特定個人情報保護評価書（全項目評価書）

評価書番号	評価書名
55	大阪市　住民基本台帳事務　全項目評価書（令和8年1月以降）

個人のプライバシー等の権利利益の保護の宣言

大阪市は、住民基本台帳事務で特定個人情報ファイルを取扱うにあたり、特定個人情報の不適切な取扱いが個人のプライバシー等の権利利益に影響を及ぼしかねないことを認識し、特定個人情報の漏えいその他の事態を発生させるリスクを分析した上で、当該リスクを軽減させるための適切な措置を講じ、もって個人のプライバシー等の権利利益の保護に取り組んでいることを宣言する。

特記事項	住民基本台帳事務では、委託先による特定個人情報の不正入手・不正使用等への対策として、委託契約書にデータ機密保持事項を明記し、委託先における情報保護管理体制の確認及びデータ保護に関する規程の確認を行うとともに、委託事業者に機密保護等の誓約書を提出させている。 また本評価書は、令和8年1月のシステム更新後の住民基本台帳事務について記載している。

評価実施機関名

大阪市長

個人情報保護委員会　承認日　【行政機関等のみ】

公表日

［平成30年5月　様式4］

項目一覧

Ⅰ　基本情報
（別添1）事務の内容
Ⅱ　特定個人情報ファイルの概要
（別添2）特定個人情報ファイル記録項目
Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策
Ⅳ　その他のリスク対策
Ⅴ　開示請求、問合せ
Ⅵ　評価実施手続
（別添3）　変更箇所

Ⅰ　基本情報

1．特定個人情報ファイルを取り扱う事務	
①事務の名称	住民基本台帳に関する事務
②事務の内容　※	住民基本台帳は住民基本台帳法（以下、「住基法」という）に基づき作成されるものであり、住民に関する正確な記録を整備し、居住関係の公証、その他住民に関する事務処理の基礎となるものである。また、住基法に基づいて住民基本台帳のネットワーク化を図り、全国共通の本人確認システム（住基ネット）を都道府県と共同して構築している。 住基法及び行政の手続き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（以下、「番号法」という）の規定に従い、特定個人情報を以下の事務で取り扱う。（別添1を参照） ①個人を単位とする住民票を世帯ごとに編成し、住民基本台帳を作成 ②転入届、転居届、転出届、世帯変更届等の届出又は職権に基づく住民票の記載、消除又は記載の修正 ③住民基本台帳の正確な記録を確保するための措置 ④転入届に基づき住民票の記載をした際の転出元市町村に対する通知 ⑤本人又は同一の世帯に属する者の請求による住民票の写し等の交付 ⑥住民票の記載事項に変更があった際の都道府県知事に対する通知 ⑦地方公共団体情報システム機構（以下、「機構」という）への本人確認情報の照会 ⑧住民からの請求に基づく住民票コードの変更 ⑨個人番号の通知及び個人番号カードの交付 ⑩個人番号カード等を用いた本人確認 ＜中間サーバ＞ ・情報保有機関は情報提供ネットワークシステムに接続し、各情報保有機関が保有する個人情報について情報連携を行うことが必要である。また、この情報提供ネットワークシステムにおいては、各機関は特定個人情報を分散管理することとされていることから、情報提供のために既存システムのデータベースを他情報保有機関から直接参照することは、セキュリティ上好ましくない。各情報保有機関は情報提供ネットワークシステムに接続するに当たり、情報提供に必要な情報を「副本」として装備した中間サーバを設置することとする。 ・中間サーバは、機構が設置するものを共同利用する。
③対象人数	[　30万人以上　] ＜選択肢＞ 1）1,000人未満　2）1,000人以上1万人未満 3）1万人以上10万人未満　4）10万人以上30万人未満 5）30万人以上

2. 特定個人情報ファイルを取り扱う事務において使用するシステム	
システム1	
①システムの名称	住民記録システム
②システムの機能	1. 住民基本台帳の記載 転入、出生、入国、職権等により住民基本台帳に新たに住民を記載(住民票を作成)する機能 2. 住民基本台帳の記載変更 住民基本台帳に記載されている事項に変更があったときに、記載内容を修正する機能 3. 住民基本台帳の消除処理 転出、死亡、出国、職権等により住民基本台帳から住民に関する記載を消除(住民票を除票)する機能 4. 住民基本台帳の照会 住民基本台帳から該当する住民に関する記載(住民票)を照会する機能 5. 帳票の発行機能 住民票の写し、住民票記載事項証明書、転出証明書、住民票コード通知書等の各種帳票を発行する機能 6. 住民基本台帳の統計機能 異動集計表や、人口統計用の集計表を作成する機能 7. 住民基本台帳ネットワークシステムとの連携機能 機構、県、他自治体、市内他区と住民基本台帳ネットワークシステムを通じ連携する機能 8. 出入国在留管理庁への通知事項の作成機能 外国人住民票の記載等に応じて、市町村通知の作成及び出入国在留管理庁通知等の取込等の連携を行う機能 9. 統合基盤システムとの連携機能 他機関からの住民票情報の提供依頼に対して、統合基盤システムを通じて情報提供ネットワークシステムに当該住民票情報を提供する機能
③他のシステムとの接続	[○] 情報提供ネットワークシステム　　[○] 庁内連携システム [○] 住民基本台帳ネットワークシステム　　[　　] 既存住民基本台帳システム [○] 宛名システム等　　[○] 税務システム [○] その他　（ 申請管理システム　　）

システム2	
①システムの名称	住民基本台帳ネットワークシステム（以下、「住基ネット」という） ※「3. 特定個人情報ファイル名」に示す「本人確認情報ファイル」及び「送付先情報ファイル」は、住基ネットの構成要素のうち、市町村CS（コミュニケーション・サーバ）において管理されているため、以降は、住基ネットの内の市町村CS部分について記載する。
②システムの機能	1. 本人確認情報の更新 住民記録システムにおいて住民票の記載事項の変更又は新規作成が発生した場合に、当該情報を元に市町村CSの本人確認情報を更新し、都道府県サーバへ更新情報を送信する機能。 2. 本人確認 特例転入処理や住民票の写しの広域交付などを行う際、窓口における本人確認のため、提示された個人番号カード等を元に住基ネットが保有する本人確認情報に照会を行い、確認結果を画面上に表示する機能。 3. 個人番号カードを利用した転入（特例転入） 個人番号カードの交付を受けている者等の転入が予定される場合に、転出証明書情報をCSを通じて受け取り、その者に係る転入の届出を受け付けた際に、個人番号カードを用いて転入処理を行う（一定期間経過後も転入の届出が行われない場合は、受け取った転出証明書情報を消去する。）。 4. 本人確認情報検索 統合端末において入力された4情報（氏名、住所、性別、生年月日）の組合せをキーに本人確認情報の検索を行い、検索条件に該当する本人確認情報の一覧を画面上に表示する機能。 5. 機構への情報照会 全国サーバに対して住民票コード、個人番号又は4情報の組合せをキーとした本人確認情報照会要求を行い、該当する個人の本人確認情報を受領する機能。 6. 本人確認情報整合 本人確認情報ファイルの内容が都道府県知事が都道府県サーバにおいて保有している都道府県サーバ保存本人確認情報ファイル及び機構が全国サーバにおいて保有している機構保存本人確認情報ファイルと整合することを確認するため、都道府県サーバ及び全国サーバに対し、整合性確認用本人確認情報を提供する機能。 7. 送付先情報通知 個人番号の通知に係る事務の委任先である機構において、住民に対して番号通知書類(個人番号通知書、個人番号カード交付申請書（以下、「交付申請書」という）等)を送付するため、住民記録システムから当該市町村の住民基本台帳に記載されている者の送付先情報を抽出し、当該情報を、機構が設置・管理する個人番号カード管理システムに通知する機能。 8. 個人番号カード管理システムとの情報連携 機構が設置・管理する個人番号カード管理システムに対し、個人番号カードの交付、廃止、回収又は一時停止解除に係る情報や個人番号カードの返還情報等を連携する機能。
③他のシステムとの接続	[　] 情報提供ネットワークシステム　　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　　[　] 既存住民基本台帳システム [　] 宛名システム等　　[　] 税務システム [○] その他　（ 住民記録システム　　）

システム3	
①システムの名称	統合基盤システム
②システムの機能	1. 統合宛名番号付番機能 団体内統合宛名番号が未登録の個人について、新規に団体内統合宛名番号を付番する機能。付番した団体内統合宛名番号を業務システム、中間サーバーに連携する機能。 2. 宛名情報等管理機能 宛名情報等を団体内統合宛名番号、個人番号と紐付けて保存し、管理する機能。 3. 中間サーバー連携機能 中間サーバーからの要求に基づき、団体内統合宛名番号に紐付く宛名情報を通知する機能。 4. 業務システム連携機能 業務システムからの要求に基づき、団体内統合宛名番号を通知する機能。 5. セキュリティ関連機能 業務システムのサーバや端末に対し、ウイルスのパターンファイルの配布を行う機能。 6. 認証機能 業務システムを利用できるユーザとその業務権限について認証を行う機能。
③他のシステムとの接続	[　] 情報提供ネットワークシステム　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[　] 既存住民基本台帳システム [　] 宛名システム等　[　] 税務システム [○] その他　（ 住民記録システム、中間サーバ、連携するシステム全て　）
システム4	
①システムの名称	中間サーバ
②システムの機能	1. 符号管理機能 符号管理機能は情報照会、情報提供に用いる個人の識別子である「符号」と、本市内で個人を特定するために利用する「団体内統合宛名番号」とを紐付け、その情報を保管・管理する。 2. 情報照会機能 情報照会機能は、情報提供ネットワークシステムを介して、特定個人情報（連携対象）の情報照会及び情報の受領を行う。 3. 情報提供機能 情報提供機能は、情報提供ネットワークシステムを介して、情報照会要求の受領及び当該特定個人情報（連携対象）の提供を行う。 4. 既存システム接続機能 中間サーバーと既存システム、統合基盤システム及び住民基本台帳システムとの間で情報照会内容、情報提供内容、特定個人情報（連携対象）、符号取得のための情報等について連携する。 5. 情報提供等記録管理機能 特定個人情報（連携対象）の照会、又は提供があった旨の情報提供等記録を生成し、管理する。 6. 情報提供データベース管理機能 特定個人情報（連携対象）を副本として、保持・管理する。 7. データ送受信機能 中間サーバーと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）との間で情報照会、情報提供、符号取得のための情報等について連携する。 8. セキュリティ管理機能 9. 職員認証・権限管理機能 中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報（連携対象）へのアクセス制御を行う。 10. システム管理機能 バッチ処理の状況管理、業務統計情報の集計、稼働状態の通知、保管切れ情報の削除を行う。
③他のシステムとの接続	[○] 情報提供ネットワークシステム　[○] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[　] 既存住民基本台帳システム [○] 宛名システム等　[　] 税務システム [○] その他　（ 住民記録システム　）

システム5	
①システムの名称	申請管理システム
②システムの機能	（マイナポータル連携機能） LGWAN系ネットワークとマイナンバー利用事務系ネットワークの間にDMZ（隔離された領域）内の連携サーバを利用し、サービス検索・電子申請機能（マイナポータルぴったりサービス）で受け付けた電子申請データを申請管理システムに連携する（受け渡す）機能 （申請管理システム） ・連携サーバから連携された電子申請データを参照する機能 ・電子申請データを地方公共団体の基幹システムに連携する（受け渡す）機能
③他のシステムとの接続	[　] 情報提供ネットワークシステム　　[○] 庁内連携システム [　] 住民基本台帳ネットワークシステム　　[　] 既存住民基本台帳システム [　] 宛名システム等　　[　] 税務システム [○] その他　（住民記録システム、サービス検索・電子申請機能（マイナポータルぴったりサービス））

3. 特定個人情報ファイル名

（1）住民基本台帳ファイル
（2）本人確認情報ファイル
（3）送付先情報ファイル

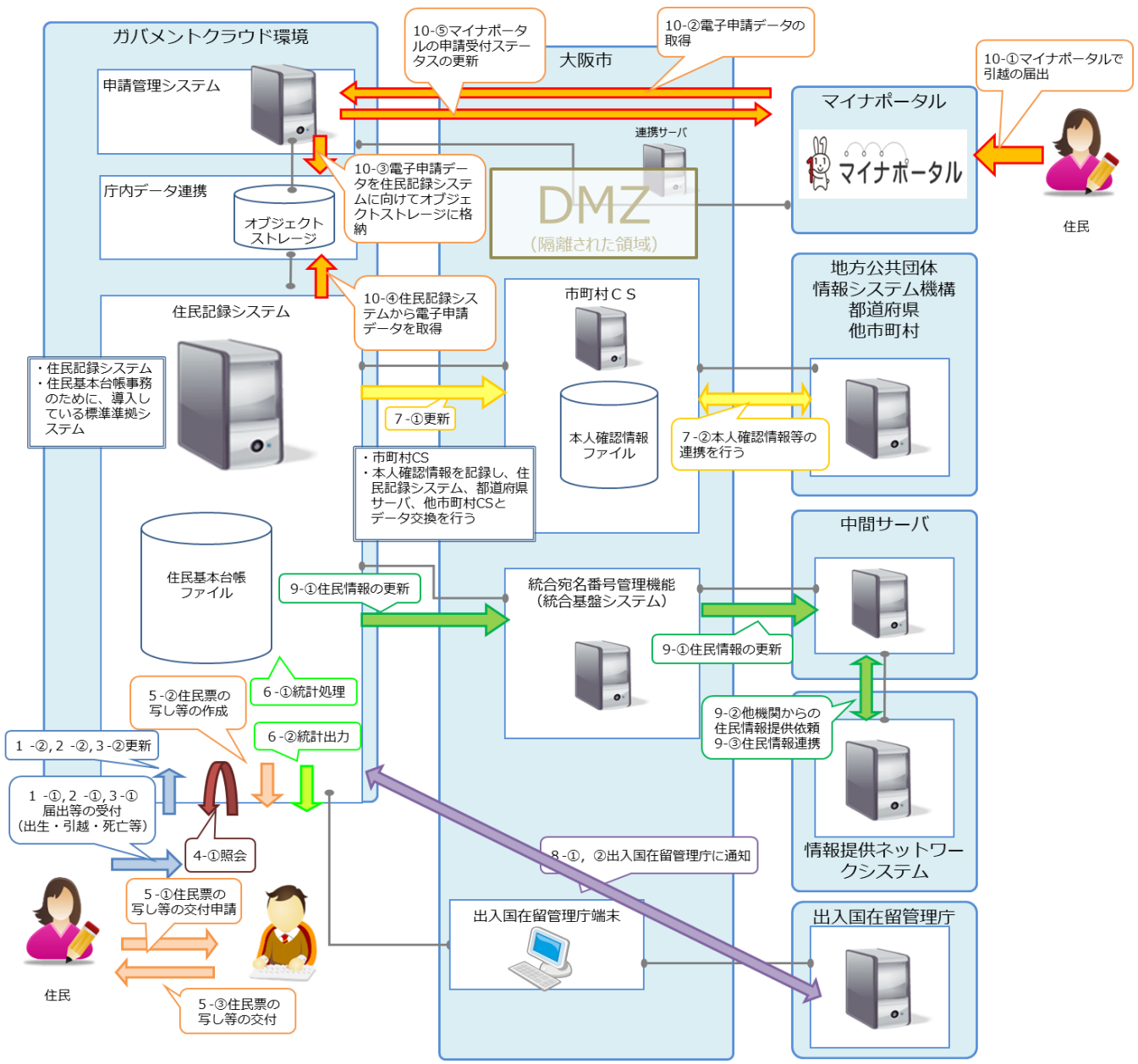
4. 特定個人情報ファイルを取り扱う理由

①事務実施上の必要性	大阪市では、次の3ファイルを下記に記載のとおりの必要性から取り扱う。 （1）住民基本台帳ファイル ・個人番号が住民票の記載事項（住基法第7条）として定められ、以下の用途に用いられる。 ①出生等や個人番号が変更となる時、機構から通知された個人番号とすべき番号を住民票に記載する。 ②転入により市の区域内に住民票を作成する時、転出証明書（転出証明書情報）に記載されている個人番号を住民票に記載する。 ③住基ネットへ本人確認情報として送信する。 （2）本人確認情報ファイル ・本人確認情報ファイルは、転出入があった場合等にスムーズな住民情報の処理を行うため、また全国的な本人確認手段として、1つの市町村内にとどまらず、全地方公共団体で、本人確認情報を正確かつ統一的に記録・管理することを目的として、以下の用途に用いられる。 ①住基ネットを用いて市町村の区域を越えた住民基本台帳に関する事務の処理を行うため、区域内の住民に係る最新の本人確認情報を管理する。 ②都道府県に対し、本人確認情報の更新情報を通知する。 ③申請・届出の際に提示された個人番号カード等を用いた本人確認を行う。 ④個人番号カードを利用した転入手続きを行う。 ⑤住民基本台帳に関する事務において、本人確認情報を検索する。 ⑥都道府県知事保存本人確認情報及び機構保存本人確認情報との整合性を確認する。 （3）送付先情報ファイル ・市町村長が個人番号を指定した際は個人番号通知書の形式にて全付番対象者に個人番号を通知するものとされている（番号法第7条第1項）。個人番号通知書による番号の通知及び個人番号カード交付申請書の送付については、事務効率化等の観点から、市町村から、機構に委任しており、機構に個人番号通知書及び交付申請書の送付先情報を提供する。
②実現が期待されるメリット	住民票の写し等にかえて本人確認情報を利用することにより、これまでに窓口で提出が求められていた行政機関が発行する添付書類（住民票の写し等）の省略が図られ、住民の負担軽減（各機関を訪問し、証明書等を入手する金銭的、時間的コストの節約）につながることが見込まれる。また、個人番号カードによる本人確認、個人番号の真正性確認が可能となり、行政事務の効率化に資することが期待される。

5. 個人番号の利用 ※	
法令上の根拠	1. 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（番号法） （平成25年5月31日法律第27号） ・第7条（指定及び通知） ・第16条（本人確認の措置） ・第17条（個人番号カードの交付等） 2. 住民基本台帳法（住基法）（昭和42年7月25日法律第81号） （平成25年5月31日法律第28号施行時点） ・第5条（住民基本台帳の備付け） ・第6条（住民基本台帳の作成） ・第7条（住民票の記載事項） ・第8条（住民票の記載等） ・第12条（本人等の請求に係る住民票の写し等の交付） ・第12条の4（本人等の請求に係る住民票の写しの交付の特例） ・第14条（住民基本台帳の正確な記録を確保するための措置） ・第22条（転入届） ・第24条の2（個人番号カードの交付を受けている者等に関する転入届の特例） ・第30条の6（市町村長から都道府県知事への本人確認情報の通知等） ・第30条の10（通知都道府県の区域内の市町村の執行機関への本人確認情報の提供） ・第30条の12（通知都道府県以外の都道府県の区域内の市町村の執行機関への本人確認情報の提供）
6. 情報提供ネットワークシステムによる情報連携 ※	
①実施の有無	[　　実施する　　] ＜選択肢＞ 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	・番号法第19条第8号（特定個人情報の提供の制限）及び番号法第19条8号に基づく利用特定個人情報に関する命令 （命令第2条の表における情報提供の根拠） 第三欄（情報提供者）が「市町村長」の項のうち、第四欄（利用特定個人情報）に「住民票関係情報」が含まれる項（1、2、3、5、7、11、13、15、20、28、37、39、48、53、57、58、59、63、65、66、69、73、75、76、81、83、84、86、87、91、92、96、106、108、110、112、115、118、124、129、130、132、136、137、138、141、142、144、149、150、151、152、155、156、158、160、163、164、165、166の項） （命令第2条の表における情報照会の根拠） なし（住民基本台帳に関する事務において情報提供ネットワークシステムによる情報照会は行わない）
7. 評価実施機関における担当部署	
①部署	大阪市市民局総務部住民情報担当（住民情報グループ）
②所属長の役職名	市民局長
8. 他の評価実施機関	
なし	

（別添1）事務の内容

「（1）住民基本台帳ファイル」を取り扱う事務の内容（住基等システムを中心とした事務の流れ）

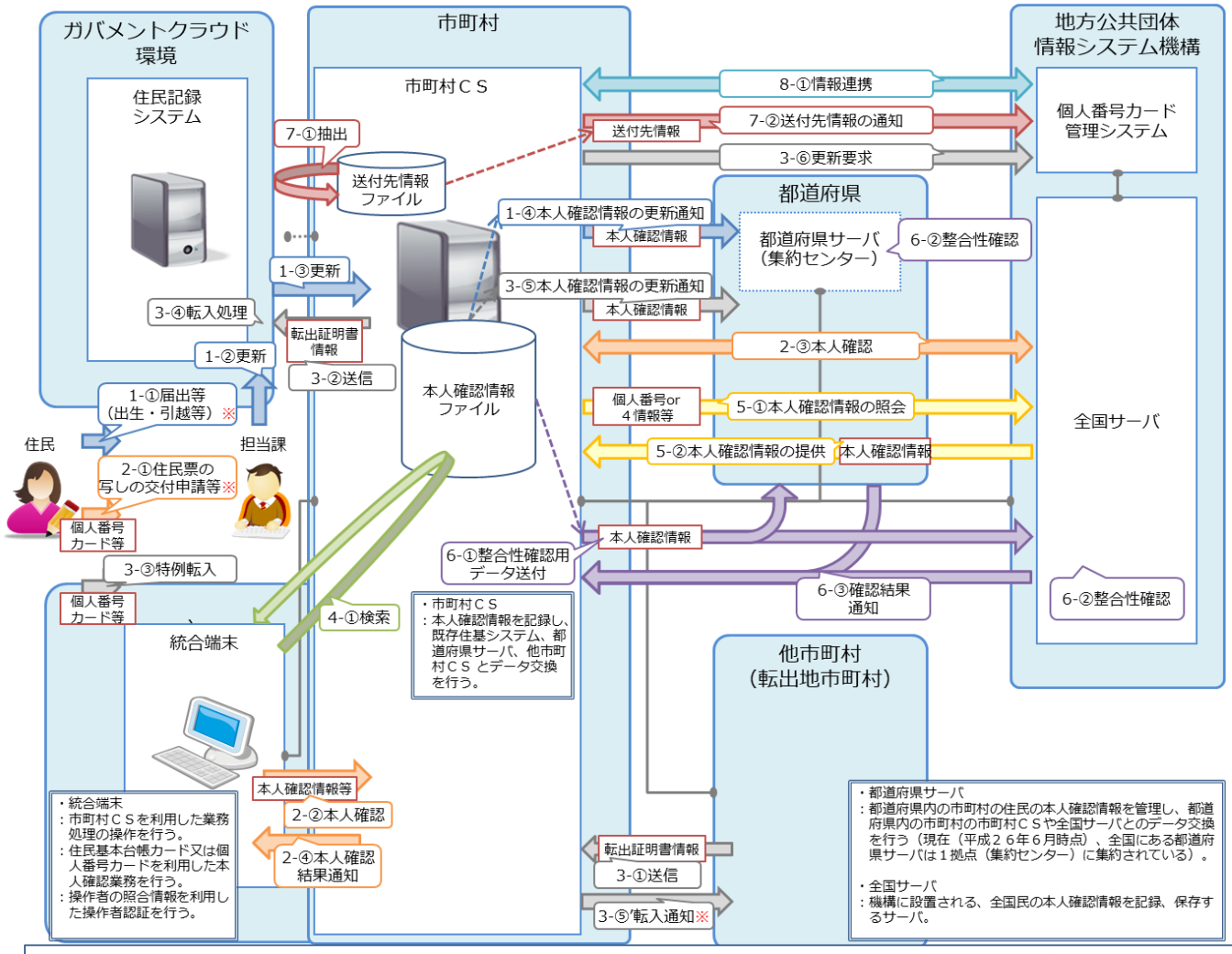


（備考）

1．住民基本台帳の記載に関する事務
1-① 住民より転入、出生等の届出等を受け付ける。
1-② 異動情報を住民基本台帳ファイルに更新する。
2．住民基本台帳の記載変更に関する事務
2-① 住民より転居等の届出等を受付する。
2-② 異動情報を住民基本台帳ファイルに更新する。
3．住民基本台帳の消除に関する事務
3-① 住民より転出、死亡等の届出等を受付する。
3-② 異動情報を住民基本台帳ファイルに更新する。
4．住民基本台帳の照会
4-① 基本4情報の組み合わせや個人番号をキーワードとして、住民基本台帳ファイルを検索する。
5．帳票の発行に関する事務
5-① 住民より住民票の写し等の交付申請を受付する。
5-② 住民記録システムより該当証明書を作成、発行する。
5-③ 発行した住民票の写し等の証明書を住民に交付する。
6．住民基本台帳の統計
6-① 住民記録システムにて各種統計処理を行う。
6-② 住民記録システムより各種統計情報を出力する。
7．住基ネットとの連携
7-① 住民基本台帳にて更新された住民情報を基に、市町村CSの本人確認情報を更新する。
7-② 市町村CSにて更新された本人確認情報を当該都道府県の都道府県サーバに通知する。
8．出入国在留管理庁との連携
8-① 外国人住民の異動情報を市町村通知として出入国在留管理庁に通知する。
8-② 出入国在留管理庁通知により外国人住民の住民票記載情報等の更新をする。
9．団体内統合宛名システムとの連携
9-① 住民情報に変更等があった場合、統合宛名番号管理機能及び中間サーバの住民情報を更新する。
9-② 情報提供ネットワークシステムを通じての他機関からの住民票情報の提供依頼を受け付ける。
9-③ 該当する住民票情報を団体内統合宛名システムを通じて情報提供ネットワークへ連携する
10．申請管理システムとの連携
10-① 住民がサービス検索・電子申請機能（マイナポータルぴったりサービス）で転入、転出の届出等を行う。
10-② 申請管理システムにて電子申請データを取得する。
10-③ 申請管理システムにて電子申請データを住民記録システムに向けてオブジェクトストレージに格納する。
10-④ 住民記録システムにて電子申請データを取得する。
10-⑤ 申請管理システムにてサービス検索・電子申請機能（マイナポータルぴったりサービス）上の申請受付ステータスを更新する。

（別添1）事務の内容

「(2)本人確認情報ファイル」及び「(3)送付先情報ファイル」を取り扱う事務の内容（市町村CSを中心とした事務の流れ）



※個人番号カードに係る事務（個人番号通知書／個人番号カードの発行・送付など）については地方公共団体情報システム機構（機構）が評価書を作成しますので、機構が評価する「住民基本台帳ネットワーク及び番号制度関連事務」をご覧ください。

（注）図中に※が付されている箇所は、特定個人情報を含まない事務の流れを指す。

（備考）

１．本人確認情報の更新に関する事務

1-①. 住民より転入、転出、転居、出生、死亡等の届出等を受け付ける(※特定個人情報を含まない)。
1-②. 市町村の住民基本台帳（住民記録システム）を更新する。
1-③. 市町村の住民基本台帳にて更新された住民情報を基に、市町村ＣＳの本人確認情報を更新する。
1-④. 市町村ＣＳにて更新された本人確認情報を当該都道府県の都道府県サーバに通知する。

２．本人確認に関する事務

2-①. 住民より、住民票の写しの交付申請等、本人確認が必要となる申請を受け付ける(※特定個人情報を含まない)。
2-②,③. 統合端末において、住民から提示された個人番号カードに記録された住民票コード（又は法令で定めた書類に記載された４情報）を送信し、市町村ＣＳを通じて、全国サーバに対して本人確認を行う。
2-④. 全国サーバより、市町村ＣＳを通じて、本人確認結果を受領する。

３．個人番号カードを利用した転入（特例転入）

3-①. 市町村ＣＳにおいて転出地市町村より転出証明書情報を受信する。
3-②. 住民記録システムにおいて、市町村ＣＳから転出証明書情報を受信する。
3-③. 転入手続を行う住民から提示された個人番号カードを利用して本人確認(「２．本人確認」を参照)を行う。
※転出証明書情報に記載の転出の予定年月日から３０日後までに転入手続が行われない場合には、当該転出証明書情報を消去する。
※3-③の転入手続時に転出証明書情報を受信していない場合又は消去している場合には、統合端末から、市町村ＣＳを経由して転出地市町村に対し転出証明書情報の送信依頼を行い(※特定個人情報を含まない)、その後、3-①・②を行う。
3-④. 住民記録システムにおいて、転入処理を行う。
3-⑤. 市町村ＣＳより、住民記録システムから転入処理完了後に受け渡される転入通知情報(※特定個人情報を含まない)を転出地市町村へ送信すると同時に、都道府県サーバへ本人確認情報の更新情報を送信する。
3-⑥. 転入処理完了後、個人番号カードの継続利用処理を行い、個人番号カード管理システムに対し、個人番号カード管理情報の更新要求を行う。

４．本人確認情報検索に関する事務

4-①. 住民票コード、個人番号又は４情報の組み合わせをキーワードとして、市町村ＣＳの本人確認情報を検索する。
※検索対象者が自都道府県の住所地市町村以外の場合は都道府県サーバ、他都道府県の場合は全国サーバに対してそれぞれ検索の要求を行う。

５．機構への情報照会に係る事務

5-①. 機構に対し、個人番号又は４情報等をキーワードとした本人確認情報の照会を行う。
5-②. 機構より、当該個人の本人確認情報を受領する。

６．本人確認情報整合に係る事務

6-①. 市町村ＣＳより、都道府県サーバ及び全国サーバに対し、整合性確認用の本人確認情報を送付する。
6-②. 都道府県サーバ及び住基全国サーバにおいて、市町村ＣＳより受領した整合性確認用の本人確認情報を用いて保有する本人確認情報の整合性確認を行う。
6-③. 都道府県サーバ及び全国サーバより、市町村ＣＳに対して整合性確認結果を通知する。

７．送付先情報通知に関する事務

7-①. 住民記録システムより、当該市町村における個人番号カードの交付対象者の送付先情報を抽出する。
7-②. 個人番号カード管理システムに対し、送付先情報を通知する。

８．個人番号カード管理システムとの情報連携

8-①. 個人番号カード管理システムに対し、個人番号カードの交付、廃止、回収又は一時停止解除に係る情報や個人番号カードの返還情報等を連携する。

Ⅱ　特定個人情報ファイルの概要

1. 特定個人情報ファイル名		
住民基本台帳ファイル		
2. 基本情報		
①ファイルの種類 ※		[　　システム用ファイル　　] ＜選択肢＞ 1）システム用ファイル 2）その他の電子ファイル（表計算ファイル等）
②対象となる本人の数		[　100万人以上1,000万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
③対象となる本人の範囲 ※		区域内の住民（住基法第5条（住民基本台帳の備付け）に基づき住民基本台帳に記録された住民を指す） ※住民基本台帳に記録されていた者で、転出等の事由により住民票が消除（死亡による消除を除く。）された者（以下「消除者」という。）を含む。
	その必要性	法令に基づき住民基本台帳を作成し必要に応じて住民票に記載、消除又は修正すべきとされているため。
④記録される項目		[　　100項目以上　　] ＜選択肢＞ 1）10項目未満　2）10項目以上50項目未満 3）50項目以上100項目未満　4）100項目以上
	主な記録項目 ※	・識別情報 [○] 個人番号　[○] 個人番号対応符号　[○] その他識別情報（内部番号） ・連絡先等情報 [○] 4情報（氏名、性別、生年月日、住所）　[　] 連絡先（電話番号等） [○] その他住民票関係情報 ・業務関係情報 [　] 国税関係情報　[　] 地方税関係情報　[　] 健康・医療関係情報 [○] 医療保険関係情報　[○] 児童福祉・子育て関係情報　[　] 障害者福祉関係情報 [　] 生活保護・社会福祉関係情報　[○] 介護・高齢者福祉関係情報 [　] 雇用・労働関係情報　[○] 年金関係情報　[　] 学校・教育関係情報 [　] 災害関係情報 [○] その他　（　選挙権の有無　）
	その妥当性	・個人番号、4情報（氏名、性別、生年月日。住所）、その他住民票関係情報 住民票の記載事項であるため。（住基法第7条）
	全ての記録項目	別添2を参照。
⑤保有開始日		平成27年7月18日
⑥事務担当部署		各区役所住民情報事務所管課（24区、2出張所、北部・南部サービスセンター、南港ポートタウンサービスコーナー）、サービスカウンター（梅田、難波、天王寺）、郵送事務処理センター、市民局総務部住民情報担当

3. 特定個人情報の入手・使用	
①入手元 ※	[○] 本人又は本人の代理人 [○] 評価実施機関内の他部署 （ デジタル統括室基盤担当、福祉局生活福祉部保険年金課、福祉局高齢施策部介護保険課、こども青少年局子育て支援部管理課、選挙管理委員会事務局 ） [○] 行政機関・独立行政法人等 （ 地方公共団体情報システム機構、出入国在留管理庁 ） [○] 地方公共団体・地方独立行政法人 （ 市町村 ） [ ] 民間事業者 （ ） [ ] その他 （ ）
②入手方法	[○] 紙 [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 電子メール [ ] 専用線 [○] 庁内連携システム [ ] 情報提供ネットワークシステム [○] その他 （ 住基ネット、出入国在留管理庁連携ネットワークシステム、申請管理システム ）
③入手の時期・頻度	入手元（本人又は本人の代理人） ・住民異動届（転入・転居・転出・世帯変更届）／届出を受けた都度／入手方法は紙 ・転入届出に伴う転出証明書情報／届出を受けた都度／入手方法は紙 ・マイナポータルで受け付けた電子申請を申請管理システムから入手／随時 入手元（評価実施機関内の他部署） ・統合基盤システムから団体内統合宛名番号等の情報／新規付番、変更された都度 ・住基法第7条第10号～第11の2号までに規定する情報／1日1回 入手元（地方公共団体・地方独立行政法人） ・転入前市町村からの転出証明書情報／届出を受けた都度／入手方法は住基ネット ・転出先市町村からの転入通知情報／届出を受けた都度／入手方法は住基ネット ・本籍地市町村からの戸籍届出の写し、住民票記載事項通知（住基法第9条2項通知）／戸籍届出を受けた都度／入手方法は紙 入手元（行政機関・地方独立行政法人） ・出入国在留管理庁連携ネットワークシステムからの出入国在留管理庁通知／1日1回
④入手に係る妥当性	法令に基づき、入手する。 住民異動届は本人および本人の代理人（以下、本人等）が書面（住民異動届）で行わなければならない（住基法第27条）届出の根拠は下記のとおり。 ・転入届（住基法第22条） ・転居届（住基法第23条） ・転出届（住基法第24条） ・転入届の特例（住基法第24条の2） ・世帯変更届（住基法第25条） 転入届出に伴う転出証明書情報 ・転入届（住基法第22条）の場合は、本人等から転出証明書（転出地市町村で交付）の提出を受ける。 ・転入届の特例（住基法第24条の2）の場合は、転出地市町村から住基ネットを通じて入手する。 転出先市町村からの転入通知情報 ・転出先市町村から住基ネットを通じて入手する。（住基法第9条第1項、第9条第3項） 戸籍届出の写し、住民票記載事項通知（住基法第9条2項通知） ・本人等から本籍市町村へ提出された、戸籍異動に関する届出（出生・婚姻・死亡など）に伴い、本籍地市町村から書面（戸籍届出の写し、戸籍通知）を通じ入手する。 定期的に入手 ・外国人住民の在留資格等更新に関する届出（本人等が出入国在留管理局等に届出）に伴い、出入国在留管理局から出入国在留管理庁連携ネットワークシステムを通じて1日に1回提供があるので、出入国在留管理庁通知情報として入手する。（住基法第30条の50） ・資格情報に関する新規・変更・修正情報が業務システムから統合基盤システムを通じて1日に1回提供があるので、提供の都度入手する。（住基法第7条第10号～第11の2号）

⑤本人への明示		・住民異動届の入手：住基法第21条～第27条に記載されている。 ・転出証明書情報の入手：住基法施行令　第23条～第24条の3に記載されている。 ・転入通知情報の入手：住基法第9条第1項、第9条第3項に記載されている。 ・戸籍届出の写し、戸籍通知（住基法第9条2項通知）の入手：住民基本台帳法　第9条第2項に記載されている。 ・出入国在留管理庁通知情報の入手：住基法第30条の50に記載されている。 ・資格情報の入手：住基法施行令第12条第2項の3～5に記載されている。
⑥使用目的 ※		個人番号が住民票の記載事項（住基法第7条）として定められているため、住民票に記載する。また、住基ネットへも本人確認情報として送信する。
	変更の妥当性	―
⑦使用の主体	使用部署 ※	各区役所住民情報事務所管課（24区、2出張所、北部・南部サービスセンター、南港ポートタウンサービスコーナー）、サービスカウンター（梅田、難波、天王寺）、郵送事務処理センター、市民局総務部住民情報担当
	使用者数	［　500人以上1,000人未満　］ ＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
⑧使用方法 ※		住基法に基づき使用する。主な方法は以下のとおり。 ・住民票へ記載し、公証する。 ・本人確認情報として住基ネットへ送信する。 ・窓口における本人確認に使用する。（個人番号等をキーとして住民票を検索し、届出書等の記載内容と照合） ・「サービス検索・電子申請機能（マイナポータルぴったりサービス）」を通じて申請された電子申請データの受理、審査等
	情報の突合 ※	・本人等届出により入手 住民異動届出書または戸籍届出書の写しに記載の内容と個人番号又は住民票情報との突合／対象者特定のために実施 ・住基ネットを通じて入手 住基ネットの本人確認情報と個人番号又は住民票情報との突合／対象者特定のために実施 ・出入国在留管理庁連携ネットワークを通じて入手 基本情報及び在留カード等番号と住民票情報との突合／対象者を特定するために実施 ・申請者を確認するために住民記録システムを通じて取り込んだ番号紐付情報と突合する
	情報の統計分析 ※	個人に着目した分析・統計は行わず、住民基本台帳関係年報、事務処理実績等の確認のための統計のみ行う。
	権利利益に影響を与え得る決定 ※	該当なし
⑨使用開始日		平成27年10月5日

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※		[委託する] <選択肢> 1）委託する 2）委託しない （ 5 ） 件
委託事項1		システム保守業務
①委託内容		住民記録等システム保守作業
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体] <選択肢> 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	[100万人以上1,000万人未満] <選択肢> 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲 ※	特定個人情報ファイルの範囲と同様
	その妥当性	住民記録システムの安定稼働のため、パッケージシステム提供業者に保守業務を委託する。個人番号は住民基本台帳の記載事項となっており、特定個人情報ファイルを含む保守作業が必須となる。
③委託先における取扱者数		[10人以上50人未満] <選択肢> 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[ ]専用線 [ ]電子メール [ ]電子記録媒体（フラッシュメモリを除く。） [ ]フラッシュメモリ [ ]紙 [○]その他 （ 特定個人情報ファイルの提供はしていないが、必要に応じて本市指定の保守作業場所にて、システムの直接操作を認めている。 ）
⑤委託先名の確認方法		大阪市ホームページの入札契約情報にて確認できる。
⑥委託先名		株式会社 NTTデータ関西
再委託	⑦再委託の有無 ※	[再委託する] <選択肢> 1）再委託する 2）再委託しない
	⑧再委託の許諾方法	業務契約書の規定に基づく再委託承諾申請書の提出があった場合、申請内容を審査した結果、再委託が適当と判断した場合は再委託先に対し承諾書を交付する。
	⑨再委託事項	住民記録システム改修（一部の機能）、住民記録システム保守作業（ライブラリ管理等）等
委託事項2		区役所住民情報業務等委託
①委託内容		区役所における住民情報業務等委託業務
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体] <選択肢> 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	[100万人以上1,000万人未満] <選択肢> 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲 ※	特定個人情報ファイルの範囲と同様
	その妥当性	住民基本台帳関係業務等に係る市町村窓口業務に関して民間事業者に委託することができる業務の範囲について（平成20年3月31日総行市第75号 総務省自治行政局市町村課長通知）に基づき入札を実施
③委託先における取扱者数		[100人以上500人未満] <選択肢> 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上

④委託先への特定個人情報ファイルの提供方法		[　　]専用線　[　　]電子メール　[　　]電子記録媒体(フラッシュメモリを除く。) [　　]フラッシュメモリ　[○]紙 [○]その他　(設置端末の操作による提供)
⑤委託先名の確認方法		大阪市ホームページの入札契約情報にて確認できる。
⑥委託先名		(株)パソナ　外3社
再委託	⑦再委託の有無 ※	[　　再委託しない　　]　<選択肢> 1) 再委託する　2) 再委託しない
	⑧再委託の許諾方法	
	⑨再委託事項	
委託事項3		中央情報処理センター運用業務
①委託内容		中央情報処理センターで運用する業務システムの実行監視
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体]　<選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部
	対象となる本人の数	[100万人以上1,000万人未満]　<選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
	対象となる本人の範囲 ※	特定個人情報ファイルの範囲と同様
	その妥当性	システムの安定した運用実現のため専門的な知識を有する民間事業者に委託する。
③委託先における取扱者数		[　　10人以上50人未満　　]　<選択肢> 1) 10人未満　2) 10人以上50人未満 3) 50人以上100人未満　4) 100人以上500人未満 5) 500人以上1,000人未満　6) 1,000人以上
④委託先への特定個人情報ファイルの提供方法		[　　]専用線　[　　]電子メール　[　　]電子記録媒体(フラッシュメモリを除く。) [　　]フラッシュメモリ　[　　]紙 [○]その他　(特定個人情報ファイルの提供はしていないが、必要に応じて本市指定の保守作業場所にて、システムの直接操作を認めている。)
⑤委託先名の確認方法		大阪市ホームページの入札契約情報にて確認できる。
⑥委託先名		株式会社　NTTデータ関西
再委託	⑦再委託の有無 ※	[　　再委託する　　]　<選択肢> 1) 再委託する　2) 再委託しない
	⑧再委託の許諾方法	業務委託契約書の規定に基づく再委託承諾申請書の提出があった場合は、申請内容を審査した結果、再委託が適当と判断した場合は委託先に対し承諾書を交付する。
	⑨再委託事項	中央情報処理センターで運用する業務システムの実行監視、入出力媒体の管理における一部業務
委託事項4		統合基盤システム運用保守業務
①委託内容		統合基盤システムの維持管理に係る運用保守
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体]　<選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部
	対象となる本人の数	[100万人以上1,000万人未満]　<選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
	対象となる本人の範囲 ※	特定個人情報ファイルの範囲と同様
	その妥当性	システムの安定した運用実現のため専門的な知識を有する民間事業者に委託する。

③委託先における取扱者数		[　　10人以上50人未満　　] <選択肢> 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[　]専用線　[　]電子メール　[　]電子記録媒体（フラッシュメモリを除く。） [　]フラッシュメモリ　[　]紙 [○]その他　（特定個人情報ファイルは提供していないが、サーバ設置場所、または中央情報処理センターにおける運用保守を行っている。）
⑤委託先名の確認方法		大阪市ホームページの入札契約情報にて確認できる。
⑥委託先名		株式会社　NTTデータ関西
再委託	⑦再委託の有無　※	[　　再委託する　　] <選択肢> 1）再委託する　2）再委託しない
再委託	⑧再委託の許諾方法	業務契約書の規定に基づく再委託承諾申請書の提出があった場合、申請内容を審査した結果、再委託が適当と判断した場合は再委託先に対し承諾書を交付する。
再委託	⑨再委託事項	統合基盤システムに関する製造、試験、環境構築（本番・保守）及び運用保守における一部業務
委託事項5		申請管理システム構築・運用保守業務
①委託内容		申請管理システムの運用・保守業務
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの一部] <選択肢> 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	[　　1万人以上10万人未満　　] <選択肢> 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲　※	特定個人情報ファイルの範囲と同様
	その妥当性	申請管理システムの安定した運用実現のために、専門的な知識を有する民間事業者にシステム構築業務と一体的に委託する。
③委託先における取扱者数		[　　] <選択肢> 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[　]専用線　[　]電子メール　[　]電子記録媒体（フラッシュメモリを除く。） [　]フラッシュメモリ　[　]紙 [○]その他　（特定個人情報ファイルは提供していないが、必要に応じてガバメントクラウド上のシステムを専用線で接続して直接操作を認めている。）
⑤委託先名の確認方法		大阪市ホームページの入札契約情報にて確認できる。
⑥委託先名		委託先事業者未定（今後調達予定）
再委託	⑦再委託の有無　※	[　　] <選択肢> 1）再委託する　2）再委託しない
再委託	⑧再委託の許諾方法	
再委託	⑨再委託事項	
委託事項11～15		
委託事項16～20		

5. 特定個人情報の提供・移転（委託に伴うものを除く。）	
提供・移転の有無	[○] 提供を行っている （ 60 ）件 [○] 移転を行っている （ 38 ）件 [ ] 行っていない
提供先1	番号法第19条第8号に基づく利用特定個人情報の提供に関する命令第2条の表に定める情報照会者（別紙1参照）
①法令上の根拠	番号法第19条第8号及び番号法第19条第8号に基づく利用特定個人情報の提供に関する命令第2条の表
②提供先における用途	番号法第19条第8号に基づく利用特定個人情報の提供に関する命令第2の表に定める各事務（別紙1参照）
③提供する情報	住基法第7条第4号に規定する住民票関係の情報であって主務省令で定めるもの
④提供する情報の対象となる本人の数	[100万人以上1,000万人未満] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	特定個人情報ファイルの範囲と同様
⑥提供方法	[○] 情報提供ネットワークシステム [ ] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [ ] その他 （ ）
⑦時期・頻度	情報提供ネットワークシステムを通じて特定個人情報の提供依頼のあった都度
提供先2～5	
提供先6～10	
提供先11～15	
提供先16～20	
移転先1	番号法第9条第1項別表に定める事務実施所管課（別紙2参照）
①法令上の根拠	番号法第9条第1項別表
②移転先における用途	番号法第9条別表に定める各事務（別紙2参照）
③移転する情報	住所、氏名、生年月日、性別等の住民基本台帳情報
④移転する情報の対象となる本人の数	[100万人以上1,000万人未満] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤移転する情報の対象となる本人の範囲	特定個人情報ファイルの範囲と同様
⑥移転方法	[ ] 庁内連携システム [ ] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [○] フラッシュメモリ [○] 紙 [○] その他 （ 統合基盤システム ）
⑦時期・頻度	住民基本台帳ファイルの更新の都度
移転先2～5	
移転先11～15	
移転先16～20	

6. 特定個人情報の保管・消去		
①保管場所 ※		＜特定個人情報の保管場所＞ ・特定個人情報は、システム用ファイルとしてガバメントクラウドの住民記録システムに格納することとしている。 なお、標準化以前の除票データについては、ガバメントクラウド上の除票管理システムに格納することとしている。 ・申請書等の紙媒体は鍵のかかるロッカーや保管庫で保管している。 ＜中間サーバ・プラットフォームにおける措置＞ ①中間サーバ・プラットフォームはデータセンターに設置し、データセンターへの入館及びサーバ室への入室を厳重に管理する。 ②特定個人情報は、サーバ室に設置される中間サーバのデータベース内に保存され、バックアップもデータベース上で保存される。 ＜ガバメントクラウドにおける措置＞ ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。 ＜申請管理システムにおける措置＞ 申請管理システムはガバメントクラウドで稼働するため、保管場所は「ガバメントクラウドにおける措置」に記載するとおりとする。
②保管期間	期間	[20年以上] ＜選択肢＞ 1）1年未満　2）1年　3）2年 4）3年　5）4年　6）5年 7）6年以上10年未満　8）10年以上20年未満　9）20年以上 10）定められていない
	その妥当性	・住民基本台帳に記載されている限り保管が必要。 ・住基法施行令第8条（住民票の消除）、第8条の2（日本の国籍の取得又は喪失による住民票の記載及び消除）、第10条（転居又は世帯変更による住民票の記載及び消除）若しくは第12条第3項（職権による住民票の記載等）の規定により削除された住民票について、住基法施行令第34条（保存）に基づいて150年間保管する。
③消去方法		＜住民記録システム＞ 住民基本台帳データベースに記録されたデータのうち、住民票の削除後150年を経過したデータをシステムにて一括して消去する仕組みとする。 【電子データ】 ・データについては、保管期間の満了後システムにてデータベースより削除する。 ・CD等の外部媒体については、物理的破壊を行う。 【紙書類】 ・申請書等の紙媒体については、外部業者による溶解処理を行う。 ＜中間サーバ・プラットフォームにおける措置＞ ①特定個人情報の消去は本市からの操作によって実施されるため、通常、中間サーバ・プラットフォームの保守・運用を行う事業者が特定個人情報を消去することはない。 ②ディスク交換やハード更改等の際は、中間サーバ・プラットフォームの保守・運用を行う事業者において、保存された情報が読み出しできないよう、物理的破壊により完全に消去する。 ＜ガバメントクラウドにおける措置＞ ①特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報を消去することはない。 ②クラウド事業者がHDDやSSDなどの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等にしたがって確実にデータを消去する。 ③既存システムについては、地方公共団体が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。 ＜申請管理システムにおける措置＞ ・申請管理システムはガバメントクラウドで稼働するため、保管場所は「ガバメントクラウドにおける措置」に記載するとおりとする。 ・サービス検索・電子申請機能（マイナポータルぴったりサービス）の電子申請データの取得に利用するDMZ（隔離された領域）内の連携サーバには個人番号付電子申請データを保有しない。 ・申請管理システムを利用する端末に一時的に記録した個人番号付電子申請データは、住民記録システムでの業務処理後は速やかに完全消去する。
7. 備考		

Ⅱ　特定個人情報ファイルの概要

1. 特定個人情報ファイル名		
本人確認情報ファイル		
2. 基本情報		
①ファイルの種類 ※		[　　システム用ファイル　　] ＜選択肢＞ 1）システム用ファイル 2）その他の電子ファイル（表計算ファイル等）
②対象となる本人の数		[　100万人以上1,000万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
③対象となる本人の範囲 ※		区域内の住民（住基法第5条（住民基本台帳の備付け）に基づき住民基本台帳に記録された住民を指す） ※住民基本台帳に記録されていた者で、転出等の事由により住民票が消除（死亡による消除を除く。）された者（以下「消除者」という。）を含む
	その必要性	住基ネットを通じて全国共通の本人確認を行うため、本特定個人情報ファイル(本人確認情報ファイル)において区域内の全ての住民の情報を保有し、住民票に記載されている住民全員の記録を常に正確に更新・管理・提供する必要があるため。
④記録される項目		[　10項目以上50項目未満　] ＜選択肢＞ 1）10項目未満　2）10項目以上50項目未満 3）50項目以上100項目未満　4）100項目以上
	主な記録項目 ※	・識別情報 [○] 個人番号　[　] 個人番号対応符号　[　] その他識別情報（内部番号） ・連絡先等情報 [○] 4情報（氏名、性別、生年月日、住所）　[　] 連絡先（電話番号等） [○] その他住民票関係情報 ・業務関係情報 [　] 国税関係情報　[　] 地方税関係情報　[　] 健康・医療関係情報 [　] 医療保険関係情報　[　] 児童福祉・子育て関係情報　[　] 障害者福祉関係情報 [　] 生活保護・社会福祉関係情報　[　] 介護・高齢者福祉関係情報 [　] 雇用・労働関係情報　[　] 年金関係情報　[　] 学校・教育関係情報 [　] 災害関係情報 [　] その他　（　　）
	その妥当性	・個人番号、4情報（氏名、性別、生年月日、住所）、その他住民票関係情報 住基ネットを通じて本人確認を行うために必要な情報として、住民票の記載等に係る本人確認情報（個人番号、4情報、住民票コード及びこれらの変更情報）を記録する必要があるため。
	全ての記録項目	別添2を参照。
⑤保有開始日		平成27年7月18日
⑥事務担当部署		各区役所住民情報事務所管課（24区、2出張所、北部・南部サービスセンター、南港ポートタウンサービスコーナー）、サービスカウンター（梅田、難波、天王寺）、郵送事務処理センター、市民局総務部住民情報担当

3. 特定個人情報の入手・使用		
①入手元 ※		[　] 本人又は本人の代理人 [　] 評価実施機関内の他部署　（　） [　] 行政機関・独立行政法人等　（　） [　] 地方公共団体・地方独立行政法人　（　） [　] 民間事業者　（　） [○] その他　（ 自部署　）
②入手方法		[　] 紙　[　] 電子記録媒体（フラッシュメモリを除く。）　[　] フラッシュメモリ [　] 電子メール　[　] 専用線　[　] 庁内連携システム [　] 情報提供ネットワークシステム [○] その他　（ 住民記録システム　）
③入手の時期・頻度		住民基本台帳への記載事項において、本人確認情報に係る変更又は新規作成が発生した都度入手する。
④入手に係る妥当性		法令に基づき住民に関する記録を正確に行う上で、住民に関する情報に変更があった又は新規作成された際は、住民からの申請等を受け、まず住民記録システムで情報を管理した上で、全国的なシステムである住基ネットに格納する必要があるため。
⑤本人への明示		市町村CSが住民記録システムより本人確認情報を入手することについて、住基法第30条の6（市町村長から都道府県知事への本人確認情報の通知等）及び平成14年6月10日総務省告示第334号（第6－7市町村長から都道府県知事への通知及び記録）に記載されている。
⑥使用目的 ※		住基ネットを通じて全国共通の本人確認を行うため、本特定個人情報ファイル（本人確認情報ファイル）において区域内の全ての住民の情報を保有し、住民票に記載されている住民全員の記録を常に正確に更新・管理・提供する。
	変更の妥当性	—
⑦使用の主体	使用部署 ※	各区役所住民情報事務所管課（24区、2出張所、北部・南部サービスセンター、南港ポートタウンサービスコーナー）、サービスカウンター（梅田、難波、天王寺）、郵送事務処理センター、市民局総務部住民情報担当
	使用者数	[　500人以上1,000人未満　] ＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
⑧使用方法 ※		・住民票の記載事項の変更又は新規作成が生じた場合、住民記録システムから当該本人確認情報の更新情報を受領し(住民記録システム→市町村CS)、受領した情報を元に本人確認情報ファイルを更新し、当該本人確認情報の更新情報を都道府県知事に通知する（市町村CS→都道府県サーバ）。 ・住民から提示された個人番号カードに登録された住民票コードをキーとして本人確認情報ファイルを検索し、画面に表示された本人確認情報と申請・届出書等の記載内容を照合し確認することで本人確認を行う（個人番号カード→市町村CS）。 ・住民票コード・個人番号又は4情報（氏名、住所、性別、生年月日）の組合せをキーに本人確認情報ファイルの検索を行う。 ・本人確認情報ファイルの内容が都道府県知事保存本人確認情報ファイル（都道府県サーバ）及び機構保存本人確認情報ファイル（全国サーバ）と整合することを確認するため、都道府県サーバ及び全国サーバに対し、整合性確認用本人確認情報を提供する（市町村CS→都道府県サーバ／全国サーバ）。
	情報の突合 ※	・本人確認情報ファイルを更新する際に、受領した本人確認情報に関する更新データと本人確認情報ファイルを、住民票コードをもとに突合する。 ・個人番号カードを用いて本人確認を行う際に、提示を受けた個人番号カードと本人確認情報ファイルを、住民票コードをもとに突合する。
	情報の統計分析 ※	個人に着目した分析・統計は行わず、本人確認情報の更新件数の集計等、事務処理実績の確認のための統計のみ行う。
	権利利益に影響を与え得る決定 ※	該当なし
⑨使用開始日		平成27年10月5日

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※		[委託する] <選択肢> 1）委託する 2）委託しない （ 2 ） 件
委託事項1		システム保守業務
①委託内容		市町村CS運用等保守作業
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体] <選択肢> 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	[100万人以上1,000万人未満] <選択肢> 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲 ※	特定個人情報ファイルの範囲と同様
	その妥当性	市町村CS運用の安定稼働のため、専門的な知識を有する民間事業者に委託している。 送付先情報ファイルにも個人番号が含まれるため、個人番号を含めた保守作業が必須となる。
③委託先における取扱者数		[10人以上50人未満] <選択肢> 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[ ] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [○] その他 （ 特定個人情報ファイルの提供はしていないが、必要に応じて本市指定の保守作業場所にて、システムの直接操作を認めている。 ）
⑤委託先名の確認方法		大阪市ホームページの入札契約情報にて確認できる。
⑥委託先名		株式会社 NTTデータ関西
再委託	⑦再委託の有無 ※	[再委託する] <選択肢> 1）再委託する 2）再委託しない
	⑧再委託の許諾方法	業務契約書の規定に基づく再委託承諾申請書の提出があった場合、申請内容を審査した結果、再委託が適当と判断した場合は再委託先に対し承諾書を交付する。
	⑨再委託事項	住民記録システム改修（一部の機能）、住民記録システム保守作業（ライブラリ管理等）等

委託事項2		バックアップ用媒体の運搬および保管業務委託
①委託内容		災害時等のデータ復旧のためバックアップデータを記録した外部記憶媒体の運搬および保管。 外部記憶媒体を保護ケースに格納し施錠したうえで遠隔地へ保管を委託する。また、当該データ必要時には本市へ当該媒体を格納した保護ケースを配送する。
②取扱いを委託する特定個人情報ファイルの範囲		［ 特定個人情報ファイルの全体 ］　＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	［ 100万人以上1,000万人未満 ］　＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲 ※	特定個人情報ファイルの範囲と同様
	その妥当性	災害時においてもシステムを復元し稼働を継続させるため、復元対象となる情報の保管を専門の民間事業者に委託している。なお、保管するのみで直接的に個人情報にアクセスすることはないが、基本的な個人情報の取り扱いについては契約条項に定めている。
③委託先における取扱者数		［ 10人以上50人未満 ］　＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		［ ］専用線　［ ］電子メール　［ ］電子記録媒体（フラッシュメモリを除く。） ［ ］フラッシュメモリ　［ ］紙 ［ ○ ］その他　（ 鍵付の保護ケースに媒体を格納し、委託業者に預けている。 ）
⑤委託先名の確認方法		大阪市ホームページの入札契約情報にて確認できる。
⑥委託先名		阪急阪神エステート・サービス株式会社
再委託	⑦再委託の有無 ※	［ 再委託しない ］　＜選択肢＞ 1）再委託する　2）再委託しない
	⑧再委託の許諾方法	
	⑨再委託事項	
委託事項6～10		
委託事項11～15		
委託事項16～20		

5. 特定個人情報の提供・移転（委託に伴うものを除く。）	
提供・移転の有無	[○] 提供を行っている （ 2 ）件 [ ] 移転を行っている （ ）件 [ ] 行っていない
提供先1	都道府県
①法令上の根拠	住基法第30条の6（市町村長から都道府県知事への本人確認情報の通知等）
②提供先における用途	・市町村より受領した住民の本人確認情報の変更情報（当該提供情報）を元に都道府県知事保存本人確認情報ファイルの当該住民に係る情報を更新し、機構に通知する。 ・住基法に基づいて、本人確認情報の提供及び利用等を行う。
③提供する情報	住民票コード、氏名、生年月日、性別、住所、個人番号、異動事由、異動年月日
④提供する情報の対象となる本人の数	[100万人以上1,000万人未満] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	「2. ③対象となる本人の範囲」と同上。
⑥提供方法	[ ] 情報提供ネットワークシステム [ ] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [○] その他 （ 住民基本台帳ネットワークシステム ）
⑦時期・頻度	住民基本台帳への記載事項において、本人確認情報に係る変更又は新規作成が発生した都度、随時。
提供先2	都道府県及び地方公共団体情報システム機構（以下「機構」という）
①法令上の根拠	住基法第14条（住民基本台帳の正確な記録を確保するための措置）
②提供先における用途	住民基本台帳の正確な記録を確保するために、本人確認情報ファイルの記載内容（当該提供情報）と都道府県知事保存本人確認情報ファイル及び機構保存本人確認情報ファイルの記載内容が整合することを確認する。
③提供する情報	住民票コード、氏名、生年月日、性別、住所、個人番号、異動事由、異動年月日
④提供する情報の対象となる本人の数	[100万人以上1,000万人未満] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	「2. ③対象となる本人の範囲」と同上。
⑥提供方法	[ ] 情報提供ネットワークシステム [ ] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [○] その他 （ 住民基本台帳ネットワークシステム ）
⑦時期・頻度	必要に応じて随時（1年に1回程度）
提供先3	
提供先4	
提供先5	
提供先6～10	
提供先11～15	
提供先16～20	

移転先1		
①法令上の根拠		
②移転先における用途		
③移転する情報		
④移転する情報の対象となる本人の数	[ ]	＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤移転する情報の対象となる本人の範囲		
⑥移転方法	[ ] 庁内連携システム [ ] 電子メール [ ] フラッシュメモリ [ ] その他 （ ）	[ ] 専用線 [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] 紙
⑦時期・頻度		
移転先2～5		
移転先6～10		
移転先11～15		
移転先16～20		
6．特定個人情報の保管・消去		
①保管場所 ※		＜特定個人情報の保管場所＞ ・特定個人情報は、システム用ファイルとして統合基盤システムのサーバ内に格納することとしている。 ・バックアップデータを記録したCD等の外部媒体は情報システム室内の保管庫に格納している。また、災害等に備えて大阪府外の遠隔地にも保管している。 ・申請書等の紙媒体は鍵のかかるロッカーや保管庫で保管している。 ＜保管場所の状況＞ ①サーバ ・統合基盤システムのサーバーは、入退館管理を24時間行う警備員を配置し、機械警備の実施や館内に監視カメラを設置する中央情報処理センター第二別館（民間データセンター）内の情報システム室に設置している。 ・中央情報処理センター第二別館（民間データセンター）は入退館時にID及び生体認証装置による認証を行っており、情報システム室はICカードと生体認証装置により入室制限を行っている。 ②外部媒体 ・情報システム室については、上記①に同じ。 ・遠隔地保管については、専門事業者に委託し、媒体を保護ケースに格納し施錠のうえ、入退館管理を行っている遠隔地で保管している。
②保管期間	期間	[20年以上] ＜選択肢＞ 1）1年未満　2）1年　3）2年 4）3年　5）4年　6）5年 7）6年以上10年未満　8）10年以上20年未満　9）20年以上 10）定められていない
	その妥当性	・住民票の記載の修正後の本人確認情報は、新たに記載の修正の通知を受けるまで保管する。 ・住民票の記載の修正前の本人確認情報（履歴情報）及び消除者の本人確認情報は、住民基本台帳法施行令第34条第2項（保存）に定める期間（150年間）保管する。
③消去方法		・保存期間が終了した本人確認情報は、システムにて一括して消去する仕組みとする。 ・電子データについては、保管期間の満了後システムにてデータベースより削除する。 ・CD等の外部媒体については、物理的破壊を行う。 ・申請書等の紙媒体については、外部業者による溶解処理を行う。
7．備考		

Ⅱ　特定個人情報ファイルの概要

1. 特定個人情報ファイル名		
送付先情報ファイル		
2. 基本情報		
①ファイルの種類 ※		[　　システム用ファイル　　] ＜選択肢＞ 1）システム用ファイル 2）その他の電子ファイル（表計算ファイル等）
②対象となる本人の数		[　100万人以上1,000万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
③対象となる本人の範囲 ※		区域内の住民（住基法第5条（住民基本台帳の備付け）に基づき住民基本台帳に記録された住民を指す）
	その必要性	番号法第7条第1項（指定及び通知）及び個人番号カード省令第7条（個人番号の通知）に基づき、個人番号通知書を個人番号の付番対象者に送付する必要がある。 また、通知カード所持者にあっては、個人番号カードは通知カードと引き換えに交付することとされている。 市町村は、法令に基づき、これらの事務の実施を機構に委任する。
④記録される項目		[　50項目以上100項目未満　] ＜選択肢＞ 1）10項目未満　2）10項目以上50項目未満 3）50項目以上100項目未満　4）100項目以上
	主な記録項目 ※	・識別情報 [○] 個人番号　[　] 個人番号対応符号　[　] その他識別情報（内部番号） ・連絡先等情報 [○] 4情報（氏名、性別、生年月日、住所）　[　] 連絡先（電話番号等） [○] その他住民票関係情報 ・業務関係情報 [　] 国税関係情報　[　] 地方税関係情報　[　] 健康・医療関係情報 [　] 医療保険関係情報　[　] 児童福祉・子育て関係情報　[　] 障害者福祉関係情報 [　] 生活保護・社会福祉関係情報　[　] 介護・高齢者福祉関係情報 [　] 雇用・労働関係情報　[　] 年金関係情報　[　] 学校・教育関係情報 [　] 災害関係情報 [○] その他　（　個人番号通知書及び交付申請書の送付先の情報　）
	その妥当性	・個人番号、4情報（氏名、性別、生年月日、住所）、その他住民票関係情報 個人番号カードの券面記載事項として、法令に規定された項目を記録する必要がある。 ・その他（個人番号通知書及び交付申請書の送付先の情報） 機構に対し、個人番号カード省令第23条の2（個人番号通知書及び個人番号カードに関し機構が処理する事務）に基づき個人番号通知書及び交付申請書の印刷、送付並びに個人番号カードの発行を機構が行うために、個人番号カードの券面記載事項のほか、個人番号通知書及び交付申請書の送付先に係る情報を記録する必要がある。
	全ての記録項目	別添2を参照。
⑤保有開始日		平成27年10月2日
⑥事務担当部署		各区役所住民情報事務所管課（24区、2出張所）、サービスカウンター（梅田、難波）、市民局総務部住民情報担当

3. 特定個人情報の入手・使用		
①入手元 ※		[　　] 本人又は本人の代理人 [　　] 評価実施機関内の他部署　（　　） [　　] 行政機関・独立行政法人等　（　　） [　　] 地方公共団体・地方独立行政法人　（　　） [　　] 民間事業者　（　　） [○] その他　（ 自部署　　）
②入手方法		[　　] 紙　[　　] 電子記録媒体（フラッシュメモリを除く。）　[　　] フラッシュメモリ [　　] 電子メール　[　　] 専用線　[　　] 庁内連携システム [　　] 情報提供ネットワークシステム [○] その他　（ 住民記録システム　　）
③入手の時期・頻度		個人番号通知書に係る送付先情報は、新たに個人番号の通知対象者が生じた都度入手する。
④入手に係る妥当性		送付先情報の提供手段として住基ネットを用いるため、市町村CSにデータを格納する必要がある。 また、提供手段として電子記録媒体を用いる場合には、暗号化の機能を備える市町村CSにおいて電子記録媒体を暗号化した後に提供する必要がある。
⑤本人への明示		
⑥使用目的 ※		個人番号カード省令第23条の2（個人番号通知書及び個人番号カードに関し機構が処理する事務）に基づき個人番号通知書及び交付申請書の印刷、送付並びに個人番号カードの発行を行う機構に対し、個人番号通知書及び交付申請書の送付先情報を提供するため。
	変更の妥当性	—
⑦使用の主体	使用部署 ※	各区役所住民情報事務所管課（24区、2出張所）、サービスカウンター（梅田、難波）、市民局総務部住民情報担当
	使用者数	[　500人以上1,000人未満　]　＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
⑧使用方法 ※		・住民記録システムより個人番号の通知対象者の情報を抽出し、個人番号通知書及び交付申請書等の印刷及び送付に係る事務を個人番号カード省令第23条の2（個人番号通知書及び個人番号カードに関し機構が処理する事務）に基づいて行う機構に対し提供する（住民記録システム→市町村CS又は電子記録媒体→個人番号カード管理システム（機構））。
	情報の突合 ※	入手した送付先情報に含まれる4情報（氏名、性別、生年月日、住所）等の変更の有無を確認する（最新の4情報等であることを確認する）ため、機構（全国サーバ）が保有する「機構保存本人確認情報」との情報の突合を行う。
	情報の統計分析 ※	送付先情報ファイルに記録される個人情報を用いた統計分析は行わない。
	権利利益に影響を与え得る決定 ※	該当なし
⑨使用開始日		平成27年10月5日

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※		[委託する] <選択肢> 1）委託する 2）委託しない （ 2 ） 件
委託事項1		システム保守業務
①委託内容		市町村CS運用等保守作業
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体] <選択肢> 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	[100万人以上1,000万人未満] <選択肢> 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲 ※	特定個人情報ファイルの範囲と同様
	その妥当性	市町村CS運用の安定稼働のため専門的な知識を有する民間事業者に委託している。 送付先情報ファイルにも個人番号が含まれるため、個人番号を含めた保守作業が必須となる。
③委託先における取扱者数		[10人以上50人未満] <選択肢> 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[ ]専用線 [ ]電子メール [ ]電子記録媒体（フラッシュメモリを除く。） [ ]フラッシュメモリ [ ]紙 [○]その他 （ 特定個人情報ファイルの提供はしていないが、必要に応じて本市指定の保守作業場所にて、システムの直接操作を認めている。 ）
⑤委託先名の確認方法		大阪市ホームページの入札契約情報にて確認できる。
⑥委託先名		株式会社 NTTデータ関西
再委託	⑦再委託の有無 ※	[再委託する] <選択肢> 1）再委託する 2）再委託しない
	⑧再委託の許諾方法	業務契約書の規定に基づく再委託承諾申請書の提出があった場合、申請内容を審査した結果、再委託が適当と判断した場合は再委託先に対し承諾書を交付する。
	⑨再委託事項	住民記録システム改修（一部の機能）、住民記録システム保守作業（ライブラリ管理等）等

委託事項2		バックアップ用媒体の運搬および保管業務委託
①委託内容		災害時等のデータ復旧のためバックアップデータを記録した外部記憶媒体の運搬および保管。 外部記憶媒体を保護ケースに格納し施錠したうえで遠隔地へ保管を委託する。また、当該データ必要時には本市へ当該媒体を格納した保護ケースを配送する。
②取扱いを委託する特定個人情報ファイルの範囲		［ 特定個人情報ファイルの全体 ］　＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	［ 100万人以上1,000万人未満 ］　＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲 ※	特定個人情報ファイルの範囲と同様。
	その妥当性	災害時においてもシステムを復元し稼働を継続させるため、復元対象となる情報の保管を専門の民間事業者に委託している。なお、保管するのみで直接的に個人情報にアクセスすることはないが、基本的な個人情報の取り扱いについては契約条項に定めている。
③委託先における取扱者数		［ 10人以上50人未満 ］　＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		［ ］専用線　［ ］電子メール　［ ］電子記録媒体（フラッシュメモリを除く。） ［ ］フラッシュメモリ　［ ］紙 ［ ○ ］その他　（ 鍵付の保護ケースに媒体を格納し、委託業者に預けている。 ）
⑤委託先名の確認方法		大阪市ホームページの入札契約情報にて確認できる。
⑥委託先名		阪急阪神エステート・サービス株式会社
再委託	⑦再委託の有無 ※	［ 再委託しない ］　＜選択肢＞ 1）再委託する　2）再委託しない
	⑧再委託の許諾方法	
	⑨再委託事項	
委託事項6～10		
委託事項11～15		
委託事項16～20		

5. 特定個人情報の提供・移転（委託に伴うものを除く。）	
提供・移転の有無	[○] 提供を行っている （ 1 ）件 [ ] 移転を行っている （ ）件 [ ] 行っていない
提供先1	地方公共団体情報システム機構（以下、「機構」という）
①法令上の根拠	個人番号カード省令第23条の2（個人番号通知書及び個人番号カードに関し機構が処理する事務）
②提供先における用途	個人番号カード省令第23条の2（個人番号通知書及び個人番号カードに関し機構が処理する事務）に基づき個人番号通知書及び交付申請書を印刷し、送付する。
③提供する情報	「2. ④記録される項目」と同様
④提供する情報の対象となる本人の数	[100万人以上1,000万人未満] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	「2. ③対象となる本人の範囲」と同様
⑥提供方法	[ ] 情報提供ネットワークシステム [ ] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [○] その他 （ 住基ネット ）
⑦時期・頻度	個人番号通知書に係る送付先情報は、新たに個人番号の通知対象者が生じた都度提供する。
提供先2～5	
提供先6～10	
提供先11～15	
提供先16～20	

移転先1		
①法令上の根拠		
②移転先における用途		
③移転する情報		
④移転する情報の対象となる本人の数	[ ]	＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤移転する情報の対象となる本人の範囲		
⑥移転方法	[ ] 庁内連携システム [ ] 電子メール [ ] フラッシュメモリ [ ] その他 （ ）	[ ] 専用線 [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] 紙
⑦時期・頻度		
移転先2～5		
移転先6～10		
移転先11～15		
移転先16～20		
6．特定個人情報の保管・消去		
①保管場所 ※	＜特定個人情報の保管場所＞ ・特定個人情報は、システム用ファイルとして統合基盤システムのサーバ内に格納することとしている。 ・バックアップデータを記録したCD等の外部媒体は情報システム室内の保管庫に格納している。また、災害等に備えて大阪府外の遠隔地にも保管している。 ・申請書等の紙媒体は鍵のかかるロッカーや保管庫で保管している。 ＜保管場所の状況＞ ①サーバ ・統合基盤システムのサーバーは、入退館管理を24時間行う警備員を配置し、機械警備の実施や館内に監視カメラを設置する中央情報処理センター第二別館（民間データセンター）内の情報システム室に設置している。 ・中央情報処理センター第二別館（民間データセンター）は入退館時にID及び生体認証装置による認証を行っており、情報システム室はICカードと生体認証装置により入室制限を行っている。 ②外部媒体 ・情報システム室については、上記①に同じ。 ・遠隔地保管については、専門事業者に委託し、媒体を保護ケースに格納し施錠のうえ、入退館管理を行っている遠隔地で保管している。	
②保管期間	期間	[1年未満] ＜選択肢＞ 1）1年未満　2）1年　3）2年 4）3年　5）4年　6）5年 7）6年以上10年未満　8）10年以上20年未満　9）20年以上 10）定められていない
	その妥当性	送付先情報は機構への提供のみに用いられ、送付後の変更は行わないことから、セキュリティ上、速やかに削除することが望ましいため。
③消去方法		・保存期間が終了した送付先情報は、システムにて一括して消去する仕組みとする。 ・電子データについては、保管期間の満了後システムにてデータベースより削除する。 ・CD等の外部媒体については、物理的破壊を行う。 ・申請書等の紙媒体については、外部業者による溶解処理を行う。
7．備考		

（別添2）特定個人情報ファイル記録項目

（1）住民基本台帳ファイル
1. 区コード、2. 整理番号1、3. 登録状態区分、4. 個人最新__削除区分、5. 増減区分、6. 最新フラグ、7. 個人最新__住外異動__連番、8. 個人最新__市内異動__連番、9. 個人最新__区内異動__連番、10. 個人最新__版数、11. 住民区分、12. 整理番号2、13. 世帯区分、14. 出力順位、15. 住民票コード、16. 個人番号、17. 改製年月日__元号区分、18. 改製年月日__年月日、19. 住定異動日__元号区分、20. 住定異動日__年月日、21. 住定届出日__元号区分、22. 住定届出日__年月日、23. 住定事由__異動事由コード、24. 住定事由__1__一部・全部区分、25. 住定事由__2__一部・全部区分、26. 現住所__自治体コード、27. 現住所__町丁目コード、28. 現住所__番、29. 現住所__号、30. 現住所__枝、31. 現住所__地番編集コード、32. 現住所__郵便番号、33. 現住所__方書、34. 現住所__管轄区分、35. 世帯主__整理番号1、36. 世帯主名__漢字氏名、37. 世帯主名__英字氏名、38. 消除事由__異動年月日__元号区分、39. 消除事由__異動年月日__年月日、40. 消除事由__届出年月日__元号区分、41. 消除事由__届出年月日__年月日、42. 消除事由__異動事由__異動事由コード、43. 消除事由__異動事由__1__一部・全部区分、44. 消除事由__異動事由__2__一部・全部区分、45. 消除事由__法務省異動事由発生日、46. 消除事由__法務省通知異動事由コード、47. 消除事由__職権処理異動事由詳細コード、48. 消除事由__消除事由区分、49. 消除事由__住所種別区分、50. 消除事由__定型事由コード、51. 消除事由__自治体コード、52. 消除事由__町丁目コード、53. 消除事由__漢字自治体、54. 消除事由__漢字町丁目、55. 消除事由__郵便番号、56. 消除事由__世帯主名__漢字氏名、57. 消除事由__世帯主名__英字氏名、58. 確定転出先住所__処理年月日__元号区分、59. 確定転出先住所__処理年月日__年月日、60. 確定転出先住所__異動年月日__元号区分、61. 確定転出先住所__異動年月日__年月日、62. 確定転出先住所__届出年月日__元号区分、63. 確定転出先住所__届出年月日__年月日、64. 確定転出先住所__異動事由__異動事由コード、65. 確定転出先住所__異動事由__1__一部・全部区分、66. 確定転出先住所__異動事由__2__一部・全部区分、67. 確定転出先住所__住所種別区分、68. 確定転出先住所__自治体コード、69. 確定転出先住所__町丁目コード、70. 確定転出先住所__漢字自治体、71. 確定転出先住所__漢字町丁目、72. 確定転出先住所__郵便番号、73. 確定転出先住所__世帯主名__漢字氏名、74. 確定転出先住所__世帯主名__英字氏名、75. 消除区分、76. 予定転出__確定日__年月日、77. 氏名__カナ氏名、78. 氏名__漢字氏名、79. 氏名__英字氏名、80. 検索用カナ氏、81. 検索用カナ名、82. 検索用カナミドル、83. 検索用漢字氏、84. 検索用漢字名、85. 検索用漢字ミドル、86. 検索用英字氏、87. 検索用英字名、88. 検索用英字ミドル、89. 通称名__カナ氏名、90. 通称名__漢字氏名、91. 検索用通称名カナ氏、92. 検索用通称名カナ名、93. 検索用通称名漢字氏、94. 検索用通称名漢字名、95. 生年月日__元号区分、96. 生年月日__年月日、97. 性別区分、98. 続柄コード1、99. 続柄コード2、100. 続柄コード3、101. 市民日__元号区分、102. 市民日__年月日、103. 市届出日__元号区分、104. 市届出日__年月日、105. 本籍地__住所種別区分、106. 本籍地__定型事由コード、107. 本籍地__自治体コード、108. 本籍地__町丁目コード、109. 本籍地__漢字自治体、110. 本籍地__漢字町丁目、111. 本籍地__郵便番号、112. 筆頭者__漢字氏名、113. 記載事由__異動年月日__元号区分、114. 記載事由__異動年月日__年月日、115. 記載事由__届出年月日__元号区分、116. 記載事由__届出年月日__年月日、117. 記載事由__異動事由__異動事由コード、118. 記載事由__異動事由__1__一部・全部区分、119. 記載事由__異動事由__2__一部・全部区分、120. 記載事由__法務省異動事由発生日、121. 記載事由__法務省通知異動事由コード、122. 記載事由__職権処理異動事由詳細コード、123. 記載事由__記載事由区分、124. 記載事由__住所種別区分、125. 記載事由__定型事由コード、126. 記載事由__自治体コード、127. 記載事由__町丁目コード、128. 記載事由__漢字自治体、129. 記載事由__漢字町丁目、130. 記載事由__郵便番号、131. 記載事由__世帯主名__漢字氏名、132. 記載事由__世帯主名__英字氏名、133. 国籍コード、134. 第30条の45に規定する区分、135. 在留資格コード、136. 在留期間等__年月コード、137. 在留期間等__日、138. 在留期間等の満了の日__元号区分、139. 在留期間等の満了の日__年月日、140. 在留カード等の番号、141. 交付日__元号区分、142. 交付日__年月日、143. 氏名のカタカナ表記、144. 設置場所コード、145. 更新番号、146. 端末ID、147. 更新年月日、148. 更新ユーザID、149. 画面・バッチID、150. 処理ID、151. レコード適用開始日

（2）本人確認情報ファイル
1. 住民票コード、2. 漢字氏名、3. 外字数（氏名）、4. ふりがな氏名、5. 清音化かな氏名、6. 生年月日、7. 性別、8. 市町村コード、9. 大字・字コード、10. 郵便番号、11. 住所、12. 外字数（住所）、13. 個人番号、14. 住民となった日、15. 住所を定めた日、16. 届出の年月日、17. 市町村コード（転入前）、18. 転入前住所、19. 外字数（転入前住所）、20. 続柄、21. 異動事由、22. 異動年月日、23. 異動事由詳細、24. 旧住民票コード、25. 住民票コード使用年月日、26. 依頼管理番号、27. 操作者ID、28. 操作端末ID、29. 更新順番号、30. 異常時更新順番号、31. 更新禁止フラグ、32. 予定者フラグ、33. 排他フラグ、34. 外字フラグ、35. レコード状況フラグ、36. タイムスタンプ、37.旧氏　漢字、38. 旧氏　外字数、39. 旧氏　ふりがな、40. 旧氏　外字変更連番

（3）送付先情報ファイル
1. 送付先管理番号、2. 送付先郵便番号、3. 送付先住所　漢字項目長、4. 送付先住所　漢字、5. 送付先住所　漢字外字数、6. 送付先氏名　漢字項目長、7. 送付先氏名　漢字、8. 送付先氏名　漢字　外字数、9. 市町村コード、10. 市町村名　項目長、11. 市町村名、12. 市町村郵便番号、13. 市町村住所　項目長、14. 市町村住所、15. 市町村住所　外字数、16. 市町村電話番号、17. 交付場所名　項目長、18. 交付場所名、19. 交付場所名　外字数、20. 交付場所郵便番号、21. 交付場所住所　項目長、22. 交付場所住所、23. 交付場所住所　外字数、24. 交付場所電話番号、25. カード送付場所名　項目長、26. カード送付場所名、27. カード送付場所名　外字数、28. カード送付場所郵便番号、29. カード送付場所住所　項目長、30. カード送付場所住所、31. カード送付場所住所　外字数、32. カード送付場所電話番号、33. 対象となる人数、34. 処理年月日、35. 操作者ID、36. 操作端末ID、37. 印刷区分、38. 住民票コード、39. 氏名　漢字項目長、40. 氏名　漢字、41. 氏名　漢字　外字数、42. 氏名　かな項目長、43. 氏名　かな、44. 郵便番号、45. 住所　項目長、46. 住所、47. 住所　外字数、48. 生年月日、49. 性別、50. 個人番号、51. 第30条の45に規定する区分、52. 在留期間の満了の日、53. 代替文字変換結果、54. 代替文字氏名　項目長、55. 代替文字氏名、56. 代替文字住所　項目長、57. 代替文字住所、58. 代替文字氏名位置情報、59. 代替文字住所位置情報、60. 外字フラグ、61. 外字パターン、62.旧氏　漢字、63. 旧氏　外字数、64. 旧氏　ふりがな、65. 旧氏　外字変更連番、66. ローマ字　氏名、67. ローマ字　旧氏

＜統合基盤システム＞
（団体内宛名）
1. 個人番号、2. 統合宛名番号、3. 氏名（漢字）、4. 氏名（カナ）、5. 住所、6. 生年月日、7. 性別、8. 業務システム固有宛名番号、9. 異動事由、10. 識別項目1、11. 識別項目2、12. 識別項目3、13. 識別項目4、14. 登録日時、15. 更新日時

＜中間サーバー＞
（中間サーバー）
1. 情報提供用識別符号、2. 情報提供記録

Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※（7. リスク1⑨を除く。）

1. 特定個人情報ファイル名	
住民基本台帳ファイル	
2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）	
リスク1： 目的外の入手が行われるリスク	
対象者以外の情報の入手を防止するための措置の内容	【本人からの情報入手】 ・本人が書面を提出する際に、本人が本人（世帯員含む。以降、同様の定義とする）以外の情報を誤って記載することがないようチェックを行う。 ・住民基本台帳事務に係る各種申請に関し、運転免許証、個人番号カード、住基ネットによる本人確認などで申請者の本人確認を行う。 【他部署からの情報入手】 ・他部署からの情報入手は、原則システムによる連携とし、他部署の業務システムおよび住民記録システムで共有する個人を特定するためのキー項目にて対象者を特定することにより、対象者以外の情報を入手するリスクを低減する。
必要な情報以外を入手することを防止するための措置の内容	【本人からの情報入手】 ・本人が必要な情報以外を誤って記載することがないような書面様式とする。また、記載要領を充実し、必要最小限の情報の記載となるようにする。 【他部署からの情報入手】 ・情報入手の際、不要な項目は取得できないようにすることにより、対象外の項目を入手するリスクを低減する。
その他の措置の内容	
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2： 不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	【本人からの情報入手】 ・個人情報の収集にあたっては、本人から収集することを原則としている。 ・権利のない者からの届出を受付ないように届出人要件の確認を徹底する。 【他部署からの情報入手】 ・住民記録システム、および統合基盤システムへのアクセスは権限が付与された者しか利用できないよう認証機能を設けている。また、業務に必要な情報のみを入手できるようにする。
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3： 入手した特定個人情報が不正確であるリスク	
入手の際の本人確認の措置の内容	住民基本台帳事務に係る各種申請に関し、本人確認は運転免許証、個人番号カード、住基ネットにより行う。
個人番号の真正性確認の措置の内容	個人番号の生成元である機構が設置・管理する全国サーバから住民票コードに対応する個人番号を適切に取得できることを、システムにより担保する。
特定個人情報の正確性確保の措置の内容	【本人からの情報入手】 ・受付時に転出証明書や住基ネットによる住民情報の照合を行う。 ・届出書内容と照合内容が異なった場合は、届出人へのヒアリングによる確認を行う。 ・郵送による転出届や代理人による届出時など、届出内容の事実を確認する必要があるときは、本人に対して受理通知を郵送し届出内容の確認を行う。 ・システムへの入力は、届出内容の入力作業から決裁まで、複数人による確認作業を経て登録を完了させる。 【他部署からの情報入手】 ・住民票の記載事項の情報については、他部署で管理するシステムから情報を定期的に取得する。
その他の措置の内容	
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	【本人からの情報入手】 ・届出関係の書類は、受付後は専用の収納ケースに保管する。 ・システム画面が市民側から見えないように端末機を配置する。 ・LGWAN系ネットワークとマイナンバー利用事務系ネットワークの間にDMZ（隔離された領域）を設け、申請管理システムから外部への直接通信を遮断することにより、安全を確保している。また外部とのネットワーク接続について、境界FWや連携サーバで接続先との通信を限定している。 【他部署からの情報入手】 ・他部署が管理する業務システムから入手する際は本市専用回線によるセキュアなネットワーク利用に限定する。 【その他】 ・情報セキュリティポリシーの周知等を職員に行う。また、情報漏えい等の防止のため、責任者の許可なく端末機又は記録媒体等を執務室以外に持出すことの禁止や、アクセス権限の管理、システムへのアクセス記録、コンピュータウィルス対策などを実施。 ・定期的および随時にウイルスソフトウェアの更新を行う。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置	

3. 特定個人情報の使用

リスク1： 目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク	
宛名システム等における措置の内容	・統合基盤システム（統合宛名番号付番機能、宛名情報等管理機能）に接続できるシステムは番号法で定められたものに限定しており、番号法に関係しないシステムが連携することはできない。 ・統合基盤システム（統合宛名番号付番機能、宛名情報等管理機能）から住民記録システムには直接アクセスできない仕組みのため、統合基盤システム（統合宛名番号付番機能、宛名情報等管理機能）が情報の紐付けを行うことはできない。 ・統合基盤システム（統合宛名番号付番機能、宛名情報等管理機能）には個別業務の特定個人情報を保有しない。 ・番号法に関係する事務を行う部署において、権限を付与された者のみ統合基盤システム（統合宛名番号付番機能、宛名情報等管理機能）にアクセス可能な仕組みとする。
事務で使用するその他のシステムにおける措置の内容	・住民記録システムでは、他のシステムとの紐付け機能を有していないため、必要のない情報との紐付けは行えない。 ・住民記録システム及び統合基盤システムは、中間サーバには番号法において各事務で提供が求められた情報のみを登録・変更できる仕組みとする。
その他の措置の内容	
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている

リスク2： 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク		
ユーザ認証の管理		［　行っている　］　＜選択肢＞ 1）行っている　2）行っていない
	具体的な管理方法	【認証方法】 ＜住民記録システムにおける措置＞ ・住民記録システムを利用する必要がある職員を特定し、個人ごとにユーザーIDを割り当てるとともに、IDとパスワードによる認証を行っている。 ・ネットワークユーザIDについては、管理者が管理し、人事異動等でシステム操作者に変更があれば、無効の設定を行う。パスワードはシステム的に変更させる設定としている。 ・パスワードは定期的に変更するよう周知するとともにシステム的に変更させる設定としている。 ＜統合基盤システムにおける措置＞ ・統合基盤システムへの利用権限を持つ従事者にのみユーザIDを付与し、ユーザIDとパスワードによる認証、生体情報（指静脈）による認証を行う。 ・パスワードは定期的及び随時に変更するよう周知するとともにシステム的に変更させる設定としている。 ＜申請管理システムにおける措置＞ ・申請管理システムを利用する必要がある職員を特定し、適切なユーザ割り当て及び認証を行う。 【なりすまし防止策】 従事者は以下を遵守し、利用ユーザIDを適切に管理する。 ・パスワードは第三者に知られないように管理する。 ・パスワードを秘密にし、パスワードの照会等には一切応じない。 ・パスワードは十分な長さとし、文字列は想像しにくいものとする。 ・パスワードは定期的に変更する。 ・端末機等のパスワードの記憶機能を利用しない。 ・パスワードが流出した可能性がある場合は、速やかに端末機管理者に報告し、パスワードを変更する。 ・使用する機器や記録媒体について、権限を有しない者の使用や閲覧を防止するため、端末から離れる場合にはログオフにする等適切な措置を講じる。
アクセス権限の発効・失効の管理		［　行っている　］　＜選択肢＞ 1）行っている　2）行っていない
	具体的な管理方法	＜住民記録システムにおける措置＞ 【アクセス権限の発効管理】 ・従事者が所属する部署、住民記録システムを所管する部署の管理者が業務上必要なユーザIDを確認し、アクセス権限管理を行う管理者へ発効の申請を行う。 【アクセス権限の失効管理】 ・従事者が所属する部署、住民記録システムを所管する部署の管理者が業務上不要となったユーザIDを確認し、アクセス権限管理を行う管理者へ失効の申請を行う。 ＜統合基盤システムにおける措置＞ 【アクセス権限の発効管理】 ・統合基盤システムを操作する従事者の権限に応じたユーザID、アクセス権限の割付を行う。 【アクセス権限の失効管理】 ・担当替え等により操作権限を無くした者のユーザIDやアクセス権限について利用無効や権限削除を行う。 ＜申請管理システムにおける措置＞ 【アクセス権限の発効管理】 ・申請管理システムを操作する従事者の権限に応じたユーザID、アクセス権限の割付を行う。 【アクセス権限の失効管理】 ・担当替え等により操作権限を無くした者のユーザIDやアクセス権限について利用無効や権限削除を行う。

アクセス権限の管理		[　行っている　] <選択肢> 1）行っている　2）行っていない
	具体的な管理方法	<住民記録システムにおける措置> ・共用IDは発行せず、必ず個人に対しユーザIDを発行する。 ・ユーザID単位で業務権限を設定し、システム内で利用可能な業務を制限している。 ・ユーザIDやアクセス権を住民記録システム担当課長と事業所管課が定期的に確認し、業務上アクセスが不要となったIDやアクセス権を変更又は削除する。 <統合基盤システムにおける措置> ・操作部署や住民記録システムの管理者からの申請に基づき、従事者へユーザIDおよび権限を付与する。担当替え等の際は、システムおよび管理者により利用を無効とする。 <申請管理システムにおける措置> ・共用IDは発行せず、必ず個人に対しユーザIDを発行する。 ・ユーザID単位で業務権限を設定し、システム内で閲覧・審査可能な業務を制限している。 ・担当替え等の際は、管理者により利用を無効とする。 ・定期的にユーザID一覧とアクセス権限の突合を行い確認する。
特定個人情報の使用の記録		[　記録を残している　] <選択肢> 1）記録を残している　2）記録を残していない
	具体的な方法	<住基記録システムにおける措置> ・住基記録システムへのログイン記録、個人を特定した検索及び特定後の操作ログの記録を行う。操作者は個人まで特定でき、記録は永年保存する。 <統合基盤システムにおける措置> ・システムの操作履歴（アクセスログ・操作ログ）を記録する。 ・操作履歴について、各事務運用で必要となる期間と同一の期間、保管する。 <申請管理システムにおける措置> ・システムの操作履歴（アクセスログ・操作ログ）を記録する。 ・操作履歴について、各事務運用で必要となる期間と同一の期間、保管する。
その他の措置の内容		
リスクへの対策は十分か		[　十分である　] <選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3：従業者が事務外で使用するリスク		
リスクに対する措置の内容		【職員の情報管理】 ・特定個人情報の利用を事務の目的の達成に必要な範囲内に限定し、事務目的外の利用・提供を禁止している。 ・研修の実施等により、個人情報保護及び情報セキュリティ意識の向上を図る。 ・利用システムに関する実施手順及び知識について研修を行う。 ・住民記録システム、統合基盤システム及び申請管理システム利用時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容を記録し、不適切な利用を抑止する。 【委託事業者の情報管理】 ・委託事業者に対しては目的外利用禁止を契約で定めており、従事者の教育訓練を義務付けている。 【職員の違反措置】 ・特定個人情報の使用記録より必要に応じて記録の解析を行い、事務外の利用有無を確認する。 ・違反行為を行った場合は法の罰則規定により措置を講ずる。なお、本市では懲戒処分に関する指針により、次の事項の違反時には懲戒処分の対象としており、事務外の使用を抑制している。 　個人情報の漏えい 　個人情報の目的外利用 　情報セキュリティポリシー違反
リスクへの対策は十分か		[　十分である　] <選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている

リスク4： 特定個人情報ファイルが不正に複製されるリスク	
リスクに対する措置の内容	【職員の情報管理】 ・システムの運用に関わる職員を対象に、システム及び当該システムにより処理されるデータに関わる情報セキュリティの実施手順並びに実施に必要な知識及び技術について研修を行う。 【委託事業者の情報管理】 ・委託先に対しては委託契約書にてデータの無断使用及び第三者への提供の禁止や、複写及び複製の禁止をしている。さらに、委託事業者において、当該従事者に対して情報セキュリティ研修を実施していることを確認している。 ＜住民記録システムにおける措置＞ ・住民記録システム利用時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容が記録されるため、不適切な利用を抑止する。 ・USBメモリやCD等の外部記録媒体への書き込みをシステム側で禁止している。 ＜統合基盤システムにおける措置＞ ・統合基盤システム利用時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容が記録されるため、不適切な利用を抑止する。 ＜申請管理システムにおける措置＞ ・申請管理システムから取得した個人番号付電子申請データ等のデータについて、改ざんや業務目的以外の複製を禁止する。
リスクへの対策は十分か	[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置	

4. 特定個人情報ファイルの取扱いの委託		[　　] 委託しない
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク		
情報保護管理体制の確認	【業者選定時】 ・委託先を選定する際の要件に、プライバシーマークを取得していることもしくはISMS（情報セキュリティマネジメントシステム）の認証を受けていることを義務付けている。 【契約時】 ・契約書において次の事項を定めている。 ア 個人情報保護に関する規程、体制の整備 イ 個人情報保護に関する安全管理措置 ウ 情報セキュリティ対策の実施責任者の配置 ・適切な社内における情報保護管理体制が構築されているか、管理体制の説明を求め確認している。 ・必要に応じ、事業者の管理記録簿の確認又は作業場所の立入検査等を実施する。	
特定個人情報ファイルの閲覧者・更新者の制限	[　制限している　]	＜選択肢＞ 1）制限している　2）制限していない
具体的な制限方法	委託契約書に以下の規定を設ける。 ①アクセス権限を付与する業務員の名簿の提出と、それ以外の者が作業場所に立ち入ることを禁止している。 ②データの機密保持に関する事項を明記し、委託処理の際にデータ保護に関する委託先の規程の確認を行っている。 ③委託事業者に対しては業務外で使用しないように委託契約書に定め、機密保護等の誓約書を提出させている。 ④委託事業者において、当該職員に対して情報セキュリティ研修を実施していることを確認している。	
特定個人情報ファイルの取扱いの記録	[　記録を残している　]	＜選択肢＞ 1）記録を残している　2）記録を残していない
具体的な方法	・特定個人情報が記録されたサーバ等での作業については、事前に作業報告の提出を求める。 ・システム作業のためにサーバ等のメンテナンス用のID、パスワード及びデータベースのメンテナンス用ID、パスワードを利用させており、当日の作業報告と照合することで作業者の特定ができる。 ・上記の作業実績等については、磁気ディスクに記録し毎日蓄積・保存する。保存した記録については、1か月分を磁気ディスクにまとめて保管委託を行っている。 ・システムの改修や設定変更に係る作業については、作業対象となるOSやミドルウェアが保有する機能によりID単位の操作内容が記録される。	
特定個人情報の提供ルール	[　定めている　]	＜選択肢＞ 1）定めている　2）定めていない
委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	委託先から第三者への特定個人情報の提供は認めていない。	
委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	・委託先へ特定個人情報ファイルを提供することはなく、特定個人情報を取扱う作業を行う場合は本庁舎等設置端末を利用するなど、特定の作業場所で行うこととしている。 ・委託元は、必要があると認めるときは、委託先の個人情報等の保護状況について立入検査を実施する。	
特定個人情報の消去ルール	[　定めていない　]	＜選択肢＞ 1）定めている　2）定めていない
ルールの内容及びルール遵守の確認方法	委託事業者には特定個人情報の持ち出しは許可していないため、消去対象の情報はない。	

委託契約書中の特定個人情報ファイルの取扱いに関する規定		[　　定めている　　] ＜選択肢＞ 1）定めている　2）定めていない
	規定の内容	・漏えい、滅失、き損等の防止その他個人情報等の保護に必要な体制の整備及び措置を講じなければならない ・個人情報等の授受・搬送・保管・廃棄等について、管理責任者を定める ・個人情報等の管理が適切でないと認められる場合、委託業者に対し改善を求めるとともに、個人情報等の管理状況を適切であると認めるまで委託業務を中止させることができる ・目的外利用の禁止及び第三者への提供禁止 ・個人情報等の外部への持ち出し禁止 ・個人情報等を複写又は複製禁止(本市の同意を得た場合を除く) ・個人情報等の保護状況について立入検査を実施することが可能 ・一括再委託等の禁止
再委託先による特定個人情報ファイルの適切な取扱いの確保		[　　十分に行っている　　] ＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない　4）再委託していない
	具体的な方法	・個人情報保護の遵守を契約書に記載している ・業務に対する再委託先従事者の名簿提出を義務付けている ・秘密保持義務に関し覚書を交わしている ・情報セキュリティ確認書（※）により個人情報保護に関する必要な措置等について誓約させている （※）委託契約に際し、再委託先から委託先に対して提出させており、契約書に添付されている。
その他の措置の内容		
リスクへの対策は十分か		[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		

5．特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		**[　　] 提供・移転しない**
リスク1：　不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録		[　　記録を残している　　] ＜選択肢＞ 1）記録を残している　2）記録を残していない
	具体的な方法	【提供】 ・情報提供ネットワークシステムを通じない特定個人情報の提供は行わない。 【移転】 ・移転については、住民記録システムから対象となる業務システムに対し、オペレータが操作することなく決められた時間に自動的に移転される。また、その内容は全て記録するように構築する。
特定個人情報の提供・移転に関するルール		[　　定めている　　] ＜選択肢＞ 1）定めている　2）定めていない
	ルールの内容及びルール遵守の確認方法	【提供】 ・情報提供ネットワークシステムを通じない特定個人情報の提供は行わない。 【移転】 ・特定個人情報の移転については、番号法の規定に基づき、認められる範囲内で提供を行う。また特定個人情報保護の理解度を高めるために、教育・指導を行う。
その他の措置の内容		USBメモリやCD等の外部記録媒体への書き込みをシステム側で禁止する
リスクへの対策は十分か		[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2：　不適切な方法で提供・移転が行われるリスク		
リスクに対する措置の内容		【提供】 ・情報提供ネットワークシステムを通じない特定個人情報の提供は行わない。 【移転】 ・住民記録システムから対象のシステムに向け、指定の日時に指定した情報を抽出するようシステムを構築し、抽出した情報を対象システムに引き渡して移転を行っている。
リスクへの対策は十分か		[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

リスク3： 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク	
リスクに対する措置の内容	【提供】 ・情報提供ネットワークシステムを通じない特定個人情報の提供は行わない。 【移転】 ・住民記録システムでは本業務で保有する情報をすべて連携することはできず、番号法に基づき認められる情報のみしか移転できないよう、仕組みとして担保されている。また、決められた移転先のみにしか情報の移転ができない仕組みとなっている。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置	

6. 情報提供ネットワークシステムとの接続	**[○] 接続しない（入手）**	**[ ] 接続しない（提供）**
リスク1： 目的外の入手が行われるリスク		
リスクに対する措置の内容		
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている	
リスク2： 安全が保たれない方法によって入手が行われるリスク		
リスクに対する措置の内容		
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている	
リスク3： 入手した特定個人情報が不正確であるリスク		
リスクに対する措置の内容		
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている	
リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク		
リスクに対する措置の内容		
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている	

リスク5： 不正な提供が行われるリスク	
リスクに対する措置の内容	＜住民記録システムの運用における措置＞ ①情報提供ネットワークシステムにおける情報連携においては、中間サーバに保有されている情報のみが連携されることになっており、中間サーバに保有される特定個人情報は、番号法の規定に基づき定められた情報のみとなっていることから、不正に提供されるリスクに対応している。 ②情報提供機能（※）により、情報提供ネットワークシステムに情報提供を行う際には、情報提供ネットワークシステムから情報提供許可証と情報照会者へたどり着くための経路情報を受領し、照会内容に対応した情報を自動で生成して送付することで、特定個人情報が不正に提供されるリスクに対応している。 ③特に慎重な対応が求められる情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報が不正に提供されるリスクに対応している。 （※）情報提供ネットワークシステムを使用した特定個人情報の提供の要求の受領及び情報提供を行う機能。 ＜中間サーバ・ソフトウェアにおける措置＞ ①情報提供機能（※）により、情報提供ネットワークシステムにおける照会許可用照合リストを情報提供ネットワークシステムから入手し、中間サーバにも格納して、情報提供機能により、照会許可用照合リストに基づき情報連携が認められた特定個人情報の提供の要求であるかチェックを実施している。 ②情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供ネットワークシステムから情報提供許可証と情報照会者へたどり着くための経路情報を受領し、照会内容に対応した情報を自動で生成して送付することで、特定個人情報が不正に提供されるリスクに対応している。 ③特に慎重な対応が求められる情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報が不正に提供されるリスクに対応している。 ④中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）情報提供ネットワークシステムを使用した特定個人情報の提供の要求の受領及び情報提供を行う機能。
リスクへの対策は十分か	[十分である]　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

リスク6： 不適切な方法で提供されるリスク	
リスクに対する措置の内容	＜中間サーバ・ソフトウェアにおける措置＞ ①セキュリティ管理機能（※）により、情報提供ネットワークシステムに送信する情報は、情報照会者から受領した暗号化鍵で暗号化を適切に実施した上で提供を行う仕組みになっている。 ②中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）暗号化・復号機能と、鍵情報及び照会許可用照合リストを管理する機能。 ＜中間サーバ・プラットフォームにおける措置＞ ①中間サーバと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、不適切な方法で提供されるリスクに対応している。 ②中間サーバと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ③中間サーバ・プラットフォームの保守・運用を行う事業者においては、特定個人情報に係る業務にはアクセスができないよう管理を行い、不適切な方法での情報提供を行えないよう管理している。 ＜中間サーバの運用における措置＞ セキュリティ実施手順等について定期的に職員へ研修を行う。また、情報漏えい等の防止のため、管理者の許可なく端末機又は記録媒体等を執務室以外に持出すことの禁止、アクセス権限の管理、システムへのアクセス記録を実施する。
リスクへの対策は十分か	[十分である]　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

リスク7： 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク	
リスクに対する措置の内容	＜住民記録システムの運用における措置＞ ①情報提供ネットワークシステムにおける情報連携においては、中間サーバに保有されている情報のみが連携されることになっており、中間サーバに保有される特定個人情報は、番号法の規定に基づき定められた情報のみとなっていることから、誤った情報の提供が行われるリスクに対応している。 ＜中間サーバ・ソフトウェアにおける措置＞ ①情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供許可証と情報照会者への経路情報を受領した上で、情報照会内容に対応した情報提供をすることで、誤った相手に特定個人情報が提供されるリスクに対応している。 ②情報提供データベース管理機能（※）により、「情報提供データベースへのインポートデータ」の形式チェックと、接続端末の画面表示等により情報提供データベースの内容を確認できる手段を準備することで、誤った特定個人情報を提供してしまうリスクに対応している。 ③情報提供データベース管理機能では、情報提供データベースの副本データを既存業務システムの原本と照合するためのエクスポートデータを出力する機能を有している。 （※）特定個人情報を副本として保存・管理する機能
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている

情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置
＜中間サーバ・ソフトウェアにおける措置＞ ①中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 ②情報連携においてのみ、情報提供用個人識別符号を用いることがシステム上担保されており、不正な名寄せが行われるリスクに対応している。 ＜中間サーバ・プラットフォームにおける措置＞ ①中間サーバと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ②中間サーバと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ③中間サーバ・プラットフォームでは、特定個人情報を管理するデータベースを地方公共団体ごとに区分管理（アクセス制御）しており、中間サーバ・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 ④特定個人情報の管理を地方公共団体のみが行うことで、中間サーバ・プラットフォームの保守・運用を行う事業者における情報漏えい等のリスクを極小化する。

7. 特定個人情報の保管・消去		
リスク1： 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[政府機関ではない]	<選択肢> 1）特に力を入れて遵守している 2）十分に遵守している 3）十分に遵守していない 4）政府機関ではない
②安全管理体制	[十分に整備している]	<選択肢> 1）特に力を入れて整備している 2）十分に整備している 3）十分に整備していない
③安全管理規程	[十分に整備している]	<選択肢> 1）特に力を入れて整備している 2）十分に整備している 3）十分に整備していない
④安全管理体制・規程の職員への周知	[十分に周知している]	<選択肢> 1）特に力を入れて周知している 2）十分に周知している 3）十分に周知していない
⑤物理的対策	[十分に行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
具体的な対策の内容	【中間サーバ・プラットフォームにおける措置】 ・中間サーバ・プラットフォームをデータセンターに構築し、設置場所への入退室者管理、有人監視及び施錠管理をすることとしている。また、設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。 【ガバメントクラウドにおける措置】 ①ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。 ②事前に許可されていない装置等に関しては、外部に持出できないこととしている。 【申請管理システムにおける措置】 ・申請管理システムはガバメントクラウド上で稼働するため、「ガバメントクラウドにおける措置」に記載のとおり。 ・申請管理システム接続端末の設置場所については業務時間外は施錠し入退室できなくするなどの物理的対策を講じる。	

⑥技術的対策		[　　十分に行っている　　] ＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない
	具体的な対策の内容	＜中間サーバ･プラットフォームにおける措置＞ ･中間サーバ･プラットフォームをデータセンターに設置し、設置場所への入退出者管理、友人監視及び施錠管理をすることとしている。また、設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。 ･中間サーバ･プラットフォームではUTM（コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置）等を導入し、アクセス制限、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 ･中間サーバ･プラットフォームでは、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ･導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ＜ガバメントクラウドにおける措置＞ ①国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。 ②地方公共団体が委託したASP（「地方公共団体情報システムのガバメントクラウドの利用に関する基準」（以下「利用基準」という。）に規定する「ASP」をいう。以下同じ。）又はガバメントクラウド運用管理補助者（利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。）は、ガバメントクラウドが提供するマネージドサービスにより、ネットワークアクティビティ、データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに、ログ管理を行う。 ③クラウド事業者は、ガバメントクラウドに対するセキュリティの脅威に対し、脅威検出やDDos対策を24時間365日講じる。 ④クラウド事業者は、ガバメントクラウドに対し、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ⑤地方公共団体が委託したASP又はガバメントクラウド運用管理補助者は、導入しているOS及びミドルウエアについて、必要に応じてセキュリティパッチの適用を行う。 ⑥ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。 ⑦地方公共団体やASP又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。 ⑧地方公共団体が管理する業務データは、国及びクラウド事業者がアクセスできないよう制御を講じる。 ＜申請管理システムにおける措置＞ ･申請管理システムはガバメントクラウド上で稼働するため、「ガバメントクラウドにおける措置」に記載するとおり。 ･LGWAN系ネットワークとマイナンバー利用事務系ネットワークの間にDMZ（隔離された領域）を設け、申請管理システムから外部への直接通信を遮断することにより、安全を確保している。また外部とのネットワーク接続について、境界FWや連携サーバで接続先との通信を限定している。
⑦バックアップ		[　　十分に行っている　　] ＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない
⑧事故発生時手順の策定・周知		[　　十分に行っている　　] ＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか		[　発生なし　] ＜選択肢＞ 1）発生あり　2）発生なし
	その内容	
	再発防止策の内容	
⑩死者の個人番号		[　　保管している　　] ＜選択肢＞ 1）保管している　2）保管していない
	具体的な保管方法	死者の個人番号は住基法第8条（住民票の記載等）の規定により削除された住民票について、住基法施行令第34条（保存）において定める期間（150年間）、システム上にて保管する。
その他の措置の内容		
リスクへの対策は十分か		[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

リスク2： 特定個人情報が古い情報のまま保管され続けるリスク	
リスクに対する措置の内容	＜住民記録システムにおける措置＞ ・住基法第14条第1項（住民基本台帳の正確な記録を確保するための措置）の規定に基づき調査等を実施することにより、住民基本台帳の正確な記録を確保する。 ＜統合基盤システムにおける措置＞ ・統合宛名に係る住民の4情報（氏名、性別、生年月日、住所）については、住基等システムから情報を提供し、最新の状態を維持する。 ＜申請管理システムにおける措置＞ ・申請データの再申請や申請情報の訂正が発生した場合には古い情報で審査等を行わないよう、履歴管理を行う。 ・サービス検索・電子申請機能（マイナポータルぴったりサービス）の電子申請データの取得に利用するDMZ（隔離された領域）内の連携サーバには個人番号付電子申請データを保有しない。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク3： 特定個人情報が消去されずいつまでも存在するリスク	
消去手順	[定めている] ＜選択肢＞ 1）定めている 2）定めていない
手順の内容	・データについては、保存期間の経過後システムにてデータベースより削除する。 ・CD等の外部媒体については、物理的破壊を行う。 ・申請書等の紙媒体については、外部業者による溶解処理を行う。 ・ガバメントクラウドにおいては、データの復元がなされないよう、クラウド事業者において、NIST800-88、ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去する。
その他の措置の内容	
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置	

Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※（7. リスク1⑨を除く。）

1. 特定個人情報ファイル名	
本人確認情報ファイル	
2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）	
リスク1： 目的外の入手が行われるリスク	
対象者以外の情報の入手を防止するための措置の内容	【本人からの情報入手】 ・本人確認情報の入手元は住民記録システムに限定される。 ・本人が書面を提出する際に、本人が本人（世帯員含む。以降、同様の定義とする）以外の情報を誤って記載することがないようチェックを行う。 ・住民基本台帳事務に係る各種申請に関し、運転免許証、個人番号カード、住基ネットによる本人確認などで申請者の本人確認を行う。
必要な情報以外を入手することを防止するための措置の内容	【本人からの情報入手】 ・本人が必要な情報以外を誤って記載することがないような書面様式とする。また,記載要領を充実し,必要最小限の情報の記載となるようにする。 ・平成14年6月10日総務省告示第334号（第6－7　本人確認情報の通知及び記録）等により市町村CSにおいて住民記録システムを通じて入手することととされている情報以外を入手できないことを、システム上で担保する。
その他の措置の内容	
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2： 不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	・本人確認情報の入手元は住民記録システムに限定される。
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3： 入手した特定個人情報が不正確であるリスク	
入手の際の本人確認の措置の内容	住民基本台帳事務に係る各種申請に関し、本人確認は運転免許証、個人番号カード、住基ネットにより行う。
個人番号の真正性確認の措置の内容	個人番号の生成元である機構が設置・管理する全国サーバから住民票コードに対応する個人番号を適切に取得できることを、システムにより担保する。
特定個人情報の正確性確保の措置の内容	【本人からの情報入手】 ・受付時に転出証明書や住基ネットによる住民情報の照合を行う。 ・届出書内容と照合内容が異なった場合は、届出人へのヒアリングによる確認を行う。 ・郵送による転出届や代理人による届出時など、届出内容の事実を確認する必要があるときは、本人に対して受理通知を郵送し届出内容の確認を行う。 ・システムへの入力は、届出内容の入力作業から決裁まで、複数人による確認作業を経て登録を完了させる。
その他の措置の内容	
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	【本人からの情報入手】 ・届出関係の書類は、受付後は専用の収納ケースに保管する。 ・システム画面が市民側から見えないように端末機を配置する。 ・LGWAN系ネットワークとマイナンバー利用事務系ネットワークの間にDMZ（隔離された領域）を設け、申請管理システムから外部への直接通信を遮断することにより、安全を確保している。また外部とのネットワーク接続について、境界FWや連携サーバで接続先との通信を限定している。 【その他】 ・情報セキュリティポリシーの周知等を職員に行う。また、情報漏えい等の防止のため、責任者の許可なく端末機又は記録媒体等を執務室以外に持出すことの禁止や、アクセス権限の管理、システムへのアクセス記録、コンピュータウィルス対策などを実施。 ・定期的及び随時にウィルスソフトウェアの更新を行う。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置	

3. 特定個人情報の使用		
リスク1： 目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク		
宛名システム等における措置の内容		・統合基盤システム（統合宛名番号付番機能、宛名情報等管理機能）との接続は行わない。
事務で使用するその他のシステムにおける措置の内容		・市町村CSへのアクセスは住民記録システムに限定している。 ・住民記録システムと市町村CS間では、法令に基づく事務で使用する以外の情報との紐付けは行わない。 ・市町村CSのサーバー上には住基ネットの管理及び運用に必要なソフトウェア以外作動させず、また、市町村CSが設置されたセグメントにあるハブには権限の無い者が機器を接続できないよう、適切な対策（物理的なアクセス制限、MACアドレスによるフィルタリング等）を講じる。
その他の措置の内容		
リスクへの対策は十分か		[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク2： 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク		
ユーザ認証の管理		[行っている] ＜選択肢＞ 1）行っている 2）行っていない
	具体的な管理方法	【認証方法】 ＜住民記録システムにおける措置＞ ・住民記録システムを利用する必要がある職員を特定し、個人ごとにユーザーIDを割り当てるとともに、IDとパスワードによる認証を行っている。 ・ネットワークユーザIDについては、管理者が管理し、人事異動等でシステム操作者に変更があれば、無効の設定を行う。パスワードはシステム的に変更させる設定としている。 ・パスワードは定期的に変更するよう周知するとともにシステム的に変更させる設定としている。 ＜住民基本台帳ネットワークシステムにおける措置＞ ・システムを利用する必要がある職員を特定し、個人ごとにユーザーIDを割り当てるとともに、生体認証による認証を行っている。 【なりすまし防止策】 従事者は以下を遵守し、利用ユーザIDを適切に管理する。 ・パスワードは第三者に知られないように管理する。 ・パスワードを秘密にし、パスワードの照会等には一切応じない。 ・パスワードは十分な長さとし、文字列は想像しにくいものとする。 ・パスワードは定期的に変更する。 ・端末機等のパスワードの記憶機能を利用しない。 ・パスワードが流出した可能性がある場合は、速やかに端末機管理者に報告し、パスワードを変更する。 ・使用する機器や記録媒体について、権限を有しない者の使用や閲覧を防止するため、端末から離れる場合にはログオフにする等適切な措置を講じる。
アクセス権限の発効・失効の管理		[行っている] ＜選択肢＞ 1）行っている 2）行っていない
	具体的な管理方法	＜住民記録システムにおける措置＞ 【アクセス権限の発効管理】 ・従事者が所属する部署、住民記録システムを所管する部署の管理者が業務上必要なユーザIDを確認し、アクセス権限管理を行う管理者へ発効の申請を行う。 【アクセス権限の失効管理】 ・従事者が所属する部署、住民記録システムを所管する部署の管理者が業務上不要となったユーザIDを確認し、アクセス権限管理を行う管理者へ失効の申請を行う。

アクセス権限の管理		[　行っている　] <選択肢> 1）行っている　2）行っていない
	具体的な管理方法	<住民記録システムにおける措置> ・共用IDは発行せず、必ず個人に対しユーザIDを発行する。 ・ユーザID単位で業務権限を設定し、システム内で利用可能な業務を制限している。 ・ユーザIDやアクセス権を住基等システム担当課長と事業所管課が定期的に確認し、業務上アクセスが不要となったIDやアクセス権を変更又は削除する。
特定個人情報の使用の記録		[　記録を残している　] <選択肢> 1）記録を残している　2）記録を残していない
	具体的な方法	<住民記録システムにおける措置> ・住民記録システムへのログイン記録、個人を特定した検索及び特定後の操作ログの記録を行う。操作者は個人まで特定でき、記録は永年保存する。
その他の措置の内容		
リスクへの対策は十分か		[　十分である　] <選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3：従業者が事務外で使用するリスク		
リスクに対する措置の内容		【職員の情報管理】 ・特定個人情報の利用を事務の目的の達成に必要な範囲内に限定し、事務目的外の利用・提供を禁止している。 ・研修の実施等により、個人情報保護及び情報セキュリティ意識の向上を図る。 ・利用システムに関する実施手順及び知識について研修を行う。 ・住民記録システム、及び統合基盤システム利用時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容を記録し、不適切な利用を抑止する。 【委託事業者の情報管理】 ・委託事業者に対しては目的外利用禁止を契約で定めており、従事者の教育訓練を義務付けている。 【職員の違反措置】 ・特定個人情報の使用記録より必要に応じて記録の解析を行い、事務外の利用有無を確認する。 ・違反行為を行った場合は法の罰則規定により措置を講ずる。なお、本市では懲戒処分に関する指針により、次の事項の違反時には懲戒処分の対象としており、事務外の使用を抑制している。 　個人情報の漏えい 　個人情報の目的外利用 　情報セキュリティポリシー違反
リスクへの対策は十分か		[　十分である　] <選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている

リスク4： 特定個人情報ファイルが不正に複製されるリスク	
リスクに対する措置の内容	【職員の情報管理】 ・システムの運用に関わる職員を対象に、システム及び当該システムにより処理されるデータに関わる情報セキュリティの実施手順並びに実施に必要な知識及び技術について研修を行う。 【委託事業者の情報管理】 ・委託先に対しては委託契約書にてデータの無断使用及び第三者への提供の禁止や、複写及び複製の禁止をしている。さらに、委託事業者において、当該従事者に対して情報セキュリティ研修を実施していることを確認している。 ＜住民記録システムにおける措置＞ ・住民記録システム利用時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容が記録されるため、不適切な利用を抑止する。 ・USBメモリやCD等の外部記録媒体への書き込みをシステム側で制限している。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置	

4. 特定個人情報ファイルの取扱いの委託		[　]委託しない
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク		
情報保護管理体制の確認	【業者選定時】 ・委託先を選定する際の要件に、プライバシーマークを取得していることもしくはISMS（情報セキュリティマネジメントシステム）の認証を受けていることを義務付けている。 【契約時】 ・契約書において次の事項を定めている。 ア 個人情報保護に関する規程、体制の整備 イ 個人情報保護に関する安全管理措置 ウ 情報セキュリティ対策の実施責任者の配置 ・適切な社内における情報保護管理体制が構築されているか、管理体制の説明を求め確認している。 ・必要に応じ、事業者の管理記録簿の確認又は作業場所の立入検査等を実施する。	
特定個人情報ファイルの閲覧者・更新者の制限	[　制限している　]	＜選択肢＞ 1）制限している　2）制限していない
具体的な制限方法	委託契約書に以下の規定を設ける。 ①アクセス権限を付与する業務員の名簿の提出と、それ以外の者が作業場所に立ち入ることを禁止している。 ②データの機密保持に関する事項を明記し、委託処理の際にデータ保護に関する委託先の規程の確認を行っている。 ③委託事業者に対しては業務外で使用しないように委託契約書に定め、機密保護等の誓約書を提出させている。 ④委託事業者において、当該職員に対して情報セキュリティ研修を実施していることを確認している。	
特定個人情報ファイルの取扱いの記録	[　記録を残している　]	＜選択肢＞ 1）記録を残している　2）記録を残していない
具体的な方法	・特定個人情報が記録されたサーバ等での作業については、事前に作業報告の提出を求める。 ・システム作業のためにサーバ等のメンテナンス用のID、パスワード及びデータベースのメンテナンス用ID、パスワードを利用させており、当日の作業報告と照合することで作業者の特定ができる。 ・上記の作業実績等については、磁気ディスクに記録し毎日蓄積・保存する。保存した記録については、1か月分を磁気ディスクにまとめて保管委託を行っている。 ・システムの改修や設定変更に係る作業については、作業対象となるOSやミドルウェアが保有する機能によりID単位の操作内容が記録される。	
特定個人情報の提供ルール	[　定めている　]	＜選択肢＞ 1）定めている　2）定めていない
委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	委託先から第三者への特定個人情報の提供は認めていない。	
委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	・委託先へ特定個人情報ファイルを提供することはなく、特定個人情報を取扱う作業を行う場合は本庁舎等設置端末を利用するなど、特定の作業場所で行うこととしている。 ・委託元は、必要があると認めるときは、委託先の個人情報等の保護状況について立入検査を実施する。	
特定個人情報の消去ルール	[　定めていない　]	＜選択肢＞ 1）定めている　2）定めていない
ルールの内容及びルール遵守の確認方法	委託事業者には特定個人情報の持ち出しは許可していないため、消去対象の情報はない。	
委託契約書中の特定個人情報ファイルの取扱いに関する規定	[　定めている　]	＜選択肢＞ 1）定めている　2）定めていない
規定の内容	・漏えい、滅失、き損等の防止その他個人情報等の保護に必要な体制の整備及び措置を講じなければならない ・個人情報等の授受・搬送・保管・廃棄等について、管理責任者を定める ・個人情報等の管理が適切でないと認められる場合、委託業者に対し改善を求めるとともに、個人情報等の管理状況を適切であると認めるまで委託業務を中止させることができる ・目的外利用の禁止及び第三者への提供禁止 ・個人情報等の外部への持ち出し禁止 ・個人情報等を複写又は複製禁止(本市の同意を得た場合を除く) ・個人情報等の保護状況について立入検査を実施することが可能 ・一括再委託等の禁止	

再委託先による特定個人情報ファイルの適切な取扱いの確保		[　　十分に行っている　　] ＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない　4）再委託していない
	具体的な方法	・個人情報保護の遵守を契約書に記載している ・業務に対する再委託先従事者の名簿提出を義務付けている ・秘密保持義務に関し覚書を交わしている ・情報セキュリティ確認書（※）により個人情報保護に関する必要な措置等について誓約させている （※）委託契約に際し、再委託先から委託先に対して提出させており、契約書に添付されている。
その他の措置の内容		
リスクへの対策は十分か		[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）	[　] 提供・移転しない
リスク1： 不正な提供・移転が行われるリスク	
特定個人情報の提供・移転の記録	[　記録を残している　] ＜選択肢＞ 1）記録を残している　2）記録を残していない
具体的な方法	【提供】 ・住民記録システムから住民基本台帳ネットワークシステムに対し、オペレータが操作することなく決められた時間に自動的に提供される。また、その内容は全て記録するように構築する。
特定個人情報の提供・移転に関するルール	[　定めている　] ＜選択肢＞ 1）定めている　2）定めていない
ルールの内容及びルール遵守の確認方法	【提供】 ・相手方（都道府県サーバ）と市町村CSの間の通信では相互認証を実施しているため、認証できない相手先への情報の提供はなされないことがシステム上担保される。
その他の措置の内容	USBメモリやCD等の外部記録媒体への書き込みをシステム側で禁止する
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である　3）課題が残されている
リスク2： 不適切な方法で提供・移転が行われるリスク	
リスクに対する措置の内容	【提供】 ・相手方（都道府県サーバ）と市町村CSの間の通信では相互認証を実施しているため、認証できない相手先への情報の提供はなされないことがシステム上担保される。また、媒体へ出力する必要がある場合には、逐一出力の記録が残される仕組みを構築する。
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である　3）課題が残されている
リスク3： 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク	
リスクに対する措置の内容	【提供】 ・システム上、照会元から指定された検索条件に基づき得た結果を適切に提供することを担保する。また、本人確認情報に変更が生じた際には、市町村CSへの登録時点で項目のフォーマットチェックや論理チェック（例えば、現存する住民に対して転入を異動事由とする更新が行われようとした場合や、転居を異動事由とする更新の際に住所以外の更新が行われようとした場合に当該処理をエラーとする）がなされた情報を通知することをシステム上で担保する。 ・相手方（都道府県サーバ）と市町村CSの間の通信では相互認証を実施しているため、認証できない相手先への情報の提供はなされないことがシステム上担保される。
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である　3）課題が残されている
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置	

6. 情報提供ネットワークシステムとの接続	[○] 接続しない（入手） [○] 接続しない（提供）
リスク1： 目的外の入手が行われるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク2： 安全が保たれない方法によって入手が行われるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク3： 入手した特定個人情報が不正確であるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク5： 不正な提供が行われるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク6： 不適切な方法で提供されるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク7： 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置	

7. 特定個人情報の保管・消去		
リスク1： 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[政府機関ではない]	<選択肢> 1）特に力を入れて遵守している　2）十分に遵守している 3）十分に遵守していない　4）政府機関ではない
②安全管理体制	[十分に整備している]	<選択肢> 1）特に力を入れて整備している　2）十分に整備している 3）十分に整備していない
③安全管理規程	[十分に整備している]	<選択肢> 1）特に力を入れて整備している　2）十分に整備している 3）十分に整備していない
④安全管理体制・規程の職員への周知	[十分に周知している]	<選択肢> 1）特に力を入れて周知している　2）十分に周知している 3）十分に周知していない
⑤物理的対策	[十分に行っている]	<選択肢> 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない
具体的な対策の内容	【中央情報処理センター第二別館（民間データセンター）サーバ室における対策】 特定個人情報を格納するサーバを設置する。サーバ室は次の対策を行っている。 ・サーバ室は無窓構造であり、入退室できるドアは1か所に限定しており、これらのドアもICカードと生体認証装置による入退室管理を行っている。 ・サーバ機器は施錠されたラック内部に格納されている。 ・サーバ室には火災報知機やガス系消火設備を設置するなどの防火措置を行っている。 ・サーバ室内に設置したサーバは、転倒・落下防止等の耐震対策を行っている。 ・サーバ室で利用する電源はCVCF装置や自家発電装置を設置し、電気的障害に対する措置を講じている。 ・職員等がサーバ室等へ入退室をする際は、データの漏洩防止のために、電子記録媒体、携帯電話、パソコン類等の不要な機器の持込みがないかを確認する。 ・作業のためにサーバ室等へ入退室する際に、電子記録媒体等の機器類を持込み、持出しする場合は、事前に責任者に申請書を提出し、承認を得ることとしている。 【記録媒体等の保管場所における対策】 ・バックアップデータは、中央情報処理センター（第二別館）内に保管し、入室者の制限を行っている。 【中間サーバ・プラットフォームにおける措置】 ・中間サーバ・プラットフォームをデータセンターに構築し、設置場所への入退室者管理、有人監視及び施錠管理をすることとしている。また、設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。	
⑥技術的対策	[十分に行っている]	<選択肢> 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない
具体的な対策の内容	【ウイルス対策】 ・ウイルス対策ソフトウェアを導入し、サーバ及び端末機に常駐させることで、コンピュータウイルス等の不正プログラム検出を行っている。 ・ウイルス対策ソフトウェアについて、定期的に当該ソフトウェア及びパターンファイルの更新を実施している。 【不正アクセス対策】 ・住民記録システム及び統合基盤システムは住民情報等を取り扱う重要システムが利用する専用ネットワークに接続しており、インターネットと物理的に接続されていない。 ・導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ・システム画面についてはスクリーンコピーを不可能とする設定を行っている。	
⑦バックアップ	[十分に行っている]	<選択肢> 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない
⑧事故発生時手順の策定・周知	[十分に行っている]	<選択肢> 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	[発生なし]	<選択肢> 1）発生あり　2）発生なし
その内容		
再発防止策の内容		

⑩死者の個人番号	[保管している]	<選択肢> 1）保管している 2）保管していない
具体的な保管方法	死者の個人番号は生存する個人の個人番号とともに、死亡による消除後、総務省告示第334号（第6－7（1）市町村長における本人確認情報の消去）に定める期間保管する。	
その他の措置の内容		
リスクへの対策は十分か	[十分である]	<選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている
リスク2： 特定個人情報が古い情報のまま保管され続けるリスク		
リスクに対する措置の内容	＜住民記録システムにおける措置＞ ・本人確認情報の入手元を住民記録システムに限定する。	
リスクへの対策は十分か	[十分である]	<選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている
リスク3： 特定個人情報が消去されずいつまでも存在するリスク		
消去手順	[定めている]	<選択肢> 1）定めている 2）定めていない
手順の内容	・データについては、保存期間の経過後システムにてデータベースより削除する。 ・CD等の外部媒体については、物理的破壊を行う。 ・申請書等の紙媒体については、外部業者による溶解処理を行う。	
その他の措置の内容		
リスクへの対策は十分か	[十分である]	<選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置		

Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※(7. リスク1⑨を除く。)

1. 特定個人情報ファイル名	
送付先情報ファイル	
2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）	
リスク1： 目的外の入手が行われるリスク	
対象者以外の情報の入手を防止するための措置の内容	【本人からの情報入手】 ・本人確認情報の入手元は住民記録システムに限定される。 ・本人が書面を提出する際に、本人が本人（世帯員含む。以降、同様の定義とする）以外の情報を誤って記載することがないようチェックを行う。 ・住民基本台帳事務に係る各種申請に関し、運転免許証、個人番号カード、住基ネットによる本人確認などで申請者の本人確認を行う。
必要な情報以外を入手することを防止するための措置の内容	【本人からの情報入手】 ・本人が必要な情報以外を誤って記載することがないような書面様式とする。また,記載要領を充実し,必要最小限の情報の記載となるようにする。 ・平成14年6月10日総務省告示第334号（第6－7　本人確認情報の通知及び記録）等により市町村CSにおいて住民記録システムを通じて入手することとされている情報以外を入手できないことを、システム上で担保する。
その他の措置の内容	
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である　3）課題が残されている
リスク2： 不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	・本人確認情報の入手元は住民記録システムに限定される。
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である　3）課題が残されている
リスク3： 入手した特定個人情報が不正確であるリスク	
入手の際の本人確認の措置の内容	住民基本台帳事務に係る各種申請に関し、本人確認は運転免許証、個人番号カード、住基ネットにより行う。
個人番号の真正性確認の措置の内容	個人番号の生成元である機構が設置・管理する全国サーバから住民票コードに対応する個人番号を適切に取得できることを、システムにより担保する。
特定個人情報の正確性確保の措置の内容	【本人からの情報入手】 ・受付時に転出証明書や住基ネットによる住民情報の照合を行う。 ・届出書内容と照合内容が異なった場合は、届出人へのヒアリングによる確認を行う。 ・郵送による転出届や代理人による届出時など、届出内容の事実を確認する必要があるときは、本人に対して受理通知を郵送し届出内容の確認を行う。 ・システムへの入力は、届出内容の入力作業から決裁まで、複数人による確認作業を経て登録を完了させる。
その他の措置の内容	
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である　3）課題が残されている

リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	【本人からの情報入手】 ・届出関係の書類は、受付後は専用の収納ケースに保管する。 ・システム画面が市民側から見えないように端末機を配置する。 【その他】 ・情報セキュリティポリシーの周知等を職員に行う。また、情報漏えい等の防止のため、責任者の許可なく端末機又は記録媒体等を執務室以外に持出すことの禁止や、アクセス権限の管理、システムへのアクセス記録、コンピュータウィルス対策などを実施。 ・定期的および随時にウィルスソフトウェアの更新を行う。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置	

3. 特定個人情報の使用		
リスク1： 目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク		
宛名システム等における措置の内容		・統合基盤システム（統合宛名番号付番機能、宛名情報等管理機能）との接続は行わない。
事務で使用するその他のシステムにおける措置の内容		・市町村CSへのアクセスは住民記録システムに限定している。 ・住民記録システムと市町村CS間では、法令に基づく事務で使用する以外の情報との紐付けは行わない。 ・市町村CSのサーバー上には住基ネットの管理及び運用に必要なソフトウェア以外作動させず、また、市町村CSが設置されたセグメントにあるハブには権限の無い者が機器を接続できないよう、適切な対策（物理的なアクセス制限、MACアドレスによるフィルタリング等）を講じる。
その他の措置の内容		
リスクへの対策は十分か		[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク2： 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク		
ユーザ認証の管理		[行っている] ＜選択肢＞ 1）行っている 2）行っていない
	具体的な管理方法	【認証方法】 ＜住民記録システムにおける措置＞ ・住民記録システムを利用する必要がある職員を特定し、個人ごとにユーザーIDを割り当てるとともに、IDとパスワードによる認証を行っている。 ・ネットワークユーザIDについては、管理者が管理し、人事異動等でシステム操作者に変更があれば、無効の設定を行う。パスワードはシステム的に変更させる設定としている。 ・パスワードは定期的に変更するよう周知するとともにシステム的に変更させる設定としている。 ＜住基ネットにおける措置＞ ・システムを利用する必要がある職員を特定し、個人ごとにユーザーIDを割り当てるとともに、生体認証による認証を行っている。 【なりすまし防止策】 従事者は以下を遵守し、利用ユーザIDを適切に管理する。 ・パスワードは第三者に知られないように管理する。 ・パスワードを秘密にし、パスワードの照会等には一切応じない。 ・パスワードは十分な長さとし、文字列は想像しにくいものとする。 ・パスワードは定期的に変更する。 ・端末機等のパスワードの記憶機能を利用しない。 ・パスワードが流出した可能性がある場合は、速やかに端末機管理者に報告し、パスワードを変更する。 ・使用する機器や記録媒体について、権限を有しない者の使用や閲覧を防止するため、端末から離れる場合にはログオフにする等適切な措置を講じる。
アクセス権限の発効・失効の管理		[行っている] ＜選択肢＞ 1）行っている 2）行っていない
	具体的な管理方法	＜住民記録システムにおける措置＞ 【アクセス権限の発効管理】 ・従事者が所属する部署、住民記録システムを所管する部署の管理者が業務上必要なユーザIDを確認し、アクセス権限管理を行う管理者へ発効の申請を行う。 【アクセス権限の失効管理】 ・従事者が所属する部署、住民記録システムを所管する部署の管理者が業務上不要となったユーザIDを確認し、アクセス権限管理を行う管理者へ失効の申請を行う。

アクセス権限の管理		[　行っている　] ＜選択肢＞ 1）行っている　2）行っていない
	具体的な管理方法	＜住民記録システムにおける措置＞ ・共用IDは発行せず、必ず個人に対しユーザIDを発行する。 ・ユーザID単位で業務権限を設定し、システム内で利用可能な業務を制限している。 ・ユーザIDやアクセス権を住民記録システム担当課長と事業所管課が定期的に確認し、業務上アクセスが不要となったIDやアクセス権を変更又は削除する。
特定個人情報の使用の記録		[　記録を残している　] ＜選択肢＞ 1）記録を残している　2）記録を残していない
	具体的な方法	＜住民記録システムにおける措置＞ ・住民記録システムへのログイン記録、個人を特定した検索及び特定後の操作ログの記録を行う。操作者は個人まで特定でき、記録は永年保存する。
その他の措置の内容		
リスクへの対策は十分か		[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3：従業者が事務外で使用するリスク		
リスクに対する措置の内容		【職員の情報管理】 ・特定個人情報の利用を事務の目的の達成に必要な範囲内に限定し、事務目的外の利用・提供を禁止している。 ・研修の実施等により、個人情報保護及び情報セキュリティ意識の向上を図る。 ・利用システムに関する実施手順及び知識について研修を行う。 ・住民記録システム、及び統合基盤システム利用時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容を記録し、不適切な利用を抑止する。 【委託事業者の情報管理】 ・委託事業者に対しては目的外利用禁止を契約で定めており、従事者の教育訓練を義務付けている。 【職員の違反措置】 ・特定個人情報の使用記録より必要に応じて記録の解析を行い、事務外の利用有無を確認する。 ・違反行為を行った場合は法の罰則規定により措置を講ずる。なお、本市では懲戒処分に関する指針により、次の事項の違反時には懲戒処分の対象としており、事務外の使用を抑制している。 　個人情報の漏えい 　個人情報の目的外利用 　情報セキュリティポリシー違反
リスクへの対策は十分か		[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

リスク4： 特定個人情報ファイルが不正に複製されるリスク	
リスクに対する措置の内容	【職員の情報管理】 ・システムの運用に関わる職員を対象に、システム及び当該システムにより処理されるデータに関わる情報セキュリティの実施手順並びに実施に必要な知識及び技術について研修を行う。 【委託事業者の情報管理】 ・委託先に対しては委託契約書にてデータの無断使用及び第三者への提供の禁止や、複写及び複製の禁止をしている。さらに、委託事業者において、当該従事者に対して情報セキュリティ研修を実施していることを確認している。 ＜住民記録システムにおける措置＞ ・住民記録システム利用時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容が記録されるため、不適切な利用を抑止する。 ・USBメモリやCD等の外部記録媒体への書き込みをシステム側で制限している。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置	

4. 特定個人情報ファイルの取扱いの委託		[　　]委託しない
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク		
情報保護管理体制の確認		【業者選定時】 ・委託先を選定する際の要件に、プライバシーマークを取得していることもしくはISMS（情報セキュリティマネジメントシステム）の認証を受けていることを義務付けている。 【契約時】 ・契約書において次の事項を定めている。 ア 個人情報保護に関する規程、体制の整備 イ 個人情報保護に関する安全管理措置 ウ 情報セキュリティ対策の実施責任者の配置 ・適切な社内における情報保護管理体制が構築されているか、管理体制の説明を求め確認している。 ・必要に応じ、事業者の管理記録簿の確認又は作業場所の立入検査等を実施する。
特定個人情報ファイルの閲覧者・更新者の制限		[　制限している　] ＜選択肢＞ 1）制限している　2）制限していない
	具体的な制限方法	委託契約書に以下の規定を設ける。 ①アクセス権限を付与する業務員の名簿の提出と、それ以外の者が作業場所に立ち入ることを禁止している。 ②データの機密保持に関する事項を明記し、委託処理の際にデータ保護に関する委託先の規程の確認を行っている。 ③委託事業者に対しては業務外で使用しないように委託契約書に定め、機密保護等の誓約書を提出させている。 ④委託事業者において、当該職員に対して情報セキュリティ研修を実施していることを確認している。
特定個人情報ファイルの取扱いの記録		[　記録を残している　] ＜選択肢＞ 1）記録を残している　2）記録を残していない
	具体的な方法	・特定個人情報が記録されたサーバ等での作業については、事前に作業報告の提出を求める。 ・システム作業のためにサーバ等のメンテナンス用のID、パスワード及びデータベースのメンテナンス用ID、パスワードを利用させており、当日の作業報告と照合することで作業者の特定ができる。 ・上記の作業実績等については、磁気ディスクに記録し毎日蓄積・保存する。保存した記録については、1か月分を磁気ディスクにまとめて保管委託を行っている。 ・システムの改修や設定変更に係る作業については、作業対象となるOSやミドルウェアが保有する機能によりID単位の操作内容が記録される。
特定個人情報の提供ルール		[　定めている　] ＜選択肢＞ 1）定めている　2）定めていない
	委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	委託先から第三者への特定個人情報の提供は認めていない。
	委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	・委託先へ特定個人情報ファイルを提供することはなく、特定個人情報を取扱う作業を行う場合は本庁舎等設置端末を利用するなど、特定の作業場所で行うこととしている。 ・委託元は、必要があると認めるときは、委託先の個人情報等の保護状況について立入検査を実施する。
特定個人情報の消去ルール		[　定めていない　] ＜選択肢＞ 1）定めている　2）定めていない
	ルールの内容及びルール遵守の確認方法	委託事業者には特定個人情報の持ち出しは許可していないため、消去対象の情報はない。
委託契約書中の特定個人情報ファイルの取扱いに関する規定		[　定めている　] ＜選択肢＞ 1）定めている　2）定めていない
	規定の内容	・漏えい、滅失、き損等の防止その他個人情報等の保護に必要な体制の整備及び措置を講じなければならない ・個人情報等の授受・搬送・保管・廃棄等について、管理責任者を定める ・個人情報等の管理が適切でないと認められる場合、委託業者に対し改善を求めるとともに、個人情報等の管理状況を適切であると認めるまで委託業務を中止させることができる ・目的外利用の禁止及び第三者への提供禁止 ・個人情報等の外部への持ち出し禁止 ・個人情報等を複写又は複製禁止(本市の同意を得た場合を除く) ・個人情報等の保護状況について立入検査を実施することが可能 ・一括再委託等の禁止

再委託先による特定個人情報ファイルの適切な取扱いの確保		[　　十分に行っている　　] ＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない　4）再委託していない
	具体的な方法	・個人情報保護の遵守を契約書に記載している ・業務に対する再委託先従事者の名簿提出を義務付けている ・秘密保持義務に関し覚書を交わしている ・情報セキュリティ確認書（※）により個人情報保護に関する必要な措置等について誓約させている （※）委託契約に際し、再委託先から委託先に対して提出させており、契約書に添付されている。
その他の措置の内容		
リスクへの対策は十分か		[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		[　　]提供・移転しない
リスク1： 不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録	[　　記録を残している　　]	＜選択肢＞ 1）記録を残している　　2）記録を残していない
具体的な方法	【提供】 ・移転については、住民記録システムから住民基本台帳ネットワークシステムに対し、オペレータが操作することなく決められた時間に自動的に提供される。また、その内容は全て記録するように構築する。	
特定個人情報の提供・移転に関するルール	[　　定めている　　]	＜選択肢＞ 1）定めている　　2）定めていない
ルールの内容及びルール遵守の確認方法	【提供】 ・相手方（都道府県サーバ）と市町村CSの間の通信では相互認証を実施しているため、認証できない相手先への情報の提供はなされないことがシステム上担保される。	
その他の措置の内容	USBメモリやCD等の外部記録媒体への書き込みをシステム側で禁止する	
リスクへの対策は十分か	[　　十分である　　]	＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
リスク2： 不適切な方法で提供・移転が行われるリスク		
リスクに対する措置の内容	【提供】 ・相手方（都道府県サーバ）と市町村CSの間の通信では相互認証を実施しているため、認証できない相手先への情報の提供はなされないことがシステム上担保される。また、媒体へ出力する必要がある場合には、逐一出力の記録が残される仕組みを構築する。	
リスクへの対策は十分か	[　　十分である　　]	＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
リスク3： 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク		
リスクに対する措置の内容	【提供】 ・システム上、照会元から指定された検索条件に基づき得た結果を適切に提供・移転することを担保する。また、本人確認情報に変更が生じた際には、市町村CSへの登録時点で項目のフォーマットチェックや論理チェック（例えば、現存する住民に対して転入を異動事由とする更新が行われようとした場合や、転居を異動事由とする更新の際に住所以外の更新が行われようとした場合に当該処理をエラーとする）がなされた情報を通知することをシステム上で担保する。 ・相手方（都道府県サーバ）と市町村CSの間の通信では相互認証を実施しているため、認証できない相手先への情報の提供はなされないことがシステム上担保される。	
リスクへの対策は十分か	[　　十分である　　]	＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置		

6. 情報提供ネットワークシステムとの接続	[○] 接続しない（入手） [○] 接続しない（提供）
リスク1： 目的外の入手が行われるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク2： 安全が保たれない方法によって入手が行われるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク3： 入手した特定個人情報が不正確であるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク5： 不正な提供が行われるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク6： 不適切な方法で提供されるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク7： 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置	

7. 特定個人情報の保管・消去		
リスク1： 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[政府機関ではない]	<選択肢> 1）特に力を入れて遵守している 2）十分に遵守している 3）十分に遵守していない 4）政府機関ではない
②安全管理体制	[十分に整備している]	<選択肢> 1）特に力を入れて整備している 2）十分に整備している 3）十分に整備していない
③安全管理規程	[十分に整備している]	<選択肢> 1）特に力を入れて整備している 2）十分に整備している 3）十分に整備していない
④安全管理体制・規程の職員への周知	[十分に周知している]	<選択肢> 1）特に力を入れて周知している 2）十分に周知している 3）十分に周知していない
⑤物理的対策	[十分に行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
具体的な対策の内容	【中央情報処理センター第二別館（民間データセンター）サーバ室における対策】 特定個人情報を格納するサーバを設置する。サーバ室は次の対策を行っている。 ・サーバ室は無窓構造であり、入退室できるドアは1か所に限定しており、これらのドアもICカードと生体認証装置による入退室管理を行っている。 ・サーバ機器は施錠されたラック内部に格納されている。 ・サーバ室には火災報知機やガス系消火設備を設置するなどの防火措置を行っている。 ・サーバ室内に設置したサーバは、転倒・落下防止等の耐震対策を行っている。 ・サーバ室で利用する電源はCVCF装置や自家発電装置を設置し、電気的障害に対する措置を講じている。 ・職員等がサーバ室等へ入退室をする際は、データの漏洩防止のために、電子記録媒体、携帯電話、パソコン類等の不要な機器の持込みがないかを確認する。 ・作業のためにサーバ室等へ入退室する際に、電子記録媒体等の機器類を持込み、持出しする場合は、事前に責任者に申請書を提出し、承認を得ることとしている。 【記録媒体等の保管場所における対策】 ・バックアップデータは、中央情報処理センター（第二別館）内に保管し、入室者の制限を行っている。 【中間サーバ・プラットフォームにおける措置】 ・中間サーバ・プラットフォームをデータセンターに構築し、設置場所への入退室者管理、有人監視及び施錠管理をすることとしている。また、設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。	
⑥技術的対策	[十分に行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
具体的な対策の内容	【ウイルス対策】 ・ウイルス対策ソフトウェアを導入し、サーバ及び端末機に常駐させることで、コンピュータウイルス等の不正プログラム検出を行っている。 ・ウイルス対策ソフトウェアについて、定期的に当該ソフトウェア及びパターンファイルの更新を実施している。 【不正アクセス対策】 ・住民記録システム及び統合基盤システムは住民情報等を取り扱う重要システムが利用する専用ネットワークに接続しており、インターネットと物理的に接続されていない。 ・導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ・システム画面についてはスクリーンコピーを不可能とする設定を行っている。	
⑦バックアップ	[十分に行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
⑧事故発生時手順の策定・周知	[十分に行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	[発生なし]	<選択肢> 1）発生あり 2）発生なし
その内容		
再発防止策の内容		

⑩死者の個人番号	[　保管していない　]	＜選択肢＞ 1）保管している　2）保管していない
具体的な保管方法		
その他の措置の内容		
リスクへの対策は十分か	[　十分である　]	＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2：特定個人情報が古い情報のまま保管され続けるリスク		
リスクに対する措置の内容	＜住民記録システムにおける措置＞ ・送付先情報の連携を行う必要が生じた都度作成・連携することとしており、システム上、連携後速やかに削除する仕組みとする。	
リスクへの対策は十分か	[　十分である　]	＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3：特定個人情報が消去されずいつまでも存在するリスク		
消去手順	[　定めている　]	＜選択肢＞ 1）定めている　2）定めていない
手順の内容	・データについては、保存期間の経過後システムにてデータベースより削除する。 ・CD等の外部媒体については、物理的破壊を行う。 ・申請書等の紙媒体については、外部業者による溶解処理を行う。	
その他の措置の内容		
リスクへの対策は十分か	[　十分である　]	＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置		

Ⅳ　その他のリスク対策 ※

1. 監査		
①自己点検		[　　十分に行っている　　] ＜選択肢＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
	具体的なチェック方法	＜住民記録システムにおける措置＞ ①大阪市情報セキュリティ検査実施要綱に基づき、毎年１回、最高情報セキュリティ責任者が実施する内部検査において全てのシステムの情報セキュリティ対策の状況について点検を行い、点検結果を評価する。点検結果の評価を踏まえ、改善が必要な事項について改善計画を作成し、速やかに対応を図る。 ②個人情報保護に係る重要管理ポイントを設定し、遵守できているかのセルフチェックを月１回行うこととしている。 ＜中間サーバ・プラットフォームにおける措置＞ 運用規則等に基づき、中間サーバ・プラットフォームの運用に携わる職員及び事業者に対し、定期的に自己点検を行うこととしている。
②監査		[　　十分に行っている　　] ＜選択肢＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
	具体的な内容	＜住民記録システムにおける措置＞ 情報セキュリティ責任者が毎年セキュリティ内部監査として、セキュリティ対策の実施状況について確認を行うこととしており、本システムについても内部監査の対象としている。また、セキュリティ内部監査の結果、 必要と認められるシステムについては、選任された外部監査人によるセキュリティ監査を受け、問題点の把握・改善を図ることとしている。 ＜中間サーバ・プラットフォームにおける措置＞ 運用規則等に基づき、中間サーバ・プラットフォームについて、定期的に監査を行うこととしている。 ＜ガバメントクラウドにおける措置＞ ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、ISMAPにおいて、クラウドサービス事業者は定期的にISMAP監査機関リストに登録された監査機関による監査を行うこととしている。
2. 従業者に対する教育・啓発		
従業者に対する教育・啓発		[　　十分に行っている　　] ＜選択肢＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
	具体的な方法	＜住民記録システムにおける措置＞ ①本システムについて、区役所等のシステム利用部署の責任者に新たに着任した者について、セキュリティ対策の研修を実施し、所管部署のセキュリティ対策の徹底に努めるよう啓発を行うこととしている。 ②セキュリティ関連規程等に変更があった場合は、それに基づく本システムのセキュリティ対策実施手順についても適宜必要な見直しを行い、利用部署等に周知し、セキュリティ対策の徹底を図るよう指導を行うこととしている。 ③委託事業者については、業務外で使用しないように委託契約書（協定書）に定め、機密保護等の誓約書を提出させることとしている。さらに、委託事業者において、当該職員に対して情報セキュリティ研修を行うこととしている。 ④違反行為を行ったものに対しては、懲戒処分に関する指針に基づき懲戒処分の対象とすることとしている。 ＜中間サーバ・プラットフォームにおける措置＞ ①中間サーバ・プラットフォームの運用に携わる職員及び事業者に対し、セキュリティ研修を行うこととしている。 ②中間サーバ・プラットフォームの業務に就く場合は、運用規則等について研修を行うこととしている。 ＜申請管理システムにおける措置＞ 申請管理システムを利用する職員に対して、セキュリティ対策の研修を実施することとしている。

3. その他のリスク対策

＜中間サーバ・プラットフォームにおける措置＞
中間サーバ・プラットフォームを活用することにより、統一した設備環境による高レベルのセキュリティ管理（入退室管理等）、ITリテラシの高い運用担当によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用・監視を実現する。

＜ガバメントクラウドにおける措置＞
ガバメントクラウド上での業務データの取扱いについては、当該業務データを保有する地方公共団体及びその業務データの取扱いについて委託を受けるASP又はガバメントクラウド運用管理補助者が責任を有する。
ガバメントクラウド上での業務アプリケーションの運用等に障害が発生する場合等の対応については、原則としてガバメントクラウドに起因する事象の場合は、国はクラウド事業者と契約する立場から、その契約を履行させることで対応する。また、ガバメントクラウドに起因しない事象の場合は、地方公共団体に業務アプリケーションサービスを提供するASP又はガバメントクラウド運用管理補助者が対応するものとする。
具体的な取り扱いについて、疑義が生じる場合は、地方公共団体とデジタル庁及び関係者で協議を行う。

Ⅴ　開示請求、問合せ

1. 特定個人情報の開示・訂正・利用停止請求	
①請求先	〒530-8201 大阪市北区中之島1丁目3番20号 大阪市総務局行政部行政課（情報公開グループ）
②請求方法	・窓口（大阪市役所本庁1階市民相談室）で直接、開示・訂正・利用停止請求 ・郵便にて開示・訂正・利用停止請求
特記事項	大阪市ホームページ上に請求先及び請求方法を掲載。
③手数料等	[　　無料　　]　＜選択肢＞ 1）有料　2）無料 （手数料額、納付方法：　　）
④個人情報ファイル簿の公表	[　　行っている　　]　＜選択肢＞ 1）行っている　2）行っていない
個人情報ファイル名	住民基本台帳
公表場所	大阪市ホームページ　https://www.city.osaka.lg.jp/shimin/page/0000609167.html
⑤法令による特別の手続	住民基本台帳法第14条等により、訂正等を受け付ける
⑥個人情報ファイル簿への不記載等	

2. 特定個人情報ファイルの取扱いに関する問合せ	
①連絡先	〒553-0005 大阪市福島区野田1丁目1番86号　業務管理棟9階　大阪市市民局分室 大阪市市民局総務部住民情報担当（住民情報グループ） 電話：06-4305-7345　FAX：06-4305-7346
②対応方法	・問い合わせ内容を十分聴き取り、申出者に説明を行い、その対応について記録を残す。 ・漏えい等に関わる問合せについては、必要に応じて調査等を実施し、申出者に説明する。

Ⅵ　評価実施手続

1. 基礎項目評価	
①実施日	
②しきい値判断結果	[　　基礎項目評価及び全項目評価の実施が義務付けられる　　] ＜選択肢＞ 1) 基礎項目評価及び全項目評価の実施が義務付けられる 2) 基礎項目評価及び重点項目評価の実施が義務付けられる（任意に全項目評価を実施） 3) 基礎項目評価の実施が義務付けられる（任意に全項目評価を実施） 4) 特定個人情報保護評価の実施が義務付けられない（任意に全項目評価を実施）
2. 国民・住民等からの意見の聴取	
①方法	大阪市ホームページへの掲載、市民局総務部住民情報担当（住民情報グループ）（市役所4階）及び市民情報プラザ（大阪市役所1階）での配架等により意見募集内容の閲覧を行い、送付、FAX、電子メール又は窓口（大阪市市民局総務部住民情報担当）への持参により意見を受け付ける。
②実施日・期間	令和6年9月　日（　）から令和6年　月　日（　）まで
③期間を短縮する特段の理由	_
④主な意見の内容	
⑤評価書への反映	_
3. 第三者点検	
①実施日	
②方法	大阪市個人情報保護審議会による点検
③結果	
4. 特定個人情報保護委員会の承認 【行政機関等のみ】	
①提出日	
②特定個人情報保護委員会による審査	

（別添3）変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
	Ⅰ基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム ①システムの名称	住民基本台帳等事務システム（以下、「住基等システム」という） ※本市における既存住民基本台帳システムを指す	住民記録システム ※以降「住基等システム」を修正	事前	標準準拠システム移行に伴う変更 ※令和6年〇月〇日公表の評価書番号1からの変更箇所を記載 以降、変更日が令和6年〇月〇日のものは同様□
	Ⅰ基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム システム1 ③他のシステムとの接続	（記載なし）	[〇]その他 （申請管理システム　　）	事前	申請管理システム導入
	Ⅰ基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム システム2 ③他のシステムとの接続	[〇]既存住民基本台帳システム	[〇]その他 （住民記録システム　　）	事前	標準準拠システム移行に伴う変更
	Ⅰ基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム システム3 ③他のシステムとの接続	[〇]その他 （中間サーバー、連携するシステム全て ）	[〇]その他 （住民記録システム、中間サーバー、連携するシステム全て）	事前	標準準拠システム移行に伴う変更
	Ⅰ基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム システム4 ③他のシステムとの接続	[〇]情報提ネットワークシステム [〇]庁内連携システム [〇]既存住民基本台帳システム [〇]宛名システム等	[〇]情報提ネットワークシステム [〇]庁内連携システム [〇]宛名システム等 [〇]その他 （住民記録システム）	事前	標準準拠システム移行に伴う変更
	Ⅰ基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム5 ①システムの名称	（記載なし）	申請管理システム	事前	申請管理システム導入
	Ⅰ基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム5 ②システムの機能	（記載なし）	（マイナポータル連携機能） LGWAN系ネットワークとマイナンバー利用事務系ネットワークの間にDMZ（隔離された領域）内の連携サーバを利用し、サービス検索・電子申請機能（マイナポータルぴったりサービス）で受け付けた電子申請データを申請管理システムに連携する（受け渡す）機能 （申請管理システム） ・連携サーバから連携された電子申請データを参照する機能 ・電子申請データを地方公共団体の基幹システムに連携する（受け渡す）機能	事前	申請管理システム導入
	Ⅰ基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム5 ③他のシステムとの接続	（記載なし）	[〇]庁内連携システム [〇]その他 （住民記録システム、サービス検索・電子申請機能（マイナポータルぴったりサービス））	事前	申請管理システム導入
	Ⅱ特定個人情報ファイルの概要（住民基本台帳ファイル） 3. 特定個人情報の入手・使用 ②入手方法	[〇]その他（住基ネット、出入国在留管理庁連携ネットワークシステム）	[〇]その他（住基ネット、出入国在留管理庁連携ネットワークシステム、申請管理システム）	事前	申請管理システム導入
	Ⅱ特定個人情報ファイルの概要（住民基本台帳ファイル） 3. 特定個人情報の入手・使用 ③入手の次期・頻度	入手元（本人又は本人の代理人） ・住民異動届（転入・転居・転出・世帯変更届）／届出を受けた都度／入手方法は紙 ・転入届出に伴う転出証明書情報／届出を受けた都度／入手方法は紙	入手元（本人又は本人の代理人） ・住民異動届（転入・転居・転出・世帯変更届）／届出を受けた都度／入手方法は紙 ・転入届出に伴う転出証明書情報／届出を受けた都度／入手方法は紙 ・マイナポータルで受け付けた電子申請を申請管理システムから入手／随時	事前	申請管理システム導入
	Ⅱ特定個人情報ファイルの概要（住民基本台帳ファイル） 3. 特定個人情報の入手・使用 ⑧使用方法	住基法に基づき使用する。主な方法は以下のとおり。 ・住民票へ記載し、公証する。 ・本人確認情報として住基ネットへ送信する。 ・窓口における本人確認に使用する。（個人番号等をキーとして住民票を検索し、届出書等の記載内容と照合）	住基法に基づき使用する。主な方法は以下のとおり。 ・住民票へ記載し、公証する。 ・本人確認情報として住基ネットへ送信する。 ・窓口における本人確認に使用する。（個人番号等をキーとして住民票を検索し、届出書等の記載内容と照合） ・「サービス検索・電子申請機能（マイナポータルぴったりサービス）」を通じて申請された電子申請データの受理、審査等	事前	申請管理システム導入
	Ⅱ特定個人情報ファイルの概要（住民基本台帳ファイル） 3. 特定個人情報の入手・使用 ⑧使用方法 情報の突合	（記載なし）	・申請者を確認するために住民記録システムを通じて取り込んだ番号紐付情報と突合する	事前	申請管理システム導入
	Ⅱ ファイルの概要（住民基本台帳ファイル） 4. 特定個人情報ファイルの取扱いの委託 委託の有無	委託する （　6　）件	委託する （　5　）件	事前	標準準拠システム移行に伴う変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
	Ⅱ ファイルの概要（住民基本台帳ファイル） 4. 特定個人情報ファイルの取扱いの委託 委託事項1 ④委託先への特定個人情報ファイルの提供方法	大阪市本庁舎及び情報システム室内にてシステムを直接操作を行うため、特定個人情報ファイルの提供は発生しない。	特定個人情報ファイルの提供はしていないが、必要に応じて本市指定の保守作業場所にて、システムの直接操作を認めている。	事前	標準準拠システム移行に伴う変更
	Ⅱ ファイルの概要（住民基本台帳ファイル） 4. 特定個人情報ファイルの取扱いの委託 委託事項3 ④委託先への特定個人情報ファイルの提供方法	情報システム室内でシステムを直接操作させており、委託先に特定個人情報を提供することはない。	特定個人情報ファイルの提供はしていないが、必要に応じて本市指定の保守作業場所にて、システムの直接操作を認めている。	事前	標準準拠システム移行に伴う変更
	Ⅱ ファイルの概要（住民基本台帳ファイル） 4. 特定個人情報ファイルの取扱いの委託 委託事項3 ⑨委託内容	中央情報処理センターで運用する業務システムの実行監視、入出力媒体の管理	中央情報処理センターで運用する業務システムの実行監視	事前	標準準拠システム移行に伴う変更
	Ⅱ ファイルの概要（住民基本台帳ファイル） 4. 特定個人情報ファイルの取扱いの委託 委託事項4 ④委託先への特定個人情報ファイルの提供方法	サーバ設置場所、または中央情報処理センターにおける運用保守のみのため、特定個人情報を提供することはない。	特定個人情報ファイルは提供していないが、サーバ設置場所、または中央情報処理センターにおける運用保守を行っている。	事前	標準準拠システム移行に伴う変更
	Ⅱ ファイルの概要（住民基本台帳ファイル） 4. 特定個人情報ファイルの取扱いの委託 委託事項5	バックアップ用媒体の運搬および保管業務委託	申請管理システム構築・運用保守業務	事前	標準準拠システム移行に伴う変更及び申請管理システム導入
	Ⅱ ファイルの概要（住民基本台帳ファイル） 4. 特定個人情報ファイルの取扱いの委託 委託事項6	中央情報処理センター第二別館運用業務委託	（削除）	事前	標準準拠システム移行に伴う変更
	Ⅱ ファイルの概要（住民基本台帳ファイル） 6. 特定個人情報の保管・消去 ①保管場所	＜特定個人情報の保管場所＞ ・特定個人情報は、システム用ファイルとして住基等システム及び統合基盤システムのサーバ内に格納することとしている。	・特定個人情報は、システム用ファイルとしてガバメントクラウドの住民記録システムに格納することとしている。 なお、標準化以前の除票データについては、ガバメントクラウド上の除票管理システムに格納することとしている。	事前	標準準拠システム移行に伴う変更
	Ⅱ ファイルの概要（住民基本台帳ファイル） 6. 特定個人情報の保管・消去 ①保管場所	＜保管場所の状況＞ ①サーバ ・住基等システム及び統合基盤システムのサーバーは、入退館管理を24時間行う警備員を配置し、機械警備の実施や館内に監視カメラを設置する中央情報処理センター第二別館（民間データセンター）内の情報システム室に設置している。 ・中央情報処理センター第二別館（民間データセンター）は入退館時にID及び生体認証装置による認証を行っており、情報システム室はICカードと生体認証装置により入室制限を行っている。 ②外部媒体 ・情報システム室については、上記①に同じ。 ・遠隔地保管については、専門事業者に委託し、媒体を保護ケースに格納し施錠のうえ、入退館管理を行っている遠隔地で保管している。	＜ガバメントクラウドにおける措置＞ ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。	事前	標準準拠システム移行に伴う変更
	Ⅱ特定個人情報ファイルの概要（住民基本台帳ファイル） 6. 特定個人情報の保管・消去 ①保管場所	（記載なし）	＜申請管理システムにおける措置＞ 申請管理システムはガバメントクラウドで稼働するため、保管場所は「ガバメントクラウドにおける措置」に記載するとおりとする。	事前	申請管理システム導入
	Ⅱ特定個人情報ファイルの概要（住民基本台帳ファイル） 6. 特定個人情報の保管・消去 ③消去方法	（記載なし）	＜ガバメントクラウドにおける措置＞ ①特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報を消去することはない。 ②クラウド事業者がHDDやSSDなどの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等にしたがって確実にデータを消去する。 ③既存システムについては、地方公共団体が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。	事前	標準準拠システム移行に伴う変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
	Ⅱ特定個人情報ファイルの概要（住民基本台帳ファイル） 6．特定個人情報の保管・消去 ③消去方法	（記載なし）	＜申請管理システムにおける措置＞ ・申請管理システムはガバメントクラウドで稼働するため、保管場所は「ガバメントクラウドにおける措置」に記載するとおりとする。 ・サービス検索・電子申請機能（マイナポータルぴったりサービス）の電子申請データの取得に利用するDMZ（隔離された領域）内の連携サーバには個人番号付電子申請データを保有しない。 ・申請管理システムを利用する端末に一時的に記録した個人番号付電子申請データは、住民記録システムでの業務処理後は速やかに完全消去する。	事前	申請管理システム導入
	Ⅱ ファイルの概要（本人確認情報ファイル） 4．特定個人情報ファイルの取扱いの委託 委託事項1 ④委託先への特定個人情報ファイルの提供方法	大阪市本庁舎及び情報システム室内にてシステムを直接操作を行うため、特定個人情報ファイルの提供は発生しない。	特定個人情報ファイルの提供はしていないが、必要に応じて本市指定の保守作業場所にて、システムの直接操作を認めている。	事前	標準準拠システム移行に伴う変更
	Ⅱ ファイルの概要（本人確認情報ファイル） 6．特定個人情報の保管・消去 ①保管場所	＜特定個人情報の保管場所＞ ・特定個人情報は、システム用ファイルとして住基等システム及び統合基盤システムのサーバ内に格納することとしている。	＜特定個人情報の保管場所＞ ・特定個人情報は、システム用ファイルとして統合基盤システムのサーバ内に格納することとしている。	事前	標準準拠システム移行に伴う変更
	Ⅱ ファイルの概要（送付先情報ファイル） 3．特定個人情報の入手・使用 ②使用方法	・既存住基システムより個人番号の通知対象者の情報を抽出し、個人番号通知書及び交付申請書等の印刷及び送付に係る事務を個人番号カード省令第23条の2（個人番号通知書及び個人番号カードに関し機構が処理する事務）に基づいて行う機構に対し提供する（既存住基システム→市町村CS又は電子記録媒体→個人番号カード管理システム（機構））。	・住民記録システムより個人番号の通知対象者の情報を抽出し、個人番号通知書及び交付申請書等の印刷及び送付に係る事務を個人番号カード省令第23条の2（個人番号通知書及び個人番号カードに関し機構が処理する事務）に基づいて行う機構に対し提供する（住民記録システム→市町村CS又は電子記録媒体→個人番号カード管理システム（機構））。 ※以降、「既存住基システム」についても「住基記録システム」へ修正	事前	標準準拠システム移行に伴う変更
	Ⅱ ファイルの概要（送付先情報ファイル） 4．特定個人情報ファイルの取扱いの委託 委託事項1 ④委託先への特定個人情報ファイルの提供方法	大阪市本庁舎及び情報システム室内にてシステムを直接操作を行うため、特定個人情報ファイルの提供は発生しない。	特定個人情報ファイルの提供はしていないが、必要に応じて本市指定の保守作業場所にて、システムの直接操作を認めている。	事前	標準準拠システム移行に伴う変更
	Ⅱ ファイルの概要（送付先情報ファイル） 6．特定個人情報の保管・消去 ①保管場所	＜特定個人情報の保管場所＞ ・特定個人情報は、システム用ファイルとして住基等システム及び統合基盤システムのサーバ内に格納することとしている。	＜特定個人情報の保管場所＞ ・特定個人情報は、システム用ファイルとして統合基盤システムのサーバ内に格納することとしている。	事前	標準準拠システム移行に伴う変更
	Ⅱ ファイルの概要（送付先情報ファイル） 6．特定個人情報の保管・消去 ①保管場所	＜特定個人情報の保管場所＞ ・特定個人情報は、システム用ファイルとして住基等システム及び統合基盤システムのサーバ内に格納することとしている。	＜特定個人情報の保管場所＞ ・特定個人情報は、システム用ファイルとして統合基盤システムのサーバ内に格納することとしている。	事前	標準準拠システム移行に伴う変更
	Ⅲ特定個人情報ファイルの取扱いプロセスにおけるリスク対策（住民基本台帳ファイル） 2．特定個人情報の入手 リスク1	【本人からの情報入手】 ・本人が書面を提出する際に、本人が本人（世帯員含む。以降、同様の定義とする）以外の情報を誤って記載することがないようチェックを行う。 ・住民基本台帳事務に係る各種申請に関し、運転免許証、個人番号カード、住基カード、国民健康保険証住基ネットによる本人確認などで申請者の本人確認を行う。	【本人からの情報入手】 ・本人が書面を提出する際に、本人が本人（世帯員含む。以降、同様の定義とする）以外の情報を誤って記載することがないようチェックを行う。 ・住民基本台帳事務に係る各種申請に関し、運転免許証、個人番号カード、住基ネットによる本人確認などで申請者の本人確認を行う。 ※以降、住基カード、国民健康保険証部分は同様に削除	事前	住基カード、国民健康保険証の発行終了による
	Ⅲ特定個人情報ファイルの取扱いプロセスにおけるリスク対策（住民基本台帳ファイル） 2．特定個人情報の入手 リスク4 リスクに対する措置の内容	【本人からの情報入手】 ・届出関係の書類は、受付後は専用の収納ケースに保管する。 ・システム画面が市民側から見えないように端末機を配置する。	【本人からの情報入手】 ・届出関係の書類は、受付後は専用の収納ケースに保管する。 ・システム画面が市民側から見えないように端末機を配置する。 ・LGWAN系ネットワークとマイナンバー利用事務系ネットワークの間にDMZ（隔離された領域）を設け、申請管理システムから外部への直接通信を遮断することにより、安全を確保している。また外部とのネットワーク接続について、境界FWや連携サーバで接続先との通信を限定している。	事前	申請管理システム導入
	Ⅲ特定個人情報ファイルの取扱いプロセスにおけるリスク対策（住民基本台帳ファイル） 3．特定個人情報の使用 リスク2 ユーザ認証の管理 具体的な管理方法	（記載なし）	＜申請管理システムにおける措置＞ ・申請管理システムを利用する必要がある職員を特定し、適切なユーザ割り当て及び認証を行う。	事前	申請管理システム導入
	Ⅲ特定個人情報ファイルの取扱いプロセスにおけるリスク対策（住民基本台帳ファイル） 3．特定個人情報の使用 リスク2 アクセス権限の発行・執行の管理 具体的な管理方法	（記載なし）	＜申請管理システムにおける措置＞ 【アクセス権限の発効管理】 ・申請管理システムを操作する従事者の権限に応じたユーザID、アクセス権限の割付を行う。 【アクセス権限の失効管理】 ・担当替え等により操作権限を無くした者のユーザIDやアクセス権限について利用無効や権限削除を行う。	事前	申請管理システム導入

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
	Ⅲ特定個人情報ファイルの取扱いプロセスにおけるリスク対策（住民基本台帳ファイル） 3. 特定個人情報の使用 リスク2 アクセス権限の管理 具体的な管理方法	（記載なし）	＜申請管理システムにおける措置＞ ・共用IDは発行せず、必ず個人に対しユーザIDを発行する。 ・ユーザID単位で業務権限を設定し、システム内で閲覧・審査可能な業務を制限している。 ・担当替え等の際は、管理者により利用を無効とする。 ・定期的にユーザID一覧とアクセス権限の突合を行い確認する。	事前	申請管理システム導入
	Ⅲ特定個人情報ファイルの取扱いプロセスにおけるリスク対策（住民基本台帳ファイル） 3. 特定個人情報の使用 リスク2 特定個人情報の使用の記録 具体的な管理方法	（記載なし）	＜申請管理システムにおける措置＞ ・システムの操作履歴（アクセスログ・操作ログ）を記録する。 ・操作履歴について、各事務運用で必要となる期間と同一の期間、保管する。	事前	申請管理システム導入
	Ⅲ特定個人情報ファイルの取扱いプロセスにおけるリスク対策（住民基本台帳ファイル） 3. 特定個人情報の使用 リスク3 リスクに対する措置の内容	・住基等システム、及び統合基盤システム利用時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容を記録し、不適切な利用を抑止する。	・住民記録システム、統合基盤システム及び申請管理システム利用時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容を記録し、不適切な利用を抑止する。	事前	申請管理システム導入
	Ⅲ特定個人情報ファイルの取扱いプロセスにおけるリスク対策（住民基本台帳ファイル） 3. 特定個人情報の使用 リスク4 リスクに対する措置の内容	（記載なし）	＜申請管理システムにおける措置＞ ・申請管理システムから取得した個人番号付電子申請データ等のデータについて、改ざんや業務目的以外の複製を禁止する。	事前	申請管理システム導入
	Ⅲ特定個人情報ファイルの取扱いプロセスにおけるリスク対策（住民基本台帳ファイル） 7. 特定個人情報の保管・消去 リスク1 ⑤物理的対策	（記載なし）	【申請管理システムにおける措置】 ・申請管理システムはガバメントクラウド上で稼働するため、「ガバメントクラウドにおける措置」に記載のとおり。 ・申請管理システム接続端末の設置場所については業務時間外は施錠し入退室できなくするなどの物理的対策を講じる。	事前	申請管理システム導入
	Ⅲリスク対策（住民基本台帳ファイル） 7. 特定個人情報の保管・消去 リスク1 ⑥技術的対策	【ウイルス対策】 ・ウイルス対策ソフトウェアを導入し、サーバ及び端末機に常駐させることで、コンピュータウイルス等の不正プログラム検出を行っている。 ・ウイルス対策ソフトウェアについて、定期的に当該ソフトウェア及びパターンファイルの更新を実施している。 【不正アクセス対策】 ・住基等システム及び統合基盤システムは住民情報等を取り扱う重要システムが利用する専用ネットワークに接続しており、インターネットと物理的に接続されていない。 ・導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ・システム画面についてはスクリーンコピーを不可能とする設定を行っている。	＜ガバメントクラウドにおける措置＞ ①国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。 ②地方公共団体が委託したASP（「地方公共団体情報システムのガバメントクラウドの利用に関する基準」（以下「利用基準」という。）に規定する「ASP」をいう。以下同じ。）又はガバメントクラウド運用管理補助者（利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。）は、ガバメントクラウドが提供するマネージドサービスにより、ネットワークアクティビティ、データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに、ログ管理を行う。 ③クラウド事業者は、ガバメントクラウドに対するセキュリティの脅威に対し、脅威検出やDDos対策を24時間365日講じる。 ④クラウド事業者は、ガバメントクラウドに対し、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ⑤地方公共団体が委託したASP又はガバメントクラウド運用管理補助者は、導入しているOS及びミドルウエアについて、必要に応じてセキュリティパッチの適用を行う。 ⑥ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。 ⑦地方公共団体やASP又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。 ⑧地方公共団体が管理する業務データは、国及びクラウド事業者がアクセスできないよう制御を講じる。	事前	標準準拠システム移行に伴う変更
	Ⅲ特定個人情報ファイルの取扱いプロセスにおけるリスク対策（住民基本台帳ファイル） 7. 特定個人情報の保管・消去 リスク1 ⑥技術的対策	（記載なし）	＜申請管理システムにおける措置＞ ・申請管理システムはガバメントクラウド上で稼働するため、「ガバメントクラウドにおける措置」に記載するとおり。 ・LGWAN系ネットワークとマイナンバー利用事務系ネットワークの間にDMZ（隔離された領域）を設け、申請管理システムから外部への直接通信を遮断することにより、安全を確保している。また外部とのネットワーク接続について、境界FWや連携サーバで接続先との通信を限定している。	事前	申請管理システム導入
	Ⅲリスク対策（送付先情報ファイル） 3. 特定個人情報の使用 リスク2 特定個人情報の使用の記録	＜住基等システムにおける措置＞ ・住基等システムへのログイン記録、個人を特定した検索及び特定後の操作ログの記録を行う。操作者は個人まで特定でき、記録は5年間保存する。	＜住民記録システムにおける措置＞ ・住民記録システムへのログイン記録、個人を特定した検索及び特定後の操作ログの記録を行う。操作者は個人まで特定でき、記録は永年保存する。	事前	標準準拠システム移行に伴う変更
	Ⅲ特定個人情報ファイルの取扱いプロセスにおけるリスク対策（住民基本台帳ファイル） 7. 特定個人情報の保管・消去 リスク2	（記載なし）	＜申請管理システムにおける措置＞ ・申請データの再申請や申請情報の訂正が発生した場合には古い情報で審査等を行わないよう、履歴管理を行う。 ・サービス検索・電子申請機能（マイナポータルぴったりサービス）の電子申請データの取得に利用するDMZ（隔離された領域）内の連携サーバには個人番号付電子申請データを保有しない。	事前	申請管理システム導入

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
	Ⅲ特定個人情報ファイルの取扱いプロセスにおけるリスク対策（住民基本台帳ファイル） 7．特定個人情報の保管・消去 リスク3	（記載なし）	・ガバメントクラウドにおいては、データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去する。	事前	標準準拠システム移行に伴う変更
	Ⅳその他のリスク対策 2．従業者に対する教育・啓発	（記載なし）	＜申請管理システムにおける措置＞ 申請管理システムを利用する職員に対して、セキュリティ対策の研修を実施することとしている。	事前	申請管理システム導入
	Ⅵ 評価実施手続 1．基礎項目評価 ①実施日	令和3年12月21日	【公表日記載予定】	事後	
	Ⅵ 評価実施手続 2．国民・住民等からの意見の聴取	②実施日・期間 令和3年9月17日（金）から令和3年10月17日（日）まで ④主な意見の内容 ご意見はありませんでした。 ⑤評価書への反映 －	【パブリックコメント終了後に記載】	事後	
	Ⅵ 評価実施手続 3．第三者点検	①実施日 令和3年11月12日（金） ③結果 特定個人情報ファイルの取扱いについては、個人のプライバシー等の権利利益に与え得る影響を予測した上で特定個人情報の漏えいその他の事態を発生させるリスクを分析し、そのリスクを軽減するための措置が講じられていると認められる。	【第三者点検終了後に記載】	事後	
	別添1事務内容（住民基本台帳ファイル）	住基等システム	住民記録システム 大阪市の環境からガバメントクラウド環境へ変更	事前	標準準拠システム移行に伴う変更
	別添1事務内容（住民基本台帳ファイル）	（記載なし）	（図）申請管理システム　追加 （備考） 10．申請管理システムとの連携 10-① 住民がサービス検索・電子申請機能（マイナポータルぴったりサービス）で転入、転出の届出等を行う。 10-② 申請管理システムにて電子申請データを取得する。 10-③ 申請管理システムにて電子申請データを住民記録システムに向けてオブジェクトストレージに格納する。 10-④ 住民記録システムにて電子申請データを取得する。 10-⑤ 申請管理システムにてサービス検索・電子申請機能（マイナポータルぴったりサービス）上の申請受付ステータスを更新する。	事前	標準準拠システム移行に伴う変更
	別添1事務内容（本人確認情報ファイル・送付先情報ファイル）	既存住基システム	住民記録システム 市町村環境からガバメントクラウド環境へ変更	事前	標準準拠システム移行に伴う変更
	別添1事務内容（住民基本台帳ファイル）	住基等システム	住民記録システム 大阪市の環境からガバメントクラウド環境へ変更	事前	標準準拠システム移行に伴う変更
	別添1事務内容（本人確認情報ファイル・送付先情報ファイル）	既存住基システム	住民記録システム 市町村環境からガバメントクラウド環境へ変更	事前	標準準拠システム移行に伴う変更