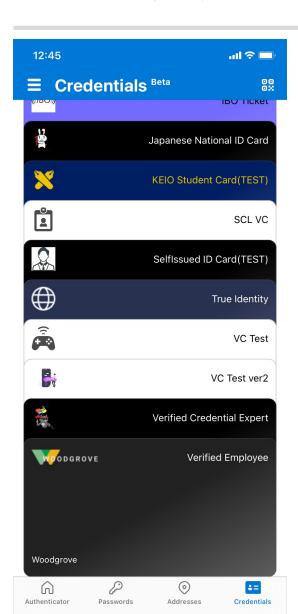


## 教育機関における デジタル資格証明の動向

2021/12/17伊藤忠テクノソリューションズ株式会社OpenIDファウンデーションジャパン富士榮 尚寛 (ふじえ なおひろ)

# デジタル資格証明の現状





- Verifiable Credentialsの実装が出てきている
- 通常「Wallet (ウォレット)」と呼ばれる スマートフォンアプリにカード型の各種証 明書(身分証明書等)を格納して、持ち運 ぶことができる仕組み
- W3C/OpenID Foundation等が標準化している標準仕様に準拠、複数ベンダが提供している基盤やWalletで相互運用性あり
- Walletとしては**Microsoft Authenticator**など も利用可能(多要素認証 + αとして利用)

# 特徴と利活用シナリオ



### 特徴

- ポータブルであること
  - スマホ等のアプリに保存できる
  - 標準化されたデータモデルとデジタル署名の利用
- 身分証明書の**真正性**を受け取り側が**発行元に問い合わせすることなく検証できる**こと
  - 都度、システム同士の連携開発が不要。疎結合なシステム構成が実現可能
  - 分散台帳を使った署名検証用の公開鍵の分散管理と鍵探索の仕組み(標準仕様)

### • 利活用シナリオ

- 身分証明(学生証、社員証等)
- 資格証明(資格試験、免許、学位等)
- 所持証明(チケット等)
- →「発行された資格情報・身分情報を、不特定な場所で検証したい」シナリオ

# 事例) 慶應義塾大学様



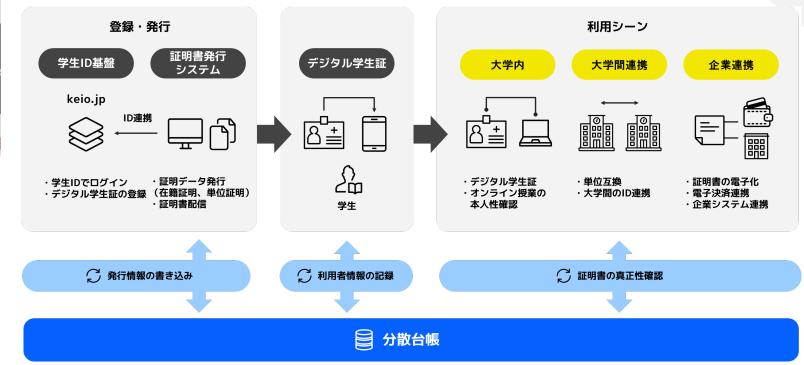


#### 参画組織

- •慶應義塾大学
- ・伊藤忠テクノソリューションズ株式会社
- ·Japan Digital Design株式会社
- ・株式会社ジェーシービー
- ·西日本電信電話株式会社
- ·BlockBase株式会社
- ·Microsoft Corporation(基盤提供)

#### 各種個人証明(在学証明、卒業証明等)をスマホアプリに格納、 ポータビリティの実現と、確実な検証を可能とする

- オンライン・オフラインの両方で利用可能な身分証明書
- ・ 塾内だけでなく大学間・企業との連携など広く展開を目指す
- ・ 大学発行の証明書以外に民間の発行する証明書も格納
- 分散型IDの標準技術利用により永続性、相互運用性を実現



## ポータブルで信頼できる姿が目標



#### ポイント

#### 物理世界のID

#### 従来のデジタルID

#### 分散型ID (DID/VC)

#### ポータブル

#### 利用者の意思で、

- いつでも使える
- 使い分けができる(持ち運べること)

- 財布に入れて免許証、社 員証などを持ち運ぶ
- ・ 使い分けができる

- IDシステム状態に依存する(システム停止、アカウント停止等)
- 提示情報の使い分けは難 しい(利用者の意思は反 映されにくい)
- スマホ、NFCチップ等に IDを入れて持ち運ぶ
- ・ 提示属性の<mark>選択・使い分</mark> **け**ができる

#### 高度な信頼

#### 受取った側が、

- 真贋判別が出来る (検証可能であること)
- 対面で表情などを含め総合的に判断
- 勘と経験で免許証の真贋を判断
- IDシステムでユーザ認証 して検証する(認証強度 によりI**D漏洩の危険性**)
- IDシステム状態に依存する(システム停止等)
- 分散台帳上の公開鍵を使い、ID発行元への問い合 わせせずに検証可能 続性の担保、事業者依存からの脱却)

対面前提、勘と経験

ID漏洩、プライバシ問題

真のDXの要として注目



#### 中心となる技術要素

- 分散台帳上で管理される分散型識別子(Decentralized Identifiers / DID)
- 分散型識別子と関連付けされた公開鍵で<mark>検証可能な属性情報</mark>(Verifiable Credentials / VC)

# 教育機関における資格証明



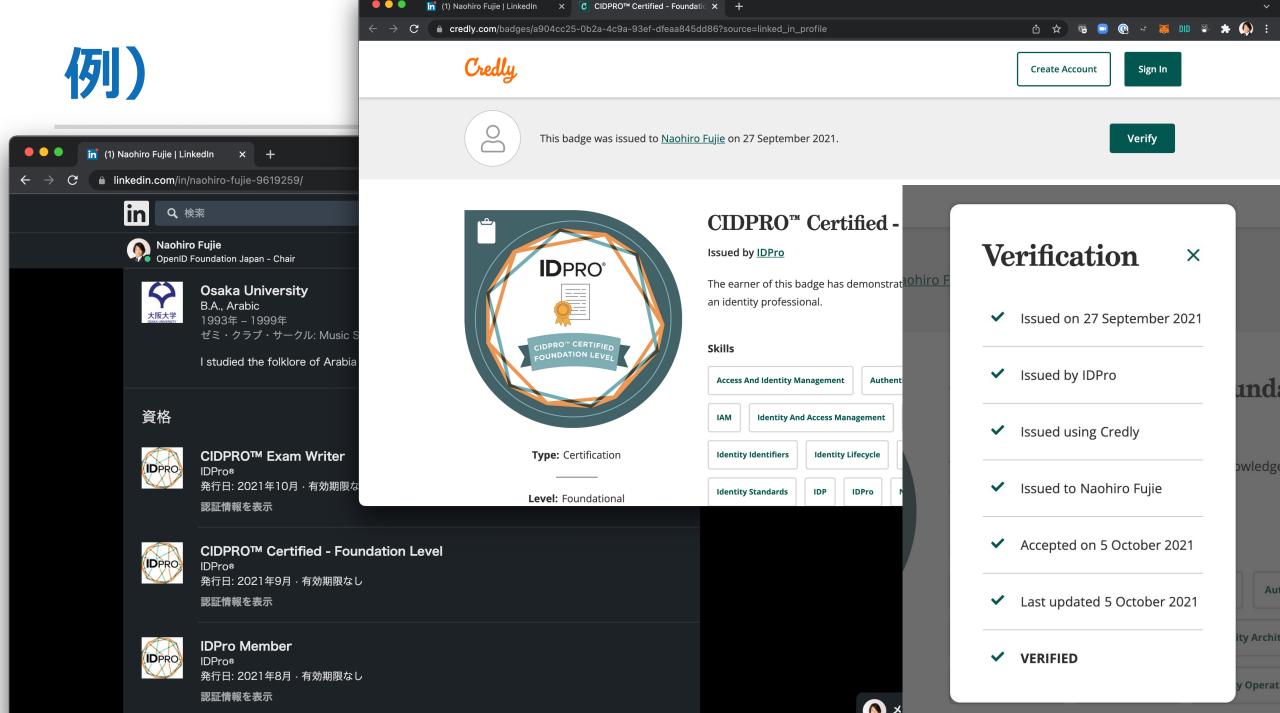
- 現状のデファクトは「オープンバッジ」
- 技術標準規格にそって発行されるデジタル証明/認証。資格情報をSNSなどで共有、オープンバッジの内容証明を行うことが可能(Wikipedia<sup>1</sup>より)
- 画像ファイル (png/svg) にメタ情報として資格情報を埋め込み (Bake) 、 発行/表示/保管を行う
- IMS Global Learning Consortium<sup>2</sup>中心に推進、国内だと一般財団法人 オープンバッジ・ネットワーク<sup>3</sup>などが認定機関となっている
- Credly⁴などで発行されたバッジをベンダ資格などで利用している例も
- 現状(v2)は資格証明の検証を行う際は問い合わせ型(Hosted)を行う実装が殆ど。自己完結型(Signed)の推進を目指している(v3)

<sup>1.</sup> https://ja.wikipedia.org/wiki/%E3%82%AA%E3%83%BC%E3%83%97%E3%83%B3%E3%83%90%E3%83%83%E3%82%B8

http://www.imsglobal.org/

https://www.openbadge.or.jp/

<sup>4.</sup> https://info.credlv.com/



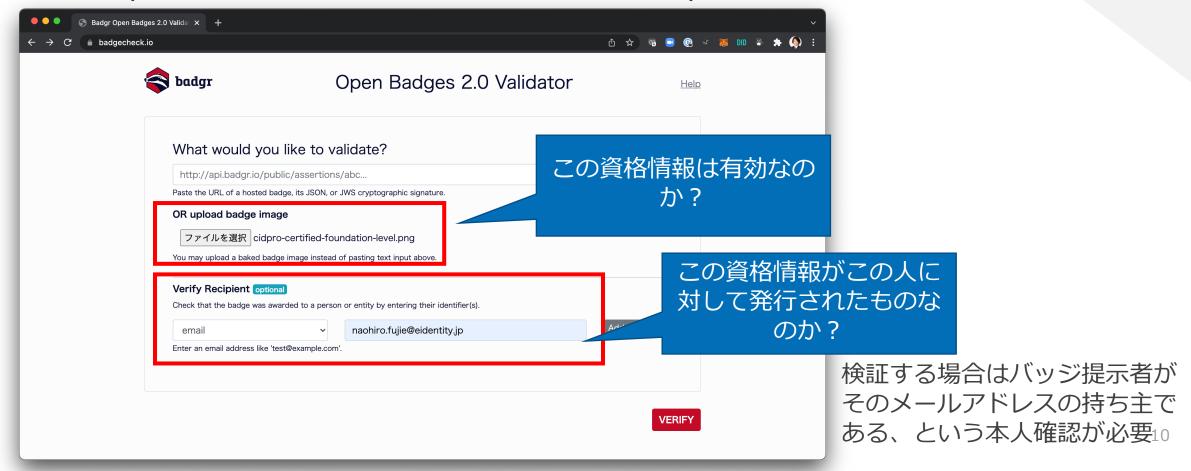
```
cidpro_badge_detail.json
     {} cidpro_badge_detail.json × {} cidpro_award_detail.json
      Users > naohirofujie > OneDrive > DOCS > セミナ > 20211217_AXIES > {} cidpro_badge_detail.json > ...
                                                                                                                  資格情報に関する情報
                "@context": "https://w3id.org/openbadges/v2".
                "criteria": {
                    "@context": "https://w3id.org/openbadges/v2",
                    "id": "https://www.credly.com/org/idpro/badge/cidpro-certified-foundation-level",
                    "narrative": "Assessment: The CIDPRO™ exam covers five areas of expertise in identity and access management: Basic elements of an identity solution Identifie
               },
                "description": "The earner of this badge has demonstrated knowledge of the foundational elements required of an identity professional.",
                "id": "https://www.credly.com/api/v1/obi/v2/issuers/efa23af3-911f-42ec-af5e-d3dfebc65eaa/badge_classes/dbc29974-badb-4fd1-8831-956f60294053",
                "image": {
                    "@context": "https://w3id.org/openbadges/v2",
                    "id": "https://images.credly.com/images/ff9ebf9e-2e1d-4b55-80d0-ead6a2a49464/IDPro_R2__CIDPRO_Foundation.png"
               "name": "CIDPRO™ Certified - Foundation Level
                "issuer": {
                    "@context": "https://w3id.org/openbadges/v2",
                    "description": "IDPro exists to globally foster ethics and excellence in the practice and profession of digital identity.",
                    "email": "info@credly.com",
                    "id": "https://www.credly.com/api/v1/obi/v2/issuers/efa23af3-911f-42ec-af5e-d3dfebc65eaa",
                    "image": "https://images.credly.com/images/c1f2e2e7-0f85-4235-9f4d-c35bf4cceca0/large_blob.png",
                    "name": "IDPro",
                    "type": "Profile",
                    "url": "https://www.idpro.org/"
               },
                                                                                                                    発行者に関する情報
                аттаннент : [],
                "tags": [
                    "Access And Identity Management",
                    "Authentication",
                    "Authorization",
       30
                    "CIAM",
                    "FIDO",
                    "Federation",
                    "IAM",
                    "IDP",
                    "IDPro",
                    "Identity And Access Management",
                    "Identity Architecture",
                    "Identity Ethics",
   行 1、列 1 タブのサイズ: 4 UTF-8 LF JSON ₽ △
```

cidpro\_award\_detail.json {} cidpro\_badge\_detail.json {} cidpro\_award\_detail.json × Users > naohirofujie > OneDrive > DOCS > セミナ > 20211217\_AXIES > {} cidpro\_award\_detail.json > ... "@context": "https://w3id.org/openbadges/v2", "badge": "https://www.credly.com/api/v1/obi/v2/issuers/efa23af3-911f-42ec-af5e-d3dfebc65eaa/badge\_classes/dbc29974-badb-4fd1-8831-956f60294053", "evidence": [ "@context": "https://w3id.org/openbadges/v2", "id": "https://idpro.org", "name": "IDPro", "genre": "UrlEvidence", "type": "Evidence" 受け取り者に関する情報 "id": "https://www.credly.com/api/v1/obi/v2/badge\_assertions/a904cc25-0b2a-4c9a-93ef-dfeaa845dd86" "issuedOn": "2021-09-27T00:00:00.0007". "recipient": { "type": "email", "identity": "sha256\$071281e466032326ffe4c3238545d31970b2b61d75fae181a283ac0aace09264", "hashed": true "type": "Assertion", "verification": { "type": "hosted" 検証方式に関する情報 24 (Hosted)  $\mathbb{F}$  Sign in to Jira > No active issue  $\,$   $\,$   $\,$  Bitbucket: Naohiro Fujie:  $\,$   $\otimes$  0  $\,$   $\!$   $\,$  0 行 24、列 2 スペース: 4 UTF-8 LF JSON 🔊 🚨



## SELMID

- バッジの検証(例:badgr\*)
- バッジ自体の有効性確認: URL or バッジ画像内のメタ情報の検証
- Recipientの有効性確認:メタ情報内のRecipient(ハッシュ)と入力の一致



# DID/VCとオープンバッジ



ゴール		DID/VC		オープンバッジ(Hosted型)	
用途		特に限定せず		学習履歴、アチーブメントデータの表現	
ポータビリティ		$\bigcirc$	Walletに入れて持ち運ぶ		画像に埋め込んで持ち運ぶ
疎結合			分散台帳上へのアクセスができれば 検証者と発行者の間の直接通信は発 生せず →利用者が発行者に知られず資格情 報を検証者へ提示可能		Linked-DataによるGraph構造 →発行者により検証が行われるため、 <b>利用者が資格情報を提示したことを 発行者は知ってしまう</b>
標準化	ベースレイヤ		DID、VCの <mark>汎用</mark> データモデルは標準化 済み(W3C)		OpenBadgeエコシステム内で標準化
	トランスポー ト	$\triangle$	発行、提示について標準化中 (OpenID Foundation、DIF等)		
	上位	×	上位スキーマは用途ごと		

Blockcertsなど分散台帳とオープンバッジを組み合わせた仕組みはあるが、汎用性はない W3C/**Verifiable Credentials for Education Task Force**(vc-edu)でDID/VCとオープンバッジの組み合わせを検討

## vc-eduでの議論



## どうやってVCとオープンバッジが共存できるか

- 標準化された方法で交換できる、というVCの利点
- 標準化された上位データ構造がある、というオープンバッジの利点

### 検討されている共存パターン

- Learning & Employment Records (LER) competency definitions with Open Badges
   JSON-LD serialization + PDF and linked
  - LERの定義をオープンバッジのスキーマで表現し、PDFに埋め込む方式
- Open Badge as Verifiable Credentials
  - オープンバッジのスキーマの不要な部分を削除しつつVCのスキーマと被らせる方式
- Prioritize Open Badge as VC
  - オープンバッジのスキーマを優先しつつVCのスキーマと被らせる方式
- VC Reference to Open Badge Assertion
  - オープンバッジのAssertion(資格証明部分)への参照をVC内に組み込む方式

## vc-eduでの議論



## どうやってVCとオープンバッジが共存できるか

- 標準化された方法で交換できる、というVCの利点
- 標準化された上位データ構造がある、というオープンバッジの利点

### 検討されている共存パターン

- Learning & Employment Records (LER) competency definitions with Open Badges JSON-LD serialization + PDF and linked 良し悪しはあるもののvc-eduでは本方式をオープ
  - LERの定義をオープンバッジのスキーマで表現し、P
- Open Badge as Verifiable Credentials
  - ・ オープンバッジのスキーマの不要な部分を削除しつつVCのスキーマと被らせる方式
- Prioritize Open Badge as VC
  - オープンバッジのスキーマを優
- vc-eduではユースケースの洗い出しを行いOpen Badge as Verifiable Credentialsでどのような課題があるか議論を進めている状態

ンバッジv3として推奨

- VC Reference to Open Badge
  - オープンバッジのAssertion(資格証明部分)への参照をVC内に組み込む方式

## 今後の課題と展開に関する提言



- 日本の教育機関で使う上で考えられる課題
  - 国際化に関する課題
    - 多言語化
    - 発行機関に関する信頼性(XX大学?と言われても・・・)
  - 日本ならではの利用シナリオの有無と適用可否の検討
    - 学割、就職活動での利用で使えるのか?
  - 資格情報のライフサイクルと運用の課題
- 我々は何をすべきか?
  - DID/VC、オープンバッジ両方の標準化の動きをウォッチし、永く・広く使える資格情報を発行・運用できるように考える。そのためにユースケースを洗い出し標準化団体ヘインプットしていく
  - 現時点のソリューションで短絡的に課題解決を目指さず、**長い目で「ちゃんと」考える**余裕が必要