5H-01

サイバネティック・アバター認証基盤の設計思想 －自己主権型／分散型アイデンティティの提案－

原田伸一朗†

静岡大学†

1. はじめに

内閣府が主導する「ムーンショット型研究開発制度」において，「ムーンショット目標 1」は，「2050 年までに，人が身体，脳，空間，時間の制約から解放された社会を実現」するとの目標を掲げている．そこでは，誰もが多様な社会活動に参画できるサイバネティック・アバター基盤を構築し，未来社会における新しい生活様式として，「サイバネティック・アバター生活」を提案，普及させるとのターゲットが示されている[1]．報告者は，当該研究開発プロジェクトの一つである「アバターを安全かつ信頼して利用できる社会の実現」（新保史生 PM）に携わるメンバーである．

2. サイバネティック・アバターの認証基盤

サイバネティック・アバター（以下 CA）とは，現在必ずしも明確に定義されているわけではないが，「身代わりとしてのロボットや 3D 映像等を示すアバターに加えて，人の身体的能力，認知能力及び知覚能力を拡張する ICT 技術やロボット技術を含む概念」[1]とされる．

サイバー・フィジカル両空間にわたる活用が期待される CA を，日常生活で安全・安心に利用できるようにするためには，「なりすまし」「乗っ取り」「違法・不正な技能模倣（他人の技能に依拠してこれと実質的に同一の技能を違法・不正に作出すること）」といった問題に対抗するための技術的・制度的基盤が必要である．そこで，本プロジェクトにおいては，①誰が CA の正当な利用者なのかを確認する「利用者認証」，②CA が誰に帰属するのかを確認する「CA 認証」，③正規の CA であるか否かを確認する「CA 公証」に関する研究をおこない，それらを統合した「CA 安全・安心確保基盤」を構築することを目標としている．

Design Philosophy of Decentralized Authentication of Cybernetic Avatars
†Shinichiro Harata, Shizuoka University

その構築に当たっては，認証技術の研究開発のほか，社会制度としての認証基盤を管理する機構・主体の検討も併せて進める必要がある．本報告においては，将来的に CA 認証基盤を整備・運用するフェーズを念頭に，その基本的な設計思想を検討したい．

3. 認証基盤の管理主体

CA といっても，あくまでそれを操作する実在の自然人が CA の「本人」として一意に認証される必要があるとすると，CA と本人を連結させて一体の法的人格主体と扱うのが合理的である．すべての人が CA を日常的に用いるような社会を念頭に置くならば，いわば「戸籍」のようなものとして，その本人確認・認証基盤を国のプラットフォームとして設計・運用することがまず考えられ，例えばマイナンバー制度の利用も想定し得る．ただし，CA の活用領域は私経済取引を含め多岐にわたる可能性があり，その認証基盤の管理主体が国であると，CA は，それを介して国家が国民を管理・監視するツールに化してしまうおそれもある[2]．また，マイナンバーは日本国民だけでなく外国人住民にも付番されるにせよ，CA のグローバルな利用を見据えるならば，国家に拠らない認証基盤が必要である．

国連の SDGs では，「2030 年までに，すべての人々に出生登録を含む法的な身分証明を提供する」との目標（16.9）が掲げられている[3]．世界には，公的な ID を持てず，「法的には存在しない」ことになっている個人が多数存在する．一方で，そうした人もソーシャルメディアのアカウントを持ち，アバターとしてメタバースで活動する．国家が身分証明を提供できなくとも，サイバー・フィジカル空間で活動するアバターとその操作者を認証できる仕組みが必要である．

CA の範疇には，メタバースなどで用いられるバーチャルアバター（CG アバター）も含まれるが，それを利用するためのアカウントは，現状それぞれのプラットフォームが個別に発行することが多い．少数のデジタル・プラットフォー

Copyright ©2023 Information Processing Society of Japan.
All Rights Reserved.

ム事業者にメタバース事業も集約されていくならば，ID 管理の集中化も必然的に進むが，多数のメタバースが相互運用性を保ちながら接続する「オープンメタバース」を志向するトレンドも強い．その実現のためには，プラットフォームをまたぐシームレスな連携を可能にするアカウント認証の仕組みが不可欠である．

4. 自己主権型 ID／分散型 ID

中央集権型 ID 管理への一種のアンチテーゼとして，管理主体を介さず，ユーザ個人が自らのアイデンティティをコントロールできるようにする「自己主権型アイデンティティ（SSI; Self-Sovereign Identity）」という思想が提起されている[4]．そして，主にブロックチェーン技術を用い，特定の管理主体に依存せず，ユーザ同士の分散型管理を実現する仕組みは「分散型アイデンティティ（DID; Decentralized Identity）」と呼ばれる．これらは厳密には概念のレベルが異なるが，以下まとめて「SSI/DID」とする．

この設計思想を CA の認証基盤に取り入れることで，国家やプラットフォーム事業者による中央集権型データベースシステムに伴う「監視」やセキュリティ・リスクを回避できる．ユーザ同士でコミュニケーションや取引の信頼性を確保でき，必要な情報のみ，都度必要な相手に提供できるという利点もある（現状は過剰提供の場合が多い）．

また，すでにメタバースの実践において明らかになっているように，ユーザがアバターを用いる目的には，実社会とは別の「人格」を持ちたいという，いわゆる「分人」主義的なニーズも多分に含まれる．CA では，1 人で複数のアバターを同時に用いることや，複数の人が 1 体のアバターをシェアして用いることも想定され，「一対一」のアイデンティティ管理は行き詰まる．次々にアバターを“脱ぎ捨て”，“重ね着”しても，CA の信頼性を途切れなく担保できるような認証基盤が求められる．

5. 自己情報コントロール権をめぐって

憲法学説では「プライバシー権」の法的性質をめぐる議論が盛んであるが，SSI/DID のコンセプトとその普及・実装が，そうした議論に及ぼし得る影響についても考察することは意義がある．日本においてプライバシー権は，「私生活をみだりに公開されないという法的保障ないし権利」として判例上承認されてきた．学説においては，「自己情報コントロール権」との理解が通説的地位を占めてきたが，その捉え方をめぐっては，実体的デュー・プロセス理論に求める見解[5]など，議論もある[6].

今後，ユーザ主権・分散型の個人情報管理が技術的・社会的に標準化し，「コントロール」という語が実を帯びるようになれば，プライバシー権をめぐる法学説の前提にも影響を与える可能性がある．

6. おわりに

近年，国家戦略として Web3 やブロックチェーン，DAO の政策活用[7]を模索する動きも加速している．中央集権型 ID の代名詞ともされるマイナンバー制度も，CA の実用化・普及が目指されている 2030～2050 年代を想定すると，SSI/DID との接合は不可避であろう．マイナンバー制度のような公的・国家的認証基盤が不要となることは考えにくいが，そうした悉皆性，唯一無二性という特徴を有する本人確認基盤を，分散型 ID のチェーンの一つに括りつけるといった発想[8]への転換が求められることになるとも考えられる．

謝辞

本研究は，JST ムーンショット型研究開発事業, JPMJMS2215 の支援を受けたものです.

参考文献

[1] 内閣府“ムーンショット目標 1”. https://www8.cao.go.jp/cstp/moonshot/sub1.html, (参照 2023-1-9).
[2] 新保史生. サイバネティック・アバターの認証と制度的課題：新次元領域法学の展開構想も踏まえて. 日本ロボット学会誌, 2023, vol. 41, no. 1.
[3] United Nations “Goal 16”. https://sdgs.un.org/goals/goal16, (参照 2023-1-9).
[4] 栗原佑介. デジタル遺品の法的問題：SNS アカウントのアクセス権の相続性を中心に. 情報ネットワーク・ローレビュー, 2020, vol. 19, p. 76.
[5] 新保史生. プライバシーの権利の生成と展開. 成文堂, 2000, 438p.
[6] 曽我部真裕, 山本龍彦. 自己情報コントロール権をめぐって. 情報法制研究, 2020, vol. 7, p. 128-140.
[7] 蒔田純. 政府機能におけるブロックチェーンの活用可能性：分散型台帳を用いた行政運営に関する一考. 公共政策志林, 2021, vol. 9, p. 41-53.
[8] 橋田浩一. 集めないビッグデータ：情報の分散管理による個人の尊厳と公共の福祉. 社会情報学, 2015, vol. 3, no. 3, p. 97.

Copyright ©2023 Information Processing Society of Japan.
All Rights Reserved.