

2025 年 4 月 1 日 全 7 頁

デジタル化が進む個人情報はい これからどのように管理すべきか

自己主権型アイデンティティ（SSI）の課題と未来

経済調査部 研究員 田邊 美穂

[要約]

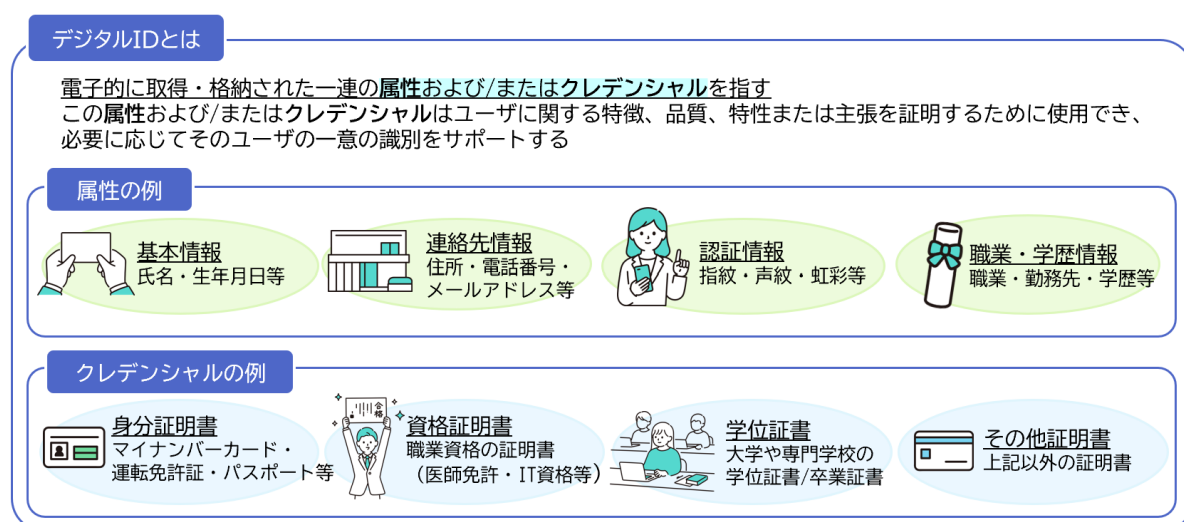
- デジタルサービスの急速な普及により、利用者自身がアイデンティティ（個人情報や資格情報等、個人を特定/証明するためのさまざまな属性）の管理を行う自己主権型アイデンティティ（Self-Sovereign Identity、以下 SSI）という新しいアプローチが注目されている。このアプローチのメリットは、分散型のアプローチや暗号技術の活用によるプライバシー保護およびセキュリティ強化にある。サービス提供側が中央集権的に利用者の個人情報や資格情報を管理する、既存手法における情報漏洩等の課題への効果が期待できる。
- 一方、SSI の実現には多くの障壁が存在する。これには、国際的な相互運用性を実現するための技術的および法的・規制的課題、新しいアイデンティティ管理方法に沿ったビジネスモデル変革、利用者の理解度向上に関連する問題等が含まれる。SSI の実現は今後の国際社会の動向に大きく依存すると考えられる。
- SSI でも利用されるデジタル証明書（デジタルな形式でアイデンティティを証明する技術）等の技術は既に運用が始まっている。そのため、デジタル証明書等の技術を用い、利用者自身がサービス提供側に共有するアイデンティティを選択できる手法等も具体化しつつある。ただし、完全な SSI ではなく、サービス提供側が利用者の情報を管理するため、情報漏洩等の課題は依然として残る。
- このような状況から、完全な SSI の実現にはまだ時間を要するだろう。しかし、身分証明書や資格証明書、学位証書等、現在アナログ形式で管理しているアイデンティティのデジタル化はますます進展すると考えられる。利用者はプライバシー保護やセキュリティ強化のメリットを受けることと引き換えに、それらについてより一層の知識と意識を持つことが求められるだろう。

1. はじめに

デジタル技術の進化により、日常生活でデジタルサービスを利用する機会が急速に拡大している。現在、多くのデジタルサービスは、利用時に個人を識別および認証するためのアカウント作成を求める。そのため、利用するデジタルサービス数に応じて管理するアカウントも増加し、アカウントに付随する個人情報や資格情報も含めて、その管理は煩雑になっていく。

このようなオンラインにおける個人の識別および認証を行うための情報の集合をデジタルアイデンティティ（以下、デジタル ID）と呼ぶ。これには個人情報や資格情報等、個人を特定/証明するためのさまざまな属性やクレデンシャルが含まれる（図表 1）。前回のレポート¹では、日本におけるデジタル ID の実現に向けた取り組みの一例としてマイナンバーを取りあげた。今回のレポートではより広範な視点から、近年その重要性が高まっているデジタル ID をどのように管理していくべきか、注目される新たな管理方法や、その課題について解説する。

図表 1 デジタルアイデンティティ（デジタル ID）のイメージ



（出所）OECD[2023] “[Recommendation of the Council on the Governance of Digital Identity](#)” (OECD/LEGAL/0491) (2023 年 6 月 8 日) 等、各種資料より大和総研作成（イラストはソコスト (<https://soco-st.com/>)）

2. デジタル ID の 3 つの管理手法

アイデンティティを「誰が」管理するのかで分けられる

デジタル ID の管理方法としては主に 3 種類、**①サイロ型**、**②フェデレーション型**、**③自己主権型**が挙げられる²（図表 2）。

¹ 田邊美穂[2024]「[デジタル時代の本人確認『デジタル ID』：日本におけるデジタル ID の実現に向けたマイナンバーの役割と課題](#)」大和総研レポート（2024 年 11 月 28 日）を参照。

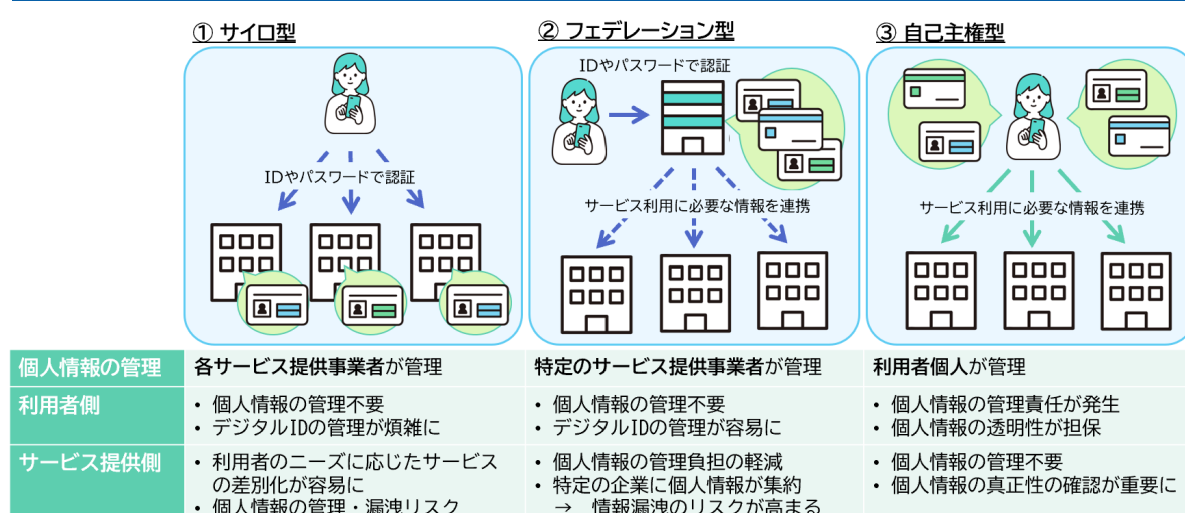
² この管理方法に関してはさまざまな分類および呼び方が存在するが、本稿ではサイロ型、フェデレーション型、自己主権型とする。

現在、利用者にとって最も一般的かつ馴染みが深い方式は、①サイロ型である。冒頭で触れた、デジタルサービス利用時にその都度アカウントを作成し個人情報や資格情報を登録、その情報をサービス提供側が中央集権的に管理する方法が、このサイロ型にあたる。利用者側は、登録した個人情報等の管理をサービス提供側に任せる一方で、ログイン ID やパスワードの管理が煩雑になる短所がある。サービス提供側は、利用者のニーズや要件に応じたサービスの差別化や最適化³に柔軟に対応できる一方で、個人情報等を管理するコストや情報漏洩等のリスクを負う。

②フェデレーション型は、①サイロ型と近い考え方を持つ、近年増えている方式である。デジタルサービス利用時に、既に保有している別のデジタルサービスのアカウントを利用する。①サイロ型と比較すると、利用者側は登録した個人情報や資格情報の管理をサービス提供側に任せる。そして、ログイン ID やパスワードは複数のサービスで共有するため、管理が容易になる。また、サービス提供側も特定の企業に個人情報等の管理を任せることでコストの削減が図れる。だがその一方で、特定の企業に個人情報等が集約されるため、情報漏洩等のリスク等が高まる懸念される。

③自己主権型は、①サイロ型や②フェデレーション型とは根本的に異なるアプローチである。利用者自身が個人情報や資格情報を管理し、デジタルサービス利用時に必要となる個人情報等をその都度選択して提示する。利用者側は、個人情報等を管理する責任が発生するが、どの情報を提供したかが明確になる。個人情報等に対する透明性が担保され、個人情報の保護が強化される。サービス提供側としては、個人情報等の管理が不要となることでコストが削減されるが、提示された個人情報等の真正性（本物であること）の確認が重要になる。

図表 2 デジタル ID の管理方法



（出所）独立行政法人情報処理推進機構 総務企画部 調査分析室『[『個人起点』がデータ流通を促進する ブロックチェーンによる自己主権型アイデンティティの実現](#)』（2021年3月31日公開、最終更新日2024年9月24日）等、各種資料より大和総研作成（イラストはソコスト（<https://soco-st.com/>））

³ 例えば、ログイン認証やアクセス制御のカスタマイズ、利用規約やプライバシーポリシーにおける利用者の同意により個人情報を利用したパーソナライズドサービスの提供等が、他の管理方法と比較して容易である。

3. 新しいデジタル ID の管理方法、自己主権型アイデンティティ (SSI)

近年注目される自己主権型アイデンティティ (SSI)

この③自己主権型は、正式には自己主権型アイデンティティ (Self-Sovereign Identity、以下 SSI) と称される。SSI は、利用者自身が個人情報や資格情報を管理及び制御するという概念であり、これを実現することでプライバシー保護とセキュリティ強化が期待できる。そのため、デジタルサービスの急速な普及の中で、次世代のアイデンティティ管理の枠組みとして注目されている。現状としては、一部企業等で実用化が進められているものの、多くは実証実験の段階である。SSI の実用化に向けた具体的な例としては、EU で進められている「EU デジタル ID ウォレット計画」が挙げられる。EU でのデジタル ID の実現に SSI の考え方が採用されており、2026 年までに全ての加盟国で広く利用可能なデジタルウォレット (デジタル環境でさまざまな情報や資産を安全に管理・保存するためのツール) の実現を目指している⁴。

プライバシー保護とセキュリティ強化が期待される

SSI の実現で期待される、プライバシー保護とセキュリティ強化について、具体的な理由を挙げて説明する。

プライバシー保護：①選択的共有、②自己管理、③データ漏洩リスクの軽減 (図表 3)

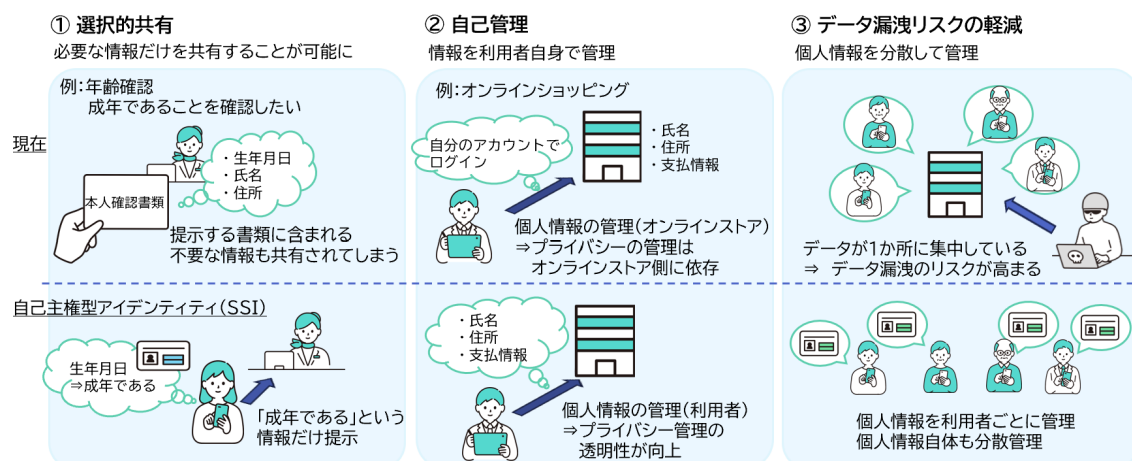
①選択的共有について、SSI では従来の手法と比較して必要最低限の情報だけを共有することが可能となる。例えば年齢確認が必要な場合、現在はマイナンバーカードや運転免許証等の身分証明書を提示するが、その際に年齢以外の情報 (氏名や住所、運転免許資格等) も共有されてしまう。これが SSI では「年齢条件を満たす」という事実だけを証明することで、それ以外の不要な情報の共有を避けることができる。

また、②自己管理について、SSI では第三者に依存せず、利用者自身で個人情報や資格情報を管理する。例えば、オンラインショッピングを行う場合、現在は事前に利用者の氏名や住所、支払情報等を登録、その情報はオンラインストア側で管理され、購入時に登録した情報を利用する方法が一般的である。一方で、SSI では事前の登録等は不要となり、購入時に利用者が必要な情報をオンラインストアに提供する。個人情報等の管理をオンラインストアに依存せず、利用者自身で行うことで、プライバシー管理の透明性が向上する。

最後に、③データ漏洩リスクの軽減について、先述の通り SSI では利用者自身で個人情報や資格情報を管理するため、現在は一般的なサイロ型やフェデレーション型のように個人情報等がいくつか所に集中することがなくなる。それにより、データ漏洩リスクが軽減される。

⁴ European Commission (EC) ウェブサイト、[EU Digital Identity Wallet](#) より

図表 3 自己主権型アイデンティティ（SSI）で期待されるプライバシー保護のイメージ

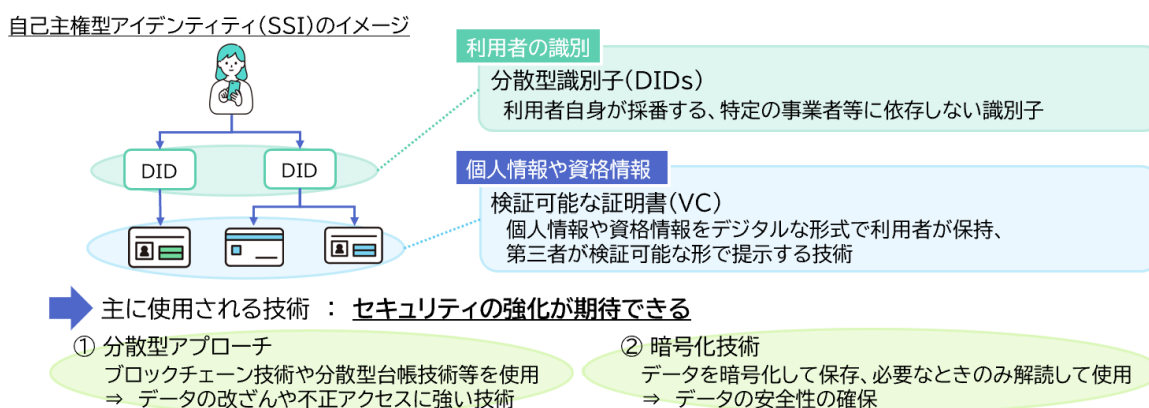


（出所）宮入暢子 [2024] 「[自己主権型・分散型モデルによる新たなデジタルアイデンティティと研究者識別子への応用可能性](#)」『情報の科学と技術』一般社団法人情報科学技術協会（2024 年 74 巻 3 号 pp. 92-98）等、各種資料より大和総研作成（イラストはソコスト（<https://soco-st.com/>））

セキュリティ強化：①分散型アプローチ、②暗号化技術（図表 4）

SSI を実現するための具体的な手法の一例として、利用者を識別するために用いる分散型識別子（Decentralized Identifiers、以下 DID）や、デジタル証明書とも呼ばれる、個人情報や資格情報をデジタルな形式で証明する検証可能な証明書（Verifiable Credentials、以下 VC）がある。これらは、ブロックチェーン技術や分散型台帳技術⁵といわれる技術を用いることが多い。中央集権的に利用者の情報を管理する企業や機関に依存せず、データを分散的に管理することが可能なことから、①分散型アプローチともいわれる。使用する技術自体がデータの改ざんや不正アクセスに強い特徴を持ち、データを分散して管理することから、セキュリティの強化が期待できる。また DID や VC は、②暗号化技術も利用しており、データを必要な時のみ解読して使用することで安全性を確保できる。

図表 4 自己主権型アイデンティティ（SSI）で期待されるセキュリティ強化のイメージ



（出所）宮入暢子 [2024] 「[自己主権型・分散型モデルによる新たなデジタルアイデンティティと研究者識別子への応用可能性](#)」『情報の科学と技術』一般社団法人情報科学技術協会（2024 年 74 巻 3 号 pp. 92-98）等、各種資料より大和総研作成（イラストはソコスト（<https://soco-st.com/>））

⁵ ブロックチェーン技術については、大和総研の用語解説サイト WORLD「[ブロックチェーン](#)」を参照。

自己主権型アイデンティティ（SSI）の実現には課題も多い

このように、デジタルサービスの普及に伴うプライバシー保護やセキュリティ強化の観点から注目されている SSI だが、実現には大きく 4 つの課題が存在する（図表 5）。

1 つ目に技術的な課題として、SSI の実現には異なるシステムやプラットフォーム間でも利用可能な相互運用性が必須となる。さらに、利用者が国境を越えたデジタルサービスを利用することも一般化している現状も踏まえると、相互運用性には国際的標準が求められる。先述の DIDs や VC の標準化を進める W3C (World Wide Web Consortium) ⁶をはじめ、いくつかの国際的な標準化団体やフォーラムによって、標準化に向けた取り組みが進められてはいる。しかし、国際的に統一された標準はいまだ確立されていない。

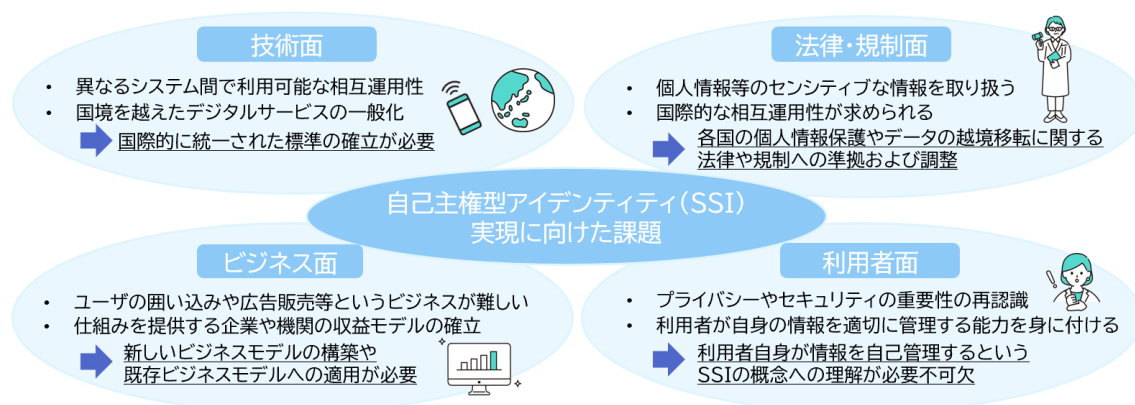
2 つ目は、法律・規制面の課題として、SSI で取り扱うのは個人情報等のセンシティブな情報であり、加えて国際的な相互運用性が必要となる。そのため、各国の個人情報保護やデータの越境移転に関する法律や規制への準拠および調整が必要となる。

3 つ目は、ビジネス面の課題として、新しいビジネスモデルの構築や既存のビジネスモデルへの適用が必要となる。SSI は利用者自身で個人情報や資格情報を管理する。そのため、現在のサイロ型やフェデレーション型のように、サービス提供側が中央集権的に利用者の情報を管理することができない。それに伴い、ユーザの囲い込みや広告販売等といった既存のビジネスモデルの維持が難しくなる。また、SSI を利用するための仕組みを提供する企業や機関（情報を共有する際に利用するアプリケーションの提供企業や VC 等の個人情報等をデジタルな形式で発行する機関等）の収益モデルの確立も必要となる。

最後に 4 つ目として、利用者の観点での課題として、利用者自身が情報を自己管理するという SSI の概念への理解が不可欠となる。先述の通り、現在のサイロ型やフェデレーション型のモデルでは、サービス提供側、すなわち中央集権的に利用者の情報を管理する企業や機関に、プライバシー管理やセキュリティ対策を委ねている。SSI では、このプライバシーやセキュリティについて、その重要性を再認識し、自身の情報を適切に管理する能力が求められる。そのためには、利用者への教育や、直感的に分かりやすいデザインの採用、利用が困難な人々への支援や代替手段の検討が重要となる。

⁶ W3C(World Wide Web Consortium)とは、WWWをはじめとする技術の標準化を行う国際的な非営利団体。2022 年に DIDs の規格 ([Decentralized Identifiers \(DIDs\) v1.0](#)) を標準規格として勧告している。

図表 5 自己主権型アイデンティティ (SSI) の実現に向けた課題



(出所) 大和総研作成 (イラストはソコスト (<https://soco-st.com/>))

4. デジタル化が進む中でプライバシーとセキュリティ意識が求められる

SSI は、デジタル化が進む現状を考えると理想的なアイデンティティの管理方法であるが、先述の通り多くの課題が存在する。特に、VC を含むデジタル証明書（デジタルな形式で提供される検証可能な証明書）においては既に本格的な運用が行われている⁷一方で、先述の EU の取り組みは進んでいるものの、DIDs（利用者を識別する分散型識別子）の普及にはまだ時間がかかると考えられる。そのため、現時点ではデジタル証明書を利用したアイデンティティ管理の具体化も進められている。例えば、アメリカの一部の州で導入が進められているモバイル運転免許証（mobile Driver's License、以下 mDL）では、州政府や特定の認証機関が、運転免許証のデジタル証明書や利用者の識別情報を発行および管理し、利用者は Apple ウォレットや Google ウォレット等のデジタルウォレットを通してこれを利用する。日本において検討が進められているマイナンバーカード機能のスマホ搭載も同様に、中央集権的に利用者の情報を管理する機関に依存する仕組みになる見込みだ。これらは、利用者の情報管理を中央集権的な機関に依存するため完全な SSI とはいえず、情報漏洩のリスク等は依然として残る。しかしながら、デジタル証明書によるプライバシー保護やセキュリティ強化については、SSI と比較すると効果は低くなるものの、現状の管理方法と比較すると一定の効果が期待される。

行政サービスにおいてもデジタル化が進められる中、日常生活で利用するさまざまなサービスが今後デジタル化されていくことが予想される。これらのサービスにおけるアイデンティティ管理が SSI の概念に沿って実現するかは、今後の国際社会の動向に左右されるだろう。しかし、従来オンラインで管理されていなかった個人情報や資格情報のデジタル化、すなわち VC を含むデジタル証明書によるアイデンティティの運用は本格的に進む可能性が高い。このようにデジタル化が急速に進行する現代社会において、自身の個人情報や資格情報がデジタル環境内でどのように管理されるのか、利用者一人ひとりがプライバシーとセキュリティに関する知識と意識を持つことが求められる。

以上

⁷ 日本における VC の活用事例としては、新型コロナワクチン接種アプリで表示される QR コードにおいて、SMART Health Cards という国際規格が採用されており、これは W3C（前掲脚注 4）の VC 規格に準拠している。