TDPF
Tokyo Data Platform

東京データプラットフォーム
データ連携基盤　要件定義書（初版）

令和４年３月　東京都

目次

第1章　概要

1　背景・目的

東京都（以下「都」という。）では、令和元年度 4 月に設置した「『Society 5.0』社会実装モデルのあり方検討会」での議論を踏まえて、令和 2 年 2 月には基本方針を公表し、データプラットフォーム構築に向けた取組を推進している。データプラットフォームの構築に向け、令和 2 年度、有識者等で構成される「官民連携データプラットフォーム運営に向けた準備会」（以下「準備会」という。）を設置し、議論を行った。令和 3 年度についても、名称を「官民連携データプラットフォーム」から「東京データプラットフォーム」（以下「TDPF」という。）に改めるとともに、準備会の検討結果を踏まえ、「東京データプラットフォーム協議会」（以下「TDPF 協議会」という。）を設置し、TDPF の注力分野やサービス内容等について、推進会議で議論を進めているところである。

TDPF の一つの事業である「データ流通推進」のうち、「データライブラリ」、「データ流通プラットフォーム」の業務を担う中核システムのことを「データ連携基盤」と呼び、今後設立を予定している TDPF 運営組織が主体となってシステム実装を行う予定である。

データ連携基盤では、API を通じた民間企業や大学・研究機関、行政機関等が保有する様々なデータの提供や国及び関連団体から展開されている外部のプラットフォームとの相互運用性の確保等により、データ提供者と利用者との間での柔軟かつ効率的なデータ連携・流通を実現し、官民の組織や分野を横断したデータ利活用の取組を促進する。

本要件定義書では、データ連携基盤の実装に向けて、令和 3 年度 TDPF 協議会第 3 回推進会議で定めた「大きなデータベースは作らない」、「リーンスタートと拡張性」、「トラストの確保」という 3 つのコンセプトの下、データ連携基盤に求められる業務要件及びシステム要件の検討を行い、その結果を初版として取りまとめたものである。今後は令和 4 年度に TDPF 関連事業からのフィードバック及び国や関連団体の動向を踏まえて改版し、TDPF 運営組織設立後の速やかなシステム構築につなげる。

全ての人が快適に暮らし働くことができる「スマート東京」の実現に向け、官民のデータを流通させ、データを活用し様々なサービスを創出できる環境を構築することで、イノベーション創出、社会的課題の解決を後押しし、都政の QOS（Quality of Service）を高め、都民の QOL(Quality of Life)を向上させることを目的とする。

2 用語の定義

本要件定義書における用語の定義は、次のとおりである。

表 1-1 用語の定義

項番	用語	内容
1	Society 5.0	サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会のこと。
2	東京データプラットフォーム（TDPF）	「スマート東京（東京版 Society 5.0）の実現に向けたデータプラットフォーム構築の基本方針（令和２年２月）」に定められた都が提唱するデータプラットフォームのこと。
3	データ連携基盤	TDPF が扱う「データ流通推進」事業のうち、「データライブラリ」、「データ流通プラットフォーム」の業務を担う中核システムのこと。
4	TDPF 運営組織	TDPF を運営する組織のこと。 社会経済状況や国の動向等を踏まえながら、適切な時期に設立することを予定している。
5	登録者	データ連携基盤の利用者のうち、入会登録申請を行い登録が完了した利用者のこと。
6	データ提供者	登録者のうち、データ連携基盤にデータを提供・登録する者のこと。
7	データ利用者	登録者のうち、データ連携基盤を流通するデータを自らのサービス・製品等への活用や、地域課題解決のために利活用する者のこと。
8	組織	民間企業、大学・研究機関及び行政機関等の団体のこと。
9	オープンデータ	国、地方公共団体及び事業者が保有する官民データのうち、国民誰もがインターネット等を通じて容易に利用（加工、編集、再配布等）できるよう、次のいずれの項目にも該当する形で公開されたデータのこと。 ①営利目的、非営利目的を問わず二次利用可能なルールが適用されたもの ②機械判読に適したもの ③無償で利用できるもの
10	シェアードデータ	国、地方公共団体及び事業者が保有する官民データのうち、定められた利用条件下で利用（加工、編集、再配布等）できるよう、次のいずれの項目にも該当する形で公開されたデータのこと。 ①データにより利用条件が定められているもの ②機械判読に適したもの

項番	用語	内容
11	PF	プラットフォームの略称。 サービス、システム及びソフトウェアを提供・カスタマイズ・運営するために必要な共通の基盤となる標準環境のこと。
12	相互運用先	データ連携基盤と相互運用するプラットフォームのこと。
13	カタログ	データ連携基盤上のデータや外部データにアクセスするためのリンク情報に対する概要情報（メタデータ等）を整理し、一覧にしたもの。
14	API	Application Programming Interface の略称。 あるコンピュータプログラム（ソフトウェア）の機能や管理するデータ等を、外部の他のプログラムから呼び出して利用するためのインタフェースのこと。
15	ロール	利用者のグループのこと。 利用者の種類（個人ユーザ、組織管理ユーザ及び組織ユーザ等）に対応するロールを作成し、各利用者はそれぞれのロールに所属する。
16	個別提供契約	データ提供者が TDPF にオープンデータ及びシェアードデータの提供を行う場合に、TDPF 運営組織と締結する個別契約のこと。
17	個別利用契約	データ利用者が TDPF のシェアードデータを利用する場合に、 TDPF 運営組織と締結する個別契約のこと。
18	利用規約	TDPF 運営組織が定める TDPF のサービス利用に関する入会登録に関する権利義務等を定めた規約（東京データプラットフォーム規約）。入会登録を申請する際は、この規約に準拠することに同意することが申請の条件となる。 令和 4 年 3 月現在、ポリシー案の改訂事業において、ポリシー案 1.1 として策定されている。

3　TDPF の取組とデータ連携基盤の概略

データの流通を推進するためには、データ連携基盤の構築に加えて多角的な取組が必要である。TDPF の取組は基盤構築を含め、表 1-2 及び図 1-1 で示す取組及び事業で構成される。

表 1-2 TDPF の取組

項番	取組	関連する事業とその概要
1	コミュニティ構築	「TDPF 協議会」 TDPF の注力分野やサービス内容等を検討するとともに、利用者とのネットワーキングやコミュニティを構築
2	ユースケース創出	「ケーススタディ事業」及び「TDPF 協議会のワーキンググループ」 TDPF を利活用する民間企業の掘り起こしや、ユースケースの創出
3	データ整備	「データ整備モデル」 データ利活用の促進に向け、行政機関が保有するデータを機械判読可能な形式へ整備する手法のモデル化 （令和 4 年度、事業範囲を行政機関と民間企業に拡大予定）
4	ポリシー整備	「ポリシー案の改訂」 データのガバナンスを築き、適切な情報の取扱いとデータの利活用促進の両立を推進
5	基盤構築	「データ連携基盤構築」 本要件定義書の範囲。「データライブラリ」、「データ流通プラットフォーム」の業務を担うデータ連携基盤の要件定義を実施

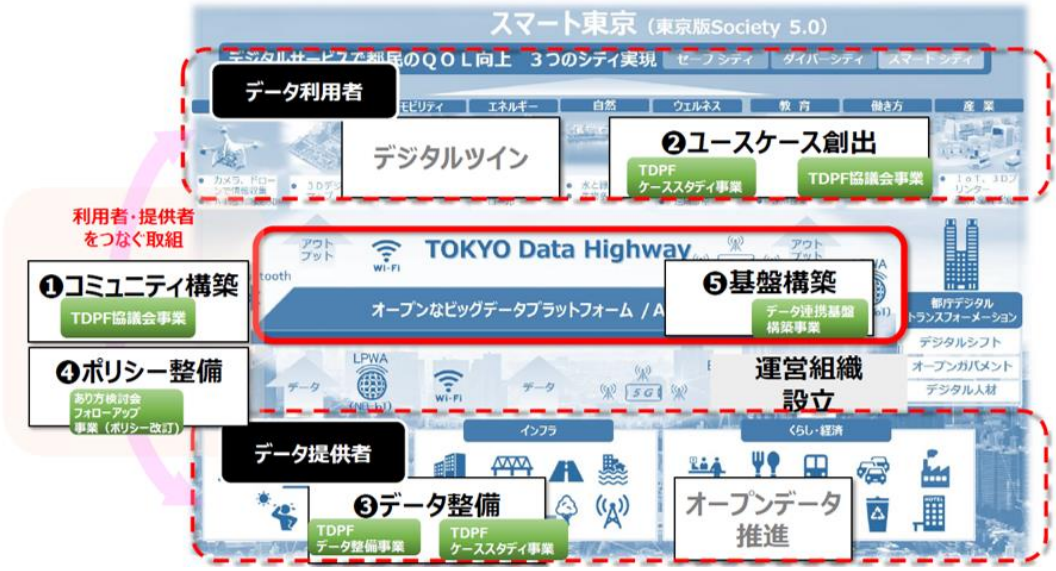

図 1-1 TDPF の取組の概略図

出典：東京データプラットフォーム協議会　第 3 回推進会議　事務局資料 3

データ連携基盤は都の推進するデジタルツイン実現プロジェクト、オープンデータ推進並びに国及び関連団体で検討・運用されている他の PF と、API 等の共通ルールに基づき、データ連携及び相互運用を実現するものとする。これにより、各システム、各サービス及び PF 内で個別に保有しているデータの流通を促進し、データ利用者及び提供者に対し、データ利活用が進めやすい仕組みを提供することで、データを通した社会的課題の解決に繋げる。

※本要件定義書は図の赤枠である「データ連携基盤構築事業」が対象であり、その他の事業は本要件定義書の対象外となる。

第2章　業務要件

データ連携基盤は、大学・研究機関、民間企業及び都、区市町村及び国等の行政機関等のオープンデータ、シェアードデータをデータ提供者、データ利用者が幅広い場面でデータ利活用することが期待される。ここでは、データ連携基盤の創成期として、短期的に実現が期待される業務要件を整理する。

1　利用者

データ連携基盤の利用者を表 2-1 に定義する。

なお、利用規約で示される「登録者」は利用者の分類の内、「個人」及び「組織」を対象とする。

表 2-1 利用者の定義

項番	利用者の分類	利用者	内容
1	非会員	非会員ユーザ	入会登録していない個人として TDPF のポータルサイトにアクセスし、オープンデータ及び利用者ポータルサイトの一部機能を利用する者
2	個人	個人ユーザ	個人として入会登録し、データ連携基盤の各種機能を利用する者
3	組織	組織ユーザ	民間企業、大学・研究機関及び行政機関等の団体として入会登録を実施し、データ連携基盤の各種機能を利用する者
4		組織管理ユーザ	当該組織内での管理権限を持ち、組織ユーザの登録等の業務を行う者
5	TDPF 運営組織	運用ユーザ	TDPF 運営組織の運営者としてデータ連携基盤を運用・管理する者
6		運用管理ユーザ	TDPF 運営組織内での管理権限を持ち、運用ユーザの登録等の業務を行う者

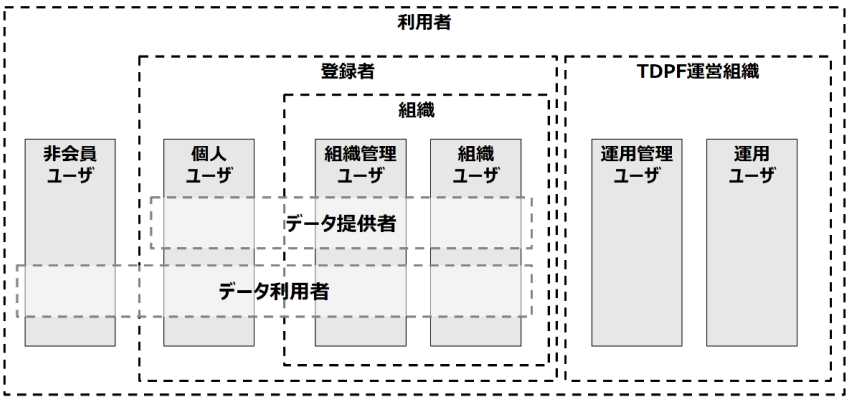

図 2-1 利用者のイメージ

2 業務一覧

データ連携基盤は以下に示すとおり、利用者との接点となるポータルサイト、登録者のアカウントを一元的に管理する機能、データ連携基盤で扱うデータの管理機能、分野や組織の壁を越えてデータ連携を行うための相互運用機能及びデータ利用動向の確認やシステム運用のための共通機能を有する。

表 2-2 業務一覧

項番	業務	説明
1	ポータル	利用者がポータルサイトを通して、入会登録申請、データ提供・利用、認証、データ連携基盤についての情報収集、問合せ及びコミュニティでの意見交換等を実施する。
2	アカウント管理	登録者のアカウントを一元的に管理する業務。アカウント管理は登録者を特定する ID の関連付け、認証・認可情報及び属性情報の管理並びに登録者のライフサイクル管理（登録、登録拒絶、任意退会、強制退会、利用停止、利用停止解除及び削除）を行う。 ・ 個人ユーザは入会登録申請時に多要素認証による本人確認によってアカウントが発行される。 ・ 組織管理ユーザは組織として入会登録申請を実施し、TDPF 運営組織の審査を経て、アカウントが発行される。 ・ 組織ユーザは組織として登録完了後に「入会登録申請を組織管理ユーザへ行う」または「組織管理ユーザからの招待」により、承認手続きを経て登録される。
3	データ管理	データ連携基盤に保存・蓄積するオープンデータ、シェアードデータの管理及び連携先のシステムに分散されたデータの仲介を行う。 データ提供者はデータ提供申請・データ登録を、データ利用者はデータ利用申請・データ利用（検索・参照及び取得）を行う。運用ユーザはデータ提供申請・データ利用申請を確認し、承諾をする。
4	相互運用	データ連携基盤及び相互運用先の PF 間での提供する機能（オープン API 等）を利用し合うことで、データの相互運用を行う。
5	共通	利用者はデータ連携基盤の扱う利用動向等の統計情報を閲覧することができる。 運用ユーザはシステム改善のための分析情報の確認、システム連携のためのインタフェースの確認及びシステム運用等の共通業務がある。

(1)ポータル

データ連携基盤では、データ提供及びデータ利用を行う利用者向けの利用者ポータルサイト、データ利活用を活発化するための利用ガイド及び API の評価環境等を備えた開発者ポータルサイト、双方向にコミュニケーションが可能な情報交換の場を提供するためのコミュニティポータルサイト及び TDPF 運営組織が情報配信並びにアカウント及びデータ管理等のサービス運用を行う運用者ポータルサイトを提供する。

データ連携基盤が提供する 4 つのポータルサイトの業務概要を以下に示す。なお、各ポータルサイトで認証情報を共有し、いずれかのポータルサイトに認証されている場合、再認証は不要とする。

表 2-3 各ポータルサイトの業務概要

項番	ポータルサイト	業務概要
1	利用者ポータルサイト	データ連携基盤の利用者を対象として、データの提供・利用関連機能、サイト利用ガイド、ランキング表示及び問合せフォーム等を提供する。
2	開発者ポータルサイト	データ連携基盤の登録者のうち開発者を対象として、基盤情報、利用ガイド、API の評価環境及び問合せフォーム等を提供する。
3	コミュニティポータルサイト	民間企業、大学・研究機関、都民及び行政機関等の利用者を対象として、双方向にコミュニケーションが可能な情報交換の場を提供する。
4	運用者ポータルサイト	運用管理ユーザ・運用ユーザを対象として、各ポータルサイトへのコンテンツ配信、お知らせ情報配信、アカウント管理及びデータ管理等を行う管理画面を提供する。

ア　利用者ポータルサイト

データ連携基盤の利用者全般が利用するポータルサイトであり、入会登録申請、データ連携基盤の利用ガイド等の閲覧及びデータの提供・利用等を利用者ポータルサイトで実施する。

表 2-4 利用者ポータルサイトの業務一覧

○：実施対象、△：オープンデータのみ実施対象、－：対象外

項番	業務	内容	非会員	個人	組織	TDPF運営組織
1	認証	資格情報（ID、パスワード等）を用いてログインする。	－	○	○	○
2	情報収集	利用ガイド、お知らせ及び FAQ 等のデータ連携基盤に関する情報を参照する。	○	○	○	○
3	問合せ	データ連携基盤に関する問合せ及び問合せに対する回答の確認をする。	－	○	○	○
4	アカウント管理	入会登録申請を行う。（(2)アカウント管理を参照）	○	－	－	－
5	データ管理	データの提供・利用を行う。（(3)データ管理を参照）	△	○	○	○
6	相互運用	他の PF 等との相互運用に必要なデータの提供・利用を行う。（(4)相互運用を参照）	－	○	○	○
7	共通	データ利用動向を確認する。（(5)共通を参照）	○	○	○	○

イ　開発者ポータルサイト

データ連携基盤の登録者のうち、API を使用してデータ提供・利用する開発者を対象としたポータルサイトであり、開発支援情報等の閲覧及び API 評価を開発者ポータルサイトで実施する。

開発者ポータルサイトの業務内容を以下に示す。

表 2-5 開発者ポータルサイトの業務一覧

○：実施対象、－：対象外

項番	業務	内容	非会員	個人	組織	TDPF 運営組織
1	認証	資格情報（ID、パスワード等）を用いてログインをする。	－	○	○	○
2	情報収集	開発支援情報（API 及びデータの検索・仕様の開示等）、参考情報（サンプルコード等）及び FAQ 等を参照する。	○	○	○	○
3	API 評価	データ連携基盤の API を評価可能な環境へアクセスし、API の試行をする。	－	○	○	○

ウ　コミュニティポータルサイト

コミュニティポータルサイトは、データ連携基盤の利用者（民間企業、大学・研究機関、都民及び行政機関等）が利用者間及び TDPF 運営組織とつながり、データ利活用について、双方向に活発な意見交換の場を提供するためのポータルサイトである。

コミュニティポータルサイトの業務内容を以下に示す。

表 2-6 コミュニティポータルサイトの業務一覧

○：実施対象、△：参照のみ実施対象、－：対象外

項番	業務	内容	非会員	個人	組織	TDPF 運営組織
1	認証	資格情報（ID、パスワード等）を用いてログインをする。	－	○	○	○
2	意見交換	民間企業、大学・研究機関、都民及び行政機関等の利用者を対象として、双方向に意見交換及びコミュニティ管理（コミュニティの作成、検索及び削除等）を行う。	△	○	○	○

エ　運用者ポータルサイト

TDPF 運営組織の運用管理ユーザ及び運用ユーザが利用するポータルサイトであり、入会登録の申請、データの提供・利用等の承諾、各ポータルサイトへのコンテンツ配信及びお知らせ情報配信等を運用者ポータルサイトで実施する。

運用者ポータルサイトの業務内容を以下に示す。

表 2-7 運用者ポータルサイトの業務一覧

○：実施対象、－：対象外

項番	業務	内容	非会員	個人	組織	TDPF 運営組織
1	認証	資格情報（ID、パスワード等）を用いてログインをする。	－	－	－	○
2	問合せ管理	データ連携基盤に関する問合せに対して回答する。 データ利用者からの提供データに関する問合せ（提供データの不備、カタログ情報の設定不備及びリンク切れ等）に対してデータ提供者へ連絡し、修正を促す。	－	－	－	○
3	コンテンツ管理	利用ガイド、お知らせ、FAQ、開発支援情報（利用規約、開発ガイド等）及び参考情報（サンプルコード等）等のデータ連携基盤に関するコンテンツを配信する。	－	－	－	○
4	アカウント管理	入会登録申請の承諾／拒絶を行う。（(2)アカウント管理を参照）	－	－	－	○
5	データ管理	データの提供・利用の承諾及びデータ利用に伴う対価の清算処理とその確認を行う。 （(3)データ管理を参照）	－	－	－	○
6	相互運用	他の PF 等との相互運用に必要なデータの提供・利用の承諾を行う。 （(4)相互運用を参照）	－	－	－	○
7	共通	データ利用動向を確認する。 （(5)共通を参照）	－	－	－	○

(2)アカウント管理

データ連携基盤の登録者のアカウントを一元的に管理する業務である。

アカウント管理は、登録者を特定する ID に関連付け、認証・認可情報及び属性情報の管理並びに表 2-8 に示す登録者のライフサイクル管理を行う。

データ連携基盤のアカウントは、未登録・利用・利用停止・退会の 4 つの状態で遷移する。

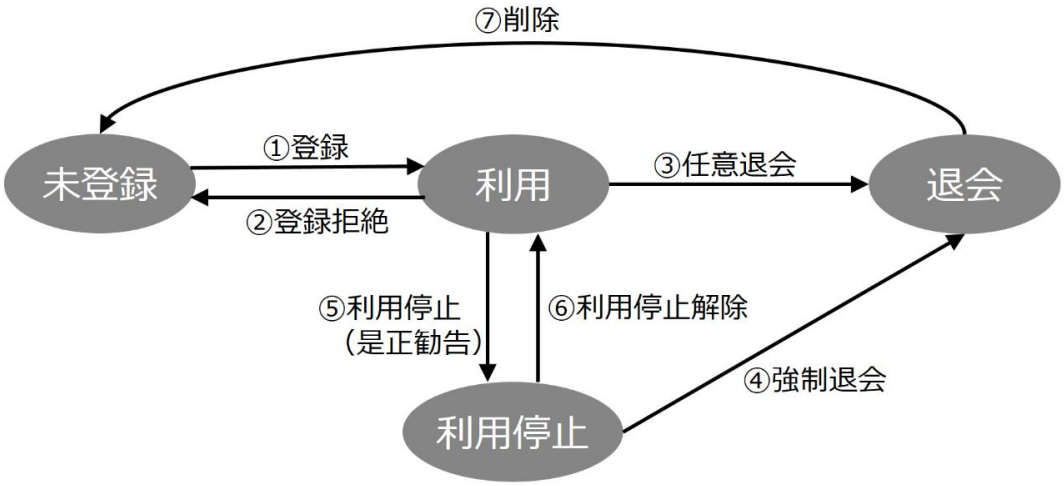

図 2-2 アカウントの状態遷移図

表 2-8 アカウントの遷移一覧

項番	遷移	状態遷移の契機
1	登録	非会員が入会登録申請を行う。
2	登録拒絶	申請内容の不備等により運用ユーザが登録拒絶を行う。
3	任意退会	登録者が任意退会申請を行う。
4	強制退会	利用規約に定める強制退会の事由に該当する場合、または利用規約に定める義務に違反したことにより、是正勧告後一定期間を過ぎた場合に運用ユーザが強制退会を行う。
5	利用停止 （是正勧告）	以下の場合に利用停止（是正勧告）となる。 ・ 登録者による利用規約の違反があった場合 ・ 認証失敗によるアカウントロック及び長期間の未利用の場合 ・ 組織ユーザからの操作又は申請があった場合 ・ セキュリティ事故等 TDPF 側の事情による緊急対応が行われる場合
6	利用停止解除	利用停止中の登録者から停止解除申請を受け、運用ユーザが承諾する。
7	削除	退会後一定期間が経過した場合 （アカウント情報の物理削除が行われる） ※強制退会の場合、再登録拒否のため 3 年間は情報を保持する。

ア　個人ユーザ

個人ユーザは、利用者ポータルサイトから利用規約の同意及び入会登録申請を実施し、多要素認証により本人性を確認することで TDPF 運営組織からの通知を伴ってアカウントが登録される。ただし、この状態ではシェアードデータの利用等一部機能を制限する。本人確認書類による本人証明及び利用規約に定める必要な情報の審査により、権限変更し個人ユーザが利用可能なすべての機能が利用できるようになる。

個人ユーザに関するアカウント管理の業務内容を以下に示す。

図 2-3 個人ユーザのアカウント管理の業務フローイメージ

表 2-9 個人ユーザのアカウント管理の業務内容

○：実施対象、－：対象外

項番	業務	内容	個人ユーザ	運用ユーザ
1	入会登録申請	利用規約を遵守することに同意し、入会登録を申請する。	○	－
2		多要素認証による本人確認を行う。	○	－
3	アカウント情報変更	アカウント情報を変更する。	○	－
4	権限変更	本人確認書類による本人証明及び利用規約に定める必要な情報を提出する。	○	－
5		申請を承諾し、権限変更を行う。	－	○
6	利用停止（是正勧告）	利用規約に基づき、停止事由に該当する場合、利用を停止する。	－	○
7	利用停止解除	利用停止解除を申請する。	○	－
8		申請を承諾／拒絶する。	－	○
9	任意退会	任意退会をする。	○	－
10	強制退会	強制退会処理をする。	－	○

イ　組織

民間企業、大学・研究機関及び行政機関等の団体として入会登録を行う場合、組織単位で入会登録申請を行い、運用ユーザによる承諾後、TDPF 運営組織からの通知を伴って組織管理ユーザのアカウントが登録される。

組織及び組織管理ユーザに関するアカウント管理の業務内容を以下に示す。

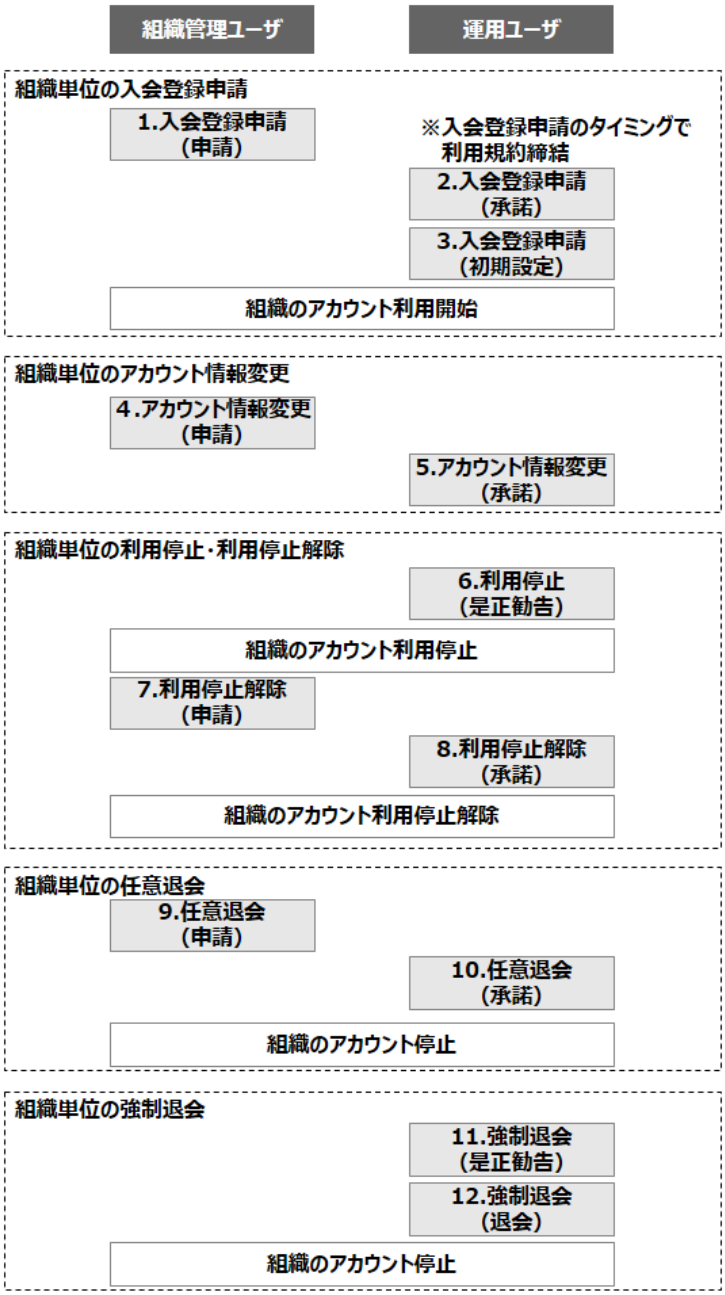

図 2-4 組織アカウント管理の業務フローイメージ

表 2-10 組織のアカウント管理の業務内容

○：実施対象、－：対象外

項番	業務	内容	組織管理ユーザ	運用ユーザ
1	入会登録申請	利用規約を遵守することに同意し、入会登録を申請する。	○	－
2		申請内容を審査し、承諾／拒絶する。	－	○
3		組織管理ユーザのアカウントを作成する。	－	○
4	アカウント情報変更	組織情報の変更を申請する。	○	－
5		申請を承諾／拒絶する。	－	○
6	利用停止（是正勧告）	組織の利用を停止する。	－	○
7	利用停止解除	組織の利用停止解除を申請する。	○	－
8		申請を承諾／拒絶する。	－	○
9	任意退会	組織として任意退会申請する。	○	－
10		組織管理ユーザ及び組織ユーザを削除する。	－	○
11	強制退会	組織へ是正勧告をする。	－	○
12		組織の強制退会処理をする。	－	○

ウ　組織管理ユーザ・組織ユーザ

上記（イ 組織）の入会登録完了後、当該組織に紐付く組織管理ユーザ及び組織ユーザのアカウントは、組織管理ユーザへの申請及び承諾をもって作成される。また、組織管理ユーザからの招待により作成することも可能とするが詳細は次工程で検討する。

組織管理ユーザ及び組織ユーザに関するアカウント管理の業務内容を以下に示す。

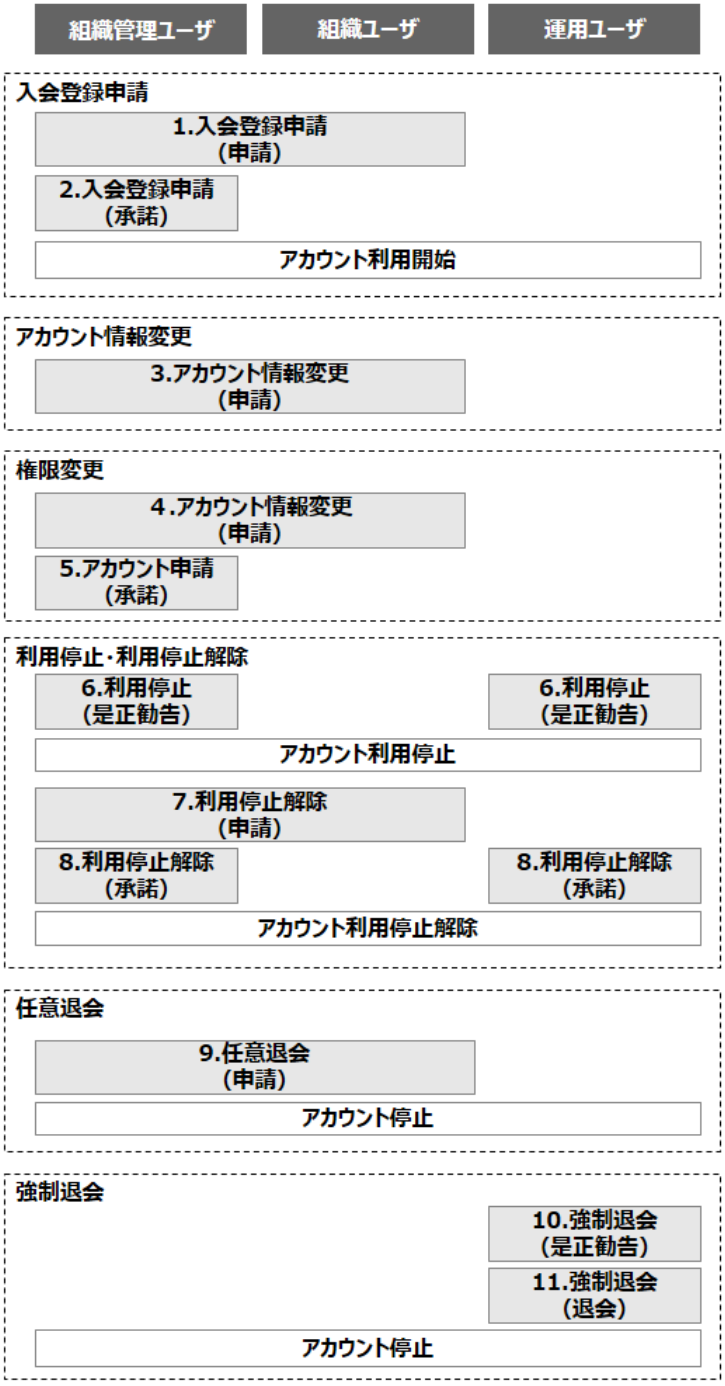

図 2-5 組織管理ユーザ・組織ユーザのアカウント管理の業務フローイメージ

表 2-11 組織管理ユーザ・組織ユーザのアカウント管理の業務内容

○：実施対象、－：対象外

項番	業務	内容	組織管理ユーザ	組織ユーザ	運用ユーザ
1	入会登録申請	入会登録を申請する。	○ ※1	○	－
2		申請を承諾／拒絶する。	○	－	－
3	アカウント情報変更	アカウント情報を変更する。	○	○	－
4	権限変更	権限変更（組織管理ユーザへの昇格または組織ユーザへの降格を含む）を申請する。	○	○	－
5		申請を承諾し、権限変更を行う。	○	－	－
6	利用停止（是正勧告）	組織管理ユーザ及び組織ユーザの利用を停止する。	○ ※2	－	○ ※3
7	利用停止解除	利用停止解除を申請する。	○	○	－
8		申請を承諾／拒絶する。	○ ※2	－	○ ※3
9	任意退会	任意退会をする。	○	○	－
10	強制退会	組織管理ユーザ及び組織ユーザへ是正勧告をする。	－	－	○
11		組織管理ユーザ及び組織ユーザの強制退会処理をする。	－	－	○

※1 組織の入会登録申請において作成された組織管理ユーザ以外を追加する場合

※2 組織管理ユーザが利用停止（是正勧告）した場合、組織管理ユーザが利用停止解除申請の承諾を行う。

※3 運用ユーザが利用停止（是正勧告）した場合、運用ユーザが利用停止解除申請の承諾を行う。

エ　運用管理ユーザ・運用ユーザ

TDPF 運営組織の運用管理ユーザ及び運用ユーザのアカウント管理は、運用管理ユーザの権限において行われる。

運用管理ユーザ及び運用ユーザに関するアカウント管理の業務内容を以下に示す。

表 2-12 運用管理ユーザ・運用ユーザに関するアカウント管理の業務内容

○：実施対象、－：対象外

項番	業務	内容	運用管理ユーザ	運用ユーザ
1	アカウント追加	運用ユーザを登録する。	○	－
2	アカウント情報変更	アカウント情報を変更する。	○	○
3	権限変更	権限変更（運用管理ユーザへの昇格または運用ユーザへの降格を含む）を申請する。	○	○
4		申請を承諾し、権限変更を行う。	○	－
5	利用停止（是正勧告）	組織管理ユーザ及び組織ユーザの利用を停止する。	○	－
6	利用停止解除	利用停止解除を申請する。	○	○
7		申請を承諾／拒絶する。	○	－
8	任意退会（アカウント削除）	離職及び異動等によりアカウントが不要になった場合に削除をする。	○	○
9	強制退会	運用管理ユーザ及び運用ユーザへ是正勧告をする。	○	－
10		運用管理ユーザ及び運用ユーザの強制退会処理をする。	○	－

(3)データ管理

データ連携基盤に保存、蓄積するオープンデータ・シェアードデータの管理及び連携システムに分散されたデータの仲介を行う業務である。データ提供及びデータ利用について、業務内容をそれぞれ示す。

ア　データ提供

データ提供者が保有しているデータを提供する場合の業務内容を以下に示す。データ提供は、個別提供契約の締結後にデータが公開され、データ利用者によるデータ利活用が可能となる。

データ提供者は、データ連携基盤の利用者のうち、個人ユーザ、組織ユーザ及び組織管理ユーザを対象とする。

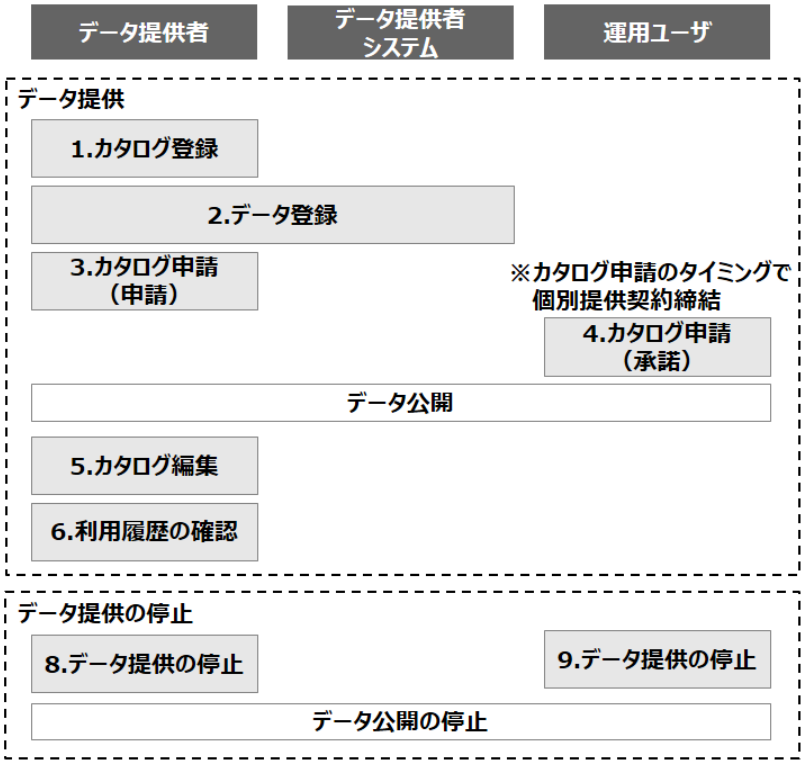

図 2-6 データ提供に関するデータ管理の業務フローイメージ

表 2-13 データ提供に関するデータ管理の業務内容

○：実施対象、－：対象外

項番	業務	内容	データ提供者	データ提供者システム	運用ユーザ
1	カタログ登録	カタログ情報（概要、インタフェース、メタデータ、利用条件及びデータ提供に対する対価等）を登録する。	○	－	－
2	データ登録	データ連携基盤が提供するポータルサイト又はデータ提供用 API を使用して、データ（リンク情報を含む）の登録を行う。	○	○	－
3	カタログ申請	個別提供契約の必要事項を入力し、データの提供を申請する。	○	－	－
4		申請内容を審査し、承諾する（承諾することで個別提供契約が締結される）。 登録データを確認後、データ利用者にカタログを公開する。	－	－	○ ※1
5	カタログ編集	カタログ情報の編集を行う。	○	－	－
6	利用履歴の確認	登録したカタログの利用履歴の確認を行う。	○	－	－
7	データ提供の停止	自身が登録したカタログの利用停止を行う。	○	－	－
8		カタログの利用停止を行う。	－	－	○

※1 当面の間、個人情報を含むパーソナルデータが含まれる場合、登録を拒否する。

イ　データ利用

データ連携基盤が保存・蓄積しているデータ及び連携システムに分散されているデータを利用する場合のオープンデータの利用及びシェアードデータの利用について、業務内容をそれぞれ示す。

(ｱ) オープンデータ

オープンデータとして登録されたデータの利用者は、非会員ユーザ、個人ユーザ、組織ユーザ及び組織管理ユーザを対象とする。

表 2-14 オープンデータ利用に関するデータ管理の業務内容

○：実施対象、－：対象外

項番	業務	内容	データ利用者	データ利用者システム	運用ユーザ
1	カタログ検索・参照	データ連携基盤に登録されているデータのカタログ情報を検索・参照する。	○	－	－
2	データ取得	データ連携基盤が提供するポータルサイト又はデータ取得用 API を使用して、データの取得を行う。	○	○	－
3	利用履歴の確認	データ利用者がカタログの利用履歴の確認を行う。	○ ※1	－	－

※1 非会員ユーザは、本データ管理業務は対象外。

(ｲ) シェアードデータ

シェアードデータを利用する場合、個別利用契約の締結後にデータの取得が可能となり、データ利用者によるデータ利活用が可能となる。

データ利用者は、組織ユーザ、組織管理ユーザ及び本人確認書類による本人証明及び利用規約に定める必要な情報の審査により承認された個人ユーザを対象とする。非会員ユーザ及び本人確認（多要素認証）のみの個人ユーザは、カタログ検索・参照のみ可能とする。

（本人確認及び本人証明に関しては、第４章　システム要件　1　機能要件　(3)認証を参照）

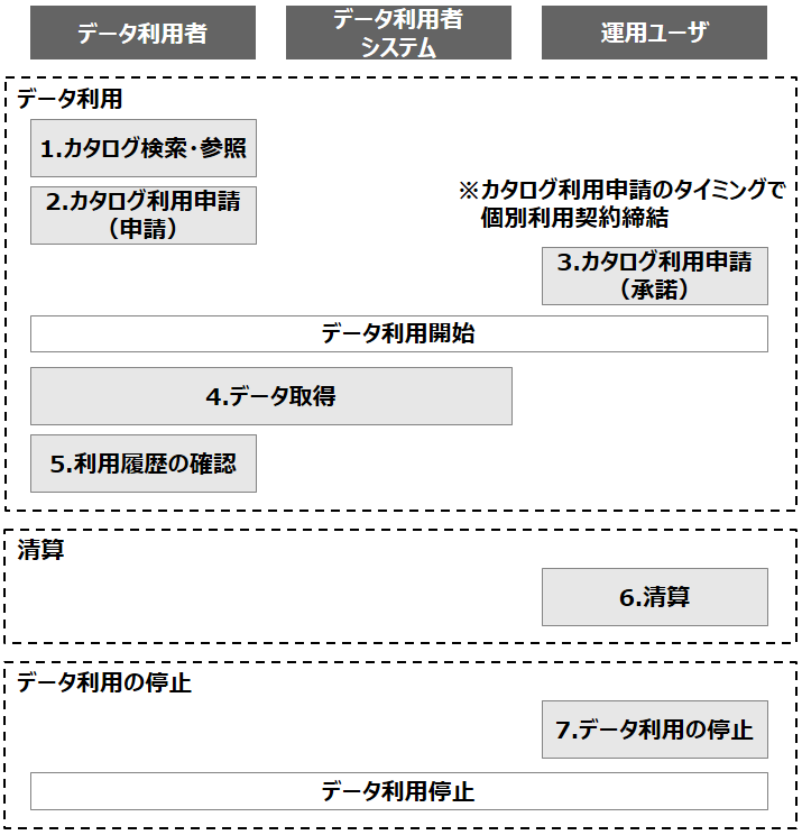

図 2-7 シェアードデータ利用に関するデータ管理の業務フローイメージ

表 2-15 シェアードデータ利用に関するデータ管理の業務内容

○：実施対象、－：対象外

項番	業務	内容	データ利用者	データ利用者システム	運用ユーザ
1	カタログ検索・参照	データ連携基盤に登録されているデータのカタログ情報を検索・参照する。	○	－	－
2	データ利用申請	個別利用契約の必要事項を入力し、データの利用を申請する。	○ ※1	－	－
3		申請内容を審査し、承諾する（承諾することで個別利用契約が締結される）。	－	－	○ ※2
4	データ取得	データ連携基盤が提供するポータルサイト又はデータ取得用 API を使用して、データの取得を行う。	○ ※1	○	－
5	利用履歴の確認	データ利用者がカタログの利用履歴の確認を行う。	○ ※1	－	－
6	清算	データ利用に伴う対価の清算処理とその確認を行う。	－	－	○
7	データ利用の停止	運用ユーザがデータ利用者のデータ利用を停止する。	－	－	○

※1 非会員ユーザ及び本人確認（多要素認証）のみの個人ユーザは本データ管理業務の対象外

※2 将来的には TDPF 運営組織が介在しない可能性がある。

(4)相互運用

データ連携基盤における相互運用とは、民間企業、国及び一般社団法人データ社会推進協議会等の関連団体並びに行政機関等の PF が提供する API やコネクタ等を活用することで、PF 間のデータ連携を可能とし、分野及び組織の壁を越えて様々なデータが流通される仕組みのことである。

具体的な要件については、令和 4 年度以降、個別のユースケース及び国や関連団体の動向を踏まえ継続検討する。

(5)共通

データ提供者・データ利用者に対して、データ利用を促進させるため、各カタログのダウンロードランキングや統計情報等を提供する。

また、運用ユーザに対して、システム改善のための分析情報、システム連携のためのインタフェース管理及びシステム運用等の共通業務を提供する。

表 2-16 共通の業務内容

○：実施対象、－：対象外

項番	業務	内容	データ提供者	データ利用者	運用ユーザ
1	可視化データの閲覧	各カタログの閲覧数及びダウンロード数並びにデータダウンロードランキング及び検索ワードランキングを閲覧する。	○	○	－
2	統計情報の確認	データ利用動向を確認する。	○	○	－
3		データ利用動向を確認し、システム改善をする。	－	－	○
4	分析情報の確認	利用者の利用動向（回遊分析等）からサービス向上施策に向けた改善をする。	－	－	○
5	インタフェース管理	相互運用先とのインタフェース管理（追加、変更及び削除）をする。	－	－	○
6	システム運用	パッチ適用及びシステム監視、システムの変更管理並びに構成管理及びインシデント管理等をする。	－	－	○

3 利用環境

データ連携基盤は、原則として 24 時間 365 日利用可能とする。また、ポータルの利用条件として、一般的に普及している OS 及び Web ブラウザを想定する。

表 2-17 データ連携基盤の利用環境

項番	項目	内容
1	利用時間	24 時間 365 日利用可能とする。ただし、保守・運用対応時間を除く。
2	ポータルの利用条件	・ Windows10 等の一般的に普及している OS で使用できること。 ・ Microsoft Edge、Google Chrome 等の一般的に普及している Web ブラウザで使用できること。 ・ プラグイン等の特別なソフトウェアのダウンロードを伴わないこと。 ・ 利用者の端末へのソフトウェアのインストールを行わずに利用ができること。

4 規模

データ連携基盤稼働当初の想定として、最低限以下の規模を許容するものとする。なお、利用規模の拡充により柔軟にスケールできるものとする。

表 2-18 データ連携基盤の規模

項番	項目	規模	内容
1	カタログ数	30 カタログ	データ連携基盤にデータ蓄積するカタログの数（リンク情報は含まない）。
2	保存データ容量	50GB	構造化データ、非構造化データを含む。
3	データ入出力性能	100pps かつ 100Kbps	ベストエフォートとする。
4	ページビュー数	26,000 ビュー/月	1 か月あたりのトップページのページビュー数。

第3章　　システム概要

1　機能構成

データ連携基盤は、サービス連携機能、アカウント管理に関する機能（認証）、データ管理に関する機能（外部データ連携、データマネジメント及びアセットマネジメント）、相互運用に関するPF間連携機能及びセキュリティ・運用に関する機能（共通）の機能群によって構成される。

データ連携基盤のシステム概要図を図 3-1 及び機能概要を表 3-1 に示す

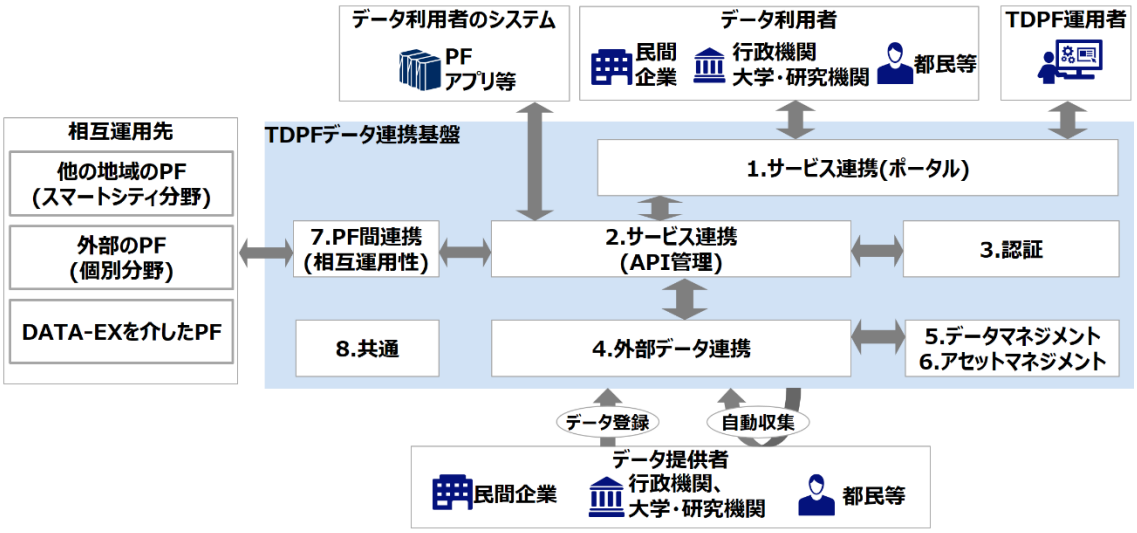

図 3-1 システム概要図

表 3-1 機能構成

項番	機能群	機能概要
1	サービス連携（ポータル）	データ連携基盤のポータルを提供する。 利用者間及び TDPF 運営組織との接点（ユーザインタフェース）を担う機能群となる。
2	サービス連携（API 管理）	データ連携基盤上で動作する各種サービスと連携する機能及び API を提供する。 マイクロサービスを API として管理する機能群であり、データ連携基盤の持つ機能を一元管理する。
3	認証	データ連携基盤の登録者及び連携システムに対して、認証を行う。
4	外部データ連携	連携システムとのインタフェースを管理し、データフォーマット及びプロトコルの差異を吸収する機能を提供する。 データ連携基盤の連携システムとの接続機能を担う機能群であり、連携システムが利用する API を提供する。 また、連携システムが提供するデータ取得用 API を利用してデータの連携を行う。
5	データマネジメント	データ連携基盤に登録するデータの管理及び連携システムに分散されたデータを仲介する機能を提供する。 登録データのほか、カタログ情報、個別提供契約情報及び個別利用契約情報等のデータ連携基盤のデータに関する情報を扱う機能が集約される。
6	アセットマネジメント	データ連携基盤と連携するシステムの連携情報及び接続状態の管理を行う。
7	PF 間連携（相互運用性）	相互運用先との認証連携及びデータ連携を行う。 様々な連携先システムが想定されることから、容易な接続のために多様なインタフェースに対応することが求められる機能群である。
8	共通	データ利活用の活性化を目的としてデータの可視化及び分析を行う機能を提供する。

2 連携システム

データ連携基盤と接続し、大学・研究機関、民間企業及び行政機関等が保有するシステム並びに相互運用を行う他の地域の PF、外部の PF 及び DATA-EX を介した PF と連携する。この連携にて様々なデータを流通させ、データ利活用の活性化を図るために連携が想定されるシステム及び PF を以下に示す。

表 3-2 連携システム

項番	連携システム		概要
1	データ提供者	大学・研究機関及び行政機関が保有するシステム	大学・研究機関及び行政機関が保有しているデータ（公共施設の情報、行政イベント及び地理空間等）を扱うシステム。保有しているデータにはオープンデータ及びシェアードデータがある。
2		民間企業が保有するシステム	交通や電力等の分野の事業者ごとに管理されているデータを扱うシステム。IoT センサー等のリアルタイムデータ（河川の水量データ及び混雑データ等）を提供する場合、API によりシステム間連携を行う。保有しているデータにはオープンデータ及びシェアードデータがある。
3	データ利用者	データ利用者のシステム（PF・アプリケーション等を含む）	データ利用者として、データ連携基盤の API を利用し、データ連携を行うシステム。
4	相互運用先	他の地域の PF（スマートシティ分野）	認証連携及び PF 間でデータ共有するための連携機能を持ち、各種機能及びデータを相互運用することのできる他の地域の PF。
5		外部の PF（個別分野）	認証連携や PF 間でデータ共有するための連携機能を持ち、各種機能やデータを相互運用することのできる個別分野の PF。
6		DATA-EX を介した PF	DATA-EX の仕様に準拠しデータの検索、提供及び利用ができ、利用条件及び来歴管理等の情報を交換できる PF。

3　ネットワーク

データ連携基盤への接続は、個人及び様々な組織が想定される。接続にはインターネット回線を利用することを前提とし、安全のため、通信には暗号化通信を行うためのプロトコルを使用する。 連携先システムのトラストを高めるため、相互運用先及びデータ提供者のシステムに対しては、接続元の制限を実施することにより、安全性を高めることとする。

また、外部からの不正なアクセスが発生しないように、データ連携基盤は外部のネットワークと切り離された専用のネットワーク内に構築する。

ネットワーク概要図を図 3-2、それぞれの接続に対するネットワークポリシーを表 3-3 に示す。

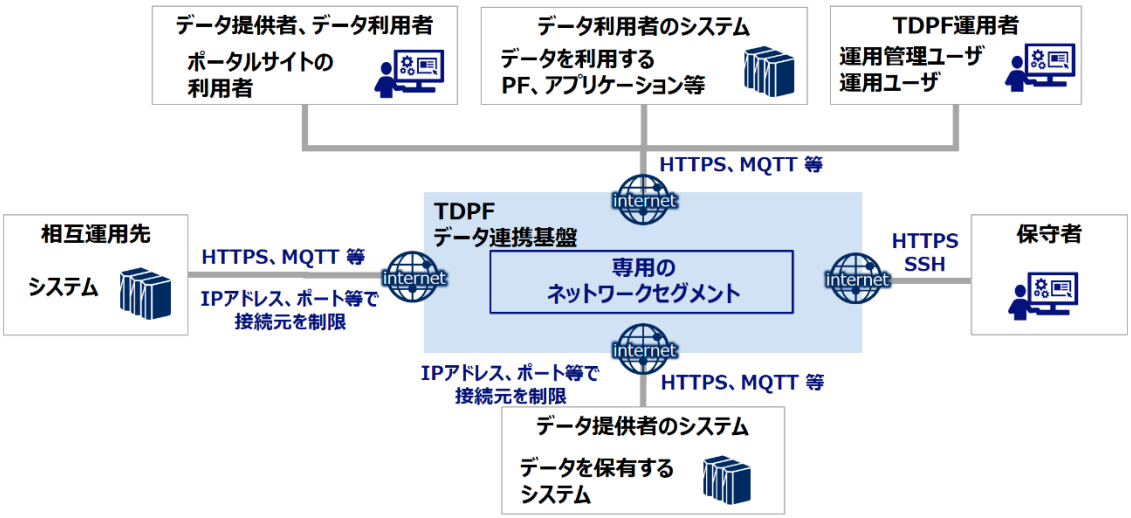

図 3-2 ネットワーク概要図

表 3-3 ネットワークポリシー

項番	ネットワーク	ポリシー
1	TDPF データ連携基盤	データ連携基盤の内部インタフェースは、専用のネットワークセグメントとする。 外部からデータ連携基盤にアクセスするため、インターネット回線に接続が可能なネットワーク環境を用意する。
2	データ提供者 データ利用者 TDPF 運用者	インターネット回線を利用する。 プロトコルは HTTPS を使用する。
3	データ利用者のシステム	インターネット回線を利用する。 プロトコルの HTTPS、MQTT 等を使用する。
4	データ提供者のシステム	インターネット回線を利用する。 プロトコルの HTTPS、MQTT 等を使用する。 セキュリティ上で必要な場合は接続元の IP アドレス及びポート番号による制限、並びに VPN 通信を利用した専用ネットワークを使用する。
5	相互運用先	インターネット回線を利用する。 プロトコルの HTTPS、MQTT 等を使用する。 セキュリティ上で必要な場合は接続元の IP アドレス及びポート番号による制限、並びに VPN 通信を利用した専用ネットワークを使用する。
6	保守者	インターネット回線を利用する。 プロトコルは HTTPS 及び SSH を使用する。

第4章　システム要件

1　機能要件

データ連携基盤はポータル、API 管理、認証、外部データ連携、データマネジメント、アセットマネジメント、PF 間連携及び共通の機能ブロックにより構成される。

機能ブロック間を疎結合にすることでリーンスタートと拡張性を実現するマイクロサービスアーキテクチャを採用する。

また、データ連携基盤の機能構成は、内閣府の「戦略的イノベーション創造プログラム（SIP）第 2 期／ビッグデータ・AI を活用した サイバー空間基盤技術のアーキテクチャ構築並びに実証研究事業」の成果である「スマートシティリファレンスアーキテクチャ ホワイトペーパー」を参照し、検討した。

データ連携基盤の実現にあたり、必要となる機能を本章に示す。

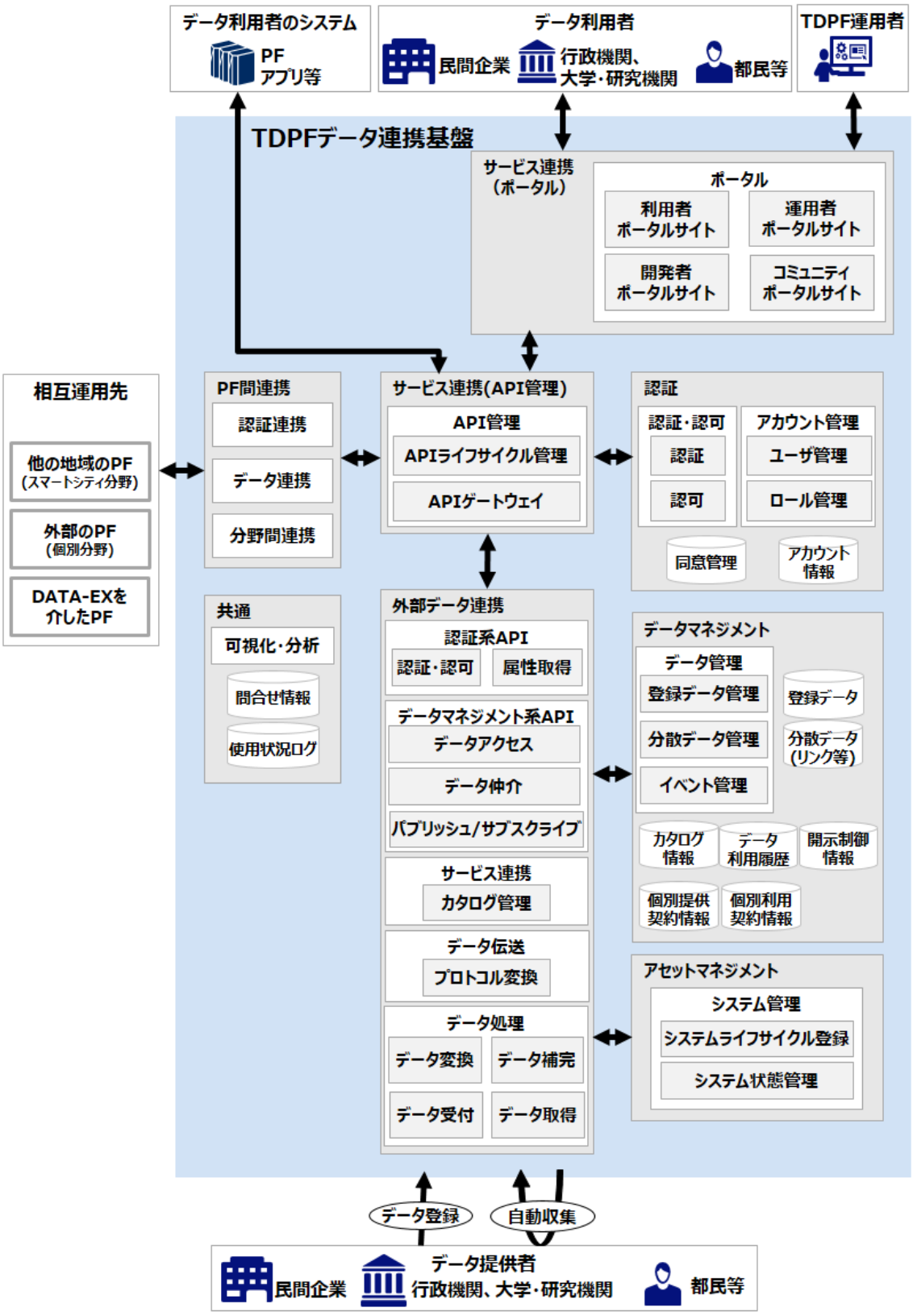
データ利用者のシステム
PF
アプリ等
データ利用者
民間企業
行政機関、
大学・研究機関
都民等
TDPF運用者
TDPFデータ連携基盤
サービス連携
（ポータル）
ポータル
利用者
ポータルサイト
運用者
ポータルサイト
開発者
ポータルサイト
コミュニティ
ポータルサイト
相互運用先
他の地域のPF
（スマートシティ分野）
外部のPF
（個別分野）
DATA-EXを
介したPF
PF間連携
認証連携
データ連携
分野間連携
サービス連携(API管理)
API管理
APIライフサイクル管理
APIゲートウェイ
認証
認証・認可
認証
認可
アカウント管理
ユーザ管理
ロール管理
同意管理
アカウント
情報
共通
可視化・分析
問合せ情報
使用状況ログ
外部データ連携
認証系API
認証・認可
属性取得
データマネジメント系API
データアクセス
データ仲介
パブリッシュ/サブスクライブ
サービス連携
カタログ管理
データ伝送
プロトコル変換
データ処理
データ変換
データ補完
データ受付
データ取得
データマネジメント
データ管理
登録データ管理
分散データ管理
イベント管理
登録データ
分散データ
(リンク等)
カタログ
情報
データ
利用履歴
開示制御
情報
個別提供
契約情報
個別利用
契約情報
アセットマネジメント
システム管理
システムライフサイクル登録
システム状態管理
データ登録
自動収集
データ提供者
民間企業
行政機関、大学・研究機関
都民等

図 4-1 機能構成図

表 4-1 機能一覧

項番	機能群	機能ブロック	機能名
1	サービス連携（ポータル）	ポータル	利用者ポータルサイト
			開発者ポータルサイト
			コミュニティポータルサイト
			運用者ポータルサイト
2	サービス連携（API）	API 管理	API ライフサイクル管理
			API ゲートウェイ
3	認証	認証・認可	認証
			認可
		アカウント管理	ユーザ管理
			ロール管理
4	外部データ連携	認証系 API	認証・認可
			属性取得
		データマネジメント系 API	データアクセス
			パブリッシュ/サブスクライブ
			データ仲介
		サービス連携	カタログ管理
		データ伝送	プロトコル変換
		データ処理	データ変換
			データ受付
			データ取得
			データ補完
5	データマネジメント	データ管理	登録データ管理
			分散データ管理
			イベント管理
6	アセットマネジメント	システム管理	システムライフサイクル登録
			システム状態管理
7	PF 間連携（相互運用性）	認証連携	認証連携
		データ連携	データ連携
		分野間連携	分野間データ検索
			分野間データ交換制御
			分野間データ交換記録
8	共通	可視化・分析	可視化・分析ダッシュボード

(1)サービス連携（ポータル）

データ連携基盤の提供するポータルサイトは、利用者向け及び TDPF 運営組織向けに分類される。

利用者向けは、データ連携基盤の各機能を利用する目的で利用者全般を対象とする「利用者ポータルサイト」、データ連携基盤にシステム接続を行い、データ提供・利用する目的の開発者を対象とする「開発者ポータルサイト」、課題解決やデータ利活用を目的とした利用者及び TDPF 運営組織が双方向に意見交換を行うための「コミュニティポータルサイト」が必要である。

また、TDPF 運営組織向けは、入会登録申請、データ提供・利用の各種申請に対する承諾及び利用者向けのコンテンツ配信、問合せ対応を行うための「運用者ポータルサイト」が必要である。

サービス連携（ポータル）機能群に関する要件の一覧を以下に示す。

表 4-2 サービス連携（ポータル）機能群の要件一覧

項番	機能ブロック	機能名	要件
1	ポータル	利用者ポータルサイト	入会登録申請を行うことができること。
			カタログ情報の登録、取得、検索及び削除ができること。
			データの提供・利用ができること。
			アクセス権限のないカタログ情報に対して開示要求ができること。
			利用ガイド、お知らせ及び FAQ 等のデータ連携基盤に関する情報を確認できること。
			データのダウンロード数や検索ワードのランキングを表示すること。
			利用したデータ、提供したデータの履歴を表示できること。
			利用データの更新情報（最終更新日等）を表示できること。
			データ連携基盤に関する問合せフォームを提供すること。
2		開発者ポータルサイト	開発者を対象とした開発支援情報（利用規約、開発ガイド、サンプルコード、活用事例、FAQ 等）を提供すること。
			開発者が開発した API の評価が可能な環境を提供すること。

項番	機能ブロック	機能名	要件
3		コミュニティポータルサイト	民間企業、大学・研究機関、都民及び行政機関等の利用者を対象として、双方向に意見交換やコミュニティ管理（コミュニティの作成や検索、削除等）ができること。
4		運用者ポータルサイト	データ連携基盤に関する問合せに対する回答ができること。
			各ポータルサイトへのコンテンツ及びお知らせ等の情報配信ができること。
			利用者のアカウント管理（申請に対する承諾等）ができること。
			運用管理ユーザ及び運用ユーザのアカウント管理（申請に対する承諾等）ができること。
			データ提供・利用に関するデータ管理（申請に対する承諾等）できること。
			清算業務のための情報を確認できること。

(2)サービス連携（API）

API 管理機能ブロックは、データ連携基盤でマイクロサービスとして実現する各機能が、API を介して利用することが前提となる。このとき、将来のデータ及び連携先の段階的拡大等に合わせ、API の追加や修正していく必要があるため、API のライフサイクルを管理するための API ライフサイクル管理機能が重要となる。

また、アクセス数や応答時間などを一元管理し、適切に制御するAPIゲートウェイとしての機能も必要となる。

このように、各マイクロサービスに求められるエンドポイント（API にアクセスするためのネットワーク上のアドレス）の管理、認証、モニタリング、アクセス制御といった機能を、API 管理機能として一元管理及び集約することで、システム全体における効率化を図る。

サービス連携（API）機能群に関する要件の一覧を以下に示す。

表 4-3 サービス連携（API）機能群の要件一覧

項番	機能ブロック	機能名	要件
1	API 管理	API ライフサイクル管理	データ連携基盤上の API のライフサイクル（登録、参照、変更及び削除）を管理する機能を提供すること。
2		API ゲートウェイ	API の輻輳制御（使用量制限やネットワーク速度制限等）機能を提供すること。
			データ連携基盤上に API のエンドポイントを提供し、データ利用者が API を利用できること。

(3)認証

都民、民間企業、大学・研究機関及び行政機関等がデータ提供・利用を安心して行うことができるように、データ提供者及びデータ利用者を審査し、信頼性を担保する。

そのため、データ連携基盤では登録者の信頼性担保を認証・認可により行い、適切にサービス提供を制御する必要がある。

認証機能群に関する要件の一覧を以下に示す。

表 4-4 認証機能群の要件一覧

項番	機能ブロック	機能名	要件
1	認証・認可	認証	「アカウント情報」に保存された資格情報（ID、パスワード等）を用いて登録者のアカウントを特定し、その真正性を証明できること。
			個人ユーザは多要素認証での本人確認により、入会登録できること。
			第三者利用を避けるために個人ユーザは、定期的に多要素認証を実施すること。
			個人ユーザは本人確認書類による本人証明を行うことができること。
			組織は運用ユーザによる書類審査の承認により、入会登録できること。
2		認可	「ユーザ管理」「ロール管理」と連携し、データ連携基盤の各種機能や管理するデータの利用範囲を許可、並びに制限できること。
3	アカウント管理	ユーザ管理	登録者を特定の ID（メールアドレス等）に関連づけ、認証情報（パスワード等）や属性情報（姓名及びメールアドレス等）の管理とアカウントのライフサイクル（登録、登録拒絶、任意退会、強制退会、利用停止、利用停止解除及び削除）を管理できること。
			データ連携基盤に入会登録を申請する場合に、利用規約の同意を得られること。 また、利用規約が変更となる時の同意管理及び任意退会時の注意事項についても同意を得られること。

項番	機能ブロック	機能名	要件
4		ロール管理	登録者が所属するグループ（個人ユーザ、組織管理ユーザ、組織ユーザ、運用管理ユーザ及び運用ユーザ）を定義するロールを管理できること。
			アカウント及びロール別にデータ連携基盤にアクセスする範囲や権限を定義する制御ポリシーを管理できること。

利用者の審査・認証を TDPF 運営組織が行う。
組織は、シェアードデータの利用を想定しているため、利用開始の時点で書類審査を必要とする。
一方、個人はデータ連携基盤への参加しやすさを考慮し、利用可能な機能は制限されるが、多要素認証による本人確認を実施すれば入会登録を可能とする。さらにその後、本人確認書類による本人証明及び書類審査を実施することで、組織同等の機能が利用できるものとする。
データ連携基盤への入会登録申請時の個人及び組織の信頼性確認は以下に示す。

表 4-5 信頼性確認

項番	利用者の分類	信頼性確認
1	個人	多要素認証による本人確認 本人確認書類による本人証明及び書類審査
2	組織	運用ユーザによる書類審査

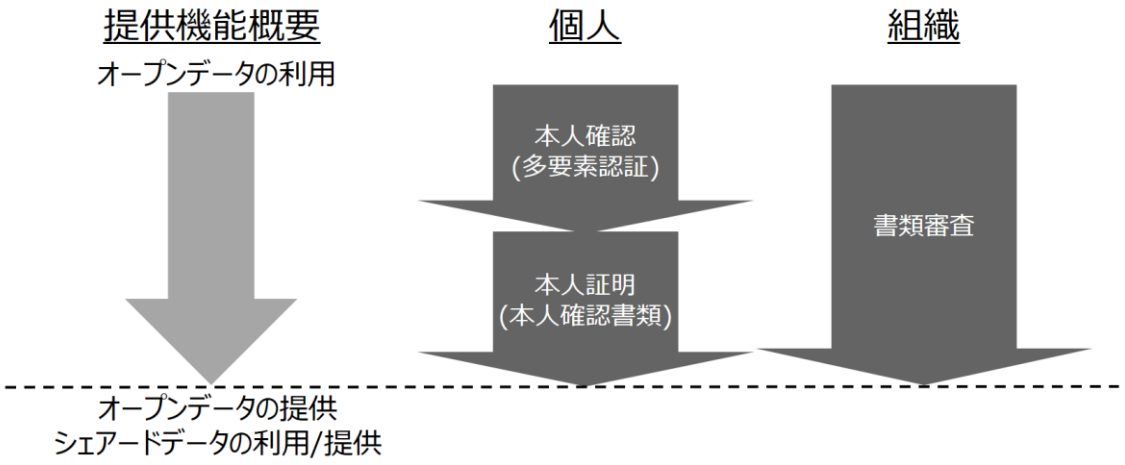

図 4-2 信頼性確認

(4)外部データ連携

外部データ連携では、大きく５つの機能ブロックを有する。

まず、外部システム向けにアカウント管理を行う機能として、認証系 API として提供し、サービス連携（ポータル）及び外部システム向けにデータ管理を行う機能として、データマネジメント系 API を提供する。これらの API 機能ブロックにより得られたデータをカタログ情報として管理するために、サービス連携機能がある。

また、外部の連携システムとの接続は、データ提供者の保有する既存のシステムであることが多く、多様なインタフェースを採用していることが多い。多様なインタフェースに対応するため、様々な接続方式に汎用的に対応できる仕組みが求められる。そのため、データ連携基盤として連携システムとのインタフェースを管理し、データ連携基盤の対応するデータフォーマット（推奨データセット等）、プロトコル差異を吸収する機能、データ処理機能及びデータ伝送機能を提供することも重要である。

外部データ連携機能群に関する要件の一覧を以下に示す。

表 4-6 外部データ連携機能群の要件一覧

項番	機能ブロック	機能名	要件
1	認証系 API	認証・認可	アカウント情報に保存された資格情報（ID、パスワード及び多要素認証等）を用いて資格情報の検証及びアクセストークンの払い出しや失効を実施できること。
			登録者の権限に応じ、利用範囲を制限できること。
2		属性取得	認証された登録者の属性情報を取得できること。
3	データマネジメント系 API	データアクセス	データ連携基盤のデータマネジメント機能群と連携し、データのライフサイクル（登録、参照、変更及び削除）を管理するためのオープン API を提供できること。
			シェアードデータの場合には認証系 API と連携し、データ利用者に対するカタログの開示制御情報に応じてデータ提供を制限できること。
			データ連携基盤の対応するデータフォーマット（推奨データセット等）のカタログを一括取得可能な API を提供すること。
4		パブリッシュ/サブスクライブ	登録データの更新を検出した際に、変更されたデータを通知先にリアルタイムで送信するためのオープン API を提供すること。
			シェアードデータの場合、個別利用契約を締結しているデータ利用者に対して変更されたデータを通知すること。
			通知先情報のライフサイクル（登録、参照、変更及び削除）を管理するためのオープン API を提供すること。

項番	機能ブロック	機能名	要件
5		データ仲介	分散するデータ（リンクデータ）に対し、その所在のライフサイクル（登録、参照、変更及び削除）を管理するためのオープン API を提供できること。
6	サービス連携	カタログ管理	データ連携基盤が保持する API を公開する機能を提供できること。
			カタログに保管されたカタログ情報（メタデータ等）の登録、検索、参照及び削除をできること。
			データ利用者に対してカタログの開示制御ができること（主に個別提供契約及び個別利用契約成立時）。
			オープンデータは全てのデータ利用者にカタログ開示できること。
			シェアードデータの開示を個人及び組織単位に管理できること。
			開示対象のデータはカタログ単位とすること。
7	データ伝送	プロトコル変換	連携システムとのデータ処理（データ受付及び取得）に使用する一般的な通信プロトコルからデータ連携基盤が対応する通信プロトコルに変換しデータ伝送ができること。
8	データ処理	データ変換	連携システムから取得したデータをデータ連携基盤が扱える形式に変換できること。 （変換対象は、語彙や、形式及び項目等）
9		データ受付	データ連携基盤にデータを蓄積するため、データ提供者や連携システムから以下の方法によるデータ登録を受け付けること。 ・API によるデータ登録（リアルタイム及びオンデマンド） ・データ受付画面からデータのリンク情報を登録 ・データ受付画面からデータ（ファイル）をアップロード
			データ連携基盤が対応するデータフォーマット（推奨データセット等）ごとにデータ受付用 API を提供すること。
10		データ取得	データ連携基盤が定期的に以下の方法によりデータを取得できること。 ・データ提供者システムからデータ登録用 API でデータを登録 ・データ提供者システムのデータ取得用 API を使用してデータ連携基盤がデータを収集

項番	機能ブロック	機能名	要件
11		データ補完	リアルタイムデータ等で欠損したデータは不正を検出し、修正を促すことができること。
			データ連携基盤が対応するデータフォーマット（推奨データセット含む）チェックによるデータ項目の不正を検出し、修正を促すことができること。
			登録されたデータの「値の有効範囲」や「タイムスタンプ不正」等の内容チェックにより不正を検出し、修正を促すことができること。
			リンク切れを定期的に自動検出し、修正を促すことができること。

(5)データマネジメント

データマネジメントは、データ連携基盤がデータを管理する機能ブロックであり、登録されたカタログ情報、データ、個別提供契約情報及び個別利用契約情報を管理する。

各データは、外部データ連携機能群を介して連携し、このデータ管理機能は主にデータ連携基盤が持つデータを管理する登録データ管理機能及びデータ連携基盤外に持つデータを管理する分散データ管理機能に分類され、それぞれデータ処理及び個別提供契約・個別利用契約のステータス管理の機能を持つ。さらに、イベント管理機能により事前に登録されたイベント発生条件及び処理内容に従い、処理を行う機能を持つ。また、データマネジメントで扱うデータ種類として、静的データ、動的データ、地理空間データ及びデータ本体に付帯するメタデータをサポートする。

データマネジメント機能群に関する要件の一覧を以下に示す。

表 4-7 データマネジメント機能群の要件一覧

項番	機能ブロック	機能名	要件
1	データ管理	登録データ管理	データ連携基盤が管理するデータに対し、データを処理（登録、参照、更新及び削除）できること。
			データ提供時のデータ提供者からの申請内容及び運用ユーザの承諾状況（個別提供契約）を管理できること。
			シェアードデータ利用時のデータ利用者からの申請内容及び運用ユーザの承諾状況（個別利用契約）を管理できること。
			データの利用履歴を管理できること。
			リアルタイムデータ等の連続したデータを時系列で登録及び参照できること。
2		分散データ管理	連携システムに分散するデータ（リンク情報等）に対し、データを仲介（登録、参照、更新及び削除）できること。
			データ提供時のデータ提供者からの申請内容及び運用ユーザの承諾状況（個別提供契約）を管理できること。
			シェアードデータ利用時のデータ利用者からの申請内容及び運用ユーザの承諾状況（個別利用契約）を管理できること。
3		イベント管理	登録データの更新を契機に、事前に登録したイベント発生条件（気温が 30℃以上等）及び処理内容（通知等）に従い、リアルタイムに処理を実施すること。

(6)アセットマネジメント

データ連携基盤は、段階的に連携システムを拡充し、将来、様々なシステムとの連携を実現する方針である。

そのため、連携システムの追加及び変更に伴い管理できる機能が必要であり、連携情報（認証情報及び接続情報等）を管理する機能並びに連携システムとのデータ連携状態及び接続状態等を管理する機能を提供する。

アセットマネジメント機能群に関する要件の一覧を以下に示す。

表 4-8 アセットマネジメント機能群の要件一覧

項番	機能ブロック	機能名	要件
1	システム管理	システムライフサイクル登録	連携システムとの連携情報（認証方式、資格情報及び接続先情報等）のライフサイクル（登録、参照、変更及び削除）を管理できること。
2		システム状態管理	連携先として登録済の連携システムに対して接続状態を管理できること。

(7)PF 間連携

データ連携基盤は、より幅広いデータ利活用を実現するため、各 PF にて管理する認証情報及びデータを連携し、相互運用を行う。相互運用の中で複数 PF との連携にあたり、多様なインタフェースが想定されるため、標準化された API 及びデータ連携方式に対応した認証連携及びデータ連携機能を提供し、PF との接続を容易にする。

また、分野間連携に関して、相互にデータ検索を行うための分野間データ検索機能、データを提供又は取得するための分野間データ交換制御機能及びデータ交換の記録をする分野間データ交換記録機能が必要となる。要件については、分野間データ連携基盤の開発状況を見極めつつ、継続検討とする。

PF 間連携機能群に関する要件の一覧を以下に示す。

表 4-9 PF 間連携機能群の要件一覧

項番	機能ブロック	機能名	要件
1	認証連携	認証連携	標準化団体の定めたオープン API を使用し、相互運用先の利用者の認証情報を元に、利用者の認証要求に対応できること。
2	データ連携	データ連携	相互運用先にデータ連携基盤のデータを提供できること。
			データ利用者に相互運用先のデータを提供できること。
3	分野間連携	分野間データ検索	データ連携基盤外に分散されたデータを、データの概要情報（カタログ）を元に検索できること。
4		分野間データ交換制御	データ連携基盤及び相互運用先の双方の取り決めによりデータの利用権限を判断し、データのアクセス範囲を制御できること。
5		分野間データ交換記録	データ連携基盤及び相互運用先の双方で連携したデータの交換履歴を記録できること。

ア　連携方式

相互運用先と容易な接続を考慮し、多様なインタフェースに対応する。

また、連携のための API は、オープン API で提供することが必須である。

イ　相互運用先

データ連携基盤は、民間企業及び行政機関等の PF が提供する API を活用することで、個別に構築された PF と連携し、分野や組織の壁を越えて様々なデータを相互に流通する。

その相互運用先を以下に示す。

表 4-10 相互運用先一覧

項番	相互運用先	概要
1	他の地域の PF （スマートシティ分野）	認証連携及び PF 間でデータ共有するための連携機能を有し、各種機能及びデータを相互運用することのできる他の地域の PF。
2	外部の PF （個別分野）	認証連携及び PF 間でデータ共有するための連携機能を有し、各種機能及びデータを相互運用することのできる個別分野の PF。
3	DATA-EX を介した PF	DATA-EX の仕様に準拠し、データの検索、データの提供及びデータの利用ができ、利用条件及び来歴管理等の情報を交換できる PF。

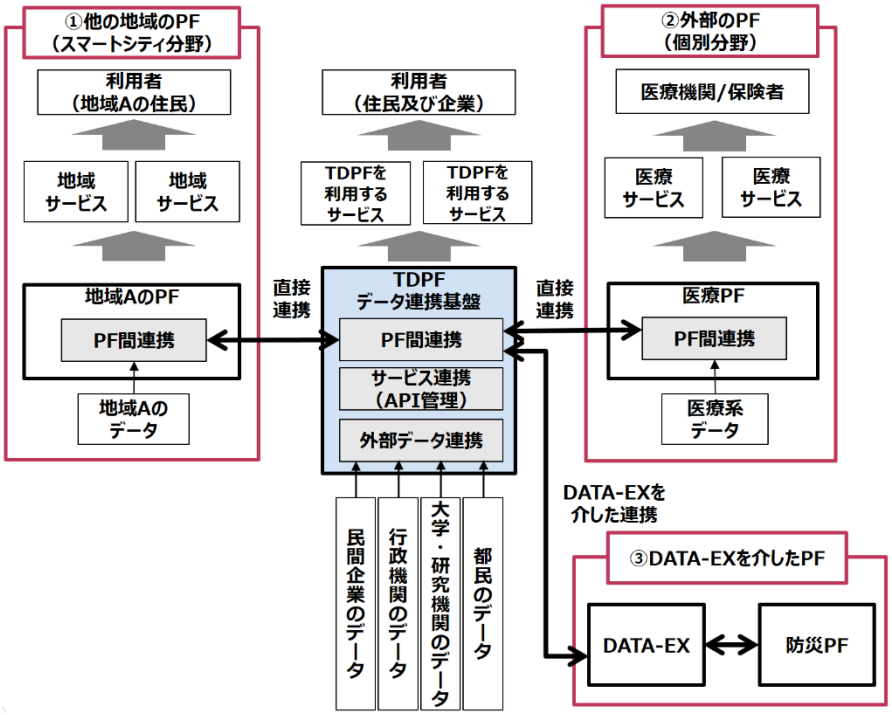

図 4-3 PF 間連携イメージ

(8)共通

データ連携基盤は、サービス連携（ポータル）に対して、データ連携基盤の持つデータを可視化する機能及びデータ連携基盤の持つデータを分析する機能を提供する。

共通機能群に関する要件の一覧を以下に示す。

表 4-11 共通機能群の要件一覧

項番	機能ブロック	機能名	要件
1	可視化、分析	可視化・分析ダッシュボード	各カタログの閲覧数及びダウンロード数並びにデータダウンロードランキング及び検索ワードランキングを可視化できること。
			利用者の利用動向（回遊分析等）及び個人別、組織別の利用者の利用頻度を分析できること。
			データ登録時にデータを分析し、メタデータ（タグ情報）の候補を表示すること。

2 画面一覧

データ連携基盤が提供する４つのポータルサイト画面の要件を示す。

(1)利用者ポータルサイト

非会員ユーザ、個人ユーザ、組織管理ユーザ及び組織ユーザに対して、入会登録申請及びデータ登録・取得関連機能を提供する。また、データ利用者の興味喚起を促すためのランキング表示並びにデータ連携基盤の利用者支援のためのサイト利用ガイド及び問合せフォームを提供する必要がある。

利用者ポータルサイトの画面要件を以下に示す。

表 4-12 利用者ポータルサイト画面要件

○：利用可能、△：参照のみ利用可能、－：利用不可

項番	画面	説明	非会員ユーザ	個人ユーザ	組織管理ユーザ	組織ユーザ
1	入会登録申請（個人ユーザ）	個人ユーザの入会登録申請を行う画面。 多要素認証による本人確認を行うことができること。	○	－	－	－
2	入会登録申請（組織）	組織として利用するための申請を行う画面。	○	－	－	－
3	入会登録申請（組織管理ユーザ及び組織ユーザ）	組織内の入会登録申請を行う画面。	－	－	○	○
4	認証	ID、パスワード等を入力して、ログインする画面。	－	○	○	○
5	検索（トップページ）	データ連携基盤の利用者ポータルサイトのカタログ検索画面。 以下の要素を含むこと。 ・ カタログ検索フォーム ・ データダウンロード数 ・ 検索ワードランキング等 ・ FAQ（よくある質問）	○	○	○	○

項番	画面	説明	非会員ユーザ	個人ユーザ	組織管理ユーザ	組織ユーザ
6	マイページ	アカウント情報の表示、変更申請及び任意退会申請を行う画面。 データ利用及びデータ提供の履歴を表示すること。 利用データの更新情報を表示すること。	–	○	○	○
7	カタログ一覧	カタログ検索の結果を一覧表示する画面。 検索条件を追加で指定し、検索結果を再抽出できること。	○	○	○	○
8	カタログ詳細	カタログ情報（データ詳細、メタデータ、閲覧数、ダウンロード数及びプレビュー等）を表示すること。	○	○	○	○
		オープンデータをダウンロードできること。	○	○	○	○
		データ提供者がオープンデータ及びシェアードデータのカタログを登録、編集及び削除できること。	–	○ ※1	○	○
		データ利用者がシェアードデータのカタログの開示要求をできること。	–	○ ※2	○	○
		シェアードデータをダウンロードできること。	–	○ ※2	○	○
9	カタログ開示状況	カタログの開示状況の確認及びカタログの開示要求に対する承諾を行う画面。	–	○	○	○
10	問合せ	データ連携基盤に関する問合せを行う画面。	△	○	○	○
11	利用ガイド	利用ガイドを表示する画面。	○	○	○	○
12	お知らせ	お知らせを表示する画面。	○	○	○	○

項番	画面	説明	非会員ユーザ	個人ユーザ	組織管理ユーザ	組織ユーザ
13	規約同意	入会登録申請時及び利用規約変更時に利用規約同意を得る画面。	○ ※3	○ ※4	○ ※4	–
14	データ提供申請	データ連携基盤へデータを提供するにあたり、TDPF 運営組織が定める必要事項の伝達及びデータの提供申請を行う画面。	–	○ ※1	○	○
15	データ利用申請	データ連携基盤のデータを利用するにあたり、データ利用目的及び TDPF 運営組織が定める必要事項の伝達、データの利用申請を行う画面。	–	○ ※2	○	○
16	アカウント管理（組織内）	組織内のアカウントを管理する画面。 組織管理ユーザ及び組織ユーザのアカウントのライフサイクル（登録、登録拒絶、任意退会、強制退会、利用停止、利用停止解除及び削除）を管理とその承諾をできること。	–	–	○	–

※1 個人ユーザがデータ提供申請する場合、本人確認書類による本人証明後に申請することが可能

※2 個人ユーザがシェアードデータのデータ利用申請する場合、本人確認書類による本人証明後に申請することが可能

※3 入会登録時の利用規約同意

※4 規約変更時の利用規約同意

(2)開発者ポータルサイト

個人ユーザ、組織管理ユーザ及び組織ユーザのうち、API 等の開発者に対してデータ連携基盤利用中の問題解決のために FAQ、稼働情報、利用ガイド、API の評価環境及び問合せフォーム等を提供する必要がある。

開発者ポータルサイトの画面要件を以下に示す。

表 4-13 開発者ポータルサイト画面要件

○：利用可能、－：利用不可

項番	画面	説明	非会員ユーザ	個人ユーザ	組織管理ユーザ	組織ユーザ
1	認証	ID、パスワード等を入力して、ログインする画面。 ※利用者ポータルサイトへのアカウント情報でログイン可能	－	○	○	○
2	トップページ	データ連携基盤の開発者ポータルサイトのトップページ画面。 以下の要素を含むこと ・ 開発ガイド（仕様、検証手順、活用事例及び API 登録方法） ・ API のサンプルコード ・ 活用事例 ・ データ連携基盤稼働状況（障害メンテナンス情報等） ・ FAQ（よくある質問）	－	○	○	○
3	お知らせ	お知らせを表示する画面。	－	○	○	○
4	API 評価	開発者が開発した API を評価するための画面。	－	○	○	○

(3)コミュニティポータルサイト

非会員ユーザ、個人ユーザ、組織管理ユーザ、組織ユーザの抱えるデータ利活用の課題及び TDPF 運営組織のサービス運用の課題を共有する双方向のコミュニケーションが可能な情報交換の場を設け、利用者の課題解決及びデータ連携基盤のサービス向上を図ることが必要である。

コミュニティポータルサイトの画面要件を以下に示す。

表 4-14 コミュニティポータルサイト画面要件

○：利用可能、△：参照のみ利用可能、－：利用不可

項番	画面	説明	非会員ユーザ	個人ユーザ	組織管理ユーザ	組織ユーザ
1	情報交換	民間企業、大学・研究機関、都民及び行政機関等の利用者を対象として、双方向の意見交換及びコミュニティ管理（コミュニティの作成や検索、削除等）ができる画面。	△	○	○	○

(4)運用者ポータルサイト

データ連携基盤として、最新の各種情報を提供することで利用者の興味喚起を継続して促すためのコンテンツ配信、アカウント管理及びデータ管理等を行う管理画面を提供するが必要である。

運用者ポータルサイトの画面要件を以下に示す。

表 4-15 運用者ポータルサイト画面要件

○：利用可能、－：利用不可

項番	画面	説明	運用管理ユーザ	運用ユーザ
1	認証	ID、パスワード等を入力して、ログインする画面。	○	○
2	アカウント管理	登録者アカウントのライフサイクル（登録、登録拒絶、任意退会、強制退会、利用停止、利用停止解除及び削除）を管理する画面。 アカウントに関する各種申請に対する承諾を行うことができること。	○	○
		利用規約で停止事由と定義された事象が発生した場合に該当のアカウントを停止できること。	○	○
		アカウント停止の理由となる事象が解決した場合に、再度利用できるように該当のアカウントの停止解除を実施できること。	○	○
3	データ管理	提供されたデータの管理を行う画面。 データ提供申及びデータ利用申請の承諾を実施できること。	○	○
4	清算	清算に関する情報の管理を行う画面。 個別利用契約の情報から請求情報を確認できること。	○	○
5	ロール管理	登録者が所属するロールを管理する画面。 アカウント及びロール別に、データ連携基盤にアクセスする範囲及び権限を定義する制御ポリシーを管理できること。	○	○
6	コンテンツ配信	お知らせ、FAQ 及び利用規約を各ポータルサイトに配信する画面。	○	○

項番	画面	説明	運用管理ユーザ	運用ユーザ
7	問合せ管理	利用者からの問合せを確認し、対応する画面。	○	○
8	アカウント追加申請（TDPF 運営組織内）	運用管理ユーザ及び運用ユーザの情報を入力してアカウント追加申請を行う画面。	○	○
9	アカウント管理（TDPF 運営組織内）	運用管理ユーザ及び運用ユーザのアカウントのライフサイクル（登録、登録拒絶、任意退会、強制退会、利用停止、利用停止解除及び削除）の管理及び TDPF 運営組織内のアカウントに関する承諾を行う画面。	○	–

3 データ概要

データ連携基盤の業務要件から、運用上必要となるデータの概要を示す。

(1)認証

利用者のアカウントを管理するためのデータを指す。アカウントに紐づく情報及び利用規約への同意情報を管理する。

表 4-16 認証データ一覧

項番	データ	説明
1	アカウント情報	アカウントを管理する情報。 キー情報（メールアドレス等）、認証情報（パスワード及び多要素認証情報）権限情報、連絡先情報及び組織情報等の項目を管理する。
2	同意情報	入会登録時及び利用規約変更時の同意情報を管理する。

(2)データマネジメント

データ連携基盤で蓄積しているデータ（リンクデータを含む）を管理するためのデータを指す。カタログ情報及び個別提供・利用契約情報、提供者からの登録データ、リンク情報、開示制御情報及び利用履歴を管理する。

表 4-17 データマネジメントデータ一覧

項番	データ	説明
1	カタログ情報	データ連携基盤上で蓄積しているデータ及び連携システムに分散するデータの概要情報。 ①登録データの概要 ・ 登録データの名称、項目及び件数等の提供対象データを特定するために必要な情報 ・ 登録データ概要の説明文やタグ情報等のデータの概要を示す情報 ・ 登録データの種類（オープンデータかシェアードデータであるか）を示す情報 ②登録データの利用条件 ・ 利用条件（データ自体又はデータの利用権を提供するか）を示す情報 ・ 提供に対する対価 ・ 提供方法 ・ データ提供停止の事前告知期限（データ提供者による任意解約の事前告知期限）

項番	データ	説明
		③登録データの更新情報 ・ 最終更新日及びデータ更新の実施有無 ④その他 ・ 登録データにおけるパーソナルデータ又は個人情報（※1）の有無 ・ 登録データの知的財産権及び営業秘密に係るデータ又は限定提供データに関する事項 ・ ライセンス情報（データ提供者の判断により Creative Commons License（※2）及び Open Database License（※3）等、複数のライセンス設定を可能とする）
2	個別提供契約情報	データ提供者と締結する個別提供契約の情報。データ提供申請を行ったカタログ情報単位で作成する。 ①提供データの概要 ・ 提供データの名称、項目及び件数等提供対象データを特定するために必要な情報 ・ 提供データの種類（オープンデータかシェアードデータであるか）を示す情報 ②提供データの利用条件 ・ 利用条件 ・ 提供に対する対価（オープンデータは無償のみ） ・ 提供方法 ・ データ提供停止の事前告知期限（データ提供者による任意解約の事前告知期限） ③提供データの更新情報 ・ 最終更新日及びデータ更新の実施有無 ④その他の個別提供契約に必要な情報 ・ 提供対象データについて TDPF に提供を認める範囲 ・ 必要に応じて定める特約事項 ⑤その他の個別提供契約に必要な同意情報 ・ TDPF における提供対象データの利用目的に対する同意 ・ 契約期間中にデータ提供者が退会した場合の措置に対する同意 ・ 提供対象データを加工、分析、編集、統合等することによって新たに生じたデータ（派生データ）の取扱いに対する同意 ・ パーソナルデータの有無 ・ 個人情報（※1）の有無

項番	データ	説明
3	個別利用契約情報	データ利用者と締結する個別利用契約の情報。データ利用申請をしたカタログ情報単位に作成する。 ①利用データの概要 ・ データの名称、項目及び件数等の提供対象データを特定するために必要な情報 ②利用データの利用条件 ・ 利用対象データの利用目的 ・ 利用対象データの利用条件 ・ 利用対象データの提供に対する対価 ・ 利用対象データの受領方法 ・ 契約期間 ③その他の個別利用契約に必要な情報 ・ 利用対象データの再提供の可否及び再提供を認める範囲 ・ 特約事項 ④その他の個別利用契約に必要な同意情報 ・ 利用対象データの知的財産権及び営業秘密に係るデータ又は限定提供データに関する事項に対する同意 ・ 派生データの取扱いに対する同意 ・ データ利用者への権利、義務及び利用上確認に対する同意 ・ 個別利用契約解除の条件に対する同意
4	登録データ	データ受付及びデータ取得によって収集したデータであり、データ連携基盤で保持するデータ。 データ整備事業で作成したデータも含まれる。
5	分散データ	連携システムに分散するデータのリンク情報。
6	開示制御情報	カタログ情報と連携した開示制御データ。
7	データ利用履歴	カタログ情報と連携したデータ提供及びデータ利用の履歴データ。

※1 当面の間、個人情報を含むパーソナルデータは取り扱わない。

※2 国際的非営利組織 Creative Commons が定義する著作権のある著作物の配布を許可する意思表示（パブリック・ライセンス）のこと。

※3 データベース利用者に対して、データベースの自由な共有、改変及び利用を認めると同時に、他者に対しても同様な自由を提供することを意図したオープンナレッジ財団の Open Data Commons が開発したライセンス契約のこと。

(3)共通

データ連携基盤の運用を行うためのデータを指す。利用者からの問い合わせ情報及びシステムの使用状況ログを管理する。

表 4-18 共通データ一覧

項番	データ	説明
1	問合せ情報	ポータルサイトからの問い合わせに関する情報。
2	使用状況ログ	監査、問合せ及び障害発生時のシステム調査を目的とした実行操作のログ情報。

4　インタフェース概要

データ連携基盤の業務要件から、運用上必要となるインタフェースの概要を示す。

(1)インタフェース

ア　データ登録

データ連携基盤へのデータ登録は、データ提供者の端末若しくはデータ提供者のシステムから行う。データ登録に必要なインタフェースを以下に示す。

インタフェースは、ポータルから利用者が手動登録するためのインタフェース及びシステムによって自動登録するためのインタフェースが必要である。システム連携の場合、データ連携基盤がデータ提供者のシステムのデータ取得用 API を利用して、データを収集するケースも存在する。

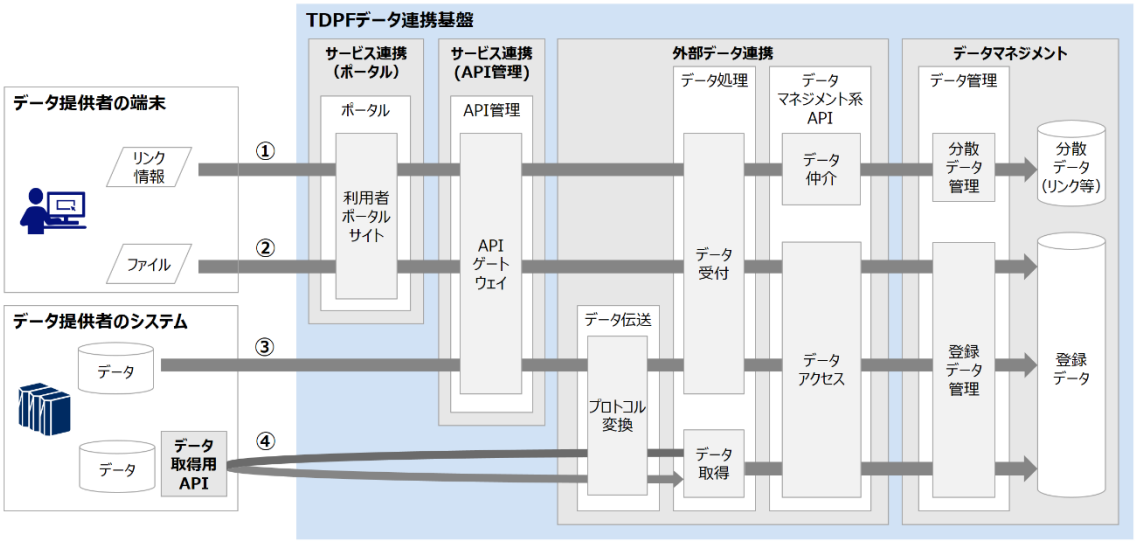

図 4-4 データ登録インタフェース概要図

表 4-19 データ登録インタフェース

項番	インタフェースの種類		概要
1	ポータル（手動登録）	ポータルからリンク情報を登録	利用者ポータルサイトからデータへのリンク情報を登録する。 データ自体はデータ提供者のシステムで管理する。
2		ポータルからファイルをアップロード	利用者ポータルサイトからデータをアップロードする。
3	システム連携（自動登録）	データ登録用 API による登録	データ提供者システムからデータ登録用 API（API ゲートウェイ）を使用してデータを登録する。
4		データ提供者システムから取得	データ提供者システムのデータ取得用 API を使用してデータ連携基盤がデータを収集する。

イ　データ取得

データ連携基盤からのデータ取得は、データ利用者の端末若しくはデータ利用者のシステムから行う。データ取得に必要なインタフェースを以下に示す。

インタフェースは、ポータルから利用者が手動取得するためのインタフェース及びシステムによって自動取得するためのインタフェースが必要である。

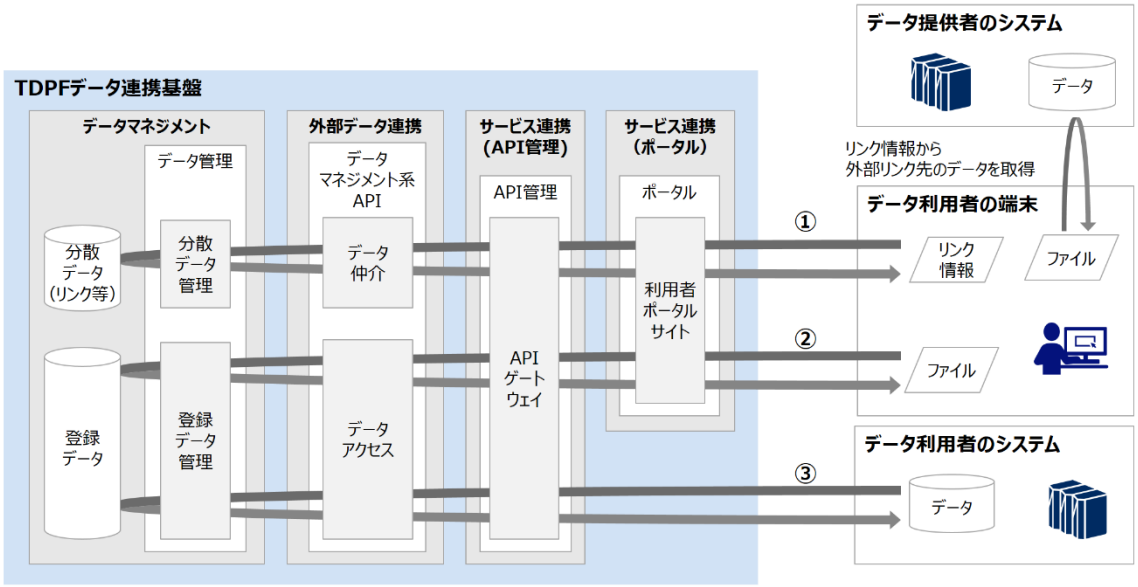

図 4-5 データ取得インタフェース概要図

表 4-20 データ取得インタフェース

項番	インタフェースの種類		概要
1	ポータル（手動取得）	ポータルからリンク情報を取得	利用者ポータルサイトからデータへのリンク情報を取得し、リンク情報から外部リンク先のデータを取得する。
2		ポータルからファイルをダウンロード	利用者ポータルサイトからからデータをダウンロードする。
3	システム連携（自動取得）	データ取得用 API による取得	データ利用者システムからデータ取得用 API（API ゲートウェイ）を使用してデータを取得する。

ウ　データ通知

データ連携基盤が保持している登録データの更新を契機に、データ利用者のシステムにデータ通知を行う。データ通知に必要なインタフェースを以下に示す。

データ連携基盤がデータ利用者のシステムのデータ受信用 API を使用して通知するためのインタフェースが必要である。

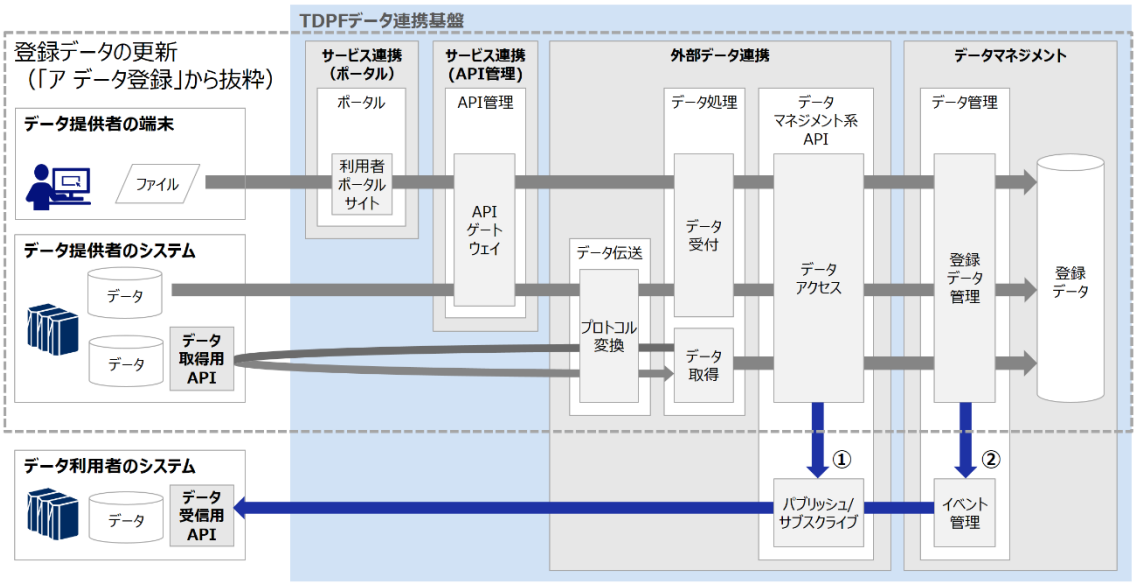

図 4-6 データ通知インタフェース概要図

表 4-21 データ通知インタフェース

項番	インタフェースの種類	概要
1	パブリッシュ/サブスクライブ機能からの通知（登録データの更新通知）	パブリッシュ/サブスクライブ機能にデータ利用者のシステムを通知先として事前登録し、登録データの更新を契機にデータ利用者のシステムのデータ受信用 API を使用して通知する。
2	イベント管理機能からの通知	イベント管理機能にイベント発生条件（気温が30℃以上等）及びパブリッシュ/サブスクライブ機能にデータ利用者のシステムを通知先として事前登録し、登録データの更新を契機にイベント発生条件と一致するデータをデータ利用者システムのデータ受信用 API を使用して通知する。

(2)プロトコル

データ提供者システムのデータ取得用 API は、既存の API であることが多く、多様な API に対応する必要があるため、汎用的なインタフェースのプロトコルに対応させる。

データ連携基盤は、データ提供者からの片方向通信によるデータ登録及びデータ取得だけでなく、データ連携基盤からデータ取得を行う場合及びデータを送信する場合があるため、双方向通信にも対応する必要がある。

表 4-22 プロトコル

項番	プロトコル	説明
1	片方向通信	汎用的な片方向通信プロトコル（※1）（HTTPS 等）によるデータアクセスを可能とする。
2	双方向通信	汎用的な双方向通信プロトコル（※2）（MQTT 等）によるデータアクセスを可能とする。

※1 送信者と受信者が固定されており、信号やデータを送信者からのみ送信することができる通信方式のこと。

※2 送信者と受信者が固定されておらず、信号やデータを各接続先から送信することができる通信方式のこと。

第5章　非機能要件

非機能要件は、独立行政法人情報処理推進機構が提供する「非機能要求グレード2018」を参照とする。非機能要件の重要項目と定義された項目及びデータ連携基盤が運用上、必要となる項目を抽出し、各項目のレベル定義を行う。

なお、データ連携基盤は、将来的に生活・社会経済活動に多大な影響を与えるものとなるため、「非機能要求グレード 2018」におけるモデルシステムでは、「社会的影響が極めて大きいシステム」に該当することが想定されるが、初期構築時においては、リーンスタートの観点から「社会的影響が限定されるシステム」と定義し、この要求レベルを採用することを基本とする。ただし、データ連携基盤の性質を踏まえ、必要に応じ上位ランクの要求レベルを一部定義するとともに、社会的重要度の変化に柔軟に対応し、継続的に要件の見直しを行うものとする。

1　非機能要件一覧

データ連携基盤の非機能要件を表 5-1 に示すとおり、システムを継続的に利用可能とするための要求である「可用性」、システムの性能と将来のシステム拡張に関する要求である「性能・拡張性」、システムの運用と保守のサービスに関する要求である「保守・運用性」、構築するデータ連携基盤の安全性の確保に関する要求である「セキュリティ」の大項目に分類し、さらに詳細な中項目を定義した。各非機能要件の項目及び要求レベルの定義は、次項以降に定義する。

表 5-1　非機能要件一覧

項番	非機能要件（大項目）	非機能要件（中項目）	説明
1	可用性	継続性	システムの運用スケジュール、業務継続性及び目標復旧水準等の要件
		回復性	復旧作業等の要件
2	性能・拡張性	業務処理量	通常時の業務量、業務量増大度及びデータの保管期間等の要件
		性能目標値	レスポンス等の要件
		リソース拡張性	CPU、メモリ及びディスクの拡張性要件

項番	非機能要件（大項目）	非機能要件（中項目）	説明
3	保守・運用性	通常運用	サーバ、端末、ストレージ及びデータ等のアセット単位の冗長化や復旧に対する要件
		保守運用	保守計画及び保守方針等の要件
		運用環境	開発用環境及び試験用環境の設置、運用のためのマニュアルの準備等の要件
		サポート体制	保守サポート契約に対する要件
		その他運用管理方針	内部統制対応及びサービスデスク設置等に対する要件
4	セキュリティ	前提条件・制約条件	遵守すべき情報セキュリティに対する要件
		セキュリティリスク分析	セキュリティリスク分析の範囲に対する要件
		セキュリティ診断	セキュリティ診断の実施に対する要件
		セキュリティリスク管理	脆弱性等に対応するための要件
		アクセス・利用制限	認証機能及び利用制限に対する要件
		データの秘匿	データの暗号化に対する要件
		不正追跡・監視	ログの取得、保管期間及び不正監視対象に対する要件
		ネットワーク対策	ネットワークの制御、不正検知及びネットワークの攻撃に対する要件
		マルウェア対策	マルウェア（※1）の感染防止に対する要件
		Web 対策	セキュアコーディング（※2）、Web サーバの設定及び WAF（Web Application Firewall）（※3）の導入に対する要件

※1 不正かつ有害に動作させる意図で作成された悪意のあるソフトウェアや悪質なコードのこと。

※2 マルウェア等による悪意ある攻撃に耐え得る堅牢なプログラムを記述すること。

※3 Web アプリケーションの脆弱性を突いた攻撃に対するセキュリティ対策のこと。

(1)可用性

本項では、システムとしてデータ連携基盤を継続的に利用可能とするための要件を記載する。

データ連携基盤の通常運用時間は、計画停止を除く 24 時間 365 日運用と定義する。

ここでは可用性に対する要件である継続性及び回復性を示す。

ア　継続性

表 5-2 継続性の定義

項番	項目	説明	要件
1	運用スケジュール	データ連携基盤の稼働時間及び停止運用に関する情報	運用時間は、計画停止を除く 24 時間 365 日運用とする。
			計画停止は、事前に調整の上、実施すること。
2	業務継続性	可用性を保証するにあたり、要求される業務の範囲とその条件	可用性を保証する業務は、データ連携基盤で提供する全ての業務とすること。
			想定できる障害（ハードウェア故障など）により業務が一時的に中断した場合、冗長構成によるハードウェア切替え等を行い 60 分以内に業務を再開すること。
			想定できる障害が二重に発生し、一時的に業務が中断した場合でも、60 分以内に業務を再開すること。
3	目標復旧水準（業務停止時）	業務停止を伴う障害が発生した際、なにをどこまで、どれ位で復旧させるかの目標	業務の復旧は、障害発生時点までデータを復旧すること。データの復旧は日次バックアップ及びアーカイブからの復旧すること。
			業務停止を伴う障害が発生した際、12 時間以内に全ての業務を復旧すること。
4	目標復旧水準（大規模災害時）	大規模災害が発生した際、どれ位で復旧させるかの目標	大規模災害時は、一週間以内に全ての業務を再開すること。
5	稼働率	明示された利用条件下で、データ連携基盤が要求されたサービスを提供できる割合	データ連携基盤の稼働率は、99.99%（1 年間で 1 時間程度の停止）とすること。

イ　回復性

表 5-3 回復性の定義

項番	項目	説明	要件
1	可用性確認	可用性として要求された項目をどこまで確認するかの範囲	可用性として定義した項目について、業務停止となる想定できる障害に対して、対策の確認を行うこと。

(2)性能・拡張性

本項では、データ連携基盤の性能及び将来のシステム拡張に関する要件を記載する。

データ連携基盤は、データ容量、機能種類及び利用者増加等によるリソースの拡張性を有した構成とする。

データ量に依存しない画面の性能目標値は、利用者がストレスを感じない画面操作の時間である 3 秒以内のレスポンスを目標とする。

ここでは性能・拡張性に対する要件の業務処理量、性能目標値及びリソース拡張性を示す。

ただし、通常時の業務量（ユーザ数、同時アクセス数及びデータ量等）及び性能目標値は継続検討とする。

ア　業務処理量

表 5-4 業務処理量の定義

項番	項目	説明	要件
1	通常時の業務量	性能・拡張性に影響を与える業務量	ユーザ数、同時アクセス数、オンラインリクエスト件数及びバッチ処理件数は継続検討とする。 また、データ量は 50BG を最大値として想定する。 データ連携基盤の業務量は、事業計画及び令和 4 年度の実証とともに見直しを行う予定。
2	業務量増大度	データ連携基盤の稼働開始時点と業務量が最大になる時点の業務量の増大率	本項は、通常時の業務量項目同様、継続検討とし見直しを行う予定。
3	保管期間	データ連携基盤で取り扱うデータに対する保管期間	データの保管期間は 5 年とする。

イ　性能目標値

表 5-5 性能目標値の定義

項番	項目	説明	要件
1	オンラインレスポンス	オンラインシステム利用時に要求されるレスポンス	通常時のレスポンス遵守率（※1）は 90%とする。 また、ピーク時のレスポンス遵守率は 80%とする。
2	ターンアラウンドタイム	バッチシステム利用時に要求されるレスポンス	ターンアラウンドタイム（※2）については、継続検討とする。

※1 利用者が端末を操作し、規定の時間以内に画面表示が開始される割合のこと。

※2 処理要求を実施した時点から、その処理が行われて結果の出力が完了するまでの時間のこと。

ウ　リソース拡張性

表 5-6 リソース拡張性の定義

項番	項目	説明	要件
1	CPU 拡張性	CPU の拡張性を確認するための項目	CPU 使用率は将来の業務量増加に備え、通常時は 50%以上 80%未満の使用率を想定し、業務量が増加した場合は、CPU を 1.5 倍まで拡張が可能なこと。
2	メモリ拡張性	メモリの拡張性を確認するための項目	メモリ使用率は将来の業務量増加に備え、通常時は 50%以上 80%未満の使用率を想定し、業務量が増加した場合は、メモリを 1.5 倍まで拡張が可能なこと。

(3)運用・保守性

本項では、データ連携基盤の正常な状態を維持するため、正常時、メンテナンス時及び障害発生時の運用に対する要件を記載する。

データ連携基盤の通常運用時間は、計画停止を除く 24 時間 365 日運用と定義する。データ連携基盤が利用するバックアップについて、復旧に必要なデータは、自動で日次バックアップを取得し、復旧を行うことができる構成とする。

ここでは運用・保守性に対する要件の通常運用、保守運用、運用環境、サポート体制及びその他の運用管理方針を示す。

ただし、保守運用、運用環境、サポート体制、その他運用管理方針は継続検討とする。

ア　通常運用

表 5-7 通常運用の定義

項番	項目	説明	要件
1	運用時間	データ連携基盤が運用を行う時間	運用時間は、計画停止を除く 24 時間 365 日運用とする。
2	バックアップ	データ連携基盤が取り扱うデータのバックアップに関する項目	全データを復旧するため、全データのバックアップを行うこと。
			データのバックアップは、障害発生時の復旧及び作業ミス等で損失したデータの回復に使用できること。
			バックアップは、自動で行うこと。
			バックアップは、週次で全体バックアップを行い、日次で差分バックを行うこと。
			バックアップは、3 年間保存すること。
3	運用監視	データ連携基盤を構成するハードウェア・ソフトウェア（業務アプリケーションを含む）に対する監視に関する項目	運用監視は、死活監視、エラー監視及びリソース監視を行うこと。
			運用監視の監視間隔は、分間隔のリアルタイム監視を行うこと。

イ　保守運用

表 5-8 保守運用の定義

項番	項目	説明	要件
1	計画停止	点検作業、領域拡張、デフラグ及びマスターデータのメンテナンス等、システムの保守作業の実施を目的とした、事前計画済みのサービス停止に関する項目	計画停止は、事前に調整の上、実施すること。
2	運用負荷削減	保守運用に関する作業負荷を削減するための設計に関する項目	運用負荷削減のため、自動化が可能な運用保守作業は自動化すること。自動化可能な作業については、継続検討とする。

ウ　運用環境

表 5-9 運用環境の定義

項番	項目	説明	要件
1	開発環境の設置	データ連携基盤の開発作業を実施する目的で導入する環境についての項目	データ連携基盤の開発環境を設置しない（ただし、検証環境と併用する）。
2	検証環境の設置	データ連携基盤の動作を検証する目的で導入する環境についての項目	データ連携基盤の検証環境を設置し、開発環境と併用する。
3	マニュアル準備レベル	運用のためのマニュアルの準備のレベル	システムの通常運用と保守運用のマニュアルを準備すること。
4	リモートオペレーション	データ連携基盤の設置環境とは離れた環境からのネットワークを介した監視や操作の可否を定義する項目	運用監視は、遠隔地からリモート監視できること。また、運用作業はリモートで操作できること。
5	外部システム接続	データ連携基盤の運用に影響する連携システムとの接続の有無に関する項目	データ連携基盤は、様々な連携システムと接続し、データ連携を行うことができる。

エ　サポート体制

表 5-10 サポート体制の定義

項番	項目	説明	要件
1	保守契約（ソフトウェア）	保守が必要な対象ソフトウェアの範囲	データ連携基盤を構成するソフトウェアのマルチベンダのサポート契約を行うことを想定する。 本項目は継続検討とする。
2	ライフサイクル期間	運用保守の対応期間及び実際にデータ連携基盤が稼動するライフサイクルの期間	本項目は継続検討とする。

オ　その他の運用管理方針

表 5-11 その他の運用管理方針

項番	項目	説明	要件
1	内部統制対応	IT 運用プロセスの内部統制対応を行うかどうかに関する項目	TDPF 運営組織の規定に従って、内部統制対応を行う。
2	サービスデスク	ユーザの問合せに対して単一の窓口機能を提供するかどうかに関する項目	マルチベンダのサポート契約を締結するベンダに既存のサービスデスクが存在し、既存のサービスデスクを利用することを想定する。 本項目は継続検討とする。

(4)セキュリティ

本項では、データ連携基盤が果たすべき情報セキュリティの確保に関する要件を記載する。

東京データプラットフォーム情報セキュリティポリシー案に準拠することを原則とし、アクセス制御、アクセス認証、マルウェア対策、侵入・攻撃対策及び不正接続対策等のセキュリティ対策を行う。

また、データ連携基盤が扱うデータについては国内に保管し、関係するポリシー案や規程類に基づき、データが安全に取り扱われるようにするための対策を行う。

ここではセキュリティに対する要件の前提条件、セキュリティリスク分析、セキュリティ診断、セキュリティパッチ適用、アクセス・利用制限、データの秘匿、不正追跡・監視、ネットワーク対策、マルウェア対策及びWeb 対策について示す。

ア　前提条件

表 5-12 前提条件の定義

項番	項目	説明	要件
1	情報セキュリティに関するコンプライアンス	遵守すべき情報セキュリティに関する組織規程、ルール、法令及びガイドライン等が存在するかどうかを確認するための項目	東京データプラットフォーム情報セキュリティポリシー案をはじめとして、TDPF の各ポリシー案に従うこと。

イ　セキュリティリスク分析

表 5-13 セキュリティリスク分析の定義

項番	項目	説明	要件
1	セキュリティリスク分析	システム開発を実施する中で、どの範囲で対象システムの脅威を洗い出し、影響の分析を実施するかの方針を確認するための項目	データ連携基盤が取り扱う全てのデータと利用者の端末及び連携先システムとデータ伝送について、リスク分析範囲として影響分析を行うこと。

ウ　セキュリティ診断

表 5-14 セキュリティ診断の定義

項番	項目	説明	要件
1	セキュリティ診断	データ連携基盤及び各種ドキュメント（設計書や環境定義書及び実装済みソフトウェアのソースコード等）に対して、セキュリティに特化した各種試験や検査の実施の有無を確認するための項目	データ連携基盤の運用開始前及び運用開始後は定期的にネットワーク診断を実施すること。
			データ連携基盤の運用開始前及び運用開始後は定期的に Web アプリケーション対するセキュリティ診断を実施すること。

エ　セキュリティリスク管理

表 5-15 セキュリティリスク管理の定義

項番	項目	説明	要件
1	セキュリティパッチ適用	データ連携基盤の脆弱性等に対応するためのセキュリティパッチ（※1）適用に関する適用範囲、方針及び適用のタイミングを確認するための項目	セキュリティパッチ適用範囲は、データ連携基盤全体に適用すること。
			セキュリティパッチ適用は、全てのセキュリティパッチを適用すること。
			セキュリティパッチの適用は、定期保守作業を実施するタイミングで実施すること。

※1 ソフトウェアにセキュリティ上の弱点（脆弱性）が発見された際に利用者に配布される修正プログラムのこと。

オ　アクセス・利用制限

表 5-16 アクセス・利用制限の定義

項番	項目	説明	要件
1	認証機能	データ連携基盤を利用する利用者及び連携先システムを特定するための認証を実施するか、また、どの程度実施するのかを確認するための項目	ログイン時は登録者及び連携先システムのアカウントを特定して、真正性を証明し、認証を実施すること。 また、個人ユーザ及び連携システムに対して、入会登録申請時及び定期的に多要素認証を実施すること。
2	利用制限	認証された利用者及び連携先システムに対して、データの利用等を、ソフトウェア及びハードウェアにより制限するか確認するための項目	データ連携基盤の各種機能及び取り扱うデータの利用制限について、アカウント情報を基に許可・制限できること。

カ　データ秘匿

表 5-17 データ秘匿の定義

項番	項目	説明	要件
1	データ暗号化	データの伝送時及びデータの蓄積時に秘匿するための暗号化を実施するかを確認するめの項目	データ連携基盤の全ての伝送データを暗号化し、データ伝送を行うこと（HTTPS 等によるデータの伝送を行うこと）。
			データ連携基盤が取り扱うデータ（ログデータ含む。）全てを暗号化し、蓄積すること。

キ　不正追跡・監視

表 5-18 不正追跡・監視の定義

項番	項目	説明	要件
1	不正監視	不正行為を検知するために、それらの不正について監視する範囲や、監視の記録を保存する量や期間を確認するための項目	使用状況ログ等のログを取得すること。なお、アカウント情報に紐づく個人情報は、ログに含めないこと。
			ログ保存期間は 3 年とする。
			データ連携基盤への不正アクセス監視のためのログを取得すること。
			ネットワーク上の不正な通信等の監視のためのログを取得すること。

ク　ネットワーク対策

表 5-19 ネットワーク対策の定義

項番	項目	説明	要件
1	ネットワーク制御	不正な通信を遮断するための制御を実施するかを確認するための項目	ファイアウォール、IPS（Intrusion Prevention System：不正侵入防止システム）（※1）等の導入を行い、不正な通信を遮断する等のネットワーク制御を行うこと。
2	不正検知	ネットワーク上において、不正追跡・監視を実施し、システム内の不正行為や、不正通信を検知する範囲を確認するための項目	データ連携基盤の全てのデータ伝送に対しIDS（Intrusion Detection System：不正侵入検知システム）（※2）等の導入を行い、不正検知を行うこと。
3	サービス停止攻撃の回避	ネットワークへの攻撃による輻輳についての対策を実施するかを確認するための項目	DoS（Denial of Service attack:サービス妨害）攻撃（※3）及びDDoS（Distributed Denial of Service attack：サービス拒否）攻撃（※4）によるサービス停止攻撃に対する対策を行うこと。

※1　外部ネットワークとの通信を監視し、侵入の試みなどの不正なアクセスを検知して攻撃を未然に防ぐシステムのこと。

※2　外部ネットワークとの通信を監視し、攻撃や侵入の試みなどの不正なアクセスを検知して管理者にメールなどで通報するシステムのこと。

※3　大量のデータや不正なデータを送りつけて相手方のシステムを正常に稼働できない状態に追い込む攻撃手法のこと。

※4　インターネット上の多数の機器から特定のネットワークやコンピュータに一斉に接続要求を送信し、過剰な負荷をかけて機能不全に追い込む攻撃手法のこと。

ケ　マルウェア対策

表 5-20 マルウェア対策

項番	項目	説明	要件
1	マルウェア対策	マルウェア（ワーム及びボット等）の感染を防止する、マルウェア対策の実施範囲を確認するための項目	データ連携基盤がマルウェア（ワーム及びボット等）の感染を防止するための、マルウェア対策を実施すること。

コ　Web 対策

表 5-21 Web 対策の定義

項番	項目	説明	要件
1	Web 実装対策	Web アプリケーション特有の脅威、脆弱性に関する対策を実施するかを確認するための項目	データ連携基盤で取り扱うデータの漏洩及び利用者への成りすまし等の脅威に対抗するために、Web サーバに対するセキュアコーディング、Web サーバの設定等による対策の強化を行うこと。
			データ連携基盤に侵入されることによる情報の漏洩及び踏み台等の脅威に対応するために、WAF（Web Application Firewall）（※1）を導入し、侵入抑止及び侵入検知を行うこと。

※1　Web アプリケーションの脆弱性を突いた攻撃に対するセキュリティ対策のこと。

第6章　サービス運用

1 サービス運用一覧

データ連携基盤のサービス運用とは、TDPF データ連携基盤事業を運営していくための、継続的な業務である。

サービス運用では、データ利活用を活性化するために、使いやすさを向上させる取組が必要である。利用者の声を集めて、要望を反映するサイクルを回すための「コミュニティ運営」、データ利活用を推進するためのプロモーション等を行う「企画」が重要となる。

これらを踏まえて、データ連携基盤で必要なサービス運用項目について以下に示す。

表 6-1 サービス運用項目一覧

項番	サービス運用項目	概要
1	サービス運用事務局運営	データ連携基盤の事業運営として、サービス運用全般の管理を行う。
2	ユーザ問合せ	ユーザからの問合せ対応を行う。
3	コンテンツ配信	お知らせ、FAQ、ガイド、マニュアル、技術資料等のコンテンツをポータルサイトに配信を行う。
4	アカウント管理	アカウントのライフサイクル管理（登録、登録拒絶、任意退会、強制退会、利用停止、利用停止解除及び削除）を行う。
5	データ管理	データ提供申請（個別提供契約）の承諾、データ利用申請（個別利用契約）の承諾及び清算を行う。
6	分析	分析結果や統計情報を確認し、サービス向上施策の検討を行う。
7	インタフェース管理	連携するシステムのライフサイクル管理及び接続状態の確認を行う。
8	システム運用	データ連携基盤のシステム運用を行う。 本章 1-(1) システム運用 参照
9	コミュニティ運営	シビックテック及びプロボノ等の団体と連携し、コミュニティの活性化を行う。 データ利活用を活性化する要望事項を集める。

項番	サービス運用項目	概要
10	企画	データ利活用を推進するためのプロモーション等の企画を行う。 シビックテックと連携したアプリコンテスト等のイベントによりデータ利活用の機会を作り、その意見を収集する。
11	ポリシー運用	情報セキュリティポリシー及び利用規約等の更新を行う。
12	認証	ISMS（※1）、プライバシーマーク（※2）等の認証制度の認証取得及び更新・審査の対応を行う。
13	監査	監査への対応を行う。
14	教育	運用管理規定の管理及び運用者への教育を行う。

※1 ISMS(Information Security Management System)：組織の情報セキュリティを管理するための仕組み。

※2 プライバシーマーク：日本産業規格「JIS Q 15001 個人情報保護マネジメントシステム－要求事項」に適合して、個人情報について適切な保護措置を講ずる体制を整備している事業者等を評価して、その旨を示すプライバシーマークを付与し、事業活動に関してプライバシーマークの使用を認める制度。

(1)システム運用

デジタル・ガバメント推進標準ガイドライン、ITIL (Information Technology Infrastructure Library)を基に、データ連携基盤のシステム運用に必要な項目を管理者及び作業者の２つの観点で整理した。

ア　管理者

管理者がシステム運用全体及び個々の活動を適切に計画・管理を行うためのシステム運用項目を以下に示す。

表 6-2 システム運用項目一覧（管理者）

項番	システム運用項目	概要
1	コミュニケーション管理	定例会を開催し、問い合わせ対応状況及びサービス稼働状況について報告する。
2	体制管理	システム運用体制の要員管理及び参加時の手続き・対応を行う。
3	作業管理	月次報告によりシステム稼働状況と運用作業・工数の管理を行う。
4	リスク管理	リスク管理簿による定期チェックと対策を実施する。 リスク管理としてキャパシティ管理を行う。
5	課題管理	問合せや監視により検出された問題のインシデントの管理及び障害対応を行う。
6	システム構成管理	システム資産の管理を行う。
7	変更管理	システム変更管理、対応要否判断及び変更対応の管理を行う。
8	情報セキュリティ対策	年 1 回のセキュリティ診断及び対処並びに SSL サーバ証明書（※1）の更新の管理を行う。 システム担当ベンダはセキュリティの脆弱性情報を収集し、対応する。
9	システム連携先の管理	システム連携先と外部仕様を調整し、API 連携を設定、API のエンドポイントを提供する。 システム連携先との接続状況の確認及びインタフェース更改対応を行う。
10	環境運用	本番環境及び検証環境の運用を行う。 本章 1-(2) 環境運用 参照

※1 Web サイトの「運営者の実在性を確認」し、ブラウザと Web サーバ間で「通信データの暗号化」を行うための電子証明書。

イ　作業者

作業者がシステム運用における定常時対応及び障害時対応を実施するためのシステム運用項目を以下に示す。

表 6-3 システム運用項目一覧（作業者）

項番	システム運用項目	概要
1	サービス監視	ログ、パフォーマンスの監視を行い、問題が検知された場合はエスカレーションを行う。
2	バックアップ運用	システムに応じて定期バックアップを実施。必要に応じてバックアップデータからデータの復旧を行う。
3	メンテナンス	ミドルウェア・ソフトウェアのリリース作業（バージョンアップ等）を行う。 プログラムへの影響調査を行い、必要に応じてプログラム改修を行う。 ※計画停止時に実施 停止を伴う場合、利用者へポータルサイトでのお知らせと、事前にメールで連絡する。
4	システム問合せ対応 （ユーザサポート）	システムの操作及び仕様に関する問合せ対応（平日日勤帯にメールでの対応）。 問い合わせに対するプログラム、データの調査及びデータ抽出等の作業を実施する。

(2)環境運用

データ連携基盤においては、本番運用で使用する「本番環境」及び開発及び検証で使用する「検証環境」の２つの環境を運用する。

表 6-4 環境一覧

項番	環境	概要
1	本番環境	本番運用する環境であり、利用者が使用する。 非機能要件にしたがった構成環境とする。
2	検証環境	開発及び検証用の環境であり、ベンダと TDPF 運営組織が使用する。 必要最小限の冗長構成の環境とする。

2 開発方式

システムをリリースするまでの期間短縮やニーズの取り込みに対応するため、特性に応じた開発方式を採用し、柔軟に開発を進める。各開発方式の概要、特性を以下に示す。

また、リリース前にシステムの使い勝手の観点で課題や改善点を発見するために、テスト工程にてシビックテック等によるユーザ検証を実施する。

表 6-5 開発方式一覧

項番	方式	概要	特性
1	ウォーターフォール型	システムの開発を要件定義、概要設計、詳細設計、製造・単体テスト、結合テスト及び総合テストという工程に分けて、順に段階を経て行う手法。 前の工程には戻らない前提であり、工程管理や資源配分が容易。要件変更が発生した場合に、工程をさかのぼって反映が必要。	スケジュールが決まっており、確定度の高い要件を効率的に実現する場合に有効。
2	アジャイル型	システムの開発を、仕様変更があるという前提で初めから厳密な仕様を決めず、イテレーション（反復）を繰り返して開発を進める手法。 イテレーションとは、開発を小さな単位に分け、計画、設計、実装及び試験を行いながら機能のリリースを繰り返すこと。	短サイクルでリリースが必要なシーンで有効。

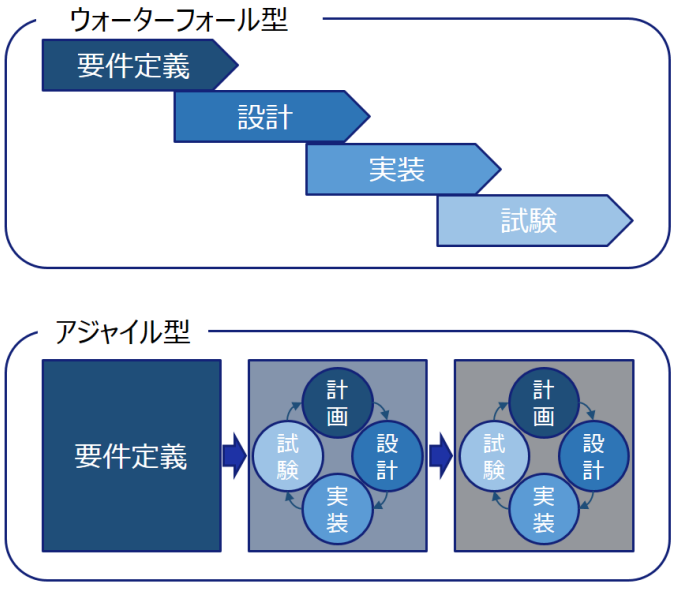

図 6-1 開発方式の進め方

第7章　ロードマップ

令和 4 年度以降適切な時期に設立される TDPF 運営組織がコミュニティ構築及び各事業のモデルづくりを先行で主導し、運営組織の円滑な事業開始につなげる。計画の後半で検討成果などを取り込み、事業基盤の拡充、産学官・他団体及び他 PF との連携を一層強化する。

また、データ流通基盤の実現に向け、図 7-1 に示すとおり、STEP1 は「ユースケース・WG のデータ流通開始」、STEP2 は「データ及び連携先の段階的拡大」、STEP3 は「データ利活用の活性化」を設定し、具体的なアクションを整理し、推進していく。

なお、今後の事業計画や TDPF 協議会などの検討結果に応じて、対応範囲や内容が変更になる可能性がある。

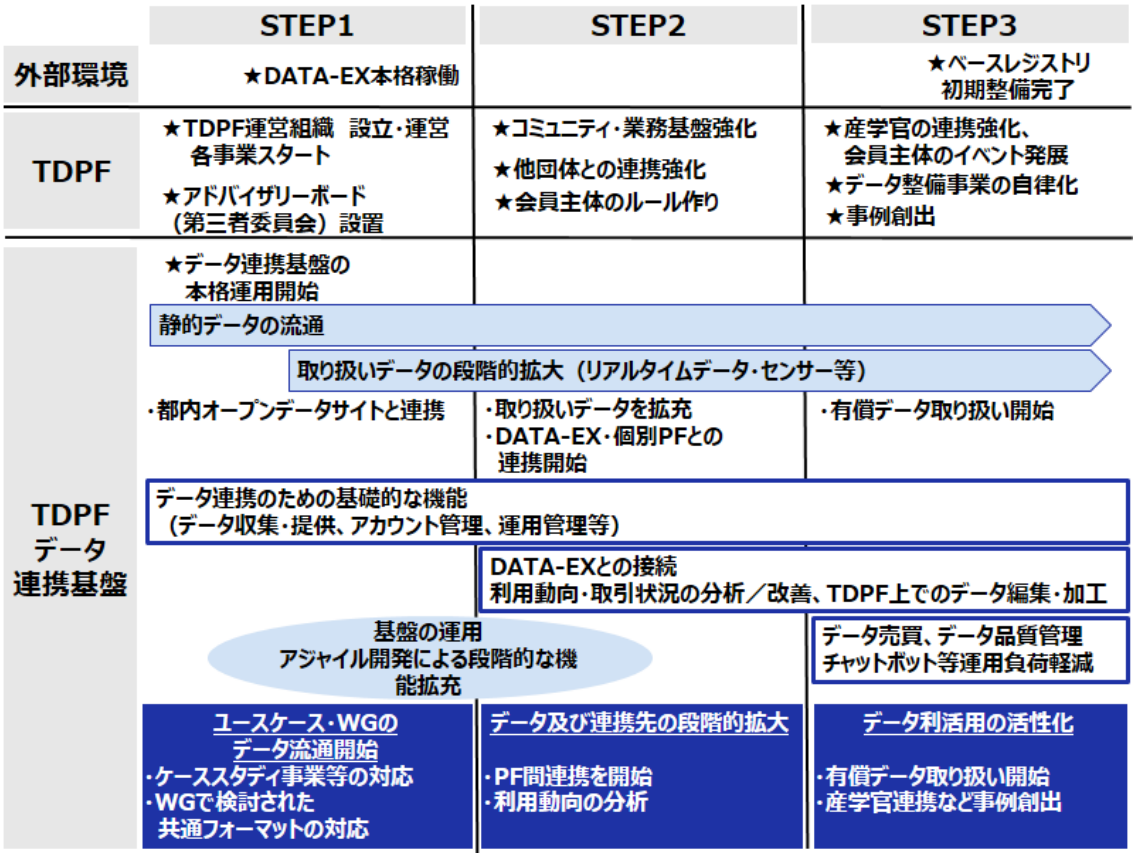

図 7-1 ロードマップ

データ連携基盤の機能ロードマップを以下に示す。STEP1 では、データを流通するために必要となる機能を提供し、STEP2 以降でデータ及び連携先の拡大、データ利活用の活性化に必要となる機能を拡充する。

現時点における各機能の開発・提供する想定時期について、以下に示す。

また、機能ロードマップについても、今後の事業計画及び TDPF 協議会などの検討結果に応じて、対応範囲及び内容が変更になる可能性がある。

表 7-1 機能ロードマップ一覧

○：実施対象、－：対象外

項番	機能群	機能ブロック	機能名	STEP1	STEP2 以降
1	サービス連携（ポータル）	ポータル	利用者ポータルサイト	○	○ ※1
2			開発者ポータルサイト	－	○
3			コミュニティポータルサイト	－	○
4			運用者ポータルサイト	○	○ ※1
5	サービス連携（API）	API 管理	API ライフサイクル管理	○	－
6			API ゲートウェイ	○	－
7	認証	認証・認可	認証	○	○ ※2
8			認可	○	－
9		アカウント管理	ユーザ管理	○	○ ※1
10			ロール管理	○	－
11	データマネジメント	データ管理	登録データ管理	○	○ ※3
12			分散データ管理	○	－
13			イベント管理	○	－
14	外部データ連携	認証系 API	認証・認可	○	○ ※4
15			属性取得	－	○

項番	機能群	機能ブロック	機能名	STEP1	STEP2 以降
16		データマネジメント系 API	データアクセス	○	–
17			パブリッシュ/サブスクライブ	○	–
18			データ仲介	○	–
19		サービス連携	カタログ管理	○	–
20		データ伝送	プロトコル変換	○	–
21		データ処理	データ変換	○	–
22			データ受付	○	–
23			データ取得	○	–
24			データ補完	○	–
25	アセットマネジメント	システム管理	システムライフサイクル登録	○	–
26			システム状態管理	○	–
27	PF 間連携 （相互運用性）	認証連携	認証連携	–	○
28		データ連携	データ連携	–	○
29		分野間連携	分野間データ検索	–	○
30			分野間データ交換制御	–	○
31			分野間データ交換記録	–	○
32	共通	可視化・分析	可視化・分析ダッシュボード	–	○

※1 有償でのデータ（利用権）取引

※2 個人ユーザの本人確認書類での本人証明

※3 データ提供履歴の追跡機能（データ提供履歴の記録は STEP1 で対応）

※4 DATA-EX 及び他 PF との相互運用に係る機能

第8章　　終わりに

要件定義書初版では、都が社会実装の実現を目指すデータ連携基盤について、概要（第 1 章）、業務要件（第 2 章）、システム概要（第 3 章）、システム要件（第 4 章）、非機能要件（第 5 章）、サービス運用（第 6 章）及びロードマップ（第 7 章）を整理した。

今後、TDPF 協議会での提言、TDPF 関連事業からのフィードバック及び国や各関連団体の動向を踏まえつつ、データ連携基盤の構築に向けた具体的なステップやアクションを検討し、逐次更新を重ねていく。

参考文献

・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
（デジタル庁、内閣府知的財産戦略推進事務局、2022 年 3 月 4 日）
・「デジタル社会の実現に向けた重点計画」別紙「包括的データ戦略」
（内閣官房情報通信技術（ＩＴ）総合戦略室、2021 年 6 月 18 日）
・スマートシティリファレンスアーキテクチャ
（戦略的イノベーション創造プログラム（SIP）、第 1 版 2020 年 3 月 31 日）
・デジタル・ガバメント推進標準ガイドライン
（内閣官房情報通信技術（ＩＴ）総合戦略室、2021 年 3 月 30 日）
・非機能要求グレード 2018
（独立行政法人情報処理推進機構（ＩＰＡ）、2018 年 4 月）
・「情報システム運用時の定量的信頼性向上方法」に関する調査報告
（独立行政法人情報処理推進機構（ＩＰＡ）、2015 年 4 月 16 日）

継続検討事項

令和４年度に要件定義書を改版するにあたり、主な継続検討事項を以下に挙げる。

継続検討項目一覧

項番	継続検討項目	課題
1	外部データをデータ連携基盤へ内包するカタログの選定及び実現方式	東京都オープンデータカタログサイトを含む他のカタログサイトの情報をデータ連携基盤のカタログに内包する場合の実現方式については、使用するソフトウェア（CKAN 等）の特性や内包するカタログを選別する等の業務要件により選定する。
2	オープンデータ及びシェアードデータで異なる管理が必要なデータ項目	カタログ情報として登録する情報のうち、オープンデータ及びシェアードデータで異なる管理が必要なデータ項目（シェアードデータの公開範囲等）を明確にする。
3	データのトラストとして扱うデータ評価項目	データのトラスト向上のため、データに対する信頼性の評価項目を検討する（現時点では、データのダウンロード数の表示及びリンク切れの検出を想定している）。
4	トランザクションのトラスト	データ連携基盤の付加価値として、トランザクションのトラストであるデータの提供履歴（いつ誰にどのようなデータを渡したかトレースできること）の保証について実現方法を検討する。
5	有償データの取扱い	有償データの利活用性向上のため、データ利用権としての提供及びデータ利用時の条件指定（データの範囲及び必要な情報項目の指定等）等の利用者のニーズに合わせた多様な提供方法を検討する。 また、請求業務の具体化が必要であるため、事業計画の進捗に合わせて検討する。
6	共通フォーマットとして扱うデータフォーマット及び登録を促進する仕組み	データ利用の利便性向上を目的として、同様の分野のデータに対してデータ提供者が複数存在する場合、データを集約するための共通フォーマットが必要となる。そのため、データ連携基盤が対応するデータフォーマットの検討及びデータ項目のチェック内容の具体化を行う。 また、データ提供者に共通フォーマットでのデータ提供を促す仕組みを検討する。

項番	継続検討項目	課題
7	相互運用先（DATA-EX、他のPF等）との接続要件の検討	DATA-EXや他のPFとの接続要件については、分野間データ連携基盤の進捗やユースケースに応じて、技術的仕様及び運用性の観点で検討を進める。
8	分析施策の選定	データ連携基盤のサービス向上のため、利用動向及び取引状況等から採用するデータ分析施策を検討する。
9	非機能要件	事業計画及び社会的重要度の変化に柔軟に対応し、継続的に非機能要件を検討する。