

# デジタルトラスト協議会

## 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3月19日

デジタルトラスト協議会 トラステッドデジタルID委員会

# 目次

1	データスペースにおけるトラストの概要	5
1.1	データスペースとは何か	5
1.2	欧州の動向と法制度・標準化	6
1.3	データスペースの分類とデジタルトラスト	6
1.4	デジタルトラストの技術	7
1.5	トラストの実装と運用：On-Boarding／On-Going／Off-Boarding	8
1.6	現状の課題と今後の展望	8
1.7	まとめ	9
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	10
2.1	データスペース構築へ	10
2.2	データ関連法制	11
2.3	欧州での標準化と本ドキュメントのスコープ	12
3	データスペースの分類（トラストの観点から）	13
3.1	分散型（非集権型）	13
3.1.1	特徴	13
3.1.2	データとユーザの管理方法	13
3.1.3	必要なトラスト	13
3.1.4	事例：Catena-X	14
3.2	集中型（集権型）	14
3.2.1	特徴	14
3.2.2	データとユーザの管理方法	14
3.2.3	必要なトラスト	14
3.2.4	事例：Google	14
3.3	連邦型	15
3.3.1	特徴	15
3.3.2	データとユーザの管理方法	15
3.3.3	必要なトラスト	15
3.3.4	事例：Ouranos Ecosystem	15
3.4	ハイブリッド型	15
3.4.1	特徴	15
3.4.2	データとユーザの管理方法	16
3.4.3	必要なトラスト	16
3.4.4	事例：PLA-NETJ	16
4	データスペースで必要とされるトラスト技術	17
4.1	データスペースにおけるトラスト管理	17
4.2	トラストアンカー	20
4.2.1	トラストアンカーの役割	20
4.2.2	トラストアンカーの機能	21
4.3	信頼できる情報源	21
4.4	トラステッドリスト	22
4.4.1	トラステッドリストの役割	22
4.4.2	トラステッドリストの機能	23
4.5	電子署名	23

4.6	e シール	23
4.7	タイムスタンプ	24
4.8	VC(Verifiable Credential)・VP(Verifiable Presentation)	24
4.8.1	基本アーキテクチャ	24
4.8.2	データモデル	25
4.8.3	VCに基づく属性ベースのアクセス制御	26
4.8.4	アーキテクチャと処理の例	27
4.8.5	VCのライフサイクル管理	28
4.8.6	Verifiable Data Registry	28
4.8.7	Self-Issued Credential	29
4.8.8	DID (Decentralized Identifier)	29
4.9	Digital Wallet	29
4.10	コネクタ	30
4.11	IAL/AAL	30
4.12	日本における組織に対する実在確認のための識別子	31
5	データスペースへのトラストの実装と運用	33
5.1	全体像	33
5.1.1	データスペースのトラスト	33
5.1.2	三層アーキテクチャ	33
5.2	データスペースの運営	35
5.2.1	On-Boarding	37
5.2.2	On-Going	39
5.2.3	Off-Boarding	42
5.2.4	属性情報の変更	43
5.3	データスペースのトラスト機能	43
5.3.1	IAL・AALの推奨レベル	43
5.3.2	データスペース運用者のトラスト管理機能	43
5.3.3	コネクタ認証のあるべき姿	47
5.3.4	権限管理	48
5.3.5	データスペース共通サービスのトラスト	52
5.3.6	トラストサービス自体の認証・監査	52
6	データスペースにおけるトラストの課題と展望	53
6.1	データ管理	53
6.1.1	現状へ対応するアーキテクチャ	53
6.1.2	インテグリティ	53
6.1.3	参加者のセキュリティ確保とガバナンス	53
6.1.4	ログ確保	54
6.2	データスペースのトラストフレームワーク	54
6.2.1	トラストレベル	54
6.2.2	信頼できる情報源	54
6.3	認証・検証	55
6.3.1	認証技術の混在と統一化	55
6.3.2	検証プロセスの透明性	55
6.4	標準化	55
6.4.1	技術と運用の標準化	55
6.4.2	アシュアランス・レベルの標準化	56

6.4.3 組織・法律の標準化 .....	56
6.4.4 国際標準との整合性 .....	56
6.5 相互承認.....	56
6.5.1 トラストサービス層の相互承認.....	56
6.5.2 データ連携層の相互承認 .....	57
6.5.3 アプリケーションサービス層の相互承認 .....	57
6.5.4 国際相互承認と日本の戦略.....	57
6.6 経済性 .....	58
6.6.1 導入コストと維持管理コスト .....	58
6.6.2 経済性とトラストレベルのバランス .....	58
6.6.3 運用負担と ROI（投資対効果） .....	58
6.7 具体的な試み.....	58
6.7.1 ODS(Open Data Spaces)エコシステム .....	58
6.7.2 DPP（デジタル・プロダクト・パスポート）への適用 .....	58
6.7.3 国際連携実証 .....	59
7 結語	60
8 参考資料	61
付録	62
A 欧州の既存例 .....	62
A.1 トラストアンカー.....	62
A.2 トラストドリスト .....	63
A.3 デジタルクリアリングハウス.....	64
A.3.1 デジタルクリアリングハウスの役割 .....	64
A.3.2 デジタルクリアリングハウスの機能 .....	65
A.3.3 具体的動作.....	65

# 1 データスペースにおけるトラストの概要

本ドキュメントは、「これからデータスペースの構築・運用を行う人」に対して、データスペースの概要とデジタルトラスト技術の必要性、デジタルトラスト技術の概要と用法、今後の課題について解説するものである。

第1章でデータスペースの概要、第2章で欧州先行事例の紹介、第3章でデータスペースの分類、第4章で個別のデジタルトラスト技術、第5章でトラスト技術の実装と運用、第6章で今後の課題について説明する。1～3章でデータスペースを概観し、4、5章で具体的なトラスト技術とその実装方法を理解して頂きたい。

データスペースに必要なデジタルトラスト技術は規模や目的によって異なる。この点の理解の助けとなるようにも記載を行っている。

## 1.1 データスペースとは何か

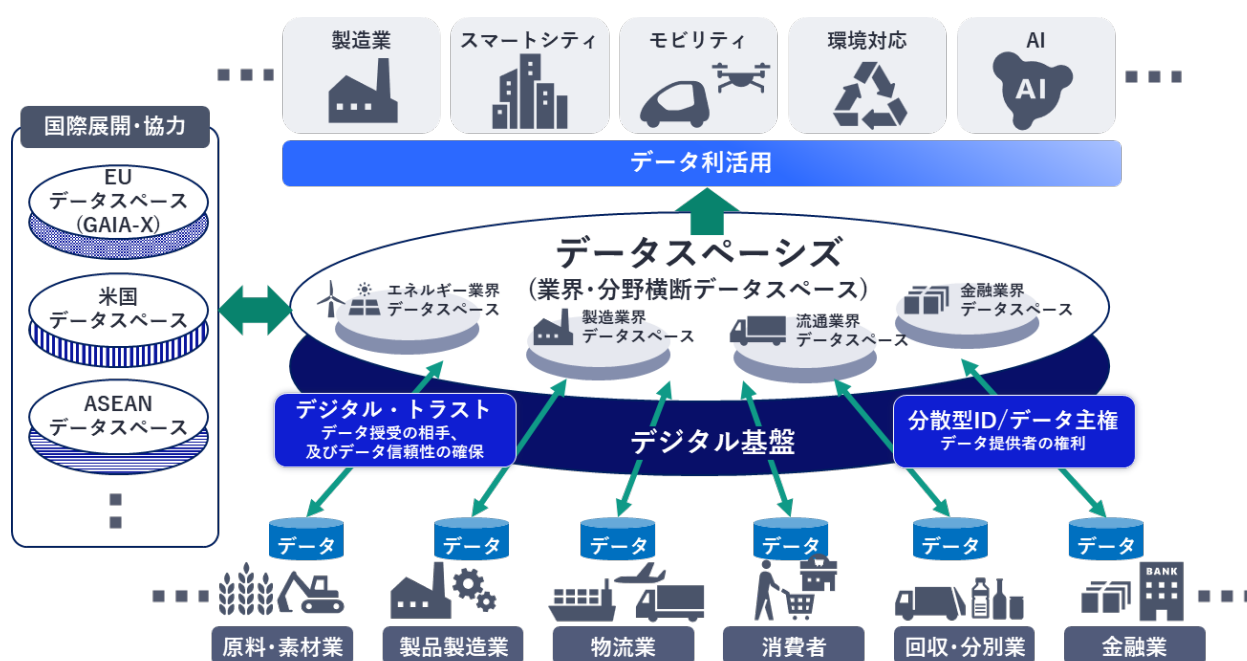


図 1-1 データスペースとは

データスペースとは、共通のガバナンスフレームワークに基づき、複数の参加者が安全かつ信頼性高くデータを共有できる分散型エコシステムである。データ主権（データ提供者が自らのデータ利用方法をコントロールできる権利）を維持しつつ、社会・産業の変革を支える基盤として注目されている。欧州では Catena-X、日本では DSA の DATA-EX や経産省のウラノス・データスペースなどが代表例である。

データスペースの運営には「トラスト（信頼）」が不可欠である。ここでトラストは、参加者や提供データの正当性・真正性が保証され、データスペース内で安心してデータ交換できる状態。また、その保証のための制度・技術的仕組みのことを指す。不正アクセスや誤用、コンプライアンス違反を防ぎ、データ主権を守るためには、技術的・法的なトラストの保証が必要である。トラストがなければ、データ所有者の参加が妨げられ、データ利活用の範囲が限定される。特に、炭素国境調整措置 Carbon Border Adjustment Mechanism[CBAM]やデジタル製品パスポート Digital Product Passport[DPP]など国際規制対応のためには、国際基準に準拠したデジタルトラストを確保する仕組みが必須である。

## 1.2 欧州の動向と法制度・標準化

データスペース構築が最も進んでいるのは欧州である。欧州委員会は「欧州データ戦略」を策定し、域内のデータの自由な流通を促進し、価値創造に結びつけるための統合的な枠組みである「データ単一市場」の構築を進めている。欧州データ戦略はデータ法[Data Act]とデータガバナンス法[Data Governance Act : DGA]から構成されており、データ法はデータの相互運用性とポータビリティを法的に義務化し、データガバナンス法は信頼と中立性を担保する制度基盤を提供する。両法は技術的・制度的に補完し合い、国際連携や越境データ流通の基盤となる。

データスペースの標準化活動は IDSA (International Data Spaces Association) が主導し、Eclipse Dataspace Working Group や ISO/IEC などと連携して進めている。これにより、データスペース間の相互運用性や共通基盤の整備が進みつつある。

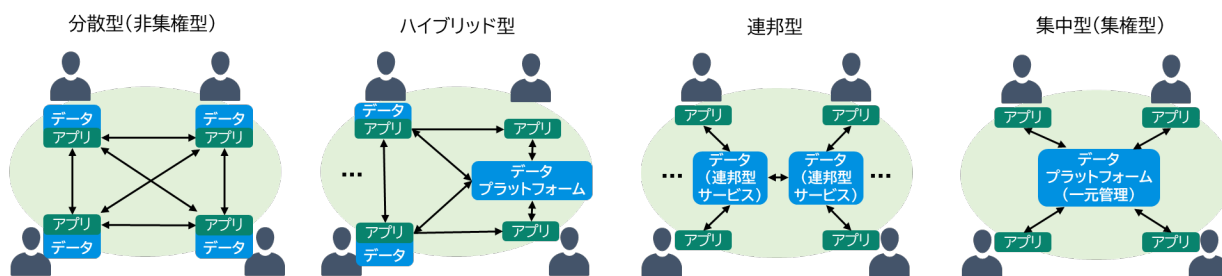
デジタルトラストに関しては、2024年3月に欧州議会により採択された eIDAS の改正案、eIDAS 2 (2025年10月時点で未施行) の中で全欧州市民が利用可能な eID の枠組みである EU Digital Identity Wallet の整備が織り込まれ、個人、法人がオンライン認証に利用できる PID (Person Identification Data : 個人ないし法人を識別するためのデータ) や EAA (Electronic Attestations of Attributes : 電子属性証明) などが定められている。

欧州データスペースの取り組みについては2章で概観し、関連情報を付録に記載する。

## 1.3 データスペースの分類とデジタルトラスト

本ドキュメントでは必要な技術や管理手法の観点からデータスペースを4分類して解説する。

- **分散型**：各参加者がデータ主権を維持し、相互認証やアクセス制御を自ら担いデータのトラストを確保する。セキュリティ事故の影響範囲が限定されるが、各参加者の運用負担が大きい。例：Catena-X。
- **ハイブリッド型**：分散型を基本とし、参加者が自身でデータを管理することもプラットフォームに管理させることもできる。認証・認可のトラスト管理は自身で行う。多様な業態や規模の参加者を受け入れやすい。例：PLA-NETJ。
- **連邦型**：サービス提供者がデータ管理や流通を代行し、参加者の負担を軽減する。サービス提供者がデータのトラストを各参加者に提供し、各参加者がトラストなデータを利用し合う。多様な参加者の包摂性と拡張性を両立する。例：Ouranos Ecosystem
- **集中型**：プラットフォーム運営主体がデータ管理・認証・認可を一元的に担い、データのトラストを確保する。各参加者の運用負担は小さいが、中央サーバ障害時のリスクが高く、データ主権の維持も部分的なものとなる。例：Google



	分散型	ハイブリッド	連邦型	集中型
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(eシール、タイムスタンプ)			(運営者責任)
トラストアンカー	トラステッドリスト 認証IDプロバイダー			(運営者責任)
運用支援	クリアリングハウス Digital Wallet 証跡管理 認定コネクタ	(運営者責任) クリアリングハウス Digital Wallet 証跡管理 認定コネクタ	(運営者責任)	(運営者責任)

図 1-2 データスペースの分類

4 種類のデータスペースと、それぞれについての特徴、データ・ユーザの管理方法、必要なトラスト、事例を 3 章で解説する。

## 1.4 デジタルトラストの技術

データスペースのデジタルトラストを支えるために様々な技術やフレームワークが開発・実装されている。

- 参加者の実在性の保証
  - **信頼できる情報源:** 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。
  - **トラステッドリスト:** 信頼済みリスト。適格トラストサービス事業者やデータソースなどをまとめた機械可読のリスト。
  - **政府認証 ID プロバイダ:** 個人や組織の身元を公的に証明する信頼性の高い機関。
- データの真正性・参加者の本人性の保証
  - **トラストアンカー:** デジタルトラストの信頼の連鎖(Chain of Trust)の起点、または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もの。認証局やトラステッドリストに掲載されているエンティティ。
  - **電子署名:** 自然人が管理している署名鍵によるデジタル署名措置。
  - **eシール:** 組織が管理している署名鍵によるデジタル署名データ。
  - **タイムスタンプ:** 対象文書に、第三者であるタイムスタンプ局が管理する信頼のおける時刻を付与し、タイムスタンプ局の署名鍵によってデジタル署名されたトークン。
  - **EAA:** 個人、法人がオンライン認証の際に自らの属性の証明に利用できる技術。EU では、公的機関が発行する Public EAA (P-EAA)、適格認定を受けた機関が発行する Qualified EAA (Q-EAA)、そのいずれにも該当しない EAA がある。データフォーマットは VC または mDL が利用でき、P-EAA 及び Q-EAA は、適格トラストサービス事業者が発行する適格電子証明書に紐

づく署名鍵により電子署名を付与することが eIDAS2 Annex V、VII にて定められている。

- **VC (Verifiable Credential) 型認証**：W3C 標準に準拠し、改ざん防止・真正性検証・プライバシー保護を実現する技術。
  - **Self-Issued Credential**：発行者自身が発行する VC。内部利用に適する。
  - **Decentralized ID**：特定組織や中央機関に依存することなく、個人やモノが自身で管理できる永続的でグローバルに一意的な識別子。
- **トラストを守り、運用するための技術**
  - **データスペース運用者のトラスト管理機能**：メンバーシップ管理とトラストアンカーの管理。
  - **Digital Wallet**：ID やデータを安全に管理・利用するためのツール。
  - **証跡管理**：データがいつ、どこで、誰によって、どのように作成、変更、共有されたかの履歴。
  - **Verifiable Data Registry**：DID に関連する情報、特に検証鍵やサービスエンドポイント、失効情報などを安全に登録する分散型データベース。
  - **認定コネクタ**：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。

これらのデータスペースのトラストを支える主要な技術・枠組みとそれぞれの役割について、4章で解説する。

## 1.5 トラストの実装と運用：On-Boarding／On-Going／Off-Boarding

データスペースを実用化するためには、どのような技術をどのように実装・運用するかについても検討しなくてはならない。データスペースの運用では参加者の加入時 (On-Boarding)、活動中 (On-Going)、脱退や資格喪失 (Off-Boarding) の3フェーズがある。

- **On-Boarding**：新規参加者がデータスペースに加入する際の手続き。法人・個人の実在性、権限、資格を確認し、電子的な会員証 (VC や e シール等) を発行する。識別子や証明書の信頼性が重視される。
  - **On-Going**：データスペース内で活動している際の手続き。会員証や e シールの検証、組織・個人の実在性の継続確認、検証データの管理・公開、コネクタの認証などを行う。継続的な信頼維持が求められる。
  - **Off-Boarding**：参加者がデータスペースから退会する際の手続き。参加資格喪失時の会員証無効化や、リアルタイムな反映・通知を行う。停止・削除プロセスの明確化と証跡管理が重要。
- 加えて、実用化の際にはトラストの基準、認証、権限管理や委任・代行の仕組みも必要である。

データスペースの実装と運用に関わる事項について、第5章で具体的に説明する。

## 1.6 現状の課題と今後の展望

将来あるべきデータスペースに向けて、データ管理、トラストフレームワーク、認証・検証、標準化、相互承認、経済性など様々な課題や留意点が残っている。

こうした未解決の課題、今後対応していかなくてはならない課題とそれらの解決を目指した具体的な試みについて、6章で紹介する。

## 1.7 まとめ

データスペースは、データの主権と信頼を両立させ、多様な参加者が安全・効率的にデータを共有・活用できる新たな社会インフラである。データスペースを構築・運用する者は、特に重要となるデジタルトラスト技術についてデータスペースの目的や規模、利用範囲などを踏まえて、検討・実装・運用していかなくてはならない。ぜひ本ドキュメントをガイドラインとして活用してほしい。

## 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

本章では、欧州におけるデータスペース構築の取り組みについて、法制度、技術的枠組み、標準化活動、関連プロジェクト等がどのように組み合わせられて歩んできたかを整理し紹介する。特定の制度モデルを前提とするものではなく、制度設計と技術実装の関係性に着目する。

### 2.1 データスペース構築へ

EU は 2020 年に「欧州データ戦略」を策定し、分野横断で利用可能な欧州共通データ空間の構築を目標とした。この基盤整備のため、共通ビルディングブロックを開発するオープンソースプロジェクト Simpl が進行している。

これと並行して、IDSA の IDS、Gaia-X、Catena-X など、加盟国および民間による多様なデータスペース関連団体・プロジェクトが立ち上がった。Gaia-X は現在、複数のデータスペースに共通するトラストフレームワークの提供者として位置付けられている。他方でデータスペース関連の標準化は主に IDSA が担い、IDS-RAM などの参照アーキテクチャを提示している。2021 年には、BDVA、IDSA、FIWARE、Gaia-X による DSBA (Data Spaces Business Alliance) が発足し、分野横断の共通アーキテクチャや最小構成要素を示す文書を 2023 年に公表するなど、技術的統合に向けた活動が進んでいる。一方で、欧州域内ではデータスペースが想像以上に多様化するという課題が生じたため、欧州委員会は 2022 年に DSSC (Data Spaces Support Centre) を設立し、データスペース間の共通要素と独自要素を整理し、共通基盤としての指針を改めて提示していくこととなった。

これらの「欧州データ戦略」に基づく欧州委員会、各加盟国、民間の動向は、先行する欧州議会による各種データ関連法制に根ざしており、eID やトラストサービスなどを定める eIDAS 規則もその基盤の一つとなっている。とりわけ、デジタルトラスト関連では、eIDAS 2.0 に基づく European Digital Identity Wallet (EUDIW) の導入が進められ、個人・法人を識別する PID や電子属性証明 (EAA) を扱う技術枠組みが整備されつつある。

このように、制度設計と技術的枠組みが連携することで、デジタル単一市場構想のもと欧州のデータスペースにおけるトラストの基盤整備が段階的に進められている。

	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		データガバナンス法成立 Data Spaces Support Centre (DSSC)設立	データガバナンス法施行開始 EU Data Act 成立	eIDAS 2.0制定	EU Data Act 施行開始
International Data Spaces Association (IDSA)	Industrial Data Space e.V.設立	Reference Architecture Mode: 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				

図 2-1 欧州におけるデータスペース関連規則と関連団体の主な動向

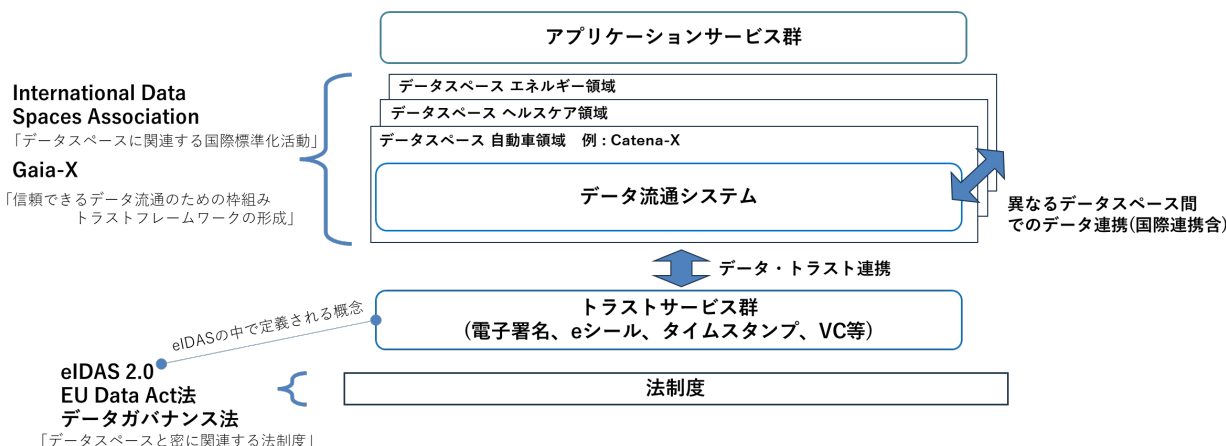


図 2-2 データスペースのエコシステムと、主な規則・団体の対応

## 2.2 データ関連法制

EU のデータスペース関連の政策を支える法制度として、EU データ法(Data Act) と EU データガバナンス法(Data Governance Act: DGA) の 2 本柱が存在する。

EU データ法は 技術的な相互運用性とデータポータビリティを法的に義務付ける法律であり、クラウドサービスやデータ処理基盤に対して、標準 API・共通データ形式・メタデータ語彙などの採用を求める。

一方、EU データガバナンス法 は 信頼性と中立性を担保したデータ取引市場のガバナンスを設計する法律であり、データ仲介者の登録制度や公的データ再利用の仕組みを整備する。

両制度の役割分担として下記のような補完関係が存在しており、下表の通り整理できる。

- ・ EU データ法：相互運用性を前提とした具体的な技術仕様の順守を義務化する。
- ・ EU データガバナンス法：データ共有における「誰を信頼できるか」という制度的基盤を提供する。

	EU データ法(Data Act)	EU データガバナンス法 (DGA)
目的	技術的な相互運用性の強制とデータアクセス権の公正化	信頼あるデータ取引の制度設計とガバナンス確立
主要な項目	API やデータ仕様の標準準拠義務、データポータビリティの権利	データ仲介者の登録制、トラスト機構の定義
域外データ連携に向けて	相互運用性を前提とした技術的実装を義務化	連携相手の信頼性(出所、権限)を判断するガバナンス基盤を提供

表 2-1 EU データ法と EU データガバナンス法

この 2 法により、EU は域外との連携（相互認証）も視野に入れた際に必要な制度的・技術的条件を法的に定義した。これは、EU のデジタルトラストの根幹である eIDAS 規則(eID とトラストサービスの法的枠組み) によるトラストアンカーと組み合わせることで、Catena-X のような具体的なユースケースにおける国際的な相互認証の枠組み構築を後押ししている。

## 2.3 欧州での標準化と本ドキュメントのスコープ

欧州のデータスペース関連の標準化を担っている IDSA は下記のスコープで活動している。なお、本ドキュメントでは、第2象限（Identity & Trust）に関する標準化動向を中心に記載する。

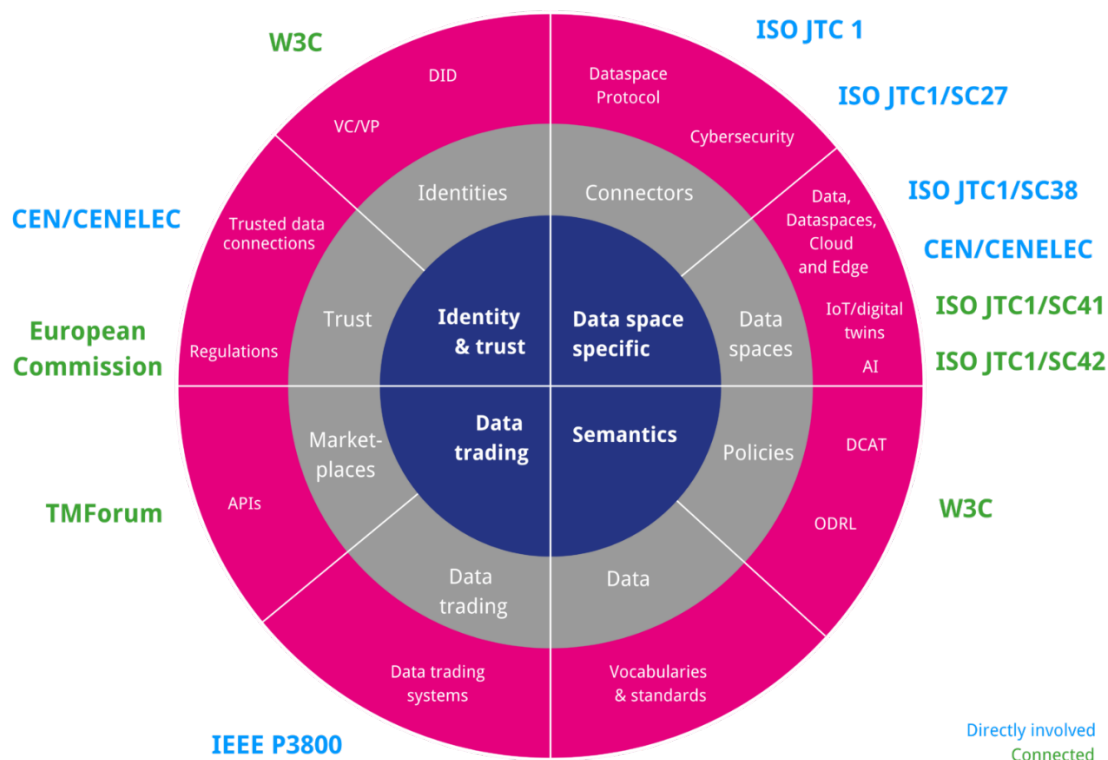


図 2-3 IDSA engagement in European and International Standardization bodies<sup>1</sup>

図中、Directly involved として青字で記載されている活動に直接参加して、データスペースに早期に必要な標準化をけん引している。

以下に主な動きを記載する。

- ・ Dataspace Protocol<sup>2</sup>

Eclipse Dataspace Working Group で標準化し、ISO/IEC Joint Technical Committee 1 に PAS（公開仕様書）提案の予定。

- ・ Dataspace concepts and characteristics<sup>3</sup>

ISO/IEC DIS 20151 Information technology — Cloud computing and distributed platforms — Dataspace concepts and characteristics

- ・ JTC25<sup>4</sup>

CEN と CENELEC がデータ管理、データスペース、クラウド、エッジに関する新しい専門委員会、JTC 25 を設立

<sup>1</sup> <https://internationaldataspaces.org/why/international-standards/>

<sup>2</sup> <https://dataspace.eclipse.org/projects/>

<sup>3</sup> [https://internationaldataspaces.org/iso-iec-20151-reaches\\_dis/](https://internationaldataspaces.org/iso-iec-20151-reaches_dis/)

<sup>4</sup> <https://webdesk.jsa.or.jp/common/W10K0620/?id=1315>

### 3 データスペースの分類（トラストの観点から）

データスペースは、各参加者がデータオーナーとしてデータ主権を維持しながら、互いにデータを提供・利用する枠組みである。これによりデータ利活用の促進、データ主権の維持、企業の秘密保持を実現できる。長期的にはデータスペースは分散型に集約されると思われるが、移行期には現実的な対応が必要になり、様々な形態が発生する。以下では、整理のため、主に流れるデータのトラスト確保の観点から見たデータスペースの分類を分散型、集中型、連邦型、ハイブリッド型に分類し、説明する。共通して必要とされるデジタルトラストと、データ管理の方法の違いから異なってくるデジタルトラストがある。

分散型(非集権型)		集中型(集権型)		連邦型		ハイブリッド型	
データ管理	分散型	データ管理	集中型	データ管理	部分集中	データ管理	分散/部分集中ハイブリッド
ユーザ認証	分散型 (DID/VC)	ユーザ認証	集中型 (ID/パスワード)	ユーザ認証	集中型 (ID/パスワード)	ユーザ認証	分散/集中ハイブリッド
データ主権	あり	データ主権	なし	データ主権	限定的	データ主権	可能 (選択可能)

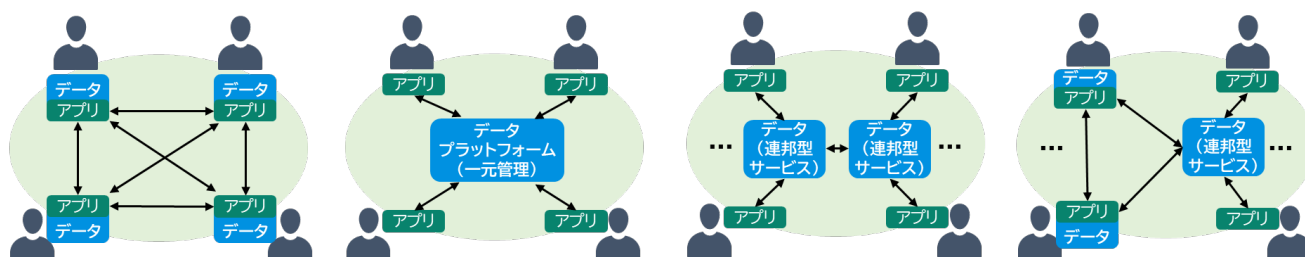


図 3-1 データスペースの分類

#### 3.1 分散型（非集権型）

##### 3.1.1 特徴

分散型では、複数の組織が互いのデジタルトラストを検証しながらデータを流通させる。参加者同士の相互認証、データの真正性の確保、アクセス制御、セキュリティ確保、データ主権の確保などは原則として参加者が各自で確保し、データ流通を行う都度参加者が検証し、実行することになる。

セキュリティ事故があっても影響範囲を限定することができるが、各ノードに運用負担は大きい。

実用上、相互運用性確保や規制対応のためにデータスペースの運営主体は必要となり、運営主体がデータスペースの参加要件や基準・標準の設定を行う。

##### 3.1.2 データとユーザの管理方法

データは各参加者が個別に管理し、原則として共通データベースのようなものはない。データ流通の実施も運営主体が関与せず分散的に行われる。データ本体も運営主体ではなく各参加者が管理する。データ主権の保持も、データ流通を行う際に相手のデジタルトラストを確認したうえで各参加者の責任において実行される。

ユーザ資格の発行は各参加者がプラットフォームの規定に従って認証者から資格を獲得することで行われる。発行された資格は各ユーザが管理し、データ流通の際に参加者同士で相互に認証を行う。

##### 3.1.3 必要なトラスト

分散型では、参加者もしくは参加者の身元を保証する機関が信頼できる情報源となる。また、参加者がデータスペースに参加する要件を満たしていることは運営主体が保証する（On-Boarding）。

参加者間の相互認証を実現するための認証方法も必要となる。（On-Going）これは VC 型が望ましい。

運営主体は運営者自体あるいは公的機関が信頼できる情報源となる。

参加者が預けるデータは参加者が電子署名・e シールで保証する。

運営主体が発行するデータは電子署名・eシールで運営主体が保証する。

### 3.1.4 事例：Catena-X<sup>5</sup>

Catena-X は、自動車産業の規制対応（バッテリーパスポート対応、GHG 報告対応、DPP）とサプライチェーンの透明性・効率性の向上を目的とするデータスペースである。

データ主権を IDS コネクタによる制御とデータスペース参加時の資格確認によって保証し、ガバナンスは Catena-X 協会が主導している。

## 3.2 集中型（集権型）

### 3.2.1 特徴

集権型では、データをプラットフォームに記録し、利用者・提供者の管理もプラットフォームが実施する。参加者はプラットフォームを信頼してデータを預け、プラットフォームから提供されるデータを信頼して業務を実施し、規制当局はプラットフォームからの報告データを信頼して企業を監督する。

そのため、プラットフォーム（運営主体）の「信頼」を確保することが重要である。

一般にセキュリティは強固だが、インシデント発生時に認証情報の大量流出等の懸念がある。一方、参加者一人一人がノードを運用する場合に比べて個々の運用負荷は小さく抑えることができる。

プラットフォーム運営主体がトラストを保証する。データ主権とセキュリティに関するビジネスニーズを満たすだけでなく、透明性、トレーサビリティ、データ精度、検証可能性に関するコンプライアンスを満たさなくてはならない。規制対応や標準化対応なども運営主体が中心となって行う。

### 3.2.2 データとユーザの管理方法

データ主権やセキュリティ確保については運営主体が保証し、参加者は運営主体を信頼する。データも運営主体が保存し、利用許可も運営主体が発行する。

ユーザの参加確認、ユーザの認証・認可は運営主体の責任において実行される。ユーザも集中管理され、従来の ID/パスワードによる認証方式が採られることが多い。

### 3.2.3 必要なトラスト

集中型では、運営主体がトラストアンカーを定め、参加者の信頼性は運営主体が On-Boarding、On-Going ともに保証する。

プラットフォーム内にあるデータの非改ざん性は運営主体が保証する。そのため、プラットフォーム自体の強固なセキュリティが重要となる。

参加者が預けるデータの出所・真正性を保証したい場合は、参加者自身が電子署名・eシールなどで保証する。

### 3.2.4 事例：Google

Google 自体はデータスペースではないが、Google のサービスでデータを共有することは多く行われており、これをデータスペースの一種と捉えることはできる。

セキュリティ確保やポリシー設定は運営主体（Google）が行い、参加者はそれを承諾して参加する。データ主権は規約によって認められる範囲に限られ、本来の意味のデータ主権があるわけではない。

---

<sup>5</sup> <https://catena-x.net/>

## 3.3 連邦型

### 3.3.1 特徴

連邦型はウラノス・エコシステムで定義された形態である。分散型は各参加者がデータ流通の運用を自分で行わなければならないため参加者への負荷が大きく、集中型は運営者を一元化するための合意形成やデータを外部に出したくない参加者がいる場合の運用が難しい。そこで、連邦型では分散のコンセプトを維持しつつ、データの管理やデータ流通などデータスペースへの参加に必要な機能をサービス提供者に委託（データスペースサービス）することで、参加者のコストやリソースの負担を小さくしている。

データ流通はコネクタを介して複数のサービス提供者間で実行される。サービス提供者が一社しか存在しない場合は集中型とほぼ同じとなるが、後述するハイブリッド型への対応など、集中型に対して将来拡張性と柔軟性で優っており、これによりデータスペースの参加者の多様化（包摂性）とデータスペースの迅速な拡大が可能となる。

### 3.3.2 データとユーザの管理方法

参加者から見た場合、データ・ユーザの管理方法は集中型と同じとなり、サービス提供者にデータを委ね、サービス提供者が指定した方法で自らの認証を行い、データ流通を行う際の相手の認証・認可はサービス提供者を信用することになる。

データ主権やセキュリティ確保についてはサービス提供者が保証し、データもサービス提供者が保存し、利用許可もサービス提供者が発行する。データのセキュリティや来歴管理もサービス提供者が提供する。

サービス提供者をまたいだ場合、サービス提供者のデータ主権確保やセキュリティ確保、認証・認可についてはサービス提供者同士で確認し合い、参加者はサービス提供者を信頼する形になる。ガバナンスは運営主体が実施する。

### 3.3.3 必要なトラスト

基本的には集中型と同様のトラスト確保が求められ、ガバナンスについては運営主体が責任を負う。

### 3.3.4 事例：Ouranos Ecosystem<sup>6</sup>

Ouranos Ecosystem は連邦型のデータスペースである。ウラノス・エコシステムは「ワンサイズ・フィットオール」のモデルを用いず、各「ドメイン」を分析して設定する。異なるドメインは異なるリスク許容度とトラスト要件を持つからである。

トラスト基盤に必要な機能（ID インフラ、トレーサビリティ基盤、など）のうち、ID インフラに国または地域のデジタルアイデンティティインフラ(gBizID など)を適用することで、迅速なデータスペースの立ち上げを実現する。

## 3.4 ハイブリッド型

### 3.4.1 特徴

目的や手法が明確であり、強い指導力や法的強制力を持って作成されるデータスペースは集中型・分散型・連邦型といったシンプルな構成を持つことができる。

一方で、ボトムアップ的なアプローチを取ったり、複数の目的を調整しながら作成されたりするデータスペースでは、複数の手法を組み合わせた構成が必要になる。例えばコスト的に有利な連邦型をベースとし、外部にデータを出すことが困難な参加者やデータ主権を厳密に維持したい参加者などには分散型を選択可

---

<sup>6</sup> [https://www.meti.go.jp/policy/mono\\_info\\_service/digital\\_architecture/ouranos.html](https://www.meti.go.jp/policy/mono_info_service/digital_architecture/ouranos.html)

能として、その上で一つのデータスペースを構成すれば参加者の多様化（包摂性）とデータスペースの迅速な拡大が可能となる。

ここでは、そうしたデータスペースを「ハイブリッド型」と分類する。

### 3.4.2 データとユーザの管理方法

自分でデータを管理することを選んだ参加者は、自身の認証手続きと相手の認証・認可も自身で行う。自分でデータを管理しないことを選んだ参加者はプラットフォームにデータ管理を委ねプラットフォームが指定した方法で自身の認証を行う。

ハイブリッド型の場合は、データを共有部分に置き利用の認可は分散型で行うケースや、一部のデータを共有部分に置き、一部のデータを自身の管理下に置く構成も可能となる。この場合の調整は運営主体が行う。

### 3.4.3 必要なトラスト

自分でデータを管理する参加者は、分散型参加者としてのデジタルトラストの用意が必要となる。自分でデータを管理しないことを選んだ参加者は、プラットフォームが提供するデジタルトラストを利用する。

構成や要件が様々であるため、トラストの要件や実装も様々なものになる。複数の認証手法、複数のトラストアンカーを持つことがあり、その複数のトラストの相互認証・相互運用性の確保と、差分への対応手法を整理は、運営主体の責任で実施する。

### 3.4.4 事例：PLA-NETJ<sup>7</sup>

SIP 第3期の「サーキュラーエコノミーシステムの構築」プロジェクトで実装している PLA-NETJ は、プラスチック素材に関する DPP を共有するデータスペースである。

回収業者、樹脂のリサイクラー、製造ベンダーだけでなく、AI 分析企業やコンサルティング企業など規模も業態も様々な企業の参加を想定しており、多様な参加者を受け入れる必要がある。特に回収業者は小企業が多く、こうした企業は簡易・安価な手順を好む。一方で大規模ベンダーや AI 分析企業はデータの管理を厳密に行いたい場合が多い。これを両立させ、参加者を広く募るためにハイブリッド型を採用している。

---

<sup>7</sup> [https://www.meti.go.jp/policy/mono\\_info\\_service/digital\\_architecture/ouranos.html](https://www.meti.go.jp/policy/mono_info_service/digital_architecture/ouranos.html)

## 4 データスペースで必要とされるトラスト技術

データスペースの構築・運営において、参加者やデータの正当性・真正性の保証、データ主権の維持、不正や誤用の防止、コンプライアンス遵守を実現し、安心してデータを交換・活用できる環境を実現する「トラスト」は不可欠である。4章ではデータスペースで利用されるトラストサービス（トラスト技術）について、どのような機能があり、どのようなときに使うのかを解説する。

データスペースアーキテクチャ（3章で解説）ごとに必要なトラスト技術は異なる。5章では、トラスト確保の具体的手順を On-boarding（参加時）/On-Going（運用中）/Off-Boarding（脱退時）に分けて解説する。

本章で解説するトラスト技術は大きく3種類に分類できる。

- ・実在性保証：参加者の実在性を保証する「信頼できる情報源」、データスペース内で信頼される情報をまとめた「トラステッドリスト」、身元の公的証明を行う「政府認証 ID プロバイダ」。
- ・真正性保証：信頼の連鎖の起点となる「トラストアンカー」、データの真正性・本人性を保証する「電子署名」、法人による電子署名と位置づけられる「eシール」、時刻証明を行う「タイムスタンプ」、真正性検証が可能な証明書「Verifiable Credential 認証（VC）」。
- ・運用関連：参加者の適格性を管理する「メンバーシップ管理」、ID やデータを安全に保管する「Digital Wallet」、データの作成・変更・共有履歴を記録する「証跡管理」、安全にデータを交換するための「コネクタ」。

本章では、こうしたトラスト技術の概要と、具体的な利用場面・選択のポイントについて解説する。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択しなくてはならない。

### 4.1 データスペースにおけるトラスト管理

4章では、データスペースが提供すべきトラストサービス、すなわちトラストアンカーサービス、ノードリーサービス、認証、電子署名を中心に説明するが、本節では、各サービスの詳細を述べる前にデータスペースにおけるトラスト確保の概要について述べる。

はじめに、データスペースにおけるトラスト管理について述べる。データスペースにおけるトラストアンカーとは、信頼の連鎖（Chain of Trust）の基点、または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決めたものである（詳細：4.2）。データスペースにおけるトラストアンカーは以下2つに大別することができる。

- (1) パブリックなトラストアンカー
- (2) プライベートなトラストアンカー

#### (1) パブリックなトラストアンカー

eシール証明書、サーバ証明書について、それらを発行している認証局（CA）の信頼の拠点はそのルートCAにある。これらのルートCAが担保するトラストは、データスペース内だけでなく、データスペース外の検証者でも検証することができる。ルートCAのように、データスペース外からもトラストを検証可能なトラストアンカーを、本ドキュメントではパブリックなトラストアンカーと定義する。トラステッドリストは、認定認証機関が認めた信頼できるパブリックなトラストアンカーをまとめたリストである。現在、EUやMozilla等の組織が認定認証機関としてトラステッドリストを作成し、公開している（詳細：4.4）。

#### (2) プライベートなトラストアンカー

データスペース内での独自認証局が発行した証明書や Issuer が発行した VC を利用する場合、データスペース内ではトラストを検証可能であるが、データスペース外からはそのトラストを検証することができない。

本ドキュメントでは、このようなトラステッドリストをプライベートなトラステッドリストと定義する<sup>8</sup>。

データスペース運営者は、データスペースにおけるトラステッドリストを事前に定義する。本ドキュメントでは、データスペースにおけるトラステッドリスト、およびその他信頼できるエンティティ等の情報をまとめたリストをデータスペーストラステッドリストと定義する（詳細：4.4）。「図 4-1 データスペースにおけるトラステッドリスト管理」にデータスペーストラステッドリストに基づくデータスペースにおけるトラステッドリスト管理の概要を示す。登録されるトラステッドリストは、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。トラステッドリスト情報として例えば以下が記載される。

- パブリックなトラステッドリスト：他組織により公開されている TL 情報
- プライベートなトラステッドリスト：独自 CA 情報、Issuer 情報

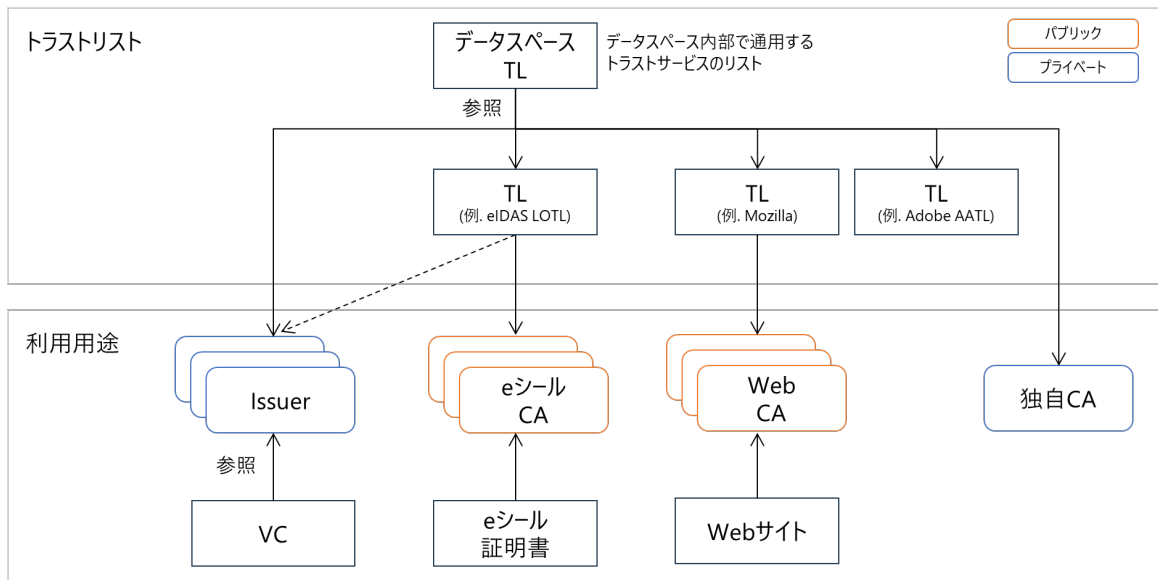


図 4-1 データスペースにおけるトラステッドリスト管理

<sup>8</sup> EU ではトラステッドリストに信頼できる Issuer を含めることを検討している。本ドキュメントではトラステッドリストに記載された Issuer はパブリックなトラステッドリストとして扱う。

続いて、データスペースにおけるパブリックトラストサービスとノータリーサービスの関係について述べる。「図 4-2 データスペースにおけるパブリックトラストサービスとノータリーサービス」にデータスペースにおける各サービスとの関係の概要を示す。ここで、パブリックトラストサービスはデータスペース外からもそのトラストを検証することができるものであり、例えば eIDAS におけるトラストサービスとしての電子署名や eシールがある。ノータリーサービスは、外部の信頼できる情報源（例. 住基台帳、法人登記）からデータスペース参加者の属性情報を取得し、データスペース参加者に対してクレデンシャルの発行を行う（詳細：4.8）。データスペースは、データスペース内の独自 CA の利用や、パブリックトラストサービス、ノータリーサービスの参照を行うことで、データスペース参加者に対してデータ連携におけるトラストを提供する。

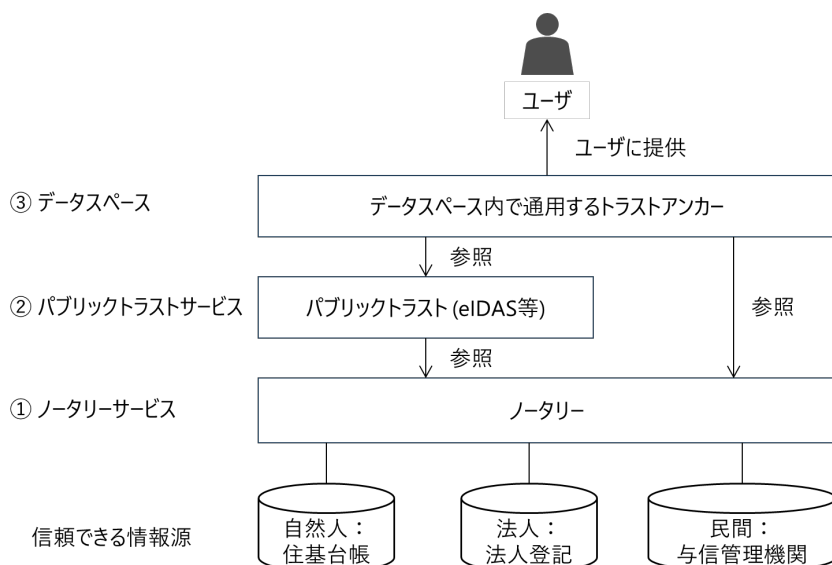


図 4-2 データスペースにおけるパブリックトラストサービスとノータリーサービス

データスペースにおけるトラストアンカーサービス、ノータリーサービス、認証、署名の関係についてメンバーシップ VC の発行を例に説明する。「図 4-3 データスペースのトラスト管理に関わる処理の例：メンバーシップ VC の発行」にメンバーシップ VC の発行に関する処理概要を示す。データスペース参加者に対するメンバーシップ VC の発行は以下手順により行われる。

- (1) データスペース参加者が自己のアイデンティティを証明するためのクレデンシャルの発行をノータリーサービスに対して要求し、ノータリーサービスがクレデンシャルを発行する。
- (2) データスペース参加者がメンバーシップ管理機能に対してメンバーシップ VC 発行を要求する。このとき、データスペース参加者はクレデンシャルを提示して認証を行う。
- (3) メンバーシップ管理機能は、提示されたクレデンシャルのトラストを検証するために、クレデンシャルの発行者がデータスペース TL に登録されていることを確認する。
- (4) (3)でトラストの検証に成功した後、メンバーシップ管理機能はデータスペース参加者にメンバーシップ VC を発行する。このとき、メンバーシップ管理機能は VC の発行者として VC に署名を行う。

このように、データスペースではトラストアンカーサービス、ノータリーサービス、認証、署名が連携することにより、トラストが確保されたデータ連携を実現する。

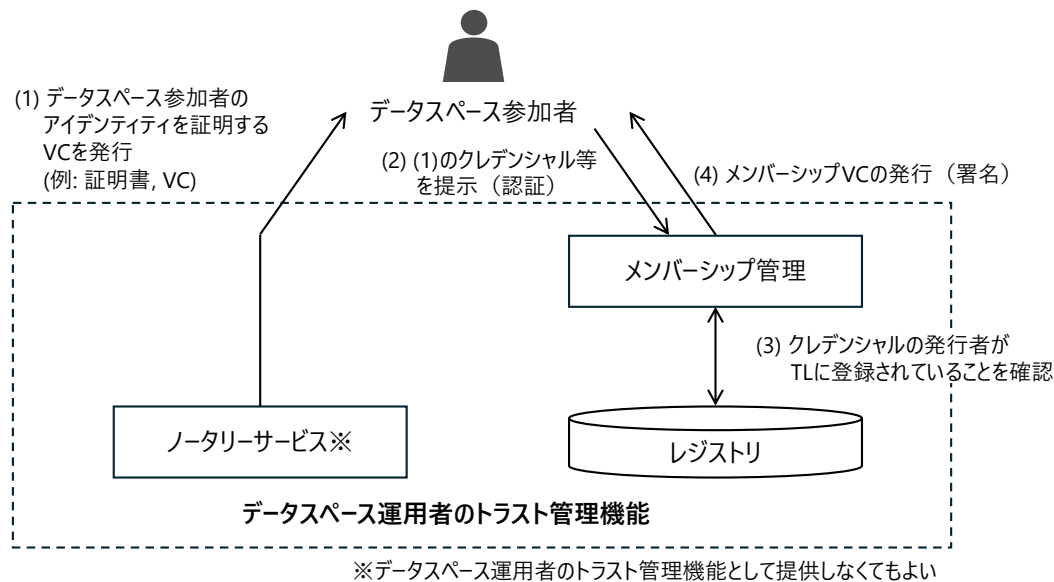


図 4-3 データスペースのトラスト管理に関わる処理の例：メンバーシップ VC の発行

## 4.2 トラストアンカー

### 4.2.1 トラストアンカーの役割

トラストアンカーとは、一般的にデジタルトラストにおける信頼の連鎖（Chain of Trust）の基点、または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ものである（参照:5.3.2）。厳密な定義は文書によって揺れがあるが、トラストアンカーの一般的な例としては、ルート認証局や 4.4 のトラステッドリストに掲載されているエンティティなどが挙げられる。

ここでは、データスペースに焦点をあて、トラストアンカーの定義と役割を欧州の Data Spaces Support Centre を参照して記載する。

トラストアンカーの定義 <sup>9</sup>	信頼が（他のものから）導出されるのではなく、信頼が前提とされている権威あるエンティティ。 各トラストアンカーは、特定の証明範囲に応じて、データスペースのガバナンスオーソリティ（運営主体）によって認定される。
トラストアンカーの役割 <sup>10</sup>	データスペース内のアイデンティティ、データサービス、トランザクションの真正性、完全性、信頼性などのセキュリティを確保すること。

従来の PKI が主に「通信の暗号化」、「ウェブサイトの認証」や「記録の保証」といった特有の範囲の信頼性を扱っていたのに対し、データスペースでは、多種多様なデジタル属性やクレーム（例：参加企業の資格、環境認証など）の信頼性も扱う。属性の信頼性を保証するために、暗号的な真正性の起点となるトラストアンカーだけでなく、その属性情報が「誰によって」「どのような権限で」発行されたのかという「情報の出所」に関する起点といった概念に拡張される。ここでは、前者をトラストアンカー、後者を信頼できる情報源（参

<sup>9</sup> Blueprint v2.0

<https://dssc.eu/space/BVE2/1071252161/Alphabetical+List+of+All+Defined+Terms+in+Blueprint+v2.0>

<sup>10</sup> Trust Framework

<https://dssc.eu/space/BVE2/1071255941/Trust+Framework#3.2.1-Trust-Anchors>

照:4.3) として区別する。具体的に、Gaia-X では、トラストアンカーとは、「図 4-4 Gaia-X システムコンテキスト」の左側にある eIDAS トラストサービスプロバイダー(TSP)と Mozilla CA 証明書リストが該当する。

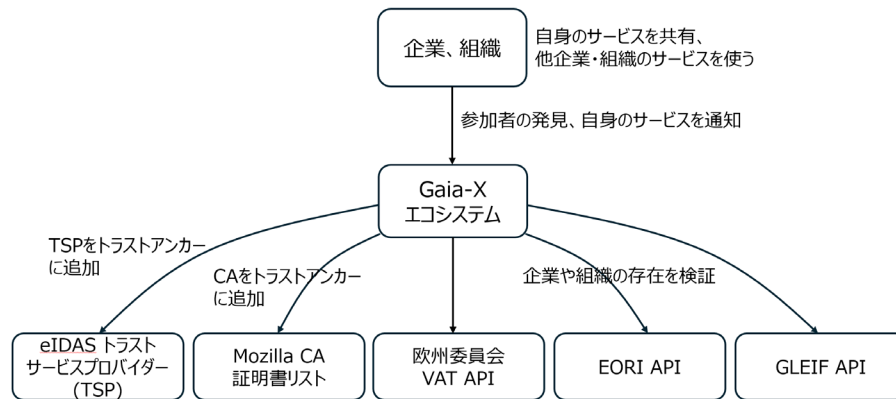


図 4-4 Gaia-X システムコンテキスト

「図 4-4 Gaia-X システムコンテキスト」に示されるように、トラストアンカーと VAT/EORI/GLEIF 等の信頼できる情報源を含めた「エコシステム」によってトラストアンカーマネジメントが実現されている。

## 4.2.2 トラストアンカーの機能

トラストアンカーは、デジタル環境における信頼の連鎖の起点を形成し、その根源的な信頼性によって多岐にわたるトラスト関連機能を提供する。これにより、デジタル証明書の真正性を担保し、安全な暗号化通信やデジタル署名を通じて、改ざん防止、本人性確認、およびシステム全体の信頼性を実現する。Gaia-X では、トラストアンカーは eIDAS 規則に基づくトラストサービスプロバイダー(電子署名用適格証明書の発行者)や EV SSL 証明書の発行者が挙げられており<sup>11</sup>、これらが信頼の連鎖の基点として機能する。Gaia-X では、既存の公的枠組み (eIDAS) による高い信頼性を重視する一方、SSI の思想に基づき DID による分散性とユーザ主権を追求する新しいアプローチも取っている。DID として did:web を使用し、既存の Web インフラ (ドメイン名システムや HTTPS 等) の信頼メカニズムが DID Document の信頼性を担保する。

DSSC においても、eIDAS 規則に基づくトラストサービスプロバイダーをトラストアンカーとしつつ、DID では did:ebis も可能となっており、ブロックチェーンの改ざん耐性で DID Document、つまり DID Document 内の検証鍵の信頼性を担保する構想がある。

## 4.3 信頼できる情報源

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<sup>12</sup>。

信頼できる情報源の代表的な例として、個人や組織の身元を公的に証明する信頼性の高い機関である政府認証 ID プロバイダが挙げられる。政府認証 ID プロバイダから発行される情報源としては、例えば運転免許証、パスポート、マイナンバーカード、商業登記電子証明書がある。

政府認証 ID プロバイダは法的に規定されたプロセスに基づきデジタル ID を発行し、信頼性とセキュリティを支える。政府認証 ID プロバイダから発行されたデジタル ID を、プライベート ID と連携することに

<sup>11</sup> <https://docs.gaia-x.eu/policy-rules-committee/trust-framework/22.10/>

<sup>12</sup> <https://dssc.eu/>

より、信頼性やセキュリティを担保した上でユーザの利便性を高めることができる。

データスペース管理者のアイデンティティ管理やノタリー（詳細：5.3.2）は、必要に応じて信頼できる情報源に基づき、データスペース参加者の実在性や属性（資格）を確認し、その証明として VC を発行する機能を担う。「図 4-4 Gaia-X システムコンテキスト」に示されるように、Gaia-X では VAT/EORI/LEI 登録・管理者等が信頼できる情報源であり、それに基づいて企業・組織等のデータスペース参加者に VC が発行される。

## 4.4 トラステッドリスト

トラステッドリストは、一般に EU List of Trusted Lists を指すことが多いが、データスペースにおいては、データスペース内で信頼されるエンティティやコンポーネント、データソースなども含めた「広義の信頼済みリスト（レジストリ）」として捉える。本章では、後者の「レジストリ」の概念も包含しながら、その役割と機能について説明する。

### 4.4.1 トラステッドリストの役割

トラステッドリストは、ETSI TS 119 612 v2.4.1 (TS 119 612 - V2.4.1 - Electronic Signatures and Trust Infrastructures (ESI); Trusted Lists) の 3.1 Definitions で以下のように定義されている。

「list that provides information about the status and the status history of the trust services from trust service providers regarding compliance with the applicable requirements and the relevant provisions of the applicable legislation.

NOTE: In the context of European Union Member States, as specified in Regulation (EU) No 910/2014, it refers to a EU Member State list including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them.

In the context of non-EU countries or international organizations, it refers to a list meeting the requirements of the present document and providing assessment scheme based approval status information about trust services from trust service providers, for compliance with the relevant provisions of the applicable approval scheme and the relevant legislation.」

EU 域では Regulation (EU) No 910/2014(eIDAS)の規定通り qualified trust service providers (QTSP) およびこのサービスによって提供される qualified trust services の情報を含むリストである。これらの情報を透明かつアクセス可能な方法で提供することで、電子署名や e シール等の利用者がトラストサービスの信頼性を検証可能とすることが目的である。eIDAS Dashboard により、EU 加盟各国および各国のトラステッドリストを 1 つにまとめた List Of Trusted List (LOTL)<sup>13</sup>が公開されており、既に利用可能である。

対してデータスペースにおいては、トラステッドリストを包含する情報を格納するものとしてレジストリが定義されている。例えば、DSSC (Data Spaces Support Centre) が公開する Data Spaces Blueprint v2.0<sup>14</sup>では、レジストリは「Public or private registry where the lists of valid and revoked trust anchors, trust service providers, trusted data sources and notaries, together with the schemas for data space credentials, are stored.」と定義されており、eIDAS で規定されたトラストサービスプロバイダー以外にもデータスペースのルールやポリシーを満たすサービスやコンポーネントを含めたリストを格納する。

---

<sup>13</sup> <https://eid.as.ec.europa.eu/efda/trust-services/browse/eidas/tls>

<sup>14</sup>

## 4.4.2 トラステッドリストの機能

データスペースにおけるトラステッドリストの機能として、1つは外部で認定されたトラストサービスプロバイダー（TSP 及びその認定履歴情報を含む）や認証局（CA：Certificate Authority）のリストを参照し、信頼できる TSP や CA を明確にすること、もう一つ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で、これらの機能によりユーザが信頼できるサービスを選択・利用可能とすることや、データスペース内の各種コンポーネントが信頼できることを検証可能とすること、を実現できる。

例えば、Gaia-X のデジタルクリアリングハウス（GXDC）では、「図 4-4 Gaia-X システムコンテキスト」に示すようにトラストアンカーとしての TSP は eIDAS のトラステッドリストを、CA は Mozilla の CA Certification List を参照して取り込んでいる。これらの情報はある企業が他の企業のサービスを発見し、利用するための情報として利用される。

## 4.5 電子署名

電子署名とは、データの真正性および署名者の本人性を保証する仕組みである。認証局による証明書発行と失効管理が必要である。検証鍵証明書と証明書失効リスト(CRL)を用いて検証鍵の有効性の確認を行う。

電子署名における署名鍵の管理は、第三者によるなりすましを防ぐために重要である。鍵管理方法として、例えばローカルの IC カードや HSM へ格納し、推測されにくいパスワードを設定して管理することがあげられる。署名鍵が第三者に渡った可能性がある場合、すみやかに電子証明書の失効手続きを行わなければならない。

電子署名の有効性を長期間確保するための方法として、長期署名がある。長期署名では、電子署名後にタイムスタンプを付与して署名時点の正しい時刻で完全性を保護した後、タイムスタンプの有効期限が近付いた際に新たなタイムスタンプの付与を行う。これにより電子署名の有効期限を延長することができる。

また、前述した電子署名は署名鍵を署名者のローカル環境で管理することを前提としていたが、署名鍵をクラウドで管理する方式もある。これをリモート署名という。リモート署名では、リモート署名事業者側で署名者の署名鍵を保管し、署名者の指示に応じてその署名鍵で署名を行う。リモート署名における署名者のメリットは、鍵の管理が不要になることやオンライン環境下であれば場所を選ばずに電子署名を行えることである。

## 4.6 e シール

e シールは、法人が電子データの発信元であることと、そのデータが改ざんされていないことを保証するための電子的な印章である。デジタル署名の一種だが、個人ではなく企業など法人名義で行われる点の特徴である。

通常の e シールでは、総務省認定の認証局（CA）が組織名義の証明書（e シール用証明書）を発行する。この証明書には企業名や ID、検証鍵などが含まれ、証明書発行時には CA が証明書署名を行い、企業に署名鍵とともに配布する。企業はこの証明書を自社のコネクタやサーバにインストールし、通信や署名時に提示する（ローカル署名方式）。他の参加企業は、その証明書が総務省認定の CA によって署名されていることを検証することで、相手が真正なメンバー企業であることを確認できる。

ローカル署名方式以外にも、企業自身が署名鍵を管理せず、トラストサービス・プロバイダー（TSP）が鍵を安全に管理し、署名時には企業が TSP にデータを送付して e シールの署名を付与してもらうリモート署名方式が存在する。署名鍵の漏洩は、たとえ一社であってもなりすましによる不正データがデータスペースに流通するリスクとなり、結果としてデータスペース全体の信頼性を損なう可能性があるため、参加企業はセキュリティ対策コストや漏洩リスクを考慮し、ローカル署名方式またはリモート署名方式を選択する。

e シールは、データの発行元と非改ざん性を証明するものであり、総務大臣による認定によってその信頼

性が保証される。なお、適格 e シール<sup>15</sup>とそうでない e シールが存在し、リモート e シールの位置付けや類似技術との使い分けについても、鍵管理方法やコスト、手続きの違いを踏まえて検討する必要がある。こうした運用においては、全参加者が一定の基準を満たすことが求められ、アシュアランス・レベルの考え方の統一も必要である。従来の e シール利用者に対して、データスペースでの利用時に必要な追加説明を実施し、合意を得る手続きが求められる。

## 4.7 タイムスタンプ

タイムスタンプとは、ある時刻にそのデータが存在していたこと、それ以降に変更されていないことを証明するものである。タイムスタンプは、一般的に総務大臣による認定を取得した第三者機関である Time-Stamping Authority (TSA) が発行処理を行う。これにより、タイムスタンプが付与された時刻に対象データが存在していたことを保証される。

デジタル署名を利用したタイムスタンプでは、データのハッシュ値と時刻情報に対して TSA が管理する署名鍵でデジタル署名を行う。タイムスタンプの検証の際は、利用者は TSA 証明書および CA から提供される失効情報を用いて検証を行う。タイムスタンプの有効性は TSA 証明書に設定された有効期間に依存し、この有効期間の間は CA により提供される失効情報により検証が可能である。タイムスタンプの有効期間を延長するためには、有効期間内に新たなタイムスタンプを追加付与することが必要である。

## 4.8 VC(Verifiable Credential)・VP(Verifiable Presentation)

Verifiable Credential (VC) は、第三者検証可能な形で属性情報を表したデータ形式のことである。暗号的な手法をとることで、データの完全性と発行者の真正性が保証されている。VC の規格は W3C によって標準化されており、相互運用性が担保されている<sup>16</sup>。VC にはいくつかのフォーマットがあるが、属性情報の選択的開示が可能なもの(例、SD-JWT)では、過剰な情報を検証者に明らかにすることなく、VC 発行対象の属性情報を証明できる。このような VC を認証や属性証明に用いることで、VC 発行対象のプライバシーを保護することができる。

### 4.8.1 基本アーキテクチャ

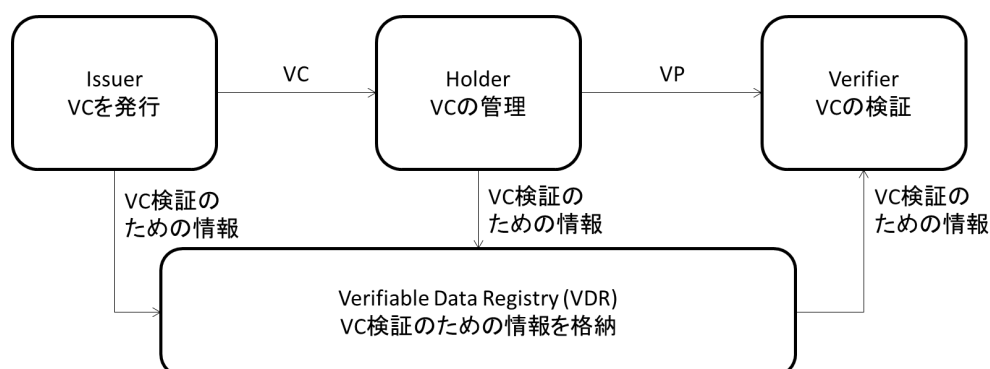


図 4-5 VC の基本アーキテクチャ

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

<sup>15</sup> [https://www.soumu.go.jp/main\\_content/000689514.pdf](https://www.soumu.go.jp/main_content/000689514.pdf)

<sup>16</sup> W3C, Verifiable Credentials Data Model v2.0, <https://www.w3.org/TR/vc-data-model-2.0/>

「図 4-5 VC の基本アーキテクチャ」に W3C に基づく基本アーキテクチャの概要図を示す。アイデンティティ管理において Issuer、Holder、Verifier のエンティティが連携するモデルを IHV モデルという。以下に IHV モデルに基づくデータスペース上の各エンティティの例を示す。

- Issuer：データスペース参加資格判定者
- Holder：データスペース参加企業（データ要求元）
- Verifier：データスペース参加企業（データ提供元）

VC の発行対象者は Holder と同一でも異なってもよい。本章では、VC 発行対象者と Holder が同一である場合を想定する。以下に IHV モデルにおける各エンティティの役割を述べる。

- Issuer  
Holder に関する本人認証、VC に含める属性情報に関する情報の収集を行った後、VC の発行を行う。
- Holder  
Issuer から発行された VC を管理する。また、Verifier に対して必要に応じて VC から Verifiable Presentation (VP) を作成し、VP の提示を行う。Digital Wallet を利用して VC の管理、VP の作成、提示を行う。
- Verifier  
Holder に対して VP を要求し、提示された VP に対して検証を行う。検証後、VP に含まれる VC 内記載の属性情報に基づき認証、認可を行う。以下に Verifier が検証すべき項目を示す。
  - VC、VP が真正であること  
VC および VP に付与された電子署名を、Issuer、Holder の検証鍵を用いてそれぞれ検証する。
  - VC が有効であること  
VC の有効期間内であることを確認する。また、VC 失効リストを用いて VC が失効していないか確認する。
  - VC 内記載の VC 発行対象者から VC が提示されていること  
VP を提示した Holder と、VC 内記載の VC 発行対象者が一致することを確認する。確認する方法として、例えば Holder の DID に紐づく鍵ペアを用いたチャレンジレスポンス等がある。
- Verifiable Data Registry (VDR)  
VC や VP の検証を行うために必要となる検証情報を管理する。検証情報とは、例えば Issuer や Holder の検証鍵、VC の失効情報、VC のメタデータ、トラステッドリストである。VDR の実装形態は必ずしもブロックチェーンである必要はない。

#### 4.8.2 データモデル

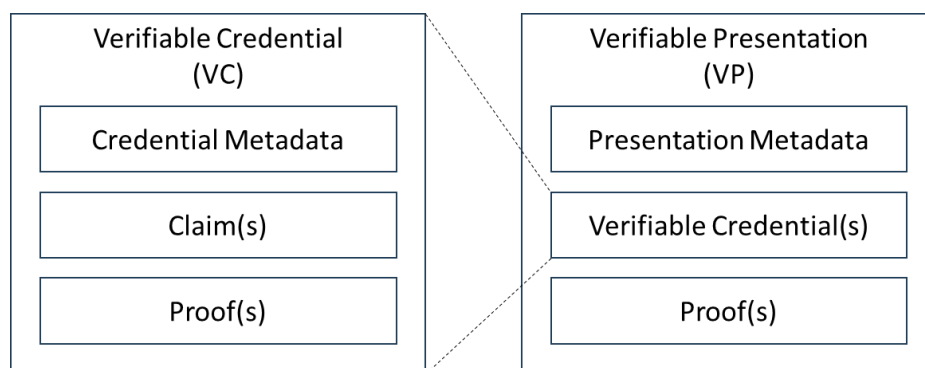


図 4-6 VC、VP の基本モデル

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

「図 4-6 VC、VP の基本モデル」に VC および VP の基本モデルを示す。Holder が Verifier に対して提示するのは VC ではなく VP であり、VP と VC の関係は図に示したとおりである。

以下に VC の各コンポーネントの概要を示す。

- Credential Metadata : VC 自体の識別子、有効期間等
- Claim(s) : VC 発行対象者の属性情報
- Proof(s) : Issuer の署名等

また、以下に VP の各コンポーネントの概要を示す。

- Presentation Metadata : VC 自体の識別子、有効期間等
- VC(s) : Verifier に提示する VC
- Proof(s) : Holder の署名等

VC および VP における Proof に含まれる電子署名について、VC は Issuer による電子署名、VP は Holder による電子署名であり、それぞれ異なる者が電子署名を行う。Issuer、Holder が電子署名に用いる署名鍵について、例えば以下が想定される。

- Issuer、Holder 自身が有する e シールに紐づく署名鍵
- Issuer、Holder 自身が有する DID に紐づく署名鍵

電子署名時に使用した署名鍵の種類により検証鍵の格納方法が異なる。そのため、Verifier は VC および VP の電子署名を検証する際、各電子署名に用いられた署名鍵の種類を特定した後、それぞれに対応した方法にて検証鍵を取得する。以下に各署名鍵の種類における検証鍵の格納方法を示す。

e シールに紐づく署名鍵を用いた電子署名の場合、その検証に用いる検証鍵は e シール用電子証明書に格納される。

DID に紐づく署名鍵を用いた電子署名の場合、その検証に用いる検証鍵の格納方法は各 VC の DID method 等によって決定される。ここで、いくつかの代表的な DID method による検証鍵の格納方法について述べる。did:key は VC 内に検証鍵情報を直接埋め込む。did:web は VDR に検証鍵を格納し、検証鍵にアクセスするためのパス情報を DID に入れこむ。did:ethr は Ethereum 上のスマートコントラクトを VDR として用いる方式であり、スマートコントラクトに検証鍵情報を格納し、この検証鍵情報にアクセスするための Ethereum アドレスを DID に入れこむ。このように、必ずしも VC に検証鍵を含むわけではないため、この点において VC は既存の検証鍵証明書と異なる。

#### 4.8.3 VC に基づく属性ベースのアクセス制御

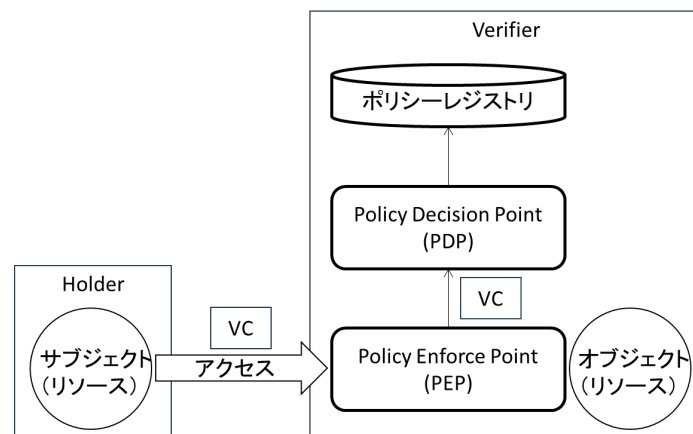


図 4-7 VC を用いた ABAC の概要

Verifier は VC に含まれている属性情報を用いて属性ベースのアクセス制御 (ABAC: Attribute Based Access Control) を行うことができる。図 4-7 に VC を用いたアクセス制御の概要図を示す。サブジェクト (Holder) からオブジェクト (Verifier) へのアクセスを行う際、Verifier はこれが正当なアクセスであるか検証、評価し、その結果を反映する。このとき、アクセス可否を評価するのが Policy Decision Point (PDP) である。ABAC は、PDP がサブジェクトの属性情報に基づきアクセス可否の評価を行う。VC に基づく ABAC では、このサブジェクト (Holder) の属性情報を、Holder から VP として渡された VC から取得する。Policy Enforce Point (PEP) が、PDP でのアクセス可否の評価に基づき実際の処理を行う。

#### 4.8.4 アーキテクチャと処理の例

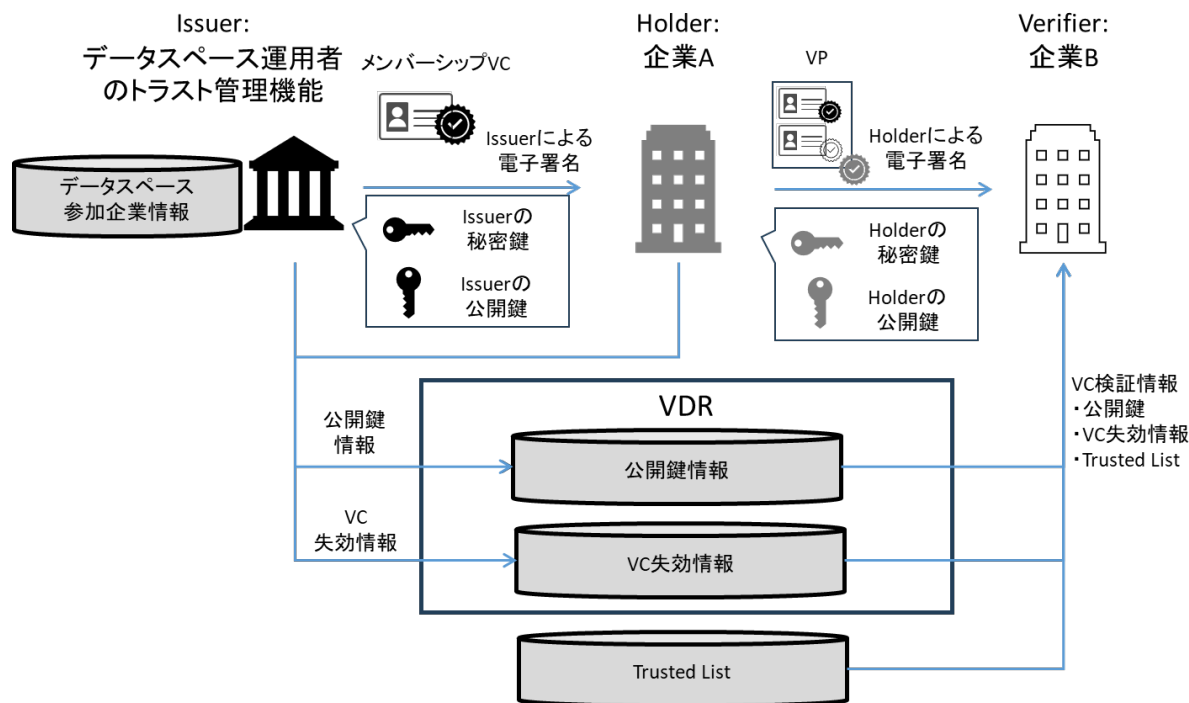


図 4-8 メンバーシップ VC の発行～提示概要

アーキテクチャと処理について、Issuer をデータスペース運用者のトラスト管理機能、Holder、Verifier をデータスペースに参加している企業 A、企業 B とし、企業 A に対するメンバーシップ VC の発行から提示までを例にとり説明する。この例では、以下を仮定する。

- ・ Issuer は DID をもち、メンバーシップ VC を発行する際の電子署名にはこの DID に紐づく署名鍵を用いる。DID に紐づく検証鍵は VDR に格納している。
- ・ Holder は DID をもち、DID に紐づく検証鍵は VDR に格納している。

はじめに、メンバーシップ VC の発行処理について述べる。企業 A は、データスペース運用者のトラスト管理機能に対して自身のメンバーシップ VC の発行を依頼する。データスペース運用者のトラスト管理機能はメンバーシップ VC の発行依頼が本当に企業 A によるものなのか認証を行う。認証成功後、データスペース運用者のトラスト管理機能は自身が所有するデータスペース参加企業情報に基づき、メンバーシップ VC を企業 A に対して発行する。このとき、メンバーシップ VC にはデータスペース運用者のトラスト管理機能が有する DID に紐づく署名鍵を用いて電子署名が付与される。

続いて、メンバーシップ VC の提示処理について述べる。企業 A は、企業 B からのメンバーシップ VC 提

示要求に対して、自身の保有するメンバーシップ VC から VP を作成し、企業 B に提示する。VP には企業 A の有する DID に紐づく署名鍵を用いて電子署名が付与される。企業 B は提示された VP の検証を行う。検証に必要な情報（データスペース運用者のトラスト管理機能の検証鍵、企業 A の検証鍵、メンバーシップ VC の失効情報、トラステッドリスト）は VDR から取得する。VP の検証に成功すれば、企業 B は企業 A がデータスペースに参加している企業であることを確認できたことになる。

#### 4.8.5 VC のライフサイクル管理

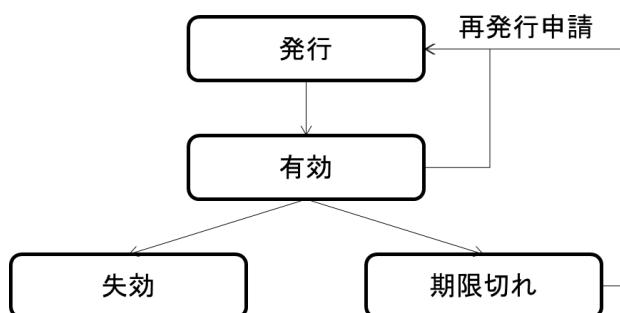


図 4-9 VC のライフサイクル

VC のライフサイクル管理を適切に行うことは VC 認証において重要である。「図 4-9 VC のライフサイクル」に VC のライフサイクルにおける概要図を示す。VC は発行された後、以下 3 つのステータスの内いずれかをとる。

- 有効(Valid)
- 失効(Revoke)
- 期限切れ(Expired)

失効とは Issuer が失効手続きを行った状態、期限切れとは VC の有効期間を超過した状態である。これらのステータスをもつ VC は認証や属性証明等に用いることができない。VC の有効期間については、用途に応じて適切な長さを設定する。VC を有効期間後も使用したい場合、VC の再発行手続きを行う。VC の再発行手続きは VC の有効期間内に行うことが望ましい。

VC 発行後にその属性情報に変更が生じた場合、Issuer はすみやかに対象となる VC の失効処理を行う。VC の失効処理方法として、例えば VDR で管理している VC の失効情報の更新がある。また、Holder が有する Wallet 側でも失効した VC はすみやかに削除する。その実現方法としては、例えば VC 失効時に Issuer から Holder の有する Wallet に対してプッシュ通知を送信し、Wallet 側で当該 VC を削除する方法がある。

#### 4.8.6 Verifiable Data Registry

Verifiable Data Registry (検証可能データレジストリ) は、分散型 ID (DID) や Verifiable Credential (VC) などの自己主権型アイデンティティ (Self-Sovereign Identity: SSI) 基盤で用いる分散型データベースまたは台帳である。主な機能は、DID に関連付けられた検証鍵やサービスエンドポイント、失効情報などの重要な情報を安全かつ改ざん困難な形で登録・管理することである。

従来の ID 管理では、中央集権的な認証局や ID プロバイダが ID 情報や検証鍵を一元的に管理していた。しかし、データスペースのような分散型システムでは、特定の管理者に依存せず、各主体が自らの ID や証明情報を管理できる仕組みが求められる。Verifiable Data Registry は、こうした分散型の信頼モデルを実現するための基盤である。

Verifiable Data Registry に登録される主な情報は以下の通りである。第一に、DID に紐づく検証鍵情報で

あり、検証者（Verifier）はレジストリを参照することで、発行者（Issuer）の検証鍵を取得し、提示された VP の署名を検証できる。第二に、サービスエンドポイント情報であり、DID を持つ主体が提供するサービスや API の接続先を示し、データ連携や相互運用性を確保できる。第三に、失効リストや失効情報であり、検証鍵が漏洩した場合や VC が無効化された場合、レジストリに失効情報を記録することで、検証者はその VC や鍵が有効かどうかをリアルタイムで確認できる。

Verifiable Data Registry は、一般にブロックチェーンや分散型台帳技術（DLT）上に構築されることが多い。これにより、単一の管理者による改ざんや不正操作のリスクを排除し、グローバルかつ永続的なデータ管理が可能となる。欧州の Gaia-X や日本の Trusted Web 構想でも、分散型レジストリの活用が想定されている。

検証者は中央集権的な ID プロバイダを介さずに、DID や VC の真正性を独立して検証でき、信頼性と透明性を両立したデータ流通を実現できる。特に、国際的な相互運用性や法規制対応が求められる場面では、Verifiable Data Registry はデジタルトラストの基盤の一つとなる。

Verifiable Data Registry の標準化や運用ガバナンス、失効管理の高度化などは重要な課題であり、各国・各業界での実装事例や国際標準化動向を注視しつつ、柔軟かつ安全なレジストリ運用体制を構築しなくてはならない。

## 4.8.7 Self-Issued Credential

Self-Issued Credential（自己発行クレデンシャル）とは、データスペース参加者が自分自身に対して発行したクレデンシャルのことである。自己発行クレデンシャルにおけるトラストについては、クレデンシャルの活用先がプライベートトラスト内であるかどうかで扱いが変わる。自己発行クレデンシャルをプライベートトラスト内で活用する場合は、発行者の本人性が担保されているため、自己発行クレデンシャルによるトラストが担保される。したがって、データスペースにおいてプライベートトラストのみを想定する場合は自己発行クレデンシャルで十分である。一方で、パブリックトラストの環境下では、パブリックトラストに属するエンティティに対して自己発行クレデンシャルのみでトラストを担保することはできないため、別途トラストを担保するためのパブリックなクレデンシャルを用意しなくてはならない。

## 4.8.8 DID (Decentralized Identifier)

Decentralized Identifier (DID) は、特定組織や中央機関に依存することなく、個人やモノが自身で管理できる永続的でグローバルに一意的識別子のことである。検証可能なレジストリである VDR に記録され、自己主権型アイデンティティ（SSI）を実現する。VDR は、この DID に関連する情報、検証鍵やサービスエンドポイント、失効情報を格納する。Verifier は、この VDR を参照することで、発行者（Issuer）の検証鍵を取得し、提示された VC を検証できる。DID や VDR により、集権的な ID プロバイダを介さずに、データの真正性とプライバシーを担保した安全な取引やサービス利用が可能になる。

## 4.9 Digital Wallet



図 4-10 Digital Wallet と各エンティティの関係

Digital Wallet は Holder が ID、VC、デジタル資産等を安全に管理・利用するためのツールである。「図 4-10 Digital Wallet と各エンティティの関係」に Digital Wallet と各エンティティの関係を示す。Digital

Wallet は暗号化によりセキュリティを確保し、データ共有を管理して自己主権を実現する。

自然人向け Digital Wallet としては例えば EUDIW(European Digital Identity Wallet)があり、EU にて活発な議論および開発が進められている。一方で法人向け Digital Wallet については、サービスとして提供されているものがあるものの、自然人 Digital Wallet と比較すると仕様に関する議論はこれからである。法人向け Digital Wallet では、DPP や Self-Issued VC についても管理を行うことが想定される。

## 4.10 コネクタ

コネクタは、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間で、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る。コネクタは、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。

## 4.11 IAL/AAL

トラストのレベルは、主に身元確認保証レベル (Identity Assurance Level, IAL) と本人確認保証レベル (Authentication Assurance Level, AAL) で決定される。IAL、AAL は、NIST の SP800-63-4<sup>17</sup>での定義が基本となる。

図 4-11 に本人確認の構成要素を示す。本人確認の構成要素には、利用者の身元を確認して利用者として登録する「身元確認 (Identity Proofing)」と、既に登録された本人であることを確認する「本人認証 (Authentication)」がある。IAL は、利用者が主張する身元がどの程度信頼できるかを表す「身元確認」に関する指標であり、利用者が本当に実在する人物であり、提示した属性が正しいかを確認するレベルを示す。AAL は本人確認済みの利用者がサービスへアクセスする際の「本人認証」に関する指標であり、アカウントにアクセスする人物が本当に正当な利用者であることを、どの程度の確実性で証明できるかのレベルを示す。

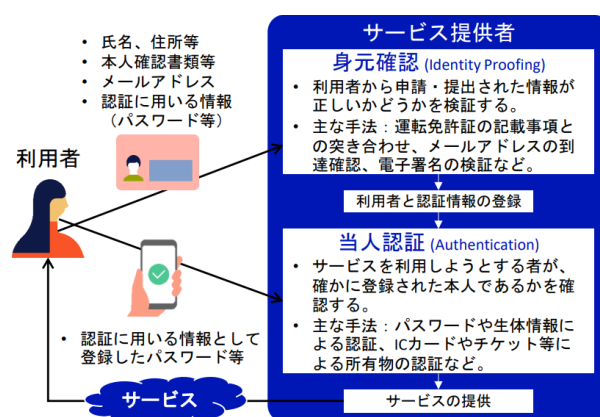


図 4-11 本人確認の構成要素 (身元確認と本人認証)

「デジタル庁、VC に関連する各種制度等について<sup>18</sup>」から引用。

<sup>17</sup> NIST SP 800-63 Digital Identity Guidelines, <https://pages.nist.gov/800-63-4/>

<sup>18</sup> [https://www.digital.go.jp/assets/contents/node/basic\\_page/field\\_ref\\_resources/5a5c145f-85f4-41a5-bc51-4e442c6154b8/4c7ac849/20250310\\_meeting\\_verifiable-credential-governance\\_outline\\_04.pdf](https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5a5c145f-85f4-41a5-bc51-4e442c6154b8/4c7ac849/20250310_meeting_verifiable-credential-governance_outline_04.pdf)

「表 4-1 Identity Assurance Level (IAL)」に IAL、「表 4-2 Authentication Assurance Level (AAL)」に AAL の定義を示す。IAL および AAL は、プライバシーやユーザビリティの観点も踏まえると、いずれも「高ければよい」ものではなく、サービスの特性やリスクに応じて選択される。

表 4-1 Identity Assurance Level (IAL)

レベル	説明
IAL0	本人確認を行わないレベルである。利用者が提示する属性は自己申告に過ぎず、検証もされない。匿名利用や低リスクのサービスに適する。
IAL1	申請された身元が現実に存在することを裏付ける。コア属性は申請者の提示した証拠や申告に基づき、権威ある情報源や信頼できるソースと照合される。
IAL2	より強力な証拠を収集し、厳格な検証プロセスを経ることで、IAL1 より高い信頼を与える。
IAL3	訓練された CSP (Credential Service Provider) の担当者が対面または監督下でリモート本人確認を実施することを要求し、非常に高い保証を提供する。

表 4-2 Authentication Assurance Level (AAL)

レベル	説明
AAL1	認証器の所持と制御を基本的に確認するレベルである。シングルファクタ認証（例：パスワード）のみでよいが、多要素認証を提供することが推奨される。
AAL2	2つの異なる認証要素を要求する。少なくとも一つはフィッシング耐性を持つ手段でなければならない。例として、パスワード+ワンタイムコードや、デバイス認証+バイオメトリクスなどがある。
AAL3	検証鍵暗号に基づく強固な仕組みを利用し、耐タンパ性を持ちフィッシング耐性のある認証器を必要とする。認証には2つの異なる要素を組み合わせ、非常に高いトラストを提供する。

## 4.12 日本における組織に対する実在確認のための識別子

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)<sup>19)</sup>」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。当該識別子を参考にして、表 4-3 にまとめる。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。

表 4-3 日本における組織識別子

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	ISO6523-2 「0188」 ISO/IEC 15459-2 「TAJ」 UN/EDIFACT 3055 「402」

<sup>19)</sup> [https://www.soumu.go.jp/main\\_content/001006115.pdf](https://www.soumu.go.jp/main_content/001006115.pdf)

	<p>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</p> <p>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</p> <p>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></p>	
会社法人等番号	<p>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。</p> <p>個人事業主は「商号登記」を行うことで発番される(任意)。</p>	
適格請求書発行事業者登録番号	<p>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。</p> <p>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></p> <p>個人事業主でも一部は発番されない。</p>	ISO6523-2「0221」
LEI	<p>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。</p> <p>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></p>	<p>ISO 17442</p> <p>参考：  <a href="https://www.gleif.org/ja/organizational-identity/introducing-the-legal-entity-identifier-lei/iso-17442-the-lei-code-structure">https://www.gleif.org/ja/organizational-identity/introducing-the-legal-entity-identifier-lei/iso-17442-the-lei-code-structure</a></p>
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。	<p>ISO6523-2「0170」</p> <p>ISO/IEC 15459-2「VTD」</p> <p>UN/EDIFACT 3055「311」</p>
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		<p>ISO6523-2「0147」</p> <p>ISO/IEC 15459-2「LA」</p> <p>UN/EDIFACT 3055「289」</p>

識別子は、1社に1コードを厳密に管理していること、倒産や廃業がリアルタイムに確認可能であること、合併や被合併等の情報も正確に反映されていることなどが求められる。

## 5 データスペースへのトラストの実装と運用

### 5.1 全体像

#### 5.1.1 データスペースのトラスト

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。主要要素は以下である。

- (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
- (2) アクセス認証・認可によるポリシー準拠の利用制御
- (3) eシールやVCを活用したデータ署名による完全性・真正性の担保

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強化すべきである。内部（単一組織内）利用では、組織内のガバナンスに依拠したトラストの確立が中心となる。国内（同一国内の複数組織間）利用では、国内における共通のルールや法的枠組みの整備が必要となる。国際利用の場合、最も高い水準のトラストが必要となる。各国のデータ保護法令、たとえばGDPRなど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しなくてはならない。すなわち、内部利用、国内利用、国際利用の順で、トラストを強化していくことになる。

#### 5.1.2 三層アーキテクチャ

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、図 5-1 に示す「アプリケーションサービス層」、「データ連携層」、「トラストサービス層」の3層で構成される。以下に、各層の役割を示す。

- 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

経団連ではデジタル庁に対し、この3層アーキテクチャを念頭に、「ユースケースの如何に関わらず共通に整備すべき要件（共通枠組み）」と、「ユースケースごとに設計すべき個別要件」を明確にした上で、共通枠組みの整備を優先して進めるべきであると提言している<sup>20</sup>。また、DSA、DPFJ、JDTFでは、国際的な相互運用性も視野に入れ、国際標準化に関与していく必要があると提言している<sup>21</sup>。

3層アーキテクチャのうち「トラストサービス層」は、データの信頼性を支えるため、国際的に通用する横断的なトラスト基盤の整備が必要となる。横断的に必要となる検証主体の真正性・実在性を証明するための基盤整備と、各サービスの保証レベルの定義・可視化が不可欠であり、我が国が標榜する信頼性のある自由なデータ流通（DFFT）<sup>22</sup>を実現するためには、このトラスト基盤が盤石ではなければならない<sup>23</sup>。

<sup>20</sup> 経団連、産業データスペースの構築に向けて求められる施策、

[https://www.cas.go.jp/jp/seisaku/digital\\_gyozaiikaku/data7/data7\\_siryou4.pdf](https://www.cas.go.jp/jp/seisaku/digital_gyozaiikaku/data7/data7_siryou4.pdf)

<sup>21</sup> DSA, DPFJ, JDTF, 声明「データスペース等に関する国際標準化の必要性」、

<https://jdtf.or.jp/news/2025/pdf/0306-01.pdf>

<sup>22</sup> <https://www.digital.go.jp/policies/dfft>

<sup>23</sup> 経団連、産業データスペースの構築に向けた第2次提言、

[https://www.cas.go.jp/jp/seisaku/digital\\_gyozaiikaku/kaigi10/kaigi10\\_siryou9.pdf](https://www.cas.go.jp/jp/seisaku/digital_gyozaiikaku/kaigi10/kaigi10_siryou9.pdf)

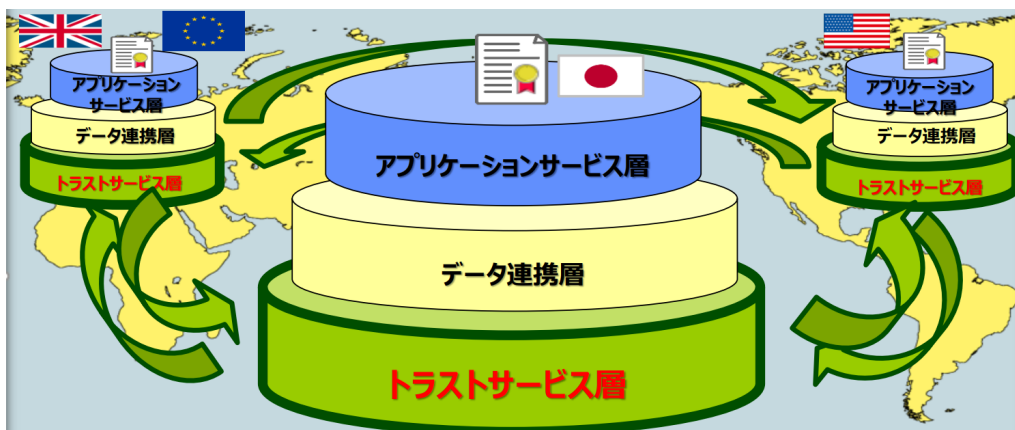


図 5-1 産業データスペースの3層アーキテクチャのイメージ

(経団連, 産業データスペースの構築に向けた第2次提言<sup>24</sup>より参照)

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、上記の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。また、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「信頼できる情報源」が必要である。データスペースは3層（アプリケーションサービス層、データ連携層、トラストサービス層）で、それらが信頼できる情報源と連携する必要がある。

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。なお、データスペースが他のデータスペースと接続する際は、データ連携層のコネクタ機能により行う。

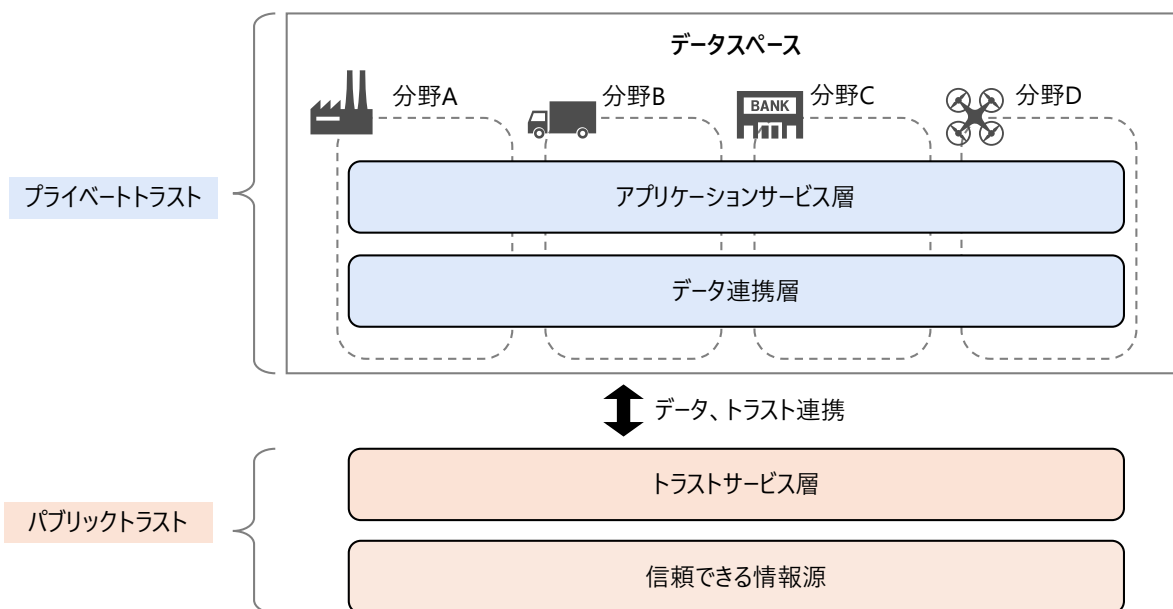


図 5-2 データスペースのあるべき姿

「図 5-2 データスペースのあるべき姿」にデータスペースの各層の機能群を示す。各層の代表的な機能は以下である。

<sup>24</sup> <https://www.keidanren.or.jp/policy/2025/026.html>

- 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

## 5.2 データスペースの運営

データスペースは基本的に会員制の組織である。会員間の信頼は会員制に依拠し維持される。会員間の信頼が存在することで、会員相互の活動（データ取引など）を円滑に行うことができる。この「会員相互に信頼し合っている状態」をトラストが確立されているという。デジタル空間を前提にしたトラストを、どのように確立し運営するかはデータスペースにとって最も重要な課題である。当該課題を解決するための技術として、暗号技術を基盤としたトラストサービスの活用が有効である。

図 5-3 に、データスペースにおける On-Boarding と On-Going の全体像を示す。「On-Boarding」として、データスペースの参加者は、データスペース運用者のトラスト管理機能から、データスペースの参加者であることを示す会員証を受け取る。この「会員証」は電子的に第三者検証可能でなくてはならない。欧州の Gaia-X では、この会員証に W3C の標準規格である VC（参照：4.8）を活用している。本ドキュメントでは、会員証として VC を用いることを前提とし、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を「メンバーシップ VC」と呼ぶ。「On-Going」では、参加者はメンバーシップ VC を用いて、他の参加者との会員相互の活動を実施する。例えば、企業 A の参加者が企業 B の参加者に自身のメンバーシップ VP を提示し、企業 B の参加者は受け取った VP の正当性を検証する。企業 B の参加者は正当性の検証後、企業 A の参加者に対して署名済みデータを提示する。その他のライフサイクルとして、データスペースへの参加を停止する「Off-Boarding」、属性情報に変更が生じた場合の「属性情報の変更」がある。以下に、「図 5-3 データスペースの全体像」の（ア）～（エ）の処理を示す。「表 5-1 フェーズごとの実施内容」には、「On-Boarding」、「On-Going」、「Off-Boarding」、「属性情報の変更」の 4 つのフェーズを示す。

- （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 VP」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 VP 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 VP を検証するため、データスペース運用者が提供する VDR（詳細は 4.8.8 参照）やノー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 VP の正当性が確認できた場合、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。

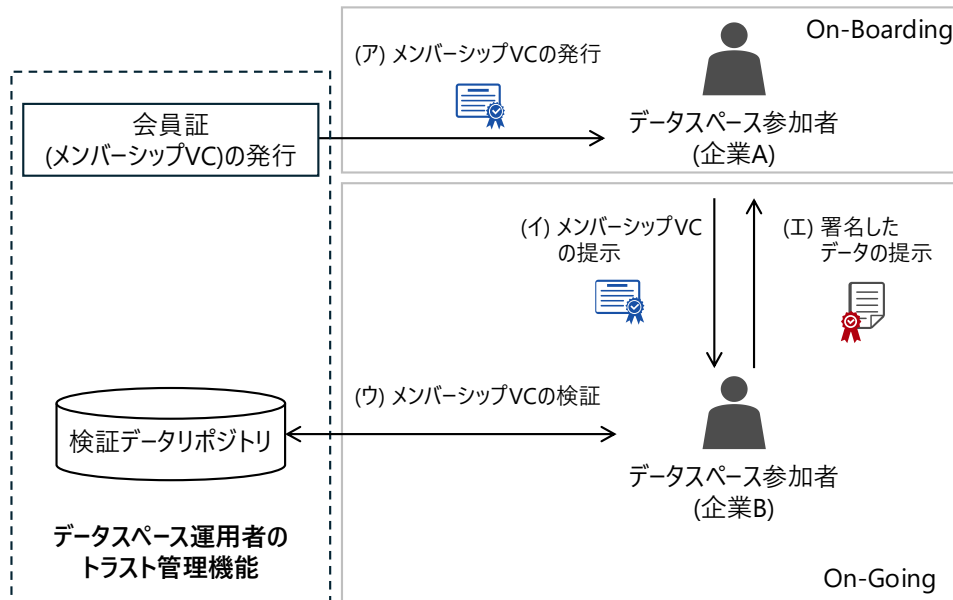


図 5-3 データスペースの全体像

表 5-1 フェーズごとの実施内容

フェーズ	内容
On-Boarding	データスペースという会員制組織への参加希望者 (Applicant) は、当該組織運営管理者に参加希望を申請する。当該組織運営管理者は、組織自身のポリシーに照会して参加候補者 (Candidate) を審査し、合格であれば加入を承認する。その際に参加資格を証明する電子的な会員証を発行する。
On-Going	データスペース参加者が組織内で活動する際には、発行された会員証を利用する。当該会員証をもとに、当該参加者の活動資格を絶えず確認、検証できる状態が整備される。
Off-Boarding	データスペース参加者が加入後に組織内の活動においてデータスペース (を運営する組織) のポリシーに違反する活動や取引等を行った場合、データスペース組織の運営管理者は当該参加者に対し所定の審査を実施したうえ処分を決定する。処分の内容として、当該参加者の組織内での活動制限や、組織からの除名などが挙げられる。処分の結果として当該処分対象者に発行された会員証は無効化の処置が実施され、他の参加者が誤認して当該処分対象者と処分内容に違反する活動、取引を行わないようにする。
属性情報の変更	データスペース参加者へ発行された会員証の属性情報に関する記載事項に変更が生じた場合は、速やかに変更の手続を実施する。

## 5.2.1 On-Boarding

データスペースにおける On-Boarding の流れを「図 5-4 On-Boarding の全体像」に示す。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。この一連の流れにより、トラストが担保されたメンバーシップ登録を実現する。

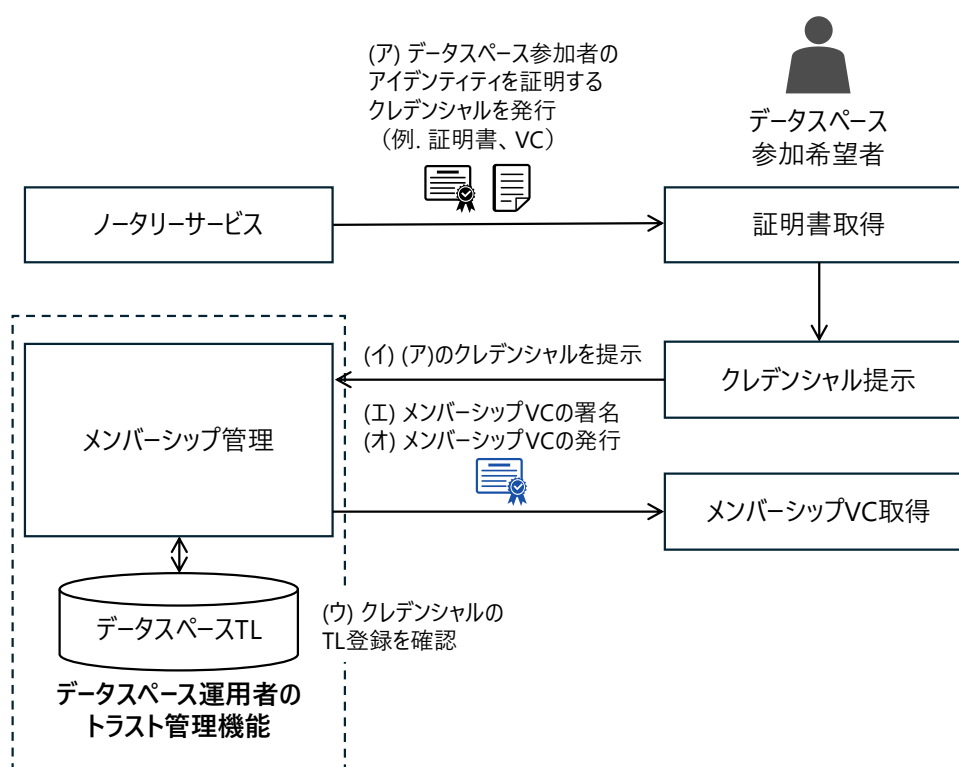


図 5-4 On-Boarding の全体像

本項では、On-Boarding において、トラストを担保する上で重要となる以下の3点について説明する。

- (1) クレデンシャルの発行・提示（「図 5-4 On-Boarding の全体像」の(ア)、(イ)、(オ)に該当）
- (2) クレデンシャルの確認（「図 5-4 On-Boarding の全体像」の(ウ)に該当）
- (3) メンバーシップ VC の署名（「図 5-4 On-Boarding の全体像」の(エ)に該当）

### (1) クレデンシャルの発行・提示

トラストを担保し相互運用性を実現するクレデンシャルの発行、提示を実現するためには国際標準に準拠しなくてはならない。例えば、VC を授受する場合は、発行には、OID4VCI<sup>25</sup> (OpenID for Verifiable Credential Issuance)、提示には、OID4VP<sup>26</sup> (OpenID for Verifiable Presentations) の採用を推奨する。OID4VCI、OID4VP は OpenID Foundation が策定する国際標準であり、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。データスペースにおけるトラストの要件を満たすためには、各組織が独自仕様に依存するのではなく、標準化されたプロトコルに準拠することが不可欠である。国際標準に準拠することは、法規制や業界ガイドラインとの整合を取り、グローバルなエコシステムとの接続性を確保する上でも重要である。

<sup>25</sup> [https://openid.net/specs/openid-4-verifiable-credential-issuance-1\\_0.html](https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html)

<sup>26</sup> [https://openid.net/specs/openid-4-verifiable-presentations-1\\_0.html](https://openid.net/specs/openid-4-verifiable-presentations-1_0.html)

## (2) クレデンシャルの確認

データスペース運用者は、データスペース参加希望者が提示した、ノー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、組織の実在性確認を行う。

組織に対する実在の確認は、総務省の e シールに関する取り組み<sup>27</sup>が参考となる。「e シールに係る認証業務の認定に関する実施要項」第 6 条第 1 号では、以下の 3 点が求められている。

- 法的な実在性確認
- 物理的実在性確認
- 運営的実在性確認

具体的な確認内容は、総務省「e シールに係る認証業務の認定に関する実施要項」で以下のように求められている。

総務省「e シールに係る認証業務の認定に関する実施要項」第 6 条第 1 号

利用者が実在することを確認するため、次のイからハまでに掲げる方法により確認を行うものとする。

- イ 我が国の法令に規定された証明書の提出を求め確認する方法又はその他同等なものとしてみなすことができる方法。
- ロ 利用申込者が申込時に申告した本店又は主たる事務所の住所とイで提出した証明書に記載された本店又は主たる事務所の住所が同一であることを確認する方法又はその他同等なものとしてみなすことができる方法。
- ハ 利用者が自らの事業を継続的に運営していることを確認する方法。

上記「イ」は、例えば商業登記を参照することで、少なくとも「法的な実在性確認」が実施可能と考えられる。

上記「ロ」や「ハ」は、例えば信頼できる第三者機関が営む法人データベースへの登録状況の確認を行う方法（総務省「e シールに係る認証業務の認定に関するガイドライン」の(7).利用者の実在性の確認の方法関係① エ）で少なくとも「物理的実在性確認」および「運営的実在性確認」が実施可能である。信頼できる第三者機関が営む法人データベースが商業登記をベースとしていれば、3 点の確認を一度に実施できる。

なお、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、4.12 にて説明した「日本における組織に対する実在確認のための識別子」を利用できる。

## (3) メンバーシップ VC の署名

メンバーシップ VC の署名には、Gaia-X では DID (did:web) に紐づく署名鍵が検討<sup>28</sup>されているが、e シール署名鍵を使用することもできる。いずれの方式を採用する場合でも、第三者が VC の真正性、完全性、失効状態を検証可能であることが本質的な要件である。そのため、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。具体的には、VDR 等のレジストリを公開し、データスペースの参加者が参照可能な状態にしておかなくてはならない。

<sup>27</sup> [https://www.soumu.go.jp/main\\_sosiki/joho\\_tsusin/top/ninshou-law/electronic\\_seal.html](https://www.soumu.go.jp/main_sosiki/joho_tsusin/top/ninshou-law/electronic_seal.html)

<sup>28</sup> [https://docs.gaia-x.eu/technical-committee/architecture-document/25.05/gaia-x\\_technical\\_compatibility\\_specifications/](https://docs.gaia-x.eu/technical-committee/architecture-document/25.05/gaia-x_technical_compatibility_specifications/)

## 5.2.2 On-Going

データスペースにおける On-Going の流れを「図 5-5 On-Going の全体像」に示す。データスペースでは、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、要求者の検証を行う。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。この一連の流れにより、トラストが担保されたデータ授受を実現する。

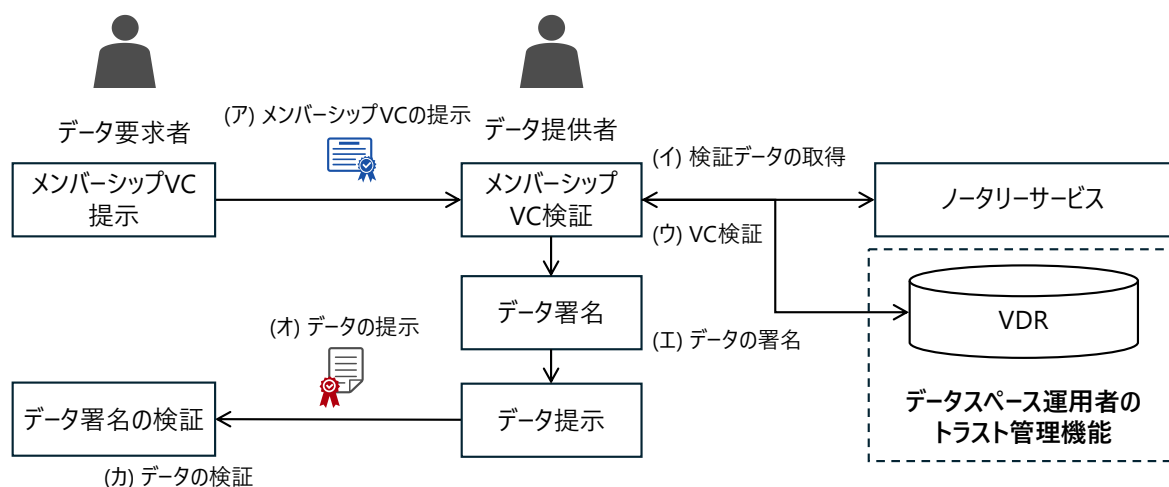


図 5-5 On-Going の全体像

本項では、On-Going において、トラストを担保する上で重要となる以下の 3 点について説明する。

- (1) クレデンシャルの発行・提示（「図 5-5 On-Going の全体像」の(ア)、(オ)に該当）
- (2) データスペースで授受される VC および e シールの検証（「図 5-5 On-Going の全体像」の(イ)、(ウ)、(カ)に該当）
- (3) データの署名（「図 5-5 On-Going の全体像」の(エ)に該当）

### (1) クレデンシャルの発行・提示

5.2.1 で述べた「クレデンシャルの発行・提示」と同様に、トラストを担保し相互運用性を実現するためには、国際標準に準拠する必要がある。データスペースにおけるメンバーシップ VC（データスペース参加者による署名済のメンバーシップ VC は、正確には VP である。参照：4.8）の提示には、OID4VP の採用を推奨する。

### (2) データスペースで授受される VC および e シールの検証

データスペースにおいて、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である。その実現手段として、e シールと VC（参照：4.8）が用いられる。

e シールおよび VC の検証方法を説明する。e シールの検証方法は e シール利用者ガイドライン v1<sup>29</sup>を参照されたい。検証者は e シールを検証するサービス等にアクセスし、e シールの正当性を検証する。具体的には、X.509 証明書の中に格納された e シール検証鍵を活用して、署名検証を行う。また、e シールを発行する認証局および当該事業者が提供する OCSP/CRL から失効情報を取得し、失効検証を行う。さらに、信

<sup>29</sup> JDTF, e シール利用者ガイドライン v1,

[https://jdtf.or.jp/report/whitepaper/file/%EF%BD%85%E3%82%B7%E3%83%BC%E3%83%AB%E5%88%A9%E7%94%A8%E8%80%85%E3%82%AC%E3%82%A4%E3%83%89%E3%83%A9%E3%82%A4%E3%83%B3\\_v1.pdf](https://jdtf.or.jp/report/whitepaper/file/%EF%BD%85%E3%82%B7%E3%83%BC%E3%83%AB%E5%88%A9%E7%94%A8%E8%80%85%E3%82%AC%E3%82%A4%E3%83%89%E3%83%A9%E3%82%A4%E3%83%B3_v1.pdf)

頼済み証明書ストアを参照して発行元認証局が信頼できることを確認し、eシール自体の有効性の検証も行う。VCの検証方法を「図 5-6 VCの検証方法」に示す。検証者はVCを検証するサービス等を介して、VCの正当性を確認する。具体的には、VDRから検証鍵の取得および失効情報を取得し、署名検証および失効検証を行う。あわせて、トラステッドリストから信頼できる発行者情報を参照し、発行元の信頼性を確認する。さらに、VC自体の有効期間の検証とともに、発行者がVCを付与した対象と、VCの提示者が同一であること（Holderがクレデンシャルに対してバインドされていること）を確認する。

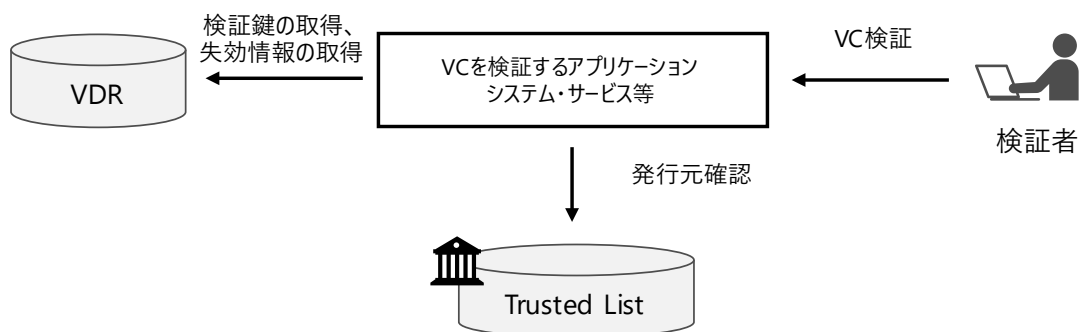


図 5-6 VCの検証方法

また、On-Goingの検証においても、On-Boardingと同様に組織の実在確認を行う。検証者は、提示されたVCやeシールをもとに組織および個人の実在を確認する。実在性確認には、4.12で説明した「日本における組織に対する実在確認のための識別子」が利用できる。On-Goingでのeシールを活用した実在性確認については、eシール利用者ガイドラインv1<sup>30</sup>を参照されたい。eシールでは、署名検証とあわせて、eシール用電子証明書の情報をもとに信頼できる情報源より企業情報を参照する。検証者はOn-Goingにおいて企業情報を参照した上で、実在性を検証する。「図 5-7 VCの実在性検証」に、On-GoingでのVCの実在性検証を示す。VCでも同様に、検証者は企業名や企業識別番号の記載されたVCから、信頼できる情報源を参照して法人の実在性を確認する。

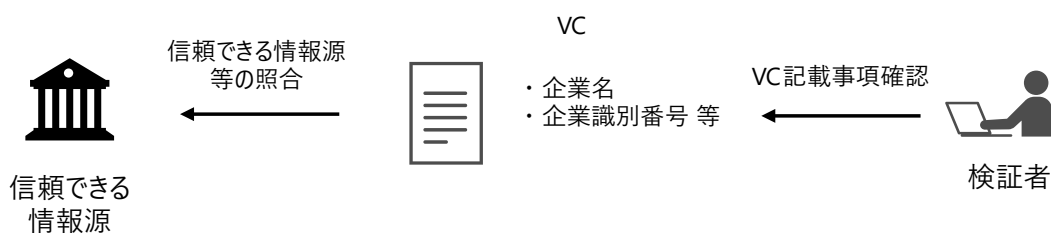


図 5-7 VCの実在性検証

<sup>30</sup> JDTF, eシール利用者ガイドライン v1,

[https://jdtf.or.jp/report/whitepaper/file/%EF%BD%85%E3%82%B7%E3%83%BC%E3%83%AB%E5%88%A9%E7%94%A8%E8%80%85%E3%82%AC%E3%82%A4%E3%83%89%E3%83%A9%E3%82%A4%E3%83%B3\\_v1.pdf](https://jdtf.or.jp/report/whitepaper/file/%EF%BD%85%E3%82%B7%E3%83%BC%E3%83%AB%E5%88%A9%E7%94%A8%E8%80%85%E3%82%AC%E3%82%A4%E3%83%89%E3%83%A9%E3%82%A4%E3%83%B3_v1.pdf)

### (3) データの署名

データスペースにおけるデータに対する署名には、DID に紐づく署名鍵（参照：4.8.8）およびeシールに紐づく署名鍵（参照：4.6）を使用する。

それぞれの使い分けを「図 5-8 DID に紐づく署名鍵と eシール署名鍵の使い分け」に示す。データへの署名用途に応じて、DID に紐づく署名鍵と eシール署名鍵を使い分ける例であり、DID に紐づく署名鍵に基づく VC 発行（Self-issued VC 等）と、eシール証明書に基づく署名を並行して運用する。データスペース内で授受するデータは DID に紐づく署名鍵による署名、データスペース外や法的裏付けが必要なユースケースは eシール署名を活用する。

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。こうして、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。

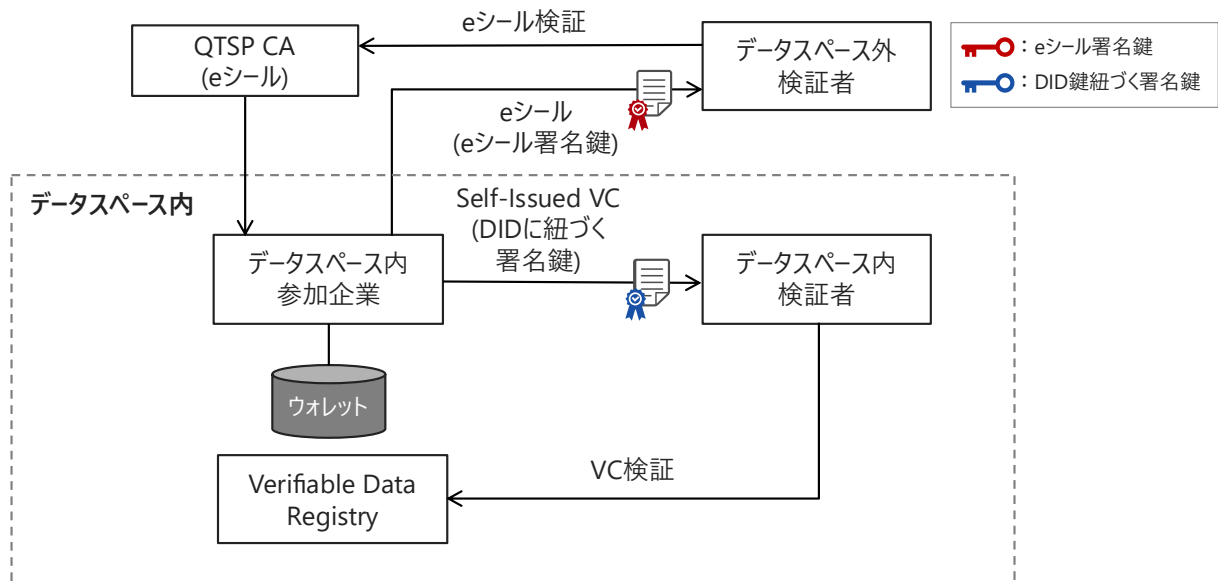


図 5-8 DID に紐づく署名鍵と eシール署名鍵の使い分け

### 5.2.3 Off-Boarding

データスペースにおける Off-Boarding の流れを「図 5-9 Off-Boarding の全体像」に示す。データスペースへの参加における On-Boarding と共に、参加終了処理である Off-Boarding も重要となる。データスペースへの参加組織からの申請に基づく Off-Boarding に加え、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にはデータスペース運用者による申請に基づく Off-Boarding が行われる。

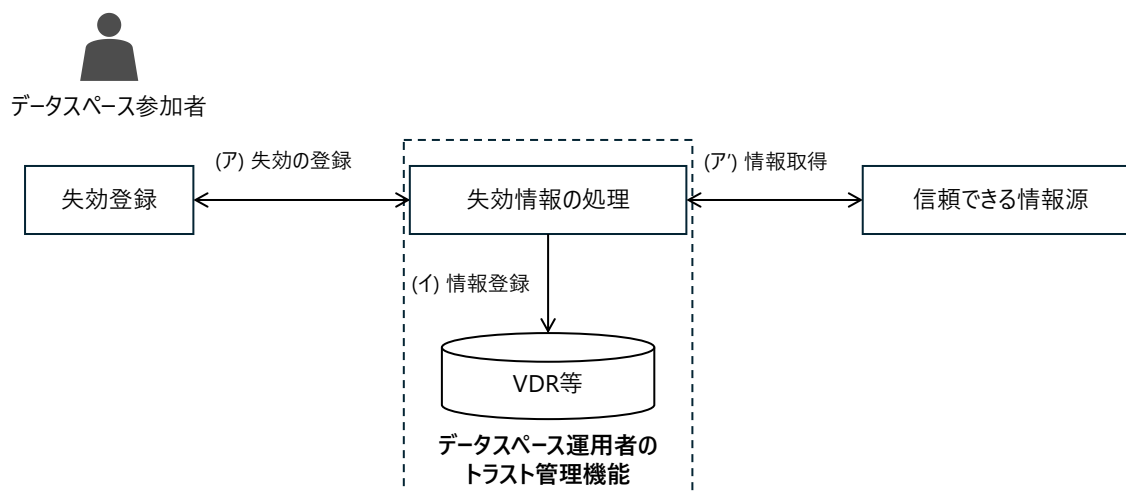


図 5-9 Off-Boarding の全体像

本項では、Off-Boarding において、トラストを担保する上で重要となる以下の 3 点について説明する。

- (1) 参加者起点の失効登録（「図 5-9 Off-Boarding の全体像」の(ア)に該当）
- (2) データスペース運用者起点の失効登録（「図 5-9 Off-Boarding の全体像」の(ア')に該当）
- (3) 失効情報の登録（「図 5-9 Off-Boarding の全体像」の(イ)に該当）

#### (1) 参加者起点の失効登録

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を行う。データスペース参加者はデータスペース運用者のトラスト管理機能に問い合わせたうえで、失効を登録する。

#### (2) データスペース運用者起点の失効登録

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。また、データスペース運営者が自らの判断に基づき、参加組織の関与がデータスペースへ悪影響を及ぼすことを判断した場合も、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

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。

Off-Boarding はアイデンティティの「停止」プロセスあるいは「削除」プロセスとなる。両者の違いを、少なくとも手続上はエンティティに明確に判別されるようにする。併せて、「停止」プロセスは「再開」プロセスと共にエンティティに認識されるようにする。また、Off-Boarding は、その性質上データスペースが稼働している日時において実施可能であること、可能な限りリアルタイムで反映されること、Off-Boarding されたエンティティには遅滞なく知らされることが必要である。

## 5.2.4 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 を発行する。(Off-Boarding におけるプロセスも参照)。

## 5.3 データスペースのトラスト機能

### 5.3.1 IAL・AAL の推奨レベル

データスペースにおける IAL および AAL の適用方針は、セキュリティ、信頼性、運用コスト、相互運用性のバランスを最適化する観点から、原則として IAL2 および AAL2 を推奨基準とする。

身元確認においては、IAL2 は公的 ID や信頼できる情報源に基づく属性検証を要求するため、虚偽申告のリスクを大幅に低減することができる。IAL3 のような対面や高度なデバイスの前提を避けることで参加障壁と運用コストを抑えられる。日本における非対面の自然人の身元確認では、マイナンバーカードを用いた電子署名を活用することで、IAL3 を実現<sup>31</sup>できるため、要件次第で IAL3 を検討し、より強固な実在性確認を組み込むことが望ましい。

本人確認においては、AAL2 は多要素認証を要求するため、パスワード単独の脆弱性を大幅に軽減することができる。また AAL3 のような専用ハードウェア必須等の高コスト運用を回避できるため、ユーザビリティの面でも合理的である。

例えば、メンバーシップ VC 発行における身元確認では、原則として IAL2 を適用する。低リスクなユースケース(役割の自己申告や組織内限定の任意属性など)には IAL1 で足りる場合もあるが、データスペースのデータスペース運用者のトラスト管理機能からの発行が前提となる場合は原則 IAL2 とし、トラストサービス層の照合を必須とする。

アプリケーションサービス層へのアクセスに関しては、原則 AAL2 を適用してフィッシング耐性のある認証器を活用する。また、機密性の高い業務については、必要に応じて AAL3 を検討する。

参加者の負荷を最小化する観点から、対面必須や専用デバイスを前提とする適用は限定的にとどめ、原則 IAL2/AAL2 を基準にしつつ、高リスク領域でのみ IAL3/AAL3 を適用することを推奨する。また、適用レベルは各アプリケーション要件とリスク評価に基づき調整し、データスペースのガバナンスにおいて最低保証レベルを定めたうえで、データスペースを運用する。

### 5.3.2 データスペース運用者のトラスト管理機能

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。

データスペース運用者のトラスト管理機能が主に担うべき役割を説明する。

<sup>31</sup> デジタル庁, トラストを確保した DX 推進 SWG (第 7 回) 事務局説明資料

[https://www.digital.go.jp/assets/contents/node/basic\\_page/field\\_ref\\_resources/ccf78f94-ac80-499d-b0db-c53840586058/20220322\\_meeting\\_trust\\_dx\\_outline\\_01.pdf](https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/ccf78f94-ac80-499d-b0db-c53840586058/20220322_meeting_trust_dx_outline_01.pdf)

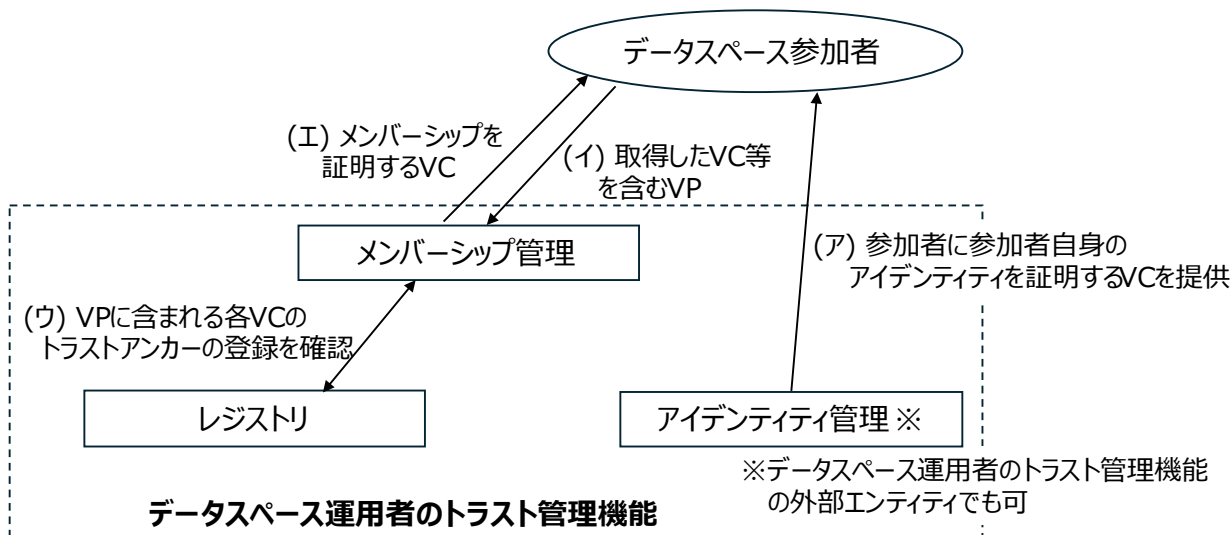


図 5-10 データスペース運用者のトラスト管理機能の主な役割

「図 5-12 データスペース運用者のトラスト管理機能の主な役割」に示す通り、データスペース運用者のトラスト管理機能は以下 (ア) ~ (エ) を担当する。

(注: 「図 5-12 データスペース運用者のトラスト管理機能の主な役割」及び (ア) ~ (エ) は、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。Gaia-X の事例については付録 1A.3 を参照)。

- (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 (参照: 5.2.1) 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の主な役割は、信頼の起点となるトラストアンカーをレジストリで確立/保持するトラストアンカー管理と、参加者のメンバーシップ管理である。以下では、データスペース運用者のトラスト管理機能を説明する。

- ① データスペースにおける信頼の起点確立 (Registry Service、「図 5-12 データスペース運用者のトラスト管理機能の主な役割」ではレジストリに相当)
- ② データスペースにおける参加者のコンプライアンス準拠の確認 (Compliance Service、「図 5-12 データスペース運用者のトラスト管理機能の主な役割」ではメンバーシップ管理に相当)
- ③ データスペースにおける参加者の認可判断 (ノタリーサービス、「図 5-12 データスペース運用者のトラスト管理機能の主な役割」ではアイデンティティ管理に相当)
- ④ (オプション) 参加者の On-Boarding のためのポータル・UI
- ⑤ (オプション) 参加者の Credential を格納または第三者に提示するための Wallet

オプションとして上記④⑤やその他などもあるが、ここでは必須の①②③について述べる。

### ① データスペースにおける信頼の起点確立 (Registry Service)

Gaia-X では、Gaia-X Registry Service として、エコシステムの中に以下を提供<sup>32</sup>する。

- Shapes：提示される VC 構造の有効性を確認できるサービス
- Trust Service Providers：トラストフレームワークに基づき資格情報等を発行することが許可されている関係者のルート証明書を確認できるサービス
- Revocation lists：失効した証明書リストを確認できるサービス
- Provided APIs：2 つの API を提供する。(i) 証明書がトラストアンカーに属しており、失効していないことを確認できる API。(ii) 信頼できる発行者情報 (例えば、GXDCH) を確認できる API。

データスペース運用者のトラスト管理機能等は、データスペースで授受される e シールおよび VC の検証のために、検証データを管理・公開しなくてはならない。すなわち、データスペースにおける VC エコシステムの Verifiable Data Registry およびトラステッドリストに相当するエンティティが必要である。

### ② データスペースにおける参加者のコンプライアンス準拠の確認 (Compliance Service)

参加者のコンプライアンス準拠や適合性を確認するために、以下を提供する。

- データスペースへの参加者 (参加申請者) が準拠すべきルール (コンプライアンス) を設計する。必要に応じて、コンプライアンスに準拠レベルを設ける。それにより、データスペース参加者をコンプライアンス準拠レベルに応じて分類・管理する。
- 参加者から提供される VC 等の内容を Registry に格納されている構造やリスト、発行者と比較し、参加者がデータスペース運用者の設計したコンプライアンスやレベルに準拠しているかを検証する。
- 検証の結果、参加者がルールやレベルに準拠していることを証明する VC (例：Membership Credential や Compliance Credential など) を参加者に発行する。

### ③ データスペースにおける参加者の認可判断 (ノータリーサービス)

参加者の認可判断のために、以下を提供する。

- 参加者のアイデンティティに関わる情報、特に参加者 (企業や組織) の実在性確認などにおいて外部の信頼できる情報源を用いて正当性を検証する。
- 検証の結果、そのアイデンティティや資格等を証明する VC を発行し、参加者が記載または宣言した情報を第三者として保証する。

データスペース参加者がアイデンティティやコンプライアンス準拠を証明するために複数の VC をエビデンスとして取得しなければならないケースもある。VC の発行 (ノータリーサービス) については、すべての VC 発行をデータスペース運用者のトラスト管理機能内で行う必要はなく、VC の発行者が外部に存在してもよい。例えば、欧州の EUDIW における PID や EAA (QEAA、non-qualified EAA) の発行者など、別の枠組み (eIDAS 規則) で役割が担保されている VC 発行者が一部の役割を担える場合もある。

データスペース運用者のトラスト管理機能が発行するメンバーシップ VC の署名鍵として、Gaia-X では DID (did:web) に紐づく署名鍵が検討されているが、ユースケースによっては e シール署名鍵を使用することもできる。

また、データスペースにおける VC エコシステムでは、VC や e シールの発行者、CA 等のトラストを検証しなくてはならない。VC 等の検証においては失効情報の管理・公開も重要であり、レジストリが、データスペースにおけるエンティティの信頼 (トラスト) の起点を確立する役割を担い、失効情報を含む様々な情報を管理する。レジストリは一つとは限らない。データスペース外の検証者の有無、ノータリーの認定者や VC の発行者などによって信頼の検証方法は異なり、データスペース運用者の外部にあるレジストリを併用する

<sup>32</sup> Gaia-X Architecture Document - 25.05 Release, 6.9.3 Using the Registry,

[https://docs.gaia-x.eu/technical-committee/architecture-document/25.05/gaia-x\\_technical\\_compatibility\\_specifications/](https://docs.gaia-x.eu/technical-committee/architecture-document/25.05/gaia-x_technical_compatibility_specifications/)

場合もある。ユースケースによっては、データスペース運用者のトラスト管理機能内で完結することもある。

従って、データスペース運用者は、データスペースやその参加者に求める要件やルール（コンプライアンス）に基づいて、外部のレジストリやノタリーを活用するか否かを設計しなくてはならない。その設計は、参照可能な法人番号基盤やトラストフレームワークの確立に依存する。これらの前提を明確にすることで、データスペース運用者のトラスト管理機能は、具体的な設計と円滑な運用が可能となる。

### 5.3.3 コネクタ認証のあるべき姿

データスペースにおいて、分野横断のデータ流通を実施するために、コネクタを認証する。本項ではコネクタの認証のあるべき姿として、「図 5-11 コネクタ認証の種類」に示すコネクタ間の認証およびコネクタへのユーザ認証について説明する。コネクタに関しては、自組織のコネクタを使うケースと、コネクタサービス提供者のコネクタを使うケースがある。コネクタサービス提供者のコネクタを使う場合、コネクタはFW外のエンティティである。「図 5-12 コネクタサービス提供者のコネクタを使う場合のシステム構成図」に示すように、自身のデータはFW内に存在するため、ビジネスアプリケーションとコネクタの間に認証が必要となる。そこで、本ドキュメントでは、コネクタ間の認証・認可だけでなく、コネクタへのユーザ認証についても記載する。

- (a) コネクタ間の認証・認可
- (b) コネクタへのユーザ認証

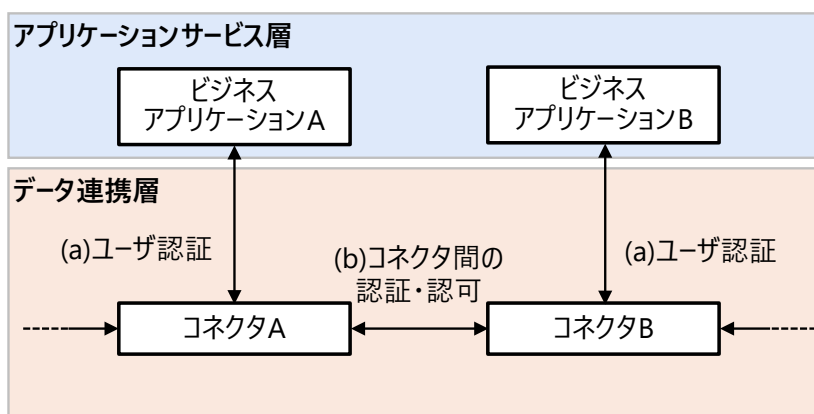


図 5-11 コネクタ認証の種類

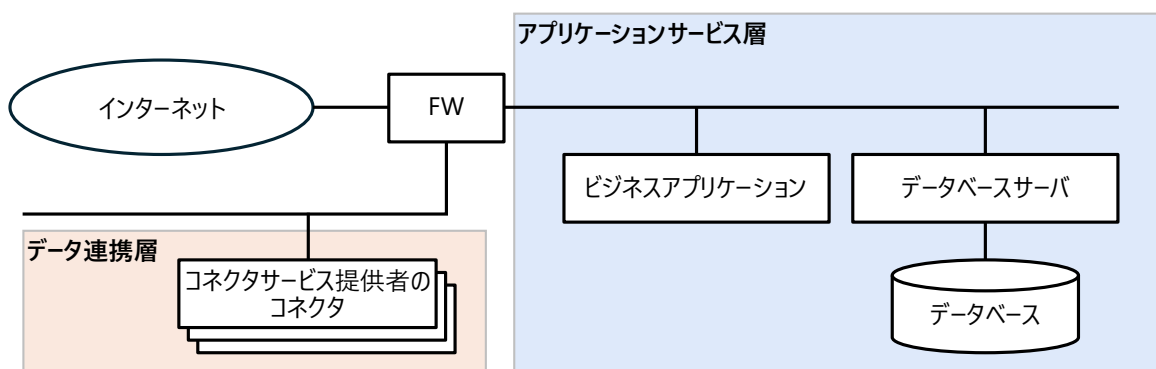


図 5-12 コネクタサービス提供者のコネクタを使う場合のシステム構成図

#### (a) コネクタ間の認証・認可

コネクタ間の通信は、暗号化されたトンネルを介する。これには、TLS や mTLS (相互 TLS 認証) などを用いる。TLS は、通信の暗号化とサーバ認証を提供する仕組みである。クライアントがサーバに接続する際に、サーバが証明書を提示し、それをクライアントが検証することで「正しいサーバと通信している」ことを確認する。ただし、この仕組みではクライアント側は認証されず、誰が接続しているのかはサーバ側からは分からない。一方、mTLS は TLS を拡張し、サーバだけでなくクライアントも電子証明書を提示する点

が異なる。これにより、サーバは接続してきたクライアントを電子証明書によって確認でき、双方が互いの正当性を検証し合うことができる。データスペースのような複数組織が相互に接続する環境では、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 が有効である。TLS 証明書を発行する認証局としては、以下の2つがある。

- パブリック CA（商用/非営利）
- データスペース内部のプライベート CA

パブリック CA が発行する TLS 証明書は相互運用性が確保されているため、データスペース外とも接続することができる。また、発行・失効・監査はパブリック CA が提供するため、運用負荷が小さい。一方で、大量発行時にコストが膨らむ可能性がある。

データスペース内部のプライベート CA は、コスト面でパブリック CA に勝るが、データスペース外と接続するときの相互運用性が確保されていない。コネクタ数が多く、データスペース内でのみデータをやり取りする場合は、データスペース内部のプライベート CA を活用する。外部接続も必要になる場合は、データスペース内の接続にはプライベート CA、データスペースを跨ぐ接続にはパブリック CA を活用するなど、ハイブリッド運用が現実的である。

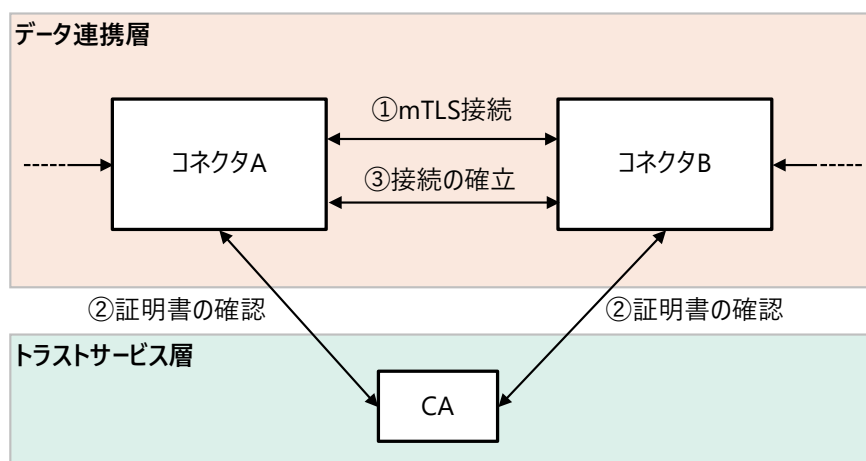


図 5-13 コネクタ認証

#### (b) コネクタへのユーザ認証

データスペースは、組織間でのデータ共有・連携を前提とし、業務上重要なデータへのアクセス等を含む。不正アクセスやなりすましは組織横断の漏えい・不正流通につながるため、フィッシング耐性のある認証方法を活用し、多要素認証の導入を前提とするべきである。また、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。したがって、AAL（詳細は 5.3.1 節を参照）を組織横断的に高いレベルに設定することで、相互信頼の土台を確保するべきである。

### 5.3.4 権限管理

データスペースでは、「データの所有者本人」が常にすべての操作を行うとは限らない。誰がどのデータにアクセスできるのか、また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げる。さらに、委任・代行の仕組みを活用すれば、本人が不在でもデータスペース上でのデータ授

受等を可能にできる。これらの仕組みがない場合、本人の ID やパスワードを共有するといった運用に陥りやすく、セキュリティリスクが高まる。

権限管理を明示的に扱うことで、最小権限の原則を徹底でき、いつ・誰が・どの権限を・誰に付与したかという証跡（監査ログ）も残せる。加えて、AI エージェントが自律的にデータスペースへアクセスし、契約・同意・電子署名等の手続きを実行するユースケースも想定される。このとき、委任関係やアクセス権限の有無を VC 等により機械可読な形で提示・検証可能にしておけば、AI エージェントによる認可判断と監査可能性を両立できる。本項では、VC を活用した権限管理の一例として、データスペースにおける委任と代行を説明する。

- (1) データスペースにおける委任
- (2) データスペースにおける代行

### (1) データスペースにおける委任

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。VC を活用した委任には、以下 2 つの方法がある。

- 委任者自身が電子委任状 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が電子委任状 VC を発行する。

表 5-2 に電子委任状法<sup>33</sup>から想定した VC を活用した委任パターンを示す。それぞれについて説明する。

**表 5-2 eIDAS2.0 と電子委任状法を照らし合わせたときの VC を活用した委任の想定**

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

「図 5-14 委任者が委任 VC を発行する場合」に委任者自身が電子委任状 VC を発行する場合の概念図を示す。また、委任の流れを以下に示す。

- ① On-Boarding：委任者は自身の検証鍵を VDR に登録する。
- ② On-Boarding：委任者は委任 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。

<sup>33</sup> デジタル庁、電子委任状法の概要について、

[https://www.digital.go.jp/assets/contents/node/basic\\_page/field\\_ref\\_resources/62459b33-c85b-421e-bd5d-e9d00d9d0ba5/e67ba9d6/20230815\\_meeting\\_digitalpoa-law\\_outline\\_02.pdf](https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/62459b33-c85b-421e-bd5d-e9d00d9d0ba5/e67ba9d6/20230815_meeting_digitalpoa-law_outline_02.pdf)

委任者が委任 VC を発行する場合、委任 VC が Self-Issued VC となるため、契約相手方がどのように信頼するかが課題となる。また、委任者自身が委任 VC を発行するため、Issuer が乱立する（=法人/従業員の数）点も課題である。

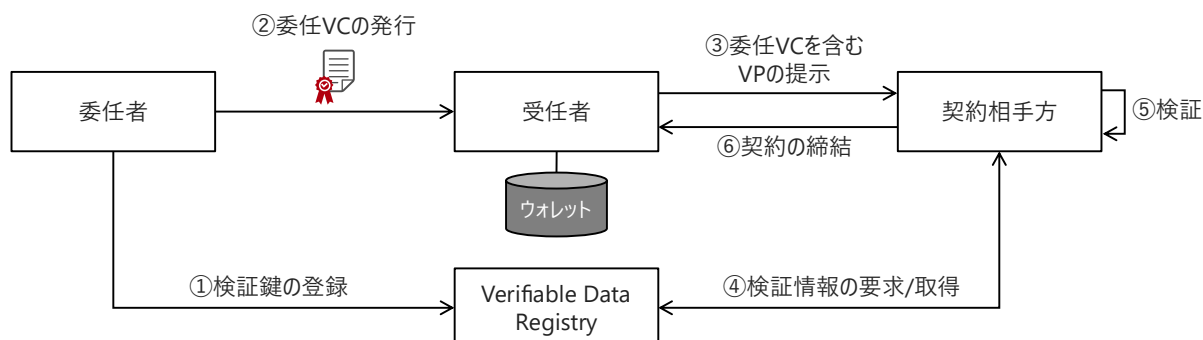


図 5-14 委任者が委任 VC を発行する場合

「図 5-15 データスペース運用者が委任 VC を発行する場合」にデータスペース運用者が委任 VC を発行する場合の概念図を示す。委任の流れを以下に示す。

- ① On-Boarding :
  - ・委任者は受任者に代理権を授与する。
  - ・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。
  - ・データスペース運用者は検証鍵を VDR に登録する。
- 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。

データスペース運用者が委任 VC を発行する場合、委任 VC は QTSP 相当の発行者が発行したものとなるため、契約相手方は委任行為を信頼することができる。一方で、すべての委任行為にデータスペース運用者が介在すると発行負担が大きくなるため、どのレベルの委任行為でデータスペース運用者が発行する委任 VC を活用するか決めなくてはならない。

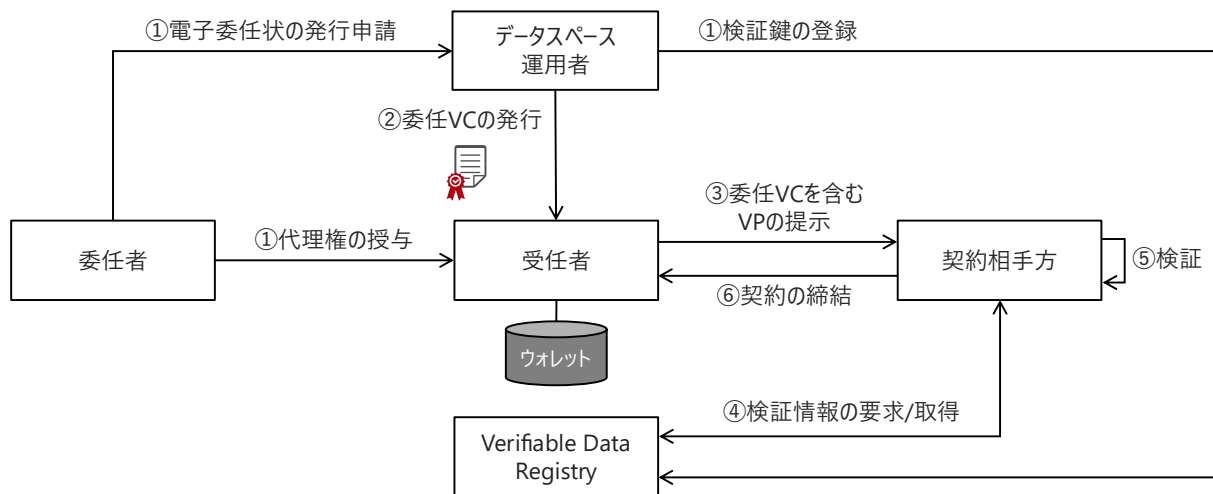


図 5-15 データスペース運用者が委任 VC を発行する場合

上記より、2社間のみなどの極小的な範囲の委任行為の場合は「委任者による委任 VC の発行」、公的な委任行為の場合は「データスペース運用者による委任 VC の発行」が適当である。また、Off-Boarding として、受任者への委任を取り下げる場合、委任者もしくはデータスペース運用者は VDR に委任 VC の失効情報を登録する。

Gaia-X における Gaia-X Power of Attorney format<sup>34</sup>を参考に、委任 VC における必要項目を以下に示す。

- 委任 VC そのものを一意に識別する ID
- 委任者を一意に識別する ID
- 委任 VC に付された署名を検証するための鍵情報
- 受任者を一意に識別する ID
- 受任者の署名を検証するための鍵情報
- 委任される権限の一覧
- 発行日
- 有効期間

## (2) データスペースにおける代行

データスペースにおいては、「委任」だけでなく「代行」の仕組みも必要である。委任は利用者本人が意思を示し、その範囲内で第三者が権限を行使することを意味するが、実際の運用においては、利用者が常にその意思表示や操作を即時に行えるとは限らない。大規模なデータ連携やリアルタイム性が求められる場面では、代表者本人の介在を前提とした委任だけでは処理が滞り、サービス品質の低下や機会損失につながる。

このような場合に必要となるのが「代行」である。代行では、あらかじめ合意されたルールや条件に基づき、代行主体が代表者に代わってデータの利用や提供を実行する。これにより、迅速かつ継続的なデータ取引やサービス提供が可能となる。

<sup>34</sup> Gaia-X Compliance Document - 25.03 Release, 10. Gaia-X Power of Attorney format, [https://docs.gaia-x.eu/policy-rules-committee/compliance-document/25.03/annex\\_power\\_of\\_attorney\\_format/#gaia-x-power-of-attorney-format](https://docs.gaia-x.eu/policy-rules-committee/compliance-document/25.03/annex_power_of_attorney_format/#gaia-x-power-of-attorney-format)

### 5.3.5 データスペース共通サービスのトラスト

データスペースでは、データスペース自体の利便性を高めるためのサービス（例. カタログサービス、来歴管理）が提供される。これらのサービスを共通サービスと呼ぶ。共通サービスにおけるトラストには、技術面、法的・組織的規約の側面といった多様な面がある。技術面では、コネクタやデータレジストリなどの共通技術標準とプロトコルが、データの真正性、完全性、利用の適切さを保証する。法的・組織的な側面では、データガバナンスの枠組み、利用ポリシー、責任の所在などが定義され、データの利用に関する透明性と説明責任を確保する。共通サービスにおけるトラストは、データスペースの参加者が個別に信頼関係を構築する負担を軽減し、スケーラブルかつ効率的にデジタルトラストを創出する基盤として重要である。

### 5.3.6 トラストサービス自体の認証・監査

トラストサービスの認定、監査は、その信頼性と安全性を保証するために重要である。EU では eIDAS 規則により、トラストサービス全体の法的効力と信頼性を確立している。日本ではデータスペースに関連する各トラストサービスについて、以下に示す認定を行っている。

- 電子署名：電子署名法により定められ、主務大臣による認証業務の認定が行われている。
- e シール：総務大臣による認証業務の認定が行われている。
- タイムスタンプ：総務大臣による認証業務の認定が行われている。

## 6 データスペースにおけるトラストの課題と展望

データスペースの社会実装に向けた動きが加速する中、その構築と運用において検討すべき課題は多岐にわたる。本章では、将来あるべきデータスペースの姿を前提とし、特に「トラスト」の観点から、現在直面している課題や留意すべき点について記載する。

### 6.1 データ管理

データ管理は、データスペースの設計において最も基本的な観点の一つである。以下に、データ管理の観点から課題を記載する。

#### 6.1.1 現状へ対応するアーキテクチャ

データ主権を確保するためには、データが各所に分散して管理される「分散型」が望ましい。しかし、分散型の理想形だけを追求しても、既存のビジネス慣習やシステム環境と合致せず、現状にマッチしないケースも多い。現時点での社会実装においては、すべてを分散させるのではなく、データを集約管理する「集中型」、あるいは分散型と集中型の組み合わせである「連邦型」や「ハイブリッド型」のアーキテクチャによる実装が必要となる。

トラストアンカーや信頼できる情報源の整備・標準化の状況を勘案しながら、現時点でどのような場合にどのアーキテクチャを採用すべきか、将来的にどのように変化させていくべきか、の整理を行わなくてはならない。

#### 6.1.2 インテグリティ

データスペースは、各参加者が自らのデータを分散して管理・提供する「分散型エコシステム」であることを基本理念としており、データの生成から流通、そして利活用に至る全プロセスを通じて、各参加者によるデータそのもののインテグリティ（真正性と完全性）の維持は重大な課題である。

現在、コネクタを用いた「経路のセキュリティ」の確保や、eシールや電子署名、タイムスタンプといったトラスト技術を組み合わせた非改ざん性の保障などが活用されているが、これらは主に流通時の保障に留まっている。さらに履歴・来歴データなどと組み合わせてデータの全ライフサイクルにおけるインテグリティ保証を確保し続けるための運用ルール・技術仕様の確立が必要である。

#### 6.1.3 参加者のセキュリティ確保とガバナンス

分散型データ管理の実現には参加者間の経路のセキュリティを確保する「コネクタ」と呼ばれる接続技術の導入が必要だが、データスペース全体におけるセキュリティ確保はそれだけでは不十分である。データスペースにおいては、各参加者（ハイブリッド型や集中型であれば参加者とセンターの両者）が通信路と自身のシステムのセキュリティ確保の責任を負っている。しかし、リソースに限りのある中小企業においては、基本的なセキュリティ対策すら取り切れていないケースが見受けられるのが現実であり、基本的なセキュリティ確保と合わせての社会実装のロードマップが必要となる。

また、技術面だけでなく、業界ごとの慣習とすり合わせたデータやセキュリティの管理のためのガバナンスルールの整備も求められる。そこでは十分なセキュリティの確保がデータスペース参加条件となるとともに、必要に応じて「相手」の「現時点」でのセキュリティを確認する「リモートアテスト (Remote Attestation)」などの仕組みの整備も必要となる。

## 6.1.4 ログ確保

データ流通においては、事前の本人確認・資格確認だけでなく、取引後のトラスト（信用）の確認・検証のためのログ確保も必要である。紛争解決については後述するが、その基盤となるログ（データ利用の履歴・来歴）を確保するための技術的・制度的基盤も整備しなくてはならない。

## 6.2 データスペースのトラストフレームワーク

デジタル社会を支える基盤として、信頼性を担保するトラストフレームワークの整備は、国家レベルの喫緊の課題である。具体的には、官民が連携して「信頼できる情報源」やノータリーサービスを含む共通基盤を構築し、国際標準との整合を図りつつ、異なるデータスペースを跨ぐ「相互承認」を技術的・制度的に可能にするトラストサービス層を構築することが求められる。データスペースの社会実装を加速させるためには、こうしたトラストフレームワークを、データスペースでのガバナンスや実装に統合し、活用していくことが必要である。

### 6.2.1 トラストレベル

データスペース全体の信頼性を担保するためには、参加者やシステムのトラストの度合いを認定する仕組みが必要である。しかし現状では、適切な認証機関の整備が整っていない。必要なトラストを適切なトラストレベル（信頼の水準）で提供する枠組みを整える施策が必要である。

### 6.2.2 信頼できる情報源

欧州では eIDAS 規則に基づき、トラストサービスプロバイダー（信頼できるサービス提供者）の制度が整備され、データスペースへの参加資格や信頼性を検証する Digital Clearing House (GXDC) も標準化されているが、日本においてはそうした制度が整っていない。

日本には、自然人を識別するためには実在性確認も含めて住民基本台帳・マイナンバーなどの仕組みがあるが、法人および個人事業主については「表 43 日本における組織識別子」に挙げた情報源が存在するものの、情報源ごとに包含する範囲が異なり、データスペースで必要な組織識別子を含む悉皆性を1つで充足可能な台帳が欠如している。また、組織識別子に紐づく属性データベースのリアルタイム性（倒産や廃業がリアルタイムに確認可能であること、合併や被合併等の情報も正確に反映されていることなど）や、収録している属性種類もデータスペースの利活用観点から併せて重要である。

なお、これらの識別子とは別に、商業登記情報を基に発行される G ビズ ID がある。G ビズ ID は、日本の事業者（法人・個人事業主）向け行政手続に用いられる共通認証基盤であり、法人の代表者等について登記情報との突合により本人確認が行われて ID（アカウント）が発行されている。業務の必要に応じ、併用・補完する形での活用が可能であるが、上記識別子とは区別される。

官民が連携して、信頼できる情報源とノータリーサービスを含むトラストフレームワークの構築を進めなくてはならない。

	台帳に関する法令	識別子に関する法令	補足	公表サイト
自然人	<a href="#">住民基本台帳法</a>	<a href="#">行政手続における特定の個人を識別するための番号の利用等に関する法律</a>	第二章：個人番号、第三章：個人番号カード	
法人	<a href="#">商業登記法</a>	<a href="#">行政手続における特定の個人を識別するための番号の利用等に関する法律</a>	第七章：法人番号	<a href="#">国税庁法人番号公表サイト</a>
個人事業主		<a href="#">消費税法</a>	適格請求書発行事業者の登録等(但し悉皆性無し)	<a href="#">国税庁適格請求書発行事業者公表サイト</a>

## 6.3 認証・検証

### 6.3.1 認証技術の混在と統一化

現在のデータスペースでは、ID/パスワード型認証、電子証明書（eシール）、Verifiable Credential（VC）など、複数の認証技術が混在して利用されている。これらは技術的基盤や運用体制がそれぞれ異なり、例えばeシールの場合は発行元の認証局の信頼性や失効管理が必須となるし、VCの場合は検証用にDID Documentや信頼できる発行者情報の取得、失効情報の管理などが必要となる。

一つのデータスペース内でこれらが混在する場合、個別技術ごとの処理だけでは、運用の複雑化や検証漏れ、信頼水準のばらつきを招く。そのため、データスペース運営者は、検証の前提条件、参照すべきトランサクションやレジストリ、失効確認の方法などを整理し、統一的な運用ルールを定める必要がある。

また、実運用において、データスペースは単独で利用されるものではなく、組織内システムや既存基盤と連携して利用される。そのため、エンドユーザ、組織内システム、データスペースの各層を個別に考えるのではなく、エンド・トゥ・エンドでの認証・検証の整合性を確保しなくてはならない。

こうした課題に対応するためには、認証技術の選択指針や組み合わせ方、検証フロー、組織内システムとの接続を含めた実装上の留意点を示すガイドラインの整備が必要である。

### 6.3.2 検証プロセスの透明性

検証プロセスが適切なものであることを参加者が検証できなければならない。このとき、検証の仕組みが揃っていないと、参加者間の信頼関係構築やデータの真正性担保に支障をきたすことになる。技術的な整合性だけでなく、運用面やガバナンス面への配慮も必要となる。具体的には、失効したVCやeシールの扱い、検証結果の共有方法、検証に用いるリスト自体の信頼性など、プロセス全体の透明性と説明責任を明確にしなければならない。

## 6.4 標準化

データスペースの相互運用性を確保するためには標準化が有効な手法である。トラスト確保の観点からは特に「技術と運用」と「組織・法律」の観点での標準化が必要となる。

### 6.4.1 技術と運用の標準化

現在、電子署名、eシール、VC、Self-Issued VCなど多様なトラスト手法が混在している。個々のトラスト手法について統一された検証手順を標準化するだけでなく、複数の手法を統合的に扱うための共通プロトコルや検証手順の整備も必要である。標準化された手順やインターフェースを確立することで、特定のベン

ダーや特定の技術に依存しないデータ連携が可能になる。

また、個々の技術の運用の標準化も必要となる。具体的には、鍵管理手法、VC Issuer の実装方法、認証局の設置・運用基準、EAA(属性証明)の発行組織の要件などを標準化しなければならない。特に VC については国内において発行基準の策定が遅れていることが大きな課題となっており、早期のルール整備が必要である。

#### 6.4.2 アシユアランス・レベルの標準化

データの信頼度や保証レベル（アシユアランス・レベル）についても、現在は都度検討する形になっているのが実情である。アシユアランス・レベル自体の定義の標準化、具体的な要件と必要なアシユアランス・レベルの結びつけ方について、国内での合意形成（参加者間の合意だけでなく、業界・国家レベルでの合意）を図る標準化活動を進めなくてはならない。

#### 6.4.3 組織・法律の標準化

トラストサービスを運用する組織のありかた、特にその法律的な位置づけや責任範囲の検討、紛争解決メカニズムの策定は現状不十分である。これらの整備は国レベルで進める必要がある。

#### 6.4.4 国際標準との整合性

今後の拡張性と包摂性を担保し、国内外のユースケースに対応するために、検証やアシユアランス・レベルの国際整合を図る必要がある。技術面では W3C の Verifiable Credentials Data Model v2.0 や NIST ガイドラインといった国際標準との整合性を確保する技術標準化活動を進め、運用やガバナンスについては eIDAS 2.0 の EAA 技術運用仕様<sup>35</sup>や関連 ETSI 規定<sup>36</sup>などの国際標準との整合を図らなくてはならない。そして単なる国際標準準拠だけでなく、日本の要件を反映させるために国際標準を提案・推進する活動が必要である。

### 6.5 相互承認

サプライチェーン・ソリューションやサーキュラーエコノミー（循環経済）などを実現するためには、複数の産業や国をまたぐデータ連携が必要となる。このとき、異なるデータスペース間での「相互承認」は必須の検討事項である。

以下では、5.1.2「三層アーキテクチャ」で示した三層モデルを用いて、「トラストサービス層」、「データ連携層」、「アプリケーションサービス層」の三層それぞれでの相互承認について説明する。

#### 6.5.1 トラストサービス層の相互承認

様々なトラストサービスの相互承認の課題は、実在性、技術的信頼性の2つにまとめることができる。

実在性の相互承認においては、「信頼できる情報源」と「IAL (Identity Assurance Level)」が重要である。認証局 (CA)、DID Registry、トラステッドリストといった「信頼できる情報源」の標準化は相互承認を

---

<sup>35</sup> eIDAS2.0 (ANNEX V,VI,VII)

<sup>36</sup> ETSI TS 119 472-1 V1.2.1 (2026-02) Profiles for Electronic Attestation of Attributes;  
Part 1: General requirements

実現するための前提となる。全く同じ標準を用いているのであれば相互承認は容易だが、異なる標準の場合には標準同士の相互承認の枠組みを整えなくてはならない。このとき、特定のコミュニティ内で完結する「プライベートトラスト」ではなく、広く一般的に信頼を担保する「パブリックトラスト」を活用することで、相互承認のハードルを下げるができる。

技術的信頼性の相互承認においては、認証方式の整合が重要となる。あるデータスペースで発行されたクレデンシャルやeシール証明書等を、別のデータスペースでも検証できるようにするためには、認証レベル（AAL）の整合、検証内容や手順の共通化、プロセスの透明性確保が必要である。できるだけ国際標準仕様を活用して発行・検証プロセスを共通化するとともに、トラステッドリストや Verifiable Data Registry などの基盤整備を進め、失効情報の共有などを通じて異なる技術間でのシームレスな認証を実現する基盤整備が必要である。

## 6.5.2 データ連携層の相互承認

データ連携層の相互承認は、複数のデータスペースが共通のルールで「安全かつ安心なデータ交換」実現するために必要となる。

データ連携層における相互承認では、コネクタ、認証局、ポリシーの適用、プロトコル、利用するトラストサービスなどが対象となる。具体的には、データを実際にやりとりするコネクタ自体の正当性と認証を相互に承認し、コネクタの証明書を発行する CA も両者が認めなくてはならない。利用条件を契約だけでなく技術的に強制するのであれば、データ利用ポリシーの強制適用技術についても相互に承認する必要がある。利用するトラストサービスについても、検証手順も含めて両者で合意する必要がある。

## 6.5.3 アプリケーションサービス層の相互承認

業界慣習をもとにした固有のルールや認定、定義の違いなどが各データスペースに存在する。共通部分についての合意形成と個別部分の調整をどのように行うのかがアプリケーションサービス層の相互承認にとって大きな課題となる。

また、営業秘密の保護やコンプライアンス遵守、履歴管理などのガバナンス体制そのもののビジネスレベルでの相互承認も必要となる。

## 6.5.4 国際相互承認と日本の戦略

国際的なデータ連携においては、三層アーキテクチャの全ての層について相互承認が必要となる。特にトラストサービス層とデータ連携層の国際相互承認については、国レベルの戦略的対応が求められる。

現実的な問題として、先行する欧州のデータスペースとの相互承認が必要である。欧州の規制（GDPR 等）や「Gaia-X」の基準に対応するため、日本のeシールや法人確認の仕組みが欧州のトラストサービスと同等の信頼性を持つことを証明し、欧州側に認めてもらう必要がある。その際、Gaia-Xの「Level3」ラベル取得など、欧州域内でのデータ処理が求められるルールに対して、日本企業が不利にならないよう、認証ルールの策定に積極的に関与する、あるいは国内基盤の強化などの戦略が必要となる。

これは、個々の団体というよりは日本の国家的課題である。「6.7.3 国際連携実証」に記載した「中間層によるデータの相互交換の実現性確認」や「日本で構築した認証構造が欧州の基盤と整合することの確認」などが始まっているが、それに留まらず、日本国内におけるトラストフレームワークの構築と合わせて着実に推進しなくてはならない。

## 6.6 経済性

トラストの確保にはコストが伴う。高度なセキュリティや認証基盤の導入・維持には継続的な投資が必要であり、コストを無視した議論は現実性を持たない。

### 6.6.1 導入コストと維持管理コスト

特に中小企業にとって、アナログデータのデジタル化にかかる初期費用（導入コスト）、技術基盤の導入費用などは大きな負担である。さらに、クラウド利用料やセキュリティ監視などのランニングコスト（維持管理コスト）も継続的に発生する。

### 6.6.2 経済性とトラストレベルのバランス

すべてのデータに最高レベルのセキュリティとトラストレベルを適用するのは非効率である。高いセキュリティ・トラストレベルが必要な場面では強固な技術と手順を、そうでない場面では軽量な手法を採用するなど、ユースケースに応じてコストとトラストレベルのバランスを柔軟に選択できる設計でなくてはならない。

### 6.6.3 運用負担と ROI（投資対効果）

分散型データスペースでは、各参加者がセキュリティ管理や認証の責任を負うため、技術的リソースが不足している組織は運用が困難になる。現状、データスペースの産み出す価値やセキュリティ・認証等の投資などに対する ROI（投資対効果）が見えにくく、参加へのインセンティブが働きにくいという課題もある。

参加者の負担を軽減するために、連邦型の運用支援サービスの提供や、ブロックチェーン技術による管理の自動化など、技術的・制度的な支援が不可欠である。また、データスペースの構築や参入に対して補助金が出ることもある（国内外ともに）が、初期費用中心であり、運用フェーズ支援は期間が限られていることが多い。将来的には価値創造により投資コストは回収されるはずであるが、そうしたロードマップの作成とそれに至る戦略的支援体制を整えなくてはならない。

## 6.7 具体的な試み

課題解決に向けた具体的な実証実験や取り組みがすでに始まっている。国際連携も、具体的なビジネス課題への対応を通じて、理論から実践のフェーズへと移行を模索しつつある。

### 6.7.1 ODS(Open Data Spaces)エコシステム

日本においては、経済産業省主導の産業データスペース ODS(Open Data Spaces)が立ち上がっている。蓄電池、プラスチック、建材、家電などを注力領域とし、組織や業界をまたいだデータ連携と、システムの安全性・信頼性・相互運用性の確保を目指している。

### 6.7.2 DPP（デジタル・プロダクト・パスポート）への適用

製品のライフサイクル情報を管理する DPP(Digital Product Passport)のためのデータスペース活用の検討が進んでいる。

具体的には、プラスチック資源循環プラットフォーム「PLA-NETJ」や、自動車・蓄電池トレーサビリティ (ABtC) において、CFP（カーボンフットプリント）データの可視化や共有が行われている。また化学・素材産業などでは、製品の組成情報の秘匿（企業秘密）と環境負荷情報の開示というトレードオフを解消する

ため、データスペースでのデータ共有の際に秘密計算などの高度なプライバシー保護技術を実装する試みも進められている。

### 6.7.3 国際連携実証

代表的な事例として以下の2点が挙げられる。

事例1：日本の「ウラノス・エコシステム」と欧州「Catena-X」の接続実証

2024年にIPAとCatena-X Automotive Network e.V.の間で締結された覚書に基づき、NEDO事業の一環として実施された。EVバッテリーのカーボンフットプリント（CFP）データの交換に焦点を当て、日本企業がEUバッテリー規則へ準拠することを目指している。

異なるアーキテクチャを持つデータスペース間において、認証方式やデータモデルなどの技術課題を明らかにした。さらに、「中間層」を設けることで、双方のアーキテクチャに影響を与えずにデータを相互交換できる仕組みの実現性を確認した。

事例2：IMX（International Manufacturing-X）のデータ連携実証

製造業を中心とした日欧間の国際的なデータスペース連携の構築を目指したもので、2025年のハノーバーメッセにおいて結果報告がなされた。製品のカーボンフットプリント（PCF）などの製造データを交換するユースケースをテーマとし、データ主権の保護と利用ポリシーの制御、および信頼された主体同士による相互認証の枠組みを検証した。

トラスト確保については、分散型識別子（DID）や検証可能クレデンシヤル（VC）を活用し、日本側で構築した認証構造が欧州側の基盤と整合的に動作することを確認した。

## 7 結語

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であり、そのための基盤として、データスペースが注目されている。昨今、国内外において、環境問題、エネルギー問題などの国際的課題に対応するための仕掛けとして、バッテリーパスポート(BP)やデジタルプロダクトパスポート(DPP)などの実現が進行しており、そこで扱うデータを複数のステークホルダー間で共有、連携するために、データ流通を担う産業用データスペースに関する議論が活発になされている。

現在、さまざまに議論されているデータスペースにおいて、データスペースの参加者の認証や、流通するデータの完全性など、トラストに関する議論もされてはいる。しかしながら、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に、何を構築、運用すればよいのかという観点では、深堀が不十分であり何をどこまで実施すればよいのか不明確な状況である。

そのため、本書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の観点を中心にまとめている。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し、データスペースを構築・運用する者に対し、トラステッドなデータスペースを実現するための機能の構成や実施方法を論じている。

要求されるトラストに関する機能としては、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が上げられている。また、流通するデータの利用用途によっては、データスペース内に閉じて流通するデータと、データスペースの外部のエンティティにも利用されるデータが存在することが想定されるため、単一データスペース内で必要となるトラストに加えて、データスペース外のエンティティや異なるトラストサービスとの連携の際に考慮すべきトラストに関して論じている。

さらに、将来的な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行っている。

本書が、データスペースを実際に構築・運用する者にとって、どのようにトラストを実現すればよいのか、理解を手助けできることが叶えば幸いである。

最後に、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ると思います。今後の改定に向けて、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）

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

## 8 参考資料

- ・ IPA(2024) データスペース入門,  
<https://www.ipa.go.jp/digital/data/jod03a000000a82y-att/dataspaces-gb.pdf>
- ・ IPA(2025) データスペースガイドブック  
<https://www.ipa.go.jp/digital/data/jod03a000000a82y-att/data-utilization-and-data-spaces-guidebook.pdf>
- ・ 経団連(2025) 産業データスペースの構築に向けた第2次提言  
<https://www.keidanren.or.jp/policy/2025/026.html>
- ・ DADC(2025) ウラノス・エコシステム・データスペースズ リファレンスアーキテクチャモデル ホワイトペーパー (2025年2月28日)  
<https://www.ipa.go.jp/digital/architecture/reports/ouranos-ecosystem-dataspaces-ram-white-paper.html>
- ・ JDTF(2025) 声明「データスペース等に関する国際標準化の必要性」  
<https://jdtf.or.jp/news/2025/0306.php>
- ・ JDTF 「デジタルトラスト用語集」  
<https://jdtf.or.jp/glossary/>

# 付録

## A 欧州の既存例

トラストアンカー、トラステッドリスト、デジタルクリアリングハウスに関し、欧州を例に補足的な情報を記載する。

### A.1 トラストアンカー

「図 A-1 Gaia-X Trust Framework 図 A-1 Gaia-X Trust Framework」に示されるように、Issuer から発行される VC や Holder が提示する VP については、トラストアンカー（例えば、4.4 章のトラステッドリストに含まれるトラストサービスプロバイダー）までトレースできる 1 つ以上の暗号化材料で署名されている必要がある。Gaia-X では、Gaia-X により認定されたトラストサービスプロバイダーは Gaia-X Compliance Document 内で決定され、これらのカテゴリーに属する有効なトラストサービスプロバイダーの詳細なリストは Gaia-X Registry に記載されている。

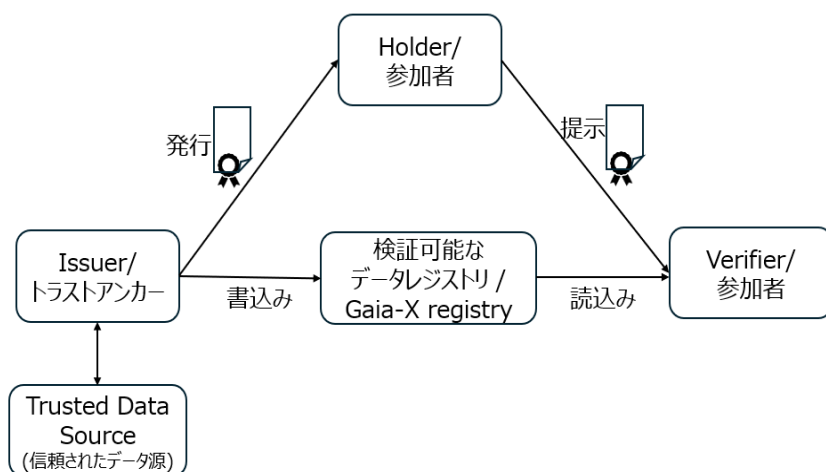


図 A-1 Gaia-X Trust Framework

情報の出所や属性に関するトラストアンカーについても触れる。Gaia-X Compliance Document - 25.03<sup>37</sup>より、Gaia-X トラストアンカーとは、特定のクレームに関する証明書を発行する資格のある者（団体/組織）として Gaia-X Association の機関によって認定された適合性評価機関または技術的手段である、と記載されている。つまり、この場合のトラストアンカーは、データスペースの運営主体によって決められたコンプライアンス要件を満足する証明情報（参加者に発行される VC）の出所として、Gaia-X が承認したノータリーや CAB を包含している。これらのプライベートな意味でのトラストアンカーは、データスペース参加者のコンプライアンスにレベルを設け、そのラベルレベルの要件に応じた証拠（の一部を）を発行する役割も担っている。

Catana-X の情報の出所や属性に関する（プライベートな）トラストアンカーは、Gaia-X デジタルクリアリングハウス(GXDCH)が担う。Catana-X のオンボーディングサービスプロバイダ/コアサービスプロバイダは、データスペース参加者のコンプライアンスチェックが Gaia-X デジタルクリアリングハウスによって実施されていることを確認しなければならない。（CX-0006 Registration and Initial Onboarding v2.0.1<sup>38</sup>より）

## A.2 トラステッドリスト

GXDCH の V2 (Loire) では、「図 A-2 Gaia-X における外部トラステッドリストの活用例」が示すように eIDAS の TSP や Mozilla Certification List の CA がトラストアンカーとして登録される。また、Gaia-X Association 自身が、Gaia-X Association メンバーに対する TSP となり得る場合もある。

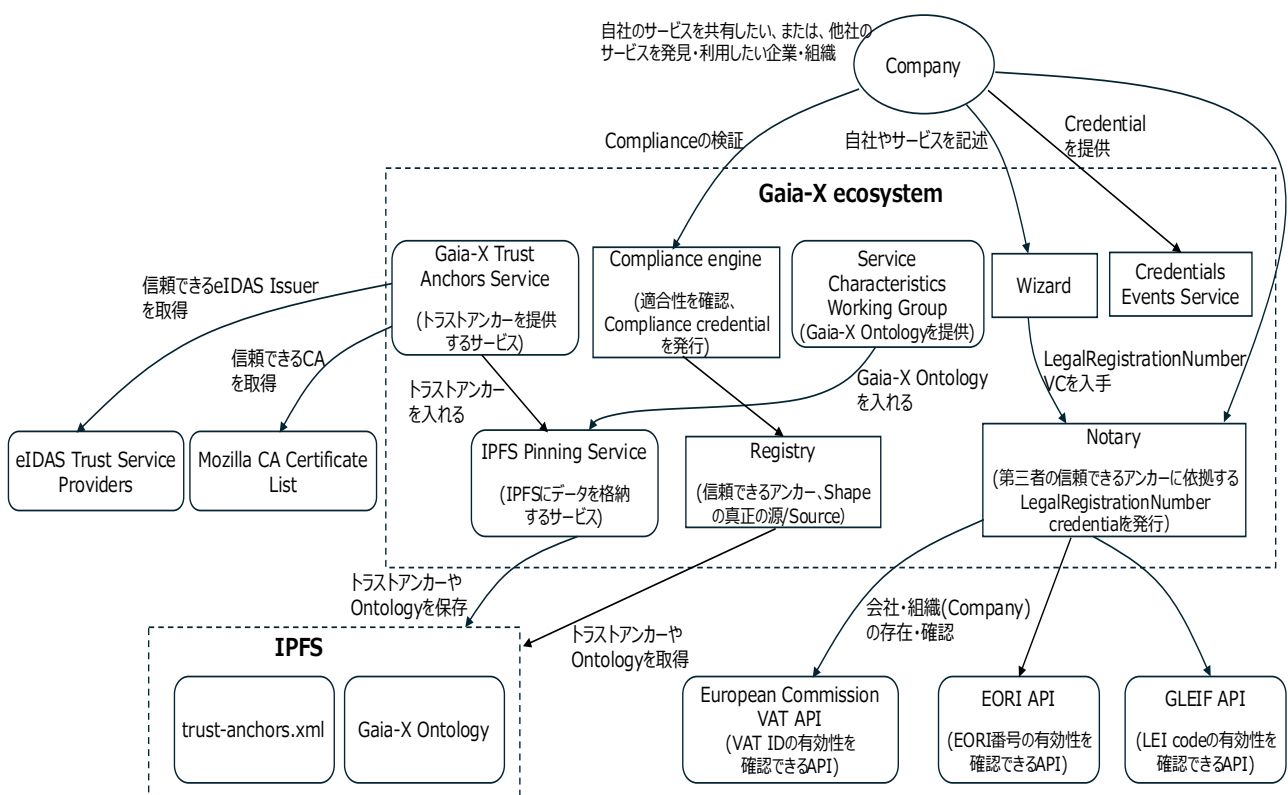


図 A-2 Gaia-X における外部トラステッドリストの活用例<sup>39</sup>

<sup>37</sup> [https://docs.gaia-x.eu/policy-rules-committee/compliance-document/25.03/Gaia-X\\_Trust\\_Anchors/](https://docs.gaia-x.eu/policy-rules-committee/compliance-document/25.03/Gaia-X_Trust_Anchors/)

<sup>38</sup> <https://catenax-ev.github.io/docs/next/standards/CX-0006-RegistrationAndInitialOnboarding>

<sup>39</sup> <https://gitlab.com/gaia-x/lab/gxdch/-/blob/main/architecture/loire/container.puml>

「図 A-5 Gaia-X Registry Service」が示すように、Registry にはトラストアンカーとして TSP や CA の情報が格納されることに加え、Trusted Issuers として Gaia-X のルールやポリシーを満たす GXDCH の情報が格納され、これがトラステッドリストに当たるものと考えられる。これら Registry の情報は、分散型のストレージサービスである IPFS (InterPlanetary File System) を用いて格納される。

### Registry に格納されたトラストアンカーや Trusted Issuers の情報は、「

図 A-4 Gaia-X Compliance Service」が示すように Compliance における Verifiable Credentials の Check 時に参照され、企業 ID や VC 発行機関 (GXDCH) の信頼性を検証する際に利用される。

## A.3 デジタルクリアリングハウス

クリアリングハウスやデジタルクリアリングハウスという用語は様々な場所で用いられている。本項目では、欧州に存在する信頼できる環境下でデータが共有・利用可能なエコシステムの構築を狙う Gaia-X による定義へ合わせた説明を行う。

### A.3.1 デジタルクリアリングハウスの役割

Gaia-X デジタルクリアリングハウス (GXDCH) は Gaia-X が定めた要件である Trust Framework に関する情報を提供し、更に Framework を満たしているかの判断機能を有する機関である。

Trust Framework は Gaia-X の定める Compliance を達成するための機能仕様、技術要件、ソフトウェアアセット等が定義されている。GXDCH はこうした Framework 要件に対する Compliance Check を実行するノードのネットワークである。[\(https://gaia-x.eu/services-deliverables/digital-clearing-house/\)](https://gaia-x.eu/services-deliverables/digital-clearing-house/)

「図 A-3 Gaia-X トラストフレームワーク」において、中央の縦軸が Gaia-X Compliance の考え方を示している。

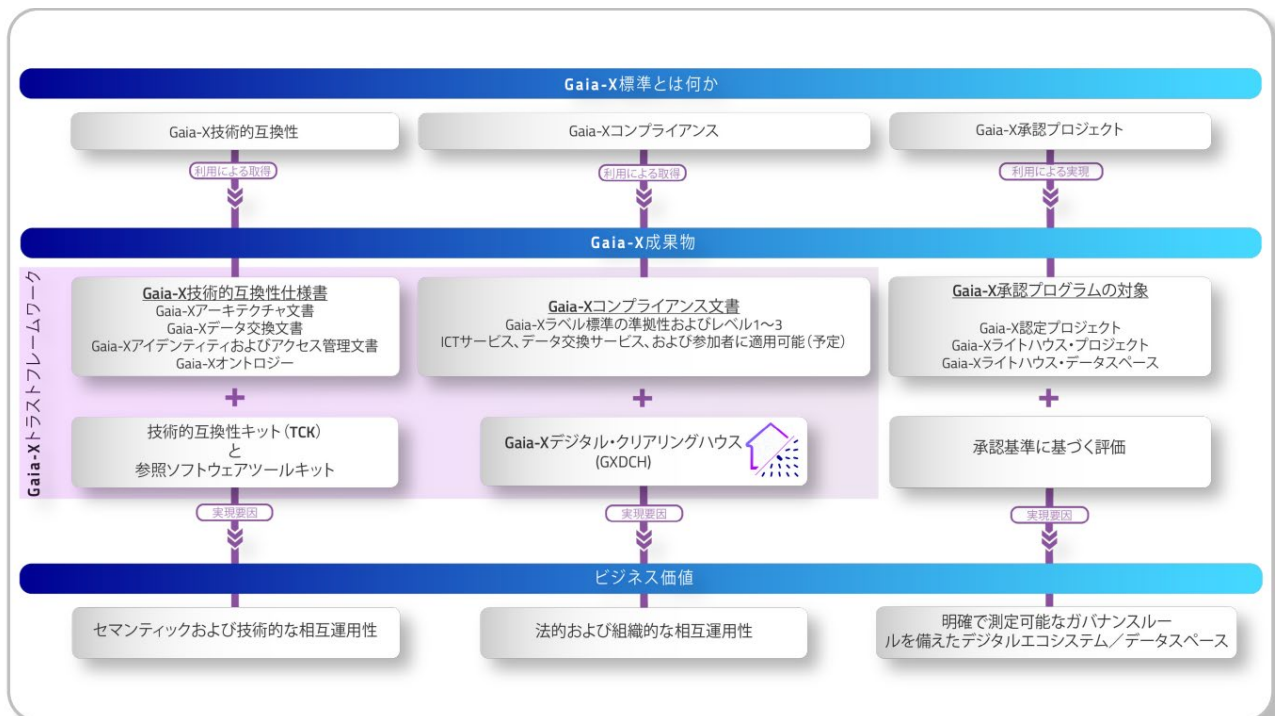


図 A-3 Gaia-X トラストフレームワーク <sup>40</sup>

<sup>40</sup> [https://gaia-x.eu/wp-content/uploads/2025/08/Gaia-X-Brochure\\_Overview\\_ONLINE\\_Japanese.pdf](https://gaia-x.eu/wp-content/uploads/2025/08/Gaia-X-Brochure_Overview_ONLINE_Japanese.pdf)

から抜粋

Gaia-Xにおいて、参加者は Verifiable Credential (VC) を用いて自身の Identity や提供するサービス、アプリケーションに係る情報を他の参加者や GXDCH に提供する。GXDCH は参加者から VC を受け取り、記載されている内容が Framework 要件を達成しているかを判断し、参加者が Gaia-X のルールに準拠している証明書として Gaia-X Compliance Credential を発行する。

Gaia-X Compliance Credential は参加者の Identity や参加者が提供するサービス、アプリケーションが Gaia-X Trust Framework に準拠していることを証明するものであり、個別のデータスペースのルールに準拠しているかまでは保証していない。しかし、データスペース側で Gaia-X Trust Framework を採用することで、GXDCH が発行する Gaia-X Compliance Credential を用いたチェックプロセスを実装できる。こうした階層構造により、データスペースのメンバーシップ要件として、Gaia-X Trust Framework を用いる、といった活用が可能となる。

### A.3.2 デジタルクリアリングハウスの機能

本項では、Gaia-X Architecture Document を参照して GXDCH が提供する主な機能を説明する。

GXDCH が提供する機能として、Registry と Compliance と呼ばれる二つのサービスが存在する。Registry は参加者が自身の Identity や提供するサービスやアプリケーションについて記載する VC の形式や、許可された VC Issuer、信頼可能な Trust Anchor のリスト等を含む。Compliance Service は Participant から提供された VC と Registry に格納されている形式、リストを比較し参加者が Gaia-X のルールに準拠しているかを検証し、Gaia-X Compliance Credential を発行する機能を持つ。

更に、Gaia-X では Notary と呼ばれるサービスが存在し、これは参加者の Identity に係る情報を外部のデータソースを用いて確認し、VC を発行する機能を持つ。これは、参加者が記載した情報を第三者として保証する重要な機能である。Notary が発行する VC も Compliance Check における検証対象となっている。

これらの機能は Gaia-X により定義された要件を満たすサービスプロバイダーによって提供される。(サービスプロバイダー一覧：<https://docs.gaia-x.eu/#/gxdch>) また、これらの機能は OSS として公開されている。

GXDCH の主なコンポーネントである Registry、Compliance、Notary Service の構成や具体的な動作については上のデジタルクリアリングハウスを参照のこと。

### A.3.3 具体的な動作

本項では、GXDCH の主なコンポーネントである Registry、Compliance、Notary Service についての目的と、具体的な動作を説明する。

(Gaia-X Architecture Loire 版のアーキテクチャを参照<sup>41</sup>)

GXDCH は、信頼できる Trust Anchor、信頼できる VC Issuer (Notary)、Trust Framework で検証対象となる VC 形式、Notary が参照する信頼できるデータソース APIなどを定義している。

---

<sup>41</sup> [https://gitlab.com/gaia-x/lab/gxdch/-/tree/main/architecture?ref\\_type=heads](https://gitlab.com/gaia-x/lab/gxdch/-/tree/main/architecture?ref_type=heads)

■ Gaia-X Compliance Service

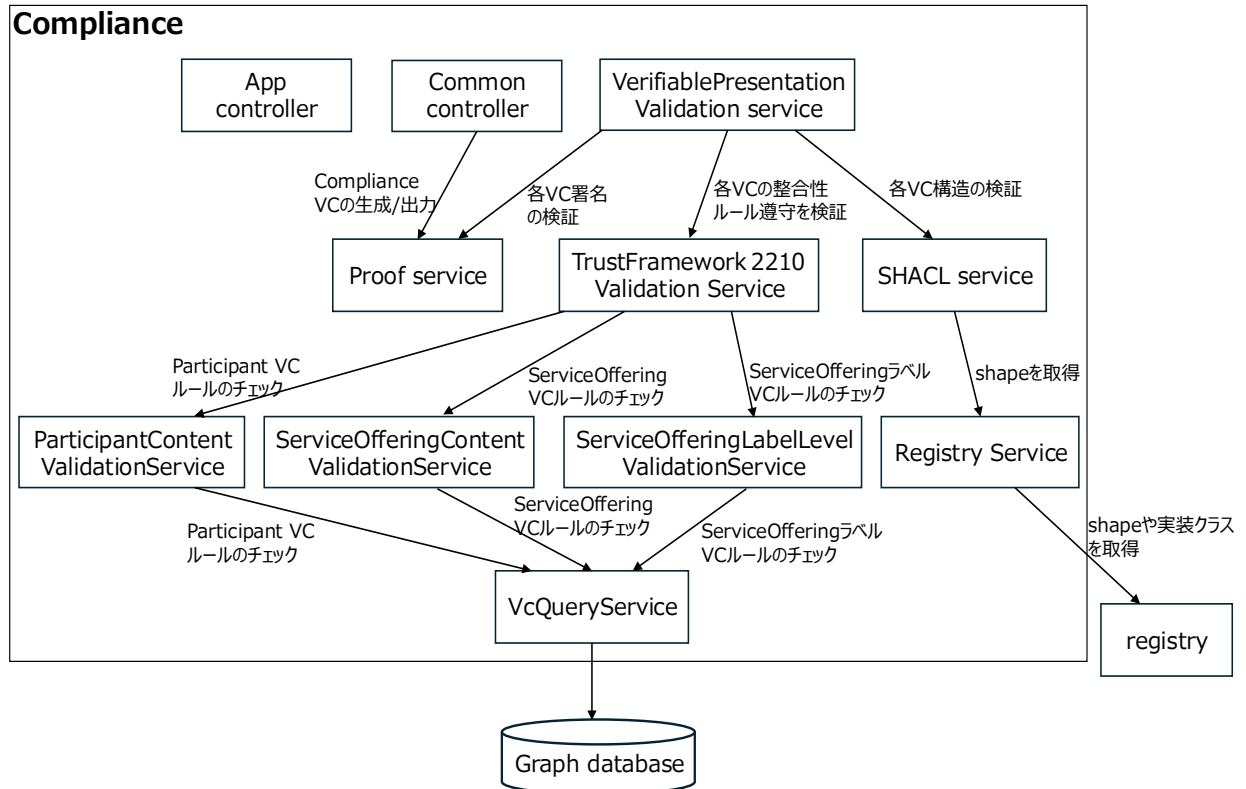


図 A-4 Gaia-X Compliance Service<sup>42</sup>

Gaia-X Compliance は Registry を参照し、Participant が Trust Framework に準拠しているかを検証、また Gaia-X Compliance VC を発行するための Component である。参加者は Gaia-X により定義されている VC (Legal Participant VC、Terms and Conditions VC、Legal Registration Number VC) を準備した上で、これらを Verifiable Presentation (VP) として Compliance Service に入力することで Compliance Check を受けることができる。

入力された VP が Compliance Check をパスすると、Gaia-X Compliance は自身が Issuer となり Compliance VC を発行する。

(注：v1 と v2 では VC の名称や発行後の形式[JSON-LD→JWT]が異なる。本文章は Tagus をベースとしている)

<sup>42</sup> <https://gitlab.com/gaia-x/lab/gxdch/->

[/blob/main/architecture/loire/component\\_compliance.puml?ref\\_type=heads](https://gitlab.com/gaia-x/lab/gxdch/-/blob/main/architecture/loire/component_compliance.puml?ref_type=heads)

■ Gaia-X Registry Service

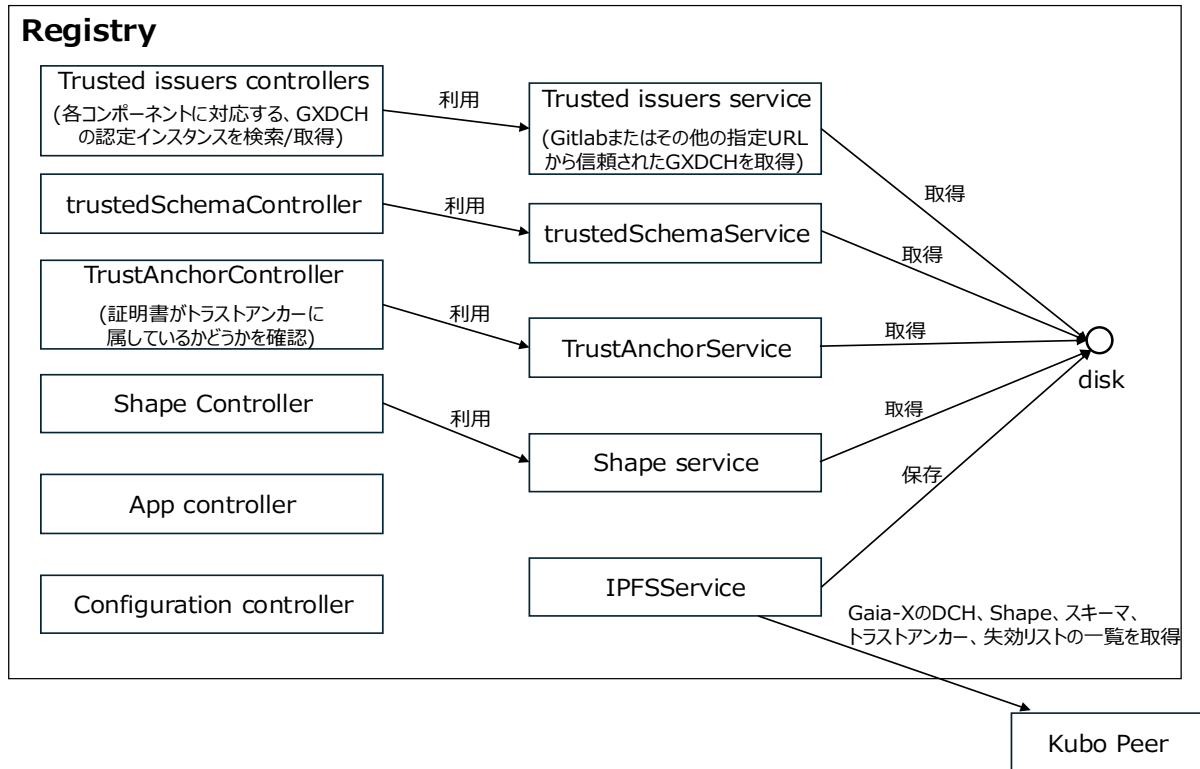


図 A-5 Gaia-X Registry Service<sup>43</sup>

Gaia-X Registry は検証の際に用いる様々な情報が格納されているコンポーネントとなる。W3C のモデルで表すと VDR に相当する。

Gaia-X が定義した VC 形式や、信頼できる VC Issuer のリストなどを持つ。さらに Trust Anchor として eIDAS の Trusted list や Mozilla CA Certificate List 等を持つ。主な役割としては、Gaia-X Compliance が VP を検証する際に、VC 形式が正しいか、Issuer が信頼できる相手か、等の確認に用いられる。

■ Gaia-X Notary Service

<sup>43</sup> [https://gitlab.com/gaia-x/lab/gxdch/-/blob/main/architecture/loire/component\\_registry\\_ipfs.puml?ref\\_type=heads](https://gitlab.com/gaia-x/lab/gxdch/-/blob/main/architecture/loire/component_registry_ipfs.puml?ref_type=heads)

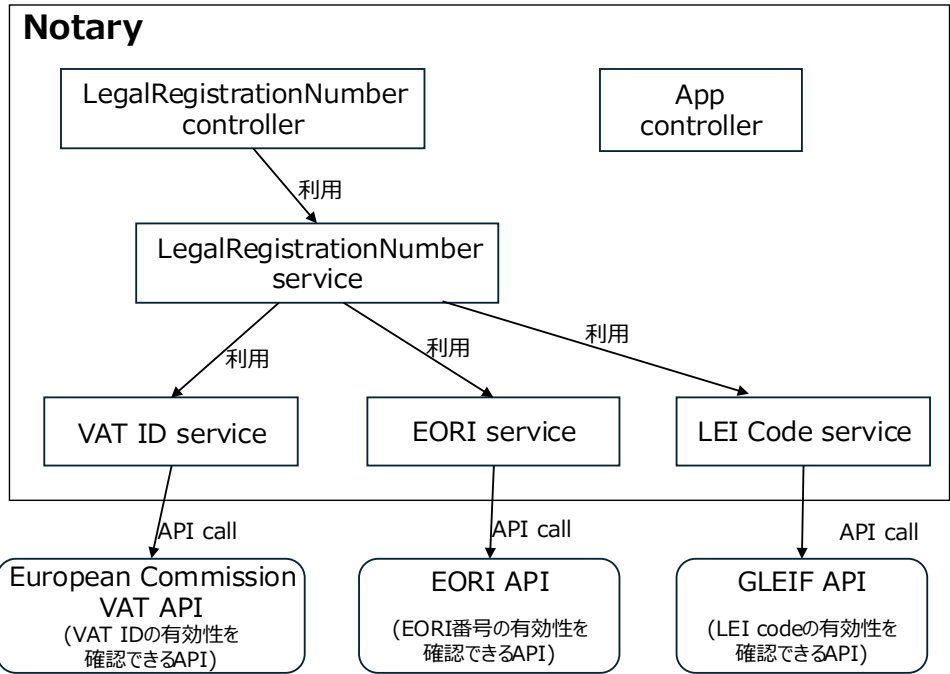


図 A-6 Gaia-X Notary Service<sup>44</sup>

Notary と呼ばれるコンポーネントは企業番号が信頼できるデータソースに存在していることを確認し、それを保証するための VC を発行する役割を持つ。

発行される VC は Legal Registration Number VC である。(v2:Loire では番号ごとに VC 形式が異なる)

企業番号と番号の形式を入力することで、形式に合った信頼できるデータソース API を利用し、番号を持つ企業の登録有無を調べる。Notary は信頼できる VC Issuer である必要があり、基本的には現在 GXDCH インスタンスを公開している企業がそれにあたる。Notary は、Trusted Issuers としてプライベートなトラステッドリストを保持するレジストリに登録されており、信頼の起点として扱われる。

<sup>44</sup> [https://gitlab.com/gaia-x/lab/gxdch/-/blob/main/architecture/loire/component\\_notary.puml?ref\\_type=heads](https://gitlab.com/gaia-x/lab/gxdch/-/blob/main/architecture/loire/component_notary.puml?ref_type=heads)