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
1	枚方市　住民基本台帳事務　全項目評価書

個人のプライバシー等の権利利益の保護の宣言

枚方市は、住民基本台帳事務において特定個人情報ファイルを取り扱うに当たり、特定個人情報ファイルの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理解し、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軽減させるために適切な措置を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、ここに宣言する。

特記事項	

評価実施機関名

枚方市長

個人情報保護委員会　承認日 【行政機関等のみ】

公表日

令和8年3月30日

［令和7年5月　様式4］

項目一覧

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　※	市町村（特別区を含む。）（以下「市町村」という。）が住民を対象とする行政を適切に行い、また、住民の正しい権利を保障するためには、市町村の住民に関する正確な記録を整備しなくてはならない。 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、作成されたものであり、市町村における住民の届出に関する制度及びその住民たる地位を記録する各種の台帳に関する制度を一元化し、もって、住民の利便性を増進するとともに、行政の近代化に対処するため、住民に関する記録を正確かつ統一的に行うものである。市町村において、住民の居住関係の公証、選挙人名簿の登録、その他住民に関する事務の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。 枚方市は、住基法及び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（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。 ①　個人を単位とする住民票を世帯ごとに編製し、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、その他法で定め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 ⑪　個人番号の変更 ※なお、⑨の「個人番号の通知及び個人番号カードの交付」に係る事務については、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の規定する個人番号、個人番号カード、特定個人情報の提供等に関する省令（平成26年11月20日総務省令第85号）（以下「個人番号カード省令」という。）第35条（個人番号通知書、個人番号カード関連事務の委任）により機構に対する事務の一部の委任が認められている。そのため、当該事務においては、事務を委任する機構に対する情報の提供を含めて特定個人情報ファイルを使用する。
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	既存住民基本台帳システム（以下「既存住基システム」という。）

②システムの機能	■住民基本台帳機能 1．住民異動処理 ：転入や出生、入国、職権等により新たに住民票を作成する。また、記載事項に変更があった場合記載内容を変更する。さらに、転出、死亡、出国、職権等により住民票を除票とする。その後、法で定めた期間を超えた除票を消除する。 2．DV被害者等支援 ：DV被害者等への支援として、証明書発行抑止等を行う。 3．住民票照会：住民票情報の照会を行う。 4．証明書交付：住民票の写し等の証明を交付する。 5．通知発行：附票通知を行う。入管への通知を行う。 6．統計と帳票出力：人口統計用などの集計表や確認のための帳票を出力する。 7．住民基本台帳閲覧：閲覧補助簿の抽出と印刷を行う。 8．開示請求：交付ログ、画面参照ログの検索を行う。 9．住基ネット：住基ネットを介して本人確認情報の送受信を行う。 10．他システムとの連携 ：本市の庁内連携システム、自動交付システム等へ本人確認情報を提供する。 11．標準システム連携：住基カードの多目的機能の設定を行う。 ■印鑑登録機能 1．印鑑登録・廃止・停止・登録保留・修正：印鑑登録情報を逐次更新する。 2．証明書交付：印鑑登録証明書を出力する。 3．住民基本台帳連携 ：死亡、転出、職権消除等があった場合、自動的に印鑑登録を消除する。
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　（ 戸籍システム、自動交付システム（コンビニ交付）、法務省端末　　）
システム2～5	
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

②システムの機能	1．本人確認情報の更新 ：既存住基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。 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。 3．個人番号カードを利用した転入（特例転入） ：転入の届出を受け付けた際に、あわせて個人番号カードが提示された場合、当該個人番号カードを用いて転入処理を行う。 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。 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。 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知事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。 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、既存住基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。 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。
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　（　　）
システム3	
①システムの名称	自動交付システム
②システムの機能	1．証明書のコンビニ交付 コンビニエンスストアより、多目的利用サービス設定をされた住基カードや個人番号カードを利用して各種証明書を発行する。 発行を行う証明書の種類は住民票の写し、印鑑登録証明書、市・府民税課税証明書
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　（ LGWAN ASP　　）
システム4	
①システムの名称	中間サーバー

②システムの機能	1. 符号管理機能 　情報照会や情報提供の際に個人の識別子として用いる「符号」と、自機関内で個人を特定するために利用する「統一識別番号」とを紐付け、その情報を保管・管理する。 2. 情報照会機能 　情報提供ネットワークシステムを介して、他機関に対して情報提供の求めを発出するとともに、他機関から提供された情報を受領する。 3. 情報提供機能 　情報提供ネットワークシステムを介して、他機関からの情報提供の求めを受領するとともに、他機関に対して提供する情報を発出する。 4. 既存システム接続機能 　既存業務システム、団体内統合宛名システム、住基システムとの間で、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。 5. 情報提供等記録管理機能 　情報照会や情報提供があった旨の記録（＝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 　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 　情報を暗号化（あるいは復号）する。鍵情報及び照会許可用照合リスト情報を管理する。 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、職員に付与された権限に基づいた各種機能の制御、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 　バッチの状況管理、業務統計情報の集計、稼動状態の通知、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　（　　）
システム5	
①システムの名称	団体内統合宛名システム（番号連携サーバ）
②システムの機能	1. 宛名情報管理機能 　統一識別番号が未登録の個人に対して統一識別番号を付番する。宛名情報を統一識別番号、個人番号と紐付けて保存し、管理する。中間サーバー、既存業務システム等の要求に基づき、個人番号や統一識別番号に紐付く宛名情報を通知する。 2. 情報照会機能 　中間サーバーを通して他機関への情報照会要求を行い、照会結果を通知する。 3. 情報提供機能 　他機関へ提供する特定個人情報（連携対象）を中間サーバーへ連携する。 4. 符号要求機能 　情報連携の際に個人の識別子として用いる符号の取得要求を、既存住基システムや住基ゲートウェイに送信する。 5. 権限管理機能 　団体内統合宛名システムを利用する職員の認証、職員に付与された権限に基づいた各種機能の制御、特定個人情報（連携対象）へのアクセス制御を行う。
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　（ 中間サーバー、既存業務システム　　）
システム6～10	
システム11～15	
システム16～20	

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	市町村では、以下の3ファイルを下記に記載の通りの必要性から取り扱う。 （1）住民基本台帳ファイル ：住民基本台帳ファイルは、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、その住民異動情報を税や国民健康保険など、本市の業務に役立てることを目的として、以下の用途に用いられる。 ①住民基本台帳に関する事務処理を行うため、区域内の住民に係る最新の本人確認情報を管理する。 ②本市の庁内連携システム（統合型データベースシステム）を介して、税や国民健康保険などの業務所管課に最新の本人確認情報を通知する。 ③番号法に定める個人番号とすべき番号の生成要求及び個人番号の指定、変更の手続を行う。 ④コンビニ交付を行う自動交付システムに対して、最新の本人確認情報を通知する。 ⑤団体内宛名を管理する統合宛名システムに最新の本人確認情報を通知する。 （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情報を提供する。（個人番号通知書及び個人番号カード省令第35条（個人番号通知書、個人番号カード関連事務の委任）により機構に対する事務の一部の委任が認められている。）
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、市民等の負担軽減につながる。 また、個人番号カードによる本人確認や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つながる。

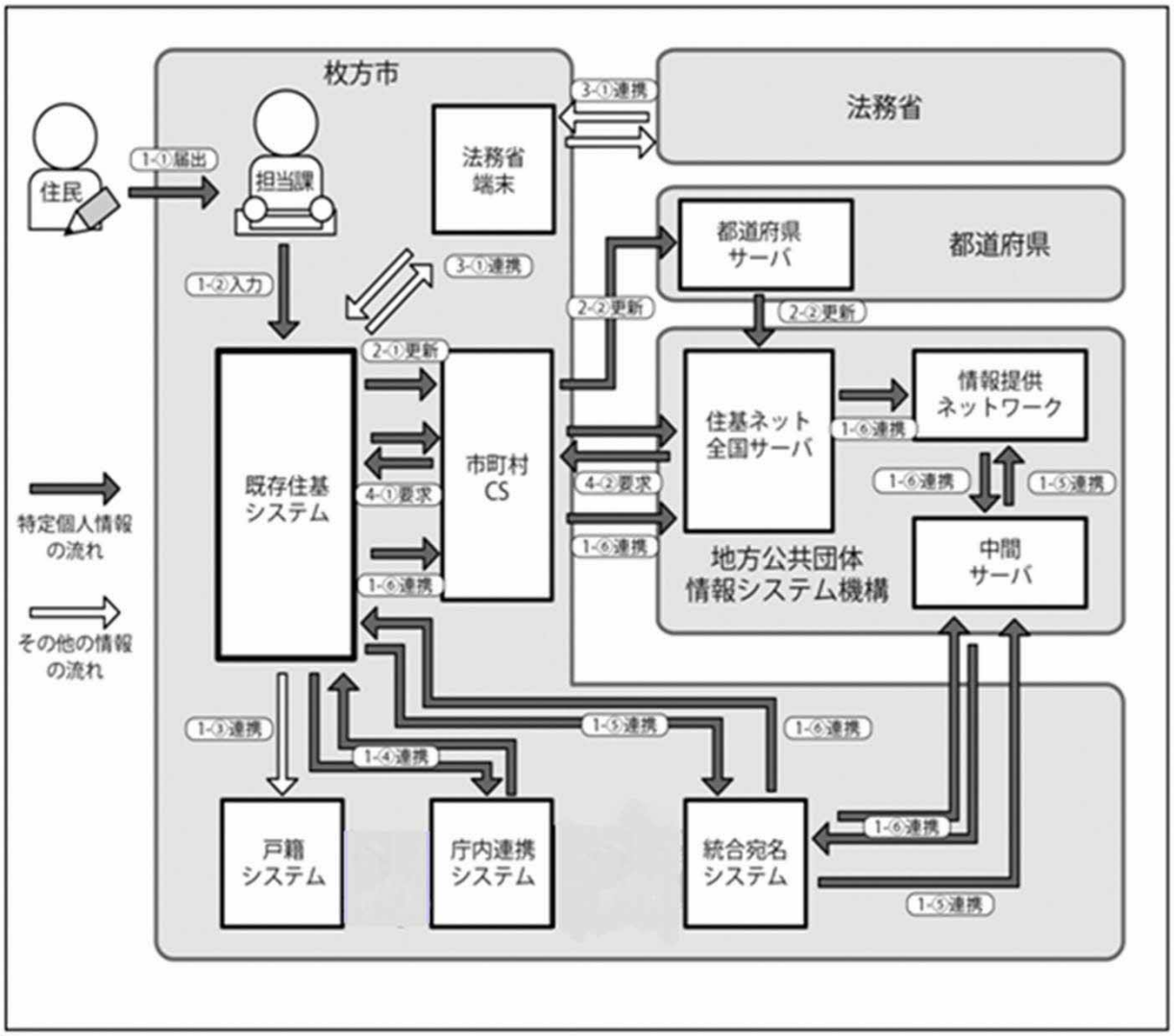
5. 個人番号の利用 ※

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）※未施行部分を含む。 ・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(本人等の請求によ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	【照会】 なし 【提供】 ・番号法、特定個人番号利用事務　別表第2の1、2、3、4、6、8、9、11、16、18、20、23、27、30、31、34、35、37、38、39、40、42、48、53、54、57、58、59、61、62、66、67、70、74、77、80、84、85の2、89、91、92、94、96、97、101、102、103、105、106、107、108、111、112、113、114、116、117、120の項
7．評価実施機関における担当部署	
①部署	枚方市　市民生活部　市民課
②所属長の役職名	市民課長
8．他の評価実施機関	
無し。	

（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（既存住基システムを中心とした事務の流れ）

① 住民基本台帳の記載・消除・変更に関する事務



（備考）

「（1）住民基本台帳ファイル」を取り扱う事務の内容（既存住基システムを中心とした事務の流れ）
① 住民基本台帳の記載・消除・変更に関する事務

1. 既存住基システムの更新と関係するシステムとの連携
1－① 住民から転入・出生（記載）、転出・死亡（消除）、転居・婚姻（変更）等の届出等を受け付ける。
1－② 住民基本台帳ファイルを更新する。
1－③ 戸籍システムの附票の情報と連携する。
1－④ 庁内連携システムの情報と連携する。
1－⑤ 統合宛名システム、中間サーバを経由して情報提供ネットワークシステムへ変更情報を連携する。
1－⑥ 統合宛名システムから住基ネットを経由して符号の要求を行い、符号を受け取る。

2. 住基ネットとの連携
2－① 市町村CS内の本人確認情報を更新する。
2－② 都道府県サーバに本人確認情報の更新情報を通知する。また、同サーバを経由して全国サーバに本人確認情報の更新情報を通知する。

3. 法務省との連携
3－① 法務省端末を通じて、外国人住民に関する市町村通知を法務省に送る。また、法務省から外国人住民に関する法務省通知を受ける。

4. 個人番号の新規取得、変更

4．個人番号の新規取得・変更
4－①②　住民票コード等を送信し、個人番号とすべき番号を受け取る。

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		
（1）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		［　10万人以上100万人未満　］　＜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	住民基本台帳法において、市町村長は、個人を単位とする住民票を世帯ごとに編成して、住民基本台帳を作成しなければならないとされているため。
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 ［ ○ ］5情報（氏名、氏名の振り仮名、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　（　戸籍に関する情報、外国籍住民に関する情報、選挙投票区情報等　）
	その妥当性	住民基本台帳法第七条(住民票の記載事項)で、住民票に記載をする事項となっているため。
	全ての記録項目	別添2を参照。
⑤保有開始日		平成27年8月2日
⑥事務担当部署		枚方市　市民生活部市　市民課

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 （ ）
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 （ 住民基本台帳ネットワークシステム ）
③入手の時期・頻度		出生や異動の届出、他市町村からの通知など、住民に関する記録項目への変更が発生する都度入手する。また、評価実施機関内の他部署からは定期的または随時に入手する。
④入手に係る妥当性		当情報は各種行政サービスの基礎となる情報であり、常に最新の状態にしておく必要があるが、枚方市の住民票に記載する時点で入手するため、上記③の時期と頻度になる。また、評価実施機関内の他部署からの情報については、資格情報に関する新規・変更・修正情報が定期的または随時提供されるので、提供の都度入手している。
⑤本人への明示		住民基本台帳法（第二章　住民基本台帳ほか）において明示されている。
⑥使用目的 ※		住民基本台帳法に基づき住民票へ記載を行う。また、住民サービスの基礎情報とする。
	変更の妥当性	使用目的を変更しない。
⑦使用の主体	使用部署 ※	市民生活部市民生活政策課（各支所、サービスセンター含む）、市民課
	使用者数	[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
⑧使用方法 ※		・住民票に記載することで、本人からの希望及び使用目的に応じて住民票の写しに記載する。 ・住民基本台帳ネットワークと本人確認情報及び転出証明書情報を連携する。 ・団体内統合宛名システム、中間サーバシステムを通じて情報提供ネットワークに住民票関連情報を連携する。 ・庁内関係各課と、番号法で定められた事務に対する住民基本台帳情報の提供を行う。 ・本市が本籍地である者の附票データを、ホストを経由して戸籍システムへ記録する。
	情報の突合 ※	・本人・代理人から入手する場合 届出書の記載内容と個人番号カード、通知カード等と突合の上、本人確認を行う。 ・住基ネットから入手する場合 住民票コードを突合し、対象者を特定する。 ・評価実施機関内の他部署から入手する場合 内部番号（識別番号）を突合し、対象者の特定をする。 ・機構で新たに個人番号が生成された場合は、個人番号の要求時に提供を行っている住民票コードと突合を行う。
	情報の統計分析 ※	個人番号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 ※	該当無し
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		戸籍・住民票・税証明申請受付及び交付（郵送請求分）一部業務委託
①委託内容		法令等により職員に限定されている事務以外の、郵送請求に関する証明書の申請受付・交付業務
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	[10万人以上100万人未満] <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じ。
	その妥当性	民間事業者に郵送請求に関する業務を一部委託することで、柔軟性のある運用体制を確保しながら、事務の効率化を図るため。
③委託先における取扱者数		[10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 （ 庁内にある既存住基システムのサーバー及び端末を直接使用する。 また、ガバメントクラウド環境に設置される住基システム等のサーバに対し、 事業者拠点よりネットワーク経由でアクセスし、運用・保守作業を行う（以下 ではこの方法を、「リモート保守」という）。 ）
⑤委託先名の確認方法		市民等から委託先名の問合せがあった場合は、枚方市が回答する。
⑥委託先名		株式会社エイジェック
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2～5		
委託事項2		既存住基システム等の運用保守
①委託内容		既存住基システム等の運用保守（システムの賃借契約に含まれるもの）
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	［ 10万人以上100万人未満 ］ ＜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じ。
	その妥当性	既存住基システムの安定稼動のため、専門的知識・技術を持つ民間事業者に運用保守を任せている。
③委託先における取扱者数		［ 10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　（ガバメントクラウド環境に設置される住基システム等のサーバに対し、事業者拠点よりネットワーク経由でアクセスし、運用・保守作業を行う（以下では　）この方法を、「リモート保守」という。）
⑤委託先名の確認方法		市民等から委託先名の問合せがあった場合は、枚方市が回答する。
⑥委託先名		行政システム株式会社大阪支店
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 （ 20 ）件 [ ] 行っていない
提供先1	番号法第19条第8号に基づく主務省令第2条の表に掲げる情報照会者（別紙1参照）
①法令上の根拠	番号法第１９条第8号に基づく主務省令第2条の表
②提供先における用途	番号法第19条第8号に基づく主務省令第2条の表第2欄に掲げる各事務
③提供する情報	住民基本台帳法第七条第四号に規定する事項（世帯主についてはその旨、世帯主でない者については世帯主の氏名及び世帯主との続柄）
④提供する情報の対象となる本人の数	[10万人以上100万人未満] ＜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	住民基本台帳ファイルに記録されているもの。
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	別紙2を参照。
①法令上の根拠	別紙2を参照。
②移転先における用途	別紙2を参照。
③移転する情報	別紙2を参照。
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	別紙2を参照。
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　（ 別紙2を参照。　　）
⑦時期・頻度	別紙2を参照。
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 ※		＜枚方市における措置＞ 入退出管理カードにより入退出管理を行っている施錠された管理区域内に設置したサーバで管理する。 サーバへのアクセスはID／パスワードによる認証が必要となる。 書類は所定の施錠可能な保管庫で保管する。 ＜ガバメントクラウドにおける措置＞ ①システムのサーバ等は、政府情報システムのセキュリティ制度であるISMAPの認証を取得したクラウド事業者が運営するデータセンターに設置し、セキュリティ管理策が適切に実施される。 ②特定個人情報は、クラウド事業者が管理する日本国内のデータセンター内に保存され、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。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームはデータセンターに設置しており、データセンターへの入館及びサーバー室への入室を厳重に管理する。 ②特定個人情報は、サーバー室に設置された中間サーバー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に保存される。
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	・住民票に記載されている限り保管をする必要がある。 ・住民基本台帳に基づき、転出等の事由で除票となった住民票については、同法施行令第34条に基づき、150年間保管する。
③消去方法		＜枚方市における措置＞ ・既存住基システムに記録されたデータのうち、平成26年6月19日以前に住民票が除票になって5年を経過したものについて、システムで判別し、出力・閲覧できないようにする。ただし、行政事務の基礎データとして直ちに不要になるものではないので、直ちには消去せず、毎年要不要の判断を行った上で、不要であれば消去する。 ・申請書等の書類は、保存年限の経過後、溶解して廃棄する。 ＜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市（委託先を含む）の操作によって実施し、国及びクラウド事業者は、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。 ＜中間サーバー・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地方公共団体からの操作によって実施されるため、通常、中間サーバー・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、中間サーバー・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、物理的破壊又は専用ソフト等を利用して完全に消去する。

7. 備考

無し。

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		
（2）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		［　10万人以上100万人未満　］　＜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 ［○］5情報（氏名、氏名の振り仮名、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、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8月2日
⑥事務担当部署		枚方市　市民生活部　市民課

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　（ 既存住基システム　　）
③入手の時期・頻度		住民基本台帳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、まず既存住基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が既存住基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6－6（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	使用目的を変更しない。
⑦使用の主体	使用部署 ※	市民生活部市民生活政策課（各支所、サービスセンターを含む）、市民課
	使用者数	[　　50人以上100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、既存住基システムから当該本人確認情報の更新情報を受領し(既存住基システム→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）。 ・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 ※	該当無し。
⑨使用開始日		平成27年8月6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 （ 1 ） 件
委託事項1		既存住基システム等の運用保守
①委託内容		既存住基システム等の運用保守（システムの賃借契約に含まれるもの）
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	[10万人以上100万人未満] <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じ。
	その妥当性	既存住基システムの安定稼動のため、専門的知識・技術を持つ民間事業者に運用保守を任せている。
③委託先における取扱者数		[10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 （ 庁内にある既存住基システムのサーバー及び端末を直接使用する。 ）
⑤委託先名の確認方法		市民等から委託先名の問合せがあった場合は、枚方市が回答する。
⑥委託先名		行政システム株式会社大阪支店
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2～5		
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	[10万人以上100万人未満] ＜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2～5	
提供先2	都道府県及び地方公共団体情報システム機構（機構）
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	[　10万人以上100万人未満　]　＜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　　[　] 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	
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 ※		入退出管理カードにより入退出管理を行っている施錠された管理区域内に設置したサーバで管理する。 サーバへのアクセスはID／パスワードによる認証が必要となる。
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、平成14年6月10日総務省告示第334号（第6－8（1）市町村長における本人確認情報の消去）に定める期間（150年間）保管する。
③消去方法		本人確認情報ファイルに記録されたデータをシステムにて自動判別し消去する。
7. 備考		
無し。		

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		
（3）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		［　10万人以上100万人未満　］　＜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）に基づき、個人番号通知書を個人番号の付番対象者全員に送付する必要がある。 また、同法第17条第1項（個人番号カードの交付等）により、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ことから、合わせて、交付申請書を通知カード又は個人番号通知書送付者全員に送付する必要がある。 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 ［ ○ ］5情報（氏名、氏名の振り仮名、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、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、法令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委任するために、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5日
⑥事務担当部署		枚方市　市民生活部　市民課

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　（ 市町村　　） [　　] 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　（ 既存住基システム　　）
③入手の時期・頻度			使用開始日から個人番号通知書送付までの一定の期間に、番号法施行日時点における住民の送付先情報をまとめて入手する（以降、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において電子記録を暗号化した後に提供する必要がある。
⑤本人への明示			個人番号の通知については、番号法第7条第1項に明示されている。
⑥使用目的 ※			法令に基づく委任を受けて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		使用目的を変更しない。
⑦使用の主体	使用部署 ※		市民生活部市民生活政策課（各支所、サービスセンターを含む）、市民課
	使用者数		[　　50人以上100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 ※			・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法令に基づいて委任する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））。
	情報の突合 ※		入手した送付先情報に含まれる4情報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 （ 1 ） 件
委託事項1		既存住基システム等の運用保守
①委託内容		既存住基システム等の運用保守（システムの賃借契約に含まれるもの）
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	[10万人以上100万人未満] <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じ
	その妥当性	既存住基システムの安定稼動のため、専門的知識・技術を持つ民間事業者に運用保守を任せている。
③委託先における取扱者数		[10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 （ 庁内にある既存住基システムのサーバー及び端末を直接使用する。 ）
⑤委託先名の確認方法		市民等から委託先名の問合せがあった場合は、枚方市が回答する。
⑥委託先名		行政システム株式会社大阪支店
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2～5
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（機構）
①法令上の根拠	番号法第19号第5号
②提供先における用途	市町村からの法令に基づく委任を受け、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」と同上。
④提供する情報の対象となる本人の数	[10万人以上100万人未満] ＜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	使用開始日から通知カード送付までの一定の期間に、番号法施行日時点における住民の送付先情報をまとめて提供する（以降、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　　[　] 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	
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 ※		入退出管理カードにより入退出管理を行っている施錠された管理区域内に設置したサーバで管理する。 サーバへのアクセスはID／パスワードによる認証が必要となる。 書類は所定の施錠可能な保管庫で保管する。
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、また、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		保存期間が到来した送付先情報は、機構より指定された方法により、システム上、一括して消去する仕組みとする。 申請書等の書類は、保存年限の経過後、溶解して廃棄する。

7. 備考
無し。

（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. 整理番号、2. 世帯番号、3. 住民票コード、4. 個人番号、5. 異動事由、6. 異動年月日、7. 届出年月日、8. 備考欄、9. 住民区分(住民、転出、死亡等)、10. 処理年月日、11. 氏名、12. かな氏名、13. 性別、14. 出生年月日、15. 世帯主名、16. 住民となった日、17. 住民でなくなった日(消除日)、18. 住所、19. 住所コード、20. 住所を定めた日、21. 転入前住所、22. 転出予定住所、23. 転出確定住所、24. 本籍、25. 筆頭者、26. 続柄、27. 30条45規定区分、28. 国籍・地域、29. 在留資格、30. 在留期間等、31. 在留期間等の満了の日、32. 外国人住民となった日、33. 外国人漢字氏名、34. 外国人英字氏名、35. 通称名、36. 通称名かな、37. 併記名、38. 在留カード等の番号、39. 特別永住者証明書の交付年月日、40. 住基カード有無、41. 国保資格記号番号、42. 国保資格得喪、43. 国保資格取得日、44. 国保資格喪失日、45. 年記号番号、46. 年金種別、47. 年金取得日、48. 年金喪失日、49. 介護資格得喪、50. 介護資格取得日、51. 介護資格喪失日、52. 介護認定有無、53. 児童手当資格取得月、54. 児童手当資格喪失月、55. 後期高齢被保険者番号、56. 後期高齢得喪、57. 後期高齢資格取得日、58. 後期高齢資格喪失日、59. 印鑑登録有無、60. コンビニ交付登録有無、61. 選挙投票区

（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

（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

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	
（1）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	・申請等の窓口において届出／申請内容や本人確認書類（身分証明書等）の確認を厳格に行い、対象者以外の情報の入手の防止に努める。 ・申請者が本人及び同一の世帯以外の情報を誤って記載しないように予め記入様式が定められた書面に必要事項のみを記入する方式とする。 ・システムへの入力後、別の職員が異動届とシステムの入力内容を照合し、確認を行う。 ・住基ネットを通じての入手は対象者以外の情報を入手できないように、仕組みとして担保されている。 ・業務に関係のない不必要な書類は受け取らないよう、職員に対する教育を徹底する。もし、不必要な書類を提出された場合は返却している。 ・資料が電子記録媒体で提出された場合、本市で受領すべきものかその内容を十分に確認し、本市分でない場合は返却している。
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	・申請等の窓口において届出／申請内容や本人確認書類（身分証明書等）の確認を厳格に行い、対象者以外の情報の入手の防止に努める。 ・申請者が本人及び同一の世帯以外の情報を誤って記載しないように予め記入様式が定められた書面に必要事項のみを記入する方式とする。 ・システムへの入力後、別の職員が異動届とシステムの入力内容を照合し、確認を行う。 ・住基ネットを通じての入手は対象者以外の情報を入手できないように、仕組みとして担保されている。 ・業務に関係のない不必要な書類は受け取らないよう、職員に対する教育を徹底する。もし、不必要な書類を提出された場合は返却している。 ・資料が電子記録媒体で提出された場合、本市で受領すべきものかその内容を十分に確認し、本市分でない場合は返却している。
その他の措置の内容	特に無し。
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	・住民異動届出においては住民基本台帳法及び関係法令の規定に基づき、書面で、本人あるいは代理人による届出のみを受領することとし、受領の際は必ず本人あるいは代理人の本人確認及び委任状の確認を行うこととしており、必要最小限の提示を求め、住民に不必要な負担を負わせないようにしている。 ・システムを通じた入手を行う必要がある職員を特定し、ユーザIDとパスワードによる認証を行う。また、認証後は利用機能の認可機能により、そのユーザがシステム上で利用可能な機能を制限することで不適切な方法での入手を行うことができないように対策を実施している。 ・システムログを取得する等して、情報の取扱状況を記録していることを職員に周知することにより、権限のない職員による情報の取扱いを抑止する。 ・業務に関係のない情報を入手しないよう、職員に対する教育を徹底する。 ・特定個人情報を入手する際は、利用目的を入手元に伝える。
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	・窓口において、対面で個人番号カードなどの本人確認資料で、本人の確認を行う。 ・代理人の場合は、まずは代理人の運転免許証、または旅券等の提示を受けて、代理人の本人確認を行う。次に、本人の個人番号カード、通知カードと運転免許証、または旅券等の提示を受けて、本人の個人番号の確認を行う。そして、委任状など代理権を証する書類を確認する。
個人番号の真正性確認の措置の内容	・出生等により新たに個人番号が指定される場合や転入の際には個人番号カード（若しくは通知カードと法令により定められた身分証明書の組み合わせ）の提示がない場合には、住基ネットにて本人確認情報と個人番号の対応付けの確認を行う。

特定個人情報の正確性確保の措置の内容	・住居表示台帳により居所の確認を行う。 ・前住所地が市外の場合、その自治体の発行する転出証明書の提出を求める。 ・住基ネットを介し機構に照会する。 ・システムへの入力後、別の職員が異動届とシステムの入力内容を照合し、確認を行う。 ・住基ネットで記載された本人確認情報と、定期的に整合性チェックを行う。 ・入手した情報については、窓口での聞き取りや添付書類との照合等を通じて確認することで正確性を確保している。
その他の措置の内容	特に無し。
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	・書面の場合は、本人もしくは代理人から直接書面を受け取ることを原則とし、郵送の場合は市役所住所を明記して、当該住所宛てに送るように説明する。 ・住民からの届出書については、特定個人情報の漏洩及び紛失を防止するため、入力及び照合した後は、鍵付の書庫に保管する。また、定期的に、漏えい・紛失がないか保管状況をチェックする。 ・窓口で対面にて受け取り、事務処理が完了したら、速やかに上記保管場所で管理する運用を徹底する。 また、郵送の場合は、必ず郵便または信書便を利用し、記載事項や添付書類に漏れがないよう十分に確認の上、市役所に送付する旨を市ホームページや広報にて案内をする。なお、返信用封筒や、記載要領に担当課の宛名・住所を明記して、確実に返送されるようにする。 ・既存住基システムは住基ネット・法務省端末以外とは外部接続していない。 ・既存住基システムの操作者の認証を行い、不特定の職員が操作できないようにしている。 ・窓口に衝立を設置することにより、応対に係る書類等の内容が、他の職員や来庁者の目に触れることを防止する。
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	
・端末のディスプレイを、来庁者から見えない位置に置く。 ・本人確認情報が表示された画面のハードコピーの取得は事務処理に必要となる範囲にとどめ、不要になったときは、シュレッダー等の復元不可能な方法により直ちに廃棄する。 ・スクリーンセーバーを利用し、離席したときも情報を覗けないようにする。	

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	個人番号利用業務以外の業務又は個人番号を必要としない業務から住民情報の要求があった場合は、個人番号が含まれない情報のみを提供するようにアクセス制御を行う。	
事務で使用するその他のシステムにおける措置の内容	・既存住基システムと市町村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。 ・戸籍システムとは個人番号を用いた連携を行わない。 ・法務省端末とも個人番号を用いた連携を行わない。 ・戸籍システム・自動交付システム以外の庁内の他の業務システムから直接アクセスできないようにシステム的に制限されている。	
その他の措置の内容	特に無し。	
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	端末にアクセスするためのカード認証とシステムにアクセスするためのID・パスワードによる認証を行っており、業務上必要最低限に限定した特定の職員や作業従事者のみが照会できるようにしている。また、利用範囲の認可機能により、その使用者がシステム上で利用可能な機能を制限することで、不適切な方法による情報の入手が行えない対策を実施している。	
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	本人確認情報の管理について、以下の管理を行う。 （1）ID/パスワードの発効管理 ・アクセス権限が必要となった場合、事務を担当する課長代理が事務ごとに更新権限の必要があるか、照会権限のみでよいかの別を確認し、事務に必要なアクセス権限のみを申請する。 ・申請に基づき、システム担当課長代理の確認の上、課長が承認する。また、当該事由が生じた際にはシステム担当がアクセス権限を更新し、別の職員が入力内容を照合・確認した上で当該IDを発効させる。 （2）失効管理 ・定期的又は異動／退職等のイベントが発生したタイミングで、権限を有していた職員の異動／退職情報をシステム担当課長代理が確認し、当該事由が生じた際には権限の失効を課長が承認する。その後、システム担当がアクセス権限を更新し、別の職員が入力内容を照合・確認した上で当該IDを失効させる。	
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	・システム担当課長代理はユーザIDやアクセス権限を、システムから出力された一覧をもとに定期的（定期異動ごと）に確認し、業務上アクセスが不要となったIDやアクセス権限を変更又は削除する。 ・委託先・再委託先のアクセス権限を持つものにたいしても、同様の扱いを行っている。	
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	・システムを操作したログ（日時・利用者・操作内容等）を取得し、磁気ディスクに記録し、必要に応じて操作履歴を解析する。 ・バックアップされたログは定められた期間、保管する。 ・操作履歴の確認により、本人確認情報の検索に関して不正な操作の疑いがある場合は、申請文書等との整合性を確認する。	
その他の措置の内容	システム画面を表示中に離席する場合は、システムからログオフする。	
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： 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	・システム全般の利用に係る証跡（ログ）を取得する。 ・職員を対象に個人情報保護及び情報セキュリティに関する研修や注意喚起を行い、業務外利用の禁止等について徹底する。新たに配属になった職員には個人情報保護及び情報セキュリティに関する研修を別途行う。 ・委託先に対しては業務外で使用しないよう仕様書に定め、個人情報保護にかかる誓約書を提出させる。再委託先も同様に扱う。 ・臨時職員、委託先等の職員以外の従業者については、契約時に、業務上知り得た情報の業務外利用の禁止に関する条項を含む誓約書に署名をさせる。 ・アクセス記録管理を行っており、業務外利用をした場合には特定可能であることを職員に周知し、事務外の利用を抑止している。
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
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	・権限を与えられていない者は情報の複製ができない仕組みとしており、端末のUSB端子からはシステム的に複製できない仕組みとなっている。また、CD・DVDへの複製もできない仕組みとなっている。 ・委託先に対しては仕様書にて許可を得ない複製を禁止し、個人情報保護にかかる誓約書を提出させる。再委託先も同様に扱う。 ・職員に対しては、個人情報保護及び情報セキュリティに関する研修や注意喚起を行う。 ・サーバが設置されている管理区域に委託業者によるスマートフォンなどの持ち込みは禁止しており、また、外部記憶媒体についても許可制としている。 ・特定個人情報の提供は、法令等の規定がある場合以外は認められない旨を職員等に周知する。 ・システムから抽出するデータには個人番号を含めないことで、端末に特定個人情報ファイルが作成されないようにしている。 ・バックアップファイルの取得は入退室管理をしているサーバ室のみでの作業に限定されている。 ・システム上、管理権限を与えられた者以外、情報の複製は行えない仕組みとする。
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
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	
・端末のディスプレイを、来庁者から見えない位置に置く。 ・本人確認情報が表示された画面のハードコピーの取得は事務処理に必要となる範囲にとどめ、不要になったときは、シュレッダー等の復元不可能な方法により直ちに廃棄する。 ・スクリーンセーバーを利用し、離席したときも情報を覗けないようにする。	

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	・システムの構築や運用を委託するときは、プライバシーマークの認証か情報セキュリティマネジメントシステムの認証の取得を要件としている。また、社内教育に関する条件として、セキュリティに関する研修及びプライバシー保護に関する研修等を実施する旨を規定し、特定個人情報の保護を適切に行える委託先であることを確認する。 ・委託にかかる実施体制の提出を義務付けている。 ・リモート保守を行う事業者の事業所については、情報セキュリティマネジメントシステム等の情報セキュリティの第三者認証を取得していることを条件とし、セキュリティ対策の実効性を確保する。第三者認証を取得していない場合等で必要と判断する場合、職員が実地確認を行い、セキュリティ対策の実効性を確保する。	
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	・委託事業者には、特定個人情報保護に関する特記仕様書の内容を順守してもらう。 ・必要に応じて、個人情報保護にかかる誓約書を提出を求める。再委託先も同様に扱う。 ・事前に申請許可された者以外はアクセスできないよう制御し、業務上必要最低限に限定したシステム操作の権限を与えている。 ・作業者を限定するために、委託作業者の名簿を提出させる。	
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	・システムを操作したログ（日時・利用者・操作内容等）を取得し、磁気ディスクに記録し、必要に応じて操作履歴を解析する。 ・バックアップされたログは定められた期間、保管する。	
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	【ルールの内容】 証明書を発行する際、本人確認を厳格におこない誤って証明書を発行することがないように徹底する。 【ルール遵守の確認方法】 委託契約の報告条項に基づき、定期的に特定個人情報の取扱いについて書面にて報告させ、必要があれば当市職員が現地調査している。	
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	【ルールの内容】 委託先との間で、以下の事項を委託先に義務付ける「個人情報保護に関する特記仕様書」を提示して契約する。 ・番号法等の関係法令の遵守・秘密の保持・取扱区域外への情報持ち出しの禁止・目的外利用の禁止・複製の禁止・情報の返却、消去、廃棄・従業員の特定・従業員への監督及び教育・市の検査、報告の求めへの応諾・漏えい等事案に係る損害の賠償・再委託の条件・再委託先に対する監督とその履行状況の報告・その他枚方市保有個人情報安全管理規程に基づき職員が実施する措置に準じた措置の実施・特記仕様書に違反する行為の契約解除事由への該当 【ルール遵守の確認方法】 業務実施内容について、定例会で定期的に報告を求めている。	
特定個人情報の消去ルール	[　　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	【ルールの内容】 特定個人情報保護に関する覚書の、提供資料の返還又は廃棄の項において、廃棄方法や、事前に書面で承認を得ること、廃棄完了後の報告、本市の立会いに応じることを定めている。 【ルール遵守の確認方法】 委託契約の報告条項に基づき、定期的に特定個人情報の取扱いについて書面にて、破棄、消去の方法、完了日等報告させ、必要があれば当市職員が現地調査することも可能とする。	

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	委託先との間で、以下の事項を委託先に義務付ける「個人情報保護に関する特記仕様書」を提示して契約する。 ・番号法等の関係法令の遵守・秘密の保持・取扱区域外への情報持ち出しの禁止・目的外利用の禁止・複製の禁止・情報の返却、消去、廃棄・従業員の特定・従業員への監督及び教育・市の検査、報告の求めへの応諾・漏えい等事案に係る損害の賠償・再委託の条件・再委託先に対する監督とその履行状況の報告・その他枚方市保有個人情報安全管理規程に基づき職員が実施する措置に準じた措置の実施・特記仕様書に違反する行為の契約解除事由への該当
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		[再委託していない] ＜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	特に無し。
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

'・サーバ室で受託業者が作業する場合は、市民課職員が立ち会う。
・委託先従業員が職員の許可を得ずに外部記憶媒体をサーバー室に持ち込む事を禁止するとともに、スマートフォン等については一切の持込を禁止する。

・リモート保守を行う事業者の事業所については、情報セキュリティマネジメントシステム等の情報セキュリティの第三者認証を取得していることを条件とし、セキュリティ対策の実効性を確保する。第三者認証を取得していない場合等で必要と判断する場合、職員が実地確認を行い、セキュリティ対策の実効性を確保する。

＜リモート保守環境におけるその他のリスクと措置＞
・リモート保守を行う事業所の執務エリアは入退室管理された区画とし、作業者の入退室記録を取得する。また保守作業に利用する端末の利用記録の取得や、監視カメラでの監視体制を敷き、作業者へも周知することで、不適切な方法での情報入手を抑止する。
・リモート保守環境とガバメントクラウドへの接続については、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し、通信経路上での第三者からの情報窃取を行えないよう対策する。
・ガバメントクラウドの管理画面に対して、例外的にインターネット経由でアクセスする場合は、多要素認証によりアクセスを行う。
・リモート保守で利用する端末等については、コンピュータウィルス対策ソフトウェアを導入しており、パターンファイルも最新版が適用されるよう管理する。また、OSには必要に応じてパッチ適用を実施する。端末内へのデータ保存を行わないシンクライアント端末を利用し、コンピュータウィルス対策ソフトウェアを導入できない場合については、シンクライアント端末からの接続先となる作業環境に対して同様の対策を実施する。
・システムのリモート保守で委託事業者が利用する端末等へは、原則として、特定個人情報の保存を行えないように措置する。端末等への特定個人情報の保存を必要とする場合、使用後は速やかに消去するとともに、端末等のディスク廃棄時には物理的破壊または専用ソフトでのデータ消去を行わせ、データ消去証明書の提出により確認する。

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	庁内連携システムを利用した情報の移転は全て記録を残している。	
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	・他課の事務に属するデータを電子計算処理において利用しようとする場合は、当該事務を所管する部署の承認を受けなければならない。 ・審査の結果、承認されたものについてのみ、データの移転・提供を行う。	
その他の措置の内容	・庁内連携システムは、データの移転が認められた移転先からのみアクセスを許可された連携システムへデータを移転する。 ・違反行為を行った場合は、法令の罰則規定により措置を講じる。 ・個人番号の盗用等が発生した場合は、番号法第7条第2項により、職権及び該当者からの申請により個人番号の変更を行う。	
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
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	庁内連携システムを通して情報照会や情報提供を一元的に行い、その記録を逐一保存することで、不適切な方法で特定個人情報がやりとりされることを防いでいる。	
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	庁内連携システムでは本業務で保有する情報を全て連携することは行わず、移転元から承認された情報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、決められた提供・移転先のみにしか情報の提供・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		
・特定個人情報をフラッシュメモリ等の外部記憶媒体を用いて移転する場合は、データの暗号化の措置を施したうえで移転を行う。 ・サーバが設置されている管理区域に委託業者によるスマートフォンなどの持ち込みは禁止しており、また、外部記憶媒体についても許可制としている。		

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	＜既存住基システムにおける措置＞ 統合宛名システム等では本業務で保有する情報を全て連携することは行わず、番号法の規定に基づき認められる情報のみしか照会できないような仕組みを構築している。 ＜中間サーバー・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の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、中間サーバーにも格納して、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中間サーバーの職員認証・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 ＜中間サーバーの運用における措置＞ ・情報提供ネットワークシステムを利用する場合は、どの職員がどの特定個人情報をいつ利用したかが記録される。番号法及び条例上認められる提供以外受け付けないようにしており、システム上提供が認められなかった場合についても記録を残す。
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	＜既存住基システムにおける措置＞ ファイアウォール等でアクセス制御を行い、インターネットに接続されている情報系のシステムとは切り離されているため、外部からの不正アクセスはできない仕組みとなっている。 また、提供の記録が逐一保存される仕組みが整備された情報提供ネットワークシステムを用いて連携することで、不適切な方法で特定個人情報が提供されることを防止する。 ＜中間サーバー・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中間サーバーの職員認証・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 ＜中間サーバー･プラットフォームにおける措置＞ ①中間サーバーと既存システム、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中間サーバーと団体についてはVPN（バーチャルプライベートネットワーク）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流出･紛失のリスクに対応している。 ③中間サーバー・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。 ＜中間サーバーの運用における措置＞ ・情報照会、情報提供の記録が保存される統合宛名システム等を通してやり取りすることで、不適切な方法で特定個人情報が流出・紛失することを防止する。
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	＜枚方市における措置＞ 統合宛名システム等では本業務で保有する情報を全て連携することは行わず、番号法の規定に基づき認められる情報のみしか照会できないような仕組みを構築している。 また、中間サーバへの連携は適切な頻度で行い、その正確性を担保する。 ＜中間サーバー・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	
＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーの職員認証・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。 ＜中間サーバー･プラットフォームにおける措置＞ ①中間サーバーと既存システム、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中間サーバーと団体については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中間サーバー・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、中間サーバー・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、中間サーバー・プラットフォームの保守・運用を行う事業者の情報流出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	＜枚方市における措置＞ ・サーバーの盗難を防ぐために、施錠ができる場所等に保管し、施錠をしている。また、設置場所への入退出はICカードにより記録している。 ・停電(落雷等)によるデータの消失を防ぐために、サーバーに無停電電源装置等を付設している。 ・火災によるデータ消失を防ぐために、施設内に消火設備を完備している。 ＜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。 ＜中間サーバー・プラットフォームにおける措置＞ ・中間サーバー・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	＜枚方市における措置＞ ・ネットワークを通じて悪意の第三者が侵入しないよう、ファイアウォール・不正侵入防止装置（IPS）を設置しており、、それらの機器は24時間の監視を行い、定期的にログの解析を行っている。 ・インターネットとつながらないようにネットワークをファイアウォールで切断している。 ・コンピュータウィルス対策ソフトウェアを導入しており、パターンファイルも最新版が適用されるよう管理している。 ・OSには必要に応じてパッチ適用を実施している。 ＜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、市の保有データにアクセスしない契約等となっている。 ②市が委託した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【第1.0版】」（令和4年10月　デジタル庁。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市が委託した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市や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市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。 ＜中間サーバー・プラットフォームにおける措置＞ ・中間サーバー・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。 ・中間サーバー・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。
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	該当無し。
	再発防止策の内容	該当無し。
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	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。その取り扱いについては、生存者の個人番号と同様の安全管理措置を講じている。
その他の措置の内容		特に無し。
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。 ・住基ネットで記載された本人確認情報と、定期的に整合性チェックを行う。
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
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	＜枚方市における措置＞ ・住民基本台帳ファイルに記録されたデータのうち、平成26年6月19日以前に住民票が除票になって5年を経過したものについて、システムで判別し、出力・閲覧できないようにする。ただし、行政事務の基礎データとして直ちに不要になるものではないので、直ちには消去せず、毎年要不要の判断を行った上で、不要であれば消去する。 ・磁気ディスクの廃棄時は、手順書等に基づき、内容の復元及び判読が不可能になるような方法により消去する。 ・住民異動届等の紙媒体については、帳簿等を作成し、保管及び廃棄の運用が適切になされていることを適時確認するとともに、その記録を残す。また、廃棄時には、規程に基づき、溶解処理による廃棄を行うとともに、廃棄文書目録を残す。 ＜ガバメントクラウドにおける措置＞ 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。
その他の措置の内容		特に無し。
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		
・サーバが設置されている管理区域に委託業者によるスマートフォンなどの持ち込みは禁止しており、また、外部記憶媒体についても許可制としている。		

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 ※（7. リスク1⑨を除く。）

1. 特定個人情報ファイル名	
（2）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	本人確認情報の入手元は既存住基システムに限定されるため、既存住基システムへの情報の登録の際に次のことを行う。 ・申請等の窓口において届出／申請内容や本人確認書類（身分証明書等）の確認を厳格に行い、対象者以外の情報の入手の防止に努める。 ・申請者が本人及び同一の世帯以外の情報を誤って記載しないように予め記入様式が定められた書面に必要事項のみを記入する方式とする。 ・システムへの入力後、別の職員が異動届とシステムの入力内容を照合し、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	・平成14年6月10日総務省告示第334号（第6－6　本人確認情報の通知及び記録）等により市町村CSにおいて既存住基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。 ・正当な利用目的以外の目的にデータベースが構成されることを防止するため、本人確認情報の検索を行う際の検索条件として、少なくとも性別を除く2情報以上（氏名と住所の組み合わせ、氏名と生年月日の組み合わせ）の指定を必須とする。 ・申請者が必要な情報だけを記載できるように書面式とする。
その他の措置の内容	特に無し。
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を既存住基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： 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	窓口において、対面で個人番号カードなどの本人確認資料で、本人の確認を行う。
個人番号の真正性確認の措置の内容	・個人番号カード等の提示を受け、本人確認を行う。 ・出生等により新たに個人番号が指定される場合や、転入の際に個人番号カード（若しくは通知カードと法令により定められた身分証明書の組み合わせ）の提示がない場合には、市町村CSにおいて本人確認情報と個人番号の対応付けの確認を行う。
特定個人情報の正確性確保の措置の内容	・本人確認情報の入力、削除及び訂正を行う際には、整合性を確保するために、入力、削除及び訂正を行った者以外の者が確認する等、必ず入力、削除及び訂正した内容を確認する。 ・入力、削除及び訂正作業に用いた帳票等は、当市で定める規程に基づいて管理し、保管する。 ・本人確認情報に誤りがあった際に訂正を行う場合には、本人確認情報管理責任者の許諾を得て行うこととする。また、訂正した内容等については、その記録を残し、法令等により定められる期間保管する。
その他の措置の内容	特に無し。
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	・機構が作成・配付する専用のアプリケーション（※）を用いることにより、入手の際の特定個人情報の漏えい・紛失の防止に努める。 ・操作者の認証を行う。 ※市町村CSのサーバ上で稼動するアプリケーション。市町村CSで管理されるデータの安全保護対策、不正アクセスの防止策には、最新の認証技術や暗号化技術を採用し、データの盗聴、改ざん、破壊及び盗難、端末の不正利用及びなりすまし等を防止する。また、市町村CSのサーバ自体には、外部からのこじあけ等に対して防御性に優れた耐タンパー装置（通信時の相互認証及びデータの暗号化に必要な情報を保管管理する）を内蔵している。
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
・端末のディスプレイを、来庁者から見えない位置に置く。 ・本人確認情報が表示された画面のハードコピーの取得は事務処理に必要となる範囲にとどめ、不要になったときは、シュレッダー等の復元不可能な方法により直ちに廃棄する。 ・スクリーンセーバーを利用し、離席したときも情報を覗けないようにする。

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	市町村CSと統合宛名システム間の接続は行わない。	
事務で使用するその他のシステムにおける措置の内容	庁内システムにおける市町村CSへのアクセスは既存住基システムに限定しており、また、既存住基システムと市町村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。 なお、市町村CSのサーバ上には住民基本台帳ネットワークシステム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）を講じる。	
その他の措置の内容	特に無し。	
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	・生体認証による操作者認証を行う。 ・システムを利用する必要がある職員を特定し、ユーザIDによる識別とパスワードによる認証を実施する。 ・なりすましによる不正を防止する観点から、共用IDの利用を禁止する。 ・業務運用中にやむを得ず離席する場合はシステムよりログオフする。	
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	本人確認情報の管理について、以下の管理を行う。 （1）ID/パスワードの発効管理 ・アクセス権限が必要となった場合、事務を担当する課長代理が事務ごとに更新権限の必要があるか、照会権限のみでよいかの別を確認し、事務に必要なアクセス権限のみを申請する。 ・申請に基づき、システム担当課長代理の確認の上、課長が承認する。また、当該事由が生じた際にはシステム担当がアクセス権限を更新し、別の職員が入力内容を照合・確認した上で当該IDを発効させる。 （2）失効管理 ・定期的又は異動／退職等のイベントが発生したタイミングで、権限を有していた職員の異動／退職情報をシステム担当課長代理が確認し、当該事由が生じた際には権限の失効を課長が承認する。その後、システム担当がアクセス権限を更新し、別の職員が入力内容を照合・確認した上で当該IDを失効させる。	
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	・システム担当課長代理はユーザIDやアクセス権限を、システムから出力された一覧をもとに定期的（定期異動ごと）に確認し、業務上アクセスが不要となったIDやアクセス権限を変更又は削除する。 ・委託先・再委託先のアクセス権限を持つものにたいしても、同様の扱いを行っている。 ・不正アクセスを分析するために、市町村CS及び統合端末においてアプリケーションの操作履歴の記録を取得し、保管している。	
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	・システムを操作したログ（日時・利用者・操作内容等）を取得し、磁気ディスクに記録し、必要に応じて操作履歴を解析する。 ・操作履歴の確認により本人確認情報の検索に関して不正な操作の疑いがある場合は、申請文書等との整合性を確認する。 ・バックアップされた操作履歴について、定められた期間、安全な場所に施錠保管する。	
その他の措置の内容	特に無し。	
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	・システム全般の利用に係る証跡（ログ）を取得する。 ・職員を対象に個人情報保護及び情報セキュリティに関する研修や注意喚起を行い、業務外利用の禁止等について徹底する。新たに配属になった職員には個人情報保護及び情報セキュリティに関する研修を別途行う。 ・委託先に対しては業務外で使用しないよう仕様書に定め、個人情報保護にかかる誓約書を提出させる。再委託先も同様に扱う。
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
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	・権限を与えられていない者は情報の複製ができない仕組みとしており、端末のUSB端子からはシステム的に複製できない仕組みとなっている。また、CD・DVDへの複製もできない仕組みとなっている。 ・委託先に対しては仕様書にて許可を得ない複製を禁止し、個人情報保護にかかる誓約書を提出させる。再委託先も同様に扱う。 ・職員に対しては、個人情報保護及び情報セキュリティに関する研修や注意喚起を行う。 ・サーバが設置されている管理区域に委託業者によるスマートフォンなどの持ち込みは禁止し、また、外部記憶媒体についても許可制としている。
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	
・端末のディスプレイを、来庁者から見えない位置に置く。 ・本人確認情報が表示された画面のハードコピーの取得は事務処理に必要となる範囲にとどめ、不要になったときは、シュレッダー等の復元不可能な方法により直ちに廃棄する。 ・スクリーンセーバーを利用し、離席したときも情報を覗けないようにする。	

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		・システムの構築や運用を委託するときは、プライバシーマークの認証か情報セキュリティマネジメントシステムの認証の取得を要件としている。 ・委託にかかる実施体制の提出を義務付けている。
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	・委託事業者と、特定個人情報保護に関する覚書を交わす。 ・個人情報保護にかかる誓約書を提出させる。再委託先も同様に扱う。 ・事前に申請許可された者以外はアクセスできないよう制御し、業務上必要最低限に限定したシステム操作の権限を与えている。
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	・システムを操作したログ（日時・利用者・操作内容等）を取得し、磁気ディスクに記録し、必要に応じて操作履歴を解析する。 ・バックアップされたログは定められた期間、保管する。
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	【ルールの内容】 ・再委託の契約の内容を書面により提出させ、当該再委託の契約の内容が、委託契約により委託先に課された全ての義務を再委託先に課すものである場合に限り、再委託の許諾を行う。また、個人情報保護に係る誓約書を提出するように求める。 【ルール遵守の確認方法】 業務実施内容について、定例会で定期的に報告を求めている。
	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	【ルールの内容】 委託先との間で、以下の事項を委託先に義務付ける「個人情報保護に関する特記仕様書」を提示して契約する。 ・番号法等の関係法令の遵守・秘密の保持・取扱区域外への情報持ち出しの禁止・目的外利用の禁止・複製の禁止・情報の返却、消去、廃棄・従業員の特定・従業員への監督及び教育・市の検査、報告の求めへの応諾・漏えい等事案に係る損害の賠償・再委託の条件・再委託先に対する監督とその履行状況の報告・その他枚方市保有個人情報安全管理規程に基づき職員が実施する措置に準じた措置の実施・特記仕様書に違反する行為の契約解除事由への該当 【ルール遵守の確認方法】 業務実施内容について、定例会で定期的に報告を求めている。
特定個人情報の消去ルール		[　　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	【ルールの内容】 特定個人情報保護に関する覚書の、提供資料の返還又は廃棄の項において、廃棄方法や、事前に書面で承認を得ること、廃棄完了後の報告、本市の立会いに応じることを定めている。 【ルール遵守の確認方法】 委託契約の報告条項に基づき、定期的に特定個人情報の取扱いについて書面にて、破棄、消去の方法、完了日等報告させ、必要があれば当市職員が現地調査することも可能とする。
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	委託先との間で、以下の事項を委託先に義務付ける「個人情報保護に関する特記仕様書」を提示して契約する。 ・番号法等の関係法令の遵守・秘密の保持・取扱区域外への情報持ち出しの禁止・目的外利用の禁止・複製の禁止・情報の返却、消去、廃棄・従業員の特定・従業員への監督及び教育・市の検査、報告の求めへの応諾・漏えい等事案に係る損害の賠償・再委託の条件・再委託先に対する監督とその履行状況の報告・その他枚方市保有個人情報安全管理規程に基づき職員が実施する措置に準じた措置の実施・特記仕様書に違反する行為の契約解除事由への該当
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		[再委託していない] ＜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	
その他の措置の内容		特に無し。
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

・サーバ室で受託業者が作業する場合は、市民室職員が立ち会う。
・委託先従業員が職員の許可を得ずに外部記憶媒体をサーバー室に持ち込む事を禁止するとともに、スマートフォン等については一切の持込を禁止する。

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	特定個人情報（個人番号、4情報等）の提供・移転を行う際に、提供・移転の記録（提供・移転日時、操作者等）をシステム上で管理し、5年分保存する。 なお、システム上、提供・移転に係る処理を行ったものの提供・移転が認められなかった場合についても記録を残す。
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	・情報の移転・提供については、番号法、住基法等の法令で定められた事項について行う。 ・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	・「サーバ室等への入室権限」及び「本特定個人情報ファイルを扱うシステムへのアクセス権限」を有する者を厳格に管理し、情報の持ち出しを制限する。 ・違反行為を行った場合は、法令の罰則規定により措置を講じる。 ・個人番号の盗用等が発生した場合は、番号法第7条第2項により、職権及び該当者からの申請により、個人番号の変更を行う。
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
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	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	・誤った情報を提供・移転してしまうリスクへの措置 ：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。 ・誤った相手に提供・移転してしまうリスクへの措置 ：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するため、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	
・特定個人情報をフラッシュメモリ等の外部記憶媒体を用いて移転する場合は、データの暗号化の措置を施したうえで移転を行う。 ・サーバが設置されている管理区域に委託業者によるスマートフォンなどの持ち込みは禁止しており、また、外部記憶媒体についても許可制としている。	

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	・サーバーの盗難を防ぐために、施錠ができる場所等に保管し、施錠をしている。また、設置場所への入退出はICカードにより記録している。 ・停電(落雷等)によるデータの消失を防ぐために、サーバーに無停電電源装置等を付設している。 ・火災によるデータ消失を防ぐために、施設内に消火設備を完備している。	
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	・ネットワークを通じて悪意の第三者が侵入しないよう、ファイアウォール・不正侵入防止装置（IPS）を設置しており、それらの機器は24時間の監視を行い、定期的にログの解析を行っている。 ・インターネットとつながらないようにネットワークをファイアウォールで切断している。 ・コンピュータウィルス対策ソフトウェアを導入しており、パターンファイルも最新版が適用されるよう管理している。 ・OSには必要に応じてパッチ適用を実施している。	
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	該当無し。	
再発防止策の内容	該当無し。	
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	生存する個人の個人番号とともに、死亡による消除後、住民基本台帳法施行令第34条第2項に定める期間保管する。	
その他の措置の内容	特に無し。	
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	既存住基システムとの整合処理を定期的に実施し、保存する本人確認情報が最新であるかどうかを確認することにより担保する。	
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	・システム上、住民基本台帳法施行令第34条第2項に定める期間を経過した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を消去する仕組みとする。 ・磁気ディスクの廃棄時は、手順書等に基づき、内容の復元及び判読が不可能になるような方法により消去する。 ・住民異動届等の紙媒体については、帳簿等を作成し、保管及び廃棄の運用が適切になされていることを適時確認するとともに、その記録を残す。また、廃棄時には、規程に基づき、溶解処理による廃棄を行うとともに、廃棄文書目録を残す。	
その他の措置の内容	特に無し。	
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		
・サーバが設置されている管理区域に委託業者によるスマートフォンなどの持ち込みは禁止しており、また、外部記憶媒体についても許可制としている。		

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 ※（7. リスク1⑨を除く。）

1. 特定個人情報ファイル名	
（3）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	送付先情報の入手元は既存住基システムに限定されるため、既存住基システムへの情報の登録の際に次のことを行う。 ・申請等の窓口において届出／申請内容や本人確認書類（身分証明書等）の確認を厳格に行い、対象者以外の情報の入手の防止に努める。 ・申請者が本人及び同一の世帯以外の情報を誤って記載しないように予め記入様式が定められた書面に必要事項のみを記入する方式とする。 ・システムへの入力後、別の職員が異動届とシステムの入力内容を照合し、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	・平成14年6月10日総務省告示第334号（第6－6　本人確認情報の通知及び記録）等により市町村CSにおいて既存住基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。 ・申請者が必要な情報だけを記載できるように書面式とする。
その他の措置の内容	特に無し。
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	送付先情報の入手元を既存住基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：　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	窓口において、対面で個人番号カードなどの本人確認資料で、本人の確認を行う。
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付く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	既存住基システムにおいて正確性が確保された送付先情報を適切に受信できることをシステムにより担保する。 なお、送付先情報ファイルは、既存住基システムから入手後、個人番号カード管理システムに送付先情報を送付した時点で役割を終える（不要となる）ため、送付後速やかに市町村CSから削除する。 そのため、入手から削除までのサイクルがごく短期間であることから、入手から削除の間の正確性を維持するための特段の対策は講じない。
その他の措置の内容	特に無し。
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	・機構が作成・配付する専用のアプリケーション（※）を用いることにより、入手の際の特定個人情報の漏えい・紛失の防止に努める。 ・操作者の認証を行う。 ※市町村CSのサーバ上で稼動するアプリケーション。市町村システムで管理されるデータの安全保護対策、不正アクセスの防止策には、最新の認証技術や暗号化技術を採用し、データの盗聴、改ざん、破壊及び盗難、端末の不正利用及びなりすまし等を防止する。また、市町村CSのサーバ自体には、外部からのこじあけ等に対して防御性に優れた耐タンパー装置（通信時の相互認証及びデータの暗号化に必要な情報を保管管理する）を内蔵している。

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
・端末のディスプレイを、来庁者から見えない位置に置く。 ・本人確認情報が表示された画面のハードコピーの取得は事務処理に必要となる範囲にとどめ、不要になったときは、シュレッダー等の復元不可能な方法により直ちに廃棄する。 ・スクリーンセーバーを利用し、離席したときも情報を覗けないようにする。

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	市町村CSと統合宛名システム間の接続は行わない。	
事務で使用するその他のシステムにおける措置の内容	庁内システムにおける市町村CSへのアクセスは既存住基システムに限定しており、また、既存住基システムと市町村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。 なお、市町村CSのサーバ上には住民基本台帳ネットワークシステム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）を講じる。	
その他の措置の内容	特に無し。	
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	・生体認証による操作者認証を行う。 ・システムを利用する必要がある職員を特定し、ユーザIDによる識別とパスワードによる認証を実施する。 ・なりすましによる不正を防止する観点から、共用IDの利用を禁止する。 ・業務運用中にやむを得ず離席する場合はシステムよりログオフする。	
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	本人確認情報の管理について、以下の管理を行う。 （1）ID/パスワードの発効管理 ・アクセス権限が必要となった場合、事務を担当する課長代理が事務ごとに更新権限の必要があるか、照会権限のみでよいかの別を確認し、事務に必要なアクセス権限のみを申請する。 ・申請に基づき、システム担当課長代理の確認の上、課長が承認する。また、当該事由が生じた際にはシステム担当がアクセス権限を更新し、別の職員が入力内容を照合・確認した上で当該IDを発効させる。 （2）失効管理 ・定期的又は異動／退職等のイベントが発生したタイミングで、権限を有していた職員の異動／退職情報をシステム担当課長代理が確認し、当該事由が生じた際には権限の失効を課長が承認する。その後、システム担当がアクセス権限を更新し、別の職員が入力内容を照合・確認した上で当該IDを失効させる。	
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	・システム担当課長代理はユーザIDやアクセス権限を、システムから出力された一覧をもとに定期的（定期異動ごと）に確認し、業務上アクセスが不要となったIDやアクセス権限を変更又は削除する。 ・委託先・再委託先のアクセス権限を持つものにたいしても、同様の扱いを行っている。 ・不正アクセスを分析するために、市町村CS及び統合端末においてアプリケーションの操作履歴の記録を取得し、保管している。	
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	・システムを操作したログ（日時・利用者・操作内容等）を取得し、磁気ディスクに記録し、必要に応じて操作履歴を解析する。 ・操作履歴の確認により本人確認情報の検索に関して不正な操作の疑いがある場合は、申請文書等との整合性を確認する。 ・バックアップされた操作履歴について、定められた期間、安全な場所に施錠保管する。	
その他の措置の内容	特に無し。	
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	・システム全般の利用に係る証跡（ログ）を取得する。 ・職員を対象に個人情報保護及び情報セキュリティに関する研修や注意喚起を行い、業務外利用の禁止等について徹底する。新たに配属になった職員には個人情報保護及び情報セキュリティに関する研修を別途行う。 ・委託先に対しては業務外で使用しないよう仕様書に定め、個人情報保護にかかる誓約書を提出させる。再委託先も同様に扱う。
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
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	・権限を与えられていない者は情報の複製ができない仕組みとしており、端末のUSB端子からはシステム的に複製できない仕組みとなっている。また、CD・DVDへの複製もできない仕組みとなっている。 ・委託先に対しては仕様書にて許可を得ない複製を禁止し、個人情報保護にかかる誓約書を提出させる。再委託先も同様に扱う。 ・職員に対しては、個人情報保護及び情報セキュリティに関する研修や注意喚起を行っている。 ・サーバが設置されている管理区域に委託業者によるスマートフォンなどの持ち込みは禁止しており、また、外部記憶媒体についても許可制としている。
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	
・端末のディスプレイを、来庁者から見えない位置に置く。 ・本人確認情報が表示された画面のハードコピーの取得は事務処理に必要となる範囲にとどめ、不要になったときは、シュレッダー等の復元不可能な方法により直ちに廃棄する。 ・スクリーンセーバーを利用し、離席したときも情報を覗けないようにする。	

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		・システムの構築や運用を委託するときは、プライバシーマークの認証か情報セキュリティマネジメントシステムの認証の取得を要件としている。 ・委託にかかる実施体制の提出を義務付けている。
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	・委託事業者と、個人情報の保護に関する特記仕様書を提示して契約する。 ・個人情報保護にかかる誓約書を提出させる。再委託先も同様に扱う。 ・事前に申請許可された者以外はアクセスできないよう制御し、業務上必要最低限に限定したシステム操作の権限を与えている。 ・作業者を限定するために、委託作業者の名簿を提出させる。
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	・システムを操作したログ（日時・利用者・操作内容等）を取得し、磁気ディスクに記録し、必要に応じて操作履歴を解析する。 ・バックアップされたログは定められた期間、保管する。
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	【ルールの内容】 ・再委託の契約の内容を書面により提出させ、当該再委託の契約の内容が、委託契約により委託先に課された全ての義務を再委託先に課すものである場合に限り、再委託の許諾を行う。また、個人情報保護に係る誓約書を提出するように求める。 【ルール遵守の確認方法】 業務実施内容について、定例会で定期的に報告を求めている。
	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	【ルールの内容】 委託先との間で、以下の事項を委託先に義務付ける「個人情報保護に関する特記仕様書」を提示して契約する。 ・番号法等の関係法令の遵守・秘密の保持・取扱区域外への情報持ち出しの禁止・目的外利用の禁止・複製の禁止・情報の返却、消去、廃棄・従業員の特定・従業員への監督及び教育・市の検査、報告の求めへの応諾・漏えい等事案に係る損害の賠償・再委託の条件・再委託先に対する監督とその履行状況の報告・その他枚方市保有個人情報安全管理規程に基づき職員が実施する措置に準じた措置の実施・特記仕様書に違反する行為の契約解除事由への該当 【ルール遵守の確認方法】 業務実施内容について、定例会で定期的に報告を求めている。
特定個人情報の消去ルール		[　　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	【ルールの内容】 個人情報保護に関する特記仕様書の、提供資料の返還又は廃棄の項において、廃棄方法や、事前に書面で承認を得ること、廃棄完了後の報告、本市の立会いに応じることを定めている。 【ルール遵守の確認方法】 委託契約の報告条項に基づき、定期的に特定個人情報の取扱いについて書面にて、破棄、消去の方法、完了日等報告させ、必要があれば当市職員が現地調査することも可能とする。
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	委託先との間で、以下の事項を委託先に義務付ける「個人情報保護に関する特記仕様書」を提示して契約する。 ・番号法等の関係法令の遵守・秘密の保持・取扱区域外への情報持ち出しの禁止・目的外利用の禁止・複製の禁止・情報の返却、消去、廃棄・従業員の特定・従業員への監督及び教育・市の検査、報告の求めへの応諾・漏えい等事案に係る損害の賠償・再委託の条件・再委託先に対する監督とその履行状況の報告・その他枚方市保有個人情報安全管理規程に基づき職員が実施する措置に準じた措置の実施・特記仕様書に違反する行為の契約解除事由への該当
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		[　再委託していない　] ＜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	
その他の措置の内容		特に無し。
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		
・サーバ室で受託業者が作業する場合は、市民室職員が立ち会う。 ・委託先従業員が職員の許可を得ずに外部記憶媒体をサーバー室に持ち込む事を禁止するとともに、スマートフォン等については一切の持込を禁止する。		

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	特定個人情報（個人番号、4情報等）の提供を行う際に、提供記録（提供日時、操作者等）をシステム上で管理し、5年分保存する。 なお、システム上、提供に係る処理を行ったものの提供が認められなかった場合についても記録を残す。
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	・情報の移転・提供については、番号法、住基法等の法令で定められた事項について行う。 ・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	「サーバ室等への入室権限」及び「本特定個人情報ファイルを扱うシステムへのアクセス権限」を有する者を厳格に管理し、情報の持ち出しを制限する。 ・違反行為を行った場合は、法令の罰則規定により措置を講じる。 ・個人番号の盗用等が発生した場合は、番号法第7条第2項により、職権及び該当者からの申請により、個人番号の変更を行う。
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
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	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移転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	・誤った情報を提供・移転してしまうリスクへの措置 ：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。 ・誤った相手に提供・移転してしまうリスクへの措置 ：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するため、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	
・特定個人情報をフラッシュメモリ等の外部記憶媒体を用いて移転する場合は、データの暗号化の措置を施したうえで移転を行う。 ・サーバが設置されている管理区域に委託業者によるスマートフォンなどの持ち込みは禁止しており、また、外部記憶媒体についても許可制としている。	

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	・サーバーの盗難を防ぐために、施錠ができる場所等に保管し、施錠をしている。また、設置場所への入退出はICカードにより記録している。 ・停電(落雷等)によるデータの消失を防ぐために、サーバーに無停電電源装置等を付設している。 ・火災によるデータ消失を防ぐために、施設内に消火設備を完備している。	
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	・ネットワークを通じて悪意の第三者が侵入しないよう、ファイアウォール・不正侵入防止装置（IPS）を設置しており、それらの機器は24時間の監視を行い、定期的にログの解析を行っている。 ・インターネットとつながらないようにネットワークをファイアウォールで切断している。 ・コンピュータウィルス対策ソフトウェアを導入しており、パターンファイルも最新版が適用されるよう管理している。 ・OSには必要に応じてパッチ適用を実施している。	
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	該当無し。	
再発防止策の内容	該当無し。	
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	保管していない。	
その他の措置の内容	特に無し。	
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	本特定個人情報ファイル（送付先情報ファイル）は、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（1営業日後）に削除する仕組みとする。 また、媒体を用いて連携する場合、当該媒体は連携後、連携先である機構において適切に管理され、市町村では保管しない。 そのため、送付先情報ファイルにおいて特定個人情報が古い情報のまま保管され続けるリスクは存在しない。	
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	システム上、保管期間の経過した特定個人情報を一括して削除する仕組みとする。	
その他の措置の内容	特に無し。	
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		
・サーバが設置されている管理区域に委託業者によるスマートフォンなどの持ち込みは禁止しており、また、外部記憶媒体についても許可制としている。 ・送付先情報ファイルは、機構への特定個人情報の提供後、速やかに市町村CSから削除される。その後、当該特定個人情報は機構において管理されるため、送付先情報ファイルのバックアップは取得しない予定である。		

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	＜枚方市の措置＞ 年に1回担当部署内において、評価書の記載内容通りの運用がなされていることについて、自己点検を行い、運用状況を確認する。 ＜中間サーバー･プラットフォームにおける措置＞ 運用規則等に基づき，中間サーバー･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実施することとしている。	
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	＜枚方市における措置＞ 枚方市情報セキュリティポリシーに基づき、枚方市の情報セキュリティ委員会が策定した年度監査計画に従い、内部監査員が情報セキュリティ内部監査を行っている。 なお、内部監査員は過去に業務システムの運用を担当したことのある者等、比較的IT知識の高い職員の中から毎年選定し、監査の経験者と未経験者を組み合わせる等により知識の継承を図っている。 また、マイナンバー監査実施要項に基づき、マイナンバー監査を実施している。 ＜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。 ＜中間サーバー･プラットフォームにおける措置＞ 運用規則等に基づき、中間サーバー・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。	

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	＜枚方市における措置＞ ・職員に対しては、情報セキュリティと個人情報保護に関する研修を行う。 ・委託業者に対しては、個人情報保護に関する特記仕様書を提示して契約し、個人情報保護に関する教育を適宜実施することを義務付ける。 ＜中間サーバー･プラットフォームにおける措置＞ ①中間サーバー･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、セキュリティ研修等を実施することとしている。 ②中間サーバー･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。	

3. その他のリスク対策

＜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、国及びクラウド事業者が対応する。また、ガバメントクラウドに起因しない事象の場合は、市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。

＜中間サーバー･プラットフォームにおける措置＞
中間サーバー・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者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。

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	郵便番号573-8666 大阪府枚方市大垣内町二丁目1番20号 枚方市役所　総務部　コンプライアンス推進課
②請求方法	個人情報の保護に関する法律に基づき、保有個人情報の開示等請求を受け付ける。
特記事項	枚方市のホームページ上に請求先、請求方法等について掲載している。
③手数料等	[　　有料　　]　　＜選択肢＞ 1) 有料　　2) 無料 （手数料額、納付方法：手数料額：保有個人情報の閲覧に係る手数料は無料だが、その写しの作成や郵送を希望する場合は、請求者の負担となる。）
④個人情報ファイル簿の公表	[　行っていない　]　　＜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	取扱い無し。
公表場所	無し。
⑤法令による特別の手続	無し。
⑥個人情報ファイル簿への不記載等	無し。

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	郵便番号573-8666 大阪府枚方市大垣内町二丁目1番20号 枚方市役所　市民生活部　市民課
②対応方法	問い合わせの受付時に受付票を起票し、対応について記録を残す。

Ⅵ　評価実施手続

1. 基礎項目評価	
①実施日	令和6年4月10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	パブリックコメント方式による意見募集を実施。実施に際しては、市広報紙「広報ひらかた」に意見を募集している旨の記事を掲載し、枚方市のホームページ及び市役所本館、別館1階受付・市民課・各支所・各生涯学習市民センター・枚方公園青少年センター・中央図書館において素案の閲覧または配付を行った。
②実施日・期間	令和4年9月1日（木）から令和4年9月30日（金）・30日間
③期間を短縮する特段の理由	無し。
④主な意見の内容	リスク対策について、委託先等からの情報漏洩の不安や情報保護対策に関する取り組み姿勢の強化についての意見。
⑤評価書への反映	無し。
3. 第三者点検	
①実施日	令和4年10月24日（月）
②方法	枚方市情報公開・個人情報審議会により第三者点検を受けた。
③結果	特定個人情報保護評価指針に定める実施手続等に適合した特定個人情報保護評価が実施されるとともに、その内容は、同指針に定める特定個人情報保護評価の目的等に照らして妥当であると認められた。
4. 個人情報保護委員会の承認 【行政機関等のみ】	
①提出日	
②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
令和6年4月10日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1、委託事項2 ④委託先への特定個人情報ファイルの提供方法	[○]その他（庁内にある既存住基システムのサーバー及び端末を直接使用する。）	[○]その他（庁内にある既存住基システムのサーバー及び端末を直接使用する。また、ガバメントクラウド環境に設置される住基システム等のサーバに対し、事業者拠点よりネットワーク経由でアクセスし、運用・保守作業を行う（以下ではこの方法を、「リモート保守」という）。）	事前	特定個人情報保護評価指針で定められている重要な変更に該当する。
令和6年4月10日	Ⅱ　特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1 ⑥委託先名	株式会社ジャパンクリエイト	株式会社エイジェック	事後	特定個人情報保護評価指針で定められている重要な変更に該当しない。
令和6年4月10日	Ⅱ 特定個人情報ファイルの概要 6. 特定個人情報の保管・消去 ①保管場所	＜枚方市における措置＞ 入退出管理カードにより入退出管理を行っている施錠された管理区域内に設置したサーバで管理する。 サーバへのアクセスはID／パスワードによる認証が必要となる。 書類は所定の施錠可能な保管庫で保管する。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームはデータセンターに設置しており、データセンターへの入館及びサーバー室への入室を厳重に管理する。 ②特定個人情報は、サーバー室に設置された中間サーバー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に保存される。	＜枚方市における措置＞ 入退出管理カードにより入退出管理を行っている施錠された管理区域内に設置したサーバで管理する。 サーバへのアクセスはID／パスワードによる認証が必要となる。 書類は所定の施錠可能な保管庫で保管する。 ＜ガバメントクラウドにおける措置＞ ①システムのサーバ等は、政府情報システムのセキュリティ制度であるISMAPの認証を取得したクラウド事業者が運営するデータセンターに設置し、セキュリティ管理策が適切に実施される。 ②特定個人情報は、クラウド事業者が管理する日本国内のデータセンター内に保存され、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。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームはデータセンターに設置しており、データセンターへの入館及びサーバー室への入室を厳重に管理する。 ②特定個人情報は、サーバー室に設置された中間サーバー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に保存される。	事前	特定個人情報保護評価指針で定められている重要な変更に該当する。
令和6年4月10日	Ⅱ 特定個人情報ファイルの概要 6. 特定個人情報の保管・消去 ③消去方法	＜枚方市における措置＞ ・既存住基システムに記録されたデータのうち、平成26年6月19日以前に住民票が除票になって5年を経過したものについて、システムで判別し、出力・閲覧できないようにする。ただし、行政事務の基礎データとして直ちに不要になるものではないので、直ちには消去せず、毎年要不要の判断を行った上で、不要であれば消去する。 ・申請書等の書類は、保存年限の経過後、溶解して廃棄する。 ＜中間サーバー・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地方公共団体からの操作によって実施されるため、通常、中間サーバー・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、中間サーバー・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、物理的破壊又は専用ソフト等を利用して完全に消去する。	＜枚方市における措置＞ ・既存住基システムに記録されたデータのうち、平成26年6月19日以前に住民票が除票になって5年を経過したものについて、システムで判別し、出力・閲覧できないようにする。ただし、行政事務の基礎データとして直ちに不要になるものではないので、直ちには消去せず、毎年要不要の判断を行った上で、不要であれば消去する。 ・申請書等の書類は、保存年限の経過後、溶解して廃棄する。 ＜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市（委託先を含む）の操作によって実施し、国及びクラウド事業者は、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。 ＜中間サーバー・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地方公共団体からの操作によって実施されるため、通常、中間サーバー・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、中間サーバー・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、物理的破壊又は専用ソフト等を利用して完全に消去する。	事前	特定個人情報保護評価指針で定められている重要な変更に該当する。

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
令和6年4月10日	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 4. 特定個人情報ファイルの取扱いの委託 情報保護管理体制の確認	・システムの構築や運用を委託するときは、プライバシーマークの認証か情報セキュリティマネジメントシステムの認証の取得を要件としている。また、社内教育に関する条件として、セキュリティに関する研修及びプライバシー保護に関する研修等を実施する旨を規定し、特定個人情報の保護を適切に行える委託先であることを確認する。 ・委託にかかる実施体制の提出を義務付けている。	・システムの構築や運用を委託するときは、プライバシーマークの認証か情報セキュリティマネジメントシステムの認証の取得を要件としている。また、社内教育に関する条件として、セキュリティに関する研修及びプライバシー保護に関する研修等を実施する旨を規定し、特定個人情報の保護を適切に行える委託先であることを確認する。 ・委託にかかる実施体制の提出を義務付けている。 ・リモート保守を行う事業者の事業所については、情報セキュリティマネジメントシステム等の情報セキュリティの第三者認証を取得していることを条件とし、セキュリティ対策の実効性を確保する。第三者認証を取得していない場合等で必要と判断する場合、職員が実地確認を行い、セキュリティ対策の実効性を確保する。	事前	特定個人情報保護評価指針で定められている重要な変更に該当する。
令和6年4月10日	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 4. 特定個人情報ファイルの取扱いの委託 特定個人情報ファイルの閲覧者・更新者の制限 具体的な制限方法	・委託事業者と、特定個人情報保護に関する覚書を交わす。 ・個人情報保護にかかる誓約書を提出させる。再委託先も同様に扱う。 ・事前に申請許可された者以外はアクセスできないよう制御し、業務上必要最低限に限定したシステム操作の権限を与えている。 ・作業者を限定するために、委託作業者の名簿を提出させる。	・委託事業者には、特定個人情報保護に関する特記仕様書の内容を順守してもらう。 ・必要に応じて、個人情報保護にかかる誓約書を提出を求める。再委託先も同様に扱う。 ・事前に申請許可された者以外はアクセスできないよう制御し、業務上必要最低限に限定したシステム操作の権限を与えている。 ・作業者を限定するために、委託作業者の名簿を提出させる。	事後	特定個人情報保護評価指針で定められている重要な変更に該当しない。
令和6年4月10日	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 4. 特定個人情報ファイルの取扱いの委託 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順守の確認方法 【ルールの内容】	委託先との間で、以下の事項を委託先に義務付ける「特定個人情報保護に関する覚書」を交換する。 ・番号法等の関係法令の遵守・秘密の保持・取扱区域外への情報持ち出しの禁止・目的外利用の禁止・複製の禁止・情報の返却、消去、廃棄・従業員の特定・従業員への監督及び教育・市の検査、報告の求めへの応諾・漏えい等事案に係る損害の賠償・再委託の条件・再委託先に対する監督とその履行状況の報告・その他枚方市特定個人情報の安全管理に関する規定に基づき職員が実施する措置に準じた措置の実施・覚書に違反する行為の契約解除事由への該当	委託先との間で、以下の事項を委託先に義務付ける「個人情報保護に関する特記仕様書」を提示して契約する。 ・番号法等の関係法令の遵守・秘密の保持・取扱区域外への情報持ち出しの禁止・目的外利用の禁止・複製の禁止・情報の返却、消去、廃棄・従業員の特定・従業員への監督及び教育・市の検査、報告の求めへの応諾・漏えい等事案に係る損害の賠償・再委託の条件・再委託先に対する監督とその履行状況の報告・その他枚方市保有個人情報安全管理規程に基づき職員が実施する措置に準じた措置の実施・特記仕様書に違反する行為の契約解除事由への該当	事後	特定個人情報保護評価指針で定められている重要な変更に該当しない。
令和6年4月10日	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 4. 特定個人情報ファイルの取扱いの委託 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 規定の内容	委託先との間で、以下の事項を委託先に義務付ける「特定個人情報保護に関する覚書」を交換する。 ・番号法等の関係法令の遵守・秘密の保持・取扱区域外への情報持ち出しの禁止・目的外利用の禁止・複製の禁止・情報の返却、消去、廃棄・従業員の特定・従業員への監督及び教育・市の検査、報告の求めへの応諾・漏えい等事案に係る損害の賠償・再委託の条件・再委託先に対する監督とその履行状況の報告・その他枚方市特定個人情報の安全管理に関する規定に基づき職員が実施する措置に準じた措置の実施・覚書に違反する行為の契約解除事由への該当	委託先との間で、以下の事項を委託先に義務付ける「個人情報保護に関する特記仕様書」を提示して契約する。 ・番号法等の関係法令の遵守・秘密の保持・取扱区域外への情報持ち出しの禁止・目的外利用の禁止・複製の禁止・情報の返却、消去、廃棄・従業員の特定・従業員への監督及び教育・市の検査、報告の求めへの応諾・漏えい等事案に係る損害の賠償・再委託の条件・再委託先に対する監督とその履行状況の報告・その他枚方市保有個人情報安全管理規程に基づき職員が実施する措置に準じた措置の実施・特記仕様書に違反する行為の契約解除事由への該当	事後	特定個人情報保護評価指針で定められている重要な変更に該当しない。
令和6年4月10日	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 4. 特定個人情報ファイルの取扱いの委託 特定個人情報ファイルの取り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	・サーバ室で受託業者が作業する場合は、市民室職員が立ち会う。 ・委託先従業員が職員の許可を得ずに外部記憶媒体をサーバー室に持ち込む事を禁止するとともに、スマートフォン等については一切の持込を禁止する。	・サーバ室で受託業者が作業する場合は、市民課職員が立ち会う。 ・委託先従業員が職員の許可を得ずに外部記憶媒体をサーバー室に持ち込む事を禁止するとともに、スマートフォン等については一切の持込を禁止する。 ・リモート保守を行う事業者の事業所については、情報セキュリティマネジメントシステム等の情報セキュリティの第三者認証を取得していることを条件とし、セキュリティ対策の実効性を確保する。第三者認証を取得していない場合等で必要と判断する場合、職員が実地確認を行い、セキュリティ対策の実効性を確保する。 <リモート保守環境におけるその他のリスクと措置> ・リモート保守を行う事業所の執務エリアは入退室管理された区画とし、作業者の入退室記録を取得する。また保守作業に利用する端末の利用記録の取得や、監視カメラでの監視体制を敷き、作業者へも周知することで、不適切な方法での情報入手を抑止する。 ・リモート保守環境とガバメントクラウドへの接続については、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し、通信経路上での第三者からの情報窃取を行えないよう対策する。	事前	特定個人情報保護評価指針で定められている重要な変更に該当する。

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
令和6年4月10日			・リモート保守で利用する端末等については、コンピュータウィルス対策ソフトウェアを導入しており、パターンファイルも最新版が適用されるよう管理する。また、OSには必要に応じてパッチ適用を実施する。 ・システムのリモート保守で委託事業者が利用する端末等へは、原則として、特定個人情報の保存を行えないように措置する。端末等への特定個人情報の保存を必要とする場合、使用後は速やかに消去するとともに、端末等のディスク廃棄時には物理的破壊または専用ソフトでのデータ消去を行わせ、データ消去証明書の提出により確認する。		
令和6年4月10日	Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 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 ⑤物理的対策 具体的な対策の内容	＜枚方市における措置＞ ・サーバーの盗難を防ぐために、施錠ができる場所等に保管し、施錠をしている。また、設置場所への入退出はICカードにより記録している。 ・停電(落雷等)によるデータの消失を防ぐために、サーバーに無停電電源装置等を付設している。 ・火災によるデータ消失を防ぐために、施設内に消火設備を完備している。 ＜中間サーバー・プラットフォームにおける措置＞ ・中間サーバー・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。	＜枚方市における措置＞ ・サーバーの盗難を防ぐために、施錠ができる場所等に保管し、施錠をしている。また、設置場所への入退出はICカードにより記録している。 ・停電(落雷等)によるデータの消失を防ぐために、サーバーに無停電電源装置等を付設している。 ・火災によるデータ消失を防ぐために、施設内に消火設備を完備している。 ＜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。 ＜中間サーバー・プラットフォームにおける措置＞ ・中間サーバー・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。	事前	特定個人情報保護評価指針で定められている重要な変更に該当する。
令和6年4月10日	Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 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 ⑥技術的対策 具体的な対策の内容	＜枚方市における措置＞ ・ネットワークを通じて悪意の第三者が侵入しないよう、ファイアウォール・不正侵入防止装置（IPS）を設置しており、、それらの機器は24時間の監視を行い、定期的にログの解析を行っている。 ・インターネットとつながらないようにネットワークをファイアウォールで切断している。 ・コンピュータウィルス対策ソフトウェアを導入しており、パターンファイルも最新版が適用されるよう管理している。 ・OSには必要に応じてパッチ適用を実施している。 ＜中間サーバー・プラットフォームにおける措置＞ ・中間サーバー・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。 ・中間サーバー・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。	＜枚方市における措置＞ ・ネットワークを通じて悪意の第三者が侵入しないよう、ファイアウォール・不正侵入防止装置（IPS）を設置しており、、それらの機器は24時間の監視を行い、定期的にログの解析を行っている。 ・インターネットとつながらないようにネットワークをファイアウォールで切断している。 ・コンピュータウィルス対策ソフトウェアを導入しており、パターンファイルも最新版が適用されるよう管理している。 ・OSには必要に応じてパッチ適用を実施している。 ＜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、市の保有データにアクセスしない契約等となっている。 ②市が委託した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【第1.0版】」（令和4年10月　デジタル庁。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。	事前	特定個人情報保護評価指針で定められている重要な変更に該当する。

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
令和6年4月10日			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市が委託した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市や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市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。 ＜中間サーバー・プラットフォームにおける措置＞ ・中間サーバー・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。 ・中間サーバー・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。	事前	特定個人情報保護評価指針で定められている重要な変更に該当する。
令和6年4月10日	Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 7．特定個人情報の保管・消去 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 手順の内容	・住民基本台帳ファイルに記録されたデータのうち、平成26年6月19日以前に住民票が除票になって5年を経過したものについて、システムで判別し、出力・閲覧できないようにする。ただし、行政事務の基礎データとして直ちに不要になるものではないので、直ちには消去せず、毎年要不要の判断を行った上で、不要であれば消去する。 ・磁気ディスクの廃棄時は、手順書等に基づき、内容の復元及び判読が不可能になるような方法により消去する。 ・住民異動届等の紙媒体については、帳簿等を作成し、保管及び廃棄の運用が適切になされていることを適時確認するとともに、その記録を残す。また、廃棄時には、規程に基づき、溶解処理による廃棄を行うとともに、廃棄文書目録を残す。	＜枚方市における措置＞ ・住民基本台帳ファイルに記録されたデータのうち、平成26年6月19日以前に住民票が除票になって5年を経過したものについて、システムで判別し、出力・閲覧できないようにする。ただし、行政事務の基礎データとして直ちに不要になるものではないので、直ちには消去せず、毎年要不要の判断を行った上で、不要であれば消去する。 ・磁気ディスクの廃棄時は、手順書等に基づき、内容の復元及び判読が不可能になるような方法により消去する。 ・住民異動届等の紙媒体については、帳簿等を作成し、保管及び廃棄の運用が適切になされていることを適時確認するとともに、その記録を残す。また、廃棄時には、規程に基づき、溶解処理による廃棄を行うとともに、廃棄文書目録を残す。 ＜ガバメントクラウドにおける措置＞ 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	特定個人情報保護評価指針で定められている重要な変更に該当する。
令和6年4月10日	Ⅳ その他のリスク対策 1．監査 ②監査 具体的な内容	＜枚方市における措置＞ 枚方市情報セキュリティポリシーに基づき、枚方市の情報セキュリティ委員会が策定した年度監査計画に従い、内部監査員が情報セキュリティ内部監査を行っている。 なお、内部監査員は過去に業務システムの運用を担当したことのある者等、比較的IT知識の高い職員の中から毎年選定し、監査の経験者と未経験者を組み合わせる等により知識の継承を図っている。 また、マイナンバー監査実施要項に基づき、マイナンバー監査を実施している。 ＜中間サーバー・プラットフォームにおける措置＞ 運用規則等に基づき、中間サーバー・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。	＜枚方市における措置＞ 枚方市情報セキュリティポリシーに基づき、枚方市の情報セキュリティ委員会が策定した年度監査計画に従い、内部監査員が情報セキュリティ内部監査を行っている。 なお、内部監査員は過去に業務システムの運用を担当したことのある者等、比較的IT知識の高い職員の中から毎年選定し、監査の経験者と未経験者を組み合わせる等により知識の継承を図っている。 また、マイナンバー監査実施要項に基づき、マイナンバー監査を実施している。 ＜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。 ＜中間サーバー・プラットフォームにおける措置＞ 運用規則等に基づき、中間サーバー・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。	事前	特定個人情報保護評価指針で定められている重要な変更に該当する。

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
令和6年4月10日	Ⅳ　その他のリスク対策 3. その他のリスク対策	＜中間サーバー･プラットフォームにおける措置＞ 中間サーバー・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者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、国及びクラウド事業者が対応する。また、ガバメントクラウドに起因しない事象の場合は、市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。 ＜中間サーバー･プラットフォームにおける措置＞ 中間サーバー・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者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。	事前	特定個人情報保護評価指針で定められている重要な変更に該当する。
令和8年3月30日	Ⅰ基本情報6.情報提供ネットワークシステムによる情報連携②法令上の根拠	【照会】 なし 【提供】 ・番号法、特定個人番号利用事務　別表第2の1、2、3、4、6、8、9、11、16、18、20、23、27、30、31、34、35、37、38、39、40、42、48、53、54、57、58、59、61、62、66、67、70、74、77、80、84、85の2、89、91、92、94、96、97、101、102、103、105、106、107、108、111、112、113、114、116、117、120の項	【照会】 ・情報提供ネットワークによる情報照会は実施しない。 【提供】 ・番号法第19条第8号に基づく主務省令第2条の表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	事後	重要な変更には当たらない。
令和8年3月30日	Ⅰ基本情報7.評価実施機関における担当部署①部署	枚方市　市民生活部　市民室　市民課	枚方市　市民生活部　市民課	事後	重要な変更には当たらない。
令和8年3月30日	Ⅰ基本情報7.評価実施機関における担当部署②所属長の役職名	市民課長	課長	事後	重要な変更には当たらない。
令和8年3月30日	Ⅱファイルの概要2. 基本情報⑥事務担当部署	枚方市　市民生活部　市民室　市民課	枚方市　市民生活部　市民課	事後	重要な変更には当たらない。
令和8年3月30日	Ⅱファイルの概要3. 特定個人情報の入手・使用⑦使用の主体　使用部署	市民生活部市民室（各支所、サービスセンター含む）	市民生活部市民生活政策課（各支所、サービスセンター含む）、市民課	事後	重要な変更には当たらない。
令和8年3月30日	Ⅱファイルの概要5. 特定個人情報の提供・移転（委託に伴うものを除く。）提供先1	番号法別表第二に掲げる情報照会者（別紙1参照）	番号法第19条第8号に基づく主務省令第2条の表に掲げる情報照会者（別紙1参照）	事後	重要な変更には当たらない。
令和8年3月30日	Ⅱファイルの概要5. 特定個人情報の提供・移転（委託に伴うものを除く。）提供先1①法令上の根拠	番号法第１９条第8号及び別表第二	番号法第１９条第8号に基づく主務省令第2条の表	事後	重要な変更には当たらない。
令和8年3月30日	Ⅱファイルの概要5. 特定個人情報の提供・移転（委託に伴うものを除く。）提供先1②提供先における用途	番号法別表第二の第二欄に掲げる各事務。	番号法第19条第8号に基づく主務省令第2条の表第2欄に掲げる各事務	事後	重要な変更には当たらない。
令和8年3月30日	Ⅱファイルの概要（2）2. 基本情報⑥事務担当部署	枚方市　市民生活部　市民室　市民課	枚方市　市民生活部　市民課	事後	重要な変更には当たらない。
令和8年3月30日	Ⅱファイルの概要（2）3. 特定個人情報の入手・使用⑦使用の主体　使用部署	市民安全部市民室（各支所を含む）	市民生活部市民生活政策課（各支所、サービスセンターを含む）、市民課	事後	重要な変更には当たらない。
令和8年3月30日	Ⅱファイルの概要（3）2. 基本情報⑥事務担当部署	枚方市　市民生活部　市民室　市民課	枚方市　市民生活部　市民課	事後	重要な変更には当たらない。
令和8年3月30日	Ⅱファイルの概要（3）3. 特定個人情報の入手・使用⑦使用の主体　使用部署	市民生活部市民室（各支所含む）	市民生活部市民生活政策課（各支所、サービスセンターを含む）、市民課	事後	重要な変更には当たらない。
令和8年3月30日	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②請求方法	枚方市個人情報保護条例に基づき、保有個人情報の開示等請求を受け付ける。	個人情報の保護に関する法律に基づき、保有個人情報の開示等請求を受け付ける。	事後	重要な変更には当たらない。
令和8年3月30日	Ⅴ開示請求、問合せ2. 特定個人情報の取扱いに関する問合せ①連絡先	郵便番号573-8666 大阪府枚方市大垣内町二丁目1番20号 枚方市役所　市民生活部　市民室　市民課	郵便番号573-8666 大阪府枚方市大垣内町二丁目1番20号 枚方市役所　市民生活部　市民課	事後	重要な変更には当たらない。