Pracs 健康手帳プロジェクト第１フェーズ報告書

Pracs 健康手帳プロジェクト [1]

概要：PHR を始めとした医療分野へのブロックチェーン技術の応用は世界的に大きな関心を集めており、すでに実装も始まりつつあります。日本でも関心が高まりつつあります。本プロジェクトは PHR 導入の初期段階として、健康手帳として個人の健康データを管理し、医療関係者と共有していくことを目的としています。本稿ではその第１フェーズとして、秘匿化した状態で個人の健康データを医療関係者へ渡す仕組みについて、実際にプロトタイプを作成し、技術的な検証を行ったので、その概要と結果及び考察について報告します。

キーワード：PHR、健康手帳、ブロックチェーン

1. はじめに

ブロックチェーン技術は、ビットコインで実証された耐障害性、耐改ざん性に優れた技術として、主に金融分野を中心に応用分野が広がってきました。世界的には金融分野以外でも、サプライチェーンや医療・ヘルスケアなどへの応用が進んでおり、エストニアなどのブロックチェーン先進国ではすでに実用段階に入っています[1]。

PHR（Personal Health Record）とは、個人が管理できる医療健康データのことで、毎日の血圧や歩数といったバイタルデータを含む様々な情報を記録し、自らの健康状態を可視化することでセルフメディケーションに生かすことができます。医療機関は PHR によって診療情報を適切に開示することで、生活者との信頼関係を醸成したりコミュニケーションを円滑にしたりして他の医療機関と差別化する狙いがあります[2]。また、日本医師会でも医療健康データを持ち歩くものとして期待されていますが、一方では、懸念点も指摘されています[3]。医療健康データは要配慮個人情報[8]であり、その機密性は重要です。そのため、個人と医療機関との間の安全なデータの受け渡しにおけるブロックチェーンの活用が期待されています。

ブロックチェーンは、書き込んだものを消すことができないという特性を持っているため、改ざんのない状態で医療・健康記録を保存できます。規制の問題もあって将来的な話になりますが、すでにエストニアで実現しているような、医療記録の相互運用時も正確な情報の利用が可能になります。医療健康データが引き継がれないことによる無駄な再検査回避や、連絡がないための薬の副作用の抑制など、実現することによるメリットは高いものがあります。

ブロックチェーン上にデータが蓄積されていけば、医療健康データを個人が特定できないように加工した上で、ビッグデータとして、研究目的で提供することも可能になります。それにより、予防医学等の分野で技術的な進歩が期待できます。

2. PoC の目的と進め方

個人の健康データ管理アプリと医療機関との連携システムをユースケースとし、ブロックチェーンを活用したシステムの技術的実現性・有効性を見極めることを PoC の目的と設定しました。技術面に着目した理由は、医療健康データが極めてセンシティブな情報であるため、最初に越えなければならないハードルであると考えたためです。

本プロジェクトは、近畿大学発ヘルステックベンチャーであるプラクス株式会社[4]とブロックチェーン専門会社のエバーシステム株式会社[5]、I.N.S. LLC で構成され、IOST 財団[7]の支援を受けて 2020 年 6 月に開始しました。私たちは、信頼性と機密性が重要な医療・ヘルスケア分野に着目し、医療関係者にも利用者にも有用なサービスの提供を目指しています。

2.1 PoC の期間と対象者

検証は、2021 年 2 月 15 日から 2021 年 2 月 19 日に実施しました。検証には、一般の利用者として５名、技術者として２名が参加しました。第１フェーズでは、疑似データによる実証実験として、利用者側アプリとサーバーデータの検証を行います。

2.2 PoC の目的

第１フェーズの目的は、次の３つを検証することです。

- 健康データを安全な方法で医療関係者への提供することです。健康情報は、**要配慮個人情報**[8]に当たりますので、サーバー管理者でもデータの内容を見ることができない仕組みを作ります。
- ブロックチェーンへの健康データのハッシュ値の登録することで、健康データが改ざんされていないことを証明します。
- 暗号化した秘密鍵を紛失した場合に鍵を再発行でき

1 和田隆夫(エバーシステム(株)), 坂上博俊(プラクス (株)), 井出直毅(I.N.S. LLC), 白濱敬也(エバーシステム(株))

るようにすることで、医療関係者の協力により鍵が再発行できるようにします。

2.3 評価軸

利用者側の視点および技術的な視点を踏まえ、検証項目を定義しました。

(1) **運用性**

利用者におけるアプリの問題点を洗い出すため、検証環境を構築し、アンケートによる検証を実施しました。

(2) **セキュリティ**

利用者-医療機関連携ブロックチェーンシステムで具備すべきセキュリティ機能（データ秘匿やアクセス制限）への整合性を見定めるため、検証環境で保存された結果について検証を実施しました。

2.4 検証環境

2.4.1 システムの全体構成

プロジェクトのシステムは、図 1 のように、ユーザー（利用者）および医療施設をアクターとして、データベースとブロックチェーンを併用したシステムとなっています。ここでは、公開鍵暗号技術をブロックチェーン内外で利用しています。重要な点は、生の暗号化されていない医療健康データは、ユーザの手元のスマホの中だけに保持するようにしています。

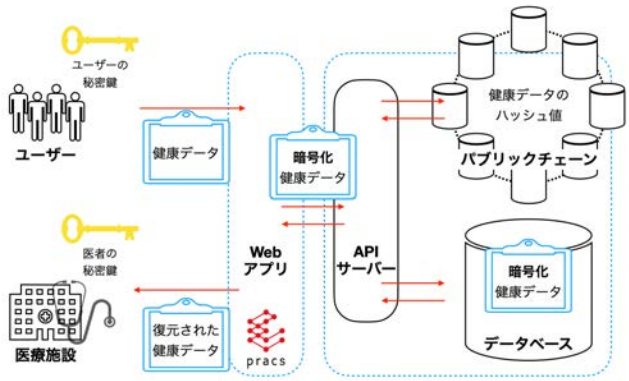


図 1　プロジェクトの全体構成

1. ユーザーが医療機関に医療健康情報を提供する場合には、ユーザーの操作で、ユーザーの秘密鍵と医療関係者の公開鍵を使って暗号化して、サーバーに格納します。その際に、元データのハッシュ値も同時にブロックチェーンに記録していきます。
2. この暗号化されたデータを、医療機関側で、医療機関の秘密鍵を使って、復号化します。これで、ユーザーの健康データを読み取ることができます。その際にはブロックチェーンで、その情報の正確性も検証します。
3. スマートフォン端末のトラブルなどで、ユーザーが秘密鍵を紛失し、データも紛失した場合は、サーバーに暗号化したデータはありますが、復号できなくなるので実質データが消失したのと同じことになります。その場合は、新たな秘密鍵、公開鍵のペアを作った上で、医療機関に依頼して、サーバーの暗号化したデータを再暗号化してもらうことで、ユーザーがデータを取り戻すことができるようにします。

2.4.2 第 1 フェーズの検証環境構成

第 1 フェーズの検証環境は、図 2 のような構成にしました。API サーバーは Amazon AWS[9]クラウド内に、EC2 上に Docker ベースで構築し、サーバーへの直接アクセスを避けて、プライベートネット内で稼働させています。セキュリティを確保するため、証明書を付与したロードバランサー経由で、HTTPS プロトコルでアクセスします。ロードバランサーには、将来的に負荷が増大した場合への対応も考慮しています。

サーバー本体は、Nest.js+TypeORM で、TypeScript 言語で実装しました。図にはありませんが、メンテナンス用に踏み台となる Bastion サーバーを利用しています。API サーバーは、基本的に REST ベースで実装し、主要な機能はクライアントとストレージとの読み書きの仲介です。

データベースとしては、MySQL ベースの AWS Aurora データベース、ブロックチェーンには第 3 世代ブロックチェーンとして期待されている IOST のプライベートチェーンを採用しています。健康データの保存 API では、データベースへの暗号化データの保存と、ブロックチェーンへのデータのハッシュ値の保存の 2 フェーズのコミットを実装しています。

クライアントアプリは Android、iOS のマルチデバイスに対応するため、Flutter フレームワーク[10]を利用して Dart 言語で制作しました。本システムは、セキュリティの観点からクライアントサイドで暗号化の主要部分を実装しています。スマートフォン内の健康データも暗号化して、ローカルのセキュアストレージに保存しています。

認証は Auth0 サービス[11]を利用し、サインアップ、サインイン、JWT アクセストークンを利用した API アクセスの機能を実装しています。API サーバーでは、アクセストークンを利用してクライアントを認証します。

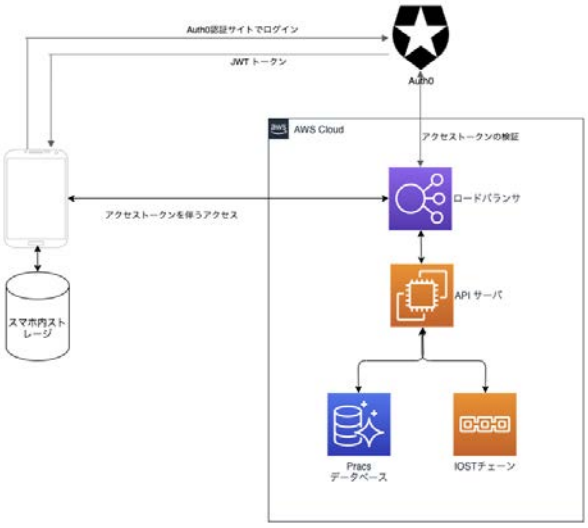


図 2　第１フェーズの検証環境構成

2.4.3 システムのアクセス手順

クライアントアプリでデータ登録し、サーバーへデータを送る手順について説明します。画面の遷移は図３のようになります。

1. ユーザはスマートフォンアプリを起動します。
2. アカウントがない場合は、サインアップします。この段階でアカウントが作成され、秘密鍵が生成され、ローカルストレージ（スマートフォン内のストレージ）に保存します。
3. Auth0 で、OAuth またはメールアドレスとパスワードでログインします。この場合は、アカウントはローカルストレージのものが利用されます。
4. 体温入力画面での体温を入力や血圧画面での血圧を入力すると、暗号化した上で、ローカルストレージに保存し、さらにサーバーへ送信します。
5. サーバでは、アクセストークンを認証した上で、送信されたデータをデータベースへ、データのハッシュ値をブロックチェーンに保存します。
6. スマートフォンの画面では、グラフで過去のデータを含めて表示されます。

図 3　利用者画面とその遷移

3. PoC の結果

3.1 セキュリティの検証

保存されたデータベースデータには、図４のように暗号化されたデータとハッシュ値、検証のための署名が保存されています。ブロックチェーンには、図５のように最新のデータ項目ごと（体温、血圧など）に医療健康データのハッシュ値が保存され、ブロックチェーン上のレシートには図６のようにその履歴が記録されています。ブロックチェーンのストレージ上のデータは最終結果ですが、レシートはブロックチェーンのデータを更新した都度書き込みがされ、永久に残されていきます。

これらのデータは、秘密鍵なしでは復号ができません。また、保存されたデータベースデータおよびブロックチェーンのデータは、クライアントアプリで正確に復号されていることが確認できました。


```
    "encrypted_data":
"M9AoqqK8NrDQu8utQqZ713quUiDZUmCq4ff1faJZPkNhdtzbT3
mD4HaVsrgrNHaHKCpwNW4UrDsBUxQYB5binRiXrrAAwNKvT
4hrb",
    "hash":
"4vuvLeS3kGWMKeMgbp1tunPGMsfGYrH1bE5eKSjyRzKsXjZc9
h8zsp8yUhLvy9TkWCFZwKTczUQTjhUbSbqTHFqk",
    "sig":
"2ULU4xFvK8izpSmaLDunddDwJ77XNfGqbMfAusm6Vxne1bfuR
dw59sp4TGC3hy2pDjiYwsZSQuyTGJ15jNeYoZJv"
```


図 4　データベースに保存されたデータの例


```
BWskxPHj8Gbog7h8DqR88f655NQUCP9cRT7LxRaYvV3v
```


図 5　ブロックチェーンに記録されたハッシュ値の例

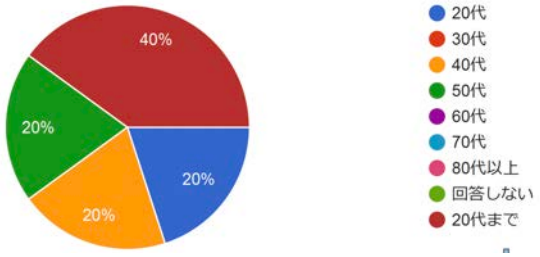

```
BWskxPHj8Gbog7h8DqR88f655NQUCP9cRT7LxRaYvV3v
```


図 6　ブロックチェーンに記録されたレシート情報の例

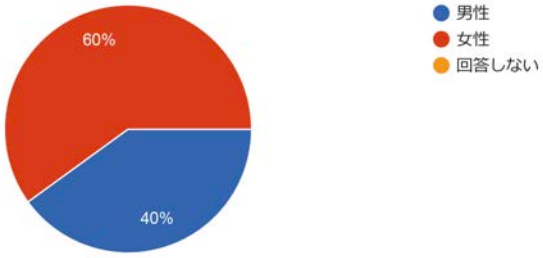
3.2 利用者アンケート

(1)　回答者について

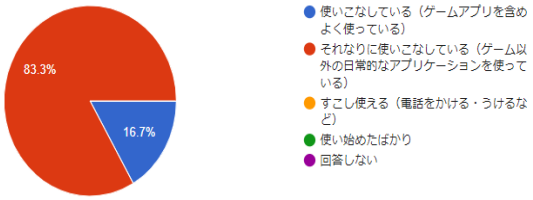
(ア) 使用いただいている方について、年齢をお教えください。



(イ) 使用していただいている方について、性別をお教えください

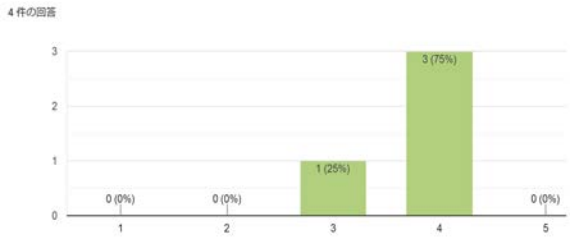


(ウ) スマートフォンの使用頻度について（自己申告で構いません）



(2)　アプリケーションについて

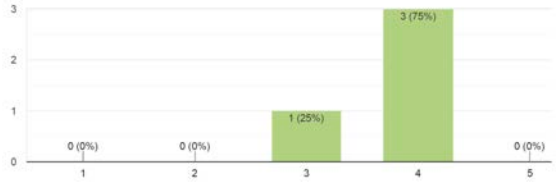
(ア) 使いやすさについて（５が良）



(イ) 使いやすい・使いにくいと感じた部分を教えてください。（自由記述）

体温を入力した時に｜←のような物が点滅して登録を押しても点滅のままで消えなかったので、℃を入力しないといけないかと思い℃で登録を押したら体温の画面が無地になってしまいました。
入力は複雑では無さそうです。

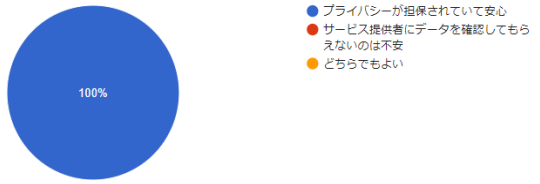
(ウ) デザインのわかりやすさについて（５が良）



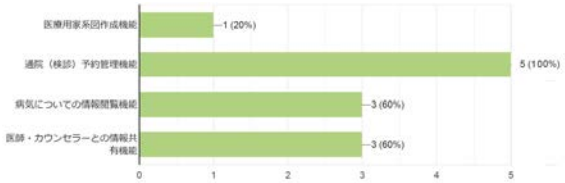
(エ) わかりやすい・わかりにくいと感じた部分を教えてください。（自由記述）

わかりやすいとは思うのですが、日本語表示がよりわかりやすいと思います。
日本市場なので体温，血圧と日本語で書けばよいのでは。次回受診日のところのデザインが切れてて何時までなのかわからない。
グラフの値遷移が集中しているように感じるので拡大機能や月指定などできれば見やすいと思います

(オ) あなたの承認した医療関係者以外は、サービス提供者(プラクス株式会社やアプリ制作会社)であったとしても、あなたの医療情報を見ることが出来ないことについてどう思いますか？



(カ) 欲しい機能・項目について（複数選択可）



(キ) 他に欲しい機能・項目について（自由記述）

自分の欲しい項目がなかったときなどに使えるメモ欄？フリーで使えるところがあるといいのかなと思ってみたりもします。
次回受診日，問診表，問診結果メモの詳細ページの実装
体重の記録もできたら便利だなと思いました。
血糖値、血液検査の結果

(ク) その他（気づきなどなんでもご自由にお書きください）

スマホを使い慣れてない方にも優しい物が出来ると嬉しいです。

3.3 技術者サイドで、上がった問題点

IT 技術者に利用してもらった際のアンケートでは、次のような回答がありました。

「鍵を共有している医師を前提でのプライバシーの担保になっている。医師からのアクセスを断ち切ることが可能かどうかわからない。」

4. 考察

今回の PoC により、秘匿化健康情報の引き渡しについては、有効性が確認できました。

ただ、クライアントアプリについては、使い勝手についてはさほど問題ないものの、アンケートで回答いただいた内容も踏まえて、データの項目やなど利用者や引き渡し先の医療関係者の要望をヒアリングした上で設定していくことが重要にだとわかりました。

技術者の医療関係者側の信頼によるセキュリティに関する指摘については、データ自体を再暗号化すれば解決はできるものの、本質的にユーザー側、医療側の立場を再度検討すべきもので、次フェーズでの検討課題としました。

5. おわりに

本稿では、健康手帳プロジェクトの第１フェーズについて報告しました。第２フェーズでは、日本での PHR 実現に向けて、ステップバイステップで実用的なシステムとして進めていきます。

謝辞　本プロジェクトに協力いただいた IOST 財団に、謹んで感謝の意を表します。

参考文献

[1] Monex Crypto Bank 編集部, “エストニアの医療分野におけるブロックチェーン活用”, https://crypto-lab.info/?p=8438, (参照 2021-03-11).

[2] “コロナ時代の武器に。医療健康データ持ち歩く「PHR」のすべて”, https://newswitch.jp/p/24054, (参照 2021-03-11).

[3] “日本医師会の主張、医療健康データ持ち歩く「PHR」の価値と懸念”, https://newswitch.jp/p/24078, (参照 2021-03-11).

[4] “プラクス株式会社 Web サイト”, https://pracs.co.jp/.(参照 2021-03-11).

[5] “エバーシステム株式会社 Web サイト”, https://eversystem.co.jp/.(参照 2021-03-11).

[6] “I.N.S. LLC Web サイト”, https://xxxxxx. (参照 2021-03-11).
[7] “IOST Foundation 公式サイト, https://iost.io. (参照 2021-03-11).
[8] “要配慮個人情報に関する政令の方向性について”,
https://www.ppc.go.jp/files/pdf/280603_siryou1.pdf.
[9] “Amzon Web サービス”, https://aws.amazon.com/jp/.
[10] “Flutter”, https://flutter.dev/.
[11] “Auth0”, https://auth0.com/jp/.