DID,VC入門(3) - DIDとVCでできること

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

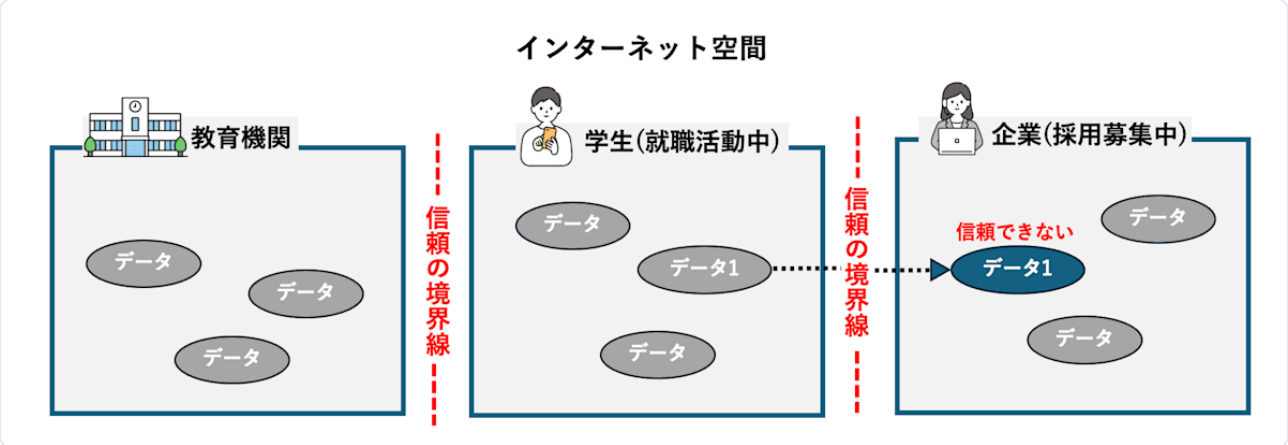
本記事は3部構成でDID,VCを使ってできることを紹介します。

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

第3部として本記事では**DIDとVCでできること**について解説します。

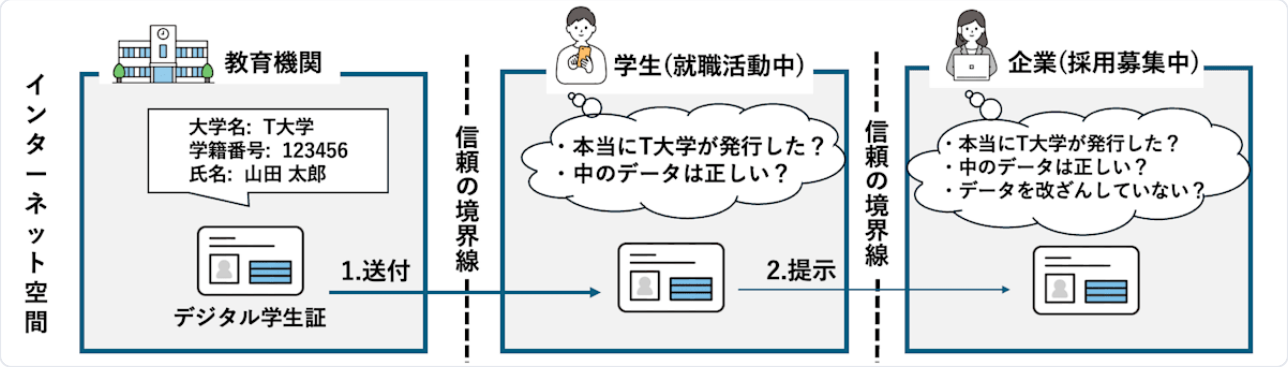
あくまで「DID,VCを使って(でも)」できることの説明です。「他の技術でもできる」「Why DID/VC?」というご指摘はおっしゃる通りであることは前置きとして書いておきます。

DIDとVCでできること



インターネット空間における「信頼の境界線」

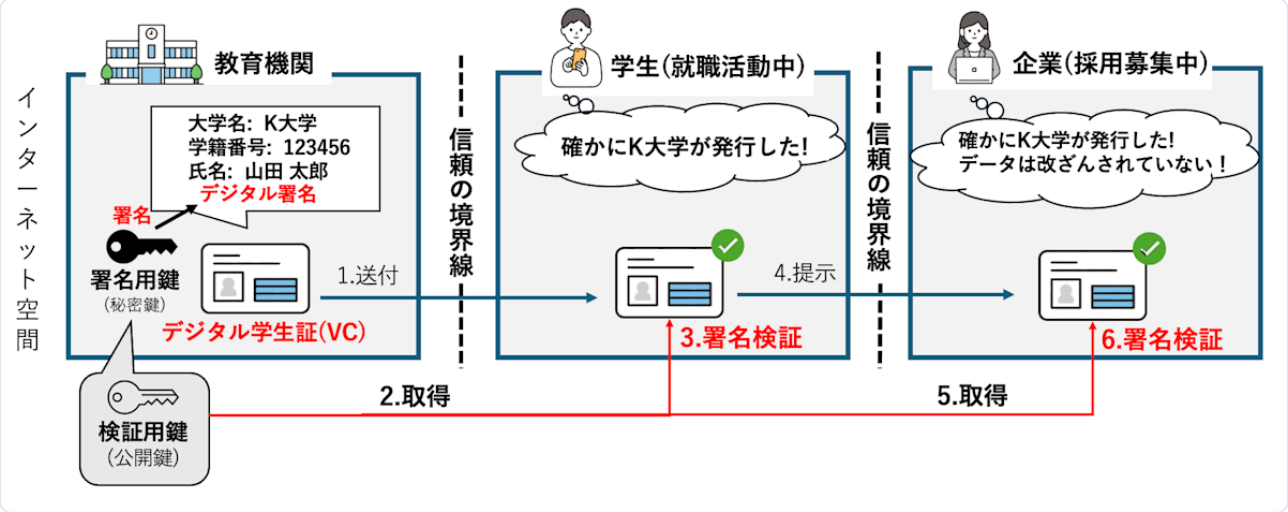
現状、インターネット空間において**信頼の境界線**が存在し、境界線を跨いだデータのやりとりを行った場合、そのデータは信頼できません。



境界線を跨ぐデジタル学生証の例

例えば、**デジタル学生証を導入した場合、受け取り手はそれが信頼できるものなのか判断できません**。 学生は、オンラインで受け取ったデジタル学生証が本当にその教育機関が発行したものなのかわかりません。検証者にとっても、同様に教育機関が発行したものなのか、また学生がデータを改ざんしていないか否かを判断しかねます。

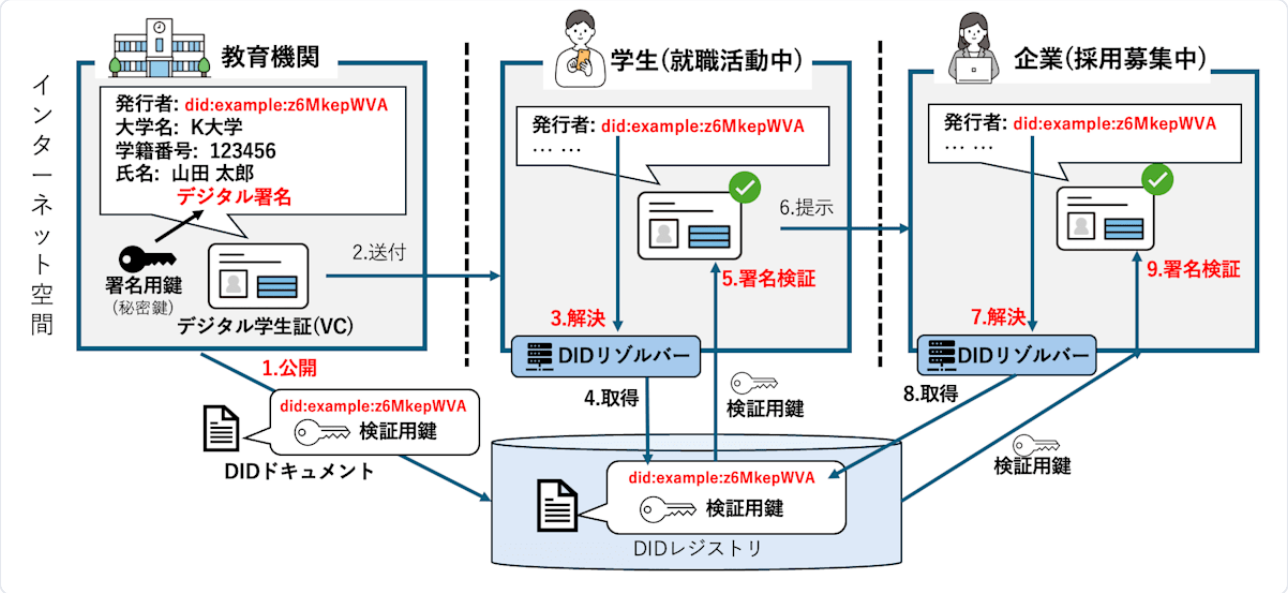
そこでまず前提として**教育機関(発行者)** がなんらかの方法で検証用鍵を公開していたとします。



検証用鍵を公開した発行者

1. デジタル学生証をVCとして発行し、学生証データ内にデジタル署名を含めた状態でデジタル学生証を発行し、**学生(保有者)** に送付します。
2. 就職活動や学割利用の際に学生証を求められた学生は、**企業(検証者)** に提示します。
3. 学生証を提示された企業は、教育機関が公開する検証用鍵を用いて**デジタル署名の検証を行い、発行者が教育機関であることの確認や改ざんの検知が可能になります。**

先ほど「教育機関がなんらかの方法で検証用鍵を公開」しているという前提を置きました。この検証用鍵の公開方法は様々ありますが、例えば発行者がDIDを利用していることとします。



DIDを用いた検証用鍵の公開と署名検証フロー

1. (発行者) DIDを生成し、DIDメソッドに応じたDIDレジストリに公開鍵情報を含むDIDドキュメントを置きます。
2. (発行者) 学生証内の発行者情報としてDIDを含め、DIDに対応した秘密鍵で学生証に対してデジタル署名を付与し、それを学生に送付します。
3. (学生) 学生は受け取った学生証が当該教育機関によって発行されたものか確認するため、学生証に記載されたDIDを解決し、DIDドキュメントに記載された公開鍵を取得します。
4. (学生) 学生は取得した公開鍵で、学生証のデジタル署名を検証し、確かに当該教育機関によって発行されたものであると確認します。
5. (学生) 学生は企業に対して学生証を提示します。
6. (企業) 企業も同様にDIDを解決して取得した公開鍵でデジタル署名検証を行います。

まとめ

3本の記事を通して、DID,VCそれぞれの説明とDIDとVCでできることについて解説しました。

- 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」

今後の記事ではよりディープな内容を書く予定です。

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を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/c398421fc23a14