デジタル庁 御中

産業用データ連携に関する機能及び実装等に係る調査研究　報告書

2022年03月30日

EYストラテジー・アンド・コンサルティング株式会社

Building a better working world

目次

目次

第1章 エグゼクティブサマリ

1.1 欧州における非個人データの保護の動き

2016 年に欧州で制定された一般データ保護規則（GDPR）が 2018 年に施行され、個人データに対する包括的な保護の枠組みが制定されたことは周知のとおりである。欧州経済領域外への個人データ移転を原則禁止とし、GDPR が設定した例外にあたる場合にのみ域外移転が可能とされることとなった。

欧州委員会は、その後、こうした個人データに比べて法的な取扱いが不明確な非個人データ（Non-personal data）を今後 EU が取り組むアジェンダとして提示した。域内の自由流通とその保護に関する検討が進められ、2020 年には「欧州データ戦略（European Data Strategy）」を発表し、単一市場である「欧州データスペース（European Data Spaces）」の構築により、産業用データの有効活用を通じて EU の国際競争力の強化を図ることとした。

IT サプライチェーンがグローバル化・複雑化しているという昨今の状況をみても、こうした動きのインパクトは大きい。以下で紹介する International Data Spaces（IDS）や Gaia-X もそうだが、標準仕様を定めることで様々な技術間のギャップを埋めなければならない事業者のリスクを軽減したり、規格をオープンに定義することで新規参入を容易にしたりすることができる可能性がある。

現在、欧州議会ではデータガバナンス法案やデータ法案が審議されている。非個人データの取扱いについて、両法案は域外移転に際し十分性の認定を必要としているところ、今後、日本においても GDPR 対応時と類似の対応が求められる可能性がある。

1.2 データスペースの構築に向けた取組

「1.1 欧州における非個人データの保護の動き」と併せて、欧州では「データ主権」の理念が提唱されはじめた。企業や団体が保有する様々なデータについて、いつ、どこで、どのように利用されるか、バリューチェーンの中でその企業や団体が自己決定できるようにすべきというものである。このデータ主権を技術的に保証する「データスペース」を構築しようとする主な取組が、本報告書にまとめた IDS イニシアティブや Gaia-X 構想である。

IDS イニシアティブは、2015 年にフラウンホーファー研究機構が立上げ、2016 年に International Data Spaces Association（IDSA）として組織化された。データスペースの構築に向けてリファレンスアーキテクチャの策定や Open Source Software（OSS）の開発、ユースケースの発展に向けた支援を行っている。

一方、Gaia-X 構想は 2019 年にドイツ・フランス両政府により立ち上げられたものである。2020 年には Gaia-X 財団が設立され、独仏の 22 の企業が創設メンバーとなった。IDS と同様にデータスペースの構築に向けた取組を行っている。

Gaia-X は IDS の流れを踏まえた取組であるが、両者の背景は異なっている。Gaia-X の普及支援を（国ごとに）行う Gaia-X Hub Germany のメンバーによると、IDS はドイツ発

の産業的ニーズに応えるものであるのに対し、Gaia-X は EU 全体の取組であって、Google、Microsoft、Alibaba 等の海外企業からの独立、すなわちデータ主権の確保に関する政治的ニーズに応えるための取組であるとのこと。

実際、Gaia-X Hub Germany は、連邦経済エネルギー省の支援を受け、ドイツ科学技術アカデミー（acatech）が主導して設立されている。企業や研究機関が参加しており、欧州のデータ戦略の目標に貢献すべく取組が進められている。

もっとも、現在のところ、Gaia-X は EU 全体を巻き込む中で組織の肥大化に関する課題に直面しているとの見方がある。委員会やワーキンググループの数が増加し、意思決定やアジェンダの進捗の遅れを懸念する声が上がっており、Gaia-X CEO も「Gaia-X の内部組織はこのような（急激な）成長を管理するように設計されていなかった」と述べるに至っている。本調査研究で IDSA や Gaia-X に精通する専門家へのインタビューを行う中でも、異口同音にロードマップの遅れが指摘されていた。

なお、Gaia-X Hub は欧州 15 か国に設置されており、2021 年には欧州外で初めて韓国に Hub が設置することが発表されている。また、IDSA も同様に Hub を設けているが、こちらは欧州 8 か国にとどまっている。

1.3 データスペースのユースケース

IDSA や Gaia-X のウェブサイトではユースケースとなるデータスペースが紹介されており（例えば、Gaia-X では Industry4.0、Health、Education & Skills といったカテゴリのデータスペース構築の取組が紹介されており）、具体的な取組が進んでいることが確認される。その中でも、本調査研究を通じて確認した範囲では、Catena-X、Smart Connected Supplier Network（SCSN）、Mobility Data space（MDS）の 3 つが事例としてよく取り上げられていたので、簡単に紹介したい。

Catena-X は、ドイツ企業がハイレベルな環境目標に対応するため、サプライチェーンのデューデリジェンス強化義務と価格上昇に直面する中で立ち上げられたプロジェクトである。トレーサビリティ、CO_2 フットプリント証明、循環型経済や MaaS といった 10 の優先分野が設定されており、例えば、循環型経済実現に向けた自動車部品リサイクル用サービスの実装等が進められている。

Catena-X がこうしたサービスの実装を進める背景には、ドイツではリサイクル業者とバリューチェーンの他の企業と情報共有が進んでいないため、自動車部品のリサイクル率が低いという現状がある。規制や基準がない中で、OEM や Tier1、Tier2 がそれぞれ独自のデータモデルを持っていることや、リサイクル業者の多くを占める中小企業のデジタル化が進んでいないことが要因と考えられている。

SCSN はハイテク製造サプライチェーンにおける製造企業と、その IT サプライヤー向けのデータ共有を想定している。主に製品を複数の団体が共同で作るような、多品種少量、複雑性の高い領域にフォーカスし、工場を越えたコミュニケーションの促進とサプライチェーンの透明性、相互運用性の確保、事務負荷の軽減等を図ろうとしている。

ハイテク製造サプライチェーンでは、OEM や Tier1、Tier2、Tier3、卸売業者、製鉄業者等様々な事業者間で見積や発注、インボイス等の情報共有が必要である。これまで企業

がデータを交換しようとする場合、EDI リンクについてその都度設定する必要があったが、今後、SCSN ネットワークに接続したサービスプロバイダと契約することで、SCSN に接続した複数のサービスプロバイダと契約する全ての企業とデータ交換を可能とするものである。

MDS は車両製造業者からライドシェアリングサービス、公共交通運営者やナビソフトウェア企業、研究機関、バイクシェアリング企業等を含むモビリティセクターの将来に焦点を当てたプロジェクトである。MDS では、共有された様々なデータ（気象データ、道路状況データ、駐車場のデータ等）を用いて最適・安全・持続可能な交通オプションの選択を可能にするサービスが既に展開されている状況にある。

1.4 IDS と Gaia-X のアーキテクチャ

IDS や Gaia-X については、そのコンセプトを実現するための技術的仕様として、アーキテクチャに関する資料を IDSA ないし Gaia-X のウェブサイトで公開している。

IDS のアーキテクチャは、認証されたデータ提供者と受信者の間で、相互に合意したルールに基づき、信頼性の高いデータ交換を可能とするため、それぞれがもつコネクタを介してデータ共有を行うことを想定している。データスペースの参加者は、IDS コネクタを利用することで、産業用データクラウド、個々の企業のクラウド、オンプレミスアプリケーション等のデバイスを IDS に接続することができる。

Gaia-X のアーキテクチャも、同じくデータ主権の理念に則ったデータ交換を可能とするものである。Gaia-X は、データスペース構築のためのアーキテクチャを 3 層で表している。すなわち、データエコシステム、フェデレーションサービス、インフラストラクチャエコシステムである。

データエコシステム層では、各産業部門から生成されるデータの相互運用やポータビリティを実現する。インフラストラクチャエコシステム層では、クラウド、高パフォーマンスコンピューティング（HPC）クラウド、エッジコンピューティング等の相互運用を実現する。フェデレーションサービスは、この 2 層をつなぐための実質的な機能であり、Gaia-X では 4 つのコア機能（ID とトラスト、フェデレーションカタログ、データ主権サービス、コンプライアンス）の開発等を進めている。

フェデレーションサービスは、ドイツとフランスにおいてコンソーシアムを設立して開発が進められている。ドイツでは 1,300 万ユーロ、フランスでは 1,200 万ユーロを得て運営されていると紹介されている。報告書では、以上の IDS や Gaia-X のアーキテクチャの全体像を比較しながら説明するとともに、その機能の開発状況について整理を行っている。

1.5 今後の展望

IDSA は現在、IDS Reference Architecture Model4.0（IDS-RAM4.0）を策定中であり、2022 年 4 月に発表予定である。これは現在の同 3.0 を更新するものであり、各機能の仕様に変更が加えられる予定である。また、Catena-X や MDS 等のプロジェクトからのフィードバックも盛り込んだ資料になる予定という。

Gaia-X の方は、コア機能であるフェデレーションサービスを開発するとともに、複数のデータスペースのプロジェクトを進めている。ドイツ連邦ネットワーク庁は、2022 年に 11 プロジェクトに 1 億 1,740 万ユーロを措置することを発表した。いずれも 2025 年には EU がグローバルデータエコノミーで活躍することを目標に取組を進めることとされているが、ロードマップの遅れ等の影響は現時点で不透明である（なお、最新の報道では、今般のウクライナ危機の影響で一部のプロジェクトの予算措置が取り下げられたとの情報がある）。

翻って日本企業においては、こうした IDS や Gaia-X に準拠するデータスペースに参加しようとすると、今後、接続のたびにそのアーキテクチャ等への対応を迫られることになりかねない。将来的には、日本が進めるデータスペース構築に向けた取組をもって、欧州側との相互認証を図り、日本企業の活動に著しい支障のないよう IDSA や Gaia-X 等と協議・連携を行っていく必要があるだろう。

第2章 調査概要

2.1 調査目的・趣旨

DX（デジタル・トランスフォーメーション）の取組みの進展に伴い、データは「21 世紀の石油」とも呼ばれるようになり、ビジネスにおいて極めて重要なものと位置づけられている。産業界では、企業の様々なクラウドサービスを単一のシステム上で統合し、業界をまたがるデータ交換を容易に行える標準的な認証の仕組みを通じて、相互運用性を実現することが求められ、各国間で競争が始まっている。

欧州では、欧州デジタル戦略や欧州データ戦略を策定され、公平かつ競争力のあるデジタル経済の実現や産業データの有効活用を通じた国際競争力強化を目指すとともに、デジタル主権を確保するため、安心で信頼できる欧州独自のデータインフラ構築を目指す取組が推進されている。

一方、日本では 2022 年 1 月から電子帳簿保存法が施行され、2023 年にはインボイス制度が開始されるものの、中小企業のデジタル化や DX の対応は浸透しているとは言い難い。これを加速するには、業界をまたがるデータ交換を容易に行える標準的な認証の仕組みを構築し、企業の能力にあったデジタル化・DX のツールを用意することが有用である。

こうした状況を踏まえ、本調査研究では、業界をまたがるデータ交換を容易に行える標準的な認証の仕組みを通じて、相互運用性を実現するために必要な要素を調査するとともに、その具体的な検証アプリを構築した。

2.2 調査対象

欧州では、相互運用性を実現するための仕組みとして、IDSA や Gaia-X といった団体を中心にデータ連携基盤の枠組みが整備されようとしている。本調査研究では、これらが整備するリファレンスアーキテクチャや開発中のコンポーネントを調査対象とし、以下の内容を中心に整理した。

- 生成されるデータの相互運用やポータビリティを実現する機能
- クラウド、高パフォーマンスコンピューティング、エッジコンピューティングの相互運用を実現する機能
- データインフラを利用する際のセキュリティ、データ主権を維持したデータ交換、データ利用カタログ、個人データ保護に関する共通ルールや標準を定める機能
- 検討されているユースケース

具体的な検証にあたっては、上記のデータ連携基盤の枠組みの中核技術と考えられる「コネクタ」について、開発状況が公開されている GitHub[1]のソースコードを踏まえてプログラムの構築を実施した。なお、その詳細等については、本報告書に併せて「8.4 コネクタを用いたデータ連携の試行」に記載した。

[1] GitHub（https://github.com/）とは、プログラムのソースコードのホスティングサービスを主とするソフトウェア開発プラットフォームサービスである。

2.3 調査期間・方法

調査は 2022 年 1 月 25 日から同年 3 月 31 日までの間に行い、以下のステップに沿って実施した。

図表 2-1 調査方法

ステップ	内容
関連団体の洗い出し	IDSA、Gaia-X 及びこれらに関連する団体とその取組の概要を調査した。
公開資料の確認	IDSA や Gaia-X の公開資料の全容を確認した。
全体像の整理。	IDSA や Gaia-X が整備するリファレンスアーキテクチャの全体像を整理した。
必要な要素の深堀り	現在も更新が進む IDSA や Gaia-X の資料やイベントのプレゼンテーション資料、GitHub の更新状況等を参照して詳細を確認するとともに、IDSA や Gaia-X に精通する専門家へのインタビューを実施した。

第3章 欧州におけるデータ連携の取組の動向

3.1 産業用データに関する戦略や規制の動向

欧州は、2016 年に一般データ保護規則（GDPR）を制定、2018 年に施行することで、個人データに対する包括的な保護枠組を設定した。この中で、個人データの欧州経済領域（EEA）外への移転を原則禁止とし、GDPR が設定した例外に該当する場合にのみ域外移転を有効とすることを規定した[2]。これに対し、非個人データ保護に関する包括的法的枠組は存在していない。

欧州委員会は 2017 年 1 月、「欧州データエコノミーの構築（Building a European Data Economy）」にて、個人データに比べて取扱が法的に不明確な非個人データについて見解を示し、EU 域内での自由なデータ移動、IoT やロボティクス分野の製品で事故が起きた場合の責任の所在、非個人データの持ち運び、データ交換の円滑化を可能とする相互運用性や標準化、他者からのアクセスの円滑化を今後 EU が取りくむべきアジェンダとして設定し、非個人データへのアクセスに関する検討を進めてきた[3]。2018 年 11 月には「非個人データの域内自由流通枠組に関する規則（Regulation（EU）2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union）」が発表され、GDPR の対象外である非個人データについて、域内における自由流通を促進するための規則が示された[4]。

このように、産業データを含む非個人データについても域内流通・保護の強化が進む中で、2020 年 2 月には「欧州データ戦略（European Data Strategy）」が発表され、データの単一市場である「欧州データスペース（European Data Spaces）」の構築を目指すこと、産業データの有効活用を通して EU の国際競争力強化を目指すことが示された[5]。

現在、データを保護しつつこれらの目標を実現するための法整備が進められており、欧州議会ではデータガバナンス法案（Data Governance Act）、デジタルサービス法案（Digital Services Act）、デジタル市場法案（Digital Markets Act）、データ法案（Data Act）が審議されている。これらの法案は Gaia-X のデータスペースやエコシステムに直接的な影響を与えるものである[6]。この中でも、データガバナンス法案とデータ法案は Gaia-X エコシステム下のデータ共有に関わる法案であり、非個人データの取り扱いについても言及している。両法案は域外移転に際し十分性の認定を求めていることから、今後は日本政府の法制面での対応が必要となることが予想される。

---

[2] 渡辺 翔太 「欧州司法裁判所 Schrems II 事件判決が越境データ流通に与える影響の考察―我が国の推進する DFFT 構想への影響を中心にして―」 （RIETI Discussion Paper Series 21-J-035、2021 年 7 月）

[3] 井上 淳「EU における「非」個人データへのアクセスに 関する政策動向及び経済分析について」（情報通信学会誌 35 巻 4 号、 2018 年）

[4] みずほ情報総研株式会社 経営・IT コンサルティング部「令和 2 年度 ウィズコロナにおけるデジタル活用の実態と利用者意識の変化に関する 調査研究の請負 －報告書－」、https://www.soumu.go.jp/johotsusintokei/linkdata/r03_01_houkoku.pdf （2022 年 3 月 16 日アクセス）

[5] 国立研究開発法人科学技術振興機構研究開発戦略センター「EU の DX ～欧州デジタル戦略 2020～」、https://www.jst.go.jp/crds/sympo/20200928/pdf/07.pdf （2022 年 3 月 16 日アクセス）

[6] “4ème plénière pour le Hub France de Gaia-X, en présentiel !” Cigref, https://www.cigref.fr/4eme-pleniere-pour-le-hub-france-de-gaia-x-en-presentiel （2022 年 3 月 28 日アクセス）

3.1.1 データガバナンス法案

データガバナンス法案は、データ取引上の信頼を担保することを目的としており、既存の保護の対象となっている公共部門のデータを再利用するための条件、特定のデータ共有サービスの提供者に対する義務を規定する。また、データ利他主義の概念を導入すると共に、欧州委員会が議長を務める新たな公式専門家グループである「欧州データ革新会議（European Data Innovation Board）」を設立することも規定している[7]。

2022 年 3 月 22 日時点で欧州議会第 1 次検討中であり、今後の推移が注目される[8]。

3.1.2 データ法案

データ法案は、データエコノミーにおける主体間でデータ価値の配分の公平性を担保することを目的としており、製品等の利用者に対して生成データを利用させる義務、第 3 者へのデータ共有義務、不公正な契約条件の制限、公的機関への情報提供義務、データ処理サービスの提供者間の乗り換えに関する義務、非個人データの国際移転に関する制限を設定している[9]。

提案されたばかりの法案であり、2022 年 3 月 22 日時点で欧州議会での法案審議準備中である[10]。

3.2 データ連携基盤に関する取組の動向

3.2.1 International Data Spaces (IDS)

(1) 立ち上げとその目的

International Data Spaces（IDS）はデータエンドポイントの分散型ネットワークであり、データのセキュアな交換を可能にし、データ主権を保証する。IDS イニシアティブは、2015 年にフラウンホーファー研究機構が開始し、2016 年に非営利団体

---

[7] 日本情報経済社会推進協会「欧米のプライバシー関連法規制」、https://www.jipdec.or.jp/library/itreport/2021itreport_winter02.html （2022 年 3 月 16 日アクセス）

[8] “2020/0340(COD) European data governance (Data Governance Act)” Legislative Observatory, European Parliament, https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2020/0340(OLP) (2022 年 3 月 22 日アクセス)

[9] Jetro「欧州委、産業データへのアクセスの包括的ルール定めたデータ法案発表」、https://www.jetro.go.jp/biznews/2022/02/225affa523fffc72.html (2022 年 3 月 16 日アクセス)

[10] “2022/0047(COD) Harmonised rules on fair access to and use of data (Data Act)” Legislative Observatory, European Parliament, https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2022/0047(OLP) (2022 年 3 月 22 日アクセス)

International Data Spaces Association(IDSA)が設立され、組織化された[11]。

IDS イニシアティブは IDS をデータ交換の基準とすること、そして国際的に拡大することを目的としている。具体的には、IDSA は、ガバナンスモデル、採用戦略、IDS リファレンスアーキテクチャを開発すること、IDS ベースのユースケースを発展させること、将来的にはデータ交換の国際標準として IDS を確立すること、認証可能なソフトウェアソリューションやビジネスモデルを支援することを目指している[12]。

思想的にはデータ主権を保ちつつデータ共有を可能にすること、データ制御をデータ所有者に戻すことを重視しており、データ主権をデジタル化時代において鍵となる機能として捉え、そのために必要な技術を提供している[13]。

(2) 現状と課題

ア IDSA の組織体制

IDSA は図表 3-1 にみられるように、執行委員会（Executive Board)、運営委員会（Steering Committee）の下に、IDSA Hubs、開発者コミュニティ、リエゾン、コミュニケーション及びマーケティング、開始連合（Launching Coalition)、ワーキンググループとタスクフォースが設置されている。

執行委員会は 12 人のメンバーから構成され、協会のビジネス活動を管理する。運営員会はワーキンググループ及びタスクフォースの議長・副議長、IDSA コミュニティから選出された代表 2 人、IDSA 採用イニシアティブから選出された代表 2 名、IDSA ヘッドオフィスの最高経営責任者、フラウンホーファー研究機構の代表者 1 名、IDSA 主要設計者から構成され、ワーキンググループやタスクフォースで決定できないトピックの判断、リコメンデーションの承認、IDSA のリリース計画の承認等を担当する[14]。

---

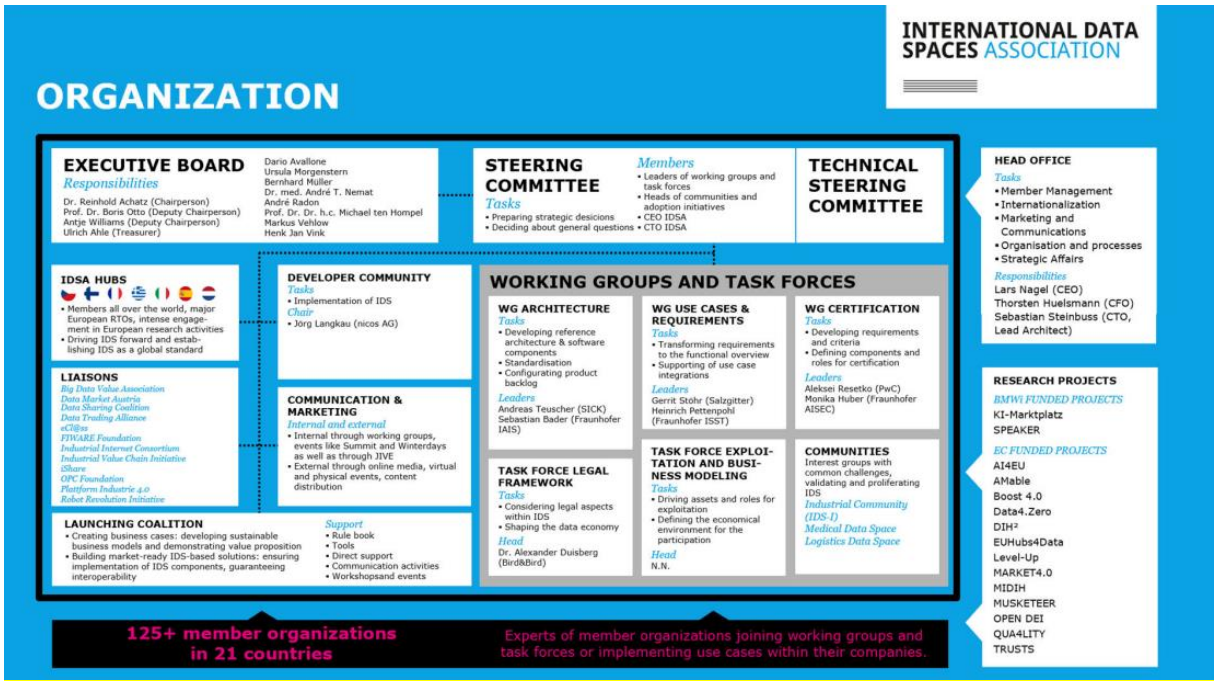
[11] フラウンホーファー研究機構は 69 の研究所・研究ユニットで構成され、約 2 万 4500 人の科学者・技術者が所属している。IDS にはそのうち 12 の研究所が参加している。”International Data Spaces” Fraunhofer-Gesellschaft, https://www.fraunhofer.de/en/research/lighthouse-projects-fraunhofer-initiatives/international-data-spaces.html (2022 年 3 月 17 日アクセス); “FAX” Fraunhofer, https://www.dataspaces.fraunhofer.de/en/faq.html#:~:text=What%20is%20the%20International%20Data%20Spaces%20initiative%3F,Association%20(IDSA)%20since%202016(2022 年 3 月 18 日アクセス)

[12] “IDSA: Driving data freedom for the whole world” International Data Spaces Association, https://internationaldataspaces.org/we/the-association/ （2022 年 3 月 17 日アクセス）

[13] “Sovereign data exchange between companies” Fraunhofer, https://www.dataspaces.fraunhofer.de/en/InternationalDataSpaces.html (2022 年 3 月 17 日アクセス)

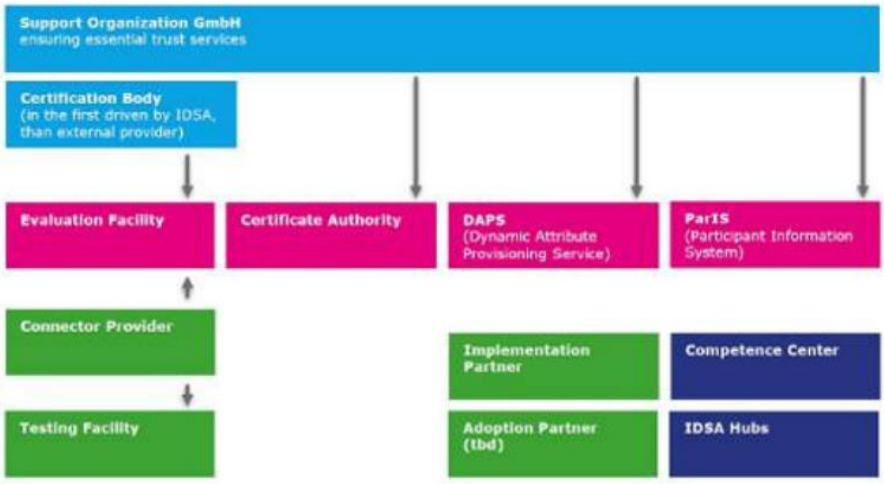
[14] IDSA Rule Book, International Data Spaces Association, 2021 (https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-White-Paper-IDSA-Rule-Book.pdf, 2022 年 3 月 24 日アクセス), pp25-26

図表 3-1 IDSA 組織図



また、図表 3-2 に見られるように、IDSA には支援組織（IDSA-SO）が存在し、IDS ルールブックに従い複数のプロバイダ企業が提供する必須サービスを調整する役割を担っている。IDSA-SO には認証機関（Certificate Authority）、評価機関（Evaluation Facilities）、動的属性提供サービス（DAPS: Dynamic Attribute Provisioning Service）、参加者情報サービス（ParIS: Participant Information Service）、有効化サービス（Enabling Services）が含まれる[15]。

図表 3-2 IDSA 支援組織



IDSA は 2020 年、データ交換に関するドイツ標準規格である DIN SPEC27070「産業データ・サービス向けセキュリティゲートウェイの要件及び参照アーキテクチャ」

[15] *IDSA Rule Book*, International Data Spaces Association, 2021 (https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-White-Paper-IDSA-Rule-Book.pdf, 2022 年 3 月 24 日アクセス), p14

を発行する等、標準化活動を進めると共に、国際展開を目指している[16]。

イ IDSA Hub

IDSA は IDS イニシアティブ推進を助けるため、IDSA Hub を各国に設置している。各 Hub は、将来的なデータエコノミー、グローバルバリューチェーンにおける主権あるデータ共有の重要性を理解する非営利団体によって運営されている。2022 年 3 月 25 日現在、IDSA ウェブサイトにはブルガリア、フィンランド、ギリシャ、オランダ、チェコ、フランス、イタリア、スペインの 8 か国の Hub が紹介されている[17]。

（ア）フランス

Institut Mines-Télécom（IMT）と IDSA は、2019 年 5 月に IMT が IDSA のフランスにおける Hub を主宰し、セキュアで主権あるデータ共有を可能にする欧州標準策定のため、フランスのエコシステムを結集することに合意した。

フランスの IDSA Hub として、IMT はフランスの官民組織に対して IDSA の概念を広め、IDS を支えるイニシアティブを推進している。具体的には、新たなイニシアティブをフランスで開始すること、欧州プロジェクトの枠内で、欧州諸国間の既存のプロジェクトつなぐことにより、データ共有分野での活動を加速させることに取り組んでいる。

IMT は IDSA のメンバーであり、WP アーキテクチャの分野で特に活発に活動している。IDSA Hub の設立は、蓄積したナレッジと経験に基づきフランスの人々がアプリ開発を行うことを可能にする[18]。

（イ）オランダ

IDSA とオランダ応用科学研究機構(TNO)は 2019 年 3 月 18 日、TNO がオランダの IDSA Hub となることを取り決める合意に署名した。オランダの IDSA Hub として、TNO はオランダのイニシアティブと国際標準化活動をつなぐ役割を果たす。

Hub の目的は、オランダで新たなイニシアティブを開始すること、また欧州諸国と既存のイニシアティブをつなぐことで、データ共有分野のイニシアティブを加速させることである。

TNO は IDSA のメンバーであり、様々なＷＧに参加している。オランダの IDSA Hub は、オランダの産業プレイヤーがナレッジと経験を活用し、アプリ開発を行

[16] “IDS is Officially a Standard: DIN SPEC 27070 is Published,“ International Data Spaces Association ウェブサイト, https://internationaldataspaces.org/ids-is-officially-a-standard-din-spec-27070-is-published/, 2020 年 2 月 21 日リリース

[17] “Join our network of international hubs” International Data Spaces, https://internationaldataspaces.org/make/hubs/ (2022 年 3 月 25 日アクセス)

[18] “L’IMT devient le hub français de l’IDSA” Institut Mines-Télécom, https://www.imt.fr/limt-devient-le-hub-francais-de-lidsa/ (2022 年 3 月 25 日アクセス)

うことを可能にする[19]。

(3) Gaia-X との関係性

当初、Gaia-X は IDS コネクタをコア技術とし、各企業のデバイス/エッジやクラウド間を接続することで、データ主権の保護、信頼できる連邦型データ流通インフラの整備等を始めとした Gaia-X の目標を達成しようとしていた。IDS、Gaia-X は、特に分散とフェデレーション(decentralization と federation）について同じゴールを持っており、同じデザイン原則に基づいている。

また、IDSA は Gaia-X Association の創立メンバーであり、IDS リファレンスアーキテクチャのコンポーネントが Gaia-X の標準アーキテクチャに用いられている[20]。IDSA 発行文書によると、IDS のビジョンと IDS リファレンスアーキテクチャモデル（IDS-RAM)は、Gaia-X の全体的なビジョンと具体的な Gaia-X アーキテクチャに必要とされる様々な概念・ソリューションを提供している。両者の違いは、Gaia-X は主権あるクラウドサービスやクラウドインフラに焦点を当てている一方、IDS はデータとデータ主権を重視している点が挙げられている[21]。

Gaia-X Hub Germany のメンバーによると、Gaia-X は IDS にインスパイアされているものの、立ち上げの背景が異なっている。前者は Google、Microsoft、Alibaba 等の非欧州企業からの独立、すなわちデータ・デジタル主権を目指す政治的ニーズから開始されたが、後者は産業的なニーズに答える形で開始された。また、前者は EU 全体で発足した取組である一方、後者はドイツ初の組織である。もちろん、Gaia-X 発足時には IDS メンバーがイニシアティブをとっていたが、規模拡大につれてドイツ以外の欧州諸国メンバーからドイツ初の組織である IDS への抵抗が生まれたことから、現在 Gaia-X は IDS から独立した動きをとっている。このような背景から、IDS から独立するため Gaia-X のテクニカルグループは独自の API コネクタの開発を模索している（Gaia-X Hub Germany メンバーへのインタビュー結果については、「エラー! 参照元が見つかりません。エラー! 参照元が見つかりません。」を参照されたい）。

また、Gaia-X Workstream 2 (Technical Implementation)コーディネータによると、IDS は自身を Gaia-X のイネーブラーであると主張する一方、Gaia-X は IDS コネクタの代替を検討しており、Eclipse Data Connector を選択肢の一つとして想定している。Gaia-X 構想は IDS より遥かに壮大であり、IDS が単なるコネクタに過ぎない一方、Gaia-X は標準化されたハードウェア及びソフトウェア、異なるデータスペースやクラウド間の相互接続等も視野に入れている。Gaia-X が 2021 年 3 月に出版した Gaia-X Architecture Document(G18)から IDS コネクタに関する記述が消えたことは、Gaia-X 内で IDS に準拠するか否かについて政治的議論が進んでいるからであり、IDS コネクタに限定したくないという思惑がある。Gaia-X の成功には強いパートナーが必須であり、Eclipse Foundation が強いコミュニティを持つことから、同団体をパートナーに選択することもあり得る（Gaia-X Workstream 2 (Technical Implementation)コーディ

[19] “TNO connects the Netherlands through a European standard for data sharing” PR-Web, https://www.pr-web.com/2019/03/18/tno-connects-the-netherlands-through-a-european-standard-for-data-sharing/ (2022 年 3 月 25 日アクセス)

[20] Boris Otto, *Creating Data Spaces based on Gaia-X and IDS*（日立総研 15 巻 2 号、2020 年)、p35

[21] *Gaia-X and IDS*, International Data Spaces Association, 2021 (https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-Position-Paper-Gaia-X-and-IDS.pdf, 2022 年 3 月 18 日アクセス), p13

ネータへのインタビュー結果については、「エラー! 参照元が見つかりません。エラー! 参照元が見つかりません。」を参照されたい)。

(4) 今後の見通し

ア IDSA の方針

IDSA Winterdays 2022（2022 年 2 月開催）のワークショップ「2025 年のデータスペース：課題とビジョン（Data Spaces in 2025: Challenges and Visions)」では、データスペース 2.0、3.0 やそれ以降を見据えてより長期的な視座を持つことが重要であり、現状数えきれないほど多くのデータスペースが独立して存在していることから、これらをつなげる方法を模索する必要があり、今後数年間は相互運用性が最大課題となるとの認識が共有された。

また、データスペース成長のためには強いガバナンスが必要であり、IDSA がリーダーシップを発揮し続け、ルール策定を主導的に行う必要性が説かれた。IDSA CEO である Lars Nagel 氏はこの問題について公共部門からの規制が遅れていることを指摘し、規制フレームワークを作り出すためには公共部門に強くフィードバックを送り続けなければならないと述べ、今後も積極的に公共部門への働きかけを行っていく方針を示した[22]。

イ IDSA RAM

IDSA は現在 IDS-RAM4.0 を策定中であり、2022 年 4 月に発表予定である。これは、IDS-RAM3.0 を更新するものであり、コネクタやクリアリングハウス、メタデータブローカー等コンポーネントの詳細な仕様や IDS ルールブックの内容に合わせて変更が加えられたものである。また、DID や認証可能なクレデンシャル（Verifiable Credentials）等現在議論中の新たなコンセプトにも言及すると共に、Mobility Data Space や Catena-X 等のプロジェクトからの情報を盛り込んだものになる予定である[23]。

3.2.2 Gaia-X

(1) 立ち上げとその目的

Gaia-X は 2019 年 10 月にドイツ・フランス両政府により開始されたイニシアティブである。2020 年 6 月に Gaia-X 財団が設立され、独仏 22 企業が創設メンバーとなった[24]。2021 年 1 月には、Gaia-X の技術的枠組の開発、Gaia-X Federation services(GXFS)の運用という目標を達成するため、Gaia-X European Association for Data and Cloud

[22] “We are working on something big” International Data Spaces, https://internationaldataspaces.org/we-are-working-on-something-big/ (2022 年 3 月 28 日アクセス)
[23] “Assets and Achievements: Reliable Base for Trust in Data Spaces” International Data Spaces, https://internationaldataspaces.org/wp-content/uploads/IDSA-Strategic-Overview-Assets-and-Achievements-.pdf (2022 年 3 月 22 日アクセス)
[24] “Establishing the Gaia-X Foundation” Federal Ministry for Economic Affairs and Climate Action, https://www.bmwi.de/Redaktion/EN/Blog/2020-06-16-establishing-the-gaia-x-foundation.html (2022 年 3 月 16 日アクセス)

AISBL（以下、Gaia-X AISBL）がベルギー法の下で国際的非営利団体として設立された。

Gaia-X は、相互運用性、可逆性、透明性、サイバーセキュリティ等ヨーロッパの主要な価値観をクラウドインフラに組み込むことを目指している。Gaia-X の 7 原則は、欧州のデータ保護、開放性と透明性、信頼性と信頼、デジタル主権と自己決定、自由な市場アクセスと欧州の価値創造、モジュール性と相互運用性、使いやすさである[25]。

Gaia-X AISBL のメンバーは増加し続けており、2022 年 3 月 28 日確認時点で 335 団体が参加している[26]。この中には非欧州の巨大企業が含まれており、欧州理念の実現、欧州企業の競争力強化という目標に反しているとの指摘もある（詳しくは「3.2.4 欧州における関連取組に関する考察」を参照されたい）。

(2) 現状と課題

ア Gaia-X 組織構成・メンバー

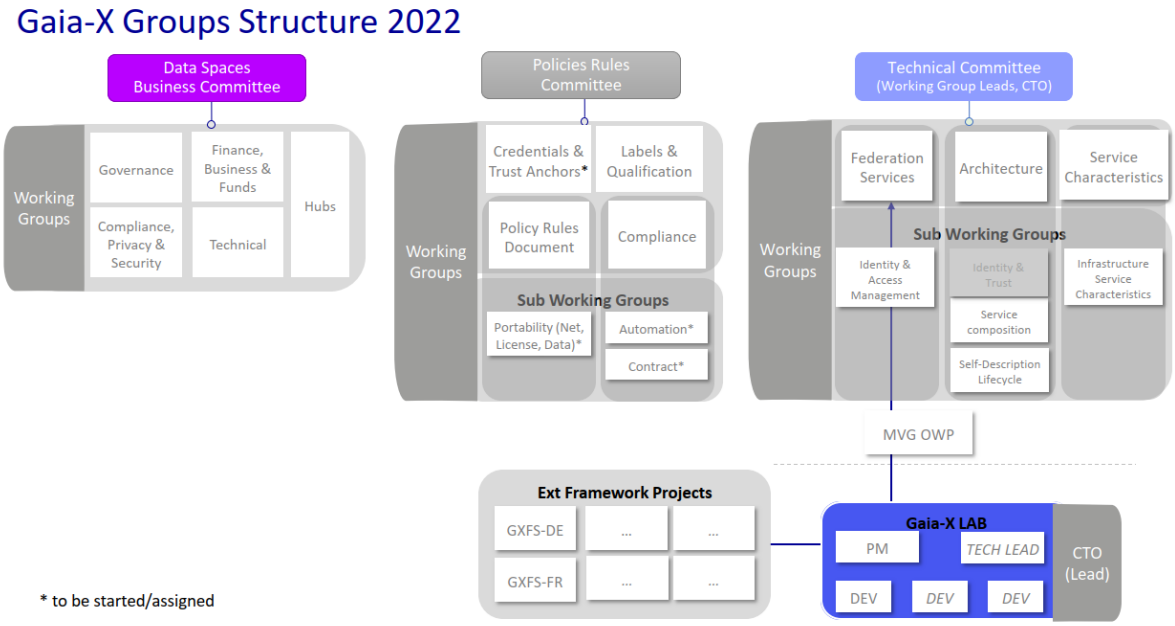
Gaia-X AISBL は図表 3-3 の通り、総会（General Assembly）、理事会（Board of Directors）、管理委員会（Management Board）、ポリシー・ルール委員会（Policy Rules Committee）、技術委員会（Technical Committee）、データスペース・ビジネス委員会（Data Space Business Committee）から構成される。

全ての Gaia-X AISBL メンバーが参加する総会は、Gaia-X AISBL の目標達成のため全ての権限を有している。理事会は Gaia-X AISBL に関わる重要問題について決定する組織である。管理委員会は CEO、COO、CTO、CFO 等で構成され、Gaia-X AISBL の日常的な活動を管理する。ポリシー・ルール委員会は Gaia-X データエコシステムとその運用に関わるポリシー・ルールを承認する。技術委員会は Gaia-X AISBL の目的に関わる技術的課題に取り組む。最後に、データスペース・ビジネス委員会はデータスペースの創設を支援する役割を担う[27]。

[25] “Gaia-X とは何か、GAFAM も巻き込む欧州のクラウド・データインフラ構想” ビジネス IT, https://www.sbbit.jp/article/cont1/56622 (2022 年 3 月 16 日アクセス)
[26] “Members” Gaia-X, https://www.gaia-x.eu/members (2022 年 3 月 16 日アクセス)
[27] “Association” Gaia-X.eu, https://gaia-x.eu/who-we-are/association (2022 年 3 月 24 日アクセス)

図表 3-3 Gaia-X AISBL の組織図

図表 3-4 Working Group の体制

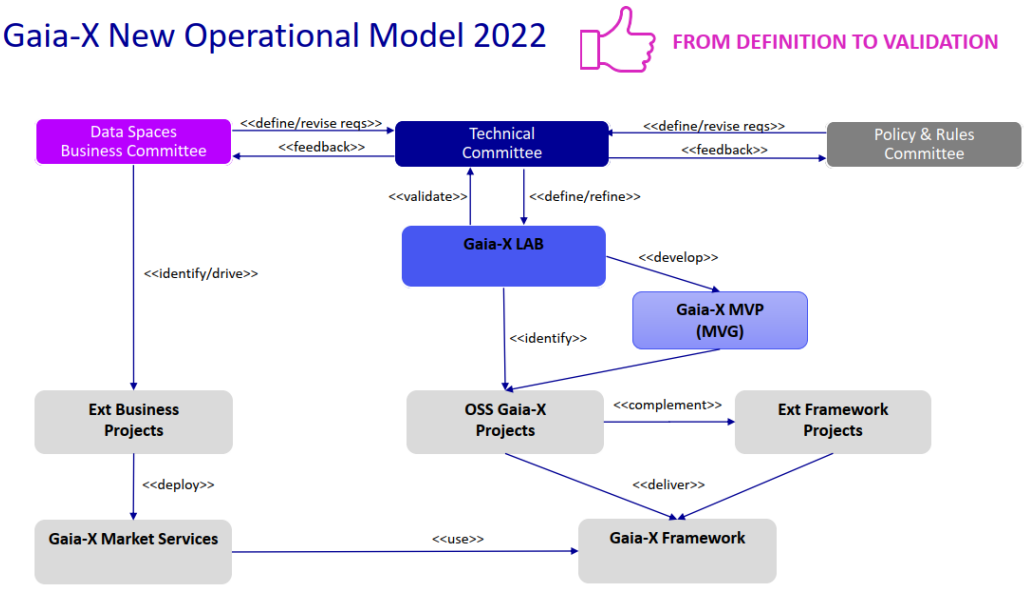


図表 3-4 にみられる通り、ポリシー・ルール委員会、技術委員会、データスペース・ビジネス委員会の下には複数のワーキンググループが設置され、各担当分野の検討が進められている[28]。図表 3-5 は各委員会や Gaia-X Lab、プロジェクトとの関係性に言

[28] “PLÉNIÈRE #4” Cigref, https://www.cigref.fr/wp/wp-content/uploads/2022/03/Master-pleniere-4.pdf (2022 年 3 月 23 日アクセス)

及した運用モデルを示している[29]。

図表 3-5 Gaia-X のオペレーショナルモデル



Gaia-X AISBL 設立時には独仏 22 団体が創設メンバーであったが、組織は拡大を続けており、2022 年 3 月 28 日時点で 335 団体がメンバーとして参画している。日本からは NEC Corporation、NTT Communication Corporation、Robot Revolution & Industrial IoT Initiative が名を連ねており、日本企業のドイツ現地法人である Fujitsu Technology Solutions GmbH、Mitsubishi Electric Europe B.V. German Branch も参加している[30]。

組織の肥大化に伴い委員会やワーキンググループの数が増加したことで意思決定が遅れ、アジェンダの進捗の遅さを懸念する声も広がっている。Gaia-X CEO の Francesco Buonfiglio 氏も「Gaia-X の内部組織はこのような（急激な）成長を管理するように設計されていなかった」と述べており、ガバナンス体制の課題に直面している[31]。

Gaia-X Hub Germany のメンバーによると、フラットな組織であるがゆえにトップダウンのリーダーシップが存在しない等、コミュニティの問題や政治的な影響により、Gaia-X はロードマップ通りに進んでいない状況である。また、非欧州国家（例えば中国やロシア）がデータに関し異なる規則を持っている場合、どのように対処するかといった様々な政治的課題に直面しており、いまだ解決していない状況である（Gaia-X Hub Germany メンバーへのインタビュー結果については、「エラー! 参照元が見つか

[29] “PLÉNIÈRE #4” Cigref, https://www.cigref.fr/wp/wp-content/uploads/2022/03/Master-pleniere-4.pdf (2022 年 3 月 23 日アクセス)
[30] “Members” Gaia-X, https://www.gaia-x.eu/members (2022 年 3 月 16 日アクセス)
[31] “Inside Gaia-X: How chaos and infighting are killing Europe’s grand cloud project” Politico, https://www.politico.eu/article/chaos-and-infighting-are-killing-europes-grand-cloud-project/ (2022 年 3 月 16 日アクセス)

りません。エラー! 参照元が見つかりません。」を参照されたい)。

イ Gaia-X Hub

Gaia-X の取組を普及・促進するため各国で Hub が設立されており、研究機関や民間企業の関与だけでなく、各国政府も積極的に参加している。Gaia-X Hub は、Gaia-X について興味を持つ団体に対し、各国における窓口の役割を果たしている。

各国の Hub は Gaia-X AISBL の一部ではないものの、Gaia-X プロジェクトのシンクタンク及び草の根サポーターとして機能する。また、Gaia-X ステークホルダをつなぎ、ユースケースを拡大するため、欧州内でもグローバルでもユーザの利益を拡大するため活動している。さらに、要件、関連規則、ポリシー定義のため Gaia-X AISBL と協力し、各国内の関連イニシアティブを統合し、効率的な協力体制を築くことで、特定産業内の不必要な重複作業を避ける役割を担っている。

各国 Hub は、特にユーザ要件について情報を取得し、Gaia-X AISBL に連携することで、ユーザのニーズに合うよう枠組を改善している。各国 Hub はワークショップやイベントを通して Gaia-X の普及活動にも取り組んでいる。

現在、欧州 15 か国に Hub が設置されており[32]、2021 年 11 月には欧州外で初めて大韓民国に Hub が設立されることが発表された[33]。Gaia-X Hub France 第 4 回総会では、日本にも 2022 年に Hub が設立されること、シンガポールも Hub の設立に興味を示したことが言及された[34]。

Gaia-X Hub Germany のメンバーによると、Gaia-X Hub は非営利団体だが、各国政府（特に経済を担当する省庁）と会議を定期的に開催している。Hub は非営利団体であり誰もが参加可能である。自国に Hub がない場合は他国の Hub に参加することも可能である（Gaia-X Hub Germany メンバーへのインタビュー結果については、「エラー! 参照元が見つかりません。エラー! 参照元が見つかりません。」を参照されたい)。

（ア）ドイツ

Gaia-X Hub Germany は、2020 年に連邦経済エネルギー省の支援を受けたドイツ科学技術アカデミー(acatech)により設立された[35]。企業や研究機関が参加しており、EU データ戦略の目標に貢献すること、EU データスペースの創設に貢献す

---

[32] “Hubs” Gaia-X, https://www.gaia-x.eu/who-we-are/hubs (2022 年 3 月 16 日アクセス)

[33] “Germany persuades S. Korea to participate in Europe's 'Gaia-X' project” Aju Business Daily, https://www.ajudaily.com/view/20211104155515369 (2022 年 3 月 16 日アクセス)

[34] “18.03.2022 – PLÉNIÈRE #4” Cigref, https://www.cigref.fr/hub-france-gaia-x#pl%C3%A9ni%C3%A8re4 (2022 年 3 月 23 日アクセス)

[35] acatech（Deutsche Akademie der Technikwissenschaften）は連邦及び州政府から予算を得る研究機関である。Gaia-X Hub Germany を主導し、ビジネスや研究機関からの参加者を束ねている。また、Mobility Data Space のユースケースにも参加している。”Data Space Radar” International Data Space, https://internationaldataspaces.org/adopt/data-space-radar/ (2022 年 3 月 16 日アクセス);” acatech – German Academy of Science and Engineering” TUM, https://www.tum.de/die-tum/auszeichnungen/weitere/acatech (2022 年 3 月 16 日アクセス); “Einwöchige Gaia-X-Veranstaltung für den Mittelstand startet heute” Bundesministerium für Wirtschaft und Klimaschutz, https://www.bmwi.de/Redaktion/DE/Pressemitteilungen/2021/09/20210906-einwoechige-gaia-x-veranstaltung-fuer-mittelstand-startet.html (2022 年 3 月 16 日アクセス)

ること、他国の Gaia-X Hub やイニシアティブ、ステークホルダに向けた窓口として機能することを目的としている。現在は、ドメイン内外での要件定義と調整、ドメイングループ設立とユースケース分析、Gaia-X Hub を最適化するための政治・組織レベルの調整等に取り組んでいる。今後も引き続き、継続的かつ詳細な要件の統合、Gaia-X の目標を共有する全てのイニシアティブとの調整、他国の Gaia-X Hub との連携強化を進めていく予定である。

Gaia-X Hub Germany ウェブサイトには、現在 10 ドメイン（農業、エネルギー、金融・経済、地理情報、ヘルス、インダストリー4.0/SMEs、モビリティ、公共部門、スマートシティ/スマートリージョン、スマートリビング）が掲載されており、Gaia-X に基づいたデータスペースを実現するアプリケーション開発が進められている。

例えば農業ドメインでは、ボルツァーノ自治県における衛星画像を用いた「南チロルにおける農業のための AgriML 機械学習」プロジェクトが進められている。これは、Gaia-X 標準に準拠したクラウドソリューションで衛星画像や匿名化された農作物のポリゴンを統合・評価し、機械学習アプリを使って衛生画像を評価することで、農地のどこでどのような耕作が実際に行われているかを判断するものである。耕作の種類によって補助金が異なることから、種類を識別することは非常に重要である。このプロジェクトにおいて、Gaia-X は、データやデータ統合により得られた情報を保護しつつ、アプリケーションが必要に応じてクラウドコンピューティングを用いてスケールされることを可能にする。

また、公共部門ドメインでは、Gaia-X に準拠することで自治体のオープンデータをエネルギー産業が利用できるようになった。相互運用性と標準化により、公共機関はメディアの中断なく、高品質のままデータを提供することができる。これにより、ネットワークオペレータは新たなビジネスモデルやプロセス改善のためにデータを使用することが可能になった[36]。

（イ）フランス

フランスでは、Cédric O デジタル移行電子通信担当大臣が、Cigref とそのパートナーである Systematic Paris-Region、French National Academy of Technologies に委託する形で Gaia-X Hub が設立された[37]。中心となる Cigref は、1970 年に大企業のネットワークとして設立された企業団体であり、メンバー企業がデジタル技術を導入・活用する支援を行っている。

Gaia-X Hub France の目的は、フランスにおける Gaia-X 活動を推進し活性化さ

[36] “Einführung in Gaia-X – Hintergrund, Ziele und Aufbau” Institut der deutschen Wirtschaft Köln e. V., https://www.iwkoeln.de/studien/christian-rusche-einfuehrung-in-gaia-x-hintergrund-ziele-und-aufbau.html (2022 年 3 月 16 日アクセス)

[37] 中心となる Cigref は、1970 年に大企業のネットワークとして設立された企業団体であり、メンバー企業がデジタル技術を導入・活用する支援を行っている。現在、大企業 150 社がメンバーとなっている。Systematic Paris-Region はイノベーション・テクノロジークラスターであり、900 のメンバーと共に Deep Tech のエコシステムを推進している。 ステークホルダをつなぎ、デジタルプロジェクトを強化する役割を果たしている。French National Academy of Technologies は 2000 年に設立された研究機関であり、ノーベル賞受賞者 4 名を含む 337 人の専門家を有する。“Gaia-X: Launch of the French Hub” Cigref, https://www.cigref.fr/gaia-x-launch-of-the-french-hub (2022 年 3 月 17 日アクセス)

せること、セクターベースのワーキンググループ間のミーティングを設定すること、サービスやユースケースの共同革新を加速させ、Gaia-X のフレームワーク内でのサービスを開発するデータスペースを作ること、また Gaia-X AISBL と協力・調整することである[38]。

（ウ）オランダ

オランダでは、TNO がコーディネータ役を務め、ECP Platform for the Information Society が支援する形で Gaia-X Hub the Netherland が設立された[39]。

この目的は、オランダ目線で欧州データ・クラウドインフラがどのような形になるべきか、どのようにオランダの意見を Gaia-X に取り入れるかを検討することである[40]。デジタル化分野で活躍する様々な団体が Hub に参加しており[41]、オランダのエコシステムを統合するため、知識の共有とユースケースの設立が進められている。

ウ GXFS

ドイツにおいては連邦経済エネルギー省がスポンサーとなって GXFS-DE コンソーシアムが設立され、eco を調整役として予算 1300 万ユーロを得て運営されている[42]。2021 年に GXFS 実装のため入札が行われ、図表 3-6 にみられるように各ロット

[38] “Gaia-X: Launch of the French Hub” Cigref, https://www.cigref.fr/gaia-x-launch-of-the-french-hub (2022 年 3 月 17 日アクセス)

[39] TNO は 1932 年にオランダ議会により設立された公的研究機関である。TNO の活動目的は、企業や政府が基盤知識を応用できるようにすることであり、3400 人以上の専門家を有し、9 つのドメイン（建設・インフラ・海洋、循環型経済・環境、エネルギー、健康的な生活、産業、情報通信技術（ICT）、交通・輸送戦略分析・政策）を重点分野としている。Gaia-X Hub the Netherland を中心となって設立し、全体的な調整、国内・国際調整、イノベーション・ソリューション、化学研究・ファンディング、Gaia-X NL サンドボックス等を担当している。また、SCSN、NL AI Coalition、ECI Gatewise、DASLOGIS、Metal Domain Data Space、Defense Data Space、Market4.0 Marketplace、Plastic Domain Data Space 等様々なデータスペース・ユースケースに参画している。tno japan 株式会社「組織」、https://japan.tno.nl/about-tno/organisation/ (2022 年 3 月 17 日アクセス)

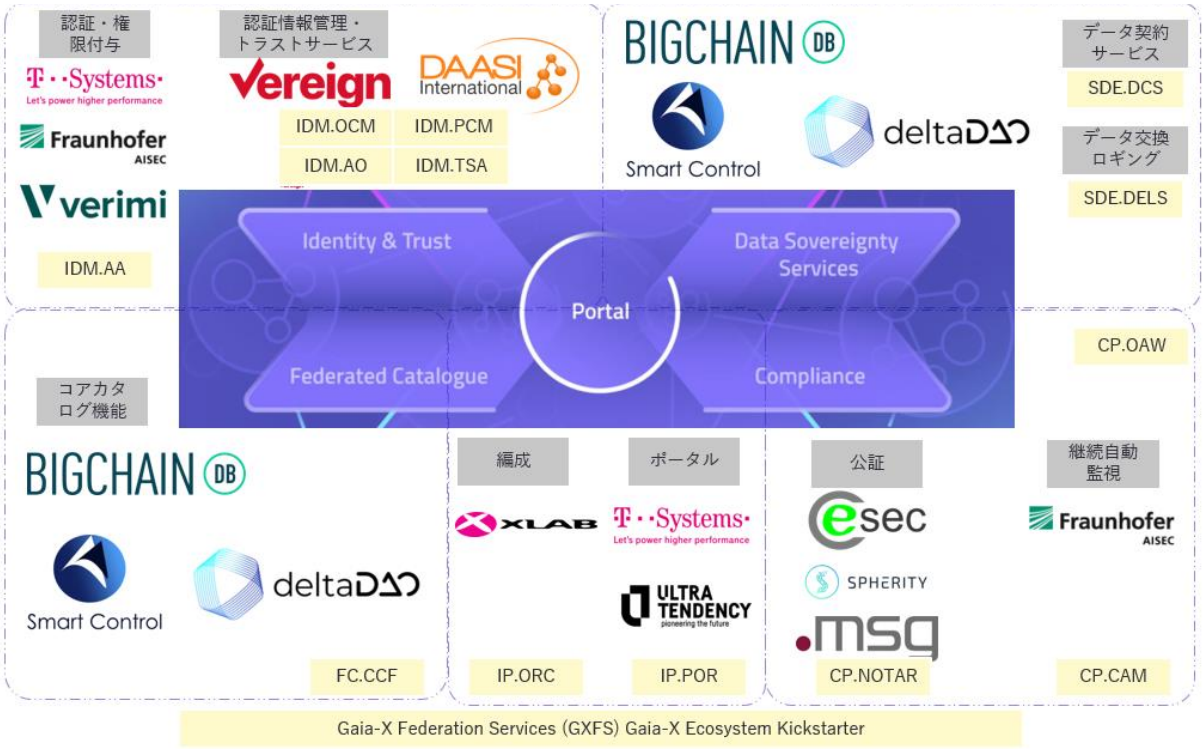
[40] ” NEDERLANDSE HUB Gaia-X VOOR INVULLING EN BIJDRAGE EUROPESE DATA- EN CLOUDINFRASTRUCTUUR” TNO, https://www.tno.nl/nl/over-tno/nieuws/2021/7/nederlandse-hub-gaia-x/ (2022 年 3 月 17 日アクセス)

[41] TNO、VNO NCW、ECP、DINL、DIGICAMPUS、オランダ経済気候戦略省、欧州委員会が全体調整を担い、Brainport Industries、SCSN、smart industry がアプリケーション・ユースケースを担当している。ドメイン別には、Phillips がヘルス、Tennet がエネルギー、内務省と VNG が政府、SURF が教育、ING と ABN-AMRO が金融ドメインのアプリ・ユースケースを担っている。また、Data Sharing Coalition、NL AI Coalities、AM d EX、iSHARE がデータを担当し、Online Trust Coalitie と DutchBlockchain Coalition がプラットフォーム・ツールに取り組んでいる。Cloud Infrastructure Coalition、Dutch Cloud Company が情報インフラストラクチャ、Future Network Services 及び amsix がコミュニティインフラストラクチャを担当し、全体に係る項目としては、セキュリティを dcqpher、サステナビリティを LEAP、標準化に NEN が取り組んでいる。”Terugkijken: Webinar Gaia-X Federation Services (GXFS) met Andreas Weiss en Frans van Ette” Gaia-X Hut the Netherlands, https://gaia-x.nl/evenementen/webinar-gaia-x-federation-services-gxfs-met-andreas-weiss/ (2022 年 3 月 17 日アクセス)

[42] eco はドイツのインターネット事業者団体であり、ロビイング企業であり、DC-IX の子会社である。世界に 1100 のメンバーを有している。Mobility Data Space をサポートしており、外部委員会のメンバーに eco 議長の Oliver Sume 氏が選出されている。また、eco は Gaia-X 外部プロジェクトの Car Repair 4.0 のコンソーシアムのメンバーである。“eco Association supports Mobility Data Space “ eco, https://www.eurocloud.de/presse/eco-verband-unterstuetzt-mobility-data-space/ (2022 年 3 月 25 日アクセス); “PLÉNIÈRE #4” Cigref, https://www.cigref.fr/wp/wp-content/uploads/2022/03/Master-pleniere-4.pdf (2022 年 3 月 23 日アクセス)

（Authentication/ Authorization、Personal Credential Manager、Organization Credential Manager、Trust Services API、Core Catalogue Functions、Data Contract Service、Data Exchange Logging Service、Continuous Automated Monitoring、Notarization API、Portal、Orchestration）に対応する企業・団体が決定し、2022 年 3 月に GXFS の実装開始が発表された[43]。

図表 3-6 GXFS-DE 実装各社及び仕様文書のマッピング

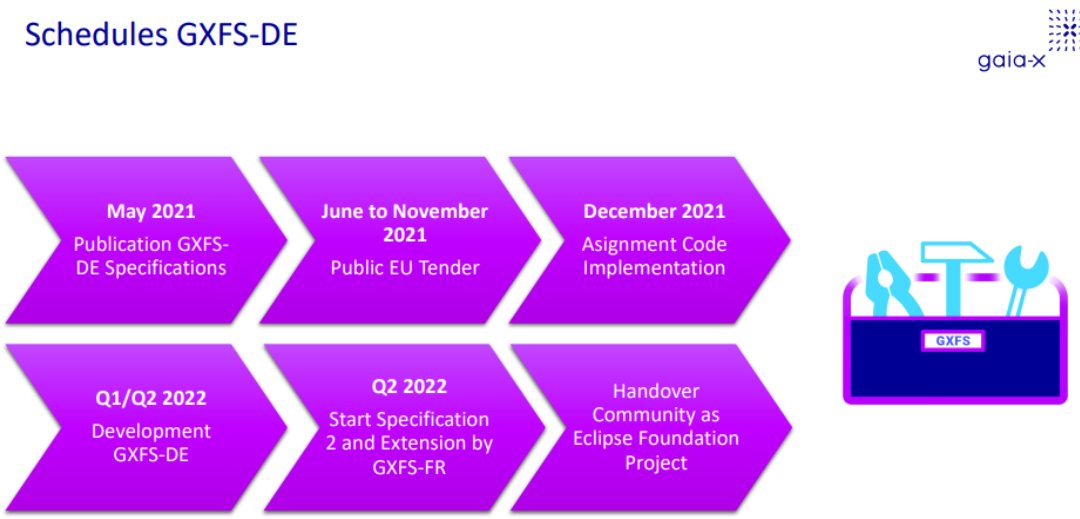


2022 年半ばまでに実装フェーズが完了し、Gaia-X が構想するフェデレーティドなエコシステムが提供される見込みである。図表 3-7 にみられるように、1 月から 6 月には GXFS-DE の開発が進められ、4 月から 6 月には GXFS-FR による仕様 2 の開始と拡大が予定されており、それ以降は Eclipse 財団プロジェクトとしてコミュニティに引き渡される予定である[44]。

[43] “Gaia-X Federation Services: Implementation Phase launched” Gaia-X, https://gaia-x.eu/news/gaia-x-federation-services-implementation-phase-launched(2022 年 3 月 16 日アクセス)

[44] “Webinar Gaia-X Federation Services (GXFS) with Andreas Weiss” Gaia-X Hub the Netherland, https://gaia-x.nl/evenementen/webinar-gaia-x-federation-services-gxfs-met-andreas-weiss/ (2022 年 3 月 16 日アクセス)

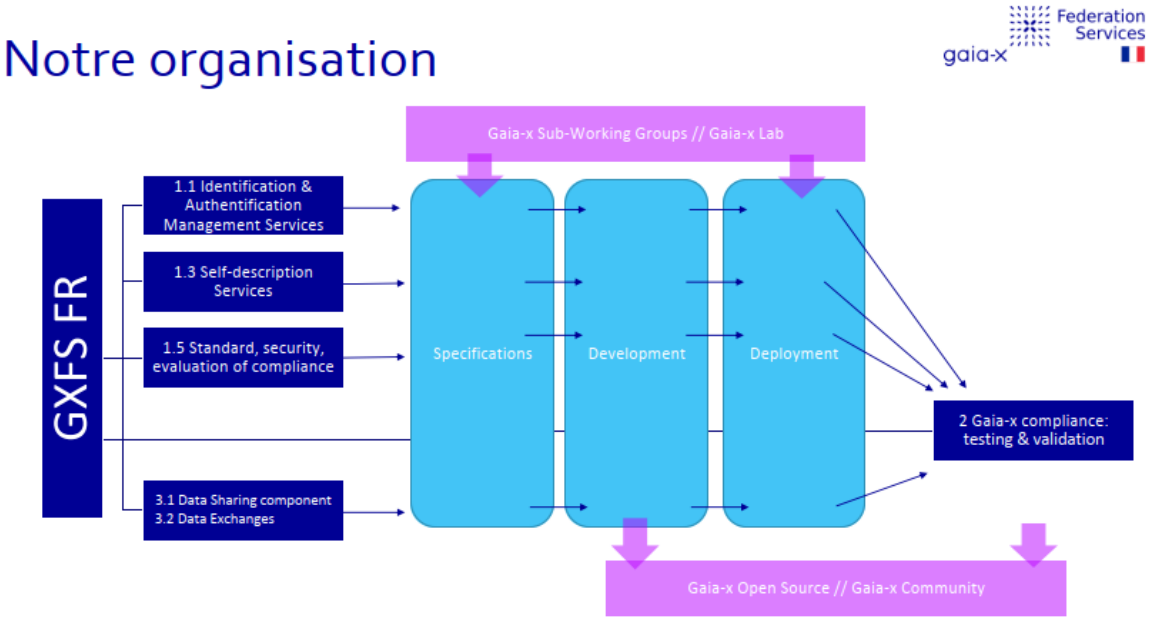
図表 3-7 GXFS-DE の 2022 年のロードマップ
（Gaia-X Hub the Netherlands2022 年 3 月 9 日ウェビナー資料）



フランスにおいてはフランス経済・財務省がスポンサーとなって GXFS-FR コンソーシアムが設立され、IMT/TeraLab を調整役として予算 1200 万ユーロを得て運営されている。各ロット（Identity Access Management, Self-description, Security and Norms, Testbeds, Data Sharing Components, Data Exchange, Management）に対応する企業、団体も決定した[45]。

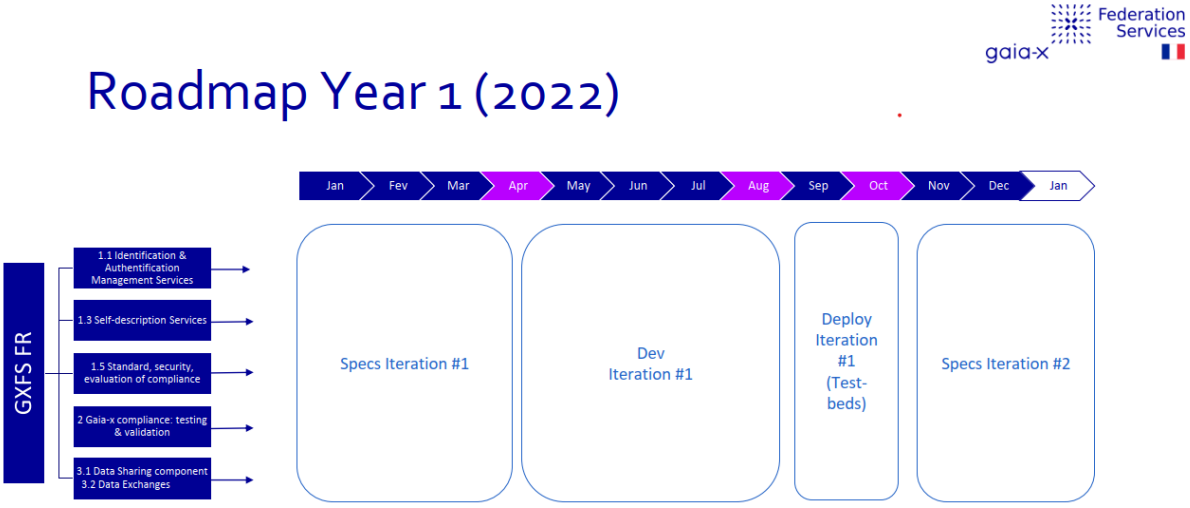
[45] Identity Access Management は 3dsoutscale、Self-description は Ovhcloud、Security and Norms は Docaposte、Testbeds は IMT 及び Teralab、Data Sharing Components は Atos、Data Exchange は Dawex、Management は IMT 及び Teralab が担当する。“PLÉNIÈRE #4” Cigref, https://www.cigref.fr/wp/wp-content/uploads/2022/03/Master-pleniere-4.pdf (2022 年 3 月 23 日アクセス)

図表 3-8 GXFS FR の組織図



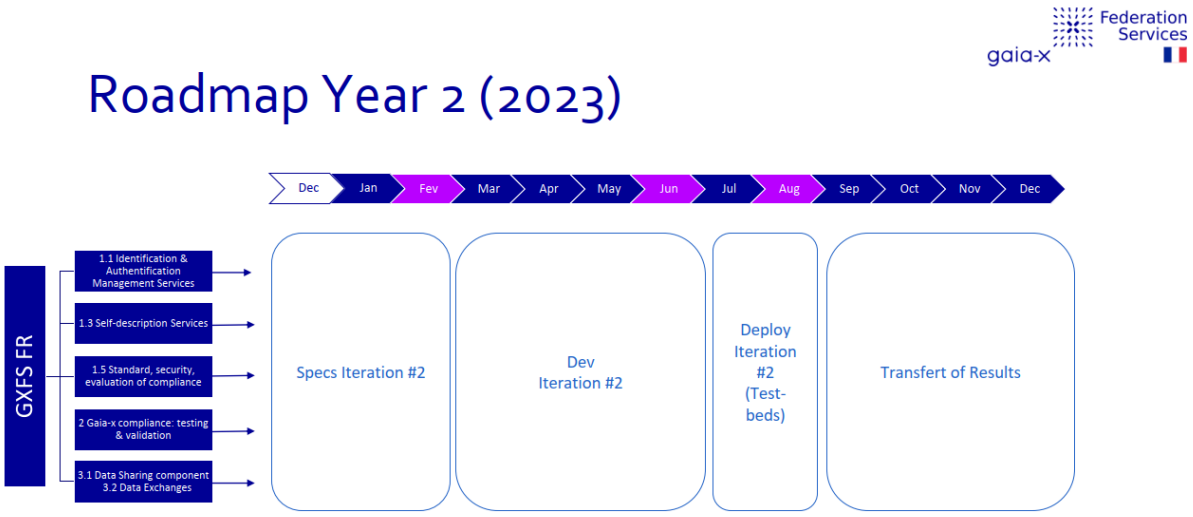
図表 3-9 及び図表 3-10 にみられるように、2022 年 1 月から 4 月にかけては仕様（#1）、4 月から 8 月にかけては開発（#1）、9 月から 10 月には配置（#1）、11 月から 2023 年 2 月にかけては仕様（#2）に取り組む予定である。そして 3 月から 6 月には開発（#2）、7 月から 8 月にかけて配置（#2）、9 月から 12 月にかけては結果の共有が行われる予定である[46]。

図表 3-9 GXFS-FR の 2022 年のロードマップ（Gaia-X Hub France 第 4 回総会資料）



[46]“PLÉNIÈRE #4” Cigref, https://www.cigref.fr/wp/wp-content/uploads/2022/03/Master-pleniere-4.pdf (2022 年 3 月 23 日アクセス)

図表 3-10　GXFS-FR の 2023 年のロードマップ
（Gaia-X Hub France 第 4 回総会資料）



フラウンホーファー研究機構のセキュアデータエコシステム研究グループ関係者によると、GXFS は将来的に分散型となることを目指しているが、現状は Gaia-X AISBL が管理しており、当面は中央集権的な運営を行う予定である。分散型 ID の実装にはかなりの時間がかかることが想定されることから、現実には特定の企業だけに利用を許可することとなる見込みである（フラウンホーファー研究機構のセキュアデータエコシステム研究グループ関係者へのインタビュー結果については、「8.3 IDSA・Gaia-X に関するインタビュー結果」を参照されたい）。

エ　Gaia-X Lab

2022 年 3 月には Gaia-X Lab の開始が発表され、Gaia-X 要件の実証が進められている[47]。Gaia-X Lab の使命は、Gaia-X ワーキンググループが作った機能や技術仮説を技術的に実証するプロトタイプを描くこと、機能するプロトタイプを示すこと、外部オープンソースソフトウェアプロジェクトの開発を促進すること、Gaia-X 仕様における機能コンポーネントの欠如を特定することとされている[48]。

(3) 今後の見通し

ア　欧州全体

Gaia-X は 2021 年から 2025 年までの中期展望を示している。この期間中に、段階的に Gaia-X から市場へプロジェクトのけん引主体を移行させていくことを想定して

[47] “Gaia-X Association moves into the adoption phase – accelerating the Gaia-X SW framework development through OSS Project and a SW Lab” Gaia-X, https://gaia-x.eu/news/gaia-x-association-moves-adoption-phase-accelerating-gaia-x-sw-framework-development-through(2022 年 3 月 16 日アクセス)
[48] “Status of Gaia-X & highlights” Gaia-X, https://gaia-x.eu/sites/default/files/2022-02/Gaia-X_standard-presentation_1422022_V10.pdf (2022 年 3 月 16 日アクセス)

いる。

2021 年は Gaia-X インフラストラクチャ及びオートメーションを重視し、リファレンスアーキテクチャ、GXFS 初版、データスペースサービスの初版に取り組んだ。

2022 年は Gaia-X データスペース、AI 及びエッジ開発に重点を置き、拡大版 GXFS、エッジクラウド実装、拡大版データスペースに取り組む。

2023 年は EU 市場での実装可能性に重点を置き、完全なフェデレーション及びコンプライアンスサービス、データスペース特有のマーケットプレイス、50%以上のメンバーによる採用を目指す。

2024 年は EU エコシステムにおける経済的実装可能性に重点を置き、40%以上の欧州 SME が Gaia-X を採用すること、50%以上の Fin/Ps/Hc（金融、電力供給、ヘルスケアを指すと考えられる）が Gaia-X を採用すること、Gaia-X サービスが独自に拡大を続ける状態となることを目指す。

2025 年には EU がグローバルデータエコノミーで活躍することが目標であり、Gaia-X の経済規模を拡大してハイパースケール CSP と競争すること、世界のトップ 10 に Gaia-X プラットフォームが入ること、欧州プラットフォーム経済が世界で 10%以上となる状態となることを目指す[49]。

イ ドイツ

Wirschafts Woche（電子版）は 2022 年 3 月 24 日、「（ロシアによる）戦争の影響で、デジタル主権の試みが鈍化している。計画されていた補助金が連邦予算から消えていた」と報道した。「ウクライナに対するロシアの侵略戦争によるターニングポイントは、ドイツのデジタルエコノミーでも感じられる。皮肉なことに、Gaia-X プロジェクトの一部であるデジタル主権に向けた試みが、一時的に鈍化させられることとなった。Wirtschafts Woche の独占取材により、予定されていた 5 プロジェクトに対する数百万ユーロの予算措置がなくなったことが分かった」と説明している。

ドイツ連邦ネットワーク庁は同年 2 月末に Gaia-X の 11 プロジェクトに対し、計 1 億 1740 万ユーロを措置すること、また 2022 年中にさらに 5 プロジェクトを承認し、予算措置する予定であることを発表していた。しかし、5 プロジェクトに支払われる予定であった数百万ユーロはキャンセルされ、そのうち 1 つのプロジェクトである Gaia-X Rescue に参画する SysEleven 社は、経済担当省から電話でキャンセルを知らされたと答えている[50]。

この報道でとり上げられた 5 プロジェクトとは、Gaia-X Hub Germany の資金調達ページに掲載されている、ZiBa（循環型建設産業）、Gaia-X Rescue（消防隊向けデータソリューション）、energy data-X（エネルギーデータスペース）、DWH4.0（森林デー

[49] Status of Gaia-X & highlights" Gaia-X, https://gaia-x.eu/sites/default/files/2022-02/Gaia-X_standard-presentation_1422022_V10.pdf (2022 年 3 月 17 日アクセス)

[50] "Aus für Gaia-X-Projekte" Wirschafts Woche, https://www.wiwo.de/politik/deutschland/fehlende-foerdergelder-aus-fuer-gaia-x-projekte/28197718.html (2022 年 3 月 28 日アクセス)

タルーム)、DIKE（法律分野のデジタルエコシステム）であるとみられる[51]。

3.2.3 主要関連団体・ドキュメント

(1) 関連団体のサマリ

Gaia-X は独仏政府から始まったイニシアティブであるが、現在は非営利団体となり、民間企業、研究機構が実質的な動きを推進している。「3.2.1 (2) イ IDSA Hub」でも述べられたように、各国 Hub は研究機関、企業団体等が主体となり運営されており、様々な団体が参加している。また、Gaia-X の GXFS については、「3.2.2 (2) ウ GXFS」でみられる企業、研究機関が実装を進めている。

また、Gaia-X は関連団体について、データ共有・データ主権、行動規範、ポリシー・認証・コンプライアンス、オープンソースフレームワークに分けて説明している。データ共有・データ主権については、IDSA（「3.2.1 International Data Spaces (IDS)」を参照されたい)、BDVA（Big Data Value Association)、UMATI[52]、行動規範については、CISPE (Cloud Infrastructure Services Providers in Europe)、EU Cloud CoC、SWIPO O (Switching Cloud Service Providers and Porting Data) [53]、ポリシー・認証・コンプライアンスについては AUDITOR : (European Cloud Service Data Protection Certification)、BSI C5、Trusted Cloud、CSPCERT (European Cloud Service Provider Certification) [54] 、オープンソースフレームワークについては OS(Open Source Business Alliance と FIWARE を挙げている[55]。

---

[51] “Förderwettbewerb Gaia-X” Bundesministerium für Wirtschaft und Klimaschutz, https://www.bmwi.de/Redaktion/DE/Dossier/gaia-x.html (2022 年 3 月 28 日アクセス)

[52] BDVA は Big Data Value Public Private Partnership プログラムを実装する団体であり、欧州が信頼ある、価値重視の AI、データ、ロボティクスの研究、開発、応用について主導的地位を維持することを目的としている。UMATI は相互運用性のための機会レベルの国際語である。*Gaia-X: The European project kicks off the next phase*, Gaia-X, 2020(https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/gaia-x-the-european-project-kicks-of-the-next-phase.pdf?__blob=publicationFile&v=7, 2022 年 3 月 17 日), p9

[53] CISPE は CISPE データ保護規範を運営する IaaS クラウドプロバイダを集めた事業者団体である。EU Cloud CoC は SCOPE Europe BVBA が主催しており、欧州データ保護要件に準拠するクラウド XaaS 行動規範 である。SWIPO はマルチステークホルダーグループであり、非個人データの EU 内の自由なフローに関する規則の第 6 条「データの移植」の適切な適用を可能にするための行動規範を運用している。*Gaia-X: The European project kicks off the next phase*, Gaia-X, 2020(https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/gaia-x-the-european-project-kicks-of-the-next-phase.pdf?__blob=publicationFile&v=7, 2022 年 3 月 17 日アクセス), p9

[54] AUDITOR は、GDPR 第 42 条に沿った EU 全体のデータ保護認証を開発している。BSI C5 は、BSI が発行したクラウドコンピューティングコンプライアンスコントロールカタログであり、クラウドコンピューティング向け情報セキュリティの要件を定義し、情報セキュリティ認証の基礎となりうるものである。Trusted Cloud はクラウドサービス向けに Trusted Cloud ラベルを発行するコンペテンスネットワークであり、クラウドラベルと認証に関する欧州基準の設定について積極的に活動している。CSPCERT は官民ステークホルダグループであり、クラウドサービスのセキュリティ認証に関連したリコメンデーションを提供している。*Gaia-X: The European project kicks off the next phase*, Gaia-X, 2020(https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/gaia-x-the-european-project-kicks-of-the-next-phase.pdf?__blob=publicationFile&v=7, 2022 年 3 月 17 日アクセス), p9

[55] OS は、デジタル主権ある社会のためのオープンソースソフトウェアとオープン標準の最重要性を人々に広め、世論を形成するための活動を行う団体である。FIWARE は様々等メイン内でスマートソリューションの開発を加速させるオープンソースプラットフォームコンポーネントを収集、整理、要約、公開したフレームワークである。*Gaia-X: The European project kicks off the next phase*, Gaia-X, 2020(https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/gaia-x-the-european-project-kicks-of-the-next-phase.pdf?__blob=publicationFile&v=7, 2022 年 3 月 17 日アクセス), p9

なお、Gaia-X、BDVA、FIWARE、IDSA は 2021 年 9 月に欧州及び欧州を越えた地域でデータスペースの採用を促進するため、Data Spaces Business Alliance(DSBA)を組織した。この団体は、産業プレイヤーが、組織や個人がデータの全ての価値を活用できる、データドリブンな将来を実現することを目標としている。

4 団体は合わせて 1,000 以上の主要産業プレイヤー、協会、研究機関、イノベーター、ポリシーメーカーを代表しており、産業を越えた専門知識、リソース、ノウハウを統合することで、認知度を向上させ、技術を広め、標準を形作り、産業を越えたインテグレーションを可能にする。

特に、既存のアーキテクチャやモデルを基に、共通参照モデルを定義すること、既存組織とデータスペースをサポートすること（ハンドブック、ロードマップ、個々の革新計画等）、合同で「Data Space Radar」を設立してデータスペースイニシアティブの全体像をつかむこと、フロントランナーであるデータスペースイニシアティブを特定し支援すること等について協力を進めていく[56]。2022 年第 1 四半期には、技術ロードマップとアジェンダを策定する予定である[57]。

(2) 団体別・時系列ドキュメント一覧

ア IDSA

IDSA は、欧州データエコノミーの中で IDS が果たす役割、IDS が依拠する概念、IDSA の戦略的立場等、全体的な概要や立場を示す戦略文書と、リファレンスアーキテクチャモデル、コネクタ、各種技術と IDS との関係性を示す技術文書、またユースケースの紹介やガバナンスに関わるその他文書を発行してきた（IDSA が発行した文書の一覧は、「8.1 IDS 発行文書」を参照されたい）。なお、本段落では文書名の後に（）で番号を付しているが、これは、「8.1 IDS 発行文書」の文献一覧の番号と対応している。

戦略文書については、IDS の全体的な概要を示した文書として、2018 年 10 月に発行された「Sharing Data while Keeping Data Ownership」（I01）にてデータ所有者がデータ価値を活用するため IDSA が推進する施策を紹介、2019 年 8 月に発行された「Fact Sheet and Core Statement Version 1.0」（I07）では IDSA の戦略的立場やコンセプトについて説明、同年 9 月に発行した「IDS Der Standard fur Datensourveranitat Und」（I08）では、データ主権の概念やデータエコシステムの重要要素について概説、2021 年 4 月に発行された「Data Sovereignty—Critical Success Factor for the Manufacturing Industry」（I24）では製造業におけるデータ主権等 IDS 主要概念の応用について解説した。

また、欧州政策や他団体との関係を示す文書としては、欧州データ戦略における IDS の役割について、2019 年 10 月に「The Role of IDS for the European Data Economy」（I09）、2020 年 4 月に「Implementing the European Strategy on Data Role of the

[56] Gaia-X: BDVA, FIWARE, Gaia-X and IDSA Launch an Alliance to Accelerate Business Transformation in the Data Economy, Gaia-X.eu ウェブサイト, https://www.gaia-x.eu/news/bdva-fiware-gaia-x-and-idsa-launch-alliance-accelerate-business-transformation-data-economy, 2021 年 9 月 23 日リリース

[57] “Assets and Achievements: Reliable Base for Trust in Data Spaces” International Data Spaces, https://internationaldataspaces.org/wp-content/uploads/IDSA-Strategic-Overview-Assets-and-Achievements-.pdf (2022 年 3 月 22 日アクセス)

IDS」（I18）を発行している。

Gaia-X との関係性については、2021 年 1 月に「Gaia-X and IDS」（I22）にて、IDS リファレンスアーキテクチャモデルがどのように Gaia-X の原則とアーキテクチャ要素と噛み合うかを説明している。

技術文書については、他の団体や技術との調整について、2018 年 10 月に「Jointly Paving the Way for a Data Driven Digitisation of European Industry」(I02)を発行、IDS におけるブロックチェーン技術の活用について、2019 年 3 月に「Blockchain Technology in IDS」(I05)を発行、また同年 12 月に GDPR 準拠のための IDS リファレンスアーキテクチャモデル向け要件を考察した「GDPR Related Requirements and Recommendations for the IDS reference Architecture」(I12)を発行した。

IDS のリファレンスアーキテクチャモデルの全体像を示す資料としては、2019 年 4 月に「IDSA Reference Architecture Model v3」（I06）を発行しており、各コンポーネントについては、IDS コネクタについて「Criteria Catalogue: Components - Connector」(I16)、クリアリングハウスについては 2020 年 4 月に「Specification: IDS Clearing House」(I17)、ブローカーについては 2020 年 5 月に「Specification: IDS Meta Data Broker」(I19)、2020 年 9 月に「Criteria Catalogue: Components - Broker」(I20)を発行した。また、データスペース設計について、2021 年には「Design Principles for Data Spaces Position Paper 2021」(I26)を発行している。

その他、IDS ユースケースに関する資料（I03、I13、I25）、ガバナンス面では IDS 認証基準（I04、I11、I14）やデータ起源・データ使用制御（I10、I23）について説明した資料、IDS ルールブック（I21）を発行している。

このように、IDS のデータエコシステムがスムーズに機能するよう、戦略・技術・応用・ガバナンス面で検討を進めている。

イ Gaia-X

Gaia-X はこれまで、イニシアティブの概念や全体像を示す戦略文書と、技術アーキテクチャ、GXFS 仕様、ラベリング等に関する技術文書を発行してきた（Gaia-X が発行した文書の一覧は、「8.2 Gaia-X 発行文書」を参照されたい）。なお、本段落では文書名の後に（）で番号を付しているが、これは「8.2 Gaia-X 発行文書」の文献一覧の番号と対応している）。

戦略文書については、2019 年 10 月に発行された、Gaia-X 誕生の背景や Gaia-X の目標、ソリューション等について説明した「Project Gaia-X」（G01）に始まり、2020 年 2 月には独仏政府が Gaia-X に関する共同声明(G02)を発表した。また同年 6 月には「Gaia-X-the European project kicks off the next phase」(G03)、「Gaia-X: A Pitch Towards Europe」(G04)、「Gaia-X: Driver of digital innovation in Europe」(G06)、「Gaia-X: Policy Rules and Architecture of Standards」(G07)の 4 文書を発行し、Gaia-X の全体像や意義、ポリシーを表明している。

2021 年に 4 月には Gaia-X エコシステムの原則、付加価値を守るハイレベルな目的を定義するポリシー・規則を記載した「Policy Rules Document (PRD 21.04)」(G19)を発表し、同年 12 月には Gaia-X のビジョンと使命、主要課題、コアバリューやベネ

フィットについて説明した「Vision & Strategy」(G27)を発行した。

技術文書については、初の技術アーキテクチャ文書（G05）を 2020 年 6 月に発行して以降、四半期ごとに技術アーキテクチャの更新版を発行している（G18、G21、G24、G28)。2022 年 3 月 18 日時点で最新版は「Gaia-X Architecture Document 21.12 Release」（G28）であるものの、2022 年にも第 1 四半期、第 2 四半期、第 4 四半期に更新版が発行される予定である[58]。

また、ラベリングに関しては、2021 年 11 月にラベリングの意義、コンプライアンス、価値や原則を説明し、ラベル所有者や発行者を定義した「Gaia-X Labelling Framework」(G25)を発行し、2022 年 2 月にはラベリング施策や具体的基準を詳説した「Gaia-X Labelling Criteria Version 0.7」(G42)を公開した。

各ドメインにおける検討も進んでおり、2021 年 1 月から 3 月にかけては農業、金融、モビリティ、スマートシティ/スマートリージョン、ヘルス、地理情報、エネルギー、インダストリー4.0/SME、公共部門におけるデータスペースの現状、課題、ユースケースについて説明した政策方針書を発行している（G08-17)。

図表 3-11 Gaia-X 発行の技術文書とその他文書の時系列
（各文書の詳細は「8.2 Gaia-X 発行文書」を参照）

発行状況	2020	2021				2022			
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
アーキテクチャ	6月 G05	3月 G18	6月 G21	9月 G24	12月 G28	3月 22.03	6月 22.06		出版月不明
GXFS			春 G29-41		12月 G26				
ラベリング				11月 G25		2月 G42			
技術仕様						出版月不明		出版月不明	
Gaia-X コンプライアンス						出版月不明	出版月不明	出版月不明	出版月不明
ビジネス適用・ユースケース				8月 G22					
ドメイン別ユースケース		1月-3月 G08-17	4月 G20	9月 G23					

3.2.4 欧州における関連取組に関する考察

「3.2.2（1）立ち上げとその目的」で述べた通り、Gaia-X が拡大する中で、非欧州の巨

[58] “Status of Gaia-X & highlights” Gaia-X, https://gaia-x.eu/sites/default/files/2022-02/Gaia-X_standard-presentation_1422022_V10.pdf (2022 年 3 月 17 日アクセス)

大企業がメンバーに加わって存在感を発揮するようになったことから、Gaia-X が欧州理念の実現や欧州競争力の強化といった当初の目的にそぐわない組織と化したとの批判が噴出している。Gaia-X 内には非欧州企業にオープンなグループとその参加に反対するグループが存在する。概して、前者には産業プレイヤー、ドイツやオランダの団体が多く、後者はクラウドプロバイダ、フランス、イタリア、スペインの団体が多い。

この問題は、2021 年 11 月にミラノで開催された Gaia-X 第 2 回サミットのスポンサーに中国企業の Huawei と Alibaba がなったことで顕在化し、フランスのクラウドプロバイダ企業で Gaia-X 創設メンバーである Scaleway が Gaia-X 脱退を表明、同じくフランスのクラウドプロバイダ企業 Hosteir も続いた。これらの企業は、ドイツ・オランダ政府が非欧州企業に Gaia-X の門戸を開くことを支持しており、理事会メンバーである Digital Europe、CISPE、Bitkom 等の協会は、Amazon や Google 等米国の巨大企業の利益を支持していると批判した[59]。Gaia-X Hub France を主宰する Cigref の CEO は、Hub 開設時のインタビューにて、Gaia-X が自己決定権を持つこと（外部圧力に影響を受けず、欧州プレイヤーが中心となって執行すること）、欧州と欧州市民に資すること、欧州経済復興と将来への準備に資することを重視していると表明しており[60]、概してフランスに本拠地を置く団体は欧州のデータ主権を取り戻すこと、また欧州発のインフラストラクチャを活用することに大きな期待を寄せていると言える。

一方、国ごとの対立ではなく、各企業・団体の利害関係のため意見の衝突が発生している見方もある。これは、既存の（米国の）インフラストラクチャを用いて発展したい産業プレイヤーと、独自に構築した欧州産のインフラストラクチャ、クラウド、サービスの欧州での利用を拡大したいクラウドサービスプロバイダ間の対立であるとも考えられる。

非欧州企業の参画にオープンなグループには、ドイツの産業プレイヤー、BMW、フォルクスワーゲン、ドイツ銀行等、既に非欧州のクラウド技術に依存している企業が多く[61]、欧州企業は米国企業により既に広められた基礎インフラの上にクラウドを設計することで機会を得ることができると考えている。

このグループは、欧州でのデータ保存や欧州産のクラウドプラットフォーム利用は、ユーザに対してベネフィットなしでコストを増大させ、結果的に米国巨大企業の市場占有を高めると考えている。欧州ユーザは欧州クラウドインフラのために不要な追加料金を払わされることを恐れており、公的に支援された欧州公共クラウドが民間クラウドのように高いセキュリティや環境をもたない可能性があることも懸念していると強調する。

実際、Microsoft は既存の Microsoft Azure の料金に 30%上乗せすることで、データをドイツ国内に保存するサービスを提供したが、需要は非常に弱く、サービスを停止した。このように、非欧州企業の参入にオープンなグループは、欧州産のサービス、欧州内のデー

[59] “Inside Gaia-X: How chaos and infighting are killing Europe’s grand cloud project” Politico, https://www.politico.eu/article/chaos-and-infighting-are-killing-europes-grand-cloud-project/ (2022 年 3 月 24 日アクセス)

[60] “#Gaia-X: Cigref welcomes the launch of the Gaia-X initiative, in favour of the emergence of a trusted European cloud market,” Cigref ウェブサイト, https://www.cigref.fr/gaia-x-cigref-welcomes-launch-initiative-trusted-european-cloud-market, 2020 年 6 月 4 日リリース

[61] “Full steam ahead towards a true multi-cloud offering to deliver on broken promises,” Scaleway ウェブサイト, https://blog.scaleway.com/full-steam-ahead-towards-a-true-multi-cloud-offering-to-deliver-on-broken-promises/, 2021 年 11 月 30 日リリース

タ保存は、現実的にユーザに受け入れられないと主張しているのである[62]。

Gaia-X Workstream 2（Technical Implementation）コーディネータは、Gaia-X は米中IT 企業への対抗というより、欧州の法律に従ってシステムを構築するために開発されたのであり、米中企業も Gaia-X 標準に従えば参画を歓迎されると述べている（Gaia-X Workstream 2（Technical Implementation）コーディネータへのインタビュー結果については、「エラー! 参照元が見つかりません。エラー! 参照元が見つかりません。」を参照されたい）。

一方の非欧州企業の参画に反対するグループは、非欧州企業の参加は Gaia-X の当初の目的である「信頼できる、主権ある欧州のためのデジタルインフラ」創設に反しており、Gaia-X 理事会のガバナンスを非欧州企業が担うべきではないと主張する[63]。このように、両者の間に Gaia-X の目的について大きな認識の差が存在しているといえる。

Gaia-X への非欧州企業の影響力の懸念は欧州議会でも取り上げられており、2021 年 11 月 22 日にはオランダ選出の Sophia in 't Veld 議員が書面で質問状を提出し、欧州委員会に対して Gaia-X に対する姿勢を問いただした。具体的には、①中国企業の支援を受けた Gaia-X が、EU の目標である欧州データ主権の主要な貢献者であると考えているのか②欧州委員会の計画に Gaia-X を含める明確な戦略を持っているのか③戦略がないのであれば、Gaia-X の年次総会でどのようなメッセージを送るかである[64]。2022 年 3 月 29 日時点で、この質問に対する回答は出されていない。

また、2021 年 11 月 30 日には、フランス選出の Joëlle Mélin 議員が書面で質問状を提出し、Gaia-X が今や米中企業の影響下にあり、Scaleway が Gaia-X を去った中で、①欧州委員会は欧州のデータセキュリティとデジタル依存をどのように担保しようと考えているか②欧州委員会が執行責任を持つ反保護主義、非差別原則と矛盾しない、正当な目標であると言えるかと尋ねている[65]。

これに対し、2022 年 3 月 1 日に欧州委員会の Breton 委員が下記の回答を出している。

「Gaia-X は民間主導のイニシアティブである。欧州委員会は Gaia-X に関係なく（not affiliated to it）、EU 内で活動する組織として、Gaia-X に競争法に関連する EC 法に準拠することを求めている。欧州委員会は（Gaia-X の）メンバーシップに関する判断に何の影響力も有していない。

欧州委員会の目標は、欧州市民や企業が自身のデータに対するコントロールを保持し、EU の高度なデータ保護、セキュリティ基準を尊重したデータ処理を担保することである。EU データポリシーは、データインフラのレジリエンスやインテグリティを担保する必要があるデジタル主権に向けて、オープンだが強いアプローチを反映している。

欧州委員会は European Alliance on Industrial Data, Edge and Cloud を設立し、産業と加盟国間の投資を調整・合理化する支援をしようとしている。この Alliance はさらなる市

---

[62] “Europe’s Cloud Dreams Come Crashing Down to Earth” CEPA, https://cepa.org/europes-cloud-dreams-come-crashing-down-to-earth/ (2022 年 3 月 24 日アクセス)

[63] “Full steam ahead towards a true multi-cloud offering to deliver on broken promises,” Scaleway ウェブサイト, https://blog.scaleway.com/full-steam-ahead-towards-a-true-multi-cloud-offering-to-deliver-on-broken-promises/, 2021 年 11 月 30 日リリース

[64] “Question for written answer E-005217/2021” European Parliament, https://www.europarl.europa.eu/doceo/document/E-9-2021-005217_EN.html (2022 年 3 月 17 日アクセス)

[65] “Question for written answer E-005332/2021” European Parliament, https://www.europarl.europa.eu/doceo/document/E-9-2021-005332_EN.html (2022 年 3 月 17 日アクセス)

場の分裂を防ぎ、EC 法に準拠したデータ処理能力の連合（federation)を促進すべきである。Alliance は全てのステークホルダからの出願に対しオープンである。

しかし、入会については、Alliance の目的に関して出願者の実質的有用性の詳細な評価、また出願者による全ての合理的技術・法・組織的な手法の実装に関する詳細な評価によって決定される。これは、EU 又は加盟国法の下で違法となる EU 内にあるデータへのアクセス又は移転を防ぐためである。

このアプローチは EU の、非差別原則に則っており、オープンで競争あるデジタル単一市場を強化するものである。Alliance はステークホルダが主体となったイニシアティブである。欧州委員会は議論やデリバラブルの実装のため共通の土台を見つける調整者の役割を果たす[66]。」

つまり、Gaia-X はあくまで民間主導のイニシアティブであり、欧州委員会は何ら関与していないと述べた上で、欧州委員会は European Alliance on Industrial Data, Edge and Cloud を通してビジョンを実現しようとしているということを強調しているのである。

上記の通り、非欧州企業が Gaia-X に影響力を行使しているとの懸念が広がる一方、非欧州企業が Gaia-X を既に見限ったという指摘もある。グローバルリサーチ・コンサルティング企業である Forrester 社のアナリスト Paul McKay 氏は、Gaia-X が開始から 2 年経っても約束したサービスを提供していない中、米国の巨大企業に影響を与えてきたのは独仏政府の（Gaia-X 以外の）イニシアティブであったと主張している。これらのイニシアティブが AWS や Azure、Google GCP の透明性を向上させ、結果的に米国大企業が公共クラウドプロジェクトを独占する助けとなったと説明する。

同氏はクラウド主権に関する主要なプロジェクトは Gaia-X 抜きで進められ、欧州国家と米国のクラウド大企業の間で設立されると考えており、2022 年にクラウド主権の中心に Gaia-X はもはや存在しないと主張している。Gaia-X の進捗の遅さにフラストレーションを覚えた米国の巨大企業も、Gaia-X を通してではなく直接欧州諸国の政府と対話することを模索していると指摘しているのである[67]。

このように、Gaia-X 以外のクラウド主権に関するイニシアティブや、Gaia-X に似た団体が存在していることから、これらの活動についても留意していく必要があろう。

(1) European Alliance on Industrial Data, Edge and Cloud

European Alliance on Industrial Data, Edge and Cloud（以降、Alliance と呼ぶ）は 2021 年 7 月に欧州委員会によって設立された。将来の欧州クラウドサービス開発を活発化させ、EU 産業の地位強化を図ることを目的としている。2022 年 2 月 17 日時点で 47 団体が参加しており、その中には Gaia-X を脱退した Scaleway や、現 Gaia-X メンバーも多数も含まれる。

主なタスクとしては投資シナジー効果を最大化させること、共通欧州データスペース

[66] “Answer given by Mr Breton on behalf of the European Commission (1 March 2022), European Parliament, https://www.europarl.europa.eu/RegData/questions/reponses_qe/2021/005332/P9_RE(2021)005332_EN.pdf (2022 年 3 月 17 日アクセス)

[67] “Cloud souverain : « Gaia-X n’est plus au centre des discussions »” LeMagIT, https://www.lemagit.fr/actualites/252512041/Cloud-souverain-Gaia-X-nest-plus-au-centre-des-discussions (2022 年 3 月 24 日アクセス)

のシナジー創出プラットフォームを提供すること、EU クラウドルールブックの準備の文脈で窓口となること、クラウドサービス公共調達の共通標準や要件について専門知識を提供し、データ処理サービスの公共調達向け共通仕様を含めて欧州委員会と加盟国間の調整プラットフォームを提供することを掲げている。

Gaia-X との差異については、Alliance は Gaia-X と同じ目標を追求しているわけではなく、同じようなガバナンス体制を持つわけではないと、Alliance メンバーの多くが説明している。Alliance はクラウドやエッジ技術産業が直面する主要課題を議論する場であり、技術要件を調整することを目的とした標準化団体ではないとされる。

Gaia-X を脱退した Scaleway は、「Alliance は欧州事業者を一つにし、欧州のイノベーションを作り出すことで、米国やアジアの巨大企業にクラウドやエッジの分野で依存しなくて済むようにすることを重視している」とし、「Gaia-X のようなイニシアティブに比べて、この Alliance は公から始まったものであることから、正当性がある」とコメントしている。

また、Gaia-X メンバーである Clever Cloud も、同 Alliance の発足に際して「Gaia-X の背景にある思想は、「欧州にあるクラウド」を達成することであり、「欧州クラウド」ではなかったということを、最初から勘違いしていた」とコメントしている[68]。

このように、目的やガバナンス構造、機能は異なるものの、類似した団体が欧州委員会主導で設立されたことは、欧州におけるクラウドに対する欧州プレイヤーの多様な立場を示している。Alliance は発足から日が浅く、その活動の詳細は現段階で情報が少ないが、今後 Gaia-X とどのような関係を築いていくかに注目が集まる。

(2) European Cloud Industrial Alliance（EUCLIDA）

European Cloud Industrial Alliance（EUCLIDA)は、欧州が米国又はアジアのモデルに従わずに最先端のクラウド技術でグローバルリーダーとなることを目的とし、2021 年 7 月に欧州企業 23 社が設立した団体である。EUCLIDA には Clever Cloud、Nextcloud、RapidSpace、Scaleway、XWiki 等 Gaia-X メンバー（及び元メンバー）も参加している[69]。

Gaia-X との関係性については、EUCLIDA は理事会、メンバー、主要目的の観点で差異を説明している。理事会については、EUCLIDIA は独自のクラウド技術を作り出す欧州企業（中小企業が多い）の CEO で構成されている一方で、Gaia-X の理事会は欧州大企業又は研究機関で、AWS、 Azure や Google と戦略的パートナーシップを結びクラウドを運用又は使用する機関のマネージャで構成されている。

メンバーについては、EUCLIDIA は、欧州ベースの企業であり、独自のクラウド技術を作り出す欧州ベースのシェアホルダーが参加する一方で、Gaia-X は全ての国のクラウドユーザやクラウドプロバイダで構成されている。

主要目標については、EUCLIDA は欧州で作られたクラウド技術の採用と推進を目指

[68] “European Commission launches new data and cloud alliance” EURACTIV, https://www.euractiv.com/section/digital/news/european-commission-launches-new-data-and-cloud-alliance/ (2022 年 3 月 17 日アクセス)
[69] “Members” European Cloud Industrial Alliance, https://www.euclidia.eu/members/ (2022 年 3 月 17 日アクセス)

す一方、Gaia-X はクラウドプロバイダ向けコンプライアンスポリシーを開発することを目指している。[70]

3.3 ユースケース

将来的に、Gaia-X は様々なクラウドプロバイダから製品やサービスポートフォリオにアクセスすることを可能にし、全てのユーザが各々のニーズに最適なソリューションを選ぶことができるようにすることを目指している。

ユーザは Gaia-X の開発とデータスペース革新の基礎を築く役割を果たす。Gaia-X において、ユーザは自身のデータに対する主権を保持しており、全てのユーザと全ての企業が自身のデータをどこに保存するか、誰が何の目的でデータを処理するかを決定することができる。また、データインフラを通してデータプールや AI アプリケーションにアクセスすることも可能である。

データは企業間で交換可能で、他のデータとリンクされ、価値を生み出すために処理・使用される。このプロセスがイノベーションを促進し、シナジーを可能にし、新たなビジネスモデル開発を促進する。

Gaia-X Hub では異なる産業から様々なユースケースが示されており、データインフラストラクチャの価値を示している。Gaia-X Hub の目標は、主権あるデータインフラストラクチャの付加価値やニーズを提示しつつ、継続的に新たなユースケースを特定、開発、実装することである。 更に、ユースケースはセクター特有、セクターを越えた要件を定義する助けとなり、Gaia-X の開発に組み込まれる[71]。

3.3.1 IDSA のデータスペース・ユースケース

IDSA は、データスペースをデータの将来を担う場（Where the future of data happens）と呼んでおり、IDSA のビジョンが、セキュアで主権あるデータ交換、データスペース（欧州及び世界中の企業・産業のガバナンスと認証について、IDSA 標準が規定する信頼あるパートナー間の関係を構築する役割を果たす）に依拠していると説明している。

企業は保護・シェア・マネタイズできない膨大な価値あるデータを保有している。IDSA 標準は統一規則、認証データプロバイダ、受領者、パートナー間の信頼が特徴であるデータスペースを通してデータ共有を可能にする。データスペースは実りあるコラボレーションの基礎を提供し、参入障壁を下げ、データエコノミーにおける将来の限りないイノベーションを可能にする。

このため、より多くの企業が IDS をデータ共有のモードとして実装し、政府機関が IDS をグローバルスタンダードとして採用した時、データの未来が真に訪れると IDSA は主張している[72]。

---

[70] “FAQ” European Cloud Industrial Alliance, https://www.euclidia.eu/faq/ (2022 年 3 月 17 日アクセス)
[71] “Use cases” Gaia-X.eu, https://www.gaia-x.eu/use-cases (2022 年 3 月 17 日アクセス)
[72] “DATA SPACES Where the future of data happens” International Data Spaces Association, https://internationaldataspaces.org/why/data-spaces/ (2022 年 3 月 17 日アクセス)

IDSA はウェブサイトで参画企業・団体が実装した 17 ユースケースを紹介している。Fraunhofer ISST 及び COSMOPlat による Intelligent Clothing Detection Within A Washing Machine、IBM、Fraunhofer ISST 及び thyssenkrupp による Industrial Additive Manufacturing Services - Solving the Trust Issue in Distributed Production Networks、German Edge Cloud による ONCITE - Sharing Data in the Supply Chain、SAP 及び Fraunhofer による Collaborative Warranty and Quality Management、Deutsche Telekom による Telekom Data Intelligence Hub - Creating Value from Data 等、幅広い分野でユースケースが実装されている。

3.3.2 Gaia-X のデータスペース・ユースケース

Gaia-X において、データスペースとは、概してデータの補完と共有について同等の高度な標準や規則を持つ信頼あるパートナー間のデータ関係の一類型を指す。データスペース概念の重要性は、データが中央ではなく情報源に保存されており、必要な時にだけ相互運用性を通して共有されることにある。

Gaia-X の文脈では、データスペースにあるデータは Gaia-X AISBL のメンバーによってのみ保持される。データスペースは、データプロバイダ、ユーザ、仲介者等全ての参加者により構成される。データスペースはネスト化され、重なり合うこともあるため、データプロバイダは一度にいくつものデータスペースに参加することがあり得る。

データ主権とトラストはデータスペースの機能及び参加者間の関係のため必須であり、これを担保するため Gaia-X AISBL の創設者の一つである IDSA は参加者向けにリファレンスアーキテクチャモデルを提供している。各データスペースは特定のデータを提供し、各エコシステムの基礎を築く。データスペース実装に必要となるソフトウェアは、クラウド/エッジクラウドインフラストラクチャ上で動作する[73]。

Gaia-X.eu はウェブサイト上で下記 7 種のデータスペースを紹介している。

(1) Industry4.0/ Small to medium-sized enterprises

本データスペースには 50 以上の参加者がおり、共同製造やサプライチェーンプロセス、仮想アバター、サプライチェーン・輸送・ヘルス等異なる 2 産業間のインターフェース等のユースケースが進められている[74]。

2022 年 3 月 17 日時点で、Gaia-X のウェブサイト上では EuProGigant - European Production Giganet、Integration of Data along the Life Cycle of Production Machines、Enabling Full Transparency in the Supply Chain、Improving the User Experience and developing innovative Forms of User Experience、Collaborative Condition Monitoring 等多数のユースケースが紹介されている[75]。

[73] “Data spaces” Gaia-X.eu, https://www.gaia-x.eu/what-is-gaia-x/data-spaces (2022 年 3 月 17 日アクセス)
[74] “ Data spaces” Gaia-X.eu, https://www.gaia-x.eu/what-is-gaia-x/data-spaces (2022 年 3 月 17 日アクセス)
[75] “Use cases” Gaia-X.eu, https://www.gaia-x.eu/use-cases (2022 年 3 月 17 日アクセス)

(2) Health

本データスペースは、ヘルスケアの提供を変革するデジタル技術やクラウドソリューションの利用を促進することを目的に、官民コンソーシアムを設立するため活動している。Gaia-X のセキュアなエコシステムは、ヘルスデータサイロの普及やシステム間の相互運用性の欠如を含む、COVID-19 パンデミックによって注目された課題に対応することができると考えられている[76]。

2022 年 3 月 17 日時点で、Gaia-X のウェブサイト上では AIQNET、Berlin Health Data Space、Smart Health Connect、Research Platform Genomics、Future Care Platform 等多数のユースケースが紹介されている[77]。

(3) Education & Skills

本データスペースは教育コミュニティ全体の利益のためのデータスペースを作ることを目的としている。2021 年にフランスのイニシアティブとして開始し、官民からステークホルダを集めて様々なワーキンググループを設立した。現在、品質の高い教育と生涯学習のため、信頼あるデータと透明性を持ったオープンで相互運用可能なデジタルエコシステムを推進する欧州ロードマップを構築するため、幅広い企業に参加を要請している[78]。

2022 年 3 月 17 日時点で、Gaia-X のウェブサイト上では Integration of Data along the Life Cycle of Production Machines、Soil-X、Green Energy Certification、Automatic 3D Spatial Content Generation、iMouse - Development of a holistic digital medical record for laboratory rodents 等、多数のユースケースが紹介されている[79]。

(4) Energy

本データスペースは、エネルギーサービスを支援する。全てのステークホルダ間の協力を強化するデータスペースは、エネルギーセクターにおける脱炭素化の基礎である。今日、幅広い欧州エネルギー企業、アカデミア、技術パートナーが Gaia-X に参加し、欧州エネルギーデータスペースを構築しようとしている。

本データスペースは、エネルギー効率やセクター結合の強化、欧州電気システムにおける再生可能エネルギーを統合する柔軟性の拡大、エネルギーシステムのデジタル化の推進、エネルギーセクターにおける欧州連合技術主権とグローバル競争力の維持といった課題に取り組んでいる。また、再生可能エネルギー、水素、原子力、エネルギー効率、電気自動車、ローカルエネルギーコミュニティ、ネットワーク・コンプライアンス・トレーサビリティの 8 トピックについてユースケースの開発を進めている[80]。

2022 年 3 月 17 日時点で、Gaia-X のウェブサイト上では Green Energy Certification、Data Space Energy: Renewables、Data Space Energy: Compliance and Traceability、

---

[76] “Data spaces” Gaia-X.eu, https://www.gaia-x.eu/what-is-gaia-x/data-spaces (2022 年 3 月 17 日アクセス)
[77] “Use cases” Gaia-X.eu, https://www.gaia-x.eu/use-cases (2022 年 3 月 17 日アクセス)
[78] “Data spaces” Gaia-X.eu, https://www.gaia-x.eu/what-is-gaia-x/data-spaces (2022 年 3 月 17 日アクセス)
[79] “Use cases” Gaia-X.eu, https://www.gaia-x.eu/use-cases (2022 年 3 月 17 日アクセス)
[80] “Data spaces” Gaia-X.eu, https://www.gaia-x.eu/what-is-gaia-x/data-spaces (2022 年 3 月 17 日アクセス)

Data Space Energy: Energy Networks、Data Space Energy: Local Energy Communities 等多数のユースケースが紹介されている[81]。

(5) Mobility

本データスペースは、エコシステムメンバー向けに新たなビジネス機会を創出しつつ、モビリティにおけるユーザ体験を強化することを目的としている。トラベルデータは航空会社やホテル等多くの異なる場所に保存されることが多いという課題に対処しつつ、どのようにデータ主権を担保し、プライバシーを守り、産業が流動性を持つ中でも産業を助成するかを主要課題としている[82]。

2022 年 3 月 17 日時点で、Gaia-X のウェブサイトでは 5 つのユースケースが紹介されている（Decentralized in-vehicle MLaaS to EV energy efficiency、Mobility - Data Interoperability and Data Sovereignty、Digital Parking Management、Testbed Lower Saxony、Smart Mobility Innovation）[83]。

(6) Finance and Insurance

本データスペースは、独仏銀行、欧州クラウドサービスプロバイダ、公共機関や保険企業によって設立されたが、現在はイタリア、ルクセンブルク、ベルギー、フィンランド、オーストリア、ポーランド等にも広がっている。現在、ワークショップを通して 2022 年目標の優先付けを行っている[84]。

2022 年 3 月 17 日時点で、Gaia-X のウェブサイト上では 3 つのユースケースが紹介されている（Financial Big Data Cluster (FBDC)、Sustainable Finance、Pay-per-Use Supply Chain Finance）[85]。

(7) Space

本データスペースは 2020 年 11 月末に設立された。我々の生活が空間（又は宇宙）データに依拠している度合いを鑑みると、欧州データ主権を保ちつつこのデータを安全に効率的に取り扱うことは必須であると考えられる[86]。

2022 年 3 月 17 日時点で、Gaia-X のウェブサイト上では Geoinformation の分野で 5 つのユースケースが紹介されている（Automatic 3D Spatial Content Generation、Earth Observation federated data access for European Economy、Space4Cities、Smart Infrastructure Management、Smart Urban Planning）[87]。

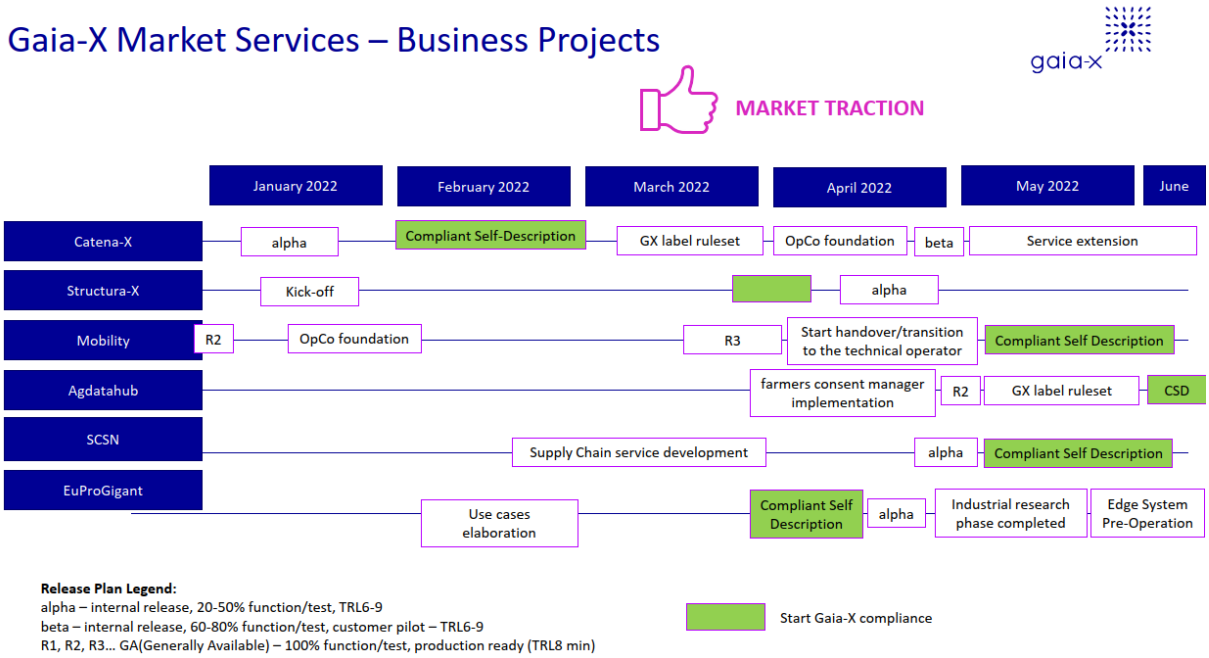
---

[81] “Use cases” Gaia-X.eu, https://www.gaia-x.eu/use-cases (2022 年 3 月 17 日アクセス)
[82] “Data spaces” Gaia-X.eu, https://www.gaia-x.eu/what-is-gaia-x/data-spaces (2022 年 3 月 17 日アクセス)
[83] “Use cases” Gaia-X.eu, https://www.gaia-x.eu/use-cases (2022 年 3 月 17 日アクセス)
[84] “Data spaces” Gaia-X.eu, https://www.gaia-x.eu/what-is-gaia-x/data-spaces (2022 年 3 月 17 日アクセス)
[85] “Use cases” Gaia-X.eu, https://www.gaia-x.eu/use-cases (2022 年 3 月 17 日アクセス)
[86] “Data spaces” Gaia-X.eu, https://www.gaia-x.eu/what-is-gaia-x/data-spaces (2022 年 3 月 17 日アクセス)
[87] “Use cases” Gaia-X.eu, https://www.gaia-x.eu/use-cases (2022 年 3 月 17 日アクセス)

3.3.3 Gaia-X 関連イニシアティブ

様々なセクターで Gaia-X に準拠したイニシアティブが進められている。ここでは先行して既にユースケースが多数公開されている Catena-X、Mobility Data Space、SCSN や、2021 年末に開始された Structura-X について概説する。

図表 3-12 Gaia-X に準拠したビジネスプロジェクトの 2022 年ロードマップ
（Gaia-X Hub France 第 4 回総会資料）



(1) Catena-X

ア 組織概要・現状

Catena-X は自動車のバリューチェーンにおける安全なデータ交換、透明性を担保することで産業全体のコラボレーションを促進し、イノベーションを生み出すこと、サプライチェーンの最適化による環境対策強化等を目標とし、2021 年 3 月に発足、同年 5 月 7 日に創立会議が開催された。

2022 年 3 月 1 日時点で 88 メンバーが所属しており、日系企業としては Asahi Kasei Europe GmbH、Denso Automotive Deutschland GmbH、NTT Communications Corporation が含まれる[88]。資金面ではドイツエネルギー省が 2022 年まで同プロジェクトに 1 億 3,600 万ユーロの予算措置を発表している[89]。

ドイツ企業は高い環境目標への対応、サプライチェーンのデューデリジェンス強化

[88] “Catena-X Automotive Network e.V.” Catena-X, https://catena-x.net/fileadmin/user_upload/downloads/20220301_catena-x_aktuelle_mitgliederliste_eng.pdf （2022 年 3 月 23 日アクセス）
[89] “Projekte zur Stärkung der digitalen Souveränität” Bundesministerium für Wirtschaft und Energie, https://www.bmwi.de/Redaktion/DE/Parlamentarische-Anfragen/2022/02/1-76-anlage.pdf?__blob=publicationFile&v=4 (2022 年 3 月 18 日アクセス)

義務、サプライチェーンの逼迫やそれに伴う価格上昇に直面しており[90]、Catena-X は自動車産業における安全なデータ交換、透明性の担保、最適化により、これらの課題に対するソリューションを提供する。

イ 2022 年の動き

2022 年 1 月にはα版（内部リリース、20-50%の機能/テスト、TRL 6-9）を発表し、2 月には Gaia-X への準拠を開始、Self-description についても準拠する予定である。3 月には GX ラベルルールセット、4 月には OpCo foundation（オープンコードファウンデーションと想定される）及びβ版（内部リリース、60-80%の機能/テスト、カスタマーパイロット、TRL 6-9)の発表、5 月にはサービス拡張が予定されている[91]。

また、5 月 30 日から 6 月 2 日に開かれる Hannover Messe にて、始めて現状について紹介される見込みである[92]。また、SME マチュリティレベルの飛躍と価値創造のため、1,000 のパートナーとの接続・検証を行い、ユースケースが機能的に完成、自動車データスペース標準化を目指している[93]。さらに、SME 向けに Catena-X の働きと結果について包括的なノウハウが公開される予定である（2022 年初めとの記載あり）[94]。

[90] “デューデリジェンス法が成立、2023 年 1 月に施行” JETRO, https://www.jetro.go.jp/biznews/2021/06/e19fe7d028599c7e.html (2022 年 3 月 16 日アクセス); “ドイツ企業、6 割超がサプライチェーン逼迫や価格上昇の課題に直面” JETRO, https://www.jetro.go.jp/biznews/2022/02/c0dab67316278e01.html?_previewDate_=null&revision=0&viewForce=1&_tmpCssPreview_=0 (2022 年 3 月 16 日アクセス)

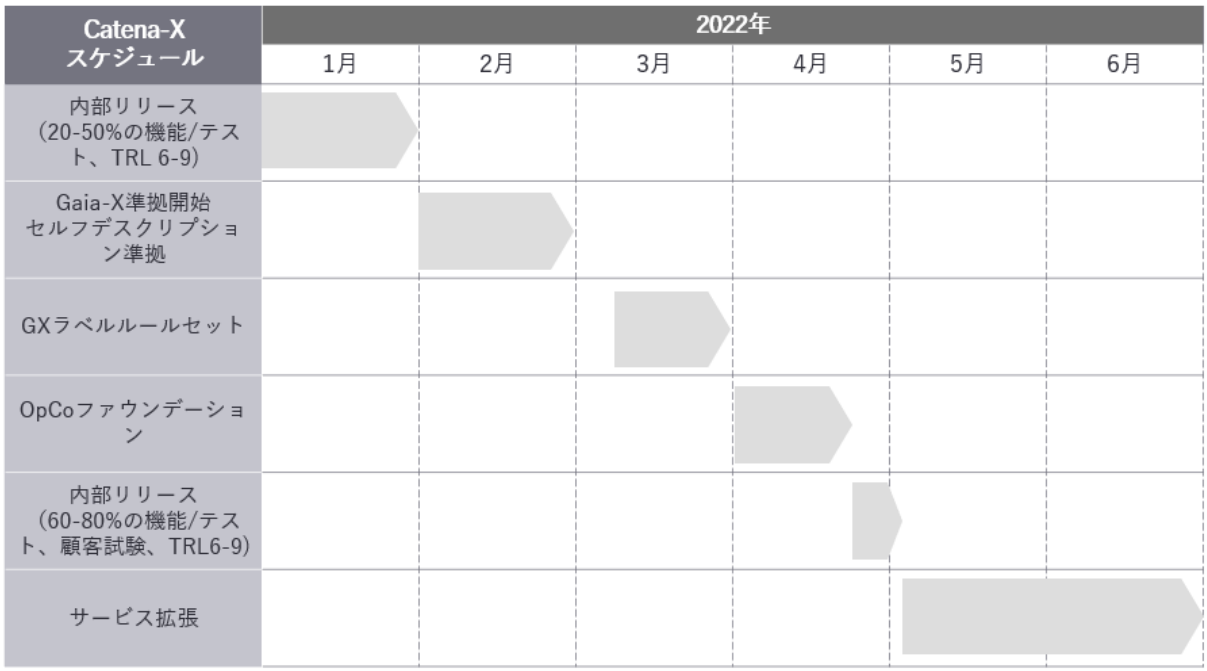
[91] “PLÉNIÈRE #4” Cigref, https://www.cigref.fr/wp/wp-content/uploads/2022/03/Master-pleniere-4.pdf (2022 年 3 月 23 日アクセス)

[92] “Catena-X will be presented for the first time at the Hannover Messe 2022,” Catena-X ウェブサイト, https://catena-x.net/de/news/18-feb-2022-catena-x-praesentiert-sich-erstmals-auf-der-hannover-messe-2022, 2022 年 2 月 18 日リリース

[93] “Catena-X Automotive Network- Building the First Operating System for a Data Driven Value Chain - “ Catena-X, https://catena-x.net/fileadmin/user_upload/intro_praesenationen/catena-x_overview_eng_v2.2.pdf (2022 年 3 月 16 日アクセス)

[94] “Catena-X Automotive Network - Building the First Operating System for a Data Driven Value Chain - “ Gaia-X Mittelstand, https://www.gaia-x-mittelstand.de/Media/1/210906_Oliver_Ganser&Co_Industrie40_CatenaX.pdf (2022 年 3 月 16 日アクセス)

図表 3-13 2022 年の Catena-X ロードマップ

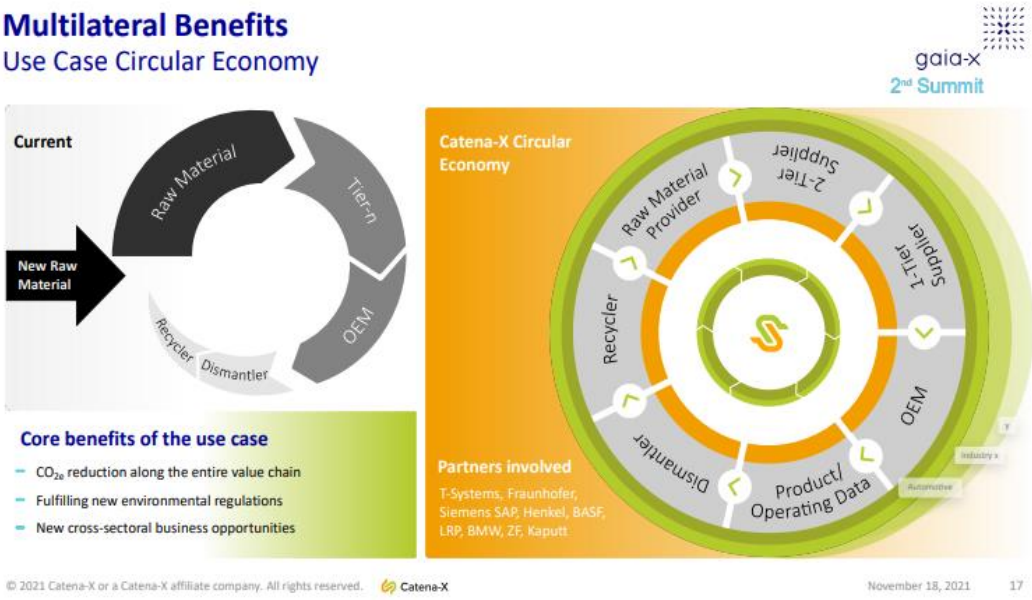


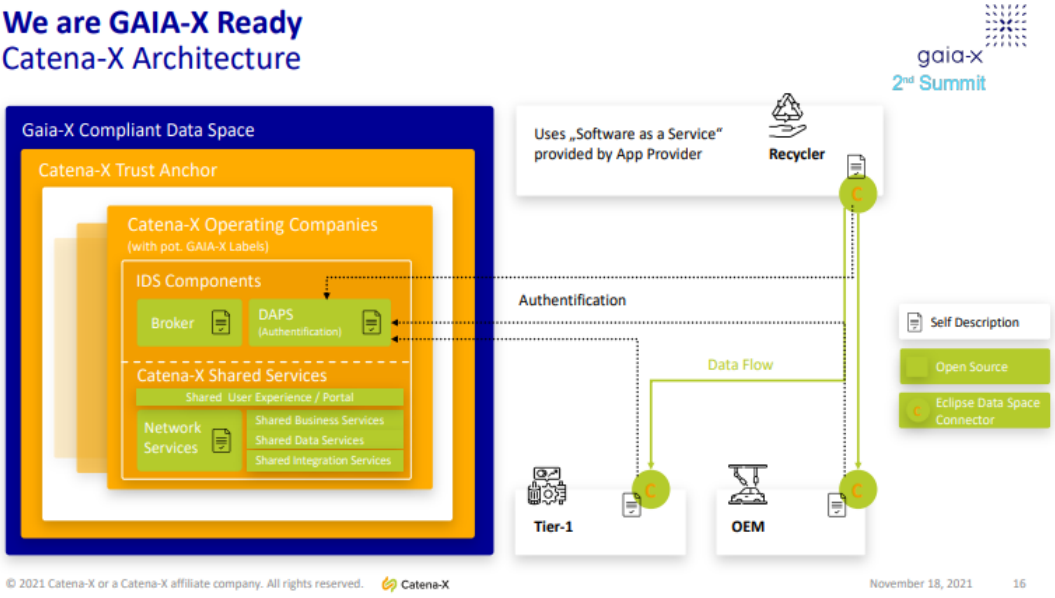
ウ ユースケース

Catena-X は優先 10 分野（ビジネスパートナーデータ管理、トレーサビリティ、ユーティリティサービス、CO2 フットプリント証明、品質管理、循環型経済、MaaS、リアルタイムコントロール、モジュラー生産、デジタルツイン）を設定しており、循環型経済実現に向けた自動車部品リサイクル用サービスが公開されている[95]。同サービスは、セマンティックハブやデジタルツインレジストリ、リレーションサービスを提供し、各自動車部品のライフサイクル情報をユーザが獲得することを可能にする。

[95] “Catena-X Automotive Network- Building the First Operating System for a Data Driven Value Chain-“ Catena-X, https://catena-x.net/fileadmin/user_upload/intro_praesenationen/catena-x_overview_eng_v2.2.pdf (2022 年 3 月 16 日アクセス)

図 3-14 Catena-X 循環型経済ユースケースの概念



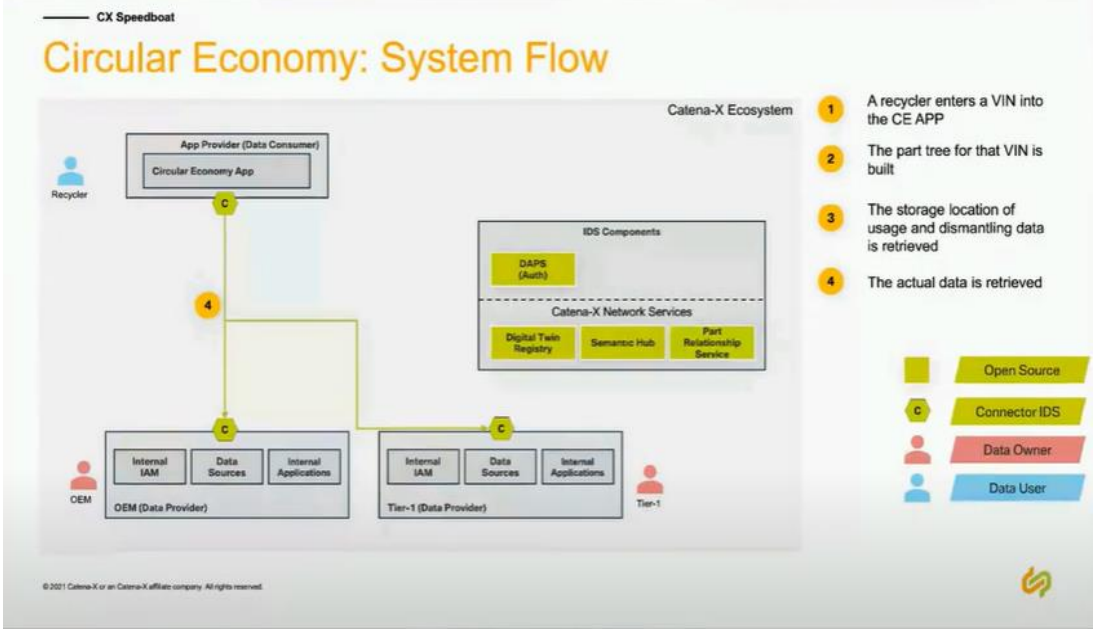


ドイツではリサイクル業者がバリューチェーン上の他の企業とコネクションを持たず、情報が共有されていないため、自動車部品のリサイクル率が 5－7%に留まっている。これは、規制や基準がなく、OEM や Tier 1、Tier2 がそれぞれ独自のデータモデル、パーツの説明方法を用いていること、リサイクル業者の多くを占める SME のデジタル化が進んでいないことが大きな要因とされている。

これに対し、Catena-X が安全な情報共有、透明性を担保することで、バリューチェーン参加者をつなぎ、最適化された自動車部品のリサイクルを可能にする[96]。

[96] “Gaia-X Status-Data Space Manufacturing,” https://www.afnet.fr/Content/2021-12-ABI/15-Hubert-Tardieu-4.pdf （2022 年 3 月 16 日アクセス）

図表 3-15 Catena-X　データ共有イメージ



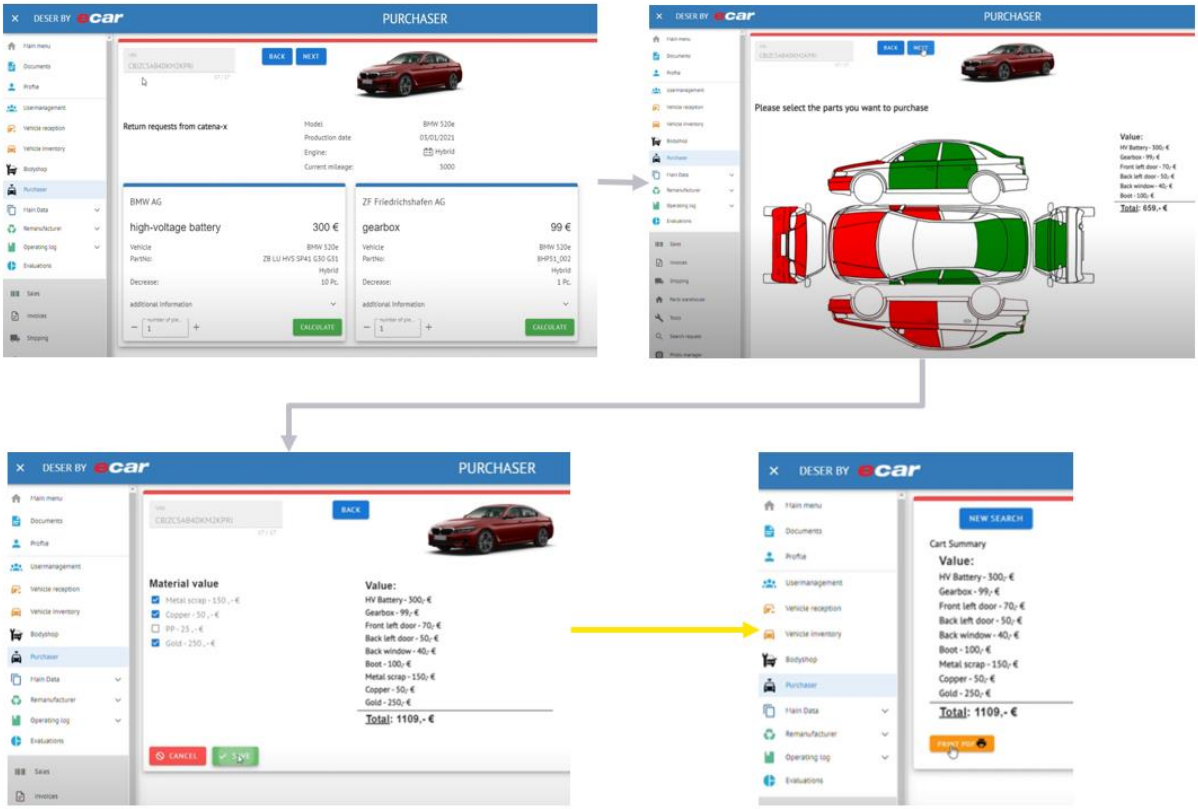
Catena-X の循環型経済を目指すユースケースのデータ共有フローイメージは、①リサイクル業者が VIN（各車両に割り当てられたナンバー）を循環型経済アプリケーションに入力すると、アプリケーションが車両情報（分解や使用状況）を提供②リレーションサービスが各 VIN に対しパーツツリーを作り出し、ユーザが車両構成（パーツ構成）、各パーツの使用状況について知ることを可能にする③デジタルツインレジストリから、特定データの保管場所を獲得④ユーザに情報が提供されるという流れが想定されている[97]。

（ア）ユースケースの具体例 Kaputt 社提供の車両売却者向けサービス）

Catena-X メンバーである Kaputt 社は、車両リサイクルのため VIN ナンバーに部品情報を紐づけ管理・視覚化するウェブサービスを提供している。本項では車両を売却したい所有者向け情報共有サービスを紹介する[98]。

[97] “Unboxing the Automotive Supply Chain Data Space Catena-X,” https://www.youtube.com/watch?app=desktop&v=bIkpyiaC4vI（2022 年 3 月 16 日アクセス）
[98] “MVP dismatler program on Catena-X” YouTube, https://www.youtube.com/watch?v=MmFOF30KYa4（2022 年 3 月 16 日アクセス）

図表 3-16 車両を売却したい所有者向けサービス



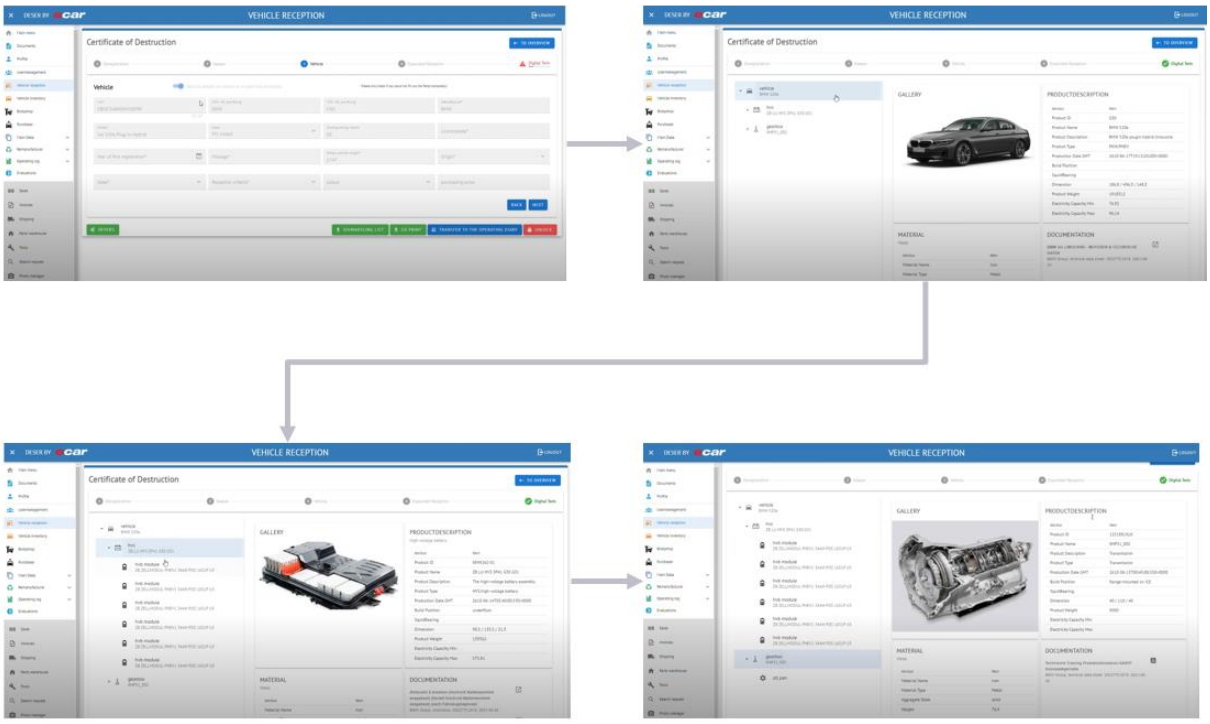
図表 3-16 の左上の画像は、ユーザが VIN をアプリケーションに入力すると、Catena－X から車両情報が提供される画面を示している。右上の画面は、壊れたパーツ、売却できないパーツをクリック（赤く表示）、売却したいパーツをクリック（緑で表示）する画面である。その後、左下の画面で売却する原材料（金属、銅、金等）を選択すると、最後に右下の画面で残価、実際の販売価格の計算結果が表示される。このように、売却希望者が車両構成を把握し、売却可能な部品、マテリアルの価格を査定することを可能にすることで、部品の循環を促進する。

（イ）ユースケースの具体例 Kaputt 社提供の車両解体業者向けサービス）

さらに、Kaputt 社は、Catena-X を用いて、車両リサイクルのため VIN ナンバーに部品情報を紐づけ管理・視覚化するウェブサービスを提供している[99]。本項では車両所有者が部品を売却する際に使用するサービスを紹介する。

[99] “MVP dismatler program on Catena-X” YouTube, https://www.youtube.com/watch?v=MmFOF30KYa4 (2022 年 3 月 16 日アクセス)

図表 3-17　車両解体業者向け部品情報共有サービス



図表 3-17 の左上の画像は、車両解体業者が VIN をアプリケーションに入力する画面であり、右上の画像は Catena－X から車両情報が提供され、デジタルツインが作成される画面である。ここでは、車両の詳細、マテリアル、ドキュメンテーション、車両が寿命を終えるまでの背景情報が表示される。

この画面から車両のパーツ、バッテリーモジュール、ギアボックスの項目をクリックすると、左下及び右下の画像のように、各構成部品の製品紹介、素材の詳細が表示される。このように、車両解体業者が各車両を構成する部品情報を詳細に把握することで、再利用可能な部品の廃棄を防ぎ、資源の有効活用を可能にする。

(2) Structura-X

Structura-X は 2021 年 11 月に開催された第 2 回 Gaia-X サミットで登場した、既存のクラウドサービスとインフラストラクチャプロバイダ（CSP)のデータ及びインフラサービスを、Gaia-X 認証可能にするためのプロジェクトである。

Structura-X は既存のイニシアティブ（Catena-X、AgriGaia、 EuroDat 等)を補完するものであり、初期認証サービスは 2022 年半ばに公開可能となる見込みとなっている。28 団体が参加しており、メンバーはインフラストラクチャサービスを審議するとともに、クラウドフェデレーションサービスを実行可能にするためオープンソース技術を利用することに合意している。

Structura-X は、クラウドにおける新たなクロスセクター及び国を越えた協力のために必要なスケールを有効化し、欧州クラウド市場の分断を解消する支援を行うとともに、Gaia-X や他のライトハウスプロジェクトと密に連携し、データ主権のための技術フレー

ムワークを定義する[100]。2022 年 1 月にキックオフし、3 月から 4 月にかけて Gaia-X 準拠を開始、4 月にはα版の発表を予定している[101]。

(3) Smart Connected Supplier Network (SCSN)

SCSN はハイテク製造サプライチェーンにいる製造企業とその IT サプライヤー向けに、受発注等におけるデータ共有を効率化・低コスト化させる、Gaia-X に沿ったオープンデータエコシステムである。

ア 組織概要・現状

SCSN は主に製品を複数の団体が共同で作るような、多品種少量、複雑性の高いセクターにフォーカスしており、サプライチェーン内のシームレスなデータ交換を提供することで、工場を越えたコミュニケーションの促進とサプライチェーンの透明性、相互運用性を確保し、事務負荷の軽減、サプライチェーンパートナーとのコラボを推進する[102]。

SCSN 財団は提携するサービスプロバイダと企業から決まった金額を受け取ることで運営されている。企業は契約するサービスプロバイダに支払いを行い、サービスプロバイダが財団に支払いを行う形式をとっている[103]。

SCSN はスタートアップ段階にあり、SCSN 利用企業は約 200 社程度である。SCSN と契約したサービスプロバイダ―は 8 社存在し、うち一つは富士通 Glovia である[104]。サービスプロバイダによって提供されるサービス、コストが異なるため、企業は自身のニーズに合わせてプロバイダを選択するよう求められている[105]。

SCSN は IDSA のメンバーであり、Gaia-X にも積極的に参加する等、欧州でのデータ共有イニシアティブ間の協力を進めている[106]。2022 年 2 月から 3 月にかけてサプ

---

[100] “Structura-X - Lighthouse project for European cloud infrastructure is launched. Concrete implementation and alignment with the Gaia-X Roadmap of compatible services,” Gaia-X.eu ウェブサイト, https://gaia-x.eu/news/structura-x-lighthouse-project-european-cloud-infrastructure-launched-concrete-implementation, 2022 年 2 月 21 日リリース

[101] “PLÉNIÈRE #4” Cigref, https://www.cigref.fr/wp/wp-content/uploads/2022/03/Master-pleniere-4.pdf (2022 年 3 月 23 日アクセス)

[102] “Introduction” Smart Connected Supplier Network, https://smart-connected-supplier-network.gitbook.io/processmanual/ (2022 年 3 月 23 日アクセス)

[103] Marktonderzoek SCSN Service Providers, smart industry, 2022 (https://smartindustry.nl/projecten/marktverkenning-naar-scsn-providers-van-geautomatiseerd-berichtenverkeer, 2022 年 3 月 24 日アクセス), p5

[104] 富士通 TDS はドイツに拠点があり、Seeburger Business Integration Suite プラットフォーム技術に基づくコミュニケーションプラットフォームを含むサービスを世界中の顧客に提供している。最近 SCSN に参加したことから、現在はテスト段階にある。Marktonderzoek SCSN Service Providers, smart industry, 2022 (https://smartindustry.nl/projecten/marktverkenning-naar-scsn-providers-van-geautomatiseerd-berichtenverkeer, 2022 年 3 月 24 日アクセス), p11

[105] Marktonderzoek SCSN Service Providers, smart industry, 2022 (https://smartindustry.nl/projecten/marktverkenning-naar-scsn-providers-van-geautomatiseerd-berichtenverkeer, 2022 年 3 月 24 日アクセス), 4.

[106] Marktonderzoek SCSN Service Providers, smart industry, 2022 (https://smartindustry.nl/projecten/marktverkenning-naar-scsn-providers-van-geautomatiseerd-berichtenverkeer, 2022 年 3 月 24 日アクセス), p3

ライチェーンサービスの開発を行い、4 月末にはα版を発表、5 月に Gaia-X 準拠を開始、Self-description についても準拠する予定である[107]。

イ SCSN の機能・技術ストラクチャ

ハイテク製造サプライチェーンでは、OEM、Tier1、Tier2、Tier3、卸売業者、製鉄業者等、様々なアクター間で発注、インボイス等様々な情報共有が必要となる[108]。

従来、2 つの企業でデータを交換する場合、EDI リンクを都度設定する必要があった。この場合、ある企業がデータを新しいパートナーと交換したいとき、新たな EDI コネクションを設定しなければならず、図表 3-18 のように複数のアクターが存在する場合、各企業間でのリンク開設・管理に時間とコストを要していた（2 コーナーモデル）。

企業は SCSN ネットワークに接続したサービスプロバイダと契約することで、SCSN に接続した複数のサービスプロバイダと契約する全ての企業とデータを交換することが可能になる（4 コーナーモデル）[109]。効率化の結果、全体的な生産性の向上（20%）が可能になると見込まれている。

伝統的な中央集権的なプラットフォームイニシアティブと異なり、SCSN にデータを制御する中央機関は存在せず、デジタルとデータ主権に完全に依拠している[110]。

---

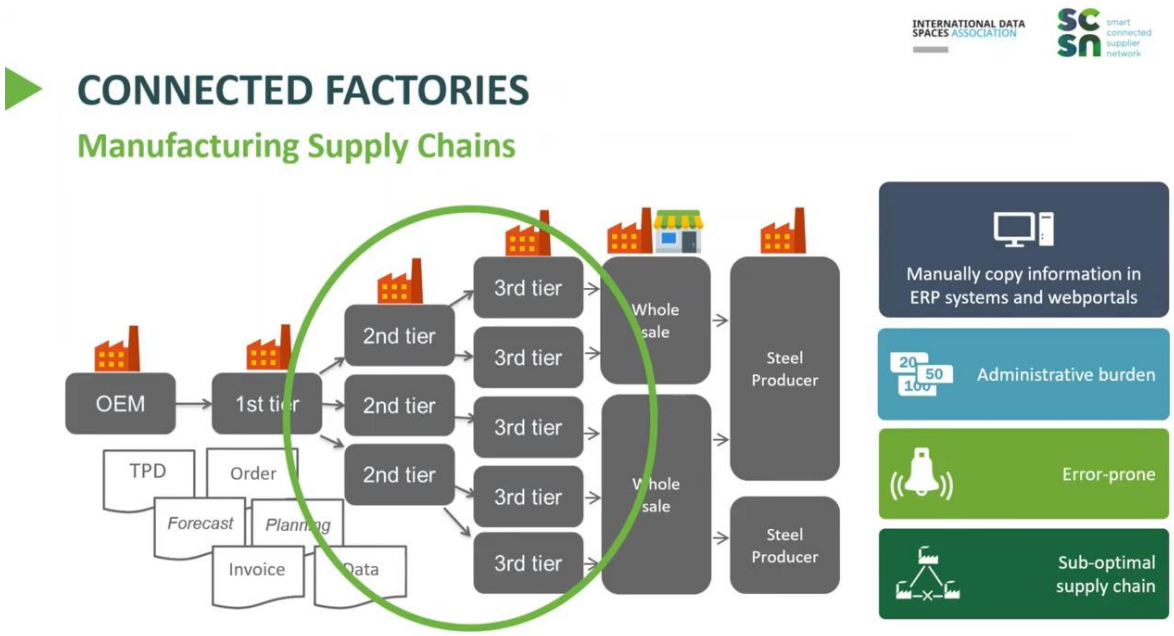
[107] “PLÉNIèRE #4” Cigref, https://www.cigref.fr/wp/wp-content/uploads/2022/03/Master-pleniere-4.pdf (2022 年 3 月 23 日アクセス)

[108] “TNO: The Smart Connected Supplier Network” YouTube, https://www.youtube.com/watch?v=IPxzJpQYpMg (2022 年 3 月 24 日アクセス)

[109] 接続可能な SCSN ユーザは、SCSN Address Book で確認可能である。SCSN ネットワークに加入を希望する製造業者は、まずどのようなユースケースを想定しているか（最重要顧客やサプライヤーはだれか、どのようなデータを共有するか）を検討し、SCSN 提携サービスプロバイダの中でどの企業と契約するかを選定する。サービスプロバイダと契約しコネクションが設定されると、SCSN 内の全ての企業と接続が可能となる。 “Hoe het werkt” Smart Connected Supplier Network, https://smart-connected.nl/en/about-scsn/how-it-works (2022 年 3 月 16 日アクセス); “Hoe sluit je als maakbedrijf aan op SCSN” Smart Connected Supplier Network, https://smart-connected.nl/nl/deelnemen-aan-scsn/voor-maakbedrijven (2022 年 3 月 24 日アクセス)

[110] “Data Space Radar” International Data Spaces Association, https://internationaldataspaces.org/adopt/data-space-radar/ (2022 年 3 月 16 日アクセス)

図表 3-18 製造業のサプライチェーン



図表 3-19　SCSN を通してやり取りされるメッセージの種類

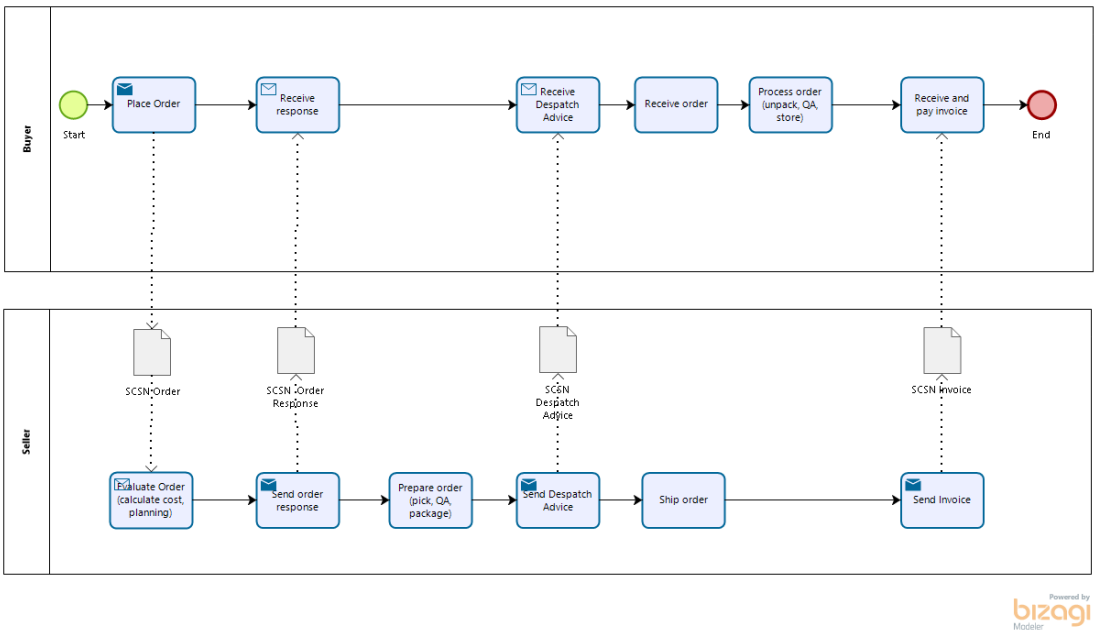
メッセージ種類	概要
発注メッセージ	• 発注：団体に発注を送る • 発注返答：発注を受領又は拒否する • 発注状況：バイヤーに発注情報の変更について通知する
発送通知書	• バイヤーにロジ情報を通知する
技術製品データ（TDP）	• バイヤーが送る技術情報
部品表（BoM）	• 部品関連の仕様書
予測	• 今後の発注の予測を送信
仮説	• 仮設要求：セラーに発注変更の可能性について尋ねる • 仮説返答：バイヤーに需要変更への対応が可能かを通知する
見積書	• 見積書要求：セラーに見積書作成を依頼する • 見積書返答：バイヤーに見積書を通知する
測定	• 購入品の測定データ又は材料証明書をバイヤーに送る

SCSN の分散モデルの基盤技術は IDS の国際 DIN-SPEC 27070（「産業データ・サービス向けセキュリティゲートウェイの要件及び参照アーキテクチャ」）であり、これによりデータへの制御を失うことなく安全な方法でデータを共有することが可能となる。IDS ベースのイニシアティブと互換可能であるため、SCSN はシームレスに複数のイ

ニシアティブと適合する[111]。

SCSN のメッセージ標準は Universal Business Language of OASIS （UBL）（広く国際的に認められたドメイン言語であり、ISO/IEC 19845:2015 として知られる）に基づいている[112]。参加企業・団体間で情報交換を行うため、SCSN は発注メッセージ、発送通知書、技術製品データ(TDP)、部品表(BoM)、予測、仮説、見積書、測定の 8 種類のメッセージを定義している[113]。

図表 3-20 単純な発注プロセスにおける SCSN の役割



ウ SCSN 利用例

金属加工業の Brans Metaalbewerking 社は、SCSN リンクを設定することにより、これまで全て手動で行われてきた作業を単純化した。

具体的には、デジタルに発注を受け取り、ERP システムがデジタルデータを読み込むようになったことで、顧客からの発注をタイプしなおす必要がなくなった。また、ERP システムが必要な確認を行い、発注確認がデジタルで送られ、顧客がシステム内で直接処理するようになったため、注文確認を送信・確認することが簡単になった。

サプライヤーからの梱包伝票もデジタルで受信するため、受領が簡単になった上、デジタルメッセージを通して認証を実施・顧客に送信することができるようになった。

111 “Hoe het werkt” Smart Connected Supplier Network, https://smart-connected.nl/en/about-scsn/how-it-works (2022 年 3 月 16 日アクセス)
112“Hoe het werkt” Smart Connected Supplier Network, https://smart-connected.nl/en/about-scsn/how-it-works (2022 年 3 月 16 日アクセス).
113 “Introduction” Smart Connected Supplier Network, https://smart-connected-supplier-network.gitbook.io/processmanual/ (2022 年 3 月 24 日アクセス)

さらに、請求書の送受信もデジタルで完結するようになった。

このように、同社は SCSN と接続することで、これまで手動で行われていた雑務がデジタル化され、企業は成長を遂げたと述べている[114]。

(4) Mobility Data Space (MDS)

MDS は車両製造業者からライドシェアリングサービス、公共交通運営者やナビソフトウェア企業、研究機関、バイクシェアリング企業等を含むモビリティセクター全体の将来に焦点を当てたプロジェクトである。acatech が主導し、ドイツ連邦交通デジタルインフラ省（BMVI）が予算を拠出している[115]。

MDS の主要な目標の一つは、Gaia-X に準拠したデータ交換を促進することである。EU の共通価値に基づき公平な形で、革新的かつ環境的に持続可能で、ユーザーフレンドリーなモビリティを可能にすることを目指している。

Mobility Data Space ウェブサイトでは 11 団体によるユースケースが紹介されており、Mobility Data Space を通して共有された様々なデータ（気象データ、道路状況データ、駐車場のデータ等）を用いて最適・安全・持続可能な交通オプションの選択を促進するサービス例を参照することができる[116]。

2022 年後半に MDS は実装される見込みであり[117]、2022 年 1 月には R2（リリース 2 と想定される）、OpCo foundation（オープンコードファウンデーションと想定される）、3 月には R3（リリース 3 と想定される）を予定しており、4 月には技術オペレータへの移行・引き渡しを開始し、5 月に Gaia-X 準拠を開始、Self-description についても準拠する予定である[118]。

---

[114] Marktonderzoek SCSN Service Providers, smart industry, 2022 (https://smartindustry.nl/projecten/marktverkenning-naar-scsn-providers-van-geautomatiseerd-berichtenverkeer, 2022 年 3 月 24 日アクセス), p6

[115] “Sicherer Austausch von Mobilitätsdaten über Mobility Data Space” Public Manager, https://www.public-manager.com/aktuelles/einzelansicht/archive/2021/december/article/sicherer-austausch-von-mobilitaetsdaten-ueber-mobility-data-space.html (2022 年 3 月 28 日アクセス)

[116] “Use Cases” Mobility Data Space, https://mobility-dataspace.eu/use-cases (2022 年 3 月 16 日アクセス)

[117] “Gaia-X, making a stride in navigating digital transformation with its lighthouse projects targeting multiple industries,” Gaia-X.eu ウェブサイト, https://www.gaia-x.eu/news/gaia-x-making-stride-navigating-digital-transformation-its-lighthouse-projects-targeting, 2022 年 1 月 31 日リリース

[118] “PLÉNIÈRE #4” Cigref, https://www.cigref.fr/wp/wp-content/uploads/2022/03/Master-pleniere-4.pdf (2022 年 3 月 23 日アクセス)

第4章 IDS・Gaia-X が実現するデータ連携のコンセプト

4.1 IDS・Gaia-X のコンセプト

4.1.1 IDS のコンセプト

IDS は、IDS の定義や目的、目的を実現するためのハイレベルな要件について、IDS リファレンスアーキテクチャモデルのイントロダクションとして示している[119]。ここでは、同箇所からの引用を中心に、IDS のコンセプトとして紹介する。

IDS とは、既存の標準や技術、データエコシステムで広く受け入れられているガバナンスモデルを活用した仮想データスペースであり、信頼できるビジネスエコシステムにおいて安全かつ標準的なデータ交換とデータ連携を促進するものである。IDS の目的は、データ所有者のデータ主権を保証すると同時に、スマートサービスシナリオを作成し、企業間の革新的なビジネスプロセスを促進するための基礎を提供することである。

上記の目的を達成するため、IDS は図表 4-1 の通り、戦略的要件を定めている。それぞれの戦略的要件は運用モデル（「5.1.1 (3) 運用モデル」）によって幾つかの項目に具体化されている。そして、（運用モデルを含めて）参加者やコンポーネントの役割やセキュリティ要件等を定義する IDS アーキテクチャ（概要レベルは「4.2.1 IDS アーキテクチャの全体像」、詳細レベルは「5.1.1 アーキテクチャの観点」）、及びこれらに準拠した参加者やコンポーネント間のインタラクションにより、IDS のコンセプトは実現されている。

図表 4-1 IDS の戦略的要件

戦略的要件	概要
トラスト	各参加者が信頼されたビジネスエコシステムへのアクセスを許可される前に評価や認定が行われることが求められる。
セキュリティ	IDS の全てのコンポーネントには、最先端のセキュリティ対策に準拠していることが求められる。 このため、IDS はアーキテクチャの仕様とは別にセキュリティに関する要件を定めており、主に IDS で使用される各コンポーネントの評価と認証により担保される。
データ主権	データ主権の確保のため、データ所有者（(以下、データオーナー）は、データ利用者（以下、データコンシューマ）へのデータ転送を行う際に、当該データにユーセージコントロールに関する情報（以下、ユーセージポリシー）を付加する。 データコンシューマに対してデータオーナーのユーセージポリシーを受け入れることが強制される仕組みを実現することにより、データオーナーのデータ主権が担保されることが求められる。
データエコシステム	IDS アーキテクチャは、データストレージの分散化を追求しており、信頼できる第三者に転送されるまでデータは物理的にそれぞれのデータオーナーの元に留まることが求められ

[119] *REFERENCE ARCHITECTURE MODEL 3.0*, INTERNATIONAL DATA SPACES ASSOCIATION, December 2020, p9-p10, https://internationaldataspaces.org/wp-content/uploads/IDS-Reference-Architecture-Model-3.0-2019.pdf, 16 March 2022（2022 年 3 月 17 日アクセス）

戦略的要件	概要
	る。
標準化された相互運用性	アーキテクチャの中心的なコンポーネントである IDS コネクタは、IDS のエコシステム内の他のコネクタ（又は他のコンポーネント）と通信することが可能であることが求められる。
付加価値を提供するアプリケーション	IDS の参加者に対してアプリケーションを提供することが求められる。 IDS 参加者はアプリケーションをコネクタ内部に実装することで、ユーザエンドでのデータ処理、データフォーマットの整合、データ交換プロトコルのサービス、データ分析等のアルゴリズムの実行が可能となる。
データマーケット	IDS 参加者による革新的でデータドリブンのサービスの創出を促進することが求められる。 この実現のため、IDS はクリアリングメカニズムや請求機能を提供し、ドメイン固有のメタデータブローカーソリューションやマーケットプレイスを構築している。 さらに、IDS では、参加者がユーセージポリシーの指定や法的な情報を要求する際に使用するテンプレート、その他の方法論的なサポートを提供している。

4.1.2 Gaia-X のコンセプト

Gaia-X のコンセプトについて「Project Gaia-X Executive Summary」[120]を引用して説明する。欧州のためのデータインフラ構想である Gaia-X の目的は、①データ連携基盤に係るインフラ構築に向けた技術的・経済的な取組を始動すること、②行政、医療、企業、科学分野におけるサービス提供者側と利用者側に対する共通のエコシステムを創造すること、③前述の目的を達成するためのフレームワークを確立することである。

Gaia-X は欧州諸国と協力し、欧州、国、企業、個人のための次世代のデータ連携基盤を構築することを目標としている。このようなデータインフラを実現するにあたって、7 つの原則を定めている。

① データ保護

② 開放性・透明性

③ 認証とトラスト

④ デジタルデータの自己主権性・自己決定性

⑤ 市場への自由な参入・EU の価値創出

⑥ モジュール性と相互運用性

⑦ ユーザーフレンドリー

Gaia-X は、データへのアクセス、保存、交換、使用に関してポリシー・ルールを適用可能なコンポーネントとサービスから構成される技術基盤を定義する。また、デジタルエコ

[120] Project Gaia-X Executive Summary, Gaia-X AISBL, October 2019, https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/das-projekt-Gaia-X-executive-summary.pdf?__blob=publicationFile&v=8（2022 年 3 月 17 日アクセス）

システムは、デジタル製品やサービスの開発者、提供者、利用者のネットワークにおいて、透明性を通じて連携しているものと解釈している。このようなシステムは、欧州の成長、デジタル・イノベーション、新しいビジネスモデルのための重要な基盤として機能する。

Gaia-X は、欧州で多額の投資がされているデジタル技術を連携させ、より大きな効果を発揮させたいと考えている。そのため、特にクラウド基盤やエッジコンピューティング基盤等のクラウドサービスを連携させ、シームレスなシステムとして提供できるようにすることを目標としている。Gaia-X のデータ連携基盤のアーキテクチャに関するコンセプトは、下記のような技術要件に基づいている。

① データ主権

② OSS 等を活用した透明性・安全性の高い技術

③ マルチエッジ、マルチクラウド、エッジ To クラウドによる分散データ処理

④ 技術標準、ネットワーク、データ、相互接続性における相互運用性

⑤ Gaia-X エコシステム参加者の認証と契約

⑥ 認証等の中心的なサービスの提供

⑦ 自己記述による透明性の促進と新しいビジネス・アプリケーションモデルの創出

Gaia-X と共通する目的を持つ国や欧州の団体と連携し、欧州のデータインフラに係る課題の解決を図る。その上で、既存の技術と Gaia-X 主導によるコンポーネントの開発によって、欧州から世界市場へ競争力のあるサービスを展開したいと考えている。サービス提供者側の透明性の向上、データ流通の促進、相互運用性の向上によって、大手企業から中小企業、ベンチャー企業等、あらゆる規模の企業を結びつけることを実現したいと考えている。データ連携基盤を構築するためは、欧州としての中央組織が必要であり、Gaia-X は、上記のような技術要件に基づくリファレンスアーキテクチャ及びアーキテクチャ標準を定義し、欧州におけるビジネス、科学、国家、社会においてデータ革新を進めることを目指している。

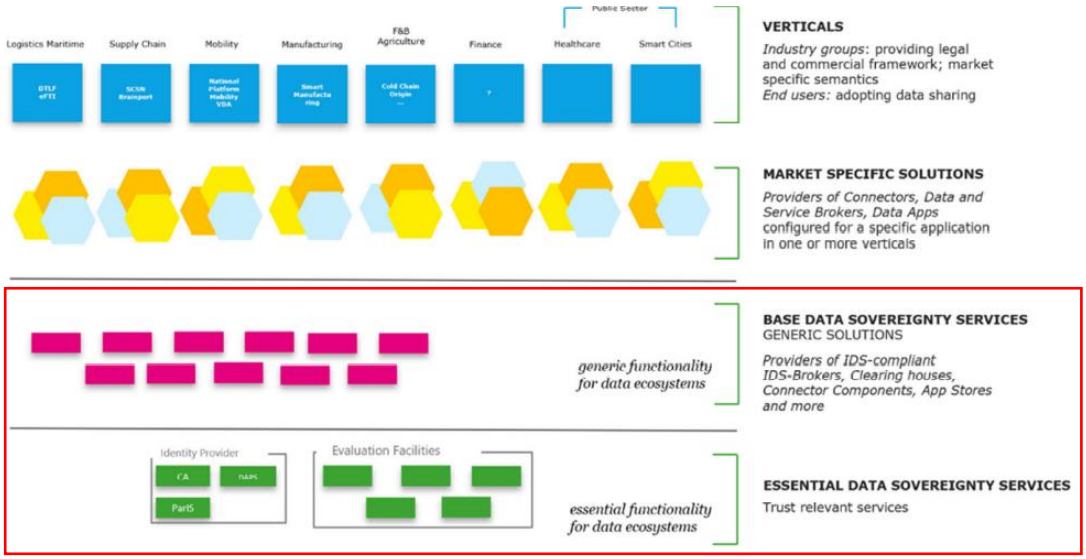
上記のような原則及び技術的要件を満たす Gaia-X のアーキテクチャについて、「5.1.2 Gaia-X のアーキテクチャ」で説明する。具体的には、Gaia-X のアーキテクチャの前提事項となる要素について「5.1.2 (1) 前提事項」で、Gaia-X のアーキテクチャを構成するフェデレーションサービスのコア機能について「5.1.2 (2) コンポーネント」で、そのようなコンポーネントを用いてどのように運用していくかについて「5.1.2 (3) 運用モデル」で詳述する。さらに、「5.2.2 Gaia-X におけるプロセス」にて Gaia-X の利用者がどのようにコア機能を利用してデータ交換等を行うのかプロセスレベルで解説する。また、Gaia-X と IDS では認証とトラストという観点で異なるコンセプト及び技術を採用しているため、「5.3.2 Gaia-X」にて Gaia-X における認証・認可を詳述する。最後に、フェデレーションサービスを構成するコンポーネントのより具体的な仕様について、「6.2 Gaia-X コンポーネント」で説明する。

4.2 IDS・Gaia-X のアーキテクチャの全体像

4.2.1 IDS アーキテクチャの全体像

「4.1.1 IDS のコンセプト」の通り、IDS は自身が掲げるコンセプトの実現のため、ビジネスモデルや製品、サービスの基盤となるデータスペースを構築するために使用できるアーキテクチャやフレームワーク等を定義しており、その全体像は 図表 4-2[121]のように示されている。

図表 4-2 IDSA ルールブックのスコープとゴール



Gaia-X との関連においては、データ主権の実現にあたり実質的な機能を担う BASE DATASOVEREIGNTY SERVICE 及び ESSENTIAL DATA SOVERREIGNTY SERVICES を中心として、産業やマーケットごとのデータの相互運用性やポータビリティの実現を目指しているという点で共通項があることが伺える。

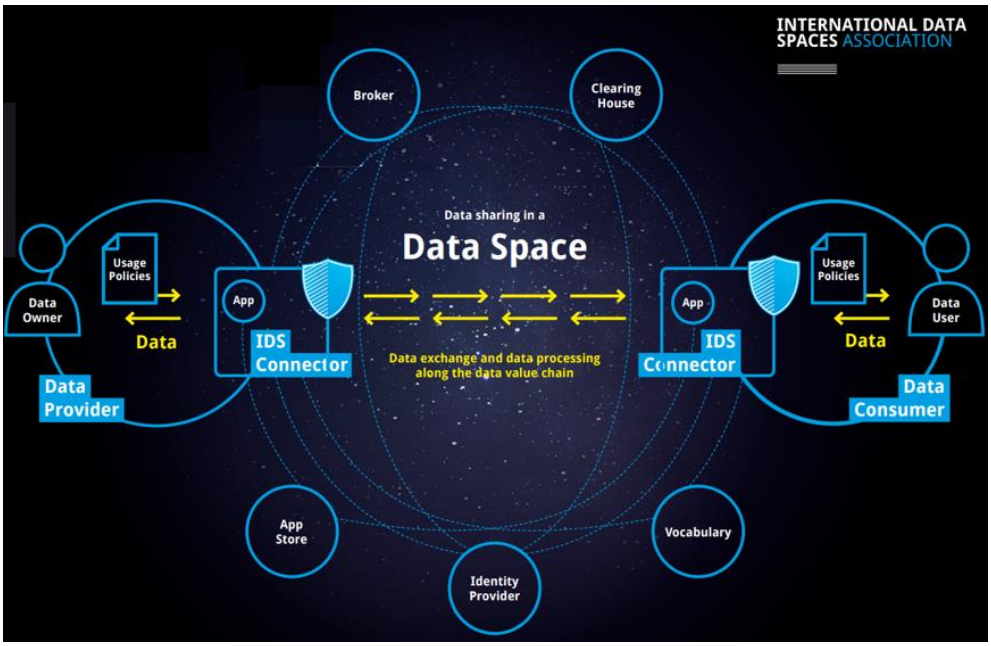
IDS は、これらの実質的な機能部分におけるアーキテクチャの全体像について

図表 4-3[122]の通りに紹介しており、IDS の参加者や主なコンポーネントの役割とその間のインタラクションに関する概要が示されている。

121 *IDSA Rule Book 1.0*, INTERNATIONAL DATA SPACES ASSOCIATION, April 2019, p6, https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-White-Paper-IDSA-Rule-Book.pdf（2022 年 3 月 17 日アクセス）

122 *IDS Infographic: Data Sharing in a Data Space*, INTERNATIONAL DATA SPACES ASSOCIATION, March 2021, https://internationaldataspaces.org/wp-content/uploads/IDSA-Infographic-Data-Sharing-in-a-Data-Space.pdf（2022 年 3 月 17 日アクセス）

図表 4-3 IDS インフォグラフィック



IDS は、認証されたデータの提供者と受信者の間で、相互に合意したルールに基づき、信頼性の高いデータ交換を可能にするデータスペースであり[123][124]、それぞれが持つ IDS コネクタを中心としたデータ共有を行う[125]。図表 4-4 に示すように、参加者は IDS コネクタを利用することで産業用データクラウド、個々の企業クラウド、オンプレミスアプリケーション、個々の接続デバイス等を IDS に接続することができる[126]。

[123] IDSA Rule Book 1.0, INTERNATIONAL DATA SPACES ASSOCIATION, April 2019, p6, https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-White-Paper-IDSA-Rule-Book.pdf（2022 年 3 月 17 日アクセス）

[124] IDS リファレンスアーキテクチャモデルには International Data space と industrial dataspace の両方の表現が登場するが、後者であっても前者と同義と考えられる場合には、IDS と省略することとした。それ以外の場合は、産業用データスペースと記載している。

[125] IDSA Rule Book 1.0, INTERNATIONAL DATA SPACES ASSOCIATION, April 2019, p6-8, https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-White-Paper-IDSA-Rule-Book.pdf（2022 年 3 月 17 日アクセス）

[126] *REFERENCE ARCHITECTURE MODEL 3.0*, INTERNATIONAL DATA SPACES ASSOCIATION, December 2020, p18-p19, https://internationaldataspaces.org/wp-content/uploads/IDS-Reference-Architecture-Model-3.0-2019.pdf, 16 March 2022（2022 年 3 月 28 日アクセス）

図表 4-4 異なるクラウドプラットフォームと接続可能な IDS コネクタ

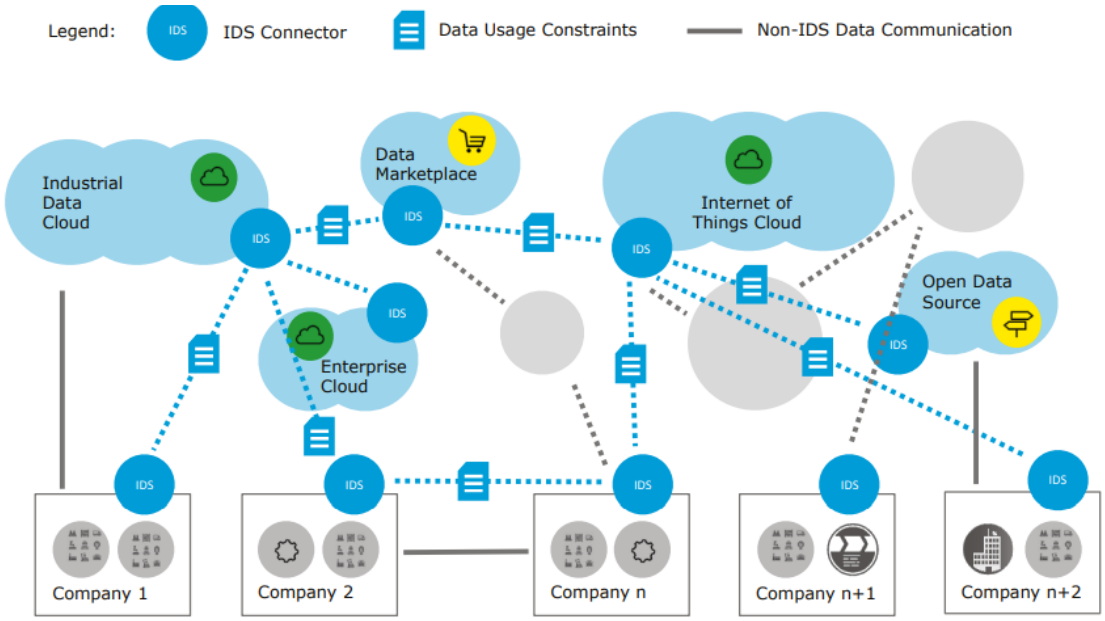


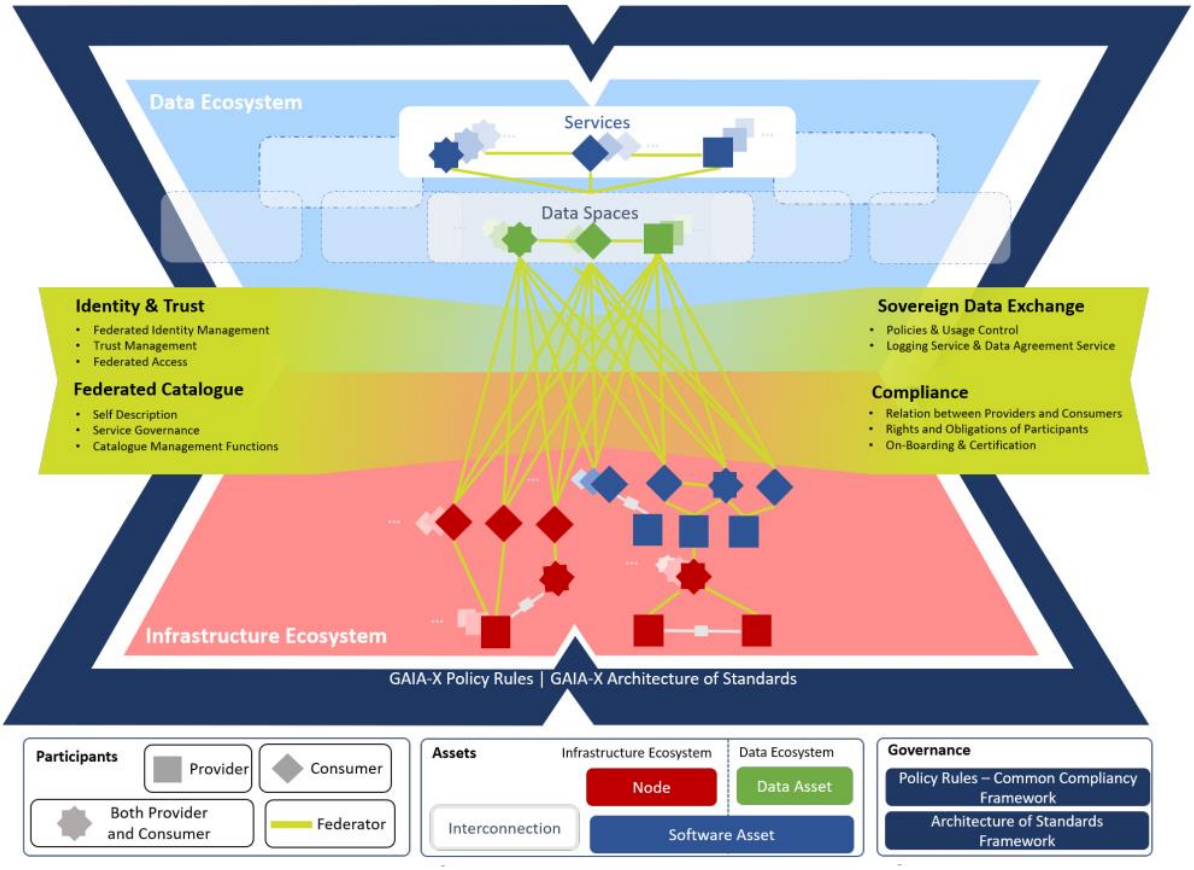
Figure 2.6: International Data Spaces connecting different cloud platforms

なお、IDS はその構築にあたって General Data Protection Regulation（GDPR）や electronic IDentification（eIDAS）、The Revised Payment Services Directive（PSD2）等の EU 規則や勧告を考慮する必要があるとしており[127]、IDS のアーキテクチャ及びエコシステムが個人情報を処理･共有する組織による GDPR の遵守にどの程度まで貢献できるか、またどの側面が IDS の範囲外であるか等についての検討を行っている[128]。

[127] Design Principles for Data Space 1.0, INTERNATIONAL DATA SPACES ASSOCIATION, April 2021, p34.（2022 年 3 月 17 日アクセス）
[128] GDPR Related Requirements and Recommendations for the IDS Reference Architecture Model, INTERNATIONAL DATA SPACES ASSOCIATION, December 2019, p5,（2022 年 3 月 17 日アクセス）

4.2.2 Gaia-X アーキテクチャの全体像

図表 4-5 Gaia-X のアーキテクチャ



Gaia-X は、IDS のイニシアティブほどには成熟していないが、データ主権の理念を広め、データ共有のための信頼のエコシステムを構築するという同じビジョンに従っている[129]。

Gaia-X アーキテクチャは、目的、原則及び概念を具体化するため、IDS の全体像と類似するインフラストラクチャエコシステム、データエコシステム及びフェデレーションサービスの 3 つの層で構成されている。Gaia-X では、特にフェデレーションサービスのアーキテクチャ・標準アーキテクチャを定め、データ連携基盤を構築することを目指している。フェデレーションサービスは 4 つのコア機能（ID とトラスト・フェデレーションカタログ・データ主権サービス・コンプライアンス）で構成され、インフラストラクチャエコシステムとデータエコシステムにおける連携を実現するための実質的な機能を持つ。データエコシステムでは、各産業部門から生成されるデータの相互運用やポータビリティを実現する。インフラストラクチャエコシステムでは、クラウド、高パフォーマンスコンピューティング（HPC） クラウド、エッジコンピューティングの相互運用性を実現する。

[129] Gaia-X and IDS, INTERNATIONAL DATA SPACES ASSOCIATION, January 2021, https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-Position-Paper-Gaia-X-and-IDS.pdf（2022 年 3 月 17 日アクセス）

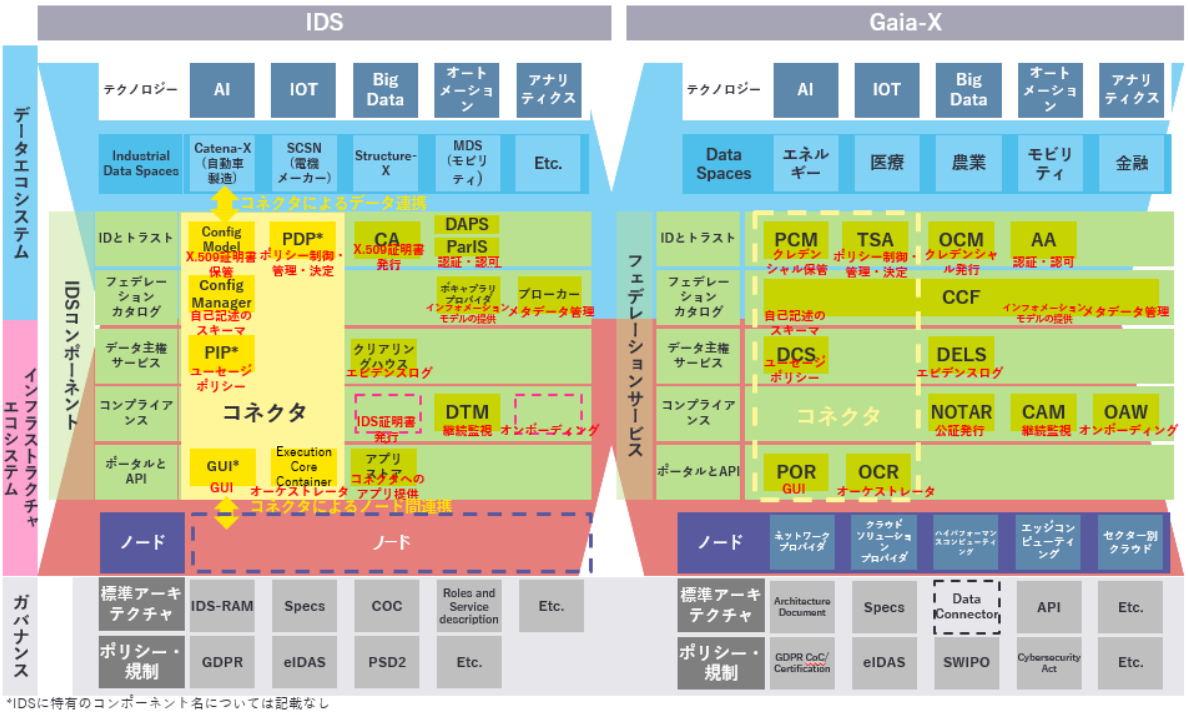
なお、Gaia-X Hub Germany のボードメンバー及び Siemens の Principal Key Expert Digital Industries によると、SAP 等の企業が有している既存のシステムがインフラストラクチャエコシステムに相当するとのことである。信頼性の高いコネクティビティを実現するフェデレーションサービスによってこのような既存システム同士が連携され、新しいサービスが生み出されることが期待されている。本ボードメンバー及びプリンシパルへのインタビュー結果については、「8.3 IDSA・Gaia-X に関するインタビュー結果」を参照されたい。

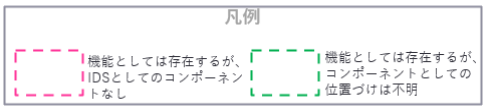
Gaia-X エコシステムは、Gaia-X の標準アーキテクチャに適合する個々のエコシステムの全体で構成される。例えば、Catena-X 等の個別のエコシステムは、Gaia-X のアーキテクチャを使用することで Gaia-X エコシステムの一部としてみなされる。ガバナンスは、エコシステム内の参加者の活動を管理するため、EU の法規制に基づくポリシー・ルールを適用している。さらに、標準アーキテクチャは、フェデレーションサービスのコンポーネントを定義している。

4.3 IDS と Gaia-X の関係

Gaia-X は、フェデレーションサービスの 4 つのコア機能（ID とトラスト・フェデレーションカタログ・データ主権サービス・コンプライアンス）にポータルと API を加えた 5 つの機能を構成する 13 個のコンポーネントを開発している。各コンポーネントはそれぞれ認証・認可やポリシー制御、ログの管理等を行うが、これらは概ね IDS の各コンポーネントの役割とも対応している。この関係性は、図表 4-6 の通りにプロットすることができる。

図表 4-6 IDS における機能と Gaia-X における機能の比較





IDS コンポーネントの中心をなすコネクタは、Gaia-X のアーキテクチャ上においても、データエコシステムとインフラストラクチャエコシステムにおけるデータ及びノード間の連携に用いることができる。

4.4 IDS と FIWARE の関係

FIWARE とは、スマートシティ等のスマートソリューションの開発を加速するためのオープンソースソフトウェアコンポーネントのフレームワークであり、FIWARE Foundation を中心としつつ FIWARE Community メンバー企業が主体的にオープンソースソフトウェアコンポーネントの実装・利用を進めている[130]。

FIWARE では、オープンソースソフトウェアコンポーネントのことを Generic Enablers（以下、GEs）と呼称している。FIWARE はマイクロサービスアーキテクチャ 指向を有しており、そのため GEs は機能ごとにコンポーネントとして分割されている。FIWARE の利用はすべての GEs を利用するか一つも利用しないかの 2 択ではなく、利用者は要件に応じて自由に GEs を組み合わせて利用する。GEs として多くの機能がすでに開発済みである。主要な GEs の機能分類ごとの一覧を図表 4-7 に示す[131]。

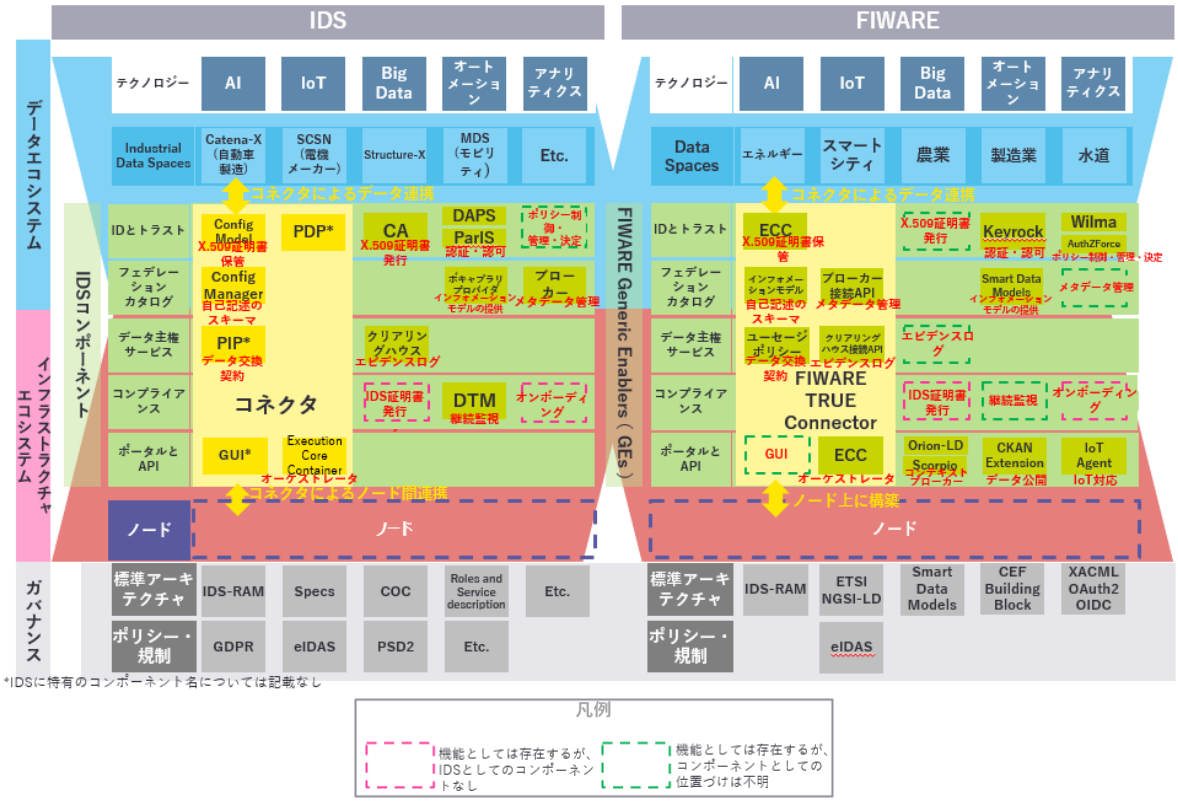
図表 4-7 FIWARE GEs の機能分類ごと一覧（GitHub 掲載情報から EY 作成）

機能分類	GEs
Core Context Management ※コンテキストブローカー	Orion, Cygnus, Draco, STH-Comet, QuantumLeap, Orion-LD Context Broker, Scorpio Broker, Stellio Broker
IoT Agents ※IoT 系のインターフェイス	IoT Agent Node, IoT Agent for JSON, IoT Agent for LWM2M, IoT Agent for Ultralight, IoT Agent for LoRaWAN, IoT Agent for OPC-UA, IoT Agent for Sigfox, OpenMTC
Interface to Robotics ※ロボティクス系のインターフェイス	Fast-RTPS, Micro-XRCE-DDS, FIROS
Security ※認証・認可	Keyrock, Wilma, Authzforce, APInf, Telefónica Steelskin PEP, Telefónica Keystone SCIM, Telefónica sPassword, Telefónica Keypass
Context Data Publication and Monetization ※データ公開	CKAN extensions, Biz Framework, Idra
Processing ※データ分析	Wirecloud, Knowage, Kurento, Cosmos, FogFlow, Perseo

[130] “About FIWARE” FIWARE Foundation, https://www.fiware.org/about-us/ （2022 年 3 月 17 日アクセス）
[131] “GitHub - FIWARE/awesome” GitHub, https://github.com/FIWARE/awesome#fiware-catalogue （2022 年 3 月 17 日アクセス）

FIWARE は CEF Building Block とともに IDS との互換性を有していることが FIWARE Foundation から言明されている通り 、GEs を用いた IDS Connector を含む IDS の機能の実装が可能である。IDS の機能と GEs が実現する機能の対応を図表 4-8 に示す。

図表 4-8 FIWARE GEs が実現する機能と IDS における機能の対応図



FIWARE を用いて IDS の機能を実装する場合には、GEs の一つである FIWARE TRUE Connector[132]の利用が推奨される。FIWARE TRUE Connector は IDS の定義するメタデータブローカーやクリアリングハウスとの接続をサポートしているが、メタデータブローカーやクリアリングハウス自体の実装ではない点に留意が必要である。FIWARE を用いて IDS の機能を実装する場合に FIWARE TRUE Connector の他に活用が想定される GEs は、認証・認可に関する機能を有する Keyrock、Wilma、AuthZForce 等がある。これらの GEs は XACML、OAuth2、OpenID Connect といった主要な認証・認可プロトコルをサポートしており、IDS の機能を実装するのみならず、企業内業務システムとの連携等の実現にも活用できるだろう。

また、FIWARE を用いて IDS の機能の実装する際には、上述した GEs の活用のみならず、GEs と合わせて GEs 以外のオープンソースソフトウェアを同時に活用することを FIWARE Foundation は考えている。具体的には、IDS Connector 間のデータの送受信の制御のみならず、送受信後のデータの流通やデータに対するユーセージポリシーの強制等を実現する手段として、オープンソースソフトウェアのコンテナオーケストレーション基盤

132 “GitHub - Engineering-Research-and-Development/fiware-true-connector” GitHub, https://github.com/Engineering-Research-and-Development/fiware-true-connector/ （2022 年 3 月 17 日アクセス）

である Kubernetes[133]や Kubernetes 内のデータの送受信等を管理するサービスメッシュソフトウェアである Istio[134]の名称を挙げている[135]。

4.5 IDS・Gaia-X の開発状況

4.5.1 IDS の開発状況

IDSA 技術運営委員会の傘下にある IDS-G は、IDSA による仕様とさらなるドキュメントを一般に提供することを目的としている。IDS-G は、IDS ベースのソリューションを開発及びテストするための文書及び仕様の公開に重点を置いており、これには技術文書やインターフェースの記述が含まれる[136]。主なコンポーネントの具体的な開発状況は図表 4-9 の通りである[137]。

図表 4-9 IDS の主なコンポーネントの開発状況

コンポーネント名	開発状況
IDS Connector	開発済（改善中）
Certification Authority	開発中
Dynamic Attribute Provisioning Service	開発済
Participant Information System	レビュー中（会員限定公開）
Broker	開発済
Vocabulary Provider	開発状況非公開
Clearing House	開発中
Dynamic Trust Monitoring	開発状況非公開
IDS Information Model	開発中

なお、IDS コネクタとは、IDSA が開発に関与しているコネクタの総称である。フラウンホーファー研究機構のウェブサイトによると、Eclipse Data Connector（以下、EDC）、Trusted Connector、Open Data Connector の 3 種類のコネクタが存在する。

上記のうち、本報告書の執筆時点において主要コネクタとして採用されているのは、EDC である。EDC は、IDS のデータ主権の概念をデータ交換の面から実現し、IDS と Gaia-X に実装とユースケースのフィードバックを提供することに主眼を置いたコネクタである。

---

133 “Kubernetes” Kubernetes official website, https://kubernetes.io/ja/ （2022 年 3 月 18 日アクセス）
134 “Istio” Istio official website, https://istio.io/ （2022 年 3 月 18 日アクセス）
135 “FIWARE for Data Spaces Version 2.0” FIWARE Foundation, https://docs.google.com/document/d/1AKAsEEYmP9RVqJLtb4HWpDki222NFF4Hmh7OFuS0DrA/ （2022 年 3 月 17 日アクセス）
136 *IDSA Rule Book 1.0*, INTERNATIONAL DATA SPACES ASSOCIATION, April 2019, p20-21, https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-White-Paper-IDSA-Rule-Book.pdf （2022 年 3 月 17 日アクセス）
137 “GitHub - International-Data-Spaces-Association/IDS-G” GitHub, https://github.com/International-Data-Spaces-Association/IDS-G （2022 年 3 月 17 日アクセス）
“GitHub - International-Data-Spaces-Association/idsa” GitHub, https://github.com/International-Data-Spaces-Association/idsa/blob/main/overview_repositories.md （2022 年 3 月 17 日アクセス）

当初、IDSA の GitHub 上では Dataspace Connector の名称で開発されていたが、現在では EDC に引き継がれている。

EDC の初版は 2022 年 5 月末に EDC Official Release v.1 としてリリースされているが、現在においても GitHub 上で更新されており、技術改良が進められている。直近のロードマップによると、2022 年 9 月以降に Gaia-X Federation Service との互換性の観点から要件定義開始が開始される見通しである。

上記の通り、2022 年 3 月 1 日時点で GitHub のドキュメントを元に、dataspace コネクタの開発は Eclipse Foundation に引き継がれた。しかし、2022 年 3 月 25 日現在、github の内容が変更されている。GitHub には、dataspace コネクタの開発は、IDS 運営会社である Sovity 社[138]が担当することが記載されている[139]。

今後の EDC の開発ロードマップについては、図表 4-10 の通りに公表されている。

図表 4-10 EDC の開発ロードマップ

スケジュール	重要なマイルストーン
2022 年 5 月 29 日頃	Gaia-X レジストリ拡張機能 Gaia X 自己記述拡張 IDS リファレンスアーキテクチャモデル 4.0 要件定義 プロトコルネゴシエーション アプリ発行
2022 年 6 月 17 日頃	アプリ統合とルーティング データプロトコルのネゴシエーション インフラ情報の公開 - スコープ設定 制御 API の実装（強化）
夏季休業期間後 6～8 週目	GXFS-DE(alpha)との互換性 - 要件定義 実装を公開するインフラ情報の公表

今後、コネクタの提供形態は SaaS や IaaS といったクラウド展開、オンプレミス及びその他あらゆる方法が今後可能になる模様。また、コネクタの開発や配布にはサービスプロバイダを使う方法があり（「5.1.1 (1) イ (ウ)a サービスプロバイダ」）、例えば Sovity 社がサービスプロバイダの役割を担うことになる。Sovity 社は営利企業であり、コネクタの開発や維持運用を行う。現在、設立の段階で年内にサービス開始を予定している。将来的には、Sovity 社と同様のサービスを提供する企業が現れることが想定される。上記のような会社は、IDSA への参加手続を行うことで、正式にサービスプロバイダとして認定されることとなる（「5.3.1 (1) イ (ア)d 参加者別の特記事項」）。今後、利用者は Eclipse Data Space Connector 又は Sovity 社のようなサービスプロバイダが開発するコネクタを選んで採用することが可能である[140]。

今後、利用者は Eclipse Data Space Connector もしくは Sovity 社のようなサービスプロバイダが開発するコネクタを選んで採用することが可能である。Eclipse Data Connector のメリットは、自由な開発が可能で、Gaia-X 及び IDS 両方の機能を持ち合わ

[138] “Sovity” Sovity official website, https://sovity.de/（2022 年 3 月 29 日アクセス）
[139] “GitHub - International-Data-Spaces-Association/DataspaceConnector”, https://github.com/International-Data-Spaces-Association/DataspaceConnector （2022 年 3 月 28 日アクセス）
[140] フランホーファ研究機構よりヒアリング

せる。ただし、Eclipse のルールに従う必要がある。例えば、pull request しても Eclipse に却下される場合がある。一方、Sovity 社が開発するコネクタはオープンソースではない模様。Sovity 社は kubernetes でコネクタの開発をコンテナ化し、導入するために低コストで実現可能にすると推察している[141]。

4.5.2 Gaia-X の開発状況

Gaia-X AISBL は、欧州の法規制に基づく Gaia-X としてのポリシー・ルールを制定し、それらに基づく技術的要件から Gaia-X のアーキテクチャを設計している。Gaia-X のアーキテクチャをより具体的なアプリケーション要件として落とし込むため、ビルディングブロック単位の仕様書が作成されている。2022 年 3 月時点ではフェデレーションサービスの要件及び仕様が本仕様書に書かれており、一部のコンポーネントについては開発フェーズに入っていることを確認している[142]。

Gaia-X のコンポーネントは、ID とトラスト（WP1）、フェデレーションカタログ（WP2）、データ主権サービス（WP3）、コンプライアンス（WP4）、ポータルと API（WP5）の 5 つのワーク・パッケージに分かれて開発されている。各コンポーネントは開発の優先度が割り振られており、ID トラストの Authentication・Authorization、Personal Credential Manager、Organization Credential Manager、Trust Services API、フェデレーションカタログの Core Catalogue Functions、データ主権サービスの Data Contract Service、コンプライアンスの Continuous Automated Monitoring、Notarization API が優先度 1 に指定されている。具体的な開発状況は図表 4-11 の通りである[143]。

図表 4-11 Gaia-X Federation Service の主なコンポーネントの開発状況

コンポーネント名	開発状況
Authentication and Authorization	開発状況非公開
Personal Credential Manager	alpha 版開発済(本稼働未定)
Organization Credential Manager	beta 版開発中(本稼働未定)
Trust Services API	開発状況非公開
Core Catalogue Functions	一部について alpha 版開発済 （本稼働未定）
Data Contract Service	開発状況非公開
Data Exchange Logging Service	開発状況非公開
Onboarding & Accreditation Workflows	開発状況非公開
Notarization API	alpha 版開発済（本稼働未定）
Continuous Automated Monitoring	alpha 版開発済（本稼働未定）
Onboarding & Accreditation Workflows	alpha 版開発済（本稼働未定）
Orchestration	開発状況非公開
Portal	開発状況非公開

141 フランホーファ研究機構よりヒアリング

142 Gaia-X 2nd Summit, Gaia-X AISBL, November 2021, https://Gaia-X.eu/sites/default/files/2021-12/ALL%20Day1_Gaia-X%20Summit21.pdf（2022 年 3 月 17 日アクセス）

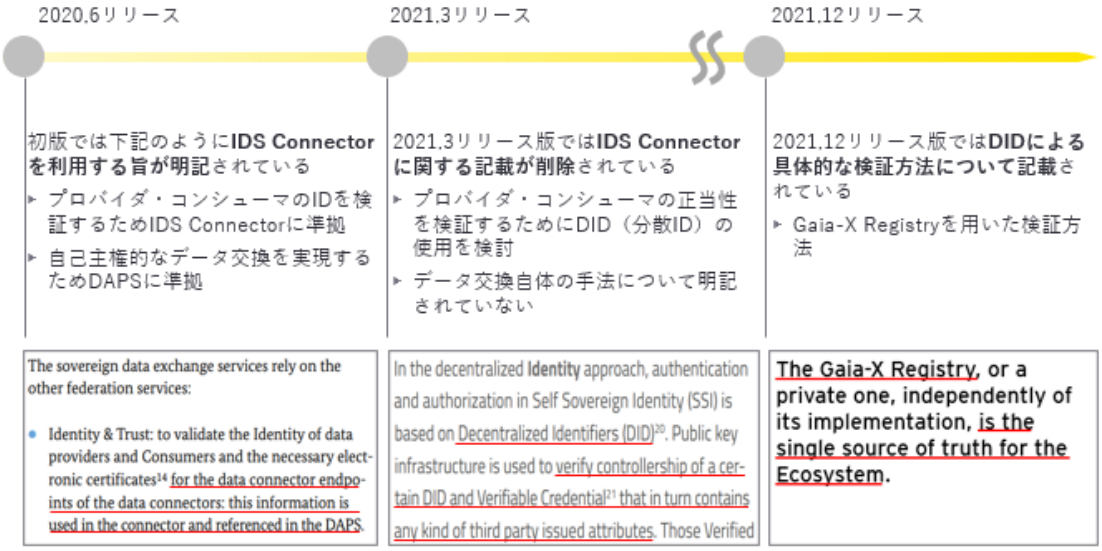
143 Status of Gaia-X & highlights, Gaia-X AISBL, February 2022,https://gaia-x.eu/sites/default/files/2022-02/Gaia-X_standard-presentation_1422022_V10.pdf（2022 年 3 月 25 日アクセス）

4.5.3 IDS コネクタの Gaia-X への実装予定等

IDSA は Gaia-X Association の創立メンバーであり、IDS のビジョンと IDS リファレンスアーキテクチャモデルは、Gaia-X の全体的なビジョンと具体的な Gaia-X アーキテクチャに必要とされる様々な概念・ソリューションを提供していることは第 2 章で述べた通りである。しかし、IDS の中心的なコンポーネントである IDS コネクタを Gaia-X に実装するかについては Gaia-X 内部で議論が進められている状況にある。

議論が複雑化している状況は、Gaia-X の技術アーキテクチャを示すドキュメントにおける IDS コネクタに関する記述内容の変遷から伺うことができる（図表 4-12 を参照されたい）。Gaia-X AISBL は、2020 年 6 月から 2021 年 3 月にかけて Gaia-X: Technical Architecture の初版及び第二版をリリースしているが、初版では ID 検証のために IDS コネクタに準拠する旨が示されていたのに対して、第二版では IDS コネクタへの言及箇所は削除されている。2021 年 12 月に発行された第三版においても、IDS コネクタの記載はない。

図表 4-12 Gaia-X Architecture Document における IDS コネクタの記載状況



この点について、Gaia-X 側と IDS 側の双方のエキスパートに対してインタビューを実施した結果、両者によってスタンスの差異がある一方で、一定の共通見解があることを確認することができた。このうち、実装予定を展望する上で有益な情報は、下記 3 点である。

第 1 に、「3.2.3 主要関連団体・ドキュメント」にて紹介した Gaia-X 関連イニシアティブの 1 つである Catena-X については IDS コネクタを利用する予定である。

第 2 に、IDS コネクタの一つである Eclipse Dataspace Connector では、現在少なくとも 1 つの Gaia-X 準拠のコネクタが開発されている。公式 HP には、「Eclipse Dataspace Connector は、IDS 及び Gaia-X に関連するプロトコルや要件を実装し、それによってこれらのイニシアティブに実装とフィードバックを提供する。しかし、このコネクタは

拡張可能であり、別のプロトコルをサポートすることができる。」との記載がある。

第 3 に、Gaia-X が IDS コネクタを採用するかは Gaia-X が用いるデータ連携基盤次第であるとする意見が上がった一方で、現状において IDS コネクタは安全で信頼できるデータ交換のための中心的な技術要素であることから、IDS コネクタを保有していないデータ連携基盤と繋がる可能性は低いという認識を持つ Gaia-X Hub のメンバーも存在した。

以上を踏まえると、IDS コネクタの Gaia-X への実装については Gaia-X フェデレーションサービスの実装次第である反面、Catena-X のように実際のユースケースで IDS コネクタが採用されていく過程において、IDS コネクタの更なる改善や Gaia-X への互換性の向上に向けた取組が引き続き行われていくものと思われる。

第5章 IDS・Gaia-X のテクニカルアーキテクチャ（概要）

5.1 アーキテクチャの観点

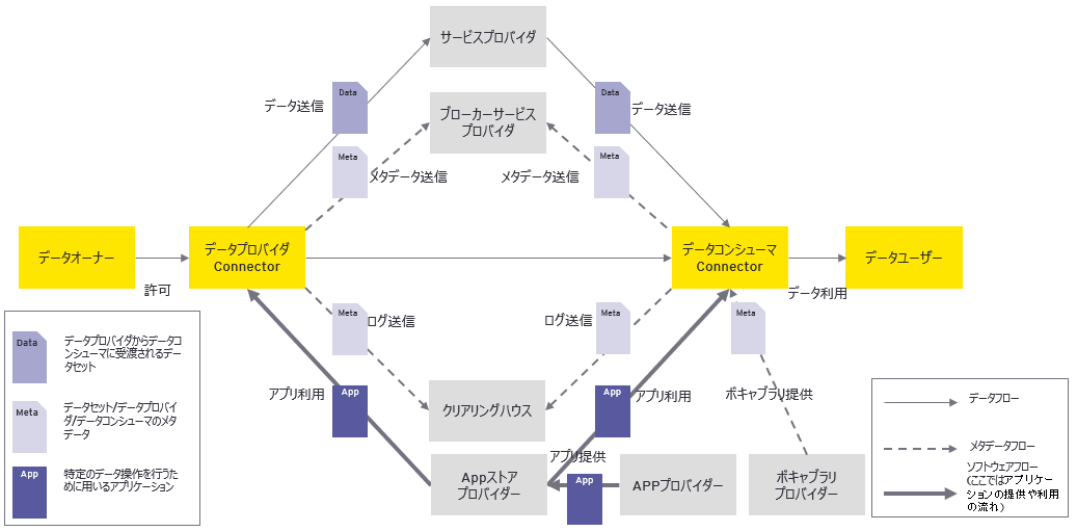
5.1.1 IDS のアーキテクチャ

(1) 前提事項

ア IDS のコンセプト図

「第 4 章 IDS・Gaia-X が実現するデータ連携のコンセプト」で述べた通り、IDS コネクタは、データ共有・利用を行う上で中核となるコンポーネントであり、IDS アーキテクチャの全体像は、コネクタを中心としたインタラクションに着目することで理解が容易になると思われる。図表 5-1 は、IDS コネクタを中心にデータスペースにおけるデータ交換とデータ共有のためのインタラクションを概要レベルで示したものである。

図表 5-1 IDS における役割とインタラクション
（「IDS Reference Architecture Model 」より EY 作成）



なお、上図に示されていない参加者やコンポーネントも存在するが、日常的なオペレーションに関与していない参加者（証明書発行機関や評価機関）や、他の全てのコンポーネントと接続する必要があるコンポーネント（ソフトウェアプロバイダ、ID プロバイダ）については、記載を省略している。

以下では、上図で省略しているものも含めて、IDS アーキテクチャへの参加者及び参加者が提供や利用を行うコンポーネントについて概要レベルで説明する。それぞれの説明にあたっては、IDS の参加者や各コンポーネントの役割に焦点を当てる。デー

タプロバイダ及びデータコンシューマが持つコネクタを中心とした具体的なデータ交換の流れについては、「5.2.1 IDS におけるプロセス」に記載する。

イ 参加者

以下、IDS の参加者の役割について紹介する[144]。それぞれの役割を担おうとする参加者は、目的等に応じて、技術的、物理的、組織的なセキュリティレベルを満たしているかという観点で、認証を受ける必要がある。これは、IDS に参加しようとする組織の認証は、全ての参加者間の信頼を確立するための基本的な手段であると考えられていることによる。参加者の認証プロセスに適用されるスキームの詳細については、で詳述する。参加者の役割は、主要な参加者（Core Participant）、仲介者（Intermediary）、ソフトウェア・サービスプロバイダ、ガバナンス機関の 4 種類に分類することができる。以下、それぞれに分けて説明する。

（ア）主要な参加者（Core Participant）

Core Participant（以下、主要な参加者）は、IDS におけるデータ交換プロセスに主体的に関与する。このカテゴリに属する参加者は、データオーナー、データプロバイダ、データコンシューマ、データユーザ、及びアプリプロバイダである。コア参加者の役割は、データを所有又は提供若しくは消費又は利用しようとするあらゆる組織が担うことができる。以下、それぞれのコア参加者の役割、ならびに他の参加者及びそれらが提供するコンポーネントとの関係等について記載する。

a データオーナー

通常、データオーナーの役割を担う参加者とデータプロバイダの役割を引き受ける参加者は同一である。しかし、データプロバイダがデータオーナーでない場合もある。例えば、企業がデータ管理のために外部の IT サービスプロバイダを使用している場合や、データ管理がデータ受託者に引き継がれている場合等、技術的にデータオーナーとは異なる主体がデータを管理している場合が想定される。データオーナーがデータプロバイダと同一の主体ではない場合、データオーナーは、データプロバイダがデータコンシューマに提供しようとしているデータにつき、提供の認否を判断する。上記の内容は契約によって文書化されなければならない。契約には、提供するデータのユーセージポリシー（後述）に関する情報についても含めるべきである。

b データプロバイダ

データプロバイダの主な活動は、データオーナーのデータをデータユーザに提供することである。前述の通り、データプロバイダはデータオーナーと同一である場合が多いが、必ずしも同一である必要はない。データプロバイダは、図表 5-2 に

---

144 *REFERENCE ARCHITECTURE MODEL 3.0,* INTERNATIONAL DATA SPACES ASSOCIATION, December 2020, p21-p25, https://internationaldataspaces.org/wp-content/uploads/IDS-Reference-Architecture-Model-3.0-2019.pdf（2022 年 3 月 17 日アクセス）

ある参加者及びそれらが提供するコンポーネントとのインタラクションを、コネクタを介して行う。

図表 5-2 データプロバイダと他コンポーネントとのインタラクション

対象	データプロバイダとの関係
ブローカーサービス プロバイダ	データプロバイダは、データユーザがデータプロバイダに対してデータ要求を円滑に行えるよう、データに関するメタデータをブローカーサービスプロバイダに提供する。
クリアリングハウス	データプロバイダは、データプロバイダは請求や紛争解決のため、クリアリングハウスに対して取引完了（又は失敗）の詳細を記録する。
アプリストア プロバイダ	データプロバイダは、提供するデータの品質向上等を目的として、アプリケーションを活用することができる。その際、アプリストアプロバイダから提供されるアプリケーションをダウンロードし、コネクタ内に実装する。
サービスプロバイダ	IDS に参加するための技術的インフラがデータプロバイダによって整備されていない場合、データプロバイダはサービスプロバイダを利用して、IDS に接続することができる。

c データコンシューマ

データコンシューマは、データプロバイダからデータを受け取る。データコンシューマはデータプロバイダのカウンターパートであり、データコンシューマが行う活動はデータプロバイダが行う活動と類似している。データコンシューマもデータプロバイダと同様、自身が持つコネクタを介して仲介者及びそれらが提供するコンポーネント（後述）とインタラクションを行う。

d データユーザ

データオーナーが提供するデータを法的に管理する法的主体であるのと同様に、データユーザは、ユーセージポリシーによって指定されたデータオーナーのデータを使用する法的権利を有する法的主体である。通常、データユーザはデータコンシューマと同一だが、これらの役割が異なる参加者によって担われることがある点においても、データオーナーとデータプロバイダの関係と同様である。

e アプリプロバイダ

アプリプロバイダは、IDS で利用されるアプリケーションを開発する。IDS の文脈では、アプリケーションとは参加者が IDS に参加するために必要な中核的な技術コンポーネントであるコネクタ内に配置できるアプリケーションを指し、データプロバイダとデータコンシューマ間におけるコネクタを介したデータ交換プロセスします。アプリケーションを展開するためには、IDS のシステムアーキテクチャに準拠する必要がある。特に機密情報を処理するアプリケーションは、アプリケーションの信頼性を高めるために、証明書発行機関による認証が必要な場合もある。各アプリケーションは、データプロバイダやデータコンシューマが使用でき

るよう、アプリストアで公開される。

（イ）仲介者（Intermediary）

Intermediary（以下、仲介者）は、主要な参加者によるデータ交換プロセスを仲介し、データ交換に必要なコンポーネントの提供を担う。このカテゴリに属する参加者は、ブローカーサービスプロバイダ、クリアリングハウス、ID プロバイダ、アプリストアプロバイダ及びボキャブラリプロバイダである。これらは、コア参加者同士の信頼の確立、メタデータの提供及びサービスに関するビジネスモデルの構築により、IDS の参加者に利益を創出する。それぞれが提供する各コンポーネントが果たしている機能の概要について、「5.1.2 (2) コンポーネント」、機能詳細については「6.1 IDS コンポーネント」にて詳述する。

a メタデータブローカーサービスプロバイダ

ブローカーサービスプロバイダは、IDS で利用可能なデータソースの情報を保管・管理する仲介業者であり、複数のブローカーサービスプロバイダが同時に存在することも想定されている。IDS でメタデータブローカーサービスを提供する組織は、同時に他の仲介者の役割（クリアリングハウスや ID プロバイダ）を担うこともできる。

ブローカーサービスプロバイダの役割は、データプロバイダがデータコンシューマに対してメタデータを提供する際の仲介である。メタデータの内容はデータプロバイダ自身の情報に関する自己記述であり、IDS インフォメーションモデル（「5.1.1 (3) ウ（エ)IDS インフォメーションモデル」）等に準拠してデータプロバイダが自己記述を行う。

b クリアリングハウスプロバイダ

クリアリングハウスプロバイダは、すべてのデータ交換取引の清算・決済サービスを提供する仲介業者である。IDS では、清算業務はメタデータリポジトリの維持とは技術的に異なるため、メタデータブローカー業務と分離されている。だが、既に述べたように、クリアリングハウスプロバイダとブローカーサービスプロバイダの両者の役割は、データプロバイダとデータコンシューマの双方からの信頼を得た仲介者として行動する必要があるため、同じ組織が担うことも可能である。

クリアリングハウスは、データ交換の過程で実行されたすべての活動を記録する。データ交換又はその一部が完了すると、データプロバイダとデータコンシューマの双方は、クリアリングハウスで取引の詳細を記録することにより、データ転送が正常に行われていることを確認する。この記録情報に基づいて、その取引は課金される。また、ログ情報はコンフリクトの解消（データプロバイダからのデータをデータコンシューマが受け取ったかの確認等）にも利用される。 クリアリングハウスプロバイダは、課金やコンフリクト解消等のために、実行された（記録された）トランザクションに関するレポートも提供する。

c ID プロバイダ

ID プロバイダは、IDS 参加者の ID 情報を作成、維持、管理、監視、検証するサービスを提供する。ID プロバイダの役割は、IDS の安全な運用と、データの不正アクセスを回避するために不可欠である。 ID プロバイダは、Certification Authority（以下 CA、IDS の参加者の電子証明書を管理）、Dynamic Attributes Provisioning Service（以下 DAPS、参加者の動的属性を管理）、Personal Information Service（以下、ParIS）、Dynamic Trust Monitoring（以下 DTM、ネットワークのセキュリティと動作を継続的に監視するサービス）の 4 つの技術コンポーネントから構成されている。それぞれの基本的な機能については、コンポーネントとして後述する。

d アプリストアプロバイダ

アプリストアは、アプリプロバイダが提供するアプリケーションに関する情報を管理しており、データプロバイダやデータコンシューマに対してアプリを提供する。アプリストアは、データプロバイダ、データコンシューマ、アプリプロバイダの三者を仲介者として、アプリケーションとそれに対応するメタデータの公開や取得を行うためのインターフェースを提供する。

e ボキャブラリプロバイダ

ボキャブラリプロバイダは、データプロバイダやデータコンシューマがデータセットの注釈やコネクタ等の自己記述に使用できるボキャブラリの管理・提供を行う。ボキャブラリプロバイダは、自己記述の基礎となる IDS インフォメーションモデル（「5.1.1 (3) ウ (エ)IDS インフォメーションモデル」）を提供しているほか、他のドメイン固有のボキャブラリを提供することもできる。

(ウ) サービス・ソフトウェアプロバイダ

a サービスプロバイダ

データプロバイダやデータコンシューマ自身が IDS への参加のための技術基盤を導入していない場合、参加者は IDS で利用できるようにするためのデータを、他の組織のために必要なインフラをホストしているサービスプロバイダに転送することができる。この役割には、IDS データ処理機能を向上させるために、データプロバイダやデータコンシューマに対して追加のデータ処理機能（データ分析、データ統合、データクレンジング等）を提供するプロバイダも含まれる。なお、データ処理機能の向上には、データプロバイダやデータコンシューマ自身でアプリストアプロバイダから提供されるアプリケーションをコネクタ内に実装するという方法もあり、この場合にはデータをサービスプロバイダに転送する必要はない。すなわち、技術基盤から機能レベルまでの包括的なサービス提供者となり得るのがサービスアプリストアプロバイダであるのに対して、あくまでアプリケーション提供を通じた追加機能の拡充をサポートするのがアプリストアプロバイダである

という区別がある。

b ソフトウェアプロバイダ

ソフトウェアプロバイダは、IDS が必要とする機能を実装するためのソフトウェアを提供する。 アプリケーションとは異なり、ソフトウェアはアプリストアプロバイダから提供されるのではなく、ソフトウェアプロバイダの通常の流通経路で提供され、ソフトウェアプロバイダとユーザ（データプロバイダ、データコンシューマ、ブローカーサービスプロバイダ等）との個別契約に基づいている。このことは、ソフトウェアプロバイダとデータプロバイダ、データコンシューマ等との間の契約が、IDS の範囲外に留まることを意味する。

（エ）証明書発行機関（Certification Body）及び評価機関（Evaluation Facility）

Certification Body（以下、証明書発行機関）及び Evaluation Facility（以下、評価機関）は、IDS への参加を希望する組織及び使用を希望するソフトウェアコンポーネントに対して認証プロセス及び証明書の発行を行うことにより、IDS の参加者の利益を創出する。

証明書発行機関は、指定された評価機関とともに、IDS の参加者とコア技術コンポーネントの認証を担当する。これにより、準拠した組織のみが信頼できるビジネスエコシステムへのアクセスを許可されることを保証する役割を果たす。証明書発行機関は、評価機関の行動と決定を監督する。 このプロセスの詳細については、「5.2.1 (1) オンボーディング」にて詳述する。

ウ デジタル ID

データ共有やデータ交換のための信頼関係の確立は基本的な要件である。これに必要なプロセスは大別して 2 段階あり、証明書発行機関及び評価機関を中心とする IDS-ID の発行に必要な評価プロセス、並びに CA や DAPS による認証・認可からなる。以下、これらのプロセスを IDS リファレンスアーキテクチャモデルに基づいてデジタル ID として紹介する[145]。

前者の評価プロセスは、IDS への参加や IDS へのコンポーネントの提供を希望する組織（以下、申請者）に対する参加者及びコンポーネントに対して行われる。申請者の要求に応じて実行され、参加者と評価機関の間の契約に依存する。同様に、サービスプロバイダは、コンポーネントの評価を要求することができる。このプロセスにおいて、証明書発行機関は関係する評価機関の監督に責任を負う。

一方、後者の認証・認可は、参加者が実際のデータ交換に際して参加者が電子証明書（X.509 証明書）の呼び出しや Dynamic Attribute Token（以下、DAT）等を要求することで行われる。前者のプロセスによる評価結果は証明書発行機関から CA に通知

[145] *REFERENCE ARCHITECTURE MODEL 3.0*, INTERNATIONAL DATA SPACES ASSOCIATION, December 2020, p26-p27, https://internationaldataspaces.org/wp-content/uploads/IDS-Reference-Architecture-Model-3.0-2019.pdf（2022 年 3 月 17 日アクセス）

され、結果に応じて CA は参加者に対して IDS-ID 及び電子証明書（X.509 証明書）を付与する。参加者は、X.509 証明書をコンポーネント内に配置することに成功した後、DAPS に登録する。

DAPS がエコシステム内のすべての参加者の信頼性を分類するためには、参加者の継続的なモニタリングが必要である。DTM は、IDS コンポーネントごとに監視機能を実装しており、DTM は DAPS と情報を共有し、データ交換トランザクションにおいて 2 つの参加者のそれぞれに現在のレベルを通知する。これにより、DAPS が参加者に対して DAT を発行することで、参加者がデータ交換時に必要な認証・認可を受けることができる。

上記の参加者と ID プロバイダの関係は、図表 5-3 のように示すことができる。

図表 5-3　IDS でデジタル ID を発行するために必要なインタラクション

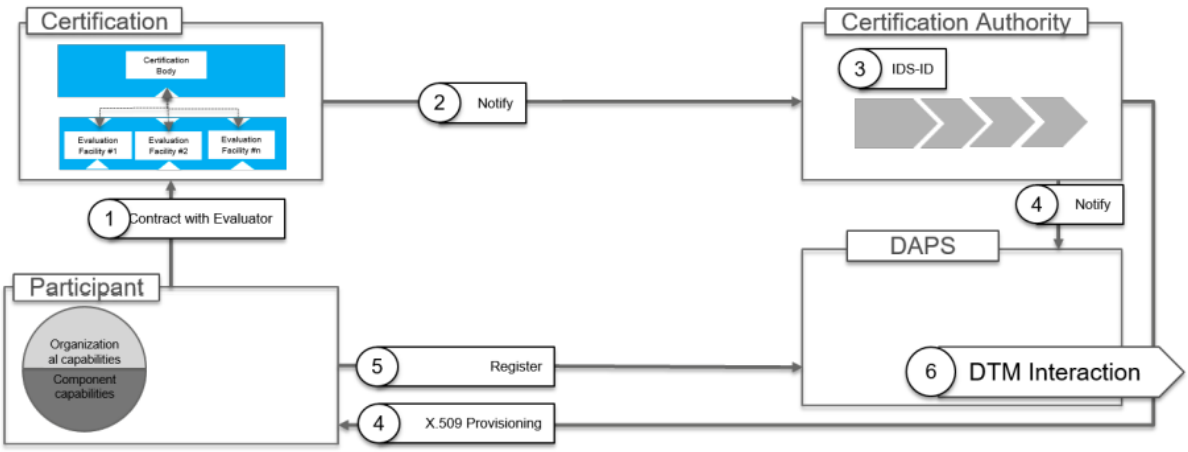


Figure 3.2: Interactions required for issuing a digital identity in the IDS

エ　ユーセージコントラクト

契約書の内容の多くは、マシンリーダブルな形でモデル化することができない。しかし、IDS は、適用可能な契約のカテゴリを定義する方法を規定し、その使用状況を観察し、検証を報告するパターンを提示できるようにする取組を行っている。IDS は既存の法的拘束力のある契約とは別に、技術的に強制される契約のための技術的な枠組みをユーセージコントラクトとして提供する。以下、IDS リファレンスアーキテクチャモデルに基づき、ユーセージコントロールについて概説する[146]。

ユーセージコントラクトは、カテゴリごとのユーセージポリシーで構成される。各ユーセージポリシーには、IDS リソースの特定の許可又は義務が記述される。ユーセージコントラクトはマシンリーダブルな形式で記述される。いかなる場合においても、ユーセージコントラクトは常に複数の IDS 参加者間の既存の法的合意の延長とみなさ

[146] *REFERENCE ARCHITECTURE MODEL 3.0*, INTERNATIONAL DATA SPACES ASSOCIATION, December 2020, p28, https://internationaldataspaces.org/wp-content/uploads/IDS-Reference-Architecture-Model-3.0-2019.pdf（2022 年 3 月 17 日アクセス）

れなければならず、ユーセージコントラクトは常に締結された契約に沿ったものでなければならない。 IDS 参加者間の契約は、技術的な部分と非技術的な部分から構成される。技術的な部分は、インターフェース（API）とユーセージポリシーの記述に重点を置いており、IDS インフォメーションモデル（後述）に基づくことが求められる。非技術的な部分はデータ交換の法的側面に焦点を当てているが、図表 5-4 のように、IDS 側の責任では技術的な部分に落とし込めていない要素と解釈することもできよう。

図表 5-4　ユーセージコントロールの技術的実施と組織的実施

Figure 3.3: Technical Enforcement and Organizational Enforcement of Usage Policies

(2) コンポーネント

IDS のコンポーネントは、ID プロバイダ（CA、DAPS、ParIS）、ボキャブラリプロバイダ、メタデータブローカー、クリアリングハウス、アプリストア、コネクタ等から構成されている。これらと関連して、コネクタ、メタデータブローカー、アプリケーション及びサービス、アプリストア、ハードウェアはコアコンポーネントと定義されており[147]、参加者と同様セキュリティレベルを満たしているか等の観点から、コアコンポーネントとしての証明書発行を受ける必要がある。その詳細については、「5.3.1 (1) 証明書の発行」に記載の通りである。

コンポーネントの概要レベルでの機能概要は、図表 5-5[148]の通りである。

147

148 *REFERENCE ARCHITECTURE MODEL 3.0*, INTERNATIONAL DATA SPACES ASSOCIATION, December 2020, p21-p27, https://internationaldataspaces.org/wp-content/uploads/IDS-Reference-Architecture-Model-3.0-2019.pdf（2022 年 3 月 17 日アクセス）

図表 5-5　各コンポーネントの機能概要

コンポーネント	機能概要
CA	ID プロバイダの構成要素の一つ。電子証明書（X.509 証明書）の発行、有効性確認及び失効に責任を負う。
DAPS	ID プロバイダの構成要素の一つ。動的属性トークン（DAT）を発行し、参加者又はコネクタの動的属性を検証する。DAT には参加者とコネクタの署名が入った動的な属性が含まれており、コネクタの自己記述が事実かつ有効であることを示す機能を持つ。DAT はコネクタの通信ごとに提示されるため、通信中のコネクタは、いつでも通信相手の信頼性を確認することができるようになる。
DTM	ID プロバイダの構成要素の一つ。ネットワークのセキュリティと挙動を継続的に監視する。コネクタの完全性をより長い期間検証することを目的としており、完全性違反の重大性に応じて、参加者への通知から X.509 証明書の失効に至るまで、特定のアクションを起動することができる。
ParIS	ID プロバイダの構成要素の一つ。ParIS は、IDS 参加者の属性を公開したり問い合わせたりするためのインタラクションメカニズムを提供する。
ボキャブラリプロバイダ	（再掲）データプロバイダやデータコンシューマがデータセットの注釈やコネクタ等の自己記述に使用できるボキャブラリの管理・提供を行う。
クリアリングハウス	（再掲）すべてのデータ交換取引の清算・決済サービスを提供する仲介業者である。 データ交換の過程で実行されたすべての活動を記録する。データ交換又はその一部が完了すると、データプロバイダとデータコンシューマの双方は、クリアリングハウスで取引ログを記録することにより、データ転送が正常に行われていることを確認する。この記録情報に基づいて、その取引は課金される。 ログ情報はコンフリクトの解消（データプロバイダからのデータをデータコンシューマが受け取ったかの確認等）にも利用される。 課金やコンフリクト解消等のために、実行された（記録された）トランザクションに関するレポートも提供する。
アプリストア	（再掲）アプリプロバイダが提供するアプリケーションに関する情報を管理しており、データプロバイダやデータコンシューマに対してアプリを提供する。 また、データプロバイダ、データコンシューマ、アプリプロバイダの三者を仲介者として、アプリケーションとそれに対応するメタデータの公開や取得を行うためのインターフェースを提供する。

(3) 運用モデル

IDS は、既存の技術やアプリケーションに関係なく、IDS の機能要件と、その結果として実装されるべき機能を IDS リファレンスアーキテクチャモデルの「3.2 FUNCTIONAL LAYER として定めている。

以下、各コンポーネントによって具体的に落とし込まれていない機能も含めて紹介するという趣旨で、IDS リファレンスアーキテクチャモデルの「3.2 FUNCTIONAL LAYER」への記載事項を IDS の運用モデルとして紹介する[149]。なお、運用モデルが既に参加者の役割やコンポーネントによって具体化されている場合は、該当箇所にリファレンスを示

[149] *REFERENCE ARCHITECTURE MODEL 3.0*, INTERNATIONAL DATA SPACES ASSOCIATION, December 2020, p29-p32, https://internationaldataspaces.org/wp-content/uploads/IDS-Reference-Architecture-Model-3.0-2019.pdf（2022 年 3 月 17 日アクセス）

す。

ア トラスト

「トラスト」グループは、3 つの主要な側面（役割、ID 管理、ユーザ認証）から構成され、ガバナンス側面によって補完される。

（ア）役割

IDS の参加者が担う各役割は、一定の権利と義務を有する。たとえば、ID プロバイダは、IDS の参加者の ID 情報を作成、維持、管理、監視及び検証するサービスを提供する責任がある。各役割の概要については、「5.1.1 (1) 前提事項」によって具体化されており、「仲介者」の参加者等が提供する各コンポーネントの詳細は「6.1 IDS コンポーネント」に記載の通りである。

（イ）ID 管理

IDS に参加するすべてのコネクタは、一意の識別子と有効な証明書を持つ必要がある。さらに、各コネクタは他のコネクタの ID を確認できなければならない。ID 管理を行う仕組みは、「4.1.1 IDS のコンセプト」により実現されている。

（ウ）参加者認証

IDS の各参加者は、参加者間の信頼を確立するために、認証を受ける必要がある。参加者認証を行う仕組みは、「5.3.1 (1) イ (ア)参加者への証明書発行」により実現されている。

イ セキュリティとデータ主権

「セキュリティとデータ主権」グループには、コアコンポーネントへの証明書発行、認証と認可、ユーセージポリシーとポリシーエンフォースメント、信頼できる通信とセキュリティという 4 つの主要な側面が含まれる。

（ア）証明書発行

IDS のコアコンポーネント、特にコネクタは、すべての参加者の間で信頼を確立するために、証明書発行機関の認証が必要である。証明書発行プロセスの詳細については、「5.3.1 (1) 証明書の発行」 に記載されている。

（イ）認証・認可

各コネクタには有効な X.509 証明書が必要である。この証明書により、IDS の

各参加者は他の参加者の ID やセキュリティ機能等のコネクタの機能を確認することができる。特定の条件（例：セキュリティプロファイル）が適用される場合がある。認証・認可の詳細については、「5.3.1 (2) 認証・認可の仕組み」により実現されている。

(ウ) ユーセージポリシーとポリシーエンフォースメント

IDS では、データオーナー（多くの場合、データプロバイダと同一組織）とデータユーザ（多くの場合、データコンシューマと同一組織）は、自分のデータが指定されたユーセージポリシーに従ってデータコンシューマによって扱われることを常に確認することができる。各参加者はユーセージポリシーを定義し、送信データに添付することができる。ポリシーには、例えば、データの永続化の禁止や、データの他者への転送禁止等の制限が含まれる場合がある。 ユーセージポリシーとポリシーエンフォースメント（ポリシーの強制）に関する詳細は、「5.3.1 (3) エンフォースメント」を中心に記載されている。

(エ) 信頼できる通信とセキュリティ

コネクタ、アプリストア及びメタデータブローカーは、接続相手のコネクタが信頼できる（すなわち認証された）ソフトウェアスタックを実行しているかどうかを確認できる。外部コネクタとの通信はすべて暗号化され、完全性が保護される。各データオーナーとデータプロバイダは、そのデータが指定されたユーセージポリシーに従ってデータコンシューマのコネクタによって処理されることを確認できなければならない。また、万が一アプリケーションの機能が侵害された場合でも影響を軽減することができるよう、アプリケーション同士やコネクタを分離すること等の適切な技術的手段を適用しなければならない。

データプロバイダとデータコンシューマは、選択したセキュリティプロファイルをサポートするコネクタをデプロイすることで、それぞれのコネクタに適用するセキュリティレベルを決定することができる。信頼できる通信セキュリティのうち、アプリケーションやコネクタの分離ついては「5.3.1 (2) ク トラストプラットフォーム」、コネクタを含むコアコンポーネントのセキュリティレベルについては「5.3.1 (1) イ（イ)b セキュリティプロファイル」及び「5.3.1 (2) キ（カ)コネクタのセキュリティプロファイル」に記載の通りである。

ウ データエコシステム

データの記述、検出及び正確な交換も、IDS が満たすべき重要な要素である。この実現のため、IDS におけるすべてのデータソースは IDS インフォメーションモデルに沿って記載される。「データエコシステム」グループは、データソースの記述、メタデータブローカーリング、ボキャブラリの 3 つの主要な側面から構成されている。

(ア) データソースの記述

参加者は、異なるバージョンのメタデータを記述、公開、維持、管理する機会を持たなければならない。メタデータは、データソースのセマンティクスと同様に、構文とシリアライゼーションを記述する必要がある。さらに、メタデータは、データソースのアプリケーション領域を記述する必要がある。コネクタのオペレータ（ここでは、データプロバイダ）は、特定のデータに関する価格、価格設定モデル及びユーセージポリシーを定義できなければならない。

(イ) メタデータブローカーリング

各コネクタは、そのデータソースのメタデータをメタデータブローカーに送信することができなければならない。各参加者は、参加者がメタデータにアクセスする権利を持っている場合、メタデータリポジトリのメタデータを閲覧及び検索できなければならない。さらに、各参加者はメタデータブローカーに登録されている参加者のリストを閲覧できなければならない。

(ウ) ボキャブラリ

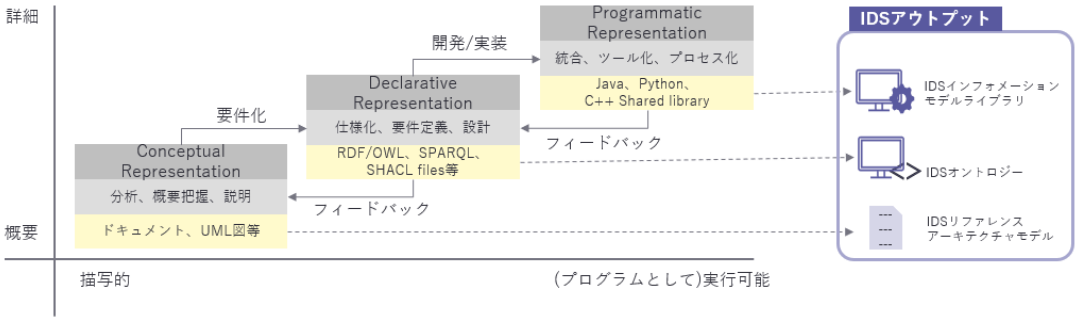
メタデータを作成及び構造化するために、コネクタのオペレータ（ここでは、データプロバイダやデータコンシューマ等）はボキャブラリを使用することができる。その際、コネクタのオペレータは、既存のボキャブラリを使用し、独自のボキャブラリを作成し又はボキャブラリハブによって提供される新しいボキャブラリで他の参加者と作業することができます。ボキャブラリハブとは、ボキャブラリの保存やコラボレーションを可能にする中央サーバである。コラボレーションには、検索、選択、マッチング、更新、変更要求、バージョン管理、削除、重複識別、未使用ボキャブラリ等が含まれることがある。

(エ) IDS インフォメーションモデル

IDS インフォメーションモデルは、参加者のデータアセット及び再利用可能なデータ処理ソフトウェア（以下、「リソース」と言う。）の記述、公開及び識別をサポートする。実際に各参加者やコンポーネントが IDS インフォメーションモデルを用いてリソースの記述、公開及び識別を行う際のインタラクションについては、「5.2.1 IDS におけるプロセス」を参照されたい。ここでは、運用モデルに関する説明として、IDS インフォメーションモデルの規定方法及びそれぞれの規定方法における内容につき、概説する。

IDS インフォメーションモデルは 3 段階の形式化レベルで規定され、概念レベル（Conceptual Representation）からコードレベル（Programmatic Representation）までで規定されている。それぞれの形式化レベルにおける関係性は図表 5-6 の通りであり、内容は図表 5-7 の通りである。

図表 5-6 IDS インフォメーションモデルの形式化レベルとそれぞれの関係（図）
（「IDS Reference Architecture Model」より EY 作成）



図表 5-7 IDS インフォメーションモデルの形式化レベルとそれぞれの関係（表）

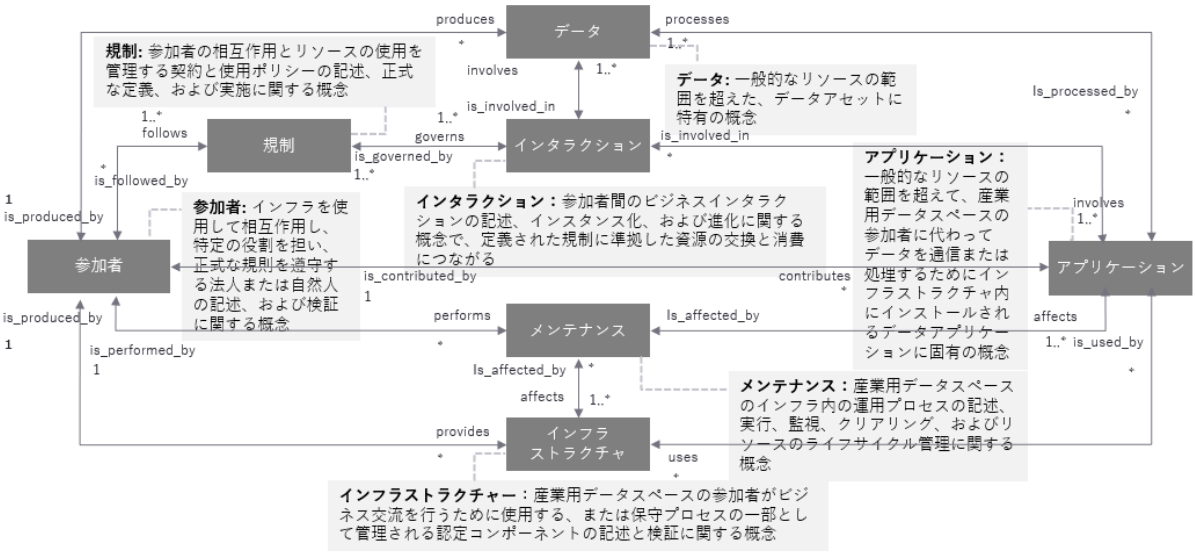
形式化レベル	内容
Conceptual Representation	• IDS インフォメーションモデルに関する基本的な情報を提供する。 • IDS 参加者内における概念の共有を促進する汎用的なものである。 • 特定の技術やドメインに依存しないハイレベルな概要を提示する。テキスト文書と視覚的な表記(UML 図等)によって、IDS 参加者内における概念の共有理解を促進する。その内容の概要は図表 5-8 の通りである。 • Conceptual Representation としてのアウトプットは、IDS リファレンスアーキテクチャモデルの「3.4 INFORMATION LAYER」に記載されている。
Declarative Representation	• IDS インフォメーションモデルを W3C のセマンティックウェブ技術標準と標準的なモデリング語彙（DCAT、ODRL 等）をベースに規定する。 • Conceptual Representation で想定される概念を機械的に解釈可能な形式で規定する。その規定内容のイメージは図表 5-9 の通りである。 • Declarative Representation としてのアウトプットは、IDS オントロジーとして参加者に公表されている[150]。
Programmatic Representation	• Declarative Representation で規定された IDS オントロジーを対象プログラミング言語のネイティブ構造（Java、Python、C++クラス等）に可能な範囲で開発や実装を行う。 • Programmatic Representation としてのアウトプットは、IDS インフォメーションモデルライブラリとして参加者に公表されている[151]。

[150] “GitHub - International-Data-Spaces-Association/International Data Spaces Information Model”. https://international-data-spaces-association.github.io/InformationModel/docs/index.html（2022 年 3 月 28 日アクセス）
[151] “GitHub - International-Data-Spaces-Association/InformationModel”. https://github.com/International-Data-Spaces-Association/InformationModel#:~:text=The%20International%20Data%20Spaces%20%28IDS%29%20Information%20Model%20The,participants%20by%20means%20of%20the%20IDS%20infrastructure%20components.（2022 年 3 月 28 日アクセス）

図表 5-8　Conceptual Representation の記載内容（概要）

項目	概要	概念図
Content	リソースに内在する実体として機械的に解釈可能な任意のバイナリ形式な方法での「コンテンツ」の記述方法を対象とする	
Concept	ContentやContextといったリソースに関連したエンティティの意味、注釈、解釈のモデル化を対象とする	
Community of Trust	データ所有者のデータ主権を維持しつつ、データ提供者とデータ消費者の間で安全かつ信頼できる方法でリソースを交換し共有するためのIDSの基本要件を対象とする	
Commodity	リソースの資源の価値と実用性の評価を対象とする	
Communication	リソースのコンテンツを利用可能なRepresentationの1つで通信する手段を対象とする	
Context	時間的、空間的な側面と、リソースのコンテンツが関連する実世界のエンティティを対象とする	

図表 5-9 Declarative Representation の記載内容（概要）
（「Ontology Draft」より EY 作成）



エ　標準化された相互運用性

参加者間の標準的なデータ交換は、IDS の基本的な側面である。IDS コネクタは、この目的のための主要な技術コンポーネントである。

（ア）オペレーション

参加者は、自分の IT 環境でコネクタソフトウェアを実行できる必要がある（モバイル又は組み込みデバイスでコネクタを実行することでも可能）。加えて、コネクタ内のデータワークフローを定義することができなければならない。コネクタのユーザは識別及び管理可能でなければならない。パスワード及びキーストレー

ジは保護されなければならない。すべてのアクション、データアクセス、データ送信、インシデント等はログに記録されなければならない。このログデータは、データ使用状況等の評価やインシデントが発生した場合の自動通知等に用いられる必要がある。

（イ）データ交換

コネクタは、プッシュ・メカニズム又はプル・メカニズムによって、企業のバックエンドシステムからデータを受信する必要がある。データは、インターフェースを介して提供されるか、他の参加者に直接プッシュされる。そのためには、各コネクタは一意に識別可能でなければならない。他のコネクタは、データソースの購入やこれらのソースからデータの抽出を行うことができる。データは、他の参加者のバックエンドシステムに書き込むことができる。

オ 付加価値を提供するアプリケーション

実際のデータ交換の前後において、データの処理や変換が必要になることがある。そのために、IDS はアプリケーションを提供している。各アプリケーションには、その実装、アプリストアでの提供、インストール、サポートに至るライフサイクルがある。アプリストアはすべての参加者がはっきりと目にし、認識できるようにする必要がある。

（ア）データ処理とデータ交換

データ処理アプリ（データアプリの一種）は、期待される出力を生成するために入力データに適用される単一の明確に定義された処理関数を提供する必要がある。データ変換アプリ（データ処理アプリと同様、データアプリの一種）は、データコンシューマの要件に適合するように、データを入力形式から別の出力形式に変換できる必要がある（データに含まれる情報に大きな変更を加えることなく、すなわち、損失なしの変換を行う）。

（イ）アプリケーションの実装

アプリケーションの開発者は、ソフトウェアにメタデータ（機能やインターフェース、価格モデル、ライセンス等）を注釈できるようにする必要がある。アプリケーションは、インターフェース、依存関係、アクセス要件を明示的に定義する必要がある。

（ウ）アプリケーションの提供

認定されたアプリケーション開発者であれば、誰でもソフトウェア提供プロセス（アプリストアでの公開）を開始することができる。アプリストアでの公開に先

立ち、アプリケーションは証明書発行機関が管理する任意の評価及び認証プロセスに合格する必要がある。アプリストアは、認可されたユーザが適切なアプリケーションを検索することを適切にサポートする必要がある。特権を持つユーザ（管理者、オペレーター等）のアクセスには、強力な認証（2 ファクタ認証等）が必要である。

（エ）アプリのインストールとアフターサポート

専用のコネクタサービスは、公式アプリストアに由来しないアプリケーションの（アン）インストールにおいて、認定ユーザをサポートする必要がある。さらに、アプリストアから取得したアプリケーションの検索、インストール及び管理（削除又は自動更新等）をユーザが行えるようにする必要がある。

カ データマーケット

IDS で交換されるデータは、金銭的な価値を持つ場合もある。したがって、IDS は、清算や課金のようなデータマーケットの概念だけでなく、ガバナンスも統合しなければならない。

（ア）清算と課金

データオーナー（多くの場合、データプロバイダと同一）は価格モデル（転送毎、アクセス毎、日毎・月毎・年毎等）とデータの価格を定義することができる。あらゆる参加者のあらゆる取引を記録することができる。清算・課金プロセスはシンプルで標準化されていなければならない。

（イ）利用制限とガバナンス

IDS におけるガバナンスは、商品としてのデータ、データ所有権、データ主権、データ品質、データの出所という 5 つの側面から構成される。

（ウ）法的側面

データマーケットプレイスでのデータ取引には、自動で交渉できる法的な契約や条件が必要である。 そのため、典型的なデータ交換取引に関する標準的な契約が必要である。

5.1.2 Gaia-X のアーキテクチャ

本項では、Gaia-X において前提として把握すべき事項（例：参加者等）について「5.1.2 (1) 前提事項」で説明する。次に、フェデレーションサービスを構成する 5 つのコア機能（ID とトラスト、フェデレーションカタログ、データ主権サービス、コンプライアンス及びポータルと API）の概観について「5.1.2 (2) コンポーネント」で説明する。最後に、Gaia-X における運用上の仕組みについて「5.1.2 (3) 運用モデル」にて詳述する。

(1) 前提事項

最初に、Gaia-X において前提事項として把握すべきエンティティやリソース等とそれらの関係について説明する。ここで、エンティティとは、ID 管理に係る ISO 標準である ISO/IEC 24760-1 の 3.1.11「entity」[152]の定義に準拠する。まず、図表 5-10 でエンティティやリソース等の関係を示し、各項目の詳細について「5.1.2 (1) ア 参加者」、「5.1.2 (1) イ リソース」、「5.1.2 (1) ウ フェデレーションサービス」、「5.1.2 (1) エ サービスオファリング」、「5.1.2 (1) オ 契約」にて説明する。なお、各項目の説明は Gaia-X AISBL によって公開されている Gaia-X Architecture Document の第 3 章「Conceptual Model」[153]を参照している。なお、ここで紹介するエンティティ及びリソースはデータ交換に直接係るものであり、Gaia-X エコシステムへのオンボーディング時に登場する組織等については「5.2.2 Gaia-X におけるプロセス」等にて解説する。

図表 5-10 中に黄色でハイライトされている項目は Gaia-X のスコープ内であることを示している。図の上部は Gaia-X に登場する参加者を示し、下部はデータ交換に係る要素と Gaia-X のスコープ外の項目との関係を示している。

各項目間の関係について、SaaS の個人財務管理サービス（PFM）のオープンバンキングの具体例を用いて説明する。MyPFM という会社が、銀行 A と銀行 B に口座を持つエンドユーザにサービスを提案すると仮定する。MyPFM は、銀行 A と銀行 B が提供するサービスを利用して、エンドユーザの取引履歴を取得し、これらの銀行明細を集計して、財務ダッシュボードを作成する。銀行 A と銀行 B は、取引履歴データを提供するサービスオファリングを定義し、対応するサービスインスタンスを運用するサービス及びデータのプロバイダである。それと同時に、取引履歴データのリソース所有者でもあり、これはサービスオファリングを構成するリソースである。

MyPFM は、銀行 A と銀行 B が提供するサービスインスタンスを利用して、財務ダッシュボードを作成し、エンドユーザに提供するコンシューマという立場である。また、MyPFM は、ダッシュボードの作成や独自のアプリケーションを動作させるプログラムコードを実行するために、他のプロバイダから提供されるサービスインスタンスを利用する可能性もある。

上記の例から、Gaia-X ではプロバイダによって提供されるサービスオファリングをコンシューマが利用してサービスを作り出し、それらをエンドユーザが利用するという関

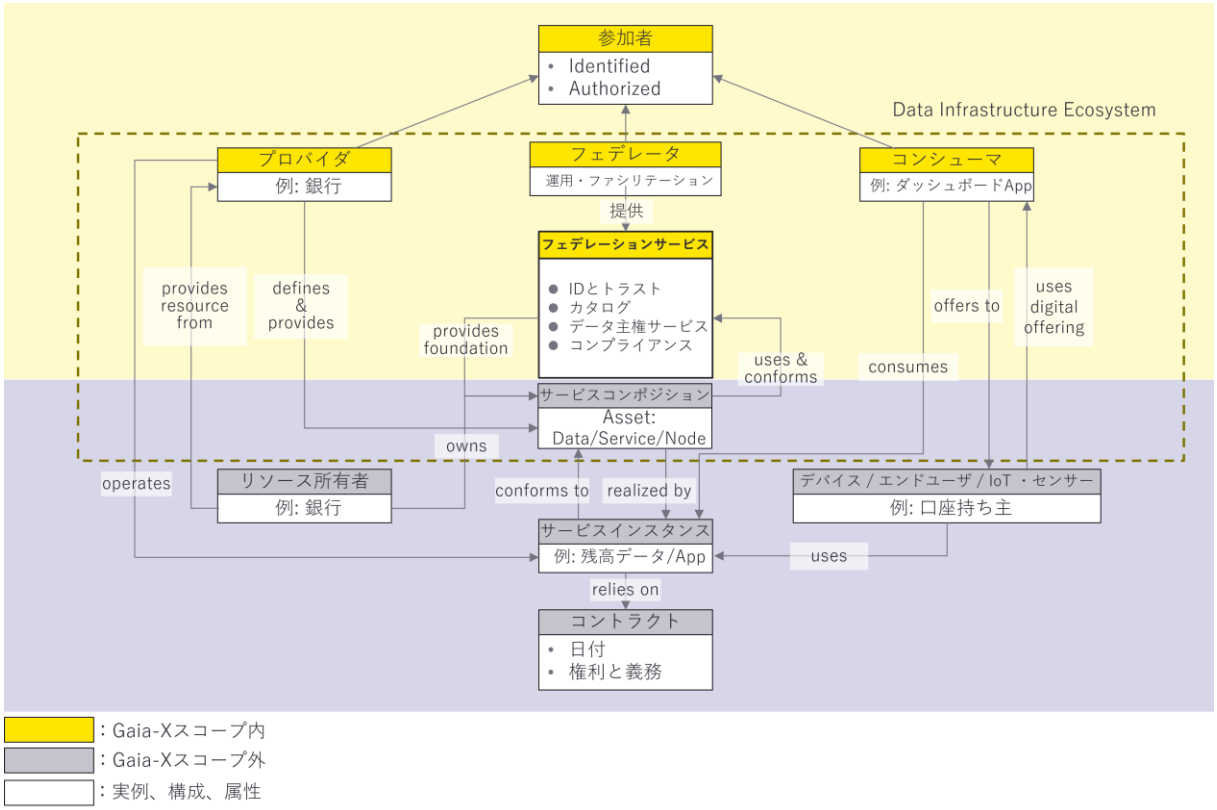
---

[152] IT Security and Privacy – A framework for identity management – Part 1: Terminology and concepts, ISO, January 2019, https://www.iso.org/standard/77582.html （2022 年 3 月 17 日アクセス）

[153] *Gaia-X Architecture Document*, Gaia-X European Association for Data and Cloud AISBL, December 2021, https://Gaia-X.eu/sites/default/files/2022-01/Gaia-X_Architecture_Document_2112.pdf （2022 年 3 月 17 日アクセス）

係となっている。

図表 5-10 「Gaia-X Architecture Document」より EY 作成



ア 参加者

Gaia-X における参加者は上述した ISO 標準のエンティティに準拠する。まず、参加者は Gaia-X エコシステムへオンボーディングし、自身のアイデンティティに紐づく自己記述を所有していることが前提である。参加者は、①プロバイダ、②コンシューマ、③フェデレータのうち 1 つ以上の役割を持つ。プロバイダとコンシューマはビジネス関係にあるのに対し、フェデレータは両者のやりとりを可能にする存在である。図表 5-11 は各参加者の役割を示している。

図表 5-11 Gaia-X における参加者

参加者	説明
プロバイダ	Gaia-X エコシステムにおいてリソースを提供する参加者を指す。ここで、Gaia-X エコシステムは、Gaia-X AISBL が定義した要件に適合するアーキテクチャを使用した個々のエコシステムの集合体を指す。プロバイダは、技術的なポリシーと利用規約を含む形でサービスオファリングを定義し、自己記述を含むサービスインスタンスを提供する。
コンシューマ	Gaia-X エコシステムでサービスオファリングを検索し、プロバイダが提供するサービスインスタンスを利用して、エンドユーザ向けのデジタルオファリングを提供する参加者を指す。

参加者	説明
フェデレータ	フェデレーションサービスの運用を担う。フェデレーションサービスの種類ごとに、1 人又は複数のフェデレータが存在する。

イ リソース

リソースとは、一般的に Gaia-X エコシステムにおけるオブジェクトを表す。リソースはデータリソース、ソフトウェアリソース、ノード、相互接続のいずれかを指す。各リソースはエンドポイントとアクセス権が紐づけられており、リソース所有者に属することを表している。

データリソースは、様々な形式のデータと、データ共有に必要な情報から構成される。ノードは、物理的あるいは仮想的なコンピュートリソースとしてのエンティティを指す。ソフトウェアリソースは非物理的な機能で構成される。相互接続は、2 つ以上のノード間の接続を示すリソースである。相互接続された複数のノードは、一般的に異なるインフラ環境としてデプロイされており、異なるコンシューマやプロバイダによって管理されていることを想定する。ノード間の相互接続により、レイテンシ、帯域幅、セキュリティ保証等の観点で通常のインターネット上の経路特性を上回ることが可能となる。リソーステンプレートとは、リソースを利用できるようにするためにプロバイダが提供するエンティティである。

なお、Gaia-X Workstream 2 Technical Implementation のコーディネータによると、相互接続リソースは、物理的なケーブルや Wi-Fi 等一般的なネットワーク機器による接続を含むより大きなスコープとして定義されるとのことである。本コーディネータへのインタビュー結果は、「8.3 IDSA・Gaia-X に関するインタビュー結果」を参照されたい。

リソーステンプレートはそれぞれのリソースに依存し、データスキーマ等の仕様と使用権等が定義されている。リソーステンプレートはサービスオファリングを構成するために使用される。

次にリソースに関して適用されるポリシー・ルールについて説明する。ポリシーとは、Gaia-X 内の参加者のアクティビティに適用されるルールとして定義され、Gaia-X の各リソースに関する自己記述の属性として存在する。技術的な観点では、ポリシーはあるエンティティの正しい又は期待される動作を規定するルールの位置づけである。

ポリシー・ルールは、Gaia-X AISBL がプロバイダとサービスオファリングに向けて定義した一般的なポリシーに該当する。例えば、GDPR 等の法規制に基づくプライバシーポリシーやサイバーセキュリティポリシー等があり、フェデレーションサービスのコア機能の一つであるコンプライアンスを通じて、各サービスオファリングが準拠しているか検証される。検証プロセスに関する説明は、「5.1.2 (2) エ コンプライアンス」にて述べる。これらの一般的なポリシーは、特定のサービスオファリングに紐づく詳細なポリシーの基礎であり、それを基に個別のポリシーを追加で設定できる。すなわち、個々のプロバイダやコンシューマによって定義された個別の制限等を含むことを意味する。これらのポリシーは、プロバイダポリシー（別名：ユーセージポリシー）又はコンシューマーポリシー（別名：検索ポリシー）として定義される。

プロバイダポリシー・ユーセージポリシー
コンシューマによるリソースの利用を制約する。例えば、データのユーセージポリシー

によって、x 回又は y 日間のみ使用可能というような制限を設けることができる。

コンシューマポリシー
コンシューマが要求するリソースに関して制限を記述する。例えば、コンシューマは、あるサービスのプロバイダが、特定の管轄区域に所在すること、あるいは特定のサービスレベルを満たすこと等の要求を満たすよう制限を加えることができる。

ウ フェデレーションサービス

フェデレーションサービスは Gaia-X エコシステムを実現するために必要なサービスである。フェデレーションサービスは ID とトラスト、フェデレーションカタログ、データ主権サービス、コンプライアンスの 4 つのコア機能によって構成される。フェデレーションサービスを構成するコア機能及びコンポーネントについて、「5.1.2 (2) コンポーネント」にて詳述する。

エ サービスオファリング

サービスオファリングは、プロバイダによって複数のリソース群を集約されたものを指し、フェデレーションカタログに単一のエントリとして公開される。サービスオファリングは、それ自体がサービス構成を実現するために集約されることがある。サービスオファリングをホスティングするインスタンスは、プロバイダからコンシューマに提供されるものである。フェデレーションサービスは、サービスオファリングの基礎を提供し、サービスオファリングはフェデレーションサービスを使用し、これに準拠する。

オ 契約

Gaia-X AISBL は、契約の実現には関与しない前提である。しかしながら、参加者がスムーズに契約を締結することができるように、以下のような一般的な契約モデルのコンセプトを定義している。

- 契約はビジネス関係の基本である。
- リソースに関する権利を有するライセンサーは、定義した条件に従って本権利が利用されることを許諾する。
- ライセンシーは、ライセンサーによって定義された条件に従ってリソースを利用する権利の許諾を受ける。
- ライセンサーとライセンシーは、契約という形式で合意する。
- Gaia-X における全ての役割は法人とみなすことができ、ライセンサー、ライセンシー又はその両方としての役割を有することができる。
- 従来の中央集権的なエコシステムでは、エコシステムの所有者であるプラットフォーム提供者が契約フレームワークを定義し、参加者は交渉の余地なくそれを受け入れる必要がある。
- 分散型エコシステムやフェデレーションエコシステムでは個々の契約がより重要である。

- 契約について交渉することは主権的な観点で重要である。契約に係る当事者全員が合意した契約内容を履行すること、権利を確認すること、義務を果たすこと、情報が悪用されていないことを裏付けることが重要である。
- 「Computable Contract」は、契約設計、契約交渉、契約締結、契約解除の複雑なプロセスを容易にし、契約義務の履行と国内法の遵守を監視することを目的とする。

(2) コンポーネント

Gaia-X のフェデレーションサービスを構成するコア機能及びコンポーネントについて説明する。なお、本章における各コンポーネントの説明は Gaia-X Architecture Document の第 5 章「Federation Services」及び「Federation Services Specification」[154]を参照している。フェデレーションサービスは、インフラストラクチャとデータの連携を可能にするものであり、OSS として提供される。フェデレーションサービスは 4 つのコア機能（ID とトラスト、フェデレーションカタログ、データ主権サービス、コンプライアンス）と、それらを利用するためのインターフェースとしての 1 つのコア機能（ポータルと API）で構成される。

ID とトラストは認証・認可、Verifiable Credential（以下、VC）[155]管理、Distributed ID（以下、DID）[156]管理及び VC を検証する役割を果たす。フェデレーションカタログは自己記述のスキーマ及び自己記述のインデックス付きストレージを提供し、プロバイダによって登録されたサービスオファリングの検索と取得を可能にする。データ主権サービスはユーセージコントロールを実現するデータコントラクトサービスとロギングサービスを提供することにより、参加者のデータ主権を実現する。コンプライアンスは参加者のオンボーディング及びサービス提供に関してセキュリティ、プライバシー、透明性、相互運用性等の観点でポリシー・ルールを順守させるために必要な監視機能等を提供する。ポータルと API は参加者のオンボーディング、サービス検出、オーケストレーション、サンプルサービスのプロビジョニング等を可能にする。

各コア機能の詳細については、それぞれ、「5.1.2 (2) ア ID とトラスト」、「5.1.2 (2) イ フェデレーションカタログ」、「5.1.2 (2) ウ データ主権サービス」、「5.1.2 (2) エ コンプライアンス」、「5.1.2 (2) オ ポータルと API」にて詳述する。

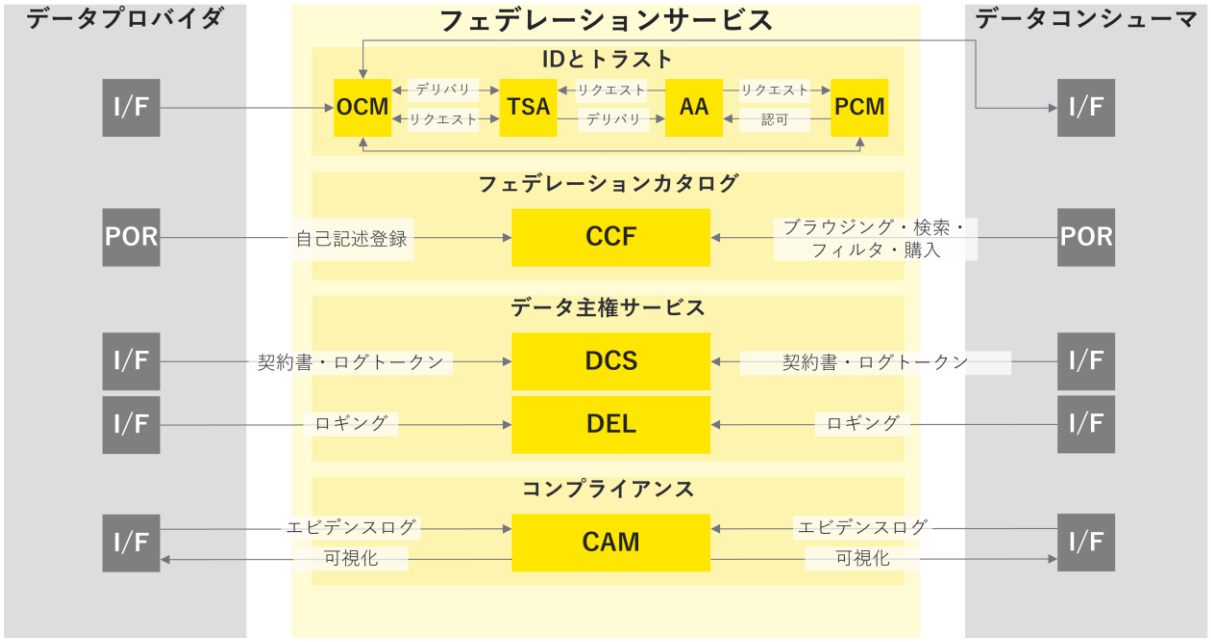
---

[154] Federation Service Specifications, Gaia-X Overview Specification Documents - DRAFT version 4b20f7c4, Gaia-X European Association for Data and Cloud AISBL, December 2021, https://Gaia-X.gitlab.io/technical-committee/federation-services/federation-service-specifications/ （2022 年 3 月 17 日アクセス）

[155] Verifiable Credentials Data Model v1.1, W3C Recommendation, March 2022, https://www.w3.org/TR/vc-data-model/ （2022 年 3 月 17 日アクセス）

[156] Decentralized Identifiers (DIDs) v1.0, W3C Recommendation, August 2021, https://w3c.github.io/did-core/ （2022 年 3 月 17 日アクセス）

図表 5-12 フェデレーションサービスの全体像（EY 作成）



ア ID とトラスト

まず、Gaia-X のフェデレーションサービスの主要コンポーネントの 1 つである ID とトラストについて説明する。ID とトラストは、主に ID とトラストフレームワークの 2 つに焦点が当てられている。ここで、ID とはアイデンティティの略語であり、任意のエンティティを表現する[157]。Gaia-X では、Self-Sovereign Identity（以下、SSI）の考え方に基づく分散型方式を採用する。この方式では、各 ID は、現在一般的に採用されている海外のクラウドプロバイダに依存するような中央集権的な方式ではなく、ユーザ自身によって分散的に管理される。

このような分散型方式において、ID はユニークな識別子と、対象のエンティティを一意に識別できる複数の属性から構成される。Gaia-X では識別子のユニーク性が重要視されている一方で、個人を特定できるような情報は ID に含まないことを前提とする。ID やそれに関する属性は Gaia-X によって直接管理されず、参加者自身で生成、管理することを想定している。また、このようにして生成された識別子は永久的に使用できる。なお、異なるエンティティに対して同一の識別を用いることはできない。

次に、Gaia-X におけるトラストフレームワークについて説明する。トラストフレームワークの目的は、全参加者の間でトラストを確立し、Gaia-X におけるサービスの提供と利用を促進することである。Gaia-X 参加者は AISBL が定めたルールに従い自分たちのトラストアンカーを選出することができる。トラストアンカーについては、「5.1.2（3）イ トラストアンカー」にて詳述する。電子署名等の信頼情報は証明書発行機関によって検証される必要がある。

上記のような ID とトラストのコア機能は、Authentication/Authorization（以下、AA）、Personal Credential Manager（以下、PCM）、Organization Credential Manager

[157] X.1252 : Baseline identity management terms and definitions, ITU, April 2021, https://www.itu.int/rec/T-REC-X.1252-202104-I/en （2022 年 3 月 17 日アクセス）

（以下、OCM）、Trust Services API（以下、TSA）の 4 つのコンポーネントによって実現される。AA の目的は Gaia-X の参加者が分散型の自己主権方式でユーザとシステムを認証し、ID データと分散管理された Credential 情報に基づいてアクセスやサービス利用の認可を保証することである。なお、Gaia-X における分散型 ID については、「5.3.2 (1) ア SSI と DIDs」にて詳述する。AA は OIDC（OpenID Connect）[158]互換のソフトウェア（Keycloak、Gluu、WSO2 等）と SSI を実現するモジュールとの統合を可能にする。

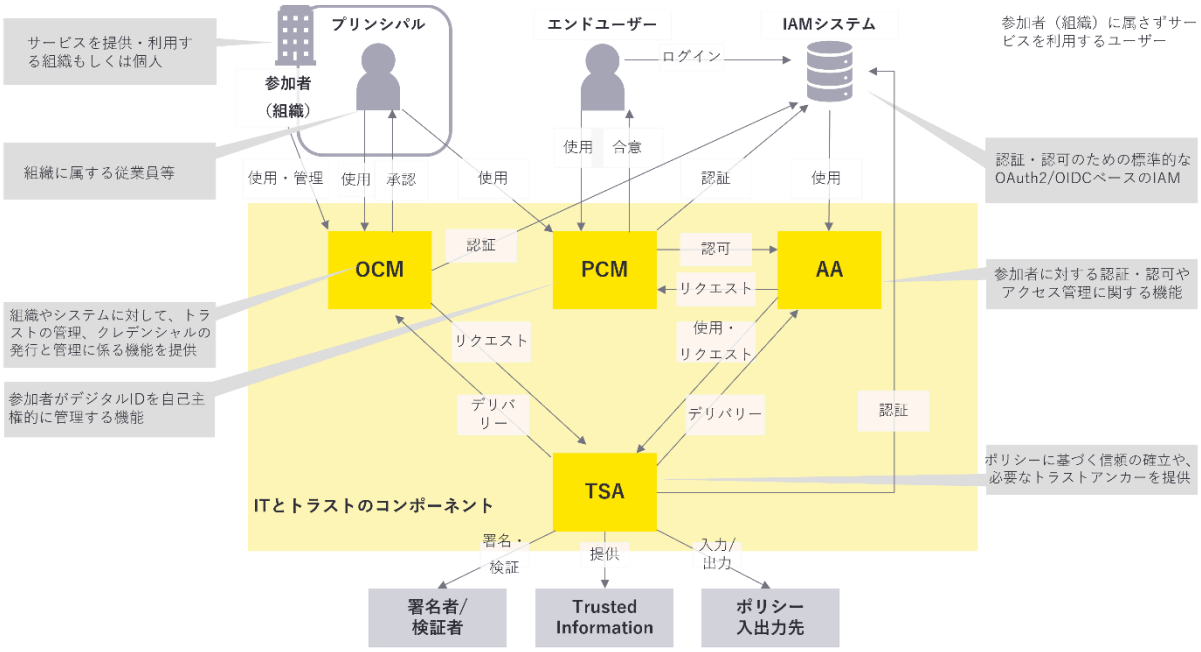
PCM は DID や VC を安全に保管し、認証やサービス利用のために必要な VC を提示するためのウォレットの役割を果たす機能であり、主な目的は他の参加者との信頼できる接続を確立することである。プリンシパルは PCM を用いることで VC を安全に保管することができる。ここで、プリンシパルとは、Gaia-X 参加者を代理して行動する自然人である。具体的には、参加者とは会社等の組織に該当し、プリンシパルはその組織に属する従業員が相当する。更に他のプリンシパル等から提示される VC の受領と管理もできる。

OCM は Gaia-X の SSI ベースのエコシステムで組織参加者のデジタル ID を管理するために必要な機能を提供する、異なる参加組織間の信頼できる接続を確立する目的として機能している。OCM により参加者及び組織は Credential の発行と保管が可能となる。OCM は ID に対応したデジタル署名を持つ VC を生成でき、参加者が有する VC に基づいて VC を発行することができる。

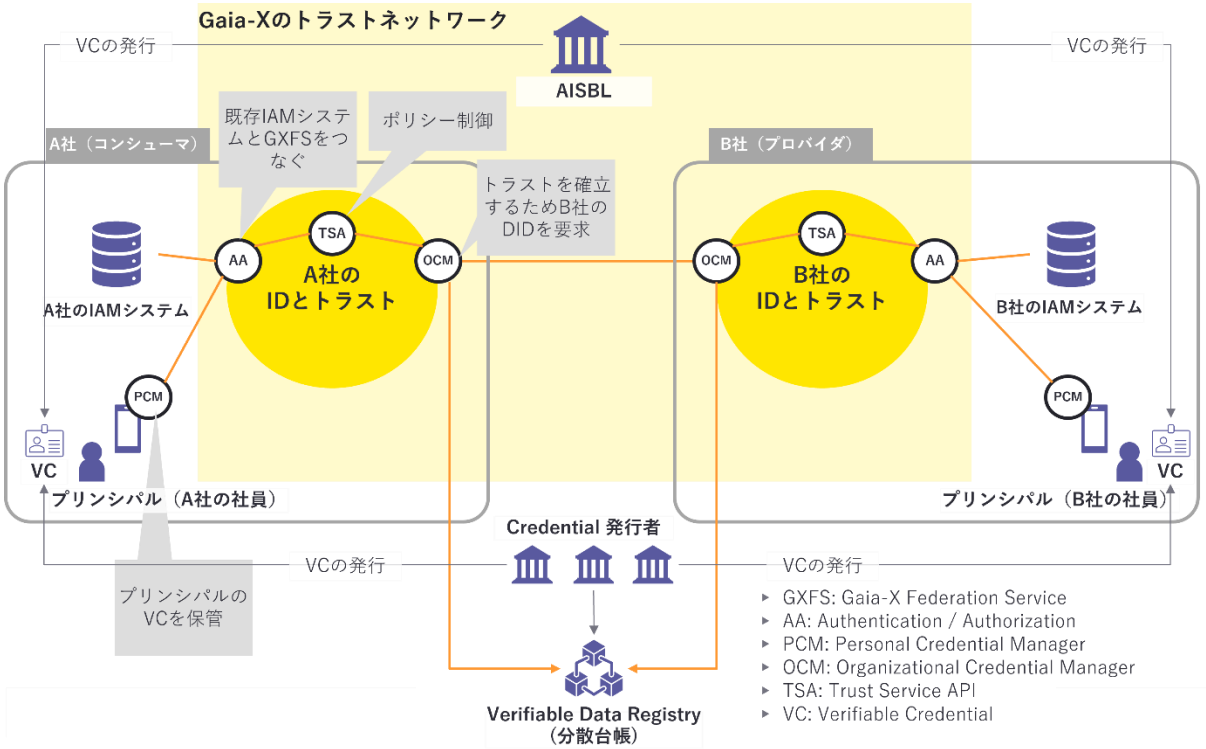
最後に、TSA について説明する。TSA はポリシー管理、評価、決定、情報の機能や、Gaia-X エコシステム内の全ての参加者とアセットがフェデレーションカタログに追加される際の署名検証プロセスのサポート機能を有する。TSA によるデジタル署名の検証やポリシーベースのトラスト確立を通じ、参加者間で一貫したレベルの信頼性を確保できる。

[158]OpenID Connect Core 1.0 incorporating errata set 1, OpenID, November 2014, https://openid.net/specs/openid-connect-core-1_0.html（2022 年 3 月 17 日アクセス）

図表 5-13 「Reference Document Identity and Access Management Gaia-X Community Document IAM」より EY 作成



図表 5-14 ID とトラストのコンポーネント連携図（EY 作成）



なお、ID とトラストにおいてベースとなっている分散型方式の認証・認可について、Gaia-X Workstream 2 Technical Implementation のコーディネータ及びフラウンホーファー研究機構の Head of Research Group Secure Data Ecosystems によると、図

表 5-14 のような分散型方式はあくまでも Gaia-X の理想であり、当面は中央集権的な ID 管理の方式を用いて運用することが想定されるとのことである。その際、ID とトラストで用いられるコンポーネントは Gaia-X AISBL によって管理される。本 Head へのインタビュー内容については「8.3 IDSA・Gaia-X に関するインタビュー結果」を参照されたい。

イ フェデレーションカタログ

次に、フェデレーションカタログについて説明する。フェデレーションカタログは各種リソース、サービスオファリング、参加者の特性及び一意な識別子を含む自己記述が公開されるデータカタログの機能を有する。なお、自己記述に含まれる内容や仕組みについては「5.1.2 (3) オ Gaia-X の自己記述」にて詳述する。

本コア機能により、プロバイダがフェデレーションカタログ上にデータリソースやサービスオファリングの自己記述を登録することや、コンシューマがフェデレーションカタログ上に公開されている自己記述を参照し、所望のサービスオファリングを検索すること等が可能となる。これらに加えて、プロバイダがカタログ上に登録した自己記述の公開範囲を制御する機能や、プロバイダによってサービスオファリングに含まれるポリシーやメタデータ等が変更された場合にコンシューマが通知を受けるモニタリング機能が含まれる。ユーザがフェデレーションカタログにアクセスする手段としては GUI を使用することを想定している。その際、バックエンド側では REST API によってカタログと対話する。

また、フェデレーションカタログは、トップレベルの分散カタログ、領域レベルの分散カタログと企業レベルの分散カタログの三つに分かれて運用されることを想定しており、各階層のフェデレーションカタログはカタログ間同期機能によって同期される。

フェデレーションカタログを実現するコンポーネントは Core Catalogue Function（以下、CCF）である。CCF は主に自己記述のストレージ、スキーマ管理機能、内部カタログ同期機能等から構成される。CCF の機能によってフェデレーションカタログに自己記述をレジストレーションすることが可能になる。

なお、Gaia-X Workstream 2 Technical Implementation のコーディネータ及びフラウンホーファー研究機構の Head of Research Group Secure Data Ecosystems によると、フェデレータカタログのカタログ間同期機能に関する具体的な仕様については現在検討中の段階であるが、全てのフェデレーションカタログにて同一の自己記述セットが格納されている状態が理想とのことである。

ウ データ主権サービス

次に、データ主権サービスについて説明する。データ主権サービスは、参加者のデータ交換、利用に係る自己決定権の保障を実現するためのサービスである。本コア機能によってコンシューマによるデータ利用に関する透明性と、データの利用に関する制御を行うユーセージコントロールが実現される。データ主権サービスは、従来のアクセスコントロールを拡張した既存のユーセージコントロールの概念を基礎としている。

参加者はデータ主権サービスを介さずにデータを取りすることも認められている。

データ主権サービスは、Data Contract Service（以下、DCS）と Data Exchange Logging Service（以下、DELS）の 2 つのコンポーネントで構成される。DCS はプロバイダとコンシューマ間の正式なデータ交換に係る契約の合意形成をサポートする機能である。DCS によって安全性、信頼性を保ち、監査可能な方法でデータの取引が可能になる。DCS では、プロバイダとコンシューマは相互に契約のオファーとカウンターオファーを送信し、契約に対して合意又は拒否することができる。

契約書は、ODRL（Open Digital Rights Language）をベースにしたフォーマットに準拠している。ODRL はコンテンツやサービスの利用に関する文章を表すためのインターオペラブルな情報モデル及びエンコード方式を提供する表現言語であり、W3C によって定義されている[159]。DCS は契約の締結時及び締結後に使用されることを想定しており、契約書発行と取得用の API エンドポイントをユーザに提供する。更に、DCS はユーザに対して、DELS のエビデンスログを参照する際に必要なログトークンを付与する。

ここで、ログトークンの具体的な内容は明らかにされていないが、エビデンスログを取得するための認可トークンに相当すると推測する。

次に、DELS について説明する。DELS によって、Gaia-X の運用上の問題特定や、不正取引の防止が可能になる。DELS によって記録されるエビデンスログは、コンシューマによるデータ利用費に関する清算や請求に必要な根拠資料としても使用できるのに加え、ユーザがユーセージポリシーに従っているか又は違反しているかについても追跡することができる。Gaia-X のエコシステムにおいて、DELS は主にデータの送信、受信とユーザ操作がユーセージポリシーに従っているかの 3 つの観点でログを記録する。ユーザは専用の UI を使用してログの通知確認や、エビデンスログの追跡機能を利用することができる。DELS のロギング機能の仕組みは W3C のリンクトデータ通知に準拠して規定されている。リンクトデータ通知は、アプリケーションがサーバにメッセージをプッシュする方法や、アプリケーションが通知を取得する方法を記述するプロトコルである[160]。

なお、フラウンホーファー研究機構の Head of Research Group Secure Data Ecosystems によると、データ主権サービスにおいて重要な役割を果たすユーセージポリシーを入力するタイミングは、プロバイダ及びコンシューマによる自身やリソースに紐づく自己記述の作成時であるとのことである。

エ コンプライアンス

Gaia-X は、行動規範、サードパーティによる証明書及び認証、利用規約の承諾という形でコンプライアンスの枠組みを定義している。本項目に関する詳細は、Policy Rules Document[161]に記載されている。データ暗号化・保護、相互運用性等のセキュリ

[159] ODRL Information Model 2.2, W3C Recommendation, February 2018, https://www.w3.org/TR/odrl-model/（2022 年 3 月 17 日アクセス）
[160] Linked Data Notifications, W3C Recommendation, May 2017, https://www.w3.org/TR/ldn/), （2022 年 3 月 17 日アクセス）
[161] Policy Rules Document, Policy Rules Committee Gaia-X AISBL, April 2021, https://www.Gaia-X.eu/sites/default/files/2021-05/Gaia-X_Policy%20Rules_Document_2104.pdf （2022 年 3 月 17 日アクセス）

ティに関する要件は、コンプライアンスフレームワークの基礎となっている。フェデレーションサービスとしてのコンプライアンスの主な目的は、Gaia-X ユーザにサービスオファリングのコンプライアンスに関する透明性を提供することである。フェデレーションサービスは、Onboarding and Accreditation Workflow（以下、OAW）と Continuous Automated Monitoring（以下、CAM）と Notarization API（以下、NOTAR）の 3 つのコンポーネントで構成される。

図表 5-15 コンプライアンスを構成するコンポーネント

コンポーネント	概要
OAW	Gaia-X の全ての参加者、リソース及びサービスオファリングがフェデレーションカタログに登録されるにあたって正当性の検証プロセスを受けることを保証する機能。検証プロセスの内容について「5.1.2 (3) ウ (ア)初期ルールセット」にて詳述する。
CAM	自己記述に基づくコンプライアンスのモニタリングを可能にする機能。
NOTAR	公証発行者が Gaia-X エコシステム参加希望者に対して VC を発行できるようにする機能。ここで、公証発行者とは Gaia-X AISBL によって参加希望者への VC 発行が許可された組織を指す。

なお、Gaia-X Workstream 2 Technical Implementation のコーディネータ及びフラウンホーファー研究機構の Head of Research Group Secure Data Ecosystems によると、OAW は GUI ベースの Web システムとして実装される可能性が高いとのことである。また、CAM による監視機能ついては完全に自動化される想定である一方、OAW によるオンボーディングは一部マニュアルで行われる想定である。

オ ポータルと API

Gaia-X ポータルは、参加者がユーザインターフェース及び API を通じてフェデレーションサービスの各コンポーネントを利用することを可能にする。特定のドメインに特化したエコシステムでフェデレーションサービスを使用する場合、ポータルと API の OSS を拡張して、独自にカスタマイズしたポータルをデプロイすることも可能である。ポータルで実現される一部の機能について下記にて説明する。

- 新規参加者としての組織の登録をサポートする
- Gaia-X AISBL のメンバーとしての参加を希望する組織をサポートする
- 参加者は、自己記述、Credential を管理・変更できる
- フェデレーションカタログに基づき、サービスオファリングと参加者の検索とフィルタリング機能を提供する
- 複数のサービスオファリングを選択し、一つのソリューションパッケージとしてエンドユーザに公開するための機能を提供する。

上記機能を実現するコンポーネントとして、PORTAL（以下、POR）が定義されている

また、様々な API をオーケストレーションするために、API フレームワークが導入

され、API アクセスとライフサイクルのための Orchestrator（以下、ORC）が提供される。ORC は、サービスのインスタンス化と管理を担当する。例えば、参加者が特定のサービスオファリングを選択した後、当該サービスオファリングに対応するサービスインスタンスのデプロイ等をサポートする。API ゲートウェイは、全てのサービスのセキュリティを確保する。ここで、API ゲートウェイは、フェデレーションサービスとして提供される REST API のエンドポイントに HTTP/HTTPS でアクセスする際に共通的に通過するリバースプロキシに相当すると考えられる。最後に、API ポータルは、利用可能な API サービスやバージョン管理に関する情報の一元化を実現する。

(3) 運用モデル

Gaia-X は、高度に規制された市場の企業や、中小企業から大企業まで幅広く採用され、持続可能かつスケーラブルなエコシステムであるための運用モデルが必要である。なお、本章における説明は Gaia-X Architecture Document の第 4 章「Gaia-X Operating Model」を参照している。

上記の目的を達成するための CSF（Critical Success Factors）として、以下の点が挙げられている。

- 運用モデルは、全ての参加者に明確な付加価値を提供するものでなければならない。
- 運用モデルは、説明責任、透明性のあるガバナンス、信頼モデルを有していなければならない。
- 全ての参加者にとって使いやすい運用モデルであること。
- Gaia-X エコシステムが、経済的に持続可能な運用モデルであること。
- 環境面でも持続可能な運用モデルであること。

ア Gaia-X エコシステムと Gaia-X エコシステムの拡張

Gaia-X 参加者は、カスタムポリシールールのもと、特定の種類のサービスについては多くの他の参加者と同時に提供又は利用したいと考える一方で、あるサービスに関しては特定の参加者間のみで提供及び利用したいと考える可能性がある。このようなモチベーションから、1 つのグローバルなエコシステムに加えて、参加者が個別にエコシステムを構築するケースが想定される。参加者が個別のエコシステムを構築する具体的な理由は、(1)特定のエコシステムに限り自己記述を公開するため、(2)Gaia-X 準拠のカスタムトラストアンカーを使用するためである。

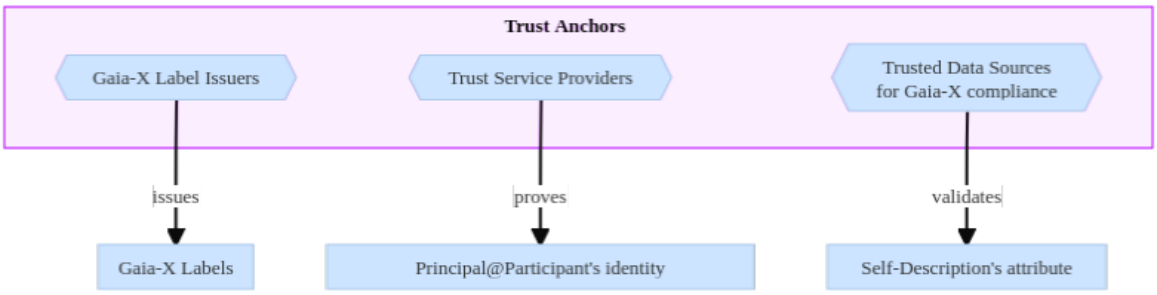
イ トラストアンカー

トラストアンカーは、証明書チェーンにおいて、Gaia-X の全ての参加者が信頼できると判断する存在である。個々のエコシステムは独自のトラストアンカーを選出することができるが、エコシステム間でトラストを確立するためには、独自のトラストアンカーが少なくとも Gaia-X エコシステムのトラストアンカーが遵守すべきルールに準拠している必要があり、そのようなルールに関して Gaia-X AISBL は以下の 3 項目を定義する。

- トラストアンカーを定義するためのルールセット
  - トラストサービスプロバイダ
  - Gaia-X Label 発行者
  - Gaia-X 準拠のための信頼できるデータソース
- 自己記述の形式とコンプライアンスルール
- Gaia-X Labels ルールブック

トラストアンカーは、図表 5-16 に示されるように、Gaia-X AISBL によって定義された 3 項目に従って Gaia-X ラベルの発行や、自己記述の属性の検証を行わなければならない。

図表 5-16 トラストアンカーが遵守すべきルール



参加者によって選出されたトラストアンカーの正当性を確認するため、Gaia-X AISBL が定義したルールセットを検証する仕組みが実装される想定である。また 2022 年 3 月時点で参加者によるトラストアンカーの具体的な選出方法について明らかになっていない。

ウ Gaia-X のコンプライアンス

Gaia-X におけるコンプライアンスは、ルールセットを実行するプロセスとして定義される。ルールセットとは、Gaia-X の Compliance Service によって自動的に実行される自己記述の互換性検証プロセスに用いられるルールであると考えられる。下記のような項目が互換性チェックの主な観点として挙げられる。

- シリアライゼーションフォーマットとシンタックスの検証
- 暗号署名の検証
- 属性値の一貫性
- 属性値の検証

自己記述の属性値の検証は、公開されているオープンデータを用いて検証するか、トラストアンカーが提供するデータを用いて行われる。

コンプライアンスのルールセットバージョン管理されており、法的要件等に適応するため、適宜アップデートされる想定である。Gaia-X は、自己記述の FAIR ナレッジグラフを作成することにより、高度なクエリ検索を実現しようとしている。FAIR とは、データを「Findable（発見できる）」、「Accessible（アクセスできる）」、「Interoperable

（相互運用できる）」、「Reusable（再利用できる）」ようにするための原則を指し、2016年3月に「Scientific Data」ジャーナルにて定義された[162]。コンプライアンスの「Set of Rules」は OSS として実装され、本 OSS がデプロイされるサービスインスタンスは Gaia-X Compliance Service と呼ばれる。Gaia-X Compliance Service は OSS として、Gaia-X エコシステム以外のエコシステムにおけるデータカタログに組み込めるようにすることを想定している。

（ア）初期ルールセット

Gaia-X の Compliance Service にて自動的に検証されるルールセットの一例を図表 5-17 に示す。

図表 5-17 Compliance Service で検証されるルールセット

ルール	検証内容
シリアライゼーションフォーマットとシンタックスの検証	• 自己記述文は、成型の JSON-LD としてパースされた状態である必要がある。シリアライゼーションによって定義された RDF（Resource Description Framework）グラフは、Gaia-X によって定義された SHACL 形式に対して検証されなければならない。SHACL は、W3C によって定義されている、RDF グラフの制約を記述する言語である[163]。 • すべての欧州のプロバイダは、欧州委員会施行規則（EU）2015/884 の第 8 項[164]に規定される ISO 6523[165]に準拠する自社の EUID を明記するものとする。
暗号署名の検証	• サービスプロバイダの身元は、Gaia-X が承認したいずれかのトラストサービスプロバイダによって検証されなければならない。 • すべての自己記述の必須属性の署名は、少なくとも 1 つのトラストアンカーをルート認証局としなければならない。
属性値の一貫性	• service.jurisdiction 属性の値は service.provided_by.location 属性と一致する必要がある。 • service.jurisdiction 属性の値は、利用規約文書の service.terms_and_conditions 属性の準拠法と一致する必要がある。
属性値の検証	• GDPR 準拠の値は、CISPE（Cloud Infrastructure Services Providers in Europe）や EU Cloud COC（EU Code of Conduct for Cloud Service Provider）等、EDPB（European Data

[162] The FAIR Guiding Principles for scientific data management and stewardship, scientific data, March 2016, https://www.nature.com/articles/sdata201618 （2022 年 3 月 17 日アクセス）
[163] Shapes Constraint Language, W3C Recommendation, July 2017, https://www.w3.org/TR/shacl/ （2022 年 3 月 17 日アクセス）
[164] COMMISSION IMPLEMENTING REGULATION (EU) 2015/884, An official website of the European Union, June 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2015.144.01.0001.01.ENG, （2022 年 3 月 17 日アクセス）
[165] ISO/IEC 6523-1:1998, ISO, December 1998, https://www.iso.org/standard/25773.html, （2022 年 3 月 17 日アクセス）

ルール	検証内容
	Protection Board）が承認した行動規範のいずれかに準拠するものである必要がある。 • European Cybersecurity Certification Scheme for Cloud Services（EUCS）への準拠は、Cloud Computing Compliance Criteria Catalogue（C5）や SecNumCloud[166]等、ENISA が認定したスキームのいずれかによるものでなければならない。

（イ）「Trusted data sources」の活用

「自己記述」に関する正当性の検証にはコストがかかることが予想される。後述の「5.1.2 (3) カ 分散型・自律エコシステム」では、フェデレーションサービスの運営コストの対応案が示されている。

エ Gaia-X のラベル

コンプライアンスとラベリングのフレームワークは、Gaia-X アーキテクチャの必須コンポーネントであり、Gaia-X サービスのコントロールとガバナンスにおいて重要である。Gaia-X におけるラベルは参加者やデータアセット等のエンティティに紐づく自己記述の中の VC として格納され、Gaia-X は、特定のラベルとして指定された VC のフォーマットを検証する。一方で、政府、産業界、標準化団体等の外部団体は、領域固有のラベルを定義することができる。Gaia-X のコンプライアンスとラベリングのフレームワークは、あらゆるエンティティが望むレベルの信頼を得るために定義する、特定の要件に対応することができる。コンプライアンスとラベルによって付与される VC は発行者主体が異なる。コンプライアンスでは Gaia-X コンプライアンスサービスによって発行されるのに対し、ラベリングでは特定の業界や団体等によって発行される。また、コンプライアンスによる VC は Gaia-X エコシステムに参加する全てのエンティティに対して発行される必要があるが、ラベルはサービスオファリングに限定される点も特徴的である。

オ Gaia-X の自己記述

Gaia-X における自己記述により、プロバイダ、コンシューマ等の Gaia-X エコシステム上のエンティティをマシンリーダブルな形式で記述することができる。自己記述は、リソーステンプレート、リソース、サービスオファリング、参加者の一意な識別と紐づいており、それぞれの特徴を表現する。一般的に、自己記述はプロバイダによって作成される。図表 5-18 は、自己記述の目的及び特徴を示している。

[166] PRESTATAIRES DE SERVICE D'INFORMATIQUE EN NUAGE (SECNUMCLOUD), National Agency for the Security of Information Systems, https://www.ssi.gouv.fr/entreprise/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-service-dinformatique-en-nuage-secnumcloud/ （2022 年 3 月 17 日アクセス）

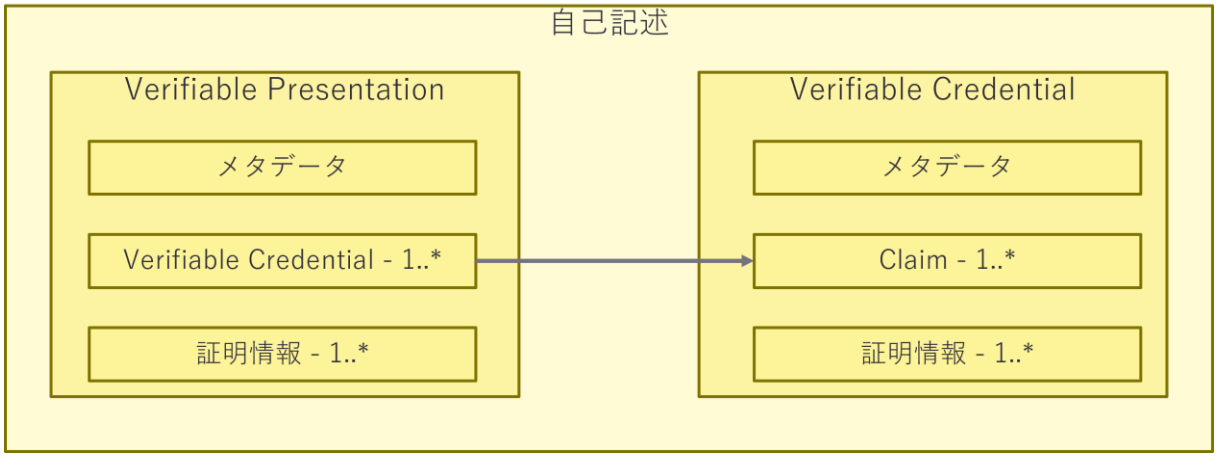
図表 5-18 自己記述の目的と特徴

項目	説明
目的	• カタログに記載されたサービス提供の発見と構成 • サービスインスタンスとリソースの評価、選択、統合、オーケストレーションのツール支援 • 使用ポリシーに沿った施行、継続的検証、信頼性監視 • サービス提供のリソースと参加者に関する契約条項の交渉
特徴	• マシンリーダブル • 特定の技術に依存しない • オントロジーと検証ルールを持つスキーマに準拠 • フォーマット、構造、含まれる表現（セマンティクス）の面で標準に準拠した相互運用性 • 新しいプロパティを簡単に追加できる柔軟性、拡張性 • 分散化された方式でどこからでも閲覧・参照可能 • 証明書や署名等を添付し、安全かつ検証可能な情報を提供することによる信頼性の向上

自己記述には、図表 5-19 に示すように、アセット、リソース又は参加者の識別子、メタデータ及び 1 つ又は複数の Verifiable Credential（以下、VC）が含まれる。VC には、サブジェクト、プロパティ、値で構成される複数の Claim[167]が含まれる。ここで、Claim とは身分を証明する個々の情報を表しており、運転免許証であれば住所や生年月日等が相当する。各 VC のメタデータは、発行タイムスタンプ、有効期限、発行者リファレンス等を含む。各 VC には、信頼できる第三者機関による署名を付与することができる。W3C が定義する Verifiable Credentials の Data Model は、JSON-LD[168]を使用して VC と Claim を表現する技術標準である。対象の参加者、もしくはリソース等に複数の VC が紐づく場合、これらの VC は一つの Verifiable Presentation（以下、VP）[169]にバンドルされる。具体的には、プロバイダ自身によって発行され署名された VC と、独立した外部機関によって提供される証明書等の VC が一つのリソースに紐づくケース等が該当する。

[167] Verifiable Credentials Data Model v1.1 Claims, W3C Recommendation, March 2022, https://www.w3.org/TR/vc-data-model/#claims（2022 年 3 月 28 日アクセス）
[168] JSON-LD, W3C Recommendation, https://www.w3.org/TR/json-ld11/（2022 年 3 月 28 日アクセス）
[169] Verifiable Credentials Data Model v1.1 Presentation, W3C Recommendation, March 2022, https://www.w3.org/TR/vc-data-model/#presentations（2022 年 3 月 28 日アクセス）

図表 5-19 自己記述の構成



あるエンティティの自己記述は、その識別子によって別のエンティティを参照することができる。Gaia-X において識別子として採用されている仕様は RFC3986 で定義されている URI である。Gaia-X では、一つの識別子が複数のエンティティを参照しないことを前提としているが、 同じエンティティを参照する複数の識別子存在する可能性はある。しかしながら、このような識別子を複数生成することは推奨しない。また、URI のプレフィックスによって識別子の一意性を確保することが可能である。例えば、ドメインを識別子の一部として使用する場合、当該ドメインの所有者のみが識別子を作成することができる。

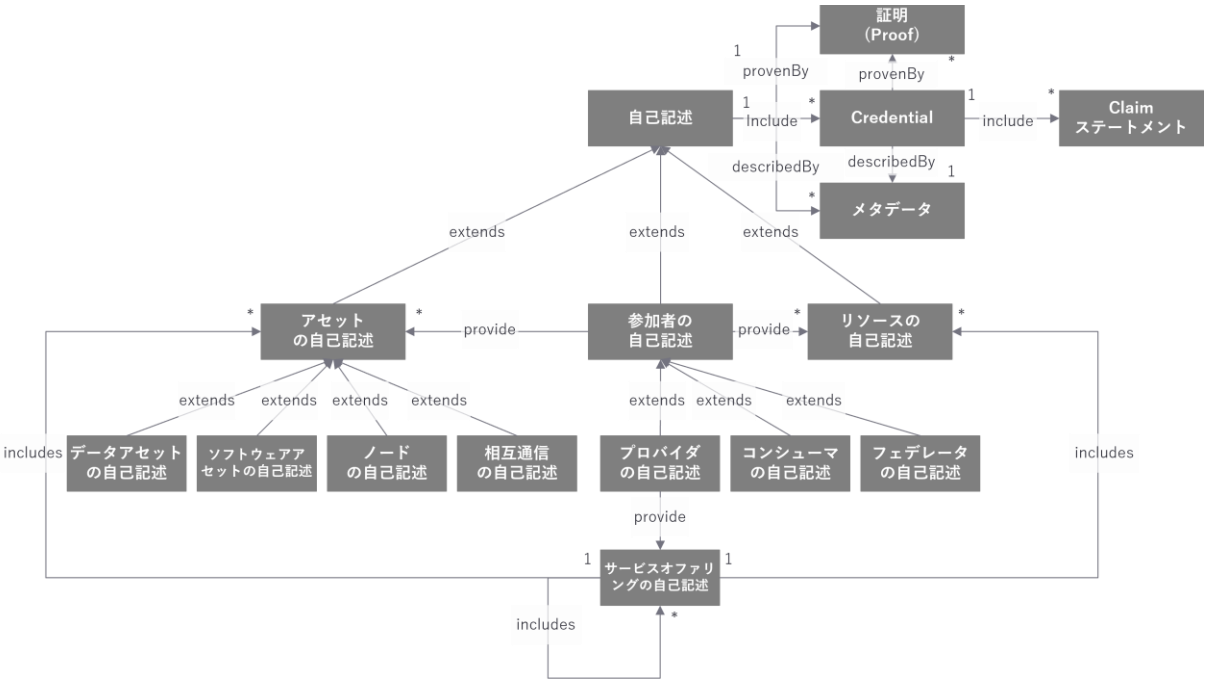
自己記述間の関係はグラフ構造で表現することができ、これを自己記述グラフと呼ぶ。フェデレーションカタログは、コンシューマが所望のサービスオファリングを効率的に検索できるようにするため、自己記述グラフ上でクエリアルゴリズムを実装している。さらに、グラフ構造によって個々の自己記述からは判断できないユーセージポリシーを表現することができる。例えば、あるコンシューマはフェデレータカタログを利用してあるサービスインスタンスが、コンシューマが指定した許容国以外のノードにデプロイされた他のサービスインスタンスに依存できないように要求することができる。

Gaia-X における自己記述は、相互運用性を高めるために、自己記述スキーマが定義されている。自己記述スキーマはクラスの概念を導入し、拡張することが可能である。各クラスには、そのクラスのインスタンスが持つことのできるプロパティが定義されている。このようなプロパティは、（1）データ型のリテラル値（W3C Web Ontology Language OWL では「データ型プロパティ」）、（2）補助クラスのインスタンス値（例えば、サービスデプロイに関連するすべての情報をグラフ内の単一のノードとしてグループ化するクラス）、（3）コントロールボキャブラリーの概念のインスタンスであり再利用できる値の 3 つの属性が含まれる。

プロパティには関係も含まれ、Gaia-X Conceptual model の他のクラスのインスタンスである値を持つ（例えば、アセットとそのプロバイダの関係、これも OWL オブジェクトプロパティである）。自己記述スキーマには、ある自己記述が特定のクラスとプロパティに従っているかどうかを検証するために使用される条件セットが存在する。この条件セットは、特定のクラスにおいて必須となるプロパティを指定している。自己記述では、このようにして指定されたプロパティ及びリレーションのみが使用されるべきである。

コア自己記述スキーマとは、「5.1.2 (1) 前提事項」にて示されている Gaia-X に登場するエンティティやリソース等とそれらの関係に基づいて定義された、ベースとなる自己記述スキーマである。図表 5-20 は、コア自己記述スキーマの継承関係を示している。個々の Gaia-X エコシステムは、ドメイン固有の要件に合わせてコア自己記述スキーマを拡張することができる。

図表 5-20 「コア自己記述スキーマの継承関係」より EY 作成



自己記述の技術的な仕様は、RDF グラフデータモデルの JSON-LD シリアライゼーションにおける W3C VP に準拠する。参加者はフェデレーションカタログに自己記述を登録する前に、Gaia-X に準拠した自己記述書を Gaia-X コンプライアンスサービスに提示しなければならない。Gaia-X コンプライアンスサービスは、提示された自己記述の形式等をチェックし、自己記述に挿入可能な VC を発行する。コンプライアンスサービスは、「5.1.2 (2) エ コンプライアンス」にて詳述している。

自己記述が無効となる 3 つの状態を図表 5-21 に示す。

図表 5-21 自己記述が無効となる状態

ステータス	説明
End-of-Life	有効期限の超過を指す。(暗号署名の有効期限等)
Deprecated	新しい自己記述への置き換え
Revoked	不正確又は不正な内容を含んでおり、元の発行者又は信頼できる当事者によって無効化されるケース。

カ 分散型・自律エコシステム

Gaia-X エコシステムは、DAO（Decentralized Autonomous Organization）[170]の原則に従い、以下のような特徴を持つ分散型自律エコシステムの創出を目指している。

- コンプライアンスは、自動的に適用されるポリシー・ルールによって達成され、コミュニティのメンバーは共通の目的を達成するためのインセンティブを与えられる。
- 中央集権的なガバナンスを最小化することで、責任追及と規制の取り込みを最小化する。
- エコシステムは、自己資金の管理を含む独自のルールを持つ。
- エコシステムの参加者によって運営される。

（ア）Gaia-X Registry

Gaia-X Registry は、分散型インフラとコード実行の自動化機能を備えた、パブリックな分散型、不変性、パーミッションレスのデータベースである。Gaia-X レジストリはエコシステムにおけるガバナンスを強化するために重要であり、以下のような情報を格納している。

- トラストアンカーの指名について
- トラストアンカー検証プロセスの結果
- トラストアンカーのアイデンティティの失効の可能性
- 欧州議会のプレナリーのルールと同様の、Gaia-X Association の点呼による投票とその結果
- Gaia-X で定義された自己記述スキーマの URL
- カタログの自己記述の URL

また、下記のような機能のプロビジョニングを容易化する。

- スマートコントラクト機能を持つ分散型ネットワークである
- 完全性、非否認性、機密性を保証する投票メカニズム
- Gaia-X Compliance Service のインスタンスへのアクセス
- 完全に動作し、分散化され、簡単に検索できるカタログ
- Gaia-X の会員規約に違反する参加者の ID 及び自己記述 URL リスト。このリストは、すべての Gaia-X Trusted Catalogue プロバイダが、不適切なコンテンツをフィルタリングするために使用しなければならない。
- Gaia-X Ecosystem の運営コストをカバーするためのトークン。Gaia-X AISBL のメンバーのためにトークンを発行することが検討されている。本トークンに関する説明を含む Gaia-X ビジネスモデルを説明するドキュメントは、2021 年第 4 四半期にリリースされる予定である[171]。

Gaia-X Registry の各エントリは、1 つのトランザクションとしてみなされる。トランザクションには、そのトランザクションに関与する全てのステークホルダの DID と、トランザクションに関するメタデータが含まれている。トランザクショ

---

[170] Tokenized Networks: What is a DAO?, Blockchain Hub, July 2019, https://blockchainhub.net/dao-decentralized-autonomous-organization/ （2022 年 3 月 17 日アクセス）

[171] 2022 年 3 月 18 日時点でビジネスモデルに関するドキュメントのリリースは確認されていない。

ンに含まれる全ての DID がルート認証局であるトラストアンカーまで辿ることができる場合、当該トランザクションは有効であるとみなされる。また、Gaia-X Registry は、失効したトラストアンカーを記録している。

このモデルにより、参加者は Gaia-X エコシステムの中で活動し、自律的に情報を登録し、他の参加者が検証可能な情報にアクセスすることができる。

5.1.3 IDS・Gaia-X の関係

(1) Gaia-X への IDS コンポーネントのマッピング

「3.2.1 (3) Gaia-X との関係性」で述べた通り、IDS は Gaia-X のイネーブラーであると主張しており、IDS と Gaia-X との技術的な関連性については、GAIA-X and IDS[172] にて示されている。以下、同ドキュメントの内容を中心に、Gaia-X と IDS のコンポーネント間の対応関係について概説する。

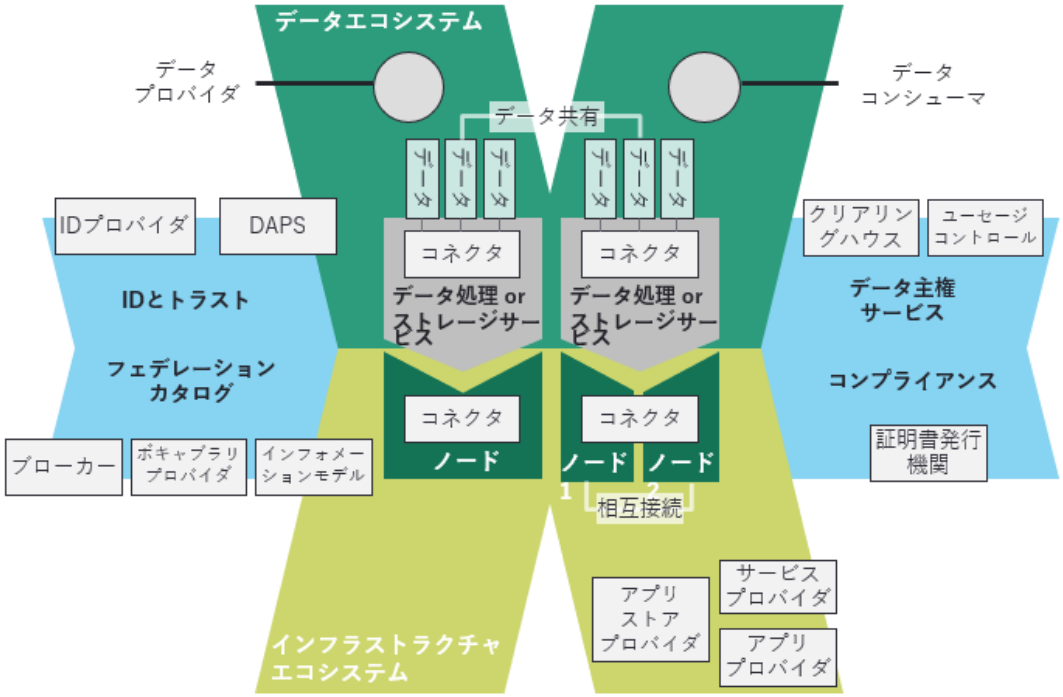
Gaia-X と IDS は、相互に連携可能なエコシステムにおいて、エンドツーエンドのデータバリューチェーンのためのクラウドとデータ主権を確保するため、補完関係になりうる。

図表 5-22 は、IDS のコンポーネントを Gaia-X のアーキテクチャにマッピングしたものである。データプロバイダとデータコンシューマは Gaia-X データエコシステムにマッピングされ、アプリストアプロバイダ、アプリプロバイダ、サービスプロバイダは Gaia-X インフラストラクチャエコシステムに配置される。 IDS コネクタはセキュアゲートウェイとして機能するため、Gaia-X ノードに統合することができる。ここで重要なのは、コネクタは Gaia-X データエコシステムに限定されず、セキュリティ上の理由から Gaia-X インフラストラクチャエコシステムを含む全体に及ぶということである。

Gaia-X のフェデレーションサービス（ID とトラスト、データ主権サービス、フェデレーションカタログ、コンプライアンス）は、様々な IDS のコンセプトにも合致している。重要な要素は Gaia-X フェデレーションカタログであり、これは IDS ではブローカー、ボキャブラリプロバイダ、IDS インフォメーションモデルに対応している。データ主権サービスのコンポーネントは、IDS ではクリアリングハウスとユーセージコントロールのコンセプトで表現されている。さらに、ID とトラスト及びコンプライアンスは、IDS による ID プロバイダ（CA、DAPS、ParIS 等）と証明書発行機関を利用することができる。

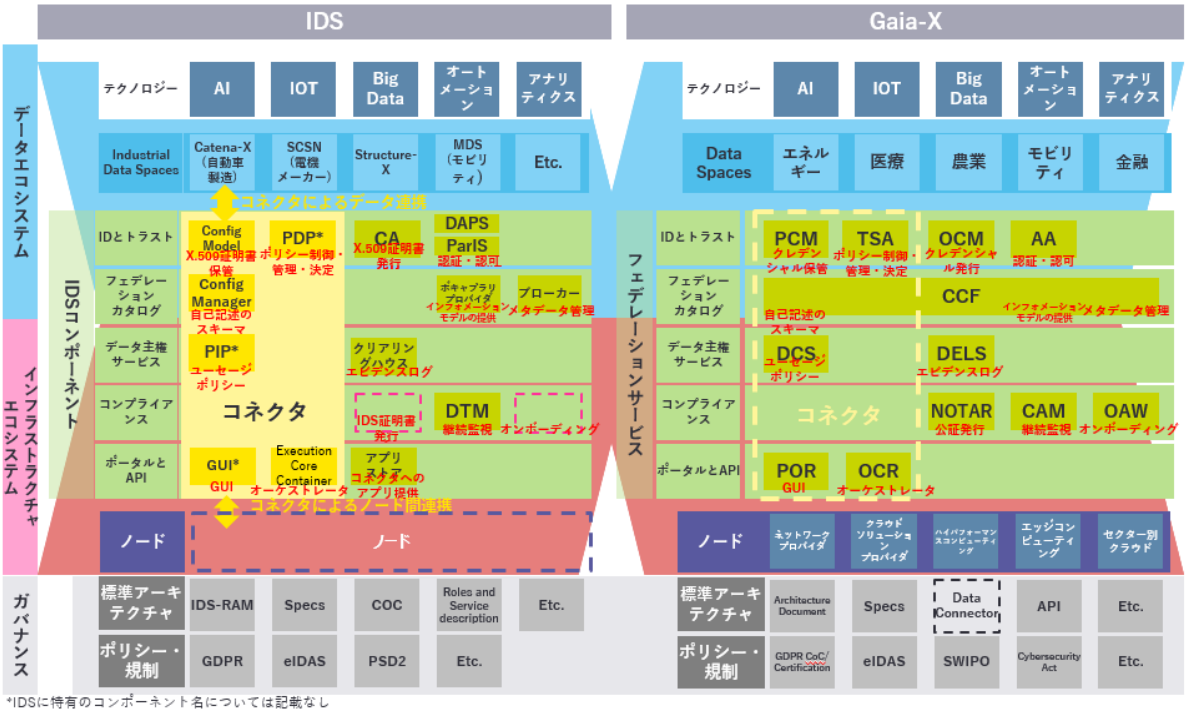
[172] *GAIA-X and IDS 1.0*, INTERNATIONAL DATA SPACES ASSOCIATION, January 2021, https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-Position-Paper-GAIA-X-and-IDS.pdf（2022 年 3 月 17 日アクセス）

図表 5-22 IDS コンポーネントの Gaia-X アーキテクチャへのマッピング
（「GAIA-X and IDS」より EY 作成）



上記のコンポーネント間の関係性を踏まえ、図表 5-23 は、IDS と Gaia-X のコンポーネント間の対応関係について示したものである。

図表 5-23 IDS における機能と Gaia-X における機能の比較（再掲）



(2) IDS・Gaia-X アーキテクチャの共通点及び相違点

本節の記載内容に基づいて、IDS・Gaia-X のアーキテクチャに関する両者の共通点及び相違点を列挙すると、図表 5-24 の通りとなる。

図表 5-24 IDS・Gaia-X アーキテクチャの共通点及び相違点

比較項目			IDS	Gaia-X
Lv1	Lv2	Lv3		
ID とトラスト	デジタル ID		中央集権型 ID を採用[173]	分散型 ID を採用
	証明書発行		X.509 証明書を採用	VC を採用
フェデレーションカタログ	自己記述	特性	• マシンリーダブルであること • 相互運用性が担保されていること	
		データアプリ	IDS コネクタ上に実装することを想定	クラウド全体に接続されたノード上にデプロイすることを想定
		インフォメーションモデル	OWL 機能の使用が制限された単純なオントロジー	グラフ構造に基づくクエリアルゴリズムを想定した階層化情報
データ主権サービス	ユーセージコントロール		ヒューマンリーダブルなポリシーとマシンリーダブルな技術的なポリシーの 2 軸を考慮	
コンプライアンス	モニタリング		技術的なエビデンスを収集し、ユーセージポリシーやセキュリティ要件等に準拠しているか評価	技術的なエビデンスを収集し、コンプライアンスに準拠するか評価

[173] なお、EDC は自身の特徴の一つとして複数の ID プロバイダ（Web DID、OAuth2、ION/Blockchain 等）をサポートすることが可能であることを挙げていることから（「26.1.8 (1) コネクタの特徴（Eclipse Dataspace Connector を中心に）」）、将来的には分散型 ID も想定していることが推察される。

5.2 プロセスの観点

5.2.1 IDS におけるプロセス

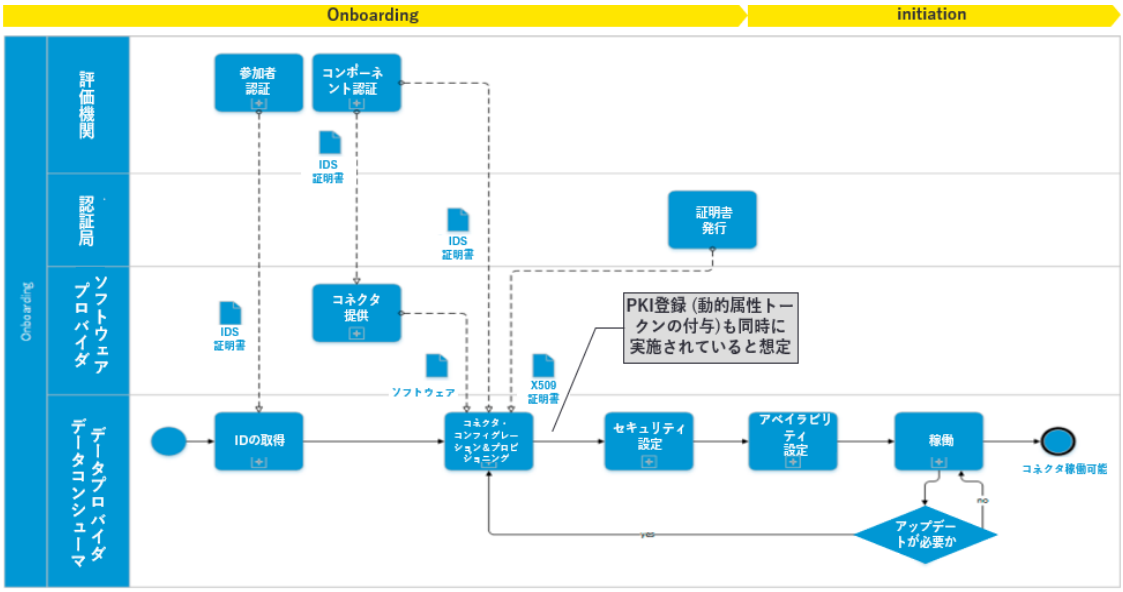
Gaia-X と同様、IDS におけるプロセスにおいても、参加を希望する組織は証明書発行機関や評価機関による認証プロセスを受ける必要がある（=オンボーディング）。その後、参加者はコネクタに関する初期設定を行うことで(=イニシエーション)、IDS のデータスペースへのアクセスが可能となる。参加者は、IDS のデータスペースでデータ交換を行うが（=データ送受信）、その際にデータコンシューマは目的に合ったデータを提供しているデータプロバイダを検索し、データプロバイダとの間でユーセージポリシーに関する合意を得る必要がある。データの送受信を行った履歴は取引ログとして記録・保存され、将来の取引時の認可プロセスの際に参照されることとなる （=データ利用時）。IDS におけるプロセスにおいては、退会時のルールに関するフローは明らかにされていない。

なお、同項の記載は、主に IDS リファレンスアーキテクチャモデルの「3.3 PROCESS LAYER」に基づくものである[174]。コネクタを中心とするインタラクションを時系列で示すという趣旨で、図表 5-1 に基づいて対応箇所を示している。各コンポーネントの機能詳細については、「6.1 IDS コンポーネント」の各コンポーネントの詳細を確認されたい。

(1) オンボーディング

IDS に参加を希望する組織のオンボーディングプロセスについて説明する。オンボーディングプロセスの概要に関するフロー図は、図表 5-25 の通りである。

図表 5-25 オンボーディングプロセス
（「IDS Reference Architecture Model 」より EY 作成）



[174] *REFERENCE ARCHITECTURE MODEL 3.0*, INTERNATIONAL DATA SPACES ASSOCIATION, December 2020, p33-38, https://internationaldataspaces.org/wp-content/uploads/IDS-Reference-Architecture-Model-3.0-2019.pdf（2022 年 3 月 17 日アクセス）

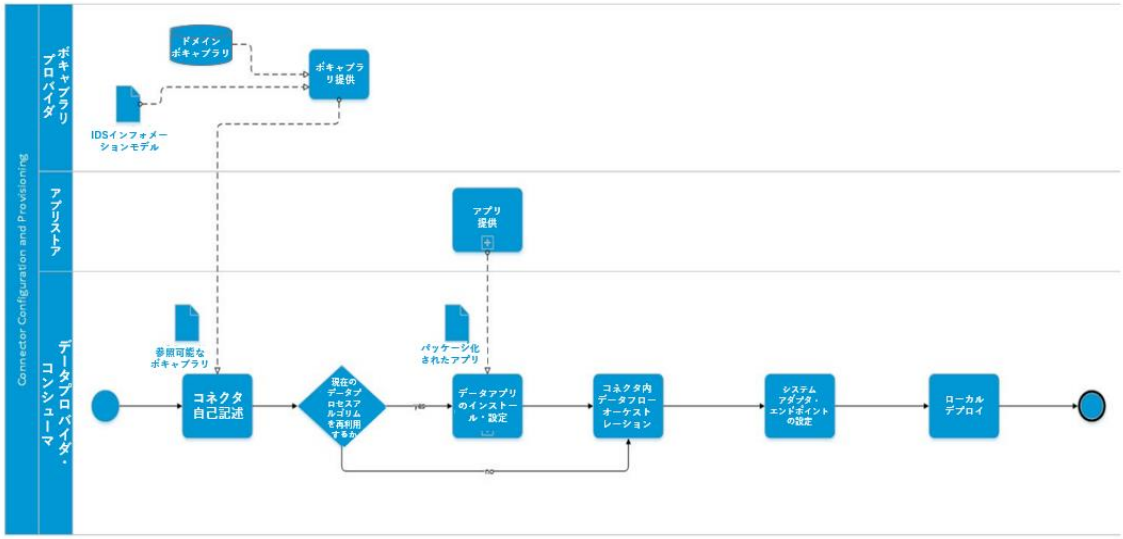
オンボーディングプロセスは、①IDS への参加又はコンポーネントの提供を希望する組織が評価機関から認証を受けて IDS 証明書を取得すること、②認証局（CA）から X.509 証明書の発行を受けること、③コネクタの初期設定を行うこと、の 3 つのステップに大別される。

認証プロセスを経て、参加者には IDS 証明書が発行され、続けて認証局（CA）から電子証明書（X.509 証明書等）の発行と IDS-ID の付与を受ける。認証局は、電子証明書を発行する信頼できる第三者機関であり、発行された証明書を検証するサービスをホストすることができる。

続けて、データプロバイダ及びデータコンシューマは、コネクタの初期設定やセキュリティ設定を行う。このプロセスは、コネクタコンフィギュレーション＆プロビジョニングとセキュリティ設定から構成される。

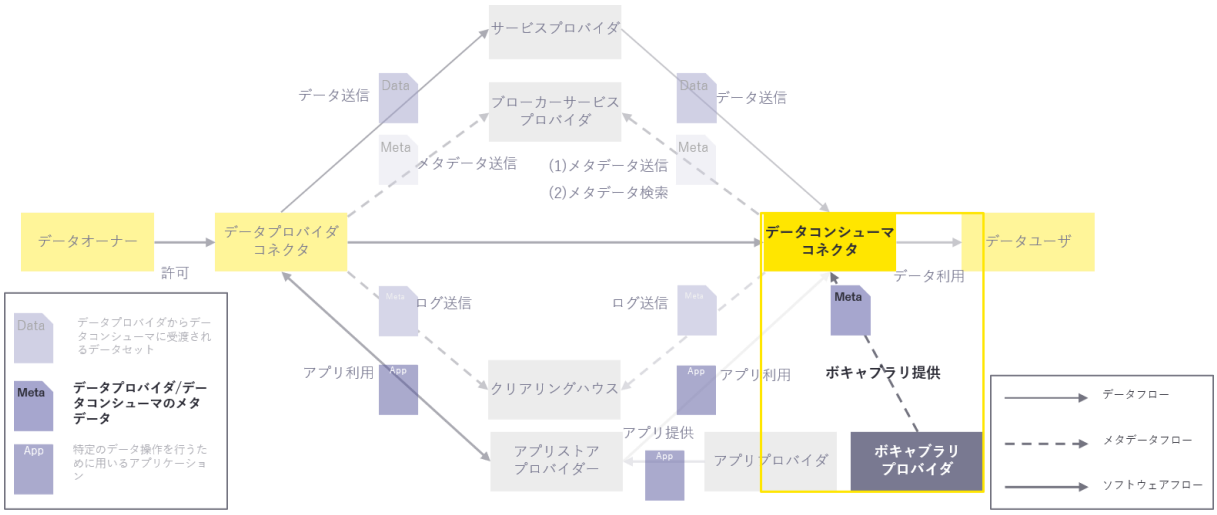
コネクタコンフィギュレーション＆プロビジョニングの詳細フローについては、図表 5-26 の通りである。

図表 5-26 コネクタコンフィギュレーション＆プロビジョニングサブプロセス
（「IDS Reference Architecture Model 」より EY 作成）



データコンシューマ及びデータプロバイダは、ボキャブラリプロバイダからメタデータで提供されるボキャブラリを参照し、コネクタの自己記述を行う。ボキャブラリプロバイダは、IDS インフォメーションモデルとドメインボキャブラリに基づき、データプロバイダ及びデータコンシューマに対して自己記述に必要なボキャブラリを提供する（図表 5-27 を参照されたい）。

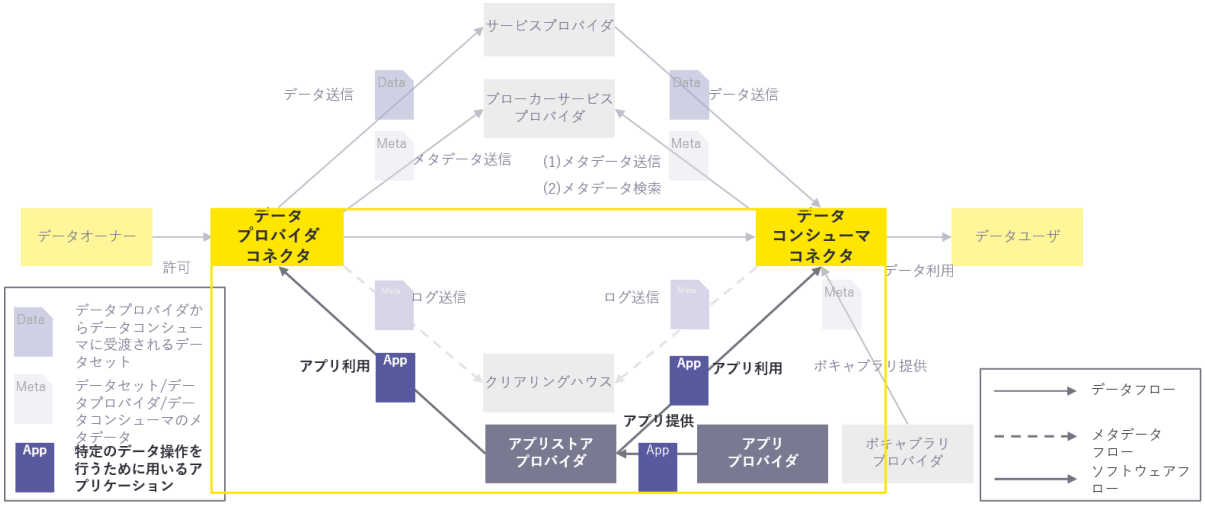
図表 5-27 IDS における役割とインタラクションとの関連（ボキャブラリプロバイダ）
（「IDS Reference Architecture Model 」より EY 作成）



IDS インフォメーションモデルは主に産業用データスペース内のデータアセットや再利用可能なデータ処理ソフトウェアの自己記述、公開、識別をサポートするモデルであるのに対して、ドメインボキャブラリは各分野内でしか使用されない専門的なボキャブラリをいう。IDS ドキュメント内には、いずれの場合にドメインボキャブラリの提供が行われるかに関する具体的な記載はないが、上記の IDS インフォメーションモデルの目的や機能に照らすと、産業用データスペースで指定されていないボキャブラリを用いてデータプロバイダ及びデータコンシューマが自己記述を行う必要がある場合が該当すると思われる。

現在のデータプロセスアルゴリズムを再利用することが出来ない場合には、アプリストアプロバイダからパッケージされたアプリの提供を受け、コネクタにインストールを行う（図表 5-28 を参照されたい）。

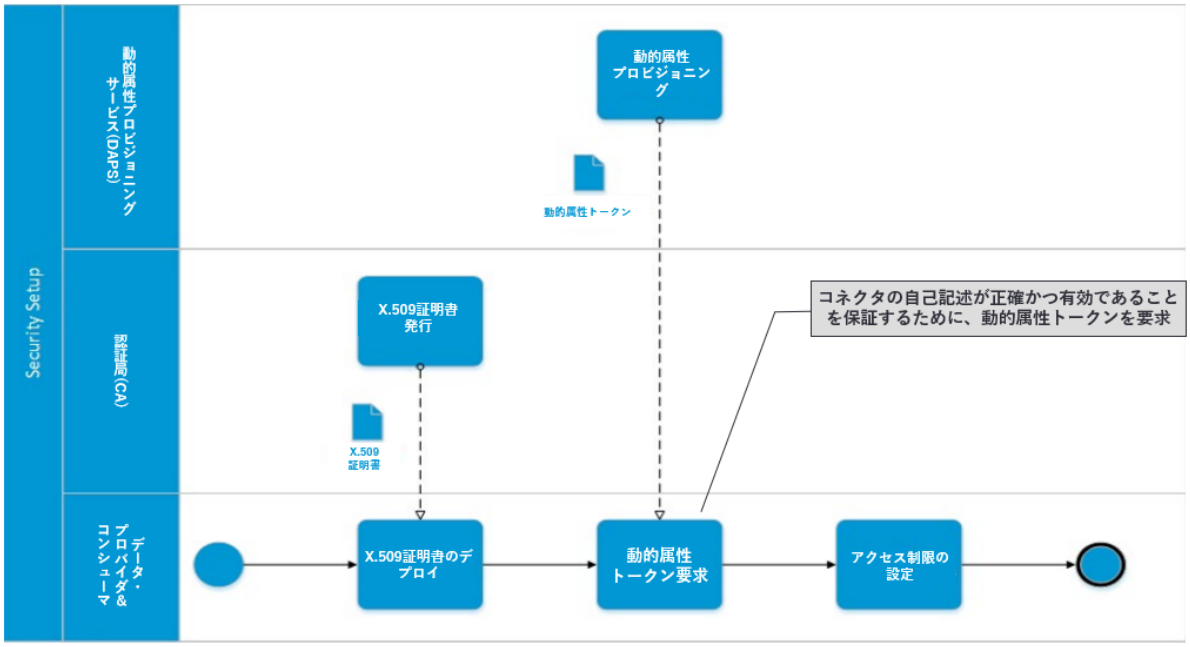
図表 5-28 IDS における役割とインタラクションとの関連（アプリストア）
（「IDS Reference Architecture Model 」より EY 作成）



その後、コネクタ内においてデータフローオーケストレーションを行う。データフローオーケストレーションの意味するところは、IDS ドキュメント内に具体的な記載がないが、コネクタの内部及び外部コネクタへの接続に使用されるネットワークパラメータ（ポート、IP 等）の定義や、接続に使用する必要がある SSL 証明書又は公開鍵インフラストラクチャに関する情報やコネクタの展開前に Validator によってチェックされるルール等をコネクタに設定することを指していると思われる[175]。その後、システムアダプタやエンドポイントの設定を経て、コネクタの設定が完了する。

後続のセキュリティ設定の詳細フローは図表 5-29 の通りである。

図表 5-29 セキュリティ設定サブプロセス
（「IDS Reference Architecture Model 」より EY 作成）



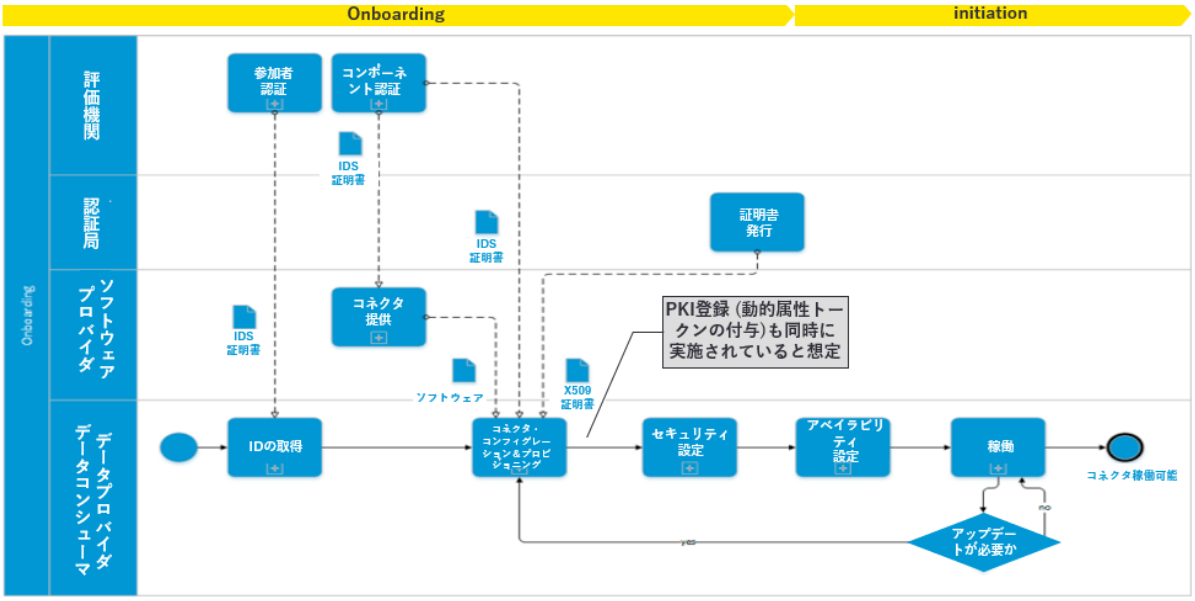
まず、データプロバイダ及びデータコンシューマは、オンボーディングプロセスにおいて認証局から発行された X.509 証明書をコネクタ内に実装する。その後、データプロバイダ及びデータコンシューマは、動的属性トークン（DAT）の発行を動的属性プロビジョニングサービス（DAPS）に対して要求する。DAT には参加者とコネクタの署名が入った動的な属性が含まれており、参加者が DAT を受け取ることで、自身のコネクタの自己記述が正確かつ有効であることを示すことができる。DAT はコネクタの通信ごとに提示されるため、通信中のコネクタは、いつでも通信相手の信頼性を確認することができる。DAT の発行によってコネクタの信頼性が保証された後、データプロバイダ及びデータコンシューマは、自らが定義するアクセスポリシーに基づいてアクセスコントロールの設定を行う。

[175] IDS はコネクタコンフィギュレーションモデルを規定している（“IDS REFERENCE ARCHITECTURE MODEL 3.5.1 Connector Architecture“）。当プロセスとの関連は明らかではないが、コネクタコンフィギュレーションモデルにデータフローのコンフィギュレーションに関する説明箇所があるため、データフローオーケストレーションが意味するものとして関連づけられると推測した。

(2) イニシエーション

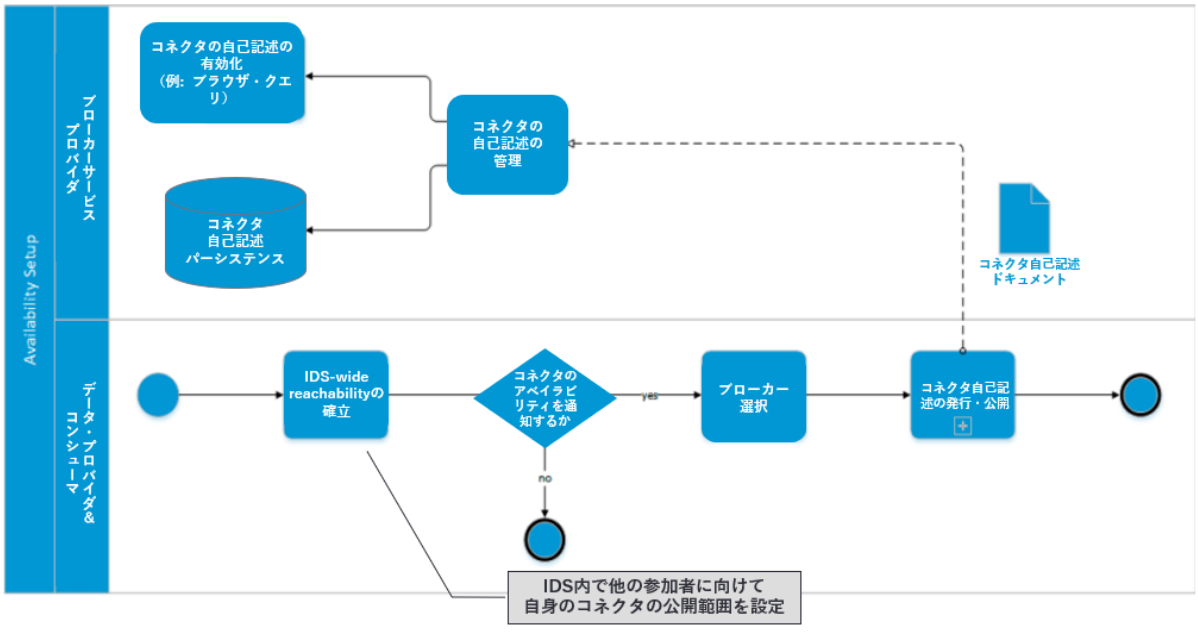
イニシエーションプロセスの概要に関するフロー図は図表 5-30 の通りである。

図表 5-30 イニシエーションプロセス
（「IDS Reference Architecture Model 」より EY 作成）



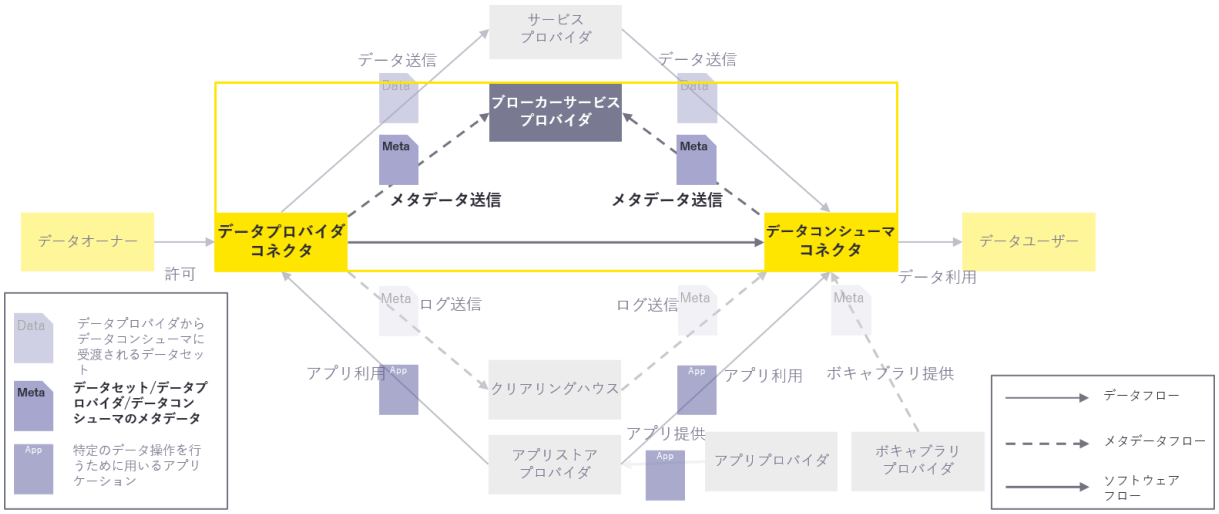
コネクタのアベイラビリティ設定を行うことで、コネクタは稼働可能となる。アベイラビリティ設定の詳細フローは図表 5-31 の通りである。

図表 5-31 アベイラビリティ設定
（「IDS Reference Architecture Model 」より EY 作成）



アベイラビリティ設定のプロセスでは、コネクタの公開範囲の設定やメタデータブローカーの選択、コネクタの自己記述のブローカーサービスプロバイダへの登録を行う（図表 5-32 を参照されたい）。

図表 5-32 IDS における役割とインタラクションとの関連（登録時・ブローカー）
（「IDS Reference Architecture Model 」より EY 作成）

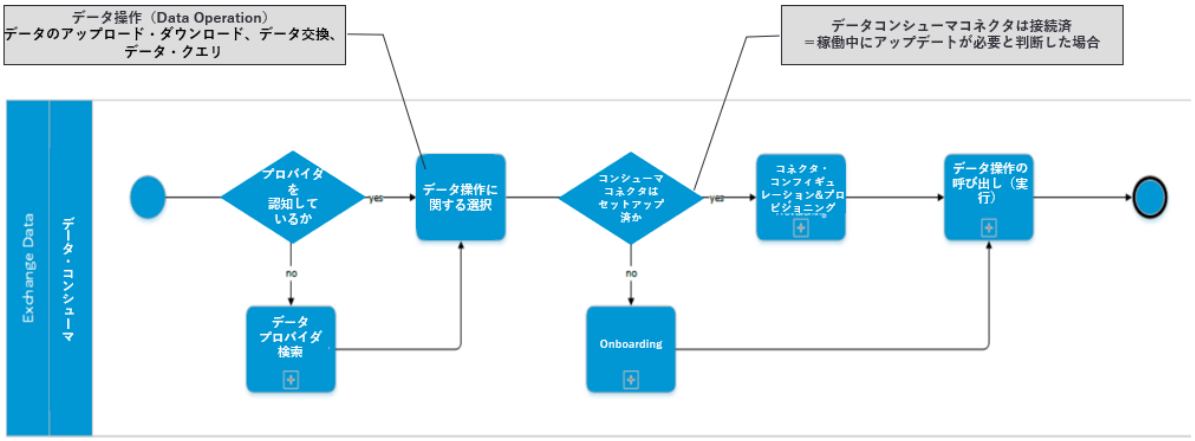


データプロバイダ及びデータコンシューマからブローカーサービスプロバイダに提供されたコネクタの自己記述はパーシステンスに保存され、ブローカーサービスプロバイダによって管理される。ブローカーサービスプロバイダがコネクタの自己記述を有効化することによって、データコンシューマがデータプロバイダを検索する際のクエリ処理の結果にデータプロバイダの自己記述に関する情報が表示されるようになる（データ検索プロセスは「5.2.1 (3) データ送受信・利用時」に記載の通り）。なお、コネクタ稼働後であってもアップデートが必要な際には、前述のコネクタコンフィギュレーションプロセスやセキュリティ設定プロセスを経て、アベイラビリティ設定を行うこととなる。

(3) データ送受信・利用時

データ送受信時の概要に関するフロー図は図表 5-33 の通りである。

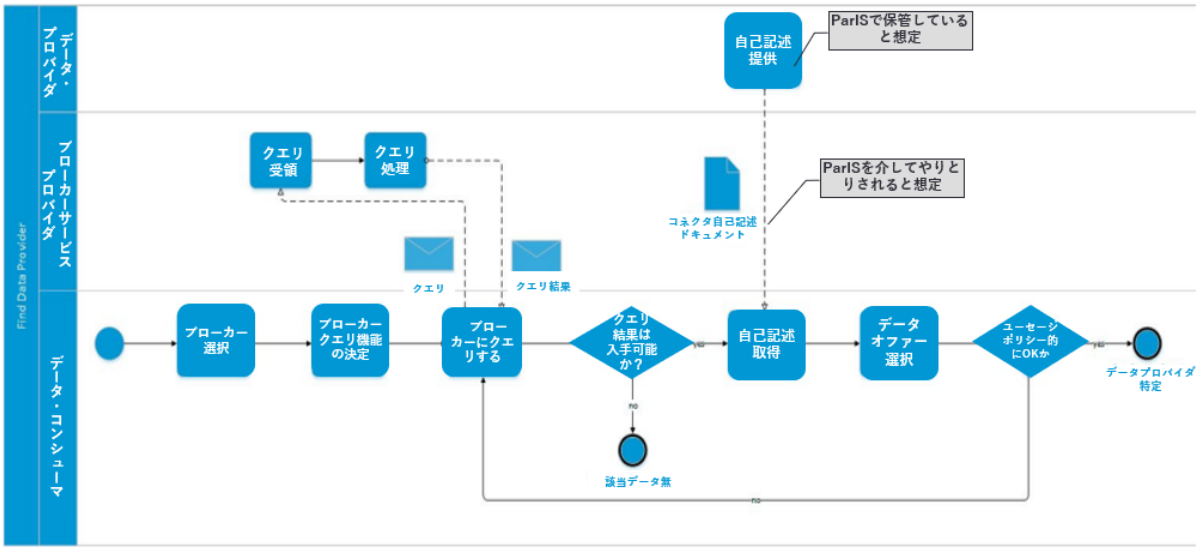
図表 5-33 データ送受信プロセス
（「IDS Reference Architecture Model 」より EY 作成）



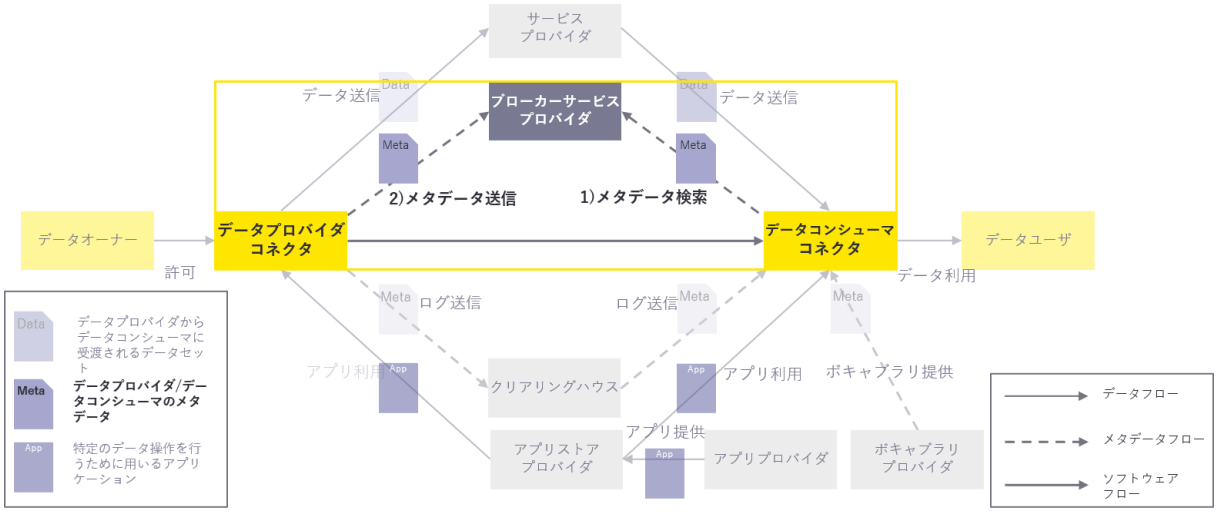
データコンシューマがデータプロバイダを認知していない場合には、最初にデータプロバイダ検索を行う。その後、データコンシューマはデータ操作に関する選択（データのアップロードやダウンロード、データ交換、データクエリ等）を行い、データ操作の呼び出し、すなわち選択したデータ操作の実行を行う。なお、基本的にはデータ送受信時にはアップデートが必要であり、前述のコネクタコンフィギュレーション＆プロビジョニングプロセスを経ることとなる。また、コンシューマのコネクタのセットアップからやり直す必要がある場合には、前述のオンボーディングプロセス全体を経由することとなる。

データプロバイダ検索の詳細フローは図表 5-34 の通りであり、データコンシューマはデータプロバイダから自己記述を取得し、データプロバイダを特定する（図表 5-35 を参照されたい）。

図表 5-34 データプロバイダ検索サブプロセス
（「IDS Reference Architecture Model 」より EY 作成）



図表 5-35 IDS における役割とインタラクションとの関連（検索時・ブローカー）
（「IDS Reference Architecture Model 」より EY 作成）



まず、データコンシューマは、取得を希望するデータを提供しているデータプロバイダに関する自己記述に関するメタデータを保管していると思われるブローカーサービスプロバイダを選択し、選択したメタデータブローカーに対して行うクエリ処理を決定する。これに基づき、ブローカーサービスプロバイダに対してクエリ処理を行うことで、ブローカーサービスプロバイダはデータコンシューマに対してクエリ結果を返す。該当データが存在した場合には、データプロバイダから自己記述を取得する。その後、データコンシューマは取得を希望するデータに関するオファーを行い、ユーセージポリシーで合意がなされた場合には、データプロバイダが確定する。

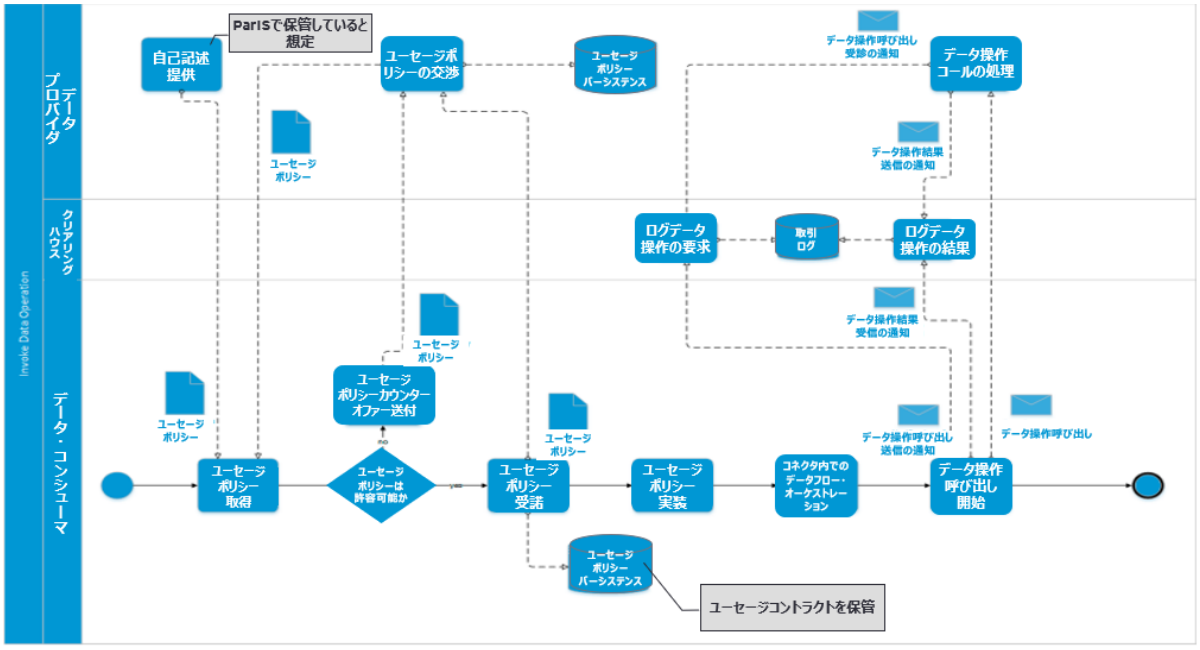
なお、ユーセージポリシーとは、データオーナーが指定したデータ利用を制限するルールセットであり、この内容については必要に応じてデータコンシューマとデータプロバイ

ダとの間で交渉を行う。このプロセスの詳細については、後続するデータ操作の呼び出し（実行）に記載する。

データプロバイダの自己記述の保管を行う主体に関しては、IDS ドキュメント内に具体的な記載がないが、IDS 参加者の属性の公開や問い合わせを行うためのインタラクションメカニズムを提供する IDS のコンポーネントである ParIS が保管していると想定される。そうだとすれば、データプロバイダからデータコンシューマに対してコネクタの自己記述が提供される際には、ParIS を経由しているものと考えられる。

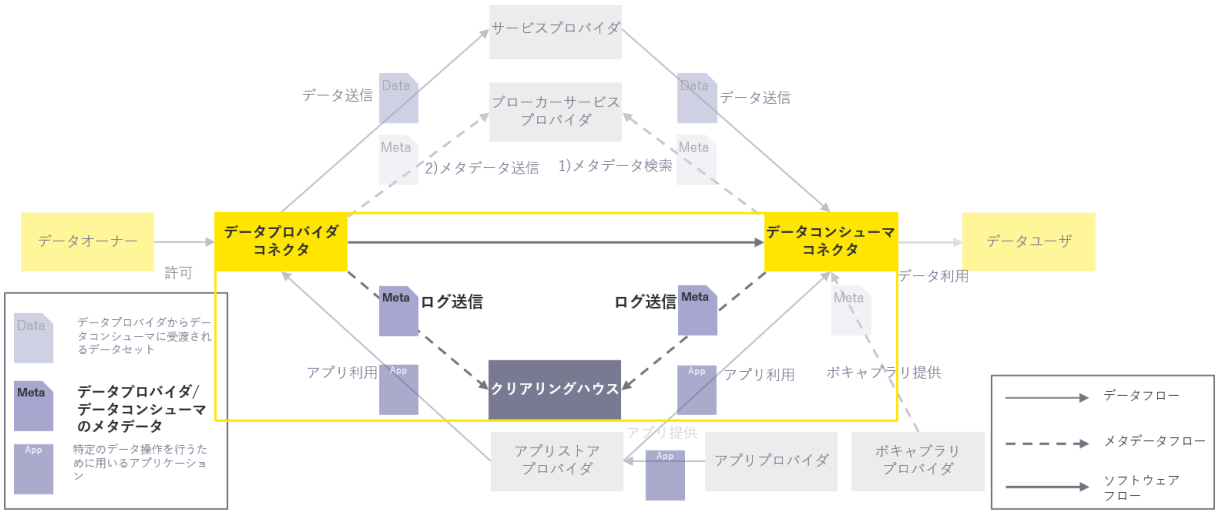
データ操作の呼び出し（実行）の詳細フローは図表 5-36 の通りであり、データコンシューマとデータプロバイダとの間で合意されたユーセージポリシーを実装し、データ操作を行うまでのプロセスを表している。

図表 5-36 データ操作の呼び出し（実行）サブプロセス
（「IDS Reference Architecture Model 」より EY 作成）



まず、データコンシューマはデータプロバイダから自己記述の提供を受けた後、必要に応じてデータプロバイダに対してユーセージポリシーの交渉を行う。データプロバイダからのカウンターオファーを受諾した場合（ユーセージコントラクトの成立）には、二者間での合意内容にユーセージポリシーは更新され、それぞれのユーセージポリシーパーシステンス上に保存される。その後、データコンシューマはユーセージポリシーの実装を行うが、データ操作の呼び出し（=実行）を行う前にコネクタコンフィギュレーション＆プロビジョニングを行う必要があることは、前述の通りである。データ操作の呼び出し（=実行）が行われることで、データコンシューマはデータプロバイダからデータを取得することができ、その際の取引ログはクリアリングハウスに保管される（図表 5-37 を参照されたい）。

図表 5-37 IDS における役割とインタラクションとの関連（クリアリングハウス）
（「IDS Reference Architecture Model 」より EY 作成）



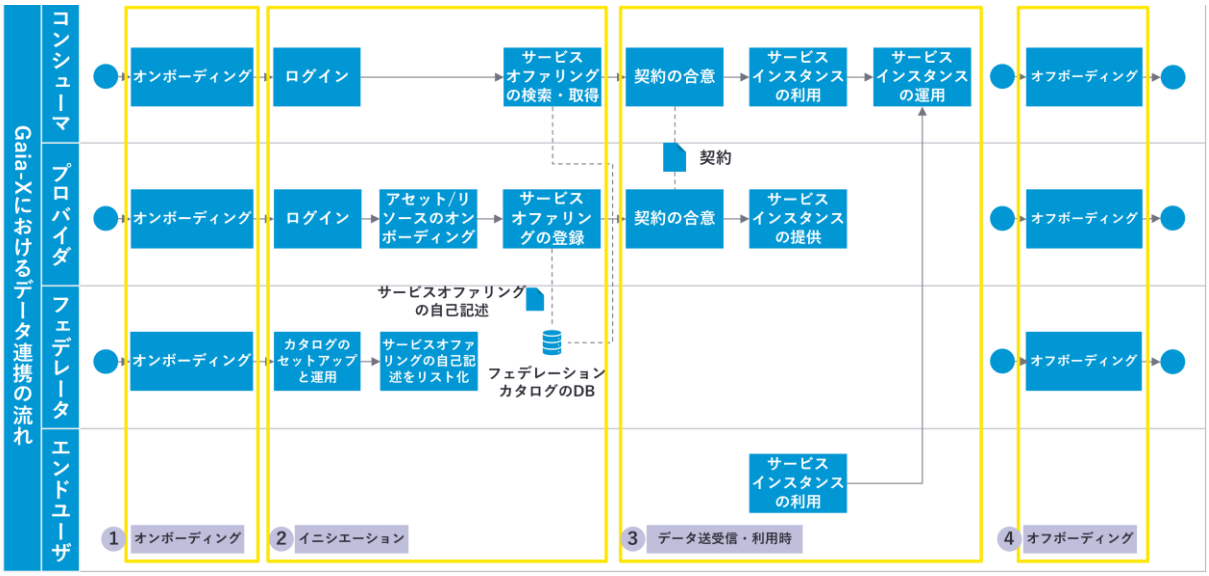
クリアリングハウスには、この取引ログとデータユーセージポリシーとの整合性を検証する機能がある。これにより、データ利用時においてクリアリングハウスはユーセージポリシーのエンフォースメントを強制させる役割を果たす。

5.2.2 Gaia-X におけるプロセス

本項では、Gaia-X におけるデータ取引に係るプロセスについて説明する。図表 5-38 は、Gaia-X のデータ取引の一連のプロセスを示している。

Gaia-X エコシステムに参加を希望する組織や個人は AISBL もしくは公証発行者による認証プロセス（＝オンボーディング）を受けなければならない。認証プロセスにて Gaia-X エコシステムへの参加が認められると、参加組織はデータを利用・登録を開始するためにポータルへのログインやプロバイダが所有するサービスオファリングの登録・検索等（＝イニシエーション）を実行できる。その後、コンシューマが所望のサービスオファリングを利用するためにプロバイダと契約を合意し、サービスインスタンスの利用・運用を開始する（＝データ送受信・利用時）。サービスインスタンスの利用時、コンシューマがユーセージポリシーに従って利用しているか証明するエビデンスログが記録される。参加組織内の任意のプリンシパルや、参加組織自体、あるいは公証発行者等を Gaia-X エコシステムから脱退させるためには対象の VC を破棄する（＝オフボーディング）必要がある。

図表 5-38 「Basic Interactions of Participants」より EY 作成

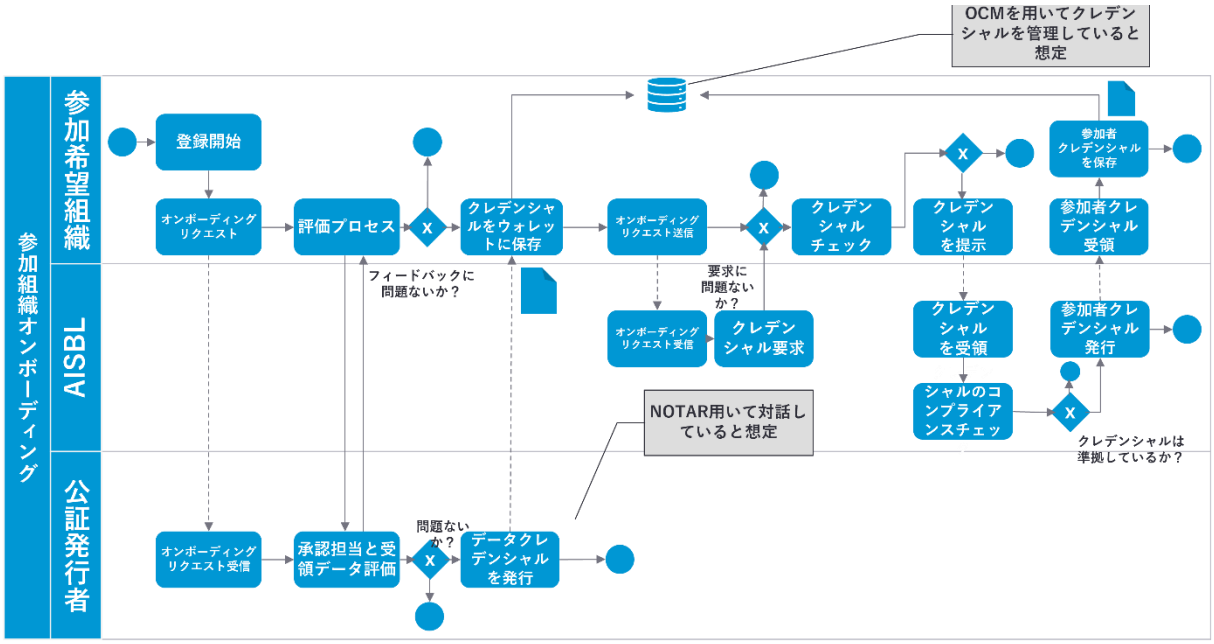


(1) オンボーディング

図表 5-39 は、Gaia-X エコシステムに参加を希望する組織のオンボーディングプロセスを示している。参加組織のオンボーディングプロセスの目的は、参加希望組織が公証発行者及び AISBL によって Gaia-X エコシステムへの参加を認められ、Gaia-X エコシステムにおいてサービスオファリングの登録や利用に必要な Verifiable Credential を AISBL から発行してもらうことである。ここで、公証発行者とは、Gaia-X へのオンボーディングを希望する組織がコンプライアンス等に準拠しているか評価する機関であり、Gaia-X AISBL によって認証されている。

まず、参加希望組織は公証発行者に対して、オンボーディングに必要なデータと共にオンボーディングリクエストを送信する。公証発行者は、参加希望組織によって提示されたデータを基に参加希望組織が Gaia-X のコンプライアンスに準拠する組織であるか評価する。公証発行者によって問題ないと判断された参加希望者は公証発行者からデータ Credential を受領し、Gaia-X AISBL にオンボーディングリクエストを送信する。データ Credential の定義は明記されていないが、参加希望組織が評価プロセスによって正当な組織であると判断された場合に公証発行者から発行される Credential であると想定される。AISBL は参加希望者から受領したデータ Credential のコンプライアンスをチェックし、問題なければ参加希望組織に紐づく Verifiable Credential を発行する。参加組織は Verifiable Credential を OCM に保管する。

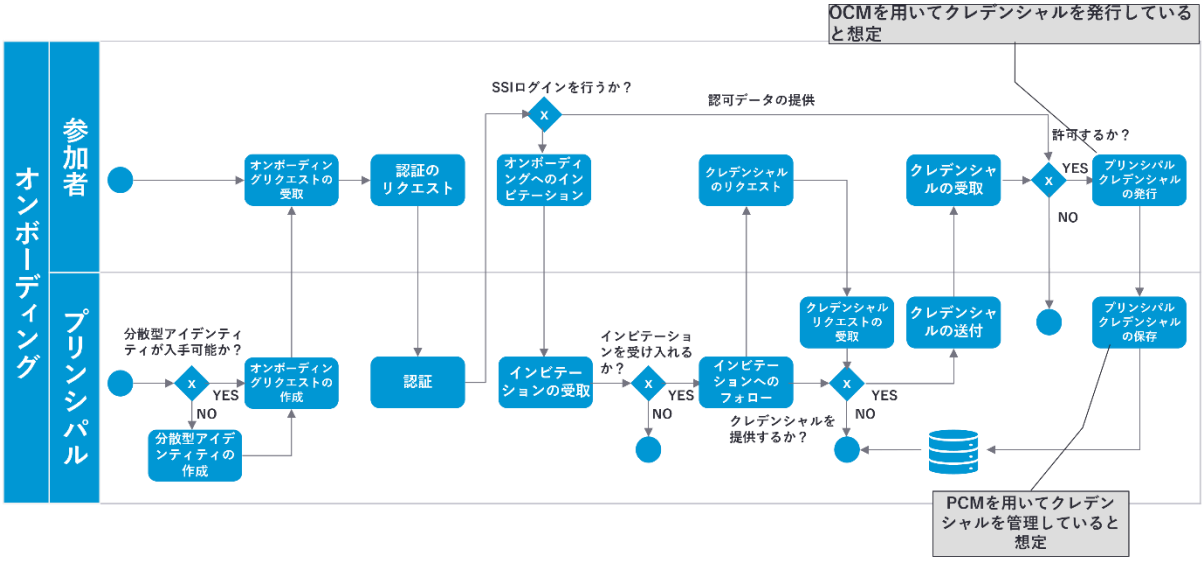
図表 5-39 「Reference Document Identity and Access Management Gaia-X Community Document IAM」より EY 作成



図表 5-40 は、参加組織内の従業員等に相当するプリンシパルのオンボーディングプロセスを示している。プリンシパルのオンボーディングプロセスの目的は、プリンシパルが Gaia-X エコシステムにおいてサービスオファリングの登録や利用時にポータルにログインする際に必要な Verifiable Credential を参加組織から発行してもらうためである。

まず、参加を希望するプリンシパルは参加組織に対してオンボーディングリクエストを送信する。本リクエストを受領した参加組織はプリンシパルに対して認証を要求し、問題ない場合はオンボーディングインビテーションを送信する。プリンシパルはインビテーションに従って登録処理を実行し、自身の Credential を参加組織に送信する。ここで送信される Credential は誰によってどのように生成されたものか仕様書上に明記されていないため、今後アップデートされる中で明らかになると想定される。本 Credential を受領した参加組織は、プリンシパルに紐づく Verifiable Credential を発行、送信し、プリンシパルによって PCM 上に保管される。

図表 5-40 「Reference Document Identity and Access Management Gaia-X Community Document IAM」より EY 作成

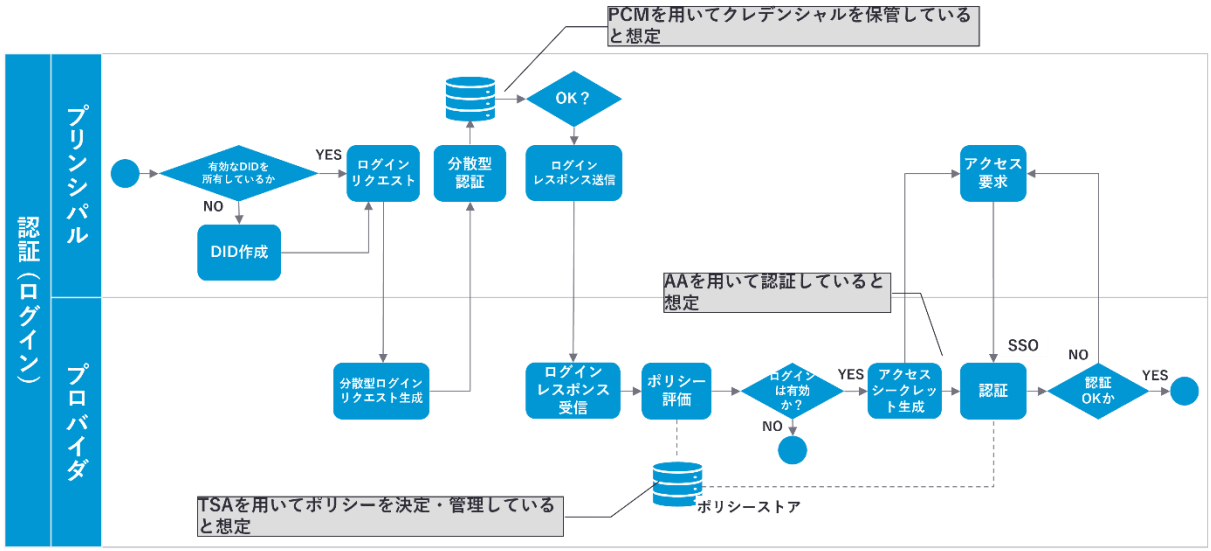


(2) イニシエーション

イニシエーションプロセスは、①ポータルへのログイン、②アセット/リソースのオンボーディング、③サービスオファリングの検索・取得・登録の 3 つのサブプロセスで構成される。

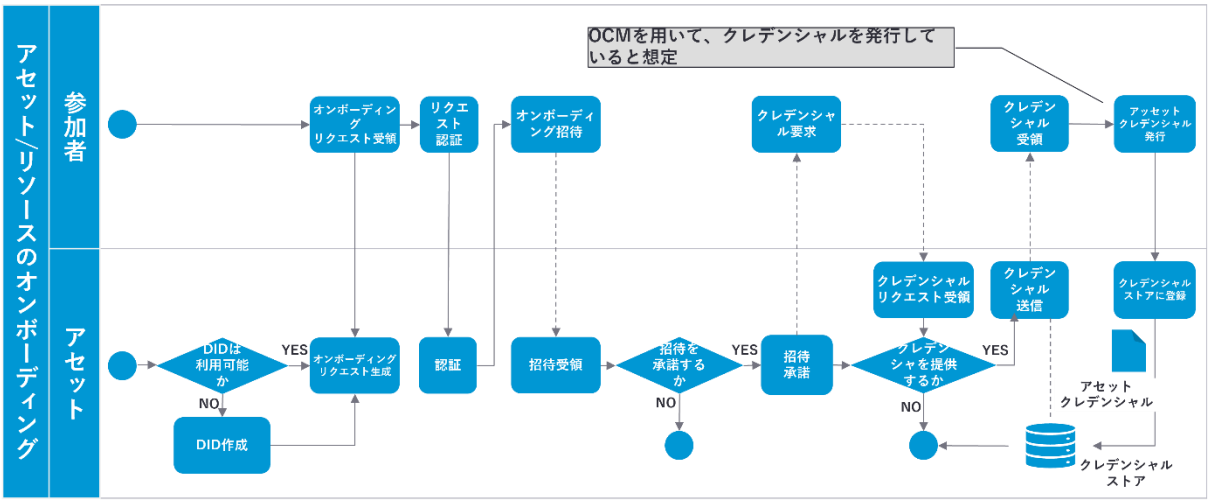
①ポータルへのログインの目的は、プリンシパルがサービスオファリングを検索したり、利用したりするために、Gaia-X のポータル上にて自身の VC を用いた分散型認証結果をプロバイダに提示し、認証を受けることである。図表 5-41 はポータルへのログインプロセスを示している。まず、プリンシパルはログインリクエストをプロバイダに送信し、その後、PCM を用いて分散型認証を実行する。分散型認証が成功した際に出力されるログインレスポンスをプロバイダに提供し、プロバイダは TSA を用いてプリンシパルのポリシーを評価する。ログインが有効であると判断された場合、プリンシパルに対してアクセスシークレットを発行する。

図表 5-41 「Reference Document Identity and Access Management Gaia-X Community Document IAM」より EY 作成



図表 5-42 は、②アセット/リソースのオンボーディングのプロセスを示している。本プロセスの目的は、フェデレーションカタログに掲載したいアセットに紐づく Verifiable Credential を発行することである。最初に、対象アセットのオンボーディングリクエストを作成し、参加組織に送信する。参加組織から送信されるオンボーディングインビテーションに従い登録処理を実行し、参加組織に登録したいフェデレーションカタログのスキーマに準拠する自己記述を送信する。その後、参加組織によって対象アセットの Verifiable Credential が発行される。

図表 5-42 「Reference Document Identity and Access Management Gaia-X Community Document IAM」より EY 作成

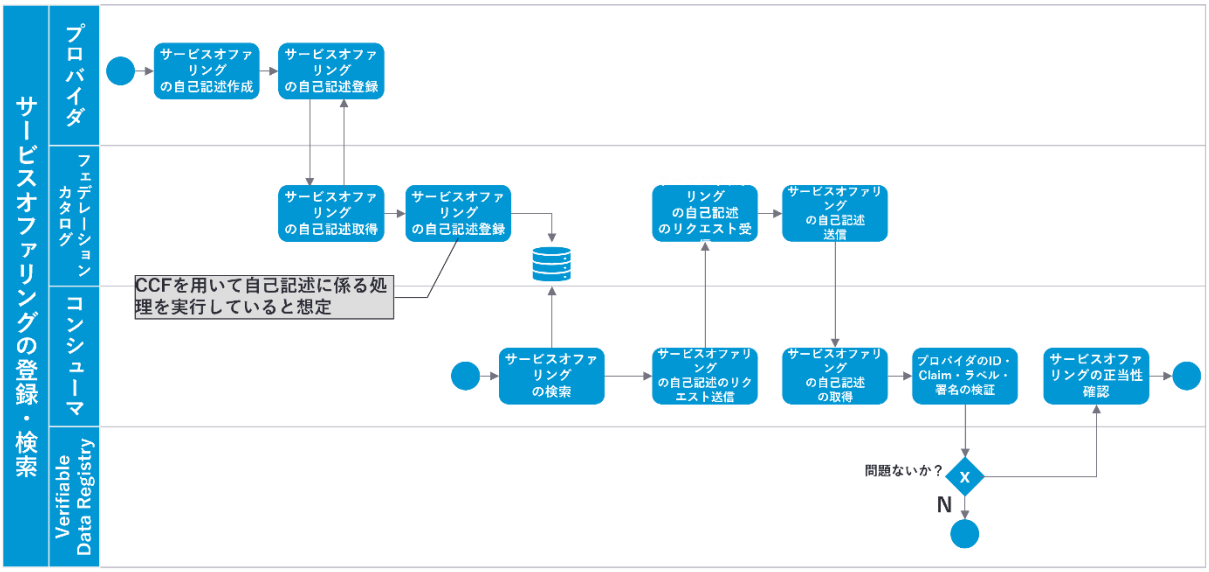


最後に、③サービスオファリングの検索・取得・登録のプロセスについてプロバイダ視点とコンシューマ視点から説明する。プロバイダ視点では、プロバイダが公開したい

サービスオファリングに関する自己記述を作成し、フェデレーションカタログに登録する。その際、フェデレーションカタログ上では自己記述ストレージに対象の自己記述を格納する。次に、コンシューマ視点では、フェデレーションカタログを参照し所望のサービスオファリングを検索する。利用したいサービスオファリングの自己記述をリクエストし、フェデレーションカタログから当該自己記述を受領する。対象のサービスオファリングの正当性を検証するため、Verifiable Data Registry を参照し自己記述に含まれている Claim やラベル情報を確認する。

なお、本フローは Gaia-X AISBL によって執筆されたドキュメントには直接含まれておらず、アーキテクチャ及び仕様書にて言及されている各コンポーネントの係る説明より推測して作成している[176]。

図表 5-43　サービスオファリングの登録・検索の流れ



(3) データ送受信・利用時

次に、Gaia-X エコシステムにおけるデータの送受信・利用時のプロセスについて説明する。データ送受信・利用時のプロセスは、①契約の合意、②サービスインスタンスの提供・利用・運用の 2 つのサブプロセスで構成される。

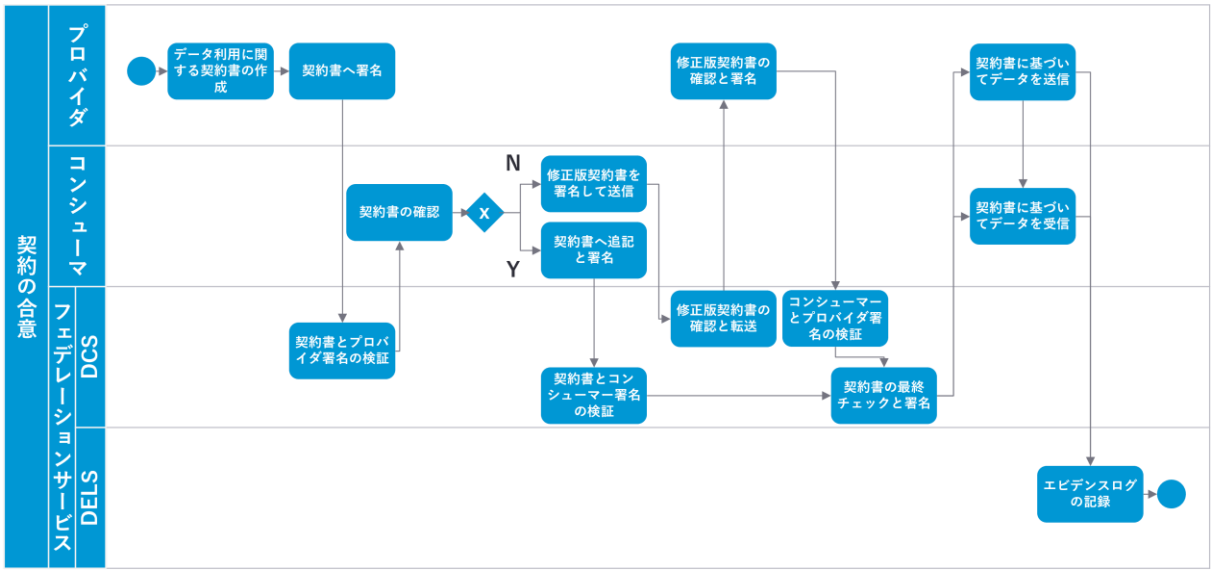
コンシューマによるサービスオファリングの検索・取得後、実際にサービスオファリングを利用するにあたってプロバイダとコンシューマ間で①契約の合意を実施する必要がある。まず、プロバイダはデータ利用に関する契約書を作成し、自身の電子署名を付与して DCS コンポーネントへ送信する。DCS 上では契約書とプロバイダによる署名が検証され、検証プロセスを通過するとコンシューマに転送される。コンシューマは契約書に合意する場合は自身の電子署名を付与し DCS に送信する。契約に合意できない場合は、契約内容を修正し、修正版契約書を DCS に転送する。DCS 上で契約書内容の

[176] Federation Service Specifications, Gaia-X Overview Specification Documents - DRAFT version 4b20f7c4, Gaia-X European Association for Data and Cloud AISBL, December 2021, https://Gaia-X.gitlab.io/technical-committee/federation-services/federation-service-specifications/ （2022 年 3 月 17 日アクセス）

確認及び電子署名の検証完了後、プロバイダに修正版契約書が送信され、プロバイダによって確認するプロセスが発生する。ここでプロバイダが契約内容に合意する場合、DCS 上にて契約書の最終チェックが行われ、契約の合意が完了する。

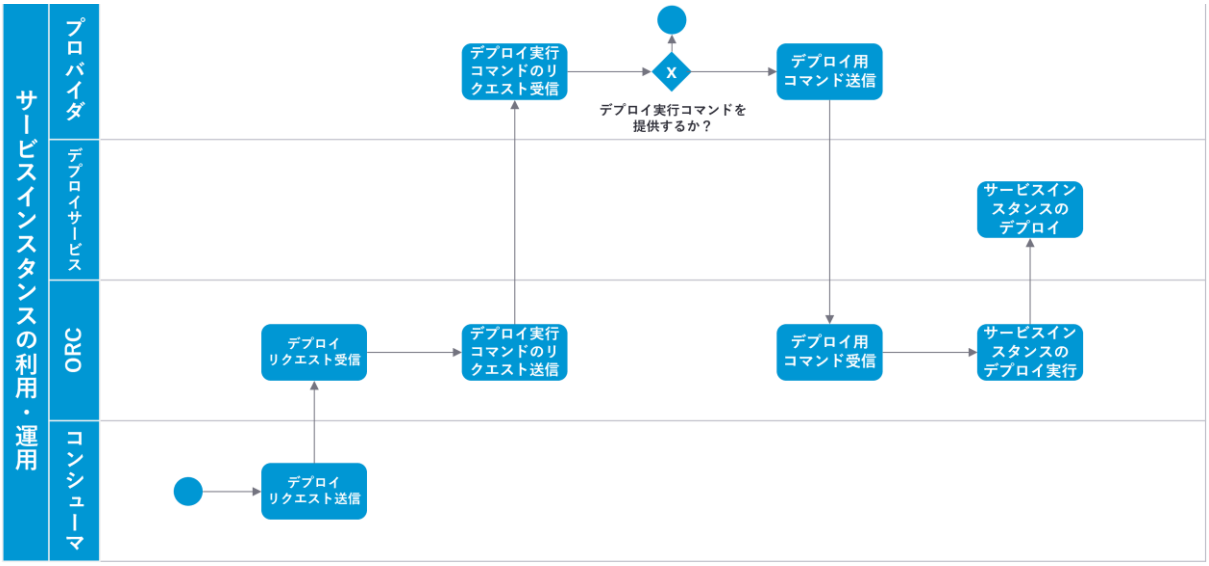
その後、プロバイダとコンシューマは契約書の内容に基づいてデータを送受信し、ユーセージポリシーに従って利用されているかエビデンスログが DELS 上に記録される。

図表 5-44　契約合意の流れ（EY 作成）



次に、プロバイダとコンシューマ間の契約の合意後にサービスオファリングを利用する際に必要なサービスインスタンスの利用・運用プロセスについて説明する。最初に、コンシューマはサービスインスタンスのデプロイリクエストを ORC に送信する。ORC はデプロイリクエストに基づき、プロバイダに対してデプロイ実行コマンドをリクエストする。プロバイダはデプロイ実行コマンドを提供するか判断し、提供する場合は ORC 対してデプロイ実行コマンドを送信する。ORC は受領したコマンドを実行してサービスオファリングの実行環境であるサービスインスタンスをデプロイする。

図表 5-45　サービスインスタンスの利用・運用の流れ（EY 作成）

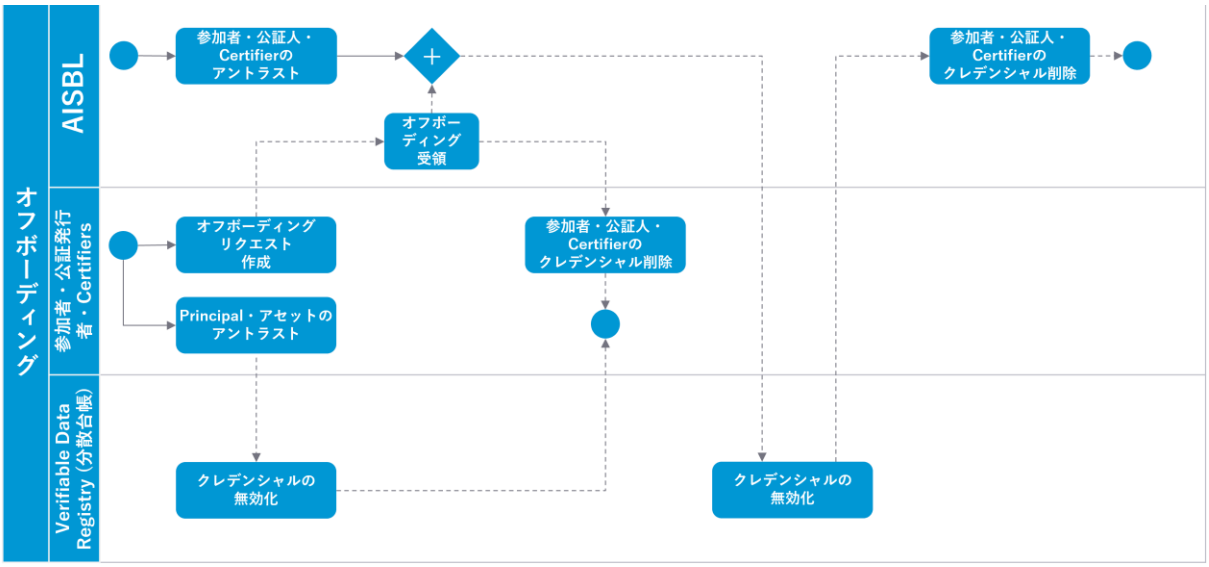


(4) オフボーディング

参加組織内の任意のプリンシパルや、参加組織自体、あるいは公証発行者等を Gaia-X エコシステムから脱退させるオフボーディングプロセスについて、図表 5-46 に基づいて説明する。

アントラストによるオフボーディングプロセスは①参加組織・公証発行者・Credential 発行者によってプリンシパルやアセットを脱退させるケースと、②AISBL がアントラスト対象として指定した参加組織・公証発行者・Credential 発行者らが、複数組織（参加組織・公証発行者・Credential 発行者）にもアントラスト対象として指定されている場合に当該組織を脱退させるケースが存在する。①の場合、アントラスト対象のプリンシパルやアセットをオフボーディングさせるため、VC を無効化する。②の場合、AISBL が保管しているオフボーディング対象の組織（参加組織・公証発行者・Credential 発行者）の VC を破棄する。

図表 5-46 「Reference Document Identity and Access Management Gaia-X Community Document IAM」より EY 作成



5.2.3 「IDS・Gaia-X のプロセスの共通点・相違点とその背景にある違い

まず、オンボーディングプロセスにおける共通点、相違点について述べる。

IDS と Gaia-X 両者に共通するのは、信頼できる第三者機関から認証を受けて X.509 証明書ないし VC が発行されることによって、参加者が自身の正当性を証明するという点である。信頼できる第三者機関の役割を、IDS では評価機関及び認証局が、Gaia-X では公証発行者及び Gaia-X　AISBL が担っている。IDS の評価機関と Gaia-X の公証発行者は、オンボーディングを経てそれぞれ IDSA、Gaia-X AISBL に認められた機関でなければならない。つまり、IDS と Gaia-X ではオンボーディングに関して近しい体制を取っていると言える。

また、IDS におけるセキュリティ設定では DAT の発行プロセスが含まれており、Gaia-X でこの DAT に相当するのが Credential 発行者によって発行される VC であると想定される。サービスの提供、消費に際して必要な属性を DAPS ないし Credential 発行者より受領し、それらを用いてデータ交換に係る認証・認可を行うという点で両者の共通点が伺える。

オンボーディングにおける両者の違いは 2 点ある。まず、IDS ではコネクタコンフィギュレーション及びプロビジョニング、セキュリティ設定、アベイラビリティ設定のプロセスが定義されているのに対し、Gaia-X では現時点でコネクタに関する各種設定プロセスが定義されていない点である。Gaia-X ではデータ交換に用いるコネクタの仕様についてアップデート版仕様書にて明記するとされているため[177]、今後のアップデート版でコネクタ設定に係る具体的なプロセスが明らかになると想定される。コネクタコンフィギュレーションにおいて、IDS ではボキャブラリプロバイダから自己記述に必要なインフォメーションモデルの提供を受けているが、Gaia-X ではどの段階で自己記述のスキーマ（IDS のインフォ

[177] Data Contract Service, Gaia-X Overview Specification Documents - DRAFT version 4b20f7c4, August 2021, (accessed via Data Contract Service - Gaia-X Overview Specification Documents - DRAFT version 4b20f7c4,16 March 2022.)

メーションモデルに相当）に関する情報を取得するのか明らかにされていない。

２つ目の大きな違いは、Gaia-X では参加組織のオンボーディング後に当該組織内のプリンシパルのオンボーディングが定義されているのに対して、IDS ではそのようなプロセスが定義されていない点である。Gaia-X ではプリンシパルが参加組織の代表者として自己記述の登録やデータ交換等を行うが、IDS ではコネクタ自体に証明書をインストールして用いるという点で違いが見られる。

次に、イニシエーションプロセスにおける共通点、相違点について述べる。IDS、Gaia-X 両者で共通するのは、データカタログの役割を持つメタデータブローカーないしフェデレーションカタログに自己記述を登録し、他ユーザによって検索できるようにするという点である。IDS ではデータカタログの機能を提供するメタデータブローカーという役割が存在するのに対し、Gaia-X ではフェデレーションサービスの一つとしてデータカタログを提供するという位置づけであり、役割の持たせ方の違いが見られる。また、Gaia-X ではリソースのオンボーディングプロセスが定義されているのに対して、IDS ではそれに相当するプロセスが定義されていないという違いも伺える。

データ送受信・利用時の共通点、相違点について説明する。まず、両者の共通点として、データ交換前にプロバイダとコンシューマ間で契約の合意を行っている。IDS と Gaia-X の両者ともプロバイダとコンシューマ間でユーセージポリシーをやりとりし、実際のデータ交換時もユーセージポリシーに従って利用されているかエビデンスログを蓄積している。その際、IDS ではクリアリングハウスに格納されるのに対し、Gaia-X ではフェデレーションサービスのコンポーネントの一つである DELS に格納される。

最後に、オフボーディングについては Gaia-X では定義されているが、IDS では該当するプロセスが定義されていない。

5.3 認証・認可の観点

5.3.1 IDS

データセキュリティとデータ主権は、IDS の基本的な価値提案である。データ主権とは、自然人又は法人がそのデータを完全にコントロールできることと定義できる。したがって、IDS へのアクセス許可を得ようとする組織又は個人はすべて認証され、参加者同士が安全にデータを交換するために使用するコアソフトウェアコンポーネント（コネクタ等）も認証される。組織と個人の認証はセキュリティとトラストに焦点を当てており、コンポーネントの認証は相互運用性を確保する技術要件への準拠も含んでいる。参加者とコアコンポーネントの認証に一貫したプロセスを確保するため、IDS は認証プロセスを管理するすべてのプロセス、規則及び標準から成る認証スキームを使用している。IDS の認証制度は、国際的に認定されている他の認証概念から得られたベストプラクティスに準拠している。なお、以下では主として IDS リファレンスアーキテクチャモデルの「4.2.2 CERTIFICATION PROCESS」及び WHITE PAPER CERTIFICATION FRAMEWORK FOR THE IDS CERTIFICATION SCHEME を参照した[178]。

(1) 証明書の発行

図表 5-47 は、証明書発行プロセスの基本構造及びこのプロセスに関わる役割の概要を示すものである。このセクションで説明されているすべての役割は、IDS に特有であることに留意が必要である。すなわち、「証明書発行機関」等の用語を、IDS と関係なく証明書を発行している既存の組織を指すと誤解してはならない。

[178] *REFERENCE ARCHITECTURE MODEL 3.0*, INTERNATIONAL DATA SPACES ASSOCIATION, December 2020, p69-p97, https://internationaldataspaces.org/wp-content/uploads/IDS-Reference-Architecture-Model-3.0-2019.pdf（2022 年 3 月 27 日アクセス）
WHITE PAPER CERTIFICATION FRAMEWORK FOR THE IDS CERTIFICATION SCHEME VERSION 2, INTERNATIONAL DATA SPACES ASSOCIATION, 2019, https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-White-Paper-certification-scheme-V.2.pdf（2022 年 3 月 29 日アクセス）

図表 5-47 証明書発行プロセス（概要）

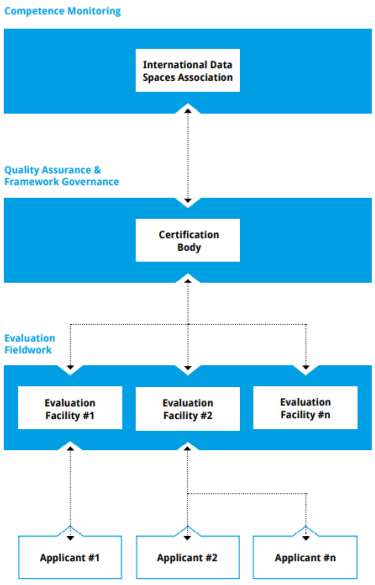


Figure 4.23: Certification process

ア 証明書発行機関・評価機関・申請者の役割

（ア）証明書発行機関

証明書発行機関は、品質保証とフレームワークのガバナンスに関して認証プロセスを監督する。標準的な評価手順を定義し、評価機関の行動を監督する。IDS-ID は、評価機関（下記参照）と証明書発行機関の両方が、認証の前提条件がすべて満たされているという結論に達した場合にのみ付与される。

（イ）評価機関

申請者（下記参照）と契約した評価機関は、認証プロセスにおいて詳細な技術的・組織的評価作業を行う責任を負う。評価機関は、組織又はコアコンポーネントに対して、評価プロセスの詳細と確認されたセキュリティレベルに関する情報（後者は、実施された評価活動の深さと範囲を決定する）を記載した評価報告書を発行する。

「評価機関」とは、マネジメントシステム評価（参加者認証）については認定審査員、製品評価（コアコンポーネント認証）については認定評価員を指す。従って、証明書発行機関は複数の評価機関を統括し、協力することになる。ただし、組織又はコアコンポーネントの各評価には、1 つの評価機関のみが関与する。

（ウ）申請者

申請者は、評価・認証プロセスの対象であるだけでなく、積極的な役割を担っている。申請者は、証明書発行プロセスを開始するために、積極的に申請書を提出する必要がある。これは、IDS への展開を意図したソフトウェアコンポーネントを開

発する組織（すなわち、ソフトウェアプロバイダ候補）及び IDS 参加者になろうとする組織にも適用される。

イ 申請者とコアコンポーネントへの証明書発行

（ア）参加者への証明書発行

IDS の参加者は、有益な情報やデータを共有することで協業することになる。この連携には、参加者間の信頼関係が必要である。さらに、参加者が信頼できることは、IDS とその評判にとっても不可欠である。この信頼は、インフラの信頼性やプロセスのコンプライアンス等、定義されたセキュリティレベルを満たしているかどうかで参加者を評価することで達成される。この参加者への証明書発行プロセスは、次の「認証基準カタログ」で説明するように、確立された認証基準や手法に基づいており、可用性、機密性、完全性に関するセキュリティレベルを証明するものである。中小企業に適した低い参入障壁と、高い情報セキュリティ要件を満たす拡張性のある認証を保証するため、マトリックスで示される評価方式が図表 5-48 の通り定義されている。横軸は「評価レベル」であり、評価範囲の深度を示している。縦方向は、満たすべきセキュリティ要求事項の範囲レベルである。

図表 5-48 証明書発行におけるセキュリティレベルと評価レベル（参加者）

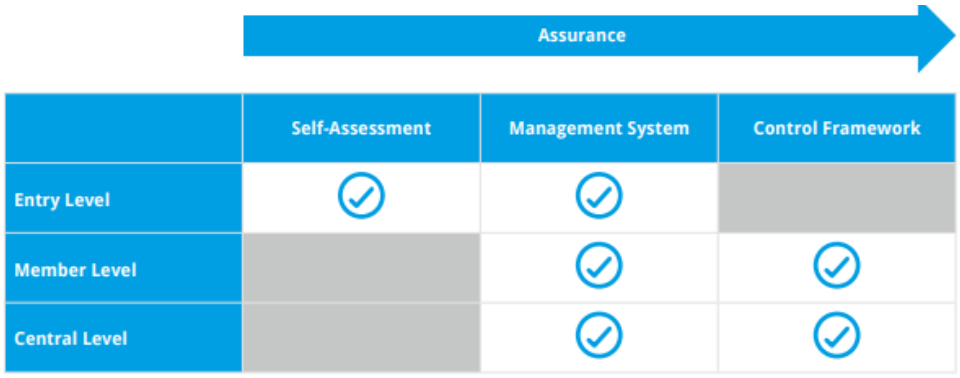


Figure 4: Certification Approach for participants of the Industrial Data Space

a 評価レベル

横軸の評価レベルは以下の三段階であり、それぞれのアプローチは図表 5-49 の通りである。

図表 5-49 評価レベルごとのアプローチ

評価レベル	概要
自己評価	• 自己評価とは、参加希望者が参加者自身の情報を開示し、参加者のシステムに関する情報を提供するために行う自己申告ベースで行われる取組である。 • 自己評価の実施にガバナンス機関は関与せず、自己評

評価レベル	概要
	価の対象に含まれる情報が評価機関によって検証されることはない。自己評価には評価者が関与しないため、参加者に完全な資格を持つ IDS 証明書は交付されない。 • 自己評価を行うことで、選択したユースケースで産業用データスペースの機能を探索し、テストすることが可能となる。また、自己評価を行うことで、評価されたサービスプロバイダによって運営されるマネージドコネクタを使用することができるようになる。 • 将来的に IDS への参加を希望するエンドユーザの参入障壁の最小化に資するものである。
マネジメント体制に対する評価	参加者のマネジメントシステムの評価が評価機関によって行われる。これは、申請者がマネジメント体制を適切に定義しているかどうか、定義されたマネジメントシステムに従って積極的に活動しているかどうかを分析するものである。 通常、ある時点の情報と証拠のインタビュー、現場監査、典型的なレビューが行われる。
コントロールフレームワークの分析	この評価には、マネジメント体制の見直しのみならず、マネジメント体制の運用の有効性や申請者のコントロールフレームワーク内で定義されたコントロールの評価も含まれる。これには通常、インタビュー、実地監査及び一定期間にわたってコントロールが実行されたことを証明するための無作為抽出に基づく証拠収集活動が含まれる。マネジメントシステム評価と同様に、その結果は証明書発行機関によって承認される。

b セキュリティ要件レベル

セキュリティ要件の範囲はエントリーレベル～セントラレベルの 3 段階で構成され、全てのレベルは ISO/IEC27001 と整合性のある要求事項が含まれた形で相互に構築されている。各参加者に求められるレベルは図表 5-50 の通りであり、エントリーレベル～セントラルレベルごとのセキュリティ要件については図表 5-51 の通りである。

図表 5-50 各コンポーネントの提供者に必要な評価レベル

	Entry Level	Member Level	Central Level
Data Owner	Required	Recommended	Optional
Data Provider	Required	Recommended	Optional
Data Consumer	Required	Recommended	Optional
Broker Service Provider		Required	Optional
App Store Provider		Required	Optional
Vocabulary Provider		Required	Optional
Service Provider		Required	Optional
Clearing House			Required
Identity Provider			Required

Figure 3: Mapping of the roles in the Industrial Data Space to the levels of certification

図表 5-51　参加者のレベルごとのセキュリティ要件

参加者レベル	求められるセキュリティ要件
エントリーレベル	エントリーレベルは、産業用データスペースの参加者が満たすべき基本的なセキュリティ要件のみを対象としている。 エントリーレベルは、産業用データスペースへの参加に関心のある企業（特に中小企業）にとって、多額の先行投資をすることなく、低い障壁となるものである。そのため、このレベルは、低コストの自己評価と参加者の管理システムの評価と組み合わされるのみとなっている。
メンバーレベル	メンバーレベルは中核となる参加者のほとんど（データオーナー、データプロバイダ、データコンシューマ、ブローカーサービスプロバイダ、アプリストアプロバイダ、ボキャブラリプロバイダ、サービスプロバイダ）に適した高度なセキュリティレベルを保証し、すべての関連するセキュリティ要件をカバーしている。 機密データの交換を伴うほとんどのユースケースでは、メンバーレベルで十分である。
セントラルレベル	セントラルレベルには、産業用データスペース内で重要な機能と役割を果たそうとする産業用データスペース参加者のために必要な特別な要件が含まれている。 これらの役割は特別な責任を負っているため、セキュリティ違反があれば、産業用データスペース全体又はそのかなりの部分に影響を及ぼす危険性があり、具体的にはクリアリングハウス及び ID プロバイダが対象となる。

c 参加者証明書発行基準カタログ

産業用データスペース申請者の経済的な参入障壁をさらに低くするため、参加者への証明書発行のアプローチは、他の認証制度、基準、規範に準拠して得られた既存の証明書の再利用を可能にするように設計されている。例えば、ある特定のコントロールテストは、ISAE3000 認証フレームワークから継承されるような関係にある。

参加者が既存の証明書を再利用できるようにするため、参加者証明書発行基準カタログ（CRIT-P）は、確立されたセキュリティ基準に基づいて作成されている。産業用データスペースの性質と国際的なアプローチから、ISO/IEC 27001 と BSI C5（ドイツ連邦情報セキュリティ局のクラウドコンピューティング準拠コントロールカタログ）が選択された。ISO/IEC 27001 は、国際的に普及していること、情報セキュリティに対する評価が高いことから選ばれている。 BSI C5 は、クラウドコンピューティングのような最新の IT 環境向けに開発された情報セキュリティの規格である。両規格のうち、産業用データスペースに関連する要件は、異なるレベルに関して適用可能なものが選択されている。これらの要件は、レベル毎に異なる種類の要件を持つ 16 のセクションにグループ化されている。レベル毎の段階的なアプローチにより、エントリーレベルのすべての要件は、メンバーレベルとセントラルレベルにも関連し、メンバーレベルのすべての要件は、セントラルレベルにも関連する。

d 参加者別の特記事項

証明書発行プロセスにおける参加者の役割ごとの特記事項は図表 5-52 の通りである。なお、下表にある主要な参加者・仲介者・サービス/ソフトウェアプロバイダの分類は、「5.1.1 (1) イ 参加者」に記載の分類と同一である。具体的な参加者及びコンポーネントについては、上記を参照されたい。

図表 5-52 証明書発行における参加者の役割

参加者	役割
主要な参加者	• データオーナー（多くの場合、データプロバイダと同一）は、自らが公開・提供するデータの完全性、機密性、可用性に対して責任を負う。データオーナーが採用するセキュリティ機構の評価及び認証は、関連するセキュリティ要件（データの完全性、機密性、可用性等）が攻撃によって損なわれるリスクに対して、十分なセキュリティの程度を提供するものとする。 • データオーナーとデータプロバイダが異なる主体である場合（データオーナーが自らデータを公開せず、データプロバイダに引き継ぐ場合）、データオーナーとデータプロバイダの両方がデータの完全性と機密性に責任を負う。しかし、データの利用可能性については、データオーナーがデータプロバイダにデータを引き渡した場合、データプロバイダのみが責任を負うことになる。データオーナーがデータプロバイダとして行動していない場合、採用されている技術的、物理的、組織的なセキュリティ機構の評価と証明は、攻撃によってデータの完全性と機密性が損なわれるリスクに対して十分なセキュリティレベルを

参加者	役割
	提供することを必要とする。 • データオーナーから提供されたデータにアクセスする組織として、データコンシューマもそのデータの機密性と完全性に責任を負う。また、データが許可された目的以外に使用されないことも保証しなければならない。
仲介者	• IDS は、ブローカーサービスプロバイダ、クリアリングハウスプロバイダ、アプリストアプロバイダ、ボキャブラリプロバイダに対して、リスクとしての考慮事項と参加者が希望するセキュリティレベルに合わせた評価を行い、リスクに対する十分な安全性を確保することを提案している。 • 上記の仲介者の中でも、アプリストアプロバイダに関しては、攻撃者が正規のアプリを改変したものに置き換えることに成功し、間接的にペイロードデータを脅かすという点で追加のリスクが存在する。しかし、IDS は、このリスクを低減するためには、アプリストアプロバイダ側の組織的対策よりも、アプリストアへの実装段階における対策（アプリプロバイダが暗号署名したアプリのみを受け付け、配布する等）の方が効果的であることも認識している。
サービス・ソフトウェアプロバイダ	• ソフトウェアプロバイダは通常、機密データに触れることはなく、適切な非機密性のテストデータを用いてテストを実行する。したがって、ほとんどの場合、組織のセキュリティに関する認証は必要ない。産業用データスペースの実際のデータへのアクセスが必要な場合、ソフトウェアプロバイダは、そのアクセスが必要とされる限り、データコンシューマ又はデータプロバイダの役割を引き受ける。この場合、対応する役割のセキュリティ要件が適用される。 • 参加者が産業用データスペースに参加するために必要な技術基盤を自ら配置しない場合、参加者は、産業用データスペースにおけるデータの公開等特定の作業を必要な基盤をホストするサービスプロバイダにアウトソーシングすることができる。この場合、このサービスプロバイダは、データプロバイダ、データコンシューマ、ブローカーサービスプロバイダ等の役割を担い、対応する活動を実行する。サービスプロバイダは、元の役割の責任とリスクを引き継ぐため、それぞれの役割に対応する要求事項に従わなければならない。

（イ）コアコンポーネントへの証明書発行

IDS のコアコンポーネントは、産業界や企業間の情報交換を安全に行うために、必要な機能と適切なセキュリティレベルを提供する必要がある。そのため、コアコンポーネントの認証は、相互運用性とセキュリティに重点を置き、その開発・保守プロセスの強化を目的としている。参加者への証明書発行の場合と同様に、IDS のコアコンポーネントについても、マトリックスで示される評価方式が下表の通り定義されている。これにより、中小企業に適した低い参入障壁と、高い情報セキュリティ要件に対応した拡張性のある認証が保証される。以下、図表 5-53 の縦軸及び横軸で示されている評価レベル及びセキュリティプロファイルについて概説する。

図表 5-53 証明書発行におけるセキュリティプロファイルと評価レベル（コンポーネント）

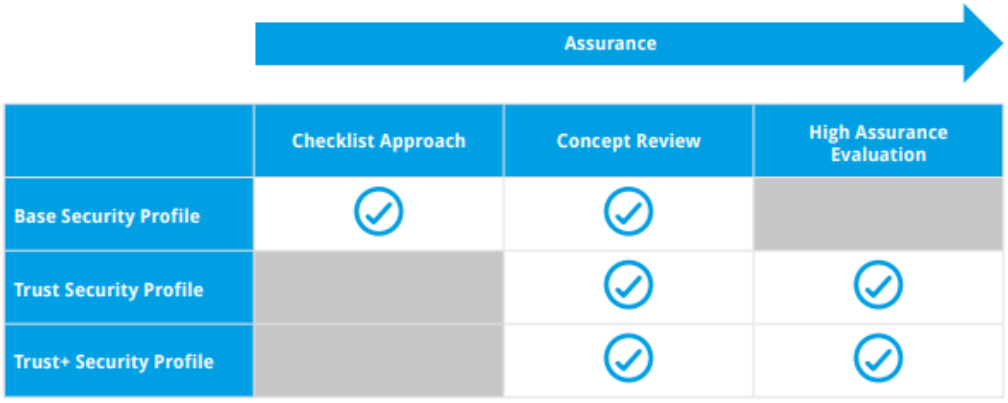


Figure 5: Certification Approach for core components of the Industrial Data Space

a 評価レベル

証明書発行に際して行われる評価の厳格性は、IDS 証明書発行スキームで定義された三段階の評価レベルで構成される。評価レベルごとのアプローチは図表 5-54 の通りである。

図表 5-54 評価レベルごとのアプローチ

評価レベル	概要
チェックリストアプローチ	コアコンポーネントは、対応するチェックリストで定義されたセキュリティ機能（セキュリティ要件、セキュリティ特性、セキュリティ機能）を満たす必要がある。 コンポーネントのベンダは、実装に関する主張を検証する。さらに、自動化されたテストスイートを使用して、コンポーネントのセキュリティ機能を検証する。
コンセプトレビュー	2 番目のレベルでは、チェックリスト方式ではなく、産業用データスペースの評価機関による詳細なレビューが必要である。このレビューには、提供されたコンセプトの評価と、実用的な機能テストとセキュリティテストが含まれる。
高レベルな保証機関	3 番目のレベルでは、機能テストとセキュリティテストに加えて、ベンダはすべてのセキュリティ関連コンポーネントのソースコードを提供しなければならず、評価機関による詳細なソースコードレビューが実施される。さらに、開発現場の監査等、開発プロセスの評価も行われる。

b セキュリティプロファイル

複数のコンポーネントが通信チャネルを確立する場合、データオーナー（多くの場合、データプロバイダと同一）がどの情報を通信相手に送るかの決定を行う上では、データコンシューマが持つコンポーネントに関する ID やセキュリティレベルに関する情報が不可欠である。そのため、（参加者とコンポーネントの両方の）ID やセキュリティレベルは、この情報を含むデジタル証明書の形で各コンポーネントから提供されなければならない。参加者証明書と同様のアプローチにより、データオーナー（多くの場合、データプロバイダと同一）とデータコンシューマは、データ交換時に使用されるコアコンポーネントに必要なセキュリティプロファイルを指定することができる。このため、IDS 認証スキームでは、コアコンポーネントについて 3 段階のセキュリティプロファイルを定義している。それぞれに求められるセキュリティ要件については、図表 5-55 の通りである。

図表 5-55　セキュリティプロファイルごとのセキュリティ要件

セキュリティプロファイル	求められるセキュリティ要件
ベースセキュリティプロファイル	ソフトウェアコンポーネントの限定的な分離、暗号化と完全性保護を含む安全な通信、コンポーネント間の相互認証、基本的なアクセス制御とロギングといった基本的なセキュリティ要件が含まれている。 ただし、セキュリティ関連データ（キーマテリアル、証明書）の保護や信頼性の検証は必要とされていない。永続的なデータは暗号化されず、コンテナ（5.3.1 (2) ク (ア)コンテナ化とリモート実行の保証）に対する完全性保護も提供されない。 したがって、このセキュリティプロファイルは、単一のセキュリティドメイン内の通信に使用される。
トラストセキュリティプロファイル	ソフトウェアコンポーネント（アプリケーション及びサービス）の隔離、隔離された環境での暗号鍵の安全な保管、暗号化、認証、完全性保護、アクセス及びリソース制御、使用制御、信頼できる更新メカニズム等の安全な通信が含まれる。永続的なメディアに保存されるデータ又はネットワークを介して送信されるデータはすべて暗号化されていなければならない。
トラスト＋セキュリティプロファイル	ハードウェアベースのトラストアンカー（TPM 又はハードウェアによる分離環境の形）が必要で、リモート完全性検証（リモート証明）をサポートする。すべてのキーマテリアルは、ハードウェアで隔離された専用エリアに保管される必要がある。

c コアコンポーネント証明書発行基準カタログ

IDS コアコンポーネントの認証基準カタログ（CRIT-C）は、フラウンホーファー研究機構の研究プロジェクトの一環として定義され、WG のメンバーと共に調整が行われた。このカタログは 3 つのセクションで構成され、IDS 固有の要件、業界標準 ISA/IEC 62443-4-2 から引用した機能要件、安全なソフトウェア開発のためのベストプラクティス要件からなる。各セクションは、一連の評価目標を対象として

おり、その内容は図表 5-56 の通りである。

図表 5-56 コアコンポーネント証明書発行基準カタログの評価目標

CRIT-C の各セクション	評価目標
IDS 固有の要件	機能性（IDS インフォメーションモデルのサポート等）とセキュリティ（IDS セキュリティアーキテクチャへの適合等）の両方に関して、コアコンポーネントの IDS リファレンスアーキテクチャモデルへの適合性を評価することを目標とする。
ISA/IEC 62443-4-2 の要件	認証プロセス中における認証情報のフィードバックの不明瞭化等、産業自動化や制御システム等の分野・業界全体で受け入れられている要件に関連して、実装された機能及びセキュリティ対策を評価することを目標とする。
ベストプラクティス要件	安全なソフトウェア開発を目的としており、設計文書、物理的なセキュリティ対策、テストプロセス等、コンポーネントの開発中のプロセスのセキュリティを評価することを目標とする。

IDS の参加者やコアコンポーネントの開発者の経済的な参入障壁を減らすため、コンポーネント認証のアプローチは、合理的な範囲で既存の認証スキームを使用するよう設計されている。そのような認証スキームが存在しない、あるいは広く認知されていない場合、例えば産業用データスペース特有の側面については、産業用データスペース認証スキームの中で定義された基準が採用される。

評価対象となるコアコンポーネントの機能及びセキュリティ要件は、IDS 参照アーキテクチャモデル、コネクタ仕様等の特定のコンポーネント仕様及び ISA/IEC 62443-4-2 等広く認知された要件カタログ（データの機密性やシステムの完全性等の機能要件）に基づいて定義される。また、ISA/IEC 62443-4-2 で定義されているように、コンポーネントのライフサイクルを通じて、セキュリティ要件の徹底的な抽出、アーキテクチャレベルでのセキュリティ要件の実施、安全な実装レベルまでの追跡、関連ガイダンス文書、検証・確認アプローチ、安全欠陥管理、安全更新管理等の適切な手段を求めることで、各種保証レベルでの評価を支援・促進することが可能である。

d コアコンポーネント別の特記事項

証明書発行の対象となるコアコンポーネント別の特記事項は図表 5-57 の通りである。

図表 5-57 証明書発行に関するコアコンポーネント別の特記事項

コアコンポーネント	特記事項
コネクタ	産業用データスペースへのアクセスポイントであるコネクタは、データの処理と交換のための制御された環境を提供し、データプ

コアコンポーネント	特記事項
	ロバイダからデータコンシューマへの安全なデータ転送を保証する。そのため、IDS リファレンスアーキテクチャモデル及びコネクタ仕様で要求される機能の正確かつ完全な実装に必要な信頼は、承認された評価機関並びに産業用データスペースの証明書発行機関からの独立した評価及び認証によってのみ確保されることができる。
メタデータブローカー	メタデータブローカーサービスは、一次データにはアクセスできず、データプロバイダから提供されるメタデータにのみアクセスする。 同様に、メタデータブローカーサービスはアクセス権を割り当てたり強制したりせず、単にデータ交換をサポートするのみである。しかし、メタデータの完全性と可用性（メタデータを正しく安全に保存し、取り扱うこと）の確保は非常に重要である。そのため、証明書発行機関が定義する必要な機能との互換性の評価を通じた証明書の発行プロセスが必要となる。
データアプリ	アプリケーションは一次データに直接接触するため、アプリケーションが侵害されると、データの完全性が損なわれる可能性がある。 しかし、（データアプリを含む）アプリケーション及びサービスは、通常はコネクタによって提供されるセキュリティ機能を使用することになる。したがって、IDS で利用可能になるすべてのアプリケーションやサービスに高い保証レベルの認証が必要なわけではない。
アプリストア	アプリストア自体は一次データに直接触れることはないが、アプリストアが提供するアプリは一次データに触れる。アプリストアのセキュリティ、特にアプリやサービスのアップロード時に使用されるテストスイートが侵害された場合、侵害されたアプリやサービスが流通する可能性がある。そのため、要求される機能及びセキュリティ機能との互換性の評価を通じた証明書の発行プロセスが必要となる。
ハードウェア	IDS リファレンスアーキテクチャモデルで定義されている特定のセキュリティプロファイルでは、機密データへのアクセスに対する適切なレベルの保護を実現するために、追加のハードウェアセキュリティコンポーネ ントが必要となる。 産業用データスペースのコアソフトウェアコンポーネントに加えて、これらのハードウェアコンポーネントも認証の文脈で考慮されなければならない。 信頼性の観点から、また二重認証を避けるために、第三者認証のハードウェアコンポーネント（例：保護プロファイル BSICC-PP-0030-2008 又は ANSSI-CC-PP-2015/07 に従って認証された Trusted Platform Modules）の使用が要求されることになる。これらのコンポーネントに関する産業用データスペースの認証活動は、既存のベース証明書の有効性を確認することに限定される。

ウ 証明書発行の具体的プロセス

証明書発行までのプロセスは、申請・評価・証明書発行の 3 フェーズに分かれる。

証明書発行機関が発行する IDS 証明書には有効期限があり、有効期限が切れる前に証明書を更新するためには、その間に起こった関連する外部動向を考慮し、再認証を行う必要がある。また、認証対象が変更された場合も同様に再認証が必要である。

後続の認証・認可のためには、各 IDS コンポーネントは有効な X.509 証明書を有していなければならない。X.509 証明書は、IDS 証明書の発行をトリガーとして CA が発行する（「5.2.1 (1) オンボーディング」）。この X.509 証明書と動的属性トークンの発行により、IDS 内でのデータ転送前に参加者間の認証・認可が可能となる。

(ア) 申請フェーズ

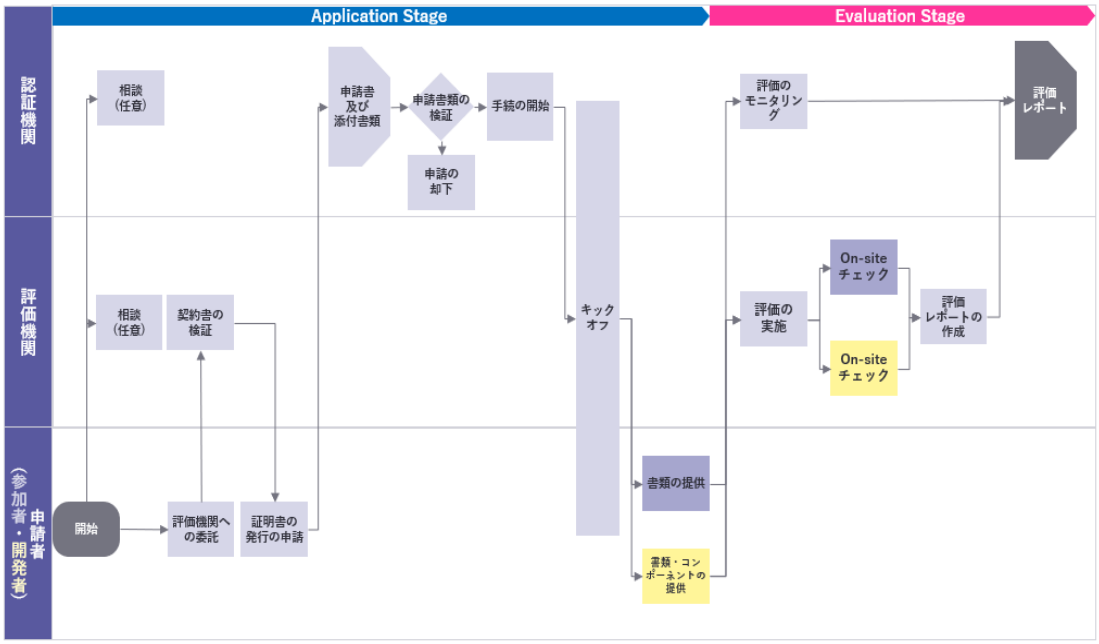
当フェーズの主な目標は、IDS の評価と証明書発行フェーズを正常に開始することである。申請者は、IDS 証明書発行スキーマに従って評価を実施するために、証明書発行機関によって承認された評価機関から選択する。申請者は、証明書発行機関が申請を確認するために必要な証拠を提供しなければならない。申請者が受け入れられた場合、評価手続が開始され、すべての関係者とのキックオフが行われる。

(イ) 評価フェーズ

当フェーズの主な目標は、定義された評価基準に基づいて申請者又はコアコンポーネントを評価することである。評価機関は、詳細な結果を評価報告書として文書化する。IDS 認証スキーマからの逸脱が確認された場合、その是正措置の実施は申請者の責任となる。この評価は、IDS 認証スキームが正しく実施されているか、証明書発行機関により監視される。

申請フェーズ及び評価フェーズは図表 5-58 のように示すことができる。

図表 5-58 証明書発行フロー（申請フェーズ及び評価フェーズ）
（「WHITE PAPER CERTIFICATION FRAMEWORK FOR THE IDS CERTIFICATION SCHEME」より EY 作成）

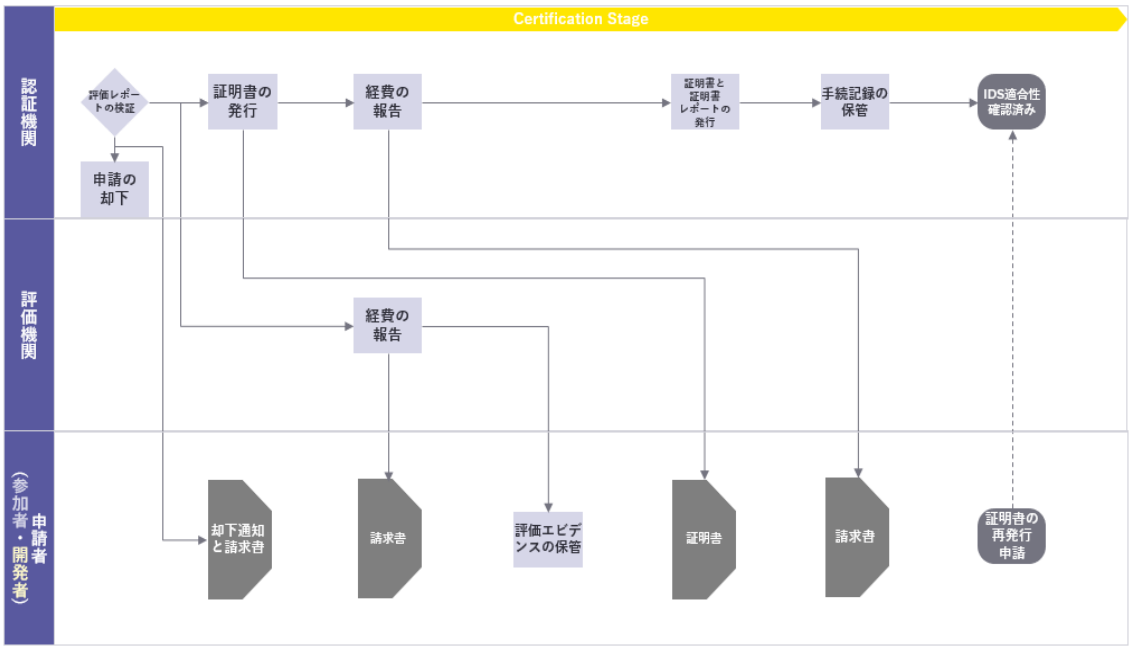


（ウ）証明書発行フェーズ

当フェーズの主な目標は、証明書発行機関による評価レポートの審査であり、評価プロセスの結果が肯定的であれば、IDS 証明書が発行される。証明書発行機関は、評価機関から評価報告書を受領し、認証の授与又は拒否に関する最終的な決定に責任を負う。判定が肯定的な場合、申請者は IDS に適合していることが確認される。証明書発行機関は証明書を発行する。

証明書発行フェーズは図表 5-59 のように示すことができる。

図表 5-59 証明書発行フロー（証明書発行フェーズ）
（「WHITE PAPER CERTIFICATION FRAMEWORK FOR THE IDS CERTIFICATION SCHEME」より EY 作成）



(2) 認証・認可の仕組み

データ交換の機密性と真正性を確保するために、コネクタ間の通信は保護されなければならない。 IDS コネクタを使用する場合、2 つのレイヤーのセキュリティが確保される。このレイヤーは、暗号化トンネル（TLS 等）を使用したポイントツーポイント暗号化（コネクタ間）及びエンドツーエンド認証（アプリケーション間）から構成される。ある外部コネクタから別のコネクタへのデータは、インターネット又は仮想プライベートネットワーク（VPN）を介して送信されるが、その仕様は IDS セキュリティアーキテクチャの範囲外である。

セキュリティアーキテクチャは、IDS 通信プロトコル（IDSCP; IDS Communication Protocol。以下、「IDSCP」という。）を定義する。IDSCP は信頼されたコネクタによってサポートされなければならず、他のコネクタによってもサポートされることができる。IDSCP の目的は、機密性、認証された通信を確立し、データプロバイダとデータ消費者の間でデータを交換し、相互のリモート認証を確立することである。

IDS コネクタは、図表 5-60 に示すように、暗号化トンネル（TLS 等）を介して互いに通信する必要があり、IDSCP の他に https 及び mqtt 等の他の適切なプロトコルを使用することができる。

図表 5-60 IDS における通信

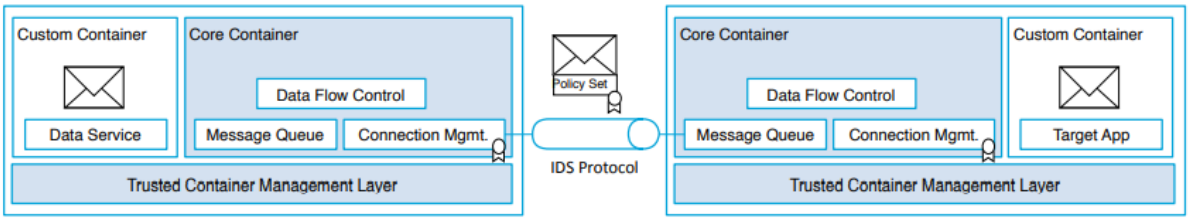


Figure 4.1: IDS Communication

IDSCP は、WebSocket over TLS（WSS）を介して確立された高レベルのプロトコルである。これにはいくつかの「会話」が含まれており、どちらか一方から開始することができ、相手側から確認されなければ「会話」に入ることができない。現在提供されているのは、リモート認証とメタデータ交換の 2 つの「会話」である。プロトコル自体はトンネル接続の内部で実行される。このプロトコルを用いることにより、識別と認証、リモート認証、メタデータ交換、データ交換（利用ポリシー情報付き）が可能となる。データ交換の際には、データ利用者がどのようにデータを利用するかを指定するためのユーセージポリシーに関する情報を添付することが可能であり、ユーセージコントロールの基本的な仕組みを提供するものである。

ア ID 管理

各参加者が他の参加者の ID やプロパティに基づいてアクセスコントロールに関する決定を行えるようにするためには、ID とアクセス管理（IAM）のコンセプトが必須である。この概念では、識別、認証及び認可の側面が中心である。CA はすべてのエンティティに対して証明書を発行する。これらの証明書は、コネクタ間の認証と暗号化に使用される。ID は、その ID に紐づけられる複数の属性を持つことができる。DAPS は、参加者とコネクタに関する動的な最新の属性情報を提供するために使用される。

イ 参加者証明書とコアコンポーネント証明書の ID 管理へのマッピング

証明書発行の対象は 2 つあり、参加者（参加者証明書）とコアコンポーネント（コアコンポーネント証明書）からなる（「5.3.1 (1) イ 申請者とコアコンポーネントへの証明書発行」）。参加者（企業等）は、参加者証明書とコアコンポーネント証明書を証明書発行機関から受けることで、IDS に参加することができる。参加者は、参加者証明書とコアコンポーネント証明書の両方の証明書を使用し、識別、認証及び暗号化のためのデジタル X.509 証明書を要求することができる。

X.509 証明書には、企業の所在国や企業名、部署名、グローバル一意識別子（UUID）、

サブジェクト代替名（X.509 X509v3 Subject Alternative Name）等の静的な情報のみが含まれる。

属性の変更は、証明書の失効と再発行につながるので注意が必要である。このため、証明書に含まれる属性の数は最小限にとどめる必要がある。動的属性は、動的属性提供サービス（DAPS）により保持される。

ウ 公開鍵基盤（PKI）の階層化に関する提案

一般的に、公開鍵基盤（PKI）には階層構造を持たせることができる。適用されるビジネスモデルやデプロイモデルによっては、複数の Sub-CA を存在させることにより、特定の当事者が特定の目的のために証明書を発行することができる。PKI 構造は IDS では定義されないが、その概要は図表 5-61 で示されている。

図表 5-61 PKI の階層化例（概念図）

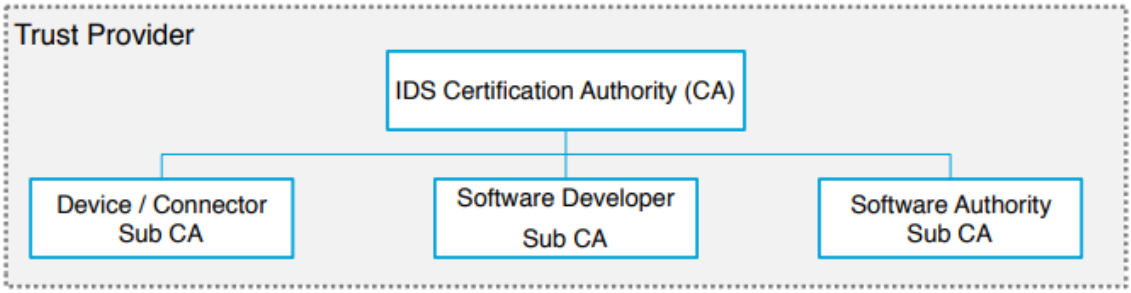


Figure 4.2: PKI structure (example)

エ コネクタ証明書のデプロイ

属性の変更は、証明書の失効と再発行につながるので注意が必要である。このため、証明書に含まれる属性の数は最小限にとどめる必要がある。動的属性は、動的属性提供サービス（DAPS）により保持される。コネクタ証明書の受領後、参加者はコネクタ証明書をコネクタにデプロイすることができる。X.509 証明書は、データが常に認証され、暗号化された方法で交換されることを保証する。

オ ID 管理のための動的属性提供サービス（DAPS）の利用

DAPS を利用してコネクタに動的属性に関する情報を渡すことで、証明書の失効を減らし、IDS の参加者がより柔軟に属性を扱えるようにする。

DAPS は、コネクタインスタンスに属性とステータスフラグを動的に割り当てることができる。ステータスフラグの例としては、既知の脆弱性が修正されていない場合にセキュリティステータスを撤回することや、X.509 証明書を再発行することなく、認証ステータスをアップグレードすること、契約者のいるワークフローに会員ステータスを割り当てること、参加者の信頼レベルの一時的な変更を通知すること、変更可能な属性（組織の住所等）を提供すること等が挙げられる。参加者は必要に応じて新

しい動的属性を含めることができるため、X.509 証明書の失効を回避することができる。

DAPS は、データコンシューマ又はデータプロバイダからのリクエストを受け、動的属性トークン（DAT）を発行する。その具体的な手順は図表 5-62 の通りである（詳細は後述）。

なお、図表 5-62 に記載の IDS Operating Company に関する具体的な記述は IDS のドキュメントからは確認することができなかった。

図表 5-62 DAT 発行プロセス（概念図）

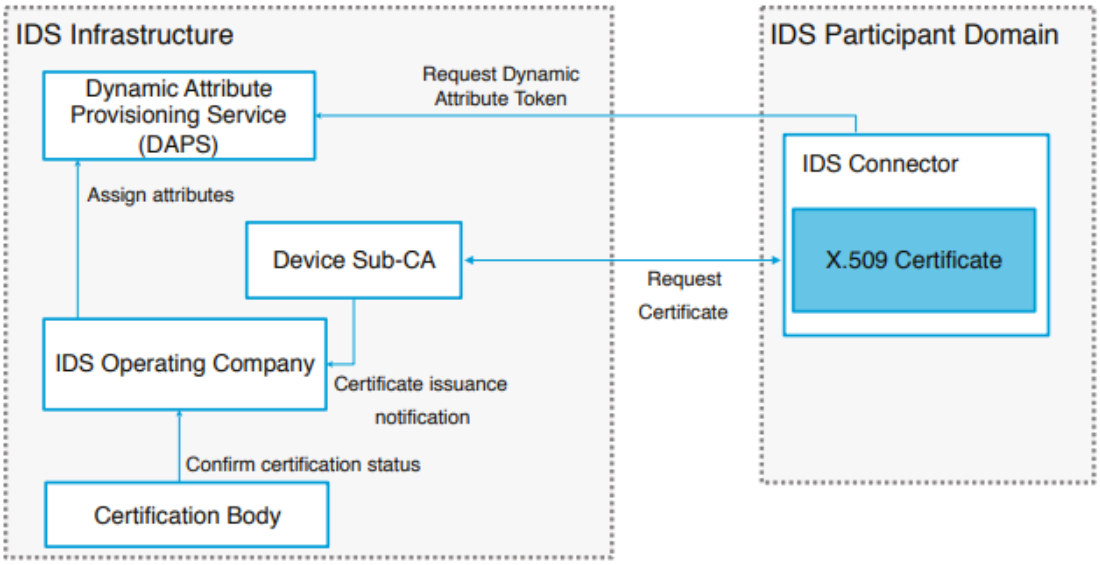


Figure 4.3: Embedding the Connector Certificate

カ　認可サービスによるリソースへのアクセスコントロール

認可サービス（アクセストークンを使用）の利用により、ユースケース別のアクセスコントロールに関する決定のモデル化やアクセス判断の委譲が可能となる。複雑なワークフローでは、複数のコネクタが専用の認可サービスを使用して、リソースへのアクセス決定を委譲することができる。DAPS は、IDS の認可サービスとして機能する。

動的属性とアクセストークンを使用してリソース（データサービス等）にアクセスする手順は、次のように定義される。

- 動的属性トークン（DAT）を DAPS にコネクタの X.509 証明書を提示して要求する。指定された検証ポリシーにより、属性は CA で検証することができる。
- リソースにアクセスする前に、同じ X.509 証明書を使用して通信経路暗号化のための TLS トンネルが確立される。ここでも、指定されたポリシーに応じて、証明書は CA で検証することができる。
- （オプション）複数のアクセストークン（AT）を使用する場合、ユースケースオ

ペレータのドメイン並びにコネクタ又はより具体的にはリソースの所有者のドメイン内の別の認可サービスでトークン要求が実行される。
- リソースは、DAT 又は AT のいずれかを渡すことによって要求される。

上記の手順を図示すると、図表 5-63 の通りとなる。

図表 5-63 リソースへのアクセスコントロール（概念図）

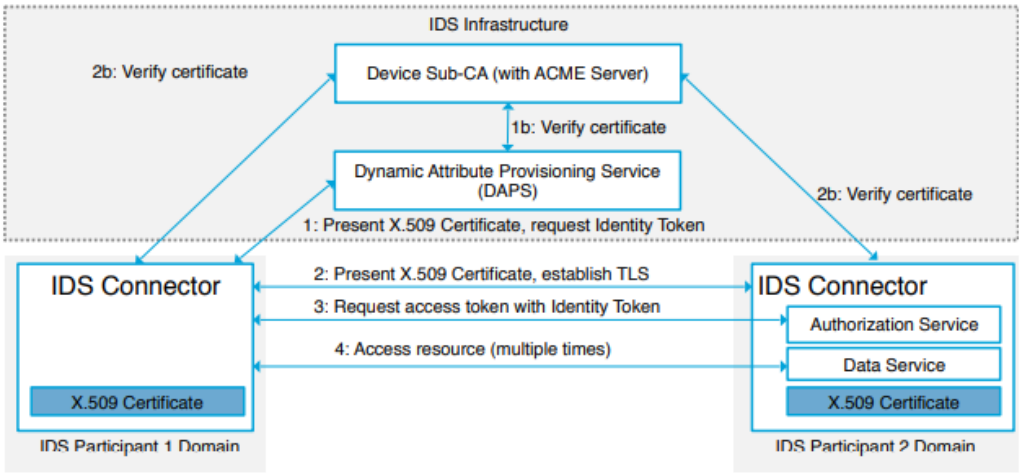


Figure 4.4: Resource access workflow

アクセストークンのデータサイズは小さいため、これらのトークンをあらゆるリソースへのアクセス要求に組み込むことができ、ステートレスなアクセスコントロールをサポートすることが可能である。DAT と AT はともに JSON Web Token（IETF RFC 7519）を使用している。

キ トラスト管理

参加者を不正から守り、指定されたルールを遵守させるため（トラスト管理）、IDS は暗号を利用している。その方法の 1 つが公開鍵基盤（PKI）である。PKI の中心原理は、各エンティティに秘密鍵が割り当てられ、その秘密鍵に対応する公開鍵は各エンティティに公開されており、その公開鍵を用いて各エンティティが他の参加者に対して認証を行うことができるようになることである。IDS は、PKI に基づいて、ID プロバイダが他のエンティティに証明書を発行し、そのエンティティが他のエンティティに証明書を発行するといった階層の形成を提案している（前述）。この概念図は図表 5-64 の通りである。

図表 5-64 IDS における PKI の階層化

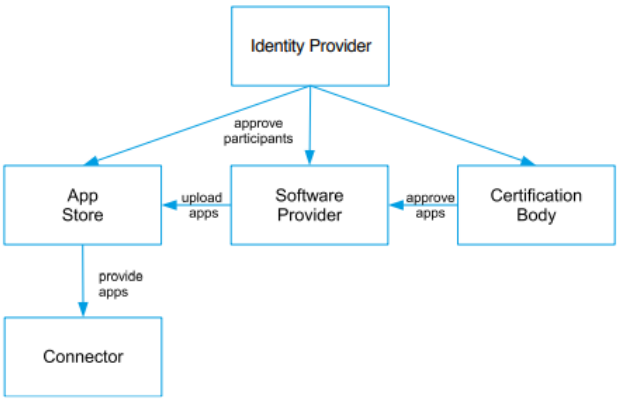


Figure 4.5: Technical roles in the International Data Spaces

以下、IDS に必要な役割とエンティティをマッピングするための PKI のデプロイについて説明する。

（ア）公開鍵基盤（PKI）実装における参加者の役割等

IDS は、安全な ID 管理を保証するために、各参加者の役割をサポートするのに十分な柔軟性を持つ PKI システムを実装するための技術的な役割を定義している。特に以下 6 つの参加者やコンポーネントが関連しており、それぞれの技術的役割やそれらのインタラクションについては図表 5-65 の通りである。

図表 5-65 公開鍵基盤（PKI）実装における参加者・コンポーネントの役割等

参加者・コンポーネント	技術的役割及び他の参加者とのインタラクション
ID プロバイダ	• IDSA の代理人として活動する。IDS の参加者になることを承認された当事者に対して、技術的な ID を発行する責任を負う。ID プロバイダは、承認された役割（アプリストアプロバイダやアプリプロバイダ等）に基づいて ID を発行するよう指示される。このような ID を持つ参加者やコンポーネントのみが、IDS 上でデータ提供やアプリケーションの公開等の様々な活動を行うことができる。ID プロバイダは、指示があれば、参加者を IDS から排除することができる。 • ID プロバイダは PKI のデプロイの管理を担い、証明書の有効期限切れや失効する場合に対処する。 ソフトウェア署名用（ソフトウェア署名ルート CA）とコネクタ用（サービスルート CA）の 2 種類の PKI 階層を想定しており、エンティティには、エンド証明書とサブ・ルート CA 証明書のいずれかが割り当てられる。この 2 つの階層が、6 つのエンティティの利益を保護する。また、ID プロバイダは DAPS を組み込むことで、認可サービス（前述）としても機能する。

参加者・コンポーネント	技術的役割及び他の参加者とのインタラクション
ソフトウェアプロバイダ	• IDS への加入を希望するすべてのソフトウェアプロバイダに対して、ID プロバイダはサービスサブ CA 要求を発行する。 • 承認されたソフトウェアプロバイダは、コネクタのロールアウト及び配備の間、初期の有効な事前設定されたシステムを提供するために、サービスサブ CA 使用する。
コネクタ	• コネクタは、承認されたソフトウェアプロバイダから取得した場合にのみ、他のコネクタとの通信が許可される。 • コネクタは、アプリストアからアプリケーションをダウンロードする。ダウンロードされた各アプリケーションについて、コネクタはサービスキーペアと証明書署名要求（CSR）を作成する。秘密鍵はアプリケーションの識別とデータ保護に使用され、CSR はアプリストアに送信され、アプリストアはそれを使用して証明書を発行する。これにより、エンティティは、あるアプリケーションのライセンスの有効性を確認することもできる。さらに、秘密鍵と証明書は、他のコネクタと安全なチャネルを確立するために使用される。 • ソフトウェアプロバイダは初期システムをコネクタに展開し、初期システムに対するコネクタの対応するサービス CSR に署名する。サブ CA は、他のコネクタによってダウンロードされたサービスの有効性を保証するために、アプリストアによって使用される。つまり、アプリストアが CSR に署名（すなわち、証明書を発行）すると、コネクタはダウンロードされたアプリケーションの証明書を受け取ることになる。
アプリプロバイダ	• 証明書発行機関にアプリケーションの証明書発行を求める。 • アプリケーションの証明書発行に成功した場合、アプリストアにアプリケーションをアップロードすることで、アプリケーションを公開することができる。 • 各アプリプロバイダは、ID プロバイダが発行する証明書により一意に特定することができる。
証明書発行機関	• 証明書発行機関は、アプリプロバイダがアプリケーションをアップロードする際に、当該アプリケーションが承認されたアプリプロバイダによるものかどうかを確認するのみならず、当該アプリケーションが一定の品質及びセキュリティ基準を満たしているかどうかも確認する。そのため、アプリプロバイダはアプリケーションを証明書発行機関に送付し、検査を受けなければならない。 • 証明書発行機関は、アプリプロバイダの署名の有効性を確認する。署名が有効である場合、それぞれのアプリケーションのソースコードが検査される。アプリケーションが品質とセキュリティの基準を満たしている場合、証明書発行機関は証明書の秘密鍵でアプリケーションに署名する。その際、署名のみで証明書を作成しないため、サブ CA は不要である。

（イ）コネクタのマニフェステーション

コネクタは内部にアプリケーションをインストールすることによって、さまざまなサービスを実行し、他のコネクタと通信することができる。認証や機密性の観点では、コネクタは公開鍵基盤（PKI）を使用することで、そのサービスの永続的な保存と他のコネクタとの通信を保護する。

各コネクタは、アプリケーション等に対する PKI 署名を検証できるよう、信頼できるルート証明書（サービスルート CA 及びソフトウェア署名 CA）について、整合性を保つことができる方法で保存する（コネクタのマニフェステーション）。上記に関する概念図は図表 5-66 の通りである。

図表 5-66 コネクタの役割とマニフェステーション（概念図）

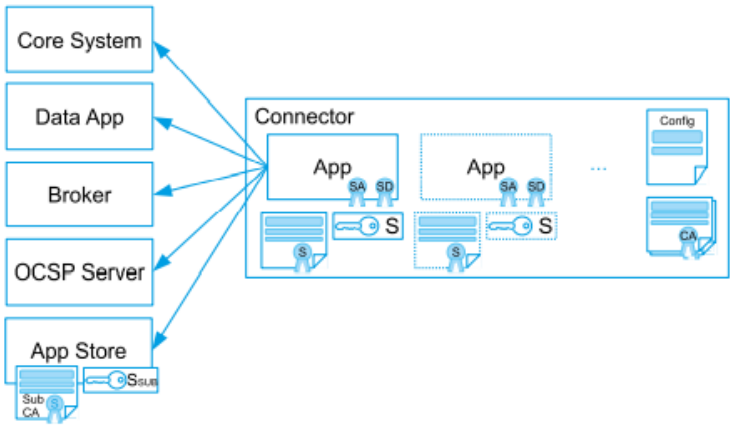


Figure 4.7: Connector roles and manifestations

（ウ）コネクタに実装されるアプリケーション

IDS でアプリストアを介して提供されるアプリケーションは、コネクタ内にある隔離されたコンテナ内で実行される。コネクタは、ダウンロードするすべてのアプリケーションに対してキーペアを作成する。秘密鍵は、アプリの永続的なデータを保護する。アプリストアからアプリをダウンロードする際に、コネクタは公開鍵を使用して CSR を作成する。アプリストアは CSR に署名し、証明書を発行する。コネクタはこの証明書を使用して、実行中のアプリが有効であることを確認する。

アプリストアは、サービスサブ CA を持つ。IDSA は、新規のアプリストアが開設されるたびに、この CSR に署名する。これにより、参加者はアプリストアを識別し、アプリケーションを要求するコネクタからのサービス CSR に署名することができるようになる。

コネクタに実装されるアプリケーションの種類は図表 5-67 の通りである。

図表 5-67 コネクタに実装されるアプリケーションの種類

アプリケーションの種類	概要
コアシステム	各コネクタは、それぞれにつき 1 つのコアシステムを実行する。コアシステムとその証明書は、コネクタを提供するソフトウェアプロバイダから取得された、コネクタにデプロイされる。 コアシステムの証明書は、基礎となるハードウェアデバイスを識別する。コアシステムは、他のコネクタに接続することができる（たとえば、アプリのダウンロードのためにアプリストアと通信する等）。コネクタが他のコネクタとの通信チャネルを確立する際には、コアシステムの秘密鍵及び証明書を認証に使用する。
データアプリ	データ処理やデータ収集のためのアプリケーション又はシステムアダプタのことである。
メタデータブローカー	メタデータブローカーサービスを提供するコネクタのことである。
OCSP サーバ	コネクタが OCSP サーバアプリを実行する場合、コネクタは OCSP サーバとみなされる。

(エ) データアプリの開発と実装

以下では、IDS で使用されるデータアプリのライフサイクルを、アプリ開発からコネクタへのデプロイまでの時系列順に説明する。

- ID プロバイダは、IDSA に代わって各ソフトウェアプロバイダのキーペアと証明書に署名する。アプリ開発が完了し、提供する準備が整うと、ソフトウェアプロバイダはその秘密鍵を使用してデータアプリに署名し、署名されたデータアプリは信頼できる証明書発行機関に送信される。
- 証明書発行機関がデータアプリを承認した場合、データアプリに 2 つ目の署名が追加される。
- ソフトウェアプロバイダがデータアプリをアプリストアにアップロードすることで、そのデータアプリを IDS 参加者が利用できるようになる。アプリストアは、有効な（すなわち、正しく署名された）データアプリのみを受け入れる（アプリストアは対応するルート CA とのコネクタであるため、すべての署名を確認することができる）。
- データアプリをダウンロードするコネクタは、アプリストアと接続する。コネクタは、サービスキーペアと CSR を作成し、サービスのダウンロードを要求し、CSR をアプリストアに送信する。アプリストアは、サービスサブ CA を使用して CSR に署名し、それをコネクタに返送する。
- コネクタはデータアプリをダウンロードし、その署名を確認する。署名が有効であることが確認されると、コネクタはデータアプリをインストールする。コネクタは、受領した証明書に基づいて、ダウンロードしたデータアプリの有効性を確認することができるようになる。

上記のプロセスは、図表 5-68 のように示される。

図表 5-68 データアプリの開発・承認・ダウンロードフロー

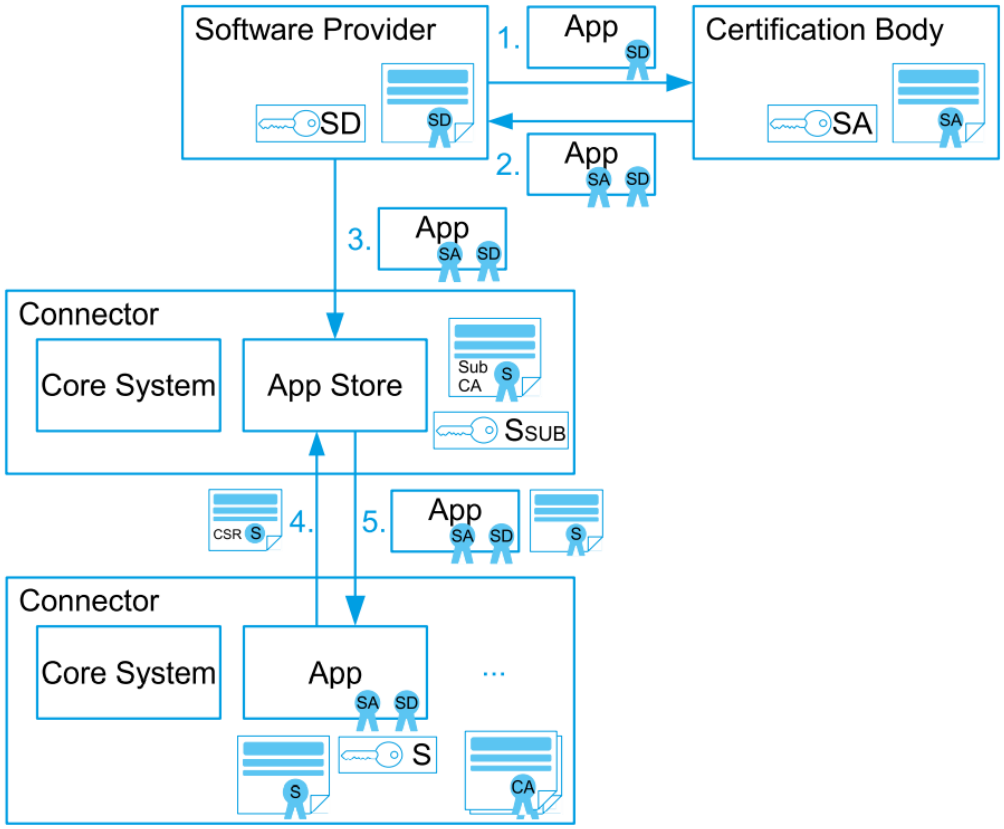


Figure 4.8 Software development, approval, and download process

(オ) コネクタのデリバリ

コネクタの初回デプロイに際して、コネクタはコンフィギュレーションされた状態でオペレータ（データプロバイダやデータコンシューマ等）に提供される。コネクタのデプロイのため、ソフトウェアプロバイダは署名を行うためのサブ CA キーペアと CSR（アプリストアプロバイダと同様）を保持している。ID プロバイダがサブ CA の CSR に署名すると、要求しているソフトウェアプロバイダが IDS の規制とポリシーに準拠していることが確認される。コネクタのオペレータは、必要に応じてコンフィギュレーションやルート証明書、コアシステムを変更することができる。

(カ) コネクタのセキュリティプロファイル

IDS は各参加者の個々のセキュリティニーズに対して柔軟であり続けるように設計されており、各参加者が各参加者によりカスタマイズされた基準に基づいてアクセスコントロールを決定できる余地を残している。アクセスコントロールポリシーは、コネクタの一連の属性に基づくことができる。これらの属性には、一意の識別子やデータアプリのセキュリティレベル、コネクタコンフィギュレーションのセキュリティ特性及び参加者の組織としてのケイパビリティを説明する一連のプロパティが含まれている。このセキュリティプロパティのセットは、セキュリ

ティプロファイルと呼ばれる。

セキュリティプロファイルはコネクタの属性で構成され、属性ベースのアクセスコントロールポリシーで使用される場合がある。各コネクタは、他の参加者による要求に応じてそのセキュリティプロファイルを提供しなければならない。

セキュリティプロファイルの情報に基づいて、データコンシューマはデータプロバイダのエンドポイントによって提供されるデータを信頼するかについて決定することができ、データプロバイダは機密データをデータコンシューマに提供してもよいかどうかを決定することができる。

IDS は 4 種類の異なるセキュリティプロファイルを定義している（「5.3.1 (1) イ (イ)b セキュリティプロファイル」を参照されたい[179]）。それぞれのセキュリティプロファイルに応じたコネクタの主な特徴や利用範囲については図表 5-69 の通りである[180]。

図表 5-69 セキュリティプロファイル別のコネクタの主な特徴や利用範囲

セキュリティプロファイル	利用範囲や主な特徴
ベースフリー	• 誰でも自由に利用・再利用・配布が可能であり、任意のデータソースへの接続を実現するための API 仕様を提供する。 • データソースアダプタを使用し、自身のデータソースやその他のデータソースを接続することができる。コネクタの機能範囲を個々のニーズに応じて拡張することが可能。 • ベースフリーのコネクタに関しては、IDS 外部における利用範囲に留まる（例：研究プロジェクトや社内ネットワーク等特定のセキュリティドメイン内での運用）。
ベース	
トラスト	• オープンな IoT ゲートウェイプラットフォームであり、DIN Spec 27070 及び ISO 62443-3 規格に準拠している。 • 多くの種類のプロトコルアダプタを用いることで、クラウドサービスや他のコネクタとの接続が可能である。 • ユースケースの一つとして、IoT 機器のセンサー同士の連携が挙げられる。
トラスト＋	

セキュリティプロファイルの属性は IDS リファレンスアーキテクチャモデルの付録 B に記載されている[181]。属性は、すべての IDS 参加者及びコネクタの「共通

[179] 4.3.1 5.3.1 (1) イ（イ)b では、証明書発行が必要なレベルとしてベース、トラスト、トラスト＋の 3 段階を紹介した。ここでは、証明書不要で IDS のエコシステム外での利用を想定したベースフリーが含まれていることに留意されたい。

[180] “GitHub -IDS Trusted Connector” GitHub, https://industrial-data-space.github.io/trusted-connector-documentation/docs/overview/（2022 年 3 月 17 日アクセス）及び“Open Data Connector”, Fraunhofer, https://www.dataspaces.fraunhofer.de/en/software/connector/open_data_connector.html（2022 年 3 月 17 日アクセス）。

[181] *REFERENCE ARCHITECTURE MODEL 3.0*, INTERNATIONAL DATA SPACES ASSOCIATION, December 2020, p111-p115, https://internationaldataspaces.org/wp-content/uploads/IDS-Reference-Architecture-Model-3.0-2019.pdf, 16 March 2022（2022 年 3 月 27 日アクセス）

認識」を定義し、異なるセキュリティプロファイルを区別するため、図表 5-70 の通り 4 つの側面から定義されている。ベースフリー～トラスト＋の各レベルに対応する 4 つの側面におけるセキュリティプロファイルの仕様は、図表 5-70 の通りである。

図表 5-70 セキュリティプロファイルの 4 つの側面

各側面	概要
開発	コンポーネントの開発に関する要件及び能力に関連する。
サポートされる IDS の役割	それぞれのセキュリティプロファイルによってサポートされる IDS 参加者の役割に関連する。
サポートされる通信能力	それぞれのセキュリティプロファイルによってサポートされる通信機能を規定する。
セキュリティ機能	それぞれのセキュリティプロファイルによって提供されるセキュリティレベルを規定する。

図表 5-71 セキュリティプロファイルと各側面の関係

	Base Free	Base	Trust	Trust+
Development	Developed as Open Source	Developed in the IDSA Community	Developed in the IDSA Community	Developed in the IDSA Community and bound to strong SLA regarding security updates.
IDS Roles supported	Not certified, therefore the public IDS infrastructure is not available	All IDS Roles (section 3.1.1) supported, but support for Clearing House is optional	All IDS Roles (section 3.1.1) supported,	All IDS Roles (section 3.1.1) supported,
Communication abilities supported	Cannot connect to public IDS services or connectors.	Can connect to other connectors and exchange data.	Can connect to other connectors and exchange data. Can refuse a connection with a Connector with Base Profile.	Can connect to other connectors and exchange data. Can refuse a connection with a Connector with Base Profile.
Higher security features	Security level not defined	Standard security level	Extended security level	High security level

Table 4.1: Overview of IDS Security Profiles and related dimensions

ク トラストプラットフォーム

IDS は、コネクタアーキテクチャ（メタデータブローカーやアプリストア等で使用されている）の複数のマニフェステーションで構成されている。このため、信頼できるプラットフォームは、信頼できるデータ交換の中心的な要素となっている。トラストプラットフォームの重要な観点は以下 3 点である。

- データ交換を希望する参加者間で必要最小限の要件を指定できるようにするため、互いのセキュリティプロファイルに関する共通の理解を確立する必要がある。コネクタは、これらのプロファイルの相互検証をサポートする。
- データアプリの信頼できる実行を可能にし、システムの完全性を保証するために、コンポーネントの強力な分離が必要である。コネクタ内にあるアプリケーションのコンテナ管理は、展開されたデータアプリケーションの完全な分離と、不正な通信チャネルの制限をサポートする。これは、データアプリが明示的に意図されたデータのみにアクセスできることを意味する。
- 別の参加者との信頼関係を確立し、コネクタのプロパティを検証するため、リモート完全性検証が必要である。コネクタは、ハードウェアベースのトラストアンカーと、信頼できるソフトウェアを備えている。

（ア）コンテナ化とリモート実行の保証

コンテナ化は、データアプリのランタイム環境に対する完全性の強制の一形態である。図表 5-72 に示すように、データアプリをそれぞれ別のコンテナ内に配置することで、データアプリを互いに分離することができる。これにより、完全なコンテナのインスタンス化に対する有効期限ポリシーの実施等、追加のセキュリティ機能の実装が可能になる。コネクタは、アプリケーション同士の干渉を防ぐために、データアプリ、システムアプリ及びコアプラットフォームを互いに分離する何らかのメカニズムを提供する必要がある。各コネクタには、その分離機能を説明するセキュリティプロファイルが付属している。データアプリのユーザは、セキュリティプロファイルに記載されている分離機能のセットに基づいて、データのアクセスコントロールに関する決定を行うことができる。

図表 5-72 コンテナ化によるデータアプリの隔離

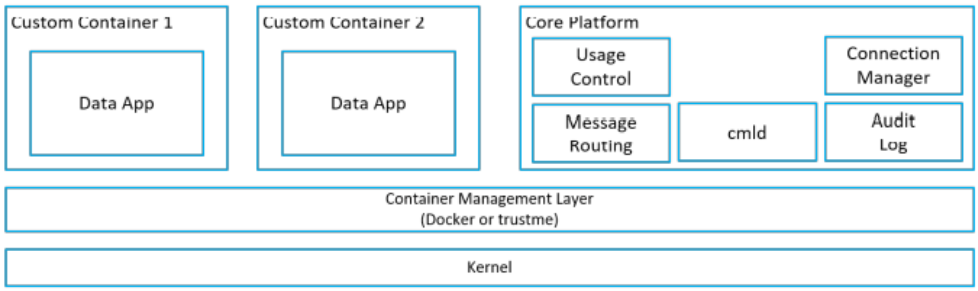


Figure 4.10: Container isolation for Data Apps

（イ）リモート完全性検証

IDS では図表 5-73 の通り 2 種類の検証をサポートしている。リモート完全性検証は、参加者間の ID 検証による当事者の ID に対する信頼の確保を前提として、各コネクタのソフトウェアスタックの完全性の検証によって実現される。

図表 5-73 参加者間の ID 検証と各コネクタのソフトウェアスタックの完全性検証

2 種類の検証	概要
参加者間の ID 検証	両参加者が信頼するエンティティ（信頼できる PKI によって署名された Credential 又は信頼できる ID プロバイダによって発行された ID トークン等）から発信された Credential を交換する。
各コネクタのソフトウェアスタックの完全性検証	信頼できるプラットフォームモジュールを使用した完全性に関する測定を実施し、リモート認証による各コネクタのソフトウェアスタックの完全性の検証を行う。

コネクタのソフトウェアスタック及びコンフィギュレーションの完全性の検証は、信頼できるデータアプリをデプロイするために必要である。完全性が検証されない場合、以下のような問題が発生するおそれがある。

- 悪意のあるコネクタが実際よりも高いセキュリティレベルを保持していること偽装するために、認証され信頼されたソフトウェアスタックを実行するように装う可能性がある。
- コネクタが期待通りにデータアプリを実行しない可能性がある。データアプリが CPU 及びメモリに関して必要とする量の計算リソースを利用できないために実行も通信も信頼できない場合、そのコネクタプラットフォームで実行されているデータアプリによって消費及び提供されるデータは、信頼できない。
- データコンシューマがデータアプリをデータソース（リモートコネクタ）にプッシュするエッジコンピューティングの場合は、これらのデータアプリの正しい実行が保証されないため、実装が困難となる可能性がある。

コネクタがソフトウェアスタックの完全性と他のコネクタのランタイム構成に関する技術的に信頼できる情報を取得できるよう、コネクタはより安全なコネクタインスタンスのためにリモート認証をサポートすることができる。信頼性を確保する手段として、例えばコネクタで TPM1.2/2.0 又は同等のセキュリティ対策を適用することが可能である。

（ウ）動的トラストモニタリング（DTM）

上記のリモート完全性検証はコネクタの現在のステータスのみを検証することができるが、動的信頼モニタリング（DTM）は、より長い期間にわたってコネクタの完全性を検証することを意図している。さらに、DTM は、完全性違反の重大性に応じて、参加者への単純な通知から X.509 証明書の失効に至るまで、特定のアクションを起動することが可能である。

(3) エンフォースメント

ア アクセスコントロールとユーセージコントロール

一般的に、情報セキュリティ分野におけるアクセスコントロールとは、リソースへのアクセスを制限することを指す。権限付与とは、リソースに対して許可を与えることである。アクセス制御には、裁量アクセス制御（DAC)、強制アクセス制御（MAC)、役割ベースアクセス制御（RBAC)、属性ベースアクセス制御（ABAC）等、いくつかのモデルが存在する。RBAC と ABAC は最も頻繁に使用されるモデルである。

アクセス制御の分野でよく使われる用語を紹介するために、ここでは XACML（eXtensible Access Control Markup Language）規格を用いる。XACML とは、ABAC のルールを表現するためのポリシー言語である。この言語の主な構成要素は図表 5-74 の通りである。サブジェクト、アクション、リソース及びコンテキストである。

図表 5-74 XACML の構成要素

構成要素	概要
サブジェクト	データアセットにアクセスする人（例：ユーザ）を表す。
アクション	サブジェクトがデータアセットに対して何を行いたいかを記述する（例：読み取り、書き込み)。
リソース	データアセットを記述する。
コンテキスト	アクションのコンテキストを指定する（例：時間、場所)。

XACML のデータフロー図とそれを実現する主なアクターやコンポーネントは図表 5-75 の通りであり、Policy Enforcement Point（PEP)、Policy Decision Point（PDP)、Policy Information Point （PIP)、 Policy Administration Point （PAP）からなる。

図表 5-75 XACML データフロー（概念図）

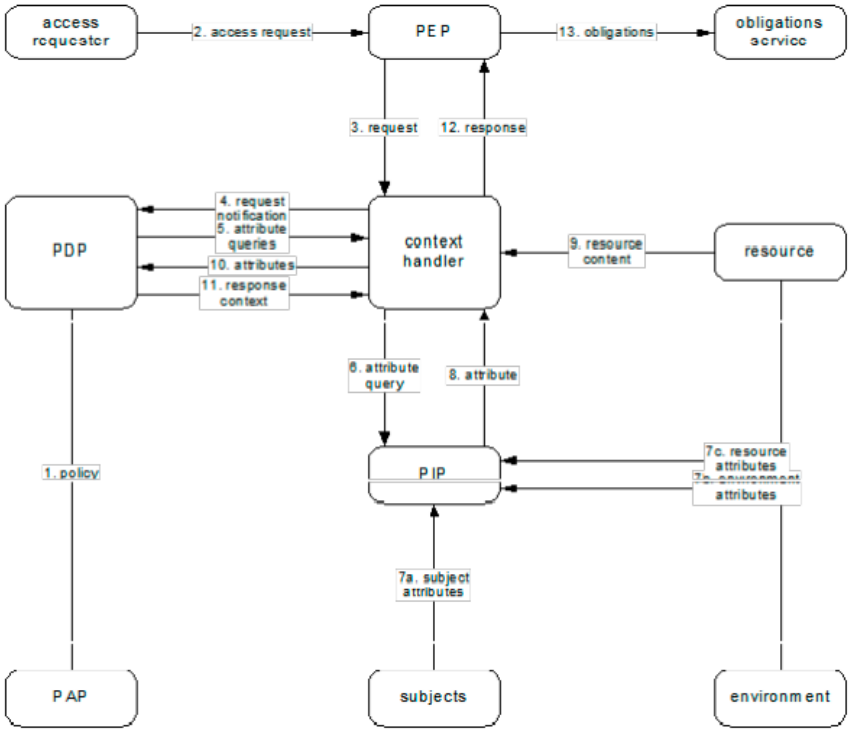


Figure 4.11: XACML data flow diagram [Source: eXtensible Access Control Markup Language (XACML) Version 3.0]

属性として記述事項は、図表 5-76 にある 4 種類のカテゴリに大別することができる。

図表 5-76 XACML の各属性と記述事項（例）

属性	記述事項（例）
サブジェクト属性	年齢、役割、権限等ユーザを表す属性
アクション属性	サブジェクトがデータアセットに対して行うアクションを表す属性（例：読み取り、書き込み）。
リソース	リソース自体を表す属性（オブジェクトタイプ、場所、分類等）
コンテキスト	時間、場所、その他の動的側面に対処する属性

IDS では、アクセスコントロールは、サブジェクト（IDS 参加者）からリソース（データサービス）へのアクセス要求についてリソース中心で規制する。データオーナー（多くの場合、データプロバイダと同一）は、自分のエンドポイントに対して属性ベースのアクセスコントロールポリシーを定義する。さらに、データオーナーは、リソースへのアクセスを許可するために、サブジェクトが証明しなければならない属性値を定義する。これらの属性には以下のものが含まれる。

- コネクタの ID（特定コネクタからのアクセス要求のみ許可される）
- コネクタの属性（特定属性を持つコネクタからのアクセス要求のみ許可される）
- セキュリティプロファイル要件（特定のセキュリティ要件を満たすコネクタからのアクセス要求のみ許可される）

実際のアクセスコントロールの決定はコネクタ内で行わなければならず、コネクタのデプロイに際して、XACML 又は Java 認証・認可サービス（JAAS）のような技術を使用して実装することができる。ただし、IDS は、特定のアクセス制御実施言語又は実装を指示していない。

特定のデジタルリソース（例：サービス又はファイル）へのアクセスを規制するデータアクセスコントロールのみならず、IDS セキュリティアーキテクチャはデータユーセージコントロールもサポートする。ユーセージコントロールの全体的な目標は、データへのアクセスが許可された後にデータコンシューマ側でデータの利用制限を実施することである。 ユーセージコントロールはアクセスコントロールを拡張したものである（図表 5-77 を参照されたい）。

図表 5-77 ユーセージコントロールとアクセスコントロールの関係（概念図）

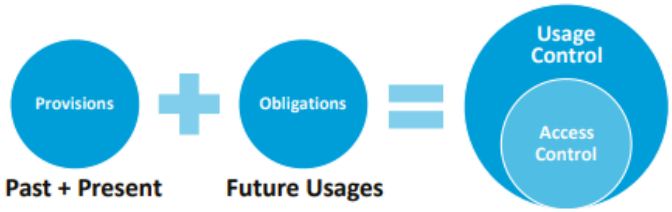


Figure 4.12: Data usage control – an extension of data access control

ユーセージコントロールは、データアセットに対して何ができて、何ができないかを規制する制限を指定し、実施することである。したがって、ユーセージコントロールはデータへのアクセスではなく、データ処理に関連する要件に関連しており、知的財産権保護、規制遵守、デジタル著作権管理等の文脈で重要となる。IDS におけるデータユーセージポリシーは、基本的に、交換されるデータにデータユーセージポリシーに関する情報を付加し、データの処理、集約、他のエンドポイントへの転送の方法を継続的に制御することで機能する。このデータ中心の視点により、データプロバイダはサービスへのアクセス時に留まることなく、データフローを継続的に制御することができる。コネクタコンフィギュレーションに際して、データユーセージポリシーは、開発者や管理者が正しいデータフローを設定できるようにサポートする。

実行時には、データユーセージコントロールの実施により、IDS コネクタがデータプロバイダにとって望ましくない方法でデータ処理することを防ぐ役割を果たす（例えば、個人データをパブリックエンドポイントに転送する等）。このように、データユーセージコントロールは、システムインテグレータがセキュリティ要件に違反するアーキテクチャを構築しないようにするためのツールであると同時に、準拠したデータ使用の証拠を提供する監査メカニズムでもある。

図表 5-78 は、アクセスコントロールでは実現できないが、データを中心としたユーセージコントロールを必要とする要件を例示している。 前述の通り、ユーセージポリシーは参加者間の合意に基づくもののであるため、下記事項がユーセージポリシーに必ずしも含まれるわけではない。

図表 5-78 ユーセージコントロールで定める要件（例）

項目	要件（例）
セキュリティ	機密データは、個別のアクセス権を持っていない参加者やコンポーネントに転送してはならない。
完全性	重要なデータは、信頼できない参加者によって変更されてはならない。
TTL （有効期限）	データは一定期間経過後にストレージから削除されなければならない。
データ集約による匿名化	データを属性に応じてグループ化し、匿名化しなければならない。そのために、そのためには、個々の記録が匿名化されないよう、十分な数の異なるデータ記録を集計しなければならない（ミクロアグリゲーション）。
データ代替による匿名化	データ項目の一部を書き換えて、匿名化しなければならない。例えば、個人を特定できるデータ（例：ビデオファイルの顔）は、個人の匿名化を防止するために適切な代替物（例：ピクセル化）に置き換えなければならない。
SoD （職務分離）	競合する事業体からのデータセット（例：2 つの自動車 OEM）は、決して同じサービスで集約又は処理されてはならない。
使用範囲	データは、コネクタ内のデータパイプの入力としてのみ使用することができ、コネクタ外部のエンドポイントに送信してはならない。

ユーセージコントロールの目的は、上記のような制約を指定し、それぞれのシステムでそれを実施することであることに注意することが重要である。ユーセージコントロールの前提条件は、実施メカニズム自体が信頼できることである。すなわち、ユーセージコントロール自体はエンドポイントに信頼を確立するのではなく、既存の信頼関係を基に、サービスレベル合意（SLA）やデータプライバシー規制等の法的又は技術的要件の実施を容易にするものである。したがって、ユーザは、ユーセージコントロールは IDS の規定するような高度に信頼されたプラットフォーム上で適用された場合にのみ、一定の実施保証を提供することを認識する必要がある。

イ テクニカルエンフォースメント・組織内規則・法的契約

ユーセージコントロールの技術的強制（テクニカルエンフォースメント）には、参加者間での合意に基づく履行が期待されており、かつ契約がマシンリーダブルな形式で表すことができていることを前提として、異なるシステム内で使用されるデータを追跡し、合意された使用制約に違反した証拠を収集する方法が確立されていることが必要である。

一方で、ユーセージコントロールの実施形態は、組織的な規則や法的な契約から、完全に技術的に利用制限を実施する方法まで、多岐にわたる。例えば、組織内規則（例：社内規定）として、従業員は USB メモリ等のリムーバブルストレージデバイスを使用してはいけないとすることができる。同様に、Windows OS によって指定されたグループポリシー等の技術的規則によっても、従業員がリムーバブルストレージデバイスを使用することを防止することができる。同一内容を組織的なルール、法的契約及び技術的規則において同時に定めることが適切な場合もあれば、これらの実施形態を相互

補完的に用いることもできる。将来的には、組織的なルールと法的な契約は、技術的な実施形態に取って代わられることが予想される。

ユーセージコントロールの施行は、様々な形態で特徴付けられ、実施される可能性がある。組織的な規則や法的な契約は、新しいレベルのセキュリティを導入する技術的な解決策に置き換わるか、少なくともそれに付随するものとなりえる。逆もまた然りであり、技術的解決策は、(例えば、技術的解決策に欠けている能力を補うために)組織的規則又は法的契約を伴うこともある。ユーセージコントロールを社内規定で対処するのはよくある解決策であるが、IDS リファレンスアーキテクチャモデルは技術的な実施に焦点を合わせている。

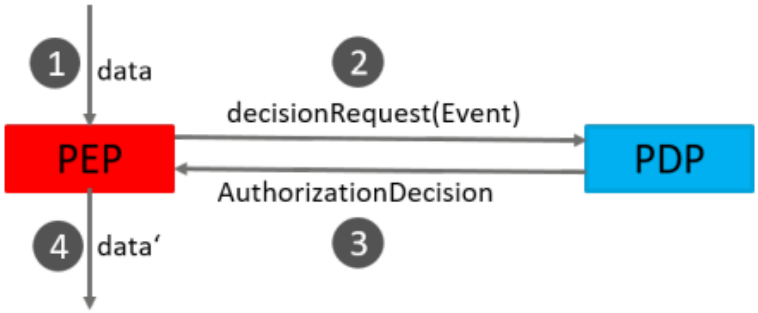
ウ エンフォースメント

データのユーセージコントロールを実施するためには、データはシステムの挙動を監視するコントロールポイント(すなわち PEP)によって仲介される必要がある。システムの各アクションは、許可又は拒否を要求するための意思決定エンジン(すなわち PDP)によって判断される必要がある。意思決定エンジンは、アクションを許可又は拒否するのみならず、アクションの修正を要求することもある。PEP は、以下のような実施方法をカプセル化する。

(ア) 決定と情報

エンフォースメントは PDP による個々の決定によって実施される。図表 5-79 に示す通り、PDP には、PEP からのアクション要求(システムアクション等)に、決定という形で答える役割がある。

図表 5-79 PDP と PEP の関係(概念図)



ユーセージコントロールに基づく意思決定は、ポリシー評価とも呼ばれる。ポリシー評価には、イベントベースやフローベース等の複数の処理方法がある。イベントベースの処理では、データ交換に際してのトランザクションは、データ利用を特徴付ける属性を含むイベントとして表現される。

上記の概念に基づくと、データ交換に際してのトランザクションをデータ自身と受信者に関する属性を持つイベントとしてモデル化することが可能である。例

えば、受信者に関する属性には、メタデータと受信を希望する対象のシステムに関する情報が含まれるとする。対象のシステムに該当しない場合、決定エンジンは否定的な決定を下す。ポリシーの決定は、傍受されたシステムアクション自体には存在しない追加情報にも依存する場合がある。これには、データフローやエンティティの地理的位置等、コンテキストに関する情報が含まれる。

また、意思決定前（例えば、コンテキストの完全性チェック）と後（例えば、データ項目が使用後に削除される）に保持しなければならない事前条件と事後条件を指定することも可能である。また、利用中の条件（例：営業時間内のみ）を定義することも可能である。図表 5-80 に示されるように、これらの条件は通常、データの利用前、利用中、利用後に満たすべき制約や許可を指定する。

図表 5-80　意思決定前-中-後におけるユーセージコントロールの役割

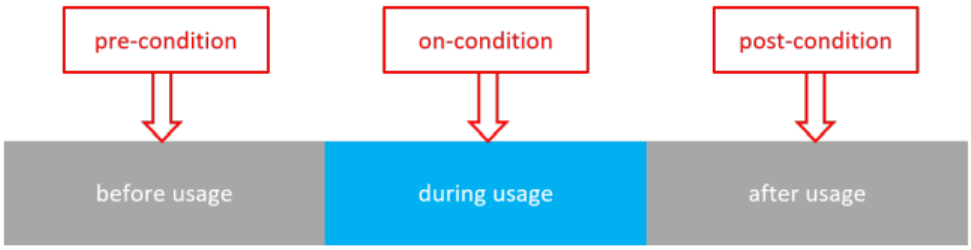


Figure 4.15: Usage Control Pre-, On-, and Post-Conditions

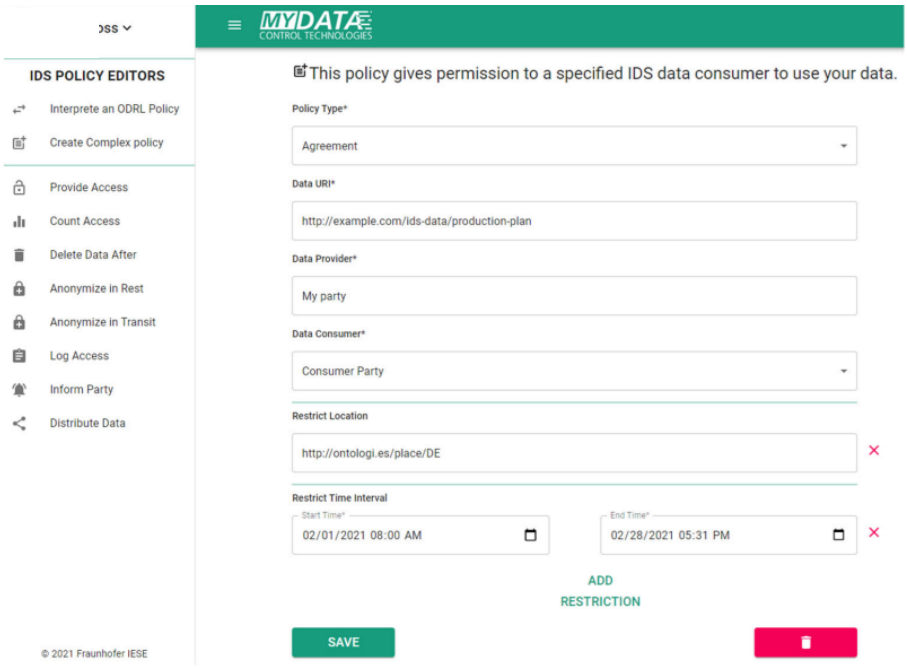
PIP は、意思決定のために不足している情報を提供する。さらに、このようなコンポーネントを使用して、傍受されたシステムアクションのコンテキスト情報（要求デバイスの地理的位置等）を取得することができる。

（イ）ユーセージコントロールの指定・管理・交渉

ユーセージコントロールのもう一つの重要な側面は、ユーセージコントロールの指定と管理である。データプロバイダはデータのユーセージコントロールを正式な形で表現しなければならない。ユーセージコントロールのテクニカルエンフォースメントを実現するためには、マシンリーダブルな出力でなければならない。PAP は、ユーセージポリシーを指定するためのエントリーポイントであり、多くの場合、グラフィカルユーザインターフェース（GUI）を介して指定される。現状においては、図表 5-81 のような GUI が開発されている[182]。

[182] *Usage Control in the International Data Spaces 3.0.* INTERNATIONAL DATA SPACES ASSOCIATION, March 2021, p35,https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-Position-Paper-Usage-Control-in-the-IDS-V3..pdf（2022 年 3 月 22 日アクセス）

図表 5-81　ユーセージポリシー設定画面



PMP は、ユーセージポリシーの管理に責任を持つ。したがって、このコンポーネントはポリシーのライフサイクルに関係する。これには、ユーセージポリシーのインスタンス化、交渉、デプロイ、失効及びコンフリクトの検出と解決が含まれる。

ユーセージポリシーの情報を利用可能にするための方式は、図表 5-82 に示す 2 種類がある。

図表 5-82 ユーセージポリシー情報の共有方式

方式	概要
ユーセージポリシー情報をデータに添付する方式	ユーセージポリシーの情報は、交換対象となるデータに添付することができる。このようなポリシーはスティッキーポリシーと呼ばれる。この方式では、データはデータ利用者に送信される前に暗号化され、データ利用者が指定された利用制限を完全かつ明示的に受け入れた場合にのみ復号化される。
ユーセージポリシー情報を中央コンポーネントで共有する方式	ユーセージポリシーは、交換対象となるデータとは独立して（例えば、PMP や PRP のような中央のコンポーネントに）保存することができる。この場合、中央コンポーネントは、異なるシステム間でユーセージポリシーの情報を交換する責任を負う。 ユーセージポリシーの管理は、データがシステムの境界を越えて交換される場合に特に重要となる。 データがシステム間で通信されるたびに、対象のシステムは受信するデータの保護に備えなければならない（すなわち、対応するユーセージポリシーを展開しなければならない）。

ユーセージポリシーの交渉もまた、ポリシー管理の一部である。異なるシステム又は技術間でポリシーエンフォースメントの実施方法が異なるように、抽象的なポリシーは異なるインスタンス化を持つことができる。したがって、ユーセージポ

リシーは常に対象システム上でインスタンス化されなければならない。

エ ユーセージコントロールの構成要素

以下、IDS がデータユーセージポリシーに関する技術を統合するために使用している構成要素を概説する。最初のサブセクションでは、IDS インフォメーションモデルとユーセージコントロールを扱うモジュールについて説明する。続くサブセクションでは、コネクタと Apache Camel インターセプタについて説明する。

(ア) IDS インフォメーションモデル

IDS インフォメーションモデルは、コネクタ等の機能を記述したモジュール毎のメタモデルである。コネクタ等が提供するデータの自己記述は、専用のメタデータブローカーレジストリで公開される。データコンシューマは、特定の目的に関連しており、かつ適用可能なデータを検索して識別し、データの価格や利用制限を事前に評価することができる。

W3C 標準の Open Digital Rights Language（ODRL）を拡張した IDS インフォメーションモデルのユーセージコントロールモジュールは、ユーセージポリシーをマシンリーダブルな仕様で提供するものである。これは、あるデータアセットに関して、当事者が行うことを禁止又は許可される行為を規定するものである。この規定内容は、ユーセージポリシーとして求められる潜在的なあらゆる義務を規定するものである。図表 5-83 に示すような単純なコアモデルであるが、ODRL ポリシーは仕様レベルで使用契約を宣言的に表現する正式な方法である。

図表 5-83 ODRL Core Model 2.1

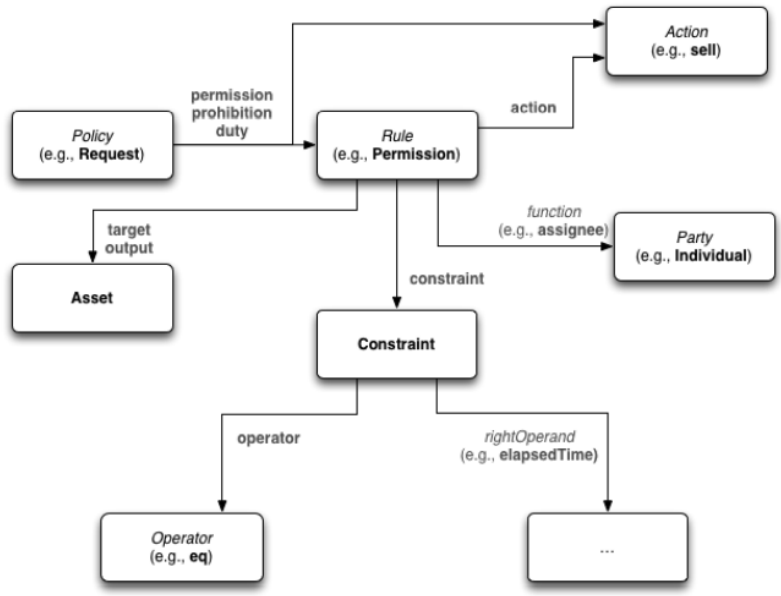


Figure 4.16: ODRL Core Model 2.1 (ODRL Version 2.1 Common Vocabulary Final Specification: 5 March 2015)

上記の方法により、IDS インフォメーションモデルは、IDS におけるユーセージポリシーを一貫性のある方法で表現することを可能にしている。

個々のターゲット環境において仕様レベルでユーセージポリシーを実装・実施するためには、組織的・技術的な手段を個々のターゲット環境にマッピングする必要がある。

組織的手段はここでは対象外であるが、技術的手段には、様々な追加情報源（PIP）とホスト環境との緊密な統合（PEP）が含まれる。IDS インフォメーションモデルは、ユーセージポリシーをマシンリーダブルな形式で事前定義することによって ODRL の構成を強化し、それにより低レベルの実装指向のポリシー言語（例：IND²UCE XML）へのマッピングをサポートする。

以下、図表 5-84 を用いて具体的に説明する。ODRL Constraint クラスは、ルールの適用可能性を判断するための論理条件を表現する。ここでは、演算子（eq）が左オペランド（absolutePosition のような述語）と右オペランド（動的又は事前定義された値）を関連付ける。 IDS インフォメーションモデルは、IDS の特定のシナリオ、例えばデータの残留性における意思決定を支援するために、一方では、定義済み述語群を拡張し、他方では、図表 5-84 に示すように、抽象述語（a）をそれぞれのターゲット環境から提供される操作可能なプログラミングロジック（c）に結びつけるための設定オーバーレイ（b）を定義している。

図表 5-84 ポリシー言語レベル間のマッピング（例）

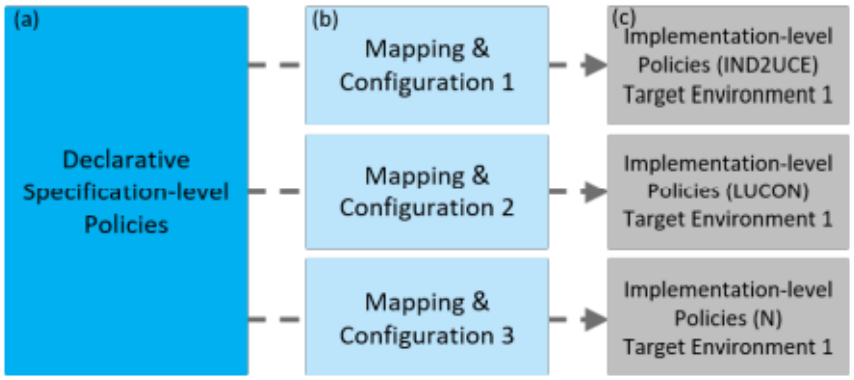


Figure 4.17: Examples of mapping among policy language levels

（イ）コネクタ

ユーセージコントロールは、すべての参加者に対して一定の信頼が確立され維持されるエコシステムにおいてのみ意味を持つ。信頼関係の確立を可能にするためには、データ処理やデータ交換に使用される中心的な技術要素が信頼できるものである必要がある。IDS コネクタは、IDS におけるデータ交換とデータ処理のための中心的なコンポーネントであり、信頼される必要がある中心的なコンポーネントである。

IDS コネクタはセキュリティに重点を置き、下記のような重要なビルディングブロックを組み込んで、信頼できるプラットフォームを提供する。

- 通信当事者（他のコネクタ等）を認証し、パートナー間の信頼関係を形成するためのアイデンティティと信頼管理
- 安全なデータ処理のためのベースラインとしての信頼できるプラットフォーム
- 認証及び暗号化接続に基づく信頼できる通信
- アクセスコントロール及びユーセージコントロール

コネクタのインスタンスは、リモート完全性検証を可能にし、データへのアクセスを許可する前に、展開されたソフトウェアスタックの完全性を保証することができる。物理的又は論理的なアクセスが管理者に許可されている限り、悪意のあるパートナーによるデータ盗難を防ぐことはほとんど不可能である。IDS は、義務を果たすための技術的手段と、どのパートナーを信頼するかを決め、合理的なアクセス条件を定義するためのサポートが提供されるネットワークと見なされている。

（ウ）Apache Camel インセプタ （例）

IDS コネクタは、異なるシステムやアプリケーション間のデータフローを調整するために Apache Camel[183]を使用する場合がある。技術的な観点から、開発者はパイプラインを使用する。パイプラインは、ルート定義で異なるノードを接続するための Apache Camel のパラダイムである。パイプラインの基本的な考え方は、Apache Camel があるノードの出力を次のノードへの入力として使用することである。このようなルートのすべてのノードは、最初のエンドポイントを除いて、プロセッサである （図表 5-85 に示す）。

図表 5-85 Apache Camel によるパイプライン （例）

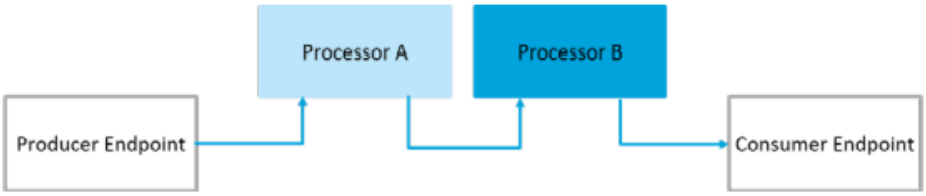


Figure 4.18: Apache Camel pipeline (example)

データのユーセージコントロールを実現するために、サービスとアプリケーションの間のデータフローを傍受することが一つのアプローチとなり得る。図表 5-86 は、開発者がこれを行う方法の一例である。

[183] “Home - Apache Camel” Apache Camel official website, https://camel.apache.org/ （2022 年 3 月 29 日アクセス）

図表 5-86 Apache Camel によるデータフローの傍受

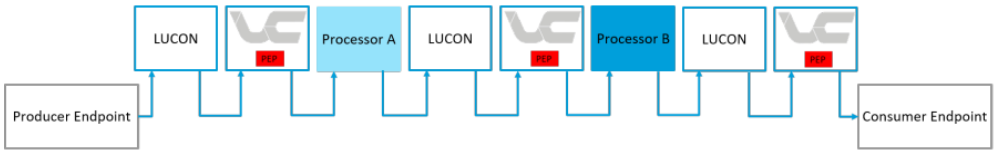


Figure 4.19: Intercepting Apache Camel data flows

Apache Camel を用いることで、プロセッサが動作する前と後に毎回実行するインターセプタを統合することができる。IDS は IDS インフォメーションモデルを提供するため、追加のメタデータはルータを経由して転送されるデータを強化し、それによってより良いユーセージコントロールの実施を可能にする。コネクタは、メタデータをデータパッケージに付加する。さらに、PIP は必要に応じて、意思決定プロセスでより多くのメタデータを扱うことができる。

上記の方法を用いることで、データが常に IDS コネクタと Apache Camel インターセプタをそれぞれ通過するため、企業の境界を越えても機能する（図表 5-87 を参照）。

図表 5-87 企業間のデータ連携（概念図）

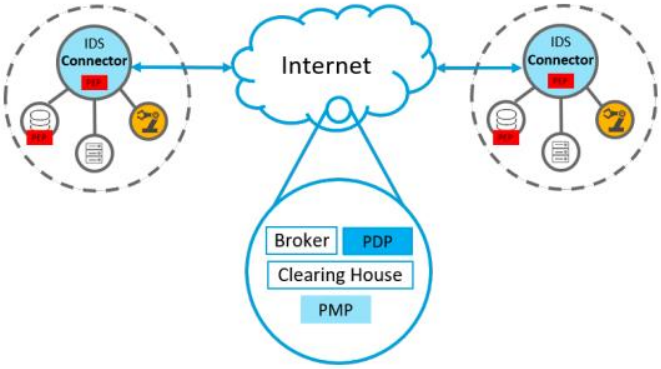


Figure 4.20: Data flow across company borders

データが受信側のコネクタに到達すると、データを保護するための各ポリシーが自動的にインスタンス化される。ただし、利用するポリシーによっては、すべての起こりうるユースケースに対応できるという意味で完全なユーセージコントロールを実現することはできないことに留意する必要がある。

オ ユーセージコントロールに関連する各コンポーネントの役割

ユーセージコントロールは、複数の IDS の各コンポーネントが関与する横断的な概念・技術である。具体的な関連については、図表 5-88 の通りである。

図表 5-88 ユーセージコントロールと各コンポーネントの関係

コンポーネント	ユーセージコントロールとの関連
メタデータブローカー	• メタデータブローカーは、ユーセージポリシーを含むコネクタの自己記述を管理する。したがって、メタデータブローカーはユーセージポリシーをサポートできる必要がある。 • メタデータブローカーを担うコネクタの自己記述自体がユーセージポリシーに従わなければならない場合もある。
コネクタ	• コネクタは、ユーセージポリシーを実装するための主要な技術コンポーネントである。 • コネクタは、データコンシューマ（PEP、Apache Camel インターセプタ等、PDP、PMP）としてユーセージポリシーのエンフォースメントを行うための関連コンポーネントを含んでいる。ただし、PMP 及び PDP はコネクタの一部である必要はない。 • データプロバイダとしてのコネクタは、提供するデータにエンフォースメントに必要な技術に対応するポリシーを添付する必要がある。
クリアリングハウス	次項のデータプロバナンストラックにより、データの利用状況や利用制限の実施状況を追跡することが可能である。クリアリングハウスは、このデータをデータ交換後に利用することができる。
アプリストア	データアプリは、ユーセージコントロールの技術を実装させることができる。 アプリストアは、データアプリがそのような技術を実装しているかどうかについての情報を提供できる必要がある。
アプリプロバイダ	データアプリがユーセージコントロールの技術を活用するため、アプリプロバイダはコントロールポイント（PEP）等のコンポーネントをアプリケーションに実装する必要がある。

カ データプロバナンストラック

データプロバナンストラックは、ユーセージコントロールと密接に関連し、また補完し合うものである。その起源は科学的コンピューティングの領域にあり、データの系統を追跡するために導入された。これにより、いつ、どのように、誰がデータを変更したのか、またどのデータが新しいデータ項目を作成するプロセスに影響を与えたのかを知ることができる。

上記のようなトレーサビリティは、データ管理者がデータ主体へのアクセス権を得るために遵守が必要とされるデータ保護要件と類似している。また、契約、協定、法的規制の遵守を証明する問題にも密接に関連している。また、データプロバナンストラックは、データ交換取引やデータ使用に関する情報を集約することができるため、分散型データエコシステムにおけるクリアリングを促進するために利用することができる。

しかし、ユーセージコントロールがシステム間におけるデータ交換に際しての参加者の権利と義務のエンフォースメントに関係しているのに対し、データプロバナンストラックは透明性と説明責任に焦点を当てている。つまり、ユーセージコントロールのための PEP は、フロー内のデータ利用に関する各アクションをデータ交換前に阻止する必要があるのに対して、データプロバナンストラックのための PEP は、データ交換トランザクションとデータ利用を観察、解釈、記録し、事後的に検証する必要があるのみである。その意味で、両者の違いは、ユーセージコントロールは予防的実施で

あるのに対して、データプロバナンストラックは事後的な措置に関連することにあると言える。

上記の違いがあるとは言え、データプロバナンストラックは、データユーセージコントロールと同じ PEP に基づいて構築することが可能である。さらに、データプロバナンストラックは、ポリシー仕様言語を必要としない一方で、観測されたアクションをデータフローやデータ利用の観点からどのように解釈するかの仕様（いわゆるデータフロー・セマンティクス仕様）を必要とする。このような情報は、上記のデータフローモデルを PIP として実装することによって、ユーセージコントロールの実施にも活用することができる。

（ア）オペレーションにおける原則

データプロバナンストラックの動作原理がユーセージコントロールの動作原理と類似していることは、前述の通りである。データプロバナンストラックは、PEPs 等の受動的なモニタリング技術に依存し、データの使用状況やデータフローを示すイベントを配信してログを取得する。このため、PEP は、そのイベントが示すデータ使用又はデータフローのセマンティックな記述を伝える必要がある。データプロバナンストラックは、このようなセマンティックの仕様を理解するデータフロー追跡コンポーネントを提供する。PEP はまた、イベントをメタデータ（データ内容の一意な識別子を含む）と共に転送する必要があり、これにより、データ実績が集計又は照会されたときに、記録されたトランザクションをデータ内容に関連付けることができる。

（イ）アーキテクチャ

PEP は、コネクタ（又はデータアプリ）のメッセージルーティングコンポーネント内に存在する。それは、レジストリコンポーネント（すなわち、ローカル・ポリシー管理ポイント、PMP）を介して、データフロートラッキングコンポーネントで登録される。データフロートラッキングコンポーネントも同様である。これにより、PEP は PMP にデータフロートラッキングコンポーネントの通信インターフェースを問い合わせることができ、この通信インターフェースは、観測されたイベントに対するセマンティクス仕様を展開し、動作中の実際のイベントを転送するために使用される。

データプロバナンストラックの情報は、クリアリングハウスを介してアクセス可能なプライバシーダッシュボードで照会される。プライバシーダッシュボードは、データコンテンツの一意な識別子に対する出所グラフを返す。データプロバナンストラックの情報を保存するアーキテクチャ方式には、集中型と分散型の 2 つの方式がある。それぞれの方式の概要と概念図は図表 5-89 並びに図表 5-90 及び図表 5-91 の通りである。

図表 5-89 データプロバナンストラックの情報を保存するアーキテクチャ方式

アーキテクチャ方式	概要
集中型アーキテクチャ	• 集中型アーキテクチャの概念図は図表 5-90 の通りである。 • クリアリングハウスにプロベナンスストレージポイント（ProSP）が接続されている。 • データ使用又はデータフローがコネクタ内のデータフロートラッキングコンポーネントによって観測された後、そのトランザクションはこの ProSP に記録される。
分散型アーキテクチャ	• 分散型アーキテクチャの概念図は図表 5-91 の通りである。 • 各コネクタは ProSP を備え、この ProSP はデータフロートラッキングコンポーネントに直接接続されている。 • クリアリングハウスにはステートレスなプロベナンスコレクションポイント（ProCP）のみがあり、プライバシーダッシュボードでクエリが発生すると、ProSP から入ってくるデータプロバナンストラックの情報を集約する。

図表 5-90 集中型アーキテクチャの概念図

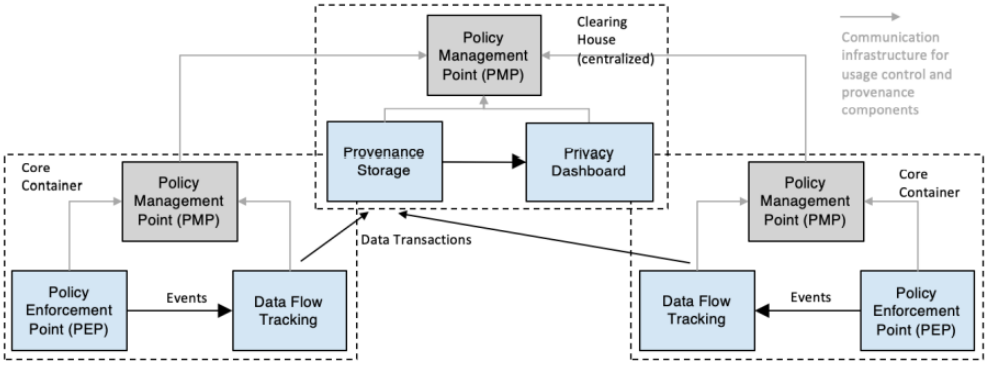


Figure 4.21: Architecture with centralized component for provenance information storage

図表 5-91 分散型アーキテクチャの概念図

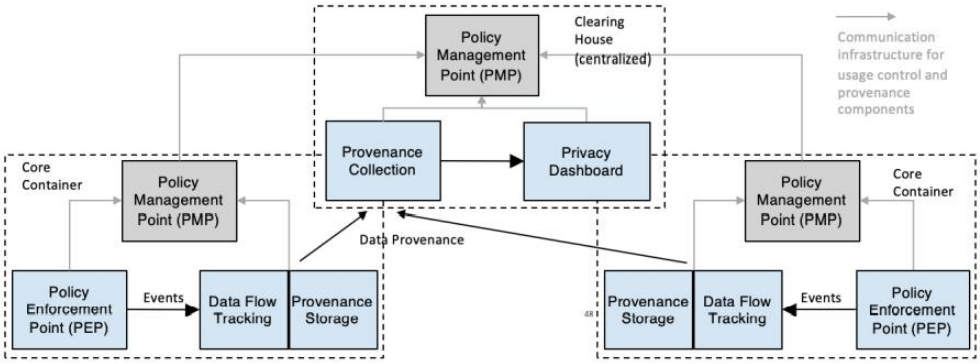


Figure 4.22: Architecture with distributed component for provenance information storage

(ウ) コミュニケーション

コネクタ内のデータフロートラッキングコンポーネントは、ProSP 又は ProCP と通信できる必要がある。このため、クリアリングハウスにいわゆるルート PMP が接続されている。ここで、コンポーネントは通信インターフェースを登録し、コネクタの PMP も同様に登録する。これらのインターフェースを利用して、中央の ProSP 及び ProCP に出自情報が渡される。

このような階層的な通信インフラと同様に、データコンテンツ単位での出所情報はツリー状、いわゆる出所グラフとなる。これは、中央の ProSP で管理される場合と、コネクタ内に分散配置された ProSP で管理される場合とがある。後者の場合、クリアリングハウスにある中央の ProCP は、分散した ProSP から一意のデータコンテンツ識別子に関するさまざまなサブツリーを集約する（つまり、サブツリーを結合することでデータプロバナンスの情報を統合する）。

(エ) ユーセージコントロールとの関連

グローバルに分散したサプライチェーンを管理するためのデータ主権を確立するようなシナリオでは、データはあるデータコンシューマから別のデータコンシューマに転送される。ユーセージポリシーによっては、データはそのままの形で転送されることもあれば、転送される前に何らかの処理、集約、匿名化等が行われることもある。

このことは、ユーセージポリシー、ビジネス契約又は法的規制に従って、データの流れやデータの使用に関する透明性を確立することの重要性を示している。この目的のために、分散型データユーセージコントロールとデータプロバナンストラックは、互いに補完し合う関係にある。

先に説明したように、ユーセージコントロール（検知の実施）に使用される PEP はデータ実績追跡の基礎としても機能し、逆にデータ実績情報は利用制御の実施にフィードバックすることができる（すなわち、利用制御 PDP はユーセージコントロールポリシーによって保護されているあるデータコンテンツの表現のすべての位置を問い合わせることができる）。

また、分散型データユーセージコントロールとデータプロバナンストラックに同じ通信インフラを使用することで、さらなる相乗効果が期待できる。階層的な PMP 構造を用いることで、ユーセージコントロールのコンポーネントが異なるコネクタ間で相互作用することが可能となる（例えば、他のコネクタへのポリシー送信、ポリシーの展開と失効等）。

(オ) クリアリングハウス等との関連

データプロバナンストラックは、データ交換トランザクション及びデータ使用に関する追跡情報を集約した集中監査ログを確立する手段を提供することで、主にクリアリングハウスの業務をサポートする。

データプロバナンストラックは、通常、ユーセージコントロール機能を持つイン

フラ上に実装されるか、モニタリング技術に基づくため、IDS の中核機能には直接影響を与えない。しかし、データプロバナンストラックは、トラッキングが十分に正確であれば、清算や会計の機能を提供することによって、IDS の機能を強化することができる。

データプロバナンストラックは、「データ交換」プロセスに位置付けられている。データプロバイダのコネクタとデータコンシューマのコネクタにあるデータプロバナンストラックに関連するコンポーネントが、クリアリングハウスのデータプロバナンスストレージコンポーネントに、それぞれデータの送信又は受信が正常に行われたことを通知する。この通知機能は、ユーセージコントロールのために PEP が傍受したイベントに基づいて実装されている。

データプロバナンストラックは、様々な目的のためにオーケストレーションすることができる。IDS の最も重要な目的は、透明性を確立し、契約、協定又は法的規制への準拠を証明できるようにすることである。コンテンツの信頼性は、IDS におけるデータプロバナンストラックの二次的な目標である。データの系統を追跡可能にすることがデータプロバナンストラックの本来の目的であるが、そのためには、特定のデータアプリか、これらのデータアプリ専用の PEP を使用する必要がある。データプロバナンストラックによる情報の信頼性は、信頼できるコネクタとデータアプリ（その PEP を含む）に強く依存する。このため、データプロバナンストラックを信頼できるコネクタに統合し、データプロバナンストラックとデータユーセージコントロールが可能なデータアプリを認証することが推奨される。

5.3.2 Gaia-X

本項では、分散型及びハイブリッド型の Gaia-X エコシステムの ID 管理及び信頼性に関する要件を満たすためのフレームワークについて説明する。なお、本項の内容は Gaia-X フェデレーションサービスの Specification を参考に作成している[184]。GDPR の規制に準拠するため、ID とトラストは、W3C が定義した Decentralized Identifiers（以下、「DIDs」という。）と VC に基づく Self-Sovereign Identity（以下、「SSI」という。）のコンセプトに従う。Decentralized Identity Foundation （以下、「DIF」という。）から借用した先進的な DID と OpenID Connect のコンセプトを適用することにより、この標準を拡張し、OpenID Connect、OAuth2、JWT 等の既存で一般的に使用されている技術標準を統合するアプローチを定義する。 現在の実装方針としては、Minimal Viable Gaia-X （MVG）を提示しており、基本的な運用に必要な機能のみを優先的に実装する。なお、現時点で機能仕様として定義されていない技術的なコンセプトが追加されることもある。

(1) Verifiable Credential の発行

ア SSI と DIDs

従来は、政府や司法当局が特定のシステムにアクセスするためには裁判所の命令が

[184] *Reference Document Identity and Access Management Gaia-X Community Document IAM*, Gaia-X AISBL, https://www.gxfs.eu/download/1716/ （2022 年 3 月 17 日アクセス）

必要であったため、政府や司法当局が異なるシステムのデータを入手することは非常に困難であった。当局は、単一のシステムごとに裁判所の命令を必要としていたが、一部の米国企業の影響力によって、米国政府は、米国企業が所有する各システムに常時アクセスできるようにする CLOUD 法[185]を制定した。これにより、米国企業が所有するシステムを利用するユーザは、アカウントがロックされたり、知らないうちにデータが窃取されたり、操作されたりする等、データ主権を失うことになってしまう。こういった事態を回避するために、下記のような取組が必要とされている。

- ユーザの追跡や操作の可能性を排除した分散型でなければならない。
- ユーザは、自分の ID データについて主権的なコントロールを必要とする。
- GDPR 適合を含むデータプライバシーの観点から保護され、追跡や作成が不可能でなければならない。

上記のような取組を実現するために、SSI の考え方を用いた分散型アプローチを確立する必要がある。このアプローチでは、各 ID は現在のように海外のクラウドプロバイダに依存する中央集権的な方式ではなく、ユーザ（ID の保有者）自身によって分散的に管理される。なお、分散型アプローチは、ゼロ知識証明アルゴリズムに基づいている。

SSI のアプローチを用いてプライバシーを保護する具体例を説明する。ある顧客が店でワインを買おうとしており、売り手はその客の年齢を知りたいと思っている。売り手は身分証明書を見ることによって、その顧客が十分な年齢であるかどうかを確認できる。しかし、売り手は身分証明書を確認することによって、生年月日や居住地等、他の全てのデータも見ることができてしまう。これは、顧客が身分証明書を提示したときに、売り手がどのデータを受け取るかを制御できないことを意味する。身分証明書は、年齢チェックに必要な範囲を超えたデータを提示してしまうのである。SSI 方式のアプローチを用いると、「その人はこの商品を購入できる年齢である」という 1 つの情報のみを明らかにするようなカードを提示できる。そのような ID は顧客が自身で作成し、政府等の信頼できる機関によって署名されることで、売り手はこの ID を信用することが可能になる。

具体的には、販売者が QR コードを提示し、チャレンジ・レスポンス方式で年齢を問う。このコードは、スマートフォン等のデバイスで読み取ることができる。その後、売り手に対して必要な情報が提示され、ワインを購入するにあたって「十分な年齢である」又は「十分な年齢ではない」という必要な情報を受け取ることができる。これは、ID を提示する人がその ID の持ち主であることが前提である。

この例から分かるように、サービス提供者側は利用者側の有する全ての情報を必要とするわけではない。場合によっては、ユーザがサービスを利用できるかどうかを知るために、1 つの情報で十分な場合もある。

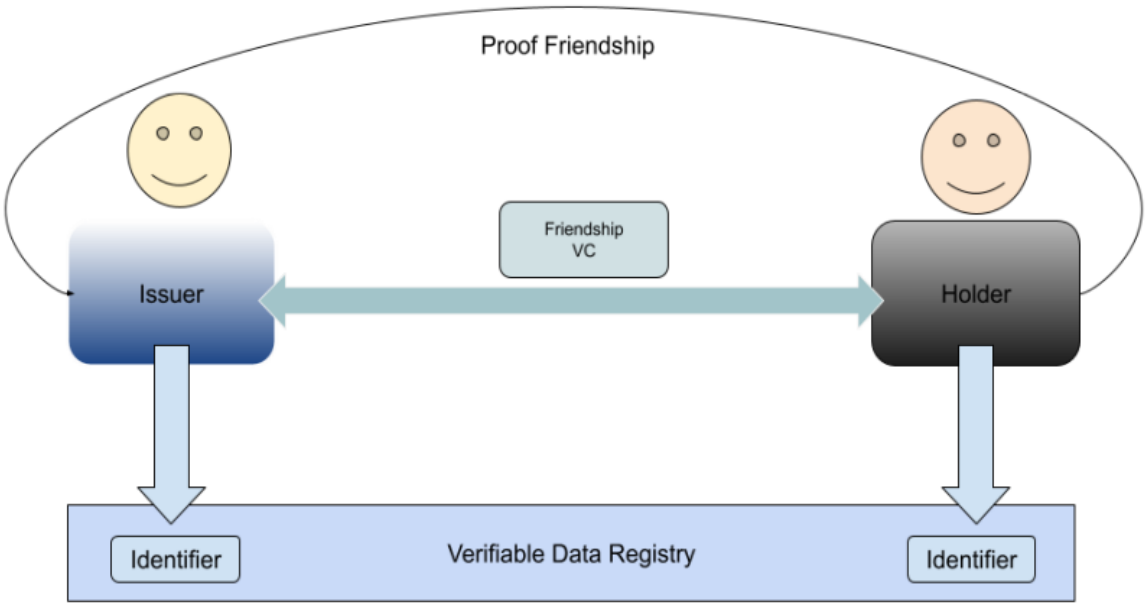
デジタルの世界において上記のような SSI アプローチを実現するためには、公開鍵暗号技術と Claim が必要である。SSI アプローチでは、ユーザは自分の公開鍵・秘密鍵を用いて他のユーザに公開するために用いるものと、自身で保管する 2 つの ID を作成する必要がある。他のユーザに公開する ID は、分散型台帳である Verifiable Data Registry に保管する。そして、分散システムの全参加者が自分の公開用 ID の「保有者」となる。関連する鍵のペアは「リポジトリ」と呼ばれるウォレットに保管される。

[185] “Cloud Act Resources” 米国司法省, https://www.justice.gov/dag/cloudact （2022 年 3 月 29 日アクセス）

ユーザはこの ID を破棄することも、使うことも、使わないことも自己主権的に決定できる。

このような ID を作成することにより、ユーザは友人との友好関係を証明することが可能になる。具体例を用いて説明すると、A は「発行者」として、自分の鍵ペア（kA）と B の ID を組み合わせて署名した VC を B に発行する。その後、B が A へのチャレンジ・レスポンス実施中に VC を提供すると、A は「検証者」として行動でき、自分の署名をチェックできるようになる。B に対するトラストがある場合、A が発行した Credential を提供し、その ID が B によるチャレンジ・レスポンスに成功したことになり、A は B を信用することができる。この Credential には、必要な情報がすべて含まれている。例えば、「私のコンピュータを利用可能である」というような追加情報が含まれている可能性がある。その場合、「A は私の友人であり、彼は私のコンピュータを利用可能である」という 2 つの情報を受領することになる。

図表 5-92　Friendship VC



イ　VC 発行に関するトラストのトライアングル

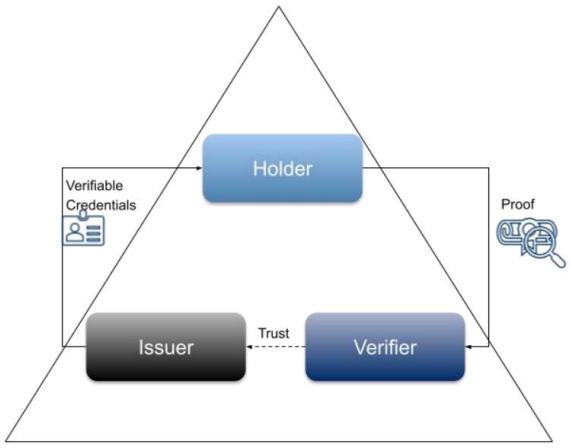
次に、VC と用いたトラストの確立におけるステークホルダの主な関係を表すトラストのトライアングルについて説明する。トラストのトライアングルの主な部分は、保有者／プロバイダ、発行者、検証者である。それぞれの役割は図表 5-93 の通りである。

図表 5-93 トラストのトライアングルにおける役割

役割	内容
保有者	保有者は、検証者に対して、検証者から要求された VC を提示する。また、保有者は、発行者に対して VC の発行をリクエストする。保有者は、VC を発行するのに必要

役割	内容
	なすべての情報を提供しなければならない。
発行者	保有者に対して VC を発行する。
検証者	検証者は、VC が暗号的に安全であり信頼できるか検証する。また、提示された ID が保有者によって所有されているかも検証する。検証プロセスにおいて、検証者は発行者と接触することなくトラストを得ることができる。

図表 5-94　トラストのトライアングル



自己主権 ID システムでは、エンティティが複数の ID を持つことができる。例えば、ある企業で働くエンティティは、特定の役職に就いている従業員の ID を有する。本エンティティがオンラインショップで個人としてサービスを利用することも可能であり、その場合、別の ID を使用することになる。どのような ID も、デジタル世界では参照可能である必要があり、そのためには、ユニークで解決可能な（一意に特定可能な）識別子が必要である。

ウ　分散型のコンセプト

中央集権型の ID 管理から分散型のアプローチへの転換が Gaia-X における鍵であるが、実際のユースケースを想定した DID 管理を実現するために考慮すべき設計上の要件が存在する。

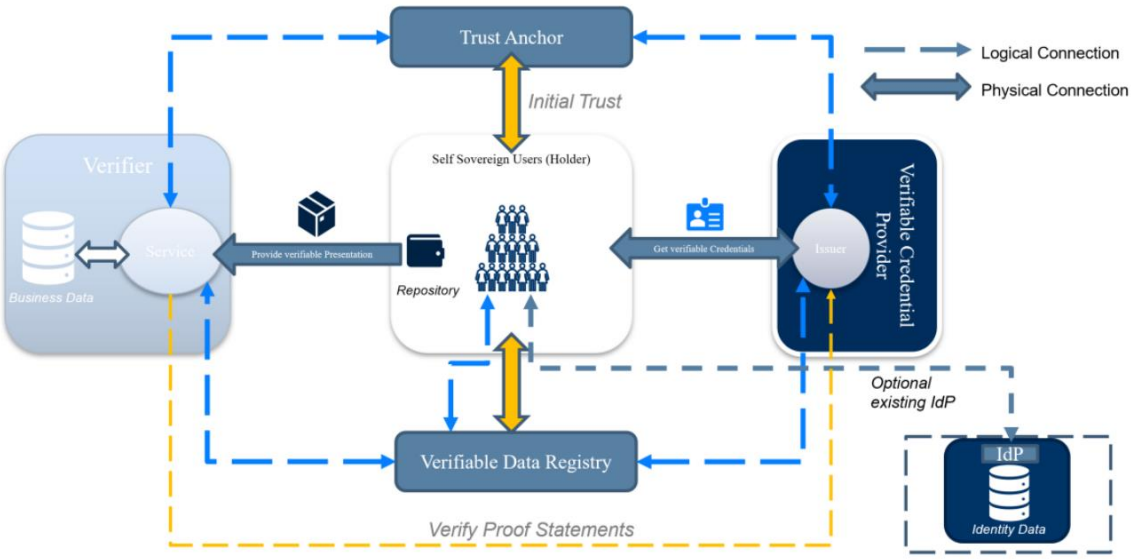
まず、保有者は自身が選択した Verifiable Data Registry 上で DID を生成し、それを管理する必要がある。

第二に、保有者は検証者や発行者を信頼するために、何らかのトラストアンカーを必要とする。実際には、企業の評判や、eIDAS による適合性等の暗号化された証明等がこれに該当する。また、検証者や発行者の信頼度は、各保有者の判断による。また、各保有者が発行者でもあり検証者でもあることを考慮する必要がある。

実際には、プロセスの中で役割は変化する。図表 5-95 は、異なるステークホルダがどのように関係しているかを示している。DID 管理において、ユーザは、Credential 発行者を信頼するか、検証者に Credential を提供するかを常に選択できる。この自己

主権の考え方は、サーバやデバイスのような技術システムにも有効であり、従来とはまったく異なる方法で本コンセプトに関するアクセス及びユーセージコントロールを行うことができる。このことは、認証やアクセス管理の方法にも影響を与える。

図表 5-95　分散型のトラスト



エ　Notarization API による VC の発行

Notarization API は、信頼できる発行者が VC を発行できるようにするために必要である。Notarization API を使用することで、公認審査員（Certifier Auditor）は物理的な文書や様式が定まっていない電子文書をデジタル VC 形式に変換し、オンボーディングやデータ取引時にトラストを確立できる。その結果は、自己記述に埋め込まれるか、参照される。これは、これまで構造化されていなかった紙や PDF 等の認証文書からトラストを構築することを可能にする。

(2) 認証・認可の仕組み

ア　認証

分散型コンセプトにおける認証と認可は、自己主権の考え方に従っている。従来の集中型アプローチでは、ユーザは ID プロバイダの所有者が要求する様々な種類の情報が紐づいたアカウントを作成することが一般的である。この場合、中央 ID プロバイダはユーザのデータに対してあらゆる制御ができる状態となる。

それに対し、非中央集権的アプローチでは、要求側はサービスの利用に際して必要なデータのみを要求する。この場合、ホルダーは分散型 ID プロバイダの役割となり、要求側を信頼する場合に分散型 ID を提供することができる。

以前は、認証は中央の ID プロバイダ（IdP）で行われることが一般的であったが、

現在は、ホルダーが所有する PCM（スマートフォンウォレット）や OCM（サーバウォレット）等の分散型システム上で認証するケースが増えてきている。PCM や OCM 等の Credential・マネージャは、要求側に対して、秘密鍵や公開鍵で識別される ID 情報を提示する必要があるため、高いレベルのセキュリティ要件が満たされる必要がある。

また、リソース等人間以外に紐づくものは、内部ウォレット又は各サーバウォレットに格納されている ID データと関連する秘密鍵を使用して認証することができる。

イ 認可

認可は主に 2 つの側面から構成される。

第一の側面は、ユーザ又はその他のエンティティの ID に紐づいたデータの使用に対する認可又は同意である。分散型システムでは、ID データは VC という形で ID 所有者が自己主権的に管理し、ウォレットに保管される。ユーザは、データが第三者と共有してよいかどうか、またどの範囲まで共有されるかを自己主権的な方法で決定することができる。従来の IdP モデルとは異なり、データはいかなる第三者管理のサーバ等に保管されていないため、第三者によってセンシティブなデータが公開されることはない。

第二の側面は、API インタラクションやデータ交換の際に行われるリソース利用の認可である。従来のモデルでは、アクセスは常に API やデータストレージのプロバイダでローカルに割り当てられた ID、役割、権利にリンクされていた。分散型モデルでは、ユーザやエンティティは、異なるセキュリティドメインにまたがるリソースにアクセスするために、自己主権型の ID を 1 つだけ使用することになる。VC 形式の ID 情報は、アクセスポリシーを実行するために使用され、最終的にはアクセスの決定をサポートする。

現在のコンセプトでは、認証フェーズでは DIDComm[186]ベースのログインを使い、アプリケーション上では DIDComm ベースのバックチャネル認証に支えられた動的クライアント登録を使って同様の Credential 交換が行われる。ポリシー評価の中核となるのは、属性ベースのアクセスコントロールシステムであり、ID データに基づく詳細なポリシー設定が可能になる。従来のロールベースのアクセスコントロールは、VC に含まれている Claim を評価することによって実現することができる。

このようなアーキテクチャは、既存の認証ソリューションやプロトコルを置き換えることを目的としたものではなく、自己主権型 ID と VC に基づく認証の側面から、そのような標準ベースのシステムの機能を補強するものである。将来的には、この仕様の範囲外であるが、バックグラウンドで動的に VC をロードする手段や、DIDComm 上のバックチャネルでの Credential 交換（結果としてアクセストークンを持つことができる）等により、個々のデータやリソースアクセスのレベルで、特定の VC を要求できるようになると想定している。

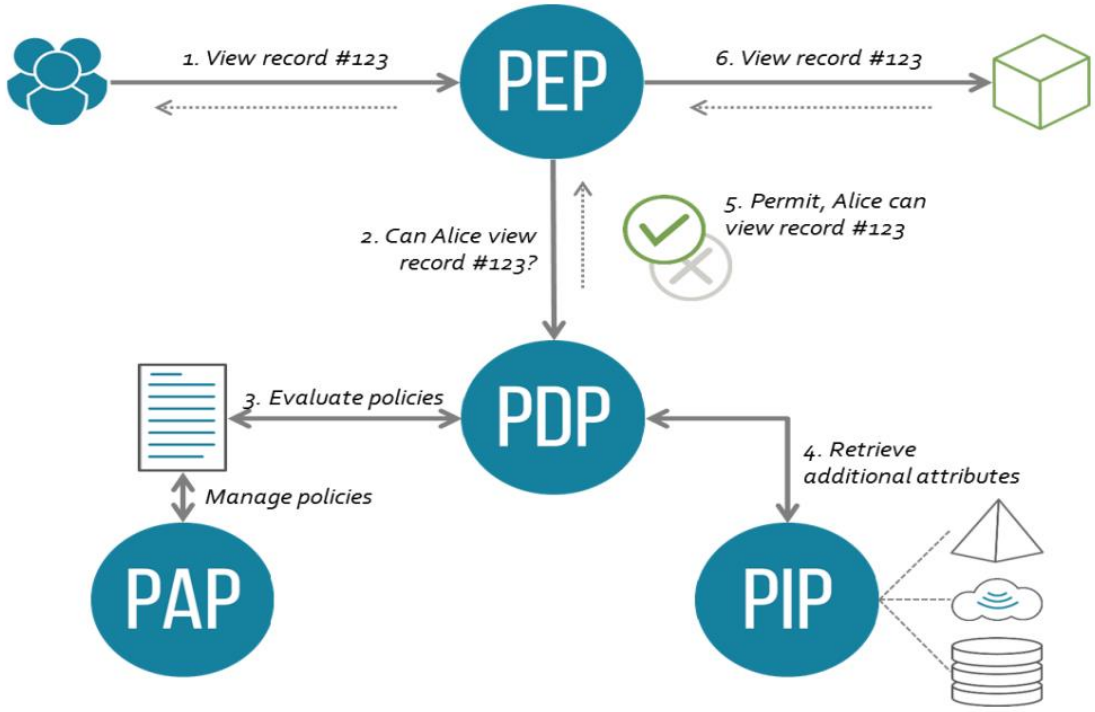
(3) エンフォースメント

アクセスコントロールの目的は、認可プロセスを複数のサブプロセスに分離すること

[186] DIDComm Messaging, Sam Curren, etc., , https://identity.foundation/didcomm-messaging/spec/, （2022 年 3 月 24 日アクセス）

である。一般的に、認可プロセスでは、クライアントがリソースにアクセスできるか否かを様々な方法で決定する。例えば、アプリケーションのロールパーミッションに基づくモデルや、Claim に基づく決定を含む属性評価によるルールベースのアプローチがこれに該当する。これらの方法は、個々のアプリケーションの機能に最適な方式でハードコードされてしまうことが多い。特別なユーザグループのための新しいパーミッションを追加する等、アプリケーションの権限を変更する場合、実装、設定、テストが必要になる。このような状況において柔軟に対応するために、アクセスコントロールは図表 5-96 及び図表 5-97 のように分離して考慮する必要がある。

図表 5-96　アクセスコントロールのアーキテクチャ（処理フロー）



図表 5-97 アクセスコントロールのアーキテクチャ（処理内容）

コントロールポイントの名称	処理内容
PEP（Policy Enforcement Point）	エッジサービス又はアプリケーションフレームワーク内に実装された PEP は、ポリシー決定のために PDP を呼び出し、呼び出したコンテキスト内で適切に受け取ったポリシー決定に基づいて行動する。
PDP（Policy Decision Point）	PDP は、管理されたポリシー定義に基づき、アクセスオブジェクトを評価する。
PIP（Policy Information Point）	PIP は、PDP によるポリシー決定プロセスで使用される属性値プロバイダとして機能する。情報の値は、主に VC、データ及びサービス等、外部を参照する。
PAP（Policy Administration Point）	PAP は、ポリシーの更新を管理し、受信したリクエストにマッチしたポリシーを転送する。
PRP（Policy Retrieval Point）	PRP は、ファイルシステムやデータベース等の、ポリシーが物理的に保存される場所である。

アクセスコントロールアーキテクチャは、異なるコンポーネントとして機能の分離を行う。次に、自己主権型システムとアクセスコントロールアーキテクチャの関連について説明する。

アクセスコントロールアーキテクチャは、例えば REST API 等、あらゆる種類のサービスの一部である。API 自体が ID を持ち、保有者の役割を果たす。これにより、サービスを利用しようとするクライアントは、必要な属性を記述した VC の提示を要求することで、まずサービスの信頼性を検証することができる。

API 自体へのリクエストがあった場合、PDP は正しいアクセストークンの提示を制限するポリシーを評価することができる。トークンが存在しない場合、PDP はレスポンスを返し、相手側にこの API へのアクセス権を持ち、有効なクレジットカード等のアクセス条件を満たしていることを証明するよう要求できる。

この証明は、VC とともに提示され、PDP が API コールを通過させることができる正しいアクセストークンを得ることができる。API は検証者として、提示された VC を独自のトラスト基準に照らしてチェックすることができる。

その結果、PDP は API コールを許可するか、アクセストークンを生成することができる。もう一つの選択肢は、PIP を直接使用して、バックグラウンドで他のホルダーから必要な情報を動的に取得することである。

どの方法を選んでも、API は自己主権的な存在であり、誰がアクセス権を持つかどうかを決定することができる。中央集権的な ID 管理は必要なく、トラストポリシーが代替の役割を果たす。

第6章 IDS・Gaia-X のテクニカルアーキテクチャ（詳細）

6.1 IDS コンポーネント

6.1.1 CA

CA（認証局）は、全てのエンティティに対して証明書を発行する。これらの証明書は、コネクタ間の認証と暗号化に利用される。認証の対象は参加者とコアコンポーネントの 2 つであり、各々に証明書が付与される。両証明書により、参加者は識別・認証・暗号化のための X.509 証明書を要求することができる。

IDS の各コネクタは有効かつ永続的な一意の識別子を必要としており、IDS 内の他のリソースに再利用されることはない。このアーキテクチャは、証明書を発行する複数の認証局（CA）に対してオープンであることを目指している。つまり、真にユニークな ID は、証明書の発行者とサブジェクトの ID で構成される必要がある。マシンリーダブルな ID のため、X.509v3 の 2 つの拡張機能：Subject Key Identifier （SKI） と Authority Key Identifier （AKI）が使用される。SKI と AKI を連結することで、複数の企業が有効な証明書を発行しても、有効な一意の ID を提供する。

例：

```
...
X509v3 extensions:
    X509v3 Subject Key Identifier:
        DD:CB:FD:0B:93:84:33:01:11:EB:5D:94:94:88:BE:78:7D:57:FC:4A
    X509v3 Authority Key Identifier:
        keyid:CB:8C:C7:B6:85:79:A8:23:A6:CB:15:AB:17:50:2F:E6:65:43:5D:E8
...
```

…コネクタの一意な ID に接続する：

```
DD:CB:FD:0B:93:84:33:01:11:EB:5D:94:94:88:BE:78:7D:57:FC:4A:keyid:CB:8C:C7:B6:85:79:A8:23:A6:CB:15:AB:17:50:2F:E6:65:43:5D:E8
```

簡潔に記述すると、下記の通りとなる。

```
SKI:AKI
```

なお、上記の記述にあたっては IDS リファレンスアーキテクチャモデル及び GitHub 上の関連箇所を参照した[187]。

6.1.2 DAPS

動的属性提供サービス（DAPS）は参加者・コネクタに関する、動的かつ最新の属性情報を提供する。

IDS エコシステムのインフラコンポーネントである動的属性提供サービス（DAPS）は、

[187] “GitHub -International-Data-Spaces-Association/IDS-G” Github, https://github.com/International-Data-Spaces-Association/DataspaceConnector （2022 年 3 月 11 日アクセス）

組織やコネクタの ID を追加属性で強化することができる。

DAPS は（認証局と同様に）、IDS アイデンティティ・プロバイダーの構成要素として理解することができる。これらの属性は DAPS によって動的属性トークン（DAT）に埋め込まれ、次のような利点がある。

- 属性の失効により、証明書の失効・再発行が強制されることはない。これは、新しい属性が追加された場合も同様である。
- スコープ又は属性セットを定義することにより、必要な属性のみを DAT に含めることができる。 これにより情報漏洩が制限されるため、必要な属性のみが伝達される。
- ベースライン証明書を発行して、コネクタの展開を簡単に行うことができる。
- 後に属性が割り当てられるとすぐに、より複雑なシナリオを作成できる。

DAPS は、認証が成功した場合、 “access_token” キーの下の JSON オブジェクトに埋め込まれた要求された DAT を発行する。

例：

```
{
    "access_token": "<DAT>",
    "scope": "ids_connector_attributes",
    "token_type": "bearer",
    "expires_in": "3600"
}
```

本フォーマットに関するより詳細な情報は、RFC 6749 のセクション 5.1 を参照されたい[188]。

ヘッダーとペイロードを含む、完全にデコードされた DAT の例を以下に示す。

[188] “The OAuth 2.0 Authorization Framework” Internet Engineering Task Force (IETF), https://datatracker.ietf.org/doc/html/rfc6749#section-5.1 （2022 年 3 月 11 日アクセス）

なお、上記の記述にあたっては GitHub 上の関連箇所を参照した[189]。

6.1.3 ParIS

ParIS は技術的にはメタデータブローカーに類似しており、IDS 参加者の属性を公開及び照会するためのやり取り仕組みを提供する。メタデータブローカーと同様、ParIS もコネクタの一つであるため、すべての IDS 認証基準に準拠する必要がある。

ParIS は、CA や DAPS と同様、 ID プロバイダの一部である。ビジネスエンティティとして参加者の属性を含み、必要な情報を一貫性のある統一された方法で収集し提供する。他の参加者は、ビジネスパートナーの VAT、法定代理人又は組織構造を照会することができる。

このような情報は、エコシステムを管理する法人である IDS のサポート組織が提供・維持する。サポート組織は、デジタル ID を作成して新規参加者を紹介すると同時に、セキュリティ上重要な属性を DAPS に、ビジネス上重要な属性を ParIS に登録する。ParIS は、これらの属性へのアクセスを他の IDS 参加者とコンポーネントに提供し、一意の参加者 ID（URI）を追加のメタデータに連結させる。通常、各 IDS エコシステムは少数の ParIS インスタンスのみを運用し、通常は 1 つだけである。したがって、IDS 参加者は、潜在的なビジネスパートナーに関する詳細情報の照会先を特定することができ、データ交換を開始するかどうかを決定することができる。

他の IDS コンポーネントとは異なり、ParIS の提供する情報の信頼性は、署名や証明書のような技術的な手段ではなく、サポート組織が管理する管理プロセスに基づいている。このプロセスの直接的な結果として、ParIS のデータベースに追加する前に、各変更要求を手動で確認する必要がある。

ParIS は、IDS の技術基盤（主にサポート機関の管理能力）とコネクタ通信の仲介する

[189] GitHub -International-Data-Spaces-Association/IDS-G” GitHub, https://github.com/International-Data-Spaces-Association/IDS-G/blob/main/Components/IdentityProvider/DAPS/README.md （2022 年 3 月 14 日アクセス）

ことで、データのエコシステムを実現する。ParIS は、ビジネスクリティカルな情報や法的側面へのアクセスを可能にするために必要な、標準化された相互運用性を実現するものである。これにより、データマーケットの基盤が構築される。

全ての ParIS インスタンスがサポートする必要があるいくつかのインタラクションプロセスは図表 6-1 の通りである。

図表 6-1 ParIS がサポートするインタラクション

操作	概要	実行するロール	備考
参加者エントリの作成	ParIS に新規参加者エントリが追加される	ID プロバイダ・サポート組織の運営者又は参加者自身	参加者の自己記述は、それぞれの IDS エコシステムで照会可能
参加者エントリの更新	参加者の自己記述の属性を変更したり、新規属性を追加したり、古い属性を削除する必要がある	ID プロバイダ・サポート組織の運営者又は参加者自身	古い自己記述は、新しい自己記述に完全に置き換えられる。古い自己記述は記録目的で保存されることはあるが、IDS エコシステムで提供されてはならない
特定の参加者エントリの照会	要求者は、明示的に特定された 1 人の参加者の 1 つの自己記述に関心がある	ParIS のデータスペースを利用している IDS コネクタ	参加者の自己記述の最新版を配信する
複数の参加者の自己記述に対する照会	要求者は、複数の自己記述を含む等、自己記述やその属性のフィルタ・結合・集約に影響するような複雑なファクトに関心がある	ParIS のデータスペースを利用しているあらゆる IDS コネクタ	基礎となる自己記述の最新版に基づいた Result オブジェクトを配信する

IDS インフォメーションモデルは、以下 2 点において ParIS と関連がある。第 1 に、参加者の自己記述に使用され、ParIS に表示される属性と値を定義している。第 2 に、IDS インフォメーションモデルは、コンポーネント自体（ids: ParIS クラスを使用）及びインタラクションメソッド、特に適用可能な IDS メッセージタイプを定義している。具体的な定義内容に関しては、図表 6-2 及び図表 6-2 中にあるリンクを参照されたい。

図表 6-2 IDS インフォメーションモデルと ParIS

属性	データタイプ・ターゲットクラス	概要
gr:legalName	xsd:string	IDS 参加者の完全な法人名。 例えば、IDSA の法人名は「International Data Spaces e. V.」である
gr:name	xsd:string	IDS 参加者の一般的な名称又は用語。 例えば、法人「International Data Spaces e. V.」は「IDSA」
ids:corporateEmailAddress	xsd:string	参加者と一般的レベルで連絡を取るための電子メールアドレス

属性	データタイプ・ ターゲットクラス	概要
ids:corporateHomepage	xsd:anyURI	参加者の一般的な正式ホームページ
ids:memberParticipant	ids:Participant	参加者がさらに参加者であるメンバーを持っていることを示す。これは、参加者の組織内の階層的な関係を定義し、コラボレーションのメンバー等、把握すべき参加者のグループを特定するのに役立つ
ids:participantRefinement	ids:AbstractConstraint	一人の参加者が対象参加者の一員とみなされるために満たす必要のある条件。例えば、ヨーロッパに本社を置くすべての参加者は、GDPR 関連データの潜在的なコンシューマとなる可能性がある
ids:memberPerson	ids:Person	組織への所属を示す
ids:participantCertification	ids:ParticipantCertification	参加者に発行された認証
ids:primarySite	ids:Site	組織の主要所在地を示す。これは組織に連絡することができるデフォルトの手段であり、必ずしも正式な本社である必要はない
gr:vatID	xsd:string	参加者の VAT（Value Added Tax）番号
gr:taxID	xsd:string	IDS 参加者の税務・財務 ID。例えば、米国の TIN やスペインの CIF/NIF 等。通常、居住国によって割り当てられる
ids:registryCourt	xsd:string	組織の担当裁判所。通常は都市名と国名
ids:legalForm	xsd:string	IDS 参加者の法的形態
ids:hasRole	xsd:anyURI	参加者がデータ利用を制限するために、ビジネスパートナーに公表したい組織内の役割。例えば、組織に専属の「リスク管理者」がいる場合、データプロバイダはこの役割を持つユーザだけが IDS リソースにアクセスできることを表明することができる。役割は、例えば、https://<company-domain/role#のように、有効で一意の URI で符号化されなければならない。

ParIS の内部アーキテクチャはその運営者の責任であり、それ以上規制されることはない。しかし、ParIS は IDS コネクタとして登場するため、コネクタに適用されるすべての要件が ParIS にも適用される。さらに、IDS エコシステムでは複数の ParIS インスタンスがアクティブになる可能性があることに留意する必要がある。その場合でも、単一の ParIS インスタンスには、コンテンツを同期させたり、リクエストに対して他のインスタンスの存在を通知したりする義務はない。

なお、上記の記述にあたっては IDS リファレンスアーキテクチャモデル及び GitHub 上

の関連箇所を参照した[190]。

6.1.4 ボキャブラリプロバイダ

ボキャブラリプロバイダは、ボキャブラリを管理・提供する機能を持つ。オントロジー、参照データモデル、メタデータを使用して、データセットに注釈を付けたり記述したりすることができる。具体的には、自己記述の基礎となる IDS インフォメーションモデルを提供する。さらに、その他のドメイン固有のボキャブラリを提供することができる。

なお、上記の記述にあたっては IDS Meta Data Broker の関連箇所を参照した[191]。

6.1.5 メタデータブローカー

メタデータブローカーは、IDS 参加者間でコネクタやリソースのメタデータを公開・検索するためのサービスである。必要な相互運用性と一般的なインタラクションを確保するため、メタデータブローカー（アプリストア等）は専用の IDS コネクタとしても定義されている。コネクタとメタデータブローカー間の通信は、IDS 内の他のコネクタ同士の通信と同じ原則に基づいているが、メタデータブローカーは下記 2 点の役割を果たすようなコレクションを提供している。

- 効果的かつ効率的にクエリに応答し、既知のコネクタ及びその他のリソースを表示するためのインデックスサービス
- 保存された情報へのアクセスを保証するためのユーザ又は IDS-Message のためのインターフェース

ソフトウェアコンポーネントは、IDS に準拠した CA が必要な機能を備え、IDS に準拠した方法で動作することを確認した後でのみ、IDS コネクタとして記述することが許可される。認証基準のリストには、それぞれの要件が記載されている。メタデータブローカーについても同様の手順が有効で、このリストに記載されているメタデータブローカー機能の追加要件がある。コネクタとして、またメタデータブローカーとして関連する基準の認証に合格すると、ソフトウェアコンポーネントは自己記述に次の RDF ステートメントを含めることができるようになる。

```
<Connector/Broker URI>
                <http://www.w3.org/1999/02/22-rdf-syntax-ns#type>
<https://w3id.org/idsa/core/Broker> .
```

しかし、他のいかなるエンティティも、追加証明なしにこの主張を信じる義務はない。信頼できる情報提供のための IDS メソッドは、動的属性提供サービス（DAPS）が提供する動的属性トークン（DAT）である。認証されたメタデータブローカーは、担当する DAPS に DAT を要求することができる。信頼できる DAPS から正しく署名された DAT が上記

[190] “GitHub -International-Data-Spaces-Association/IDS-G” GitHub, https://github.com/International-Data-Spaces-Association/IDS-G/blob/main/Components/IdentityProvider/ParIS/README.md （2022 年 3 月 14 日アクセス）

[191] *REFERENCE ARCHITECTURE MODEL 3.0*, INTERNATIONAL DATA SPACES ASSOCIATION, December 2020, http://archives.greenairnews.com/www.fraunhofer.de/content/dam/zv/en/fields-of-research/industrial-data-space/IDS-Reference-Architecture-Model.pdf （2022 年 3 月 15 日アクセス）

の主張を含む場合のみ、他の IDS エンティティは潜在的なメタデータブローカーの主張を受け入れる必要がある。

メタデータブローカーの役割の詳細は図表 6-3 の通りである。

図表 6-3 メタデータブローカーの役割

B 001（B1）	IDS メタデータブローカーは、IDS のオプションコンポーネントである。
B 002（B3）	IDS メタデータブローカーは、コネクタから送信されたメタデータを公開するシステムであるインデックスサービスを提供する。
B 003	IDS メタデータブローカーは、データソースのリンクベースの発見を可能にする必要がある。
B 004（B4）	プロバイダとコンシューマのコネクタ間のメタデータを除く実際のデータ転送には、いかなる場合も IDS メタデータブローカーは関与しない。
B 005（B6）	IDS には複数のメタデータブローカーが存在する可能性がある。
B 006（B7）	IDS では、プロバイダによって異なるメタデータブローカーの実装が存在する可能性がある。
B 007（B10）	コネクタオペレータは、そのコネクタのどの（メタ）データパーティションが 1 つ又は複数の IDS メタデータブローカーに送信されるかを独自に定義することができる。
B 008	IDS 参加者は、IDS エンティティのメタデータをホストするために、一般に知られている、 又はその他の方法で公表されているサーバを使用することができる。推奨される手順は、このために IDS メタデータブローカーを使用することである。
B 009（B13）	コネクタと IDS メタデータブローカー間の通信はメッセージ志向である。メタデータブローカーメッセージには 2 つのカテゴリがある。 • パブリッシングメッセージ（インデックスサービスに対するメタデータの配信） • クエリメッセージ（インデックスサービスからのメタデータの照会）
B 010	パーシステントストレージは、トリプルストアや他の適切なストレージバックエンドを使用して実現することができる。
B 011（B24）	インデックスサービスの永続性は、あらかじめ定義されていない。以下は、オプションの一覧である。 • File system • NoSQL • RDBMS • LDAP・ActiveDirectory • RDF
B 012	コネクタとリソースのメタデータは、削除するよりも無効化する方が望ましい。コネクタやリソースが再び出現した場合、IDS メタデータブローカーは以前の状態を認識し、エントリを再アクティブ化できる必要がある。
B 013	メタデータの RDF シリアライゼーション方法は、JSON-LD が推奨されている。
B 014	IDS メタデータブローカーは、有効な IDS コネクタからの登録の試行を受け入れる必要がある。
B 015（B28）	IDS メタデータブローカーは、照会結果に影響を与えない限り、メタデータブローカーメッセージの処理を並列化することができる。

なお、上記の記述にあたっては IDS Meta Data Broker の関連箇所を参照した[192]。

コネクタ要件、機能要件、メッセージ要件、動作要件、ビジネス要件、情報要件、インターフェース要件、条件要件についても、上記ドキュメントを参照されたい。

6.1.6 クリアリングハウス

IDS クリアリングハウスは、IDS エコシステムで行われる全ての財務取引及びデータ交換取引に対して、取引ログに基づく清算・決済からなる 2 つの基本的な機能を提供する。IDS では、IDS クリアリングハウスが行う活動は、データ共有サポートプロセスのライフサイクルの異なる段階で実行されるため、他のサービスから分離されている。

IDS クリアリングハウスは、ID プロバイダ・動的トラストモニタリング（DTM）・PEP・IDS メタデータブローカーとインターフェースで接続し、取引に関する情報を収集している。IDS クリアリングハウスは、データプロバイダとデータコンシューマが合意したデータ共有・決済プロセスの管理機能（データ共有契約に基づく実際のデータ共有取引とそのロギング・レポート管理）を提供する。具体的には、図表 6-4 及び

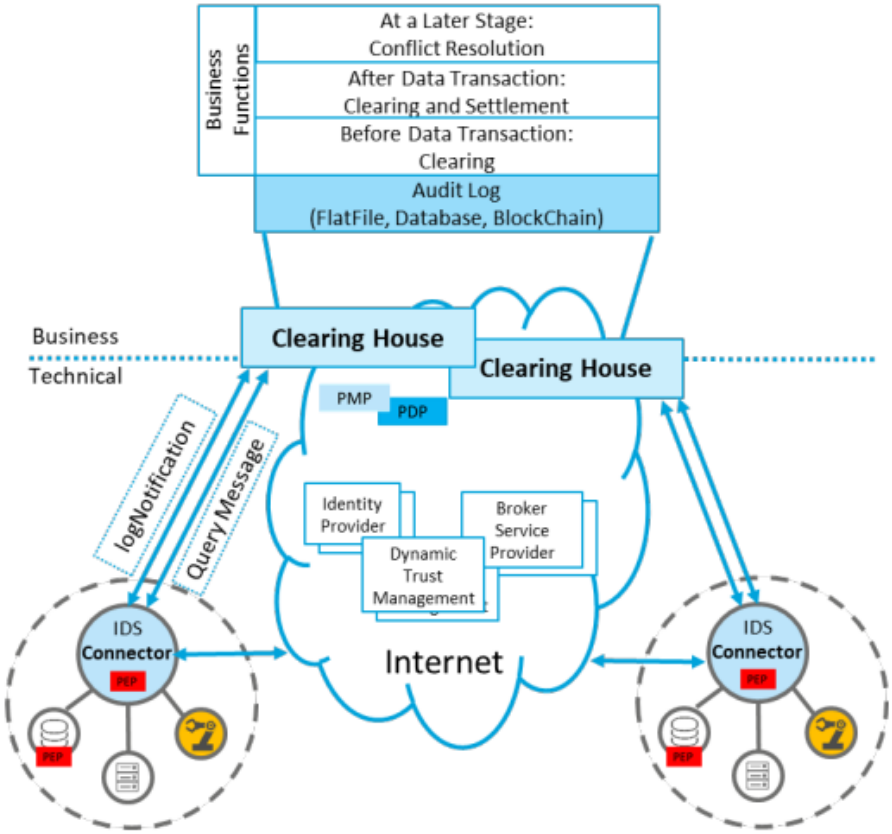
図表 6-5 に示す通り、データ交換取引前の清算機能、データ交換取引後の決済機能等、法務・財務・技術面でのサポートが重要な役割を担っている。

なお、上記の記述にあたっては IDS Clearing House の関連箇所を参照した[193]。

[192] *Specification: IDS Meta Data Broker* International Data Spaces Association, https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-White-Paper-Specification-IDS-Meta-Data-Broker.pdf （2022 年 3 月 15 日アクセス）

[193] *Specification: IDS Clearing House* International Data Spaces Association, https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-White-Paper-Specification-IDS-Clearing-House-.pdf （2022 年 3 月 17 日アクセス）

図表 6-4 クリアリングハウスの機能（図）



図表 6-5 クリアリングハウスの機能（表）

プロセスフェーズ	機能
データ共有前	データ共有取引の清算機能 • 法的：利用契約とデータ利用ポリシーの確認 • 財務的：支払条件の確認 • 技術的：データ共有に関する合意・利用契約に準拠した取引実行の有効化
データ共有中	監視・ロギング機能と決済機能（データ共有プロセス前・中） • データ共有取引の破棄 • 取引のメタデータのロギング • データ出所の追跡 • データ取引の監視・報告 • データ取引の監査・追跡 • データ取引の課金・請求
データ共有後	決済機能（データ共有後又はデータを共有しない場合） • 利用契約やデータ利用ポリシーの違反に関するクレームの調査 • 利用契約やデータ利用ポリシーに違反した場合の措置の実施 • 法的：裁判所への提訴 • 財務的：金銭的補償の要求 • 技術的：ID プロバイダ経由で参加者をブロック又は参加者の信頼度をグレードダウン

6.1.7 アプリストア

アプリストアはデータアプリを提供する。これは、IDS コネクタにデプロイして、データの変換・集約・分析等のタスクを実行することができるアプリケーションである。データアプリは、IDS が承認した証明書発行機関によって認証される場合がある。

なお、上記の記述にあたっては IDS リファレンスアーキテクチャモデルの関連箇所を参照した[194]。

6.1.8 コネクタ

(1) コネクタの特徴（Eclipse Data Connector を中心に）

コネクタは、参加企業又はプラットフォームを利用するためのコンポーネントであり、これにより IDS エコシステムへの技術的なアクセスを提供する。コネクタは、IDS リファレンスアーキテクチャモデルの仕様とそれを基にした IDS の認定基準に準拠したもので構成されている。

コネクタを使うことで、高い信頼性かつ共有ルールでデータ連携が可能になる。その他のデータ連携方法には、EDI やオープン API があるが、EDI はアプリケーションに依存する部分があり、信頼性を確立するための共通認識が EDI には存在しない。また、オープン API も IDS コネクタのように共通のルールが存在しない[195]。

フラウンホーファー研究機構のウェブサイトによると、Eclipse Data Connector、Trusted Connector、Open Data Connector の 3 種類のコネクタが存在する。各コネクタの違いについては、図表 6-6 の通りである。

図表 6-6 コネクタの種類・用途等

Eclipse Data Connector	Trusted Connector	Open Data Connector
Connector は、フラウンホーファー研究機構で生まれた OSS で、IDS のデータ主権の概念をデータ交換の面から実装している。	Trusted Connector は、他の分野にも容易に適用できるオープンな IoT エッジゲートウェイプラットフォームである。 IDS のセキュリティアーキテクチャとトラストプロファイルのリファレンス実装の位置づけである。	Open Data としてデータを公開するための、即時で利用可能なコネクタである。このコネクタは、さまざまな種類のデータソースに対応するアダプタを提供し、新しいデータソースアダプタを開発するための無駄のない仕様を提供している。

上記のうち、本報告書の執筆時点において主要コネクタとして IDS により採用されているのは、Eclipse Dataspace Connector（EDC）である。

異なるコネクタ間の接続は同じプロトコルを採用する必要があり、現在 IDS コネクタは IDSCP と IDS multipart の 2 つプロトコルを持っている。

---

194 *REFERENCE ARCHITECTURE MODEL 3.0*, INTERNATIONAL DATA SPACES ASSOCIATION, December 2020, http://archives.greenairnews.com/www.fraunhofer.de/content/dam/zv/en/fields-of-research/industrial-data-space/IDS-Reference-Architecture-Model.pdf （2022 年 3 月 17 日アクセス）

195 フラウンホーファー研究機構よりヒアリング

IDSCP は接続元と接続先にトンネルを作って秘匿性の高いコンピューティングアプローチでセキュリティに優れている。膨大データの送受信等性能面も優れている。セキュリティの性能面が優れている一方、IDSCP は SI 型でクライアントごとに実装が必要で、少し複雑である。また、メッセージ形式等に対する特別なサポートも必要とされる。

IDS multipart は https ベースの RESTful アプローチであり、セキュリティ的に IDSCP ほど高くはない。なお、本報告書を執筆する時点で、EDC では IDS multipart のみ存在している[196]。

EDC は、データ共有にまつわる課題（マルチクラウド共有、共有後の管理、安全なデータ公開）を解決するためのオープンソースプラットフォームであり、Eclipse Foundation によって開発されている。

EDC の特徴は下記 5 点である。これらの実現を可能とする仕組は図表 6-7 の通りであり、特徴の各番号は下図中の赤字で表示されている番号に対応している。また、図表 6-7 に記載のコンポーネントの概要については、図表 6-8 の通りである。

① 複数の ID プロバイダ（Web DID、OAuth2、ION（Blockchain）等）をサポートすることが可能である。

② アセットカタログとアクセスコントロールのコントロールを維持する。

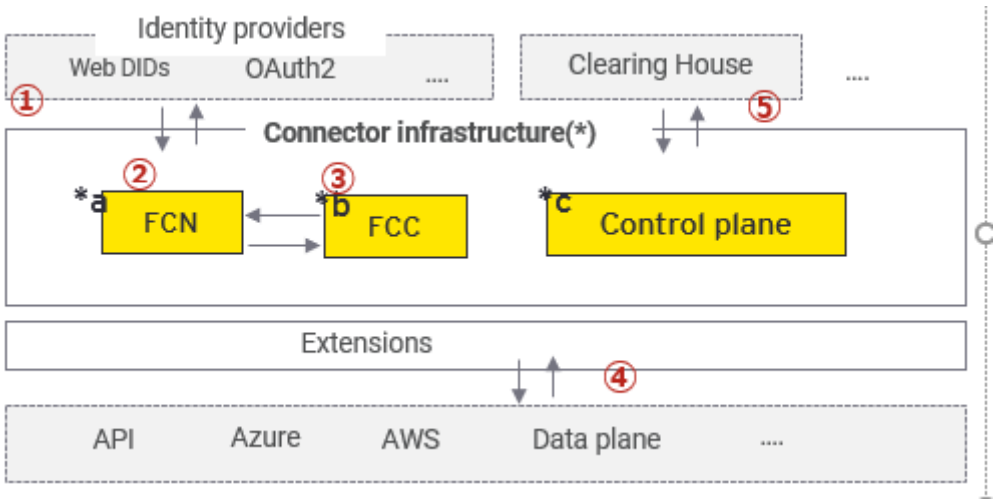
③ 高いスケーラビリティと信頼性を有する。

④ コントロールプレーンとデータプレーンの分離、マルチクラウドへの対応が可能である。

⑤ 監視・監査への対応が可能である。

なお、上記の記述にあたっては GitHub の関連箇所を参照した[197]。

図表 6-7 EDC の特徴



196 フラウンホーファー研究機構よりヒアリング

197 “GitHub -eclipse-dataspaceconnector/DataSpaceConnector” GitHub, https://github.com/eclipse-dataspaceconnector/DataSpaceConnector（2022 年 3 月 17 日アクセス）

図表 6-8 EDC を特徴づけるコンポーネント

コンポーネント	概要
*a） FCN（Federated Cache Node）	アセットカタログを他のコネクタに対して利用可能にし、ポリシーによるアクセスやアクセスコントロールのチェックを行い、他のコネクタから送付されるアセットのフィルタリングを行う。
*b） FCC（Federated Cache Crawler）	FCN に ID と Credential を提示し、他の FCN インスタンスを定期的にクロールして結果をキャッシュする。アセットカタログがローカルにミラーリングされるため、瞬時に分散クエリが可能であり、オリジン FCN がダウンしても既にローカルキャッシュされたコピーが機能する。
*c） コントロールプレーン	検証、契約交渉、ポリシー強制、プロビジョニング管理を担う。

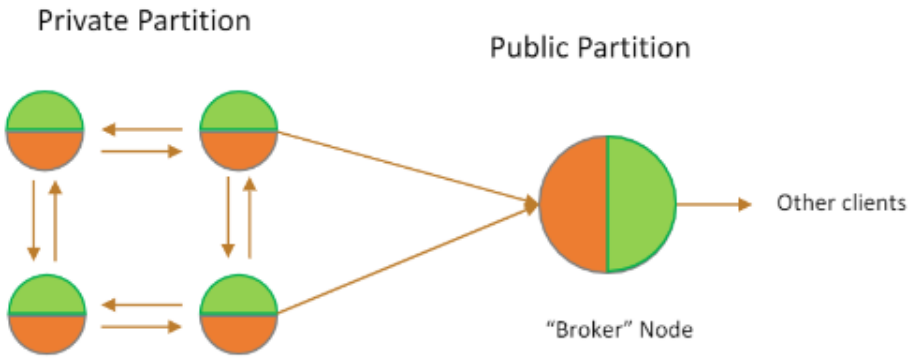
EDC の優位性は 6 点にあり、それぞれ図表 6-9 の通りである。

図表 6-9 EDC の優位性

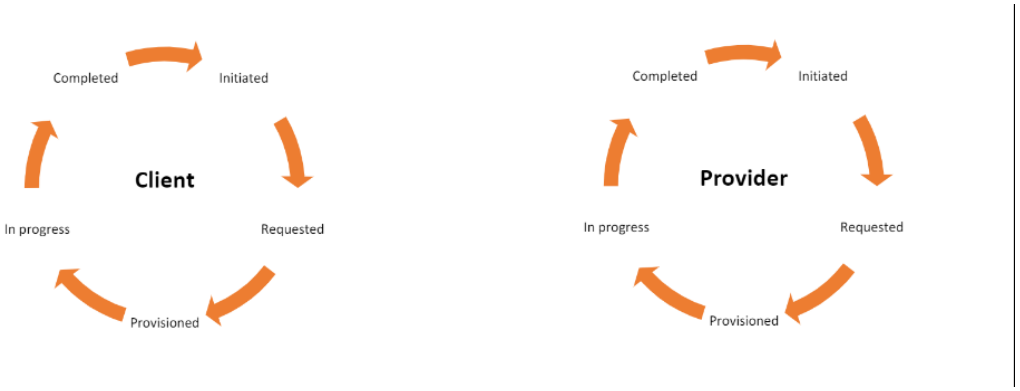
コンポーネント	概要
プライベートデータとパブリックデータへの対応可能性	• クローラーアーキテクチャは P2P（ピアツーピア）で設計されているが、メタデータブローカーモデルやハイブリッドな組み合わせもサポート可能である。 • データスペースには、P2P で共有されるプライベートデータと、ブローカー経由で提供されるパブリックデータが存在する場合があるが、FCC と FCN のノードで設定することでいずれの場合にも対応することが可能である（図表 6-10 の概念図を参照されたい）。 • 組織は、目的やプライバシーの許容範囲に応じて適切にデータを分類し、非公開にすることができる。
シンプルなモジュール方式	プログラムの機能は、独立した交換可能なモジュールに分離され、それぞれが目的の機能の一面のみを実行するのに必要なすべてを含んでいる。これにより、他の機能への依存や影響を排除して、機能の修正や改良を容易に行うことが可能である。
非同期かつ高可用性のシステム	コネクタは非同期システムであり、リクエストはクライアントとプロバイダのコネクタ上であらかじめ定義された一連の状態を非同期に遷移する。
転送プロセスへの監査可能	取引は、クリアリングハウス上のログ記録機能により、完全に監査可能である。クリアリングハウスは、必要に応じて全取引の分散型かつ監査可能なトレーサビリティを提供する。
シングルポイントオブフェイルの排除（クラウドアウェアのポリシー実施とプロジェクション）	• 各 FCN は、他の FCN インスタンスを定期的にクロールした結果をキャッシュしている。これにより、アセットカタログがローカルにミラーリングされるため（クライアントノードが閲覧する権利を持つアセットのみ）、瞬時に分散クエリが可能である（図表 6-11 の概念図を参照されたい）。 • 上記ミラーリングにより、オリジンの FCN がダウンした場合においても、ローカルにキャッシュされたコ

コンポーネント	概要
	ピーが機能するため、データスペースの耐障害性と弾力性が確保されることになる。
GDPR や eIDAS 等の一般的なルールやポリシーに準拠した設計	コネクタは EU の規制に基づいて開発されており、コネクタを使用することにより、すべてのユーザが EU のルールに準拠することが可能になる。

図表 6-10 EDC によるプライベートデータとパブリックデータへの対応（概念図）



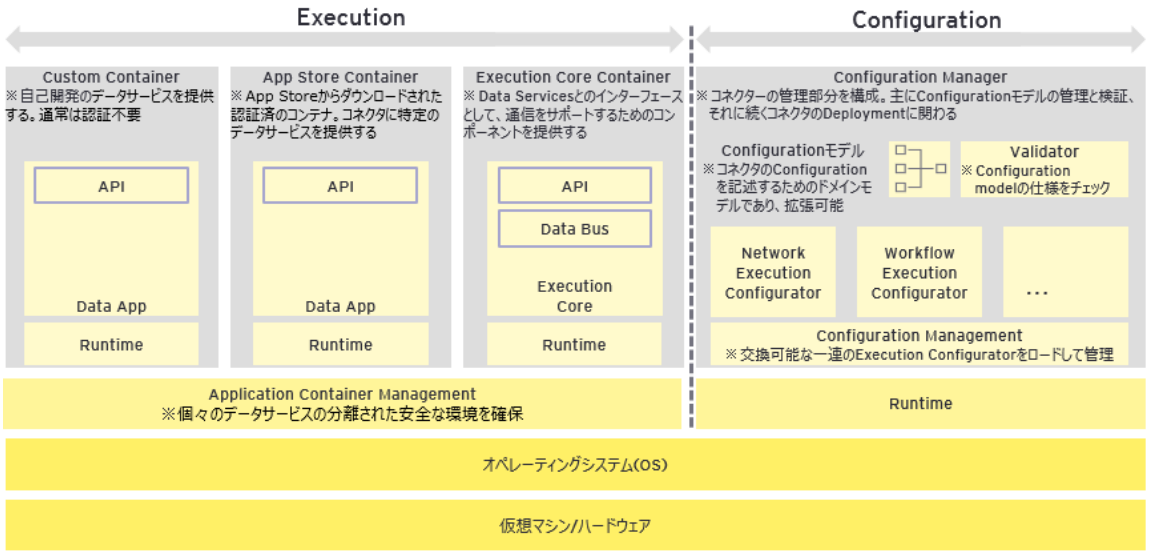
図表 6-11 EDC によるミラーリング（概念図）



(2) コネクタ内部のアーキテクチャ

コネクタアーキテクチャは、アプリケーションコンテナ管理技術を利用して、個々のデータサービスのための分離された安全な環境を確保するためのものであり、図表 6-12 の通りである。データサービスは、データを保存、アクセス又は処理するための API を提供するシステムと一致している。

図表 6-12 コネクタアーキテクチャ



IDS Reference Architecture Model(p.62) : FIGURE 3.32: CONNECTOR ARCHITECTURE

機密データのプライバシーを確保するため、データ処理はできるだけデータソースに近い場所で行われる必要がある。つまり、データの前処理（フィルタリング、匿名化、分析等）はすべて内部コネクタで実行され、他の参加者が利用できるようにすることを意図したデータのみが外部コネクタを通じて見えるようにする必要がある。

データアプリは、データ処理やデータ変換機能をカプセル化し、アプリケーションコンテナ管理で簡単にインストールできるようにコンテナイメージとしてバンドルされたデータサービスである。

具体的にコネクタを設置する場合、既存のコンポーネントを変更したり、オプションのコンポーネントを追加したりすることができるため、この構造とは異なる場合がある。図表 6-12 に示すコンポーネントは、Connector Execution と Connector Configuration の 2 種類に大別され、それぞれデータ交換時点とそれに先行する設定時点のフェーズに対応している。

Connector Execution フェーズには、図表 6-13 にあるコンポーネントが含まれる。

図表 6-13 Connector Execution に含まれるコンポーネント

コンポーネント	概要
Application Container Management	• データサービスとコンテナの拡張制御を実施するための機能を提供する。 • 開発時やリソースが限られたシステムにおいては、アプリケーションコンテナ管理を省略することができる。
Execution Core Container	• データサービスとのインターフェースとして、通信をサポートするためのコンポーネント（データルータ、コネクタへのデータバス等）を提供する。 • データルータは、事前定義された Configuration パラメータに従って呼び出されるデータサービスとの通信を処理する。 • データバスは、他のコネクタのデータサービス及びデータバスコンポーネントとデータを交換する。
App Store Container	App Store からダウンロードされた認定コンテナであり、コネクタに特定のデータサービスを提供する。
Custom Container	• 自己開発のデータサービスを提供する。 • カスタムコンテナは通常、認証を必要としない。
Data Service	• データルータから呼び出されるパブリック API を定義する。この API は、構成モデルにインポートされるメタディスクリプションで正式に指定される。 • データサービスはあらゆるプログラミング言語で実装することができ、様々な実行環境を対象とすることができる。 • 既存のコンポーネントを再利用することで、他の統合プラットフォームからの移行を簡素化することができる。
Runtime of Data Service	• データサービスのランタイムは、選択したテクノロジーとプログラミング言語によって異なる。 • 使用可能なランタイムは、ホストコンピュータの基本オペレーティングシステムのみに依存する。

Configuration フェーズには、図表 6-14 のコンポーネントが含まれる。

図表 6-14 Connector Configuration に含まれるコンポーネント

コンポーネント	概要
Configuration Manager	• コンテナ化されたアプリケーションの管理を行う機能群（コレクション）であり、主に Configuration モデルの管理と検証、その後のコネクタのデプロイを担う。 • コネクタのデプロイに際しては、Configuration Manager（後述）が管理する Execution Configurator（後述）のコレクションに処理を実行させる（デレゲーション）。

コンポーネント	概要
Configuration Model	• コネクタの Configuration を記述するための拡張可能等メインモデルである。 • 特定のテクノロジーに依存しない相互接続に関わる Configuration の側面で構成するためのモデルである。 モデルの構成要素については、 • 図表 6-15 の通りである。
Configurator Management	• Execution Configurator のコレクションをロードし、それぞれを管理する。 • コネクタがデプロイされると、Configurator Management は各タスクを Execution Configurator に実行させる（デレゲーション）
Execution Configurator	• Configuration Model の特定の側面を実行又は特定のテクノロジーに変換する交換可能なプラグインである。 • Configuration を実行する手順は使用するテクノロジーによって異なる。 • 一般的な例に、Configuration ファイルの生成や Configuration API の使用がある。
Validator	• Configuration Model が自己定義したルールと IDS で指定された一般的なルールにそれぞれ準拠しているかどうかをチェックする。

図表 6-15 Connector Configuration Model の構成要素

コンポーネント			概要
General Information			下記事項を定義 • Configuration タイプ • コネクタのタイプ（ベース・トラスト・トラスト＋のステータス、モバイル、組み込み、開発者） • コネクタのバージョン • Configuration に加えられた最後の変更のタイムスタンプ • Configuration ステータス（開発、テスト、ライブ） • 担当者の名前
Lifecycle	Data Flow （データサービスとデータバスの間でデータルータによって確立されるタスクと接続の Configuration を定義）	Networking	コネクタの内部及び外部コネクタへの接続に使用されるネットワークパラメータ（ポート、IP 等）を定義
		Security	接続に使用する必要がある SSL 証明書又は使用する必要がある公開鍵基盤（PKI）に関する情報を定義
		Compliance/ Data Sovereignty	コネクタのデプロイに際して Validator（前述）によってチェックされるルールを定義
	Service Configuration	Metadata	さまざまなコネクタ・コンポーネントによって使用される入力及び出力のデータ型を定義

コンポーネント			概要
	Publishing （外部の参加者に提供されるデータフロー又はデータサービスを定義）	Identity Management	コネクタに対応する ID プロバイダを定義
		Accounting	参加者間のデータ交換トランザクションの「アカウンティング」に際して、契約仕様、価格設定モデル、請求の詳細等の追加情報の記録方法を定義
		Clearing	特定のデータ交換取引に関してどのクリアリングハウスに通知する必要があるかを定義

Connector Execution と Connector Configuration と 2 つのフェーズが分離しているため、これらのコンポーネントを独立して開発し、後に運用することが可能である。また、コネクタのデプロイに際しては、与えられた要件に応じて、さまざまな種類の通信及び暗号化技術を使用することができる。

なお、上記の記述にあたっては IDS リファレンスアーキテクチャモデルの関連箇所を参照した[198]。

[198] *REFERENCE ARCHITECTURE MODEL 3.0*, INTERNATIONAL DATA SPACES ASSOCIATION, December 2020, p62-p66, http://archives.greenairnews.com/www.fraunhofer.de/content/dam/zv/en/fields-of-research/industrial-data-space/IDS-Reference-Architecture-Model.pdf （2022 年 3 月 18 日アクセス）

6.2 Gaia-X コンポーネント

6.2.1 ID とトラスト

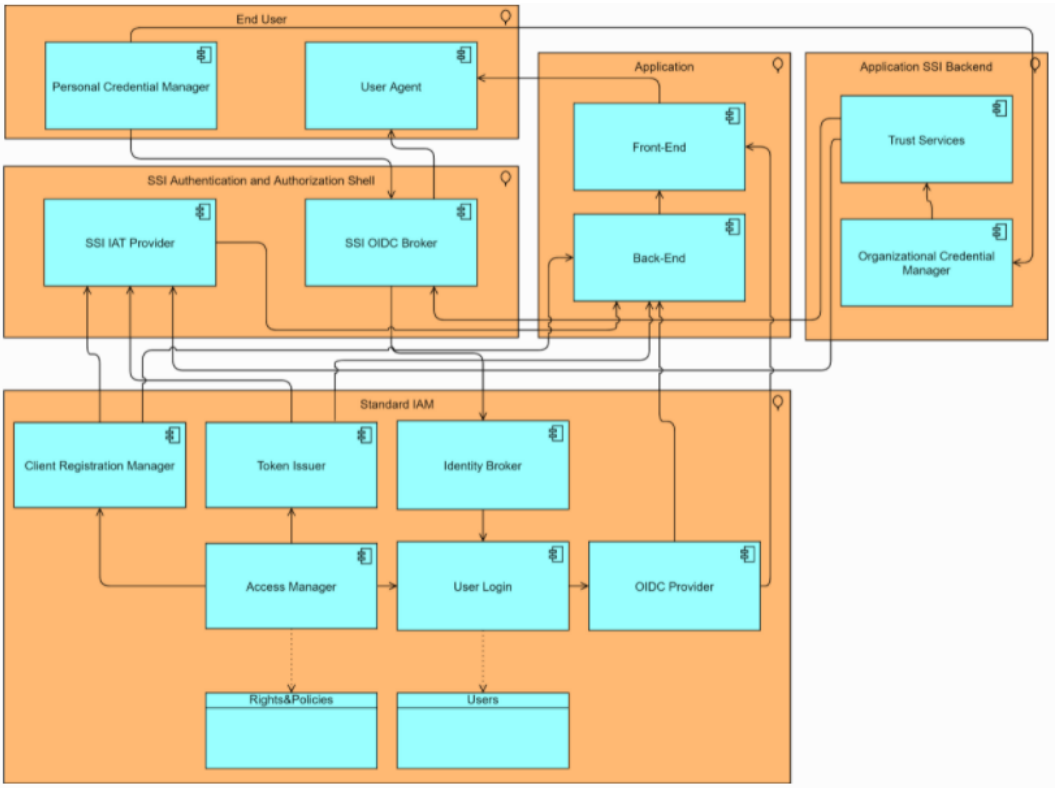
(1) Authentication / Authorization

AA[199]はいくつかのモジュールに分けられており、SSI を実現するモジュールと SSO として一般的に利用されている IAM システムを統合することにより、Gaia-X 環境での ID と ID に紐づく属性の操作及び他の参加者との交換を実現する。

AA は、SSI ベースのユーザログインを可能にする SSI OIDC Broker と SSI ベースの動的クライアント登録を可能にする SSI IAT Provider の 2 つのモジュールで構成される。具体的には、これらのモジュールによって IAM SSI Adoption Shell が形成される。IAM SSI Adoption Shell は、SSI ベースのプロトコルに必要な機能をカプセル化し、標準 IAM システムが処理できるデータ形式に変換する。

図表 6-16 に示すように、AA によって、SSI ベースのモジュールを、標準的な OpenID Connect 及び OAuth2 準拠の IAM に追加することで、既存の IAM に適応させることが可能になる。

図表 6-16 SSI Adoption Shell と各モジュールの連携

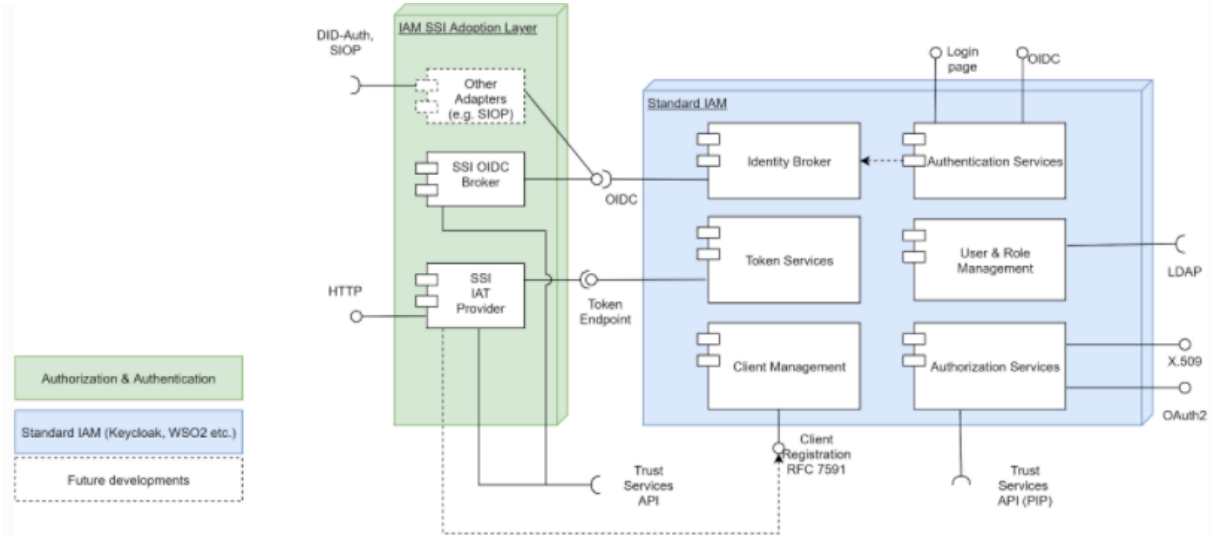


[199] Authentication / Authorization, Gaia-X AISBL Technical Committee, August 12, 2021, https://gaia-x.gitlab.io/technical-committee/federation-services/federation-service-specifications/L02_IDM_PCM/idm_pcm/#etyol9z2mbht, （2022 年 3 月 24 日アクセス）

上図は、AA のモジュールが SSI ベースのアプリケーションバックエンドに接続されていることを示している。また、上図の矢印はユーザ又はバックエンドによるアクションによるデータフローを示している。なお、各モジュール間の連携は、HTTP 通信を介して行われる。図中に登場する「Trust Services」と「Organizational Credential Manager」は、ID とトラストにおける他のコンポーネントであり、「6.2.1 (3) Organization Credential Manager」「6.2.1 (4) Trust Services API」にて詳述する。

図表 6-17 は AA のモジュール部分を緑色、標準 IAM のモジュール部分を青色で示している。

図表 6-17 AA と標準 IAM のモジュール



AA によって下記の機能が実現される。

- SSI ベースの初期アクセストークンの発行（IAT）
- SSI ベースのログイン

上記の機能は、Trust Service API を介してトリガーされるバックチャネル認証で実現される。TSA は、バックグラウンドで HTTP を通じて関連するバックチャネル認証ポイントを接続するステートレスポリシー評価を行う。また、バックチャネルを通じてクライアント側で検証する必要のあるすべての情報を送信する。これは、OpenID Connect Client Initiated Backchannel Authentication（CIBA）[200]の原則に基づいている。

DID SIOP（Self-Issued OpenID Provider）[201]のような他の機能は、OpenID Foundation によって仕様が定義される可能性がある。特に、DID SIOP のフローは現在初期バージョンであり、アップデート版の仕様については OpenID Foundation にて現在検討中であ

[200] OpenID Connect Client-Initiated Backchannel Authentication Flow - Core 1.0, Gonzalo Fernandez Rodriguez, etc., September 1, 2021, https://openid.net/specs/openid-client-initiated-backchannel-authentication-core-1_0.html, （2022 年 3 月 24 日アクセス）
[201] Self-Issued OpenID Connect Provider DID Profile v0.1, Oliver Terbu, etc., February 18, 2021, https://identity.foundation/did-siop/, （2022 年 3 月 24 日アクセス）

る。

(2) Personal Credential Manager

PCM[202]は、プリンシパルによって使用される。プリンシパルは、自分に発行された VC を格納したり、サービスを受けるために必要な発言を証明したりするために、PCM を利用する。

PCM により以下のプロセスがサポートされる。

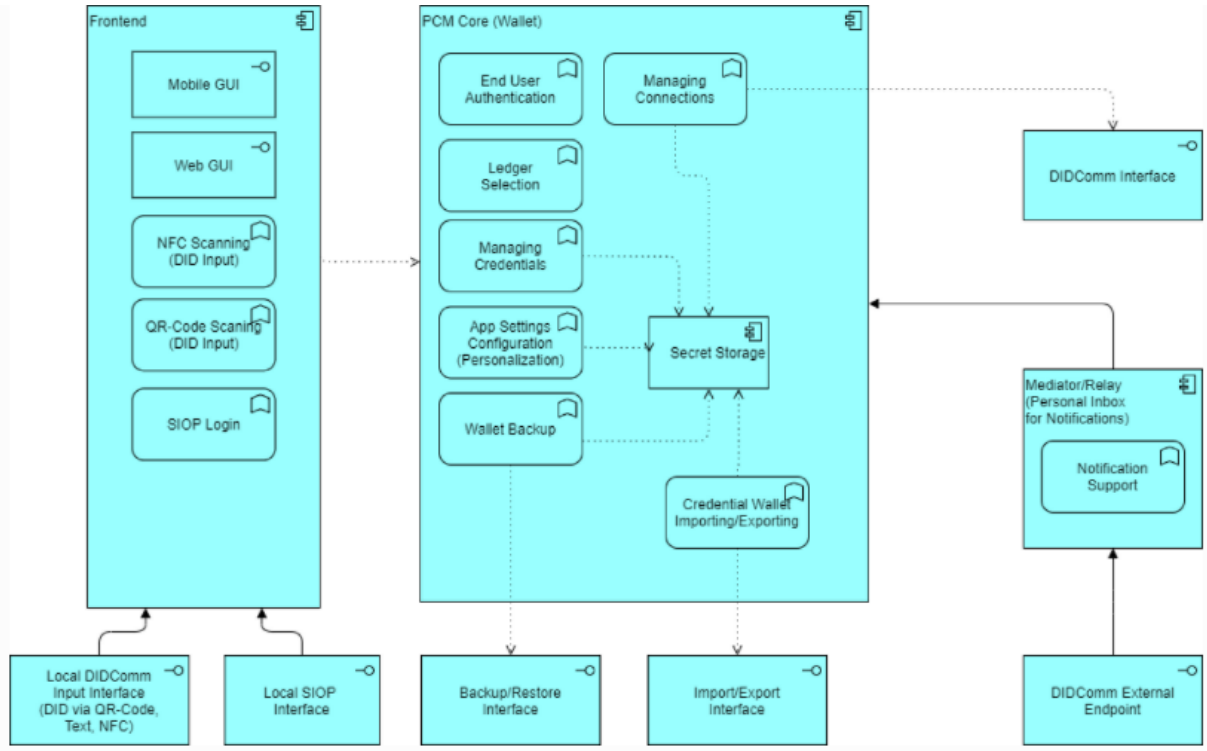
- プリンシパルのオンボーディング
- プロバイダから認証してもらう際の方式としての DIDComm 認証
- 既存の OIDC クライアントや OpenID プロバイダとの互換性がある SIOP DID
- 他者との安全かつ信頼できる接続の確立
- 分散台帳の選択
- 認証当事者からの VC の受領（例：Gaia-X 参加者から発行されるプリンシパル用の Credential）
- 他者への VP の提示
- PCM へのアクセス時における多要素認証
- バックアップとリストア
- パーソナライゼーション
- アクセシビリティ

PCM を使用すると、エンドユーザはプライバシーを保護された状態で DID ベースのエコシステムと対話できる。PCM は、取得した DID と ID 属性を安全に保管するコンポーネントであり、認証とサービス利用のために必要な ID 属性を選択的に提示することができる。

図表 6-18 は、PCM のモジュールのアーキテクチャを表している。

[202] Personal Credential Manager, Gaia-X AISBL Technical Committee, August 12, 2021, https://gaia-x.gitlab.io/technical-committee/federation-services/federation-service-specifications/L02_IDM_PCM/idm_pcm/#etyol9z2mbht, （2022 年 3 月 24 日アクセス）

図表 6-18 PCM のモジュールのアーキテクチャ



図表 6-18 に示されているように、PCM は、下記のレイヤーで構成されている。

- フロントエンドレイヤー
- コアウォレットレイヤー
- リレーレイヤー
- さらに、フロントエンドレイヤーは、次の機能とモジュールで構成されている。
- エンドユーザ認証
- GUI
- 入力インターフェース

エンドユーザ認証モジュールによって、スマートフォンの場合の指紋認証、PIN、パスワード等の安全なユーザ認証方式が実現される。

また、プリンシパルは GUI モジュールを介して PCM 機能を使用できる。

入力インターフェースによって、QR コード処理、近距離無線通信（NFC）等が可能となり、ピアツーピアでの情報交換や、近くのユーザに対して Credential 情報を提示可能である。

コアウォレットレイヤーは、次の機能とコンポーネントで構成されている。

- 接続の管理
- パーソナライズ
- Credential の管理
- ウォレットのバックアップ
- ウォレットのインポート/エクスポート
- シークレットストレージ

各機能の内容を図表 6-19 に示す。

図表 6-19 コアウォレットの機能

機能	内容
パーソナライズ	特定のエンドユーザのニーズと要件に合わせて PCM の設定変更を可能にする。
Credential の管理機能	他の参加者によって発行された Credential を受領する機能を担っており、ユーザは自分の Credential を提示及び検証できる。また、他の参加者に Credential 属性を証明するための基本機能を有している。 Credential の管理機能は、どの属性をどの参加者に提示するか等、ユーザが有する Credential を制御できる。さらに、DIDComm を用いた通信や SIOP 方式のログイン等を実現できる。
ウォレットのバックアップ機能	取得した Credential とアプリ設定のバックアップ及びリストアを可能にする。
ウォレットのインポート/エクスポート機能	ウォレットのインポート/エクスポート機能は、Credential を別の PCM に安全にエクスポートすることや、保有している PCM に Credential をインポートすることが可能になる。これにより、いわゆるクロスウォレット互換性（Credential の管理機能に関して同じ技術仕様に準拠する PCM 間の互換性）を将来的に保証できる。
シークレットストレージ	対応するシークレット部分を含む、取得した Credential の安全なストレージを提供する。

リレーレイヤーは、通知管理を効果的に提供するリレーコンポーネントであり、接続確立のために外部から受信した通知を PCM に転送する。

次に、PCM の 3 つのフォームファクタについて説明する。まず、スマートフォンベースのアプリケーションは、GUI 機能、接続機能、Credential 及びパーソナルウォレット管理機能で構成されている。バックアップ/リストアとパーソナライズは、モバイルスマートフォンアプリでも実装される。スマートフォンベースのアプリでは、接続のインビテーションや NFC 通信、QR コードをスキャンするためのカメラ等、物理的な I/O インターフェースを利用することを想定している。スマートフォンには通常、固定の通信エンドポイントを持たないため、SSI リレーレイヤーは PCM への通知を送信するためクラウド上にデプロイされることを想定している。そのため、スマートフォンの紛失等により発生するリスクへの対処が重要である。可用性とスケーラビリティを改善し、Gaia-X エコシステムに柔軟にアクセスすることを可能にするために、本機能をクラウド環境に移行することを検討している。

2 つ目のフォームファクタとしてデスクトップ及びラップトップ PC 向けブラウザ用アプリケーション及びアドオンについて説明する。GUI 機能、接続機能、Credential 及びウォレット管理、バックアップ/リストア及びパーソナライズは、ローカルブラウザ内で処理される。接続インビテーションは、電子メール又はその他の通信手段よってサポートされる。スマートフォンアプリと同様に、ローカルユーザのデスクトップ及びラップトップ PC についても、固定通信エンドポイントがないことが想定される。そのため、リレーレイヤーは PCM への通知のためにクラウド上にデプロイされる必要がある。

最後に、クラウドベースのフォームファクタについて説明する。プリンシパルはクラウドにデプロイされたエージェントに安全に接続して認証し、そこからエージェントは

PCM の全機能を利用できる。これは、ユーザが物理的な端末の損失によるリスクを回避することができる。

いずれのフォームファクタの場合においても、PCM に必要なプライバシーとセキュリティを確保する必要がある。

(3) Organization Credential Manager

OCM[203]は、Gaia-X エコシステム内の異なる参加者間で分散型方式に基づくトラストを確立するために用いられる。

OCM は、ID プロバイダが集中型方式で提供する一般的な機能の一部を、分散型 ID、VC、VP の概念を用いて実現する。

上記を実現するために、様々な属性及び文書に対して署名するための参加者 ID の管理や、受領した外部文書を検証することができる機能が必要である。具体的には、ID に対応するデジタル署名付きの VC の作成、既存の VC や既に受け取った VC に基づく VP の発行、自身の属性の証明のための第三者からの VC の要求、接続要求や証明要求の検証も含まれる。通信に使用されるフォーマットは、Hyperledger Indy のコンテキストで記述された RFC と W3C の標準に準拠する。

OCM により以下のプロセスがサポートされる。

- 参加者のオンボーディング
- プリンシパルのオンボーディング
- オフボーディング
- 認証
- トラストの確立

Hyperledger Indy における Hyperledger Aries Cloud Agent[204]と Hyperledger Labs の Business Partner Agent[205]は、OCM の機能をサポートするフレームワークとコンポーネントを構築する上で重要である。

OCM の機能は、ランタイムコンポーネントとして提供され、エンドポイントを REST API として公開し、HTTPS 等を用いた暗号化接続を使用してネットワーク経由でアクセスできるようにしなければならない。OCM は、マイクロサービスベースのアーキテクチャや負荷分散等を用いてスケーラビリティを考慮することが求められる。

本コンポーネントは Gaia-X エコシステムの参加者間でのトラスト確立において鍵となるため、セキュリティ対策は特に重要である。具体的には、公開された REST API の保護、データストレージの保護、アクセスコントロール等を考慮する必要がある。秘密鍵等の保管は、ハードウェアに対してセキュリティモジュールを組み込む等して、特に安全性を確保しなければならない。また、OCM は、GDPR に準拠し、監査可能でなけれ

---

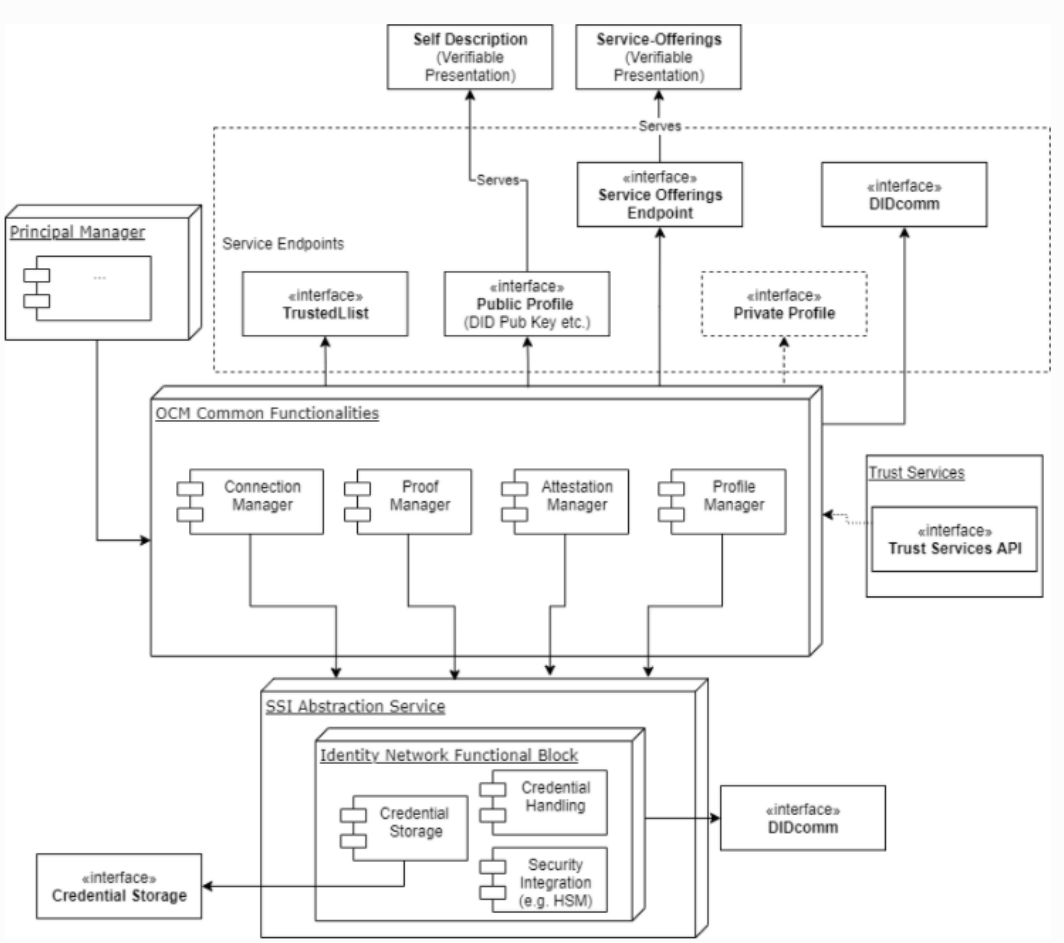
[203] Organization Credential Manager, Gaia-X AISBL Technical Committee, August 12, 2021, https://gaia-x.gitlab.io/technical-committee/federation-services/federation-service-specifications/L03_IDM_OCM/idm_ocm/, （2022 年 3 月 24 日アクセス）

[204] Hyperledger Aries (2021), Hyperledger Aries Cloud Agent Python, andrewwhitehead, March 29, 2021, (https://github.com/hyperledger/aries-cloudagent-python, （2022 年 3 月 24 日アクセス）

[205] Hyperledger Aries (2021), Business Partner Agent, etschelp, March 29, 2021, (https://github.com/hyperledger-labs/business-partner-agent, （2022 年 3 月 24 日アクセス）

ばならない。

図表 6-20 OCM コンポーネントの概観



OCM の中核機能は図表 6-21 の通りである。

図表 6-21 OCM の中核機能

中核機能	内容
エンティティ間の信頼できる接続の確立	• コネクションインビテーションの作成 • 受信した接続インビテーションの処理 • 既存接続の管理 • 接続と証明された属性のマッピングを行い、信頼できる接続を可能にする
VC 交換	• 参加者、プリンシパル、アセットに対する Credential 発行 • 受領した Credential 要求の処理
Verifiable Proof 交換	• エコシステム内の他の参加者等に対する証明の要求と検証 • 受領した証明依頼の処理 • Credential の保管

中核機能	内容
	• 証明提示の有効性確認
検証可能なサービス エンドポイントの提供	• 公開プロフィール 一般に公開されている企業情報（押印等）。Gaia-X の仕様に準拠する自己記述が提供する必要がある。 • 非公開プロフィール 特定の組織に加入していることを証明することで閲覧可能になる企業情報 • サービスオファリング 参加者が Gaia-X で提供したいサービスリスト • TrustedList OCM によって信頼されている参加者のリスト。

トラストサービスとの連携は、下記のモジュールで実装される。

- コネクションマネージャ
- 証明マネージャ
- 公認マネージャ

(4) Trust Services API

TSA[206]の基本的な要件は、ポリシー評価、ポリシードリブントラスト、トラストアンカー管理、DID サ、署名・検証の機能を提供し、他のコンポーネントをサポートすることである。これを実現するため、TSA は、他のコンポーネントによって利用可能な REST API のエンドポイントを提供するか、コンポーネントのライブラリとして機能を提供する。さらに、ポリシー組み込み機能によってサービス信頼性を高めることが可能である。

例えば、ポリシー評価のために検証されたデータを収集することができ、トラストチェーンとトラストセットの署名と検証を行うことができる。全てのポリシーは、部分的に事前に定義され、部分的に参加者自身によって決定される。ポリシーは GitOps の原則によって管理可能であるべきであり、安全なストレージへの接続が確保されなければならない。

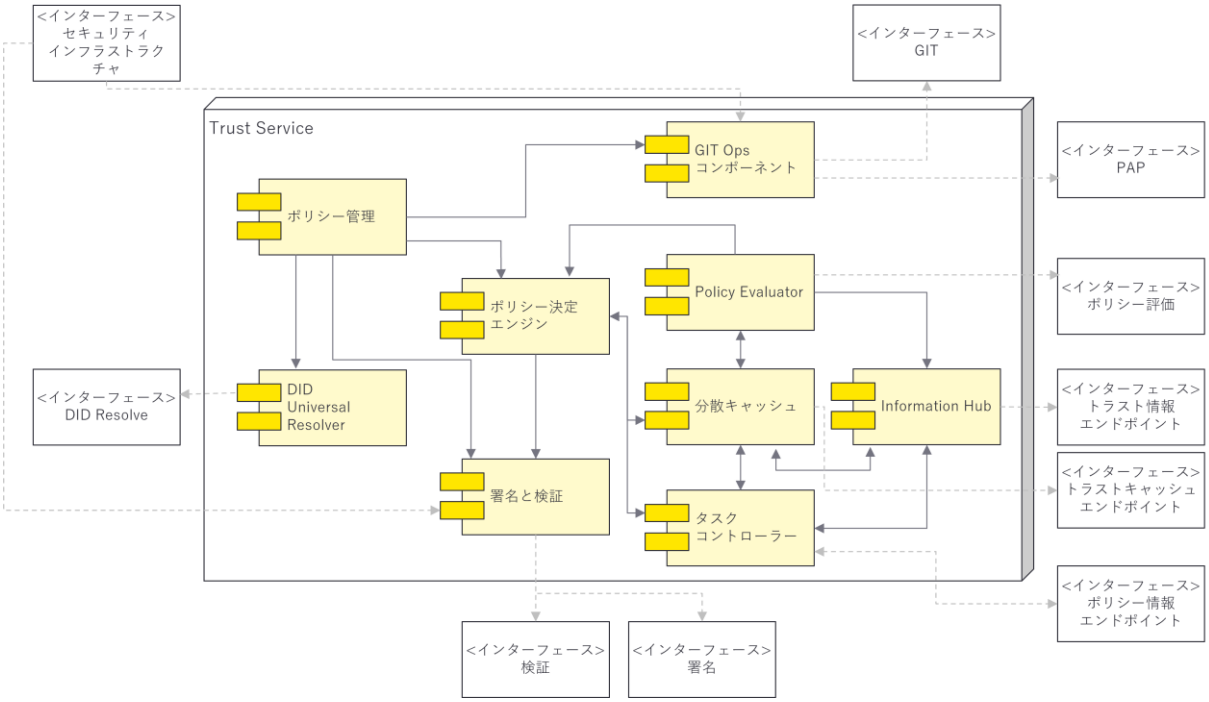
TSA の機能は、ランタイムコンポーネント又はライブラリコンポーネントとして提供される。ランタイムコンポーネントは、エンドポイントを REST サービスとして公開しなければならない。また、ポリシーのプロビジョニングと共有を可能にするために、GitOps によるポリシーコンフィギュレーションを使用する必要がある。このコンポーネントは Gaia-X Trust 及び ID 管理ツールの一部であり、一元的に提供されるものではない。本コンポーネントを維持、更新するためには、データストレージの保護、アクセスコントロール等の適切なセキュリティ対策が施されていなければならない。また、TSA の全体的な機能は、GDPR に準拠し、監査可能でなければならない。

[206] Trust Services API, Gaia-X AISBL Technical Committee, August 12, 2021, https://gaia-x.gitlab.io/technical-committee/federation-services/federation-service-specifications/L04_IDM_TSA/idm_tsa/, （2022 年 3 月 24 日アクセス）

TSA の中核となる機能は以下の通りである。

- VC のデジタル署名の検証
- JSON-LD のプルーフチェーンとプルーフセットの署名と検証
- GitOps による JSON-LD ポリシーの管理
- ポリシーに基づいた信頼性を確保するためのポリシー評価
- DID ドキュメントを解決するための DID 解決エンドポイント

図表 6-22 TSA コンポーネントの概観



6.2.2 フェデレーションカタログ

(1) Core Catalogue Functions

CCF[207]には、公開された自己記述ファイルのための自己記述ストレージと、自己記述グラフの 2 種類のストレージが含まれている。自己記述グラフ内の自己記述間の参照をたどることで、個々の自己記述にまたがる高度なクエリが可能になる。

自己記述は暗号化された署名で保護されているため、一度公開されると変更することができない。自己記述のライフサイクルの状態は、追加のメタデータに記述される。自己記述のライフサイクルには、「Active」、「Revoked」、「Deprecated」、「End-of-Life」の 4 つの状態がある。カタログは、ライフサイクルメタデータを含む、読み込まれている自己記述へのアクセスを可能にする。これにより、コンシューマは自己記述とそれに含まれる証明書を自己主権的に検証することができる。

[207] Core Catalogue Functions, Gaia-X AISBL Technical Committee, August 12, 2021, https://gaia-x.gitlab.io/technical-committee/federation-services/federation-service-specifications/L05_FC_CCF/fc_ccf/, （2022 年 3 月 24 日アクセス）

自己記述グラフには、カタログに掲載されている自己記述のうち、ライフサイクルが「Active」なものからインポートされた情報が含まれている。自己記述グラフは、自己記述にまたがる複雑なクエリを可能にする。

検索結果を客観的かつ無差別に表示するために、内部ランキングを持たないグラフ・クエリ言語を使用する。ユーザによって定義されたフィルタとソート基準に基づき、結果はランダムに並べられる。

プライベート環境でホストされているカタログでは、認証情報は、ユーザが新しい自己記述のアップロードや既存の自己記述のライフサイクル状態を変更することができる。公開カタログでは、自己記述の暗号署名に関して、自己記述の発行者が自己記述の所有者であることを検証される。本検証プロセスにて正当性が確認できる場合、その自己記述はカタログに登録可能である。自己記述ファイルをプライベートチャネルで受け取った第三者が、公開カタログにコピーすることを防ぐために、発行者は自己記述を非公開設定にすることができる。

ビジターとは、そのセッションのアカウント所有していない状態でカタログにアクセスする匿名のユーザである。ビジター以外の全てのユーザは、カタログ REST API を通じてフェデレーションカタログとやりとりする。また、Gaia-X ポータルやカスタム GUI を使用して、バックエンドでカタログ REST API を使用し、カタログと対話することも可能である。カタログと GUI フロントエンドの間の連携は、GUI フロントエンドの個々のユーザの認証されたセッションに基づいて行われる。

プロバイダは、API 又はポータルを使用して、フェデレーションカタログに自己記述を送信することができる。フェデレーションカタログは自己記述を自己記述グラフに保存し、インデックスを付け、他の Gaia-X 参加者やビジターが参照できるようにする。

自己記述を含むファイルは、メタデータとともにカタログに保存される。自己記述はいつでも自己記述グラフにインポートすることができ、グラフを再作成し、その内容を他のカタログと同期させることも可能である。

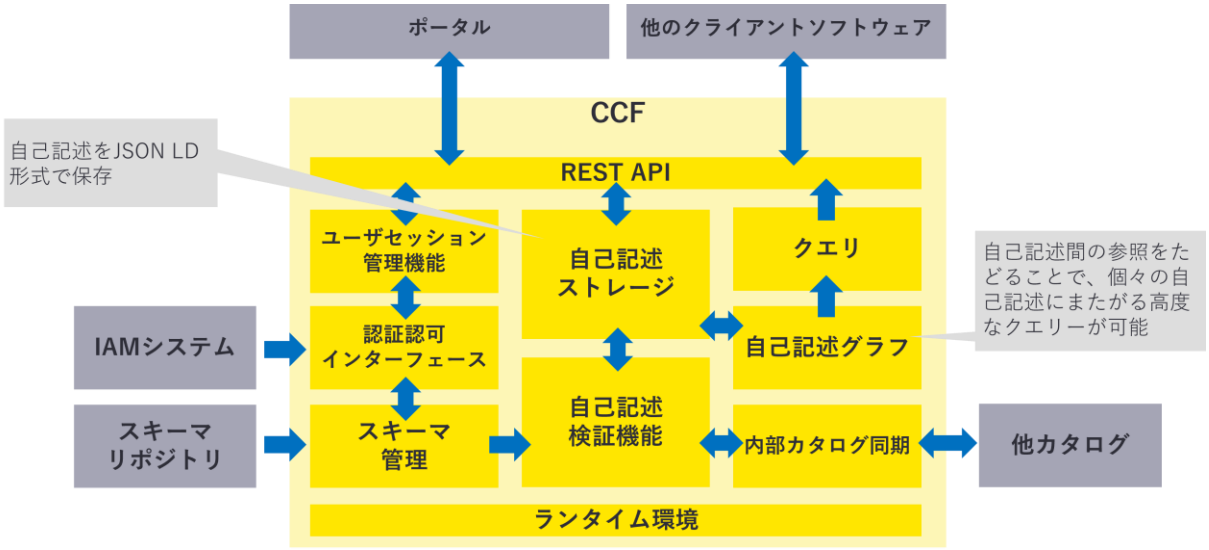
本章では、Gaia-X に登場するエンティティやフェデレーションカタログにおいて重要な要素を説明する。

図表 6-23 CCF に関する重要な項目の説明

項目	説明
参加者	参加者は、自己記述によって記述され、カタログ内のすべてのオブジェクトの所有者となる。登録に成功すると、参加者は自身で全てのパーミッションを持つ初期アカウントを取得する。また、参加者に紐づく複数のプリンシパルが存在する。
プリンシパル	プリンシパルは、特定の参加者に所属し、ロールが割り当てられる。既存の IAM システムを使用せずスタンドアロンのカタログの場合、当該カタログに関連するユーザはカタログ自体によって管理される。
自己記述	カタログの全項目は、自己記述によって記述される。自己記述管理者の役割は、参加者やユーザの自己記述に関する権限は含まれない。自己記述の閲覧は、各登録ユーザと非登録ユーザ（ビジター）に対して許可されている。 自己記述の検証は 2 つの部分に分けられ、各登録ユーザ及び非登録ユーザに対して許可される。 • 信頼性 - 自己記述の署名を確認する。

項目	説明
	• 構文 - スキーマに対する自己記述のシンタックスをチェックする。 自己記述のインポートとエクスポートは、カタログ間同期を目的としており、関連する API コールを持たない想定である。
クエリ	全ての登録ユーザとビジターは、カタログの自己記述グラフ上にて自分で定義したクエリを実行することができる。
スキーマ	スキーマは自己記述の構造を定義する。各登録ユーザ及びビジターは、全てのスキーマの最新バージョンにアクセスすることができる。
ロール	カタログのスタンドアロン展開では、ロールはカタログ自体によって管理される。

図表 6-24 CCF のモジュールの概観



次に、図表 6-24 にて示されている CCF に含まれる各モジュールについて図表 6-25 にて説明する。

図表 6-25 CCF の各モジュールの説明

モジュール	説明
自己記述ストレージ	本モジュールは、JSON-LD 形式の自己記述と、ライフサイクルのためのメタデータ情報を保持する。JSON-LD 部分は暗号署名で保護され、変更できないため、JSON-LD 形式の自己記述自体にメタデータを格納することはできない。
スキーマ管理	全ての自己記述はスキーマ定義に準拠しなければならない。これにより、情報が統一された方法で構造化され、エンドユーザによる検索が可能になる。スキーマ管理、カタログに関連するスキーマのバージョンを保存する。
自己記述検証	自己記述がカタログにアップロードされると、自己記述ストレージに追加される前に、構文及び信頼性の適合性が検証される。
自己記述グラフ	自己記述は、互いに相互参照することができるため、カタログのクエリはこれらの参照を追跡できるようする。クエリを効率的に処理するために、ライフサイクル状態が「Active」の自己記述は、グラフデータベースに読み込まれる。
ユーザセッション管理	カタログソフトウェアは、SSI システムと連携して又はスタンドア

モジュール	説明
	ロンで、非公開にする自己記述に対して操作することが可能である。このような環境では、カタログは自身の参加者を管理する必要がある。
カタログ REST API	本 REST API は、ユーザがカタログと対話するための主要な外部インターフェースである。

6.2.3 データ主権サービス

(1) Data Contract Service

本章で説明する DCS[208]は、Gaia-X データエコシステムにおいて重要な役割を果たす。DCS に関する用語と説明については、図表 6-26 の通りである。現時点で詳細の仕様が固まっていない部分もあるが、将来的にはステートレスなマイクロサービス、技術的なポリシーを強制させるデータ交換のコネクタ、データアプリ、Enclaves 機能等を搭載することが可能になると見込んでいる。

前提として、Gaia-X のデータ取引は、以下の部分から構成される。

図表 6-26 DCS に係る用語と説明

項目	説明
データアセット	既存のデータセット、データベース等が該当する。これらは、購入又はレンタルされる可能性があり、センサー等で取得されるデータ、3D プリンタ用のモデル、監視カメラの映像等、静的又は動的なあらゆるデータである。
データアセットの自己記述	自己記述は全てのサービスオファリングや参加者が有しており、データアセットも同様である。データアセットの自己記述には、データ形式、サイズ、コンテンツ等の通常のメタデータ情報だけでなく、キーバリューデータから法的拘束力のある契約のテンプレートに変換するデータも含まれるため、かなり厳しい制限と要件がある。 データ契約交渉は、手動又は自動トリガーによるデータアセットの送信につながるが、データアセットがデータコンシューマの手に渡るとすぐに、データアセットのユーセージポリシーの施行は不可能になる。そのため、法的なポリシー適用が自然な選択肢となるが、信頼できる法的根拠を得るためには、データプロバイダとデータコンシューマの間で実際の契約を結ぶ必要がある。自己記述とはリカルディアン契約であり、人間が読むことも機械が読むこともでき、暗号的に署名され改ざんできないようにされ、分散型方式で検証可能であり、データアセットに紐づく法律上の契約である。データ契約は、必要な条件が満たされた場合にデータ取引が自動的に実行されるという意味で、スマートコントラクトであることに留意されたい。
データアセットの自己記述の公開	データアセットはデータプロバイダに存在するが、データプロバイダはデータアセットの自己記述をフェデレーションカタログに公開する必要がある。
データコンシューマによるデータアセット	データコンシューマは、フェデレーションカタログの API にアクセスして、利用可能なデータアセットの自己記述を検索することができる。フェデレーションカタログでは、データ形式、伝送方式、キーワード、価格、交渉可能

[208] Data Contract Service, Gaia-X AISBL Technical Committee, August 12, 2021, https://gaia-x.gitlab.io/technical-committee/federation-services/federation-service-specifications/L08_SDE_DCS/sde_dcs/, （2022 年 3 月 24 日アクセス）

項目	説明
の検索と選択	性、伝送詳細等、データアセット自己記述に関連するパラメータで検索、フィルタリングできる必要がある。データコンシューマが、フェデレーションカタログ上で所望のデータアセットを見つけた場合、契約オファーがDCS に転送され、そこで契約交渉が行われる。
契約交渉と契約締結	契約交渉は、データ契約書に署名するだけで、データプロバイダに転送され、データプロバイダはデータ転送を開始することができる。しかし、多くの場合、データプロバイダが個々のデータコンシューマに応じて価格や利用条件を決めると想定される。このため、DCS では、自動あるいは手動で契約交渉を行うことができる。 一般的な交渉パターンは次のように動作する。まず、データプロバイダはデータアセットの一般的なルールを定義する。データアセットを標準的なデータ契約を使って受け取ることができる場合（自動実行）、データコンシューマは顧客固有の詳細を記入し、データ契約に署名することで、記述されたとおりにアセットを注文することができる。データプロバイダは、そのようなデータ契約が有効になる前に、その確認を義務付けることができる。DCS が条件付きポリシーにおいて自動実行できない契約内容を発見した場合、データコンシューマは当該データ契約への提案として、テンプレートに自分側からのオファーを記入し、署名することができる。この提案はデータプロバイダに転送され、データプロバイダが提案に同意した場合、データ契約に署名する。 最終的に合意に至れば、データ転送を開始することができる。なお、データ転送の遅延や時間指定は、データアセット自己記述の将来のバージョンで実装される可能性がある。
データの送受信とロギング	データアセットがプロバイダからコンシューマに送られるため、「交換」ではなく「伝送」という位置付けである。ただし、固定価格やサブスクリプション費用等の形で、あらかじめ定義された、あるいは交渉による対価が発生する可能性がある。そこで、DCS の付属サービスである Data Exchange Logging Service（DELS）により、ロギングを実現する。DCS はロギングに必要なログ認証トークンを発行・更新する。また、DCS は以下のデータ転送モードをサポートしている。 • Pull：データプロバイダが定義したエンドポイントから直接ダウンロードする。 ストリーム：データプロバイダが定義したエンドポイントから連続的にダウンロードする。 • プッシュ：データプロバイダは、データアセットをデータコンシューマが定義するエンドポイントに送信する。 • パブリッシュ/サブスクライブ：データプロバイダは、データコンシューマによって定義されているエンドポイントにデータアセットの新しいバージョンを提出する。これは、頻繁に更新されるデータアセット（例えば、天気予報、株式市場の警告）のためのプッシュ送信の特殊なケースである。
課金	データエコシステムが完全に機能するには、データアセットが売買されるマーケットプレイスが必要であり、Gaia-X には最初の段階で「Billing-as-a-Service」は含まれていない。しかし、データアセット自己記述には価格設定の詳細が含まれており、支払いプロセス自体はデータプロバイダによって実現されなければならない。将来のバージョンでは、Gaia-X の課金サービスは、適切な DELS インスタンス上のデータ転送ログを検索し、送金を開始することができるようになる。

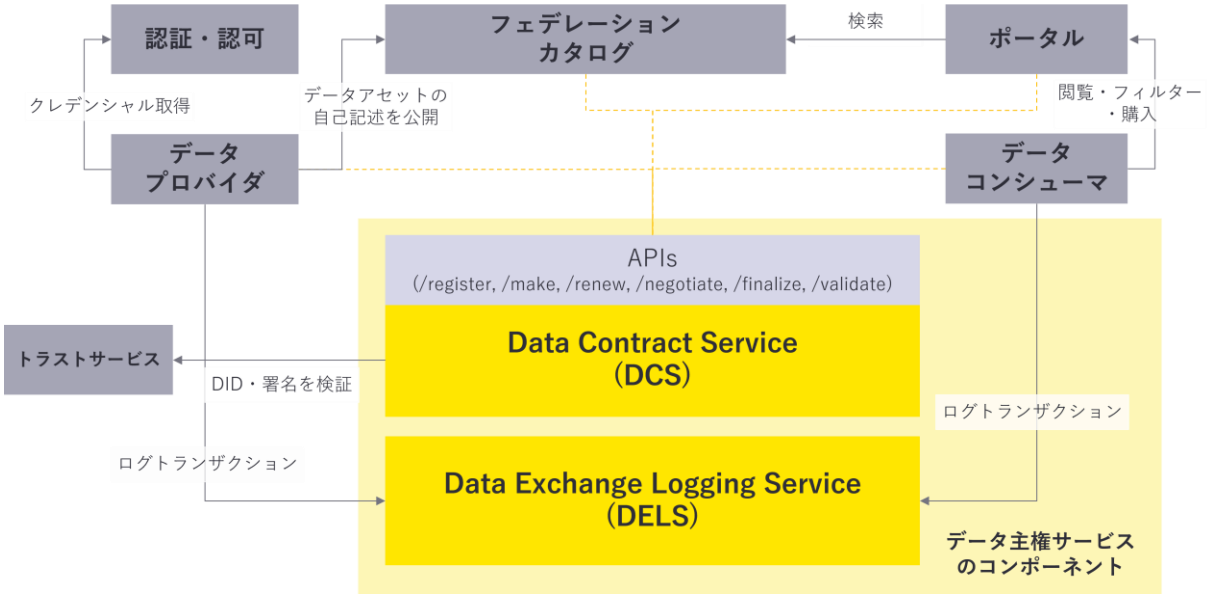
DCS はステートレスマイクロサービスである。図表 6-28 にデータ主権サービスのコ

ンポーネントとそれ以外の主要なコンポーネントとの関係を示す。また、主要コンポーネントについて簡単に説明する。

図表 6-27 データ主権サービスと関わる主要コンポーネント

項目	説明
フェデレーションカタログ	データプロバイダがデータアセットの自己記述を公開するデータカタログである。詳細の説明は割愛するが、一般的にデータプロバイダがデータアセットの自己記述を閲覧できるエンドポイントを提供する。
Gaia-X ポータル	様々な種類のアセットを閲覧、検索、比較するためのフロントエンドである。バックエンドではフェデレーションカタログから情報を取得しており、ポータルの大部分はフェデレーションカタログの GUI となっている。
トラストサービス	署名の検証を行う上で、最も重要なのが「トラストサービス」である。このため、DID を解決し、参加者の公開鍵を取得する機能を提供する。トラストサービスは、Gaia-X のアイデンティティ及びアクセス管理フレームワークの一部に過ぎないが、DCS では必要なコンポーネントである。
Data Exchange Logging Service	DELS は DCS を補完するもので、後者は主に処理、前者は主にストレージとして機能する。将来の Gaia-X では、データ取引ログは課金、監視、監査に重要な役割を果たす。DELS は、ログの取得を要求する全ての参加者に対して有効な認可トークンを求める。本認可トークンは DCS から発行される。

図表 6-28 フェデレーションサービスと DCS、DELS の概観



図表 6-28 には、データプロバイダとデータコンシューマの間に、実際のデータ転送に関するやりとりは記されていない。v1 ではデータ転送に関する仕様の定義はスコープ外であり、データプロバイダは安全なデータ転送のためにエンドポイントを利用できる

ようにするという単純な理由によるものである。もちろん、今後のアップデート版では、Specification で説明した基盤の上に、安全なデータ転送経路を構築することができる。

図表 6-28 に示すように、DCS には主な 6 つのエンドポイントが含まれる。

- データ資産登録（/register）
- 契約を結ぶ（/make/contract）
- 契約交渉（/negotiate）
- 契約の確定（/finalize）
- 契約の有効化（/validate）
- ログトークンの取得 （/log/token）

(2) Data Exchange Logging Service

DELS[209]は、データが（１）送信、（２）受信されたこと、（３）ルールやユーセージポリシーが遵守された、あるいは違反されたことを証明するものである。DELS は運用上の問題の解決や、最終的には不正取引の解決をサポートする。データプロバイダは、そのデータがどのように提供されたかを追跡することができ、コンシューマに通知することができる。データコプロバイダは、データを正常に受信できたこと、受信できなかったことを追跡することができる。さらに、データコンシューマは、ユーセージポリシーの遵守や違反について追跡し、エビデンスログをプロバイダに提供することができる。ログはデータ利用に係る清算や請求の根拠として利用できるが、データ主権サービスにおける主な目的ではない。

機能的な観点からは、DELS は、ロギング通知を追跡し、ロギングメッセージを読み込むためのインターフェースを提供する。ロギングの仕組みは，W3C のリンクデータ通知に準拠する。

従って、通知には、日付、時間、送信者、データプロバイダ、データコンシューマ、データ交換契約等の最小限の要件が含まれる。データ交換に関わる当事者は、通常、通知の送信者とコンシューマである。

GX-DELS はステートレスマイクロサービスである。DELS は単独で存在することはできない。図表 6-28 に示すように、有効なデータ交換契約が必要である。

DELS の主な機能は以下の 2 である。

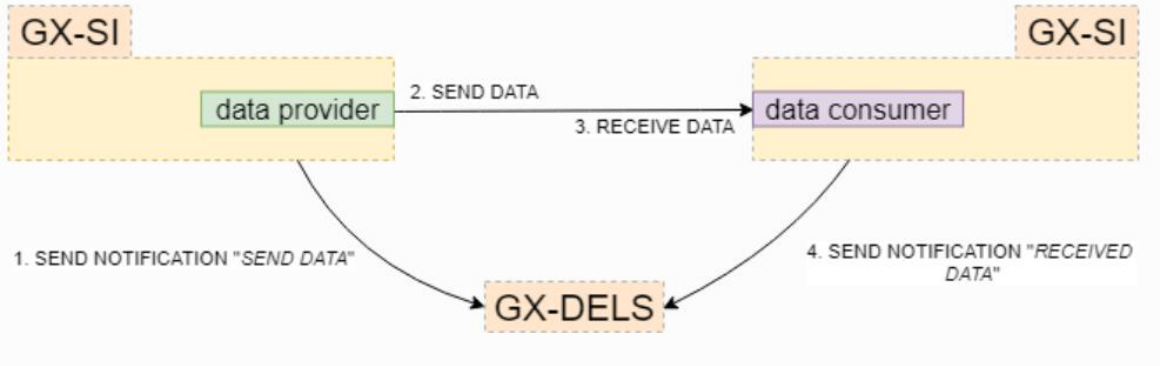
- DELS Inbox へのログ通知。データプロバイダとデータコンシューマは、契約の存在を確認するためのログトークンを含むイベント通知を DELS Inbox に送信することができる。
- DELS Inbox からログ通知を取得する。データプロバイダとデータコンシューマは、DELS の受信トレイからログ通知を取得することができる。第三者が DELS から情報を取得することも可能である。

この機能は、強制ログ取得のサポートによって拡張されている。ここでは、認証トークンは強制的な確認ロギングが有効かどうかの情報を含んでいる。

---

[209] Data Exchange Logging Service, Gaia-X AISBL Technical Committee, August 12, 2021, https://gaia-x.gitlab.io/technical-committee/federation-services/federation-service-specifications/L09_SDE_DELS/sde_dels/, （2022 年 3 月 24 日アクセス）

図表 6-29　DELS の概観



- これにより、データプロバイダはデータを暗号化して送信し、ロギング確認を受信した後に復号化キーを提供することが可能になる。
- 注：信頼できる第三者からの復号鍵の送信を DELS が代行することは、特許上の制約から実現できない。

ア　データプロバイダが「SEND DATA」通知を送信

サービスインスタンスを与えられたデータプロバイダは、データコンシューマにデータを送信する準備を整え、最初の通知を DELS に送信する。ペイロードには、一意の識別子と、受信側のデータコンシューマの所定の識別子が付与されている。これにより、DELS にログエントリーが作成される。DELS は、対応する通知識別子で応答する。

イ　データプロバイダがデータを送信

データプロバイダは、与えられたデータコンシューマが期待する主要な情報であるデータを送信する。このペイロードは、いくつかのメタデータでラップされているが、GX-DELS の「SEND NOTIFICATION "SEND DATA"」に対する応答で公開される通知識別子にもラップされている。

ウ　データコンシューマがデータを受信

データプロバイダから送信されたデータをデータコンシューマが受信する。

エ　データコンシューマが「RECEIVED DATA」通知を送信

データコンシューマは、データプロバイダから提供された通知識別子を含む通知を DELS に送信する。これにより、DELS にログエントリーが生成される。

- DELS は、与えられた通知識別子に関連するデータコンシューマが正しいかどうか確認する

- DELS が終了し、DELS が応答する

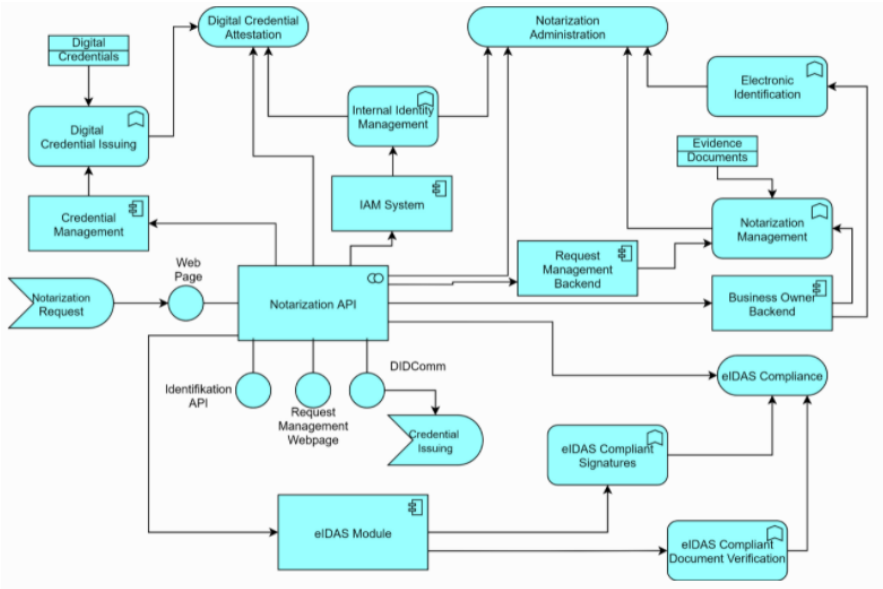
6.2.4 コンプライアンス

(1) Notarization API

NOTAR[210]を開発する背景は、Gaia-X 参加者が所有する紙媒体あるいはデジタル媒体で公開されるデータに関する信頼を確立するための要件に基づく。この目標を達成するには、デジタル証明書を VC で出力するコンポーネントが必要である。これにより、認証機関（政府、弁護士等）は、Gaia-X への参加を希望する組織の身元を証明し、必要な電子証明書を提供できるようになる。本プロセスは、物理的及び非構造化電子文書を W3C が定義する VC 形式に変換して、組織のオンボーディング、認定及び信頼性をサポートするために用いられる。各 VC は、自己記述から参照される。

NOTAR は、eSSIF[211]が提示する公証のコンセプトを取り入れている。NOTAR は W3C の定義に準拠する VC を発行するために AISBL 又は認証された組織によって使用される。このサービスは、紙ベースの「古い」世界での信頼とデジタルの「新しい」世界での信頼のギャップを埋めることを可能にするコンポーネントである。

図表 6-30　Notarization API のアーキテクチャ概観



本コンポーネントは、マイクロサービスアーキテクチャの設計原則に従う。機能は REST API として公開され、HTTPS でアクセスできる。コンポーネントは複数の場所にインストールする必要がある。マルチユーザアクセス機能を備えた発行者の組織内にイ

[210] Notarization API, Gaia-X AISBL Technical Committee, August 12, 2021, https://gaia-x.gitlab.io/technical-committee/federation-services/federation-service-specifications/L12_CP_NOTAR/cp_notar/, （2022 年 3 月 24 日アクセス）

[211] High-level scope (ESSIF), EBSI Documentation, https://ec.europa.eu/digital-building-blocks/wikis/pages/viewpage.action?pageId=379913698（2022 年 3 月 28 日アクセス）

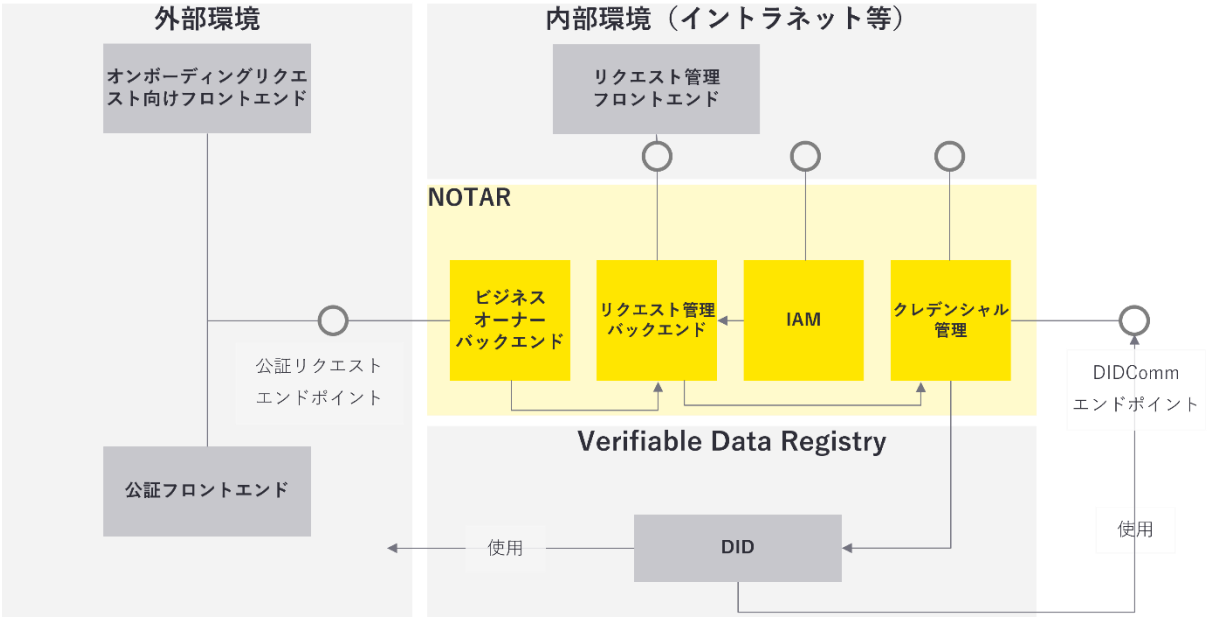
ンストールできる必要がある。複数のユーザに使用されることを考慮し、本コンポーネントへのアクセスは保護されなければならない。これには、ロールの概念、データストレージ保護、アクセスコントロールが含まれる。NOTAR の全体的な機能は GDPR に準拠し、監査可能である必要がある。

NOTAR の主な機能は、公証要求を受信し、法的に保証されたデジタル Credential を発行するために必要な外部インターフェースを提供することである。これを実現するには、VC の署名は、eIDAS に準拠する必要がある。

NOTAR のコア機能は下記の通りである。

- 公証要求に応答する外部 API
- Gaia-X へのオンボーディング及び認定ワークフローをサポートするために、新しい参加者組織へのデジタル Credential 発行
- 認定リクエストの管理と処理
- 任意の証明書のデジタル Credential の生成（例：ISO27001、IOS9001 等）
- 発行されたデジタル Credential の取り消し
- 事業主を確認するための電子 ID（eId、Video-Ident 等）
- Gaia-X スキーマ定義を含む Credential の定義

図表 6-31 Notarization API のモジュール概観



(2) Continuous Automated Monitoring

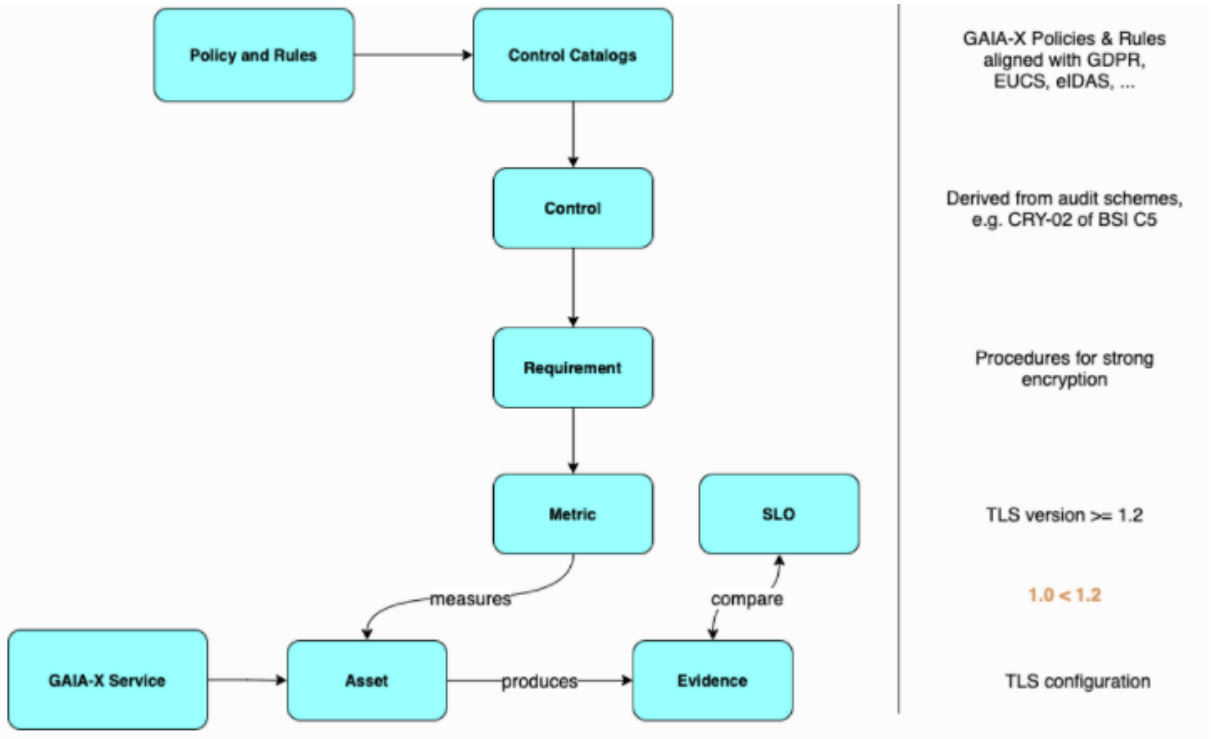
CAM[212]は、フェデレーションサービス内のコアサービスである。主な目的は、フェデ

[212] Continuous Automated Monitoring, Gaia-X AISBL Technical Committee, August 12, 2021, https://gaia-x.gitlab.io/technical-committee/federation-services/federation-service-specifications/L10_CP_CAM/cp_cam/, （2022 年 3 月 24 日アクセス）

レーションカタログで提供される個々のサービスのコンプライアンスについて Gaia-X のユーザに透明性を提供することである。コンプライアンスのベースとなる考えは、Gaia-X がシステムに対して求める特定の要件とルールである。例えば、暗号化、データのプライバシー、相互運用性等のセキュリティの観点での要件が挙げられる。多くの場合、BSI C5（ドイツ連邦情報セキュリティ庁 Cloud Computing Compliance Criteria Catalogue）や EUCS（European Cybersecurity Certification Scheme for Cloud Services）等の既存の認定基準が使用される。

CAM は、Gaia-X 上の特定のサービスがコンプライアンスに準拠するか否かを示すエビデンスを自動的に収集することを可能にする。本機能は、Gaia-X エコシステム上で提供されるサービスが、EU Cybersecurity Certification の「High」の基準に相当するような機密データを処理している場合に、特に必要とされる。

図表 6-32　CAM に関連する用語の関係



図表 6-32 は、この CAM に関連する用語の関係を表している。コンプライアンスにおいて最も基本的な部分は、Policy and Rules（以下、ポリシーとルール）である。これは、EUCS 等の Control Catalogs に基づく個々のコントロールを参照している。Control Catalogue（以下、コントロールカタログ）とは、クラウドコンピューティングに関するセキュリティ要件を提供するカタログである[213]。各 Control（以下、コントロール）には通常、コントロールの詳細を示す一連の Requirement（以下、要件）があり、通常はさまざまなアシュアランスレベルを参照する。要件のレベルまでは、OSCAL（Open

[213] Criteria Catalogue C5, Federal Office for Information Security, https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Criteria_Catalogue/Compliance_Criteria_Catalogue_node.html（2022 年 3 月 24 日アクセス）

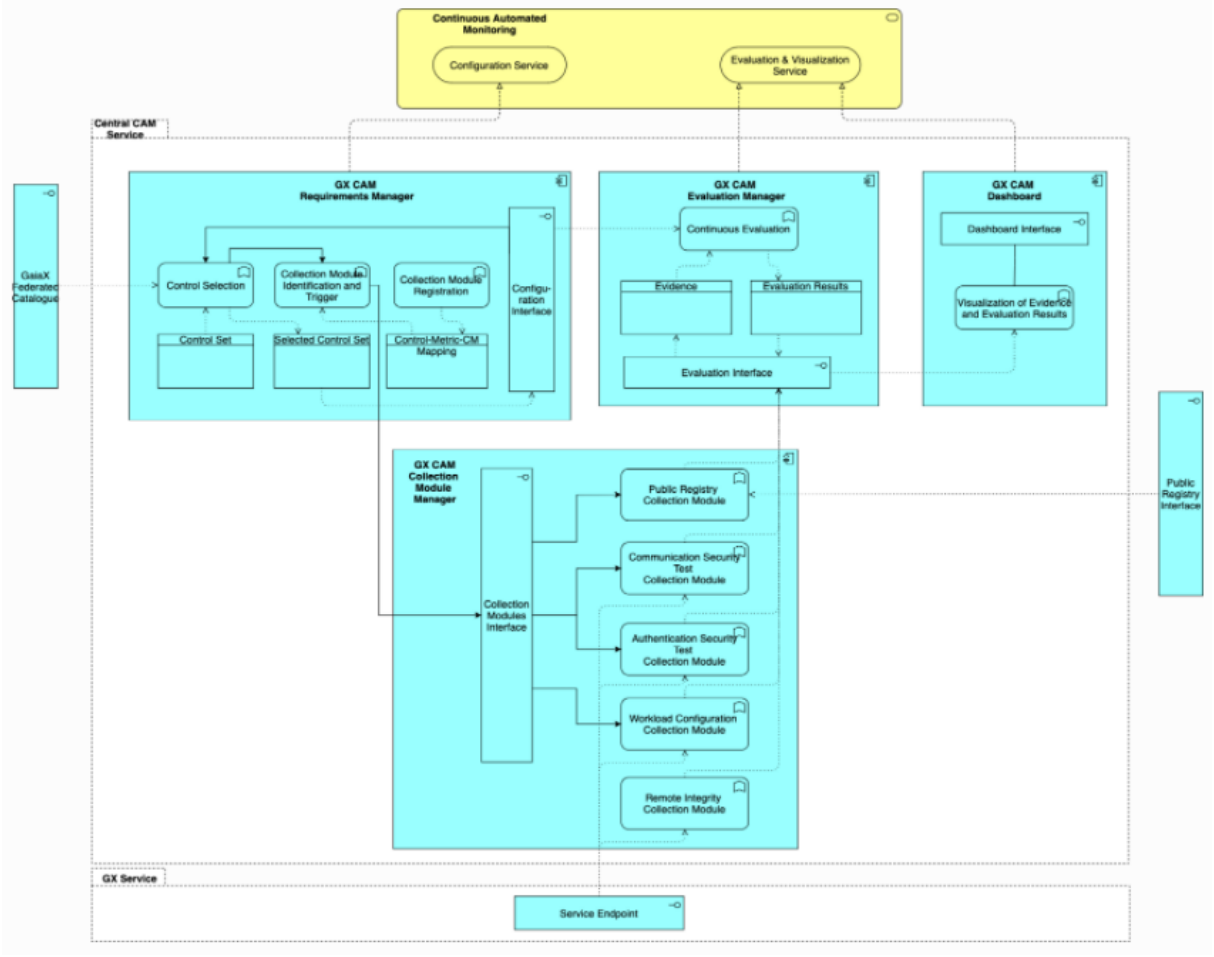
Security Controls Assessment Language）[214]等の言語でのモデリングが推奨されているが、コントロールのテキストによる説明が使用されることが多い。ただし、セキュリティ制御の自動監視には、マシンリーダブルな表現が必要である。そのため、Metric（以下、メトリック）は各要件に関連付けられている。技術的に言えば、メトリックは測定に用いられる定義である。

メトリックは特定の Asset（以下、アセット）のプロパティに適用され、対象のサービスがメトリックの基準を満たしているか否かを示す Evidence（以下、エビデンス）が記録される。例えば、TLS 暗号化に関する要件が満たされているかどうかを確認するために、CAM は TLS プロトコルを使用して対象サービスと対話し、使用されている TLS バージョンと使用されている Cipher スイートに関する Evidence を収集する。次に、収集されたエビデンスは、コントロールカタログ上で参照されている一般的なベストプラクティスと比較される。この例では、少なくとも TLS バージョン 1.2 を使用する必要があると述べられている。

CAM の主な機能は、特定の対象システムが Gaia-X のコンプライアンスに準拠しているかどうかを評価することである。これは、対象システムに対して技術的なチェックを行うか、API を用いて情報を取得し、その状態を監視することによって行われる。

[214] Open Security Controls Assessment Language, National Institute of Standards and Technology, https://csrc.nist.gov/Projects/open-security-controls-assessment-language（2022 年 3 月 24 日アクセス）

図表 6-33 CAM のモジュール概観



図表 6-33 は、CAM とそのモジュールの想定される全体的なアーキテクチャの概要を示している。以下では、各主要コンポーネントについて簡単に説明する。

ア CAM Requirements Manager （GX-CAM-RM）

本モジュールの主な目的は、要件を管理し、それに応じて継続的な監視プロセスを開始することである。GX-CAM-RM は、監視に適した一連のコントロールと、特定のメトリックの測定を実装する Collection Module へのマッピングを保持する必要がある。GX-CAM-RM は、Collection Module を登録及び登録解除する機能も提供する。

イ CAM Collection Module Manager （GX-CAM-CMM）

このコンポーネントは、様々な Collection Module の集合体である。各 Collection Module は、特定のメトリックに従ってエビデンスを収集する。

現時点での仕様では、図表 6-34 で示されている 5 つの Collection Module が定義されている。

図表 6-34 各 Collection Module の概要

モジュール	説明
Public Registry Collection Module	フェデレーションカタログ等のパブリックレジストリからセキュリティ及び認証関連情報を収集する。
Communication Security Collection Module	TLS 接続の品質測定等を通じて通信セキュリティに関する情報を収集する。
Authentication Security Collection Module	テストベース又は監視ベースで、クラウドサービスで採用されている認証技術の品質に関する情報を収集する。例えば、相互運用性の観点で OAuth/OpenID 等のプロトコルが正しく実装されているかという情報を収集する。
Remote Integrity Collection Module	Gaia-X のサービスインスタンスを実行しているソフトウェアスタックに関する情報を収集する。ソフトウェアスタックは、デプロイされたコンポーネントのリストを表す。このリストを利用して、サービスインスタンスの信頼性及び脆弱性をチェックする。
Workload Configuration Collection Module	Gaia-X サービスの特定のインスタンス化に関するセキュリティ及びプライバシー関連の構成情報を収集する。上記の 4 つのモジュールは、サービス全体に適用される情報を収集するが、本モジュールは、Gaia-X エコシステムの特定のユーザに対するサービスのインスタンス化について評価する。テストベースで OpenStack や Kubernetes API 等のクラウドプロバイダが提供する標準 API を用いて情報を収集する。

全ての Collection Module は技術的なエビデンスを生成し、Evaluation Manager のインターフェースに転送される。

ウ CAM Evaluation Manager （GX-CAM-EM）

GX-CAM-CMM によってエビデンスを収集した後、それが要件をどの程度満たしているか評価する必要がある。例えば、エビデンスの評価の結果、TLS バージョン 1.0 が使用されているケースを考える。コントロール又は要件では、TLS バージョン 1.2 以上のみを使用する必要があると規定されているため、要件を満たしていないと評価され、評価結果が生成される。次に、ダッシュボード等を通じて、他のステークホルダ及び承認された関係者によって、本評価結果を照会することができる。

エ GX CAM Dashboard

本モジュールは、Web アプリケーションを使用して評価結果を可視化するために使用される。GX CAM ダッシュボードは GX-CAM-EM から評価結果を取得して可視化し、承認された関係者が照会できるようにする。

上記で説明したモジュールは分散可能であり、他のモジュールとは独立して機能する必要があるためパーシステンスについて特に定義されていない。従って、必要なパーシステンスを用意することは、コンポーネントごとに行う必要がある。Collection Module 等の特定のモジュールは、情報をまったく保持しないこともある。

(3) Onboarding & Accreditation Workflows

OAW の主な目的は、Gaia-X フェデレーションカタログで提供される個々のソフトウェア・アセットとノードのコンプライアンスについて、コンシューマに透明性を提供することである。OAW は、プロバイダとアセットのオンボーディングと認定を可能にする様々な機能を提供する。

OAW エンジンは、特に、AISBL 又は AISBL によって認可された CAB によって、ソフトウェア・アセットとノードの適合性を証明する認定を行うために使用される。

OAW エンジンは、オンボーディングと認定ワークフロー、とそれらの管理プロセスに関する 6 つの主要な機能を提供する。OAW の構成要素について、以下で簡単に説明する。

ア プロバイダのオンボーディング

Gaia-X でアセットを提供する前に、プロバイダは Gaia-X にオンボーディングする必要がある。これは、プロバイダのオンボーディングワークフローを通じて行われる。オンボーディングの間、プロバイダは関連するオンボーディングに必要な自己記述等のデータを作成し、利用規約と認定契約に署名する必要がある。その後、プロバイダはオンボーディングリクエストをオンボーディング機関に提出することができ、オンボーディング機関は認定ワークフローを開始する。

イ プロバイダの認定ワークフロー

プロバイダ認定ワークフローの中で、Gaia-X オンボーディング機関は、CAB のサポートにより、プロバイダのオンボーディング情報の完全性、整合性、公正性を検証する。オンボーディング機関がオンボーディングを承認した場合、公証サービス（NOTAR）を使用して、VC が作成される。

ウ ソフトウェア・アセットとノードのオンボーディング

プロバイダのオンボーディングと同様に、各新規ソフトウェア・アセットやノードは、Gaia-X エコシステムに掲載される前にオンボーディングプロセスを受けなければならない。その目的は、各アセットが Gaia-X の原則と MVSC（Minimal Viable Set of Controls）を満たしていることを保証するオンボーディングフローを設計することである。MVSC とは、ポリシー・ルール委員会及び Gaia-X AISBL が、ソフトウェア・アセットやノードが Gaia-X のコンプライアンスに準拠するために満たすべき最低限の基準を指す。プロバイダはアセットの自己記述を提出し、決定されたアシュアランスレベルに該当する MVSC を満たすことが証明されたことを裏付けるために「Declaration of Adherence」に署名する。また、プロバイダによって提出された保証情報（ISO/IEC 27001 等ソフトウェア・アセットの既存の認証等）は、オンボーディング機関が行う認定ワークフローで評価される。

エ ソフトウェア・アセットとノードの公認

Gaia-X は、ソフトウェア・アセット及びノードに対して Basic、Substantial、High の 3 つの異なるアシュアランスレベルを定義している。例えば、各ソフトウェア・アセットやノードがあるアシュアランスレベルを満たす場合、それによって「個人データを処理するために GDPR への準拠が必要である」というような特定の基準を満たすことが保証される。要求されるアシュアランスレベルに応じて、認定ワークフローはソフトウェア・アセット又はノードが Gaia-X MVSC に準拠しているかどうかを検証する。Basic アシュアランスレベルでは、認定は大幅に簡素化され、オンボーディング機関からの明確な要求があれば、プロバイダが提供する自己評価証拠のみで判断される。Substantial アシュアランスレベルは、Basic アシュアランスレベルの検証プロセスをベースとしているが、検証範囲及び検証内容が異なる。特に、セルフアセスメントは Substantial アシュアランスレベルには十分ではないため、Gaia-X は、Substantial アシュアランスレベルの MVSC を満たす適切な既存の規格、認証、証明書、行動規範、監査結果等の基準を定めている。High アシュアランスレベルの検証プロセスは、Substantial アシュアランスレベルの検証プロセスをベースとするが、検証範囲及び検証内容が異なる。Substantial レベルの管理に加えて、例えばサイバーセキュリティの場合、ソフトウェア・アセット及びノードが満たすべき追加的な管理が存在することになる。さらに、さらなる検証プロセス及び測定が適用される。特に、コンプライアンスに準拠していることをモニタリングするために、CAM が適用されることがある。

オ 管理ワークフロー

OAW エンジンは、上記で説明したオンボーディングと認定のワークフローに加えて、ソフトウェア・アセットとノードの MVSC への継続的な準拠を保証するための監視と再評価のワークフロー、Gaia-X 準拠証明の取り消しや制限を実行するワークフロー等の管理ワークフローについてもサポートする。

カ オフボーディング

プロバイダ、ソフトウェア・アセット、ノードが、プロバイダの要求やアセットの MVSC 違反により Gaia-X エコシステムから撤退する場合、OAW エンジンはオフボーディングワークフローを提供する。

6.2.5 ポータルと API

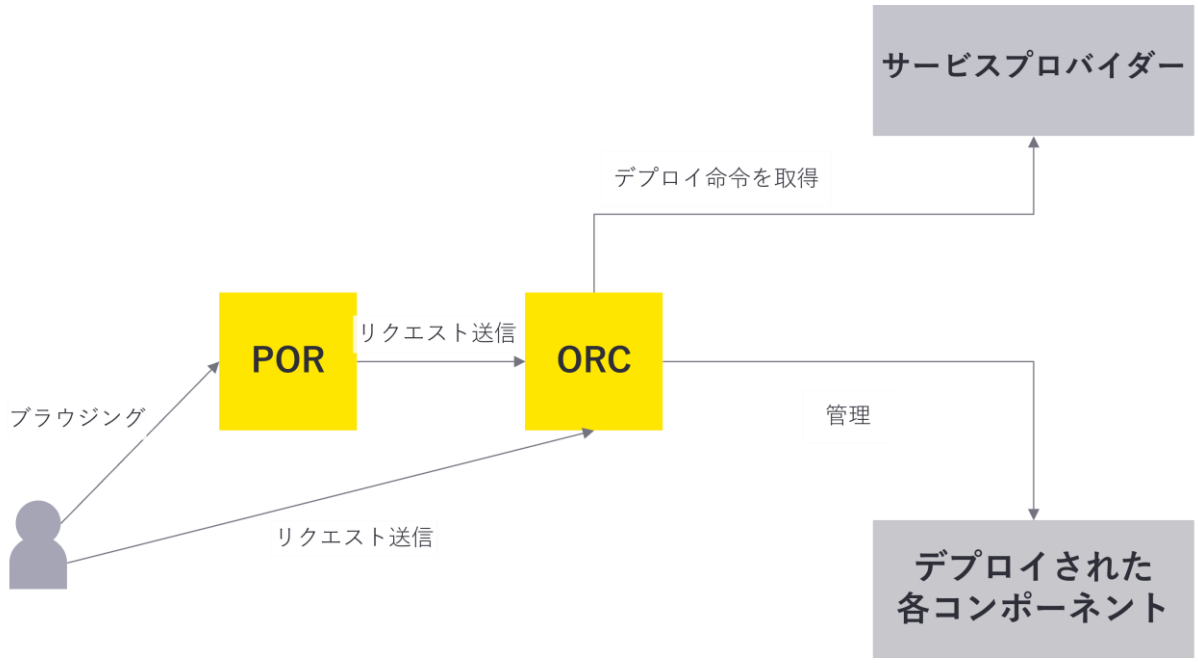
(1) Orchestration

ORC[215]は、サービスのインスタンス化と管理を行う。参加者がサービスを選択した後又は POR で新規のサービスを作成して使用したい場合に、一連のプロセスを実行する。

[215] Orchestration, Gaia-X AISBL Technical Committee, August 12, 2021, https://gaia-x.gitlab.io/technical-committee/federation-services/federation-service-specifications/L14_IP_ORC/ip_orc/, （2022 年 3 月 24 日アクセス）

ORC は、サービスインスタンスをデプロイ、更新及び削除できる。これらのプロセスは、ポータルを介したコンシューマ（ポータルでのサービスを選択する等）又はプロバイダ（セキュリティ/互換性の理由で、サービスの最新バージョンへの更新をトリガーする等）によって実行される。ORC は、Gaia-X のコンシューマ及びプロバイダに、サービスインスタンスのデプロイ成否に関するステータス等のフィードバック情報も提供する。

図表 6-35 ORC のコンポーネント概観

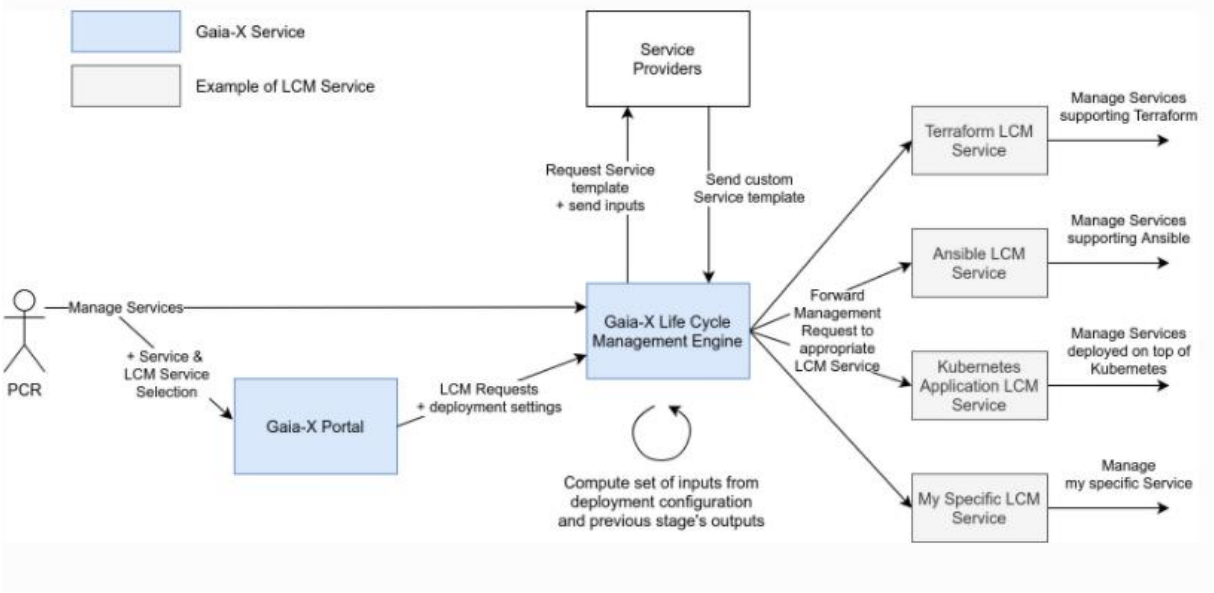


ORC へのコントロールに関しては、ポータル経由の操作又は参加者から API 等を通じて直接アクセスできるような仕組みとなっている。

プロバイダは、自身が提供するサービスの管理方法について説明しなければならない。サービスをデプロイ及び管理するためのツールとして Terraform、Ansible、Kubernetes 等様々なものが存在するため、ORC はデプロイと管理に係るコンポーネント実装はスコープ外とする。代わりに、ORC は「ライフサイクルマネジメント（LCM）サービス」の実装において準拠する必要がある API 標準を提供する。

LCM とは、例えば、あるコンピュートリソースの生成、アップデート、削除といった一連の流れに相当する。 LCM サービスは、前述の Terraform、Ansible 等のツールをサポートしてサービスインスタンスをデプロイ及び管理するために使用されるコンポーネントである。LCM サービスは、プロバイダによって提供される標準の Gaia-X サービスである。ORC は、さまざまな LCM サービスのオーケストレーション及び ORC が提供する API 標準を使用した LCM サービス間の通信機能を担う「LCM エンジン」を提供する。

図表 6-36 ORC のモジュール概観



ORC の概観セクションで説明したように、コンシューマは自分たちのサービスを管理できる。コンシューマは、LCM エンジンと通信することによってサービスを直接管理するか、LCM エンジンとの通信をサポートする Gaia-X ポータルを介して管理することもできる。

LCM エンジンはプロバイダからデプロイ用のコマンドを取得し、コンシューマ及びプロバイダによって提供されるパラメータからサービスデプロイのコンフィグレーションを準備することができる。そして、LCM エンジンはそのようなデプロイ用のコマンドを、対象の LCM サービスに転送する機能を有している。

(2) Portal

フェデレーションサービスでは、リファレンス実装として Minimal Viable Gaia-X（MVG）を設計、実装、デプロイすることが求められている。MVG が提供するコア機能は、Web ベースのユーザインターフェースを持つ POR として提供される。ビジター、参加者、フェデレータ等の役割に応じて、それぞれウェブページが提供される。

ポータル[216]の主な機能は、フェデレーションカタログ上でのコンテンツの検索、表示である。また、新しい参加者の登録やオンボードも可能である。参加者向けのページでは参加者の詳細を編集することや、フェデレータ向けページでは新しい Gaia-X 参加者のオンボーディング情報にアクセスすることができる。Gaia-X の参加者は、ポータルを介してサービスインスタンスのデプロイ等、オーケストレーションツールを利用することもできる。この場合、プロバイダはフェデレーションカタログからアクセス可能なサービスの自己記述の一部として、サービスのインスタンス化に必要なコマンド等を提

[216] Portal, Gaia-X AISBL Technical Committee, August 12, 2021, https://gaia-x.gitlab.io/technical-committee/federation-services/federation-service-specifications/L13_IP_POR/ip_por/, （2022 年 3 月 24 日アクセス）

供する必要がある。

図表 6-37 Gaia-X の役割に応じたポータルの要件

役割	要件
ビジター	• 対象のサービスオファリングが認証されていることを示すアイコンを表示すること。 • フォントサイズは 14 ピクセル以上であること。 • フォントと背景色のコントラストが高いこと。 • 情報の詳細の表示フォーマットが、サービス、データセット、参加者等で一貫していること。 • フォームが構造化されていること。 • テキストフィールドは常にプレースホルダーテキストを含むこと。 • テキストフィールドは、マウスによるポインタがホバーする際に表示されるラベルを持つこと。 • アイコン及びアイコンボタンには、説明文を付与すること。
コンシューマ	• サービスやデータセットのデプロイは、プロバイダによる自動的なものと、コンシューマによる手動的なものの 2 つの方法で行うこと。 • プロバイダによるサービスやデータセットの変更が許可されている場合は、その旨が表示されること。 • サービスオファリングに関する情報は一般的なものでないこと。
プロバイダ	• ユーザの行動に対して非同期的及び同期的なフィードバックを提示すること。 • 電子メール通知を送信することによって、非同期的なフィードバックを提示すること。 • ダイアログと入力補助テキストを使用することによって、同期的なフィードバックを提示すること。
全ロール共通	• ポータルのアクセシビリティを保証するため、WCAG2.1 規格[217]に準拠したインターフェースの開発を行うこと。 • ポータルは様々な言語でアクセスでき、UTF-16 をサポートすること。

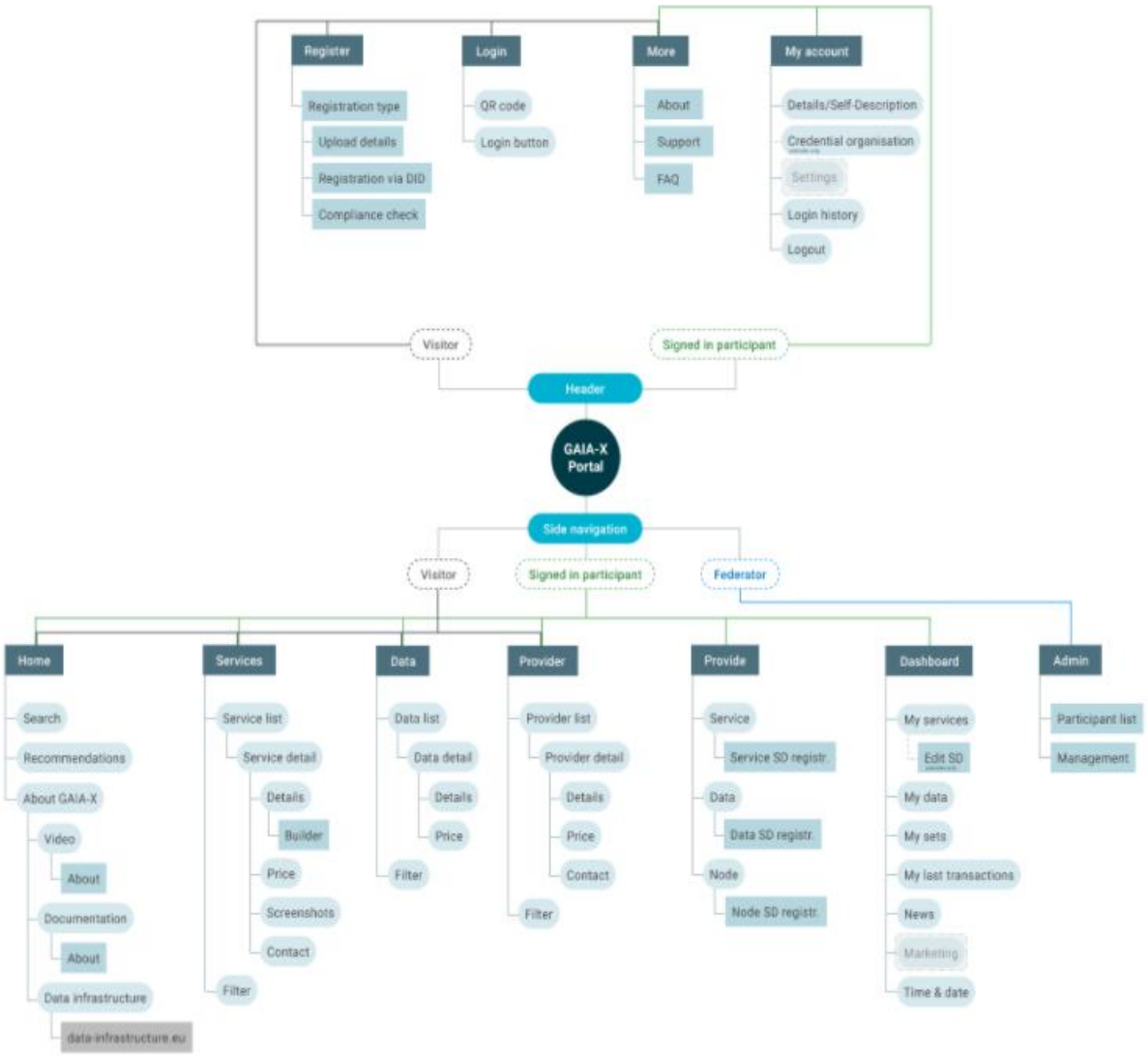
Gaia-X のポータルは下記のコア機能を含む。

- 登録プロセス
- ログインプロセス
- ユーザーアカウント情報
- 自己記述の登録、検索
- サービスのパッケージング
- ダッシュボード

Gaia-X のポータルは上記のようなコア機能を実現するため、図表 6-38 のサイトストラクチャに示されているページ、サブページ及びセクションで構成される。

[217] Web Content Accessibility Guidelines (WCAG) 2.1, , June 2018, W3C Recommendation, https://www.w3.org/TR/WCAG21/（2022 年 3 月 26 日アクセス）

図表 6-38　Gaia-X ポータルのサイトストラクチャ



第7章 IDS や Gaia-X と日本との相互認証等に向けて

7.1 環境整備に関する課題

IDS や Gaia-X に準拠するデータスペース上でのデータ連携を実現するためには、一定の認証ルールやプロセスに従うことが必要である。例えば、日本企業が欧州企業や自社の現地法人とのデータ連携をしようとする場合、その都度要求されるコネクタ等を用意し、CA、DAPS 等による認証を要求されるものと想定される。

現在、欧州議会ではデータガバナンス法案やデータ法案が審議されている。非個人データの取扱いについて、両法案は域外移転に際し十分性認定を必要としているところであり、今後の動向によっては、欧州のデータスペース上のデータを日本に配置又は移転できなくなるのではないかといった懸念が生じる。そもそも日本企業の機密データを全て欧州と共有してよいのか、といった点にも留意が必要である。

データスペースとしては、IDS に準拠する Catena-X が早ければ今夏にも立ち上がってくると予想されるところ、日本企業の活動に著しい支障がでないようにするためには、こうした欧州側の動きをにらみながら、国際的な相互認証に向けた取組を進めていくことが重要と考えられる。

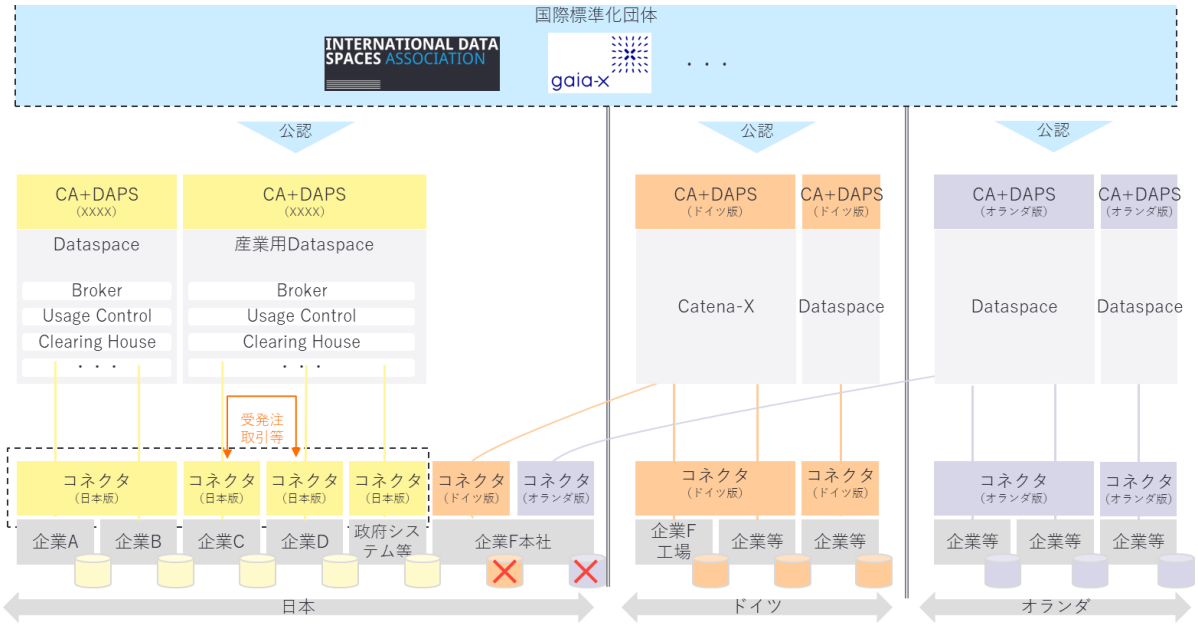
こうした環境の変化に対応するためには、日本における新たなデータ連携の枠組みの整備や、データ連携を実現するためのコンポーネントの技術仕様、OSS の管理、国際的な相互認証の枠組み等の整備に今後対応していくことが必要と考えられる。

日本における新たなデータ連携の枠組みの整備としては、欧州側と同様に日本側にも CA、DAPS 等による認証を行う機関（認証機関）や、当該機関により正しく認証が行われることを担保する機関（認定機関）が必要と想定される。

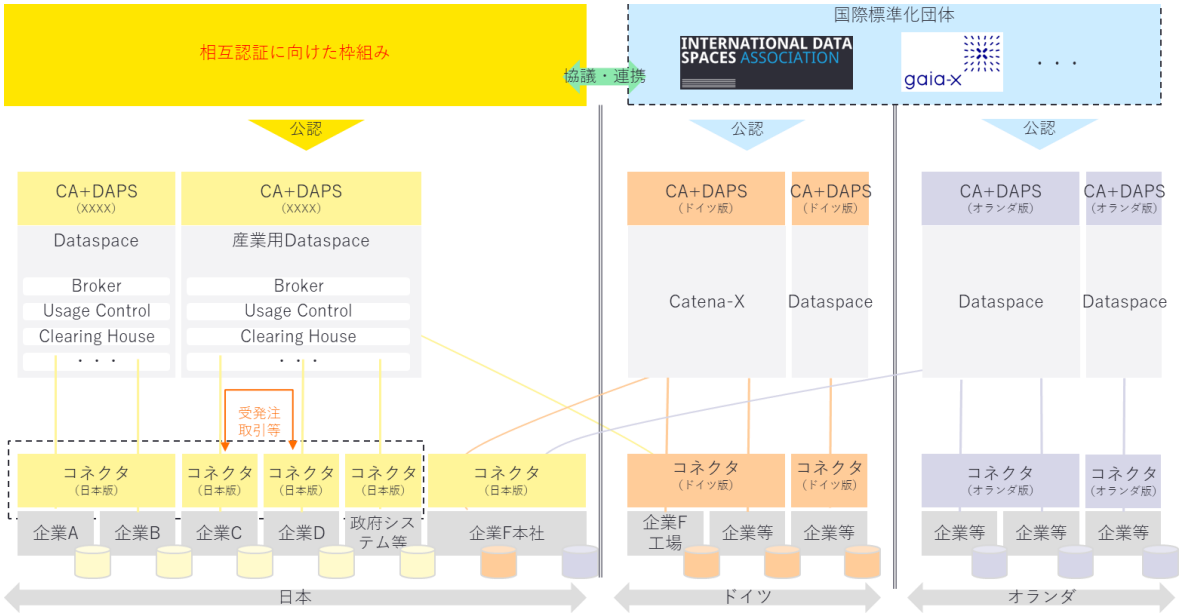
これらの認証・認定機関に対する政府機関の関与についても整理が必要であり、また、DATA-EX の取組を進める一般社団法人データ社会推進協議会（DSA）や、データ連携に係るアーキテクチャを検討する独立行政法人情報処理推進機構のデジタルアーキテクチャ・デザインセンター（IPA・DADC）とも連携することが重要になると考えられる。

また、データ連携を実現するためのコンポーネントの技術仕様や OSS の管理方針を決定し、必要に応じてこれらのコンポーネント等の改良を行っていくことも必要と考えられる。これらは、必ずしも IDS や Gaia-X と全く同じというわけではなく、管理団体やデータスペースに参画する事業者等とも連携し、必要な改良を加えていく方向になるものと考えられる。また、日本で取り組む中で生じた課題については、IDS や Gaia-X にフィードバックを行いつつ、将来的には、ドイツやオランダをはじめ、国際的な相互認証を行う枠組みを整備していくことが求められるだろう。

図表 7-1 欧州側でのみ認証が行われる場合



図表 7-2 日本側と欧州側で相互認証を行う場合



7.2 コンポーネントの構築に関する課題

「8.4 コネクタを用いたデータ連携の試行」結果を踏まえ、今後、コネクタについては以下の課題に対応していくことが必要と考えられる。

まず、コネクタの稼働環境である。試行ではアマゾンウェブサービス（AWS）を採用したが、今後広く展開していくにあたっては、複数の異なるプラットフォームに展開する方法

を策定する必要がある。そのためには、

- コネクタが多くの稼働環境に容易に展開できるためのパッケージング方法の策定、実装
- いくつかのパブリッククラウド、オンプレミス（プライベートクラウドを含む）、それらのハイブリットでの稼働検証

を行う必要があるだろう。

このほか、実際のデータスペースで想定されている異なるシステム間でのコネクタの接続方法や、データのセキュリティを保証するための共通ルールや標準の定義についても整理が必要である。

特に、データ主権の観点からは、データへのアクセスが許可された後であっても、いつまでデータにアクセスできるか等、継続的にデータへのアクセスを制限する必要があるところ、例えば、以下のようにデータの使用制御の設定に留意する必要がある。

- 必要な認定書をもたないコネクタに機密データを転送しない
- 競合企業のデータは、同じサービスによって集約、処理しない
- コネクタ間でのみ通信を可能とし、他システムへの連携はしない

なお、今回、受発注取引をユースケースとした試行を行う中で、異なる EDI 間でのデータ連携の実現を見据え、一部のデータ項目に限定したデータの翻訳（変換処理）を行った。ただし、様々な分野や業界をまたがる受発注取引の実現に向けては、ビジネスプロセスやデータ項目の共通化・標準化検討等が必要になると考えられる。

第8章 Appendix

8.1 IDS 発行文書

#	発行年月	文献名	概要	URL
I01	2018/10	SHARING DATA WHILE KEEPING DATA OWNERSHIP	戦略（IDS 全体概要）【全 6 ページ】 保有データの価値を活用できていない現状を説明し、IDSA がこれを解決するため進めている施策を紹介している。具体的には、IDSA 仕様が欧州の価値観に基づくデータマーケットプレイスの基礎を築くこと、IoT のデータ作成と機会学習や AI アルゴリズムのデータ使用の間に戦略的リンクを作り出すことを説明している。また、リファレンスアーキテクチャの定義や参入障壁の削減等にも触れている。	https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/Whitepaper-2018.pdf
I02	2018/10	JOINTLY PAVING THE WAY FOR A DATA DRIVEN DIGITISATION OF EUROPEAN INDUSTRY	技術（IDS 関連団体・技術）【全 14 ページ】 データエコノミーの課題や機会、データオーナーシップを保ちつつデータを共有する IDS アプローチ、FIWARE と IDSA の関係、IIRA、RAMI、IVI、IoT-A とのアーキテクチャ調整、EU 内の選択肢について記載している。	https://internationaldataspaces.org/wp-content/uploads/IDSA-Position-paper-Jointly-Paving-the-Way-For-Data-Driven-Digitisation-European-Industry.pdf
I03	2018/12	OPEN DATA SPACES TOWARDS THE IDS OPEN DATA ECOSYSTEM	その他（IDS ユースケース）【全 29 ページ】 IDSA のコンセプト、技術、ユースケースについて概要を示す資料。第 1 部ではオープンデータについて、現在の組織的・技術的な状況を概説し、第 2 部では IDS とオープンデータの関係性について、第 3 部は IDS オープンデータエコシステムについて記載している。	https://www.internationaldataspaces.org/wp-content/uploads/2020/09/IDSA-Position-Paper-Open-Data-Spaces.pdf
I04	2018	CERTIFICATION : FRAMEWORK FOR THE IDS CERTIFICATION SCHEME	その他（IDS 認証基準）【全 25 ページ】 IDS の認証スキームについて説明した資料。柔軟性が高く、コスト効率が良い認証スキームについて説明しており、認証フレームワーク、参加者認証、コアコンポーネンツ認証、IDS 認証プロセス、今後の活動について記載している。	https://www.internationaldataspaces.org/wp-content/uploads/2020/01/IDSA-Strategy-paper-certification-scheme-V.2.pdf

#	発行年月	文献名	概要	URL
I05	2019/3	BLOCKCHAIN TECHNOLOGY IN IDS	技術（IDS とブロックチェーン）【全 16 ページ】 ブロックチェーン技術の概要を説明した資料。ブロックチェーン技術のコアコンセプト、IDS の文脈でのブロックチェーン技術活用シナリオ、ブロックチェーン技術を用いた IDS アーキテクチャコンセプトの実装可能性、既存プロジェクトがどのように IDS をブロックチェーン技術と合わせて使用しているかの事例紹介を含んでいる。	https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-Position-Paper-Blockchain-Technology-in-IDS.pdf
I06	2019/4	IDSA REFERENCE ARCHITECTURE MODEL v3	技術（IDS リファレンスアーキテクチャモデル）【全 118 ページ】 IDSA リファレンスアーキテクチャモデルを説明した資料。IDS の概要（目標、目的とリファレンスアーキテクチャモデルの構成）、IDS のコンテキスト（データドリブンなエコシステムやスマートサービス、データ主権、経済財としてのデータ、データ交換とデータ共有、産業クラウドプラットフォーム、ビッグデータと AI、IoT と産業 IoT、ブロックチェーン、インダストリー4.0 とデータエコノミーへの IDS の貢献）、リファレンスアーキテクチャモデルのレイヤー（ビジネス、機能、プロセス、情報、システム）、リファレンスアーキテクチャモデルの視点（セキュリティ、認証、ガバナンス）について記載している。	https://www.internationaldataspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf
I07	2019/8	FACT SHEET AND CORE STATEMENTS Version 1.0	戦略（IDS 全体概要）【全 4 ページ】 IDSA の戦略的立場、IDS の一般的コンセプト、コネクタと実装、コンセプトについて概説した文書。	https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-Fact-sheet-and-core-statements.pdf
I08	2019/9	IDS – DER STANDARD FÜR DATENSOUVERÄNITÄT UND ESSENZIELLES ELEMENT VON DATENÖKOSYSTEMEN	戦略（IDS 全体概要）【全 4 ページ】 データ主権の概念の説明、データエコシステムの重要要素について概説した文書。	https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDS-Der-Standard-fur-Datensouveranitat-Deutsch.pdf
I09	2019/10	The Role of IDS	戦略（IDS 全体概要）【全 4 ページ】	https://inte

#	発行年月	文献名	概要	URL
		for the European Data Economy	IDS が欧州データエコノミーで果たす役割について概説した資料。欧州委員会、各国関連団体の IDS に関する声明を掲載（日本からはインダストリアル・バリューチェーン・イニシアティブの後川彰久氏の声明が掲載されている）	rnationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-digital-summit-international-statements-neutral.pdf
I10	2019/11	USAGE CONTROL IN THE INTERNATIONAL DATA SPACES	その他（IDS データ起源・データ使用制御）【全 61 ページ】 データ主権の課題に対応する概念的・技術的ソリューションであるデータ起源及びデータ使用に焦点をあて、サプライチェーン管理におけるリスク軽減のため、サプライヤーや相手先商標製品の製造会社（OEM)がデータを交換するインダストリー4.0 時代向けの共通シナリオを紹介する。アクセスコントロールと使用コントロール、使用コントロールのコンセプトやデジタル権管理等関連コンセプトの違いについて説明している。	https://www.internationaldataspaces.org/wp-content/uploads/2020/09/IDSA-Position-Paper-Usage-Control-in-IDS.pdf
I11	2019/11	IDS Certification explained	その他（IDS 認証基準）【全 13 ページ】 IDS の 2 つの基礎を保証する IDS 内のコアコンポーネント認証と参加者へのアプローチを概説した資料。参加者認証、コアコンポーネント認証、IDS 認証プロセス、関連分与等について記載している。	https://www.internationaldataspaces.org/wp-content/uploads/2020/09/IDSA-Position-Paper-IDS-Certification-Explained.pdf
I12	2019/12	GDPR RELATED REQUIREMENTS AND RECOMMENDATIONS FOR THE IDS REFERENCE ARCHITECTURE	技術（GDPR と IDS リファレンスアーキテクチャモデル）【全 54 ページ】 GDPR 準拠をサポートするため、IDS リファレンスアーキテクチャモデル向け要件を引き出すことを目的に作成された資料。IDS リファレンスアーキテクチャモデルが GDPR に準拠することを支援する技術方策、IDS エコシステムが GDPR に準拠することを支援する組織的な方策、技術要件の優先順位付けとカテゴリ化、ユニークなセールスポイント、組織要件の実現、今後の活動の概要について記載している。	https://www.internationaldataspaces.org/wp-content/uploads/2020/09/IDSA-Position-Paper-GDPR-and-IDS.pdf
I13	2019	Anforderungsdokument InDaSpace Plus –	その他（IDS ユースケース）【全 29 ページ】 ユースケースに関する要件を記載した資料。デジタルサプライチェーンとスマートアーバンモビリティのユースケースについて、IDS を通して得られ	https://www.internationaldataspaces.org/wp-content/upl

#	発行年月	文献名	概要	URL
		Anwendungsfälle	る付加価値や今後の開発について説明し、ユーザストーリーを紹介、ユースケース間のつながりについて記載している。	oads/2020/09/IDSA-Position-Paper-InDaSpace-plus-Anforderungsdokument.pdf
I14	2020/2	Criteria Catalogue: Operational Environments	その他（IDS 認証基準）【全 38 ページ】 コンポーネントの運用環境に対し、基準カタログを提示する資料。認証レベルマッピングの基準、運用環境基準について記載している。	https://www.internationaldataspaces.org/wp-content/uploads/2020/10/IDSA-White-Paper-Criteria-Catalogue-Operational-Environments.pdf
I15	2020/2	DIN SPEC 27070	技術（IDS コネクタ）【全 25 ページ】 データ交換に関するドイツの標準規格。DIN SPEC 27070 のタイトルは「産業データ・サービス向けセキュリティゲートウェイの要件及び参照アーキテクチャ」であり、IDSA の一部として準備された。そのセキュリティアーキテクチャの基礎は IDS コネクタにある。Confidential 文書のため、取得には個人情報、取得目的等の入力が必要。	https://forms.office.com/Pages/ResponsePage.aspx?id=NNZGs_usx0K9RPFVfuibG9xxhhCfXtVCkmnOynWLvcdUOUNIM1Y2QUlINUI5WUg1NE1YRzdORDdZMyQlQCN0PWcu
I16	2020/3	Criteria Catalogue: Components – Connector	技術（IDS コネクタ）【全 43 ページ】 コネクタ・コンポーネント向けの基準カタログを示す資料。認証レベルマッピングの基準、IDS 仕様、IEC 62443-4-2 等について記載されている。	https://www.internationaldataspaces.org/wp-content/uploads/2020/10/IDSA-White-Paper-Criteria-Catalogue-Components-Connector.pdf
I17	2020/4	Specification: IDS Clearing	技術（IDS クリアリングハウス）【全 23 ページ】	https://www.internatio

#	発行年月	文献名	概要	URL
		House	データ交換を支援する IDS コアコンポーネント/ロールの一つとして、IDS クリアリングハウスによって満たされる最低限の要件を記載した資料。	naldataspaces.org/wp-content/uploads/2020/09/IDSA-White-Paper-Specification-IDS-Clearing-House.pdf
I18	2020/4	IMPLEMENTING THE EUROPEAN STRATEGY ON DATA. ROLE OF THE IDS	戦略（IDS と欧州データ戦略）【全 7 ページ】 欧州データ戦略を実装する上での IDS の役割を記した資料。現状の課題、欧州データ戦略、IDS の儀容、貢献、要請について記載している。	https://www.internationaldataspaces.org/wp-content/uploads/2020/09/IDSA-Position-Paper-Implementing-European-Data-Strategy-Role-of-IDS.pdf
I19	2020/5	Specification: IDS Meta Data Broker	技術（IDS メタデータブローカー）【全 37 ページ】 IDS コネクタと連動して動作するインデックスサービスとしての IDS メタデータブローカーの最低限の機能を説明した資料。IDS メタデータブローカーの仕様を記載しており、IDS メタデータブローカー向け認証基準の基礎を提供している。	https://www.internationaldataspaces.org/wp-content/uploads/2020/09/IDSA-White-Paper-Specification-IDS-Meta-Data-Broker.pdf
I20	2020/9	Criteria Catalogue: Components – Broker	技術（IDS ブローカー）【全 55 ページ】 ブローカーコンポーネント向け基準カタログを提供する資料。認証レベルマッピングの基準、IDS 仕様（コンポーネント）、IDS 仕様（コンポーネント：ブローカー）、62443-4-2 等について記載している。	https://www.internationaldataspaces.org/wp-content/uploads/2020/10/IDSA-White-Paper-Criteria-Catalogue-Components-Broker-1.pdf
I21	2020/12	IDSA Rule Book	その他（IDS ルールブック）【全 60 ページ】 将来的にデータエコノミーがスムーズに機能し価	https://internationaldataspaces.org

#	発行年月	文献名	概要	URL
			値を提供できるよう、全てのプレイヤーが共通のガバナンスフレームワークに準拠する必要がある。このフレームワークについて要点を説明した資料。P2P のデータ共有、データ共有エコシステム、データマーケットプレイス、データドリブンなプラットフォーム、データドリブンなビジネスモデル、Gaia-X 参加者についてルールを記載している。	/wp-content/uploads/dlm_uploads/IDSA-White-Paper-IDSA-Rule-Book.pdf
I22	2021/1	Gaia-X and IDS	技術（Gaia-X と IDS）【全 33 ページ】 IDS リファレンスアーキテクチャモデルがどのように Gaia-X の原則とアーキテクチャ要素と噛み合うかを説明した資料。Gaia-X は IDS ほどマチュアではないが、データ主権を拡大させ、データ共有に向けたトラストエコシステムを作り出すという共通のビジョンを持っている。IDS イニシアティブと IDS リファレンスアーキテクチャモデルは Gaia-X の全体的なビジョンに資する様々なコンセプトやソリューションを提供する。一方で、Gaia-X はデータ保管やクラウド関連のエレメントを提供する。	https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-Position-Paper-Gaia-X-and-IDS.pdf
I23	2021/3	USAGE CONTROL IN THE INTERNATIONAL DATA SPACES	その他（IDS データ起源・データ仕様制御）【全 87 ページ】 データ主権に取り組むための、概念上及び技術的なソリューションとしてのデータ使用制御やデータ起源について説明する資料。	https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-Position-Paper-Usage-Control-in-the-IDS-V3..pdf
I24	2021/4	Data Sovereignty – Critical Success Factor for the Manufacturing Industry	戦略（IDS 全体概要）【全 22 ページ】 製造業プレイヤーが構想力を保ち、顧客の要望をより適切に叶え、総合設備効率を向上させ、新たな未来志向のビジネスモデルやサービスを作り出し、実装するため、どのようにデータ主権等 IDS の主要な概念が彼らを支援するかを説明した資料。また、どのように IDS のコンセプトが製造企業にデータをスケールし、データと共に成長することを可能にするかも記載している。	https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-Position-Paper-Data-Sovereignty%E2%80%93Critical-Success-Factor-for-the-Manufacturing-Industry.pdf
I25	2021/4	New Business Models for Data Spaces	その他（IDS ビジネス適用・ユースケース）【全 26 ページ】 データスペースやデータ主権を土台とした新たな	https://internationaldataspaces.org/wp-

#	発行年月	文献名	概要	URL
		Grounded in Data Sovereignty	製品やサービスの創出を促す資料。データスペースは汎ヨーロッパの主権あるデータインフライニシアティブである Gaia-X の重要な特徴である。本資料は、ビジネスモデルやビジネスエコシステムキャンバスを含むフレームワークや手法を IDS 視点に応用するものである。これらはビジネス計画目的で体系的なアプローチやチェックリストを提供する。また、ビジネス視点を提示し、ガバナンス、参加者、サポートサービスプロバイダに向けて、初期導入者の具体的ユースケース例を示す。結論として、本資料はデジタル化に直面する全ての企業がビジネス機会し、データ主権を重視した市場により生み出される将来により、自社がいかに影響を受けるかを再確認すべきであると呼びかけている。	content/uploads/IDSA-Position-Paper-New-Business-Models-sneak-preview-version.pdf
I26	2021	Design Principles for Data Spaces Position Paper 2021	技術（IDS データスペース設計）【全 111 ページ】 データスペースを築くために必要な、セクターやイニシアティブを越えた基本的デザイン原則を初めて定義した資料であり、将来のデータエコノミー創生における主権あるデータ共有の重要性を強調している。IDSA と、13 の Horizon 2020 プロジェクトや類似イニシアティブに参加する 25 組織の 40 人以上のデータスペース、産業ドメイン専門家が協力して作成された。データスペースのデザイン原則、ソフトインフラとデータスペースガバナンスの構成要素に関する合意を定義する初のアプローチを示している。	https://design-principles-for-data-spaces.org/

8.2 Gaia-X 発行文書

#	発行年月	文献名	概要	URL
G01	2019/10	Project Gaia-X	戦略（Gaia-X の目指す姿）【全 56 ページ】 ドイツ連邦政府、企業、科学コミュニティがハイパフォーマンスで競争力を持ち、セキュアで信頼あるデータインフラストラクチャを欧州に構築する努力を続ける中で、Gaia-X が誕生した背景を説明。ドイツ産業界・政府視点で現状とモチベーション、トレンド、目標を説明した後、Gaia-X のターゲット、ソリューション、ユーザ視点から見た Gaia-X プロジェクト（インダストリー4.0/SMEs、スマートリビング、金融セクター、ヘルスケア、公共機関とサイエンス）、プロバイダ視点から見た付加価値について記載している。	https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/project-gaia-x.html
G02	2020/2	Franco-German Position on Gaia-X	戦略（ドイツとフランスの共同声明）【全 5 ページ】 ドイツ及びフランスの産業代表者及び政府が、欧州データ及び AI ドリブンなエコシステムの創設を促進し、データ主権を担保し、各参加者が創出価値の恩恵を受けること保証するという目標を持った Gaia-X を支援することを表明した資料。	https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Downloads/franco-german-position-on-gaia-x.pdf?__blob=publicationFile&v=4
G03	2020/6	Gaia-X - the European project kicks off the next phase	戦略（Gaia-X 主要ドキュメント出版）【全 13 ページ】 Gaia-X の全体像を概説した資料。Gaia-X の 7 原則、GXFS を含めた Gaia-X のアーキテクチャ概念、Gaia-X の背景にある欧州の価値観、ユーザ視点、各ドメインとユースケース、Gaia-X 要件、Gaia-X 関連イニシアティブ（データ共有・データ主権、行動規範、ポリシー・認証・コンプライアンス、オープンソースフレームワークにわけて団体を紹介）、技術アーキテクチャ概念の設計、今後の展望について記載している。	https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/gaia-x-the-european-project-kicks-of-the-next-phase.html
G04	2020/6	Gaia-X: A Pitch Towards Europe	戦略（Gaia-X 主要ドキュメント出版）【全 40 ページ】 Gaia-X の紹介、ユーザ視点からの Gaia-X の付加価値、Gaia-X 開発におけるユーザ視点の動員と統合、Gaia-X のベネフィット、Gaia-X エコシステム、Gaia-X エコシステムの参加者、Gaia-X エコシステムの主要要件、ドメイン特有の要件（ヘルス、公共部門、スマートリビング、金融）等について記載している。	https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/gaia-x-a-pitch-towards-europe.html
G05	2020/6	Gaia-X: Technical	技術（Gaia-X 技術アーキテクチャ）【全 56 ページ】 関連する定義、コンセプト、アーキテクチャ面につ	https://www.data-infrastructur

#	発行年月	文献名	概要	URL
		Architecture	いて、Gaia-X の基礎をサマライズした資料。Gaia-X の新規参加者に熟読が進められている。コアアーキテクチャエレメント、組織及びガバナンス視点、エコシステム視点、情報セキュリティ及びデータ保護視点、オンボーディング及び認証、今後の展望について記載されている。	e.eu/GAIAX/Redaktion/EN/Publications/gaia-x-technical-architecture.html
G06	2020/6	Gaia-X: Driver of digital innovation in Europe	戦略（Gaia-X 主要ドキュメント出版）【全 30 ページ】 幅広い読者向けに、Gaia-X のメカニズム、コンポーネント、プロセスをハイレベルな視点で説明した文書。ワーキンググループの検討結果をサマライズし、技術アーキテクチャ、ポリシーやフェデレーションサービスに関する提案を含んでいる。	https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/gaia-x-driver-of-digital-innovation-in-europe.html
G07	2020/6	Gaia-X: Policy Rules and Architecture of Standards	戦略（Gaia-X 主要ドキュメント出版）【全 19 ページ】 データ共有、相互運用性と相互接続を可能にする重要要素として、関連する標準、ポリシー、オープン APIs を収集するメソドロジーを説明する。相互に同意されたポリシーや規則がどのように Gaia-X の基本理念を支えるかについて、共通理解を提供する。Gaia-X のゴールが、オープンさ、透明性、全ての関連ステークホルダコミュニティの統合を保証する標準化されたコンポーネントと可逆性原則に基づくことを示す。	https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/gaia-x-policy-rules-and-architecture-of-standards.html
G08	2021/1	Gaia-X Domain Agriculture	その他（Gaia-X の分野別ユースケース）【全 22 ページ】 農業分野におけるデータスペースの現状、課題、ユースケースについて記載	https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/211116-pp-agriculture.pdf?__blob=publicationFile&v=3
G09	2021/1	Gaia-X Domain Finance Position Paper Version 1.0 2021	その他（Gaia-X の分野別ユースケース）【全 5 ページ】 金融エコシステムにおける Gaia-X 実装ロードマップ（2021－2025）を記載	https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/211116-pp-finance.pdf?__blob=publicationFile&v=3
G10	2021/1	Gaia-X Domain	その他（Gaia-X の分野別ユースケース）【全 7 ペー	https://www

#	発行年月	文献名	概要	URL
		Mobility Position Paper Version 1.0 2021	ジ】 モビリティデータスペース向け Gaia-X ロードマップ(2021-2025)を記載	.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/211116-pp-mobility.pdf?__blob=publicationFile&v=3
G11	2021/1	Gaia-X Domäne Smart City/ Smart Region Positionpapier Version 1.0 2021	その他(Gaia-X の分野別ユースケース)【全 14 ページ】 スマートシティ、地域向け Gaia-X を概説し、ドイツにおける先端事例を紹介	https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/211116-pp-scsr.pdf?__blob=publicationFile&v=3
G12	2021/1	Gaia-X Domain Smart Living Position Paper Version 1.0 2021	その他(Gaia-X の分野別ユースケース)【全 26 ページ】 スマートリビング分野のデータスペースの目標、課題、ソリューション、ユースケース、データスペースのマチュリティについて記載	https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/211116-pp-smartliving.pdf?__blob=publicationFile&v=3
G13	2021/1	Gaia-X Domain Health Position Paper Version 1.0 2021	その他(Gaia-X の分野別ユースケース)【全 39 ページ】 ヘルス分野のデータスペースの目標、ソリューション、データバリューチェーン、データスペースのマチュリティについて記載	https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/211116-pp-health.pdf?__blob=publicationFile&v=3
G14	2021/1	Gaia-X Domain Geoinformation Position Paper Version 1.0 2021	その他(Gaia-X の分野別ユースケース)【全 17 ページ】 地理情報分野のデータスペースの目標、課題、ソリューション、ユースケース、データスペースのマチュリティについて記載	https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/211116-pp-geoinformation.pdf?__blob=publicationFile&v=3
G15	2021/1	Gaia-X Domain Energy	その他(Gaia-X の分野別ユースケース)【全 55 ペー	https://www.bmwi.de/Re

#	発行年月	文献名	概要	URL
		Position Paper Version 1.0 2021	ジ】 エネルギー分野のデータスペースの目標、課題、ソリューション、ユースケース、マチュリティ、ロードマップについて記載	daktion/EN/Publikationen/Digitale-Welt/211116-pp-energy.pdf?__blob=publicationFile&v=3
G16	2021/1	Gaia-X Domain Industry4.0 / SME Position Paper Version 1.0 2021	その他（Gaia-X の分野別ユースケース）【全 7 ページ】 インダストリー4.0 がもたらすデジタルエコシステムについて記載	https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/211116-pp-industry40.pdf?__blob=publicationFile&v=3
G17	2021/3	Gaia-X Domain Public Sector Position Paper Version 1.0 2021	その他（Gaia-X の分野別ユースケース）【全 9 ページ】 公共部門のデジタル化の重要性、Gaia-X 公共部門の目標等について記載	https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/211116-pp-public.pdf?__blob=publicationFile&v=3
G18	2021/3	Gaia-X Architecture Document	技術（Gaia-X 技術アーキテクチャ）【全 47 ページ】 トップレベルの Gaia-X アーキテクチャモデルを説明した資料。概念モデルに重点を置いており、Gaia-X アーキテクチャの基本的なコンセプトや諸条件について、様々な Gaia-X ステークホルダグループが明確に理解できるようにすることを目的としている。さらなる Gaia-X アーキテクチャの精緻化、仕様、実装のための基礎を形作り、Gaia-X フェデレーションサービス仕様のリファレンスを提供している。	https://www.gaia-x.eu/sites/default/files/2021-05/Gaia-X_Architecture_Document_2103.pdf
G19	2021/4	Policy Rules Document (PRD 21.04)	戦略（Gaia-X ポリシー・ルール）【全 7 ページ】 Gaia-X エコシステムの原則、付加価値を守るハイレベルな目的を定義するポリシー・規則に関する資料。定義、クラウドサービスプロバイダ（GDPR 準拠、透明性、サイバーセキュリティ、ポータビリティ、契約）、データスペース内でのデータ共有について記載している。	https://www.gaia-x.eu/sites/default/files/2021-05/Gaia-X_Policy%20Rules_Document_2104.pdf
G20	2021/4	The energy data space	その他（Gaia-X の分野別ユースケース）【全 36 ページ】	https://gaia-

#	発行年月	文献名	概要	URL
		The path to a European approach for energy	エネルギーデータスペースについて、目標と課題、各分野におけるソリューション、ロードマップを記載した資料。	x.eu/sites/default/files/2021-06/Gaia-X_Data-Space-Energy_Position-Paper.pdf
G21	2021/6	Gaia-X Architecture Document 21.06 Release	技術（Gaia-X 技術アーキテクチャ）【全 89 ページ】 Gaia-X のコンセプトモデル、運用モデル（コンセプト）、フェデレーションサービス、参加者のユースケース、エコシステム、グロッサリーを記載した資料。	https://www.gaia-x.eu/sites/default/files/2021-06/Gaia-X_Architecture_Document_2106.pdf
G22	2021/8	Data Space Business Committee: Position Paper	その他（Gaia-X のビジネス適用・ユースケース）【全 177 ページ】 Gaia-X に基づくデータ共有エコシステムへの参加アプローチ、ユースケース、計画、初期アイデアについてまとめた資料。農業、教育、エネルギー、金融、ヘルス、インダストリー4.0、モビリティ、公共部門、地理情報、スマートリビング分野の現状を示している。データスペースの現在の目標、課題、計画されるユースケース及び実装されたユースケースのロードマップの情報を含む。	https://gaia-x.eu/sites/default/files/2021-08/Gaia-X_DSBC_PositionPaper.pdf
G23	2021/9	Gaia-X and European Smart Cities and Communities white paper V21.09	その他（Gaia-X の分野別ユースケース）【全 19 ページ】 欧州のスマートシティ部門において、Gaia-X の応用がもたらす効果についてまとめた資料。様々な視点を結びつけること、Gaia-X と主要なローカル技術コンセプトの共通認識、それらがどのように関連するかに関する共通認識を確立することを目的としている。市の行政機関、IT 産業、EU 政策決定者や Gaia-X メンバーに向けて発行された。本資料は欧州スマートシティ・コミュニティの文脈で Gaia-X のアプリケーションドメインの枠組みを作る初の試みであるとされる。	https://gaia-x.eu/sites/default/files/2021-10/Gaia-X%20SCC%20white%20paper.pdf
G24	2021/11	Gaia-X Architecture Document 21.09 Release	技術（Gaia-X 技術アーキテクチャ）【全 101 ページ】 Gaia-X のコンセプトモデル、運用モデル、フェデレーションサービス、参加者のユースケース例、エコシステム、グロッサリーについて記載した資料。	https://www.gaia-x.eu/sites/default/files/2021-10/Gaia-X_Architecture_Document_2109.pdf
G25	2021/12	Gaia-X Labelling	技術（Gaia-X ラベリング）【全 5 ページ】	https://gaia-

#	発行年月	文献名	概要	URL
		Framework	Gaia-X のラベル付けに関する資料。ラベルの意義、コンプライアンス、価値、原則、ラベル所有者と発行者、Gaia-X ベーシックラベルについて記載している。	x.eu/sites/default/files/2021-11/Gaia-X%20Labelling%20Framework_0.pdf
G26	2021/12	Gaia-X Federation Services (GXFS) Gaia-X Ecosystem Kickstarter	技術（Gaia-X GXFS）【全 10 ページ】 より広い Gaia-X エコシステムの一部として、GXFS のコンセプトを説明した資料。読者に Gaia-X プロジェクトについて紹介し、GXFS がなぜ Gaia-X の中で主要な役割を果たすのかを説明し、非技術者である読者に対し様々な GXFS の概要を提供している。	https://gaia-x.eu/sites/default/files/2022-01/Gaia-X_Federation_Services_White_Paper_1_December_2021.pdf
G27	2021/12	Vision & Strategy	戦略（Gaia-X の目指す姿）【全 15 ページ】 Gaia-X イニシアティブの核となる要素のハイレベルな概要を提供する資料。Gaia-X のビジョンと使命、主要課題、コアバリュー、ステークホルダにもたらすベネフィットについて説明している。また、プロジェクトの使命、スコープ、主要デリバラブル、戦略プランについて詳説している。	https://gaia-x.eu/sites/default/files/2021-12/Vision%20%26%20Strategy.pdf
G28	2021/12	Gaia-X Architecture Document 21.12 Release	技術（Gaia-X 技術アーキテクチャ）【全 119 ページ】 フェデレーティドオープンデータインフラのコンセプトとコンセプト間の関係を特定・説明した資料。欧州デジタルエコノミーの全ての参加者間の相互接続、相互運用性、統合を Gaia-X がいかに促進するかを説明している。この版は、過去のアーキテクチャ資料に代わるものである。Gaia-X はデータやクラウド主権に関する欧州の価値観に基づくフェデレーティドオープンデータインフラの策定を目的としている。Gaia-X の使命はデータ共有、ベストプラクティス、ツール、ガバナンスメカニズムの共通基準を構成するデータ共有アーキテクチャを設計・実装することであると記載されている。	https://gaia-x.eu/sites/default/files/2022-01/Gaia-X_Architecture_Document_2112.pdf
G29	2021	Software Requirements Specification for Gaia-X Federation Service Sovereign Data Exchange Data Exchange Logging Service	技術（Gaia-X GXFS）【全 35 ページ】 Gaia-X 主権データ交換サービスのサブコンポーネント「データ交換ロギングサービス（Data Exchange Logging Service)」の要件、特長、構成を定義している。	https://www.gxfs.eu/specifications/

#	発行年月	文献名	概要	URL
		SDE.DELS		
G30	2021	Gaia-X Federation Services for Identity & Trust Architecture Overview IDM.AO	技術（Gaia-X GXFS）【全 77 ページ】 SSI と DIF に沿った分権化された識別管理、署名や認証メカニズムを持つトラストレイヤー、組織・参加者・社長向けオンボーディング/オフボーディングプロセスを支援するサービスコンポーネント・機能、アクセス管理（認証と権限付与）といったサービス機能について特定し、基礎を示している。	https://www.gxfs.eu/specifications/
G31	2021	Software Requirements Specification for Gaia-X Federation Services Compliance Continuous Automated Monitoring CP.CAM	技術（Gaia-X GXFS）【全 31 ページ】 Gaia-X 内のコアサービスである継続自動監視（CAM）の機能・非機能要件、アーキテクチャを記載している。	https://www.gxfs.eu/specifications/
G32	2021	Software Requirements Specification for Gaia-X Federation Services Compliance Notarization API CP.NOTAR	技術（Gaia-X GXFS）【全 46 ページ】 コンプライアンスのサブコンポーネントである「公証 API（Notarization API)」の要件を定義している。	https://www.gxfs.eu/specifications/
G33	2021	Software Requirements Specification for Gaia-X Federation Services Compliance Onboarding & Accreditation Workflows CP.OAW	技術（Gaia-X GXFS）【全 54 ページ】 Gaia-X エコシステムのオンボーディングと認証評価ワークフローを定義している。	https://www.gxfs.eu/specifications/
G34	2021	Software Requirements Specification for Gaia-X Federation Services Federated Catalogue Core Catalogue Features	技術（Gaia-X GXFS）【全 96 ページ】 GXFS「連合カタログ（Federated Catalogue)）の要件、外部インターフェース、主要な設計判断について説明している。	https://www.gxfs.eu/specifications/

#	発行年月	文献名	概要	URL
		FC.CCF		
G35	2021	Software Requirements Specification for Gaia-X Federation Services Authentication/ Authorization IDM.AA	技術（Gaia-X GXFS）【全 37 ページ】 識別管理とトラストコンポーネント「認証・権限付与（Authentication/Authorization)」の要件を定義している。	https://www.gxfs.eu/specifications/
G36	2021	Software Requirements Specification for Organization Credential Manager IDM.OCM	技術（Gaia-X GXFS）【全 52 ページ】 識別管理とトラストサブコンポーネント「組織認証情報管理者（Organization Credential Manager)」の要件を定義している。	https://www.gxfs.eu/specifications/
G37	2021	Software Requirements Specification for Gaia-X Federation Services Personal Credential Manager IDM.PCM	技術（Gaia-X GXFS）【全 41 ページ】 識別管理とトラストサブコンポーネント「個人認証情報管理者（Personal Credential Manager)」の要件を定義している。	https://www.gxfs.eu/specifications/
G38	2021	Software Requirements Specification for Gaia-X Federation Services Trust Services API IDM.TSA	技術（Gaia-X GXFS）【全 58 ページ】 識別管理とトラストサブコンポーネント「トラストサービス API(Trust Services API)」の要件を定義している。	https://www.gxfs.eu/specifications/
G39	2021	Software Requirements Specification for Gaia-X Federation Services Integration & Portal Orchestration	技術（Gaia-X GXFS）【全 17 ページ】 公開入札の参加者向けに、編成サービス（Orcehstration Service)について説明している。編成サービスは Gaia-X のコアサービスとはみられていないが、Gaia-X ポータル、API フレームワーク、ワークフローエンジン、コア Gaia-X サービスと共に、実装プロトタイプを示すものである。	https://www.gxfs.eu/specifications/
G40	2021	Software Requirements Specification for Gaia-X	技術（Gaia-X GXFS）【全 115 ページ】 ウェブベースのユーザインターフェースを持つ Gaia-X ポータルの要件について説明している。	https://www.gxfs.eu/specifications/

#	発行年月	文献名	概要	URL
		Federation Services Integration & Portal		
G41	2021	Software Requirements Specification for Gaia-X Federation Services Sovereign Data Exchange Data Contract Service SDE.DCS	技術（Gaia-X GXFS）【全 59 ページ】 Gaia-X エコシステムを最低限実行可能とするため必要とみなされる GXFS の一機能である、Gaia-X データ契約サービスの仕様を提示している。	https://www.gxfs.eu/specifications/
G42	2022/2	Gaia-X Labelling Criteria Version 0.7	技術（Gaia-X ラベリング）【全 30 ページ】 Labelling Framework は Gaia-X Labelling Criteria 資料で示された方策や具体的基準を更に詳説した資料。基準リストは、要件が満たされることを担保する包括的認証手法と合わせ、Policies and Rules Committee, Technical Committee, Data Spaces and Business Committee が策定したポリシーと要件を統合している。異なる目的やニーズのためサービスを探すユーザが必要とする、サービス間の差別化を可能にする。また、本資料は透明性フレームワークで説明されるアトリビュートの最低資格レベルを定義している。	https://gaia-x.eu/sites/default/files/2022-02/Labelling_Criteria_Whitepaper_v07.pdf

8.3 IDSA・Gaia-X に関するインタビュー結果

個人の見解が含まれているため略

8.4 コネクタを用いたデータ連携の試行

本調査研究では、相互運用性の実現のための必要な要素の調査とともに、その具体的な機能を検証するため、中核技術であるコネクタの試行的なプログラムの構築等を実施した。

具体のユースケースとしては、「デジタル社会の実現に向けた重点計画」（令和 3 年 12 月 24 日閣議決定）において、取組分野を超えた横断的な連携が重要な相互連携分野として「取引（受発注・請求・決済）」、「スマートシティ」の 2 分野を指定されていることや、本調査研究が（「生活用」と並行して行われている）「産業用」であることを踏まえ、「取引（受発注・請求・決済）」を対象に構築を進めることとした。

構築にあたっては、業界をまたぐ異なる EDI 間の受発注取引を想定し、コネクタを介したデータの送受信を行うとともに、両者の間でデータの翻訳（変換処理）を行うこととした。

- 発注者が、Android アプリ上で商品バーコードを読み取り、必要な項目を入力し、発注者が利用する EDI ベースの発注データを作成する。
- 発注者と受注者が、コネクタ同士でデータの送受信を実施する。
- 受注者は、受注者が利用する EDI ベースのデータ構造に変換した上で、発注データを確認する。

なお、報告書本文に述べたように、コネクタにはいくつか種類があるが、本試行においては、なかでも主要なものと目される Eclipse Data Connector（EDC）を構築することとした。

以上に関するコンポーネントプログラム、試作アプリケーションは別添 1 のとおりであり、それらの取扱説明書等一式は別紙 1～4、別添 2 のとおりである。

別紙 1　EDC 検証テスト　環境構築手順書
別紙 2　EDC 検証テスト　アプリ導入手順書
別紙 3　コネクタクラス図
別紙 4　コネクタに関するライセンス条件案

別添 1　コネクタのコンポーネントプログラム、受発注取引のアプリケーションに関するソースコード（テストデータを含む。）
別添 2　動画による手順書