安心・安全なブロックチェーンサービス基盤（SSBSI）
Secure and Safe Blockchain Service Infrastructure

才所敏明*[1]
Toshiaki Saisho

あらまし　インターネット上のサイバー社会の発展は目覚ましく，インターネットは各国の重要な社会基盤となっている．一方で，セキュリティ上の課題への対応の遅れから，さまざまの不正・不法な利用や，悪意のある・無責任な行為や発言が氾濫している．本稿では，インターネット上の現在のサイバー社会の二つの課題，問題ある行為者や発言者の特定を困難としている利用者の強い匿名性，個人情報漏洩事件の多発の主因であるサービス事業者への個人情報・プライバシー情報の集積，の克服を目指した，安心・安全なサイバー社会の基盤を目指したブロックチェーンサービス基盤 SSBSI 構想を提案する．SSBSI は，利用者の確実な本人確認および匿名性と特定性の両立の仕組み，個人情報・プライバシー情報の利用者自身による利用制御が可能な仕組み，を組み込んだブロックチェーンサービス基盤構想である．一方，EU では EBP（European Blockchain Partnership）を設立，EU 全体で信頼できる公共サービス向けのブロックチェーンサービス基盤 EBSI（European Blockchain Services Infrastructure）の構築を進めており，現時点で一部のサービスの運用が始まっている．本稿では，EBSI の関連仕様を整理し，SSBSI と類似点・相違点等についても考察する．

キーワード サイバー社会，セキュリティ課題，利用者の匿名性，利用者の特定性，個人情報の集積，匿名性と特定性の両立，本人確認基盤，NAF，自己主権型アイデンティティ基盤，SSIF，アプリケーション基盤，ASF，ブロックチェーンサービス基盤，BSI，SSBSI，W3C，自己主権型アイデンティティ，SSI，分散型 ID，DID，検証可能属性証明，VC，検証可能属性提示，VP，EU，EBSI，EBP，EUROPEUM-EDIC

Abstract　The development of the online cyber society has been remarkable, and the internet has become an essential social infrastructure for various countries. However, due to the slow response to security challenges, various fraudulent and illegal uses, as well as malicious and irresponsible actions and statements, have proliferated. This paper proposes the SSBSI blockchain service infrastructure, a platform aimed at creating a safe and secure cyber society, addressing two key challenges of the current online cyber society: the strong anonymity of users, which makes it difficult to identify problematic actors and speakers, and the accumulation of personal information and privacy data by service providers, a major cause of frequent personal information leaks. SSBSI is a blockchain service infrastructure concept that incorporates mechanisms for reliable user identification, coexistence of anonymity and identifiability, and user-controlled management of personal information and privacy data. On the other hand, the EU established the EBP (European Blockchain Partnership) and started developing the EBSI (European Blockchain Services Infrastructure) for reliable public services across the EU, with some services already operational. This paper summarizes the relevant specifications of EBSI and discusses its similarities and differences with SSBSI.

Keyword　Cyber society, security challenges, user anonymity, user identifiability, collection of personal information, balancing anonymity and identifiability, identity verification infrastructure, NAF, self-sovereign identity framework, SSIF, application framework, ASF, blockchain service infrastructure, BSI, SSBSI, W3C, self-sovereign identity, SSI, decentralized identifier, DID, verifiable credential, VC, verifiable presentation, VP, EU, EBSI, EBP, EUROPEUM-EDIC

[1] (株)IT 企画　Advanced IT Corporation
toshiaki.saisho@advanced-it.co.jp
https://advanced-it.co.jp/

1. はじめに

1961 年の米国ユタ州で発生したテロにより 3 ヶ所の電話中継基地が破壊され軍用回線も一時的に完全停止したことを契機に，新たな通信システムの研究に着手，米空軍のシンクタンクであるランド研究所がパケット通信を提唱，1969 年に米国防総省の ARPA（高等研究計画局）が ARPANET を構築，世界最初のパケット通信網が稼働した．

インターネットで採用されているプロトコル TCP/IP は，1974 年に Vinton Gray Cerf と Robert Elliot Kahn により発表された．ARPA から改称された米国防総省の DARPA は，大学等で幅広く利用されていた BSD 版 UNIX を ARPANET の開発プラットフォームに採用し，1983 年には TCP/IP の実装を含む 4.2BSD UNIX が開発され，その年に，ARPANET のプロトコルが NCP から TCP/IP へ移行され，更に ARPANET から軍事部門が切り離され，ARPANET が大学間を結ぶインターネット（TCP/IP ネットワーク）となった．

以上の経緯で誕生したインターネット，1984 年に日本に上陸，更に 1991 年には米国でインターネットの商用利用が可能となり，日本でも 1992 年にはインターネット接続サービスを提供する ISP が営業を開始した．その後，日本でのインターネット利用は急拡大し，2002 年にはインターネット人口普及率が 50%を超え，インターネットが日本の重要な社会基盤の一つとなった．その後も利用は拡大し続け，2023 年にはインターネット人口普及率は 85.6%に達している．

一方，現在はインターネットの不正・不法な利用や，悪意のある/無責任な発言や行為が氾濫している．その原因は，インターネットの生い立ちからくる利用者の強い匿名性にある．2002 年には日本の社会基盤の一つとなりつつも，社会の安心・安全の維持に必要な対策，匿名性の強い利用者に対しての特定性を確保できる仕組みが実装されてこなかった．

もう一つは，インターネット上での個人情報の漏洩・悪用の事故･事件の多発である．1991 年に CERN の Tim Berners-Lee が開発した WWW を利用した，サービス利用者の個人情報を集積する現在の Web サービスの爆発的普及にある．個人情報のサービス事業者への集積を抑止する仕組み，個人情報の自己利用制御性を高める仕組みが必要であるが，未だ研究開発フェーズである．

本稿で提案する安心・安全なブロックチェーンサービス基盤（SSBSI）構想は，インターネット上のサイバー社会の二つの大きな課題，利用者の強い匿名性の課題を克服する利用者の確実な本人確認および匿名性と特定性の両立の仕組み，サービス事業者への個人情報・プライバシー情報の集積の課題を克服する利用者による個人情報・プライバシー情報の利用制御が可能な仕組みの実現による，安心・安全なサイバー社会の基盤となることを目指したブロックチェーンサービス基盤である．本稿では，まず提案する SSBSI 構想を報告し，その日本版としての SSBSIjp の構成例を示す．

次に，EU で構築が進められ，一部のサービスについては運用が始まっている EBSI ，EU 全体で信頼できる公共サービス向けのブロックチェーン基盤 EBSI について，サイバー社会の大きなセキュリティ課題への対応策，利用者の強い匿名性の課題を克服する確実な本人確認および匿名性と特定性の両立の仕組み，サービス事業者への個人情報の集積の課題を克服する利用者による個人情報・プライバシー情報の利用制御が可能な仕組みを整理し，本稿で提案する SSBSI 構想との類似点・相違点等を考察する．

2. SSBSI

筆者は，2016 年より日本における本人確認基盤の研究に着手し，2019 年に構想概要を発表([9],[10])，2020 年には本人確認基盤のグローバル連携方式等を発表([8])した．この本人確認基盤の研究成果が，SSBSI の構成要素 NAF（National Authentication Framework）の原型となっている．

また 2020 年より，利用者の匿名性と特定・追跡性の両立に関する研究開発および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研究開発に着手，2021 年に第 1 報を発表([7])し，2022 年にはそれらの成果を発展させ自己主権型アイデンティティ情報利活用基盤（SSIUF）を発表([3],[4])した．この SSIUF が，SSBSI の構成要素 SSIF（Self-Sovereign Identity Framework）の原型となっている．

その後，SSIUF 上での様々のアプリケーションの実装可能性の検証を続け，2023 年にブロックチェーンサービス基盤（BSI）構想の第 1 報([2])を発表した．今回報告する SSBSI は，その BSI 構想をさらに発展させた構想である．

SSBSI は，各国の，確実な個人の身元確認/法人の実在確認により識別コード（個人 ID/法人 ID）と鍵ペア等を発行する認証基盤（NAF），サイバー社会で活動する個人や法人に紐づけられたサイバーエンティティの DID/VC ベースの活動を可能とする自己主権型アイデンティティ基盤（SSIF），および SSIF 上で DID/VC ベースの様々のサービスを提供するアプリケーションサービス基盤（ASF : Application Service Framework），により構成されることを想定している（図 1）．

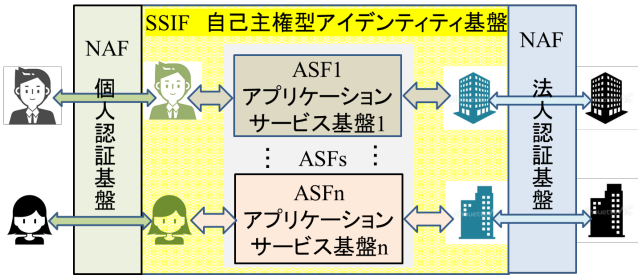

図 1　SSBSI 構成

本章では，日本をはじめ各国のサイバー社会の基盤となっているインターネットの課題，第１章で述べたサイバー・フィジカル社会の更なる発展のために克服が必要なサイバー社会の二つの大きな課題，利用者の強い匿名性の課題を克服する利用者の確実な本人確認および匿名性と特定性の両立の仕組み，サービス事業者への個人情報・プライバシー情報の集積の課題を克服する利用者による個人情報・プライバシー情報の利用制御が可能な仕組みの，SSBSI での実現方式および運用・管理上の要件について記載する．

2.1　利用者の強い匿名性の課題への対応策

サイバー社会での利用者の安心・安全な活動には，利用者の匿名性は必要であるが，一方，社会の安心・安全の維持には，不正・不法な利用や，悪意のある/無責任な発言・行為を実施した利用者の特定性が必要である．

SSBSI では，利用者の確実な本人確認を前提としつつも，この矛盾する利用者の匿名性と特定性の両立を可能とする仕組みを組み込んでいる．

2.1.1.　利用者の確実な本人確認方式

既に多くの国で運用されているように，フィジカル社会の個人は，国民登録制度等の NAF にて確実な本人確認後，個人識別コード NAF-IDp および鍵ペアが付与され，名前，住所等の個人情報と紐づけられ管理されるとともに，NAF-IDp および鍵ペアの情報等を内蔵する個人カード等が配布されることを前提としている．SSBSI での利用者の確実な本人確認は，既存の国民登録制度等の NAF の利用を想定している．

NAF 登録済み利用者の，SSIF を構成するサービス事業者（SSIF 事業者）への利用登録に際しては，提示された NAF-IDp と対応する秘密鍵を使用した署名による当人確認により利用登録申請者が本人確認済みの NAF 利用者であることを確認の上，新たに SSIF で使用する個人識別コード SSIF-DIDp（W3C の仕様に準じた DID）および鍵ペアが生成され，SSIF では NAF-IDp と SSIF-DIDp が紐づけられ管理されるとともに，個人は SSIF-DIDp および鍵ペアにより SSIF の利用者として活動する([12]，[13])．このように，SSIF 事業者は，NAF の PKI ベース等の認証基盤から W3C の DID ベースの認証基盤へのゲートウェイとしての役割を担っている．SSBSI では，確実な本人確認済み個人識別コード NAF-IDp との確実な当人確認後に付与された SSIF-DIDp も，確実な本人確認済みの個人識別コードとして扱っている．

SSIF に登録済みの利用者は SSIF-DIDp および対応する鍵ペアにより，希望するアプリケーションサービスを提供する事業者（ASF 事業者）の当人確認を受け，新たな個人識別コード ASF-DIDp （W3C の仕様に準じた DID）および鍵ペアが生成され，ASF 事業者では SSIF-DIDp と ASF-DIDp が紐づけられ管理されるとともに，個人は ASF-DIDp および鍵ペアにより ASF の利用者として活動する．SSBSI では，本人確認済み個人識別コード SSIF-DIDp との確実な当人確認後に付与された ASF-DIDp も，確実な本人確認済みの個人識別コードとして扱っている．

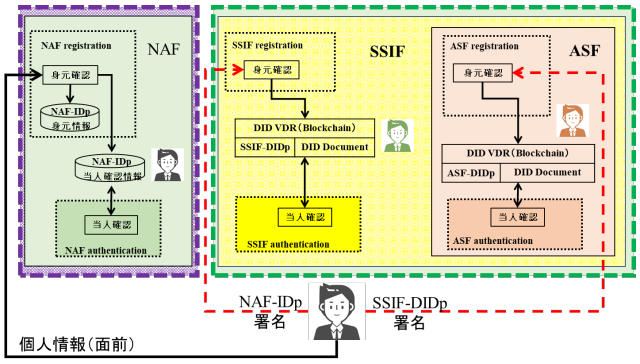

図２　サービス利用登録時の利用者の本人確認

2.1.2.　利用者の匿名性確保方式

SSBSI では，サービス登録時および利用時に個人の名前･住所等の個人情報を扱うのは NAF のみである．NAF は，個人の身元確認・当人確認後，匿名性確保のため，個人を特定･推定できない個人識別コード NAF-IDp と，以降の当人確認に使用される鍵ペアを，利用者へ発行する．

NAF 登録者が SSIF 事業者への利用登録時には，名前・住所等の個人情報を SSIF 事業者へ提示する必要は無く，匿名性の高い NAF 個人識別コード NAF-IDp との当人確認のみで登録可能で，更に NAF-IDp を推定できない新たな利用者識別コード SSIF-DIDp を付与することにより，匿名性を確保している．

同様に，SSIF 利用者が ASF 事業者への利用登録時には，名前・住所等の個人情報を ASF 事業者へ提示する必要は無く，匿名性の高い利用者識別コード SSIF-IDp との当人確認のみで登録可能で，更に SSIF-DIDp を推定できない新たな利用者識別コード ASF-DIDp を付与することにより，匿名性を確保している．

フィジカル社会の個人は，名前や住所等の個人情報を一切提供することなく，また個人情報と紐づけられた NAF-IDp を推定できない個人識別コード SSIF-DIDp，ASF-DIDp を使用しサイバー社会で活動でき，利用者の匿名性を確保している．

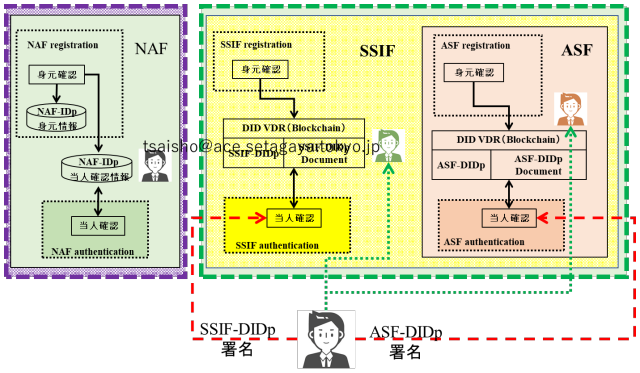

図３　サービス利用時の登録利用者との当人確認と登録サイバーエンティティ経由のサービス利用

2.1.3. 利用者の特定性確保方式

ASF を構成する事業者のサービス内で何らかの不正・不法な行為，悪意のある・無責任な行為が検知された場合，行為者の個人識別コード ASF-IDp を特定できても，サービス内のサイバーエンティティの匿名性によりその個人識別コードからは直接フィジカルエンティティ（利用者個人）を特定できない．

そこで SSBSI では，ASF 事業者への利用登録時に提示された SSIF の個人識別コード SSIF-DIDp と新たに付与された ASF-DIDp の対応を格納・管理しておき，必要な場合は ASF-DIDp と紐づけられた SSIF-DIDp を確認できることを想定している．同様に，SSIF 事業者は，利用登録時に提示された NAF の個人識別コード NAF-IDp と新たに付与された SSIF-DIDp の対応を格納・管理しておき，必要な場合は SSIF-DIDp と紐づけられた NAF-IDp を確認できることを想定している．

このような各サービスの提供者が格納・管理する個人識別コードの対応情報を利用し，匿名性が確保された ASF 事業者のサービスにおける識別コード ASF-DIDp から，SSIF-DIDp，NAF-IDp，最後に利用者の身元情報を特定し，ASF を構成する事業者のサービス内で何らかの不正・不法なあるいは悪意のある・無責任な利用者・個人を特定できる方式を想定している．

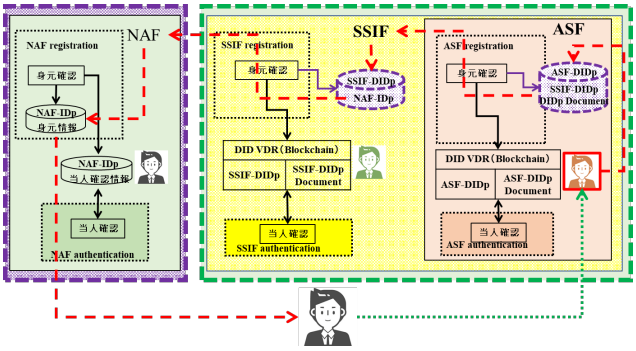

図 4　ASF 内のサイバーエンティティに対応するフィジカルエンティティ（利用者個人）の特定方式

2.1.4. 利用者の匿名性と特定性の両立を可能とするための要件

利用者の匿名性確保方式および特定性確保方式のそれぞれについては既述の通りであるが，その両立のためには以下の運用上の要件が必要となる．

① 個人識別コードの対応情報の安全・確実な管理

すべての SSIF 事業者，ASF 事業者は，利用者の登録時には，個人識別コードの対応情報の作成・管理が必要となる．

万一その情報が漏洩した場合は，利用者の匿名性へのリスクとなり，万一その情報を消失した場合は，利用者の特定が困難となる．

サイバー社会上のサービス事業者，SSIF 事業者および ASF 事業者には，利用者の匿名性と特定性の両立に不可欠な，個人識別コードの対応表の安全・確実な管理が求められる．

② 開示請求とサービス事業者の順守に関する法制度等の整備

開示請求にはその必要性に関する合法性の確認，客観的評価の仕組みが必要であり，また合法的な開示請求に対しては，サービス事業者の確実な対応を求める法制度の整備が必要である．

2.2 サービス事業者への個人情報・プライバシー情報の集積の課題への対応策

Web サービスの爆発的普及はサイバー社会の発展に大きく寄与したが，一方では多くのサービス事業者へ個人情報・プライバシー情報が集積されることになり，漏洩事件や悪用事件が多発することになった．

SSBSI では，サービス事業者への情報の集積を抑止する仕組み，個人情報・プライバシー情報の自己利用制御性を可能とする仕組みを組み込んでいる．

2.2.1. 名前・住所等の個人情報の集積抑止

SSBSI では，SSIF 事業者・ASF 事業者への利用登録時の本人確認には，本人確認済みのサイバーエンティティとの当人確認により本人確認を行う方式であり，名前・住所等の個人情報の集積は行わない．

なお，SSIF および ASF では，利用登録の判断のエビデンスとして，新たに付与された個人識別コードに紐づけて，本人確認に使用したサイバーエンティティの個人識別コードの情報を登録・管理する．管理する情報には名前，住所等の個人情報は含まれず，漏洩しても利用者個人を直接特定はできないが，利用者固有の識別符号であり，漏洩した場合は匿名性へのリスクとなり，安全な管理が求められる．

2.2.2. 個人情報を含む様々の属性情報の自己利用制御方式

SSBSI では，SSI を原則とし，W3C で標準化が進められている DID, VC を活用する構想である([12],[13])．

SSIF 事業者・ASF 事業者のサービスでは，利用者に対応するサイバーエンティティに付与されたそれぞれ異なる個人識別コード DID および鍵ペアを使用した署名検証による登録利用者との当人確認により利用が可能となる．このような登録している各サービスの利用に不可欠な DID および鍵ペアは利用者自身が SSBSI Wallet で安全・確実に管理することを想定している．

また，利用者の様々の属性情報は，属性を管理する信頼できる組織から属性証明書として利用者へ VC の形式で発行され，利用者自身が SSBSI Wallet にて管理し，他のサイバーエンティティへの提供時には，VC 内の必要な情報項目だけを開示できる，選択開示可能な署名方式の採用やハッシュ値ベースの VC 等の利用により，個人情報・属性情報・秘密情報の必要な範囲だけの選択開示が可能な仕組みを想定している．

なお，SSBSI Wallet については，耐タンパー性が確保されたセキュアなポータブルデバイスを想定しているが，仕様は別途検討予定．

3. SSBSIjp：日本向けの SSBSI 構想

本章では，SSBSIjp における，サイバー社会の大きなセキュリティ課題への対応策，利用者の強い匿名性の課題を克服する確実な本人確認および匿名性と特定性の両立の仕組み，サービス事業者への個人情報の集積の課題を克服する利用者による個人情報・プライバシー情報の利用制御が可能な仕組みを利用者（個人）向けの仕組みについて報告する．

3.1 NAFjp：日本の個人認証基盤

日本の個人認証基盤として，現状の個人番号制度の利用を想定している．自治体における確実な身元確認・当人確認のもと，マイナンバーが割り当てられ，署名用電子証明書，利用者証明用電子証明書および両電子証明書の秘密鍵等を内蔵するマイナンバーカードが利用者へ提供される．

NAFjp-IDp として使用する識別コードとしては, マイナンバーカードに内蔵されている利用者証明用電子証明書内の利用者証明用 ID（JPKI 固有 ID）を想定している．

JPKI 固有 ID は, 住民基本台帳法, マイナンバー法（番号利用法），において，民間利用は禁止されているため, SSIFjp を構成する事業者（SSIFjp 事業者）としては，現状では自治体等の公的機関に限らざるを得ない．しかし，将来的には，急拡大するサイバー社会の基盤的サービスを支えるために，信頼できる民間企業を SSIFjp 事業者として認定の上, SSIFjp の運用を担ってもらうことを想定している．

なお，NAFjp-IDp として JPKI 固有 ID の使用が難しい場合は，新たな JPKI 固有 ID を推定できない，新たな識別コードを生成，マイナンバーカードへ格納し，利用することも想定している．

3.2 SSIFjp：日本の自己主権型アイデンティティ基盤

SSIFjp 事業者は，NAFjp の JPKI ベースの認証基盤から W3C の DID ベースの認証基盤へのゲートウェイとして機能する．

SSIFjp 事業者は, 利用者へチャレンジと共に認証要求を提示すると，利用者はマイナンバーカードをカードリーダ等で読み取り，利用者証明用電子証明書に対応する秘密鍵でチャレンジに署名し利用者証明用電子証明書と共に事業者へ提示する．事業者は電子証明書内の公開鍵でチャレンジへの署名を検証し，利用者が身元確認済みの利用者証明用電子証明書の所有者であることを確認の上，利用者の識別コードである電子証明書内の利用者証明用 ID（JPKI 固有 ID）を確認する．

その後に，利用者は手元で SSBSI Wallet を使用し新たな識別コード SSIFjp-DIDp および鍵ペアを生成し，SSIFjp 事業者へ新たな識別コード SSIFjp-DIDp および公開鍵を提供する．事業者は，VDR（Verifiable Data Registry）へ SSIFjp-DIDp および DIDp Document を登録する．最後に，利用者証明用 ID（JPKI 固有 ID）と新たな識別コード SSIFjp-DIDp との対応情報を格納する．

3.3 ASFjp: 日本のアプリケーションサービス基盤

SSIFjp 上でアプリケーションサービスを提供する事業者（ASFjp 事業者）は，利用者へ認証要求と共にチャレンジを提示すると，利用者は SSIFjp-DIDp に対応する秘密鍵でチャレンジに署名し SSIFjp-DIDp と共に ASFjp 事業者へ提示する. ASFjp 事業者は DID Method Resolver 等を利用し SSIFjp-DIDp に対応する DIDp Document を入手し公開鍵を確認，その公開鍵でチャレンジへの署名の検証し，利用者が身元確認済みの識別コード SSIFjp-DIDp の所有者であることを確認する．

その後に，利用者は手元で SSBSI Wallet を使用し新たな識別コード ASFjp-DIDp および鍵ペアを生成し，ASFjp 事業者へ新たな識別コード ASFjp-DIDp および公開鍵を提供する．事業者は，VDR へ ASFjp-DIDp および DIDp Document を登録する. 最後に, SSIFjp-DIDp と新たな識別コード ASFjp-DIDp との対応情報を格納する．

3.4 SSBSIjp における利用者の匿名性と特定性の両立

NAFjp が発行する NAFjp-IDp ，SSIFjp で使用する SSIFjp-DIDp，ASFjp で使用する ASFjp-DIDp は，相互に関連を特定できない識別コードとすることにより，SSBSIjp における利用者の匿名性を確保している．

また，SSIFjp 事業者，ASFjp 事業者等は，利用者の登録時に確認した身元確認済みの識別コードと，新たな識別コードの対応情報を確実に管理することにより，SSBSIjp における利用者の特定性を確保している．

利用者の匿名性と特定性の両立の確保には，各事業者による新旧の識別コードの対応情報を安全・確実に管理する必要があり，またサイバー社会の安心・安全維持のために必要と判断された合法的開示請求には各事業者の対応が不可欠である．

3.5 SSBSIjp における利用者の個人情報の集積抑止と自己利用制御方式

SSBSIjp においても，SSIFjp 事業者，ASFjp 事業者等で利用者の情報として集積管理されるのは，名前，住所等の個人情報ではなく，新たな識別コードに紐づけられた，身元確認済みの識別コードのみである．

以上のように，SSBSIjp においても，SSIFjp，ASFjp における利用登録時の名前，住所等の個人情報の集積は行わない方式である．

また，個人情報・プライバシー情報等の自己利用制御方式は，SSBSI 構想と同一方式とし，同様に個人情報の自己利用制御方式を実現している．

4. EBSI（European Blockchain Services Infrastructure）概要

EBSI は，ブロックチェーンを活用して，EU 各国の行政機関と様々のサービス提供者による情報の検証を可能とし，国境を越えたサービスの信頼性を高め，サービスの導入・普及を加速することを目指した，EU のブロックチェーンサービス基盤である．

2018 年に，EC(European Commission）と EU 加盟国が共同で EBP(European Blockchain Partnership）を設立，EU 全体で信頼できる公共サービス向けのブロックチェーン基盤の検討に着手，翌年から EBP のもとで EBSI の構築および EBSI 上で様々のパイロット PJ が展開された．2024 年 5 月には，EC は EBSI の運用・管理主体を EBP から新たに設立した EUROPEUM-EDIC （European Digital Infrastructure Consortium for Blockchain and DLT)へ移し，EBSI の本格稼働・実用化へと動き始めた．

EBSI を支えるブロックチェーンネットワークは，現在も拡大中であるが，15 程度のバリデータノード，オブザーバノードを含めると欧州全体で 40 程度のノードで構成されている．また，Trust Registry 運営機関（各加盟国の規制当局や認定機関）が EBSI ブロックチェーンへ，信頼できる VC 発行者や検証者を登録している．具体的には，VC 発行者や検証者が信頼できるかどうか，VC 発行者がどの属性・資格を発行する権限があるか，提示された VC がどのスキーマ・定義に基づく VC かどうか，等が確認できる情報が登録されている．

なお，EBSI 上で直接活動するのは公共的・基盤的なサービス提供機関（大学，行政，商工会など）で，SSBSI の ASF で想定している SNS やショッピングのような商用サービスの EBSI 上での展開は想定されていないが，EBSI の VC や DID を認証手段として利用することは検討されている模様．

4.1 EBSI における市民の登録・利用概要

利用者としての市民は，個人用のウォレットやサービスを通じて EBSI を利用する．

利用手続きは以下の通り．

①個人用 EU Digital Identity Wallet（EUDI Wallet）を取得

②サービス提供者（大学・行政・企業など）に VC（証明書）を要求

③EUDI Wallet での確認操作により VC を受領

④検証者に VC の必要な情報項目のみを提示

EUDI Wallet の取得手続きは以下の通り．

①EUDI Wallet アプリをダウンロード

②EUDI Wallet の初期化により，DID・鍵ペアを生成

③各国の「認定資格情報発行機関（QTSP/Qualified Issuer)」が，国民電子 ID（eID)，国民 ID カード，パスポート等で本人確認

④本人確認後に，基盤的 VC（eID 属性 VC）（名前，生年月日，国籍，国民 ID 番号あるいは住民登録番号の識別コード等）および本人確認済み VC を EUDI Wallet へ登録

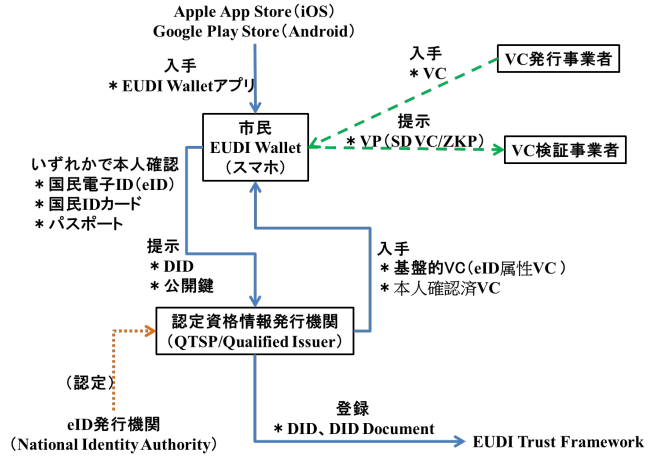

図５　EBSI における市民の利用登録・利用概要

4.2 EBSI における事業者の登録・利用

利用者としての事業者は，法人用 EUDI Wallet を利用し，ビジネス取引時の相手の事業者資格証明 VC の検証等で，EBSI を利用する．

利用手続きは以下の通り．

①法人用 EUDI Wallet を取得

②市民の要求に応じ，VC（証明書）を発行

③市民提供の VP および内蔵する他の事業者発行の VC を確認（検証）

法人用 EUDI Wallet の取得手続きは以下の通り．

①事業者名義で公開鍵基盤を作成

②QTSP（Qualified Trust Service Provider）へ法人用 EUDI Wallet を申請

＊事業者の法的存在証明，事業者識別番号，法定代表者，ドメイン名の所有証明等を QTSP へ提示

③法人用 EUDI Wallet を受領

＊QTSP 証明書を格納（秘密鍵は QTSP 管理）

＊事業者 DID，法人識別子，等

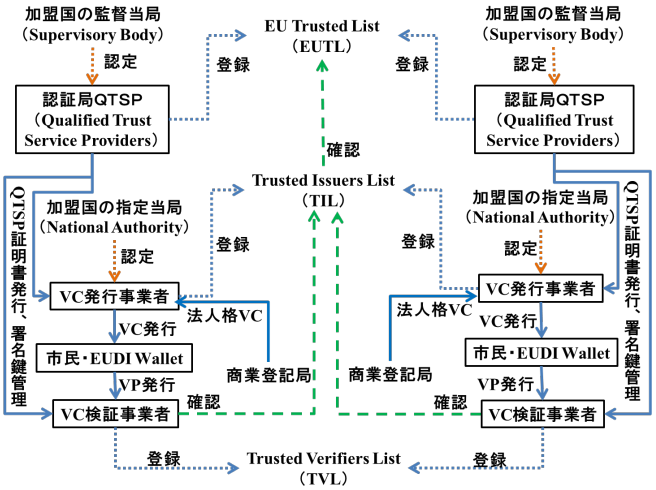

図６　EBSI における事業者の登録・利用

4.3 EBSI における利用者の匿名性と特定性の両立

SSBSI は構想レベルであるが，サイバー社会のサービスのすべてがブロックチェーン上で展開されることを想定し，商用サービスも含め，利用者の匿名性と特定性の両立を実現する仕組みを提案している．

EBSI は実運用が始まっており，現状は公共的・基盤的なサービス提供機関（大学，行政，商工会など）を対象，SSBSI の NAF+SSIF の範囲を対象としている．SSBSI における ASF は対象外であるが，今後，様々の商用サービスへの対応も，検討されるものと考えている．

本節では，EBSI における利用者の匿名性と特定性の両立の仕組みを整理し，NAF+SSIF の範囲の SSBSI との類似点・相違点等を考察する．

4.3.1. 確実な本人確認

EBSI を利用する各国では，それぞれ固有の国民認証基盤，確実な本人確認のもとに発行される国民電子 ID（eID），国民 ID カード，パスポート等を利用した認証基盤が運用されている．

EBSI では，各国の認定資格情報発行機関（QTSP/Qualified Issuer）が，それぞれの国民認証基盤をベースに申請者の本人確認を実施し，EUDI Wallet に EBSI 利用に必要な情報を，基盤的 VC（eID 属性 VC）として格納する．

なお，本人確認方法は各国にて異なるが，eIDAS 2.0 では「利用者の身元確認をどの程度厳密に行ったか」を示す 3 段階（Low / Substantial / High）のレベル（LoA）が定義されており，EUDI Wallet の有効化には Substantial レベル以上の LoA が必須となっている．ただし，国民カードと同等の情報を含む基盤的 VC（eID 属性 VC）が EUDI Wallet に格納されるのは，High レベルの身元確認が実施された場合のみである．基盤的 VC が内蔵されていない EUDI Wallet を使用して，確実な本人確認が必要なサービスへの登録を行う際には，追加の本人確認が必要となる．

また，EUDI Wallet で生成した DID と基盤的 VC とのリンクを示す情報を，本人確認済み VC として格納する．利用者が誰であるかを示す必要がある場合は基盤的 VC を使用するが，本人確認済みのみを示せばよい場合は，本人確認済み VC を使用する．

SSBSI の EBSI との類似点・相違点は以下の通り．

①SSBSI では，本人確認済み VC 発行の代わりに，SSIF 事業者が国民認証基盤 NAF を使用し利用者を確実に本人確認後に DID Document を VDR に登録し，検証者が VDR を利用し本人確認済み利用者であることを確認できる仕組みを想定している．

②基盤的 VC については，SSBSI も必要な場合は同様の住民票 VC 等を発行することを想定している．

③SSBSI ではすべての利用者は確実な身元確認済みを前提としており，EBSI における High レベルを必須としている点が，EBSI と異なる．

4.3.2. 利用者の匿名性の確保

EBSI では，利用者が新たなサービスへの利用登録時には，利用者の判断で EUDI Wallet で新たな DID，鍵ペアを生成し利用可能で，利用者の推定が困難な DID，公開鍵の使用，その使いまわしの回避により，利用者の匿名性を確保されている．

また，利用登録時の本人確認に，本人確認済み VC を使用する場合にサービス事業者が残すエビデンスは，使用された VC の識別情報や本人確認レベル（LoA），検証時の署名確認結果等で，利用者の属性情報は含まれず，匿名性に配慮されている．

なお，利用者がだれであるかまで確認する必要があるサービスへの利用登録時には基盤的 VC を使用せざるを得ないが，サービス事業者が残すエビデンスは，使用された VC の識別情報，検証時の署名確認結果等の他，検証に必要だった VC 内の利用者の属性情報（例：「氏名」「住所」「生年月日」など）のみとし，匿名性へ配慮されている．なお，選択開示には，BBS+署名の採用やゼロ知識証明（ZKP）の利用を想定している．

SSBSI の EBSI との類似点・相違点は以下の通り．

①サービスごとに異なる DID の使用による匿名性確保の仕組みは同じ．

②SSBSI で本人確認時にエビデンスに残すのは新旧の識別コード DID のみで，EBSI と仕組みは異なるが，匿名性の確保については同程度．

4.3.3. 利用者の特定性の確保

EBSI では，基盤的 VC を利用し登録したサービスにおける事故・事件が発生した場合は，サービス事業者はその利用者の本人確認時のエビデンスに含まれている VC の情報から，あるいは VC の識別情報により VC 発行事業者を特定でき，その事業者から利用者を特定可能である．

また，本人確認済み VC を利用した場合も，本人確認時のエビデンスに含まれている基盤的 VC の識別情報により VC 発行事業者が特定でき，その事業者から利用者を特定可能である．

SSBSI は，事故・事件が発生したサービスの事業者が管理する本人確認に使用した本人確認済み DID から，その DID Document から本人確認を行った事業者を特定でき，同様の手順を繰り返し，利用者を特定する方式である．SSBSI とは，仕組みが若干異なるが，同様の利用者の特定性を確保している．

4.3.4. 利用者の匿名性と特定性の両立

利用者の匿名性確保方式および特定性確保方式については既述の通りであるが，その両立のために，SSBSI と同様の，以下のような運用上の要件が検討されている模様．

①サービス事業者による本人確認時のエビデンスの安全・確実な管理

EBSI では，サービス事業者に対しエビデンスの

収集や安全な管理が，eIDAS2.0，実装ガイドライン等で規定される模様.

②合法的開示請求へのサービス事業者の確実な対応

EBSI では，合法的なインシデント対応のためのエビデンス開示請求へのサービス事業者の対応については，eIDAS2.0，実装ガイドライン等で規定される模様.

SSBSI は未だ構想段階であるが，実装フェーズにおいては，サービス事業者によるエビデンスの安全・確実な管理および合法的開示請求へのサービス事業者の確実な対応について，サービス事業者向けのガイドラインや法制度の整備も並行し検討されることを期待している.

4.4 利用者の個人情報の集積抑止と自己利用制御について

本節では，EBSI における利用者の個人情報の集積抑止と自己利用制御の仕組みと，NAF+SSIF の範囲の SSBSI との相違点等を考察する.

4.4.1. 名前，住所等の個人情報の集積抑止

基盤的 VC を使用した場合は，サービス事業者が本人確認に必要だった個人情報もエビデンスとして管理するため，必要最小限の個人情報の集積は避けられない．本人確認済み VC を使用した場合は，サービス事業者が管理するエビデンスには利用者の名前，住所等の個人情報は含まれず，個人情報の集積は無い.

SSBSI においては，EBSI で基盤的 VC を使用する必要がある場合，SSBSI においても同様の個人情報の管理が必要で，やはり個人情報の集積は避けられない．本人確認済み VC を使用した場合は，本人確認済みの確認に使用した利用者の DID およびサービス事業者の情報のみで，SSBSI においても同様に名前，住所等の個人情報の集積は無い.

EBSI は SSBSI と同程度の個人情報の集積抑止と想定される.

4.4.2. 個人情報の自己利用制御方式

EBSI も，SSBSI と同様，SSI を原則とし，W3C で標準化が進められている DID，VC を活用する構想である([12]，[13]).

EBSI では，利用者向けに発行された様々の個人情報を含む属性情報の証明書 VC は利用者自身が EUDI Wallet で管理する.

サービス事業者へ VC を提供する場合も，利用者が，その必要性の判断，VC 内の個々の属性情報の開示・非開示の判断を行い，その判断に基づいた VC の選択開示が可能な仕組みや，VC 内の個々の属性値そのものではなく，属性を持っていることを証明できる仕組み，が提供されており，利用者による個人情報を含む属性情報の自己利用制御が可能である.

SSBSI でも，個人情報を含む属性情報の管理には SSBSI Wallet の使用を想定している．EBSI は SSBSI と同程度の個人情報の集積抑止と想定される.

なお，SSBSI Wallet の具体的な検討は今後の課題となっている．検討にあたっては，EUDI Wallet や，様々の用途を対象に研究開発されている SSBSI Wallet の仕様をベースに，SSBSI としての Wallet の仕様検討を進める予定である.

5. おわりに

本稿では，インターネット上のサイバー社会の二つの大きな課題，利用者の強い匿名性の課題を克服する利用者の確実な本人確認および匿名性と特定性の両立の仕組み，サービス事業者への個人情報・プライバシー情報の集積の課題を克服する利用者による個人情報・プライバシー情報の利用制御が可能な仕組みの実現による，安心・安全なサイバー社会の基盤となることを目指したブロックチェーンサービス基盤 SSBSI を提案した.

また，EU で社会実装が始まった EBSI の仕様を整理し，SSBSI との類似点･相違点を指摘した. 結論として，SSBSI と EBSI，目指す安心・安全なサイバー社会，その実現のための仕組みについては，大きな違いは無いことを確認できた.

一方，SSBSI の仕組み，技術上の実装可能な仕組みを提示したが，社会実装にあたっては，まだ多くの検討課題がある.

一つは，SSBSI Wallet の検討である．. 検討にあたっては，EUDI Wallet や，様々の用途を対象に研究開発されている Secure Wallet の仕様をベースに，SSBSI としての Wallet の仕様を検討する必要があろう.

もう一つは，SSIF を担当する事業者，ASF を構成する様々のサービス事業者の果たすべき機能・責任を明確に定義したガイドラインや法制度の整備である. 29 か国が参加している EBSI は既に運用が始まっており，ガイドラインや法制度の整備も進められている．EBSI をサポートするガイドラインや法制度等を参考に，各国の事情を加味した，しかし相互運用が可能なガイドラインや法制度の整備が期待される.

サイバー・フィジカル社会の発展は目覚ましく，その中でもサイバー社会の役割はますます増大し，社会の安心・安全の維持・高度化のためには，サイバー社会の安心･安全の維持･高度化が喫緊の課題である. サイバー・フィジカル社会の健全な発展，安心・安全の維持・高度化に向けた研究開発の一層の活発化と，成果のすみやかな社会実装に期待したい.

参考文献

[1] 才所敏明,”遠隔生体認証機能を備えたブロックチェーンサービス基盤の提案 BSIwRBA -Blockchain Service Infrastructure with Remote Biometric Authentication-”. 電子情報通信学会・情報セキュリティ研究会（ISEC）. 2024.

[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”. 暗号と情報セキュリティシンポジウム（SCIS2023）. 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,”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

[4] 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”. 電子情報通信学会・暗号と情報セキュリティシンポジウム（SCIS2022）. https://advanced-it.co.jp/2016_wp/wp-content/pdf/20211028CSS2021Paper.pdf

[5] 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

[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

[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

[8] 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

[9] 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

[10] 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

[11] “Digital Identity Guidelines”, NIST Special Publication 800-63-4. 2025. https://www.nist.gov/publications/nist-sp-800-63-4-digital-identity-guidelines

[12] Decentralized Identifiers (DIDs) v1.1 Core architecture, data model, and representations. World Wide Web Consortium. 2025. https://www.w3.org/TR/did-1.1/

[13] Verifiable Credentials Data Model v2.0. World Wide Web Consortium. 2025. https://www.w3.org/TR/vc-data-model-2.0/

[14] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, 2024. https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng

[15] Welcome to EBSI hub. https://hub.ebsi.eu/

[16] EBSI's Blockchain. https://hub.ebsi.eu/blockchain-network