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

奈良県は、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	・奈良県知事は、住民基本台帳法（以下「住基法」という。）に基づき、住民の利便の増進と国及び地方公共団体の行政の合理化に資するため、全国共通の本人確認を行うために必要最小限の住民の本人確認情報のみ保有する。具体的には、4情報（氏名、性別、生年月日、住所。以下同じ。）、個人番号、住民票コード及びこれらの変更情報であり、社会保障給付情報や所得額などの社会保障・税・災害対策業務情報は保有しない。 ・内部による不正利用の防止のため、システム操作者に住基法に基づく守秘義務を課し、生体認証により操作者を限定、システムの操作履歴を保存、照会条件を限定する等の対策を講じている。 ・外部との接続にあたっては、専用回線および専用交換装置で構成されたネットワークを介して行い、県および地方公共団体情報システム機構（以下「機構」という。）が管理するファイアウォールによる厳重な通信制御、侵入検知システム（IDS）による侵入検知、通信相手となるコンピュータとの相互認証、通信データの暗号化、通信プロトコルに独自のアプリケーションを用いる等の厳格な不正アクセス対策を講じている。 ・都道府県サーバは全都道府県分を1か所（集約センター）に集約し、その運用・監視を機構に委託している。 ・番号制度の運用において発生する、団体内統合宛名システムとの本人確認情報の突合及び中間サーバとの符号取得要求受け渡し時の情報連携において、都道府県サーバの代表端末または業務端末側と団体内統合宛名システムに受渡し専用フォルダを設けて、要求ファイル等の受け渡しを行うことで、電子記録媒体の紛失等のリスクがなくなり、情報連携時のセキュリティ向上が見込まれる。

評価実施機関名

奈良県知事

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3月27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　※	奈良県（以下「県」という。）は、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を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住所に関する届出等の簡素化を図り、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合理化を図るため、住民の住所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、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。 県では、住基法の規定に基づき、特定個人情報（都道府県知事保存本人確認情報）を以下の事務で取り扱う。（別添1を参照） 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県知事から本人確認情報に係る県の他の執行機関への提供または他部署への移転 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、追加又は削除の申し出に対する調査 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 ※「3. 特定個人情報ファイル名」に示す「都道府県知事保存本人確認情報ファイル」は、住民基本台帳ネットワークシステムの構成要素のうち、都道府県サーバにおいて管理がなされているため、以降は、住民基本台帳ネットワークシステムの内の都道府県サーバ部分について記載する。
②システムの機能	1. 本人確認情報の更新 ：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、市町村コミュニケーションサーバ（以下「市町村CS」という。）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、全国サーバに対して当該本人確認情報の更新情報を通知する。 2. 県の他の執行機関への都道府県知事保存本人確認情報の提供または他部署への移転 ：県の他の執行機関また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、4情報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. 都道府県知事保存本人確認情報の開示 ：住基法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. 機構保存本人確認情報の照会 ：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. 本人確認情報の検索 ：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. 本人確認情報の整合性確認 ：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。 7. 個人番号制度の運用に伴う情報連携 ：団体内統合宛名システムと本人確認情報を初期突合するための本人確認情報ファイルの提供及び中間サーバ上で作成される符号取得依頼ファイルを、地方公共団体情報システム機構の全国センターに送信するため、都道府県サーバの代表端末または業務端末側と団体内統合宛名システム側に受渡し専用フォルダを設けて、本人確認情報ファイル等の受け渡しを行う。
③他のシステムとの接続	[　] 情報提供ネットワークシステム　　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　　[　] 既存住民基本台帳システム [○] 宛名システム等　　[　] 税務システム [　] その他　（　　）

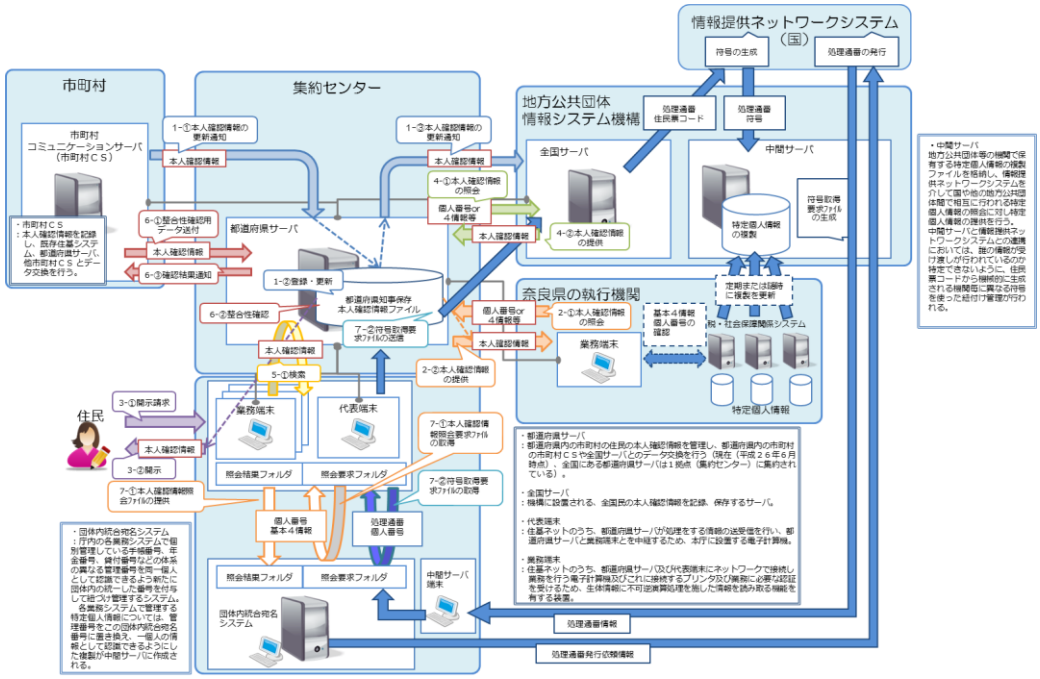
システム2	
①システムの名称	団体内統合宛名システム
②システムの機能	1．符号管理対応機能 中間サーバの符号管理機能に対応するための機能 2．情報照会支援機能 中間サーバの情報照会機能に対応する機能 3．情報提供支援機能 中間サーバの情報提供機能に対応し、既存システムが行うべき情報提供等を支援する機能 4．4情報等の出力機能 中間サーバからの情報提供要求に対応し、個人番号および4情報のデータを中間サーバに通知する機能 5．団体内統合宛名番号付番機能 団体内統合宛名システム端末及び既存システムからの要求に対し、団体内統合宛名番号の割り当てを行い、業務利用番号や4情報と紐付ける機能 6．宛名情報等管理機能 団体内統合宛名番号を主キーとして、各情報を適切に管理する機能 7．未電算業務等対応機能 団体内統合宛名システム運用端末を用いて未電算業務等に対応するための機能 8．共通変換機能 既存システムの中間サーバ連携を支援するため、既存システムからの入出力データについて共通的に変換する機能 9．職員認証・権限管理機能 システムへログインするための認証機能およびログイン後の権限管理の機能 10．システム管理機能 システムの安定運用のために必要な機能 11．住民基本台帳ネットワークシステムとの回線連携機能 住民基本台帳ネットワークシステムと回線連携するため機能
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　（ 中間サーバ　　）

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、符号取得要求ファイル

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	県では、都道府県知事保存本人確認情報ファイルおよび符号取得要求ファイルを、下記に掲げ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住民基本台帳ネットワークシステム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（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）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県の他の執行機関または他部署による住基法に基づく都道府県知事保存本人確認情報の照会に基づき、当該情報を提供・移転する。 ④住民からの請求に基づき、当該個人に係る都道府県知事保存本人確認情報を開示する。 ⑤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いて、都道府県知事保存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。 ・番号制度の運用において、県の中間サーバに登録されている特定個人情報（県外者を含む）を情報提供ネットワークステムを介して情報連携するために必要な符号生成のため、中間サーバから出力された符号取得要求ファイルを取得し、全国センターへ送信する必要がある。
②実現が期待されるメリット	住民票の写し等に代えて本人確認情報を利用することにより、これまで行政手続きの際に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、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。

5. 個人番号の利用 ※	
法令上の根拠	住民基本台帳法（昭和42年7月25日法律第81号） （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に等に関する法律（平成25年5月31日法律第28号）（以下「整備法」という。）附則第3号施行日時点） ・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13（都道府県の条例による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	地域振興部市町村振興課
②所属長	市町村振興課長　山下　保典
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. 県の他の執行機関への情報提供または他部署への移転
  2-①.県の他の執行機関または他部署において、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.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・移転する。
  ※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。
  ※県の他の執行機関または他部署に対し、住民基本台帳ネットワークシステムに係る本人確認情報を一括して提供する
    場合（一括提供の方式（注1）により行う場合）には、県の他の執行機関または他部署において、都道府県サーバの
    代表端末又は業務端末を操作し、媒体連携（注2）または回線連携（注3）により行う。
    （注1）県の他の執行機関又は他部署においてファイル化された本人確認情報照会対象者の情報（検索条件のリスト）を
      元に都道府県サーバに照会し、照会結果ファイルを提供する方式を指す。
    （注2）媒体連携とは、一括提供の方式により本人確認情報の提供を行う場合に、情報連携に電子記録媒体を用いる方法を指す。
    （注3）回線連携とは、一括提供の方式により本人確認情報の提供を行う場合に、情報連携に通信回線（庁内LAN等）を用いる方法
      を指す。具体的には、都道府県サーバの代表端末又は業務端末と庁内システム（宛名管理システムを含む。）のみが
      アクセス可能な領域（フォルダ）を設け、当該領域内で照会要求ファイル及び照会結果ファイルの授受を行う。

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. 機構保存本人確認情報の照会に関する事務
  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。

7. 個人番号制度の運用に伴う情報連携
  7-①.団体内統合宛名システムと本人確認情報との初期突合を行うため、団体内統合宛名システム側と代表端末または
    業務端末側とに受渡し専用フォルダを設けて、本人確認情報照会要求ファイルや本人確認情報ファイルの受け渡しを行う。
  7-②.中間サーバ上で作成される符号取得依頼ファイル（処理通番、個人番号）を団体内統合宛名システム側と代表端末または
    業務端末側との受渡し専用フォルダを介して受領し、全国サーバに送信する。
    ※全国サーバは、個人番号を住民票コードに置き換えて、情報提供ネットワークシステムに（処理通番、住民票コード）を
      送信する。報提供ネットワークシステムは、受信した情報を元に符号を生成し中間サーバに通知して、符号による情報の
      紐づけを行う。

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 ※		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）に基づき住民基本台帳に記録された住民※を指す。） ※住民基本台帳に記録されていた者で、転出等の事由により住民票が消除（死亡による消除を除く。）された者（以下「消除者」という。）を含む。
	その必要性	住民基本台帳ネットワークシステムを通じて全国共通の本人確認を行うため、都道府県知事保存本人確認情報ファイルにおいて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 ：住民基本台帳ネットワークシステム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		地域振興部市町村振興課

3. 特定個人情報の入手・使用			
①入手元 ※			[　　]本人又は本人の代理人 [　　]評価実施機関内の他部署　（　　） [　　]行政機関・独立行政法人等　（　　） [○]地方公共団体・地方独立行政法人　（ 市町村　　） [　　]民間事業者　（　　） [　　]その他　（　　）
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、都道府県知事保存本人確認情報に係る変更又は新規作成が発生した都度入手する。
④入手に係る妥当性			住基法第30条の6の規定により、市町村長は住民票の記載、消除等を行った場合には、当該住民票の記載等に係る本人確認情報を市町村長の使用に係る電子計算機（市町村CS）から電気通信回線を通じて都道府県知事の使用に係る電子計算機（都道府県サーバ）へ送信することにより通知するものとされている。
⑤本人への明示			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）に明示されている。
⑥使用目的 ※			住民基本台帳ネットワークシステムを通じて全国共通の本人確認を行うため、都道府県知事保存本人確認情報ファイルにおいて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。
	変更の妥当性		ー
⑦使用の主体	使用部署 ※		地域振興部市町村振興課
	使用者数		[　　10人未満　　]　＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
⑧使用方法 ※			・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）。 ・県の他の執行機関または他部署からの都道府県知事保存本人確認情報の照会要求を受け（県の他の執行機関または他部署→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、該当する個人の都道府県知事保存本人確認情報を照会元へ提供・移転する（都道府県サーバ→県の他の執行機関または他部署）。 ・住民からの開示請求に基づき（住民→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機構へ機構保存本人確認情報の照会を行い（都道府県サーバ→全国サーバ）、該当する個人の本人確認情報を受領する（全国サーバ→都道府県サーバ）。 ・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内の検索を行う。 ・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。 ・県の他の執行機関または他部署からの照会に基づいて都道府県知事保存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。 ・請求に基づいて都道府県知事保存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）の規定に基づいて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 （ 3 ） 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、本人確認情報に直接係わらない（本人確認情報に直接アクセスできず、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」と同上
	その妥当性	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」の通り、委託事項は、本人確認情報に直接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		委託先が決定した際に県ホームページにて公開する。
⑥委託先名		地方公共団体情報システム機構（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	委託契約において、原則として再委託を禁止しているが、再委託を実施する必要がある場合は、事前に書面により委託者の承諾を得ることとしている。
	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、本人確認情報に直接係わらない（本人確認情報に直接アクセスできず、閲覧・更新・削除等を行わない）業務を対象とする。 なお、「①委託内容」の通り、委託事項は、本人確認情報に直接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。

委託事項2		代表端末、業務端末等機器の保守管理に関する業務
①委託内容		県が設置する代表端末、業務端末及びファイアウォール等の構成機器について、保守管理業務を委託する。 委託する業務は、本人確認情報に直接係わらない（本人確認情報に直接アクセスできず、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」と同上
	その妥当性	住民基本台帳ネットワークシステムを安全かつ適切に運用するため、県が設置する代表端末、業務端末及びファイアウォール等の機器について保守管理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、本人確認情報に直接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		委託先が決定した際に入札結果を県ホームページにて公開する。
⑥委託先名		NECキャピタルソリューション株式会社
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	委託契約において、原則として再委託を禁止しているが、再委託を実施する必要がある場合は、事前に書面により委託者の承諾を得ることとしている。
	⑨再委託事項	県が設置する代表端末、業務端末及びファイアウォール等の機器に関する保守管理。 なお、「①委託内容」の通り、委託事項は、本人確認情報に直接係わらない事務を対象としているため、再委託先においても、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。

委託事項3		代表端末、業務端末等機器の運用管理に関する業務
①委託内容		県が設置する代表端末、業務端末及びファイアウォール等の構成機器の利用ログ採取や性能監視等の運用管理業務を委託する。 委託する業務は、本人確認情報に直接係わらない（本人確認情報に直接アクセスできず、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」と同上
	その妥当性	住民基本台帳ネットワークシステムを安全かつ適切に運用するため、県が設置する代表端末、業務端末及びファイアウォール等の構成機器の利用ログ採取や性能監視等の運用管理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、本人確認情報に直接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		委託先が決定した際に入札結果を県ホームページにて公開する。
⑥委託先名		日本電気株式会社
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	委託契約において、原則として再委託を禁止しているが、再委託を実施する必要がある場合は、事前に書面により委託者の承諾を得ることとしている。
	⑨再委託事項	県が設置する代表端末、業務端末及びファイアウォール等の構成機器の利用ログ採取や性能監視等の運用管理。 なお、「①委託内容」の通り、委託事項は、本人確認情報に直接係わらない事務を対象としているため、再委託先においても、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。

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（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	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、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	[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」と同上
⑥提供方法	[ ] 情報提供ネットワークシステム [ ] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [○] その他 （ 住民基本台帳ネットワークシステム ）
⑦時期・頻度	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、随時。
提供先2	県の他の執行機関（教育委員会など）
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）、奈良県住民基本台帳法施行条例第3条
②提供先における用途	住基法別表第六及び奈良県住民基本台帳法施行条例別表第二に掲げられた県の他の執行機関への情報提供が認められる事務の処理に用いる。（ただし、個人番号については、県の他の執行機関が番号法第9条第1項又は第2項の規定により個人番号を利用することができる場合に限り、利用することができるものとする。）
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 ※住民票コードについては、整備法第20条第9項及び第22条第7項に基づく経過措置である。
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」と同上
⑥提供方法	[ ] 情報提供ネットワークシステム [ ] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [○] フラッシュメモリ [ ] 紙 [○] その他 （ 住民基本台帳ネットワークシステム ）
⑦時期・頻度	県の他の執行機関からの情報照会の要求があった都度、随時。

提供先3	住民（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	都道府県知事保存本人確認情報ファイルに記録されている自己の本人確認情報を確認し、必要に応じてその内容の全部または一部の訂正、追加または削除の申出を行う。
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	［　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」と同上
⑥提供方法	［　　］情報提供ネットワークシステム　　［　　］専用線 ［　　］電子メール　　［　　］電子記録媒体（フラッシュメモリを除く。） ［　　］フラッシュメモリ　　［ ○ ］紙 ［ ○ ］その他　（ 端末機の画面の閲覧、端末機から出力された帳票の閲覧　）
⑦時期・頻度	当該住民から開示請求があった都度、随時。
移転先1	県の他部署（税務課など）
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）、奈良県住民基本台帳法施行条例第3条
②移転先における用途	住基法別表第五に掲げる、または住基法施行条例別表第一に掲げられた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、性別、生年月日、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、整備法第20条第9項及び第22条第7項に基づく経過措置である。
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」と同上
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	県の他部署からの検索要求があった都度、随時。

6. 特定個人情報の保管・消去

①保管場所 ※		＜住民基本台帳ネットワークシステムにおける措置＞ ・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。 ・県においては、代表端末及び記録媒体を施錠管理及び入退室管理を行っているサーバ室に保管し、業務端末にはセキュリティワイヤを施し、当該端末を設置した執務室は職員が退庁する際は施錠するなど必要な措置を講じる。 ＜団体内統合宛名システムにおける措置＞ ・入退室管理を行っているサーバ室で管理すると共に、監視カメラによる入退室者及びシステム操作者の監視を行う。 ・特定個人情報はサーバ室内に設置された団体内統合宛名システムのデータベース内に保存し、バックアップも同室内の機器に保存することとしている。
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（履歴の情報：5年間、消除者の情報：原則5年間（最長80年間）。ただし、平成27年10月1日以降はいずれも150年間）保管する。
③消去方法		＜住民基本台帳ネットワークシステムにおける措置＞ 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。 ＜団体内統合宛名システムにおける措置＞ ・ディスク交換やハード更改等の際は、団体内統合宛名システムの保守・運用を行う事業者において、保存された情報が読み出しできないよう、物理的破壊又は専用ソフト等を利用して完全に消去する。 ・住民基本台帳ネットワークシステムの最新4情報で洗い替えをするため、住民基本台帳法施行令の本人確認情報の保存期間に従う。平成27年10月1日までは、除票（死亡を除く）となってから5年間、以降は、150年間保存する。

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	
符号取得要求ファイル	
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 ※	日本国内の住民（国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）に基づき住民基本台帳に記録された住民※を指す。） ※住民基本台帳に記録されていた者で、転出等の事由により住民票が消除（死亡による消除を除く。）された者（以下「消除者」という。）を含む。
その必要性	番号制度の運用において、県の各業務システムで保有している、社会保障・税関係の特定個人情報（県外者を含む）の対象者が連携対象となるため、県内在住者だけでなく、日本国内の住民が、番号制度の連携対象となる。
④記録される項目	[　　10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、その他識別情報（内部情報） 番号制度の運用において、県の中間サーバに登録されている特定個人情報（県外者を含む）を情報提供ネットワークステムを介して情報連携するために必要な符号を生成するため、中間サーバから出力された符号取得要求ファイルを取得し、全国センターへ送信する必要がある。
全ての記録項目	別添2を参照。
⑤保有開始日	平成27年10月予定
⑥事務担当部署	地域振興部市町村振興課

3. 特定個人情報の入手・使用			
①入手元 ※			[　　]本人又は本人の代理人 [　　]評価実施機関内の他部署　（　　） [　　]行政機関・独立行政法人等　（　　） [○]地方公共団体・地方独立行政法人　（ 市町村　　） [　　]民間事業者　（　　） [　　]その他　（　　）
②入手方法			[　　]紙　[　　]電子記録媒体（フラッシュメモリを除く。）　[　　]フラッシュメモリ [　　]電子メール　[　　]専用線　[○]庁内連携システム [　　]情報提供ネットワークシステム [　　]その他　（　　）
③入手の時期・頻度			番号制度の運用において、中間サーバ未登録者の特定個人情報の情報連携が発生した都度入手する。
④入手に係る妥当性			番号法第19条第7項に規定する別表第二の特定個人情情報を法第21条に規定する情報提供ネットワークシステムを介して情報提供する際に、番号法施行令第20条第1項に規定する情報提供用個人符号（符号）の生成が必要となる。この生成の際、番号法施行令第20条第3項の方法により機構（全国サーバ）へ送付することとされている。
⑤本人への明示			番号法第19条第7項及び番号法施行令第20条
⑥使用目的 ※			番号制度の運用において、県の中間サーバに登録されている特定個人情報（県外者を含む）を情報提供ネットワークステムを介して情報連携するために必要な符号を生成する。
	変更の妥当性		ー
⑦使用の主体	使用部署 ※		地域振興部市町村振興課
	使用者数		[　　10人未満　　]　＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
⑧使用方法 ※			・中間サーバで生成された符号取得要求ファイル（処理通番、個人番号）を団体内統合宛名システム端末の受渡し専用フォルダに保存する。 ・住民基本台帳ネットワークシステムの業務端末又は都道府県サーバの代表端末側から、団体内統合宛名システムの受渡し専用フォルダ内の符号取得要求ファイルを取り込む。 ・業務端末又は都道府県サーバの代表端末から「ファイル転送機能」で都道府県サーバに符号取得要求ファイルを転送する。 ・都道府県サーバは「符号取得要求ファイル送信処理機能」で全国サーバにファイル転送する。 ・全国サーバは「情報提供ネットワークとの情報連携処理機能」で、個人番号を住民票コードに変換し、情報提供ネットワークシステムに符号取得要求ファイル（処理通番、住民票コード）を送付する。 ・情報提供ネットワークシステムは、処理通番、住民票コードから符号を生成し保管すると共に県に中間サーバに生成した符号を送付する。 ・県の中間サーバは、処理通番を元に団体統合宛名番号と符号を紐付管理する。 ・この一連の処理において、県の中間サーバと国の情報提供ネットワークシステムは、符号で連携できるようになるため、符号生成後は、個人番号、4情報及び住民票コードなどの本人確認情報は使用されない。
	情報の突合 ※		・中間サーバで生成された符号取得要求ファイルを（処理通番、個人番号、団体統合宛名番号）を全国サーバから情報提供ネットワークシステムに送付する際に、「情報提供ネットワークとの情報連携処理機能」で、個人番号で全国サーバの本人確認情報と突合し、住民票コードに変換する。
	情報の統計分析 ※		符号生成のみの利用となるため、統計分析には利用しない。
	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 ※	[　　委託しない　　]　＜選択肢＞ 1）委託する　2）委託しない （　　）件

5. 特定個人情報の提供・移転（委託に伴うものを除く。）		
提供・移転の有無		[○] 提供を行っている （ 1 ）件 [ ] 移転を行っている （ ）件 [ ] 行っていない
提供先1		地方公共団体情報システム機構（機構）
①法令上の根拠		番号法第19条（特定個人情報の制限）第7項及び番号法施行令第20条（情報提供用個人符号の取得）
②提供先における用途		県の中間サーバより受領した符号取得要求ファイルを元に情報提供ネットワークシステムと県の中間サーバ間で特定個人情報を連携するための符号を生成する。
③提供する情報		住民票コード、処理通番
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」と同上
⑥提供方法		[ ] 情報提供ネットワークシステム [ ] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [○] その他 （ 住民基本台帳ネットワークシステム ）
⑦時期・頻度		番号制度の運用において、中間サーバ未登録者の特定個人情報の情報連携が発生した都度入手する。
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。 ・県においては、代表端末及び記録媒体を施錠管理及び入退室管理を行っているサーバ室に保管し、業務端末にはセキュリティワイヤを施し、当該端末を設置した執務室は職員が退庁する際は施錠するなど必要な措置を講じる。
②保管期間	期間	[ ] ＜選択肢＞ 1）1年未満 2）1年 3）2年 4）3年 5）4年 6）5年 7）6年以上10年未満 8）10年以上20年未満 9）20年以上 10）定められていない
	その妥当性	情報提供ネットワークシステムにファイル送付が完了した時点で消去し保管は行わない。 受領した処理通番、個人番号は、情報提供ネットワークシステムと中間サーバとの間で使用する符号生成に必要な情報であるため、符号生成後、不要な特定個人情報は消去する。
③消去方法		ファイルを転送後、自動判別し消去する。
7. 備考		
－		

（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

符号取得要求ファイル

1. 処理通番
2. 個人番号
3. 符号再発行フラグ

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	＜住民基本台帳ネットワークシステムにおける措置＞ 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（住基法第30条の6第1項に基づき通知）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。 ＜団体内統合宛名システムにおける措置＞ 業務所管課において届出内容や本人確認書類（身分証明等）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	＜住民基本台帳ネットワークシステムにおける措置＞ 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を、システム上で担保されている。（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（住基法第30条の6第1項に基づき通知）される本人確認情報に限定される。） ＜団体内統合宛名システムにおける措置＞ ・団体内統合宛名システムは、番号制度利用対象システムのみ接続し、対象外のシステムは接続しない。 ・団体内統合宛名システムは、主に業務システムから統合宛名管理上で必要な項目のみ連携することを想定しており、業務データは保有しない。
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：　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	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（住基法第30条の6第1項に基づき通知）される本人確認情報に限定される。
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
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	＜住民基本台帳ネットワークシステムにおける措置＞ 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（住基法第30条の6第1項に基づき通知）される本人確認情報に限定される。対象者の本人確認は市町村に委ねられている。なお、市町村窓口にて住民基本台帳に関する届出がされる場合は住基法第27条の規定に基づき、現に届出の任に当たっている者に対し、身分証明書（個人番号カード等）を提示させることにより厳格な本人確認を行う。 ＜団体内統合宛名システムにおける措置＞ 特定個人情報の入手の際には、業務所管課の事務で確立された手順に従って本人であることが担保されたデータのみを連携する。
個人番号の真正性確認の措置の内容	＜住民基本台帳ネットワークシステムにおける措置＞ 市町村において真正性が確認された情報を市町村CSを通じて入手できることを、システムで担保する。 ＜団体内統合宛名システムにおける措置＞ 業務所管課の事務で個人番号の真正性が確認されたデータを連携する。

特定個人情報の正確性確保の措置の内容	＜住民基本台帳ネットワークシステムにおける措置＞ 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。 また、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。 ＜団体内統合宛名システムにおける措置＞ ・特定個人情報を取り扱うネットワークやシステムに対して、アクセス制御の措置を講じている。 ・ウィルス対策ソフトウェアを導入し、常に最新のパターンファイルを適用することで、セキュリティ上の有効性を確認している。 ・OSや導入するソフトウェアに対するセキュリティパッチはその有効性や必要性等を検証した上で適用し、その動作の安定性も確認している。 ・特定個人情報にアクセスする端末はインストールする標準ソフトウェアを定めており、システム管理者の許可なくソフトウェアをインストールすることを禁止している。
その他の措置の内容	ー
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ほか、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。 都道府県内の市町村の住民の本人確認情報を管理し、都道府県内の市町村の市町村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	
ー	

3. 特定個人情報の使用	
リスク1： 目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク	
宛名システム等における措置の内容	・本人確認情報の一括提供機能の利用について、これまで用いてきた電子記録媒体による連携方式の代わりに代表端末または業務端末側と団体内統合宛名システム側に受渡し専用フォルダを設けて、要求ファイル等の受け渡し連携を行う。これにより、媒体紛失等のリスクがなくなり、セキュリティ向上が見込まれる。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に対する措置として、①宛名システム側から住民基本台帳ネットワークシステムを操作できない②両システム間にファイアウォールを設置し特定の通信方式を用いなければ通信できない仕組みとする。 ・団体内統合宛名システムは、番号法別表第1及び関係主務省令に定められた業務に従事する職員以外からの特定個人情報へのアクセスが行えないような仕組みであり、団体内統合宛名システムへは個人番号、氏名や生年月日等の基本的な情報のみ保持しており、当該事務に必要のない情報との紐付けは物理的に不可能である。
事務で使用するその他のシステムにおける措置の内容	都道府県サーバと庁内システム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	＜住民基本台帳ネットワークシステムにおける措置＞ 都道府県サーバへのアクセスは代表端末及び業務端末から行うものであり、当該端末の操作にあたっては、事前にシステム管理者の承認を得た操作者のみに付与された照合ID及び照合情報（静脈による生体認証）による操作者認証を行う。 ＜団体内統合宛名システムにおける措置＞ ・システムを利用する必要がある職員を特定し、ユーザIDによる識別とパスワードによる認証を実施する。 ・なりすましによる不正を防止する観点から、共用IDの利用を禁止し、個人ごとにユーザIDを付与する。 ・認証後は、利用機能の認可機能により、そのユーザがシステム上で利用可能な機能を制限することで不正利用が行えない対策を実施する。
アクセス権限の発効・失効の管理	[行っている] ＜選択肢＞ 1）行っている 2）行っていない
具体的な管理方法	＜住民基本台帳ネットワークシステムにおける措置＞ ・操作者照合情報登録者名簿を作成し、アクセス権限の発効・失効の履歴を適切に管理する。 ・退職や人事異動（担当替え含む。）等により、操作者照合情報の削除依頼通知を受けたときは、直ちにアクセス権限を無効化する。 ＜団体内統合宛名システムにおける措置＞ ・ユーザID及びパスワードの発行管理・・・アクセス権限と業務の対応表を作成する。 ・失効管理・・・権限を有していた職員の異動退職情報を確認し、異動退職があった際はアクセス権限を更新し、当該IDを失効させる。
アクセス権限の管理	[行っている] ＜選択肢＞ 1）行っている 2）行っていない
具体的な管理方法	＜住民基本台帳ネットワークシステムにおける措置＞ ・操作者に対し、業務に応じた必要範囲内の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及び業務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。 ＜団体内統合宛名システムにおける措置＞ ・ユーザIDやアクセス制御を定期的に確認し、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または削除する。

特定個人情報の使用の記録		[　　記録を残している　　] ＜選択肢＞ 1）記録を残している　　2）記録を残していない
	具体的な方法	・業務端末の使用にあたっては、事前に操作者の属する部署の長より申請書を提出させるとともに、業務端末使用簿に利用日時、所属、氏名を記載する。 ・システムの操作履歴（業務アクセスログ・操作ログ）を採取・保管し、月１回程度、定期的に分析を行う。 ・システムの操作履歴については7年間、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		＜住民基本台帳ネットワークシステムにおける措置＞ ・システムの操作履歴（業務アクセスログ・操作ログ）を採取・保管し、月１回程度、定期的に分析を行う。 ・住民基本台帳ネットワークシステム利用にあたっての留意事項を記載したレジュメを作成し、業務上必要のない本人確認情報検索又は抽出を行わないようシステム操作者に対し厳格に指導する。 ・システム利用職員への研修会において、事務外利用の禁止等について指導する。 ・操作者への権限付与に際して、操作者本人から、「住基法その他関係法令等の遵守」「目的外利用を行わない」、「個人情報保護およびセキュリティの確保に努める」旨を記した誓約書の提出を求める。 ・「奈良県住民基本台帳ネットワークシステム管理規程」「奈良県住民基本台帳ネットワークシステムセキュリティ基本方針書」「奈良県住民基本台帳ネットワークシステムの管理者等が定める事項」「奈良県住民基本台帳ネットワークシステム用業務端末運用管理要領」「本人確認情報開示等実施要領」を策定している。 ・違反行為を行った場合は、法令の罰則規定により措置を講じる。 ＜団体内統合宛名システムにおける措置＞ ・システムの操作履歴（操作ログ）を記録する。 ・職員に対しては、特定個人情報保護委員会が作成した「特定個人情報の適正な取扱いに関するガイドライン」を参考にしてデータ保護に関する研修を行う。 ・委託先に対しては業務外で使用しないよう、上記と同様にガイドラインを参考にして仕様書に定め、個人情報保護にかかる誓約書を提出させる。 ・違反行為を行った場合は、法令の罰則規定により措置を講じる。
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		＜住民基本台帳ネットワークシステムにおける措置＞ ・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。 ・システムの操作履歴（業務アクセスログ・操作ログ）を採取・保管し、月１回程度、不正なファイル複製がないことを確認する。 ・違反行為を行った場合は、法令の罰則規定により措置を講じる。 ＜団体内統合宛名システムにおける措置＞ ・委託先に対しては、仕様書にて許可を得ない複製を禁止し、個人情報保護にかかる誓約書を提出させる。 ・職員に対しては、データ保護に関する研修を行う。 ・違反行為を行った場合は、法令の罰則規定により措置を講じる。
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		
本人確認情報の利用にあたり、以下の措置を講じる。 ＜住民基本台帳ネットワークシステムにおける措置＞ ・スクリーンセーバ等を利用して、長時間にわたり本人確認情報を表示させない。 ・都道府県サーバの代表端末を施錠管理された安全な場所に設置する。 ・すべての業務端末のディスプレイに覗き見防止用シートを貼付するとともに、来庁者から見えない位置に設置する。 ・システム操作者は本人確認情報が表示された画面のハードコピーを取得しない。 ・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。 ＜団体内統合宛名システムにおける措置＞ ・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。 ・端末機のディスプレイを来庁者から見えない位置に設置する。		

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	＜住民基本台帳ネットワークシステムにおける措置＞ ①都道府県サーバの運用及び監視に関する業務 ・平成24年6月12日、住民基本台帳ネットワークシステム推進協議会（47都道府県が構成員）において、都道府県サーバ集約化の実施および集約化された都道府県サーバの運用及び監視に関する業務を機構へ委託することを議決している。 ・委託先として議決された機構は、地方公共団体情報システム機構法（平成25年5月31日法律第29号）に基づき平成26年4月1日に設立された組織であり、住基法に基づく指定情報処理機関として住民基本台帳ネットワークシステムの運用を行っている実績がある。また、前身の財団法人地方自治情報センターにおいて平成14年8月5日から平成26年3月31日まで、指定情報処理機関であった。 ・そのため、委託先として社会的信用と特定個人情報の保護を継続的に履行する能力があると認められるとともに、プライバシーマークの付与を受けており、情報保護管理体制は十分である。 ②代表端末、業務端末等機器の保守管理に関する業務 ③代表端末、業務端末等機器の運用管理に関する業務 ・委託契約書において、秘密保持義務および個人情報保護の徹底、セキュリティ要件（情報資産の管理方法、遵守すべき事項及び判断基準等）を明記し、受託者および事前に承諾を得た再委託事業者（いずれも従業者を含む。）に対し、遵守させることを義務づける。 ・受託者から業務に従事する者に係るセキュリティチェックの実施状況について毎月報告を受ける。 ＜団体内統合宛名システムにおける措置＞ システムの運用等を委託するときは、あらかじめ管理者と協議を行い、特定個人情報の保護を適切に行える委託先であることを確認する。
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	＜住民基本台帳ネットワークシステムにおける措置＞ ・委託業務に従事する者に都道府県知事保存本人確認情報ファイルに直接アクセスする権限を付与しない。 ①都道府県サーバの運用及び監視に関する業務 ・委託先（再委託先を含む。）には、本人確認情報の更新及び本人確認情報の整合性確認業務のため特定個人情報ファイルを提供する場合が想定されるが、その場合はシステムで自動的に暗号化を行った上で提供することとしており、システム設計上、特定個人情報にアクセスできず閲覧／更新もできない。 ・委託先（再委託先を含む。）は、災害等におけるデータの損失等に対する対策のため、日次で特定個人情報ファイルをバックアップすることが想定されるが、バックアップのために特定個人情報ファイルを媒体に格納する場合は、システムで自動的に暗号化を行うこととしており、システム設計上、特定個人情報にアクセスできず閲覧／更新もできない。 ②代表端末、業務端末等機器の保守管理に関する業務 ③代表端末、業務端末等機器の運用管理に関する業務 ・委託業務に従事する者の名簿を提出させる。 ・システムの操作履歴（業務アクセスログ・操作ログ）を採取・保管し、月1回程度、定期的に分析を行う。 ＜団体内統合宛名システムにおける措置＞ ・委託にかかる実施体制の提出を義務づける。 ・委託事業者に対し、個人情報保護にかかる誓約書を提出させる。 ・誓約書の提出があった要員に対してのみ、システム操作の権限を与える。

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	＜住民基本台帳ネットワークシステムにおける措置＞ ①都道府県サーバの運用及び監視に関する業務 ・委託先（再委託先を含む。）には、本人確認情報の更新及び本人確認情報の整合性確認業務のため特定個人情報ファイルを提供する場合が想定されるが、その場合はシステムで自動的に暗号化を行った上で提供することとしており、システム設計上、特定個人情報にアクセスできず閲覧／更新もできない。 ・委託先（再委託先を含む。）は、災害等におけるデータの損失等に対する対策のため、日次で特定個人情報ファイルをバックアップすることが想定されるが、バックアップのために特定個人情報ファイルを媒体に格納する場合は、システムで自動的に暗号化を行うこととしており、システム設計上、特定個人情報にアクセスできず閲覧／更新もできない。 ・上記のとおり、委託先（再委託先を含む。）は特定個人情報にアクセスできないが、バックアップ媒体については、記録簿により管理し、保管庫に保管している。週次で管理簿と保管庫の媒体をチェックし、チェックリストに記入している。バックアップの不正取得や持ち出しのリスクに対し、サーバ室に物理的対策（監視カメラなど）を講じ、不正作業が行われないようにしている。 ・チェックリストの結果について、委託先である機構より、月次で書面により「都道府県サーバ集約センターの運用監視等に係る作業報告について　6．セキュリティ確認結果報告」の報告を受けている。 ②代表端末、業務端末等機器の保守管理に関する業務 ③代表端末、業務端末等機器の運用管理に関する業務 ・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。 ・契約書等に基づき、受託者から業務報告書の提出を受ける。また、必要に応じて、受託者に対して必要な指示を行うとともに、調査を実施する。 ・システムの操作履歴（業務アクセスログ・操作ログ）を採取・保管し、月１回程度、定期的に分析を行う。 ・システムの操作履歴については7年間、安全な場所に施錠保管する。 ＜団体内統合宛名システムにおける措置＞ 委託先における特定個人情報についてのシステム利用履歴について、利用者ID、操作日時などデータベースアクセスログを7年間保管する。

特定個人情報の提供ルール		[　　定めている　　] ＜選択肢＞ 1）定めている　　2）定めていない
	委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	＜住民基本台帳ネットワークシステムにおける措置＞ ①都道府県サーバの運用及び監視に関する業務 ・委託先である機構に対し、特定個人情報の目的外利用及び提供は認めないことを契約書上明記している。 ・委託先である機構は、日次、月次、年次で目的外利用及び提供についてのチェックを含むセキュリティチェックを行い、委託元である当県は、チェックリストの結果について、機構より、月次で書面により「都道府県サーバ集約センターの運用監視等に係る作業報告について　6．セキュリティ確認結果報告」の報告を受けている。 ・必要があれば、当県職員が委託業務について機構の履行状況を立ち会いまたは報告を受けることを契約書上明記している。 ②代表端末、業務端末等機器の保守管理に関する業務 ③代表端末、業務端末等機器の運用管理に関する業務 ・委託する業務は、本人確認情報に直接係わらない（本人確認情報に直接アクセスできず、閲覧・更新・削除等を行わない）業務を対象とする。 ・委託契約書において、秘密保持義務および個人情報保護の徹底、セキュリティ要件（情報資産の管理方法、遵守すべき事項及び判断基準等）を明記し、受託者および事前に承諾を得た再委託事業者（いずれも従業者を含む。）に対し、遵守させることを義務づける。 ・受託者から業務に従事する者に係るセキュリティチェックの実施状況について毎月報告を受ける。 ＜団体内統合宛名システムにおける措置＞ ・委託契約書に基づき、委託先は県の指示がある場合を除き、特定個人情報の目的外利用及び第三者に提供してはならない。 ・委託先は県の承認があるときを除き、特定個人情報の複写・複製、又はこれらに類する行為をすることができない。 ・委託契約書に基づき、必要があると認めるときは調査を行い、または報告を求める。
	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	＜住民基本台帳ネットワークシステムにおける措置＞ ①都道府県サーバの運用及び監視に関する業務 ・委託先（再委託先を含む。）に送付する特定個人情報ファイルは暗号化されているため、委託先（再委託先を含む。）がファイル内の特定個人情報にアクセスしないシステム設計としている。 ②代表端末、業務端末等機器の保守管理に関する業務 ③代表端末、業務端末等機器の運用管理に関する業務 ・委託する業務は、本人確認情報に直接係わらない（本人確認情報に直接アクセスできず、閲覧・更新・削除等を行わない）業務を対象とする。 ・委託契約書において、秘密保持義務および個人情報保護の徹底、セキュリティ要件（情報資産の管理方法、遵守すべき事項及び判断基準等）を明記し、受託者および事前に承諾を得た再委託事業者（いずれも従業者を含む。）に対し、遵守させることを義務づける。 ・受託者から業務に従事する者に係るセキュリティチェックの実施状況について毎月報告を受ける。 ＜団体内統合宛名システムにおける措置＞ ・運用保守委託やオペレーション業務委託に関しては、仕様書にて委託業務実施場所を県庁舎内に限定し、外部への持ち出しを禁止する。 ・委託契約に基づき、必要があると認めるときは調査を行い、または報告を求める。

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	①都道府県サーバの運用及び監視に関する業務 ・委託契約上、委託先である機構に提供された特定個人情報ファイルについては、住基法施行令第30条の6に規定された本人確認情報の保存期間（150年間）が過ぎた際に、システムにて自動判別し消去することを規定している。 ・バックアップ媒体については、「運用設計書」において、「媒体が破損や耐用年数、耐用回数を超過したとき、管理簿に理由を明記し、媒体は引き続きデータ保管庫に格納」することにしているが、委託契約上、委託先である機構に提供された特定個人情報ファイルについては、契約完了時に返還または廃棄することを規定する。 ・委託契約の報告条項に基づき、月次の完了届において、特定個人情報の取扱いについて書面にて報告を受ける。また、必要があれば、当県職員又は監査法人などの第三者が現地調査し、適正に運用されているか確認する。 ②代表端末、業務端末等機器の保守管理に関する業務 ③代表端末、業務端末等機器の運用管理に関する業務 ・委託する業務は、本人確認情報に直接係わらない（本人確認情報に直接アクセスできず、閲覧・更新・削除等を行わない）業務を対象としている。 ・委託契約書において、受託者が委託者から提供された業務遂行のために必要な情報等について、業務の遂行に不要となった場合は直ちに委託者に返還させることを義務づける。
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	＜住民基本台帳ネットワークシステムにおける措置＞ ①都道府県サーバの運用及び監視に関する業務 ・秘密保持義務 ・事業所内からの特定個人情報の持出しの禁止 ・特定個人情報の目的外利用の禁止 ・再委託における条件 ・漏えい事案等が発生した場合の委託先の責任 ・委託契約終了後の特定個人情報の返却又は廃棄 ・従業者に対する監督・教育 ・契約内容の遵守状況について報告を求める規定 等を契約書において定めるとともに、当県と同様の安全管理措置を義務付ける。 ②代表端末、業務端末等機器の保守管理に関する業務 ③代表端末、業務端末等機器の運用管理に関する業務 【契約書で定める事項】 ・善管注意義務 ・委託業務遂行上の義務 ・原始資料等の管理及び返還（目的外使用の禁止を含む） ・秘密の保持及び個人情報の保護（契約終了（または解除）後においても同様である旨を含む） ・再委託の禁止（承諾を受けたものは除く） 【契約書に付随する文書（仕様書等）で定める事項】 ・資料等の管理及び返還 ・秘密保持義務及び個人情報保護義務（個人情報取扱特記事項） ・セキュリティ要件（情報資産の管理方法、遵守すべき事項及び判断基準等） ＜団体内統合宛名システムにおける措置＞ 委託契約書において個人情報取扱特記事項を明記している。 ・秘密の保持 ・収集の制限 ・目的外利用・提供の禁止 ・漏えい、滅失及びき損の防止 ・複写又は複製の禁止 ・再委託の禁止（承諾を受けたものは除く） ・資料等の返還等 ・取扱状況についての指示等 ・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	①都道府県サーバの運用及び監視に関する業務 ・委託先である機構と再委託先の契約において、個人情報保護の条項を設けており、従事者への周知を契約で規定している。 ・再委託する業務は、直接本人確認情報に係らない（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）業務を対象としている。 ・委託元は、委託を受けた者に対して、委託元自らが果たすべき安全管理措置と同等の措置が講じられるよう必要かつ適切な監督を行っている。再委託を行う場合は、委託元がその必要性を厳しく審査し、再委託先に対して、委託先と同等の安全管理措置を義務付け、必要かつ適切な監督を行っている。 ②代表端末、業務端末等機器の保守管理に関する業務 ③代表端末、業務端末等機器の運用管理に関する業務 ・再委託する業務は、本人確認情報に直接係わらない（本人確認情報に直接アクセスできず、閲覧・更新・削除等を行わない）業務を対象としている。 ・上記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について、当該契約書内において再委託先も対象としている。
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
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		
都道府県サーバの運用及び監視に関する業務において、再委託先の選定については、平成25年1月24日、都道府県サーバ集約に伴う調達評価委員会（都道府県の各ブロックから推薦された新潟県、長野県、富山県、和歌山県、香川県、愛媛県、岡山県および福岡県により構成）が、入札の評価基準の作成に参加し、適切な再委託先となるよう監督している。		

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）	[　　] 提供・移転しない
リスク1： 不正な提供・移転が行われるリスク	
特定個人情報の提供・移転の記録	[　　記録を残している　　] ＜選択肢＞ 1）記録を残している　2）記録を残していない
具体的な方法	・都道府県知事保存本人確認情報の提供・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年間保存する。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	・都道府県知事保存本人確認情報の提供・移転は番号法及び住基法の規定により制限される。 ・操作者が業務を行う上で必要な範囲内の権限のみを付与し、操作権限のない者はアクセスできない。 ・システムの操作履歴（業務アクセスログ・操作ログ）を採取・保管し、月１回程度、定期的に分析を行う。
その他の措置の内容	「サーバ室等への入室権限」及び「操作者権限」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、媒体へのデータ出力（書き込み）の際にその記録を残すとともに、必要に応じてシステムを管理する職員が立会う。
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	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、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、システム管理者の承認を必要とし、媒体へのデータ出力（書き込み）の際にはその記録を残すとともに、必要に応じてシステムを管理する職員が立会う。 回線連携を用いる場合、都道府県サーバの代表端末または業務端末から庁内システム（宛名管理システムを含む。）へのアクセスは、共有フォルダだけに制限する。また、都道府県サーバの代表端末または業務端末と庁内のネットワーク間の接続はファイアウォールを経由することとし、必要な通信以外は行えないように制限する。
リスクへの対策は十分か	[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である　3）課題が残されている
リスク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。 ・都道府県知事保存本人確認情報の開示請求があった場合は、当該情報と請求書の突合を複数の職員により実施する。 《誤った相手に提供・移転してしまうリスクへの措置》 ・市町村CSおよび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。 ・回線連携を用いる場合、都道府県サーバの代表端末または業務端末から庁内システム（宛名管理システムを含む。）へのアクセスは、共有フォルダだけに制限する。また、都道府県サーバの代表端末または業務端末と庁内のネットワーク間の接続はファイアウォールを経由することとし、必要な通信以外は行えないように制限する。 ・都道府県知事保存本人確認情報の開示請求については、請求者に対し、身分証明書（個人番号カード等）を提示させることにより厳格な本人確認を行う。
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	
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	＜住民基本台帳ネットワークシステムにおける措置＞ ・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。 ・集約センターにおいては、サーバ設置場所、記録媒体の保管場所を施錠管理する。 ・県においては、代表端末及び記録媒体を保管する室の出入口に機械による入退室管理設備を設置し、代表端末設置場所への入退室者を特定、管理するとともに、さらに代表端末及び記録媒体の保管場所を施錠管理する。 ・県においては、すべての業務端末に覗き見防止フィルタを貼付するとともに、担当者以外の職員や来庁者等からのぞき込めない場所に設置する。また、すべての業務端末にセキュリティワイヤを施し、端末が室外に持ち出されることがないよう措置を講じる。 ・磁気ディスクを廃棄するときは、物理的破壊することにより記録された情報を読み出せないようにする。 ＜団体内統合宛名システムにおける措置＞ ・団体内統合宛名システムをデータセンターに設置し、入館管理及び監視カメラによる監視を行う。 ・データセンターにおいて、サーバ、サーバの管理機能にアクセス可能な端末、及び特定個人情報の保存媒体等を設置しているサーバ室への入退室管理、監視及び施錠管理する。	
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	＜住民基本台帳ネットワークシステムにおける措置＞ ・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の適用、住基ネット業務アプリケーションの修正プログラムの適用、ウイルス対策ソフトの定期的パターン更新を随時行う。 ・庁内の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。 ・集約センターにおいて、ファイアウォールを導入し、ログの解析を行う。 ＜団体内統合宛名システムにおける措置＞ ・ネットワークを通じて悪意の第三者が侵入しないよう、ファイアウォールを設置する。 ・コンピュータウィルス対策ソフトウェアを導入する。 ・OSには随時パッチ適用を実施する。	
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	＜住民基本台帳ネットワークシステムにおける措置＞ 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民基本台帳ネットワークシステムを通して都道府県知事保存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。 ＜団体内統合宛名システムにおける措置＞ 各業務システムから提供される団体内統合宛名システムの登録者については、住民基本台帳ネットワークシステムから定期的に4情報を受領して最新の情報に更新する。	
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	＜住民基本台帳ネットワークシステムにおける措置＞ ・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）に定める期間を経過した後にシステム的に消去する。 ・磁気ディスクの廃棄時は、物理的破壊などの方法により内容を読み出すことができないようにするとともに、その記録を残す。また、廃棄を外部委託する場合は、受託者に廃棄証明書の提出を義務づける。 ・帳票の廃棄時には、裁断または溶解等を行うとともに、その記録を残す。 ＜団体内統合宛名システムにおける措置＞ ・システム上、保管期間を経過した特定個人情報は一括して削除する仕組みとする。 ・磁気ディスクの廃棄時は、規定に基づき、帳票等を作成し、保管及び廃棄の運用が適切になされていることを適時確認するとともに、その記録を残す。	
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		
＜団体内統合宛名システムにおける措置＞ 団体内統合宛名システムにおいて、団体内統合宛名番号で管理する必要がなくなった時点で、不要な特定個人情報は随時システムから削除する。		

Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※（7. リスク1⑨を除く。）

1. 特定個人情報ファイル名	
符号取得要求ファイル	
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	符号取得要求ファイルは、県が各業務システムで保有する社会保障・税関連の特定個人情報の複製を中間サーバに生成する際、対象者が中間サーバに未登録であった場合のみ作成される。 この未登録チェックは中間サーバに複製を作成する前作業において、個人番号と4情報を元に厳重な名寄せ確認作業を団体統合宛名システム上で実施した後に自動生成されるため、対象者以外の符号生成要求は発生しない。
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	符号取得要求ファイルは、番号法施行令第20条（情報提供用個人符号の取得）により、情報提供ネットワークシステムと連携して中間サーバ上で生成されるファイルであり、人的な操作を介さないことから必要な情報以外を入手することがないようシステム上担保されている。
その他の措置の内容	―
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2： 不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	符号取得要求ファイルは、番号法施行令第20条（情報提供用個人符号の取得）により、情報提供ネットワークシステムと連携して中間サーバ上で生成されるファイルであり、人的な操作を介さないことから不適切な方法で入手することがないようシステム上担保されている。
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
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	符号取得要求ファイルは、県が各業務システムで保有する社会保障・税関連の特定個人情報の複製を中間サーバに生成する際、対象者が中間サーバに未登録であった場合のみ作成される。 この未登録チェックは中間サーバに複製を作成する前作業において、個人番号と4情報を元に厳重な名寄せ確認作業を団体統合宛名システム上で実施した後に自動生成されるため、厳格な本人確認ができている。
個人番号の真正性確認の措置の内容	団体内統合宛名システムと中間サーバ間で、確実にデータ連携ができていることをシステム上で論理チェックを行う仕組みとする。
特定個人情報の正確性確保の措置の内容	システムから出力された符号取得要求ファイルについては、人的な編集作業を一切行わないこととし、業務端末又は代表端末に引き継いで正確性を確保する。
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	符号取得要求ファイルは、中間サーバ端末から団体内統合宛名システムの受渡し専用フォルダ内に書き出し後、住民基本台帳ネットワークシステムの業務端末又は代表端末側から、その受渡し専用フォルダ内の符号取得要求ファイルを取り込むこととし、入手の際に符号取得要求ファイルを外部に取り出すことができないよう措置を講じる。
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		団体内統合宛名システムで厳格に紐付け管理された特定個人情報のみが対象となるので、目的を超えた紐付けが行われることはない。
事務で使用するその他のシステムにおける措置の内容		符号生成に必要のない情報は保有しない。
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	符号取得要求ファイルの受け渡しを行う団体内統合宛名システムの受渡し専用フォルダへのアクセスは代表端末及び業務端末から行うものであり、当該端末の操作にあたっては、事前にシステム管理者の承認を得た操作者のみに付与された照合ID及び照合情報（静脈による生体認証）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	・操作者照合情報登録者名簿を作成し、アクセス権限の発効・失効の履歴を適切に管理する。 ・退職や人事異動（担当替え含む。）等により、操作者照合情報の削除依頼通知を受けたときは、直ちに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	・操作者に対し、業務に応じた必要範囲内の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及び業務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	・業務端末の使用にあたっては、事前に操作者の属する部署の長より申請書を提出させるとともに、業務端末使用簿に利用日時、所属、氏名を記載する。 ・システムの操作履歴（業務アクセスログ・操作ログ）を採取・保管し、月１回程度、定期的に分析を行う。 ・システムの操作履歴については7年間、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		・システムの操作履歴（業務アクセスログ・操作ログ）を採取・保管し、月１回程度、定期的に分析を行う。 ・住民基本台帳ネットワークシステム利用にあたっての留意事項を記載したレジュメを作成し、業務上必要のない本人確認情報検索又は抽出を行わないようシステム操作者に対し厳格に指導する。 ・システム利用職員への研修会において、事務外利用の禁止等について指導する。 ・操作者への権限付与に際して、操作者本人から、「住基法その他関係法令等の遵守」「目的外利用を行わない」、「個人情報保護およびセキュリティの確保に努める」旨を記した誓約書の提出を求める。 ・「奈良県住民基本台帳ネットワークシステム管理規程」「奈良県住民基本台帳ネットワークシステムセキュリティ基本方針書」「奈良県住民基本台帳ネットワークシステムの管理者等が定める事項」「奈良県住民基本台帳ネットワークシステム用業務端末運用管理要領」「本人確認情報開示等実施要領」を策定している。 ・違反行為を行った場合は、法令の罰則規定により措置を講じる。
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。 ・システムの操作履歴（業務アクセスログ・操作ログ）を採取・保管し、月１回程度、不正なファイル複製がないことを確認する。 ・違反行為を行った場合は、法令の罰則規定により措置を講じる。
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
本人確認情報の利用にあたり、以下の措置を講じる。 ・スクリーンセーバ等を利用して、長時間にわたり本人確認情報を表示させない ・都道府県サーバの代表端末を施錠管理された安全な場所に設置する ・すべての業務端末のディスプレイに覗き見防止用シートを貼付するとともに、来庁者から見えない位置に設置する ・システム操作者は本人確認情報が表示された画面のハードコピーを取得しない ・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			
特定個人情報ファイルの閲覧者・更新者の制限	[ ]	＜選択肢＞ 1）制限している	2）制限していない
具体的な制限方法			
特定個人情報ファイルの取扱いの記録	[ ]	＜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			
特定個人情報の提供ルール	[ ]	＜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			
特定個人情報の消去ルール	[ ]	＜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			
委託契約書中の特定個人情報ファイルの取扱いに関する規定	[ ]	＜選択肢＞ 1）定めている	2）定めていない
規定の内容			
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	[ ]	＜選択肢＞ 1）特に力を入れて行っている 3）十分に行っていない	2）十分に行っている 4）再委託していない
具体的な方法			
その他の措置の内容			
リスクへの対策は十分か	[ ]	＜選択肢＞ 1）特に力を入れている 3）課題が残されている	2）十分である

特定個人情報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	符号取得要求ファイルの受け渡し記録はシステム上で管理し、7年間保存する。
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	・都道府県知事保存本人確認情報の提供・移転は番号法及び住基法の規定により制限される。 ・操作者が業務を行う上で必要な範囲内の権限のみを付与し、操作権限のない者はアクセスできない。 ・システムの操作履歴（業務アクセスログ・操作ログ）を採取・保管し、月1回程度、定期的に分析を行う。
その他の措置の内容	「サーバ室等への入室権限」及び「操作者権限」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、媒体へのデータ出力（書き込み）の際にその記録を残すとともに、必要に応じてシステムを管理する職員が立会う。
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	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、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、システム管理者の承認を必要とし、媒体へのデータ出力（書き込み）の際にはその記録を残すとともに、必要に応じてシステムを管理する職員が立会う。 回線連携を用いる場合、都道府県サーバの代表端末または業務端末から庁内システム（宛名管理システムを含む。）へのアクセスは、共有フォルダだけに制限する。また、都道府県サーバの代表端末または業務端末と庁内のネットワーク間の接続はファイアウォールを経由することとし、必要な通信以外は行えないように制限する。
リスクへの対策は十分か	[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である　3）課題が残されている
リスク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	システムから出力された符号取得要求ファイルについては、人的な編集作業を一切行わないこととし、業務端末又は都道府県サーバの代表端末に引き継いで正確性を確保する。
リスクへの対策は十分か	[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である　3）課題が残されている
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	＜住民基本台帳ネットワークシステムにおける措置＞ ・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。 ・集約センターにおいては、サーバ設置場所、記録媒体の保管場所を施錠管理する。 ・県においては、代表端末及び記録媒体を保管する室の出入口に機械による入退室管理設備を設置し、代表端末設置場所への入退室者を特定、管理するとともに、さらに代表端末及び記録媒体の保管場所を施錠管理する。 ・県においては、すべての業務端末に覗き見防止フィルタを貼付するとともに、担当者以外の職員や来庁者等からのぞき込めない場所に設置する。また、すべての業務端末にセキュリティワイヤを施し、端末が室外に持ち出されることがないよう措置を講じる。 ・磁気ディスクを廃棄するときは、物理的破壊することにより記録された情報を読み出せないようにする。 ＜団体内統合宛名システムにおける措置＞ ・団体内統合宛名システムをデータセンターに設置し、入館管理及び監視カメラによる監視を行う。 ・データセンターにおいて、サーバ、サーバの管理機能にアクセス可能な端末、及び特定個人情報の保存媒体等を設置しているサーバ室への入退室管理、監視及び施錠管理する。	
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	＜住民基本台帳ネットワークシステムにおける措置＞ ・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の適用、住基ネット業務アプリケーションの修正プログラムの適用、ウイルス対策ソフトの定期的パターン更新を随時行う。 ・庁内の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。 ・集約センターにおいて、ファイアウォールを導入し、ログの解析を行う。 ＜団体内統合宛名システムにおける措置＞ ・ネットワークを通じて悪意の第三者が侵入しないよう、ファイアウォールを設置している。 ・コンピュータウィルス対策ソフトウェアを導入する。 ・OSには随時パッチ適用を実施する。	
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	符号取得要求ファイルは、新たに特定個人情報を中間サーバに登録する者が対象となるため、死者の符号取得要求ファイルの受け渡しは発生しない。	
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： 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	符号取得要求ファイルは、新たに特定個人情報を中間サーバに登録際に、一時的に使用され、符号生成後は消去されるファイルであるため、古い情報が保管される続けるリスクは発生しない。	
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	符号取得要求ファイルは、新たに特定個人情報を中間サーバに登録際に、一時的に使用され、符号生成後は消去されるファイルであるため、特定個人情報が消去されずいつまでも存在するリスクは発生しない。	
その他の措置の内容	―	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の保管・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	＜住民基本台帳ネットワークシステムにおける措置＞ 機構（住民基本台帳ネットワークシステム全国センター）が作成するセキュリティ対策規定等の項目に係る自己点検チェックリスト（都道府県版）を用いて、定期的（年１回）に職員による自己点検項目の遵守状況の確認を実施する。 ＜団体内統合宛名システムにおける措置＞ 内部手順書等に基づき、運用に携わる職員及び事業者に対し、定期的に自己点検を実施することとしている。
②監査		[　　十分に行っている　　] ＜選択肢＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
	具体的な内容	＜住民基本台帳ネットワークシステムにおける措置＞ ・住基ネット管理規程等に基づき、住基担当職員および住基担当以外の県職員による自己監査を毎年定期的に行うこととしている。 ・操作ログの監視等により不適切な取扱いが判明した場合や自己点検において結果が不十分な所属に対して、現地監査を行うこととしている。（現地監査は、システム管理者である市町村振興課が、システム利用部署（旅券事務所・建築課など業務端末設置部署　等）に対し、現地へ赴き、監査を実施する。） ・外部監査は5年毎を目処に定期的に行うこととしている。 ＜団体内統合宛名システムにおける措置＞ 内部手順書等に基づき、定期的に監査を行うこととしている。
2. 従業者に対する教育・啓発		
従業者に対する教育・啓発		[　　十分に行っている　　] ＜選択肢＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
	具体的な方法	＜住民基本台帳ネットワークシステムにおける措置＞ ・新規配属時（異動・担当替えを含む。）に前任者等から十分な引き継ぎを行うとともに、システム管理者が実施する研修会の受講を義務づける。 ・年１回、機構が実施するe-ラーニングによるセキュリティ研修およびシステム管理者が実施する研修会の受講を義務づける。 ＜団体内統合宛名システムにおける措置＞ ・職員に対しては、特定個人情報を扱う業務に携わる前に個人情報保護に関する研修を行う。 ・委託業者に対して、契約内容に個人情報保護に関する特記事項を明記し、秘密保持契約を締結している。 ・委託業者に対しては、契約内容に個人情報保護に関する研修の実施を義務付けている。 ・違反行為を行った者に対しては、その都度指導する。違反行為の程度によっては懲戒の対象となりうる。
3. その他のリスク対策		
－		

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	総務部総務課県政情報係 〒630－8501　奈良市登大路町30番地 TEL:0742-27-8348　FAX:0742-27-1323
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	県ホームページ上に、請求先、請求方法、諸費用等を掲載する。
③手数料等	[　　有料　　]　　＜選択肢＞ 1) 有料　　2) 無料 （手数料額、納付方法：　手数料額：請求、閲覧は無料。写しの交付を希望する場合は、写しの作成費用（白黒1枚10円、カラー1枚50円）の負担が必要　） 納付方法：現金
④個人情報ファイル簿の公表	[　　行っている　　]　　＜選択肢＞ 1) 行っている　　2) 行っていない
個人情報ファイル名	個人情報取扱事務登録簿のうち ・住民基本台帳ネットワークシステムに関する事務 ・同　（本人確認情報の提供及び利用の状況に関する情報の保存）
公表場所	県庁東棟1階県政情報センター
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	・地域振興部市町村振興課 〒630-8501　奈良市登大路町30番地 TEL:0742-27-8422　FAX:0742-23-8439 ・総務部情報システム課 〒630-8501　奈良市登大路町30番地 TEL:0742-27-2052　FAX:0742-23-4196
②対応方法	問い合わせ受付時に受付票を起票し、対応について記録を残す。

Ⅵ　評価実施手続

1. 基礎項目評価	
①実施日	平成26年12月22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	奈良県パブリックコメント手続要綱に基づき実施
②実施日・期間	平成27年1月14日～平成27年2月13日
③期間を短縮する特段の理由	－
④主な意見の内容	意見なし
⑤評価書への反映	－
3. 第三者点検	
①実施日	平成27年2月12日（木）、平成27年3月3日（火）、平成27年3月19日（木）
②方法	奈良県個人情報保護審議会において第三者点検を受けた。
③結果	第三者点検により以下の答申を受けた。 「　特定個人情報保護評価指針（平成26年4月18日特定個人情報保護委員会告示第４号）第10の1(2)に定める適合性及び妥当性を有していると認められます。 　なお、番号制度の導入により個人の権利利益が侵害されることへの住民の懸念を払拭するために、実施機関においては、当該評価書に記載されたリスク対策を確実に実施するとともに、実施状況について住民に説明できるよう、その記録及び保存に努められたい。」
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