一般社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report

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－

才所 敏明

(株)IT 企画 〒158-0083 東京都世田谷区奥沢 6-18-10
https: https://advanced-it.co.jp/
E-mail: toshiaki.saisho@advanced-it.co.jp

あらまし サイバー社会における利用者の安心・安全な活動には利用者の匿名性が重要であるが，社会の安心・安全，公平・公正の維持のためには，不正・不法・不適切な利用者の特定・追跡性もまた重要であるとの認識から，筆者は 2023 年に，利用者の匿名性と特定・追跡性を両立可能な安心・安全なサイバー社会の基盤としてのブロックチェーンサービス基盤（BSI）構想を提案した．

一方，ネット上の様々のサービスでは，利用者の本人確認が重要である．本稿では，ネット経由の本人確認への生体認証の安心・安全な適用を目指した，遠隔生体認証（SSRBA）構想を提案する．SSRBA は，ネット経由の利用者が利用者管理下のシステムにて生体認証を実施し，サービス提供者がその認証結果の信頼性を確認できるクライアント認証型の遠隔生体認証方式である．

本稿では更に，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（BSIwRBA）構想を提案する．BSIwRBA は，公開鍵暗号技術ベースの当人確認の仕組みを内包するブロックチェーンサービス基盤（BSI）へ，SSRBA 構想に基づく遠隔生体認証機能の組込みを目指した構想である．

キーワード 遠隔認証，生体認証，遠隔生体認証，ブロックチェーンサービス基盤，SSRBA，BioRAIN，ACBio，BSI，BSIwRBA，FIDO，NIST

Blockchain Service Infrastructure with Remote Biometric Authentication

Toshiaki SAISHO

Advanced IT Corporation 6-18-10 Okusawa, Setagaya-ku, Tokyo, 158-0083 Japan
https: https://advanced-it.co.jp/
E-mail: toshiaki.saisho@advanced-it.co.jp

Abstract While anonymity of users is important for safe and secure activities in cyber society, the identifiability and trackability of fraudulent, illegal, and inappropriate users is also important for maintaining social safety and security, fairness, and justice. Based on this recognition, the author proposed the Blockchain Service Infrastructure (BSI) concept as a foundation for a safe and secure cyber society in 2023 that can achieve both anonymity and identifiability and trackability of users.

On the other hand, identity verification of users is important for various online services. In this paper, we propose the remote biometric authentication (SSRBA) concept, which aims to safely and securely apply biometric authentication to identity verification over the Internet. SSRBA is a client-authenticated remote biometric authentication method in which users over the Internet perform biometric authentication in a system under the user's control, and the service provider can confirm the reliability of the authentication results received.

In this paper, we further propose the Blockchain Service Infrastructure with Remote Biometric Authentication (BSIwRBA) concept. BSIwRBA is a concept that aims to incorporate remote biometric authentication functions based on the SSRBA concept into the Blockchain Service Infrastructure (BSI), which includes a mechanism for identity verification based on public key cryptography technology.

Keywords Remote Authentication，Biometric Authentication，Remote Biometric Authentication ，Blockchain Service Infrastructure，SSRBA，BioRAIN，ACBio，BSI，BSIwRBA，FIDO，NIST

1. まえがき

ネット利用の増大，サイバー社会の拡大はとどまるところを知らず，サイバー・フィジカル社会におけるサイバー社会の役割はますます大きく，その責任もますます重大となりつつある．サイバー社会でも個人情報やプライバシー情報の利活用が増大する中，利用者

の匿名性はますます重要となり，一方では，社会の安心・安全，公平・公正の維持には，不正・不法・不適切な利用者の特定・追跡性もまた重要である．利用者の匿名性と特定・追跡性は，一見相反する機能ではあるが，サイバー・フィジカル社会の健全な発展には，その両立が不可欠である．

筆者は，2018 年頃よりサイバー社会における利用者の匿名性と特定・追跡性の両立に関する研究に着手，2023 年には利用者の匿名性と特定・追跡性を両立可能なサイバー社会の基盤としてのブロックチェーンサービス基盤（BSI：Blockchain Service Infrastructure）構想を提案している．BSI は，W3C で標準化が進められている DID/VC/VP をベースに，更に筆者が別途提案中の各国の認証基盤（NAF：National Authentication Framework）構想と連携させた構想である（[1]～[11]）．概要を第 2 章にて報告する．

遠隔生体認証については，2000 年頃より遠隔地で実施された生体認証の信頼性を確認できる仕組み「本人確認保証フレームワーク」の研究に着手，2002 年に BioRAIN（Biometric Result Assurance Infrastructure）という名称で構想を提案した．2004 年には，BioRAIN の詳細仕様を規定し ISO/IEC SC27 WG2 へ国際標準化を提案，2009 年に国際規格 ISO/IEC 24761：2009（名称：Authentication context for biometrics （ACBio））として承認された[1] ([12]～[14]). 今回提案する安心・安全な遠隔生体認証 SSRBA（Secure and Safe Remote Biometric Authentication）は，約四半世紀前に考案した構想 BioRAIN/ACBio の目標を，様変わりした IT 利用環境を前提にあらためて実現方式を考案した構想である．概要を第 3 章にて報告する．

本稿で提案する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 BSIwRBA（Blockchain Service Infrastructure with Remote Biometric Authentication）は，公開鍵暗号技術ベースの当人確認の仕組みを内包する BSI へ生体認証による当人確認の仕組み，SSRBA 構想に基づく遠隔生体認証機能の組込みを目指した構想である．BSIwRBA の構成，遠隔からの利用者の登録方法，遠隔からの利用者の生体情報を利用した認証方法について，第 4 章にて報告し，更に BSIwRBA の今後の検討課題等について，第 5 章にて考察する．

2. ブロックチェーンサービス基盤（BSI）

BSI は，個人や組織の認証基盤（NAF），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（ASF：Application Service Framework）により構成される（図 1）．

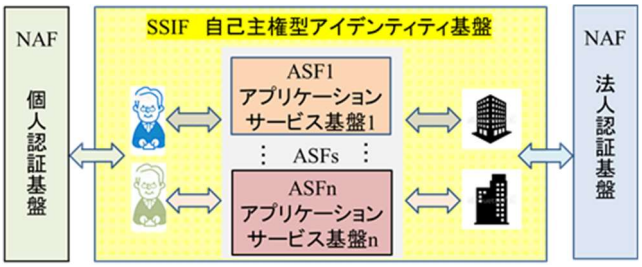


図 1 BSI 基本構成

BSI 上では，多くのサービス提供者（法人）が様々のサービスを展開し，多くの利用者（個人・法人）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 を構成する各国の認証基盤 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）と共に，公開鍵暗号の鍵ペアを付与することを想定している．日本の場合は．個人・法人番号制度の利用を想定しており，NAF-ID は，個人・法人番号に相当する．

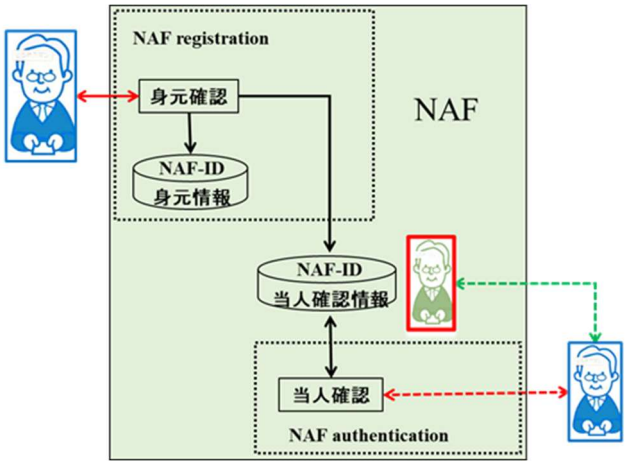
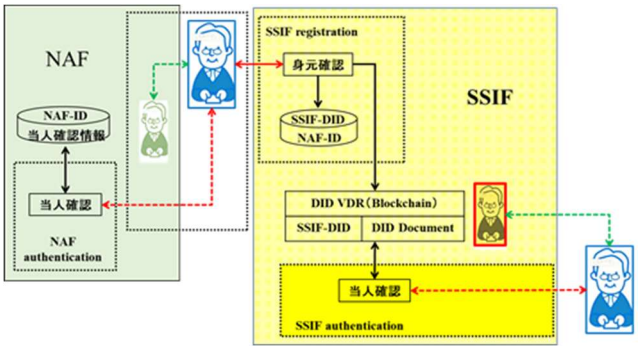


図 2　NAF における利用者の登録・認証

自己主権型アイデンティティ基盤 SSIF は，NAF にて身元確認済であることを確認された個人・法人に対し識別コード SSIF-DID（W3C で標準化が進められている DID（Decentralized Identifier）([16])）を付与すると共に，NAF-ID と SSIF-DID の対応を管理する．



[1] 国際規格 ISO/IEC 24761：2009 は，ISO/IEC 24761：2019 に改定されている

図３　SSIF における利用者の登録・認証

アプリケーションサービス基盤 ASF は，SSIF に登録された利用者（NAF にて身元確認済の利用者）であることを確認した個人･法人に対し，新たな DID, ASF-DID を付与すると共に，SSIF-DID と ASF-DID の対応を管理する．

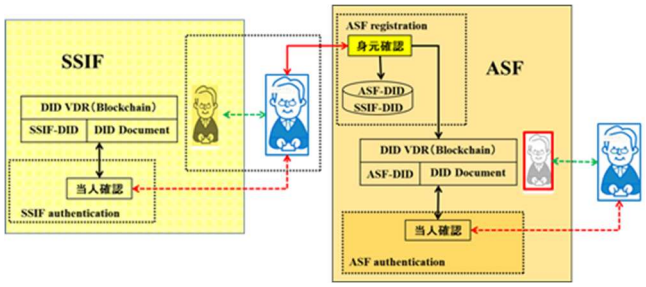


図４　ASF における利用者の登録・認証

SSIF，ASF それぞれのサービス空間では，利用者の匿名性維持のため，利用者には新たな DID が識別コードとして付与される．また，それぞれの SSIF, ASF は，身元確認に使用した SSIF/ASF の利用者識別コードである NAF-ID/SSIF-DID と新たに付与した DID との対応表を安全に管理するものとし，不正・不法・不適切な利用が発見された場合の利用者の特定・追跡性を確保している．

BSI は，W3C で標準化が進められている DID/VC/VP をベースに，確実な本人確認機能を実現する NAF（National Authentication Framework）構想を組み込み，更に利用者の匿名性と特定・追跡性の両立の仕組みを組み込んだ，安心・安全なサイバー社会の基盤を目指した構想である（[16]，[17]）．

3. 安心・安全な遠隔生体認証（SSRBA）

遠隔生体認証は，サービス提供者である認証者がネット経由で被認証者である利用者の生体情報により認証する方式である．

遠隔生体認証方式には，利用者の手元で採取した生体情報（サンプル）をサービス提供者へ送付し，確実な本人確認の元に採取・登録されている利用者の生体情報（テンプレート）との照合処理をサービス提供者のシステムで行うサーバ認証方式と，サービス提供者の管理下に無い，利用者の手元の，利用者管理下の生体認証システムにて照合処理までを行うクライアント認証方式に分類される．

本稿で提案する SSRBA は，クライアント認証方式であり，生体情報をサービス提供者へ送付せず（利用者の安心），利用者の手元で実施された生体認証結果の信頼性をサービス提供者が確認できる（サービス提供者の安全）仕組みの実現による，安心・安全な遠隔生体認証を目指している．

3.1. SSRBA 構想概要

約四世紀前に考案した BioRAIN/ACBio では，パーソナルコンピュータ（PC）での利用を想定しており，生体情報採取モジュール（センサー），特徴抽出モジュール，あらかじめ登録されている利用者のテンプレートとの照合モジュール，を担当する各モジュールを組み合わせ生体認証システムが構成されることを想定し，モジュールごとに機能・性能・セキュリティの信頼できる第三者機関の評価結果を利用する方式を採用したが，2011 年には指紋認証や顔認証によるロック解除機能付きスマートフォン出現し，その後，iOS 系，Android 系のスマートフォンの開発ベンダの技術改良・製品投入により，現在ではスマートフォンには顔または指紋または両方の生体認証プロセス全体のモジュールが統合され搭載される時代となった．そこで，SSRBA 構想の検討にあたり，利用者の手元で生体認証プロセスのすべてが実施される生体認証器の存在を前提とし，生体認証器単位で信頼できる第三者機関による機能・性能・セキュリティの評価結果が得られることを想定した．図５に SSRBA のシステム構成概要を示している．

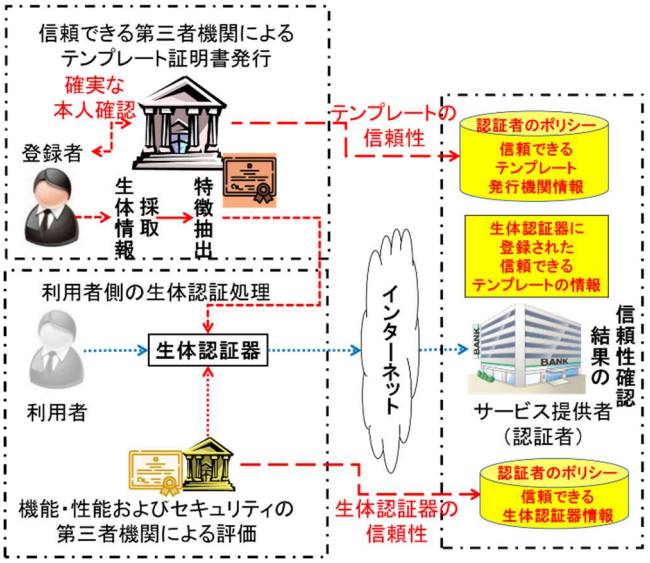


図５　SSRBA 構成概要

サービス提供者はまず，許容できる生体認証器の情報を信頼できる第三者機関の評価をベースに選定・管理しておく．その情報を利用し，利用者が指定してきた生体認証器の使用の可否を判断する．

テンプレートの方も，認証者はまず，信頼できるテンプレート証明書発行機関を選定・管理しておき，利用者が登録時に指定してきたテンプレートハッシュ証明書の発行機関の確認により，そのテンプレートの使

用可能性を判断し，可能な場合は認証時に使用するテンプレートの同一性の確認に使用される生体認証検証情報等を保管する．

利用者が生体認証を使用しサービス提供を要求する時には，生体認証に使用したテンプレートハッシュ値等から計算される実施生体認証情報等を認証者へ送付し，サービス提供者は利用者の生体認証に使用されたテンプレートが登録時に指定されたテンプレートと同一かどうかを確認する．

以上の仕組みにより，サービス提供者が，生体認証器の信頼性，使用されたテンプレートの信頼性を確認でき，結果として利用者側で実施された遠隔生体認証の結果（照合結果）の信頼性を確認できることを目指している．

4. 遠隔生体認証機能組込みブロックチェーンサービス基盤（BSIwRBA）

個人や組織の認証基盤（NAF），自己主権型のアイデンティティ基盤（SSIF），および様々のアプリケーションサービス基盤（AS）により構成するブロックチェーンサービス基盤（BSI），DID/VC/VP 技術/公開鍵暗号技術をベースにした利用者の確実な当人確認および利用者の匿名性と特定・追跡性の両立が可能な様々のアプリケーションのサービス基盤となることを目指したブロックチェーンサース基盤（BSI）へ，安心・安全な遠隔生体認証（SSRBA）構想に基づく，より確実な当人確認が可能な遠隔生体認証の機能の組込みを目指したのが，遠隔生体認証機能付きブロックチェーンサービス基盤（BSIwRBA：Blockchain Service Infrastructure with Remote Biometric Authentication）構想である．

BSIwRBA は BSI 上で提供されるサービスが生体認証による本人確認を求める場合に，SSRBA に基づく遠隔生体認証の仕組みが利用されることを想定している．

4.1. BSIwRBA 構成

BSI への遠隔生体認証機能の付加においては，NAF，SSIF，ASF は生体認証機能のための新たな情報を維持・管理する必要があり，図 6 の赤枠・赤字にて示している．

本稿で記載する BSIwRBA では，NAF 運用組織が，面前での確実な本人確認の上，生体情報を採取し，生体特徴を抽出し，テンプレート情報を生成，National Id Card へ登録する方式，を想定しているが，別の組織が同様の処理を担当することや，生体認証処理のために利用者が管理すべき情報を別の耐タンパー性が確保されたデバイスへ格納し利用することも可能である．

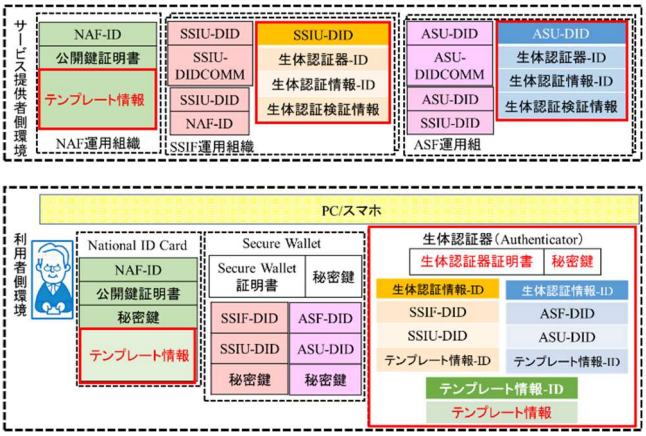


図 6　BSIwRBA 構成概要

BSIwRBA の利用者は，サービスの利用のために，それぞれ耐タンパー性が確保された National ID Card，Secure Wallet，生体認証器の利用を前提としている．Secure Wallet および生体認証器は，利用者のスマホや PC に内蔵される場合や外付けの場合も想定し，更に，Secure Wallet および生体認証器は複数利用されることも想定している．

生体認証器は，内蔵する生体認証の機能・性能，および内蔵する処理やデータの保護のためのセキュリティに関する信頼できる第三者機関の評価を受けていることを想定し，サービス提供者はその評価結果（生体認証器モデル評価結果証明書）を入手でき，利用者が使用する生体認証器の信頼性を確認できることを想定している．生体認証器証明書の構成要素は，{生体認証器-ID，生体認証器の公開鍵，製造事業者-ID，生体認証器モデル-ID，製造事業者の署名} 等を想定している．

テンプレート情報は，信頼できる第三者機関による利用者の確実な本人確認の元，採取した生体情報から発行したテンプレート証明書から構成され，テンプレート証明書の構成は，{テンプレート証明書-ID，発行機関の NAF-ID，有効期限，生体所有者の NAF-ID，生体所有者の公開鍵，対象の生体部位，テンプレート，テンプレートのハッシュ値，テンプレートハッシュ証明書としての発行機関の署名，テンプレート証明書としての発行機関の署名} 等を想定している．サービス提供者はテンプレートハッシュ証明書により，利用者が生体認証に使用するテンプレートの信頼性を確認できることを想定している．

4.2. BSIwRBA への遠隔生体認証利用登録

図 7 に，アプリケーションサービス（ASF）を例に，遠隔生体認証を利用する場合の登録手順を示している．

NAF 運用組織が，本人を面前で確認の上で生体情報を採取（①），その生体情報から生体特徴を抽出し，テ

ンプレート証明書を生成し National ID Card 内に登録する（②）ことを想定しており，利用者はテンプレート情報が格納された National ID Card を入手するものとする．

次に，利用者は，その National ID Card を利用し，利用者側環境を構成する生体認証器へ，テンプレート情報を登録する（③）

その後，利用者が利用登録を希望するアプリケーションサービス（ASF）が遠隔生体認証を求める場合は，まず利用者は生体認証器証明書およびテンプレートハッシュ証明書をアプリケーションサービスへ送付し，アプリケーションサービス側での生体認証器およびテンプレートの使用可能性の確認を求める（④，⑤）．

生体認証器およびテンプレートが共に使用可能な場合，利用者は遠隔生体認証のための登録手続きを行う（④，⑤，⑥，⑦）．

利用者側では，生体認証器内にアプリケーションサービスごと（ASF-ID）の利用者識別コード（ASU-ID）ごとに使用するテンプレート情報識別コード（テンプレート情報-ID）を，生体認証情報識別コード（生体認証情報-ID）を付与し登録する．

サービス提供者側では，利用者識別コード（ASU-DID）ごとに，使用する生体認証器識別コード（生体認証器-ID），実施する生体認証を示す生体認証情報識別コード（生体認証情報-ID），および利用者の当人確認時に，登録時に確認した生体認証器およびテンプレートが使用されたかを確認するための生体認証検証情報を登録する．（注：生体認証検証情報は，Hash｛ASF-DID；ASU-DID；生体認証器-ID；生体認証情報-ID；テンプレートハッシュ｝で計算することを想定している．）

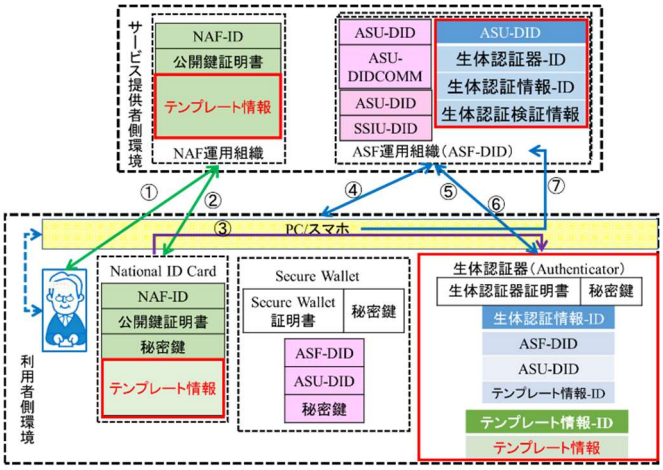


図７　遠隔生体認証利用登録手順

4.3. BSIwRBA での遠隔生体認証

図８に，アプリケーションサービス（ASF-DID）を例に，遠隔生体認証による利用者認証（当人確認）手順を示している．

利用者が，遠隔生体認証を求めるアプリケーションサービス（ASF-DID）の利用を要求すると（①），アプリケーションサービスは，その利用者（ASU-DID）と対応付けられ管理されている，生体認証器-ID，生体認証情報-ID を，利用者側に送信し遠隔生体認証を要求する（②）．

利用者側では，生体認証器を利用した生体認証が実施され，その照合結果と，実施生体認証情報をアプリケーションサービスへ送信する．（注：実施生体認証情報は，実施生体認証情報＝Hash｛ASF-DID;ASU-DID;生体認証器-ID;生体認証情報-ID;使用したテンプレートのハッシュ値｝で計算することを想定している．）

アプリケーションサービスは，その実施生体認証情報と，利用者（ASU-DID）に紐づけられ管理されている生体認証検証情報との一致の確認により，利用登録時に妥当性を確認した生体認証器およびテンプレートが使用されたことを確認し，その上で，照合結果の諾否を判断することを想定している．

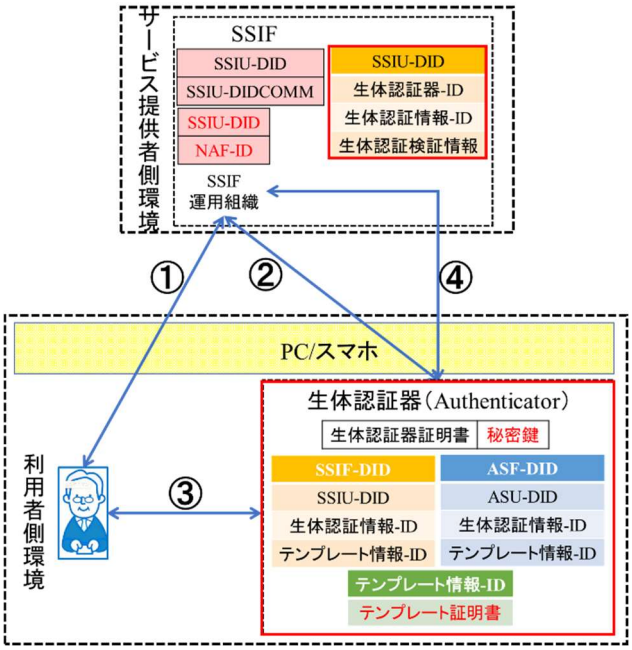


図８　遠隔生体認証による利用者認証手順

4.4. BSIwRBA が提供する主要な機能

(1)BSI が提供する機能

①NAF（各国の個人登録制度等）に期待する機能：

＊利用者の確実な身元確認，利用者への NAF-ID および鍵ペアの付与，個人識別カードの発行

②SSIF/ASF が提供する機能：

＊NAF/SSIF を利用した利用者の身元確認，当人確認情報としての DID および鍵ペアの付与

＊DID および VDR による利用者の本人確認，証明書の発行機関・発行内容の真正性確認（VC)，受信データの送信者・送信内容の真正性確認（VP）

＊利用者の特定・追跡性確保のための新旧 ID/DID 対応表の安全な維持・管理

(2)SSRBA が提供する機能

①NAF に追加で期待する機能：

＊利用者の確実な身元確認の元，テンプレート証明書の発行，個人識別カードへの格納

②生体認証器に期待する機能：

＊製造事業者が発行した生体認証器証明書の格納および生体認証器の信頼性確認のためのサービス提供者への生体認証器証明書の提供

＊生体情報証明書発行機関が発行したテンプレート証明書の格納および利用者のテンプレートの信頼性確認のためのサービス提供者へのテンプレートハッシュ証明書の提供

＊利用者のその時点の生体情報（サンプル）採取と，そのサンプルとテンプレートとの照合処理

＊照合に使用したテンプレートのハッシュ値等から実施生体認証情報を算出し，照合処理結果と共にサービス提供者へ提供

③SSIF/ASF に期待する機能

＊遠隔生体認証のための登録情報の安全な維持・管理

4.5. BSIwRBA 利用者の主要なリスク

(1)サービス登録時に提供する生体認証器証明書に起因するリスク

生体認証器証明書には生体認証器固有の情報（生体認証器-ID, 生体認証器の公開鍵)が含まれている．利用者が直接特定されることは無いが，複数のサービス提供者からの情報漏洩により利用者の特定につながる恐れがある．当該リスク軽減策は今後の検討課題．

(2)サービス登録時に提供するテンプレートハッシュ証明書に起因するリスク

テンプレートハッシュ証明書には，証明書固有の情報｛テンプレート証明書-ID, テンプレートハッシュ｝が含まれている．利用者が直接特定されることは無いが，複数のサービス提供者からの情報漏洩により利用者の特定につながる恐れがある．当該リスク軽減策は今後の検討課題．なお，テンプレートハッシュからテンプレートの導出は不可能で，個人識別符号の漏洩のリスクは無い．

(3)サービス利用時に提供する実施生体認証情報に起因するリスク

実施生体認証情報は，｛SSIF-DID, SSIU-DID, 生体認証器-ID, 生体認証情報-ID および使用したテンプレートのハッシュ値｝等を連結した情報のハッシュ値を想定している．最終的にはハッシュ値へ集約するため，実施生体認証情報の算出に使用される利用者固有の識別情報，利用者所有デバイスの固有の識別情報が導出されるリスクは無い．

5. 考察

本報告では，提案中の BSI 構想へ，今回あらためて構成した SSRBA 構想を組み込んだ，BSIwRBA 構想を提案した．いずれも構想レベルで，実装仕様の詳細検討は今後であるが，本章では BSIwRBA の構成や基本的な仕組みについて考察する．

(1) 利用者の手元の生体認証環境について

①耐タンパーなデバイス/モジュールである Secure Wallet と生体認証器の機能・役割分担

本稿では, BSI への SSRBA 構想の組込み時の追加機能を明確に示すため，BSI 使用時の利用者の情報保護のための Secure Wallet と，遠隔生体認証の情報や照合処理プロセスの保護のための生体認証器を分離し，それぞれが独立して機能することを想定している．

実際には，Secure Wallet と生体認証器の統合も想定され，また Secure Wallet でのテンプレート情報の管理等，Secure Wallet と生体認証器の異なる役割分担も想定される．

(2)利用者の生体情報の取扱いについて

①テンプレートの National ID Card から生体認証器への登録の是非

本稿では，生体認証に使用するテンプレートを利用者の生体認証器へ登録し，遠隔生体認証処理時には National ID Card は不要としている．これは利便性を考慮したものであるが，National ID Card に格納されているテンプレートを他のデバイスへも格納することにより，個人情報（個人識別符号）の漏洩等のリスクも増大する．

BSIwRBA では，National ID Card を保有する利用者が，遠隔生体認証時は National ID Card を使用することを前提とした仕組みも想定している．

②テンプレートおよびテンプレートハッシュを含むテンプレート証明書の利用の是非

テンプレート証明書は，その一部の項目を削除することにより，テンプレートハッシュ証明書を生成できる構成としている．

代替案としては，単純にテンプレート証明書とテンプレートハッシュ証明書を個々に発行・管理する方式や，部分開示可能な署名技術の利用によりテンプレートハッシュ証明書を生成する方式も

想定される．いずれの方式も BSIwRBA の機能実現には影響を与えず，実装環境に応じ選択すればよい．

(3)生体認証の安全性・信頼性の生体認証器への強い依存について

生体認証を実施する生体認証器は耐タンパーなデバイス/モジュールであり，信頼性が確認されたテンプレートが使用されること，信頼性が確認された生体認証器で採取されたサンプルとの照合処理が実施されることが，一定レベル保証されているが，現在の BSIwRBA の安全性・信頼性はこの生体認証器の安全性・信頼性に強く依存している．

生体認証器の安全性・信頼性，その持続性については，何らかの対策が必要であり，Secure Wallet も同様である．リモート検査・監査や認証の仕組みや制度，内蔵するソフトウェアのリモート更新等の仕組みが必要となろう．この問題は，BSIwRBA や SSRBA 固有の問題ではなく，様々のサービス事業者による利用者情報の集中管理型の社会から，分散管理型・自己主権型の個人による情報管理型の社会への移行が想定されており，膨大となることが想定される個人の情報の，管理・保護・利活用の仕組みの研究開発が重要となろう．

今後，関連する研究開発の動向を把握しつつ，BSIwRBA および SSRBA における Secure Wallet や生体認証器の安全性・信頼性維持のための仕組みを検討したい．

6. おわりに

DID/VC/VP 技術/公開鍵暗号技術をベースにした利用者の確実な当人確認および利用者の匿名性と特定・追跡性の両立が可能な様々のアプリケーションのサービス基盤となることを目指したブロックチェーンサース基盤（BSI）へ，安心・安全な遠隔生体認証（SSRBA）構想に基づく，より確実な当人確認が可能な遠隔生体認証の機能の組込みを目指したのが，本稿で提案した遠隔生体認証機能付きブロックチェーンサービス基盤（BSIwRBA：Blockchain Service Infrastructure with Remote Biometric Authentication）構想である．

電子的な本人確認に関する各国のガイドラインのベースとして利用されている米国 NIST 発行の SP800-63“Digital Identity Guidelines”の改定第 4 版が昨年 12 月に発行された（[15]）．本ガイドラインでは，FIDO と同様，生体認証は多要素認証の一部，暗号認証器のアクティベーション・ファクターとして使用されることが想定されている（[18]）．プレゼンテーション攻撃（[19]，[20]）等，生体認証システムへの様々の攻撃に対する防御・検知およびその評価技術が成熟していないという認識から，生体認証を単独の認証方式としてガイドラインに掲載されていない．そもそも NIST の規格やガイドラインは，連邦政府機関に対し情報セキュリティを強化することを義務付ける，その具体策を示すために開発されるもので，単独の認証方式としての生体認証も検討されているようであるが，時期尚早との判断であろう．現在，第 4 版の改定が進められているが，生体認証の扱いには変更が無さそうである．

しかし，遠隔生体認証技術の社会実装が現時点で時期尚早とはいえ，サイバー・フィジカル社会の進展，その中でのサイバー社会の役割の増大，それに応じたサイバー社会の責任・セキュリティ対策の重要性が増すのは必至である．遠隔の利用者の確実な本人確認はサイバー社会の最重要セキュリティ対策の一つであり近い将来の社会実装を目指し遠隔生体認証技術の研究開発は必要であろう．

サイバー・フィジカル社会の健全な発展のためには，サイバー社会のセキュリティを強化し，サイバー社会での無責任な利用者の多さ，サイバー社会の犯罪者・攻撃者優位の現状を改善する必要があり，そのための重要な対策の一つが，サイバー社会に参加する利用者の確実な本人確認と，様々な活動における利用者の匿名性と特定・追跡性の両立，であろう．

生体認証の本格的な活用によるサイバー社会におけるより確実な本人確認の実現と，利用者のサイバー社会での安心･安全の活動のための匿名性および不正･不法・不適切な活動を防止・抑止するための利用者の特定・追跡性の両立の実現を目指したのが，遠隔生体認証機能付きブロックチェーンサービス基盤（BSIwRBA：Blockchain Service Infrastructure with Remote Biometric Authentication）構想である．

今後，構想を構成する仕組みの具体的仕様検討，および関連構想・システムとの関係の精査等を行い，BSIwRBA の具体化・改良・拡張を目指す予定である．

文　献

[1] 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.

[2] 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.

[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.

[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”. 2022 年暗号と情報セキュリティシンポジューム（SCIS2022）. 2022.

[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（CSS2021）. 2021.

[6] 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.

[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.

[8] 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.

[9] 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（CSS2020）. 2020.

[10] 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（CSS2019）. 2019.

[11] 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.

[12] “Information technology -- Security techniques - Authentication context for biometrics ”, ISO/IEC 24761:2009.

[13] 池田竜朗,森尻智昭,才所敏明, “本人確認環境認証方式の提案”, コンピュータセキュリティシンポジューム（CSS2002）, 2002.

[14] 池田竜朗, 大岸伸之, 藤澤要, 森尻智昭, 才所敏明, “本人確認保証フレームワーク(BRAIN)の研究”, コンピュータセキュリティシンポジューム（CSS2001）, 2001.

[15] “ Digital Identity Guidelines ”, NIST Special Publication 800-63. 2023.

[16] Decentralized Identifiers (DIDs) v1.0 Core architecture, data model, and representations. World Wide Web Consortium. 2021.

[17] Verifiable Credentials Data Model. World Wide Web Consortium. 2024. .

[18] FIDO Biometrics Requirements, FIDO Alliance, 2024.

[19] Sani M. Abdullahi, Shuifa Sun, Beng Wang, Ning Wei, Hongxia Wang,“Biometric Template Attacks and Recent Protection Mechanisms: A Survey”, 2023.

[20] 宇根正志, “スマートフォンによる顔認証のセキュリティ： ディープフェイクによる脅威と対策”, 日本銀行金融研究所, 2024.