光輝会

利用者の匿名性と特定・追跡性の両立
ー ブロックチェーンサービス基盤構想 ー

2024年7月12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

自　己　紹　介

1970年4月～1994年12月　東京芝浦電気（東芝）・情報システム部門
技術開発・研究部門の計算機利用環境（ハード・ソフト・ネットワーク）の整備・高度化
技術開発・研究業務における先進的計算機利用技術の社内導入・指導・支援

1995年1月～2007年9月　東芝・セキュリティ技術研究開発部門
セキュリティ技術センター長として、セキュリティ技術開発・事業支援活動推進
国プロの企画・提案推進、受託PJの指揮・指導

2007年10月　(株)IT企画を設立
［現職］
(株)IT企画　代表取締役社長
事業支援活動（顧問・相談役）：2社（日、米）
研究開発活動：中央大学研究開発機構、九州大学大学院
技術分野：暗号・認証、秘密分散、本人確認技術（バイオメトリクス）、
電子メールセキュリティ、IoTシステム、ビッグデータ、AI、
暗号資産セキュリティ、ブロックチェーン技術、安心・安全な社会基盤

本日の説明内容

(1)インターネットの拡大・普及の歴史と顕在化した社会課題
　①不正・不法・悪意・無責任な利用の急増
　②個人情報・プライバシー情報の漏洩・不正利用の増大

(2)着目した社会課題の克服策の提案とその必要性
　①確実な本人確認と、利用者の匿名性と特定・追跡性の両立
　②個人情報・プライバシー情報等の自己主権型管理モデルへ

(3)提案した社会課題克服策を組み込んだブロックチェーンサービス基盤（BSI）の仕組み説明

(4)ブロックチェーンサービス基盤（BSI）に関連する国内外の活動概要

インターネットの拡大・普及

インターネット：技術者・研究者を対象に構築・活用

1969年：ARPANET 実験開始
1974年：TCP/IP公開
1982年：ARPANET がTCP/IP ネットワークに移行
1984年：JUNET 実験開始（東大-慶応-東工大）（➔1988年WIDE）
1985年：企業活動での活用実証実験開始 ➔ 1987年 InetClub

インターネット：一般者向けにサービス開始・普及

1990年：米国で商用ISP登場
1991年：WWWをCERNが公開（Tim Berners-Lee）
1992年：日本で AT&T Jens 商用ISP (Spin) 営業開始
1993年：IIJ営業開始（1993年）
1993 年：MosaicをNCSAが公開（Marc Andreessen）

インターネット上のサイバー社会の発展期へ

＊利用者は、技術者・研究者
　通信相手の多くは、既知技術者・研究者
＊通信相手は別途の手段で確認、
　通信時の相手を確認ができなくても
＊そもそも、通信相手を攻撃する
　利用者の存在は想定外
＊不特定多数の利用者へ拡大
＊通信相手の確認は、
　従来の簡単な本人確認方法
＊不十分な相手確認による
　事故・事件が顕在化 ▼ ★

2002年：インターネットの個人利用率が50％超

不十分な利用者確認 ➡ 不正・不法・悪意・無責任な利用の急増

インターネット上でのWebサービスの急拡大

ネットサービスサイトの急増

＊世界のWebサイト数：2022年 19億

＊国内のECサイト・ネットショップ数：2017年189万、2019年271万、2021年419万、2023年455万

➔膨大な数の個人情報を、各サイトの運用組織が管理・利用

個人情報漏洩事件の急増

＊2023年度の企業や行政機関からの個人情報の漏洩件数：1万3279件で過去最多

（個人情報保護委員会）

＊2023年上場企業の個人情報漏洩：4,090万8,718人分（東京商工リサーチ）

➔ 個人情報の集中管理は、攻撃者の対象に

個人情報の管理組織での悪用・不正利用の多発

個人情報の第三者委託 ⇒ 漏洩・不正利用の増大

サイバー・フィジカル社会の時代を迎えて
サイバー社会のセキュリティ課題への対応が急務

(1)インターネット創世記からの利用者認証の課題の克服へ

➔ 確実な本人確認と、匿名性と特定・追跡性の両立

(2)個人情報・プライバシー情報等の管理・利用の第三者依存の克服へ

➔ 自己主権型（SSI）の個人情報・プライバシー情報等の管理

（1）
インターネット創世記からの利用者認証の課題の克服へ
なぜ利用者の匿名性と特定・追跡性が必要か

利用者の匿名性の必要性

サイバー・フィジカル社会が進展する中、
増大するサイバー社会での個人の活動

個人が安心して活発に活動を展開するには
活動情報および送受情報からの
個人の特定を回避できる仕組みが必要

利用者の特定・追跡性の必要性

サイバー・フィジカル社会の安全性は
サイバー社会の安全性に強く依存へ

サイバー社会の安全性を向上させるには
不正・不法・悪意・無責任な活動を行う
個人を特定・追跡し、
抑止・防止対策が取れる仕組みが必要

**サイバー社会の一層の発展と、サイバー社会の安心・安全の実現には
利用者の匿名性と利用者の特定・追跡性の両方が重要**

利用者の匿名性と特定・追跡性の両立に向けて

両立の難しさ

匿名性と特定・追跡性は対立概念

克服の視点

それぞれの仕組みを提供する
対象者・場面の分離

克服の具体策

(1)匿名性は、利用者に対し、
通常のサービス利用の場面にて
仕組みを提供

(2)特定・追跡性は、捜査者に対し、
合法的手続きに基づく捜査の場面にて
仕組みを提供

 9

（2）
想定される個人情報の漏洩・悪用の急増の課題の克服へ
なぜ利用者の自己主権型アイデンティティ管理モデルなのか

現状の第三者組織アイデンティティ管理モデルの問題

利用者は個人は機密性の高い個人情報・認証情報を複数の第三者組織へ提供が必要

個人情報等を管理する第三者組織からの情報漏えいリスク、情報悪用のリスク

自己主権型アイデンティティ（SSI）管理モデルへ

デジタル・アイデンティティの完全な制御と所有権を個人に提供することを目的とした概念

利用者は自分の個人情報等を自分自身で管理し、個人情報等の漏えいリスクを押さえられ、

提供・開示が必要な個人情報等については、

個人の判断で選択的に提供・開示する権限を確保できる仕組み

サイバー社会での利用者の情報や活動の安心・安全を強化するには

利用者自身による個人情報等の管理・利用制御の仕組みが重要 ★

 10

自己主権型アイデンティティ（SSI）管理の実現に向けて

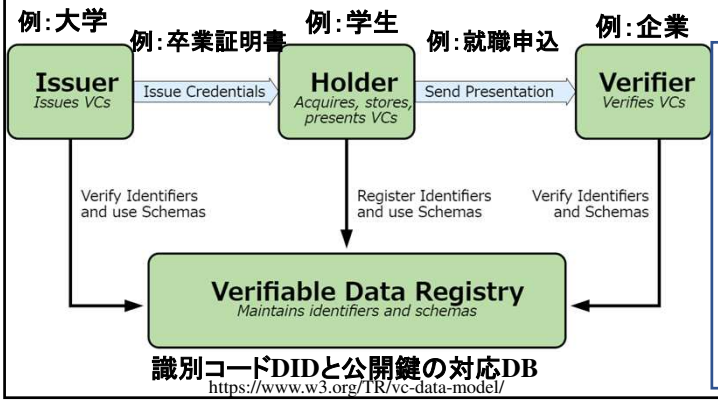
2005年に、Kim CameronがSSIの基本概念を示した含む“Seven Laws of Identity”を発表

2016年に、Cristopher Allenが発表した“Road to Self-Sovereign Identity”で

初めて“Self-Sovereign Identity”を使用

2019年に、W3CがSSIのコア技術である” Decentralized Identifier (DID) “

“Verifiable Credentials Data Model（VC）”の標準化活動を推進



識別コードDIDと公開鍵の対応DB

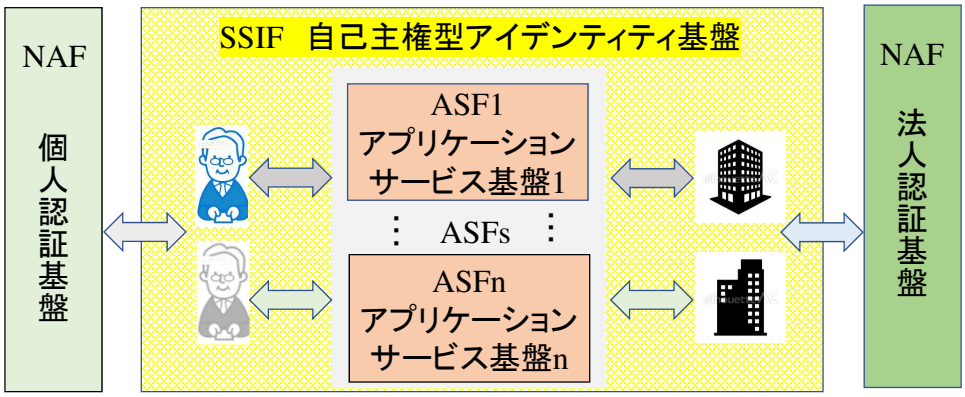
https://www.w3.org/TR/vc-data-model/

ブロックチェーンサービス基盤（BSI）
（Blockchain Service Infrastructure）

DID/VCベースのSSIへ
確実な本人確認
匿名性と特定・追跡性の両立
を組み込んだ
サイバー社会の基盤を目指した構想

 11

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構想（BSI）



個人の確実な身元確認
日本の場合は、
個人番号制度を想定

SSIF：NAFで身元確認されたエンティティへW3C標準化仕様に基づく識別子DIDを付与

ASF：SSIFでDIDを付与されたエンティティへ新たな識別子DIDを付与、様々のアプリケーションサービスを提供

法人の確実な身元確認
日本の場合は、
法人番号制度を想定

 12

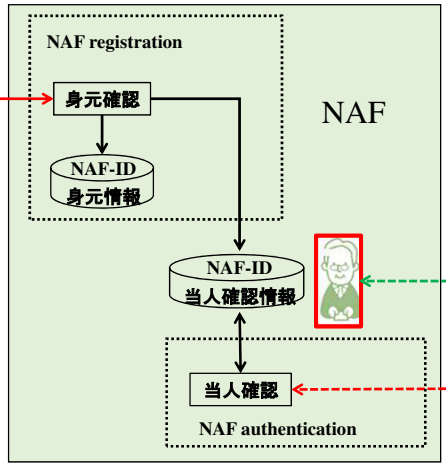
個人認証基盤における利用者登録・認証

National Authentication Framework

面前での手続きにより
確実な身元確認

NAF-ID、
当人確認情報
を入手

日本の場合、当人確認情報は
NAF-IDに対応する
公開鍵証明書と秘密鍵
（マイナンバーカード内に格納）



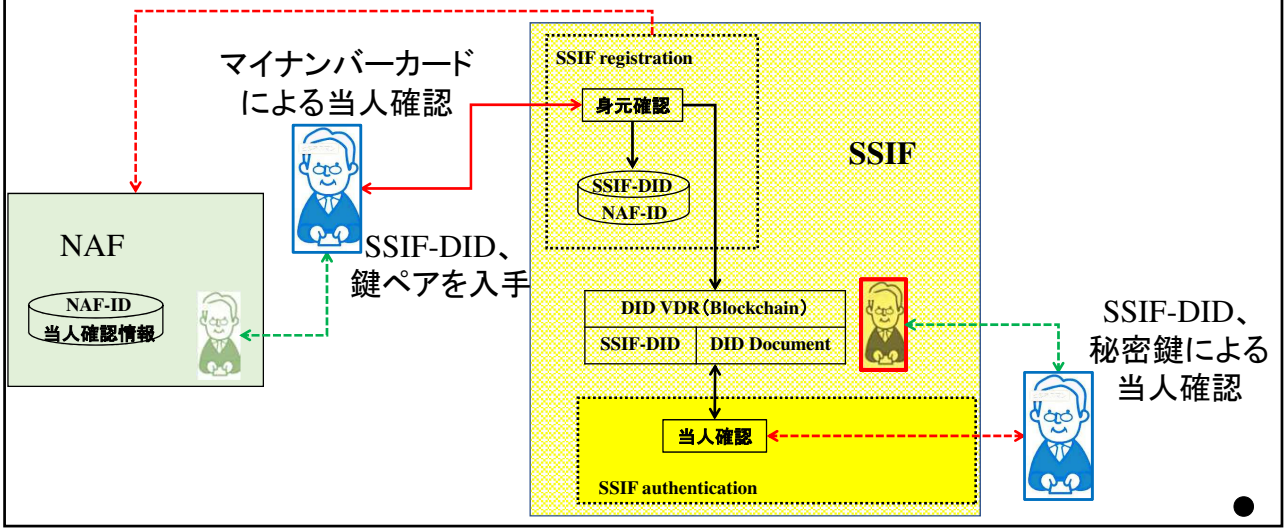
当人確認情報を利用し
当人確認

日本の場合、
マイナンバーカード
を利用し当人確認

 13

自己主権型アイデンティティ基盤における利用者登録・認証

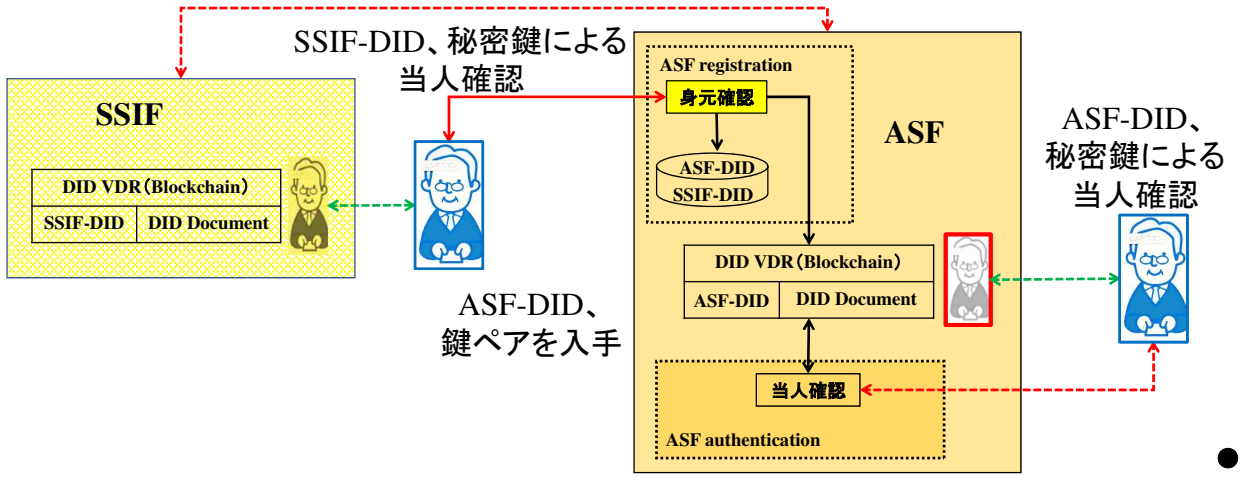
Self-Sovereign Identity Framework



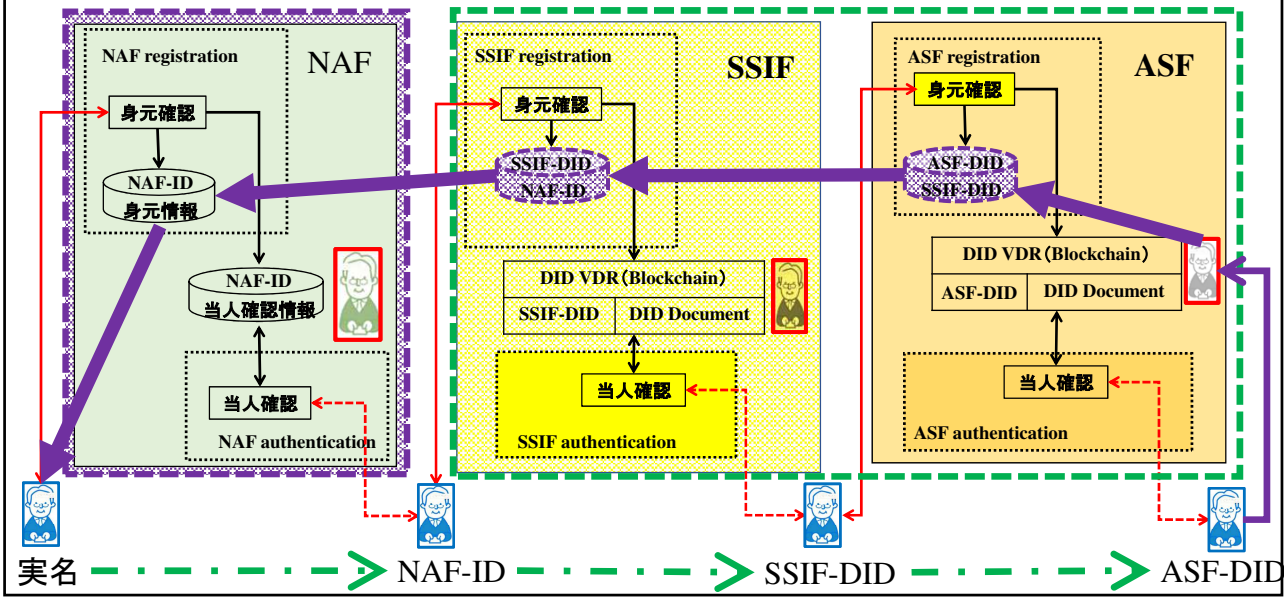
 14

アプリケーションサービス基盤における利用者登録・認証

Application Service Framework



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



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・フィジカル社会の今後も発展 ➔ 特に、サイバー社会の急速な進展は必至
現状のままのインターネット利用形態
➔ サイバー社会の不正・不法・悪意・無責任な活動の激増、および、
個人情報・プライバシー情報の漏洩・悪用・不正利用の激増、は必至

ブロックチェーンサービス基盤（BSI）が目指す、
利用者の匿名性と特定・追跡性の両立の仕組みは、
インターネット上の不正・不法・悪意・無責任な活動の抑止・防止に、必須

ブロックチェーンサービス基盤（BSI）が目指す、
個人情報・プライバシー情報の第三者依存の管理・運用から
自己主権型アイデンティティ情報管理への移行は、
個人情報漏洩事件や管理組織での悪用・不正利用の抑止・防止に、必須

ブロックチェーンサービス基盤（BSI）研究の状況

利用者の匿名性と特定・追跡性の両立に関する研究（2018～）

本人確認基盤に関する研究（2019～）

自己主権型アイデンティティ情報管理に関する研究（2021～）

ブロックチェーンサービス基盤（BSI）に関する研究（2023～）

①”メタバースにおける利用者の匿名性と特定・追跡性の両立方式の提案
およびその安心・安全な社会維持効果に関する考察”, CSS2023.

②”安心・安全な学修歴利活用基盤（SSARUF）の考察”, SCIS2024.

ブロックチェーンサービス基盤（BSI）に関連する国内外の活動

(1)W3C：World Wide Web Consortium

1994年、ティム・バーナーズ・リーによって創設されたWeb技術の標準化を行う非営利団体
SSI（Self Sovereign Identity）という概念に関連する技術の標準化を推進
「個人情報は、第三者の管理主体を介することなく、個人が主権的にコントロールすべき」
DID（Decentralized Identifier）、VC（Verifiable Credential）

➔BSIのSSIF/ASFは、まさにDID/VC技術ベースの構想

(2) EBSI：European Blockchain Services Infrastructure

ブロックチェーンを基盤とした欧州全域（29か国）に及ぶ公共サービスのインフラ

➔W3C標準化技術DID/VCベース

(3) UKAS：UK Digital Identity and Attributes Trust Framework
➔W3C標準化技術DID/VCベース

(4)Trusted Web
特定のサービスに過度に依存せずに、個人・法人によるデータの
コントロールを強化する仕組み、やり取りするデータや相手方を検証できる仕組み等の
新たな信頼の枠組みを構築するイニシアティブ（Trusted Web推進協議会が推進）
➔W3C標準化技術DID/VCベース

BSIは、W3C標準化技術DID/VCベースの、
個人情報の自己制御性、署名技術によるデータの検証可能性に加え、
確実な本人確認のためにNAFとの連携機能、
および、個人の匿名性と特定追跡性の両立のための機能、を組み込んだ構想

終

ご清聴、ありがとうございます。

なお、本スライドは以下のURLで参照できます。
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20240712KoukikaiSlide.pdf
ご意見等、いただければ幸いです。