分散型IDを活用した証明書のデジタル化と課題

鈴木茂哉

慶應義塾大学大学院政策・メディア研究科 特任教授

慶応義塾大学SFC研究所ブロックチェーン・ラボ 副所長（技術統括)

@ CAUA Forum - 2021/8/5

本日のプレゼンテーション

- デジタル化された証明書と自己主権型アイデンティティ
- Decentralized Identifier (DID), Verifiable Credentials についての概要
- 応用事例
- 活用における課題

鈴木 茂哉

慶應義塾大学大学院 政策・メディア研究科 特任教授 / 博士 (政策・メディア)

Shigeya Suzuki, Ph.D

Project Professor,
Graduate School of Media and Governance, Keio University

shigeya@wide.ad.jp
shigeya@keio.jp

主たる研究領域

ネットワーク化されたセキュアな情報システムの設計 / 開発 / 構築

情報システムアーキテクチャ / コンピューターネットワーク / 分散システム / デジタルアイデンティティ / ネットワークシステムセキュリティ / 量子インターネット

現在の主たる肩書き・活動等

慶應義塾大学SFC研究所ブロックチェーンラボラトリ副所長(技術統括)
慶應義塾大学SFC研究所Auto-ID Labs Japan副所長
WIDEプロジェクト ボードメンバ/研究者
Trusted Web推進協議会タスクフォースメンバ
(内閣官房デジタル市場競争会議)
W3C DID WG / Credentials CCG メンバ

Recent Papers and Other works　最近の主な研究業績

DID Core Specification Test Suite and Implementaiton Report *(2021)*
Orie Steele, Shigeya Suzuki, Manu Sporny, Markus Sabadello (Editors)
World Wide Web Consoritium, 30 July 2021
Identity

Attacking the Quantum Internet *(2021)*
Takahiko Satoh, Shota Nagayama, Shigeya Suzuki, Takaaki Matsuo,
Michal Hajdušek, Rodney Van Meter.
IEEE Transactions on Quantum Engineering (Early Access Available)
Security Quantum Internet

Trusted Web ホワイトペーパ *(2021)*
Trusted Web推進協議会 (内閣官房デジタル市場競争会議)
Identity Privacy Blockchain

Multistakeholder Governance for the Internet *(2020)*
Shigeya Suzuki, Financial Cryptography and Data Security.
FC 2020, LNCS vol 12063. Springer, Cham.
Multistakeholder Governance

ニューノーマル時代における人間の社会活動を支える情報基盤の在り方と
デジタルアイデンティティの位置づけ (ディスカッションペーパ 2020)
村井 純、鈴木 茂哉、松尾 真一郎、クロサカタツヤ
慶應義塾大学SFC研究所 ブロックチェーン・ラボ
Identity Privacy Blockchain

令和元年度: ブロックチェーン技術等を用いた金融システムのガバナンスに関する研究
[慶應義塾大学SFC研究所との合同研究]
金融庁 総合政策局 総合政策課 フィンテック室
Blockchain Decentralized Fiance Multistakeholder Governance

Design and Operation Practicies of Service Chaining using NFV *(2018)*
Katsuhiro Horiba, Ryo Nakamura, Shigeya Suzuki, Yuji Sekiya, Jun Murai
IPSJ Transactions on Digital Practice
Network Virtualization

Mitigating Bitcoin Node Storage Size By DHT *(2018)*
Ryosuke Abe, Shigeya Suzuki, Jun Murai,
Asian Internet Engineering Conference 2018, Bangkok, Thailand
Scalability Blockchain

Blockchain as an Audit-able Communication Channel *(2017)*
Shigeya Suzuki, Jun Murai
STPSA 2017: The 12th IEEE International COMPSAC Workshop on Security,
Trust and Privacy for Software Applications, Trino, Italy
Traceability Blockchain

Interoperablity in encoded quantum repeater networks *(2016)*
Shota Nagayama, Byung-Soo Choi, Simon Devitt, Shigeya Suzuki,
Rodney Van Meter, Phys. Rev. A 93, 042338
Quantum Internet

https://member.wide.ad.jp/~shigeya

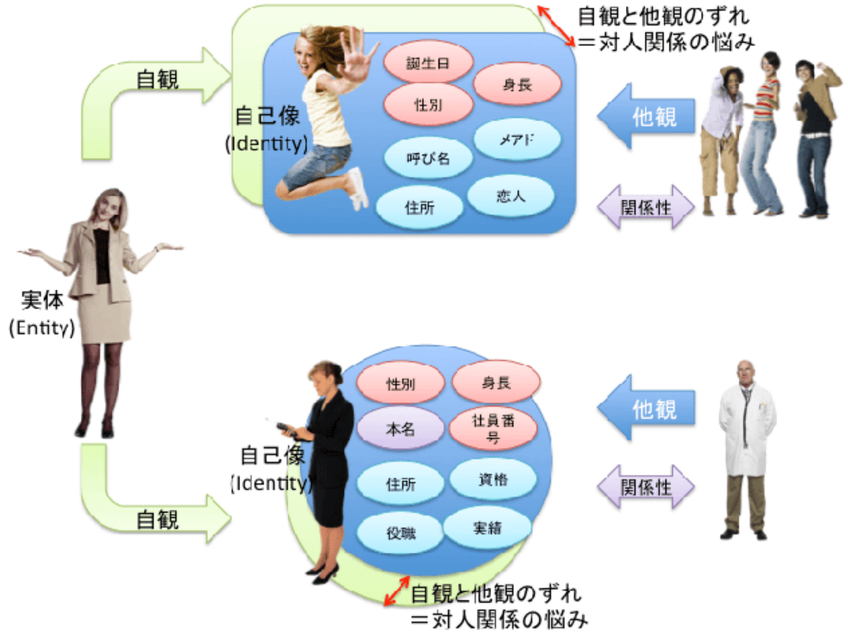
デジタルアイデンティティ

デジタルアイデンティティ

- ものすごく「丸めて」表現すると:
  「**ある人**(= 実体: 一つ)**に対応するサイバー空間中で識別可能な自己像**(複数可)」

- 実体と自己像、自己像に対する自観、
  他人からみた他観や関係性など、
  厳密に説明するのは難しい。
  [1]参照のこと（右図も同文書から)

- ISOの定義では
  「実体を構成する属性の集合」
  (ISO/IEC 24760-1)



[1] 非技術者のためのデジタル・アイデンティティ入門, @_Nat Zone, 2011/6/21
https://www.sakimura.org/2011/06/112

デジタルアイデンティティに関係する技術の発展

- **フェーズ 1：中央集権型アイデンティティ**
  (単一の、あるいは、階層化された管理権限域によるコントロール)
  - ドメイン名システム(DNS)、公開鍵認証局(CA)
- **フェーズ 2：フェデレーションされたアイデンティティ**
  (複数の管理権限域間の連合によるコントロール)
  - Liberty Alliance, Microsoft Passport
- **フェーズ 3：ユーザ中心のアイデンティティ**
  (複数の権限域にまたがる個人または管理者によるコントロール)
  - Internet Identity Workshop コミニュティなどを起点とした、様々な標準: OpenID (2005), OpenID 2.0 (2006), Open ID Connect (2014), OAuth (2010), FIDO (2013)
- **フェーズ 4：自己主権型アイデンティティ**
  (複数の権限域にまたって個人がコントロール)
  - Decentralized Identifiers (DIDs)

"The Path to Self-Sovereign Identity" からの訳。若干の修正あり

The Path to Self-Sovereign Identity

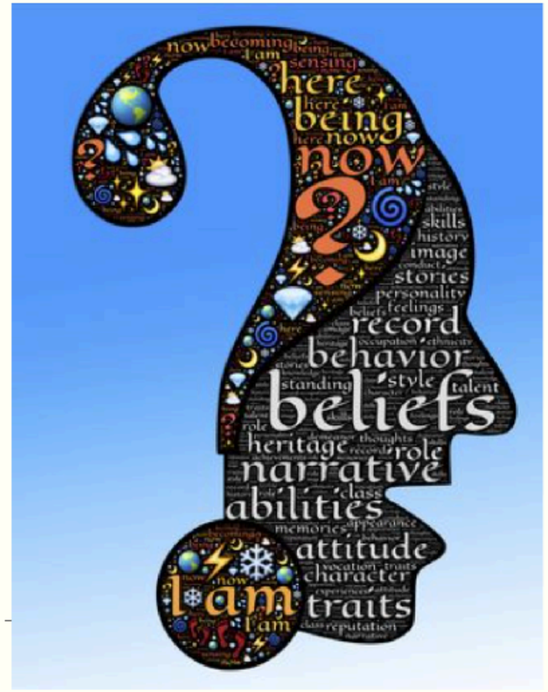
- 「自己主権型アイデンティティへ至る道筋」

- 自己主権型アイデンティティ
  (Self-Sovereign Identity - SSI)の
  生みの親の一人とも言える
  Christopher Allenによる、SSIに至る
  までの過程とSSIの定義、SSIの10個の
  基本原則についての議論

The Path to Self-Sovereign Identity

April 25 2016 - 4200 Words
by Christopher Allen

Today I head out to a month-long series of events associated with identity: I'm starting with the 22st (!) Internet Identity Workshop next week; then I'm speaking at the blockchain conference Consensus about identity; next I am part of the team putting together the first ID2020 Summit on Digital Identity at the United Nations; and finally I'm hosting the second #RebootingWebOfTrust design workshop on decentralized identity.



http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

Decentralized Identifier (DID) and Verifiable Credentials

自己主権型で実装可能な分散型ID (Decentralized Identifier) とデジタル証明書 (Verifiable Credential)

- 自己主権型デジタルアイデンティティ
  - 誰にも依存せずに自身で制御可能なデジタルアイデンティティ

- Decentralized Identifier (DID) / W3C Candidate Recommendation
  - 属性情報と紐付けられていない「限り無く無色の」アイデンティティ
  - 分散システム指向であり、自己主権型で実装可能

- Verifiable Credential / W3C Recommendation
  - 属性情報を第三者に証明してもらうための【デジタル証明書】仕様
  - ゼロ知識証明などの技術の組み合わせにより個人情報の「選択的最小開示」を実現できる

- 詳細については「大学教育におけるDXシンポジウム」のスライドを参照 [1]

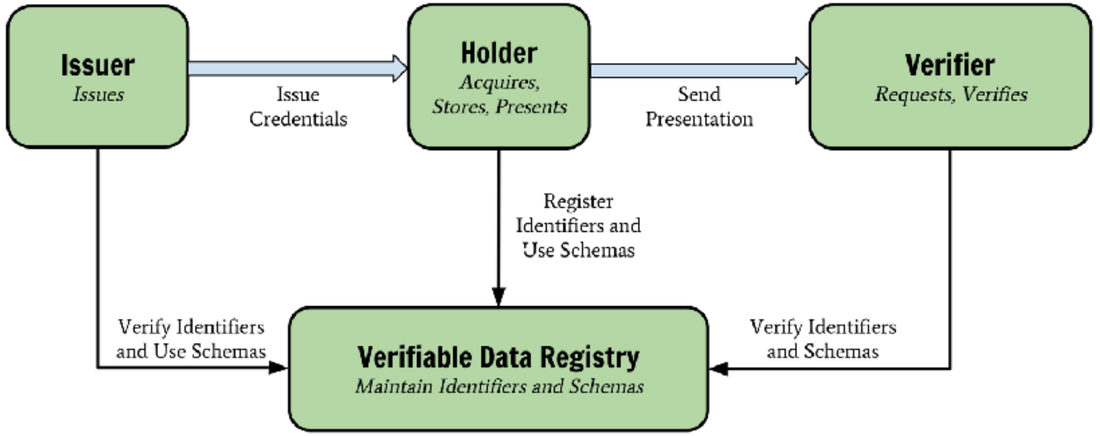
[1] https://kbcl.sfc.keio.ac.jp/events/2021_01_13-univ-dx/2021_01_13-keio-bc-univ-dx-suzuki.pdf

Verifiable Credentials - 検証可能な資格証明書

- さまざまな「証明書」のデジタル化手段
- デジタル署名技術を用いた【発行者】(Issuer)により【対象者】(Subject)が特定の条件を満たしている事を【保持者】(Holder) が示すことができる
- W3C で標準化されている [1]

- Subject / Issuer / Holder を
  示すための手段が必要

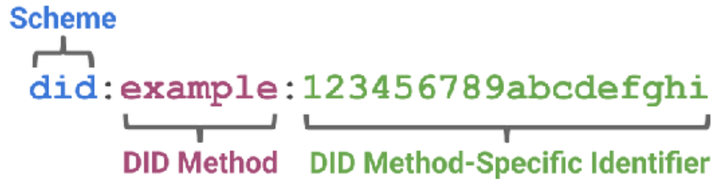
→ **デジタルアイデンティティ技術が必須**

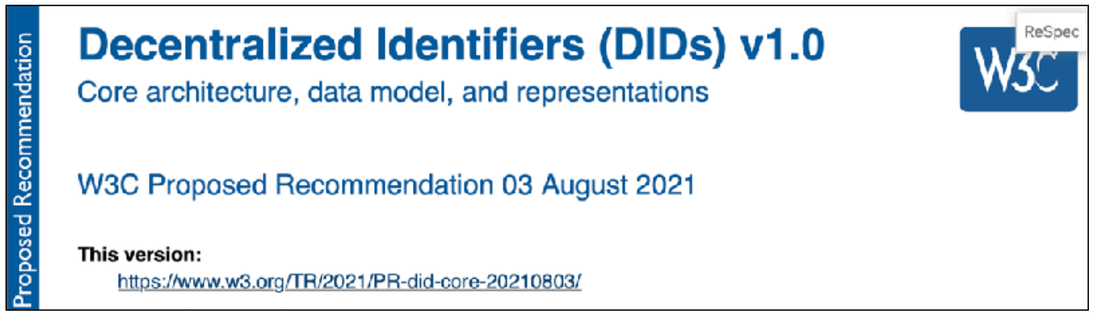


[1] Verifiable Credentials Data Model 1.0 https://www.w3.org/TR/vc-data-model/

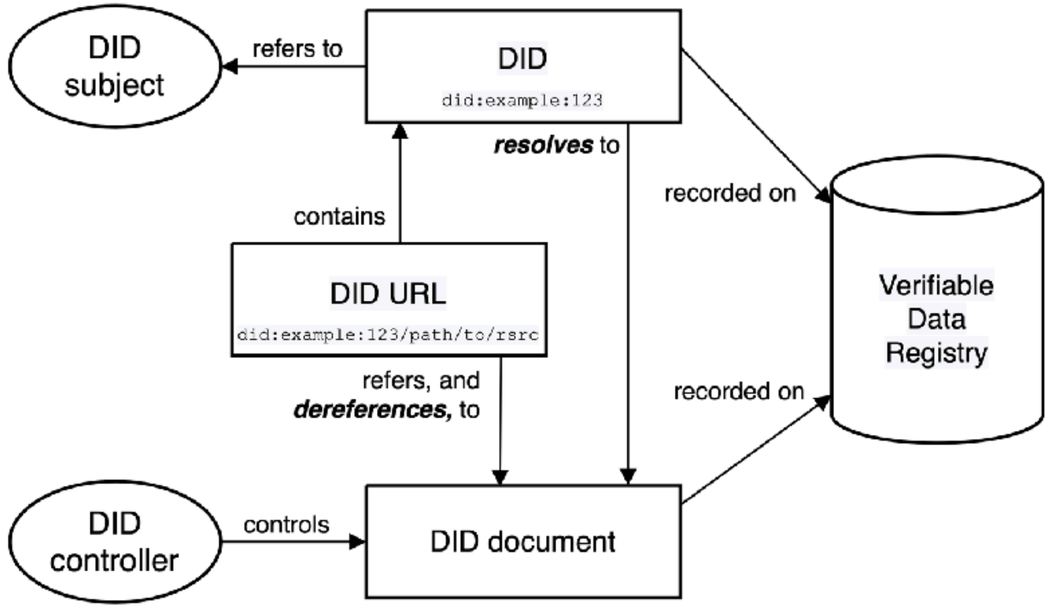
Decentralized Identifier (DIDs) v1.0

- 自己主権型の識別子にまつわる**データモデル標準**
  - 周辺技術との組み合わせで自己主権型のアイデンティティを実現できる
  - 複数の方式(メソッド)で実装され、メソッドにより、ブロックチェーン技術を下支えにするものも、しないものもある



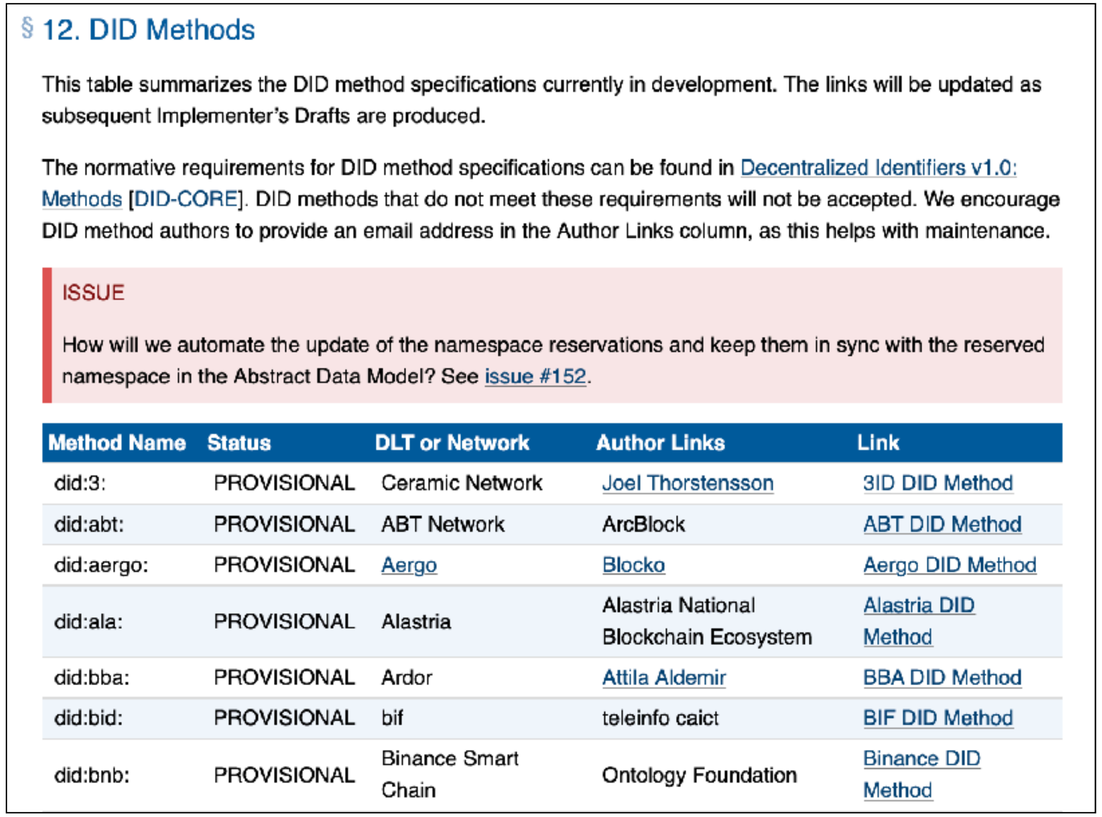


Decentralized Identifier (DIDs) v1.0 (Proposed Recommendation)
https://www.w3.org/TR/2021/PR-did-core-20210803/



DID Methodと実装状況

- DID Specification Registry に一覧がある。現在このリストには103個
- コンフォーマンステストに提出された実装の数は47個



§ 12. DID Methods

This table summarizes the DID method specifications currently in development. The links will be updated as subsequent Implementer's Drafts are produced.

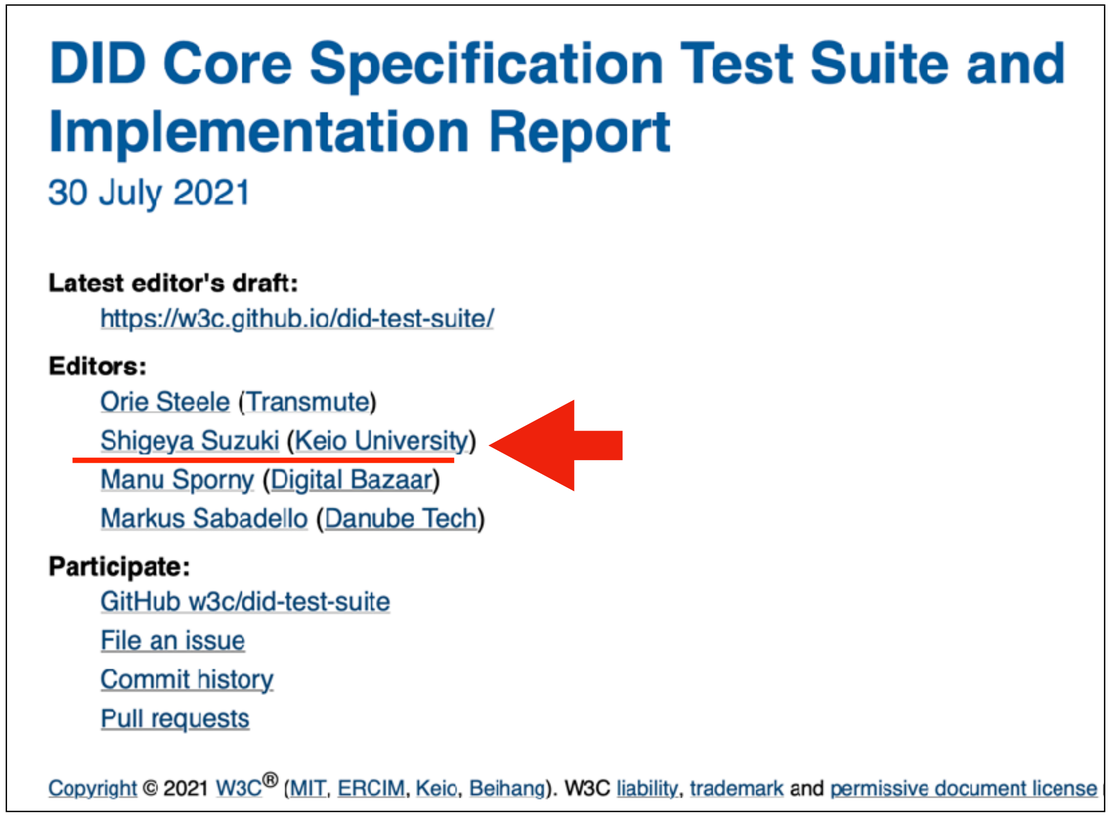
The normative requirements for DID method specifications can be found in Decentralized Identifiers v1.0: Methods [DID-CORE]. DID methods that do not meet these requirements will not be accepted. We encourage DID method authors to provide an email address in the Author Links column, as this helps with maintenance.

ISSUE

How will we automate the update of the namespace reservations and keep them in sync with the reserved namespace in the Abstract Data Model? See issue #152.

Method Name	Status	DLT or Network	Author Links	Link
did:3:	PROVISIONAL	Ceramic Network	Joel Thorstensson	3ID DID Method
did:abt:	PROVISIONAL	ABT Network	ArcBlock	ABT DID Method
did:aergo:	PROVISIONAL	Aergo	Blocko	Aergo DID Method
did:ala:	PROVISIONAL	Alastria	Alastria National Blockchain Ecosystem	Alastria DID Method
did:bba:	PROVISIONAL	Ardor	Attila Aldemir	BBA DID Method
did:bid:	PROVISIONAL	bif	teleinfo caict	BIF DID Method
did:bnb:	PROVISIONAL	Binance Smart Chain	Ontology Foundation	Binance DID Method

https://w3c.github.io/did-spec-registries/#did-methods



DID Core Specification Test Suite and Implementation Report

30 July 2021

Latest editor's draft:
https://w3c.github.io/did-test-suite/

Editors:
Orie Steele (Transmute)
Shigeya Suzuki (Keio University)
Manu Sporny (Digital Bazaar)
Markus Sabadello (Danube Tech)

Participate:
GitHub w3c/did-test-suite
File an issue
Commit history
Pull requests

Copyright © 2021 W3C® (MIT, ERCIM, Keio, Beihang). W3C liability, trademark and permissive document license

https://w3c.github.io/did-test-suite/

DID document

- DID document は DIDで示される主体を表現するのに必要なデータやメカニズムが記載されている。データとしては、公開鍵、特定のブロックチェーン中の位置を示す情報などが例としてあげられる


```
{
  "@context": "https://w3id.org/did/v0.11",
  "id": "did:web:did.actor:alice",
  "publicKey": [
    {
      "id": "did:web:did.actor:alice#z6MkrmNwty5ajKtFqc1U48oL2MMLjWjartwc5sf2AihZwXDN",
      "controller": "did:web:did.actor:alice",
      "type": "Ed25519VerificationKey2018",
      "publicKeyBase58": "DK7uJiq9PnPnj7AmNZqVBFoLuwTjT1hFPrk6LSjZ2JRz"
    }
  ],
  "authentication": [
    "did:web:did.actor:alice#z6MkrmNwty5ajKtFqc1U48oL2MMLjWjartwc5sf2AihZwXDN"
  ],
  "assertionMethod": [
    "did:web:did.actor:alice#z6MkrmNwty5ajKtFqc1U48oL2MMLjWjartwc5sf2AihZwXDN"
  ],
  "capabilityDelegation": [
    "did:web:did.actor:alice#z6MkrmNwty5ajKtFqc1U48oL2MMLjWjartwc5sf2AihZwXDN"
  ],
  "capabilityInvocation": [
    "did:web:did.actor:alice#z6MkrmNwty5ajKtFqc1U48oL2MMLjWjartwc5sf2AihZwXDN"
  ],
  "keyAgreement": [
    {
      "id": "did:web:did.actor:alice#zC8GybikEfyNaausDA4mkT4egP7SNLx2T1d1kujLQbcP6h",
      "type": "X25519KeyAgreementKey2019",
      "controller": "did:web:did.actor:alice",
      "publicKeyBase58": "CaSHXEvLKS6SfN9aBfkVGBpp15jSnaHazqHgLHp8KZ3Y"
    }
  ]
}
```


https://did.actor の https://did.actor/alice/ から

DID URL

- DIDを起点としたリソースロケータ
- DIDを含み、URLのようにパス、クエリ、フラグメント等の要素をもち、DIDで示される対象（リソース）に含まれるであろう要素を示す
- DID documentの中では、フラグメントを用い、DID document中の公開鍵を相対的に指定するために使われる (#key-1)

EXAMPLE 4: A unique verification method in a DID Document

```
did:example:123#public-key-0
```

EXAMPLE 5: A unique service in a DID Document

```
did:example:123#agent
```

EXAMPLE 6: A resource external to a DID Document

```
did:example:123?service=agent&relativeRef=/credentials#degree
```

EXAMPLE 7: A DID URL with a 'versionTime' DID parameter

```
did:example:123?versionTime=2021-05-10T17:00:00Z
```

EXAMPLE 8: A DID URL with a 'service' and a 'relativeRef' DID parameter

```
did:example:123?service=files&relativeRef=/resume.pdf
```

EXAMPLE 9: An example of a relative DID URL

```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ]
  "id": "did:example:123456789abcdefghi",
  "verificationMethod": [{
    "id": "did:example:123456789abcdefghi#key-1",
    "type": "Ed25519VerificationKey2020", // external (property value)
    "controller": "did:example:123456789abcdefghi",
    "publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }, ...],
  "authentication": [
    // a relative DID URL used to reference a verification method above
    "#key-1"
  ]
}
```

プライバシー重視の仕様策定

- DID は単一のユーザが多数用い、自由に使い分けができるようになっている
  - DID は、DID を伝える対象、組み合わせるVC等に応じて、対象ごとに都度作成 (pair-wise) で使われることが前提となっている

- DID および DID document に含まれる情報に、個人識別情報(PII)を含めるだけでなく、個人識別に繋がる可能性のある情報が含まれないように、注意深く検討、仕様化（必要に応じた注意書き）などが行われている

- DID Core仕様書の §9. Security Considerations、§10. Privacy Considerations は、デザイン上の思想が表現されている

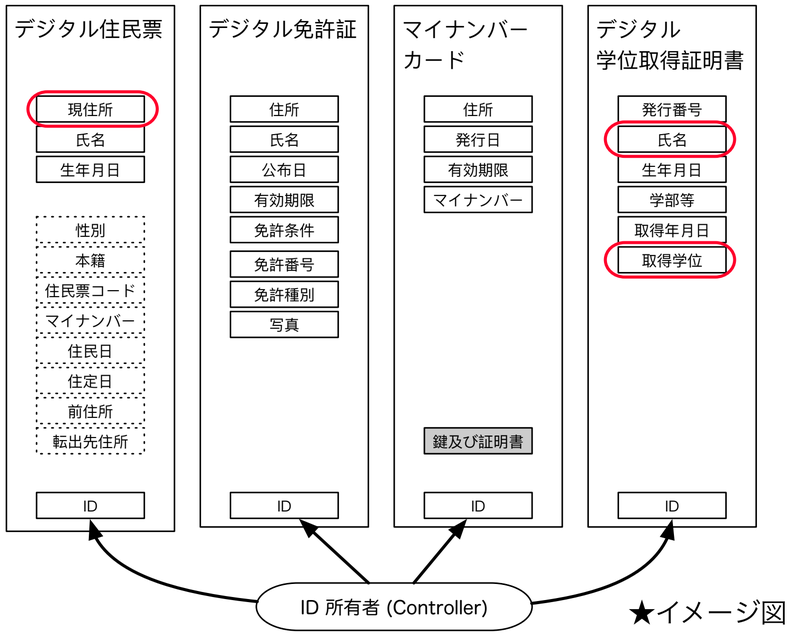
DID/VC Ecosystem

- DID
  - DID itself
  - method implementation <-> Verifiable Data Registry
  - resolver implementation
- VC
  - VC itself
  - Issuer implementation <-> Verifiable Data Registry
  - Holder implementation (= wallet)
  - Verifier implementation
- Transport between entities / Negotiation Protocols

- … Operation … Interoperability … etc.

属性情報のアンバンドリング・バンドリング

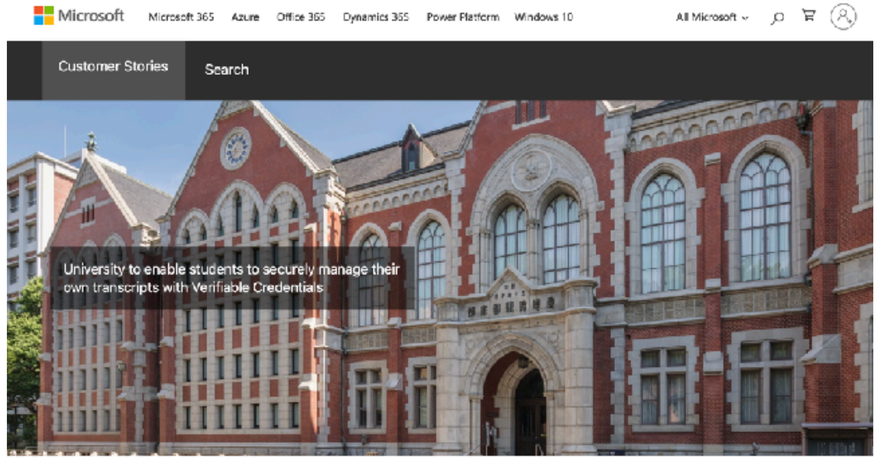
- 属性情報のアンバンドリング
  → 個人の制御下での選択的なバンドリングと開示
- 識別子の使い回しを避けることにより、情報の結合可能性を下げる
  - (システム間)連携の識別子を場面ごと (たとえば、pair-wise）に作成・利用

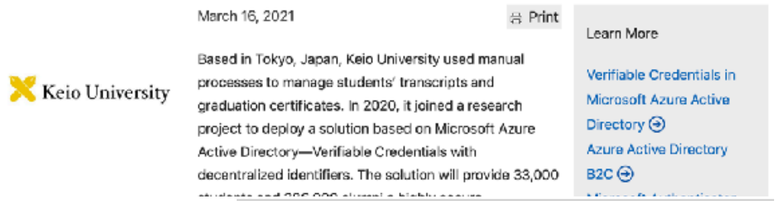


★イメージ図

大学での応用例

次世代デジタルアイデンティティ基盤@慶應義塾[1]





Microsoftの顧客事例として紹介された [2]

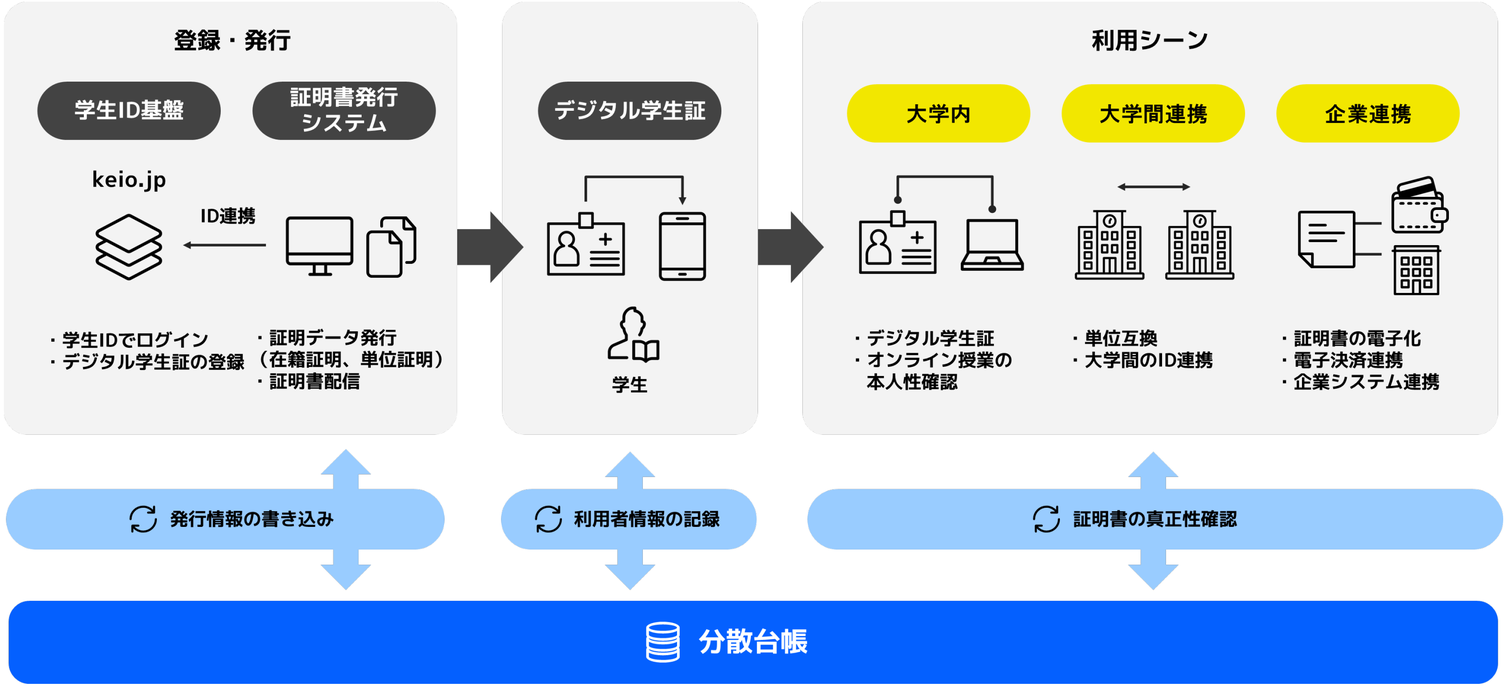
参画組織

- 慶應義塾大学
- 伊藤忠テクノソリューションズ株式会社
- Japan Digital Design株式会社
- 株式会社ジェーシービー
- 西日本電信電話株式会社
- BlockBase株式会社

+ Microsoft (基盤提供)

各種個人証明（在学証明、卒業証明等）をスマホアプリに格納、ポータビリティの実現と、確実な検証を可能とする

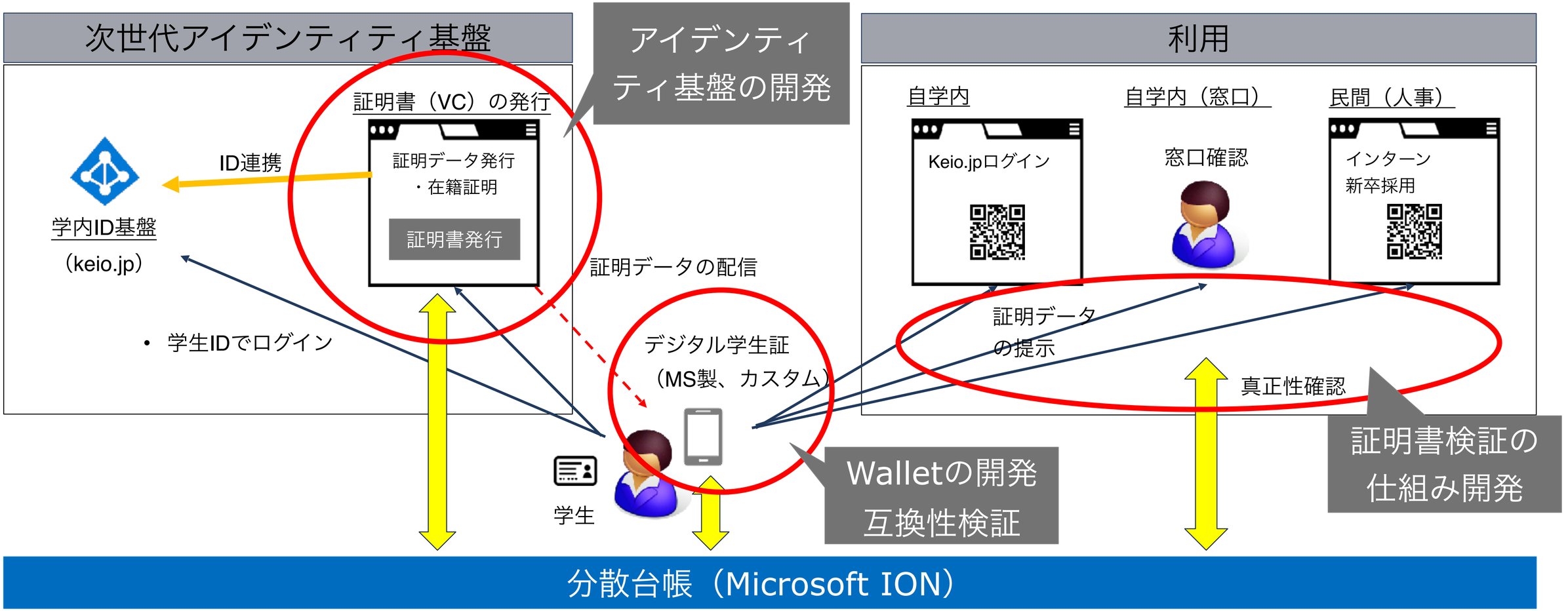
- オンライン・オフラインの両方で利用可能な身分証明書
- 塾内だけでなく大学間・企業との連携など広く展開を目指す
- 大学発行の証明書以外に民間の発行する証明書も格納
- 分散型IDの標準技術利用により永続性、相互運用性を実現



[1] https://kbcl.sfc.keio.ac.jp/events/2021_01_13-univ-dx/2021_01_13-keio-bc-univ-dx-fujie.pdf
[2] https://customers.microsoft.com/en-us/story/1349421307379340138-keio-university-higher-education-azure-active-directory

PoCシステム構成と開発内容

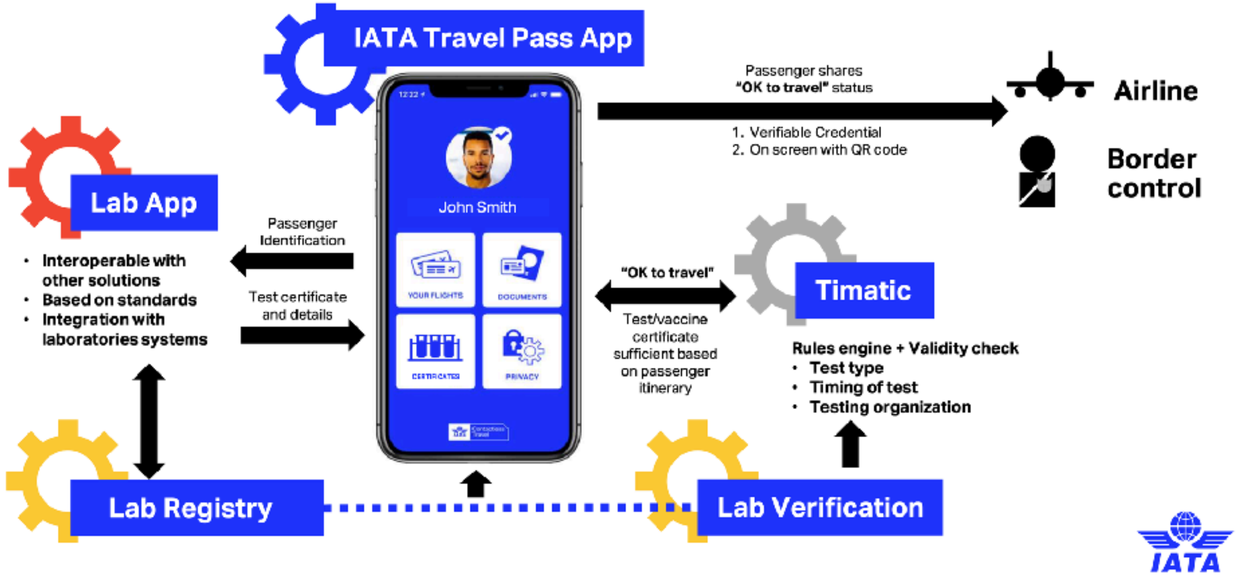
標準仕様に則り、アイデンティティ基盤、デジタル学生証（スマホWalletアプリ）、証明書検証の仕組みの開発を実施（基盤としてMicrosoft社の提供するSDK、Serviceの利用して開発）



その他の応用事例

IATA Travel Pass

- International Air Transport Association (IATA)による旅行関連情報のパッケージ化 - DID/VC を用いている
- もともとはCOVID-19向けでは無かったが、ワクチン接種記録 / 検査記録書の記録・提示機能を含む
- 国内では、ANA / JAL が実験中



IATA Travel Pass Initiative サイトから

[1] International Air Transport Association (IATA) https://www.iata.org/en/
[2] IATA Travel Pass Initiative https://www.iata.org/en/programs/passenger/travel-pass/
[3] ANA の実証実験 https://www.ana.co.jp/ja/jp/topics/IATA-travel-pass/
[4] JAL の実証実験 https://www.jal.co.jp/jp/ja/inter/iatatravelpass/

航空機搭乗時のセキュリティ確認 (Apple, iOS15)

- WWDC'2021 基調講演 [1] での空港でのセキュリティチェックでの応用

- ポイント
  - 空港のセキュリティ(TSA)を超えるのには、アメリカ国内ではReal ID[2] が必要になった
  - 運転免許証のデジタル化の議論が進んでいる[3]
    - (2018年に岡山で実験が行われている)
  - Apple は TSAと協調することをアナウンスしていた
  - mDLには選択的開示機能があるとのこと

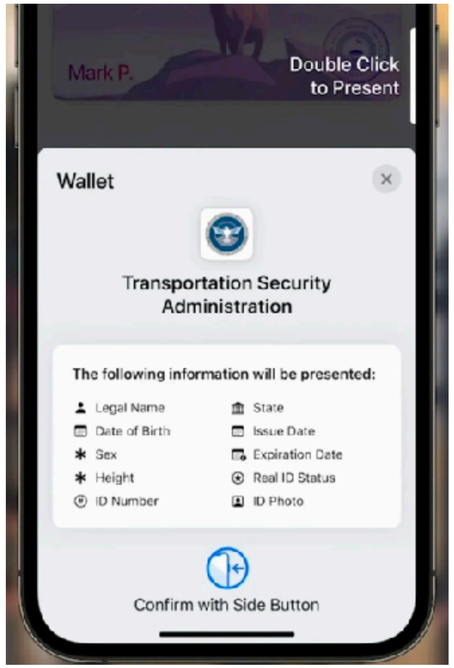


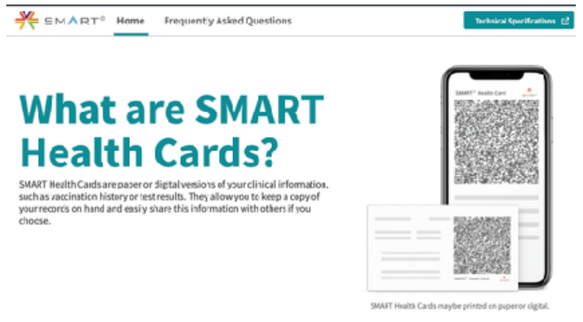
Image: Apple (via The Verge)

[1] WWDC21 Apple Keynote https://podcasts.apple.com/us/podcast/wwdc21-apple-keynote/id275834665?i=1000524551302
[2] Real ID https://www.dhs.gov/real-id
[3] Mobile Driver's License(mDL) "ISO/IEC FDIS 18013-5 Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application" (ISO/IEC JTC 1/SC 17) https://www.iso.org/standard/69084.html

確認済みの情報としての健康情報の交換 (Apple, iOS15)

- WWDC’2021 "Explore Verifiable Health Records" セッション [1]

- ポイント
  - 仕様としては SMART Health Cards [2] 標準を用いている
  - 健康情報を集中的に保持するHealthKitのデータとして保持
  - 健康情報サービス提供業者(アメリカ、イギリス、カナダのみ）から、あるいは直接のQRコードでの読み込みで取り込める
  - アプリから、取り込まれた情報の存在を問い合わせ取得できる
    - アプリからの操作は**毎回必ず**アプリに情報を渡すか否かをユーザに確認
  - アイデンティティウォレットとしての機能提供ではない



[1] Explore Verifiable Health Records https://developer.apple.com/videos/play/wwdc2021/10089/
[2] https://smarthealth.cards

DID/VC応用における課題

DID/VCの課題 (1)

- 対象領域（〜業界）毎の国際的に合意されたスキーマの作成は困難

- 玉虫色の仕様 → 複数の実装が存在するシステムの宿命
  - データモデル仕様 / Representation と Abstract Data Model
    - JSON vs JSON-LD & @context / MIME type (ふたつの `+`)
    - 署名方式 (JSON Web Tokens[1] vs LD-Proofs [2])

- Dereferencerの仕様が心配（複雑・挙動が十分に仕様化されていない）

[1] Linked Data Proofs 1.0 https://w3c-ccg.github.io/ld-proofs/
[2] The Security Vocabulary https://w3c-ccg.github.io/security-vocab/

DID/VCの課題 (2)

- 既存トラストフレームワーク/ミドルウェアとの連携あるいは構築

- DIDあるいはVCのインターオペラビリティ
  - DIDの置き換え、method レベルでの置き換え
  - VC提示・交換のプロトコル
  - クレデンシャルウォレット / アイデンティティウォレット

- セキュリティ
  - (古典的な公開鍵暗号運用の問題)
  - (ライブラリ、ツールチェインなどのトレーサビリティ問題)

大学におけるDID/VC活用における課題

- 長期間広範囲での利用の担保
  - 長期間 = 長期運用性 / 運用継続性
  - 広範囲 = 日本国内 / さらには国際　→ vc-eduでユースケースの差異を吸収できるか
  - パッケージ形式の標準化: 証明の方式と形式　→ VC/DID 標準＋暗号に関連した標準
  - パッケージの中身の形式の標準化: 学位証明の表現方式と形式　→ vc-edu 方面で整備
  - パッケージのやり取り　→ DIDCommがあるが。。

- 学内で実現する上での問題
  - 既存のID基盤との連携をどうとるか
    - → 慶応ではID基盤でのサポートを実現済み
  - 実施のための手順の策定と実施
    - 事務方との連携

本日のプレゼンテーション

- デジタル化された証明書と自己主権型アイデンティティ
- Decentralized Identifier (DID), Verifiable Credentials についての概要
- 応用事例
- 課題