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	住民基本台帳ネットワークに係る本人確認情報の管理及び提供等に関する事務　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

宮崎県は、住民基本台帳ネットワークに係る本人確認情報の管理及び提供等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当たり、特定個人情報ファイルの取扱いが個人のプライバシー等の権利利益に影響を及ぼしかねないことを認識し、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適切な措置を講じ、もって個人のプライバシー等の権利、利益の保護に取り組んでいることを宣言する。

特記事項	・住民基本台帳ネットワークにおいて、都道府県知事は、住民基本台帳法に基づき市町村から住民の本人確認情報に関する通知を受け、都道府県サーバに都道府県知事保存本人確認情報として保有する。都道府県知事保存本人確認情報は、4情報（「氏名・住所・生年月日・性別」をいう。）、個人番号、住民票コード及びこれらの変更情報に限定される。 ・住基ネットは専用回線を使用し、地方公共団体情報システム機構が管理するファイアウォールにより厳重な通信制御を行うなど厳格な不正アクセス対策を講じている。また、内部による不正利用の防止のため、アクセス管理を行い、端末操作者を限定し、操作履歴を保存する等の対策を講じている。 ・都道府県サーバーは全都道府県分を1か所（集約センター）に集約し、その運用・監視を地方公共団体情報システム機構に委託している。

評価実施機関名

宮崎県知事

特定個人情報保護委員会　承認日　【行政機関等のみ】

公表日

平成27年6月4日

[平成26年4月　様式4]

項目一覧

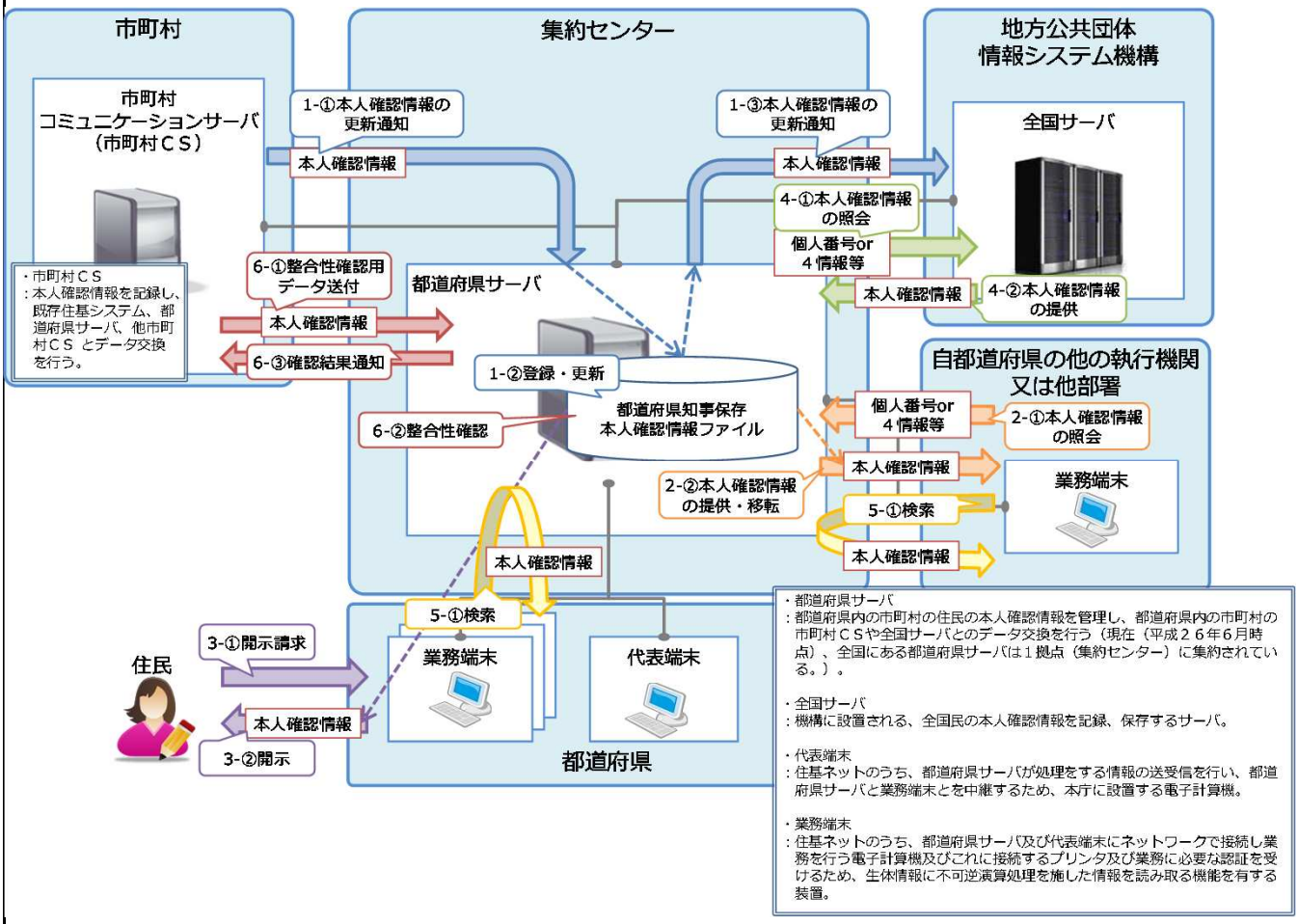
Ⅰ　基本情報

1．特定個人情報ファイルを取り扱う事務	
①事務の名称	住民基本台帳ネットワークに係る本人確認情報の管理及び提供等に関する事務
②事務の内容　※	宮崎県は、住民基本台帳法（昭和42年法律第81号。以下「住基法」という。）に基づき、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（以下「住基ネット」という。）を県内市町村と共同して構築している。 なお、住民基本台帳は、住基法に基づき作成されるものであり、市町村における住民の届出に関する制度及びその住民たる地位を記録する各種の台帳に関する制度を一元化し、もって、住民の利便を増進するとともに、情報技術の発達に伴う行政の近代化に対処するため、住民に関する記録を正確かつ統一的に行うものであり、市町村においては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。 具体的に宮崎県では、住基法の規定に従い、以下の事務で特定個人情報を取り扱う。 ①　磁気ディスクによる特定個人情報ファイルの管理 ②　市町村からの本人確認情報に係る変更の通知に基づく特定個人情報ファイルの更新及び地方公共団体情報システム機構（以下「機構」という。）への通知 ③　宮崎県知事から本人確認情報に係る宮崎県の他の執行機関への提供又は他部署への移転 ④　住民による請求に基づく当該個人の本人確認情報の開示並びに開示結果に基づく住民からの本人確認情報の訂正、追加又は削除の申出に対する調査 ⑤　機構への本人確認情報の照会
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 都道府県知事保存本人確認情報ファイルを最新の状態に保つため、市町村ＣＳ（※1）を経由して通知された本人確認情報の更新情報を元に当該ファイルを更新し、全国サーバ（※2）に対して当該本人確認情報の更新情報を通知する。 2　宮崎県の他の執行機関への情報提供又は他部署への移転 宮崎県の他の執行機関又は他部署による住基法に基づく情報照会に対応するため、照会のあった当該個人の個人番号又は4情報（氏名、住所、性別、生年月日の4情報。以下同じ。）等に対応する本人確認情報を都道府県知事保存本人確認情報ファイルから抽出し、照会元に提供・移転する。 3　本人確認情報の開示 法律に基づく住民による自己の本人確認情報の開示請求に対応するため、当該個人の本人確認情報を都道府県知事保存本人確認情報ファイルから抽出し、帳票に出力する。 4　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。 5　本人確認情報検索 都道府県サーバの代表端末又は業務端末において入力された4情報の組合せをキーに都道府県知事保存本人確認情報ファイルを検索し、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。 6　本人確認情報整合 都道府県知事保存本人確認情報ファイルの正確性を担保するため、市町村から本人確認情報を受領し、当該本人確認情報を用いて当該ファイルに記録された本人確認情報の整合性確認を行う。 ※1　市町村ＣＳとは、本人確認情報を記録し、既存住基システム、都道府県サーバ、他市町村ＣＳとデータ交換を行う、市町村コミュニケーションサーバのことをいう。 ※2　全国サーバとは、住民基本台帳法第30条の11第1項の規定により都道府県知事から指定情報処理機関に通知された全国民の本人確認情報を記録、保存するサーバのことをいう。
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　（　）

3．特定個人情報ファイル名	
都道府県知事保存本人確認情報ファイル	
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	宮崎県では、都道府県知事保存本人確認情報ファイルを、次に記載する必要性から取り扱う。 都道府県知事保存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　市町村の区域を越えた住民基本台帳に関する事務（住基ネットに係る本人確認情報の管理及び提供等に関する事務）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　市町村からの本人確認情報の更新情報の通知を受けて都道府県知事保存本人確認情報ファイルを更新し、当該更新情報を機構に対して通知する。 ③　宮崎県の他の執行機関又は他部署からの照会に基づき、本人確認情報を提供・移転する。 ④　住民からの請求に基づき、当該個人の本人確認情報を開示する。 ⑤　住基ネットに係る本人確認情報の管理及び提供等に関する事務において、本人確認情報を検索する。 ⑥　市町村において保存する本人確認情報との整合性を確認する。
②実現が期待されるメリット	・行政手続の際、本人確認情報を利用することによって、市町村が発行する住民票の写しの添付を省略することができ、住民の負担（市町村を訪問し、住民票の写しの交付を受けるという金銭的、時間的コストの節約）軽減につながるとともに、行政機関においても、より正確な本人確認の把握や事務の省力化など行政運営の適正化・効率化につながることが見込まれる。
5．個人番号の利用　※	
法令上の根拠	・住基法（平成25年5月31日法律第28号が施行された時点での条文を表示しています。） ○第7条（住民票の記載事項） ○第12条の5（住民基本台帳の脱漏等に関する都道府県知事の通報） ○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7（都道府県知事から機構への本人確認情報の通知等） ○第30条の8（本人確認情報の誤りに関する機構の通報） ○第30条の11（通知都道府県以外の都道府県の執行機関への本人確認情報の提供） ○第30条の15（本人確認情報の利用） ○第30条の32（自己の本人確認情報の開示） ○第30条の35（自己の本人確認情報の訂正）
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	[　　実施しない　　] ＜選択肢＞ 1）実施する 2）実施しない 3）未定
②法令上の根拠	ー
7．評価実施機関における担当部署	
①部署	宮崎県総務部市町村課
②所属長	総務部参事兼市町村課長　平原　利明
8．他の評価実施機関	
ー	

（別添1）事務の内容



（備考）

1　本人確認情報の更新に関する事務
　1-①.市町村において受け付けた住民の異動に関する情報を、市町村ＣＳを通じて都道府県サーバに通知する。
　1-②.都道府県サーバにおいて、市町村より受領した本人確認情報を元に都道府県知事保存本人確認情報ファイルを更新する。
　1-③.機構に対し、住民基本台帳ネットワークを介して、本人確認情報の更新を通知する。
2　宮崎県の他の執行機関への情報提供又は他部署への移転
　2-①.宮崎県の他の執行機関又は他部署において、個人番号又は4情報等をキーワードとした本人確認情報の照会を行う。
　2-②.宮崎県知事において、提示されたキーワードを元に都道府県知事保存本人確認情報ファイルを検索し、照会元に対し、当該個人の本人確認情報を提供する。
　※検索対象者が他都道府県の場合は全国サーバに対して検索の要求を行う。
　※一括提供の方式により本人確認情報を提供する場合には、宮崎県知事名において代表端末を操作し、電子記録媒体を用いて提供・移転する。
3　本人確認情報の開示に関する事務
　3-①.住民より本人確認情報の開示請求を受け付ける。
　3-②.開示請求者（住民）に対し、都道府県知事保存本人確認情報ファイルに記録された当該個人の本人確認情報を開示する。
4　機構への情報照会に係る事務
　4-①.機構に対し、個人番号又は4情報等をキーワードとした本人確認情報の照会を行う。
　4-②.機構より、当該個人の本人確認情報を受領する。
5　本人確認情報検索に関する事務
　5-①.4情報の組み合わせを検索キーに、都道府県知事保存本人確認情報ファイルを検索する。
6　本人確認情報整合
　6-①.市町村ＣＳより、都道府県サーバに対し、整合性確認用の本人確認情報を送付する。
　6-②.都道府県サーバにおいて、市町村ＣＳより受領した整合性確認用の本人確認情報を用いて都道府県知事保存本人確認情報ファイルの整合性確認を行う。
　6-③.都道府県サーバより、市町村ＣＳに対して整合性確認結果を通知する。

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		
都道府県知事保存本人確認情報ファイル		
2．基本情報		
①ファイルの種類　※		[　　システム用ファイル　　]　＜選択肢＞ 1）システム用ファイル 2）その他の電子ファイル（表計算ファイル等）
②対象となる本人の数		[　100万人以上1,000万人未満　]　＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
③対象となる本人の範囲　※		・宮崎県内の住民（県内のいずれかの市町村において、住基法第5条（住民基本台帳の備付け）により住民基本台帳に記録された住民のことを指す。） ・この場合、住民基本台帳に記録されていた者で、転出等の事由により住民票が消除（死亡による消除を除く。）された者を含む。
	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（都道府県知事保存本人確認情報ファイル）において宮崎県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。
④記録される項目		[　10項目以上50項目未満　]　＜選択肢＞ 1）10項目未満　2）10項目以上50項目未満 3）50項目以上100項目未満　4）100項目以上
	主な記録項目　※	・識別情報 [○] 個人番号　[　] 個人番号対応符号　[　] その他識別情報（内部番号） ・連絡先等情報 [○] 4情報（氏名、性別、生年月日、住所）　[　] 連絡先（電話番号等） [○] その他住民票関係情報 ・業務関係情報 [　] 国税関係情報　[　] 地方税関係情報　[　] 健康・医療関係情報 [　] 医療保険関係情報　[　] 児童福祉・子育て関係情報　[　] 障害者福祉関係情報 [　] 生活保護・社会福祉関係情報　[　] 介護・高齢者福祉関係情報 [　] 雇用・労働関係情報　[　] 年金関係情報　[　] 学校・教育関係情報 [　] 災害関係情報 [　] その他　（　　）
	その妥当性	・個人番号、4情報、その他住民票関係情報 住基ネットを通じて本人確認を行うために必要な情報として、住民票の記載等に係る本人確認情報（個人番号、4情報、住民票コード及びこれらの変更情報）を記録する必要がある。
	全ての記録項目	別添2を参照。
⑤保有開始日		平成27年6月予定
⑥事務担当部署		宮崎県総務部市町村課行政担当

3．特定個人情報の入手・使用		
①入手元 ※		[　　] 本人又は本人の代理人 [　　] 評価実施機関内の他部署　（　　） [　　] 行政機関・独立行政法人等　（　　） [○] 地方公共団体・地方独立行政法人　（　　） [　　] 民間事業者　（　　） [　　] その他　（　　）
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　（市町村ＣＳを通じて入手する　）
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
④入手に係る妥当性		・住民に関する情報の変更又は新規作成の際は、市町村がそれをまず探知した上で、全国的なシステムである住基ネットで管理する必要があるので、市町村から宮崎県へ、宮崎県から機構へと通知することとされているため
⑤本人への明示		・宮崎県知事が当該市町村の区域内の住民の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）に規定されている。
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（都道府県知事保存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 ※	宮崎県総務部市町村課行政担当
	使用者数	[　10人未満　] ＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
⑧使用方法 ※		・市町村長からの住民票の記載事項の変更又は新規作成の通知を受け(既存住基システム→市町村ＣＳ→都道府県サーバ)、都道府県知事保存本人確認情報ファイルを更新し、機構に対して当該本人確認情報の更新情報を通知する（都道府県サーバ→全国サーバ）。 ・宮崎県の他の執行機関又は他部署からの本人確認情報の照会要求を受け（宮崎県の他の執行機関又は他部署→都道府県サーバ）、照会のあった住民票コード、個人番号又は4情報の組合せを元に都道府県知事保存本人確認情報ファイルを検索し、該当する個人の本人確認情報を照会元へ提供・移転する（都道府県サーバ→宮崎県の他の執行機関又は他部署）。 ・住民からの開示請求に基づき（住民→都道府県窓口→都道府県サーバ）、当該住民の本人確認情報を都道府県知事保存本人確認情報ファイルから抽出し、書面により提供する（都道府県サーバ→帳票出力→住民）。 ・4情報の組合せをキーに都道府県知事保存本人確認情報ファイルの検索を行う。 ・都道府県知事保存本人確認情報ファイルの正確性を担保するため、市町村から本人確認情報を受領し（市町村ＣＳ→都道府県サーバ）、当該本人確認情報を用いて都道府県知事保存本人確認情報ファイルに記録された本人確認情報の整合性確認を行う。
	情報の突合 ※	・都道府県知事保存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都道府県知事保存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。 ・宮崎県の他の執行機関又は他部署からの照会に基づいて本人確認情報を提供・移転する際に、照会元から受信した対象者の4情報等との突合を行う。 ・請求に基づいて本人確認情報を開示する際に、開示請求者から受領した本人確認情報との突合を行う。 ・市町村ＣＳとの整合処理を実施するため、4情報等との突合を行う。
	情報の統計分析 ※	・住基法第30条の15第1項第4号（本人確認情報の利用）の規定により統計資料の作成を行う場合、情報の統計分析を行うことがある。 ・また、本人確認情報の更新件数や提供件数等の集計を行う。
	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6月1日

4．特定個人情報ファイルの取扱いの委託		
委託の有無 ※		[委託する] ＜選択肢＞ 1）委託する 2）委託しない （ 1 ） 件
委託事項1		都道府県サーバの運用及び監視に関する業務
①委託内容		・全国の都道府県サーバを1拠点（都道府県サーバ集約センター。以下「集約センター」という。）に集約化することとしたことに伴い、都道府県サーバの運用及び監視に関する業務を集約センター運用者に委託する。 ・委託する業務は、直接本人確認情報に係わらない（直接本人確認情報にアクセスできず、閲覧・更新・削除等を行わない）業務を対象とする。
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体] ＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	[100万人以上1,000万人未満] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲 ※	「2．③対象となる本人の範囲」に同じ
	その妥当性	・本特定個人情報ファイル（都道府県知事保存本人確認情報ファイル）が保存される都道府県サーバの運用及び監視業務を委託することによる。 ・なお、「①委託内容」のとおり、委託事項は直接本人確認情報に係わらない事務を対象としているため、委託先においては、特定個人情報ファイルに記録された情報そのものを扱う事務は実施しない。
③委託先における取扱者数		[10人未満] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[○] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [ ] その他 （ ）
⑤委託先名の確認方法		宮崎県情報公開条例に基づく開示請求
⑥委託先名		地方公共団体情報システム機構
再委託	⑦再委託の有無 ※	[再委託する] ＜選択肢＞ 1）再委託する 2）再委託しない
	⑧再委託の許諾方法	書面による承諾
	⑨再委託事項	・都道府県サーバの運用及び監視に関する業務。再委託する業務は、直接本人確認情報に係わらない（直接本人確認情報にアクセスできず、閲覧・更新・削除等を行わない）業務を対象とする。

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 （ 3 ）件 [○] 移転を行っている （ 1 ）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
①法令上の根拠	住基法第30条の7（都道府県知事から機構への本人確認情報の通知等）
②提供先における用途	都道府県知事より受領した本人確認情報を元に機構保存本人確認情報ファイルを更新する。
③提供する情報	住民票コード、氏名、生年月日、性別、住所、個人番号、異動事由、異動年月日
④提供する情報の対象となる本人の数	[100万人以上1,000万人未満] ＜選択肢＞ 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤提供する情報の対象となる本人の範囲	「2．③対象となる本人の範囲」に同じ
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 （ 住民基本台帳ネットワークシステム ）
⑦時期・頻度	市町村長からの通知に基づいて都道府県知事保存本人確認情報ファイルの更新を行った都度
提供先2	宮崎県の他の執行機関
①法令上の根拠	住基法第30条の15第2項（本人確認情報の利用）
②提供先における用途	・住基法別表第六に掲げる、宮崎県の他の執行機関への情報提供が認められる事務（例：教育委員会における特別支援学校への就学のため必要な経費の支弁に関する事務等）の処理に用いる。
③提供する情報	・住民票コード、氏名、生年月日、性別、住所、個人番号、異動事由、異動年月日 ※住民票コードについては、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施行に伴う関係法律の整備等に関する法律（平成25年5月31日法律第28号。以下「番号整備法」という。）第20条第9項及び第22条第7項の規定による経過措置である。
④提供する情報の対象となる本人の数	[100万人以上1,000万人未満] ＜選択肢＞ 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤提供する情報の対象となる本人の範囲	「2．③対象となる本人の範囲」に同じ
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 （ 住民基本台帳ネットワークシステム ）
⑦時期・頻度	宮崎県の他の執行機関からの情報照会の要求があった都度

提供先3	住基法上の住民
①法令上の根拠	住基法第30条の32（自己の本人確認情報の開示）
②提供先における用途	開示された情報を確認し、必要に応じてその内容の全部又は一部の訂正、追加又は削除の申出を行う。
③提供する情報	住民票コード、氏名、住所、生年月日、性別、個人番号、異動事由、異動年月日
④提供する情報の対象となる本人の数	[　100万人以上1,000万人未満　] ＜選択肢＞ 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤提供する情報の対象となる本人の範囲	「2．③対象となる本人の範囲」に同じ
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　（　　）
⑦時期・頻度	開示請求があった都度
移転先1	宮崎県の他部署
①法令上の根拠	住基法第30条の15第1項（本人確認情報の利用）
②移転先における用途	・住基法別表第五に掲げる、都道府県知事において都道府県知事保存本人確認情報の利用が認められた事務の処理に用いる。
③移転する情報	・住民票コード、氏名、生年月日、性別、住所、個人番号、異動事由、異動年月日 ※住民票コードについては、番号整備法第20条第9項及び第22条第7項の規定による経過措置である。
④移転する情報の対象となる本人の数	[　100万人以上1,000万人未満　] ＜選択肢＞ 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤移転する情報の対象となる本人の範囲	「2．③対象となる本人の範囲」に同じ
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　（住民基本台帳ネットワークシステム　）
⑦時期・頻度	宮崎県の他部署からの検索要求があった都度

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館管理をしている集約センターにおいて、施錠管理及び入退室管理（監視カメラを設置してサーバ設置場所への入退室者を特定・管理）を行っている部屋に設置したサーバ内に保管する。サーバへのアクセスはID／パスワードによる認証が必要となる。 ・宮崎県においては、施錠管理を行う部屋で端末類を保管する。
②保管期間	期間	[　　20年以上　　] ＜選択肢＞ 1）1年未満　2）1年　3）2年 4）3年　5）4年　6）5年 7）6年以上10年未満　8）10年以上20年未満　9）20年以上 10）定められていない
	その妥当性	・住民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、住基法施行令第30条の6（都道府県における本人確認情報の保存期間）に定める期間（150年間）保管する。
③消去方法		・都道府県知事保存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		
ー		

（別添2）特定個人情報ファイル記録項目

都道府県知事保存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　生年月日、6　性別、7　住所、8　外字数（住所）、9　個人番号、10　異動事由、11　異動年月日、12　保存期間フラグ、13　清音化かな氏名、14　市町村コード、15　大字・字コード、16　操作者ID、17　操作端末ID、18　タイムスタンプ、19　通知を受けた年月日、20　外字フラグ、21　削除フラグ、22　更新順番号、23　氏名外字変更連番、24　住所外字変更連番

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	
都道府県知事保存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	・都道府県知事保存本人確認情報ファイルにおける特定個人情報の入手手段は、市町村ＣＳからの本人確認情報更新要求の際に通知される本人確認情報に限定される。この場合、市町村ＣＳから対象者以外の情報が通知されてしまうことがリスクとして想定されるが、制度上、対象者の真正性の担保は市町村側の確認に委ねられるため、市町村において厳格な審査を行われることが前提となる。
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	・システム上、法令により市町村から通知を受けることとされている情報のみを入手できることとする。
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市町村ＣＳ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	・住民の異動情報の届出等を受け付ける市町村の窓口において、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	・システム上、市町村において真正性が確認された情報のみを市町村ＣＳを通じて入手できることとする。
特定個人情報の正確性確保の措置の内容	・システム上、本人確認情報更新の際に、論理チェックを行う（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）仕組みとする。 ・入手元である市町村ＣＳにおいて、項目（フォーマット、コード）のチェックを実施する。
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。 ・市町村ＣＳと接続するネットワーク回線に専用回線を用いるとともに、情報の暗号化を実施する等の措置を講じる。 ・特定個人情報の入手は、システム上自動処理にて行われるため、操作者は存在せず人為的なアクセスが行われることはない。 ※都道府県サーバのサーバ上で稼動するアプリケーション。 　各都道府県の市町村の住民の本人確認情報を管理し、各都道府県の市町村の市町村ＣＳや全国サーバとのデータ交換を行う。 　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。
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	・都道府県サーバ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	・庁内システムと都道府県サーバとの接続は行わない。	
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2： 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク		
ユーザ認証の管理	[行っている]	＜選択肢＞ 1) 行っている 2) 行っていない
具体的な管理方法	・生体認証による操作者認証を行う。	
アクセス権限の発効・失効の管理	[行っている]	＜選択肢＞ 1) 行っている 2) 行っていない
具体的な管理方法	・操作者名簿を調製し、アクセス権限を適切に管理する。 ・人事異動等により操作者権限解除の申請があったときは、直ちに照合情報を削除し、アクセス権限を無効化する。	
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	・アクセス権限の付与に際し、十分に審査した上で、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、都道府県サーバの検索サブシステムからアプリケーションの操作履歴を記録し、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。	
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)を記録し、保管する。 ・不適正な操作がないことについて、操作履歴により適時確認し、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、直ちに実態調査を行う。 ・定期的に監査を実施するとともに、システム利用職員を対象とする研修会において、業務外利用の禁止等について指導する。	
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
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。 ・定期運用に基づくバックアップ以外にファイルを複製しないよう、委託先を監督する。 ・本人確認情報が記載された帳票等は、必要最小限で行い、施錠可能な保管庫等で厳重に保管するとともに、廃棄の際には、情報が復元できないよう必要な措置を講じる。	
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当たり、次の措置を講じる。 ○セキュリティ責任者（所属長）は、業務端末のログオフを徹底させる。 ○窓口での来庁者対応を考慮し、本人確認情報の長時間表示を避けるために、スクリーンセーバ等を利用する。 ○業務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。 ○本人確認情報の開示・訂正の請求に対し、適切に対応する。 ○本人確認情報の提供状況の開示請求に対し、適切に対応する。		

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		・宮崎県住民基本台帳ネットワークシステムセキュリティ規程（平成19年訓令第7号）第6章「委託の管理」に基づき確認する。 ・外部委託をしようとする場合には、あらかじめ委託を受けようとする者における情報の保護に関する管理体制等について調査し、委託する。 ・委託先との委託契約書には、情報の保護に関し、再委託の禁止又は制限に関すること、情報が記録された資料の保管、返還又は廃棄に関すること、情報が記録された資料の目的外使用、複製及び複写並びに第三者への提供の禁止、情報の秘密保持、事故等の報告を明記する。 ・必要に応じて、委託先におけるセキュリティ対策の実施状況を調査する。
特定個人情報ファイルの閲覧者・更新者の制限	[　制限している　]	＜選択肢＞ 1）制限している　2）制限していない
具体的な制限方法		・作業者を限定するため、委託先に従事者名簿を提出させる。 ・委託する業務は、都道府県知事本人確認情報ファイルに直接アクセス業務ではないため、こららの権限を付与しない。
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		・委託契約書等に基づき、委託業務が実施されていることを適時確認するとともに、その記録を残す。 ・委託先から適時セキュリティ対策の実施状況の報告を受けるとともに、その記録を保存する。
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		・委託業務に関して知り得た特定個人情報の目的外使用及び第三者への提供を一切認めないことを委託契約書に明記する。 ・委託契約書の報告条項に基づき、定期的に特定個人情報の取扱いについて書面で報告させ、必要があれば委託業務に立ち会い、監督する。
委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法		・委託先に特定個人情報を提供する場合には、日付、件数等を記録した記録簿を作成し、保存する。 ・必要に応じ、委託業務に立ち会い、その履行状況を確認する。
特定個人情報の消去ルール	[　定めている　]	＜選択肢＞ 1）定めている　2）定めていない
ルールの内容及びルール遵守の確認方法		・委託契約書に、保管期間の過ぎた特定個人情報は自動判別するシステムを用いて消去すること、紙媒体は保管期間ごとに仕分保管し、保存期間が経過したものは外部業者が溶解処理すること、特定個人情報のデータが紙か否かを問わず、廃棄の際には履歴を作成し保存すること、特定個人情報と同様に保管期間が経過したバックアップデータは自動判別するシステムを用いて消去すること等を措置する旨規定する。 ・定期的に特定個人情報の取扱について書面で報告させ、必要に応じ現地調査ができることとする。
委託契約書中の特定個人情報ファイルの取扱いに関する規定	[　定めている　]	＜選択肢＞ 1）定めている　2）定めていない
規定の内容		・秘密の保持（契約終了又は解除後も同様） ・本人確認情報の管理 ・個人情報の保護 ・再委託の禁止（事前に宮崎県知事の書面による承諾を得た場合を除く） ・収集の制限 ・適正管理 ・目的外利用及び提供の禁止 ・複写又は持ち出しの禁止 ・資料等の返還又は廃棄 ・従事者への周知 ・事故発生時における報告
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、特定個人情報に直接関係のない業務を対象とする。 ・再委託を認める場合には、秘密保護に係る条項とともに、再委託先の業務について、委託先がすべての責任を負う旨の条項を設ける。
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・移転を行う際に、提供・移転の記録（提供・移転日時、操作者等）をシステム上で管理し、7年分保存する。なお、システム上、提供・移転に係る処理を行ったものの提供・移転が認められなかった場合についても記録を残す。
特定個人情報の提供・移転に関するルール	[　　定めている　　] ＜選択肢＞ 1）定めている　2）定めていない
ルールの内容及びルール遵守の確認方法	・番号法及び住基法並びに宮崎県個人情報保護条例（平成14年条例第41号）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、マニュアルどおりに特定個人情報の提供・移転を行う。
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、必要に応じて媒体へのデータ出力（書き込み）の際に職員が立会う。
リスクへの対策は十分か	[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2： 不適切な方法で提供・移転が行われるリスク	
リスクに対する措置の内容	・相手方（全国サーバ）と都道府県サーバ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、宮崎県の他の執行機関への提供及び他の部署への移転のため、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として、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。 ・誤った相手に提供・移転してしまうリスクへの措置として、相手方（全国サーバ）と都道府県サーバの間の通信では相互認証を実施しているため、認証できない相手先への情報の提供はなされないことがシステム上担保される。
リスクへの対策は十分か	[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置	
－	

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

7．特定個人情報の保管・消去		
リスク1： 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[政府機関ではない]	<選択肢> 1) 特に力を入れて遵守している 2) 十分に遵守している 3) 十分に遵守していない 4) 政府機関ではない
②安全管理体制	[十分に整備している]	<選択肢> 1) 特に力を入れて整備している 2) 十分に整備している 3) 十分に整備していない
③安全管理規程	[十分に整備している]	<選択肢> 1) 特に力を入れて整備している 2) 十分に整備している 3) 十分に整備していない
④安全管理体制・規程の職員への周知	[十分に周知している]	<選択肢> 1) 特に力を入れて周知している 2) 十分に周知している 3) 十分に周知していない
⑤物理的対策	[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
具体的な対策の内容	・都道府県サーバの集約センターにおいては、監視カメラを設置してサーバ設置場所への入退室者を特定し、管理するとともに、サーバ設置場所、記録媒体の保管場所を施錠管理する。 ・宮崎県においては、代表端末及び記録媒体の保管場所を施錠管理するとともに、業務端末設置場所を施錠管理する。	
⑥技術的対策	[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
具体的な対策の内容	・ＯＳのセキュリティホールに対するセキュリティ更新プログラムや住基ネット業務アプリケーションの修正プログラム、ウイルス対策ソフトのパターンファイルを配信される都度、更新する。 ・都道府県サーバの集約センター及び庁内ネットワークにおいて、ファイアウォールを導入し、ログの解析を行う。	
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	・生存する個人の個人番号とともに、死亡による消除後、住基法施行令第30条の６（都道府県における本人確認情報の保存期間）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	・市町村の住民基本台帳で本人確認情報の変更があった場合には住基ネットを通して本人確認情報の更新が行われる仕組みとなっているため、古い情報のまま保管されることはない。 ・また、市町村ＣＳ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。	
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法令（住基法施行令第30条の６）に定める保存期間を経過した後にシステム的に消去する。 ・帳票については、要領等に基づき、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、廃棄時には、焼却、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		
－		

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、住基ネットを利用所属において実施している自己点検チェックリストに、「評価書の記載の内容どおりの運用がなされていること」の項目を追加し、運用状況を把握する。
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	・年に1回、住基ネットを利用する所属に対し、自己点検チェックリストの結果とともに、次の項目により内部監査を実施する。 ◯評価書記載事項と運用実態との適合状況を確認 ◯個人情報保護に関する規程の遵守状況を確認 ◯個人情報利用事務に係る端末の管理状況、アクセス管理状況を確認 ◯職員の役割責任の明確化の状況、安全管理措置の周知状況を確認 ◯その他セキュリティ上必要と認める事項を確認 ・監査結果を踏まえ、体制等を改善するとともに、必要に応じて規程等を見直す。
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	・端末を操作する全職員を対象とした住基ネット担当者セキュリティ研修会を年1回開催する。 ・異動により新たに端末を操作することとなった職員を対象に、住基ネットの仕組みや操作方法、セキュリティ対策及び緊急時の対応を中心に初任者操作研修会を開催する。
3．その他のリスク対策		
ー		

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	〒８８０－８５０１ 宮崎市橘通東２丁目１０番１号 宮崎県総務部市町村課　行政担当　０９８５－２６－７１１６
②請求方法	・知事が保有する個人情報の保護等に関する規則（平成15年規則第２号）に基づく指定様式の提出により開示・訂正等の請求を受け付ける。
特記事項	－
③手数料等	[　　有料　　]　＜選択肢＞ 1) 有料　2) 無料 （手数料額、納付方法：書面の交付の場合には、１枚10円を前納する。　）
④個人情報ファイル簿の公表	[　行っていない　]　＜選択肢＞ 1) 行っている　2) 行っていない
個人情報ファイル名	－
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	宮崎県総務部市町村課行政担当（０９８５－２６－７１１６）
②対応方法	問合わせの内容について受付票を作成し、対応について記録する。

Ⅵ　評価実施手続

1．基礎項目評価	
①実施日	平成27年6月1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	・宮崎県パブリック・コメント手続（県民意見募集手続）実施要綱に基づき、意見を募集する。意見募集の実施に関しては、県のホームページに意見募集を周知し、ホームページ、担当部署及び情報センターにおいて、全項目評価書が閲覧できるようにする。 ・また、意見は、郵送、ＦＡＸ、電子メールで受け付ける。
②実施日・期間	平成27年2月12日（木）から平成27年3月13日（金）まで
③期間を短縮する特段の理由	－
④主な意見の内容	・Ⅰ－2－②－1において、「市町村ＣＳ」や「全国サーバ」についての言語定義が必要ではないか。 ・Ⅲ－②－リスク3において、対象者以外の情報の入手を防ぐためのリスク対策としてどのような対策を行うか、管理責任者と操作者の役割分担など、具体的に記載した手順書が必要ではないか。 ・Ⅲ－2－リスク4において、最近ＳＳＬサーバ証明書を悪用し、正規のウェブサイトを騙るフィッシング詐欺被害が増えているので注意を要する。 ・Ⅲ－4において、委託先機関にはＩＳＭＳ認証を取得した組織体制であることや内部監査・外部監査を受ける体制が確立されていることが求められる。
⑤評価書への反映	・Ⅰ－2－②に、「市町村ＣＳ」及び「全国サーバ」の言語定義について追記した。
3．第三者点検	
①実施日	平成27年3月25日（水）
②方法	宮崎県個人情報保護審議会による点検を受けた。
③結果	宮崎県個人情報保護審議会から以下のとおり意見を受けた。 1　本評価書案は、特定個人情報評価指針（平成26年4月18日特定個人情報保護委員会告示第4号）に定める適合性及び妥当性等に照らし妥当なものと認められる。 2　付言 　特定個人情報の評価書（案）に記載された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するための措置等を実施し、これらの発生を抑制し、特定個人情報を適切に管理すること。
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