DID調査

W3C

Decentralized Identifiers (DIDs) v1.0 2022年7月19日

Verifiable Credentials Data Model v2.0 2025年5月15日

IdM実験室

デジタルアイデンティティのすべて - O'Reilly Japan

最近の関連ニュース 2025年9月

最近関連のニュース 2025年9月

W3C DIDとKYCの現状 - Google ドキュメント(Gemini)

KYC関係

Self-Sovereign Identity (SSI)

自分の Identity を自分で管理して中央集権的サービスに依存せず証明や共有できるという概念。

DID

中央機関に依存しない主体識別子

VC

DIDを持つ主体に紐付いた検証可能な資格証明

Cryptographic Proofs

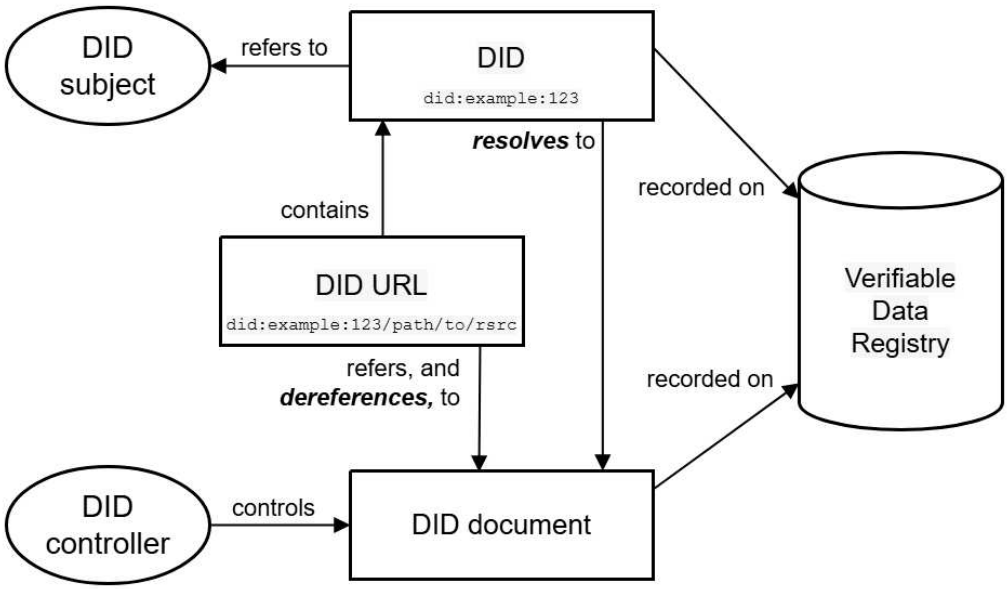
所有制や正当性を証明するための署名やゼロ知識証明などのしくみ

DID

Decentralized Identifier の略。

W3C did-core v1.0 の Terminology に従うと decentralized identifier なのだが、DIF が "identity" の略なためか identity と表現しているところも多い。

ここでは did-core にあわせて固有名詞以外は identifier とする。



W3C DID Methods

たくさんあるが、削除できるものでもないから増える一方だろう

ChatGPT

DID method と分散性レベルの一覧。

DID メソッド	基盤 / 実装	分散性レベル	特徴
`did:key`	公開鍵自己完結型	高	DID文書は公開鍵情報自体に含まれる。中央管理者不要。オンチェーン不要。
`did:ion`	Sidetree + Bitcoin	高	更新はオフチェーン Sidetree ネットワーク、整合性は Bitcoin ブロックチェーンに記録。誰でも検証可能。
`did:ethr`	Ethereum スマートコントラクト	高	DID文書をスマートコントラクトに格納。改ざん防止。誰でも読み書き可能(権限管理はコントラクト次第)。
`did:sov`	Hyperledger Indy / Sovrin	高	Indyネットワーク上で DID 登録・更新。分散型台帳により検証可能。
`did:cheqd`	cheqd ネットワーク (Cosmos SDK)	高	DID文書は Cosmos SDK ベースの分散台帳上で管理。検証可能。
`did:btcr`	Bitcoinトランザクション	高	DID 文書ハッシュを Bitcoinトランザクションに書き込み。分散型。
`did:web`	HTTPS サーバー	低	DID文書は単一 Web サーバーに依存。分散性はほぼなし。W3C では認められるが中央集権的。
`did:ion-test` / `did:example`	テスト・例	低	実運用用ではない。中央集権的または模擬的。

did:btcr

BTCR DID Method

Regtest の `bcrt` ではない。

実験的メソッド。

did:ethr / did:ethr:polygon

decentralized-identity/ethr-did-resolver: DID resolver for Ethereum Addresses with support for key management

Ethereumというよりも EVM系なので幅が広い。

EIP-1056 という uPort の規格がベースになっている。

uPort は Veramo という名前で続いている

DID - did:ethrの実験

did:sov

Sovrin Network / Foundation は 解散したようだ。

DIF

Decentralized Identity Foundation

https://identity.foundation/

https://github.com/decentralized-identity は sidetree や ion は止まっているが、universal resolver などそれ以外は今も更新され続けている

消えたプロジェクト

Microsoft

昔やっていたsidetree や ion は 2年前からリポジトリ更新が止まっている

Microsoft Entra Verified ID

`did:web` が中心。 `did:ion` も昔はあったようだが今はなさそう。

Bitcoin は使わず Azure 上のサービスを使っている

web5

昔やっていた TBDev は既にアーカイブされていた

DIF に引き継いでもらったらしい

最近のプロジェクト

CREDEBL

AYANWORKS社

SSI(Self-Sovereign Identity)プラットフォーム

Sudo Platform Edge Agent SDK

Anonyome Labs - Your identity protection journey starts here

Hyperledger Aries ベース

Verifiable Credentials SDK

The DFINITY Foundation

ICP(Internet Computer)上で Verifiable Credentials を発行・検証できる SDK

Hiero DID SDK

https://hiero.org/

OriginVault ov-id-sdk

OriginVault

Polygon ID

Home - Privado ID

昔は Polygon ID という名前だったがリブランディングして名前が変わった。

Priado.iD なのか Priado ID なのかはっきりしてほしい。。。

W3C VC Data Model v2.0

DID の標準仕様。2025年5月リリース。

Hyperledger Indy

https://www.lfdecentralizedtrust.org/projects/hyperledger-indy

カルビー、IP管理にブロックチェーン活用──「かるれっと」実証実験開始 - CoinDesk JAPAN（コインデスク・ジャパン）

proovyがトレードログとのサービス基盤接続により、DID/VC実装におけるブロックチェーンオプションを提供開始～VCの企業間利用の需要に対応～ - 株式会社Receptのプレスリリース

実例

NEC

大阪万博で パビリオンnull2(ぬるぬる)にDID/VCソリューションを提供

https://jpn.nec.com/web3/index.html

web3 とかなんとか

IDウォレット

デジタルアイデンティティ・ウォレットの技術解説：その仕組み、主要要件 - PwC Japanグループ

個人のデジタルID（分散型IDや認証用資格情報）を管理するためのウォレット

EUDIW

ChatGPT

EUデジタルアイデンティティウォレット（EUDIW）の実施規則案を読み解く｜ブログ｜NRIセキュア

The EU Digital Identity Wallet: A Beginner's Guide

日本

トラスト（デジタル・アイデンティティ等）｜デジタル庁

OpenID Connect (OIDC)

ChatGPT

分散型の認証フレームワーク。複数の認証先(IdP、OpenID Provider)を選択できるという点が「分散」。

サービスなどを利用する際にアカウントを作らず

OpenID は 1.0 と 2.0 があったが既に非推奨でサポートされていない。

OpenID Connect が今使われている技術。略称は OIDC。

OAuth2.0 からの拡張。

フィッシング対策は考慮されていないため、そこは別の対策が必要。

以下は Authorization Code Flow というシーケンス。

```
sequence
   User          Client(RP)                IdP(OP)
    |                 |                       |
```

```
|--- Login ----->|                        |
|                |--- AuthN Request ----->|
|                |<-- AuthN + Consent ----|
|                |<-- Auth Code ----------|
|                |--- Token Request ------>|
|                |<-- ID Token + AT -------|
|                |--- (UserInfo Req) ----->|
|                |<-- (UserInfo) ----------|
|<-- Auth OK ----|
```

その他

TOPPANエッジ、国際的な法人デジタル証明書「vLEI」の発行資格を取得、発行サービスを11月開始（クラウド Watch） - Yahoo!ニュース

vLEI Verifiable Legal Entity Identifier

LEI を使用したデジタル識別および検証 – 検証可能な LEI (vLEI) - 組織のアイデンティティ – GLEIF

vLEIの概要 SSI（Self Sovereign Identity）概念に基づく法人識別子 - HashHub Research

有料記事だった。。

DUNS はアメリカ企業だが LEI は非営利組織。

Verifiable Credential などと記事にあったので DID 互換かも。