ISEC

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

2024年11月14日

（株）IT企画　才所敏明
(株)ZenmuTech
中央大学研究開発機構
toshiaki.saisho@advanced-it.co.jp
http://www.advanced-it.co.jp

安心・安全なサイバー社会の基盤を目指して

①BSI（Blockchain Service Infrastructure）　＜SCIS2023にて提案＞
　利用者の確実な本人確認機能、
　および、利用者の安心・安全な活動のために必要な利用者の匿名性、
　　社会の安心・安全，公平・公正の維持のために必要な
　　不正・不法・不適切な利用者の特定・追跡性、の両立機能を提供
➔BSIは、様々のサービスから構成されるサイバー社会の、安心・安全を目指し、
　サービスが提供される基盤となることを想定し、提案中の構想

②SSRBA構想　＜今回概要提案＞
　サイバー社会の利用者の確実な特定・追跡に必要な
　　遠隔地の利用者の生体認証による、より確実な本人確認機能、
　利用者の手元で生体認証を実施し、
　　その結果の信頼性をサービス提供者が確認できる仕組み
➔SSRBAは、利用者の生体情報のサービス提供者への提供の回避を目指した
　遠隔生体認証構想

③BSIwRBA構想　＜今回概要提案＞
　BSI構想で想定する公開鍵暗号技術による本人確認に加え、
　　SSRBA構想に基づく遠隔生体認証機能の提供
➔BSIwRBAは、BSIへ本人確認機能を生体認証技術により強化した
　　より安心・安全なサイバー社会の基盤を目指す構想

●2分

①BSI

 3

BSI構想構築経緯

(1)2018年より、本人確認基盤に関する研究に着手

＊2019年　NAF（National Authentication Framework）構想発表

＊2020年　GAF（Global Authentication Framework）構想発表

(2)2020年より、自己主権型アイデンティティ情報制御に関する研究に着手

＊2022年　SSIUF（Self Sovereign Identity Utilization Framework）構想発表

＊2022年　利用者の匿名性と特定・追跡性の両立の必要性提案

(3)2022年より、ブロックチェーンサービス基盤に関する研究に着手

＊2022年　BSI（NAF＋SSIF＋ASF）構想発表

＊2023年　BSI上でのメタバース構成方法の提案

＊2024年　BSI上での学修歴利活用基盤（SSARUF）の提案

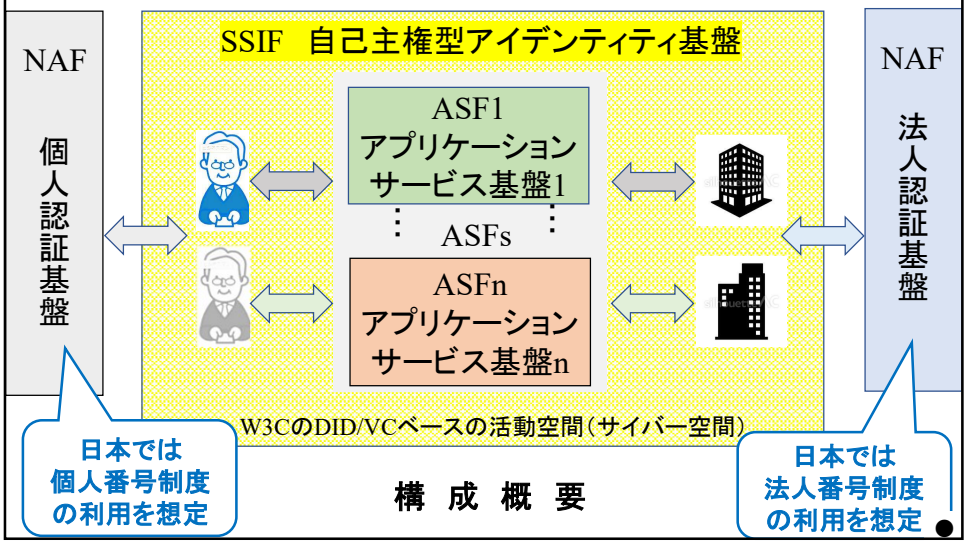
●

①BSI

 4

ブロックチェーンサービス基盤BSI

（Blockchain Service Infrastructure）



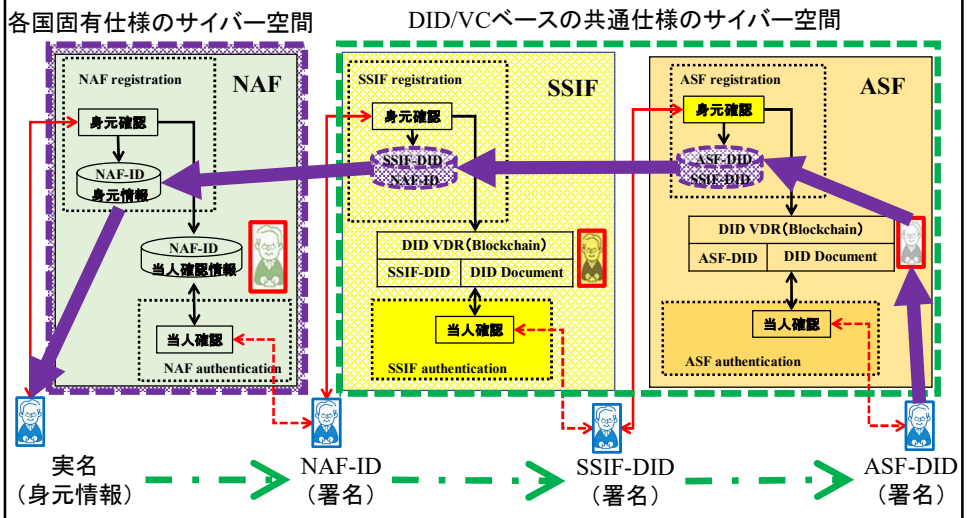
構　成　概　要

●

①BSI

 5

ブロックチェーンサービス基盤における
利用者の匿名性と特定・追跡性の両立



●7分

②SSRBA

 6

安心・安全な遠隔生体認証（SSRBA）
（Secure and Safe Remote Biometric Authentication）

遠隔生体認証：
　サービス提供者が利用者を、
　　ネット経由、利用者の生体情報により認証する方式

本稿で提案するSSRBA：
　　生体情報（個人識別符号）を含む個人情報を
　　サービス提供者へ提供せず（利用者の安心・安全）、
　　利用者管理下のシステムにて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（認証者の安心・安全）、
　安心・安全な遠隔生体認証方式（クライアント認証方式）

●

②SSRBA

SSRBA構想構築経緯

(1)2000年頃より、遠隔地での生体認証結果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）構想を提案

(2)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（ISO/IEC 24761:2019に改定されている）

＜IT利用環境の変化＞

2003年　指紋認証機能付き携帯電話

2011年　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

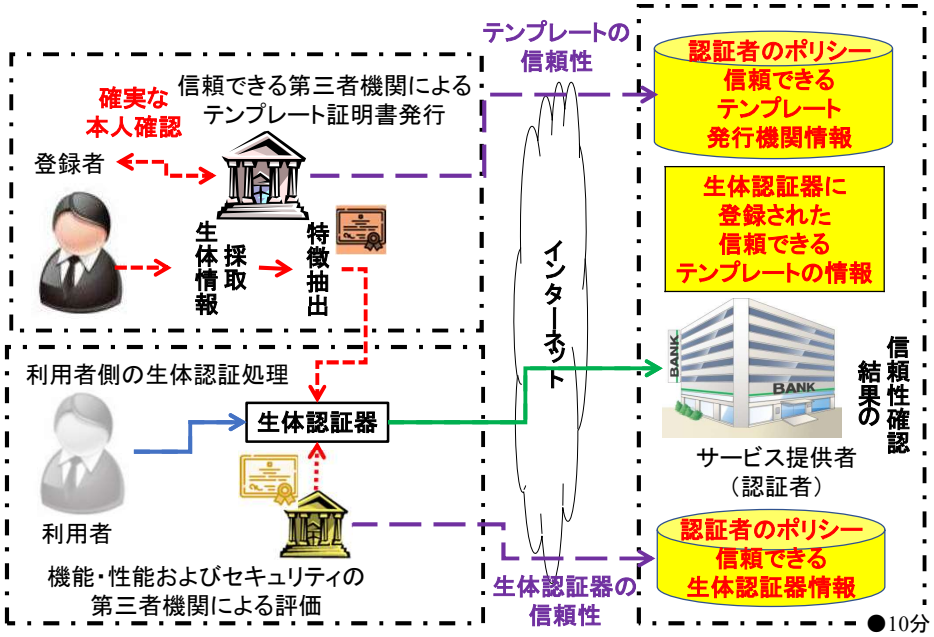
現在のスマートフォンは、指紋・顔認証機能搭載

(3)今回提案するSSRBAは，約四半世紀前に考案したBioRAIN/ACBio同様に、
クライアント認証方式を採用し、
様変わりしたIT利用環境を前提にあらためて考案した構想

●

②SSRBA

SSRBA構想



●10分

③BSIwRBA

 9

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）

Blockchain Service Infrastructure with Remote Biometric Authentication

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

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を目指した構想

遠隔生体認証（SSRBA）：安心・安全な遠隔生体認証方式

生体情報を含む個人情報を認証者に提供せず（利用者の安心・安全）

生体認証結果の信頼性を認証者が確認できる（認証者の安心・安全）

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）：

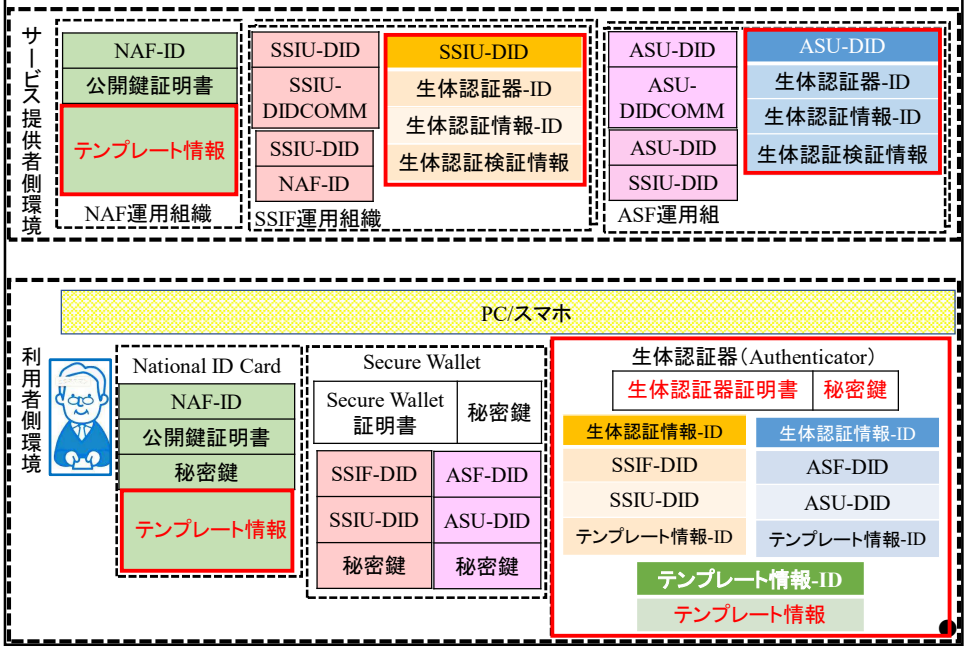
より確実な当人確認が可能な遠隔生体認証の機能の

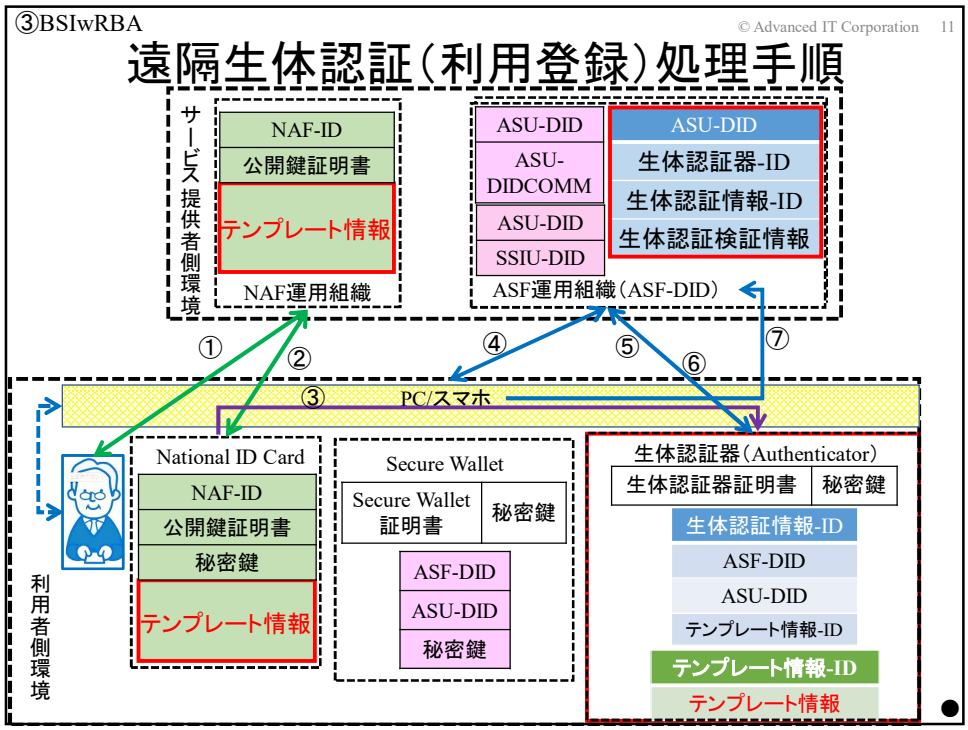
BSIへの組込みを目指した構想

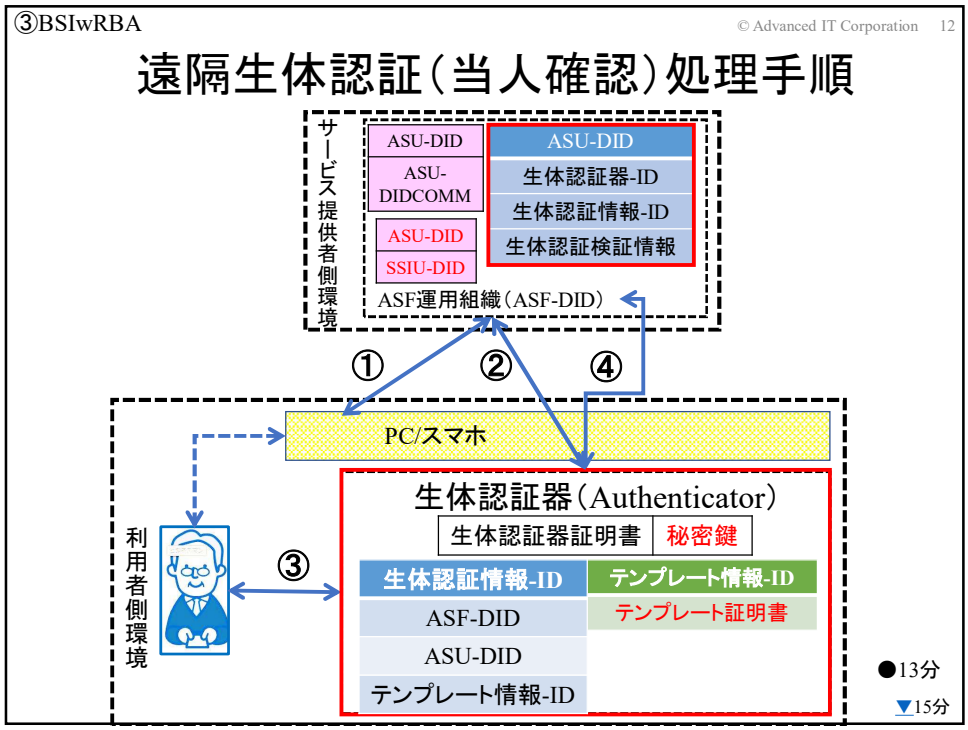
③BSIwRBA構

 10

BSIwRBAシステム構成




③BSIwRBA
© Advanced IT Corporation 11
遠隔生体認証（利用登録）処理手順
サービス提供者側環境
NAF-ID
公開鍵証明書
テンプレート情報
NAF運用組織
ASU-DID
ASU-DIDCOMM
ASU-DID
SSIU-DID
ASU-DID
生体認証器-ID
生体認証情報-ID
生体認証検証情報
ASF運用組織（ASF-DID）
①
②
④
⑤
⑥
⑦
③
PC/スマホ
利用者側環境
National ID Card
NAF-ID
公開鍵証明書
秘密鍵
テンプレート情報
Secure Wallet
Secure Wallet 証明書
秘密鍵
ASF-DID
ASU-DID
秘密鍵
生体認証器（Authenticator）
生体認証器証明書
秘密鍵
生体認証情報-ID
ASF-DID
ASU-DID
テンプレート情報-ID
テンプレート情報-ID
テンプレート情報


③BSIwRBA
© Advanced IT Corporation 12
遠隔生体認証（当人確認）処理手順
サービス提供者側環境
ASU-DID
ASU-DIDCOMM
ASU-DID
SSIU-DID
ASU-DID
生体認証器-ID
生体認証情報-ID
生体認証検証情報
ASF運用組織（ASF-DID）
①
②
④
PC/スマホ
利用者側環境
③
生体認証器（Authenticator）
生体認証器証明書
秘密鍵
生体認証情報-ID
テンプレート情報-ID
ASF-DID
テンプレート証明書
ASU-DID
テンプレート情報-ID
●13分
▼15分

BSIwRBAが提供する機能

(1)BSIが利用者へ提供する機能

①NAF（各国の個人登録制度等）が提供する機能：
＊利用者の確実な身元確認，
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，
利用者の匿名化のための新たなDIDの付与、
当人確認情報としての鍵ペアの付与
＊DIDおよびVDRによる利用者の当人確認，
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が利用者へ提供する機能

①NAFが提供する機能：
＊利用者の確実な本人確認の元，
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（NAF）が発行したテンプレート証明書の格納
および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
および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の算出
照合処理結果と共に実施生体認証情報の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

③BSIwRBA

BSIwRBA利用者のリスク

(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
生体認証器証明書内の生体認証器固有の情報の漏洩・悪用
（生体認証器-ID，生体認証器の公開鍵）
➔複数のサービス提供者からの漏洩により、利用者推定のリスク
(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内の証明書固有の情報の漏洩・悪用のリスク
（テンプレート証明書-ID，テンプレートハッシュ）
➔複数のサービス提供者からの漏洩により、利用者推定のリスク
(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，関連する情報のハッシュとして算出、
（{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}のハッシュ値）
利用者、生体認証器、テンプレートの固有の情報は含まれ無い
➔利用者推定のリスクは無い

④考察

BSIwRBAの考察

(1)利用者の手元の生体認証環境について

①Secure Walletと生体認証器の役割分担のバリエーション
＊Secure Walletと生体認証器の統合
＊Secure Walletと生体認証器の異なる役割分担
Secure Walletでテンプレート情報の管理等
➔BSIwRBAの機能・セキュリティの若干の修正・追加で対応可能

④考察

(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

＊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る
個人情報（個人識別符号）の漏洩等のリスクの増大

➔遠隔生体認証時はNational ID Cardを使用することを前提とした
仕組みも可能であり，BSIwRBAへの組込み方式等、今後検討予定

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

代替案(1)：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

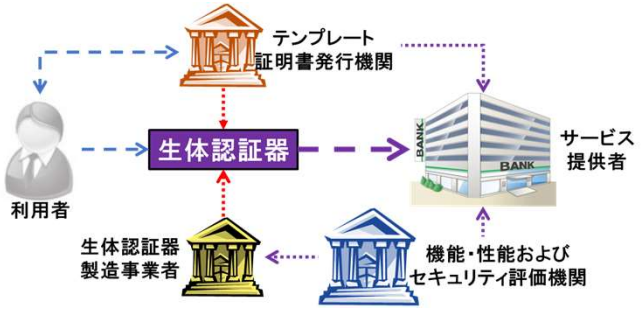
代替案(2)：部分開示可能な署名技術の利用

➔いずれの代替案も、BSIwRBAの機能実現には影響を与えず

●

④考察

(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



➔生体認証器の安全性・信頼性のリモート検証機能が必要か

なお、BSIの認証情報を管理するSecure Walletも同様である．今後、自己主権型の情報管理社会への移行が想定されており，想定される個人の情報の個人による管理・保護・利活用の仕組みが重要で、Secure Walletの研究開発が展開中。

今後，関連する研究開発の動向を把握しつつ，BSIwRBA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予定。

●

⑤おわりに

おわりに

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

ブロックチェーンサース基盤（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
利用者の匿名性と特定・追跡性の両立
を目指した、様々のアプリケーションのサービス基盤

安心・安全な遠隔生体認証（SSRBA）構想:
より確実な当人確認が可能な遠隔生体認証機能

●19分

⑤おわりに

サイバー・フィジカル社会の健全な発展のために

＊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ことが必要

＊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

＊より確実な本人確認技術としての生体認証への期待は大きく、プレゼンテーション攻撃等，生体認証システムへの様々の攻撃への防御・検知およびその評価技術の研究開発の進展に期待

＊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，利用者の匿名性と特定・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

＊今後，構想を構成する仕組みの再検討，仕様の具体化，および関連構想・システムとの関係の精査等を行い，BSIwRBAの改良・拡張を目指す予定 ●

終

（ご清聴、ありがとうございました）