

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
	住民基本台帳に関する事務 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

山形市は、住民基本台帳に関する事務における特定個人情報ファイルの取扱いにあたり、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危険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宣言する。

特記事項	なし
------	----

評価実施機関名

山形市長

個人情報保護委員会 承認日【行政機関等のみ】

公表日

項目一覧

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

I 基本情報

1. 特定個人情報ファイルを取り扱う事務

①事務の名称	住民基本台帳に関する事務
②事務の内容 ※	当市は、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、当市の住民に関する正確な記録が整備されていなければならない。 住民基本台帳法（以下「住基法」という。）に基づき、作成されるものであり、当市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行うものであり、当市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。）を都道府県と共同で構築している。 当市は、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成し、住民基本台帳を作成 ②転入届、転居届、転出届、世帯変更届等の届出又は職権に基づく住民票の記載、消除又は記載の修正 ③住民基本台帳の正確な記録を確保するための措置 ④転入届に基づき住民票の記載をした際の転出元市町村に対する通知 ⑤本人又は同一の世帯に属する者の請求による住民票の写し等の交付 ⑥住民票の記載事項に変更があった際の都道府県知事に対する通知 ⑦地方公共団体情報システム機構（以下「機構」という。）への本人確認情報の照会 ⑧住民からの請求に基づく住民票コードの変更及び個人番号の変更 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中間サーバーへの住民票関係情報の副本の登録 ⑫転出届、及び転入予定、転居予定の連絡のサービス検索・電子申請機能での受領 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に規定する個人番号、個人番号カード、特定個人情報の提供等に関する命令（平成26年11月20日号外総務省令第85号）（以下、「個人番号、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。 申請管理システムについては以下のとおり取り扱う。 ①窓口や郵送での書類の受付により基幹システムへ入力 ②「サービス検索・電子申請機能」により申請された電子申請データを「申請管理システム」により基幹システムに転記入力
③対象人数	[10万人以上30万人未満] <選択肢> 1) 1,000人未満 2) 1,000人以上1万人未満 3) 1万人以上10万人未満 4) 10万人以上30万人未満 5) 30万人以上

2. 特定個人情報ファイルを取り扱う事務において使用するシステム	
システム1	
①システムの名称	住民記録システム(既存住民基本台帳システム)
②システムの機能	1. 住民票の検索機能 4情報(氏名、住所、性別、生年月日)の組み合わせによる当市が生成した番号(以下、「宛名番号」という。)、世帯を単位とする世帯番号、住民票コード、個人番号を用いて検索照会する機能 2. 住民票の記載、削除、変更機能 転入届、出生届、在留資格取得、職権等による新規住民票の作製、転出、死亡、帰化、職権等による住民票の抹消、転居届、世帯変更、転出取消、婚姻届等による住民票の修正機能 3. 住民基本台帳の更新処理機能 住民票の異動情報を最新の状態に一括更新し、情報を保存する機能 4. 転入情報通知機能 住基ネットを通じ転出元市町村及び本籍地市町村に新住所情報を通知する機能 5. 帳票発行機能 住民票の写し、転出証明書、住民票コード通知書等の各種帳票を発行する機能 6. 住基ネットとの情報連携機能 県及び機構に住民異動による本人確認情報が変更された情報を報告通知する機能 7. 住民基本台帳の統計機能 住民異動集計、法定人口統計を行う機能 8. 戸籍システムへの連携 戸籍の附票へ住民異動情報を通知する機能 9. 法務省通知の連携機能 外国人住民異動情報の通知を取り込む機能及び記載、削除、変更等の通知を作成する機能 10. 住民票関係情報の提供 情報提供ネットワークシステムを通じ法令等に基づく住民票関係情報の提供機能 11. 個人番号カード及び住民基本台帳カードの状況確認 個人番号カード及び住民基本台帳カードの発行状況等を確認する機能 12. 個別事項情報の管理 住民票個別事項項目となる、国民健康保険、国民年金、介護保険及び後期高齢者医療の資格情報、児童手当の支給の関する情報、選挙人名簿への登録情報を連携する機能 13. 操作者利用権限による管理機能 特定個人情報の保有に対するセキュリティ(アクセスログ対応、情報保守対応)の機能
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 国民健康保険システム、国民年金システム、介護保険システム、後期高齢者医療システム、福祉手当システム(児童手当、児童扶養手当、特別児童扶養手当、国手当等)、福祉医療システム(こども医療、重度心身者障害者医療、親子健やか医療等)、保育システム、印鑑登録システム、母子健康情報システム、成人健康情報システム、住基ネットCSコネクタ(令和5年12月まで)、滞納整理システム、学齢簿システム、法務省連携システム、戸籍システム、サービス検索・電子申請機能 [○] その他 ()

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、都道府県サーバー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 : 全国サーバー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ー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ー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、都道府県サーバー及び全国サーバーに対し、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(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 [] 住民基本台帳ネットワークシステム [] 宛名システム等 [] その他 (	[] 庁内連携システム [○] 既存住民基本台帳システム [] 税務システム)

システム3

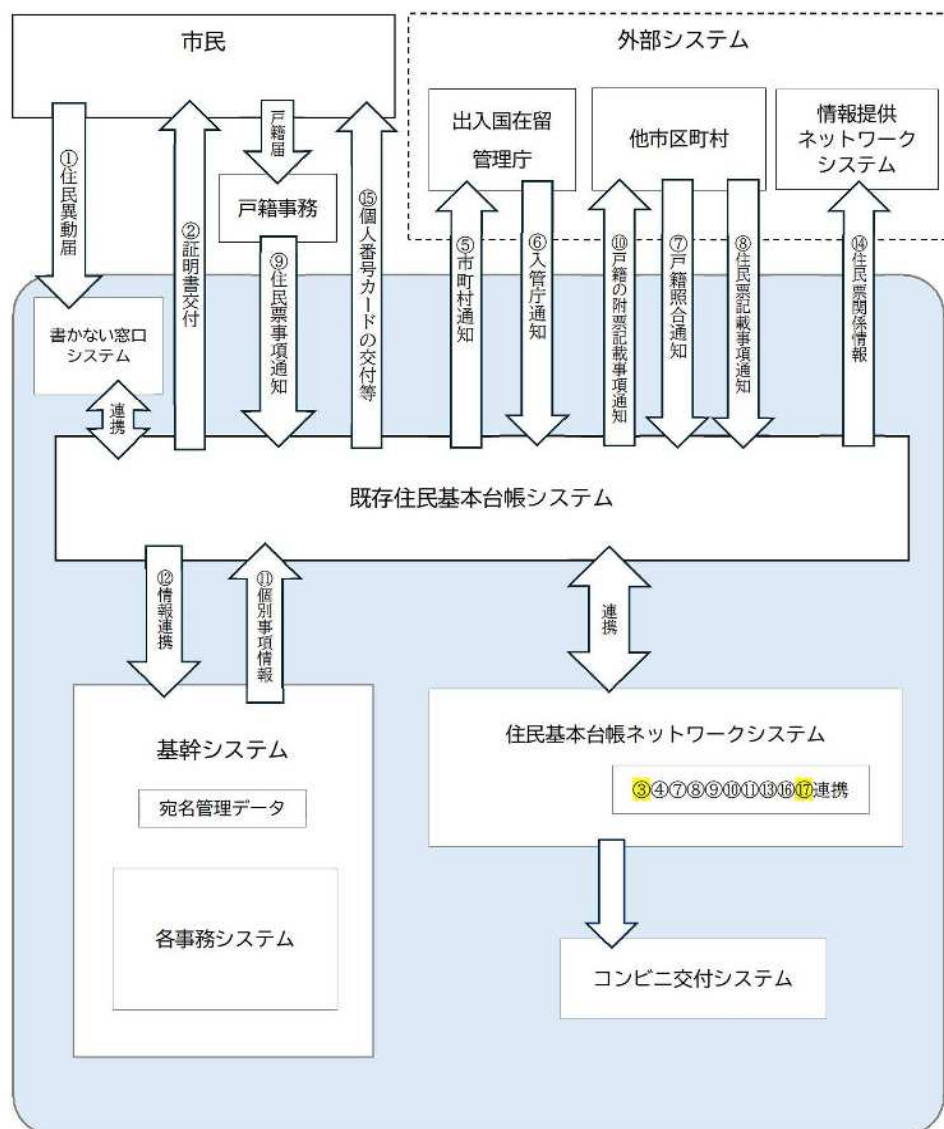
①システムの名称	庁内連携システム	
②システムの機能	庁内の各システム間のデータの連携	
③他のシステムとの接続	☐ 情報提供ネットワークシステム ☐ 住民基本台帳ネットワークシステム ☒ 宛名システム等 ☒ その他（各事務システム	☐ 庁内連携システム ☒ 既存住民基本台帳システム ☐ 税務システム

システム4	
①システムの名称	統合宛名システム
②システムの機能	1. 宛名番号付番機能 : 団体内統合宛名番号(以下「統合宛名番号」という。)が未登録の個人について、新規に統合宛名番号を付番する。各事務システムからの統合宛名番号要求に対し、統合宛名番号を付番し、各事務システム及び中間サーバーに対し返却する。 2. 宛名情報等管理機能 : 統合宛名システムにおいて宛名情報を統合宛名番号、個人番号と紐付けて保存し、管理する。 3. 中間サーバー連携機能 : 中間サーバー、又は中間サーバー端末からの要求に基づき、統合宛名番号に紐づく宛名情報等を通知する。 4. 各事務システム連携機能 : 各事務システムからの要求に基づき、個人番号、又は統合宛名番号に紐づく宛名情報を通知する。
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「統合宛名番号」とを紐付け、その情報を保管・管理する。 2. 情報照会機能 : 情報提供ネットワークシステムを介して、特定個人情報(連携対象)の情報照会及び情報提供受領(照会した情報の受領)を行う。 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及び当該特定個人情報(連携対象)の提供を行う。 4. 各事務システム接続機能 : 中間サーバーと各事務システム、統合宛名システム及び既存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。 5. 情報提供等記録管理機能 : 特定個人情報(連携対象)の照会、又は提供があった旨の情報提供等記録を生成し、管理する。 6. 情報提供データベース管理機能 : 特定個人情報(連携対象)を副本として、保持・管理する。 7. データ送受信機能 : 中間サーバーと情報提供ネットワークシステム(インターフェイスシステム)との間で情報照会、情報提供、符号取得のための情報等について連携する。 8. セキュリティ管理機能 : セキュリティを管理する。 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と職員に付与された権限に基づいた各種機能や特定個人情報(連携対象)へのアクセス制御を行う。 10. システム管理機能 : バッチ処理の状況管理、業務統計情報の集計、稼動状態の通知、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) 住民票情報ファイル (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	当市では、以下の3ファイルを下記に記載のと通りの必要性から取り扱う。 (1) 住民基本台帳ファイル ① 住基法に定める住民基本台帳の整備、正確な記録及び記録の管理等を行うため。 ② 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を行うため。 (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項及び個人番号カード省令第7条)。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、個人番号カード省令第23条の2(個人番号通知書及び個人番号カードに関し機構が処理する事務)に基づいて機構が行うこととされていることから、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. 番号法 ・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) ・第18条(個人番号カードの利用) 2. 住基法 ・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9(国の機関等への本人確認情報の提供) ・第30条の10(通知都道府県の区域内の市町村の執行機関への本人確認情報の提供) ・第30条の12(通知都道府県以外の都道府県の区域内の市町村の執行機関への本人確認情報の提供)

6. 情報提供ネットワークシステムによる情報連携 ※	
①実施の有無	[実施する] <選択肢> 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	・番号法第19条第8号(特定個人情報の提供の制限)に基づく主務省令第2条の表 (同表における情報提供の根拠) ：第三欄(情報提供者)が「市町村長」の項のうち、第四欄(特定個人情報)に「住民票関係情報」が含まれる項 第1項、2項、3項、5項、7項、11項、13項、15項、20項、28項、37項、39項、48項、53項、57項、58項、59項、63項、65項、66項、69項、73項、75項、76項、81項、83項、84項、86項、87項、91項、92項、96項、106項、108項、110項、112項、115項、118項、124項、129項、130項、132項、136項、137項、138項、141項、142項、144項、149項、150項、151項、152項、155項、156項、158項、160項、163項、164項、165項、166項 ：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別表第二の主務省令で定める事務及び情報を定める命令(平成26年12月12日号外内閣府、総務省令第7号) 第1条、2条、3条、4条、6条、7条、8条、10条、12条、13条、14条、16条、20条、22条、22条の3、22条の4、23条、24条、24条の2、24条の3、25条、26条の3、27条、28条、31条、31条の2、31条の3、32条、33条、37条、38条、39条、40条、41条、43条、43条の3、43条の4、44条の3、44条の5、45条、47条、48条、49条、49条の2、50条、51条、53条、54条、55条、56条、57条、58条、59条、59条の2の3、59条の3
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



※黄色染めは特定個人情報

(備考)

①住民情報の管理

住民異動届を受け付けて内容を審査し、住民票の記載、修正、または削除の処理を行う。(住基法第21条)

②証明書の交付

住民からの申請に応じて住民票の写しなどを交付するとともに、転出者に対しては転出証明書を発行する。(住基法第12条、住基法施行令第23条・第24条)

③住基ネットへの本人確認情報通知

住民票の記載事項に変更があった際などの本人確認情報を住民基本台帳ネットワークシステムへ速やかに通知する。(住基法第30条の6)

④ネットワークを活用した転出入処理

転入先の自治体からの請求に応じて転出証明書情報を住基ネット経由で通知する一方、他市町村からの同情報を受領した場合はマイナンバーカード等を利用した特例転入処理を進める。(住基法第24条の2第2項・第5項)

⑤外国人住民の動向に関する通知

外国人住民の住民票の作成、変更、削除を行った際、その内容を法務大臣へ通知する。(出入国管理及び難民認定法第61条の8の2等)

⑥入管庁からの通知に基づく住民票の整理

出入国在留管理庁から受領した通知内容に基づき、外国人住民の住民票の修正や削除を行う。(住基法第30条の50)

⑦戸籍附票と住民票の不一致に関する照会・通知

戸籍の附票記載事項通知の内容が実際の戸籍の記載と食い違っている場合、該当者の住所地へその旨を通知する。(住基法第19条第2項)

⑧他市町村からの転入に伴う旧住所地への通知

他の市区町村からの転入者に伴って住民票を記載した際、前住所地の自治体へ通知を行う。(住基法第9条第1項・第3項)

⑨戸籍変更に伴う住民票側への通知連携

戸籍の記載や記録をした際、それに伴う住民票に関する事項の通知を行う。(住基法第9条第2項)

⑩住民票記載に伴う戸籍附票への通知連携

住民票の記載や変更などを行った際、戸籍の附票に関する事項を通知する。(住基法第19条第1項・第4項)

⑪個別記載事項の住民票への反映

住民票に載せるべき法定の個別記載事項情報を正しく受領し、住民票に記載する。(住基法第7条)

⑫他業務への住民情報の連携

住民に関する行政事務全般の基礎とするため、住民票データを税務や福祉などの他業務へ適切に移管する。(住基法第1条)

⑬広域住民票の交付対応とデータ通知

他市区町村からの広域住民票の交付要求を受け付けた場合、請求された広域住民票情報を交付地に通知する。(住基法第12条の4)

⑭情報提供ネットワークシステムを通じた情報連携

行政機関間での情報連携を行うため、情報提供ネットワークシステムに対して住民票関連の必要情報を提供する。(番号法第22条)

⑮マイナンバーカードの交付等の手続き

住民からの申請受付からカードの作成・受渡しに至るまで、個人番号カードに関する一連の交付事務を行う。(番号法第17条)

⑯住民票コードから個人番号への指定手続き

住民票に住民票コードを記載した場合は、住基ネットを経由して地方公共団体情報システム機構(J-LIS)から個人番号となるべき番号を受領し、速やかに本人の個人番号として指定する。(番号法第7条・第8条)

⑰個人番号通知書の送付先情報の送信

住民基本台帳ネットワークシステムを通じ、地方公共団体情報システム機構に対して個人番号通知書の送付先に関するデータを送信する。(番号法第7条・第8条)

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) 住民票情報ファイル

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) ※番号法施行後は住民基本台帳に記載されていた者で、転出等の事由等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	住基法第7条第1項第8の2号(住民票の記載事項) 法令に基づき住民基本台帳を作成し、常に最新の状態を保つために必要に応じて記載、消除、修正すべきとされている。また、住民票は本人の居住について公証する唯一の証明書である。	
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 ()	
その妥当性	・個人番号・4情報・その他住民票関係情報・業務関係情報: 住基法第7条各号で規定する項目であり、住民票の記載項目として保有しなければならない。 ・その他識別情報: 当市において、個人を一意に識別するための独自の番号(宛名番号)を保有する。	
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30日	
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 ()	
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 ()	
③入手の時期・頻度		・住民記録の異動届があったとき。 ・戸籍の届出又は他市町村から通知により、住民記録記載事項に変動があったとき。 ・その他本人からの申出調査による職権記載・他市町村からの記載内容通知等があったとき。 ・個人番号の変更要求が発生したとき。	
④入手に係る妥当性		・個人番号の新規取得については、住基ネットより取得する。 ※番号法第8条 ・各異動届を受理するに当たってはまずは本人から必要情報を入手する必要がある。 ※個人番号を移記する場合は、他の住民基本台帳事務と同様に本人確認の実施。 ・他の情報については、他市町村転出証明書・庁内連携システムを通じ、必要となる情報の正確性の確認を行う。	
⑤本人への明示		・「個人番号とすべき番号」の入手については、番号法第8条にて明示されている。 ・「個人番号」の移記については、番号整備法第16条(住基法第7条第8の2号)にて記載事項である旨が明示されている。 ・番号法第7条第1項により、本人に対して通知カードを用いて個人番号を通知する旨が明示されている。 ・その他ホームページ等で当該業務に関する説明を掲載している。 ・基幹システムから連携された住民のデータを参照し、手続きガイダンスを行う際、受付部署の事務のみではなく、正確な案内を行うため、他部署の業務についても資格保有の有無等を確認するため住民のデータを参照する。その際は、窓口における掲示や口頭により本人に明示する。また、窓口DXSaaSを通じて作成した申請データについて、業務所管部署以外で作成・受付された場合は、受付部署及び業務所管部署にデータが共有されるため、その旨も口頭により本人に明示する。	
⑥使用目的 ※		住基法各章における条文に基づき、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。また、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正確に管理する。	
		変更の妥当性	－
⑦使用の主体		使用部署 ※	市民生活部市民課、国民健康保険課、健康医療部健康増進課、母子保健課、財政部市民税課、資産税課、納税課、福祉推進部介護保険課、生活支援課、障がい福祉課、こども未来部こども未来課、こども家庭支援課、まちづくり推進部管理住宅課
		使用者数	[10人以上50人未満] <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上

⑧使用方法 ※		1. 住民票の記載等 ・出生または国外からの転入届により、新規に個人番号を指定する場合は、機構から「個人番号とすべき番号」を入手して、指定し、個人番号を含む住民に関する情報を当市住民票に記載する。 ・転入届等により、個人番号を引き継ぐ場合は、届出で提示された個人番号と転出証明書に記載された個人番号との照合、または、住民記録システム、住基ネットを利用して個人番号等で検索し、個人番号を表示して真正性を確認のうえ、住民票を記載する。 ・住民からの申出や他市町村からの法定通知を受理した場合は、前項と同様に個人番号の真正性を確認のうえ、住民票を修正する。 ・転出届または死亡等により、住民票を抹消する場合は、届出で提示された個人番号と照合、または、住民記録システム、住基ネットを利用して個人番号等で検索し、個人番号を表示して真正性を確認のうえ、住民票を削除する。 2. 住民票情報の通知等 ・転入届等により、住民票の記載を行ったときは、転出証明書情報をもとに、最終住民登録市町村（未届市町村を含む。）に対し、個人番号を含む住民票情報を住基ネットを通じて送付する。 ・当市住民票の記載に変動があった場合は、都道府県知事に対して、個人番号を含む本人確認情報を住基ネットを通じて送付する。 ・個人番号カード等を利用した転入の特例の届出があった場合は、届出で提示された個人番号と照合、または、住民記録システム、住基ネットを利用して個人番号等で検索し、個人番号を表示して真正性を確認のうえ、転出証明書情報を作成する。 3. 住民票の発行 ・住基法第12条、同法12条の2による住民票の交付請求の場合、住民票への個人番号の記載を求められた際には、個人番号カード等の提示を求め、本人確認をし、申請の内容に必要性が正当と認められるときは、個人番号が記載された住民票を交付する。 ・住基法第12条の4による広域交付住民票の交付請求の場合、個人番号カード等の提示を求め、本人確認をし、住基ネットを利用して請求者の住民登録市町村へ住民票情報を請求し、当該市町村より承認されたときは、住民票を交付する。 4. 住民票関係情報の提供 ・情報提供ネットワークシステムに住民票関係情報（世帯主、世帯主との続柄、世帯番号）を提供する。 5. 「サービス検索・電子申請機能」を通じて申請された電子申請データの受理、審査等
	情報の突合 ※	・住民票情報ファイルに個人番号を新たに生成する場合は、住民票コードにより突合を行う。 ・住民票情報ファイルを更新する際は、個人番号等で検索し、履歴情報との突合を行う。履歴が確認できた場合は「当市において個人を一意に識別する番号（宛名番号）」も引き継ぐこととする。 ・住民票情報ファイルの検索は、個人番号、住民票コード、その他識別番号（内部番号）及び、4情報の組み合わせにより突合を行う。 ・申請者を確認するために既存住基システムを通じて取り込んだ番号紐付情報と突合する。
	情報の統計分析 ※	地区別・年齢別世帯・人口などの統計を行うが、特定の個人を判別しうような情報の統計や情報の分析は行わない。
	権利利益に影響を与え得る決定 ※	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 (3) 件)	
委託事項1	市民課オペレーター等業務	
①委託内容	・証明書請求等の受付審査から証明書作製、確認交付業務 ・住民異動に伴う住民票情報の入力、確認業務	
②取扱いを委託する特定個人情報ファイルの範囲	特定個人情報ファイルの一部 <選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部	
対象となる本人の数	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 ※	「Ⅱ 2. ③対象となる本人の範囲」と同様。	
その妥当性	民間の保有する高度な知識・技術を活用することにより、コストの低減及び効率的な業務を行うことが可能となる。当該委託業務で扱う情報の中に特定個人情報が含まれており、それらを分離して業務委託することは、非合理的である。	
③委託先における取扱者数	10人以上50人未満 <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上	
④委託先への特定個人情報ファイルの提供方法	○] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [] 紙 [] その他 ()	
⑤委託先名の確認方法	山形市情報公開条例に基づく情報公開請求	
⑥委託先名	株式会社アイヴィジット	
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	住民記録システムの等の保守運用業務	
①委託内容	住民記録システムの保守運用業務を行うに当たり、必要な範囲内での特定個人情報ファイルの取り扱いを委託する。	
②取扱いを委託する特定個人情報ファイルの範囲	特定個人情報ファイルの一部 <選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部	
対象となる本人の数	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 ※	「Ⅱ 2. ③対象となる本人の範囲」と同様。	
その妥当性	住民記録システムの運用保守を実施するには、特定個人情報ファイルを取扱う必要がある。	

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	再委託は、原則として禁止しているが、事前に再委託理由、事業者名、取扱情報、安全・信頼性の確保、管理監督の方法等を記載した書面を提出させ、再委託に必要性や業務内容等を確認したうえで承認する。 なお、再委託先にも受託元と同等の守秘義務等が課される。
	⑨再委託事項	コンビニ交付システムの運用保守(監視業務、事故対応業務等)
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 (60) 件 [○] 移転を行っている (18) 件 [] 行っていない	
提供先1	提供先については、別紙提供先一覧を参照のこと。	
①法令上の根拠	別紙提供先一覧に記載	
②提供先における用途	別紙提供先一覧に記載	
③提供する情報	別紙提供先一覧に記載	
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	別紙提供先一覧に記載	
⑥提供方法	[○] 情報提供ネットワークシステム [] 電子メール [] フラッシュメモリ [] その他 ([] 専用線 [] 電子記録媒体(フラッシュメモリを除く。) [] 紙)	
⑦時期・頻度	照会を受けた都度	
提供先2～5		
提供先6～10		
提供先11～15		
提供先16～20		
移転先1	福祉推進部障がい福祉課	
①法令上の根拠	番号法第9条第1項 別表9の項 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別表の主務省令で定める事務を定める命令(以下、「命令」という。)第8条	
②移転先における用途	児童福祉法による障害児通所給付費、特例障害児通所給付費、高額障害児通所給付費、肢体不自由児通所医療費、障害児相談支援給付費若しくは特例障害児相談支援給付費の支給、障害福祉サービスの提供、保育所における保育の実施若しくは措置又は費用の徴収に関する事務であって主務省令で定めるもの	
③移転する情報	個人番号、氏名、住所、生年月日、性別、世帯主氏名及び世帯主との続柄等の住民票情報	

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		
⑥移転方法	[] 庁内連携システム [] 電子メール [] フラッシュメモリ [○] その他 (オンライン照会)	[] 専用線 [] 電子記録媒体(フラッシュメモリを除く。) [] 紙
⑦時期・頻度	照会を受けた都度	
移転先2～5		
移転先2	こども未来部こども未来課、保育育成課	
①法令上の根拠	番号法第9条第1項 別表9の項 命令第8条	
②移転先における用途	児童福祉法による障害児通所給付費、特例障害児通所給付費、高額障害児通所給付費、肢体不自由児通所医療費、障害児相談支援給付費若しくは特例障害児相談支援給付費の支給、障害福祉サービスの提供、保育所における保育の実施若しくは措置又は費用の徴収に関する事務であって主務省令で定めるもの	
③移転する情報	個人番号、氏名、住所、生年月日、性別、世帯主氏名及び世帯主との続柄等の住民票情報(予定)	
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。(予定)	
⑥移転方法	[○] 庁内連携システム [] 電子メール [] フラッシュメモリ [] その他 (	[] 専用線 [] 電子記録媒体(フラッシュメモリを除く。) [] 紙
⑦時期・頻度	照会を受けた都度(予定)	
移転先3	健康医療部健康増進課、母子保健課	
①法令上の根拠	番号法第9条第1項 別表14の項 命令第10条	
②移転先における用途	予防接種法(昭和二十三年法律第六十八号)による予防接種の実施、給付の支給又は実費の徴収に関する事務であって主務省令で定めるもの	
③移転する情報	個人番号、氏名、住所、生年月日、性別、世帯主氏名及び世帯主との続柄等の住民票情報	
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 （オンライン照会）
⑦時期・頻度	照会を受けた都度
移転先4	福祉推進部障がい福祉課
①法令上の根拠	番号法第9条第1項 別表20の項 命令第11条
②移転先における用途	身体障害者福祉法(昭和二十四年法律第二百八十三号)による身体障害者手帳の交付に関する事務であって主務省令で定めるもの
③移転する情報	個人番号、氏名、住所、生年月日、性別、世帯主氏名及び世帯主との続柄等の住民票情報
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 （オンライン照会）
⑦時期・頻度	照会を受けた都度
移転先5	福祉推進部生活支援課
①法令上の根拠	番号法第9条第1項 別表23の項 命令第15条
②移転先における用途	生活保護法による保護の決定及び実施、就労自立給付金若しくは進学・就職準備給付金の支給、被保護者健康管理支援事業の実施、保護に要する費用の返還又は徴収金の徴収に関する事務であって主務省令で定めるもの
③移転する情報	個人番号、氏名、住所、生年月日、性別、世帯主氏名及び世帯主との続柄等の住民票情報
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 （オンライン照会）
⑦時期・頻度	照会を受けた都度

移転先6～10	
移転先6	財政部市民税課、資産税課、納税課、市民生活部国民健康保険課
①法令上の根拠	番号法第9条第1項 別表24の項 命令第16条
②移転先における用途	地方税法その他の地方税に関する法律及びこれらの法律に基づく条例による地方税の賦課徴収又は地方税に関する調査(犯則事件の調査を含む。)に関する事務であって主務省令で定めるもの
③移転する情報	個人番号、氏名、住所、生年月日、性別、世帯主氏名及び世帯主との続柄等の住民票情報
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 ☐ 電子メール ☐ フラッシュメモリ ☐ その他 (☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙 ☐)
⑦時期・頻度	照会を受けた都度
移転先7	まちづくり政策部住宅政策課
①法令上の根拠	番号法第9条第1項 別表27の項 命令第18条
②移転先における用途	個人番号、氏名、住所、生年月日、性別、世帯主氏名及び世帯主との続柄等の住民票情報
③移転する情報	個人番号、氏名、住所、生年月日、性別、世帯主氏名及び世帯主との続柄等の住民票情報
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 ☐ 電子メール ☐ フラッシュメモリ ☒ その他 (オンライン照会 ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙 ☐)
⑦時期・頻度	照会を受けた都度
移転先8	市民生活部国民健康保険課
①法令上の根拠	番号法第9条第1項 別表44の項 命令第24条
②移転先における用途	国民健康保険法(昭和三十三年法律第百九十二号)による保険給付の支給又は保険料の徴収に関する事務であって主務省令で定めるもの
③移転する情報	個人番号、氏名、住所、生年月日、性別、世帯主氏名及び世帯主との続柄等の住民票情報
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 ()
⑦時期・頻度	照会を受けた都度
移転先9	まちづくり政策部住宅政策課
①法令上の根拠	番号法第9条第1項 別表52の項 命令第26条
②移転先における用途	住宅地区改良法による改良住宅(同法第二条第六項に規定する改良住宅をいう。以下同じ。)の管理若しくは家賃若しくは敷金の決定若しくは変更又は収入超過者に対する措置に関する事務であって主務省令で定めるもの
③移転する情報	個人番号、氏名、住所、生年月日、性別、世帯主氏名及び世帯主との続柄等の住民票情報
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 (オンライン照会)
⑦時期・頻度	照会を受けた都度
移転先10	こども未来部こども家庭支援課
①法令上の根拠	番号法第9条第1項 別表56の項 命令第29条
②移転先における用途	児童扶養手当法(昭和三十六年法律第二百三十八号)による児童扶養手当の支給に関する事務であって主務省令で定めるもの
③移転する情報	個人番号、氏名、住所、生年月日、性別、世帯主氏名及び世帯主との続柄等の住民票情報
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 ()
⑦時期・頻度	照会を受けた都度

移転先11～15	
移転先11	福祉推進部障がい福祉課
①法令上の根拠	番号法第9条第1項 別表67の項 命令第38条
②移転先における用途	特別児童扶養手当等の支給に関する法律(昭和三十九年法律第百三十四号)による特別児童扶養手当の支給に関する事務であって主務省令で定めるもの
③移転する情報	個人番号、氏名、住所、生年月日、性別、世帯主氏名及び世帯主との続柄等の住民票情報
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 ☐ 電子メール ☐ フラッシュメモリ ☐ その他 (☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙 ☐)
⑦時期・頻度	照会を受けた都度
移転先12	福祉推進部障がい福祉課
①法令上の根拠	番号法第9条第1項 別表67の項 命令第38条
②移転先における用途	特別児童扶養手当等の支給に関する法律による障害児福祉手当若しくは特別障害者手当又は国民年金法等の一部を改正する法律(昭和六十年法律第三十四号。以下「昭和六十年法律第三十四号」という。)附則第九十七条第一項の福祉手当の支給に関する事務であって主務省令で定めるもの
③移転する情報	個人番号、氏名、住所、生年月日、性別、世帯主氏名及び世帯主との続柄等の住民票情報
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 ☐ 電子メール ☐ フラッシュメモリ ☐ その他 (☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙 ☐)
⑦時期・頻度	照会を受けた都度
移転先13	こども未来部こども家庭支援課
①法令上の根拠	番号法第9条第1項 別表81の項 命令第44条
②移転先における用途	児童手当法による児童手当又は特例給付(同法附則第二条第一項に規定する給付をいう。以下同じ。)の支給に関する事務であって主務省令で定めるもの
③移転する情報	個人番号、氏名、住所、生年月日、性別、世帯主氏名及び世帯主との続柄等の住民票情報
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 ()
⑦時期・頻度	照会を受けた都度
移転先14	市民生活部国民健康保険課
①法令上の根拠	番号法第9条第1項 別表85の項 命令第46条
②移転先における用途	高齢者の医療の確保に関する法律による後期高齢者医療給付の支給又は保険料の徴収に関する事務であって主務省令で定めるもの
③移転する情報	個人番号、氏名、住所、生年月日、性別、世帯主氏名及び世帯主との続柄等の住民票情報
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 ()
⑦時期・頻度	照会を受けた都度
移転先15	福祉推進部介護保険課
①法令上の根拠	番号法第9条第1項 別表100の項 命令第50条
②移転先における用途	介護保険法(平成九年法律第二百二十三号)による保険給付の支給、地域支援事業の実施又は保険料の徴収に関する事務であって主務省令で定めるもの
③移転する情報	個人番号、氏名、住所、生年月日、性別、世帯主氏名及び世帯主との続柄等の住民票情報
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 ()
⑦時期・頻度	照会を受けた都度

移転先16～20	
移転先16	健康医療部健康増進課
①法令上の根拠	番号法第9条第1項 別表105の項 令第52条
②移転先における用途	感染症の予防及び感染症の患者に対する医療に関する法律(平成十年法律第百十四号)による入院の勧告若しくは措置、費用の負担又は療養費の支給に関する事務であって主務省令で定めるもの
③移転する情報	個人番号、氏名、住所、生年月日、性別、世帯主氏名及び世帯主との続柄等の住民票情報
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 ☐ 電子メール ☐ フラッシュメモリ ☒ その他 (オンライン照会 ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙)
⑦時期・頻度	照会を受けた都度
移転先17	健康医療部健康増進課
①法令上の根拠	番号法第9条第1項 別表111の項 令第54条
②移転先における用途	健康増進法(平成十四年法律第百三号)による健康増進事業の実施に関する事務であって主務省令で定めるもの
③移転する情報	個人番号、氏名、住所、生年月日、性別、世帯主氏名及び世帯主との続柄等の住民票情報
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 ☐ 電子メール ☐ フラッシュメモリ ☒ その他 (オンライン照会 ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙)
⑦時期・頻度	照会を受けた都度
移転先18	福祉推進部障がい福祉課
①法令上の根拠	番号法第9条第1項 別表117の項 令第60条
②移転先における用途	障害者の日常生活及び社会生活を総合的に支援するための法律(平成十七年法律第百二十三号)による自立支援給付の支給又は地域生活支援事業の実施に関する事務であって主務省令で定めるもの
③移転する情報	個人番号、氏名、住所、生年月日、性別、世帯主氏名及び世帯主との続柄等の住民票情報
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 (オンライン照会)					
⑦時期・頻度		照会を受けた都度					
6. 特定個人情報の保管・消去							
①保管場所 ※		＜山形市における措置＞ 当市では、住民票を磁気ディスクで調製しており、高度なセキュリティを用いたサーバー内にデータとして、入退室管理を行っているセキュリティロックの設置した部屋に保管する。 サーバへのアクセスはID／パスワード認証が必要となる。 住民記録システムで保持している特定個人情報に該当する住民票情報のうち、削除された住民票については住民基本台帳法施行令34条の規定により、削除された日から150年間保存することは定義されているが、削除の定義の規定はないため、情報セキュリティポリシーにより、適切な削除処理を行う。 LGWAN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、紙に打出後、速やかに完全消去する。 外部記憶媒体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。 ＜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が適切に実施されているほか、次を満たしている。 ・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が保有・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ベース上に保存される。 ＜その他＞ 個人番号付電子申請データは連携サーバを経由するのみで保存されない。 ＜ガバメントクラウドにおける措置＞ ・保管場所について 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。 ・消去方法について 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等に当た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。					
②保管期間	期間	＜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	＜山形市における措置＞ ・山形市情報セキュリティポリシーにより、適切な削除処理を行う。 ・LGWAN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、紙に打出後、速やかに完全消去する。 ・外部記憶媒体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。 ・内部で定められた保存期間を経過した申請書等紙媒体は、内部の定めに従い廃棄処分する。 ＜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事業者及びクラウドサービス事業者が特定個人情報を消去することはない。 ②クラウドサービス事業者が保有・管理する環境において、障害やメンテナンス等によりディスクやハード等を交換する際は、クラウドサービス事業者において、政府情報システムのためのセキュリティ評価制度（ISMAP）に準拠したデータの暗号化消去及び物理的破壊を行う。さらに、第三者の監査機関が定期的に発行するレポートにより、クラウドサービス事業者において、確実にデータの暗号化消去及び物理的破壊が行われていることを確認する。 ③中間サーバー・プラットフォームの移行の際は、地方公共団体情報システム機構及び中間サーバー・プラットフォームの事業者において、保存された情報が読み出しできないよう、データセンターに設置しているディスクやハード等を物理的破壊により完全に消去する。 ＜ガバメントクラウドにおける措置＞ ①特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報を消去することはない。 ②クラウド事業者がHDDやSSDなどの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等にしたがって確実にデータを消去する。 ③既存システムについては、地方公共団体が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。
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 ☐ システム用ファイル ☐ 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 ☐ 1万人未満 ☐ 1万人以上10万人未満 ☐ 10万人以上100万人未満 ☐ 100万人以上1,000万人未満 ☐ 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) ※番号法施行後は住民基本台帳に記載されていた者で、転出等の事由等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 ☐ 10項目未満 ☐ 10項目以上50項目未満 ☐ 50項目以上100項目未満 ☐ 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、住民票の記録等に係る本人確認情報(個人番号、4情報、住民票コード及びこれらの変更情報)を記録する必要があるため。
	全ての記録項目	別添2を参照。
⑤保有開始日	平成27年7月30日	
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する都度入手する。	
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		-	
⑦使用の主体	使用部署 ※	市民生活部市民課	
	使用者数	[10人以上50人未満] <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上	
⑧使用方法 ※		・住民票の記載事項の変更又は新規作成が生じた場合、住民記録システムから当該本人確認情報の更新情報を受領し(住民記録システム→当市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(当市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→当市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(当市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		住民基本台帳ネットワークシステム運用保守管理業務
①委託内容		住民基本台帳ネットワークシステム運用保守管理の委託
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	住民基本台帳ネットワークシステムの運用保守を実施するには、特定個人情報ファイル全体を取扱う必要がある。
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 (本市の管理するシステム内から特定個人情報ファイルを取り出すことはな) い。
⑤委託先名の確認方法		山形市情報公開条例に基づく情報公開請求
⑥委託先名		【令和5年12月まで】 山形市新情報システム包括型SI業務共同企業体 代表構成員: 東日本電信電話株式会社 ビジネス&オフィス営業推進本部 山形法人営業部 【令和6年1月から】 株式会社日立システムズ東北支社
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（ ）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、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 $\lt$選択肢$\gt$ 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 ☐ 電子メール ☐ フラッシュメモリ ☒ その他（住民基本台帳ネットワークシステム） ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙	
⑦時期・頻度	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	☐ $\lt$選択肢$\gt$ 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上	
⑤移転する情報の対象となる本人の範囲		
⑥移転方法	☐ 庁内連携システム ☐ 電子メール ☐ フラッシュメモリ ☐ その他（ ） ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙	
⑦時期・頻度		
移転先2～5		
移転先6～10		
移転先11～15		
移転先16～20		

6. 特定個人情報の保管・消去

①保管場所 ※		・セキュリティゲートにて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である。
②保管期間	期間	<選択肢> 1) 1年未満 2) 1年 3) 2年 4) 3年 5) 4年 6) 5年 7) 6年以上10年未満 8) 10年以上20年未満 9) 20年以上 10) 定められていない
	その妥当性	・住民票の記載の修正後の本人確認情報は、新たに記載の修正の通知を受けるまで保管する。 ・住民票の記載の修正前の本人確認情報(履歴情報)及び消除者の本人確認情報は、住民基本台帳法施行令第34条第2項(保存)に定める期間(150年間)保管する。
③消去方法		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

--	--

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) ※番号法施行後は住民基本台帳に記載されていた者で、転出等の事由等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	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、個人番号カードは個人番号を確認して交付することとされていることから、合わせて、交付申請書を個人番号通知書送付者全員に送付する必要がある。市は、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)に基づき、これらの事務の実施をJ-LIS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、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、個人番号カード省令第23条の2(個人番号通知書及び個人番号カードに関し機構が処理する事務)に基づき個人番号通知書及び交付申請書の印刷、送付並びに個人番号カードの発行を機構が行うために、個人番号カードの券面記載事項のほか、個人番号通知書及び交付申請書の送付先に係る情報を記録する必要がある。
全ての記録項目	別添2を参照。
⑤保有開始日	平成27年10月3日
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		個人番号通知書に係る送付先情報は、新たに個人番号の通知対象者が生じた都度入手する。	
④入手に係る妥当性		送付先情報の提供手段として住基ネットを用いるため、市町村CSにデータを格納する必要がある。また、提供手段として電子記録媒体を用いる場合には、暗号化の機能を備える市町村CSにおいて電子記録媒体を暗号化した後に提供する必要がある。	
⑤本人への明示		個人番号カード省令第23条の2(個人番号通知書及び個人番号カードに関し機構が処理する事務)	
⑥使用目的 ※		個人番号カード省令第23条の2(個人番号通知書及び個人番号カードに関し機構が処理する事務)に基づ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		-	
⑦使用の主体	使用部署 ※	市民生活部市民課	
	使用者数	10人以上50人未満] <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上	
⑧使用方法 ※		住民記録システム(既存住基システム)より個人番号の通知対象者の情報を抽出し、個人番号通知書及び交付申請書等の印刷及び送付に係る事務を個人番号カード省令第23条の2(個人番号通知書及び個人番号カードに関し機構が処理する事務)に基づいて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、J-LIS(全国サーバー)が保有する「J-LIS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		住民基本台帳ネットワークシステム運用保守管理業務
①委託内容		住民基本台帳ネットワークシステム運用保守管理の委託
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	システムの運用・保守作業を実施するため、特定個人情報ファイル全体を委託の対象にする必要がある。
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 (本市の管理するシステム内から特定個人情報ファイルを取り出すことはな) い。
⑤委託先名の確認方法		山形市情報公開条例に基づく情報公開請求
⑥委託先名		【令和5年12月まで】 山形市新情報システム包括型SI業務共同企業体 代表構成員: 東日本電信電話株式会社 ビジネス&オフィス営業推進本部 山形法人営業部 【令和6年1月から】 株式会社日立システムズ東北支社
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 () 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	個人番号カード省令第23条の2(個人番号通知書及び個人番号カードに関し機構が処理する事務)
②提供先における用途	市町村から個人番号カード省令第23条の2(個人番号通知書及び個人番号カードに関し機構が処理する事務)に基づき個人番号通知書及び交付申請書を印刷し、送付する。
③提供する情報	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、通知書及び交付申請書の送付先の情報
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」と同上。
⑥提供方法	[] 情報提供ネットワークシステム [] 電子メール [] フラッシュメモリ [☐] その他 (住基ネット) [] 専用線 [] 電子記録媒体(フラッシュメモリを除く。) [] 紙
⑦時期・頻度	個人番号通知書に係る送付先情報は、新たに個人番号の通知対象者が生じた都度提供する。
提供先2～5	
提供先6～10	
提供先11～15	
提供先16～20	
移転先1	
①法令上の根拠	
②移転先における用途	
③移転する情報	
④移転する情報の対象となる本人の数	[] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤移転する情報の対象となる本人の範囲	
⑥移転方法	[] 庁内連携システム [] 電子メール [] フラッシュメモリ [] その他 () [] 専用線 [] 電子記録媒体(フラッシュメモリを除く。) [] 紙
⑦時期・頻度	
移転先2～5	
移転先6～10	
移転先11～15	
移転先16～20	

6. 特定個人情報の保管・消去		
①保管場所 ※		・セキュリティゲートにて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である。
②保管期間	期間	[1年未満] <選択肢> 1) 1年未満 4) 3年 7) 6年以上10年未満 10) 定められていない 2) 1年 5) 4年 8) 10年以上20年未満 3) 2年 6) 5年 9) 20年以上
	その妥当性	送付先情報はJ-LIS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、速やかに消去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、J-LIS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		

(別添2) 特定個人情報ファイル記録項目

(1) 住民票情報ファイル

1. 宛名番号、2. 世帯番号、3. 個人番号、4. 住民票コード、5. 氏名、6. 生年月日、7. 性別、8. 現住所、9. 方書、10. 続柄、11. 世帯主氏名、12. 本籍地、13. 筆頭者氏名、14. 在留カード等番号、15. 第30条45規定区分、16. 在留資格、17. 在留期間等、18. 在留期間の満了日、19. 国籍・地域、20. 通称履歴、21. 住民となった日、22. 住所を定めた日、23. 住民でなくなった日、24. 前住所、25. 転出予定先住所、26. 転出確定住所、27. 選挙人名簿資格、28. 国民健康保険資格情報、29. 後期高齢者医療資格情報、30. 介護保険資格情報、31. 国民年金資格情報、32. 児童手当受給資格情報、33. 個人番号カード交付状況、34. 住民基本台帳カード交付状況、35. 異動事由、36. 異動年月日、37. 届出年月日、38. 処理年月日、39. 処理時刻、40. 処理ID、41. 端末ID、42. 職員番号

(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	
住民票情報ファイル	
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	各種異動の届出における届出人の本人確認を法に定める身分証明書等、本人確認書類の提示確認を厳格に実施し、異動前後の状況を住民記録システムで確認し、確認対象者以外の情報を入手しないよう、事務手順書等を作成し順守している。また、届出に関して本人または代理人による届出のみを受領する。 その他、個人情報の取扱いに関しては、当市セキュリティポリシーに準ずる。
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	・届出書に記載された情報以外は入力できない仕組みとなっている。 ・届出書の内容をシステムへ入力後、届出書の内容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、仕組みとして担保されている。
その他の措置の内容	－
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
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基法第27条の規定に基づき、書面にて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いる。 ・システムを利用する必要がある職員を特定し、パスワードの設定及び生体認証を実施する。 ・住基ネットから入手する場合は、住基ネットCSの認証・監査、証跡機能により特定の権限者以外は操作が行えず、また情報照会・提供の記録が保持される仕組みが確立されている。 ・個人番号は原則、住民票の写し、記載事項証明書以外では明示せず、住民票の写しへの記載も本人からの特別な請求がない限り、省略して出力する。
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 that 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）の提示等を受け、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で定める書類等）の提示がない場合には、住民基本台帳ネットワーク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	・特定個人情報の入力、削除及び訂正を行う際は、整合性を確保するために、作業を行なった者以外の者が確認する等、必ずダブルチェックを実施する。 ・住民基本台帳ネットワークに記録された本人確認情報と、定期的に整合性チェックを実施している。	
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	・届出書や申請書は、使用後に鍵付の保管庫や書庫に保管し、漏えいや紛失等を防止する。 ・既存住基システムは住基ネット以外とは外部接続できない仕組みである。 ・住基ネットでの通信は全て専用回線及び専用交換装置で構成されたネットワークを介して行い、また、接続しログインするごとに、意図した通信相手に接続されたことを認証する仕組みを採用している。	
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		
・住民記録システムへの情報入力は、ユーザーIDとパスワードにより認証を行い、IDに設定された権限のみ有効とすることをシステム上制御し、入力できる項目を限定することで、不適切な方法による情報の入手が行えないことを担保している。 ・住民がサービス検索・電子申請機能から個人番号付電子申請データを送信するためには、個人番号カード等の署名用電子証明書による電子署名を付すこととなり、のちに署名検証も行われるため、本人からの情報のみが送信される。 - サービス検索・電子申請機能の画面誘導において住民に何の手続きを探し電子申請を行いたいのか理解してもらいながら操作をしていただき、たどり着いた申請フォームが何のサービスにつながるものか明示することで、住民に過剰な負担をかけることなく電子申請を実施いただけるよう措置を講じている。 ・住民がサービス検索・電子申請機能から個人番号付電子申請データを送信するためには、個人番号カード等の署名用電子証明書による電子署名を付すこととなり、電子署名付与済の個人番号付電子申請データを受領した地方公共団体は署名検証(有効性確認、改ざん検知等)を実施することとなる。これにより、本人確認を実施する。 - サービス検索・電子申請機能と地方公共団体との間は、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。 ・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。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。申請管理システムから基幹システムまでは、外部との接続が制限された環境で利用している。		
3. 特定個人情報の使用		
リスク1: 目的を超えた紐付け、事務に必要な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	個人番号利用事務以外の所属課において住民記録システムを使用した照会では、利用者権限により、個人番号が表示されない機能を構築している。 住民記録システムの稼働するLANには、外部からの侵入を防止するファイアーウォールによる適切なアクセス制御を実施している。	
事務で使用するその他のシステムにおける措置の内容	・庁内の他のシステムからアクセスできないよう適切なアクセス制御を講じており、目的を超えた紐付けは行われないようにしている。	
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	・ユーザーIDによる識別とパスワードによる認証機能により、そのユーザーがシステム上で利用可能な機能を制限することで、不正利用が行えない対策を実施している。 ・システムの利用できる端末を管理することにより、不要な端末からの利用ができない制限を実施している。 ・認証パスワードについて、現在有効であるか、適切なパスワード値であるか否かをシステムで判別している。また有効期限を設定し、期限までに変更を行わない場合は、対応するユーザーIDが失効する。
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	＜発効管理＞ 職員ごとに業務上必要な権限を特定し、必要最小限の範囲で付与している。 ＜失効管理＞ 異動・退職等が発生する都度、権限を見直し、不要となった権限を削除している。
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	・ユーザIDやアクセス権限の管理表を作成、定期的に確認し、業務上アクセスが不要となったIDやアクセス権限を変更または削除する。
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	・システムを操作した履歴を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操作履歴は定められた期間、保管する。
その他の措置の内容 住民記録システムでは、操作者による認証から認証解除を行うまでの間、監査認証を行っている。 (操作者がどの個人に対して照会・異動・証明書発行を行ったかを記録している。)		
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		・業務に応じてアクセス権限を制限し、不必要な情報にアクセスできない措置を講じる。 ・職員にセキュリティ研修を受講させ、個人情報保護の意識を徹底させる。 ・特定個人情報ファイルのアクセスに対し、ログを記録している。
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		・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している。 ・委託先に対しては個人情報の保護に関する取扱仕様書において許可を得ない複製を禁止している。
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

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		
・業務外利用したときは、操作ログを確認することで特定可能であることを職員に周知し、業務外利用の抑止に努めている。 外部媒体への出力は、管理者権限を持ったユーザーのみが、特定の操作端末機器を使用し、登録管理された記録媒体のみに限定許可している。 ・サービス検索・電子申請機能へのアクセスログ、システムへのアクセスログ、操作ログの記録を行い、操作者個人を特定できるようにする。 ・アクセスログ及び操作ログは、改ざんを防止するため、不正プロセス検知ソフトウェアにより、不正なログの書き込み等を防止する。 ・定期的に操作ログをチェックし、不正とみられる操作があった場合、操作内容を確認する。 ・外部記憶媒体にサービス検索・電子申請機能から取得した個人番号付電子申請データ等のデータを複製する場合、使用管理簿に記載し、事前に責任者の承認を得たうえで複製する。なお、外部記憶媒体は限定されたUSBメモリ等のみを使用する。 ＜申請管理システムの措置＞ ・申請管理システムを利用する必要がある職員を特定し、適切なユーザ割り当て及び認証を行う。 ・申請管理システムへのアクセスログ、操作ログの記録を行い、不正とみられる操作があった場合、操作内容を確認する。		
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	委託先情報管理体制書の提出及び委託先の監査を実施した。	
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	特定個人情報取り扱いに関する委託契約取り交わした。	
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	委託契約にて取扱いについて定めている。	
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	契約上にて再委託先への提供を禁じている。(市の承諾を得た場合の提供も契約上に明記。)	
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	必要があれば実施調査を行うとしている。	
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	委託契約終了後、速やかに削除することを定めている。	

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	（個人情報の保護） 受託者及び従事者は、この契約の履行にあたって法令等を遵守するとともに、個人情報の漏えい、滅失、き損の防止その他個人情報の保護を図るため、個人情報の保護に関する法令等、その他当市の個人情報に関する規程及びこの契約の条項を遵守しなければならない。 （秘密の保持） 受託者は、善良な管理者として注意を払う義務を有し、委託業務の処理上、直接または間接的に知り得た事項については、契約期間中及び契約終了後または解除後において、いかなる理由によっても他に漏らしてはならない。 2 受託者は、目的物を第三者に閲覧させ、または貸出、もしくは提供してはならない。 3 受託者は、当市に対し前二項の義務の履行を担保するため、従事者との連署による誓約書を提出しなければならない。 4 受託者は、従事者に対し、事前及び定期的に秘密の保持についての教育を行わなければならない。 （立ち入り検査等） 当市は、必要と認めるときは、受託者に対して委託業務の処理状況並びに個人情報の保護及び管理状況等について随時に調査し、または報告を求めることができる。 （目的外使用の禁止） 受託者は、個人情報を当市から支持された目的以外に使用し、または第三者へ提供してはならない。 （複写及び複製の禁止） 受託者は、当市から指示された場合以外に、個人情報を記録した書類を複写または複製してはならない。 （物品の持ち込み等の禁止） 受託者は、当市の許可を受けた場合を除き、従事者に作業場所への物品の持込みまたは作業場所からの物品の持出しをさせてはならない。 （入出力帳票の適正管理） 受託者は、委託業務の履行に際し、入出力帳票の滅失、き損等を防止し、その適正な管理を図らなければならない。
再委託先による特定個人情報ファイルの適切な取扱いの確保		[十分に行っている] ＜選択肢＞ 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない 4) 再委託していない
	具体的な方法	再委託は、原則として禁止しているが、事前に再委託理由、事業者名、取扱情報、安全・信頼性の確保、管理監督の方法等を記載した書面を提出させ、再委託に必要性や業務内容等を確認したうえで承認する。 なお、再委託先にも受託元と同等の守秘義務等が課される。
その他の措置の内容		－
リスクへの対策は十分か		[十分である] ＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		
・委託先の社会的信用と能力を確認するとともに、その記録を残す。 ・作業者を限定するために委託業者の名簿を提出させる。 ・閲覧、更新権限を持つもののアカウント管理を行い、システム上で操作を制限し、操作履歴（ログ）を取得し、不正な使用がないことを確認する。		
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	特定個人情報（個人番号、5情報等）の提供を行う際に、提供の記録（提供・移転日時、操作者等）をシステム上で管理し、保存している。
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
	ルール内容及びルール遵守の確認方法	山形市電子情報処理規則第24条により、住民記録ファイルの情報を使用する場合は、事前にデータの内容、利用目的、件数等の承認申請をうけ、審査し承認している。
その他の措置の内容		提供及び移転する特定個人情報ファイルについては、提供データ作成時に監査証跡に作成日時、提供日時等の実行処理結果が記録される仕組みをとっている。

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 3) 課題が残されている	2) 十分である
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	システム上、特定の権限者以外は情報照会・提供ができず、さらに、情報照会・情報提供記録がアクセスログとして記録、保管されている。		
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 3) 課題が残されている	2) 十分である
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・移転している。 また、住民基本台帳情報に変更が生じた際には、住民記録システム(既存住基システム)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している。 ・誤った相手に提供・移転してしまうリスクへの措置 接続相手方(各業務システム)と共通基盤システム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 3) 課題が残されている	2) 十分である
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			
不適切な方法での提供・移転が行われるリスクへの措置 ・住民記録システムと庁内連携システム間のデータの移転は、アクセスを許可された業務システムのみデータを移転することをシステム上制御している。 ・住基CSを介した通信では接続先と相互認証を実施しているため、認証できない相手先への提供・移転されないことをシステム上制御している。 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している。 ・本人確認情報に変更が生じた際には、住基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がなされた情報を通知することをシステム上担保している。 誤った相手に提供・移転してしまうリスクへの措置 ・住基CSを介した通信では接続先と相互認証を実施しているため、認証できない相手先への提供・移転されないことをシステム上制御している。			
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 3) 課題が残されている	2) 十分である
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 3) 課題が残されている	2) 十分である
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 3) 課題が残されている	2) 十分である

リスク4: 入手の際に特定個人情報漏えい・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	・ネットワーク接続に対してファイアーウォール等でアクセス制御している。 ・ログイン時の操作者認証のほかに、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。 <団体内統合宛名システムにおける措置> ・団体内統合宛名システムでは、個人番号利用事務システムからの接続には認証を必須としており、個人番号利用事務システム以外のアクセスはできない仕様を構築している。 ・団体内統合宛名システムでは、操作IDによる認証と許可機能により、操作者がシステム上で利用可能な機能を制限することで不正使用が行えない対策を実施している。 <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における照会許可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機微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。	
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うえ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ほかに、ログイン・ログアウトを実施した職員、時刻、操作内容が記録されるため、不適切な接続端末の操作やオンライン連携を抑止する仕組みとなっている。 (注) セキュリティ管理機能: 暗号化・復号機能と、鍵情報及び照会許可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・運用を行う事業者及びクラウドサービス事業者においては、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	・中間サーバーへの情報連携は、住民記録システム(既存住基システム)の更新の都度行い、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＞ ・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、当該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。 (注) 情報提供データベース管理機能: 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事業者及びクラウドサービス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	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にしていない
	具体的な対策の内容	<本市における措置> ・電子計算機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。 ・停電(落雷等)によるデータの消失を防ぐために、電子計算機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。 ・新耐震基準に基づいて設計、施工された施設内にサーバ室を設置している。 <中間サーバー・プラットフォームにおける措置> 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が適切に実施されているほか、次を満たしている。 ・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。 <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	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にっていない
	具体的な対策の内容	<市における措置> ・特定個人情報ファイルを管理しているサーバーは、インターネット等の外部ネットワークから隔離されたネットワーク上に設置している。 ・特定個人情報ファイルを管理している全てのサーバーには、ウイルス対策ソフトを導入しており、セキュリティパッチも必要に応じ、適切に管理している。 ・ウイルス対策ソフトのパターンファイルは定期的に更新し、常に最新の状態に保っている。 <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・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。 ②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。 ③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。 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。
⑦バックアップ	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にっていない
⑧事故発生時手順の策定・周知	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にっていない

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		[発生あり]	<選択肢> 1) 発生あり 2) 発生なし
	その内容	発生日: 令和8年4月2日 内容: 市の保有する個人情報を扱う委託業務において、受託事業者が保有するファイルサーバーが不正アクセスを受け、個人情報漏洩のおそれが発生した。 影響を受けた人数: 56,966人	
	再発防止策の内容	・委託先を含めたデータ管理の徹底、不要データの削除確認、監査体制の強化などを進めていく。 ・事故に関わる委託事業者に対して個人情報の適切な取り扱いの徹底を指導するとともに、原因究明と再発防止策の報告を求める。	
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	生存者と情報と同様の方法で保管している。	
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: 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。	
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	<本市における措置> ・住民基本台帳ファイルに記録されたデータのうち、住民票の消除後150年を経過したデータをシステムにて判別し、消去する。 ・磁気ディスクの廃棄時は、規定に基づき、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。 ・帳票については、規定に基づき、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。 ・廃棄時には、規定に基づき、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> 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等に当たって確実にデータを消去する。	
その他の措置の内容		-	
リスクへの対策は十分か		[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置

<山形市における措置>

当市では、住民票を磁気ディスクで調整しており、高度なセキュリティを用いたサーバー内にデータとして、入退室管理を行っているセキュリティロックの設置した部屋に保管する。

サーバへのアクセスはID／パスワード認証が必要となる。

不正アクセスを防止するためにアクセス制御機能として、ユーザIDによる識別とパスワードによる認証、さらに認証したユーザに対する権限機能により、そのユーザがシステム上での利用制限することで、ログイン、処理権限の付与、ログ監視を行う。

住民記録システムで保持している特定個人情報に該当する住民票情報のうち、削除された住民票については住民基本台帳法施行令34条の規定により、削除された日から150年間保存することは定義されているが、削除の定義の規定はないため、情報セキュリティポリシーにより、適切な削除処理を行う。

LGWAN接続端末については、業務時間内のセキュリティワイヤー等による固定、操作場所への入退室管理、業務時間外の施錠できるキャビネット等への保管、などの物理的対策を講じている。

外部記憶媒体については、限定されたUSBメモリ等以外の利用不可、施錠できるキャビネット等への保管、使用管理簿による管理、などの安全管理措置を講じている。

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。

サービス検索・電子申請機能と地方公共団体との間は、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。

LGWAN接続端末は、基本的には、個人番号付電子申請データの一時保管として使用するが、一時保管中に再申請や申請情報の訂正が発生した場合には古い情報で審査等を行わないよう、履歴管理を行う。

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について徹底し、必要に応じて管理者が確認する。

外部記憶媒体については、定期的に内部のチェックを行い不要なデータの確認を行い、廃棄する場合は管理者の承認を得て行う手順を定めている。

<中間サーバー・プラットフォームにおける措置>

【物理的対策】

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が適切に実施されているほか、次を満たしている。

・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。

【技術的対策】

①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。

②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。

③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。

④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、インターネットとは切り離された閉域ネットワーク環境に構築する。

⑤中間サーバーのデータベースに保存される特定個人情報は、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者がアクセスできないよう制御を講じる。

⑥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。⑦中間サーバー・プラットフォームの移行の際は、中間サーバー・プラットフォームの事業者において、移行するデータを暗号化した上で、インターネットを経由しない専用回線を使用し、VPN等の技術を利用して通信を暗号化することでデータ移行を行う。

＜申請管理システムにおける措置＞

- ・申請管理システム及び連携サーバについては、電子計算機室等の管理区域に設置しており、入室管理及び監視カメラの設置、などの物理的対策を講じている。
- ・申請管理システムに接続可能な端末については、端末本体にデータが残らないよう対策をしている。
- ・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。
- ・申請管理システムでは、申請データの再申請や申請情報の訂正が発生した場合には古い情報で審査等を行わないよう、履歴管理を行う。
- ・連携サーバは、個人番号付電子申請データは経由するのみで保存されない。

【ガバメントクラウドにおける措置】

・物理的対策

- 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。

・技術的対策

- 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。
- 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。

・消去手順

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。

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住民記録システムに限定されるため、住民記録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	・平成14年6月10日総務省告示第334号(第6ー7 本人確認情報の通知及び記録)等により当市CSにおいて住民記録システムを通じて入手することとされている情報以外を入手できないことを、システム上で担保する。 ・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。
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) 課題が残されている 2) 十分である

リスク2: 不適切な方法で入手が行われるリスク

リスクに対する措置の内容	本人確認情報の入手元は既存住基システムに限定している。
リスクへの対策は十分か	[＜選択肢＞ 1) 特に力を入れている 3) 課題が残されている 2) 十分である]

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)の提示等を受け、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で定める書類等)の提示がない場合には、住民基本台帳ネットワーク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	・特定個人情報の入力、削除及び訂正を行う際は、整合性を確保するために、作業を行なった者以外の者が確認する等、必ずダブルチェックを実施する。 ・住民基本台帳ネットワークに記録された本人確認情報と、定期的に整合性チェックを実施している。
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 3) 課題が残されている] 2) 十分である

リスク4: 入手の際に特定個人情報情報が漏えい・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		
-		
3. 特定個人情報の使用		
リスク1: 目的を超えた紐付け、事務に必要な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	当市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当市CSへのアクセスは住民記録システムに限定しており、また、住民記録システムと当市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、当市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、当市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(手のひら静脈)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	<発効管理> 職員ごとに業務上必要な権限を特定し、必要最小限の範囲で付与している。 <失効管理> 異動・退職等が発生する都度、権限を見直し、不要となった権限を削除している。	
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	・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、市町村CS及び統合端末においてアプリケーション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は、定められた期間、保管する。	
その他の措置の内容	-	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3: 従業者が事務外で使用するリスク		
リスクに対する措置の内容	・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、除外する。	

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 3) 課題が残されている	2) 十分である
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。 また、バックアップ以外にファイルを複製しないよう、職員に対し厳格に指導する。		
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 3) 課題が残されている	2) 十分である
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 ・統合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	委託先情報管理体制書の提出及び委託先の訪問監査を実施した。		
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	特定個人情報取り扱いに関する委託契約取り交わした。		
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	委託契約にて取扱いについて定めている。		
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	契約上にて再委託先への提供を禁じている。(市の承諾を得た場合の提供も契約上に明記。)		
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	必要があれば実施調査を行うとしている。		
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
ルール内容及びルール遵守の確認方法	委託契約終了後、速やかに削除することを定めている。		

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		
規定の内容		(個人情報の保護) 受託者及び従事者は、この契約の履行にあたって法令等を遵守するとともに、個人情報の漏えい、滅失、き損の防止その他個人情報の保護を図るため、個人情報の保護に関する法令等、その他当市の個人情報に関する規程及びこの契約の条項を遵守しなければならない。 (秘密の保持) 受託者は、善良な管理者として注意を払う義務を有し、委託業務の処理上、直接または間接的に知り得た事項については、契約期間中及び契約終了後または解除後において、いかなる理由によっても他に漏らしてはならない。 2 受託者は、目的物を第三者に閲覧させ、または貸出、もしくは提供してはならない。 3 受託者は、当市に対し前二項の義務の履行を担保するため、従事者との連署による誓約書を提出しなければならない。 4 受託者は、従事者に対し、事前及び定期的に秘密の保持についての教育を行わなければならない。 (立ち入り検査等) 当市は、必要と認めるときは、受託者に対して委託業務の処理状況並びに個人情報の保護及び管理状況等について随時に調査し、または報告を求めることができる。 (目的外使用の禁止) 受託者は、個人情報を当市から支持された目的以外に使用し、または第三者へ提供してはならない。 (複写及び複製の禁止) 受託者は、当市から指示された場合以外に、個人情報を記録した書類を複写または複製してはならない。 (物品の持ち込み等の禁止) 受託者は、当市の許可を受けた場合を除き、従事者に作業場所への物品の持ち込みまたは作業場所からの物品の持出しをさせてはならない。 (入出力帳票の適正管理) 受託者は、委託業務の履行に際し、入出力帳票の滅失、き損等を防止し、その適正な管理を図らなければならない。
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		
具体的な方法		再委託は、原則として禁止しているが、事前に再委託理由、事業者名、取扱情報、安全・信頼性の確保、管理監督の方法等を記載した書面を提出させ、再委託に必要性や業務内容等を確認したうえで承認する。 なお、再委託先にも受託元と同等の守秘義務等が課される。
その他の措置の内容		-
リスクへの対策は十分か		
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		
・委託先の社会的信用と能力を確認するとともに、その記録を残す。 ・作業者を限定するために委託業者の名簿を提出させる。 ・閲覧、更新権限を持つもののアカウント管理を行い、システム上で操作を制限し、操作履歴(ログ)を取得し、不正な使用がないことを確認する。		
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		
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、提供の記録(提供・移転日時、操作者等)をシステム上で管理し、保存している。
特定個人情報の提供・移転に関するルール		
ルール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の保護に関する法令等の規定に基づき認められる特定個人情報の提供・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・移転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。 媒体を用いて情報を連携する場合には、原則として媒体へのデータ出力（書き込み）の際に職員の立会いを必要とする。		
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 3) 課題が残されている	2) 十分である
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）と当市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 3) 課題が残されている	2) 十分である
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、当市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）と当市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 3) 課題が残されている	2) 十分である

特定個人情報の提供・移転(委託や情報提供ネットワークシステムを通じた提供を除く。)におけるその他のリスク及びそのリスクに対する措置

6. 情報提供ネットワークシステムとの接続 [○] 接続しない(入手) [○] 接続しない(提供)

リスク1: 目的外の入手が行われるリスク

リスクに対する措置の内容	
リスクへの対策は十分か	[] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

リスク2: 安全が保たれない方法によって入手が行われるリスク

リスクに対する措置の内容	
リスクへの対策は十分か	[] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

リスク3: 入手した特定個人情報が不正確であるリスク

リスクに対する措置の内容	
リスクへの対策は十分か	[] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

リスク4: 入手の際に特定個人情報が漏えい・紛失するリスク

リスクに対する措置の内容	
リスクへの対策は十分か	[] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

リスク5: 不正な提供が行われるリスク

リスクに対する措置の内容	
リスクへの対策は十分か	[] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

リスク6: 不適切な方法で提供されるリスク

リスクに対する措置の内容	
リスクへの対策は十分か	[] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

リスク7: 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク

リスクに対する措置の内容	
リスクへの対策は十分か	[] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置		
7. 特定個人情報の保管・消去		
リスク1: 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[政府機関ではない]	<選択肢> 1) 特に力を入れて遵守している 2) 十分に遵守している 3) 十分に遵守していない 4) 政府機関ではない
②安全管理体制	[十分に整備している]	<選択肢> 1) 特に力を入れて整備している 2) 十分に整備している 3) 十分に整備していない
③安全管理規程	[十分に整備している]	<選択肢> 1) 特に力を入れて整備している 2) 十分に整備している 3) 十分に整備していない
④安全管理体制・規程の職員への周知	[十分に周知している]	<選択肢> 1) 特に力を入れて周知している 2) 十分に周知している 3) 十分に周知していない
⑤物理的対策	[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
	具体的な対策の内容	・電子計算機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。 ・停電(落雷等)によるデータの消失を防ぐために、電子計算機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。 ・新耐震基準に基づいて設計、施工された施設内にサーバ室を設置している。
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	・特定個人情報ファイルを管理しているサーバーは、インターネット等の外部ネットワークから隔離されたネットワーク上に設置している。 ・特定個人情報ファイルを管理している全てのサーバーには、ウイルス対策ソフトを導入しており、セキュリティパッチも必要に応じ、適切に管理している。 ・ウイルス対策ソフトのパターンファイルは定期的に更新し、常に最新の状態に保っている。
⑦バックアップ	[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
⑧事故発生時手順の策定・周知	[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	[発生あり]	<選択肢> 1) 発生あり 2) 発生なし
	その内容	発生日: 令和8年4月2日 内容: 市の保有する個人情報を扱う委託業務において、受託事業者が保有するファイルサーバーが不正アクセスを受け、個人情報漏洩のおそれが発生した。 影響を受けた人数: 56,966人
	再発防止策の内容	・委託先を含めたデータ管理の徹底、不要データの削除確認、監査体制の強化などを進めていく。 ・事故に関わる委託事業者に対して個人情報の適切な取り扱いの徹底を指導するとともに、原因究明と再発防止策の報告を求める。
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	生存者と情報と同様の方法で保管している。
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 3) 課題が残されている	2) 十分である
リスク2: 特定個人情報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、連絡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。		
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 3) 課題が残されている	2) 十分である
リスク3: 特定個人情報が消去されずいつまでも存在するリスク			
消去手順	[定めている]	<選択肢> 1) 定めている	2) 定めていない
手順の内容	データ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	-		
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 3) 課題が残されている	2) 十分である
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			
入退出には入退出管理簿に入室時刻、作業内容等を記入の上、入室用磁気カードを用いて入室し、退出後は管理簿に退出時刻を記入し、磁気カードを返却する。 入退出管理を行っているセキュリティロックの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／パスワード及び生体認証が必要となる。 住民記録システムとの整合性を年間1回以上実施し、保存する本人確認情報が最新であるかどうか確認する。 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号に定める期間保存する。 【ガバメントクラウドにおける措置】 ・物理的対策 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出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。 ・技術的対策 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。 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。			

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。	
その他の措置の内容	－	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2： 不適切な方法で入手が行われるリスク		
リスクに対する措置の内容	本人確認情報の入手元は既存住基システムに限定している。	
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： 入手した特定個人情報ที่ไม่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）の提示等を受け、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で定める書類等）の提示がない場合には、住民基本台帳ネットワーク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	住民記録システム（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、住民記録システム（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、一定期間経過後に市町村CSから自動的に削除する。	
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。 ※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		
-		
3. 特定個人情報の使用		
リスク1: 目的を超えた紐付け、事務に必要な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、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(手のひら静脈)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	<発効管理> 職員ごとに業務上必要な権限を特定し、必要最小限の範囲で付与している。 <失効管理> 異動・退職等が発生する都度、権限を見直し、不要となった権限を削除している。	
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	・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、市町村CS及び統合端末においてアプリケーション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は、定められた期間、保管する。	
その他の措置の内容	-	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3: 従業者が事務外で使用するリスク		
リスクに対する措置の内容	・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。 また、バックアップ以外にファイルを複製しないよう、職員・委託先等に対し指導する。
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 ・統合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	委託先情報管理体制書の提出及び委託先の訪問監査を実施した。
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
具体的制限方法	特定個人情報取り扱いに関する委託契約取り交わした。
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	契約上にて再委託先への提供を禁じている。(市の承諾を得た場合の提供も契約上に明記。)
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	契約上にて再委託先への提供を禁じている。(市の承諾を得た場合の提供も契約上に明記。)
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	必要があれば実施調査を行うとしている。
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	委託契約終了後、速やかに削除することを定めている。

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		
規定の内容		(個人情報の保護) 受託者及び従事者は、この契約の履行にあたって法令等を遵守するとともに、個人情報の漏えい、滅失、き損の防止その他個人情報の保護を図るため、個人情報の保護に関する法令等、その他当市の個人情報に関する規程及びこの契約の条項を遵守しなければならない。 (秘密の保持) 受託者は、善良な管理者として注意を払う義務を有し、委託業務の処理上、直接または間接的に知り得た事項については、契約期間中及び契約終了後または解除後において、いかなる理由によっても他に漏らしてはならない。 2 受託者は、目的物を第三者に閲覧させ、または貸出、もしくは提供してはならない。 3 受託者は、当市に対し前二項の義務の履行を担保するため、従事者との連署による誓約書を提出しなければならない。 4 受託者は、従事者に対し、事前及び定期的に秘密の保持についての教育を行わなければならない。 (立ち入り検査等) 当市は、必要と認めるときは、受託者に対して委託業務の処理状況並びに個人情報の保護及び管理状況等について随時に調査し、または報告を求めることができる。 (目的外使用の禁止) 受託者は、個人情報を当市から支持された目的以外に使用し、または第三者へ提供してはならない。 (複写及び複製の禁止) 受託者は、当市から指示された場合以外に、個人情報を記録した書類を複写または複製してはならない。 (物品の持ち込み等の禁止) 受託者は、当市の許可を受けた場合を除き、従事者に作業場所への物品の持ち込みまたは作業場所からの物品の持出しをさせてはならない。 (入出力帳票の適正管理) 受託者は、委託業務の履行に際し、入出力帳票の滅失、き損等を防止し、その適正な管理を図らなければならない。
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		
具体的な方法		再委託は、原則として禁止しているが、事前に再委託理由、事業者名、取扱情報、安全・信頼性の確保、管理監督の方法等を記載した書面を提出させ、再委託に必要性や業務内容等を確認したうえで承認する。 なお、再委託先にも受託元と同等の守秘義務等が課される。
その他の措置の内容		-
リスクへの対策は十分か		
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		
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、提供の記録(提供・移転日時、操作者等)をシステム上で管理し、保存している。
特定個人情報の提供・移転に関するルール		
ルール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の保護に関する法令等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。 媒体を用いて情報を連携する場合には、原則として媒体へのデータ出力（書き込み）の際に職員の立会いを必要とする。		
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 3) 課題が残されている	2) 十分である
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 3) 課題が残されている	2) 十分である
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 3) 課題が残されている	2) 十分である
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置			
-			
6. 情報提供ネットワークシステムとの接続		[○] 接続しない（入手） [○] 接続しない（提供）	
リスク1： 目的外の入手が行われるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
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 3) 課題が残されている	2) 十分である
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 3) 課題が残されている	2) 十分である
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 3) 課題が残されている	2) 十分である
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 3) 課題が残されている	2) 十分である
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 3) 課題が残されている	2) 十分である
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 3) 課題が残されている	2) 十分である
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 3) 十分に遵守していない	2) 十分に遵守している 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 3) 十分に整備していない	2) 十分に整備している
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 3) 十分に整備していない	2) 十分に整備している
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 3) 十分に周知していない	2) 十分に周知している
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 3) 十分に行っていない	2) 十分に行っている
	具体的な対策の内容	・電子計算機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。 ・停電(落雷等)によるデータの消失を防ぐために、電子計算機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。 ・新耐震基準に基づいて設計、施工された施設内にサーバ室を設置している。	
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 3) 十分に行っていない	2) 十分に行っている
	具体的な対策の内容	・特定個人情報ファイルを管理しているサーバーは、インターネット等の外部ネットワークから隔離されたネットワーク上に設置している。 ・特定個人情報ファイルを管理している全てのサーバーには、ウイルス対策ソフトを導入しており、セキュリティパッチも必要に応じ、適切に管理している。 ・ウイルス対策ソフトのパターンファイルは定期的に更新し、常に最新の状態に保っている。	
⑦バックアップ	[十分に行っている]	＜選択肢＞ 1) 特に力を入れて行っている 3) 十分に行っていない	2) 十分に行っている
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 3) 十分に行っていない	2) 十分に行っている

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		[発生あり]	<選択肢> 1) 発生あり 2) 発生なし
	その内容	発生日: 令和8年4月2日 内容: 市の保有する個人情報を扱う委託業務において、受託事業者が保有するファイルサーバーが不正アクセスを受け、個人情報漏洩のおそれが発生した。 影響を受けた人数: 56,966人	
	再発防止策の内容	・委託先を含めたデータ管理の徹底、不要データの削除確認、監査体制の強化などを進めていく。 ・事故に関わる委託事業者に対して個人情報の適切な取り扱いの徹底を指導するとともに、原因究明と再発防止策の報告を求める。	
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	生存者と情報と同様の方法で保管している。	
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: 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、連絡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。	
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

【ガバメントクラウドにおける措置】

・物理的対策

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。

・技術的対策

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。

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。

・消去手順

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。

Ⅳ その他のリスク対策 ※

1. 監査		
①自己点検	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にしていない
具体的なチェック方法	<山形市における措置> 情報セキュリティに関する自己点検を年に1回実施する。 特定個人情報の取扱いに関する自己点検を年に1回実施する。 <中間サーバ・プラットフォームにおける措置> 運用規則等に基づき、中間サーバ・プラットフォームの運用に携わる職員及び事業者に対し、定期的に自己点検を実施することとしている。	
②監査	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にしていない
具体的な内容	<山形市における措置> 「情報セキュリティポリシー」及び「山形市の保有する個人情報の適切な管理のための措置に関する要領」に基づく監査を定期的または必要に応じて実施する。 <中間サーバ・プラットフォームにおける措置> ①運用規則等に基づき、中間サーバ・プラットフォームについて、定期的に監査を行うこととしている。 ②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	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にしていない
具体的な方法	<山形市における措置> 「情報セキュリティポリシー」及び「山形市の保有する個人情報の適切な管理のための措置に関する要領」に基づく監査を定期的または必要に応じて実施する。 <中間サーバ・プラットフォームにおける措置> ①運用規則等に基づき、中間サーバ・プラットフォームについて、定期的に監査を行うこととしている。 ②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。	
3. その他のリスク対策		
<データ移行にかかるリスク対策> システム更改に伴うリスク対策については、以下のとおり。 ・クラウド環境における専用領域の構築: 同じ領域に他団体等のデータを共有しない。 ・専用回線によるデータ通信: 山形市-データセンター間の専用回線(IPVPN回線)により、他者が閲覧等することがない。 ・複数回に渡る事前リハーサル: 事前のリハーサルの実施により、データを破損(取り込みエラー)等することがない。 <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	山形市市民生活部市民相談課 990-8540 山形市旅籠町二丁目3番25号 ☎023-641-1212 内線254
②請求方法	指定様式による書面の提出により、開示・訂正・追加・削除・利用停止請求を受付している。 山形市公式ホームページ上で個人情報開示請求について案内している。
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	住民基本台帳事務基幹システム(ADWORLD)ファイル
公表場所	https://www.city.yamagata-yamagata.lg.jp/shiseijoho/johokokai/1007071/1011384.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	山形市市民生活部市民課 990-8540 山形市旅籠町二丁目3番25号 ☎023-641-1212 内線352 ファックス023-624-8411
②対応方法	・問い合わせ受付時に受付票を起票し、対応について記録を残す。 ・個人情報の保護に関する法令等に従い、適正かつ迅速に対応する。

VI 評価実施手続

1. 基礎項目評価	
①実施日	
②しきい値判断結果	[基礎項目評価及び全項目評価の実施が義務付けられる] <選択肢> 1) 基礎項目評価及び全項目評価の実施が義務付けられる 2) 基礎項目評価及び重点項目評価の実施が義務付けられる(任意に全項目評価を実施) 3) 基礎項目評価の実施が義務付けられる(任意に全項目評価を実施) 4) 特定個人情報保護評価の実施が義務付けられない(任意に全項目評価を実施)
2. 国民・住民等からの意見の聴取	
①方法	
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

[illegible]