

DID,VC入門(1) - Decentralized Identifiersとは

公開: 2025/05/07 | Zenn (idroit-community)

本記事は3部構成でDID,VCを使ってできることを紹介します。

- 1部: Decentralized Identifiersとは
- 2部: Verifiable Credentialsとは
- 3部: DIDとVCでできること

第1部として本記事ではDIDについて解説します。

あくまで「DID,VCを使って(でも)」できることの説明です。「他の技術でもできる」「Why DID/VC?」というご指摘はおっしゃる通りであることは前置きとして書いておきます。

Decentralized Identifiers(DID)

DIDの技術に関して詳細かつ広範に書かれた記事としてはこちらの方が書かれた記事がおすすめです。かなり技術寄りで読み応えがあります。参考: <https://gaiax-blockchain.com/what-is-the-did-by-w3c>

本記事ではもう少し簡略化した解説をしようと思います。

DIDの概要

DIDとはW3Cが標準化した識別子の標準です。参考: <https://www.w3.org/TR/did-1.0/>

DIDは世界で唯一の番号被りのない識別子を生成することが可能なことが特徴です。番号被りのない識別子を生成する方法として、暗号学に基づくランダムな値や、ドメイン名に基づいて識別子を生成します。**識別子を変えずにその識別子に紐付いた鍵情報を更新・失効できるのも特徴の一つです(できないDIDメソッドもあります)。**

Scheme

did:example:123456789abcdefghi

DID Method **DID Method-Specific Identifier**

DIDを構成する3つの要素（スキーム / DIDメソッド / DIDメソッド固有の識別子）

1. **スキーム**: この識別子がDID標準に準拠した識別子であると表す
2. **DIDメソッド**: DIDの種類を表す。詳細は後に記します。
3. **DIDメソッド固有の識別子**: DIDメソッドに応じた固有の識別子

DIDを用いることで**識別子のコントロール権を所有していることを証明**することができます。例えば、DNSレコードの設定や公開鍵暗号における署名生成のように、**その所有者しかできない操作を行うことで、当人性の証明を行う所有の証明(Proof of Possession(PoP))**を行います。

DIDメソッド

ひとえにDIDと言っても、公開鍵の置き場所としてブロックチェーンを用いる、Webサイトを用いる、DNSを用いるなどの識別子の構成方法・構成技術によって仕様が異なります。それぞれのDIDの技術仕様をDIDメソッドと言います。

did:keyメソッド

公開鍵暗号方式をもとにしたDIDメソッドの一種であり、公開鍵をそのまま固有識別子として扱うのが特徴です。このDIDメソッドでは鍵情報の更新・失効はできません。

```
did:key:z6MkepWVAjYFGvTdffTcJJcE1sJKLHuCefxqw72dPodoxJrP
```

did:webメソッド

WebのドメインをもとにしたDIDメソッドです。管理者のWebサイト上の特定の場所にDIDドキュメントを設置します。

```
did:web:idroit-dashboard.com
```

did:ethrメソッド

Ethereumブロックチェーンを用いるDIDメソッド。スマートコントラクトを用いた鍵情報の更新・失効が可能です。

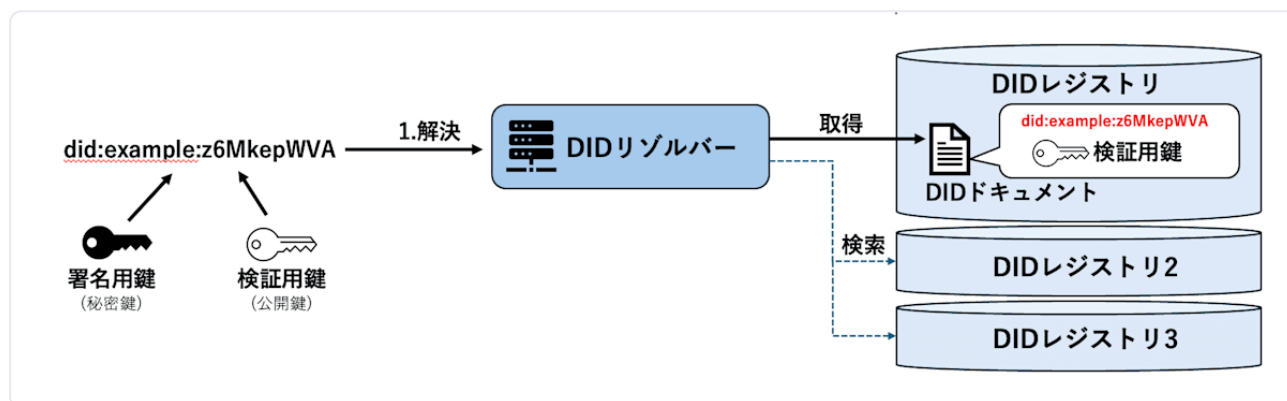
```
did:ethr:0x030a48b2e2c4890ff2c26b91b93f8f899191c21bd6d52722e62a5251c55dfa22a5
```

did:ionメソッド

Bitcoinブロックチェーンと分散ファイルシステムIPFSを用いるDIDメソッドです。Sidetreeプロトコルと呼ばれる様々なブロックチェーンと分散ファイルシステムで適用可能なDIDの仕様をもとにすることで、鍵情報の更新・失効が可能です。

```
did:ion:EiBqKd-0C-GCTZD0FuC7R0RjJsxhCN06IzWnVzM7f2c-gw
```

DIDの仕組み



DIDドキュメント・DIDリゾルバー・DIDレジストリの関係

DIDドキュメント

DIDの生成時に識別子情報と検証用鍵を記載したファイルであるDIDドキュメントを生成し、DIDレジストリに登録します。

DIDリゾルバー

DIDのルールに則ってDIDレジストリに登録されたDIDの検索(解決)を行いDIDドキュメントを取得します。基本的にオープンソースになっており、誰でも利用可能です。

DIDレジストリ

DIDドキュメントを保存する、誰でもアクセス可能なレジストリ。一般的なデータベース、ブロックチェーンや分散ファイルシステムなどをレジストリとして用います(DIDメソッドごとに異なる)。

DIDが抱える課題

一方でDIDには多くの技術的課題があり、最近は(VCほど)あまり熱心に議論されていない印象を受けます。DIDの問題点については以下の記事にまとめています。 [なぜDecentralized Identifiers\(DID\)を使う必要はないのか](#)

まとめ

本記事ではDIDの概要を説明しました。次の記事ではVerifiable Credentialsについて解説しようと思います。

- 第1部: 「Decentralized Identifiersとは」
- 第2部: 「Verifiable Credentialsとは」
- 第3部: 「DIDとVCでできること」

最後に改めて書いておきますが、この記事ではあくまでDID,VCの入門としてかなり簡略化した説明をしています。また間違いも多くあると思います。ご指摘お待ちしております。

出典: <https://zenn.dev/idroit/articles/749dec001436e7>