

Web3.0 時代における 共通基盤の実現性について

日本アクチュアリー会

IT 研究会第 4 グループ

【担当委員】

松岡 靖之	三菱 UFJ 信託銀行
勝海 宏	プルデンシャル生命

【メンバー】

佐々木 大地	明治安田生命
小山 祐輝	明治安田生命
水谷 圭祐	明治安田生命
安部 裕介	フコク情報システム
池野 僚亮	全国共済農業協同組合連合会
平賀 智之	ニッセイ情報テクノロジー
光吉 堯	ニッセイ情報テクノロジー

【目次】

- I. はじめに
- II. Web3.0 時代とは
- III. Web3.0 時代のデータ活用基盤構想
- IV. 共通基盤に求められる仕組み
- V. 共通基盤の構築
- VI. 実現可能性の検証
- VII. 課題
- VIII. 結論
- IX. 謝辞

I. はじめに

昨今、個人に関するデジタル情報¹の管理と活用に対する考え方として、Web3.0 が注目されている。Web3.0 とは「個人データは個人自身で所有し、自由に活用できるべきである」という考え方で、近年、問題視されている Google や Amazon などの巨大テクノロジー企業による個人データの独占やプライバシーの侵害に対する懸念を、解決することが期待されている。我々は、今後、Web3.0 の考え方が浸透していくことで、従来、企業中心に行われていた中央集権的な個人データの管理と活用の仕組みは衰退し、個人中心の非中央集権的な個人データの所有と活用へと、大きく変化していくものと考えており、このような世界を Web3.0 時代と定義した。

Web3.0 時代に向けては、個人データの取扱いの変化だけでなく、企業のビジネスモデルも変化していくと考えられる。従来は、企業が顧客から個人情報収集し、それを自社で利用することで提供するサービスの価値を高めてきた。しかし、これからは、従来の企業での個人情報の管理に加えて、顧客自身も個人情報を管理し、利用できるようになる。これにより、個人データの漏えいや不正利用のリスクを低減すると共に、様々なサービスで顧客自身の個人データを自由に活用することで、自身に最適化されたサービスをより多く享受できるようになると考えられる。

金融業界においても、Web3.0 時代に適応する必要があると考えた。例えば、生命保険業界の場合、複数契約の一元管理・比較や保全手続きの効率化などの顧客利便性の向上、顧客情報の共有による保険会社の業務効率化や新商品開発など、社会や顧客から求められることも変化し、これらに対応しなければならないと推察される。

また、Web3.0 時代を支える技術として、ブロックチェーン技術に大きな期待が集まっている。ブロックチェーン技術とは、分散型台帳管理技術のひとつであり、分散化によるデータ改ざんや不正の防止、データの透明性や信頼性の向上、処理の自動実行などが可能である。これにより、第三者に頼らない非中央集権的な個人データ管理が実現されることとなる。

当研究グループでは、保険業界が Web3.0 時代に対応するための手段として、ブロックチェーン技術を活用したデータ共有基盤の構想について研究を行った。当論文では、研究結果として、基盤構想とその技術的な実現方法および企業を含む利用者にとってのメリット、実現に向けた課題と解決方針について論じる。

¹ 個人情報保護法に定義される個人情報に限らず、各種 SNS への投稿内容やアプリで取得した歩数データなど、個人に関するあらゆるデジタル情報のことを指す。当論文では「個人データ」と表記する

II. Web3.0 時代とは

1. Web3.0 とは

Web3.0 とは、これまでの Web1.0／Web2.0 に続く、新たな Web システムの形態である。

1990 年代に始まった Web1.0 では、通信速度も遅く HTML など静的なもので構成された Web ページ（静的なウェブサイトや検索エンジンなど）であり、情報発信するのは一部の企業や個人に限られ、情報発信者が情報を提供し、サービス利用者はコンピューターを活用して情報を閲覧する一方向の情報伝達で成り立っていた。

次に続く 2000 年代中頃の Web2.0 は、具体的な技術を明確に指し示す用語ではなく、インターネットの通信速度が高速になり、スマートフォンを活用して誰もが自由に情報発信できるような双方向の情報伝達で成り立っている。Web2.0 は「参加する時代」のインターネットで Instagram や YouTube などのソーシャルネットワークワーキングサービス（SNS）の普及により、個人がコンテンツを作成・編集し共有することが可能となった。しかし、サービス利用者の情報は企業が中央集権でセキュアに管理している。これに対して、Web3.0 は Web1.0（一方向）／Web2.0（双方向）と異なり当事者間の相互作用で成り立っており、利用デバイスに変化はなく、個人データを企業中心（中央集権型ネットワーク）ではなく個人中心（非中央集権型ネットワーク）で管理する Web システムである。

2. Web3.0 が求められる背景

Web3.0 が求められる背景には、Web2.0 のビジネスモデルにおける問題と顧客層の変化の 2 つがある。

(1) Web2.0 のビジネスモデルにおける問題

Web2.0 では SNS などの便利なサービス提供企業に利用者の個人データが集中して保持される特徴があり、特に GAFAM（Google・Amazon・Facebook・Apple・Microsoft）に代表される巨大テクノロジー企業が独占している状態である。

Web2.0 のビジネスモデルは、利用者がサービスを利用することで、サービス提供企業に個人データが蓄積され、サービス提供企業はその膨大な個人データを活用して、利用者のニーズに適した新サービスを企画・提供し自社の価値を高める仕組みになっている。このようなビジネスモデルによってデータ活用の重要性が増したことで、サービス提供企業による個人データの囲い込みが行われるようになり、利用者とサービス提供企業以外の企業にとって様々な問題が発生している。

利用者視点では、サービスを受けるために、必要以上の使途不明なデータをサービス提供企業へ提供しなければならないなどの問題がある。

企業視点では、既存サービス提供企業が個人データを囲い込んでいるため、新しい企業が新サービスを開発して新規参入しようとしても、サービス開発に必要な情報を手に入れられない。そのため、参入障壁が高く、よりよいサービスがあっても提供する機会を損失しているという問題がある。

(2) 顧客層の変化

従来のビジネスモデル（Web2.0 のビジネスモデル）で獲得してきた顧客層に対して、これから働き盛りを迎える Z 世代はスマートフォンをメインの生活機器として利用しており、目的別に複数のサービスを使い分け、口コミ・レビューや比較検討によりタイムパフォーマンスを重視しており、自身の価値観を大切すると言われている。また、パーソナライズされた体験・経験を重視するなど既存の顧客層とは異なる傾向を持つため、Web2.0 のビジネスモデルにおける従来の広告マーケティング手法（サービス提供企業が蓄積した情報だけのマス広告やダイレクト広告など）では興味関心を持たれることが少ないことから、今後の顧客層（Z 世代）とも親和したビジネスモデルを考えていく必要がある。

3. Web2.0 から Web3.0 時代に向けた変化の方向性

(1) Web2.0 のビジネスモデルにおける問題の解消について

Web2.0 のビジネスモデルで起きている問題の解消方法を Web3.0 時代のビジネスモデルを踏まえて説明する。Web3.0 時代のビジネスモデルは利用者がサービスを利用するとこれまでサービス提供企業にのみ蓄積していた個人データを利用者も所有し活用することが可能となる。これにより、利用者は自身が利用したサービスで得たデータを、他の企業に提供してサービスを受けられるようになり、Web2.0 のビジネスモデルで問題となった「個人データの囲い込み」「新規参入時の参入障壁」が解消できる。

(2) これからの保険業界の変化について

保険会社も他のサービスと同じく、これまで各社が中央集権で顧客の個人データをセキュアに管理しており、自社のマーケティング・商品開発などに活用してきた。Web3.0 時代のビジネスモデルでは、これだけではなく利用者の持つ他の情報・属性の提供を受けることで、より利用者に寄り添ったサービスが提供できるように、自社の価値を高めていく必要があると考えられる。また、これからの保険会社のメインターゲット層である Z 世代の特徴を踏まえると

Web3.0 と親和性が高いため保険会社も Web3.0 時代に適応していく必要がある。当研究グループでは Web3.0 時代における保険業界として提供が求められる 2 つのサービスを考えた。

a. 保険提案の新たな顧客体験（パーソナライズ化）

保険会社が従来から持つ契約情報に、利用者が持つ個人データを付加することで保険会社から利用者へパーソナライズ化された保険提案を受けられるサービス

b. 保険の選択手段の多様化（保険の比較）

Z 世代の特徴を踏まえ、多くの保険会社が提供する様々な保険商品の中から顧客が重視する基準（保険料、特約種類、対面／非対面のフォローなど）で効率よく比較できるサービス

今後上記のサービスを実現するためには、資本系列を超えた複数の保険会社と横断的に協働し、多様な外部サービスと連携可能な情報活用基盤が必要となると考える。当研究グループでは Web3.0 に関連する技術であるブロックチェーン技術を活用した新たな共通基盤（情報活用基盤）を提案する。

(3) 金融業界における Web3.0 取組み状況

銀行業界では、Web3.0 に関連する技術の活用事例として、三菱 UFJ 信託銀行株式会社が、資本系列を超えた複数の金融機関と横断的に協働のうえ、日本法に準拠したステーブルコインの発行・管理基盤である「Progmatic Coin（プログラマコイン）」基盤を活用し、グローバルに流通可能な“国産ステーブルコイン”の発行に向けた共同検討を開始した状況である。

一方で、金融業界全体としての取組みは進んでおらず、アクチュアリー会員企業に「ビジネス活用に向けて取り組んでいるまたは取り組もうとしている新技術があるか」というアンケートを事前に実施したところ、ブロックチェーンに取り組んでいる（取り組もうとしている）企業は、有効回答数に対して 5%（全 44 件中 2 件）の状況であった。

III. Web3.0 時代のデータ活用基盤構想

前章では、Web3.0 時代に対応するためには、金融業界の各社が持つ個人データが、各社間で相互に利用可能になる必要があることを述べた。本章では、各社間の相互利用を実現するためのデータ活用基盤の構想について述べていく。

1. データ活用基盤の構想

データ活用基盤の構想にあたっては、2つの軸で検討を進めた。1つは誰から他社サービスで作られた個人データを受け取るかという「データ流通経路」の観点で、各社間でデータ共有する方法と個人からデータを受け取る方法の2つが考えられる。もう1つは、データ共有の仕組みを誰が作るかという「データ活用基盤を構築および運用する単位」の観点で、各社が個別に構築する方法と共通基盤を社会全体または業界で構築する方法が考えられる。

以下では、それぞれの観点でどのような形が最適であるかを考察したうえで、Web3.0時代のデータ活用基盤の構想を進める。

(1) 「データ流通経路」の考察

データ流通経路として、各社間でデータ共有する方法と個人からデータを受け取る方法の2つを考えた。そして、評価の結果、個人からデータを受け取る方法が適切であると我々は結論づけた。

その理由は、各社間でデータ共有する方法には、個人データの共有許諾の問題があると考えたためである。他社に個人データを共有する際には、当然ながら個人に対して共有の許諾が必要となる。しかしながら、共有先を一定の範囲に限定したいなどのニーズは個人に認められるべきであり、全員に対して一律に包括的なデータ共有の許諾を取り付けることは、現実的には不可能であると考えた。

個人からデータを受け取る方法であれば、この問題は解決することができる。個人がデータ活用基盤を利用して企業に個人データを提供する際に、提供する個人データの種類や開示範囲、利用範囲を指定できるようにすれば良いからである。この方法をとる前提としては、個人データを個人が所有していることが必要になる。これにより「業界や企業によるデータの囲い込み」も防ぐことが可能となる。一方、各社間でデータ共有する場合に比べて、セキュリティなどの観点で、検討すべき課題は多くなると考えられる。

上記より、一定の課題はあるものの、データ流通経路としては個人が各社にデータを提供する方法が適切であり、提供の際も個人が許可した企業に許可した個人データのみが提供される形にすることが必要であると結論づけた。

(2) 「データ活用基盤を構築および運用する単位」の考察

データ活用基盤を構築および運用する単位として、各社が個別に構築する方法と共通基盤を社会全体もしくは業界で構築する方法を考えた。我々は、その中から、業界で共通基盤を作る方法が適切であると結論づけた。

初めに、各社が個別に構築する方法には、各社の開発運用負荷の問題があると考えた。この方法では、各社がデータを個人から受け取る仕組みを構築する必要があるが、データを共有する企業の数だけデータ活用基盤が構築・運用されることになり、業界全体で考えると企業数に比例して負担も大きくなる。そのため、社会全体もしくは業界での共通基盤の構築が必要になると考えた。

他には、個人がデータ共有する負荷が高いことも問題となる。個人が各社に個人の個人データを提供するには、各社のデータ提供の仕組み（Web システムやスマートフォンアプリなど）を利用することになるため負荷が高くなる。また、保険証券などは紙媒体で発行されることが多いが、それらをデジタルデータとして提供するための入力や撮影の負荷も高いと推察される。

更に、各社から個人に対してデータ提供を依頼する方法が少ないことも実現を阻害する要因となる。個人にデータ提供を依頼する方法としては、ダイレクトメールやウェブ広告などが考えられるが、個人がサービスを実際に受けている企業以外に対して、個人データを提供するメリットはイメージしづらく、この方法でユーザーからデータを提供してもらうことは難しいと考えた。

次に、共通基盤を作る方法についてであるが、当初は社会全体で作ることが効率面でみると最適であるように考えた。しかし、検討を進める中で、誰が基盤構築および運用を統制するかという課題が出てきた。データ活用を促進するためには、基盤上で流通するデータの量と質が重要である。データの量については、他の業種のデータも基盤上に流通可能になることや業界各社のサービス競争を促すことで実現できるものと考えた。一方で、データの質を上げるためには、標準化やデータの確からしさの保証などが必要になるが、統率者がいない状態で業界をまたがって実現することは極めて困難であると考えた。したがって、業界ごとの共通基盤を業界団体が統率をとって構築することが最も現実的な解であると考えた。

既存の業界で扱う情報は似た内容・性質のことが多いと考えられるため、業界ごとに共通基盤を作る方法であれば、標準の策定なども比較的スムーズに行われることが想定される。現に、生命保険共同センターネットワーク

（LINC）や損害保険代理店ネットワーク（損保 VAN）、全国銀行資金決済ネットワーク（全銀ネット）など、当構想と目的は異なるものの、業界ごとの標準化は既に進められてきている。

こうすることで、社会全体で共通基盤を構築するよりも早くデータの量や質が向上して、個人によるデータ活用が促進されることが期待できると考えた。そのうえで、それら業界共通基盤間の連携については、個人を介して実現することが適当であると考えた。

2. 保険業界における業界共通基盤とは

前節では、Web3.0 時代のデータ活用基盤とは「ユーザーが企業に対して主体的にデータを提供して、データを活用したサービスを受けることができる業界共通基盤があり、それらがユーザーを介して連携することで実現される社会共通の基盤」と定めた。

当グループでは、当構想の実現性を研究するにあたって、当構想の最小単位である業界共通基盤を研究テーマとし、具体例として保険業界における共通基盤について研究を進めることとした。

本節では、当基盤で扱うデータの種類と構築・運用の体制について述べる。

(1) 取扱うデータ種類

当基盤では、原則、個人データはすべて個人が所有し、自由に活用できる状態にするべきであると考えた。これは、前述したとおり、データ活用を加速するにはデータの量が重要になるためであり、少しでも利用できるデータを増やすためには、出来る限りのデータを個人に所有・活用させることが必要であると考えたからである。取り扱うデータの内容としては、保険証券や控除証明書など、保険契約に関するあらゆる情報を想定している。また、生命保険会社が提供するスマートフォンアプリなどで日々計測されるデータなど、保険契約に関係しないデータも含まれる。

一方で、引受査定や支払査定などに関する情報については、慎重に取り扱う必要があると考えており、例えば告知内容や請求内容とその査定結果については個人が自由に活用することができる様にする一方で、査定結果に至った理由などは、個人にデータを提供はするもののデータとしての活用は生命保険会社側で制限をかけることが可能にするなどが考えられる。

(2) 構築体制

業界単位の共通基盤は大きく分けて、業界団体と業界各社、個人ユーザーの3者で構築・運用されることになると考えている。

保険業界を例にとると、生命保険協会と各生命保険会社、契約者および白地顧客の3者となる考えた。ここでは保険業界を例にとりそれぞれの役割について述べる。

a. 生命保険協会

当基盤構想の推進リーダーとして、全体を俯瞰してプロジェクトを推進・運用していく役割となる。

具体的には、各生命保険会社間の要件調整やコスト負担の割り当てルールなど、保険業界としての共通基盤構想を作り上げることが求められる。

また、共通基盤を生命保険会社や個人にとって、使いやすく利便性が高いものとするためにも、取り扱うデータ種類や項目の標準化、共通基盤上で稼働するアプリケーションやサービスなどの標準化、開発運用ツールの整備提供、共通基盤上で扱えるデータカタログの整備なども必要となる。

さらに、運用面でも当基盤を個人に浸透させるための施策、例えば当基盤の活用事例の紹介や他社サービスの紹介プラットフォームの構築などの施策検討やアンケートを実施しての改善など継続的な活動が必要となる。

b. 各生命保険会社

当共通基盤の開発および運用のリソース提供と、他生命保険会社のサービスで個人が得たデータを利用できるアプリケーションやサービスの提供が主な役割となる。

開発および運用のリソース提供としては、開発運用要員としての人的リソースを提供することや、基盤を維持するためのマシンリソースやコスト負担などが考えられる。また、生命保険協会のメンバーとして基盤設計に携わることが必要となる。

そして、最も重要となるのは、他社の情報を活用した良いサービス提供し続けることであり、これが当共通基盤を盛り上げる推進力となると考えている。補足となるが、これを実行するには、従来の自社でデータを集めて自社のサービスだけに活用するという Web2.0 時代の考え方を捨て、Web3.0 時代におけるユーザー中心の考え方にマインドチェンジすることが重要であり、最もハードルが高い課題になると考えている。

c. 契約者および白地顧客

従来、個人は企業の提供するサービスを受ける立場であったが、当共通基盤を構築・運用するうえでは重要な役割を持つ。それは生命保険会社間のデータ流通のハブとなるということである。

データ流通のハブとしての役割を満たすにあたっては「積極的に多くのデータを集めて活用すること」この1点が重要である。これは、当基盤構想を実現する肝の1つでもあり、生命保険会社と契約を締結する際や各社の提供するサービスを利用した際に、データを自分のスマートフォンなどに保管することと、そのデータを他社に提供してサービスを受けることなどが考えられる。

そのためには、対面や紙媒体など現物を中心としたサービスから、デジタルサービスの利用へシフトしていく必要があり、企業側の努力だけでなく、デジタルを有効的に活用するというマインドの醸成が重要となる。そういった意味でも、Z世代に代表されるデジタルネイティブ世代が、当基盤の中心ユーザーとなるであろうと考えた。

IV. 共通基盤に求められる仕組み

我々は、活発にデータ流通・活用するための共通基盤について「ユーザーが個人データを所有し、自由に活用できる業界共通基盤」をコンセプトとして、当基盤の実現方法を検討した。

1. システム構想の概要（全体感）

当基盤の実現には大きく3つの仕組みが必要になると考えた。

(1) ユーザーが個人データを所有する仕組み

ユーザーが個人データを活用するために、今まで生命保険会社で管理していたデータをユーザーに提供して、ユーザー自身でデータを所有する仕組み。これによって、ユーザー中心の個人データ活用が実現される。

(2) 個人データの開示範囲を管理する仕組み

ユーザーが所有する個人データに対して、データ種類単位やアプリケーション単位などで開示範囲を設定する仕組み。サービスで利用する最小限の個人データのみを開示できるようにすることで、セキュリティの向上だけでなく、不本意にデータを利用されることを防ぐ。

(3) 個人データを活用する仕組み

ユーザーが所有する個人データを生命保険会社に提供することで、個人データでパーソナライズされたサービスを受けられる仕組み。これによってユーザーは、これまで以上の利益を得ることができる。

2. 共通基盤を支える技術

共通基盤の実現性検討にあたって必要となる Web3.0 技術について説明する。

(1) ブロックチェーン

分散型台帳技術の1つで、中央管理者が存在せず、サーバー・PC・スマートフォンなどからネットワークに参加するすべてのノードが、P2P ネットワ

ークでつながり、同一内容のデータを共有することで、データやトランザクションを分散管理することができる。データやトランザクションは、ブロックという単位でチェーンのように前後関係をもって記録される。そのため、データの改ざんや障害に高い耐性をもつ。

また、データやトランザクションの記録以外にも、あらかじめ決められた条件で自動的に処理を行う「スマートコントラクト」や各ノードで合意形成をするための「コンセンサスアルゴリズム」などの機能を持つ。

ブロックチェーンネットワークは、以下の3種類に分類され、ネットワークへの参加ノード数や利用する業務の特性などによって、最適なものを選択する必要がある。

a. パブリック型ブロックチェーン

制限なく参加できるオープンなネットワークであり、参加者は事前に許可される必要はない。誰でも自由に取引に参加することが可能。すべての情報は公開されており非中央集権的で透明性が高い一方、参加者が多くなると処理速度の低下や運用コストが高くなる懸念がある。

b. プライベート型ブロックチェーン

特定の組織や企業のみが参加できるクローズなネットワークであり、事前に許可されたユーザーのみが参加可能。参加者が限られているため、セキュリティが高く、処理速度も高速で運用コストも低く抑えられるという特徴を持つ。一方で、管理者に集権的になるリスクや透明性の確保が難しくなる懸念などもある。

c. コンソーシアム型ブロックチェーン

パブリックとプライベートの要素を組み合わせたネットワークであり、データ共有範囲のニーズや、セキュリティと透明性のバランスを求める場合に使用される。

(2) ウォレット

ブロックチェーンで用いる秘密鍵を保存してトランザクションの署名を行う機能と、公開鍵のハッシュ値からウォレットアドレスを生成する機能を持つアプリケーションである。ウォレットアドレスはトランザクションの処理や履歴の確認などブロックチェーン上でのやり取りを行うための個人を特定しない一意の識別子である。これらの機能はブロックチェーンへの参加に必須であるため、参加ノードにはウォレットの導入が必要となる。

(3) スマートコントラクト

契約や取引を自動化するためのプログラムである。条件と処理内容を決めたコードで構成し、そのコードをブロックチェーン上で実行する。これによって実行履歴が分散管理され、信頼性と透明性が確保される。さらに自動実行されることで中央集権化された機関や第三者を排除でき、公正性が確保される。

(4) DID (Decentralized Identifier)

自己主権型 ID (SSI : Self-Sovereign Identity) を、Web3.0 において実現する手段としての分散型識別子のことを指す。DID を用いることで、生命保険会社から提供された個人データを改ざんした場合に、生命保険会社が改ざんを検知することができる。

この仕組みの説明は次の通りである。発行者は VC (Verifiable Credential) という自身が署名した信頼できるデータ形式で発行をする。この時、ブロックチェーン上に提供先の DID と発行情報を同様に署名した DID ドキュメントを登録する。データを受け取った所有者は複数または単一の VC の一部や全てを VP (Verifiable Presentation) というデータ形式で提示することができる。所有者が提示した VP は、ブロックチェーン上に登録された DID と発行情報の署名と VP の署名が一致することを確認することで信頼性を確認できる。本研究ではこの仕組みのことを DID とする。

3. 共通基盤のアーキテクチャー

この業界共通基盤は大きく 2 つの仕組みで構成される。1 つは、業務システムをユーザーが実行するためのブロックチェーンである。もう 1 つは改ざん検知用のブロックチェーンである。

それぞれのブロックチェーンにはユーザー（保険契約者などの基盤を利用する各個人）、各生命保険会社、生保協会が参加する。ユーザーはスマートフォン、PC、タブレット上のウォレットアプリをノードとして、各生命保険会社はブロックチェーン用に構築したサーバー上のウォレットをノードとしてブロックチェーンへ参加する。

さらに、各生命保険会社は自社の業務システムをブロックチェーンから呼び出せるよう、業務システム実行用の API を準備する（図 1. 共通基盤のアーキテクチャー）。2 つのブロックチェーンの役割については以下で説明する。

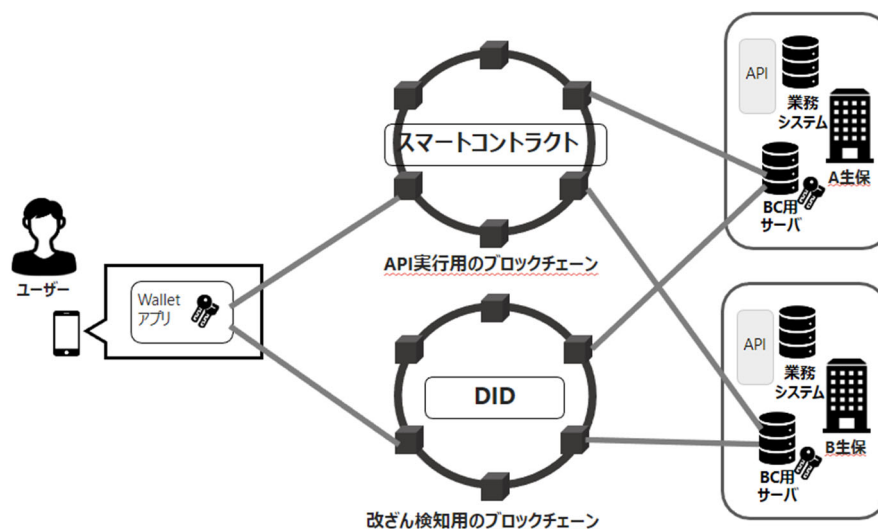


図 1. 共通基盤のアーキテクチャー

(1) 共通基盤のブロックチェーンについて

今回の共通基盤におけるブロックチェーンネットワークは、コンソーシアム型で構築することを考える。まず、パブリック型の場合は、ブロックチェーンの管理者を用意できないため業界共通基盤の運営が困難となることや共通基盤参加者以外にもデータが開示される問題がある。次にプライベート型は、個人の共通基盤への参加にも承認が必要となるため、多くのユーザーの共通基盤の利用が困難となる。その点、コンソーシアム型については、複数の管理者を用意でき、データの開示も共通基盤参加者に限定される。また個人への参加承認も不要とすることができる。以上の理由より、コンソーシアム型のブロックチェーンが共通基盤に適していると言える。

今回の共通基盤のブロックチェーンは、Hyperledger プロジェクトで開発されたブロックチェーンを利用する。このプロジェクトで開発する基盤は、コンソーシアム型であり、さらに外部システムとの連携に必要な要素の「高い柔軟性」と、多くの利用者を許容できる「スケーラビリティ」を持っているため、今回の共通基盤に適している。また、日立や富士通などのテクノロジー企業がビジネス活用に向けて、オープンソースにより開発を活発に取り組んでいるプロジェクトであるため、今後の技術革新が期待できる。また、有識者による知見や経験が蓄積されており、それらを参考にすれば共通基盤の構築もスムーズになると見込まれる。

a. 各社業務システムを呼び出す API 実行用ブロックチェーン

API 実行用ブロックチェーンは、各生命保険会社で準備した業務システムの API を呼び出すためのブロックチェーンとなる。この基盤は、保険契

約などの手続きをスマートコントラクトで自動化することで、仲介者を介さずに一括で処理することが実現できる。そのため、今回の共通基盤に適しているといえる。

このブロックチェーン基盤については、Hyperledger Fabric を利用する。Hyperledger Fabric は Hyperledger が提供するオープンソースプロジェクトの 1 つで、プライベートネットワークによるデータの共有範囲の制御が可能である。

b. 改ざん検知のための DID 用ブロックチェーン

DID 用ブロックチェーンの基盤については、Hyperledger Indy という企業向けのブロックチェーンプラットフォームを利用する。Hyperledger Indy は Hyperledger が提供するオープンソースプロジェクトの 1 つで、DID に特化したアプリケーション・フレームワークで、SSI を実装するためのツール、ライブラリ、再利用可能なコンポーネントが提供される。

4. 機能要件

本節では前述の 3 つの仕組みを実現するための機能要件について述べる。

(1) ユーザーがデータを所有する仕組み

a. データ提供機能

当機能は生命保険会社からユーザーのウォレットに保険契約データを提供する機能である。当機能はネット生保などの営業員がいない生命保険会社でも必要になるため、ユーザーから生命保険会社に申請を行う想定とする。

また、データ提供後にユーザーの契約内容に変更があった場合、変更内容を反映した最新の保険契約データを提供する機能も有する。

b. 提供データの改ざん検知用情報発行機能

当機能は生命保険会社がユーザーにデータ提供する際に、データの改ざんを検知するための情報を作成して公開する機能である。データを利用する第三者はこの情報を参照して改ざんを検知する想定とする。

(2) ユーザーにてデータ開示範囲を管理する仕組み

a. ユーザーにてデータ開示範囲を管理する機能

ウォレットアプリには企業から提供されたデータが蓄積される。ウォレットアプリと連携するスマートフォンアプリに対してどの範囲のデータを

開示するかをユーザーの意思で管理する機能である。ユーザーが管理することで企業にとってデータの価値が向上し、ユーザーから企業へのデータ提供の対価としてサービスを受けられる。また、ユーザーの意思に反してデータが使われることを防ぐことができる。

(3) 個人データを活用する仕組み

a. 各社システムの実行機能

ユーザーがウォレットアプリに保管している個人データを活用することで各生命保険会社からサービスを受けられるための機能である。

各社のシステムを実行することで、ウォレットアプリ内で管理された個人データから開示許可した個人データのみを各社に提供することを可能とする。

b. 活用データの改ざん検知機能

ユーザーがウォレットアプリに保管している個人データを各生命保険会社に提供してサービスを受ける際、ユーザーから提供された個人データに改ざんがないことを各社が確認する機能である。

V. 共通基盤の構築

1. 共通基盤を利用する準備

生命保険会社とユーザーが共通基盤のブロックチェーンに参加するための準備を説明する。

(1) 生命保険会社の準備

構想する共通基盤はブロックチェーンで構築し、そこから各社業務システムの利用を考えているため、ブロックチェーンへの参加方法の検討と業務システムとの連動の準備を考える。

a. ブロックチェーンへの参加

生命保険会社がブロックチェーンへ参加するために、ブロックチェーンのノードを立てることと、生保協会から参加承認をもらうことの2つが必要となる。

生命保険会社はまず、ブロックチェーンノードとしての専用サーバーを構築し、ウォレットを生保協会会員ページよりダウンロードしサーバーに導入する。

次に、参加承認をもらうために、生命保険会社が書類で生保協会へ参加依頼を送付する。生保協会は、受け取った書類の確認と承認を行い、ブロックチェーン参加に必要な秘密鍵を生命保険会社へ返送する。生命保険会社は、受け取った秘密鍵を前述で準備したサーバーのウォレットに配置することでブロックチェーンに参加できる。

b. 共通基盤と各社業務システムの連動

共通基盤を活用した各社スマートフォンアプリと各社の業務システムを連携するために、API は各社で事前準備をする。ブロックチェーンから各社業務システム API を各社に公開する。

(2) ユーザー側の準備

a. ブロックチェーンへの参加

ユーザー用のウォレット（ウォレットアプリ）は、各ユーザー自身のスマートフォン、タブレット向けに用意されているアプリストアよりインストールする形式とする。インストールした際に、ウォレットアプリからユーザーに対して共通基盤への参加要否を確認する。ユーザーが端末上で参加を選択することでユーザーは共通基盤のブロックチェーンに参加する。

b. 共通基盤上で稼働する各社スマートフォンアプリについて

共通基盤に対応した各社が提供するスマートフォンアプリをインストールした際、各社スマートフォンアプリとウォレットアプリの接続要否を端末上でユーザーに確認する。ユーザーが接続を許可することで、各社スマートフォンアプリはウォレットアプリを介して共通基盤を利用することができる。

2. 共通基盤上で稼働するプログラムの開発

本節では、共通基盤上で動作するプログラムの開発方法と利用の流れについて述べる。

(1) 事前準備

共通基盤上で稼働するプログラムはスマートコントラクトとして開発を行うが、事前準備として必要な作業は採用するブロックチェーンごとに異なる。今回共通基盤に採用する Hyperledger Fabric の場合、事前準備として開発端末とブロックチェーンサーバーの準備が必要となる。

開発端末は各社においてプログラム開発を行うために準備する端末であり、開発するプログラム言語に対応するコンパイラと Hyperledger Fabric 用のライブラリをインストールする。開発用のためブロックチェーンに接続する必要はなく、複数台用意することも可能である。

ブロックチェーンサーバーは各社のウォレットがインストールされたブロックチェーンに接続するためのサーバーとなる。ブロックチェーン上へのプログラムのリリースにはウォレットが必要となるため、Hyperledger Fabric 用のリリース機能をインストールする。

(2) プログラムの開発とリリースの流れ

まず開発端末を使用してプログラムを開発する。その後開発端末上で開発したプログラムをコンパイルすることでプログラムの実行ファイルが生成される。

次に生成した実行ファイルをブロックチェーンサーバー上のリリース機能を用いてブロックチェーン上へリリースすると、ブロックチェーンに参加している各サーバーに実行ファイルが配布され、ブロックチェーンに参加する全てのサーバーにてプログラムの実行が可能となる。なお、Hyperledger Fabric の場合、プログラム名を指定して実行することが可能である。

(3) プログラムの検索

ブロックチェーン技術を利用するため、プログラムはブロックチェーン上に登録される。そのため、リリースが正常に完了したことの確認やブロックチェーン上にどのようなプログラムが登録されているか検索可能な仕組みが必要となる。

ブロックチェーン上の情報を検索する仕組みとして、ブロックエクスプローラーを用いる。ブロックエクスプローラーはブロックチェーン上のブロックを遡りながら、ブロック内のトランザクションを確認する機能がある。この機能を使用することで、ブロックチェーン上のトランザクション情報からブロックチェーン上にどのようなプログラムが保存されているかを確認可能である。また、プログラム名だけではなくプログラムを利用するためのパラメータ情報や誰がいつリリースしたといった情報も確認が可能なので、自社がリリースしたプログラムの一覧の検索も可能である。

(4) ユーザー利用までの流れ

前述の仕組みを利用することで、ブロックチェーン上にて新規サービスを実行する準備まで行うことが可能である。

ユーザー側が新規サービスを利用するためには、新規サービスに対応する各社スマートフォンアプリをスマートフォンにインストールする。その後、ユーザーの操作によりスマートフォンアプリからウォレットアプリを通して新規サービスが実行され、新規サービスの利用データがウォレットアプリに保存される。

VI. 実現可能性の検証

本章では、構想した共通基盤の機能要件の実装方法を提示し、システム面と運用面での実現可能性を検証する。

1. 実現性の検証

(1) ユーザーがデータを所有する仕組み

a. データ提供機能

ア. システム面での検証

ウォレットへのデータ提供は、DID で実現可能と評価した。理由は提供データを VC として発行可能なためである。生命保険会社は、ユーザーからの申請を確認済みであること、提供データの源泉であるユーザーの契約情報の更新が完了していることの両条件を満たしたタイミングで、業務システムから自動でデータを VC としてユーザーのウォレットに提供する。

なお、データ提供の申請はユーザーから生命保険会社に行う場合と、生命保険会社からユーザーに申請要否を確認のうえ行う場合が考えられるが、当研究では前者を想定している。生命保険会社からユーザーに申請用の URL を連携し、ユーザーが URL にアクセスするとウォレットアプリが起動して申請画面に遷移する。ユーザーはこの申請画面で生命保険会社へのデータ提供申請が可能。

また、データ提供後にユーザーの契約内容に変更があった場合の最新データ提供についても、上記と同様の理由から DID で実現が可能と評価した。ユーザーのウォレットアドレスと申請を確認した情報を業務システム上に保存しておくことで、契約内容の更新処理が反映したタイミングで自動的に VC をユーザーのウォレットに提供可能である。

イ. 運用面での検証

ユーザーにデータ提供するタイミングは、ユーザーが新規契約時に希望して提供するケースと、データ提供後にユーザーの契約情報

に変更があった場合に自動で提供するケースの2つが考えられる。
いずれも以下のとおり運用可能のため実現可能と評価した。

まずは新規契約のケースについて記載する。契約締結後、その場で生命保険会社の営業員はユーザーの希望を確認のうえ、申請画面に遷移可能な URL を QR コードとして自社端末に表示してユーザーに提示する。営業員がいない生命保険会社の場合も URL をユーザーにメール送信することで代替可能である。

次にデータ提供後にユーザーの契約情報に変更があった場合のケースについて記載する。こちらはデータ提供が業務システムと DID で自動的に行われる想定のため、運用面での実現性に課題はないと評価した。

b. 提供データの改ざん検知用情報発行機能

ア. システム面での検証

DID を利用することで実現可能であると評価した。生命保険会社がデータ提供する際に、提供したデータに対応する DID ドキュメントを登録しておくことで、第三者がデータを利用する際に、該当する DID を参照することで改ざんを検知できる。

イ. 運用面での検証

DID ドキュメント登録のタイミングは、契約成立時とそれ以降の収納や支払のタイミングが考えられるが、各社の業務システムおよび共通基盤上でシステムの的に実行されるため、運用面での実現性に課題はないと評価した。

(2) ユーザーにてデータ開示範囲を管理する仕組み

a. ユーザーにてデータ開示範囲を管理する機能

ア. システム面での検証

システム面での実現性は、ウォレットに保存したデータに対して活用可否を設定するフラグを設定することで実現可能であると評価した。ウォレットアプリ内にスマートフォンアプリごとのフラグ領域を構成し、データ領域に保存されたデータの項目ごとに対応するフラグをこの領域内に設ける。作成したフラグには活用可否を保持する。連携したスマートフォンアプリからデータの要求がされると、要求されたデータに対応したフラグを参照し、アクセスの拒否または許可を判断する。この判断に基づいて許可されたデータのみ

の VP を作成して連携したアプリケーションに提供することで開示範囲を管理できる。

イ. 運用面での検証

管理するデータが大量であるとフラグ設定が煩雑になるため、データの種類ごとにレベルを設定し、ユーザーは開示するレベルを設定することで全てのデータを一元的に管理できる。レベル設定は個人情報保護法に定められた個人情報の有用性の程度などを参考にして生保協会が標準を策定することで実現可能。開示するデータのレベルを設定した後、VP の提供までの動きは自動で処理されるため運用面での課題は無いと評価した。

(3) 個人データを活用する仕組み

a. 各社システムの実行機能

ア. システム面での検証

システム面での実現性は、ユーザーが VP を発行し、共通基盤上でスマートコントラクトと DID を利用することにより実現可能であると評価した。

ユーザーは複数もしくは単一の VC から開示許可した個人データを VP として発行し、共通基盤に対して VP を送信する。

VP を受け取った共通基盤はスマートコントラクトを実行することで、該当の API を呼び出し、各生命保険会社に対して個人データ提供できる。

イ. 運用面での検証

この一連の処理は、各生命保険会社が提供するスマートフォンアプリで自動的に実行され、ユーザーが一連の動作を意識する必要がないため、運用面での実現性に課題はないと評価した。

b. 活用データの改ざん検知機能

ア. システム面での検証

システム面での実現性は、DID を利用することで実現可能であると評価した。

各生命保険会社が個人データ活用する際に、個人データを VP として受け取り、それに対して DID ドキュメントで検証することで改

ざんを検知することが可能となり、サービスを不正に利用されることを防ぐことができる。

イ. 運用面での検証

この一連の処理は、各生命保険会社の提供するスマートフォンアプリやサービスおよび共通基盤上で自動的に実行されるため、運用面での実現性に課題はないと評価した。

2. 結論

共通基盤に求められる3つの仕組みは、システム面と運用面の両方で実現可能であり「ユーザーが自身のデータを所有し、自由に活用できる業界共通基盤」は技術的に実現可能であると考えた。

VII. 課題

1. 「個人によるデータ管理」から生じる課題

ウォレットアプリで生成するキーについてはウォレットアプリ上で管理する。従来のソフトウェアであれば、端末を失くしたとしても、パスワードの再発行を行うことで、他の端末からのアクセスが可能である。しかし、ウォレット上の秘密鍵はウォレットアプリ上で生成されているため、端末を失くした際に再発行を行う手段がない。そのため、端末を失くした際に取引（共通基盤アプリの利用）ができなくなるリスクが発生する。

そのリスクを回避するために考えられる方法として、クラウドシステムで秘密鍵と個人データのバックアップを取ることが考えられる。ただし、クラウドへの侵入のリスクがある。それについては、クラウドからデータを取り出す際に、生体データとの照合を行うことでリスクを回避できるのではないだろうか。

2. DID 検索時間の短縮

ユーザーのウォレットに蓄積されたデータの改ざん有無を確認するために DID の技術を使うと述べたが、DID 登録情報の検索機能について課題が存在する。

改ざん有無を確認する際、DID の登録情報を過去に遡り該当データが見つかるまで検索を続ける必要がある。保険の中でも生命保険は契約期間が数十年になる商品があるため、契約時に提供したデータの DID 登録情報を確認する場合、数十年前に遡って検索が必要な可能性がある。この場合、検索所要時間が長期化し、共通基盤を使用したアプリケーションの性能要件を満たすことができないことが予想される。この問題を解消するため、検索所要時間の短縮化が課題となる。契約期間が

数十年単位になる商品は他業界含めても稀有であるため、保険業界特有の課題といえる。

この課題はスナップショットという技術で、DID ドキュメントデータを断面的に保存することで解決できる可能性がある。データ提供時やデータ内容変更時のDID 記録内容をスナップショットで部分的に保存しておき、データの改ざん有無を確認する際に参照することができれば、前述の過去に遡って検索する方法と比較すると検索スピードが大幅に短縮されることが期待される。

3. ブロックチェーン技術者の確保

ブロックチェーン上で稼働するプログラムの開発やブロックチェーンに接続するノードの保守・運用を行うにはブロックチェーンの知識や技術を持った技術者でなければ困難である。しかし、アクチュアリー会員企業に「ビジネス活用に向けて、取り組んでいるまたは取り組もうとしている新技術はありますか」というアンケートを実施したところ、ブロックチェーンを選択した会員企業は44社中2社であり、金融業界での活用は進んでいないことが判明した。そのため、現時点では技術者が不足していると考えられ、業界共通基盤としてブロックチェーンを採用する場合には、各社で新たにブロックチェーン技術者を確保・育成する必要がある。

4. 各生命保険会社の参加意欲の向上

当グループで研究した業界共通基盤は生命保険業界全体で使用する基盤であるため、会社の規模に関係なく多くの生命保険会社に参加してもらうことが望ましい。業界共通基盤に参加する生命保険会社が少ないとユーザーが活用できるデータも少なくなるため、ユーザーが参加のメリットを感じずにユーザー側の参加も少なくなると予想される。

大手の生命保険会社と中小の生命保険会社それぞれの事情で参加に慎重になると考えられるため、それらの内容と解決の方向性を記載する。

大手の生命保険会社の場合、すでに保険業界におけるユーザーの囲い込みもできており、従来のビジネスモデルを変えてまで共通基盤を活用することにメリットを感じにくいと考えられる。

この大手の生命保険会社の課題の解決には、保険業界全体で共通基盤の有用性や必要性を浸透させることが不可欠である。前述のとおり、共通基盤は現状ではアプローチが効果的に進んでいないZ世代への親和性が高いという有用性がある。そのほかにもユーザーとの間でデータ活用が進むことで従来では入手できなかったデータを入手できるという有用性もある。以上のような利点を生保協会が先頭に立って大手の生命保険会社と共有し、各社の参加動機付けを進めていくことが求められる。

次に中小の生命保険会社の場合、共通基盤に参加するにあたっての費用負担が相対的に大きくなるため、メリットを感じにくいと考えられる。

この中小の生命保険会社の課題の解決には、ブロックチェーン基盤の開発ツールの整備やデータ標準化を進めて、開発工数を低減させることが不可欠である。生保協会は、共通基盤の参加は費用に見合うだけの利点があることを共有するだけでなく、開発の障壁が高くないことも中小の生命保険会社に示し、各社の参加動機付けをしていく必要があると考える。

VIII. 結論

Web3.0 時代の生命保険業界における共通基盤は、ユーザーにとってのより良いサービス価値が提供され、データ活用が進むことでユーザーだけでなく生命保険会社にとってもより良いサービス開発・提供の機会につながる。この共通基盤は、ブロックチェーン技術を使うことで実現は可能であることが検証できた。

一方で、共通基盤を活用していくためには課題もある。特に各生命保険会社の参加意欲の向上においては、すべての生命保険会社にとってメリットを感じられる活用方法を検討していく必要があるなど、大きな課題も残されている。これらの課題は、保険業界全体で協力しなければ解決ができないものであると結論付けた。

今後、Web3.0 の考え方は、世界中に浸透していくものと予想される。当研究では保険業界を具体例として説明してきたが、業界共通基盤の考え方は保険業界のみならず金融業界全体に当てはまるものである。そのため、金融業界全体で検討を進める必要があり、対応を先送りするとビジネスチャンスを逃し、金融業界全体の不利益につながると考えられる。また、金融庁が定める顧客本位の業務運営には、顧客にふさわしいサービス提供を行うという原則がある。顧客に最適なサービスという観点でも、金融業界は Web3.0 時代の考え方にマインドチェンジする必要があるのではないだろうか。

共通基盤そのものの構築だけでなく、既存のビジネスモデルを変える必要もあり各企業の負担も大きい。我々研究メンバーを含む金融業界で一丸となって、Web3.0 時代の共通基盤活用に取り組んでいきたい。

IX. 謝辞

本研究を進めるにあたっては、大変多くの方々にご支援をいただきました。

レクチャーを実施いただき、幅広く見識や今後の展望をお聞かせいただきました株式会社日立製作所、並びにアンケートにご協力いただきましたアクチュアリー会法人会員各社の皆様には、特に大変感謝いたしております。私たちの活動を支えてくださった多くの方々に、この場をお借りして深く御礼申し上げます。

以上