

DID,VC入門(2) - Verifiable Credentials(VC)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。

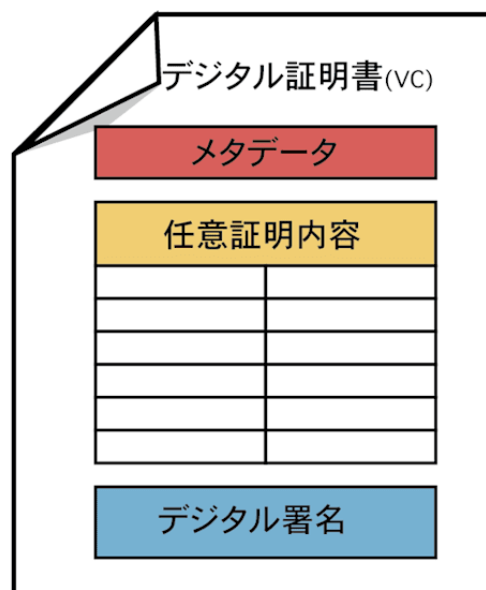
- 1部: Decentralized Identifiersとは
- 2部: Verifiable Credentialsとは
- 3部: DIDとVCでできること

第2部として本記事ではVC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。

Verifiable Credentials(VC)

VCは2021年にW3Cが標準化した**検証可能なデジタル証明書の規格**です。VCを新たな技術と捉える人も多くいますが、単に「**デジタル署名付きのデータの書き方**」です。一方で、デジタル証明書の規格が統一されることで、データの相互運用性が担保され、発行者が異なる別々のデータの連携が容易になる可能性があります。例えば、電子カルテがVCに統一されることで、違う病院同士で病歴の共有が可能になるかもしれません。



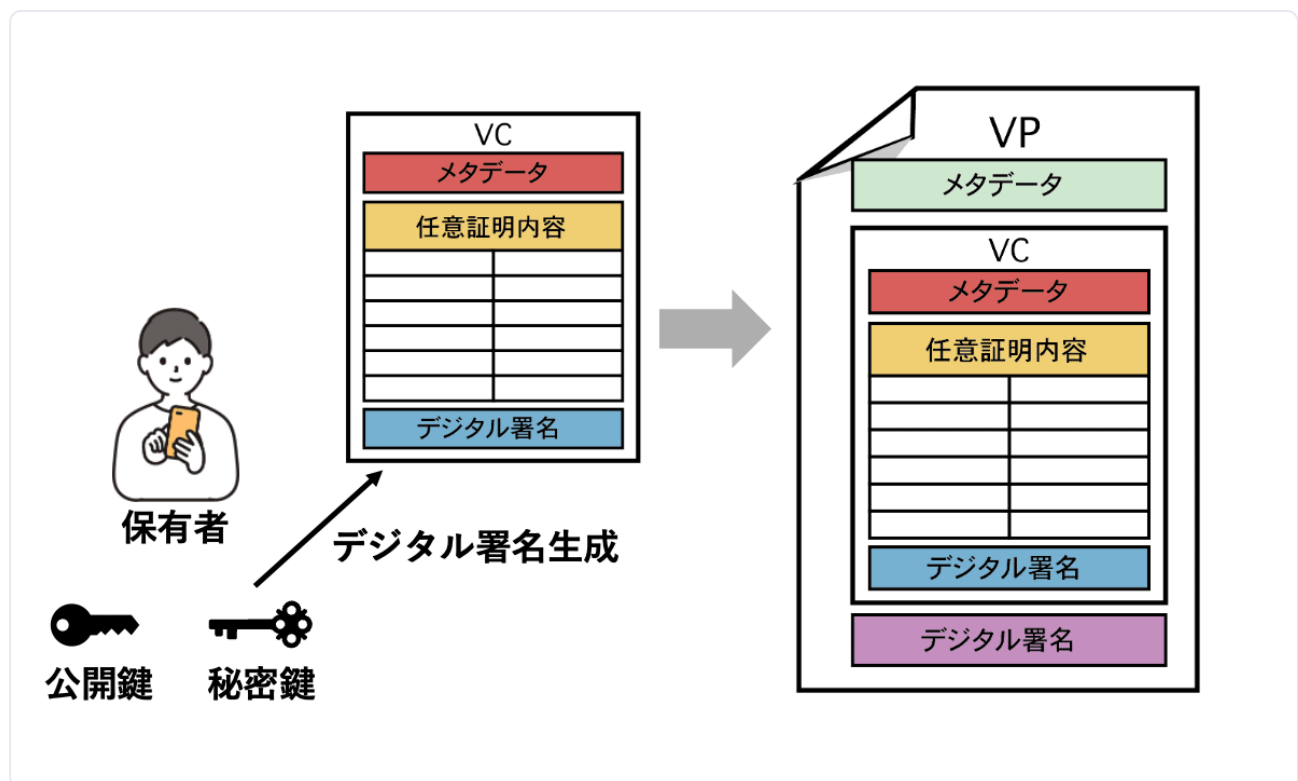
VCを構成する3要素 (メタデータ / 任意の証明内容 / デジタル署名)

VCは以下の3つの要素によって記述されます。

- **メタデータ**: 発行者の情報、発行日時、有効期限などを記載します。発行者の情報として発行者の公開鍵情報とリンクさせることで、デジタル署名検証に用いる公開鍵を明示することもできます。
- **任意の証明内容**: デジタル証明書として証明したい任意の内容をこの中に記載します。
- **デジタル署名**: デジタル署名技術によりデジタル証明書の改竄の検知が可能です。後から事実の否定を行う否認を防止します。

Verifiable Presentation(VP)

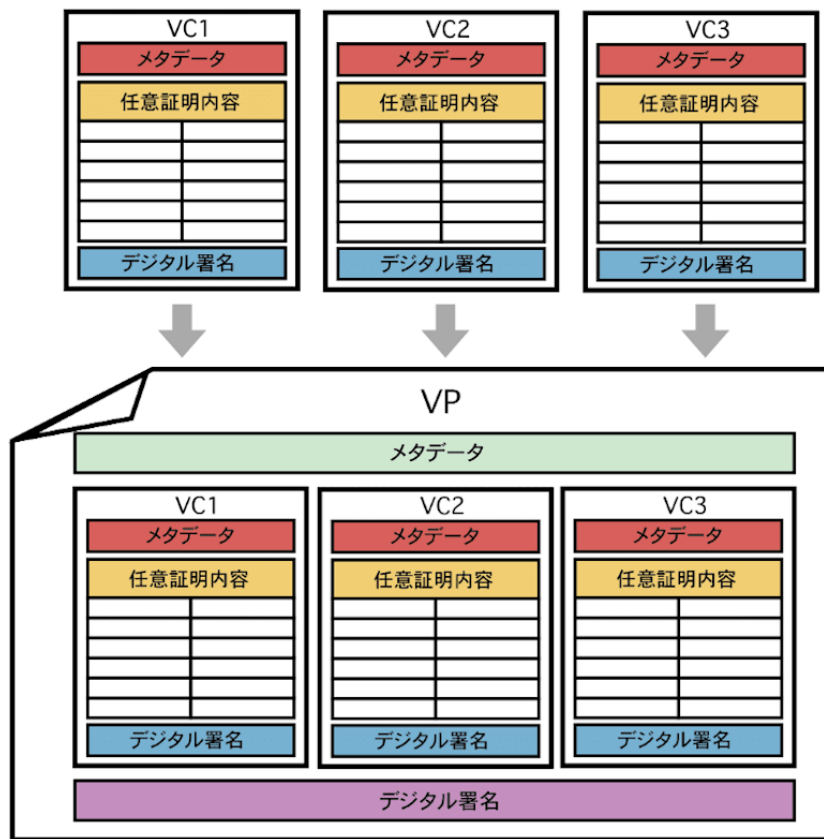
保有者が保管するVCを第三者(Verifier)に対して提示するとき、保有者が提示しているということの証拠となる情報が必要です。VCに対してHolderのメタデータを付け加え、保有者の署名鍵でデジタル署名を生成し、付与します。**提示用の保有者データを付け加えたVCをVerifiable Presentation(VP)**と言います。



VPの構成 (メタデータ / VC / 保有者によるデジタル署名)

- **メタデータ**: 保有者の情報(保有者の識別子など)、VPの生成日時などを記載します。
- **VC**: VCを載せます。
- **デジタル署名**: VPにおける上記2つの項目に対して、保有者がデジタル署名を付与します。

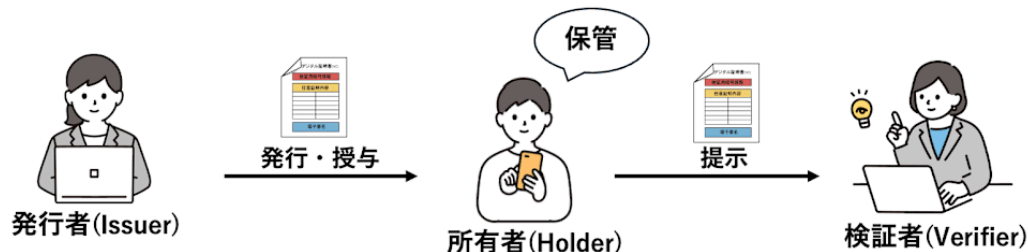
配列形式で複数のVCをまとめてセットにしたVPを作ることも可能です。



複数のVCをまとめたVP

VCの意義: IHVモデル

VCにおいて最も重要なのが**Issuer(発行者)**, **Holder(保有者)**, **Verifier(検証者)**の3者によって成り立つ**IHVモデル**です。発行者がVCを発行し、それを保有者が管理、提示された検証者が検証を行うという単純なモデルですが、この**3者の責任の分離が可能なのが重要な意義**です。特に重要なのが、**保有者がサービス提供者(検証者)に対してVCを提示したことを、発行者は感知・制御できないこと**です。



IHVモデル (Issuer / Holder / Verifier の関係)

このIHVモデルに則らず、発行者と保有者が密結合なシステムが多く存在します。VCを発行者の運用するサービス上で保管し、保有者は発行者のサービスに依存するようなサービスです。IHVモデルを壊し

たVC利用をするようなユースケースでは、VCを用いる意義が半減すると筆者は感じています。将来性のない口だけの"相互運用性の向上"を売り文句にしたVCサービスが増えることには違和感を感じます。

VCが抱える課題

VCのようなデジタル証明書の規格は、W3Cが標準化したものの他に、現状mDoc、SD-JWTの3種類があります。この分裂の経緯は複雑で、この先どの標準が普及していくのかは分かりません。分裂の経緯については以下の記事にてまとめています。

[VCの規格分裂の歴史\(W3C VC/mDoc/SD-JWT\)](#)

まとめ

本記事ではVCの概要を説明しました。次の記事ではDIDとVCの説明を踏まえ、「DIDとVCでできること」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/60c6b073440a1a>