

別紙 1

VCs と JTS 登録（リモート署名サービス：VCs 対応）の概要

属性証明をデジタル完結で実現する主要な基盤技術として、Verifiable Credentials（発行者が誰であるかおよび改ざんされていないことを検証可能な資格証明：以下「VCs」）および Verifiable Presentations（複数の VC から必要な情報を選択・組み合わせた検証可能な提示データ：以下「VPs」）があります。

※属性証明とユースケース例に関する説明は別紙 2「属性証明とユースケース例」をご参照ください。

■ VCs や VPs の社会実装

欧米では VCs や VPs の社会実装に向けた準備が進んでいますが、今後日本でも、信頼のおける VCs や VPs を活用したシステムが増えることが想定されます。

VCs や VPs の社会実装により、サービス提供側は必要以上の個人情報を保有せずに、口座開設サービス、ファン限定チケット販売、就職・転職サポートや年齢確認サービスなどの提供が、また、利用者側は自身のプライバシーを守り、なりすまし被害から守られながら、安心してサービスを利用することができます。

その安心の実現は VCs、VPs を生成するためのリモート署名サービスの安全性・信頼性の確保が重要なポイントとなります。

VCs、VPs を生成するリモート署名サービスと利用者の関係は図 1 のとおりです。

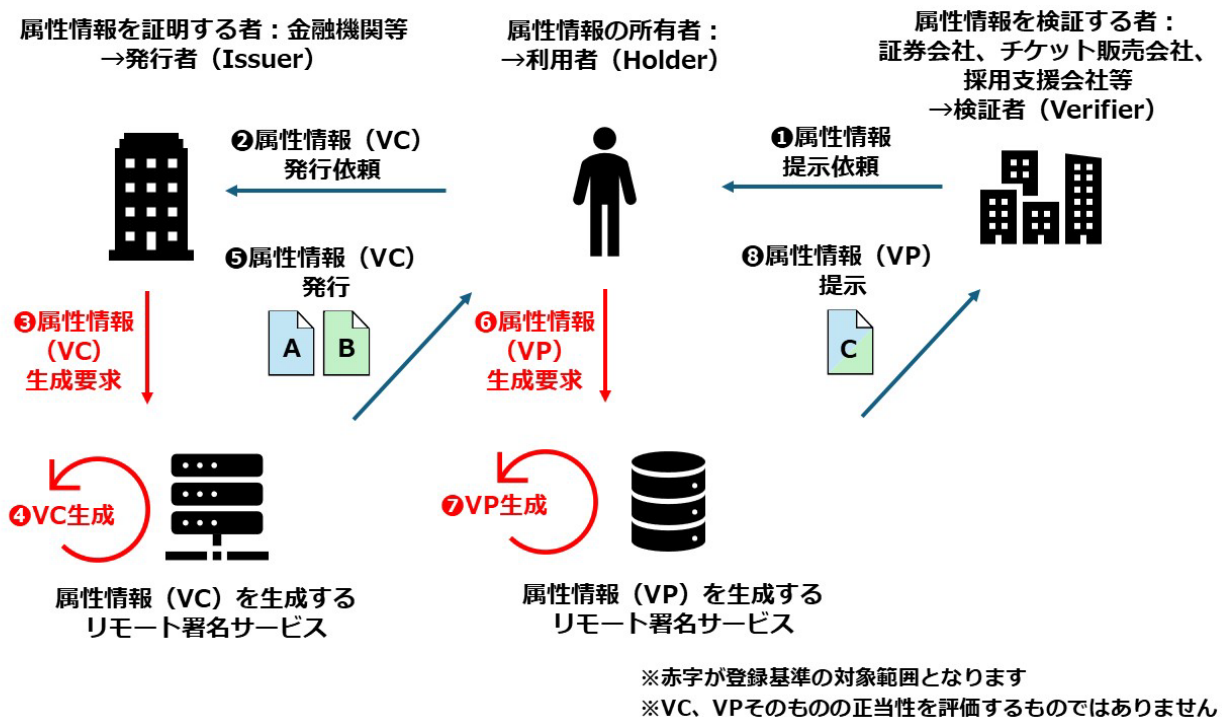


図 1：VCs、VPs を生成するリモート署名サービスと利用者の関係

■ JTS 登録の審査・登録の観点

VCs や VPs への電子署名を行う発行者（Issuer）や利用者（Holder）には、

- ・発行者や利用者の指示に基づき電子署名を生成する運用力
- ・秘密鍵を高度な暗号装置で安全に管理する技術力

が求められます。

今回、「Creclude」上での VCs 発行や VPs 提示の際に用いられるリモート署名機能の信頼性を、

- ①運用（内部牽制を考慮した運用体制の構築等）
- ②技術（世界標準に準拠した暗号装置を使用した秘密鍵の管理等）
- ③設備（厳格な入退室管理の実施等）

の三つの観点に基づき審査・評価をしました。

JIPDEC は、VCs、VPs の電子署名に使用する秘密鍵を安全に管理し、正当な署名権者からの認可に基づきリモートで電子署名を行う「リモート署名サービス」の信頼性確保や評価に向けた取り組みを進めています。今回の登録においては、両社の運営体制および技術基準を総合的に評価し、署名対象が異なる VCs および VPs へのリモート署名機能を独立して登録しました。

現在、JIPDEC では、リモート署名機能だけでなく、VCs の発行に必要な属性証明サービスの全体の運用プロセス等も含めた登録基準を検討中です。VCs に係る主要関係者間の信頼性確保の在り方や評価の方向性について検討を進め、安心して利用できるデジタル証明の普及と、信頼できるデジタルトラスト環境の形成に取り組んでいきます。