



DATA-EX 分野間データ連携基盤技術仕様書

一般社団法人データ社会推進協議会(法人番号 4011005007414)

2025 年 4 月 23 日

改版履歴

版数	発行年月日	改版内容
1.0	2025 年 4 月 23 日	初版作成

目次

1. はじめに	8
1-1. 技術仕様書の位置づけ	8
1-2. DATA-EX ドキュメント体系	9
1-3. 本仕様書のスコープ	11
1-4. 記述規則	11
2. リファレンスと用語定義	12
2-1. リファレンス	12
2-2. 用語定義	13
3. 構築の背景と目的	18
3-1. 背景	18
3-2. 構築目的と原則	19
3-3. 概念モデル	19
3-4. 利用メリット	21
3-5. 想定ユースケース	21
4. 提供サービス	23
4-1. 主要サービス	23
4-1-1. 分野間データ連携サービス	23
4-1-2. 来歴管理サービス	23
4-1-3. ポータルサービス	24
4-2. 支援サービス	24
4-2-1. データカタログ横断検索サービス	24
4-2-2. データカタログ作成サービス	24
4-2-3. 語彙管理サービス	25
4-2-4. データ取引市場サービス	25
5. 連携サービス	26
5-1. トラストサービス	26
5-1-1. 外部 IdP	26
5-1-2. e シールサービス	26
5-1-3. 電子署名サービス	26
5-1-4. タイムスタンプサービス	26
5-2. 来歴管理拡張サービス	27
6. 参加方法	28
7. DATA-EX 構成要素	29
7-1. ステークホルダー	29

7-1-1. 主要ステークホルダー	29
7-1-2. 支援ステークホルダー	30
7-1-3. 連携ステークホルダー	31
7-2. オブジェクト	31
7-2-1. アカウント情報	31
7-2-2. 認証情報	32
7-2-3. 認可情報	32
7-2-4. コネクタ設定情報	32
7-2-5. 証明書情報	32
7-2-6. コネクタロケーション情報	32
7-2-7. DDP ロケーション情報	32
7-2-8. 来歴情報	33
7-2-9. 履歴情報	33
7-2-10. 加工来歴情報	35
7-2-11. 加工履歴情報	35
7-2-12. カタログ情報	35
7-2-13. 契約情報	35
7-2-14. DDP	36
7-3. ID	37
7-3-1. DATA-EX ID	37
7-3-2. コネクタ ID	38
7-3-3. 履歴 ID	38
7-3-4. カタログ ID	38
7-3-5. 契約 ID	38
7-3-6. DDP ID	38
7-4. 機能	39
7-4-1. DATA-EX 内部の機能	39
7-4-2. DATA-EX 外部の機能	44
8. シナリオ	50
8-1. 契約を交わさずにデータ交換を行う	50
8-1-1. 利用準備	50
8-1-2. 利用	54
8-1-3. 利用停止	65
8-2. 相対取引によって契約を交わし、データ交換を行う	69
8-2-1. 利用準備	69
8-2-2. 利用	74

8-2-3. 利用停止	87
8-3. データ取引市場などを介して契約を交わし、データ交換を行う.....	91
8-3-1. 利用準備	91
8-3-2. 利用	96
8-3-3. 利用停止	112
9. コンポーネントアーキテクチャ.....	117
9-1. DATA-EX のコンポーネント間のインタラクション	118
9-2. アプリケーション層のデータ提供側のコンポーネントと DATA-EX のコンポーネント間の インタラクション	123
9-3. アプリケーション層のデータ受領側のコンポーネントと DATA-EX のコンポーネント間の インタラクション	126
9-4. トラストサービス層のコンポーネントと DATA-EX のコンポーネント間のインタラクション	128
9-5. アプリケーション層のコンポーネントとトラストサービス層のコンポーネント間のインタラク ション	130
10. API 仕様.....	132
10-1. API 一覧.....	132
10-2. API 仕様.....	132
10-2-1. データ交換機能(データ提供側).....	132
10-2-2. データ交換機能(データ受領側).....	137
10-2-3. 認証機能	142
10-2-4. 認可機能	145
10-2-5. コネクタロケーション管理機能	152
10-2-6. 来歴管理機能	155
10-3. 【付録】API 仕様の定義方法	158
11. 処理シーケンス	159
11-1. シーケンス一覧	159
11-2. 処理シーケンス図	160
11-2-1. 「契約を交わさずにデータ交換を行う」シナリオのシーケンス	160
11-2-2. 「相対取引によって契約を交わし、データ交換を行う」シナリオのシーケ ンス.....	161
11-2-3. 「データ取引市場などを介して契約を交わし、データ交換を行う」シナリ オのシーケンス.....	173
12. セキュリティ・トラスト.....	197
12-1. リソースの識別.....	197
12-2. ネットワークの保護	197

12-3. リソースの脆弱性診断	198
12-4. アクセス制御ポリシー・アクセス管理	198
12-5. 不正利用の検知	198
12-6. トラスト全体像	198
12-6-1. 参加者のトラスト	199
12-6-2. システムのトラスト	201
12-6-3. データのトラスト	202
12-6-4. データ取引の証跡管理	203
12-7. 参加者のトラスト(要件)	206
12-7-1. DATA-EX への参加	206
12-7-2. 参加者の識別	207
12-8. システムのトラスト(要件)	207
12-9. データのトラスト(要件)	208
12-9-1. トラストサービス基盤連携	208
12-9-2. トラストサービス基盤利用準備	208
12-9-3. カタログ	209
12-9-4. 契約書	209
12-9-5. DDP	209
12-10. データ取引の証跡管理(要件)	209
12-10-1. 来歴管理サービス	209
12-10-2. 来歴管理拡張サービス	211
13. ガバナンス	212
13-1. ポリシー	213
13-1-1. DATA-EX 参加者が守るべきポリシー	213
13-1-2. DATA-EX 運営事業者が守るべきポリシー	214
13-2. 契約	214
13-3. ガバナンス推進における役割	214
14. 国際連携	216
14-1. 国際連携の概要	216
14-2. 国際連携の課題と将来像	216
14-3. 国際連携のトラスト	216
14-4. 国際連携のコネクタ間連携	217
14-5. 国際連携のコネクタ間連携: 共通 I/F 方式の例	218
14-5-1. 国際連携の概念モデル	218
14-5-2. 国際連携のコネクタ・アーキテクチャ	219
14-5-3. 国際連携のコネクタ技術仕様	222

14-6. 将来像の国際連携機能について	222
15. 今後の展望.....	223
この文書について.....	224

1. はじめに

1-1. 技術仕様書の位置づけ

DATA-EX とは「分野を超えたデータ連携を実現するために、データ社会推進協議会(DSA: Data Society Alliance)が行う取り組みの総称(ブランド名)」である。本仕様書では、その取り組みの中核となる DATA-EX 分野間データ連携基盤に関して DATA-EX と呼称する。DATA-EX は分野を超えてデータの発見と利用を可能とするプラットフォームである。近年、経済的・技術的な目的で、分野内のデータの流通に閉じず、分野外のデータも連携されるケースが増えている。しかし、従来の分野内データ連携は各分野独自のルールや基盤があり、外部との連携性を考慮していなかった。そこで、分野間で広く多様なデータを活用して新たな価値を創出する目的のもと、「データ連携」とそれを「利活用したサービスを提供」する基盤として DATA-EX を提供する。

DATA-EX を利用する際に必要・参考となる各ドキュメントの位置づけは、次の通りである。上位ドキュメントとして「技術仕様書(本書)」「利用契約書」「プライバシー方針書」が存在し、更に「技術仕様書」の下位ドキュメントとして「サービスレベル保証書」、「DATA-EX データカタログ項目仕様」「DATA-EX 利用解説書」が存在する。本技術仕様書は、DATA-EX 参加者や DATA-EX 運営事業者、その他ステークホルダー(DATA-EX 支援サービス提供者等)を対象読者とする。更に、本仕様書はそれぞれのステークホルダー間の円滑・安全な情報共有・連携を図ることを目的に作成されており、DATA-EX のアーキテクチャの各種定義及び、各ステークホルダーの役割を読者が理解する為に必要な解説を記載する。特に、データ連携基盤としての技術的な概念モデルや運用モデルを記載し、詳細なテクノロジーやベンダー、開発者やシステムには依存しない。これらを本技術仕様書にて定義する事により、現時点での DATA-EX のステークホルダーや機能に関する用語・コンセプトを統一・明確化を行う。更に本技術仕様書は、今後の議論点、詳細、実装のための基礎的な情報や定義としての活用方法も想定される。今後、DATA-EX が分野間データ連携の基盤として発展する中で、分野間データ連携のビジネス要件、データ連携に関する行政側のガバナンス、技術的進化や革命に応じて、本技術仕様書の更新がなされることが想定される。

DATA-EX は分野間データ連携に関わるステークホルダーが安心・安全に交流できる環境の構築を支援する。これらの交流には真正性確認、トラストメカニズム、データ活用のルール設定と言った、様々なコンプライアンス原則があるため、DATA-EX におけるデータ連携の各ステークホルダーに必須・任意とされる行動を本技術仕様書では記載する。

技術仕様書の公開時点において、DATA-EX は企画・要求定義フェーズにある。DATA-EX の社会実装に向けて、今後は図 1 に示すように要件定義、基本設計、詳細設計、テストを実施する必要がある。各フェーズでの成果物として、下記ドキュメントを想定している。

- ・ 要件定義フェーズ
 - 要件定義書
- ・ 基本設計フェーズ
 - 基本設計書
- ・ 詳細設計フェーズ

-
- 詳細設計書
 - 運用・保守設計書
 - 導入手順書
 - ・ テストフェーズ
 - 単体テスト設計書
 - 単体テスト実施報告書
 - 単体テスト設計書(インフラテスト)
 - 単体テスト実施報告書(インフラテスト)
 - 結合テスト設計書
 - 結合テスト実施報告書
 - 結合テスト設計書(インフラテスト)
 - 結合テスト実施報告書(インフラテスト)
 - 運用手順書
 - 操作手順書
 - 総合テスト設計書
 - 総合テスト実施報告書
 - 受け入れテスト手順書(案)

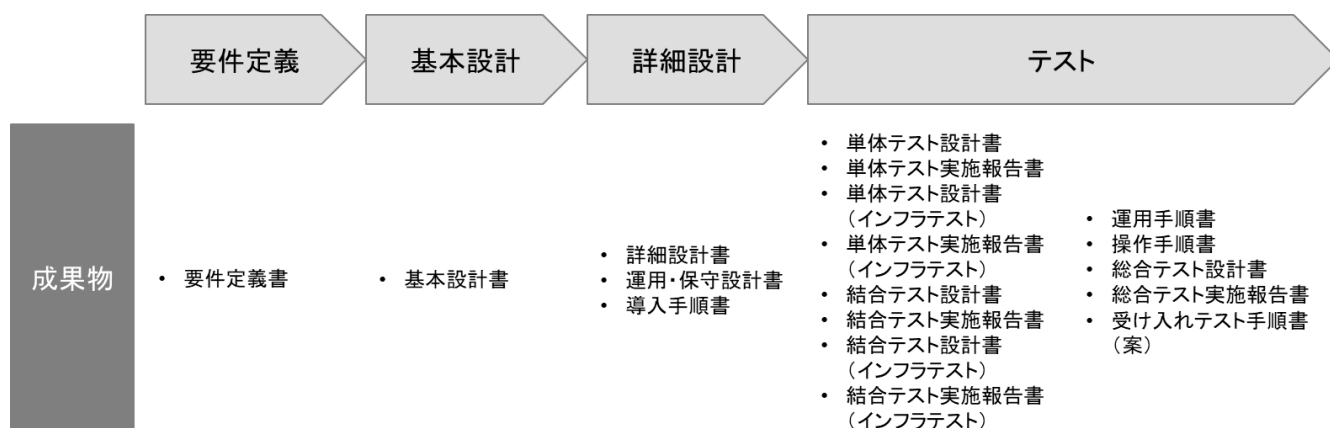


図 1:システム開発の工程と想定成果物(例)

1-2. DATA-EXドキュメント体系

本技術仕様書のドキュメント体系を以下の表 1 に示している。DATA-EX に関する「技術仕様書」が本仕様書であり、加えて「利用契約書」、「プライバシー方針書」の 3 点が上位ドキュメントとして、DATA-EX の利用に際して参照すべき文書であり、DATA-EX のステークホルダーが遵守する内容を定めている。また、「サービスレベル保証書」、「DATA-EX データカタログ項目仕様」

「DATA-EX 利用解説書」の3点は本技術仕様書の下位ドキュメントであり、必要に応じて参照すべき文書である。

なお、本技術仕様書のドキュメント体系のうち、「サービスレベル保証書」「DATA-EX データカタログ項目仕様」「DATA-EX データカタログ項目ガイドライン」「DATA-EX 利用解説書」「利用契約書」「プライバシー方針書」は DATA-EX の社会実装に合わせて今後作成する予定である。

表 1:DATA-EXドキュメント体系の文書一覧

No.	文書名	文書形態	概要
1	DATA-EX 分野間データ連携基盤技術仕様書	Word 文書	DATA-EX のアーキテクチャの各種定義及び、各ステークホルダーの役割を定めた文書 DATA-EX の在り方や今後の議論点、実装のための基礎的な情報等を理解する為に利用する
2	サービスレベル保証書	Word 文書	DATA-EX で提供されるサービスの品質保証レベルを定めた文書 DATA-EX 運営事業者が提供するサービスの品質保証レベルや責任範囲を理解する為に利用する
3	DATA-EX データカタログ項目仕様	Word 資料	DATA-EX で使用するデータカタログの項目を定め、項目の仕様を解説した文書 データカタログに記載する必要がある項目を理解する為に利用する 国際標準(W3C DCAT)に基づく項目(タイトル、説明、作成者等)、利用条件の把握や検索条件に必要な利用ライセンスに関する項目(契約形態、秘密保持義務、利用用途等)、データの内容を理解するために必要な項目(語彙、用語、スキーマ等)、データ交換を実現するために必要な項目(コネクタ ID、DDP ID 等)について記載する
4	DATA-EX データカタログ項目ガイドライン	Word 文書	データカタログ項目仕様の値設定の補足や値の候補リストのガイドラインを記載する
5	DATA-EX 利用解説書	Word 文書	DATA-EX の参加基準を定め、具体的な利用手順を解説した文書 DATA-EX への参加方法や DATA-EX の利用方法を理解する為に利用する
6	利用契約書	Word 文書	DATA-EX 利用時における参加者の権利や義務、遵守すべきルールについて定めた文書 参加者全員に適用される DATA-EX の統一的なルールを理解する為に利用する
7	プライバシー方針書	Word 文書	DATA-EX における個人情報の取扱い方針を定めた文書 DATA-EX で取得される個人情報の利用目的等を理解する為に利用する

1-3. 本仕様書のスコープ

本仕様書では、DATA-EX のサービスおよび構成要素(ステークホルダー、オブジェクト、ID、機能)を規定する。また、DATA-EX を利用したデータ交換についてのシナリオおよびシナリオを実現する上での各機能間の連携についてコンポーネントアーキテクチャ、API 仕様および処理シーケンスを規定する。

1-4. 記述規則

本仕様書では、規定的な記述の要求・禁止・許容を、以下のように記述する。

要求：

「～(L)なければならない。(SHALL)」
「～する。(SHALL)」
「～とする。(SHALL)」
「～による。(SHALL)」

禁止：

「～(L)てはならない。(SHALL NOT)」
「～(L)ない。(SHALL NOT)」

許容：

「～(L)てもよい。(MAY)」
「～差し支えない。(MAY)」と記述する。

<Note>：規定的記述の理解または利用を助けるための追加情報のみを示す。ただし、要求事項または規格を利用するために不可欠な情報を含めない。

2. リファレンスと用語定義

本仕様書にて参照あるいは、参考となる資料に関して以下の「2-1. リファレンス」にて整理する。

2-1. リファレンス

- [1] International Data Spaces Association, “REFERENCE ARCHITECTURE MODEL,” [オンライン]. Available: <https://internationaldataspaces.org/wp-content/uploads/IDS-Reference-Architecture-Model-3.0-2019.pdf>.
- [2] デジタル庁, “プラットフォームにおけるデータ取扱いルールの実装ガイダンス ver1.0,” [オンライン]. Available: https://cio.go.jp/sites/default/files/uploads/documents/digital/20220304_policies_data_strategy_outline_01.pdf.
- [3] デジタル庁, “包括的データ戦略,” [オンライン]. Available: https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/63d84bdb-0a7d-479b-8cce-565ed146f03b/02063701/policies_data_strategy_outline_02.pdf.
- [4] 経済産業省, “AI・データの利用に関する契約ガイドライン 1.1 版,” [オンライン]. Available: <https://www.meti.go.jp/press/2019/12/20191209001/20191209001.html>.
- [5] 一般社団法人 データ流通推進協議会, “パーソナルデータリファレンスアーキテクチャ,” [オンライン]. Available: <https://www8.cao.go.jp/cstp/stmain/20200318siparchitecture.html>.
- [6] 一般社団法人 データ流通推進協議会, “データ取引市場運営事業者認定基準,” [オンライン]. Available: https://data-trading.org/wp-content/uploads/2020/11/Cert_DataTradingMarketRev20.pdf.
- [7] 総務省, “データ取引市場等 SWG 取りまとめ 概要,” [オンライン]. Available: https://www.soumu.go.jp/main_content/000501157.pdf.
- [8] 総務省, “情報信託機能の認定に係る指針 Ver2.1,” [オンライン]. Available: https://www.soumu.go.jp/main_content/000764120.pdf.
- [9] 日本産業標準調査会, “JIS 規格 X 9250:2017 (ISO/IEC 29100:2011),” [オンライン]. Available: <http://www.kikakurui.com/x9/X9250-2017-01.html>.
- [10] デジタル庁, “ゼロトラストアーキテクチャ 適用方針,” [オンライン]. Available: https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/5efa5c3b/20220630_resources_standard_guidelines_guidelines_04.pdf.
- [11] National Institute of Standards and Technology, “電子認証に関するガイドライン,” [オンライン]. Available: <https://www.ipa.go.jp/files/000025342.pdf>.
- [12] Cryptography Research and Evaluation Committees, “CRYPTREC 暗号リスト,” [オンライン]. Available: <https://www.cryptrec.go.jp/list.html>.
- [13] 情報処理推進機構, “TLS 暗号設定ガイドライン～安全なウェブサイトのために(暗号設定対策編)～,” [オンライン]. Available: https://www.ipa.go.jp/security/vuln/ssl_crypto_config.html.
- [14] “SIP 分野間データ連携基盤 概説 CADDE V4.0”.
- [15] “個人情報の保護に関する法律,” [オンライン]. Available: <https://elaws.e-gov.go.jp/document?lawid=415AC0000000057>.

-
- [16] B. Otto, M. t. Hompel, S. Wrobel, “Designing Data Spaces The Ecosystem Approach to Competitive Advantage,” [オンライン].
- [17] “行政手続におけるオンラインによる本人確認の手法に関するガイドライン”, [オンライン]. Available: https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/f1be078e/20220422_resources_standard_guidelines_guideline_07.pdf
- [18] OpenID ファウンデーション・ジャパン, “民間事業者向けデジタル本人確認ガイドライン”, [オンライン]. Available: https://www.openid.or.jp/news/kyc_guideline_v1.0.pdf
- [19] デジタルトラスト協議会(JDTF), “「e シール解説～実用化に向けて～バージョン 1.0」”, [オンライン]. Available: <https://jdtf.or.jp/report/whitepaper/file/e%E3%82%B7%E3%83%BC%E3%83%AB%E8%A7%A3%E8%AA%AC%28%E3%83%90%E3%83%BC%E3%82%B8%E3%83%A7%E3%83%B31.0%29.pdf>
- [20] Open Knowledge Foundation, “CKAN v.2.9.9, 24 May 2023”, [オンライン]. Available: <https://docs.ckan.org/en/2.9/>
- [21] International Open Forum on Data Society (IOFDS), [オンライン]. Available: <https://iofds.org/>

謝辞

本仕様の策定にあたり、トラストサービス連携に関し、一般社団法人デジタルトラスト協議会 (JDTF) に協力いただきました。この場を借りて御礼申し上げます。

2-2. 用語定義

本技術仕様書で用いられる用語の定義を示す。既出の定義などがある場合の用語に関しては外部参照先を括弧表記にて表記する。

- ・ データ
情報の表現であって、伝達、解釈又は処理に適するように形式化され、再度情報として解釈できるもの(ISO/IEC 2382-1, JIS X0001)
- ・ DSA/ Data Society Alliance
データ社会推進協議会
- ・ プラットフォーム
データ連携とそれを利活用したサービスを提供するための基盤(プラットフォームにおけるデータ取扱いルールの実装ガイダンス)
- ・ ステークホルダー
DATA-EX 内でデータ流通に関わる当事者。より具体的には DATA-EX 運営事業者、DATA-EX 参加者、DATA-EX 支援サービス提供者を指す
- ・ CADDE/Connector Architecture for decentralized Data Exchange
分散型データ交換のためのコネクタ・アーキテクチャ

-
- ・ Society 5.0
サイバー空間とフィジカル空間を高度に融合させたシステムによって、経済発展と社会課題の解決を両立する人間中心の社会(プラットフォームにおけるデータ取扱いルールの実装ガイダンス)
 - ・ SIP/Cross-ministerial Strategic Innovation Promotion Program
戦略的イノベーション創造プログラム。内閣府総合科学技術・イノベーション会議が司令塔機能を発揮して、府省の枠や旧来の分野を超えたマネジメントにより、科学技術イノベーション実現のために創設した国家プロジェクト
 - ・ IDSA/International Data Space Association
「すべての企業が自主的に利用ルールを決定し、安全で信頼できる対等なパートナーシップのもと、データの価値を最大限に高めることができる世界」というビジョンを共有する、欧州を拠点とする 130 社以上の企業による連合体
 - ・ GAIA-X
欧州での連邦型の欧州クラウド／データインフラ構想。認証や契約手続きに基づいてデータへのアクセスを制御し、データ主権を保護しつつ様々なクラウドサービスとの相互運用性を確保する技術的な仕組み
 - ・ Catena-X
2021 年に結成された自動車産業全体のサプライチェーンに関するデータを共有するデータエコシステム
 - ・ データ主権
データの利用権限。すなわち、データに適法にアクセスし、その利用をコントロールできる事実上の地位、または契約によってデータの利用権限を取り決めた場合にはそのような債権的な地位(AI・データの利用に関する契約ガイドライン)
 - ・ 分散連邦型
分野ごとに独立の複数システムが、共通のツールを介して分散データベース化したデータ基盤のこと
 - ・ コネクタ
データ交換のための仲介役として働くモジュール
 - ・ トラストサービス基盤
国内・海外のデータ提供者から入手した情報を本当にそのデータ提供者が作成したことを確認するために、データの発生元の統一的な確認手段やデータの統一的な改ざん検知の機能を有した基盤のこと
 - ・ データ提供者
データ受領を担当する DATA-EX 参加者へデータを提供する者
 - ・ データ受領者
データ提供を担当する DATA-EX 参加者からデータを受領する者
-

-
- ・ ガバナンス
ステークホルダーの懸念・不安をステークホルダーにとって受容可能な水準で管理しつつ、データ流通によってソリューションを創出するために、ポリシー、契約、推進体制を用いて行われる統治システム及びプロセス(プラットフォームにおけるデータ取扱いルールの実装ガイダンス)
 - ・ データセット
複数のデータで構成されるもの
 - ・ 付帯情報
データの属性を示すメタデータのこと。具体的には、データの作成者、作成日、更新日など
 - ・ 利用条件
データ交換に際して、契約時にデータ提供者がデータ受領者に定めるデータの利用条件のこと。具体的には秘密保持義務、利用用途、有償無償など
 - ・ DDP(Data Distribution Package)
データセット、データセットの付帯情報(作成者、作成日、更新日、サイズなどのメタデータ)、データ交換の契約条項(秘密保持義務、利用用途)などが一体となったパッケージである。DATA-EX におけるデータ交換はすべて DDP 単位で行われる。
 - ・ デバイス
ステークホルダーが DATA-EX に接続するために利用する、コネクタが実装されたサーバー・クライアントのこと
 - ・ 認可サーバー
データ提供者がデータ受領者のアクセス権限を制御し、トークンを発行やエンドポイント登録を行うサーバーのこと
 - ・ ストレージ
DATA-EX 参加者がデータセットおよびデータセットのデータを格納する記憶装置
データを格納し、保持し、かつ、取り出すことのできる機能単位(ISO/IEC 2382-1,JIS X0001)
 - ・ 契約
異なるエンティティ間において、意思表示が合致することによって成立する法律行為(ISO/IEC 2382-1,JIS X0001)
 - ・ カタログサイト
データカタログを管理するためのソフトウェアであり、データカタログ作成機能等によって作成されたカタログ情報を登録し、公開する機能を持つ。またカタログサイトは、データカタログ横断検索機能からクローリングされた場合、カタログ情報をデータカタログ横断検索機能に返す機能も持つ。カタログサイトの代表的な例としてオープンソースの CKAN が挙げられる。
-

-
- ・ クローリング
プログラムが検索データベース登録のため Web サイトの情報を収集すること
 - ・ IdP/Identity Provider
サービスにアクセス時にユーザーの認証情報を保存・管理するサービスのこと
 - ・ 認証
異なるエンティティにおいて、相手方の正当性を確認する行為(ISO/IEC 2382-1,JIS X0001)
 - ・ 認可
リソースへのアクセス権限を与える行為のこと
 - ・ 認証局
他の当事者に電子証明書を発行する実体(ISO/IEC 2382-1,JIS X0001)
 - ・ エンドポイント
特定のリソースに対して与えられた固有の一意な URI
 - ・ リソース
DATA-EX 上に識別可能な状態で登録されているハードウェア・ソフトウェア・データのこと。より具体的にはアカウント、デバイス、サービス、DDP を指す
 - ・ 所有情報
要素認証において、DATA-EX 参加者が所有するものに付随する情報のこと。携帯電話やセキュリティトークンなどが該当する
 - ・ 生体情報
要素認証において、DATA-EX 参加者の身体的あるいは行動的特徴の情報。顔や指紋などが該当する
 - ・ 脆弱性
ハードウェア・ソフトウェアなどにおいて、設計上のミスやプログラムの不具合からなるセキュリティ上の欠陥のこと
 - ・ アクセス制御ポリシー
リソースへのアクセスを許可するかの一連の条件のこと
 - ・ 被観測者
データが表現する対象となる者(プラットフォームにおけるデータ取扱いルールの実装ガイドダンス)
 - ・ 個人情報
生存する個人に関する情報 生存する特定の個人を識別できる情報・個人識別符号が含まれるもの・他の情報と容易に照合でき、その結果、特定個人を識別できることとなる 情報も含む(個人情報の保護に関する法律)
 - ・ コントローラビリティ
明示された目的及びデータ取扱い方針の範囲内でデータが利用されるよう、又は明示さ
-

れた目的及びデータ取扱い方針の範囲外でデータが利用されないよう、当該データの被観測者やデータ提供者が当該データの取扱いに直接的又は間接的に関与可能なこと(プラットフォームにおけるデータ取扱いルールの実装ガイダンス)

- ・ データ取引市場

データ保有者と当該データの活用を希望する者を仲介し、売買等による取引を可能とする仕組みのこと(データ取引市場等SWG取りまとめ 概要)

3. 構築の背景と目的

3-1. 背景

近年、日本政府が主導する Society 5.0 によるデータ利活用の提唱により、国、地方公共団体、民間企業などで分散して保有するデータを連携して、施策立案や新たなサービス、ビジネスの創出などを通じた民間企業の競争力強化や行政サービスの高度化が求められてきた。政府が令和 3 年(2021 年)6 月に策定した包括的データ戦略では“信頼と公益性の確保を通じてデータを安心して効率的に使える仕組みを構築するとともに、世界からも我が国のデータそのものやその生成・流通の在り方に対する信頼を確保し、世界で我が国のデータを安心して活用でき、また、世界のデータを我が国に安心して預けてもらえるような社会”の理念のもと以下のデータ活用原則が示された。

- ①データがつながり、いつでも使える
- ②データを勝手に使われない、安心して使える
- ③新たな価値の創出のためみんなで協力する

これらを実現するためには、幅広いデータを集約、分析し、新たな視点や提言を包括的・効率的・一元的に実現できるような基盤(プラットフォーム)が求められる。データ連携の基盤の構築は包括的データ戦略において重要戦略として取り上げられており、実際に戦略的イノベーション創造プログラム(SIP)事業において分野間データ連携基盤技術の構築が開始され、データ連携を目指すプラットフォームとして DATA-EX が提供されることとなった。

一方で、国際的なデータ流通の仕組みやルール整備に向けた取り組みが、欧州で先行する形で加速化している。これらの代表的な組織・枠組みとして IDSA (International Data Space)や GAIA-X、Catena-X が挙げられる。欧州ではデータ主権を軸足としたデータ共有のルール策定や分散型のデータ共有の実現を目的としつつ、その裏付けとなるソリューション開発やその準備を行っている。また、すでに産業を超えたデータの連携だけでなく、スマートシティをはじめ都市・社会など範囲が幅広くなったことにより、データ連携の主体の多様化が進展している。

日本でのデータ連携は、産業分野内で自社や限定的な企業内でデータを囲い込む傾向があり、行政サービス組織間でもデータの連携に課題が見られた。これらの課題を解決し、日本におけるデータ共有を推進する機構として、「データ社会推進協議会(Data Society Alliance: DSA)」が設立され、分野間のデータ連携基盤の構築が急務となっている。

分野を超えたデータ連携を試みる際に、様々な課題が生じる。多様な分野内でのデータ連携基盤がある市場で、それらの基盤を分野間で接続する仕組みを取り入れる場合、各分野のデータ連携基盤のセキュリティを保つ為に、最新のセキュリティのベストプラクティスを第三者が管理する必要がある。また、現状のデータ流通市場において、データ連携を支援するサービスやデータのマネタイゼーションの推進を目的とするビジネスモデルが様々ある中で、それらの仕様には違いがある為、第三者が一定の水準を明確にする事によりサービスの統合を試みる必要性があった。

3-2. 構築目的と原則

DATA-EX では「3-1. 背景」で記載した通り、どの分野・データ種別をどの企業・大学・国からでもアクセスできる安全・安心なデータ連携をする為のセキュリティを担保しつつ、既に市場にあるデータ連携基盤の整合性を構築する為のアーキテクチャを設計することが課題となる。その他、分野ごとの語彙を定義できるサービスやデータカタログを検索できるサービス等、データの発見と交換を効率よく行う為のサービスやツールを備えた基盤を構築することも課題である。

これらの課題に対して、DATA-EX は DATA-EX 参加者、DATA-EX 運営事業者、その他ステークホルダーに円滑・安全な情報共有・連携を図ることを目的とする。分野ごとの既存のデータ連携基盤(例えば、農業データ連携基盤(WAGRI)や基盤的防災情報流通ネットワーク(SIP4D)等)を尊重するために、DATA-EX は集中型のデータ基盤を持たず、連邦型のアーキテクチャを採用し、参加者自身が機能の一部やデータ管理、ガバナンス運営を担う。外部 IdP による利用者認証、認証局、e シール、電子署名、タイムスタンプなどのトラストサービス基盤との連携仕様については、「12. セキュリティ・トラスト」を参照すること。また、DATA-EX には IDSA や GAIA-X 等との国際連携も可能な信頼性のある基盤であることが求められるため、国際的なデータ流通との接続について検証を進めていく。国際的な連携に関して、検討の詳細は「14. 国際連携」を参照すること。DATA-EX は、分野を超えた安全、安心なデータ連携を実現する為に、データ連携に係る既存の取り組みが協調したプラットフォームとして産官学、業界、組織を問わず、広く利用者に提供されることを想定している。

DATA-EX は上記を実現することを目的とし、以下の原則をもとに構築を行っている。

- ・ 分野毎のデータ基盤を繋ぎデータ流通を促進する分散連邦型アーキテクチャ
- ・ 既存技術を活用した設計
- ・ オープンデータからビジネスデータまで対応可能な、汎用性の高い機能別階層構成
- ・ データ生成から発見、契約、交換、来歴管理までデータ利用の様々な段階での支援を行う多様なサービスの提供
- ・ 国際的なデータ流通基盤との連携
- ・ トラストサービス基盤との連携
- ・ 導入が容易なシンプルなアーキテクチャ

3-3. 概念モデル

DATA-EX では、データ提供者とデータ受領者は DDP(Data Distribution Package の略称。データセット、データセットの付帯情報、データ交換の契約条項などが一体となったパッケージ)単位でデータ交換を行う。データ交換に必要な環境や機能は、分野間データ連携サービスによって提供される。DATA-EX では、分野間データ連携サービスの他に、来歴管理サービス、ポータルサービス、データカタログ横断検索サービス、データカタログ作成サービス、語彙管理サービス、データ取引市場サービスを提供する。特に、分野間データ連携サービス・来歴管理サービス・ポータル

サービスの3つを主要サービスと呼び、データカタログ横断検索サービス・データカタログ作成サービス・語彙管理サービス・データ取引市場サービスの4つを支援サービスと呼ぶ。

DATA-EXにおける分野間データ連携に直接的・間接的に係る組織または個人をステークホルダーという。DATA-EXには主に3つのステークホルダーが存在する。1つ目はDATA-EX運営事業者である。DATA-EX運営事業者は、データ交換に係る主要サービスを提供するステークホルダーである。2つ目はDATA-EX支援サービス提供者である。DATA-EX支援サービス提供者は、DATA-EXの中で支援サービスを提供するステークホルダーである。3つ目はDATA-EX参加者である。DATA-EX参加者は、DATA-EXにアクセスしてデータ交換を行うステークホルダーである。データ提供者とデータ受領者はDATA-EX参加者の一部であり、データ提供者たるDATA-EX参加者がデータ受領者たるDATA-EX参加者にデータを提供する。なお、分野間データ連携サービスの一部機能については、DATA-EX参加者自身が用意する必要がある。具体的な機能については本仕様書「7. DATA-EX 構成要素」を参照。

以上を踏まえて、DATA-EXの概念モデルを図2に示す。

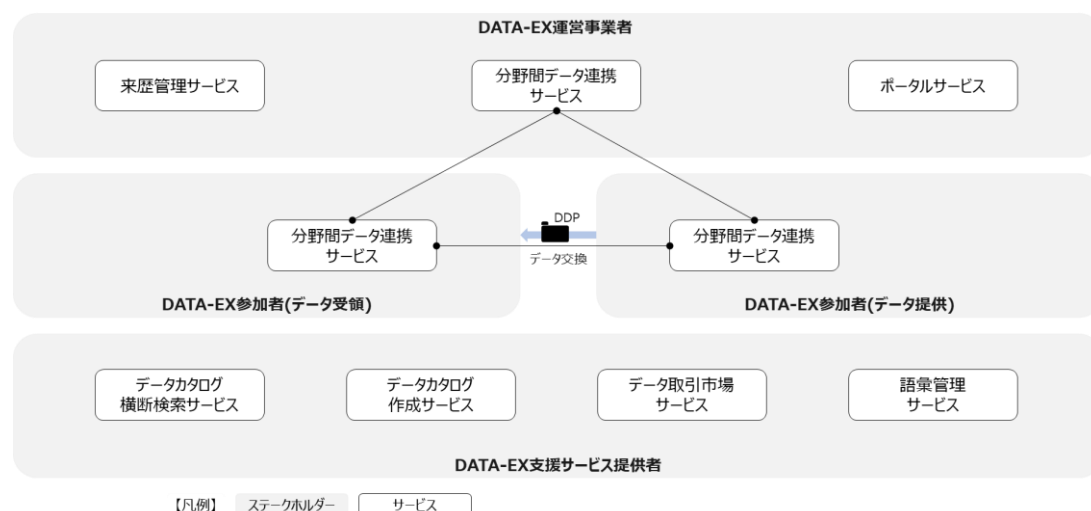


図 2: DATA-EX 概念モデル

DATA-EXは、異なる分野及び産業間において、安心・安全なデータ連携を可能にするプラットフォームである。DATA-EXのサービスを提供するに当たって必要な真正性や完全性を保証するために、トラストサービス基盤と連携し各種トラストサービスを使うものとする。

各層の定義を以下に示す。

- ・ アプリケーション層とは、データ連携基盤を利用するアプリケーションのレイヤーである。
- ・ データ連携基盤層とは、分野ごとのデータ連携基盤をつなぎ、安心・安全なデータ流通が実現されるレイヤーである。
- ・ トラストサービス層とは、DATA-EXに接続する人・組織・モノの正当性の確認や交換されるデータの完全性を確保する観点から、DATA-EX参加者の真正性を確認するための利用者認証、データ発生元を証明するeシール、意思表示のための電子署名や署

名検証、データの存在を証明するタイムスタンプ等のトラストサービスが提供されるレイヤーである。

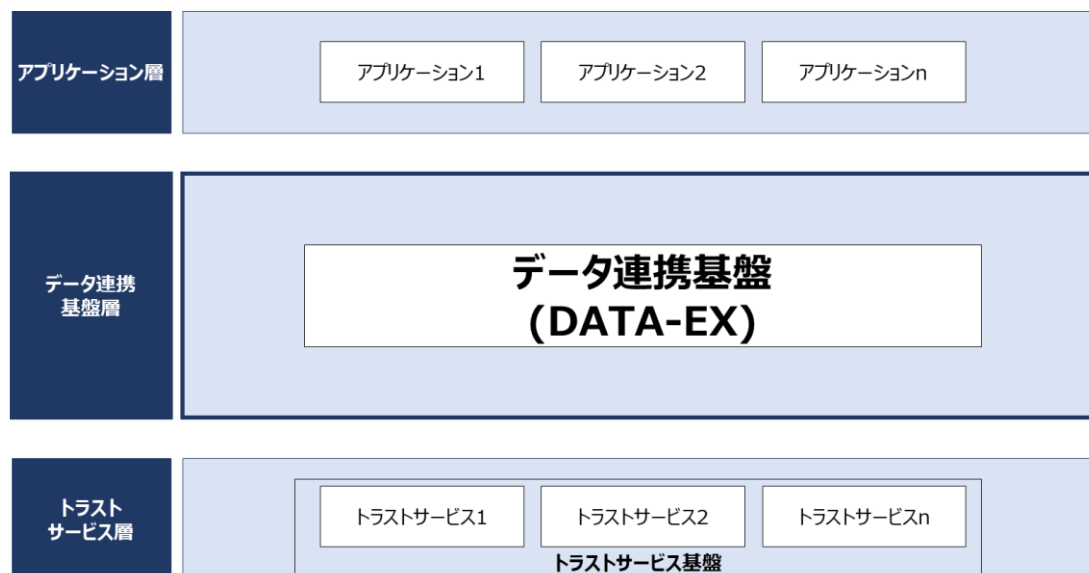


図 3: DATA-EX を利用した安全・安心なデータ連携の概念モデル

3-4. 利用メリット

DATA-EX を利用することで、以下のメリットを享受することができる。

一つ目は、DATA-EX ではサービス利用申請時に身分証明がなされているため、データ利用者にとってデータ交換時に相手先の真正性が担保された形でのデータ交換が可能となり、自身での相手先の確認が不要となることである。

二つ目は、分野をまたいだデータ公開により、データ利用者にとっても異なる分野/組織のデータが見つけやすくなることである。

三つ目は、データ利用時のコストが低減することである。DATA-EX ではデータ提供の型が決まっているため、データ交換に必要な調整が軽減する。また、コネクタを介してデータ交換を実施することで、データベースへのアクセスの手間が低減する。

最後に、国際的なデータ流通に対しても、DATA-EX によるデータ連携を実現することができれば、国際間でのデータ連携仕様に関する調整も不要となることがメリットとして挙げられる。検討中の実現方法については「14. 国際連携」にて説明する。

3-5. 想定ユースケース

分野間データ連携ニーズがあると考えられるユースケース例を以下に示す。

- ・ 国全体の災害対応力の最大化

機関・組織間で災害の状況認識を統一された的確な災害対応(被害把握・人命救助、避難所対応・物資対応)を行うために、災害対応情報提供事業者が被災自治体におけ

る災害対応に携わる機関・組織に災害対応に必要とされる情報(気象情報・病院情報・道路情報・避難所情報・車両通行実績など)を提供する。DATA-EX を利用することで、一度連携機能を開発すれば、DATA-EX 参加者すべてに対して連携機能が流用できるため、連携相手ごとに連携機能を開発する必要がなくなる。

- ・ ゼロカーボンシティ施策推進

地方自治体ごとに EV 公用車の稼働管理効率化やガソリン車と比較した CO2 削減量の可視化を行うために、モビリティ事業者発電事業者がモビリティ事業者や発電事業者に EV データ・GPS データ・エネルギーデータを提供。連携相手が DATA-EX に参加している場合、DATA-EX を利用することで、連携相手ごとに連携機能を開発する必要がなくなるため、迅速に基盤を構築できる。

- ・ 化学品の流通における安全な製品含有化学物質の管理

製品仕様の変更や関連法令変更に伴う化学品文書の流通管理を行うために、化学品製造者が化学品流通事業者へ最終製品の化学組成情報・製品含有化学物質情報などを提供し、化学品流通事業者も収集した情報の維持管理や製造工程における化学物質の変化・含有量の把握を行い、化学品使用者にそれらの化学物質の情報を提供する。DATA-EX を利用することで、情報がどこで発生し、どのように流通しているのかを追跡可能となるため、サプライチェーン全体を通じた化学物質管理の信頼性を向上できる。

- ・ モビリティ分野におけるシェアリングエコノミの促進

利用者ニーズに基づいた自動車の配置や駐車場の有効活用を行うためにカーシェアリングサービス事業者が管理するサービス利用状況やサービス利用者の要望と、駐車場経営者が持つ駐車場利用状況を相互に交換する。信頼関係を持たない連携相手が DATA-EX に参加している場合、DATA-EX を利用することで、連携相手との信頼関係を一から構築する必要がなくなる。

DATA-EX を活用することで、個別の分野間データ連携基盤の構築やデータ連携のための個別開発を抑制できると考える。

4. 提供サービス

DATA-EX 提供サービスとは、DATA-EX の分野間データ連携基盤の目的を果たす為に DATA-EX 参加者に提供するサービス群である。主に、分野間データ連携サービス、来歴管理のサービス、ポータルサービスなどがある。

DATA-EX は 24 時間 365 日稼働するプラットフォームである。DATA-EX 運営事業者は障害が発生した場合でもデータが消失しないように環境構成を維持し、可用性を担保する。性能面では、データ授受における認証やコネクタロケーション解決の際に適切なレスポンスを提供する。拡張性については、サービスを柔軟に拡張できる仕組みを採用する。また、DATA-EX 運営事業者は DATA-EX 運用時に主要サービスに関する問い合わせ窓口を担当する。ただし、DATA-EX 参加者間でやり取りされるデータや契約に関する問い合わせは受け付けない。以上を踏まえて、DATA-EX 運営事業者は提供するサービスの内容と品質について資料「サービスレベル保証書」に記載し、その基準に従ってサービスを提供する。

DATA-EX 支援サービス提供者や DATA-EX 参加者も、自身のデバイスの構成やコネクタとその環境に関して管理を行い、単一障害点対策等の責任を持つ。また、DATA-EX 支援サービス提供者と DATA-EX 参加者は各々の基準に従ってサービスを提供する。

4-1. 主要サービス

主要サービスとは、DATA-EX の分野間データ連携を実現するために DATA-EX 参加者に提供する必須のサービス群である。主に DATA-EX 運営事業者が主要サービスを提供するが、DATA-EX 運営事業者以外の事業者が主要サービスの一部を提供することもある。

4-1-1. 分野間データ連携サービス

分野間データ連携サービスは、DATA-EX 運営事業者が DATA-EX 参加者にデータ連携を行う為に必須な環境、機能を提供するサービスである。

DATA-EX 参加者は、DATA-EX 参加者同士でデータ授受を行うために、コネクタを介して分野間データ連携サービスを利用する。一部の機能については、DATA-EX 参加者自身が用意する必要がある。具体的な機能については本仕様書「7. DATA-EX 構成要素」を参照。

4-1-2. 来歴管理サービス

来歴管理サービスは、DATA-EX を介して行われる DATA-EX 参加者間でのデータ連携にて收受されたデータの收受・供与の来歴を記録管理し、DATA-EX 参加者の要望に応じてその来歴を提供するサービスである。

データ交換の来歴は提供ログと受領ログが揃って意味を成すものである。したがって、DATA-EX 参加者は、自身のデータ作成履歴、データ送信履歴及び受信履歴を登録・確認するために、来歴管理サービスを利用することが望ましい。

4-1-3. ポータルサービス

ポータルサービスは、DATA-EX に関連するサービス群の一覧とそのエンドポイントを掲載したポータルサイトを Web 上で一般公開し、DATA-EX のモニタリングダッシュボード等を公開するとともに、コネクタのバージョンを管理し、DATA-EX 参加者にコネクタを公開するサービスである。

DATA-EX 参加者は、DATA-EX 提供サービスの接続先の確認や DATA-EX に接続するコネクタのモジュールを取得するために、ポータルサービスを利用する。

4-2. 支援サービス

支援サービスとは、効率的・効果的に主要サービスを利用するために DATA-EX 参加者に提供するサービス群である。主に DATA-EX 運営事業者以外の認定事業者が支援サービスを提供する。

DATA-EX 参加者は、DATA-EX 支援サービス提供者に自らの DATA-EX ID を共有し、支援サービスの利用登録を行うことで、支援サービスの利用を開始することができる。また、支援サービスの接続先は DATA-EX のポータルサイトにて公開する。

4-2-1. データカタログ横断検索サービス

データカタログ横断検索サービスは、DATA-EX 支援サービス提供者が DATA-EX 参加者に、DATA-EX において利用可能なカタログを包括的・横断的に検索・発見できるツールを提供するサービスである。

データカタログ横断検索サービスを管理する DATA-EX 支援サービス提供事業者は、カタログの登録基準を明確にし、カタログ公開サイトを適切に審査した上でカタログデータ収集先として登録する。

DATA-EX 参加者（データ提供）は、自身または自組織が保有するデータのカタログを公開するために、データカタログ横断検索サービスにカタログを登録することが望ましい。また、DATA-EX 参加者（データ受領）は、自身が必要とするデータを探し、そのデータに関連する情報を収集するために、データカタログ横断検索サービスを利用してカタログを検索することが望ましい。

4-2-2. データカタログ作成サービス

データカタログ作成サービスは、DATA-EX 支援サービス提供者が DATA-EX 参加者に、カタログの作成・登録を支援する為のデータカタログ作成ツール等を提供するサービスである。

DATA-EX 参加者（データ提供）は、DATA-EX データカタログ項目仕様に準拠したカタログを容易に作成・登録するために、データカタログ作成サービスを利用することが望ましい。DATA-EX データカタログ項目仕様とは、データカタログ項目の国際標準である DCAT 仕様をベースとして、データ流通の観点から利用条件やコネクタ制御項目を拡張し

たものである。詳細は、「DATA-EX データカタログ項目仕様」（今後作成予定）を参照すること。

4-2-3. 語彙管理サービス

語彙管理サービスは、DATA-EX 支援サービス提供者が DATA-EX 参加者に、データの相互運用性を高める為に、提供・受領されるデータに含まれる語彙を作成するツールと、語彙を登録・公開・検索する語彙リポジトリを提供するサービスである。

DATA-EX 参加者（データ提供）は、自身の提供データに含まれる語彙の情報を整理し、他人と共有するために、語彙管理サービスを利用することが望ましい。

4-2-4. データ取引市場サービス

データ取引市場サービスは、DATA-EX 支援サービス提供者が、DATA-EX 参加者の契約に基づくデータの提供と便益の交換を支援、管理するサービスである。

DATA-EX 参加者は、第三者による保証を必要とする契約を締結するために、データ取引市場サービスを利用することが望ましい。

5. 連携サービス

連携サービスとは、DATA-EX 提供サービスと相互運用して連携するサービス群である。
DATA-EX 運営事業者とは異なる独立した事業者が連携サービスを提供する。

5-1. トラストサービス

トラストサービスとは、トラストサービス基盤のサービス事業者及び信頼できる Identity Provider(IdP)が DATA-EX 参加者に提供するサービス群であり、DATA-EX に接続する人・組織・モノの正当性の確認や交換されるデータの完全性を確保する観点から、DATA-EX 参加者の真正性を確認するための身元確認、利用者認証、データの完全性および発行元を証明する e シール、意思表示のための電子署名、ある時刻でのデータの存在を証明するタイムスタンプ等のトラストサービスを提供する。

5-1-1. 外部 IdP

外部 IdP は、DATA-EX 参加者が契約し、DATA-EX への参加、認証時に使用する IdP である。一定の基準により利用者の身元確認、ユーザー管理、認証を行う機能を有する。DATA-EX 参加者の身元を保証し、DATA-EX の代理で参加者の認証を行い、認証結果の情報を DATA-EX 分野間データ連携サービス、データ取引市場サービス等に提供する。

5-1-2. e シールサービス

e シールサービスは、トラストアンカーにより保証される DATA-EX 参加者の組織に対する電子証明書を利用して、対象となるデータの作成者または送信者の真正性およびデータの完全性を保証する e シールを生成、提供するサービスである。

5-1-3. 電子署名サービス

電子署名サービスは、トラストアンカーにより保証される DATA-EX 参加者の組織を代表する個人に対する電子証明書を利用して、対象となるデータの作成者の真正性およびデータの完全性を保証する電子署名を生成、提供するサービスである。主に、契約時に契約者の意思表示として利用される。

5-1-4. タイムスタンプサービス

タイムスタンプサービスは、ある時刻にそのデータが存在していたことおよびそれ以降改ざんされていないことを証明するタイムスタンプを生成、提供するサービスである。

5-2. 来歴管理拡張サービス

来歴管理拡張サービスは、DATA-EX 参加者間でのデータ連携にて収受された DDP に含まれるデータセットの収受・供与および作成・加工等の来歴を記録管理し、DATA-EX 参加者の要望に応じてその来歴を提供するサービスである。

6. 参加方法

DATA-EX に参加したい組織・人は、DATA-EX 運営事業者が定める方法で申請をする必要がある。組織で参加する場合、最低 1 名の組織アカウント管理者を設定する。また、参加時は DATA-EX の利用規約やポリシーを遵守することが前提となる。たとえば日本国外から参加する場合、DATA-EX 参加者は DATA-EX の利用規約に準じ、その地域において守るべき法律を遵守しなければならない。DATA-EX 運営事業者は、申請内容をもとに参加者の真正性等を確認し、参加の可否を判断する。組織・人の参加に制限を設ける場合、DATA-EX 運営事業者はその基準を公表する。

DATA-EX 運営事業者から参加が認められた場合、DATA-EX アカウントが参加者へと払い出される。参加後の DATA-EX のサービス利用の流れは以下の通りである。

まず、DATA-EX 参加者は利用を開始するために、DATA-EX 運営事業者に DATA-EX 利用申請を行う。申請が認められると DATA-EX 参加者へ利用に必要な設定情報(DATA-EX アカウントやコネクタ設定)が提供される。DATA-EX 参加者はコネクタ構築に必要な環境を準備する。構築の完了後、DATA-EX 参加者はコネクタを介して DATA-EX への接続確認を行い、データ交換を行うことが可能となる。なお、提供するデータは提供者側の環境で保持しデータの管理は DATA-EX 参加者自身が行う。

具体的な参加基準、及び参加手順は資料「DATA-EX 利用解説書」（今後作成予定）を参照すること。

7. DATA-EX 構成要素

図 4 に示すように、DATA-EX を構成する要素は「ステークホルダー」、「機能」、「ID」、「オブジェクト」である。ステークホルダーはデータ連携における主体であり、オブジェクトは DATA-EX の分野間データ連携を行う為に、ステークホルダーによってやり取りされる情報群である。データ連携は複数の機能が組み合わせられて構成され、識別が必要な要素に対して DATA-EX 内外で固有の ID が発行及び利用される。



図 4: DATA-EX 構成要素

7-1. ステークホルダー

DATA-EX の分野間データ連携を行う為に、直接的・間接的に係る組織又は個人をステークホルダーと定義する。

7-1-1. 主要ステークホルダー

主要ステークホルダーとは、主要サービスに直接的な係わりを持つ組織又は個人である。分野を超えたデータ連携を行う DATA-EX 参加者と主要サービスを提供する DATA-EX 運営事業者が含まれる。

7-1-1-1. DATA-EX 参加者

DATA-EX にアクセスをし、DATA-EX の機能を通してデータ交換を行うステークホルダーである。DATA-EX 参加者はデータ交換のプロセスの中で様々な役割が存在する。

- ・ データ生成
データを生成する役割。
- ・ データ提供
データ受領を担当する DATA-EX 参加者へデータを提供する役割。
- ・ データ受領
データ提供を担当する DATA-EX 参加者からデータを受領する役割。

-
- ・ データ利用

受領したデータを利用する役割。

- ・ データ加工

データを加工（例：特に機密性の高い情報の匿名化）する役割。

7-1-1-2. DATA-EX 運営事業者

DATA-EX を運営し、DATE-EX 参加者に、各種 ID の管理、コネクタの提供・管理、DATA-EX の運営が適正に行われているかを監督するといった、DATA-EX のサービス全体の提供を行うステークホルダーである。

- ・ システム開発・構築

DATA-EX 参加者に提供するコネクタを用いたデータ連携を行うために必要なシステムを開発する役割。

- ・ システム運用・保守

分野間データ連携サービスを安定的に稼働させる役割。

- ・ 業務運用

DATA-EX 参加者のユーザー管理、コネクタの提供等を実施する役割。

- ・ 内部監査

DATA-EX におけるプロセス・ルールの策定・監視を行う役割。

- ・ 啓蒙

DATA-EX のマーケティング、教育、アウトリーチ等をする役割。

- ・ 報告

DATA-EX の活動状況等を政府に報告する役割。

7-1-2. 支援ステークホルダー

支援ステークホルダーとは、支援サービスを提供する組織又は個人である。

7-1-2-1. DATA-EX 支援サービス提供者

DATA-EX 参加者に対して、DATA-EX 支援サービスの提供を行うステークホルダーである。また、DATA-EX 支援サービス提供者は DATA-EX 運営事業者が認定した事業者である。DATA-EX 支援サービス提供者は複数のサービスごとに様々な役割をもつ。

- ・ データカタログ横断検索

DATA-EX において利用可能なカタログを包括的に・横断的に検索・発見できる機能を提供する役割。

- ・ データカタログ作成支援

データ提供を担当する DATA-EX 参加者によるカタログの作成・登録を支援する為のデータカタログ作成ツール等を提供する役割。

- ・ データ取引市場

契約にもとづきデータの提供と便益の交換をする為に必要な機能を提供する役割。

- ・ 語彙管理

DATA-EX を介して、提供・受領されるデータに含まれる語彙リポジトリと、登録に関するツールを提供する役割。

7-1-3. 連携ステークホルダー

連携ステークホルダーとは、連携サービスを提供する組織又は個人である。

7-1-3-1. 連携サービス提供者

DATA-EX の主要ステークホルダーおよび支援ステークホルダーに対して、連携サービスの提供を行うステークホルダーである。

7-2. オブジェクト

DATA-EX の分野間データ連携を行う為に、DATA-EX ステークホルダーによってやり取りされる情報群である。

7-2-1. アカウント情報

アカウント情報は、DATA-EX ID と DATA-EX 参加者の属性をまとめたオブジェクトである。アカウントは DATA-EX ID を有する。個人は、複数のアカウントを所有する場合がある。DATA-EX 参加者が組織に属する場合、アカウントの所属属性に所属する DATA-EX 参加組織を示す DATA-

EX ID を含むこととする。主に、利用申請時やデータ授受時(認証)に DATA-EX 参加者と DATA-EX 運営事業者の間でやり取りが行われる。

7-2-2. 認証情報

認証情報は、リクエスト元である DATA-EX 参加者の身元を確認するためのオブジェクトである。認証情報は DATA-EX ID を有する。主にデータ授受時に DATA-EX 参加者と DATA-EX 運営事業者の間、または DATA-EX 参加者同士でやり取りが行われる。

7-2-3. 認可情報

認可情報は、リクエスト元である DATA-EX 参加者に DDP を受領する権限があることを確認するためのオブジェクトである。認可情報は DATA-EX ID、DDP ID を有する。主に、データ授受時に DATA-EX 参加者内でやり取りが行われる。

7-2-4. コネクタ設定情報

コネクタ設定情報は、DATA-EX 参加者が保有するコネクタを管理する為に必要なオブジェクトである。コネクタ設定情報はコネクタ ID を有する。主に、利用申請時に DATA-EX 参加者と DATA-EX 運営事業者の間でやり取りが行われる。

7-2-5. 証明書情報

証明書情報は、DATA-EX 参加者が持つコネクタの真正性を証明する為の電子証明書を登録する為に必要なオブジェクトである。証明書情報はコネクタ ID を有する。コネクタを介する通信では必ずやり取りが行われる。

7-2-6. コネクタロケーション情報

コネクタロケーション情報は、DATA-EX 上で提供されるコネクタの所在を解決する為に必要なオブジェクトである。コネクタロケーション情報はコネクタ ID を有する。コネクタロケーション情報は具体的にはエンドポイントを意味している。主に、データ授受時に DATA-EX 参加者と DATA-EX 運営事業者の間でやり取りが行われる。

7-2-7. DDP ロケーション情報

DDP ロケーション情報は、DATA-EX 上で提供される DDP の所在を解決する為に必要なオブジェクトである。DDP ロケーション情報は DDP ID を有する。DDP ロケーション情報は具体的にはエンドポイントを意味している。主に、データ授受時に DATA-EX 参加者内でやり取りが行われる。

7-2-8. 来歴情報

来歴情報は、DDP に関する作成、送受信、削除の一連のイベントを時系列順に記録するオブジェクトである。来歴情報は、特定の DDP に関する複数の履歴情報から構成される。主に、来歴確認時に DATA-EX 参加者と DATA-EX 運営事業者の間でやり取りが行われる。

(参考) 来歴情報の論理形式は、拡張 BNF 記法を使用すると、下記のように表される。

〈来歴情報〉 ::= 〈履歴情報〉+

7-2-9. 履歴情報

履歴情報は、DDP に関する作成、送受信、削除の各イベントを記録管理する為に必要なオブジェクトである。履歴情報は履歴 ID を有する。属性として、履歴の種類、送信者の DATA-EX ID、受信者の DATA-EX ID、DDP ID、DDP のハッシュ値、履歴が生じた日時、1 つ前の履歴情報の履歴 ID を持つ。主に、履歴登録時に DATA-EX 参加者と DATA-EX 運営事業者の間でやり取りが行われる。

- ・ 履歴情報は、履歴 ID、属性、履歴登録者を特定可能な情報、アクセス制御ポリシーから構成されるデータである。ただし、アクセス制御ポリシーは付与しなくてもよい。
 - 属性は、共通属性と、DDP 作成、DDP 送信、DDP 受信、DDP 削除のいずれかの属性から構成される。
 - ◇ 共通属性は、履歴の種類、DDP ID、履歴が生じた日時から構成される。
 - ◇ 履歴の種類は、DDP 作成、DDP 送信、DDP 受信、DDP 削除のいずれかを示す値である。
 - ◇ 履歴が生じた日時は、履歴情報が登録された日時を示す値である。
 - ◇ DDP 作成の属性は、DDP のハッシュ値、送信者の DATA-EX ID、受信者の DATA-EX ID から構成される。ただし、受信者の DATA-EX ID は付与しなくてもよい。
 - ◇ DDP 送信の属性は、送信者の DATA-EX ID、受信者の DATA-EX ID、1 つ前の履歴情報の履歴 ID から構成される。
 - ◇ DDP 受信の属性は、送信者の DATA-EX ID、受信者の DATA-EX ID、1 つ前の履歴情報の履歴 ID から構成される。
 - ◇ DDP 削除の属性は、送信者の DATA-EX ID、受信者の DATA-EX ID、1 つ前の履歴情報の履歴 ID から構成される。ただし、受信者の DATA-EX ID は付与しなくてもよい。
 - 履歴登録者を特定可能な情報は、履歴登録者の DATA-EX ID、履歴情報の電子署名から構成される。

-
- ◇ 履歴情報の電子署名は、履歴情報の一部の属性値に対する履歴登録者による電子署名を JWT (JSON Web Token : RFC7519) や JWS (JSON Web Signature : RFC7515)等により文字列表記したものである。
 - アクセス制御ポリシーは、1 つ以上のポリシー設定対象とポリシー設定対象の閲覧を許可するステークホルダーの組から構成される。
 - ◇ ポリシー設定対象は、履歴情報の構成要素の中でアクセス制御ポリシーを設定する対象を示す値である。例として、特定の属性や、履歴登録者を特定可能な情報などを指定できる。
 - ◇ ポリシー設定対象の閲覧を許可するステークホルダーは、ポリシー設定対象で示した対象の閲覧を許可するステークホルダーを示す値である。例として、対象 DDP のいずれかの授受に関わる参加者、対象履歴の送受信者などを指定できる。

(参考) 履歴情報の論理形式は、拡張 BNF 記法を使用すると、下記のように表される。

<履歴情報> ::= <履歴 ID> <属性> <履歴登録者を特定可能な情報> [<アクセス制御ポリシー>]
<履歴 ID> ::= 履歴 ID
<属性> ::= <共通属性> (<DDP 作成の属性> | <DDP 送信の属性> | <DDP 受信の属性> | <DDP 削除の属性>)
<共通属性> ::= <履歴の種類> <DDP ID> <履歴が生じた日時>
<DDP 作成の属性> ::= <DDP のハッシュ値> <送信者の DATA-EX ID> [<受信者の DATA-EX ID>]
<DDP 送信の属性> ::= <送信者の DATA-EX ID> <受信者の DATA-EX ID> <1 つ前の履歴情報の履歴 ID>
<DDP 受信の属性> ::= <送信者の DATA-EX ID> <受信者の DATA-EX ID> <1 つ前の履歴情報の履歴 ID>
<DDP 削除の属性> ::= <送信者の DATA-EX ID> [<受信者の DATA-EX ID>] <1 つ前の履歴情報の履歴 ID>
<履歴の種類> ::= ? DDP 作成、DDP 送信、DDP 受信、DDP 削除のいずれかを示す値 ?
<送信者の DATA-EX ID> ::= DATA-EX ID
<受信者の DATA-EX ID> ::= DATA-EX ID
<DDP ID> ::= DDP ID
<DDP のハッシュ値> ::= ? ハッシュ関数で計算された DDP のハッシュ値 ?
<履歴が生じた日時> ::= ? 履歴情報が登録された日時を示す値 ?
<1 つ前の履歴情報の履歴 ID> ::= 履歴 ID
<履歴登録者を特定可能な情報> ::= <履歴登録者の DATA-EX ID> <履歴情報の電子署名>

〈履歴登録者の DATA-EX ID〉 ::= DATA-EX ID
〈履歴情報の電子署名〉 ::= ? 履歴情報の一部に対する履歴登録者による電子署名 ?
〈アクセス制御ポリシー〉 ::= (〈ポリシー設定対象〉 〈ポリシー設定対象の閲覧を許可するステークホルダー〉)+
〈ポリシー設定対象〉 ::= ? 閲覧権の設定対象を示す値 ?
〈ポリシー設定対象の閲覧を許可するステークホルダー〉 ::= ? 〈ポリシー設定対象〉で示した対象の閲覧を許可するステークホルダーを示す値 ?

7-2-10. 加工来歴情報

加工来歴情報は、DDP に含まれるデータセットの入手元情報、加工内容の一連の履歴を時系列順に記録するオブジェクトである。加工来歴情報は、特定の DDP に関する 1 つ以上の加工履歴情報から構成される。主に、来歴確認時に DATA-EX 参加者と連携サービス提供者の間でやり取りが行われる。

7-2-11. 加工履歴情報

加工履歴情報は、DDP に含まれるデータセットの入手元情報、加工内容を記録管理する為に必要なオブジェクトである。属性として、データセット加工後の DDP ID、加工後の DDP 作成時の履歴 ID、データセット取得元の DDP ID、データセット取得元の DDP 受信時の履歴 ID、加工者の DATA-EX ID、履歴登録者を特定可能な情報、履歴が生じた日時、加工種別、加工詳細情報を持つ。加工前のデータセットを複数の DDP から取得した場合には、データセット取得元の DDP ID 及び DDP 受信時の履歴 ID は複数記録される。履歴登録者を特定可能な情報は、履歴登録者の DATA-EX ID と加工履歴情報の電子署名を有する。加工詳細情報は、加工詳細参照情報を持つことができる。主に、履歴登録時に DATA-EX 参加者と連携サービス提供者の間でやり取りが行われる。

7-2-12. カタログ情報

カタログ情報は、データセットのメタデータを管理し、公開するために必要なオブジェクトである。カタログ情報は DATA-EX ID、カタログ ID を有する。カタログには、データセットの付帯情報や利用条件等について記載する。カタログは、横断検索サイトに申請することで自動的にクロールされる。また、データ取引市場に登録することでデータ取引市場内での検索が可能となる。主に、データ発見時に DATA-EX 参加者同士でやり取りが行われる。

7-2-13. 契約情報

契約情報は、契約に基づきデータの提供と便益の交換に関する契約及びその履行状況を管理する為に必要なオブジェクトである。契約情報は DATA-EX ID、契約 ID を有する。主に、契約時に DATA-EX 参加者同士でやり取りが行われる。

7-2-14. DDP

DDP (Data Distribution Package) は、データセット、データセットの付帯情報(作成者、作成日、更新日、サイズなどのメタデータ)、データ交換の契約条項(秘密保持義務、利用用途)などが一体となったパッケージである。DATA-EX におけるデータ交換はすべて DDP 単位で行われる。したがって、契約によって提供する範囲が異なる場合や、複数のデータセットを組み合わせて提供する場合など、DATA-EX 参加者(データ提供)は必要に応じて複数の DDP を用意する必要がある。DDP は DATA-EX ID、DDP ID を有する。主に、データ授受時に DATA-EX 参加者同士でやり取りが行われる。

- ・ DDP は、DDP 本体形式に電子署名情報が付与されたデータである。ただし、電子署名情報は付与しなくてもよい。
 - DDP 本体形式は、DDP 識別情報と約定、及び 1 つ以上の、データセット付帯情報とデータセットの組、から構成される。ただし、約定は付与しなくてもよい。
 - ◇ DDP 識別情報は、DDP ID 及び DDP 作成者の DATA-EX ID から構成される。
 - ◇ 約定は、DDP の送信者と受信者の間で合意した取引条件を記載した、バイナリ形式のデータである。
 - ◇ データセット付帯情報は、対となるデータセットのメタ情報であり、W3C DCAT 標準で規定された、データセット部と配信部の項目の一部または全部を用いて記述する。W3C DCAT 標準のデータセット部及び配信部の一つ以上の任意の項目に対し、項目名と値を組として設定する。
 - ◇ データセットは DDP の送信者と受信者の間で合意したデータである。
 - 電子署名情報は、DDP 本体の電子署名及び署名者の電子証明書で構成される。
 - ◇ DDP 本体の電子署名は、DDP 本体形式への電子署名に用いた署名アルゴリズム名と DDP 本体形式への署名値から構成される。
 - ◇ 署名アルゴリズム名は、DDP 本体形式への電子署名に用いたハッシュアルゴリズムや公開鍵暗号アルゴリズムの名称を示す文字列データである。署名値は、DDP 本体形式に対する電子署名の値を示すバイナリ形式のデータである。
 - ◇ 電子証明書は、DDP 作成者の X.509 形式の電子証明書である。
- ・ DDP のファイル形式については、DATA-EX 参加者(データ提供)、もしくは、DATA-EX 参加者同士の協議により、論理形式を踏まえる前提にて、例えば zip 形式などの、任意のファイル形式とする。

(参考) DDP の論理形式は、拡張 BNF 記法を使用すると、下記のように表される。

<DDP> ::= <DDP 本体形式> [<電子署名情報>]

<DDP 本体形式> ::= <DDP 識別情報> [<約定>] (<データセット付帯情報> <データセット>)+

<DDP 識別情報> ::= <DDP ID> <DDP CREATOR>
 <DDP ID> ::= DDP ID
 <DDP CREATOR> ::= DDP 作成者の DATA-EX ID
 <約定> ::= 約定の電子データ
 <データセット付帯情報> ::= (<W3C DCAT ITEM NAME> <W3C DCAT ITEM VALUE>)+ (*
 W3C DCAT 標準のデータセット部と配信部の項目のサブセットの項目と値の組のリスト*)
 <W3C DCAT ITEM NAME> ::= STRING
 (* W3C DCAT 標準のデータセット部と配信部の中の任意の項目名 *)
 <W3C DCAT ITEM VALUE> ::= BINARY
 (* W3C DCAT ITEM NAME で指定される項目の値 *)
 <データセット> ::= BINARY (* 提供するデータセット本体データ *)
 <電子署名情報> ::= <DDP 本体の電子署名> <電子証明書>
 <DDP 本体の電子署名> ::= <署名アルゴリズム名> <署名値>
 <署名アルゴリズム名> ::= STRING
 (* 電子署名に用いたハッシュアルゴリズムや公開鍵暗号アルゴリズムの名称 *)
 <署名値> ::= BINARY (* <DDP 本体形式> のデータの電子署名の値 *)
 <電子証明書> ::= (* 署名に使った公開鍵に関する X.509 電子証明書。PEM 形式にエンコード
 されたバイナリデータ *)

7-3. ID

DATA-EX の分野間データ連携を行う為に、DATA-EX 内外で発行及び利用される以下の ID 群が必要となる。

なお、DATA-EX においては、多数の ID を使用するため、どの ID を示すのか識別する必要がある。よって、それぞれの ID の識別にあたっては、以下の表記を用いることとする。

表 2:ID を識別するための表記方法

No.	ID	表記方法
1	DATA-EX ID	DATA-EX_ID
2	コネクタ ID	CONNECTOR_ID
3	履歴 ID	EXCHANGE_HISTORY_ID
4	カタログ ID	CATALOGUE_ID
5	契約 ID	CONTRACT_ID
6	DDP ID	DDP_ID

7-3-1. DATA-EX ID

DATA-EX ID は DATA-EX 参加者を一意に識別する為の ID である。DATA-EX 内での一意性が担保される。DATA-EX 参加者からの DATA-EX 利用申請に応じて、DATA-EX 運営事業者が DATA-EX ID を発行する。また、DATA-EX 参加者が属する DATA-EX 参加組織の DATA-EX ID を発行する。

DATA-EX ID は、以下の要件を満たす ID である。

- ・DATA-EX ID は UUID とし、DATA-EX 参加者の DATA-EX 内での一意性を担保する。
- ・DATA-EX 参加者として、法人や法人内の個人、自然人が想定されるが、DATA-EX 参加者の所属する組織情報は、DATA-EX ID とは別に、DATA-EX 参加者の属性情報とする。

7-3-2. コネクタ ID

コネクタ ID はコネクタを一意に識別するための ID である。DATA-EX 運営事業者が DATA-EX 内での一意性を担保する。DATA-EX 内で、DATA-EX 参加者の DATA-EX 利用申請に応じて、DATA-EX 運営事業者がコネクタ ID を発行する。

コネクタ ID は、以下の要件を満たす ID である。

- ・コネクタ ID は UUID とし、DATA-EX 内での一意性を担保する。

7-3-3. 履歴 ID

履歴 ID は履歴情報を一意に識別するための ID である。DATA-EX 運営事業者が DATA-EX 内での一意性を担保する。DATA-EX 内で、一つ一つの DDP 作成および授受に対しての履歴発生時に DATA-EX 運営事業者が履歴 ID を発行する。

履歴 ID は、以下の要件を満たす ID である。

- ・履歴 ID は UUID とし、DATA-EX 内での一意性を担保する。

7-3-4. カタログ ID

カタログ ID はカタログ情報を一意に識別するための ID である。DATA-EX 参加者が DATA-EX ID と連携することで DATA-EX 内での一意性を担保する。カタログ作成時に DATA-EX 参加者（データ提供）がカタログ ID を発行する。

7-3-5. 契約 ID

契約 ID は契約情報を一意に識別するための ID である。DATA-EX 参加者が DATA-EX ID と連携することで DATA-EX 内での一意性を担保する。DATA-EX 参加者同士の契約締結時に、DATA-EX 参加者が契約 ID を発行する。

7-3-6. DDP ID

DDP ID は DDP を一意に識別するための ID である。DDP 作成時に DATA-EX 参加者（データ提供）が DDP ID を発行し、DDP ID を発行した DATA-EX 参加者（データ提供）の管理において一意性を担保する必要がある。

DDP ID は、以下の要件を満たす ID である。

- ・DDP ID は UUID とし、DATA-EX 内での一意性を担保する。

7-4. 機能

DATA-EX の分野間データ連携は、いくつかの機能を組み合わせた機能群で構成されている。

7-4-1. DATA-EX 内部の機能

「3-3. 概念モデル」にて示した 3 層構造のうち、データ連携基盤層の DATA-EX の機能について示す。

DATA-EX の機能は、大きく主要機能と支援機能に分かれる。

7-4-1-1. 主要機能

主要機能とは、主要サービスを提供するために必要な機能群である。主要機能は、一部の支援サービスにも用いられる。

7-4-1-1-1. データ交換機能

データ交換機能は、DATA-EX 参加者同士がデータを授受する為に必須な機能群である。データ受領・提供に必要な一連の機能(認証機能、認可機能、コネクタロケーション管理機能、DDP ロケーション管理機能)と連携してデータの授受を行う機能及び、来歴管理機能と連携する機能を持つ。

- ・ 必須事項
 - (受領側) 認証機能及びコネクタロケーション機能と連携し、提供側に DDP の送付を依頼する。(SHALL)
 - (受領側) データ受領時、来歴管理機能に受信履歴の登録を依頼する。(SHALL)
 - (提供側) 認証機能、認可機能及び DDP ロケーション管理機能と連携し、受領側に DDP を送付する。(SHALL)
 - (提供側) データ提供時、来歴管理機能に送信履歴の登録を依頼する。(SHALL)
- ・ 推奨事項
 - 更新されたバージョンは、過去のバージョンとの互換性が維持されていることが望ましい。

7-4-1-1-2. アカウント管理機能

アカウント管理機能は、DATA-EX 参加者を特定可能なアカウントを管理する機能である。

-
- ・ 必須事項
 - アカウントを発行する。(SHALL)
 - 認証機能と連携し、すべてのアカウントの認証を有効化する。(SHALL)
 - ・ 推奨事項
 - 外部で発行された ID と連携し、アカウントを発行できることが望ましい。

7-4-1-1-3. 認証機能(DATA-EX 内部の機能)

認証機能は、DATA-EX 参加者の実在性を確認し、DATA-EX ID の正当性を確認する機能である。

- ・ 必須事項
 - DATA-EX ID と、認証機能が提示する 2 要素の認証方法の選定と、認証に必要な情報（パスワードや生体情報等の入力など）を受け取って審査し、認証された場合、アカウントの認証情報を発行する。(SHALL)
 - データ交換機能や認可機能から受け取った認証情報に応じて、認証情報の正当性を確認し、確認結果を返す。(SHALL)
 - 認証情報の発行・正当性確認において、依頼元の機能・アプリケーションの正当性を事前に発行された情報をもとに検証する。(SHALL)
 - 検証に用いる情報には、クライアント ID とクライアントシークレットなどを用いてよい。
 - 認証情報の発行において、認証情報が発行依頼者本人以外の正当性確認に用いられないよう、セキュリティ対策を講じる。(SHALL)
 - セキュリティ対策には、送付先の DATA-EX 参加者や送信元デバイスを限定する方法などがある。

7-4-1-1-4. 認可機能

認可機能は、正当性を確認した DATA-EX 参加者に対して DDP への適切なアクセスを制御する機能である。また、認可機能は DATA-EX 参加者(データ提供)自身が用意しなければならない。

- ・ 必須事項
 - DDP へのアクセス権限（DDP ID と DATA-EX ID の紐付け、もしくは DDP ID と組織の紐付け、必要に応じて DDP ID と DATA-EX ID および組織の紐付け）を登録する。(SHALL)
 - データ交換機能及び認証機能と連携し、受け取った認証情報に応じて適切な認可情報をデータ交換機能(データ提供側)に返す。(SHALL)

7-4-1-1-5. 証明書登録機能

証明書登録機能は、DATA-EX 参加者が持つコネクタの真正性を証明する為の電子証明書を登録する機能である。

- ・ 必須事項
 - 外部機関（発行局）と連携し、証明書発行申請に応じて電子証明書を配付する。(SHALL)

7-4-1-1-6. コネクタロケーション管理機能

コネクタロケーション管理機能は、DATA-EX 上のコネクタの所在を管理し、コネクタロケーション解決を実施する機能である。コネクタのリゾルバとして動作する。

- ・ 必須事項
 - コネクタ ID とコネクタロケーションを紐付ける。(SHALL)
 - データ交換機能から受け取ったコネクタ ID に応じて、適切なコネクタロケーションを返す。(SHALL)
 - コネクタ ID の一意性を担保するため、コネクタ ID の重複チェックを行う。(SHALL)

7-4-1-1-7. DDP ロケーション管理機能

DDP ロケーション管理機能は、DATA-EX 上で提供される DDP の所在を管理し、DDP ロケーション解決を実施する機能である。DDP のリゾルバとして動作する。また、DDP ロケーション管理機能は DATA-EX 参加者（データ提供）自身が用意しなければいけない。

- ・ 必須事項
 - DDP ID と DDP ロケーションを紐付ける。(SHALL)
 - 設定された認可情報に応じて、適切な DDP ロケーションをデータ交換機能に返す。(SHALL)

7-4-1-1-8. 来歴管理機能

来歴管理機能は、DATA-EX を介して収受されるデータの収受来歴を記録管理する機能である。DDP 作成時・送信時・受信時の履歴情報を登録する。また、DATA-EX 参加者（データ提供）によって履歴情報の登録可否を設定することが可能である。

- ・ 必須事項
 - データ交換機能と連携し、DDP 提供時及び DDP 受領時に履歴を登録する。(SHALL)
 - DDP 作成時に履歴を登録する。(SHALL)
 - 来歴取得依頼に応じて、DATA-EX 参加者に係る来歴を返す。(SHALL)

登録した来歴は、事前に決められたステークホルダー、および、DDP の作成者と送受信のみが閲覧することができる。ただし、DATA-EX 運営事業者の認める範囲内で、DDP の作成者が DDP 固有のアクセス制御ポリシーを設定することもできる。DDP の作成者が許可する場合には、履歴登録者が個々の履歴情報に対するアクセス制御ポリシーを設定することもできる。

7-4-1-1-9. コネクタ公開機能

コネクタ公開機能は、コネクタのバージョンを管理し、DATA-EX 参加者にコネクタを公開する機能である。

- ・ 必須事項
 - 最新バージョンのコネクタモジュールを提供する。(SHALL)
- ・ 推奨事項
 - 過去のバージョンのコネクタモジュールを公開できることが望ましい。
 - コネクタのバージョンが更新された際に、DATA-EX 参加者に通知できることが望ましい。

7-4-1-1-10. ポータル機能

ポータル機能は、DATA-EX に関連するサービス群の一覧とそのエンドポイントを掲載したポータルサイトを Web 上で一般公開し、また DATA-EX のモニタリングダッシュボード等を公開する機能である。

- ・ 必須事項
 - DATA-EX のサービスを一覧化し、URL を公開する。(SHALL)
 - DATA-EX 参加者の活動の統計情報、例外処理、過失及び情報セキュリティ事象を記録したイベントログをダッシュボードで公開する。(SHALL)

7-4-1-2. 支援機能

支援機能とは、支援サービスを提供するために必要な機能群である。

7-4-1-2-1. データカタログ横断検索機能

データカタログ横断検索機能とは、DATA-EX 上で提供されているデータに関するカタログを組織横断で検索し、データの発見を支援する機能である。データカタログ横断検索機能は、カタログサイトをクローリングし、横断検索サイトの検索結果としてカタログを表示する。

- ・ 必須事項
 - CKAN 互換のカタログサイトをクローリングし、カタログを取得する。(SHALL)
 - 検索条件に合致したカタログを表示する。(SHALL)
- ・ 推奨事項
 - CKAN 互換ではないカタログサイトをクローリングできることが望ましい。

7-4-1-2-2. データカタログ作成機能

データカタログ作成機能とは、データ提供を担当する DATA-EX 参加者によるカタログの作成・登録を支援する為のデータカタログ作成ツールを提供し、データの広告、公開を支援する機能である。

- ・ 必須事項
 - DATA-EX データカタログ項目仕様に準拠したカタログを生成する。(SHALL)
- ・ 推奨事項
 - 生成したカタログをカタログサイトに登録できることが望ましい。
 - 語彙管理機能と連携し、カタログでの利用が推奨される語彙を取得できることが望ましい。

7-4-1-2-3. データ取引市場機能

データ取引市場機能とは、DATA-EX を介して、契約に基づきデータの提供と便益の交換に関する契約及びその履行状況を管理する機能である。以下のような機能を持つ。

- ・ 認証
- ・ データ検索
- ・ 商談
- ・ 決済
- ・ 契約管理
- ・ 必須事項
 - データ取引市場を利用するためのアカウントを発行し、アカウントに DATA-EX ID を紐づける。(SHALL)
 - 契約の当事者間で契約書を送受信する。(SHALL)
 - 締結した契約情報を保管する。(SHALL)
- ・ 推奨事項
 - 取引時の情報の参照先として、DATA-EX のカタログを取り込めることが望ましい。
 - データを条件検索できることが望ましい。
 - 商談開始から契約締結までの商談履歴を記録できることが望ましい。
 - 契約に係る代金の決済ができることが望ましい。

7-4-1-2-4. 語彙管理機能

語彙管理機能とは、DATA-EX を介して、提供・受領されるデータに含まれる語彙を登録、保管及び公開し、分野を超えたデータ活用を支援する機能である。

- ・ 必須事項

-
- フォーマット化された語彙セットを作成する。(SHALL)
 - 語彙セットをリポジトリに登録し、公開する。(SHALL)
 - ・ 推奨事項
 - 語彙セットを条件検索できることが望ましい。

7-4-1-3. 機能一覧

DATA-EX の分野間データ連携を構成する機能を 7-4-1-1 主要機能及び 7-4-1-2 支援機能に示した。本項では、そのまとめとして、DATA-EX の分野間データ連携を構成する機能の一覧を示す。

- ・ 主要機能
 - データ交換機能
 - アカウント管理機能
 - 認証機能
 - 認可機能
 - 証明書登録機能
 - コネクタロケーション管理機能
 - DDP ロケーション管理機能
 - 来歴管理機能
 - コネクタ公開機能
 - ポータル機能
- ・ 支援機能
 - データカタログ横断検索機能
 - データカタログ作成機能
 - データ取引市場機能
 - 語彙管理機能

7-4-2. DATA-EX 外部の機能

3 層構造のうち、アプリケーション層及びトラストサービス層の機能について示す。

本項に示す機能は、いずれも DATA-EX 外部のサービス等を構成する機能群であるため、本仕様書では機能の概要説明を示す。

7-4-2-1. アプリケーション層の機能

3 層構造のうち、アプリケーション層の機能について示す。アプリケーション層は、DATA-EX をはじめとするデータ連携基盤を利用するアプリケーションのレイヤーであり、データ受領側のユーザーとデータ提供側のユーザーが存在することが想定される。そのため、どちら側かに固有の機能か、あるいはどちらにも共通する機能かを整理して機能説明を示す。

7-4-2-1-1. データ提供側/データ受領側共通の機能

アプリケーション層の機能のうち、データ提供側/データ受領側共通の機能について示す。

7-4-2-1-1-1. 相対取引契約管理機能

DATA-EX 参加者間で取り交わすデータ交換に関する契約の交渉、締結を行うために利用される機能である。

- ・ 必須事項
 - 契約情報を契約情報格納用ストレージに格納する。(SHALL)

7-4-2-1-1-2. 契約情報格納用ストレージ

DATA-EX 参加者間で締結された契約の契約情報を格納するためのコンポーネントである。

- ・ 必須事項
 - 契約情報を格納する。(SHALL)
- ・ 推奨事項
 - 契約の履行状況が確認できることが望ましい。
 - DDP 作成時に、DDP 作成機能が契約情報を取得できることが望ましい。

7-4-2-1-1-3. DDP 格納用ストレージ

DDP を一時的に格納するためのコンポーネントである。

- ・ 必須事項
 - (提供側)作成した DDP を格納する。(SHALL)
 - (提供側)データ交換時に DDP を取得できること。(SHALL)
 - (受領側)受領した DDP を一時的に格納する。(SHALL)

7-4-2-1-2. データ提供側固有の機能

アプリケーション層の機能のうち、データ提供側の機能について示す。

7-4-2-1-2-1. アプリケーション(データ提供側)

DATA-EX 参加者(提供者)が、DATA-EX をはじめとするデータ連携基盤層の各種機能を利用するためのアプリケーションである(ブラウザ含む)。

- ・ 必須事項
 - アプリケーション(データ提供側)は、データ交換機能(データ提供側)、認可機能、DDP ロケーション管理機能、アカウント管理機能/認証機能を利用する。(SHALL)

- ・ 推奨事項

- アプリケーション(データ提供側)は、来歴管理機能を利用することが望ましい。

7-4-2-1-2-2. カタログサイト

データカタログを管理するためのソフトウェアであり、代表的な例としてオープンソースの CKAN が挙げられる。

- ・ 必須事項

- カタログ情報を登録し、公開する。(SHALL)

- ・ 推奨事項

- クローリングされた場合、データセットのメタデータの一覧(リスト)を提供する機能を持つことが望ましい。

7-4-2-1-2-3. データ管理ストレージ

データセットを格納するコンポーネントである。

- ・ 必須事項

- データセットを格納する。(SHALL)
- DDP 作成時にデータセットを提供する。(SHALL)

7-4-2-1-2-4. DDP 作成機能

DATA-EX 参加者(提供者)が DDP を作成するために利用する機能である。

- ・ 必須事項

- データセットから DDP を作成する。(SHALL)

- ・ 推奨事項

- 契約情報格納用ストレージから必要な契約条項の情報を取得できることが望ましい。

7-4-2-1-3. データ受領側固有の機能

アプリケーション層の機能のうち、データ受領側の機能について示す。

7-4-2-1-3-1. アプリケーション(データ受領側)

DATA-EX 参加者(受領者)が、DATA-EX をはじめとするデータ連携基盤層の各種機能を利用するためのアプリケーションである(ブラウザ含む)。

- ・ 必須事項

- アプリケーション(データ受領側)は、データ交換機能(データ受領側)、アカウント管理機能/認証機能を利用する。(SHALL)

- ・ 推奨事項

- アプリケーション(データ受領側)は、データカタログ横断検索機能を利用することが望ましい。
- アプリケーション(データ受領側)は、来歴管理機能を利用することが望ましい。

7-4-2-1-3-2. DDP 分解機能

受領した DDP を分解するための機能である。

- ・ 必須事項

- DDP からデータセット本体、データセットの付帯情報、契約条項に分解し、取り出す。(SHALL)

7-4-2-2. 連携サービス提供機能

連携サービス提供機能とは、連携サービスが提供する機能のうち、DATA-EX と連携し利用される機能群である。

7-4-2-2-1. トラストサービス層の機能

3 層構造のうち、トラストサービス層の機能について示す。

7-4-2-2-1-1. 身元確認機能

身元確認機能は、DATA-EX 参加者および参加組織の実在性の確認を行う機能である。(SHALL)

DATA-EX 参加申請前に、利用者が外部 IdP への登録を行う際に利用されるものである。

7-4-2-2-1-2. 認証機能(外部 IdP)

認証機能は、DATA-EX や e シールサービスなどのサービス提供者からの依頼により、外部 IdP が一定の基準により利用者の認証を行い、認証結果をサービス提供者に通知する機能である。(SHALL)

7-4-2-2-1-3. ID 発行機能

ID 発行機能は、外部 IdP において利用者を識別する識別子を発行する機能である。(SHALL)

なお、DATA-EX 内では、外部 IdP により発行される識別子と DATA-EX ID とを紐づけて ID 管理を行う。

7-4-2-2-1-4. 属性提供機能

属性提供機能は、認証された利用者の属性情報をサービス提供者に提供する機能である。(SHALL)

利用者認証連携の応答の一部として、外部 IdP が DATA-EX に属性情報を提供しても構わない。

7-4-2-2-1-5. e シール付与機能

e シール付与機能は、トラストアンカーにより保証される DATA-EX 参加者が所属する組織に対する電子証明書を利用して、対象となるデータの作成組織の真正性およびデータの完全性を保証する e シールを生成、提供する機能である。(SHALL)

対象となるデータのハッシュ値を受領し、DATA-EX 参加組織の電子証明書に紐づく秘密鍵を利用して e シールを生成する。

7-4-2-2-1-6. 電子署名付与機能

電子署名付与機能は、トラストアンカーにより保証される DATA-EX 参加者に対する電子証明書を利用して、対象となるデータの完全性および作成者の真正性を保証する電子署名を生成、提供する機能である。(SHALL)

主に、契約時に契約者の意思表示として利用される。

対象となるデータのハッシュ値を受け取り、DATA-EX 参加者の電子証明書に紐づく秘密鍵を利用して電子署名を生成する。

7-4-2-2-1-7. タイムスタンプ付与機能

タイムスタンプ付与機能は、ある時刻にそのデータが存在していたこと、およびそれ以降改ざんされていないことを証明するタイムスタンプを生成、提供する機能である。(SHALL)

対象となるデータのハッシュ値を受領し、信頼できる時刻情報のタイムスタンプを付与し、サービス提供者の電子署名を付与する。

7-4-2-2-1-8. 証明書発行機能

証明書発行機能は、DATA-EX 参加者、参加組織、デバイス、サーバーの少なくともいずれかに対して、電子証明書を発行する機能である。(SHALL)

7-4-2-2-2. 来歴管理拡張機能

来歴管理拡張機能は、DATA-EX 参加者間でのデータ連携にて収受された DDP に含まれるデータセットの収受・供与および作成・加工等の来歴を記録管理し、DATA-EX 参加者の要望に応じてその来歴を提供する機能である。(SHALL)

DDP に含まれるデータセットの入手元情報、加工内容を記録可能な加工履歴登録機能を持つ。(SHALL)

DDP に含まれるデータセットの入手元情報、加工内容の一連の履歴を時系列順に取り出す加工来歴情報提供機能を持つ。(SHALL)

【Note】DATA-EX 外部の機能により、ファイル形式以外のデータセットに対する DDP の作成や、定期的なデータ授受を想定した DDP の作成・分解を行うことも可能である。例として、NGSI 方式のような、JSON 形式かつ一定期間で更新されるデータセットのデータ授受を行う際の実施例を図 5 に示す。一つの実施例として、DDP 作成機能や DDP 分解機能が本来持つ機能を応用し、DDP 作成機能で NGSI (JSON) 形式のデータセットに基づく DDP の作成やデータセットの更新に応じた DDP の定期的な作成を実施することや、DDP 分解機能において受領した DDP から NGSI (JSON) 形式のデータ抽出を行うことが考えられる。これら機能の検討においては、本書に示される要求 (SHALL)、禁止 (SHALL NOT)、許容 (MAY) の規程に準ずること。

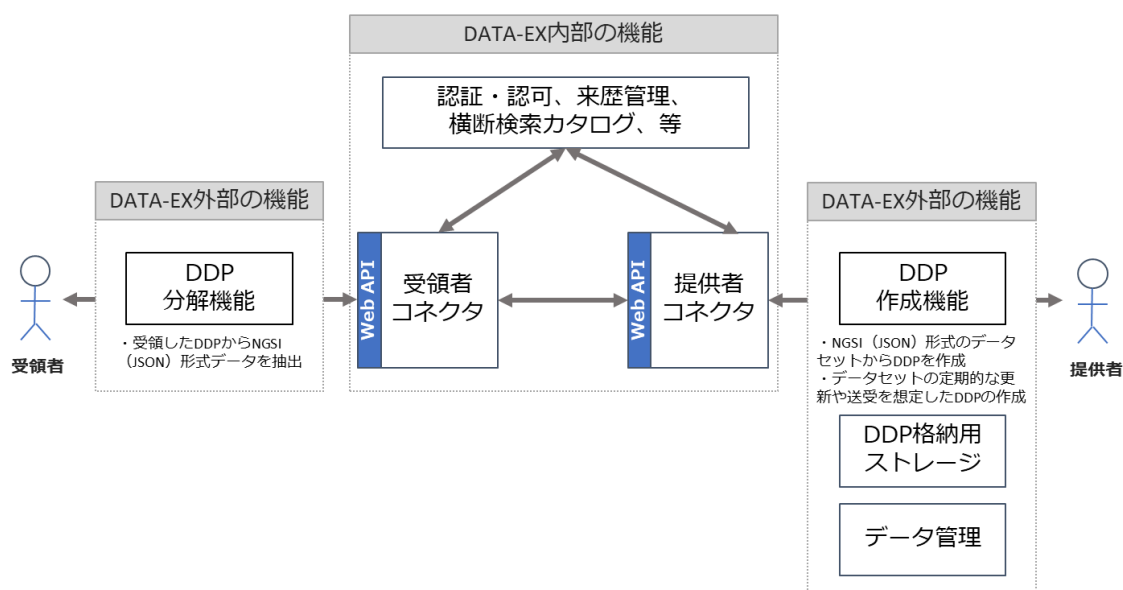


図 5: NGSI 方式のデータ授受 実施例

8. シナリオ

DATA-EX には、利用パターンとして以下の3つを想定している。

- ① 契約を交わさずにデータ交換を行う
- ② 相対取引によって契約を交わし、データ交換を行う
- ③ データ取引市場などを介して契約を交わし、データ交換を行う

8-1. 契約を交わさずにデータ交換を行う

8-1-1. 利用準備

利用準備は、DATA-EX 参加者が DATA-EX を利用する前に実施する一連の作業(利用申請、コネクタ構築)である。

8-1-1-1. 利用申請

利用申請は、DATA-EX 参加者が DATA-EX の利用を開始するために必要な一連の作業である。

- ・ 登録準備
 - DATA-EX 参加者が、外部 IdP を利用する場合、以下の作業を実施する。
 - ◇ DATA-EX 参加者が、外部 IdP に事前登録申請を依頼する。
 - ◇ 外部 IdP が、申請者が本人であることの身元確認を行う。
 - ◇ 外部 IdP と申請者間で、認証に必要な認証クレデンシャル(パスワード等)を設定する。
 - DATA-EX 参加者が、ポータルサイトを閲覧し、DATA-EX 利用解説書を取得する。
 - DATA-EX 参加者が、コネクタ構築に必要な環境(デバイス、認可サーバー、ストレージ、など)を準備する。
 - DATA-EX 参加者(データ提供)が、カタログサイトを構築する。
 - DATA-EX 参加者が、ポータルサイトを閲覧し、申請先の URL を確認する。
 - DATA-EX 参加者が、DATA-EX 運営事業者に DATA-EX の利用申請をする。
- ・ 登録
 - DATA-EX 参加者が、外部 IdP を利用しない場合、以下の作業を実施する。
 - ◇ DATA-EX 運営事業者が、申請者が本人であることの身元確認を行う。
 - DATA-EX 参加者が、外部 IdP を利用する場合、以下の作業を実施する。
 - ◇ DATA-EX 運営事業者が、申請者の認証を外部 IdP に依頼する。
 - ◇ 外部 IdP が申請者の認証を行う。
 - ◇ DATA-EX 運営事業者が、申請者の属性を含む認証結果を受け取る。
 - ◇ DATA-EX 運営事業者が、申請者が本人であることを確認する。
 - DATA-EX 運営事業者が、申請内容を審査する。

-
- DATA-EX 参加者が、外部 IdP を利用しない場合、以下の作業を実施する。
 - ◇ DATA-EX 運営事業者と申請者間で、認証に必要な認証クレデンシャル(パスワード等)を設定する。
 - DATA-EX 運営事業者が、アカウント(DATA-EX ID など)とコネクタ設定(コネクタ ID など)を発行する。(DATAEX-ID、コネクタ ID の一意性を保証)
 - DATA-EX 運営事業者が、申請者が組織に属している場合、所属する DATA-EX 参加組織に対し DATA-EX ID を発行する。
 - ・ アカウント・コネクタ設定取得
 - DATA-EX 運営事業者が、DATA-EX 参加者にアカウントとコネクタ設定を送付する。
 - DATA-EX 参加者が、アカウントとコネクタ設定を受領する。
 - ・ 支援サービス利用登録
 - DATA-EX 参加者が、DATA-EX 支援サービス提供者に支援サービスの利用申請をする。
 - DATA-EX 参加者が、外部 IdP を利用しない場合、以下の作業を実施する。
 - ◇ DATA-EX 支援サービス提供者が、申請者の認証を DATA-EX 運営事業者に依頼する。
 - ◇ DATA-EX 運営事業者が申請者の認証を行う。
 - ◇ DATA-EX 支援サービス提供者が、申請者の属性情報を含む認証結果を受け取る。
 - DATA-EX 参加者が、外部 IdP を利用する場合、以下の作業を実施する。
 - ◇ DATA-EX 支援サービス提供者が、申請者の認証を外部 IdP に依頼する。
 - ◇ 外部 IdP が申請者の認証を行う。
 - ◇ DATA-EX 支援サービス提供者が、申請者の属性情報を含む認証結果を受け取る。
 - DATA-EX 支援サービス提供者が、申請内容を審査し、支援サービスの利用を許可する。

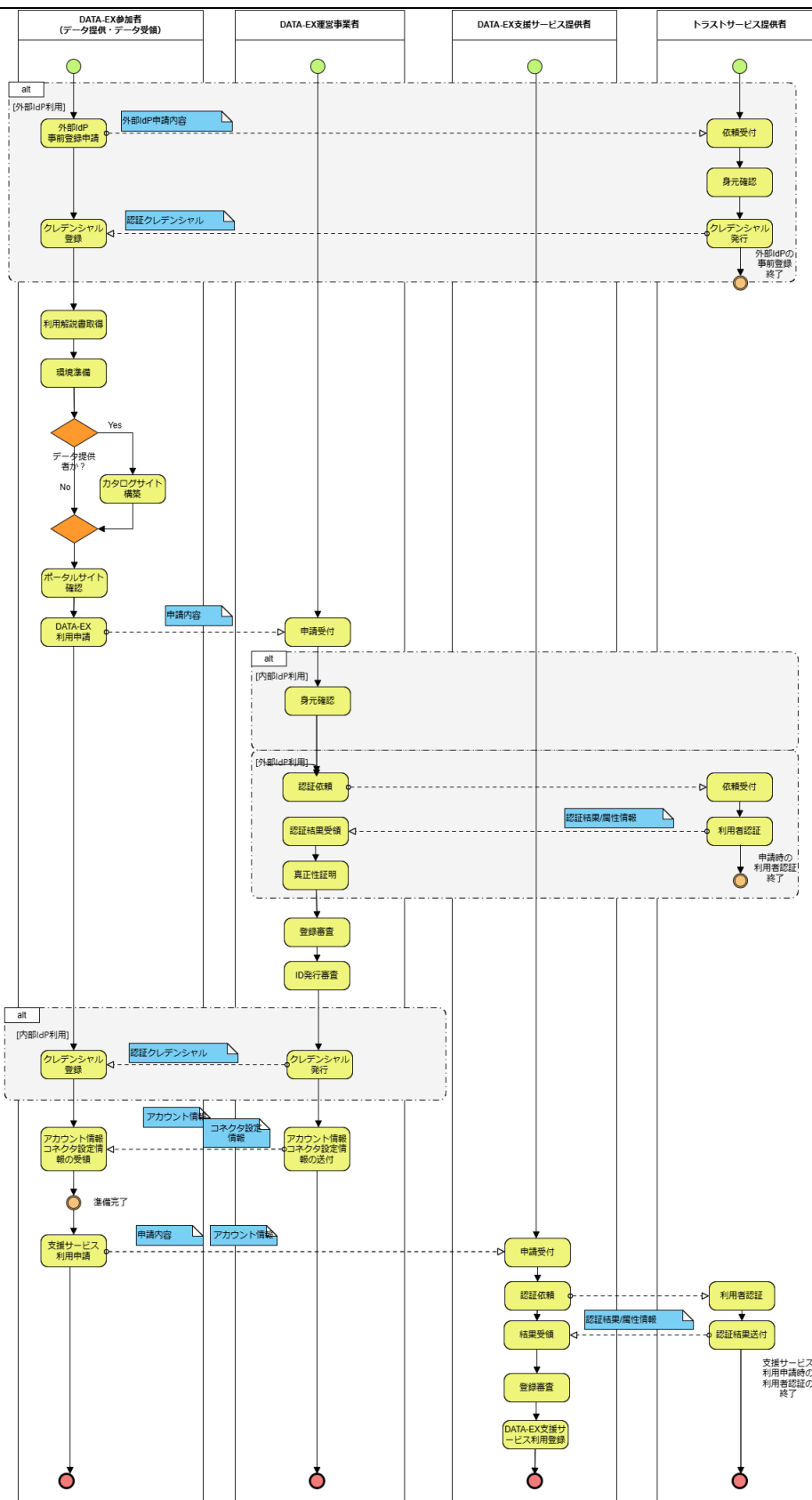


図 6: 利用申請の概要図

8-1-1-2. コネクタ構築

コネクタ構築は、DATA-EX 参加者が DATA-EX 上でコネクタを介した通信を行うために必要な一連の作業である。

- ・ コネクタ送付
 - DATA-EX 参加者が、ポータルサイトを閲覧し、コネクタ公開サイトの URL を確認する。
 - DATA-EX 参加者が、DATA-EX 運営事業者にコネクタの送付を依頼する。
 - DATA-EX 運営事業者が、DATA-EX 参加者にコネクタを送付する。
 - DATA-EX 参加者が、コネクタを受領する。
 - DATA-EX 参加者が、コネクタを構築し、コンフィグ情報を設定する。
- ・ コネクタの電子証明書発行
 - DATA-EX 参加者が、DATA-EX 運営事業者にコネクタの電子証明書発行を申請する。
 - DATA-EX 運営事業者が、コネクタの電子証明書発行申請を受け付ける。
 - DATA-EX 運営事業者が、認証局にコネクタの電子証明書の発行を依頼する。
 - 認証局が、コネクタの電子証明書を発行し、DATA-EX 運営事業者にコネクタの電子証明書を送付する。
 - DATA-EX 運営事業者が認証局で発行されたコネクタの電子証明書を配付する。
 - DATA-EX 参加者が、コネクタの電子証明書を受領する。
- ・ コネクタ起動
 - DATA-EX 参加者が、コネクタを起動する。
 - DATA-EX 参加者が、DATA-EX 運営事業者にコネクタ ID と申請者のロケーションの紐づけ登録を依頼する。
 - DATA-EX 運営事業者が、申請者のコネクタの真正性およびコネクタ ID の一意性を確認し、コネクタ ID と申請者のロケーションの紐づけを登録する。
 - DATA-EX 運営事業者が、DATA-EX 参加者にコネクタ ID と申請者のロケーションの紐づけ登録が完了したことを通知する。
 - DATA-EX 参加者が、DATA-EX 運営事業者からのコネクタ ID と申請者のロケーションの紐づけ登録完了通知を受領する。
 - DATA-EX 運営事業者が、コネクタの疎通テスト環境を提供する。
 - DATA-EX 参加者が、コネクタと DATA-EX が接続できることを確認する。

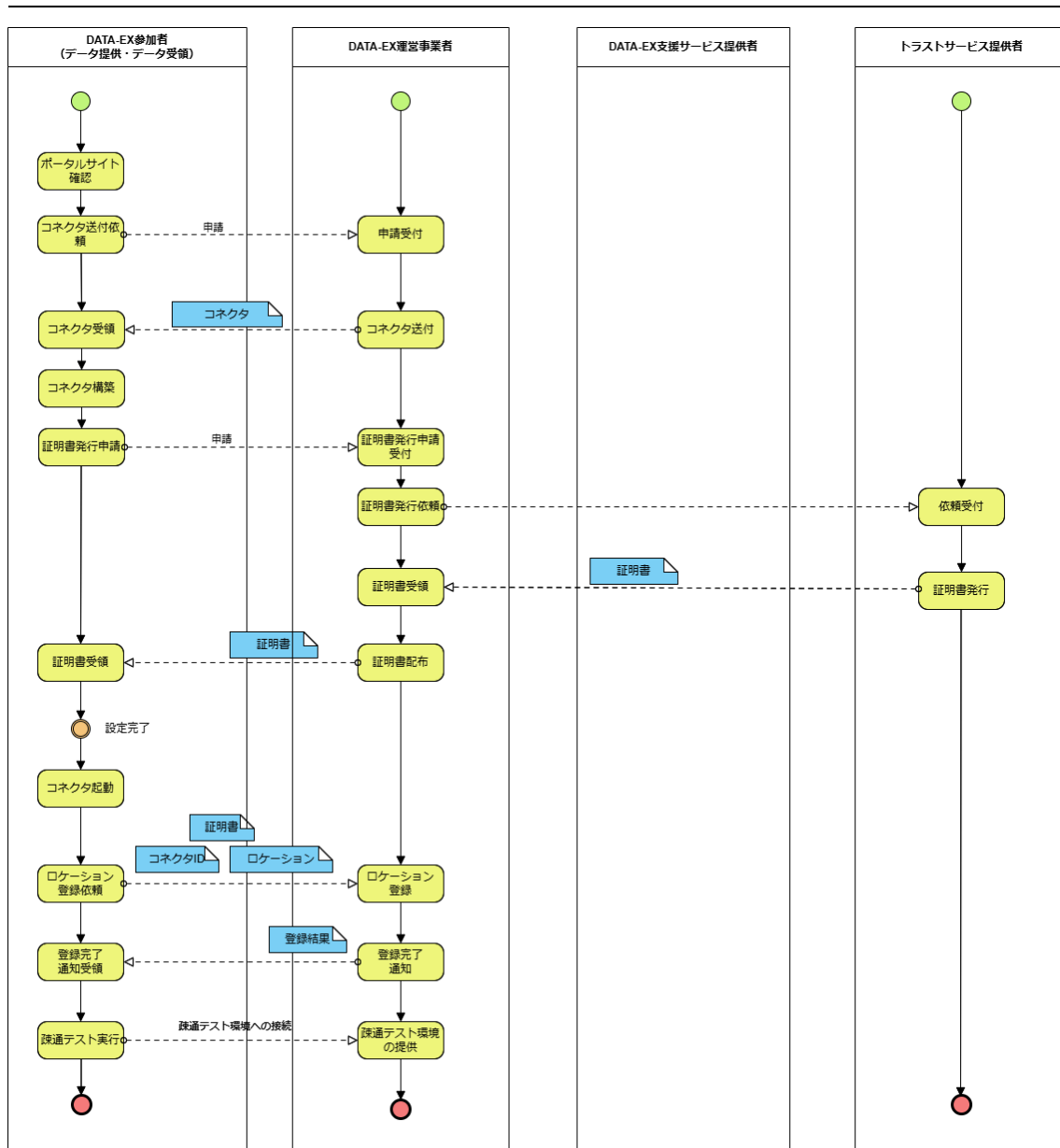


図 7:コネクタ構築の概要図

8-1-2. 利用

利用は、DATA-EX 参加者が DATA-EX を利用する際に行う一連の作業（データセット用意、データセット発見、契約・DDP 作成、DDP 授受、語彙リポジトリ登録、語彙リポジトリ参照、来歴確認、DDP 削除、データセット削除）である。

8-1-2-1. カタログ用意

カタログ用意は、DATA-EX 参加者（データ提供）が DATA-EX 上で提供するデータセットを用意するために必要な一連の作業である。

- ・ 横断検索サイト登録

-
- DATA-EX 参加者(データ提供)が、ポータルサイトを閲覧し、登録依頼先の URL を確認する。
 - DATA-EX 参加者(データ提供)が、横断検索サイトにカタログサイトの登録を依頼する。
 - DATA-EX 参加者が、外部 IdP を利用しない場合、以下の作業を実施する。
 - ✧ DATA-EX 支援サービス提供者が、申請者の認証を DATA-EX 運営事業者に依頼する。
 - ✧ DATA-EX 運営事業者が申請者の認証を行う。
 - ✧ DATA-EX 支援サービス提供者が、申請者の属性情報を含む認証結果を受け取る。
 - DATA-EX 参加者が、外部 IdP を利用する場合、以下の作業を実施する。
 - ✧ DATA-EX 支援サービス提供者が、申請者の認証を外部 IdP に依頼する。
 - ✧ 外部 IdP が申請者の認証を行う。
 - ✧ DATA-EX 支援サービス提供者が、申請者の属性情報を含む認証結果を受け取る。
 - DATA-EX 支援サービス提供者が、登録内容を審査する。
 - DATA-EX 支援サービス提供者が、横断検索サイトでカタログサイトのクローリングを実施する。
 - DATA-EX 支援サービス提供者が、横断検索サイトにカタログが表示されることを確認する。
 - DATA-EX 支援サービス提供者が、依頼者にカタログサイトの登録が完了したことを通知する。
 - DATA-EX 参加者(データ提供)が、登録完了通知を受領する。
 - ・ カタログ作成
 - DATA-EX 参加者(データ提供)が、データカタログ作成ツールでカタログを作成する。
 - DATA-EX 参加者(データ提供)が、e シールサービスに作成したカタログの e シールの付与を依頼する。
 - e シールサービスが、e シールを生成し、送付する。
 - DATA-EX 参加者(データ提供)が、e シール付きのカタログを作成する。
 - DATA-EX 参加者(データ提供)が、カタログをカタログサイトに登録する。
 - DATA-EX 支援サービス提供者が、定期的にカタログサイトのクローリングを実施する。
-

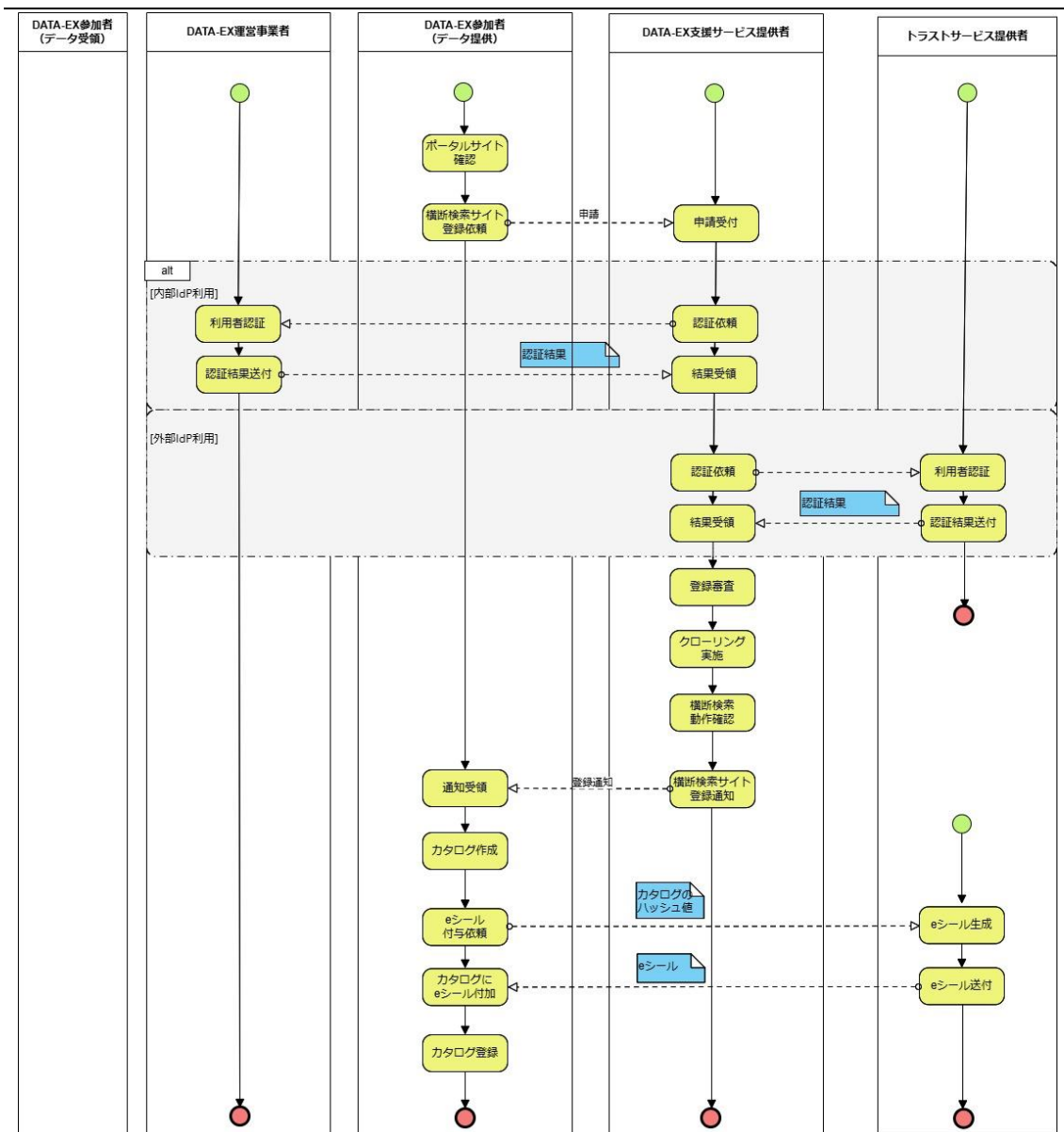


図 8:カタログ用意の概要図

8-1-2-2. データセット発見

データセット発見は、DATA-EX 参加者（データ受領）が DATA-EX 上で提供されるデータセットを発見するために必要な一連の作業である。

- ・ 横断検索サイト利用
 - DATA-EX 参加者（データ受領）が、ポータルサイトを閲覧し、横断検索サイトの URL を確認する。
 - DATA-EX 参加者（データ受領）が、横断検索サイトに検索条件を入力し、検索する。
 - DATA-EX 支援サービス提供者が、検索結果（検索条件に合致するカタログ）を送付する。

- DATA-EX 参加者(データ受領)が、横断検索サイト上で検索結果を閲覧する。
- DATA-EX 参加者(データ受領)が、カタログを選択する。
- DATA-EX 参加者(データ提供)が、カタログサイト上のカタログを送付する。
- DATA-EX 参加者(データ受領)が、カタログの e シールを検証する。
- DATA-EX 参加者(データ受領)が、DATA-EX 運営事業者に e シール作成者が DATA-EX に参加していることの確認を依頼する。
- DATA-EX 運営事業者が、e シール作成者が DATA-EX 参加者であることの確認結果を送付する。
- DATA-EX 参加者(データ受領)が、カタログサイト上のカタログを閲覧する。

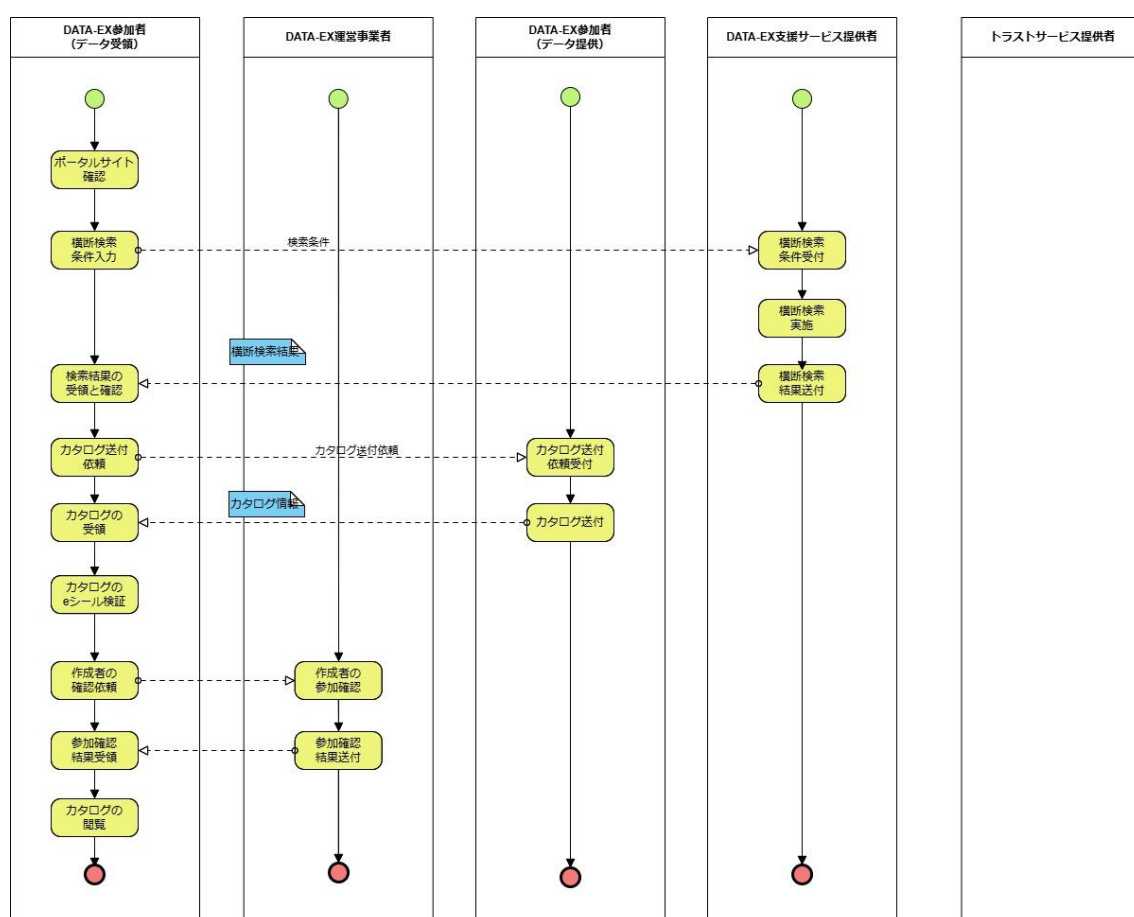


図 9: データセット発見の概要図

8-1-2-3. DDP 作成

DDP 作成は、DATA-EX 参加者同士における取得するデータの範囲や利用条件などについての協議に基づいて DDP を作成し、DDP ID とコネクタ ID を通知するために必要な一連の作業である。

- ・ DDP 作成

-
- DATA-EX 参加者同士が、取得するデータの範囲や利用条件などについて協議する。
 - DATA-EX 参加者（データ提供）が、DDP に含むデータセット・付帯情報・利用条件などを決定する。
 - DATA-EX 参加者（データ提供）が、DDP（DDP ID など）を作成する。
 - DATA-EX 参加者（データ提供）が、e シールサービスに DDP への e シールの付与を依頼する。
 - DATA-EX 参加者（データ提供）が、e シールを受け取り、DDP に付加する。
 - DATA-EX 参加者（データ提供）が、配信用のストレージに格納する。
 - DATA-EX 参加者（データ提供）が、DDP ID と DDP のロケーション情報を登録する。
 - DATA-EX 参加者（データ提供）が、DDP の認可情報を登録する。
 - DATA-EX 参加者（データ提供）が、必要に応じて DATA-EX 運営事業者に DDP 作成履歴の登録を依頼する。
 - DATA-EX 運営事業者が、履歴を登録する。
 - ・ DDP ID・コネクタ ID 通知
 - DATA-EX 参加者（データ提供）が、DATA-EX 参加者（データ受領）に DDP ID とコネクタ ID を通知する。
 - DATA-EX 参加者（データ受領）が、通知を受領する。

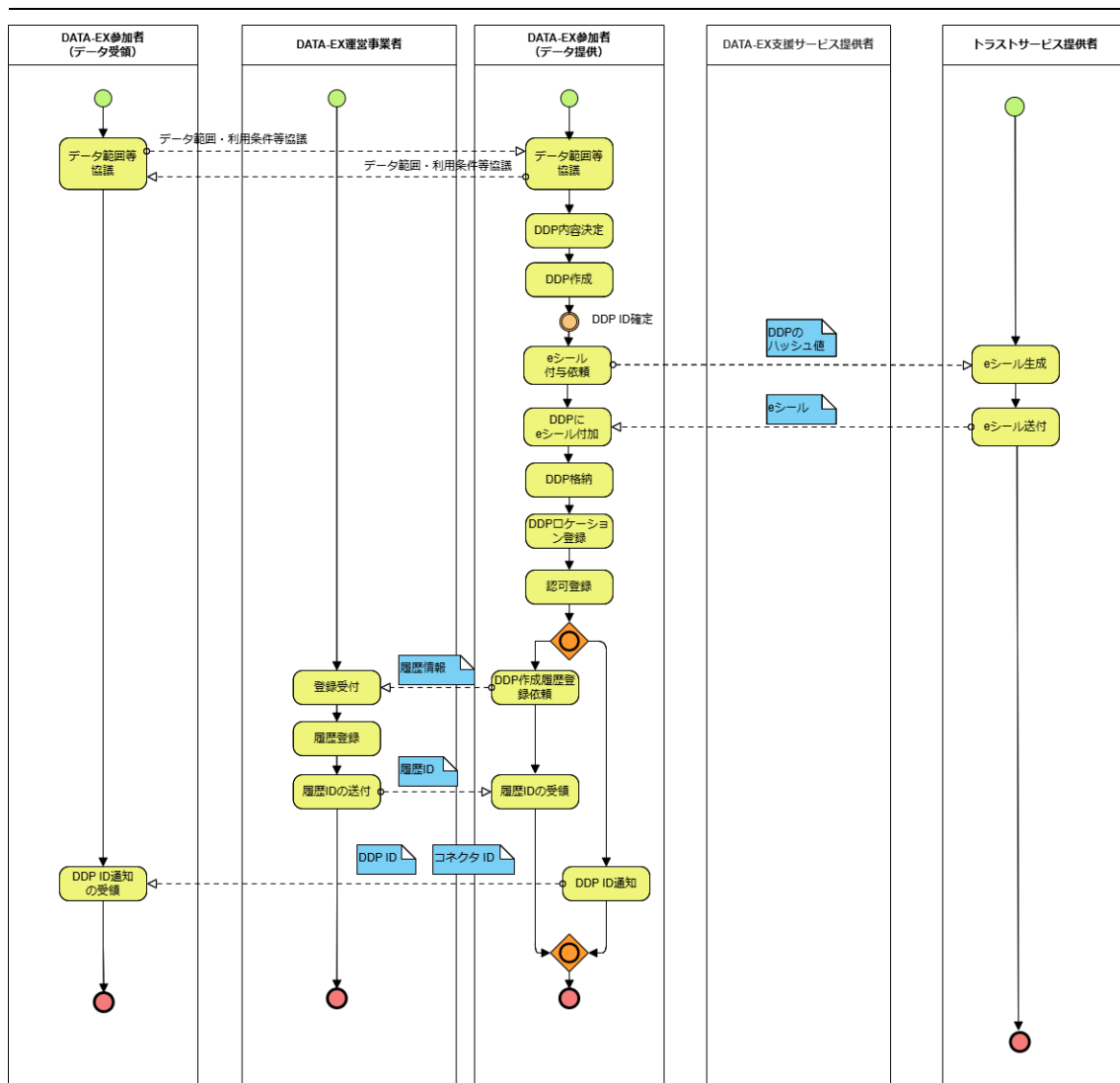


図 10:DDP 作成の概要図

8-1-2-4. データ交換

データ交換は、DATA-EX 参加者（データ提供）と DATA-EX 参加者（データ受領）がデータの交換を行うために必要な一連の作業である。DATA-EX 参加者（データ受領）が DATA-EX 参加者（データ提供）の用意した DDP を取りに来る方式となる。

- ・ 認証情報取得
 - DATA-EX 参加者（データ受領）が、DATA-EX 運営事業者に認証情報の送付を依頼する。
 - DATA-EX 参加者が、外部 IdP を利用しない場合、以下の作業を実施する。
 - ◇ DATA-EX 運営事業者が申請者の認証を行う。
 - DATA-EX 参加者が、外部 IdP を利用する場合、以下の作業を実施する。

-
- ◇ DATA-EX 運営事業者が、申請者の認証を外部 IdP に依頼する。
 - ◇ 外部 IdP が申請者の認証を行う。
 - ◇ DATA-EX 運営事業者が、申請者の属性情報を含む認証結果を受け取る。
 - DATA-EX 運営事業者が、DATA-EX 参加者(データ受領)に認証情報を送付する。
 - DATA-EX 参加者(データ受領)が、認証情報を受領する。
 - ・ データ取得リクエスト
 - DATA-EX 参加者(データ受領)が、DATA-EX 参加者(データ提供)に認証情報を含めたデータ取得リクエストを送信する。
 - データ取得リクエストを送信するにあたって、DATA-EX 運営事業者に認証情報の取得とコネクタロケーションの解決をリクエストし、コネクタ間の真正性を証明する。
 - ◇ 受領側コネクタにおける認証
 - DATA-EX 参加者(データ受領)が、DATA-EX 運営事業者に認証情報を送付する。
 - DATA-EX 運営事業者が、認証情報の正当性を確認する。
 - DATA-EX 運営事業者が、DATA-EX 参加者(データ受領)に確認結果を送付する。
 - DATA-EX 参加者(データ受領)が、確認結果を受領する。
 - ◇ コネクタロケーション取得
 - DATA-EX 参加者(データ受領)が、DATA-EX 運営事業者に提供側のコネクタロケーションの送付を依頼する。
 - DATA-EX 運営事業者が、DATA-EX 参加者(データ受領)にコネクタロケーションを送付する。
 - DATA-EX 参加者(データ受領)が、コネクタロケーションを受領する。
 - ◇ 受領側コネクタと提供側コネクタの真正性証明
 - DATA-EX 参加者(データ受領)が、提供側コネクタの証明書情報の正当性を確認する。
 - DATA-EX 参加者(データ提供)が、受領側コネクタの証明書情報の正当性を確認する。
 - ・ データ取得リクエスト受領
 - DATA-EX 参加者(データ提供)が、データ取得リクエストを受領する。
 - ・ 提供側コネクタにおける認証・認可
 - DATA-EX 参加者(データ提供)が、DATA-EX 運営事業者に受領側の認証情報を送付する。
 - DATA-EX 運営事業者が、受領側の認証情報の正当性を確認する。
 - DATA-EX 運営事業者が、DATA-EX 参加者(データ提供)に確認結果を送付する。
-

-
- DATA-EX 参加者(データ提供)が、受領側に DDP にアクセスする権限があるか確認する。
 - ・ DDP 受領
 - DATA-EX 参加者(データ提供)が、DDP ID をもとに、DDP の格納先ストレージの URL を取得する。
 - DATA-EX 参加者(データ提供)が、DATA-EX 運営事業者に送信履歴の登録を依頼する。
 - DATA-EX 運営事業者が、DATA-EX 参加者(データ提供)からの送信履歴の登録依頼を受け付ける。
 - DATA-EX 運営事業者が、履歴を登録する。
 - DATA-EX 運営事業者が、履歴 ID を DATA-EX 参加者(データ提供)へ伝達する。
 - DATA-EX 参加者(データ提供)が履歴 ID を受領する。
 - DATA-EX 参加者(データ提供)が、DATA-EX 参加者(データ受領)にストレージの DDP と送信履歴の履歴 ID を送付する。
 - DATA-EX 参加者(データ受領)が、DATA-EX 参加者(データ提供)からの DDP と送信履歴の履歴 ID を受信する。
 - DATA-EX 参加者(データ受領)が、受け取った DDP の e シールを検証する。
 - DATA-EX 参加者(データ受領)が、DATA-EX 運営事業者に e シール作成者が DATA-EX に参加していることの確認を依頼する。
 - DATA-EX 運営事業者が、e シール作成者が DATA-EX 参加者であることの確認結果を送付する。
 - DATA-EX 参加者(データ受領)が、DATA-EX 運営事業者に受信履歴の登録を依頼する。
 - DATA-EX 運営事業者が、履歴を登録する。
 - DATA-EX 運営事業者が、履歴 ID を DATA-EX 参加者(データ受領)へ伝達する。
 - DATA-EX 参加者(データ受領)が履歴 ID を受領する。

8-1-2-5. DDP 削除

DDP 削除は、DATA-EX 参加者（データ提供・データ受領）が、利用目的がなくなった DDP を削除する作業である。

なお、DDP の削除については、DATA-EX 参加者（データ提供・データ受領）の任意、もしくは DATA-EX 参加者同士での契約内容・利用条件に基づいて行われるものとする。

- ・ データ提供側の DDP 削除
 - DATA-EX 参加者（データ提供）が削除対象の DDP に対する認可を削除する。
 - DATA-EX 参加者（データ提供）が削除対象の DDP に対するロケーションを削除する。
 - DATA-EX 参加者（データ提供）が、DDP をストレージから削除する。
- ・ データ受領側の DDP 削除
 - DATA-EX 参加者（データ受領）が、DDP をストレージから削除する。

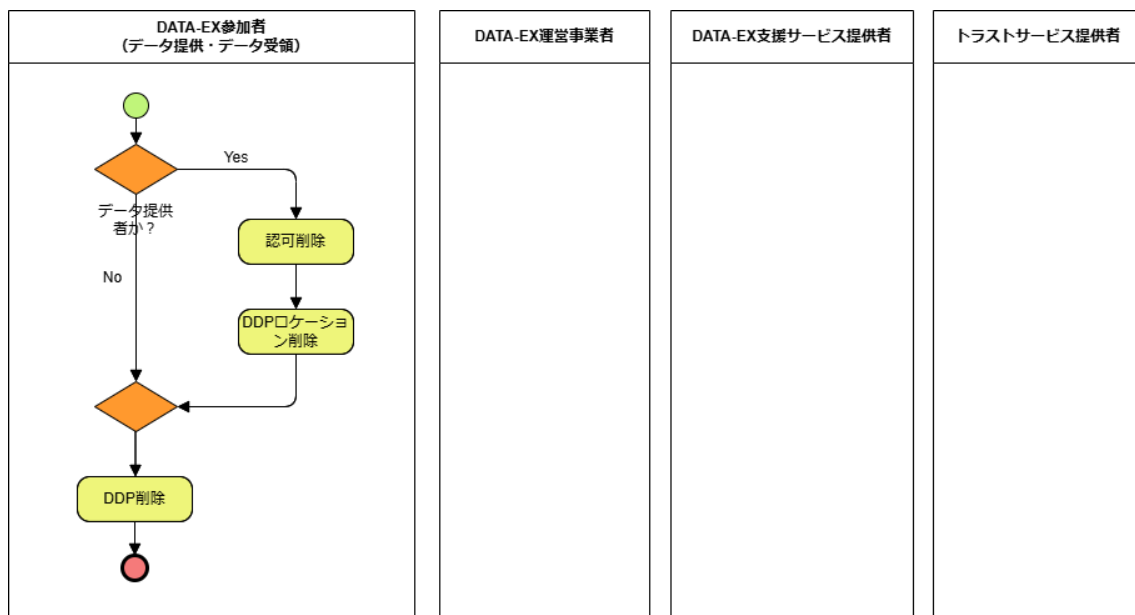


図 12: DDP 削除の概要図

8-1-2-6. 来歴確認

来歴確認は、DATA-EX 参加者が自身に関する DDP 情報の来歴を確認するために必要な一連の作業である。

- ・ 来歴情報提供
 - DATA-EX 参加者が、DATA-EX 運営事業者到来歴情報の提供を依頼する。
 - DATA-EX 運営事業者が、DATA-EX 参加者に来歴情報を提供する。
 - DATA-EX 参加者が、来歴情報を受領する。

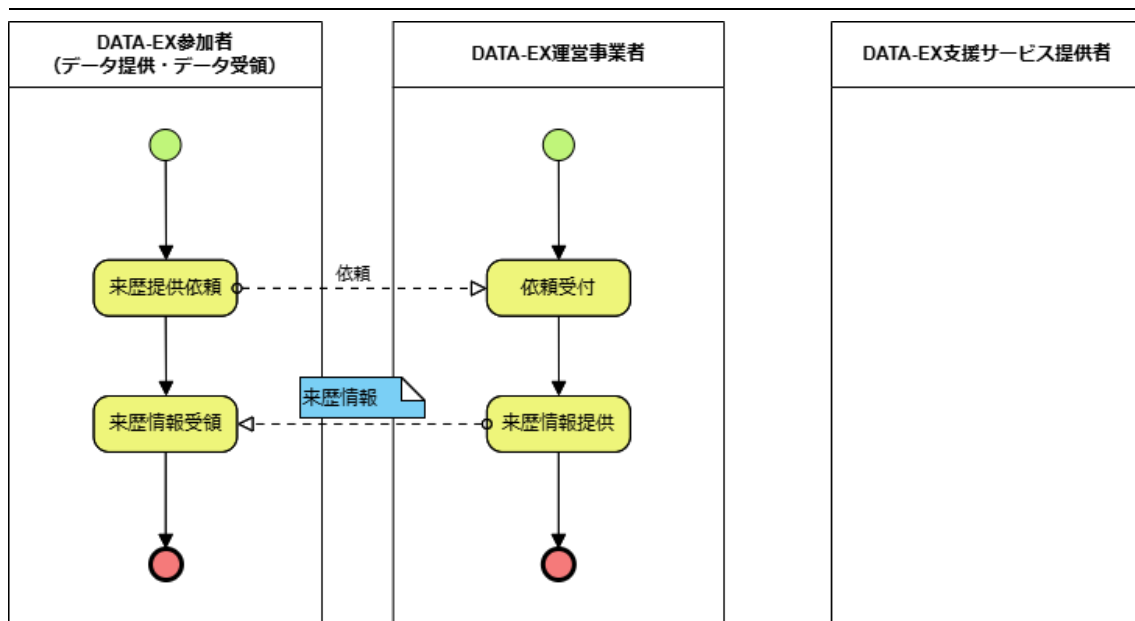


図 13: 来歴確認の概要図

8-1-2-7. カタログ削除

カタログ削除は、DATA-EX 参加者（データ提供）が、カタログサイトそのものを削除するために必要な一連の作業である。横断検索カタログサイト上の登録を削除し、DATA-EX 参加者（データ提供）のカタログサイトを削除する手順となる。

- ・ 横断検索サイト登録解除
 - DATA-EX 参加者（データ提供）が、ポータルサイトを閲覧し、登録解除依頼先の URL を確認する。
 - DATA-EX 参加者（データ提供）が、横断検索サイトにカタログサイトの登録解除を依頼する。
 - DATA-EX 参加者が、外部 IdP を利用しない場合、以下の作業を実施する。
 - ✧ DATA-EX 支援サービス提供者が、申請者の認証を DATA-EX 運営事業者に依頼する。
 - ✧ DATA-EX 運営事業者が申請者の認証を行う。
 - ✧ DATA-EX 支援サービス提供者が、申請者の属性情報を含む認証結果を受け取る。
 - DATA-EX 参加者が、外部 IdP を利用する場合、以下の作業を実施する。
 - ✧ DATA-EX 支援サービス提供者が、申請者の認証を外部 IdP に依頼する。
 - ✧ 外部 IdP が申請者の認証を行う。
 - ✧ DATA-EX 支援サービス提供者が、申請者の属性情報を含む認証結果を受け取る。
 - DATA-EX 支援サービス提供者が、解除依頼の内容を審査する。

- DATA-EX 支援サービス提供者が、カタログサイトのクローリングを停止する。
- DATA-EX 支援サービス提供者が、横断検索サイトのカタログを削除する。
- DATA-EX 支援サービス提供者が、横断検索サイトにカタログが表示されないことを確認する。
- DATA-EX 支援サービス提供者が、依頼者にカタログサイトの解除が完了したことを通知する。
- DATA-EX 参加者（データ提供）が、解除完了通知を受領する。
- ・ カタログ削除
 - DATA-EX 参加者（データ提供）が、カタログサイトを削除する。

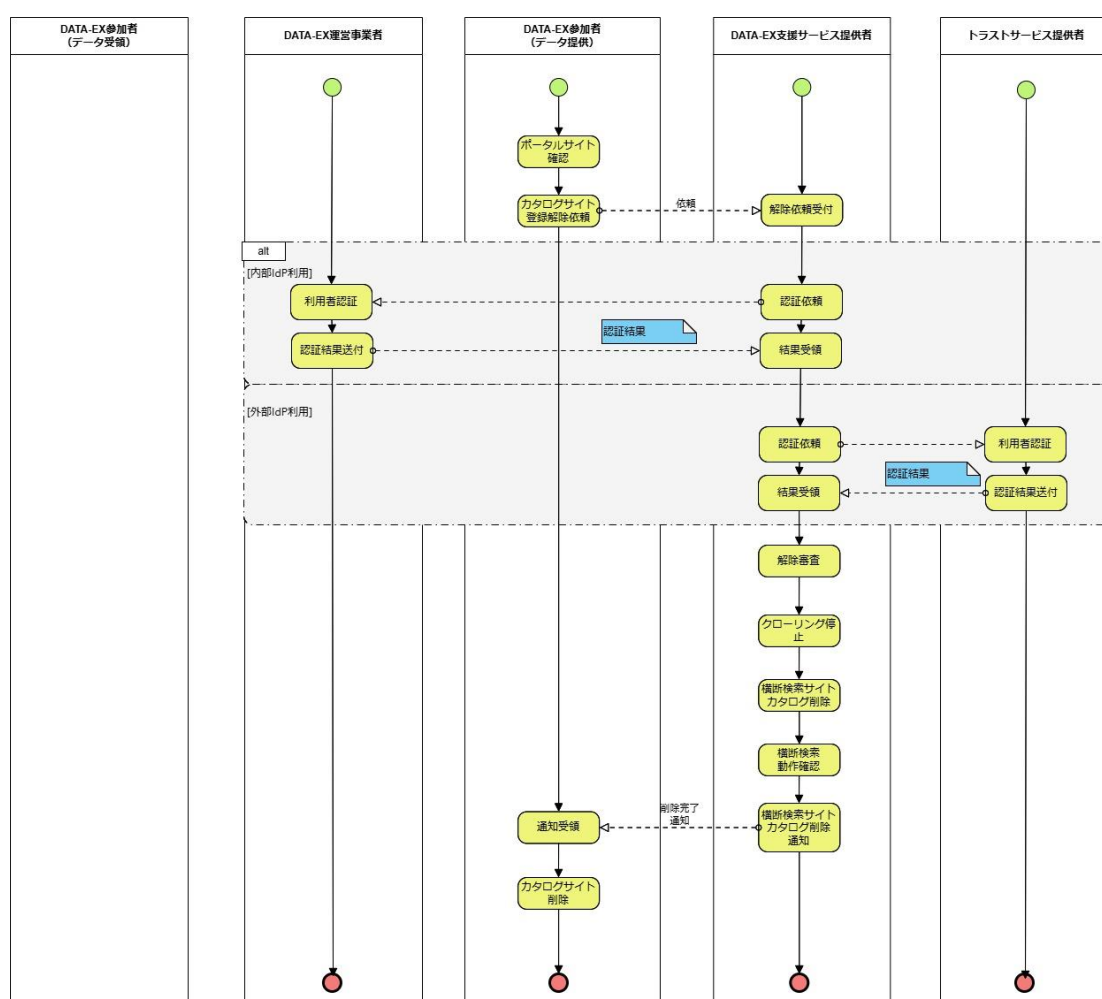


図 14: カタログ削除の概要図

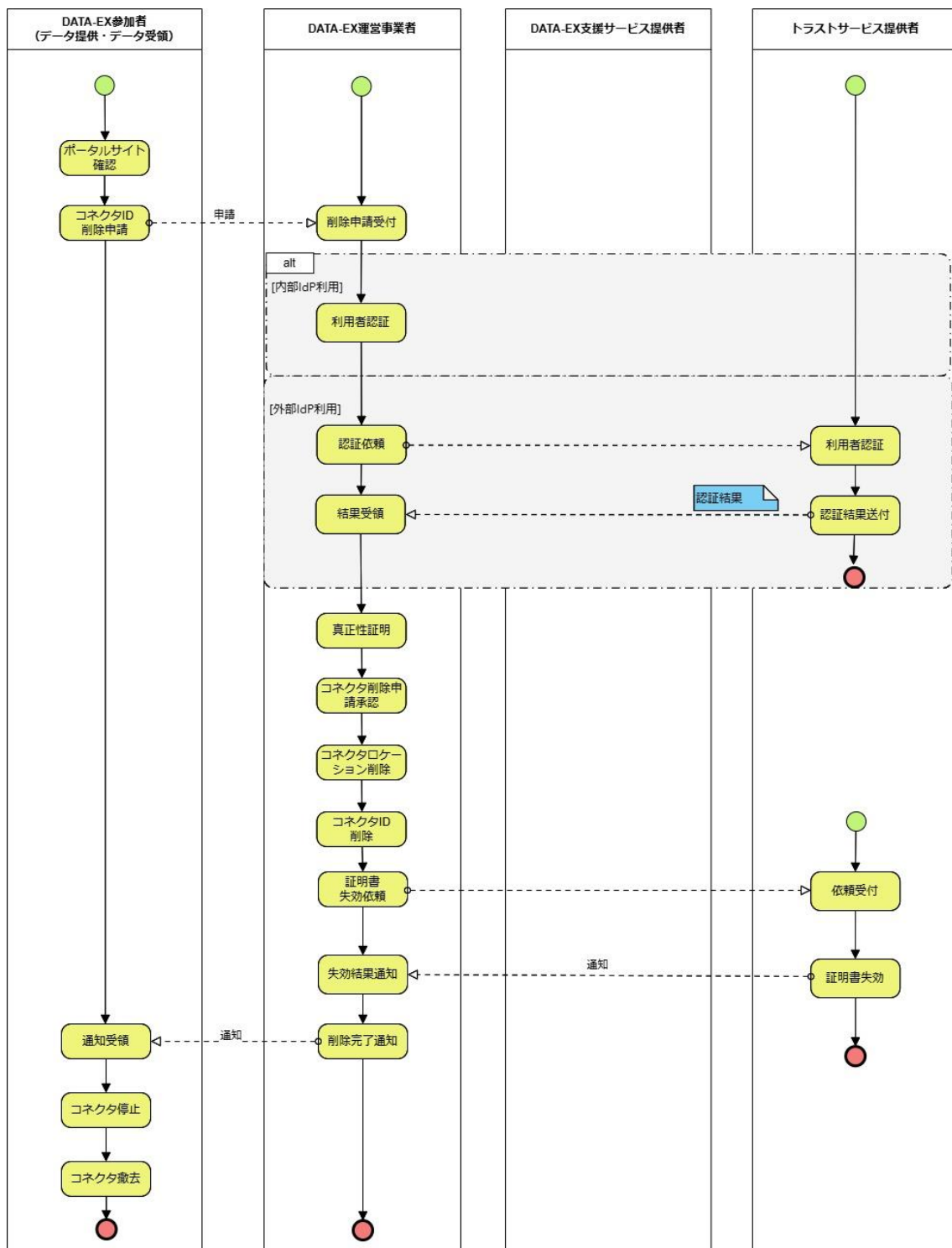
8-1-3. 利用停止

利用停止は、DATA-EX 参加者が DATA-EX の利用を停止する前に実施する一連の作業(コネクタ撤廃、退会)である。

8-1-3-1. コネクタ撤廃

コネクタ撤廃は、DATA-EX 参加者がコネクタの利用を終了するために必要な一連の作業である。

- ・ コネクタ削除
 - DATA-EX 参加者が、ポータルサイトを閲覧し、申請先の URL を確認する。
 - DATA-EX 参加者が、DATA-EX 運営事業者のコネクタ ID の削除を申請する。
 - DATA-EX 参加者が、外部 IdP を利用しない場合、以下の作業を実施する。
 - ◇ DATA-EX 運営事業者が申請者の認証を行う。
 - DATA-EX 参加者が、外部 IdP を利用する場合、以下の作業を実施する。
 - ◇ DATA-EX 運営事業者が、申請者の認証を外部 IdP に依頼する。
 - ◇ 外部 IdP が申請者の認証を行う。
 - ◇ DATA-EX 運営事業者が、申請者の属性情報を含む認証結果を受け取る。
 - DATA-EX 運営事業者が、申請者が本人であることを確認する。
 - DATA-EX 運営事業者が、申請内容を確認し、コネクタ削除申請を承認する。
 - DATA-EX 運営事業者が、コネクタロケーションを削除する。
 - DATA-EX 運営事業者が、申請者のアカウントからコネクタ ID を削除する。
 - DATA-EX 運営事業者が、認証局にコネクタの電子証明書の失効を依頼する。
 - 認証局が、コネクタの電子証明書の失効を行う。
 - DATA-EX 運営事業者が、申請者にコネクタロケーションとコネクタ ID の削除が完了したことを通知する。
 - DATA-EX 参加者が、削除完了通知を受領する。
- ・ コネクタ停止
 - DATA-EX 参加者が、コネクタを停止する。
 - DATA-EX 参加者が、コネクタを撤去する。



8-1-3-2. 退会

退会は、DATA-EX 参加者が DATA-EX の利用を終了するために必要な一連の作業である。

- ・ 退会処理

- DATA-EX 参加者が、ポータルサイトを閲覧し、申請先の URL を確認する。
- DATA-EX 参加者が、DATA-EX 運営事業者に退会申請する。
- DATA-EX 参加者が、外部 IdP を利用しない場合、以下の作業を実施する。
 - ◇ DATA-EX 運営事業者が申請者の認証を行う。
- DATA-EX 参加者が、外部 IdP を利用する場合、以下の作業を実施する。
 - ◇ DATA-EX 運営事業者が、申請者の認証を外部 IdP に依頼する。
 - ◇ 外部 IdP が申請者の認証を行う。
 - ◇ DATA-EX 運営事業者が、申請者の属性情報を含む認証結果を受け取る。
- DATA-EX 運営事業者が、申請者が本人であることを確認する。
- DATA-EX 運営事業者が、退会申請内容を審査する。
- DATA-EX 運営事業者が、DATA-EX アカウントの無効化処理を実施する。
- DATA-EX 運営事業者が、申請者に退会処理が完了したことを通知する。
- DATA-EX 参加者が、退会処理完了通知を受領する。

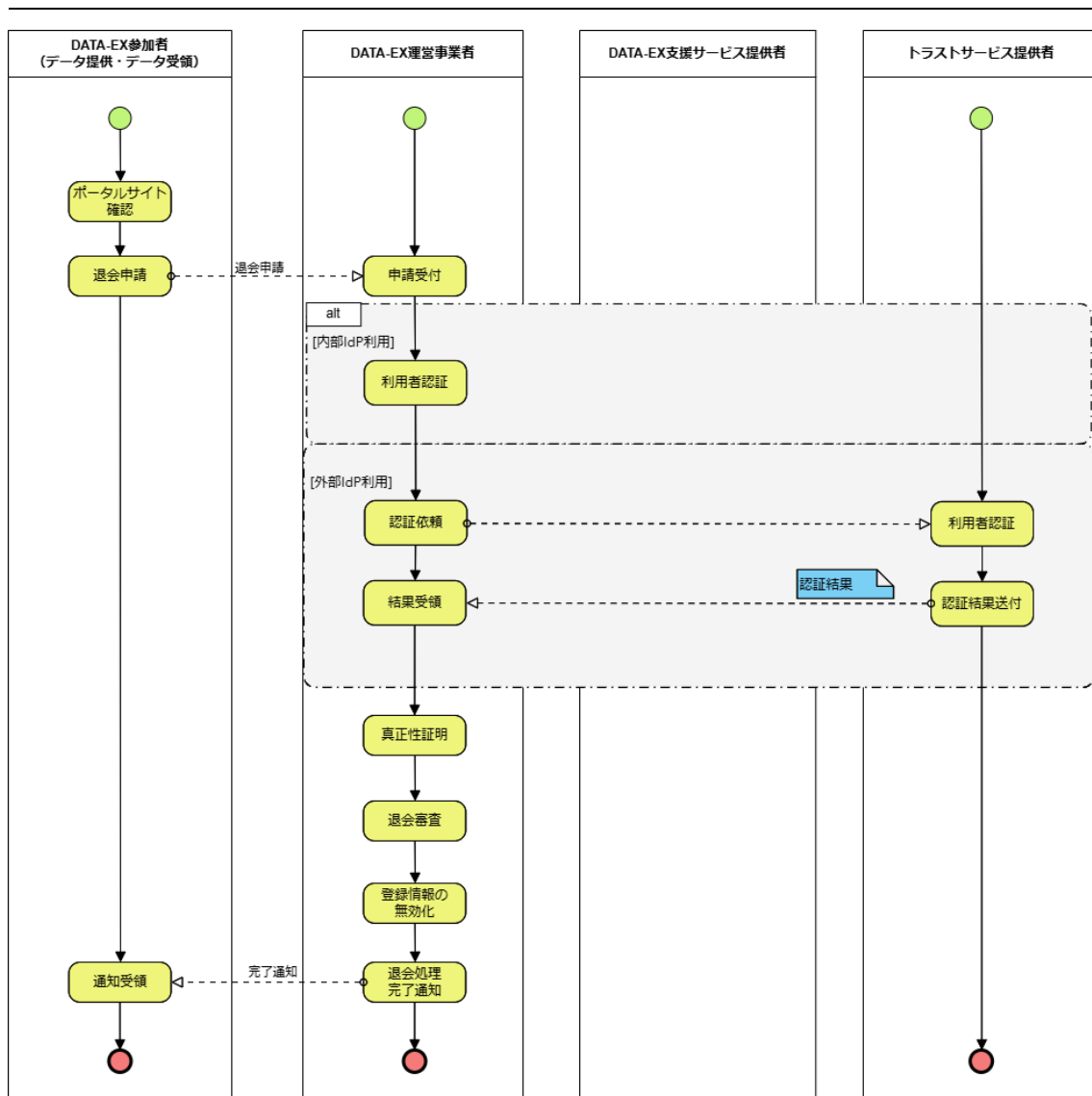


図 16: 退会の概要図

8-2. 相対取引によって契約を交わし、データ交換を行う

8-2-1. 利用準備

利用準備は、DATA-EX 参加者が DATA-EX を利用する前に実施する一連の作業(利用申請、コネクタ構築)である。

8-2-1-1. 利用申請

利用申請は、DATA-EX 参加者が DATA-EX の利用を開始するために必要な一連の作業である。

- ・ 登録準備
 - DATA-EX 参加者が、外部 IdP を利用する場合、以下の作業を実施する。

-
- ◇ DATA-EX 参加者が、外部 IdP に事前登録申請を依頼する。
 - ◇ 外部 IdP が、申請者が本人であることの身元確認を行う。
 - ◇ 外部 IdP と申請者間で、認証に必要な認証クレデンシャル(パスワード等)を設定する。
 - DATA-EX 参加者が、ポータルサイトを閲覧し、DATA-EX 利用解説書を取得する。
 - DATA-EX 参加者が、コネクタ構築に必要な環境(デバイス、認可サーバー、ストレージ、など)を準備する。
 - DATA-EX 参加者(データ提供)が、カタログサイトを構築する。
 - DATA-EX 参加者が、ポータルサイトを閲覧し、申請先の URL を確認する。
 - DATA-EX 参加者が、DATA-EX 運営事業者に DATA-EX の利用申請をする。
 - ・ 登録
 - DATA-EX 参加者が、外部 IdP を利用しない場合、以下の作業を実施する。
 - ◇ DATA-EX 運営事業者が、申請者が本人であることの身元確認を行う。
 - DATA-EX 参加者が、外部 IdP を利用する場合、以下の作業を実施する。
 - ◇ DATA-EX 運営事業者が、申請者の認証を外部 IdP に依頼する。
 - ◇ 外部 IdP が申請者の認証を行う。
 - ◇ DATA-EX 運営事業者が、申請者の属性を含む認証結果を受け取る。
 - ◇ DATA-EX 運営事業者が、申請者が本人であることを確認する。
 - DATA-EX 運営事業者が、申請内容を審査する。
 - DATA-EX 参加者が、外部 IdP を利用しない場合、以下の作業を実施する。
 - ◇ DATA-EX 運営事業者と申請者間で、認証に必要な認証クレデンシャル(パスワード等)を設定する。
 - DATA-EX 運営事業者が、アカウント(DATA-EX ID など)とコネクタ設定(コネクタ ID など)を発行する。(DATAEX-ID、コネクタ ID の一意性を保証)
 - DATA-EX 運営事業者が、申請者が組織に属している場合、所属する DATA-EX 参加組織に対し DATA-EX ID を発行する。
 - ・ アカウント・コネクタ設定取得
 - DATA-EX 運営事業者が、DATA-EX 参加者にアカウントとコネクタ設定を送付する。
 - DATA-EX 参加者が、アカウントとコネクタ設定を受領する。
 - ・ 支援サービス利用登録
 - DATA-EX 参加者が、DATA-EX 支援サービス提供者に支援サービスの利用申請をする。
 - DATA-EX 参加者が、外部 IdP を利用しない場合、以下の作業を実施する。
 - ◇ DATA-EX 支援サービス提供者が、申請者の認証を DATA-EX 運営事業者に依頼する。
 - ◇ DATA-EX 運営事業者が申請者の認証を行う。
-

-
- ◇ DATA-EX 支援サービス提供者が、申請者の属性情報を含む認証結果を受け取る。
 - DATA-EX 参加者が、外部 IdP を利用する場合、以下の作業を実施する。
 - ◇ DATA-EX 支援サービス提供者が、申請者の認証を外部 IdP に依頼する。
 - ◇ 外部 IdP が申請者の認証を行う。
 - ◇ DATA-EX 支援サービス提供者が、申請者の属性情報を含む認証結果を受け取る。
 - DATA-EX 支援サービス提供者が、申請内容を審査し、支援サービスの利用を許可する。

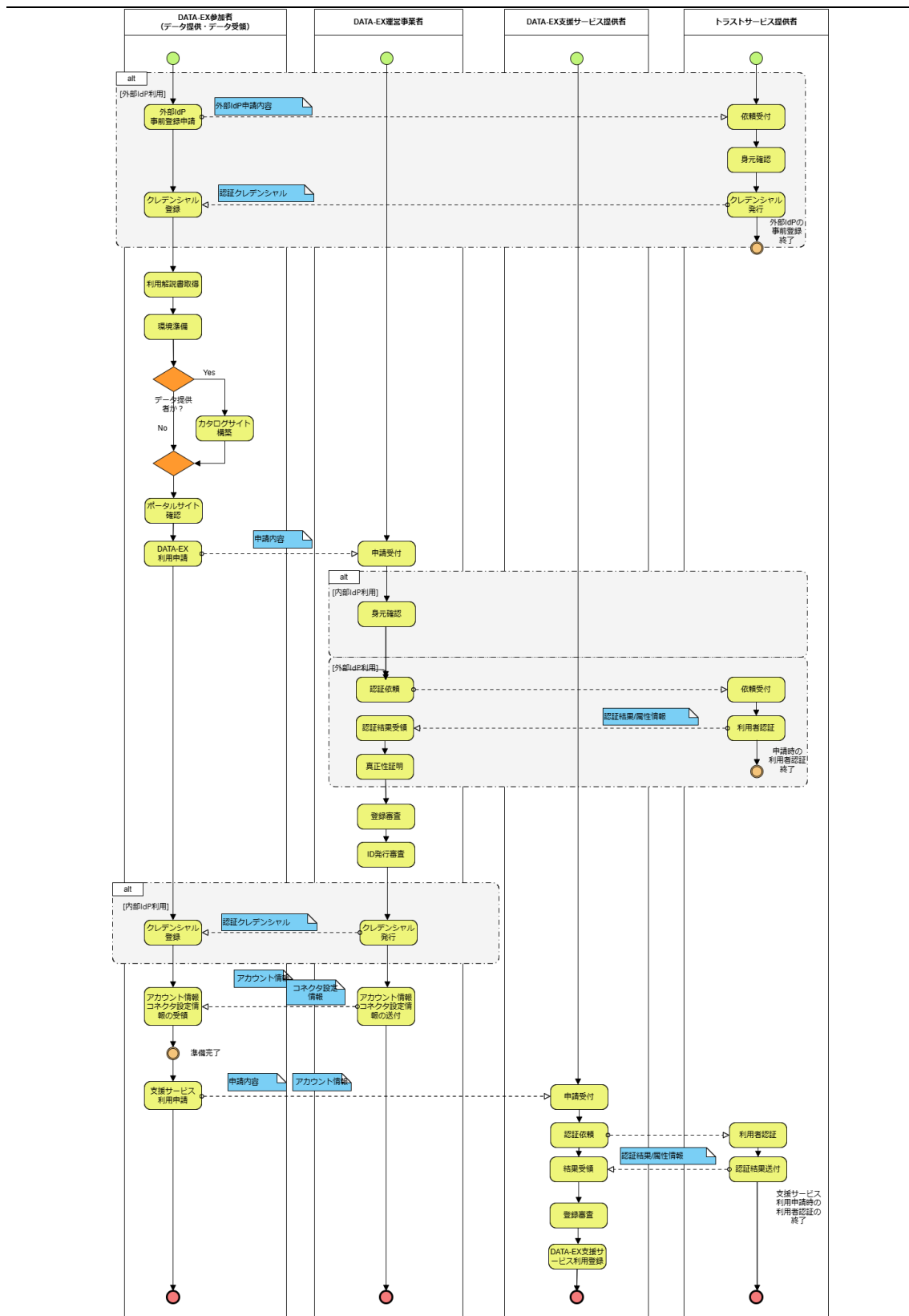


図 17: 利用申請の概要図

8-2-1-2. コネクタ構築

コネクタ構築は、DATA-EX 参加者が DATA-EX 上でコネクタを介した通信を行うために必要な一連の作業である。

- ・ コネクタ送付
 - DATA-EX 参加者が、ポータルサイトを閲覧し、コネクタ公開サイトの URL を確認する。
 - DATA-EX 参加者が、DATA-EX 運営事業者のコネクタの送付を依頼する。
 - DATA-EX 運営事業者が、DATA-EX 参加者にコネクタを送付する。
 - DATA-EX 参加者が、コネクタを受領する。
 - DATA-EX 参加者が、コネクタを構築し、コンフィグ情報を設定する。
- ・ コネクタの電子証明書発行
 - DATA-EX 参加者が、DATA-EX 運営事業者のコネクタの電子証明書発行を申請する。
 - DATA-EX 運営事業者が、コネクタの電子証明書発行申請を受け付ける。
 - DATA-EX 運営事業者が、認証局にコネクタの電子証明書の発行を依頼する。
 - 認証局が、コネクタの電子証明書を発行し、DATA-EX 運営事業者のコネクタの電子証明書を送付する。
 - DATA-EX 運営事業者が認証局で発行されたコネクタの電子証明書を配付する。
 - DATA-EX 参加者が、コネクタの電子証明書を受領する。
- ・ コネクタ起動
 - DATA-EX 参加者が、コネクタを起動する。
 - DATA-EX 参加者が、DATA-EX 運営事業者のコネクタ ID と申請者のロケーションの紐づけ登録を依頼する。
 - DATA-EX 運営事業者が、申請者のコネクタの真正性およびコネクタ ID の一意性を確認し、コネクタ ID と申請者のロケーションの紐づけを登録する。
 - DATA-EX 運営事業者が、DATA-EX 参加者にコネクタ ID と申請者のロケーションの紐づけ登録が完了したことを通知する。
 - DATA-EX 参加者が、DATA-EX 運営事業者からのコネクタ ID と申請者のロケーションの紐づけ登録完了通知を受領する。
 - DATA-EX 運営事業者が、コネクタの疎通テスト環境を提供する。
 - DATA-EX 参加者が、コネクタと DATA-EX が接続できることを確認する。

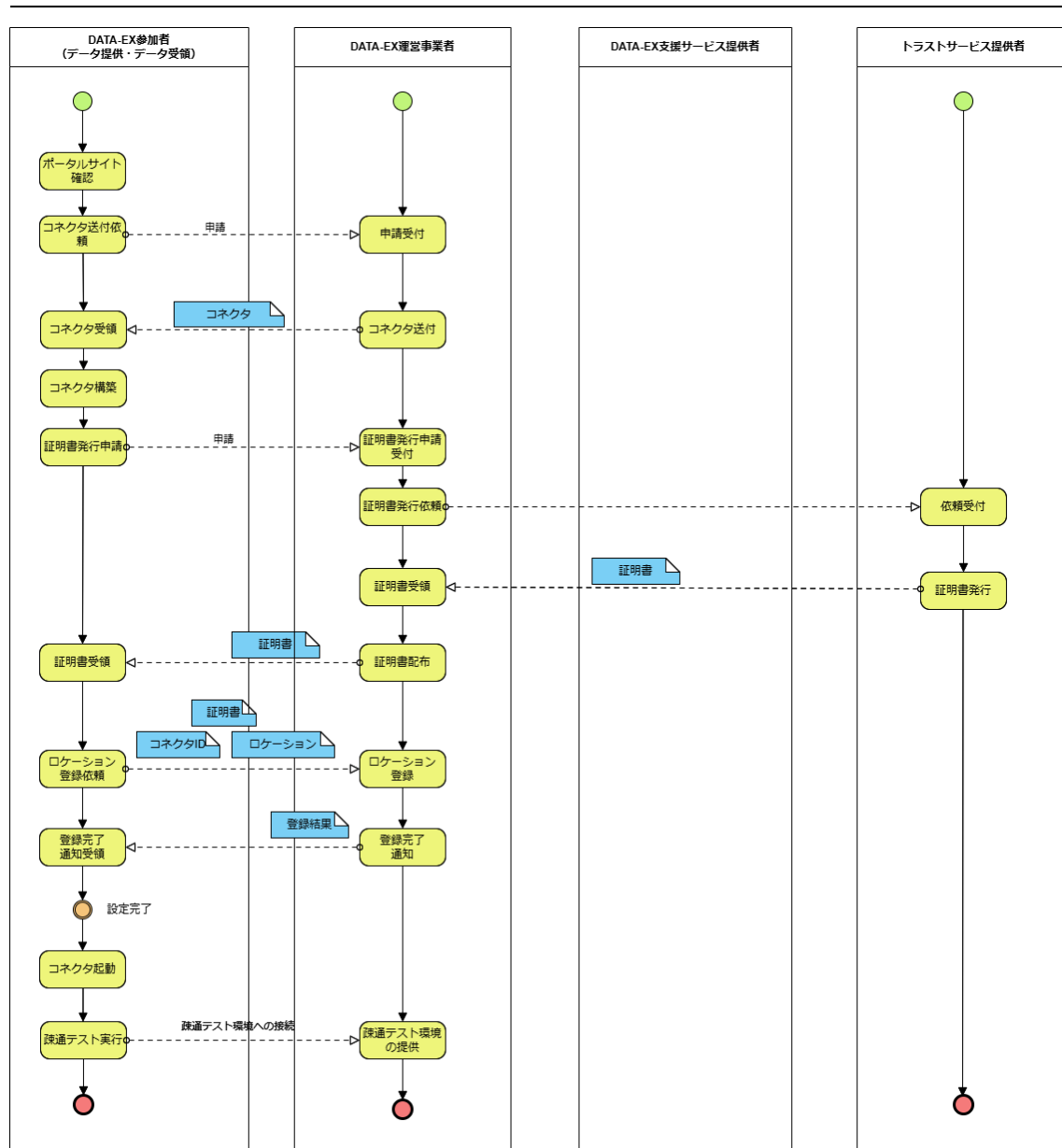


図 18:コネクタ構築の概要図

8-2-2. 利用

利用は、DATA-EX 参加者が DATA-EX を利用する際に行う一連の作業（データセット用意、データセット発見、契約・DDP 作成、DDP 授受、語彙リポジトリ登録、語彙リポジトリ参照、来歴確認、DDP 削除、データセット削除）である。

8-2-2-1. カタログ用意

カタログ用意は、DATA-EX 参加者（データ提供）が DATA-EX 上で提供するデータセットを用意するために必要な一連の作業である。

- ・ 横断検索サイト登録

-
- DATA-EX 参加者(データ提供)が、ポータルサイトを閲覧し、登録依頼先の URL を確認する。
 - DATA-EX 参加者(データ提供)が、横断検索サイトにカタログサイトの登録を依頼する。
 - DATA-EX 参加者が、外部 IdP を利用しない場合、以下の作業を実施する。
 - ✧ DATA-EX 支援サービス提供者が、申請者の認証を DATA-EX 運営事業者に依頼する。
 - ✧ DATA-EX 運営事業者が申請者の認証を行う。
 - ✧ DATA-EX 支援サービス提供者が、申請者の属性情報を含む認証結果を受け取る。
 - DATA-EX 参加者が、外部 IdP を利用する場合、以下の作業を実施する。
 - ✧ DATA-EX 支援サービス提供者が、申請者の認証を外部 IdP に依頼する。
 - ✧ 外部 IdP が申請者の認証を行う。
 - ✧ DATA-EX 支援サービス提供者が、申請者の属性情報を含む認証結果を受け取る。
 - DATA-EX 支援サービス提供者が、登録内容を審査する。
 - DATA-EX 支援サービス提供者が、横断検索サイトでカタログサイトのクローリングを実施する。
 - DATA-EX 支援サービス提供者が、横断検索サイトにカタログが表示されることを確認する。
 - DATA-EX 支援サービス提供者が、依頼者にカタログサイトの登録が完了したことを通知する。
 - DATA-EX 参加者(データ提供)が、登録完了通知を受領する。
 - ・ カタログ作成
 - DATA-EX 参加者(データ提供)が、データカタログ作成ツールでカタログを作成する。
 - DATA-EX 参加者(データ提供)が、e シールサービスに作成したカタログの e シールの付与を依頼する。
 - e シールサービスが、e シールを生成し、送付する。
 - DATA-EX 参加者(データ提供)が、e シール付きのカタログを作成する。
 - DATA-EX 参加者(データ提供)が、カタログをカタログサイトに登録する。
 - DATA-EX 支援サービス提供者が、定期的にカタログサイトのクローリングを実施する。
-

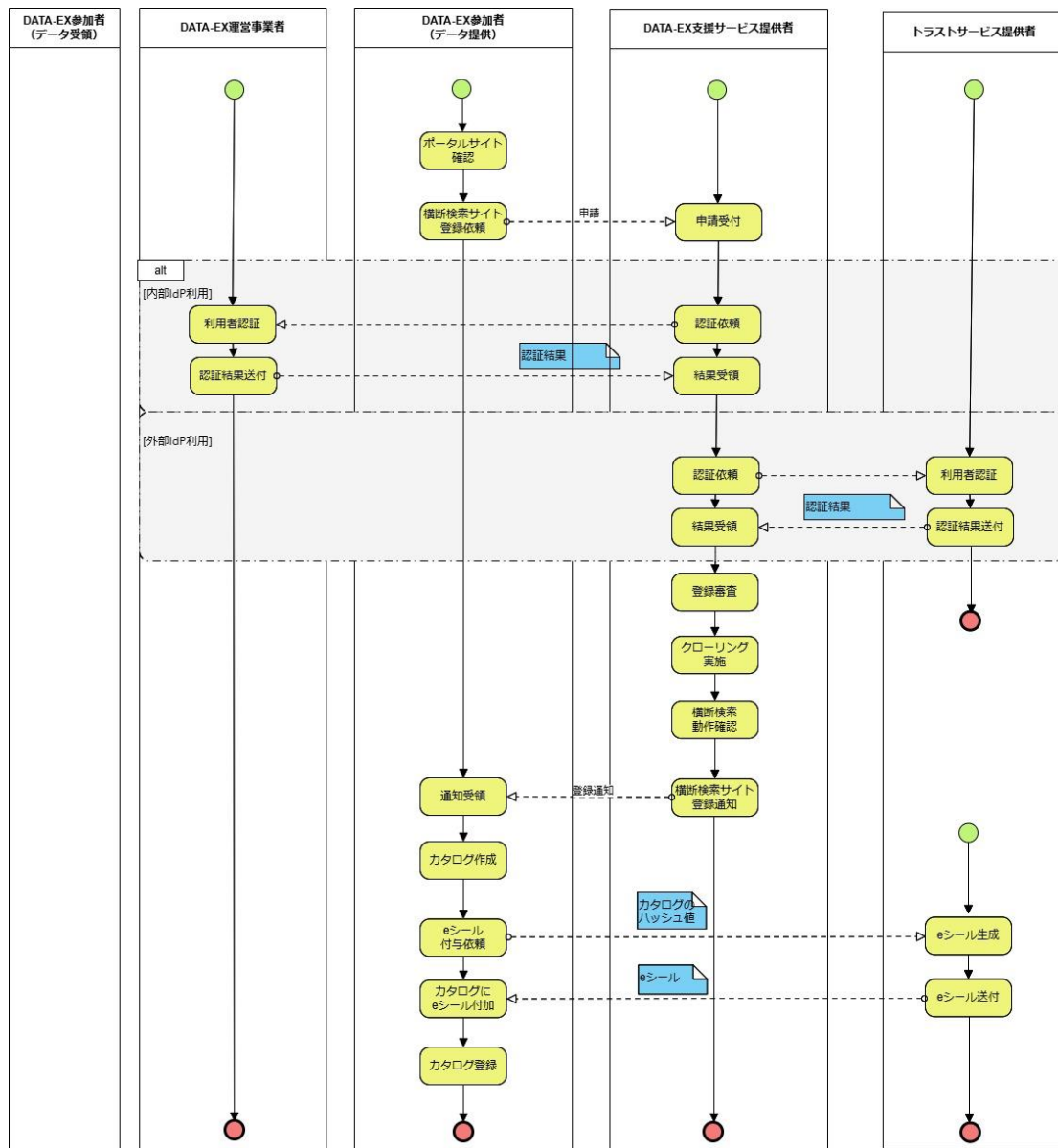


図 19: カタログ用意の概要図

8-2-2-2. データセット発見

データセット発見は、DATA-EX 参加者（データ受領）が DATA-EX 上で提供されるデータセットを発見するために必要な一連の作業である。

- ・ 横断検索サイト利用
 - DATA-EX 参加者（データ受領）が、ポータルサイトを閲覧し、横断検索サイトの URL を確認する。
 - DATA-EX 参加者（データ受領）が、横断検索サイトに検索条件を入力し、検索する。

- DATA-EX 支援サービス提供者が、検索結果（検索条件に合致するカタログ）を送付する。
- DATA-EX 参加者（データ受領）が、横断検索サイト上で検索結果を閲覧する。
- DATA-EX 参加者（データ受領）が、カタログを選択する。
- DATA-EX 参加者（データ提供）が、カタログサイト上のカタログを送付する。
- DATA-EX 参加者（データ受領）が、カタログの e シールを検証する。
- DATA-EX 参加者（データ受領）が、DATA-EX 運営事業者に e シール作成者が DATA-EX に参加していることの確認を依頼する。
- DATA-EX 運営事業者が、e シール作成者が DATA-EX 参加者であることの確認結果を送付する。
- DATA-EX 参加者（データ受領）が、カタログサイト上のカタログを閲覧する。

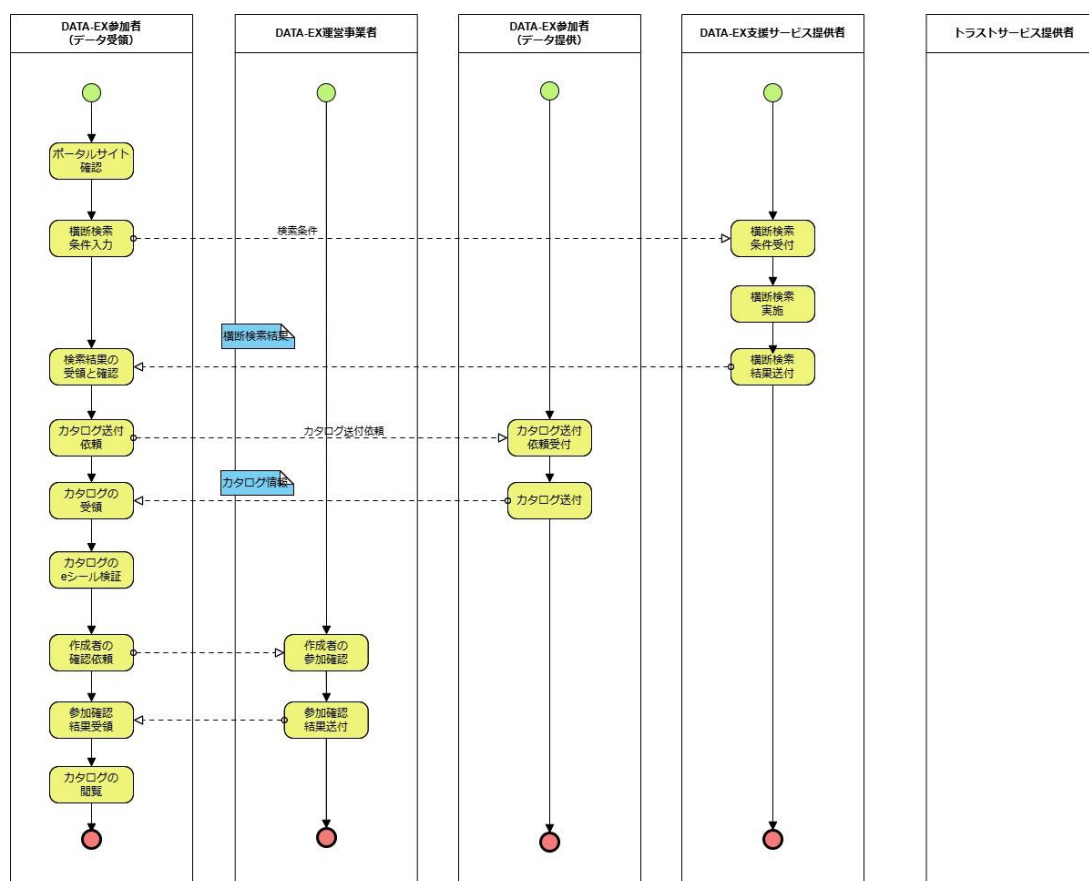


図 20: データセット発見の概要図

8-2-2-3. 契約

契約は、DATA-EX 参加者がデータの提供と便益の交換に関する契約を行うために必要な一連の作業である。

DATA-EX 参加者間において執り行われる契約書などの取り交わしについては、相互の信頼の下に、電子的または一般的な方式にて、相互の認証と真正性を確認した上で行われることが望ましい。電子的な方式として、例えば電子署名など、第三者による電子署名サービスや e シールサービス等を用いて契約を取り交わす場合には、下記の手順に示す方法がある。

- ・ 契約

- DATA-EX 参加者(データ受領)が、DATA-EX 参加者(データ提供)にデータ取得をリクエストする。
- DATA-EX 参加者同士が、取得するデータの範囲や契約条件などについて協議する。
- DATA-EX 参加者(データ提供)が、契約書を作成する。
- DATA-EX 参加者(データ提供)が、電子署名サービスに契約書への電子署名を依頼する。
- 電子署名サービスが契約書への電子署名を生成し、送付する。
- DATA-EX 参加者(データ提供)が、電子署名を受け取る。
- DATA-EX 参加者(データ提供)が、e シールサービスに契約書への e シールの付与を依頼する。
- DATA-EX 参加者(データ提供)が、e シールを受け取る。
- DATA-EX 参加者(データ提供)が、DATA-EX 参加者(データ受領)に契約書を送付する。
- DATA-EX 参加者(データ受領)が、契約内容に合意する。
- DATA-EX 参加者(データ受領)が、電子署名サービスに契約書への電子署名を依頼する。
- 電子署名サービスが契約書への電子署名を生成し、送付する。
- DATA-EX 参加者(データ受領)が、電子署名を受け取る。
- DATA-EX 参加者(データ受領)が、e シールサービスに契約書への e シールの付与を依頼する。
- DATA-EX 参加者(データ受領)が、e シールを受け取る。
- DATA-EX 参加者(データ受領)が、DATA-EX 参加者(データ提供)に契約書を送付する。
- DATA-EX 参加者(データ提供)が、タイムスタンプサービスにタイムスタンプ付与を依頼する。
- タイムスタンプサービスは、タイムスタンプを生成し、送付する。
- DATA-EX 参加者(データ提供)はタイムスタンプを付与した契約書を保存し、DATA-EX 参加者(データ受領)にタイムスタンプ付きの契約書を送付する。

- DATA-EX 参加者（データ受領）が、タイムスタンプ付きの契約書を受け取り、保存する。

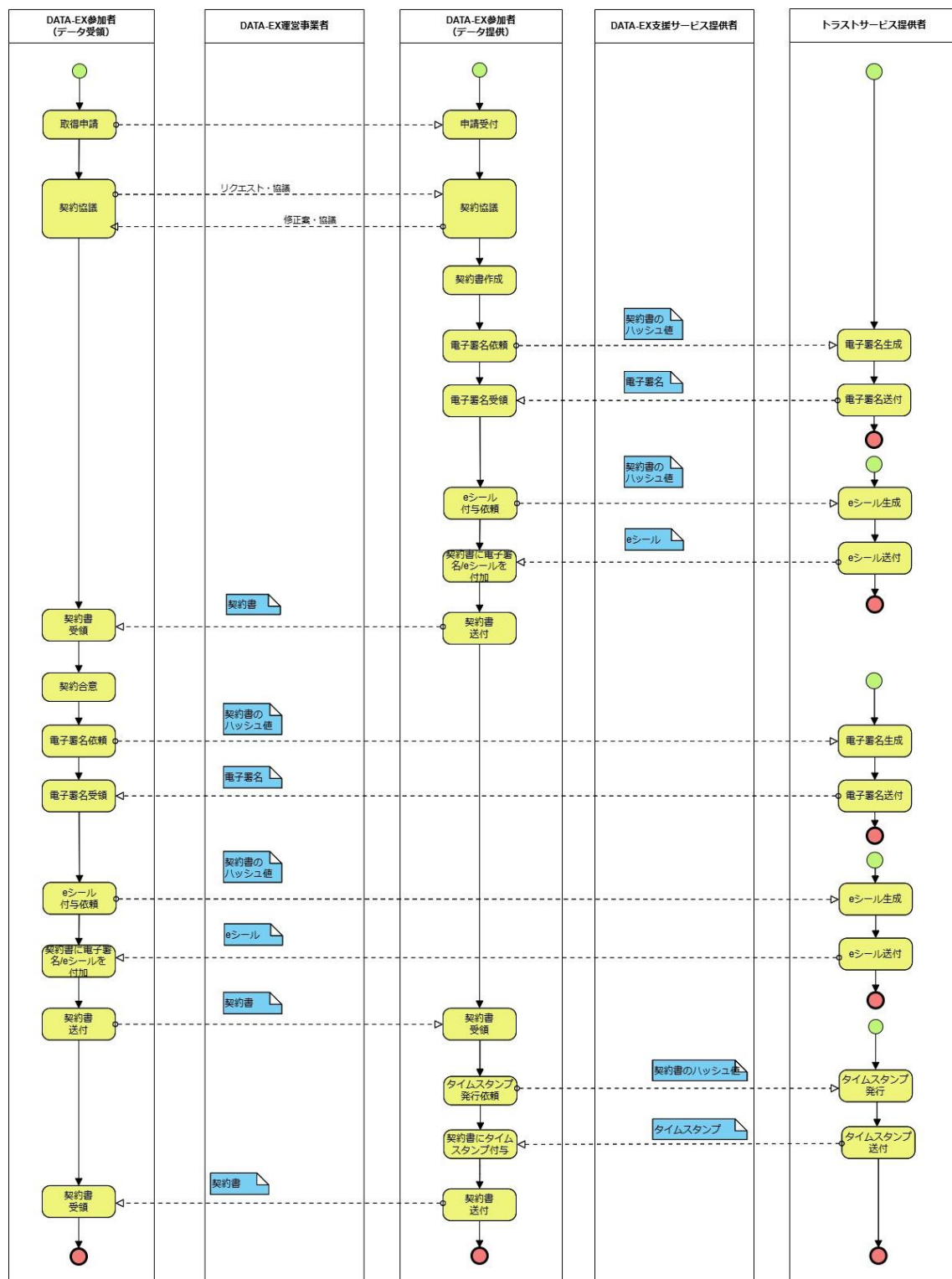
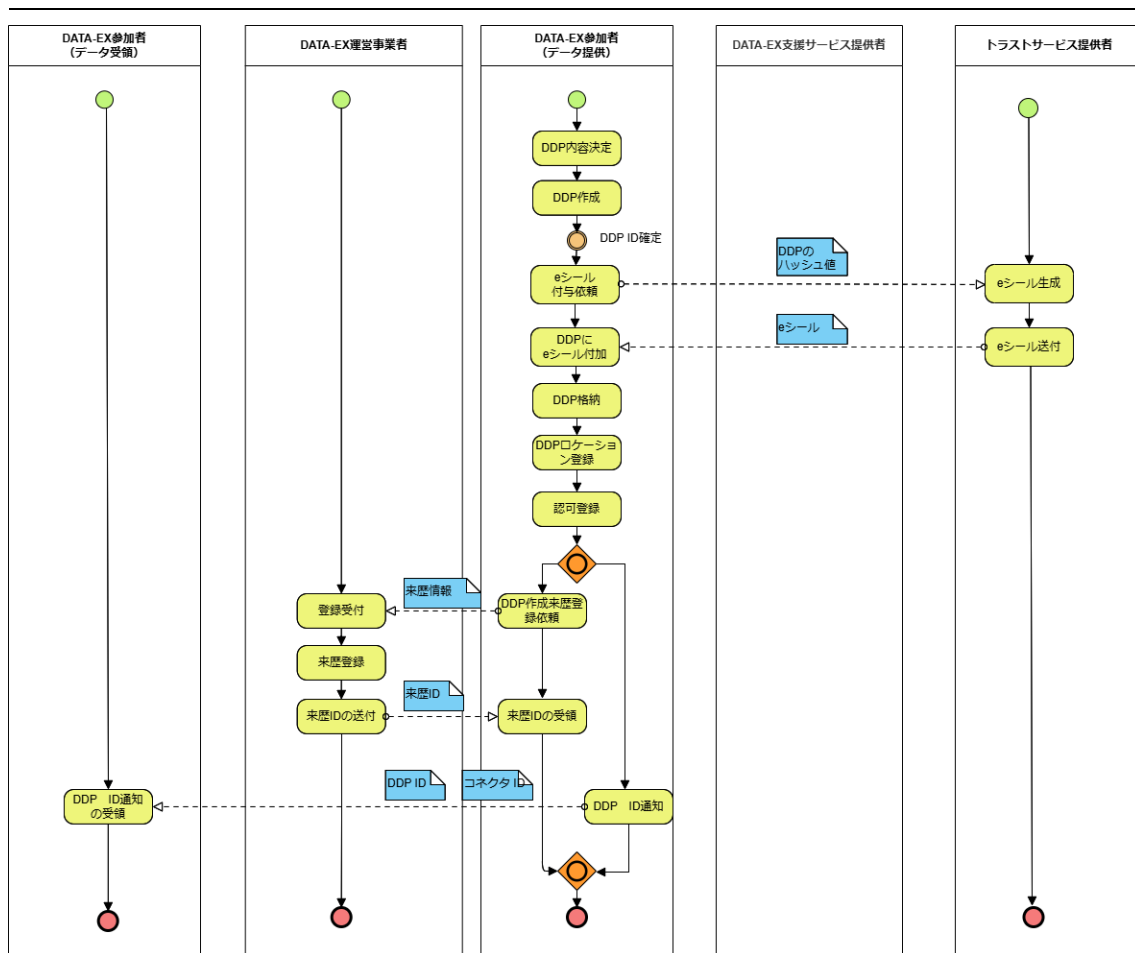


図 21: 契約の概要図

8-2-2-4. DDP 作成

DDP 作成は、DATA-EX 参加者(データ提供)が契約に基づいて DDP を作成し、DDP ID とコネクタ ID を通知するために必要な一連の作業である。

- ・ DDP 作成
 - DATA-EX 参加者(データ提供)が、DDP に含むデータセット・付帯情報・契約情報を決定する。
 - DATA-EX 参加者(データ提供)が、契約をもとに DDP (DDP ID など)を作成する。
 - DATA-EX 参加者(データ提供)が、e シールサービスに DDP への e シールの付与を依頼する。
 - DATA-EX 参加者(データ提供)が、e シールを受け取り、DDP に付加する。
 - DATA-EX 参加者(データ提供)が、配信用のストレージに格納する。
 - DATA-EX 参加者(データ提供)が、DDP ID と DDP のロケーション情報を登録する。
 - DATA-EX 参加者(データ提供)が、DDP の認可情報を登録する。
 - DATA-EX 参加者(データ提供)が、必要に応じて DATA-EX 運営事業者に DDP 作成履歴の登録を依頼する。
 - DATA-EX 運営事業者が、履歴を登録する。
- ・ DDP ID・コネクタ ID 通知
 - DATA-EX 参加者(データ提供)が、DATA-EX 参加者(データ受領)に DDP ID とコネクタ ID を通知する。
 - DATA-EX 参加者(データ受領)が、通知を受領する。



8-2-2-5. データ交換

- ・ 認証情報取得

-
- DATA-EX 参加者(データ受領)が、認証情報を受領する。
 - ・ データ取得リクエスト
 - DATA-EX 参加者(データ受領)が、DATA-EX 参加者(データ提供)に認証情報を含めたデータ取得リクエストを送信する。
 - データ取得リクエストを送信するにあたって、DATA-EX 運営事業者に認証情報の取得とコネクタロケーションの解決をリクエストし、コネクタ間の真正性を証明する。
 - ◇ 受領側コネクタにおける認証
 - DATA-EX 参加者(データ受領)が、DATA-EX 運営事業者に認証情報を送付する。
 - DATA-EX 運営事業者が、認証情報の正当性を確認する。
 - DATA-EX 運営事業者が、DATA-EX 参加者(データ受領)に確認結果を送付する。
 - DATA-EX 参加者(データ受領)が、確認結果を受領する。
 - ◇ コネクタロケーション取得
 - DATA-EX 参加者(データ受領)が、DATA-EX 運営事業者提供側のコネクタロケーションの送付を依頼する。
 - DATA-EX 運営事業者が、DATA-EX 参加者(データ受領)にコネクタロケーションを送付する。
 - DATA-EX 参加者(データ受領)が、コネクタロケーションを受領する。
 - ◇ 受領側コネクタと提供側コネクタの真正性証明
 - DATA-EX 参加者(データ受領)が、提供側コネクタの証明書情報の正当性を確認する。
 - DATA-EX 参加者(データ提供)が、受領側コネクタの証明書情報の正当性を確認する。
 - ・ データ取得リクエスト受領
 - DATA-EX 参加者(データ提供)が、データ取得リクエストを受領する。
 - ・ 提供側コネクタにおける認証・認可
 - DATA-EX 参加者(データ提供)が、DATA-EX 運営事業者受領側の認証情報を送付する。
 - DATA-EX 運営事業者が、受領側の認証情報の正当性を確認する。
 - DATA-EX 運営事業者が、DATA-EX 参加者(データ提供)に確認結果を送付する。
 - DATA-EX 参加者(データ提供)が、受領側に DDP にアクセスする権限があるか確認する。
 - ・ DDP 受領
 - DATA-EX 参加者(データ提供)が、DDP ID をもとに、DDP の格納先ストレージの URL を取得する。
-

-
- DATA-EX 参加者(データ提供)が、DATA-EX 運営事業者に送信履歴の登録を依頼する。
 - DATA-EX 運営事業者が、DATA-EX 参加者(データ提供)からの送信履歴の登録依頼を受け付ける。
 - DATA-EX 運営事業者が、履歴を登録する。
 - DATA-EX 運営事業者が、履歴 ID を DATA-EX 参加者(データ提供)へ伝達する。
 - DATA-EX 参加者(データ提供)が履歴 ID を受領する。
 - DATA-EX 参加者(データ提供)が、DATA-EX 参加者(データ受領)にストレージの DDP と送信履歴の履歴 ID を送付する。
 - DATA-EX 参加者(データ受領)が、DATA-EX 参加者(データ提供)からの DDP と送信履歴の履歴 ID を受信する。
 - DATA-EX 参加者(データ受領)が、受け取った DDP の e シールを検証する。
 - DATA-EX 参加者(データ受領)が、DATA-EX 運営事業者に e シール作成者が DATA-EX に参加していることの確認を依頼する。
 - DATA-EX 運営事業者が、e シール作成者が DATA-EX 参加者であることの確認結果を送付する。
 - DATA-EX 参加者(データ受領)が、DATA-EX 運営事業者に受信履歴の登録を依頼する。
 - DATA-EX 運営事業者が、履歴を登録する。
 - DATA-EX 運営事業者が、履歴 ID を DATA-EX 参加者(データ受領)へ伝達する。
 - DATA-EX 参加者(データ受領)が履歴 ID を受領する。

8-2-2-6. DDP 削除

DDP 削除は、DATA-EX 参加者（データ提供・データ受領）が、利用目的がなくなった DDP を削除する作業である。

なお、DDP の削除については、DATA-EX 参加者（データ提供・データ受領）の任意、もしくは DATA-EX 参加者同士での契約内容・利用条件に基づいて行われるものとする。

- ・ データ提供側の DDP 削除
 - DATA-EX 参加者（データ提供）が削除対象の DDP に対する認可を削除する。
 - DATA-EX 参加者（データ提供）が削除対象の DDP に対するロケーションを削除する。
 - DATA-EX 参加者（データ提供）が、DDP をストレージから削除する。
- ・ データ受領側の DDP 削除
 - DATA-EX 参加者（データ受領）が、DDP をストレージから削除する。

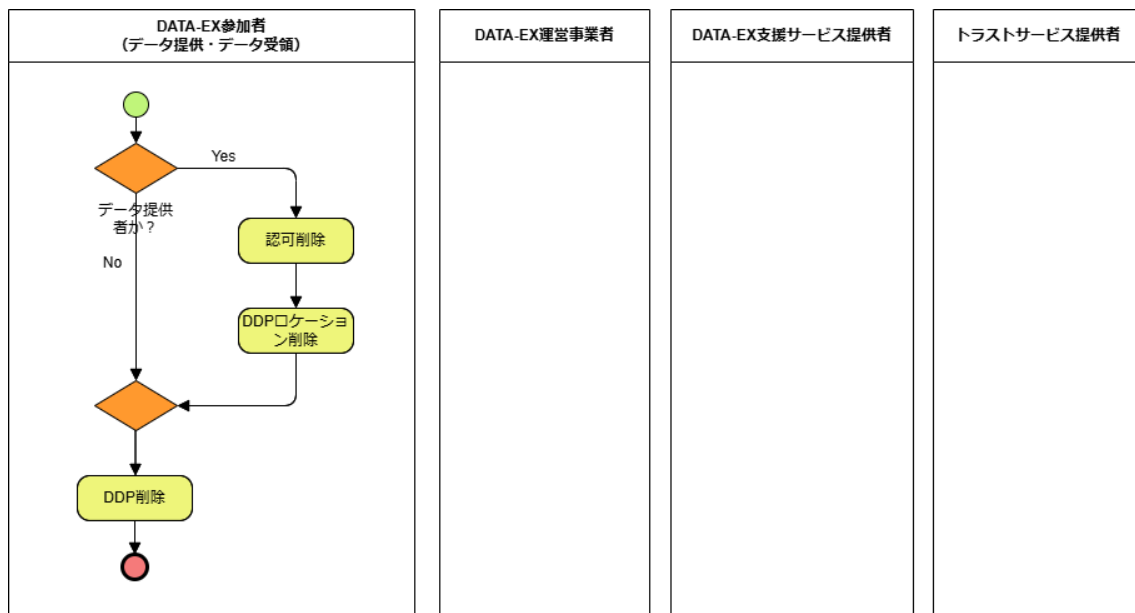


図 24: DDP 削除の概要図

8-2-2-7. 来歴確認

来歴確認は、DATA-EX 参加者が自身に関係する DDP 情報の来歴を確認するために必要な一連の作業である。

- ・ 来歴情報提供
 - DATA-EX 参加者が、DATA-EX 運営事業者到来歴情報の提供を依頼する。
 - DATA-EX 運営事業者が、DATA-EX 参加者に来歴情報を提供する。
 - DATA-EX 参加者が、来歴情報を受領する。

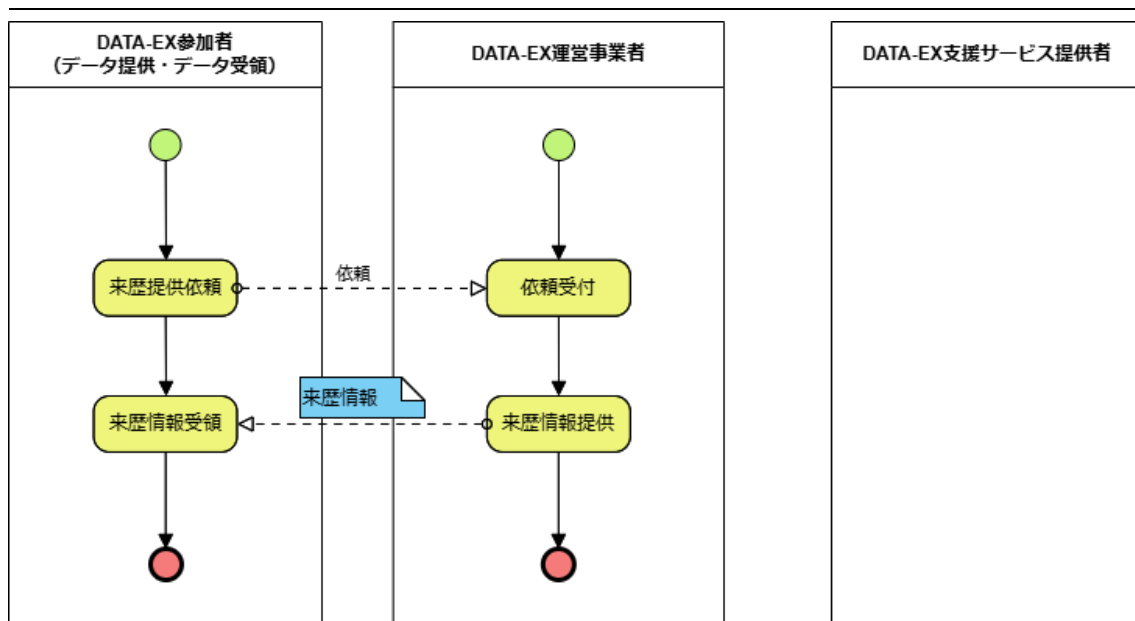


図 25: 来歴確認の概要図

8-2-2-8. カタログ削除

カタログ削除は、DATA-EX 参加者（データ提供）が、カタログサイトそのものを削除するために必要な一連の作業である。横断検索カタログサイト上の登録を削除し、DATA-EX 参加者（データ提供）のカタログサイトを削除する手順となる。

- ・ 横断検索サイト登録解除
 - DATA-EX 参加者（データ提供）が、ポータルサイトを閲覧し、登録解除依頼先の URL を確認する。
 - DATA-EX 参加者（データ提供）が、横断検索サイトにカタログサイトの登録解除を依頼する。
 - DATA-EX 参加者が、外部 IdP を利用しない場合、以下の作業を実施する。
 - ✧ DATA-EX 支援サービス提供者が、申請者の認証を DATA-EX 運営事業者に依頼する。
 - ✧ DATA-EX 運営事業者が申請者の認証を行う。
 - ✧ DATA-EX 支援サービス提供者が、申請者の属性情報を含む認証結果を受け取る。
 - DATA-EX 参加者が、外部 IdP を利用する場合、以下の作業を実施する。
 - ✧ DATA-EX 支援サービス提供者が、申請者の認証を外部 IdP に依頼する。
 - ✧ 外部 IdP が申請者の認証を行う。
 - ✧ DATA-EX 支援サービス提供者が、申請者の属性情報を含む認証結果を受け取る。
 - DATA-EX 支援サービス提供者が、解除依頼の内容を審査する。

- DATA-EX 支援サービス提供者が、カタログサイトのクローリングを停止する。
- DATA-EX 支援サービス提供者が、横断検索サイトのカタログを削除する。
- DATA-EX 支援サービス提供者が、横断検索サイトにカタログが表示されないことを確認する。
- DATA-EX 支援サービス提供者が、依頼者にカタログサイトの解除が完了したことを通知する。
- DATA-EX 参加者（データ提供）が、解除完了通知を受領する。
- ・ カatalog削除
 - DATA-EX 参加者（データ提供）が、カタログサイトを削除する。

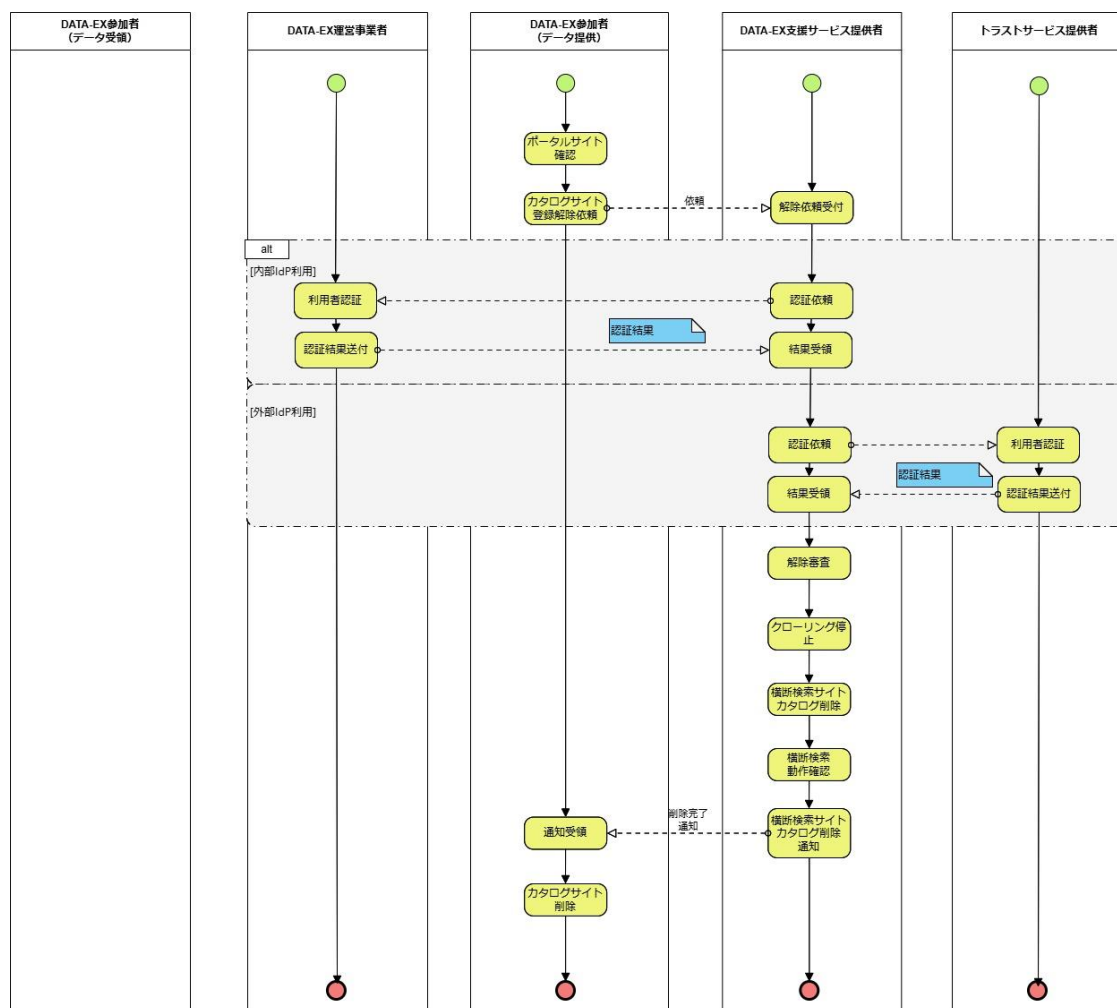


図 26: カatalog削除の概要図

8-2-3. 利用停止

利用停止は、DATA-EX 参加者が DATA-EX の利用を停止する前に実施する一連の作業(コネクタ撤廃、退会)である。

8-2-3-1. コネクタ撤廃

コネクタ撤廃は、DATA-EX 参加者がコネクタの利用を終了するために必要な一連の作業である。

- ・ コネクタ削除
 - DATA-EX 参加者が、ポータルサイトを閲覧し、申請先の URL を確認する。
 - DATA-EX 参加者が、DATA-EX 運営事業者のコネクタ ID の削除を申請する。
 - DATA-EX 参加者が、外部 IdP を利用しない場合、以下の作業を実施する。
 - ◇ DATA-EX 運営事業者が申請者の認証を行う。
 - DATA-EX 参加者が、外部 IdP を利用する場合、以下の作業を実施する。
 - ◇ DATA-EX 運営事業者が、申請者の認証を外部 IdP に依頼する。
 - ◇ 外部 IdP が申請者の認証を行う。
 - ◇ DATA-EX 運営事業者が、申請者の属性情報を含む認証結果を受け取る。
 - DATA-EX 運営事業者が、申請者が本人であることを確認する。
 - DATA-EX 運営事業者が、申請内容を確認し、コネクタ削除申請を承認する。
 - DATA-EX 運営事業者が、コネクタロケーションを削除する。
 - DATA-EX 運営事業者が、申請者のアカウントからコネクタ ID を削除する。
 - DATA-EX 運営事業者が、認証局にコネクタの電子証明書の失効を依頼する。
 - 認証局が、コネクタの電子証明書の失効を行う。
 - DATA-EX 運営事業者が、申請者にコネクタロケーションとコネクタ ID の削除が完了したことを通知する。
 - DATA-EX 参加者が、削除完了通知を受領する。
- ・ コネクタ停止
 - DATA-EX 参加者が、コネクタを停止する。
 - DATA-EX 参加者が、コネクタを撤去する。

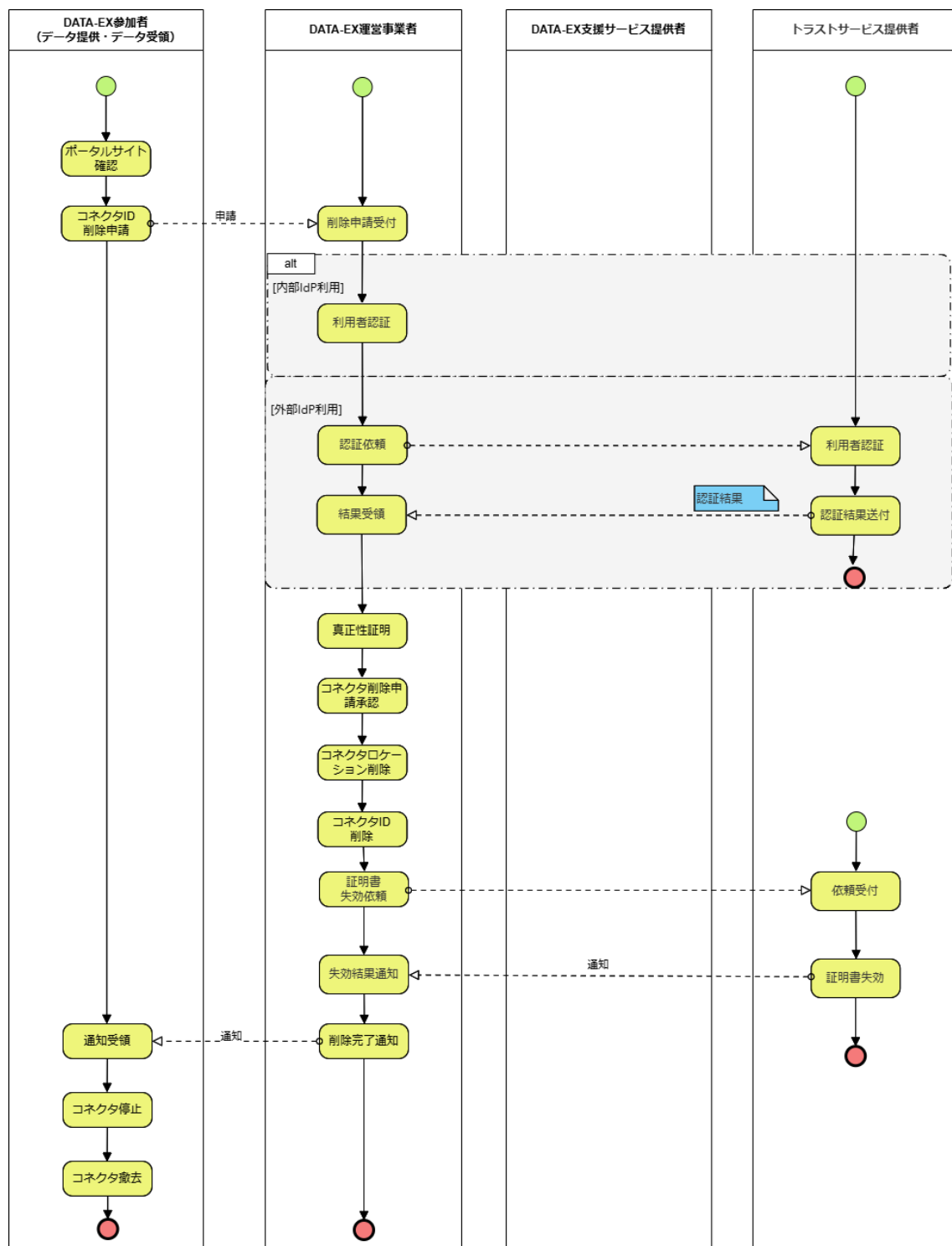


図 27:コネクタ撤廃の概要図

8-2-3-2. 退会

退会は、DATA-EX 参加者が DATA-EX の利用を終了するために必要な一連の作業である。

- ・ 退会処理

- DATA-EX 参加者が、ポータルサイトを閲覧し、申請先の URL を確認する。
- DATA-EX 参加者が、DATA-EX 運営事業者に退会申請する。
- DATA-EX 参加者が、外部 IdP を利用しない場合、以下の作業を実施する。
 - ◇ DATA-EX 運営事業者が申請者の認証を行う。
- DATA-EX 参加者が、外部 IdP を利用する場合、以下の作業を実施する。
 - ◇ DATA-EX 運営事業者が、申請者の認証を外部 IdP に依頼する。
 - ◇ 外部 IdP が申請者の認証を行う。
 - ◇ DATA-EX 運営事業者が、申請者の属性情報を含む認証結果を受け取る。
- DATA-EX 運営事業者が、申請者が本人であることを確認する。
- DATA-EX 運営事業者が、退会申請内容を審査する。
- DATA-EX 運営事業者が、DATA-EX アカウントの無効化処理を実施する。
- DATA-EX 運営事業者が、申請者に退会処理が完了したことを通知する。
- DATA-EX 参加者が、退会処理完了通知を受領する。

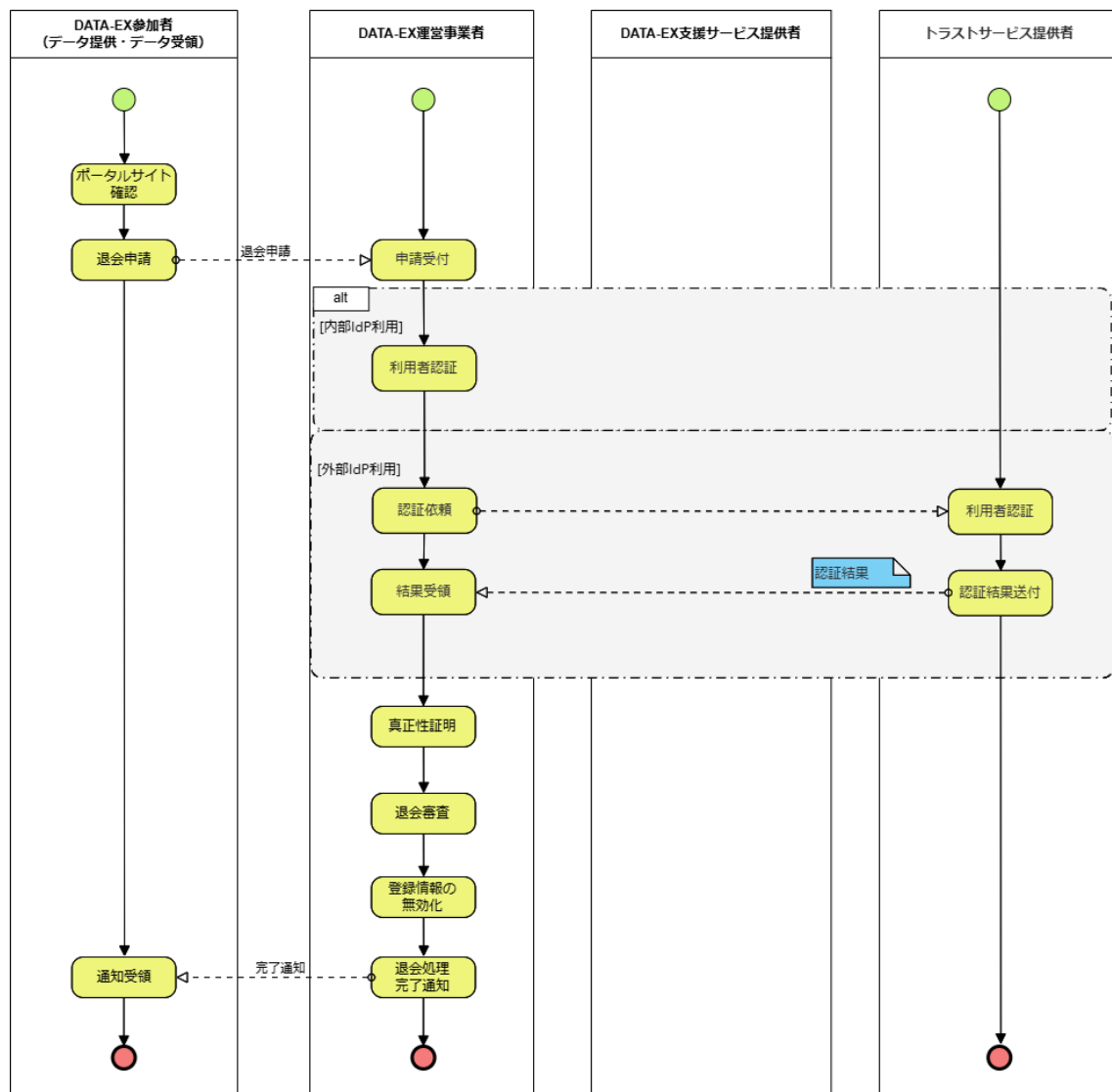


図 28:退会の概要図

8-3. データ取引市場などを介して契約を交わし、データ交換を行う

8-3-1. 利用準備

利用準備は、DATA-EX 参加者が DATA-EX を利用する前に実施する一連の作業(利用申請、コネクタ構築)である。

8-3-1-1. 利用申請

利用申請は、DATA-EX 参加者が DATA-EX の利用を開始するために必要な一連の作業である。

- ・ 登録準備

-
- DATA-EX 参加者が、外部 IdP を利用する場合、以下の作業を実施する。
 - ◇ DATA-EX 参加者が、外部 IdP に事前登録申請を依頼する。
 - ◇ 外部 IdP が、申請者が本人であることの身元確認を行う。
 - ◇ 外部 IdP と申請者間で、認証に必要な認証クレデンシャル(パスワード等)を設定する。
 - DATA-EX 参加者が、ポータルサイトを閲覧し、DATA-EX 利用解説書を取得する。
 - DATA-EX 参加者が、コネクタ構築に必要な環境(デバイス、認可サーバー、ストレージ、など)を準備する。
 - DATA-EX 参加者(データ提供)が、カタログサイトを構築する。
 - DATA-EX 参加者が、ポータルサイトを閲覧し、申請先の URL を確認する。
 - DATA-EX 参加者が、DATA-EX 運営事業者に DATA-EX の利用申請をする。
 - ・ 登録
 - DATA-EX 参加者が、外部 IdP を利用しない場合、以下の作業を実施する。
 - ◇ DATA-EX 運営事業者が、申請者が本人であることの身元確認を行う。
 - DATA-EX 参加者が、外部 IdP を利用する場合、以下の作業を実施する。
 - ◇ DATA-EX 運営事業者が、申請者の認証を外部 IdP に依頼する。
 - ◇ 外部 IdP が申請者の認証を行う。
 - ◇ DATA-EX 運営事業者が、申請者の属性を含む認証結果を受け取る。
 - ◇ DATA-EX 運営事業者が、申請者が本人であることを確認する。
 - DATA-EX 運営事業者が、申請内容を審査する。
 - DATA-EX 参加者が、外部 IdP を利用しない場合、以下の作業を実施する。
 - ◇ DATA-EX 運営事業者と申請者間で、認証に必要な認証クレデンシャル(パスワード等)を設定する。
 - DATA-EX 運営事業者が、アカウント(DATA-EX ID など)とコネクタ設定(コネクタ ID など)を発行する。(DATAEX-ID、コネクタ ID の一意性を保証)
 - DATA-EX 運営事業者が、申請者が組織に属している場合、所属する DATA-EX 参加組織に対し DATA-EX ID を発行する。
 - ・ アカウント・コネクタ設定取得
 - DATA-EX 運営事業者が、DATA-EX 参加者にアカウントとコネクタ設定を送付する。
 - DATA-EX 参加者が、アカウントとコネクタ設定を受領する。
 - ・ 支援サービス利用登録
 - DATA-EX 参加者が、DATA-EX 支援サービス提供者に支援サービスの利用申請をする。
 - DATA-EX 参加者が、外部 IdP を利用しない場合、以下の作業を実施する。
 - ◇ DATA-EX 支援サービス提供者が、申請者の認証を DATA-EX 運営事業者に依頼する。
-

-
- ◇ DATA-EX 運営事業者が申請者の認証を行う。
 - ◇ DATA-EX 支援サービス提供者が、申請者の属性情報を含む認証結果を受け取る。
 - DATA-EX 参加者が、外部 IdP を利用する場合、以下の作業を実施する。
 - ◇ DATA-EX 支援サービス提供者が、申請者の認証を外部 IdP に依頼する。
 - ◇ 外部 IdP が申請者の認証を行う。
 - ◇ DATA-EX 支援サービス提供者が、申請者の属性情報を含む認証結果を受け取る。
 - DATA-EX 支援サービス提供者が、申請内容を審査し、支援サービスの利用を許可する。

8-3-1-2. コネクタ構築

コネクタ構築は、DATA-EX 参加者が DATA-EX 上でコネクタを介した通信を行うために必要な一連の作業である。

- ・ コネクタ送付
 - DATA-EX 参加者が、ポータルサイトを閲覧し、コネクタ公開サイトの URL を確認する。
 - DATA-EX 参加者が、DATA-EX 運営事業者にコネクタの送付を依頼する。
 - DATA-EX 運営事業者が、DATA-EX 参加者にコネクタを送付する。
 - DATA-EX 参加者が、コネクタを受領する。
 - DATA-EX 参加者が、コネクタを構築し、コンフィグ情報を設定する。
- ・ コネクタの電子証明書発行
 - DATA-EX 参加者が、DATA-EX 運営事業者にコネクタの電子証明書発行を申請する。
 - DATA-EX 運営事業者が、コネクタの電子証明書発行申請を受け付ける。
 - DATA-EX 運営事業者が、認証局にコネクタの電子証明書の発行を依頼する。
 - 認証局が、コネクタの電子証明書を発行し、DATA-EX 運営事業者にコネクタの電子証明書を送付する。
 - DATA-EX 運営事業者が認証局で発行されたコネクタの電子証明書を配付する。
 - DATA-EX 参加者が、コネクタの電子証明書を受領する。
- ・ コネクタ起動
 - DATA-EX 参加者が、コネクタを起動する。
 - DATA-EX 参加者が、DATA-EX 運営事業者にコネクタ ID と申請者のロケーションの紐づけ登録を依頼する。
 - DATA-EX 運営事業者が、申請者のコネクタの真正性およびコネクタ ID の一意性を確認し、コネクタ ID と申請者のロケーションの紐づけを登録する。
 - DATA-EX 運営事業者が、DATA-EX 参加者にコネクタ ID と申請者のロケーションの紐づけ登録が完了したことを通知する。
 - DATA-EX 参加者が、DATA-EX 運営事業者からのコネクタ ID と申請者のロケーションの紐づけ登録完了通知を受領する。
 - DATA-EX 運営事業者が、コネクタの疎通テスト環境を提供する。
 - DATA-EX 参加者が、コネクタと DATA-EX が接続できることを確認する。

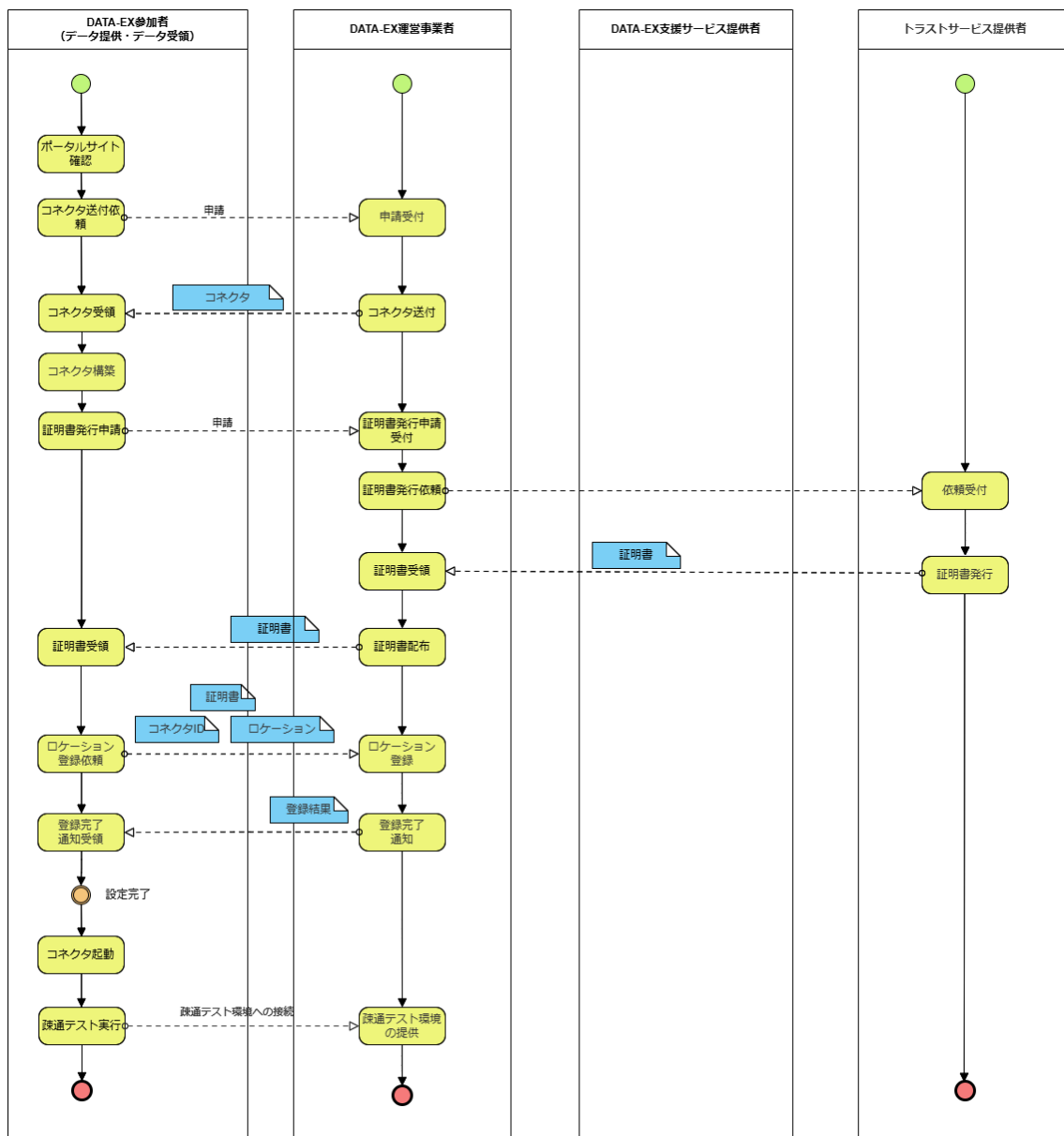


図 30:コネクタ構築の概要図

8-3-2. 利用

利用は、DATA-EX 参加者が DATA-EX を利用する際に行う一連の作業（データセット用意、データセット発見、契約・DDP 作成、DDP 授受、語彙リポジトリ登録、語彙リポジトリ参照、来歴確認、DDP 削除、データセット削除）である。

8-3-2-1. カタログ用意

カタログ用意は、DATA-EX 参加者（データ提供）が DATA-EX 上で提供するデータセットを用意するために必要な一連の作業である。

-
- ・ 横断検索サイト登録
 - DATA-EX 参加者(データ提供)が、ポータルサイトを閲覧し、登録依頼先の URL を確認する。
 - DATA-EX 参加者(データ提供)が、横断検索サイトにカタログサイトの登録を依頼する。
 - DATA-EX 参加者が、外部 IdP を利用しない場合、以下の作業を実施する。
 - ◇ DATA-EX 支援サービス提供者が、申請者の認証を DATA-EX 運営事業者に依頼する。
 - ◇ DATA-EX 運営事業者が申請者の認証を行う。
 - ◇ DATA-EX 支援サービス提供者が、申請者の属性情報を含む認証結果を受け取る。
 - DATA-EX 参加者が、外部 IdP を利用する場合、以下の作業を実施する。
 - ◇ DATA-EX 支援サービス提供者が、申請者の認証を外部 IdP に依頼する。
 - ◇ 外部 IdP が申請者の認証を行う。
 - ◇ DATA-EX 支援サービス提供者が、申請者の属性情報を含む認証結果を受け取る。
 - DATA-EX 支援サービス提供者が、登録内容を審査する。
 - DATA-EX 支援サービス提供者が、横断検索サイトでカタログサイトのクローリングを実施する。
 - DATA-EX 支援サービス提供者が、横断検索サイトにカタログが表示されることを確認する。
 - DATA-EX 支援サービス提供者が、依頼者にカタログサイトの登録が完了したことを通知する。
 - DATA-EX 参加者(データ提供)が、登録完了通知を受領する。
 - ・ カタログ作成
 - DATA-EX 参加者(データ提供)が、データカタログ作成ツールでカタログを作成する。
 - DATA-EX 参加者(データ提供)が、e シールサービスに作成したカタログの e シールの付与を依頼する。
 - e シールサービスが、e シールを生成し、送付する。
 - DATA-EX 参加者(データ提供)が、e シール付きのカタログを作成する。
 - DATA-EX 参加者(データ提供)が、カタログをカタログサイトに登録する。
 - DATA-EX 支援サービス提供者が、定期的にカタログサイトのクローリングを実施する。
 - ・ データ取引市場向けカタログ登録
 - DATA-EX 参加者(データ提供)が、DATA-EX 支援サービス提供者(データ取引市場)にデータ取引市場向けカタログ登録を依頼する。
-

-
- DATA-EX 支援サービス提供者（データ取引市場）が、DATA-EX 参加者（データ提供）からのカタログ登録依頼を受け付ける。
 - DATA-EX 支援サービス提供者（データ取引市場）が、DATA-EX 参加者（データ提供）にカタログ情報の取得を依頼する。
 - DATA-EX 参加者（データ提供）が、DATA-EX 支援サービス提供者（データ取引市場）からのカタログ情報の取得依頼を受け付ける。
 - DATA-EX 参加者（データ提供）が、DATA-EX 支援サービス提供者（データ取引市場）にカタログ情報を送信する。
 - DATA-EX 支援サービス提供者（データ取引市場）が、DATA-EX 参加者（データ提供）のカタログ情報をデータ取引市場向けカタログに登録する。
 - DATA-EX 参加者（データ提供）が、DATA-EX 支援サービス提供者（データ取引市場）が登録したデータ取引市場向けカタログ情報を確認する。
 - DATA-EX 参加者（データ提供）が、DATA-EX 支援サービス提供者（データ取引市場）にデータ取引市場向けカタログ情報の確認が完了したことを通知する。
 - DATA-EX 参加者（データ提供）がデータ取引市場向けカタログ情報の登録を完了する。

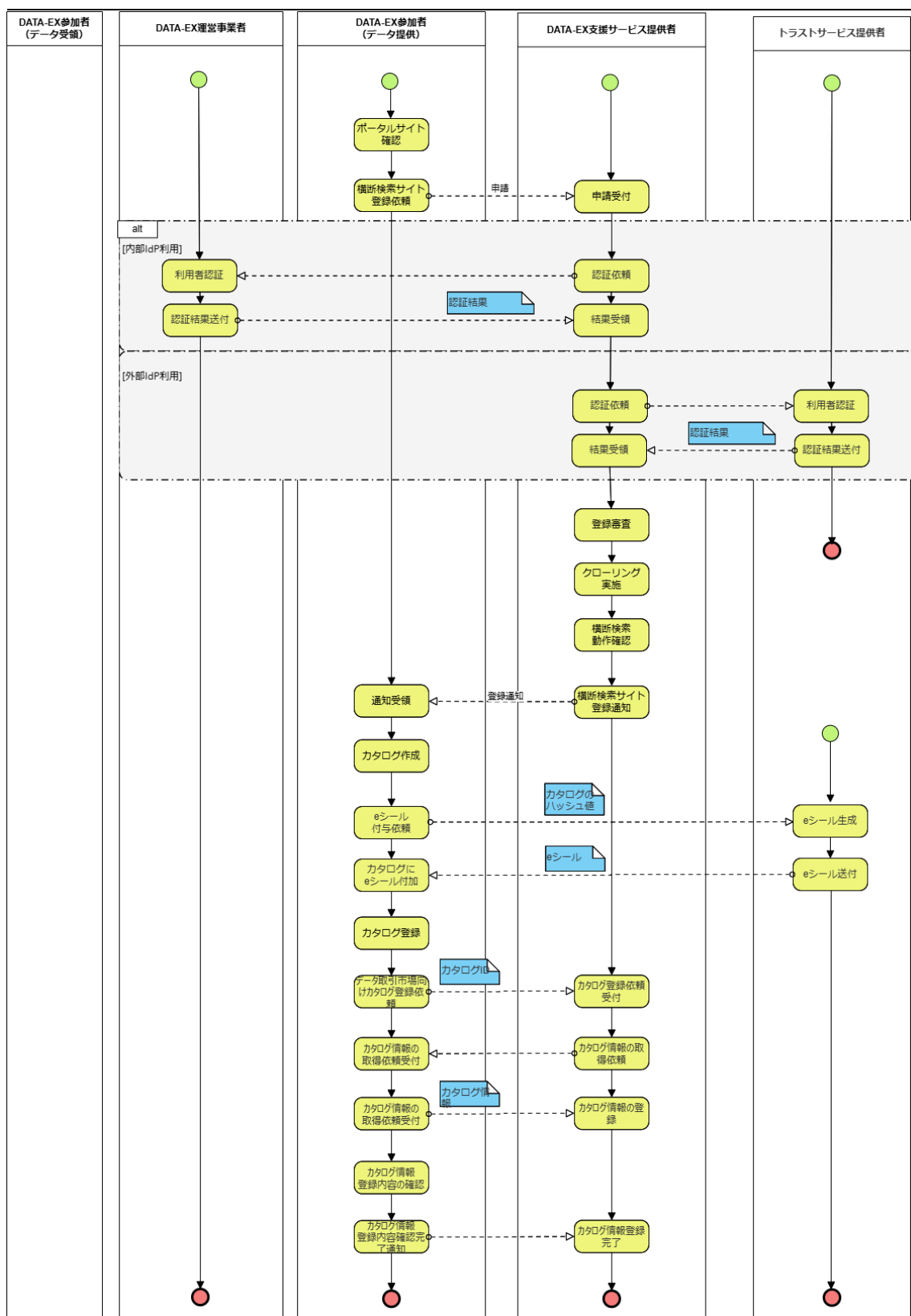


図 31:カタログ用意の概要図

8-3-2-2. データセット発見

データセット発見は、DATA-EX 参加者（データ受領）が DATA-EX 上で提供されるデータセットを発見するために必要な一連の作業である。

- ・ 横断検索サイト利用
 - DATA-EX 参加者（データ受領）が、ポータルサイトを閲覧し、横断検索サイトの URL を確認する。
 - DATA-EX 参加者（データ受領）が、横断検索サイトに検索条件を入力し、検索する。
 - DATA-EX 支援サービス提供者が、検索結果（検索条件に合致するカタログ）を送付する。
 - DATA-EX 参加者（データ受領）が、横断検索サイト上で検索結果を閲覧する。
 - DATA-EX 参加者（データ受領）が、カタログを選択する。
 - DATA-EX 参加者（データ提供）が、カタログサイト上のカタログを送付する。
 - DATA-EX 参加者（データ受領）が、カタログの e シールを検証する。
 - DATA-EX 参加者（データ受領）が、DATA-EX 運営事業者に e シール作成者が DATA-EX に参加していることの確認を依頼する。
 - DATA-EX 運営事業者が、e シール作成者が DATA-EX 参加者であることの確認結果を送付する。
 - DATA-EX 参加者（データ受領）が、カタログサイト上のカタログを閲覧する。

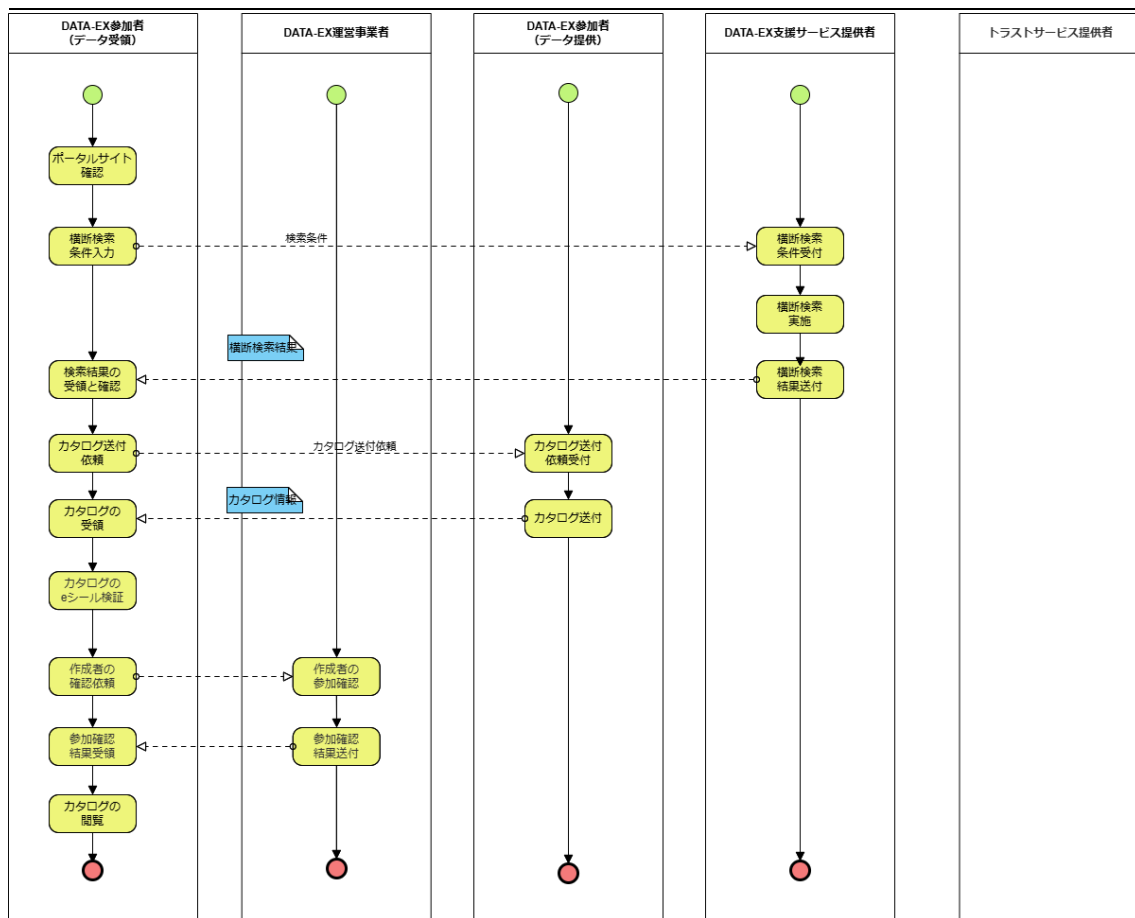


図 32: データセット発見の概要図

8-3-2-3. 契約

契約は、DATA-EX 参加者がデータの提供と便益の交換に関する契約を行うために必要な一連の作業である。

- ・ 契約
 - DATA-EX 参加者(データ受領)が、DATA-EX 支援サービス提供者(データ取引市場)にデータ取得をリクエストする。
 - DATA-EX 支援サービス提供者(データ取引市場)が、DATA-EX 参加者(データ受領)からのデータ取得リクエストを受け付ける。
 - DATA-EX 支援サービス提供者(データ取引市場)が、DATA-EX 参加者(データ受領)からのデータ取得リクエストがあったことを DATA-EX 参加者(データ提供)に通知する。
 - DATA-EX 参加者(データ提供)が、DATA-EX 支援サービス提供者からの DATA-EX 参加者(データ受領)からのデータ取得リクエストがあったことの通知を受領する。

-
- DATA-EX 参加者同士が、取得するデータの範囲や契約条件などについて協議する。
 - DATA-EX 支援サービス提供者（データ取引市場）が、DATA-EX 参加者同士の協議内容を登録する。
 - DATA-EX 参加者（データ受領）が、注文内容を確定する。
 - DATA-EX 支援サービス提供者（データ取引市場）が、注文内容が確定したことを受け付ける。
 - DATA-EX 支援サービス提供者（データ取引市場）が、DATA-EX 参加者（データ受領）に注文内容が確定したことを通知する。
 - DATA-EX 参加者（データ提供）が、DATA-EX 支援サービス提供者（データ取引市場）からの注文確定通知を受領する。
 - DATA-EX 参加者（データ提供）が、DATA-EX 参加者（データ受領）からの注文内容に合意し、注文請書を作成する。
 - DATA-EX 支援サービス提供者（データ取引市場）が、DATA-EX 参加者（データ受領）からの注文請書を受領する。
 - DATA-EX 支援サービス提供者（データ取引市場）が、DATA-EX 参加者（データ受領）に注文請書を送信する。
 - DATA-EX 参加者（データ受領）が、DATA-EX 支援サービス提供者（データ取引市場）からの注文請書を受領する。

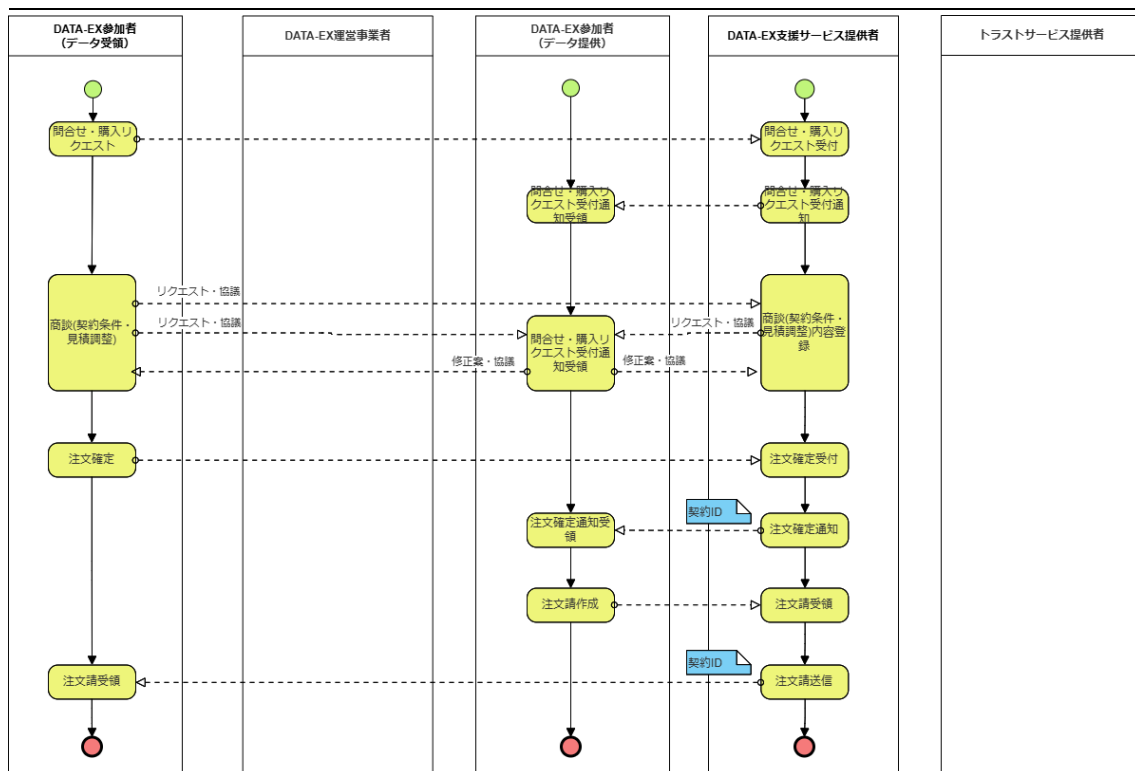


図 33: 契約の概要図

8-3-2-4. DDP 作成

DDP 作成は、DATA-EX 参加者（データ提供）が契約に基づいて DDP を作成し、DDP ID とコネクタ ID を通知するために必要な一連の作業である。

- ・ DDP 作成
 - DATA-EX 参加者（データ提供）が、DDP に含むデータセット・付帯情報・契約情報を決定する。
 - DATA-EX 参加者（データ提供）が、契約をもとに DDP (DDP ID など)を作成する。
 - DATA-EX 参加者（データ提供）が、e シールサービスに DDP への e シールの付与を依頼する。
 - DATA-EX 参加者（データ提供）が、e シールを受け取り、DDP に付加する。
 - DATA-EX 参加者（データ提供）が、配信用のストレージに格納する。
 - DATA-EX 参加者（データ提供）が、DDP ID と DDP のロケーション情報を登録する。
 - DATA-EX 参加者（データ提供）が、DDP の認可情報を登録する。
 - DATA-EX 参加者（データ提供）が、必要に応じて DATA-EX 運営事業者に DDP 作成履歴の登録を依頼する。
 - DATA-EX 運営事業者が、履歴を登録する。
- ・ DDP ID・コネクタ ID 通知

- DATA-EX 参加者(データ提供)が、DATA-EX 参加者(データ受領)に DDP ID とコネクタ ID を通知する。
- DATA-EX 参加者(データ受領)が、通知を受領する。

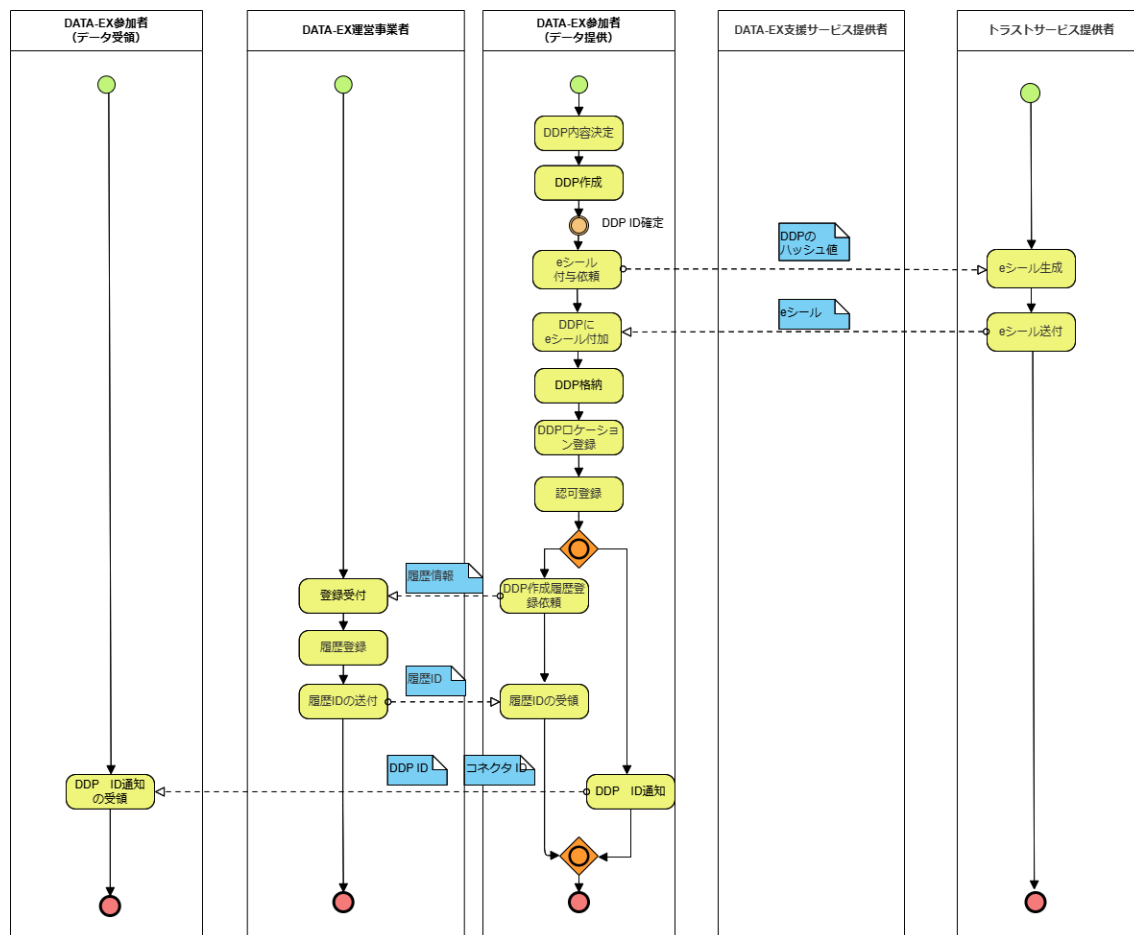


図 34: DDP 作成の概要図

8-3-2-5. データ交換

データ交換は、DATA-EX 参加者(データ提供)と DATA-EX 参加者(データ受領)がデータの交換を行うために必要な一連の作業である。DATA-EX 参加者(データ受領)が DATA-EX 参加者(データ提供)の用意した DDP を取りに来る方式となる。

- ・ 認証情報取得
 - DATA-EX 参加者(データ受領)が、DATA-EX 運営事業者に認証情報の送付を依頼する。
 - DATA-EX 参加者が、外部 IdP を利用しない場合、以下の作業を実施する。
 - ◇ DATA-EX 運営事業者が申請者の認証を行う。
 - DATA-EX 参加者が、外部 IdP を利用する場合、以下の作業を実施する。

-
- ◇ DATA-EX 運営事業者が、申請者の認証を外部 IdP に依頼する。
 - ◇ 外部 IdP が申請者の認証を行う。
 - ◇ DATA-EX 運営事業者が、申請者の属性情報を含む認証結果を受け取る。
 - DATA-EX 運営事業者が、DATA-EX 参加者(データ受領)に認証情報を送付する。
 - DATA-EX 参加者(データ受領)が、認証情報を受領する。
 - ・ データ取得リクエスト
 - DATA-EX 参加者(データ受領)が、DATA-EX 参加者(データ提供)に認証情報を含めたデータ取得リクエストを送信する。
 - データ取得リクエストを送信するにあたって、DATA-EX 運営事業者に認証情報の取得とコネクタロケーションの解決をリクエストし、コネクタ間の真正性を証明する。
 - ◇ 受領側コネクタにおける認証
 - DATA-EX 参加者(データ受領)が、DATA-EX 運営事業者に認証情報を送付する。
 - DATA-EX 運営事業者が、認証情報の正当性を確認する。
 - DATA-EX 運営事業者が、DATA-EX 参加者(データ受領)に確認結果を送付する。
 - DATA-EX 参加者(データ受領)が、確認結果を受領する。
 - ◇ コネクタロケーション取得
 - DATA-EX 参加者(データ受領)が、DATA-EX 運営事業者に提供側のコネクタロケーションの送付を依頼する。
 - DATA-EX 運営事業者が、DATA-EX 参加者(データ受領)にコネクタロケーションを送付する。
 - DATA-EX 参加者(データ受領)が、コネクタロケーションを受領する。
 - ◇ 受領側コネクタと提供側コネクタの真正性証明
 - DATA-EX 参加者(データ受領)が、提供側コネクタの証明書情報の正当性を確認する。
 - DATA-EX 参加者(データ提供)が、受領側コネクタの証明書情報の正当性を確認する。
 - ・ データ取得リクエスト受領
 - DATA-EX 参加者(データ提供)が、データ取得リクエストを受領する。
 - ・ 提供側コネクタにおける認証・認可
 - DATA-EX 参加者(データ提供)が、DATA-EX 運営事業者を受領側の認証情報を送付する。
 - DATA-EX 運営事業者が、受領側の認証情報の正当性を確認する。
 - DATA-EX 運営事業者が、DATA-EX 参加者(データ提供)に確認結果を送付する。
-

-
- DATA-EX 参加者(データ提供)が、受領側に DDP にアクセスする権限があるか確認する。
 - ・ DDP 受領
 - DATA-EX 参加者(データ提供)が、DDP ID をもとに、DDP の格納先ストレージの URL を取得する。
 - DATA-EX 参加者(データ提供)が、DATA-EX 運営事業者に送信履歴の登録を依頼する。
 - DATA-EX 運営事業者が、DATA-EX 参加者(データ提供)からの送信履歴の登録依頼を受け付ける。
 - DATA-EX 運営事業者が、履歴を登録する。
 - DATA-EX 運営事業者が、履歴 ID を DATA-EX 参加者(データ提供)へ伝達する。
 - DATA-EX 参加者(データ提供)が履歴 ID を受領する。
 - DATA-EX 参加者(データ提供)が、DATA-EX 参加者(データ受領)にストレージの DDP と送信履歴の履歴 ID を送付する。
 - DATA-EX 参加者(データ提供)が、DATA-EX 支援サービス提供者(データ取引市場)に DDP を送信したことを通知する。
 - DATA-EX 支援サービス提供者(データ取引市場)が、DATA-EX 参加者(データ提供)からの DDP 送信通知を受領する。
 - DATA-EX 支援サービス提供者(データ取引市場)が、DATA-EX 参加者(データ提供)からの DDP 送信通知を受領したことを通知する。
 - DATA-EX 参加者(データ提供)が、DATA-EX 支援サービス提供者(データ取引市場)からの受領完了通知を受領する。
 - DATA-EX 参加者(データ受領)が、DATA-EX 参加者(データ提供)からの DDP と送信履歴の履歴 ID を受信する。
 - DATA-EX 参加者(データ受領)が、受け取った DDP の e シールを検証する。
 - DATA-EX 参加者(データ受領)が、DATA-EX 運営事業者に e シール作成者が DATA-EX に参加していることの確認を依頼する。
 - DATA-EX 運営事業者が、e シール作成者が DATA-EX 参加者であることの確認結果を送付する。
 - DATA-EX 参加者(データ受領)が、DATA-EX 支援サービス提供者(データ取引市場)に DDP を受信したことを通知する。
 - DATA-EX 支援サービス提供者(データ取引市場)が、DATA-EX 参加者(データ受領)からの DDP 受信通知を受領する。
 - DATA-EX 支援サービス提供者(データ取引市場)が、DATA-EX 参加者(データ受領)からの DDP 受信通知を受領したことを通知する。
-

-
- DATA-EX 参加者(データ受領)が、DATA-EX 支援サービス提供者(データ取引市場)からの受領完了通知を受領する。
 - DATA-EX 参加者(データ受領)が、DATA-EX 運営事業者を受信履歴の登録を依頼する。
 - DATA-EX 運営事業者が、履歴を登録する。
 - DATA-EX 運営事業者が、履歴 ID を DATA-EX 参加者(データ受領)へ伝達する。
 - DATA-EX 参加者(データ受領)が履歴 ID を受領する。

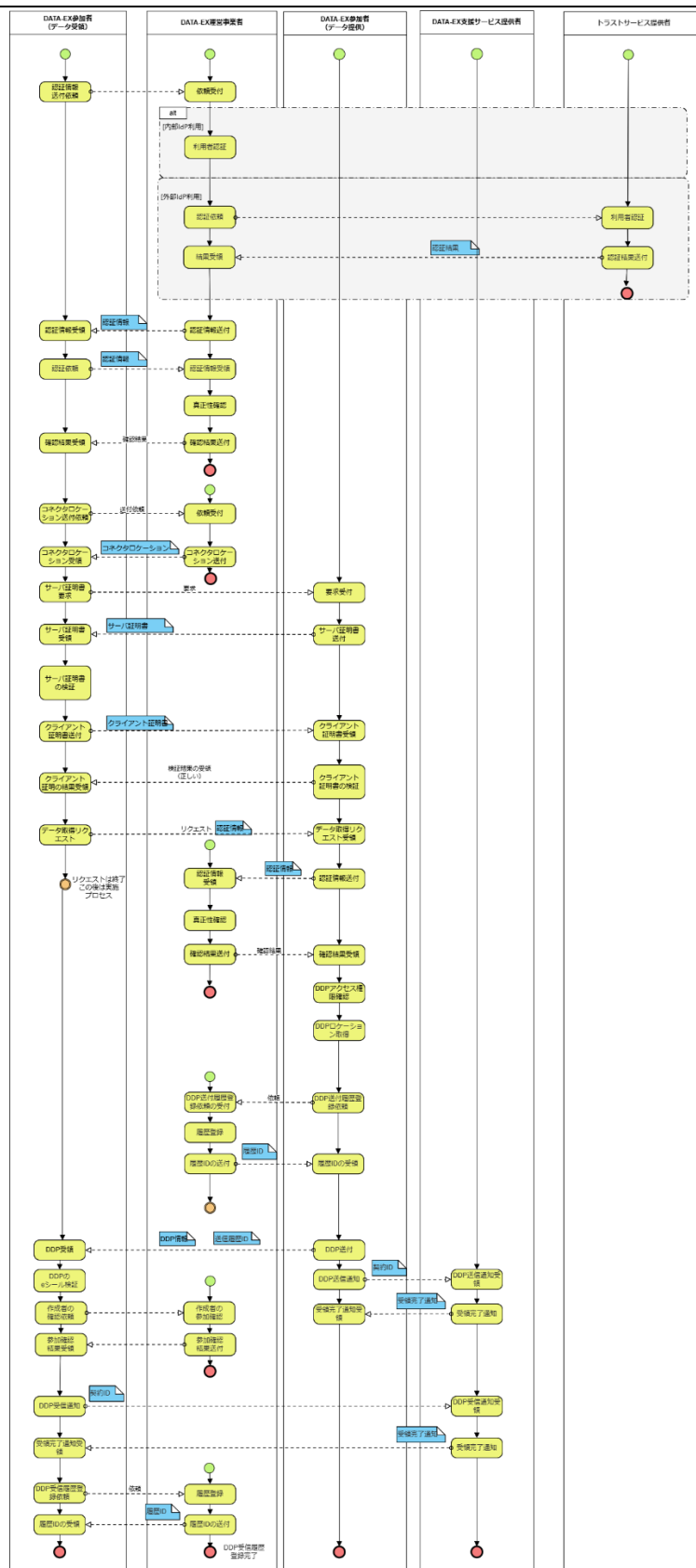


図 35: データ交換の概要図

8-3-2-6. DDP 削除

DDP 削除は、DATA-EX 参加者（データ提供・データ受領）が、利用目的がなくなった DDP を削除する作業である。

なお、DDP の削除については、DATA-EX 参加者（データ提供・データ受領）の任意、もしくは DATA-EX 参加者同士での契約内容・利用条件に基づいて行われるものとする。

- ・ データ提供側の DDP 削除
 - DATA-EX 参加者（データ提供）が削除対象の DDP に対する認可を削除する。
 - DATA-EX 参加者（データ提供）が削除対象の DDP に対するロケーションを削除する。
 - DATA-EX 参加者（データ提供）が、DDP をストレージから削除する。
- ・ データ受領側の DDP 削除
 - DATA-EX 参加者（データ受領）が、DDP をストレージから削除する。

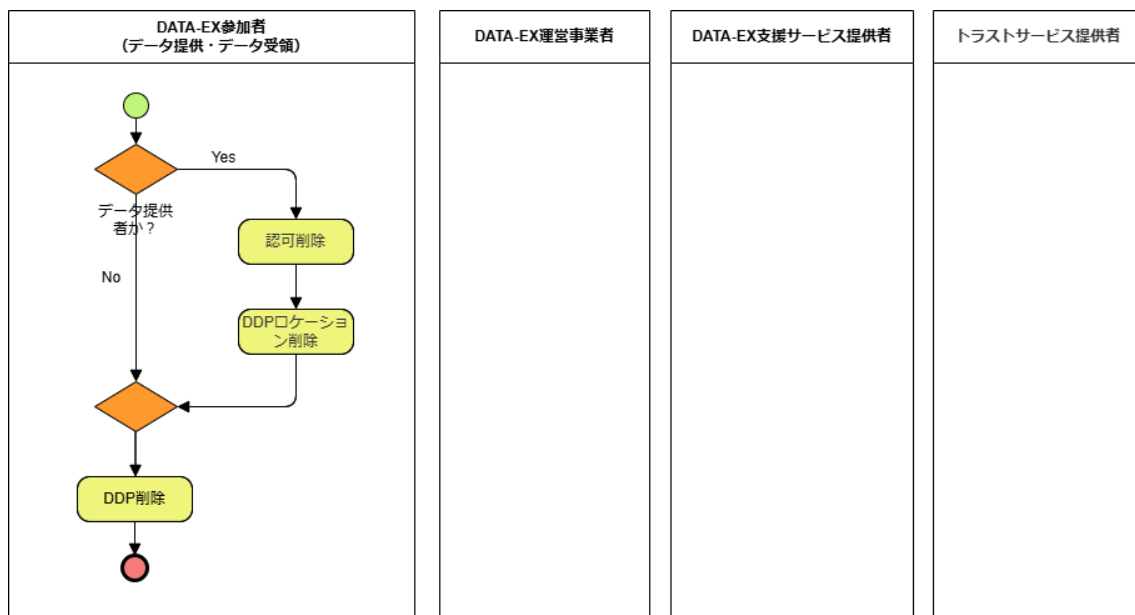


図 36:DDP 削除の概要図

8-3-2-7. 来歴確認

来歴確認は、DATA-EX 参加者が自身に関する DDP 情報の来歴を確認するために必要な一連の作業である。

- ・ 来歴情報提供
 - DATA-EX 参加者が、DATA-EX 運営事業者到来歴情報の提供を依頼する。
 - DATA-EX 運営事業者が、DATA-EX 参加者に来歴情報を提供する。
 - DATA-EX 参加者が、来歴情報を受領する。

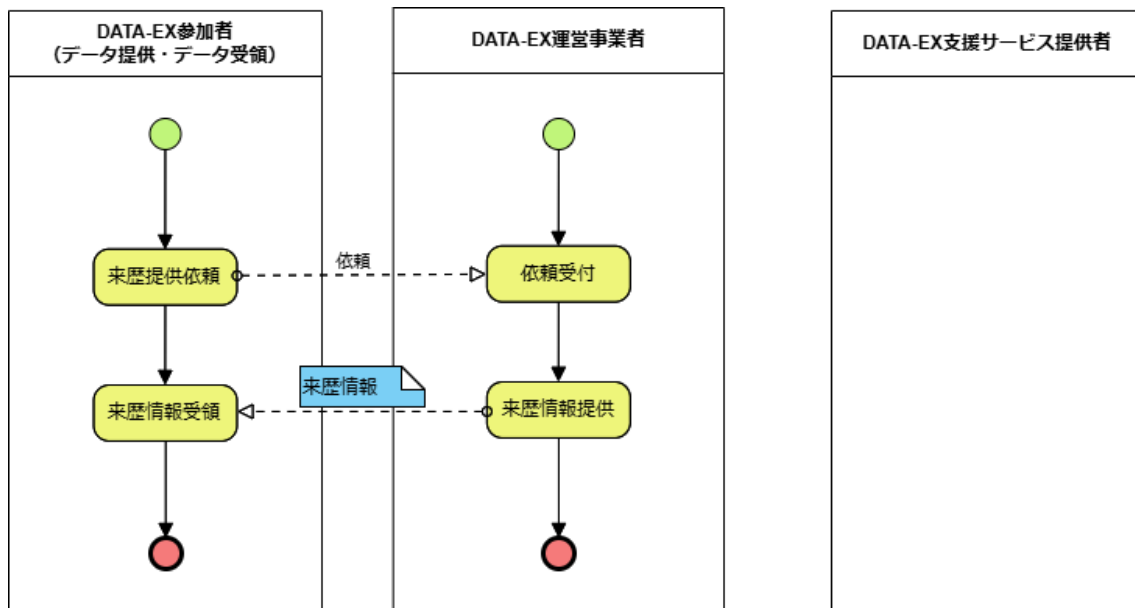


図 37: 来歴確認の概要図

8-3-2-8. カタログ削除

カタログ削除は、DATA-EX 参加者（データ提供）が、カタログサイトそのものを削除するために必要な一連の作業である。横断検索カタログサイト上の登録を削除し、DATA-EX 参加者（データ提供）のカタログサイトを削除し、データ取引市場向けのカタログを削除する手順となる。

- ・ 横断検索サイト登録解除
 - DATA-EX 参加者（データ提供）が、ポータルサイトを閲覧し、登録解除依頼先の URL を確認する。
 - DATA-EX 参加者（データ提供）が、横断検索サイトにカタログサイトの登録解除を依頼する。
 - DATA-EX 参加者が、外部 IdP を利用しない場合、以下の作業を実施する。
 - ✧ DATA-EX 支援サービス提供者が、申請者の認証を DATA-EX 運営事業者に依頼する。
 - ✧ DATA-EX 運営事業者が申請者の認証を行う。
 - ✧ DATA-EX 支援サービス提供者が、申請者の属性情報を含む認証結果を受け取る。
 - DATA-EX 参加者が、外部 IdP を利用する場合、以下の作業を実施する。
 - ✧ DATA-EX 支援サービス提供者が、申請者の認証を外部 IdP に依頼する。
 - ✧ 外部 IdP が申請者の認証を行う。
 - ✧ DATA-EX 支援サービス提供者が、申請者の属性情報を含む認証結果を受け取る。

-
- DATA-EX 支援サービス提供者が、解除依頼の内容を審査する。
 - DATA-EX 支援サービス提供者が、カタログサイトのクローリングを停止する。
 - DATA-EX 支援サービス提供者が、横断検索サイトのカタログを削除する。
 - DATA-EX 支援サービス提供者が、横断検索サイトにカタログが表示されないことを確認する。
 - DATA-EX 支援サービス提供者が、依頼者にカタログサイトの解除が完了したことを通知する。
 - DATA-EX 参加者（データ提供）が、解除完了通知を受領する。
 - ・ カタログ削除
 - DATA-EX 参加者（データ提供）が、カタログサイトを削除する。
 - DATA-EX 参加者（データ提供）が、DATA-EX 支援サービス提供者（データ取引市場）にデータ取引市場向けカタログの削除を依頼する。
 - DATA-EX 支援サービス提供者（データ取引市場）が、DATA-EX 参加者（データ提供）からのデータ取引市場向けカタログの削除依頼を受け付ける。
 - DATA-EX 支援サービス提供者（データ取引市場）が、データ取引市場向けカタログを削除する。
 - DATA-EX 支援サービス提供者（データ取引市場）が、DATA-EX 参加者（データ提供）にデータ取引市場向けカタログの削除が完了したことを通知する。
 - DATA-EX 参加者（データ提供）が、DATA-EX 支援サービス提供者（データ取引市場）からのデータ取引市場向けカタログ削除完了通知を受領する。

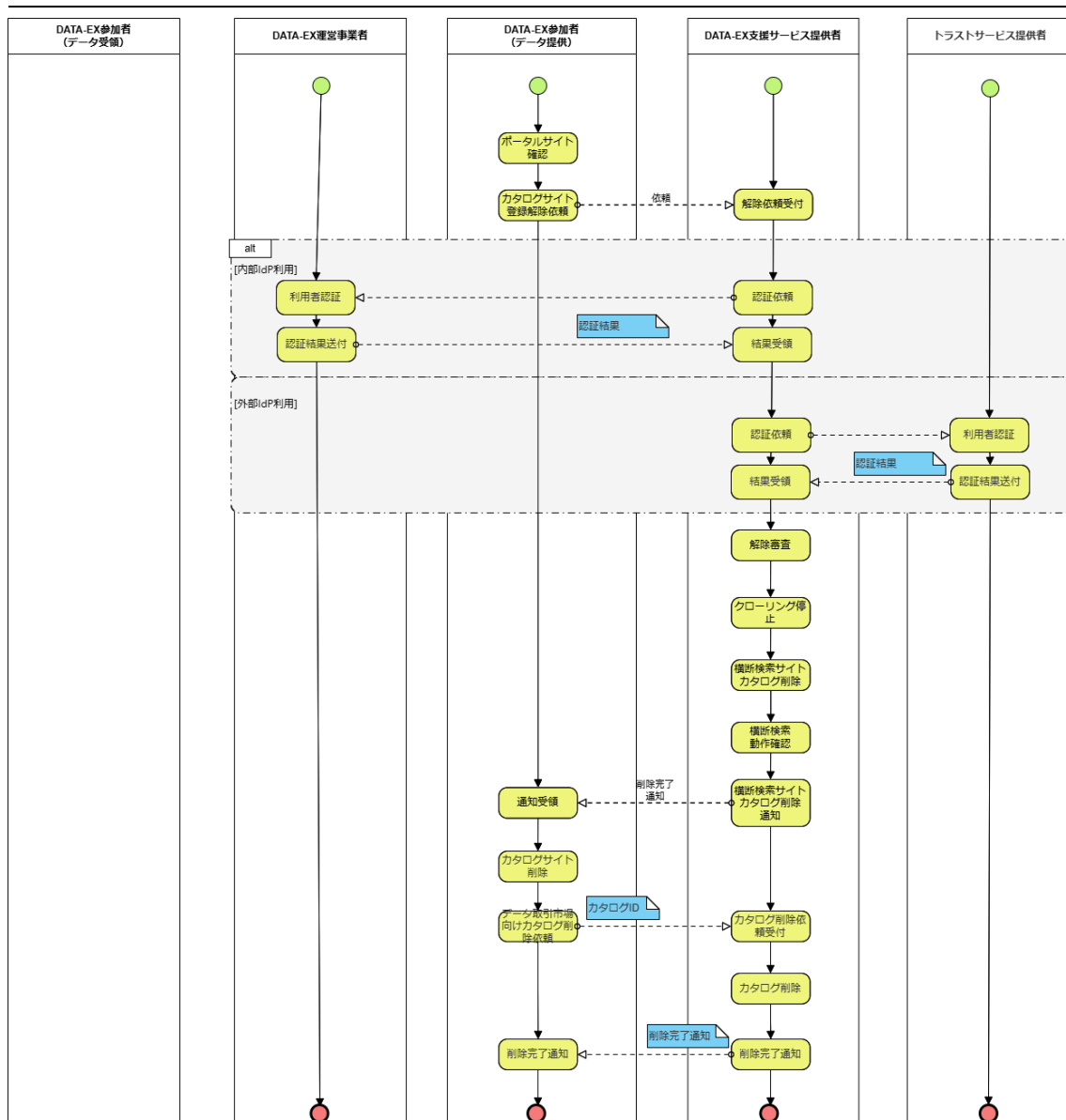


図 38: カタログ削除の概要図

8-3-3. 利用停止

利用停止は、DATA-EX 参加者が DATA-EX の利用を停止する前に実施する一連の作業(コネクタ撤廃、退会)である。

8-3-3-1. コネクタ撤廃

コネクタ撤廃は、DATA-EX 参加者がコネクタの利用を終了するために必要な一連の作業である。

- ・ コネクタ削除

- DATA-EX 参加者が、ポータルサイトを閲覧し、申請先の URL を確認する。
- DATA-EX 参加者が、DATA-EX 運営事業者にコネクタ ID の削除を申請する。

-
- DATA-EX 参加者が、外部 IdP を利用しない場合、以下の作業を実施する。
 - ◇ DATA-EX 運営事業者が申請者の認証を行う。
 - DATA-EX 参加者が、外部 IdP を利用する場合、以下の作業を実施する。
 - ◇ DATA-EX 運営事業者が、申請者の認証を外部 IdP に依頼する。
 - ◇ 外部 IdP が申請者の認証を行う。
 - ◇ DATA-EX 運営事業者が、申請者の属性情報を含む認証結果を受け取る。
 - DATA-EX 運営事業者が、申請者が本人であることを確認する。
 - DATA-EX 運営事業者が、申請内容を確認し、コネクタ削除申請を承認する。
 - DATA-EX 運営事業者が、コネクタロケーションを削除する。
 - DATA-EX 運営事業者が、申請者のアカウントからコネクタ ID を削除する。
 - DATA-EX 運営事業者が、認証局にコネクタの電子証明書の失効を依頼する。
 - 認証局が、コネクタの電子証明書の失効を行う。
 - DATA-EX 運営事業者が、申請者にコネクタロケーションとコネクタ ID の削除が完了したことを通知する。
 - DATA-EX 参加者が、削除完了通知を受領する。
 - ・ コネクタ停止
 - DATA-EX 参加者が、コネクタを停止する。
 - DATA-EX 参加者が、コネクタを撤去する。

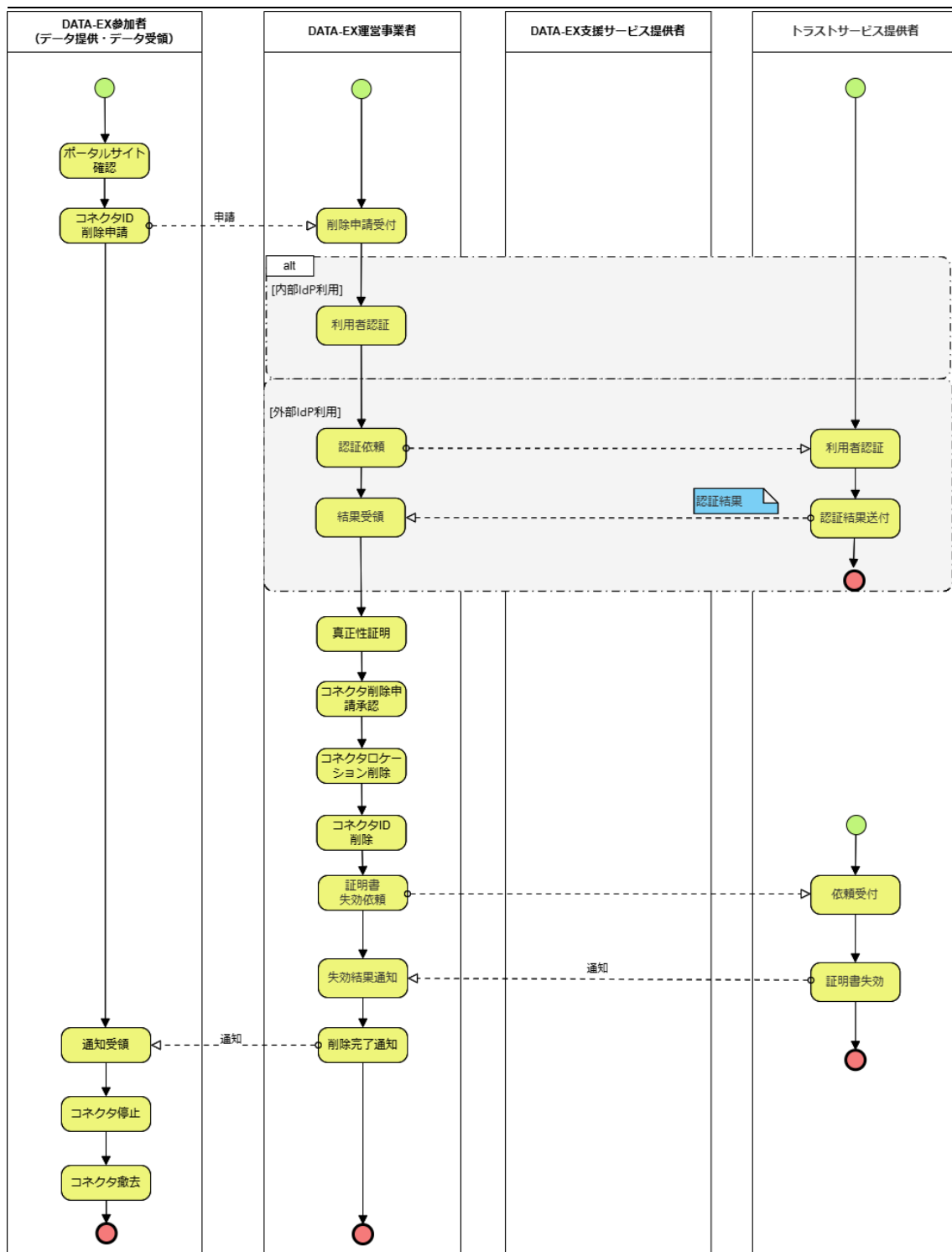


図 39:コネクタ撤廃の概要図

8-3-3-2. 退会

退会は、DATA-EX 参加者が DATA-EX の利用を終了するために必要な一連の作業である。

- ・ 退会処理

-
- DATA-EX 参加者が、ポータルサイトを閲覧し、申請先の URL を確認する。
 - DATA-EX 参加者が、DATA-EX 運営事業者に退会申請する。
 - DATA-EX 参加者が、外部 IdP を利用しない場合、以下の作業を実施する。
 - ◇ DATA-EX 運営事業者が申請者の認証を行う。
 - DATA-EX 参加者が、外部 IdP を利用する場合、以下の作業を実施する。
 - ◇ DATA-EX 運営事業者が、申請者の認証を外部 IdP に依頼する。
 - ◇ 外部 IdP が申請者の認証を行う。
 - ◇ DATA-EX 運営事業者が、申請者の属性情報を含む認証結果を受け取る。
 - DATA-EX 運営事業者が、申請者が本人であることを確認する。
 - DATA-EX 運営事業者が、退会申請内容を審査する。
 - DATA-EX 運営事業者が、DATA-EX アカウントの無効化処理を実施する。
 - DATA-EX 運営事業者が、申請者に退会処理が完了したことを通知する。
 - DATA-EX 参加者が、退会処理完了通知を受領する。

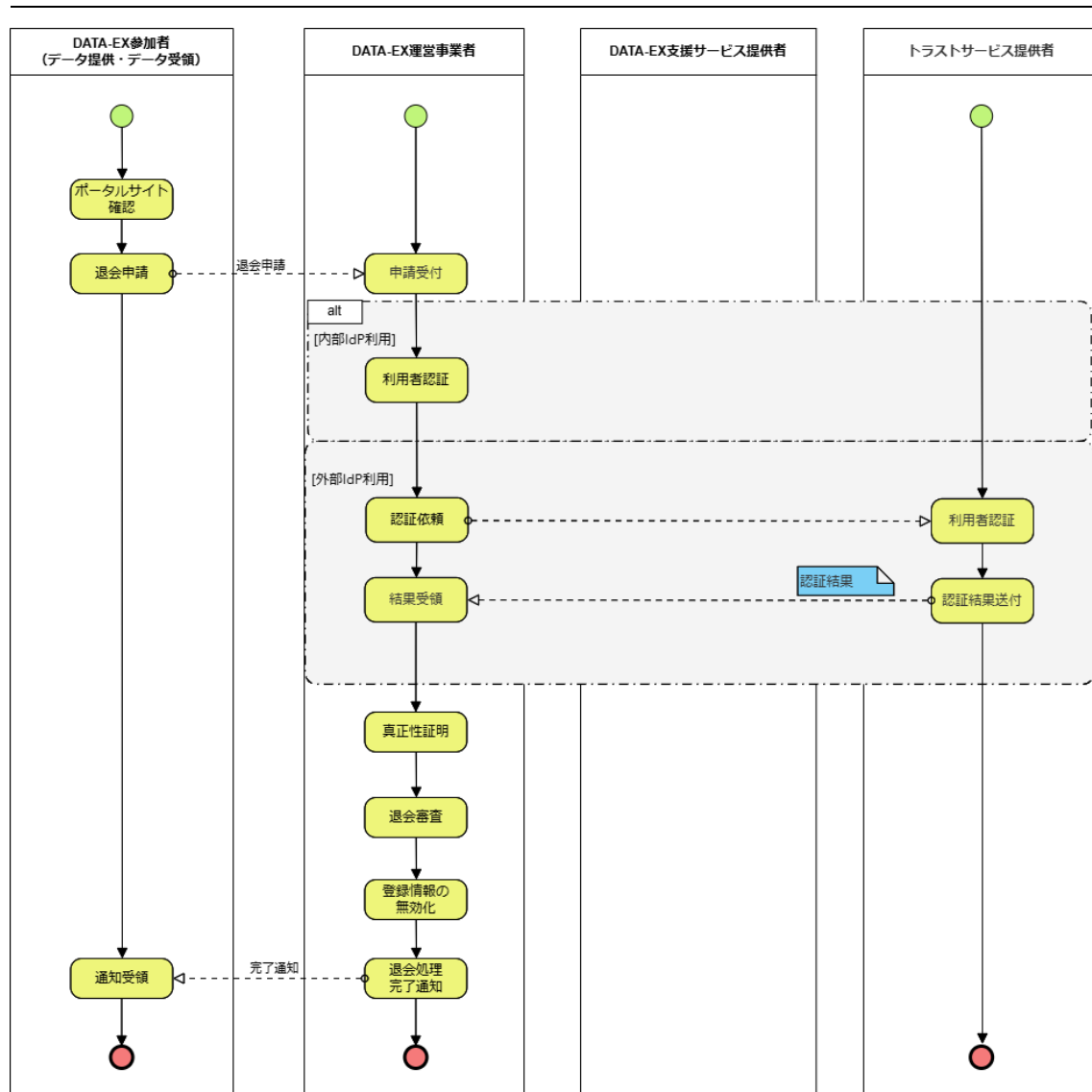


図 40: 退会の概要図

9. コンポーネントアーキテクチャ

DATA-EX の分野間データ連携は、7-4 機能に示す各機能コンポーネント(以降、コンポーネントという)が、8 章記載のシナリオを実現するために相互に関連することによって実現される。ここでコンポーネント間の相互の関連(以降、インタラクションという)とは、「A 機能が B 機能を利用することで、B 機能により C という処理が行われ、D という結果が A 機能に返ってくる」といった関係性のことである。

コンポーネント間のインタラクションは、DATA-EX 内のコンポーネント間だけでなく、3 層構造の他の層のコンポーネントとの間にも存在する。例えば、概念モデルの 3 層構造におけるアプリケーション層に位置付けられるデータ提供側/データ受領側のアプリケーションが、DATA-EX を利用する際には、当該アプリケーションが DATA-EX のコンポーネントを利用することによって、認証情報を取得したり、コネクタを利用したりする。

本章では、このような DATA-EX の分野間データ連携を実現するために必要な、コンポーネント間のインタラクションを定義していく。なお、コンポーネント間のインタラクションは、接続線で示すこととし、各接続線は次のような意味を持つものとして記載する。また各接続線には識別子を付番し、文章説明と対応付ける。

- ・ 接続線の意味 : (A 機能と B 機能が接続している場合)
 - A 機能が B 機能を利用することで、B 機能により C という処理が行われ、D という結果が A 機能に返ってくる。

以降、以下の切り口で DATA-EX の分野間データ連携を実現するコンポーネント間のインタラクション関係を示す。

- ・ DATA-EX のコンポーネント間のインタラクション
- ・ アプリケーション層のデータ提供側のコンポーネントと DATA-EX のコンポーネント間のインタラクション
- ・ アプリケーション層のデータ受領側のコンポーネントと DATA-EX のコンポーネント間のインタラクション
- ・ トラストサービス層のコンポーネントと DATA-EX のコンポーネント間のインタラクション
- ・ アプリケーション層のコンポーネントとトラストサービス層のコンポーネント間のインタラクション

9-1. DATA-EX のコンポーネント間のインタラクション

DATA-EX のコンポーネント間のインタラクションを示す。各説明冒頭の識別子は、下部に示す図中の識別子と対応している。

- CA1-① データカタログ作成機能は、語彙管理機能を利用することで、カタログでの利用が推奨される語彙を取得してもよい。
- CA1-② データ交換機能(データ受領側)は、アカウント管理機能/認証機能に対して認証情報を送付し、認証情報の検定を依頼する。アカウント管理機能/認証機能は、受領した認証情報の検定を行い、データ交換機能(データ受領側)に対して確認結果を返す。
- CA1-③ データ交換機能(データ受領側)は、コネクタロケーション管理機能に対してデータ提供側のコネクタ ID を送ることで、データ提供側のコネクタロケーション情報の送付を依頼する。コネクタロケーション管理機能は、送られてきたコネクタ ID に対応するコネクタロケーション情報を、データ交換機能(データ受領側)に返す。
- CA1-④ データ交換機能(データ受領側)は、データ交換機能(データ提供側)に対してデータ取得リクエストを送るに当たって、互いのコネクタの証明書情報を送り合い、相互認証を実施する。認証に問題ない場合、データ交換機能(データ受領側)からデータ交換機能(データ提供側)に対して、データ受領側の認証情報やデータ受領者が所望する DDP ID 等を含むデータ取得リクエストが送付され、以下に示す CA1-⑤～CA1-⑨の処理が実施される。CA1-⑤～CA1-⑨の処理が問題なく完了した場合、データ交換機能(データ提供側)から、データ交換機能(データ受領側)に対して、DDP が返される。
- CA1-⑤ データ交換機能(データ提供側)は、アカウント管理機能/認証機能に対して、データ交換機能(データ受領側)から受領した認証情報を送付し、認証情報の検定を依頼する。アカウント管理機能/認証機能は、受領した認証情報の検定を行い、データ交換機能(データ提供側)に対して、確認結果を返す。
- CA1-⑥ データ交換機能(データ提供側)は、認可機能に対して、データ取得リクエストを送ってきているデータ受領者の認証情報を送ることで、当該データ受領者が DDP にアクセスする権限があるか(認可されているか)を確認する。認可機能は、アカウント管理機能/認証機能に対して、CA1-⑦に示す処理を行うことで、データ取得リクエストを送ってきているデータ受領者の認証情報の検定を依頼する。検定に問題がない場合、認可機能は認可情報を発行し、データ提供者(データ提供側)に返す。

-
- CA1-⑦ 認可機能は、アカウント管理機能/認証機能に対して、CA1-⑥の処理で受領したデータ受領者の認証情報の検定依頼を行う。アカウント管理機能/認証機能は、認可機能から受領した認証情報を検定し、確認結果を認可機能に返す。
- CA1-⑧ データ交換機能(データ提供側)は、CA1-④の処理でデータ交換機能(データ受領側)から受領した DDP ID と、CA1-⑥の処理で受領した認可情報を DDP ロケーション管理機能に対して送付する。DDP ロケーション管理機能は、受領した情報に応じて、適切な DDP ロケーションをデータ交換機能(データ提供側)に返す。
- CA1-⑨ データ交換機能(データ提供側)は、来歴管理機能に対して DDP の送信履歴の登録を依頼する。来歴管理機能は、依頼に基づき送信履歴の登録を行い、送信履歴の登録が完了した旨の情報を、データ交換機能(データ提供側)に対して返す。
- CA1-⑩ データ交換機能(データ受領側)は、来歴管理機能に対して、DDP の受信履歴の登録を依頼する。来歴管理機能は、依頼に基づき受信履歴の登録を行い、受信履歴の登録が完了した旨の情報を、データ交換機能(データ受領側)に返す。
- CA1-⑪ 来歴管理機能は、来歴情報を連携させるために、来歴管理拡張機能に対して DDP に関連する加工等の来歴の送付を依頼する。来歴管理拡張機能は、来歴管理機能に対して来歴を返す。
- CA1-⑫ コネクタロケーション管理機能は、アカウント管理機能/認証機能に対して認証情報を送付し、認証情報の検証を依頼する。アカウント管理機能/認証機能は、受領した認証情報の検証を行い、コネクタロケーション管理機能に対して確認結果を返す。
- CA1-⑬ コネクタ構築時のコネクタ初期起動時に、データ交換機能(データ提供側)は、コネクタロケーション管理機能に対してコネクタ ID およびロケーション情報を送付し、ロケーション情報の登録を依頼する。コネクタロケーション管理機能は、受領したコネクタ ID の重複検証を行い、重複がなければロケーション情報を登録し、データ交換機能(データ提供側)に対して検証結果および登録完了通知を返す。
- また、コネクタ構築後のコネクタ起動時に、データ交換機能(データ提供側)は、コネクタロケーション管理機能に対してコネクタ ID およびロケーション情報を送付し、ロケーション情報の検証を依頼する。コネクタロケーション管理機能は、受領したコネクタ ID の重複検証を行い、データ交換機能(データ提供側)に対して検証結果を返す。
-

-
- CA1-⑭ コネクタ構築時のコネクタ初期起動時に、データ交換機能(データ受領側)は、コネクタロケーション管理機能に対してコネクタ ID およびロケーション情報を送付し、ロケーション情報の登録を依頼する。コネクタロケーション管理機能は、受領したコネクタ ID の重複検証を行い、重複がなければロケーション情報を登録し、データ交換機能(データ受領側)に対して検証結果および登録完了通知を返す。また、コネクタ構築後のコネクタ起動時に、データ交換機能(データ受領側)は、コネクタロケーション管理機能に対してコネクタ ID およびロケーション情報を送付し、ロケーション情報の検証を依頼する。コネクタロケーション管理機能は、受領したコネクタ ID の重複検証を行い、データ交換機能(データ受領側)に対して検証結果を返す。
- CA1-⑮ ポータル機能は、アカウント管理機能/認証機能に対して認証情報を送付し、認証情報の検証を依頼する。アカウント管理機能/認証機能は、受領した認証情報の検証を行い、ポータル機能に対して確認結果を返す。
- CA1-⑯ 来歴管理機能は、アカウント管理機能/認証機能に対して認証情報を送付し、認証情報の検証を依頼する。アカウント管理機能/認証機能は、受領した認証情報の検証を行い、来歴管理機能に対して確認結果を返す。
- CA1-⑰ ポータル機能は、来歴管理機能に対して送受信来歴情報の取得を依頼する。来歴管理機能は、依頼に基づき送受信来歴情報を返す。

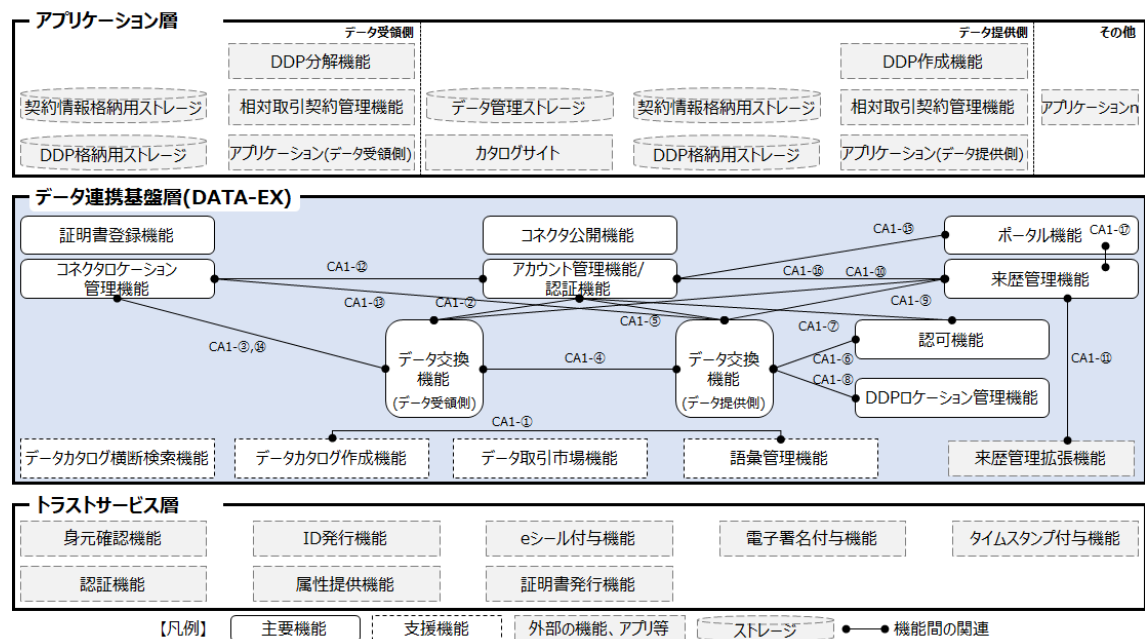


図 41: DATA-EX のコンポーネント間のインタラクション

DATA-EX のコンポーネント間のインタラクションとシナリオについて、各インタラクションがどのシナリオを実現するためのものか、対応関係を以下の表に示す。

表 3: DATA-EX のコンポーネント間のインタラクションとシナリオとの対応関係

インタラク ション	対応するシナリオ	
	章節	対応するシナリオ
CA1-①	8-1-2-1 カタログ用意 8-2-2-1 カタログ用意 8-3-2-1 カタログ用意	・カタログ作成 ・データカタログ作成ツールと語彙管理機能の連携 ※CA1-①は、シナリオ上は明記されないバックエンドの処理
CA1-②	8-1-2-4 データ交換 8-2-2-5 データ交換 8-3-2-5 データ交換	・データ取得リクエスト ・受領側コネクタにおける認証
CA1-③	8-1-2-4 データ交換 8-2-2-5 データ交換 8-3-2-5 データ交換	・データ取得リクエスト ・コネクタロケーション取得
CA1-④	8-1-2-4 データ交換 8-2-2-5 データ交換 8-3-2-5 データ交換	・データ取得リクエスト ・受領側コネクタと提供側コネクタの真正性証明 ・データ取得リクエスト受領
CA1-⑤	8-1-2-4 データ交換 8-2-2-5 データ交換 8-3-2-5 データ交換	・提供者側コネクタにおける認証・認可

CA1-⑥	8-1-2-4 データ交換 8-2-2-5 データ交換 8-3-2-5 データ交換	・提供者側コネクタにおける認証・認可
CA1-⑦	8-1-2-4 データ交換 8-2-2-5 データ交換 8-3-2-5 データ交換	・提供者側コネクタにおける認証・認可 ※CA1-⑦は、シナリオ上は明記されないバックエンドの処理
CA1-⑧	8-1-2-4 データ交換 8-2-2-5 データ交換 8-3-2-5 データ交換	・提供者側コネクタにおける認証・認可
CA1-⑨	8-1-2-4 データ交換 8-2-2-5 データ交換 8-3-2-5 データ交換	・DDP 受領 ※送信履歴登録
CA1-⑩	8-1-2-4 データ交換 8-2-2-5 データ交換 8-3-2-5 データ交換	・DDP 受領 ※受信履歴登録
CA1-⑪	－	－ ※シナリオ記載なし
CA1-⑫	－	－ ※シナリオ記載なし
CA1-⑬	8-1-1-2 コネクタ構築 8-2-1-2 コネクタ構築 8-3-1-2 コネクタ構築	・コネクタ起動 申請者のコネクタの真正性およびコネクタIDの一意性を確認し、コネクタIDと申請者のロケーションの紐づけを登録 ※コネクタ構築後のコネクタ起動についてはシナリオ記載なし
CA1-⑭	8-1-1-2 コネクタ構築 8-2-1-2 コネクタ構築 8-3-1-2 コネクタ構築	・コネクタ起動 申請者のコネクタの真正性およびコネクタIDの一意性を確認し、コネクタIDと申請者のロケーションの紐づけを登録 ※コネクタ構築後のコネクタ起動についてはシナリオ記載なし
CA1-⑮	－	－ ※シナリオ記載なし
CA1-⑯	－	－ ※シナリオ記載なし
CA1-⑰	－	－ ※シナリオ記載なし

9-2. アプリケーション層のデータ提供側のコンポーネントと DATA-EX のコンポーネント間のインタラクション

アプリケーション層のデータ提供側のコンポーネントと DATA-EX のコンポーネント間のインタラクションを示す。各説明冒頭の識別子は、下部に示す図中の識別子と対応している。

CA2-① アプリケーション(データ提供側)は、アカウント管理機能/認証機能に対してアカウント情報等を送付し、認証情報の発行を依頼する。アカウント管理機能/認証機能は、受領したアカウント情報等の検定を行い、問題がない場合、アプリケーション(データ提供側)に対して認証情報を返す。

CA2-② DATA-EX(データ提供)は、データカタログ作成機能を利用してカタログを作成し、カタログサイトに登録する。カタログサイトは、データカタログ作成機能に対して、登録完了した旨を返す。

CA2-③ データカタログ横断検索機能は、カタログサイトのクローリングを行う。カタログサイトは、データカタログ横断検索機能に対して、カタログ情報を返す。

CA2-④ アプリケーション(データ提供側)は、作成した DDP の ID(DDP ID)と、DDP の URL を紐づけて DDP ロケーション管理機能に登録する。DDP ロケーション管理機能はアプリケーション(データ提供側)に対して、登録完了した旨を返す。

CA2-⑤ アプリケーション(データ提供側)は、契約を交わした DATA-EX 参加者(データ受領)が DDP にアクセスできるよう、認可機能に対して認可登録を行う。認可機能は、アプリケーション(データ提供側)に対して、登録完了した旨を返す。

CA2-⑥ データ交換機能(データ提供側)は、DDP 格納用ストレージに対して、指定の DDP の取得を要求する。DDP 格納用ストレージは、データ交換機能(データ提供側)から指定された DDP を返す。

CA2-⑦ アプリケーション(データ提供側)は、来歴管理機能に対して DDP ID 等を送付し、登録された来歴情報の取得を依頼する。来歴管理機能は、アプリケーション(データ提供側)が所望する来歴情報を返す。

CA2-⑧ DDP 作成機能は、来歴管理機能に対して、DDP 作成に関する履歴情報の登録を依頼する。来歴管理機能は履歴情報を登録し、DDP 作成機能に対して登録が正常に完了した結果を返す。

CA2-⑨ DDP 作成機能は、来歴管理拡張機能に対して、DDP 作成時の加工等に関する履歴情報の登録を依頼する。来歴管理拡張機能は履歴情報を登録し、DDP 作成機能に対して登録が正常に完了した結果を返す。

CA2-⑩ アプリケーション(データ提供側)は、来歴管理拡張機能に対して、DDP の加工等に関連する来歴の送付を依頼する。来歴管理拡張機能は、アプリケーション(データ提供側)に対して DDP の加工等に関連する来歴を返す。

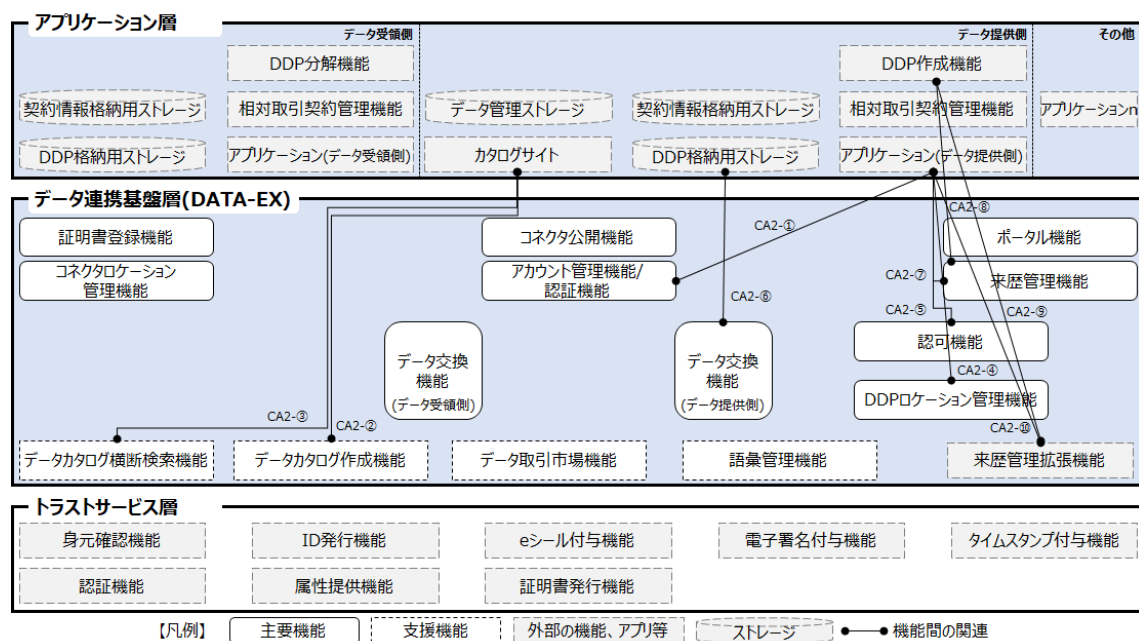


図 42: アプリケーション層のデータ提供側のコンポーネントと DATA-EX のコンポーネント間のインタラクション

アプリケーション層のデータ提供側のコンポーネントと DATA-EX のコンポーネント間のインタラクションとシナリオについて、各インタラクションがどのシナリオを実現するためのものか、対応関係を以下の表に示す。

表 4: アプリケーション層のデータ提供側のコンポーネントと DATA-EX のコンポーネント間のインタラクション

インタラクション	対応するシナリオ	
	章節	対応するシナリオ
CA2-①	—	— ※シナリオ記載なし
CA2-②	8-1-2-1 カタログ用意 8-2-2-1 カタログ用意 8-3-2-1 カタログ用意	・カタログ作成

CA2-③	8-1-2-1 カタログ用意 8-2-2-1 カタログ用意 8-3-2-1 カタログ用意	・横断検索サイト登録
CA2-④	8-1-2-3 DDP 作成 8-2-2-4 DDP 作成 8-3-2-4 DDP 作成	・DDP 作成 ・DDP ID と DDP のロケーション情報の登録
CA2-⑤	8-1-2-3 DDP 作成 8-2-2-4 DDP 作成 8-3-2-4 DDP 作成	・DDP 作成 ・認可登録
CA2-⑥	8-1-2-4 データ交換 8-2-2-5 データ交換 8-3-2-5 データ交換	・提供側コネクタにおける認証・認可 ・DDP の格納先ストレージの URL の取得
CA2-⑦	8-1-2-6 来歴確認 8-2-2-7 来歴確認 8-3-2-7 来歴確認	・来歴情報提供
CA2-⑧	8-1-2-3 DDP 作成 8-2-2-4 DDP 作成 8-3-2-4 DDP 作成	・DDP 作成
CA2-⑨	-	- ※シナリオ記載なし
CA2-⑩	-	- ※シナリオ記載なし

9-3. アプリケーション層のデータ受領側のコンポーネントと DATA-EX のコンポーネント間のインタラクション

アプリケーション層のデータ受領側のコンポーネントと DATA-EX のコンポーネント間のインタラクションを示す。各説明冒頭の識別子は、下部に示す図中の識別子と対応している。

CA3-① アプリケーション(データ受領側)は、アカウント管理機能/認証機能に対してアカウント情報等を送付し、認証情報の発行を依頼する。アカウント管理機能/認証機能は、受領したアカウント情報等の検定を行い、問題がない場合、アプリケーション(データ受領側)に対して認証情報を返す。

CA3-② アプリケーション(データ受領側)は、データカタログ横断検索機能を利用してカタログ情報を検索する。データカタログ横断検索機能は、カタログ情報の検索結果をアプリケーション(データ受領側)に返す。

CA3-③ アプリケーション(データ受領側)は、CA3-①で取得した認証情報を送付し、データ交換機能(データ受領側)を起動する。データ交換機能(データ受領側)は、CA1-②、CA1-③、CA1-④等 to 示す各処理を行う。その結果として、DDP がデータ交換機能(データ受領側)から、アプリケーション(データ受領側)に返ってくる。

CA3-④ アプリケーション(データ受領側)は、来歴管理機能に対して DDP ID 等を送付し、登録された来歴情報の取得を依頼する。来歴管理機能は、アプリケーション(データ受領側)が所望する来歴情報を返す。

CA3-⑤ アプリケーション(データ受領側)は、来歴管理拡張機能に対して、DDP の加工等に関連する来歴の送付を依頼する。来歴管理拡張機能は、アプリケーション(データ受領側)に対して DDP の加工等に関連する来歴を返す。

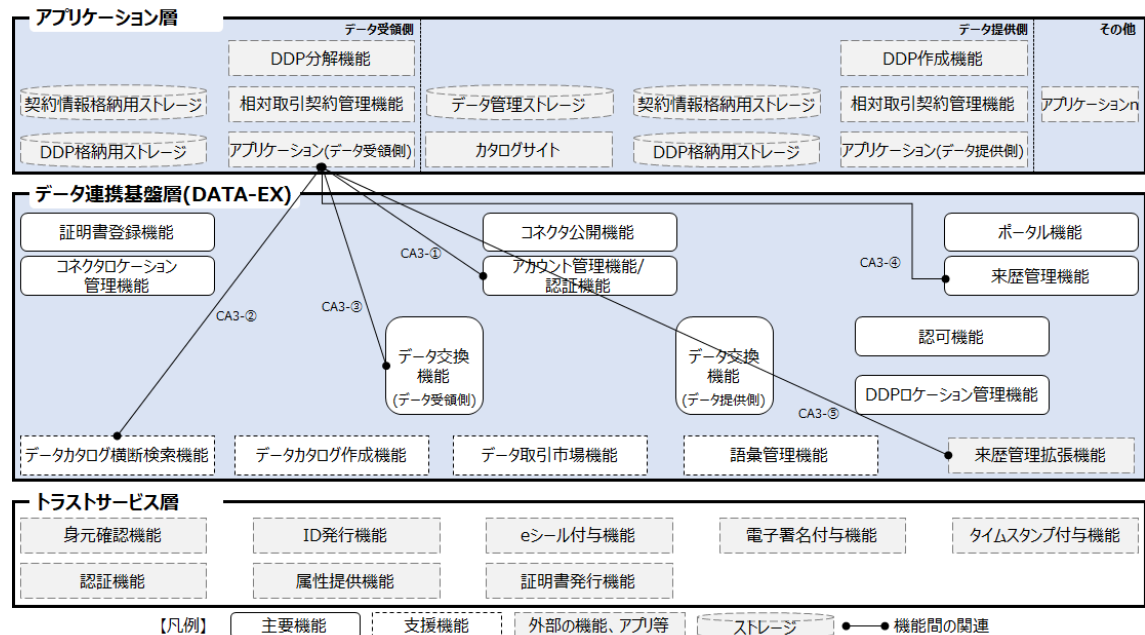


図 43:アプリケーション層のデータ受領側のコンポーネントと DATA-EX のコンポーネント間のインタラクション

アプリケーション層のデータ受領側のコンポーネントと DATA-EX のコンポーネント間のインタラクションとシナリオについて、各インタラクションがどのシナリオを実現するためのものか、対応関係を以下の表に示す。

表 5:アプリケーション層のデータ受領側のコンポーネントと DATA-EX のコンポーネント間のインタラクション

インタラクション	対応するシナリオ	
	章節	対応するシナリオ
CA3-①	8-1-2-4 データ交換 8-2-2-5 データ交換 8-3-2-5 データ交換	・認証情報取得
CA3-②	8-1-2-2 データセット発見 8-2-2-2 データセット発見 8-3-2-2 データセット発見	・横断検索サイト利用
CA3-③	8-1-2-4 データ交換 8-2-2-5 データ交換 8-3-2-5 データ交換	・認証情報取得 ・受領側コネクタにおける認証
CA3-④	8-1-2-6 来歴確認 8-2-2-7 来歴確認 8-3-2-7 来歴確認	・来歴情報提供
CA3-⑤	-	- ※シナリオ記載なし

9-4. トラストサービス層のコンポーネントと DATA-EX のコンポーネント間のインタラクション

トラストサービス層のコンポーネントと DATA-EX のコンポーネント間のインタラクションを示す。
各説明冒頭の識別子は、下部に示す図中の識別子と対応している。

- CA4-① 証明書登録機能は、証明書発行機能に対してコネクタの電子証明書の発行を依頼する。証明書発行機能は、コネクタの電子証明書を作成し、証明書登録機能に対してコネクタの電子証明書を返す。
- CA4-② アカウント管理機能/認証機能は、トラストサービス層の認証機能に対して、DATA-EX 参加者の認証を依頼する。トラストサービス層の認証機能は、DATA-EX 参加者に対する認証を実施し、アカウント管理機能/認証機能に対して認証結果を返す。
- CA4-③ アカウント管理機能/認証機能は、属性提供機能に対して、DATA-EX 参加者の属性情報の送付を依頼する。属性提供機能は、アカウント管理機能/認証機能に対して DATA-EX 参加者の属性情報を返す。
- CA4-④ データカタログ作成機能は、e シール付与機能に対して、カタログの e シール作成を依頼する。e シール付与機能は、カタログの e シールを生成し、データカタログ作成機能に対して e シールを返す。
- CA4-⑤ データ取引市場機能は、e シール付与機能に対して、契約書等の e シールの作成を依頼する。e シール付与機能は、契約書等の e シールを生成し、データ取引市場機能に対して e シールを返す。
- CA4-⑥ データ取引市場機能は、電子署名付与機能に対して、契約書等への電子署名の作成を依頼する。電子署名付与機能は、契約書等への電子署名を生成し、データ取引市場機能に対して電子署名を返す。
- CA4-⑦ データ取引市場機能は、タイムスタンプ付与機能に対して、契約書等へのタイムスタンプの作成を依頼する。タイムスタンプ付与機能は、契約書等へのタイムスタンプを生成し、データ取引市場機能に対してタイムスタンプを返す。

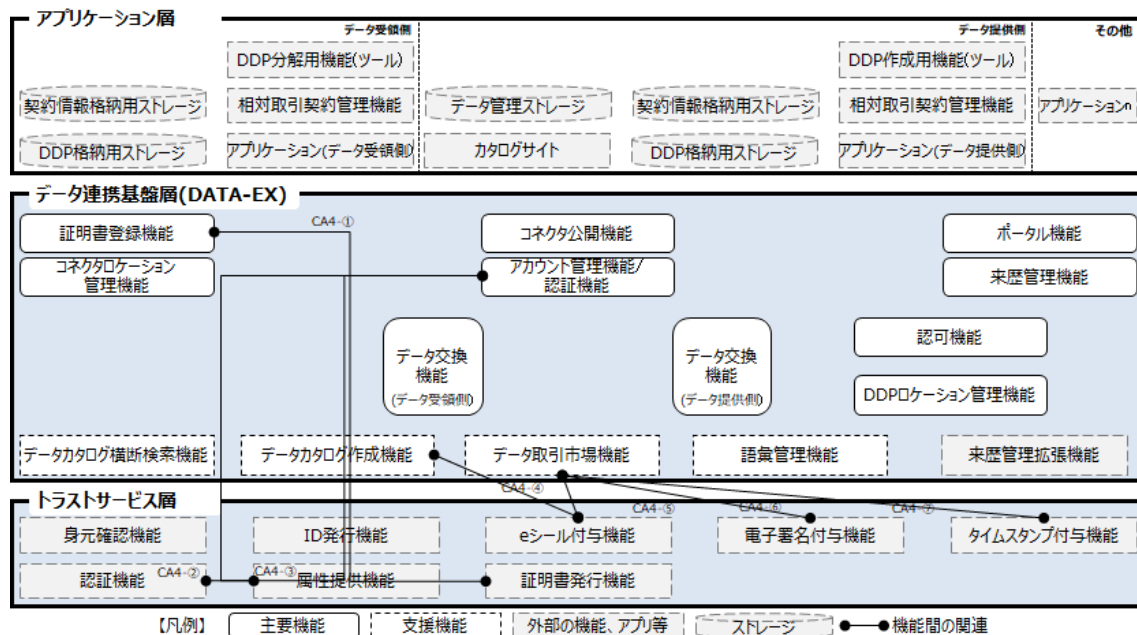


図 44:トラストサービス層のコンポーネントと DATA-EX のコンポーネント間のインタラクション

トラストサービス層のコンポーネントと DATA-EX のコンポーネント間のインタラクションとシナリオについて、各インタラクションがどのシナリオを実現するためのものか、対応関係を以下の表に示す。

表 6:トラストサービス層のコンポーネントと DATA-EX のコンポーネント間のインタラクション

インタラクション	対応するシナリオ	
	章節	対応するシナリオ
CA4-①	8-1-1-2 コネクタ構築 8-2-1-2 コネクタ構築 8-3-1-2 コネクタ構築	・コネクタの電子証明書発行
CA4-②	8-1-1-1 利用申請 8-2-1-1 利用申請 8-3-1-1 利用申請 他(サービス利用時)	・登録 ・支援サービス利用登録
CA4-③	8-1-1-1 利用申請 8-2-1-1 利用申請 8-3-1-1 利用申請	・登録 ・支援サービス利用登録
CA4-④	8-1-2-1 カタログ用意 8-2-2-1 カタログ用意 8-3-2-1 カタログ用意	・カタログ作成
CA4-⑤	-	- ※シナリオ記載なし

CA4-⑥	-	- ※シナリオ記載なし
CA4-⑦	-	- ※シナリオ記載なし

9-5. アプリケーション層のコンポーネントとトラストサービス層のコンポーネント間のインタラクション
 アプリケーション層のコンポーネントとトラストサービス層のコンポーネント間のインタラクション
 を示す。各説明冒頭の識別子は、下部に示す図中の識別子と対応している。

- CA5-① 相対取引契約管理機能(データ受領側)は、電子署名付与機能に対して、契約書等への電子署名の作成を依頼する。電子署名付与機能は、契約書等への電子署名を生成し、相対取引契約管理機能(データ受領側)に対して電子署名を返す。
- CA5-② 相対取引契約管理機能(データ受領側)は、e シール付与機能に対して、契約書等の e シールの作成を依頼する。e シール付与機能は、契約書等の e シールを生成し、相対取引契約管理機能(データ受領側)に対して e シールを返す。
- CA5-③ 相対取引契約管理機能(データ提供側)は、電子署名付与機能に対して、契約書等への電子署名の作成を依頼する。電子署名付与機能は、契約書等への電子署名を生成し、相対取引契約管理機能(データ提供側)に対して電子署名を返す。
- CA5-④ 相対取引契約管理機能(データ提供側)は、e シール付与機能に対して、契約書等の e シールの作成を依頼する。e シール付与機能は、契約書等の e シールを生成し、相対取引契約管理機能(データ提供側)に対して e シールを返す。
- CA5-⑤ 相対取引契約管理機能(データ提供側)は、タイムスタンプ付与機能に対して、契約書等へのタイムスタンプの作成を依頼する。タイムスタンプ付与機能は、契約書等へのタイムスタンプを生成し、相対取引契約管理機能(データ提供側)に対してタイムスタンプを返す。
- CA5-⑥ DDP 作成機能は、e シール付与機能に対して、作成した DDP の e シールの作成を依頼する。e シール付与機能は、DDP の e シールを生成し、DDP 作成用機能に対して e シールを返す。

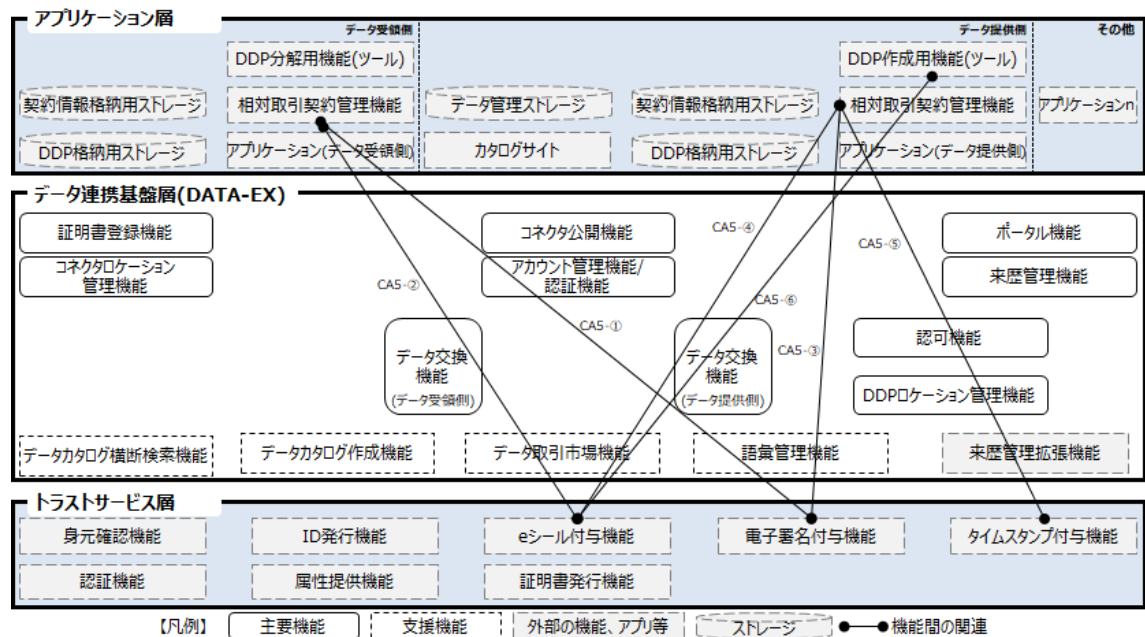


図 45: アプリケーション層のコンポーネントとトラストサービス層のコンポーネント間のインタラクション

トラストサービス層のコンポーネントと DATA-EX のコンポーネント間のインタラクションとシナリオについて、各インタラクションがどのシナリオを実現するためのものか、対応関係を以下の表に示す。

表 7: アプリケーション層のコンポーネントとトラストサービス層のコンポーネント間のインタラクション

インタラクション	対応するシナリオ	
	章節	対応するシナリオ
CA5-①	8-2-2-3 契約	・契約
CA5-②	8-2-2-3 契約	・契約
CA5-③	8-2-2-3 契約	・契約
CA5-④	8-2-2-3 契約	・契約
CA5-⑤	8-2-2-3 契約	・契約
CA5-⑥	8-1-2-3 DDP 作成 8-2-2-4 DDP 作成 8-3-2-4 DDP 作成	・DDP 作成

10. API 仕様

本章においては、DATA-EX の機能が提供する API について記載する。

10-1. API 一覧

DATA-EX の機能が提供する API について、一覧を記す。

表 8:API 一覧

機能	#	API
データ交換機能 (データ提供側)	1-1	カタログ検索
	1-2	データ交換
	1-3	認可トークン取得
	1-4	認可確認
	1-5	データ証憑通知(送信)
データ交換機能 (データ受領側)	2-1	カタログ検索
	2-2	データ交換
	2-3	認証トークン検証
	2-4	データ証憑通知(受信)
認証機能	3-1	トークン取得
	3-2	トークン取得(認可コード)
	3-3	トークン更新
	3-4	トークン検証
認可機能	4-1	認証機能連携(トークン交換)
	4-2	認可確認
	4-3	認可情報一覧取得
	4-4	認可情報取得
	4-5	認可情報登録
	4-6	認可情報削除
コネクタロケーション 管理機能	5-1	ロケーション情報取得
	5-2	ロケーション情報登録
	5-3	ロケーション情報削除
	5-4	全ロケーション情報取得
来歴管理機能	6-1	履歴登録
	6-2	来歴確認

10-2. API 仕様

10-2-1. データ交換機能(データ提供側)

10-2-1-1. カタログ検索

【API を提供する機能】 データ交換機能(データ提供側)

【API の機能概要】 カタログ情報を取得する。API ユーザーが指定した条件に従いカタログ情報を取得する。

【制約条件】 特になし

【HTTP メソッド】 GET

【URL パス】 /dataex/api/v1/catalog

【クエリパラメータ】

- q (string, optional)
CKAN 検索条件クエリ CKAN API [20] に準拠

【ヘッダパラメータ】

- Authorization (string, optional)
認証方式: Bearer。認証トークン(アクセストークン)

【必須 HTTP ヘッダ】 特になし

【レスポンス】

200: CKAN から取得したカタログ情報を返す。

【使用例】

API 呼び出しの curl コマンドの記述例を示す。

・ リクエスト例

```
curl -v -X GET 'https://provider01.r6-h.data-ex.org/dataex/api/v1/catalog?q=9e5ddec8-42c8-58fe-abc2-efde485ad674' ¥
```

```
-H "Authorization:Bearer 認証トークン"
```

・ レスポンス例

HTTP/1.x 200 OK

```
{"help": "https://ckan01.r6-h.data-ex.org/api/3/action/help_show?name=package_search",  
"success": true, "result": {"count": 15, カタログ情報、以下略}}
```

10-2-1-2. データ交換

【API を提供する機能】 データ交換機能(データ提供側)

【API の機能概要】 DDP ID に指定された DDP を取得する。

【制約条件】 特になし

【HTTP メソッド】 GET

【URL パス】 /dataex/api/v1/file

【ヘッダパラメータ】

- Authorization (string, optional)
認証方式: Bearer。認証トークン(アクセストークン)
- x-dataex-ddp-id (string, required)
DDP ID。DATA-EX 参加者(データ提供者)より通知された DDP ID を設定する。
- x-dataex-resource-api-type (string, required)

リソース提供手段識別子 FTP、HTTP のいずれかを指定する(FTP:file/ftp,
HTTP:file/http)

【必須 HTTP ヘッダ】 特になし

【レスポンス】

200: 取得したファイルを返す。

400: パラメータ確認時に必須パラメータが存在しない場合のエラーメッセージを返す。

403: 認証情報不正の場合のエラーメッセージを返す。

500: サーバーの内部処理で異常が発生した場合のエラーメッセージを返す。

[使用例]

API 呼び出しの curl コマンドの記述例を示す。

・ リクエスト例

```
curl -v -X GET 'https://provider01.r6-h.data-ex.org/dataex/api/v1/file' -H "x-dataex-ddp-id: 633db413-5bda-ae46-2568-f0ca23c8609e" -H "x-dataex-resource-api-type: file/http" ¥  
-H "Authorization:Bearer 認証トークン"
```

・ レスポンス例

HTTP/1.x 200 OK

{ [2993 bytes data] } ※ファイル(DDP)が返される

10-2-1-3. 認可トークン取得

【API を提供する機能】 データ交換機能(データ提供側)

【API の機能概要】 認可サーバーに対して、トークンフェデレーションリクエストを行い、認可トークンを返す。

【制約条件】 特になし

【HTTP メソッド】 GET

【URL パス】 /dataex/api/v1/token_federation

【ヘッダパラメータ】

- Authorization (string, required)
認証方式: Bearer。認証トークン
- x-dataex-provider (string, required)
DATA-EX ID(データ提供側)
- x-dataex-provider-connector-id (string, required)
コネクタ ID(データ提供側)
- x-dataex-provider-connector-secret (string, required)
データ提供側コネクタの電子証明書

【必須 HTTP ヘッダ】 特になし

【レスポンス】

200: 認可トークンを返す。

500: サーバーの内部処理で異常が発生した場合のエラーメッセージを返す。

【使用例】

API 呼び出しの curl コマンドの記述例を示す。

・リクエスト例

```
curl -v -X GET "http://provider_authorization:8080/dataex/api/v1/token_federation" -H
"Authorization: Bearer $access_token" -H "x-dataex-provider: f71ca873-5ca7-c158-b4ed-
1406c183c63c" -H "x-dataex-provider-connector-id: dc83d49-8c04-4662-9dcd-
547db8b465e7" -H "x-dataex-provider-connector-secret:
ENFHCyI6ri8idHABKbrg8s4bLm62GWi8"
```

・レスポンス例

HTTP/1.x 200 OK

x-dataex-auth-token: 認可トークン

x-dataex-consumer-id: m43kcyujiqyev4cqteekbtly3ivnc2bz

10-2-1-4. 認可確認

【API を提供する機能】 データ交換機能(データ提供側)

【API の機能概要】 認可サーバーに対して、認可確認をリクエストし、レスポンスを取得する。

【制約条件】 特になし

【HTTP メソッド】 GET

【URL パス】 /dataex/api/v1/token_contract

【ヘッダパラメータ】

- Authorization (string, required)
認証方式: Bearer。認証トークン
- x-dataex-provider (string, required)
DATA-EX ID(データ提供側)
- x-dataex-provider-connector-id (string, required)
コネクタ ID(データ提供側)
- x-dataex-provider-connector-secret (string, required)
データ提供側コネクタの電子証明書
- x-dataex-ddp-id (string, required)
DDP ID。DATA-EX 参加者(データ提供者)より通知された DDP ID を設定する。

【必須 HTTP ヘッダ】 特になし

【レスポンス】

200: 認可情報を返す。

403: 認証情報不正の場合のエラーメッセージを返す。

500: サーバーの内部処理で異常が発生した場合のエラーメッセージを返す。

【使用例】

API 呼び出しの curl コマンドの記述例を示す。

・ リクエスト例

```
curl -v -X GET "http://provider_authorization:8080/dataex/api/v1/token_contract" -H
"Authorization: Bearer $authz_token" -H "x-dataex-provider: f71ca873-5ca7-c158-b4ed-
1406c183c63c" -H "x-dataex-provider-connector-id: dc83d49-8c04-4662-9dcd-
547db8b465e7" -H "x-dataex-provider-connector-secret:
ENFHCyI6ri8idHABKbrg8s4bLm62GWi8" -H "x-dataex-ddp-id: 633db413-5bda-ae46-2568-
f0ca23c8609e"
```

・ レスポンス例

HTTP/1.x 200 OK

10-2-1-5. データ証憑通知(送信)

【API を提供する機能】 データ交換機能(データ提供側)

【API の機能概要】 データ取引市場等の契約管理サービスにデータ証憑通知(送信)を行う。

【制約条件】 特になし

【HTTP メソッド】 POST

【URL パス】 /dataex/api/v1/voucher/sent

【ヘッダパラメータ】

- Authorization (string, required)
認証方式: Bearer。認証トークン
- x-dataex-provider (string, required)
DATA-EX ID(データ提供側)
- x-dataex-consumer (string, required)
DATA-EX ID(データ受領側)
- x-dataex-contract-id (string, required)
データ取引市場等で設定される取引 ID
- x-dataex-hash-get-data (string, required)
ハッシュ値 取得したデータを特定のハッシュアルゴリズムによってハッシュ化した値
- x-dataex-contract-management-service-url (string, required)
データ取引市場等の契約管理サービス URL

【必須 HTTP ヘッダ】 特になし

【レスポンス】

200: 処理完了のレスポンスを返す。

500: サーバーの内部処理で異常が発生した場合のエラーメッセージを返す。

【使用例】

API 呼び出しの curl コマンドの記述例を示す。

・リクエスト例

```
curl -v -X POST "http://provider_provenance_management:8080/dataex/api/v1/voucher/sent"
¥
```

```
-H "x-dataex-provider: f71ca873-5ca7-c158-b4ed-1406c183c63c" ¥
```

```
-H "x-dataex-consumer: m43kcyujiqyev4cqteekbtly3ivnc2bz" ¥
```

```
-H "x-dataex-contract-id: 2501210657166581" ¥
```

```
-H "x-dataex-hash-get-data:
```

```
3cf46a39747c7e41ee10bc0ca63575a81507b4e0f1596eea4c0e759028a258a931b82152cb71031e52
f688f2afda62999709796d2c22cd4a4968345b93cf000b" ¥
```

```
-H "x-dataex-contract-management-service-url: https://data-ex.every-sense.com" ¥
```

```
-H "Authorization: Bearer 認証トークン
```

・レスポンス例

HTTP/1.x 200 OK

10-2-2. データ交換機能(データ受領側)

10-2-2-1. カタログ検索

【APIを提供する機能】 データ交換機能(データ受領側)

【APIの機能概要】 カタログ情報を取得する。API ユーザーが指定した条件に従いカタログ情報を取得する。

【制約条件】 特になし

【HTTP メソッド】 GET

【URL パス】 /dataex/api/v1/catalog

【クエリパラメータ】

- q (string, optional)
CKAN 検索条件クエリ CKAN API [20]に準拠

【ヘッダパラメータ】

- Authorization (string, optional)
認証方式: Bearer。認証トークン(アクセストークン)
- x-dataex-search (string, required)
検索種別
 - ・ 横断検索: meta 横断検索サーバーから検索する。
※x-dataex-dataspace が「ids-dsc」の場合はブローカ検索を実施

-
- ・ 提供者内検索: detail 提供者内カタログを検索する。
※x-dataex-dataspace が「ids-dsc」の場合は x-dataex-provider で指定する提供者から検索を実施

- x-dataex-provider (string, optional)

提供者コネクタ ID。提供者コネクタを利用する場合に提供者コネクタ ID を設定する。
提供者コネクタを利用しない場合は x-dataex-provider のヘッダ自体を設定しない。
※x-dataex-dataspace が「ids-dsc」の場合は、検索対象とする提供者コネクタの URL を指定する。

- x-dataex-dataspace (string, optional)

コネクタ識別子。本識別子により、DATA-EX のコネクタを使用するか、DATA-EX 以外のコネクタを使用するかを判断する。省略した場合は、DATA-EX のコネクタを使用する。

dataex: DATA-EX のコネクタ

ids-dsc: IDS Dataspace Connector (Fraunhofer Dataspace Connector)

【必須 HTTP ヘッダ】 特になし

【レスポンス】

200: CKAN から取得したカタログ情報を返す。

400: パラメータ確認時に必須パラメータが存在しない場合のエラーメッセージ

403: 認証情報不正の場合のエラーメッセージ

500: サーバーの内部処理で異常が発生した場合のエラーメッセージ

【使用例】

API 呼び出しの curl コマンドの記述例を示す。

・ リクエスト例

```
curl -v -X GET 'https://consumer03.r6-h.data-ex.org/dataex/api/v1/catalog?q=dataex_dataset_id_for_detail:85ecfdd0-ea3c-503a-9ca8-584326810e7c' ¥
```

```
-H "x-dataex-search:detail" ¥
```

```
-H "x-dataex-provider: dc83d49-8c04-4662-9dcd-547db8b465e7" ¥
```

```
-H "Authorization:Bearer 認証トークン"
```

・ レスポンス例

HTTP/1.x 200 OK

```
{"help": "https://ckan01.r6-h.data-ex.org/api/3/action/help_show?name=package_search",  
"success": true, "result": {"count": 1, カタログ情報、以下略}}
```

10-2-2-2. データ交換

【API を提供する機能】 データ交換機能(データ受領側)

【API の機能概要】 DDP ID に指定された DDP を取得する。

【制約条件】 特になし

【HTTP メソッド】 GET

【URL パス】 /dataex/api/v1/file

【ヘッダパラメータ】

- Authorization (string, optional)
認証方式: Bearer。認証トークン(アクセストークン)
- x-dataex-ddp-id (string, required)
DDP ID。DATA-EX 参加者(データ提供者)より通知された DDP ID を設定する。
- x-dataex-resource-api-type (string, required)
リソース提供手段識別子 FTP、HTTP のいずれかを指定する(FTP:file/ftp, HTTP:file/http)
- x-dataex-provider (string, optional)
提供者コネクタ ID 提供者コネクタを利用する場合に提供者コネクタ ID を設定する。提供者コネクタを利用しない場合は x-dataex-provider のヘッダ自体を設定しない。※x-dataex-dataspace が「ids-dsc」の場合は、本パラメータを参照しない。
- x-dataex-dataspace (string, optional)
コネクタ識別子。本識別子により、DATA-EX のコネクタを使用するか、DATA-EX 以外のコネクタを使用するかを判断する。省略した場合は、DATA-EX のコネクタを使用する。
dataex: DATA-EX のコネクタ
ids-dsc: IDS Dataspace Connector (Fraunhofer Dataspace Connector)

【必須 HTTP ヘッダ】 特になし

【レスポンス】

200: 取得したファイルを返す。

400: パラメータ確認時に必須パラメータが存在しない場合のエラーメッセージを返す。

403: 認証情報不正の場合のエラーメッセージを返す。

500: サーバーの内部処理で異常が発生した場合のエラーメッセージを返す。

【使用例】

API 呼び出しの curl コマンドの記述例を示す。

```
curl -v -X GET 'https://consumer03.r6-h.data-ex.org/dataex/api/v1/file' ¥
-H "x-dataex-ddp-id: 633db413-5bda-ae46-2568-f0ca23c8609e" ¥
-H "x-dataex-resource-api-type:file/http" ¥
-H "x-dataex-provider: dc83d49-8c04-4662-9dcd-547db8b465e7" ¥
-H "x-dataex-dataspace:dataex" ¥
-H "Authorization:Bearer 認証トークン"
```

・レスポンス例

HTTP/1.x 200 OK

{ [2993 bytes data] } ※ファイル(DDP)が返される

10-2-2-3. 認証トークン検証

【API を提供する機能】 データ交換機能(データ受領側)

【API の機能概要】 認証機能に対して、トークンイントロスペクションを行い、DATA-EX ID(データ受領側)を返す。

【制約条件】 特になし

【HTTP メソッド】 GET

【URL パス】 /dataex/api/v1/token_introspect

【ヘッダパラメータ】

- Authorization (string, required)
認証方式: Bearer。認証トークン
- x-dataex-consumer-connector-id (string, required)
コネクタ ID(データ受領側)

【必須 HTTP ヘッダ】 特になし

【レスポンス】

200: DATA-EX ID(データ受領側)を返す。

400: パラメータ不正の場合のエラーメッセージを返す。

403: 認証情報不正の場合のエラーメッセージを返す。

500: サーバーの内部処理で異常が発生した場合のエラーメッセージを返す。

【使用例】

API 呼び出しの curl コマンドの記述例を示す。

・リクエスト例

```
curl -v -X GET "http://consumer_authentication:8080/dataex/api/v1/token_introspect" -H  
"Authorization: Bearer $access_token" -H "x-dataex-consumer-connector-id: 060f4b69-a539-  
4664-b7ba-68be89b304e5"
```

・レスポンス例

HTTP/1.x 200 OK

x-dataex-consumer-id: m43kcyujiqyev4cqteekbtly3ivnc2bz

10-2-2-4. データ証憑通知(受信)

【API を提供する機能】 データ交換機能(データ受領側)

【API の機能概要】 データ取引市場等の契約管理サービスにデータ証憑通知(受信)を行う。

【制約条件】 特になし

【HTTP メソッド】 POST**【URL パス】** /dataex/api/v1/voucher/received**【ヘッダパラメータ】**

- Authorization (string, required)
認証方式: Bearer。認証トークン
- x-dataex-provider (string, required)
DATA-EX ID (データ提供側)
- x-dataex-consumer (string, required)
DATA-EX ID (データ受領側)
- x-dataex-contract-id (string, required)
データ取引市場等で設定される取引 ID
- x-dataex-hash-get-data (string, required)
ハッシュ値 取得したデータを特定のハッシュアルゴリズムによってハッシュ化した値
- x-dataex-contract-management-service-url (string, required)
データ取引市場等の契約管理サービス URL

【必須 HTTP ヘッダ】 特になし**【レスポンス】**

200: 処理完了のレスポンスを返す。

500: サーバーの内部処理で異常が発生した場合のエラーメッセージを返す。

【使用例】

API 呼び出しの curl コマンドの記述例を示す。

・ リクエスト例

```
curl -v -X POST
```

```
"http://consumer_provenance_management:8080/dataex/api/v1/voucher/received" ¥
```

```
-H "x-dataex-provider: f71ca873-5ca7-c158-b4ed-1406c183c63c" ¥
```

```
-H "x-dataex-consumer: m43kcyujiqyev4cqteekbtly3ivnc2bz" ¥
```

```
-H "x-dataex-contract-id: 2501210657166581" ¥
```

```
-H "x-dataex-hash-get-data:
```

```
3cf46a39747c7e41ee10bc0ca63575a81507b4e0f1596eea4c0e759028a258a931b82152cb71031e52  
f688f2afda62999709796d2c22cd4a4968345b93cf000b" ¥
```

```
-H "x-dataex-contract-management-service-url: https://data-ex.every-sense.com" ¥
```

```
-H "Authorization: Bearer 認証トークン"
```

・ レスポンス例

```
HTTP/1.x 200 OK
```

10-2-3. 認証機能

10-2-3-1. トークン取得

【API を提供する機能】 認証機能

【API の機能概要】 アクセストークンを取得する。

【制約条件】 特になし

【HTTP メソッド】 POST

【URL パス】 /dataex/api/v1/token

【リクエストボディ】

- user_id (string, required)
DATA-EX ID
- password (string, required)
パスワード
- totp (string, required)
ワンタイムパスワード

【必須 HTTP ヘッダ】

Authorization ヘッダ

「クライアント ID:シークレット」を Base64 エンコードした値

【レスポンス】

200: アクセストークン、リフレッシュトークンを返す。

401: 認証情報不正の場合のエラーメッセージを返す。

422: リクエストのフォーマット不正の場合のエラーメッセージを返す。

500: サーバーの内部処理で異常が発生した場合のエラーメッセージを返す。

【使用例】

API 呼び出しの curl コマンドの記述例を示す。

・ リクエスト例

```
curl -v -X POST https://authn.r6-h.data-ex.org/dataex/api/v1/token ¥  
-H "Authorization:Basic  
N2RhMTc2N2YtYjJjNi1hM2Q2LTFiMjctOGYwNDdhMTY5NTAyOnI5YUYwVnZlSlp0eXRiVGhZdE41  
dmQyUXIzcnRCcEdP" ¥  
-d '{"user_id": "c4b64ef6-8da4-f108-a0e8-7bd1fed94162", "password": "pass", "totp":  
"183490"}'
```

・ レスポンス例

HTTP/1.x 200 OK

```
{"access_token": "アクセストークン", "refresh_token": "リフレッシュトークン"}
```

10-2-3-2. トークン取得(認可コード)

【API を提供する機能】 認証機能

【API の機能概要】 アクセストークンを取得する。

【制約条件】 特になし

【HTTP メソッド】 POST

【URL パス】 /dataex/api/v1/token/authorizationCode

【リクエストボディ】

- code (string, required)
認可コード
- redirect_uri (string, required)
リダイレクト URI

【必須 HTTP ヘッダ】

Authorization ヘッダ

「クライアント ID:シークレット」を Base64 エンコードした値

【レスポンス】

200: アクセストークン、リフレッシュトークンを返す。

401: 認証情報不正の場合のエラーメッセージを返す。

422: リクエストのフォーマット不正の場合のエラーメッセージを返す。

500: サーバーの内部処理で異常が発生した場合のエラーメッセージを返す。

【使用例】

API 呼び出しの curl コマンドの記述例を示す。

・ リクエスト例

```
curl -v -X POST "https://authn.r6-h.data-ex.org/dataex/api/v1/token/authorizationCode" \
-H "Authorization: Basic
MDYwZjRiNjktYTUzOS00NjY0LWI3YmEtNjhiZTg5YjMwNGU1OnFMaUt1S3V4UjhvaHZzcVpnbNny
eHI3NEE1MkRPNINP" \
-d '{
  "code": "6c480bfa-c797-45fd-aa51-d8e2a24d8d3c.3d1041cd-7030-4684-8142-
7f5924bdfcc0.9b205b0c-9abc-4863-b1d6-2cdd1507d1e7",
  "redirect_uri": "http://localhost:8080"
}'
```

・ レスポンス例

HTTP/1.x 200 OK

{“access_token”:アクセストークン,“refresh_token”:リフレッシュトークン}

10-2-3-3. トークン更新

【API を提供する機能】 認証機能

【API の機能概要】 認証トークンを更新する。

【制約条件】 特になし

【HTTP メソッド】 POST

【URL パス】 /dataex/api/v1/token/refresh

【リクエストボディ】

- refresh_token (string, required)

リフレッシュトークン

【必須 HTTP ヘッダ】

Authorization ヘッダ

「クライアント ID:シークレット」を Base64 エンコードした値

【レスポンス】

200: アクセストークン、リフレッシュトークンを返す。

401: 認証情報不正の場合のエラーメッセージを返す。

422: リクエストのフォーマット不正の場合のエラーメッセージを返す。

500: サーバーの内部処理で異常が発生した場合のエラーメッセージを返す。

【使用例】

API 呼び出しの curl コマンドの記述例を示す。

・ リクエスト例

```
curl -v -X POST https://authn.r6-h.data-ex.org/dataex/api/v1/token/refresh ¥
-H "Authorization:Basic
N2RhMTc2N2YtYjJjNi1hM2Q2LTFiMjctOGYwNDdhMTY5NTAyOnI5YUYwVnZlSlp0eXRiVGhZdE41
dmQyUXIzcnRCcEdP" ¥
-d '{"refresh_token": "リフレッシュトークン"}
```

・ レスポンス例

HTTP/1.x 200 OK

```
{"message": "success", "access_token": "アクセストークン", "refresh_token": "リフレッシュトークン"}
```

10-2-3-4. トークン検証

【API を提供する機能】 認証機能

【API の機能概要】 認証トークンを検証する。

【制約条件】 特になし

【HTTP メソッド】 POST

【URL パス】 /dataex/api/v1/token/introspect

【リクエストボディ】

-
- access_token (string, required)

アクセストークン

【必須 HTTP ヘッダ】

Authorization ヘッダ

「クライアント ID:シークレット」を Base64 エンコードした値

【レスポンス】

200: 正常終了し、DATA-EX ID を返す。

401: 認証情報不正の場合のエラーメッセージを返す。

422: リクエストのフォーマット不正の場合のエラーメッセージを返す。

500: サーバーの内部処理で異常が発生した場合のエラーメッセージを返す。

【使用例】

API 呼び出しの curl コマンドの記述例を示す。

・リクエスト例

```
curl -v -X POST https://authn.r6-h.data-ex.org/dataex/api/v1/token/introspect ¥  
-H "Authorization:Basic  
N2RhMTc2N2YtYjJiNi1hM2Q2LTFiMjctOGYwNDdhMTY5NTAyOnI5YUYwVnZlSlp0eXRiVGhZdE41  
dmQyUXIzcnRCcEdP" ¥  
-d '{"access_token":アクセストークン}'
```

・レスポンス例

```
HTTP/1.x 200 OK  
{"user_id":"c4b64ef6-8da4-f108-a0e8-7bd1fed94162"}
```

10-2-4. 認可機能

10-2-4-1. 認証機能連携(トークン交換)

【API を提供する機能】 認可機能

【API の機能概要】 認証機能と連携し、認証トークンと引き換えに認可トークンを取得する

【制約条件】 特になし

【HTTP メソッド】 POST

【URL パス】 /dataex/api/v1/token/federate

【リクエストボディ】

- access_token (string, required)
アクセストークン(認証トークン)
- provider_id (string, required)
DATA-EX ID(データ提供側)

【必須 HTTP ヘッダ】

Authorization ヘッダ

「クライアント ID:シークレット」を Base64 エンコードした値

【レスポンス】

200: アクセストークン(認可トークン)を返す。

403: 認証トークン不正の場合のエラーメッセージを返す。

422: リクエストのフォーマット不正の場合のエラーメッセージを返す。

【使用例】

API 呼び出しの curl コマンドの記述例を示す。

・リクエスト例

```
curl -v -X POST https://authz01.r6-h.data-ex.org/dataex/api/v1/token/federate ¥
-H "Authorization:Basic
ZGM4M2Q0OS04YzA0LTQ2NjltOWRjZC01NDdkYjhiNDY1ZTc6RU5GSEN5STZyaThpZEhBQkticm
c4czRiTG02MkdXaTg=" ¥
-d '{
  "access_token":アクセストークン,"provider_id": "f71ca873-5ca7-c158-b4ed-1406c183c63c"
}
```

・レスポンス例

HTTP/1.x 200 OK

{“access_token”:アクセストークン(認可トークン)}

10-2-4-2. 認可確認

【API を提供する機能】 認可機能

【API の機能概要】 認可トークンにより DDP にアクセスしてよいかを確認する

【制約条件】 特になし

【HTTP メソッド】 POST

【URL パス】 /dataex/api/v1/authz/confirm

【リクエストボディ】

- access_token (string, required)
アクセストークン(認可トークン)
- provider_id (string, required)
DATA-EX ID(データ提供側)
- x-dataex-ddp-id (string, required)
DDP ID。DATA-EX 参加者(データ提供者)より通知された DDP ID を設定する。

【必須 HTTP ヘッダ】

Authorization ヘッダ

「クライアント ID:シークレット」を Base64 エンコードした値

【レスポンス】

200: アクセス権限ありを返す。
403: アクセス権限なしを返す。
404: DDP ID が存在しないを返す。
422: リクエストのフォーマット不正の場合のエラーメッセージを返す。
500: サーバーの内部処理で異常が発生した場合のエラーメッセージを返す。

[使用例]

API 呼び出しの curl コマンドの記述例を示す。

・リクエスト例

```
curl -v -X POST https://authz01.r6-h.data-ex.org/dataex/api/v1/authz/confirm ¥  
-H "Authorization:Basic  
ZGM4M2Q0OS04YzA0LTQ2NjltOWRjZC01NDdkYjhiNDY1ZTc6RU5GSEN5STZyaThpZEhBQkticm  
c4czRiTG02MkdXaTg=" ¥  
-d '{  
  "access_token":アクセストークン,"provider_id": "f71ca873-5ca7-c158-b4ed-1406c183c63c",  
  "x-dataex-ddp-id": "633db413-5bda-ae46-2568-f0ca23c8609e"  
}'
```

・レスポンス例

HTTP/1.x 200 OK

10-2-4-3. 認可情報一覧確認

【API を提供する機能】 認可機能

【API の機能概要】 認可情報一覧を取得する

【制約条件】 特になし

【HTTP メソッド】 GET

【URL パス】 /dataex/api/v1/authorization_list

【クエリパラメータ】

- assigner (string, optional)
DATA-EX ID(データ提供側)

【必須 HTTP ヘッダ】

Authorization ヘッダ

Bearer トークンとして認証トークンを付与する

【レスポンス】

200: 認可情報を返す。
403: 認証トークン不正の場合のエラーメッセージを返す。
404: 認可情報が存在しないを返す。
422: リクエストのフォーマット不正の場合のエラーメッセージを返す。

500: サーバーの内部処理で異常が発生した場合のエラーメッセージを返す。

[使用例]

API 呼び出しの curl コマンドの記述例を示す。

・リクエスト例

```
curl -v -X GET https://authz01.r6-h.data-ex.org/dataex/api/v1/authorization_list?assigner=f71ca873-5ca7-c158-b4ed-1406c183c63c ¥  
-H "Authorization:Bearer 認証トークン"
```

・レスポンス例

HTTP/1.x 200 OK

```
{ "permission": { "assignee": { "user": "m43kcyujiqyev4cqteekbtly3ivnc2bz" }, "target": "633db413-5bda-ae46-2568-f0ca23c8609e", "assigner": "f71ca873-5ca7-c158-b4ed-1406c183c63c" },  
  [ "permission": { "assignee": { "user": "ec8cb701-f4bf-c1fe-7470-b5b084ce94e9" }, "target": "633db413-5bda-ae46-2568-f0ca23c8609e", "assigner": "f71ca873-5ca7-c158-b4ed-1406c183c63c" } ] }
```

10-2-4-4. 認可情報取得

【API を提供する機能】 認可機能

【API の機能概要】 指定した DDP ID に関する認可情報を取得する

【制約条件】 特になし

【HTTP メソッド】 GET

【URL パス】 /dataex/api/v1/authorization

【クエリパラメータ】

- assigner (string, required)
DATA-EX ID(データ提供側)
- target (string, required)
DDP ID

【必須 HTTP ヘッダ】

Authorization ヘッダ

Bearer トークンとして認証トークンを付与する

【レスポンス】

200: 認可情報を返す。

403: 認証トークン不正の場合のエラーメッセージを返す。

404: 認可情報が存在しないを返す。

422: リクエストのフォーマット不正の場合のエラーメッセージを返す。

500: サーバーの内部処理で異常が発生した場合のエラーメッセージを返す。

[使用例]

API 呼び出しの curl コマンドの記述例を示す。

・ リクエスト例

```
curl -v -X GET "https://authz01.r6-h.data-  
ex.org/dataex/api/v1/authorization?assigner=f71ca873-5ca7-c158-b4ed-  
1406c183c63c&target=633db413-5bda-ae46-2568-f0ca23c8609e" ¥  
-H "Authorization:Bearer 認証トークン"
```

・ レスポンス例

```
HTTP/1.x 200 OK  
{"permission":{"assignee":{"user":"m43kcyujiqyev4cqteekbtly3ivnc2bz"},"target":"633db413-  
5bda-ae46-2568-f0ca23c8609e"},"assigner":"f71ca873-5ca7-c158-b4ed-1406c183c63c"}}
```

10-2-4-5. 認可情報登録

【API を提供する機能】 認可機能

【API の機能概要】 認可情報を登録・更新する

【制約条件】 特になし

【HTTP メソッド】 POST

【URL パス】 /dataex/api/v1/authorization

【リクエストボディ】

- target (string, required)
DDP ID
- assigner (string, required)
DATA-EX ID(データ提供側)
- user (string, optional)
DATA-EX ID(データ受領側)
- org (string, optional)
組織レベルでの DATA-EX ID(データ受領側)
- aal (string, optional)
当人認証レベル
- extras (string, optional)
その他の属性
- trade_id (string, optional)
取引 ID
- contract_url (string, optional)
契約管理サービス URL
- contract_type (string, optional)
契約形態

【必須 HTTP ヘッダ】

Authorization ヘッダ

Bearer トークンとして認証トークンを付与する

【レスポンス】

200: 認可情報更新成功。

403: 認証トークン不正の場合のエラーメッセージを返す。

404: 認可情報が存在しないを返す。

422: リクエストのフォーマット不正の場合のエラーメッセージを返す。

500: サーバーの内部処理で異常が発生した場合のエラーメッセージを返す。

【使用例】

API 呼び出しの curl コマンドの記述例を示す。

・ リクエスト例

```
$ curl -v -X POST "https://authz01.r6-h.data-ex.org/dataex/api/v1/authorization" ¥
```

```
-H "Authorization:Bearer 認証トークン" ¥
```

```
-d '{
```

```
  "permission": {
```

```
    "target": "633db413-5bda-ae46-2568-f0ca23c8609e",
```

```
    "assigner": "f71ca873-5ca7-c158-b4ed-1406c183c63c",
```

```
    "assignee": {
```

```
      "user": "test-user",
```

```
      "org": "",
```

```
      "aal": 2,
```

```
      "extras": ""
```

```
    }
```

```
  },
```

```
  "contract": {
```

```
    "trade_id": "",
```

```
    "contract_url": "",
```

```
    "contract_type": ""
```

```
  }
```

```
}'
```

・レスポンス例

HTTP/1.x 200 OK

```
{"message": "success"}
```

10-2-4-6. 認可情報削除

【API を提供する機能】 認可機能

【API の機能概要】 認可情報を削除する

【制約条件】 特になし

【HTTP メソッド】 DELETE

【URL パス】 /dataex/api/v1/authorization

【リクエストボディ】

- target (string, required)
DDP ID
- assigner (string, required)
DATA-EX ID(データ提供側)
- user (string, optional)
DATA-EX ID(データ受領側)
- org (string, optional)
組織レベルでの DATA-EX ID(データ受領側)
- aal (string, optional)
当人認証レベル
- extras (string, optional)
その他の属性
- trade_id (string, optional)
取引 ID

【必須 HTTP ヘッダ】

Authorization ヘッダ

Bearer トークンとして認証トークンを付与する

【レスポンス】

200: 認可情報削除成功。

403: 認証トークン不正の場合のエラーメッセージを返す。

404: 認可情報が存在しないを返す。

422: リクエストのフォーマット不正の場合のエラーメッセージを返す。

500: サーバーの内部処理で異常が発生した場合のエラーメッセージを返す。

【使用例】

API 呼び出しの curl コマンドの記述例を示す。

・ リクエスト例

```
curl -v -X DELETE "https://authz01.r6-h.data-ex.org/dataex/api/v1/authorization" \
-H "Authorization:Bearer 認証トークン" \
-d '{
```

```
"permission": {
  "target": "633db413-5bda-ae46-2568-f0ca23c8609e",
  "assigner": "f71ca873-5ca7-c158-b4ed-1406c183c63c",
  "assignee": {
    "user": "test-user",
    "org": "",
    "aal": 2,
    "extras": ""
  }
},
"contract": {
  "trade_id": ""
}
}
```

・レスポンス例

HTTP/1.x 200 OK

```
{"message": "success"}
```

10-2-5. コネクタロケーション管理機能

10-2-5-1. ロケーション情報取得

【APIを提供する機能】 コネクタロケーション管理機能

【APIの機能概要】 指定したコネクタ ID に該当するコネクタ URL を取得する

【制約条件】 特になし

【HTTP メソッド】 GET

【URL パス】 /dataex/api/v1/location/{connector_id}

【ヘッダパラメータ】

- Authorization (string, required)
認証方式: Bearer。認証トークン

【リクエストパラメータ】

- connector_id (string, required)
コネクタ ID

【必須 HTTP ヘッダ】 特になし

【レスポンス】

200: コネクタ URL を返す。

401: 認証トークン不正の場合のエラーメッセージを返す。

404:コネクタ ID が存在しない場合のエラーメッセージを返す。

422:リクエストのフォーマット不正の場合のエラーメッセージを返す。

[使用例]

API 呼び出しの curl コマンドの記述例を示す。

・ リクエスト例

```
curl -v GET http://localhost:8080/dataex/api/v1/location/35e6f89e-cab4-f459-2eda-8ce46d16d5bc ¥
```

```
-H "Authorization:Bearer 認証トークン"
```

・ レスポンス例

HTTP/1.x 200 OK

```
{ "connector_id": "35e6f89e-cab4-f459-2eda-8ce46d16d5bc", "connector_url": "https://provider02.r6-h.data-ex.org/" }
```

10-2-5-2. ロケーション情報登録

【API を提供する機能】 コネクタロケーション管理機能

【API の機能概要】 コネクタのロケーション情報を登録する。

【制約条件】 特になし

【HTTP メソッド】 POST

【URL パス】 /dataex/api/v1/location/{connector_id}

【リクエストパラメータ】

- connector_id (string, required)
コネクタ ID
- connector_url (string, required)
コネクタ URL

【必須 HTTP ヘッダ】 特になし

【レスポンス】

200:登録成功。

403:認証情報不正の場合のエラーメッセージを返す。

422:リクエストのフォーマット不正の場合のエラーメッセージを返す。

[使用例]

API 呼び出しの curl コマンドの記述例を示す。

・ リクエスト例

```
curl -v -X POST http://localhost:8080/dataex/api/v1/location ¥  
-d '{  
  "connector_id": "api_test",  
  "connector_url": "https://api_test"
```

```
}'
```

・レスポンス例

HTTP/1.x 200 OK

```
{"connector_id":"api_test","connector_url":"https://api_test/"}
```

10-2-5-3. ロケーション情報削除

【APIを提供する機能】 コネクタロケーション管理機能

【APIの機能概要】 コネクタのロケーション情報を削除する。

【制約条件】 特になし

【HTTP メソッド】 DELETE

【URL パス】 /dataex/api/v1/location/{connector_id}

【ヘッダパラメータ】

- Authorization (string, required)
認証方式: Bearer。認証トークン

【リクエストパラメータ】

- connector_id (string, required)
コネクタ ID

【必須 HTTP ヘッダ】 特になし

【レスポンス】

200: 削除成功。

403: 認証情報不正の場合のエラーメッセージを返す。

409: リクエストが競合した場合のエラーメッセージを返す。

422: リクエストのフォーマット不正の場合のエラーメッセージを返す。

【使用例】

API 呼び出しの curl コマンドの記述例を示す。

・リクエスト例

```
curl -v -X DELETE http://localhost:8080/dataex/api/v1/location/api_test ¥  
-H "Authorization:Bearer 認証トークン"
```

・レスポンス例

HTTP/1.x 200 OK

10-2-5-4. 全ロケーション情報取得

【APIを提供する機能】 コネクタロケーション管理機能

【APIの機能概要】 全てのコネクタのロケーション情報を取得する。

【制約条件】 特になし

【HTTP メソッド】 GET

【URL パス】 /dataex/api/v1/locations

【ヘッダパラメータ】

- Authorization (string, required)
認証方式: Bearer。認証トークン

【必須 HTTP ヘッダ】 特になし

【レスポンス】

- 200: コネクタ ID とコネクタ URL を返す。
- 403: 認証情報不正の場合のエラーメッセージを返す。
- 422: リクエストのフォーマット不正の場合のエラーメッセージを返す。

【使用例】

API 呼び出しの curl コマンドの記述例を示す。

・ リクエスト例

```
curl -v GET http://localhost:8080/dataex/api/v1/locations ¥  
-H "Authorization:Bearer 認証トークン"
```

・ レスポンス例

HTTP/1.x 200 OK

```
{"connector_id": "aaa", "connector_url": "bbb", "id": 4},  
{"connector_id": "35e6f89e-cab4-f459-2eda-  
8ce46d16d5bc", "connector_url": "https://provider02.r6-h.data-ex.org/", "id": 5}
```

10-2-6. 来歴管理機能

10-2-6-1. 履歴登録

【API を提供する機能】 来歴管理機能

【API の機能概要】 指定した DDP ID の履歴情報を登録する

【制約条件】 特になし

【HTTP メソッド】 POST

【URL パス】 /dataex/api/v1/eventwithhash

【ヘッダパラメータ】

- Authorization (string, required)
認証方式: Bearer。認証トークン

【リクエストパラメータ】

- eventtype (string, required)
履歴の種類
- ddp_id (string, required)
DDP ID

-
- dataprovider (string, required)
DATA-EX ID(データ提供側)
 - datauser (string)
DATA-EX ID(データ受領側)
 - timestamp (string, required)
履歴が生じた日時
 - previousevents (string[])
1つ前の履歴情報の履歴 ID
 - ddp_hash (string)
DDP のハッシュ値
 - access_control_policy (string[])
アクセス制御ポリシー

【必須 HTTP ヘッダ】 特になし

【レスポンス】

200: 履歴 ID を返す。

400: パラメータ確認時に必須パラメータが存在しない場合のエラーメッセージを返す。

401: 認証情報不正の場合のエラーメッセージを返す。

500: サーバーの内部処理で異常が発生した場合のエラーメッセージを返す。

【使用例】

・リクエスト例

```
{  
  "eventtype": "string",  
  "ddp_id": "string",  
  "dataprovider": "string",  
  "datauser": "string",  
  "timestamp": "string",  
  "previousevents": "string"  
}
```

・レスポンス例

```
{  
  "event_id": "string"  
}
```

10-2-6-2. 来歴確認

【APIを提供する機能】 来歴管理機能

【APIの機能概要】 指定した DDP ID に関連する来歴情報を取得する

【制約条件】 特になし

【HTTP メソッド】 GET

【URL パス】 /dataex/api/v1/lineage/{ddp_id}

【ヘッダパラメータ】

- Authorization (string, required)
認証方式: Bearer。認証トークン

【必須 HTTP ヘッダ】 特になし

【レスポンス】

200: 来歴情報を返す。

400: パラメータ確認時に必須パラメータが存在しない場合のエラーメッセージを返す。

401: 認証情報不正の場合のエラーメッセージを返す。

500: サーバーの内部処理で異常が発生した場合のエラーメッセージを返す。

【使用例】

・レスポンス例

```
[[
  "evend_id": "string",
  "eventtype": "string",
  "ddp_id": "string",
  "dataproducer": "string",
  "datauser": "string",
  "timestamp": "string",
],
[
  "evend_id": "string",
  "eventtype": "string",
  略
  "timestamp": "string",
  "previousevents": "string"
],
[
  "evend_id": "string",
  "eventtype": "string",
  略
  "timestamp": "string",
  "previousevents": "string"
]]
```

10-3. 【付録】API 仕様の定義方法

API の定義は、【XXX】で示したタグに対して、その値となる文字列の記載方法を示す。

【API を提供する機能】

API を提供する DATA-EX の機能の名前を記載する。

【API の機能概要】

API の機能を説明する文字列を記載する。

【制約条件】

API の利用時の制約条件(アクセスコントロール情報等)を文字列で示す。

【HTTP メソッド】

HTTP メソッドを表現する文字列を記載する。

【URL パス】

API のパス名を URL で示す。

【パラメータ】

パラメータの分類、パラメータ名、パラメータの必須区分および説明を表現する文字列を記載する。

【必須 HTTP ヘッダ】

必須の HTTP ヘッダ名および当該ヘッダ名の説明を表現する文字列を記載する。なお、ない場合は「特になし」と文字列を記載する。

【レスポンス】

レスポンスとして返す内容を表現する文字列を記載する。

【使用例】

API の使用例を記載する。

11. 処理シーケンス

本章においては、「8. シナリオ」を基に、システム処理に関するシーケンスについて記載する。

11-1. シーケンス一覧

処理シーケンスについて、一覧を記す。

1. 契約を交わさずにデータ交換を行う

表 9:「契約を交わさずにデータ交換を行う」シナリオのシーケンス一覧

1-1. 利用準備	1-1-1. 利用申請
	1-1-2. コネクタ構築
1-2. 利用	1-2-1. カタログ用意
	1-2-2. データセット発見
	1-2-3. DDP 作成
	1-2-4. データ交換
	1-2-5. DDP 削除
	1-2-6. 来歴確認
	1-2-7. カタログ削除
1-3. 利用停止	1-3-1. コネクタ撤廃
	1-3-2. 退会

2. 相対取引によって契約を交わし、データ交換を行う

表 10:「相対取引によって契約を交わし、データ交換を行う」シナリオのシーケンス一覧

2-1. 利用準備	2-1-1. 利用申請
	2-1-2. コネクタ構築
2-2. 利用	2-2-1. カタログ用意
	2-2-2. データセット発見
	2-2-3. 契約
	2-2-4. DDP 作成
	2-2-5. データ交換
	2-2-6. DDP 削除
	2-2-7. 来歴確認
	2-2-8. カタログ削除
2-3. 利用停止	2-3-1. コネクタ撤廃
	2-3-2. 退会

3. データ取引市場などを介して契約を交わし、データ交換を行う

表 11:「データ取引市場などを介して契約を交わし、データ交換を行う」シナリオのシーケンス一覧

3-1. 利用準備	3-1-1. 利用申請
-----------	-------------

	3-1-2. コネクタ構築
3-2. 利用	3-2-1. カタログ用意
	3-2-2. データセット発見
	3-2-3. 契約
	3-2-4. DDP 作成
	3-2-5. データ交換
	3-2-6. DDP 削除
	3-2-7. 来歴確認
	3-2-8. カタログ削除
3-3. 利用停止	3-3-1. コネクタ撤廃
	3-3-2. 退会

11-2. 処理シーケンス図

11-2-1. 「契約を交わさずにデータ交換を行う」シナリオのシーケンス

11-2-1-1. 利用準備

11-2-1-1-1. 利用申請

「データ取引市場などを介して契約を交わし、データ交換を行う」シナリオの「利用申請」シーケンスを参照

11-2-1-1-2. コネクタ構築

「データ取引市場などを介して契約を交わし、データ交換を行う」シナリオの「コネクタ構築」シーケンスを参照

11-2-1-2. 利用

11-2-1-2-1. カタログ用意

「相対取引によって契約を交わし、データ交換を行う」シナリオの「カタログ用意」シーケンスを参照

11-2-1-2-2. データセット発見

「データ取引市場などを介して契約を交わし、データ交換を行う」シナリオの「データセット発見」シーケンスを参照

11-2-1-2-3. DDP 作成

「データ取引市場などを介して契約を交わし、データ交換を行う」シナリオの「DDP 作成」シーケンスを参照

11-2-1-2-4. データ交換

「相対取引によって契約を交わし、データ交換を行う」シナリオの「データ交換」シーケンスを参照

11-2-1-2-5. DDP 削除

「データ取引市場などを介して契約を交わし、データ交換を行う」シナリオの「DDP 削除」シーケンスを参照

11-2-1-2-6. 来歴確認

「データ取引市場などを介して契約を交わし、データ交換を行う」シナリオの「来歴確認」シーケンスを参照

11-2-1-2-7. カタログ削除

「相対取引によって契約を交わし、データ交換を行う」シナリオの「カタログ削除」シーケンスを参照

11-2-1-3. 利用停止

11-2-1-3-1. コネクタ撤廃

「データ取引市場などを介して契約を交わし、データ交換を行う」シナリオの「コネクタ撤廃」シーケンスを参照

11-2-1-3-2. 退会

「データ取引市場などを介して契約を交わし、データ交換を行う」シナリオの「退会」シーケンスを参照

11-2-2. 「相対取引によって契約を交わし、データ交換を行う」シナリオのシーケンス

11-2-2-1. 利用準備

11-2-2-1-1. 利用申請

「データ取引市場などを介して契約を交わし、データ交換を行う」シナリオの「利用申請」シーケンスを参照

11-2-2-1-2. コネクタ構築

「データ取引市場などを介して契約を交わし、データ交換を行う」シナリオの「コネクタ構築」シーケンスを参照

11-2-2-2. 利用

11-2-2-2-1. カタログ用意

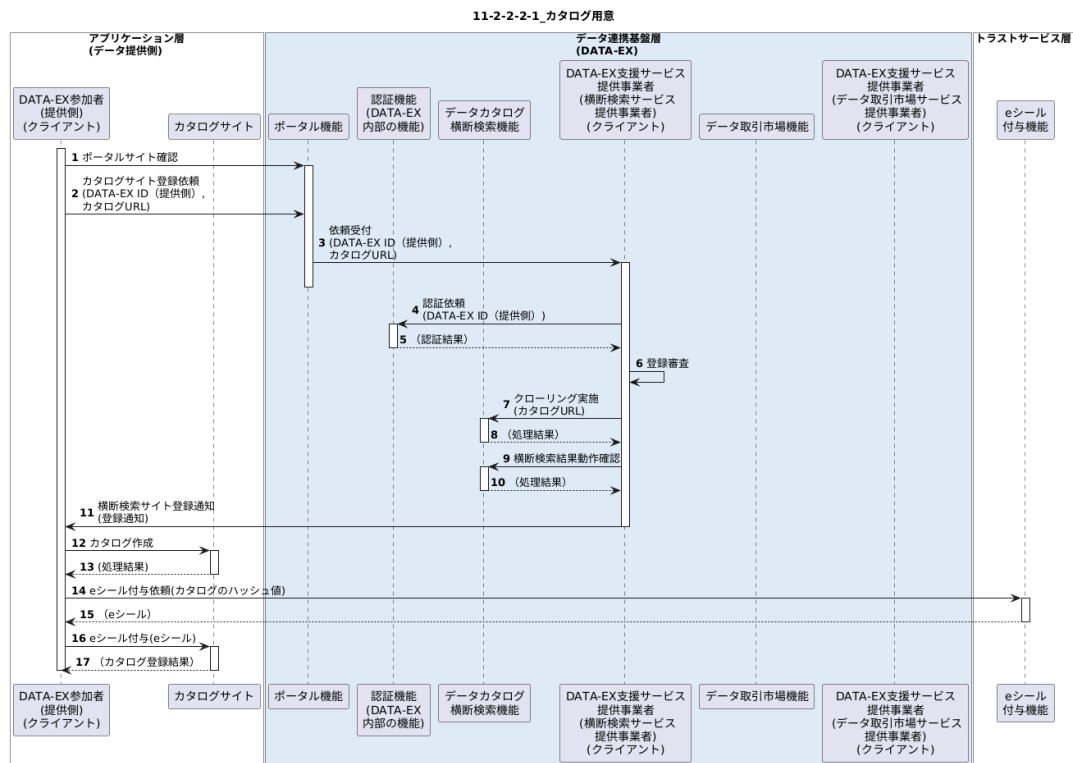


図 46:カタログ用意

1. DATA-EX 参加者(提供側)が、ポータルサイトを確認する。
2. DATA-EX 参加者(提供側)が、DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)に、カatalogサイトの登録を依頼する。
3. DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)が、DATA-EX 参加者(提供側)からの依頼を受け付ける。
4. DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)が、DATA-EX 参加者(提供側)の認証を認証機能(DATA-EX 内部の機能)に依頼する。
5. 認証機能(DATA-EX 内部の機能)が、DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)に、認証結果を送信する。
6. DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)が、依頼内容を審査する。

-
7. DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)が、データカタログ横断検索機能にて、クローリングを実施する。
 8. データカタログ横断検索機能が、処理結果を DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)に送信する。
 9. DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)が、データカタログ横断検索機能にて、DATA-EX 参加者(提供側)のカタログサイトが表示されることを確認する。
 10. データカタログ横断検索機能が、DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)に処理結果を送信する。
 11. DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)が、DATA-EX 参加者(提供側)にカタログサイトの登録が完了したことを通知する。
 12. DATA-EX 参加者(提供側)が、カタログサイトにカタログを登録する。
 13. カタログサイトが、DATA-EX 参加者(提供側)に処理結果を通知する。
 14. DATA-EX 参加者(提供側)が、e シール付与機能に、登録したカタログの e シールの付与を依頼する。
 15. e シール付与機能が、e シールを生成し、DATA-EX 参加者(提供側)に送付する。
 16. DATA-EX 参加者(提供側)が、カタログに e シールを付与する。
 17. カタログサイトが、DATA-EX 参加者(提供側)に処理結果を通知する。

11-2-2-2. データセット発見

「データ取引市場などを介して契約を交わし、データ交換を行う」シナリオの「データセット発見」シーケンスを参照

11-2-2-2-3. 契約

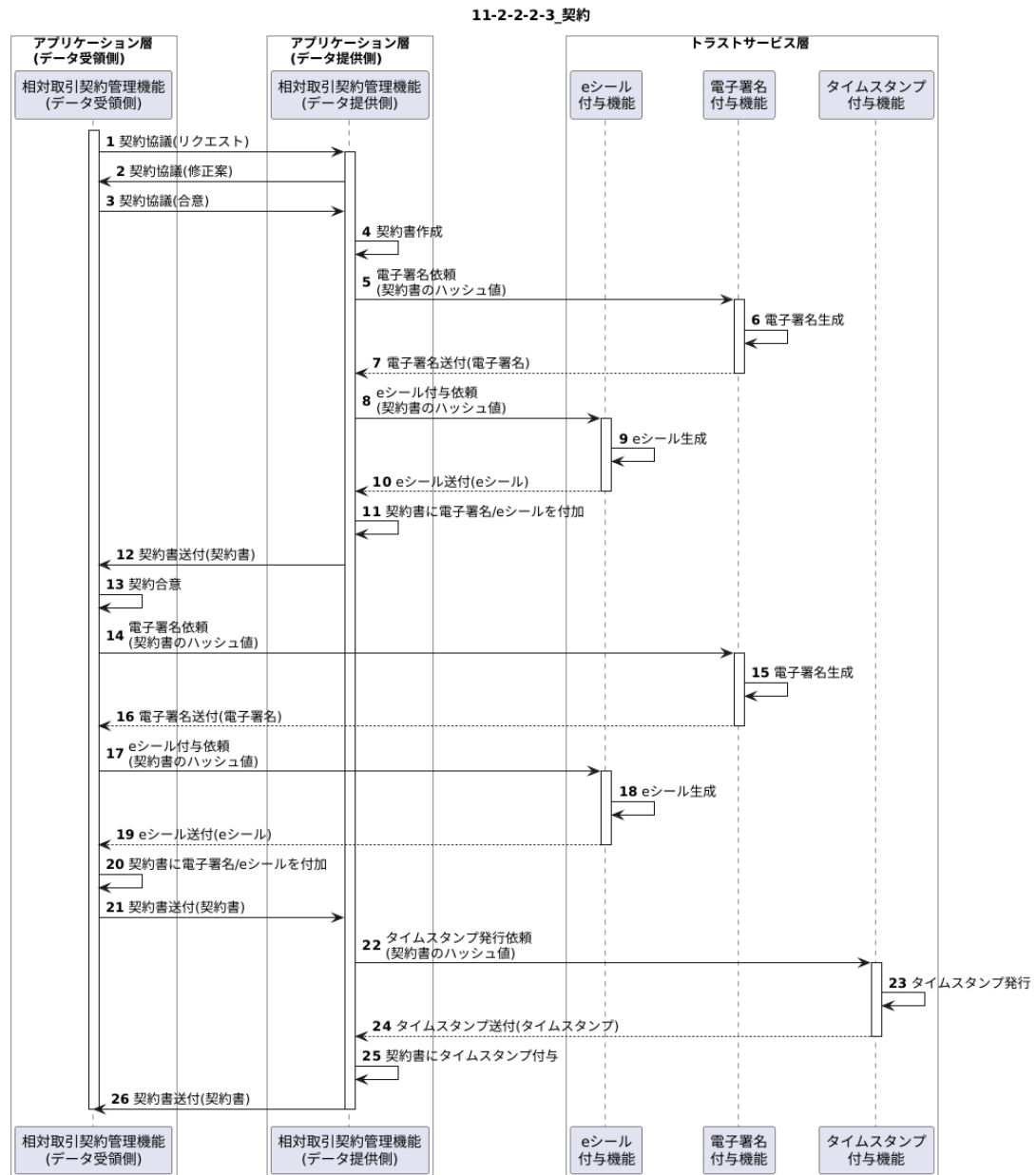


図 47: 契約

1. 相対取引契約管理機能(データ受領側)は、契約協議(リクエスト)を相対取引契約管理機能(データ提供側)に送信する。

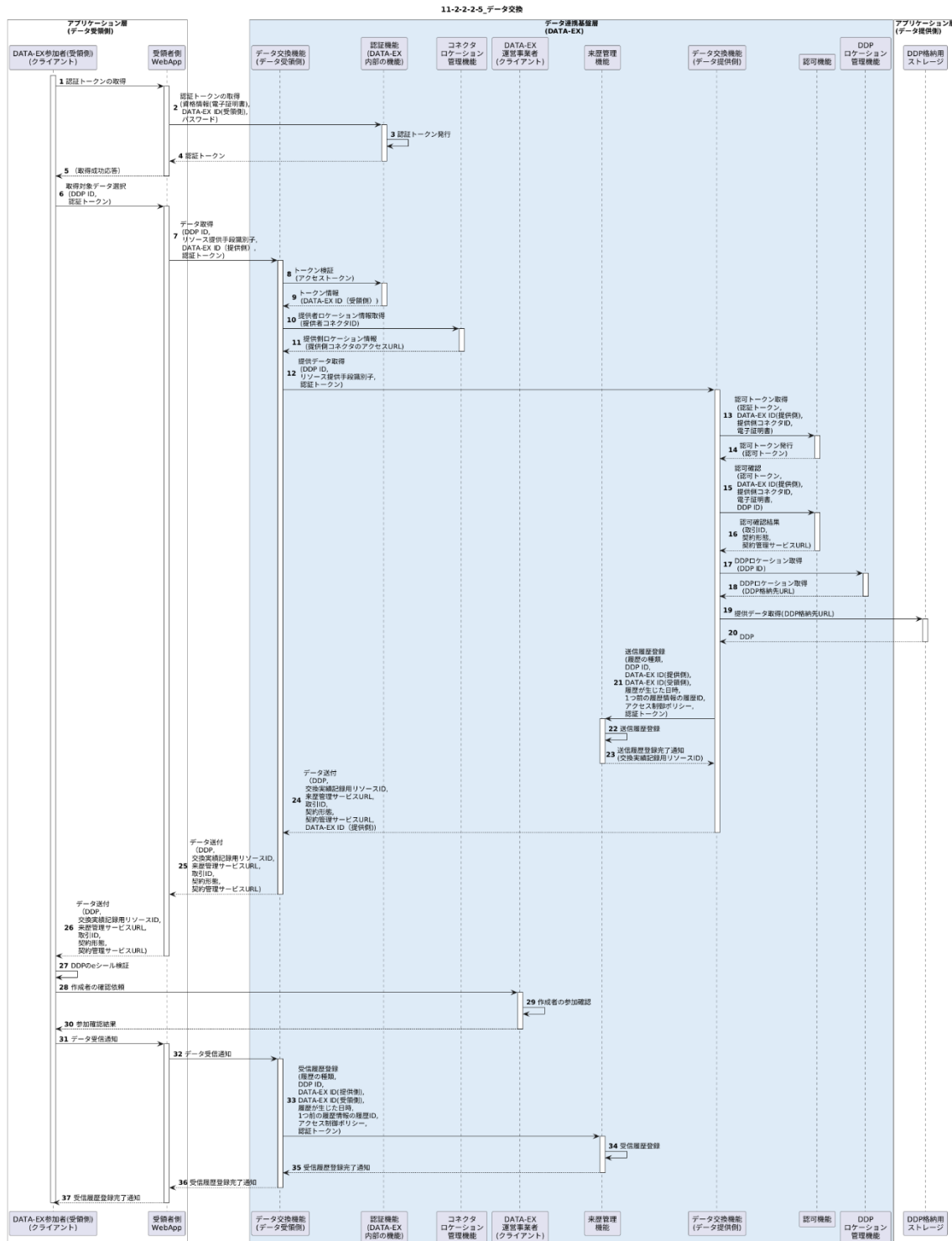
-
2. 相対取引契約管理機能(データ提供側)は、契約協議(修正案)を相対取引契約管理機能(データ受領側)に送信する。
 3. 相対取引契約管理機能(データ受領側)は、契約協議(合意)を相対取引契約管理機能(データ提供側)に送信する。
 4. 相対取引契約管理機能(データ提供側)は、契約書を作成する。
 5. 相対取引契約管理機能(データ提供側)は、電子署名付与機能に対して、契約書等への電子署名の作成を依頼する。
 6. 電子署名付与機能は、契約書等への電子署名を生成する。
 7. 電子署名付与機能は、相対取引契約管理機能(データ提供側)に対して電子署名を送付する。
 8. 相対取引契約管理機能(データ提供側)は、e シール付与機能に対して、契約書等の e シールの作成を依頼する。
 9. e シール付与機能は、契約書等の e シールを生成する。
 10. e シール付与機能は、相対取引契約管理機能(データ提供側)に対して e シールを送付する。
 11. 相対取引契約管理機能(データ提供側)は、契約書に電子署名/e シールを付加する。
 12. 相対取引契約管理機能(データ提供側)は、契約書を相対取引契約管理機能(データ受領側)に送信する。
 13. 相対取引契約管理機能(データ受領側)は契約合意処理を行う。
 14. 相対取引契約管理機能(データ受領側)は、電子署名付与機能に対して、契約書等への電子署名の作成を依頼する。
 15. 電子署名付与機能は、契約書等への電子署名を生成する。
 16. 電子署名付与機能は、相対取引契約管理機能(データ受領側)に対して電子署名を送付する。
 17. 相対取引契約管理機能(データ受領側)は、e シール付与機能に対して、契約書等の e シールの作成を依頼する。
 18. e シール付与機能は、契約書等の e シールを生成する。
 19. e シール付与機能は、相対取引契約管理機能(データ受領側)に対して e シールを返す。
 20. 相対取引契約管理機能(データ受領側)は、契約書に電子署名/e シールを付加する。
 21. 相対取引契約管理機能(データ受領側)は、契約書を相対取引契約管理機能(データ提供側)に送信する。
 22. 相対取引契約管理機能(データ提供側)は、タイムスタンプ付与機能に対して、タイムスタンプ発行を依頼する。
 23. タイムスタンプ付与機能は、タイムスタンプを発行する。
 24. タイムスタンプ付与機能は、相対取引契約管理機能(データ提供側)に対してタイムスタンプを送付する。
 25. 相対取引契約管理機能(データ提供側)は契約書にタイムスタンプを付与する。
-

26. 相対取引契約管理機能(データ提供側)は、契約書を相対取引契約管理機能(データ受領側)に送信する。

11-2-2-2-4. DDP 作成

「データ取引市場などを介して契約を交わし、データ交換を行う」シナリオの「DDP 作成」シーケンスを参照

11-2-2-2-5. データ交換



-
1. DATA-EX 参加者(受領側)は、アプリケーション(受領側 WebApp)に、認証トークンの取得を依頼する。
 2. アプリケーション(受領側 WebApp)は、認証機能(DATA-EX 内部の機能)に、資格情報(電子証明書)、DATA-EX ID(受領側)、パスワードを送信し、認証トークンの取得を依頼する。
 3. 認証機能(DATA-EX 内部の機能)は、認証トークンを発行する。
 4. 認証機能(DATA-EX 内部の機能)は、アプリケーション(受領側 WebApp)に、認証トークンを送信する。
 5. アプリケーション(受領側 WebApp)は、DATA-EX 参加者(受領側)に、認証トークン取得成功応答を通知する。
 6. DATA-EX 参加者(受領側)は、アプリケーション(受領側 WebApp)を介し、取得したいデータのデータ選択を行う。
 7. アプリケーション(受領側 WebApp)は、データ交換機能(データ受領側)に、DDP ID、リソース提供手段識別子、認証トークン、を送信し、データ取得を行う。
 8. データ交換機能(データ受領側)は、認証機能に、アクセストークンを送信し、トークン検証を行う。
 9. 認証機能は、トークンの有効性を確認できた場合、DATA-EX ID(受領側)を送信する。トークンの有効性を確認できない場合、エラーを返却する。
 10. データ交換機能(データ受領側)は、コネクタロケーション管理機能に提供側コネクタ ID を送信し、データ取得を依頼する提供側のロケーション情報を取得する。
 11. コネクタロケーション管理機能はデータ交換機能(データ受領側)に提供側のロケーション情報(提供側コネクタのアクセス URL)を返却する。
 12. データ交換機能(データ受領側)は、データ交換機能(データ提供側)に、DDP ID、リソース提供手段識別子、認証トークンを送信し、データ取得を行う。
 13. データ交換機能(データ提供側)は、認可機能に、DATA-EX ID(提供側)、認証トークン、提供者コネクタ ID、電子証明書を送信し、認可トークン取得を行う。
 14. 認可機能は、認証トークンが有効であった場合、認可トークンを送信する。トークンが無効であった場合、エラーを返却する。
 15. データ交換機能(データ提供側)は、認可機能に認可トークン、DATA-EX ID(提供側)、提供側コネクタ ID、電子証明書、DDP ID を送信し、認可確認を行う。
 16. 認可機能は、認可の有効性を確認できた場合、取引 ID、契約形態、契約管理サービス URL を送信する。認可の有効性を確認できない場合、エラーを返却する。
 17. データ交換機能(データ提供側)は、DDP ロケーション管理機能に、DDP ID を送信し、DDP ロケーションの取得を行う。
 18. DDP ロケーション管理機能は、データ交換機能(データ提供側)に、DDP 格納先 URL を返却する。
-

-
19. データ交換機能(データ提供側)は、DDP 格納 URL を元に、DDP 格納用ストレージから、データ取得を行う。
 20. DDP 格納用ストレージは、データ交換機能(データ提供側)に DDP を返信する。
 21. データ交換機能(データ提供側)は、来歴管理機能に、履歴の種類、DDP ID、DATA-EX ID(受領側)、DATA-EX ID(提供側)、履歴が生じた日時、1 つ前の履歴情報の履歴 ID、アクセス制御ポリシー、認証トークンを送信し、送信履歴登録を行う。
 22. 来歴管理機能は、送信履歴登録を行う。
 23. 来歴管理機能は、データ交換機能(データ提供側)に送信履歴登録完了を通知する。
 24. データ交換機能(データ提供側)は、データ交換機能(データ受領側)に DDP、交換実績記録用リソース ID、来歴管理サービス URL、取引 ID、契約形態、契約管理サービス URL、DATA-EX ID(提供側)を返信する。
 25. データ交換機能(データ受領側)は、アプリケーション(受領側 WebApp)に DDP を返信する。
 26. アプリケーション(受領側 WebApp)は、DATA-EX 参加者(受領側)に DDP を返信する。
DATA-EX 参加者(受領側)は、画面表示などで提供データを確認する。
 27. DATA-EX 参加者(受領側)は、受け取った DDP の e シールを検証する。
 28. DATA-EX 参加者(受領側)は、DATA-EX 運営事業者に、e シール作成者が DATA-EX に参加していることの確認を依頼する。
 29. DATA-EX 運営事業者が、e シール作成者が DATA-EX 参加者であることを確認する。
 30. DATA-EX 運営事業者が、e シール作成者が DATA-EX 参加者であることの確認結果を送付する。
 31. DATA-EX 参加者(受領側)は、アプリケーション(受領側 WebApp)に、データ受信通知を依頼する。
 32. アプリケーション(受領側 WebApp)は、データ交換機能(データ受領側)に、データ受信通知を依頼する。
 33. データ交換機能(データ受領側)は、来歴管理機能に、履歴の種類、DDP ID、DATA-EX ID(受領側)、DATA-EX ID(提供側)、履歴が生じた日時、1 つ前の履歴情報の履歴 ID、アクセス制御ポリシー、認証トークンを送信し、受信履歴登録を行う。
 34. 来歴管理機能は、受信履歴登録を行う。
 35. 来歴管理機能は、データ交換機能(データ受領側)に、受信履歴登録完了を通知する。
 36. データ交換機能(データ受領側)は、アプリケーション(受領側 WebApp)に、受信履歴登録完了を通知する。
 37. アプリケーション(受領側 WebApp)は、DATA-EX 参加者(受領側)に、受信履歴登録完了を通知する。
-

11-2-2-2-6. DDP 削除

「データ取引市場などを介して契約を交わし、データ交換を行う」シナリオの「DDP 削除」シーケンスを参照

11-2-2-2-7. 来歴確認

「データ取引市場などを介して契約を交わし、データ交換を行う」シナリオの「来歴確認」シーケンスを参照

11-2-2-2-8. カタログ削除

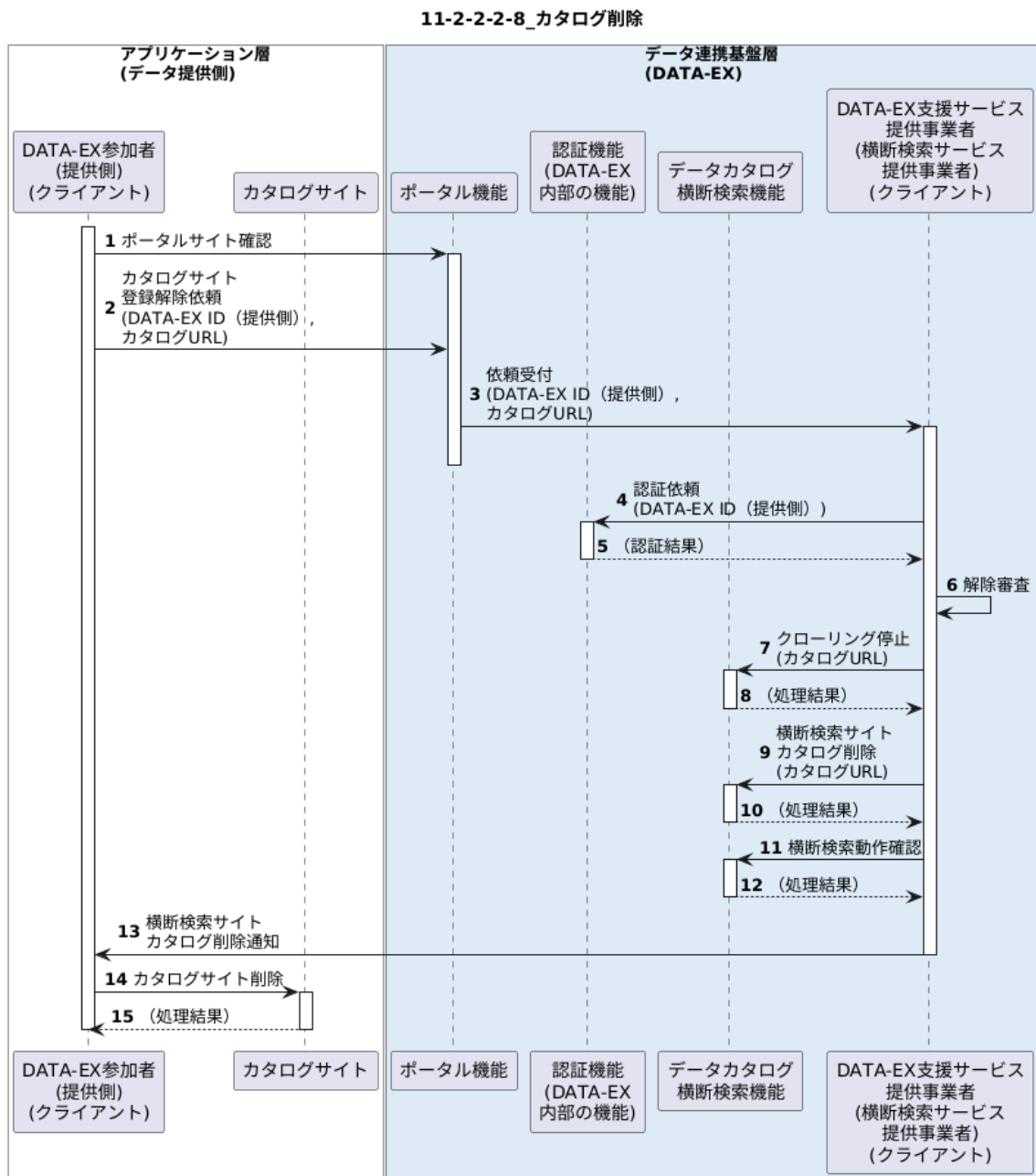


図 49:カタログ削除

1. DATA-EX 参加者(提供側)が、ポータルサイトを確認する。
2. DATA-EX 参加者(提供側)が、DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)に、カタログサイトの登録解除を依頼する。
3. DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)が、DATA-EX 参加者(提供側)からの依頼を受け付ける。

-
4. DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)が、申請者の認証を、認証機能(DATA-EX 内部の機能)に依頼する。
 5. 認証機能(DATA-EX 内部の機能)が、申請者の認証を行い、認証結果を、DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)に通知する。
 6. DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)が、解除依頼の内容を審査する。
 7. DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)が、データカタログ横断検索機能に対し、カタログサイトのクローリングを停止する。
 8. データカタログ横断検索機能が、DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)に、処理結果を通知する。
 9. DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)が、データカタログ横断検索機能に対し、横断検索サイトのカタログを削除する。
 10. データカタログ横断検索機能が、DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)に、処理結果を通知する。
 11. DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)が、データカタログ横断検索機能にカタログが表示されないことを確認する。
 12. データカタログ横断検索機能が、DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)に、処理結果を通知する。
 13. DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)が、DATA-EX 参加者(提供側)に、カタログサイトの登録解除を通知する。
 14. DATA-EX 参加者(提供側)が、カタログサイトを削除する。
 15. カatalogサイトが、DATA-EX 参加者(提供側)に、処理結果を通知する。

11-2-2-3. 利用停止

11-2-2-3-1. コネクタ撤廃

「データ取引市場などを介して契約を交わし、データ交換を行う」シナリオの「コネクタ撤廃」シーケンスを参照

11-2-2-3-2. 退会

「データ取引市場などを介して契約を交わし、データ交換を行う」シナリオの「退会」シーケンスを参照

11-2-3. 「データ取引市場などを介して契約を交わし、データ交換を行う」シナリオのシーケンス

11-2-3-1. 利用準備

11-2-3-1-1. 利用申請

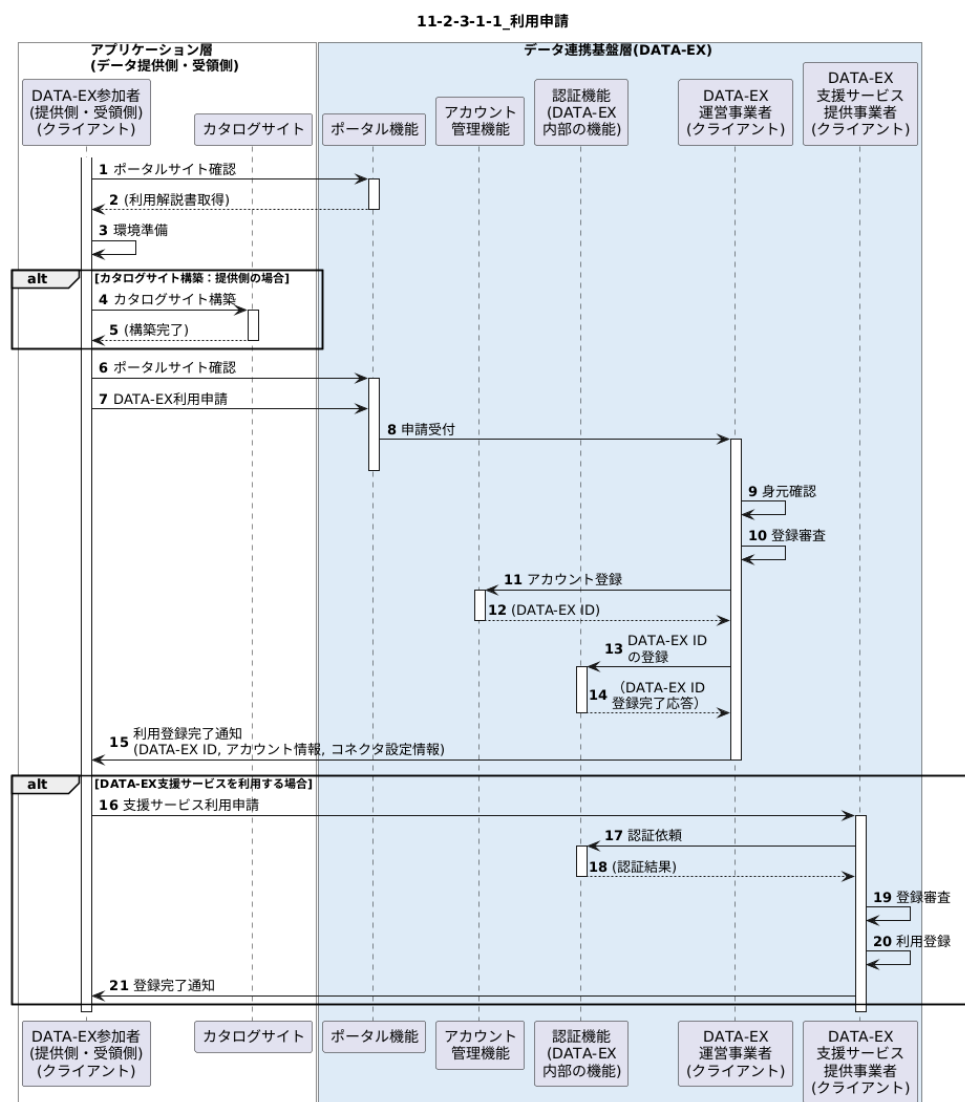


図 50: 利用申請

1. DATA-EX 参加者がポータルサイトを確認する。

-
2. DATA-EX 参加者が、ポータルサイトより DATA-EX 利用解説書を取得する。
 3. DATA-EX 参加者が、コネクタ構築に必要な環境(デバイス、ストレージ、など)を準備する。
 4. DATA-EX 参加者(データ提供側)の場合、必要に応じて以下の 4 および 5 の作業を実施する。
 5. DATA-EX 参加者(データ提供側)が、カタログサイトを構築する。
 6. DATA-EX 参加者(データ提供側)が、カタログサイトの構築を完了する。
 7. DATA-EX 参加者がポータルサイトを確認する。
 8. DATA-EX 参加者が、ポータルサイトにて DATA-EX の利用申請を行う。
 9. DATA-EX 運営事業者が、DATA-EX 利用申請を受け付ける。
 10. DATA-EX 運営事業者が、申請者が本人であることの身元確認を行う。
 11. DATA-EX 運営事業者が、申請内容を審査する。
 12. DATA-EX 運営事業者が、アカウント管理機能に、申請者のアカウント情報を登録する。
 13. アカウント管理機能が DATA-EX ID を発行する。
 14. DATA-EX 運営事業者が、認証機能(DATA-EX 内部の機能)に、申請者の DATA-EX ID を登録する。
 15. 認証機能(DATA-EX 内部の機能)は、登録完了応答を送信する。
 16. DATA-EX 運営事業者が、申請者に、DATA-EX ID、アカウント情報およびコネクタの設定情報を送信する。
 17. DATA-EX 支援サービスを利用する場合、以下の作業を実施する。
 18. DATA-EX 参加者が、DATA-EX 支援サービス提供事業者に支援サービスの利用申請を行う。
 19. DATA-EX 支援サービス提供事業者が、申請者の認証を認証機能(DATA-EX 内部の機能)に依頼する。
 20. 認証機能(DATA-EX 内部の機能)が、DATA-EX 支援サービス提供事業者に、申請者の認証結果を送信する。
 21. DATA-EX 支援サービス提供事業者が、申請者の申請内容を審査する。
 22. DATA-EX 支援サービス提供事業者が、申請者の利用登録を行う。
 23. DATA-EX 支援サービス提供事業者が、申請者に、登録完了通知を送信する。

11-2-3-1-2. コネクタ構築

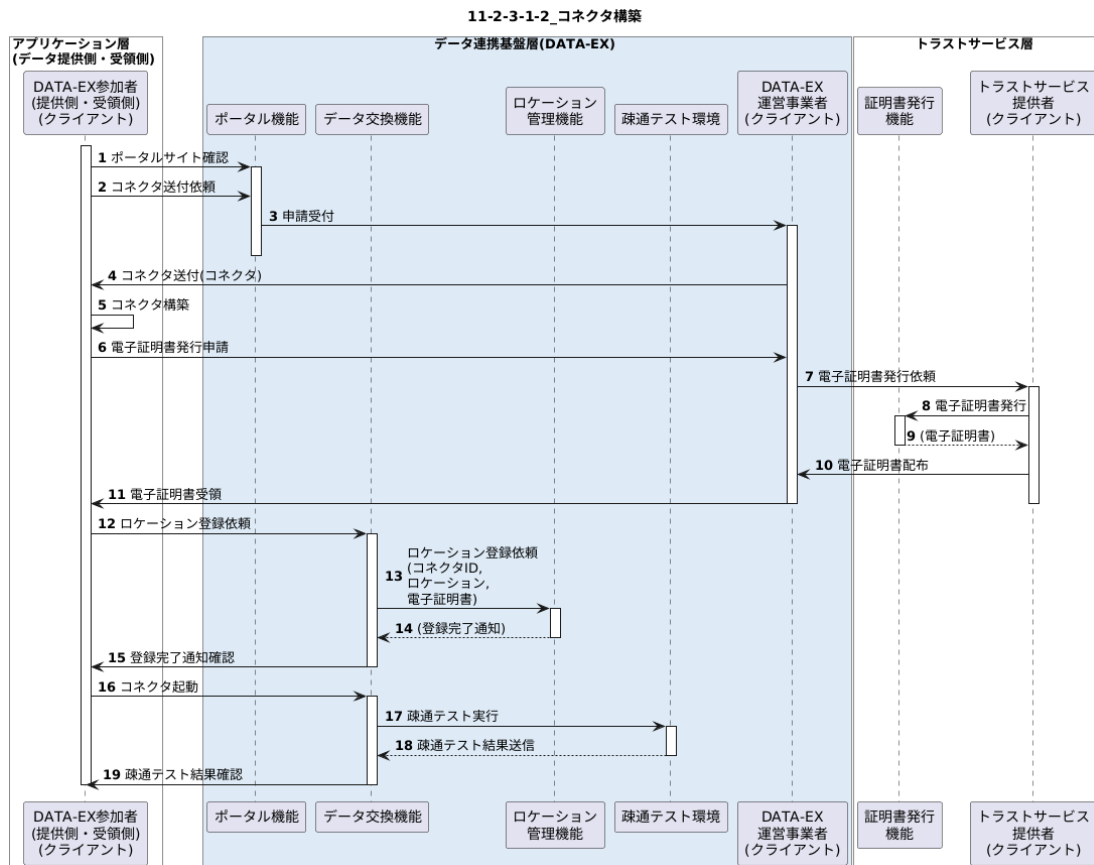


図 51:コネクタ構築

1. DATA-EX 参加者が、ポータルサイトを閲覧し、コネクタ送付依頼先を確認する。
2. DATA-EX 参加者が、ポータルサイトより、コネクタの送付を依頼する。
3. DATA-EX 運営事業者が、DATA-EX 参加者からのコネクタ送付依頼を受け付ける。
4. DATA-EX 運営事業者が、DATA-EX 参加者にコネクタを送付する。
5. DATA-EX 参加者が、コネクタを構築する。
6. DATA-EX 参加者が、DATA-EX 運営事業者にコネクタの電子証明書発行を申請する。
7. DATA-EX 運営事業者が、トラストサービス提供者に、コネクタの電子証明書の発行を依頼する。
8. トラストサービス提供者が、証明書発行機能に、電子証明書の発行を依頼する。
9. 証明書発行機能が、トラストサービス提供者に、電子証明書を発行する。
10. トラストサービス提供者が、DATA-EX 運営事業者に、電子証明書を配布する。
11. DATA-EX 運営事業者が、DATA-EX 参加者に、電子証明書を配布する。

-
12. DATA-EX 参加者がコネクタ(データ交換機能)を起動し、ロケーションの登録を依頼する。
 13. コネクタ(データ交換機能)が、ロケーション管理機能にロケーションの登録を依頼する。
 14. ロケーション管理機能が、コネクタ(データ交換機能)にロケーションの登録完了を通知する。
 15. DATA-EX 参加者が、ロケーションの登録完了通知を確認する。
 16. DATA-EX 参加者がコネクタを起動し、疎通テストを実行する。
 17. コネクタ(データ交換機能)が、疎通テスト環境へアクセスし、疎通テストを実行する。
 18. 疎通テスト環境が、コネクタ(データ交換機能)に、疎通テスト結果を送信する。
 19. DATA-EX 参加者が、疎通テスト結果を確認する。

11-2-3-2. 利用

11-2-3-2-1. カタログ用意

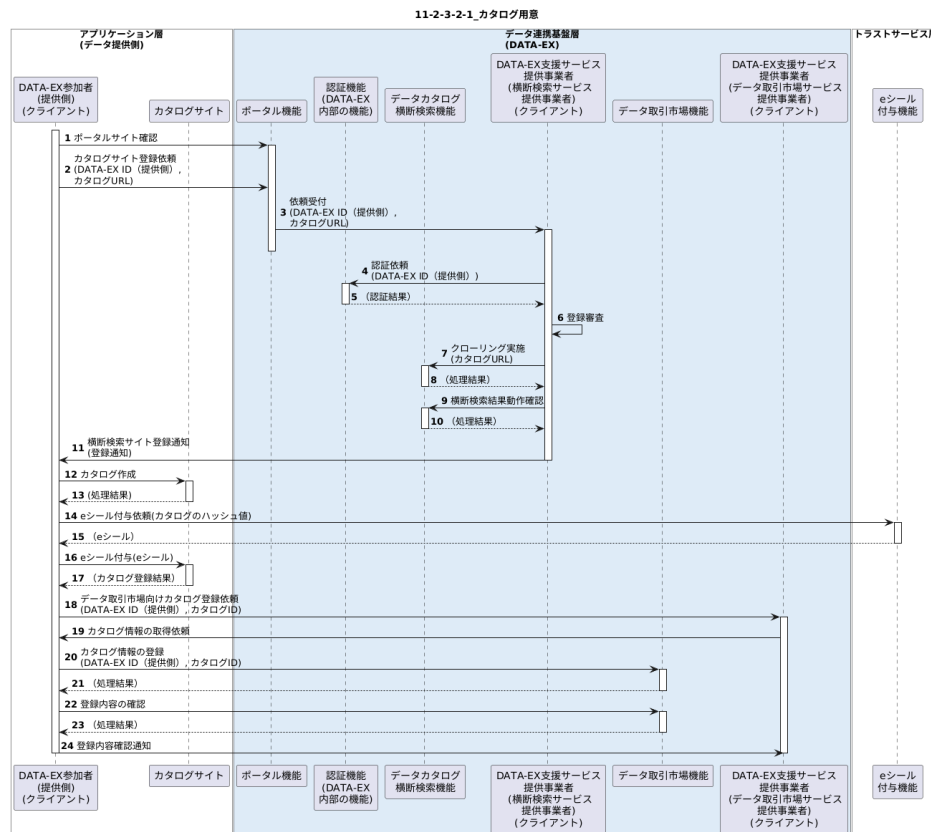


図 52: カタログ用意

1. DATA-EX 参加者(提供側)が、ポータルサイトを確認する。
2. DATA-EX 参加者(提供側)が、DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)に、カタログサイトの登録を依頼する。
3. DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)が、DATA-EX 参加者(提供側)からの依頼を受け付ける。
4. DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)が、DATA-EX 参加者(提供側)の認証を認証機能(DATA-EX 内部の機能)に依頼する。
5. 認証機能(DATA-EX 内部の機能)が、DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)に、認証結果を送信する。
6. DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)が、依頼内容を審査する。

-
7. DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)が、データカタログ横断検索機能にて、クローリングを実施する。
 8. データカタログ横断検索機能が、処理結果を DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)に送信する。
 9. DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)が、データカタログ横断検索機能にて、DATA-EX 参加者(提供側)のカタログサイトが表示されることを確認する。
 10. データカタログ横断検索機能が、DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)に処理結果を送信する。
 11. DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)が、DATA-EX 参加者(提供側)にカタログサイトの登録が完了したことを通知する。
 12. DATA-EX 参加者(提供側)が、カタログサイトにカタログを登録する。
 13. カatalogサイトが、DATA-EX 参加者(提供側)に処理結果を通知する。
 14. DATA-EX 参加者(提供側)が、e シール付与機能に、登録したカタログの e シールの付与を依頼する。
 15. e シール付与機能が、e シールを生成し、DATA-EX 参加者(提供側)に送付する。
 16. DATA-EX 参加者(提供側)が、カタログに e シールを付与する。
 17. カatalogサイトが、DATA-EX 参加者(提供側)に処理結果を通知する。
 18. DATA-EX 参加者(提供側)が、DATA-EX 支援サービス提供事業者(データ取引市場サービス提供事業者)に、データ取引市場向けカタログの登録を依頼する。
 19. DATA-EX 支援サービス提供事業者(データ取引市場サービス提供事業者)が、DATA-EX 参加者(提供側)に、カタログ情報の取得を依頼する。
 20. DATA-EX 参加者(提供側)が、データ取引市場機能にカタログ情報を登録する。
 21. データ取引市場機能が、DATA-EX 参加者(提供側)に処理結果を通知する。
 22. DATA-EX 参加者(提供側)が、データ取引市場機能にて、登録内容を確認する。
 23. データ取引市場機能が、DATA-EX 参加者(提供側)に処理結果を通知する。
 24. DATA-EX 参加者(提供側)が、DATA-EX 支援サービス提供事業者(データ取引市場サービス提供事業者)に、データ取引市場向けカタログ情報の確認が完了したことを通知する。

11-2-3-2-2. データセット発見

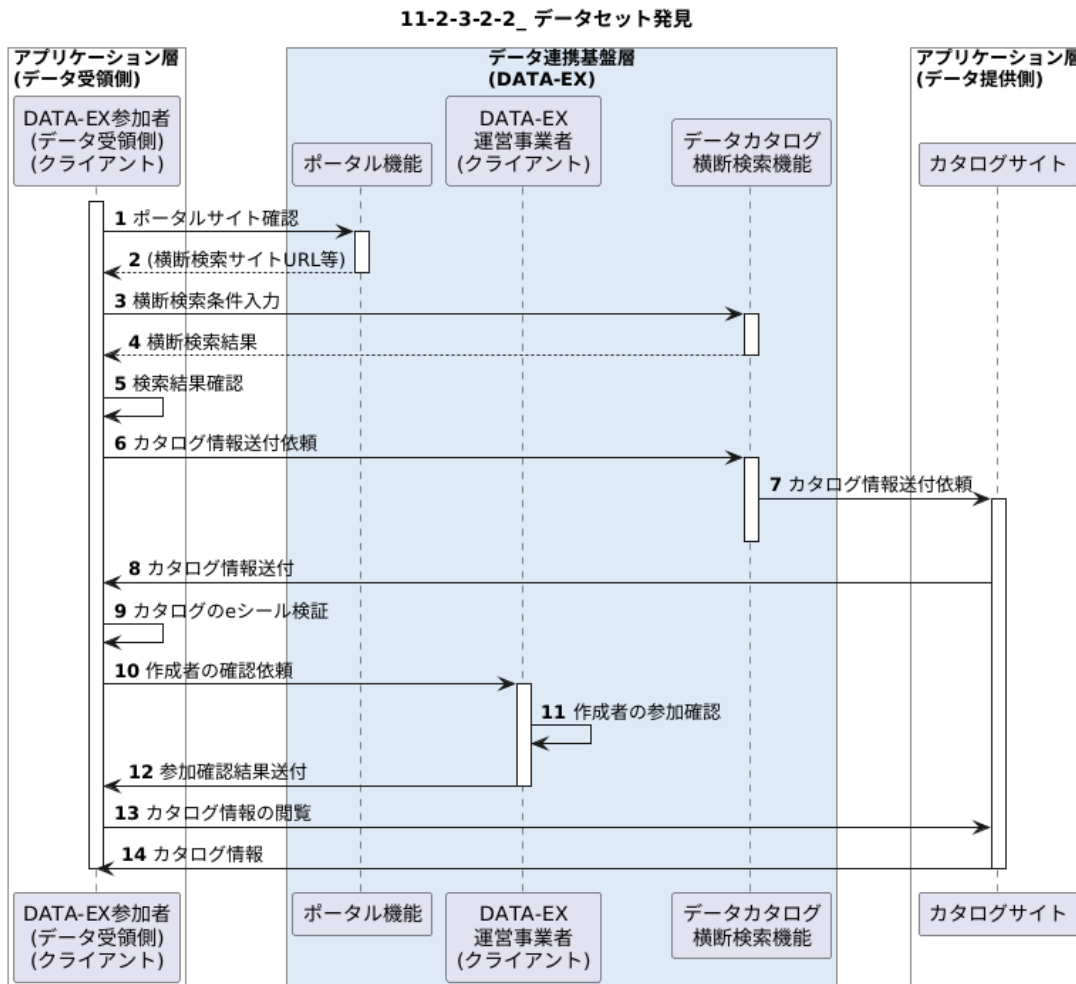


図 53: データセット発見

1. DATA-EX 参加者(データ受領側)がポータルサイトを閲覧する。
2. DATA-EX 参加者(データ受領側)が、ポータルサイトにて、横断検索サイトの URL 等の横断検索に必要となる情報を確認する。
3. DATA-EX 参加者(データ受領側)が、データカタログ横断検索機能にアクセスし、検索条件を指定し、横断検索を行う。
4. データカタログ横断検索機能が、DATA-EX 参加者(データ受領側)に、横断検索の結果を提示する。
5. DATA-EX 参加者(データ受領側)が、横断検索結果を確認する。
6. DATA-EX 参加者(データ受領側)が、データカタログ横断検索機能に対して、参照したいカタログを指定する。

-
7. データカタログ横断検索機能が、カタログサイトに、DATA-EX 参加者(データ受領側)が指定したカタログ情報の参照を依頼する。
 8. カタログサイトが、DATA-EX 参加者(データ受領側)に、指定されたカタログ情報を送付する。
 9. DATA-EX 参加者(データ受領側)が、カタログの e シールを検証する。
 10. DATA-EX 参加者(データ受領側)が、DATA-EX 運営事業者に e シール作成者が DATA-EX に参加していることの確認を依頼する。
 11. DATA-EX 運営事業者が、e シール作成者が DATA-EX 参加者であることを確認する。
 12. DATA-EX 運営事業者が、e シール作成者が DATA-EX 参加者であることの確認結果を送付する。
 13. DATA-EX 参加者(データ受領側)が、カタログサイト上のカタログを閲覧する。
 14. カタログサイトが、DATA-EX 参加者(データ受領側)に、カタログ情報を表示する。

11-2-3-2-3. 契約

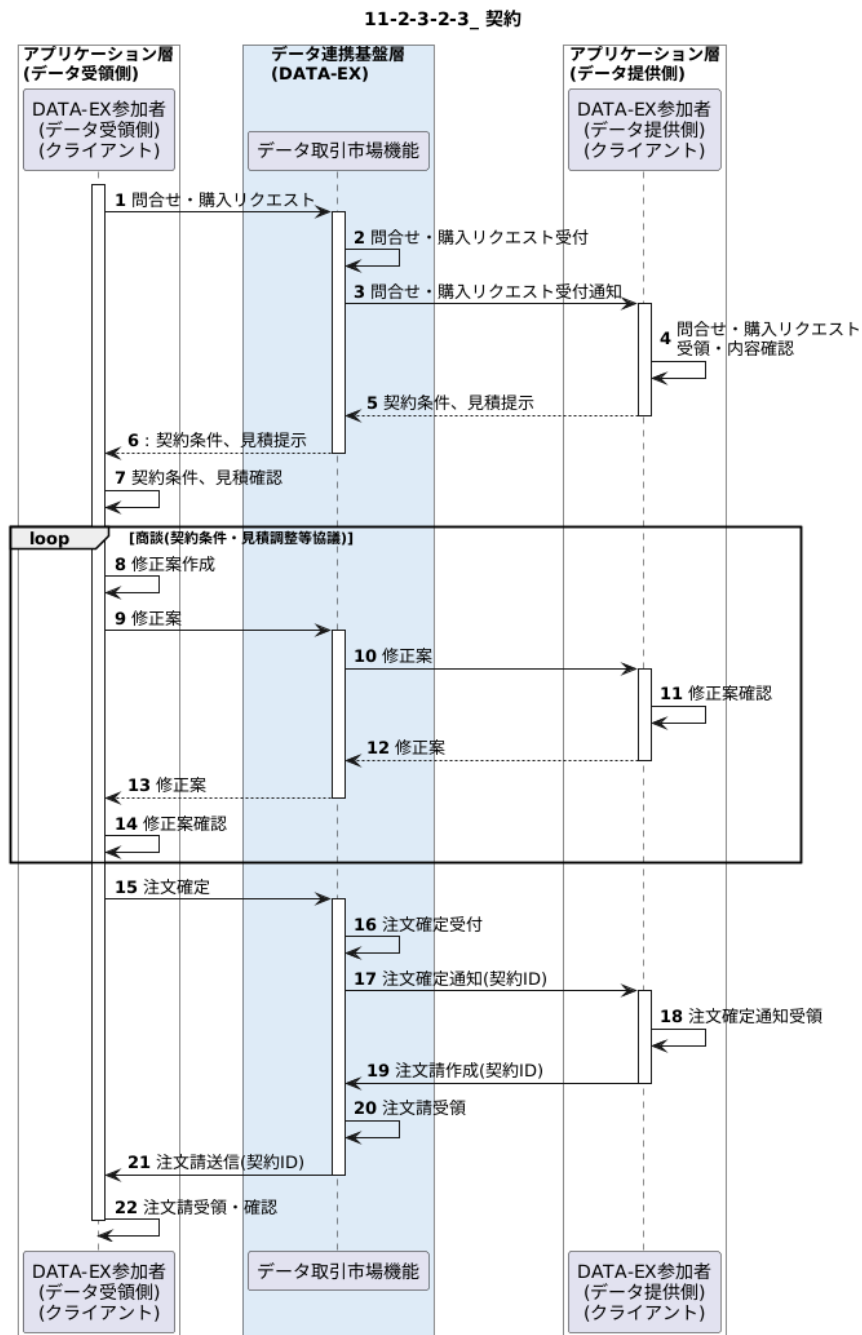


図 54: 契約

-
1. DATA-EX 参加者(データ受領側)が、データ取引市場機能に問合せ・購入リクエストを発行する。
 2. データ取引市場機能が、DATA-EX 参加者(データ受領側)からの問合せ・購入リクエストを受け付ける。
 3. データ取引市場機能が、対象データを管理する DATA-EX 参加者(データ提供側)に、問合せ・購入リクエストが発生したことを通知する。
 4. DATA-EX 参加者(データ提供側)が、データ取引市場機能からの問合せ・購入リクエストを受領し、内容を確認する。
 5. DATA-EX 参加者(データ提供側)が、データ取引市場機能に、契約条件・見積を入力する。
 6. データ取引市場機能が、DATA-EX 参加者(データ提供側)による契約条件・見積を、DATA-EX 参加者(データ受領側)に通知する。
 7. DATA-EX 参加者(データ受領側)が、DATA-EX 参加者(データ提供側)による契約条件・見積を確認する。

DATA-EX 参加者(データ提供側)と DATA-EX 参加者(データ受領側)の間で契約交渉が発生する場合、8.から 14.を繰り返す。(特に交渉が発生しない場合は 15.に進む)

8. DATA-EX 参加者(データ受領側)が、修正案を作成する。
9. DATA-EX 参加者(データ受領側)が、データ取引市場機能に、修正案を入力する。
10. データ取引市場機能が、DATA-EX 参加者(データ受領側)による修正案を、DATA-EX 参加者(データ提供側)に通知する。
11. DATA-EX 参加者(データ提供側)が、修正案を確認する。
12. DATA-EX 参加者(データ提供側)が、データ取引市場機能に修正案を入力する。
13. データ取引市場機能が、修正案を、DATA-EX 参加者(データ受領側)に通知する。
14. DATA-EX 参加者(データ受領側)が、修正案を確認する。
15. 契約交渉がまとまった場合、DATA-EX 参加者(データ提供側)が、データ取引市場機能にて、注文を確定する。
16. データ取引市場機能が、注文確定を受け付ける。
17. データ取引市場機能が、注文確定を DATA-EX 参加者(データ提供側)に通知する。
18. DATA-EX 参加者(データ受領側)が、データ取引市場機能からの注文確定通知を受領する。
19. DATA-EX 参加者(データ受領側)が、データ取引市場機能に、注文請を作成する。
20. データ取引市場機能が、DATA-EX 参加者(データ受領側)からの注文請を受領する。
21. データ取引市場機能が、DATA-EX 参加者(データ受領側)からの注文請を DATA-EX 参加者(データ提供側)に送信する。
22. DATA-EX 参加者(データ提供側)が、DATA-EX 参加者(データ受領側)からの注文請を受領し、確認する。

11-2-3-2-4. DDP 作成

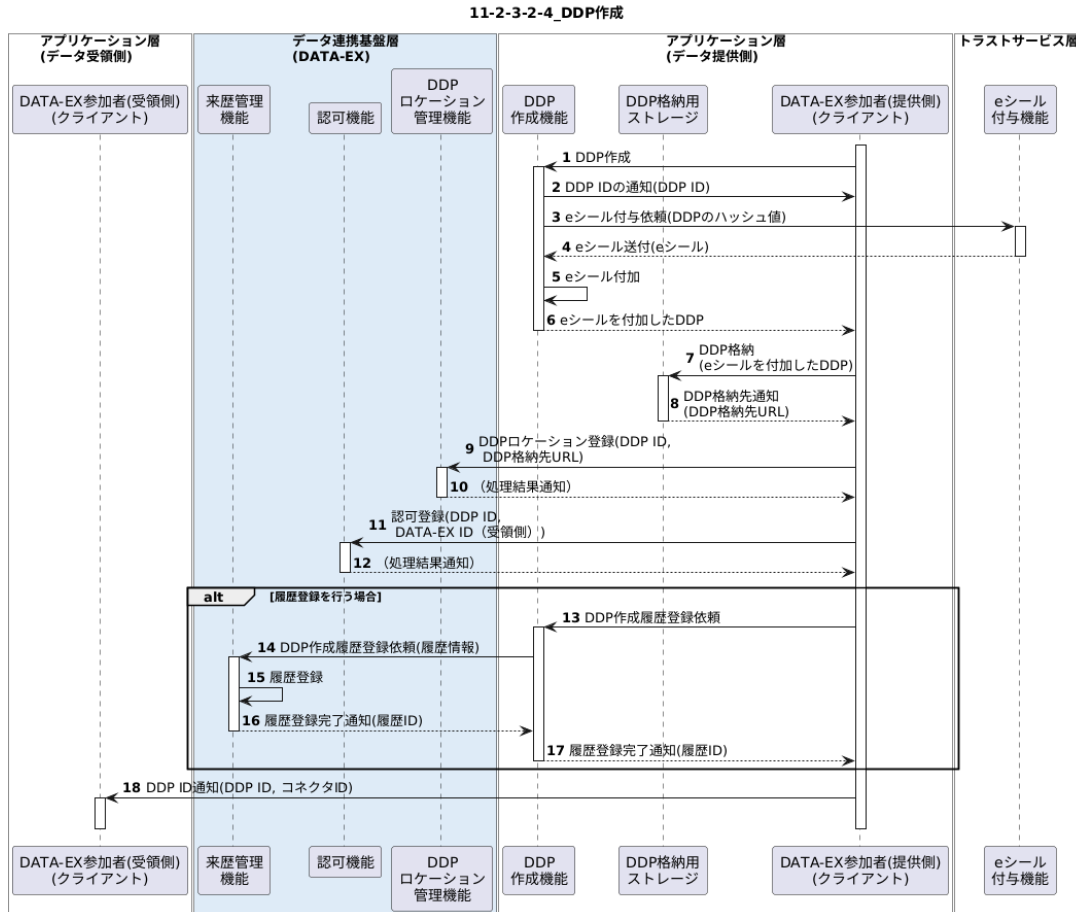
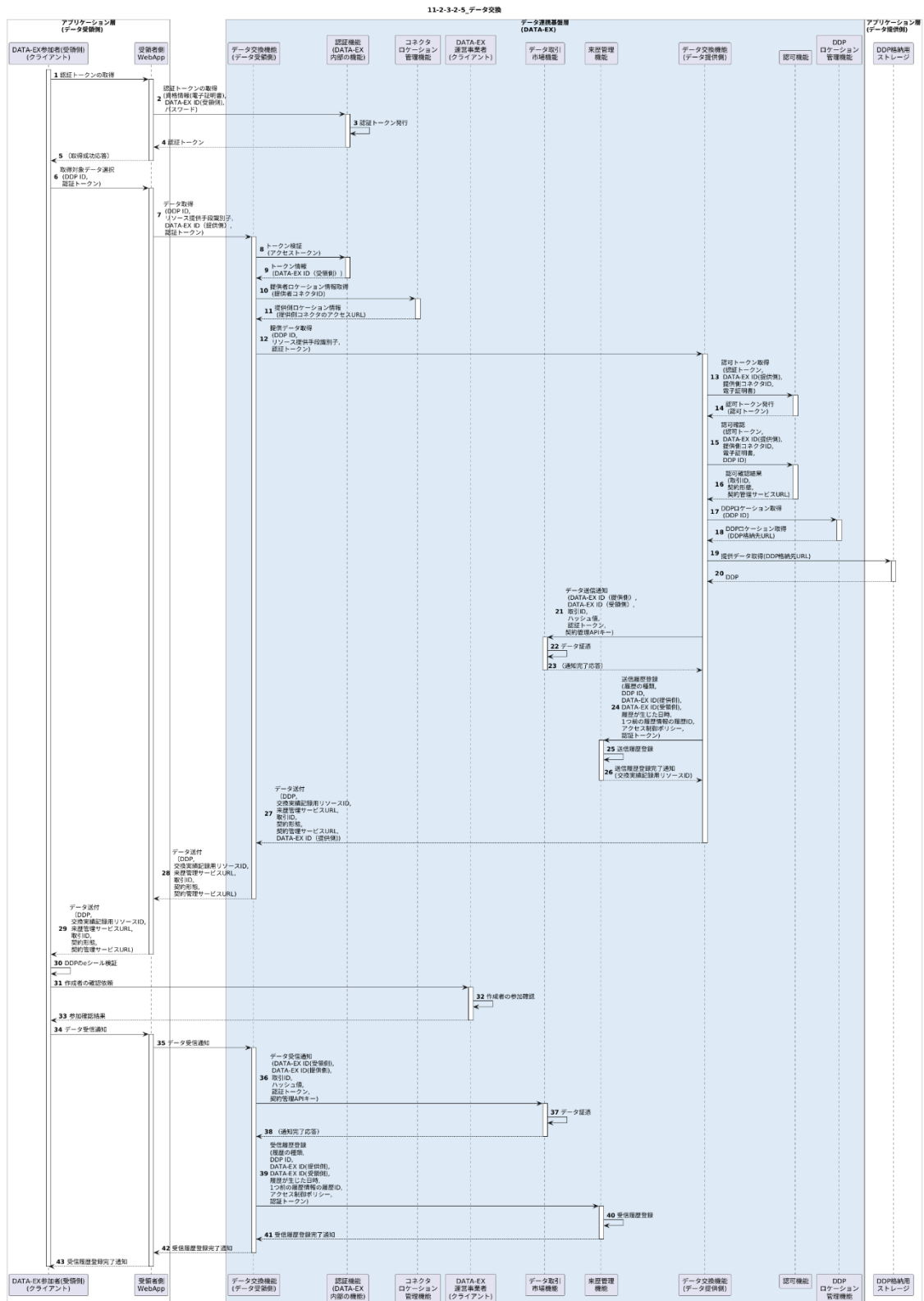


図 55: DDP 作成

1. DATA-EX 参加者(提供側)が、DDP 作成機能を用いて、DDP を作成する。
2. DDP 作成機能が、DATA-EX 参加者(提供側)に、作成した DDP の DDP ID を通知する。
3. DDP 作成機能が、e シール付与機能に、e シール付与の依頼を行う。
4. e シール付与機能が、DDP 作成機能に、e シールを送付する。
5. DDP 作成機能が、DDP に e シールを付加する。
6. DDP 作成機能が、DATA-EX 参加者(提供側)に、e シールを付加した DDP を提供する。
7. DATA-EX 参加者(提供側)が、DDP 格納用ストレージに、e シールを付加した DDP を格納する。
8. DDP 格納用ストレージが、DATA-EX 参加者(提供側)に、DDP の格納先を通知する。
9. DATA-EX 参加者(提供側)が、DDP ロケーション管理機能に、DDP ID と DDP の格納先 URL を登録する。
10. DDP ロケーション管理機能が、DATA-EX 参加者(提供側)に、処理結果を通知する。

-
11. DATA-EX 参加者(提供側)が、認可機能に、作成した DDP の認可情報を登録する。
 12. 認可機能が、DATA-EX 参加者(提供側)に、処理結果を通知する。
- 履歴登録を行う場合は、以下の 13.から 17.を行う。
13. DATA-EX 参加者(提供側)が、DDP 作成機能に、DDP 作成履歴登録依頼を行う。
 14. DDP 作成機能が、来歴管理機能に、DDP 作成履歴登録依頼を行う。
 15. 来歴管理機能が、履歴登録を行う
 16. 来歴管理機能が、DDP 作成機能に、履歴 ID を通知する。
 17. DDP 作成機能が、DATA-EX 参加者(提供側)に、履歴 ID を通知する。
 18. DATA-EX 参加者(提供側)が、DATA-EX 参加者(受領側)に、DDP ID とコネクタ ID を通知する。

11-2-3-2-5. データ交換



-
1. DATA-EX 参加者(受領側)は、アプリケーション(受領側 WebApp)に、認証トークンの取得を依頼する。
 2. アプリケーション(受領側 WebApp)は、認証機能(DATA-EX 内部の機能)に、資格情報(電子証明書)、DATA-EX ID(受領側)、パスワードを送信し、認証トークンの取得を依頼する。
 3. 認証機能(DATA-EX 内部の機能)は、認証トークンを発行する。
 4. 認証機能(DATA-EX 内部の機能)は、アプリケーション(受領側 WebApp)に、認証トークンを送信する。
 5. アプリケーション(受領側 WebApp)は、DATA-EX 参加者(受領側)に、認証トークン取得成功応答を通知する。
 6. DATA-EX 参加者(受領側)は、アプリケーション(受領側 WebApp)を介し、取得したいデータのデータ選択を行う。
 7. アプリケーション(受領側 WebApp)は、データ交換機能(データ受領側)に、DDP ID、リソース提供手段識別子、認証トークン、を送信し、データ取得を行う。
 8. データ交換機能(データ受領側)は、認証機能に、アクセストークンを送信し、トークン検証を行う。
 9. 認証機能は、トークンの有効性を確認できた場合、DATA-EX ID(受領側)を送信する。トークンの有効性を確認できない場合、エラーを返却する。
 10. データ交換機能(データ受領側)は、コネクタロケーション管理機能に提供側コネクタ ID を送信し、データ取得を依頼する提供側のロケーション情報を取得する。
 11. コネクタロケーション管理機能はデータ交換機能(データ受領側)に提供側のロケーション情報(提供側コネクタのアクセス URL)を返却する。
 12. データ交換機能(データ受領側)は、データ交換機能(データ提供側)に、DDP ID、リソース提供手段識別子、認証トークンを送信し、データ取得を行う。
 13. データ交換機能(データ提供側)は、認可機能に、DATA-EX ID(提供側)、認証トークン、提供者コネクタ ID、電子証明書を送信し、認可トークン取得を行う。
 14. 認可機能は、認証トークンが有効であった場合、認可トークンを送信する。トークンが無効であった場合、エラーを返却する。
 15. データ交換機能(データ提供側)は、認可機能に認可トークン、DATA-EX ID(提供側)、提供側コネクタ ID、電子証明書、DDP ID を送信し、認可確認を行う。
 16. 認可機能は、認可の有効性を確認できた場合、取引 ID、契約形態、契約管理サービス URL を送信する。認可の有効性を確認できない場合、エラーを返却する。
 17. データ交換機能(データ提供側)は、DDP ロケーション管理機能に、DDP ID を送信し、DDP ロケーションの取得を行う。
 18. DDP ロケーション管理機能は、データ交換機能(データ提供側)に、DDP 格納先 URL を返却する。
-

-
19. データ交換機能(データ提供側)は、DDP 格納 URL を元に、DDP 格納用ストレージから、データ取得を行う。
 20. DDP 格納用ストレージは、データ交換機能(データ提供側)に DDP を返信する。
 21. データ交換機能(データ提供側)は、データ取引市場機能に、DATA-EX ID(受領側)、DATA-EX ID(提供側)、取引 ID、ハッシュ値、認証トークン、契約管理 API キーを送信しデータ証憑通知(送信)を行う。
 22. データ取引市場機能は、データ証憑を確認する。
 23. データ取引市場機能は、データ証憑通知(送信)を受領し、データ交換機能(データ提供側)に、通知完了応答を送信する。
 24. データ交換機能(データ提供側)は、来歴管理機能に、履歴の種類、DDP ID、DATA-EX ID(受領側)、DATA-EX ID(提供側)、履歴が生じた日時、1 つ前の履歴情報の履歴 ID、アクセス制御ポリシー、認証トークンを送信し、送信履歴登録を行う。
 25. 来歴管理機能は、送信履歴登録を行う。
 26. 来歴管理機能は、データ交換機能(データ提供側)に送信履歴登録完了を通知する。
 27. データ交換機能(データ提供側)は、データ交換機能(データ受領側)に DDP、交換実績記録用リソース ID、来歴管理サービス URL、取引 ID、契約形態、契約管理サービス URL、DATA-EX ID(提供側)を返信する。
 28. データ交換機能(データ受領側)は、アプリケーション(受領側 WebApp)に DDP を返信する。
 29. アプリケーション(受領側 WebApp)は、DATA-EX 参加者(受領側)に DDP を返信する。
DATA-EX 参加者(受領側)は、画面表示などで提供データを確認する。
 30. DATA-EX 参加者(受領側)は、受け取った DDP の e シールを検証する。
 31. DATA-EX 参加者(受領側)は、DATA-EX 運営事業者に、e シール作成者が DATA-EX に参加していることの確認を依頼する。
 32. DATA-EX 運営事業者が、e シール作成者が DATA-EX 参加者であることを確認する。
 33. DATA-EX 運営事業者が、e シール作成者が DATA-EX 参加者であることの確認結果を送付する。
 34. DATA-EX 参加者(受領側)は、アプリケーション(受領側 WebApp)に、データ受信通知を依頼する。
 35. アプリケーション(受領側 WebApp)は、データ交換機能(データ受領側)に、データ受信通知を依頼する。
 36. データ交換機能(データ受領側)は、データ取引市場機能に、DATA-EX ID(受領側)、DATA-EX ID(提供側)、取引 ID、ハッシュ値、認証トークン、契約管理 API キーを送信し、データ証憑通知(受信)を行う。
 37. データ取引市場機能は、データ証憑通知(受信)を受領し、データ送受信に関する証憑を実施する。
 38. データ交換機能(データ受領側)に、成功応答を送信する。
-

-
39. データ交換機能(データ受領側)は、来歴管理機能に、履歴の種類、DDP ID、DATA-EX ID(受領側)、DATA-EX ID(提供側)、履歴が生じた日時、1 つ前の履歴情報の履歴 ID、アクセス制御ポリシー、認証トークンを送信し、受信履歴登録を行う。
 40. 来歴管理機能は、受信履歴登録を行う。
 41. 来歴管理機能は、データ交換機能(データ受領側)に、受信履歴登録完了を通知する。
 42. データ交換機能(データ受領側)は、アプリケーション(受領側 WebApp)に、受信履歴登録完了を通知する。
 43. アプリケーション(受領側 WebApp)は、DATA-EX 参加者(受領側)に、受信履歴登録完了を通知する。

11-2-3-2-6. DDP 削除

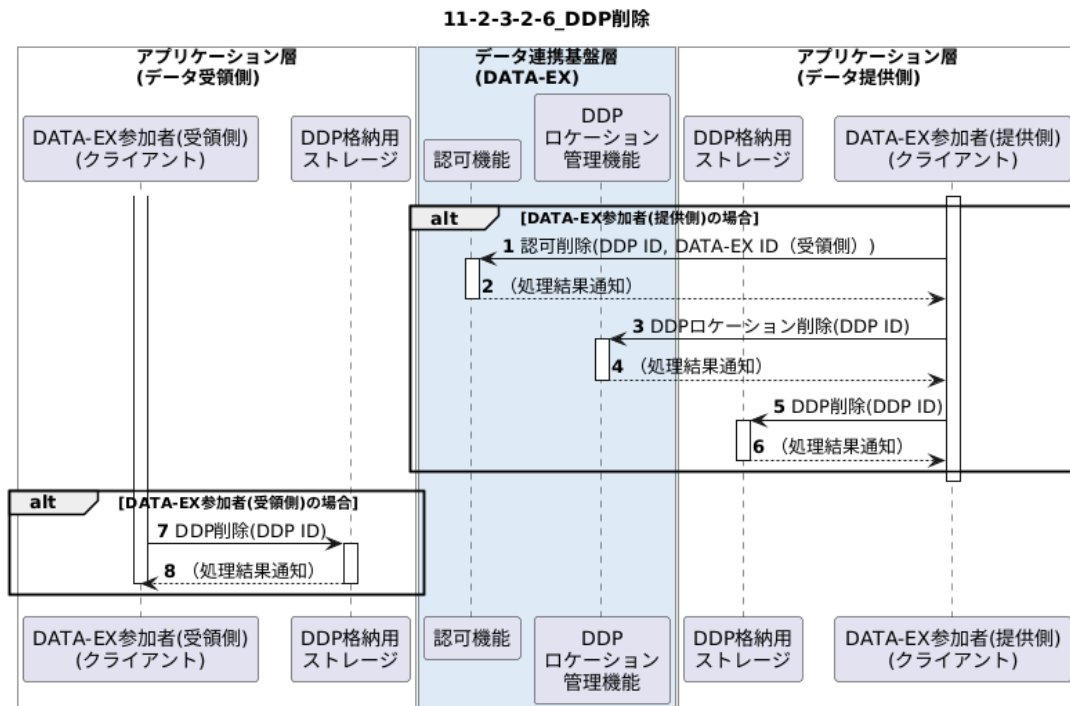


図 57: DDP 削除

DATA-EX 参加者(提供側)の場合、以下の 1.から 6.を行う。

1. DATA-EX 参加者(提供側)は、認可機能に対して、DDP ID、DATA-EX ID(受領側)を指定し、認可を削除する。
2. 認可機能は、処理結果を、DATA-EX 参加者(提供側)に送信する。
3. DATA-EX 参加者(提供側)は、DDP ロケーション管理機能に対して、DDP ID を指定し、DDP のロケーション情報を削除する。
4. DDP ロケーション管理機能は、処理結果を、DATA-EX 参加者(提供側)に送信する。
5. DATA-EX 参加者(提供側)は、DDP 格納用ストレージに対して、DDP ID を指定し、DDP を削除する。
6. DDP 格納用ストレージは、処理結果を、DATA-EX 参加者(提供側)に送信する。

DATA-EX 参加者(受領側)の場合、以下の 7.から 8.を行う。

7. DATA-EX 参加者(受領側)は、DDP 格納用ストレージに対して、DDP ID を指定し、DDP を削除する。
8. DDP 格納用ストレージは、処理結果を、DATA-EX 参加者(受領側)に送信する。

11-2-3-2-7. 来歴確認

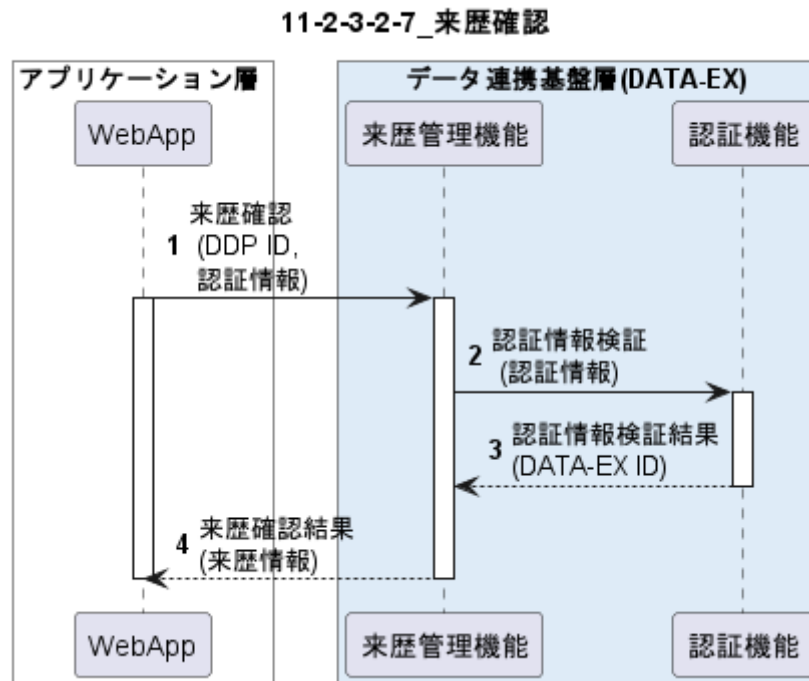


図 58: 来歴確認

1. アプリケーションは、来歴管理機能に、DDP ID、認証情報を送信し、来歴確認を行う。
2. 来歴管理機能は、認証機能に、認証情報を送信し、認証情報検証を行う。
3. 認証機能は、認証情報の有効性を確認できた場合、DATA-EX ID を送信する。認証情報の有効性を確認できない場合、エラーを返却する。
4. 来歴管理機能は、アプリケーションに、DDP ID に紐づく来歴情報を送信する。

11-2-3-2-8. カタログ削除

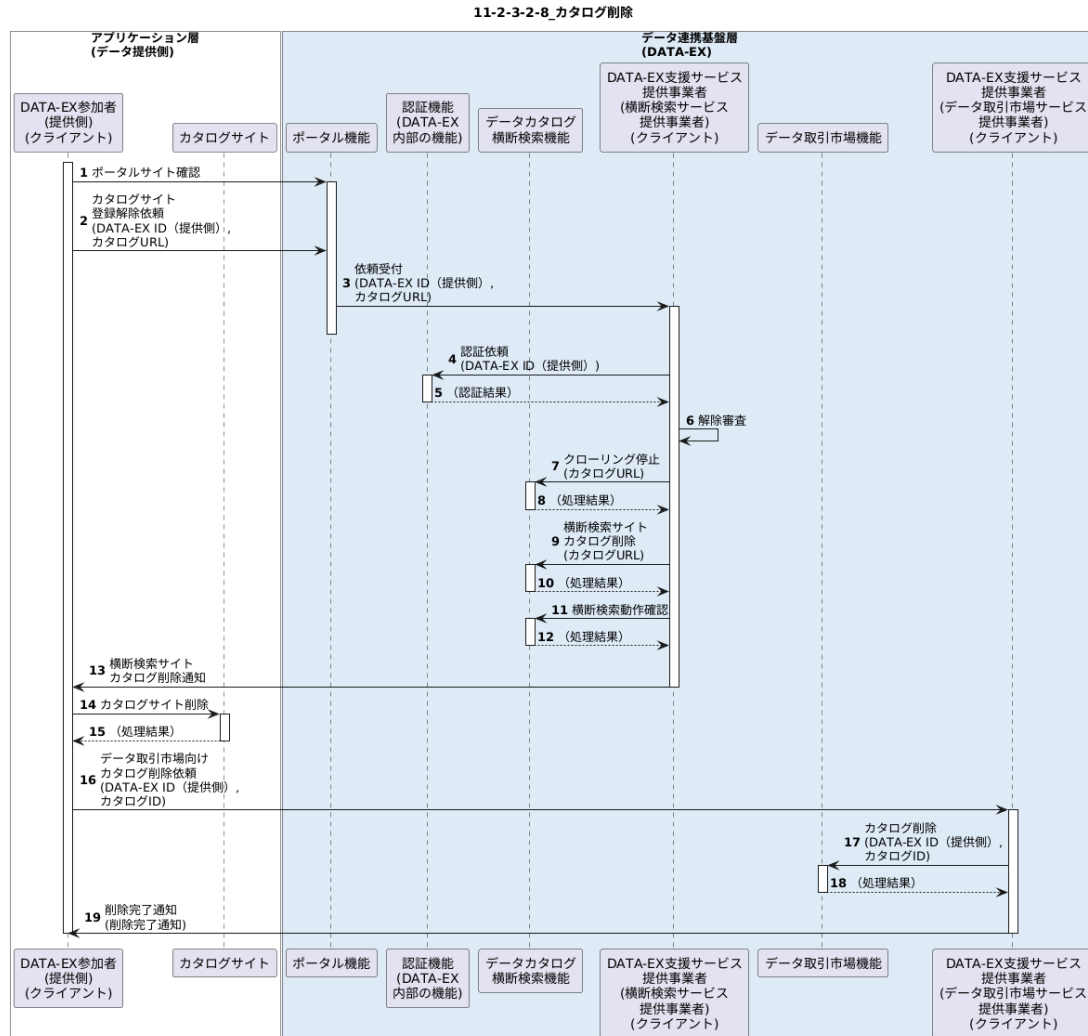


図 59:カタログ削除

1. DATA-EX 参加者(提供側)が、ポータルサイトを確認する。
2. DATA-EX 参加者(提供側)が、DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)に、カタログサイトの登録解除を依頼する。
3. DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)が、DATA-EX 参加者(提供側)からの依頼を受け付ける。
4. DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)が、申請者の認証を、認証機能(DATA-EX 内部の機能)に依頼する。
5. 認証機能(DATA-EX 内部の機能)が、申請者の認証を行い、認証結果を、DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)に通知する。

-
6. DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)が、解除依頼の内容を審査する。
 7. DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)が、データカタログ横断検索機能に対し、カタログサイトのクローリングを停止する。
 8. データカタログ横断検索機能が、DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)に、処理結果を通知する。
 9. DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)が、データカタログ横断検索機能に対し、横断検索サイトのカタログを削除する。
 10. データカタログ横断検索機能が、DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)に、処理結果を通知する。
 11. DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)が、データカタログ横断検索機能にカタログが表示されないことを確認する。
 12. データカタログ横断検索機能が、DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)に、処理結果を通知する。
 13. DATA-EX 支援サービス提供事業者(横断検索サービス提供事業者)が、DATA-EX 参加者(提供側)に、カタログサイトの登録解除を通知する。
 14. DATA-EX 参加者(提供側)が、カタログサイトを削除する。
 15. カatalogサイトが、DATA-EX 参加者(提供側)に、処理結果を通知する。
 16. DATA-EX 参加者(提供側)が、DATA-EX 支援サービス提供事業者(データ取引市場サービス提供事業者)に、データ取引市場向けカタログの削除を依頼する。
 17. DATA-EX 支援サービス提供事業者(データ取引市場サービス提供事業者)が、データ取引市場機能のカタログを削除する。
 18. データ取引市場機能が、処理結果を DATA-EX 支援サービス提供事業者(データ取引市場サービス提供事業者)に通知する。
 19. DATA-EX 支援サービス提供事業者(データ取引市場サービス提供事業者)が、DATA-EX 参加者(提供側)に、削除完了を通知する。

11-2-3-3. 利用停止

11-2-3-3-1. コネクタ撤廃

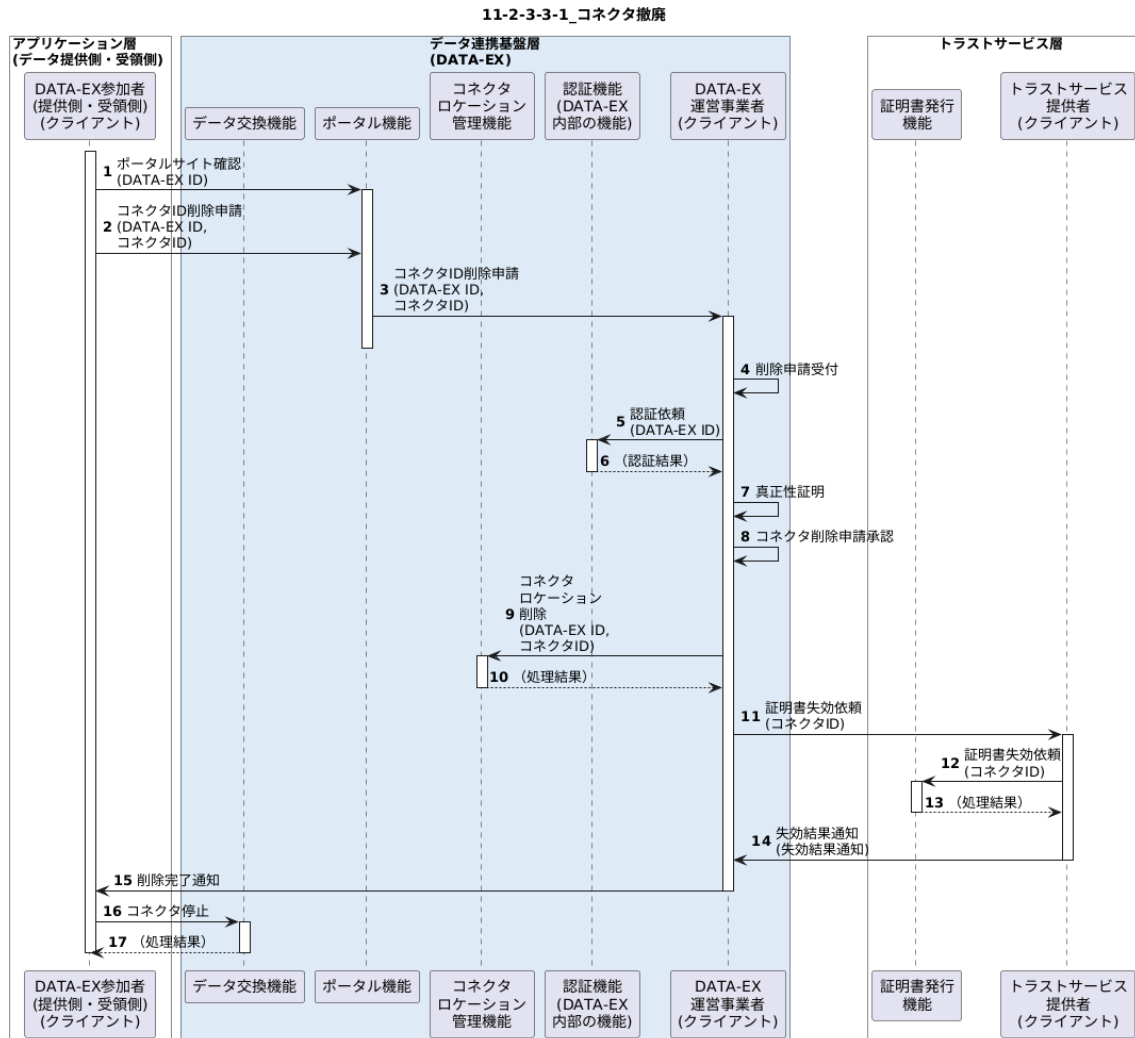


図 60:コネクタ撤廃

1. DATA-EX 参加者(提供側・受領側)が、ポータルサイトを確認し、コネクタ撤廃の申請先を確認する。
2. DATA-EX 参加者(提供側・受領側)が、ポータルサイトにて、コネクタ ID の削除を申請する。
3. ポータル機能が、DATA-EX 運営事業者(クライアント)に、コネクタ ID 削除申請を送信する。
4. DATA-EX 運営事業者が、削除申請を受け付ける。
5. DATA-EX 運営事業者が、申請者の認証を、認証機能(DATA-EX 内部の機能)に依頼する。
6. 認証機能(DATA-EX 内部の機能)が、申請者の認証を行い、認証結果を、DATA-EX 運営事業者(クライアント)に通知する。

-
7. DATA-EX 運営事業者が、申請者が本人であることを確認する。
 8. DATA-EX 運営事業者が、申請内容を確認し、コネクタ ID の削除申請を承認する。
 9. DATA-EX 運営事業者が、コネクタロケーション管理機能にて、コネクタロケーションを削除する。
 10. コネクタロケーション管理機能が、処理結果を、DATA-EX 運営事業者に通知する。
 11. DATA-EX 運営事業者が、トラストサービス提供者に、コネクタの電子証明書の失効を依頼する。
 12. トラストサービス提供者が、証明書発行機能に、コネクタの電子証明書の失効を依頼する。
 13. 証明書発行機能が、トラストサービス提供者に、処理結果を通知する。
 14. トラストサービス提供者が、DATA-EX 運営事業者に、コネクタの電子証明書の失効結果を通知する。
 15. DATA-EX 運営事業者が、DATA-EX 参加者(提供側・受領側)に、コネクタ ID の削除完了を通知する。
 16. DATA-EX 参加者(提供側・受領側)が、データ交換機能(コネクタ)を停止する。
 17. データ交換機能(コネクタ)が、処理結果を、DATA-EX 参加者(提供側・受領側)に通知する。

11-2-3-3-2. 退会

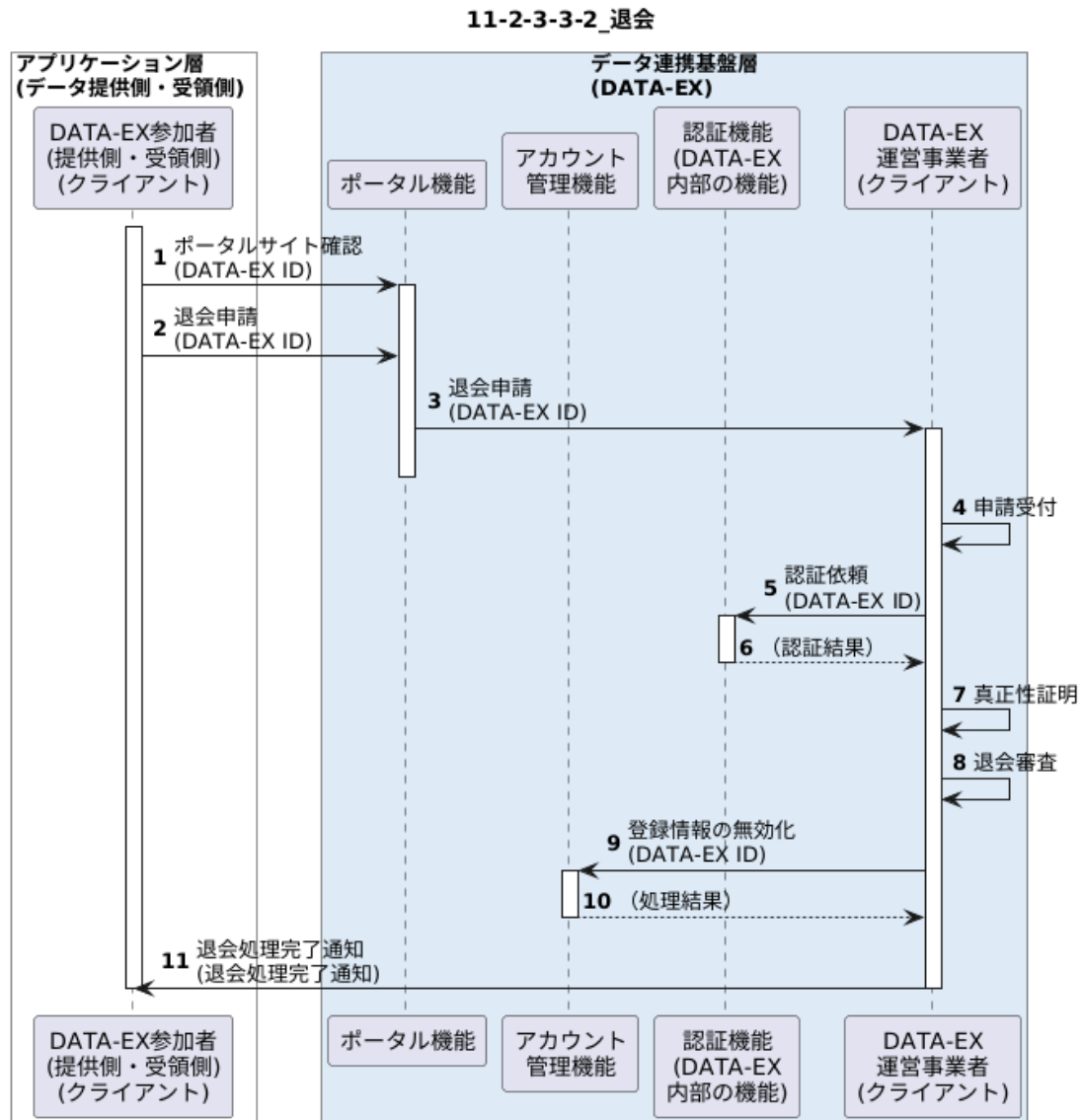


図 61: 退会

1. DATA-EX 参加者(提供側・受領側)が、ポータルサイトを確認し、退会の申請先を確認する。
2. DATA-EX 参加者(提供側・受領側)が、ポータルサイトにて、退会を申請する。
3. ポータル機能が、DATA-EX 運営事業者に、退会申請を送信する。
4. DATA-EX 運営事業者が、退会申請を受け付ける。
5. DATA-EX 運営事業者が、申請者の認証を、認証機能(DATA-EX 内部の機能)に依頼する。

-
6. 認証機能(DATA-EX 内部の機能)が、申請者の認証を行い、認証結果を、DATA-EX 運営事業者に通知する。
 7. DATA-EX 運営事業者が、申請者が本人であることを確認する。
 8. DATA-EX 運営事業者が、退会申請内容を審査する。
 9. DATA-EX 運営事業者が、アカウント管理機能にて、アカウントの無効化を行う。
 10. アカウント管理機能が、処理結果を、DATA-EX 運営事業者に通知する。
 11. DATA-EX 運営事業者が、DATA-EX 参加者(提供側・受領側)に、退会処理の完了を通知する。

12. セキュリティ・トラスト

DATA-EX では、すべてのステークホルダーが安心してデータ授受やその他 DATA-EX サービスを利用することができる状態を目指している。ステークホルダーに損害を与えうるリスクを DATA-EX から排除し、あらゆるリスクを想定して DATA-EX 内のリソースの監視と制御を行う。

なお、本章におけるリソースとは、安全安心なデータ管理を実現するために DATA-EX のセキュリティで保護する対象を指す。

また、トラストサービス基盤等を利用し、DATA-EX 上の参加者のトラスト、利用されるシステム及び扱われるデータのトラストを確保する。

12-1. リソースの識別

リソースは、常に識別できる状態で DATA-EX に登録されている必要がある。

DATA-EX では、以下をセキュリティ保護対象のリソースとして定義する。

- アカウント

DATA-EX に接続することができるあらゆるステークホルダーのアカウント情報。

- デバイス

ステークホルダーが DATA-EX に接続するために利用する、コネクタが実装されたサーバー・クライアント。

- サービス

オンプレミスなデータセンターやクラウドといった場所を問わず、DATA-EX 参加者が DATA-EX で利用するサービス。

- DDP

DATA-EX 参加者同士が実際にやり取りする、データセット、データセットの付帯情報、契約情報などが一体になったパッケージ。

12-2. ネットワークの保護

ネットワーク、すなわちコネクタ間の通信経路は適切な暗号化によって安全性を確保する。

DATA-EX 内の通信については、DATA-EX 運営事業者が指定するセキュリティ対策（通信の暗号化など）を実施する。また、DATA-EX 外の通信については、DATA-EX 外の通信の安全性を確保できるように DATA-EX 参加者がセキュリティ対策を講じる。この際には原則「CRYPTREC 暗号リスト」や「TLS 暗号設定ガイドライン～安全なウェブサイトのために（暗号設定対策編）～」を参照し、適切な暗号技術を実装する。もし DATA-EX 参加者がこれらのガイドラインとは異なる方法で通信を行う場合、DATA-EX 参加者同士が交わす契約書でその旨を明記する必要がある。

12-3. リソースの脆弱性診断

各種リソースは恒常的に安全とはいえないため、各種リソースの状態や構成が安全か確認する必要がある。各ステークホルダーは、自らが提供あるいは管理するリソースの構成を定期的に取り得て脆弱性診断を実施し、適切なセキュリティ対策を講じる。

脆弱性診断に用いられる各種リソース構成の具体例を以下に記す。

- DATA-EX 参加者の属性情報
- 当人認証に利用した認証要素
- デバイスの構成情報(型番、OS、ミドルウェアのバージョン、FQDN 等)

12-4. アクセス制御ポリシー・アクセス管理

認証機能におけるアクセス制御ポリシーは DATA-EX 運営事業者が設定し、それ以外のアクセス制御ポリシーは必要に応じて DATA-EX 参加者が各自設定する。

12-5. 不正利用の検知

システムの信頼性を高めるためにシステムに対する不審な動きを早期に検知する必要がある。そのために、各ステークホルダーはリソースのログの取得、アラートの通知など、DATA-EX のリソースとアクセスの監視を行う。DATA-EX を相互運用するにあたって、ステークホルダー間で責任範囲、監視の範囲を明確化する。DATA-EX 運営事業者が管理するサービスについては、適切な監視ポイントを設置し、DATA-EX が定めるポリシーに従ってセキュリティ状況を監視する。その際 DATA-EX 参加者の活動、例外処理、過失及び情報セキュリティ事象を記録したイベントログ(システム動作、システムへのアクセス記録、データへのアクセス、システム構成の変更、ウイルス対策・侵入検知システムの作動など)を取得、保持し、定期的にレビューを行う。コネクタとそれに付随する環境、あるいは DATA-EX 支援サービスについては、必要に応じて DATA-EX 参加者や DATA-EX 支援サービス提供者が各自で管理・監視する。

12-6. トラスト全体像

分野間データ連携基盤である DATA-EX 上のデータ交換では、参加者のトラスト、利用されるシステム及び扱われるデータのトラストが確保されている必要がある。

DATA-EX では、連携サービスとしてトラストサービス等を利用し、信頼できるデータの流通を実現する。

トラストサービス基盤と DATA-EX の各種機能、ステークホルダーを含む、トラスト全体像を図 62 に示す。

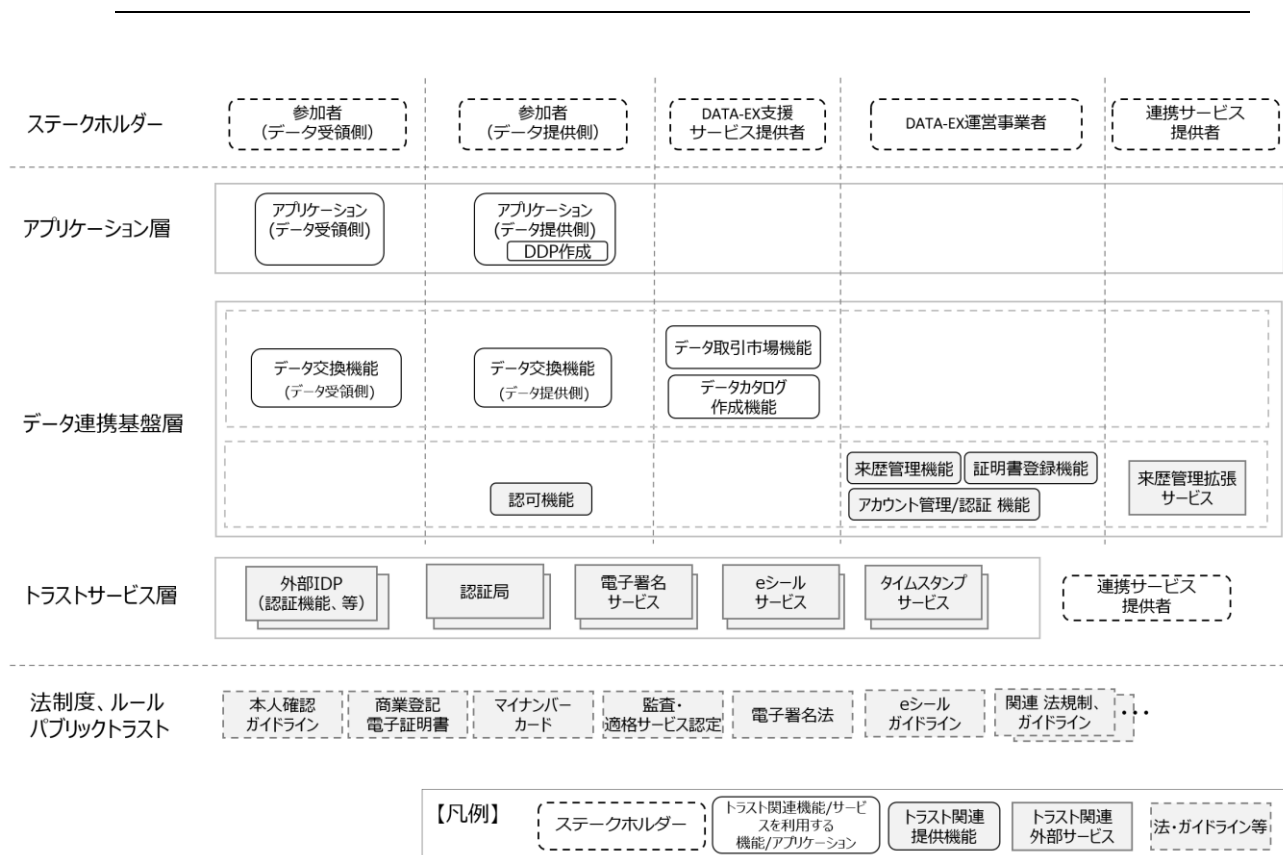


図 62:トラスト全体像

DATA-EX が利用を想定する連携サービスは、トラストサービスとして外部 IdP、認証局、e シールサービス、電子署名サービス、タイムスタンプサービス、その他として来歴管理拡張サービスである。

12-6-1. 参加者のトラスト

参加者のトラストとは、参加者が DATA-EX のサービスを利用する際の本人性の確認のことである。

DATA-EX 参加者は、DATA-EX 運営事業者によって組織に所属する個人単位で管理され、参加組織内の個人に対して DATA-EX ID が割り当てられる。

組織が DATA-EX に参加する際には、組織を代表する権限を持つ個人が参加を申請し、DATA-EX 運営事業者による組織、個人の身元確認および DATA-EX の規定に即するかの審査を経て、DATA-EX への参加が許可（認可）される。この際、DATA-EX 内での組織アカウント管理者を 1 名以上設定する。また、DATA-EX 参加組織を示す DATA-EX ID が割り当てられる。

法人組織等に所属せず個人単位での活動を行う申請者についても、DATA-EX 運営事業者は個人事業主またはそれに準じたものとして、組織と関連付けて管理を行う。

DATA-EX 参加者は、DATA-EX 運営事業者があらかじめ規定した基準に従い、身元確認、当人認証を受けた上で、DATA-EX を利用する。また、DATA-EX 運営事業者は基準に従って身元確認・当人認証を実施し、その基準を一般に公表しなければいけない。

身元確認および当人認証は外部 IdP に委任し、外部 IdP により実施される身元確認のレベルと当人認証のレベルをもって、DATA-EX の基準を満たすか否かの判定を行ってもよい。

既に DATA-EX に参加している組織に属する個人を新たに追加で参加させる場合には、DATA-EX 運営事業者が、追加申請する個人の身元確認と、個人が組織に属することの確認を行う。個人が組織に属することの確認は、信頼できる外部 IdP による属性情報の提供、または組織アカウント管理者による承認によって行うことができる。

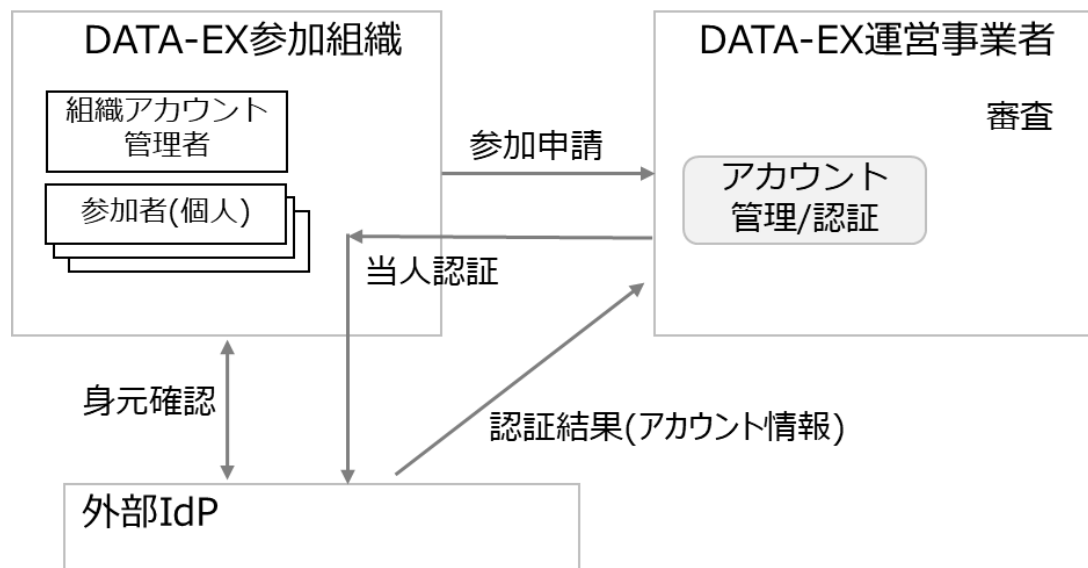


図 63: DATA-EX への参加

身元確認のレベルおよび当人認証のレベルは、一般に米国 NIST SP800-63 の IAL (Identity Assurance Level: 身元確認保証レベル) と AAL (Authentication Assurance Level: 当人認証保証レベル) を参考として、DATA-EX 運営事業者によって予め定めるものとする。

日本における基準としては、「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」や「民間事業者向けデジタル本人確認ガイドライン」等のガイドラインを参考にできる。

トラストサービス基盤が行う身元確認においては、例えば、マイナンバーカードを用いた公的個人認証サービスや Identity Wallet などの改ざん防止機能を利用する、対面による公的証明書をを用いるなどの IAL2 以上のレベルを要求する。

当人認証においては、二要素認証以上を用いた AAL2 レベル以上を要求する。

① 身元確認

参加者の身元確認は、DATA-EX 参加者の実在性および参加申請する個人と組織の関係を確認する行為を指す。

DATA-EX 参加者(個人)の身元確認にあたっては、登録する氏名・住所・生年月日等が正しいことを、リモートまたは対面で確認する。

DATA-EX 運営事業者は、DATA-EX 参加組織の実在性および申請者が参加組織に所属し申請権限をもっていることを、所定の基準を元に確認を行う。確認にあたっては、外部 IdP により実施可能な方法を考慮し、DATA-EX 運営事業者が基準を決定、運用する。

現時点では、前記「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」で法人共通認証基盤として言及されている gBizID の利用が候補の1つである。gBizID は個人の認証を2要素認証で行え、身元確認済みの組織情報の取得も可能である。

その他に、商業登記電子証明書等、法人向け電子証明書を使った確認(民間利用が可能なもの)や、法制度の改定等が検討されている電子委任状を活用するといった手段が想定されるが、法制度やガイドラインの制定、外部 IdP サービスの提供状況に応じて、DATA-EX 運営者が基準や対応サービスを見直していく必要がある。

② 当人認証

当人認証はリソースの利用を試みる DATA-EX 参加者(個人)に対して要素認証を行うことである。当人認証は2要素以上で行い、特に2要素目は所有情報か生体情報で認証しなければならない。

12-6-2. システムのトラスト

DATA-EX を構成するサービスが稼働するサーバーや、コネクタが実装されたデバイスは、認証局が発行した電子証明書を用いて通信時に自身の正当性を証明する。アカウントや DDP などの高度なセキュリティ保護を要するリソースを保有する場合、自身の正当性の証明に加えて、通信相手の正当性を検証する。通信相手の正当性を判断する情報として、例えば電子証明書、クライアント ID とクライアントシークレットなどを利用する。

コネクタ登録時に DATA-EX 運営事業者は、デバイスの実在性を確認する身元確認として、購入時に入手したシリアル番号や割り当てた IP アドレスなどの管理上の情報と、実際に当該デバイス上で確認できる情報を照合する。コネクタロケーションの情報は、DATA-EX 運営事業者が管理を行う。

12-6-3. データのトラスト

データのトラストは、データ、オブジェクトの内容の完全性の保証に加え、データ作成者、送信者の真正性、契約内容に対する契約者の意思表示、その時刻での存在証明など、目的、用途によって各種のトラストサービスを利用し、確認を行う。

目的、用途に応じて異なる検証内容の例として、対象となるデータ、オブジェクトと、検証すべき内容、検証を行う主体の関係を表 8 に示す。

表 8: 対象となるデータ、オブジェクトと検証内容、検証主体

No	対象	検証内容	検証主体
1	DDP	DDP 提供者の真正性、データの完全性	DATA-EX 参加者(データ受領)
2	カタログ	カタログ作成者の真正性、データの完全性	DATA-EX 参加者
3	契約書	契約者の真正性、意志、データの完全性、作成日時	DATA-EX 参加者(提供、受領の双方)

上記を保証するトラストサービスとして、電子署名サービス、e シールサービス、タイムスタンプサービスがある。

電子署名サービスと e シールサービスを利用する際には、DATA-EX 参加者は事前に認証局で、DATA-EX 参加者の個人、組織に関する電子証明書を発行しておかなければならない。

これらのトラストサービスとの契約や電子証明書の発行は DATA-EX とは独立して各参加者によって行われるものであり、DATA-EX 運営事業者は、DATA-EX で利用可能と認定するトラストサービス、トラストアンカーを規定する。

トラストサービス基盤の電子署名サービスと e シールサービスを利用する際の認証・認可についても、「12-6-1. 参加者のトラスト」に記載と同等の保証レベルをもつ IdP を利用しなければならない。

e シールに利用する組織に関する電子証明書の内容は総務省を中心に検討されている状況であるが、デジタルトラスト協議会(JDTF)から「e シール解説～実用化に向けて～バージョン 1.0」がガイドラインとして発行されており、これらの内容、今後の検討状況も踏まえて、トラストサービス基盤を利用していく必要がある。

DATA-EX としては、e シール用電子証明書に記載される組織識別子と組織名が、「12-6-1. 参加者のトラスト」で申請を受け付け、認可した組織と対応付け可能とする必要がある。

組織識別子としては、前記 gBizID でも利用されている法人番号や、取引主体識別子(Legal Entity Identifier)が例として記載されている。

DATA-EX では、データを提供することを目的としてカタログを作成する DATA-EX 参加者がカタログに対して e シールを作成、付与することで、カタログ作成者の真正性と内容の完全性を担

保する。また、DDP を作成する DATA-EX 参加者が DDP に対して e シールを作成、付与することで、DDP 作成者の真正性と内容の完全性を担保する。

契約書に対する電子署名、e シール、タイムスタンプ付与も含めた DATA-EX におけるトラストサービス利用例は、「8.シナリオ」にトラストサービス提供者とのやりとりとして記載している。

12-6-4. データ取引の証跡管理

データの生成、加工、授受のタイミングで、履歴情報を保存することにより、証跡を管理できる。DATA-EX はデータ連携基盤であることから、DATA-EX 内での参加者間のデータの受け渡しの事実は重要な情報となるため、来歴管理サービスにより DDP の作成・送受に対する来歴管理を行う。

また、連携サービスである来歴管理拡張サービスにより、データの加工等の証跡も管理できる。DDP の作成・送受の来歴に対してデータの加工等の来歴を補完的に参照することで、データの成り立ちを確認できる。

来歴は、特定の DDP に係る複数の履歴情報を時系列に連結した構造を持つ。履歴情報同士は、属性値「1つ前の履歴情報の履歴 ID」により表現される。これにより、特定 DDP に係る一連の流れの参照を容易にするとともに、各履歴情報に電子署名を付与する事などで高い改ざん耐性を保証している。具体例を、図 64: 来歴の具体例に示す。

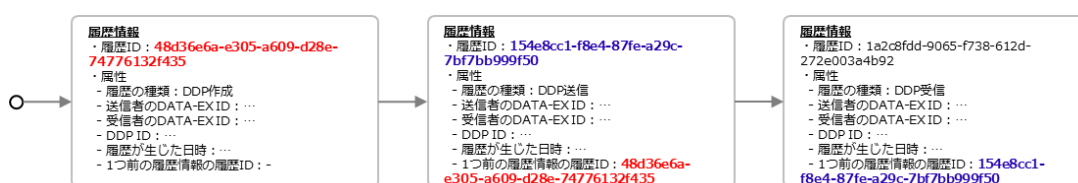


図 64: 来歴の具体例

来歴は DATA-EX ID を含むため、個人情報保護の観点から、DDP の授受に無関係な DATA-EX 参加者による来歴の閲覧を制限する必要がある。DDP の授受に関係する DATA-EX 参加者が 3 者以上になる場合、より細かい単位でのアクセス制御を必要とする可能性があるため、柔軟にアクセス制御ポリシーを定められる事が望ましい。

アクセス制御ポリシーは、ポリシー設定対象と、ポリシー設定対象の閲覧を許可するステークホルダーの組み合わせの集まりから構成される。ポリシー設定対象は、履歴情報の各属性値を指定する。

DDP の作成者は、DDP 作成履歴情報を登録する際に、その後の DDP 送受を含めた来歴全体に対するアクセス制御ポリシーを設定できる。来歴全体に対するアクセス制御ポリシーは、個々の履歴情報のアクセス制御ポリシーの設定よりも優先される。

閲覧を許可するステークホルダーには、対象となる DATA-EX ID、対象の履歴情報より前の履歴登録者、または対象の履歴情報より後の履歴登録者といった対象を指定できる。

DATA-EX で DDP 作成・送受の履歴情報が登録される契機には以下のようなものがある。

- ① 「8-2-2-4. DDP 作成」における DDP 作成履歴登録依頼
DATA-EX 参加者(データ提供)が、DDP の作成者が自身である事を DATA-EX 参加者(データ受領)に示すために、DDP 作成の履歴情報を登録する。
- ② 「8-2-2-5. データ交換」における DDP 送付履歴登録依頼
DATA-EX 参加者(データ提供)が、DDP の送付者が自身である事を DATA-EX 参加者(データ受領)に示すために、DDP 送信の履歴情報を登録する。
- ③ 「8-2-2-5. データ交換」における DDP 受信履歴登録依頼
DATA-EX 参加者(データ受領)が、DDP の受領者が自身である事を DATA-EX 参加者(データ提供)に示すために、DDP 受信の履歴情報を登録する。

DATA-EX で DDP 削除の履歴情報が登録される契機はシナリオ上存在しない。ただし、DATA-EX 参加者(提供者)と DATA-EX 参加者(受領者)の間で契約等によりデータ交換後の DDP 削除について取り決めを行った場合、DATA-EX 参加者(受領者)が DDP 削除を履行した事実を記録するために、DDP 削除の履歴情報を登録する事は考えられる。

DATA-EX で DDP 作成・送受の来歴情報が参照される契機には以下のようなものがある。

- ① 「8-2-2-7. 来歴確認」における DATA-EX 参加者(データ受領)の来歴情報提供依頼
DATA-EX 参加者(データ受領)が、受領した DDP の作成者や送信者の正当性を確認するために、DDP の来歴を参照する。また、監査等の用途で利用するために、過去受信した複数の DDP の来歴を参照する。
- ② 「8-2-2-7. 来歴確認」における DATA-EX 参加者(データ提供)の来歴情報提供依頼
DATA-EX 参加者(データ提供)が、送付した DDP の受信者の正当性を確認する事を目的に、DDP の来歴を参照する。また、監査等の用途で利用するために、過去送付した複数の DDP の来歴を参照する。
- ③ DATA-EX 運営事業者による確認
DATA-EX 運営事業者が、分野間データ連携サービスの利用状況を把握する事等を目的に、複数の DATA-EX 参加者に係る DDP の来歴を参照する。

DDP に含まれるデータセットに関する加工等の履歴を来歴情報として登録管理する場合には、来歴管理拡張サービスを用いる。

来歴管理拡張サービスが履歴管理する対象となる加工の種類としては、例えば下記のようなものがある。

-
- ・複数の DDP に含まれるデータセットを結合して、新たに DDP を作成
 - ・1 つの DDP に含まれるデータセットのうち、一部のデータセットを取り出し、新たに DDP として作成
 - ・DDP として受領するデータセットは使わずに、新規にデータセットを集約し、新たに DDP を作成。(DDP の新規作成ではあるが、加工の種類の一つとして扱うこととする)
 - ・受領した DDP に含まれるデータセットと、自分が準備するデータセットを組み合わせ、新たに DDP を作成
 - ・DDP に含まれるデータセットの一部のデータに演算処理、エンコード処理(難読化、暗号化等)を行い、新たに DDP を作成

来歴管理拡張サービスは、これらの加工処理に関する情報を、元となるデータセットを含む DDP の DDP ID および、その DDP を受信した際の受信履歴 ID と紐づけ、新たに作成した DDP の DDP ID および、その作成履歴 ID とともに、加工履歴情報として、データの加工等の証跡を保存し、依頼に応じて加工来歴情報を要求元に提供する。

加工の詳細情報は、組織の競争力につながる情報や、データ交換を行う DATA-EX 参加者が秘密にすべき情報を含みうるため、加工履歴情報内に保存する内容に加えて、加工を行った処理のログや加工仕様を、データ加工者である DATA-EX 参加者が保存、管理を行い、その情報にアクセスするための加工詳細参照情報を加工履歴情報内に保存することもできる。

DATA-EX 参加者が保存、管理を行う加工の詳細情報へのアクセス管理は、データ加工者である DATA-EX 参加者の責任にて実施する。

来歴管理拡張サービスは、保存する履歴情報について、電子署名などを用いて改ざん対策を講じて、履歴情報のトラストを保証する。

DDP の加工履歴を含んだ来歴情報を確認したい DATA-EX 参加者は、該当 DDP の加工来歴情報を来歴管理拡張サービスから取得し、取得した加工来歴情報に含まれる、加工に利用した受信 DDP および該当 DDP の送受履歴等の来歴情報を DATA-EX 内部の来歴管理機能から取得し、連結することで、加工履歴を含んだ一連のデータの来歴を確認できる。

12-7. 参加者のトラスト(要件)

12-7-1. DATA-EX への参加

DATA-EX へ参加する個人、組織の真正性を担保するために、DATA-EX 運営事業者は、DATA-EX への参加を希望する個人、組織に対して、あらかじめ規定した参加基準を満たすことの確認、審査を行わなければならない。(SHALL)

DATA-EX に参加する組織は、組織アカウント管理者を 1 名以上設定し、DATA-EX 運営事業者に通知しなければならない。(SHALL)

DATA-EX 運営事業者は、DATA-EX 参加組織の実在性確認、および組織アカウント管理者など個人の身元確認を、下記の個人、組織それぞれの確認手段に従って行う。

DATA-EX 運営事業者は、DATA-EX に参加申請する個人の実在性を確認し、参加資格を満たすことを確認しなければならない。(SHALL) DATA-EX 運営事業者は、個人の実在性の確認のために、外部 IdP による身元確認結果や、申請者から提供されるアカウント情報を利用できる。(MAY)

DATA-EX 運営事業者は、申請された組織が実在すること、及び組織アカウント管理者がその組織に所属していることを確認しなければならない。(SHALL)

組織が実在し、かつ、なりすましでないことは、例えば、商業登記電子証明書や民間の電子証明書等の法人向け電子証明書を使って確認できる。(MAY)

DATA-EX 運営事業者は、組織の実在確認または組織アカウント管理者が組織に所属していることを外部 IdP に委任してもよい。(MAY)

DATA-EX 運営事業者は、DATA-EX に参加した個人、組織およびその関係性を管理する。

DATA-EX 運営事業者は、DATA-EX 参加者(個人)の属性として、所属する組織を紐づけて管理しなければならない。(SHALL) 法人番号等の組織に対する情報をもたない個人事業主の場合には、適格請求書発行事業者の登録番号や個人名などをもとにした組織情報を作成し、個人の属性と関連付ける方法がある。(MAY)

DATA-EX 参加者(組織)の属性として、組織アカウント管理者を紐づけて管理しなければならない。(SHALL)

組織アカウント管理者および組織が DATA-EX に参加後は、組織に所属する個人が DATA-EX に参加申請する際に、組織アカウント管理者は、申請者が組織に所属している関係性を保証できる。(MAY)

組織アカウント管理者を含めた DATA-EX 参加者(個人)が、DATA-EX 運営事業者が運営するサービスを利用する際には、2 つ以上の認証要素を用いた本人認証を受けなければならない。(SHALL) DATA-EX 運営事業者は、本人認証を外部 IdP に委任する場合、外部 IdP が実施する本人認証の方法及び本人認証のレベルの情報を入手し、DATA-EX 運営事業者があらかじめ定めた基準を満たすものかを確認しなければならない。(SHALL)

12-7-2. 参加者の識別

コネクタを介した DATA-EX 参加者の識別には、DATA-EX 参加者の認証情報を利用する。(SHALL)

DATA-EX 運営事業者は、認証に成功した DATA-EX 参加者に対して、認証情報を発行できる。

認証情報には、DATA-EX 参加者の識別情報を含まなければならない。(SHALL)

自身の身元の真正性を証明したい DATA-EX 参加者は、DATA-EX 運営事業者に対して、自身に関する認証情報の発行を依頼し、取得する。

認証情報を受け取った DATA-EX 参加者は認証情報提供者が真正であることを、DATA-EX 運営事業者を確認しなければならない。(SHALL)

12-8. システムのトラスト(要件)

DATA-EX の提供サービスは、サービスの利用者に対して、信頼できる認証局により発行された電子証明書を提示し、自身の真正性を証明しなければならない。(SHALL) 保有するリソースのセキュリティ要件に応じて、利用元サーバー・クライアントに真正性の証明を求めてよい。(MAY)

DATA-EX 運営事業者は、DATA-EX 参加者からの利用申請に応じて、デバイスのシリアル番号や割り当てられた IP アドレスなどの管理上の情報と、実際に当該デバイス上で確認できる情報を照合し、デバイスの実在性の確認を行ってもよい。(MAY)

DATA-EX 運営事業者は、DATA-EX 参加者からの利用申請に応じて、コネクタ ID の発行、コネクタロケーション情報の登録、および、電子証明書の作成を行い、証明書情報を含むコネクタ設定情報を参加者に提供しなければならない(SHALL)

コネクタロケーション情報については、参加者のコネクタのエンドポイントとコネクタ ID と対応付けてコネクタロケーション管理機能に登録しなければならない。(SHALL)

電子証明書については、参加者から受領した情報をもとにトラストサービスの認証局と連携を行うことで作成できる。(MAY)

DATA-EX 参加者は、コネクタ設定情報を用いてコネクタを設定しなければならない。(SHALL)

コネクタは、データ交換相手のコネクタについて、コネクタ ID をもとにコネクタロケーション管理機能からエンドポイントを取得し、通信時に DATE-EX 運営事業者から受領した証明書情報を用いて相互認証を行うことで、互いの正当性を確認しなければならない。(SHALL)

12-9. データのトラスト(要件)

DATA-EX 参加者により作成され、提供されるオブジェクトであるカタログ、契約書、DDP は、取り扱う内容の重要度、必要性に応じて、作成者の真正性および内容が保証される形で、DATA-EX 内で取り扱われる必要があり、トラストサービス基盤を利用することにより、データのトラストを実現する。

12-9-1. トラストサービス基盤連携

DATA-EX 運営事業者は、トラストサービス基盤に関する認定指針又はガイドラインに基づき、DATA-EX で利用可能な電子署名および e シールに関する認証局、リモート電子署名事業者、リモート e シール事業者、タイムスタンプ事業者または、その基準を選定、公開しなければならない。(SHALL)

e シールに含まれる電子証明書には、組織等の識別子および組織名が含まなければならない。(SHALL)

組織等の識別子は、DATA-EX 運営事業者が管理する DATA-EX 参加者の組織に関する属性情報と対応付けられる形式のものでなくてはならない。(SHALL)

12-9-2. トラストサービス基盤利用準備

データ提供を担当する DATA-EX 参加者は、e シール用の電子証明書を認証局に申請し、リモート e シールサービスの利用可能な状態にしなければならない。(SHALL)

契約を伴うデータ提供を担当する DATA-EX 参加者および契約を伴うデータ受領を担当する DATA-EX 参加者は、電子署名用の電子証明書を認証局に申請し、リモート電子署名サービスの利用可能な状態にしなければならない。(SHALL)

トラストサービス基盤の電子署名サービスと e シールサービスを利用する際の認証・認可についても、「12-7. 参加者のトラスト(要件)」に記載と同等の保証レベルをもつ IdP を利用しなければならない。(SHALL)

12-9-3. カタログ

データを提供することを目的としてカタログを作成する DATA-EX 参加者は、カタログに対して e シールを付与しなければならない。(SHALL)

カタログを受領した DATA-EX 参加者は、カタログの作成者の真正性とカタログの完全性を確認する為に、e シールの検証を行わなければならない。(SHALL)

12-9-4. 契約書

DATA-EX 参加者は、契約書に対して電子署名を付与してもかまわない。(MAY)

DATA-EX 参加者は、契約書に対して e シールを付与してもかまわない。(MAY)

データの提供を担当する DATA-EX 参加者は、契約書に対して DATA-EX 運営事業者が示す基準を満たすタイムスタンプをしてもかまわない。(MAY)

DATA-EX 参加者は、付与されている場合には、契約相手の電子署名を検証し、付与されている場合は e シールの検証も行わなければならない。(SHALL)

12-9-5. DDP

データ提供を担当する DATA-EX 参加者は、DDP に対して e シールを付与してもよい。(MAY)

データ受領を担当する DATA-EX 参加者は、受領した DPP が e シールを付与したものである場合には、e シールの検証を行わなければならない。(SHALL)

データ提供、受領を担当する DATA-EX 参加者は、「12-10. データ取引の証跡管理(要件)」機能を利用することにより、DDP の提供、受領時の日時情報としてタイムスタンプを残すことができる。(MAY)

12-10. データ取引の証跡管理(要件)

DATA-EX 参加者は、DDP の作成・送受の証跡管理に来歴管理サービスを利用できる。(MAY)

また、DATA-EX 参加者は、DDP に含まれるデータセットの加工の証跡管理に来歴管理拡張サービスを利用できる。(MAY)

12-10-1. 来歴管理サービス

来歴管理サービスは、DDP の来歴について、DATA-EX 参加者からの履歴登録依頼と来歴情報提供依頼を受け付ける機能を提供しなければならない。(SHALL)

来歴管理サービスは、履歴登録依頼者・来歴情報提供依頼者を DATA-EX ID により認証しなければならない。(SHALL)

来歴管理サービスは、履歴登録依頼に対し、履歴 ID、履歴が生じた日時、および、履歴登録者を特定可能な情報を生成し、履歴情報と組み合わせで保存しなければならない。(SHALL)

履歴が生じた日時には、サービスが履歴登録依頼を受け付けた日時などを用いる。(MAY)

履歴登録者を特定可能な情報には、履歴登録者の DATA-EX ID、電子証明書、デジタル署名などを用いてよい。(MAY)

履歴登録依頼時の履歴情報は、履歴情報に対するアクセス制御ポリシーを含んでよい。(MAY)

来歴管理サービスは、履歴登録依頼に対し、生成した履歴 ID を履歴登録依頼者に通知しなければならない。(SHALL)

来歴管理サービスは、保存する履歴情報について、電子署名などを用いて改ざん対策を講じなければならない。(SHALL)

来歴管理サービスは、履歴登録依頼として、DDP 作成履歴登録依頼、DDP 送付履歴登録依頼、DDP 受信履歴登録依頼、DDP 削除履歴登録依頼を受け付けなければならない。(SHALL)

来歴管理サービスは、DDP 作成履歴登録依頼に対し、履歴の種類、送信者の DATA-EX ID、DDP ID、DDP のハッシュ値を属性として持つ履歴情報を保存できなければならない。(SHALL)

DDP 作成履歴登録依頼時の履歴情報は、DDP の来歴全体に対するアクセス制御ポリシーを含んでよい。(MAY)

来歴管理サービスは、DDP 送付履歴登録依頼に対し、履歴の種類、送信者の DATA-EX ID、受信者の DATA-EX ID、DDP ID、1つ前の履歴情報の履歴 ID を属性として持つ履歴情報を保存できなければならない。(SHALL)

来歴管理サービスは、DDP 受信履歴登録依頼に対し、履歴の種類、送信者の DATA-EX ID、受信者の DATA-EX ID、DDP ID、1つ前の履歴情報の履歴 ID を属性として持つ履歴情報を保存できなければならない。(SHALL)

来歴管理サービスは、DDP 削除履歴登録依頼に対し、履歴の種類、送信者の DATA-EX ID、受信者の DATA-EX ID、DDP ID、1つ前の履歴情報の履歴 ID を属性として持つ履歴情報を保存できなければならない。(SHALL)

来歴管理サービスは、来歴情報提供依頼に対し、指定された DDP の来歴を依頼者に提供しなければならない。(SHALL)

来歴管理サービスは、来歴情報提供依頼に対して提供する来歴を、事前に決められた範囲、または、依頼者が送信者または受信者となっている DDP の来歴に限定しなければならない。(SHALL)

提供する来歴情報にアクセス制御ポリシーが含まれる場合、アクセス制御ポリシーに従い提供する情報を限定しなければならない。(SHALL)

来歴管理サービスは、来歴情報提供依頼に対し、履歴が生じた日時などの属性を対象とした来歴検索を行い、複数の DDP の来歴を依頼者に提供してもよい。(MAY)

12-10-2. 来歴管理拡張サービス

来歴管理拡張サービスは、DDP に含まれるデータセットの来歴について、DATA-EX 参加者からの加工履歴登録依頼と加工来歴情報提供依頼を受け付ける機能を提供しなければならない。(SHALL)

来歴管理拡張サービスは、履歴登録依頼者・来歴情報提供依頼者を DATA-EX ID により認証しなければならない。(SHALL)

来歴管理拡張サービスは、履歴登録依頼に対し、履歴が生じた日時、および、履歴登録者を特定可能な情報を生成し、履歴情報と組み合わせて保存しなければならない。(SHALL)

履歴が生じた日時には、サービスが履歴登録依頼を受け付けた日時などを用いる。(MAY)

履歴登録者を特定可能な情報には、履歴登録者の DATA-EX ID、電子証明書、デジタル署名などを用いてよい。(MAY)

来歴管理拡張サービスは、保存する履歴情報について、電子署名などを用いて改ざん対策を講じなければならない。(SHALL)

来歴管理拡張サービスは、加工履歴登録依頼に対し、加工後の DDP ID と DDP 作成時の履歴 ID、加工者の DATA-EX ID、データセット取得元の DDP ID と DDP 受信時の履歴 ID、加工種別、加工詳細情報を属性として持つ加工履歴情報を保存できなければならない。(SHALL)

来歴管理拡張サービスは、加工来歴情報提供依頼に対し、指定された DDP の加工来歴を依頼者に提供しなければならない。(SHALL)

13. ガバナンス

DATA-EX は分野間のデータを広く活用し、「新たな価値を創出する」ことを目的としている。DATA-EX におけるステークホルダーが上記の目的を果たすために必要となる指針や運用プロセス、その体制をガバナンスとして定める。ガバナンスは「ポリシー」「契約」「ガバナンス推進における役割」の要素からなり、詳細はそれぞれの節にて説明する。

DATA-EX でのガバナンスは次に説明する「データガバナンス」と「DATA-EX ガバナンス」の2つの要素から構成される。データを取り扱う際に一般的に考慮すべきガバナンスを「データガバナンス」と呼称し、これとは区別して DATA-EX として考慮すべきガバナンスを「DATA-EX ガバナンス」と定義する。

データガバナンス

「AI・データの利用に関する契約ガイドライン」ではデータの特徴は以下のように示されている。

データは無体物であり、民法上、所有権や占有権、用益物権、担保物権の対象とはならないため、所有権や占有権の概念に基づいてデータに係る権利の有無を定めることはできない(民法 206 条、同法 85 条参照)。そして、知的財産権として保護される場合や、不正競争防止法上の営業秘密として法的に保護される場合は、後記第 3-2-(2)で述べるように限定的であることから、データの保護は原則として利害関係者間の契約を通じて図られることになる。

ここで明示されるように現行法ではデータには知的財産権や営業秘密の場合を除いて、所有権が認められず、データの保護を法的権利によって行うことができない。そのため、同ガイドラインではデータ保護や利用目的をコントロールする権利について、利害関係者間で利用権利を取り決める契約を交わすことを推奨している。

本仕様書ではデータの利用権を同ガイドラインの「当該契約当事者が他の当事者に対して、データの利用権限を主張することができる債権的な地位」を定義として用いる。また、DATA-EX においてデータの利用権やその目的に対してデータの利用をコントロールする権利は契約当事者である DATA-EX 参加者が持ち、データ管理も DATA-EX 参加者にゆだねられることを前提とする。

DATA-EX におけるデータ(DDP)の関与者には「被観測者」「DATA-EX 参加者(提供者)」「DATA-EX 運営事業者」「DATA-EX 参加者(受領者)」「DATA-EX 支援サービス事業者」が存在する。データ利用の権利を持つのは、DATA-EX 参加者の「提供者」側であり、「DATA-EX 運営事業者」はデータの権利を持たない仲介者である。そのため、利用に際してのデータ利用の範囲や責任は当事者間の個別の契約にて定め、そのガバナンスの責任も DATA-EX 参加者が負うものである。また、DATA-EX 運営事業者においても DATA-EX 参加者の個人情報の取り扱いに関する責任を負う。

契約を伴わない公開情報の形式で提供を行う DATA-EX 参加者(提供者)は、データの公開に関して一定限度の責任を負う。データの信頼性を保証し、データの提供者としての情報開示を行うことと社会上の説明責任を負うことが DATA-EX において推奨される。

DATA-EX ガバナンス

DATA-EX に関してのガバナンスをここで定める。前提として DATA-EX は異なる分野間のデータを繋ぐ連邦型のシステムであり、DATA-EX 運営事業者はデータの保護を行わず、データの管理は各 DATA-EX 参加者にゆだねられる。そのため、データ授受を行う DATA-EX 参加者間で相互自律的にポリシーや契約に基づく対応が求められる。

契約に伴う対価を得る場合は、データ取引市場(DATA-EX 支援サービス提供者)の利用が推奨される。DATA-EX はデータ取引市場への接続を提供する。

ここで DATA-EX でのデータに関しての責任範囲を明確化する。データの管理は DATA-EX 参加者の責任で行い、交換するデータそのもののセキュリティについても DATA-EX 参加者が責任を負う。

DATA-EX は日本国内にて展開するサービスであり、国内法規制に従う。DATA-EX 運営事業者や DATA-EX 参加者、関連する全てのステークホルダーが法令遵守することを前提とする。別途、DATA-EX 参加者は利用規約にも従うことが求められる。DATA-EX 参加者は自らが影響を受ける法域の開示が求められ、データが国境を越えて流通する場合は、取引相手国と日本国のいずれの法令にも遵守することに留意が必要である。

13-1. ポリシー

「ポリシー」ではデータを取り扱うに際して、DATA-EX 参加者と DATA-EX 運営事業者が守るべき原則を提示する。前提として、DATA-EX は日本国内でのサービスのため、DATA-EX の全てのステークホルダーは国内一般法令に遵守する必要がある。データを取り扱うに際してのプライバシーの尊重、データ提供者の経営上の機微情報の尊重を目的とした DATA-EX の価値観や方針についてここで示す。DATA-EX 参加者は資料「利用契約書」を遵守する。また、DATA-EX 運営事業者は資料「プライバシー方針書」に則り、DATA-EX 参加者の個人情報を適切に取り扱い、DATA-EX における中立的な立場を堅持し、自身が定めた「公平性・透明性」の原則を遵守し、適切な DATA-EX の運営を行う。

13-1-1. DATA-EX 参加者が守るべきポリシー

DATA-EX は日本国内でのサービスのため、DATA-EX 参加者や DATA-EX 支援サービス事業者は国内一般法令に遵守する必要がある。特にデータの取り扱いに関しては、個人情報保護法や不正競争防止法などの法令を遵守する。

提供データに関しての責任は DATA-EX 参加者(提供)側が持つ。DATA-EX 運営事業者は参加者間で結ばれる契約には関わらず、DATA-EX 参加者がポリシーを遵守しているかの確認を行

うことはできない。

13-1-2. DATA-EX 運営事業者が守るべきポリシー

DATA-EX 運営事業者は健全なデータ連携サービスを行うために、自らが定めたポリシーを遵守する必要がある。DATA-EX 運営事業者が守るべきポリシーは DATA-EX 参加者の「個人情報（アカウント情報）の保護」と DATA-EX サービス利用における DATA-EX 参加者に対しての「公平性・透明性の確保」の 2 種類ある。それぞれを以下に示す。

DATA-EX 参加者は DATA-EX 利用時に入会の審査のために、DATA-EX 運営事業者への個人情報の提供が求められる。DATA-EX 運営事業者は個人情報の処理について、改正個人情報保護法に対応したプライバシーポリシー（個人情報保護方針）に則り慎重な取扱いを行う。DATA-EX のプライバシーポリシーに関しては資料「プライバシー方針書」を参照すること。

DATA-EX 上で不当な目的のためのデータの流通や不当な条件でのデータ流通が生じることを防止するために、DATA-EX 運営事業者・参加者は以下の公平性と透明性の原則を守る。

- DATA-EX 参加時の公平性・透明性

DATA-EX 運営事業者は、DATA-EX 参加者が DATA-EX に参加する際に特定参加者に不利益となるような不当な条件を課すことを行わず、DATA-EX 参加者間での公平性を担保する。参加条件や審査基準を明らかに、条件変更の際は必要に応じて事前説明と同意取得を行い、透明性を担保する。

- DATA-EX 利用時の公平性・透明性

DATA-EX 運営事業者は契約の管理を行わないため、DATA-EX 参加者同士が、データ取引時に公平性・透明性が担保されるよう努める必要がある。データ取引で特定の DATA-EX 参加者が有利となるやり取りが行われないように、DATA-EX 参加者間での契約時の取り決めの作成を通して取引の公平性や契約条件の透明性を担保する。

13-2. 契約

DATA-EX ではデータの利用の目的や範囲、責任は DATA-EX 参加者間の契約を通して図られる。「契約」ではデータに関する取り決めにおける DATA-EX 参加者間での契約においての推奨事項を示す。データの利用権を確保するために DATA-EX 参加者は取引において利用目的、期間、第三者提供範囲を定めることが必要である。具体的には「AI・データの利用に関する契約ガイドライン」のひな型を参考に契約を作成することを推奨する。その際、データのコントローラビリティをいかに確保するかに関して契約に定めることが望ましい。DATA-EX 参加者間の契約を、第三者による保証を必要とする場合はデータ取引市場の活用を推奨する。

13-3. ガバナンス推進における役割

DATA-EX 運営事業者が DATA-EX のポリシーを遵守するためのガバナンスの推進体制における役割を以下に示す。

-
- ・ DATA-EX 運営事業者
 - 内部監査
 - ◇ DATA-EX の組織、運営、管理その他法人に関する一切の事項の決議をする役割を持つ。
 - ◇ DATA-EX の業務・財産の状況を調査し、理事の職務の執行を監査する役割を持つ。
 - ◇ DATA-EX の業務上の意思決定に参画し、業務執行を指導監督する役割を持つ。
 - ◇ DATA-EX におけるプロセス・ルールの策定・監視を行う役割を持つ。
 - システム運用・保守
 - ◇ プロセス・ルールに基づき業務を執行する役割を持つ。
 - 業務運用
 - ◇ プロセス・ルールに基づき業務を執行する役割を持つ。
 - ・ DATA-EX 参加者
 - ◇ DATA-EX 申請時の利用規約を遵守する役割を持つ。
 - ・ DATA-EX 支援サービス提供者
 - ◇ DATA-EX 申請時の利用規約を遵守する役割を持つ。

14. 国際連携

14-1. 国際連携の概要

DATA-EX は国際的なデータ連携の検討を進め、全世界のデータ流通を加速・拡大し、様々な情報が連携することにより、日本や世界各国の産業や社会の発展を目指す。DATA-EX は、国内の分野間データ連携基盤になるとともに、GAIA-X 等の国際的なデータ連携基盤との相互運用を見据え、海外の主要団体とも議論を重ね、社会実装を進める。

上記のビジョンを実現するためには、ナショナルセキュリティや各国の法律への適応等の観点から、DATA-EX は他国と対等な主権を保った上で、他国のデータ連携基盤との相互連携が必要である。しかしながら、各国データ連携基盤のルールが異なる他、異なるデータ経済圏を繋ぐ共通のルールもなく、国際的な相互連携が困難である。そこで、国際連携の将来像と当面的な対応策について、本技術仕様書では記載する。

14-2. 国際連携の課題と将来像

前述に示した異なるデータ経済圏を跨いだ国際的なデータ連携の課題について以下に示す。現状では、各データ経済圏が採用する分野間データ連携サービスの標準仕様や実装系の技術機能群が異なる他、トラストやガバナンスもデータ経済圏により違いがあり、データ経済圏を越えたクロスドメインのデータ連携が困難である。中でも、データ経済圏を跨いで、連携相手のアクセス先や利用可能な通信プロトコル等を識別し、参加者間でネゴシエーションを行うシステム的な手段が存在しない。

前述の課題を踏まえ、国際的なデータ連携を実現する将来像を以下に記す。はじめに、異なるデータ経済圏の分野間データ連携サービスが存在し、それぞれのデータ経済圏内では、それぞれのルールの基で運用されることを相互に認め合うことが必要である。更に、異なるデータ経済圏のアクセス先やオブジェクトを一意に識別可能とし、相互に通信を可能とする最低限必要となる国際共通のルールが必要となる。そして、分野間データ連携サービスの標準仕様、実装系の技術機能群、トラスト等の各レイヤーの要素は各レイヤーで繋がる必要がある。これらの要件を満たすことにより、互いのデータ経済圏におけるデータ所有者の意思を尊重し、公平性・透明性を確保した安心・安全なデータ流通を基に、双方のガバナンスの存在を認め合いながら連携することを目指す。

14-3. 国際連携のトラスト

前述に示した国際連携の将来像を目指すうえで、データ経済圏間におけるトラストの互換性確保を図っていくことが重要となる。とりわけ、参加者のトラストは、データカタログ、データセット、契約書など他リソースのトラストに与える影響が大きいことから、最も重要である。データ経済圏間における参加者のトラストについて、現状を踏まえたロードマップを図 65 に示す。

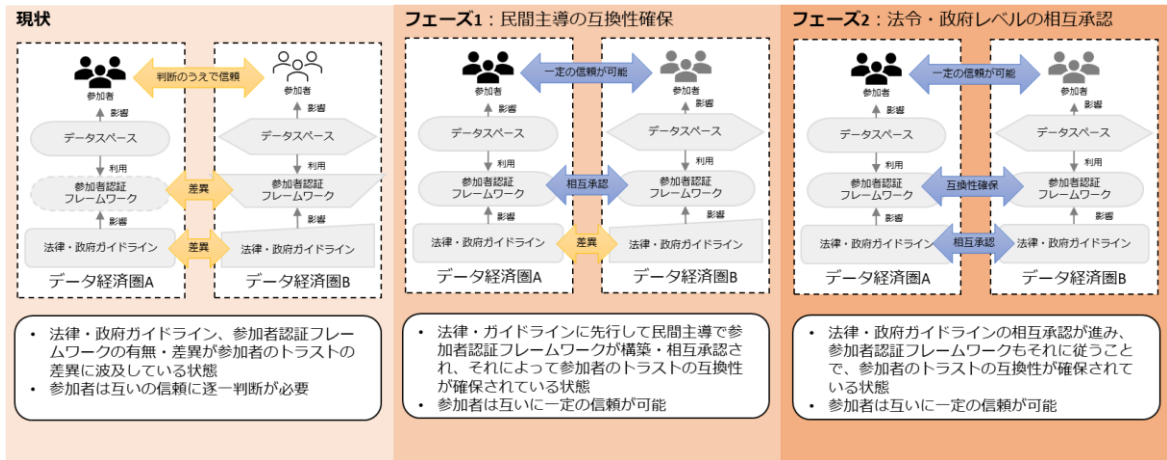


図 65: 参加者の信頼の相互性確保に向けたロードマップ

現状、データスペースは参加者認証フレームワークにより、または独自に参加者の信頼を確保している。参加者認証フレームワークは法律・政府ガイドラインの影響を受けるが、各データ経済圏の法律・政府ガイドラインは相互承認されておらず、内容・整備状況に差異がある。この差異が参加者認証フレームワークの有無・差異に繋がり、さらには参加者の信頼の差異に繋がっている。この現状に対し、データ経済圏間の法律・政府ガイドラインの相互承認には時間を要することから、参加者認証フレームワークの相互承認を先行させる形態（フェーズ 1）が想定される。フェーズ 1 の期間、参加者認証フレームワークは最新の法律・政府ガイドラインへの追従を継続的に行う。法律・政府ガイドラインの相互承認が完了したとき、最終形態であるフェーズ 2 に移行する。

本ロードマップを踏まえ、DATA-EX は現状のフェーズを認識し、最新の参加者認証フレームワークへの対応を行っていく必要がある。また、DATA-EX 運営事業者は、この対応に伴いシステムに変更が発生することを認識し、適切に運営する必要がある。

14-4. 国際連携のコネクタ間連携

国際連携におけるコネクタ間連携のマイルストーン図 66 に示す。「国際連携の課題と将来像」に示した各レイヤー間の連携が困難である課題より、現状においては、DATA-EX 参加者が海外のデータを利用する際は、連携先の分野間データ連携サービスに加入し、複数の仕様を使い分ける必要がある。将来は、国際標準仕様を策定の基、双方を尊重した相互連携を理想とする。しかしながら、仕様の共通化は他国との協議に時間を要するため、Step1として、インターフェイスの共通化を実施し、DATA-EX 参加者視点において仕様差異を隠蔽することにより、DATA-EX 参加者が一律の手順でデータ共有を実施可能とする。

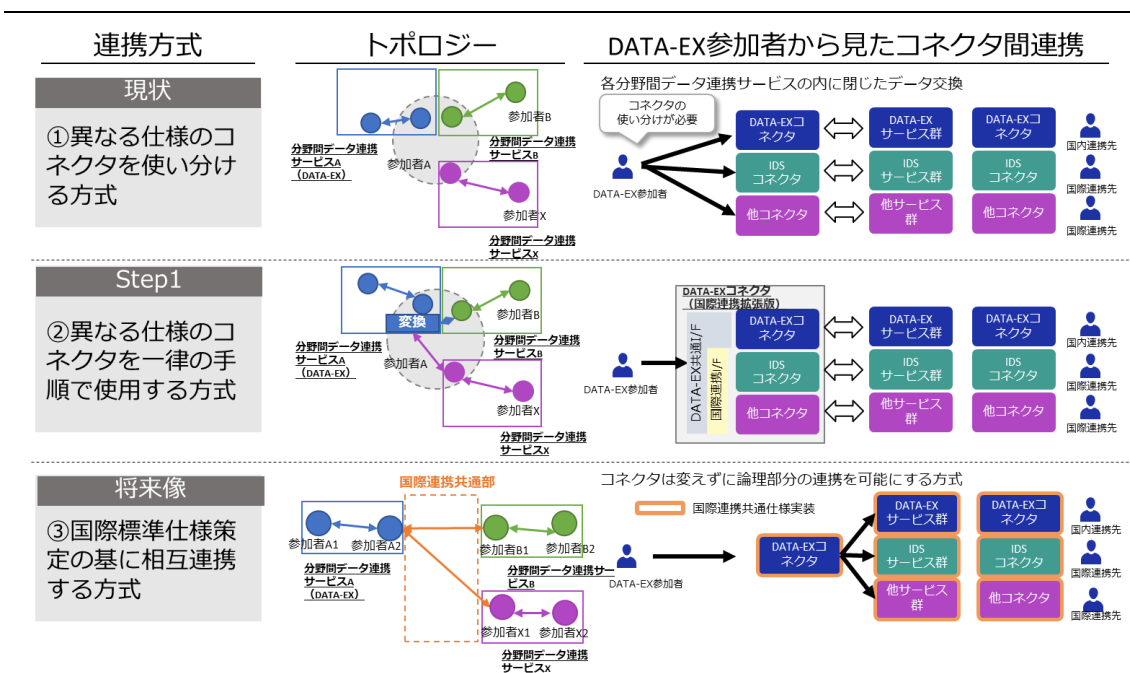


図 66:コネクタ間連携のマイルストーン

14-5. 国際連携のコネクタ間連携:共通 I/F 方式の例

14-5-1. 国際連携の概念モデル

コネクタ間連携のマイルストーンにおける Step1 の説明を記す。Step1 として、インターフェイスの共通化を実施し、利用者視点において仕様差異を隠蔽することにより、利用者が一律の手順でデータ連携を実施可能とする。

- トポロジー: DATA-EX 参加者が連携したい先の分野間データ連携サービスのアカウントを持ち、データ交換したい国際連携先の仕様へ変換し、国際連携先のメンバーとして、データ交換を実施する。

図 67 に示すように、DATA-EX に所属する参加者 A は、異なる仕様の分野間データ連携サービス B (欧州想定) と分野間データ連携サービス X (日本・欧州以外の他国のデータスペースを想定) と連携をする際は、分野間データ連携サービス B と分野間データ連携サービス X にも参画し、アカウントを持ち、国際連携先の分野間データ連携サービス内でデータ交換を実施する。

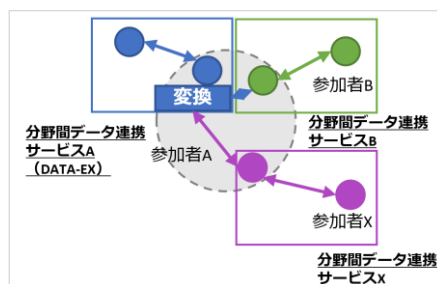


図 67: Step1 のトポロジー図

- ・ DATA-EX 参加者から見たコネクタ間連携

図 68 に示す DATA-EX コネクタ(国際連携拡張版)には、複数の分野間データ連携サービスのコネクタと、異なるインターフェイス仕様を変換する機能を内部に実装する。これにより、DATA-EX 参加者視点では、仕様を使い分けることなく、DATA-EX のインターフェイスのみを使用し、内部で仕様変換が処理された後に、内包されている国際連携先のコネクタを通じて、異なる分野間データ連携サービスの利用者とのデータ交換が可能になる。

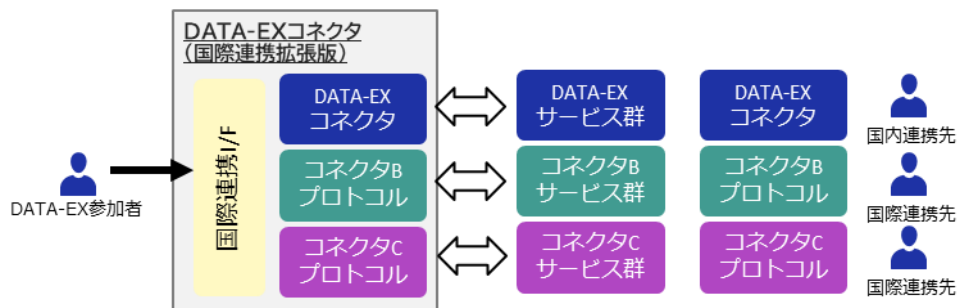


図 68: DATA-EX のデータ受領者の視点から見たコネクタ連携の概念図
(データ受領(DATA-EX 参加者)／データ提供(国際連携先))

- ・ 課題
 - ・ DATA-EX 参加者は、国際連携先の仕様に依存し、国際連携先の利用者としてデータ交換が行われるため、相手先のルールやポリシーに準拠する必要があるため、DATA-EX 側のポリシーは考慮されない。
 - ・ DATA-EX 参加者が他の分野間データ連携サービスとデータ交換をする際に、DATA-EX 側の認証ポリシーに基づいた認証認可ができない。
 - ・ トラストの確保において、国際で一律に共有にすべき要素と個別にするべき要素を決める必要がある。

実装面においては、コネクタの種類が増えると、実装されたコネクタの数だけメンテナンス作業が必要になる。

14-5-2. 国際連携のコネクタ・アーキテクチャ

国際連携機能は将来的なあるべき姿を目指しながらも、並行して STEP1 で示す方式のコネクタ・アーキテクチャを検討する。ここで、コネクタ・アーキテクチャとは、国際連携機能を実現するために必要な構成要素の全体像(概要)を示すものとする。以下、データ受領(DATA-EX 参加者)／データ提供(国際連携先)、ならびにデータ受領(国際連携先)／データ提供(DATA-EX 参加者)それぞれについて、コネクタ・アーキテクチャを示す。

14-5-2-1. データ受領(DATA-EX 参加者)／データ提供(国際連携先)のケース

図 69 に、DATA-EX 参加者が国際連携先からデータを受領する際のコネクタ・アーキテクチャを示す。DATA-EX 参加者(データ受領)が持つ分野間データ連携サービス内に、DATA-EX データ交換機能に加え、国際連携先が持つコネクタプロトコルを 1 つ以上内包し、DATA-EX 参加者(データ受領)の要求に応じて、国際連携インタフェース(以下、「I/F」とする)が適切な国際連携先のコネクタプロトコルに振り分けを行う。このとき、DATA-EX 参加者(データ受領)は、国内に閉じたデータ受領手順と同様のインタフェース(DATA-EX 共通 I/F)を用い、国内連携先からデータを受領できるようにする。

以下に、図 69 の①～⑤に示すデータ授受の一連の流れを示す。

- ① DATA-EX 参加者(データ受領)は、DATA-EX による国内へのデータ取得要求時と同一の I/F(DATA-EX 共通 I/F)を通じて操作を行い、各コネクタが持つ既存の手段でデータを発見し、国際連携先へデータ取得リクエストを送信する。
- ② DATA-EX 運営事業者が提供する分野間データ連携サービス、及び DATA-EX 支援サービスは、①のリクエストに応じたサービスを提供する(認証、来歴管理等)。
- ③ DATA-EX 参加者(データ受領)が持つ分野間データ連携サービスは、国際連携 I/F によりデータ取得リクエストに適合するコネクタプロトコルを選択する。
- ④ 選択されたプロトコルから、当該コネクタが提供する関連サービスへアクセスし、必要な認証手続きなどを得る。ここで、「関連サービス」は、DATA-EX 運営事業者が提供する分野間データ連携サービス、及び DATA-EX 支援サービスに相当するサービスとする。
- ⑤ 国際連携先のデータ提供者は、④を経て受領したデータ取得リクエストを確認し、必要な認可設定を行い、DATA-EX 参加者(データ受領)へデータを提供する。

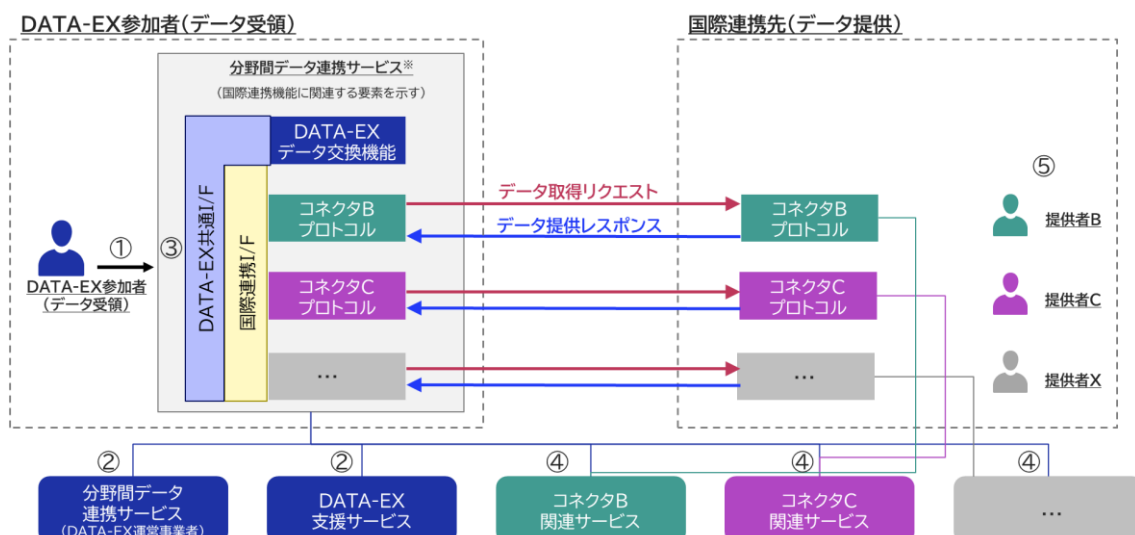


図 69: 国際連携のコネクタ・アーキテクチャ
(データ受領(DATA-EX 参加者)／データ提供(国際連携先))

14-5-2-2. データ受領(国際連携先)／データ提供(DATA-EX 参加者)のケース

次に、図 70 へ DATA-EX 参加者が国際連携先にデータを提供する際のコネクタ・アーキテクチャを示す。コネクタ・アーキテクチャの構成、並びに STEP1 の前提条件は図 69 と同様であり、国際連携先のデータ取得リクエストに応じて、DATA-EX 参加者(データ提供)が持つ分野間データ連携サービス内の国際連携 I/F が、データ提供のために必要な情報等の変換などを行う。

以下に、図 70 の①～④に示すデータ授受の一連の流れを示す。

- ① 国際連携先(データ受領)は、各々が持つコネクタプロトコルを用いたデータ取得要求時と同一の I/F を通じて、各コネクタが持つ既存の手段でデータを発見し、DATA-EX 参加者(データ提供)が持つ分野間データ連携サービス内の対向となるコネクタプロトコルへデータ取得リクエストを送信する。
- ② 国際連携先(データ受領)の関連サービスは、①のリクエストに応じたサービスを提供する(認証、来歴管理等)。
- ③ DATA-EX 参加者(データ提供)が持つ分野間データ連携サービスの国際連携先 I/F は、同サービス内の国際連携先コネクタを追経由して受領したデータ取得リクエストを参照し、DATA-EX 参加者(データ受領)が国内へのデータ提供と同様の操作で国際連携先へデータを提供できるよう、必要な変換処理を行う。
- ④ DATA-EX 参加者(データ提供)は、③を経て受領したデータ取得リクエストを確認し、必要な認可設定を行い、国際連携先(データ受領)へデータを提供する。このとき、DATA-EX による国内へのデータ取得要求時と同一の I/F (DATA-EX 共通 I/F) を通じて操作を行う。

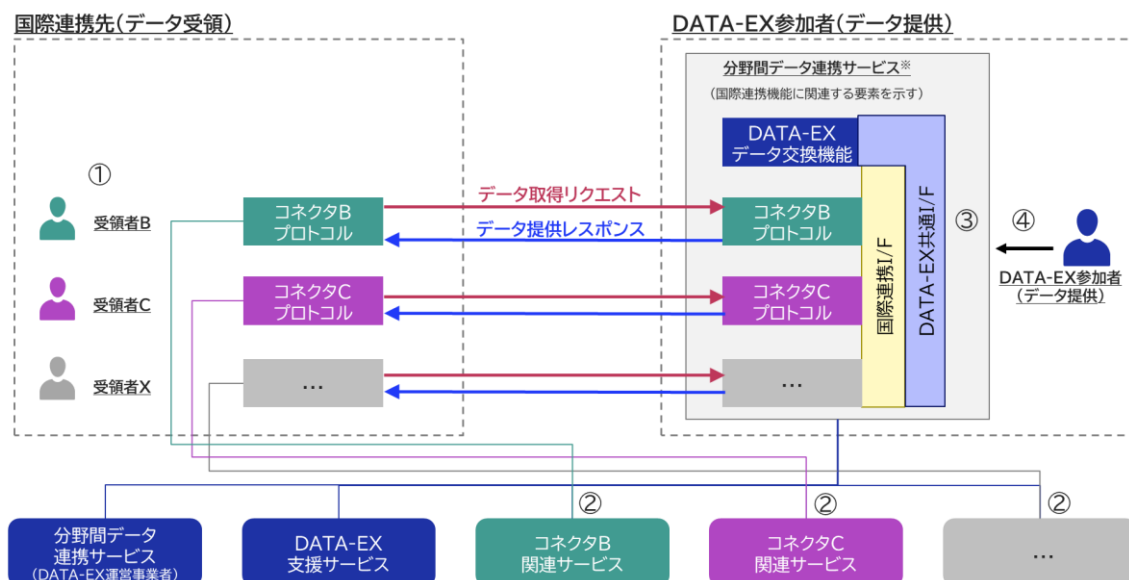


図 70: 国際連携のコネクタ・アーキテクチャ
(データ受領(国際連携先)／データ提供(DATA-EX 参加者))

14-5-3. 国際連携のコネクタ技術仕様

本章では、14-5-2.に示す国際連携のコネクタ・アーキテクチャに必要な国際連携機能への要求事項を示す。

- ・ 必須事項
 - DATA-EX 参加者（データ受領、データ提供）が持つ分野間データ連携サービスの国際連携機能は、1 つ以上の国際連携先コネクタプロトコルを利用したデータ授受を可能にする。
 - DATA-EX 参加者（データ受領、データ提供）が持つ分野間データ連携サービスの国際連携機能は、国際連携 I/F を備え、DATA-EX 参加者（データ受領、データ提供）が国内向けのデータ授受と同じ I/F による操作で国際連携先とのデータの授受を可能にする。
 - 国際連携 I/F は、DATA-EX 参加者（データ受領）及び国際連携先（データ受領）からのデータ取得リクエストに対し、リクエスト先が国内（DATA-EX データ交換機能）であるか、国際連携先（国際連携先コネクタプロトコル）であるかを、識別できる。
 - DATA-EX 参加者（データ受領）からのデータ取得リクエストに対し、リクエスト先の特定の国際連携先コネクタプロトコルを識別できる。

14-6. 将来像の国際連携機能について

DATA-EX は、国内の分野を超えたデータ連携を推進するとともに、GAIA-X 等の国際的なデータ連携推進団体との相互運用を見据えた社会実装を目指す。DSA と GAIA-X 等の国際的なデータ連携推進団体は、データ主権を確立し、トラストを保ったデータの相互連携を目指す、という共通の思想を基に、国際的なデータ連携の実現方法の検討を進めている。将来像の国際連携については、国際標準化を推進するための IOFDS (International Open Forum on Data Society) を共同設置し、国際的なデータ連携を推進する関係機関と議論を重ねていくとともに、IEEE SASB (Standard Association Standard Board)、ISO/IEC/JTC1、CEN/CENELEC などの国際標準化団体による活動とも協調を行う。なお、IOFDS では、参加する関係機関とデータスペースの定義を検討し、以下の通り合意している。

“Data Space” is a decentralized ecosystem with common policy and rules defined by a governance framework that enables secure and trustworthy data transactions between participants while supporting trust and data sovereignty.

これらの活動を通して、DATA-EX が最新の国際標準化と連動する取り組みが今後も推進される。

15. 今後の展望

本技術仕様書では、DATA-EX のアーキテクチャの各種定義及び、各ステークホルダーの役割を読者が理解する為に必要な解説を記載した。ただし、本技術仕様書に記載していないサービスや機能についても技術的な検証を続けており、今後技術仕様書が更新される可能性がある。特に国際的なデータ流通との連携については、DATA-EX における実装を目指しているものの本技術仕様書公開時点で実現方法が定まっていないため、今後も在り方の検討を続ける必要がある。

この文書について

- 名称 DATA-EX 分野間データ連携基盤技術仕様
- ファイル名 DATA-EX-Technological-specification-document.pdf
- 掲載 URL <https://data-society-alliance.org/data-ex/techspecs-v1>
- 概要

本技術仕様書は、DATA-EX 参加者や DATA-EX 運営事業者、その他ステークホルダー (DATA-EX 支援サービス提供者等) を対象読者とし、それぞれのステークホルダー間の円滑・安全な情報共有・連携を図ることを目的に、DATA-EX のアーキテクチャの各種定義及び、各ステークホルダーの役割を読者が理解する為に必要な解説を記載しています。特に、データ連携基盤としての技術的な概念モデルや運用モデルを記載し、詳細なテクノロジーやベンダー、開発者やシステムには依存しないものと位置付けています。これらを本技術仕様書にて定義する事により、現時点での DATA-EX のステークホルダーや機能に関する用語・コンセプトの統一・明確化を行っています。更に、本技術仕様書は、今後の議論点、詳細、実装のための基礎的な情報や定義としての活用方法も想定されます。

DATA-EX は分野間データ連携に関わるステークホルダーが安心・安全に交流できる環境の構築を支援します。これらの交流には真正性確認、トラストメカニズム、データ活用のルール設定と言った、様々なコンプライアンス原則があると考えられます。そのため、DATA-EX におけるデータ連携の各ステークホルダーに必須・任意とされる行動を本技術仕様書では記載しています。なお、今後、DATA-EX が分野間データ連携の基盤として発展する中で、分野間データ連携のビジネス要件、データ連携に関する行政側のガバナンス、技術的進化や革新に応じて、本技術仕様書の更新がなされることが想定されます。

- 基本情報
 - DSA 基準文書区分 技術基準仕様書
 - 作成者 一般社団法人データ社会推進協議会 4011005007414
 - 公開者 一般社団法人データ社会推進協議会 4011005007414
 - 著作権者 一般社団法人データ社会推進協議会 4011005007414
 - 発行日 2025 年 4 月 23 日
 - 公開日 2025 年 5 月 29 日
 - 作成アプリケーション Microsoft Word
 - 公開形式 PDF
 - ページ数 225 ページ
- 利用条件
 - 本書を利用したこと、利用しなかったことにより直接または間接に生じた損害に対して、DSA は一切の責任を負いません。
 - 本書を組織や団体として活用される際は、DSA へご一報いただければ幸いです。

本書に関するお問い合わせ

一般社団法人データ社会推進協議会(DSA) 4011005007414

E-mail dsa-office@data-society-alliance.org

ホームページ <https://data-society-alliance.org/contact/>