

データ連携基盤
要件定義書
【中間案】

令和 6 年（2024 年）7 月

【目次】

1.	システム開発の基本事項.....	4
1-1	背景.....	4
1-2	情報システムの市役所 DX モデル.....	4
1-3	対象範囲・業務.....	5
1-4	関連システム・インフラ基盤.....	6
1-5	システムの前提・制約条件.....	9
2.	システムの機能要件.....	10
2-1	機能概要.....	10
2-2	共通機能一覧.....	10
2-3	インターフェース一覧.....	11
3.	システムの非機能要件.....	12
3-1	可用性設計.....	12
3-2	性能・拡張性設計.....	12
3-3	運用・保守性設計.....	12
3-4	セキュリティ設計.....	13

改定履歴

No.	修正日	修正内容	修正者	版数
1	-	新規作成		中間案
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

1. システム開発の基本事項

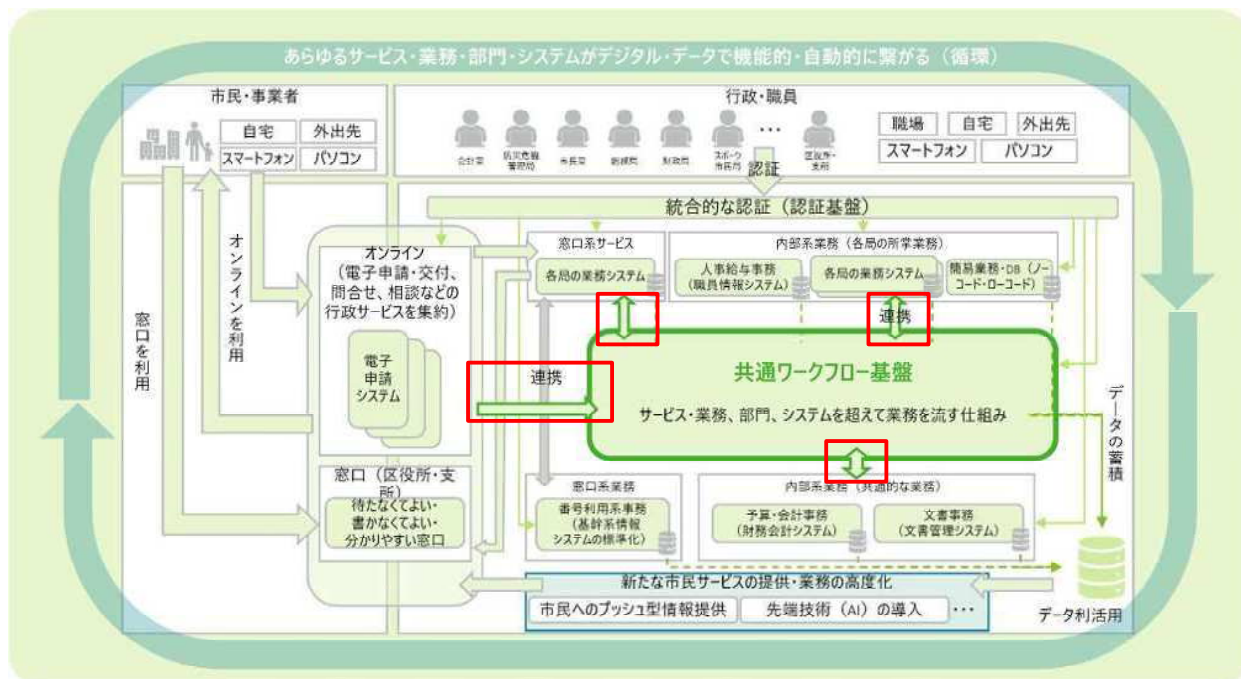
本要件定義書は、共通ワークフロー基盤（以下「共通 WF 基盤」という。）の一部であるデータ連携基盤について、令和 8 年度の稼働時に必要な要件を定めるものである。

1-1 背景

本市では個別最適化された要素（縦割りに分断しているサービス・業務・部門・システム）を、全体最適の視点で繋ぎなおし、デジタル化されたあらゆるサービス・業務・部門・システムが機能的に繋がることで、これまではできなかった新たなサービス・業務を展開することを目指し、「情報システムの市役所 DX モデル」（以下「市役所 DX モデル」という。）に基づく情報システムの整備・運用を行っていることとしている。

市役所 DX モデルの実現に向けて、共通 WF 基盤を活用し、サービス・業務、部門、システムを超えて業務を流す仕組みを構築するため、データ連携基盤の要件を定めるものである。

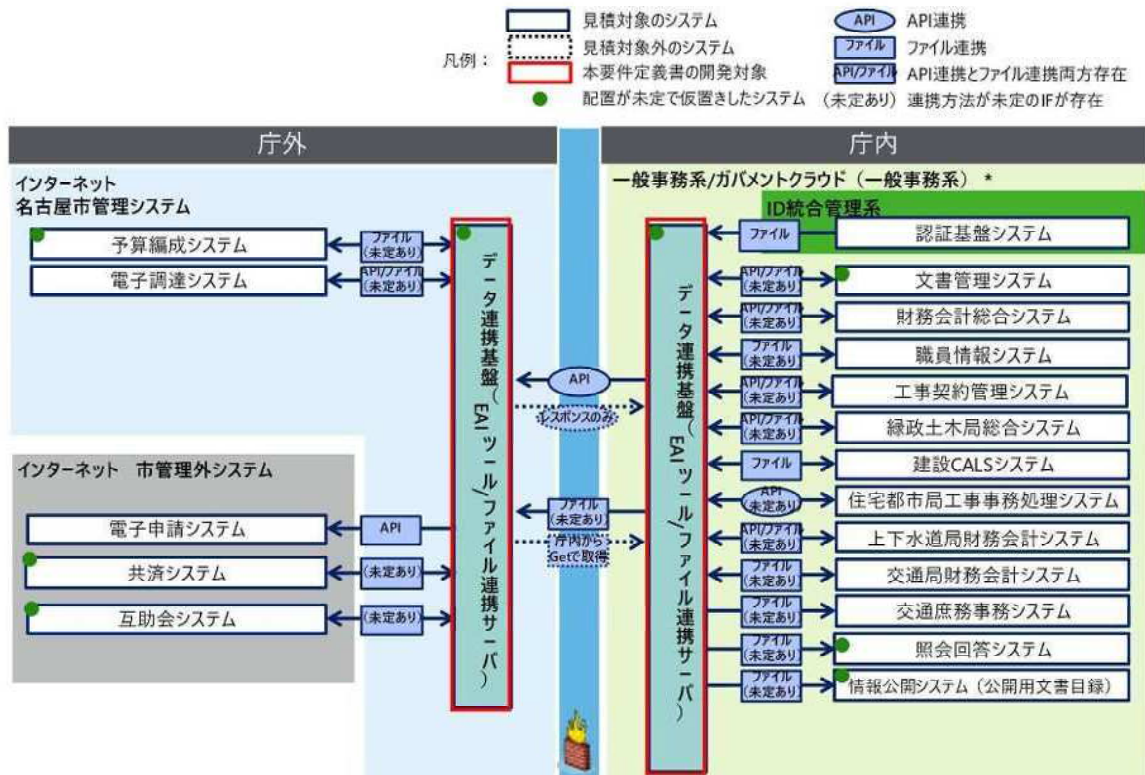
1-2 情報システムの市役所 DX モデル



・・・本書に該当する範囲

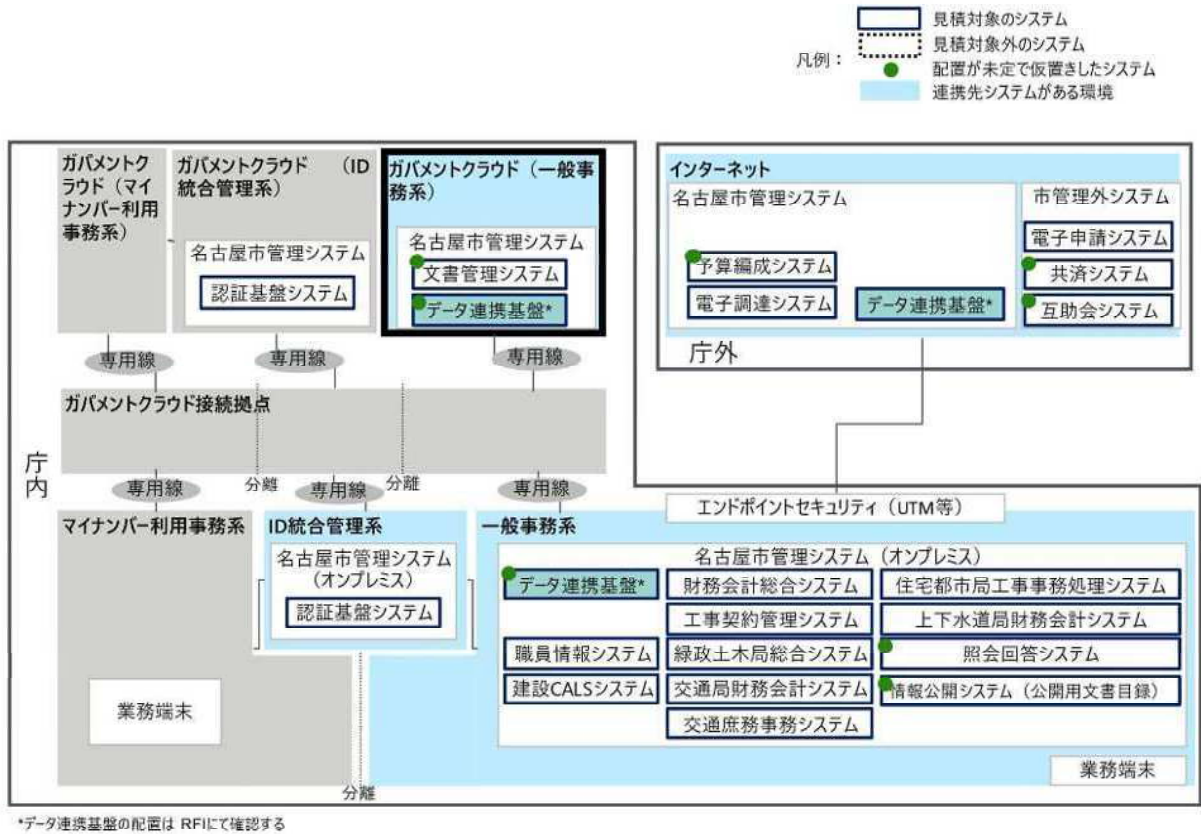
1-3 対象範囲・業務

本要件定義書における対象は以下のシステム関連図において、データ連携基盤（EAI ツール/ファイル連携サーバ）と記載された箇所である。



1-4 関連システム・インフラ基盤

データ連携基盤稼働開始時点（令和8年度）のネットワーク構成図は以下の図と表の通りである。



No	区分	ネットワーク名	説明
1	庁内	ガバメントクラウド（マイナンバー利用事務系）	マイナンバーを扱う業務システムを設置するための政府共通のクラウド利用環境を用いた庁内ネットワーク（庁内環境とは専用線を使い接続されている）
2		ガバメントクラウド（ID 統合管理系）	ID 統合管理系システムを設置するための政府共通のクラウド利用環境を用いた庁内ネットワーク（庁内環境とは専用線を使い接続されている）
3		ガバメントクラウド（一般事務系）	一般事務を扱うシステムを設置するための政府共通のクラウド利用環境を用いた庁内ネットワーク（庁内環境とは専用線を使い接続されている）
4		ガバメントクラウド接続拠点	各庁内ネットワークと各庁外ガバメントクラウドを専用線で接続するための拠点
5		マイナンバー利用事務系	マイナンバーを扱う業務システム・端末を設置

			するための庁内ネットワーク
6		ID 統合管理系	ID 統合管理系システムを設置するための庁内ネットワーク
7		一般事務系	マイナンバーを扱う業務及び ID 統合管理業務を除く、一般事務業務を扱う業務システムを設置するための庁内ネットワーク
8	庁外	インターネット	パブリッククラウド上に構築された市のサービスを提供するネットワーク

データ連携基盤の連携対象とするシステムは以下の表の通りである。ただし、将来的な連携対象システムは以下の表の限りではない。

No	システム名	説明	配置ネットワーク
1	予算編成システム	予算要求、集計作業、議案等の予算編成に関する資料を作成するシステム	インターネット (未定)
2	電子調達システム	入札やそれに関連した入札参加者登録(業者登録)や入札情報の公開を電子(インターネット経由)で行うシステム	インターネット
3	電子申請システム	国のデジタル手続法や名古屋市 ICT 活用に関する基本方針等に基づき、行政手続のオンライン化を推進するために、行政手続のオンライン化に必要な機能を備えたシステム	インターネット
4	共済システム	市管理外システム	インターネット (未定)
5	互助会システム	市管理外システム	インターネット (未定)
6	認証基盤システム	パソコンのログオン時の ID 管理・認証、業務システムへのシングルサインオン(SSO)機能の提供により統合的な認証を行うシステム	ID 統合管理系
7	文書管理システム	行政文書の収受、起案、決裁、保存、廃棄等の事務の処理及び行政文書に係る情報の総合的な管理を行うシステム	一般事務系
8	財務会計総合システム	財務事務に関する法令に基づき、予算データの管理から予算執行、決算管理に至る一連の財務会計事務(企業会計を除く。)、物品出納事務を処理するシステム	一般事務系
9	職員情報システム	職員の人事・給与情報を管理するシステム	一般事務系
10	工事契約管理システム	財政局担当局長(契約監理)に委任された工事契約の締結に関する事務を行うシステム	一般事務系
11	緑政土木局総合	緑政土木局の積算業務及びデータ管理、各種事務処理の	一般事務系

	システム	事務及びデータ管理を行うシステム	
12	建設 CALS システム	電子化された工事等の図面・施工写真等納品物を一元管理し、公共事業執行に関する事務や緑政土木局が所管する施設情報の管理を行うシステム	一般事務系
13	住宅都市局工事事務処理システム	住宅都市局の発注案件実績管理、入札・契約実績管理、施設台帳管理、アスベスト情報管理を行うシステム	一般事務系
14	上下水道局財務会計システム	予算管理、契約監理、固定資産管理等の上下水道局の企業会計全般を管理するシステム	一般事務系
15	交通局財務会計システム	バス、地下鉄両事業の予算管理、決算管理、固定資産管理等交通局の企業会計全般を管理するシステム	一般事務系
16	交通庶務事務システム	交通局職員の勤務、人事、諸手当および被服の貸与履歴を管理するシステム	一般事務系
17	照会回答システム	未実装だが構築について検討中	一般事務系
18	情報公開システム（公開用文書目録）	未実装だが構築について検討中	一般事務系

1-5 システムの前提・制約条件

「共通ワークフロー基盤にかかるガバナンス方針書」に基づき、共通 WF 基盤にかかる取り組みを組織横断で継続的に推進するグループを推進 G という。データ連携基盤導入時における、開発サイクルごとの推進 G とシステム所管課の実施事項は以下の表の通りである。

No	開発サイクル	推進 G 実施事項	システム所管課実施事項
1	業務要件定義	● データ連携基盤で実施するデータ連携・変換の内容等（インターフェース一覧）を取りまとめ	● データ連携基盤で実施するデータ連携・変換の内容等（インターフェース一覧）を、推進 G に共有
2	システム要件定義	● データ連携基盤要件定義書の作成 ● データ連携開発・運用標準（システム間連携要件標準仕様書を含む。）の作成	● データ連携基盤要件定義書及びデータ連携開発・運用標準の確認、フィードバック
3	設計	● データ連携基盤要件定義書に基づく基本設計・詳細設計	● 連携インターフェースなどの基本設計・詳細設計
4	構築	● 設計に基づくデータ連携基盤の構築	● 連携インターフェースなどの構築
5	テスト	● データ連携基盤のテスト実施及び連携インターフェースなどのテスト計画・支援 ・ 単体テスト ・ 結合テスト ・ 総合テスト	● 連携インターフェースなどのテスト実施 ・ 単体テスト ・ 結合テスト ・ 総合テスト
6	リリース	● データ連携基盤リリース	● 連携インターフェース等リリース ● 本番環境モジュールへの移送
7	運用	● 保守・運用	● 保守・運用

2. システムの機能要件

2-1 機能概要

庁外・庁内向けに以下の機能を実装すること。

なお、以下に記載しているトリガとは、今回の開発では API の呼び出し、ファイル転送コマンドの実行、ジョブの実行を想定している。今後の拡張性として、DB 更新、ファイル更新、メッセージキューなどにも対応する可能性がある。

(1) データ連携基盤（庁外）の機能

(ア) 連携先システム（庁外）からの連携データ等受信

データ連携基盤（庁外）を用いて、連携データを取得する。

(イ) 連携先システム（庁外）への連携データ等送信

データ連携基盤（庁外）を用いて、連携データを送信する。

(ウ) データ連携基盤（庁内）からの連携データ等受信

データ連携基盤（庁内）側がトリガとなる連携により連携データを受信する。

(エ) 連携ツール（庁内）への連携データ等送信

データ連携基盤（庁内）側がトリガとなる連携により連携データを提供する。

(2) データ連携基盤（庁内）の機能

(ア) 連携先システム（庁内）からの連携データ等受信

データ連携基盤（庁内）を用いて、連携データを取得する。

連携先システム（庁内）側がトリガとなる連携により、連携データを受信する。

(イ) 連携先システム（庁内）への連携データ等送信

データ連携基盤（庁内）を用いて、連携データを送信する。

連携先システム（庁内）側がトリガとなる連携により、連携データを提供する。

(ウ) データ連携基盤（庁外）からの連携データ等受信

データ連携基盤（庁内）を用いて、連携データを取得する。

(エ) データ連携基盤（庁外）への連携データ等送信

データ連携基盤（庁内）を用いて、連携データを送信する。

2-2 共通機能一覧

データ連携基盤の機能を以下に示す。

(1) API によるデータ連携

API により JSON、バイナリまたは XML 形式でのデータ連携を行うこと。

連携元システムの認証は API キーを使用すること。連携先システムへの認証は API キー又は JWT を使用する認証に対応すること。ただし、JWT を使用する認証においては、認証プロバイダーなどを連携先システム又は連携元システムにおいて用意するものとする。

(2) ファイルによるデータ連携

SFTP などのファイルによるデータ連携手法により CSV、txt またはバイナリ形式などでのデータ連携を行うこと。

(3) メールによるデータ連携

メール形式やメールの添付ファイルとしてデータ連携を行うこと。

(4) データ変換

連携元から抽出したデータに対し、連携先の要件に合わせたデータの分割・統合や文字コードの変換、プロトコルの変換などを行うこと。

(5) ジョブスケジューリング機能

ジョブの起動の制御やジョブの実行・終了状態の監視・報告を行うこと。

(6) 非同期連携機能

接続先のメンテナンス時間や要件を考慮して、連携元から連携先へ非同期でデータ連携が可能となるようデータ連携基盤で受信データを保持し、定められたタイミングで連携先へデータを送信できる機能を有すること。

(7) エラーハンドリング機能

通信の障害や連携先サーバの障害が発生してデータ連携が行えなかった場合に、指定した回数・間隔でリトライを行えること。

データの不整合、通信障害、サーバ障害などを検知した場合はエラーログを生成し、メールやコミュニケーションツール、API により通知すること。

(8) セキュリティ機能

データの暗号化、連携元システムの認証、アクセス制御を行うこと。加えて、セキュリティ監査、ログ管理機能を提供すること。詳細は 3-4. セキュリティ設計を参照のこと。

2-3 インターフェース一覧

データ連携基盤で実現する IF の機能概要及び連携方式は、別紙「インターフェース一覧」を参照のこと。

3. システムの非機能要件

3-1 可用性設計

(1) 継続性

本システムのスコープにおいては冗長化構成をとることにより、障害発生時のサービス切り替え時間は 60 分未満を目標とすること。障害が起きた箇所を復旧し、冗長構成全体が通常通りの状態になるまでの障害復旧対応時間は 24 時間とすること。目標復旧水準は障害発生時点（日次バックアップ+アーカイブからの復旧）とし、稼働率は 99.9%を目指すこと。

(2) 災害対策

本システムはパブリッククラウド上にシステムを構築する前提であるが、マルチリージョンには対応しない。

(3) 耐障害性

定められた一定の連携の開始から完了までは処理データを保持し続け、エラーが起きた場合やレスポンスが遅れた場合にデータを損なわないようにすること。

3-2 性能・拡張性設計

(1) 業務量

令和 8 年度においてはインターフェース一覧にある業務量を処理する性能が必要であり、見積誤差を考慮して、全体としてその 1.2 倍の量を処理できるようにリソースを用意すること。その後、数年にわたり連携するシステムや処理量が数倍になるため、処理量増に対してはアーキテクチャの変更、プログラムの改修変更（設定変更は可とする）を必要とせず、リソースを増やすことで対応できる構造とすること。

(2) 連携先システムや連携データの増加

前述のとおり、本開発後継続して連携するシステムが増加し、それに伴って連携されるデータも増加していく。その際に、本システムへの改修を少なくするため、拡大を見越した設定、共通機能や再利用可能な機能の開発を行うこと。

(3) 性能目標値

インターフェース一覧にあるそれぞれの性能目標を全体として満たすように設計を行うこと。

3-3 運用・保守性設計

(1) 運用時間

原則として、24 時間 365 日の常時利用を可能とすること。ただし、保守等のための計画停止を除く。

(2) 運用監視

運用監視として以下を行うこと。

死活監視：対象のステータスがオンラインの状態にあるかオフラインの状態にあるかを判断する

監視し、異常がありシステム継続ができない場合にはシステム管理者へ通知し、対応を開始できるようにすること。

エラー監視：対象が出力するログ等にエラー出力が含まれているかどうかを判断し、エラー内容によってはシステム管理者へ通知し、対応を開始できるようにすること。

リソース監視：対象が出力するログや別途収集するパフォーマンス情報に基づいて CPU やメモリ、ディスク、ネットワーク帯域といったリソースの使用を確認できるようにすること。

パフォーマンス監視：対象が出力するログや別途収集するパフォーマンス情報に基づいて、業務アプリケーションやディスク I/O、ネットワーク転送等の応答時間やスループットについて確認できるようにすること。

(3) 保守運用

点検作業やパッチあて作業等を計画し、実行できるようにすること。

(4) 運用環境

本番リリース前までに他システムと接続し、本番と同等のスケジュールでの試験や単体での性能試験を行うためそれに応じた環境を用意すること。本番リリース後には、不具合の改修や解析のために本番環境とは別に検証環境を用意するが、この検証環境はテスト対象の処理量や目的に応じた適切なサイジングや運用時間を制御することでコストダウンをはかること。

3-4 セキュリティ設計

- (1) 名古屋市情報あんしん条例（16 年名古屋市条例第 41 号）、名古屋市個人情報保護条例（17 年名古屋市条例第 26 号）その他関係法令や、名古屋市情報セキュリティ管理基準、名古屋市情報セキュリティ対策基準などの市のセキュリティポリシーを遵守するとともに、下記（ア）から（オ）に掲げる要件を満たすこと。

（ア）情報システム及びネットワークの管理

本システムへの不正アクセスを防止・検知する機能をもつこと。データ連携基盤へのアクセスログを 1 年は保存し、必要に応じて確認できる状態にすること。

（イ）ネットワークの接続制御、経路制御、接続制限

接続先は限定されるため、最低限の通信のみを許可すること。外部及び内部からの不正アクセスを防止する対策を講じること。情報の改ざん、破壊、盗聴、漏えい等を防止する対策を講じること。通信、データベース及びバックアップデータを暗号化すること。

（ウ）データのバックアップ

データやプログラム等の滅失、毀損に備えて、取り扱う電子情報を定期的にバックアップすること。

(エ) 脆弱性診断の実施

アプリケーション診断及びプラットフォーム診断を行うなど、ウェブアプリケーションや、ネットワーク機器・OS・サーバ・ミドルウェア等に脆弱性がないことを確認し、最新バージョン又はベンダーのサポートが受けられるバージョンを利用すること。定期的にセキュリティパッチ等を適用すること。緊急性の高いセキュリティパッチはシステムへの影響を確認後速やかに適用すること。

(オ) 庁内セキュリティポリシー

本市にて導入しているウイルス対策ソフトウェアや EDR の導入が可能であること。

(カ) 庁外－庁内間のセキュリティ条件

庁外から庁内へのインバウンド通信は行えない条件として構築すること。仮にインバウンド通信を必要とする場合には、その対応によりセキュリティ上、世間一般的に妥当と思われる対策を提案すること。

[illegible]