間の収集情報、情報源のカテゴリーと収集目的、過去 12 ヶ月間の販売・共有、情報と販売・共有先のカテゴリーと目的、16 歳未満の情報販売・共有の認識等

【本人の権利】

CPRA では、消費者は以下のような権利を有する。

開示請求権、訂正請求権、削除請求権、販売・共有オプトアウト権またはオプトイン権、機微個人情報の利用・開示制限権、データ・ポータビリティの権利、自動意思決定に関する開示請求権、権利行使を理由に差別・報復されない権利

【罰則】

CPRA に違反した場合、違反件数 1 件につき最大 2,500 ドルの罰金が科される。またその違反が故意である場合には最大 7,500 ドルまで金額が増える。

16 歳未満の消費者の個人情報に関連する違反については故意等関係なく 7,500 ドルの制裁金が科される。

【法令（その他）】

Intuit Mint では GRBA、CPRA の他に利用者が居住する州によって、各州の個人情報保護関連法令が適用される場合がある。該当する州に居住している利用者には、以下のような権利が認められる。ただし、これらの権利については絶対的なものではなく、場合によっては法律に則り要求を拒否する場合もある。（表 6-2-4）

表 6-2-4：UK GDPR の義務および罰則について

州	内容
コロラド州 居住者	コロラド州プライバシー権法（CPA）が適用 コロラド州居住者として、利用者には以下の権利がある（ただし、これらの権利は絶対的なものではなく、場合によって、法律で認められているように、利用者の要求を拒否する場合あり） 利用者は Intuit アカウント内の個人情報のアクセスおよびコピーの請求 個人情報の編集・修正 個人情報の削除を要求する権利 利用者はターゲット広告を目的としたトラッキングおよび個人データの自動処理（プロファイリング）のオプトアウトを要求する権利 利用者の同意なしに機密性の高い個人情報を処理しない 利用者は CPA 行使に関連する差別または報復を受けない 利用者が Intuit のアカウントを持っていない、またはアカウントが利用者の許可なくアクセスされた疑いがある場合、確認のために追加の個人情報の提供をお願いする可能性あり
コネチカット州 居住者	コネチカット州データプライバシー法（CDPA）が適用（内容についてはコロラド州プライバシー権法と同様）
バージニア州 居住者	バージニア州消費者データ保護法（VCDPA）が適用（内容についてはコロラド州プライバシー権法、コネチカット州データプライバシー法と同様）
カナダ 居住者	カナダ居住者には以下の権利がある プライバシー設定の更新：利用者は、アカウントの設定でプライバシー設定の変更が可能 マーケティングコミュニケーション管理：利用者は、マーケティング設定ツールで、マーケティング E メール等の配信停止等可能 オプトアウト：利用者はサービスとして提供されているインタレストベースの広告配信に使用される個人情報のオプトアウトを要求できる 個人情報のアクセス・修正・削除：利用者は、自身の個人情報へのアクセス、修正、削除の要求が可能（ただし、利用者の個人情報を保持する業務上の必要性がなくなった場合） 同意の撤回：利用者は、個人情報の収集、使用、開示に対する同意をいつでも削除可能 苦情申し立て：利用者は、Intuit による利用者の個人情報の収集・処理について該当するプライバシーコミッショナーに苦情を申し立てる権利がある

- 利用規約

【規約への同意】

Intuit Mint においてはアプリケーションの利用やアクセスをすることにより、利用規約の各規定やプライ

バシーポリシー、18 歳以上であること、Intuit 社と法的拘束力のある契約を締結できること等に同意したとみなされる。

Intuit 社によって利用規約が変更された場合も、アプリケーション等の利用を継続すると、変更後の新規約に同意したと見なされる。

【禁止事項】

Intuit Mint では以下のような禁止事項が規定されており、これらに違反した場合にはアカウント停止、終了の措置、他の利用者に損害等が発生し、訴訟となった場合には違反した利用者にその責任が課せられる等の処分がある。

【禁止事項】
法律や規制に違反する行為、中傷的、わいせつな、攻撃的なコンテンツの投稿や共有、ウイルスや有害なソフトウェアの送信、スパムや未承諾の広告の送信、Intuit になりすます行為、プラットフォームの不正な複製・変更・再販、リバースエンジニアリングや逆コンパイルの試み、不正アクセス・妨害、バックアップ目的でのプラットフォームの使用、他者を奨励または支援して契約違反をする行為、著作権を侵害する行為

【サービス提供者の責任】

Intuit Mint では、利用者の損失に関して、Intuit Mint 側に問題があり、直接的被害が発生した場合にのみ損害賠償をするとの規程が定められており、間接的な理由等での損失については責任を負わないと規定されている。

また、Intuit Mint のサービスについてはサービスを「現状有志」で提供しており、データ損失や本プラットフォームの正確性、信頼性、可用性、利用可能なコンテンツや情報に関しては保証をしないと規定している。

- プライバシーポリシー（Intuit 社グローバルプライバシーステートメント）

【収集する情報】

Intuit Mint では以下のような個人情報を収集する可能性があると規定している。

- 利用者が Intuit に提供する可能性のある情報（サービスによって使用する等の差有）
  - 連絡先データとアカウントプロファイルデータ（アカウント作成時に要求する情報等）、本人確認情報（氏名、生年月日、社会保障番号等）等
- 第三者の情報源から取得される可能性のある情報
  - リンクされたサービス、本人確認プロバイダー、カスタマーサポートプロバイダー、信用情報機関等から得られた情報
- 自動データ収集される情報
  - デバイス情報、利用情報、位置情報、ローカルに保存された情報、通信インタラクションデータ、オンライン行動、データクッキー、生体情報等（事前の通知と同意のもとに収集）

【情報の使用】

Intuit Mint では収集した個人情報について、以下のような場合に使用されると規定している。

サービスの提供および運営、研究開発（製品・サービスの開発・改善等）、マーケティング・広告、レコメンデーションの調整、内部通報（報告された懸念事項の調査中の個人情報の処理）、コンプライアンスと保護、法的義務への対応時、AI と自動処理　等

【情報の共有】

収集した個人情報については、以下のような場合に共有される可能性がある規定している。

- 特定の製品機能の利用（YouTube や Twilio のような第三者が提供するサービスの利用）
- 提携企業とのやり取り
- Intuit の機能を通じたソーシャルメディアとの接続
- ジョイントベンチャーとは同意のもと、共同で提供する機能等のために情報共有の可能性あり
- ワイヤレスキャリアとの連携時
- 研究目的（個人を特定できないようにした情報のみ提供）
- 金融サービスプロバイダーとのやり取り
- 合併・買収時、関連会社・子会社、広告および分析、法的理由等で情報共有の可能性あり

【データの削除】

Intuit Mint では、利用者が削除依頼をしない限り、Intuit はデータ保持要件を遵守し、利用者へサービスの提供等を行うためデータを保持する（削除依頼があった場合でも法令や規制等に従い保持する場合あり）

【標準規格（ISO27001）】

Intuit Mint も Patients Know Best と同様に ISO27001 を取得している。（ISO27001 の詳細については P.71 標準規格（ISO27001）を参照）

- 標準規格（TRUSTe）

【認証内容】

TRUSTe 認証とは、企業向けにプライバシー管理サービスを提供する企業である「TRUSTe」が提供している Web での個人情報の取扱いに特化した認証のことで、事業者が経済協力開発機構（OECD）のプライバシーガイドラインに基づいた個人情報の取扱いを実践している旨を公表し、プライバシーステートメントの内容審査を受け、適合した事業者に対して送られるものである。

TRUSTe の認証は国内のみならず米国等でも実施されており、Web 上でサービスを提供している企業での認知度は高い。[26]

[26] 一般社団法人日本プライバシー認証機構.「信頼という名の個人情報保護認証」.
https://www.truste.or.jp/

【利点】

TRUSTe 認証の取得を通して、個人情報保護体制の見直し・構築や企業の信頼性の向上等が見込まれる他、認証がされたサイトについては TRUSTe が定期的に監視をしており、問題を発見した場合の改善指導がなされる他、認証サイト・アプリに関する苦情の仲介、売上高 1,000 万円未満の事業者については損害賠償制度が付帯するという利点等が存在する。

【取得要件】

TRUSTe の認定取得のためには、以下のような要件を満たす必要がある。

- 個人情報の利用と保管
- アクセス管理
- 個人情報の提供
- 個人情報の正確性、最新性および訂正手続き
- 情報セキュリティ
- 個人情報保護に関するマネジメント、インシデント対応
- 個人情報に関連する苦情への対応

【取得方法】

TRUSTe の認証を取得するには、自己査定書を作成した後、認定コンサルティング・審査機関にコンサルティングおよび審査の申し込みを行い、コンサルティングによる体制構築後に審査機関による現地審査、現地審査結果に基づく TRUSTe 認証機関による審査に合格する必要がある。

【取得費用】

TRUSTe の取得費用は、TRUSTe 取得はドメインサイト単位が基本として、企業の年間総売上高によって 72,000 円から約 180 万円まで変動をする。（表 6-1-4）

表 6-1-4：TRUSTe ライセンス料 [27]

企業の年間総売上高	年間ライセンス料（税別）
1 億円未満	72,000 円
1 億円～5 億円未満	96,000 円
5 億円～10 億円未満	120,000 円
10 億円～25 億円未満	200,000 円
25 億円～50 億円未満	360,000 円
50 億円～75 億円未満	520,000 円
75 億円～100 億円未満	680,000 円
100 億円～1,000 億円未満	840,000 円
1,000 億円～2,000 億円未満	1,000,000 円

[27] テレコムクレジット株式会社.「ライセンス料について」.
https://www.telecomcredit.co.jp/truste/price.html

2,000 億円以上	1,800,000 円
TRUSTe 取得はドメインサイト単位が基本となる	

- 標準規格（PCI DSS（Payment Card Industry Data Security Standard））

【認証内容】

加盟店やサービスプロバイダーにおいて、クレジットカード会員データを安全に取り扱う事を目的として策定された、クレジットカード業界のセキュリティ基準であり、国際カードブランド５社（American Express、Discover、JCB、MasterCard、VISA）が共同で設立した PCI SSC（Payment Card Industry Security Standards Council）によって運用、管理されている。[28,29]

【利点】

PCI DSS の取得を通して、カードデータセキュリティ体制の強化や関係企業からの信頼性の向上等が見込まれる。

【取得要件】

PCI DSS の取得のためには、以下のような要件を満たす必要がある。

- 安全なネットワークとシステムの構築と維持
- アカウントデータの保護
- 脆弱性管理プログラムの維持
- 強力なアクセス制御手法の導入
- ネットワークの定期的な監視およびテスト
- 情報セキュリティポリシーの維持

【取得方法】

認定を取得するためには加盟店の規模等によってレベルが設定されている要件に合わせ、以下の 3 つの取得方法がある。

① PCI 国際協議会によって認定された審査機関（QSA=Qualified Security Assessor）による訪問審査を受けて、認証を得る

② WEB サイトから侵入されて、情報を盗み取られることがないか、PCI 国際協議会によって認定されたベンダー（ASV=Approved Scanning Vendor）のスキャンツールによって、四半期に 1 回以上の点検を受けて、サイトに脆弱性のないことの認証を得る

③ PCI DSS の要求事項に基づいた、アンケート形式によるチェック項目に回答して、全て「Yes」であれば、準拠していると判断（取り扱うクレジットカード情報量が比較的少ない事業者向けの取得方法）

[28] 日本カード情報セキュリティ協議会.「PCI DSS とは」. https://www.jcdsc.org/pci_dss.php

[29] PCI DSS Ready Cloud.「PCI DSS におけるカード情報の定義」. https://pcireadycloud.com/blog/2022/06/18/3376/#PCI_DSS4

【取得費用 [30]】

PCI DSS の取得について、初期費用は約 1,500 万円以上、保守等の月額費用で 120 万円以上かかる可能性がある。

【テクノロジー】

DID/VC 等の技術の有無

Intuit Mint のサービスについて、DID/VC 等の Trusted Web 関連の技術の使用については確認できなかった。

【使用している技術】

Intuit Mint では、情報セキュリティのために以下のようなテクノロジーが使用されている。

- ■ 多要素認証の使用
  - ➢ 利用者が Intuit 社のサービスにサインインするたびに、多要素認証を使用して本人確認を実施
  - ➢ 利用者のデバイスやサインイン時の現在地など、認識できるものを探したり、送信したコードの入力を求めたりする場合あり。
- ■ データの暗号化
  - ➢ 利用者の情報を暗号化してシステム内に保存することにより、利用者の情報を保護。Intuit 社が使用する暗号化の種類は AES-256（256 ビットキーを使用した高度な暗号化標準）と呼ばれる、最高レベルの暗号化セキュリティを採用
- ■ 継続的な検索およびセキュリティ通知
  - ➢ 利用者が Intuit 社と共有する情報を保護するだけでなく、利用者に影響を与える可能性のある詐欺や詐欺を積極的に検索し、セキュリティ通知により Intuit の偽のメールやカスタマーサポート詐欺に関する情報および対処方法に関する情報を定期的に提供
- ■ 優れたセキュリティを構築するためのパートナーシップ
  - ➢ 利用者のデータ保護のため、複数のセキュリティ組織やアライアンスと確立されたパートナーシップを締結し、最善のセキュリティ方法を提供
- ■ 不正防止システム
  - ➢ Intuit の詐欺防止技術により、常にシステムをスキャンし、不審な動きが確認された場合、不正を行う前に即座にブロック可能
- ■ 同一アカウントでのサインイン
  - ➢ 数個の Intuit 製品の使用について、同一の Intuit アカウントで製品にサインイン可能。1 つのアカウントを持つことで、利用者が Intuit と共有する全ての情報が 1 か所で安全に管理される。

6.2.4 調査結果の比較整理

- ビジネスモデル
  - Patients Know Best と ORPHE についてはウェアラブルデバイスの情報をサービスとして

[30] PCI DSS Ready Cloud.「PCI DSS 認定取得の方法」.
https://pcireadycloud.com/blog/2022/06/18/3376/#PCI_DSS

活用する点で共通している。

- Patients Know Best、Intuit Mint ともに、利用者は無料でサービスを利用できる。
- Patients Know Best、Intuit Mint ともに、元からあった情報の一元管理が可能であるところがインセンティブとしてあげられる。

- サービス環境
  - 英国では国の施策等により、2018 年時点で電子カルテ普及率は 95%以上となっているが、日本ではコストや従来の型式からの変化に対する不安感等もあり、電子カルテ普及率は 2020 年で 57%となっている。
  - 英国の医療制度に関しては日本と同様に全ての国民を対象とした医療制度で、国民は少ない負担で医療を受けることができるが、英国は日本のフリーアクセス制と異なり、登録制で救急以外は登録したかかりつけ医（GP）の診察を受けなければならない。
  - また、英国のかかりつけ医の報酬制度は、日本の出来高払い制度と異なり、診療所に登録している住民の数に応じて支払われる人頭報酬制度である（慢性疾患等の改善に対する報酬等の制度もあり）。
  - Intuit Mint については、日米の税制度、特に確定申告について差異が見られる。日本の多くの給与取得者は、雇用されている企業が手続きの多くを実施するため、自営業以外は個人で確定申告を行うことがないが、米国では収入のあった者全てが自ら確定申告を行う必要があり、電子申告等可能であるが、申告にかかる時間は平均して 13 時間にもなる。
- トラスト（ガバナンス）
  - ➢ 法令
    - 日本の個人情報保護法と英国の UK GDPR は個人情報を提供している企業については、全て法規制の対象となっているが、米国の CPRA は、年間総収入、個人情報の件数、収入の中の個人情報が占める割合等で法規制の対象となるか否かが変化する。
    - UK GDPR については、個人情報保護法、CPRA と異なり、機微情報の取扱い要件が細かく規定されている。
    - CPRA は、個人情報保護法、UK GDPR と異なり、人種、信条等の一般的なものに加えて、運転免許証番号、クレジットカードの情報等も機微情報に含まれる。
    - 日本の個人情報保護法、英国の UK GDPR は原則オプトインを採用しているが、米国の 2 つの法律については原則オプトアウトを採用している。（取り扱う情報対象者の年齢や情報の種類による例外あり）
    - 各法令とも違反した際に罰金が科されるが、その金額関しては、UK GDPR が一番多く罰金が最大 1750 万ポンド（約 31 億円）と一番大きい金額である。
    - CPRA については違反 1 件ごとの金額は比較的少ないが、違反件数ごとに制裁金金額は加算されていくため、違反件数が多いと金額も大きくなる。
  - ➢ 利用規約
    - Patients Know Best、Intuit Mint 共に規約の変更後もサービス利用を継続した場合、規約の変更に同意したと見なされる他、Patients Know Best ではサービスの利用

がない場合でも規約の通知後、一定期間に拒否の申し出が無ければ承諾したと見なされる。
- 両サービスともそれぞれ禁止事項が定められており、これらの規約に違反した場合についてはサービスの利用停止等の措置がとられる可能性がある。
- 両サービスともサービス提供側の問題により、直接的な侵害が発生した場合のみに損害賠償の範囲を限定しており、間接的等の理由での損失に関しては責任を負わない
- また、サービス内容についても現状有志での提供であり、情報の正確性、信頼性等については保証していない（Patients Know Best では情報の正確性等は医療提供者等に依存していると記載）。

➢ プライバシーポリシー
- 両サービスとも情報を第三者に提供する可能性はあるが、個人を特定できないように加工した情報、暗号化した情報を提供する等、提供される情報の範囲を限定した手段が採られている。
- Intuit Mint では利用者の削除依頼に応じて基本的にデータを削除するが、Patients Know Best では、取り扱うデータが医療データであり、記録の削除については、組織（医療機関）側からの要求に応じてのみ対応する。（削除できるのは、組織側が閲覧していない、利用者が自ら追加した情報のみ）
- また、Patients Know Bestとの契約を終了後もデータを保持する場合は保持のみの契約が確立する。

➢ 認証
- 認証については両サービスともに、企業としての信頼性向上のため ISO27001 の認証を取得している。
- Intuit Mint は ISO27001 以外に Web 上の個人情報保護（TRUSTe）、クレジットカード（PCI DSS）等の媒体、分野に適合した認証等を取得し、データ等の信頼性の向上に努めている。
- 認証の取得は、信頼性向上のための有効な手段であるが、取得のために多額の費用と審査対応所要等が発生する等負担が増加することがある。

● トラスト（テクノロジー）
- テクノロジーについて、両サービスともに DID/VC 等の Trusted Web に関連した技術は使用されていないものの、多要素認証、データの暗号化、不正防止をスキャンし、ブロックするシステム、セキュリティ情報に関する通知等を活用して、データの技術的な保護を実施している。

6.2.5 結論

【ビジネスモデル】
- Patients Know Best と ORPHE についてはウェアラブルデバイスの情報をサービスとして活用する点で共通している。
- Patients Know Best と Intuit Mint は基本的に患者や利用者の使用料については

無料で運営しており、専門家・組織からの使用料、企業からの広告料、紹介料でサービスが成立していることから、それら患者・利用者の情報の価値づけ、インセンティブ設計について関係する組織や企業は金銭を支払っても得られるインセンティブが大きいと考えていると推察。

【サービス環境】

- Patients Know Best については、英国の施策により、医療情報の IT 化が促進され、電子カルテ普及率も 95%以上という状況になっており、NHS に医師が記録した情報は、別の医療機関にも共有される等、Patients Know Best のような医療情報を共有するサービスが醸成される基盤ができていた。
- 日本については、英国の施策のようにはいかず、電子カルテ普及率は 57%であるため、更なる医療情報の IT 化のためには国の積極的な関与・支援が必要である。
- 英国の NHS の報酬制度の関係から、診療所のサービスを向上させ、診療所の登録者数を増やすことに対してインセンティブが存在していたため、サービス向上の一手段として Patients Know Best が活用されたと考えられる。
- Intuit Mint についても米国の税制度の関係上、日本の企業勤務者と違い、収入のある者全員が自ら確定申告を行う必要があり、申告にかかる平均時間 13 時間という部分からも、確定申告の負担軽減のため、金銭管理を行うことができるアプリケーションサービスのニーズが高い状態であったと考えられる。

【トラスト（ガバナンス）】

- 法令については、対象となる企業、同意の要件、罰金額等で差異はあるものの、各企業が所在している国、州で適用されている法令を遵守しているという点以外にサービス普及・継続の要因は確認できなかった。
- 利用規約およびプライバシーポリシーについても法令と同様に規定事項に差異は認められるものの、法令に基づいた規約・ポリシーを設定し、遵守している点以外にサービス普及・継続の要因は確認できなかった。
- 認証については両サービスともに、企業としての信頼性向上のため ISO27001 の認証を取得している他、Intuit Mint は ISO27001 以外に Web 上の個人情報保護（TRUSTe）、クレジットカード（PCI DSS）等の媒体、分野に適合した認証等を取得し、データ等の信頼性の向上に努めている。
- 認証の取得は、信頼性向上のための有効な手段であることは明確であるが、その取得のために、多額の費用と審査対応所要等が発生する等デメリットが存在していることも意識をしなければならない。

【トラスト（テクノロジー）】

- テクノロジーについて、両サービスともに DID/VC 等の Trusted Web に関連した技術は使用されていないものの、多要素認証、データの暗号化、不正防止をスキャンし、ブロック

するシステム、セキュリティ情報に関する通知等の手段を活用して、データの技術的な保護、データとしての信頼性の向上に努めている。

7. 実証終了後の社会実装に向けた実現案と今後の見通し

7.1 残課題対応方針一覧

本実証を通して明らかとなった課題のうち、今後のサービスの社会実装に影響するものとして、1）既存の業界ポリシー・ガバナンスへの準拠、2）ポイント導入に際するエコシステムの確立、3）コミュニティ形成、が主なものとして挙げられる。

1）は、個人情報保護法、次世代医療基盤法、景品表示法などの法や医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン、民間事業者の PHR サービスに関わるガイドラインなどといったガイドラインを中心に対応すべき項目を整理し、今後対応していく。特に、個人情報保護法の観点から、個人情報を共有する場合の同意取得には、データ共有先およびデータの利用目的の設定が必要になる。データ利用目的がデータ利用機関ごとに幅広く異なることが想定されており、法に準拠した同意取得とデータ利用者・データ提供者のユーザビリティを両立させる UI の設計やガバナンスの整理が必要になると考えられる。

2）には、ポイント付与レートの決定、ポイント利用の選択肢の準備、ポイント返戻規約の決定、関連ルールへの準拠（景品表示法など）など、いくつかの課題が見つかった。データの価値付けが現時点では難しいことや歩行データの臨床評価活用にはある程度のエビデンス確立が必要であることなどから、まずは医師と患者間のデータ共有からサービスを展開することとした。これらの展開を進めつつ、データを蓄積し、データ利用者への提供サービス、そして患者ユーザに還元できるポイントレートの設定を行い、ポイントシステムの導入によって継続的運営可能なエコシステムの構築を目指す。

3）コミュニティ形成に関しては、医療情報・PHR を含む個人方法をやり取りするシステムに関するガバナンスを整理しつつ、参加可能な医療関係者・データ利用企業・患者を巻き込みコミュニティの形成を図っていく。特にデータを主体的にコントロールしつつ、合意のもとデータ流通を促すシステムであるため、データ提供者（患者ユーザ）の巻き込みが重要であると考えており、サービス提供者と医療関係者に構成が偏らないコミュニティ形成を意識する。

7.2 ユースケース実現モデル

7.2.1 ビジネスモデル案

本実証事業を通して議論・検討を行い、最終的に以下のビジネスモデルが適していると考えた。医療機関は、ORPHE へサービス利用料を支払って、サービスを利用し、アプリを介してデータを共有した患者に対して、データに基づく適切な指導を行うサービスを提供する。患者は、医療機関が提供するサービスを有料でうけ、医療機関へデータを共有し、データに基づく診断/アドバイスを受ける。また、研究機関/製薬企業などの第三者のデータ共有リクエストを承認し、データを共有した場合は、システムを介してポイントを獲得できる。研究機関/製薬企業などは、サブスクリプション形式でサービス利用料を支払い、データ共有リクエストを送る場合には必要なトークンを購入する。以上のモデルにすることにより、費用・ポイントの支払い先や受け取り先が複数にならず、明瞭なフローになると思われる。また、企業ヒアリングの結果から、企業が利用する際に必要な最低限のデータ数が数千人～数万人と多く必要だったことも分かったことから、まずは医師と患者間で提供されるサービス・ビジネスモデルから展開することで段階的なサービス拡大をできると考えている。

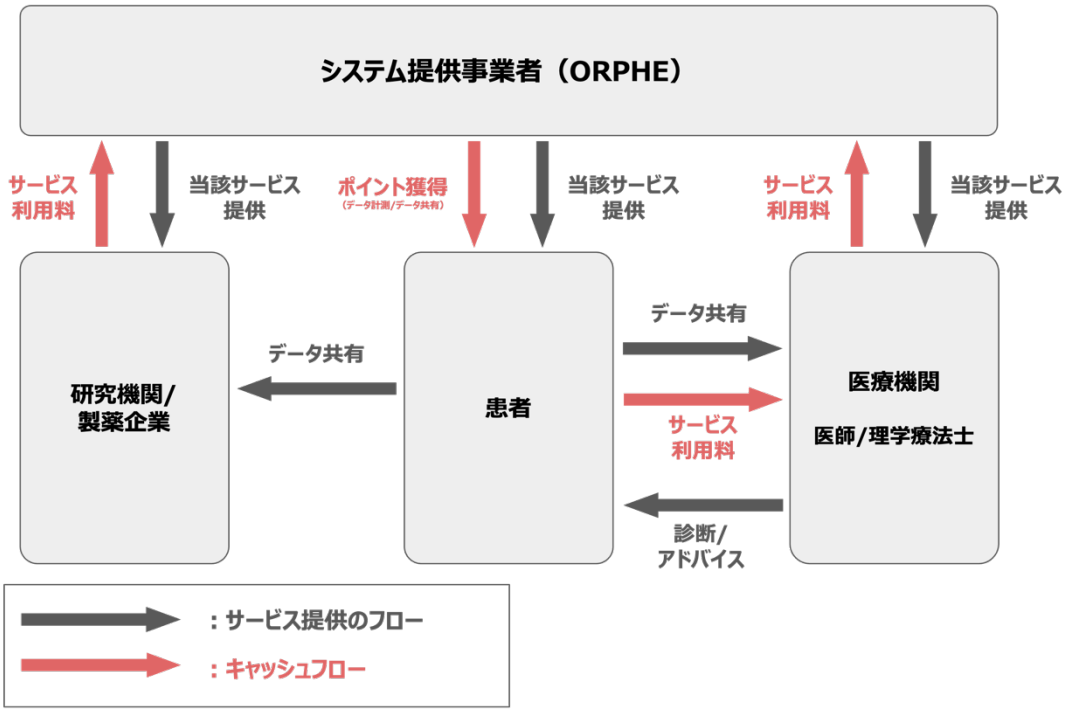


図 7-2-1：ビジネスモデル案

7.2.2　システム案

システムアーキテクチャは以下に示す通りである。実証実験を通して、技術仕様やアーキテクチャに大きな問題は見られなかったため、実装した通りのアーキテクチャを採用する。

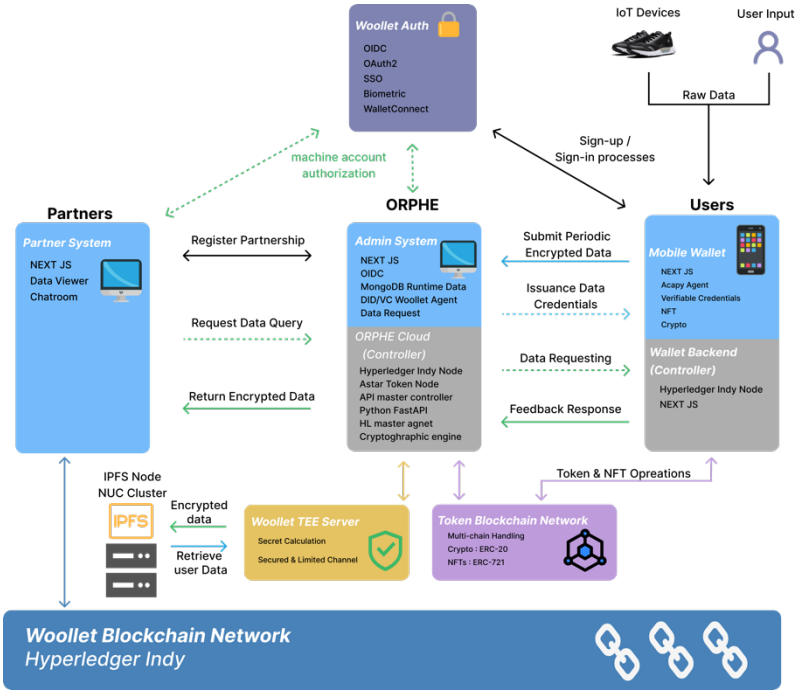


図 7-2-2：アプリ・システム案

7.2.3　ガバナンス・ルール案

実証事業における調査・検討を通して、医療情報・PHR を含む個人情報をやり取りするシステムにおいて準拠すべき業界・コミュニティのポリシーには、個人情報保護法、次世代医療基盤法、医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン、民間事業者の PHR サービスに関わるガイドラインなど、多く該当するものがあることが分かった。本システム・サービスに関わるステークホルダにかかるガバナンス・ルールを定める必要があると考える。現時点で想定するサービス実装に必要なガバナンス・ルールは以下の通りである。

表 7-2-1：TRUSTe ライセンス料

ステークホルダ	ガバナンス	ルール
患者	**利用規約**	• **不正なデータ計測を行わない。** • **第三者にアカウントを譲渡しない。** • **データの改ざんを行わない。** • **複数のアカウントを作成しない。** • **第三者へのポイントの売買を行わない。** • リバースエンジニアリングや逆コンパイルを試みない。
医師・医療機関	• 個人情報保護法 • 次世代医療基盤法	• 第三者提供しない。 • データ漏洩させない。 • 利用目的の詐称をしない。 • 利用目的外のデータ利用をしない。
	利用規約	• **アカウントを付与したものの行為に対しても利用契約機関に責任が生じる。** • **機関に所属するもの以外にアカウントを付与しない。** • **第三者にアカウントを譲渡しない。** • 不正な患者データ入力を行わない。
データ利用者（研究機関/製薬企業など）	• 個人情報保護法 • 次世代医療基盤法	• 個人情報を第三者に提供しない。
	利用規約	• 医師・医療機関と同様。
サービス提供者	• 個人情報保護法 • 次世代医療基盤法	• 個人情報を第三者に提供しない。 • 情報漏洩が生じた場合に報告する。
	利用規約	• ユーザの許可なく、ユーザ情報にアクセスできない。

7.3 実現に向けたアクション・ロードマップ

タイムライン	マイルストン	マイルストンに向けて実施すること
2024 年 04 月	ISMS の確立	ISMS 認証取得に向け、外部コンサルタントとのやり取りを進めていく。
2024 年 04 月	各種法律・ガイドラインの準拠対応を始める	以下の法律・ガイドラインへの準拠・整合性確認を弁護士と進める。 • 個人情報保護・次世代医療基盤法 • 医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン • 民間事業者の PHR サービスに関わるガイドライン
2024 年 08 月	ガバナンス/利用規約の 整理・作成	法律と技術で担保できない部分を再度整理し、弁護士と連携のもとサービス利用規約の作成を行う。
2025 年 04 月	患者-医療機関のシステムとしてサービス化	サービス内容の決定・サービス利用料を設定した PoC 実施なども想定。
2026 年 04 月	研究機関/製薬企業などの 第三者のデータ共有リクエスト機能サービス開始	• ポイントレートの決定 • ポイント利用の選択肢の準備 • ポイント返戻規約の決定 • 関連ガバナンスへの準拠（景品表示法等）

8. Trusted Web に関する考察

8.1 求める機能や Trusted Web ホワイトペーパーver.1.0 の原則に関する課題と提言

求める機能について

【課題】

いずれの機能についても実装できている状態ではあるが、合意の元になる内容（情報）をどのようなプロセスで設定すべきか判断が難しい。現状では、データ共有リクエスト送信者毎に利用目的の設定が必要になると考えられる。

Trusted Web ホワイトペーパーver.1.0 の原則について

【課題】

ユニバーサル性：ビジネスとしてユニバーサル性の追求をどこまで求めるべきなのかの判断が難しい。収益性が高いターゲティングは行わず、全ての世代、属性のユーザを対象にすべきということか。それとも単にユニバーサルな UX とすべきということか。仮に後者の場合、原則として提示するほど特徴的な項目ではないと思料する。原則の中でも must な原則、desirable な原則で強弱をつけた方が良いと思われる。

相互運用性：何と何の相互運用性を図るべきかが分かりにくい。国同士のフレームワークレベルなのか、業界固有のアーキテクチャレベルなのか、もしくは、事業者個々で作成するシステム・サービスレベルなのか。また相互運用性を担保するためには、セキュリティレベルなど、明確な基準や規格が存在することが前提として考えているが、Trusted Web としての相互運用性を担保するには、現状のホワイトペーパーでは情報が不足していると思われる。

【提言】

各原則に対して、Trusted Web の特徴を表すという視点で強弱（重要度）を付けるべき。現状の原則は一般的（汎用的）な非機能要件に見受けられてしまう。すべて Trusted Web として外せない要素だとしても、せめて優先順位や重要度で区分しないと Trusted Web らしさが見えてこない。

推進ステップ内の各項目で指し示すものを明確化しないと新規参入する企業が何を対象として、原則について考慮すれば良いかわからない。（例：「特定の基準」や「類似のシステム」、「グローバルで動作する」など）

8.2 Trusted Web のガバナンスに関する課題と提言

【課題と提言】

- 医療・ヘルスケア分野においては医療情報交換の次世代フレームワークとして「HL7 FHIR」が存在しており、日本でも推奨されている状況である。一部にセキュリティや認証に関する規格も規定されており、本フレームワークにトラスト（Trusted Web）の要素を組み込んでいくことが、医療業界で Trusted Web に基づくガバナンスを浸透させる一番の近道であると考える（合意形成やデータ主体によるコントロールなどの考え方・仕組みは HL7 FHIR には存在しないため、ブラッシュアップを図れる可能性があると思料）。

- 他方、「HL7 FHIR」では具体の推奨規格まで規定されており（そのため諸外国含めて採用率が高い）、Trusted Web（のホワイトペーパー）で掲げるコンセプチュアルな内容とやや乖離がある。「HL7 FHIR」と Trusted Web が連携を図るためには、Trusted Web 側の基準や規格を明確にし、歩調を合わせる必要があると考える。
- Trusted Web の概念に対して、サービス事業者（開発者）が守るべき基準が現状のホワイトペーパーの中で明確に示されていない認識である（民間事業者の履行確保する仕組みが整備できていない）。この状態ではデファクトとして民間事業者や業界団体が Trusted Web のガバナンスを図っていくことは困難である。
- そもそも日本は米中と比較してデファクトでルールを形成できるほど規模と影響力のある企業は存在しないため、ガバナンスを図っていくためには政府のリードが必要であると考える。（業界団体で一体化したとしても業界団体を主導できる強力なリーダーが必要と考えるが、そのような人物に期待するのであれば、政府が音頭をとることが効率的と思われる）

8.3 Trusted Web のアーキテクチャに関する課題と提言

- 相互運用性を意識してアーキテクチャを作成していると認識しているが、Trusted Web のアーキテクチャと相互運用性が保たれている、他国・他団体のアーキテクチャを示していただきたい。Trusted Web のアーキテクチャに従って構築されたシステム・サービスは、どの国、どの企業、どの団体が構築したシステム、サービスと相互運用性があることが分かれば、アーキテクチャを活用するインセンティブを見出しやすい。

8.4 その他 Trusted Web に関する課題と提言

- Trusted Web はイニシアティブであるということであるが、最終的な目標・到達点を明確に示した方が、民間事業者や関連ステークホルダが連携・協調しやすいと思う。現状、何を目指しているのかが分からないので、どのような寄与が可能なのか判断しかねる。
- AI サービスなどがトレンドになっている昨今、よりデータや情報の信頼性への価値が高まってきている。他方、本実証事業で作成したプロトタイプシステムやサービスは自走していくことは難しいと考える（トラストに対して支払う対価の定量化で出来ておらず、システム・サービスを運用するためのコストに見合う利用料の徴収は難しいのではないかと考える）。そのため、現状は基礎技術やプロトシステム開発への政府援助が行われているが、実用化の初期フェーズまで含めた補助施策（または政府ファンドの構築など）を講じることが望まれる。これにより、例えば、利用料を無料にすることで UX と向上と初期利用者の拡大を同時行うことができると考える。
- 政府の中でも複数の団体で「トラスト」を議論していると認識している。日本のトラスト政策の中での Trusted Web の位置づけを明確にしていただきたい。

Appendix

用語集

用語	内容
プレサイスターゲティング	ゼロ知識証明と Verifiable credential を用いて、データの機密性を保ったまま任意のデータを持つユーザを、woollet を通じて発見し、ユーザ同意のもとで当該データへのアクセスをする仕組み（特許申請済：特願 2022-146935）。本ケースの場合、パートナーが求める一定の条件を満たす対象（例：性別やデータの取得期間など）のみにデータリクエストを送りたい場合にも、患者情報がパートナーには共有されない状態で、データリクエストを送ることができる。データリクエストを受けた患者は、共有をしてもよい項目に対して共有への同意を行った後に、該当データのみがパートナーに共有される。

本実証で開発したシステムの第三者による再現可能性

本実証事業で企画・開発するプロトタイプシステムはアプリ、ストレージ、認証といった多くの開発要素においてオープンソースのコンポーネントを使用しており、構成要素ごとの詳細な機能要件や実装プロトコルを開示することで第三者が容易に再現することが可能である。

また本実証事業で開発するデジタルウォレットは DataGateway PTE LTD 製の Woollet Core システムを組み込んで実装しており同製品のライセンスを利用することで使用可能となる。またスマートフットウェアを使用した歩行データの取得については ORPHE 社製の SDK（ORPHE-CORE.js）や ORPHE 社より一般発売されているセンサー（ORPHE CORE）を利用することで第三者による再現が可能である。

- 本実証事業で企画・開発するプロトタイプシステムはアプリ、ストレージ、認証といった多くの開発要素においてオープンソースのコンポーネントを使用しており、構成要素ごとの詳細な機能要件や実装プロトコルを開示することで第三者が容易に再現することが可能である。
- 本実証事業で開発するデジタルウォレットは DataGateway PTE LTD 製の Woollet Core システムを組み込んで実装しており同製品のライセンスを利用することで使用可能となる。また、スマートフットウェアを使用した歩行データの取得については ORPHE 社製の SDK（ORPHE-CORE.js）や ORPHE 社より一般発売されているセンサー（ORPHE CORE）を利用することで第三者による再現が可能である。

システム・ライブラリ名	開発区分（新規・既存）	ライセンス取得有無（予定含む）	第三者による再現方法
デジタルウォレットシステム、VC / DID の付与	開発済	取得済	• DataGateway 社サービスのデジタルウォレット「Woollet」を導入することで、利用可能
スマートフットウ	開発済	取得済	• 弊社センサ（ORPHE CORE）を

ェア	（特許取得）	（一部機能のオープンソース化済）	購入することで利用可能 • ソフトウェアはオープンソースのライブラリ（ORPHE CORE.js）を利用することで大部分の機能は第三者も開発、再現可能
利用者アプリ	新規（一部開発済）	取得予定なし	• フロントアプリは納品するソースコードで再現可能 • 「デジタルウォレットシステム」と API 連携することでアプリが正しく稼働する
顔認証等の生体認証	新規	取得予定	• iOS の標準認証機能を利用することで再現可能

ヒアリング詳細・結果

- 下肢運動器疾患患者

【論点】

医師や研究機関、製薬企業などへデータを共有することに懸念や不安感はあるか。

【解答や示唆】

利用目的や共有されるデータの説明はされるが、どのようなデータが共有されるとリスクがあるのかの判断が難しい。また、実際にどのように利用されているかを知りようがないため、同意に意味があるのかよくわからない。