

SKKN

認証器に紐づいた検証可能なデジタル証明書

渡邊 健

川原 悠佑

水野 重弦

福田 岐弦

GitHub repo

<https://github.com/dorakemon/passkey-hackathon-2024-sakolab>



SKKN = SaKoKeN

早稲田大学の佐古研究室です！



プライバシーに配慮してモザイクを適用



作ったプロダクト

認証器に紐づいたVerifiable Credentialsの発行と提示！



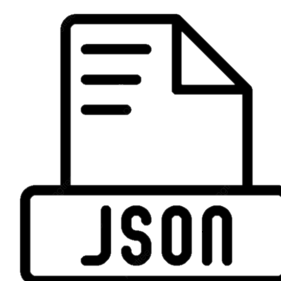
疑問

Verifiable
Credentials(VC)
って何だっけ...?

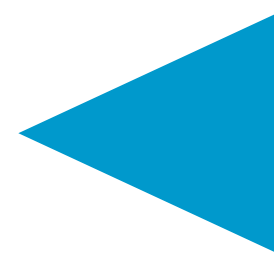


背景知識

VCとは、あなたの氏名、所属、住所などの情報を証明する、デジタル証明書です
(ニュアンス👉)



VC



Issuer

パスキー太郎氏の所属する
Zoozle社

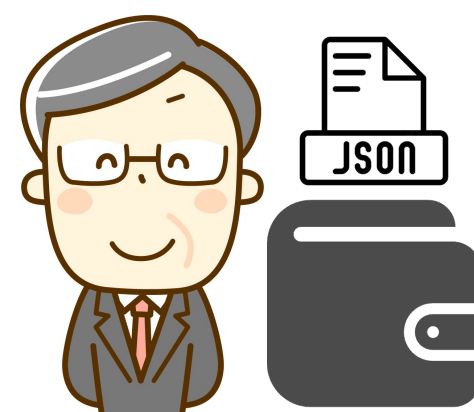
Zoozle



VC発行

Holder

VCを受け取ったパスキー太郎氏
ウォレットに保管



会社の発行した部
長の社員証VCだ！

VP提示

Verifier

機密データを守る扉。部長以外開けられない。



背景知識

Issuer

パスキー太郎氏の所属する
Zoozle社

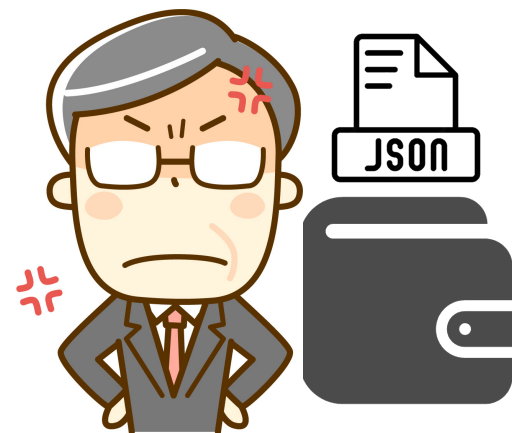
Zoozle



VC発行

Holder

VCを受け取ったパスキー太郎氏
ウォレットに保管



VP提示

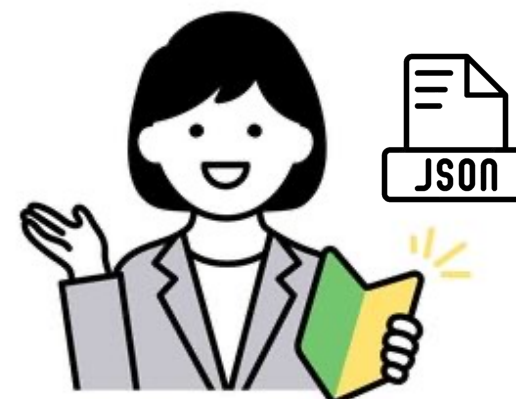
Verifier

機密データを守る扉。部長以外開けられない。



部長が脆弱なウォレットを
使ってるらしい！

ハッキングが得意な新入社員Aさん

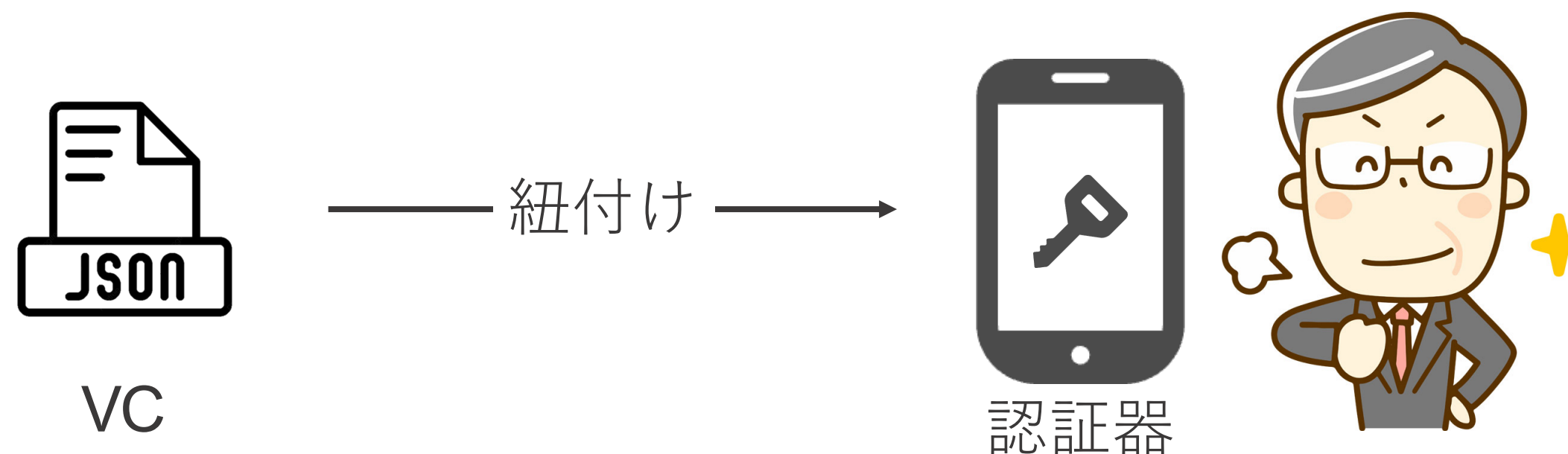


VP提示



やりたいこと

FIDO keyを持つ人(部長)だけがVCを提示できるようにしたい！



信頼できるウォレットサービスだけでVCを扱えるようにしたい！

Zoozle



信頼

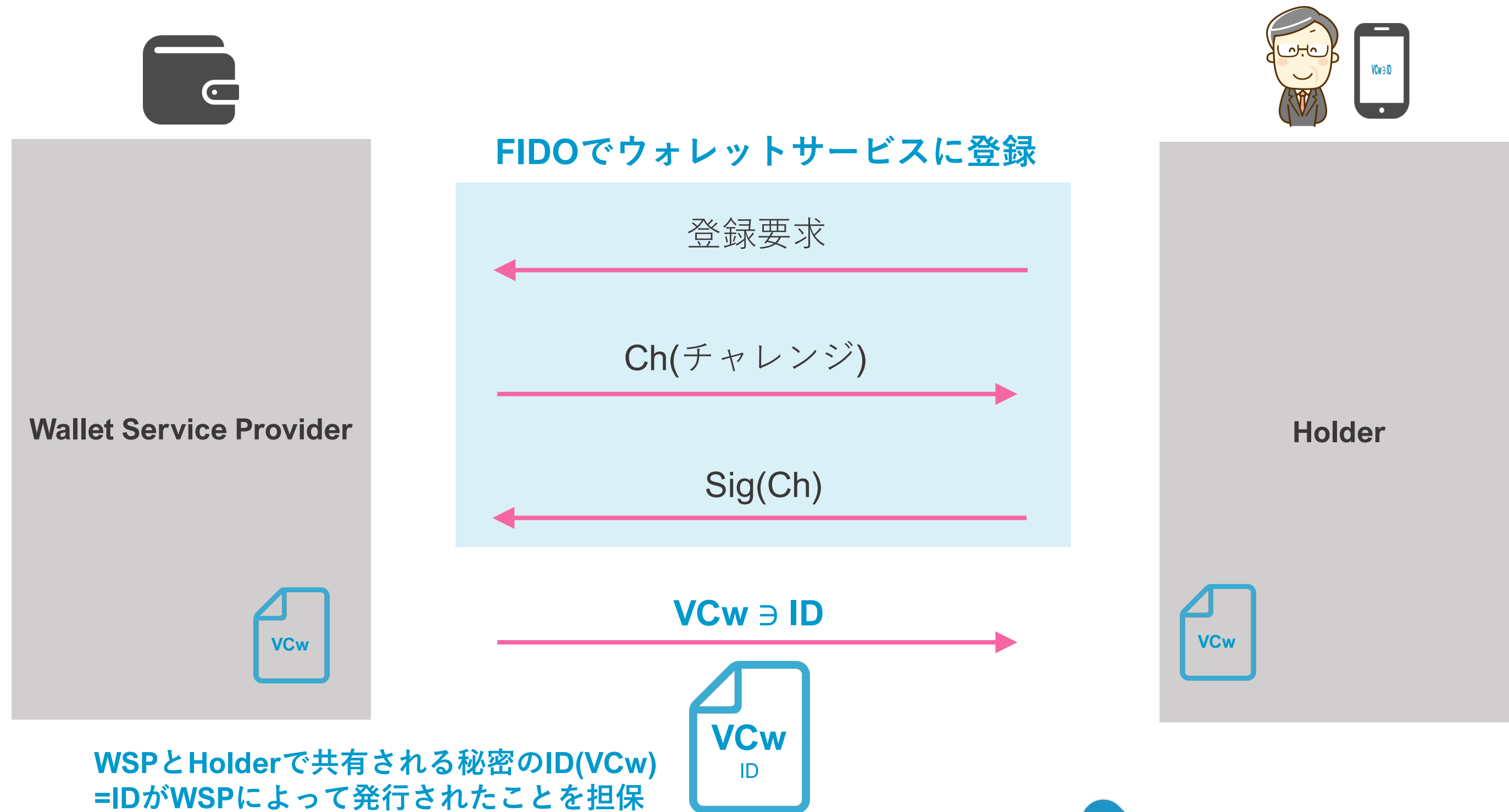


Zoozle



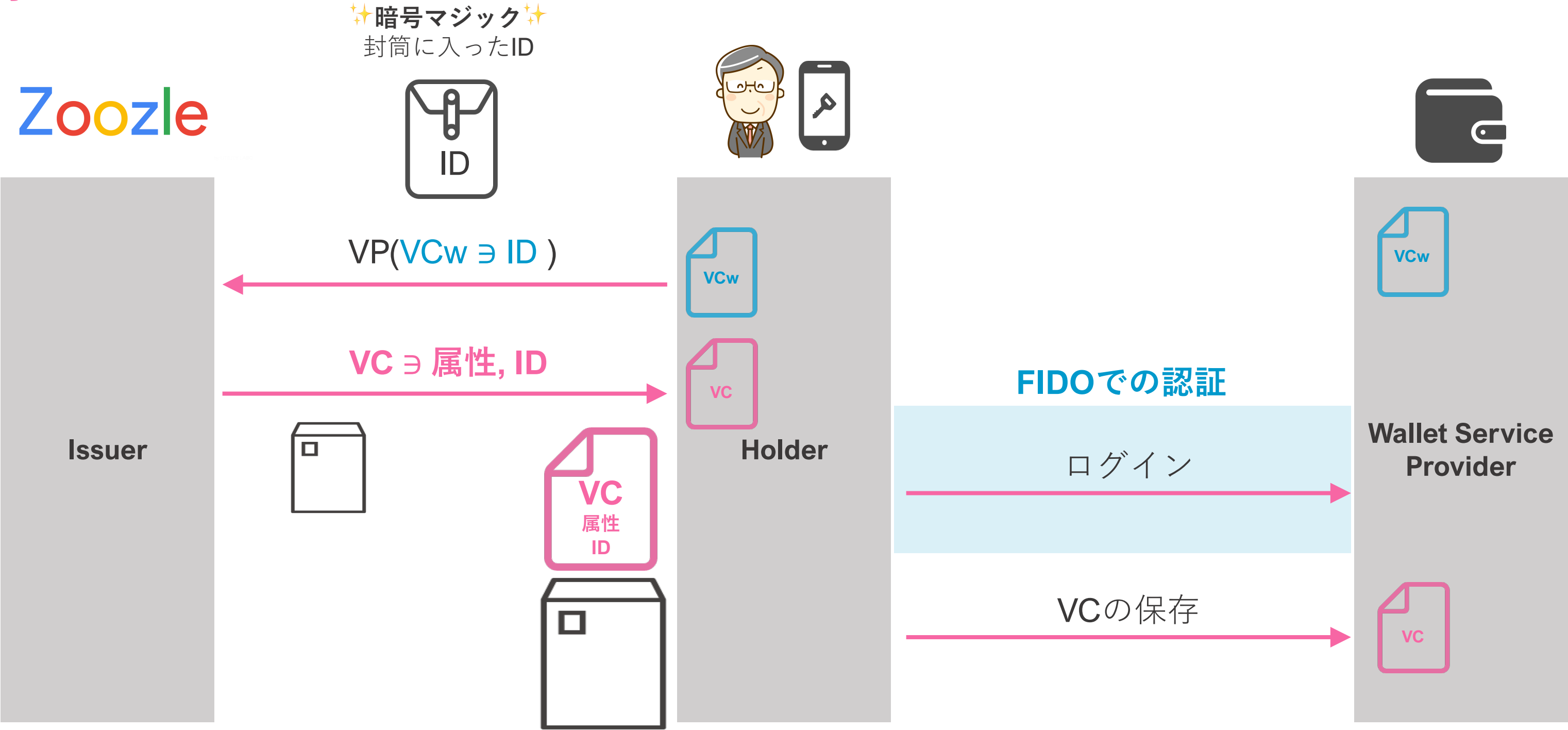
プロトコル

ウォレットサービスへの登録



プロトコル

VCの発行



プロトコル

VCの提示



VCwを持っている
(=FIDOで認証された)
人からのVCだ！



Verifier

Holder

Wallet Service Provider

$VP(VCw \ni ID)$

VCwに書かれたID=VCに書かれたID
のゼロ知識証明

$VP(VC \ni \text{属性}, ID)$

ウォレットにより担保されている
人間からの提示と分かる

VCwとVCの2段階認証

VCの取り出し



プロトコル

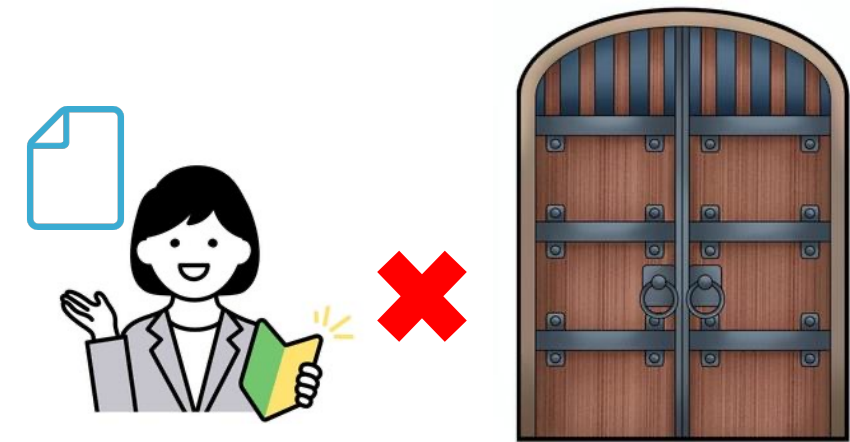
バックアップ(端末の移行)



嬉しいポイント

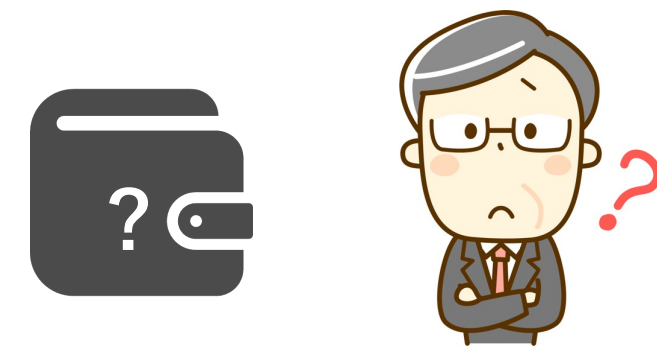
1. VCとFIDO keyを紐付けて発行、提示ができる

ハッキングの上手い新入社員がVCを知ってしまっても、
VCwを知らなければドアを開けられない！
=VCと認証器のバインディングができる



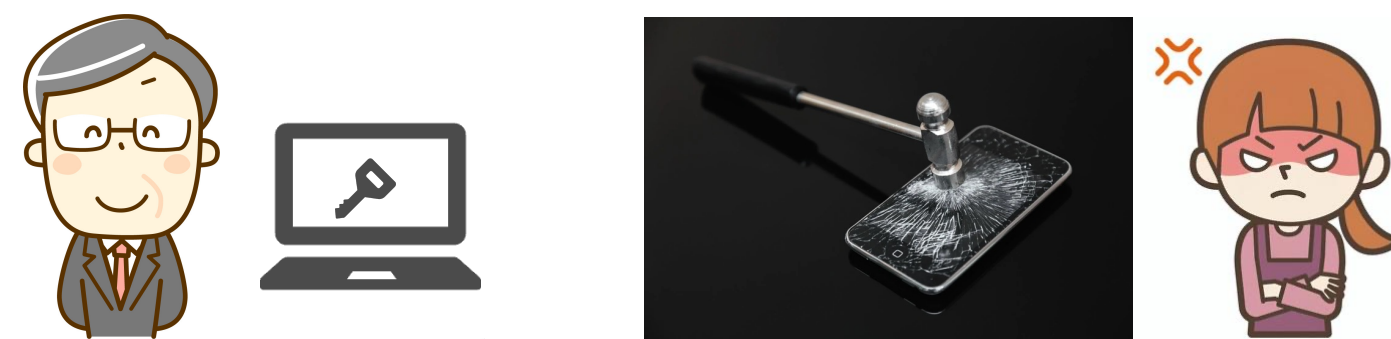
2. Issuer、Verifierが信頼したウォレットサービスだけ利用可能

部長が怪しいウォレットサービスを使っている場合、
VCwの検証によって会社はVC発行、ドアはVP提示を拒否できる
=ウォレットサービスのトラスト形成



3. FIDOを使ってVC, ウォレットのアカウントのバックアップが可能

部長がスマホ(認証器)を壊されても、パスキーを同期した別のデバイスでリカバリーできる
=UX改善



それでは

デモへ

