

# データスペースにおけるトラスト ～概要と用法、今後の課題～

2026年5月7日（木）

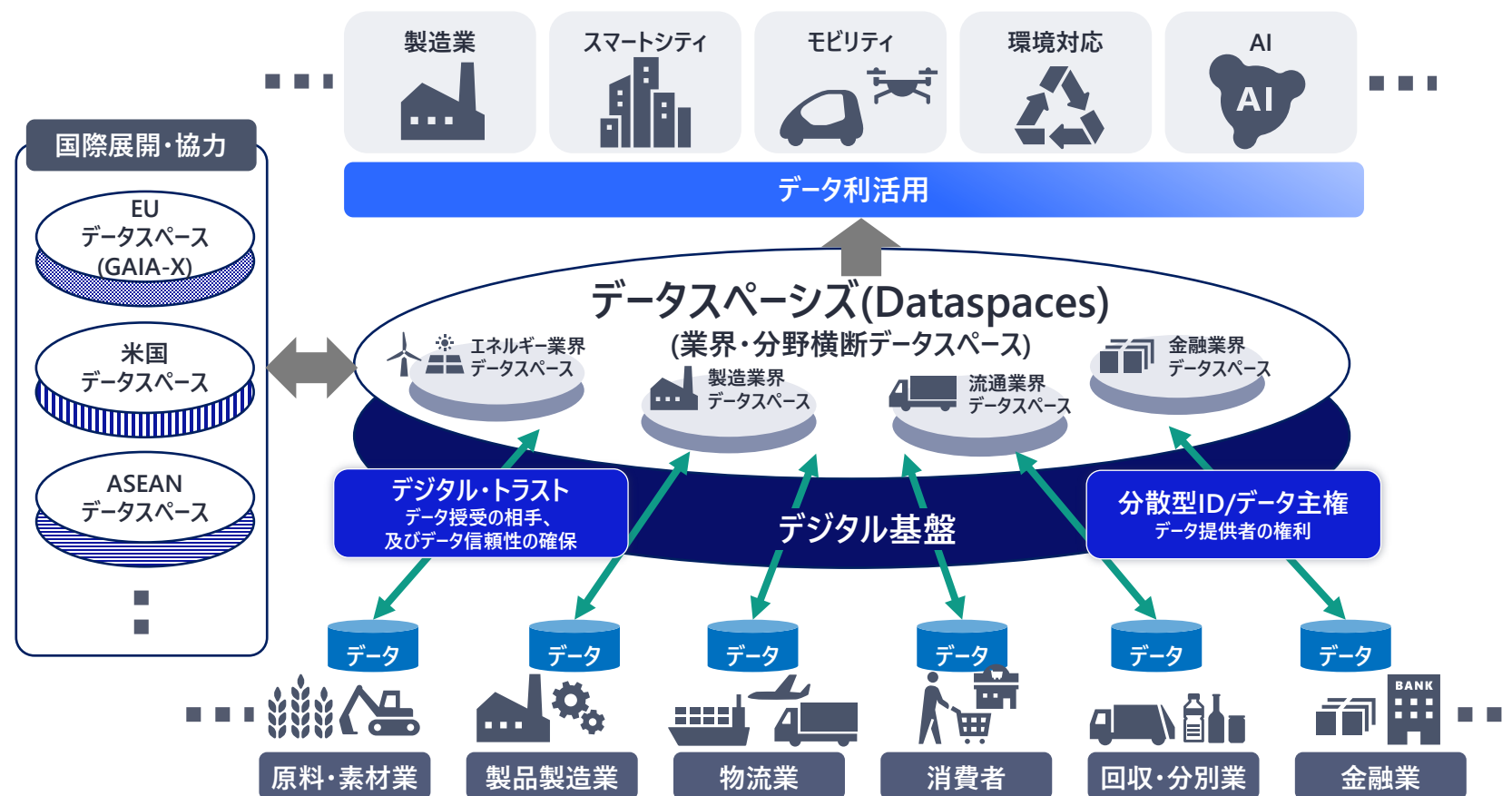
JDTF トラストッドデジタル ID 委員会

1. データスペースにおけるトラストの概要
2. 欧州の取り組み：データ流通基盤の制度設計とトラスト関連のこれまでの歩み
3. データスペースの分類とトラスト要件
4. データスペースで必要とされるトラスト技術
5. データスペースへのトラストの実装と運用
6. データスペースにおけるトラストの課題と展望
7. あとがき

1. データスペースにおけるトラストの概要
2. 欧州の取り組み：データ流通基盤の制度設計とトラスト関連のこれまでの歩み
3. データスペースの分類とトラスト要件
4. データスペースで必要とされるトラスト技術
5. データスペースへのトラストの実装と運用
6. データスペースにおけるトラストの課題と展望
7. あとがき

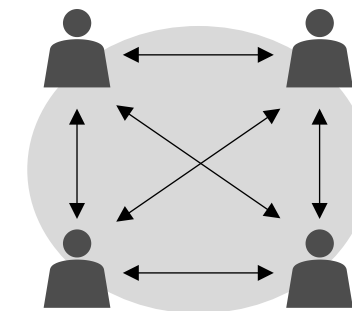
# データスペースとは何か

- データスペース： 共通ガバナンスの下で、複数参加者が安全・信頼性高くデータ共有できるエコシステム
- データ主権： 提供者が開示内容・範囲・期間をコントロールできること
- デジタルトラスト： 参加者とデータの真正性を担保する  
(以後、本ドキュメントで「トラスト」は「デジタルトラスト」の意味で用いる)



## データスペースにおけるトラスト

- 参加者が安心してデータ交換できる状態を担保するための制度・技術・運用
- N : Mな分散環境での安全な相互データ共有をデータ主権を保持しつつ実現



## トラストの目的



参加者の適格性確保と  
コンプライアンス違反防止



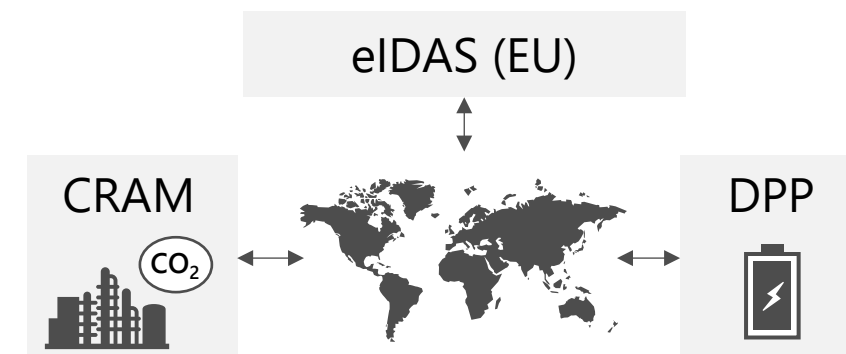
認証・認可による  
不正アクセス防止



共有するデータの正当性、  
真正性保証

## 国際相互運用性の確保

- 国際基準 (eIDASなどのトラスト) との同等性確保が必要
- 例：炭素国境調整措置 (CBAM)、デジタル製品パスポート (DPP) など



eIDAS: Electronic Identification, Authentication and Trust Services  
 CBAM: Carbon Border Adjustment Mechanism  
 DPP: Digital Product Passport

1. データスペースにおけるトラストの概要
- 2. 欧州の取り組み：データ流通基盤の制度設計とトラスト関連のこれまでの歩み**
3. データスペースの分類とトラスト要件
4. データスペースで必要とされるトラスト技術
5. データスペースへのトラストの実装と運用
6. データスペースにおけるトラストの課題と展望
7. あとがき

## 欧州の状況：法制度と主な取り組み

欧州は、政策を起点に**法制度** (Data Act、DGA、eIDAS等) → **標準化・技術的フレームワーク** (IDSA、Gaia-X等)  
 → **実装** (Catena-X等) を連動させ、データスペースとデジタルトラストの基盤を段階的に整備してきた。

	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
欧州委員会 (EU)	eIDAS規則施行		「共通の欧州データ空間に向けて」公表		欧州データ戦略公表		<ul style="list-style-type: none"> <li>データガバナンス法成立</li> <li>Data Spaces Support Centre (DSSC) 設立</li> </ul>	<ul style="list-style-type: none"> <li>データガバナンス法施行開始</li> <li>EU Data Act成立</li> </ul>	<ul style="list-style-type: none"> <li>eIDAS 2.0制定</li> <li>EU Digital Identity Wallet (EUDIW) 制度化</li> <li>EUDIW Architecture Reference Framework 実施規則採択</li> </ul>	EU Data Act 施行開始
International Data Spaces Association (IDSA)	Industrial Data Space e.V.設立	Reference Architecture Model for the Industrial Data Space公表	International Data Spaces Associationに改称	IDS Reference Architecture Model ver3.0 公表			IDS Reference Architecture Model ver4.0 公表			
Gaia-X				Project Gaia-X公表	Gaia-X Technical Architecture 公表	Gaia-X AISBL 設立				
Catena-X						Catena-X Automotive Network設立				

EUのデータスペース関連の政策を支える法制度として、下記の3本柱が存在する。

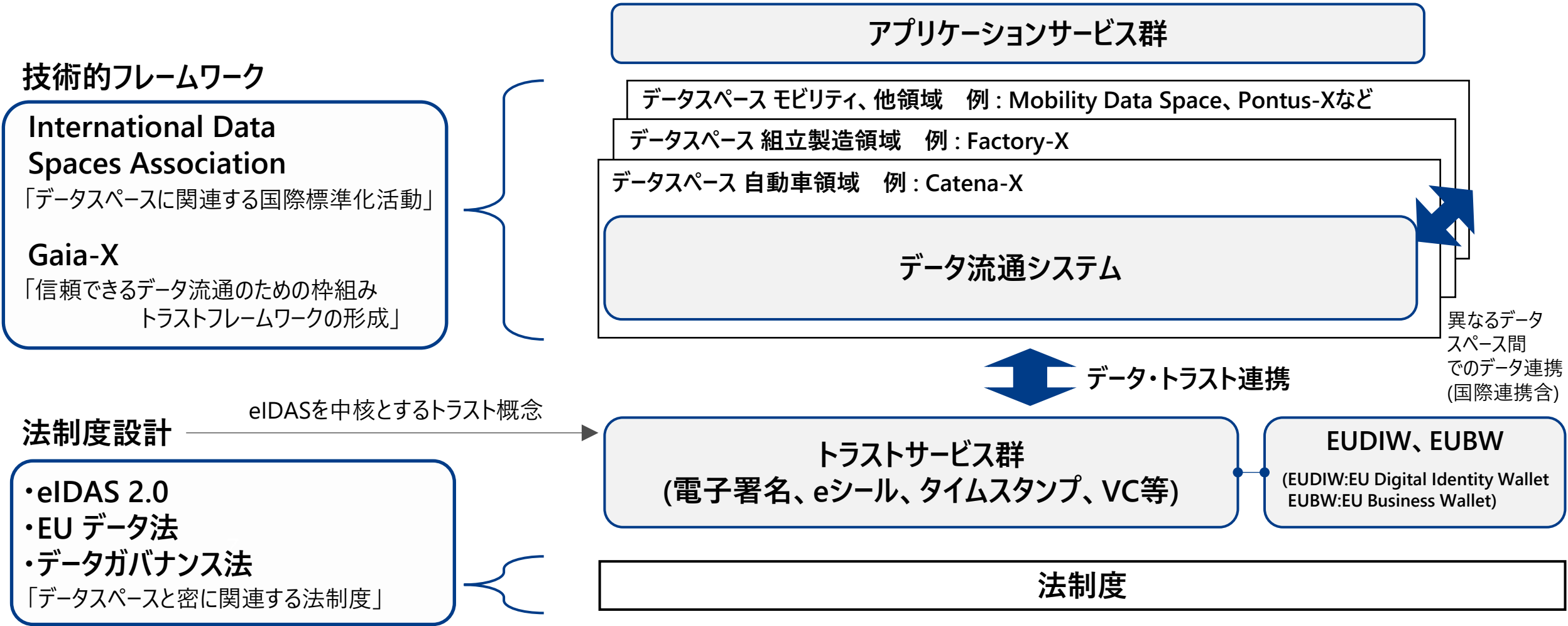
- **EUデータ法(Data Act):** 技術要件を法的に規定
  - データスペースの相互運用を前提とした具体的な技術仕様の順守を義務化する。
- **データガバナンス法(Data Governance Act : DGA):** 誰を信頼するかの制度基盤
  - データ仲介・利活用主体について「誰を信頼できるか」を制度的に定義・監督し、信頼あるデータ共有の基盤を整備する。
- **eIDAS規則(Electronic Identification, Authentication and Trust Services Regulation):** デジタルトラストの根幹
  - 電子署名・eシール等をEU全域で相互承認する法的トラストアンカーを提供し、データスペースの信頼の起点となる。

これらの3本柱により、EUはEU域内におけるデータスペース構築のみならず、**EU域外との連携（相互運用・相互認証）**を視野に入れた場合に必要となる制度的・技術的条件を法的に定義した。

特に、EUのデジタルトラストの根幹であるeIDAS規則をEUデータ法及びデータガバナンス法と組み合わせることで、Catena-Xに代表されるような具体的なユースケースにおいて、**国際的なデータ共有・相互認証が成立する枠組みの構築**を後押ししている。

# 標準化の動き：データスペースのエコシステムにおける関連規制・団体の役割

データスペースのエコシステムの中で、下図のように制度設計と技術的フレームワークが連携することで、欧州のデータスペースにおける標準化・トラストの基盤整備が着実に進められている。



- Catena-X等の法人を対象とするユースケースでは、法人PID + EAA + eシールが信頼の根拠となる。
- データスペースのトラスト設計と、EUデジタルアイデンティティウォレットは強く結びついている。
- EUデジタルアイデンティティウォレットに格納されるEAAは、データスペースにおける認証・認可の要。
- EUデジタルアイデンティティウォレットは「単なる保管」ではなく、「提示・検証・連携」の中核。

## eIDAS 2.0 の位置づけ

- eIDAS 2.0 は EU Digital Identity Wallet (EUDIW) の枠組みを法的に規定。
- PID (識別データ) およびEAA を定義。
- 自然人だけでなく、法人の識別・属性証明も対象。

\* EAA (電子属性証明: Electronic Attestation of Attributes)

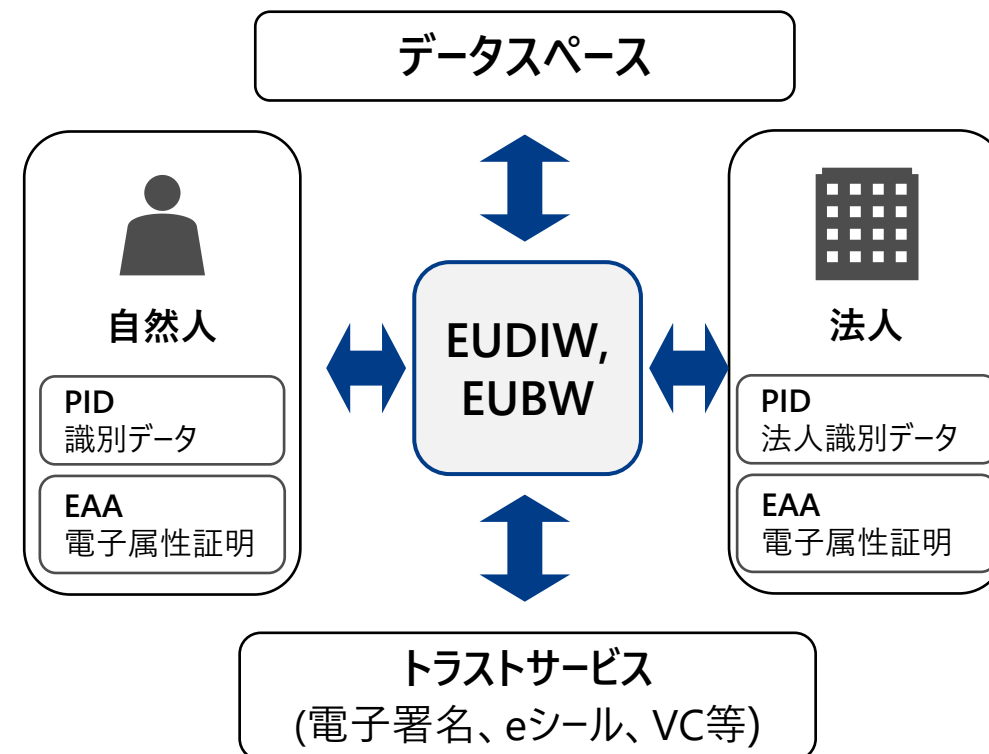
\* EUBWは法案提出中の状況

## EUDIW, EUBW の役割

- 電子署名、eシール、VC などのトラストサービスを提示・検証するエンドポイント。
- 自然人・法人の PID/EAA をデータスペースやトラストサービスに安全に提示。
- データスペースにおける「誰のデータか」「信頼できるか」を機械的に判断可能にする。

## 日本側の論点

- 法人識別子・法人属性・信頼できる証明をどのような制度・実装で整備するか。
- それをEU等との国際的な相互承認にどう繋げていけるか。



1. データスペースにおけるトラストの概要
2. 欧州の取り組み：データ流通基盤の制度設計とトラスト関連のこれまでの歩み
- 3. データスペースの分類とトラスト要件**
4. データスペースで必要とされるトラスト技術
5. データスペースへのトラストの実装と運用
6. データスペースにおけるトラストの課題と展望
7. あとがき

# トラスト要件によって変わるデータスペースの分類

データスペースはデータの**管理・トラスト確保**の観点から、「分散型」、「ハイブリッド型」、「連邦型」、「集中型」の4つに分類される。

	分散型	ハイブリッド型	連邦型	集中型
概念図				
特徴	<ul style="list-style-type: none"> <li>データは各参加者が直接管理する。</li> <li>参加者同士がトラストを相互検証しながらデータを流通させる。</li> </ul>	<ul style="list-style-type: none"> <li>データの管理は、参加者が自身で行うこともプラットフォームに管理させることもできる。</li> <li>トラスト確保（認証・認可・管理・運用）は参加者が行う。</li> </ul>	<ul style="list-style-type: none"> <li>データはサービスPF提供者が代行管理する。</li> <li>サービスPF提供者がトラスト確保（認証・認可・管理・運用）も行う。</li> </ul>	<ul style="list-style-type: none"> <li>データはデータプラットフォームで管理される。</li> <li>トラスト確保（認証・認可・管理・運用）はPF運用者が一元的に行う。</li> </ul>
参加者の認証・認可	DID/VC	DID/VC	ID/パスワード DID/VC	ID/パスワード
真正性	電子署名 (VC、e シール、タイムスタンプ)			[PF運営者]
トラストアンカー	トラステッドリスト (トラストサービスプロバイダー)			[PF運営者]

1. データスペースにおけるトラストの概要
2. 欧州の取り組み：データ流通基盤の制度設計とトラスト関連のこれまでの歩み
3. データスペースの分類とトラスト要件
- 4. データスペースで必要とされるトラスト技術**
5. データスペースへのトラストの実装と運用
6. データスペースにおけるトラストの課題と展望
7. あとがき

- 本ドキュメントでは、トラスト技術を**実在性保証**、**真正性保証**、**運用関連**の3つに分けて説明する。
- データスペースにおけるトラスト技術は、参加者の利便性や運用負担、国際標準や法制度、業界ガイドラインへの準拠を考慮し、**バランスを取って技術を選定**する必要がある。

## 実在性保証

- 信頼できる情報源
  - 参加者の実在性を保証する情報源
- ノタリーサービス
  - 信頼できる情報源から情報を取得し、参加者にクレデンシャルを発行するサービス
- トラステッドリスト
  - データスペース内で信頼される情報をまとめたリスト

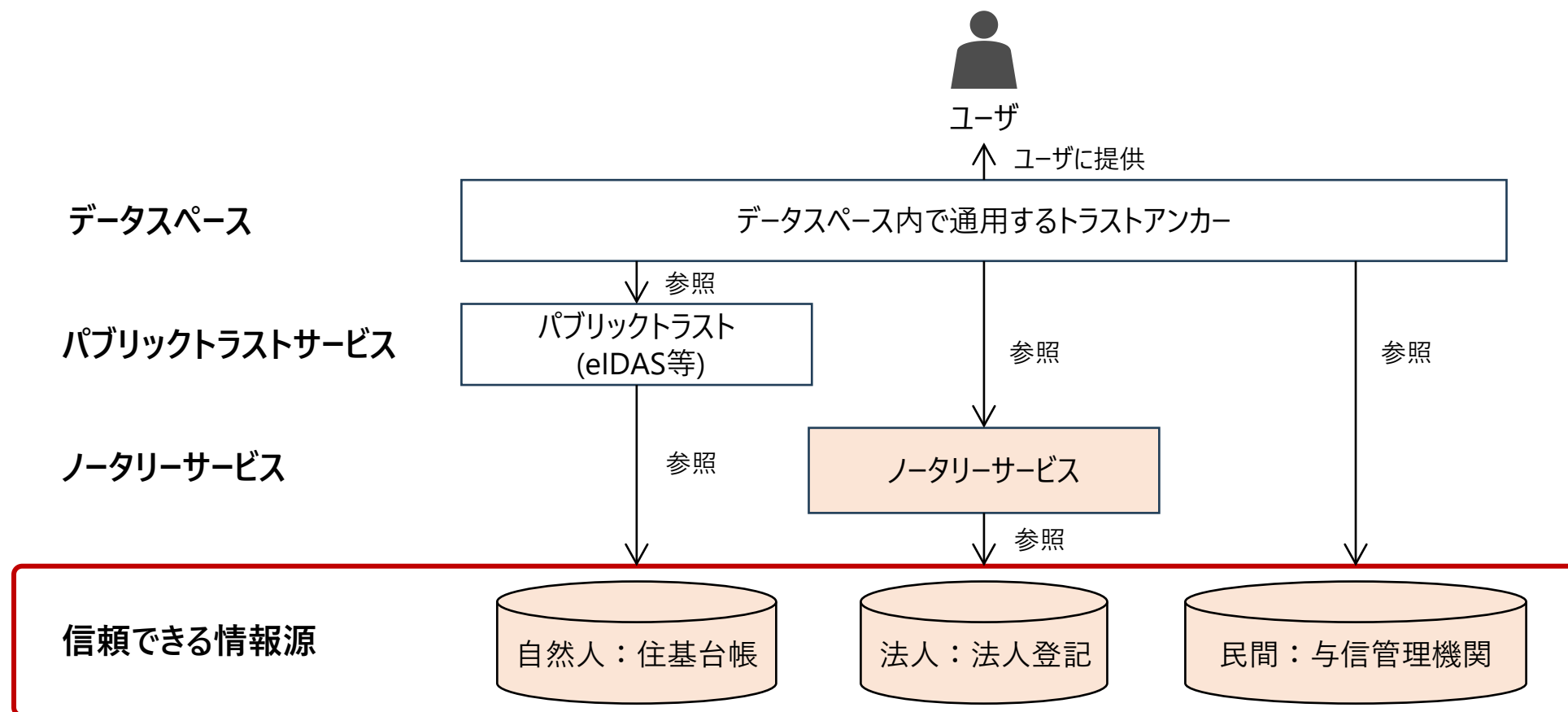
## 真正性保証

- トラストアンカー
  - トラストの起点
- 電子署名
  - データの真正性・本人性を保証する技術
- eシール
  - 法人等による電子署名
- タイムスタンプ
  - データの時刻証明
- Verifiable Credential (VC)
  - 検証可能な証明書

## 運用関連

- メンバーシップ管理
  - 参加者の適格性の管理
- デジタルIDウォレット
  - IDやデータを安全に保管するウォレット
- コネクタ
  - 安全なデータ交換とデータ共有を実現する技術

- 信頼できる情報源とは、企業・組織等(Holder)に対して資格や属性の証明を発行する主体(Issuer)が、その証明の妥当性を裏付けるために使用する情報の出所を指すものである。
- ノタリーサービスとは、外部の信頼できる情報源（例：住民基本台帳、法人登記）から属性情報を取得し、データスペース参加者に対してクレデンシャルを発行するサービスである。



- 日本における組織の実在確認のための識別子を説明する。一意に特定可能な識別子としては、総務省「eシールに係る指針(第2版：令和6年4月) [1]」の「図8 保証レベル2の認定eシール用認証業務におけるeシール用電子証明書に使用する組織識別子」が候補となる。
- 以下識別子の源泉となるデータベースは、**信頼される情報源**ともなる。

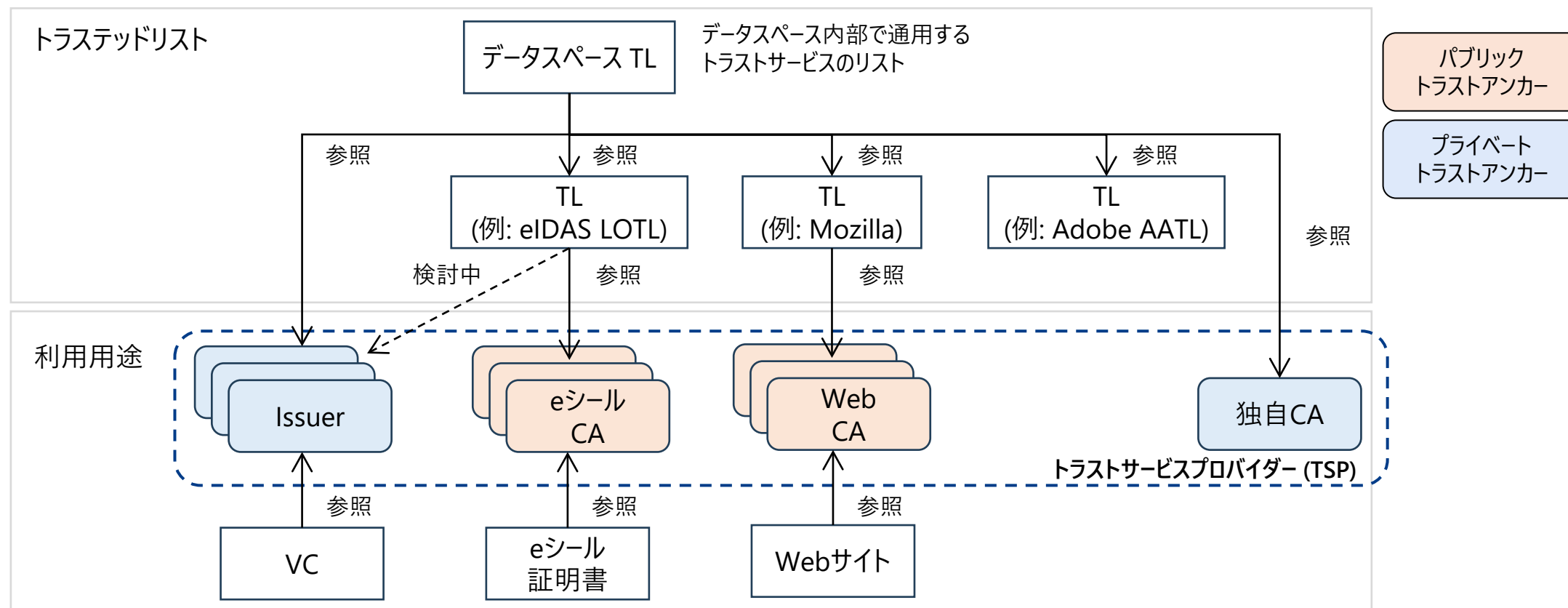
組織識別子	内容および補足事項	国際標準規格 発番機関
法人番号	国税庁長官が、次の法人等に対して法人番号を指定。 1. 国の機関, 2. 地方公共団体, 3. 設立登記法人, 4. 1～3以外の法人又は人格のない社団等であって、所定の税法上の届出書を提出することとされている者, 5. 1～4以外の法人又は人格のない社団等であって、税務書類を提出するなど、一定の要件に該当する者で、国税庁長官に届け出た者 参考：法人番号とは <a href="https://www.houjin-bangou.nta.go.jp/setsumei/">https://www.houjin-bangou.nta.go.jp/setsumei/</a>	ISO6523-2「0188」, ISO/IEC 15459-2「TAJ」, UN/EDIFACT 3055「402」
会社法人等番号	日本で商業登記されている法人等に対して法務局が付与する番号。 個人事業主は「商号登記」を行うことで発番される(任意)。	
適格請求書 発行事業者登録番号	適格請求書発行事業者の登録を受けようとする事業者が、納税地を所轄する税務署長に「適格請求書発行事業者の登録申請書」を提出し、税務署長の登録を受けた場合に事業者へ通知される番号。 参考：登録番号とは <a href="https://www.invoice-kohyo.nta.go.jp/about-toroku/index.html">https://www.invoice-kohyo.nta.go.jp/about-toroku/index.html</a> 個人事業主でも一部は発番されない。	ISO6523-2「0221」
LEI	国際標準化機構 (ISO) が定めたISO 17442に基づく20文字の英数字コード。 参考：組織の特定 - 取引主体識別子 (LEI) とは <a href="https://www.gleif.org/ja/organizational-identity/introducing-the-legal-entity-identifier-lei/">https://www.gleif.org/ja/organizational-identity/introducing-the-legal-entity-identifier-lei/</a>	ISO 17442
TDB企業コード	株式会社帝国データバンクが独自管理する9桁の企業識別番号。	ISO6523-2「0170」, ISO/IEC 15459-2「VTD」, UN/EDIFACT 3055「311」
TSR企業コード	株式会社東京商工リサーチが独自管理する9桁の企業識別コード。	
標準企業コード		ISO6523-2「0147」, ISO/IEC 15459-2「LA」, UN/EDIFACT 3055「289」

[1] [https://www.soumu.go.jp/main\\_content/001006115.pdf](https://www.soumu.go.jp/main_content/001006115.pdf)

※GビズIDは共通認証基盤であり、識別子そのものではないため、上記識別子とは区別される。

# 実在性保証：トラステッドリスト

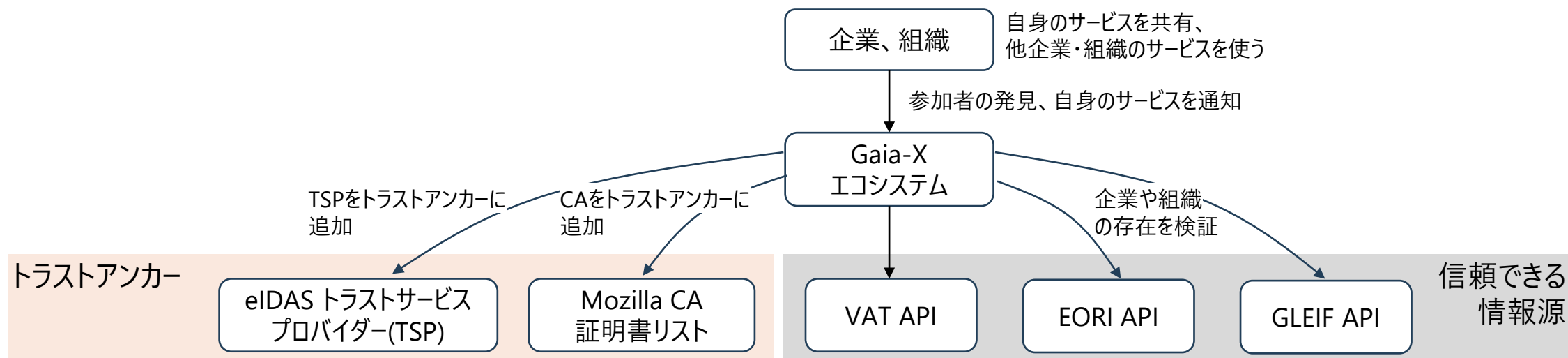
- **トラステッドリストとは、信頼できるトラストサービスプロバイダー (TSP) を参照するリストであり、データスペースでの利用時には、独自のルールやポリシーを満たす信頼できるデータスペース内のサービスやコンポーネントを明確にすることができる。**
- **登録されるトラスタンカーは、運営者の判断によりパブリックなものやプライベートなものが混在していてもよい。**
  - **パブリックトラスタンカー**：公的機関や他組織により管理され広い範囲で参照可能なTL情報
  - **プライベートトラスタンカー**：当該データスペース内で有効な独自CA情報、Issuer情報



# 真正性保証：トラストアンカー

- データスペースにおけるトラストアンカーは、“デジタルトラストにおける信頼の連鎖の基点/根源となるエンティティであると、データスペースの運営者が定めた対象”である。
  - 信頼が前提とされている権威あるエンティティ
  - 例：ルート認証局や、トラステッドリストに掲載されたエンティティ
- 従来、PKIは通信/署名の正当性を保証する信頼が中心である。データスペースでは、誰がその属性※を発信したのかという、情報の信頼の起点も重要である。
  - 情報の出所に関する起点は、「信頼できる情報源」として区別して扱う
  - 例：Gaia-Xシステムでは、VAT/EORI/GLEIFが「信頼できる情報源」に該当

※「属性」とは、企業や組織等に関する情報。  
 例えば「所在地」「資格」など、信頼できる形で発行されることを含む

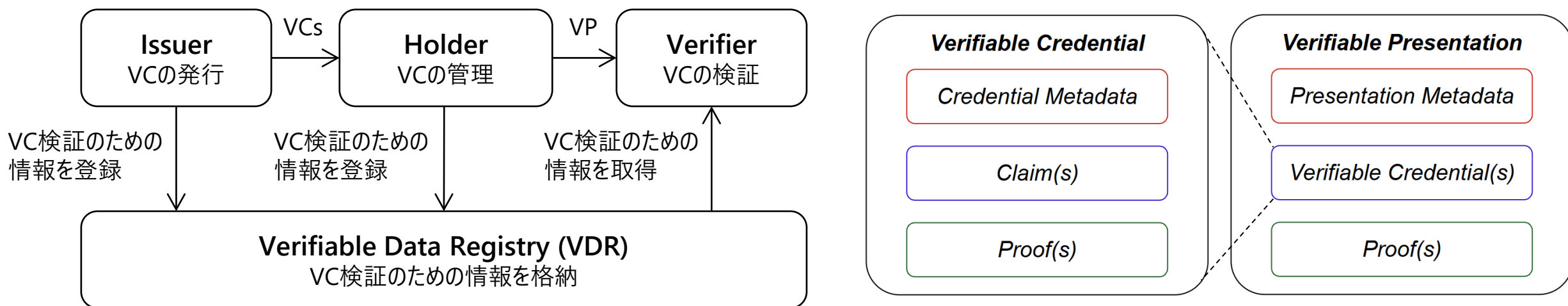


Gaia-Xシステム [1]

[1] <https://gitlab.com/gaia-x/lab/gxdch/-/blob/main/architecture/loire/softwareSystem.puml>

# 真正性保証：VC(Verifiable Credential) / VP(Verifiable Presentation)

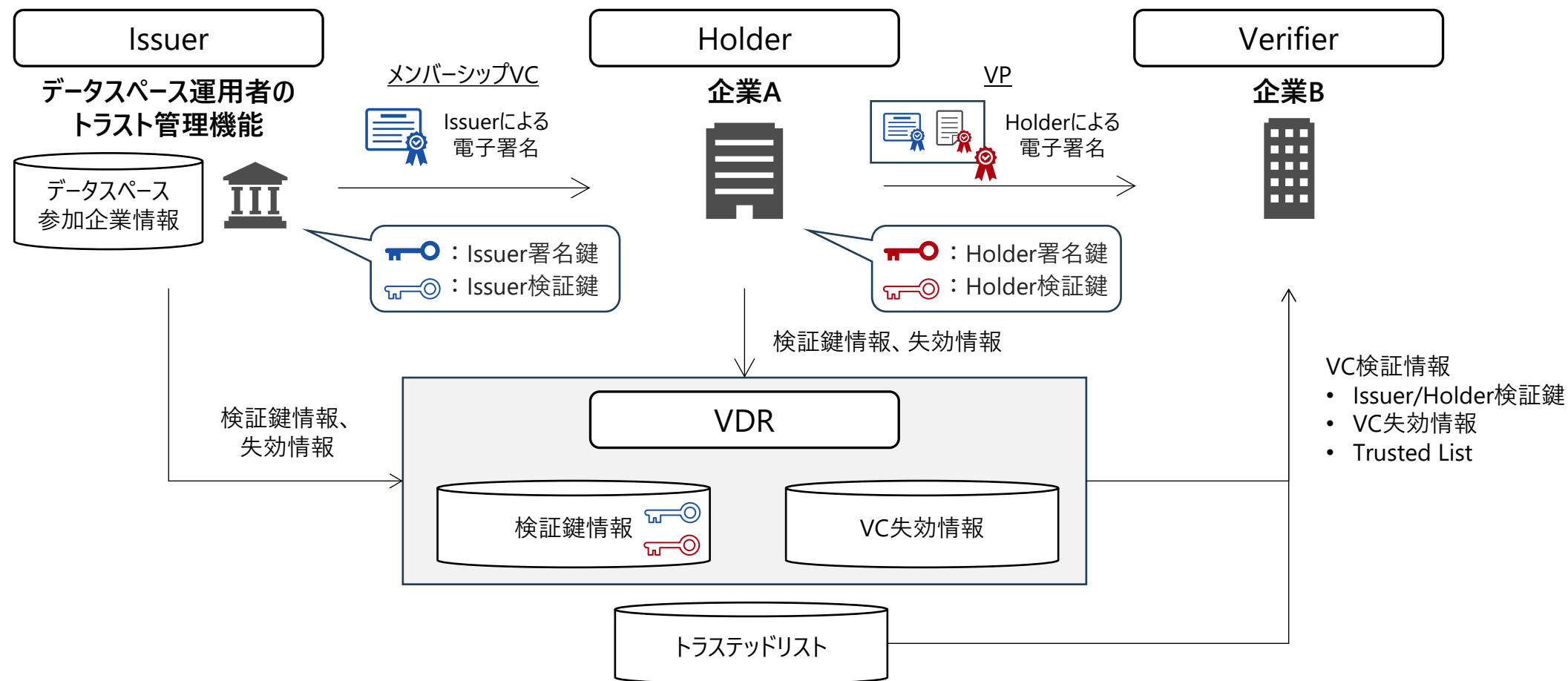
- VC (Verifiable Credential) は、属性情報や証明を第三者へ伝えるための資格情報のフォーマットである。Issuerが署名を行うことで、データの完全性と発行者の真正性が保証される。VCにはClaimやMetadata、Proofが含まれ、Claimは属性情報、ProofはIssuerによる署名である。
- HolderはVCをもとにVP (Verifiable Presentation) としてVerifierに提示し、VPには複数のVCやHolderの署名が含まれる。署名にはHolderの署名鍵が用いられる。検証にはDID (Decentralized Identifier) に紐づく検証鍵などが活用され、検証時にVDR等から取得される。これにより、安全かつプライバシー保護を考慮した証明が可能となる。



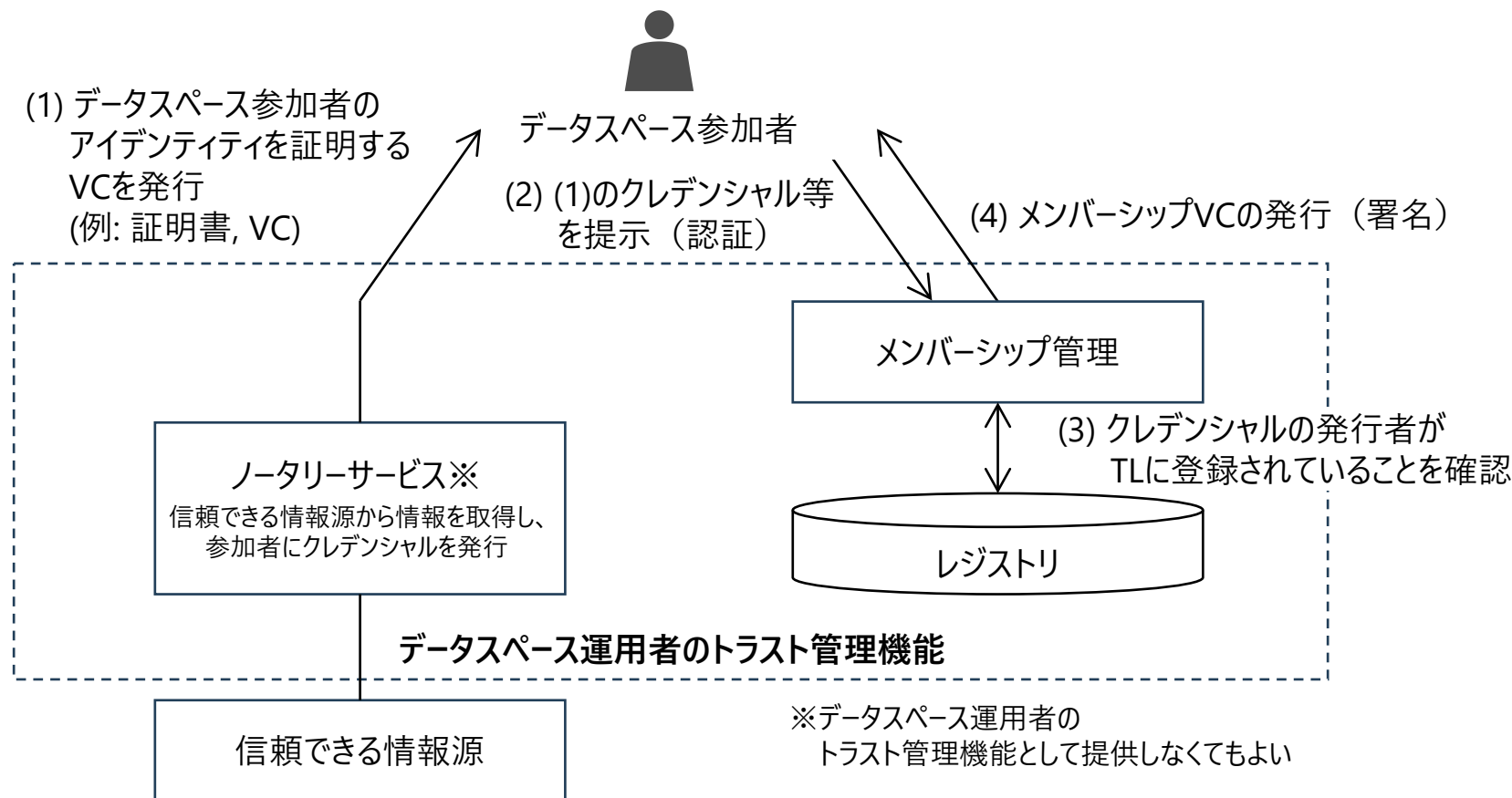
W3C, Verifiable Credentials Data Model v2.0, <https://www.w3.org/TR/vc-data-model-2.0/>を元に作成

# 真正性保証：データスペースにおけるVC/VPの活用例

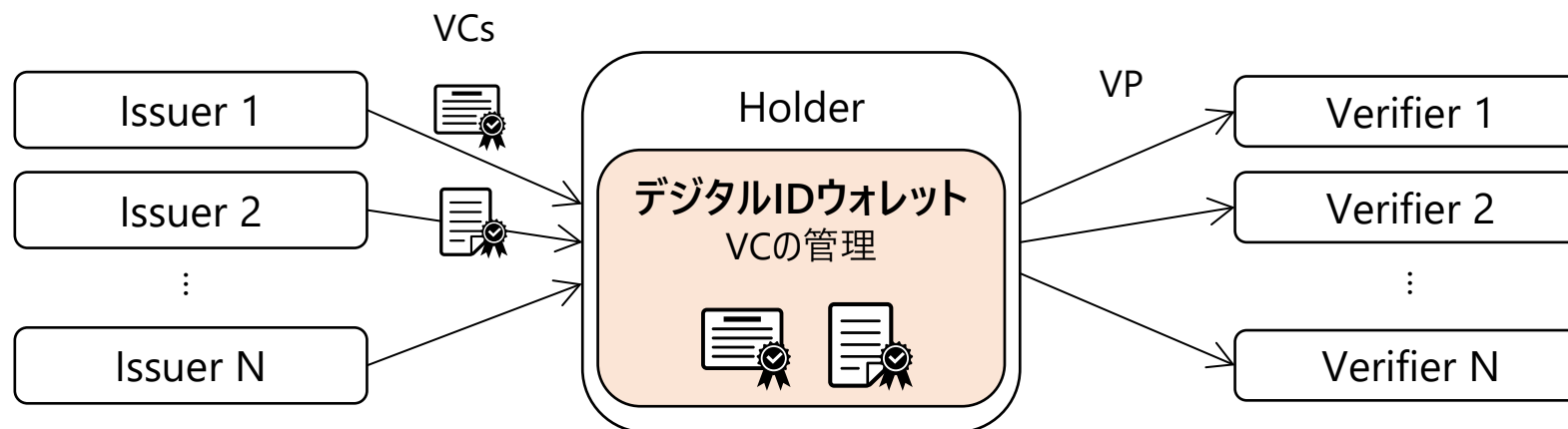
企業Aはデータスペース運用者のトラスト管理機能にメンバーシップVCを発行依頼し、Issuerの署名鍵で署名されたVCを受け取る。企業AはこのVCをもとにHolderの署名鍵で署名されたVPを作成し、企業Bに提示する。企業BはVP検証のために、IssuerとHolderの検証鍵、失効情報をVDRから取得し、検証に成功すれば企業Aの参加資格を確認できる。



- データスペースでは、データスペース運用者のトラスト管理機能が、ノタリーサービス、VC、署名、トラステッドリストなどを活用し、トラストを担保したメンバーシップ管理を実現する。
- メンバーシップ管理機能は、クレデンシャルの発行者が登録されたトラステッドリストに存在することを確認した上で、署名したメンバーシップVCを発行し、安全なデータ連携を実現する。



- デジタルIDウォレットとは、デジタルID (デジタル化されたユーザ (個人・組織) の身元識別情報) による身元提示や自らの属性情報の提供を、HolderがPCやモバイル端末上で管理する仕組みである [1]。
- 自然人向けのデジタルIDウォレットとしては、EUDIW (EU Digital Identity Wallet) があり、欧州にて活発な議論および開発が進められている [2]。
- 法人向けのデジタルIDウォレットとしては、EBW (EU Business Wallet) の議論が開始されている。法案提出中の状況であり、自然人向けのデジタルIDウォレットと比較すると仕様に関する議論はこれからである [3]。

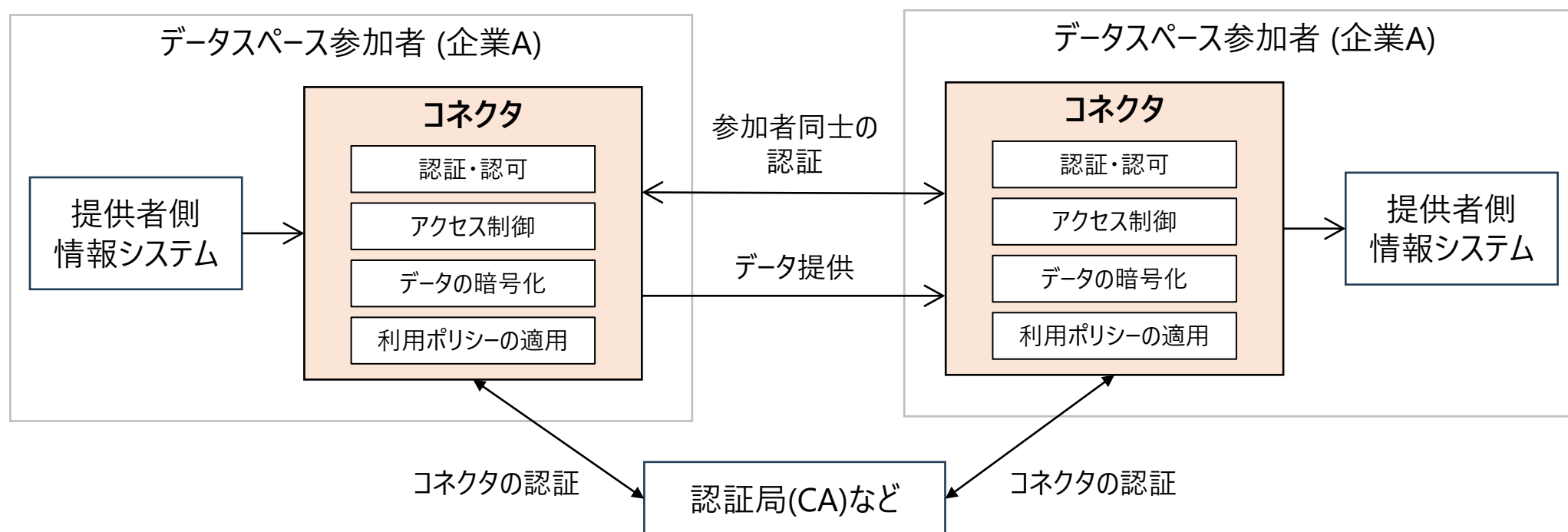


[1] <https://www.hitachi-hri.com/research/researchreport/short/k141.html>

[2] <https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/694487738/EU+Digital+Identity+Wallet+Home>

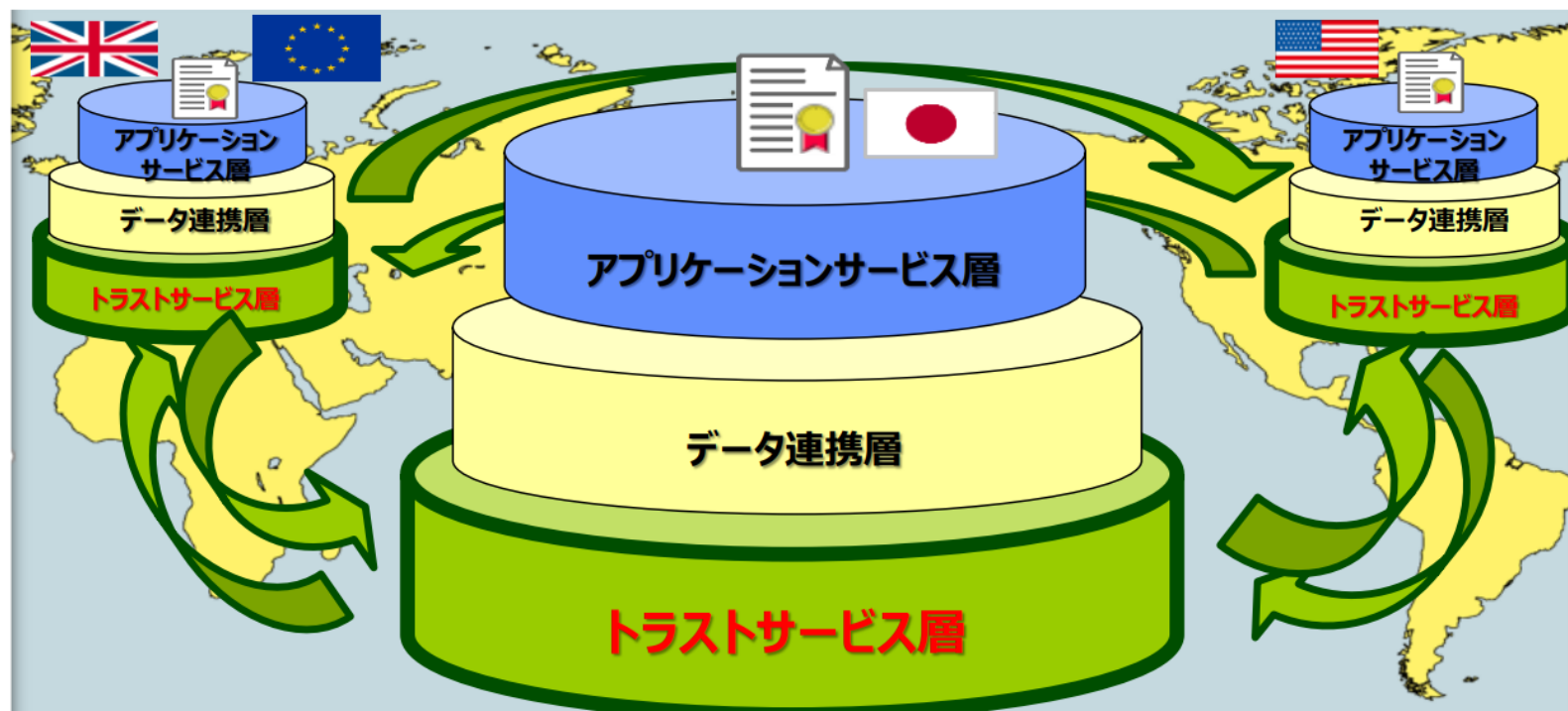
[3] <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0838>

- コネクタとは、異なるシステムや組織間でデータを安全かつ効率的に交換するためのコンポーネントである。
- データスペースのルールやプロトコルに準拠し、データの提供者と利用者の中で、データの発見、アクセス、交換、利用の仲介を行う。
- コネクタには、アクセス制御、認証、データの暗号化、利用ポリシーの適用などの機能が含まれ、データ主権とプライバシーを保護し、指定された目的や条件に従って共有されていることを保証し、データスペースにおけるデータエコシステム全体の相互運用性を高める。
- コネクタを使用する際には、コネクタ自体の認証を行うことが必要である。



1. データスペースにおけるトラストの概要
2. 欧州の取り組み：データ流通基盤の制度設計とトラスト関連のこれまでの歩み
3. データスペースの分類とトラスト要件
4. データスペースで必要とされるトラスト技術
- 5. データスペースへのトラストの実装と運用**
6. データスペースにおけるトラストの課題と展望
7. あとがき

- 産業データスペースは、データ連携時の機能・サービスの観点からユースケースに関わらず3層で構成される。
  - アプリケーションサービス層：ユーザがデータ連携・利活用を通じて、価値創出に結びつけるサービスを提供する層
  - データ連携層：ユーザ間での安全・安心なデータ連携を支える層
  - トラストサービス層：改ざんやなりすましを防ぎ、信頼性を担保するサービスを提供する層

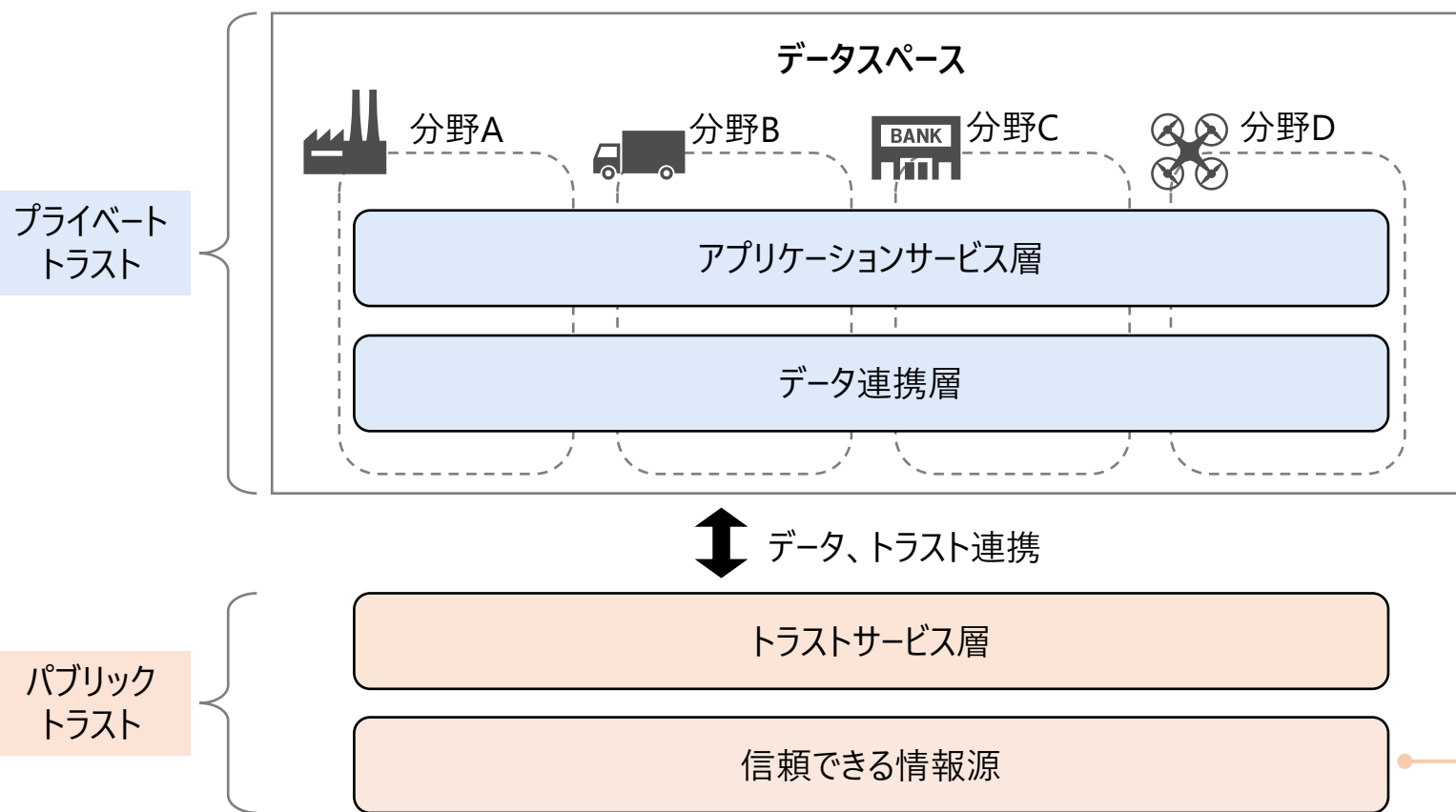


産業データスペースの「3層構造」のイメージ [1]

[1] [https://www.cas.go.jp/jp/seisaku/digital\\_gyozaikaikaku/kaigi10/kaigi10\\_siryou9.pdf](https://www.cas.go.jp/jp/seisaku/digital_gyozaikaikaku/kaigi10/kaigi10_siryou9.pdf)

# 産業データスペースの3層アーキテクチャとトラストの切り分け

- トラストに裏打ちされたデータ連携と利活用を実現するためには、前頁の3層アーキテクチャが互いに連携し合うことが必要である。
- 組織や個人の実在性確認等を行うための「信頼できる情報源」が必要である。
- 本ドキュメントでは、アプリケーションサービス層およびデータ連携層は、データスペース内のプライベートトラスト、トラストサービス層および信頼できる情報源はパブリックトラストと定義する。



データスペースのあるべき姿におけるデータスペースの各層の機能群

層	機能
アプリケーションサービス層	各種サービス・機能を提供するアプリケーション等
データ連携層	コネクタ、データスペース運用者のトラスト管理機能等
トラストサービス層	CA、トラステッドリスト等
信頼できる情報源	自然人：住基台帳、法人：法人登記、JPX-LEI制度 (LEI)等

公的なレジストリや民間の情報提供サービスにより、組織や個人の実在性確認等を行うための「信頼できる情報源」が必要

# データスペースとトラスト

- データスペースはデータ連携を安全・持続的に行うための基盤であり、技術とガバナンスを統合してトラストを担保する。
- 主要要素はメンバーシップ管理、アクセス認証・認可、データ真正性確保の3つである。

## メンバーシップ管理 1

参加企業の実在確認とメンバーシップの管理、ならびに、参加企業（メンバーシップ）に関する属性情報の提供



参加企業の実在性の確認やメンバーシップ管理が必要

## アクセス認証・認可 2

アクセス認証・認可でポリシー準拠の利用を制御



不正利用を防ぐためにポリシー準拠の利用制御が必要

## データ真正性確保 3

eシールやVCを活用したデータ署名により真正性(完全性、発信者認証)を担保



デジタル署名を活用した真正性(完全性、発信者認証)の担保が必要

- データスペースにおけるトラストは、**利用範囲の拡大に応じて適切に担保されるべきである。**
- すなわち、内部利用、国内利用、国際利用の順で、トラストを適切に設定すべきである。

内部（単一組織内）利用



国内（同一国内の複数組織間）利用



国際（国を跨る複数組織間）利用

利用範囲  
拡大における  
トラスト

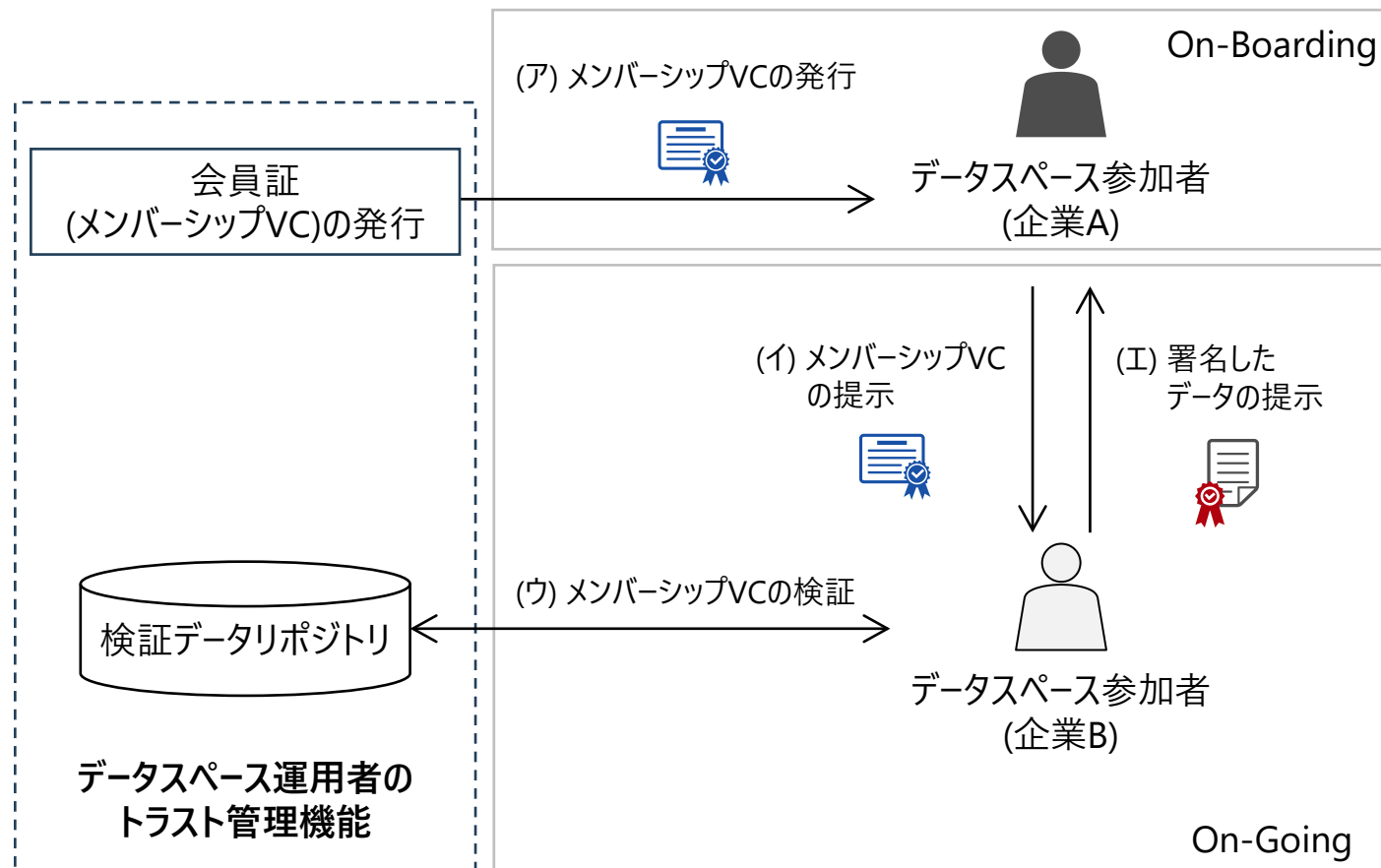
組織内のガバナンスに  
依拠したトラストの確立が必要

国内における共通のルールの策定や  
法的枠組みの整備が必要

各国のデータ保護法令への  
適合を前提とし、国際標準への準拠によって  
相互運用性を担保が必要

# データスペースにおけるメンバーシップの運営 (4フェーズ)

- データスペースは基本的に会員制の組織であり、会員間の信頼は会員制に依拠し維持される。
- データスペース運用者のトラスト管理機能から受け取る会員証 (=メンバーシップVC) をもとに、「On-Boarding」、「On-Going」、「Off-Boarding」、「属性情報の変更」の4つのフェーズで運営される。



#	内容
(ア)	企業Aの参加者は、データスペース運用者のトラスト管理機能から、データスペースの会員証である「メンバーシップVC」を受け取る。
(イ)	企業Aの参加者は、企業Bの参加者にデータを要求する際に、自身のメンバーシップVCを提示する。
(ウ)	企業Bの参加者は、企業AのメンバーシップVCを検証するため、データスペース運用者が提供するVDRやノタリーから検証情報を取得し、その正当性を確認する。
(エ)	メンバーシップVCの正当性が確認でき、適切なアクセス権限を確認できた場合、企業Bの参加者は自身の署名鍵でデータに署名し、企業Aの参加者に提示する。

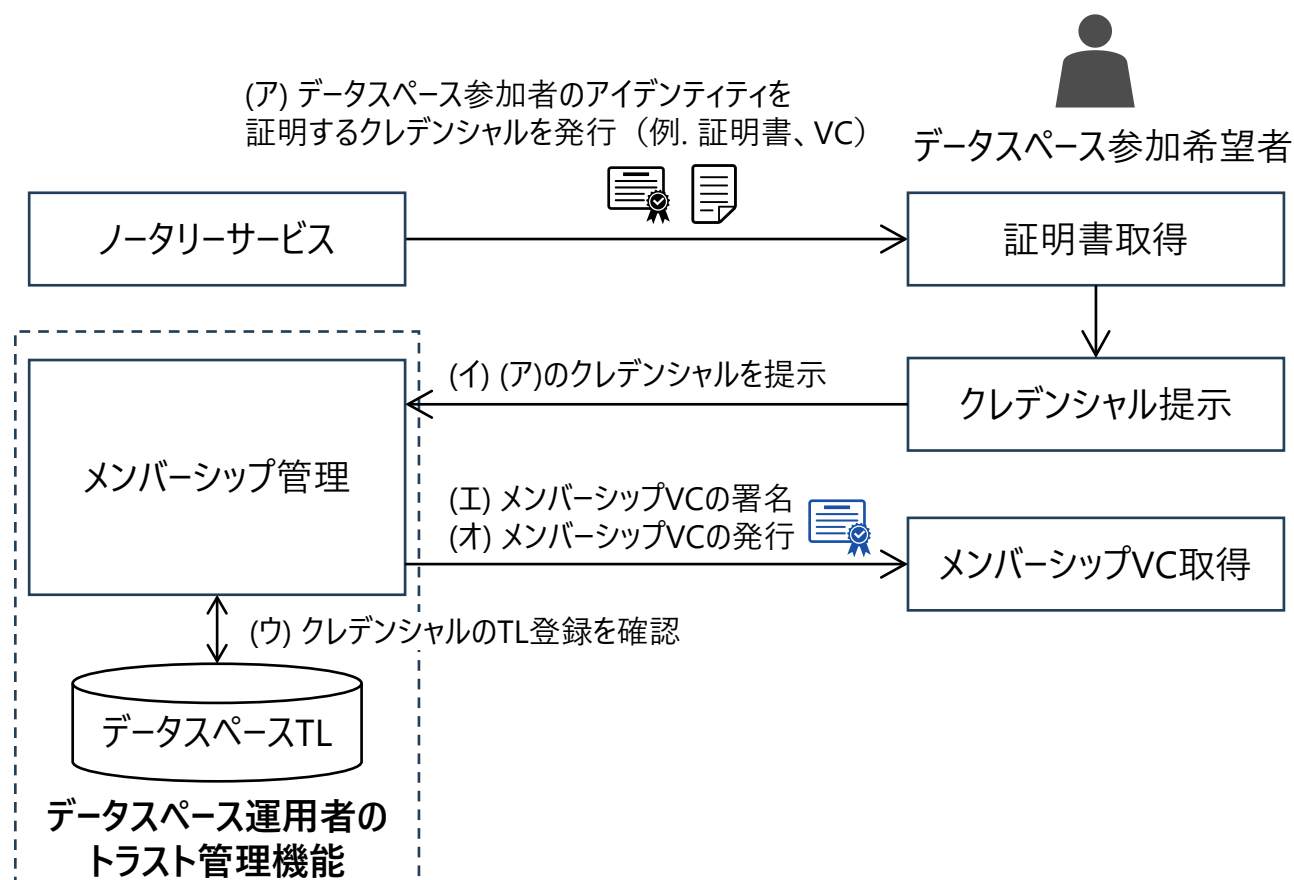
# On-Boarding：実在性確認とメンバーシップVCの発行

メンバーシップ管理

アクセス認証・認可

データ真正性確保

- データスペースへの参加希望者は、ノタリーサービス等から発行されたクレデンシャルを用いて、データスペース運用者にメンバーシップVCの発行を要求する。
- データスペース運用者は、参加希望者から受け取ったクレデンシャルを確認し、組織のポリシーに照らして審査する。審査に合格した場合、参加資格を証明するメンバーシップVCを発行する。



- クレデンシャルの発行・提示：(ア), (イ), (オ)**  
相互運用性を担保した設計と実装エコシステムを有する国際標準に準拠する必要がある。例えば、VCを授受する場合は、OID4VCI/OID4VPの採用を推奨。
- クレデンシャルの確認：(ウ)**  
組織に対する実在の確認として以下が必要。
  - 法的な実在性確認
  - 物理的実在性確認
  - 運営的実在性確認
 組織を確認して識別するにあたっては、一意に特定可能な識別子として、4章にて説明した「現状の日本における組織に対する実在確認のための識別子」の活用が考えられる。
- メンバーシップVCの署名：(エ)**  
第三者がVCの真正性、完全性、有効性（失効有無を含む）を検証可能であることが本質的な要件である。メンバーシップVCを発行するデータスペース運用者は、検証に必要な公開情報を整備し、継続的に維持する責務を負う。（VDR等のレジストリを公開するなど）

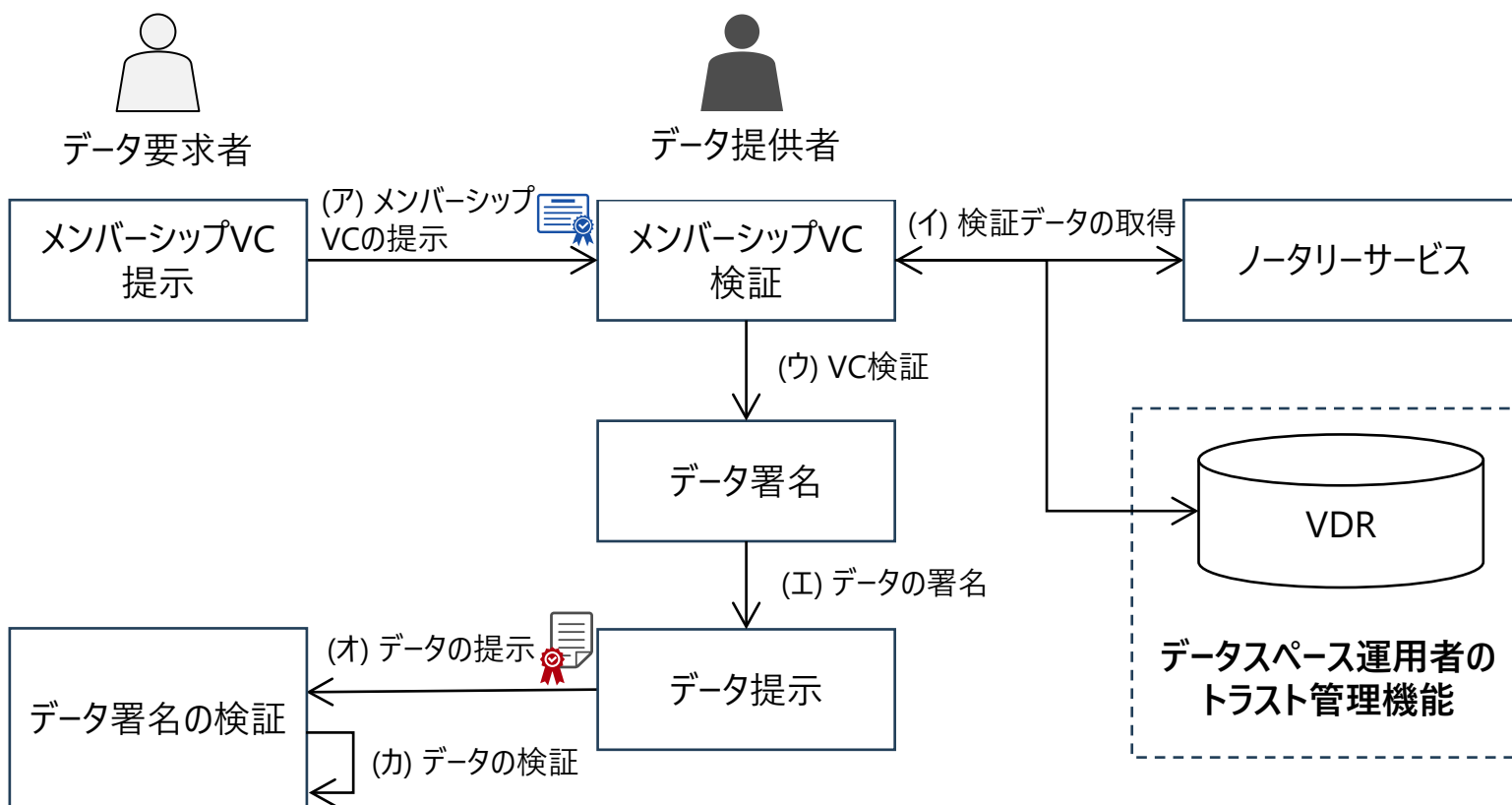
# On-Going : メンバーシップVCの検証とデータへの署名/検証

メンバーシップ管理

アクセス認証・認可

データ真正性確保

- データ要求者がデータをリクエストし、データ提供者がメンバーシップVCをもとに、要求者の検証を実施する。
- データ提供者は署名したデータを送り、データ要求者は受け取ったデータを検証する。
- 検証は都度実施し、運用中は有効性（失効有無を含む）を継続的に確認する。



- クレデンシャルの発行・提示 : (ア), (オ)**  
On-Boardingと同様に国際標準に準拠する必要がある。
- データスペースで授受されるVCおよびeシールの検証 : (イ), (ウ), (カ)**  
参加者間のデータ共有を実現するためには、参加者および発行主体の正当性を担保することが不可欠。実現手段として、eシールとVCが用いられる。
- データの署名 : (イ)**  
DIDに紐づく署名鍵およびeシールに紐づく署名鍵を活用し、検証可能な形式でデータに署名する。

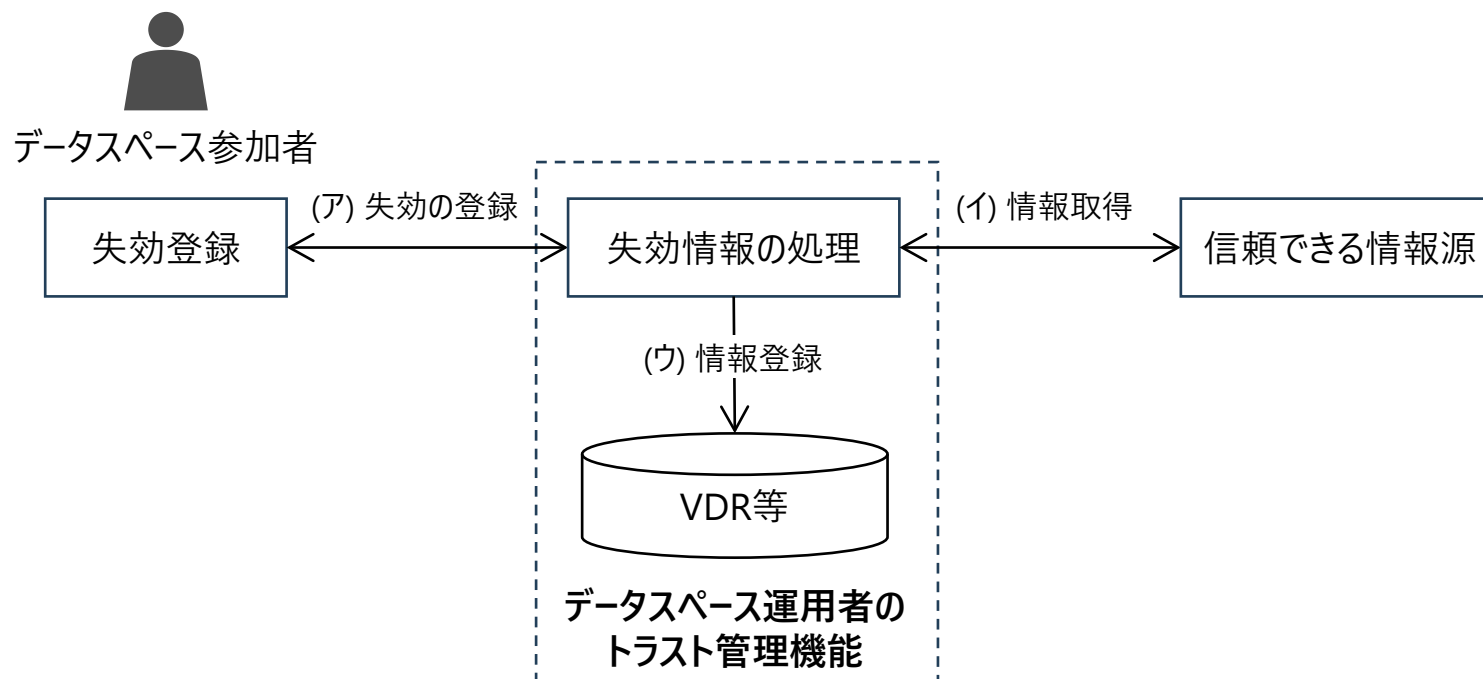
# Off-Boarding：メンバーシップVCの失効

メンバーシップ管理

アクセス認証・認可

データ真正性確保

- 参加資格喪失時に、会員証（メンバーシップVC）を確実に無効化し、他者が誤認しない状態を作る。
- データスペースへの参加組織からの申請に基づくOff-Boardingを実施する。
- データスペースにおけるポリシー上、参加が不適切と判断される場合は、データスペース運用者によるOff-Boardingを実施する。

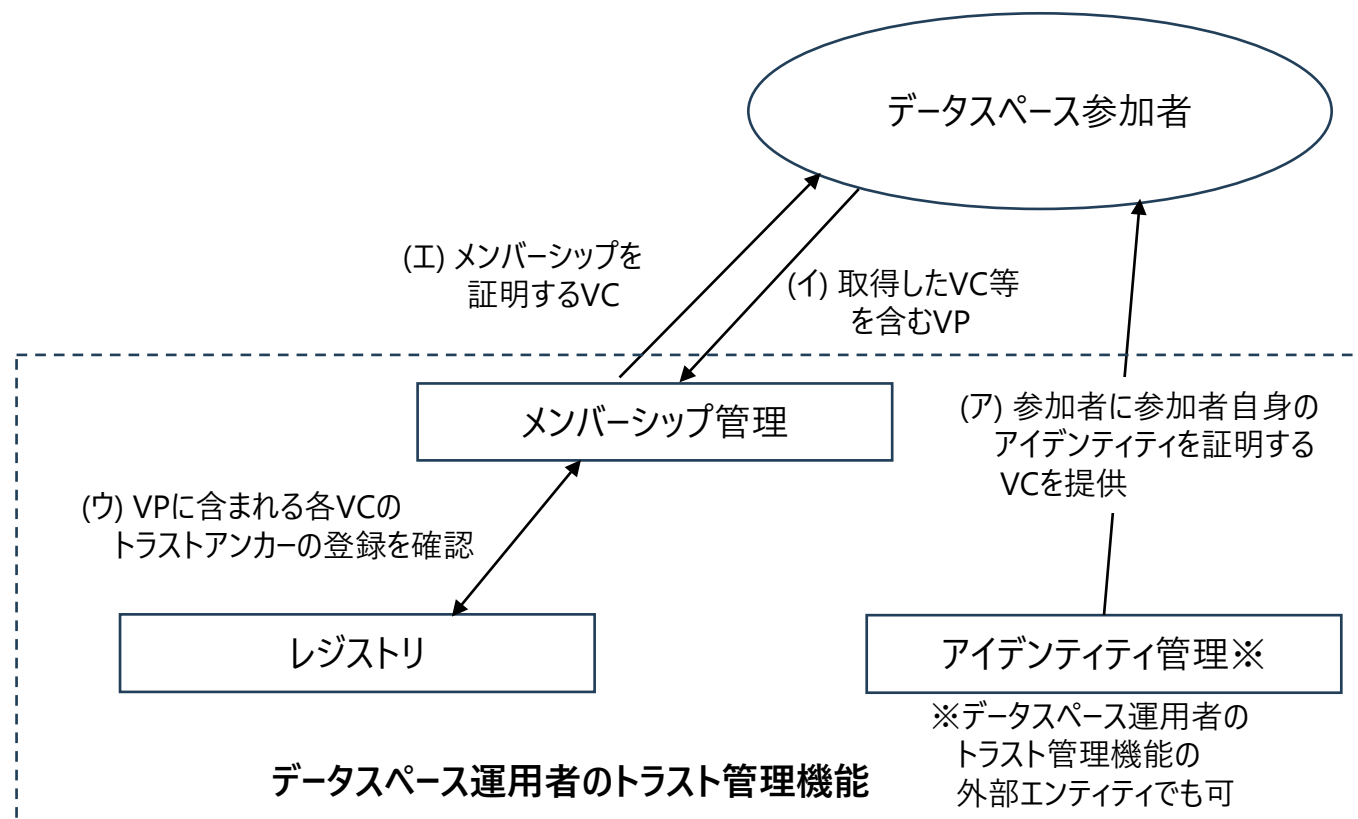


- (1) 参加者起点の失効登録：(ア)**  
データスペース参加者がデータスペースの不参加を決定する、もしくは、データスペースの担当から離れる場合、参加者起点で失効登録する。
- (2) データスペース運用者起点の失効登録：(イ)**  
外部の信頼される情報源のモニタリング結果に基づき、組織の廃業が確認された場合や、データスペースの参加資格の見直しに基づいて参加資格喪失が確定した場合などは、データスペース運用者起点で失効を登録する。
- (3) 失効情報の登録：(ウ)**  
データスペース運用者は、参加者もしくは運用者起点で失効情報の登録を行う。この失効情報は、第三者が検証可能であることが求められるため、VCのステータス参照やCRL、OCSPを通じて検証時点の有効性確認を可能にするべき。

## 属性情報の変更

- On-Boarding時に確認した組織や組織内個人の属性(例として商号や、組織内個人の部署名変更など)は時間の経過とともに変化する。
- 当該属性がeシールやVCの記載事項である場合は、記載されているeシールやVCの利用を中止するとともに、新たな属性を確認したうえで新たなeシールやVCが発行されなければならない。

- データスペース運用者のトラスト管理機能は、データスペースエコシステムにおいて参加者間のトラストを構築・維持するための中心的な基盤であり、データの公正かつセキュアな利活用を保証する重要な役割を担う。
- 単なるデータ交換プラットフォームではなく、信頼の起点を提供し、参加者の身元確認、資格・属性管理、コンプライアンスの準拠確認などを一元的に管理する中核的インフラとして機能する。

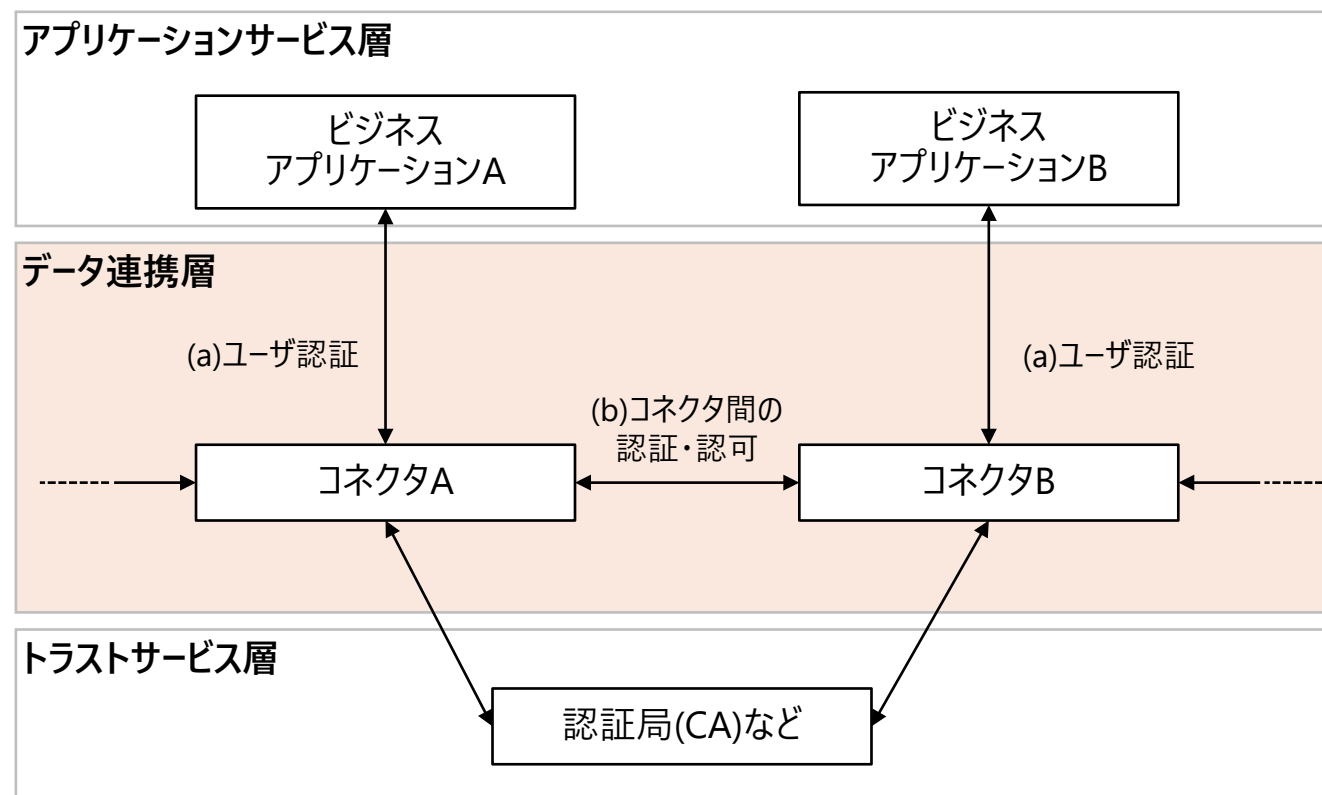


#	内容
(ア)	アイデンティティ管理が、データスペース参加者のOn-Boardingの結果として、参加者のアイデンティティを証明するVC（データスペース運用者が定めた形式）を提供する
(イ)	メンバーシップ管理が、データスペース参加者から上記（ア）のVC等を含むVPを受信する
(ウ)	レジストリに、上記（イ）のVPに含まれる各VCのトラストアンカーが登録されていることを確認する
(エ)	メンバーシップ管理が、データスペース参加者にメンバーシップ資格を証明するVCを発行する

データスペース運用者のトラスト管理機能は(ア)～(エ)を担当する。

※データスペース運用者のトラスト管理の様々な機能と役割を簡潔に表現するため、特に重要な側面を抽出したものであり、実際の構成や詳細な役割は、データスペースの特性に応じて多岐にわたる。

- コネクタの認証として、(a)コネクタへのユーザ認証および(b)コネクタ間の認証・認可およびが重要である。
  - (b)コネクタへのユーザ認証：データスペースは複数の事業者が参加するため、各参加者が他者のユーザ認証に依存するため、**AALを組織横断的に高いレベルに設定することが有効**
  - (a)コネクタ間の認証・認可：単に暗号化するだけでなく「相手が正しい組織であること」を担保する仕組みが必要であり、**mTLSなどが有効**



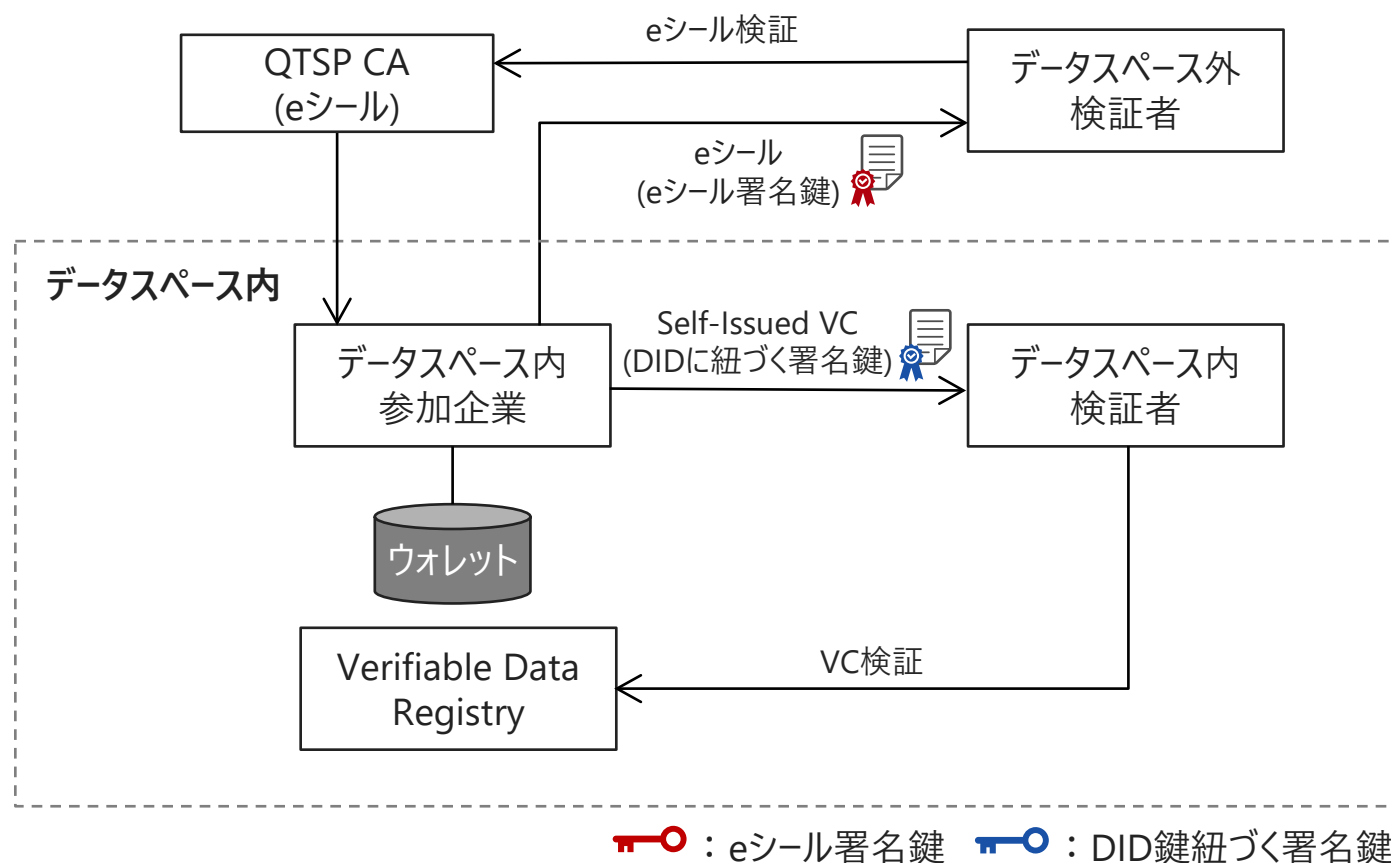
## 署名鍵の使い分け

メンバーシップ管理

アクセス認証・認可

データ真正性確保

- DIDに紐づく署名鍵およびeシールに紐づく署名鍵は用途に応じて使い分ける必要がある。
  - eシール (X.509, CA) : 外部の第三者が検証する用途に適する。
  - VC (DID, VDR) : 属性認可やプライバシー配慮に適する。
- 「使い分け」を前提に、相互運用可能なエコシステムを実現することがトラストの担保されたデータのやり取りに寄与する。



データスペース内でのやりとりする製品情報においては、データの署名にDIDに紐づく署名鍵を活用する。  
 ➔ データスペース内の検証者は、データスペース内のVDRから検証情報を取得することで、VCの署名検証をすることができる。

データスペース内でやりとりした製品情報のデータをデータスペース外に提示するときは、データの署名に参加企業のeシール署名鍵を利用する。  
 ➔ データスペース外の検証者は発行元認証局や失効確認を行うことで、eシールの署名検証ができる。



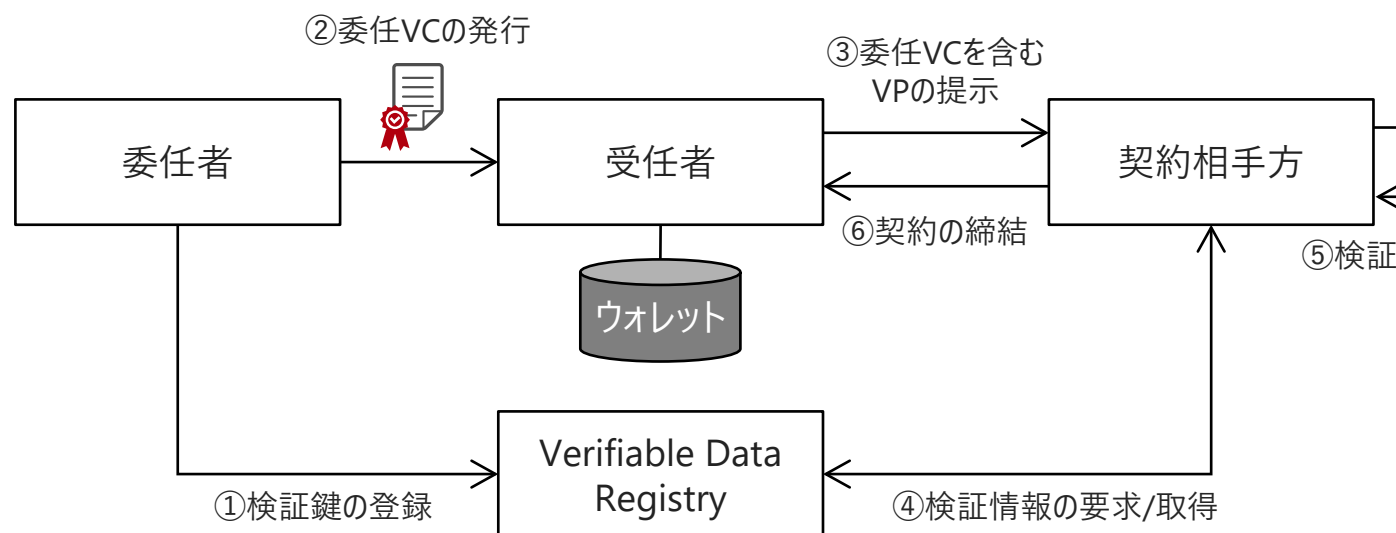
データスペース内外の検証者のニーズに合わせた柔軟な署名鍵の選択を実現し、トラストの担保されたやり取りを実現できる

- データスペースにおいては、必ずしも「データの主体本人」がすべての操作をするわけではない。
- 誰がどのデータにアクセスできるのか、アクセス権を誰に委任できるのかを明確にすることで、不正利用や責任のあいまいさを防ぐ。
- データスペースにおける委任は、VCを活用することで実現できる。

## データスペースにおけるVCを活用した委任の例

委任VC発行者	発行者の要件	内容
委任者	—	委任者が電子委任状を受任者に発行する
データスペース運用者	QTSP相当の発行機関	データスペース運用者のトラスト管理機能が電子委任状取扱事業者としての役割を負い、電子委任状を受任者に発行する

## 委任VC発行者が「委任者」の例



#	内容
① On-Boarding	<ul style="list-style-type: none"> <li>委任者は受任者に代理権を授与する。</li> <li>委任者はデータスペース運用者に委任VCの発行申請を行う。</li> <li>データスペース運用者は検証鍵をVDRに登録する。</li> </ul>
② On-Boarding	データスペース運用者は自身が署名した委任VCを受任者に発行する。
③ On-Going	受任者は契約相手方に委任VCを含むVPを提示する。
④ On-Going	契約相手方はVDRに検証情報を要求し、取得する。
⑤ On-Going	契約相手方は委任VCの検証を行う。
⑥ On-Going	契約相手方は受任者と契約の締結を行う。

1. データスペースにおけるトラストの概要
2. 欧州の取り組み：データ流通基盤の制度設計とトラスト関連のこれまでの歩み
3. データスペースの分類とトラスト要件
4. データスペースで必要とされるトラスト技術
5. データスペースへのトラストの実装と運用
- 6. データスペースにおけるトラストの課題と展望**
7. あとがき

## 課題と展望：技術と体制整備

現実的には、**技術混在の状態**で進めていかななくてはならない。諸体制の整備とロードマップ整備が必要。また、日本として「信頼できる情報源」を含むトラストフレームワーク構築が求められる。

### データ管理

- データ主権の観点からは「分散型」が理想的だが、当面の導入ハードルが高い
- 全ライフサイクルにわたるインテグリティ確保
- 特に中小企業でのセキュリティレベルの維持が困難
- データ取引前後の信用確認や紛争解決の基盤が必要

- 当面の「連邦型/ハイブリッド型」の導入と長期的ロードマップの策定
- 全ライフサイクルに亘る運用ルール・技術仕様の策定
- セキュリティ確保とガバナンスルール整備
- ログ（証跡）を担保する技術基盤の整備

### フレームワーク トラスト

- 適切なトラストレベル（IAL/AAL）の合意がない
- トラストリストの未整備
- 法人に対する信頼できる情報源が未整備
- 特に法人に対する欧州のデジタルクリアリングハウスに対応する国内の取り組みが未確定

- トラスト認定の仕組みと認証機関の整備
- 国内におけるトラストリストの整備
- 幅広く適用可能な法人ID体系の整備
- 官民連携して、「信頼できる情報源」+「ノータリー」他をあわせた「トラストフレームワーク」構築

### 認証・検証

- ID/パスワード、デジタル証明書、VCなどが混在
- 認証や検証の基準が未定義だったり、分かりにくかったりする
- エンドツーエンドでの認証・検証の統合が必要
- 検証プロセスの透明性確保

- データスペース内での統一的な運用ルール策定
- 認証・検証の整合性を確保する実装ガイドライン整備
- プロセス全体の透明性と説明責任の明確化

どこを共通化（標準化）し、どこを個別最適化するか検討し、業界間、国際間の相互承認を推進する必要がある。  
 特に国際対応は国家的課題である。

## 標準化

- 多様なトラスト手法の混在
- データの信頼度やアシュアランス・レベルが都度検討になっている
- 「技術」と「組織・法律」の標準化は必須だが未完成
- 「運用ルール」や「紛争解決」などのルールは遅れがち
- 検証やアシュアランス・レベルの国際統合が必要

- 技術的トラスト（AAL整合、検証内容・手順、透明性確保）、運用の標準化を国際標準を活用して推進。特に国内でのVC発行基準のルール整備
- アシュアランスレベルについての国内合意形成
- 運用組織のありかた、法的位置付けや紛争解決メカニズムの法的整備
- 既存国際標準への適合と国際標準提案

## 相互承認

- サプライチェーンや循環経済などの実現には、データスペース間の相互承認が必須だが、現状、データスペース間の差が大きい
- 「信頼できる情報源」の標準化は相互承認の前提
- 認証レベルの整合、検証の共通化、プロセスの透明性確保が必要
- 現実課題として、先行する欧州データスペースとの相互承認が未完成

- 異なるデータスペース間での相互承認検討は必須
- パブリックトラストを活用した、信頼できる情報源とIALの標準化
- データ交換を実現するためのデータ連携層相互承認
- ガバナンス/マネジメント体制の相互承認
- 欧州規制対応などで日本が不利にならないためのルール策定への関与と国内基盤強化

現実的課題対応のためには経済性への配慮が不可欠である。  
既にデータスペースの試みは始まっており、成果の反映と更なる発展を推進する。

## 標準化

- コストとトラストの最適バランスの確立

- 導入運用コストの解決支援（特に中小企業）
- トラストレベルのユースケース別最適化
- 運用支援、制度的支援、ロードマップ作成

## 試み

- ウラノス・エコシステム（経産省主導）
  - 蓄電池・プラスチック・建材・家電等でデータ連携と安全性/相互運用性を目指す
- DPPへの適用
  - PLA-NETJ、ABtCでCFP可視化/共有、秘密計算等の高度プライバシー保護も検討
- 国際連携実証
  - 事例1：ウラノス×Catena-X（EVバッテリーCFP交換、中間層で相互交換）
  - 事例2：IMX（PCF等の交換、データ主権・ポリシー制御・DID/VCによる相互認証）

1. データスペースにおけるトラストの概要
2. 欧州の取り組み：データ流通基盤の制度設計とトラスト関連のこれまでの歩み
3. データスペースの分類とトラスト要件
4. データスペースで必要とされるトラスト技術
5. データスペースへのトラストの実装と運用
6. データスペースにおけるトラストの課題と展望
- 7. あとがき**

- デジタル技術を活用したトランスフォーメーション(DX)を推進する上で、様々なステークホルダー間でデータ活用することは必然。  
⇒そのための基盤として、データスペースが注目されており、バッテリーパスポートやデジタルプロダクトパスポートの実現進行中。
- データ流通を担う産業用データスペースの議論が活発化しているが、トラストに関して、実際にデータスペースを構築運用する際の深堀が不十分。
- 本ドキュメントでは、データスペースにおいて期待されるトラストをどう実現するのかをまとめた。  
特に、データスペース上で稼働するアプリケーション、サービスに必要なトラストに関する機能を整理。
- 要求されるトラストに関する機能として、データスペースの参加者やデータコネクタの本人性確認や当人認証、それに基づくアクセス権限の管理やデータの生成元、発信元の証明やデータ自身に対する完全性の確保など様々な機能を整理。
- トラストサービスの国際連携も視野に入れ、欧州での議論なども参照し、国際な同等性確保を実現するための整理も実施。
- 本資料は初版の段階であり、まだまだ不十分なところもあります。今後の改定に向け、忌憚なきご意見をいただけますと幸いです。

# ホワイトペーパー作成委員名簿（所属団体 50 音順、敬称略）

	氏名	所属
委員長	藤城 孝宏	株式会社日立製作所
副委員長	阿部 晋樹	日本電気株式会社
委員	小谷 雅俊	SBIホールディングス株式会社
委員	藤本 守	SBIホールディングス株式会社
委員	柴田 孝一	セイコーソリューションズ株式会社
委員	小田嶋 昭浩	電子認証局会議
委員	西山 晃	電子認証局会議
委員	高橋 一裕	日本電気株式会社
委員	安細 康介	株式会社日立製作所
委員	片山 堅斗	株式会社日立製作所
委員	鈴木 麻奈美	株式会社日立製作所
委員	宮本 大輔	株式会社日立製作所
委員	伊藤 俊輔	富士通株式会社
委員	榊原 宏紀	富士通株式会社
委員	中村 洋介	富士通株式会社



**JDTF**  
JAPAN DIGITAL TRUST FORUM