

デジタル資格証明に関する技術標準

2023/03/13

一般社団法人OpenIDファウンデーションジャパン代表理事
OpenID Foundation eKYC and Identity Assurance WG Co-Chair
伊藤忠テクノソリューションズ株式会社
富士栄 尚寛



自己紹介

経験・役割

- デジタルアイデンティティ分野で約20年の経験を持ち、大手自動車製造業のグローバルID基盤に関するコンサルティング～PMなどを歴任。
- 2018年よりOpenIDファウンデーション・ジャパンの理事に就任、KYC WGを設立。2020年1月より米国OpenID FoundationにてeKYC and Identity Assurance Working Groupの設立および共同議長に就任。2021年6月よりOpenIDファウンデーション・ジャパンの代表理事に就任。
- CTCでは分散型IDとVerifiable Credentialsを利用したオンラインでの各種属性証明を含むデジタルIDビジネスの責任者を務める。

関連する団体

- OpenIDファウンデーション・ジャパン代表理事/KYC WG発起人
- 米OpenID Foundation/eKYC&Identity Assurance WG共同議長
- 日本ネットワークセキュリティ協会/デジタルアイデンティティWG, ISOリエゾン
- 内閣官房Trusted Web推進協議会TFメンバ
- 国立情報学研究所/次世代認証連携検討作業部会メンバ
- 大学ICT推進協議会/認証基盤部会

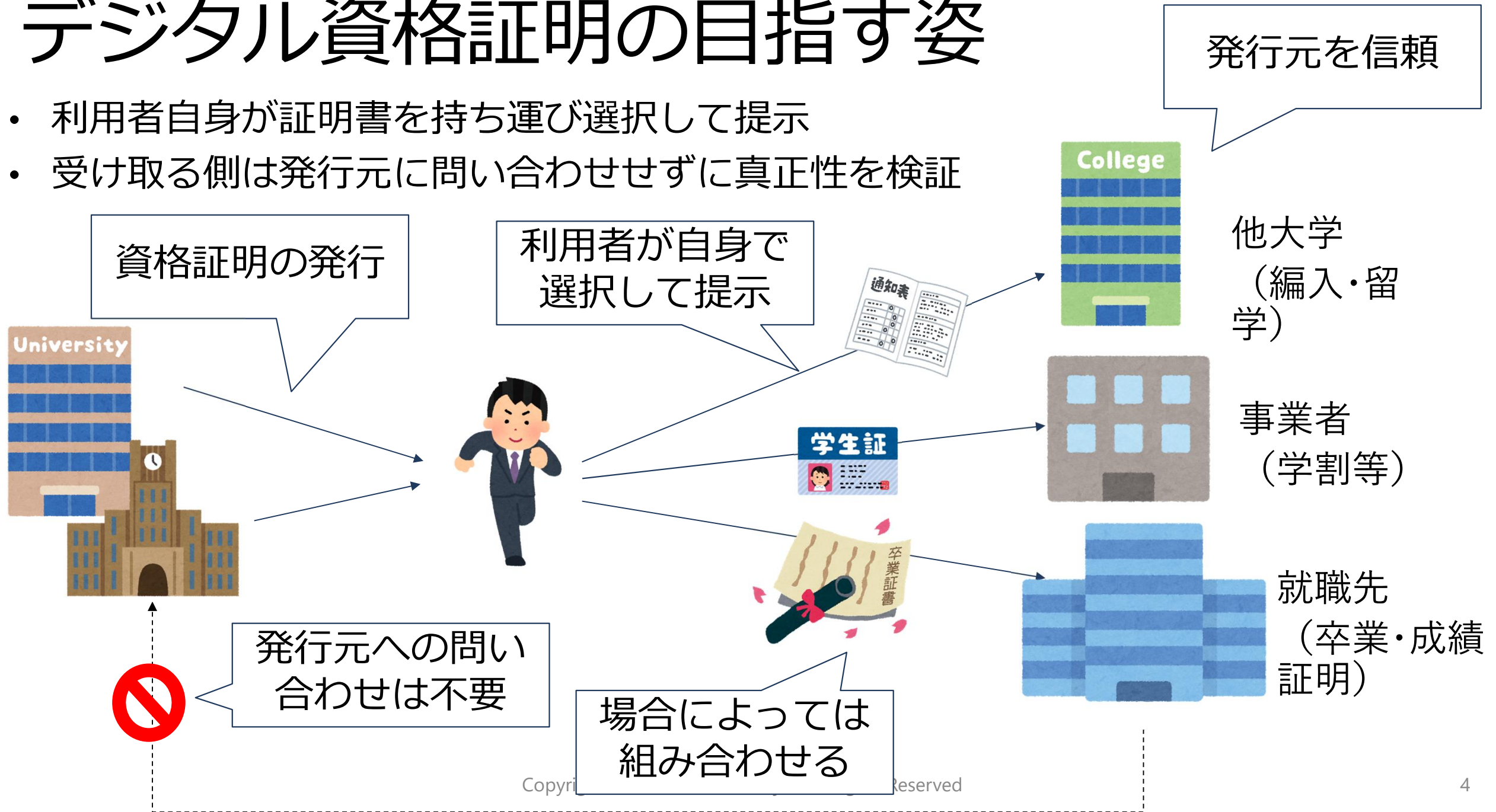
資格証明をデジタル化する際に求められること

- 広くあまねく、永く*1、正しく利用できることが求められる
 - その大学の中だけ、日本の中だけで使えても意味・意義は薄い
 - 在学中だけでなく、卒業後も永く使える必要がある
 - 正しく発行されたものであることを「検証」できる必要がある
- 要件に適した「デジタル化」を考える必要がある
 - 単純なデジタル化 = Digitization
 - 紙をスキャンしてPDF化、結局は人が確認する
 - 真のデジタル化 = Digital Transformation（いわゆるDX）
 - 機械可読な形、発行～検証プロセスそのものをデジタル化・自動化

*1 長期署名的な意味合いではなく、エコシステムとして長期検証可能性を担保できる、といった意味合い

デジタル資格証明の目指す姿

- ・ 利用者自身が証明書を持ち運び選択して提示
- ・ 受け取る側は発行元に問い合わせせずに真正性を検証



では、デジタル化（DX）するには？

・要件は様々

レイヤ	対象	広く使えること	永く使えること	検証できること
データ	対象となる資格	グローバルで合意できていること（学生証、学習歴、などなど）		発行事実、有効性、属性値の検証ができること
	資格情報に含める属性			
	データフォーマット	グローバルで合意できており、業界を超えて利用できること	ある程度長期保存できること、発行者がいなくなっても検証できること	デジタル署名等により真正性の担保ができること
トランスポート	資格証明の発行		グローバルで合意できており、業界を超えて利用できること	セッション乗っ取りなどに対して安全なプロトコルであること
	資格証明の提示			
アイデンティティ	発行者（大学等）	グローバルで一意に識別できること	識別子の払い出しを行うシステム（および事業者）の継続性に信頼がおけること	発行組織と識別子の紐付けができること
	保有者（学生等）			保有者と識別子の紐付けができること
	検証者（他大学、サービス提供者等）			検証組織と識別子の紐付けができること

では、デジタル化（DX）するには？

- ・特に広く、永く使うことを考えると標準化が必須

レイヤ	対象	広く使えること	永く使えること	検証できること	
データ	対象となる資格	教育機関としての標準スキーマ (属性セット)		業界としての検証機能	
	資格情報に含める属性				
	データフォーマット	業界を超えて検証可能な標準データモデル (機械可読なデータ形式)			
トランスポート	資格証明の発行	業界を超えたデータ受け渡しのためのプロトコル			
	資格証明の提示				
アイデンティティ	発行者 (大学等)	業界を超えて一意に識別できる標準的な識別子形式	一部の機関や組織に依存しない識別子の管理システム	既存ガバナンスモデルと連携した検証システム	
	保有者 (学生等)				
	検証者 (他大学、サービス提供者等)				

では、デジタル化（DX）するには？

- 標準化の状況。足回りは固まりつつある。

レイヤ	対象	広く使えること	永く使えること	検証できること
データ	対象となる資格	業界により様々（教育機関ならOpenBadge？）		
	資格情報に含める属性			
	データフォーマット	W3C Verifiable Credentials		
トランスポート	資格証明の発行	OpenID for Verifiable Credentials		
	資格証明の提示			
アイデンティティ	発行者（大学等）	W3C Decentralized Identifiers	W3C Decentralized Identifiers on DLT	DIF Well-known DID Configuration
	保有者（学生等）			
	検証者（他大学、サービス提供者等）			

現状を見据えると今やるべきことは何か？

- 個別に実装方式を考えるフェーズは終わっている
 - にもかかわらず独自実装が次々と出てくるのは大きな問題
- ドメインに特化した部分の標準化が急務

レイヤ	対象	広く使えること	永く使えること	検証できること
データ	対象となる資格	業界により様々（教育機関ならOpenBadge？）		
	資格情報に含める属性			
	データフォーマット	W3C Verifiable Credentials		
トランスポート	資格証明の発行	OpenID for Verifiable Credentials		
	資格証明の提示			
アイデンティティ	発行者（大学等）	W3C Decentralized Identifiers	W3C Decentralized Identifiers on DLT	DIF Well-known DID Configuration
	保有者（学生等）			
	検証者（他大学、サービス提供者等）			

ドメインに特化した部分の標準化の加速が急務

ドメイン特化部分の標準化状況をインプットとして技術レイヤのブラッシュアップするサイクルを回す

技術面での標準はほぼコンセンサスが取れた状態

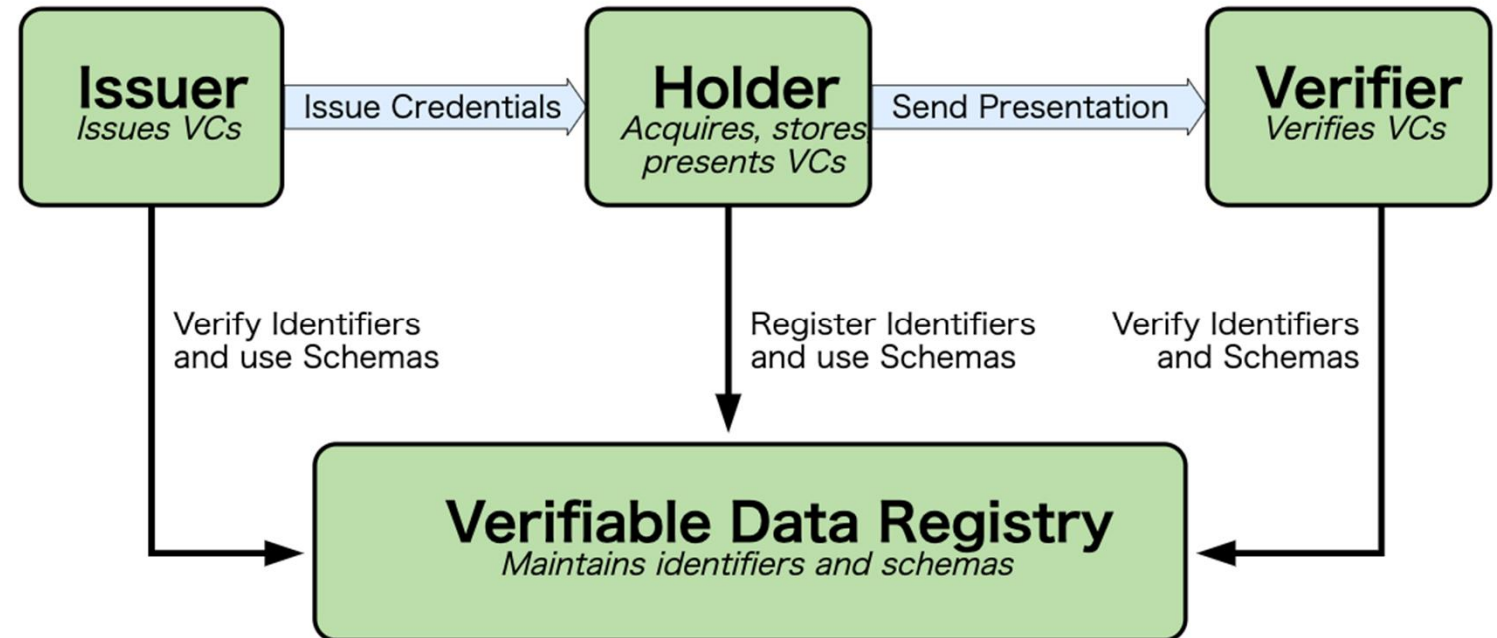
関連する標準技術群

- ・ 特に下支えする領域の技術は固まってきている

カテゴリ	仕様	関連団体	ステータス	概要
識別子	Decentralized Identifiers v1.0	W3C	勧告	識別子とメタ情報（DID Document）のデータモデルとロケータに関する仕様
資格情報	Verifiable Credentials Data Model v1.1	W3C	勧告	検証可能な資格情報のデータモデルに関する仕様
DNSドメインとのDIDの紐付け	Well Known DID Configuration	DIF	Working Group Approved Draft	DIDとDNSドメインを紐付け、識別子が指す主体の検証により信頼性を向上するための仕様
資格情報の状態管理	Status List 2021	W3C	Community Group Draft Report	発行済みのVCの状態（取り消し状態）の管理を行うための仕様
資格情報の送受信	OpenID for Verifiable Credentials •OpenID for Verifiable Credential Issuance •OpenID for Verifiable Presentation •Self-Issued OpenID Provider v2	OpenID Foundation	OID4VCI (Working group draft) OID4VP (Implementer's draft 1) SIOPv2 (Implementer's draft 1)	VCおよびVP (Verifiable Presentation) を発行者、利用者、検証者の間でやりとりするための仕様 利用者が自身の管理するOpenIDプロバイダから属性を発行するための仕様
	DIDComm Messaging v2.0	DIF	DIF-Ratified	DIDを持つ主体の間でのメッセージ送受信を行うための仕様
データストレージとメッセージリレー	Decentralized Web Node	DIF	Draft	DIDを持つ主体の間でメッセージの送受信を行う際のトランザクション管理やデータ保管、メッセージリレーを行うための仕様

Verifiable Credentials Data Model v1.1

- 検証可能なデジタル証明書のデータモデル標準
- さまざまな「証明書」のデジタル化手段
- デジタル署名技術を用いた【発行者】(Issuer)により【対象者】(Subject)が特定の条件を満たしている事を【保持者】(Holder) が示すことができる
- 多言語化を含めVC2.0に向けた検討



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（Wikipedia¹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 Consortium²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³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

1. <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>

2. <http://www.imsglobal.org/>

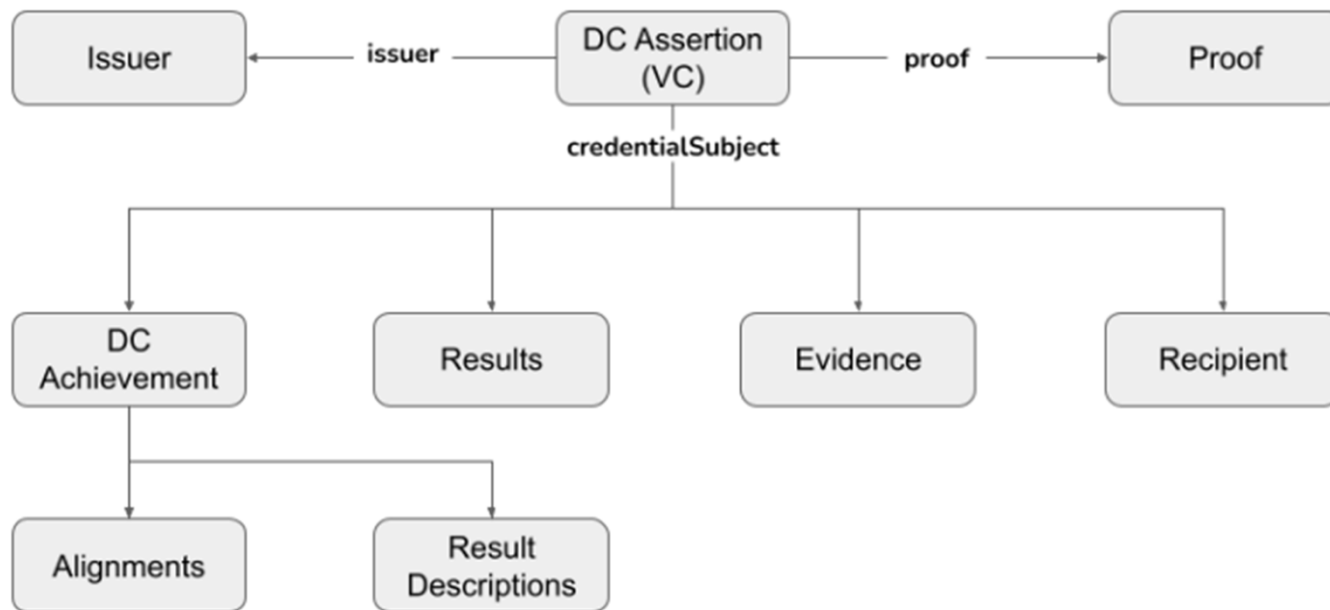
3. <https://www.openbadge.or.jp/>

4. <https://info.credly.com/>

OpenBadge v3とVerifiable Credentials

- OpenBadge v3はVerifiable Credentials (VC) ベース

Digital Credential Assertion (VC)



利点

- 既存のVCエコシステムとの互換性
 - Wallet、他のVCと併せた利用
- 学習者のプライバシーと信頼性
 - OB2は発行者がデータを保持
- 分散型、自己主権型
 - 識別子に柔軟性を持たせる
- CLRとの共通化
 - VCを使うことでOBをCLRへ束ねることができる

参考)

<https://www.imsglobal.org/spec/ob/v3p0/>

<https://www.imsglobal.org/spec/clr/v2p0/>

互換性検証の取り組み（W3C VC-Edu/JFF）

- 2022年11月に2回目のPlugfestを開催
 - <https://w3c-ccg.github.io/vc-ed/plugfest-2-2022/>
- WalletとIssuerに要件を定め互換性を検証
 - Wallet
 - 少なくとも2つの異なるIssuerからVC/OBv3を受け入れる
 - バッジのイメージ、Issuer名、Achievement名、Achievementの説明、Criteriaの表示
 - Issuer
 - 少なくとも2つの異なるWalletへのVC/OBv3の発行
 - 対応プロトコルはCHAPI、VC-API、OpenID for Verifiable Credential Issuance
- 3回目も？

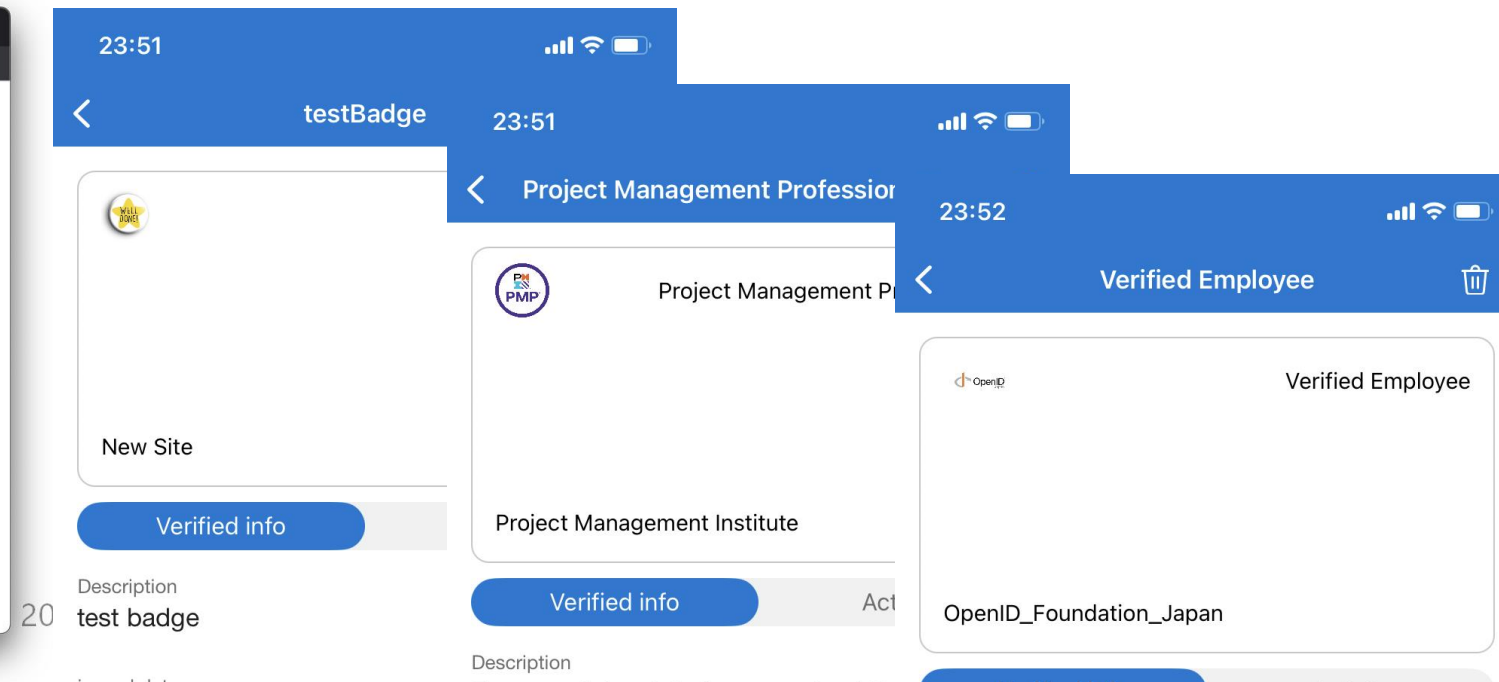
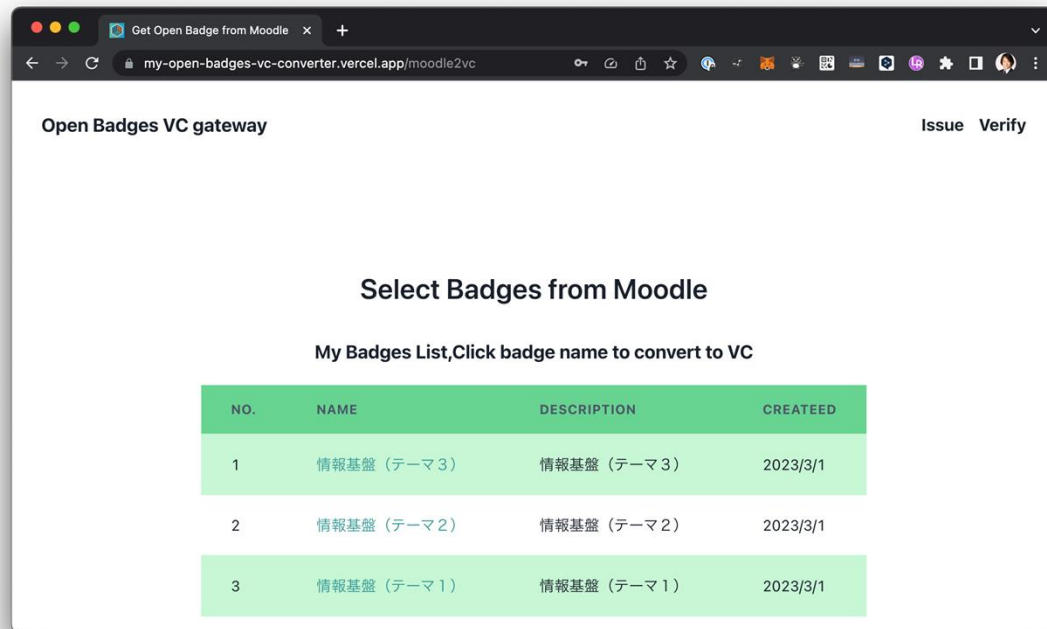
内閣官房/Trusted Web推進協議会

- ・ 検証可能な領域の拡大により「信頼できるインターネット」を実現
- ・ 令和4年度は13事業者の公募によりユースケースの実証（学習歴も）

No.	事業者名・コンソーシアム名	代表団体名 (コンソーシアムの場合)	ユースケース概要
01	Trusted Workplace Solution by TTEC and CG	東芝テック株式会社	ワークプレイスの信頼できる電子化文書の流通システム
02	株式会社ORPHE	—	下肢運動器疾患患者と医師、研究者間の信用できる歩行データ流通システム
03	人材育成のためのTrustedな学修情報流通システム開発コンソーシアム	富士通Japan株式会社	人材育成のためのTrustedな学修情報流通システム
04	DataGateway PTE LTD	—	分散型IDを活用した炭素排出量トレースシステム
05	SSI/FIDOコンソーシアム	国立大学法人 東京大学	学修歴等の本人管理による人材流動の促進
06	ヤンマーホールディングス株式会社	—	機械製品サプライチェーンにおけるトレーサビリティ管理
07	株式会社DataSign	—	オンラインマーケティングにおけるパーソナルデータの流通
08	電通・ISID パブリックDXコンソーシアム	株式会社 電通	中小法人・個人事業者を対象とする補助金・給付金の電子申請における「本人確認・実在証明」の新しい仕組み
09	工業会証明書デジタル化コンソーシアム	一般社団法人情報サービス産業協会	法人税制と工業会証明書
10	ヘルスケア情報流通システム開発コンソーシアム	シミック株式会社	臨床試験及び医療現場における信頼性及び応用可能性の高い情報流通システム
11	アラクサラネットワークス株式会社	—	Trusted Networkによる社会ITインフラの信頼性・強靱性向上の実現
12	大日本印刷株式会社	—	共助アプリにおけるプラットフォームを超えたユーザートラストの共有
13	メタバース×自己主権型IDコンソーシアム	NRIデジタル株式会社	仮想現実空間におけるサービス利用資格と提供データのTrust検証

NIIでの実証実験

- Moodleで発行するOpenBadge v2をVerifiable Credentialsへ変換するゲートウェイの構築中
 - WalletにMoodleでの学習歴証明を入れて持ち運ぶ
 - 学習歴証明を提示することで追加権限を付与（異なるVCと併せて提示可）



まとめ～今、取り組むべきこと

- 学修歴を含むデジタル資格証明の標準化・相互運用の取り組みがグローバルで進行
 - 2023年4月・11月にもInternet Identity Workshop@サンフランシスコが開催、Plugfestの続きの議論あり、日本からも数名参加見込み
 - 留学を含む教育の国際化の推進においてはガラパゴス化は禁物、デジタル学修歴の相互運用に向けた議論・実装が進んでいる
- 目先のソリューションではなく、先を見据えた標準対応へ
 - 今なら日本の事情をグローバル標準へ入れていくことが可能
 - 仲間作りから始めているのでご興味のある方はぜひご連絡を！