メタバース利用者の匿名性と特定・追跡性の両立に関する考察
― 安心・安全なメタバースを目指して ―

才所 敏明 [1]　　櫻井 幸一 [2]　　辻井 重男 [3]

概要：メタバースは，サイバー空間に構築された，人々がデジタル的に交流し活動するサイバー社会であり，現在はゲームやエンターテインメントの分野を中心に活発に使用されているが，今後はビジネス，教育，医療等の分野での活用も期待されている．一方，フィジカル社会とメタバースの関係が密になるにつれ，メタバースのセキュリティリスクがフィジカル社会の安心・安全に直結するリスクとなることが想定される．メタバースを活用するサイバー・フィジカル社会の安心・安全を維持するには，十分なセキュリティ対策を施した安心・安全なメタバースの構築が重要となる．
本稿では，フィジカル社会の利用者（個人・法人）と紐づけられたメタバースのエンティティ間のコミュニケーション，エンティティ間の取引，フィジカル社会の利用者とその利用者に紐づけられたエンティティ間の資金移転，等の基本的なサービスを提供するメタバースを対象に，セキュリティ対策としての利用者のメタバースでの匿名性と特定・追跡性の両立を目指した，メタバースの構成・仕組み等を提案する．

Study on Coexistence of Anonymity and Identifiability/Traceability of Metaverse Users
― Aiming for a safe and secure Metaverse ―

Toshiaki Saisho [1]　Kouichi Sakurai [2]　Shigeo Tsujii[3]

1. はじめに

メタバースは，サイバー空間に構築された，人々がデジタル的に交流し活動する場であり，2003 年に最初のメタバース Second Life がリンデン・ラボによりリリースされた（[23]）．

その後の，仮想現実（VR）技術や VR 用機器の発展，SNS 等によるオンライン交流の普及等により，メタバースにおける交流が活発化し，2020 年代に入るとメタバースがビジネスやエンターテインメント等の分野での可能性が認識され，メタバースが一気に注目を集めることとなった．

現在，メタバースはゲームやエンターテインメントの分野を中心に使用され始めており，デジタルアートなどのデジタル資産を交換するためのマーケットプレイスが運用され，経済的な活動も展開され始めている．将来的にはビジネス，教育，医療，社会的交流などの分野でも利用されることが期待されている．

メタバースの応用は未だ発展初期段階であるが，各分野での具体的応用が進むにつれ，メタバース（サイバー社会）での活動と現実社会（フィジカル社会）の活動との連携も強くなるものと想定される．このようなメタバースのフィジカル社会との連携の緊密化は，メタバースにおけるセキュリティ課題がフィジカル社会にも様々の新たなセキュリティ課題を突き付けることが想定される．

本稿では，安心・安全なサイバー・フィジカル時代を目指して，メタバース利用者の匿名性と特定・追跡性の両立によるセキュリティリスクの回避・対応の可能性を検討する．具体的には，フィジカル社会の利用者と紐づけられたメタバースのエンティティ間のコミュニケーション，エンティティ間の取引，フィジカル社会の利用者とその利用者に紐づけられたメタバースのエンティティとの間の資金移転，等のサービスを提供するメタバースを対象とし，利用者のメタバースでの活動時の匿名性と特定・追跡性の両立の仕組みの組込等のセキュリティ機能を強化した，メタバースの構成を提案する．

2. メタバース概要

メタバースについては様々の定義があるが，本稿では，メタバースを

①ネット上（サイバー空間）に構築されたサイバー社会
②個人がメタバースに定義したエンティティを通じ，様々の生活・社会活動を展開でき，法人もメタバース

1 （株）IT 企画　http://advanced-it.co.jp/
（株）ZenmuTech　https://www.zenmutech.com/
mail: toshiaki.saisho@advanced-it.co.jp
2 九州大学大学院システム情報科学研究院
&サイバーセキュリティーセンター
（株）国際電気通信基盤技術研究所
mail: sakurai@inf.kyushu-u.ac.jp
3 中央大学研究開発機構
mail: tsujii@tamacc.chuo-u.ac.jp

に定義したエンティティを通じ様々の経済活動を展開できるサイバー社会

と定義している．

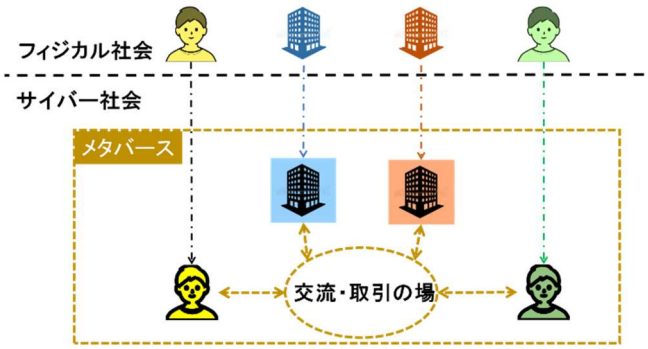


図１　個人・法人の様々の活動の場としてのメタバース

メタバースは技術，応用の両面で未だ発展途上であり，全体像は把握できないが，本稿では以下の三つの基本的なサービスを提供するメタバースを検討の対象としている．（以降，本稿では想定する検討対象メタバースを，単にメタバースと記載）．

①エンティティ間のコミュニケーション

エンティティはフィジカル社会の個人あるいは法人と紐づけされており，利用者（個人・法人）の制御の元，他のエンティティ（他の利用者）とのコミュニケーションが可能

②エンティティ間の取引

エンティティは，メタバース通貨（メタバース独自の暗号資産）の資金を保有でき，その資金を使用しメタバースに登録されているデジタル資産の取引が可能

③フィジカル社会とメタバース間の資金移転

フィジカル社会の利用者は，メタバースに登録したエンティティとの間で資金の移転が可能

3.　メタバースの実現方針（概要）

本章では，2 章で述べたメタバースの基本的なサービス提供に必要な以下の各機能の，想定する実現方針を記載する．

3.1　メタバースの利用登録機能・利用制御機能

フィジカル社会の利用者がメタバースで活動を行う場合，まずメタバースへ登録手続きを行い，対応するエンティティを定義，その識別コード，表示されるアバター，利用制御に使用される認証情報，等を登録する．また，実際の利用時には，識別コード，認証情報を提示し登録されているエンティティとの当人確認を受け，そのエンティティを通じメタバースの利用を開始することを想定している．

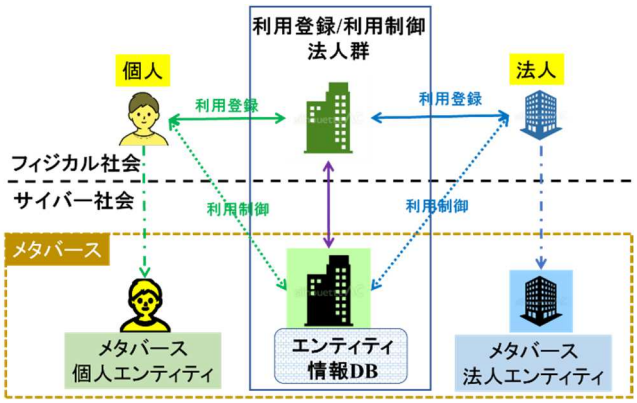


図２　想定する利用登録・利用制御（概要）

3.2　メタバースエンティティ間のコミュニケーション機能

エンティティ間のコミュニケーションは，SNS 等の専用のツールを利用し行う方法と，メタバースの市街地・景勝地等の散策サービスを利用し Face-to-Face のコミュニケーションを利用する方法を想定している．

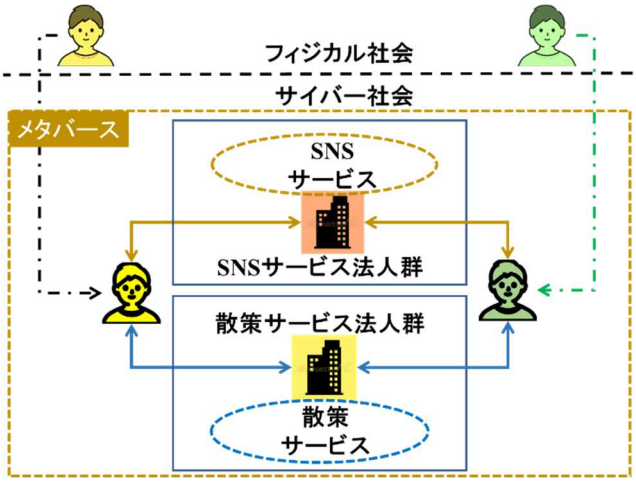


図３　想定するコミュニケーションサービス（概要）

3.3　メタバースエンティティ間のサービス機能・取引機能

メタバースではサービスの提供・利用やデジタル資産の取引等の活動を想定している．

サービスの提供・利用については，対価は暗号資産であるメタバース通貨での決済を想定している．

デジタル資産の取引については，メタバースで登録されているデジタル資産を対象とし，当該デジタル資産の所有権の移転，メタバース通貨による決済にて実施されることを想定している．

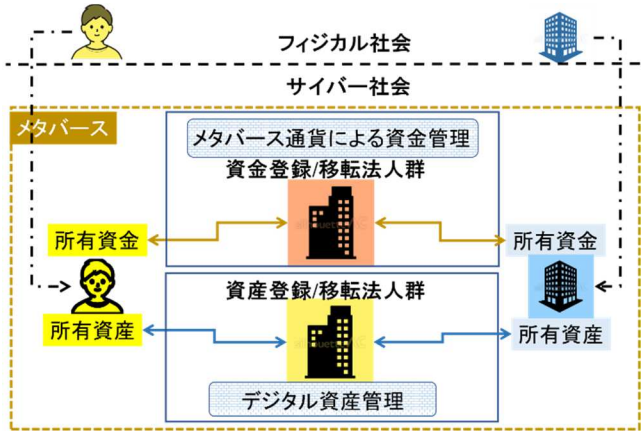


図４　想定するデジタル資産取引（概要）

3.4　メタバースとフィジカル社会の通貨交換機能

メタバースのエンティティの活動には資金が必要な場合も多く，対応する利用者がフィジカル社会の通貨により必要な資金を送金可能であることを想定，また，逆にエンティティのメタバース通貨による所有資金を対応する利用者へ送金可能であることを想定している．

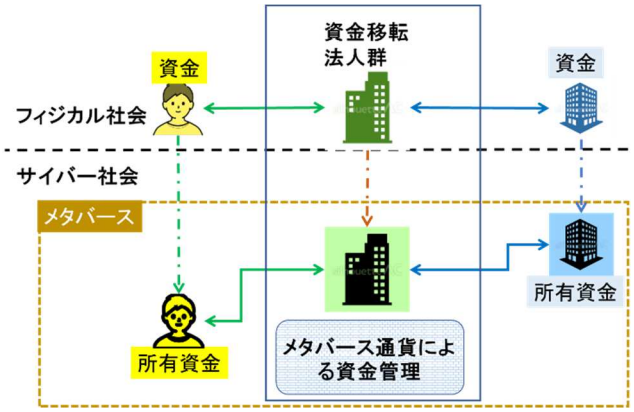


図５　フィジカル社会との資金移転（概要）

4.　安心・安全なメタバースの具体的構成提案

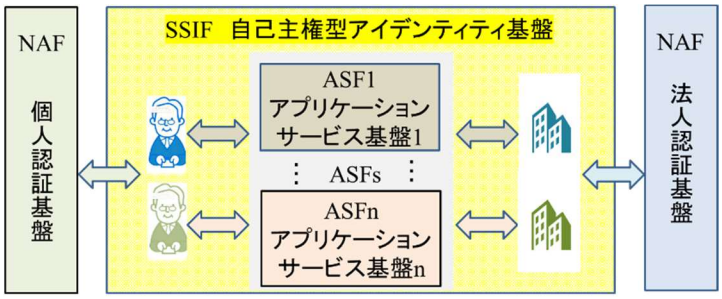
本章では，メタバース実現に必要な各機能について，フィジカル社会の利用者の，メタバース利用時の匿名性と特定・追跡性の両立を可能とする仕組みを内包する，具体的な仕組み・構成を提案する．

4.1　メタバースの利用登録機能・利用制御機能

フィジカル社会の利用者がメタバース利用開始時には，メタバースは利用者の身元確認を行い，登録時点で利用者の一定の信頼性の確認を行うことを想定している．

なお，筆者らはアプリケーションごとの直接の身元確認を不要とする，アプリケーションが身元確認済の利用者であることを確認できる仕組みを提供するブロックチェーンサービス基盤（BSI：Blockchain Service Infrastructure）の構築を提案している（図６，[1]）．

BSI では，構成要素である各国の認証基盤（NAF：National Authentication Framework）にて利用者の確実な身元確認が行われ，自己主権型アイデンティティ基盤（SSIF：Self-Sovereign Identity Information Framework）にて NAF により身元確認済の利用者であることを確認の上，標準化団体 W3C の勧告仕様に従った利用者識別コード SSIF-DID（Decentralized Identifier）が付与され，更に SSIF 上で利用するアプリケーション基盤（ASF：Application Service Framework）では，SSIF により身元確認済の利用者であることを確認の上，新たな利用者識別コード ASF-DID を付与し，利用者は ASF-DID を使用しアプリケーションサービス基盤で活動することを想定している．



NAF：National Authentication Framework
SSIF：Self-Sovereign Identity-information Framework
ASF：Application Service Framework
図６　ブロックチェーンサービス基盤（BSI）の構成

メタバースも，この BSI 上のアプリケーションサービス基盤の一つとして動作することを想定しており，メタバース利用者は，SSIF により身元確認済の利用者であることが前提である．

利用者のメタバース登録を担当する利用登録法人は，利用者が登録時に提示する SSIF-DID の所有者確認の上，またその他のメタバース登録条件を確認の上，利用登録法人は利用者の登録を承認し，以下のような手続きを行うことを想定している．

①メタバースでの利用者識別コード MV-DID および公開鍵暗号の鍵ペアの発行（鍵ペアは利用者発行も可能とする）

②MV-DID と身元確認に使用された SSIF-DID（SSIF で身元確認済）との対応情報の安全・確実な管理

③MV-DID，公開鍵および別途指定されたニックネーム，アバター等を，新たなエンティティとしてメタバースエンティティ VDR（Verifiable Data Registry）へ登録

④MV-DID および鍵ペアを利用者へ提供（鍵ペアを利用者が生成した場合は MV-DID のみ）

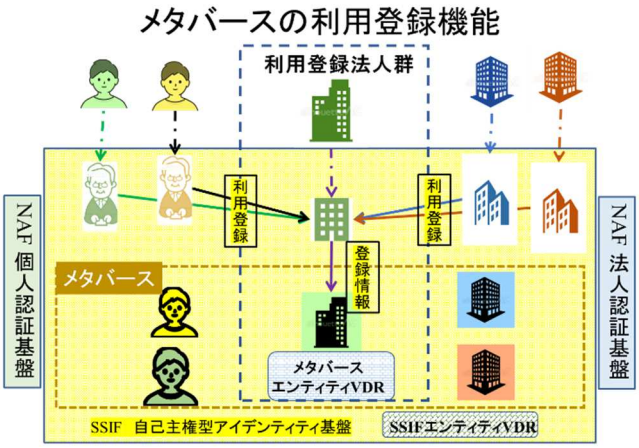


図７　BSI を使用したメタバース利用登録の仕組み・構成

利用者がメタバース利用時には，利用制御法人は利用者が提示した MV-DID および対応する秘密鍵による署名を，メタバースエンティティ VDR を利用し確認，利用者に対応するエンティティとの当人確認を行うことを想定している．

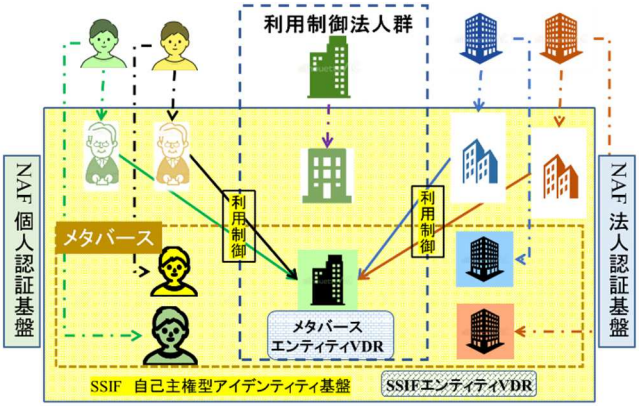


図８　BSI を利用したメタバース利用制御の仕組み・構成

BSI を利用したメタバースの利用登録/利用制御により，利用者の通常利用時の匿名性確保が可能となり，また，不正・不法や悪意のある活動が確認された場合は合法的手続きにより，利用登録法人が管理するメタバースが発行した MV-DID と SSIF で身元確認後に発行された SSIF-DID との対応情報の入手により，対応する利用者の特定・追跡が可能となる．

4.2　エンティティ間のコミュニケーション機能

利用者がコミュニケーションサービスを利用する場合は，メタバースのエンティティ経由，サービス事業者へ利用登録を行うことを想定している．コミュニケーションサービス（SNS サービス/散策サービス）事業者は，利用者が身元確認済の利用者かどうか，メタバース利用者かどうかを MV-DID の所有者確認により行うことを想定している．利用者として登録する場合は，新たな利用者識別コード SW-DID 等が付与される．なお，アバター，ニックネームも新たに定義可能だが，メタバース登録時に選択したアバター，ニックネームをそのまま使用可能とすることも想定している．また，不正・不法や悪意のある活動が確認された場合は合法的手続きにより，コミュニケーションサービス事業者が発行した SW-DID とメタバースが発行した MV-DID との対応情報の入手により，対応する利用者の特定・追跡が可能となる．

なお，具体的なコミュニケーションで使用するニックネームやアバターはユニークである保証はなく，コミュニケーションをとる際の相手のエンティティを正確に把握できるわけではなく，フィジカル社会のコミュニケーションと同等のリスクの存在を想定している．もちろん，必要があれば SW-DID および対応する秘密鍵による署名の交換により，公開されている SNS/散策エンティティ VDR から，相手のエンティティを把握できる仕組みも想定している．

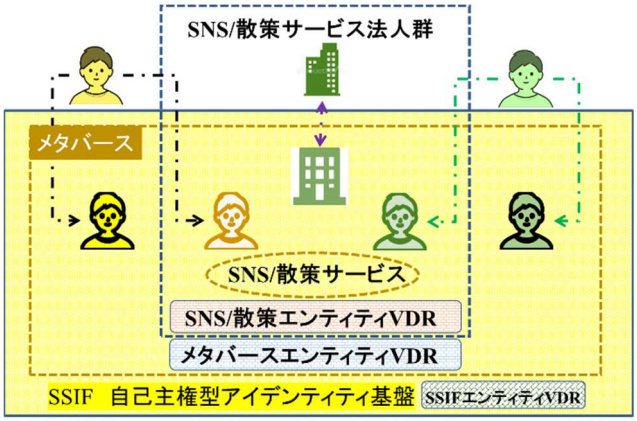


図９　コミュニケーションサービスの仕組み・構成

4.3　エンティティ間の取引（決済）機能

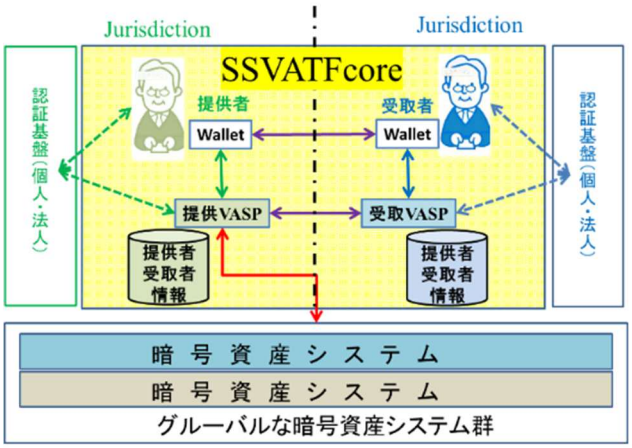
メタバースでは，メタバース固有の暗号資産システムにてエンティティの保有資金の管理を想定している．資金は暗号資産システムのアドレスと対応付けられブロックチェーンに記録され，その資金の保有者であるエンティティに対応する利用者はアドレスに対応する秘密鍵を暗号資産ワレットにて安全に管理すること，取引の決済にあたっては，アドレスに対応する秘密鍵の保有を示すことにより，そのアドレスに対応する資金の使用が可能となることを想定している．

エンティティが資金を受け取る際に指定するアドレスは都度異なるアドレスを使用することを想定している．同じアドレスを繰り返し使用することは，ブロックチェーンで公開される資金の移動情報からアドレスに対応するエンティティが推定されるリスクが増大するためである．決済時の資金移転では，ワンタイムアドレスの使用により資金を保有するエンティティや対応する利用者の匿名性の確保を想定している．

一方，資金移転や資金保有に使用されるアドレスの強い匿名性は，メタバースの不正・不法な決済への悪用リスク

が増大する．通常運用時は利用者の匿名性の確保が重要であるが，不正・不法な決済の調査・捜査の仕組みは必要である．ワンタイムアドレスとそのアドレスの保有者（資金を保有するエンティティ）の対応情報等を安全・確実に管理する仕組み，資金保有者のエンティティを特定し，更に対応する利用者を特定・追跡できる仕組みは不可欠である．

このような仕組みは既存の暗号資産システムでも重要で，筆者らは既存の暗号資産システムにおける利用者の匿名性と特定・追跡性の両立を実現する安心・安全な暗号資産移転基盤（SSVATF（Secure and Safe Virtual Asset Transfer Framework）を提案している（図１０，[2]）．



VASP：Virtual Asset Service Provider

図１０　安心・安全な暗号資産移転基盤（SSVATF）概要

メタバースにおける決済においても，通常運用時は資金の提供者も受取者も匿名性を確保でき，不正・不法な決済が疑われる場合は，合法的な手続きにより，利用者の特定・追跡が可能となる仕組み，SSVATF と同等の仕組みを想定している．

利用者がメタバース資金管理サービスへ登録する場合は，メタバースのエンティティ経由，サービス事業者へ利用登録を行うことを想定している．サービス事業者は，利用者が身元確認済の利用者かどうか，メタバース利用者かどうかを MV-DID の所有者確認により行うことを想定している．利用者として登録する場合は，新たな利用者識別コード FM-DID 等が付与される．不正・不法や悪意のある活動が確認された場合は合法的手続きにより，サービス事業者が発行した FM-DID とメタバースが発行した MV-DID との対応情報の入手により，対応する利用者の特定・追跡が可能となる．

利用者が暗号資産サービス事業者（VASP）へ登録する場合は，メタバース資金管理サービス事業者は利用者から FM-DID と対応する秘密鍵による署名の提供を受け，利用者が資金管理サービス利用者であることを確認の上，その VASP として新たな利用者識別コード VS-DID および公開鍵暗号の鍵ペア（鍵ペアは利用者発行も可能とする）を付与することを想定している．

利用者のエンティティが登録した VASP 経由で決済する場合，資金の提供や受取に指定するアドレスとその秘密鍵を保有するエンティティの VS-DID との対応情報を，提供エンティティ，受取エンティティそれぞれが利用登録済みの VASP で安全・確実に管理することを想定している．

また必要時には，調査・捜査当局の合法的手続きにより，VASP から調査・捜査対象のアドレスに対応する VS-DID を入手，更に VS-DID に対応する FM-DID を入手により，対応する利用者の特定・追跡が可能な仕組みを想定している．

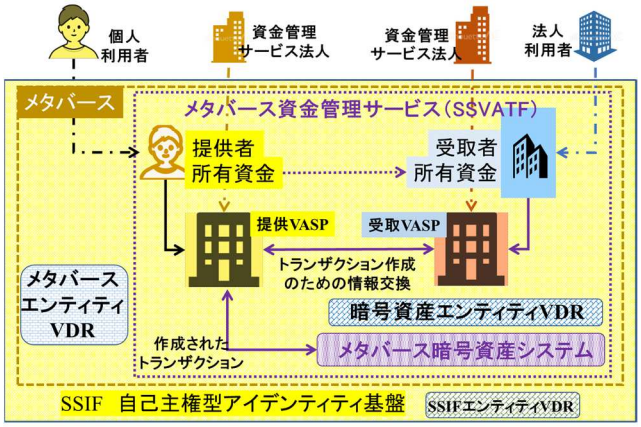


図１１　SSVATF を利用した資金移転の仕組み・構成

4.4　エンティティ間の取引（所有権移転）機能

メタバースにおけるデジタル資産の所有権移転においても，通常運用時はデジタル資産の提供者も受取者も匿名性を確保でき，不正・不法な決済が疑われる場合は，合法的な手続きにより，利用者の特定・追跡が可能となる仕組み，SSVATF と同等の仕組みを想定している．

利用者がメタバース資産管理サービスへ登録する場合は，メタバースのエンティティ経由，サービス事業者へ利用登録を行うことを想定している．サービス事業者は，利用者が身元確認済の利用者かどうか，メタバース利用者かどうかを MV-DID の所有者確認により行うことを想定している．利用者として登録する場合は，新たな利用者識別コード DM-DID 等が付与される．不正・不法や悪意のある活動が確認された場合は合法的手続きにより，サービス事業者が発行した DM-DID とメタバースが発行した MV-DID との対応情報の入手により，対応する利用者の特定・追跡が可能となる．

利用者がデジタル資産サービス事業者（DASP：Digital Asset Service Provider）へ登録する場合は，メタバース資産管理サービス事業者は利用者から DM-DID と対応する秘密鍵による署名の提供を受け，利用者がメタバース利用者であることを確認の上，DASP としての新たな利用者識別コード DS-DID および公開鍵暗号の鍵ペア（鍵ペアは利用者発行も可能とする）を付与することを想定している．また，DASP は，登録した利用者の DM-DID と DS-DID の対応情

報を安全・確実に管理することを想定している．

メタバースで取引の対象となる資産は，メタバース資産システムに登録されているデジタル資産を想定している．デジタル資産システムには，デジタル資産識別コード DA-DID，所有者識別コード DAH-DID（暗号資産システムのワンタイムアドレスに相当），デジタル資産の格納場所等が管理されており，デジタル資産の実体は，別途，安全・確実に保管されているものとする．

利用者のエンティティが登録した DASP 経由でデジタル資産の所有権移転を行う場合，移転対象のデジタル資産の DA-DID，デジタル資産の提供や受取に指定するワンタイムの DAH-DID，それを生成したエンティティの DS-DID との対応情報等を，提供エンティティ，受取エンティティそれぞれが利用登録済みの DASP で安全・確実に管理することを想定している．

以上の仕組み，エンティティ間のデジタル資産の所有権の移転は，関係する提供者および受取者の匿名性を維持しつつ，不正・不法な取引の場合は DASP の協力を得て，提供者および受取者の DM-DID と対応する DS-DID との対応を確認でき，更に対応する利用者を特定・追跡できる仕組みを想定している．

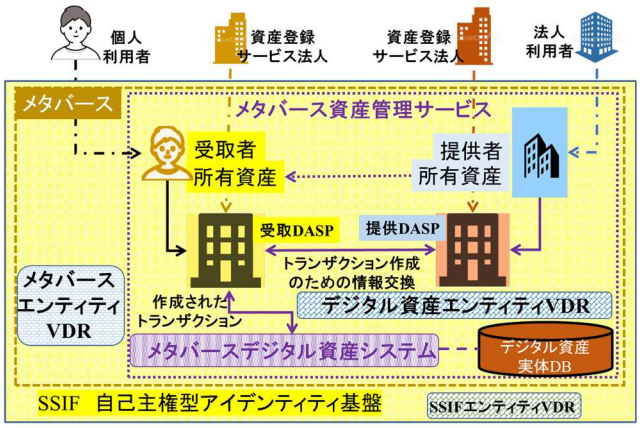


図１２　SSVATF を利用した資産移転の仕組み・構成

なお，デジタル資産の登録にあたっては，登録するエンティティに対応する利用者がデジタル資産の適切な権利を保有してことを前提としている．

4.5 メタバースとフィジカル社会の間の資金移転機能

フィジカル社会の利用者がメタバース上のサービス費用やデジタル資産の購入費用の支払い（決済）には，利用者に対応するエンティティのメタバース通貨を使用する．そのエンティティのメタバース資金を確保する等のため，利用者はフィジカル社会の資金（法定通貨）を資金移転サービス法人へ送金することにより，その法人に対応するメタバースのエンティティが VASP 経由，等価のメタバース資金を利用者と紐づけられたエンティティのメタバースの資金として暗号資産システムへ登録し，資金の移転が実施されるものとする．

逆に，エンティティが保有するメタバース資金は，利用者に対応するエンティティが通貨交換法人に対応するエンティティへメタバース資金を送金することにより，通貨交換法人から利用者へ法定通貨による等価の資金が移転され，資金の移転（交換）が実施されるものとする．

以上のようなフィジカル社会とメタバース間の資金移転においても，メタバース暗号資産システムの利用により，メタバースのエンティティや利用者の匿名性は維持されることを想定している．なお，フィジカル社会での資金移転は現状通り実名を想定しているが，メタバースでの資金移転との関連は公開されないため，メタバースのエンティティやそのエンティティに紐づけられている利用者の匿名性は維持されることを想定している．

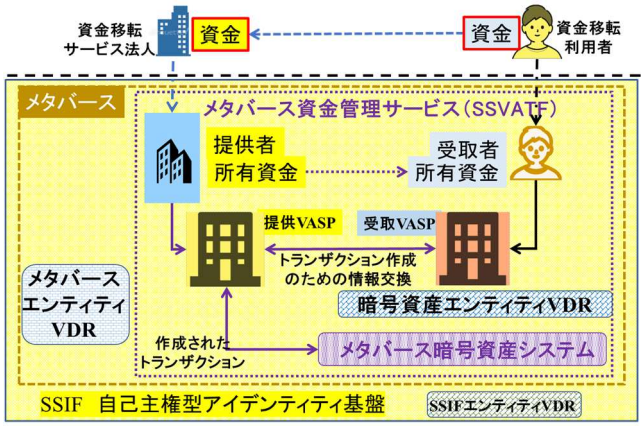


図１３　メタバースとフィジカル社会間の資金移転の仕組み・構成

なお，メタバース通貨と他の暗号資産との資金移転も，同様の仕組みでの実現を想定している．

5. おわりに

メタバースは，構成する要素技術もシステム技術も発展途上，応用分野も拡大中であるが，事故・事件の多発，不正・不法な利用や悪意のある利用の増大が，メタバース活用の大きな問題となることが想定される．

本稿では，基本的なサービスを提供するメタバースを対象に，メタバース利用者の安心・安全な活動，フィジカル社会の安心・安全を脅かすメタバース上での活動の防止・抑止に配慮した，メタバースシステムの仕組み・構成を提案した．

メタバース利用者の安心・安全な活動のための対策として，利用者の匿名性確保の仕組みを，フィジカル社会の安心・安全を脅かすメタバース上での活動の防止・抑止を目指すための対策として，利用者の特定・追跡性確保の仕組みを，組み込んだシステムを考案した．

具体的には，メタバースでの活動における利用者の匿名性と特定・追跡性の両立を確保する仕組みとして，別途提案中の，各国の認証基盤（NAF）を含むブロックチェーン

サービス基盤（BSI）の適用による実現を目指した（[1]）．また，メタバースにおける資金や資産の安全・確実な移転の仕組みや，その過程での利用者の匿名性と特定・追跡性の両立を確保する仕組みとしては，別途提案中の安心・安全な暗号資産移転基盤（SSVATF）をベースに考案した（[2]）．

今回は，構想レベルの実現方式の提案である．今後，詳細な仕様を定めつつ，実装の可能性，本方式の可能性と限界を見極める予定である．

メタバースの利用に関する法制度やガイドライン等の整備が急がれるが，その動向を把握しつつ，安心・安全なメタバースの実現の仕組みや構成に関する研究も活発に展開されることを期待したい．

参考文献

[1] 才所敏明, 辻井重雄. “ブロックチェーンサービス基盤に関する考察”. 2023 年 暗号と情報セキュリティシンポジューム（SCIS2023）. 2023.
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20230124SCIS2023BSIpaper.pdf

[2] 才所敏明, 辻井重雄, 櫻井幸一. “安心・安全な暗号資産取引基盤の提案ーSSVATF：Secure and Safe Virtual Asset Transfer Frameworkー”. 情報処理学会・コンピュータセキュリティシンポジューム 2022（CSS2022）. 2022.
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20221027CSS2022SSVATFPaper.pdf

[3] 才所敏明, 辻井重雄, 櫻井幸一. “トラベルルール（FATF 勧告 16）の現状・課題・考察ー暗号資産業界の健全な発展のために”. 情報処理学会・第 97 回コンピュータセキュリティ研究会（CSEC97）. 2022.
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20220519CSEC97TravelRulePaper.pdf

[4] 才所敏明, 辻井重雄, 櫻井幸一. “自己主権型アイデンティティ情報利活用基盤（SSIUF：Self-Sovereign Identity-information Utilization Framework）― 利用者の匿名性と特定・追跡性の両立―”. 情報処理学会・第 84 回全国大会. 2022.
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20220305IPSJ84SSIUFPaper.pdf

[5] 才所敏明, 辻井重雄, 櫻井幸一. “分散型 ID（DID）/検証可能属性証明（VC）技術を利用した自己主権型アイデンティティ情報利活用基盤（SSIUF）に関する考察”. 2022 年暗号と情報セキュリティシンポジューム（SCIS2022）. 2022.
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20220119SCISPaper.pdf

[6] 才所敏明, 辻井重雄, 櫻井幸一. “自己主権型アイデンティティ情報利活用基盤に関する考察”. 情報処理学会・コンピュータセキュリティシンポジューム. 2021.
http://advanced-it.co.jp/2016_wp/wp-content/pdf/20211028CSS2021Paper.pdf

[7] 才所敏明, 辻井重雄, 櫻井幸一. “自己主権型アイデンティティ情報管理システム（uPort,Sovrin）考察”. 電子情報通信学会ソサイエティ大会. 2021.
http://advanced-it.co.jp/2016_wp/wp-content/pdf/20210916IEICE_soc2021Paper.pdf

[8] 才所敏明, 辻井重雄, 櫻井幸一. “ビットコイン利用者の特定・追跡の仕組みに関する考察（２）“. 情報通信システムセキュリティ研究会（ICSS）. 2021.
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20210719CSECPaper.pdf

[9] 才所敏明, 辻井重雄, 櫻井幸一. “ビットコイン利用者の特定・追跡の仕組みに関する考察“. 電子情報通信学会総合大会. 2021.
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20210302ICSSPaper.pdf

[10] 才所敏明, 辻井重雄, 櫻井幸一. “自己主権型アイデンティティ情報管理システムに関する一考察“. 電子情報通信学会総合大会. 2021.
http://advanced-it.co.jp/2016_wp/wp-content/pdf/20210312IEICE_gen2021Paper.pdf

[11] 才所敏明, 辻井重男. “インターネット上のサービスにおける利用者の匿名性と特定・追跡性の両立”. 2021 年暗号と情報セキュリティシンポジューム（SCIS2021）. 2021.
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20210120SCIS2021Paper.pdf

[12] 才所敏明, 辻井重男, 櫻井幸一. “暗号資産の封印・償還における利用者の匿名性および特定・追跡性の考察”. 2021 年暗号と情報セキュリティシンポジューム（SCIS2021）, 2021.
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20210119SCIS2021Paper.pdf

[13] 才所敏明, 辻井重男. “インターネット時代の本人確認基盤に関する考察ー NAF から GAF へ ー“. コンピュータセキュリティシンポジューム. 2020.
http://advanced-it.co.jp/2016_wp/wp-content/pdf/20201026CSS2020Paper.pdf

[14] 才所敏明, 辻井重男, 櫻井幸一..” 暗号資産の匿名性要件の整理と対応レベルの比較”. コンピュータセキュリティシンポジューム 2020（CSS2020）. 2020.
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20201027CSS2020Paper.pdf

[15] 才所敏明, 辻井重男, 櫻井幸一..” 暗号資産台帳の匿名性と特定・追跡性についての考察”. 2020 年電子情報通信学会ソサイエティ大会. 2020.
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20200917IEICE-SocietyPaper.pdf

[16] 才所敏明, 辻井重男, 櫻井幸一.” DAG 技術ベースの暗号資産の匿名性に関する考察”. 2020 年暗号と情報セキュリティシンポジューム（SCIS2020). 2020.
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20200131_SCIS2020_paper.pdf

[17] 才所敏明, 辻井重男, 櫻井幸一..” 匿名暗号資産（Monero/Zcash/Grin）ブロックチェーンの匿名性に関する考察”. コンピュータセキュリティシンポジューム２０１９（CSS2019）. 2019.
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20191022CSS-MZG_paper.pdf

[18] 才所敏明.“NAFJA における本人確認方法に関する考察 ー National Authentication Framework in Japan ー”. コンピュータセキュリティシンポジューム. 2019.
http://advanced-it.co.jp/2016_wp/wp-content/pdf/20191021CSS-NAFJP_paper.pdf

[19] 才所敏明, 辻井重男.“日本における本人確認基盤（NAFJA）の考察 ー National Authentication Framework in Japan ー”. 情報処理学会・第 85 回コンピュータセキュリティ研究発表会. 2019.
http://advanced-it.co.jp/2016_wp/wp-content/pdf/20190524CSEC85_paper.pdf

[20] 才所敏明, 辻井重男.“暗号仮想通貨における匿名化技術の現状と展望”. 情報処理学会第 81 回全国大会. 2019.
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20190316IPSJ81_paper.pdf

[21] 才所敏明, 辻井重男.“仮想通貨の匿名性の現状と課題”. 2019 年暗号と情報セキュリティシンポジューム（SCIS2019）. 2019.
https://advanced-it.co.jp/2016_wp/wp-

content/pdf/20190125_SCIS2019_paper.pdf
[22] 宇根正志，“暗号資産における取引の追跡困難性と匿名性：研究動向と課題”，金融研究/2019.7.
http://www.imes.boj.or.jp/research/papers/japanese/kk38-3-4.pdf
[23] Second Life，https://secondlife.com/?lang=ja.
[24] “Digital Identity Guidelines - Enrollment and Identity Proofing”. NIST Special Publication 800-63A. 2017.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf
[25] “Digital Identity Guidelines - Authentication and Lifecycle Management”. NIST Special Publication 800-63B. 2017.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf
[26] Decentralized Identifiers (DIDs) v1.0 Core architecture, data model, and representations. World Wide Web Consortium. 2021.
https://www.w3.org/TR/did-core/
[27] Verifiable Credentials Data Model v1.1. World Wide Web Consortium. 2021.
https://www.w3.org/TR/vc-data-model/
[28] Verifiable Credentials Data Model v1.1. World Wide Web Consortium. 2021.
https://www.w3.org/TR/vc-data-model/
[29] FATF，“INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION（FATF Recommendations 2012（Updated October 2021））”，2021.
https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf
[30] FATF，“Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers”，2021.
https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf
[31] FATF，“Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers”，2019.
https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.htmll
[32] FATF，“SECOND 12-MONTH REVIEW OF THE REVISED FATF STANDARDS ON VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS”，2021.
https://www.fatf-gafi.org/media/fatf/documents/recommendations/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASP