

Self-Sovereign Identityはなぜ"幻想"とされるのか — 新しいデジタルアイデンティティを考える

公開: 2025/09/30 | Zenn (idroit-community)

以前、このブログでは Decentralized Identifiers (DID) に対して否定的な立場から考察した記事を公開しました。 [なぜ Decentralized Identifiers \(DID\) を使う必要はないのか](#)

この記事は、デジタルアイデンティティ研究や実務のコミュニティにおける DID に対する一般的な見解とも重なる部分が多く、一読する価値があると考えています。しかし、**私は現在のデジタルアイデンティティをめぐる議論が、政府や大企業による「個人の集中的な管理」という枠組みに過度に依拠しているのではないかと感じています**。そこで本稿では、従来とは異なる視点から、デジタルアイデンティティのあり方を改めて論考してみたいと思います。

デジタルアイデンティティの刷新の必要性

Self-Sovereign Identity (SSI) は昨今、理想的ではあるものの、現実には実現不可能であるという批判的な見方をされることが多くなっています。その理由の多くは、SSIを既存の「デジタルアイデンティティ」の定義や枠組みの中で評価していることに起因しています。すなわち、**「デジタルアイデンティティとは何か」という前提そのものを刷新しなければ、SSIの有用性を正しく理解することはできません**。

現状のデジタルアイデンティティは「属性情報の集合」として捉えられてきました (Windley, 2005)。たとえば、政府が発行する公的証明書や、大企業・組織が提供するアカウントサービスは、現実世界（物理空間）における人間のアイデンティティと、デジタル空間におけるログイン情報や利用履歴とを強く結び付けることを前提としています。**このモデルは「実名性」に依存し、オンライン上の行為主体が現実世界の個人と同一であることを保証することに重きを置いています**。

しかし、**SSIやそれを支える一技術であるDIDの真の可能性は、このような現実世界のアイデンティティへの依存を前提としないところにあると考えます**。むしろ、現実世界のアイデンティティとは切り離し、デジタル空間そのものに固有のアイデンティティの概念を構築する必要があるのではないのでしょうか。この方向性では「属性の集合としての一貫性」よりも、「状況に応じて切り替え可能な仮名性」や「複数の人格を同時に持つ自由」が重視されます。

厳格なデジタル仮名性

この問題意識は、1980年代にDavid Chaumが提唱した**Digital Pseudonym（デジタル仮名）**の概念に先駆けて表現されています。Chaumは「Security without Identification: Transaction Systems to Make Big Brother Obsolete」（Chaum, 1985）において、匿名性を保持しつつ一貫性のある仮名を維持できるシステムを提案しました。これは、実名と切り離されたが責任追跡可能な仮名を持つことで、匿名性と説明責任を両立させる試みであり、後の匿名認証やゼロ知識証明研究（Goldwasser et al., 1989; Camenisch & Lysyanskaya, 2001）にも大きな影響を与えました。

また、「複数の人格を持ち、状況に応じて切り替える自由」を重視する考え方は、オンライン・アイデンティティ研究においても議論されてきました。Turkle（1995）は『Life on the Screen』において、インターネット上で人は複数の「自己」を表現しうることが指摘していますし、Nissenbaum（2004）はプライバシーを「文脈に依存する情報フローの適切性」と定義し、必ずしも実名性と結び付ける必要はないことを論じています。これらの議論は、DIDの応用可能性を「実名との一貫性」に限定するのではなく、「デジタル空間固有の仮名的アイデンティティ」として再構築すべきことを示唆しています。

したがって、DIDを有用に活用するためには、従来の「属性集合モデル」に基づいたデジタルアイデンティティ観を超えて、「**デジタル仮名性**」を前提とする新しいアイデンティティの概念を受け入れる必要があります。現実世界の身元とデジタル空間の人格を一対一で結び付けるのではなく、デジタル空間における多様で可変的な自己を支える仕組みとしてDIDを位置付けることこそが、次の段階の論点であると考えます。

新しいデジタルアイデンティティにおけるDIDの役割

Decentralized Identifier（DID）は、従来のアイデンティティシステムの枠組みを超えて機能する可能性を持っています。その本質は「主体が自らコントロールする識別子」であり、必ずしも現実世界の実名や属性情報と紐づく必要はありません。むしろ、新しいデジタルアイデンティティのあり方においては、DIDは以下の三つの観点で重要な役割を果たすと考えます。

1. 仮名性を支える識別子としてのDID

ChaumのDigital Pseudonymの思想が示すように、デジタル空間における一貫した仮名性は、匿名性と説明責任を両立する基盤となります。DIDは中央集権的な発行者を必要とせず、個人が生成・管理できるため、複数の仮名的アイデンティティを自由に作り分けることが可能です。これは、Nissenbaum（2004）が論じた「文脈依存のプライバシー」を支える仕組みとも親和性が高いです。利用者は状況に応じて異なるDIDを用いることで、情報の流通範囲を制御しつつ一貫性を保持することができます。

2. 多様な人格の切り替えを可能にする技術的基盤

従来のアイデンティティは「唯一の自己」を前提としていましたが、Turkle（1995）が指摘したように、オンライン環境では複数の自己を持ち、状況に応じて切り替えることが一般的です。DIDは技術的に「一人対一つの識別子」の関係を強制しません。**利用者は複数のDIDを管理し、職業人としての自分、趣味活動における自分、実験的な人格としての自分などを自由に切り替えることができます。**この柔軟性は、SSIの文脈で求められる「自己主権」よりもむしろ「自己多元性」を支える仕組みであると言えます。

3. 信頼と検証のための相互運用的メタレイヤー

属性情報や証明書が不要になるわけではありません。むしろ**DIDは、それらを可選的に関連付けるメタレイヤーとして機能します。**たとえば、特定の取引や契約においては、特定のDIDに対してゼロ知識証明（Goldwasser et al., 1989; Camenisch & Lysyanskaya, 2001）を用いて必要最小限の属性を提示することができます。これにより、実名に依存しない形で「年齢確認」「資格証明」「所属確認」といった機能を果たすことが可能になります。DIDは「属性集合としての自己」と「仮名的で多重的な自己」との橋渡しを行う存在となります。

参考文献

1. Chaum, D. (1985). Security without Identification: Transaction Systems to Make Big Brother Obsolete. Communications of the ACM, 28(10), 1030–1044. <https://dl.acm.org/doi/10.1145/4372.4373>
2. Goldwasser, S., Micali, S., & Rackoff, C. (1989). The Knowledge Complexity of Interactive Proof Systems. SIAM Journal on Computing, 18(1), 186–208. <https://dl.acm.org/doi/10.1137/0218012>
3. Camenisch, J., & Lysyanskaya, A. (2001). An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. EUROCRYPT 2001. <https://dl.acm.org/doi/10.5555/647086.715698>
4. Turkle, S. (1995). Life on the Screen: Identity in the Age of the Internet. Simon & Schuster. <https://dl.acm.org/doi/10.5555/526517>
5. Nissenbaum, H. (2004). Privacy as Contextual Integrity. Washington Law Review, 79(1), 119–157. <https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/>
6. Cameron, K. (2005). The Laws of Identity. Microsoft. <https://www.identityblog.com/?p=1065>
7. Windley, P. (2005). Digital Identity. O'Reilly Media.
8. Preukschat, A., & Reed, D. (2021). Self-Sovereign Identity. Manning.

出典: <https://zenn.dev/idroit/articles/e07456e5f55244>