特定個人情報保護評価書（全項目評価書）

評価書番号	評価書名
1	宮崎市　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

宮崎市は、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リスクを軽減させるために十分な措置を行い、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	－

評価実施機関名

宮崎市長

特定個人情報保護委員会　承認日　【行政機関等のみ】

公表日

令和3年5月21日

［平成26年４月　様式4］

項目一覧

Ⅰ　基本情報

1. 特定個人情報ファイルを取り扱う事務	
①事務の名称	住民基本台帳に関する事務
②事務の内容　※	宮崎市（以下、「本市」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、本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。 住民基本台帳は、住民基本台帳法（以下、「住基法」という。）に基づき作成されるものであり、本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に行うものであり、本市において、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の処理の基礎となるものである。 また、住基法に基づいて住民基本台帳のネットワーク化を図り、全国共通の本人確認システム（住基ネット）を都道府県と共同して構築している。 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（以下、「番号法」という。）の規定に従い、特定個人情報を以下の事務で取り扱う。（別添1を参照） 1. 個人を単位とする住民票を世帯ごとに編成し、住民基本台帳を作成 2. 転入届、転居届、転出届、世帯変更届等の届出又は職権に基づく住民票の記載、消除又は記載の修正 3. 住民基本台帳の正確な記録を確保するための措置 4. 転入届に基づき住民票の記載をした際の転出元市町村（特別区を含む。以下に同じ）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 なお、9. の「個人番号の通知及び個人番号カードの交付」に係る事務については、行政手続における特定の個人を識別するための番号の利用等に関する法律の規定する個人番号、個人番号カード、特定個人情報の提供等に関する省令（平成26年11月20日総務省令第85号）（以下、「個人番号通知書、個人番号カード省令」という。）第35条（個人番号通知書、個人番号カード関連事務の委任）により機構に対する事務の一部の委任が認められている。 そのため、当該事務においては、事務を委任する機構に対する情報の提供を含めて特定個人情報ファイルを使用する。
③対象人数	[　30万人以上　] ＜選択肢＞ 1) 1,000人未満　2) 1,000人以上1万人未満 3) 1万人以上10万人未満　4) 10万人以上30万人未満 5) 30万人以上

2. 特定個人情報ファイルを取り扱う事務において使用するシステム	
システム1	
①システムの名称	住民記録システム（既存住民基本台帳システム）（以下、「住記システム」という。）
②システムの機能	1. 異動入力機能 ：届出や通知に基づく異動時における、入力機能および入力された住民基本台帳を管理する機能 2. 照会機能 ：住民基本台帳を検索、照会する機能 3. 帳票発行機能 ：住民票の写し、記載事項証明書等の各種証明書の発行や、付帯帳票の発行機能 4. 一括処理機能 ：転入通知等に基づく異動を一括で住民基本台帳に記載する機能 5. 庁内連携機能 ：庁内の各システムへの基礎データとして利用するため、宛名システムや他システムへの連携機能 6. 庁外連携機能 ：住基ネット（庁外）とのデータ連携を行い、各種通知情報の収受を行う機能 7. 印鑑登録機能 ：印鑑登録情報の管理機能や印鑑登録証明書の交付機能 8. カード管理機能 ：住民基本台帳カード等の管理機能 9. 住民基本台帳の統計機能 ：異動集計表や、人口統計用の集計表を作成する機能
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（住基ネット）
②システムの機能	1．本人確認情報の更新 ：住記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、当該情報を基に市町村CSの本人確認情報を更新し、都道府県サーバへ更新情報を送信する。 2．本人確認 ：特例転入処理や住民票の写しの広域交付などを行う際、窓口における本人確認のため、提示された個人番号カード等を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4情報（氏名、性別、生年月日、住所）の組合せをキーに本人確認情報の検索を行い、検索条件に該当する本人確認情報の一覧を画面上に表示する。 5．機構への情報照会 ：全国サーバに対して住民票コード、個人番号又は4情報の組合せをキーとした本人確認情報照会要求を行い、該当する個人の本人確認情報を受領する。 6．本人確認情報整合 ：本人確認情報ファイルの内容が都道府県知事が都道府県サーバにおいて保有している都道府県知事保存本人確認情報ファイル及び機構が全国サーバにおいて保有している機構保存本人確認情報ファイルと整合することを確認するため、都道府県サーバ及び全国サーバに対し、整合性確認用本人確認情報を提供する。 7．送付先情報通知 ：個人番号の通知に係る事務の委任先である機構において、住民に対して番号通知書類(個人番号通知書、個人番号カード交付申請書（以下、「交付申請書」という。）等)を送付するため、住記システムから当該市町村の住民基本台帳に記載されている者の送付先情報を抽出し、当該情報を、機構が設置・管理する個人番号カード管理システムに通知する。 8．個人番号カード管理システムとの情報連携 ：機構が設置・管理する個人番号カード管理システムに対し、個人番号カードの交付、廃止、回収又は一時停止解除に係る情報や個人番号カードの返還情報等を連携する。
③他のシステムとの接続	[　] 情報提供ネットワークシステム　　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　　[○] 既存住民基本台帳システム [　] 宛名システム等　　[　] 税務システム [　] その他　（　）

システム3	
①システムの名称	団体内統合宛名システム
②システムの機能	1．宛名管理機能 （1）サーバ内の宛名データベースのセットアップ （2）宛名の異動データを取り込み、宛名データベースへ反映 （3）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 （4）宛名データベースの検索、参照、更新 （5）オンラインで入力したデータを業務システムに連携 （6）団体内統合宛名番号を業務システムに連携 2．情報提供機能 （1）中間サーバに連携する各業務情報をデータベースへセットアップ （2）各業務の異動データを取り込み、データベースに反映 （3）各業務情報の参照、入力、変更、削除を行う。 （4）各業務情報を一括で中間サーバに連携 （5）各業務の異動情報を中間サーバに連携 3．情報照会機能（他機関への情報照会） （1）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、オンラインにて表示する。 （2）情報照会の対象者情報を基に、中間サーバに情報を要求し、一括ファイルを作成する。 4．符号要求 （1）処理通番を要求・受信し、符号要求データを住記システムに送信する。
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　）

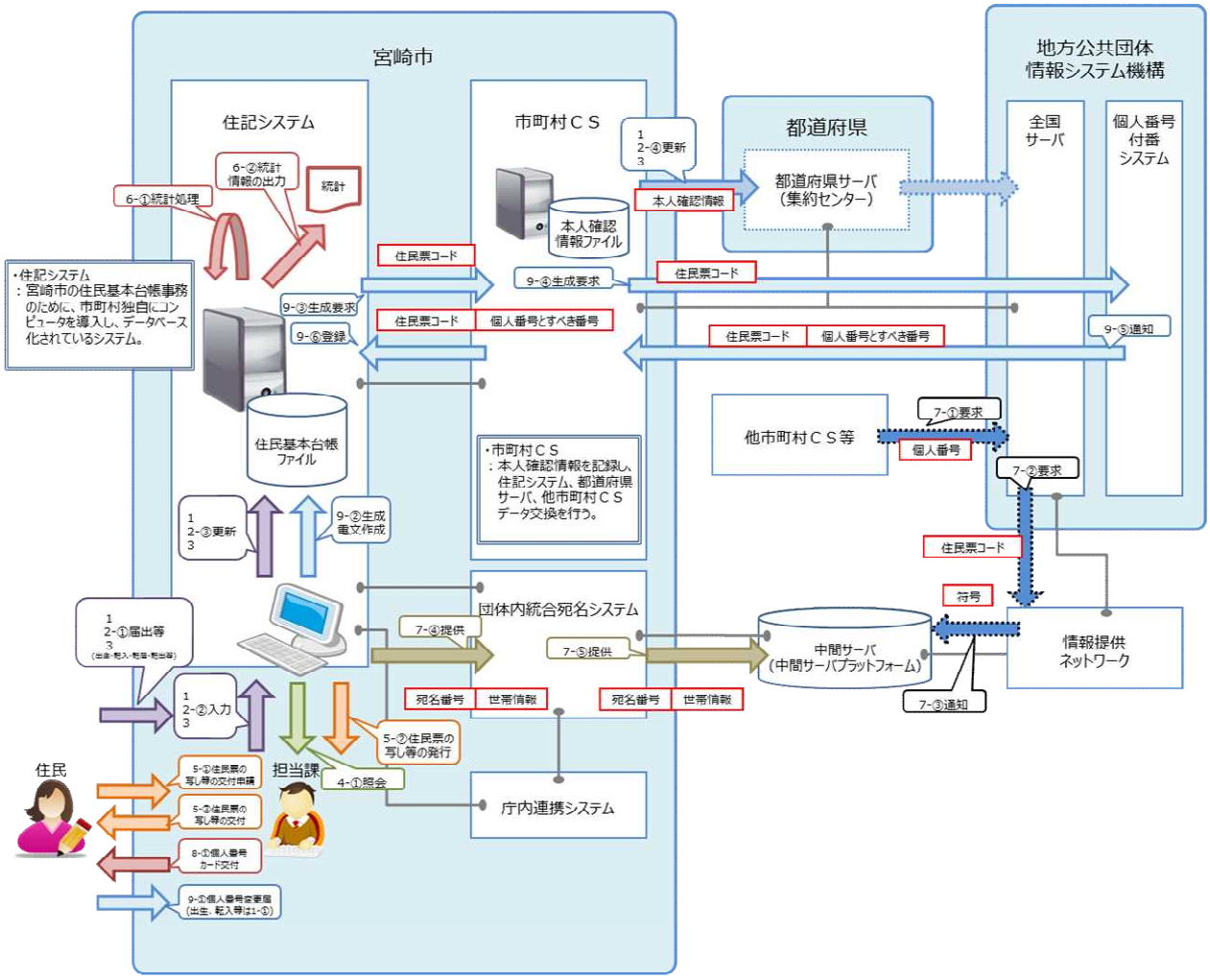
システム4	
①システムの名称	中間サーバ
②システムの機能	中間サーバは、情報提供ネットワークシステム、団体内統合宛名システムとのデータ受け渡しを行うことで、符号の取得（※）や各情報保有機関で保有する特定個人情報の照会と提供等の業務を実現する。 1. 符号管理機能 ：情報保有機関内で個人を特定するために利用する「団体内統合宛名番号」と、情報照会、情報提供に用いる個人の識別子である「符号」とを紐付け、その情報を保管・管理する機能 2. 情報照会機能 ：情報提供ネットワークシステムを介して、特定個人情報（連携対象）の情報照会及び情報提供受領（照会した情報の受領）を行う機能 3. 情報提供機能 ：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及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 ：中間サーバと既存システム、団体内統合宛名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 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 ：中間サーバと情報提供ネットワーク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機能 9. 職員認証・権限管理機能 ：中間サーバ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、稼動状況の通知、保管期限切れ情報の削除を行う機能 （※）セキュリティの観点により、特定個人情報の照会と提供の際は、「個人番号」を直接利用せず「符号」を取得して利用する。
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　（　　）

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	1. 住民基本台帳ファイル :行政手続における特定の個人を識別するための番号の利用等に関する法律の施行に伴う関係法律の整備等に関する法律第16条 （住基法第7条8の2号） により、個人番号が住民基本台帳の記載事項として追加されたため、住民基本台帳ファイルにおいて個人番号を含む個人情報の管理を行う。 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。(個人番号通知書、個人番号カード省令第35条(個人番号通知書、個人番号カード関連事務の委任)により機構に対する事務の一部の委任が認められている。)
②実現が期待されるメリット	住民票の写し等にかえて本人確認情報を利用することにより、これまでに窓口で提出が求められていた行政機関が発行する添付書類(住民票の写し等)の省略が図られ、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(本人等の請求に係る住民票の写しの交付) ・第12条の4(本人等の請求に係る住民票の写しの交付の特例) ・第14条(住民基本台帳の正確な記録を確保するための措置) ・第22条(転入届) ・第24条の2(個人番号カードの交付を受けている者等に関する転入届の特例) ・第30条の6(市町村長から都道府県知事への本人確認情報の通知等) ・第30条の10 (通知都道府県の区域内の市町村の執行機関への本人確認情報の提供) ・第30条の12 (通知都道府県以外の都道府県の区域内の市町村の執行機関への本人確認情報の提供)

6. 情報提供ネットワークシステムによる情報連携 ※		
①実施の有無	[　　実施する　　]	<選択肢> 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	・番号法第19条第7号（特定個人情報の提供の制限）及び別表第二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日内閣府・総務省令第7号。以下「別表第二主務省令」という。） [情報提供の根拠] ・別表第二 （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、101、102、103、105、106、108、111、112、113、114、116、117、120の項） ・別表第二主務省令 （1、2、3、4、6、7、8、10、12、13、14、16、20、22、22条の3、22条の4、23、24、24条の2、24条の3、25、26条の3、27、28、31、31条の2、31条の3、32、33、37、38、39、40、41、43、43条の3、43条の4、44条の2、45、47、48、49条の2、50、51、53、55、56、57、58、59、59条の2、59条の2の2、59条の3） [情報照会の根拠] なし（情報提供ネットワーク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	宮崎市地域振興部市民課	
②所属長	課長	
8. 他の評価実施機関		
―		

（別添1）事務の内容

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



（備考）

＜「1　住民基本台帳ファイル」を取扱う事務の内容（住記システムを中心とした事務の流れ）＞

1．住民基本台帳情報の記載に関する事務
1-①．住民から転入、出生等の届出を受け付ける。
1-②．住記システムにて異動情報を入力する。
1-③．住民基本台帳ファイルを更新する。
1-④．市町村CSにて更新された本人確認情報を当該都道府県の都道府県サーバに通知する。

2．住民基本台帳の記載の変更に関する事務
2-①．住民から転居等の届出を受け付ける。
2-②．住記システムにて異動情報を入力する。
2-③．住民基本台帳ファイルを更新する。
2-④．市町村CSにて更新された本人確認情報を当該都道府県の都道府県サーバに通知する。

3．住民基本台帳の消除に関する事務
3-①．住民から転出、死亡等の届出を受け付ける。
3-②．住記システムにて異動情報を入力する。
3-③．住民基本台帳ファイルを更新する。
3-④．市町村CSにて更新された本人確認情報を当該都道府県の都道府県サーバに通知する。

4．住民基本台帳の照会
4-①．基本4情報（氏名、住所、生年月日、性別）の組み合わせや個人番号をキーとして、
住記システムから住民基本台帳を検索する。

5．帳票の発行に関する事務
5-①．住民から住民票の写し等の交付申請を受け付ける。
5-②．住記システムから当該証明書を作成して発行する。
5-③．発行して住民票等の写し等の証明書を住民へ交付する。

6．住民基本台帳の統計
6-①．住記システムにて各種統計処理を実施する。
6-②．住記システムにて各種統計情報を出力する。

7．情報連携
7-①．他市町村CS等から住基ネット全国サーバへの符号要求処理。
7-②．住基ネット全国サーバから情報提供ネットワークへの符号要求処理。
7-③．情報提供ネットワークから中間サーバへ符号を通知。
7-④．住記システムから団体内統合宛名システムへ世帯情報を提供する。
7-⑤．団体内統合宛名システムから中間サーバへ世帯情報を提供する。

8．個人番号カード交付に関する事務
8-①．個人番号カードを窓口にて住民へ交付する。

9．個人番号生成要求、変更要求に関する事務
9-①．住民から出生の届出又は個人番号の変更等の届出を受け付ける。
9-②．住記システムから個人番号の生成電文の作成を行う。
9-③．住記システムから市町村CSに対し通知を行う。
9-④．市町村CSから機構の個人番号付番システムへ個人番号の生成要求を通知する。
9-⑤．機構の個人番号付番システムから生成された個人番号が市町村CSへ通知される。
9-⑥．市町村CSにて受領した個人番号を住記システムに登録する。

Ⅱ　特定個人情報ファイルの概要

1. 特定個人情報ファイル名		
(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 ※		住民基本台帳に登録されている者のうち、個人番号を有する者
	その必要性	住民に関する市町村事務の処理の基礎として利用する。 :住基法第7条において、住民基本台帳の記載項目と規定されるため。 :番号法第19条　別表第二の事務において、符号の取得に利用するため。
④記録される項目		[　50項目以上100項目未満　] ＜選択肢＞ 1）10項目未満　2）10項目以上50項目未満 3）50項目以上100項目未満　4）100項目以上
	主な記録項目 ※	・識別情報 [○]個人番号　[　]個人番号対応符号　[○]その他識別情報（内部番号） ・連絡先等情報 [○]4情報（氏名、性別、生年月日、住所）　[○]連絡先（電話番号等） [○]その他住民票関係情報 ・業務関係情報 [　]国税関係情報　[　]地方税関係情報　[　]健康・医療関係情報 [○]医療保険関係情報　[○]児童福祉・子育て関係情報　[　]障害者福祉関係情報 [　]生活保護・社会福祉関係情報　[○]介護・高齢者福祉関係情報 [　]雇用・労働関係情報　[○]年金関係情報　[　]学校・教育関係情報 [　]災害関係情報 [○]その他　（　印鑑登録情報、カード管理情報　）
	その妥当性	個人番号、4情報、その他住民票関係情報については、住基法第7条各号で定められた項目であり、住民票への記載が必要な情報である。 業務関係情報については、住民異動に伴う他の行政手続きの案内を行うため、必要となる情報である。
	全ての記録項目	別添2を参照。
⑤保有開始日		平成27年9月24日
⑥事務担当部署		宮崎市地域振興部市民課

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 （ 戸籍通知（住基法9条2項通知） ） [ ] 民間事業者 （ ） [ ] その他 （ ）
②入手方法		[○] 紙 [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 電子メール [ ] 専用線 [ ] 庁内連携システム [ ] 情報提供ネットワークシステム [○] その他 （ 住基ネット ）
③入手の時期・頻度		出生や異動の届出、他市町村からの通知など、住民に関する記録項目への変更が発生する都度入手する。
④入手に係る妥当性		当情報は各種行政サービスの基礎となる情報であり、住民へのサービスを正確に継続して提供を行うために、住民に関する記録を正確かつ統一的に行い、常に最新の状態にしておく必要がある。
⑤本人への明示		住民票への記載事項については、住基法第7条各号により明示されている。番号法7条に基づく本人への通知による。
⑥使用目的 ※		住民基本台帳の整備、証明書等への記載、住民サービスの基礎情報とするため。
	変更の妥当性	―
⑦使用の主体	使用部署 ※	市民課、各総合支所、各地域センター、各出張所、各地域事務所、各市民サービスコーナー
	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 ※		・届出や職権等に基づき、住民票の記載及び記載事項の修正を行う。 ・本人等の請求に基づき、住民票の写し等の交付を行う。 ・住所地市町村以外の市町村長への住民票の写し請求に基づき、住民票の写しに関する情報を請求先の市町村長に通知する。 ・住民票の記載及び記載事項の修正を行った場合、本人確認情報を県知事へ通知する。 ・転入届の特例による転入地市町村長からの通知に基づき、転出証明書情報の通知を行う。 ・住民に関する事務処理において使用する宛名情報を提供する。 ・番号表別表第二に基づき、情報提供ネットワークシステムへ住民票関係情報を提供する。
	情報の突合 ※	窓口業務において本人確認書類に通知カード、個人番号カードが使われた際に個人番号で単件検索を行う。
	情報の統計分析 ※	個人番号を使用した統計分析は行わず、市政の基礎資料となる人口統計、事務処理件数の確認のための統計のみを行う。
	権利利益に影響を与え得る決定 ※	―
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		住記システム、住基ネット、団体内統合宛名システム、中間サーバ（以下、「住民記録システム等」という。）の保守・運用
①委託内容		住民記録システム等のパッケージアプリケーション保守作業、ジョブスケジューリングや帳票印刷等のシステム運用作業、職員からの問い合わせに対する調査、作業指示に基づくデータ抽出等
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 ※	住民基本台帳に登録されている者のうち、個人番号を有する者
	その妥当性	住民記録システム等の保守・運用を委託するため、システムで管理される全対象が範囲となる。
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 （ 本市のサーバ設置場所において、直接端末操作を行う。 ）
⑤委託先名の確認方法		宮崎市情報公開条例に基づく開示請求を行うことで確認ができる。
⑥委託先名		富士通株式会社 宮崎支店
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	委託業務の附属業務についてやむを得ず再委託する必要があるときは、再受託者に、当該委託契約書に記載された情報セキュリティに関する特記事項を遵守させるとともに、再受託者の氏名、再委託の内容及び業務執行場所を、本市に事前に通知し、その承認を得ることを委託契約上の条件としている。
	⑨再委託事項	システム運用状況の管理、バッチジョブ運用、リハーサル（事前検証）支援、障害発生時の対応支援等

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 （ 56 ）件 [○] 移転を行っている （ 40 ）件 [ ] 行っていない
提供先1	番号法第19条第7号別表第二の第一欄に掲げる者（別紙1を参照）
①法令上の根拠	番号法第19条第7号及び別表第二（別紙1を参照）
②提供先における用途	番号法第19条第7号別表第二の第二欄に掲げる事務（別紙1を参照）
③提供する情報	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	住民基本台帳に登録されている者のうち、個人番号を有する者
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	随時
移転先1	番号法第9条第1項別表第一の第一欄に掲げる者（別紙2を参照）
①法令上の根拠	番号法第9条第1項及び別表第一（別紙2を参照）
②移転先における用途	番号法第9条第1項別表第一の第二欄に掲げる事務（別紙2を参照）
③移転する情報	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	住民基本台帳に登録されている者のうち、個人番号を有する者
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	随時

6. 特定個人情報の保管・消去		
①保管場所 ※		＜本市における措置＞ ・サーバ設置場所に指紋認証装置や静脈認証装置を設置し、あらかじめ許可された者のみが入室できる。 ・記録媒体等については、耐火金庫を利用し施錠管理をしている。 ・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、施設内に消火設備の完備や消化器具の設置を行っている。 ＜中間サーバ・プラットフォームにおける措置＞ ・中間サーバ・プラットフォーム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室への入室を厳重に管理する。 ・特定個人情報は、サーバ室に設置された中間サーバのデータベース内に保存され、バックアップもデータベース上に保存される。
②保管期間	期間	［　定められていない　］ ＜選択肢＞ 1）1年未満　2）1年　3）2年 4）3年　5）4年　6）5年 7）6年以上10年未満　8）10年以上20年未満　9）20年以上 10）定められていない
	その妥当性	住民基本台帳法に基づく事務であるため、消除後5年度が経過することがない限り消去はしない。
③消去方法		＜本市における措置＞ ・データベースに記録されたデータは、システム機能にて完全に消去する。 ・保存された情報が読み出しできないよう、専用ソフトウェア等を用いて完全に消去する。 ・申請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行う。 ＜中間サーバ・プラットフォームにおける措置＞ ・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・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。 ・ディスク交換やハード更改等の際は、中間サーバ・プラットフォームの保守・運用を行う事業者において、保存された情報が読み出しできないよう、物理的破壊又は専用ソフトウェア等を用いて完全に消去する。

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 ※		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 ※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		[　10項目以上50項目未満　] ＜選択肢＞ 1) 10項目未満　2) 10項目以上50項目未満 3) 50項目以上100項目未満　4) 100項目以上
	主な記録項目 ※	・識別情報 [○] 個人番号　[　] 個人番号対応符号　[　] その他識別情報(内部番号) ・連絡先等情報 [○] 4情報(氏名、性別、生年月日、住所)　[　] 連絡先(電話番号等) [○] その他住民票関係情報 ・業務関係情報 [　] 国税関係情報　[　] 地方税関係情報　[　] 健康・医療関係情報 [　] 医療保険関係情報　[　] 児童福祉・子育て関係情報　[　] 障害者福祉関係情報 [　] 生活保護・社会福祉関係情報　[　] 介護・高齢者福祉関係情報 [　] 雇用・労働関係情報　[　] 年金関係情報　[　] 学校・教育関係情報 [　] 災害関係情報 [　] その他　(　　)
	その妥当性	住基ネットを通じて本人確認を行うために必要な情報として、住民票の記載等に係る本人確認情報(個人番号、4情報、住民票コード及びこれらの変更情報)を記録する必要があるため。
	全ての記録項目	別添2を参照。
⑤保有開始日		平成27年9月24日
⑥事務担当部署		宮崎市地域振興部市民課

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　（ 住記システム　）
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、まず住記システムで情報を管理した上で、全国的なシステムである住基ネットに格納する必要があるため。
⑤本人への明示		市町村CSが住記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6－6（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	ー
⑦使用の主体	使用部署 ※	市民課、各総合支所、各地域センター、各出張所
	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、住記システムから当該本人確認情報の更新情報を受領し（住記システム→市区町村CS）、受領した情報を基に本人確認情報ファイルを更新し、当該本人確認情報の更新情報を都道府県知事に通知する（市区町村CS→都道府県サーバ）。 ・住民から提示された個人番号カードに登録された住民票コードをキーとして本人確認情報ファイルを検索し、画面に表示された本人確認情報と申請・届出書等の記載内容を照合し確認することで本人確認を行う（個人番号カード→市区町村CS）。 ・4情報（氏名、性別、生年月日、住所）の組合せをキーに本人確認情報ファイルの検索を行う。 ・本人確認情報ファイルの内容が都道府県知事保存本人確認情報ファイル（都道府県サーバ）及び機構保存本人確認情報ファイル（全国サーバ）と整合することを確認するため、都道府県サーバ及び全国サーバに対し、整合性確認用本人確認情報を提供する（市区町村CS→都道府県サーバ／全国サーバ）。
	情報の突合 ※	・本人確認情報ファイルを更新する際に、受領した本人確認情報に関する更新データと本人確認情報ファイルを、住民票コードをもとに突合する。 ・個人番号カードを用いて本人確認を行う際に、提示を受けた個人番号カードと本人確認情報ファイルを、住民票コードをもとに突合する。
	情報の統計分析 ※	個人に着目した分析・統計は行わず、本人確認情報の更新件数の集計等、事務処理実績の確認のための統計のみ行う。
	権利利益に影響を与え得る決定 ※	該当なし
⑨使用開始日		平成27年10月5日

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※		[委託する] ＜選択肢＞ 1）委託する 2）委託しない （ 1 ） 件
委託事項1		住基ネットCSの保守・運用
①委託内容		住基ネットCSのアプリケーション保守作業、ジョブスケジューリングや帳票印刷等のシステム運用作業、職員からの問い合わせに対する調査等
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」と同じ
	その妥当性	住基ネットCSの保守・運用を委託するため、システムで管理される全対象が範囲となる。
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 （ 本市のサーバ設置場所において、直接端末操作を行う。 ）
⑤委託先名の確認方法		宮崎市情報公開条例に基づく開示請求を行うことで確認ができる。
⑥委託先名		富士通株式会社 宮崎支店
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	委託業務の附属業務についてやむを得ず再委託する必要があるときは、再受託者に、当該委託契約書に記載された情報セキュリティに関する特記事項を遵守させるとともに、再受託者の氏名、再委託の内容及び業務執行場所を、本市に事前に通知し、その承認を得ることを委託契約上の条件としている。
	⑨再委託事項	住基ネットCSのアプリケーション保守作業、ジョブスケジューリングや帳票印刷等のシステム運用作業、職員からの問い合わせに対する調査等

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）を基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、性別、生年月日、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」と同じ
⑥提供方法	[ ] 情報提供ネットワークシステム [ ] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [○] その他 （ 住基ネット ）
⑦時期・頻度	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	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、性別、生年月日、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」と同じ
⑥提供方法	[ ] 情報提供ネットワークシステム [ ] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [○] その他 （ 住基ネット ）
⑦時期・頻度	必要に応じて随時（1年に1回程度）

6. 特定個人情報の保管・消去		
①保管場所 ※		＜本市における措置＞ ・サーバ設置場所に指紋認証装置や静脈認証装置を設置し、あらかじめ許可された者のみが入室できる。 ・記録媒体等については、耐火金庫を利用し施錠管理をしている。 ・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、施設内に消火設備の完備や消化器具の設置を行っている。
②保管期間	期間	[　　20年以上　　]　＜選択肢＞ 1）1年未満　2）1年　3）2年 4）3年　5）4年　6）5年 7）6年以上10年未満　8）10年以上20年未満　9）20年以上 10）定められていない
	その妥当性	・住民票の記載の修正後の本人確認情報は、新たに記載の修正の通知を受けるまで保管する。 ・住民票の記載の修正前の本人確認情報（履歴情報）及び消除者の本人確認情報は、住民基本台帳法施行令第34条第3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 ※		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
	その必要性	番号法第7条第1項（指定及び通知）に基づき、個人番号通知書を個人番号の付番対象者全員に送付する必要がある。 また、同法第17条第1項（個人番号カードの交付等）により、個人番号カードは通知カードと引き換えに交付することとされていることから、合わせて、交付申請書を通知カード送付者全員に送付する必要がある。 市町村は、個人番号通知書、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機構に委任する。
④記録される項目		［　50項目以上100項目未満　］　＜選択肢＞ 1）10項目未満　2）10項目以上50項目未満 3）50項目以上100項目未満　4）100項目以上
	主な記録項目 ※	・識別情報 ［ ○ ］個人番号　［　］個人番号対応符号　［　］その他識別情報（内部番号） ・連絡先等情報 ［ ○ ］4情報（氏名、性別、生年月日、住所）　［　］連絡先（電話番号等） ［ ○ ］その他住民票関係情報 ・業務関係情報 ［　］国税関係情報　［　］地方税関係情報　［　］健康・医療関係情報 ［　］医療保険関係情報　［　］児童福祉・子育て関係情報　［　］障害者福祉関係情報 ［　］生活保護・社会福祉関係情報　［　］介護・高齢者福祉関係情報 ［　］雇用・労働関係情報　［　］年金関係情報　［　］学校・教育関係情報 ［　］災害関係情報 ［ ○ ］その他　（　通知カード及び交付申請書の送付先の情報　）
	その妥当性	個人番号、4情報、その他住民票関係情報 ：個人番号カードの券面記載事項として、法令に規定された項目を記録する必要がある。 その他（個人番号通知書及び交付申請書の送付先の情報） ：機構に対し、個人番号通知書、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、個人番号カードの券面記載事項のほか、個人番号通知書及び交付申請書の送付先に係る情報を記録する必要がある。
	全ての記録項目	別添2を参照。
⑤保有開始日		平成27年10月5日
⑥事務担当部署		宮崎市地域振興部市民課

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　（ 住記システム　）
③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。）。
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		個人番号通知書、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）に記載されている。
⑥使用目的 ※		個人番号通知書、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、通知カード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 ※	市民課、各総合支所、各地域センター、各出張所
	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 ※		住記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（住記システム→市町村CS又は電子記録媒体→個人番号カード管理システム（機構））。
	情報の突合 ※	入手した送付先情報に含まれる4情報等の変更の有無を確認する（最新の4情報等であることを確認する）ため、機構（全国サーバ）が保有する「機構保存本人確認情報」との情報の突合を行う。
	情報の統計分析 ※	送付先情報ファイルに記録される個人情報を用いた統計分析は行わない。
	権利利益に影響を与え得る決定 ※	該当なし
⑨使用開始日		平成27年10月5日

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※		[委託する] ＜選択肢＞ 1）委託する 2）委託しない （ 1 ） 件
委託事項1		住基ネットCSの保守・運用
①委託内容		住基ネットCSのアプリケーション保守作業、ジョブスケジューリングや帳票印刷等のシステム運用作業、職員からの問い合わせに対する調査等
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」と同じ
	その妥当性	住基ネットCSの保守・運用を委託するため、システムで管理される全対象が範囲となる。
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 （ 本市のサーバ設置場所において、直接端末操作を行う。 ）
⑤委託先名の確認方法		宮崎市情報公開条例に基づく開示請求を行うことで確認ができる。
⑥委託先名		富士通株式会社 宮崎支店
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	委託業務の附属業務について、やむを得ず再委託する必要があるときは、当該委託契約書に記載された「情報セキュリティに関する特記事項」を遵守させるとともに、再受託者の氏名、再委託の内容及び業務執行場所を、事前に本市に通知し、その承認を得ることを委託契約上の条件としている。
	⑨再委託事項	住基ネットCSのアプリケーション保守作業、ジョブスケジューリングや帳票印刷等のシステム運用作業、職員からの問い合わせに対する調査等

5. 特定個人情報の提供・移転（委託に伴うものを除く。）	
提供・移転の有無	[○] 提供を行っている （ 1 ）件 [ ] 移転を行っている （ ）件 [ ] 行っていない
提供先1	地方公共団体情報システム機構（機構）
①法令上の根拠	個人番号通知書、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）
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、通知カード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」と同じ
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」と同じ
⑥提供方法	[ ] 情報提供ネットワークシステム [ ] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [○] その他 （ 住基ネット ）
⑦時期・頻度	使用開始日から通知カード送付までの一定の期間に、番号法施行日時点における住民の送付先情報をまとめて提供する（以降、新たに個人番号の通知対象者が生じた都度提供する。）。

6. 特定個人情報の保管・消去		
①保管場所 ※		＜本市における措置＞ ・サーバ設置場所に指紋認証装置や静脈認証装置を設置し、あらかじめ許可された者のみが入室できる。 ・記録媒体等については、耐火金庫を利用し施錠管理をしている。 ・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、施設内に消火設備の完備や消化器具の設置を行っている。
②保管期間	期間	[　　1年未満　　]　＜選択肢＞ 1）1年未満　2）1年　3）2年 4）3年　5）4年　6）5年 7）6年以上10年未満　8）10年以上20年未満　9）20年以上 10）定められていない
	その妥当性	送付先情報は機構への提供のみに用いられ、また、送付後の変更は行わないことから、セキュリティ上、速やかに削除することが望ましいため。
③消去方法		保存期間が到来した送付先情報は、機構より指定された方法により、システム上、一括して消去する仕組みとする。
7. 備考		
－		

（別添2）特定個人情報ファイル記録項目

（1）住民基本台帳ファイル
＜住民基本台帳情報＞
1. 宛名番号
2. 住民票コード
3. 個人番号
4. 世帯番号
5. 氏名情報
6. 生年月日
7. 性別
8. 現住所情報
9. 住民区分（日本人、外国人）
10. 世帯主情報
11. 続柄
12. 住民となった年月日
13. 住民となった届出年月日
14. 住民となった事由
15. 住所を定めた年月日
16. 住所を定めた届出年月日
17. 前住所情報
18. 転入元住所情報
19. 転出先住所情報
20. 本籍・筆頭者情報
21. 備考欄履歴情報
22. 事実上の世帯主情報
23. 消除情報
24. 外国人住民となった年月日（外国人住民のみ）
25. 国籍（外国人住民のみ）
26. 法30条45規定区分（外国人住民のみ）
27. 在留カード等の番号（外国人住民のみ）
28. 在留資格情報（外国人住民のみ）
29. 通称（外国人住民のみ）
30. 通称の記載と削除関する事項（外国人住民のみ）
31. 個別記載情報（国民健康保険、後期高齢者医療保険、児童手当、介護保険、国民年金、選挙）
32. 転出予定者情報
33. 除票住民票情報
＜付帯事務情報＞
34. 証明書発行履歴情報
35. 異動履歴情報
36. 住基カード発行状況
37. 個人番号カード等情報
38. 自動交付機カード情報
39. 在留カード等情報
40. 法務省通知履歴
41. 市町村通知履歴
42. 戸籍附票通知履歴
43. 処理停止情報
＜印鑑情報＞
44. 印鑑登録情報
45. 印影情報
46. 印鑑登録異動履歴
47. 印鑑証明書発行履歴
＜カード利用者管理情報＞
48. 自動交付カード情報、自動交付カード資格情報
49. 自動交付カード履歴
50. 自動交付カード資格履歴
51. カナ旧氏
52. 旧氏

（別添2）特定個人情報ファイル記録項目

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

（別添2）特定個人情報ファイル記録項目

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

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・申請等の窓口において、身分証明書（個人番号カード等）として写真付きの書類又は複数点の書類の提示を求めるとともに、届出・申請内容と住民記録システムに入力された内容を複数人で確認し、対象者以外の情報の入手の防止に努める。 ・住基ネットを通じての情報の入手は対象者以外の情報を入手できないような検索方法になっている。 ・法務省からの通知は対象者以外の情報を入手できないような検索方法になっている。
必要な情報以外を入手することを防止するための措置の内容	・届出・申請等の様式において届出・申請等を行う者が記載する部分は、住民基本台帳事務処理要領に掲載の参考様式をもとに、住民基本台帳業務に必要な項目のみに限っている。 ・住民票の記載等に係る住民基本台帳情報以外を登録できないことを、システム上で担保している。 ・住基ネットを通じての入手は、必要な情報以外の情報を入手できないような検索方法になっている。 ・法務省からの通知は必要な情報以外の情報を入手できないような検索方法になっている。
その他の措置の内容	住民基本台帳ファイルを照会する他部署には、権限設定を行い各部署にとって必要な項目のみを表示させている。
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、受領の際に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っている。 ・システムを利用する必要がある職員を特定し、ユーザIDによる識別とパスワード及び静脈による認証を実施している。また、認証後は権限設定により、その職員がシステム上で利用可能な機能を制限することで不適切な方法で入手が行えない対策を施している。
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	職員が対象者から身分証明書（個人番号カード等）の提示を受け、本人確認を行う。
個人番号の真正性確認の措置の内容	・個人番号カード等の提示を受け、本人確認を行う。 ・出生等により新たに個人番号が指定される場合や、転入の際に個人番号カード若しくは通知カードと法令により定められた身分証明書の組み合わせの提示がない場合には、市町村CSにおいて本人確認情報と個人番号の紐付けの確認を行う。
特定個人情報の正確性確保の措置の内容	住民基本台帳情報の入力、削除及び訂正を行う際は、整合性を確保するため、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し、届出・申請等に直接確認結果を記載することとしている。
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	・届出書等の書類については、入力及び確認作業の完了後に施錠して保管している。 ・住記システム端末等のディスプレイは来庁者から見えない場所に設置している。
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又は個人番号を必要としない業務では、権限設定を行い個人番号が含まれない画面表示とする。 ・個人番号利用業務以外又は、個人番号を必要としない業務から住民情報の要求があった場合は、権限設定により個人番号を表示（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	他業務からアクセスされる住民情報の基本情報を保持するテーブルと、特定個人情報を含むデータベースを切り離して管理している。
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IDとパスワード及び静脈による認証を行っている。 ・認証後は、ユーザ毎に利用可能な機能を制限している。 ・パスワードについては、定期的に変更することを義務付けている。
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	・人事異動があった場合や権限変更があった場合には担当課内で閲覧権限等を書面にて決裁し、システムに反映させている。 ・ユーザIDやアクセス権限を定期的に確認し、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又は削除する。
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	・共用IDは発効せず、個人に対してユーザIDを発行する。 ・端末操作資格者のアクセス権限表を作成している。
特定個人情報の使用の記録	[記録を残している] ＜選択肢＞ 1）記録を残している 2）記録を残していない
具体的な方法	・端末から参照、更新した場合のアクセスログを記録している。 ・記録項目：処理更新日、処理更新時間、職員番号、宛名番号、世帯番号、改製番号、届出日、異動日、異動事由（詳細事由）、端末名、処理場所を記録する。 ・バックアップされた操作履歴は情報開示請求等に備えて操作ログ管理手順書に定められた期間、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	担当部署が定期的に実施する全庁的な情報セキュリティ研修等を通して、特定個人情報の業務外利用の禁止や漏えい時の罰則、アクセスログが確実に記録されていること等について、従業者に周知徹底する。
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	通常ユーザ用と管理者用にアクセス権限を分け、システムのバックアップデータ等の重要データには管理者権限のみがアクセスできるようにする。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置	
・端末機は、スクリーンセーバ等を利用して、長時間にわたり特定個人情報を表示させない。 ・特定個人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。	

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、個人情報保護や対策を目的として公共機関の認定・認証を取得していることを契約要件としているほか、事業実績など社会的信用と能力があることを確認している。	
特定個人情報ファイルの閲覧者・更新者の制限	[　制限している　]	<選択肢> 1）制限している　2）制限していない
具体的な制限方法	委託契約において、委託業務で取り扱う情報の目的外使用や複写等の禁止、委託業務の終了後の情報の消去及び消去内容の報告、委託業務で使用するパソコン等の盗難防止対策の実施、システム用IDの適切な管理等の対策の実施、情報セキュリティに関する教育の実施等、情報セキュリティの確保に必要な人的・物的・技術的対策の実施を義務づけている。	
特定個人情報ファイルの取扱いの記録	[　記録を残している　]	<選択肢> 1）記録を残している　2）記録を残していない
具体的な方法	・システムへのログイン記録やシステム保守における作業記録を残している。 ・電子記録媒体等については、管理簿を作成し、引渡し及び返却を管理する。	
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提供は認めていない。	
委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	・業務委託に関しては、仕様書等にて委託業務実施場所を本市が定める場所内に限定し、外部への持ち出しを禁止している。 ・本市より受領した情報資産を適切に管理するため、情報資産の受渡資産管理表を作成する。 ・貸与期間終了後は、受注者は、原本をすみやかに発注者に返却するものとする。また、複製品は廃棄するものとする。	
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	・委託契約において、委託業務で取り扱う情報の目的外使用や複写等の禁止、契約の終了後直ちに返還又は引渡しをするものとしている。 ・情報セキュリティに関する教育の実施等を義務付けている。	
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	・目的外利用の禁止 ・特定個人情報の閲覧者・更新者を制限 ・特定個人情報の提供先の限定 ・情報漏えいを防ぐための保管管理に責任を負う ・情報が不要になったとき又は要請があったときに情報の返還又は消去などの必要な措置を講じる ・保管期間の過ぎた特定個人情報及びそのバックアップを完全に消去する ・必要に応じて、本市が委託先の視察・監査を行うことができる ・再委託の原則禁止	
再委託先による特定個人情報ファイルの適切な取扱いの確保	[　十分に行っている　]	<選択肢> 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない　4）再委託していない
具体的な方法	契約書において、「受注者は、委託業務の処理を他に委託し、又は請け負わせてはならない。ただし、書面により発注者の承諾を得たときは、この限りでない。」としている。許可した場合は、通常の委託と同様の措置を義務づけている。	
その他の措置の内容	－	
リスクへの対策は十分か	[　十分である　]	<選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		
－		

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		[　　] 提供・移転しない
リスク1： 不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録	[　　記録を残している　　]	＜選択肢＞ 1）記録を残している　　2）記録を残していない
具体的な方法	移転は庁内ネットワークや庁内システム間連携のみであり、連携時のログ、アクセスログ等により記録する。	
特定個人情報の提供・移転に関するルール	[　　定めている　　]	＜選択肢＞ 1）定めている　　2）定めていない
ルールの内容及びルール遵守の確認方法	情報の提供・移転を行う場合、利用部署からデータ利用申請を提出させ、データ利用に関し法的根拠等があるかを調査し、許可されればデータ利用が可能となる。	
その他の措置の内容	設置された端末では、宮崎市情報セキュリティポリシーで定める情報セキュリティ管理者の許可がなければ情報の取り出しができないようにしている。	
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2： 不適切な方法で提供・移転が行われるリスク		
リスクに対する措置の内容	・庁内ネットワーク以外での提供・移転を禁止する。 ・既存システム相互間の連携はシステム上、番号法及び条例上認められる提供及び移転のみが行われる仕組みとなっており、不適切な方法で提供又は移転されることはない。	
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： 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク		
リスクに対する措置の内容	・庁内連携では、番号法及び条例にて規定された部署のみ照会可能となっている。 ・庁内連携では、本業務で保有する情報をすべて連携することは行わず、限定された情報のみ照会対象としている。 ・移転に関する連携システムでの十分な検証を行う。	
リスクへの対策は十分か	[　　十分である　　]	＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
特定個人情報の提供・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	＜中間サーバ・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。 ・中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 (※)情報提供ネットワークシステムを使用した特定個人情報の提供の要求の受領及び情報提供を行う機能。
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1) 特に力を入れている　2) 十分である 3) 課題が残されている
リスク6： 不適切な方法で提供されるリスク	
リスクに対する措置の内容	＜中間サーバ・ソフトウェアにおける措置＞ ・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。 ・中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 (※)暗号化・復号機能と、鍵情報及び照会許可用照合リストを管理する機能 ＜中間サーバ・プラットフォームにおける措置＞ ・中間サーバと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク(総合行政ネットワーク等)を利用することにより、不適切な方法で提供されるリスクに対応している。 ・中間サーバと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ・中間サーバ・プラットフォームの保守・運用を行う事業者においては、特定個人情報に係る業務にはアクセスができないよう管理を行い、不適切な方法での情報提供を行えないよう管理している。 ＜中間サーバの運用における措置＞ ・情報照会、情報提供の記録が逐一保存される仕組みが確立した庁内連携システムを通してやりとりすることで、不適切な方法で特定個人情報がやりとりされることを防止する。
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1) 特に力を入れている　2) 十分である 3) 課題が残されている

リスク7： 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク	
リスクに対する措置の内容	＜中間サーバ・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・ソフトウェアにおける措置＞ ・中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 ・情報連携においてのみ、情報提供用個人識別符号を用いることがシステム上担保されており、不正な名寄せが行われるリスクに対応している。 ＜中間サーバ・プラットフォームにおける措置＞ ・中間サーバと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ・中間サーバと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ・中間サーバ・プラットフォームでは、特定個人情報を管理するデータベースを地方公共団体ごとに区分管理（アクセス制御）しており、中間サーバ・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 ・特定個人情報の管理を地方公共団体のみが行うことで、中間サーバ・プラットフォームの保守・運用を行う事業者における情報漏えい等のリスクを極小化する。	

7. 特定個人情報の保管・消去		
リスク1： 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[政府機関ではない]	<選択肢> 1）特に力を入れて遵守している 2）十分に遵守している 3）十分に遵守していない 4）政府機関ではない
②安全管理体制	[十分に整備している]	<選択肢> 1）特に力を入れて整備している 2）十分に整備している 3）十分に整備していない
③安全管理規程	[十分に整備している]	<選択肢> 1）特に力を入れて整備している 2）十分に整備している 3）十分に整備していない
④安全管理体制・規程の職員への周知	[十分に周知している]	<選択肢> 1）特に力を入れて周知している 2）十分に周知している 3）十分に周知していない
⑤物理的対策	[十分に行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
具体的な対策の内容	＜本市における措置＞ ・サーバ設置場所に指紋認証装置や静脈認証装置を設置し、あらかじめ許可された者のみが入室できる。 ・記録媒体等については、耐火金庫を利用し施錠管理をしている。 ・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、施設内に消火設備の完備や消化器具の設置を行っている。 ＜中間サーバ・プラットフォームにおける措置＞ ・中間サーバ・プラットフォーム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室への入室を厳重に管理する。 ・特定個人情報は、サーバ室に設置された中間サーバのデータベース内に保存され、バックアップもデータベース上に保存される。	
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	＜本市における措置＞ ・ウイルス対策ソフトの定期的パターンファイルの更新を行っている。 ・外部ネットワークから遮断された独自のネットワークで運用することで、不正アクセス対策を行っている。 ＜中間サーバ・プラットフォームにおける措置＞ ・中間サーバ・プラットフォームではUTM（コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置）等を導入し、アクセス制限、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 ・中間サーバ・プラットフォームでは、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ・導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。	
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	住民基本台帳においては死者も除票住民票として管理しているため、現存者と同様の管理となっている。	
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： 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	住基法および同施行令に規定される届出および記載等があった都度、住民基本台帳ファイルへの入力、削除および修正を行うとともに、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）および第34条（調査）の規定に基づき、実態調査等を実施することにより、住記システムの情報が正確であることを確保する。	
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	住民基本台帳ファイルに記録された、住民票消除後のデータについて、住基法に定められた保存期間の経過後、年に1度内容を精査し処理を実施し、当該データが抹消されていることを確認する。また、紙・媒体により保管された当該データについては専門業者に物理抹消を委託する。	
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		
サーバ、端末（パソコン）、記録媒体、紙文書等の情報資産を廃棄する場合は、情報を復元できないように処置した上で廃棄する。機器リース終了による返却の場合も、同様とする。 ・紙文書は、溶解又はシュレッダー処分を行う。 ・電磁的な記録媒体は、破砕処理、電磁気破壊、データ消去ソフトウェアによるデータ消去を行った上で廃棄する。 ・サーバ、パソコン等情報機器については、記録装置に対し、物理破壊、磁気破壊、データ消去ソフトウェアによるデータ消去を行う。 ・データ消去を業者に委託した場合は、消去作業証明書を提出させる。		

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記システムに限定されるため、住記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・申請内容や身分証明書（個人番号カード等）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6－6　本人確認情報の通知及び記録）等により市町村CSにおいて住記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で検索できないようにするため、本人確認情報の検索条件として、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を住記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。
個人番号の真正性確認の措置の内容	・個人番号カード等の提示を受け、本人確認を行う。 ・出生等により新たに個人番号が指定される場合や、転入の際に個人番号カード若しくは通知カードと法令により定められた身分証明書の組み合わせの提示がない場合には、市町村CSにおいて本人確認情報と個人番号の紐付けの確認を行う。
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、帳票管理手順書に基づいて管理し、保管する。 ・本人確認情報に誤りがあった際に訂正を行う場合には、宮崎市情報セキュリティポリシーで定める情報セキュリティ管理者の許可を得て行うこととする。また、訂正した内容等については、その記録を残し、法令等により定められる期間保管する。
その他の措置の内容	システムでは対応できない事象が発生した際に、本人確認情報の正確性を維持するため、本人確認情報取扱手順書等に基づいて本人確認情報の入力、削除及び訂正が行われていることを定期的に確認する。
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、事務に必要のない情報との紐付けが行われるリスク		
宛名システム等における措置の内容	市町村CSと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へのアクセスは住記システムに限定しており、また、住記システムと市町村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のサーバ上には住基ネットの管理及び運用に必要なソフトウェア以外作動させず、また、市町村CSが設置されたセグメントにあるハブには権限の無い者が機器を接続できないよう、適切な対策（IPアドレスによる制限、使用可能ポートのフィルタリング等）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	・ユーザIDとパスワード及び静脈による認証を行っている。 ・認証後は、ユーザ毎に利用可能な機能を制限している。 ・パスワードについては、定期的に変更することを義務付けている。	
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	・人事異動があった場合や権限変更があった場合には書面にて決裁し、システムに反映させている。 ・ユーザIDやアクセス権限を定期的に確認し、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又は削除する。	
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	―	
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	担当部署が定期的に実施する全庁的な情報セキュリティ研修等を通して、特定個人情報の業務外利用の禁止や漏えい時の罰則、アクセスログが確実に記録されていること等について、従業者に周知徹底する。	
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		
・端末機は、スクリーンセーバ等を利用して、長時間にわたり特定個人情報を表示させない。 ・特定個人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。		

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、個人情報保護や対策を目的として公共機関の認定・認証を取得していることを契約要件としているほか、事業実績など社会的信用と能力があることを確認している。	
特定個人情報ファイルの閲覧者・更新者の制限	[　制限している　]	<選択肢> 1）制限している　2）制限していない
具体的な制限方法	委託契約において、委託業務で取り扱う情報の目的外使用や複写等の禁止、委託業務の終了後の情報の消去及び消去内容の報告、委託業務で使用するパソコン等の盗難防止対策の実施、システム用IDの適切な管理等の対策の実施、情報セキュリティに関する教育の実施等、情報セキュリティの確保に必要な人的・物的・技術的対策の実施を義務づけている。	
特定個人情報ファイルの取扱いの記録	[　記録を残している　]	<選択肢> 1）記録を残している　2）記録を残していない
具体的な方法	・システムへのログイン記録やシステム保守における作業記録を残している。 ・電子記録媒体等については、管理簿を作成し、引渡し及び返却を管理する。	
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提供は認めていない。	
委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	・業務委託に関しては、仕様書等にて委託業務実施場所を本市が定める場所内に限定し、外部への持ち出しを禁止している。 ・本市より受領した情報資産を適切に管理するため、情報資産の受渡資産管理表を作成する。 ・貸与期間終了後は、受注者は、原本をすみやかに発注者に返却するものとする。また、複製品は廃棄するものとする。	
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	・委託契約において、委託業務で取り扱う情報の目的外使用や複写等の禁止、契約の終了後直ちに返還又は引渡しをするものとしている。 ・情報セキュリティに関する教育の実施等を義務付けている。	
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	・目的外利用の禁止 ・特定個人情報の閲覧者・更新者を制限 ・特定個人情報の提供先の限定 ・情報漏えいを防ぐための保管管理に責任を負う ・情報が不要になったとき又は要請があったときに情報の返還又は消去などの必要な措置を講じる ・保管期間の過ぎた特定個人情報及びそのバックアップを完全に消去する ・必要に応じて、本市が委託先の視察・監査を行うことができる ・再委託の原則禁止	
再委託先による特定個人情報ファイルの適切な取扱いの確保	[　十分に行っている　]	<選択肢> 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない　4）再委託していない
具体的な方法	契約書において、「受注者は、委託業務の処理を他に委託し、又は請け負わせてはならない。ただし、書面により発注者の承諾を得たときは、この限りでない。」としている。許可した場合は、通常の委託と同様の措置を義務づけている。	
その他の措置の内容	－	
リスクへの対策は十分か	[　十分である　]	<選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		
－		

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）	[　　] 提供・移転しない
リスク1： 不正な提供・移転が行われるリスク	
特定個人情報の提供・移転の記録	[　　記録を残している　　] ＜選択肢＞ 1）記録を残している　2）記録を残していない
具体的な方法	特定個人情報（個人番号、4情報等）の提供を行う際に、提供記録（提供日時、操作者等）をシステム上で管理し、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	都道府県サーバと市町村CSの間の通信では相互認証を実施しているため、認証できない相手先への情報の提供はなされないことがシステム上担保される。
その他の措置の内容	・サーバ室等への入室権限及び本特定個人情報ファイルを扱うシステムへのアクセス権限を有する者を厳格に管理し、情報の持ち出しを制限する。 ・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　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	都道府県サーバと市町村CSの間の通信では相互認証を実施しているため、認証できない相手先への情報の提供はなされないことがシステム上担保される。また、媒体へ出力する必要がある場合には、逐一出力の記録が残される仕組みを構築する。
リスクへの対策は十分か	[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である　3）課題が残されている
リスク3： 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク	
リスクに対する措置の内容	誤った情報を提供・移転してしまうリスクへの措置 ：システム上、照会元から指定された検索条件に基づき得た結果を適切に提供・移転することを担保する。また、本人確認情報に変更が生じた際には、市町村CSへの登録時点で項目のフォーマットチェックや論理チェック（例えば、現存する住民に対して転入を異動事由とする更新が行われようとした場合や、転居を異動事由とする更新の際に住所以外の更新が行われようとした場合に当該処理をエラーとする）がなされた情報を通知することをシステム上で担保する。 誤った相手に提供・移転してしまうリスクへの措置 ：都道府県サーバと市町村CSの間の通信では相互認証を実施するため、認証できない相手先への情報の提供はなされないことがシステム上担保される。
リスクへの対策は十分か	[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である　3）課題が残されている
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置	
－	

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

7. 特定個人情報の保管・消去		
リスク1： 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[政府機関ではない]	<選択肢> 1）特に力を入れて遵守している 2）十分に遵守している 3）十分に遵守していない 4）政府機関ではない
②安全管理体制	[十分に整備している]	<選択肢> 1）特に力を入れて整備している 2）十分に整備している 3）十分に整備していない
③安全管理規程	[十分に整備している]	<選択肢> 1）特に力を入れて整備している 2）十分に整備している 3）十分に整備していない
④安全管理体制・規程の職員への周知	[十分に周知している]	<選択肢> 1）特に力を入れて周知している 2）十分に周知している 3）十分に周知していない
⑤物理的対策	[十分に行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
具体的な対策の内容	・サーバ設置場所に指紋認証装置や静脈認証装置を設置し、あらかじめ許可された者のみが入室できる。 ・記録媒体等については、耐火金庫を利用し施錠管理をしている。 ・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、施設内に消火設備の完備や消化器具の設置を行っている。	
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	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。 ：宮崎市住民基本台帳ネットワークシステム運用管理規程に基づき、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ソフトウェア管理手順書等を整備する。また、同規程に基づき、オペレーティングシステム管理に係る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 ：宮崎市住民基本台帳ネットワークシステム運用管理規程に基づき、ネットワークの適正な管理のため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、住民基本台帳法施行令第34条第3項（保存）に定める期間（150年間）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	CSの情報を基に住記システムとの整合処理を定期的に実施し、保存する本人確認情報が最新であるかどうかを確認することにより担保する。	
リスクへの対策は十分か	[十分である]	<選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている

リスク3： 特定個人情報が消去されずいつまでも存在するリスク		
消去手順		[定めている] <選択肢> 1）定めている 2）定めていない
	手順の内容	・システム上、住民基本台帳法施行令第34条第3項（保存）に定める期間（150年間）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、磁気ディスク管理手順書等に基づき、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、帳票管理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、帳票管理手順書等に基づき、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	送付先情報の入手元は住記システムに限定されるため、住記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・申請内容や身分証明書（運転免許証等）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6－6　本人確認情報の通知及び記録）等により市町村CSにおいて住記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で検索できないようにするため、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	－ ＜選択肢＞
リスクへの対策は十分か	[　十分である　] 1）特に力を入れている　2）十分である　3）課題が残されている
リスク2： 不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	送付先情報の入手元を住記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住記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（運転免許証等）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基づ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	住記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、住記システムから入手後、個人番号カード管理システムに送付先情報を送付した時点で役割を終える（不要となる）ため、送付後速やかに市町村CSから削除する。 そのため、入手から削除までのサイクルがごく短期間であることから、入手から削除の間の正確性を維持するための特段の対策は講じない。
その他の措置の内容	－
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、事務に必要のない情報との紐付けが行われるリスク		
宛名システム等における措置の内容	市町村CSと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へのアクセスは住記システムに限定しており、また、住記システムと市町村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のサーバ上には住基ネットの管理及び運用に必要なソフトウェア以外作動させず、また、市町村CSが設置されたセグメントにあるハブには権限の無い者が機器を接続できないよう、適切な対策（IPアドレスによる制限、使用可能ポートのフィルタリング等）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	・ユーザIDとパスワード及び静脈による認証を行っている。 ・認証後は、ユーザ毎に利用可能な機能を制限している。 ・パスワードについては、定期的に変更することを義務付けている。	
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	・人事異動があった場合や権限変更があった場合には書面にて決裁し、システムに反映させている。 ・ユーザIDやアクセス権限を定期的に確認し、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又は削除する。	
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	・送付先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	－	
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	担当部署が定期的に実施する全庁的な情報セキュリティ研修等を通して、特定個人情報の業務外利用の禁止や漏えい時の罰則、アクセスログが確実に記録されていること等について、従業者に周知徹底する。	
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		
・端末機は、スクリーンセーバ等を利用して、長時間にわたり特定個人情報を表示させない。 ・特定個人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。		

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、個人情報保護や対策を目的として公共機関の認定・認証を取得していることを契約要件としているほか、事業実績など社会的信用と能力があることを確認している。	
特定個人情報ファイルの閲覧者・更新者の制限	[　制限している　]	<選択肢> 1）制限している　2）制限していない
具体的な制限方法	委託契約において、委託業務で取り扱う情報の目的外使用や複写等の禁止、委託業務の終了後の情報の消去及び消去内容の報告、委託業務で使用するパソコン等の盗難防止対策の実施、システム用IDの適切な管理等の対策の実施、情報セキュリティに関する教育の実施等、情報セキュリティの確保に必要な人的・物的・技術的対策の実施を義務づけている。	
特定個人情報ファイルの取扱いの記録	[　記録を残している　]	<選択肢> 1）記録を残している　2）記録を残していない
具体的な方法	・システムへのログイン記録やシステム保守における作業記録を残している。 ・電子記録媒体等については、管理簿を作成し、引渡し及び返却を管理する。	
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提供は認めていない。	
委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	・業務委託に関しては、仕様書等にて委託業務実施場所を本市が定める場所内に限定し、外部への持ち出しを禁止している。 ・本市より受領した情報資産を適切に管理するため、情報資産の受渡資産管理表を作成する。 ・貸与期間終了後は、受注者は、原本をすみやかに発注者に返却するものとする。また、複製品は廃棄するものとする。	
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	・委託契約において、委託業務で取り扱う情報の目的外使用や複写等の禁止、契約の終了後直ちに返還又は引渡しをするものとしている。 ・情報セキュリティに関する教育の実施等を義務付けている。	
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	・目的外利用の禁止 ・特定個人情報の閲覧者・更新者を制限 ・特定個人情報の提供先の限定 ・情報漏えいを防ぐための保管管理に責任を負う ・情報が不要になったとき又は要請があったときに情報の返還又は消去などの必要な措置を講じる ・保管期間の過ぎた特定個人情報及びそのバックアップを完全に消去する ・必要に応じて、本市が委託先の視察・監査を行うことができる ・再委託の原則禁止	
再委託先による特定個人情報ファイルの適切な取扱いの確保	[　十分に行っている　]	<選択肢> 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない　4）再委託していない
具体的な方法	契約書において、「受注者は、委託業務の処理を他に委託し、又は請け負わせてはならない。ただし、書面により発注者の承諾を得たときは、この限りでない。」としている。許可した場合は、通常の委託と同様の措置を義務づけている。	
その他の措置の内容	－	

リスクへの対策は十分か	[十分である]	<選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		
―		
5．特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		**[ ]提供・移転しない**
リスク1： 不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録	[記録を残している]	<選択肢> 1）記録を残している 2）記録を残していない
具体的な方法	特定個人情報（個人番号、4情報等）の提供を行う際に、提供記録（提供日時、操作者等）をシステム上で管理し、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	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。	
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 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	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、住記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 ：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提供はなされないことがシステム上担保される。	
リスクへの対策は十分か	[十分である]	<選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置		
―		

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

7. 特定個人情報の保管・消去		
リスク1： 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[政府機関ではない]	<選択肢> 1）特に力を入れて遵守している 2）十分に遵守している 3）十分に遵守していない 4）政府機関ではない
②安全管理体制	[十分に整備している]	<選択肢> 1）特に力を入れて整備している 2）十分に整備している 3）十分に整備していない
③安全管理規程	[十分に整備している]	<選択肢> 1）特に力を入れて整備している 2）十分に整備している 3）十分に整備していない
④安全管理体制・規程の職員への周知	[十分に周知している]	<選択肢> 1）特に力を入れて周知している 2）十分に周知している 3）十分に周知していない
⑤物理的対策	[十分に行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
具体的な対策の内容	・サーバ設置場所に指紋認証装置や静脈認証装置を設置し、あらかじめ許可された者のみが入室できる。 ・記録媒体等については、耐火金庫を利用し施錠管理をしている。 ・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、施設内に消火設備の完備や消化器具の設置を行っている。	
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	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。 ：宮崎市住民基本台帳ネットワークシステム運用管理規程に基づき、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ソフトウェア管理手順書等を整備する。また、同規程に基づき、オペレーティングシステム管理に係る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 ：宮崎市住民基本台帳ネットワークシステム運用管理規程に基づき、ネットワークの適正な管理のため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、市町村では保管しない。そのため、送付先情報ファイルにおいて特定個人情報が古い情報のまま保管され続けるリスクは存在しない。	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク3： 特定個人情報が消去されずいつまでも存在するリスク		
消去手順	[定めている]	＜選択肢＞ 1）定めている 2）定めていない
手順の内容	システム上、保管期間の経過した特定個人情報を一括して削除する仕組みとする。	
その他の措置の内容	－	
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		
・送付先情報ファイルは、機構への特定個人情報の提供後、速やかに市町村CSから削除される。 ・その後、当該特定個人情報は機構において管理されるため、送付先情報ファイルのバックアップは取得しない予定である。		

Ⅳ　その他のリスク対策 ※

1. 監査		
①自己点検		[　　十分に行っている　　] ＜選択肢＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
	具体的なチェック方法	年に1回、担当部署（市民課等）内において実施している自己点検に用いるチェック項目に、「評価書の記載内容通りの運用がなされていること」に係る内容を追加し、運用状況を確認する。
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	宮崎市住民基本台帳ネットワークシステム運用管理規程に基づき、下記の監査を実施するものとする。 （1）内部監査 ：2年に1回、組織内に置かれた監査担当により、以下の観点による自己監査を実施し、監査結果を踏まえて体制や規定を改善する。 ・評価書記載事項と運用実態のチェック ・個人情報保護に関する規定、体制整備 ・個人情報保護に関する人的安全管理措置 ・職員の役割責任の明確化、安全管理措置の周知・教育 ・個人情報保護に関する技術的安全管理措置 （2）外部監査 ：民間機関等の外部監査事業者による監査を実施し、監査結果を踏まえて体制や規定を改善する。
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	宮崎市住民基本台帳ネットワークシステム運用管理規程に基づき、下記の研修を実施するものとする。 ・住基ネット関係職員(任用された派遣要員、非常勤職員、臨時職員等を含む。)に対して、初任時及び一定期間毎に、必要な知識の習得に資するための研修を実施するとともに、その記録を残している。 ・住基ネットの各責任者に対して、その管理に関する必要な知識や技術を習得させる研修を実施するとともに、その記録を残している。
3. その他のリスク対策		
＜中間サーバ･プラットフォームにおける措置＞ ・中間サーバ・プラットフォームを活用することにより、統一した設備環境による高レベルのセキュリティ管理（入退室管理等）、ITリテラシーの高い運用担当者によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用・監視を実現する。		

Ⅴ　開示請求、問合せ

1. 特定個人情報の開示・訂正・利用停止請求	
①請求先	宮崎市市民情報センター（市役所本庁舎3階） 〒880-8505　宮崎市橘通西一丁目1番1号
②請求方法	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：写しの交付を希望する場合は、別途コピー代が必要　　）
④個人情報ファイル簿の公表	［　行っていない　］　＜選択肢＞ 1) 行っている　2) 行っていない
個人情報ファイル名	－
公表場所	－
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	宮崎市地域振興部市民課（市役所本庁舎1階） 〒880-8505　宮崎市橘通西一丁目1番1号 電話番号0985-21-1752
②対応方法	問い合わせの受付時に受付票を起票し、対応について記録を残す。

Ⅵ　評価実施手続

1．基礎項目評価	
①実施日	令和2年6月12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	宮崎市パブリックコメント制度実施要綱に基づくパブリックコメント手続により意見聴取を実施する。実施に際しては、宮崎市ホームページ及び市民課、市民情報センター等において全文を閲覧できるようにした。
②実施日・期間	（初回）平成27年3月23日から4月21日（30日間） （再実施）令和3年1月12日から2月9日（30日間）
③期間を短縮する特段の理由	―
④主な意見の内容	（初回） ・項目一覧にページを記載してはどうか。 ・事務実施上の必要性について、災害対策に関する明確な記載がないのではないか。 ・評価実施機関における担当部署が市民課であるのはどうか。 ・担当部署内で行っている自己点検について、主語が明確ではない。 ・内部監査は「2年に1回」と記載しているが、評価書の見直しは「1年に1回」とあるがこの整合性はどうか。 ・内部監査を明確な要領又は手順書に従って確実に実施する。 ・外部監査の明確な定期監査が必要とされるのではないか。また、委託業者のISMS適合性評価可能な責任者を明確にする必要があるのではないか。 ・従業者に対して実施する研修について、必要な教育・訓練要領及び手順書に従って教育・訓練を実施プロセスを記録する。職員は要領や手順書は日常見られる状況として知識の高揚を図る。 （再実施） ・意見なし
⑤評価書への反映	（初回） ・項目一覧にページを記載した。 ・担当部署内で行っている自己点検について、「担当部署内において実施している」を「担当部署である市民課が実施している」と変更し、主語を明確にした。 （再実施） なし
3．第三者点検	
①実施日	令和3年3月15日
②方法	宮崎市個人情報保護審査会による第三者点検を実施した。
③結果	評価書の内容は、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取扱いプロセスごとに分析し、そのリスクを軽減させるために適切な措置を講じていると認められるとのことで了解を得た。
4．特定個人情報保護委員会の承認 【行政機関等のみ】	
①提出日	
②特定個人情報保護委員会による審査	

（別添3）変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
平成28年4月1日	Ⅰ－6－②法令上の根拠		74、85の2の項を追加	事前	法改正に伴う変更
平成28年4月1日	Ⅰ－7－②所属長	課長　毛利　博	課長　内藤　和弘	事後	人事異動に伴う変更
平成28年4月1日	Ⅱ（住民基本台帳ファイル）－2－⑤保有開始日	平成27年9月予定	平成27年9月24日	事後	予定の削除
平成28年4月1日	Ⅱ（住民基本台帳ファイル）－3－⑨使用開始日	平成27年10月5日予定	平成27年10月5日	事後	予定の削除
平成28年4月1日	Ⅱ（住民基本台帳ファイル）－4－⑨再委託事項	システム運用状況の管理、バッチジョブ運用、リハーサル支援、障害発生時の対応支援等	システム運用状況の管理、バッチジョブ運用、リハーサル（事前検証）支援、障害発生時の対応支援等	事後	文言の補記
平成28年4月1日	Ⅱ（住民基本台帳ファイル）－5－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（ 40 ）件	[○] 提供を行っている（ 57 ）件 [○] 移転を行っている（ 41 ）件	事前	法改正に伴う変更
平成28年4月1日	（別紙1） 番号法第19条第7号別表第二に定める事務		提供先No.35、39の追加	事前	法改正に伴う変更
平成28年4月1日	（別紙2） 番号法第9条第1項別表第一に定める事務		移転先No.33の追加	事前	法改正に伴う変更
平成28年4月1日	Ⅱ（本人確認情報ファイル）－2－⑤保有開始日	平成27年9月予定	平成27年9月24日	事後	予定の削除
平成28年4月1日	Ⅱ（本人確認情報ファイル）－3－⑨使用開始日	平成27年9月予定	平成27年10月5日	事後	予定の削除
平成28年4月1日	Ⅱ（送付先情報ファイル）－2－⑤保有開始日	平成27年10月予定	平成27年10月5日	事後	予定の削除
平成28年4月1日	Ⅱ（送付先情報ファイル）－3－⑨使用開始日	平成27年10月5日予定	平成27年10月5日	事後	予定の削除
平成28年4月1日	Ⅲ（住民基本台帳ファイル）－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	・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。 ・法務省からの通知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。	・住基ネットを通じての情報の入手は対象者以外の情報を入手できないような検索方法になっている。 ・法務省からの通知は対象者以外の情報を入手できないような検索方法になっている。	事後	文言の修正
平成28年4月1日	Ⅲ（住民基本台帳ファイル）－2－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	・住基ネットを通じての入手は、必要な情報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。 ・法務省からの通知は必要な情報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。	・住基ネットを通じての入手は、必要な情報以外の情報を入手できないような検索方法になっている。 ・法務省からの通知は必要な情報以外の情報を入手できないような検索方法になっている。	事後	文言の修正
平成28年4月1日	Ⅲ（住民基本台帳ファイル）－2－リスク1－その他の措置の内容	住民基本台帳ファイルを照会する他部署には各部署にとって必要な項目のみを表示させている。	住民基本台帳ファイルを照会する他部署には、権限設定を行い各部署にとって必要な項目のみを表示させている。	事後	文言の修正
平成28年4月1日	Ⅲ（住民基本台帳ファイル）－2－リスク2－リスクに対する措置の内容	・システムを利用する必要がある職員を特定し、ユーザIDによる識別とパスワードによる認証を実施している。また、認証後は利用機能の認可機能により、その職員がシステム上で利用可能な機能を制限することで不適切な方法で入手が行えない対策を施している。	・システムを利用する必要がある職員を特定し、ユーザIDによる識別とパスワードによる認証を実施している。また、認証後は権限設定により、その職員がシステム上で利用可能な機能を制限することで不適切な方法で入手が行えない対策を施している。	事後	文言の修正
平成28年4月1日	Ⅲ（住民基本台帳ファイル）－2－リスク3－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。	職員が対象者から身分証明書（個人番号カード等）の提示を受け、本人確認を行う。	事後	文言の修正
平成28年4月1日	Ⅲ（住民基本台帳ファイル）－2－リスク3－特定個人情報の正確性確保の措置の内容	住民基本台帳情報の入力、削除及び訂正を行う際は、整合性を確保するため、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し、届出・申請等の様式の行政側使用欄に確認結果を記載することとしている。	住民基本台帳情報の入力、削除及び訂正を行う際は、整合性を確保するため、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し、届出・申請等に直接確認結果を記載することとしている。	事後	文言の修正
平成28年4月1日	Ⅲ（住民基本台帳ファイル）－3－リスク1－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又は個人番号を必要としない業務では、個人番号が含まれない画面表示とする。 ・個人番号利用業務以外又は、個人番号を必要としない業務から住民情報の要求があった場合は、個人番号が含まれない情報のみを提供するような仕組みを構築する。	・個人番号利用業務以外又は個人番号を必要としない業務では、権限設定を行い個人番号が含まれない画面表示とする。 ・個人番号利用業務以外又は、個人番号を必要としない業務から住民情報の要求があった場合は、権限設定により個人番号を表示（提供）しない。	事後	文言の修正

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
平成28年4月1日	Ⅲ（住民基本台帳ファイル）－3－リスク2－アクセス権限の発効・失効の管理　具体的な管理方法	・人事異動があった場合や権限変更があった場合には書面にて決裁し、システムに反映させている。	・人事異動があった場合や権限変更があった場合には担当課内で閲覧権限等を書面にて決裁し、システムに反映させている。	事後	文言の修正
平成28年4月1日	Ⅲ（住民基本台帳ファイル）－3－リスク2－特定個人情報の使用の記録　具体的な方法	・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。	・バックアップされた操作履歴は情報開示請求等に備えて操作ログ管理手順書に定められた期間、保管する。	事後	文言の修正
平成28年4月1日	Ⅲ（住民基本台帳ファイル）－3－リスク3－リスクに対する措置の内容	定期的に実施する情報セキュリティ研修等を通して、特定個人情報の業務外利用の禁止や漏えい時の罰則、アクセスログが確実に記録されていること等について、従業者に周知徹底する。	担当部署が定期的に実施する全庁的な情報セキュリティ研修等を通して、特定個人情報の業務外利用の禁止や漏えい時の罰則、アクセスログが確実に記録されていること等について、従業者に周知徹底する。	事後	文言の修正
平成28年4月1日	Ⅲ（住民基本台帳ファイル）－5－リスク1－その他の措置の内容	設置された端末では、権限を持った職員の許可がなければ情報の取り出しができないようにしている。	設置された端末では、宮崎市情報セキュリティポリシーで定める情報セキュリティ管理者の許可がなければ情報の取り出しができないようにしている。	事後	文言の修正
平成28年4月1日	Ⅲ（住民基本台帳ファイル）－7－リスク3－消去手順　手順の内容	住民基本台帳ファイルに記録された、住民票消除後のデータについて、住基法に定められた保存期間の経過後、年に1度内容を精査し処理を実施し、当該データが物理抹消されていることを確認する。	住民基本台帳ファイルに記録された、住民票消除後のデータについて、住基法に定められた保存期間の経過後、年に1度内容を精査し処理を実施し、当該データが抹消されていることを確認する。また、紙・媒体により保管された当該データについては専門業者に物理抹消を委託する。	事後	文言の修正
平成28年4月1日	Ⅲ（本人確認情報ファイル）－2－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	・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。	・正当な利用目的以外で検索できないようにするため、本人確認情報の検索条件として、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。	事後	文言の修正
平成28年4月1日	Ⅲ（本人確認情報ファイル）－2－リスク3－特定個人情報の正確性確保の措置の内容	・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。 ・本人確認情報に誤りがあった際に訂正を行う場合には、本人確認情報管理責任者の許可を得て行うこととする。また、訂正した内容等については、その記録を残し、法令等により定められる期間保管する。	・入力、削除及び訂正作業に用いた帳票等は、帳票管理手順書に基づいて管理し、保管する。 ・本人確認情報に誤りがあった際に訂正を行う場合には、宮崎市情報セキュリティポリシーで定める情報セキュリティ管理者の許可を得て行うこととする。また、訂正した内容等については、その記録を残し、法令等により定められる期間保管する。	事後	文言の修正
平成28年4月1日	Ⅲ（本人確認情報ファイル）－2－リスク3－その他の措置の内容	システムでは対応できない事象が発生した際に、本人確認情報の正確性を維持するため、要領・手順書等に基づいて本人確認情報の入力、削除及び訂正が行われていることを定期的に確認する。	システムでは対応できない事象が発生した際に、本人確認情報の正確性を維持するため、本人確認情報取扱手順書等に基づいて本人確認情報の入力、削除及び訂正が行われていることを定期的に確認する。	事後	文言の修正
平成28年4月1日	Ⅲ（本人確認情報ファイル）－3－リスク3－リスクに対する措置の内容	定期的に実施する情報セキュリティ研修等を通して、特定個人情報の業務外利用の禁止や漏えい時の罰則、アクセスログが確実に記録されていること等について、従業者に周知徹底する。	担当部署が定期的に実施する全庁的な情報セキュリティ研修等を通して、特定個人情報の業務外利用の禁止や漏えい時の罰則、アクセスログが確実に記録されていること等について、従業者に周知徹底する。	事後	文言の修正
平成28年4月1日	Ⅲ（本人確認情報ファイル）－5－リスク1－特定個人情報の提供・移転に関するルール　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・移転を行う。	都道府県サーバと市町村CSの間の通信では相互認証を実施しているため、認証できない相手先への情報の提供はなされないことがシステム上担保される。	事後	文言の修正
平成28年4月1日	Ⅲ（本人確認情報ファイル）－7－リスク1－⑥技術的対策　具体的な対策の内容	不正プログラム対策 ：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。	不正プログラム対策 ：宮崎市住民基本台帳ネットワークシステム運用管理規程に基づき、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ソフトウェア管理手順書等を整備する。また、同規程に基づき、オペレーティングシステム管理に係る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 ：宮崎市住民基本台帳ネットワークシステム運用管理規程に基づき、ネットワークの適正な管理のためファイアウォールを導入する。	事後	文言の修正

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
平成28年4月1日	Ⅲ（本人確認情報ファイル）－7－リスク2－リスクに対する措置の内容	住記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。	住基GW（ゲートウェイ）から送付される情報を基に住記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。	事後	文言の修正
平成28年4月1日	Ⅲ（本人確認情報ファイル）－7－リスク3－消去手順　手順の内容	・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。	・磁気ディスクの廃棄時は、磁気ディスク管理手順書等に基づき、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、帳票管理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、帳票管理手順書等に基づき、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。	事後	文言の修正
平成28年4月1日	Ⅲ（送付先情報ファイル）－2－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	・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。	・正当な利用目的以外で検索できないようにするため、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。	事後	文言の修正
平成28年4月1日	Ⅲ（送付先情報ファイル）－3－リスク3－リスクに対する措置の内容	定期的に実施する情報セキュリティ研修等を通して、特定個人情報の業務外利用の禁止や漏えい時の罰則、アクセスログが確実に記録されていること等について、従業者に周知徹底する。	担当部署が定期的に実施する全庁的な情報セキュリティ研修等を通して、特定個人情報の業務外利用の禁止や漏えい時の罰則、アクセスログが確実に記録されていること等について、従業者に周知徹底する。	事後	文言の修正
平成28年4月1日	Ⅲ（送付先情報ファイル）－5－リスク1－特定個人情報の提供・移転に関するルール　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・移転を行う。	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。	事後	文言の修正
平成28年4月1日	Ⅲ（送付先情報ファイル）－7－リスク1－⑥技術的対策　具体的な対策の内容	不正プログラム対策 ：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。	不正プログラム対策 ：宮崎市住民基本台帳ネットワークシステム運用管理規程に基づき、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ソフトウェア管理手順書等を整備する。また、同規程に基づき、オペレーティングシステム管理に係る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 ：宮崎市住民基本台帳ネットワークシステム運用管理規程に基づき、ネットワークの適正な管理のためファイアウォールを導入する。	事後	文言の修正
平成28年4月1日	Ⅳ－1－①自己点検　具体的なチェック方法	年に1回、担当部署内において実施している自己点検に用いるチェック項目に、「評価書の記載内容通りの運用がなされていること」に係る内容を追加し、運用状況を確認する。	年に1回、担当部署（市民課等）内において実施している自己点検に用いるチェック項目に、「評価書の記載内容通りの運用がなされていること」に係る内容を追加し、運用状況を確認する。	事後	文言の修正
平成28年4月1日	Ⅳ－1－②監査　具体的なチェック方法		宮崎市住民基本台帳ネットワークシステム運用管理規程に基づき、下記の監査を実施するものとする。	事後	文言の追加
平成28年4月1日	Ⅳ－2－従業者に対する教育・啓発　具体的な方法		宮崎市住民基本台帳ネットワークシステム運用管理規程に基づき、下記の研修を実施するものとする。	事後	文言の追加
平成29年4月1日	Ⅰ－6－②法令上の根拠		・項番117を削除 ・項番120を119に変更	事後	法改正に伴う変更
平成29年4月1日	Ⅰ－7－②所属長	課長　内藤　和弘	課長　大賀　ユキ	事後	人事異動に伴う変更
平成29年4月1日	Ⅱ（住民基本台帳ファイル）－5－提供・移転の有無	[○] 提供を行っている（ 57 ）件 [○] 移転を行っている（ 41 ）件	[○] 提供を行っている（ 56 ）件 [○] 移転を行っている（ 40 ）件	事後	重要な変更でないため
平成29年4月1日	（別紙1）　番号法第19条第7号別表第二に定める事務		・項番117を削除 ・項番120を119に変更	事後	法改正に伴う変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
平成29年4月1日	（別紙2） 番号法第9条第1項別表第一に定める事務	・項番7 健康管理部健康支援課 ・項番8 福祉部子ども課 ・項番9 福祉部子育て支援課 ・項番10 健康管理部健康支援課 ・項番15 福祉部社会福祉課 ・項番37 福祉部子育て支援課 ・項番43 福祉部子育て支援課 ・項番44 福祉部子育て支援課 ・項番45 福祉部子育て支援課 ・項番49 健康管理部健康支援課 ・項番56 福祉部子ども課 ・項番63 福祉部社会福祉課 ・項番84 健康管理部健康支援課 ・項番94 福祉部子ども課	・項番7 福祉部子ども未来局親子保健課 ・項番8 削除 ・項番9 福祉部子ども未来局子育て支援課 ・項番10 健康管理部健康支援課、福祉部子ども未来局親子保健課 ・項番15 福祉部社会福祉第一課・第二課 ・項番37 福祉部子ども未来局子育て支援課 ・項番43 福祉部子ども未来局子育て支援課 ・項番44 福祉部子ども未来局子育て支援課 ・項番45 福祉部子ども未来局子育て支援課 ・項番49 福祉部子ども未来局親子保健課 ・項番56 福祉部子ども未来局保育幼稚園課 ・項番63 福祉部社会福祉第一課 ・項番84 福祉部子ども未来局親子保健課 ・項番94 福祉部子ども未来局保育幼稚園課	事後	重要な変更でないため
平成29年4月1日	Ⅲ（住民基本台帳ファイル）－2－リスク2－リスクに対する措置の内容	・システムを利用する必要がある職員を特定し、ユーザIDによる識別とパスワードによる認証を実施している。	・システムを利用する必要がある職員を特定し、ユーザIDによる識別とパスワード及び静脈による認証を実施している。	事後	重要な変更でないため
平成29年4月1日	Ⅲ（住民基本台帳ファイル）－3－リスク2－具体的な管理方法	・ユーザIDとパスワードによる認証を行っている。	・ユーザIDとパスワード及び静脈による認証を行っている。	事後	重要な変更でないため
平成29年4月1日	Ⅲ（本人確認情報ファイル）－3－リスク2－具体的な管理方法	・ユーザIDとパスワードによる認証を行っている。	・ユーザIDとパスワード及び静脈による認証を行っている。	事後	重要な変更でないため
平成29年4月1日	Ⅲ（送付先情報ファイル）－3－リスク2－具体的な管理方法	・ユーザIDとパスワードによる認証を行っている。	・ユーザIDとパスワード及び静脈による認証を行っている。	事後	重要な変更でないため
平成30年4月1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7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、101、102、103、105、106、108、111、112、113、114、116、119の項） （別表第二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）	・番号法第19条第7号（特定個人情報の提供の制限）及び別表第二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日内閣府・総務省令第7号。以下「別表第二主務省令」という。） [情報提供の根拠] ・別表第二 （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、101、102、103、105、106、108、111、112、113、114、116、119の項） ・別表第二主務省令 （1、2、3、4、6、7、8、10、12、13、14、16、20、22、22条の3、22条の4、23、24、24条の2、24条の3、25、26条の3、27、28、31、31条の2、31条の3、32、33、37、38、39、40、41、43、43条の3、43条の4、44条の2、45、47、48、49条の2、50、51、53、55、56、57、58、59、59条の2、59条の3） [情報照会の根拠] なし（情報提供ネットワークによる情報照会は行わない）	事後	重要な変更事項でないため
平成30年4月1日	（別紙2） 番号法第9条第1項別表第一に定める事務	・項番14 建設部住宅課 ・項番32 建設部住宅課	・項番14 建設部建築住宅課 ・項番32 建設部建築住宅課	事後	重要な変更でないため
平成30年7月1日	Ⅵ 評価実施手続 1. 基礎項目評価 ①実施日	平成27年3月17日	平成30年7月1日	事後	重要な変更事項でないため
令和1年6月28日	Ⅰ－7－②所属長	課長 大賀 ユキ	課長	事後	重要な変更事項でないため
令和1年6月27日	Ⅱ 特定個人情報ファイル概要 （住民基本台帳ファイル） 2. 基本情報 ④記録されている項目 主な記録項目	[ ]医療保険関係情報 [ ]児童福祉・子育て関係情報 [ ]介護・高齢者福祉関係情報 [ ]年金関係情報	[○]医療保険関係情報 [○]児童福祉・子育て関係情報 [○]介護・高齢者福祉関係情報 [○]年金関係情報	事後	重要な変更事項でないため
令和1年6月27日	Ⅱ 特定個人情報ファイル概要 （住民基本台帳ファイル） 3特定個人情報の入手・使用 ①入手元	【○】行政機関・独立行政法人等（機構）	【○】行政機関・独立行政法人等（ ）	事後	重要な変更事項でないため
令和1年6月27日	Ⅱ 特定個人情報ファイル概要 （住民基本台帳ファイル） （別添2）特定個人情報ファイル記録項目		51. カナ旧字 52. 旧氏	事後	重要な変更事項でないため
令和1年6月27日	Ⅱ 特定個人情報ファイル概要 （本人確認情報ファイル） （別添2）特定個人情報ファイル記録項目		37. カナ旧字 38. 旧氏	事後	重要な変更事項でないため
令和1年6月27日	Ⅱ 特定個人情報ファイル概要 （送付先情報ファイル） （別添2）特定個人情報ファイル記録項目		62. ローマ字旧氏	事後	重要な変更事項でないため
令和1年6月27日	Ⅵ 評価実施手続 ①実施日	平成27年3月17日	令和1年6月28日	事後	重要な変更事項でないため

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6月12日	Ⅰ基本情報 1. 特定個人情報ファイルを取り扱う事務 ②事務の内容	なお、9. の「個人番号の通知及び個人番号カードの交付」に係る事務については、行政手続における特定の個人を識別するための番号の利用等に関する法律の規定による通知カード及び個人番号カード並びに情報提供ネットワークシステムによる特定個人情報の提供等に関する省令（平成26年11月20日総務省令第85号）（以下、「通知カード及び個人番号カード省令」という。）第35条（通知カード、個人番号カード関連事務の委任）により機構に対する事務の一部の委任が認められている。	なお、9. の「個人番号の通知及び個人番号カードの交付」に係る事務については、行政手続における特定の個人を識別するための番号の利用等に関する法律の規定による個人番号、個人番号カード、特定個人情報の提供等に関する省令（平成26年11月20日総務省令第85号）（以下、「個人番号通知書、個人番号カード省令」という。）第35条（個人番号通知書、個人番号カード関連事務の委任）により機構に対する事務の一部の委任が認められている。	事後	法改正に伴う変更
令和2年6月12日	Ⅰ基本情報 2. 特定個人情報を取り扱う事務において使用するシステム ②システムの機能	7. 送付先情報通知 ：個人番号の通知に係る事務の委任先である機構において、住民に対して番号通知書類(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、住記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。	7. 送付先情報通知 ：個人番号の通知に係る事務の委任先である機構において、住民に対して番号通知書類(個人番号通知書、個人番号カード交付申請書（以下、「交付申請書」という。）等)を送付するため、住記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。	事後	法改正に伴う変更
令和2年6月12日	Ⅰ基本情報 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	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。（通知カード及び個人番号カード省令第35条（通知カード、個人番号カード関連事務の委任）により機構に対する事務の一部の委任が認められている。）	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。（個人番号通知書、個人番号カード省令第35条（個人番号通知書、個人番号カード関連事務の委任）により機構に対する事務の一部の委任が認められている。）	事後	法改正に伴う変更
令和2年6月12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7号（特定個人情報の提供の制限）及び別表第二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日内閣府・総務省令第7号。以下「別表第二主務省令」という。） [情報提供の根拠] ・別表第二 （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、101、102、103、105、106、108、111、112、113、114、116、119の項） ・別表第二主務省令 （1、2、3、4、6、7、8、10、12、13、14、16、20、22、22条の3、22条の4、23、24、24条の2、24条の3、25、26条の3、27、28、31、31条の2、31条の3、32、33、37、38、39、40、41、43、43条の3、43条の4、44条の2、45、47、48、49条の2、50、51、53、55、56、57、58、59、59条の2、59条の3） [情報照会の根拠] なし（情報提供ネットワークによる情報照会は行わない）	・番号法第19条第7号（特定個人情報の提供の制限）及び別表第二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日内閣府・総務省令第7号。以下「別表第二主務省令」という。） [情報提供の根拠] ・別表第二 （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、101、102、103、105、106、108、111、112、113、114、116、117、120の項） ・別表第二主務省令 （1、2、3、4、6、7、8、10、12、13、14、16、20、22、22条の3、22条の4、23、24、24条の2、24条の3、25、26条の3、27、28、31、31条の2、31条の3、32、33、37、38、39、40、41、43、43条の3、43条の4、44条の2、45、47、48、49条の2、50、51、53、55、56、57、58、59、59条の2、59条の2の2、59条の3） [情報照会の根拠] なし（情報提供ネットワークによる情報照会は行わない）	事後	法改正に伴う変更
令和2年6月12日	Ⅱ特定個人情報ファイルの概要 （3）送付先情報ファイル 2. ③対象となる本人の範囲 その必要性	番号法第7条第1項（指定及び通知）に基づき、通知カードを個人番号の付番対象者全員に送付する必要がある。 また、同法第17条第1項（個人番号カードの交付等）により、個人番号カードは通知カードと引き換えに交付することとされていることから、合わせて、交付申請書を通知カード送付者全員に送付する必要がある。 市町村は、通知カード及び個人番号カード省令第35条（通知カード・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、個人番号通知書を個人番号の付番対象者全員に送付する必要がある。 また、同法第17条第1項（個人番号カードの交付等）により、個人番号カードは通知カードと引き換えに交付することとされていることから、合わせて、交付申請書を通知カード送付者全員に送付する必要がある。 市町村は、個人番号通知書、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機構に委任する。	事後	法改正に伴う変更
令和2年6月12日	Ⅱ特定個人情報ファイルの概要 （3）送付先情報ファイル 2. ④記録される項目　その妥当性	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、通知カード及び個人番号カード省令第35条（通知カード・個人番号カード関連事務の委任）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、個人番号カードの券面記載事項のほか、通知カード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。	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、個人番号通知書、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、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。	事後	法改正に伴う変更
令和2年6月12日	Ⅱ特定個人情報ファイルの概要 （3）送付先情報ファイル 3. ⑤本人への明示	通知カード及び個人番号カード省令第35条（通知カード・個人番号カード関連事務の委任）に記載されている。	個人番号通知書、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）に記載されている。	事後	法改正に伴う変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和2年6月12日	Ⅱ特定個人情報ファイルの概要 (3)送付先情報ファイル 3. ⑥使用目的	通知カード及び個人番号カード省令第35条(通知カード・個人番号カード関連事務の委任)に基づく委任を受けて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行う機構に対し、通知カード及び交付申請書の送付先情報を提供するため。	個人番号通知書、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、通知カード及び交付申請書の送付先情報を提供するため。	事後	法改正に伴う変更
令和2年6月12日	Ⅱ特定個人情報ファイルの概要 (3)送付先情報ファイル 3. ⑦使用方法	住記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(住記システム→市町村CS又は電子記録媒体→個人番号カード管理システム(機構))。	住記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(住記システム→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))。	事後	法改正に伴う変更
令和2年6月12日	Ⅱ特定個人情報ファイルの概要 (3)送付先情報ファイル 5. ①法令上の根拠	通知カード及び個人番号カード省令第35条(通知カード、個人番号カード関連事務の委任)	個人番号通知書、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)	事後	法改正に伴う変更
令和2年6月12日	Ⅵ 評価実施手続 1. 基礎項目評価 ①実施日	令和1年6月28日	令和2年6月12日	事後	重要な変更事項でないため
令和2年6月12日	Ⅵ 評価実施手続 2. 国民・住民等からの意見の聴取 ②実施日・期間	平成27年3月23日から4月21日(30日間)	(初回)平成27年3月23日から4月21日(30日間) (再実施)令和3年1月12日から2月9日(30日間)	事後	重要な変更事項でないため
令和2年6月12日	Ⅵ 評価実施手続 4. 主な意見の内容 ②実施日・期間	・項目一覧にページを記載してはどうか。 ・事務実施上の必要性について、災害対策に関する明確な記載がないのではないか。 ・評価実施機関における担当部署が市民課であるのはどうか。 ・担当部署内で行っている自己点検について、主語が明確ではない。 ・内部監査は「2年に1回」と記載しているが、評価書の見直しは「1年に1回」とあるがこの整合性はどうか。 ・内部監査を明確な要領又は手順書に従って確実に実施する。 ・外部監査の明確な定期監査が必要とされるのではないか。また、委託業者のISMS適合性評価可能な責任者を明確にする必要があるのではないか。 ・従業者に対して実施する研修について、必要な教育・訓練要領及び手順書に従って教育・訓練を実施プロセスを記録する。職員は要領や手順書は日常見られる状況として知識の高揚を図る。	(初回) ・項目一覧にページを記載してはどうか。 ・事務実施上の必要性について、災害対策に関する明確な記載がないのではないか。 ・評価実施機関における担当部署が市民課であるのはどうか。 ・担当部署内で行っている自己点検について、主語が明確ではない。 ・内部監査は「2年に1回」と記載しているが、評価書の見直しは「1年に1回」とあるがこの整合性はどうか。 ・内部監査を明確な要領又は手順書に従って確実に実施する。 ・外部監査の明確な定期監査が必要とされるのではないか。また、委託業者のISMS適合性評価可能な責任者を明確にする必要があるのではないか。 ・従業者に対して実施する研修について、必要な教育・訓練要領及び手順書に従って教育・訓練を実施プロセスを記録する。職員は要領や手順書は日常見られる状況として知識の高揚を図る。 (再実施) ・意見なし	事後	重要な変更事項でないため
令和2年6月12日	Ⅵ 評価実施手続 5. 評価書への反映 ②実施日・期間	・項目一覧にページを記載した。 ・担当部署内で行っている自己点検について、「担当部署内において実施している」を「担当部署である市民課が実施している」と変更し、主語を明確にした。	(初回) ・項目一覧にページを記載した。 ・担当部署内で行っている自己点検について、「担当部署内において実施している」を「担当部署である市民課が実施している」と変更し、主語を明確にした。 (再実施) なし	事後	重要な変更事項でないため