Computer Security Symposium 2020
26 - 29 October 2020

主体的なアクセスコントロールのための 自己主権型アイデンティティに基づく認証機能と データ共有機能を備えたシステムアーキテクチャ

野村 健太[1,*] 熊谷 裕志[1] 神薗 雅紀[1]

概要：ウェブサービスの普及に伴い，一人のユーザが複数のウェブサービスに対してそれぞれアカウントを有することが一般的となった．更に，自身の利用データをサービス提供事業者に共有することで新たなサービスを享受できるようになった．しかし，各サービスでユーザは個別に認証を受ける必要があり，認証情報やアイデンティティ情報の管理が煩雑化している．データの利活用についても，特定のプラットフォーマーにユーザ及び利用データが集中した結果，サービスの囲い込みへ繋がっている．個別認証によって管理が煩雑化したことや囲い込みによってデータのコントロールが難しくなった結果，本人の意図しないプライバシー侵害が発生している．その対策として個人が主体的にアイデンティティ情報とデータの共有範囲や共有相手を管理する仕組みが求められている．本稿では既存のアイデンティティ管理及びデータ共有に伴う課題を提示し，解決に向けたシステムアーキテクチャを提案する．提案アーキテクチャの利点を整理した上で，実装への課題と検討事項について考察し，ユースケースについて検討する．

キーワード：自己主権型アイデンティティ，分散 ID，属性ベース暗号，分散台帳，分散ストレージ

A System Architecture with Self-Sovereign Identity-based Authentication and Data Sharing for Proactive Access Control

Kenta Nomura[1,*] Hiroshi Kumagai[1] Masaki Kamizono[1]

Abstract: With the spread of web services, a user has a separate account for multiple services. Users can enjoy new services by sharing their usage data with service providers. However, users have to be authenticated individually for each service, which makes the management of authentication and identity information more complicated. The concentration of users and usage data on a specific platformer leads to the enclosure of services. As a result of the complicated management due to individual authentication and the difficulty in controlling data due to enclosure, unintentional privacy violations have occurred. As a countermeasure, individuals are required to manage their own identity information and the content and scope of data sharing. In this paper, we propose a system architecture to solve the problems of identity management and data sharing. After summarizing the advantages of the proposed architecture, issues and considerations for implementation are discussed and use cases are discussed.

Keywords: Self-Sovereign Identity, Decentralized Identifier, Attribute-Based Encryption, Distributed Ledger Technology, Distributed storage

1. はじめに

インターネットの普及に伴い，ユーザは様々なサービスをオンライン上で受けられるようになった．利用時にはユーザのアカウントを登録し，認証を受けることでサービスを受けることができる．独立した複数のウェブサービスを利用する際には，各サービスでユーザのアカウントを登録し，個別に認証を受ける必要がある．個別に認証が行われるため，認証情報やアカウントに付随するアイデンティティ情報の管理が煩雑なものになっている．

個別認証の煩雑さを解消するために，複数のサービス間でアカウントを関連付けて，統一した認証情報で認証を行うフェデレーション認証モデルが注目されている．しかし，ウェブサービスに関連付けられるアカウントの種類は限定されている場合が多く，大きなシェアを持つウェブサービスのアカウントがほとんどである．そのため，結果的にユーザがフェデレーション認証を利用して認証を統合化するためには，特定のウェブサービスのアカウントを保有することが必要となる．こうした背景もあり，大きなシェアを持つプラットフォームに個人のアイデンティティ情報が集中していることが問題視されている．プラットフォームが集中すると，市場の独占や寡占によって新規参入を拒んだり，不当な価格設定が行われたりするおそれがある．更に，プラットフォームが保有する個人データが多くなればなるほど，漏えいした際の被害も大きなものになる．SNS（social networking service）で最大のシェアを誇る Facebook は複数回情報漏えいの被害にあっており[1, 2]，Google が運営する SNS でも情報漏えいが疑われる事象が発生したことから，サービスの休止を余儀なくされた[3]．こうした現状を受け，オンラインのアイデンティティ情報は特定の企業が

1 デロイト トーマツ サイバー合同会社
Deloitte Tohmatsu Cyber LLC
* kenta.nomura@tohmatsu.co.jp

管理するのではなく個人ユーザが主体的に管理・維持していくべきだという考え方が広まってきている．

ユーザのアイデンティティ情報と合わせて，ユーザの収集するデータやユーザがサービスに活用するデータにも注目が集まっている．日本でも情報通信技術を活用し，サイバー空間とフィジカル空間を融合させて，データの利活用サイクルを回す Society5.0 と呼ばれる取り組みが行われている[4, 5]. フィジカル空間のデータには個人のプライバシー情報が含まれていることも多く，世界各地で OECD8 原則[6]に基づくプライバシー情報保護規則が進めている．各企業には規則の遵守が求められ，違反すると賠償責任が発生する場合がある．例えば，「EU 一般データ保護規則（GDPR: General Data Protection Regulation）」では最大で全世界売上高の 4%もしくは 2000 万ユーロもの制裁金の支払いが科せられる．2019 年 7 月には GDPR 違反として，イギリスの航空会社ブリティッシュ・エアウェイズに 1 億 8300 万ポンドの制裁金が科されたことが話題となった[7].

規制を遵守するために，取り扱うデータの整理やそれに伴うシステムの改修、運用フローの修正が必要となる場合があり，サービス提供事業者にとって大きなコストになりうる．一方で，サービス提供事業者がデータを保有しなければ，対応コストの削減やレギュレーション違反の削減につながる場合がある．プライバシー情報の観点からも個人ユーザが主体的に自らのデータを保護する仕組みづくりが求められている．

ユーザが主体的に自らのデータを管理する仕組みとして情報銀行と呼ばれるものがある．日本では総務省が[8]で，ユーザの指示または予め指定した条件に基づいて，ユーザに変わって第三者へ提供する事業と定義している．情報銀行では第三者である情報銀行事業者がユーザのデータをサービス提供事業者と仲介することで，ユーザの個人情報の提供範囲や内容の把握を支援する．サービス提供事業者へのデータ提供によってユーザ本人に対して何らかの利益が還元される場合もある．一方で，プライバシーの完全な確保が難しい点，情報銀行事業者が必要以上に開示してしまうリスク等，課題が山積している．

こうしたアイデンティティ管理とデータ保護に関する課題を解決する次世代アーキテクチャの提案・構築が進められている[9]．本稿ではアイデンティティの管理だけではなく，サービスに活用するデータの共有においてもユーザが主体的にデータを管理するためのシステムアーキテクチャを提案する．構築に向けたアイディアとして，自己主権型アイデンティティ（SSI: Self-Sovereign Identity）の概念に基づく DID（Decentralized Identifier）[10]と属性ベース暗号による分散ストレージのデータ共有を組み合わせたアーキテクチャを検討する．提案アーキテクチャの利点及び実装に向けた課題や検討事項を考察し，ユースケースについても検討する．

2. 既存手法の課題

2.1 アイデンティティ管理

オンライン上でのアイデンティティ管理で現在主流となっているのは，サービス提供事業者が独自の識別子（ID: identifier）を使ってユーザのアイデンティティを管理する集中型モデルや複数のサービスに対して，単一の ID を使って認証を行うフェデレーションモデルといった仕組みである[11]. これらの仕組みが抱えている課題をユーザ, サービス提供事業者のそれぞれの視点から挙げる．

2.1.1 ユーザにおける課題

(1) アイデンティティの非永続性

サービス提供事業者が提供するユーザアカウントは，サービス提供事業者の一存でアカウントが停止されてしまうおそれがある．電子書籍や配信楽曲等の購入が当該 ID に紐付いていた場合，アカウントの停止に伴って該当コンテンツも利用できなくなる．また，サービス自体が休止してしまうと，ID 自体が利用できなくなる．このように，特定のサービスに依存したアイデンティティは永続性を持たず，サービス提供事業者にコントロールされている状態と言える．

(2) サイロ化したアイデンティティ

ビジネス・IT 領域において，業務プロセスや各種システムが孤立して情報や運用フローが連携されていない様子を，家畜の飼料や農産物を貯蔵する倉庫に例えてサイロ化した状態と呼ぶことがある．個人のアイデンティティでも同様のことが発生している．独立した複数のサービスを利用する際には, 各サービスでアカウントを作成する必要がある．各サービスでアイデンティティ情報や認証情報を管理する必要があり，ユーザの負担は少なくない．住所変更等に伴うアイデンティティ情報の変更も全てのサービスに対して行う必要がある．各サービスのプライバシーポリシーにはユーザのアイデンティティ情報に関する扱いが明記されているため，ユーザはサービス利用時に確認することが求められる．しかし，各サービスでプライバシーポリシーは異なるため，ユーザは各プライバシーポリシーの内容や違いを把握する必要があり，大きな負担を強いられている．

(3) セキュリティ意識の低下

ID に紐付く氏名や住所等のアイデンティティ情報はサービス提供事業者側が保有・管理する．サービス提供事業者のセキュリティ対策状況はユーザからは確認できないため, セキュリティリスクを正確に見積もることが難しい．ユーザ側でも一部の対策は可能であるが，非コントロール性やサイロ化によって不可能もしくは対応がしづらい状況となっている．ID とパスワードの使い回しや必要以上の個人情報を登録する等，利便性やサービス利用を優先した結果，セキュリティへの意識や対策が疎かになるおそれがある．特定のサービスに多くのアイデンティティ情報を登録した

結果，他のサービスでも同程度の情報を登録しても構わない，といった考えになることも考えられる．

2.1.2 サービス提供事業者における課題

(1) 情報の真正性の担保／本人確認の困難さ

ウェブサービスはアカウント登録がオンライン上で完結できる利便性があるが，オンライン上ではイデンティティ情報の真正性の保証や本人確認が難しい．インターネットバンキングやクレジットカードサービス等のアカウント発行には本人確認書類のスキャンをアップロードして本人確認を行うこともある．電話番号の存在確認には，携帯電話の SMS（short message service）を利用した SMS 認証を利用する例もある．こうした認証作業に係る確認コストも無視できないものと考える．

(2) なりすまし／不正アクセスの防止

ID とパスワードで認証を行うサービスはどこからでもアクセスやサービス利用できる一方で，正規のユーザを確かめることが難しい．対策として二要素認証を備えるサービスもあるが，オプションの設定である場合が多く，抜本的な解決には至っていない．

(3) 取得情報の保護

e コマースのアカウントにはクレジットカードの情報が紐付いていることも多く，当該アカウントにおけるアイデンティティ情報が漏えいすると，不正利用のリスクも生じる．情報漏えいを引き起こしてしまうと，GDPR の制裁金のような直接的な処罰に加えて，会社のレピュテーション毀損にも繋がり，経営的にも大きな影響を受ける．こうした事態を避けるためにもサービス提供事業者はユーザのアイデンティティ情報を厳格に管理する必要がある．

2.2 データ共有

本稿では個人ユーザとサービス提供事業者がデータを共有，もしくは個人ユーザからサービス提供事業者にデータを提供するシナリオを想定する．

2.2.1 ユーザにおける課題

(1) 囲い込みのリスク

Society5.0 ではデータの利活用サイクルが注目されているが，各サービスだけでサイクルが完結してしまうと，ユーザやデータの囲い込みにも繋がる．ユーザのデータを反映したサービスを提供できる一方で，ユーザ側からは特定のサービス提供事業者にロックインされてしまうおそれがある．

(2) データの非コントロール性

サービス提供事業者がユーザのデータを第三者へ提供する際に，第三者提供の合意をユーザに取得することが求められているが，取得の方法は厳格には定義されていない．サービス利用規約に記載されている場合も少なくないが，規約自体が長文かつ冗長な表現になっている場合も多く，確認はユーザの負担となる．確認が不十分だった結果，本人が意図しない第三者提供やプライバシー侵害に繋がる場合もある．また，提供したデータの削除や利用停止についてはユーザ側から利用停止の申請が必要な場合もあり，ユーザ自身のデータであっても，コントロールが難しい状況が発生する．情報銀行を利用して包括的な管理を行った場合でも，全てのサービスに対してユーザの意図通りに開示される保証はない．

(3) ストレージの可用性

サービス提供事業者が用意したストレージでデータを利活用する場合，可用性も課題の一つとして挙げられる．事業者側の不具合やメンテナンスがあった場合，ユーザは当該ストレージにアクセスできなくなり，完全なサービスを受けられない場合がある．

2.2.2 サービス提供事業者における課題

(1) データそのものの取り扱い

サービス提供事業者には各種規制を遵守した個人データの厳格な取り扱いが欠かせない．ユーザとの合意形成や利用停止を受け付けるオプトアウトへの対応に加えて，それらを実現するためのシステム改修や運用フローの修正等，様々な対応が必要となる．更に，他の企業と連携してデータを活用する場合には匿名化の処理や適切な受け渡し等，より慎重な取り扱いが求められ，ユーザのデータを保有することはメリットである一方で，デメリットとなる点も少なくない．

(2) データ共有ストレージの運用コスト及び設計コスト

データ共有のために自前もしくはクラウドサービスを利用する場合，ストレージの容量を定める必要がある．自前のストレージを用意する場合は，利用者数に合わせてシステム設計が必要となる．クラウドサービスを利用する場合，従量課金によって柔軟に対応ができる一方で，急激なデータ量の増加によって想定外のコストが発生するおそれもある．

(3) 各種設定の厳格化

自社でデータを取り扱う場合，システム上の設定も慎重な対応が求められる．社員のアクセス制御やサーバの公開設定の設定ミスによって，情報漏えいのインシデントにつながった例も少なくない．

3. 周辺知識

3.1 SSI

SSI とはユーザ自身が自身のデジタルアイデンティの利用範囲と資格情報を管理できることを目指した概念である．厳格な定義は定まっていないものの，Allen らは SSI が備えるべき原則として，Existence, Control, Access, Transparency, Persistence， Portability， Interoperability， Consent， Minimalization，Protection の 10 原則を提案しており[12]，当該原則がデファクトスタンダードとして扱われている．

3.2 DID

SSI を実現する技術として，DID の検討が進められてい

る．これは分散的に管理される識別子を実現する仕組みであり，分散台帳や分散データベースを利用することで該当の識別子を取得できる．これまではサービス提供事業者がIDを発行し，ユーザが利用する形式だったが，DIDはユーザ自身が発行し，既存のIDやアイデンティティ情報を関連付けて利用する．ウェブ技術の標準化を行うWorld Wide Web Consortium（W3C）が中心となって標準化が進められており，データモデルやライフサイクル等がまとめられている[10].

3.3 Verifiable Credential Data Model

アイデンティティ情報をオンライン上で検証する仕組みとして，W3Cが提案するVerifiable Credential Data Modelがある．第三者が検証できるアイデンティティ情報をVerifiable Credential（VC）として定義しており，VCには証明したいアイデンティティ情報や発行者の情報，検証のための情報が含まれる．他者への提供・連携のために，一つ以上のVCを取りまとめてPresentationと呼ばれる単位で扱うこともできる．また，Presentationに対して，証明のための情報を付け加えたものを，Verifiable Presentation（VP）と呼ぶ．当該モデルを構成するエンティティと各エンティティの役割は以下の通り．

- Issuer: Holderに対してVCを発行する．
- Holder: 一つ以上のVCを保有し，Verifierに提供するためのPresentationを作成できる．
- Verifier: Presentationを受け取る．必要に応じて，検証のための処理を実行する．
- Verifiable Data Registry: 識別子，鍵情報，VC，失効情報等，VCの作成と検証を仲介するために必要なシステムのこと．信頼されたデータベース，分散データベース，分散台帳技術等によって実現される．

3.4 InterPlanetary File System（IPFS）

IPFS[13]はPeer to Peerに基づく分散ファイルシステムであり，ネットワーク内の各ノードがデータを保有して参加者同士がデータのやり取りを行う．既存のクラウドストレージと比較して，IPFSは中央集権的なサーバが不要であり，データの実体が様々な場所に分散されている点がメリットとして挙げられる．IPFSにファイルをアップロードすると，ユニークなハッシュ文字列を取得できる．当該文字列がコンテンツの識別子として利用され，コンテンツを取得するためには当該文字列が必要となる．

3.5 属性ベース暗号

特定のデータを複数人で共有する際のアクセスコントロールの手段として，属性ベース暗号（Attribute-Based Encryption: ABE）[15]-[17]が提案されている．ABEは個人を文字列で区別するIDベース暗号[14]を拡張した方式としてSahaiらによって提案された[15]．ABEには鍵ポリシー属性ベース暗号（key-policy ABE: KP-ABE）[16]と暗号文ポリシー属性ベース暗号（ciphertext-policy ABE: CP-ABE）[17]がある．前者は復号ができる属性条件がユーザの秘密鍵に関連付けられており，後者は暗号文に関連付けられている．

4. システムアーキテクチャ

4.1 アプローチ

個別認証による煩雑化，本人確認の困難さを解消するために，統一したアイデンティティ管理基盤を構築する．更に特定プラットフォーマーによる囲い込みを防ぎ，ユーザデータのプライバシーを保護するため，アクセス制御可能なデータ共有機能を備えるものとする．構築はDIDを前提としたID設計に基づき，VCによって第三者がユーザのアイデンティティ情報を検証可能であるのとする．また，特定のプラットフォーマーによらないデータ共有のためにIPFSを利用してデータを共有するものとする．データの暗号化にはCP-ABEを使い，サービス提供事業者の持つ秘密鍵の属性を復号条件として設定して暗号化することで，柔軟なアクセス制御を可能にする．

4.2 エンティティ

本稿で提案するシステムアーキテクチャを図 1 に示す．当該システムアーキテクチャを構成する要素は以下の通り．

- ユーザ: サービス提供事業者が提供するサービスを利用する．DIDと関連付くVCを提示し，認証を受ける．VC Data ModelにおけるHolderの役割を果たす．
- 個人デバイス: サービスへの認証，DID及びVCの管理，共有データのアップロード，属性ベース暗号の鍵の管理，分散台帳への書き込みを行う．各種処理に必要な情報はデバイス内の専用モジュールで管理する．
- サービス提供事業者: ユーザに対して特定のサービスを提供する．ユーザの認証はID基盤に基づくDIDとVCで行う．VC Data ModelにおけるVerifierの役割を果たす．
- 運用ノード: 分散台帳のトランザクションデータを管理する．また，分散ストレージとしての役割も担い，各個人デバイスからのデータアップロード及びサービス提供事業者へのデータ提供を行う．
- VC発行機関: ユーザの申請に対してDIDと関連付けたVCを発行し，分散台帳に記録する．発行機関自体もDIDを持ち，自らが発行したことを保証する．VC Data ModelにおけるIssuerの役割を果たす．
- 分散台帳: 本アーキテクチャにおける各処理をトランザクションデータとして記録する．VC Data ModelにおけるVerifiable Data Registryの役割を果たす．
- ID基盤: 各ユーザは一つ以上DIDを持ち，各DIDにVCを関連付けることができる．関連付けの情報は分散台帳に書き込まれ，真正性が保たれる．

4.3 対象範囲と前提

本稿ではアイデンティティ管理に求められる機能のうち，ユーザのアイデンティティ情報を発行し，発行した情報に

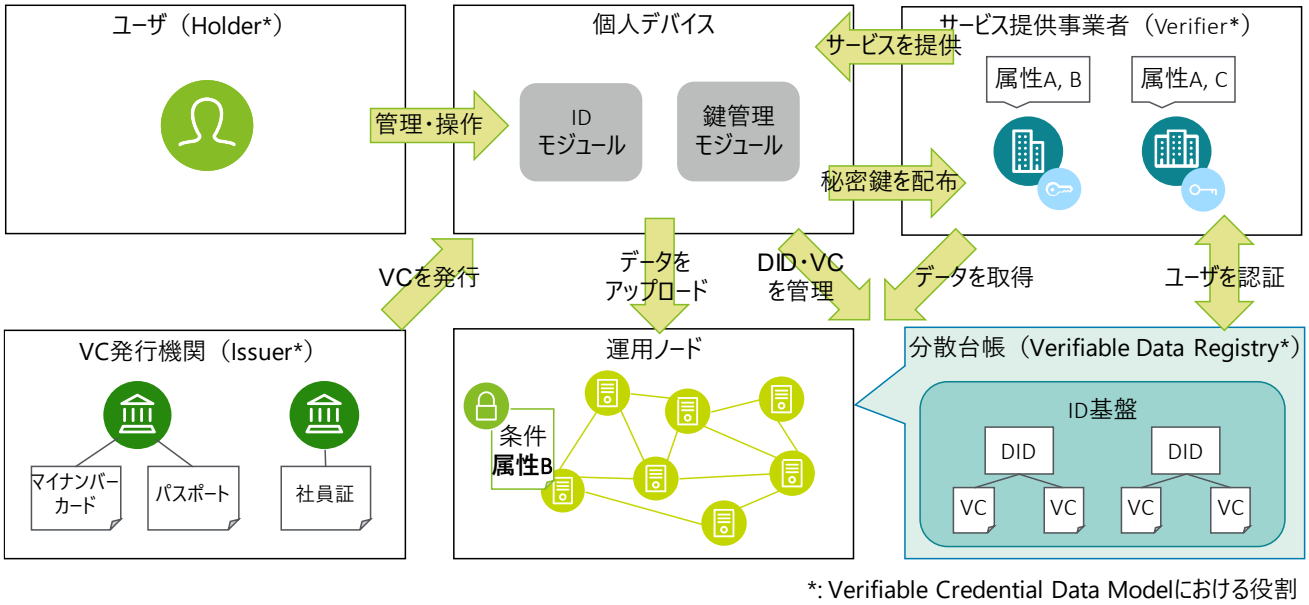

図 1 システムアーキテクチャの概要図

基づいてサービス提供事業者から認証を受ける機能を対象範囲とする．データ共有に関してはユーザからサービス提供事業者へデータを共有する機能を対象範囲とする．前提条件は以下の通りとする．

- エンティティ間の通信では処理に影響を与える遅延は発生せず，秘密鍵のやり取りには安全な経路を利用する．
- VC 発行機関は全てのエンティティから信頼されているものとする．
- ユーザ側から見たサービス提供事業者自身の信頼性及び属性の真正性は保証されているものとする

4.4 処理フロー

4.4.1 アイデンティティ管理

本稿ではユーザが DID を発行し，VC を関連付けた上で，サービス提供事業者がユーザの VC を検証して認証する機能を検討する．本機能の流れは図 2 の通り．本機能を構成する 2 つのフェーズを説明した上で，既存のアイデンティティ情報のライフサイクルとの関連性を述べる．

(1) 登録フェーズ

ユーザは自身を表す DID を発行し，分散台帳上に記録する．VC 発行機関はユーザの申請に基づいて VC を発行し，ユーザに提供する．VC には VC 発行機関自身の DID 及び発行相手であるユーザの DID 等の情報が含まれる．VC を受け取ったユーザは自身のデバイス内に VC の情報を保存する．

(2) 認証フェーズ

サービス提供事業者は事前に認証に必要な情報を提示しておく．ユーザが当該サービスを利用する際に，ユーザは個人デバイス内に保存されている VC の中から認証条件に合致する VC を 1 つ以上選択し，VP としてサービス提供事業者に提示する．サービス提供事業者はその情報を分散台帳上の記載に基づいて検証し，問題がなければサービスを提供する．

(3) ライフサイクル上における処理

既存のアイデンティティ管理ではアイデンティティ情報に関するライフサイクルを踏まえた処理の定義が必要となる[18]．具体的には「登録」「有効化」「更新」「休止」「抹消」の 5 処理を定義する必要がある．本稿では各処理の詳細については省略するが，登録フェーズ及び認証フェーズの処理で内包できると考えている．具体的には，「登録」「有効化」は登録フェーズの一連の処理で定義でき，「更新」は登録フェーズの VC 発行処理を再度繰り返すことと定義できる．「休止」「抹消」は認証フェーズにおいて情報を提示する際に「休止」もしくは「抹消」したい情報をユーザ自らが指定できるため，各処理を代替できると考える．

4.4.2 データ共有

本稿におけるデータ共有機能は，ユーザが運用ノードによる共有ストレージにデータを保存する「保存フェーズ」とサービス提供事業者が保存されたデータを取得する「共有フェーズ」から構成される．本機能の流れは図 3 の通り．

(1) 保存フェーズ

ユーザの個人デバイス上で属性ベース暗号の初期設定を行う．その後，復号条件を設定してデータを暗号化し，運用ノードへ送信する．運用ノードは送られたデータに対して，適切に保存されたことを証明するために署名を付与し，分散台帳上に記録する．運用ノードは保存したデータの電子署名や保存場所の情報等をユーザへと送信する．ユーザはそれらの情報を受け取り，正しいことを確認した上で，個人デバイス上に記録する．

(2) **共有フェーズ**

データを取得するサービス提供事業者はユーザに対して，秘密鍵の配布を要求する．ユーザは事業者の属性に基づいた秘密鍵を作成し，事業者に配布する．その後，共有データが必要になったとき，事業者はユーザにデータ提供を依頼し，ユーザは事業者にデータの場所を提示する．事業者が暗号化データを取得する際には，付属する電子署名の情報を分散台帳上で確認してデータの真正性を検証する．正しいデータであることを確認した上でデータを復号し，利用する．

5. 考察

5.1 提案アーキテクチャにおける利点

4 章で提案したシステムアーキテクチャを利用することで得られる利点をアイデンティティ管理とデータ共有の観点から考える．

5.1.1 アイデンティティ管理

(1) **アイデンティティの永続性**

ユーザの ID が特定のサービスに紐付いていないため，ユーザは自身の DID を半永続的に利用することができる．複数のサービスや VC と関連付けることができるため，利用サービスのサイロ化も防ぐことができ，ユーザのアイデンティティ情報の管理における利便性向上に寄与できる．

(2) **アイデンティティ情報のポータビリティの担保**

サービス提供事業者同士の合併やサービスの売却によって運営組織が変わる場合がある．そうした状況においてはユーザの ID やアイデンティティ情報を組織間で移行する必要がある．移行に伴うユーザの合意取得やシステム改修等には様々なコストや手続きが必要となる．本アーキテクチャにおいてはユーザのアイデンティティ情報はユーザ自身で保有・管理しているためサ，サービスの運営組織が変わったとしてもユーザのアイデンティティ情報の移行は不要である．

(3) **サービス提供事業者における管理負担の削減**

アイデンティティ情報には個人情報も多く含まれており，ID とパスワードも含めて厳格な管理が求められる．サービス提供事業者側でアイデンティティ情報を保有しない場合，それらの管理に伴う運用コストや負担が抑えられる．

5.1.2 データ共有

(1) **実データの永続性の担保**

分散ストレージ上にデータを保存した場合，データは単一のストレージに保存されるのではなく，複数のストレージにまたがって保存される．そのため，データの破損に耐性を持ち，半永続的にデータを保有することが可能となる．

(2) **データ単位のアクセス制御**

CP-ABE の特徴として，復号できる相手を予め決めておく必要がなく，複数の相手にデータを提供することができる．複数のサービス提供事業者が同一のデータを利用するような状況では，サービス提供事業者単位でのアクセス制御よりもデータ単位でのアクセス制御が望ましい．

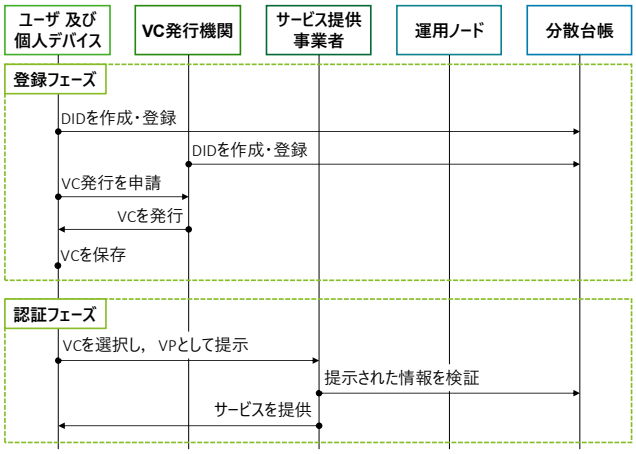

図 2 ユーザの認証に伴う処理フロー

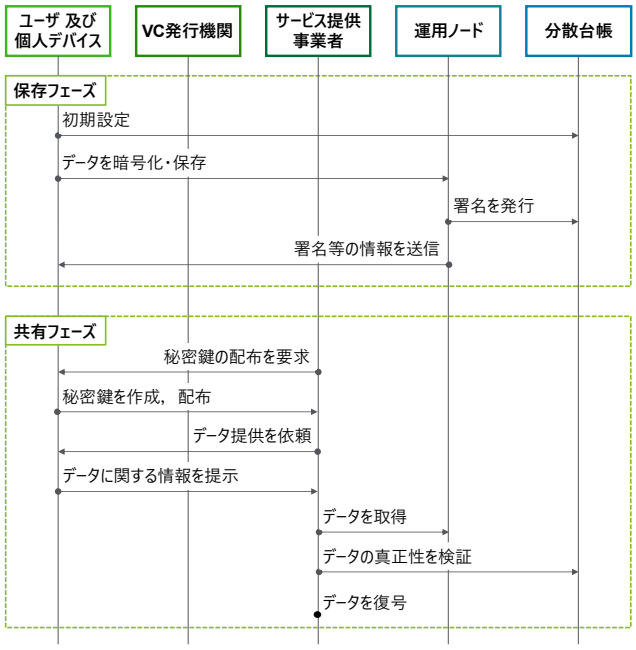

図 3 データ共有におけるフロー

(3) **プライバシー保護の対応コストの削減**

ユーザの利用データを取得する場合，様々なプライバシー保護規則を遵守する必要がある．取り扱うデータの種類によっては一定期間の保有や監査への報告が必要となる場合がある．本アーキテクチャでは実データはサービス提供事業者が保有していないため，それらの対応コストが削減できる可能性がある．

5.2 実装に向けた課題と検討事項

本アーキテクチャに関わる技術は未だ発展途上のものも多く，実世界への活用に向けた課題は少なくない．本節ではそれらの実装に向けた課題と検討事項について考察する．

(1) **分散台帳の設計・信頼性**

提案アーキテクチャにおいて，資格情報の保有やデータの真正性を証明するために分散台帳は重要な役割を果たす．

複数組織における分散台帳を実現するためにブロックチェーンの技術がある．ブロックチェーンは以下のような種類があり，それぞれ前提やメリット等が異なる．デメリットなりうる特徴もあるため，想定するユースケースや目的に照らして選択する必要がある．

パブリックチェーン

全てのユーザがトランザクションの閲覧及び承認が可能できるものが該当する．非中央集権性，透明性，耐改ざん性等の一般的なブロックチェーンのメリットを持っている．一方で，トランザクションの処理に時間がかかり，即時性を持たない欠点がある．また，管理組織が不在であるため，責任の所在が明確ではない．ブロックチェーンのシステム変更には大きな手間やコストがかかり，ハードフォークによるシステム改修ではチェーン自体が分離してしまうおそれがある．

プライベートチェーン

特定の組織が管理し，トランザクションの承認・管理を行うものが該当する．トランザクションの公開範囲は管理組織が選択できる．トランザクションの承認を早くすることができ，処理能力はパブリックチェーンよりも高い．データの公開範囲も選択できることから機密性は向上できる一方で，透明性は薄い．更に，トランザクションの承認は運営組織の処理ノードが担うため，不具合や攻撃等によって機能しなくなるとトランザクションの承認が行えなくなるため，可用性が低い課題も存在する．

コンソーシアムチェーン

複数の企業・団体がコンソーシアムを組み，加入者が利用するものが該当する．基本的な特徴はプライベートチェーンと類似しているが，複数組織が関わっているためトランザクションの管理・承認に相互監視が働き，不正が起きにくい状況を保てる．一方で，どのようなコンソーシアムを形成するか，インフラやシステムはどの組織が構築・管理するのか，といった当該タイプに固有の課題も存在する．

その他のタイプ

上記以外として，トランザクションの閲覧・作成はすべてのユーザが可能であるが，承認は許可されたノードしかできないタイプも存在する．トランザクションのデータは誰もが確認したいが，承認は信頼できる組織に行わせたいという目的に適しており，分散 ID 技術サービスの一つである Sovrin ID の開発・運用を行う Sovrin Foundation[19]は当該タイプのブロックチェーンに基づいて開発が行われている．

(2) **トラストアンカーの信頼性**

VC の証明は ID 基盤の真正性を保つための基礎要素である．したがって，VC を発行する VC 発行機関は本アーキテクチャにおけるトラストアンカーとして存在する．VC 発行機関に関する規約や定義は定まっていないため，現状は誰もが VC 発行機関を担うことができる．そのため，実世界における証明書とオンライン上の VC を紐付けることが検討されている．すなわち，現実世界で厳格に本人確認済みの書類の情報を VC として発行し，DID と関連付けることで唯一性を保証する．特にマイナンバーカードは電子証明書が埋め込まれていることから，活用が期待されている．

(3) **トラストアンカーへの攻撃**

既存の公開鍵基盤のトラストアンカーである認証局に対する攻撃は多岐にわたる．それらの攻撃は本アーキテクチャの VC 発行機関に対しても成立しうる．また，分散台帳上の記録から VC 発行機関の運営組織を特定され，特定組織を狙った攻撃のおそれもある．

(4) **運用ノード群の運用コスト負担**

運用ノードが構築する共有ストレージを利用する場合，サービス提供事業者はストレージの運用コストは担わなくてもよい一方で，運用ノードの構築や管理コストが課題となる．特に分散台帳上の全てのデータを保持するフルノードとして運用するためには，十分なストレージとメモリが求められる．専用のサーバ等が必要となるため，運用の敷居が高い．一方で，個人のモバイルデバイスに分散台帳の技術を適用した製品の開発も進められている．ビットコインのフルノードとして運用ができるスマートフォン[20]や独自の OS を備え，送受信する全データを分散台帳上で実行できるスマートフォン[21]が開発・販売されている．こうした端末が広く普及していくことで，負担の分散化に繋がっていくと考える．

(5) **既存技術との連携**

本アーキテクチャの目的として様々なサービスにおける ID 管理負担の削減やサービス提供事業者の運用コストの削減があり，そのために多くのユーザ及び事業者に利用される必要がある．幅広い利用のためには，既存の仕組みと連携して利用できることが不可欠である．現状の仕組みでもユーザ認証やデータ流通の標準や技術が乱立しており，統一されているとは言えない．実証実験等を通して，連携のメリットを評価する必要がある．

6. ユースケース

ユーザのメリットである，各サービスに対して統一した認証の仕組みが利用できることやアイデンティティ情報の構成要素を独自で決められることを検証するユースケースとして県をまたぐ引っ越しの例を考える．本ユースケースの概要は図 4 の通りである．

ユーザは事前に運転免許証を保有していることを証明するため，運転免許証番号等を VC として発行してもらい，自身の DID と関連付ける．ユーザはその VC から不動産会社に提示する VP を作成し，不動産会社と物件の契約を締結する（①）．不動産会社は個人との賃貸契約を結び，新しい住所等，契約書の一部の情報をユーザの DID と関連付けた VC として発行する（②）．既存の仕組みでは契約には対

面でのやり取りや厳格な本人確認が必要となるため，ユーザ及び不動産会社共に大きな負担となっていた．本アーキテクチャを利用することで，オンライン上で不動産契約が完結できる可能性がある．

次に，ユーザは居住中の自治体 A に対して転出届を提出する．提出時に，運転免許証番号の VC と不動産との契約書類の VC を VP として利用する（③：点線）．これにより，本人確認と新住所の証明を同時に行うことができる．同時に転出届を暗号化し，分散ストレージ上に保存する（③'）．自治体 A はユーザからの通知を検証した後，転出届を取得し（④），復号して内容を確認する（④'）．暗号化には「地方公共団体」といったサービス提供事業者の属性の他に日時も指定できる方式を利用することで，一定期間後は秘密鍵を持つユーザも含めた全ユーザが閲覧できないようにすることもできる．

転出届の内容を確認した自治体 A は転出証明書を発行し，②の処理と同様に，転出証明書の一部の情報をユーザの DID と関連付けた VC として発行する（⑤）．更にユーザから許可があった場合には，③で利用した VP を水道や電気等の公共サービス提供事業者に提供する（⑤'）．これにより水道や電気の停止をユーザに代わって申請することができる．ユーザのアイデンティティ情報を全て持たなくても，各書類が発行されていることは VP によって証明できるため，ユーザ本人以外でも本人確認ができることも本アーキテクチャにおける利点と考える．ユーザは運転免許証番号の VC と転出証明書の VC を VP として自治体 B に提示し（⑥：破線），自治体 B での本人確認を行う．自治体 B は⑤'と同様に，公共サービス提供事業者に対して，VP を利用し，ユーザに代わって水道や電気の開通申請ができる（⑦）．

本アーキテクチャに基づいた場合，ユーザは本人確認を統一した仕組みで利用でき，対象に合わせて提示するアイデンティティ情報を選択することができる．各自治体にとっても本人確認がオンライン上で完結し，他の組織とも柔軟に連携することができるようになると考える．

7. おわりに

本稿では，近年のデジタルアイデンティが抱える課題とデータ流通の懸念に着目し，ユーザが主体的にアイデンティティと共有データを管理するためのシステムアーキテクチャを検討，提案した．今後は本アーキテクチャの性能を評価するための実証実験に向けて，アプリケーションの開発及び実装を行う．

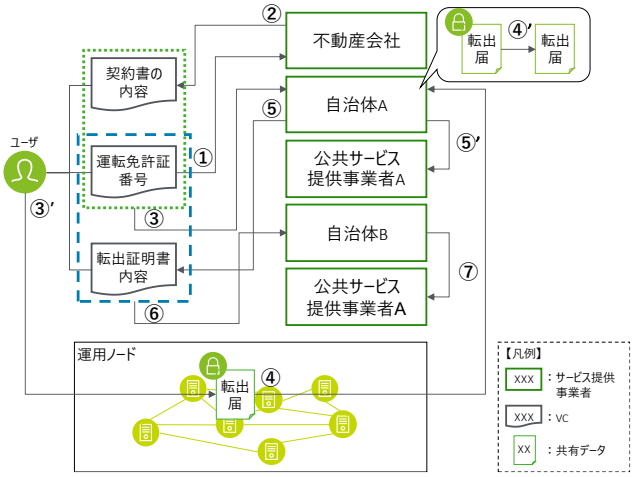

図 4 ユースケースの概要

参考文献

[1] M. Isaac and S. Frenkel, “Facebook Security Breach Exposes Accounts of 50 Million Users,” The New York Times, https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html (参照 2020-08-19).

[2] P. Bischoff, “Report:267 Million Phone Numbers & Facebook User IDs Exposed Online,” Comparitec, https://www.comparitech.com/blog/information-security/267-million-phone-numbers-exposed-online/ (参照 2020-08-19).

[3] “Google+ 閉鎖へ 50 万人の個人情報流出の恐れ，” 日本経済新聞, https://www.nikkei.com/article/DGXMZO36245390Z01C18A0MM0000/ (参照 2020-08-19).

[4] 内閣府, “Society 5.0,” https://www8.cao.go.jp/cstp/society5_0/.

[5] “第 5 期科学技術基本計画 本文,” 内閣府, https://www8.cao.go.jp/cstp/kihonkeikaku/5honbun.pdf (参照 2020-08-19).

[6] OECD, “OECD Privacy Guidelines,” 2013, 154p.

[7] ico.,“Intention to fine British Airways £183.39m under GDPR for data breach,” https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/ (参照 2020-08-14).

[8] 情報信託機能の認定スキームの在り方に関する検討会, “情報信託機能の認定に係る指針 ver1.0（案）,” https://www.soumu.go.jp/main_content/000550647.pdf (参照 2020-08-19).

[9] デジタル市場競争会議, “デジタル市場競争に係る中期展望レポート ～ Society 5.0 におけるデジタル市場のあり方～,” http://www.kantei.go.jp/jp/singi/digitalmarket/kyosokaigi/dai4/siryou3s.pdf （参照 2020-08-14).

[10] Decentralized Identifiers (DIDs) v1.0, https://www.w3.org/TR/did-core/.

[11] M.S. Ferdous, F. Chowdhury, and M. O. Alassafi, “In search of self-sovereign identity leveraging blockchain technology,” IEEE Access, vol. 7, 2019, pp. 103059-103079.

[12] C. Allen, “Self-sovereign identity principles,” Life With Alacrity, http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html (参照 2020-08-19).

[13] J. Benet, “IPFS-content addressed, versioned, P2P file system,” arXiv preprint arXiv:1407.3561, 2014.

[14] A. Shamir, “Identity-Based Cryptosystems and Signature Schemes,” in Proc. CRYPTO 84, LNCS, 1984, vol. 196, pp. 47-53.

[15] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Proc. Eurocrypt, 2005, pp. 457–473.

[16] V.Goyal, O.Pandey, A.Sahai, and B.Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proc. ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

[17] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attributebased encryption,” in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334.

[18] 独立行政法人 情報処理推進機構 技術本部 セキュリティセンター, “アイデンティティ管理技術解説 —ドラフト—,” https://www.ipa.go.jp/files/000014270.pdf, (参照 2020-08-19).

[19] Sovrin https://sovrin.org/

[20] EXODUS, “Cryptophone,” https://www.htcexodus.com/sg/cryptophone/ (参照 2020-08-19).

[21] Function X Foundation, “Blok On Blok (BOB) Innovation From Within,” https://functionx.io/#/bob (参照 2020-08-19).