VCを用いたgaia-xにおける Self-Sovereign Identity

NII学術情報基盤オープンフォーラム2023
認証・RCOS合同トラック

国立情報学研究所 特任技術専門員
相沢　啓文

タイトルを分解

VCを用いたgaia-xにおけるSelf-Sovereign Identity

＝技術の名前　　＝プロジェクトの名前　　＝概念（世界観・思想）の名前

“gaia-xというプロジェクトで、VCを活用して
Self-Sovereign Identity（自己主権型アイデンティティ）
に基づくデータ流通の世界を実現しようとしている”という意味。

目次

- Self-Sovereign Identityとは
- Verifiable Credentialとは
- gaia-xとは
- 国内外のVC応用事例

Self-Sovereign Identityとは

本日のキーワード

ソブリニティ
Sovereignty ＝「主権」

- 元々は「至上、最高」を表す政治学用語。一般には国家主権を指す（ex. 国民主権＝Popular sovereignty）。
- 基本的な意義は以下の3点。
  1. 国家の統治権
  2. 他国の支配に服さない独立性（対外主権）
  3. 国家の政治のあり方を最終的に決める権利のこと

Self-Sovereign Identity（自己主権型アイデンティティ）

Self ＝ 「自分自身が」
Sovereign ＝ 「主権者の」
Identity ＝ 「アイデンティティ」

ユーザが自らを表す属性情報等を、
ユーザ自身で管理するという概念。

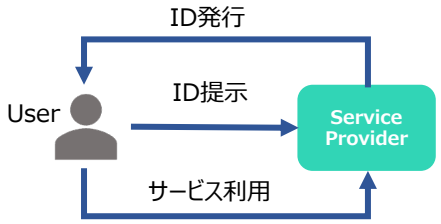
Self-sovereign Identity is an approach to digital identity that gives individuals control over the information they use to prove who they are to websites, services and applications across the web. (Wikipedia)

自己主権型アイデンティティとは、web上のwebサイト、サービス、アプリケーションに対して、自分が誰であるかを証明するために使用する情報を個人がコントロールできるようにするデジタルアイデンティティのアプローチである。

自分のアイデンティティを自分でコントロールできない？？

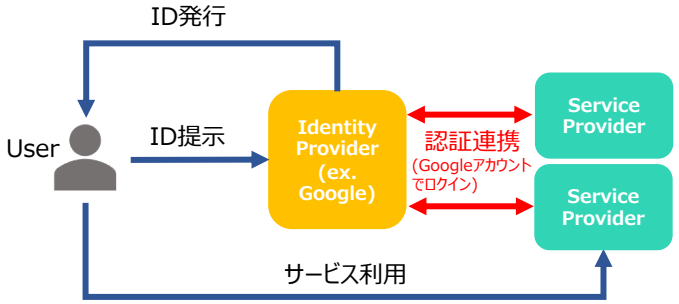
デジタルアイデンティティの３類型

モデル1
中央集権型（Centralized）



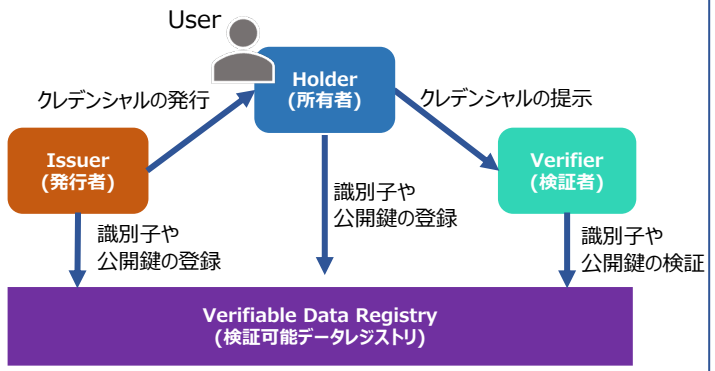
- サービス事業者、ドメインレジストラ、個々のサイト等によってIdentityが集中的にコントロールされる形態。
- インターネットが広がるに従ってIdentityのコントローラは増殖し、1人のユーザのアイデンティティがサイト毎に分散。

モデル2
連合型（Federation）



- 異なるID基盤を相互連携させる形態で、Identityの分散の問題を解決し、１つのIDを複数のサービスで使用できるようにすることを目的とする。
- ただし、依然としてそれぞれのIDはそれぞれの基盤で管理される。

モデル3
自己主権型（Self-Sovereign）

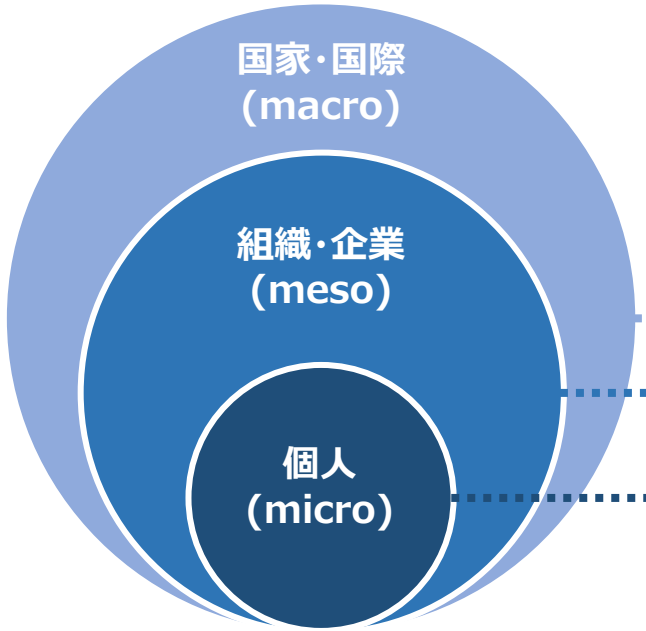


- ユーザ自身が完全にIdentityの管理（コントロール）を行う。ユーザが自身のIdentityの「支配者」になる。

現在の主流はモデル2
→ユーザではなく、SPまたはIdPがユーザのIdentityを管理（ユーザに“主権”がない状態）

枠内の文章はOne Tech Blog「Self Sovereign Identity (SSI)の現在地」(https://tech.gmogshd.com/self-sovereign-identity-ssi/)より引用

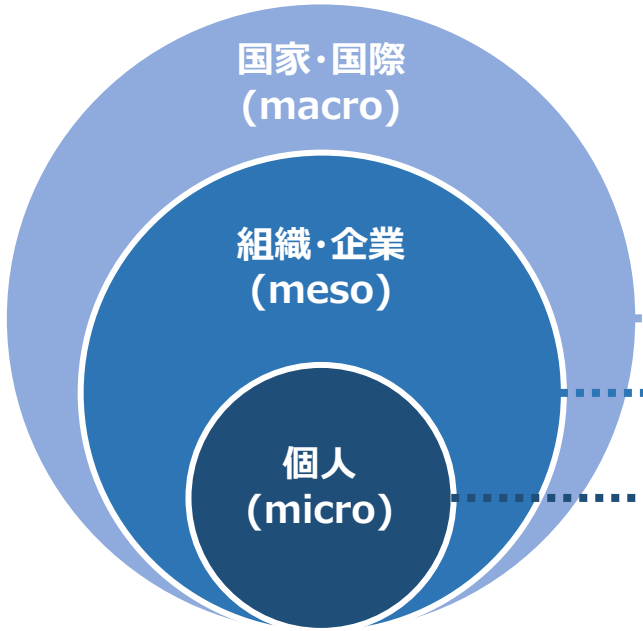
従来型のデジタルアイデンティティをめぐる課題



	個人データの流出・悪用 プライバシー侵害	発行元による否認・改竄 発行元の消滅	ルールの複雑化 管理コスト増
国家・国際 (macro)	✓ 海外巨大プラットフォーム企業による個人データ・行動履歴データ等の囲い込みリスク。 ✓ 政府機関等による民間部門が保有する情報への強制力を持ったアクセス（ガバメントアクセス）。	✓ 難民・移民を含め、世界で11億人以上の人々が公的なIDを持たない（→国連、ID2020の取り組み）。	✓ 国境を越えた人やデータの移動に対し、国家・地域間で異なるルールが障壁に（GDPRなど）。
組織・企業 (meso)	✓ 個人識別データの意図しない誤用に伴う、法令違反のリスク。	✓ 所属組織の消滅や否認により身元確認できない人への採用やサービス提供は一律排除？	✓ 認証連携の多様化（連携先の増加、条件の複雑化、保証レベルの違いなど）により、スケーラビリティが問題になる。 ✓ 滅多に使わない人のユーザIDも継続的な維持管理が必要（ライセンスコスト増）。
個人 (micro)	✓ 個人の行動把握、行動介入の危険性（ケンブリッジ・アナリティカ事件）。	✓ IdPにアカウントを停止されるリスク（いわゆる垢バン）。 ✓ 悪意あるIdPにアイデンティティを改竄されるリスク。 ✓ （現在・過去の）所属組織が閉学・倒産した場合の所属証明は？	✓ 個人で持つアカウント数が増加し、使い回しなどによる漏洩リスク増。 ✓ そもそも電子化されていない所属証明（卒業証明をもらいに大学訪問・郵送取り寄せ）

将来的なデータ量の増加や
技術革新、データ流通の促進により、
これらの課題は一層深刻化。

従来型のデジタルアイデンティティをめぐる課題

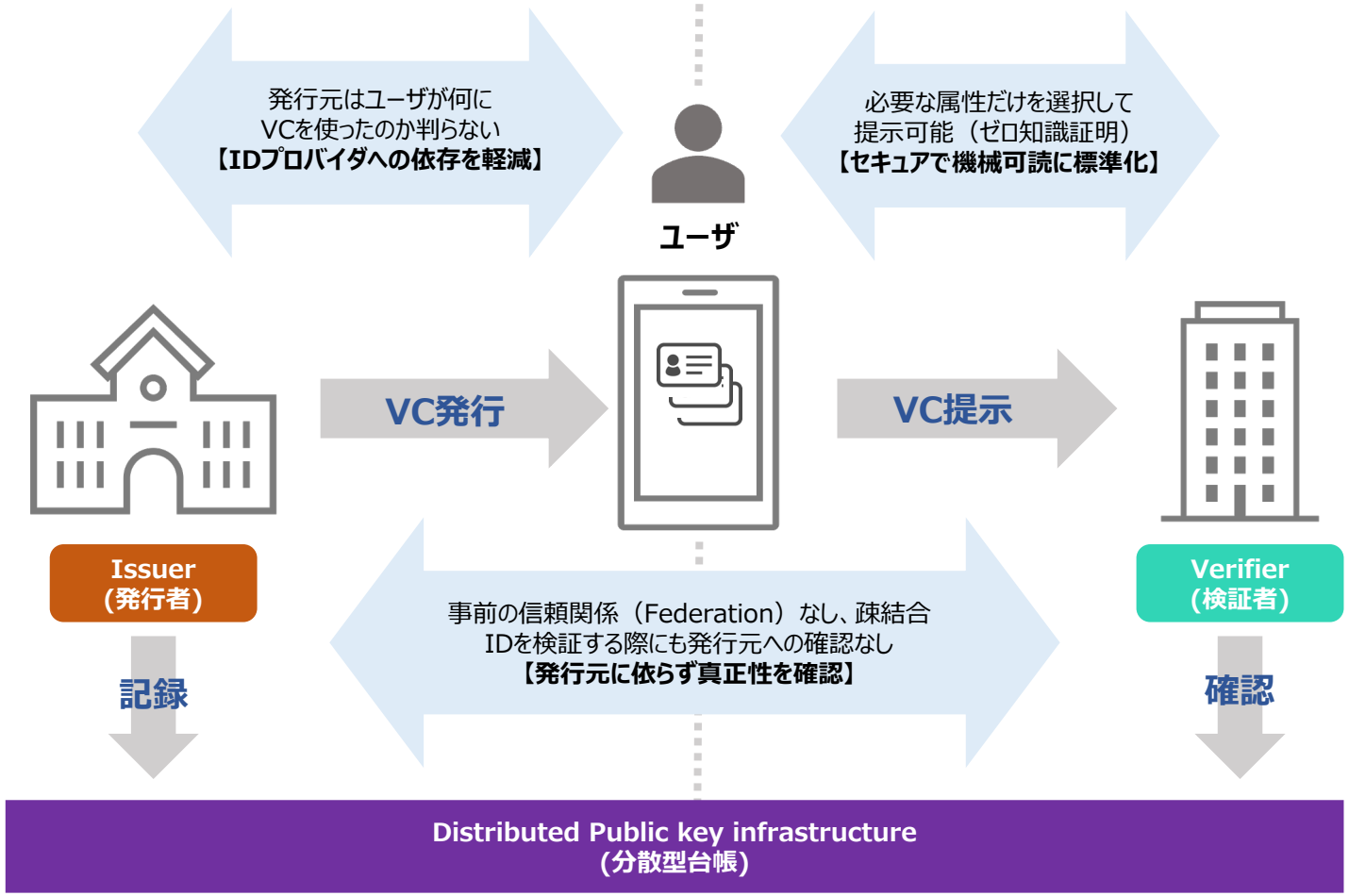


個人データの流出・悪用 プライバシー侵害	発行元による否認・改竄 発行元の消滅	ルールの複雑化 管理コスト増
IDプロバイダへの 依存を軽減する方法	属性発行元が 無くても真正性 を証明できる方法	セキュアで機械可読な 形式で標準化された 方法

富士尚寛「組織におけるアイデンティティ管理に関する基本的な考え方」（2019/02/09）より一部引用

SSIによる課題解決

発行プロセスと提示プロセスを分離



兒玉雄介「S13 レガシー ID 管理者でも分かる Verifiable Credentials のセッション | 日本マイクロソフト」（YouTube）をもとに作成

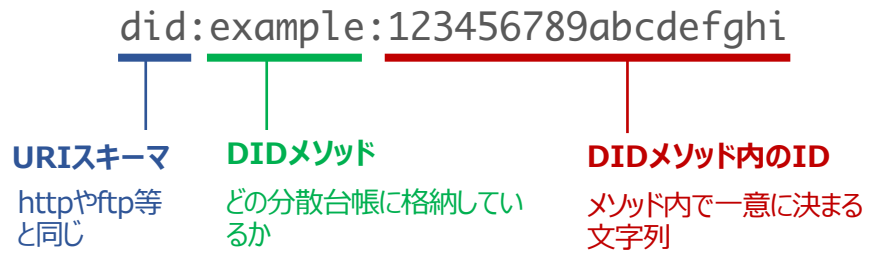
Verifiable Credentialとは

SSIを実現する手段：DID/VC

DID … Decentralized Identifier（分散型ID）

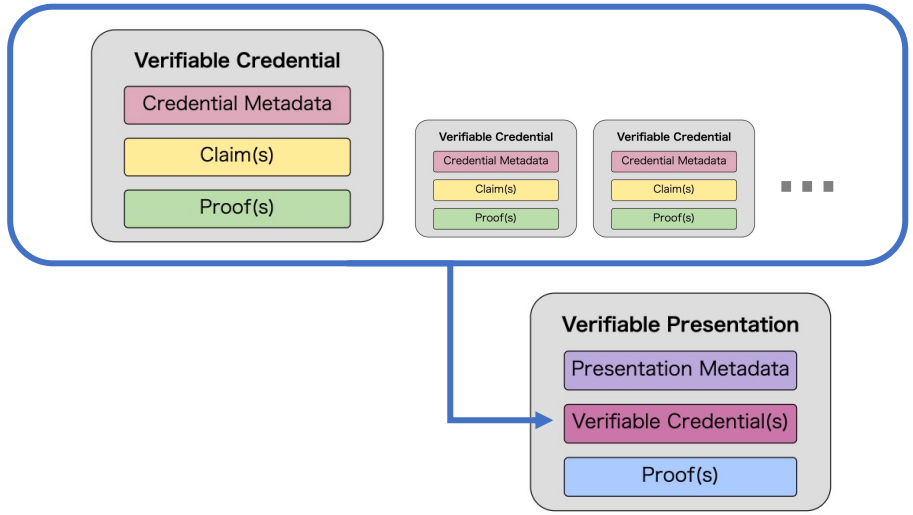
- 特定の事業者に依存しない識別子（Identifier）
  ※Identity（属性の集合）ではない
- 識別子に紐づくメタデータ（DID Document）が分散台帳などで公開される

  → DIDに紐づく秘密鍵で署名したデータを、DID Document上の公開鍵で検証することで、DIDの「持ち主」が発行したデータであることを検証可能になる。
  (VCはこの仕組みを利用)



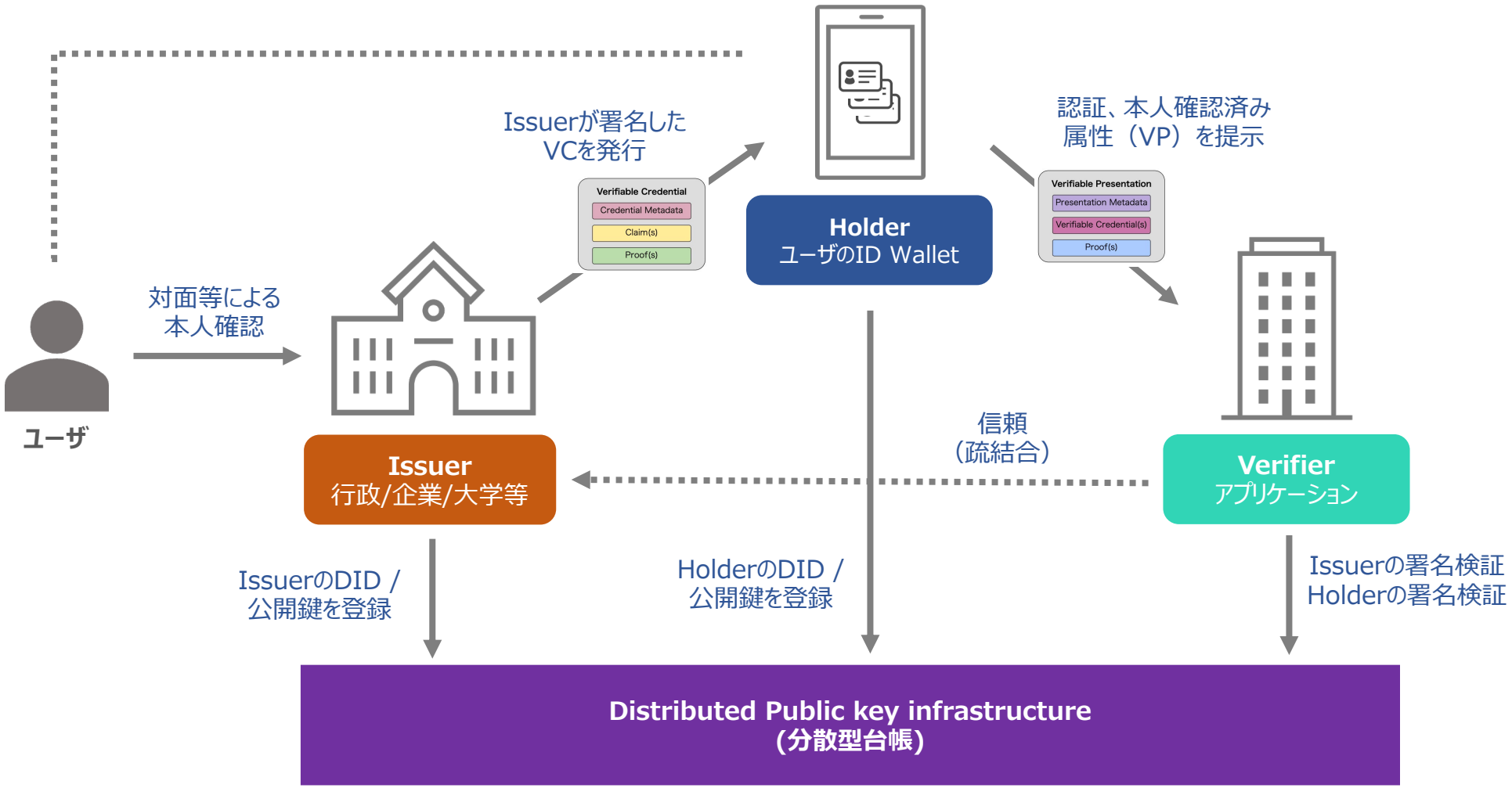
VC … Verifiable Credential（検証可能な資格情報）

- 認証に必要な属性情報をデジタル署名を使って機械的に検証するためのデータモデル（＝セキュアかつ機械可読な形で属性情報を共有）
- 中身はJWTやJSON-LD
- いくつかのVCを束ねて新しいJWTを作ることができる（Verifiable Presentation）



富士榮尚寛「分散型IDと検証可能なアイデンティティ技術概要」（2022/07/29）より一部引用

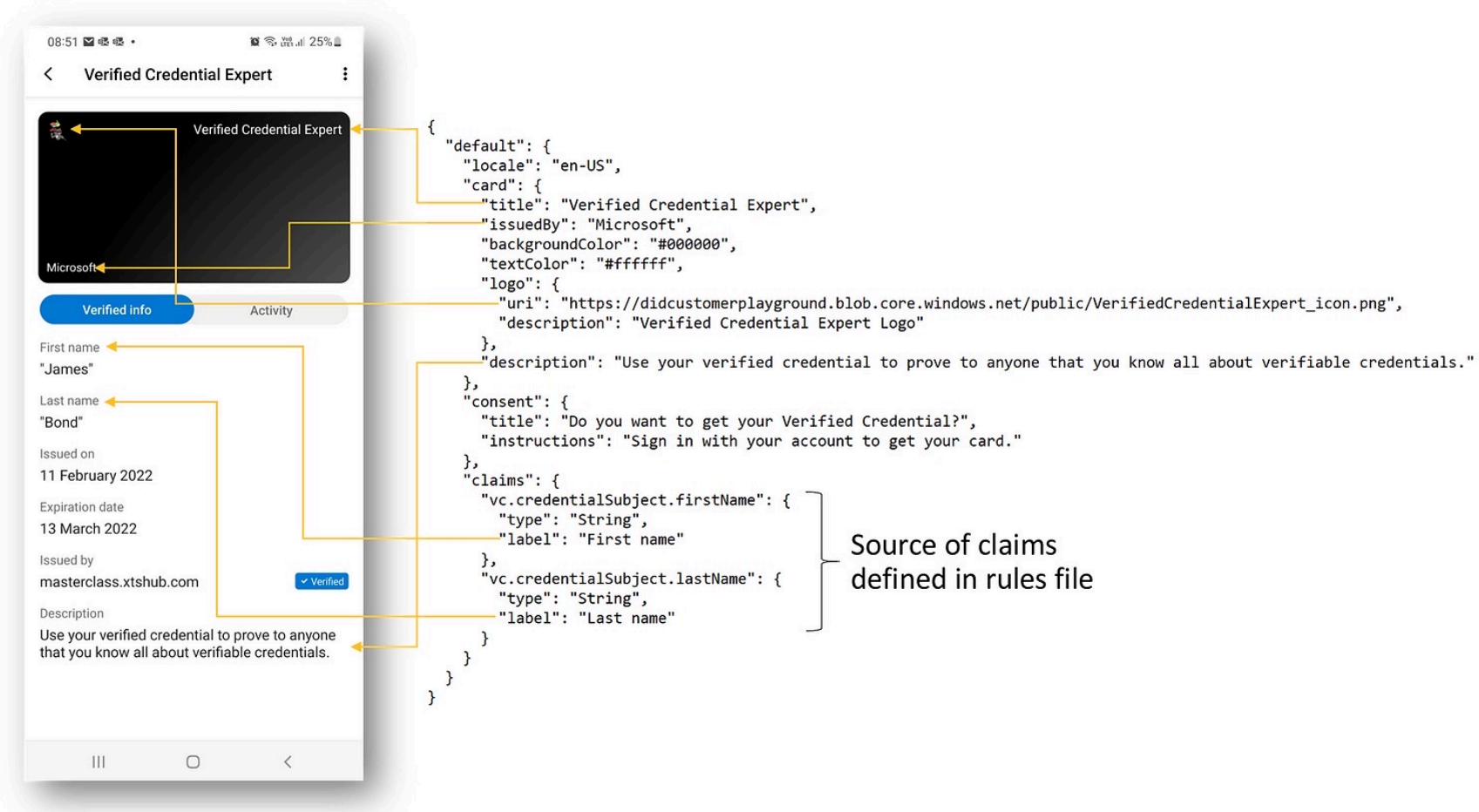
VCの検証の流れ



富士榮尚寛「分散型IDと検証可能なアイデンティティ技術概要」（2022/07/29）より一部引用

VCの実装イメージ

例）Microsoft Entra Verified ID（旧 Azure AD Verifiable Credential ）



Craddock, J(2022). “Creating your own Azure AD Verifiable Credentials”
https://www.xtseminars.co.uk/post/creating-your-own-azure-ad-verifiable-credentials-with-the-microsoft-sample-app

gaia-xとは

gaia-xの概要

経緯

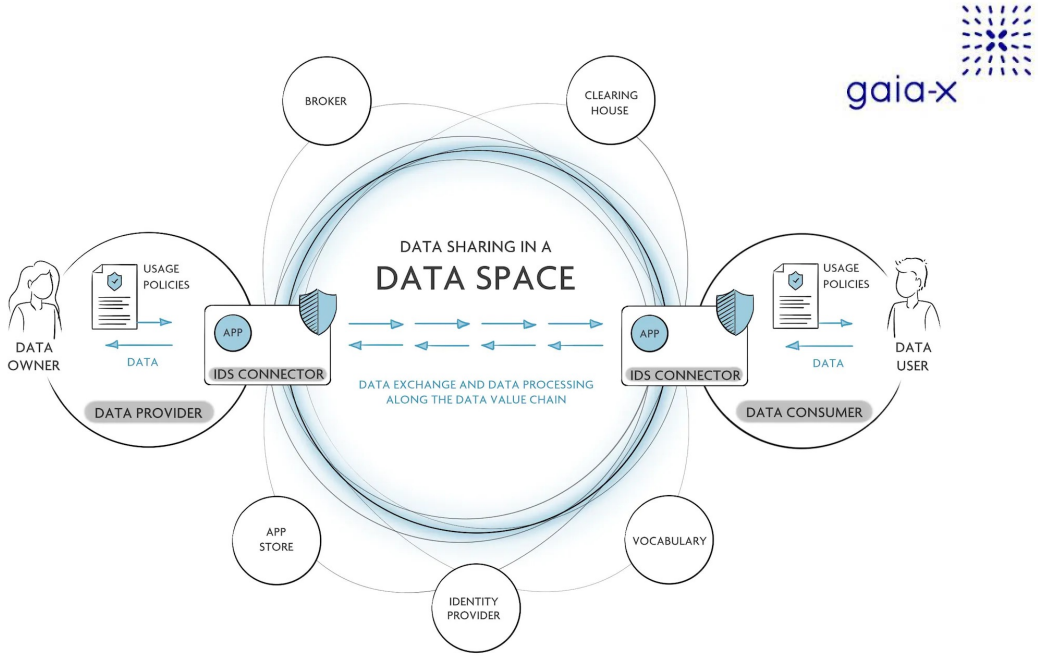
米中のメガプラットフォーム企業の台頭や米国CLOUD法などに対する危機感を背景に、2019年アルトマイヤー独経済・エネルギー相が欧州のための信頼できるデータ流通基盤の構築を提唱。

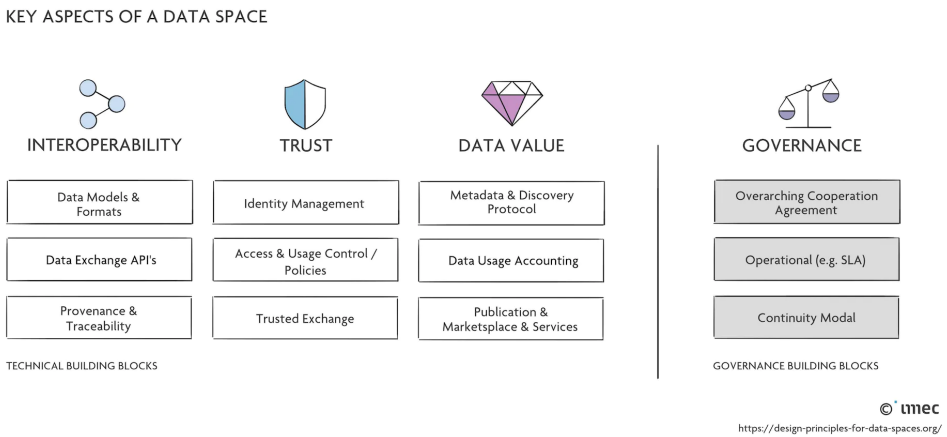
目的

欧州を中心として、様々な国家・企業・人がデータを交換・利用するためのデジタル経済圏を作ること。

目標

データの所有者が、データに対する完全な主権（データ主権）を保持したまま、信頼できる環境でデータを交換し相互利用できるエコシステムを確立する。





【参考】gaia-x Federation Services（GXFS）

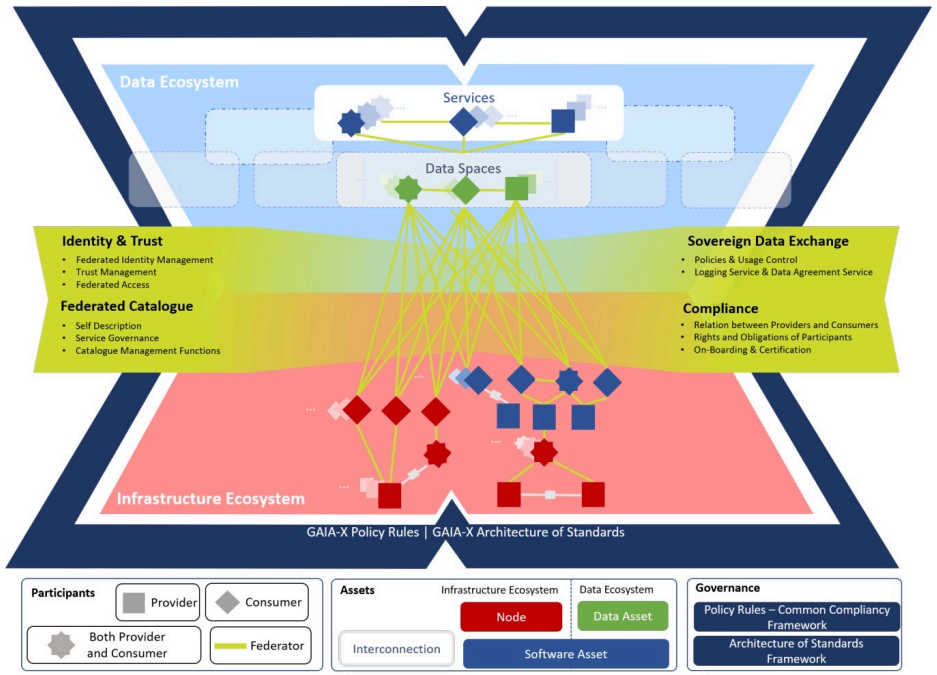
- GXFSとは、Gaia-Xエコシステムを実現するために必要なサービスのこと。
- 「IDとトラスト」「フェデレーションカタログ」「データ主権サービス」「コンプライアンス」の４つから構成される。

IDとトラスト（Identity&Trust）
認証・認可、DID/VC管理およびVCの検証を行う。

フェデレーションカタログ（Federated Catalogue）
自己記述（Self-Description）のスキーマおよびインデックス付きストレージを提供し、プロバイダによって登録されたサービスの検索と取得を可能にする。

データ主権サービス（Sovereign Data Exchange）
ユーセージコントロールを実現するデータコントラクトサービスとロギングサービスを提供することにより、参加者のデータ主権を実現する。

コンプライアンス（Compliance）
参加者にサービス提供に関するセキュリティ、プライバシ、透明性、相互運用性等の観点でポリシー・ルールを遵守させるために必要な監視機能等を提供する。



Gaia-X Ecosystem Visualization

Point① データ主権（Data Sovereignty）

「データ主権とは、データの所有者がデータの場所と使用に関する完全な制御とガバナンスを実現すること」

“Data Sovereignty is the execution of full control and governance by a Data Owner over data location and usage.” (gaia-x technical architecture)

Point② Federation

gaia-xの参加者は、自動車業界や保険業界などの単位で組織化されたFederationに属する。

→参加者同士は、gaia-xおよび各Federationのルールに基づき対等な立場で関与。

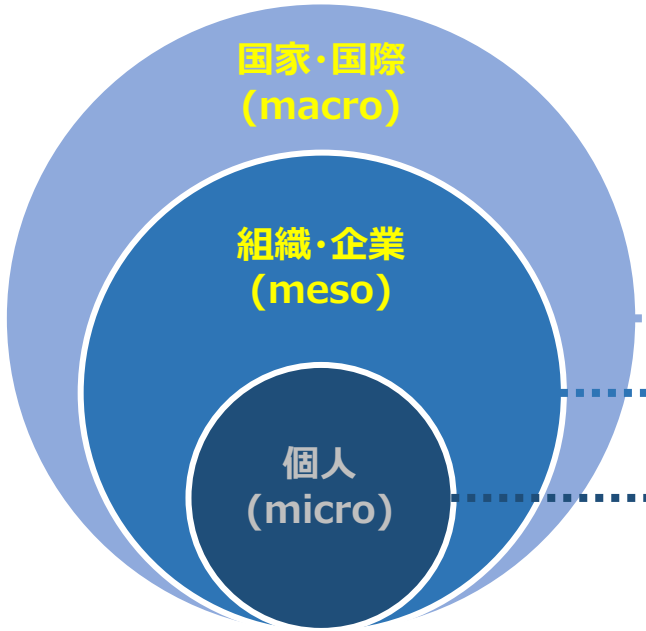
Point③ Federator

各Federationによって異なる特性に応じたサービスを提供するため、Federationごとに任命されたFederatorがサービス（Federation Services）の構築と運用を担う。

アイデンティティ管理モデルのデータ管理への拡張

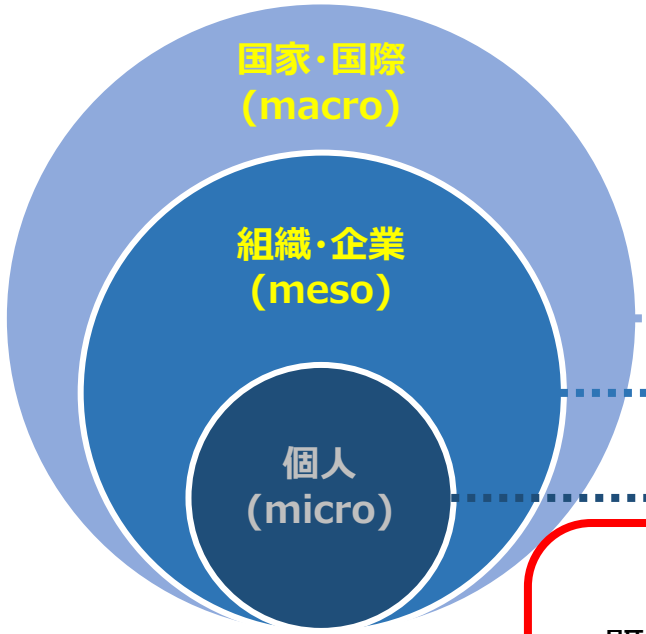
	SSIモデル	拡張SSIモデル（gaia-x）
目的	アイデンティティ情報の コントローラビリティの確保	保有データの コントローラビリティの確保 （データ主権）
主体	個人	企業・法人
対象	個人データ	非個人データ（産業データ） ＋個人データ

gaia-xのスコープ



	個人データの流出・悪用 プライバシー侵害	発行元による否認・改竄 発行元の消滅	ルールの複雑化 管理コスト増
国家・国際 (macro)	✓ 海外巨大プラットフォーム企業による個人データ・行動履歴データ等の囲い込みリスク。 ✓ 政府機関等による民間部門が保有する情報への強制力を持ったアクセス（ガバメントアクセス）。	✓ 難民・移民を含め、世界で11億人以上の人々が公的なIDを持たない（→国連、ID2020の取り組み）。	✓ 国境を越えた人やデータの移動に対し、国家・地域間で異なるルールが障壁に（GDPRなど）。
組織・企業 (meso)	✓ 個人データの意図しない誤用に伴う、法令違反のリスク。	✓ 所属組織の消滅や否認により身元確認できない人への採用やサービス提供は一律排除？	✓ アイデンティティ連携の多様化（連携先の増加、条件の複雑化、保証レベルの違いなど）により、スケーラビリティが問題になる。 ✓ 滅多に使わない人のユーザIDも継続的な維持管理が必要（ライセンスコスト増）。
個人 (micro)	✓ 個人の行動把握、行動介入の危険性（ケンブリッジ・アナリティカ事件）。	✓ IdPにアカウントを停止されるリスク（いわゆる垢バン）。 ✓ 悪意あるIdPにアイデンティティを改竄されるリスク。 ✓ （現在・過去の）所属組織が閉学・倒産した場合の所属証明は？	✓ 個人で持つアカウント数が増加し、使い回しなどによる漏洩リスク増。 ✓ そもそも電子化されていない所属証明（卒業証明をもらいに大学訪問・郵送取り寄せ）

gaia-xのスコープ

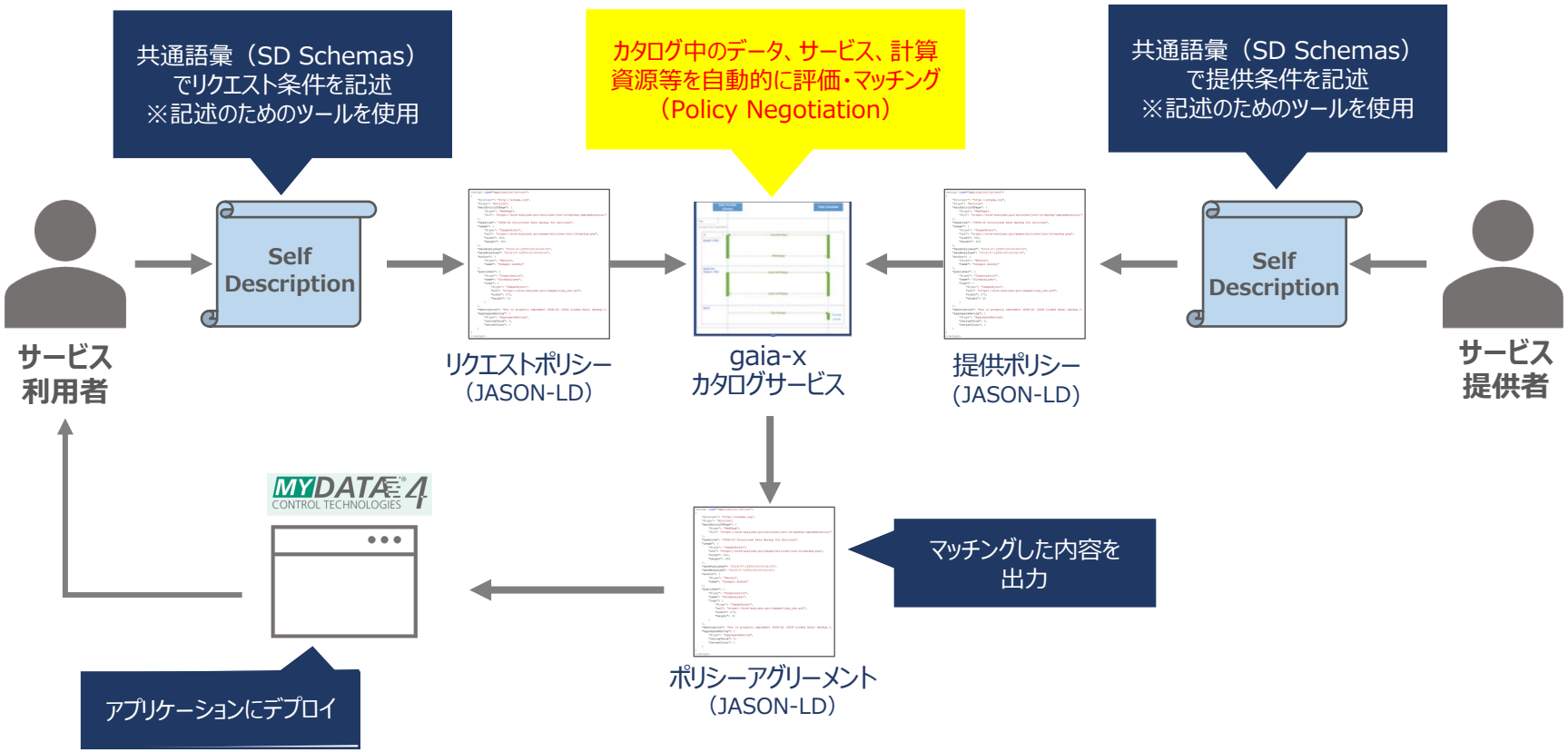


個人データの流出・悪用 プライバシー侵害	発行元による否認・改竄 発行元の消滅	ルールの複雑化 管理コスト増
✓ 海外巨大プラットフォーム企業による個人データ・行動履歴データ等の囲い込みリスク。 ✓ 政府機関等による民間部門が保有する情報への強制力を持ったアクセス（ガバメントアクセス）。	✓ 難民・移民を含め、世界で11億人以上の人々が公的なIDを持たない（→国連、ID2020の取り組み）。	✓ 国境を越えた人やデータの移動に対し、国家・地域間で異なるルールが障壁に（GDPRなど）。
	✓ 所属組織の消滅や否認により身元確 ビス提供	✓ アイデンティティ連携の多様化（連携先の増加、条件の複雑化、保証レベルの違いなど）により、スケーラビリティが問題になる。 ✓ 滅多に使わない人のユーザIDも継続的な維持管理が必要（ライセンスコスト増）。
ク（い 改竄 閉学・		✓ 個人で持つアカウント数が増加し、使い回しなどによる漏洩リスク増。 ✓ そもそも電子化されていない所属証明（卒業証明をもらいに大学訪問・郵送取り寄せ）

既存のアイデンティティ分野での課題解決の仕組み（「IDプロバイダへの依存軽減」「セキュアで機械可読に標準化」）に加えて、

データのコントローラビリティを確保するための
コンテクストベースのルールに対する制御の仕組みが必要

課題解決：機械可読なポリシーによるガバナンスの実現



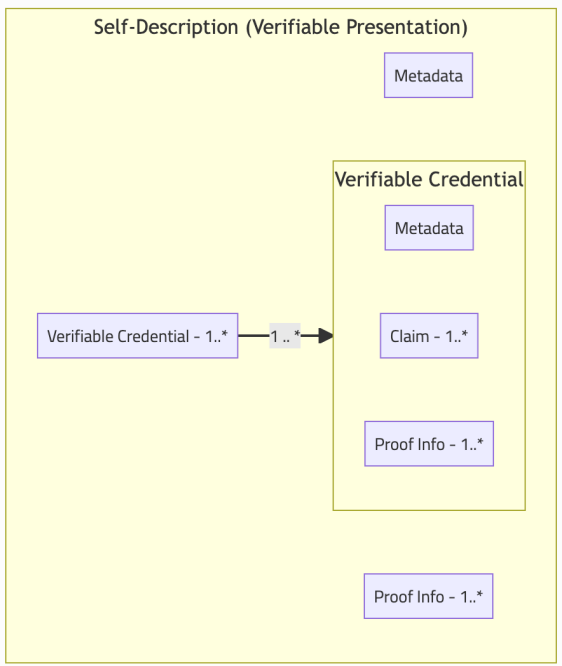
gaia-xでは、「Self-Description」と呼ばれる、参加者自身が記述するメタデータの要件に基づき、カタログ中のデータ、サービス、計算資源等を自動的にマッチング。

→これにより、データ提供の際のコンプライアンスの確保、利用者ー提供者間の条件合意など、複雑な条件の制御を自動的に行うデータ交換を実現する。

課題解決：機械可読なポリシーによるガバナンスの実現

Self-Description（SD：自己記述）

- 対象となるデータに関する情報や、セキュリティ／プライバシー等の要件を機械可読な形式で記述したメタデータ
- gaia-xのプロバイダがリソース（データ、サービス、計算資源等）を提供する際には、SDをgaia-xのツールを利用して記述し、登録しなければならない



Graph: Self-Description assembly model

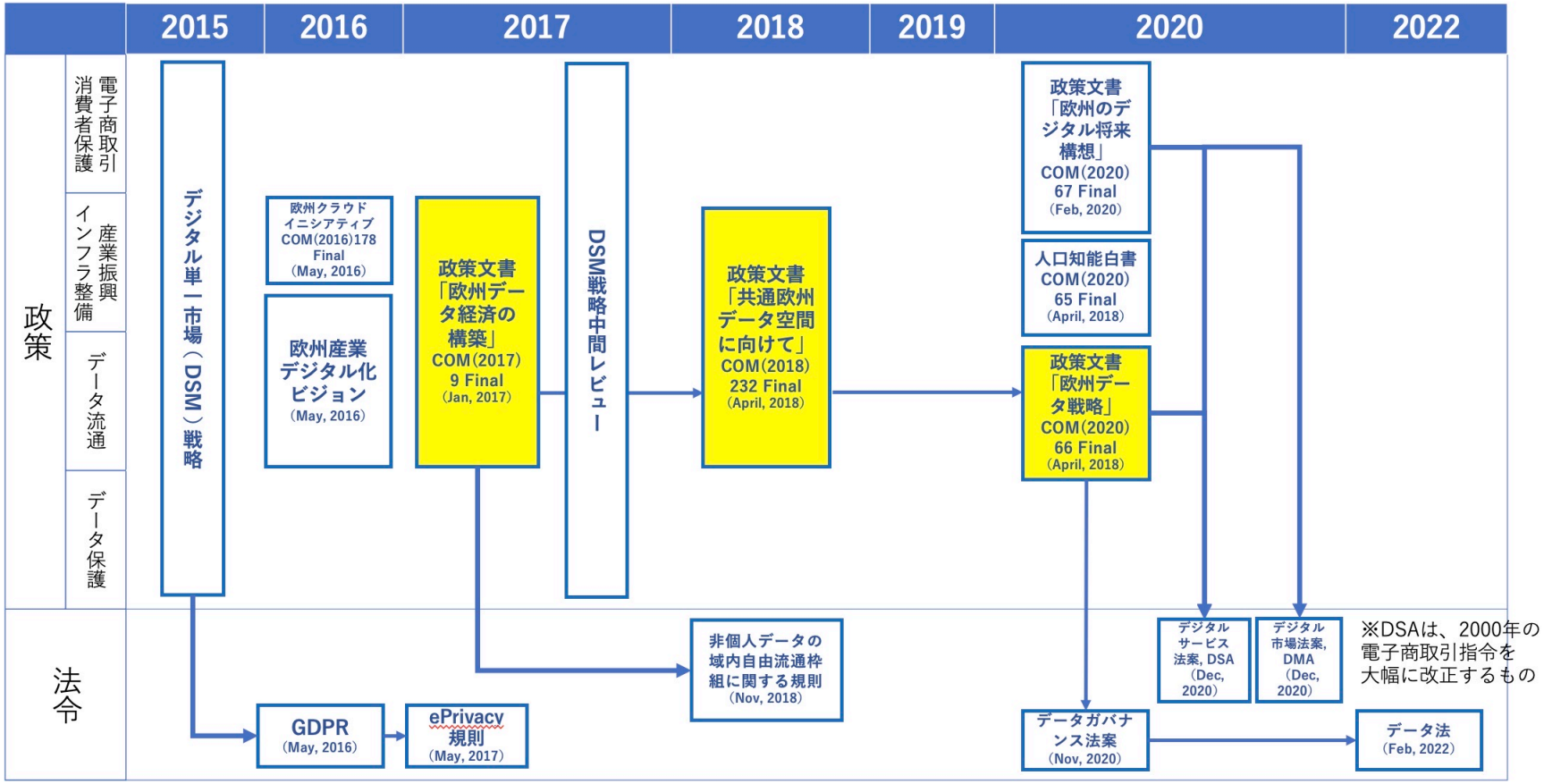
【SDの実装】

- ✓ SDの実装はJASON-LD形式のVerifiable Presentationであり、その仕様はW3C VC Data Modelにしたがっている。
- ✓ SDの記述には拡張可能なSDスキーマ（Self-Description Schemas）が用いられ、統一的な表現を保証。
- ✓ VCのクレームには、主語-述語-目的語トリプル（RDFモデル）に基づく、エンティティの属性（attributes）と他のエンティティとの関係（relations）についての情報が含まれる。

ex. プロバイダ「NodeProvider123」によるサービス「NodeABC」に関するペイロード情報は以下のように表現される。

(NodeABC, isA, Node)
(NodeABC, providedBy, NodeProvider567)
(NodeABC, hasRAMCapacity, 2TB)
(NodeABC, hasCertificate, ISO27001)

【参考】欧州における近年のデジタル政策・法令（データ関連のみ抜粋）

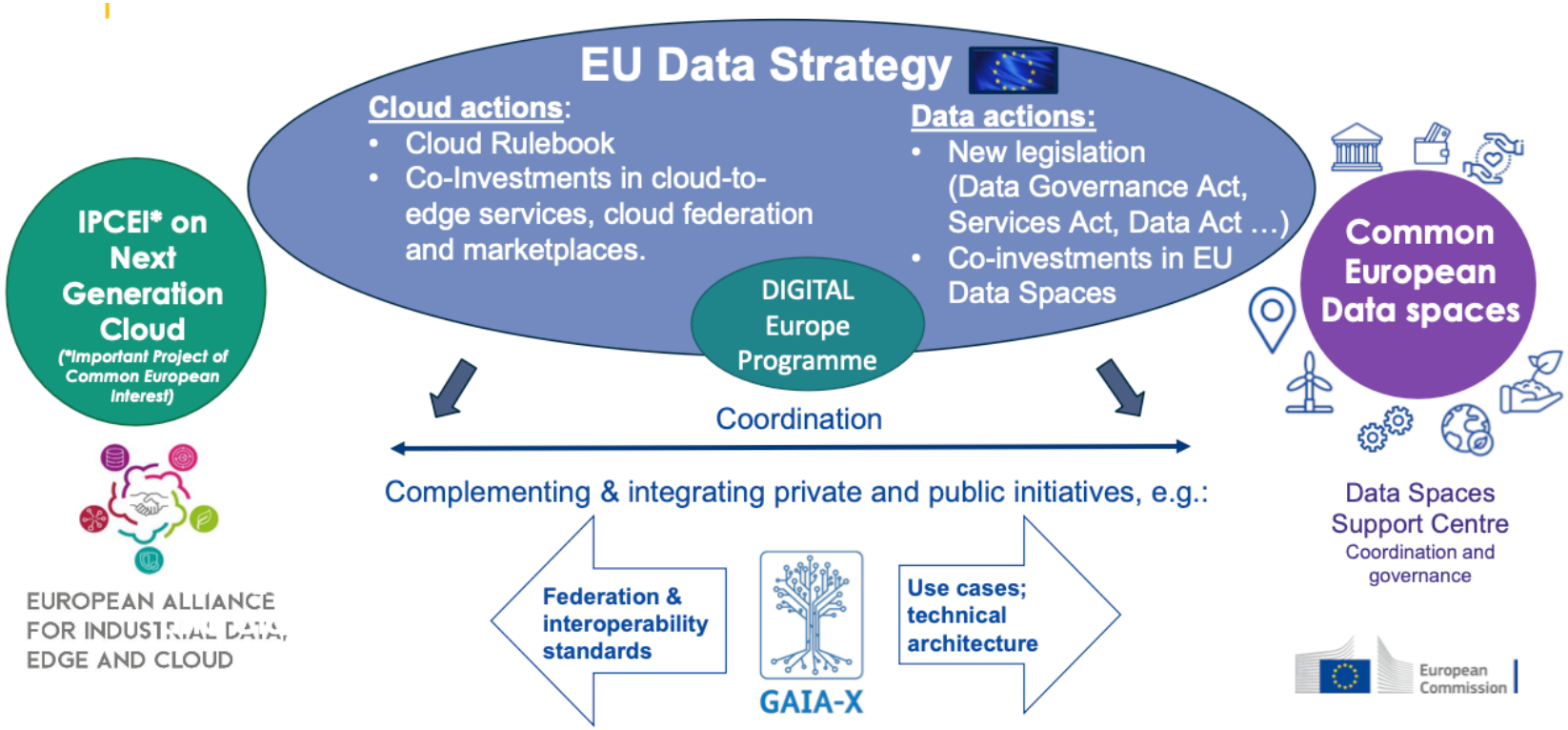


欧州はデータ「保護」から「共有」へと政策を転換。

“EUは、長い間、プライバシー規制の先駆者であった。（中略）しかし、新たな欧州データガバナンス戦略は、これまでとは根本的に異なる態勢をとる。EUは同戦略で、市民の個人データの使用と収益化を促進する積極的な立役者となるつもりだ。この新戦略は、EUの重点が、個人のプライバシーを保護することから、データ共有を市民の義務として促進することに一大転換したことを示している。」

Anna Artyushina（2020）, “The EU is launching a market for personal data. Here’s what that means for privacy.”, MIT Technology Review

【参考】欧州データ戦略とgaia-x



- 欧州データ戦略（European Strategy for Data）は、欧州の世界での競争力とデータ主権を確保するため、データの単一市場である「欧州データ空間」の創出を目標に掲げている。
- 同戦略において、９分野のデータ空間が例示され、その構築に向けた仕組みづくりが行われている。

【参考】主要9分野の欧州データ空間

分野	支援内容
産業（製造業）	EUの産業競争力向上（製造業における非個人データの潜在的価値は2027年までに1兆5千億ユーロと推定）
グリーンディール	気候変動、循環型経済、ゼロ汚染、生物多様性、森林破壊等の優先行動
モビリティ	コネクテッドカーを含むインテリジェント輸送システムの開発等
健康	病気の予防・発見・治療への進歩、医療システムへのアクセス性・有効性の改善
金融	イノベーション、市場の透明性、持続可能な金融、欧州企業の資金調達へのアクセス等
エネルギー	セクター間のデータ共有の促進による脱炭素化のサポート
農業	農業部門の持続可能性と競争力の強化、農場レベルでの生産アプローチの個別最適化
行政	公的支出の透明性・説明責任の向上等
スキル	教育・訓練システムと労働市場のニーズとの間の技能ミスマッチの減少

※欧州委員会は上記９分野に加え、学術分野におけるEuropean Open Science Cloud(EOSC)を支援

国内外のVC応用事例

教育機関でのデジタル資格証明（AXIESでの富士榮さん資料）

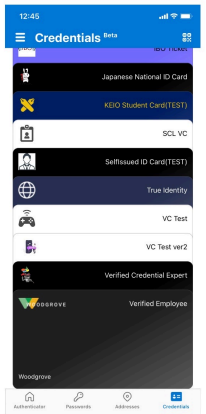
SELMID

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

SELMID



- **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）

2

教育機関における資格証明

SELMID

- 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[1]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**[2]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
- Credly[4]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）

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/

6

DID/VCとオープンバッジ

SELMID

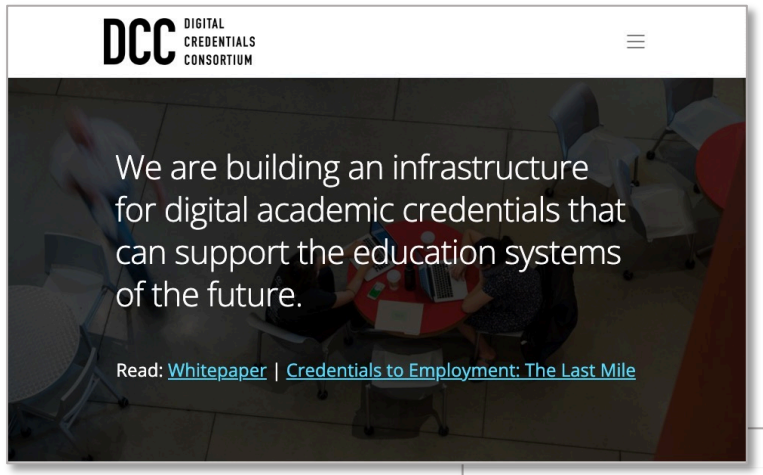
ゴール		DID/VC		オープンバッジ（Hosted型）	
用途		特に限定せず		学習履歴、アチーブメントデータの表現	
ポータビリティ		○	Walletに入れて持ち運ぶ	○	画像に埋め込んで持ち運ぶ
疎結合		○	分散台帳上へのアクセスができれば検証者と発行者の間の直接通信は発生せず →**利用者が発行者に知られず資格情報を検証者へ提示可能**	△	Linked-DataによるGraph構造 →発行者により検証が行われるため、**利用者が資格情報を提示したことを発行者は知ってしまう**
標準化	ベースレイヤ	○	DID、VCの**汎用**データモデルは標準化済み（W3C）	△	**OpenBadge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

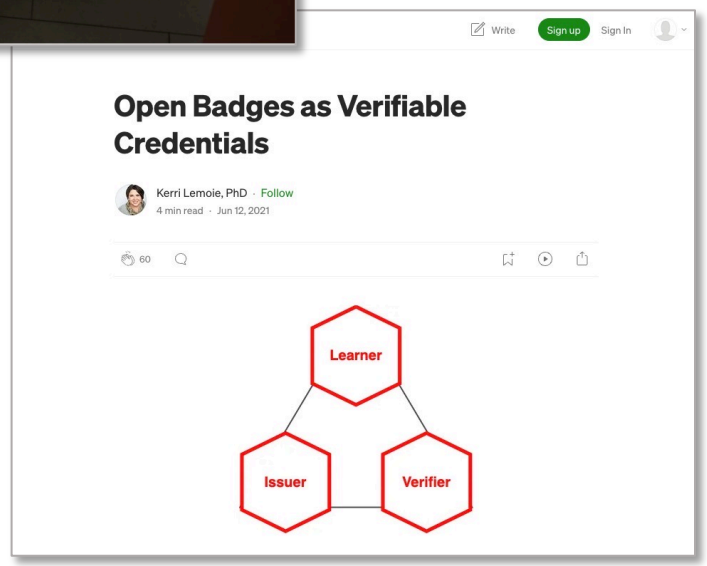
Blockcertsなど分散台帳とオープンバッジを組み合わせた仕組みはあるが、汎用性はない
W3C/**Verifiable Credentials for Education Task Force**（vc-edu）でDID/VCとオープンバッジの組み合わせを検討

11

https://auth.axies.jp/_media/sites/9/2021/12/AXIES2021_fujie.pdf

DID/VCとオープンバッジ：海外での取り組み





Digital Credentials Consortium

12 Founding Members

- Delft University of Technology (Netherland)
- Georgia Institute of Technology (USA)
- Harvard University (USA)
- Hasso Plattner Institute, Potsdam (Germany)
- Massachusetts Institute of Technology (USA)
- McMaster University (Canada)
- Tecnologico De Monterrey (Mexico)
- Technical University of Munch (Germany)
- University of California, Berkeley (USA)
- University of California, Irvine (USA)
- University of Milano-Bicocca (Italy)
- University of Toronto (Canada)

ご清聴ありがとうございました。