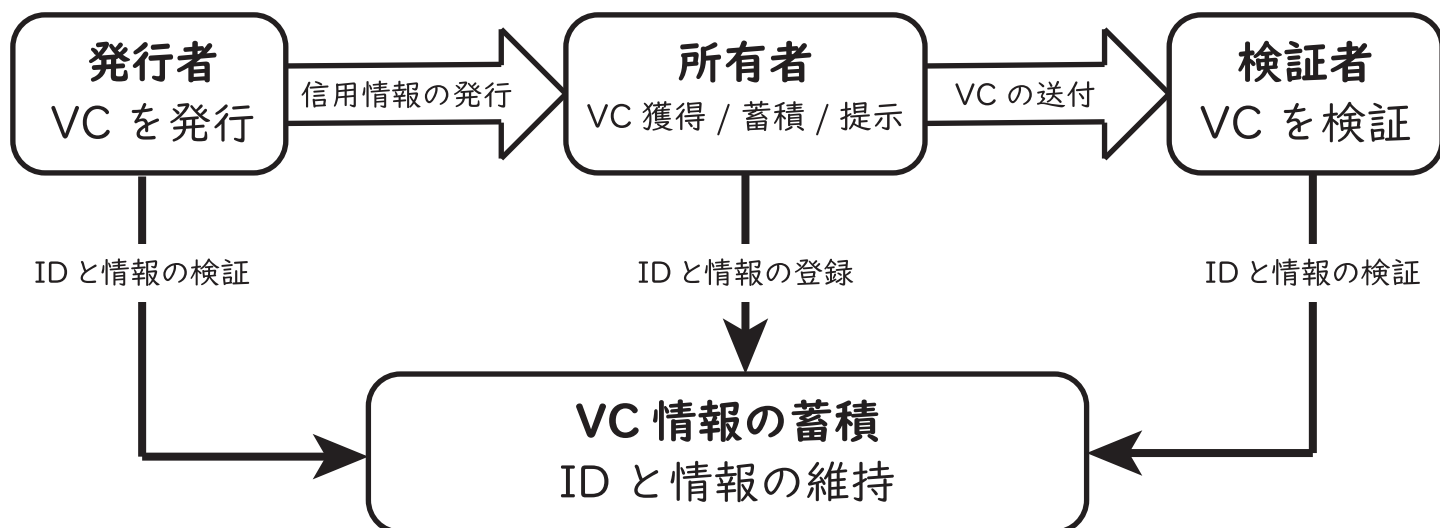


Verifiable Credentials 2.0 を 2025 年 5 月 15 日に発行

デジタル・クレデンシャルの表現、交換、検証をより簡単かつセキュアに

2019年に 1.0 が公開されて以来、さまざまなアプリケーションで利用され続けている Verifiable Credentials 仕様。暗号的に安全で、プライバシーを尊重し、機械的に検証可能な方法でデジタル・クレデンシャルを表現するメカニズムを提供するとともに、特定のアプリケーション（ID クレデンシャル、大学クレデンシャルなど）が独自の用語を使用できるように拡張メカニズムを提供する Verifiable Credentials Data Model 2.0 が 2025 年 5 月に勧告仕様として公開されました。

クレデンシャルの所有者は、それを検証者に提示することができ、検証者はその主張が真に発行者からのものであり、改ざんされていないことを確認できます。検証可能なクレデンシャルの真正性と完全性は、暗号技術の使用、特にデジタル署名と関連する数学的証明の使用によるコンテンツの構造的妥当性のチェックによってもたらされます。これにより、発行者、所有者、検証者の 3 者すべてが、提供する、あるいは提供されるデータの解釈において一貫した信頼メカニズムを持つことになります。



検証可能なクレデンシャルの所有者は、検証者にクレデンシャルのサブセットを提供するとか（プライベート・データの選択的開示を提供）、複数のクレデンシャルを一つにまとめることもできます。これらのいわゆる「検証可能な提示」は通常短命であり、長期間保存されることは意図されていません。ただし一度期限切れになった認証情報をリフレッシュさせるサービスも組み込まれています。署名と暗号化に使用される標準は、エコシステムで広く採用され展開されている暗号化手法に基づいています。

これはあなた個人の信用情報（人に限らない）が正しいということを第三者が検証して確認できる仕組みです。

コロナ禍の最中にはワクチン接種証明書がスマホで発行されていましたね。日本ではかなり早いうちから VC が使われてきたのです。



また貿易などのサプライチェーンにおいては多くのステークホルダー間で正確な情報をセキュアにやり取りする必要があるため VC の適用が検討されています。

一方 VC の中でも使われる DID は分散型 ID と呼ばれ、従来の企業などが集中で管理する ID・パスワードに代わり、個人が自分で ID を管理して、必要な情報だけを必要な人と共有する仕組みです。

例えば米国カリフォルニア州の DMV（運転免許システム）では、発行者および所持者のデバイスを識別するために使用される検証可能な証明書に DID を活用しています。2024 年 9 月現在では 600,000 件、1 日あたり 1,200 件が追加されています。

