日本総研
The Japan Research Institute, Limited

自己主権型アイデンティティの動向と考察

～企業のデジタルアイデンティティ戦略へ向け～

株式会社 日本総合研究所
先端技術ラボ

2024年4月26日

本資料に関するお問い合わせ 市原紘平 (ichihara.kohei@jri.co.jp)

日本総研
The Japan Research Institute, Limited

サマリ ~自己主権型アイデンティティの動向と考察~

- デジタルアイデンティティへの注目の高まり
  - ✓ さまざまなITサービスの利便性向上へ向けた検討や、個人の属性情報に基づく広告ビジネスの隆盛などにより、デジタルな情報によるアイデンティティ(デジタルアイデンティティ)が注目されている。
  - ✓ 個人情報を大量集積するITプラットフォーマへの問題意識などから、個人が自身で自身のデータを扱う権限を持って自身のアイデンティティを管理するSelf-Sovereign Identity(SSI, 自己主権型アイデンティティ)というムーブメントも隆盛している。

- 関連技術の概要
  - ✓ Verifiable Credentials(VC, 検証可能な資格証明書)とは、属性情報を第三者に証明するためのデジタルの証明書の仕様。W3C(Webで使用される技術の国際標準化団体)によって標準化されている。保持者が、発行者から発行された対象者についてのVCを検証者へ提示する際に、電子署名技術や標準化されたデータ形式などによって、検証可能な資格証明を実現するもの。
  - ✓ Decentralized Identifiers(DIDs, 分散型識別子)とは、特定の事業者等に依存しない方式の識別子(Identifier)に関するデータモデル標準。W3Cによって標準化されている。他の技術と組み合わせることで自己主権型アイデンティティ(SSI)を実現し得るとされる。(SSIを実現する要素技術となり得るもの)

- 考察
  - ✓ アイデンティティ管理において自己主権型が最適解かは、ユーザのニーズや知識水準を考慮して慎重に判断する必要がある。ユーザの利便性や安全性が向上せず、イデオロギーを押し付けるだけになってしまうとユーザや社会からの理解は得られない。
  - ✓ 企業側の検討余地として、データを自身で管理するというユーザの能動的な行動が、コミュニティへの帰属感や企業へのエンゲージメント向上へつながるという仮説[1]を立てられるのではないか。
  - ✓ 一方、政府のデジタルアイデンティティの取り組みとして、『公的個人認証サービスと紐付けられた民間ID』[2]があり、本人確認が確実に行われた民間IDは活用の幅が広く、企業としては目的志向で最適なデジタル戦略を採ることが望まれる。

[1] https://www.smfg.co.jp/dx_link/article/0072.html
[2] https://www.soumu.go.jp/main_content/000762342.pdf

日本総研
The Japan Research Institute, Limited

自己主権型アイデンティティの動向 目次

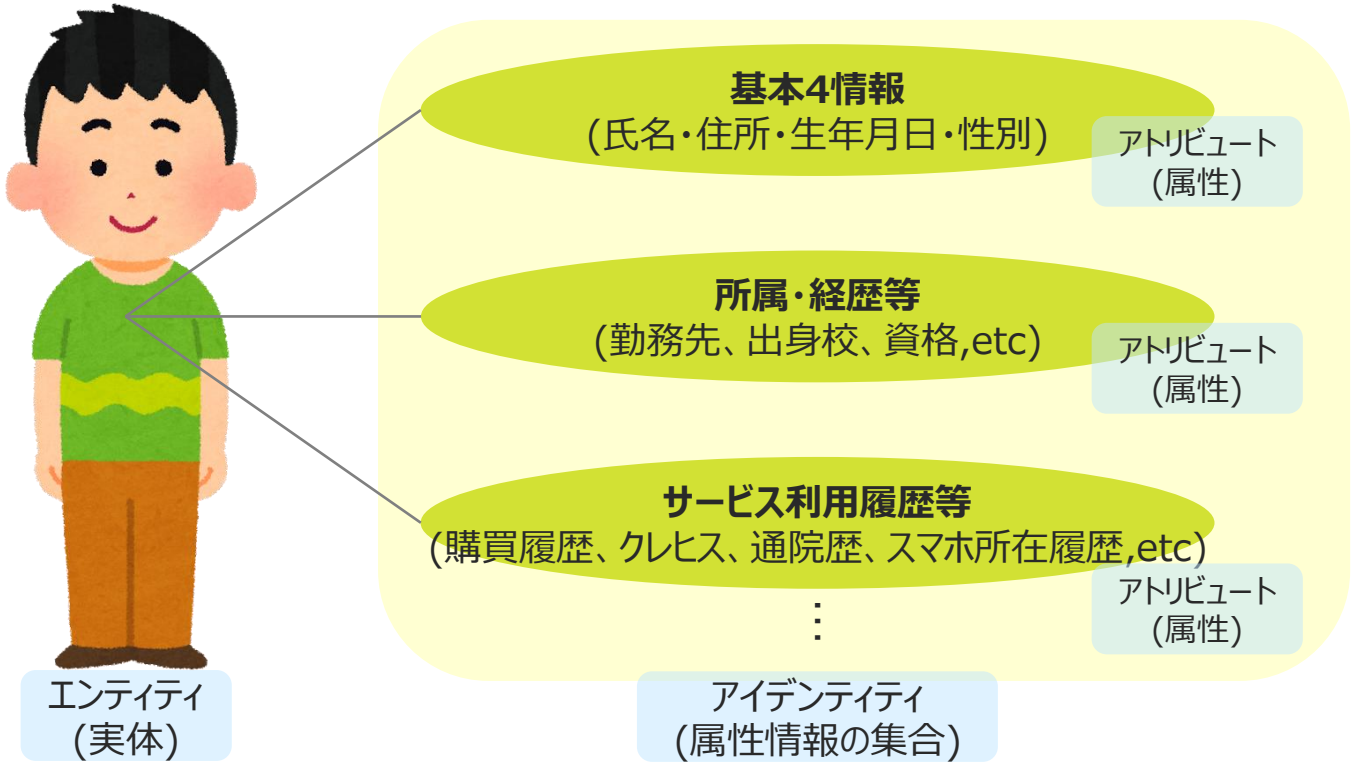
1章 自己主権型アイデンティティの概要

- 1.1 アイデンティティとは
- 1.2 デジタルアイデンティティと自己主権型アイデンティティ

日本総研
The Japan Research Institute, Limited

1.1 アイデンティティとは

- アイデンティティとは、『実体に関する属性情報の集合』(国際標準化機構(ISO)による定義)[1]
- 「ISO/IEC 24760-1:2019 Information security, cybersecurity and privacy protection」[1]では関連用語が以下のように定義される。
  - エンティティ(entity)：明確に存在が区別されるドメインの運用目的に関連するアイテム
  - アトリビュート(attribute)：エンティティの特性または性質
  - アイデンティティ(identity)：エンティティに関連するアトリビュートの集合



[1] https://www.iso.org/standard/77582.html

日本総研 The Japan Research Institute, Limited

1.2 デジタルアイデンティティと自己主権型アイデンティティ

- さまざまなITサービスの利便性向上へ向けた検討や、個人の属性情報に基づく広告ビジネスの隆盛などにより、デジタルな情報によるアイデンティティ(デジタルアイデンティティ[1])が注目されている。
- 個人情報を大量集積するITプラットフォーマへの問題意識などから、個人が自身で自身のデータを扱う権限を持って自身のアイデンティティを管理するSelf-Sovereign Identity(SSI, 自己主権型アイデンティティ)というムーブメントも隆盛している。
- 現在用いられているOpen ID Connectといった技術によるアイデンティティ管理を『ユーザ中心アイデンティティ』とした上で、次のフェーズとして自己主権型アイデンティティがあるとする専門家もいる。(セキュリティプロトコルTLS1.0の作成者の1人としても著名なクリストファー・アレン氏)

クリストファー・アレン氏によるデジタルアイデンティティ管理進展の解説[2]

段階	名称	概略	利用技術等	推進団体等
Phase 1	集権型アイデンティティ (Centralized Identity)	単一、または一部階層化された管理権限域によるコントロール	• Domain Name System(DNS) • 公開鍵認証局(CA)	• IANA • ICANN
Phase 2	フェデレイティッドアイデンティティ (Federated Identity)	複数の管理権限域間の連合によるコントロール	• Microsoft Passport • Liberty Alliance	• Microsoft • Sun Microsystems*
Phase 3	ユーザ中心アイデンティティ (User-Centric Identity)	複数の管理権限域をまたいだ個人または管理者によるコントロール	• OpenID, Open ID Connect, OAuth, FIDO	• OIDF(Open ID Foundation), IIW, ASN
Phase 4	自己主権型アイデンティティ (Self-Sovereign Identity)	複数の管理権限域をまたいだ個人によるコントロール	• VC(Verifiable Credentials) • DIDs(Decentralized Identifiers)	• W3C, OIDF, DIF(Decentralized Identity Foundation)

*2010年Oracleにより吸収合併

[1] NIST SP 800-63(https://pages.nist.gov/800-63-3/)では『"Digital identity is the unique representation of a subject engaged in an online transaction."[仮訳]「デジタルIDは、オンライン取引に関与する主体を一意に表現したもの」』とされている。
[2] Christopher Alen, “The Path to Self-Sovereign Identity”, Life With Alacrity, 2016/4/26, https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/などから弊社作成。なお、アレン氏はTLSの共著者として知られる。

日本総研 The Japan Research Institute, Limited

[参考]自己主権型アイデンティティの説明と10原則

- Sovrin Foundation(SSIに関するガバナンスフレームワークの1つを管理する非営利団体)による自己主権型アイデンティティ(SSI)の説明は以下の通り。(弊社仮訳)なお、SSIはムーブメントを表す用語であり特定の技術や仕様を表すものではない。
  - ✓『自己主権型アイデンティティ(SSI)は、個人が行政当局の介入なしに自分のアイデンティティを所有および管理する必要があると認識するデジタルムーブメントを表すために使用される用語』[1]
  - ✓『SSIとは、個人(または組織)がアイデンティティを構成する要素を管理し、それらの資格情報へのアクセスをデジタル的に制御することを意味する。SSIでは、個人データを管理する権限は個人にあり、これらの資格情報へのアクセスを許可または追跡する管理上の第三者ではない。』[1]
- クリストファー・アレン氏(著名セキュリティ専門家)は、以下の『自己主権型アイデンティティの10原則』[2]も提唱している。(弊社仮訳)

項番	原則	概略
1	存在 (Existence)	『ユーザは独立した存在であり、デジタル上のみの存在であることはない。』
2	コントロール (Control)	『ユーザは自分のアイデンティティ、プライバシー、または名声を好みに応じてコントロールする必要がある。』
3	アクセス (Access)	『ユーザは自分のデータにアクセスできる必要がある。ゲートキーパーはおらず、何も隠されない。』
4	透明性 (Transparency)	『システムとアルゴリズムはオープンで透明でなければならない。』
5	永続性 (Persistence)	『アイデンティティはユーザが望む限り存続する必要がある。』
6	ポータビリティ (Portability)	『アイデンティティに関する情報とサービスは、ユーザが持ち運び可能である必要がある。』
7	相互運用性 (Interoperability)	『アイデンティティは可能な限り広く使用できる必要がある。 例えば国境を越える。』
8	同意 (Consent)	『ユーザは、自分のアイデンティティ情報がどのように使用されるかについて自由意志の下に同意する必要がある。』
9	最小化 (Minimization)	『アイデンティティに関する主張の開示は可能な限り少なくする必要がある。』
10	保護 (Protection)	『個々のユーザの権利は、強権から保護されなければならない。』

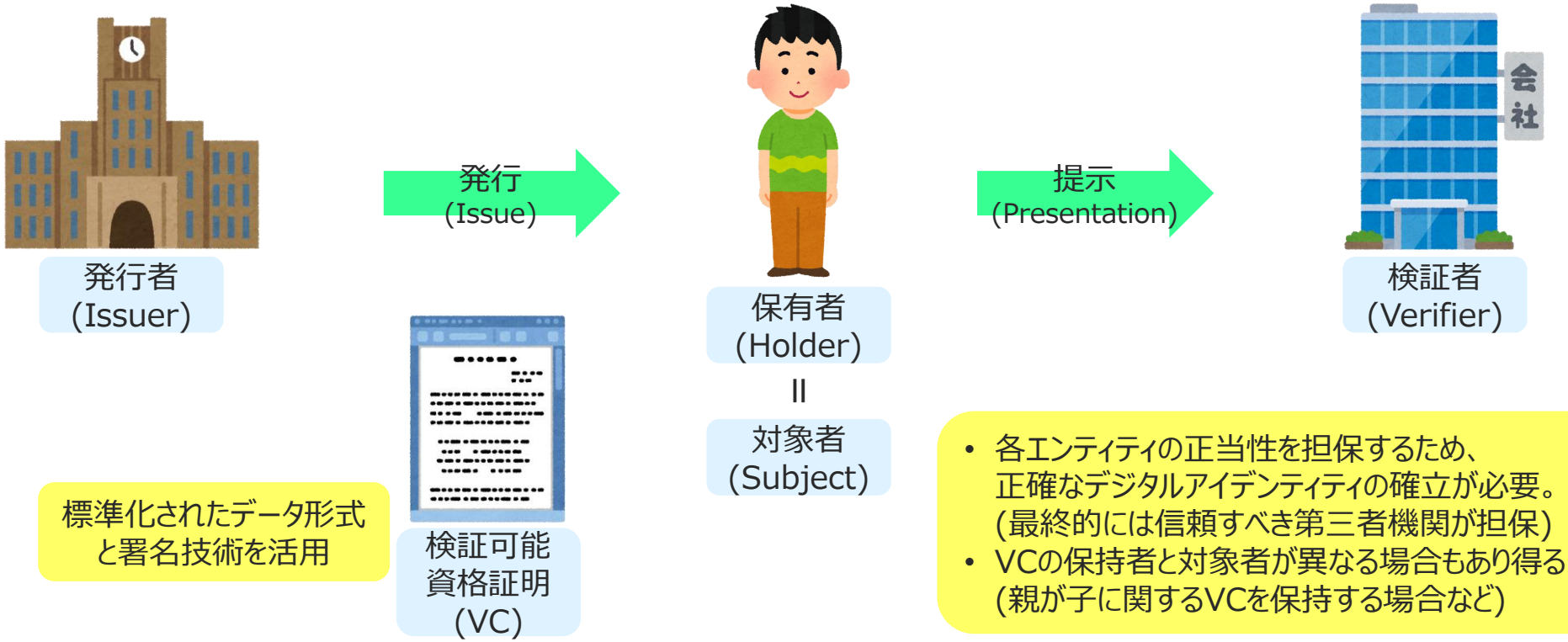
[1] Sovrin Foundation, "What is self-sovereign Identity?", Sovrin Foundation, 2018/12/6, https://sovrin.org/faq/what-is-self-sovereign-identity/ (accessed on 2024/4/1)
[2] Christopher Alen, "Self-Sovereign Identity - Ideology & Architecture", SSIMEETUP, 2020/3/16, https://ssimeetup.org/self-sovereign-identity-why-we-here-christopher-allen-webinar-51/ (accessed on 2024/4/1)

2章 デジタルアイデンティティ関連技術の概要

- 2.1 Verifiable Credentials(VC, 検証可能な資格証明書)
- 2.2 Decentralized Identifiers(DIDs, 分散型識別子)

2.1 Verifiable Credentials(VC, 検証可能な資格証明書)

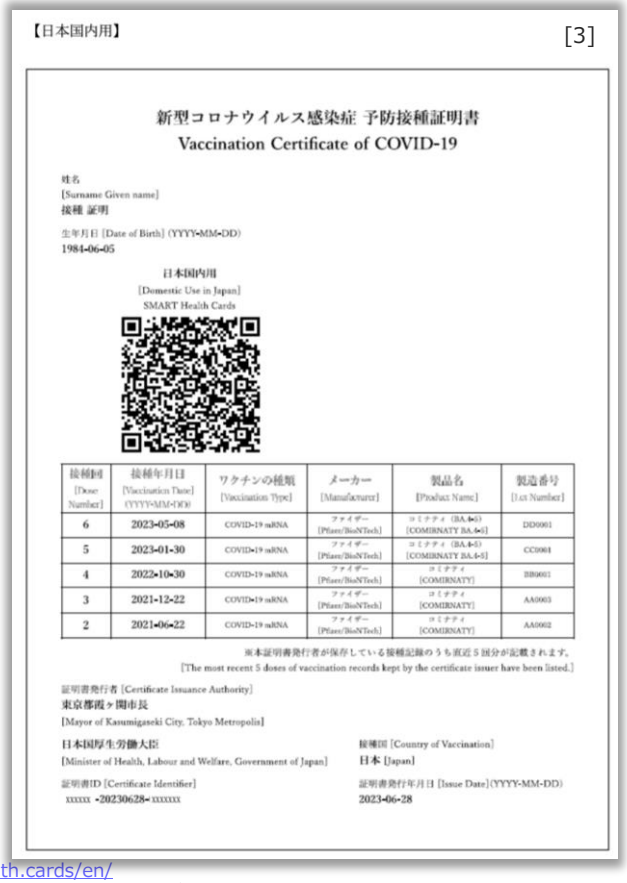
- Verifiable Credentials(VC, 検証可能な資格証明書)とは、属性情報を第三者に証明するためのデジタルの証明書の仕様。W3C(Webで使用される技術の国際標準化団体)によって標準化されている。[1]
- 保有者(Holder)が、発行者(Issuer)から発行された対象者(Subject)についてのVCを検証者(Verifier)へ提示する際に、電子署名技術や標準化されたデータ形式などによって、検証可能な資格証明を実現する。



[1] Verifiable Credentials Data Model v1.1, https://www.w3.org/TR/vc-data-model/

[参考]Verifiable Credentialsの実用例 - 新型コロナワクチン接種証明書アプリ(デジタル庁)

- 日本のデジタル庁が公開した「新型コロナワクチン接種証明書アプリ」で表示されるQRコードは、SMART Health Card[1]という仕様のデータであるが、これはW3CのVC(Verifiable Credentials)に準拠している。
  発行者(Issuer)には、デジタル庁の下のURLが記載されている。("iss": "https://vc.vrs.digital.go.jp/issuer")[2]
- また、対象者(Subject)は、DID(後述)で指定されていない。("credentialSubject":配下にDIDの記載はない。)
- このように、VCとDIDは併せて語られることが多いが、セットで用いる必要はなく[2]、VCは既に本格的に実用されている。



【日本国内用】 [3]

新型コロナウイルス感染症 予防接種証明書
Vaccination Certificate of COVID-19

姓名
[Surname Given name]
接種 証明

生年月日 [Date of Birth] (YYYY-MM-DD)
1984-06-05

日本国内用
[Domestic Use in Japan]
SMART Health Cards

接種回 [Dose Number]	接種年月日 [Vaccination Date] (YYYY-MM-DD)	ワクチンの種類 [Vaccination Type]	メーカー [Manufacturer]	製品名 [Product Name]	製造番号 [Lot Number]
6	2023-05-08	COVID-19 mRNA	ファイザー [Pfizer/BioNTech]	コミナティ（BA.4-5） [COMIRNATY BA.4-5]	DD0001
5	2023-01-30	COVID-19 mRNA	ファイザー [Pfizer/BioNTech]	コミナティ（BA.4-5） [COMIRNATY BA.4-5]	CC0001
4	2022-10-30	COVID-19 mRNA	ファイザー [Pfizer/BioNTech]	コミナティ [COMIRNATY]	BB0001
3	2021-12-22	COVID-19 mRNA	ファイザー [Pfizer/BioNTech]	コミナティ [COMIRNATY]	AA0003
2	2021-06-22	COVID-19 mRNA	ファイザー [Pfizer/BioNTech]	コミナティ [COMIRNATY]	AA0002

※本証明書発行者が保存している接種記録のうち直近5回分が記載されます。
[The most recent 5 doses of vaccination records kept by the certificate issuer have been listed.]

証明書発行者 [Certificate Issuance Authority]
東京都霞ヶ関市長
[Mayor of Kasumigaseki City, Tokyo Metropolis]

日本国厚生労働大臣
[Minister of Health, Labour and Welfare, Government of Japan]

接種国 [Country of Vaccination]
日本 [Japan]

証明書ID [Certificate Identifier]
xxxxx -20230628- xxxxxx

証明書発行年月日 [Issue Date] (YYYY-MM-DD)
2023-06-28

- 『SMART Health Cards規格：民間IT企業の共同プロジェクト「VCI」が策定した健康証明書用の規格。』[4]
  「接種アプリ」では国内用QRコードの規格として採用されている。
- 「海外用+国内用」はVDS-NC(ICAO)という別規格。[4]
  『ICAO VDS-NC規格：国連専門機関の一つである国際民間航空機関(ICAO)が策定した健康証明書用の規格。』[4]

[1] https://smarthealth.cards/en/
[2] 富士榮 尚寛, "分散型IDと検証可能なアイデンティティ技術概要", SlideShare, 2022/7/29, https://www.slideshare.net/naohiro.fujie/id-252360106 (accessed on 2024/4/1)
[3] https://www.mhlw.go.jp/content/001117346.pdf
[4] https://www.digital.go.jp/policies/vaccinecert/faq_06

[参考]Verifiable Credentialsの実態 - JSON-LD形式の例

- VCのJSON-LD形式での記載例(Verifiable Credentials Data Model v1.1[1]より)は以下の通り。
  (JSON-LD(JavaScript Object Notation for Linked Data)はJSONを利用してLinked Dataを表現する手法)

EXAMPLE 1: A simple example of a verifiable credential

```
{
  // set the context, which establishes the special terms we will be using
  // such as 'issuer' and 'alumniOf'.
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  // specify the identifier for the credential
  "id": "http://example.edu/credentials/1872",
  // the credential types, which declare what data to expect in the credential
  "type": ["VerifiableCredential", "AlumniCredential"],
  // the entity that issued the credential
  "issuer": "https://example.edu/issuers/565049",
  // when the credential was issued
  "issuanceDate": "2010-01-01T19:23:24Z",
  // claims about the subjects of the credential
  "credentialSubject": {
    // identifier for the only subject of the credential
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    // assertion about the only subject of the credential
    "alumniOf": {
      "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",
      "name": [{
        "value": "Example University",
        "lang": "en"
      }, {
        "value": "Exemple d'Université",
        "lang": "fr"
      }]
    }
  },
```

発行者(Issuer)

証明内容

対象者(Subject)

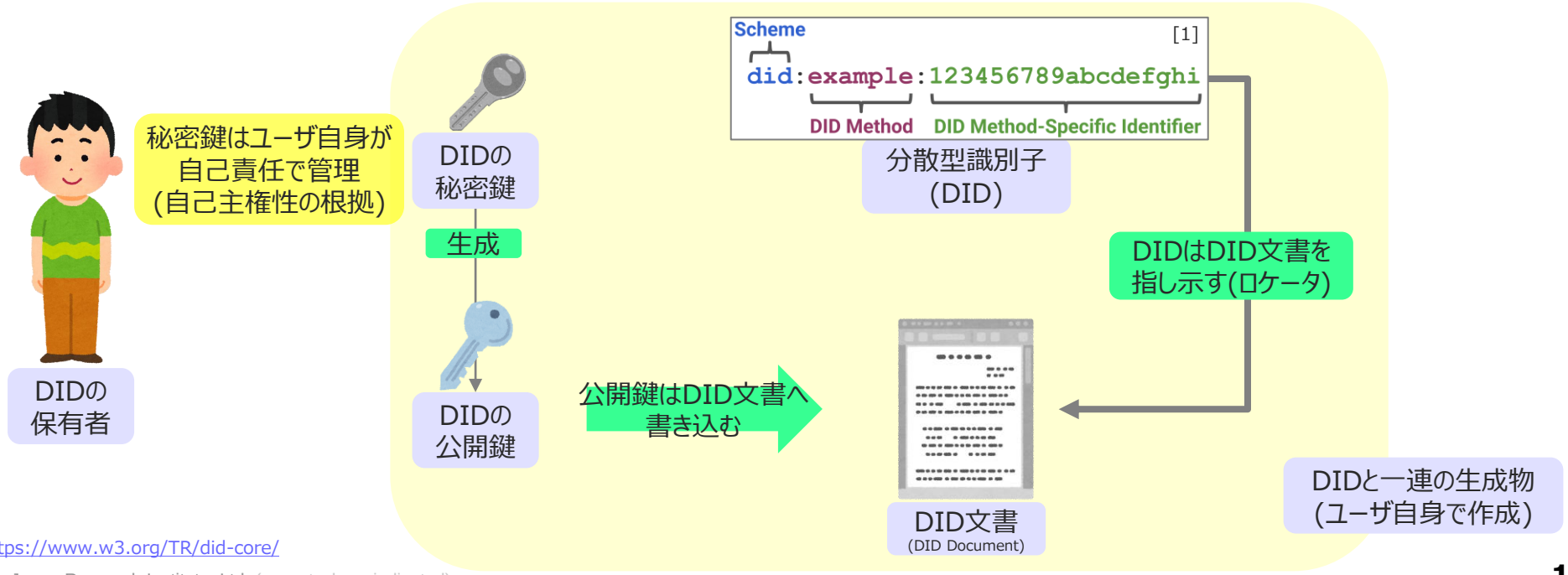
紙面都合上以下割愛

- 例では対象者をDID(後述)で指定しているが、必ずしもDIDで示す必要はない。
  (VCはあくまでデジタル署名されたデータセット)

[1] Verifiable Credentials Data Model v1.1, https://www.w3.org/TR/vc-data-model/

2.2.1 Decentralized Identifiers(DIDs, 分散型識別子)の概要

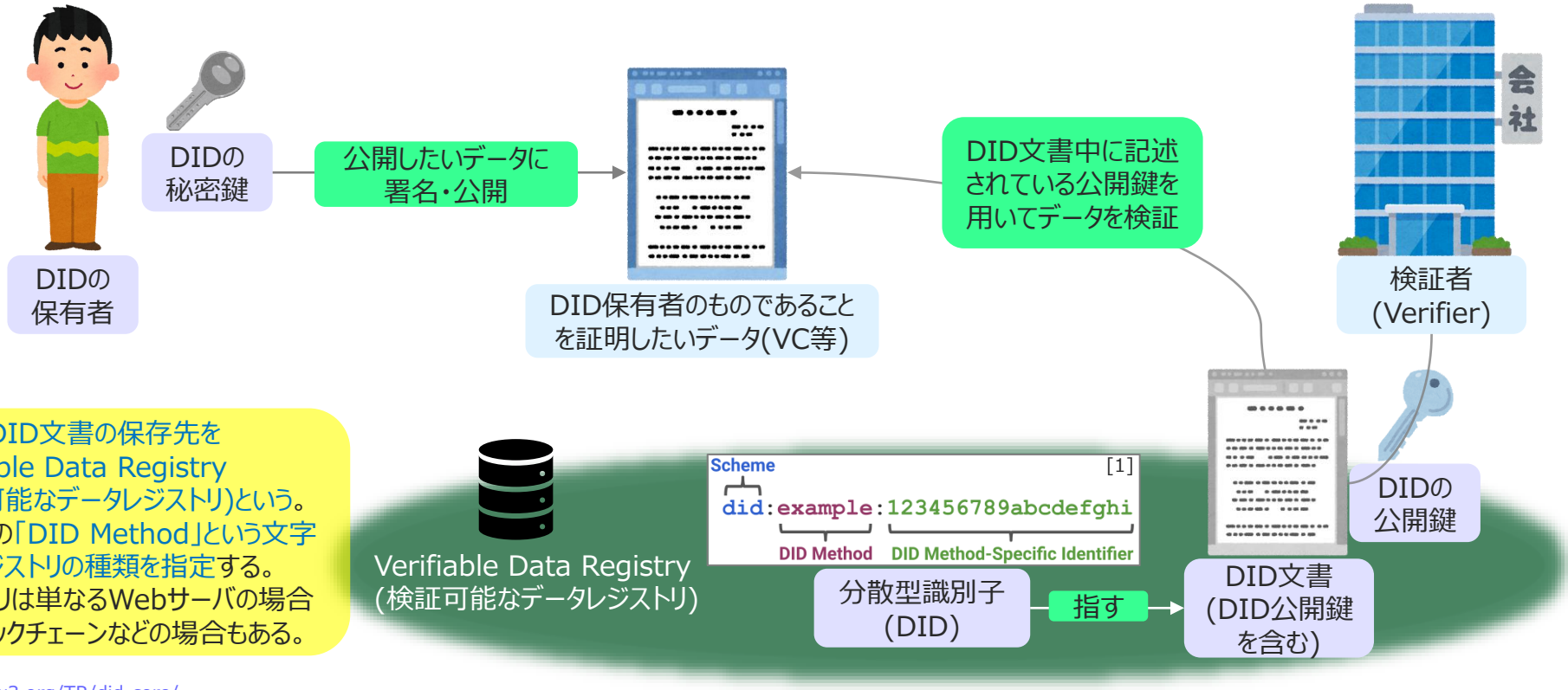
- Decentralized Identifiers(DIDs, 分散型識別子)とは、特定の事業者等に依存しない方式の識別子(Identifier)に関するデータモデル標準。W3Cによって標準化されている。[1]
- 他の技術と組み合わせることで、自己主権型アイデンティティ(SSI)を実現し得るとされる。(SSIを実現する要素技術となりうるもの)
  - ユーザが自身で秘密鍵・公開鍵のペアを用意し、鍵ペアに紐付いたDIDを作成する。(DIDsは各ユーザが自身で採番する)
    秘密鍵を自己管理することで特定の事業者などに依存せず、識別子を自身で「保有」していると主張される。
- 実態はURI(Uniform Resource Identifier: URLのようにネット上のリソースを特定するための記号の並び)で、「did」という文字列から始まる。(URIの最初の部分の文字列(本件ではdid)をScheme(スキーマ)という)
  - DIDはDID文書(DID Document)を指し、DID文書はDIDに紐付く公開鍵やDIDで示される主体に関するデータ等を含む。
    DID、DID文書は公開情報となるため、個人情報(個人につながる可能性のあるものを含む)を含めないよう注意する必要がある。



[1] https://www.w3.org/TR/did-core/

2.2.2 Decentralized Identifiers(DIDs, 分散型識別子)の用法

- DIDに紐付く秘密鍵でデータに署名し公開した後、検証者がDID文書上の公開鍵でデータを署名検証することで、DIDの保有者が発行したデータ(VC等)であるかを検証できる。
  - ユーザはDIDで示したい内容に応じて、都度DID(及び紐付く鍵ペアやDID文書)を作成し、使い分けることで主体的に公開したい情報をコントロールできる。
- DIDやDID文書の保存先は様々な形式が想定されており、「メソッド」として規定されている。
  - 保存先がパブリックブロックチェーン等の場合は、識別子の記録の特定の主体への依存度を特に下げることができる一方、情報の削除ができなくなるため特に注意が必要となる。また、データの書き込みには基本的に暗号資産による支払いが必要。



- DIDやDID文書の保存先をVerifiable Data Registry(検証可能なデータレジストリ)という。
- DID中の「DID Method」という文字列でレジストリの種類を指定する。
- レジストリは単なるWebサーバの場合も、ブロックチェーンなどの場合もある。

[1] https://www.w3.org/TR/did-core/

3章 自己主権型アイデンティティに関する考察

- 3.1「自己主権型アイデンティティの10原則」充足性評価
- 3.2 まとめ

日本総研 The Japan Research Institute, Limited

3.1「自己主権型アイデンティティの10原則」充足性評価

- 『自己主権型アイデンティティの10原則』[1]が、VCやDIDsといった技術によってどの程度充足可能か検討した。(下表)
  - 関係者(保有者・発行者等)の振る舞いや法制度など、技術以外の側面に依存する部分が多く見られる。
  - データへのアクセス性や永続性の観点からブロックチェーン活用の可能性がある一方、データ削除ができない点は注意を要する。

項番	原則	概略 (弊社仮訳)	評価 (筆者考察)	
1	存在 (Existence)	『ユーザは独立した存在であり、デジタル上のみの存在であることはない。』	発行者依存	・自己主権型アイデンティティ(SSI)の発行にあたり、発行者が実在性を確認することで可能。
2	コントロール (Control)	『ユーザは自分のアイデンティティ、プライバシー、または名声を好みに応じてコントロールする必要がある。』	保有者依存	・技術的には可能。保有者が都度DIDsを作成、管理する必要があるため高いスキルとアクションを要する。
3	アクセス (Access)	『ユーザは自分のデータにアクセスできる必要がある。ゲートキーパーはおらず、何も隠されない。』	基盤依存	・パブリックブロックチェーン等アクセスを妨げられない基盤や、自前のサーバに記録した場合、実現可能。
4	透明性 (Transparency)	『システムとアルゴリズムはオープンで透明でなければならない。』	○	・公開されている標準化技術を用いれば満たす。
5	永続性 (Persistence)	『アイデンティティはユーザが望む限り存続する必要がある。』	基盤依存	・自前のサーバにDIDsを記録した場合、実現可能。(ブロックチェーンの場合、逆にデータの削除が不可能)
6	ポータビリティ (Portability)	『アイデンティティに関する情報とサービスは、ユーザが持ち運び可能である必要がある。』	△	・DIDsを用いた場合、現状メソッドをまたいだ可搬性はない。(別の基盤へは別途発行する必要あり)
7	相互運用性 (Interoperability)	『アイデンティティは可能な限り広く使用できる必要がある。 例えば国境を越える。』	法制依存	・各法域において公に認められるかは各国の法制次第。
8	同意 (Consent)	『ユーザは、自分のアイデンティティ情報がどのように使用されるかについて自由意志の下に同意する必要がある。』	保有者依存	・保有者が自己責任で行うため、結果を正しく予測できる判断力や知識が必要。
9	最小化 (Minimization)	『アイデンティティに関する主張の開示は可能な限り少なくする必要がある。』	保有者依存	・技術的には可能。保有者が自己責任で行うため、正確な判断力に加え高いスキルと都度のアクションが必要。
10	保護 (Protection)	『個々のユーザの権利は、強権から保護されなければならない。』	法制依存	・各法域において公にどの程度保護されるかは各国の法制次第。

[1] Christopher Alen, "Self-Sovereign Identity - Ideology & Architecture", SSIMEETUP, 2020/3/16, https://ssimeetup.org/self-sovereign-identity-why-we-here-christopher-allen-webinar-51/ (accessed on 2024/4/1)

日本総研 The Japan Research Institute, Limited

3.2 まとめ

- エンドユーザ観点
  - ✓ 自己主権型アイデンティティ(SSI)は、その名の通り、ユーザ自身で自己のアイデンティティを管理するため、管理の責任もユーザ自身が負うこととなる。(前頁p.14の表でも確認の通り)
  - ✓ 「10原則」[1]以外の観点として、自己の情報の共有先の信頼性を自身で判断し、自己責任で情報提示する必要もある。しかし、専門家でない個人がWeb上でアクセス先の信頼性を自身で確認するのは現実的に困難。このため、一般個人への利用拡大には、信頼できる第三者機関(例えば政府や業界団体等)が、ホワイトリスト(安全なアクセス先であることを確認したリスト)を用意するといった対応が必要ではないか。
  - ✓ アイデンティティ管理において自己主権型が最適解かは、ユーザのニーズや知識水準を考慮して慎重に判断する必要がある。利便性や安全性が向上せず、単に「自己主権型が理想である」という(推進団体等からの)イデオロギーの押し付けとなってしまうとユーザや社会からの理解は得られない。

- 企業側観点
  - ✓ 自己主権型アイデンティティ(SSI)に関連して、検証可能な資格情報等をユーザに提供する側になる可能性のある企業側の戦略としても、顧客の情報は貴重であり、基本的には自社で収集・囲い込みをしようとすると考えられる。
  - ✓ 企業側として自己主権型の取り組み意義を模索するとすれば、顧客との密なコミュニティの形成に検討余地があるのではないか。データを企業側に管理されるのではなく自身で管理するという能動的な行動が、コミュニティへの帰属感や企業へのエンゲージメント向上へつながるのではないかという仮説[2]を立てることができる。(ただし、本仮説について実証的な効果測定をした事例は現状見当たらない)

- 政府によるデジタルアイデンティティの観点
  - ✓ 政府によるデジタルアイデンティティ関連の取組として、『公的個人認証サービスと紐付けられた民間ID』[3]がある。
  - ✓ マイナンバーカードの公的個人認証サービスによって本人確認が確実に行われた民間IDは、本人性が求められる手続きをWebで可能にするなど、活用の幅が広い。
  - ✓ 自身の情報へのアクセス性やシステムの透明性、サービスの永続性などを求めることで、「10原則」[1]を満たす設計も可能である。
  - ✓ 政府に信頼を依拠することで便利で安全なアイデンティティ管理が実現する可能性が考えられ、企業としても目的志向で最適なデジタル戦略を採ることが望まれる。

[1] Christopher Alen, "Self-Sovereign Identity - Ideology & Architecture", SSIMEETUP, 2020/3/16, https://ssimeetup.org/self-sovereign-identity-why-we-here-christopher-allen-webinar-51/ (accessed on 2024/4/1)
[2] https://www.smfg.co.jp/dx_link/article/0072.html
[3] https://www.soumu.go.jp/main_content/000762342.pdf

[参考]SBTと自己主権型アイデンティティ

- SBTとは
  - SBT(Soulbound Token)とは、ブロックチェーン上のアカウントへ発行された後、移転ができないNFT。
    (アカウントに紐付いて移転しないことから、同種の技術仕様をAccount Bound Tokenともいう)
    なお、NFT(Non-Fungible Token)とは、1つ1つのトークンが識別可能な固有のトークン。
  - アカウントから移転できない識別可能な固有のトークンであるSBTをブロックチェーンアカウントへ発行することで、
    そのアカウントがどういったアカウントであるのかといった情報をブロックチェーン上で示すことができる。

- SBTとVC/DID
  - SBTが参照する外部のメタデータとしてVCを指定する、さらにそのVCの持ち主であることをDIDを用いて検証させるなど、
    SBTとVC/DIDは組み合わせて使用することが可能。
  - DID(及びDID文書)同様、公開するデータに個人情報を含まないように注意する必要がある。
    特にブロックチェーンは一度公開したデータを削除することができないため要注意。

- SBTによるアイデンティティ提示の具体例
  - VCなどを組み合わせた事例か不明ながら、SBTによって身元を確認する事例として、トークン化された証券に対する投資の有資格性をSBTを用いて確認可能した、ドイツ銀行シンガポール支店のトライアル[1]が存在する。

[1]Zhiyuan Sun, “ドイツ銀行、トークン化された投資プラットフォームのトライアルを完了”, Cointelegraph, 2023/2/22, https://jp.cointelegraph.com/news/deutsche-bank-completes-trial-of-tokenized-investment-platform

日本総研 The Japan Research Institute, Limited

[参考]分散型アイデンティティ(Decentralized Identity)

- Decentralized Identifiers(DIDs, 分散型識別子)と混同しやすい用語として、Decentralized Identity(分散型アイデンティティ)が存在する。
  - 標準化団体(W3C)によって規定された標準化技術であるDecentralized Identifiers(DIDs, 分散型識別子)と違い、Decentralized Identity(分散型アイデンティティ)は特定の技術仕様を指す言葉ではない。
  - むしろ、自己主権型アイデンティティ(SSI)同様、ある種のムーブメント(あるいは、理念、イデオロギー)を指すものとして使用されているように見て取れる。特に、特定のアイデンティティプロバイダーへの依存度を下げるという点を強調して捉えている例も見られるが、本質的に自己主権型アイデンティティ(SSI)と違いがない。

- Microsoft社による解説[1]も以下の通りであり、明確に自己主権型アイデンティティの言い換えと表現している。
  - ✓ 『自己主権型アイデンティティとも呼ばれる分散型アイデンティティは、自己所有で独立しており、信頼できるデータ交換を可能にするデジタル識別子と検証可能な資格情報を使用するオープンスタンダードベースのアイデンティティフレームワークです。ブロックチェーン、分散台帳技術、秘密/公開キー暗号化を使用して、プライバシーを保護し、オンラインでのやり取りを安全にすることを目的としています。』(弊社仮訳)

[1] https://www.microsoft.com/en-us/security/business/solutions/decentralized-identity

お問い合わせ

- 本稿は、作成日時点で弊社が信頼できると考えた資料に基づき作成したものですが、情報の正確性・完全性・有用性・安全性等を保証するものではありません。また、実際の技術動向等は経済情勢等の変化により本レポートの内容と大きく異なる可能性もあります。ご了承ください。

本件に関するお問い合わせ・ご確認は、以下までお願いいたします。

株式会社日本総合研究所　先端技術ラボ

101360-advanced_tech@ml.jri.co.jp

市原 紘平　ブロックチェーン・スペシャリスト　ichihara.kohei@jri.co.jp

株式会社
日本総合研究所

東京本社
〒141-0022
東京都品川区東五反田2-18-1
大崎フォレストビルディング