

「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」

－中間サーバー技術標準の検討に係る報告書－

平成２５年３月２９日

目 次

はじめに	1
1. 用語の定義	2
2. 情報提供ネットワークシステム及び中間サーバーの概要	4
2.1 情報提供ネットワークシステムの概要	4
2.2 中間サーバーの概要	5
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	6
3. 中間サーバー検討の概要	9
3.1 中間サーバー検討の範囲	9
3.2 中間サーバー検討の概要	10
4. 全体機能構成・機能配置	11
4.1 機能概要	11
4.2 インターフェイスシステムの機能構成（概要）	13
4.3 中間サーバーの機能構成（概要）	14
5. 中間サーバーの導入に係る前提条件	16
5.1 調達範囲	16
5.2 技術標準	16
5.3 中間サーバーの設置単位	17
6. 機能要件	18
6.1 機能一覧	18
6.2 符号管理機能	24
6.3 情報照会側機能	27
6.4 情報提供側機能	40
6.5 既存システム接続機能	50
6.6 情報提供記録管理機能	59
6.7 情報提供 DB 管理機能	61
6.8 データ送受信機能	64
6.9 セキュリティ管理機能	66
6.10 職員認証・権限管理機能	67
6.11 システム管理機能	70
7. 画面要件	71
7.1 画面一覧	71
7.2 画面定義	72
8. データ要件	85
8.1 中間サーバーで管理する情報（一覧）	85

8.2 中間サーバーで管理する情報（詳細）	86
8.3 情報提供 DB へのデータの記録年数	89
9. 稼働環境	90
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	90
9.2 LAN 上の配置.....	91
9.3 クラウド環境への導入	93
10. 非機能要件	97
10.1 前提条件	97
10.2 規模要件	97
10.3 可用性要件	97
10.4 セキュリティ要件	101
10.5 運用・保守要件	103
10.6 運用プロジェクト管理	104
10.7 構成管理・変更管理	105
10.8 オペレーション	105
10.9 ヘルプデスク	106
10.10 監視	106
10.11 障害対応	107
10.12 保守環境	108

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った。

本書は、中間サーバーの技術標準(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中間サーバーの概要

本章では、情報提供ネットワークシステム及び中間サーバー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。

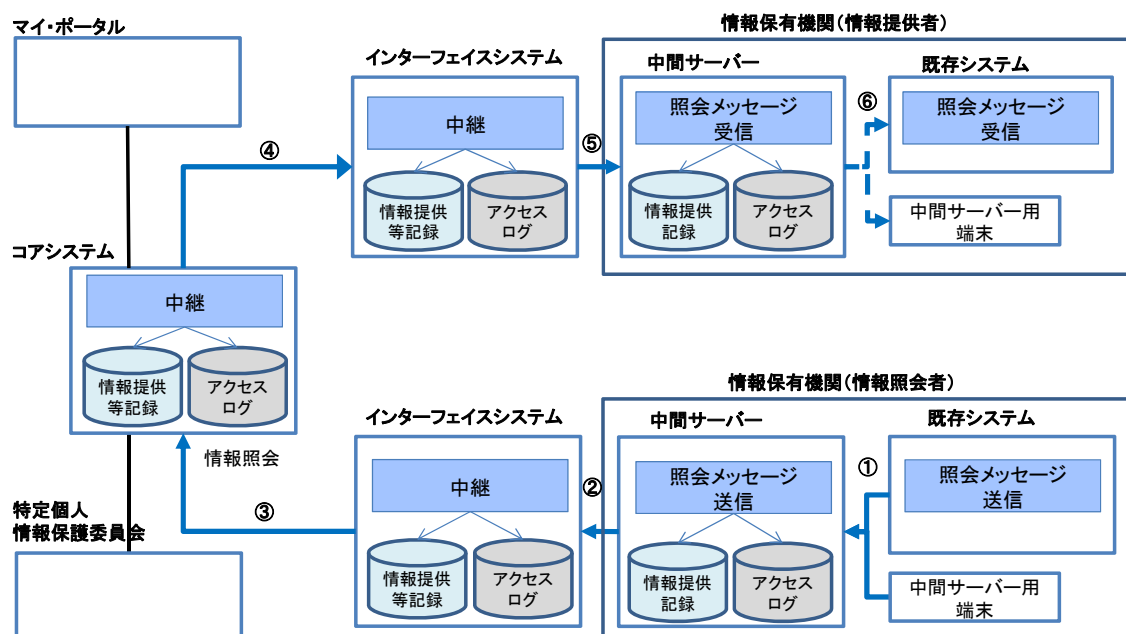


図 1 情報提供ネットワークシステムを用いた情報照会の流れ

- ・ 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。

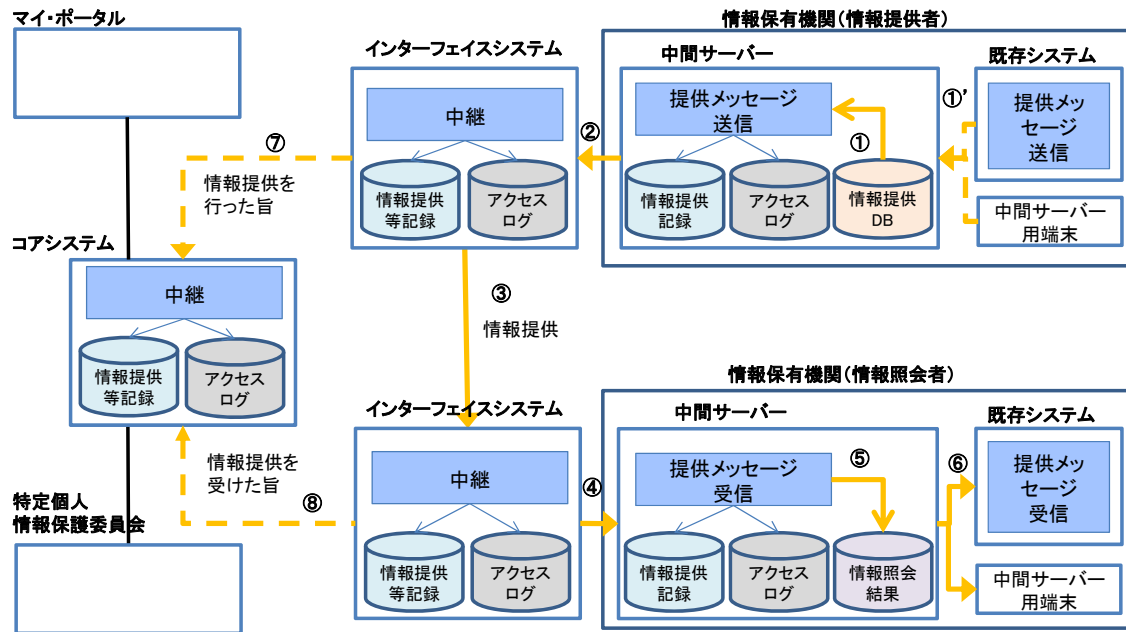


図 2 情報提供ネットワークシステムを用いた情報提供の流れ

- ・ 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 中間サーバーの概要

中間サーバーとは、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が保有する既存システムとの間で、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 中間サーバーは、情報照会・情報提供において、各情報保有機関が保有する宛名番号と符号を 1 対 1 で紐付・管理する仕組みを有する。
- 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、情報提供ネットワークシステムにて、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他情報保有機関からの情報照会に応じ、情報提供を自動で行うことを基本とする。
このために、既存システムが保有する特定個人情報の複製を、情報提供 DB として保持する。なお、情報提供においては、情報照会時に付番された処理通番を付して返答する（情報提供時に符号は返さない）。
- ④中間サーバーは、個人番号及び基本 4 情報を保有しないことを基本とする。

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. 中間サーバー検討の概要

本章では、中間サーバー検討の概要や位置付けについて述べる。

3.1 中間サーバー検討の範囲

本書は、中間サーバー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「C. 中間サーバー技術標準の検討」の部分である。

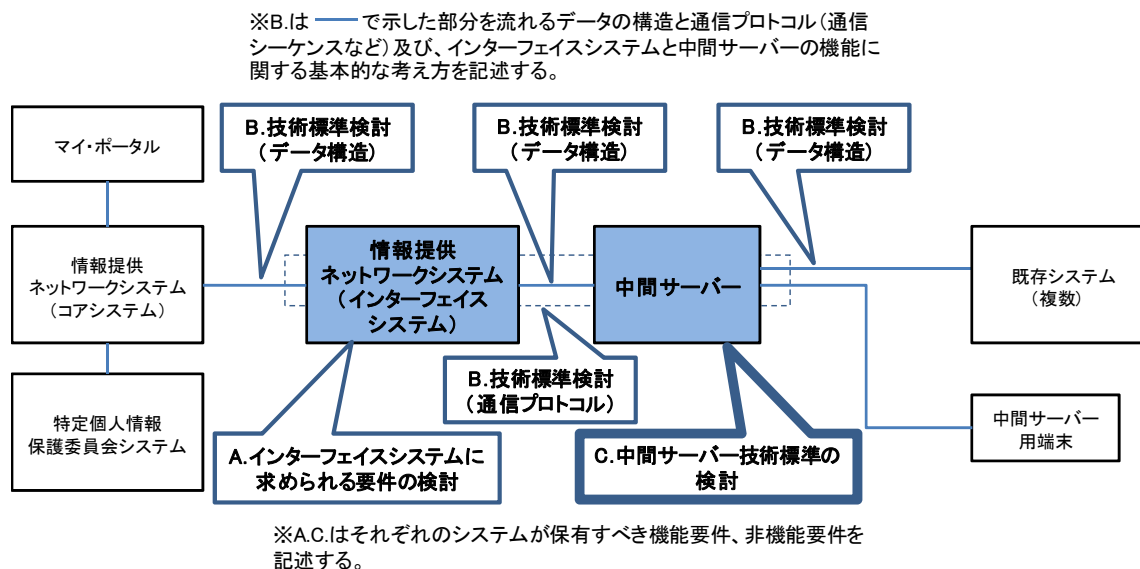


図 3 中間サーバー技術標準の検討範囲

インターフェイスシステムが保有すべき機能要件、非機能要件については、「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」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 中間サーバー検討の概要

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) 中間サーバーの導入に係る前提条件

中間サーバー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中間サーバー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) 画面要件

中間サーバーにおいて具備する画面について整理したもの。

(5) データ要件

中間サーバーにおいて管理する情報（データ）について整理したもの。

(6) 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。

(7) 非機能要件

中間サーバーの規模、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。

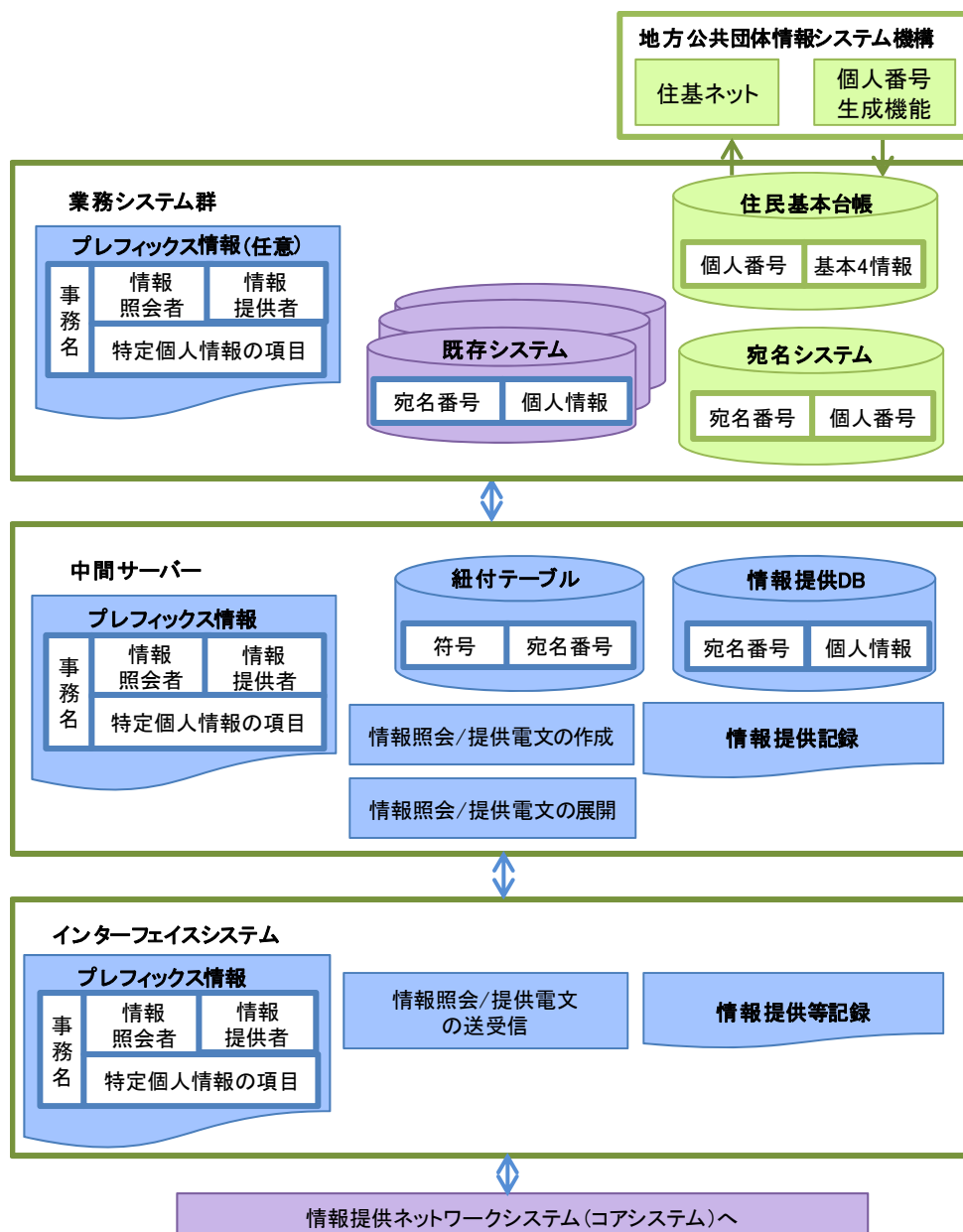


図 4 インターフェイスシステム及び中間サーバーで保持する主な情報とその関係

5. 中間サーバーの導入に係る前提条件

本章では、中間サーバーの導入に係る前提条件について述べる。

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 中間サーバーの設置単位

中間サーバー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、中間サーバーの 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、中間サーバー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中間サーバー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、対応画面等については、今後予定される中間サーバー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) 符号管理機能

符号管理機能について、以下を示す。

表 6 符号管理機能

#	機能中分類	機能小分類	対応画面
1.	符号の取得・紐付	符号取得用ファイル出力	符号取得用ファイル出力画面
2.		符号の取得・登録	—
3.	符号—宛名紐付管理	—	符号—宛名紐付管理画面
4.	宛名番号→符号変換	—	—
5.	符号→宛名番号変換	—	—

(2) 情報照会側機能

① 情報照会

情報照会側機能（情報照会）について、以下に示す。

表 7 情報照会側機能（情報照会）

#	機能中分類	機能小分類	対応画面
1.	入力・登録	情報照会内容入力	情報照会内容入力画面
2.		情報照会ファイル登録	情報照会ファイル登録画面
3.		既存システムファイル連携	—
4.		既存システム即時連携	—
5.	表示・出力	情報照会内容表示	情報照会内容表示画面
6.		情報照会内容 PDF 出力	情報照会内容 PDF 出力画面
7.	送信準備・送信	処理通番発行依頼	情報照会電文送信画面
8.		プレフィックス情報照合依頼	
9.		情報提供許可証発行依頼	

#	機能中分類	機能小分類	対応画面
10.		情報照会電文作成	
11.		情報照会電文送信	
12.		情報照会バッチ実行	

② 情報提供受領(情報照会先からの情報提供取得時)

情報照会側機能（情報提供受領）について、以下に示す。

表 8 情報照会側機能（情報提供受領（情報照会先からの情報提供取得時））

#	機能中分類	機能小分類	対応画面
1.	受信・展開	情報提供電文受信	情報照会側状況表示画面
2.		情報提供電文展開（復号）	
3.		情報提供受領通知送信	
4.		情報提供内容一時保存	
5.		情報提供記録送信	
6.	表示・出力	情報提供内容表示	情報提供内容表示画面
7.		提供情報ファイル出力	情報提供ファイル出力画面
8.		提供情報 PDF 出力	情報提供 PDF 出力画面
9.		既存システムファイル連携	—
10.		既存システム即時連携	—

③ 情報照会側状況管理

情報照会側機能（情報照会側状況管理）について、以下に示す。

表 9 情報照会側機能（情報照会側状況管理）

#	機能中分類	機能小分類	対応画面
1.	情報照会側状況管理	情報照会側状況表示	情報照会側状況表示画面
2.		情報照会側状況連携	—

(3) 情報提供側機能

① 情報照会受領(他情報保有機関からの情報照会)

情報提供側機能（情報照会受領）について、以下に示す。

表 10 情報提供側機能（情報照会受領（他情報保有機関からの情報照会））

#	機能中分類	機能小分類	対応画面
1.	受信・展開	情報照会電文受信	情報提供側状況表示画面
2.		情報提供許可証チェック	
3.		情報照会電文展開・確認	
4.		情報照会受付完了送信	
5.		情報照会内容一時保存	
6.	表示・出力	情報照会内容表示	情報照会内容表示画面
7.		情報照会ファイル出力	情報照会ファイル出力画面
8.		照会情報 PDF 出力	情報照会 PDF 出力画面
9.		既存システムファイル連携	—

② 情報提供

情報提供側機能（情報提供）について、以下に示す。

表 11 情報提供側機能（情報提供）

#	機能中分類	機能小分類	対応画面
1.	入力・登録	情報提供内容入力	情報提供内容入力画面
2.		情報提供ファイル登録	情報提供ファイル登録画面
3.		既存システムファイル連携	—
4.	表示	情報提供内容表示	情報提供内容表示画面
5.	送信準備・送信	情報提供内容抽出	情報提供側状況表示画面
6.		情報提供電文作成（暗号化）	
7.		情報提供電文送信	
8.		情報提供受領通知受信	
9.		情報提供記録送信	
10.	自動応答	—	情報提供側状況表示画面

③ 情報提供側状況管理

情報提供側機能（情報提供側状況管理）について、以下に示す。

表 12 情報提供側機能（情報提供側状況管理）

#	機能中分類	機能小分類	対応画面
1.	情報提供側状況管理	情報提供側状況表示	情報提供側状況表示画面
2.		情報提供側状況連携	—

(4) 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 13 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.	Web サービス連携	PUSH 型サービス受付	—
2.		PULL 型サービス受付	—
3.		連携制御	—

(5) 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 14 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	—	—
2.	情報提供記録検索	—	情報提供記録表示画面
3.	情報提供記録ファイル出力	—	—
4.	情報提供記録削除	—	—
5.	情報提供記録電文の作成	—	—

(6) 情報提供 DB 管理機能

情報提供 DB 管理機能について、以下に示す。

表 15 情報提供 DB 管理機能

#	機能中分類	機能小分類	対応画面
1.	情報提供 DB 更新（一括）	—	—
2.	情報提供 DB 更新（都度）	—	—
3.	保存期限切れデータ削除 機能	—	—

(7) 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 16 データ送受信機能

#	機能中分類	機能小分類	対応画面
1.	送付先管理	—	送付先管理画面
2.	通信制御	—	—
3.	送信	ヘッダチェック	—
4.		ボディチェック	—
5.		送信・記録	—
6.	受信	受信・記録	—
7.		ヘッダチェック	—
8.		ボディチェック	—

(8) 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 17 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.	暗号化	—	—
2.	復号	—	—
3.	鍵管理	—	—
4.	プレフィックス情報取得	※情報提供ネットワークシステムより	—
5.	プレフィックス情報配信	※既存システムへ	—

(9) 職員認証・権限管理機能

職員認証・権限管理機能について、以下に示す。

表 18 職員認証・権限管理機能

#	機能中分類	機能小分類	対応画面
1.	職員認証	—	—
2.	職員認証連携	—	—
3.	職員権限管理	—	職員権限設定画面

(10) 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 19 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.	ジョブ管理	—	—
3.	バックアップ管理	—	—
4.	運用監視	—	—

6.2 符号管理機能

(1) 前提条件

中間サーバーが対象とする宛名体系は、以下に示すとおり、宛名番号：符号＝1：1で、かつ、それぞれに重複がない形式とする。

統一的な 宛名番号	符号	業務X			業務Y	
		項目X1	...	項目Xn	項目Y1	...
0001	A氏の符号	X1の値	...		Y1の値	...
0002	B氏の符号	X1の値	...		Y1の値	...
...	...					

図 5 統一的な宛名体系のイメージ図

中間サーバーにて、「符号から宛名番号への変換」及び「宛名番号から符号への変換」を実現するために、中間サーバーは、同一個人に対して、一つの宛名番号(統一的な宛名番号)及び、それに対応する一つの符号を保持する紐付情報を持つ。このため、中間サーバーと接続する既存システムは、同一個人に対して一つの宛名番号を保持することを前提とする。

(2) 機能要件

符号管理機能の機能要件について、以下に示す。

中間サーバーは、符号管理に関する以下の処理の流れを実現する機能を提供する。

- ・既存システムは、符号を取得する宛名番号を中間サーバーに送付する。
- ・中間サーバーは、処理通番発行依頼電文を作成し、インターフェイスシステムから処理通番を取得する。
- ・中間サーバーの操作者（管理者又はは職員）が、中間サーバーより「処理通番＋宛名番号」のセットを取得し、既存システムに送付する。
- ・「処理通番＋宛名番号」を受け取った既存システムは、「処理通番＋個人番号（又は基本4情報）」のセットに再構成する。この際、都道府県については、基本的に住基ネットサーバに媒体で転送し、市町村については、住基ネットのCS（コミュニケーション・サーバ）に既存住基ネットの回線又は媒体で転送する。
- ・既存システムの操作者（管理者又は職員）が、「当該処理通番と住民票コード」を情報提供ネットワークシステムに通知する。
- ・中間サーバーは、情報提供ネットワークシステムから「処理通番に対応する符号」を取得し、宛名番号と紐付ける。

符号の取得と紐付に係る機能の概要について、以下に示す。

表 20 符号の取得と紐付に係る機能の概要

#	機能中分類	機能小分類	概要
1.	符号の取得・紐付	符号取得用ファイル出力	中間サーバー側で処理通番発行依頼電文を作成し、インターフェイスシステムから処理通番を取得し、「処理通番＋宛名番号」のセットをファイルに出力する。 ※既存システムとオンライン連携することもある。この場合は既存システムからの PULL 型 Web サービスとする。
2.		符号の取得・登録	情報提供ネットワークシステムから処理通番に対応する符号を取得し、符号―宛名紐付テーブルに格納する。
3.	符号―宛名紐付管理	—	宛名番号と符号の紐付をメンテナンスする。 具体的には、画面及び Web サービスにて、宛名番号の登録・修正、符号の登録・修正を行えること。Web サービスの要求元は既存システムを想定する。
4.	宛名番号→符号変換	—	宛名番号を該当する符号に変換する。
5.	符号→宛名番号変換	—	符号を該当する宛名番号に変換する。

現在検討されている符号の初期生成の方法について、以下に示す。

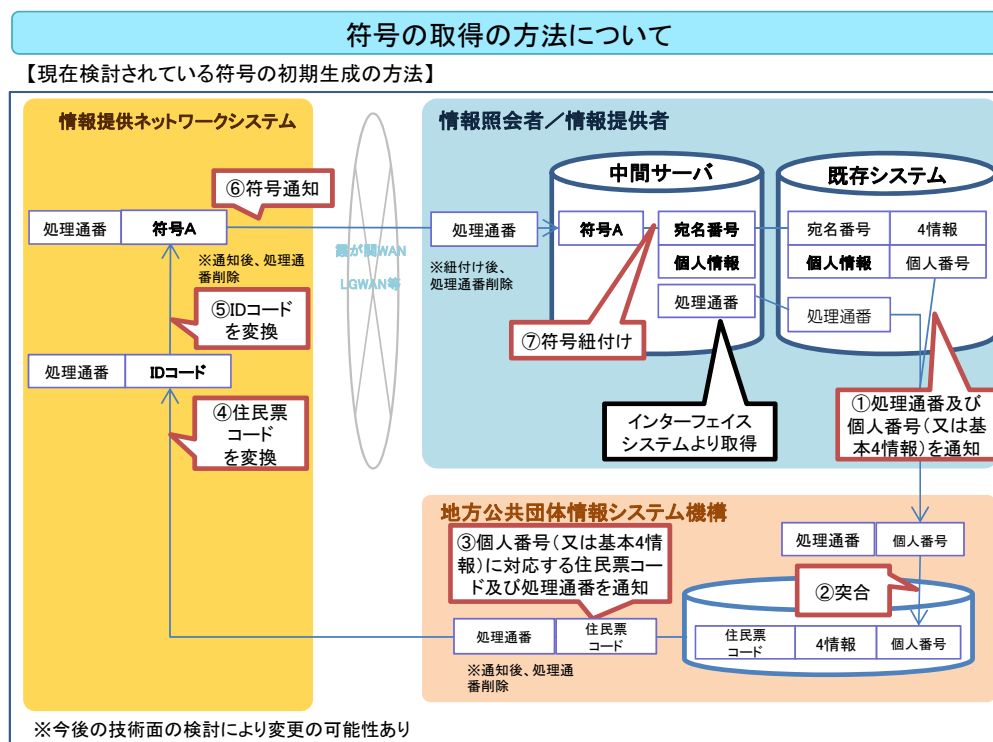


図 6 現在検討されている符号の初期生成の方法

6.3 情報照会側機能

(1) 前提条件

情報照会とは、当該情報保有機関が、番号法案別表第2に規定された事務を行う上で、他情報保有機関が保有する特定個人情報に照会する必要がある場合に、他情報保有機関に、「符号、事務名、特定個人情報の項目コード」にて照会を行うことである。

① 情報照会の接続パターン

情報照会の接続パターンとして、業務的な観点から、以下の2ケースを想定する。

- ・ 情報保有機関の窓口等で、住民からの申請等を受け付けた職員が、端末を使って情報照会を実施する。
- ・ 他情報保有機関への複数件の情報照会を、一括で実施する。

上記を、システムにて実現する方法として以下の3パターン（画面入力、バッチ及び即時連携）を想定する。

- 1) 中間サーバーに接続された端末の画面から、情報照会内容を入力する
- 2) 予め登録した情報照会内容のファイルを、バッチ処理で送信する
- 3) 既存システムから中間サーバーに情報照会内容を連携し中間サーバーにて即時に情報照会を行う（その後、中間サーバーが他情報保有機関から取得した情報提供内容を、情報照会元の既存システムへ返す）

情報照会の接続パターンについて、以下に示す。

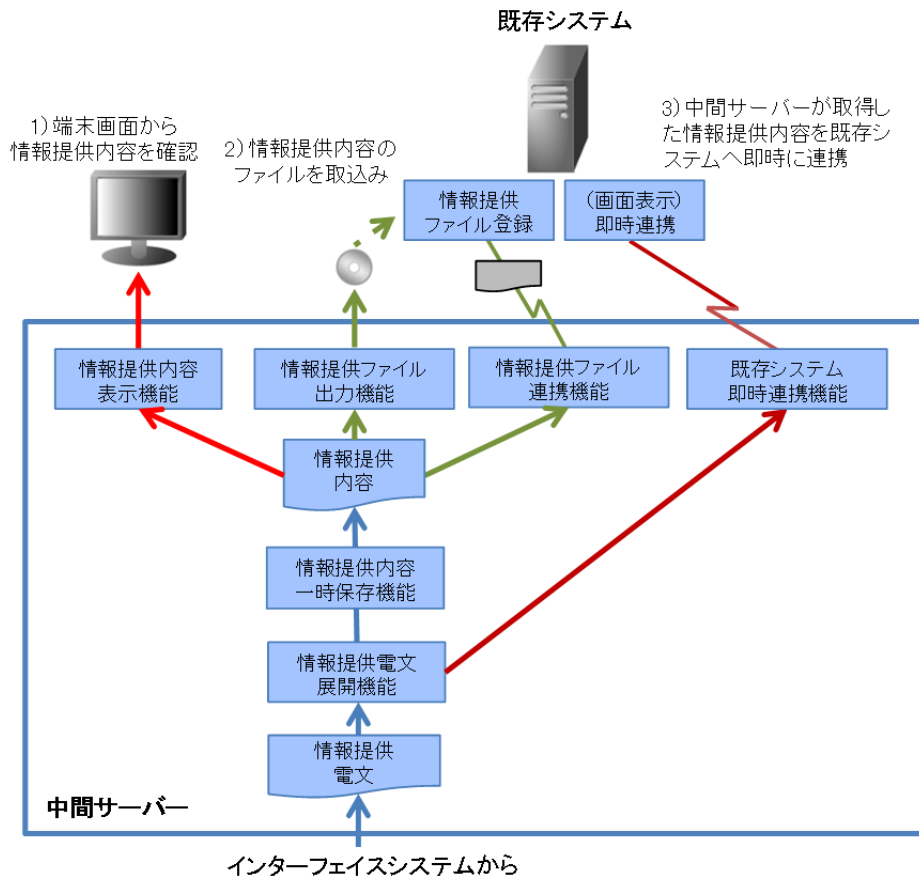


図 8 情報提供内容の確認・取込時の接続パターン

③ その他の前提条件

情報照会におけるその他の前提条件について、以下に示す。

- ・ 情報照会においては、必ず個人を特定した照会を行う（情報照会電文中には必ず符号が設定される）。
- ・ 問い合わせ条件及び回答を求める項目（特定個人情報の項目コードのリスト）は、情報照会時に情報照会者が設定し、情報提供側の情報提供にあたっては、当該情報照会項目のみを回答する。
- ・ 複数の情報保有機関に同じ内容の情報照会を行う場合は、中間サーバーにて照会する情報保有機関ごとに分解した情報照会電文を作成し、実施する。
- ・ 番号法案別表第2の事務ごとに、同一事務かつ同一情報保有機関に対して、同一対象者であれば、情報照会者の判断により複数の特定個人情報を問い合わせることも可能とする。ただし、複数の対象者にまたがる問い合わせは許可しない。
- ・ 中間サーバーは、個人番号及び基本4情報を保有しないことを基本とする。宛名番号と基本4情報を紐付て画面に表示するしくみが必要な場合は、既存システム側で対応する。

(2) 機能要件

情報照会側機能の機能要件について、以下に示す。

各機能の操作者は適切な権限を有するもののみとする。

なお各種電文の定義及び送受信シーケンスは、「技術標準の検討に係る報告書」を参照のこと。

① 情報照会

情報照会側機能（情報照会）の機能要件について、以下に示す。

表 21 情報照会側機能（情報照会）の機能要件

#	機能中分類	機能小分類	機能概要
1.	入力・登録	情報照会内容入力	情報照会内容を画面から入力する機能。1 件ごとの作成及び複数件の作成を可能とする。検索条件及び回答を求める項目を入力できること。
2.		情報照会ファイル登録	情報照会内容を媒体から登録（アップロード）する。
3.		既存システムファイル連携	情報照会内容ファイルを既存システムから連携・登録する。連携においては認証機能により権限の制御を行うこと。
4.		既存システム即時連携	情報照会内容を既存システムから中間サーバーに連携し、中間サーバーにて即時に情報照会を行う。連携においては認証機能により権限の制御を行うこと。
5.	表示・出力	情報照会内容表示	入力・登録した情報照会内容を画面に表示する。
6.		情報照会内容 PDF 出力	入力・登録した情報照会内容を PDF 出力する。
7.	送信準備・送信	処理通番発行依頼	インターフェイスシステムに処理通番の発行を依頼し、結果を取得する。
8.		プレフィックス情報照合依頼	インターフェイスシステムにプレフィックス情報の照合を依頼し、結果を取得する。
9.		情報提供許可証発行依頼	インターフェイスシステム経由でコア

#	機能中分類	機能小分類	機能概要
			システムに情報提供許可依頼を送り、結果を取得する。 情報提供許可証には情報提供側から情報照会側への経路情報が含まれる。
10.		情報照会電文作成	入力・登録した情報照会内容から情報照会電文を作成する。この際、宛番号→符号変換機能により、宛番号を符号に変換する。また、中間サーバーで管理している暗号化鍵及び情報提供許可証を添える。複数の情報保有機関に同じ内容の情報照会を行う場合には、情報保有機関ごとに分解した電文を作成する。
11.		情報照会電文送信	データ送受信機能を用いて情報照会電文を送信する。
12.		情報照会バッチ実行	入力・登録した情報照会内容を（即時送信しない場合を想定し）バッチ処理にて情報照会電文として送信する。

② 情報提供受領(情報照会先からの情報提供取得時)

情報照会側機能（情報提供受領）の機能要件について、以下に示す。

表 22 情報照会側機能（情報提供受領）の機能要件

#	機能中分類	機能小分類	機能概要
1.	受信・展開	情報提供電文受信	データ送受信機能を用いて情報提供電文、情報照会受付完了通知を受信する。自動受信を想定し、結果は、情報照会側状況表示画面に表示する。
2.		情報提供電文展開 (復号)	情報照会の返信として他情報保有機関から提供された情報提供電文（情報照会時と同じ処理通番の電文）の開封（電文からヘッダとボディを取出す）・ボディの復号・確認を行う。
3.		情報提供受領通知送信	データ送受信機能を用いて、情報提供受領通知をインターフェイスシステム

#	機能中分類	機能小分類	機能概要
			に送信する。
4.		情報提供内容一時保存	後続の機能のために、情報提供内容を一時的に中間サーバーに保存する。
5.		情報提供記録送信	データ送受信機能を用いて、情報提供記録をインターフェイスシステムを経由してコアシステムに送信する。
6.	表示・出力	情報提供内容表示	情報提供内容を画面に表示する。複数の情報提供内容の表示も想定する。
7.		提供情報ファイル出力	情報提供内容を媒体に出力する。複数の情報提供内容の出力も想定する。
8.		提供情報 PDF 出力	情報提供内容を PDF 出力する。複数の情報提供内容の出力も想定する。
9.		既存システムファイル連携	情報提供内容ファイルを、既存システムにオンラインで連携する。複数の情報提供内容の出力も想定する。連携においては認証機能により権限の制御を行う。
10.		既存システム即時連携	中間サーバーが、他情報保有機関より取得した情報提供内容を、即時に既存システムに連携する。連携においては認証機能により権限の制御を行う。

中間サーバーに一時保存された受信情報を既存システムファイル連携において連携する場合は、下図のように PULL 型 Web サービスにて既存システムに取り込むことを想定する。

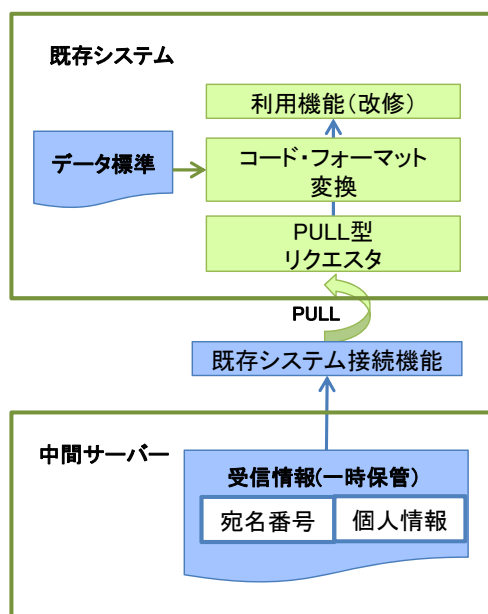


図 9 提供情報の既存システムへの連携

③ 情報照会側状況管理

情報照会側機能（情報照会側状況管理）の機能要件について、以下に示す。

表 23 情報照会側機能（情報照会側状況管理）の機能要件

#	機能中分類	機能小分類	機能概要
1.	情報照会側状況管理	情報照会側状況表示	以下の状況を一覧で表示する。 - 送信した情報照会電文の宛先（情報保有機関）、事務名、宛名番号、処理通番、送信状況（ステータス）、ステータス更新日時 - 他情報保有機関からの情報提供電文の受信状況、ステータス更新日時、情報提供の状況（該当データの有無等） 情報照会と情報提供は、処理通番にて、対として状況を管理できること。 複数の情報照会の状況一覧のうち、一

#	機能中分類	機能小分類	機能概要
			つを指定して、当該電文の内容を確認できること。この際、適切な権限管理を行えること。
2.		情報照会側状況連携	上記の内容について、既存システムからの PULL 型 Web サービスを通じて、既存システムに提供する。

④ 即時連携のシーケンス

情報照会側の即時連携のシーケンスについて、以下に示す。

(a) 所定時間内に情報提供を完了した場合

所定時間内に情報提供を完了した場合のシーケンスについて、以下に示す。

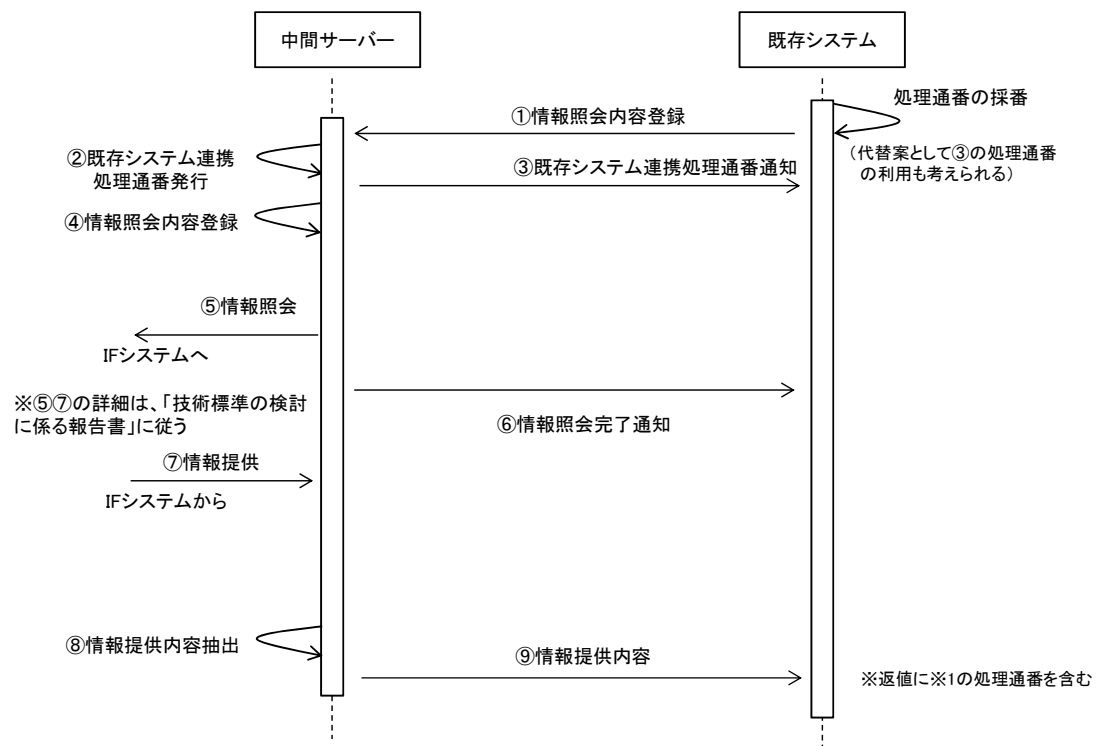


図 10 即時連携シーケンス図(所定時間内に情報提供を完了した場合)

※既存システムにおいて、①の情報照会内容登録の要求から、⑨の情報提供内容の受信までの状況は、「情報照会側状況照会」機能で確認する。

(b) 所定時間内に情報提供を完了しない場合

所定時間内に情報提供を完了しない場合のシーケンスについて、以下に示す。

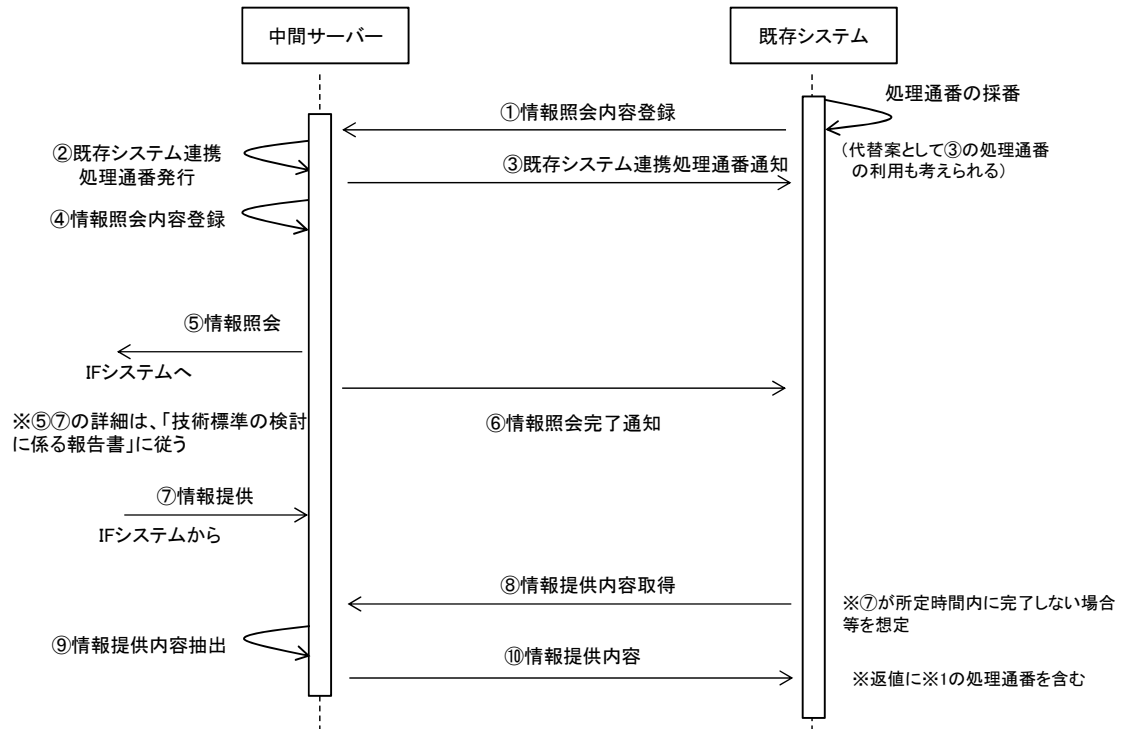


図 11 即時連携シーケンス図(所定時間内に情報提供を完了しない場合)

(3) 情報照会送受信ステータス

情報照会の送受信ステータスについて、以下に示す。

情報照会に際しては、以下のステータスを管理・表示できることとする。

なお、内部的に管理するステータスのすべてを画面に表示するか否かについては、設計時に検討するものとする。

表 24 情報照会送受信ステータス

#	分類	ステータス（正常系）	ステータス（異常系）
1.	情報照会（送信）	電文作成済み	宛名番号→符号変換失敗 情報照会電文作成失敗
2.		処理通番発行依頼済み	処理通番発行依頼送信失敗
3.		プレフィックス情報照合依頼済み	プレフィックス情報照合依頼送信失敗
4.		プレフィックス情報照合済み ※プレフィックス情報照合結果通知の内容が可の場合	プレフィックス情報照合失敗 プレフィックス情報照合結果受信タイムアウト
5.		情報提供許可依頼済み	情報提供許可依頼送信失敗
6.		情報提供許可済み ※情報提供許可通知が可の場合	情報提供許可失敗 情報提供許可通知受信タイムアウト
7.		情報照会電文送信済み	情報照会電文送信失敗
8.		情報照会受付完了受信済み	情報照会電文受付失敗 受信タイムアウト
9.	情報提供（受信）	情報提供電文受信済み	情報提供電文受信タイムアウト
10.		情報提供受領通知送信済み	情報提供受領通知送信失敗
11.		情報提供記録送信済み	情報提供記録送信失敗

(4) 情報照会・情報提供電文の構造(案)

情報照会・情報提供電文の構造について、「技術標準の検討に係る報告書」に記載されている内容の一部を、参考として以下に示す。

① 情報照会電文の構造(案)

(a) ヘッダ部

情報照会電文のヘッダ部について、以下に示す。

表 25 情報照会電文の構造(案)(ヘッダ部)

#	項目名	概要
1.	電文種別	“情報照会” を示すコード。
2.	処理日時	電文を生成した日時。
3.	情報照会機関コード	情報保有機関ごとに振られるコード。
4.	情報提供機関コード	情報保有機関ごとに振られるコード。
5.	事務コード	番号法案別表第2の事務コード。
6.	符号	情報照会において個人を一意に識別するための情報。
7.	特定個人情報名コードのリスト ※	番号法案別表第2の特定個人情報名コードと特定個人情報の項目コードのセット。コードが複数格納される場合もある。
8.	特定個人情報の項目コードのリスト ※	番号法案別表第2の特定個人情報名ごとに回答を要求する特定個人情報の項目コードのリスト。コードが複数格納される場合もある。
9.	問い合わせ条件	問合せ対象データの範囲(年度又は基準年月日(自～至)) ※以下、例： 年度を指定する場合： ＜対象年度＞H24＜/対象年度＞ 基準年月日を指定する場合： ＜基準年月日＞H241201＜/基準年月日＞ 基準年月日の自～至を指定する場合： ＜基準年月日自＞H241201＜/基準年月日自＞ ＜基準年月日至＞H250331＜/基準年月日至＞
10.	処理通番	情報照会ごとに採番される通番。

※ 特定個人情報名コードのリストと特定個人情報の項目コードのリスト例を以下に示す。なお、本データ構造は例示であり、今後のメッセージシーケンス等の検討を踏まえて決定する。また、以降の表において、特定個人情報名コードと特定個人情報の項目コードについて同様の記載がある場合は、本注釈を参照

のこと。

【特定個人情報名コードと特定個人情報の項目コードのリスト（例）】

<特定個人情報名コード>01</特定個人情報名コード>

<DETAIL>

<特定個人情報の項目コード>001</特定個人情報の項目コード>

<特定個人情報の項目コード>002</特定個人情報の項目コード>

</DETAIL>

<特定個人情報名コード>03</特定個人情報名コード>

<DETAIL>

<特定個人情報の項目コード>003</特定個人情報の項目コード>

<特定個人情報の項目コード>004</特定個人情報の項目コード>

</DETAIL>

(b) ボディ部(空欄)

情報照会電文のボディ部については、空欄となる。

(c) 許可証

情報照会電文の許可証について、以下に示す。

表 26 情報照会電文の構造（案）（許可証）

#	項目名	概 要
1.	経路情報	情報照会の経路情報。
2.	情報照会機関コード	情報保有機関ごとに振られるコード。
3.	情報提供機関コード	情報保有機関ごとに振られるコード。
4.	事務コード	番号法案別表第2の事務コード。
5.	特定個人情報名コードのリスト	番号法案別表第2の特定個人情報名コードと特定個人情報の項目コードのセット。コードが複数格納される場合もある。
6.	特定個人情報の項目コードのリスト	番号法案別表第2の特定個人情報名ごとに回答を要求する特定個人情報の項目コードのリスト。コードが複数格納される場合もある。
7.	処理通番	情報照会ごとに採番される通番。

(d) 暗号化鍵

暗号化鍵について、以下に示す。

表 27 情報照会電文の構造（案）（暗号化鍵）

#	項目名	概要
1.	暗号化鍵	情報照会者側の暗号化鍵。

② 情報提供電文の構造(案)

(a) ヘッダ部

情報提供電文のヘッダ部について、以下に示す。

表 28 情報提供電文の構造（案）（ヘッダ部）

#	項目名	概要
1.	電文種別	“情報提供”を示すコード。
2.	処理日時	電文を生成した日時。
3.	情報照会機関コード	情報保有機関ごとに振られるコード。
4.	情報提供機関コード	情報保有機関ごとに振られるコード。
5.	特定個人情報名コードのリスト	番号法案別表第2の特定個人情報名コードと特定個人情報の項目コードのセット。コードが複数格納される場合もある。
6.	特定個人情報の項目コードのリスト	番号法案別表第2の特定個人情報名ごとに回答を要求する特定個人情報の項目コードのリスト。コードが複数格納される場合もある。
7.	処理通番	情報照会ごとに採番される通番。

(b) ボディ部

情報提供電文のボディ部について、以下に示す。

表 29 情報提供電文の構造（案）（ボディ部）

#	項目名	概要
1.	問い合わせ結果	対象データの更新日時、照会結果等。

※網掛け部分について、情報提供時に更新を行う。

情報照会及び情報提供電文の構造は、今後のメッセージシーケンス等の検討を踏まえて決定する。

6.4 情報提供側機能

情報提供とは、当該情報保有機関が、情報照会を受けた場合に、保有する当該特定個人情報を提供することである。

(1) 前提条件

情報提供においては、情報提供 DB を用いた自動応答を基本とする。ここで、自動応答とは、中間サーバーが他情報保有機関より情報照会電文を受け取り、その内容に応じて、情報提供 DB より回答となる情報提供電文を作成し、情報照会元情報保有機関へ返す、一連の処理を自動で行うことである。

自動応答の流れについて、以下に示す。

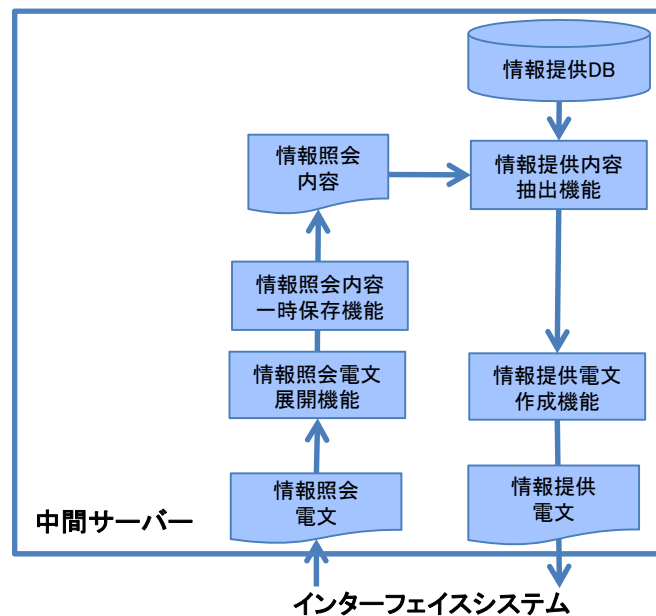


図 12 情報提供における自動応答の概念図

① 情報照会内容の確認の接続パターン

他情報保有機関から情報照会を受けた場合の情報照会内容の確認方法として以下の2パターンを想定する。

- 1) 中間サーバーに接続された端末の画面から、情報照会内容を確認する
- 2) 既存システムから情報照会内容のファイルを取り込み、中間サーバーへ取込む

情報照会内容の確認の接続パターンについて、以下に示す。

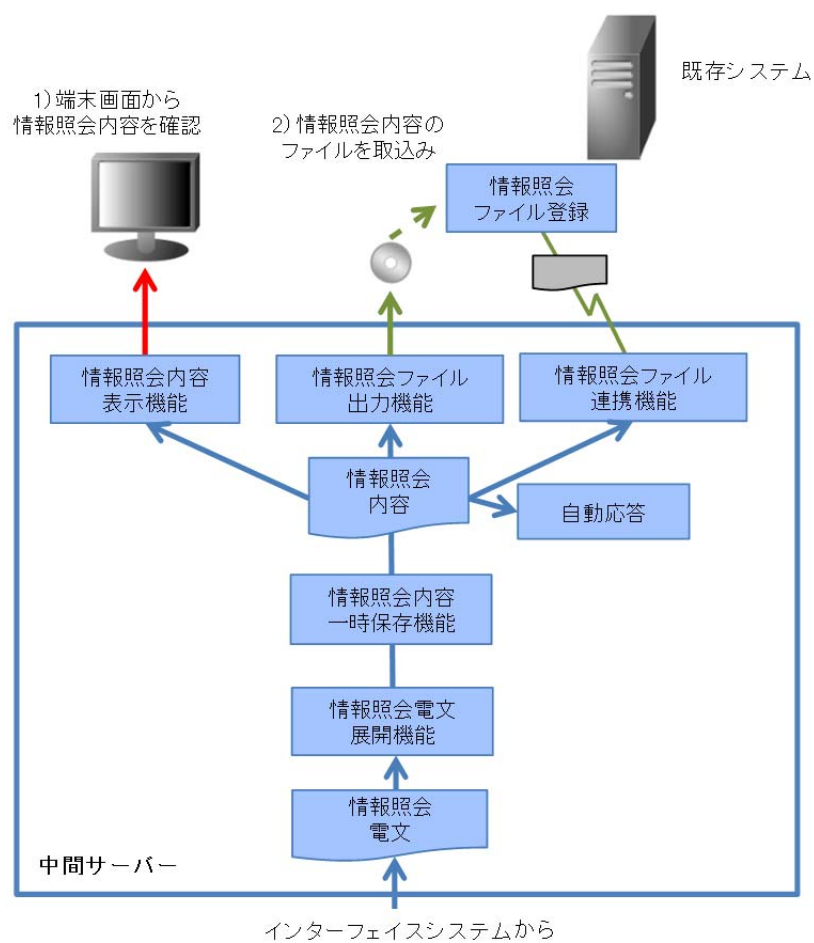


図 13 情報照会内容の確認の接続パターン

② 情報提供の接続パターン

情報提供の実現方法として以下の2パターンを想定する。

- 1) 中間サーバーに接続された端末の画面から、情報提供内容を入力する
- 2) 中間サーバーの情報提供 DB より情報提供内容のファイルを自動で提供する

情報提供の接続パターンについて、以下に示す。

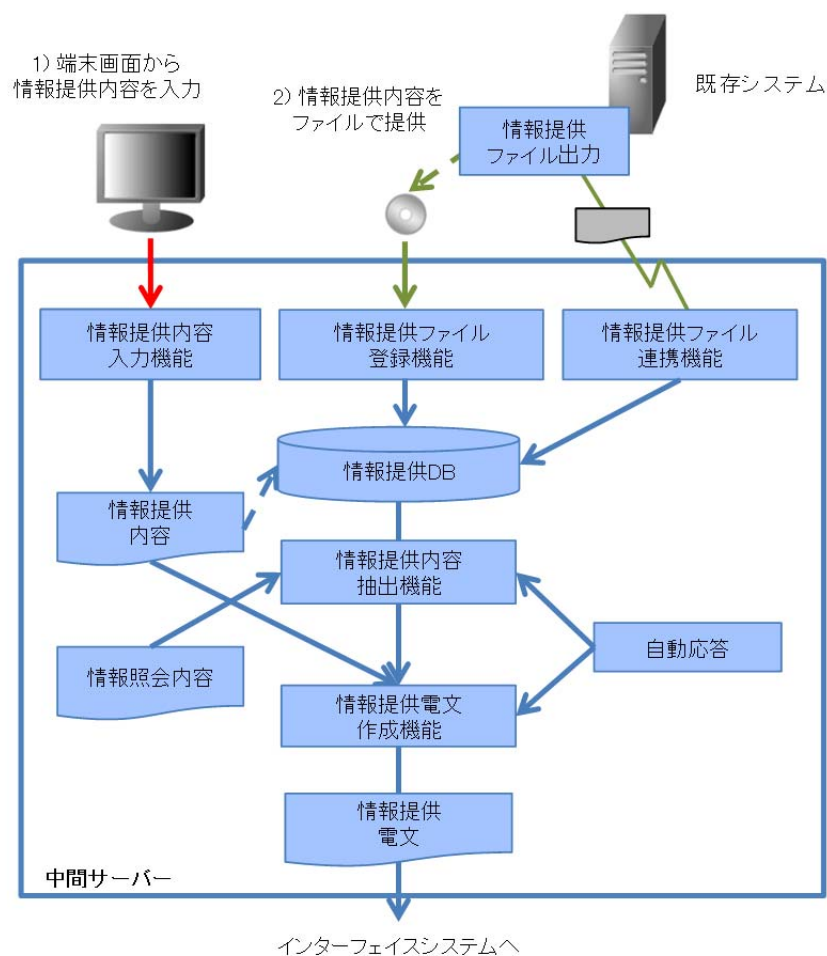


図 14 情報提供の接続パターン

※問い合わせ条件及び回答を求める項目（特定個人情報の項目コードのリスト）は、情報照会時に情報照会者が設定し、情報提供側の情報提供にあたっては、当該情報照会項目のみを回答する。

(2) 機能要件

情報提供側機能の機能要件について、以下に示す。

なお、各機能の操作者は適切な権限を有するもののみとする。

① 情報照会受領(他情報保有機関からの情報照会)

情報提供側機能（情報照会受領）の機能要件について、以下に示す。

表 30 情報提供側機能（情報照会受領）の機能要件

#	機能中分類	機能小分類	概要
1.	受信・展開	情報照会電文受信	データ送受信機能を用いて情報照会電文を受信する。自動受信を想定し、結果は情報提供側状況表示画面に表示する。
2.		情報提供許可証チェック	情報提供許可証のチェックを行い、暗号化鍵や情報照会側への経路制御情報を受領する。
3.		情報照会電文展開・確認	情報照会電文を展開・確認し、情報照会内容（検索条件等）を取り出す。この際、符号→宛名番号変換を行う。
4.		情報照会受付完了送信	照会元情報保有機関に、情報照会受付完了を送信する。
5.		情報照会内容一時保存	情報照会内容を中間サーバー上に一時的に保存する。
6.	表示・出力	情報照会内容表示	情報照会内容を画面に表示する。
7.		情報照会ファイル出力	情報照会内容をファイルに出力する。
8.		照会情報 PDF 出力	情報照会内容をファイルに出力する。
9.		既存システムファイル連携	情報照会内容ファイルを既存システムに連携する。

② 情報提供

情報提供側機能（情報提供）の機能要件について、以下に示す。

表 31 情報提供側機能（情報提供）の機能要件

#	機能中分類	機能小分類	概要
1.	入力・登録	情報提供内容入力	情報提供内容を画面から入力する。1 件ごとの作成、複数件の作成を可能とする。情報照会電文中に回答項目として指定されたものだけを回答するように制御する。
2.		情報提供ファイル登録	情報提供内容を媒体から登録（アップロード）する。
3.		既存システムファイル連携	情報提供内容ファイルを既存システムから連携する。
4.	表示	情報提供内容表示	入力・登録した情報提供内容を画面に表示する。
5.	送信準備・送信	情報提供内容抽出	情報提供 DB から情報提供対象となるデータを抽出する。
6.		情報提供電文作成（暗号化）	情報提供内容から情報提供電文を作成する。この際、問い合わせ結果については暗号化を行う。
7.		情報提供電文送信	データ送受信機能を用いて情報提供電文を送信する。
8.		情報提供受領通知受信	データ送受信機能を用いて情報提供受領通知を受信する。
9.		情報提供記録送信	インターフェイスシステムを経由してコアシステムに情報提供記録を送信する。
10.	自動応答		情報照会を受けて、該当する情報を自動で提供する。詳細は情報提供の処理フローを参照のこと。

③ 情報提供内容抽出機能の補足

データ標準（データレイアウト）、中間サーバーに保有する特定個人情報、情報提供電文のイメージを以下に示す。

①データレイアウト(特定個人情報別／事務別データ項目対応欄付)イメージ

・情報提供者側が用意するデータセットを作成する際に利用するデータレイアウト

医療保険給付関係情報		〇〇に関する事務		△△に関する事務		□□に関する事務	
データ項目	データ属性	厚労省	都道府県	市町村	健保組合	...	...
AAA	XXXXX	○		○			
BBB	YYYYY	○				○	
CCC	ZZZZZ	○		○		○	
...	...			○			

情報提供DB
更新機能

②中間サーバーに蓄積するデータ(DB)イメージ

宛名-符号紐付テーブル

宛名番号	符号
0001	
0002	
...	

情報提供用DB

〇〇年度	医療保険給付関係情報				...	XX情報
宛名番号	AAA	BBB	...			
0001						
0002						
...						
XX年度						

情報提供内容
抽出機能

③情報提供電文イメージ

ヘッダ情報	
000Xの符号	
提供データの更新年月日	
〇〇に関する事務	
厚労省	××県
AAAの値	
BBBの値	
...	

図 15 データ標準、中間サーバーに保有する特定個人情報、情報提供電文のイメージ

情報提供内容抽出機能は、上図の②から③を作成する。

情報提供内容抽出機能とは、情報提供の対象となる事務に応じて、情報提供 DB から、必要な特定個人情報の項目を抽出して、情報提供電文を作成する機能である。

情報提供内容抽出機能の概念図について、以下に示す。図は、事務が異なる場合、抽出対象となる特定個人情報の項目が異なることを示している。

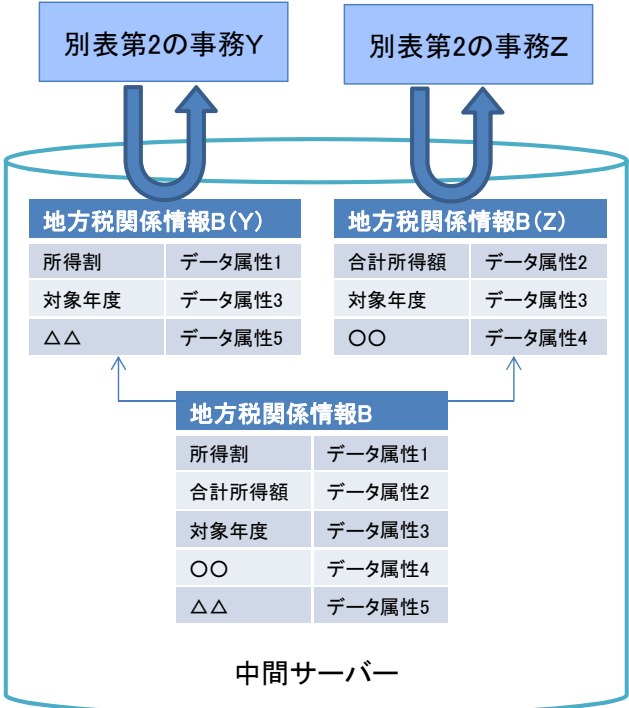


図 16 情報提供内容抽出の概念図

④ 情報提供側状況管理

情報提供側機能（情報提供側状況管理）の機能要件について、以下に示す。

表 32 情報提供側機能（情報提供側状況管理）の機能要件

#	機能中分類	機能小分類	概要
1.	情報提供側状況管理	情報提供側状況表示	以下の状況を一覧で表示する。 ・他情報保有機関からの情報照会電文の送信元（情報保有機関）、事務名、宛名番号、処理通番、受信状況（ステータス）、ステータスの更新日時 ・送信した情報提供電文の送信状況（ステータス）、ステータス更新日時、情報提供の状況（該当データの有無等） 情報照会と情報提供は、処理通番にて、対として状況を管理できること。 一覧から権限者が、電文の内容を確認できること。
2.		情報提供側状況連携	上記の内容について、PULL 型 Web サービスを通じて既存システムに連携する。

(3) 情報提供送受信ステータス

情報提供の送受信ステータスを以下に示す。

情報提供に際しては、以下のステータスを管理・表示できること。

なお、内部的に管理するステータスのすべてを画面に表示するか否かについては、設計時に検討するものとする。

表 33 情報提供送受信ステータス

#	分類	ステータス（正常系）	ステータス（異常系）
1.	情報照会（受信）	情報照会電文受信済み	情報提供許可証チェック失敗 符号→宛名番号変換失敗 情報照会電文展開失敗
2.		情報照会受付完了送信済み	情報照会受付完了送信失敗
3.	情報提供（送信）	情報提供電文作成済み	情報提供電文作成失敗
4.		情報提供電文送信済み	情報提供電文送信失敗
5.		情報提供受領通知受信済み	情報提供受領通知受信タイムアウト
6.		情報提供記録送信済み	情報提供記録送信失敗

(4) 情報提供の処理フロー

情報提供においては、情報提供側が「意図的に情報提供しない特定個人情報」について、情報提供 DB 上にフラグを設け、当該特定個人情報の提供は、自動応答せず、職員が対応する。

また、情報提供の決裁について、情報提供 DB の特定個人情報の単位で決裁区分を持つことにより、決裁済のものだけ情報提供することを可能とする。これらを加味した、情報提供のフローについて、以下に示す。

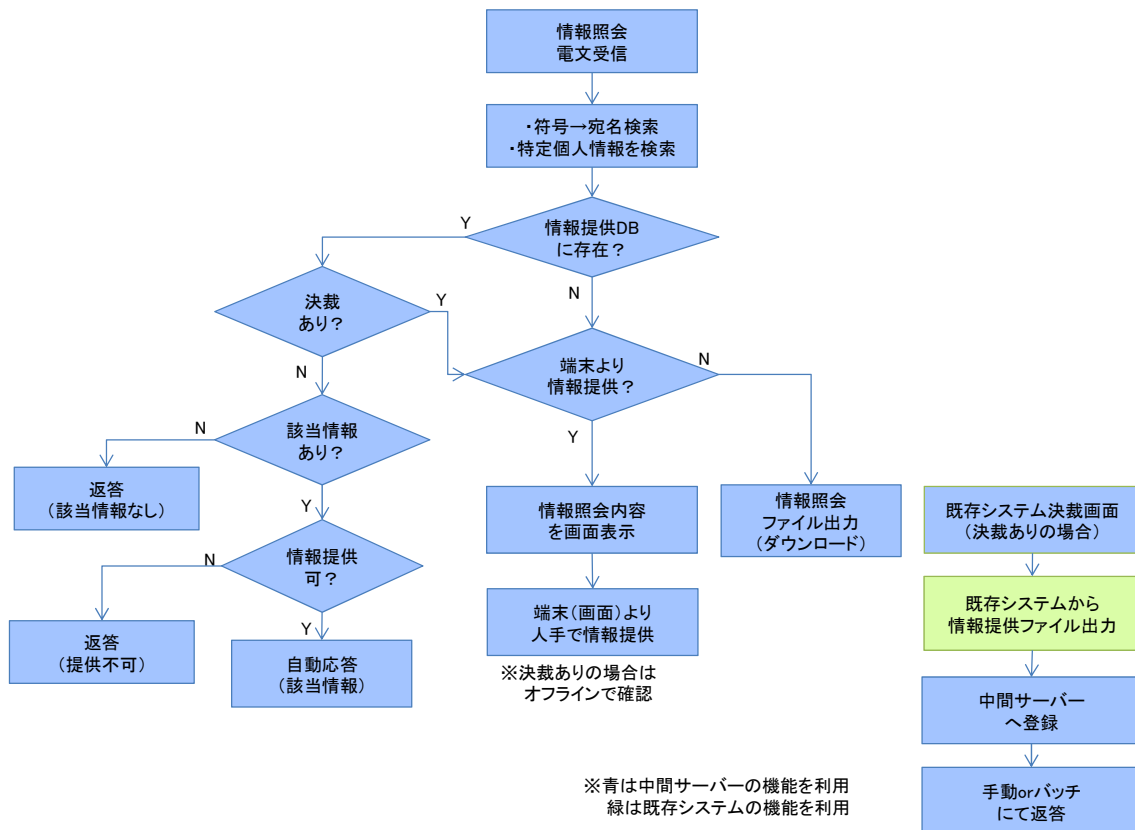


図 17 情報提供の処理フロー

情報提供時の状況に関するステータス一覧の案について、以下に示す。

表 34 情報提供時の状況一覧

#	ステータス	備考
1.	該当者なし	情報照会対象者の「符号→宛名変換」が失敗。 該当者なし。
2.	該当者はあるが該当データなし	情報照会対象者の「符号→宛名変換」が成功。 該当データなし。
3.	該当者があるが一部データのみ該当	情報照会対象者の「符号→宛名変換」が成功。 要求された特定個人情報の項目のうち一部の項目 のデータのみが該当。
4.	該当者があり、全データが該当	情報照会対象の該当者があり、全データが該当。
5.	情報提供要確認	情報保有機関が意図的に情報提供を要確認と判断 したもの。

なお、端末認証や、画面表示やファイル出力のアクセス制御については、別途、検討することとする。

6.5 既存システム接続機能

(1) 前提条件

既存システム連携のパターンとして以下を想定し、既存システムと連携する機能を提供する。

表 35 既存システム連携のパターン

役割	#	既存システムからの要求	既存システムからの要求方向	連携方法 (Web サービス)
情報照会側	1	(送信用) 情報照会内容の登録	PUSH	File／即時連携
	2	(受信済) 情報提供内容の取得	PULL	File／即時連携
	3	情報照会側状況（一覧）の取得	PULL	File
情報提供側	4	(受信済) 情報照会内容の取得	PULL	File
	5	(送信用) 情報提供内容の登録	PUSH	File
	6	情報提供側状況（一覧）の取得	PULL	File
	7	情報提供 DB 更新データの登録	PUSH	File
—	8	プレフィックス情報の取得	PULL	File

なお、既存システムは、中間サーバーより可用性が劣る可能性及びセキュリティを考慮し、上記では、中間サーバーから既存システムへのデータの PUSH は、想定していない。

各要求メッセージの共通のヘッダ部で保有する項目について、以下に示す。

表 36 共通のヘッダ部で保有する項目

#	項目名	概要
1.	リクエストコード	既存システムから中間サーバーへのサービス要求の種類を一意に規定するコード。
2.	既存システム連携処理通番 (中間サーバー)	既存システムから中間サーバーへのサービス要求の受付ごとに、中間サーバーが一意に採番する番号。中間サーバーが情報提供ネットワークシステムとやりとりする処理通番とは異なる。
3.	既存システム連携処理通番 (既存システム)	即時連携の際、既存システム側で、要求ごとに一意に採番する番号。

各要求メッセージのボディ部で保有する項目について、以下に示す。

【情報照会側のメッセージ】

①（送信用）情報照会内容の登録

(a) 要求メッセージボディ(複数件の場合あり)：

要求メッセージボディについて、以下に示す。

表 37 （送信用）情報照会内容の登録（要求メッセージボディ）

#	項目名	概要
1.	送信先機関コード	情報保有機関ごとに振られるコード。情報提供機関コード。
2.	事務コード	番号法案別表第2の事務コード。
3.	宛名番号	情報照会の対象者の宛名番号
4.	特定個人情報名コードのリスト	番号法案別表第2の特定個人情報名コードと特定個人情報の項目コードのセット。コードが複数格納される場合もある。
5.	特定個人情報の項目コードのリスト	番号法案別表第2の特定個人情報名ごとに回答を要求する特定個人情報の項目コードのリスト。コードが複数格納される場合もある。
6.	問い合わせ条件	問合せ対象データの範囲（年度又は基準年月日（自～至）） ※以下、例： 年度を指定する場合： ＜対象年度＞H24＜/対象年度＞ 基準年月日を指定する場合： ＜基準年月日＞H241201＜/基準年月日＞ 基準年月日の自～至を指定する場合： ＜基準年月日自＞H241201＜/基準年月日自＞ ＜基準年月日至＞H250331＜/基準年月日至＞
7.	既存システム連携処理通番	情報照会時に設定したもの。

(b) 返信メッセージボディ：

返信メッセージボディについて、以下に示す。

表 38 (送信用) 情報照会内容の登録 (返信メッセージボディ)

#	項目名	概要
1.	成功/エラー	エラーの場合はエラーコード。

② (受信済) 情報提供内容の取得

(a) 要求メッセージボディ:

要求メッセージボディについて、以下に示す。

表 39 (受信済) 情報提供内容の取得 (要求メッセージボディ)

#	項目名	概要
1.	既存システム連携処理通番	情報照会時に設定したもの。

(b) 返信メッセージボディ(複数件の場合あり):

返信メッセージボディについて、以下に示す。

表 40 (受信済) 情報提供内容の取得 (返信メッセージボディ)

#	項目名	概要
1.	情報提供機関コード	情報保有機関ごとに振られるコード。
2.	事務コード	番号法案別表第 2 の事務コード。
3.	宛名番号	情報照会の対象者の宛名番号。 中間サーバーにて情報照会時の符号を元にセット。
4.	特定個人情報名コードのリスト	番号法案別表第 2 の特定個人情報名コードと特定個人情報の項目コードのセット。コードが複数格納される場合もある。
5.	特定個人情報の項目コードのリスト	番号法案別表第 2 の特定個人情報名ごとに回答を要求する特定個人情報の項目コードのリスト。コードが複数格納される場合もある。
6.	処理通番	情報照会ごとに採番される通番。
7.	問い合わせ結果	対象データの更新日時、照会結果等。

③ 情報照会側状況(一覧)の取得

(a) 要求メッセージボディ: なし

要求メッセージボディは存在しない。

(b) 返信メッセージボディ(複数件の場合あり):

返信メッセージボディについて、以下に示す。

表 41 情報照会側状況（一覧）の取得（返値メッセージボディ）

#	項目名	概要
1.	更新時刻	
2.	送信した情報照会電文の宛先	
3.	処理通番	情報照会ごとに採番される通番。
4.	事務コード	番号法案別表第2の事務コード。
5.	プレフィックス情報照合結果	
6.	送信時刻	
7.	受付完了時刻	
8.	他情報保有機関から受信した 情報提供電文の受信時刻	
9.	受領通知送信時刻	
10.	情報提供記録送信時刻	

【情報提供側のメッセージ】

④（受信済）情報照会内容の取得

(a) 要求メッセージボディ:なし

要求メッセージボディは存在しない。

(b) 返信メッセージボディ(複数件の場合あり):

返信メッセージボディについて、以下に示す。

表 42 （受信済）情報照会内容の取得（返信メッセージボディ）

#	項目名	概要
1.	送信元機関名	中間サーバーにてコードから名前に変換することを想定。
2.	事務コード	番号法案別表第2の事務コード。
3.	宛名番号	情報照会の対象者の宛名番号。 中間サーバーにて符号から宛名番号に変換。
4.	特定個人情報名コードのリスト	番号法案別表第2の特定個人情報名コードと特定個人情報の項目コードのセット。コードが複数格納される場合もある。
5.	特定個人情報の項目コードのリスト	番号法案別表第2の特定個人情報名ごとに回答を要求する特定個人情報の項目コードのリスト。コードが複数格納される場合もある。
6.	問い合わせ条件	問合せ対象データの範囲（年度又は基準年月日（自～至）） ※以下、例： 年度を指定する場合： ＜対象年度＞H24＜/対象年度＞ 基準年月日を指定する場合： ＜基準年月日＞H241201＜/基準年月日＞ 基準年月日の自～至を指定する場合： ＜基準年月日自＞H241201＜/基準年月日自＞ ＜基準年月日至＞H250331＜/基準年月日至＞
7.	処理通番	情報照会ごとに採番される通番。

⑤（送信用）情報提供内容の登録

(a) 要求メッセージボディ(複数件の場合あり):

要求メッセージボディについて、以下に示す。

表 43 (送信用) 情報提供内容の登録 (要求メッセージボディ)

#	項目名	概要
1.	送信先機関コード	情報保有機関ごとに振られるコード。情報照会機関コード。
2.	事務コード	番号法案別表第 2 の事務コード。
3.	宛名番号	情報照会の対象者の宛名番号。 中間サーバーにて情報照会時の処理通番に変換。
4.	特定個人情報名コードのリスト	番号法案別表第 2 の特定個人情報名コードと特定個人情報の項目コードのセット。コードが複数格納される場合もある。
5.	特定個人情報の項目コードのリスト	番号法案別表第 2 の特定個人情報名ごとに回答を要求する特定個人情報の項目コードのリスト。コードが複数格納される場合もある。
6.	問い合わせ結果	対象データの更新日時、照会結果等。
7.	処理通番	情報照会ごとに採番される通番。

(b) 返値メッセージボディ:

返値メッセージボディについて、以下に示す。

表 44 (送信用) 情報提供内容の登録 (返値メッセージボディ)

#	項目名	概要
1.	成功/エラー	エラーの場合はエラーコード。

⑥ 情報提供側状況(一覧)の取得

(a) 要求メッセージボディ:なし

要求メッセージボディは存在しない。

(b) 返値メッセージボディ(複数件の場合あり):

返値メッセージボディについて、以下に示す。

表 45 情報提供側状況(一覧)の取得 (返値メッセージボディ)

#	項目名	概要
1.	他情報保有機関から受信した 情報照会電文の送信元	
2.	受信時刻	
3.	処理通番	情報照会ごとに採番される通番。
4.	事務コード	番号法案別表第 2 の事務コード。

#	項目名	概要
5.	受領通知送信時刻	
6.	他情報保有機関へ送信した情報提供電文の送信時刻	
7.	受領通知送信時刻	
8.	情報提供記録送信時刻	

⑦ 情報提供 DB 更新データの登録

(a) 要求メッセージボディ:

要求メッセージボディについて、以下に示す。

表 46 情報提供 DB 更新データの登録（要求メッセージボディ）

#	項目名	概要
1.	更新対象コード	情報提供 DB のテーブル名等。
2.	更新内容	複数件を想定。

(b) 返値メッセージボディ:

返値メッセージボディについて、以下に示す。

表 47 情報提供 DB 更新データの登録（返値メッセージボディ）

#	項目名	概要
1.	成功／エラー	エラーの場合はエラーコード。

【その他のメッセージ】

⑧ プレフィックス情報の取得

(a) 要求メッセージボディ:なし

要求メッセージボディは存在しない。

(b) 返値メッセージボディ:

返値メッセージボディについて、以下に示す。

表 48 プレフィックス情報の取得（返値メッセージボディ）

#	項目名	概要
1.	プレフィックス情報	
2.	取得時刻	

(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 49 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	機能概要
1.	Web サービス連携	PUSH 型サービス受付	既存システムからの PUSH 型の Web サービスリクエストを受け付け、実行する。 受け付けたデータの形式チェックを行い、エラーであった場合はその旨を要求元に返すこと。
2.		PULL 型サービス受付	既存システムからの PULL 型の Web サービスリクエストを受け付け、実行する。 受け付けたデータの形式チェックを行い、エラーであった場合はその旨を要求元に返すこと。
3.		連携制御	上記における連携制御を行う。 具体的には、認証機能と連携したサービスリクエストの認証、サービスの真正性チェック、エラー時のリカバリ等を行う。

① 連携制御機能の詳細

既存システムとの連携において、一連の処理と整合しない要求を受信した場合、連携相手方に理由を付してエラーを返すこと。

連携相手から所定の時間内に期待する応答がない場合、予め規定した回数だけ連携のリトライを実施すること。リトライによっても応答が得られない場合や相手方からシステム停止中の旨を受信した場合は、適切な手続きによりクローズできること。

既存システムから中間サーバーの稼働状況を把握できること。

稼働状況には以下の状態を含む。

- ・ 起動
- ・ 停止

6.6 情報提供記録管理機能

情報提供記録管理機能の想定概要について、以下に示す。

(1) 前提条件

番号法案では、情報提供記録について、以下のように記載されている。

【法案】

(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。(後略)

上記の記載を整理した結果について、以下に示す。

表 50 情報提供記録のタイミング、場所、記録項目

記録する主体	記録するタイミング	記録する場所	記録する項目
情報照会者及び 情報提供者	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及び提供があったとき	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	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 四 前三号に掲げる もののほか、総務省令 で定める事項
総務大臣	同上	情報提供ネットワークシステム	同上

(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 51 情報提供記録管理機能の概要

#	機能中分類	機能概要
1.	情報提供記録生成	データ送受信機能における送信、受信から情報提供記録を生成し、保存する。
2.	情報提供記録検索	保有している情報提供記録を検索・抽出する。
3.	情報提供記録ファイル出力	保有している情報提供記録を媒体等へ出力する。 ※情報提供記録の記憶容量を確保するため、媒体等への出力後は削除する運用を想定する。
4.	情報提供記録削除	保有している情報提供記録を削除する。 ※情報提供記録の記憶容量を確保するため、媒体等への出力後は削除する運用を想定する。
5.	情報提供記録電文の作成	情報提供記録電文を作成する。

中間サーバーにおける情報提供記録の項目に関する案について、以下に示す。

表 52 情報提供記録の項目

記録する項目	番号法案
処理通番	
符号	
提供の求めの日時	○
提供があったときの日時	○
情報照会者	○
情報提供者	○
特定個人情報の項目	○
事務	

また、ログの暗号化については、暗号化に伴うリスク（漏洩、改ざん、原本としての価値の損失等）も踏まえ、検討する必要がある。

6.7 情報提供 DB 管理機能

(1) 前提条件

① 情報提供 DB

中間サーバーに構築する、番号法案別表第2に規定される情報提供のための特定個人情報の複製を格納したデータベースを情報提供 DB と呼ぶ。

中間サーバーにおいては、データ標準に基づく標準的な情報提供 DB を構築する。情報提供 DB の仕様は中間サーバーの設計段階において策定し、情報保有機関に向けて公開するものとする。

当該仕様は、情報提供 DB のスキーマ、情報提供 DB の更新（時期、方法等）にかかるガイドライン、情報提供 DB 更新のための具体的なインターフェイス仕様を含む想定とする。詳細は、中間サーバー構築に係る調達仕様書作成又は設計書作成時に検討する。

② 情報提供 DB の更新

情報提供 DB を更新する方法について、以下に示す。下図のうち、赤線で示した範囲（既存システムのデータを抽出し、情報提供 DB が扱う標準形式のデータ変換（コード・フォーマット変換）し、PUSH 型 Web サービスでデータを提供する機能）については、既存システム側で実現するものとする。ただし、データ変換の機能のうち、中間サーバーで保有することが効率的な機能がある場合には、中間サーバーに設けることもありうる。

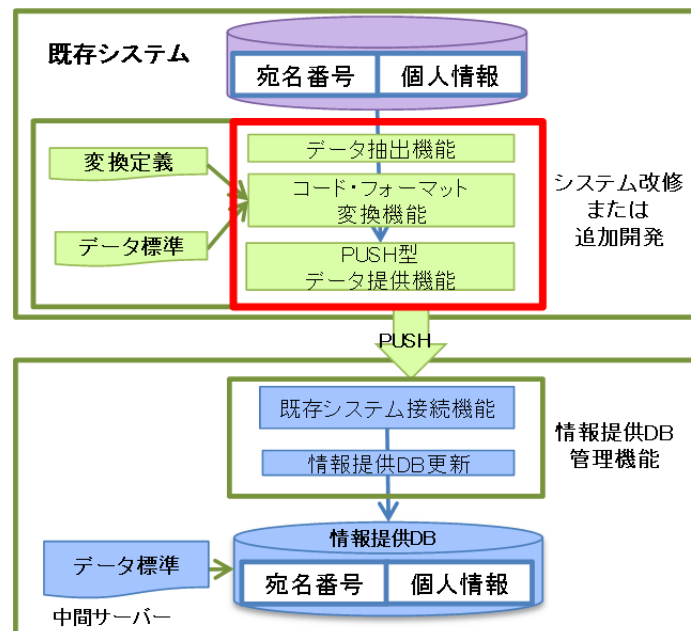


図 18 情報提供 DB 更新の概要

変換定義とは、既存システムのデータから標準形式のデータへ変換方法の定義であり、コードやフォーマット変換の具体的な方法について記述したものである。既存システム側から標準形式に変換したデータを、PUSH 型データ提供機能にて、中間サーバーに送付し、情報提供 DB を更新する。

(2) 機能要件

情報提供 DB 管理機能の機能要件について、以下に示す。

中間サーバーにおける機能要件について、以下に示す。

表 53 情報提供 DB 管理機能の機能要件（中間サーバー）

#	機能中分類	機能概要
1.	情報提供 DB 更新（一括）	認証を行った上で、標準形式のデータを用いて、バッチ等で複数件を一括で情報提供 DB を更新する。 導入時及び年次データの大量データの更新を想定し、PUSH 型 Web サービス以外の方法（オフライン・媒体経由による大量データの一括更新等）を想定する。 なお、登録時にエラーが生じた場合は、ログに出力すること。
2.	情報提供 DB 更新（都度）	認証を行った上で、標準形式のデータを用いて、PUSH 型 Web サービスにてオンラインで都度、情報提供 DB を更新する。 既存システム連携／PUSH 型サービス受付の利用を想定する。
3.	保存期限切れデータ削除機能	保存期間を過ぎたデータを削除する機能。

既存システム側が用意する想定機能要件について、以下に示す。

表 54 情報提供 DB 管理機能の機能要件（既存システム）

#	機能中分類	機能概要
1.	データ抽出機能	既存システムが保有するデータのうち、データ標準を参照し、提供情報に該当するものを抽出する。 抽出データは予め定めた範囲とする。
2.	コード・フォーマット変換	既存システムのデータについて、データ標準及び変換定義に基づき、以下の変換を実施し、標準形式のデータへ変換する。 ・文字コードの変換（例：SJIS→UTF） ・フォーマット変換（変換定義に基づき、既存システムのデータ項目を標準形式のデータ項目へ変換）

#	機能中分類	機能概要
		・コードの変換や0 (ゼロ) ・NULL ・マイナス等に特別な意味がある場合の変換（変換定義に基づき、各データ項目の値を標準形式に変換）
3.	PUSH 型データ提供機能	上記のデータを既存システムから中間サーバーへ PUSH する。

6.8 データ送受信機能

データ送受信機能の想定概要について、以下に示す。

(1) 前提条件

データ送受信機能に係る送受信データ標準及びプロトコル標準等の前提条件については、「技術標準の検討に係る報告書」にて検討を実施しているため、当該報告書を参照のこと。また、インターフェイスシステムの要件については、「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」にて検討を実施しているため、当該報告書を参照のこと。

(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 55 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.	送付先管理	—	送付可能な情報保有機関の宛先を管理する。
2.	通信制御	—	インターフェイスシステムとの通信における制御を行う。詳細は後述。
3.	送信	ヘッダチェック	送信電文のヘッダが所定のものであるかチェックを行い、エラーの場合は、その旨を呼出した機能に返す。
4.		ボディチェック	送信電文のボディが所定のものであるかチェックを行い、エラーの場合は、その旨を呼出した機能に返す。
5.		送信・記録	インターフェイスシステムに電文を送信し、送信記録を出力する。
6.	受信	受信・記録	インターフェイスシステムから電文を受信し、送信記録を出力する。
7.		ヘッダチェック	受信電文のヘッダが所定のものであるかチェックを行い、エラーの場合は、その旨を呼出した機能に返す。
8.		ボディチェック	受信電文のボディが所定のものであるかチェックを行い、エラーの場合は、その旨を呼出した機能に返す。

① 通信制御機能の詳細

インターフェイスシステムとの通信において、一連の処理と整合しない電文を受信した場合、通信相手方に理由を付してエラーを返すこと。

通信相手から所定の時間内に期待する応答がない場合、予め規定した回数だけ通信のリトライを実施すること。リトライによっても応答が得られない場合や相手方からシステム停止中の旨を受信した場合は、適切な手続きによりクローズできること。

中間サーバーの稼働状況をインターフェイスシステムに通知できること。

稼働状況には以下の状態を含む。

- ・ 起動
- ・ 停止

6.9 セキュリティ管理機能

セキュリティ管理機能の想定概要について、以下に示す。

(1) 前提条件

① 暗号化の場所

中間サーバーにおいて暗号化／復号を行う。

② 暗号化の対象

情報提供電文のボディ部に対して暗号化を行う。

③ 暗号化方式

公開鍵又はハイブリッド暗号方式とする。

④ 鍵管理

自らの暗号化鍵を中間サーバー自身で管理する。

(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 56 セキュリティ管理機能の機能要件

#	機能名	概要
1.	暗号化	情報提供電文について、送信電文のボディ部分を受け取った暗号化鍵で暗号化する。
2.	復号	情報提供電文について、受信電文のボディ部分を自らの暗号化鍵で復号する。
3.	鍵管理	自らの暗号化鍵を生成し、中間サーバー上に保持する。保持する暗号化鍵については、第三者に容易に窃取されることのないよう、必要なセキュリティ対策を施す。
4.	プレフィックス情報取得	※情報提供ネットワークシステムからプレフィックス情報を取得。
5.	プレフィックス情報配信	※既存システムへプレフィックス情報を配信。

6.10 職員認証・権限管理機能

(1) 前提条件

① 中間サーバーの認証の考え方

中間サーバーのアクセス制御の考え方について以下に示す。

表 57 中間サーバーのアクセス制御

#	認証ポイント	内容
1.	端末へのログイン	番号法案に基づき、(中間サーバーに接続された) 端末にログインできる職員を設定する。IC カード、ID、パスワード等によりログインする職員を認証する。
2.	端末から中間サーバーへのログイン(中間サーバー上のアクセス制御)	番号法案に基づき、職員の所属等により、ログイン後にアクセスできる画面及びデータを制限する。 この制御は、事務又は特定個人情報の項目単位のアクセス制御であり、端末へのログインより細かい制御を想定する。
3.	既存システム連携	既存システムと中間サーバーを連携する場合は、サーバー間で認証を実施する。

② 利用端末

中間サーバーの機能を用いて、又は既存システムと中間サーバーを連携して、情報照会や情報提供を行うための端末の種類と特徴について、以下に示す。

当該情報保有機関の状況に応じて、いずれかを選択又は組み合わせて利用することを想定する。いずれも、コアシステムから配信されるプレフィックス情報を踏まえ、当該情報保有機関の組織と担当者（ログイン者）を適切に管理し、アクセス制御することを前提とする。

表 58 利用端末の種類

端末の種類	説明
中間サーバー専用 端末	中間サーバーの操作に特化した専用の端末。 中間サーバーの機能にて、情報照会・情報提供する際に利用する。
職員端末 (情報系端末)	庁内 LAN 等に接続され、職員の IC カード等で認証される情報系端末で、ネットワーク環境及び設定によるが、中間サーバーのみならず、他のシステムも利用可能。
既存システム端末 (業務系端末)	既存システムの業務系端末。 既存システムから中間サーバーへ即時連携して、情報照会・情報提供する際に利用する。この場合は、既存システム端末から直接中間サーバーへの接続ではなく、既存システムと中間サーバーのサーバー間連携により間接的に中間サーバーを利用する形となる。

上記を踏まえ、中間サーバーの利用端末について、以下のパターンを想定する。いずれのパターンにおいても、中間サーバーに係る認証機能は、必要があると考えられる（その上で、既存システムの職員認証基盤と中間サーバーの連携や役割分担について検討する必要がある）。

- 1) 中間サーバー専用端末からのみ利用可能とする
- 2) 情報系端末から利用可能とする
- 3) 業務系端末から利用可能とする

また、情報提供ネットワークシステムへの接続権限の判定や、端末操作ログの取得管理等について、既存システムと中間サーバーのいずれで実施するか、役割分担を別途検討する必要がある（端末操作ログの取得管理は、必要となるログの内容や取得方法等が情報提供ネットワークシステム側に依存することから、中間サーバーで実施することが望ましいと考えられる）。

(2) 機能要件

職員認証・権限管理機能の機能要件について、以下に示す。

中間サーバーに専用端末を接続することを想定すると、中間サーバー上に、職員認証・職員権限管理等の機能が必要となる。当該サービスを実現する機能として、以下を想定する。

表 59 職員認証・権限管理機能の機能要件

#	機能中分類	機能小分類	機能概要
1.	職員認証	—	職員が端末から中間サーバーへのログインする際の認証を実現する。プレフィックス情報に従ったアクセス制御が可能なこと。 ログイン／ログアウトの職員に係る情報、時刻、操作内容等について記録できること。
2.	職員認証連携	—	既存システムと中間サーバー間で、既存システムで認証された認証情報を連携し、シングルサインオンを実現する。 中間サーバーは、上記の際の認証情報を受け取り、認証連携を実現できること。

#	機能中分類	機能小分類	機能概要
3.	職員権限管理	—	中間サーバーへログインする職員のアクセス権の管理（登録・更新・削除等）を実現する。 操作対象職員とプレフィックス情報の関連づけが行えること。 中間サーバーで定める標準形式にて、既存の職員情報をインポートして設定することもできること。

6.11 システム管理機能

(1) 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。

システム管理要件は、非機能要件及び SLA (Service Level Agreement) により詳細に規定されるものであり、また、アプリケーションの機能ではなくエージェント／サーバー型の運用監視ソフトの導入等も想定されるため、中間サーバー構築に係る調達仕様書作成時に検討する。

表 60 システム管理機能の機能要件

#	機能中分類	機能小分類	機能概要
1.	時刻同期	—	NTP サーバーと連携し、サーバーの時刻同期を行う。
2.	ジョブ管理	—	ジョブスケジューリング等のバッチジョブの管理を行う。
3.	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を行う。
4.	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。

7. 画面要件

本章では、機能要件から想定される画面要件について述べる。

7.1 画面一覧

中間サーバーの機能要件から想定される画面要件について、以下に示す。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除いている。画面構成を含む詳細要件は、調達仕様書作成又は設計書作成において検討する。

表 61 画面一覧

#	機能大分類	機能中分類	画面名	利用者
1.	符号管理	符号の取得・紐付	符号取得用ファイル出力画面	職員／管理者
2.		符号—宛名紐付管理	符号—宛名紐付管理画面	職員／管理者
3.	情報照会側	入力・登録	情報照会内容入力画面	職員
4.	情報照会		情報照会ファイル登録画面	職員／管理者
5.		表示・出力	情報照会内容表示画面	職員
6.			情報照会内容 PDF 出力画面	職員
7.		送信準備・送信	情報照会電文送信画面	職員
8.	情報照会側 情報提供受領 情報照会側状況管理	受信・展開、情報照会側状況管理	情報照会側状況表示画面	職員
9.	情報照会側	表示・出力	情報提供内容表示画面	職員
10.	情報提供受領		情報提供ファイル出力画面	職員
11.			情報提供 PDF 出力画面	職員
12.	情報提供側 情報照会受領 情報提供 情報提供側状況管理	受信・展開、送信準備・送信、自動応答、情報提供側状況管理	情報提供側状況表示画面	職員
13.	情報提供側	表示・出力	情報照会内容表示画面	職員
14.	情報照会受領		情報照会ファイル出力画面	職員
15.			情報照会 PDF 出力画面	職員
16.	情報提供側	入力・登録	情報提供内容入力画面	職員

#	機能大分類	機能中分類	画面名	利用者
17.	情報提供		情報提供ファイル登録画面	職員／管理者
18.		表示	情報提供内容表示画面	職員
19.	情報提供記録管理	情報提供記録検索	情報提供記録表示画面	職員／管理者
20.	データ送受信	送付先管理	送付先管理画面	管理者
21.	職員認証・権限管理	職員権限管理	職員権限設定画面	管理者

上記のうち、利用者が「職員」となっている画面については、職員認証機能によりログイン後、プレフィックス情報等を参照し、適切な権限のある者のみが操作できるよう制御を行う。

7.2 画面定義

(1) 画面要件(符号管理)

符号取得用ファイル出力画面の画面要件について、以下に示す。

表 62 符号取得用ファイル出力画面

画面 ID	1.
機能名	符号管理／符号の取得・紐付
画面名	符号取得用ファイル出力画面
利用者	当該宛名情報の管理担当職員又は管理者
画面概要	
中間サーバー側で処理通番発行依頼電文を作成し、インターフェイスシステムから処理通番を取得し、「処理通番＋宛名番号」のセットをファイルに出力する。 ※既存システムとオンライン連携することもある。この場合は既存システムからの PULL 型 Web サービスとする。	

符号―宛名紐付管理画面の画面要件について、以下に示す。

表 63 符号―宛名紐付管理画面

画面 ID	2.
機能名	符号管理／符号―宛名紐付管理
画面名	符号―宛名紐付管理画面
利用者	当該宛名情報の管理担当職員又は管理者
画面概要	
符号と宛名番号の紐付テーブルのメンテナンスを行う。 検索範囲を指定して、符号から宛名番号の検索、宛名番号から符号の検索を実施し、符号又は宛名番号の更新・削除ができること。	

(2) 画面要件(情報照会側)

情報照会内容入力画面の画面要件について、以下に示す。

表 64 情報照会内容入力画面

画面 ID	3.
機能名	情報照会側／情報照会／入力・登録
画面名	情報照会内容入力画面
利用者	職員（当該事務の情報照会担当者）
画面概要	
情報照会内容を作成する画面。 以下の項目の入力が想定される。 ・送付先の情報保有機関 ・照会対象者（個人）の宛名番号 ・事務名、特定個人情報名（コード）、特定個人情報の項目（コード）の選択・指定 ・問い合わせ条件（検索条件及び回答項目） 1 件ごと及び複数件の入力が可能なこと。	

情報照会ファイル登録画面要件について、以下に示す。

表 65 情報照会ファイル登録画面

画面 ID	4.
機能名	情報照会側／情報照会／入力・登録
画面名	情報照会ファイル登録画面
利用者	職員（当該事務の情報照会担当者）又は管理者
画面概要	
情報照会ファイルを登録する画面。 以下の項目からなるファイルの登録が想定される。 ・送付先の情報保有機関 ・照会対象者（個人）の宛名番号 ・事務名、特定個人情報名（コード）、特定個人情報の項目（コード） ・問い合わせ条件（検索条件及び回答項目） 複数件の出力が可能なこと。	

情報照会内容表示画面の画面要件について、以下に示す。

表 66 情報照会内容表示画面

画面 ID	5.
機能名	情報照会側／情報照会／表示・出力
画面名	情報照会内容表示画面
利用者	職員（当該事務の情報照会担当者）
画面概要	
情報照会内容を表示する画面。 以下の項目の表示が想定される。 ・送付先の情報保有機関 ・照会対象者（個人）の宛名番号 ・事務名、特定個人情報名（コード）、特定個人情報の項目（コード） ・問い合わせ条件（検索条件及び回答項目） 1 件ごと及び複数件の表示が可能なこと。	

情報照会内容 PDF 出力画面の画面要件について、以下に示す。

表 67 情報照会内容 PDF 出力画面

画面 ID	6.
機能名	情報照会側／情報照会／表示・出力
画面名	情報照会内容 PDF 出力画面
利用者	職員（当該事務の情報照会担当者）
画面概要	
情報照会内容を PDF 出力する画面。 以下の項目の表示が想定される。 ・送付先の情報保有機関 ・照会対象者（個人）の宛名番号 ・事務名、特定個人情報名（コード）、特定個人情報の項目（コード） ・問い合わせ条件（検索条件及び回答項目） 1 件ごと及び複数件の出力が可能なこと。	

情報照会電文送信画面の画面要件について、以下に示す。

表 68 情報照会電文送信画面

画面 ID	7.
機能名	情報照会側／情報照会／送信準備・送信
画面名	情報照会電文送信画面
利用者	職員（当該事務の情報照会担当者）
画面概要	
「情報照会内容入力画面」で作成した内容に基づき、「情報照会電文作成機能」にて、情報照会電文を作成し、情報照会電文を送信するための画面。 送信状態を記録・表示する。	

情報照会側状況表示画面の画面要件について、以下に示す。

表 69 情報照会側状況表示画面

画面 ID	8.
機能名	情報照会側／情報提供受領、情報照会側状況管理／受信・展開、情報照会側状況管理
画面名	情報照会側状況表示画面
利用者	職員（当該事務の情報照会担当者）

画面概要

以下の状況を一覧で表示する。

- ・他情報保有機関へ送信した情報照会電文の宛先（情報保有機関名）、送信情報、送信状況
- ・他情報保有機関から受信した情報提供電文の受信状況

情報照会と情報提供は、処理通番にて対にして状況を管理できること。

一覧の一つを指定して、権限者が、情報照会又は情報提供電文の内容を確認できること。

情報照会の結果が受信できていない電文のみを選択して表示することもできること。

以下に画面イメージを示す。

情報照会(送信)							情報提供(受信)			
情報照会先		送信情報		送信状況		内容	受信状況			内容
機関名	事務名	宛名 番号	処理 通番	ステータス	日時		ステータス	日時	提供 状況	

情報提供内容表示画面の画面要件について、以下に示す。

表 70 情報提供内容表示画面

画面 ID	9.
機能名	情報照会側／情報提供受領／表示・出力
画面名	情報提供内容表示画面
利用者	職員（当該事務の情報照会担当者）
画面概要	
情報照会の返答として得られた情報提供の内容を表示する画面。 以下の項目の表示が想定される。 ・送付先の情報保有機関 ・照会対象者（個人）の宛名番号 ・事務名、特定個人情報名（コード）、特定個人情報の項目（コード） ・問い合わせ結果（特定個人情報） 1 件ごと及び複数件の表示が可能なこと。	

情報提供ファイル出力画面の画面要件について、以下に示す。

表 71 情報提供ファイル出力画面

画面 ID	10.
機能名	情報照会側／情報提供受領／表示・出力
画面名	情報提供ファイル出力画面
利用者	職員（当該事務の情報照会担当者）
画面概要	
情報照会の返答として得られた情報提供の内容をファイルに出力する画面。 以下の項目のファイルの出力が想定される。 ・送付先の情報保有機関 ・照会対象者（個人）の宛名番号 ・事務名、特定個人情報名（コード）、特定個人情報の項目（コード） ・問い合わせ結果（特定個人情報） 1 件ごと及び複数件の出力が可能なこと。	

情報提供 PDF 出力画面の画面要件について、以下に示す。

表 72 情報提供 PDF 出力画面

画面 ID	11.
機能名	情報照会側／情報提供受領／表示・出力
画面名	情報提供 PDF 出力画面
利用者	職員（当該事務の情報照会担当者）
画面概要	
情報照会の返答として得られた情報提供の内容を PDF 出力する画面。 以下の項目の PDF 出力が想定される。 ・送付先の情報保有機関 ・照会対象者（個人）の宛名番号 ・事務名、特定個人情報名（コード）、特定個人情報の項目（コード） ・問い合わせ結果（特定個人情報） ・メッセージ等 1 件ごと及び複数件の出力が可能なこと。	

(3) 画面要件(情報提供側)

情報提供側状況表示画面の画面要件について、以下に示す。

表 73 情報提供側状況表示画面

画面 ID	12.									
機能名	情報提供側／情報照会受領、情報提供、情報提供側状況管理／受信・展開、送信準備・送信、自動応答、情報提供側状況管理									
画面名	情報提供側状況表示画面									
利用者	職員（当該事務の情報提供担当者）									
画面概要										
以下の状況を一覧で表示する。										
・他情報保有機関から受信した情報照会電文の情報照会元（情報保有機関名）、受信情報、受信状況										
・他情報保有機関へ送信した情報提供電文の送信状況										
情報照会と情報提供は、処理通番にて、対にして状況を管理できること。										
一覧の一つを指定して、権限者が、情報照会又は情報提供電文の内容を確認できること。										
未回答の電文のみ等を選択して表示できること。										
以下に画面イメージを示す。										
情報照会(受信)							情報提供(送信)			
情報照会元		受信情報		受信状況		内容	送信状況			内容
機関名	事務名	宛名 番号	処理 通番	ステータス	日時		ステータス	日時	提供 状況	

情報照会内容表示画面の画面要件について、以下に示す。

表 74 情報照会内容表示画面

画面 ID	13.
機能名	情報提供側／情報照会受領／表示・出力
画面名	情報照会内容表示画面
利用者	職員（当該事務の情報提供担当者）
画面概要	
情報照会電文を受取った後、その内容を表示する画面。 以下の項目の表示が想定される。 ・送付先の情報保有機関 ・照会対象者（個人）の宛名番号 ・事務名、特定個人情報名（コード）、特定個人情報の項目（コード） 1 件ごと及び複数件の表示が可能なこと。	

情報照会ファイル出力画面の画面要件について、以下に示す。

表 75 情報照会ファイル出力画面

画面 ID	14.
機能名	情報提供側／情報照会受領／表示・出力
画面名	情報照会ファイル出力画面
利用者	職員（当該事務の情報提供担当者）
画面概要	
情報照会電文を受取った後、その内容をファイル出力する画面。 以下の項目のファイルの出力が想定される。 ・送付先の情報保有機関 ・照会対象者（個人）の宛名番号 ・事務名、特定個人情報名（コード）、特定個人情報の項目（コード） 1 件ごと及び複数件の出力が可能なこと。	

情報照会 PDF 出力画面の画面要件について、以下に示す。

表 76 情報照会 PDF 出力画面

画面 ID	15.
機能名	情報提供側／情報照会受領／表示・出力
画面名	情報照会 PDF 出力画面
利用者	職員（当該事務の情報提供担当者）
画面概要	
情報照会電文を受取った後、その内容を PDF 出力する画面。 以下の項目の PDF 出力が想定される。 ・送付先の情報保有機関 ・照会対象者（個人）の宛名番号 ・事務名、特定個人情報名（コード）、特定個人情報の項目（コード） 1 件ごと及び複数件の出力が可能なこと。	

情報提供内容入力画面の画面要件について、以下に示す。

表 77 情報提供内容入力画面

画面 ID	16.
機能名	情報提供側／情報提供／入力・登録
画面名	情報提供内容入力画面
利用者	職員（当該事務の情報提供担当者）
画面概要	
情報提供内容を作成する画面。 以下の項目の入力が想定される。 ・送付先の情報保有機関の選択・指定 ・提供対象者（個人）の宛名番号の指定 ・事務名、特定個人情報名（コード）、特定個人情報の項目（コード） ・問い合わせ結果（特定個人情報） ・メッセージ等 1 件ごと及び複数件の入力が可能なこと。	

情報提供ファイル登録画面の画面要件について、以下に示す。

表 78 情報提供ファイル登録画面

画面 ID	17.
機能名	情報提供側／情報提供／入力・登録
画面名	情報提供ファイル登録画面
利用者	職員（当該事務の情報提供担当者）又は管理者
画面概要	
情報提供ファイルを登録する画面。 以下の項目のファイルが想定される。 ・送付先の情報保有機関の選択・指定 ・提供対象者（個人）の宛名番号の指定 ・事務名、特定個人情報名（コード）、特定個人情報の項目（コード） ・問い合わせ結果（特定個人情報） 1 件ごと又は複数件の登録が可能なこと。	

情報提供内容表示画面の画面要件について、以下に示す。

表 79 情報提供内容表示画面

画面 ID	18.
機能名	情報提供側／情報提供／表示
画面名	情報提供内容表示画面
利用者	職員（当該事務の情報提供担当者）
画面概要	
情報提供内容を表示する画面。 以下の項目の表示が想定される。 ・送付先の情報保有機関 ・提供対象者（個人）の宛名番号 ・事務名、特定個人情報名（コード）、特定個人情報の項目（コード） ・問い合わせ結果（特定個人情報） 1 件ごと及び複数件の表示が可能なこと。	

(4) 画面要件(情報提供記録管理)

情報提供記録表示画面の画面要件について、以下に示す。

表 80 情報提供記録表示画面

画面 ID	19.
機能名	情報提供記録管理／情報提供記録検索
画面名	情報提供記録表示画面
利用者	職員又は管理者
画面概要	
情報提供記録を表示する画面。 検索・表示、(必要に応じて) ファイル出力等を行えるものとする。	

(5) 画面要件(送受信)

送付先管理画面の画面要件について、以下に示す。

表 81 送付先管理画面

画面 ID	20.
機能名	データ送受信／送付先管理
画面名	送付先管理画面
利用者	管理者、職員（当該事務の情報提供担当者）
画面概要	
送受信時の送付先機関を管理する画面。	

(6) 画面要件(職員認証・権限管理)

職員権限設定画面の画面要件について、以下に示す。

表 82 職員権限設定画面

画面 ID	21.
機能名	職員認証・権限管理／職員権限管理
画面名	職員権限設定画面
利用者	システム管理者
画面概要	
中間サーバーへログインする職員のアクセス権の管理（登録・更新・削除等）を実現する。 プレフィックス情報に従ったアクセス制御が可能なこと。 中間サーバーで定める標準形式にて、職員情報をインポートして設定することもできること。 権限は、職員の所属、職位等により実現するが、具体的な設定方法については、番号法案及び 関連する法令等の遵守を前提として、各情報保有機関で定めるものとする。	

8. データ要件

本章では、中間サーバーが管理する主要な情報について述べる。

なお、インターフェイスシステム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 中間サーバーで管理する情報（一覧）

中間サーバーで管理する情報（一覧）について、以下に示す。

表 83 中間サーバーで管理する情報（一覧）

#	情報名	概要
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.	符号—宛名番号紐付テーブル	符号—宛名番号を紐付したテーブル。
7.	情報提供記録	情報提供を実施した記録。
8.	アクセスログ	中間サーバー上の操作記録。
9.	情報提供 DB	情報提供のための既存システムの特定個人情報の複製。
10.	他機関からの提供情報	情報照会の結果として、他の情報保有機関から提供された情報

8.2 中間サーバーで管理する情報(詳細)

中間サーバーで管理する情報（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、今後予定される中間サーバー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 84 行政機関マスタ

#	項目名	Key	概要
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 85 情報提供事務マスタ

#	項目名	Key	概要
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 86 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 87 特定個人情報の項目マスタ

#	項目名	Key	概要
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

本情報の詳細は、情報提供ネットワークシステムにて別途定義される想定である。

(6) 符号―宛名番号紐付テーブル

符号―宛名番号紐付テーブルの詳細について、以下に示す。

表 88 符号―宛名番号紐付テーブル

#	項目名	Key	概要
1.	宛名番号	PK	符号に 1 : 1 で対応した情報保有機関独自の番号。
2.	符号		情報照会において個人を一意に識別するための情報。
3.	更新日		

(7) 情報提供記録

本情報の詳細は、「6.6 情報提供記録管理機能」の項を参照のこと。

(8) 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 89 アクセスログ

#	項目名	Key	概要
1.	連番	PK	
2.	操作時刻		
3.	操作端末		

#	項目名	Key	概要
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) 情報提供 DB

本情報の詳細は、今後予定される中間サーバー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。

なお、情報提供においては、情報提供側が「意図的に情報提供しない特定個人情報」について、情報提供 DB 上にフラグを設け、当該特定個人情報の提供は、自動応答せず、職員が対応することとする。

情報提供 DB の構成情報の検討に当たっては、各事務における項目の更新頻度の違い（随時更新か、年次更新か等）に留意する必要がある。

また、情報提供 DB は、中間サーバーの導入段階で構築することを想定する。この際、情報提供 DB の容量や割当サイズ等については、各情報保有機関の規模や特性に応じて設定するものとする。

以下に、データ標準及び提供情報 DB のイメージを示す。

医療保険給付関係情報		〇〇に関する事務		△△に関する事務		□□に関する事務	
データ項目	データ属性	厚労省	都道府県	市町村	健保組合	...	...
AAA	XXXXX	○		○			
BBB	YYYYY	○				○	
CCC	ZZZZZ	○		○		○	
...	...			○			

図 19 データ標準のイメージ図

医療保険給付関係情報					
宛名番号	AAA	BBB	...		
0001					
0002					
...					

図 20 提供情報 DB のイメージ図

(10) 他機関提供情報

情報照会の結果、他の情報保有機関から提供された情報について、以下に示す。

表 90 他機関提供情報

#	項目名	Key	概要
1.	連番	PK	
2.	取得日時		情報提供電文の取得日時。
3.	情報提供機関コード		情報提供機関のコード。
4.	事務コード		番号法案別表第 2 の事務コード。
5.	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。
6.	問い合わせ条件		情報照会電文中の問合せ条件。

8.3 情報提供 DB へのデータの記録年数

情報提供 DB に何年分のデータを保存するかについては、過年度分のデータ提供の必要性についての制度面での検討及びニーズを踏まえる必要がある。

9. 稼働環境

本章では、中間サーバー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。特定個人情報を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

中間サーバーの 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、中間サーバーは外部（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、中間サーバーを設置する構成がより望ましいと考えられる。

(1) 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

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について、以下に示す。

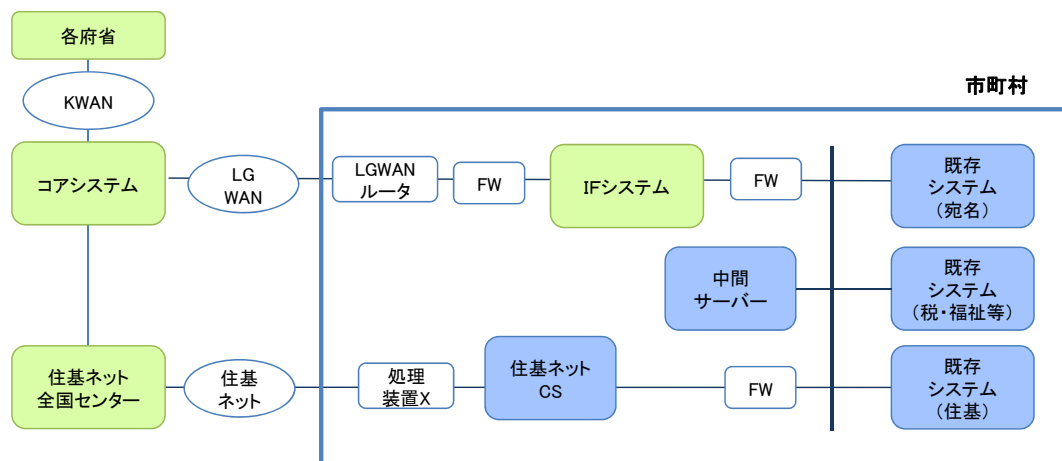


図 21 中間サーバーを既存システムと同じセグメントに置く構成

(2) 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

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について、以下に示す。

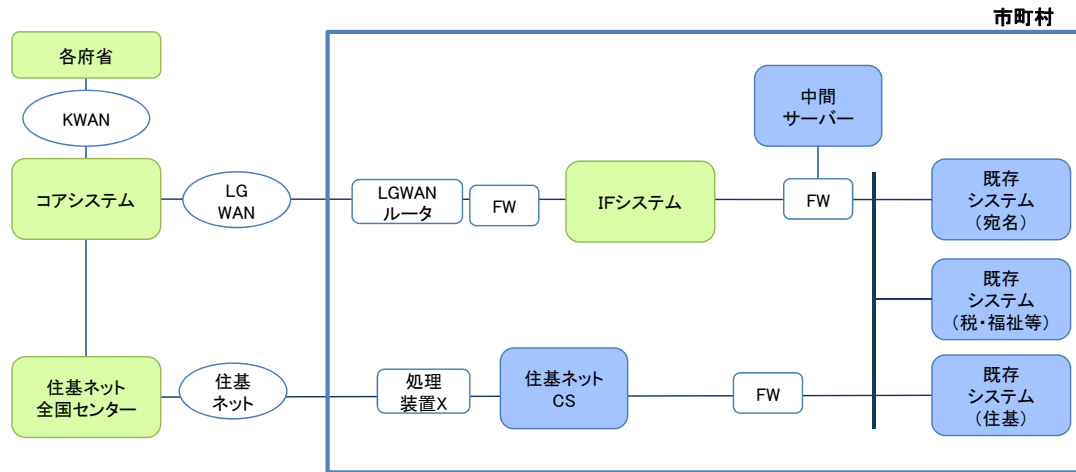


図 22 中間サーバーを既存システムと異なるセグメントに置く構成

(3) 基幹系 LAN 及び情報系 LAN の構成

中間サーバーの 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

中間サーバーのクラウドへの導入は、設置する情報保有機関における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 91 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。

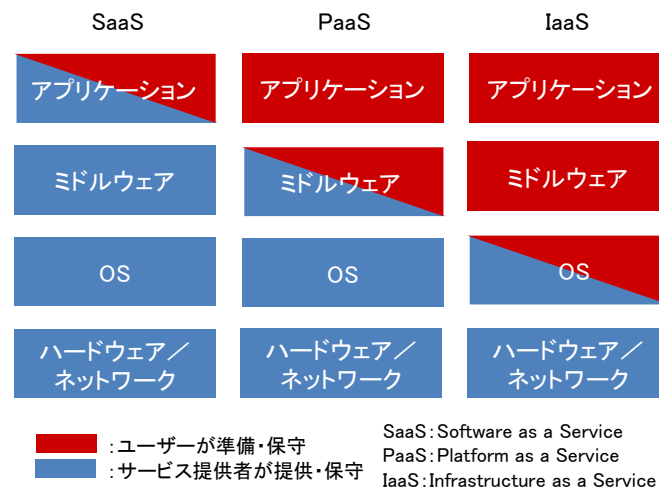


図 23 サービス形態の範囲

（出典：総務省「スマート・クラウド研究会報告書」）

中間サーバーについては、各情報保有機関の既存システム等に影響される要素が大きく、インターフェイスシステムと比べた場合、比較的 PaaS 又は IaaS 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。

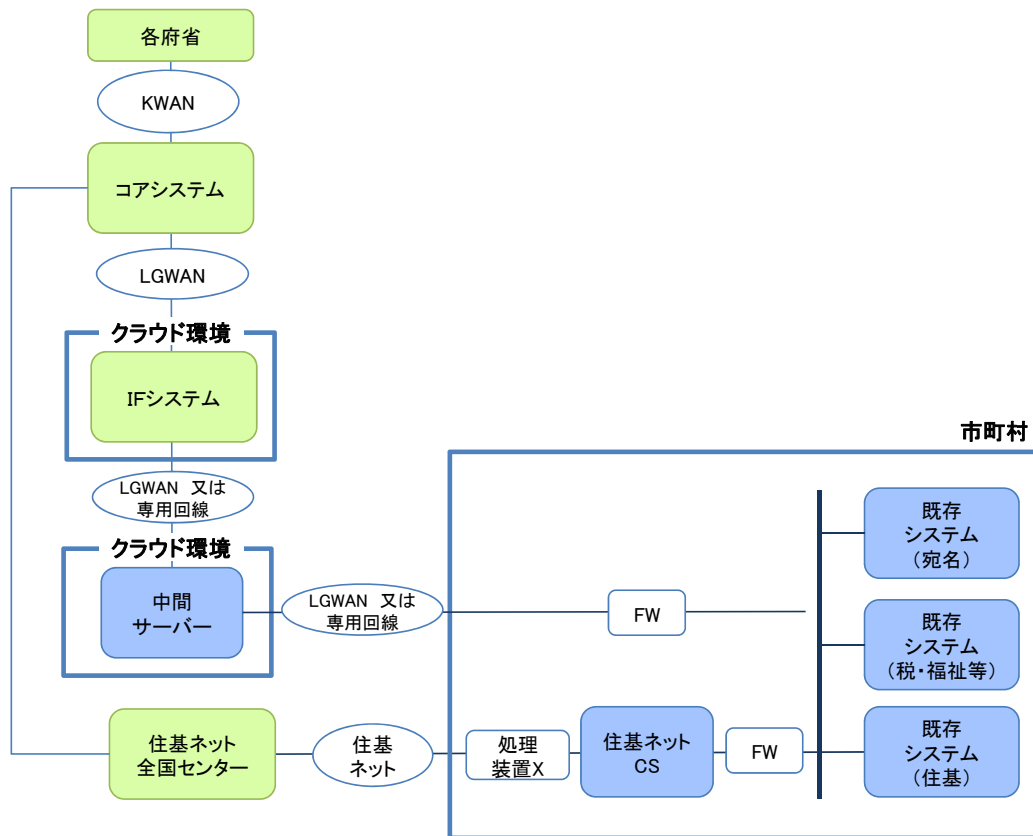


図 24 インターフェイスシステムと中間サーバーが異なるクラウド環境にある場合

(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。

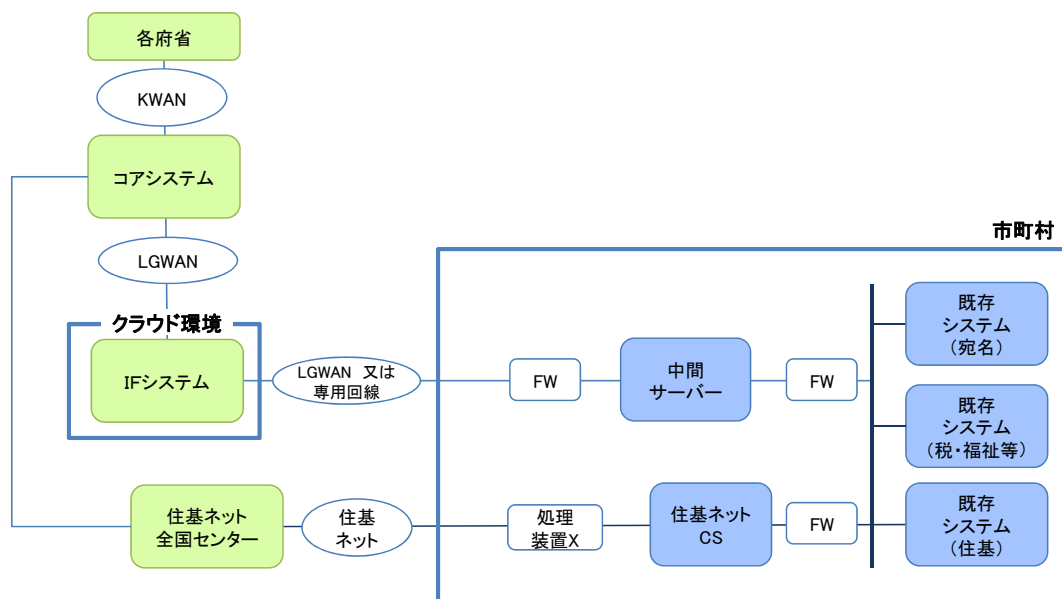
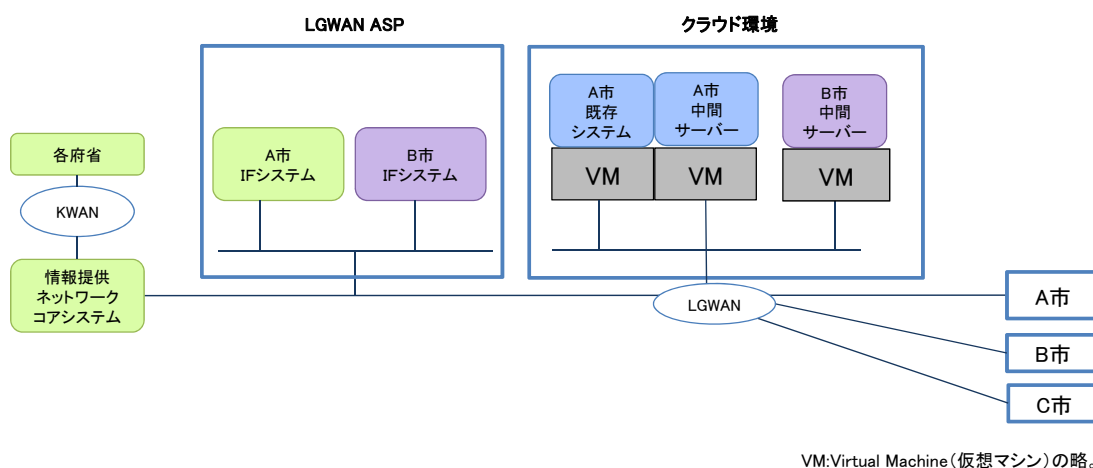


図 25 インターフェイスシステムのみがクラウド環境にある場合

(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 26 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、中間サーバーの非機能要件について述べる。

10.1 前提条件

中間サーバーの非機能要件は、原則情報保有機関ごとに定めることとするが、情報提供ネットワークシステムへの接続にあたって最低限遵守すべき要件については、別途ガイドライン等により全国統一で定めることも検討する（特にサービス稼働時間、セキュリティ要件等）。

10.2 規模要件

規模要件は、情報保有機関が蓄積するデータ量とトラフィック量に依存する。これらは情報保有機関側での固有要件及び調達されるハードウェアに依存するため、

- ・ 自庁内のネットワーク構成、帯域
- ・ 各情報提供者において中間サーバーに蓄積する複製のデータ項目、データ量
- ・ 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

中間サーバー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で共通ルール化する

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検討する必要がある。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について、以下に示す。

表 92 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 93 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

中間サーバー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ごとに異なる事情（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で定められた事務に基づく特定個人情報の提供に係る、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事情（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 94 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、情報照会における処理状況及び要求内容を一時的に保存するデータ（提供ステータス、提供の求め）、業務データ（特定個人情報等）、符号に分けて考える。

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 95 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について、以下に示す。

表 96 データ種別の例

観点	データ種別
データ	業務データ（特定個人情報等）
	符号
	提供ステータス、提供の求め
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ごとに異なる事情（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

中間サーバーは、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。

中間サーバーの耐障害性要件は、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 97 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

中間サーバー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、別途ガイドライン等により全国統一で定めることも検討する。

中間サーバーの構築・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中間サーバー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

- ・ 中間サーバーは、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

- ・ 中間サーバーの構築・運用においては、中間サーバーにアクセス可能なすべての職員について、適切な職員認証を実施すること。この際、中間サーバーへのログインは、組織単位ではなく、人単位で実施すること。
- ・ 中間サーバー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。
- ・ 情報提供 DB の暗号化、及び適切な暗号鍵管理を検討すること。
- ・ 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

- ・中間サーバー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

中間サーバーの運用・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 98 中間サーバーの運用・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
2.		運用ドキュメント管理

#	作業区分	作業項目
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（アプリケーション、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（アプリケーション、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。

特に中間サーバーにおいては、以下に示すアプリケーション、データ標準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 データ標準の変更対応

データ標準（特定個人情報の項目等）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。

③ 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情報の変更を実施する。

(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

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

中間サーバーのシステム監視機能を用いて、各既存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、即座に担当者及び既存システム運用保守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

中間サーバーに、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

中間サーバー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、中間サーバーの稼働に必要な各機器の 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こと。

なお、開催時期・回数等は別途協議の上決定すること。

また、指示要望があれば速やかに情報提供を行うこと。

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、中間サーバー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、障害が中間サーバーで発生しているのか、他システム（既存システムを含む）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、インターフェイスシステム及び既存システム等の運用保守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。