Trusted Web の実現に向けたユースケース実証事業

基本設計書

令和 6 年

電通総研

目次

1. 業務フロー

本システムでは、所有者が法人口座開設に必要な KYC(本人確認)・KYB(法人確認)・在籍証明のデジタル証明(VC)を取得し、最後にそれらを金融機関へ提出して口座を開設するフローを想定している。

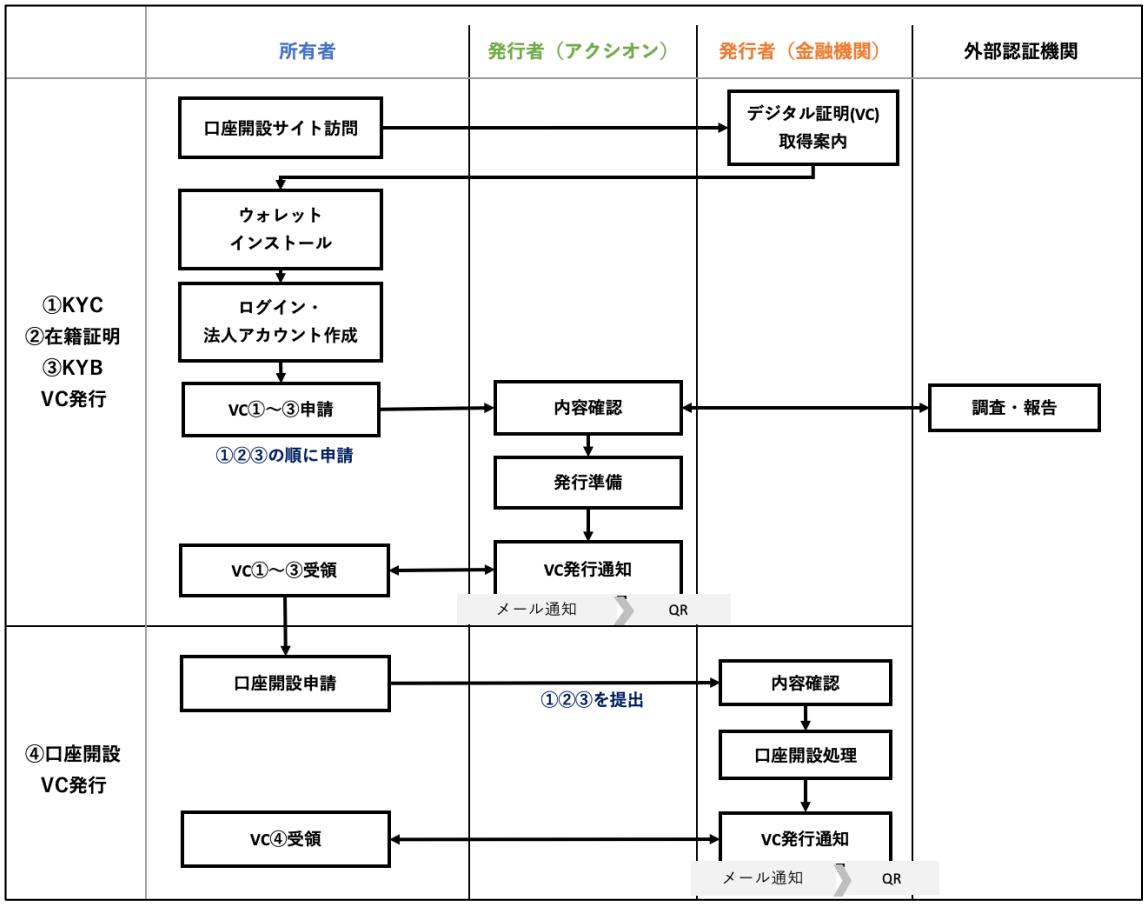

図 1.1

※在籍確認は KYC VC 取得後、又は並行して所有者が自身の企業へ依頼を行う。デモでは事前に在籍確認を行なっている想定のため、本フローには入れていない。

2. 機能一覧

機能/ 非機能	機能名	機能概要
機能	アカウント管理	VC 発行の申請を行うための個人・法人のアカウント管理機能
機能	KYC VC 発行申請	所有者が口座開設に必要な KYC VC の発行を申請する機能
機能	在籍証明 VC 発行申請	所有者が口座開設に必要な在籍証明 VC の発行を申請する機能
機能	KYB VC 発行申請	所有者が口座開設に必要な KYB VC の発行を申請する機能
機能	口座開設申請	所有者が口座開設の申請を行う機能
機能	デジタル証明申請一覧	過去の申請一覧。承認された申請は VC の発行（受取）が可能。
機能	デジタル証明一覧	過去に発行したデジタル証明の一覧。
非機能	可用性	プロトタイプのため障害発生時の機能停止は実装していないが、クラウドとブロックチェーンがベースにあるため基本的にはノンストップで稼働。
非機能	運用・保守性	・プロトタイプのため、メンテナンスの実施は計画していない。 ・バックアップ方針について 秘密鍵に関して Threshold ECDSA Signature（tECDSA）を使う場合は、ICP のルールに従って行う。tECDSA のかわりに Passkey を使う場合、サーバ（Firebase）に保存する認証関連情報は Firestore に保存され、Google が保守運用を行う。秘密鍵自体のバックアップは Passkey によって複数端末に保管される。VC のバックアップと共に今回は実装外。将来的には、WebAuthn の prf extension を使って暗号化し、クラウドに保存する予定。
非機能	性能・拡張性	業務量及び機能が増加した場合も、tECDSA 部分以外は Firebase・Expo/React-Native を活用してスケールアウトによるシステム運用を行うことができる。

非機能	セキュリティ	・今回のスコープでは暗号化は行わない。将来暗号化を行う場合、WebAuthn の prf extension を使用する。パスワードを使っているのは tECDSA で Google 認証を使うケースであり、本システムでパスワードは管理しない。 ・現在の実装方式だと、Wallet で署名して、IdToken と署名を同時に Canister に送るので、トークンインジェクションの問題は起こらない認識。 ただし、Passkey/WebAuthn 固有のセキュリティリスクには、常に備えておく必要がある。
非機能	移行性	VC を使った業務は現状行われていないため、現行業務からそのままトランジションすることは難しいが、KYC に関する現状ノウハウは活用することができる。

3. ネットワーク構成

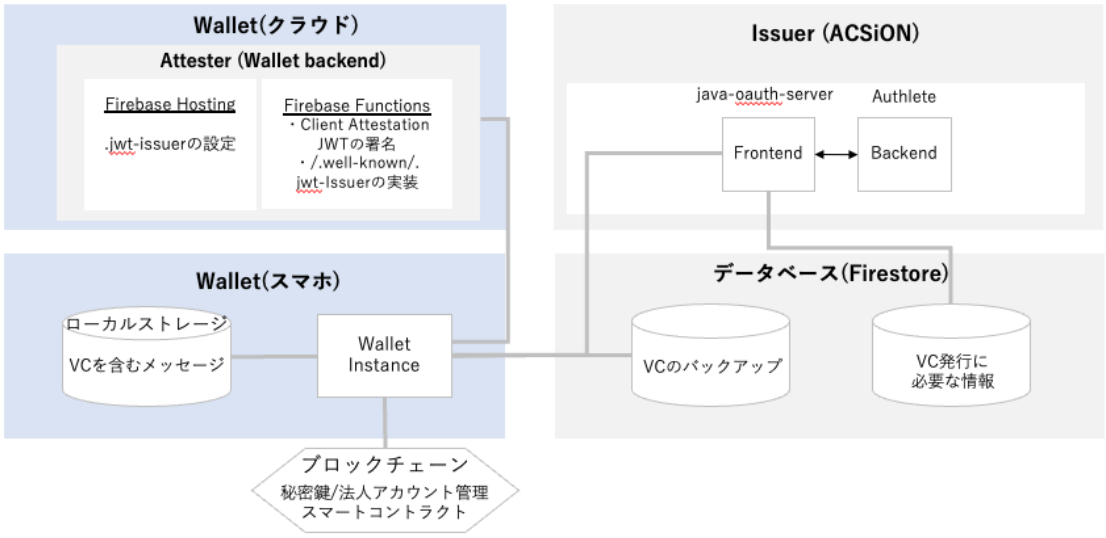

図 3.1

4. 画面遷移

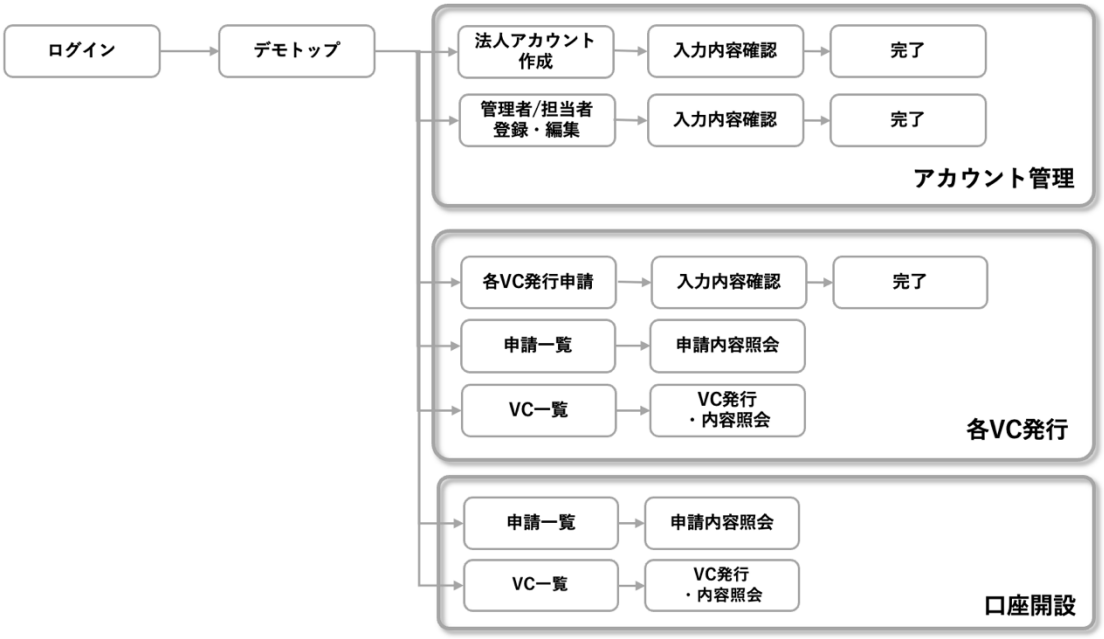

図 4.1

5. データモデル定義

属性値	属性取得元	属性値 （vc 内）
姓	holder	firstName
姓（カナ）	holder	firstNameKana
名	holder	lastName
名（カナ）	holder	lastNameKana
生年月日	holder	birthday
氏名	holder	name
性別	holder	sex
住所（都道府県）	holder	prefecture
住所（市区町村）	holder	city
住所（番地）	holder	block
住所（建物）	holder	building
法人名	holder	corporateName
入社年月日	holder	employmentDate

勤続年数	holder	serviceYears
法人番号	holder	corporateNumber
設立年月日	holder	establishDate
口座種別	holder	accountType
振込形態	holder	transferType
発行元	issuer	Issuer
発行日	issuer	issuanceDate
有効期限	issuer	expireAt