

和文タイトル：高付加価値サービスに関するサービス連携基盤技術

和文著者名、所属：

- ・ 日立製作所 小池博、高橋規生、里佳史、宮本大輔
- ・ デュオシステムズ 牛山克彦
- ・ 日本電気 菊地伸治、島村栄、神南吉宏、山本拓磨、斉藤 嗣治
- ・ 富士通 金井剛、加藤光幾、石井章夫
- ・ NTT コミュニケーションズ 島谷明、奥平禎、田原聡士

和文抄録：

高付加価値サービスは、多様なネットワーク、システム上にあるサービスが連携し、クロスサイト環境においても多種多様なサービスを安全かつ柔軟に統合したサービスの提供を行うことであると位置付けられる。例えば、地方公共団体が提供する行政サービスには、住民記録サービスや国民保険サービス、児童手当サービス等があり、それらサービスを連携させ、ワンストップサービスを提供することが可能となる。

本論文では、「デザインパターン適用開発技法」「観測情報統合提供技術」「認証・認可に関する技術」「サービス提供者または管理者におけるサービス管理基盤技術」について述べる。

英文タイトル：Service Interaction Platform Technologies Regarding High Value-added Services

英文著者名、所属：

- ・ Hitachi, Co., Ltd. Hiroshi Koike, Norio Takahashi, Yoshifumi Sato, and Daisuke Miyamoto
- ・ Duo Systems, Co., Ltd. Katsuhiko Ushiyama
- ・ NEC, Co., Ltd. Shinji Kikuchi, Sakae Shimamura, Yoshihiro Jinnann, Takuma Yamamoto, and Tsuguharu Saitou
- ・ Fujitsu, Co., Ltd. Takeshi Kanai, Mitsuki Katou, and Akio Ishii
- ・ NTT Communications Co., Ltd. Akira Shimatani, Tadashi Okudaira, and Satoshi Tahara

英文抄録：

Service interaction platform technologies are essential to realize high value-added services. Service interaction platform technologies are mainly applied in the public field and enable one-stop online services by securely and flexibly combining various kinds of services, which are operated under different policies or established under different system architectures. One-stop services transform citizens' daily lives more convenient by, for example, improving online application procedures to the local administrations and companies. The core components of service interaction platform technologies are development techniques applying design patterns, technologies offering integrated monitoring information, technologies regarding authentication and approval, and service management technologies for service providers and managers.

1. 概要

IT新改革戦略「－いつもでも、どこでも、誰でもITの恩恵を実感できる社会の実現－」では、行政サービスや医療、教育分野等でのIT利用・活用における国民満足度の向上、地域や世代間における情報活用における格差の是正等が課題として挙げられている。ユビキタス・ネットワーク社会に向けた高付加価値サービスの提供が求められている。

高付加価値サービスとは、地域における官民の様々なサービスが連携し、それが複数のサイトに跨る環境においても多種多様なサービスを安全かつ柔軟に統合したサービスの提供を行うことと位置付けられる。この基盤としてユビキタスプラットフォーム技術に関する研究開発（※1）が進められている。

本セッションでは、特に、官民が連携する地域サービスでは、ベンダ独自の技術や個別仕様で連携されているものが多く、更なるサービスの追加、個人情報保護法などの対象となるプライバシー情報の保護、サービス全体を

俯瞰して監視するといった地域サービスの高度化に必要な技術が欠けている。地域サービスが高度化されると、地方公共団体が提供する転入サービス、国民健康保険加入サービス等、民間が提供するガス・電気・水道等の新規申し込みサービス等といった自治体内外のサービスを利用者のニーズに応じて連携し提供することが可能となる。

このような課題の解決を行うための研究技術について紹介する。

※1 ユビキタスプラットフォーム技術に関する研究開発：総合科学技術会議における科学技術政策のなかで推進されている。

(<http://www8.cao.go.jp/cstp/budget/h17101804.pdf>)

2. 研究技術内容

2.1. デザインパターン適用開発技法

2.1.1 技術課題

地域における様々なサービス連携を実現するためのアーキテクチャとして現在提言されているものが、SOA(Service Oriented Architecture)である。SOAはWebServices技術をシステム連携技術に適用したものであるが、利用事例が少ないのが現実である。その原因として、システムの非機能要件を満たすための処理方式検討コストがかかることがあり、その開発技法が確立されていないことが挙げられる。本研究においては、上記課題を解決するためにSOAシステム開発技法へ、非機能要件の検討方法とデザインパターン技術を適用する検討を実施した。

2.1.2. SOAパターン定義言語

設計ノウハウの集まりであるデザインパターン技術のメリットをSOA設計へ取り込むためには、(1)事前決定事項(パターン)(2)設計事項(カスタマイズ)(3)必須記載事項を明確にする必要がある。また、課題解決のために、性能や品質、運用等のシステムの性質を記述した要件である非機能要件の記述形式の規定が必要となる。

本研究では、WSDL, WS-BPELといった標準仕様を拡張することにより、非機能要件の記述方法を追加し、パターン言語の記述方法として規定した。

デザインパターン技術をSOA設計に導入すると以下になる。(1)事前決定事項(パターン)：一連のサービス呼出しから構成される処理フロー定義のうち、呼出順序、分岐条件(AND, OR, XOR等)を固定化したもの。(2)設計事項(カスタマイズ)：上記処理フローを構成する個々のサービスが満たすべき非機能要件(適合条件)。(3)必須記載事項：上記処理フロー定義のシステムが提供する非機能要件。

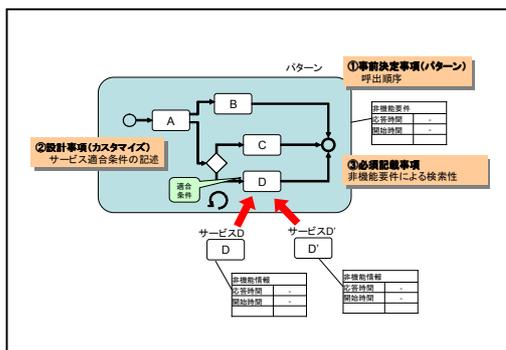


図2.1-1デザインパターン技術の導入

2.1.3. SOAパターンを用いた開発

SOAシステム設計は以下の手順で行う。

(1) 処理フロー設計

業務分析の結果として作成されたビジネスプロセス(業務フロー図)を入力とし、システムが動作可能なレベルの処理フロー図(BPMN図)を作成する工程。

(2) サービス選定

処理フロー図(BPMN図)の各アクティビティへ実際のサービスを割り当てる作業。サービスの検索、適合性の検討を行う工程。

(3) 全体検証

システム全体としての整合性、非機能要件を満たしているか否かの検討。

デザインパターンを利用することにより、上記作業内容で以下のメリットがある。

(1) 処理フロー設計

手で書き起こさなくても、必要なパターンを検索するだけで行える。

(2) サービス選定

ツールによって、パターンへ適合するサービスを検索し、適合性判断を自動で行える。

(3) 全体検証

パターンには非機能要件が設定されており、その確認のみ行えばよい。

以上のことから本研究結果を用いると、設計効率の向上が図られる。

2.1.4. UMLによるSOAパターンの記述

従来の設計手順においては、処理フロー図作成工程の入力となる業務フロー図は、UML(Unified Modeling Language)アクティビティ図で記述されており、これはBPMNやWS-BPELとの間に互換性がないことから、処理フロー図を手作業で一から作成することとなり、作業工数が多くなっている。また、BPMNやWS-BPELの記述のためにはモデリングツールを別途使用する必要があり、開発コストの増加、生産性の低下のおそれがある。

そこで、デザインパターンを利用した処理フロー図をUMLで記述し、さらにその結果をWS-BPELとして出力することにより、業務フロー図をそのまま入力として処理フロー図を作成することができ、また業務フロー図と処理フロー図を同一のモデリングツールによって記述できることから、工数の減少を図ることができる。

以上のことから本研究結果を用いると、設計効率の向上が図られる。

2.1.5. 評価、効果

上記定義言語パターンサンプルを記述し、開発実験を行った。設計工程で上記パターンサンプルを使用する場合/使用しない場合の作業工数を計測した。その結果、有意な工数差が発生することが判明した。

以上の検討から、SOAシステム開発技法へデザインパターン技術を適用し、さらに非機能要件記述方法を規定することにより、SOAシステム設計における課題を解決することが可能となった。

今後、実験結果を工数算出モデルへ適用して検証を行い、本研究成果の評価を行う予定である。

2.2. モニタリングと観測情報統合提供技術

2.2.1. 内容と対象

一般にモニタリングとは、観測目標・目的

を定義し、時刻等に対して、その状態変化等を捕捉するものと考えられ、運用管理の一領域として定義される。運用管理という言葉には広範囲の概念を含み、ITサービス、運用規則に関するベストプラクティスを包括的にまとめたITILを主に、セキュリティに関する運用規定事項などがその範囲に含まれる。このような背景の元、高付加価値サービスに関するサービス連携基盤に対して、運用モニタリング機能を、次の様に定義する。定義：

システム稼動情報から利用者が欲しい情報群を収集し、それらを必要とするシステム群に配信し、当該情報群を分析して表示する機能のこと。

また、その対象を以下とする。

- ・ プロセスレベル：狭義のビジネスプロセスであり、WS-BPEL言語により定義されるプロセス各層の実施状況。
- ・ サービスレベル：狭義のサービスであり、エンドポイントに位置付けられるサービスの実施状況、並びに二者間合意条件の遵守度状況。
- ・ システムリソース：システムを構成する要素機器構成、並びに稼動状況。

2.2.2. 課題

SOAにおいては、各種アプリケーション群が起動しているシステムプラットフォームのベンダ依存性を無くし、異機種でも連動動作を可能とした上で、当該アプリケーション群を要素サービス群と見立て、インターネットを介してこれらを連動、実施することが重要になる。しかし複数異種のシステムプラットフォーム、各種アプリケーションが複数のサービス群を大規模に連携する程、各々の運用課題や、障害要因等が混在しやすくなり、組み合わせにより想定もしていない新たな問題も顕在化し易い。

このため、安定的に稼動できるためには、これを下支えする複数の異機種システムプラットフォーム群、アプリケーション要素に関する構成情報の適切な捕捉と、継続的な監視、それらを利用する複数の要素サービス群自体の監視、そして、当該要素サービス群を連結して生成されるマルチサイトプロセスとして実施される実施ログの適正な捕捉、監視が必要であり、その結果を元に改善活動に繋げて行く必要がある。

しかし現時点では、複数の異種システムプラットフォームごとに、システムアーキテクチャ上の各層の運用情報をベンダ独自の方法で収集するため、この領域での規約は定義されているものの、統一性、相互運用性に欠けて、標準規約類の整備は、未だ途上にある。このため、マルチサイトプロセスを監視する運用モニタリング機能の実現技術も未確立、不完全である。

既存運用モニタリング製品でも相互参照性を保証していないため、見える化の上で阻害点になっている。

2.2.3. モニタリングのフレームワーク

運用モニタリング領域は極めて多岐に渡り複合的であるが故、各分野に共通的な統合フレームワークを確立しつつ、各分野固有の課題を解決するアプローチが必要となる。現在、解決すべき優先課題は、プロセス、サービス、システムリソースの各層にあり、その各々に対して、下記機能群を提供することで、顕在問題の解決を図ろうとしている。

- ・ 任意の複数サイトで実行される複数のサービス群が連結・統合して定義、実施されるマルチサイトプロセスモニタリング
- ・ 複数サービスから抽出される管理データを統合的に管理し、利用者要求に基づき、加工、提供するログアグリゲータ
- ・ サービス連携している全体システムにおいてシステム構成運用状況を把握するリソースモニタリング

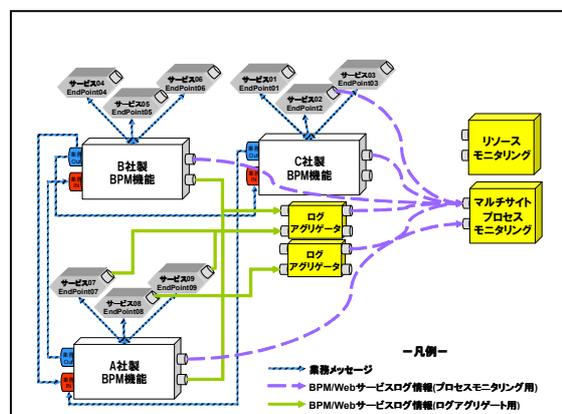


図 2.2-1 モニタリングフレームワーク構成

2.2.4. マルチサイトプロセスモニタリング

マルチサイトプロセスをモニタリングする機能は、共通的な統合フレームワークを継承しつつ、下記要素を含んで実現する。

- ・ 複数サイト間で分散して実施される要素サービス群が送受信するメッセージ群のログをログアグリゲータ、もしくはBPM機能他サイトに埋め込んだログ情報捕捉機能により捕提取集。
- ・ マルチサイトプロセスモニタリング機能内には、専用解析プロセスが存在し、当該解析プロセスは、前述捕捉されたメッセージ群のログに付与されたメッセージ識別子や、要素サービスの識別子等を手掛かりに、対応・因果関係を探り出し、複数サイトに跨ったマルチサイトプロセスを抽出。

2.2.5. ログアグリゲータ

これは、複数サイトにまたがるサービスのログデータを収集し、統合的に管理・加工・提供する機能である。多種多様なシステムプラットフォーム上で要素サービス群を連携させ、それを安定的・効率的に提供していくためには、各要素サービス群の稼動状況を示す

サービス管理データ、ログ、イベント情報の収集が不可欠である。そこで、この機能はサービス管理データとしての様々なログデータを束ねて、多面性・汎用性を伴う各種アプリケーション向けに、高可用性のある形式・粒度で各種加工データを提供する。そして、共通的な統合フレームワークを継承しつつ、下記要素を含んで実現する。

- ・ サービス管理データの多面的・汎用的なデータの利用、加工を実現する統合化機能で各機能層、多様な情報源からログ、イベント情報と言ったサービス管理データを、統一したデータフォーマットで蓄積・管理。
- ・ サービス管理データの多面的・汎用的なデータの利用、加工を実現する提供機能で対象となるアプリケーション群からの要件に適合し、指定された高可用性のある形式・粒度に、サービス管理データを加工して提供。オンデマンド、サブスクライブの2通りの供給形態がある。

2.2.6. 評価

従来、システム運用領域ではITILが標準として存在するが、これはモニタリング対象の定義と枠組みに留まっており、クロスサイトプロセスレベルによるサービスの運用状態のモニタリング迄、至っておらず、DMTFのCIM等でも、クロスサイトプロセスレベルの論点を明示的に記しているわけではない。そこで要素サービス、プロセス群を統合的に俯瞰し、クロスサイトプロセスレベルのモニタリングのビューを提供し得るメタモデルを定義することは必要とされる研究課題であったが、その案を定義出来た意義は大きい。

2.3. 認証・認可に関する技術

2.3.1 背景・目的

地域における様々なサービスにおいて、複数のサービスを連携させた高付加価値サービスを適切に動作させるため、サービスの提供者は、サービスの利用者の認証を行ったり、サービスの利用者に関するプライバシー情報を蓄積しサービスの提供にあたってプライバシー情報を参照する場合や、リアルタイムの稼働情報をもとに、挙動分析を行いながらサービスを安定稼働させる自律制御を行い、認証後のサービス利用権限の判断を行う必要がある。本節では、高付加価値サービスの実行・制御技術に関して認証・認可に関していくつかの要素技術についての取り組みを紹介する。

2.3.2 課題

サービス利用時のプライバシー情報公開の局面においての課題として、プライバシー情報の利用目的と、プライバシー情報の主体の利用許諾意志との間の調整が必要となる。これを解決するのが、「プライバシー情報公開調整技術」である。

他方、サービス提供のために個人を特定する認証を必要としない局面も考えられ、この

ような場合に、匿名での認証を実現する必要がある。「匿名認証技術」では、個人は特定できないが、ある一定の権限を持つことを保証する技術である。さらに、安易な認証を行うユーザのIDを使いまわすようなシングルサインオンシステムでは名寄せによってプライバシー情報が統合され、漏えい時の被害が拡大する危険性があるためこれを解決する「プライバシー保護型認証連携基盤技術」や多様な認証手段を容易に利用可能とするための、「認証フレームワーク技術」も必要である。また、利用者が多種多様なプラットフォーム上のアプリケーションを利用する際に、利用者のID情報と権限情報の管理が必要である。しかし、現状ではプラットフォームごと、アプリケーションごとに個別に管理されている状況であり、利用者や利用者を管理する管理者にとっても利用者の登録、削除の操作が発生するたびにそれに伴う権限情報のマッピングを手作業で行っている状況である。

2.3.3 手段・効果

(1) プライバシー情報公開調整技術

サービスの提供、およびサービスの連携の局面において、サービスの提供者におけるプライバシー情報の利用目的と、サービスの利用者のプライバシー情報の利用許諾意志との間の調整を行い、サービスの利用者の意図したプライバシー情報の公開のみを保証する。

(2) 匿名認証技術

サービスの利用者を特定する必要がない場合に対応するために、匿名性を有する認証を実現する。結果、プライバシー情報の漏えいを無くすことが可能であるとともに、特権をもつサービスの管理者のみはサービスの利用者を特定することが可能である。緊急時などには利用者を特定することができる。

(3) プライバシー保護型認証連携技術

認証情報の名寄せによるプライバシー情報の統合を防止するため、サービス毎のIDを連携させることでシングルサインオンを実現する。本技術の研究開発の際には、様々なサービス間の連携において認証情報を交換するための標準仕様をベースとして採用し、サービスの連携を実現する上で最適な仕様を認証連携プロトコルとして利用する。

(4) 認証フレームワーク技術

ID/パスワード、ハードディスクにセキュアに格納した公開鍵証明書といった安全な認証手段を統一的なインタフェースで提供することで、認証のなりすましによるプライバシー情報の不正利用防止を実現する。

(5) 権限管理基盤技術

複数のアプリケーションで使用される利用者のIDと権限情報を一元的に管理する手法、アプリケーションが個別に管理しているIDや権限情報も同期を取り整合性を維持する手法、アプリケーションごとのアクセス制御ルールを一元管理する手法の有効性を評価することで、権限管理基盤技術を確立する。

具体的には、図 2.3-1 に示すような権限管理基盤を導入することによって、マルチベンダ、マルチプラットフォーム環境における ID と権限管理の一元管理（ID と権限管理の紐付け）やアクセス制御ルールの一元管理が可能にある。また、マルチベンダ、マルチプラットフォーム環境における ID と権限管理に関する同期を取った整合性の維持も可能になる。

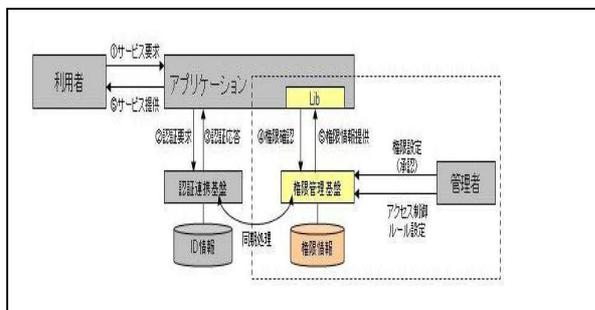


図 2.3-1 権限管理基盤

2.4. サービス提供者または管理者におけるサービス管理基盤技術

2.4.1. 背景・目的

ユビキタス・ネットワーク社会の環境下では、広範囲な分野から提供されているサービスを複数サイトに跨り、利用者の利便性向上を図れる高付加価値サービスとして提供することが求められる。

地域における様々なサービスにおいて、サービス間連携が促進され、様々な高付加価値サービスを提供することが求められる。

本来、利用者はそれぞれのニーズに沿った形でサービスを利用できることが望ましいが、現状取り組まれている標準化ではアプリケーション間の相互接続プロトコル等が中心であり、サービス利用者（連携する他のサービス含む）と提供者の関係と、この2者間で適用されるサービス運用条件等サービスに関する情報の管理については、十分な検討が行われていない。

2.4.2 課題

本研究においては、2つの課題を設定している。1つ目は、現状の運用形態が提供者中心のサービス運用になっている点である。これは利用者ニーズを反映する手段がなく、サービス提供者からサービス利用者への一方向の情報生成・伝達しかされず、サービス利用者はサービスの運用状況を把握することができない点である。

2つ目は、サービス利用者のサービス利用形態ごとにサービスのカスタマイズが必要になっており、サービス提供者（またはサービス管理者）の管理作業が複雑かつ非効率になっている。

本研究を通して、これらの課題に対する解決策としての統合レジストリを検討し、サービス情報管理制御技術を使った、統合レジストリ機能の検討を行った。

2.4.3 手法・効果

サービス利用者とサービス提供者間の合意の策定、管理、監視を可能とする、統合レジストリを検討した。統合レジストリは現状の標準である UDDI、ebXML レジストリを拡張した構成になっており、WSDL で表現されたサービス呼び出し情報に加えて、統合レジストリは補足説明やマニュアル等、WSDL だけでは表現されないサービスについての付加情報についても管理する。

統合レジストリは、UDDI、ebXML レジストリが保持するサービス呼び出し情報や、サービス利用者と提供者間の合意交渉、合意内容等のサービス情報の管理、策定された合意のサービスへの適用、策定した合意の実施状況の監視を行う。

サービス提供者とサービス利用者は、統合レジストリが提供するユーザインタフェースを通して合意の策定を行う。合意する項目は、セキュリティ（暗号化）、SLA(Service Level Agreement)、合意運用ログ取得条件であり、策定された合意はサービス利用者毎に管理されている。

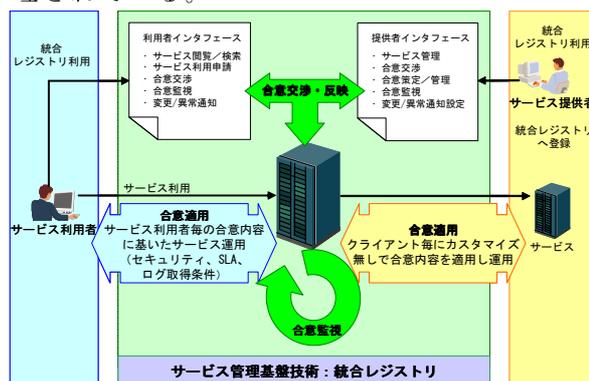


図 2.4-1 統合レジストリ

2.5. 高付加価値サービスを提供するためのサービス連携基盤とその有効性評価に関する考察

2.5.1. 背景

自治体や民間等のシステム構築において、複数のシステムからなる多種多様なサービスを、安全かつ柔軟に統合し、高付加価値サービスを実現するニーズが高まっている。本節では、SOA の考え方にに基づき、異なる運用ポリシーや異なるアーキテクチャのサービスが連携し高付加価値サービスを提供するための「サービス連携基盤」の要件と、それを実現するための ICT の標準化ポイントについて述べる。さらに、そのサービス連携基盤における有効性評価の方法について述べる。

2.5.2. 高付加価値サービスを提供するためのサービス連携の要件

現在の個々のシステムを組合せてワンストップサービス等の高付加価値サービスを実現する場合の課題を図 2.5-1 に示す。さらに、この課題を解決するための「サービス連携基

盤」に対する要件も図 2.5-1 に記載した。

2.5.3. サービス連携基盤の実現上の課題と解決のアプローチについて

サービス連携の要件に対する実現上の課題としては、(1)異なるアーキテクチャを連携する課題と、(2)異なる運用ポリシーのシステムを連携する課題がある。これらを解決するため、図 2.5-2 に示す標準化やユースケース分析のアプローチを行った。

2.5.4. 異なるアーキテクチャの課題への対応

サービス連携させるために、システムの機能をサービスとして規定し、インタフェースを標準化するアプローチを採用した。具体的には、サービス通信 (SOAP) のための WSDL インタフェース、及び、サービスが他のサービスに公開するアクセスインタフェースを標準化し、同じ標準仕様の他ベンダのサービスや、異なるハードや OS 上のサービスを差し替え可能とした。更に、全体を連携するアーキテクチャとして、サービス標準 IF、ワストップ用標準ビジネスプロセス等から構成されるサービス連携基盤からなる、統一アーキテクチャを採用。これをビジネスプロセスベースにサービスの連携を実現する SOA 型のアーキテクチャとした。これにより、ワストップサービスも実現可能となる (図 2.5-3)。

2.5.5. 異なる運用ポリシーの課題への対応

サービス連携でのその他の課題としては、異なる運用ポリシーを持つサイト間を連携する課題がある。例えば、自治体と民間では、認証に関するポリシーが異なったり、ビジネスプロセスの監視やハードリソースの監視に関する運用監視のポリシーが異なるという課題がある。

異なる運用ポリシーの課題に対しては、

(1) 実際のユースケースの分析、(2) ユースケース別の運用系 IT 要件の明確化と、標準化のアプローチで検討した。図 2.5-4 がユースケースと IT 要件を整理した情報である。認証のポリシーが同一である場合サービス連携の IT 要件は、現在、Web サービスセキュリティ技術と電子証明書技術を用いて実現可能である。異なる認証ポリシーのサイト間の連携、モニタリングと監視データの対象やその収集方法に関する技術については、2.3.2.4 で検討が行われている。

2.5.6. サービス連携基盤の有効性評価の検討

サービス連携して高付加価値サービスを提供するサービス連携基盤の有効性について、評価を行う手法を検討している。その検討結果の一部を図 2.5-5 に示す。評価の手順としては、(1) 対象システムの機能の明確化とその実現、(2) サービス評価項目の検討、(3) ステークホルダ毎の評価内容と評価尺度の決定、(4) 評価の測定方法 (アンケートや実測方法) の決定、(5) 評価対象

システムの構築と評価の実施、の順で行う。現在、本アプローチでの自治体や官民連携におけるサービス連携技術の評価を検討中である。

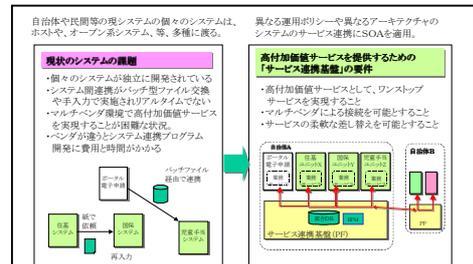


図2-5-1 高付加価値サービスを提供するための「サービス連携基盤」の要件

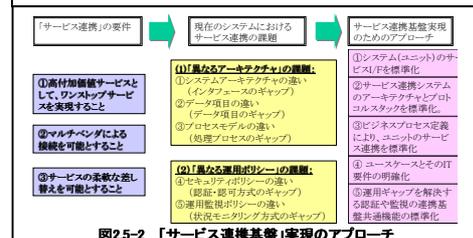


図2-5-2 「サービス連携基盤」実現のアプローチ

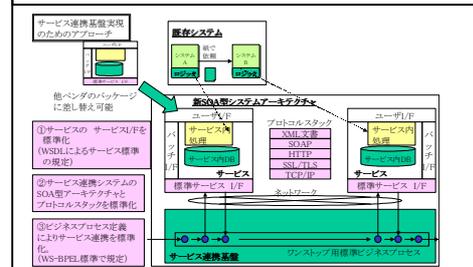


図2-5-3 「サービス連携基盤」の標準化ポイント

運用シナリオ	AP連携の例	連携、IDM、統合ID、セキュリティの要件	認証・認可、監視の要件
①自治体のAP連携	人が電子申請⇒住民(他自治体)⇒住民	・同期サービス連携基盤 ・非同課連携サービス連携 ・IDM+統合DB基盤 ・サービス連携の認証 ・電子署名の付与/検証	認証:自治体間認証 監視:自治体間監視、他自治体間監視、自治体内監視
②他ベンダからの自治体単独AP連携	人が他ベンダから申請、システムキー申請交付(自治体)⇒住民⇒住民	・同期サービス連携基盤 ・非同課連携サービス連携 ・IDM+統合DB基盤 ・サービス連携の認証 ・電子署名の付与/検証	認証:自治体、ベンダの認証、ユーザ認証 監視:自治体間監視(ベンダ)、自治体内監視
③他ベンダからによる民間と自治体のAP連携	人が他ベンダから申請、システムキー申請交付(自治体)⇒自治体⇒住民⇒住民	・同期サービス連携基盤 ・非同課連携サービス連携 ・IDM+統合DB基盤 ・サービス連携の認証 ・電子署名の付与/検証	認証:自治体、ベンダの認証、ユーザの認証 監視:自治体間監視(ベンダ)、自治体内監視

図2-5-4 異なる運用ポリシーのサイト間のユースケースとIT要件

評価対象システム決定	例: ①既存SOA型システム、②「1」に認証や運用機能を追加したシステム		
サービスの評価項目	連携技術評価に関連する評価項目を以下から抽出する。基本的には、JISX0129-1のソフトウェア品質特性をベースとして抽出する。 ・機能性: 目的性、正確性、相互運用性、セキュリティ ・信頼性: 信頼性、障害耐性、回復性 ・使用性: 理解性、習得性、適用性 ・効率性: 時間効率性、資源効率性 ・保守性: 解析性、変更性、安定性、試験性 ・移植性: 環境適応性、設置性、規格適合性、置換性		
利用者、提供者、運用者、関係者の視点で捉えた連携技術評価の評価尺度の決定			
評価者	カテゴリ	評価内容	評価尺度
住民	機能	ワストップサービスにおける住民側処理は適切か	5(高い)4(やや高い)3(標準)2(やや低い)1(低い)
職員	機能	ワストップサービスの職員側処理は適切か	5(高い)4(やや高い)3(標準)2(やや低い)1(低い)
運用者	機能	サービスの入替えは容易か	5(高い)4(やや高い)3(標準)2(やや低い)1(低い)
運用者	コスト/性能	ビジネスプロセス管理の作業負担	5(高い)4(やや高い)3(標準)2(やや低い)1(低い)

図2-5-5 「サービス連携基盤」の有効性評価方法

謝辞
本研究は、独立行政法人情報通信研究機構 (NiCT) の委託研究開発「異なる運用ポリシーや異なるアーキテクチャのサービスが連携し、高付加価値サービスを提供するためのサービス連携基盤技術の研究開発」の成果の一部である。ここに記して謝意を表する。

以上