メタバースにおける利用者の匿名性と特定・追跡性の実現方式の提案およびその安心・安全な社会維持効果についての考察

才所 敏明[1]　　辻井 重男[2]

概要：メタバースは，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メントの分野を中心に使用されているが，将来はビジネス，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（サイバー社会）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・安全を大きく左右することになる．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．

筆者らは，ネット上の様々のサービス・活動におけるセキュリティ維持には，利用者の匿名性と特定・追跡性の両立が重要であることを示し，ネット上の各種サービスにおける利用者の匿名性と特定・追跡性の両立の実現方式に関する研究を進めている．本稿では，複数のサービスから構成された一つのコミュニティであるメタバースにおける，利用者の匿名性と特定・追跡性の両立について考察する．

具体的には，利用者間のコミュニケーションや取引等の基本的な機能を提供するメタバースを対象に，利用者のメタバースでの匿名性と特定・追跡性の両立を実現するメタバースの構成・仕組みを提案する．更に，提案した利用者の匿名性と特定・追跡性の両立方式について，社会の安心・安全の維持に対する効果について考察する．

キーワード：メタバース，セキュリティ，サイバー・フィジカル社会，社会の安心・安全，利用者の匿名性，利用者の特定・追跡性，連結可能匿名化，ブロックチェーンサービス基盤，安心・安全な暗号資産取引基盤，分散型 ID

Proposal of a Method for Realizing User Anonymity and Identifiability/Trackability in the Metaverse, and Considerations on Its Effect on Maintaining a Safe and Secure Society

Toshiaki Saisho[1]　　Shigeo Tsujii[2]

Abstract: The Metaverse is a cyber society where people interact and act digitally. Currently, it is mainly used in the fields of games and entertainment, but it is expected to be used in fields such as business, education, and medicine in the future. On the other hand, as the relationship between the physical society and the Metaverse (cyber society) becomes closer, the security risks of the Metaverse will greatly affect the safety and security of the physical society. In order to maintain the safety and security of the cyber-physical society that utilizes the Metaverse, it is important to construct a safe and secure Metaverse with sufficient security measures.

The authors have been conducting research, arguing that it is important to achieve both anonymity and identifiability/trackability of users in order to maintain security in various services and activities on the Internet. In this paper, we consider achievement both anonymity and identifiability/trackability of users as one of the measures to maintain the security of the Metaverse.

Specifically, for the Metaverse that provides basic functions such as communication and transactions between users, we will propose the structure and mechanism of the Metaverse that achieves both anonymity and identifiability/trackability of users in the Metaverse. Furthermore, regarding the structure and mechanism of the proposed Metaverse, we consider on effects in maintaining a safe and secure society by achieving both user anonymity and identifiability/trackability.

Keywords: Metaverse, Security, User Anonymity, User Identifiability/Trackability, Linkable anonymization, Blockchain service Infrastructure, Secure and Safe Virtual Asset Transfer Framework, Decentralized Identifier

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により，メタバースの利用が活発化し，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メントの分野

1 （株）IT 企画　http://advanced-it.co.jp/
（株）ZenmuTech　https://www.zenmutech.com/
mail: toshiaki.saisho@advanced-it.co.jp

2 中央大学研究開発機構
mail: tsujii@tamacc.chuo-u.ac.jp.

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等も運用され，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．

筆者らは，ネット上の様々のサービス・活動におけるセキュリティ維持には，利用者の匿名性と特定・追跡性の両立が重要であることを示し，ネット上の各種サービスにおける利用者の匿名性と特定・追跡性の両立の実現方式に関する研究を進めている．

具体的には，利用者の匿名性のみを重視した多くの暗号資産システムの課題を克服すべく，暗号資産システム利用者の匿名性と特定・追跡性の両立を可能とする安心・安全な暗号資産取引基盤 SSVATF（Secure and Safe Virtual Asset Transfer Framework）([3]，[4])を提案中であり，またネット上の様々のサービスにおける利用者の匿名性と特定・追跡性の両立をサポートするブロックチェーンサービス基盤 BSI（Blockchain Service Infrastructure）([2]) を提案中である．

本稿は，提案中の BSI および SSVATF 両構想をベースに，メタバース利用者の匿名性と特定・追跡性の両立による安心・安全なメタバースの構成や仕組みについて考察した“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―”([1]) の第 2 稿である．本稿では，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を組み込んだメタバース構成を提案する．更に，提案したメタバース構成について，利用者の匿名性と特定・追跡性の両立が，社会の安心・安全の維持に対する効果について考察する．

2. 検討対象メタバース

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エンティティ間の交流

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）との交流（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

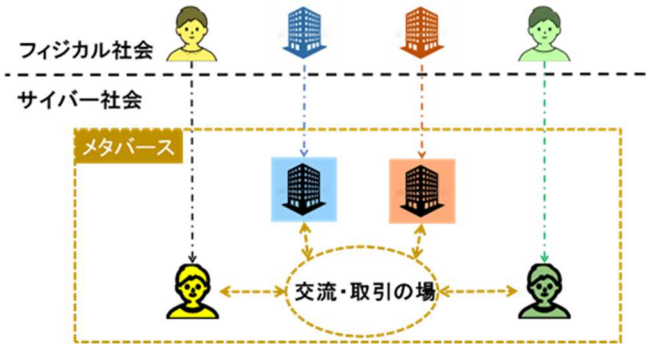


図１　個人・法人の様々な活動の場としてのメタバース

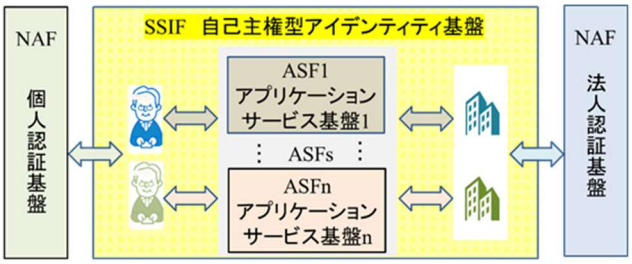
3. メタバースの具体的構成・仕組みの提案

本章では，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組み込んだ，検討対象メタバースにおける各機能の実現方式，構成案を示す．

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 を提案している（図２）．BSI では，構成要素である各国の認証基盤 NAF（National Authentication Framework）([13]，[18]，[19]）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）([2]，[5]～[7]）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（[26]）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サービス基盤 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，それぞれのアプリケーションサービスごとに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２　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，利用登録法人は利用者の登録を承認後には，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（ASF-DID のメタバース版）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）

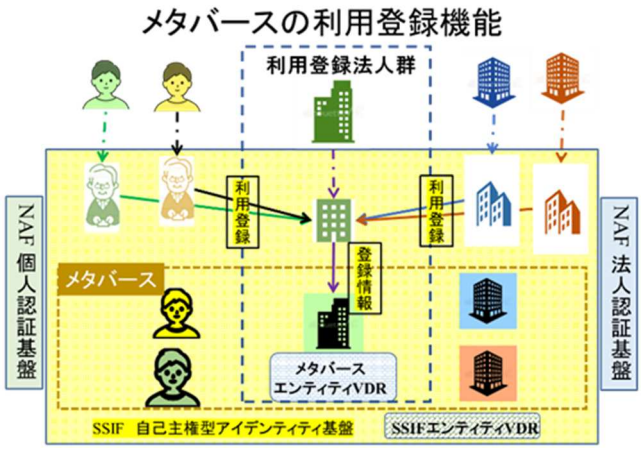


図３　BSI を使用したメタバース利用登録

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．

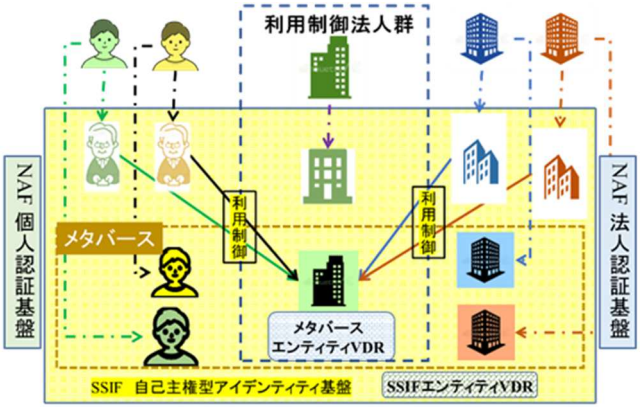


図４　BSI を利用したメタバース利用制御

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を確保しており，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・追跡性を確保している．

3.2　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，メタバース上のエンティティ経由，サービス事業者へ利用登録申請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，利用者はコミュニケーションサービス内ではその SW-DID を使用し活動することを想定しているが，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，サービス事業者が管理する 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・追跡性を確保している．

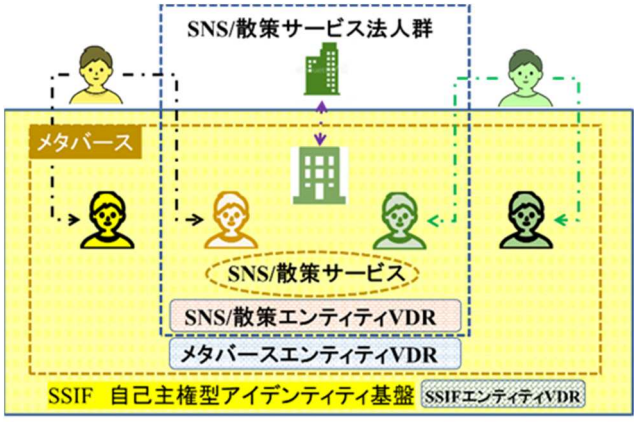


図５　コミュニケーションサービスの仕組み・構成

3.3　エンティティ間の取引機能

検討対象メタバースでの取引機能は，取引に伴う決済機能および取引結果としてのデジタル資産の所有権移転機能

から構成されることを想定している．なお，所有権の移転をともなわない様々の有償のサービス機能においても，決済機能が利用されることを想定している．

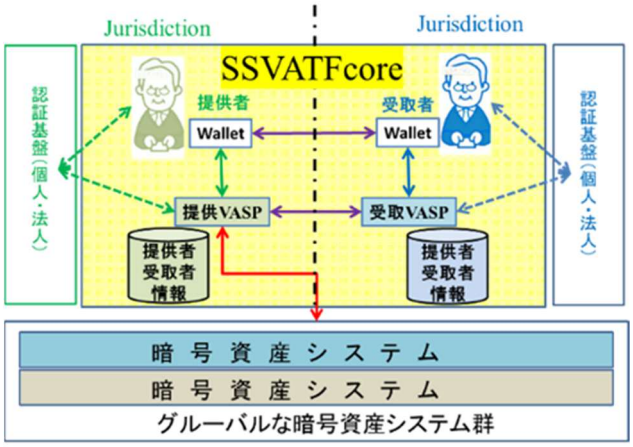
3.3.1 エンティティ間の決済機能

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．

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ワンタイムアドレスを使用することによる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・捜査のための利用者の特定・追跡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・安全な暗号資産取引基盤 SSVATF を提案している（図６）．



VASP：Virtual Asset Service Provider

図６　安心・安全な暗号資産取引基盤 SSVATF の概要

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，メタバース上のエンティティ経由，サービス事業者へ利用登録申請を行うことを想定している．サービス事業者は，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 等が付与されるが，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，サービス事業者が管理する 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・追跡性を確保している．

更に，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，更に暗号資産サービス事業者（VASP）が管理する対応情報から VS-DID に対応する FM-DID の入手により，対応する利用者の特定・追跡性を確保している．

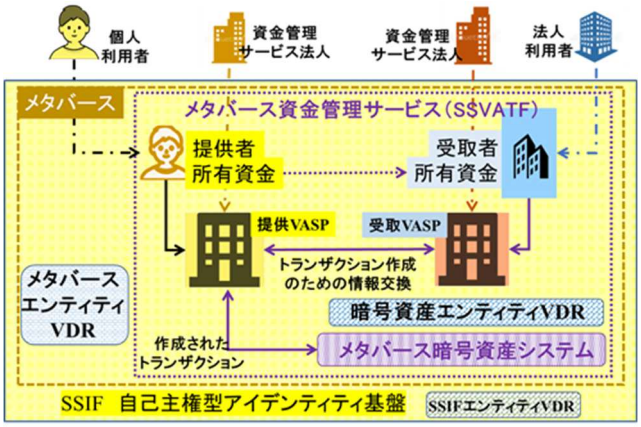


図７　SSVATF を利用した資金移転の仕組み・構成

3.3.2 エンティティ間の所有権移転機能

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・不法な取引が疑われる場合は，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申請を行うことを想定している．サービス事業者が利用者として登録する場合は，利用者には新たな利用者識別コード DM-DID 等が付与されるが，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，サービス事業者が管理する 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・追跡性を確保している．

更に，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，利用者が資産管理サービ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・不法な移転の場合は 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．

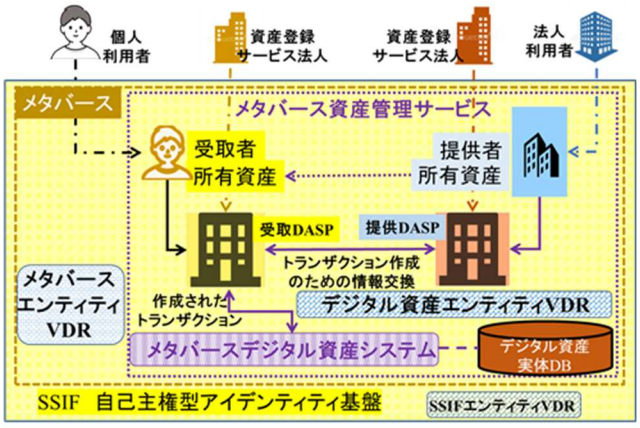


図８　SSVATF を利用した資産移転の仕組み・構成

3.4 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フィジカル社会の資金移転サービスを利用し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ける，メタバース上での資金移転は 3.3.1 にて述べた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，また必要な場合の対応する利用者の特定・追跡が可能である．

フィジカル社会での資金移転においては，安心・安全な暗号資産取引基盤 SSVATF を利用した暗号資産による資金移転の場合は，利用者の匿名性の維持および特定・追跡が可能である．なお，フィジカル社会の資金移転において従来の法定通貨による資金移転サービスを利用する場合も，実名による資金移転とはなるが，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．

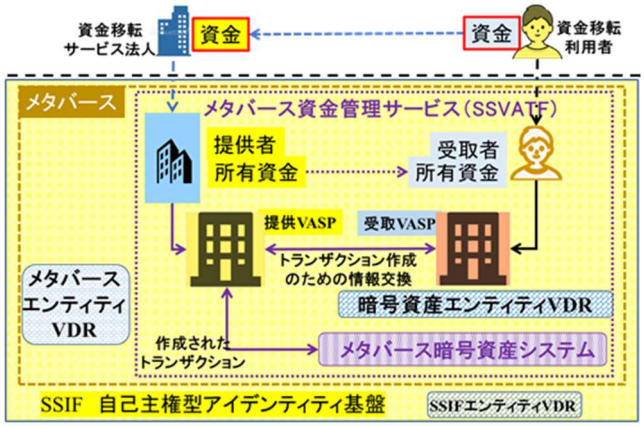


図９　メタバースとフィジカル社会間の
資金移転の仕組み・構成

4. 利用者の匿名性と特定・追跡性の両立による社会の安心・安全維持効果

本章では，社会の安心・安全を維持するための施策として導入した，メタバースにおける利用者の匿名性と特定・追跡性の両立の効果を考察する．

図１０に，連結可能匿名化による匿名性と特定・追跡性の両立の仕組み，を示している．

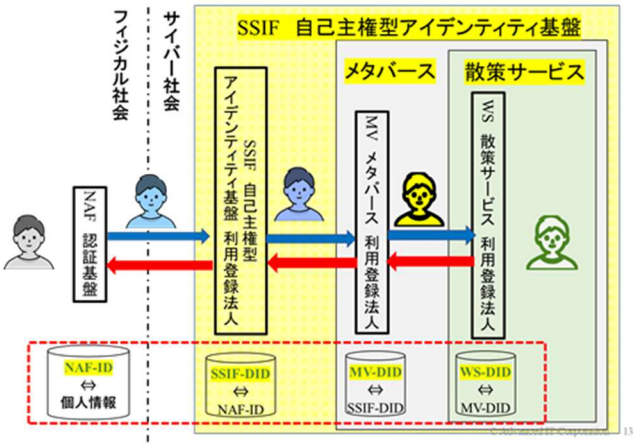


図１０　散策サービス（例）における
利用者の匿名性と特定・追跡性の両立の仕組み

利用者の匿名性は，新たなサービスへ登録の都度，新たな利用者識別コードを付与する方式（図１０の青矢印）により確保しており，利用者の特定・追跡性は各サービスの利用者登録法人が管理する新旧の利用者識別コード対応表を利用し連結をさかのぼること（図１０の赤矢印）により確保している．なお，本方式による利用者の匿名性と特定・追跡性の両立の確実な実現には，認証基盤 NAF による利用者の身元確認の確実さ，および各サービスの利用登録法人の新旧の利用者識別コード対応表の安全・確実な管理が重要となる．

以下，メタバースの各機能における利用者の匿名性と特定・追跡性の両立による社会の安心・安全維持効果を表にまとめている．

表１　メタバース利用登録・利用制御における効果

	想定リスク	リスク対応機能	対応効果
利用登録	利用者のリスク ＊なりすまし利用登録 事業者のリスク ＊不正・不法・悪意 利用者の登録	＊利用者の各国の 認証基盤NAFによる 確実な身元確認の利用 ＊認証基盤のID/ SSIFの DID/ メタバースのDIDの 対応の安全・確実な管理	＊なりすまし利用登録は排除可能 ＊不正・不法・悪意利用者の登録には 一定の抑止効果
利用制御	利用者のリスク ＊なりすましアクセス ＊事業者の 不正なアクセス	＊利用者のDIDおよび 利用者の管理している 秘密鍵による署名の検証	＊なりすましアクセスは排除可能 ＊事業者の不正なアクセスも排除可能 ＜秘密鍵生成・管理を利用者が行う場合＞

表２　コミュニケーションにおける効果

	想定リスク	リスク対応機能	対応効果
ＳＮＳサービス	利用者のリスク ＊通信相手のなりすまし ＊通信情報の信頼性の無さ ＊通信情報の漏洩 ＊悪意のある通信情報 事業者のリスク ＊不正・不法行為を 目的とした通信	＊事業者による 通信者のDID把握 ＊通信相手の DIDの確認機能 ＊通信内容の 暗号化機能（想定）	＊通信相手のなりすましは排除可能 ＊通信内容の信頼性の判断は自己責任 （フィジカル社会と同様） ＊通信内容は漏洩防止可能 （暗号化機能を利用する場合） ＊不正・不法・悪意の通信の 事業者による検知は困難
散策サービス	利用者のリスク ＊会話相手のなりすまし ＊会話の内容の信頼性の無さ ＊会話の内容の漏洩 ＊悪意のある会話の内容 事業者のリスク ＊不正・不法行為を 目的とした会話	＊会話相手の DID確認機能 ＊会話の 暗号化機能（想定） ＊会話の 録音機能（想定）	＊会話相手のなりすましは排除可能 ＊会話の内容の信頼性の判断は自己責任 （フィジカル社会と同様） ＊会話の内容は漏洩防止可能 （暗号化機能を利用する場合） ＊不正・不法・悪意の会話の 事業者による検知は困難

表３　取引（決済・所有権移転）における効果

想定リスク	提案方式	対応効果
利用者のリスク ＊決済相手のなりすまし ＊保有資金の盗難 （不正な出金） ＊不正資金の受取 （不正な入金）	＊決済相手のDID確認機能 ＊暗号資産システムによる 保有資金管理 ＊SSVATFを利用した 決済関係者の資金移転の承認 および特定・追跡の仕組み	＊決済相手の なりすましは排除可能 ＊保有資金の盗難は排除可能 ＊未承認の資金受取は排除可能
利用者のリスク ＊資産と資金の移転の 不整合	＊取引相手のDID確認機能 ＊決済相手と所有権移転相手の 同一性確認機能（別途検討予定）	＊取引相手のなりすまし排除可能 ＊取引相手の 取引不履行への対応可能 ＜取引相手間の通信機能および 決済相手と所有権移転相手の同 一性確認機能は別途検討予定＞
利用者のリスク ＊移転相手のなりすまし ＊保有資産の盗難 （不正な所有権喪失） ＊不正資産の受取 （不正な所有権付与）	＊移転相手のDID確認機能 ＊暗号資産と同様の 資産の移転・保有資産管理 ＊SSVATFと同等の仕組みにより 所有権移転関係者の移転の承認 および特定・追跡の仕組み	＊所有権移転相手の なりすましは排除可能 ＊保有資産の盗難は排除可能 ＊未承認の資産受取は排除可能

表４　フィジカル社会との資金移転における効果

	想定リスク	提案方式	対応効果
（メタバース）資金の移転	利用者・事業者のリスク ＊資金移転相手のなりすまし ＊保有資金の盗難 （不正な出金） ＊不正資金の受取 （不正な入金）	＊移転相手のDID確認機能 ＊暗号資産システムによる 資金移転・保有資金管理 ＊SSVATFを利用した 資金移転関係者の移転の承認 および特定・追跡の仕組み	＊資金移転相手の なりすましは排除可能 ＊保有資金の盗難は排除可能 ＊未承認の資金受取は排除可能
（同期）	利用者・事業者のリスク ＊両資金の移転の不整合	＊利用者・事業者のDID確認機能 ＊利用者・事業者の資金移転相手の 同一性確認機能（別途検討予定）	＊利用者・事業者の なりすまし排除可能 ＊利用者・事業者の 資金移転不履行への対応可能 ＜利用者・事業者の通信機能および 資金移転相手の同一性確認機能は 別途検討予定＞
（フィジカル社会）資金の移転	利用者・事業者のリスク ＊資金移転相手のなりすまし ＊保有資金の盗難 （不正な出金） ＊不正資金の受取 （不正な入金）	＜暗号資産利用＞ ＊移転相手のDID確認機能 ＊暗号資産システムによる 資金移転・保有資金管理 ＊SSVATFを利用した 資金移転関係者の移転の承認 および特定・追跡の仕組み ＜法定通貨利用＞ ＊銀行等の金融機関の移転機能	＜暗号資産利用＞ ＊資金移転相手の なりすましは排除可能 ＊保有資金の盗難は排除可能 ＊未承認の資金受取は排除可能 ＜法定通貨利用＞ ＊資金移転相手の なりすましは排除可能 ＊保有資金の盗難は排除可能 ＊未承認の資金受取は排除不可

今回の検討は，提案するメタバースの概要レベルの仕様ではあるが，利用者の匿名性と特定・追跡性の両立の仕組みによる社会の安心・安全維持に対し大きな効果が期待できる．

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提案した．

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，BSI で採用している多段の連結可能匿名化の利用により利用者の匿名性と特定・追跡性の両立の実現を目指した（[2]）．また，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，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を考案した（[3]）．

本稿ではまた，検討対象メタバースを対象に提案した利用者の匿名性と特定・追跡性の両立方式の，社会の安心・安全の維持効果を，メタバースの利用登録・利用制御機能および三つの基本的なサービスごとに，考察した．利用者の匿名性と特定・追跡性の両立の社会の安心・安全維持に対する主たる効果は，安心・安全を脅かす不正・不法あるいは悪意のある活動を検知した場合に，活動に関連する利用者をすみやかに特定・追跡の上，調査・捜査でき，不正・不法あるいは悪意のある活動の再発を防ぐ対応が可能なことである．また，このような特定・追跡性の仕組みは不正・不法あるいは悪意のある活動を未然に防ぐことは難しいが，不正・不法あるいは悪意のある活動を利用者に思いとどまらせる抑止効果は大きいと考えられる．

メタバースを始めネット上のサービス利用者には，第三者の目を気にすることなくネット上で自由な活動を保証するのが望ましいが，自由な活動といえどもその活動が社会の安心・安全を脅かすような不正・不法あるいは悪意のある無責任な活動は許されず，責任ある活動を求める必要がある．また，ネット上の様々のサービスを提供する事業者には自由なサービスビジネスの企画・展開を保証することが望ましいが，そのサービスが社会の安心・安全を脅かすことが無いよう，不正・不法あるいは悪意のある無責任な活動の抑止・防止の仕組みの組込みを求める必要があろう．

利用者の匿名性と特定・追跡性の両立の仕組みは，サイバー社会における利用者の自由なサービス利用，事業者の自由なサービスビジネス展開と共に，利用者・事業者の社会の安心・安全維持に対する責任を果たしうる具体的な方法と考えている．

参考文献

[1] 才所敏明, 櫻井幸一, 辻井重男．“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―”. 情報処理学会・DICOMO202 シンポジューム. 2023.
http://advanced-it.co.jp/2016_wp/wp-content/pdf/2023DICOMO2023MVpaper.pdf

[2] 才所敏明, 辻井重男．“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

[3] 才所敏明, 辻井重男, 櫻井幸一．“安心・安全な暗号資産取引基盤の提案－SSVATF：Secure and Safe Virtual Asset Transfer Framework－”．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

[4] 才所敏明, 辻井重男, 櫻井幸一．“トラベルルール（FATF 勧告 16）の現状・課題・考察－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

[5] 才所敏明, 辻井重男, 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

[6] 才所敏明, 辻井重男, 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

[7] 才所敏明, 辻井重男, 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

[8] 才所敏明, 辻井重男, 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

[9] 才所敏明, 辻井重男, 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

[10] 才所敏明, 辻井重男, 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

[11] 才所敏明, 辻井重男, 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

[12] 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

[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－ NAF から GAF へ －“. 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 － National Authentication Framework in Japan －”．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 － National Authentication Framework in Japan －”．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] 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
[29] 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
[30] 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
[31] 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