**Trusted Web の実現に向けたユースケース実証事業**

**プロトタイプアプリ要件定義書**

下肢運動器疾患患者と医師，研究者間の信用できる  
歩行データ認証・流通システム

2024年3月15日

代表機関：株式会社ORPHE

**目次**

[1. プロトタイプシステムの概要 1](#_Toc163653871)

[1.1 プロトタイプシステムの概要 1](#_Toc163653872)

[1.2 事業スキーム 1](#_Toc163653873)

[1.3 業務要件 2](#_Toc163653874)

[1.4 企画・開発するプロトタイプシステムにおけるユースケースの検証範囲 3](#_Toc163653875)

[2 実証内容 4](#_Toc163653876)

[2.1 実証の実施事項，論点及び判断 4](#_Toc163653877)

[2.1.1 プロトタイプの機能要件，非機能要件 4](#_Toc163653878)

[2.2 検証できる領域を拡大する仕組み 6](#_Toc163653879)

[2.2.1 データフロー 6](#_Toc163653880)

[2.2.2 データフローに登場する主体とその概要 7](#_Toc163653881)

[2.2.3 検証できる領域を拡大し，Trustを向上するために本システムで検証を行うデータ及びデータのやり取りの内容 8](#_Toc163653882)

[2.2.4 本システムで形成を目指す合意とその履行のトレースの内容 8](#_Toc163653883)

# プロトタイプシステムの概要

## プロトタイプシステムの概要

変形性膝関節症などの運動器系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し，分散型ID技術(DID/VC)とブロックチェーン技術を組み合わせることで，ユーザー管理の記録領域にデータを記録可能とするプロトタイプシステムを実装する．ユーザー同意に基づいたデータの拠出に紐づけてポイント発行するとともに，そのデータを医師や研究機関などに患者の同意を得た上で活用可能とするシステムの構築を目指す（図1）．

**ダイアグラム

自動的に生成された説明**

**図1**　**将来的なユースケースのイメージ**

## 事業スキーム

　本実証事業における事業には，患者，医療機関（医師），研究機関・製薬機関が関わり，データのやりとりとポイントの発行がなされる（図２）．

ダイアグラム

自動的に生成された説明

**図2**　**事業スキーム**

上記事業スキームにおける患者，医療機関，研究機関/製薬会社のそれぞれの詳細な設定・役割は表1に示す通りである．

**表 1　事業スキームに登場する主体とその概要**

| 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． |
| 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 |
| 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合せを行い，取得するデータに応じたポイントを購入し，データの取得を行う． |

## 業務要件

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」において，プロトタイプアプリで開発した機能と，本実証事業の取り組みの差分を以下に示す（図３）．特に本実証実験では，以下の機能を実装する．

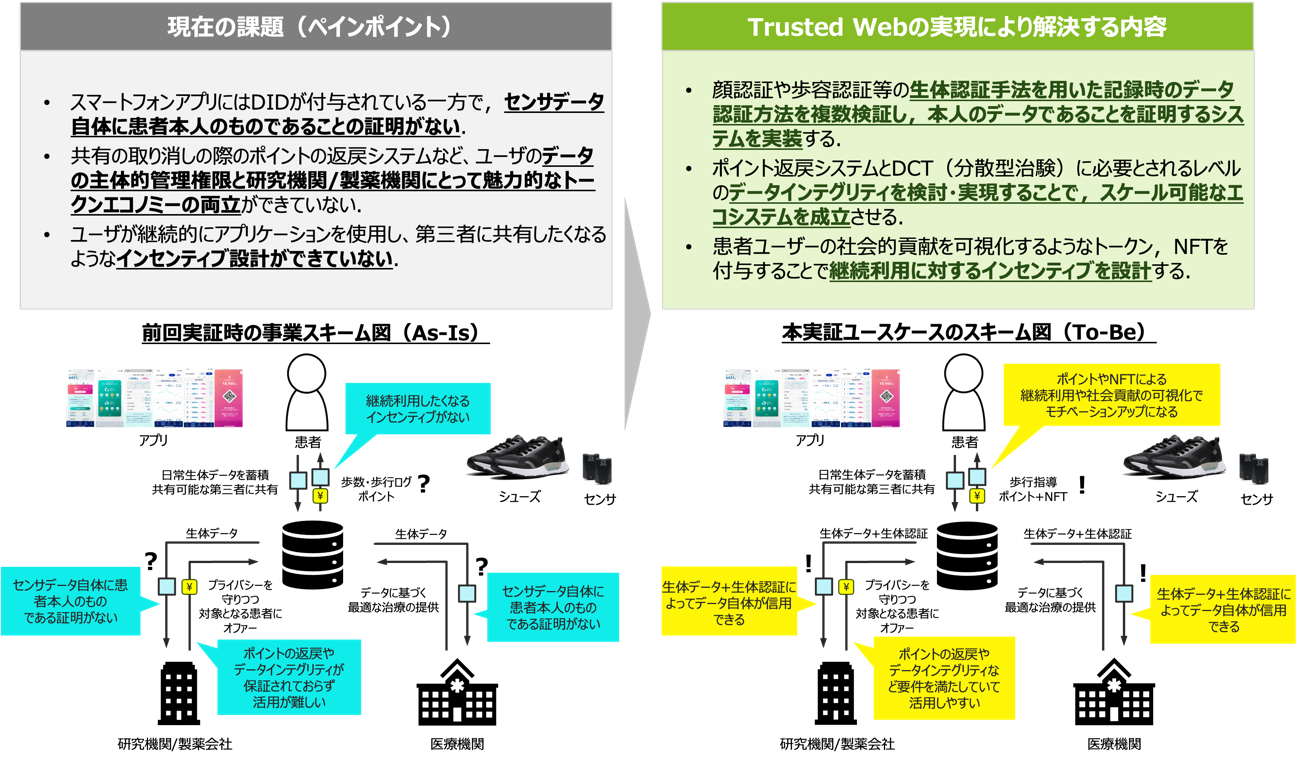
* 生体認証によって，データが本人のものであることを担保した状態でデータVCの発行できる機能
* データ共有の同意撤回を行なった際にポイントが返戻されるような機能（ポイント返戻機能）
* 患者ユーザの行動（アクション）に応じて，さまざまなNFT（条件達成バッジ）を付与し，アプリで表示・管理できる機能

図3 本実証事業で開発する機能とスキーム図

## 企画・開発するプロトタイプシステムにおけるユースケースの検証範囲

本実証事業では，下記のやり取りを実現するプロトタイプシステムの企画・開発を行う．

＜プロトタイプシステムで行うやり取り＞

**患者**

1. 主に医師の推薦により，またスマートフォンアプリをダウンロードする．
2. アプリを起動し，web walletのアカウント作成を行う．
3. 患者は，医師がORPHE Desktop Systemで発行したQRを読み込むことで診断情報を呼び込み，本人の基本情報入力追加入力し，ユーザ情報登録を行う．
4. 患者はスマートフォンアプリを通じて，自身のデータ計測・入力を行う．
   1. 日常生活の中でスマートフットウェアを履いて歩行データを記録する．
   2. Numeric Rating Scale (NRS) (患者が感じている痛みを数字で評価するための指標．0が痛みなし，10が想像できる最大の痛みとして，0～10までの11段階に分けて，現在の痛みがどの程度かを指し示す段階的スケール)などを用いて主観的な痛みや体調などのデータを記録する．
   3. Apple ヘルスケアと連動し，iPhoneで記録された歩数データを読み込む．
5. 医師や研究機関/企業などからデータ共有リクエストがきた場合は，申請相手，内容，利用目的，共有されるデータを確認し，承認/非承認を行う．
6. データ計測などに応じて獲得されるポイントを好きな景品などに交換できる．

**医師/理学療法士**

1. 医師・理学療法士は，アプリをダウンロードし，web walletアカウントを作成する．利用契約を結んだ所属機関のアカウントに対して，機関所属証明VCの発行を依頼し，許可を受けることで患者登録などの機能が利用を開始する．
2. 医師は，患者診察時にORPHE Desktop Systemを用いて，患者情報の入力・QRコードの発行を行い，患者にQRコードを読み込ませる．
3. 医師/理学療法士は，必要に応じて，データ共有リクエストを患者に送信する．データ共有が許可された場合，データを閲覧・問診の補助などに利用することができる．

**研究機関/企業**

1. ORPHEから発行されるアカウントを利用して，ORPHE Desktop Systemにログインする．
2. プレサイスターゲティング機能を利用して，条件を満たすユーザに対して，データ共有リクエストを送信することができる．
3. ユーザからデータ共有が許可された場合には，データのグラフ閲覧，詳細確認ができる．

研究機関や企業はプレサイステーゲティング技術を活用することで以下のような利用を実施することが可能になる．

下肢運動器疾患の研究，人工関節メーカなどの開発を行いたい第三者機関はシステムに問い合わせることで患者の個人情報に触れることなく対象となる患者のデータに提供オファーを出すことができる（例：６０代女性で重症度Kellgren/Lawrence（KL）分類が４の方の日常データを集めたい）．第三者機関はトークンを購入し，トークンを使ってデータを取得することができる．

# 実証内容

## 実証の実施事項，論点及び判断

### プロトタイプの機能要件，非機能要件

1. 要件定義

我々は令和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」において，以下のような議論を通して，本システムの開発に必要な機能の設定を実施した．本実証においても，システムの技術要件に関してはこれらの要件を引き継ぐ．

患者，医療機関，研究機関といった多様なステークホルダーにシステムを活用してもらうために，歩行データ等の患者個人のデータを患者から医療機関，研究機関にセキュアかつユーザ同意をもとに譲渡する必要性が議論されてきた．そこでDID（分散型ID）を使用することで，患者のデータのプライバシーを保護し，セキュアなデータ共有を可能とすること，また，DIDにより，患者は自分のデジタルアイデンティティを独立して管理し，データアクセスを制御できるようになることが必要であると考え，下記の要件をTWの４要件として対応した状態で検討した．

1. IoTセンサーから取得したデータを改竄不可な状態で記録する．
2. ユーザのウォレットにDIDを付与する（モバイルでのDID発行）
3. ユーザの同意のもとにデータを譲渡する．（検証可能な属性情報による動的な合意形成）
4. 医療機関や研究機関は個人情報にアクセスすることなく，条件に合致するユーザのデータを検索し，データの譲渡を依頼できる（ユーザのプライバシーを保ったまま属性情報をもとに正確なターゲティングをできるシステムの構築）
5. 管理画面上で医者や研究機関向けにグラフなどに患者データを可視化できる機能の付与（第三者機関が統計データにアクセスするためのシステム構築）
6. ユーザにデータ譲渡のインセンティブとしてポイント付与を行うが，将来的な相互運用性を踏まえてパブリックブロックチェーン上にあるトークンとして取り扱う．

【機能要件】

ウォレットは，本事業で提供するプロトタイプアプリ内に組み込まれるもので，アプリ内のウォレットによって，患者は自分のデータとデジタルアイデンティティを管理できるようになる．DIDの付与に関しては，アプリを通じて患者が自身のデジタルアイデンティティを作成する際に，システムが自動的に生成し，ウォレットに格納される．これにより，患者はデータ共有やアクセス制御が行えるようになる．この要件を満たすためにDataGateway社との打ち合わせを実施し，必要となる機能として以下の3点を抽出した（表2）．

**表2　Trusted Webの要件によって実証事項が実現可能な根拠**

| 機能 | 該当する要件定義 | 該当するTWの要件 | 機能の詳細/実現方法 |
| --- | --- | --- | --- |
| A．ORPHE CloudによるDID発行と，ユーザデバイスへの付与 |  | 要件１ | * QRコードを利用してDIDを発行し，署名鍵によってユーザデバイスとORPHEクラウドの紐付けが可能 |
| B．検証可能な属性情報による動的な合意形成 | ③ | 要件２  要件３ | * 検証可能な資格情報(VC)を提供するAPIを構築し，モバイルからアクセス可能とする． |
| C．ユーザーのプライバシーを保ったまま属性情報をもとに正確なターゲティングをできるシステムの構築 |  | 要件１  要件２ | * データ送信時に，データの種類や値に応じてユーザーに属性クレデンシャルを発行するORPHE Cloud(Woollet Coreシステムを組み込んで実装したデータ送信時にVCを発行し，ユーザーのプライバシーを保護しながらデータ共有を可能にするプラットフォーム)を構築． |

Aについては，ユーザー（患者）とパートナー（医療従事者等）の両方にDIDを発行し一連の認証クレデンシャルとともに運用されることで，要件１のようなデータのコントロールを可能とする．

B，Cについては管理画面から閲覧したいデータを期間と種類を選択することで，今回登録しているユーザー全てのウォレットに対してクエリが発行され，ユーザーウォレット側で内容についてゼロ知識証明を通じた参照を行い，閲覧したいデータの対象となるデータが内部に存在する場合にユーザーにデータをシェアするかどうかの確認が表示される．それを認証することで個人情報にアクセスすることなくお互いが望むデータ共有であることを確認し合意形成を可能とする（要件３）．実装についてはW3C[[1]](#footnote-1) とHyperledger Aries[[2]](#footnote-2)に詳しく記載がある．

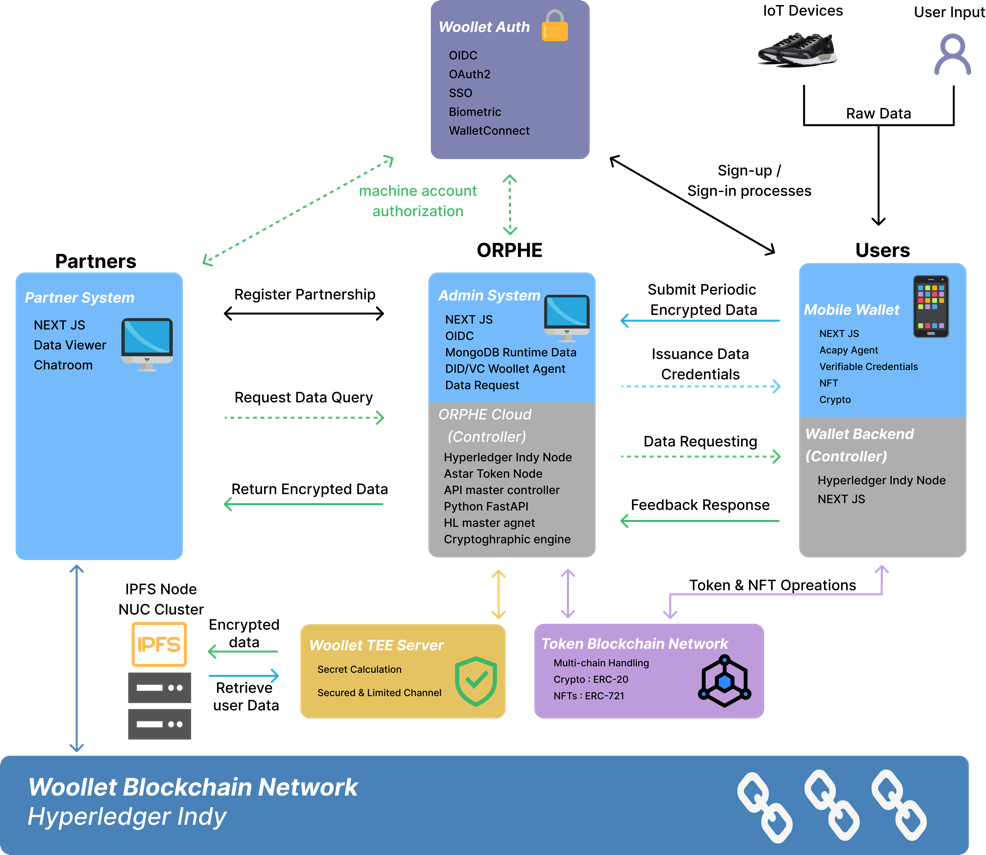
【非機能要件】

データ記録に関して，蓄積されるデータが増えてくることを想定し，ユーザウォレットに記録しきれない分の大容量のデータを記録できる媒体であることとデータの耐改ざん性を担保する必要があると考えられた．

1. 基本設計

以上のような要件を踏まえて，以下のようなシステム構成（図3.1-1）を設計した．

1. 患者向けユーザーモバイルアプリ（ORPHE Mobile App）
   1. IoTセンサとユーザー入力でログの形成機能
   2. ウォレット機能（DIDに基づいたVCの管理，通信ノード）
   3. セキュアストレージ機能（DID保管）
2. IoTセンサ（ORPHE CORE）
   1. 歩行データ収集
3. パートナー（医療機関，研究機関）アプリ（ORPHE Desktop System（Partner system））
   1. データリクエスト機能
   2. データ閲覧機能
   3. ウォレット機能（DIDに基づいたVCの管理，通信ノード）
4. データ管理（ORPHE Cloud）
   1. 患者データ管理
   2. DID管理
   3. 属性クレデンシャル管理
   4. ゼロ知識証明処理
   5. 合意形成処理
   6. 認証トークンの付与
   7. パートナー条件へのクエリUI
   8. ユーザーからのデータ照会UI
5. Private Data Lake Inter Planetary File System (IPFS)
   1. ユーザーデータ収集・保存
   2. ユーザーデータの検索
6. ブロックチェーンネットワーク
   1. トランザクション記録
   2. トークン（ポイント）管理
   3. NFT管理
7. Woolletブロックチェーンネットワーク（Hyperledger Indy）
   1. DIDに紐づく公開鍵基盤



**図4　システム構成図**

## 検証できる領域を拡大する仕組み

### データフロー

情報要求者（医療機関）が条件に当てはまるデータの保有者（患者）を検索し，データの保有者（患者）にリクエストを表示し，データの保有者（患者）の認証が得られた場合は開示を行う（図5）．開示を行うか否か，開示する期間については患者が主体的に選択することが可能である．

ダイアグラム

自動的に生成された説明

**図5　データフロー図**

### データフローに登場する主体とその概要

以下に，図5に示したデータフロー図に登場する各ステークホルダーの設定・役割について示す．

* 患者（情報所有者(Holder)/情報要求者（Verifier））
  + ヘルスケア情報やセンサ情報の所有権を持ち，Walletを通じて自分に関するデータを収集し必要な情報のみ共有する．ORPHE CloudにメタデータVC発行を依頼する．
  + IoTデバイスから取得したデータに対するメタデータVCに対する所有権を持ち，Wallet上に自分に関する属性情報を保存し，情報要求者の依頼に基づき，合意形成された必要な情報のみ選択的にデータ共有要求者に提示する．情報共有に必要な各種証明を取得するため，証明書発行者にVC発行依頼をする．
* 医師，理学療法士（情報要求者（Verifier）/情報所有者(Holder)）
  + 希望する患者（情報所有者）のデータの共有を受けるため，ORPHE（証明書発行者）に情報要求を行う．Web上のシステムを通じて情報所有者の承認を経て証明書発行者からVC付データを受領し，日常で取得された患者のデータを受け取り，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．また，患者の条件やデータの種類などについてゼロ知識証明をもとにした突合により，プライバシーを保ったまま適切なデータにのみアクセス可能．
* 研究機関，研究者（情報要求者（Verifier）/情報所有者(Holder)）
  + 希望する患者（情報所有者）のデータの共有を受けるため，ORPHE（証明書発行者）に情報要求を行う．Web上のシステムを通じて情報所有者の承認を経て証明書発行者からVC付データを受領し，日常で取得された患者のデータを受け取り，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，それぞれの課題の研究を進めることができる．また，患者の条件やデータの種類などについてゼロ知識証明をもとにした突合により，プライバシーを保ったまま適切なデータにのみアクセス可能．
* ORPHE（証明書発行者（Issuer））
  + 証明書発行者として依頼に基づいて各情報所有者へVCの発行を行う．また患者の行動に基づいてポイントの付与を行う．
  + 情報要求者からの要求を受領し，情報所有者に承認を取る．パブリックブロックチェーンを介して情報要求者に要求資格があるか，対象情報は存在するかといった条件の確認を行い，条件が満たされた場合VCを発行してデータを情報要求者に送付する．

### 検証できる領域を拡大し，Trustを向上するために本システムで検証を行うデータ及びデータのやり取りの内容

以下表3にて検証できる領域を拡大し，Trustを向上するために本システムで検証を行うデータ及びデータのやり取りの内容についてまとめを示す．

**表3　検証を行うデータ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **証明書名** | **記載情報** | **要件** | **活用する規格** | **規格選定理由** |
| 患者情報 | 性別，生年月日，身長/体重，疾患名，治療情報など | ゼロ知識証明で検索できる  疾患名/治療情報は医師が記録できるものとする | Aries RFC 0036: Issue Credential Protocol 1.0 / Aries RFC 0453: Issue Credential Protocol 2.0 | データに対してZk-SNARKによる検索を行う必要性があったため。 |
| 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 | 左記の情報が検証できる | SD-JWT  AnonCreds |  |
| 法人に所属することを示すVC（VP） | ・所属機関  ・権限  ・ライセンス有効期限 | 左記の情報が検証できる | Aries RFC 0023: DID Exchange Protocol 1.0 / Aries RFC 0037: Present Proof Protocol 1.0 / Aries RFC 0454: Present Proof Protocol 2.0 | 個人間でのP2Pデータ受け渡しが前提となっているため。 |
| 歩容/患者データ | ・所有者  ・センサから取得された歩行パラメータ  ・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 | 左記の情報が検証できる | SD-JWT  AnonCreds | 選択的提示が可能かつ、EUDIWでも対応必須のものとして指定。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のデータモデルの規格と併せるようバージョンアップが検討される。 |

### 本システムで形成を目指す合意とその履行のトレースの内容

　本システムで形成を目指す合意及びその履行のトレースは以下の通りである．

* 患者と医師/理学療法士間の患者の歩行，日常の痛み，体調のデータの共有
  + 医師または理学療法士がWeb上のシステムを通じてVC付きでデータ共有の要求を行い，患者が自身のスマートフォンアプリ上で承認する．
  + 履行された上記の合意について，患者はアプリ内のデータ共有履歴画面でVCの発行記録を確認，合意の取り消しが可能
  + 履行された合意/合意撤回などのトレースはブロックチェーンによるレジストリ照会によってトレース可能としている．
* 患者と研究機関または製薬会社間の患者の歩行，日常の痛み，体調のデータの共有
  + 研究機関または製薬会社がWeb上のシステムを通じてVC付きでデータ共有の要求を行い，患者が自身のスマートフォンアプリ上で承認する
  + 履行された上記の合意について，患者はアプリ内のデータ共有履歴画面でVCの発行記録を確認，合意の取り消しが可能
  + 履行された合意/合意撤回などのトレースはブロックチェーンによるレジストリ照会によってトレース可能としている．

1. https://www.w3.org/ [↑](#footnote-ref-1)
2. https://wiki.hyperledger.org/display/ARIES [↑](#footnote-ref-2)