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
23	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

富山市は、住民基本台帳事務における特定個人情報ファイルを取り扱うにあたり、その取り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軽減させるために適切な措置を講じ、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ここに宣言する。

特記事項	

評価実施機関名

富山市長

個人情報保護委員会　承認日 【行政機関等のみ】

公表日

［令和7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	住民基本台帳事務
②事務の内容　※	市区町村（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、市区町村の住民に関する正確な記録が整備されている必要がある。 住民基本台帳は、住民基本台帳法（昭和42年法律第81号。以下「住基法」という。）に基づき作成されるものであり、市区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り、市区町村において、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。））を都道府県と共同して構築している。 本市は、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（平成25年法律第27号。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ものとする。（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区町村に対する通知 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 ⑪証明書のコンビニ交付
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	1　住民基本台帳管理機能 異動処理機能および、異動入力された個人データを住民基本台帳として記録する。 2　通知機能 住民票コード通知書を発行する。 3　証明書発行機能 住民票の写し、記載事項証明書などの各種証明書を発行する。 4　住基ネット連携機能 住基ネットへの本人確認情報の連携、転出証明書情報などの市町村間の通知、個人番号の要求、個人番号通知書の送付先を連携するための機能を有する。 5　庁内連携機能 庁内の各システムで住民登録者を基礎データとして利用するため、宛名システムや他関連システムへ情報連携する。 6　庁外連携機能 住基ネットや法務省との庁外データ連携を行い、各種通知情報の収受を行う。 7　符号要求 処理通番の要求・受信を中間サーバー経由で行い、符号要求データを既存住基システムに送信する。 8　コンビニ交付システムへの連携 住民票等の各種証明書に記載する情報をコンビニ交付システムと連携する。
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　（ 申請管理システム、コンビニ交付システムなど　）

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 ※「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、住民基本台帳ネットワークシステムの構成要素のうち、市町村CSにおいて管理がなされているため、以降は、住民基本台帳ネットワークシステムの内の市町村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 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、当該情報を基に本市の市町村CS（以下「本市CS」という。）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基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5情報（氏名、氏名の振り仮名、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5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本市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	宛名管理システム
②システムの機能	1 宛名基本管理機能 税関係（法人、共有者含む）、国民健康保険、国民年金、保育料、児童手当、福祉等の住民登録者及び住民登録外者の宛名を一括管理する。 2 宛名送付先管理機能 各システムで出力する送付物に対する送付先宛名を管理する。送付先は使用する業務別に設定する。 3 納税関係者管理機能 固定資産税、個人住民税、軽自動車税の納税義務者に対する納税管理人を管理する。また、相続代表人の管理も行う。 4 送達不能管理機能 送達不能の管理を行う。 5 関連宛名管理機能 再転入等による同一人の管理を行う。
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　（各事務システム　）

システム4	
①システムの名称	団体内統合宛名（連携）システム
②システムの機能	1　宛名管理機能 個人番号にて同一人判定を行い、団体内統合宛名番号を採番し管理する。 統合宛名情報の検索・参照・更新を行う。 2　情報提供機能(業務情報を中間サーバーに提供するための機能) 各業務情報を一括データで中間サーバーに連携する。 各業務の異動情報を中間サーバーに連携する。 3　情報照会機能(他機関へ問合せをするための機能) 各業務の宛名番号で対象者を検索し、他自治体への情報提供を依頼し、結果をオンラインにて表示する。
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　（ 中間サーバー　　）

システム5	
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、情報提供に用いる個人の識別子である「符号」と、情報保有機関内で個人を特定するために利用する「団体内統合宛名番号」とを紐づけ、その情報を保管・管理する機能。 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、特定個人情報（連携対象）の情報照会および情報提供受領（照会した情報の受領）を行う機能。 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、情報照会要求の受領および当該特定個人情報（連携対象）の提供を行う機能。 4　既存システム接続機能 中間サーバーと既存システム、団体内統合宛名（連携）システム及び住基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ための機能。なお、本市においては、中間サーバーとの接続連携は、団体内統合宛名システムにおいて行う。 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、または提供があった旨の情報提供等記録を生成し、管理する機能。 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・管理する機能。 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ための機能。 8　セキュリティ管理機能 セキュリティを管理するための機能。 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機能。 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、保管期限切れ情報の削除を行う機能。
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　（　　）

システム6～10	
システム6	
①システムの名称	ダウンリカバリーシステム
②システムの機能	1．ダウンリカバリーデータベースの更新 障害・保守メンテナンス、休日・時間外等で既存住基システムが利用できない場合に備え、ダウンリカバリーシステムのデータベースを更新(同期)する。 2．住民票の写し及び印鑑証明書の交付機能 既存住基システムが利用できない場合に、代替機として、発行業務を代行する。
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7	
①システムの名称	コンビニ交付システム
②システムの機能	1．既存システム連携機能 住民票等の各種証明書の記載事項に変更または新規作成が発生した場合に、既存業務システムからデータを受信し、各種証明書に記載する情報を更新する。 2．証明書発行機能 証明書交付センターからの証明書発行要求に対して、住民票等の各種証明書データを作成し、送付する。
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　（証明書交付センター　）
システム8	
①システムの名称	申請管理システム
②システムの機能	①次期オンライン申請連携機能：次期オンライン申請に、市民が直接届出する転入・転居・転出の情報を連携する機能 ②次期オンライン申請から受信した届出・申請情報を庁内の各業務システムへ連携する機能
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　（　）
システム9	

システム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	・本市では、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 住民に関する記録を正確かつ統一的に管理し、届出等に基づく住民票の記載、修正、消除の他、本人等からの請求による住民票の写し等の交付に必要となる。コンビニ交付で住民票の写し、印鑑登録証明書を交付するためにも利用する。 （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ファイル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、機構に委任することを予定しており、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、もって国民（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条の1（本人等の請求に係る住民票の写し等の交付） ・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号に基づく主務省令第2条の表 [主務省令における情報提供の根拠] （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、110、115、118、124、129、130、132、136、137、138、141、142、144、149、150、151、152、155、156、158の項） [主務省令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	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	

（別添1）事務の内容
別添１のとおり
（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		
(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・死亡等の事由により住民票が消除された者(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		[　　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 [○] 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　(　印鑑登録情報、支援措置情報　)
	その妥当性	・個人番号、5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、5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
⑥事務担当部署		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　(　J-LIS、法務省　) [○] 地方公共団体・地方独立行政法人　(　他市区町村　) [　] 民間事業者　(　　) [○] その他　(　申請管理システム　)

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		・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		・住民に関する記録は、住基法及び同施行令に規定される届出及び記載等によるものとされている。
⑤本人への明示		・住民票の記載事項は、住基法第7条に規定されている。
⑥使用目的　※		・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　※	市民生活部市民課、各行政サービスセンター市民生活課及び各中核型地区センター、とやま市民交流館、各地区センター
	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　※		・住民票の記載事項の変更又は新規作成が生じた場合、当該情報を元に既存住基システムの住民基本台帳を更新し、本人確認情報ファイルを本市CSに送信する。 ・住民から申請又は届出があった場合、申請書又は届出書の記載内容と登録された住民基本台帳情報を照合する。 ・住民が個人番号カードを用いてコンビニ店舗から住民票の写し等の請求を行い、コンビニ店舗から住民票の写し等の交付を行う。
	情報の突合　※	・住民票の記載事項変更又は新規作成が生じた場合、個人番号、5情報、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1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 （　3）　件
委託事項1		住民基本台帳情報データ入力業務
①委託内容		・住民基本台帳に係る届出や申請に基づく既存住基システムへのデータ入力及び住民票の写し等の発行業務
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　※	「2. ③対象となる本人の範囲」と同様。
	その妥当性	住民基本台帳に係る届出や申請は、「2. ③対象となる本人の範囲」のいずれの者からも行われる可能性があるため。

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　(既存住基システムを利用)
⑤委託先名の確認方法		確認できる。(公表はされていないが、問合せがあれば回答可能)
⑥委託先名		プライムビジネススタッフ株式会社
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2～5		
委託事項2		既存住基システムの運用・保守業務
①委託内容		既存住基システムの運用・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 ※	「2. ③対象となる本人の範囲」と同様。
	その妥当性	・既存住基システムの対象は、「2. ③対象となる本人の範囲」の全ての者となるため。
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　(既存住基システムを利用)
⑤委託先名の確認方法		確認できる。(公表はされていないが、問合せがあれば回答可能)
⑥委託先名		TISI株式会社　行政システム営業部
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		コンビニ交付システムのサービス利用
①委託内容		コンビニ交付システムの開発・保守・運用業務
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様
	その妥当性	コンビニ交付システムと既存住基システムの連携には専門的な知識を有する必要があり、既存住基システム運用保守業務の委託先と同じ民間業者に委託することで、コンビニ交付システムの安定した稼働が可能となる。
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　（ 特定のコンビニシステム端末の直接操作　）
⑤委託先名の確認方法		確認できる。（公表はされていないが、問合せがあれば回答可能）
⑥委託先名		TISI株式会社　行政システム営業部
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	書面による事前承諾
	⑨再委託事項	ソフトウェア保守等
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　（　72　）件　[○]移転を行っている　（　36　）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条の表の第1欄に掲げる者（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条の表の第2欄に掲げる事務
③提供する情報		番号法第19条第8号に基づく主務省令第2条の表で規定する住民票関係情報
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介して特定個人情報の提供を求められた都度

提供先2～5	
提供先2	番号法第19条第10号に基づく条例に定める情報照会者
①法令上の根拠	番号法第19条第10号に基づく条例
②提供先における用途	番号法第19条第10号に基づく条例に定める事務
③提供する情報	番号法第19条第10号に基づく条例に定める特定個人情報
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介して特定個人情報の提供を求められた都度
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を実施する者 （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条第1項別表の第2欄に掲げる事務
③移転する情報	番号法第19条第8号に基づく主務省令第2条の表で規定する住民票関係情報
④移転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移転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　（ 庁内連携システム　）
⑦時期・頻度	住民異動が生じる都度
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　※		・入退室管理を行っている部屋に設置したサーバ内に保管する。 ・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。 ＜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、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者が保有・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サービス事業者が実施する。なお、クラウドサービス事業者は、セキュリティ管理策を適切に実施しているほか、次の事項についても満たしている。 ・ISO/IEC27017、ISO/IEC27018の認証を受けている。 ・日本国内でデータを保管している ②特定個人情報は、クラウドサービス事業者保有・管理する環境に構築する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バース上に保存される。 ＜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。
②保管期間	期間	［　　5年　　］ ＜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	・住基法施行令第34条に規定されている。
③消去方法		・住民基本台帳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。 　業務アプリケーションによるデータ消去は、論理的な消去に過ぎないため、ディスク交換やハード更改等の際は、論理的に消去されたデータが復元できないように、専用ソフトによる消去及び物理的な破壊を行うことで完全に消去する。なお、委託事業者がデータ消去を行う際は、作業完了の報告（実施日時、実施方法、証拠画像等）を書面により求めている。 ・申告書及び届出書等の紙媒体については、外部業者による溶解処理を実施している。 ・LGWAN接続端末に一時的に記録した団体間回送ファイル等は、使用の都度速やかに完全消去する。 ＜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。 ＜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。 ＜マイナポータル申請管理における措置＞ ①LGWAN接続端末に一時的に記録した個人番号付電子申請データは、使用の都度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		
（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） ※消除者を含む。
	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、5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、5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
⑥事務担当部署		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　※	市民生活部市民課、各行政サービスセンター市民生活課及び各中核型地区センター、とやま市民交流館、各地区センター
	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→本市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。(本市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→本市CS) ・5情報(氏名、氏名の振り仮名、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。(本市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7月1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		本市CSの保守業務
①委託内容		本市CSの保守作業
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	[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 ※	「2. ③対象となる本人の範囲」と同様。
	その妥当性	・保守業務の範囲は、「2. ③対象となる本人の範囲」のいずれの者も対象となるため。
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　（　）
⑤委託先名の確認方法		確認できる。（公表はされていないが、問合せがあれば回答可能）
⑥委託先名		TISI株式会社　行政システム営業部
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）をもと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。 ・都道府県の執行機関に対し本人確認情報を提供する。
③提供する情報		住民票コード、氏名、氏名の振り仮名、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、氏名の振り仮名、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	
提供先16	
提供先17	
提供先18	
提供先19	
提供先20	
移転先1	
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 ※		・入退室管理を行っている部屋に設置したサーバ内に保管する。 ・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、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（5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
業務アプリケーションによるデータ消去は、論理的な消去に過ぎないため、ディスク交換やハード更改等の際は、論理的に消去されたデータが復元できないように、専用ソフトによる消去及び物理的な破壊を行うことで完全に消去する。なお、委託事業者がデータ消去を行う際は、作業完了の報告（実施日時、実施方法、証拠画像等）を書面により求めている。

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		
(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、個人番号通知書及び個人番号カード交付申請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（個人番号カード交付等）により、当該市町村が備える住民基本台帳に記録されている者に対し、その者の申請により、その者に係る個人番号カードを交付するものとすることから、交付申請書を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		[　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　（　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、5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、個人番号通知書及び交付申請書の送付先に係る情報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
⑥事務担当部署		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		・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、本市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本市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		・番号法第7条第1項（指定及び通知）に基づき、個人番号通知書に関する必要な事項は、総務省令に記載。 また、同法第17条第8項（個人番号カードの交付等）により、個人番号カードに関する必要な事項は、総務省令に記載。
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、個人番号通知所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 ※	市民生活部市民課
	使用者数	[　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
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→本市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5情報等の変更の有無を確認する（最新の5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		本市CSの保守業務
①委託内容		本市CSの保守作業
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	[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 ※	「2. ③対象となる本人の範囲」と同様。
	その妥当性	・保守業務の範囲は、「2. ③対象となる本人の範囲」のいずれの者も対象となるため。
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 （ ）
⑤委託先名の確認方法		確認できる。（公表はされていないが、問合せがあれば回答可能）
⑥委託先名		TISI株式会社 行政システム営業部
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	機構
①法令上の根拠	・番号法第17条第8項（個人番号カードの交付等）により、個人番号カードに関する必要な事項は、総務省令に記載。
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」と同様。
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2	
①法令上の根拠	
②提供先における用途	
③提供する情報	
④提供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 （ ）
⑦時期・頻度	
提供先6～10	
提供先11～15	
提供先16～20	
移転先1	
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 ※		・入退室管理を行っている部屋に設置したサーバ内に保管する。 ・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	[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本人確認情報は、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。

7. 備考
業務アプリケーションによるデータ消去は、論理的な消去に過ぎないため、ディスク交換やハード更改等の際は、論理的に消去されたデータが復元できないように、専用ソフトによる消去及び物理的な破壊を行うことで完全に消去する。なお、委託事業者がデータ消去を行う際は、作業完了の報告（実施日時、実施方法、証拠画像等）を書面により求めている。

（別添2）特定個人情報ファイル記録項目

別添2のとおり

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	・届出については住基法第27条の規定に基づき、本人又は代理人によるものに限定し受領する。受領の際は必ず本人若しくは代理人の本人確認、委任状の確認を実施している。 ・郵送による届出の場合も、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に関する法律施行規則第11条の規定に基づき厳格に実施する。 ・既存住基システムへの情報の登録の際に、届出／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、対象者以外の情報を入手することはできない。 ・システム利用の権限は業務上必要な職員のみに与えられており、権限を付与されていない職員が情報を入手することはできない。また、メンテナンス作業や権限を付与されている者の操作ログは保管されており、情報の不正入手を防止している。 ・該当ファイルに対して、他のシステムで情報を入手（入力）することはできない仕組みになっている。 ・コンビニ交付システムは、個人番号カードを使用して認証を受けた本人及び同一世帯人からの交付請求に対してのみ証明書の発行を行う。
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	・申請書等は必要な情報のみ記載する様式としているため、必要な情報以外を入手することはない。また、申請書等を受付ける際には、余白等に必要のない情報が記載されていないか確認する。 ・管理項目は予め決められており、それ以外の項目は入力できない仕組みになっている。
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
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	・届出／申請等の様式が決められており、住民が記載事項を誤ることの無いよう工夫している。 ・届出／申請等の際、様式において住民が使用目的を認識できるようになっている。 ・連携する事務システムにおいて、必要な情報のみにアクセスできるようになっており、操作者がそれ以外の情報にアクセスすることはできない。また、メンテナンス等を行う際には、操作ログを保管する機能を有している。
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、対面で身分証明書（個人番号カード等）の提示を受け、本人確認を行う。 ・申請者が代理人である場合には、委任状に記載してある代理人であることを個人番号カードなどの身分証明書の提示により確認する。
個人番号の真正性確認の措置の内容	・提出された申請書等に記載されている個人番号とシステムに表示される個人番号を突合させることで、個人番号の真正性を確認する。 ・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の提示がない場合には、基本5情報に基づき住基ネットに照会し、真正性を確認する。
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。 ・データ入力委託業者が入力した結果を職員が再チェックを行うことで入手(入力)結果の妥当性を担保している。 ・入力、削除及び訂正作業に用いた帳票等は、本市で定める規程に基づいて管理し、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	・窓口で離席する場合は、必ず端末画面が見られないよう措置を講ずるものとする。 ・入手する情報は情報漏えいの防止措置がとられた専用回線（住民基本台帳ネットワークシステム）のみである。 ・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 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、境界 FW や連携サーバで外部接続先との通信を制限している。
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	・個人番号利用業務以外、または個人番号を必要としない業務においては、個人番号を含んだ情報は提供しない。
事務で使用するその他のシステムにおける措置の内容	・事務で使用する他のシステムからは、番号法に則りアクセス制限が施されており、個人番号を参照することはできなくなっている。 ・システムにアクセスできる端末を限定し、許可無くシステムに接続して紐付けできないようになっている。
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
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	・既存住基システムを利用する職員を特定し、システム管理者がユーザーIDを割当てパスワードによる認証を行っている。 ・IDカードとパスワードによる認証を行っている。 ・ユーザIDごとの使用履歴を取得し管理している。
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	・申請に基づき、個人ごとに必要最小限の権限を付与し、必要以上の情報参照ができないようにしている。 ・退職した元職員や異動した職員等のアクセス権限の失効管理を適切に行う。 ・アクセス権限を失効させたことについて、管理簿に記録を残す。 ・アクセス権限の発効・失効は、各課からの申請書に基づき、情報統計課で行う。
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	・既存住基システムを利用する職員に異動があれば、システム管理者への申請によりユーザーIDの発行・失効が行われる。 ・操作者の権限等に応じたアクセス権限が付与されるよう管理する。 ・責任者は、ユーザIDや付与されているアクセス権限を定期的に確認し、業務上不要なユーザIDやアクセス権限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	・住民基本台帳情報を扱うシステムの操作履歴（アクセスログ・操作ログ）を記録する。 ・不正な操作が無いことについて、操作履歴により適時確認する。
その他の措置の内容	USB等の記録媒体によるデータの持ち出しは、富山市情報セキュリティポリシーにより、原則禁止している。業務遂行上必要な場合に限り、所属長の許可のもと持ち出しを認めているが、担当者を特定のうえ、情報を取得する端末及び使用する媒体を限定している。

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	・システムの操作履歴(操作ログ)を記録する。 ・担当者へのヒアリングを実施し、業務上必要のない検索又は抽出が行われていないことを確認する。 ・システム利用職員への研修会において、事務外利用の禁止等について指導する。 ・職員以外の従業者（委託先等）には、当該事項についての誓約書の提出を求める。
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	・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。 ・管理権限を与えた職員等へ、バックアップ用ファイル以外でファイルを複製しないよう指導する。 ・コンビニ交付システムでは保有する住民基本台帳ファイルの操作や保存を行うことができないよう、システムで制御されている。
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	
・その他、特定個人情報の使用にあたり、以下の措置を講じる。 ※スクリーンセーバ等を利用して、長時間にわたり本人確認情報を表示させない。 ※ディスプレイを来庁者から見えない位置に置く。 ※大量のデータ出力に際しては、事前に管理責任者の承認を得る。	
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	・外部委託業者を選定する際、委託先の情報保護管理体制としてプライバシーマーク等の公共機関の認定・認証を取得していることを契約要件としている。 ・委託先の社会的信用と能力を確認する。また、委託業者が選定基準を引き続き満たしていることを適時確認するとともに、その記録を残す。
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	・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。 ・閲覧／更新権限を持つものを必要最小限にする。 ・閲覧／更新権限を持つ者のアカウント管理を行い、システム上で操作を制限する。 ・閲覧／更新の履歴（ログ）を取得し、不正な使用がないことを確認する。
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	・契約書等に基づき、委託業務が実施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。 ・委託業者から適時セキュリティ対策の実施状況の報告を受けるとともに、その記録を残す。 ・庁舎から書類を持ち出す場合は、枚数を確認し作業終了時に全て返却されていることを確認する。
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	・委託先から他者への特定個人情報の提供は一切認めないことを契約書上明記する。 ・また、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、必要に応じて本市職員が現地（委託先）での調査を行う。
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	・委託先に情報を提供する際は、担当部署を通じて申請書を提出し、日付及び件数を記録する。

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	・委託契約書に、以下の措置をとる旨を規定する。 ・保管期間の過ぎた特定個人情報をシステムにて自動判別し消去 ・紙媒体は、保管期間ごとに分けて保管し、保管期間が過ぎているものを外部業者にて溶解処理 ・データか紙かを問わず、廃棄の際は廃棄履歴を作成し保存 ・特定個人情報と同様、保管期間の過ぎたバックアップを、システムにて自動判別し消去 ・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、必要に応じて本市職員が現地（委託先）での調査を行う。
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	・秘密の保持 ・目的外の利用禁止 ・無断複製の禁止 ・秘密情報の返却・廃棄 ・再委託の禁止・目的外利用の禁止
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		[　　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	・再委託していない
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	・特定個人情報（個人番号、5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、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	・番号法及び住基法並びに個人情報保護条例の規定に基づき認められる特定個人情報の移転について、本業務では具体的に誰に対し何の目的で提供できるかを書き出したマニュアルを整備し、マニュアル通りに特定個人情報の提供を行う。	
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。	
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	・相手方庁内システムと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。 ・情報提供の記録が逐一保存され、その記録を監視することで不適切な方法による提供・移転を防止する。	
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	・既存住基システムにおいては、認証されない相手方への情報の移転・提供はされないことがシステム上で担保される。	
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3： 入手した特定個人情報が不正確であるリスク	
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	＜団体内統合宛名（連携）システムにおける措置＞ ・予め権限が付与された職員のみが利用できる。番号法第19条第8号に基づく主務省令第2条の表で定められた事務以外において、情報提供することはできない。 ＜中間サーバー・ソフトウェアにおける措置＞ ・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。 ・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。 ・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。 ・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。
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	＜中間サーバー・ソフトウェアにおける措置＞ ・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。 ・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＞ ・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。 ・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漏えい・紛失のリスクに対応している。 ・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。
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	＜団体内統合宛名（連携）システムにおける措置＞ ・業務システムの情報を副本として中間サーバーへ連携するものであり、情報が改変されない仕組みであることが担保されている。 ＜中間サーバー・ソフトウェアにおける措置＞ ・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。 ・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。 ・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＞ ・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＞ ・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。 ・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。 ・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。 ・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	＜既存住基システム＞ ・サーバー室と、データ、プログラム等を含んだ記録媒体及び帳票等の可搬媒体を保管する保管室は、他の部屋とは区別して専用の部屋とする。 ・出入口には機械による入退室を管理する設備を設置する。 ・入退室管理を徹底するため出入口の場所を限定する。 ・特定個人情報を管理しているコンビニ交付システムの設置場所は、次の対策を行っている。 ①ICカード、静脈認証方式による入退室管理及び監視カメラの設置による入退室者監視を行っている。 ②不正アクセスを防止するサーバーを設置し、外部からの不正アクセスを防止している。 ③各サーバーはサーバーラックに収納し、施錠した状態でサーバー室に設置している。 ＜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。 ＜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。	
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	＜既存住基システム＞ ・コンピュータウイルス監視ソフトを使用し、サーバー・端末双方でウイルスチェックを実施する。また、新種の不正プログラムに対応するために、ウイルスパターンファイルは定期的に更新し、可能な限り最新のものを使用する。 ・既存住基システムを利用できる職員を特定し、個人ごとにIDを割り当て、操作履歴（アクセスログ・操作ログ）を記録する。 ・コンビニ交付システムにおける証明書発行サーバーへの接続には、不正アクセスを防止するサーバーを介して接続することで、証明書発行サーバーへ直接接続することを防止し、アクセスの監視を行っている。 ＜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。 ＜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【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＞ ・LGWAN接続端末へのウイルス検出ソフトウェア等の導入により、ウイルス定義ファイルの定期的な更新及びウイルスチェックを行い、マルウェア検出を行う。 ・マイナポータル申請管理と本市との間は、専用線であるLGWAN回線を用いた通信を行うことで、外部からの盗聴、漏えい等が起こらないようにしており、さらに通信自体も暗号化している。
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	・死者の個人番号と生存する個人の個人番号とを分けて管理しないため、生存する個人の個人番号と同様の管理を行う。
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

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	・住民基本台帳法第14条（住民基本台帳の正確な記録を確保するための措置）及び第34条（調査）の規定に基づき、実態調査を実施することにより正確性を確保する。		
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	＜既存住基システム＞ ・特定個人情報の消去は、住民基本台帳ファイルと既存住基システムのデータを判別し消去する。 ＜中間サーバー・ソフトウエアにおける措置＞ ・中間サーバーにおいては、保存期限がその仕様上定められており、その仕様にあわせて消去される。 ＜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。 ＜申請管理システムにおける措置＞ ・LGWAN接続端末については、業務終了後の不要な個人番号付電子申請データ等の消去を徹底し、必要に応じて管理者が確認する。		
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			
業務アプリケーションによるデータ消去は、論理的な消去に過ぎないため、ディスク交換やハード更改等の際は、論理的に消去されたデータが復元できないように、専用ソフトによる消去及び物理的な破壊を行うことで完全に消去する。なお、委託事業者がデータ消去を行う際は、作業完了の報告（実施日時、実施方法、証拠画像等）を書面により求めている。			

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、届出／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。
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	・総務省告示第334号（第6－7　本人確認情報の通知及び記録）等により本市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（氏名又は氏名の振り仮名と住所の組み合わせ、氏名又は氏名の振り仮名と生年月日の組み合わせ）の指定を必須とする。
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： 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、対面で身分証明書（個人番号カード等）の提示を受け、本人確認を行う。 ・申請者が代理人である場合には、委任状に記載してある代理人であることを個人番号カードなどの身分証明書の提示により確認する。
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の提示がない場合には、本市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、本市で定める規程に基づいて管理し、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。 ※本市CSのサーバ上で稼動するアプリケーション。本市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、本市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		
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	・本市CSと宛名管理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本市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本市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、本市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、本市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	・生体認証による操作者認証を行う。	
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	・退職した元職員や異動した職員等のアクセス権限の失効管理を適切に行う。 ・アクセス権限を失効させたことについて、管理簿に記録を残す。	
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	・操作者の権限等に応じたアクセス権限が付与されるよう管理する。 ・不正アクセスを分析するために、本市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	・本人確認情報を扱うシステムの操作履歴（アクセスログ・操作ログ）を記録する。 ・不正な操作が無いことについて、操作履歴により適時確認する。 ・操作者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	USB等の記録媒体によるデータの持ち出しは、富山市情報セキュリティポリシーにより、原則禁止している。業務遂行上必要な場合に限り、所属長の許可のもと持ち出しを認めているが、担当者を特定のうえ、情報を取得する端末及び使用する媒体を限定している。	
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	・システムの操作履歴(操作ログ)を記録する。 ・担当者へのヒアリングを実施し、業務上必要のない検索又は抽出が行われていないことを確認する。 ・システム利用職員への研修会において、事務外利用の禁止等について指導する。 ・職員以外の従業者(委託先等)には、当該事項についての誓約書の提出を求める。
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	・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。 ・管理権限を与えた職員等へ、バックアップ用ファイル以外でファイルを複製しないよう指導する。
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	
その他、特定個人情報の使用にあたり、以下の措置を講じる。 ・スクリーンセーバ等を利用して、長時間にわたり本人確認情報を表示させない。 ・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る。 ・大量のデータ出力に際しては、事前に管理責任者の承認を得る。	

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	・外部委託業者を選定する際、委託先の情報保護管理体制としてプライバシーマーク等の公共機関の認定・認証を取得していることを契約要件としている。 ・委託先の社会的信用と能力を確認する。また、委託業者が選定基準を引き続き満たしていることを適時確認するとともに、その記録を残す。	
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	・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。 ・閲覧／更新権限を持つものを必要最小限にする。 ・閲覧／更新権限を持つ者のアカウント管理を行い、システム上で操作を制限する。 ・閲覧／更新の履歴（ログ）を取得し、不正な使用がないことを確認する。	
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	・契約書等に基づき、委託業務が実施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。 ・委託業者から適時セキュリティ対策の実施状況の報告を受けるとともに、その記録を残す。	
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	・委託先から他者への特定個人情報の提供は一切認めないことを契約書上明記する。 ・また、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、必要に応じて本市職員が現地（委託先）での調査を行う。	
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	・委託先に情報を提供する際は、担当部署を通じて申請書を提出し、日付及び件数を記録する。	
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	・委託契約書に、以下の措置をとる旨を規定する。 ・保管期間の過ぎた特定個人情報をシステムにて自動判別し消去 ・紙媒体は、保管期間ごとに分けて保管し、保管期間が過ぎているものを外部業者にて溶解処理 ・データか紙かを問わず、廃棄の際は廃棄履歴を作成し保存 ・特定個人情報と同様、保管期間の過ぎたバックアップを、システムにて自動判別し消去 ・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、必要に応じて本市職員が現地（委託先）での調査を行う。	
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	・秘密の保持 ・目的外の利用禁止 ・無断複製の禁止 ・秘密情報の返却・廃棄 ・再委託の禁止・目的外利用の禁止	
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	[　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		
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
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	・特定個人情報（個人番号、5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、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	・番号法及び住基法並びに個人情報保護条例の規定に基づき認められる特定個人情報の移転について、本業務では具体的に誰に対し何の目的で提供できるかを書き出したマニュアルを整備し、マニュアル通りに特定個人情報の提供を行う。
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。
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）と本市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。 ・情報提供の記録が逐一保存され、その記録を監視することで不適切な方法による提供・移転を防止する。
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移転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3: 入手した特定個人情報が不正確であるリスク		
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5: 不正な提供が行われるリスク		
リスク6: 不適切な方法で提供されるリスク		
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		
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	・サーバー室と、データ、プログラム等を含んだ記録媒体及び帳票等の可搬媒体を保管する保管室は、他の部屋とは区別して専用の部屋とする。 ・出入口には機械による入退室を管理する設備を設置する。 ・入退室管理を徹底するため出入口の場所を限定する。	
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	・不正プログラム対策 コンピュータウイルス監視ソフトを使用し、サーバ・端末双方でウイルスチェックを実施する。また、新種の不正プログラムに対応するために、ウイルスパターンファイルは定期的に更新し、可能な限り最新のものを使用する。 本人確認情報の管理について定めた規程に基づき、コンピュータウイルス等の有害なソフトウェアへの対策を行う場合の手順等を整備する。 また、同規程に基づき、オペレーション管理に係る手順等を整備し、当該手順に従って、情報セキュリティホールに関連する情報(コンピュータウイルス等の有害なソフトウェアに関連する情報を含む)を定期的(コンピュータウィルス関連情報は毎日、その他の情報は少なくとも半年に一度)に入手し、機器の情報セキュリティに関する設定の内容が適切であるかどうかを確認する。 ・不正アクセス対策 本人確認情報の管理について定めた規程に基づき、ネットワーク管理に係る手順等を整備し、ファイアウォールを導入する。	
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	・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6－8（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		・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、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）に定める保存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、要領・手順書等に基づき、内容の消去、破壊等を行うとともに、磁気ディスク管理簿にその記録を残す。また、専用ソフトによるフォーマット、物理的粉砕等を行うことにより、内容を読み出すことができないようにする。 ・帳票については、要領・手順書等に基づき、帳票管理簿等を作成し、受渡し、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。 ・廃棄時には、要領・手順書等に基づき、裁断、溶解等を行うとともに、帳票管理簿等にその記録を残す。
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	
(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	・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、届出／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。
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	・総務省告示第334号（第6－7　本人確認情報の通知及び記録）等により本市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（氏名又は氏名の振り仮名と住所の組み合わせ、氏名又は氏名の振り仮名と生年月日の組み合わせ）の指定を必須とする。
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： 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	・特定個人情報の入手元である既存住基システムへの情報の登録の際、窓口において、対面で身分証明書の提示を受け、本人確認を行う。
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、送付後速やかに本市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	
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。 ※本市CSのサーバ上で稼動するアプリケーション。本市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、本市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	

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	・本市CSと宛名管理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本市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本市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、本市CSのサーバ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、本市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	・生体認証による操作者認証を行う。	
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	・退職した元職員や異動した職員等のアクセス権限の失効管理を適切に行う。 ・アクセス権限を失効させたことについて、管理簿に記録を残す。	
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	・操作者の権限等に応じたアクセス権限が付与されるよう管理する。 ・不正アクセスを分析するために、本市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	・本人確認情報を扱うシステムの操作履歴（アクセスログ・操作ログ）を記録する。 ・不正な操作が無いことについて、操作履歴により適時確認する。 ・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	USB等の記録媒体によるデータの持ち出しは、富山市情報セキュリティポリシーにより、原則禁止している。業務遂行上必要な場合に限り、所属長の許可のもと持ち出しを認めているが、担当者を特定のうえ、情報を取得する端末及び使用する媒体を限定している。	
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	・システムの操作履歴(操作ログ)を記録する。 ・担当者へのヒアリングを実施し、業務上必要のない検索又は抽出が行われていないことを確認する。 ・システム利用職員への研修会において、事務外利用の禁止等について指導する。 ・職員以外の従業者（委託先等）には、当該事項についての誓約書の提出を求める。	
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	・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。 ・管理権限を与えた職員等へ、バックアップ用ファイル以外でファイルを複製しないよう指導する。
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

その他、特定個人情報の使用にあたり、以下の措置を講じる。
・スクリーンセーバ等を利用して、長時間にわたり本人確認情報を表示させない。
・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る。
・大量のデータ出力に際しては、事前に管理責任者の承認を得る。

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	・外部委託業者を選定する際、委託先の情報保護管理体制としてプライバシーマーク等の公共機関の認定・認証を取得していることを契約要件としている。 ・委託先の社会的信用と能力を確認する。また、委託業者が選定基準を引き続き満たしていることを適時確認するとともに、その記録を残す。	
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	・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。 ・閲覧／更新権限を持つものを必要最小限にする。 ・閲覧／更新権限を持つ者のアカウント管理を行い、システム上で操作を制限する。 ・閲覧／更新の履歴（ログ）を取得し、不正な使用がないことを確認する。	
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	・契約書等に基づき、委託業務が実施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。 ・委託業者から適時セキュリティ対策の実施状況の報告を受けるとともに、その記録を残す。	
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	・委託先から他者への特定個人情報の提供は一切認めないことを契約書上明記する。 ・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、必要に応じて本市職員が現地（委託先）での調査を行う。	
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	・委託先に情報を提供する際は、担当部署を通じて申請書を提出し、日付及び件数を記録する。	
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	・委託契約書に、以下の措置をとる旨を規定する。 ・保管期間の過ぎた特定個人情報をシステムにて自動判別し消去 ・紙媒体は、保管期間ごとに分けて保管し、保管期間が過ぎているものを外部業者にて溶解処理 ・データか紙かを問わず、廃棄の際は廃棄履歴を作成し保存 ・特定個人情報と同様、保管期間の過ぎたバックアップを、システムにて自動判別し消去 ・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、必要に応じて本市職員が現地（委託先）での調査を行う。	
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	・秘密の保持 ・目的外の利用禁止 ・無断複製の禁止 ・秘密情報の返却・廃棄 ・再委託の禁止・目的外利用の禁止	
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	[　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		
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	・特定個人情報（個人番号、5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、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	・番号法及び住基法並びに個人情報保護条例の規定に基づき認められる特定個人情報の移転について、本業務では具体的に誰に対し何の目的で提供できるかを書き出したマニュアルを整備し、マニュアル通りに特定個人情報の提供を行う。	
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。	
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（個人番号カード管理システム）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、既存住基システムから入手した情報の内容に編集を加えず、適切に個人番号カード管理システムに提供することを担保する。 ・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（個人番号カード管理システム）と本市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移転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3： 入手した特定個人情報が不正確であるリスク	
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5： 不正な提供が行われるリスク	
リスク6： 不適切な方法で提供されるリスク	
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	
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	・サーバー室と、データ、プログラム等を含んだ記録媒体及び帳票等の可搬媒体を保管する保管室は、他の部屋とは区別して専用の部屋とする。 ・出入口には機械による入退室を管理する設備を設置する。 ・入退室管理を徹底するため出入口の場所を限定する。	
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	・不正プログラム対策 　コンピュータウイルス監視ソフトを使用し、サーバ・端末双方でウイルスチェックを実施する。また、新種の不正プログラムに対応するために、ウイルスパターンファイルは定期的に更新し、可能な限り最新のものを使用する。 　本人確認情報の管理について定めた規程に基づき、コンピュータウイルス等の有害なソフトウェアへの対策を行う場合の手順等を整備する。 　また、同規程に基づき、オペレーション管理に係る手順等を整備し、当該手順に従って、情報セキュリティホールに関連する情報（コンピュータウイルス等の有害なソフトウェアに関連する情報を含む）を定期的（コンピュータウィルス関連情報は毎日、その他の情報は少なくとも半年に一度）に入手し、機器の情報セキュリティに関する設定の内容が適切であるかどうかを確認する。 ・不正アクセス対策 　本人確認情報の管理について定めた規程に基づき、ネットワーク管理に係る手順等を整備し、ファイアウォールを導入する。	
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	・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、本市では保管しない。 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		
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	＜本市における措置＞ ・評価書の記載内容通りの運用ができているか、定期的に担当部署内において自己点検によるチェックを実施する。 ＜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	＜本市における措置＞ ・富山市情報システム等の管理運営に関する規則等に基づき、年次計画を策定し内部監査を実施している。監査項目に評価書に記載してある項目の確認や個人情報に関する管理体制等を加え、監査結果を踏まえて管理方法や体制の改善を図る。 ＜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関する項目について監査項目に加えるとともに、定期的な監査以外にも不定期に監査を実施し、厳格な管理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	＜本市における措置＞ ・事務担当部署が移転先部署に対し、個人情報の管理や運用に必要となる手順等を周知する。 ・情報システムを取り扱う職員に対し情報セキュリティ確保のための研修の受講を義務付け、富山市情報セキュリティーポリシーおよび富山市情報セキュリティ共通実施手順等を遵守させている。 ・委託業者については、契約内容にポリシーの遵守に関する項目を設けている。 ＜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。 ・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

＜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	〒930-8510 富山県富山市新桜町7番38号　企画管理部 文書法務課 電話番号　076-443-2261　ファックス番号　076-443-2170
②請求方法	本人確認書類の提示及び指定様式による書面の提出により開示・訂正・利用停止請求を受け付ける。
特記事項	
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	住民記録システム
公表場所	富山市ホームページ https://www.city.toyama.lg.jp/shisei/jyohokokai/1010947/1012727.html
⑤法令による特別の手続	
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	〒930-8510 富山県富山市新桜町7番38号　企画管理部 情報システム課 電話番号　076-443-2015
②対応方法	・問い合わせ受付票を準備し、対応記録を残す ・規定に定められた担当部署に速やかに連絡し、協議のうえ対応する

Ⅵ　評価実施手続

1．基礎項目評価	
①実施日	令和8年6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	富山市ホームページ及び情報統計課において評価書案を公表し、意見を求めた。なお、意見募集時には事前に広報誌において、意見募集の周知を図った。
②実施日・期間	
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	
③結果	
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1年6月21日	Ⅰ－7．－②	市民課長　中村　正美	市民課長	事後	
令和1年6月21日	Ⅴ－1．－①	〒930-8510 富山県富山市新桜町7番38号　　企画管理部 情報統計課　　電話番号　076-443-2015 ファックス番号　076-443-2202	〒930-8510 富山県富山市新桜町7番38号　　企画管理部 文書法務課　　電話番号　076-443-2261 ファックス番号　076-443-2170	事後	
令和2年2月3日	Ⅰ－1－②	＜省略＞	＜省略＞ ＜追加＞ ⑪証明書のコンビニ交付	事前	
令和2年2月3日	Ⅰ－2．－システム1－②	＜1～7＞省略	＜1～7＞省略 8　コンビニ交付システムへの連携 住民票等の各種証明書に記載する情報をコンビニ交付システムと連携する。	事前	
令和2年2月3日	Ⅰ－2．－システム1－③	＜省略＞ [○]その他　（戸籍システムなど）	＜省略＞ [○]その他　（戸籍システム、コンビニ交付システム）	事前	
令和2年2月3日	Ⅰ－2．－システム7	なし	追加	事前	
令和2年2月3日	Ⅰ－4．－①	＜省略＞ （1）住民基本台帳ファイル 住民に関する記録を正確かつ統一的に管理し、届出等に基づく住民票の記載、修正、消除の他、本人等からの請求による住民票の写し等の交付に必要となる。 ＜省略＞	＜省略＞ （1）住民基本台帳ファイル 住民に関する記録を正確かつ統一的に管理し、届出等に基づく住民票の記載、修正、消除の他、本人等からの請求による住民票の写し等の交付に必要となる。コンビニ交付で住民票の写し、印鑑登録証明書を交付するためにも利用する。 ＜省略＞	事前	
令和2年2月3日	Ⅰ－（別添1）事務の内容－（図）	―	別紙「（別添1）事務の内容」参照	事前	
令和2年2月3日	Ⅰ－（別添1）事務の内容－（備考）	＜1～3省略＞	＜1～3省略＞ 4．コンビニ店舗における証明書交付事務 4-①　コンビニ店舗に設置されたキオスク端末からの発行要求に基づき、証明書データを作成し、証明書交付センターと連携する。	事前	
令和2年2月3日	Ⅱ－3．－特定個人情報の入手・使用－⑧	＜省略＞	＜省略＞ ＜追加＞ ・住民が個人番号カードを用いてコンビニ店舗から住民票の写し等の請求を行い、コンビニ店舗から住民票の写し等の交付を行う。	事前	
令和2年2月3日	Ⅱ－4．－委託の有無　※	2件	3件	事前	
令和2年2月3日	Ⅱ－4．－委託事項3	なし	追加	事前	
令和2年2月3日	Ⅲ－2．－リスク1－対象者以外の情報の入手を防止するための措置の内容	＜省略＞	＜省略＞ ＜追加＞ ・コンビニ交付システムは、個人番号カードを使用して認証を受けた本人及び同一世帯人からの交付請求に対してのみ証明書の発行を行う。	事前	

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2年2月3日	Ⅲ－3．－リスク4－リスクに対する措置の内容	＜省略＞ ・・管理権限を与えた職員等へ、バックアップ用ファイル以外でファイルを複製しないよう指導する。	＜省略＞ ・管理権限を与えた職員等へ、バックアップ用ファイル以外でファイルを複製しないよう指導する。 ＜追加＞ ・コンビニ交付システムでは保有する住民基本台帳ファイルの操作や保存を行うことができないよう、システムで制御されている。	事前	
令和2年2月3日	Ⅲ－7．－リスク1－⑤－具体的な対策の内容	＜既存住基システム＞ ＜省略＞	＜既存住基システム＞ ＜省略＞ ＜追加＞ ・特定個人情報を管理しているコンビニ交付システムの設置場所は、次の対策を行っている。 ①ICカード、静脈認証方式による入退室管理及び監視カメラの設置による入退室者監視を行っている。 ②不正アクセスを防止するサーバーを設置し、外部からの不正アクセスを防止している。 ③各サーバーはサーバーラックに収納し、施錠した状態でサーバー室に設置している。	事前	
令和2年2月3日	Ⅲ－7．－リスク1－⑥－具体的な対策の内容	＜既存住基システム＞ ＜省略＞	＜既存住基システム＞ ＜省略＞ ＜追加＞ ・コンビニ交付システムにおける証明書発行サーバーへの接続には、不正アクセスを防止するサーバーを介して接続することで、証明書発行サーバーへ直接接続することを防止し、アクセスの監視を行っている。	事前	
令和3年3月1日	Ⅱ－1（1）住民基本台帳ファイル．3⑦使用の主体（使用部署）	市民生活部、各総合行政センター市民生活課及び市民福祉課、とやま市民交流館、各地区センター	市民生活部市民課、各行政サービスセンター市民生活課及び市民福祉課、各中核型地区センター、とやま市民交流館、各地区センター	事後	
令和3年3月1日	Ⅱ－1（1）住民基本台帳ファイル．4委託事項1⑥委託先名	富山総合ビルセンター株式会社	株式会社スキル	事後	
令和3年3月1日	Ⅱ－1（1）住民基本台帳ファイル．4委託事項3⑦再委託の有無	再委託しない	再委託する		
令和3年3月1日	Ⅱ－1（1）住民基本台帳ファイル．4委託事項3⑧再委託の許諾方法	なし	＜追加＞ 書面による事前承諾		
令和3年3月1日	Ⅱ－1（1）住民基本台帳ファイル．4委託事項3⑨再委託事項	なし	＜追加＞ ソフトウェア保守等		
令和3年3月1日	Ⅱ－1（2）本人確認情報ファイル．3⑦使用の主体（使用部署）	市民生活部、各総合行政センター市民生活課及び市民福祉課、とやま市民交流館、各地区センター	市民生活部市民課、各行政サービスセンター市民生活課及び市民福祉課、各中核型地区センター、とやま市民交流館、各地区センター		
令和3年3月1日	Ⅱ－1（3）送付先情報ファイル．2③対象となる本人の範囲（その他必要性）	・番号法第7条第2項（指定及び通知）に基づき、通知カード及び個人番号カード交付申請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（個人番号カード交付等）により、当該市町村が備える住民基本台帳に記録されている者に対し、その者の申請により、その者に係る個人番号カードを交付するものとすることから、交付申請書を通知カード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。	・番号法第7条第1項（指定及び通知）に基づき、個人番号通知書及び個人番号カード交付申請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（個人番号カード交付等）により、当該市町村が備える住民基本台帳に記録されている者に対し、その者の申請により、その者に係る個人番号カードを交付するものとすることから、交付申請書を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。		

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3年3月1日	Ⅱ－1（3）送付先情報ファイル．2④記録される項目（その妥当性）	・個人番号、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（通知カード及び交付申請書の送付先の情報） 　機構に対し、法令に基づき通知カード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、通知カード及び交付申請書の送付先に係る情報に係る情報を記録する必要がある。	・個人番号、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、個人番号通知書及び交付申請書の送付先に係る情報に係る情報を記録する必要がある。		
令和3年3月1日	Ⅱ－1（3）送付先情報ファイル．2⑤保有開始日	平成27年10月予定	平成27年10月		
令和3年3月1日	Ⅱ－1（3）送付先情報ファイル．3⑤本人への明示	・番号法第7条第2項（指定及び通知）に基づき、通知カードに関する必要な事項は、総務省令に記載予定。 また、同法第17条第8項（個人番号カードの交付等）により、個人番号カードに関する必要な事項は、総務省令に記載予定。	・番号法第7条第1項（指定及び通知）に基づき、個人番号通知書に関する必要な事項は、総務省令に記載。 また、同法第17条第8項（個人番号カードの交付等）により、個人番号カードに関する必要な事項は、総務省令に記載。		
令和3年3月1日	Ⅱ－1（3）送付先情報ファイル．3⑧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、通知カード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→本市CS又は電子記録媒体→個人番号カード管理システム（機構））。	・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→本市CS又は電子記録媒体→個人番号カード管理システム（機構））。		
令和3年3月1日	Ⅱ－1（3）送付先情報ファイル．5提供先1①法令上の根拠	・番号法第7条第8項（指定及び通知）に基づき、通知カードに関する必要な事項は、総務省令に記載予定。 ・また、同法第17条第8項（個人番号カードの交付等）により、個人番号カードに関する必要な事項は、総務省令に記載予定。	・番号法第17条第8項（個人番号カードの交付等）により、個人番号カードに関する必要な事項は、総務省令に記載。		
令和3年3月1日	Ⅱ－1（3）送付先情報ファイル．5提供先1②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、通知カード及び交付申請書を印刷し、送付する。	・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。		
令和3年3月1日	Ⅱ－6.－②	＜省略＞	＜追加＞ ［別表第二における情報提供の根拠］ 74、85の2、97		
令和3年3月1日	「（別添2）ファイル記録項目」シート	＜省略＞	＜追加＞ ［旧氏漢字］［旧氏かな］		
令和3年9月1日	Ⅰ2．－システム1．－②	4　住基ネット連携機能 　住基ネットへの本人確認情報の連携、転出証明書情報などの市町村間の通知、個人番号の要求、通知カードの送付先を連携するための機能を有する。	4　住基ネット連携機能 　住基ネットへの本人確認情報の連携、転出証明書情報などの市町村間の通知、個人番号の要求、個人番号通知書の送付先を連携するための機能を有する。	事後	
令和3年9月1日	Ⅰ2．－システム2．－②	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(通知カード、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本市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。	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本市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。	事後	

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3年9月1日	Ⅰ4．－①	（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通知カード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）。通知カード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、機構に委任することを予定しており、機構に通知カード及び交付申請書の送付先情報を提供する。	（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、機構に委任することを予定しており、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。	事後	
令和3年9月1日	Ⅰ6．－②	番号法第19条第7号	番号法第19条第8号	事後	法改正に伴う修正
令和3年9月1日	Ⅱ－1（1）住民基本台帳ファイル．3⑦使用の主体（使用部署）	市民生活部市民課、各行政サービスセンター 市民生活課及び市民福祉課、各中核型地区センター、とやま市民交流館、各地区センター	市民生活部市民課、各行政サービスセンター 市民生活課及び各中核型地区センター、とやま市民交流館、各地区センター	事後	
令和3年9月1日	Ⅱ－1（1）住民基本台帳ファイル．5提供先1	番号法第19条第7号	番号法第19条第8号	事後	法改正に伴う修正
令和3年9月1日	Ⅱ－1（1）住民基本台帳ファイル．5提供先1①	番号法第19条第7号	番号法第19条第8号	事後	法改正に伴う修正
令和3年9月1日	Ⅱ－1（1）住民基本台帳ファイル．5提供先1②	番号法第19条第7号	番号法第19条第8号	事後	法改正に伴う修正
令和3年9月1日	Ⅱ－1（1）住民基本台帳ファイル．5提供先1③	番号法第19条第7号	番号法第19条第8号	事後	法改正に伴う修正
令和3年9月1日	Ⅱ－1（1）住民基本台帳ファイル．5提供先2	番号法第19条第9号	番号法第19条第10号	事後	法改正に伴う修正
令和3年9月1日	Ⅱ－1（1）住民基本台帳ファイル．5提供先2①	番号法第19条第9号	番号法第19条第10号	事後	法改正に伴う修正
令和3年9月1日	Ⅱ－1（1）住民基本台帳ファイル．5提供先2②	番号法第19条第9号	番号法第19条第10号	事後	法改正に伴う修正
令和3年9月1日	Ⅱ－1（1）住民基本台帳ファイル．5提供先2③	番号法第19条第9号	番号法第19条第10号	事後	法改正に伴う修正
令和3年9月1日	Ⅱ－1（2）本人確認情報ファイル．3⑦使用の主体（使用部署）	市民生活部市民課、各行政サービスセンター 市民生活課及び市民福祉課、各中核型地区センター、とやま市民交流館、各地区センター	市民生活部市民課、各行政サービスセンター 市民生活課及び各中核型地区センター、とやま市民交流館、各地区センター	事後	
令和3年9月1日	Ⅱ－1（3）送付先情報ファイル．2④記録される項目（主な記録項目）	・業務関係情報　その他（通知カード及び交付申請書の送付先の情報）	・業務関係情報　その他（個人番号通知書及び交付申請書の送付先の情報）	事後	
令和3年9月1日	Ⅱ－1（3）送付先情報ファイル．3③入手の時期・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）。	・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）。	事後	
令和3年9月1日	Ⅲ－1．（1）2．－リスク3－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、基本4情報に基づき住基ネットに照会し、真正性を確認する。	・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の提示がない場合には、基本4情報に基づき住基ネットに照会し、真正性を確認する。	事後	

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3年9月1日	Ⅲ－1．(2)2．－リスク3－ 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、本市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。	・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の提示がない場合には、本市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。	事後	
令和7年3月25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	・番号法第19条第8号（特定個人情報の提供の制限）及び別表第二 [別表第二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（特定個人情報）に「住民票関係情報」が含まれる項（1、2、3、4、6、8、9、11、16、18、20、21、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、108、111、112、113、114、116、117、120の項） [別表第二における情報照会の根拠] （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）	番号法第19条第8号に基づく主務省令第2条の表 [主務省令における情報提供の根拠] （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、110、115、118、124、129、130、132、136、137、138、141、142、144、149、150、151、152、155、156、158の項） [主務省令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）	事後	法改正に伴う修正
令和7年3月25日	Ⅱ特定個人情報ファイルの概要 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	・番号法第19条第8号別表第二の第1欄に掲げる者 （別紙1参照）	番号法第19条第8号に基づく主務省令第2条の表の第1欄に掲げる者（別紙1参照）	事後	法改正に伴う修正
令和7年3月25日	Ⅱ特定個人情報ファイルの概要 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 ①法令上の根拠	・番号法第19条第8号別表第二	番号法第19条第8号に基づく主務省令第2条の表	事後	法改正に伴う修正
令和7年3月25日	Ⅱ特定個人情報ファイルの概要 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 ②提供先における用途	・番号法第19条第8号別表第二の第2欄に掲げる事務	番号法第19条第8号に基づく主務省令第2条の表の第2欄に掲げる事務	事後	法改正に伴う修正
令和7年3月25日	Ⅱ特定個人情報ファイルの概要 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 ③提供する情報	・番号法第19条第8号別表第二で規定する住民票関係情報	番号法第19条第8号に基づく主務省令第2条の表で規定する住民票関係情報	事後	法改正に伴う修正
令和7年3月25日	Ⅱ特定個人情報ファイルの概要 5. 特定個人情報の提供・移転（委託に伴うものを除く。） 移転先1	番号法第9条第1項別表第一に定める事務を実施する者 （別紙2参照）	番号法第9条第1項別表に定める事務を実施する者 （別紙2参照）	事後	法改正に伴う修正
令和7年3月25日	Ⅱ特定個人情報ファイルの概要 5. 特定個人情報の提供・移転（委託に伴うものを除く。） 移転先1 ①法令上の根拠	番号法第9条第1項別表第一	番号法第9条第1項別表	事後	法改正に伴う修正
令和7年3月25日	Ⅱ特定個人情報ファイルの概要 5. 特定個人情報の提供・移転（委託に伴うものを除く。） 移転先1 ②移転先における用途	番号法第9条第1項別表第一の第2欄に掲げる事務	番号法第9条第1項別表の第2欄に掲げる事務	事後	法改正に伴う修正

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7年3月25日	Ⅱ特定個人情報ファイルの概要 5. 特定個人情報の提供・移転（委託に伴うものを除く。） 移転先1 ③提供する情報	住民票関係情報	番号法第19条第8号に基づく主務省令第2条の表で規定する住民票関係情報	事後	法改正に伴う修正
令和7年3月25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 6. 情報提供ネットワークシステムとの接続 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	＜団体内統合宛名（連携）システムにおける措置＞ ・予め権限が付与された職員のみが利用できる。番号法の別表第二で定められた事務以外において、情報提供することはできない。	＜団体内統合宛名（連携）システムにおける措置＞ ・予め権限が付与された職員のみが利用できる。番号法第19条第8号に基づく主務省令第2条の表で定められた事務以外において、情報提供することはできない。	事後	法改正に伴う修正
令和7年3月25日	Ⅳ開示請求、問い合わせ 2. 特定個人情報ファイルに関する問い合わせ	〒930-8510 富山県富山市新桜町7番38号　企画管理部情報統計課 電話番号　076-443-2015　ファックス番号　076-443-2202	〒930-8510 富山県富山市新桜町7番38号　企画管理部情報システム課 電話番号　076-443-2015	事後	
令和7年3月25日	Ⅳ評価実施手続 1.基礎項目評価 ①実施日	2021/3/1	2025/2/1	事後	
	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 ①システムの名称	住基ネットCS部分	住民基本台帳ネットワークシステム ※「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、住民基本台帳ネットワークシステムの構成要素のうち、市町村CSにおいて管理がなされているため、以降は、住民基本台帳ネットワークシステムの内の市町村CS部分について記載する。	事後	
	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 ②システムの機能 4　本人確認情報検索	・4情報（氏名、住所、性別、生年月日）	・5情報（氏名、氏名の振り仮名、住所、性別、生年月日）	事後	法改正に伴う修正
	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 ②システムの機能 5. 機構への情報照会	・4情報	・5情報	事後	法改正に伴う修正
	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9	なし	1. システムの名称　申請管理システム 2. システムの機能 ①次期オンライン申請サービス連携機能：次期オンライン申請サービスに、市民が直接届出する転入・転居・転出の情報を連携する機能 ②次期オンライン申請サービスから受信した届出・申請情報を庁内の各業務システムへ連携する機能	事後	基幹系システム標準化に伴う修正
	Ⅰ－（別添1）事務の内容－（図）	―	「（別添1）事務の内容」参照	事後	基幹系システム標準化に伴う修正

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－（別添1）事務の内容－（備考）	―	「（別添1）事務の内容」参照	事後	基幹系システム標準化に伴う修正
	Ⅱ特定個人情報 ファイルの概要(1) 2. 基本情報 ④記録される項目	10項目以上50項目未満	100項目以上	事後	基幹系システム標準化に伴う修正
	Ⅱ特定個人情報 ファイルの概要(1) 2. 基本情報 ④記録される項目 主な記録項目	・4情報（氏名、住所、性別、生年月日） ・その他（なし）	・5情報（氏名、氏名の振り仮名、住所、性別、生年月日） ・その他（印鑑登録情報、支援措置情報）	事後	・法改正に伴う修正 ・基幹系システム標準化に伴う修正
	Ⅱ 特定個人情報ファイルの概要(1) 2. 基本情報 ④記録される項目 その妥当性	・4情報	・5情報	事後	法改正に伴う修正
	Ⅱ 特定個人情報ファイルの概要(1) 3. 特定個人情報の入手・使用 ①入手元	・評価実施機関内の他部署（介護保険課） ・行政機関・独立行政法人（機構、法務省） ・その他（なし）	・評価実施機関内の他部署（なし） ・行政機関・独立行政法人（J-lis、法務省） ・その他（申請管理システム）	事後	基幹系システム標準化に伴う修正
	Ⅱ 特定個人情報ファイルの概要(1) 3. 特定個人情報の入手・使用 ⑧使用方法 情報の突合	4情報	5情報	事後	法改正に伴う修正
	Ⅱ特定個人情報ファイルの概要(1) 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	株式会社スキル	プライムビジネススタッフ株式会社	事後	
	Ⅱ特定個人情報ファイルの概要(1) 4. 特定個人情報ファイルの取扱いの委託 委託事項2 ⑥委託先名	株式会社インテック　行政システム事業本部	TISI株式会社　行政システム営業部	事後	
	Ⅱ特定個人情報ファイルの概要(1) 4. 特定個人情報ファイルの取扱いの委託 委託事項3 ⑥委託先名	株式会社インテック　行政システム事業本部	TISI株式会社　行政システム営業部	事後	
	Ⅱ 特定個人情報ファイルの概要(1) 5. 特定個人情報の提供・移転 提供・移転の有無	提供を行っている（55件）移転を行っている（36件）	提供を行っている（72件）移転を行っている（36件）	事後	

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(1) 6. 特定個人情報の保管・消去 ①保管場所	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。	・入退室管理を行っている部屋に設置したサーバ内に保管する。 ・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。 ＜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、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者が保有・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サービス事業者が実施する。なお、クラウドサービス事業者は、セキュリティ管理策を適切に実施しているほか、次の事項についても満たしている。 ・ISO/IEC27017、ISO/IEC27018の認証を受けている。 ・日本国内でデータを保管している ②特定個人情報は、クラウドサービス事業者保有・管理する環境に構築する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バース上に保存される。 ＜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。	事後	

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(1) 6．特定個人情報の保管・消去 ③消去方法	－	・住民基本台帳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。 　業務アプリケーションによるデータ消去は、論理的な消去に過ぎないため、ディスク交換やハード更改等の際は、論理的に消去されたデータが復元できないように、専用ソフトによる消去及び物理的な破壊を行うことで完全に消去する。なお、委託事業者がデータ消去を行う際は、作業完了の報告（実施日時、実施方法、証拠画像等）を書面により求めている。 ・申告書及び届出書等の紙媒体については、外部業者による溶解処理を実施している。 ・LGWAN接続端末に一時的に記録した団体間回送ファイル等は、使用の都度速やかに完全消去する。 ＜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。 ＜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。 ＜マイナポータル申請管理における措置＞ ①LGWAN接続端末に一時的に記録した個人番号付電子申請データは、使用の都度速やかに完全消去する。	事後	

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(2) 2. 基本情報 ④記録される項目	10項目未満	10項目以上50項目未満	事後	
	Ⅱ 特定個人情報ファイルの概要(2) 2. 基本情報 ④記録される項目 主な記録項目	・4情報（氏名、住所、性別、生年月日）	・5情報（氏名、氏名の振り仮名、住所、性別、生年月日）	事後	法改正に伴う修正
	Ⅱ 特定個人情報ファイルの概要(2) 2. 基本情報 ④記録される項目 その妥当性	・4情報	・5情報	事後	法改正に伴う修正
	Ⅱ 特定個人情報ファイルの概要(2) 3. 特定個人情報の入手・使用 ⑧使用方法	・4情報	・5情報	事後	法改正に伴う修正
	Ⅱ特定個人情報ファイルの概要(2) 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	株式会社インテック　行政システム事業本部	TISI株式会社　行政システム営業部	事後	
	Ⅱ特定個人情報ファイルの概要(3) 2. 基本情報 ④記録される項目	10項目未満	10項目以上50項目未満	事後	
	Ⅱ 特定個人情報ファイルの概要(3) 2. 基本情報 ④記録される項目 主な記録項目	・4情報（氏名、住所、性別、生年月日）	・5情報（氏名、氏名の振り仮名、住所、性別、生年月日）	事後	法改正に伴う修正
	Ⅱ 特定個人情報ファイルの概要(3) 2. 基本情報 ④記録される項目 その妥当性	・4情報	・5情報	事後	法改正に伴う修正

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(3) 3. 特定個人情報の入手・使用 ⑧使用方法 情報の突合	・4情報	・5情報	事後	法改正に伴う修正
	Ⅱ特定個人情報ファイルの概要(3) 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	株式会社インテック　行政システム事業本部	TISI株式会社　行政システム営業部	事後	
	(別添2)特定個人情報ファイル記録項目	―	「(別添2)ファイル記録項目」参照	事後	
	Ⅲ特定個人情報ファイルの取り扱いプロセスにおけるリスク対策(1) 2. 特定個人情報の入手 リスク1 個人番号の真正性確認の措置の内容	基本4情報	基本5情報	事後	法改正に伴う修正
	Ⅲ特定個人情報ファイルの取り扱いプロセスにおけるリスク対策(1) 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	―	・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 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、境界 FW や連携サーバで外部接続先との通信を制限している。	事後	法改正に伴う修正
	Ⅲ特定個人情報ファイルの取り扱いプロセスにおけるリスク対策(1) 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	―	IDカードとパスワードによる認証を行っている。	事後	法改正に伴う修正
	Ⅲ特定個人情報ファイルの取り扱いプロセスにおけるリスク対策(1) 5. 特定個人情報の提供・移転 リスク1 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 具体的な方法	4情報等	5情報等	事後	法改正に伴う修正
	Ⅲ特定個人情報ファイルの取り扱いプロセスにおけるリスク対策(1) 7. 特定個人情報の保管・消去 リスク1 ⑤物理的対策 具体的な対策の内容	―	＜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。	事後	法改正に伴う修正

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り扱いプロセスにおけるリスク対策(1) 7. 特定個人情報の保管・消去 リスク1 ⑥技術的対策 具体的な対策の内容	―	＜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【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＞・LGWAN接続端末へのウイルス検出ソフトウェア等の導入により、ウイルス定義ファイルの定期的な更新及びウイルスチェックを行い、マルウェア検出を行う。・マイナポータル申請管理と本市との間は、専用線であるLGWAN回線を用いた通信を行うことで、外部からの盗聴、漏えい等が起こらないようにしており、さらに通信自体も暗号化している。	事後	法改正に伴う修正
	Ⅲ特定個人情報ファイルの取り扱いプロセスにおけるリスク対策(1) 7. 特定個人情報の保管・消去 リスク3 消去手順 手順の内容	―	＜中間サーバー・ソフトウエアにおける措置＞ ・中間サーバーにおいては、保存期限がその仕様上定められており、その仕様にあわせて消去される。 ＜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。 ＜申請管理システムにおける措置＞ ・LGWAN接続端末については、業務終了後の不要な個人番号付電子申請データ等の消去を徹底し、必要に応じて管理者が確認する。	事後	法改正に伴う修正

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り扱いプロセスにおけるリスク対策(2) 2. 特定個人情報の入手 リスク1 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	氏名と住所の組み合わせ、氏名と生年月日の組み合わせ	氏名又は氏名の振り仮名と住所の組み合わせ、氏名又は氏名の振り仮名と生年月日の組み合わせ	事後	法改正に伴う修正
	Ⅲ特定個人情報ファイルの取り扱いプロセスにおけるリスク対策(2) 5. 特定個人情報の提供・移転 リスク1 特定個人情報の提供・移転の記録 具体的な方法	4情報	5情報	事後	法改正に伴う修正
	Ⅲ特定個人情報ファイルの取り扱いプロセスにおけるリスク対策(3) 2. 特定個人情報の入手 リスク1 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	氏名と住所の組み合わせ、氏名と生年月日の組み合わせ	氏名又は氏名の振り仮名と住所の組み合わせ、氏名又は氏名の振り仮名と生年月日の組み合わせ	事後	法改正に伴う修正
	Ⅲ特定個人情報ファイルの取り扱いプロセスにおけるリスク対策(3) 5. 特定個人情報の提供・移転 リスク1 特定個人情報の提供・移転の記録 具体的な方法	4情報等	5情報等	事後	法改正に伴う修正
	Ⅳその他リスク対策 1. 監査 ②監査 具体的な内容	―	＜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。	事後	

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
	Ⅳその他リスク対策 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。	事後	
	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 ④個人情報ファイル簿の公表 個人情報ファイル名	住民基本台帳システム	住民記録システム	事後	
	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 ④個人情報ファイル簿の公表 公表場所	市役所東館3階　市政情報コーナー	富山市ホームページ https://www.city.toyama.lg.jp/shisei/jyohokokai/1010947/1012727.html	事後	
	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 ②対応方法	－	・規定に定められた担当部署に速やかに連絡し、協議のうえ対応する	事後	
	Ⅵ評価実施手続 1．基礎項目評価 ①実施日	令和7年2月1日	令和8年6月10日	事後	