地域情報プラットフォームガイドライン
技術解説　要約

V2.2

財団法人全国地域情報化推進協会

はじめに

本書は、「地域情報プラットフォームガイドライン」の「第 3 章　技術解説」を要約したものであり、単独自治体の庁外との通信で使用するプラットフォーム通信機能とプラットフォーム共通機能について説明しています。

本マニュアルの目的

- 地域情報プラットフォーム導入時に、技術的な解説の参考とする

対象読者

- 自治体においてサービス基盤および業務アプリケーションを導入する調達者

前提知識

- システム構築に関する一般的な知識
- ネットワーク構築に関する一般的な知識
- アプリケーション開発に関する一般的な知識
- オペレーティングシステムに関する一般的な知識

アイコンについて

アイコン	意味
	【ヒント】 役に立つ情報や関連情報などを表します。
	【重要】 記載内容のまとめや特に重要な情報を表します。

目次

第１章 概要

ここでは、地域情報プラットフォーム標準仕様の体系と本書の位置付けについて説明します。

■ 地域情報プラットフォーム標準仕様の体系

地域情報プラットフォーム標準仕様は、業務モデル標準、サービス協調技術標準で規定する標準仕様、およびガイドラインで構成されます。

地域情報プラットフォーム標準仕様の体系を、図 1.1 に示します。

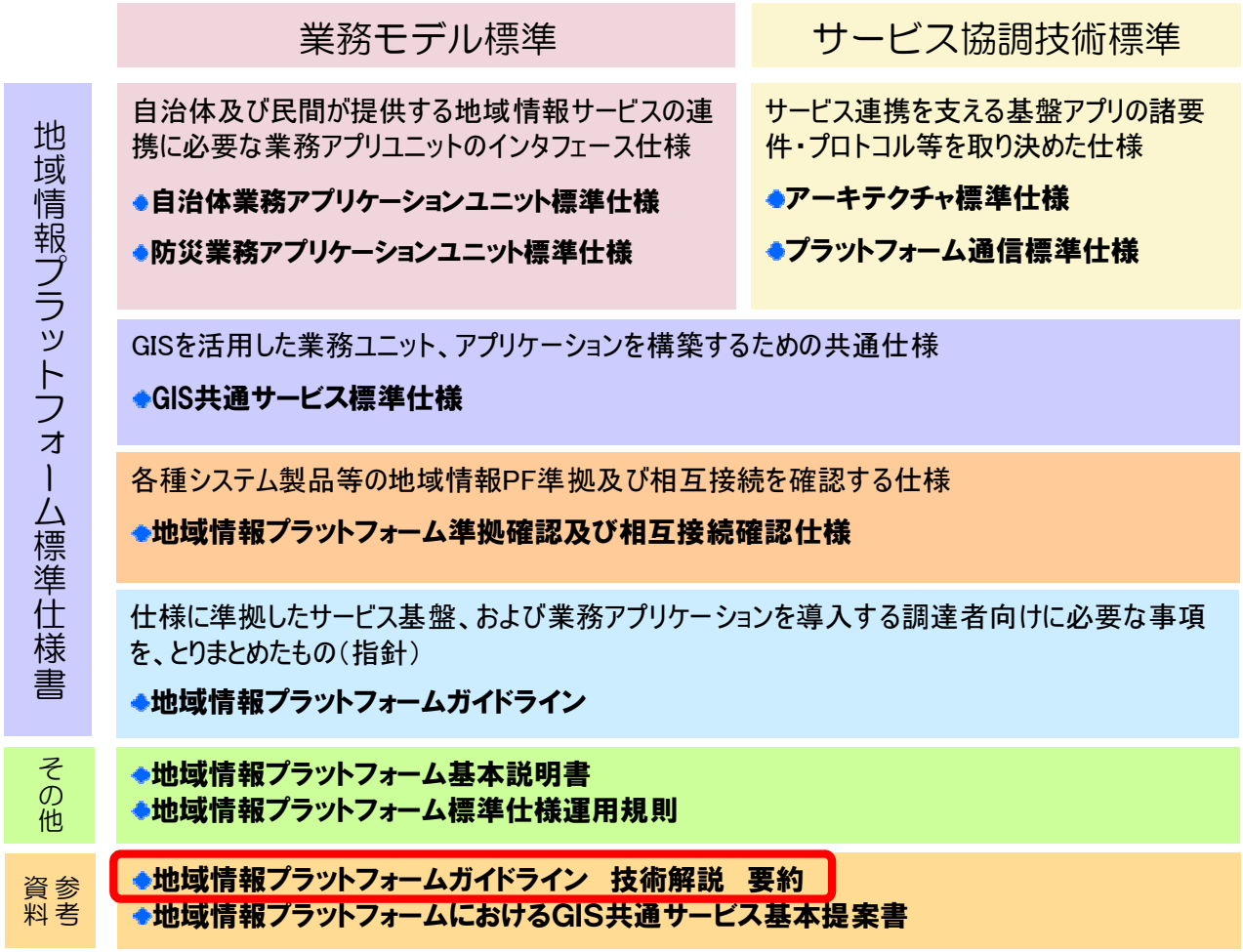


図 1.1　地域情報プラットフォーム標準仕様の体系

『地域情報プラットフォームガイドライン』は、業務モデル標準とサービス協調技術標準における仕様に準拠したサービス基盤、および業務アプリケーションを導入するときに必要な事項をとりまとめたものです。

第 1 章、第 2 章では、調達者向けに必要な情報を集約してまとめ、第 3 章では PF 通信機能、PF 共通機能と、その利用方法についての技術解説としてまとめています。第 4 章ではワンストップ導入および連携定義手順、別冊として GIS 共通サービスガイドラインを紹介しています。

本書の位置付け

本書は、『地域情報プラットフォームガイドライン』の 3 章の一部を簡単に要約したものです。
プラットフォーム共通機能のごとに、概要、導入時のメリット、留意事項、ユースケースを説明しています。
地域情報プラットフォームのシステム基盤の概念を図 1.2 に示します。
下図の赤枠内が、本書の「第 2 章　機能説明」で説明している機能です。

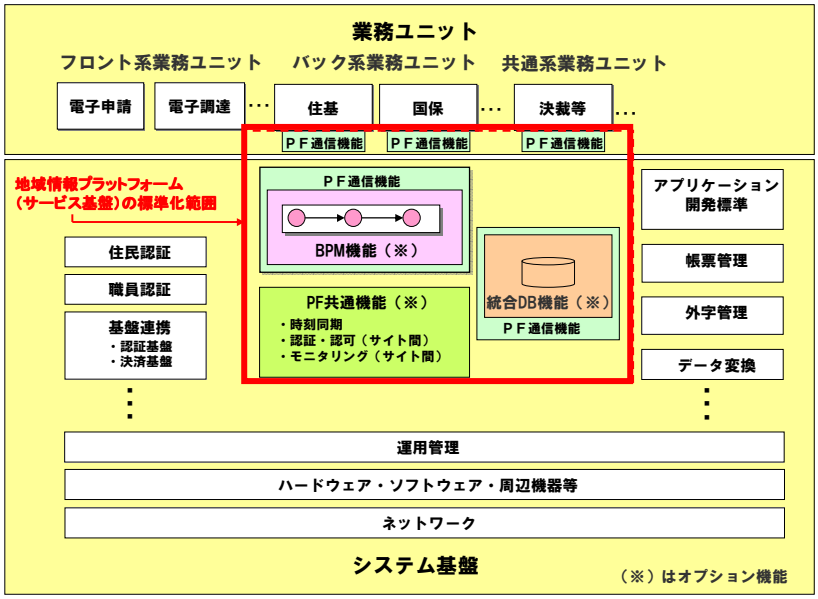


図 1.2　システム基盤の概念図

プラットフォーム共通機能（PF 共通機能）の扱いについて

PF 共通機能とは、自治体単独のサイト内や、庁外の異なるサイトにまたがった業務サービスを連携するときに必要となる、プラットフォームに共通の機能群のことです。

現在（平成 20 年 3 月）は技術仕様を明確にした段階であり、各ベンダが製品を提供するには、もう少し時間を要すると想定されます。したがって現段階においては、PF 共通機能は調達の対象外とします。「地域情報プラットフォームガイドライン」の第 3 章では、PF 共通機能と利用方法の紹介という扱いとし、周辺環境の整備や留意事項もあわせて記載しています。

第 2 章 機能説明

ここでは、PF 通信機能とPF 共通機能ごとに、概要、導入時のメリット、留意事項、ユースケースを説明します。

2.1　PF 通信機能

■ PF 通信機能とは

プラットフォーム通信機能（以降、PF 通信機能）とは、業務ユニットと業務サービスが標準インタフェースや標準規約（セキュリティ、メッセージなど）に準拠して連携を実現するための機能群のことです。次の 9 つの機能を実現できることが求められています。

- **HTTP 通信（IPv4、HTTP1.1）**
- 通信セキュリティ（通信路暗号 SSL3.0(TLS1.0)、サーバ認証）
- 通信セキュリティ（通信路認証 SSL3.0(TLS1.0)、クライアント認証）
- 通信セキュリティ（通信路認証 HTTP のベーシック認証）
- **SOAP 通信（SOAP1.1、document/literal、WS-I ベーシックプロファイル 1.0）**
- 高信頼性通信（WS-Reliability1.1、WS-ReliableMessaging1.1）
- 高信頼通信（MEP 方式）
- **メッセージの XML 定義仕様（XML Schema　1.0、PF 仕様の XML プロファイル）**
- **サービスインタフェースの XML 定義仕様（WSDL1.1、PF 仕様の XML プロファイル）**

PF 通信機能は、業務ユニットや BPM 機能、統合 DB 機能など、他のシステム構成単位の前提ソフトウェアとなります。上記の太字の機能が、最低限必要な機能です。
また、PF 通信機能単独でシステム構成単位とはなりません。

■ 導入時のメリット

PF 通信機能を導入すると、次のようなメリットがあります。

- サービス連携実現に採用している SOAP (Simple Object Access Protocol) 1.1 により、下位通信プロトコルに依存しません。
  現在は、下位プロトコルとして HTTP を使用することが主流ですが、今後、必要に応じて他のプロトコルを採用できます。
- SOAP 通信により、さまざまな機能を提供する Web サービスの仕様のスタックを利用できます。
  ミドルウェアが標準仕様のスタックの実装を提供することにより、セキュリティ、高信頼性などの機能を利用できるようになります。
- 高信頼性通信機能により、SOAP 通信処理の信頼性を向上させ、メッセージの送達保証（失敗時再送）、重複排除、順序保証が実現されます。
  送信側アプリケーションは高信頼性通信処理系にメッセージを渡すだけで、送信側と受信側の高信頼性通信処理系の間のメッセージ交換により、メッセージは高信頼で受信側アプリケーションに渡されます。
- MEP（メッセージ交換パターン）により、通信上で発生した障害は統一的に処理されます。
  高信頼性通信機能を利用すると、回復可能な障害は高信頼性通信機能のレベルで吸収され、回復不能な致命的な障害は、上位層で扱われます。

留意事項

サービスが他のサービスと通信（連携）するためには、通信先のサービスの各種情報を設定しておく必要があります。設定すべき項目として、次のようなものが考えられます。

- HTTP のタイムアウト
- 本文メッセージの最大サイズ（最大バイト数など）
- 各サービスのエンドポイント URL (Uniform Resource Locator)、DNS (Domain Name System)
- 認証機能
- 認証方式の選択（SSL (Secure Sockets Layer) クライアント認証、HTTP ベーシック認証など）
- 認証情報の交換（信頼できる CA (Certification Authority) 情報や ID、パスワードなど）

また、採用するオプション機能に応じて、そのオプション機能に固有の設定が必要になる場合もあります。

これらの情報は、通信するサービス間で何らかの方法で交換される必要があります。将来的にはサービスレジストリ機能などを利用して交換されることが想定されますが、現時点では、サービスの管理者間の情報交換などにより、手動で設定することが現実的です。

2.2　統合 DB 機能

■ 統合 DB 機能とは

統合 DB 機能とは、業務ユニット間で必要となるデータを統一的に管理することで、業務ユニット間のデータ交換を効率的に実現する機能です。このため、業務ユニット同士がデータ交換（情報を共有または連携）できるための機能を有する必要があります。

統合 DB 機能の役割は、提供側業務ユニットを意識することなく、提供側業務ユニットで管理されているデータを利用側業務ユニットから利用するための「データの受け渡し」です。業務間の連携を疎とすることを目的としており、統合 DB 機能におけるデータの管理方法(実装方式)は規定していません（一般的に統合 DB 機能は複数のデータを組み合わせて必要なデータを利用するための「データ統合機能」を持っていますが、この機能については標準化していません）。統合 DB 機能は、業務ユニットが利用するときの利用側インタフェースとして必要な単位で自治体業務アプリケーションユニット標準仕様に準拠した SOAP の業務ユニットインタフェースを有するものとします。オプションとして SQL インタフェースも採用できます。

統合 DB 機能の役割と標準化ポイントを、図 2.2.1 に示します。

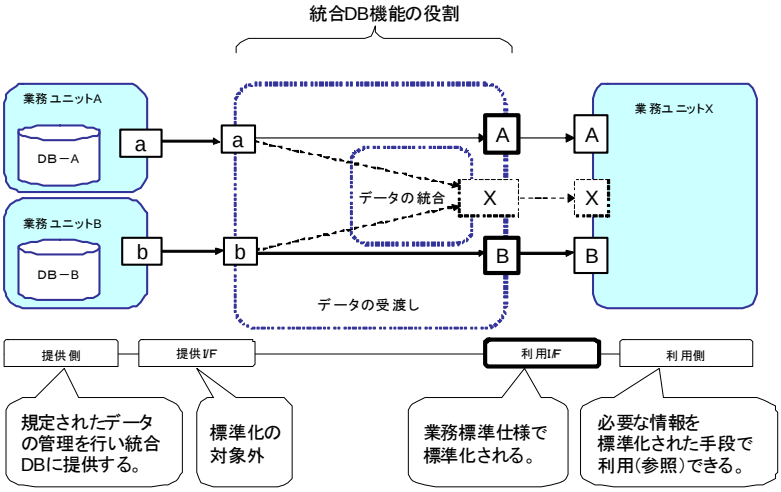


図 2.2.1　統合 DB 機能の役割と標準化ポイント

統合 DB 機能には、次の 2 種類の実装方式があります。

- 公開用 DB 方式（業務ユニット相当の SOAP インタフェース）
  統合 DB 機能として、物理的な DBMS に公開対象の 2 次データ（提供側から提供されたデータ）を保持し、この 2 次データを介してデータを受け渡す方式です。
- 共通インタフェース方式
  統合 DB 機能内に物理的な DBMS による 2 次データの保持を必須とせず、提供側業務ユニットから公開される情報を利用側業務ユニットが必要とする情報として仮想的にアクセスするためのプログラムとして構成された統合 DB 機能です。

「提供側業務ユニット」と「利用側業務ユニット」

自らデータを管理（保持）して、他の業務ユニットにデータを提供する役割を持つ業務ユニットを「提供側業務ユニット」、他の業務ユニットのデータを利用（参照）する業務ユニットを「利用側業務ユニット」と呼びます。これは、データ交換における業務ユニットの役割により区別するもので、1 つの業務ユニットが「提供側業務ユニット」として他の業務ユニットにデータを提供し、「利用側業務ユニット」として他の業務ユニットのデータを利用するのが一般的です。
統合 DB 機能の視点からは、統合 DB 機能にデータを提供する役割を持つ「提供側業務ユニット」、統合 DB 機能を利用する「利用側業務ユニット」と、統合 DB 機能に関する役割によって使い分けています。

統合 DB 機能は、業務ユニット間のデータ連携時に、性能、その他の要件から柔軟にデータ交換を行えるように、必要に応じて採用を検討するオプション機能です。

■ 導入時のメリット

統合 DB 機能を導入すると、次のようなメリットがあります。

- 自治体内における業務ユニット間のデータ連携を効率的に行えます。
- データ交換の側面から、業務ユニットの差し替えが容易になります。
- 既存の業務システムへの地域情報プラットフォーム（以降、地域情報 PF）導入を、段階的に進めることができます。
- 利用側業務ユニットから SOAP インタフェースを使用して統合 DB 機能を利用すると、統合 DB 機能の方式や実装に依存することなく、利用側業務ユニットは必要なデータを取得できます。
- 共通インタフェース方式の統合 DB 機能は、利用側から要求された最新のデータを提供側からオンデマンドで取得するため、リアルタイム性（情報の鮮度）が高くなります。

■ 留意事項

統合 DB 機能の導入時には、次の事項に留意します。

- 統合 DB 機能は多くの業務ユニットのデータを公開する機能であるため、次のようなセキュリティに対する考慮が必要です。
  - 自治体外部（サイト外）からの統合 DB 利用を制限する。
  - 統合 DB 機能で公開するデータは、そのデータごとに、利用側業務ユニット単位で制御する。
  - 統合 DB 機能で公開するデータは、データ項目ごとに、公開または非公開とする業務を規定する。
  - 利用記録としてアクセスログを取得する。
  - 提供側業務ユニットへのアクセス権は適切に管理する。
- 統合 DB 機能の運用が停止すると、地域情報 PF 全体の業務が継続できなくなるため、運用への配慮が重要です。運用に関する事項は、特に採用する製品が持つ機能に依存する部分が多いため、製品の利点や留意点を考慮して検討します。
  - メタ定義や環境設定類は、構成変更ごとに確実なバックアップを取得し、復旧可能な状況にする。
  - 運用時の負荷見積や検証を確実に行い、柔軟な負荷分散によってスケーラブル性を確保する。

- 冗長運転構成によって可用性を確保する。

公開用 DB 方式の統合 DB 機能の導入時には、次の事項に留意します。

- 物理的な DBMS で 2 次データの集中管理を行うため、統合 DB 機能に対する提供側および利用側からのアクセスが集中し、性能が劣化する恐れがあります。性能への配慮が特に重要です。
- 統合 DB 機能で交換対象の 2 次データの実体を保持して管理するため、統合 DB 機能内の DBMS が管理するデータベース容量に留意する必要があります。

共通インタフェース方式の統合 DB 機能の導入時には、次の事項に留意します。

- すべてメモリ上で処理されるデータ統合ミドルウェアによる実装、および専用アプリケーションによる実装では、複数のデータ統合サーバ(統合 DB 機能)を並列運用することが容易であるため、性能面で有利である一方、検索結果を処理できるだけのメモリ量に留意する必要があります。また、提供側業務ユニットへの影響を抑える目的で提供側のレプリカを使用する場合は、提供側にレプリカ用の DBMS が必要です。

ユースケース

公開用 DB 方式の統合 DB 機能の実装パターンを、図 2.2.2 に示します。

統合 DB 機能は物理的な RDBMS(リレーショナルデータベース管理システム)を使用して実装するのが一般的です。XML データベースを使用して実装することもできますが、この場合、多くの提供インタフェース、利用インタフェースは SOAP を使用して実装されます。

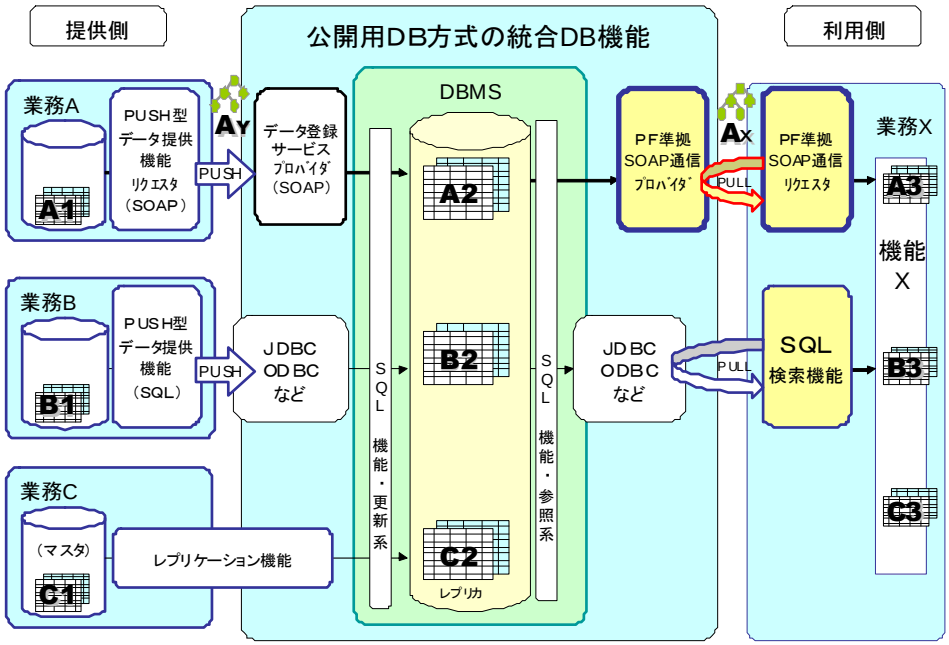


図 2.2.2 公開用 DB 方式の統合 DB 機能の実装パターン

共通インタフェース方式の統合 DB 機能の実装には、次の 3 種類が考えられます。

- データ統合機能を持つ DBMS による実装
  統合 DB 機能として 2 次データを保持せず、利用側からのリクエストに従って提供側にアクセスを行い、PULL型のデータ検索によってデータを獲得します。
- データ統合ミドルウェアによる実装
  統合 DB 機能に DBMS を使用しないで、データ統合ミドルウェアに提供側業務ユニットのスキーマと、利用側に必要なスキーマを定義し、ミドルウェア(またはそのアプリケーション)の機能として利用インタフェースを実現します。具体的には、利用側からの検索要求を統合 DB 機能が受け取ると、必要な提供側業務ユニットに対する検索要求に分解して提供側業務ユニットを検索し、その結果を統合して利用側に応答する処理が動的に行われます。
- 専用アプリケーションによる実装
  利用インタフェースを含めて、地域情報 PF の統合 DB 機能専用のアプリケーションとして実装するパターンです。特徴や留意点は、データ統合ミドルウェアによる実装と同じです。

共通インタフェース DB の長所を最も引き出せる実装パターン

データ統合ミドルウェアによる実装が、オンデマンド、リアルタイム、柔軟な統合パターン、提供側の地域情報 PF 対応が容易など、共通インタフェース DB の長所を最も引き出せます。

データ統合ミドルウェアとしては、EII(Enterprise Information Integration)という分野のソフトウェアが数社から提供されており、フェデレーション機能と呼ばれることもあります。

データ統合機能を持つ DBMS による実装パターンを図 2.2.3 に示します。

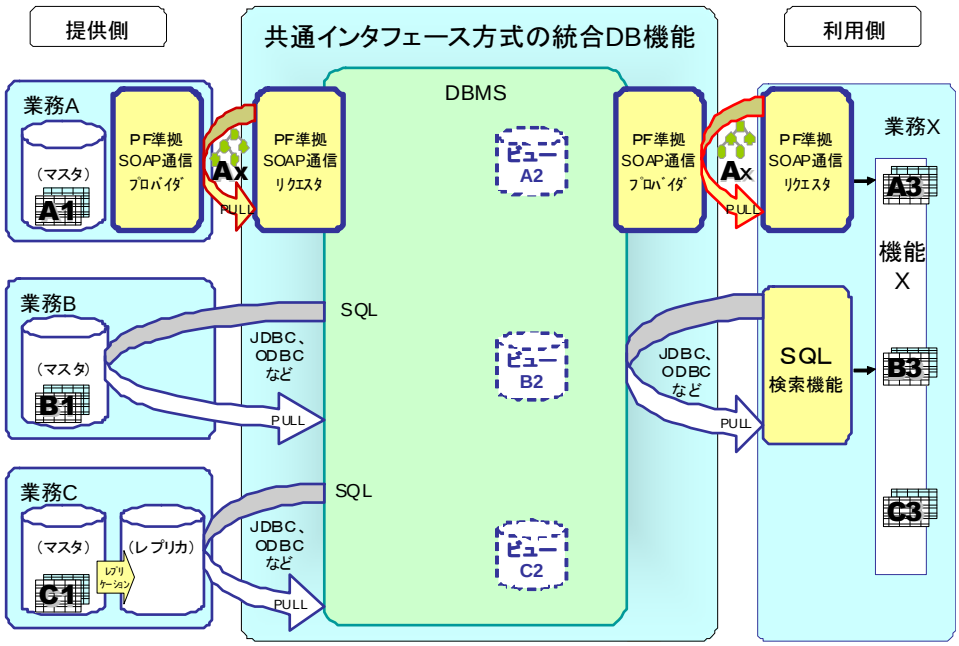


図 2.2.3　共通インタフェース方式の統合 DB 機能のデータ統合機能を持つ DBMS による実装パターン

データ統合ミドルウェアによる実装パターンを図 2.2.4 に示します。

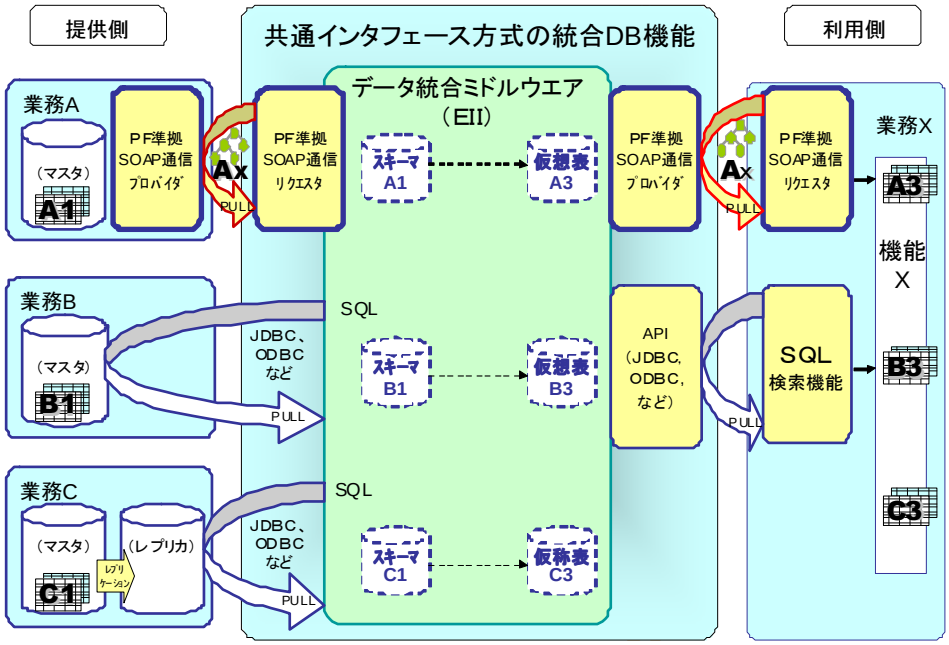


図 2.2.4　共通インタフェース方式の統合 DB 機能のデータ統合ミドルウェアによる実装パターン

専用アプリケーションによる実装パターンを図 2.2.5 に示します。

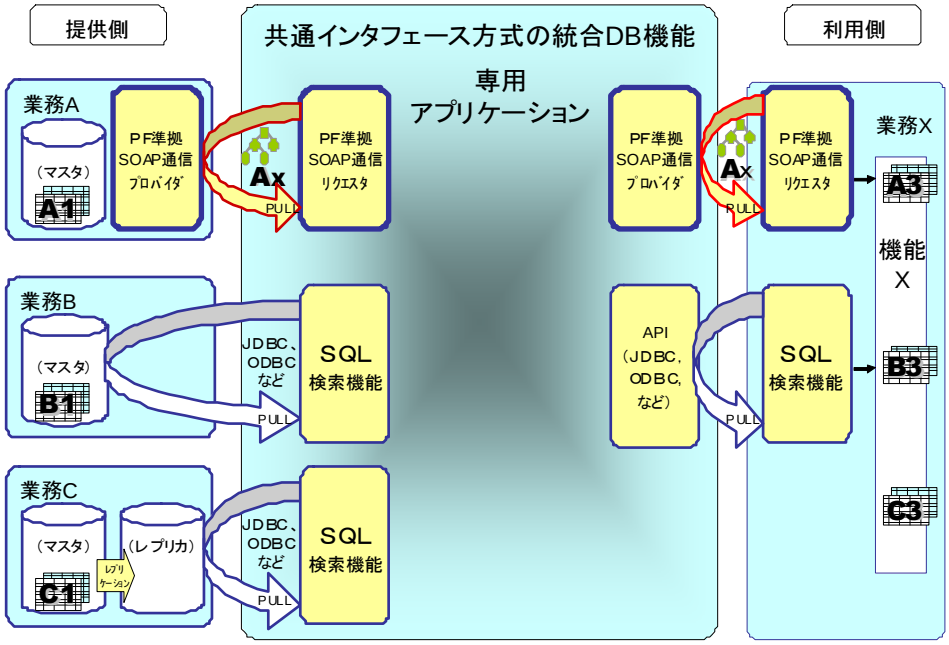


図 2.2.5　共通インタフェース方式の統合 DB 機能の専用アプリケーションによる実装パターン

2.3 BPM 機能

BPM 機能とは

ビジネスプロセス管理（Business Process Management）機能（以降、BPM 機能）とは、自治体の業務サービスおよび自治体間、官民連携業務サービスの実行を制御する機能です。BPM 機能は、業務サービスインタフェースを組み合わせてビジネスプロセスを組み上げ、ワンストップサービスや高付加価値サービスを構築できます。

BPM 機能は、プラットフォーム通信標準仕様に従う機能内容でなければならず、プロセス定義のためのスクリプトは、プラットフォーム通信標準仕様に従うものでなければなりません。

アーキテクチャには、SOAP 通信などと親和性が高く、最新版である WS-BPEL(Web Services Business Process Execution Language) 2.0 を全面的に採用しています。WS-BPEL2.0 の、次の機能を実現できる必要があります。

- 基本アクティビティ（receive、reply、invoke）対応
- 構造化アクティビティ（sequence、flow、if、while）対応
- 変数処理（assign、XPath1.0 利用可能）対応
- エラーハンドリング（fault、throw）対応

ワンストップサービスとは

必要とする作業を一度の手続きですべて完了でき、真に利便性に優れた住民サービスを提供できるサービスのことです。

日本 BPM 協会の定義によるビジネスプロセスマネージメント

日本 BPM 協会は、ビジネスプロセスマネージメントを次のように定義しています。

- 経営目標を実現させる業務（ビジネスプロセス）を迅速に設計し、その改善サイクルを継続的に進める新しい経営手法
- 業務の可視化、デザイン、業務プロセス構築、業務モニタリング、業務実績評価という一連の業務改善サイクルを、ICT(Information and Communication Technology)を利用して継続的に実施すること

地域情報 PF では、このビジネスプロセスマネージメントの考え方を広義概念として取り込み、普及促進を図っています。

BPM 機能は、ワンストップサービスなどでサービスを順次実行するときに利用するオプションです。システム構成上、サービス通信を実施するため、PF 通信機能を有することが前提となります。

■ 導入時のメリット

BPM 機能を導入すると、次のようなメリットがあります。

- 高付加価値で利便性の高いワンストップサービスを導入できます。
  さらに、BPM 機能を応用した利便性の高いサービスを提供できます。
- 自治体内のプロセスと同等のインタフェースを維持しながら、次のようなことを実施できます。
  - 単純に繰り返して行われる操作プロセスの自動化
  - 不必要な手続きの効率化、省力化
  - 1 つの自治体内部のビジネスプロセスの改善
  - 民間等へのアウトソーシング、BPO(Business Process Outsourcing)

■ 留意事項

BPM 機能の製品選定時には、次の事項に留意します。

- プラットフォーム通信標準仕様の要件を満足する製品であること
- セキュリティ要件に対して準拠、または柔軟に対応できる製品であること
- MDA などの開発環境と親和性が高く、開発および実行環境が統合化された製品であること
- 安定したサポートが供給され、実績のある製品であること
- システム運用ツールと連携できる製品であること

次の技術的なポイントにも留意します。

- トランザクション、補償動作
  メッセージ交換パターンおよび異常系処理は、プラットフォーム通信標準仕様で定める方式に従います。
- アクティビティセット
  独自アクティビティセットの利用を含めた拡張機能をどこまで利用するか、そのポリシーを統一的に定めておきます。
- WS-BPEL の記述
  WS-BPEL の記述が複雑な構造になっているものについては、共通ルーチンとしてローカルに配置されるサービス化を行います。
  ローカルサービス化にあたっては、処理性能とのトレードオフを考慮して実装します。
- モニタリング機能との連携
  障害発生時の対応などに有効なモニタリング機能と連携するためのインタフェースをサポートできるように留意します。
- 「リクエスト・レスポンス型同期型受領 Ack＋非同期型レスポンス」時の対応
  地域情報プラットフォームで選択可能なメッセージ交換パターンの 1 つである「リクエスト・レスポンス型同期型受領 Ack＋非同期型レスポンス」時のリクエストの処理とレスポンスの処理を連携させる方式を、業務ユニットの機能の一部として実装します。
- WS-BPEL が受信側となった場合の非同期型の受信タイムアウトの実装
  呼出元の業務ユニットで、タイムアウト監視を行うことを推奨します。
- 排他制御
  排他制御は、一般には業務ユニット内部での実施を基本とします。しかし、これが困難である場合は、WS-BPEL 処理系側でも特別な対処を考慮します。

ユースケース

一般的な民間企業で BPM 機能を導入する手順については、いくつかの文献や、各ベンダが提供するホワイトペーパーなどが存在します。たとえば、日本 BPM 協会の定義している BPM 推進フレームワークが該当します。

地域情報 PF の展開においても、ほぼ同等の技術的な考え方を継承しています。ただ、自治体などの個々の組織体に限らず、全国の自治体、関係団体において高付加価値で利便性の高いワンストップサービスを共通して定義するために、標準的な業務標準、業務インタフェースを定義するという点において、一般の民間企業におけるビジネスプロセスマネージメントの実施手順とは質的に異なる面があります。その差分を、図 2.3.1 に示します。

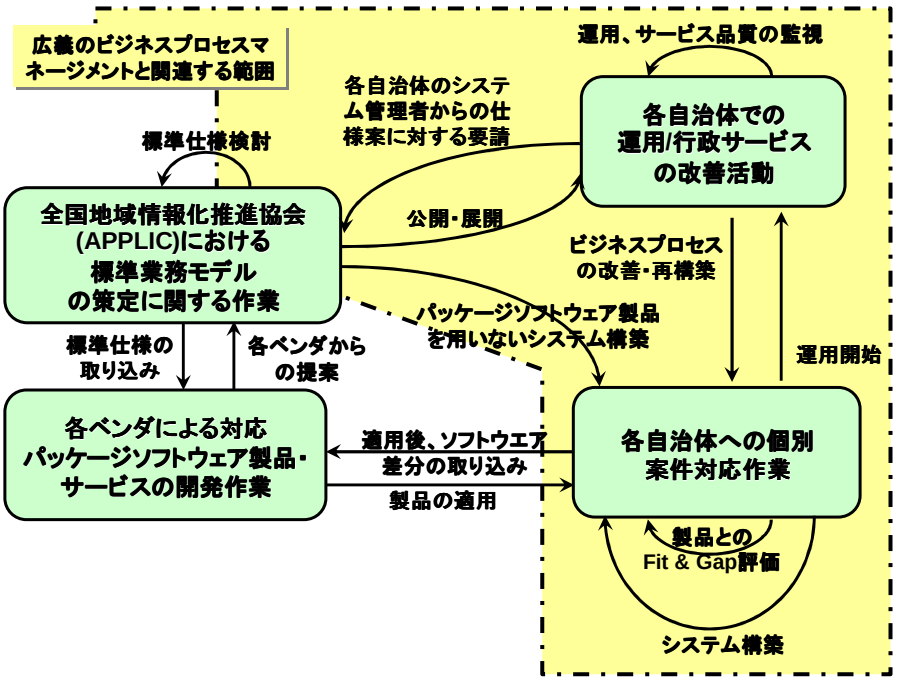


図 2.3.1　地域情報 PF におけるビジネスプロセスマネージメント

上図の一点鎖線で囲まれた部分は、各自治体、関連団体によって実施されるモデリング(分析)から再設計などの、一連のビジネスプロセスマネージメントに関連した作業に該当します。

地域情報 PF では、自治体固有の問題を除外したうえで、汎用的な標準業務モデルの構築を目指しています。これが、従来のフレームワークに基づくアプローチ方法とは異なる点の 1 つです。

参照

- ワンストップサービスの導入については、『地域情報プラットフォームガイドライン』の「第 4 章　ワンストップサービスの導入」を参照

2.4　セキュリティ対策

本節では、地域情報 PF に関連するネットワークのセキュリティ対策について説明します。
最初にセキュリティの脅威について説明し、自治体間および自治体と外部接続のセキュリティ対策と課題について説明します。

■ セキュリティの脅威

地域情報 PF に関連するネットワークと接続パターンを、図 2.4.1 に示します。

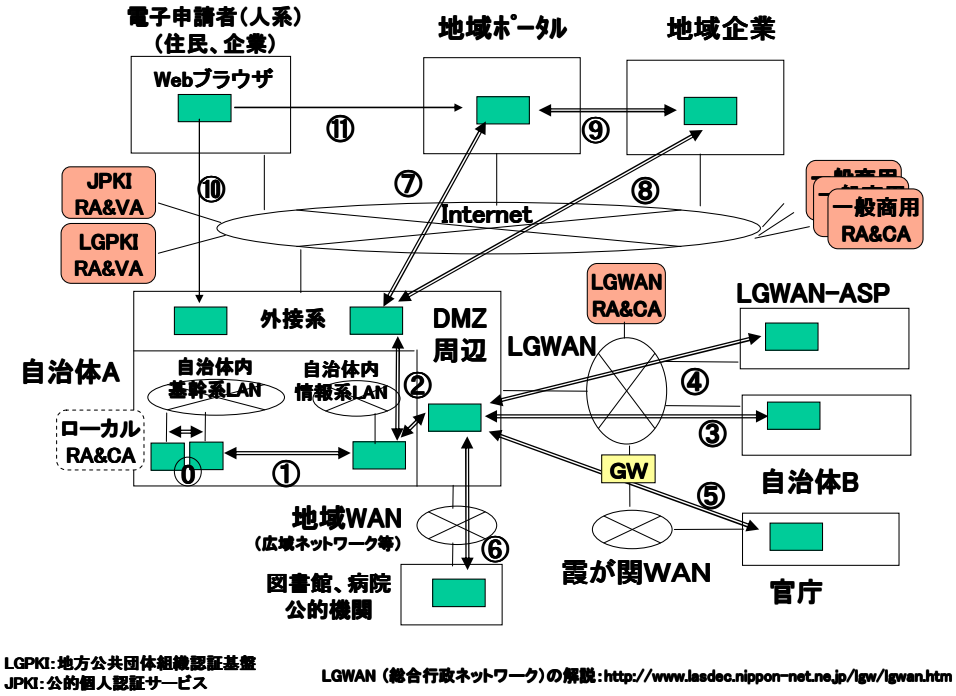


図 2.4.1　地域情報 PF に関連するネットワークと接続パターン

このようなネットワーク接続において、次のようなセキュリティへの脅威に対応する必要があります。

- なりすまし（他人になりすましたサービスの利用、文書の偽り）
- 否認（送信の否認、受信の否認など）
- 通信上の盗聴（送信データの盗聴）
- 通信上の改ざん（送信データの改ざん、破壊）
- データへの不正アクセス（データの改ざん、漏えい、削除、追加）
- システムへの不正侵入（システム侵入、不正なサービス利用）
- ウィルス侵入（感染したビジネス文書やウィルスそのものが侵入）
- DDoS 攻撃（多量の送信データを送信してシステム性能を劣化させる）
- プライバシ情報の不正利用、漏えい

これらのセキュリティへの脅威に対応するために、自治体などの 1 つの組織がセキュリティポリシーを定めています。管理対象全体のセキュリティを確保するための技術は、既存の PKI 技術やファイアウォールなどのインターネットの技術として確立されています。

自治体間や自治体と民間間など、異なるサイト間におけるセキュリティ上の課題を図 2.4.2 に、セキュリティ上の課題への対策技術を、表 2.4.1 に示します。

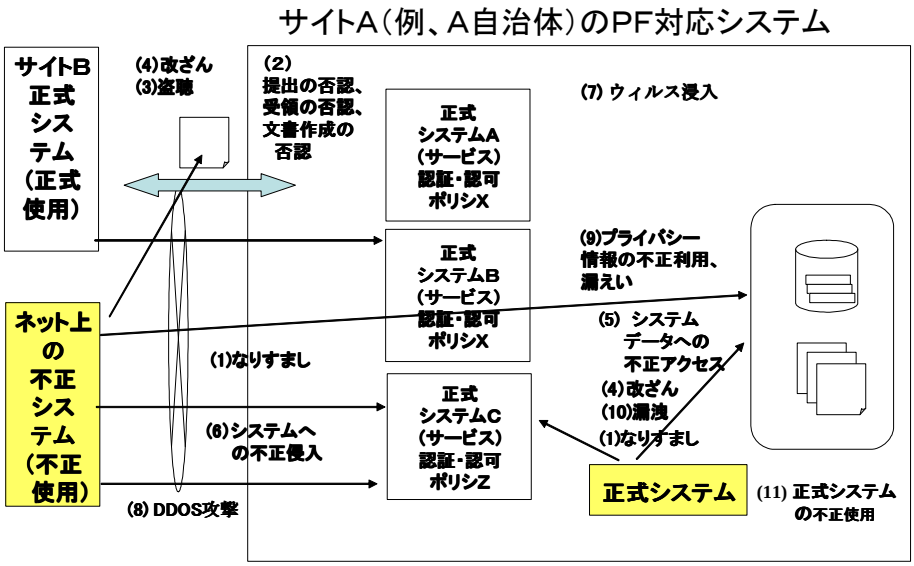


図 2.4.2　異なるサイト間におけるセキュリティ上の課題

表 2.4.1　異なるサイト間におけるセキュリティ上の課題への対策技術

対策技術	内容	対象課題
認証(Authentication)	本人(クライアントのユーザ、マシン、サービス)であることを判定し証明する	・なりすまし ・不正侵入
認可(Authorization)	認証されたユーザに対し、システムまたはアプリケーションの使用許可を判定する	・盗聴 ・漏えい
秘匿性確保	通信内容を第三者が参照できないようにする	・盗聴 ・漏えい
電子署名と検証	情報に対して電子的な署名を行い、情報の改ざん検知や署名者の確認を可能にする	・なりすまし ・改ざん
サービス認証 サービス認可連携	ワンストップ用のサービス認証・サービス認可情報の管理、伝播方法、およびそのモデルに関する技術で、シングルサインオンなどを実現する	・なりすまし ・データの不正アクセス ・不正侵入
プライバシ情報公開	認証時、認可時、およびサービス処理時におけるプライバシ情報の不正利用防止および交換許諾	・プライバシ情報の不正利用 ・漏えい
監査証跡	正式なシステムを不正に使用していないか、情報を統一的に収集し監査したい場合に使用する	・正式システムの不正使用
ウィルス対策	感染したビジネス文書やウィルスそのものの侵入の検知や、感染したデータの駆除など	・ウィルス侵入
DDoS 攻撃対策	負荷集中の監視やネットワーク機器の IP フィルタリング設定などで、複数のサイトからの特定サイトへの集中アクセスによるシステムダウンやサービス停止に対応する	・DDoS 攻撃

自治体のネットワーク設置状況

平成 18 年度 APPLIC で実施の自治体アンケート(母数 108 自治体)の結果を次に示します。

- 54%の自治体が、基幹系業務ネットワークおよび内部系業務ネットワークを物理的に分離しています。
  さらに、この自治体のほとんどが、基幹系業務ネットワークおよび内部系業務ネットワークは分離していますが、ファイアウォール、VLAN で接続可能としています。
- 25%の自治体が、ネットワーク分離の条例などを制定しています。
- 97%の自治体が、セキュリティポリシーを策定しています。

自治体に地域情報 PF を導入するときは、ネットワークポリシーを参照し、システム連携の方針を策定する必要があります。

自治体間でのセキュリティ対策と課題

ここでは、地域情報 PF に基づく自治体間のシステム連携に影響を与えるセキュリティ要件について、ユースケースを考慮しながら説明します。

地域情報 PF で想定する、申請者、地域ポータル、自治体、連携する自治体、民間のシステム連携のユースケースを図 2.4.3 に示します。

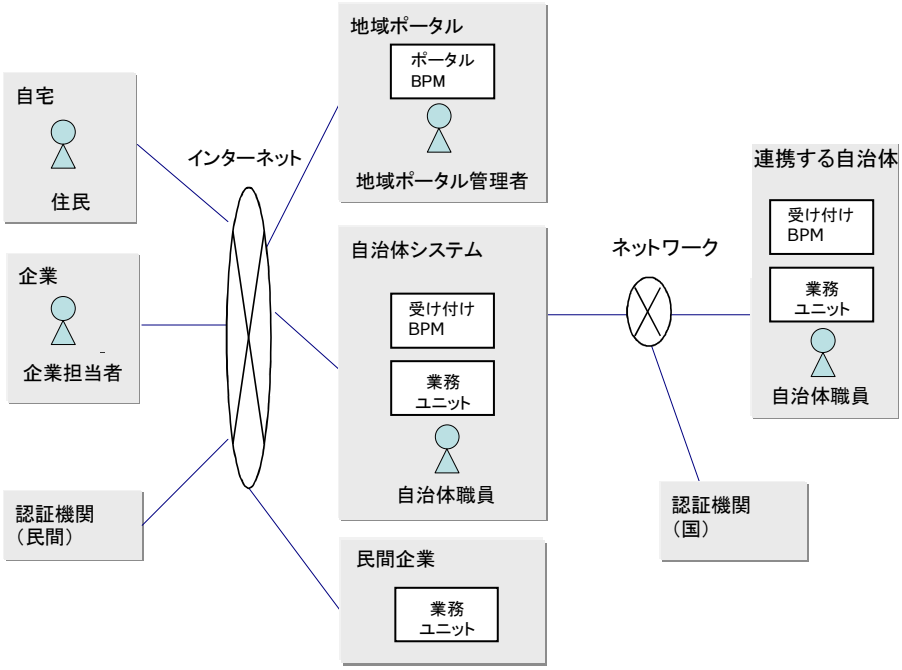


図 2.4.3 地域情報 PF で想定するシステムのユースケース例

上図のユースケースでは、地域ポータル、自治体、連携する自治体および民間をサイトとみなし、主に次の 4 つの業務処理を想定しています。

- 申請者による申請書の送信
- 申請者による進捗状況の問い合わせ

・ 自治体から他自治体への照会
・ 自治体による公文書の配布

これらの業務処理シーケンスを、図 2.4.4 に示します。

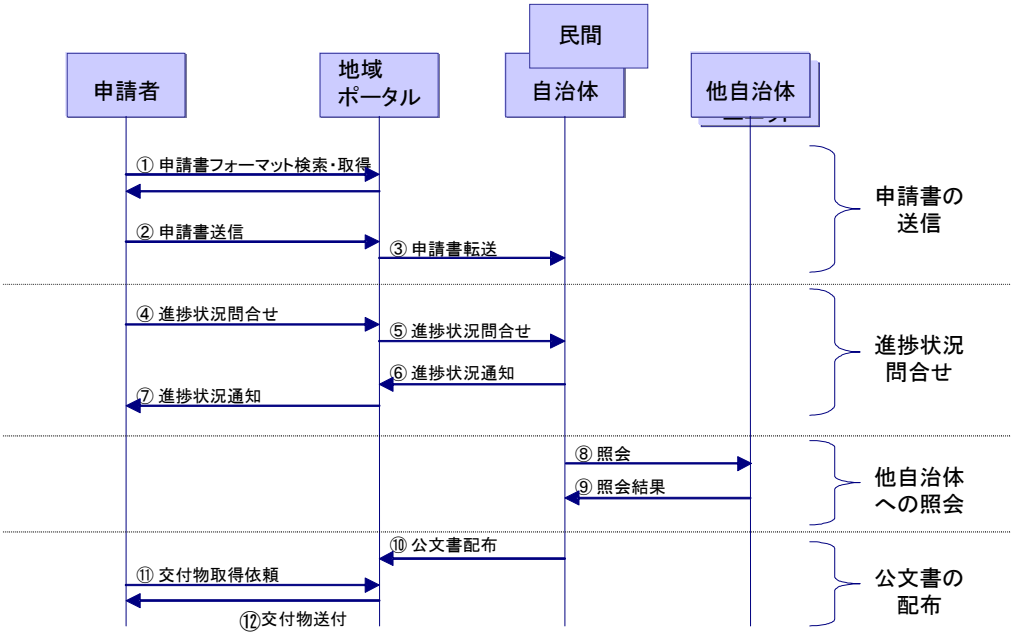


図 2.4.4 地域情報 PF のシステム連携で想定する処理の流れ

上図で想定するセキュリティ要件を、次に示します。

・ データは他の人に読み取れられないようにすること
　： 秘匿性確保
・ データの改ざんを検出できること
　： 改ざん防止、なりすまし防止
・ 他のサイトからの処理依頼において、依頼元を認証できること
　： なりすまし防止
・ 正式システムの不正使用を監査できること
　： 不正使用
・ 複数サイト間の連携処理に認証や認可処理の一元化が必要な場合、認証認可が連携できること
　： 改ざん防止、なりすまし防止
・ 複数サイト間の連携処理に認証や認可処理の一元化が必要な場合、認証のための他サイトへのプライバシ情報公開制御ができること
　： プライベート情報の不正利用や漏えい、なりすまし、不正侵入の防止

自治体内システムの職員端末とサーバマシン間のセキュリティに関する仕様

自治体内システムの職員端末とサーバマシン間のセキュリティに関しては、すでに自治体内で採用されている仕様があり、プラットフォーム標準仕様としては特に規定していません。

■ 自治体の外部接続のセキュリティ対策と課題

ここでは、地域情報 PF における自治体の外部接続の実現と検討ポイントについて説明します。
自治体の外部接続の実現イメージを、図 2.4.5 に示します。

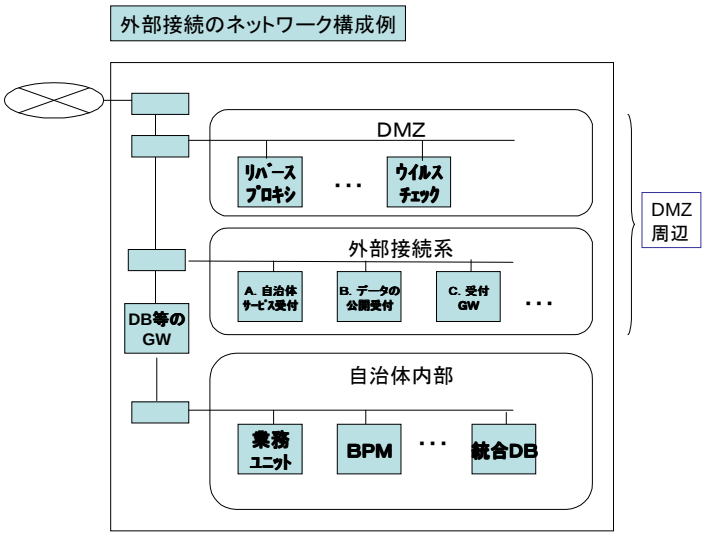


図 2.4.5　自治体の外部接続の実現イメージ（ネットワークとシステム構成）

上図では、ネットワークのセグメントとして、次の 3 エリアを想定しています。

- DMZ（緩衝エリア、外部と内部とが両方アクセスできるエリア）
  ファイアウォール、NAT（アドレス変換）、リバースプロキシ、プロキシなどを設置
- 外部接続エリア（外部接続サーバを配置）
  外部に公開されるサービスを実施するサーバを配置し、自治体内部とデータ交換する
- 自治体内部エリア
  自治体内部のサーバ群（情報系ネットワークと基幹系ネットワークで分断されている場合がある）

このような場合、次のような対策が必要です。

- 自治体内部のサーバと、外部接続サーバとデータ交換するサーバは、IP リーチャビリティを遮断するため、DB や共有サーバを中継して、外部接続サーバとデータ交換します。
- 同様に、自治体内部で情報系ネットと基幹系ネットで分断されている場合は、DB や共有サーバを中継してデータ交換します。

汎用受付システムなどを構築するときの参考資料

汎用受付システム構築の参考資料（調達編・共同方式の場合　最新 V1.2 版）が、次のサイトに公開されています。

http://www.lasdec.nippon-net.ne.jp/rdd/elg15/02_kouchikuchoutatsu.pdf

これは、汎用受付システムなどの構築、運用に関する共通事項（平成 15 年 6 月 6 日改定、共通システム専門部会了承）をふまえていますので参照してください。

次に、外部接続サーバと外部、自治体内部とのサービス呼び出しの関連図を、図 2.4.6 に示します。
これは、論理的なサービスの呼び出し図です。物理的にネットワークが分断されている場合は、データ交換やサービス呼び出しの中継を行うゲートウェイ機能を、両方のネットワークの中間に設置する必要があります。

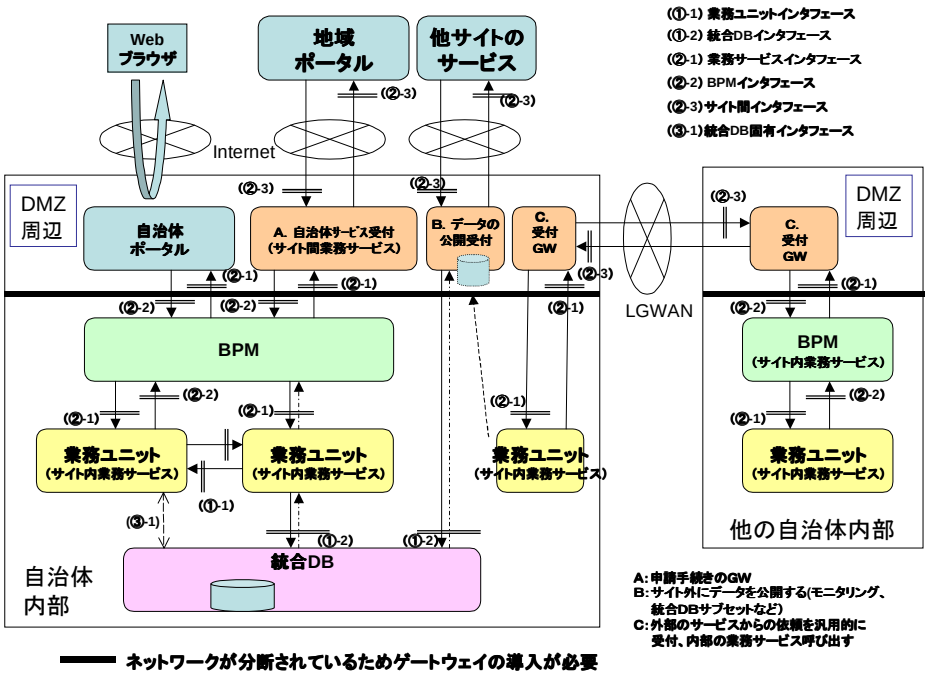


図 2.4.6　自治体の外部接続の実現イメージ（サービスの呼び出し）

2.5　認証・認可機能

■ 認証・認可機能とは

認証とは、本人であることを判定し証明することです。ここでいう本人とは、クライアントのユーザ、マシン、サービスの抽象的表現です。

認可とは、認証されたユーザに対し、システムまたはアプリケーションの使用許可を判定することです。

地域情報 PF においては、自治体職員の認証・認可と、公開している Web サイトのログイン時に行う住民に対する認証・認可を考慮する必要があります。

自治体職員の認証・認可では、次の 2 つを考慮します。

- 業務ユニットの職員認証

  これは地域情報 PF の標準規定の範囲外ですが、次の 2 つの認証方式が採用されています。

  - 個別業務システムごとのログイン（認証と認可）
  - Web アプリケーションや統合ソフトウェアによるシングルサインオン（SSO）

  現在は、認証方式も個別のベンダーソリューションが多く採用されています。

- サイト間の職責認証

  今後、自治体間で職員による問い合わせ型の文書照会型のサービス（自治体間での処理依頼と結果通知）が、職員の職責で実施される場合が想定されます。

  この場合の処理フローを、図 2.5.1 に示します。

  - 依頼元自治体内の業務ユニットで、職員を認証し、起案、承認後、この職員が依頼文書に対し LGPKI で職責署名（PF 自治体組織電子署名・検証仕様）し、他自治体へ依頼文書を送付する。
  - 受けた自治体は LGPKI の証明書検証により、依頼元の職責を確認（PF 自治体組織電子署名・検証仕様）し、依頼された照会業務を職員が業務ユニットで実施し、回答文書を作成し、返す。

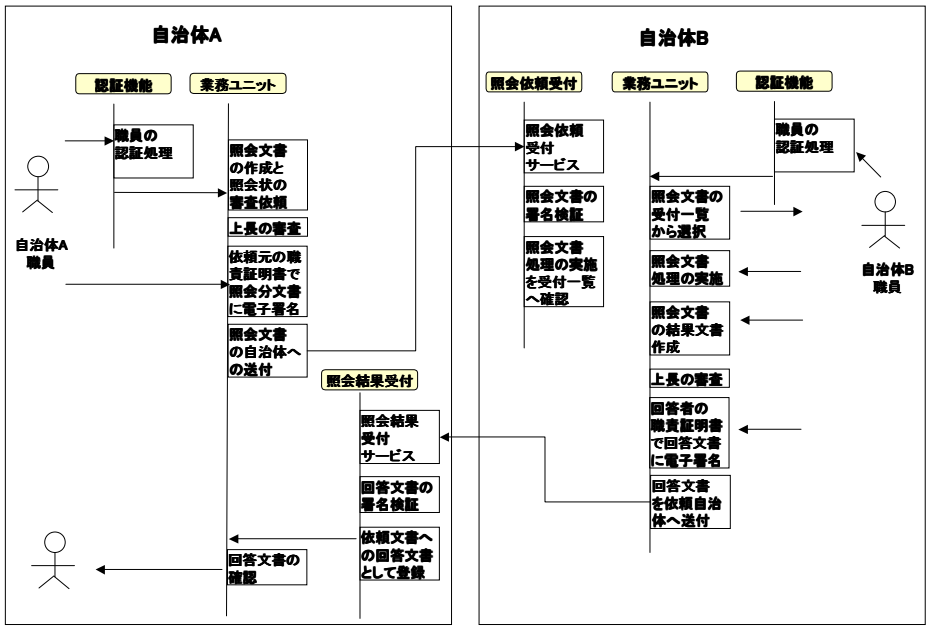


図 2.5.1　サイト間の自治体職員の職責認証の処理方式

住民に対する認証・認可では、次の 2 つの場合を考慮します。

- 住民が単一 Web サイトを利用する場合
  これは、地域情報 PF の標準規定の範囲外です。
  この場合の処理フローを、図 2.5.2 に示します。
- 住民がポータル経由で複数 Web サイトを利用する場合
  地域情報 PF では、住民が地域ポータルで認証を受け、自治体や民間の地域サービスを使う場合が想定されます。この場合、PF 通信で接続する自治体などのサービスの認証処理のための ID と認証情報（パスワードなど）を、地域ポータルに登録する必要があります。この実現方式の例を、図 2.5.3 に示します。
  なお、この実現方式には、いくつかの課題があります。課題への対策については、以降の「■ユースケース」の【サービス認証連携】を参照してください。

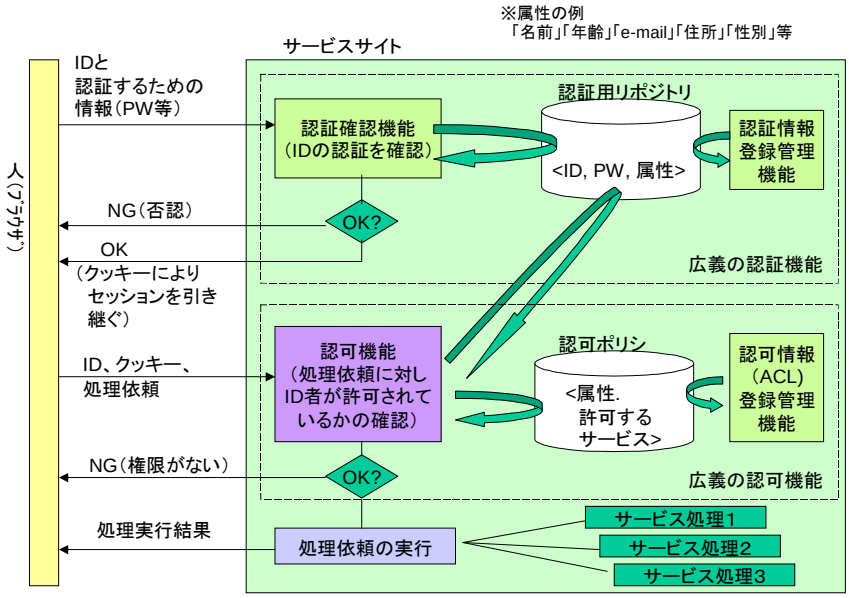


図 2.5.2　Web アプリケーションにおける認証・認可の処理方式

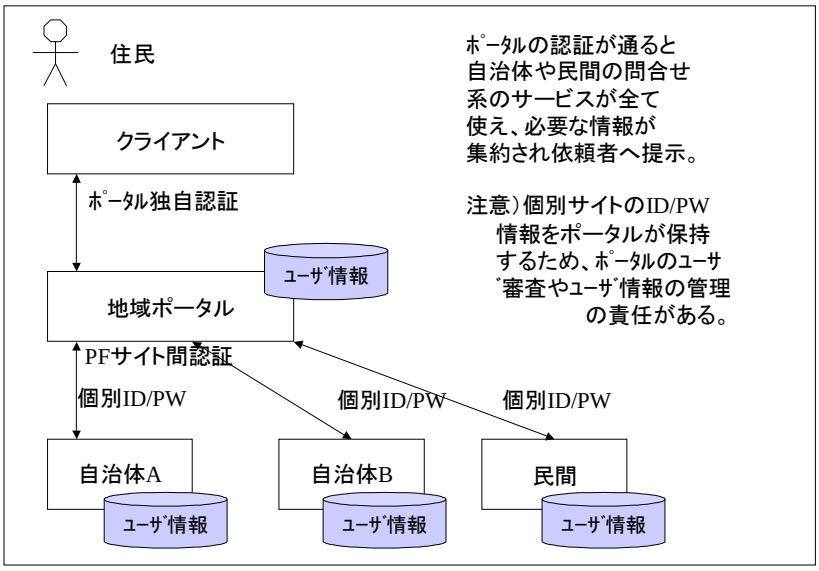


図 2.5.3　住民がポータル経由で複数 Web サイトを利用する場合の認証・認可実現方式例

■ 導入時のメリット

サイトをまたがる業務連携システムにおける認証・認可情報を、継承できます。

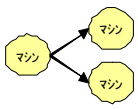
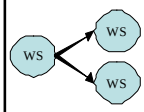
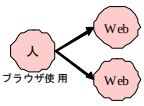
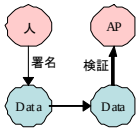
■ ユースケース

【認証】

地域情報 PF では、次の 4 つが認証の対象として想定されます。

- 人(Web ブラウザなどのアプリケーション画面を操作する人)
- サービス(Web サービス)
- 文書
- マシン

認証の対象「人」は、PF 標準規定の範囲外となります。
これらの認証のユースケースと実現技術の関係を図 2.5.4 に、認証の要件を表 2.5.1 に示します。

区分	技術要件	ユースケース	自治体内	民間ー自治体 自治体ー自治体	一般用語	証明書・運用
マシン系 L1	・マシーンからの 接続要求の認証 ⇒ **マシン認証**	 L1	**標準化済み:** ・SSL(TLS)認証 ・HTTPベーシック 認証	**標準化済み:** ・ SSL(TLS)認証 ・HTTPベーシ ック認証	・サーバ認証 ・クライアント 認証	・自治体内: 独自 ・自治体間: LGPKI ・民間と自治体: 民間
サービス系 L2	・依頼元のサービス 認証 ⇒ **サービス認証**	 L2ー1 L2ー2	**標準化対象:** 申請を各ユニット へ: ・WSS (ID/PW) ・独自	**標準化対象:** 地域ポータルか ら自治体へ ・WSS(ID/PW) ・WSS+SAML(★)	・サービス認証	・自治体内: 独自 ・自治体間: LGPKI ・民間と自治体: 民間
Web系 L3	・人に割付けた ID/PW or 証明書 でブラウザからの アクセスを認証 ⇒**Webユーザ認証** **(PF標準規定の範囲外)**	 L3	**標準化対象外** 職員ポータル: ・クッキー(独自)	**標準化対象外** 住民が官と民へ: ・SAML (★) ・クッキー(独自)	・SSO (シングルサインオン)	・自治体内: 独自 ・自治体間: 未整備 ・民間と自治体: 未整備
文書系 L4	・データ作成者の 認証 ⇒ **電文認証**	 L4ー1 L4ー2 L4ー3	**標準化済み:** ・電子申請形式	**標準化済み:** 自治体間: ・電子申請形式 民間ー自治体: ×標準化未だ	・署名検証 ・証明書検証	・自治体へ申請:JPKI ・自治体間: JPKI ・民間と自治体: (JPKIは使えない、 新しい枠組みが 必要)

人:申請者や自治体職員など特定の個人を示し、人がブラウザや電子申請ソフトウェアを使って操作することを意味する。

WS:Web サービスのサービス要求者や Web サービス提供者のアプリケーションを示す。

Web:Web アプリケーションを示し、人が Web ブラウザで操作する対象アプリケーションを示す。

AP:Data の署名を検証し、正しい署名のとき、その申請者の権限に基づき、処理を行うアプリケーションを示す。

(★) 異なる運用組織間での SSO の実現では、IDP(ID プロバイダ)の運営母体の不在が課題になる。

図 2.5.4 認証のユースケースと実現技術の関係

表 2.5.1　認証の要件定義例

	#	誰(何)を (IDの保持者)	IDを何によって 認証し	IDに何の属性を 付与するか？
L1	マシン系	・サーバ （レスポンダ側） ・クライアント （リクエスタ側）	・SSLサーバ証明書 ・SSLクライアント証明書 ・HTTPベーシック認証	マシーンの分類: ・接続許可
L2	サービス系	・PF管理主体を同じくするサービス(AP) ・PF管理が異なるサービス(AP) ・異なるPFのサービス(AP)	認証連携: ・Webサービスセキュリティ ・XML署名、SAML　等	同一PF内: ・認証グループ 異なるPF間: ・管理団体
L3	Web系	・一般の人 ・職員(事務系) ・職員(システム系) ・民間サービスの人(事務系) ・民間サービスの人(システム系)	個人認証: ・電子証明書(PKCS＃12)認証 ・パスワード認証 ・ICカード認証や生体認証 シングルサインオン: ・シングルサインオン(SSO)技術	ロール: ・自治体内の住民 ・システム管理者(自治体) ・業務実施者(自治体) ・システム管理者(民間) ・業務実施者(民間)
L4	文書系	・申請文書 ・起案文書 ・交付文書	個人認証: ・電子証明書(PKCS＃12)認証 ・XML署名	ロール: ・自治体内の住民 ・システム管理者(自治体) ・業務実施者(自治体)

【認可】

地域情報 PF では、認可については規定していませんが、認可の要件を表 2.5.2 に、認可のユースケースを図 2.5.5 に示します。

表 2.5.2　認可の要件

ID に対する属性	認可の条件	許可の対象	認可の範囲
申請人	サービス時間内	申請(CRUD)	同じ自治体内
システム管理者(自治体)	何時でも	システムモニタ(CRUD)	同じ自治体内の全システム
業務実施者(自治体)	サービス時間内	ビジネスプロセス状態(R)	同じ自治体内の BP 状態のみ
システム管理者(民間)	サービス時間内	自治体受付システムの状態(R)	管理対象自治体の受付システムのみ
業務実施者(民間)	サービス時間内	自治体の××文書(R)	自治体内で正式承認されたもののみ

C:作成、R:参照、U:更新、D:削除

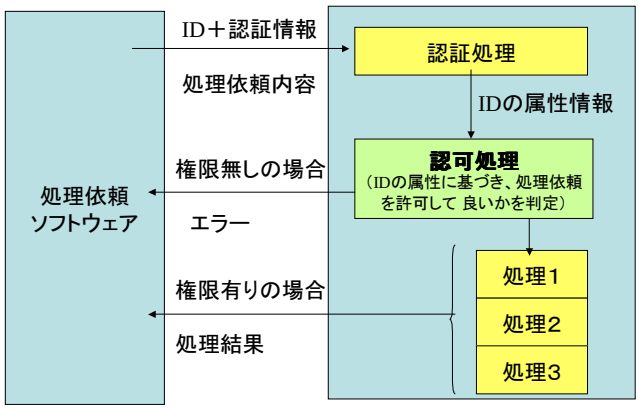


図 2.5.5　認可のユースケース

【サービス認証連携】

Web サービスなどを利用したワンストップサービスを実現する場合、一般的な Web アプリケーションとは異なり、必ずしもエンドユーザがサービスの利用者とはなりません。このため、呼び出された側の Web サービスではエンドユーザの認証を必ずしも行うことができないという問題があります。

例:エンドユーザが Web ブラウザを用いてポータルにログインした後、ポータルが自治体 A の Web サービスを呼び出す場合

呼び出された自治体 A の Web サービスで、エンドユーザの認証を行うには、ポータルと自治体 A で同一のユーザ ID を共有し、これを使う手段が考えられます。しかし、これを行うには、ポータルとポータルが呼び出す全サービスで、ユーザ ID の共有が必要となります。

これを自治体・民間間のように異なる ID 体系で連携して適用するのは、困難です。

これに対応するための、自治体と民間でサービス認証処理を連携させる場合のユースケースを、図 2.5.6 に示します。

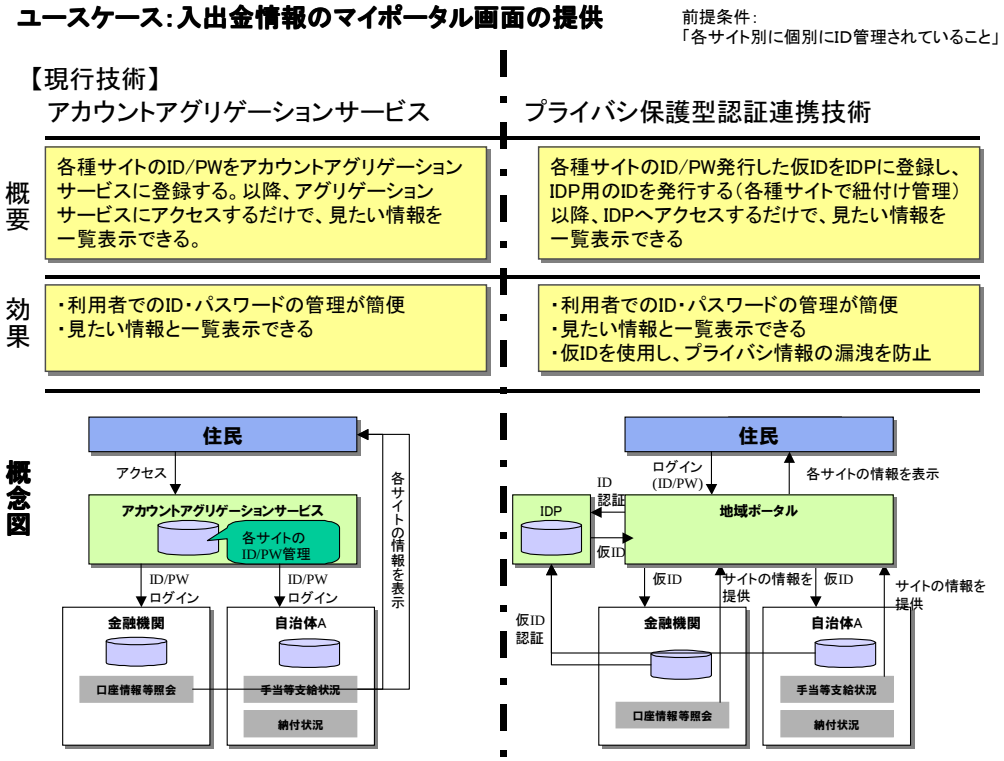


図 2.5.6　サービス認証処理連携のユースケース

【認証・認可連携】

自治体間の情報照会処理における認証・認可連携のユースケースを、図 2.5.7 に示します。このユースケースでは、権限管理基盤技術を使用しています。これは、自治体間の所得照会などの業務において、将来的な適用の検討が想定されます。

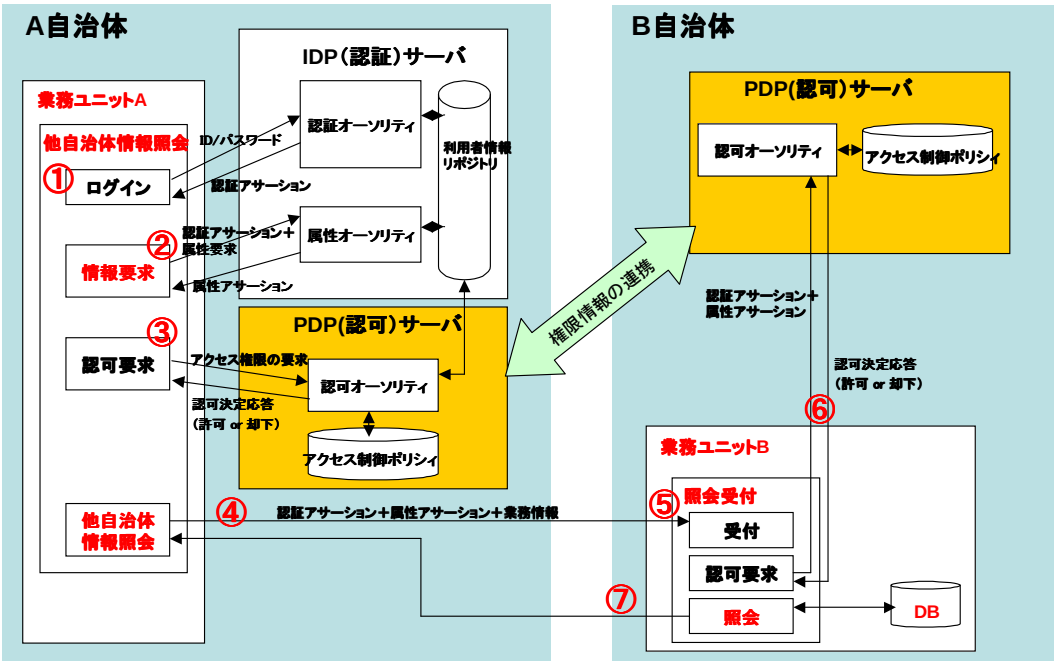


図 2.5.7　権限管理基盤技術を使用した認証・認可連携のユースケース

① A自治体の業務ユニットAが、ある申請者のB自治体での情報を照会したい場合に、他自治体情報照会機能にログインする。

② IDP による認証を受け、認証アサーションと属性アサーションを受け取る。

③ 他自治体情報照会機能は、ログオンした職員が B 自治体へのアクセス権限があるかを PDP に対し問い合わせる。

④ 職員に権限がある場合は、情報照会に進み、B 自治体の業務ユニット B に対し認証アサーション、属性アサーション、業務情報（対象の申請者情報等）を送付し、照会を依頼する。

⑤ B 自治体の業務ユニットBでは、情報照会受付機能が④の認証アサーション、属性アサーション、業務情報を受け取る。

⑥ 情報照会受付機能では、A 自治体から受け取った照会を依頼している職員に情報照会の権限があるかを PDP に問い合わせる。

⑦ 職員に権限がある場合は、対象申請者の情報を A 自治体に送信する。

権限管理基盤技術とは

異なるサイト間の認可において、複数のアプリケーションで使用されるサービス利用者の権限情報を一元的に管理し、サイトをまたがったサービス利用者に対しても権限情報の整合性を維持する機能です。

2.6　モニタリング機能

■ モニタリング機能とは

モニタリング機能とは、散在する情報を Audit として収集する仕組みを提供し、実施状況の把握、進捗管理を通して「可視化」の基盤を提供する機能です。

SOA (Service Oriented Architecture)は、運用のポリシー、アーキテクチャが異なる複数組織間連携の基盤として注目を浴びています。これは、各組織が利用・保持する機能を外部から利用しやすい形に切り出し、サービスとして定義・提供し、さらには複数のサービスを組み合わせることでシステム間連携を実現するアーキテクチャです。SOA 化が進展することで、組織をまたがるシステム間の連携を大規模に実現でき、この結果としてビジネスプロセスと呼ばれる大きなサービス実施、ワンストップサービスの実現が可能になります。

このように、高い潜在力を持つ SOA ですが、さらに、より高い価値を提供するためには、そのうえで進められるビジネスプロセスの実施状況・品質をモニタリングでき、サービス選択の幅が広いことも重要です。ビジネスプロセスの実施状況・品質をモニタリングできれば、その品質を低下させているサービスや、それを実施しているシステムリソースを特定でき、対策を講じることができます。

なお、モニタリングの範囲はワンストップサービス実施時における BPM の追跡までとし、システム稼働状況（パフォーマンス監視、生死監視、ネットワーク監視など）は対象外とします。

「Audit」とは

「サービスやシステムリソースの、ある一時点の状態を示すもの」を一般化した名称です（「ログ」の概念を一般化したもの）。従来この概念は、話題となる領域によって「ログ」、「イベントログ」、「Audit Trail」など、さまざまな名称で呼ばれてきました。モニタリング機能は複合的な領域を対象とするため、地域情報 PF の仕様では、これらを統一した概念として「Audit」を用います。

地域情報 PF の仕様では、次の Audit を定義しています。

- BPM(Business Process Management) Audit
- WS アプリケーション Audit
- メッセージ Audit

■ 導入時のメリット

モニタリング機能を導入すると、ビジネスプロセスの改善を促進できます。

特にビジネスプロセスが複数組織をまたがって実行された場合の、実施状況の把握、進捗管理に直接的な効果があります。

モニタリング機能をより高次な段階まで利用するために

サービス、ビジネスプロセスの種々の特性や KPI (Key Performance Indicator)は、事象が発生した段階で発生する Audit を収集し、解析することで把握できます。よって、Audit 収集の密度が高く、その品質が高いほど、モニタリング機能をより高次な段階まで利用できます。

留意事項

モニタリング機能を実装するときは、次の点に留意します。

- Audit の提供時には、柔軟なインタフェースの構成と、柔軟に変換モジュールなどを組み込める設計が求められます。
  - Audit 機能に関して、今後、国際標準化の検討が進むと予想されるため、Audit 提供の配置について実際の運用条件に柔軟に対応するため、緩やかな構成を推奨します。
  - Audit の形式についても推奨案を定義していますが、これも実際の運用条件に柔軟に対応するため、緩やかな定義を前提としています。このため、柔軟性を確保するためには、インタフェースの運用の段階で、必要に応じて公開するなどの処置が必要となります。
- モニタリング機能のアーキテクチャ標準仕様に基づき、監視アプリケーションなどのアーキテクチャについては規定していません。このため、監視アプリケーションの配置位置を柔軟に選択・構成できますが、より広域にモニタリングを実現するうえで、Audit Proxy などとの密結合な実装は推奨しません。
- 監視クライアントと監視アプリケーション間のインタフェースについても、仕様事項としては規定しません。

ユースケース

自治体、民間会社、地域ポータルなどの横断的なサービスを事例とした、モニタリング機能の実装例を模式化したものを図 2.6.1 に示します。

この図は、モニタリング機能の実装・配置に力点を置いているため、ファイアウォール装置、ルータ装置、LGWAN（総合行政ネットワーク）などは省略しています。

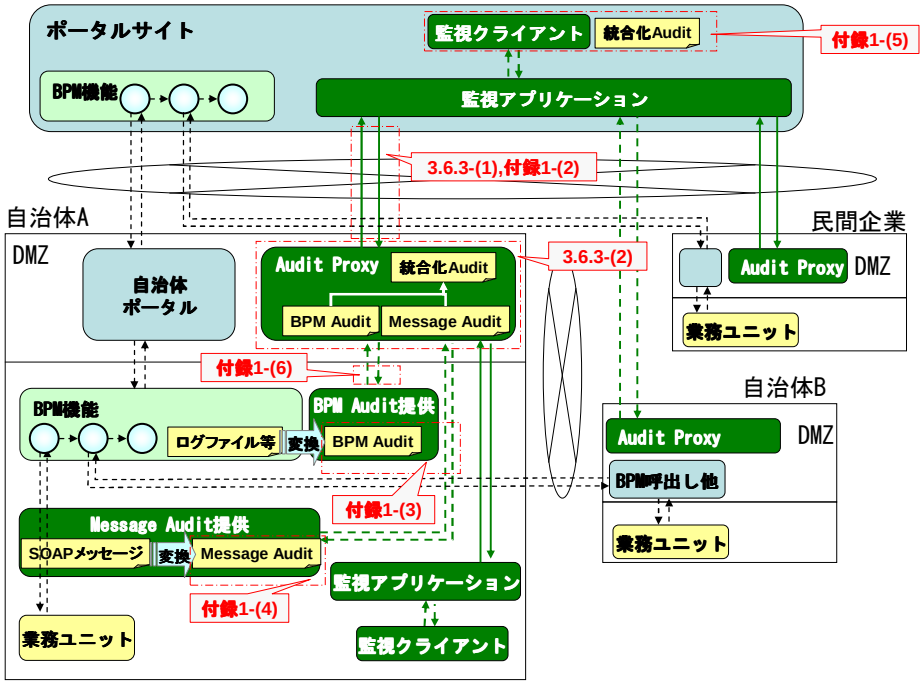


図 2.6.1　モニタリング機能の実装模式図

モニタリング機能の各要素は分散的に配置され、監視アプリケーションがその中心となり、大きくは 4 つ配置されています。

- 1 つは、ポータルサイトまたは集中管理センターに配置されるべき監視アプリケーション、監視クライアントであり、当該モニタリング機能の通常利用を想定しています。
- 他の 3 つは、地域ポータル、自治体 A、民間企業などに配置される Audit Proxy や監視アプリケーションであり、当該モニタリング機能の拡張利用時を想定しています。各組織体内または組織体からプロセス監視、サービス監視を行います。

地域ポータル、自治体 A、自治体 B、民間企業に配置される BPM 機能、業務ユニットなどはマルチベンダ条件下で調達されるため、各 Audit 提供機能とその変換機能は、それぞれ Audit のガイドラインに適合しつつも調達機器に適合する形で実装されます。たとえば、BPM Audit の提供は、図 2.6.1 の自治体 A のように BPM 機能のサーバに組み込まれる場合もありますが、専用のアダプタ装置が置かれる場合もあります。また、メッセージ Audit の取得にあたっては、専用の収集モジュールを配した装置が置かれる場合があります。

監視アプリケーションと Audit Proxy 間の通信プロトコルは、十分な柔軟性を許容しているアーキテクチャ標準仕様に基づいて実装され、その問い合わせには受付番号などが用いられます。監視アプリケーションと Audit Proxy 間の通信プロトコルは、プラットフォーム通信標準仕様である SOAP(Simple Object Access Protocol)を許容していますが、限定的に利用可能な場合は、プラットフォーム通信標準仕様との相互連携を前提のうえで他方式も利用可能とします。

モニタリング機能では、アーキテクチャ標準仕様で定義されるように、次の 4 つのインタフェースがあります(図 2.6.1 内の赤い一点破線枠、参照先は『地域情報プラットフォームガイドライン』の「第 3 章　技術解説」)。

- モニタリング問い合わせインタフェース
- 監視クライアントインタフェース
- BPM・WS アプリケーション Audit 提供インタフェース
- メッセージ Audit 提供インタフェース

参照

- マルチベンダ下でのモニタリング機能実装例については、『地域情報プラットフォームガイドライン』の「第 3 章　技術解説」の「付録 4」を参照

2.7　ユーティリティ機能

本節では、次の 5 つのユーティリティ機能について説明します。

- 時刻同期機能
- サービスレジストリ機能
- リポジトリ機能
- 統合レジストリ機能
- ビジネスメッセージルーティングゲートウェイ機能

時刻同期機能

■ 時刻同期機能とは

時刻同期機能とは、地域情報 PF 標準を採用して動作するサーバなどのマシンの「時刻同期」を実施する機能のことです。

本機能はサイト内で使用するため、調達範囲になります。

■ 導入時のメリット

時刻同期機能を導入すると、次のようなメリットがあります。

- モニタリング機能、監査証跡機能など、マシン間の時刻を統一できます。
- 問題発生時のトラブルシューティングに、マシン間の時刻をふまえて対応できます。

■ 留意事項

次の場合に、時刻同期機能は必須です。

- モニタリング機能、監査証跡機能など、マシン間の時刻が一致していることを前提にしている機能がある場合
- 問題発生時のトラブルシューティングに、マシン間の時刻をふまえたログなどから責任を切り分ける必要がある場合

■ ユースケース

階層的に配置した NTP サーバと NTP クライアントのシステム例を、図 2.7.1 に示します。

サイト内の業務ユニットや BPM 機能、統合 DB 機能などのサーバマシンが、NTP クライアントとなります。NTP クライアントは、マシンが起動された段階で、サイト内の NTP サーバにアクセスし、時刻同期を行います。

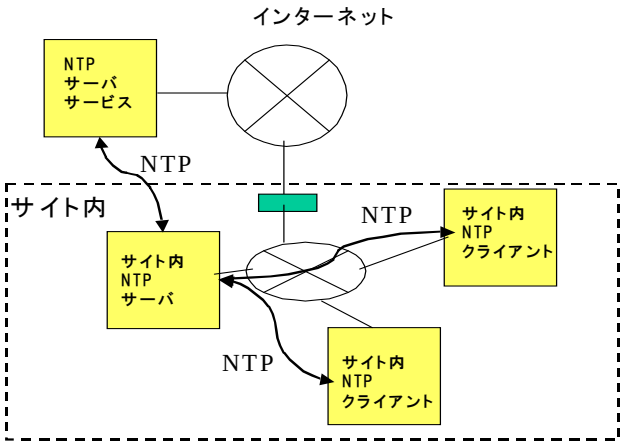


図 2.7.1　時刻同期の実装例

NTP（Network Time Protocol）とは

ネットワークに接続される機器において、機器が持つ時計を正しい時刻へ同期するためのプロトコルです。

参照

- NTP サーバと NTP クライアントの設置と設定に関する定義については、『アーキテクチャ標準仕様』の「4.5.3.3　ユーティリティ機能」を参照

サービスレジストリ機能

■ サービスレジストリ機能とは

サービスレジストリ機能とは、サービス情報を管理する蓄積庫のことです。サービス情報のライフサイクル（登録、更新、削除）を管理し、これら登録されたサービス情報を検索できるサービスを提供します。

サービスの提供には、次の 2 つの方法があります。

- UDDI(Universal Description, Discovery and Integration)などを使用して、動的にサービス先を探す方法
- Web サイトなどでサービス情報を公開する静的な方法

参照

- 詳細な定義については、『アーキテクチャ標準仕様』の「4.5.3.3　ユーティリティ機能」を参照

■ 導入時のメリット

サービス情報のライフサイクル（登録、更新、削除）を管理でき、これら登録されたサービスを提供できます。

■ ユースケース

プラットフォーム標準仕様に基づく各種 Web サービスの登録、検索、公開のユースケースを次に示します。

- 管理者
  各種サービスを提供するコミュニティの主体者（地域ポータル運営者など）
- 使用者
  登録された各種 Web サービスを利用し、地域サービスなどを提供する主体者
- 要件
  管理者が管理、登録するWebサービス（自治体や民間など）のカタログ情報を、使用者が検索し、ダウンロードできること

リポジトリ機能

■ リポジトリ機能とは

リポジトリ機能とは、標準仕様関連書類、システム開発仕様、プログラム、用語定義、項目辞書などを蓄積、管理するデータベースなどの、蓄積機能のことです。

参照

・ 詳細な定義については、『アーキテクチャ仕様書』の「4.5.3.3　ユーティリティ機能」を参照

■ 導入時のメリット

統一された規約、制度のもとで、各種ドキュメント類を管理できます。

■ ユースケース

【ユースケース 1】

プラットフォーム標準仕様の、バージョン別の各種ドキュメントの蓄積と公開のユースケースを次に示します。

- 管理者
  プラットフォーム標準仕様の管理者
- 使用者
  公開する各種ドキュメントを参照する人（自治体、製品ベンダなど）
- 要件
  管理者は、地域情報プラットフォーム標準仕様運用規則に基づき、次のプラットフォーム標準仕様の管理と使用者への公開ができること

  【ドキュメント類の例】

  - 自治体業務アプリケーションユニット標準仕様
  - アーキテクチャ標準仕様、プラットフォーム通信標準仕様
  - 地域情報プラットフォーム準拠および相互接続仕様
  - 地域情報プラットフォームガイドライン
  - 地域情報プラットフォーム基本説明書

【XML 定義類の例】

- 自治体業務アプリケーションユニット標準仕様で規定される XML 定義類
  - 業務ユニットインタフェースに関する標準規定の XML 定義類(WSDL/XSD)
  - ワンストップサービスに関するサンプル XML 定義類(BPEL/WSDL/XSD など)

【ユースケース 2】

プラットフォーム標準仕様を活用した、自治体の設計共通リポジトリ(文書管理)のユースケースを次に示します。

- 管理者
  地域情報 PF に対応した、自治体システムの調達から運用、保守までを担当する自治体の管理者
- 使用者
  地域情報 PF に対応した、自治体システムの開発を実施する担当者
- 要件
  管理者は、使用者が作成した次の自治体システムに関する設計情報を管理できること
  - プラットフォーム標準仕様や自治体個別要件に基づいてカスタマイズした自治体内標準仕様書
  - 工程管理資料、設計ドキュメント、UML、ソースコードなど

統合レジストリ機能

■ 統合レジストリ機能とは

統合レジストリ機能とは、多様化するサービス利用者とサービス提供者間の関係(サービス利用形態)を二者間の「合意」として策定し、UDDI(Universal Description, Discovery and Integration)などの従来のレジストリが管理する情報と合わせて「サービス情報」として管理、監視する機能のことです。サービス提供者またはサービス管理者が、サービスの運用状況や、サービス利用者との合意に基づいた目標品質を管理、把握し、これら「サービス情報」をサービスの品質にフィードバックできるサービス管理基盤を、本機能で構築できます。

アーキテクチャ標準仕様の統合レジストリに記載されている機能要件を満たした統合レジストリ機能では、次の 2 つのエージェント機能を提供できます。

- 暗号化処理
  サイトをまたがってサービス利用者とサービス提供者間でメッセージを交換するとき、サービス提供者側がメッセージを暗号化できない場合、エージェントが代理でメッセージを暗号化することで通信路上のセキュリティを確保します。
- 目標品質(サービスレスポンスタイム)の管理
  サイトをまたがってサービス利用者とサービス提供者間がサービス連携をするとき、あらかじめサービス利用者とサービス提供者の間で取り交わしたレスポンスタイムなどに基づき、サービス提供者側のリクエスト、レスポンスタイムの計測によって目標品質を管理できます。

統合レジストリ機能の処理フローと処理概要を、図 2.7.2 に示します。

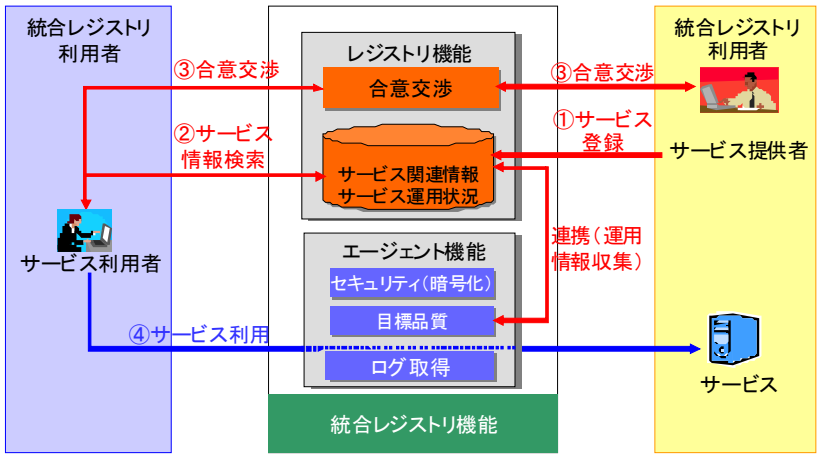


図 2.7.2　統合レジストリ機能の処理フローと処理概要

統合レジストリ機能の利用シーンを、図 2.7.3 に示します。

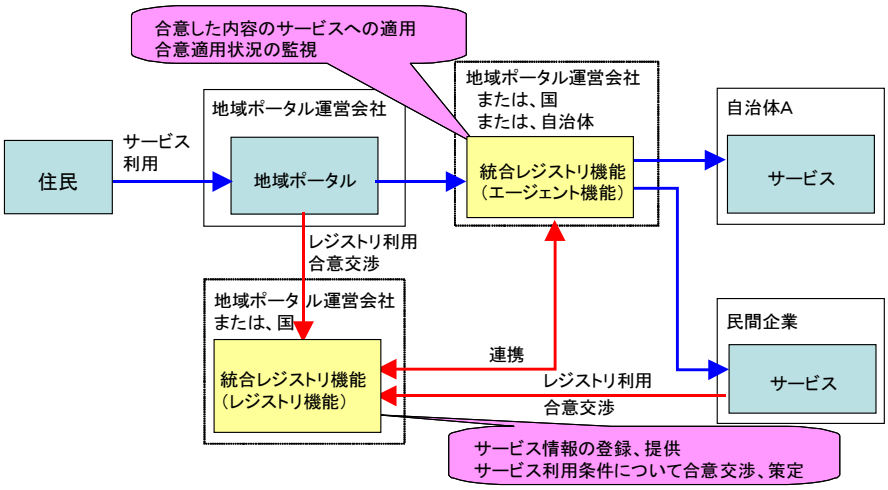


図 2.7.3　統合レジストリ機能の利用シーン

■ 導入時のメリット

統合レジストリ機能を導入すると、サービス利用者に、高付加価値サービスを迅速に安定して提供できます。

■ 留意事項

統合レジストリで管理する範囲、運用主体などを、今後精査しておく必要があります。

ユースケース

統合レジストリ機能の実装モデルを、図 2.7.4 に示します。

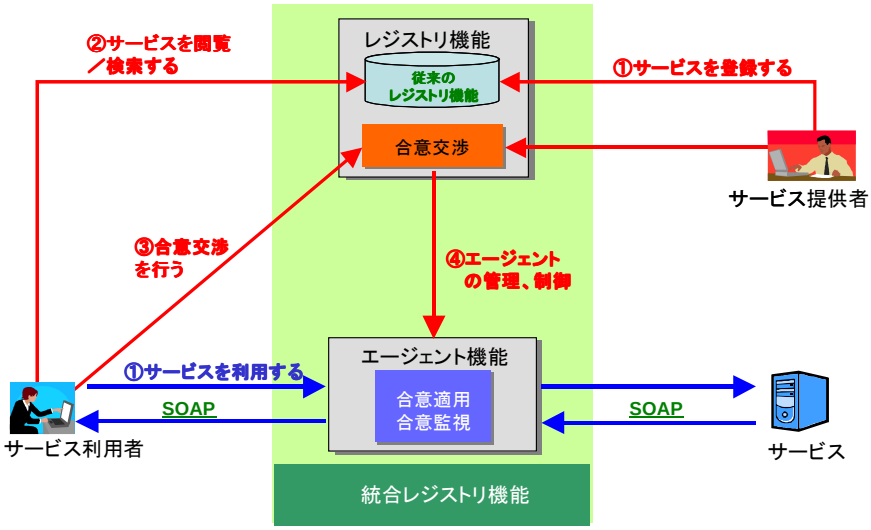


図 2.7.4　統合レジストリ機能の実装モデル

ビジネスメッセージルーティングゲートウェイ機能

ビジネスメッセージルーティングゲートウェイ機能とは

ビジネスメッセージルーティングゲートウェイ機能とは、メッセージヘッダ部に記載された送信先（To タグ項目の値）に、メッセージ本体を動的に送信代行する Proxy として動作する機能のことです。

たとえば次のようなシーンでは、業務メッセージの送信先を、受信した申請書類の内容や業務プロセスの処理結果に応じて動的に変更する必要があります。

- ポータルからの情報照会の申請書類から照会先団体を取り出し、その団体名に基づいて照会依頼を送信する（図 2.7.5）
- ある団体からの業務メッセージの処理結果を後日返信する場合、業務メッセージの送信元に応じた返信先の動的変更が必要となる（図 2.7.6）

地域情報 PF では、この動的な業務メッセージ送信先を制御する機能を「ビジネスメッセージルーティングゲートウェイ機能（略称：BMR-GW 機能）」と呼びます。

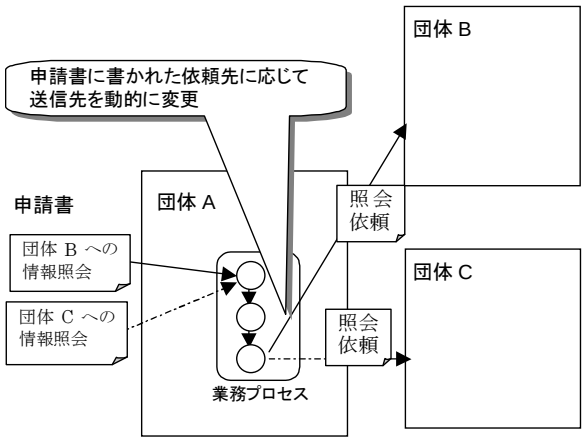


図 2.7.5 動的な送信先変更

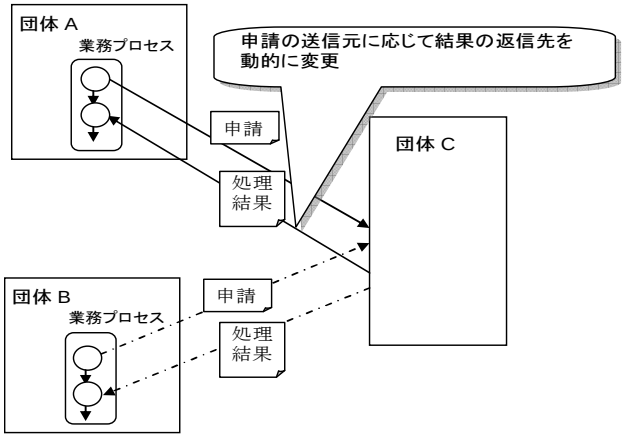


図 2.7.6 送信元に応じた動的な返信先の変更

■ 導入時のメリット

業務メッセージの送信先を、受信した申請書類の内容や業務プロセスの処理結果に応じて動的に変更できます。

■ 留意事項

ビジネスメッセージルーティングゲートウェイ機能は、オプションです。

ただし次のような場合は、動的に送信先を変更する本機能をプラットフォームに実装します。

- 複数箇所から呼び出される非同期呼び出しがある場合
- WS-BPEL で記述されたビジネスプロセスで、送信先の動的変更を実現する場合
  WS-BPEL 仕様に従って EndpointReference を使用することが考えられますが、ビジネスプロセス配備時に送信先を静的にバインドする WS-BPEL 処理系の場合、こうした機能が使用できない可能性があります。
- 一般的な業務ユニットで、複数の呼び出し元から非同期で呼び出される場合
- 一般的な業務ユニットで、業務内容によって呼び出し先の業務ユニットを動的に変える必要がある場合

2.8　メッセージ交換パターン

■ メッセージ交換パターンとは

メッセージ交換パターンとは、メッセージ群の交換の類型を定義するものです。
地域情報 PF では、次の 3 種類のメッセージ交換パターンを標準仕様として採用しています。

・ リクエスト型受領 Ack あり
同期型のメッセージ交換パターンです。開始側は、処理要求などの要求メッセージを送信するとともに、同一セッションで応答側からの受領 Ack の受信も行います。応答側では、要求メッセージに対する応答メッセージは返しませんが、受領 Ack を同一セッションで送信するパターンです。
処理概要を図 2.8.1 に示します。

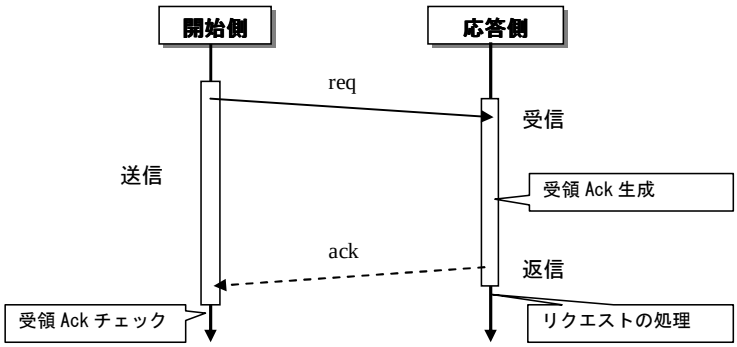


図 2.8.1 「リクエスト型受領 Ack あり」の処理概要

・ リクエスト・レスポンス型同期型レスポンス
要求メッセージの送信と同一のセッションで、応答側からの業務処理結果情報の応答メッセージを返す同期型のパターンです。受領 Ack の通知は行いません。開始側は、要求メッセージの送信を行った後に、同一のセッションで応答側からの応答メッセージを受信します。応答側は、要求メッセージを受信後、受信確認用の受領 Ack を返すことなく、要求された業務処理を実施し、その後、その結果情報を開始側に応答メッセージとして返します。
処理概要を図 2.8.2 に示します。

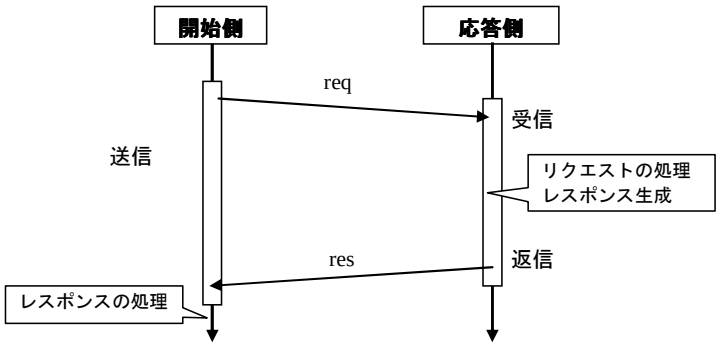


図 2.8.2「リクエスト・レスポンス型同期型レスポンス」の処理概要

- リクエスト・レスポンス型同期型受領 Ack＋非同期型レスポンス
  要求メッセージの送信とは別セッションで、応答側から業務処理結果情報の応答メッセージを返す非同期型です。要求メッセージと応答メッセージのそれぞれに対して、相手側から受領 Ack を受信します。応答側（レスポンス送信側）で、応答メッセージに対する受領 Ack を無視することも許容しています。
  処理概要を図 2.8.3 に示します。

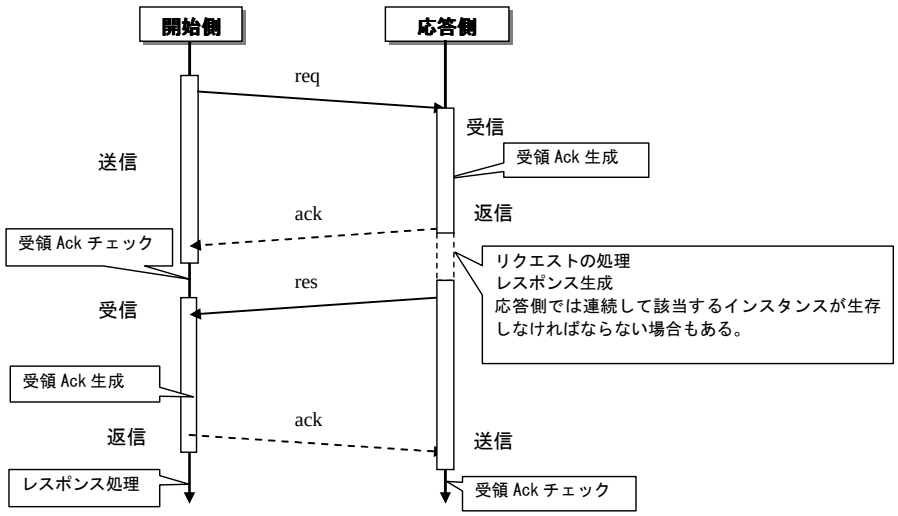


図 2.8.3「リクエスト・レスポンス型同期型受領 Ack+非同期型レスポンス」の処理概要

リクエスト型のメッセージ交換パターンとは

要求メッセージだけで構成され、業務処理結果を含んだ応答メッセージが存在しないパターンです。業務ユニットからの帳票出力指示、バッチプログラムや他の業務ユニットへの通知などが想定されます。受領 Ack の有無と受信の仕方によって、次の 3 パターンがあります。

- リクエスト型受領 Ack なし
- リクエスト型受領 Ack あり
- リクエスト型非同期型受領 Ack

リクエスト・レスポンス型のメッセージ交換パターンとは

リクエストと、それに対する業務データを含むレスポンスの組で構成されるパターンです。受領 Ack の有無、受領 Ack とレスポンスの送受信の仕方によって、次の 4 パターンがあます。

- リクエスト・レスポンス型同期型レスポンス
- リクエスト・レスポンス型非同期型レスポンス
- リクエスト・レスポンス型同期型受領 Ack＋非同期型レスポンス
- リクエスト・レスポンス型非同期型受領 Ack＋非同期型レスポンス

■ 導入時のメリット

地域情報プラットフォームが標準仕様として採用しているメッセージ交換パターンを導入すると、次のメリットがあります。

- 実装が容易である
- 障害検知が容易である
- 障害検知の仕組みを明確に定義できる
- 業務の要件に応じて最適な方式を選択できる
- SOAP 1.1 などの Req-Res パターンに合致する

■ 留意事項

メッセージ交換パターンを実装するときは、次の点に留意します。

- 業務処理時間やタイムアウト時間などを含めた業務要件に応じて、メッセージ交換パターンを選択します。
- 「リクエスト型受領 Ack あり」では、応答側での処理結果が開始側に返されないため、要求メッセージに基づく処理が成功したかどうかを開始側で確認できません。
- 「リクエスト・レスポンス型同期型レスポンス」では、開始側のセッションのタイムアウト時間内に応答側の処理が終了しなかった場合、開始側ではすべてタイムアウトとして検知されます。このため開始側では、通信障害なのか業務処理の遅延によるタイムアウトなのかを判断できません。

■ ユースケース

プラットフォーム通信標準仕様では、メッセージ交換パターンを要求側と応答側間の一般的なメッセージのやり取りとして定義しています。このため、地域情報 PF のすべての点で適用できます。しかし、応答側には、メッセージ交換パターンの組み合わせに関する制約事項も、一部存在します。

参照

- メッセージ交換パターンの奨励する基本的な構成、一般的構成、および奨励しない構成と制約事項については、『地域情報プラットフォームガイドライン』の「3.8.2 応答側処理におけるメッセージ交換パターンの制約」を参照