SCIS 2023 2023 Symposium on
Cryptography and Information Security
Fukuoka, Japan, Jan. 24 – 27, 2023
The Institute of Electronics,
Information and Communication Engineers

ブロックチェーンサービス基盤に関する考察
Considerations on Blockchain Service Infrastructure（BSI）

才所 敏明[*1] 辻井 重男[*2]
Toshiaki Saisho Shigeo Tsujii

あらまし 個人や組織の様々の活動がインターネット上で展開される時代へと移行する中，活動の過程で求められる個人や組織のアイデンティティ情報もネット経由の提供へ移行することが想定される．筆者らが提案している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）は，インターネット上での個人や組織間での安全なアイデンティティ情報の流通およびアイデンティティ情報の検証を可能とする情報流通基盤である．本稿では，SSIUF 構想を発展させ，様々のアプリケーションの安心・安全なサービス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（BSI：Blockchain Service Infrastructure）構想を提案する．BSI は，各国の個人や組織の認証基盤（NAF：National Authentication Framework），自己主権型アイデンティティ基盤（SSIF：Self-Sovereign Identity Framework），多様なアプリケーションサービス（ASF：Application Service Framework）から構成され、個人や組織間での情報の送受信には W3C（World Wide Web Consortium）で標準化が進められている分散型 ID（DID：Decentralized Identifier）/検証可能属性証明（VC：Verifiable Credential）関連技術の活用を想定している。また，日本で早期の実現が期待されている NAFjp（NAF in Japan）を利用した日本におけるブロックチェーンサービス基盤 BSIjp（BSI in Japan）の構成案を示す。

キーワード 自己主権型アイデンティティ，SSI，自己主権型アイデンティティ情報利活用基盤，SSIUF，ブロックチェーン，ブロックチェーンサービス基盤，BSI，本人確認基盤，NAF，自己主権型アイデンティティ基盤，SSIF，W3C，分散型 ID，DID，検証可能属性証明，VC，検証可能属性提示，VP，匿名性，特定性，追跡性

1 はじめに*

1974 年の TCP/IP 発表に始まるインターネットの歴史は高々半世紀ではあるが，今やインターネット無しでは産業界の経済活動も国民の生活活動も成り立たない，まさにインターネット（依存）社会である．個人や組織の活動がインターネット上の活動へ移行する中，個人や組織のアイデンティティ情報や様々の属性情報のインターネット上でのやり取りも必要となり，アイデンティティ情報や属性情報の信頼性と個人情報保護・プライバシー保護を個別に工夫しつつ，実際に行われ始めている．

今後，インターネット経由での個人や組織の活動が増加し，アイデンティティ情報や様々の属性情報の流通がますます活発になることが想定される．インターネット上でのアイデンティティ情報や様々の属性情報の安全な管理，提供，活用を可能とする基盤は，インターネット社会の発展を支える基盤となるものと想定され，早期の構築が期待される．

筆者らが提案している SSIUF（Self-Sovereign Identity-information Utilization Framework）は，このようなインターネット社会を支える基盤，アイデンティティ情報保有者による自身の情報への確実な制御を可能とする自己主権型アイデンティティ情報利活用基盤である（[1]～[3]）．

本稿では，SSIUF を更に発展させ，利用者の一定の匿名性を確保しつつも利用者の不正・不法な利用や悪意のある利用の場合は利用者の特定・追跡を可能とする，社会の安心・安全の維持に必要な機能を提供するアプリケーションサービス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（BSI：Blockchain Service Infrastructure））構想を提案する．

BSI は，個人や組織の認証基盤（NAF：National

*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

Authentication Framework)，自己主権型のアイデンティティ基盤（SSIF：Self-Sovereign Identity Framework)，および様々のアプリケーションサービス基盤(AS:Application Service Framework）により構成されることを想定している（図 1)．本稿では，BSI を構成する NAF，SSIF，ASF に期待する機能や要件の概要を示し，BSI の全体像を示す．

また，BSI の日本におけるインスタンス，想定する日本のブロックチェーンサービス基盤（BSIjp：Blockchain Service Infrastructure in Japan）の概要を示す．

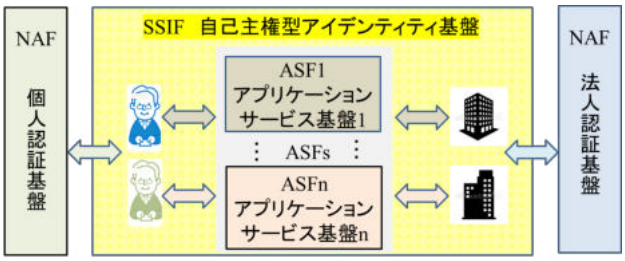

図 1　BSI 基本構成

2　ブロックチェーンサービス基盤（BSI）

BSI 上では，多くの法人（組織・団体）が様々のサービスを展開し，多くの個人（利用者）がそれらを活用し活動を展開することを想定している．

BSI を構成する認証基盤 NAF は，個人・法人の確実な身元確認を実施し，NAF としての識別コード（NAF-ID）を付与する．

自己主権型アイデンティティ基盤 SSIF では，NAF にて身元確認済であることを確認した個人・法人に対し識別コード，W3C で標準化が進められている DID（Decentralized Identifier）([9]) を付与すると共に，NAF-ID と DID の対応を管理する．

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 では，サービス提供者である SSIF 登録済みの法人がサービスの利用を希望する個人が提示する SSIF で付与された DID の所有者であることの確認により，その利用者が身元確認済であることを確認し，その上でサービス提供の可否を判断する．ASF で使用される利用者の識別コードは，SSIF で付与された識別コードを利用する場合や ASF における利用者識別コードとしてあらためて DID を付与する場合等，それぞれの ASF のサービス内容やポリシーに応じ選択されることを想定している．

SSIF や ASF で付与される DID には個人を特定する情報は含まないことを想定しており，利用者が個人情報漏洩につながる情報を自ら開示しない限り，利用者の一定の匿名性が確保されることを想定している．

一方，一定の匿名性を維持している ASF での利用者の活動において，何らかの事故・事件の発生あるいは不正・不法が疑われる活動が発見された場合には，合法的手続きにより，SSIF が管理する NAF-ID と DID の対応情報から NAF-ID を特定し，NAF が管理する身元情報から利用者の特定・追跡が可能となることを想定している

以上のように，BSI では利用者の一定の匿名性および合法的手続きの元の利用者の特定・追跡性の確保を想定しており，BSI は，利用者である個人，サービス提供者である法人の安心・安全な活動基盤であると共に，社会の安心・安全の維持の仕組みを備えた活動基盤となることを目指している．

BSI は，W3C で標準化が進められている DID を利用し，確実な本人確認と，利用者の匿名性と特定・追跡性の両立を実現した方式であり，個人情報・プライバシー情報のやり取りにおいては，情報の真正性検証を可能とするため，W3C で標準化が進められている VC（Verifiable Credential）/VP（Verifiable Presentation）([10]) の利用を想定している．

2.1　個人認証基盤（NAF for Natural Person）

個人の様々の活動がインターネット上の活動へと移行する中，各国はインターネット上での本人確認の仕組みである個人認証基盤（NAF for Natural Person）の整備・高度化を進めている（[4]）．

BSI においても本人確認は必須であり，各国の個人認証基盤の活用を想定している．本人確認は身元確認と当人確認から構成され，個人認証基盤もこの二つの機能から構成されている．

個人の身元確認は，面前での確認を基本に各国で運用されている住民登録制度等をベースに実施されることが多く，各国固有の仕組みとなっている．多くの国では，登録された個人にはインターネット上での識別コード NAF-ID（eID）も付与されている．

個人の当人確認は，サービスを要求する個人が NAF-ID が付与された身元確認済の個人と同一であることをインターネット上で確認する仕組みで，各国の IT 利用環境の整備状況に応じた当人確認方法が使用されているが，一般には公開鍵暗号技術を利用した当人確認が実施されている．

本人確認の信頼レベルは，身元確認の信頼レベル，当人確認の信頼レベルに依存する．身元確認および当人確認の信頼レベルについては，米国 NIST がガイドラインを発行している（[7]，[8]）．BSI は，アイデンティティ情報の安全な活用，自己主権型の活用を支える基盤であり，NIST で規定している身元確認レベルとしては IAL3，当人確認レベルとしては AAL3 と，高い信頼レベルが採用されることを想定している．

BSI で想定している個人認証基盤（NAF for Natural Person）の概要を図 2 に示している．

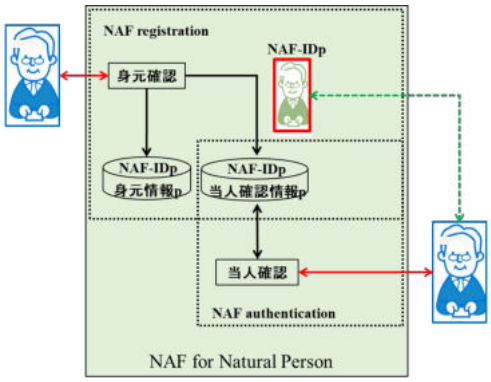

図２　個人認証基盤（NAF for Natural Person）

2.2　法人認証基盤（NAF for Legal Entity）

法人の活動もインターネット上へ急速に移行する中，インターネット上での法人確認の仕組み，法人認証基盤（NAF for Legal Entity）もまた各国で整備・高度化が進められている．

法人確認も，法人としての身元確認と当人確認から構成され，法人認証基盤もこの二つの機能から構成されている．

法人としての身元確認は，各国で既に運用されている法人登録制度等をベースに構築されることが多く，各国固有の仕組みとなっている．多くの国では，登録された法人にはインターネット上での識別コードNAF-ID（eID）が付与されている．

法人としての当人確認は，SSIF へ登録を申請した法人が NAF-ID が付与された身元確認済の法人と同一であることをインターネット上で確認する仕組みで，各国の IT 利用環境の整備状況に依存するが，一般には公開鍵暗号技術を利用した当人確認が実施されている．

BSI で想定している法人認証基盤（NAF for Legal Entity）の概要は，図 2 に示す個人認証基盤とは身元確認，当人確認の内容が異なるが，ほぼ同じ構成を想定している．

2.3　自己主権型アイデンティティ基盤（SSIF）

自己主権型アイデンティティ基盤 SSIF においても利用者の本人確認が必要であるが，SSIF の利用は NAF 登録者を前提としており，NAF 登録者の身元確認は実施済みであるため，SSIF における身元確認は NAF における当人確認の仕組みを利用することを想定している．具体的な当人確認方法の例を図３に示している．

NAF-ID を提示しサービスを要求する個人が NAF にて当人確認済であれば，SSIF は利用者として登録を受け付け，W3C で標準化が進められている DID を新たに発行すると同時に，その DID に対応する公開鍵暗号の鍵ペアを生成し，サービスを要求した個人には SSIF 識別コードとして使用される DID および DID に対応する鍵ペアを交付する．SSIF はまた，非改ざん性が検証可能な DID VDR（ブロックチェーン等）へ DID および DID に対応する公開鍵を含む DID Document を登録し，この公開鍵が SSIF における利用者の当人確認に使用される．

DID VDR に登録され当人確認に使用される DID および DID Document には個人を特定する情報は含めず、個人の匿名性が確保されることを想定している．

SSIF はまた，個人の特定・追跡性を確保するため，発行した DID と NAF-ID の対応を確実に管理し，合法的な開示要求には対応することを想定している．

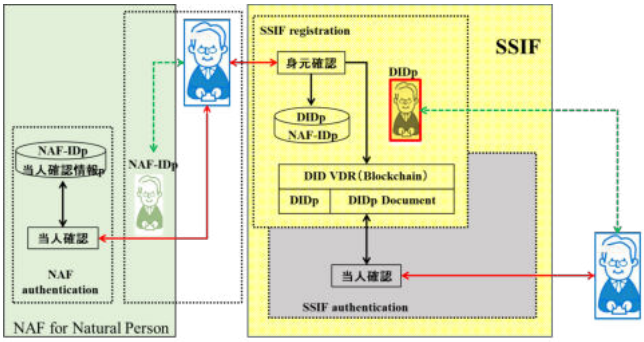

図３　自己主権型アイデンティティ基盤（SSIF）

2.4　アプリケーションサービス基盤（ASF）

アプリケーションサービス基盤 ASF は，サービス利用者（個人・法人）の識別方法により以下の三つのタイプへの分類を想定している．

タイプ A：共有 DID 型 ASF
　個人・法人に付与された SSIF 利用者識別コードをそのまま ASF 利用者識別コードとして使用するサービス

タイプ B：独自 DID 型 ASF
　個人・法人に新たな DID を付与し，その DID を AS 独自の VDR に登録し，その DID を AS 利用者識別コードとして使用するサービス

タイプ C：独自非 DID 型 ASF
　個人・法人に新たな ID（DID とは異なる従来型の ID）を付与し，その ID は AS で独自に管理し，その ID を AS 利用者識別コードとして使用するサービス

以上の BSI を構成する三つのタイプのアプリケーションサービス基盤 ASF のそれぞれが、利用者の一定の匿名性を確保しつつも利用者の不正・不法な利用や悪意のある利用の場合は利用者の特定・追跡を可能とする，社会の安心・安全の維持に必要な機能を提供するアプリケーションサービス基盤となるために必要な利用者の匿名性と特定・追跡性の両立の仕組み、想定している仕組みを以下に記載する．

2.4.1.　共有 DID 型 ASF（タイプ A）

利用を希望する個人・法人は，SSIF 登録時に付与された DID をそのまま利用者識別コードとしてサービスを利用することを想定している．

ASF としての本人確認は，サービス利用時に提示される SSIF 登録時に付与された DID および DID に対応する

秘密鍵による署名の，VDR に登録されている DID に対応する公開鍵による署名検証により，当人確認を実施する．この当人確認は身元確認済 DID との当人確認のため，ASF としての身元確認も兼ねている．

利用者識別コードである DID には，付与された個人を特定する情報は含まれず，ASF 利用時の匿名性も確保されることを想定している．

一方，ASF 利用時に何らかの問題があった場合は，SSIF 利用者識別コード DID から，その利用者を SSIF に登録した登録法人（DID 発行法人）経由 NAF-ID を特定でき，NAF 経由でその NAF-ID から身元情報を入手でき，利用者の特定・追跡を可能としている．

2.4.2. 独自 DID 型 ASF（タイプ B）

利用を希望する個人・法人は，ASF 利用登録時に新たな利用者識別コード DID を付与され，その DID を使用しサービスを利用することを想定している．

AS 利用登録時の本人確認は，共有 DID 型 ASF と同様，サービス利用時に提示される SSIF 登録時に付与された DID と DID に対応する秘密鍵による署名により，当人確認を実施する．この当人確認は身元確認済 DID との当人確認のため，ASF としての身元確認も兼ねている．

ASF は利用登録時に，新たな DID の他，対応する新たな鍵ペアを個人・法人に付与し，ASF はまた当人確認のため，DID と DID Document を，その ASF 独自の DID VDR に登録する．

共有 DID 型 ASF と同様，DID には付与された個人を特定する情報は含まれず，ASF 利用時には匿名性が確保されることを想定している．

ASF 利用時に何らかの問題があった場合の利用者の特定・追跡には，ASF 利用者識別コードの DID から，その DID を発行した ASF サービス法人経由で SSIF 利用者識別コードを特定でき，以降は共有 DID 型 ASF と同様の利用者の特定・追跡の仕組みを想定している．

2.4.3. 非 DID 型 ASF（タイプ C）

利用を希望する個人・法人は，ASF 利用登録時に新たな利用者識別コード ID，DID とは異なる従来型の ID を付与され，その ID を使用しサービスを利用することを想定している．

利用登録時の ASF による本人確認は，共有 DID 型 ASF と同様，サービス利用時に提示される SSIF 登録時に付与された DID と DID に対応する秘密鍵による署名により，当人確認を実施する．この当人確認は身元確認済 DID との当人確認のため，ASF としての身元確認も兼ねている．

ASF が利用者登録を承認する場合は，個人・法人には ASF 固有の ID 生成ルールにより新たな ID を付与し，ASF のポリシーに合致した当人確認情報の登録を要請する．個人・法人には新たに付与した ID を利用者識別コードとしてサービスを提供する．

独自 ID を使用する ASF は，ASF のポリシーやサービス内容にもよるが，一般には発行する ID には個人を特定する情報を含めず，ASF 利用時には匿名性が確保されることを想定している．

ASF 利用時に何らかの問題があった場合の利用者の特定・追跡には，ASF 利用者識別コードの ID から，その ID を発行した ASF サービス法人経由で SSIF 利用者識別コード DID を特定でき，以降は共有 DID 型 ASF と同様の利用者の特定・追跡の仕組みを想定している．

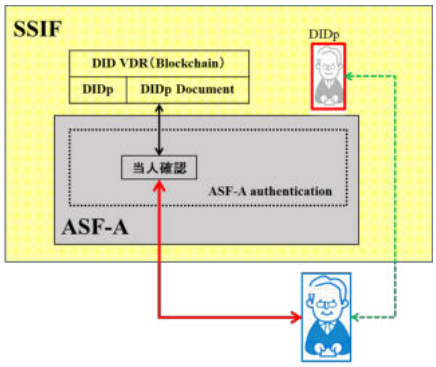

図４　共有 DID 型 ASF（タイプ A）

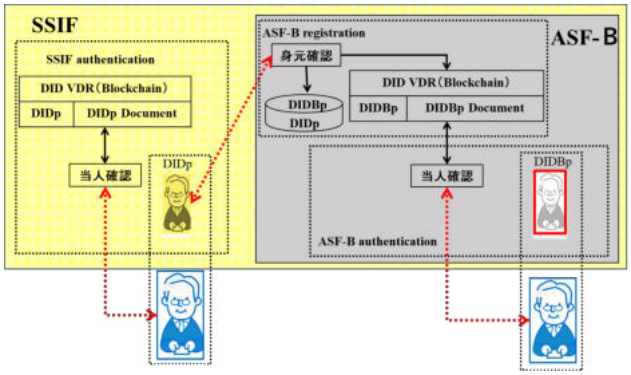

図５　独自 DID 型 ASF（タイプ B）

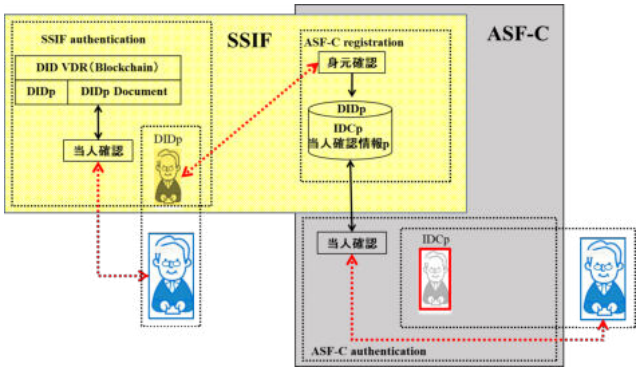

図６　非 DID 型 ASF（タイプ C）

3　日本のブロックチェーンサービス基盤（BSIjp：BSI in Japan）

本章では，ブロックチェーンサービス基盤（BSI）の日本でのインスタンス，日本のブロックチェーンサービス基盤（BSIjp：BSI in Japan）構想を示す．

BSIjp も，個人や組織の認証基盤（NAFjp：National Authentication Framework in Japan），自己主権型のアイデンティティ基盤（SSIFjp：Self-Sovereign Identity Framework in Japan），および多様なアプリケーションサービス（ASFjp：Application Service Frameworkin Japan）により構成されることを想定している．本章では，BSIjp を構成する NAFjp，SSIFjp，ASFjp として想定する具体的仕組みおよび機能・要件の概要を示し，BSIjp の全体像を示す．

3.1　日本の個人認証基盤（NAFjp for Natural Person）

日本では，2016 年 1 月 1 日より社会保障・税番号制度（マイナンバー制度）が導入され，行政を効率化し，国民の利便性を高め，公平・公正な社会を実現する社会基盤として期待されている．マイナンバー制度では，住民票を有する国民一人一人に固有の生涯変更されない識別コードとしてのマイナンバーが付与される．

マイナンバー制度では，インターネット上での本人確認には，マイナンバー制度で別途発行されるマイナンバーカードの活用が想定されている．マイナンバーカードには，身元確認の上で付与されたマイナンバーおよびマイナンバーに紐づけられた公開鍵暗号の鍵ペアが格納されており，カード内の秘密鍵による署名付与およびその検証によるマイナンバー保有者との当人確認の仕組みを提供している．

自治体等の行政サービス部門は，提供される利用者のマイナンバーカードによる署名および電子証明書を使用し，公開鍵による署名検証，電子証明書の有効性をデジタル庁所管の地方公共団体情報システム機構（JLIS）に確認することにより，本人確認が実施されている．しかし民間サービス分野では，マイナンバーカードを利用した本人確認は，未だ十分活用されていないのが実情である．

日本のブロックチェーンサービス基盤（BSIjp）では，このマイナンバーカードによる本人確認を，日本の個人向けの本人確認基盤（NAFjp for Natural Person）として活用することを想定している．マイナンバーそのものを NAFjp-ID（eID）とし，NAFjp-ID で識別される利用者の当人確認に，マイナンバーと共に付与される公開鍵暗号の鍵ペアによる署名の使用を想定している（図 7）．なお，NAFjp については，2019 年より NAFJA，NAFJP と名前を変えながら具体化してきた構想であり，詳細は参考文献[4]～[6]を参照願いたい．

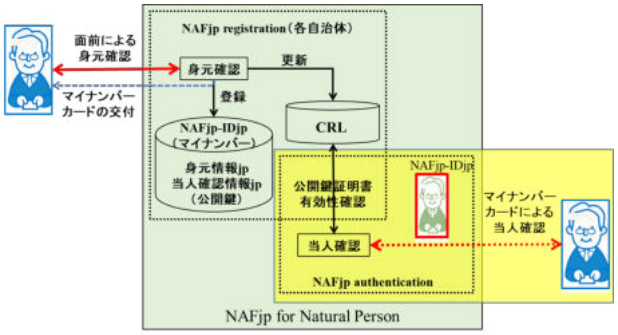

図 7　日本の個人認証基盤（NAFjp for Natural Person）

3.2　日本の法人認証基盤（NAFjp for Legal Entity）

日本では，商業登記に基づく電子認証制度が 2000 年 10 月より運用されており，商業登記済みの法人は商業登記電子証明書の利用が可能である．商業登記電子証明書および対応する秘密鍵による署名の付与により，身元を確認された商業登記済みの法人であることが確認（当人確認）されるため，法人向け手続きの多くはインターネット経由で利用可能となっている．

日本のブロックチェーンサービス基盤（BSIjp）では，この商業登記に基づく電子認証制度を利用した法人認証基盤（NAFjp for Legal Entity）の仕組みを想定している．商業登記済み法人に付与される会社法人等番号（≒法人番号）を法人の NAFjp-ID（eID）とし，NAFjp-ID で識別される法人の当人確認には，電子認証制度で発行される電子証明書内の公開鍵に対応する秘密鍵による署名の利用を想定している（図 8）．

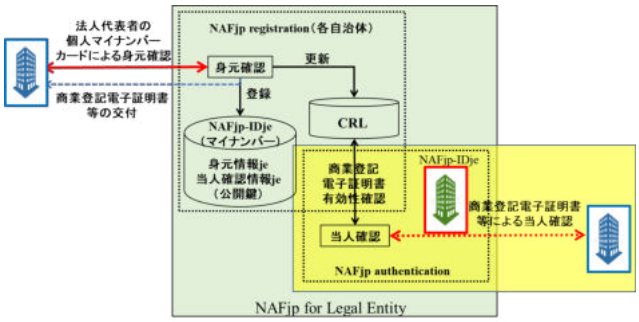

図 8　日本の法人認証基盤（NAFjp for Legal Entity）

3.3　日本の自己主権型アイデンティティ基盤（SSIFjp）

利用者が日本の自己主権型アイデンティティ基盤 SSIFjp へ登録する際には，マイナンバーカードによる本人確認を想定している．マイナンバーカード内の秘密鍵による署名と公開鍵証明書，および公開鍵証明書の有効性確認による身元確認済の NAFjp 登録者との当人確認により，SSIFjp としての身元確認とする．

身元確認が済んだ利用者には，W3C で標準化が進んでいる DID および鍵ペアを割り当て付与すると共に，他の利用者（個人）やサービス事業者（法人）が当人確認に使用できるよう，DID および鍵ペアの内の公開鍵を含む DID Document を SSIFjp の DID VDR に登録する．

SSIFjp における利用者登録を担当する法人としては，あらかじめ定められた事業者としての機能要件，セキュリティ要件を確認・評価の上で認定された法人，複数の民間事業者が担当することを想定している．SSIFjp の DID VDR も，認定された複数の法人により，安全・確実に維持・更新されることを想定している．

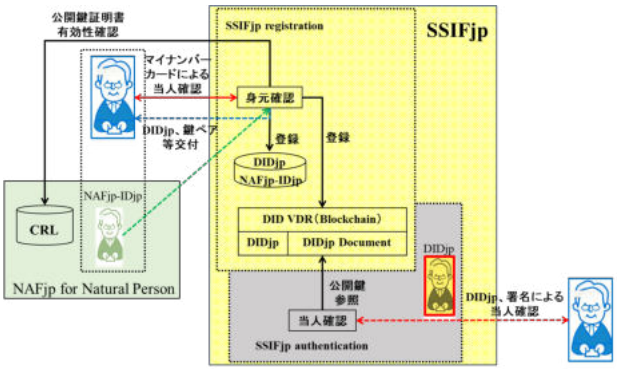

図９　日本の自己主権型アイデンティティ基盤（SSIFjp）

3.4　日本のアプリケーションサービス基盤（ASFjp）

サービス利用者（個人・法人）の識別方法による三つの分類，共有 DID 型 ASF（タイプ A），独自 DID 型 ASF（タイプ B），非 DID 型 ASF（タイプ C）ごとに，日本のアプリケーションサービス基盤 ASFjp で想定している利用者の匿名性と特定・追跡性の両立の仕組み，具体的アプリケーション例等について、以下に記載する．

3.4.1.　共有 DID 型 ASFjp（タイプ A）

アプリケーションサービス ASFjp を提供する法人も，そのサービスの利用を希望する個人・法人も，SSIFjp に登録されている個人・法人であり，DID VDR にそれぞれの DID と対応する公開鍵を含む DID Document が登録されており，相互の認証には DID と DID に対応する公開鍵による署名検証で行われることを想定している．

DID には利用者を特定する情報は含まれず，利用者の一定の匿名性が確保されており，一方，DID で識別される利用者の特定・追跡が必要な場合は DID 発行法人への要請により，対応する NAFjp-ID を特定でき，NAFjp への要請により身元情報を入手でき，利用者の特定・追跡性を確保する仕組みを想定している．もちろん，このような利用者の特定・追跡のための DID 発行法人や NAFjp への情報開示要請には合法的手続きが不可欠であることを想定している．

ASFjp の例としては，国・自治体の様々のサービスが想定される．自治体自らあるいは代行する法人が DID 発行し，住民票や納税証明書など多くの行政サービスで NAFjp-ID（マイナンバー）に対応する識別コードとして DID が利用されることを想定している．なお，国や自治体が提供するサービスで異なる DID を使用すること，利用者に複数の DID が付与されることも想定している．

利用者は，付与されている DID を使用し証明書等の発行を依頼し，ASFjp は DID による本人確認の上，本人の了解の元，必要な情報を入手し証明書等を発行する．証明書は W3C で標準化が進められている VC（Verifiable Credential）として発行されることを想定し，受け取った利用者は提供先の法人宛に，VC を内蔵する VP（Verifiable Presentation）として，検証可能な形式で提供することを想定している．

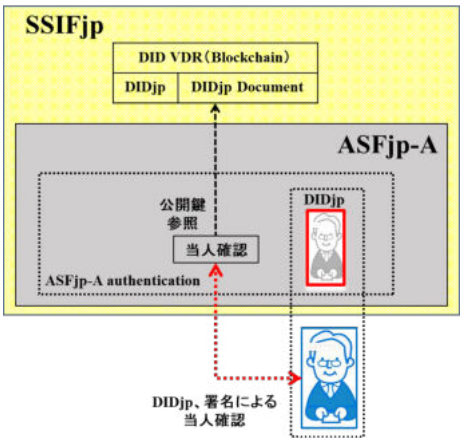

図１０　共有 DID 型 ASFjp（タイプ A）

3.4.2.　独自 DID 型 ASFjp（タイプ B）

ASFjp は利用を希望する個人の DID，SSIFjp 登録時に付与された DID による本人確認後，更に利用者としての要件を確認後，利用者として登録する．利用者には新たな DID および鍵ペアを付与し，ASFjp 独自の DID VDR へ新たに付与した DID と DID Document を登録すると共に，ASFjp は本人確認に使用した SSIFjp の DID と新たに発行した DID との対応情報を安全に管理することを想定している．

このタイプの ASFjp としては，民間の様々のサービスが想定される．具体的には，様々の属性証明を発行する教育機関，医療機関，資格認証企業等が想定される．教育機関が発行する卒業証明書，医療機関が発行する健康診断書，資格認証企業が発行する資格証明書等は，利用者の DID を使用し VC として発行されることを想定している．利用者は，自身の学歴や保有資格，健康状態等を証明する VC を，VP として提供し企業への就職活動等での利用を想定している．

ASFjp が新たに付与した DID には利用者を特定する情報は含まれず，利用者の一定の匿名性が確保されており，一方，DID で識別される利用者の特定・追跡が必要な場合は DID 発行法人への要請により，対応する SSIFjp で付与された DID を特定でき，更にその DID の発行法人への要請により NAFjp-ID を特定でき，NAFjp への要請

により身元情報を入手でき，利用者の特定・追跡性を確保する仕組みを想定している．もちろん，このような利用者の特定・追跡のための DID 発行法人や NAFjp への情報開示要請には合法的手続きが不可欠であることを想定している．

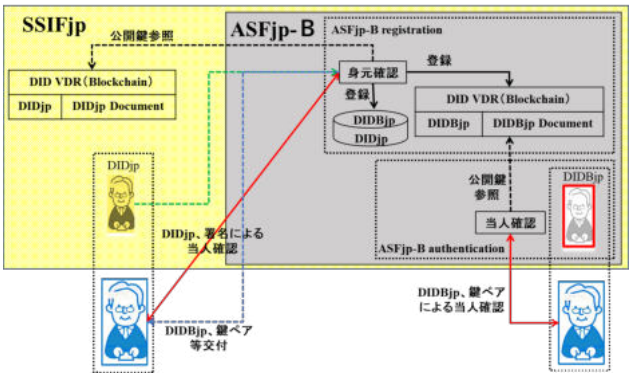

図１１　独自 DID 型 ASFjp（タイプ B）

3.4.3.　独自非 DID 型 ASFjp（タイプ C）

ASFjp は利用を希望する個人の DID，SSIFjp 登録時に付与された DID による本人確認後，更に利用者としての要件を確認後，利用者として登録する．利用者には ASFjp のルールで生成される新たな ID および ASFjp で使用する利用者の当人確認方法で使用する当人確認情報の登録を利用者に求める．このような連携の仕組みにより既存のインターネット上のアプリケーションサービスを，BSI 上で利用可能となることを想定している．

このタイプの ASFjp としては，多くのインターネット上の既存のアプリケーションサービスが対象となりうるが，NIST で規定している当人確認が AAL3 相当の当人確認方法を採用しているアプリケーションサービスを対象とすることを想定している．なお，ASFjp 上で個人情報・プライバシー情報の安全なやり取りを可能とするにはそれぞれ独自の仕組みが必要となることに留意する必要がある．

ASFjp が新たに付与した ID には利用者を特定する情報は含まないようにすることを想定し，利用者の一定の匿名性が確保し，一方，ID で識別される利用者の特定・追跡が必要な場合は ID 発行した ASFjp への要請により，対応する SSIFjp で付与された DID を特定でき，更にその DID の発行法人への要請により NAFjp-ID を特定でき，NAFjp への要請により身元情報を入手でき，利用者の特定・追跡性を確保する仕組みを想定している．もちろん，このような利用者の特定・追跡のための ASFjp，DID 発行法人や NAFjp への情報開示要請には合法的手続きが不可欠であることを想定している．

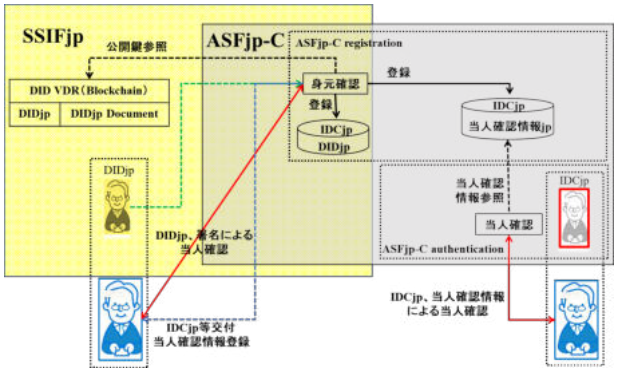

図１２　非 DID 型 ASFjp（タイプ C）

4　おわりに

個人や組織の活動が国を問わずインターネット上へと大きくシフトする中，インターネット上で様々のサービスを提供する組織，利用する個人，サービスが展開される社会の安心・安全を実現するためには，個人・法人の認証や個人（利用者）の匿名性と特定・追跡性の両立の仕組みがますます重要となる．

本稿では，筆者らが提案してきた自己主権型アイデンティティ情報利活用基盤（SSIUF）構想を更に発展させ，組織・個人の確実な認証，利用者個人の匿名性と特定・追跡性の両立が実現可能なブロックチェーンサービス基盤（BSI）構想を提案した．

更に，日本の既存の組織や制度を考慮しつつ，ブロックチェーンサービス基盤（BSI）の日本での構成方法について検討した．今後，アプリケーションサービスのタイプごとに具体的なアプリケーションサービス基盤（BSIjp 上の ASFjp）としての実現方式を検討し，社会実装上・利用上・運用上の課題を整理，克服策等を検討する予定である．

BSI は，日本のみならず各国の安心・安全なインターネット社会の基盤として期待されている．インターネット上のサービスがグローバル化する中，認証基盤 NAF は各国固有の制度・仕組みに依存しながらも，自己主権型アイデンティティ基盤 SSIF 上のアプリケーションサービス基盤 ASF では，サービス提供事業者の信頼性の確認や利用者の匿名性と特定・追跡性の両立を可能とするグローバルな連携の仕組みも重要となろう．BSIjp の具体化にあたっても，グローバルな連携をも視野に入れつつ検討する必要があろう．

日本をはじめ各国でも，個人や組織の様々の活動がインターネット上での活動へ移行しつつあり，社会の安心・安全はインターネット上の安心・安全に強く依存する社会となることが想定される．BSI は，インターネット上のサービスの利用者である個人，サービス提供者である法人の安心・安全な活動基盤と同時に，インターネット社会の安心・安全の維持の仕組みを備えた活動基盤を目指した構想であり，早期の実現を期待したい．

参考文献

[1] 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

[2] 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

[3] 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

[4] 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

[5] 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

[6] 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

[7] “Digital Identity Guidelines - Enrollment and Identity Proofing”. NIST Special Publication 800-63A. 2017. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf

[8] “Digital Identity Guidelines - Authentication and Lifecycle Management”. NIST Special Publication 800-63B. 2017. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

[9] Decentralized Identifiers (DIDs) v1.0 Core architecture, data model, and representations. World Wide Web Consortium. 2021. https://www.w3.org/TR/did-core/

[10] Verifiable Credentials Data Model v1.1. World Wide Web Consortium. 2021. https://www.w3.org/TR/vc-data-model/