「社会保障・税に関わる番号制度が情報システムへ与える影響に関する調査研究」

－インターフェイスシステムに求められる要件の検討に係る報告書－

平成２５年３月２９日

目　次

はじめに

社会保障･税に関わる番号制度が情報システムへ与える影響に関する調査研究(以下「本調査研究」という。)では、情報提供ネットワークシステムにおけるインターフェイスシステムと各情報保有機関の既存システムとの間で情報のやり取りを行うために必要な機能群（以下「中間サーバー」という。）及び各情報保有機関の既存システム等において必要となる措置について、各情報保有機関における既存システムの現状及び影響範囲を調査し、その結果を踏まえ、各情報保有機関が番号制度に係る準備作業を円滑に進めるために必要となる技術的事項に関する検討を行う。

本書は、インターフェイスシステムに求められる要件（機能要件、非機能要件）の検討結果についてとりまとめたものである。

番号法案及び関連法案は平成 25 年 3 月時点で未成立であり、今後の法制化、法案審議や後に公布される政省令等の内容、その他の制度検討内容によっては、記載内容に変更が生じる可能性がある。

1. 用語の定義

本章では、本書で用いる用語の定義について述べる。

表 1　用語の定義

用語	定義
番号制度	「社会保障・税に関わる番号制度」の略称。
インターフェイスシステム	「情報提供ネットワークシステム（インターフェイスシステム)」の略称。
コアシステム	「情報提供ネットワークシステム（コアシステム)」の略称。
マイ・ポータル	「マイ・ポータルシステム」の略称。
既存システム （既存業務システム）	個人情報を保有し、中間サーバーを介して外部機関へ情報提供する元となる各情報保有機関の既存業務システム（基幹システム、システム共通基盤等)。
中間サーバー	インターフェイスシステムと既存システムとの情報の授受の仲介をする役割を担うサーバー。
基本 4 情報	住民基本台帳の 4 情報（氏名、住所、性別、生年月日)。
符号	情報提供ネットワークシステムにおいて、個人を一意に識別するための情報。
宛名番号	当該情報保有機関の既存システムにおいて個人を一意に識別するための番号。
世帯番号	当該情報保有機関の住基システムで管理している番号。同じ世帯番号を付与された個人が同一世帯構成員であることを示す。
情報提供 DB	中間サーバーにおいて外部機関への提供情報を保持する DB。
番号法案	「行政手続における特定の個人を識別するための番号の利用等に関する法律案」の略称。
データ標準	番号法案別表第 2 に規定される情報照会者、事務、情報提供者、特定個人情報の項目を整理・標準化したもの。
情報保有機関	番号法案別表第 2 の第 1 欄に規定される情報照会者及び第 3 欄に規定される情報提供者。
事務	番号法案別表第 2 の第 2 欄に規定される 115 事務。
特定個人情報	個人番号（個人に対応し、当該個人番号に代わって用いられる番号、記号その他の符号であって、住民票コード以外のものを含む。）をその内容に含む個人情報。
特定個人情報名	番号法案別表第 2 の第 4 欄に規定される内容に列挙された個別

用語	定義
	の情報（例：番号法案別表第 2 の 18 の第 4 欄における「地方税関係情報」及び「住民票関係情報」）。
特定個人情報名コード	特定個人情報名に対して一意に付与されるコード。（例：01）
特定個人情報の項目	特定個人情報名ごとに、根拠法令等で規定され特定個人情報を構成すると想定される個々の項目の名称。ひとつの特定個人情報名当たり複数存在する可能性がある。（例：市町村民税所得割額）
特定個人情報の項目コード	特定個人情報の項目に対して一意に付与されるコード。 （例：001）
特定個人情報の項目値	特定個人情報の項目の内容。（例：〇〇円）
番号制度研究会	平成 24 年度において、番号制度の在り方についての検討のために設置された総務省主催の研究会。地方公共団体における番号制度の活用に関する研究会。
プレフィックス情報	番号法案別表第 2 で規定される、情報照会者、事務、情報提供者、特定個人情報の項目等を元にアクセス制御を実施するための定義。
情報提供記録	情報照会者と情報提供者との間で行った、特定個人情報の情報照会及び情報提供に係る記録。

2. 情報提供ネットワークシステム及びインターフェイスシステムの概要

本章では、情報提供ネットワークシステム及びインターフェイスシステムの概要について述べる。

2.1 情報提供ネットワークシステムの概要

情報提供ネットワークシステムは、行政運営の効率化及び国民の利便性向上のために、迅速かつ安全な情報の授受の仕組みを提供するシステムである。

(1) 情報提供ネットワークシステムを用いた情報照会の流れ

情報提供ネットワークシステムを用いた情報照会の流れについて、以下に示す。

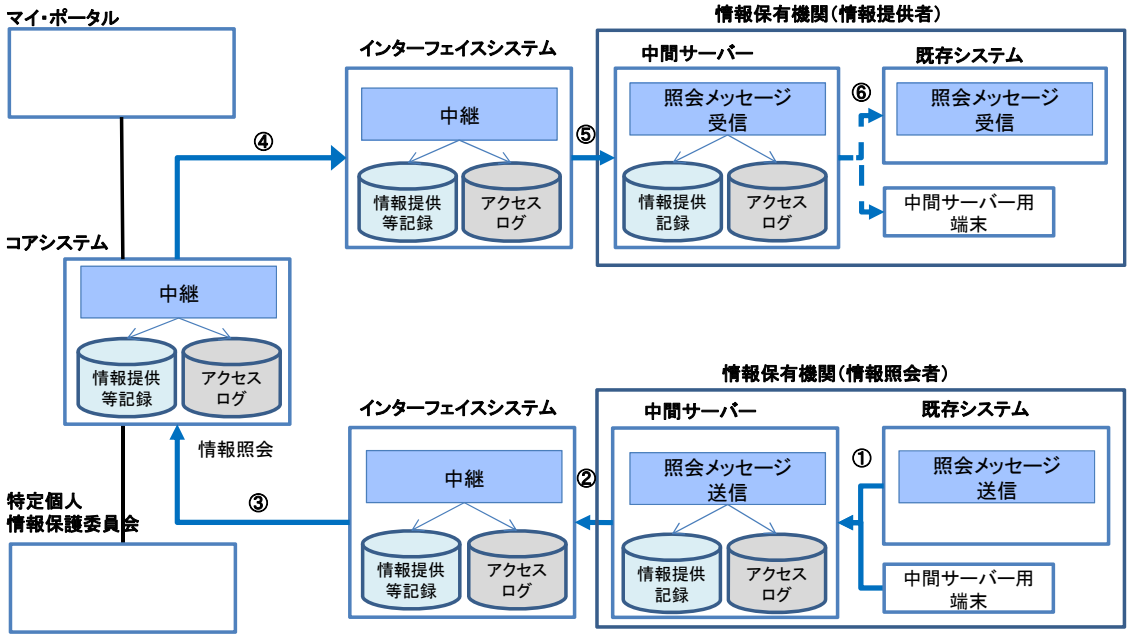


図 1 情報提供ネットワークシステムを用いた情報照会の流れ

・中間サーバーにて問い合わせた宛名番号を符号に変換し、情報照会を行う。

(2) 情報提供ネットワークシステムを用いた情報提供の流れ

情報提供ネットワークシステムを用いた情報提供の流れについて、以下に示す。

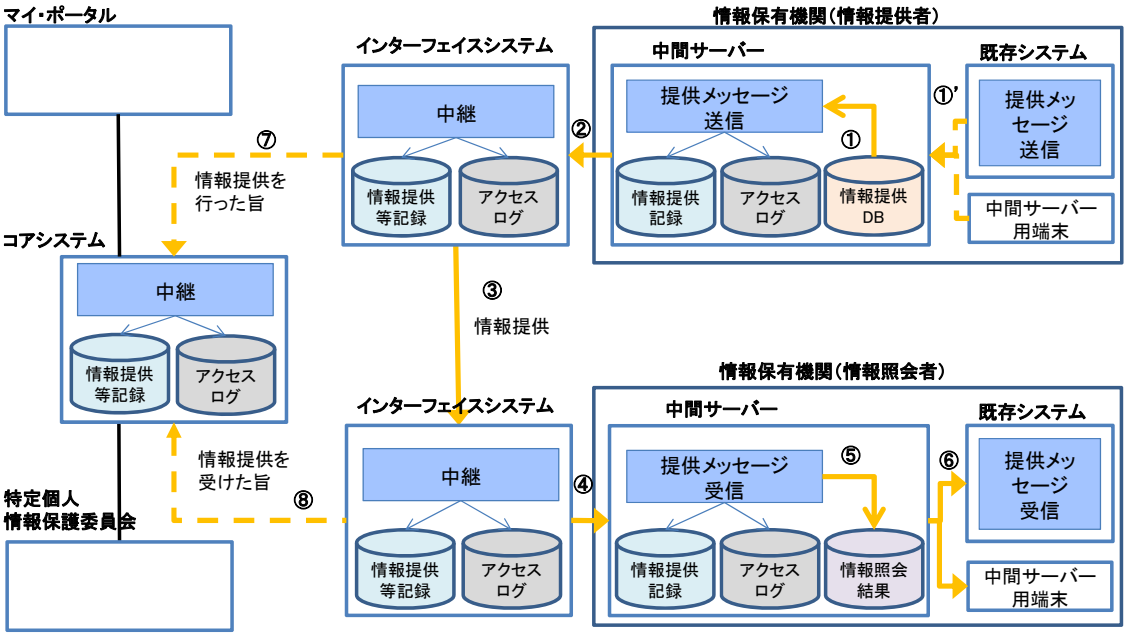


図 2 情報提供ネットワークシステムを用いた情報提供の流れ

・情報提供は、情報提供 DB を用いた自動応答を基本とする。
・情報提供者は、情報照会元の情報保有機関に、処理通番とともに返信する。
・情報提供電文のボディは中間サーバーにて暗号化する。

2.2 インターフェイスシステムの概要

インターフェイスシステムとは、情報提供ネットワークシステムにおけるコアシステムと中間サーバーとの間で、上述したような情報のやり取りを行うために必要な機能群を提供するシステムであり、以下の特徴を有する。

①インターフェイスシステムは、情報照会・情報提供において、コアシステムや中間サーバーを経由して、情報照会側と情報提供側との間を中継する。

②情報照会においては、情報照会者の宛名番号に対応した符号、及びインターフェイスシステムから取得した処理通番等を用いて照会を行う。この際、処理通番の発番を行う。また、プレフィックス情報を用いて、正しい情報照会であるかをチェックし、許可された情報照会のみ実行可能とする。

③インターフェイスシステムは、個人番号及び基本 4 情報を保有せず、いずれも情報提供ネットワークシステムに流通させない。

2.3 番号法案における情報提供ネットワークシステムの位置付け

本調査研究では、平成 25 年 3 月 1 日、第 183 回通常国会に提出された「行政手続における特定の個人を識別するための番号の利用等に関する法律案」（以下「番号法案」という。）に記載された事項を遂行するために必要な業務及びシステム機能を前提とした検討を行う。

番号制度導入の目的は法案第 1 条に記載されているが、地方公共団体等は、個人番号および法人番号を利用して効率的な情報管理、利用及び迅速な情報の授受を行うことができるようにするとともに、届出その他の手続きを行う国民が、手続きの負担軽減及び本人確認の簡易な手段を得られるようにすることとされている。

また、法案第 3 条において、国民又は法人が一度行政機関に提出した情報について、国民の負担軽減のため、同一の内容の情報を求めないとされている。

【法案】
（基本理念）
第三条　個人番号及び法人番号の利用は、この法律の定めるところにより、次に掲げる事項を旨として、行われなければならない。
一　行政事務の処理において、個人又は法人その他の団体に関する情報の管理を一層効率化するとともに、当該事務の対象となる者を特定する簡易な手続を設けることによって、行政運営の効率化を図り、もって国民の利便性の向上に資すること。
二　情報提供ネットワークシステムその他これに準ずる情報システムを利用して迅速かつ安全に情報の授受を行い、情報を共有することによって、社会保障制度、税制その他の行政分野における給付と負担の適切な関係の維持に資すること。
三　個人又は法人その他の団体から提出された情報については、これと同一の内容の情報の提出を求めることを避け、国民の負担の軽減を図ること。

さらに、法案第 19 条では、第 19 条各号に記載された場合を除き、特定個人情報については、他の機関に提供することが禁止されている。

一方、第 22 条より、第 19 条第 7 号の規定により、情報提供者は特定個人情報の提供を求められた場合、情報照会者に対し、当該特定個人情報を提供しなければならないとされている。

なお、第 19 条第 7 号の規定による特定個人情報の照会、提供は、情報提供ネットワークシステムを使用して行うこととなっており、これは第 21 条により総務大臣が設置、

管理することとなっている。また、第 19 条第 7 号の規定によりなされた情報提供の求め又は情報提供について、情報照会者及び情報提供者及び総務大臣は、第 23 条により、情報照会者、情報提供者の名称、提供の求め、提供の日時、特定個人情報の項目を記録、保管することとなっている。

【法案】

（特定個人情報の提供の制限）

第十九条 何人も、次の各号のいずれかに該当する場合を除き、特定個人情報の提供をしてはならない。（中略）

七 別表第二の第一欄に掲げる者（法令の規定により同表の第二欄に掲げる事務の全部又は一部を行うこととされている者がある場合にあっては、その者を含む。以下「情報照会者」という。）が、政令で定めるところにより、同表の第三欄に掲げる者（法令の規定により同表の第四欄に掲げる特定個人情報の利用又は提供に関する事務の全部又は一部を行うこととされている者がある場合にあっては、その者を含む。以下「情報提供者」という。）に対し、同表の第二欄に掲げる事務を処理するために必要な同表の第四欄に掲げる特定個人情報（情報提供者の保有する特定個人情報ファイルに記録されたものに限る。）の提供を求めた場合において、当該情報提供者が情報提供ネットワークシステムを使用して当該特定個人情報を提供するとき。（後略）

（情報提供ネットワークシステム）

第二十一条　総務大臣は、特定個人情報保護委員会と協議して、情報提供ネットワークシステムを設置し、及び管理するものとする。

２　総務大臣は、情報照会者から第十九条第七号の規定により特定個人情報の提供の求めがあったときは、次に掲げる場合を除き、政令で定めるところにより、情報提供ネットワークシステムを使用して、情報提供者に対して特定個人情報の提供の求めがあった旨を通知しなければならない。（後略）

（特定個人情報の提供）

第二十二条　情報提供者は、第十九条第七号の規定により特定個人情報の提供を求められた場合において、当該提供の求めについて前条第二項の規定による総務大臣からの通知を受けたときは、政令で定めるところにより、情報照会者に対し、当該特定個人情報を提供しなければならない。（後略）

（情報提供等の記録）

第二十三条　情報照会者及び情報提供者は、第十九条第七号の規定により特定個人情報の提供の求め又は提供があったときは、次に掲げる事項を情報提供ネットワークシステ

ムに接続されたその者の使用する電子計算機に記録し、当該記録を政令で定める期間保存しなければならない。

一　情報照会者及び情報提供者の名称

二　提供の求めの日時及び提供があったときはその日時

三　特定個人情報の項目（中略）

３　総務大臣は、第十九条第七号の規定により特定個人情報の提供の求め又は提供があったときは、前二項に規定する事項を情報提供ネットワークシステムに記録し、当該記録を第一項に規定する期間保存しなければならない。

3. インターフェイスシステム検討の概要

本章では、インターフェイスシステム検討の概要や位置付けについて述べる。

3.1 インターフェイスシステム検討の範囲

本書は、インターフェイスシステムに求められる機能要件、非機能要件等についてとりまとめたものである。

本書で検討される範囲は、下図における「A.インターフェイスシステムに求められる要件の検討」の部分である。

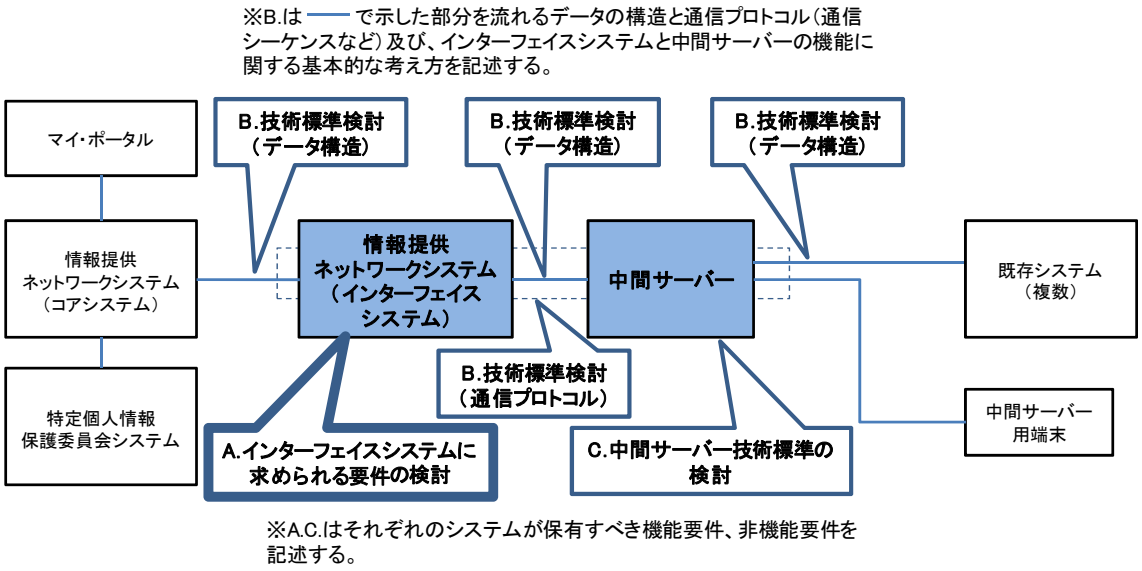


図 3 インターフェイスシステム検討の範囲

中間サーバーのシステムが保有すべき機能要件、非機能要件については、「中間サーバー技術標準の検討に係る報告書」において取りまとめる。また、情報照会／情報提供等に係る送受信におけるデータ構造や通信プロトコルについては、「技術標準の検討に係る報告書」において取りまとめる。

3.2 インターフェイスシステム検討の概要

本書では、以下について記載する。

(1) 全体機能構成・機能配置

インターフェイスシステム及び中間サーバーに係る全体の機能構成と、インターフェイスシステム、中間サーバーそれぞれへの機能配置について整理したもの。

(2) インターフェイスシステムの導入に係る前提条件

インターフェイスシステムを導入するに当たり、調達範囲、調達単位、設置単位等について検討・整理したもの。

(3) 機能要件

全体機能構成・機能配置において記載したインターフェイスシステムの各機能について細分化し、機能詳細を検討・整理したもの。

(4) データ要件

インターフェイスシステムにおいて管理する情報(データ)について整理したもの。

(5) 稼働環境

インターフェイスシステム及び中間サーバーについて、ハードウェアの分離、ネットワーク上の配置、クラウド環境等の稼働環境について検討・整理したもの。

(6) 非機能要件

インターフェイスシステムの規模、可用性、運用・保守等の非機能要件について検討・整理したもの。

4. 全体機能構成･機能配置

本章では、インターフェイスシステム及び中間サーバーの全体機能構成及び機能配置について述べる。

4.1 機能概要

インターフェイスシステム及び中間サーバーが提供する機能概要を以下に示す。

表 2　機能概要

#	機能名	概要
1.	符号管理機能	情報提供に用いる個人の識別子である符号と情報保有機関内で固有の宛名番号を紐付け、その情報を保管・管理するための機能。
2.	情報照会側機能	他情報保有機関が保有する特定個人情報を照会するために、情報提供ネットワークシステムを介して、情報照会及び情報提供の受領を実施するための機能。
3.	情報提供側機能	他情報保有機関からの情報照会を受け、情報提供ネットワークシステムを介して、情報照会の受領及び当該特定個人情報の提供を実施するための機能。
4.	既存システム接続機能	コアシステム、インターフェイスシステム、中間サーバー及び既存システムとの間で情報照会、情報提供の内容について連携するための機能。
5.	情報提供記録管理機能	特定個人情報の提供の求め又は提供があった旨の情報提供記録を生成し、管理するための機能。
6.	情報提供 DB 管理機能	情報提供 DB を更新・管理するための機能。
7.	情報提供関連機能	処理通番の発行、プレフィックス情報のチェックや管理、運用状態の管理等を行うための機能。
8.	データ送受信機能	情報照会、情報提供、情報提供記録等のデータを送受信するための機能。
9.		プレフィックス情報やこれに基づく電文定義、アクセス権定義を随時更新するための機能。
10.	セキュリティ管理機能	ユーザ管理、暗号化／復号、鍵管理等のセキュリティ管理を実現するための機能。
11.	職員認証・権限管理機能	（特に、専用端末からのログインを許容する場合）職員認証システムと連携し、職員認証を実現するための機能。
12.	システム管理機能	時刻同期、稼働監視、運用管理、バックアップ等のシス

#	機能名	概要
		テム管理全般を実現するための機能。

※上記の他、マイ・ポータルが想定する機能の内、一部に対応するための機能が必要となる可能性がある。

インターフェイスシステム及び中間サーバーの機能構成・機能配置を次節以降に定める。

4.2 インターフェイスシステムの機能構成（概要）

インターフェイスシステムの機能構成概要について、以下に示す。

表 3　インターフェイスシステムの機能構成

#	機能名	概　要
1.	既存システム接続機能	コアシステム、他のインターフェイスシステム及び中間サーバーとの間で必要な処理を行い、連携、接続するための機能。
2.	情報提供記録管理機能	特定個人情報の提供の求め又は提供があった旨の情報提供記録を生成し、管理するための機能。 ※中間サーバーと同等の機能であるが、要件や記録の相違について検討する。
3.	情報提供関連機能	処理通番の発行、プレフィックス情報のチェックや管理、運用状態の管理等を行うための機能。
4.	データ送受信機能	情報照会、情報提供、情報提供記録、プレフィックス情報等のデータを送受信するための機能。
5.	セキュリティ管理機能	ユーザ管理等のセキュリティ管理を実現するための機能。
6.	システム管理機能	時刻同期、稼働監視、運用管理、バックアップ等のシステム管理全般を実現するための機能。

4.3 中間サーバーの機能構成（概要）

中間サーバーの機能構成概要について、以下に示す。

表 4　中間サーバーの機能構成

#	機能名	概　要
1.	符号管理機能	情報提供に用いる個人の識別子である符号と情報保有機関内で固有の宛名番号を紐付け、その情報を保管・管理するための機能。
2.	情報照会側機能	他情報保有機関が保有する特定個人情報を取得するために、情報提供ネットワークシステムを介して、情報照会及び情報提供の受領を実施するための機能。
3.	情報提供側機能	他情報保有機関からの情報照会を受け、情報提供ネットワークシステムを介して、情報照会の受領及び当該特定個人情報を提供するための機能。
4.	既存システム接続機能	既存システムとの間で情報照会、情報提供の内容について連携するための機能。
5.	情報提供記録管理機能	特定個人情報の提供の求め又は提供があった旨の情報提供記録を生成し、管理するための機能。
6.	情報提供 DB 管理機能	情報提供 DB を更新・管理するための機能。
7.	データ送受信機能	情報照会、情報提供、情報提供記録、プレフィックス情報等に関するデータを送受信するための機能。
8.	セキュリティ管理機能	暗号化／復号、鍵管理等のセキュリティ管理を実現するための機能。
9.	職員認証・権限管理機能	（特に、専用端末からのログインを許容する場合）職員認証システムと連携し、職員認証を実現する機能。
10.	システム管理機能	時刻同期、稼働監視、運用管理、バックアップ等のシステム管理全般を実現するための機能。

インターフェイスシステム及び中間サーバーの機能構成・機能配置に従い、インターフェイスシステム及び中間サーバーで保持する主な情報とその関係を下図に示す。

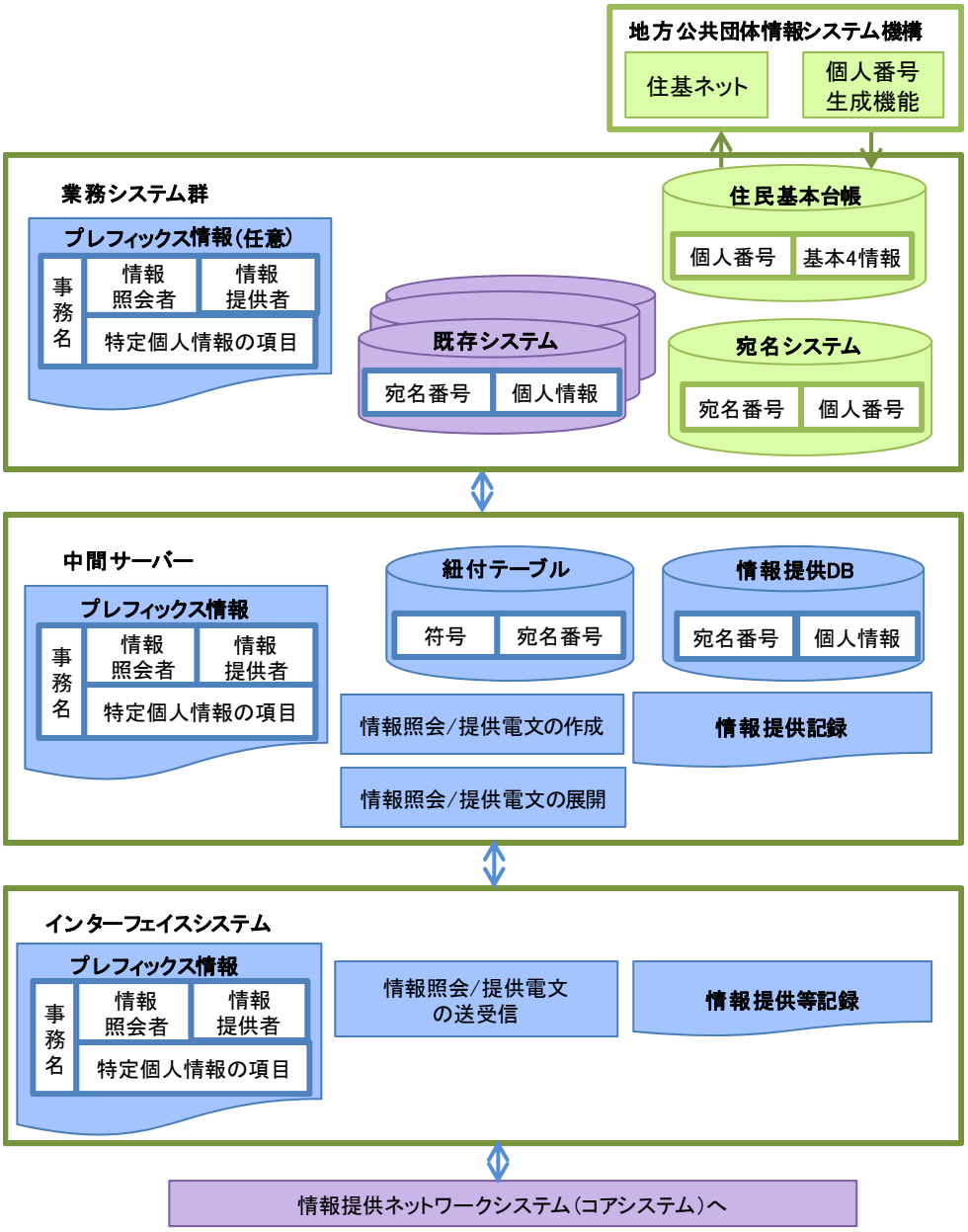


図 4　インターフェイスシステム及び中間サーバーで保持する主な情報とその関係

5. インターフェイスシステムの導入に係る前提条件

本章では、インターフェイスシステムの導入に係る前提条件について述べる。

・インターフェイスシステムは情報保有機関に設置する。
・提供情報は中間サーバー上で暗号化する。
・提供情報は情報提供ネットワークシステムを通じて他情報保有機関に送信する方式とする。

5.1 調達範囲

番号制度導入に係る情報保有機関に設置するシステムの調達範囲について、以下に示す。

表 5　システムの調達範囲

システム	調達者	運用者
インターフェイスシステム	ハードウェア：情報保有機関 ソフトウェア：国	国
中間サーバー	ハードウェア：情報保有機関 ソフトウェア：国	情報保有機関
既存システム改修	情報保有機関	情報保有機関

※インターフェイスシステム、中間サーバーの共同利用について、別途考慮する必要があり、また、それにより調達者などが変更されることも想定される。

5.2 技術標準

以下については、「技術標準の検討に係る報告書」に記載した内容を前提とする。

① 送受信データ標準
・データ標準
・データ構造
② 通信プロトコル標準
・メッセージ交換全体仕様
・メッセージ交換技術標準
・制御用通信プロトコル標準
・情報照会／情報提供用通信プロトコル標準
・プレフィックス情報等配布用通信プロトコル標準

5.3 インターフェイスシステムの設置単位

インターフェイスシステムは各地方公共団体に一つ設置（但し、クラウド環境ではこの限りではない）することとする。

また、インターフェイスシステムのLAN上の配置、クラウド環境への導入については、「稼働環境」の項を参照のこと。

6. 機能要件

本章では、インターフェイスシステムの機能要件について述べる。

6.1 機能一覧

現時点で想定されるインターフェイスシステムの機能一覧について、以下に示す。

なお、機能の詳細及びその実現方法等については、今後予定されるインターフェイスシステム構築に係る調達仕様書作成時又は設計書作成時に検討する。

(1) 既存システム接続機能

既存システム接続機能について、以下に示す。

表 6　既存システム接続機能

#	機能中分類	機能小分類	対応画面
1.	電文変換・生成	情報提供ネットワークシステム電文形式→中間サーバー電文形式変換	－
2.		中間サーバー電文形式→情報提供ネットワークシステム電文形式変換	－

(2) 情報提供記録管理機能

情報提供記録管理機能について、以下に示す。

表 7　情報提供記録管理機能

#	機能中分類	機能小分類	対応画面
1.	情報提供記録生成	情報照会記録生成	－
2.		情報提供記録生成	－
3.	情報提供記録検索	－	－
4.	情報提供記録媒体出力	－	－
5.	情報提供記録削除	－	－
6.	アクセスログ生成	－	－
7.	アクセスログ削除	－	－

(3) 情報提供関連機能

情報提供関連機能について、以下に示す。

表 8　情報提供関連機能

#	機能中分類	機能小分類	対応画面
1.	処理通番発番・通知	処理通番発番	－
2.		処理通番通知	－
3.	プレフィックス情報チェック	プレフィックス情報チェック	－
4.		プレフィックス情報チェック結果通知	－
5.		プレフィックス情報による制御	－
6.	情報照会許可依頼・通知	情報照会許可依頼に係る電文中継	－
7.		情報照会許可通知に係る電文中継	－
8.	情報照会電文中継	情報照会に係る電文中継	－
9.		情報照会の受付に係る電文中継	－
10.		情報照会受付完了に係る電文中継	－
11.		情報照会完了通知に係る電文中継	－
12.		形式チェック	－
13.	情報提供電文中継	情報提供に係る電文中継	－
14.		情報提供の受領に係る電文中継	－
15.		情報提供受領通知に係る電文中継	－
16.		情報提供完了通知に係る電文中継	－
17.		形式チェック	－
18.	プレフィックス情報配布・更新	プレフィックス情報受信	－
19.		プレフィックス情報更新・保持	－
20.		プレフィックス情報送信	－

(4)　データ送受信機能

データ送受信機能について、以下に示す。

表 9　データ送受信機能

#	機能中分類	機能小分類	対応画面
1.	通信制御	処理状況管理	－
2.		通信リトライ	－
3.		稼働状況通知	－
4.		再送処理	－
5.	対コアシステム送受信	対コアシステム送信	－

#	機能中分類	機能小分類	対応画面
6.		対コアシステム受信	－
7.	対中間サーバー送受信	対中間サーバー送信	－
8.		対中間サーバー受信	－
9.	対インターフェイスシステム送受信	対インターフェイスシステム送信	－
10.		対インターフェイスシステム受信	－

(5) セキュリティ管理機能

セキュリティ管理機能について、以下に示す。

表 10　セキュリティ管理機能

#	機能中分類	機能小分類	対応画面
1.	ユーザ管理	ユーザ登録、変更、削除	－
2.		アクセス権限設定	－
3.	ログイン認証	認証	－
4.		パスワード変更	－

(6) システム管理機能

システム管理機能について、以下に示す。

表 11　システム管理機能

#	機能中分類	機能小分類	対応画面
1.	時刻同期	－	－
2.	バックアップ管理	－	－
3.	運用監視	－	－
4.	資源管理	－	－

6.2 既存システム接続機能

(1) 前提条件

既存システム接続機能の前提条件について、以下に示す。

・ 情報提供ネットワークシステムで取り扱う電文形式と、中間サーバーで取り扱う電文形式とを変換する必要がある場合に、電文変換・生成機能により電文形式を相互に変換する。

(2) 機能要件

既存システム接続機能の機能要件について、以下に示す。

表 12　既存システム接続機能の機能要件

#	機能中分類	機能小分類	概要
1.	電文変換・生成	情報提供ネットワークシステム電文形式→中間サーバー電文形式変換	コアシステムから受けた情報照会電文、情報提供電文等の形式を、中間サーバーに中継する情報照会電文、情報提供電文等の形式に変換する。
2.		中間サーバー電文形式→情報提供ネットワークシステム電文形式変換	中間サーバーから受けた情報照会電文、情報提供電文等の形式を、コアシステムに中継する情報照会電文、情報提供電文等の形式に変換する。

※上記のそれぞれの電文形式は基本的に共通であることを想定している。したがって、その限りにおいて本機能は不要である。

6.3 情報提供記録管理機能

(1) 前提条件

情報提供記録管理機能の前提条件について、以下に示す。

・ インターフェイスシステムにおいても、コアシステムと同様に、番号法案第 23 条に定められた要件を満たす情報提供記録を生成し、管理する。

(2) 機能要件

情報提供記録管理機能の機能要件について、以下に示す。

表 13　情報提供記録管理機能の機能要件

#	機能中分類	機能小分類	概要
1.	情報提供記録生成	情報照会記録生成	情報提供記録を生成し、保存する。
2.		情報提供記録生成	
3.	情報提供記録検索	－	蓄積された情報提供記録を検索する。
4.	情報提供記録媒体出力	－	蓄積された情報提供記録を媒体等に出力する。
5.	情報提供記録削除	－	蓄積された情報提供記録を削除する。
6.	アクセスログ生成	－	アクセスログを生成し、保存する。
7.	アクセスログ削除	－	蓄積されたアクセスログを削除する。

機能の詳細について、以下に示す。

① 情報提供記録生成

以下の場合において､番号法案第 23 条に定められた要件を満たす情報提供記録を自動的に生成し、蓄積できること。

なお、情報照会、情報提供に係る一連のプロセスに係る記録は、後述するアクセスログ生成機能においても生成、保存される。

情報提供記録の内容には、少なくとも以下を含むこと。

・ 情報照会要求の処理日時
　情報照会要求を行った日時

・ 情報提供の処理日時
　情報提供を行った日時
・ 処理通番
　情報照会、情報提供を行う一連の処理に対して一意に付与された番号
・ プレフィックス情報
　番号法案別表第 2 に基づき情報照会、情報提供を行う情報照会者、事務、情報提供者、特定個人情報の項目の組み合わせ
・ 符号
　情報照会、情報提供の対象となる個人に対して、情報照会者側において付与された符号又は情報提供者側において付与された符号
・ 特定個人情報保護委員会向けの情報
　特定個人情報保護委員会が情報提供記録を確認するために必要なその他の情報

② 情報提供記録検索

蓄積された情報提供記録を、検索できること。

また、情報提供記録検索は、インターフェイスシステム上の簡易なユーザインターフェイスから指定できるものとする。

本機能は、専ら運用・保守の目的で使用する。

③ 情報提供記録媒体出力

蓄積された情報提供記録を、外部記録媒体等に出力できること。また、情報提供記録検索機能を利用して、特定の情報提供記録について外部記録媒体等に出力できること。

外部記録媒体は、外部記録装置をインターフェイスシステムへ接続してセットすることを想定している。

また、情報提供記録媒体出力は、インターフェイスシステム上の簡易なユーザインターフェイスから指定できるものとする。

本機能は、専ら運用・保守の目的で使用する。

④ 情報提供記録削除

蓄積された情報提供記録を、最低限保存すべき期間等、別途定められる運用方針に従って削除できること。

情報提供記録削除は、インターフェイスシステム上の簡易なユーザインターフェイスから指定できるものとする。また、誤って情報提供記録削除をすることのないよう、削除する前に利用者に確認を求める等の仕組みを備えること。

本機能は、専ら運用・保守の目的で使用する。

⑤ アクセスログ生成

情報照会／情報提供に係る電文だけでなく、インターフェイスシステムにおいて処理する電文の送受信すべてについての記録を自動的に生成し、蓄積できること。

本機能は、専ら運用・保守の目的で使用する。

⑥ アクセスログ削除

蓄積されたアクセスログを、別途定められる運用方針に従って削除できること。

本機能は、専ら運用・保守の目的で使用する。

6.4 情報提供関連機能

(1) 前提条件

情報提供関連機能の前提条件について、以下に示す。

- 処理通番はインターフェイスシステムにおいて発番する。
- インターフェイスシステムで予めプレフィックス情報のチェックを行う。
- 情報照会の許可はコアシステムが行う。インターフェイスシステムはそれを中継する。
- コアシステムからプレフィックス情報やマスタ情報が配布される。

(2) 機能要件

情報提供関連機能の機能要件について、以下に示す。

表 14　情報提供関連機能の機能要件

#	機能中分類	機能小分類	概要
1.	処理通番発番・通知	処理通番発番	情報照会又は符号付番の一連の処理のための通番を発番する。
2.		処理通番通知	
3.	プレフィックス情報チェック	プレフィックス情報チェック	情報照会の正当性についてチェックする。
4.		プレフィックス情報チェック結果通知	
5.		プレフィックス情報による制御	
6.	情報照会許可依頼・通知	情報照会許可依頼に係る電文中継	情報照会許可についての依頼と、許可通知を行う。
7.		情報照会許可通知に係る電文中継	
8.	情報照会電文中継	情報照会に係る電文中継	情報照会について中間サーバーとコアシステムとの間を中継する。
9.		情報照会の受付に係る電文中継	
10.		情報照会受付完了に係る電文中継	
11.		情報照会完了通知に係る電文中継	
12.		形式チェック	
13.	情報提供電文中継	情報提供に係る電文中継	情報提供について中間サーバーと相手方インターフェイスシステムとの間を中継する。
14.		情報提供の受領に係る電	

#	機能中分類	機能小分類	概要
		文中継	
15.		情報提供受領通知に係る電文中継	
16.		情報提供完了通知に係る電文中継	
17.		形式チェック	
18.	プレフィックス情報配布・更新	プレフィックス情報受信	プレフィックス情報の配布、更新を行う。 マスタ情報の配布を含む。
19.		プレフィックス情報更新・保持	
20.		プレフィックス情報送信	

機能の詳細について、以下に示す。

① 処理通番発番･通知

インターフェイスシステムとして、情報照会時に中間サーバーからの処理通番発番依頼を受けて、一意な処理通番を発番できること。

また､符号付番時に中間サーバーから処理通番発番依頼を受けた場合も同様とする。

(a) 処理通番発番

中間サーバーから処理通番発番依頼を受け、一意な処理通番を発番すること。このとき、これまで発行した処理通番について管理し、新たな処理通番を付与することにより処理通番の重複がないようにすること。

(b) 処理通番通知

発番した処理通番を中間サーバーに通知すること。

② プレフィックス情報チェック

情報照会側のインターフェイスシステムとして、中間サーバーからプレフィックス情報チェック依頼を受けた場合、これから情報照会を行おうとする情報照会者、事務名、情報提供者、特定個人情報の項目の組み合わせの正当性についてチェックできること。また、チェックした結果を中間サーバーに通知できること。

プレフィックス情報チェックにあたっては、番号法案別表第2に基づく最新のプレフィックス情報のリストをインターフェイスシステムに保持し､これと照合すること。照合結果は、OK 又は NG のいずれかを中間サーバーに通知すること。OK の場合には、プレフィックス情報と処理通番との組み合わせについてインターフェイスシステムに

保持すること。

⑷ プレフィックス情報チェック

中間サーバーからプレフィックス情報チェック依頼を受け、これから情報照会を行おうとする情報照会者、事務名、情報提供者、特定個人情報の項目の組み合わせの正当性についてチェックすること。

正当な最新のプレフィックス情報は、インターフェイスシステム上に予め保持しておく。以下の観点からプレフィックス情報のチェックを行うこと。

・ 情報照会者が当該中間サーバーの情報保有機関になっているか。
・ 中間サーバーからのプレフィックス情報照合依頼に含まれる情報照会者、事務名、情報提供者、特定個人情報の項目の組み合わせが、予め保持していた最新のプレフィックス情報の組み合わせの中に含まれているか。

チェックの結果問題がなければOKとし、問題があればNGとする。

⑸ プレフィックス情報による制御

プレフィックス情報のチェック結果がOKだった場合､プレフィックス情報と処理通番との組み合わせをインターフェイスシステム上に保持すること。対象の情報提供処理の完了後、組み合わせ管理情報を消去すること。

③ 情報照会許可依頼･通知

情報照会側のインターフェイスシステムとして、中間サーバーからの情報照会許可依頼を受け、コアシステムに情報照会許可依頼を中継できること。

また、コアシステムから情報照会許可依頼の結果として情報提供許可証を受領し、これを中間サーバーに通知できること。情報照会許可依頼の結果が不許可だった場合には、その旨をコアシステムから受領し、中間サーバーに通知できること。

情報提供許可証には、次の情報を含むこと。

・ コアシステムが許可証を発行する情報
・ 情報照会者、事務名、情報提供者、特定個人情報の項目
・ 情報提供者から情報照会者に情報提供するにあたっての、情報照会者への通信経路に係る情報
・ 処理通番

なお、改ざんがないことを証明する情報も必要となる可能性がある。

⑷ 情報照会許可依頼に係る電文中継

中間サーバーからの情報照会許可依頼を受け、コアシステムに情報照会許可依頼を中継すること。

ただし、情報照会許可依頼が、インターフェイスシステムにおいて保持するプレフィックス情報と処理通番の組み合わせと合致していない場合、情報照会許可依頼を中継せず、NG の旨を中間サーバーに返すこと。

(b) 情報照会許可通知に係る電文中継

コアシステムから情報照会許可依頼の結果として情報提供許可証を受領し、これを中間サーバーに通知すること。情報照会許可依頼の結果が不許可だった場合には、その旨をコアシステムから受領し、中間サーバーに通知すること。

④ 情報照会電文中継

情報照会側のインターフェイスシステムとして、中間サーバーからの情報照会電文を受け、コアシステムに中継できること。また、コアシステムからの情報照会受付完了電文を受け、中間サーバーに中継できること。

情報提供側のインターフェイスシステムとして、コアシステムからの情報照会電文を受け、中間サーバーに中継できること。また、中間サーバーからの情報照会受付完了電文を受け、コアシステムに中継できること。

情報照会電文の中継にあたっては、処理通番とプレフィックス情報が正しいこと、暗号化のための公開鍵が含まれていること、情報提供許可証が添えられていることに関する形式チェックを行うこと。

(a) 情報照会に係る電文中継(情報照会者側)

中間サーバーからの情報照会電文を受け、コアシステムに中継すること。

(b) 情報照会の受付に係る電文中継(情報提供者側)

コアシステムからの情報照会電文を受け、中間サーバーに中継すること。

(c) 情報照会受付完了に係る電文中継(情報提供者側)

中間サーバーからの情報照会受付完了電文を受け、コアシステムに中継すること。

(d) 情報照会受付完了に係る電文中継(情報照会者側)

コアシステムからの情報照会受付完了電文を受け、中間サーバーに中継すること。

(e) 情報照会完了通知に係る電文中継(情報照会者側)

中間サーバーからの情報照会完了通知電文を受け、コアシステムに中継すること。

(f) 形式チェック

電文の形式チェックを行うこと。形式チェックの結果 OK であればそのまま中継を行うが、NG の場合、中継せずに NG の旨とその理由を電文の送信元に通知すること。

形式チェックの内容として以下を含むこと。

・電文の書式が正しいこと。
・処理通番とプレフィックス情報が正しいこと。
・暗号化のための公開鍵が含まれていること。
・情報提供許可証が添えられていること。

⑤ 情報提供電文中継

情報提供側のインターフェイスシステムとして、中間サーバーからの情報提供電文を受け、情報照会側のインターフェイスシステムに中継できること。また、情報照会側のインターフェイスシステムからの情報提供受領電文を受け、中間サーバーに中継できること。更に、中間サーバーからの情報提供完了電文を受け、コアシステムに中継できること。

情報照会側のインターフェイスシステムとして、情報提供側のインターフェイスシステムからの情報提供電文を受け、中間サーバーに中継できること。また、中間サーバーからの情報提供受領通知電文を受け、情報提供側のインターフェイスシステムに中継できること。更に、中間サーバーからの情報提供完了電文を受け、コアシステムに中継できること。

(a) 情報提供に係る電文中継(情報提供者側)

中間サーバーからの情報提供電文を受け、情報照会側のインターフェイスシステムに中継すること。

(b) 情報提供の受領に係る電文中継(情報照会者側)

情報提供側のインターフェイスシステムからの情報提供電文を受け、中間サーバーに中継すること。

(c) 情報提供受領通知に係る電文中継(情報照会者側)

中間サーバーからの情報提供受領通知電文を受け、情報提供側のインターフェイスシステムに中継すること。

(d) 情報提供受領通知に係る電文中継(情報提供者側)

情報照会側のインターフェイスシステムからの情報提供受領通知電文を受け、中間サーバーに中継すること。

(e) 情報提供完了通知に係る電文中継(情報提供者側)

中間サーバーからの情報提供完了通知電文を受け、コアシステムに中継すること。

(f) 形式チェック

処理通番とプレフィックス情報が正しいこと等に関するヘッダ部分の形式チェックを行うこと。形式チェックの結果 OK であればそのまま中継を行うが、NG の場合、中継せずに NG の旨とその理由を電文の送信元に通知すること。

形式チェックの内容として以下を含むこと。

・電文の書式が正しいこと。

・処理通番とプレフィックス情報が正しいこと。

⑥ プレフィックス情報配布･更新

最新のプレフィックス情報のリストをコアシステムより受領し、更新・保持できること。

また、それを中間サーバーに配布できること。

(a) プレフィックス情報受信

最新のプレフィックス情報のリストをコアシステムより受信すること。

(b) プレフィックス情報更新･保持

これまでインターフェイスシステム上に保持していたプレフィックス情報を、コアシステムより受信した最新のプレフィックス情報で置き換えて保持すること。

(c) プレフィックス情報送信

コアシステムより受信した最新のプレフィックス情報を、中間サーバーに送信すること。

6.5 データ送受信機能

(1) 前提条件

データ送受信機能の前提条件について、以下に示す。

・ コアシステムは、稼働状況についてインターフェイスシステムから情報を取得する。

(2) 機能要件

データ送受信機能の機能要件について、以下に示す。

表 15　データ送受信機能の機能要件

#	機能中分類	機能小分類	概要
1.	通信制御	処理状況管理	データ送受信に当たり諸機能を呼び出すなど一連の通信制御を行う。
2.		通信リトライ	
3.		稼働状況通知	
4.		再送処理	
5.	対コアシステム送受信	対コアシステム送信	電文をコアシステムに送信又は受信する。
6.		対コアシステム受信	
7.	対中間サーバー送受信	対中間サーバー送信	電文を中間サーバーに送信又は受信する。
8.		対中間サーバー受信	
9.	対インターフェイスシステム送受信	対インターフェイスシステム送信	電文を相手方のインターフェイスシステムに送信又は受信する。
10.		対インターフェイスシステム受信	

機能の詳細について、以下に示す。

① 通信制御

データ送受信に当たり諸機能を呼び出すなど一連の通信制御を行えること。

(a) 処理状況管理

通信相手方であるコアシステム、インターフェイスシステム、中間サーバーとの間の処理状況について管理し、一連の処理と整合しない電文を受信した場合については、通信相手方に理由を付してエラーを返すこと。

ここでいう一連の処理とは、情報照会／提供に係る処理通番発番／プレフィックス情報チェックの依頼から情報照会／提供完了に至るまでの処理等を指す。

・ 一連の処理と整合しない処理通番の電文を受信した場合

・ 一連の処理と整合しないプレフィックス情報の電文を受信した場合等

⑹ 通信リトライ

以下に例示するような通信において、通信相手方から一定時間内に応答が返ってこない場合、予め規定された回数だけ通信をリトライできること。

・ 通信相手方のコアシステム、インターフェイスシステム、中間サーバーと通信を確立できない場合
・ 情報提供許可証発行依頼時に、一定時間内に情報照会許可通知（情報提供許可証）が返ってこない場合
・ 情報照会電文の中継時に、一定時間内に情報照会受付完了電文又は即時応答による情報提供電文が返ってこない場合
・ 情報提供電文の中継時に、一定時間内に情報提供完了電文が返ってこない場合

上記のリトライによっても応答が得られない場合や、通信相手方からシステム停止中の旨を受信した場合等においては、適切な手続きにより一連の処理をクローズできること。

⑹ 稼働状況通知

インターフェイスシステムの稼働状況について、コアシステム及び当該情報保有機関の中間サーバーに通知できること（既存の運用管理ソフトウェア等の利用可）。稼働状況には以下の状態を含む。

・ 起動
・ 停止

⑹ 再送処理

稼働して通信可能となったコアシステム及び当該情報保有機関の中間サーバーに対する再送処理ができること。

② 対コアシステム送受信

情報提供ネットワークシステムにおけるコアシステムの宛先や通信経路に関する情報を参照し、コアシステムに対して電文を送信できること。

また、インターフェイスシステムの稼働中は、情報提供ネットワークシステムにおけるコアシステムからの通信を常時受け付けられる状態とし、コアシステムから電文を受信できること。

⑷ 対コアシステム送信

情報提供ネットワークシステムにおけるコアシステムの宛先や通信経路に関する情報を参照し、コアシステムに対して電文を送信できること。

⑸ 対コアシステム受信

インターフェイスシステムの稼働中は、情報提供ネットワークシステムにおけるコアシステムからの通信を常時受け付けられる状態とし、コアシステムから電文を受信できること。

③ 対中間サーバー送受信

インターフェイスシステムの情報保有機関における中間サーバーの宛先や通信経路に関する情報を参照し、中間サーバーに対して電文を送信できること。

また、インターフェイスシステムの稼働中は、中間サーバーからの通信を常時受け付けられる状態とし、中間サーバーから電文を受信できること。

⑷ 対中間サーバー送信

インターフェイスシステムの情報保有機関における中間サーバーの宛先や通信経路に関する情報を参照し、中間サーバーに対して電文を送信できること。

⑸ 対中間サーバー受信

インターフェイスシステムの稼働中は、中間サーバーからの通信を常時受け付けられる状態とし、中間サーバーから電文を受信できること。

④ 対インターフェイスシステム送受信

情報提供時に、情報照会側のインターフェイスシステムへの経路情報を情報提供許可証の情報から取得することにより、情報照会側のインターフェイスシステムに対して情報提供に係る電文を送信できること。

また、インターフェイスシステムの稼働中は、情報提供ネットワークシステムにおける他のインターフェイスシステムからの通信を常時受け付けられる状態とし、情報照会時に、情報提供側のインターフェイスシステムから情報提供に係る電文を受信できること。

⑷ 対インターフェイスシステム送信

情報提供時に、情報照会側のインターフェイスシステムへの経路情報を情報提供許可証の情報から取得することにより、情報照会側のインターフェイスシステムに対して情報提供に係る電文を送信できること。

(b) 対インターフェイスシステム受信

インターフェイスシステムの稼働中は、情報提供ネットワークシステムにおける他のインターフェイスシステムからの通信を常時受け付けられる状態とし、情報照会時に、情報提供側のインターフェイスシステムから情報提供に係る電文を受信できること。

6.6 セキュリティ管理機能

(1) 前提条件

セキュリティ管理機能の前提条件について、以下に示す。

・ 電文の暗号化は中間サーバーで行い、インターフェイスシステムでは行わない。

(2) 機能要件

セキュリティ管理機能の機能要件について、以下に示す。

表 16　セキュリティ管理機能の機能要件

#	機能中分類	機能小分類	概要
1.	ユーザ管理	ユーザ登録、変更、削除	主にシステムの運用保守に係るユーザ及びアクセス権限の登録、変更、削除を管理する。
2.		アクセス権限設定	
3.	ログイン認証	認証	ユーザのログイン認証を行う。
4.		パスワード変更	

機能の詳細について、以下に示す。

① ユーザ管理

主にシステムの運用保守に係るユーザの登録、変更、削除ができること。また、ユーザに対して必要なアクセス権限の登録、変更、削除ができること。

インターフェイスシステムでは、いわゆる一般ユーザは想定しない。

(a) ユーザ登録、変更、削除

簡易なユーザインターフェイスを通じて、主にシステムの運用保守に係るユーザの登録、変更、削除が行えること。

(b) アクセス権限設定

簡易なユーザインターフェイスを通じて、ユーザに対して必要なアクセス権限の登録、変更、削除が行えること。

② ログイン認証

ユーザについては、ID、パスワードによる認証に加えて生体認証等を組み合わせるなどして、セキュアなログイン認証が行えること。

⑷ 認証

ID、パスワードによる認証に加えて生体認証等を組み合わせるなどして、セキュアなログイン認証が行えること。

⑸ パスワード変更

ユーザに対しパスワード変更を促し、パスワード変更が行えること。

6.7 システム管理機能

(1) 前提条件

システム管理機能の前提条件について、以下に示す。

・ 情報提供ネットワークシステム上に参照可能な NTP サーバーが設置されている。

(2) 機能要件

システム管理機能の機能要件について、以下に示す。

表 17　システム管理機能の機能要件

#	機能中分類	機能小分類	概要
1.	時刻同期	－	NTP サーバーを参照し時刻同期を行う。
2.	バックアップ管理	－	定期的なバックアップを管理する。
3.	運用監視	－	サーバー、ネットワーク、プロセス等の死活監視、リソース監視、セキュリティ監視を行う。
4.	資源管理	－	資源管理（配布）を行う。

機能の詳細について、以下に示す。

① 時刻同期

情報提供ネットワークシステム上に設置された NTP サーバーを参照し、時刻同期が行えること。

② バックアップ管理

システムバックアップ及びデータバックアップについてスケジューリングし、定期的あるいは随時で外部記憶媒体等に必要なバックアップができること。

③ 運用監視

インターフェイスシステムにおけるサーバー、ネットワーク、プロセス等の死活監視、リソース監視、セキュリティ監視を行えること。

④ 資源管理

データやソフトウェア等の配布を含む資源管理が行えること。

7. 画面要件

インターフェイスシステムでは、いわゆる一般ユーザは想定しないため、一般ユーザが直接操作する画面は存在しないと考えられる。なお、システム管理に必要となる稼働状況監視、リソース監視等に係る画面は検討から除いている。

今後の画面の要否は、今後予定されるインターフェイスシステム構築に係る調達仕様書作成時又は設計書作成時に検討する。

8. データ要件

本章では、インターフェイスシステムが管理する主要な情報について述べる。

なお、中間サーバーとやりとりするデータの標準については、「技術標準の検討に係る報告書」を参照のこと。

8.1 インターフェイスシステムで管理する情報（一覧）

インターフェイスシステムで管理する情報（一覧）について、以下に示す。

（1） インターフェイスシステムで管理する情報（一覧）

インターフェイスシステムで管理する情報について、以下に示す。

表 18　インターフェイスシステムで管理する情報（一覧）

#	情報名	備 考
1.	行政機関マスタ	情報照会／情報提供の対象となる行政機関の一覧。 （A 県、B 県、…、C 市、…、国家公務員共済組合等）。
2.	情報提供事務マスタ	番号法案別表第 2 で規定される事務（場合によっては、主務省令で規定される事務の細目を含む）の一覧。
3.	特定個人情報名マスタ	番号法案別表第 2 で規定される特定個人情報名の一覧。
4.	特定個人情報の項目マスタ	番号法案別表第 2 で規定される特定個人情報の項目の一覧。
5.	プレフィックス情報	情報照会者、事務（場合によっては、主務省令で規定される事務の細目を含む）、情報提供者、特定個人情報の項目（場合によっては、情報項目（複数）を含む）の組より規定される連携（情報照会／情報提供）の定義。
6.	情報提供記録	情報提供を実施した記録。
7.	アクセスログ	インターフェイスシステム上の操作記録。

8.2 インターフェイスシステムで管理する情報（詳細）

インターフェイスシステムで管理する情報（詳細）について、以下に示す。なお、データベースの設計については、今後予定されるインターフェイスシステム構築に係る調達仕様書作成時又は設計書作成時に検討する。

凡例：

PK(Primary Key)：当該データを一意に識別するための主キーとなる主キー項目。

FK(Foreign Key)：他のデータの項目を参照する外部キー項目。

(1) 行政機関マスタ

行政機関マスタの詳細について、以下に示す。

表 19　行政機関マスタ

#	項目名	Key	備 考
1.	行政機関コード	PK	
2.	行政機関名		個別の行政機関名を指す。

(2) 情報提供事務マスタ

情報提供事務マスタの詳細について、以下に示す。

表 20　情報提供事務マスタ

#	項目名	Key	備 考
1.	事務コード	PK	番号法案別表第 2 の事務コード。
2.	事務名		番号法案別表第 2 の「事務（場合によっては、主務省令で規定される事務の細目を含む)」欄に示される事務名を指す。

(3) 特定個人情報名マスタ

特定個人情報名マスタの詳細について、以下に示す。

表 21　特定個人情報の項目マスタ

#	項目名	Key	備 考
1.	特定個人情報名コード	PK	
2.	特定個人情報名		番号法案別表第 2 の「特定個人情報」の欄に示される特定個人情報名を指す。

(4) 特定個人情報の項目マスタ

特定個人情報の項目マスタの詳細について、以下に示す。

表 22　特定個人情報の項目マスタ

#	項目名	Key	備 考
1.	特定個人情報名コード	PK	
2.	特定個人情報の項目コード	PK	
3.	特定個人情報の項目名		番号法案別表第 2 の「特定個人情報（場合によっては、情報項目（複数）を含む)」の欄に示される特定個人情報の項目名を指す。
4.	事務コード	FK	番号法案別表第 2 の事務コード。

(5) プレフィックス情報

プレフィックス情報の詳細について、以下に示す。

表 23　プレフィックス情報

#	項目名	Key	備 考
1.	送信元機関コード	PK	情報照会者の情報保有機関コード。
2.	送信先機関コード	PK	情報提供者の情報保有機関コード。
3.	事務コード	PK	事務手続き名のコード。
4.	特定個人情報名コード	PK	特定個人情報名のコード。
5.	特定個人情報の項目コード	PK	特定個人情報の項目コード。

(6) 情報提供記録

情報提供記録の詳細について、以下に示す。

表 24　情報提供記録

#	項目名	Key	備 考
1.	照会要求日時	PK	情報照会を要求した日時。
2.	情報提供日時	PK	情報提供を行った日時。
3.	処理通番		情報照会／情報提供を行う一連の処理に対して一意に付与された番号。
4.	プレフィックス情報		情報照会者、事務、情報提供者、特定個人情報の項目の組（場合によっては、情報項目（複数）を含む）よ

#	項目名	Key	備 考
			り規定される連携（情報照会／情報提供）の定義。
5.	符号		情報照会／情報提供の対象となる個人に対して、情報照会者側において付与された符号又は情報提供者側において付与された符号。
6.	特定個人情報保護委員会向けの情報		特定個人情報保護委員会が情報提供記録を確認するために必要なその他の情報。

(7) アクセスログ

アクセスログの詳細について、以下に示す。

表 25　アクセスログ

#	項目名	Key	備 考
1.	連番	PK	
2.	操作日時		
3.	操作端末		
4.	操作機関		
5.	操作職員		
6.	操作種別		
7.	事務コード		※複数
8.	特定個人情報名コード		※複数
9.	特定個人情報の項目コード		※複数

9. 稼働環境

本章では、インターフェイスシステムの稼働環境について述べる。

9.1 インターフェイスシステムと中間サーバーのハードウェアの分離

インターフェイスシステムと中間サーバーのハードウェアは、以下の理由により、異なるハードウェア上に稼働させ、責任分界点を明確化させるのが望ましい。

(1) 「個人情報の扱い」に係る責任分界点について

「情報提供ネットワークシステムは、特定個人情報の”中身”には関知できない」というのが前提である。[1]

コアシステムとインターフェイスシステムは情報提供ネットワークシステムの一部であり、一方、中間サーバーは情報保有機関側のシステムの一部である。特定個人情報は中間サーバーで暗号化する場合、情報提供ネットワークシステム側（コアシステムとインターフェイスシステム）は特定個人情報の内容を把握できない。

一方、インターフェイスシステムと中間サーバーを同一筐体とすると、論理的には別システムであるものの、「見た目」は「インターフェイスシステムと中間サーバーが一体化」してしまい、国が管理することへの国民の懸念の払拭という観点から課題がある。

(2) 「情報セキュリティ」に係る責任分界点について

情報提供ネットワークシステムにおいて、コアシステムとインターフェイスシステム間のネットワークは国で所管し、中間サーバーと既存システム間のネットワークは情報保有機関側で所管することが想定される。「両者の間を FW（ファイアウォール）を介してつなぐ」とするとネットワークセキュリティ上の責任分界点が明確化される。

一方、「インターフェイスシステムと中間サーバーを同一筐体とする」と、各ネットワークの情報セキュリティ面の所管が曖昧になってしまう。

[1] 内閣官房が全国 47 都道府県で開催する番号制度に関するシンポジウムにおける政府説明資料の「16. 番号制度における安心・安全の確保」に「国家管理の懸念を払拭する必要性等から、システム上の安全措置として個人情報を分散管理する」旨が示されていることに鑑み、国が所管する情報提供ネットワークシステムは個人情報（特定個人情報から“個人番号ないし符号”を除いたもの）には関知できないものと考えられる。

9.2 LAN 上の配置

インターフェイスシステムの LAN 上の配置は、設置する情報保有機関にてその状況を鑑みて検討することとする。参考として、インターフェイスシステムと中間サーバーの LAN 上の配置パターンについて、以下に示す。

ネットワークセキュリティ上、インターフェイスシステムと中間サーバーの責任分界点の明確化のために両者の間に FW を設置することを推奨する。

上記の構成に加え、インターフェイスシステムは外部（他の情報保有機関など）からアクセスされるため、既存システムと同じセグメントに配置することで、既存システムのセキュリティが確保できなくなる恐れがある。従って、既存システムと異なるセグメントに、インターフェイスシステムを設置する構成がより望ましいと考えられる。

インターフェイスシステムを既存システムと異なるセグメントに設置し、中間サーバーを既存システムと同じセグメントに置く構成パターンについて、以下に示す。

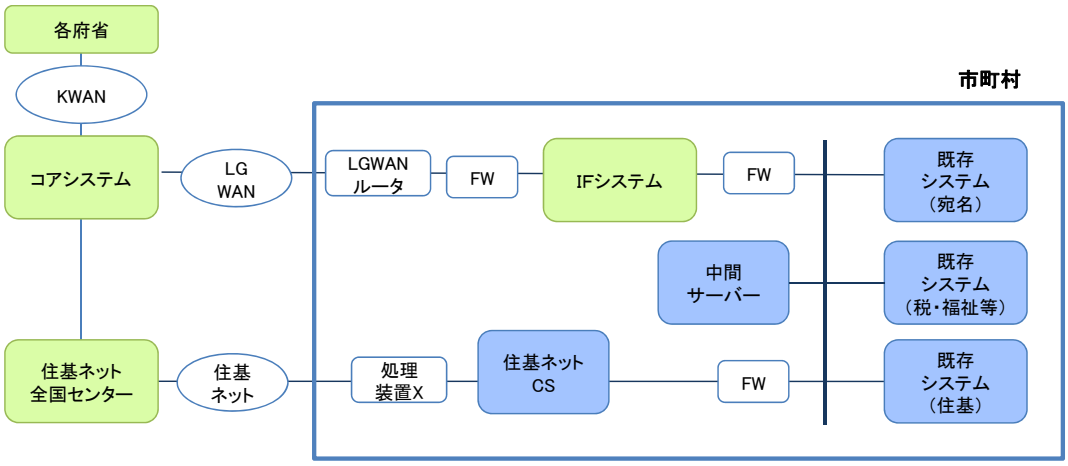


図 5　中間サーバーを既存システムと同じセグメントに置く構成

インターフェイスシステムを既存システムと異なるセグメントに設置し、中間サーバーも既存システムと異なるセグメントに置く構成パターンについて、以下に示す。

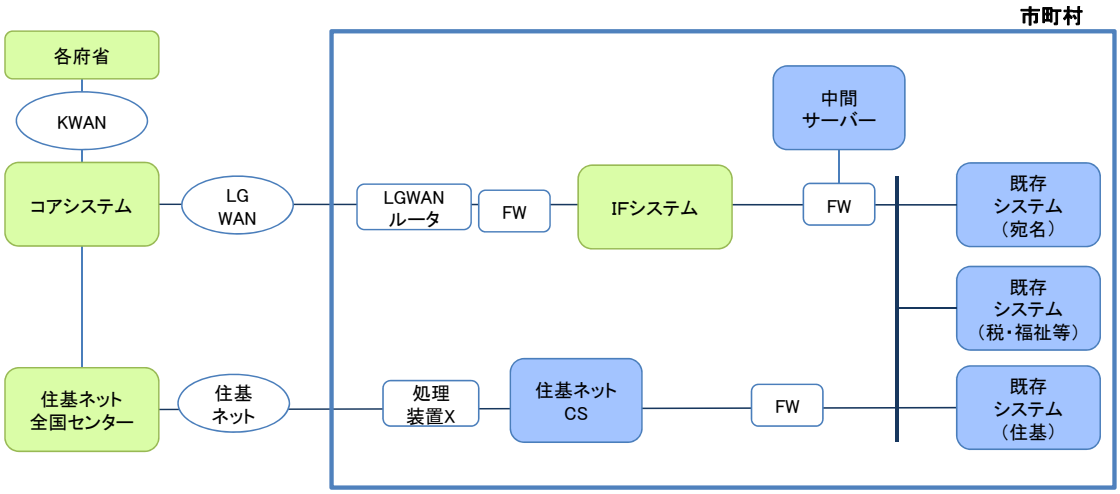


図 6　中間サーバーを既存システムと異なるセグメントに置く構成

インターフェイスシステムの LAN 上の配置は、設置する情報保有機関における基幹系 LAN 及び情報系 LAN の構成や、既存システムの接続形態にも影響するため、その状況を鑑みて検討することとする。

9.3 クラウド環境への導入

インターフェイスシステムのクラウドへの導入は、設置する情報保有機関にてその状況を鑑みて検討することとする。クラウド環境を用いる場合、提供されるサービスの形態は、一般的に以下の 3 つを想定する。

表 26　サービス形態の特徴

サービス形態	備 考
SaaS （Software as a Service）	アプリケーション（ソフトウェア）をサービスとして提供する。
PaaS （Platform as a Service）	アプリケーションを稼働させるための基盤（プラットフォーム）をサービスとして提供する。
IaaS （Infrastructure as a Service）	サーバー、CPU、ストレージなどのインフラをサービスとして提供する。

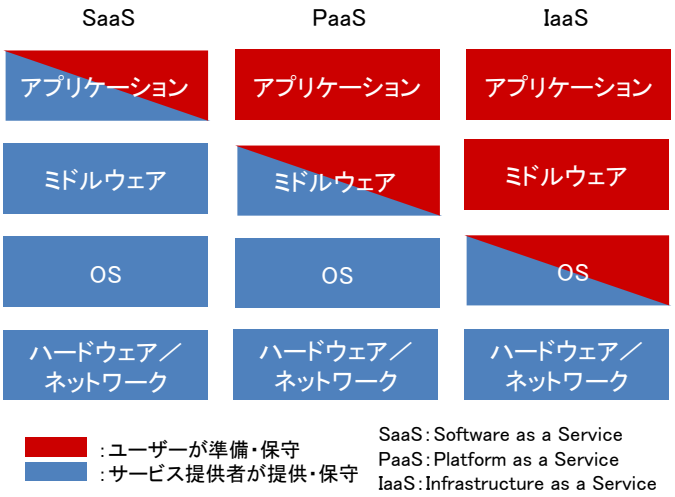


図 7　サービス形態の範囲

（出典：総務省「スマート・クラウド研究会報告書」）

インターフェイスシステムについては、各情報保有機関の既存システム等に影響される要素が少なく、中間サーバーと比べた場合、比較的 SaaS 又は PaaS が適していると考えられる。

クラウド環境を用いたインターフェイスシステムと中間サーバーの構成例について、以下に示す。

(1) インターフェイスシステムと中間サーバーが異なるクラウド環境にある場合

インターフェイスシステムと中間サーバーが異なるクラウド環境にある場合について、以下に示す。

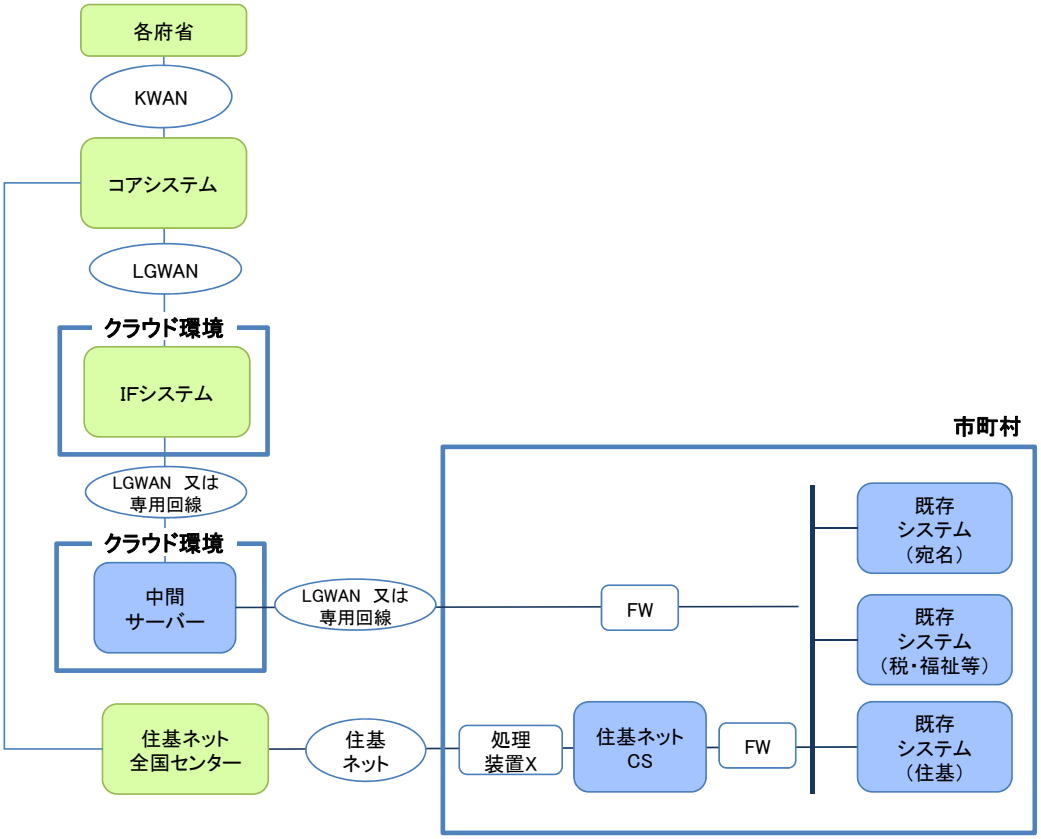


図 8　インターフェイスシステムと中間サーバーが異なるクラウド環境にある場合

(2) インターフェイスシステムのみがクラウド環境にある場合

インターフェイスシステムのみがクラウド環境にある場合について、以下に示す。

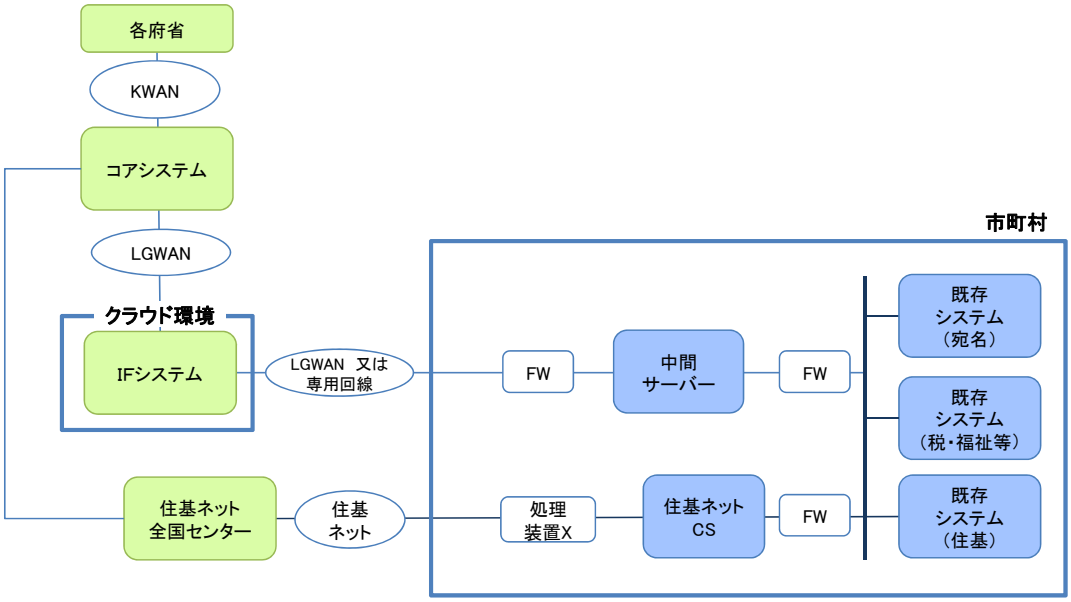
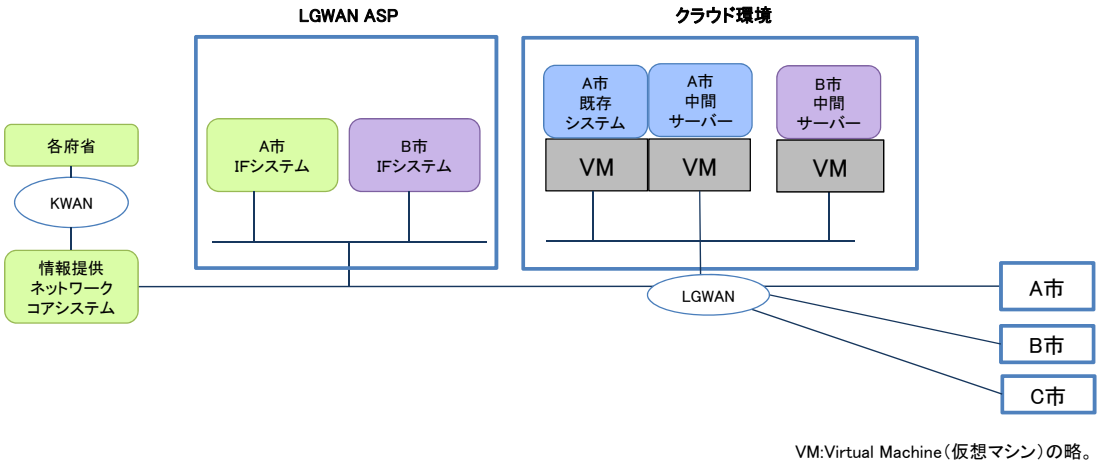


図 9　インターフェイスシステムのみがクラウド環境にある場合

(3)　複数の情報保有機関による共同利用を行う構成

クラウド環境で、複数の情報保有機関による共同利用を行う構成について、以下に示す。



VM:Virtual Machine（仮想マシン）の略。

図 10　クラウド環境で、複数の情報保有機関による共同利用を行う構成

クラウド環境において共同利用を行う場合、以下の点について、情報保有機関間で調整のうえ、合意を得る必要がある。

・情報保有機関ごとの既存システム改修や連携試験の実施内容、時期等（クラウド環境の調達時期に合わせ、各情報保有機関である程度統一する必要がある）。

・情報保有機関ごとの個別要件を許容する範囲（例：ハードウェアスペックなど）

と、情報保有機関間の共通要件として統一する範囲（例：運用・保守要件やサービス稼働時間など）。
・情報保有機関間での費用分担の方式（例：人口で按分する、トラフィック量で按分するなど）。

また、既存システムがクラウド環境で共同利用されているケースも想定される。既存システム側のクラウド環境において、物理的にサーバーが分割されている（IP アドレスが分かれている）場合は、IP アドレス等に基づくルーティングテーブルを用いたルーティングが可能である。

10. 非機能要件

本章では、インターフェイスシステムの非機能要件について述べる。

10.1 前提条件

特になし

10.2 規模要件

規模要件は蓄積するデータ量とトラフィック量に依存する。これらは各情報保有機関固有の要件に依存するため、各情報保有機関における、情報照会／情報提供の頻度及び提供データ量等を考慮して、必要な帯域、サーバー諸元等について検討する必要がある。

10.3 可用性要件

(1) サービス稼働時間

インターフェイスシステムのサービス稼働時間の設定方法は、以下の 3 パターンが想定される。

1）各情報保有機関が個別に設定可能とする。
2）特定個人情報保護委員会システム、情報提供ネットワークシステム等と合わせた共通運用時間帯を設定し、それ以外の時間帯は各情報保有機関が個別に設定可能とする。
3）情報提供ネットワークシステム等と合わせた共通運用時間帯を設定し、それ以外の時間帯についても全情報保有機関共通ルール化する。

最低限の共通運用時間帯を保証しながらも、各情報保有機関の意向や目的によって個別に稼働時間の延長も可能となる、2）が望ましいと考えられるが、サービス稼働時間帯の設定方法は別途決定する必要がある。なお、共通運用時間帯の設定に当たっては、全国一律で情報照会・情報提供をどの時間帯まで可能とするか、という観点からも検討する必要がある。

また、サービス稼働時間の検討に当たっては、独立行政法人情報処理推進機構が非機能要求の確認を行うことを目的として策定した「非機能要求グレード」を元に検討を行うが、サービス稼働時間については、各情報保有機関の業務時間の実情を考慮したものとすることが望ましい。例えば、レベル 1 は「非機能要求グレード」では、定時内の目安を 9 時から 17 時としているが、現在の情報保有機関の業務時間を勘案する

と、8 時から 18 時とする、などである。「非機能要求グレード」の原版及び、現在の情報保有機関の業務時間を勘案して修正した版を以下に示す。

表 27　非機能要求グレード（原版）による運用時間レベル

指標	レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5
運用時間（平日）	規定無し（非稼働）	定時内（9 時～17 時）	夜間のみ停止（9 時～21 時）	1 時間程度の停止（9 時～翌朝 8 時）	若干の停止（9 時～翌朝 8 時 55 分）	24 時間無停止
運用時間（休日、祝祭日）	規定無し（非稼働）	定時内（9 時～17 時）	夜間のみ停止（9 時～21 時）	1 時間程度の停止（9 時～翌朝 8 時）	若干の停止（9 時～翌朝 8 時 55 分）	24 時間無停止

表 28　非機能要求グレード（業務時間を勘案して修正した版）による運用時間レベル

指標	レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5
運用時間（平日）	規定無し（非稼働）	定時内（8 時～18 時）	夜間のみ停止（8 時～21 時）	1 時間程度の停止（8 時～翌朝 7 時）	若干の停止（8 時～翌朝 7 時 55 分）	24 時間無停止
運用時間（休日、祝祭日）	規定無し（非稼働）	定時内（8 時～18 時）	夜間のみ停止（8 時～21 時）	1 時間程度の停止（8 時～翌朝 7 時）	若干の停止（8 時～翌朝 7 時 55 分）	24 時間無停止

インターフェイスシステムのサービス稼働時間のうち、共通運用時間帯については、特定個人情報保護委員会システム、情報提供ネットワークシステム及び既存システム（関連情報保有機関（市町村、都道府県等）も含まれる）等の運用時間にも影響し、それらとの整合を図ることが望ましい。ここでは、平日、休日、祝祭日ともにレベル 2 を想定するが、詳細については、上記システムの検討内容も踏まえ別途定めることとする。

個別の運用時間帯は情報保有機関の個別状況（要件）等を勘案して、情報保有機関が個別に決定する必要がある。

- 業務時間（特に、窓口対応等の住民サービス提供時間）
- 番号法案別表第 2 で定められた事務及び特定個人情報に対する、即時応答や即時更新の必要性

・ 運用コスト

情報保有機関において具体的に想定される個別状況（要件）と、それに対応するサービス稼働時間の例について以下に示す。

表 29　個別状況とサービス稼働時間の例

想定される事情（要件）	設定するサービス稼働時間の例
・情報照会、情報提供の量が多く、より長時間のサービス提供が求められる。 ・窓口対応等の住民サービス提供時間が長い。 ・土日、祝日も窓口対応している等。	平日：レベル 3 休日、祝祭日：レベル 2 等
・情報照会、情報提供の量が少なく、業務時間内に情報照会、情報提供業務を完了できる。 ・窓口対応等の住民サービス提供時間が比較的短い。 ・土日、祝日は閉庁している等。	平日：レベル 2 休日、祝祭日：レベル 0 等

(2) 目標復旧水準

業務停止を伴う障害が発生した際、何をどこまで復旧させるかの目標を定める必要がある。目標復旧水準には RPO（目標復旧地点）及び RTO（目標復旧時間）の 2 種類がある。

RPO（目標復旧地点）は、データ量、再処理の負荷を考慮し、データ種別ごとに定める必要がある。例えば、処理通番、プレフィックス情報、情報提供記録等に分けて考える。

RTO(目標復旧時間)は､国の行政機関等からの情報照会等が発生することも考慮し、12 時間以内の復旧が望ましいと考えられる。

「非機能要求グレード」における RPO 及び RTO の記載について、以下に示す。

表 30　非機能要求グレードによる RPO・RTO のレベル

指標	レベル 0	レベル 1	レベル 2	レベル 3	レベル 4
RPO	復旧不要	5 営業日前時点	1 営業日前時点	障害発生時点	―
RTO	1 営業日以上	1 営業日以内	12 時間以内	6 時間以内	2 時間以内

RPO、RTO を定めるべきデータ種別の例を以下に示す。

表 31　データ種別の例

観点	データ種別
データ	処理通番
	プレフィックス情報
	情報提供等記録
ログ	アクセスログ等

目標復旧水準は、情報保有機関で保有するデータ種別ごとに、以下に示す情報保有機関の個別状況（要件）等を勘案して、情報保有機関が個別に決定する必要がある。

- 当該データ種別の重要性、復旧優先度
- 当該データ種別を管理する既存システムの RPO・RTO
- 住民に対するサービスレベル
- 運用コスト

(3) 耐障害性要件

インターフェイスシステムは、障害が発生した場合でも情報照会や情報提供業務に支障を来たさないように、ハードディスク、電源、ネットワークインターフェイス等の部品の冗長化やクラスタ構成によるサーバー本体の冗長化等の対応を行う必要がある。

インターフェイスシステムの耐障害性要件は、情報保有機関ごとに、以下のような個別状況、要件等を勘案して決定する必要がある。想定される個別要件と、対応するサービス稼働時間の例について、以下に示す。

・障害発生時から復旧完了までの時間（MTTR）

表 32　個別状況と耐障害性要件の例

個別状況、要件の例	耐障害性要件の例
・完全無停止（MTTR=0）	サーバー本体の冗長化（ホットスタンバイ）
・原則即時復旧（MTTR=数分～数十分を想定）	サーバー本体の冗長化(コールドスタンバイ)
・障害発生日内での復旧（MTTR=数時間を想定）	部品の冗長化（ハードディスク、電源、ネットワークインターフェイス等の冗長化等）
・翌日以降の復旧（MTTR=1 日以上）	冗長化なし

10.4 セキュリティ要件

インターフェイスシステムのセキュリティ要件として、以下を実施する。なお、情報提供ネットワークシステム等の外部との通信に影響する要件（暗号化／復号要件、ウィルス対策要件等）については、安全性を確保するため、別途検討する。

インターフェイスシステムの構築・運用においては、セキュリティ対策に係る以下の 1)～3)の対策を実現するために、(1)～(3)の具体策を実施すること。

1)機密性対策

個人情報保護等の観点から、許可された者以外が情報の閲覧等を行った場合、問題が生じる又は生じる可能性があるものに対する対策。

2)完全性対策

破壊や改ざん等の意図しない情報の不備が発生することにより、問題が生じる又は生じる可能性があるものに対する対策。

3)可用性対策

許可された利用者が必要な時に情報及びインターフェイスシステムを利用できない状況になった場合、問題が生じる又は生じる可能性があるものに対する対策。

(1) 物理的対策

1)機密性対策・完全性対策

・インターフェイスシステムは、物理的対策の取られた管理エリアに保管又は配置すること。
・管理エリアの入退室の制限を行うこと。
・管理エリアの鍵の管理を行うこと。
・管理エリア内の情報機器の持ち出し、及び管理エリアへの個人所有のパソコンの持込を行わないこと。

2)可用性対策

・可搬媒体移送中の物理的な損傷から保護するための措置を講ずること。

(2) 技術的対策

1)機密性対策

・インターフェイスシステムの構築・運用においては、インターフェイスシステムにアクセス可能なすべての操作者について、適切な認証を実施すること。この際、インターフェイスシステムへのログインは、組織単位ではなく、人単位で実施すること。
・インターフェイスシステムに接続する機器に関し、IP アドレス、MAC アドレス等による適切な認証を実施すること。
・必要に応じて暗号化対策を検討すること。
・不正アクセス監視機能を実装すること。
・アクセスログ取得機能を実装すること。
・なりすまし防止機能を実装すること。
・他の情報システムと論理的又は物理的に区分されたネットワーク構成とすること。

2)完全性対策

・バックアップ取得機能を実装すること。
・ウィルス対策機能を実装すること。
・プログラム改ざん検出機能を実装すること。
・改ざんデータ検出機能を実装すること。

3)可用性対策

・バックアップ取得機能を実装すること。
・他の可用性要件を満たすために必要な場合は、情報システム及びネットワークの二重化を考慮すること。
・ウィルス対策機能を実装すること。
・開発環境と本番環境を分離すること。

(3) 人的対策

1)機密性対策

・機密性保持のための教育・訓練を実施すること。
・機密性区分を確実に遵守できるような可搬媒体の保管を行うこと。
・可搬媒体の処分の際、物理的な破壊等、情報を完全に判読不能な状態にしてから廃棄すること。
・可搬媒体の輸送中の紛失から保護するための措置を講ずること。
・無許可の機器接続等を監視すること。
・ユーザ ID 及びパスワードを適切に管理すること。

・機器の盗難防止に努めること。
・システムからの印刷物を適切に管理すること。
・情報システムの動作に不要なソフトウェア及びサービスの実装を禁止すること。
・不必要な機能を停止するための設定を行うこと。
・システム・リソースを適切に管理すること。
・開発及び運用ドキュメントを適切に管理すること。

2)完全性対策
・インターフェイスシステムの管理者権限は必要最小限のものに付与すること。
・ユーザ ID 及びパスワードを適切に管理すること。
・定期的にウィルスチェックを行うこと。
・システム・リソースを改ざんから保護すること。
・定期的にバックアップを取得すること。
・バックアップの保管期限を定めること。

3)可用性対策
・障害対応体制を確立すること。
・可用性保持のための教育・訓練を実施すること。
・運用管理手順書を整備すること。
・情報システム障害記録を整備すること。
・定期的にウィルスチェックを行うこと。
・ウィルスに関する情報収集を行うこと。
・定期的にバックアップを取得すること。
・潜在的な障害の可能性を把握すること。
・障害監視を実施すること。
・システム設定情報を必要以上に変更しないこと。
・システム設定情報を変更する場合は事前に検証の上、履歴を管理すること。
・災害復旧手順書を整備すること。

10.5 運用･保守要件

インターフェイスシステムの運用・保守要件は、以下に示す作業区分及び作業項目に従って記載する。各作業項目における運用･保守要件は、次ページ以降に記載する。

表 33　インターフェイスシステムの運用・保守要件

#	作業区分	作業項目
1.	運用プロジェクト管理	運用プロジェクト管理

#	作業区分	作業項目
2.		運用ドキュメント管理
3.		サービスレベル管理
4.	構成管理等	構成管理
5.		変更管理
6.		リリース管理
7.	オペレーション	バッチ処理管理
8.		システム起動・停止
9.		バックアップ
10.	ヘルプデスク	問合せ対応
11.		問合せ管理
12.	監視	ハードウェア監視
13.		ソフトウェア監視
14.		リソース情報収集・監視
15.		収集情報の提供
16.	障害対応	インシデント管理
17.		障害検知・通報
18.		障害原因一次切り分け・障害対応調整
19.		障害原因調査
20.		復旧措置
21.		障害対応
22.		履歴管理
23.		障害連絡体制
24.	保守環境	保守環境

10.6 運用プロジェクト管理

(1) 運用プロジェクト管理

業務実施計画に基づき、運用保守が円滑に実施されるよう、進捗管理、品質管理、課題管理等の必要なプロジェクト管理を行う。また、その状況について発注者に定期的に報告する。

(2) 運用ドキュメント管理

運用に係る各種ドキュメントを適切に管理し、最新の状態を維持する。

(3) サービスレベル管理

業務実施計画にあたり、データセンターや回線の提供に係る適切なサービスレベルを策定し、発注者と合意する。また、策定したサービスレベルについて測定・監視し、発注者に定期的に報告すると共に、目標値を達成しなかったときの対応策について検討し実施する。

10.7 構成管理・変更管理

(1) 構成管理

システム構成（ソフトウェア、ハードウェア、ネットワーク構成）を管理し、ドキュメントを最新の状態に維持する。

(2) 変更管理

システム構成（ソフトウェア、ハードウェア、ネットワーク構成）の変更を管理し、ドキュメントを最新の状態に維持する。

ソフトウェアについては、各種設定及び、パッチの提供状態も含め管理する。

ハードウェアについては、設定変更、ファームウェアの更新状況を含めて管理する。

特にインターフェイスシステムにおいては、以下に示すアプリケーション及びプレフィックス情報の変更対応が重要となる。

① アプリケーションの変更対応

アプリケーションに変更が生じた場合に、定期的（夜間バッチによる一斉配信等）及び緊急時に、その変更を反映する。

② プレフィックス情報の変更対応

上記に連動して、適切なタイミングでプレフィックスの変更を実施する。

(3) リリース管理

ソフトウェアのリリース状態（版管理を含む）を管理する。

10.8 オペレーション

(1) バッチ処理・スケジュール管理

日次稼働、週次稼働、月次稼働、年次稼働のバッチジョブのスケジュール管理、起動・停止（自動運転）、正常稼働確認等を行う。

(2) システム起動・停止オペレーション作業

運用スケジュールに従ってシステムの起動、停止作業、確認作業等のオペレーション作業を行う。

(3) バックアップ

バックアップジョブ（自動運転）の正常稼働確認を行う。また、外部保管を行う場合は、バックアップ媒体の外部保管用の媒体交換作業を行う。

10.9 ヘルプデスク

(1) 問合せ対応

電話、電子メールにて、利用者からの各種問合せを受け付ける。

(2) 問合せ管理

問合せの受付から、回答までの履歴を記録し、対応状況を管理する。

頻発する問合せ内容についてはFAQ作成を行う。

10.10 監視

インターフェイスシステムのシステム監視機能を用いて、各業務システムの稼働状況を確認し、異常な状態（もしくは異常な状態を招く兆候）を検知する。

また、異常を示す事象を自動的に検知可能な運用環境を構築し、異常が検知された場合には、即座に担当者へ連絡できること。また、運用要件に応じて一時的に監視を抑止することができる。

(1) ハードウェア監視

インターフェイスシステムに、運用管理ソフトウェアを導入し、構成管理、性能管理、セキュリティ管理、システム監視、ジョブ実行管理等、各ハードウェアの稼働状況を監視する。

マシンのランプ点灯状況を定期的に巡回監視する。

(2) ソフトウェア監視

インターフェイスシステムを構成するソフトウェアに対して、システム監視機能等を利用し、OS、ミドルウェア、アプリケーションの稼働状況等を監視する。

(3) リソース情報収集・監視

システム監視機能等を利用し、各機器の CPU、メモリ、ディスク、ファイル等のリソース使用状況を定期的に監視する。

システム・リソースが枯渇状態になる前に対策が行えるよう、警戒すべきリソース使用率の閾値を一定時間超過した状態を検知すること。また、リソースの枯渇状態は即時に対応が行える重要度で検知する。

システム・リソースの使用状況は統計的な分析が行えるよう、データを保管する機

能を設ける。

(4) 収集情報の提供

統合運用に必要な管理情報（リソース使用状況）、報告資料等を定期的に作成した上で、定期報告会を開催し、運用状況の報告を行う。なお、開催時期・回数等は別途協議の上決定する。

また、指示要望があれば速やかに情報提供を行う。

10.11 障害対応

(1) インシデント管理

障害等の各種インシデントについて検知・記録し、インターフェイスシステムへの影響度や緊急度等について分析した上で、必要な対応を実施する。

(2) 障害検知・通報

障害を検知した場合又は不具合が判明した場合は、障害時の対応マニュアルに従い、発注者及び関係業者に速やかに連絡を行う。

(3) 障害原因一次切り分け・障害対応調整

障害原因の一次切り分けとして、障害がインターフェイスシステムで発生しているのか、他システムで発生しているのかを特定する。

障害復旧予定時刻、影響範囲、対応方法等について発注者及び関係業者と調整し、速やかに報告する。

(4) 障害原因調査

障害の原因及び状況を調査し、速やかに報告する。

他システムとの調整が必要とされる場合にはこれに協力する。

(5) 復旧措置

障害内容、影響を考慮し、速やかに復旧作業を実施する。

他システムとの調整が必要とされる場合にはこれに協力する。

(6) 障害対応

障害が発生した根本原因を調査し、速やかに発注者及び関係業者に報告するとともに、解決に向けた対策を実施する。

障害対応の事象、影響や原因、暫定対応策や恒久対応策は障害対応記録として管理し、報告する。

他システムとの調整が必要とされる場合にはこれに協力する。

(7) 履歴管理

障害対応について実績を管理する。

(8) 障害連絡体制

障害発生時には、コアシステム、中間サーバー及び既存業務システム等の運用業者等と連絡できる体制を整備し、障害の復旧に努めること。

10.12 保守環境

稼働後のテスト、検証等に用いる保守環境を用意する。