自己主権型アイデンティティ情報利活用基盤（SSIUF）
― 利用者の匿名性と特定・追跡性の両立 ―

才所　敏 明[†1]　　辻井　重男[†2]　　櫻井　幸一[†3]

（株）IT 企画　　中央大学研究開発機構　　九州大学大学院システム情報科学研究院
（株）ZenmuTech　　（株）国際電気通信基盤技術研究所

１．問題提起

個人の社会活動がネット上で実施される時代へ移行しつつあり，個人の活動の DX の進展が期待される．個人の社会活動では，個人情報・プライバシー情報の塊であるアイデンティティ情報の提供が求められる場合が多く，ネット上でのアイデンティティ情報の安心・安全な流通を可能とする仕組みが，個人の活動の DX の進展を左右する重要な課題となっている．

筆者らはこの課題を克服すべく，自己主権型アイデンティティ利活用基盤（SSIUF：Self-Sovereign Identity-information Utilization Framework：以下，SSIUF と略記）を提案した（[1]）．既提案 SSIUF では，利用者の身元確認および利用者の特定・追跡に不可欠な身元情報の管理機能を内蔵する構成である．３．にて既提案 SSIUF の概要をまとめている．

一方，利用者の身元確認および身元情報の管理は，ネット上の多くのアプリケーションに共通に必要な機能である．利用者の個人情報の拡散の回避，サービス事業者の身元確認の負担，個人情報管理のリスク等の軽減を目指し，アプリケーションとは独立した国別の本人確認基盤（NAF：National Authentication Framework：以下，NAF と略記）を提案中である（[2]）．２．にて NAF の概要をまとめている．

本稿では，身元確認および身元情報の管理に NAF を活用した，利用者の匿名性と特定・追跡性の両立を可能とする SSIUF の構成を提案する．

Self-Sovereign Identity information Utilization Framework
- coexistence of the user anonymity and the user identifiability / trackability -

[†1]Toshiaki Saisho
Advanced IT Corporation
[†2]Shigeo Tsujii
Research and Development Initiative, Chuo University
[†3]Kouichi Sakurai
Graduate School and Faculty of Information Science and Electrical Engineering, Kyushu University
Advanced Telecommunications Research Institute international (ATR)

２．本人確認基盤（NAF）

インターネットの課題は利用者の匿名性の強さである．社会がインターネット依存を強める中，社会の安心・安全の維持のためには，利用者の特定・追跡性が確保された上での匿名性の確保，が不可欠である．

筆者らは，Cyber World 内でのアプリケーション利用時の利用者の一定レベルの匿名性を確保しつつも，社会の安心・安全維持のための合法的捜査時には，利用者の特定・追跡を可能とする NAF を提案中である（図１）．

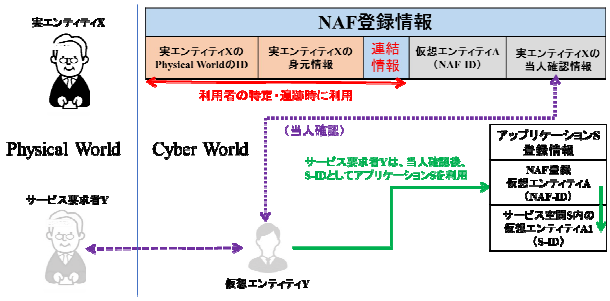

図１ NAF の仕組み

図１に示すように，アプリケーション利用時には利用者の匿名性は確保され，必要時には NAF の協力を得ることにより，利用者の特定・追跡が可能な仕組みである．

３．自己主権型アイデンティティ情報利活用基盤（SSIUF）

筆者らは，利用者の匿名性を確保しつつも利用者の特定・追跡を可能とする SSIUF の構成，分散型 ID（Decentralized Identifier：以下，DID と略記）/検証可能属性証明（Verifiable Credential：以下，VC と略記）技術を利用した SSIUF の構成を提案中である（図２）．

身元確認を実施する DID 発行組織では，新たに発行する DID と公開鍵等の DID 保有者の情報を示す DID Document を Blockchain 等の VDR（Verifiable Data Registry：以下，VDR と略記）へ登録する際に，身元確認済であることを示す情報を付加すると同時に，発行した DID と身元情報を紐づけて安全に管理するものとする（身元情報 DB）．

利用者が新たに DID の発行を依頼する際に身元確認済の DID を提示した場合は，DID 発行組織は

身元確認を省略し，新たに発行する DID Document 内に身元確認済であることを示す情報を含めると同時に，新たに発行する DID と利用者が提示した身元確認済 DID の対応を安全に管理するものとする（DID 対応 DB）．

このような仕組みにより，身元確認を省略した DID についても，DID 対応 DB を次々とたどることにより身元確認を実施した DID の発行組織を特定し，その発行組織の協力により利用者の身元情報を入手でき，特定・追跡が可能となる．

一方，以上のような仕組みの追加にもかかわらず，利用者（アイデンティティ情報保有者），アイデンティティ情報発行組織，アイデンティティ情報使用組織間の情報の授受は，発行された DID という仮名で行われ，一定の匿名性は維持されている．

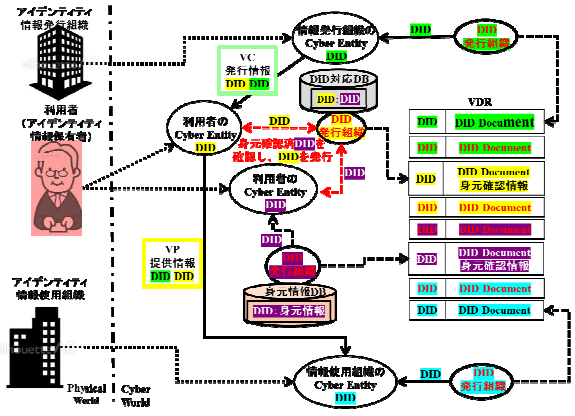

図２ 既提案 SSIUF の構成

４．NAF を活用した SSIUF の構成

SSIUF で必要な機能のうち，DID 発行組織による身元確認を NAF による身元確認に置き換えた構成（関連する部分のみ）を図３に示す．

利用者は NAF を利用し NAF-ID および当人確認情報を登録しておくものとする．NAF の身元確認を利用し新たな DID を発行する DID 発行組織は，利用者の NAF-ID の保有を確認した上で DID を発行し，VDR の DID Document には身元確認済であることを明記しておく．その DID を利用し，新たな DID を発行する DID 発行組織は，DID の保有を確認し，VDR の DID Document には身元確認済であることを明記しておく．

DID を使用する SSIUF 領域では利用者はそれぞれの（複数の）DID という仮名で識別され一定の匿名性が確保されている．また，万一，その利用者を特定・追跡する必要がある場合は，SSIUF 領域では DID 対応 DB をたどり，最終的には NAF-ID 対応 DB により NAF-ID を特定でき，NAF 運用組織の協力により利用者の追跡に必要な身元情報を入手できる．

このようにして，利用者の匿名性と特定・追跡性の両立を実現している．

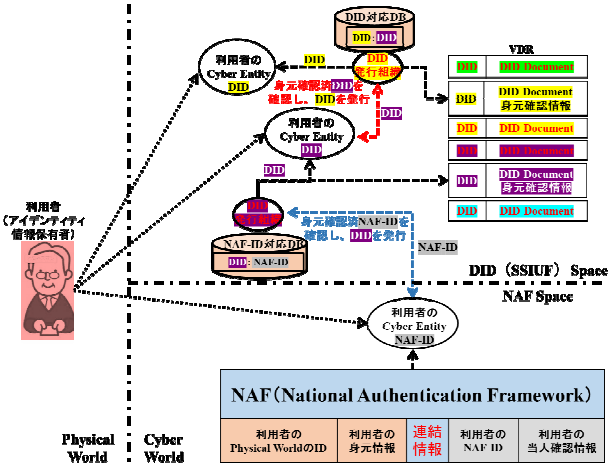

図３ NAF 利用 SSIUF の DID 発行の仕組み

インターネット上のアプリケーションの利用者の確実な本人確認を支援する NAF は，各国の公的機関との連携・支援・管理の元で構築・運用が期待されている．SSIUF もアプリケーションの一つとして NAF を利用することにより，身元確認機能内蔵の NAF に比べ，SSIUF 自体の身元確認の負担，身元情報管理のリスクも軽減できる．

今後，SSIUF の応用分野を具体的に調査・分析しつつ，また W3C の DID/VC 関連技術の標準化化動向を把握しつつ，提案した SSIUF の構成の詳細仕様の検討を進める予定である．

謝辞：本研究の一部は，一般財団法人テレコム先端技術研究支援センターの研究助成の支援を受けている．

参考文献

[1]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“，SCIS2022. http://advanced-it.co.jp/2016_wp/wp-content/pdf/20220119SCISPaper.pdf

[2]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－”. CSS2020. http://advanced-it.co.jp/2016_wp/wp-content/pdf/20201026CSS2020Paper.pdf

[3]“Decentralized Identifiers (DIDs) v1.0 Core architecture”. World Wide Web Consortium. 2021. https://www.w3.org/TR/did-core/

[4] “Verifiable Credentials Data Model 1.0”. World Wide Web Consortium. 2021. https://www.w3.org/TR/vc-data-model/