

吹田市新共通基盤システム構築
(標準化対応)
共通基盤システムの活用方針

1.0 版

吹田市
令和 7 年(2025 年)12 月

改版履歴

版数	制定／改訂 ／廃止日	該当頁 該当項目	制定理由／改訂の要点／廃止 理由	承認	査閲	作成
1.0 版	2025/12/26	全頁	新規作成	和田	水谷	玉置

目次

1	共通基盤システムの機能概要	1
(1)	はじめに	1
(2)	共通基盤システム構築の目的	1
(3)	提供機能一覧	2
2	提供機能説明	5
(1)	認証・ポータル機能	5
(2)	システム間連携・変換機能	7
(3)	統合データベース機能	7
(4)	統合運用管理機能	14
(5)	文字管理機能	18
(6)	共通印刷機能	18
(7)	EUC・帳票作成機能	21
(8)	ファイル共有機能	21
(9)	統合ハードウェア	22
(10)	シンククライアント・FAT クライアント	28
(11)	セキュリティ	31
(12)	中間サーバー連携機能	31
(13)	標準連携用オブジェクトストレージ機能	32
(14)	認証認可機能	32
3	導入プロセスと提供サービス	33
(1)	導入準備フェーズ	33
(2)	構築フェーズ	33
(3)	運用フェーズ	34

1 共通基盤システムの機能概要

(1) はじめに

本書は、共通基盤システムの概要について記載したものである。共通基盤システムのサービス／機能を利用する場合や共通基盤連携を実施するにあたっては、本書を参照し、適切に対応を実施すること。

(2) 共通基盤システム構築の目的

各システムには、セキュリティ対策やバックアップなど、共通的に実装する機能が存在する。これらの機能を各システムに実装すると重複投資となり、開発コストの増加や運用の煩雑化を招く原因となる。

また、各システム間では住記情報や税情報など、他システムとの情報連携が数多く存在する。各システム間で直接連携をすると、制度改正などで一方のシステムが改修になった場合に、連携するシステムにも影響が及び、運用コストの増加やシステムの複雑化を招く原因となる。

これらの問題を解決するため、システム間で共通的に使用する機能や情報連携を一元管理する共通基盤システムを構築する。

共通基盤システムの導入により、各システム間の結合度を下げ、制度改正時などのシステム改修による他システムへの影響を低減させるとともに、共通機能を一元管理することによって、トータルコストの適正化と運用の効率化を実現することを目的とする。

(3) 提供機能一覧

ア 共通基盤システムが提供する機能を以下に示す。各機能の詳細は、2章以降に記載する。

表 1-1 共通基盤システム提供機能一覧

項番	機能名	機能概要
1	認証・ポータル機能	・二要素認証 SJ系 FAT 端末にログインするための顔認証機能、及びポータルログインにおけるシングルサインオン(SSO)機能を提供する。 ・ポータル 業務システムを起動するためのポータル画面及び認証成否や起動業務システムのログ出力、管理を行う。
2	システム間連携機能	業務システム間でのデータ連携基盤としてデータ授受機能を提供する。その際連携が正しく行われたか、どのような連携が行われたかログ出力する。 またファイル連携の際には文字コード、業務コード等の変換機能を提供する。
3	統合データベース・共通データ管理機能	各業務システムが管理するデータを統合し、副本として管理する。市が保有する各種情報を有効活用するために使用可能とする。
4	統合運用管理機能	統合運用管理機能として、共通基盤システムは、システム監視、通報機能、ジョブ管理、バックアップを提供する。
5	外字管理機能	外字の登録、配信を行い、外字の一元管理を実現する。 (標準化前における)吹田市明朝の文字フォントは MS 明朝、文字セットは、JIS X 0213:2004、文字コードは Unicode とする。
6	共通印刷機能	業務システムが出力する帳票(印刷ジョブ)を集中管理し、印刷ジョブの再印刷及び印刷履歴ログを出力、管理する。
7	EUC・帳票作成機能	EUC・帳票作成機能については、各室課からの依頼を受け、統合運用業者及び吹田市行政経営部デジタル政策室が使用する。本書での詳細は割愛する。
8	ファイル共有機能	利用者間のデータのやり取りを行う上でのデータ保管場所(共有フォルダ)を提供する。このファイル共有は Active Directory (以下、「AD」という。)による共有フォルダ機能を利用した権限管理、アクセス管理を行う。
9	統合ハードウェア	仮想化技術を用いたハードウェア統合により、ハードウェア設置場所の省スペース化を図る。また、複数のシステムでハードウェアを共有することで、必要な電気代の削減を行う。原則、(標準準拠外または特定移行支援となる)業務システムは、共通基盤システムから提供された環境に構築する。
10	クライアント管理	SJ 系端末として、ローカルに個人情報を持たない仮想化端末を導入し、セキュリティの向上を図る。
11	セキュリティ管理機能	セキュリティ管理機能として、ウイルス対策機能、パッチ適用機能を提供する。また、ログの統合管理機能を提供する。
12	中間サーバ連携機能	各業務システム(標準準拠システム)が中間サーバーと連携する際に、住民・住登外者を一意に特定する団体内統合宛名番号を付番するとともに、団体内統合宛名番号に係る副本情報等を標準準拠システムから受信し、中間サーバーに送信する機能(中間サーバーコネクタ)を提供する。
13	標準連携用オブジェクトストレージ機能	標準化対応後の各業務システムに対して、標準連携で利用するオブジェクトストレージ(AWS の S3 バケット)を提供する。

14	認証認可機能	AWS 以外の環境 (本庁内、AWS 以外の CSP) から標準連携用オブジェクトストレージを利用するための認証認可機能を提供する。
----	--------	--

- イ 共通基盤システムの全体イメージを以下に示す。
 -なお、各機能の番号は表 1-1 の項番と対応している。

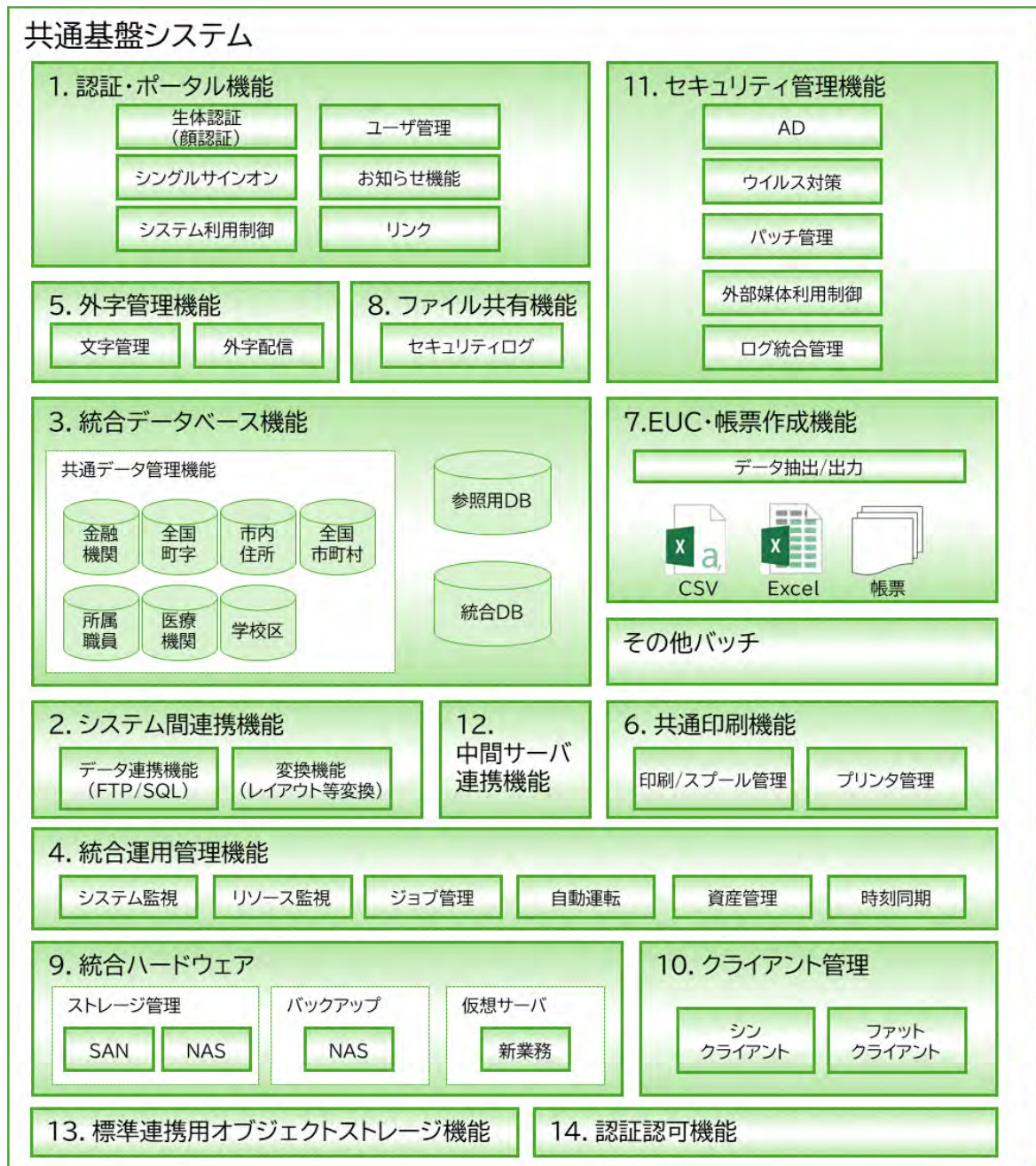


図 1-1 共通基盤システム 全体イメージ図

2 提供機能説明

共通基盤システムが提供する機能について、機能ごとに記載する。あわせて、業務システム側が共通基盤システムを利用するための要件も記載する。

(1) 認証・ポータル機能

ア 機能説明

(ア) 共通基盤システム実装機能

共通基盤システムでは認証・ポータル機能として以下の機能を実装する。

表 2-1 認証・ポータル機能一覧

機能名	概要
ログイン画面	ポータル画面を開くためのログイン画面。事前に顔認証にて端末にログインを行い、シングルサインオンにてログインを行う。
生体認証	顔認証による認証機能。
ポータル画面	業務システムへのリンクを表示する画面。 業務システムへのリンクは、全利用者で共通の表示となる。
ユーザ ID 送信	シングルサインオンのために、業務システムに対して POST メソッドによりユーザ ID を送信する ¹ 。
アクセスログ出力	認証成否ログ、ポータル画面の操作ログや誰が、いつ、どの業務システムを起動したかをログ出力する。
ユーザ情報管理	ユーザ ID や認証情報等のユーザ情報を一元管理する機能。
お知らせ	ポータル画面に基幹系システム利用者に向けたお知らせを表示する機能。 お知らせは、全利用者で共通の表示となる。

(イ) 処理フロー

認証・ポータル機能を用いた業務システム起動までの流れは以下となる。

表 2-2 認証・ポータル起動の流れ

処理 順序	処理内容	補足
1	Windows ログイン	SJ ネットワーク ² 内で使用する Windows クライアント OS へのログインとなる。SA ネットワーク ³ 内の Windows クライアント OS は共通基盤システムの対象外となる。
2	ポータル画面ログイン	共通基盤システムのログイン画面を起動し、シングルサインオン認証を行う。認証成功時にポータル画面が表示される。Windows ログインとは別にログインを行う。
3	業務システム起動	業務システムへのリンクをクリックすると別ウィンドウでブラウザが起動される。起動されたブラウザから、業務システムに対して、HTTP リクエストが POST メソッドで送信される。POST メソッド中にユーザ ID が含まれており、業務システムは、ユーザ ID を取得して業務システムを起動することになる ¹ 。

¹ Microsoft Edge の仕様により IE モードでのみ有効な機能となる。

² 基幹系システムが稼動する住民情報系ネットワークを指す。

³ 本市内部事務系ネットワークを指す。SJ ネットワークと SA ネットワークは別セグメントである。

イ 業務システムに求める要件

業務システムを起動する場合、以下の要件を満たすこと。

- 業務システムの起動は、共通基盤システムが提供するポータル画面から行うこと。
- 業務システムを起動するための URL を統合運用管理者に通知すること。
- ポータル画面から業務システムを起動する際は、ユーザ ID の入力等の操作を行わずに業務システムを起動できること。
- 業務システムを起動する場合のユーザ ID は、共通基盤システムが POST メソッドで送信するユーザ ID を取得して操作者を判断すること¹。
- なりすましやポータル画面以外からの不正アクセスを防止するため、共通基盤システムが提示するセキュリティ確保のための機能を有すること。
- 具体的な対応内容については、セキュリティの関係上、本資料では記載しない。共通基盤システム が提示するセキュリティを確保するための機能実装のための対応工数を見込むこと。
- ポータル画面では、全業務システムの起動リンクが表示される⁴。業務システムでは、操作者に対する利用権限のチェックを行い、業務システムの利用可否を判断すること。
- ポータル画面から業務システムを起動する際、ポータル機能では業務システムの画面サイズ等の指定は行わない。業務システムで適切な画面をオープンする必要がある場合は、業務システムで画面サイズ等のウィンドウ制御を行うこと。
- 万一ポータル画面が使用できない場合等に備え、共通基盤システムのポータル画面以外からも業務システムにログインできる機能を有すること。業務システム独自のログイン機能は、ユーザ ID の指定が可能であり、業務システムにログインしたことが分かるよう、アクセスログを出力できること。
- シングルサインオンの際は、共通基盤からユーザ ID が連携できること。なお、ユーザ ID は POST メソッドで送信する¹。

⁴ ポータル画面ではログインユーザが使用可能な業務システムリンクのみを表示する、といった表示制御を行わない

(2) システム間連携・変換機能

(3) 統合データベース機能

ア 機能説明

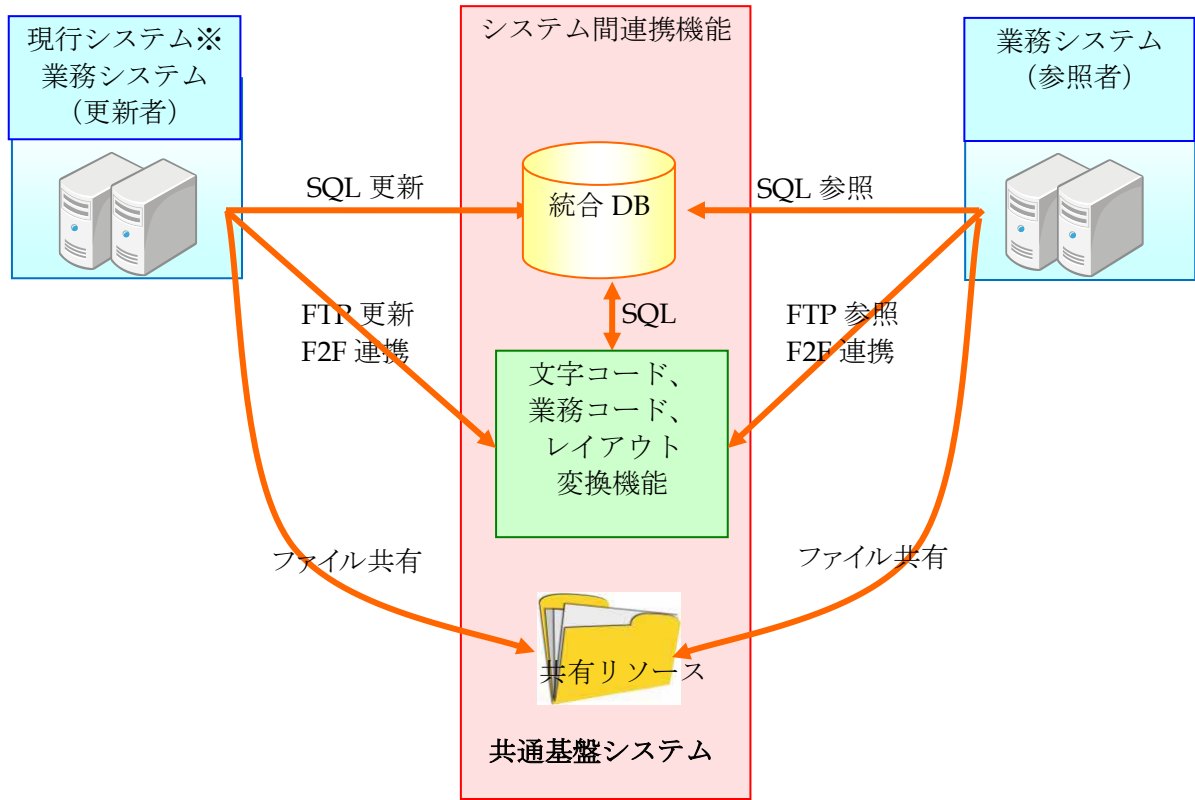
システム間連携機能の概要を以下に示す。各機能の詳細は次頁以降に記載する。

表 2-3 システム間連携機能一覧

機能	概要
データベース連携(SQL)	JDBC 等の Oracle データベース(以下、DB)接続ドライバを利用したデータ連携機能を提供する。 統合 DB へのアクセスルールを定義する。 ※新規構築の業務システムにおいては、原則データベース連携を選択すること。
ファイル連携(FTP)	FTP を利用したファイル送受信機能を提供する。 ファイル連携時に、文字コード変換及び、業務コード変換、レイアウト変換機能を提供する。 ※ファイル連携は、現行システムかつ SQL での連携機能構築が困難な場合に限り選択できる。
ファイル連携(共有リソース)	Windows 共有リソースを利用したファイル連携方式を提供する。 業務システム間にて1対1でファイルを直接やり取りする場合に利用する。他の連携方式との違いは、到達保障をしないことと、文字コード変換等のサービスを提供しないことである。 共通基盤システムとしては、データ連携用の共有リソース(フォルダ)を提供するのみである。

(ア) システム構成図

公開用 DB 方式によるデータ連携のシステム構成図を以下に示す。尚、連携方式として採用する公開用 DB 方式は、地域情報プラットフォームに準拠した方式である。各項番の概要については(イ)を参照すること。



※現行システム … 既に共通基盤システムと連携する業務システム
業務システム … 新たに導入し、共通基盤システムと連携するシステム

図 2-1 システム構成図(公開用DB方式)

(イ) 連携パターンの分類

システム間連携機能で定義する連携パターンを以下に示す。

表 2-4 システム間連携機能一覧

項番	機能名	概要	各業務システムの作業、利用にあたっての留意点
1	SQL 参照機能	OracleDB 12c で構築した統合 DB に JDBC 等の接続ドライバ経由で参照 SQL が発行された際、結果を返す。 DB 参照用のアクセスルールを定義する。	業務システムが、統合 DB の業務テーブルを参照する場合には、基本的にこの機能を利用する。 尚、文字コードの変換が必要な場合には、業務システムが文字コード変換を実施すること。

2	SQL 更新機能	OracleDB 12c で構築した統合 DB に JDBC 等の接続ドライバ経由で更新 SQL が発行された際、データベースを更新する。 データベース更新用のアクセスルールを定義する。	業務システムが、統合 DB の業務テーブルを更新する場合には基本的にこの機能を利用する。 業務システムが、共通基盤システムより提供される文字コード変換テーブルを用いて文字コード変換を実施すること。
3	FTP 参照機能	統合 DB からデータを抽出し、参照用ファイルを作成する。 現行システムが、参照用ファイルの文字コード、業務コード、レイアウト変換を実現不可能な場合、共通基盤システムと協議の上、共通基盤システムが参照用ファイルの文字コード、業務コード、レイアウト変換を提供する。参照用ファイルを FTP 連携用フォルダ（共通基盤システム側）へ格納する（連携先システムが参照用ファイルを取得する）。	現行システムが、統合 DB の業務テーブルをファイルとして取得する場合に利用する。 業務システムが、統合 DB の業務テーブルと各業務システムの業務テーブルのデータ整合性を確認する場合に利用する（業務システム側突合処理）。
4	FTP 更新機能	現行システムから連携される更新用ファイルを FTP 連携用フォルダ（共通基盤システム側）へ格納する。 現行システムが、更新用ファイルの文字コード、業務コード、レイアウト変換を実現不可能な場合、共通基盤システムと協議の上、共通基盤システムが更新用ファイルの文字コード、業務コード、レイアウト変換を提供する。 更新用ファイルから、統合 DB を更新する。	現行システムが共通基盤システムに更新用ファイルを格納し、統合 DB の業務テーブルを更新する場合に利用する。
5	F2F 連携機能	現行システム又は業務システムとで直接ファイル連携する。 連携元となる業務システムから連携用ファイルを FTP 連携用フォルダへ格納する。 必要に応じ、文字コード変換、ファイル形式変換を行う。 連携先システムが FTP 連携用フォルダから連携ファイルを取得する。	各業務システム間で直接ファイルを連携し、統合 DB には登録しない場合に利用する。
6	ファイル共有連携	業務システム間で直接ファイルを連携するためのファイル格納場所を提供する。 システム間でのファイル共有が必要な場合は、共通基盤システムと協議の上、ファイル共有機能を提供する。	業務システム（連携元）が出力したファイルを業務システム（連携先）が直接参照する場合に利用する。

(ウ) SQL連携について
以下に SQL 連携の概要を示す。

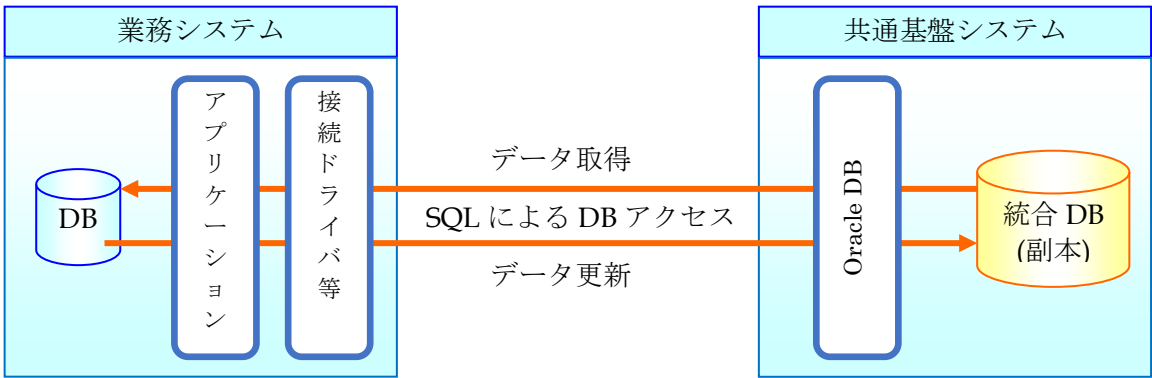


図 2-2 SQL 連携 概要図

a. 統合 DB へアクセスする際の考え方

SQL 連携では、用途に合わせて必要な表(ビュー)を公開する。公開制御に関しては、OracleDB の機能によってオブジェクトの割り当て制限(ロール)を行う。公開情報はデジタル政策室、及び主管課も含めて協議し決定する。また、コネクション確立方法(データベースリンクの作成等)についても合わせて協議し決定する。

b. 統合 DB へアクセスする際の考え方、SQL 連携に必要なソフトウェア

共通基盤システムの統合 DB へアクセスするために必要なソフトウェアを以下に記載する。統合 DB のデータベースのバージョンに合わせて業務システム側で用意すること。

表 2-5 SQL 連携に必要なソフトウェア一覧

機能	必要なソフトウェア	概要
データベース機能	接続用ドライバ	OracleDB 用の JDBC 等接続用ドライバ。
	データベースクライアント	SQL 接続に必要なデータベースクライアント機能。(OracleClient)

(エ) FTP連携

システム間のデータ連携を行う上で様々なシステムが対応できるデータ連携機能である。FTP を用いてデータ送受信が行われる中間に介在して制御する機能を実装する。

以下に、FTP 連携の概要を示す。

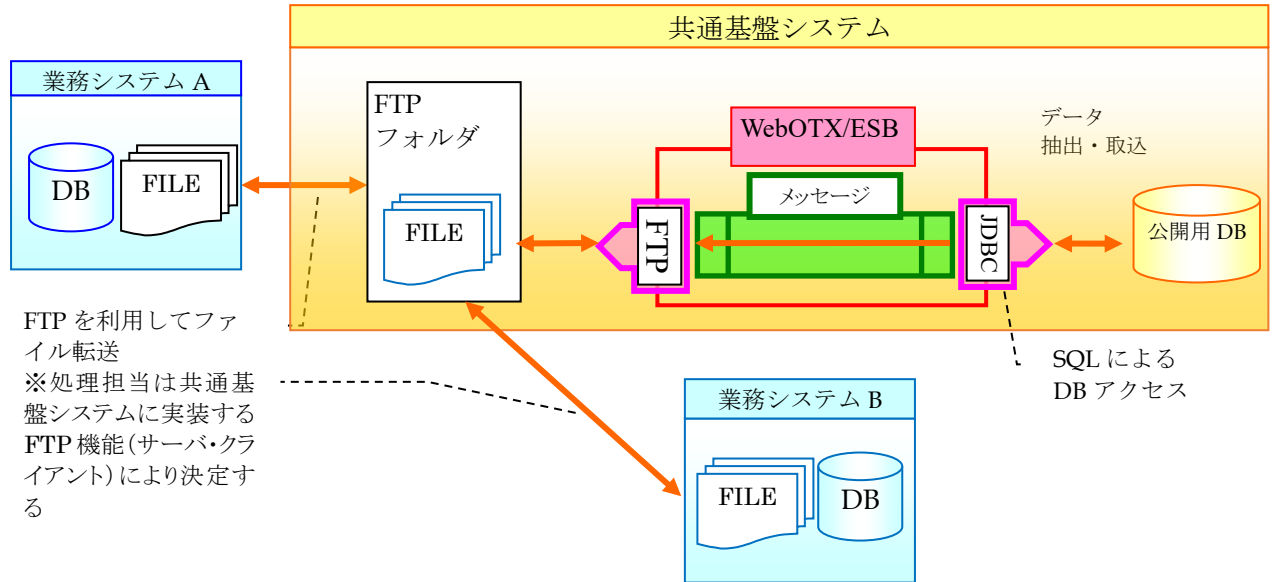


図 2-3 FTP 連携機能 概要図

FTP 連携は、ファイル(CSV ファイル、または固定長ファイル)の受け渡しを基本とした連携であり、以下の構成を前提とする。

- ファイルの受け渡しに適用するプロトコルは FTP とする。
- 共通基盤システムは FTP 連携用のディレクトリを用意し、共通基盤システムが準備したフォルダに対して現行システム又は各業務システム側からファイルの送信 (Put)あるいは取得 (Get)を行うこととする。
- FTP 連携処理では完了ファイルをもって、業務システム側へ連携ファイル作成処理完了を保証する。
- F2F 連携処理では、統合 DB を介さず現行システム又は業務システムとでファイル連携する機能を提供する。その際必要に応じて共通基盤システムは、文字コード変換機能を提供する。
- FTP 連携の際、業務システムで考慮すべき点として、業務システム単位にデータベースの利用ユーザを割り当てること。各業務システムは、割り振られたユーザ及び、パスワードにて処理することで、必要な情報のみを取得するよう構築すること。また、FTP 連携機能を利用するために各業務システム側に必要な機能を次項に記載する。

表 2-6 連携元システムとして想定される機能

機能名	機能	概要
連携ファイル作成機能	到達確認ファイル作成	到達確認ファイルの作成。
	業務データ作成	CSV 形式(または固定長)の業務データファイルの作成。
	完了ファイル作成	完了ファイルの作成。 作成は、業務データ作成完了後に行う。
通信機能	FTP クライアント	作成したファイルを共通基盤システム上の連携サーバ(FTP サーバ)に送信する FTP クライアント機能。到達確認ファイル、業務データ、完了ファイルの 3 ファイルの送信を行うが、到達確認ファイルと業務データファイルの送信後に完了ファイルを送信する。完了ファイルの送信をもって完了とする。
	再送機能	タイムアウト時等にデータの再送を行う。
管理機能	障害検知	連携元システム、共通基盤システム間のシステム間連携の障害発生時に障害を検知し、共通基盤システムの提供する障害通報装置に通知する。
	送信履歴	障害対応や監査のため、各連携ファイル単位で定められた期間の送信ファイルを保持する。
	手動再送	送信保留したファイル及び、送信履歴から、手動によりファイルの再送を行う。
	ログ出力	システム間連携の障害発生時に、どこまで正常に処理がされているかを把握し、再投入を判断するとともに、障害解析に用いる。
制約条件	ファイル送信順序保証	連携ファイルの送信は、連続した送信連番により、送信順序を保証する。

表 2-7 連携先システムとして想定される機能

機能	詳細機能	概要
連携ファイル取込機能	業務データ利用	取得した連携ファイルのデータを用いて各種処理を実行する。
	連携ファイル重複チェック	取得した連携ファイルの連番を参照し、すでに取得済みの連番を持つ連携ファイルについては、受け付けない。
	順序保証	共通基盤システム上の FTP フォルダから連携ファイルを取得する際、複数の連携ファイルセットがある場合は、連携ファイルセットの昇順で取得することで、順序性を担保する。また、取得した連携ファイルの連番を参照し、確実に連番になっていることを確認する。純リアル連携時に連番になっていない場合、データ反映を中止し、更新保留を行う。

		う。
	例外処理	不正データ、桁あふれ等の例外処理を行う。
通信機能	FTP クライアント	共通基盤システム上の連携サーバ(FTP サーバ)から連携ファイルを取得する FTP クライアント機能を実装する。FTP フォルダ上の完了ファイルの存在を確認し、取得を行う。到達確認ファイル、業務データファイル、完了ファイルの 3 ファイルの取得をもって完了とする。
	ファイル削除	共通基盤システム上の連携サーバ(FTP サーバ)から連携ファイルを取得完了後、FTP フォルダ上の連携ファイルを削除する機能。到達確認ファイル、業務データファイル、完了ファイルの 3 ファイルとも削除する。
管理機能	障害検知	共通基盤システム、連携先システム間のデータ連携の障害発生時に、障害を検知し、共通基盤システムの提供する障害通報装置に通知する。
	更新保留	準リアル連携の場合、順序不整合が発生した場合は、一時的にデータ反映を保留し、保留中は、取得したファイルを保持する。
	受信履歴	障害対応や監査のため、各連携ファイル単位で定められた期間の受信ファイルを保持する。
	手動更新	更新保留したファイルから、手動によりデータ反映を行う。
	更新再開	更新保留や障害により、データ反映が停止している時に、手動(CUIもしくは GUI)により更新を再開する。
	ログ出力	データ連携の正常終了時及び障害発生時にログを出力する。
	連携ファイルバックアップ	必要に応じて連携ファイルをバックアップする。

(オ) 統合 DB の利用条件

統合 DB は、各業務システム間で受け渡しするデータを共通基盤システム上で保持する。ただし、統合 DB で管理するデータは「副本」であり、「正本」は各業務システムにおいて管理するものとする。統合 DB はベンダーロックを排除するため地域情報プラットフォーム v3.0 に準拠して構成されるが、保持するデータ項目については共通基盤システムが掲示する仕様を基本として本市と協議し、決定すること。

ア 業務システムに求める要件

- オープン系システムは原則 SQL 連携による連携を行うこと

イ データ突合処理

- 原則、各業務システムが、共通基盤システムより突合データを受け取り、統合 DB との整合性を確認する。
- 共通基盤システムが提供する突合用データ(図 2-10 参照)は、住記・住登外・個人住民税情報の業務対象全レコードとする。

ウ データ参照時の利用条件

以下にデータ参照時考慮が必要な情報の一例を示す。

- 住民基本台帳、住登外に関する情報を参照する場合、同情報の DV 対象者も同様に統合 DB からの参照が必要となる。
- 個人住民税に関する情報を参照する場合、必要最小限のデータのみ参照するよう対象者情報の更新が必要となる。
- 住登外情報は複数の業務から更新が行われるため、データクリーニングを主管課にて実施する。その為、参照した個人を各業務システムから利用していることを申告する利用課フラグ情報の更新が必要となる。

(4) 統合運用管理機能

本項目は、共通基盤システムで実施する統合運用管理の各機能の説明、および業務システム側で実施する内容について記載する。統合運用管理は、**共通基盤環境で稼働**している業務システムに対して提供するサービスである。

ア 機能説明

(ア) 管理監視スコープ

統合運用管理におけるシステム監視は、指定の監視ソフトウェア(以下、「監視エージェント」という。)を各サーバに導入することで機能提供を行う。システム監視は、図 2-11「統合運用管理によるシステム監視項目図」中の「統合運用監視対象」とし、サーバ毎にハードウェア・OS レベルまでの監視を行う。

図 2-8「統合運用管理によるシステム監視項目図」中の「アプリケーション性能・サービスレベル監視」については、業務システムが利用するアプリケーションが不明な状態で監視サービスの提供が出来ないため、統合運用としては実施しない。アプリケーションレベル監視が必要であれば業務システムで監視機能を準備すること。

各項目の詳細な監視内容は、業務システムからの申請に応じて監視するものとする。

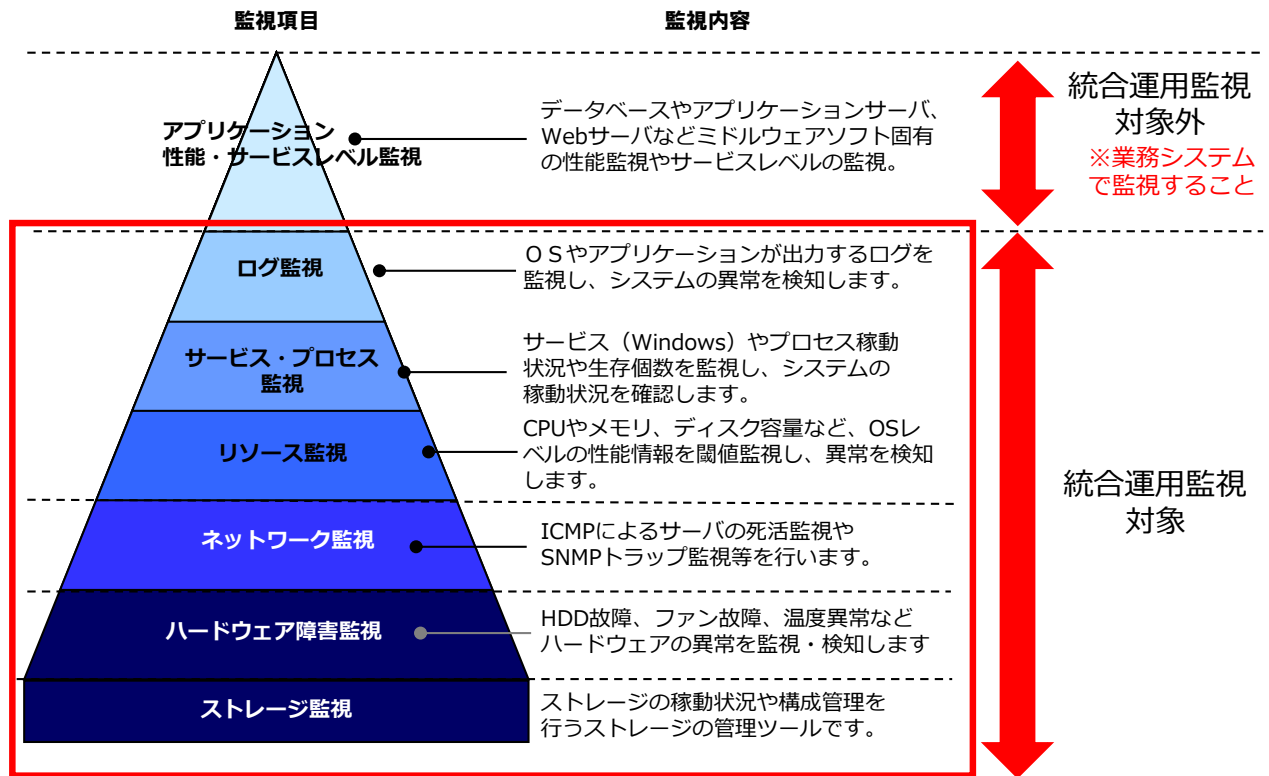


図 2-4 統合運用によるシステム監視項目図

(イ) ログ監視等の具体的手法

ログ監視は、「(ア) 管理監視スコープ」に記載した、ログ監視機能を用いてサーバ上のイベントログや Syslog、テキスト出力されているログの監視を実現する。

監視対象のログは、特定のキーワードや条件での絞り込みが可能であり、特定ログのみ通報を実行することが可能である。なお、テキスト出力されているログファイル監視は、1 件のログが複数行になる場合は行数によってはソフトウェア制限により監視できない場合がある。その場合は、業務システムでのログ監視を実現すること。

(ウ) 通報ルート

統合運用管理における監視において異常を検知した際の通報は、以下の通報方式を準備する。

- 統合運用監視端末への通報
- メールによる関係者への通報

異常を検知した統合運用業者が一次切り分けを行い、予め定められた手順に従い、業務システムベンダー及び本市担当者に連絡を行う。

(エ) ジョブ管理

統合運用管理におけるジョブの管理方針は以下のとおりとする。

表 2-8 ジョブ管理一覧表
「○」管理可能 「△」制限付で管理可能 「-」管理不可能

ジョブ管理作業	作業実施者		備考
	統合運用管理	業務システム	
ジョブ作成・設計・修正	-	○	ジョブの作成、設計は各業務システムで行うこと。統合運用業者で業務ジョブの作成はしない。
ジョブ定義の管理	○	○	ジョブ定義管理は、統合運用業者でも業務システムでも管理可能。
ジョブ実行スケジュール設定	○	○	各業務システムでジョブ実行スケジュールを作成し、統合運用業者に申請する。統合運用業者は申請に基づき、全体調整のうえ、ジョブ実行スケジュールの登録、設定を行う。
結果管理	○	-	統合運用業者にて管理を実施。
随時ジョブの実行	○	-	各業務システムからの依頼に基づき、統合運用業者で実行する。
ジョブ実行成功通知	○	-	業務システムからの申請により必要に応じてジョブ実行の成功通知を実施し、統合運用管理にて検知する。
ジョブ実行エラー検知	○	-	ジョブの実行エラーは、統合運用管理にて検知を行い、業務システム業者に連絡する。
スケジュールジョブ実行エラー(1次切り分け)	○	○	ジョブ管理製品に出力されているログの確認までは、統合運用業者で実施。業務システムで結果の確認をすることも可能。
スケジュールジョブ実行エラー(本調査)	-	○	エラーの本調査は、業務システムで実施すること。
随時ジョブ実行エラー(1次切り分け)	△	○	随時ジョブのエラー調査は、基本的に業務システムが実施すること。ただし、統合運用管理にて実行した随時ジョブの場合は、統合運用業者が結果確認を実施。
随時ジョブ実行エラー(本調査)	-	○	エラーの本調査は、業務システムで実施すること。

(オ) バックアップ管理

共通基盤システムで提供するバックアップは、Disk To Disk To Disk (D2D2D) の手法で実施する。バックアップ対象および頻度、手法等は、以下のとおりである。尚、バックアップサーバは、共通基盤システムが提供する。

表 2-9 バックアップ管理一覧

		業務システムサーバ上のバックアップ対象		
		OS 領域	データベース領域	データファイル等(業務システムでバックアップ必要なファイル・データ)
ディスクバックアップ	頻度	随時	日次	任意
	取得タイミング	サーバ設定の変更時等、業務システム側で任意に判断	業務システムの静止点を設けて、そのタイミングにバックアップを取得する	任意
	バックアップ先	バックアップサーバのローカルディスク	ストレージ装置内のデータ複製領域(Veeam で作成したバックアップジョブを、運用ジョブ・業務ジョブと連携してコマンド実行することで対応)	バックアップサーバにマウントしているデータバックアップ用領域
	バックアップ方法	共通基盤システムが提供するサーバ管理ソフトウェアを用いて実施	ストレージ機能により実施	任意(コピーコマンド、FTP、バックアップソフトなど自由)
	バックアップ条件	バックアップ時は OS の停止が必要	DB ソフトウェアの停止が必要	バックアップの手段は、業務システムで準備すること
(ディスクバックアップストレージ)	頻度	日次		
	バックアップ先	バックアップストレージ(iStorage HS)		
	バックアップ方法	バックアップサーバのバックアップソフトウェアを利用して実施		
	バックアップ条件	特に無し		

イ 業務システムに求める要件

統合運用を実施するに当たり、必要となる要件を以下に示す。

(ア) 管理監視スコープ

- ・ 監視対象の検討、申請シートの作成
- ・ OS 以外で性能等の監視が必要なソフトウェアがある場合、監視手段の準備

(イ) ログ監視等の具体的手法

- ・ 監視対象となるログの申請シート作成
- ・ 統合運用で監視出来ないログの監視手段の検討

(ウ) 通報ルート

- 平日・休日の統合運用管理からの連絡先の決定

(エ) ジョブ管理

- ジョブの作成
- 統合運用で監視するジョブの申請シート作成

(オ) バックアップ管理

- 業務システムサーバからバックアップサーバのデータバックアップ用領域にバックアップ(ファイルを移動)する仕組みの準備。
- DB ソフトウェアのサービスを停止し起動するジョブの準備

(5) 文字管理機能

ア 機能説明

(ア) 吹田市明朝

共通基盤システムでは吹田市明朝として、以下を採用する。各業務システムもこの吹田市明朝を採用すること。

- 文字フォント:MS 明朝
- 文字コード:Unicode
- 文字セット:JIS X 0213:2004

(イ) 文字管理

共通基盤システムでは以下の文字を管理する。

- MS 明朝 / Unicode
- 行政事務標準文字(MJ+)

(ウ) 外字作成

外字の作成は市民課が行う。

共通基盤システムの文字管理機能において、吹田市明朝(MS 明朝 / Unicode)の外字作成時に、MJ+との文字同定(文字コード変換テーブルの修正)を行う。

(エ) 配信

外字登録、文字同定により作成された外字ファイル、文字コード変換テーブルは共通基盤システムの外字管理サーバで管理する。各システムのサーバへ配信が必要な場合は共通基盤システムの外字管理サーバの共有フォルダを用いて配布する。なお、クライアントへの配布は SKYSEA を用いて行う。

(オ) 文字コード変換

文字コード変換機能は連携元、連携先の各システム間で異なる文字コード体系を使用している場合、その差を吸収するために文字コードの変換機能を提供する。(2(2)システム間連携・変換機能参照)

(6) 共通印刷機能

ア 機能説明

共通印刷機能は、業務システムが大量に出力する帳票(印刷ジョブ)を集中管理し、印刷ジョブの印刷及び印刷履歴ログを出力、管理する機能である。印刷データが残っている間は再印刷を行う。

(ア) 印刷

印刷時に設定可能な項目は「プリンタ」「印刷ページ」となる。なお、再印刷時にもこれを実現する。

(イ) 印刷履歴ログ

印刷時に誰が、いつ、どのプリンタに出力したのかをログ出力する。

イ 業務システムに求める要件

業務システム帳票をセンタープリンタで印刷する場合、以下の要件を満たすこと。

(ウ) 印刷データを共通印刷機能からセンタープリンタに印刷する方式は以下の 3 パターンがあり、そのどれかを利用すること。

a. PDF 出力方式(推奨)

業務システムで印刷データを PDF 形式で生成する。生成した PDF ファイルを所管課職員から統合運用管理業者に引き渡し、統合運用管理業者が共通印刷機能に取り込み印刷する方式。

デジタル庁において文字情報基盤として整備された文字セット(MJ+)を含む印刷データは、本方式で出力することを想定している。

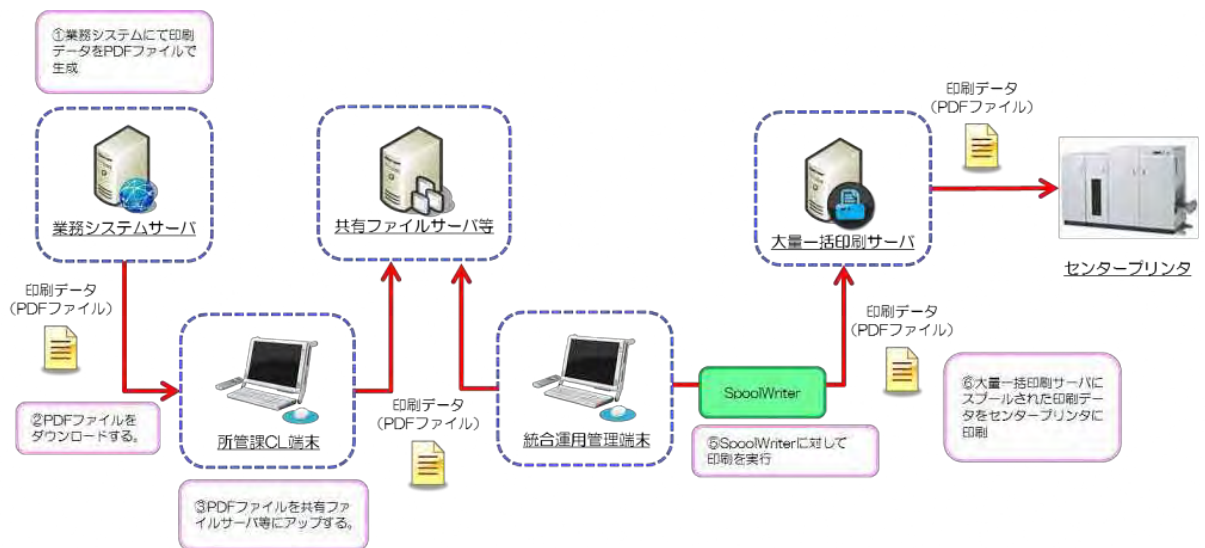


図 2-5 PDF 出力方式図

b. サーバ連携印刷方式(所管課CL端末経由)

業務システムで生成した印刷データを業務システム側の所管課CL端末経由で共通印刷機能に対してスプールする方式。統合運用管理業者は共通印刷機能にスプールされた印刷データを確認し印刷実行を行う。なお、本方式を利用する際は、業務システム側所管課CL端末に仮想プリンタドライバ(SpoolWriter)をインストールする必要がある。

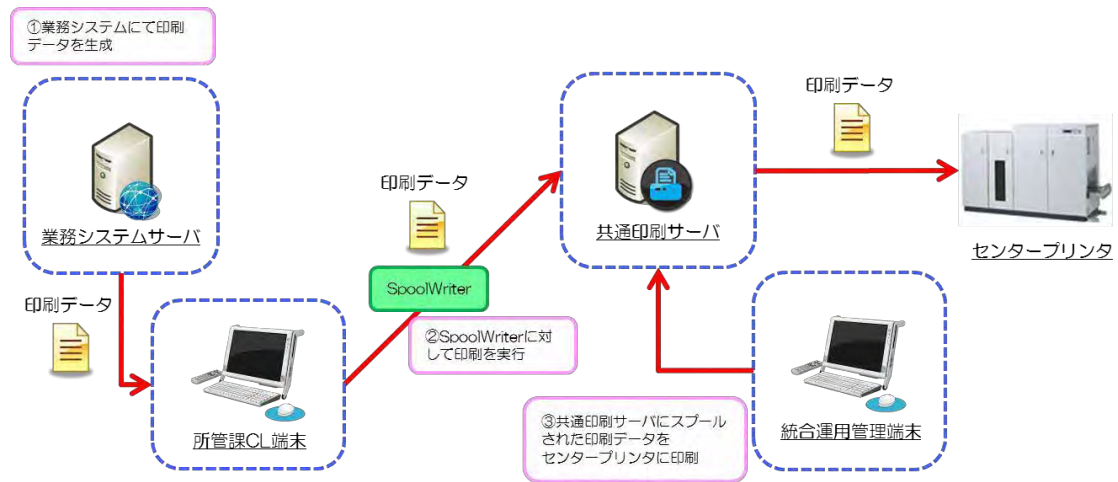


図 2-6 サーバ連携印刷方式(所管課CL端末経由)図

c. サーバ連携印刷方式(直接)

業務システムで生成した印刷データを直接業務サーバより共通印刷機能に対してスプールする方式。統合運用管理業者は共通印刷機能にスプールされた印刷データを確認し印刷実行を行う。なお、本方式を利用する際は、仮想プリンタドライバ(SpoolWriter)をサーバにインストールする必要がある。

※ライセンスが印刷するサーバ台数分必要(検証サーバ分も必要となる。)

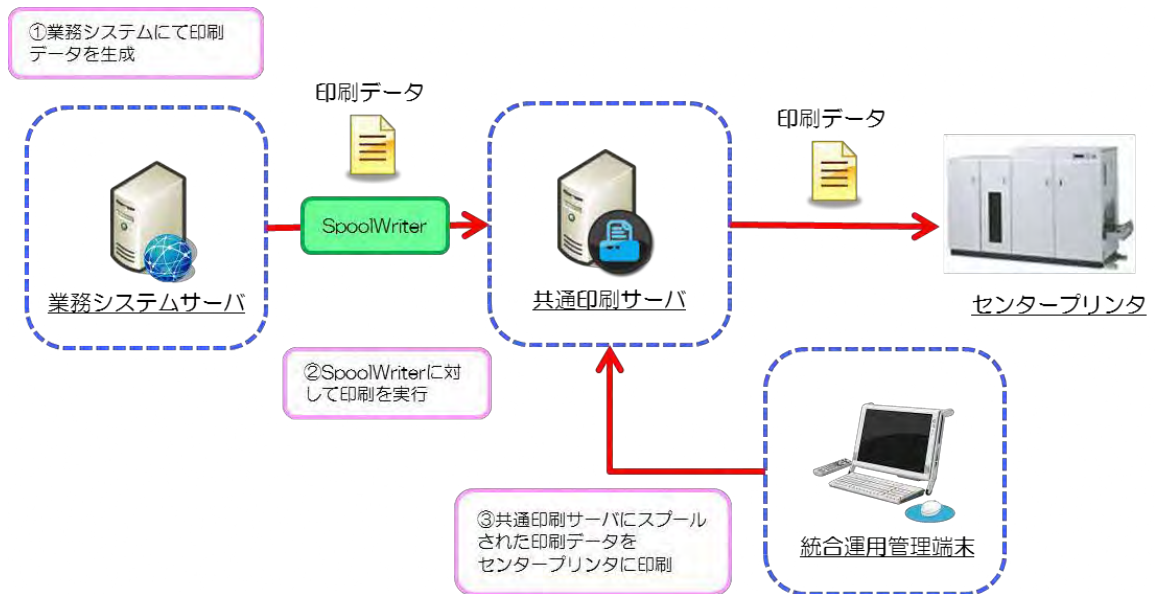


図 2-7 サーバ連携印刷方式(直接)図

(エ) 共通印刷機能に対して印刷ジョブを送ること。

印刷ジョブを共通印刷機能に送る場合、以下の対応が必要となる。

a. 業務システム帳票を出力する OS が Windows の場合

共通基盤システムが指定する仮想プリンタドライバを対象 OS にインストールし、この仮想ドライバに対して印刷を行うこと。なお、仮想プリンタドライバの必要数を見積もり、通知すること。仮想プリンタドライバの必要数は、センタープリンタへ印刷する業務システムサーバ台数と同数となる。

※帳票生成サーバから直接センタープリンタに印刷する場合は、帳票生成サーバ台数分を通知する(クラス構成の場合は、待機系サーバも台数に含めること)

業務システム内で帳票管理サーバを構築し、この帳票管理サーバのみからセンタープリンタに印刷する場合は、帳票管理サーバ台数分を通知する。

b. 業務システム帳票を出力する OS が Linux の場合

lpr コマンドを使用して共通印刷機能サーバのプリンタに対し、印刷データを送信すること。

なお、lpr コマンドにより共通印刷機能に印刷データを送信した場合、印刷データの総ページ数が取得できないため、ページ範囲指定による印刷が実行できない。

(オ) 共通印刷機能に印刷ジョブを送る際は、センタープリンタに紙出力する場合と同様の印刷ジョブを送ること。

共通印刷機能は全ページ印刷、ページ指定印刷といった印刷が可能となる(ページ指定印刷は lpr コマンドによる連携時は不可)。

(7) EUC・帳票作成機能

割愛

(8) ファイル共有機能

ア 機能説明

利用者間のデータのやり取りを行う上でのデータ保管場所(共有フォルダ)を提供する。このファイル共有は AD による共有フォルダ機能を利用した権限管理、アクセス管理を行う。

(ア) 容量

共通基盤システムが管理する共有フォルダは利用する室課単位に容量の割振りを実施する。割り振られる容量については吹田市行政経営部デジタル政策室と協議のうえ、決定する。

(イ) 権限

権限制御は、ファイルの参照・更新権限のみを利用する。

権限付与は室課単位で行う。

(ウ) セキュリティ

セキュリティ対策として、AD 機能を利用したアクセス管理、端末監視製品を用いたログ管理を行う

イ 業務システムに求める要件

ファイル共有機能の使用対象は利用者となり、業務システム間連携時のファイル格納や業務システムバックアップとしては使用しない。

(9) 統合ハードウェア

本項目は、共通基盤システムで実施する統合ハードウェアの基本的な考え方及び提供する機能について説明する。加えて統合ハードウェアを利用するために業務システムに求める要件を記載する。

ア 基本の方針

(ア) サーバの仮想化

各業務システムにて仮想化が可能と判断されたサーバについては、**Windows Server 2022 Hyper-V** で実装された仮想サーバを提供する。仮想サーバはローカル HDD ブートで実装されており全てのデータは Fiber Channel 接続されたストレージ(以下、「FC ストレージ」という。)上に保存される。

(イ) リソースの共有

各業務システムは「リソースブロック」に配備される。リソースブロックとは仮想サーバに割り当てるリソース(CPU、メモリ、FC ストレージ内のディスク)を、業務システム間・サーバ間で共有することが可能な単位である。

複数の業務システムを同一のリソースブロックに配備し、リソースブロック内でリソースの共有を可能にする。運用開始後はリソース利用状況を監視し性能余剰が発生している場合、リソースの再利用を行う。リソースの監視と制御については、統合運用管理で実施する。

リソースブロックのイメージ図を以下に示す。

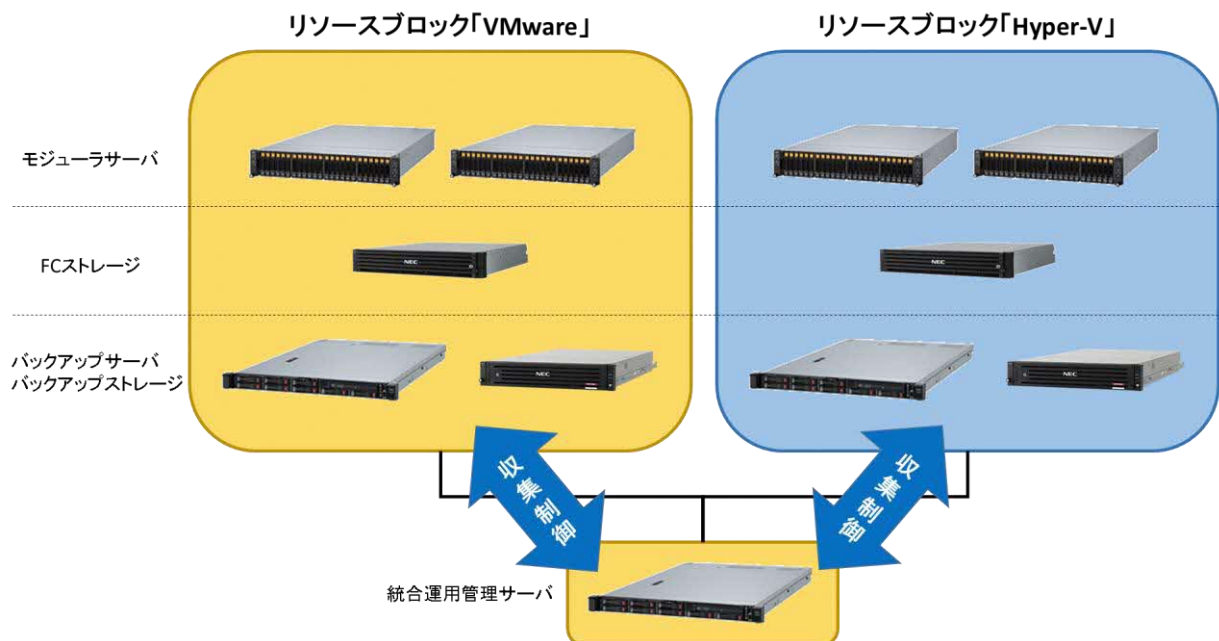


図 2-8 リソースブロックイメージ図

(ウ) ハードウェア統合管理

各リソースブロックに複数業務を配置する環境であるが、それらの管理は統合管理機能で行う。統合管理の機能は以下の通り。

- ・ 物理環境・仮想環境の監視機能(ハードウェア、ハイパーバイザー、リソース、OS、ネットワーク機器)
- ・ 仮想化基盤制御機能(監視機能と連携した復旧処置ライブマイグレーション、N+1 リカバリ、電源制御)

- 仮想マシンのプロビジョニング機能

イ 機能説明

(ア) 主要ハードウェア

主要ハードウェアの一覧を以下に示す。各システムのリソース割り当ては別紙「ハードウェアスペックシート」にて提示する。

表 2-10 主要ハードウェア一覧

ハードウェア	主要スペック
仮想化基盤サーバ	CPU: Xeon Gold 6542Y 2.90GHz 24C×2 メモリ: 384GBHDD:2.4TB(RAID5、SAS10Krpm1.2TB×3) インターフェイス: 1000BASE×8、10GBASE×2、FC×2 冗長電源
FC ストレージ	183.6TB(Read Intensive NVMe SSD(2.5 型 15.3TB×12)) 電源・コントローラ等主要部品は筐体内で冗長化ホストポート数: 32Gbps FC×8 本キャッシュメモリ:256GB 搭載
統合運用管理サーバ#1	CPU: Xeon Silver 4509Y 2.60GHz 8C×2 メモリ:16GB HDD: 2.4TB(RAID5、SAS10Krpm 1.2TB) インターフェイス:1000BASE×8 冗長電源
バックアップサーバ#1、 #2	CPU: Xeon Silver 4510 2.40GHz 12C×2 メモリ: 64GB HDD: 300GB(RAID1、SAS10Krpm 300GB×2)、6TB(RAID5、 SAS10Krpm 1.2TB×6) インターフェイス:1000BASE×4、10GBASE×2 冗長電源
バックアップストレージ	ストレージ容量:72TB(分散冗長配置(Distributed Resilient Data (DRD))) インターフェイス:10GBASE×2 冗長電源

※物理サーバは、統合運用管理サーバ、バックアップサーバのスペックを記載している。

(イ) ストレージ構成

FC ストレージの構成イメージとディスク構成を以下に示す。

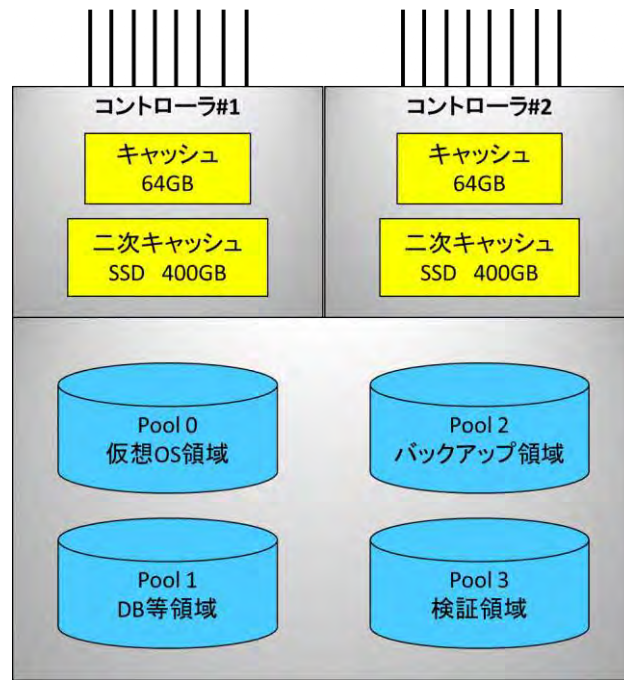


図 2-9 FC ストレージイメージ図

- コントローラは FC(16Gbps)×8 ポートが接続。負荷分散で稼働し、16Gbps×16 の帯域が利用可能。片方に障害が発生した場合は 1 コントローラで稼働する。
- キャッシュはそれぞれ 64GB のメモリを搭載。また二次キャッシュとして 400GB の SSD を Read/Write で利用可能。
- 筐体内レプリケーション機能(Dynamic Data Replication。以下「DDR」という。)を有しており、上記 DB 等領域をバックアップ領域に複製することが可能。

表 2-11 FC ストレージディスク構成

用途	DDR ※	RAID 方式	構成 ディスク	備考
仮想 OS 領域	－	RAID-10	SAS 2.5 型 2.4TB/10krpm	仮想サーバの OS やアプリケーション インストール用領域。(物理サーバの ローカル HDD と同義の領域)
DB 等領域	MV	RAID-5	Read Intensive SAS SSD 2.5 型 3.84TB	DB など DDR で保護すべきデータを格 納する領域。
バックアップ領域	RV	RAID-6	NL-SAS 3.5 型 8TB/7.2krpm	DDR の複製領域として利用する。その 他ネットワーク経由でのバックアップ先 や開発用途のストレージとしても利用 可能。
検証領域	MV	RAID-6	NL-SAS 3.5 型 8TB/7.2krpm	開発環境や検証環境の仮想サーバ OS やアプリケーションインストール用 領域。その他高いディスク IO を必要と

用途	DDR ※	RAID 方式	構成 ディスク	備考
				しないストレージとしても利用可能。

(ウ) 業務サーバのソフトウェア構成

業務システムへ引き渡しを行うサーバにインストールするソフトウェアを以下に示す。

表 2-12 業務サーバのソフトウェア構成

ソフトウェア	品名	インストール先
サーバ監視エージェント	WebSAM SystemManagerG エージェント	全業務サーバ
サーバハードウェア監視エージェント	ESMPRO/ServerAgent ESMPRO/ServerAgentService	物理サーバのみ
FC パスの冗長化制御ソフト	WebSAM StoragePathSavior	Hyper-V 上の業務サーバ 物理サーバ
ログ収集エージェント	LogStorage	なし(エージェントレス)
ジョブ管理エージェント	WebSAM JobCenter エージェント	全業務サーバ
アンチウィルスソフトウェア	Symantec EndPoint Protection	全業務サーバ

(エ) ハードウェア冗長機能について

VMware 仮想サーバの冗長化はライブマイグレーション N+1 リカバリにて実現する。リソースブロック毎に予備のサーバを 1 台配備しており、リソースブロック内の仮想サーバの再配置を行う。

Hyper-V 仮想サーバの冗長化はライブマイグレーションにて実現する。リソースブロック内の仮想化基盤サーバで障害が発生した場合は、リソースブロック内の仮想サーバを正常な仮想化基盤サーバへ再配置を行う。

物理サーバに関しては冗長化機能を持っていないため、各業務システムでクラスタ構築を行う必要がある。また、仮想サーバの再配置ではサービス起動障害等のソフトウェア障害に対応できないため、必要に応じて各業務システムで仮想サーバのクラスタ構築を行うか、物理サーバでクラスタを構築する必要がある。

(オ) 監視及びバックアップ機能

本資料の「2 提供機能説明 (4) 統合運用管理機能」を参照すること。

(カ) Oracleのライセンスポリシー

本サーバ統合基盤は Oracle 専用の領域(Oracle 島)を用意している。Oracle 島上で Oracle データベースを使用するライセンスはサーバ統合側で用意する。従ってシステム側において、Oracle のデータベースを Oracle 島に構築し、利用する場合は Oracle ライセンスの調達は不要である。

※Oracle 島ではない個別環境において Oracle データベースを構築する場合は、Oracle ライセンスを見積もりに含めること。

※Oracle 以外のデータベースライセンスは用意しないため、Oracle 以外のデータベースを利用する場合は見積もりに含めること。

ウ 業務システムに求める要件

(ア) スペックシートの記載について

- ・各システムで利用を想定しているスペックリソースを別紙「ハードウェアスペックシート」に提示すること。
- ・OS 及び各サーバのサイジング情報を記載の上、所定の期日までに提出すること。
- ・提示リソースに追加変更が必要な場合は、追加変更リソース詳細と根拠を記載すること

(イ) 統合ハードウェアでサポートする OS

c. 仮想化基盤ゲストマシンでサポートする OS

- (a) Microsoft Windows Server 2016 Standard
- (b) Microsoft Windows Server 2016 Datacenter
- (c) Microsoft Windows Server 2019 Standard
- (d) Microsoft Windows Server 2019 Datacenter
- (e) Microsoft Windows Server 2022 Standard
- (f) Microsoft Windows Server 2022 Datacenter
- (g) Red Hat Enterprise Linux 8.4 以降(x64)
- (h) Red Hat Enterprise Linux 9.0 以降 (x64)

d. 物理サーバでサポートする OS

- (a) Microsoft Windows Server 2016 Standard
- (b) Microsoft Windows Server 2016 Datacenter
- (c) Microsoft Windows Server 2019 Standard
- (d) Microsoft Windows Server 2019 Datacenter
- (e) Microsoft Windows Server 2022 Standard
- (f) Microsoft Windows Server 2022 Datacenter
- (g) Red Hat Enterprise Linux 8.4 以降(x64)
- (h) Red Hat Enterprise Linux 9.0 以降 (x64)

(ウ) 不足機能について

機能説明に記載されている以外の冗長機能、負荷分散機能、監視・バックアップ機能が必要な場合は、業務システム側で準備すること。

(10) シンククライアント・FAT クライアント

ア 機能説明

新基幹系システムの端末は、ローカルに住民データを持たないシンククライアントと FAT クライアントが利用できる。

シンククライアントシステムとして使用するソフトウェアを表 2-14 に示す。

表 2-13 シンククライアントシステム使用ソフトウェア一覧

用途	品名	主要機能
シンククライアント基盤	Citrix XenDesktop	シンククライアント接続先の仮想 PC を作成する基盤
仮想化基盤	VMware vSphere	シンククライアント基盤を作成するための仮想基盤

上記ソフトウェアを使用した、仮想マシン型のシンククライアントシステムを導入する。
仮想マシンへの接続は、SA環境の端末を使用する。

FAT クライアントは、新基幹系ネットワーク上に配備されており、シンククライアントで対応できない業務システムや周辺機器(外部デバイス)を利用する必要がある場合等で利用することができる。

イ 業務システムに求める要件

(ア) シンククライアント

シンククライアントを利用するにあたり、以下に要件を示す。

- Citrix XenDesktopを用いたシンククライアントに対応が可能であること。
- 現行のシンククライアントで稼働しているシステムへ影響を与えないシステムとすること。
- 影響があるのかを判断できない場合は、テストとして現行システムが稼働しているクライアントでの評価を行い、影響の無いことを確認すること。
- 表 2-15 に示すシンククライアントのクライアント要件で稼働が行えること。
- シンククライアントの制限事項として、周辺機器(外部デバイス)の使用を行わない設定となっているため周辺機器を原則使用しないこととする。

表 2-14 シンククライアント要件

リソース	要件
CPU	2 コア Xeon Gold 6142(16C/32T, 2.60 GHz)
メモリ	4GB
HDD	40GB(システム領域) ※データ領域は各室課ごとに設定された共有フォルダを使用すること。
OS	Microsoft Windows 10 Pro 64bit OR Microsoft Windows 10 Ent 64bit

ブラウザ	Microsoft Edge(Chromium 版)
------	----------------------------

(イ) FAT クライアント

FAT クライアントを利用するにあたり、以下に要件を示す。

- 業務システムが現行の FAT クライアントで稼働しているシステムへ影響を与えないシステムとすること。
- 影響があるのかを判断できない場合は、テストとして現行システムが稼働している FAT クライアントでの評価を行い、影響の無いことを確認すること。
- 表 2-16 に示す FAT クライアントのクライアント要件で稼働が行えること。
- 業務システムで個別に必要な周辺機器がある場合は、その理由と数量を記載すること。

表 2-15 クライアント要件 (H31 年度調達ノート PC 例)

リソース	要件
CPU	Intel Core i3(2.0GHz)以上 又は同等品以上
メモリ	4GB 以上
SSD	128GB 以上
OS	Microsoft Windows 10 Pro 64bit
ブラウザ	Microsoft Edge(Chromium 版)

(ウ) クライアント共通

シンクライアント・FAT クライアントを利用するにあたり、以下に共通となる要件を示す。

- 先行構築されている業務システムと共通の端末を利用する場合には、業務システム導入時に十分な動作確認を行うこと。その際、先行構築されている業務システムに影響を与えないこと。
- クライアントのフォルダにアクセスする業務システムは、以下の点に留意すること。
業務システムを利用する一般職員の Windows アカウントは、デスクトップを含めローカルディスクへデータ保存は認めていないため、ローカルディスクのフォルダに対するアクセス権限は持っていない。また、管理者アカウントの権限で動作する Windows サービスは、全てのフォルダに対するアクセス権限を有する。
- ブラウザは、Microsoft Edge(Chromium 版)であり、業務システムは、以下の点に留意すること。
 - ゾーンのセキュリティレベルは、“中低”である。変更は認めない。
 - 信頼済みサイトへの登録は、原則認めていない。必要な場合は、所定の手続きを行い、市から事前に許可を得ること。
 - ActiveX の利用は、原則認めていない。
 - 業務システムで、Microsoft Edge(Chromium 版)の Enterprise Mode の利用が必要な場合は、URL の一覧を申請すること。

- 現行のクライアントへ業務システムの利用にアプリケーションのインストール等が必要となる場合は、業務システム構築業者が実施すること。但し、既に導入されているツール等で対応が可能な場合には、市へ相談の上、許可を得ること。端末の作業には、以下の点に留意すること。
 - クライアントの設定変更は、業務システムの範囲となる。Windows 及び Microsoft Edge(Chromium 版)の変更が必要な場合は、市から事前に許可を得て、Active Directory の各業務システムに割り当てられたグループポリシーに設定すること。
 - ローカルディスクのパーティション分割は原則認めていない。
 - デスクトップは、共有していない。必要な場合は、ユーザのデスクトップごとに設定すること。
 - ユーザープロファイルの設定を変更する場合は、全てのユーザーアカウントに設定すること。
 - 業務システムを起動するためのアクセス方法は、認証ポータル画面のみとし、デスクトップ等へ業務システムのショートカットの配置は認めない。
 - 表 2-15 シンクライアント要件を参照し、負荷の大きな業務処理の実行は、FAT クライアントに設定すること。
- ハードコピーは、原則禁止とする。但し、市指定のハードコピーツールを用いることは可能である。その場合、誰がどのような操作をしたか、全て記録されることになる。

(11) セキュリティ

ア 機能説明

(ア) Active Directory

本市が提供する Active Directory を利用すること。

(イ) ウィルス対策

a. 端末のウィルス対策

端末のウィルス対策製品は、端末導入業者が導入する。ウィルスパターンファイルの配信・適用は、共通基盤システムが一括して実施する。ウィルススキャンは、リアルタイムスキャン、定期スキャンを実施する。

b. サーバへのウィルス対策

サーバへのウィルス対策製品は、統合運用業者が導入する。ウィルスパターンファイルの配信・適用は、共通基盤システムより一括して実施する。ウィルススキャンの定期スキャンは実施する。リアルタイムスキャンは、業務システムからの要望に応じて実施する。

(ウ) パッチ適用

a. 端末のパッチ適用

端末への OS パッチ配信・適用は、共通基盤システムより実施する。OS 以外で端末に適用が必要なパッチについては、統合運用業者・各業務システムの業者と協議をして決めるものとする。

b. サーバのパッチ適用

サーバへの OS パッチ配信・適用は、共通基盤システムでは実施しない。業務システムで必要な OS パッチは、判断のうえ収集・配信・適用を実施すること。また、その他ミドルウェア等のパッチも必要に応じて業務システムが収集し適用すること。

(エ) ログ管理

a. ログ収集

業務システムの監査証跡ログを一元管理するためにログの収集を行う。業務システム側にて収集対象のログファイルを所定の格納フォルダへ格納することとする。

b. ログ管理

業務システムの監査証跡ログを一元管理する。監査証跡ログに対する改竄チェックを行う。

イ 業務システムに求める要件

サーバへのパッチ適用の運用の実施

ログ管理について、共通基盤側で収集管理を行うが、各業務システム側でもログ管理は行うこと。

(12) 中間サーバー連携機能

ウ 機能説明

(ア) 中間サーバーコネクタとのデータ連携

中間サーバーコネクタは、団体内統合宛名番号の付番、管理及び、中間サーバーとの連携機能を実現するシステムを指し、共通基盤システムはこの中間サーバーコネクタへの連携機能を提供する。

(イ) 団体内統合宛名情報 VIEW

共通基盤システムは、各業務システムより団体内統合宛名番号を取得する為の VIEW(以下、団体内統合宛名情報 VIEW)を作成し、公開する。なお団体内統合宛名情報 VIEW を参照する SQL ユーザは、統合 DB 連携用ユーザとは別のものを払い出す。

エ 業務システムに求める要件

- 必要に応じ、中間サーバーコネクタの仕様に基づく連携方式(SOAP)、レイアウト(※)に従い構築すること。
- ※国の公開するデータ標準レイアウトに、中間サーバーコネクタ連携用の項目を加えたレイアウトとなる。
- 団体内統合宛名番号を取得するため、団体内統合宛名情報 VIEW を参照する SQL 連携機能を構築すること。
- 中間サーバー連携機能、団体内統合宛名情報 VIEW 参照の可否については、市と協議の上決定すること。
- 共通基盤システム・中間サーバーコネクタとの連携が確立できなかった場合、各業務システムにて検知する機能を有すること。
- 共通基盤システム・中間サーバーコネクタとの連携のログを出力し、管理する機能を有すること。
- 団体内統合宛名情報 VIEW 以外は中間サーバーコネクタと直接連携を行うこと。

(13) 標準連携用オブジェクトストレージ機能

ア 機能説明

(ア) オブジェクトストレージ(Amazon S3)の提供

標準化対応済みの各業務システム間で標準連携を行う場合に利用するオブジェクトストレージを提供する。オブジェクトストレージは Amazon S3 サービスを利用する。

オブジェクトストレージはデジタル庁の標準連携に関する技術仕様書にて定義されている構成をもとにバケット名称、構造を決定する。

また、利用する業務システムに対して操作権限の付与を実施する。

イ 業務システムに求める要件

- AWS 上の標準準拠システムから利用する場合は、各業務システムのアカウント内からオブジェクトストレージへのアクセスが可能であること(エンドポイントや名前解決環境・暗号鍵)
- AWS 外から利用する場合は、後述の認証認可機能を併用すること

(14) 認証認可機能

ア 機能説明

(ア) AWS 外からオブジェクトストレージ(Amazon S3)を利用するための認証・認可機能の提供

AWS 外の環境(本庁内に設置されている業務システムや AWS 以外のクラウドサービスプロバイダ上に構築された標準準拠システム等)から(11)の標準連携用オブジェクトストレージを利用する場合に、認証および認可機能を提供する。

イ 業務システムに求める要件

- AWS 外からアクセスする場合、接続元システムから吹田市のガバクラ環境(AWS)へ接続可能な NW 環境および名前解決環境が整備されていること

3 導入プロセスと提供サービス

(1) 導入準備フェーズ

業務システムの構築業者が決定した段階で、共通基盤システムを活用するために以下のサービスを提供する。

ア 共通基盤システム・ガイドラインの提供

共通基盤システムを活用するためのガイドラインを提供する。業務システムの実施計画立案時に共通基盤システムを理解し、構築プロセス上考慮すること。また、疑問点等があれば、QA対応は随時行う。

表 3-1 共通基盤システム・ガイドライン一覧

機能名	ガイドライン
認証・ポータル機能	認証・ポータル機能利用ガイドライン
システム間連携・変換機能	共通基盤連携ガイドライン
統合データベース・共通データ管理機能	
統合運用管理機能	統合運用機能_システム監視機能利用ガイドライン 統合運用機能_ジョブ管理機能利用ガイドライン 統合運用機能_バックアップ・リストア管理機能利用ガイドライン 統合運用機能_時刻同期利用ガイドライン
外字管理機能、外字配信機能	外字配信機能利用ガイドライン
共通印刷機能	共通印刷機能利用ガイドライン
EUC・帳票作成機能	個別支援対応のため提供なし。
ファイル共有機能	※業務システム側にて対応がないため提供なし。
統合ハードウェア	※個別支援対応のため提供なし。
クライアント管理	
セキュリティ管理機能	統合運用機能_セキュリティ管理機能利用ガイドライン 統合運用機能_ログ管理機能利用ガイドライン
中間サーバー連携機能	団体内統合宛名の基本設計(中間サーバコネクタ連携概要)
標準連携用オブジェクトストレージ機能	標準連携用オブジェクトストレージ機能利用ガイドライン
認証認可機能	認証認可機能利用ガイドライン

イ 共通基盤システム活用説明会

業務システムの所管課及び構築業者向けに、共通基盤システムの活用に向けた説明会を実施する。説明会では、主要な機能の説明を実施するとともに、事前に提供したガイドラインにおけるQA対応も実施する。

業務システム側においては、構築スケジュール、体制等のプロジェクトの概要説明をお願いする。

なお、共通基盤システム活用説明会は、原則として1業務システム1回を想定している。その他サーバ等の複数同時期に構築されるケースでは、複数の業務システムと合同で実施することもある。開催については、本市にて調整を実施する。

(2) 構築フェーズ

業務システムの構築フェーズにおいて、共通基盤システムが提供するサービスを説明する。

ア QA対応

構築途中において発生する疑問点、課題については随時QA対応を行う。

QAは、共通基盤システムが予め提供する連絡票を利用する。なお、別途会議を行う場合は、本市が開催有無の判断、開催調整を実施する。

イ 統合ハードウェアリソース提供

(ア) リソース設計の実施

業務システムを統合ハードウェア上に構築する際、ディスクパーティション等のリソース設計が必要となる。リソース設計においては、共通基盤システムが提供するリソースシートに必要な情報を記載の上、提出していただく。リソース設計において、リソースの過不足等の課題が発生した場合には、リソース割り当て含め調整が必要となる。別途会議を行う場合は、本市が開催有無の判断、開催調整を実施する。

(イ) リソースの提供

構築にあたっては、業務システムに対して3つの環境を提供する。

表 3-2 提供リソース一覧

環境名	役割／制限事項
本番環境	各業務システムの本番稼働に用いる。 本稼働後、定められた手続きなしでプログラムやパラメータの変更ができないように制限する。
検証環境	開発環境における開発・変更作業の完了分の品質や性能検証に用いる。 本番環境と同等のシステム構成 ⁵ やシステム間連携などを保持する。 総合テスト、運用テスト、研修、移行リハーサルなどに利用し、本市職員向けの研修用として使用することを想定している。
開発環境	パッケージのプログラム開発(カスタマイズ)やパラメータ変更に用いる。単体テストや結合テスト向けとし、各SEが自由にデータを入れ替えできる。 尚、原則、開発環境は受託ベンダーで用意すること。 開発環境の構築作業、必要なライセンスは構築業者が準備すること。

ウ テスト支援(結合、総合、運用)

業務システムの構築において、テスト時に共通基盤の検証用環境を提供し、主に技術的な観点でのテストを実施する。

エ システム切り替え時支援

本番稼働におけるシステムの切り替え時には、統合運用業者が立ち会う。必要があれば共通基盤システムの保守SEも立ち会う。本市にて支援内容の調整を実施する。

オ 障害発生時の切り分け支援

テスト時に発生した障害については共通基盤システムに関係するか判断し、関係する場合には、障害発生時の切り分け等の支援作業を実施する。

カ ヘルプ窓口の提供

仮想環境上に構築するため、VMware、Hyper-V への問い合わせ窓口の開設を希望するベンダーに対しては、共通基盤から問合せ窓口を設定する。各ベンダーは構築期間だけでなく、稼働後の保守期間にも直接問合せを行うことができる。

(3) 運用フェーズ

本市では、統合運用管理を行う想定をしているため、業務システムの開発業者は、適切に運用設計を行った上で、統合運用管理業者への運用業務引継ぎを行う必要がある。

⁵ リソースやライセンスの関係で本番環境と完全に同一でなくても良い。業務システムの動作検証に必要な環境であること。

ア 運用管理設計

運用管理設計は、下記運用管理設計方針に則り、本市及び統合運用管理業者への報告及び適宜協議を行った上で、実施すること。

(ア) 運用管理設計方針

- 人的側面、システムの側面から、システム運用サービスの向上、運用費用削減が可能なこと。
- 本市と同規模の他自治体での実績が十分であり、標準的な(ITIL及びISO20000等に即した)運用設計手法であること。
- 本市の基幹系業務システムの現状を考慮した内容であること

また、運用管理に係る成果物は、統合運用管理業者が指定するドキュメント、フォーマット等に従い作成すること。

運用管理設計の作業内容を以下に示す。

(イ) 成果物の作成及び中間報告

統合運用管理業者が適切に運用業務を実施可能となる、運用管理に係る成果物(運用計画書、システム操作、運用マニュアル等)を作成すること。

なお、上記運用管理設計における成果物の作成にあたっては、適宜、定例報告会等で、本市及び統合運用管理業者と協議を実施すること。

(ウ) 成果物の作成及び報告

運用管理設計における成果物の更新状況等を実績報告書に取りまとめ、定例報告会において本市へ報告すること。

更新された運用管理設計における成果物を、運用管理設計における成果物として取りまとめ、本市及び統合運用管理業者へ提示し、双方の承認を受けること。

イ 運用業務引継ぎ

業務システムの開発受託者(以下、「受託者」という。)は、本市及び統合運用管理業者と調整・協議を実施したうえで、運用業務の引継ぎを実施すること。(統合運用業者への運用引継ぎはシステム設計・開発業務における運用テスト時に実施することを想定している。)

なお、統合運用業者への運用業務引継ぎが十分でないと判断された場合(システム操作/運用マニュアルを参照しても該当運用業務を遂行できない場合など)には、運用業務引継ぎが十分に行われたと判断されるまで、本市及び統合運用管理業者に対して運用業務のサポートを行うこと。

(ア) 運用テストスケジュール策定

受託者は本市及び統合運用管理業者と協議のうえ、運用テストスケジュールを作成すること。

なお、スケジュール作成には現行システムの稼動状況及び業務繁忙期等の状況を考慮し、本市職員(統合運用管理業者を含む)への作業負荷が過大とならないスケジュールを策定すること。

(イ) 運用研修(初回運用研修)

システム操作、運用マニュアルの記述内容だけでは運用実施に不十分であると考えられる処理の実施については、必要に応じて本市職員及び統合運用管理業者への運用研修を実施すること。

また、運用研修の実施対象となる処理の判断については、本市職員、統合運用管理業者及び受託者間で協議・検討し、決定すること。

(ウ) 運用業務引継ぎ状況報告

受託者は統合運用管理業者と共に運用業務引継ぎにおける実施状況等を報告書に取りまとめ、工程完了報告会等において本市へ報告すること。実績報告書については本市の承認を受けること。