

# 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。
- ・都道府県サーバ及び附票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、都道府県サーバ及び附票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装置を設けて、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

## 個人情報保護委員会 承認日【行政機関等のみ】

## 公表日

## 項目一覧

<b>I 基本情報</b>
(別添1) 事務の内容
<b>II 特定個人情報ファイルの概要</b>
(別添2) 特定個人情報ファイル記録項目
<b>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</b>
<b>IV その他のリスク対策</b>
<b>V 開示請求、問合せ</b>
<b>VI 評価実施手続</b>
(別添3) 変更箇所

# I 基本情報

## 1. 特定個人情報ファイルを取り扱う事務

①事務の名称	住民基本台帳ネットワークに関する事務
②事務の内容 ※	<p>住民基本台帳ネットワークに関する事務は、「1. 本人確認情報の管理及び提供等に関する事務」及び「2. 附票本人確認情報の管理及び提供等に関する事務」に分かれる。</p> <p>1. 本人確認情報の管理及び提供等に関する事務          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(住基ネット)を市町村と共同して構築している。</p> <p>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、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。</p> <p>県では、住基法の規定に従い、特定個人情報を以下の事務で取り扱う。(別添1を参照)</p> <p>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機構への通知          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</p> <p>2. 附票本人確認情報の管理及び提供等に関する事務          県は、市町村における市町村CS、都道府県における附票都道府県サーバ及び機構における附票全国サーバ等により構成される「附票連携システム」において、国外転出者に係る本人確認を行うための社会的基盤としての役割を担うため、4情報(氏名、住所、生年月日、性別)、住民票コード及びこれらの変更情報で構成される「都道府県知事保存附票本人確認情報ファイル」を作成し、戸籍の附票に関する記録を正確に行う責務がある。そのため、附票本人確認情報の管理及び提供等に係る以下の事務を実施する。なお、都道府県知事保存附票本人確認情報(以下条文に併せて記載する場合は、「都道府県知事保存附票本人確認情報」とし、それ以外の記載は、「附票本人確認情報」とする。)には、個人番号は含まれない。</p> <p>①磁気ディスクによる特定個人情報ファイルの管理          ②市町村からの附票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機構への通知          ③都道府県知事から附票本人確認情報に係る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附票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附票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機構への附票本人確認情報の照会</p>
③対象人数	<p>[ 30万人以上 ]</p> <p>&lt;選択肢&gt;          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</p>

## 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	<p>住民基本台帳ネットワークシステム</p> <p>※「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。</p>
	<p>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。</p> <p>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。</p>

## ②システムの機能

### 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

：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の間を受渡し専用装置を設けて、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
	[ <input checked="" type="radio"/> ] 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	附票連携システム ※「3. 特定個人情報ファイル名」に示す「都道府県知事保存附票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、附票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、附票連携システムの中の附票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	<p>1. 附票本人確認情報の更新          : 都道府県知事保存附票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を経由して通知された附票本人確認情報の更新情報を元に当該ファイルを更新し、附票全国サーバに対して当該附票本人確認情報の更新情報を通知する。</p> <p>2. 県の他の執行機関への情報提供又は他部署への移転          : 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4情報等に対応付く附票本人確認情報を都道府県知事保存附票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。          その際、番号法で認められた場合に限り、県の他の執行機関又は他部署からの求めに応じ、附票本人確認情報の提供・移転に併せて当該個人の住民票コードを用いて、都道府県知事保存本人確認情報ファイルから個人番号を抽出し、照会元に提供・移転する場合がある。</p> <p>3. 附票本人確認情報の開示          : 法律に基づく住民による自己の附票本人確認情報の開示請求に対応するため、当該個人の附票本人確認情報を都道府県知事保存附票本人確認情報ファイルから抽出し、帳票に出力する。</p> <p>4. 機構への情報照会          : 附票全国サーバに対して住民票コード又は4情報の組合せをキーとした附票本人確認情報照会要求を行い、該当する個人の附票本人確認情報を受領する。</p> <p>5. 附票本人確認情報検索          : 附票都道府県サーバの代表端末又は業務端末(都道府県サーバと共用する。)において入力された4情報(氏名、住所、性別、生年月日)の組合せをキーに都道府県知事保存附票本人確認情報ファイルを検索し、検索条件に該当する附票本人確認情報の一覧を画面上に表示する。</p> <p>6. 附票本人確認情報整合          : 都道府県知事保存附票本人確認情報ファイルの正確性を担保するため、市町村から附票本人確認情報を受領し、当該附票本人確認情報を用いて当該ファイルに記録された附票本人確認情報の整合性確認を行う。</p> <p>7. 個人番号制度の運用に伴う情報連携          : 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の間に受渡し専用装置を設けて、本人確認情報ファイル等の受け渡しを行う。</p>
----------	---

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
	[ <input checked="" type="radio"/> ] 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
----------	-------------



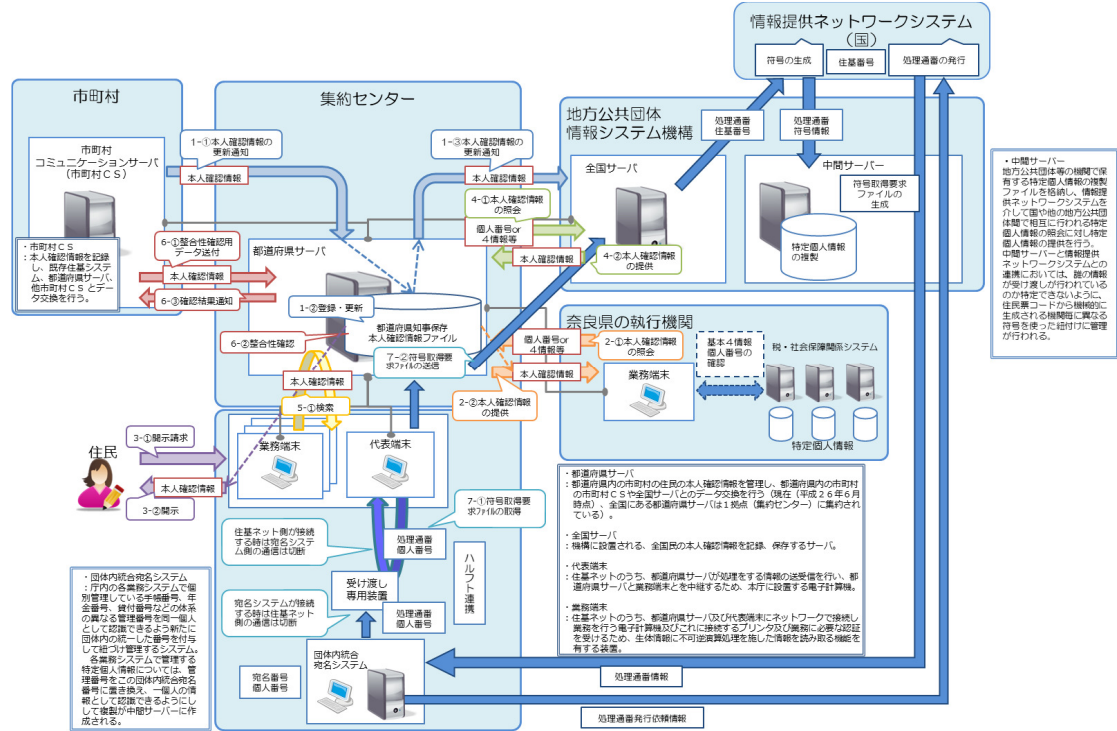
3. 特定個人情報ファイル名	
(1) 都道府県知事保存本人確認情報ファイル (2) 都道府県知事保存附票本人確認情報ファイル (3) 符号取得要求ファイル	
4. 特定個人情報ファイルを取り扱う理由	
①事務実施上の必要性	<p>県では、都道府県知事保存本人確認情報ファイル、都道府県知事保存附票本人確認情報ファイル及び符号取得要求ファイルを、下記に記載の通りの必要性から取り扱う。</p> <p>(1) 都道府県知事保存本人確認情報ファイル            ・都道府県知事保存本人確認情報ファイルは、転出入があった場合等にスムーズな住民情報の処理を行うため、また全国的な本人確認手段として、1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。</p> <p>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(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、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。</p> <p>(2) 都道府県知事保存附票本人確認情報ファイル            ・都道府県知事保存附票本人確認情報ファイルは、国外転出者に係る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、附票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。</p> <p>①附票連携システムに係る附票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附票本人確認情報を管理する。            ②市町村からの附票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附票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県の他の執行機関又は他部署からの照会に基づき、附票本人確認情報を提供・移転する。その際、番号法で認められた場合に限り、県の他の執行機関又は他部署からの求めに応じ、附票本人確認情報の提供・移転に併せて当該個人の住民票コードを用いて、都道府県知事保存本人確認情報ファイルから個人番号を抽出し、照会元に提供・移転する場合がある。            ④本人からの請求に基づき、当該個人の附票本人確認情報を開示する。            ⑤附票本人確認情報の管理及び提供等に関する事務において、附票本人確認情報を検索する。            ⑥市町村において保存する附票本人確認情報との整合性を確認する。</p> <p>(3) 符号取得要求ファイル            ・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シ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。</p>
②実現が期待されるメリット	<p>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)につながるが見込まれる。            また、国外転出者を含め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。</p>
5. 個人番号の利用 ※	
	<p>住民基本台帳法(昭和42年7月25日法律第81号)            ・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)</p>

法令上の根拠	<ul style="list-style-type: none"> <li>・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)</li> <li>・第30条の8(本人確認情報の誤りに関する機構の通報)</li> <li>・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)</li> <li>・第30条の13(都道府県の条例による本人確認情報の提供)</li> <li>・第30条の15(本人確認情報の利用)</li> <li>・第30条の22(市町村間の連絡調整等)</li> <li>・第30条の32(自己の本人確認情報の開示)</li> <li>・第30条の35(自己の本人確認情報の訂正)</li> <li>・第30条の44の6第3項(都道府県知事保存附票本人確認情報(住民票コードに限る。)の利用)</li> </ul>
<b>6. 情報提供ネットワークシステムによる情報連携 ※</b>	
①実施の有無	<div style="display: flex; justify-content: space-between; align-items: center;"> <span>[ 実施しない ]</span> <div style="text-align: right;"> <p>&lt;選択肢&gt;</p> <p>1) 実施する</p> <p>2) 実施しない</p> <p>3) 未定</p> </div> </div>
②法令上の根拠	-
<b>7. 評価実施機関における担当部署</b>	
①部署	知事公室市町村振興課
②所属長の役職名	市町村振興課長
<b>8. 他の評価実施機関</b>	
-	



**(別添1) 事務の内容**

**(1) 本人確認情報の管理及び提供等に関する事務**



**(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(特定個人情報を含まない)。
- 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側と代表端末または業務端末側との間に受渡し専用装置を設けて、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間に受渡し専用装置を介して受領し、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。情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。



- 6-①.市町村CSより、附票都道府県サーバに対し、整合性確認用の附票本人確認情報を送付する。
- 6-②.附票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附票本人確認情報を用いて都道府県知事保存附票本人確認情報ファイルの整合性確認を行う。
- 6-③.附票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側と代表端末または業務端末側との間に受渡し専用装置を設けて、附票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間に受渡し専用装置を介して受領し、附票全国サーバに送信する。  
※附票全国サーバは、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。情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	
(1)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 [ <input type="checkbox"/> ] 個人番号 [ <input type="checkbox"/> ] 個人番号対応符号 [ <input type="checkbox"/> ] その他識別情報(内部番号) ・連絡先等情報 [ <input type="checkbox"/> ] 4情報(氏名、性別、生年月日、住所) [ <input type="checkbox"/> ] 連絡先(電話番号等) [ <input type="checkbox"/> ] その他住民票関係情報 ・業務関係情報 [ <input type="checkbox"/> ] 国税関係情報 [ <input type="checkbox"/> ] 地方税関係情報 [ <input type="checkbox"/> ] 健康・医療関係情報 [ <input type="checkbox"/> ] 医療保険関係情報 [ <input type="checkbox"/> ] 児童福祉・子育て関係情報 [ <input type="checkbox"/> ] 障害者福祉関係情報 [ <input type="checkbox"/> ] 生活保護・社会福祉関係情報 [ <input type="checkbox"/> ] 介護・高齢者福祉関係情報 [ <input type="checkbox"/> ] 雇用・労働関係情報 [ <input type="checkbox"/> ] 年金関係情報 [ <input type="checkbox"/> ] 学校・教育関係情報 [ <input type="checkbox"/> ] 災害関係情報 [ <input type="checkbox"/> ] 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
⑥事務担当部署	知事公室市町村振興課

3. 特定個人情報の入手・使用									
①入手元 ※	<input type="checkbox"/> 本人又は本人の代理人 <input type="checkbox"/> 評価実施機関内の他部署 ( ) <input type="checkbox"/> 行政機関・独立行政法人等 ( ) <input checked="" type="checkbox"/> 地方公共団体・地方独立行政法人 ( 市町村 ) <input type="checkbox"/> 民間事業者 ( ) <input type="checkbox"/> その他 ( )								
②入手方法	<input type="checkbox"/> 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 <input type="checkbox"/> 電子メール [ ] 専用線 [ ] 庁内連携システム <input type="checkbox"/> 情報提供ネットワークシステム <input checked="" type="checkbox"/> 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、削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	-							
⑦使用の主体	使用部署 ※	知事公室市町村振興課							
	使用者数	[ 10人未満 ] <table border="0" style="display: inline-table; vertical-align: middle;"> <tr> <td colspan="2" style="text-align: center;">&lt;選択肢&gt;</td> </tr> <tr> <td style="text-align: center;">1) 10人未満</td> <td style="text-align: center;">2) 10人以上50人未満</td> </tr> <tr> <td style="text-align: center;">3) 50人以上100人未満</td> <td style="text-align: center;">4) 100人以上500人未満</td> </tr> <tr> <td style="text-align: center;">5) 500人以上1,000人未満</td> <td style="text-align: center;">6) 1,000人以上</td> </tr> </table>	<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
<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								

<p>⑧使用方法 ※</p>	<ul style="list-style-type: none"> <li>・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)。</li> <li>・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)。</li> <li>・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)。</li> <li>・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)。</li> <li>・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。</li> <li>・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。</li> </ul>
<p>情報の突合 ※</p>	<ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> <li>・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。</li> <li>・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。</li> </ul>
<p>情報の統計分析 ※</p>	<p>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。</p>
<p>権利利益に影響を与え得る決定 ※</p>	<p>該当なし</p>
<p>⑨使用開始日</p>	<p>平成27年6月1日</p>

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	[ <input checked="" type="checkbox"/> ] 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。





<b>委託事項3</b>		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	<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	[ <input checked="" type="checkbox"/> ] 提供を行っている ( 3 ) 件 [ <input checked="" type="checkbox"/> ] 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 [ <input checked="" type="checkbox"/> ] 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、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「整備法」という。)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 [ <input checked="" type="checkbox"/> ] 電子記録媒体(フラッシュメモリを除く。) [ <input checked="" type="checkbox"/> ] フラッシュメモリ [ ] 紙 [ <input checked="" type="checkbox"/> ] 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。

<b>提供先3</b>	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    [ <input checked="" type="radio"/> ] 紙 [ <input checked="" type="radio"/> ] 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。
<b>移転先1</b>	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2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    [ <input checked="" type="radio"/> ] 電子記録媒体(フラッシュメモリを除く。) [ <input checked="" type="radio"/> ] フラッシュメモリ    [    ] 紙 [ <input checked="" type="radio"/> ] 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。



## 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)都道府県知事保存附票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 ※	県内のいずれかの市町村において、住基法第16条(戸籍の附票の作成)に基づき戸籍の附票に記録された住民。 ※消除者を含む。
その必要性	本特定個人情報ファイル(都道府県知事保存附票本人確認情報ファイル)において県内の戸籍の附票に記録された全ての住民の情報を保有し、その記録を常に正確に更新・管理・提供・移転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 ※	<ul style="list-style-type: none"> <li>・識別情報                [ <input type="checkbox"/> ] 個人番号 [ <input type="checkbox"/> ] 個人番号対応符号 [ <input type="checkbox"/> ] その他識別情報(内部番号)</li> <li>・連絡先等情報                [ <input type="checkbox"/> ] 4情報(氏名、性別、生年月日、住所) [ <input type="checkbox"/> ] 連絡先(電話番号等)                [ <input type="checkbox"/> ] その他住民票関係情報</li> <li>・業務関係情報                [ <input type="checkbox"/> ] 国税関係情報 [ <input type="checkbox"/> ] 地方税関係情報 [ <input type="checkbox"/> ] 健康・医療関係情報                [ <input type="checkbox"/> ] 医療保険関係情報 [ <input type="checkbox"/> ] 児童福祉・子育て関係情報 [ <input type="checkbox"/> ] 障害者福祉関係情報                [ <input type="checkbox"/> ] 生活保護・社会福祉関係情報 [ <input type="checkbox"/> ] 介護・高齢者福祉関係情報                [ <input type="checkbox"/> ] 雇用・労働関係情報 [ <input type="checkbox"/> ] 年金関係情報 [ <input type="checkbox"/> ] 学校・教育関係情報                [ <input type="checkbox"/> ] 災害関係情報                [ <input type="checkbox"/> ] その他 ( その他戸籍の附票関係情報(戸籍の表示に係る情報は含まない。) )</li> </ul>
その妥当性	<ul style="list-style-type: none"> <li>・4情報、その他戸籍の附票関係情報(戸籍の表示に係る情報は含まない。)</li> <li>・法令に基づき戸籍の附票に記録された者に関する記録を正確に行う上で、戸籍の附票の記載等に係る附票本人確認情報(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。なお、別添2に記載のとおり、記録項目には戸籍の表示に係る情報(本籍及び筆頭者の氏名)は含まない。</li> <li>・個人番号                国外転出者に係る事務処理に関し、番号法で認められた場合に限り、県の他の執行機関等からの求めに応じ、当該個人の住民票コードを用いて、都道府県知事保存本人確認情報ファイルから個人番号を抽出し、附票都道府県サーバに連携する場合がある。提供又は移転後、個人番号は、都道府県知事保存附票本人確認情報ファイルに保有することはない</li> </ul>
全ての記録項目	別添2を参照。
⑤保有開始日	「情報通信技術の活用による行政手続等に係る関係者の利便性の向上並びに行政運営の簡素化及び効率化を図るための行政手続等における情報通信の技術の利用に関する法律等の一部を改正する法律(令和元年法律第16号)」附則第1条第10号にて規定される公布から起算して5年を超えない範囲内の政令で定める日。
⑥事務担当部署	知事公室市町村振興課

3. 特定個人情報の入手・使用	
①入手元 ※	<input type="checkbox"/> 本人又は本人の代理人 <input type="checkbox"/> 評価実施機関内の他部署 ( ) <input type="checkbox"/> 行政機関・独立行政法人等 ( ) <input checked="" type="checkbox"/> 地方公共団体・地方独立行政法人 ( 市町村 ) <input type="checkbox"/> 民間事業者 ( ) <input checked="" type="checkbox"/> その他 ( 都道府県サーバ(※入手には該当しないが、都道府県サーバから個人番号を抽出する場合がある) )
②入手方法	<input type="checkbox"/> 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 <input type="checkbox"/> 電子メール [ <input checked="" type="checkbox"/> ] 専用線 [ ] 庁内連携システム <input type="checkbox"/> 情報提供ネットワークシステム <input type="checkbox"/> その他 ( )
③入手の時期・頻度	<p>戸籍の附票において、附票本人確認情報の変更又は新規作成(出生等)が発生した都度入手する。</p> <p>※番号法別表に掲げる事務につき、県の他の執行機関等から国外転出者に係るものに関し求めがあった場合、個人番号をその都度抽出する場合がある。</p>
④入手に係る妥当性	<p>法令に基づき、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、国外転出者に係る本人確認を行う上で、市町村の戸籍の附票の記載事項に変更が生じた都度、当該市町村を通じて入手し、機構に通知する必要がある。また、入手の手段として、法令に基づき構築された専用回線である、住基ネット(※※)を用いることで、入手に係るリスクを軽減している。</p> <p>※なお、住基法第30条の44の6第3項に基づき、都道府県知事保存附票本人確認情報(住民票コードに限る。)を利用し、第30条の15第1項又は第2項の規定による事務について個人番号を提供することができる。とされている。</p> <p>※※附票連携システムは、住基ネットを利用して構築されている。住基ネットは、保有情報・利用の制限、内部の不正利用の防止、外部からの侵入防止など、セキュリティ確保のための様々な措置が講じられており、平成14年8月5日の稼働後、住基ネットへのハッキングや情報漏えいなどの事件や障害は一度も発生していない。</p>
⑤本人への明示	<p>都道府県知事が当該市町村の区域内における附票本人確認情報を入手することについて、住基法第30条の41(市町村長から都道府県知事への附票本人確認情報の通知等)に明示されている。</p> <p>※都道府県知事が国外転出者に係る個人番号を抽出する場合があることについて、住基法第30条の44の6第3項に明示されている。</p>
⑥使用目的 ※	<p>都道府県知事保存附票本人確認情報ファイルにおいて県内の戸籍の附票に記録された県内の全ての住民の情報を保有し、その記録を常に正確に更新・管理・提供・移転する。</p> <p>※番号法別表に掲げる事務につき、県の他の執行機関等から国外転出者に係るものに関し求めがあった場合、個人番号をその都度抽出し、第30条の15第1項又は第2項の規定による事務について提供する場合がある。</p>
	<p>変更の妥当性</p> <p>-</p>
⑦使用の主体	<p>使用部署 ※</p> <p>知事公室市町村振興課</p>
	<p>使用者数</p> <p>[ 10人未満 ]</p> <p>&lt;選択肢&gt;</p> <p>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</p>
⑧使用方法 ※	<p>・県の他の執行機関又は他部署からの附票本人確認情報の照会要求を受け(県の他の執行機関又は他部署→附票都道府県サーバ)、照会のあった住民票コード又は4情報の組合せを元に都道府県知事保存附票本人確認情報ファイルを検索し、該当する個人の附票本人確認情報を照会元へ提供・移転する(附票都道府県サーバ→県の他の執行機関又は他部署)。</p> <p>※その際、番号法で認められた場合に限り、附票本人確認情報の提供に併せて、当該個人の住民票コードを用いて都道府県知事保存本人確認情報ファイルから個人番号を抽出し、照会元に提供・移転する場合がある。</p>
	<p>情報の突合 ※</p> <p>都道府県知事保存附票本人確認情報ファイルの住民票コードと都道府県知事保存本人確認情報ファイルの個人番号を突合する。</p>
	<p>情報の統計分析 ※</p> <p>該当なし</p>
	<p>権利益に影響を与え得る決定 ※</p> <p>該当なし</p>
⑨使用開始日	<p>「情報通信技術の活用による行政手続等に係る関係者の利便性の向上並びに行政運営の簡素化及び効率化を図るための行政手続等における情報通信の技術の利用に関する法律等の一部を改正する法律(令和元年法律第16号)」附則第1条第10号にて規定される公布から起算して5年を超えない範囲内の政令で定める日。</p>

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 ) 件 1) 委託する 2) 委託しない
委託事項	附票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(集約センター)に集約化することとしたことに伴い、都道府県サーバと同様に附票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、附票本人確認情報に直接係わらない(附票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 都道府県知事保存附票本人確認情報ファイルが保存される附票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、附票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) 1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	[ <input type="checkbox"/> ] 専用線 [ <input type="checkbox"/> ] 電子メール [ <input type="checkbox"/> ] 電子記録媒体(フラッシュメモリを除く。) [ <input type="checkbox"/> ] フラッシュメモリ [ <input type="checkbox"/> ] 紙 [ <input type="checkbox"/> ] 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 附票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、附票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、附票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。
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	[ <input type="checkbox"/> ] 提供を行っている ( 1 ) 件 [ <input type="checkbox"/> ] 移転を行っている ( 1 ) 件 [ <input type="checkbox"/> ] 行っていない
提供先1	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 住基法第30条の44の6第3項(都道府県知事保存附票本人確認情報(住民票コードに限る。))の利用
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、住所、生年月日、性別、個人番号(番号法に基づく県の他の執行機関からの求めがあった場合に限る。) ※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)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	<input type="checkbox"/> 情報提供ネットワークシステム <input type="checkbox"/> 専用線 <input type="checkbox"/> 電子メール <input type="checkbox"/> 電子記録媒体(フラッシュメモリを除く。) <input type="checkbox"/> フラッシュメモリ <input type="checkbox"/> 紙 <input type="checkbox"/> 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。	
<b>移転先1</b>	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2条 住基法第30条の44の6第3項(都道府県知事保存附票本人確認情報(住民票コードに限る。))の利用	
②移転先における用途	住基法別表第五及び奈良県住民基本台帳法施行条例別表第一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移転する情報	住民票コード、氏名、住所、生年月日、性別、個人番号(番号法に基づく県の他部署からの求めがあった場合に限り。) ※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)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	<input type="checkbox"/> 情報提供ネットワークシステム <input type="checkbox"/> 専用線 <input type="checkbox"/> 電子メール <input type="checkbox"/> 電子記録媒体(フラッシュメモリを除く。) <input type="checkbox"/> フラッシュメモリ <input type="checkbox"/> 紙 <input type="checkbox"/> 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。	
<b>6. 特定個人情報の保管・消去</b>		
①保管場所 ※	<附票連携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附票都道府県サーバの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と生体認証(又はパスワード)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	(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	附票本人確認情報の提供に併せて提供される個人番号は、県の他の執行機関又は他部署からの求めにより提供・移転された後は、障害発生等により提供・移転先で情報を受領できなかった場合に備えて、一時的に保存されるのみである。
③消去方法	一時的な保存後にシステムにて自動判別し消去する。	
<b>7. 備考</b>		

## 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)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 ※	<ul style="list-style-type: none"> <li>・識別情報 [ <input type="radio"/> ] 個人番号 [ <input type="checkbox"/> ] 個人番号対応符号 [ <input type="radio"/> ] その他識別情報(内部番号)</li> <li>・連絡先等情報 [ <input type="checkbox"/> ] 4情報(氏名、性別、生年月日、住所) [ <input type="checkbox"/> ] 連絡先(電話番号等) [ <input type="checkbox"/> ] その他住民票関係情報</li> <li>・業務関係情報 [ <input type="checkbox"/> ] 国税関係情報 [ <input type="checkbox"/> ] 地方税関係情報 [ <input type="checkbox"/> ] 健康・医療関係情報 [ <input type="checkbox"/> ] 医療保険関係情報 [ <input type="checkbox"/> ] 児童福祉・子育て関係情報 [ <input type="checkbox"/> ] 障害者福祉関係情報 [ <input type="checkbox"/> ] 生活保護・社会福祉関係情報 [ <input type="checkbox"/> ] 介護・高齢者福祉関係情報 [ <input type="checkbox"/> ] 雇用・労働関係情報 [ <input type="checkbox"/> ] 年金関係情報 [ <input type="checkbox"/> ] 学校・教育関係情報 [ <input type="checkbox"/> ] 災害関係情報 [ <input type="checkbox"/> ] その他 ( )</li> </ul>
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シ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
⑥事務担当部署	知事公室市町村振興課

3. 特定個人情報の入手・使用		
①入手元 ※	<input type="checkbox"/> 本人又は本人の代理人 <input type="checkbox"/> 評価実施機関内の他部署 ( ) <input type="checkbox"/> 行政機関・独立行政法人等 ( ) <input checked="" type="checkbox"/> 地方公共団体・地方独立行政法人 ( 市町村 ) <input type="checkbox"/> 民間事業者 ( ) <input type="checkbox"/> その他 ( )	
②入手方法	<input type="checkbox"/> 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 <input type="checkbox"/> 電子メール [ ] 専用線 [ ] 庁内連携システム <input type="checkbox"/> 情報提供ネットワークシステム <input checked="" type="checkbox"/> その他 ( 受け渡し専用装置 )	
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1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シ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 ※	知事公室市町村振興課
	使用者数	<input type="checkbox"/> 10人未満 ] <ul style="list-style-type: none"> <li>&lt;選択肢&gt;</li> <li>1) 10人未満</li> <li>2) 10人以上50人未満</li> <li>3) 50人以上100人未満</li> <li>4) 100人以上500人未満</li> <li>5) 500人以上1,000人未満</li> <li>6) 1,000人以上</li> </ul>
⑧使用方法 ※		<ul style="list-style-type: none"> <li>・中間サーバで生成された符号取得要求ファイルを受渡し専用装置に保存する。</li> <li>・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、受渡し専用装置内の符号取得要求ファイルを取り込む。</li> <li>・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。</li> <li>・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。</li> <li>・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。</li> <li>・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。</li> <li>・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。</li> <li>・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するため、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。</li> </ul>
	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(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	



## (別添2) 特定個人情報ファイル記録項目

### (1) 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 |
| 25. 旧氏 漢字     | 26. 旧氏 外字数   | 27. 旧氏 ふりがな  |
| 28. 旧氏 外字変更連番 |              |              |

### (2) 都道府県知事保存附票本人確認情報ファイル

#### ア 附票本人確認情報

- |              |                |                  |
|--------------|----------------|------------------|
| 1. 住民票コード    | 2. 氏名 漢字       | 3. 氏名 外字数        |
| 4. 氏名 ふりがな   | 5. 生年月日        | 6. 性別            |
| 7. 住所 市町村コード | 8. 住所 漢字       | 9. 住所 外字数        |
| 10. 最終住所 漢字  | 11. 最終住所 外字数   | 12. 異動年月日        |
| 13. 旧住民票コード  | 14. 附票管理市町村コード | 15. 附票本人確認情報状態区分 |
| 16. 外字フラグ    | 17. 外字パターン     | 18. 通知区分         |

#### イ その他 個人番号

(※国外転出者に係る事務処理に関し、番号法で認められた場合に限り、県の他の執行機関又は他部署からの求めに応じ、当該個人の住民票コードを用いて、都道府県知事保存本人確認情報ファイルから個人番号を抽出し、提供・移転する場合がある。)

### (3) 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	
(1)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（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が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	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。）
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	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。
個人番号の真正性確認の措置の内容	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。

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。 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。
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	
-	
<b>3. 特定個人情報の使用</b>	
リスク1: 目的を超えた紐付け、事務に必要な情報との紐付けが行われるリスク	
宛名システム等における措置の内容	・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の間を受渡し専用装置を設けて、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、事務に必要な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。
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。  都道府県サーバは、集約センター内において、附票都道府県サーバと接続する。  なお、都道府県サーバと附票都道府県サーバのシステム間のアクセスは、以下の場合の処理に限られるよう、システムにより制限する。  (1) 都道府県サーバ⇒附票都道府県サーバへのアクセス 番号法で認められた場合に限り、県の他の執行機関又は他部署等からの求めに応じ、国外転出者に係る個人番号を連携する場合。  (2) 附票都道府県サーバ⇒都道府県サーバへのアクセス 国外転出者に係る事務処理に関し、番号法で認められた場合に限り、県の他の執行機関又は他部署等からの求めに応じ、個人番号を入手する場合(目的を超えた紐付けが行われないよう、個人番号は附票本人確認情報DBとは別の一時保存領域で処理する。)
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: 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	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。
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	<ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> <li>・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。</li> <li>・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。</li> <li>・「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。</li> <li>・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。</li> </ul>
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	<ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> <li>・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。</li> </ul>
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	
<p>本人確認情報の利用にあたり、以下の措置を講じる。</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> <li>・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。</li> <li>・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。</li> <li>・本人確認情報の開示・訂正の請求に対し、適切に対応する。</li> <li>・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。</li> </ul>	

**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	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の前身である財団法人地方自治情報センターへ委託することを議決している。 ・委託先である機構は、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、住基法に基づき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。 ・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。
-------------	---

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。
----------	---

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	<p>①都道府県サーバの運用及び監視に関する業務</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> <li>・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。</li> <li>・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。</li> </ul> <p>②代表端末、業務端末等機器の保守管理に関する業務</p> <p>③代表端末、業務端末等機器の運用管理に関する業務</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> <li>・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。</li> <li>・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。</li> </ul>



<p>特定個人情報の消去ルール</p> <p>ルール内容及び ルール遵守の確認方法</p>	<p>[ 定めている ] &lt;選択肢&gt; 1) 定めている 2) 定めていない</p> <p>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」することとしているが、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。</p> <p>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。</p>
<p>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</p> <p>規定の内容</p>	<p>[ 定めている ] &lt;選択肢&gt; 1) 定めている 2) 定めていない</p> <p>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。</p> <p>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)</p> <p>【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)</p>

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	<input type="checkbox"/> 十分に行っている <input type="checkbox"/> <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	<p>①都道府県サーバの運用及び監視に関する業務</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> <li>・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。</li> </ul> <p>②代表端末、業務端末等機器の保守管理に関する業務</p> <p>③代表端末、業務端末等機器の運用管理に関する業務</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> </ul>
その他の措置の内容	-
リスクへの対策は十分か	<input type="checkbox"/> 十分である <input type="checkbox"/> <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
<b>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</b>	
再委託先については、毎年度の契約において、再委託先業者の業務内容や委託先との業務分担を審査した上で承認を行っているほか、随時業務状況を確認する。	

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		[ ] 提供・移転しない
リスク1： 不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録	[ 記録を残している ]	<選択肢> 1) 記録を残している 2) 記録を残していない
具体的な方法	・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	連携手段として通信の記録が逐一保存され、また、連携するデータが暗号化される仕組みが確立した住民基本台帳ネットワークシステムを用いることにより、不適切な方法による特定個人情報の提供を防止する。 全国サーバと都道府県サーバ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。 また、都道府県サーバの代表端末または業務端末と受渡し専用装置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。 ・都道府県サーバの代表端末または業務端末と受渡し専用フォルダ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 3) 課題が残されている	2) 十分である
リスク2: 安全が保たれない方法によって入手が行われるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク3: 入手した特定個人情報が不正確であるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク4: 入手の際に特定個人情報が漏えい・紛失するリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク5: 不正な提供が行われるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク6: 不適切な方法で提供されるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク7: 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置			



7. 特定個人情報の保管・消去		
リスク1: 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[ 政府機関ではない ]	<選択肢> 1) 特に力を入れて遵守している 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	<ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> <li>・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。</li> <li>・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に措置を講じる。</li> <li>・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。</li> </ul>
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	<ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> <li>・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。</li> </ul>
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	<ul style="list-style-type: none"> <li>修正前の本人確認情報(履歴情報)及び削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系統的に消去する。</li> <li>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。</li> <li>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。</li> </ul>
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	
(2)都道府県知事保存附票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	都道府県知事保存附票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41第1項に基づき通知）される附票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が行われることが前提となる。 また、対象者以外の個人番号は入手できないことを、システムにより担保する。
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	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。（都道府県知事保存附票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からの附票本人確認情報更新要求の際に通知（住基法第30条の41第1項に基づき通知）される本人確認情報に限定される。）また、対象者の個人番号以外の個人情報は入手できないことを、システムにより担保する。
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	都道府県知事保存附票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からの附票本人確認情報更新要求の際に通知（住基法第30条の41第1項に基づき通知）される附票本人確認情報に限定される。 また、国外転出者に係る事務処理に関し、番号法で認められた場合に限り、県の他の執行機関又は他部署等からの求めに応じ、個人番号を入手することを、システムにより担保する。
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： 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	都道府県知事保存附票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からの附票本人確認情報更新要求の際に通知（住基法第30条の41第1項に基づき通知）される附票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。 個人番号については、都道府県知事保存本人確認情報ファイルから入手するため、該当なし。
個人番号の真正性確認の措置の内容	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。 また、都道府県知事保存附票本人確認情報ファイルに保存される段階で真正性が担保されている。

特定個人情報の正確性確保の措置の内容	システム上、附票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。 個人番号については、都道府県知事保存附票本人確認情報ファイルに保存される段階で正確性が確保されている。
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、附票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附票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。 ・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。  ※附票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や附票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	
-	
<b>3. 特定個人情報の使用</b>	
リスク1: 目的を超えた紐付け、事務に必要な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	・附票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の間を受渡し専用装置を設けて、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、事務に必要な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。
事務で使用するその他のシステムにおける措置の内容	附票都道府県サーバと庁内システムとの接続は行わない。  附票都道府県サーバは、集約センター内において、都道府県サーバと接続する。  なお、附票都道府県サーバと都道府県サーバのシステム間のアクセスは、以下の場合の処理に限られるよう、システムにより制限する。  (1) 附票都道府県サーバ⇒都道府県サーバへのアクセス 国外転出者に係る事務処理に関し、番号法で認められた場合に限り、県の他の執行機関又は他部署等からの求めに応じ、個人番号を入手する場合(目的を超えた紐付けが行われないよう、個人番号は附票本人確認情報DBとは別の一時保存領域で処理する。)  (2) 都道府県サーバ⇒附票都道府県サーバへのアクセス 番号法で認められた場合に限り、県の他の執行機関又は他部署等からの求めに応じ、国外転出者に係る個人番号を連携する場合。
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	附票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。
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、附票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	<ul style="list-style-type: none"> <li>・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。</li> <li>・附票連携システムの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、業務上必要のない附票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。</li> <li>・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。</li> <li>・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。</li> <li>・システム管理規程、システムセキュリティ基本方針書等を策定する。</li> <li>・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。</li> </ul>
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	<ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> <li>・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。</li> </ul>
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	
<p>附票本人確認情報の利用にあたり、以下の措置を講じる。</p> <ul style="list-style-type: none"> <li>・スクリーンセーバ等を利用して、長時間にわたり附票本人確認情報を表示させない。</li> <li>・附票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。</li> <li>・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。</li> <li>・システム操作者は附票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。</li> <li>・附票本人確認情報の開示・訂正の請求に対し、適切に対応する。</li> <li>・附票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。</li> </ul>	

**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	①附票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の前身である財団法人地方自治情報センターへ委託することを議決している。 ・委託先である機構は、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、住基法に基づき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。 ・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。
-------------	---

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	・委託業務に従事する者に都道府県知事附票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附票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、附票本人確認情報の更新及び附票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。
----------	---

<p>特定個人情報ファイルの取扱いの記録</p>	<p>[ 記録を残している ] &lt;選択肢&gt;  1) 記録を残している      2) 記録を残していない</p>
<p>具体的な方法</p>	<p>①附票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、附票本人確認情報の更新及び附票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「附票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。</p> <p>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、直接附票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。</p>





<p>特定個人情報の消去ルール</p> <p>ルール内容及び ルール遵守の確認方法</p>	<p>[ 定めている ] &lt;選択肢&gt; 1) 定めている 2) 定めていない</p> <p>①附票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」することになっているが、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。</p> <p>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、附票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。</p>
<p>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</p> <p>規定の内容</p>	<p>[ 定めている ] &lt;選択肢&gt; 1) 定めている 2) 定めていない</p> <p>①附票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。</p> <p>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)</p> <p>【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)</p>

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	<input type="checkbox"/> 十分に行っている <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <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附票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、直接附票本人確認情報に係らない(直接附票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、附票本人確認情報に直接係わらない(附票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	<input type="checkbox"/> 十分である <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <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
<b>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</b>	
再委託先については、毎年度の契約において、再委託先業者の業務内容や委託先との業務分担を審査した上で承認を行っているほか、随時業務状況を確認する。	

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		[ ] 提供・移転しない
リスク1： 不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録	[ 記録を残している ]	<選択肢> 1) 記録を残している 2) 記録を残していない
具体的な方法	・都道府県知事保存附票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	・都道府県知事保存附票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	連携手段として通信の記録が逐一保存され、また、連携するデータが暗号化される仕組みが確立した附票連携システムを用いることにより、不適切な方法による特定個人情報の提供を防止する。附票全国サーバと附票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。また、附票都道府県サーバの代表端末または業務端末（都道府県サーバと共用する。）と受渡し専用装置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	<p>《誤った情報を提供・移転してしまうリスクへの措置》</p> <ul style="list-style-type: none"> <li>・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。</li> </ul> <p>《誤った相手に提供・移転してしまうリスクへの措置》</p> <ul style="list-style-type: none"> <li>・附票全国サーバと附票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。</li> <li>・附票都道府県サーバの代表端末または業務端末（都道府県サーバと共用する。）と受渡し専用フォルダ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。</li> </ul>	
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 3) 課題が残されている	2) 十分である
リスク2: 安全が保たれない方法によって入手が行われるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク3: 入手した特定個人情報が不正確であるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク4: 入手の際に特定個人情報が漏えい・紛失するリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク5: 不正な提供が行われるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク6: 不適切な方法で提供されるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク7: 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置			

7. 特定個人情報の保管・消去		
リスク1: 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[ 政府機関ではない ]	<選択肢> 1) 特に力を入れて遵守している 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	<ul style="list-style-type: none"> <li>・附票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。</li> <li>・附票都道府県サーバの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。</li> <li>・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。</li> <li>・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に措置を講じる。</li> <li>・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。</li> </ul>
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	<ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> <li>・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。</li> </ul>
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	附票本人確認情報の提供・移転に併せて提供される個人番号は、県の他の執行機関又は他部署等からの求めにより提供・移転された後は、障害発生等により提供・移転先で情報を受領できなかった場合に備えて一時的に保存がされるのみであり、情報が更新される必要はない。
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: 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	<ul style="list-style-type: none"> <li>・障害発生等により提供・移転先で情報を受領できなかった場合に備えた一時的な保存の終了後、特定個人情報を、システムにて自動判別し消去する(消去されたデータは、復元できない)。</li> <li>・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。</li> <li>・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。</li> </ul>
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	
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	<ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> </ul> <p>&lt;団体内統合宛名システムにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・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。</li> </ul>
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	<ul style="list-style-type: none"> <li>・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にシステム上担保されている。</li> </ul> <p>&lt;団体内統合宛名システムにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> </ul>
その他の措置の内容	—
リスクへの対策は十分か	<p>[ 十分である ]</p> <p>&lt;選択肢&gt;</p> <p>1) 特に力を入れている      2) 十分である</p> <p>3) 課題が残されている</p>
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	<p>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にシステム上担保されている。</p>
リスクへの対策は十分か	<p>[ 十分である ]</p> <p>&lt;選択肢&gt;</p> <p>1) 特に力を入れている      2) 十分である</p> <p>3) 課題が残されている</p>
リスク3： 入手した特定個人情報ที่ไม่正確であるリスク	
入手の際の本人確認の措置の内容	<ul style="list-style-type: none"> <li>・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。</li> <li>・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ます。</li> </ul> <p>&lt;団体内統合宛名システムにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・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。</li> </ul>
個人番号の真正性確認の措置の内容	<ul style="list-style-type: none"> <li>・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。</li> </ul> <p>&lt;団体内統合宛名システムにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・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。</li> </ul>



特定個人情報の正確性確保の措置の内容	<ul style="list-style-type: none"> <li>・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。</li> </ul> <p>&lt;団体内統合宛名システムにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・ウイ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。</li> <li>・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。</li> <li>・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。</li> </ul>
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	住民基本台帳ネットワークシステム及び附票連携システムの業務端末又は代表端末側から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	
—	
<b>3. 特定個人情報の使用</b>	
リスク1： 目的を超えた紐付け、事務に必要な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、当該事務に必要な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	符号生成に必要な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	<p>&lt;住民基本台帳ネットワークシステム及び附票連携システムにおける措置&gt;            符号取得要求ファイルの受け渡しを行う受渡し専用装置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。</p> <p>&lt;団体内統合宛名システムにおける措置&gt;            ・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。</p>
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	<p>&lt;住民基本台帳ネットワークシステム及び附票連携システムにおける措置&gt;            ・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。</p> <p>&lt;団体内統合宛名システムにおける措置&gt;            ・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。</p>
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	<p>&lt;住民基本台帳ネットワークシステム及び附票連携システムにおける措置&gt;            ・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。</p> <p>&lt;団体内統合宛名システムにおける措置&gt;            ・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。</p>
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	<p>・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。</p>
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	<p>&lt;住民基本台帳ネットワークシステム及び附票連携システムにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・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</li> <li>・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及び附票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。</li> <li>・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。</li> <li>・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。</li> <li>・システム管理規程、システムセキュリティ基本方針書等を策定する。</li> <li>・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。</li> </ul> <p>&lt;団体内統合宛名システムにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・システムの操作履歴(操作ログ)を記録する。</li> <li>・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。</li> <li>・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。</li> <li>・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。</li> </ul>
リスクへの対策は十分か	<p>[ 十分である ]</p> <p>&lt;選択肢&gt;</p> <p>1) 特に力を入れている      2) 十分である</p> <p>3) 課題が残されている</p>
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	<p>&lt;住民基本台帳ネットワークシステム及び附票連携システムにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> <li>・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。</li> </ul> <p>&lt;団体内統合宛名システムにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・職員に対しては、データ保護に関する研修を行う。</li> <li>・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。</li> </ul>
リスクへの対策は十分か	<p>[ 十分である ]</p> <p>&lt;選択肢&gt;</p> <p>1) 特に力を入れている      2) 十分である</p> <p>3) 課題が残されている</p>
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	
<p>本人確認情報及び附票本人確認情報の利用にあたり、以下の措置を講じる。</p> <p>&lt;住民基本台帳ネットワークシステム及び附票連携システムにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・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</li> <li>・都道府県サーバ及び附票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</li> <li>・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</li> <li>・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</li> <li>・本人確認情報及び附票本人確認情報の開示・訂正の請求に対し、適切に対応する</li> <li>・本人確認情報及び附票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</li> </ul> <p>&lt;団体内統合宛名システムにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> </ul>	

**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
ルール内容及びルール遵守の確認方法	<ul style="list-style-type: none"> <li>・都道府県知事保存本人確認情報及び都道府県知事保存附票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。</li> <li>・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。</li> <li>・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。</li> </ul>	
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	<p>全国サーバと都道府県サーバの間の通信及び附票全国サーバと附票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。</p> <p>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。</p> <p>また、都道府県サーバ及び附票都道府県サーバの代表端末または業務端末と受渡し専用装置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。</p>	
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及び附票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 3) 課題が残されている	2) 十分である
リスク2: 安全が保たれない方法によって入手が行われるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク3: 入手した特定個人情報ที่ไม่正確であるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク4: 入手の際に特定個人情報が漏えい・紛失するリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク5: 不正な提供が行われるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク6: 不適切な方法で提供されるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク7: 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置			

7. 特定個人情報の保管・消去		
リスク1: 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[ 政府機関ではない ]	<選択肢> 1) 特に力を入れて遵守している 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	<p>&lt;住民基本台帳ネットワークシステム及び附票連携システムにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> <li>・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。</li> <li>・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に措置を講じる。</li> <li>・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。</li> </ul> <p>&lt;団体内統合宛名システムにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> </ul>
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	<p>&lt;住民基本台帳ネットワークシステム及び附票連携システムにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> <li>・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。</li> </ul> <p>&lt;団体内統合宛名システムにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・コンピュータウイルス対策ソフトウェアを導入する。</li> <li>・OSには随時パッチ適用を実施する。</li> </ul>
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	<p>・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。</p> <p>&lt;団体内統合宛名システムにおける措置&gt;</p> <p>・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及び附票連携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。</p>
リスクへの対策は十分か	<p>[ 十分である ]</p> <p>&lt;選択肢&gt;</p> <p>1) 特に力を入れている      2) 十分である</p> <p>3) 課題が残されている</p>
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	<p>[ 定めている ]</p> <p>&lt;選択肢&gt;</p> <p>1) 定めている      2) 定めていない</p>
手順の内容	<p>・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。</p> <p>&lt;団体内統合宛名システムにおける措置&gt;</p> <p>・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。</p> <p>・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。</p>
その他の措置の内容	—
リスクへの対策は十分か	<p>[ 十分である ]</p> <p>&lt;選択肢&gt;</p> <p>1) 特に力を入れている      2) 十分である</p> <p>3) 課題が残されている</p>
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	
<p>&lt;団体内統合宛名システムにおける措置&gt;</p> <p>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。</p>	



## IV その他のリスク対策 ※

1. 監査	
①自己点検	<p>[ 十分に行っている ]      &lt;選択肢&gt; 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</p>
具体的なチェック方法	<p>&lt;住民基本台帳ネットワークシステム及び附票連携システムにおける措置&gt; 機構(住民基本台帳ネットワークシステム全国センター及び附票全国センター)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。</p> <p>&lt;団体内統合宛名システムにおける措置&gt; 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。</p>
②監査	<p>[ 十分に行っている ]      &lt;選択肢&gt; 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</p>
具体的な内容	<p>&lt;住民基本台帳ネットワークシステム及び附票連携システムにおける措置&gt; ・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・建築安全推進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。</p> <p>&lt;団体内統合宛名システムにおける措置&gt; 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。</p>
2. 従業者に対する教育・啓発	
従業者に対する教育・啓発	<p>[ 十分に行っている ]      &lt;選択肢&gt; 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</p>
具体的な方法	<p>&lt;住民基本台帳ネットワークシステム及び附票連携システムにおける措置&gt; ・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。 ・「住基ネット業務引継書」を作成のうえ組織として記録を管理することにより、引継事項の周知徹底に努める。 ・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。</p> <p>&lt;団体内統合宛名システムにおける措置&gt; ・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。</p>
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	総務部法務文書課県政情報公関係 〒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	<div style="display: flex; justify-content: space-between;"> <span>[ 有料 ]</span> <span>&lt;選択肢&gt; 1) 有料 2) 無料</span> </div> 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 ) (手数料額、納付方法: 納付方法: 現金)
④個人情報ファイル簿の公表	<div style="display: flex; justify-content: space-between;"> <span>[ 行っている ]</span> <span>&lt;選択肢&gt; 1) 行っている 2) 行っていない</span> </div>
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	・知事公室市町村振興課 〒630-8501 奈良市登大路町30番地 TEL:0742-27-8422 FAX:0742-23-8439 ・総務部デジタル戦略課 〒630-8501 奈良市登大路町30番地 TEL:0742-27-7003 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	令和5年2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	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	令和5年7月24日(月)～令和5年8月25日(金)
③期間を短縮する特段の理由	
④主な意見の内容	
⑤評価書への反映	
3. 第三者点検	
①実施日	
②方法	奈良県個人情報保護審議会において第三者点検を実施予定
③結果	
4. 個人情報保護委員会の承認【行政機関等のみ】	
①提出日	
②個人情報保護委員会による審査	

(別添3)変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
平成29年7月27日	I 基本情報 7. 評価実施機関における担当部署 ②所長	市町村振興課長 山下 保典	市町村振興課長 浅田 舜男	事後	人事異動による修正 (その他の項目の変更であり事前の提出・公表が義務付けられないため事後に報告)
平成29年7月27日	II 特定個人情報ファイルの概要(本人確認情報ファイル) 2. 基本情報 ⑤保有開始日	平成27年6月予定	平成27年6月	事後	実際の保有開始日を記載 (その他の項目の変更であり事前の提出・公表が義務付けられないため事後に報告)
平成29年7月27日	II 特定個人情報ファイルの概要(符号取得要求ファイル) 2. 基本情報 ⑤保有開始日	平成27年10月予定	平成27年10月	事後	実際の保有開始日を記載 (その他の項目の変更であり事前の提出・公表が義務付けられないため事後に報告)
平成29年7月27日	I 基本情報 (別添1) 事務の内容	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変換し専用フォルダを介して変換し、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。情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。	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変換し専用フォルダを介して変換し、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。情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。	事後	誤字脱字の修正 (その他の項目の変更であり事前の提出・公表が義務付けられないため事後に報告)
平成29年7月27日	II 特定個人情報ファイルの概要(符号取得要求ファイル) 3. 特定個人情報の入手・使用 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報情報を法第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番号(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項の方法により機関(全国サーバ)へ送付することとされている。	番号法第19条第7項に規定する別表第二の特定個人情報情報を法第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番号(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項の方法により機関(全国サーバ)へ送付することとされている。	事後	誤字脱字の修正 (その他の項目の変更であり事前の提出・公表が義務付けられないため事後に報告)
平成31年3月8日	I 基本情報 7. 評価実施機関における担当部署 ②所長 長 役職名	市町村振興課長 浅田 舜男	市町村振興課長	事後	特定個人情報保護評価に関する規則の一部改正に伴う変更
平成31年3月8日	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 ③請求先	総務部 総務課 異政情報係	総務部 法務文書課 異政情報係	事後	組織再編による修正
平成31年3月8日	IV その他のリスク対策 1. 監査 ②監査 具体的な内容	旅券事務所・建築課など業務端末設置部署等	旅券事務所・建築安全推進課など業務端末設置部署等	事後	課名変更による修正
令和2年3月17日	I 基本情報 5. 個人番号の利用 法上の根拠	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(住民基本台帳の脱退等に関する都道府県知事の通知等) 第30条の5(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関への本人確認情報の通知等) 第30条の8(本人確認情報の預りに関する機関の通知) 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22(市町村間の連絡調整等) 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)	住民基本台帳法(昭和42年7月25日法律第81号) 第7条(住民票の記載事項) 第12条の5(住民基本台帳の脱退等に関する都道府県知事の通知等) 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関への本人確認情報の通知等) 第30条の8(本人確認情報の預りに関する機関の通知) 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22(市町村間の連絡調整等) 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)	事前	重要な変更となるため事前に報告
令和2年3月17日	(別添1) 事務の内容(備考)	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. 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(特定個人情報を含まない)。	事後	その他の項目の変更であり事前の提出・公表が義務付けられないため事後に報告
令和2年3月17日	II 特定個人情報ファイルの概要 5. 特定個人情報の提供・移転(委託に伴うものを除く) 提供先2 ③提供する業務	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。	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、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「整備法」という。))第22条第7項に基づく経過措置である。	事後	その他の項目の変更であり事前の提出・公表が義務付けられないため事後に報告
令和2年3月17日	II 特定個人情報ファイルの概要 5. 特定個人情報の提供・移転(委託に伴うものを除く) 移転先1 ③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。	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22条第7項に基づく経過措置である。	事後	その他の項目の変更であり事前の提出・公表が義務付けられないため事後に報告

令和2年3月17日	Ⅱ 特定個人情報ファイルの概要 5. 特定個人情報の提供・移転 (委託に伴うものを除く.) 移転先 ⑥ 移転方法	{ } 序内連携システム { } 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 { } その他(住民基本台帳ネットワークシステム)	{ } 序内連携システム { } 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 { } その他(住民基本台帳ネットワークシステム)	事後	その他の項目の変更であり事前の提出・公表が義務付けられないため事後に報告
令和2年3月17日	Ⅱ 特定個人情報ファイルの概要 (別添2) 特定個人情報ファイル記録項目	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 符号取得要求ファイル 1. 加理通番、2. 個人番号、3. 符号再発行フラグ	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、25. 旧氏 漢字、26. 旧氏 外字数、27. 旧氏 ふりがな、28. 旧氏 外字変更連番 符号取得要求ファイル 1. 加理通番、2. 個人番号、3. 符号再発行フラグ	事後	その他の項目の変更であり事前の提出・公表が義務付けられないため事後に報告
令和2年3月17日	Ⅳ その他のリスク対策 2. 従業者に対する教育・啓発 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、特定個人情報取扱い業務に携わる前に個人情報保護に関する研修を行う。 ・委託業者に対しては、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る。	<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。 ・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。 ・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。 ・職員に対しては、特定個人情報取扱い業務に携わる前に個人情報保護に関する研修を行う。 ・委託業者に対しては、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る。	事前	重要な変更となるため事前に報告
令和2年3月17日	1. 基本情報 2. 特定個人情報ファイルを取り扱う事柄において使用システム ② システムの機能	7. 個人番号制度の運用に伴う情報連携 ① 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と、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変換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。	7. 個人番号制度の運用に伴う情報連携 ① 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間に突合専用装置を設けて、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。 ② 中間サーバ上で作成される符号取得依頼ファイル(加理通番、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間に突合専用装置を介して受渡し、全国サーバに送信する。	事後	その他の項目の変更であり事前の提出・公表が義務付けられないため事後に報告
令和2年3月17日	1. 基本情報 (別添1) 事務の内容(備考)	7. 個人番号制度の運用に伴う情報連携 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に変換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。 ② 中間サーバ上で作成される符号取得依頼ファイル(加理通番、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間に突合専用フォルダを介して受渡し、全国サーバに送信する。	7. 個人番号制度の運用に伴う情報連携 ① 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間に突合専用装置を設けて、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。 ② 中間サーバ上で作成される符号取得依頼ファイル(加理通番、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間に突合専用装置を介して受渡し、全国サーバに送信する。	事後	その他の項目の変更であり事前の提出・公表が義務付けられないため事後に報告
令和2年3月17日	Ⅱ 特定個人情報ファイルの概要 (都道府県知事保存本人確認情報ファイル) 3. 特定個人情報の入手・使用方法	{ } 序内連携システム { } その他(市町村CSを通じて入手する)	{ } 序内連携システム { } その他(市町村CSを通じて入手する)	事後	その他の項目の変更であり事前の提出・公表が義務付けられないため事後に報告
令和2年3月17日	Ⅱ 特定個人情報ファイルの概要 (符号取得要求ファイル) 3. 特定個人情報の入手・使用方法	{ } 序内連携システム { } その他	{ } 序内連携システム { } その他(受け渡し専用装置)	事後	その他の項目の変更であり事前の提出・公表が義務付けられないため事後に報告
令和2年3月17日	Ⅱ 特定個人情報ファイルの概要 (都道府県知事保存本人確認情報ファイル) 3. 特定個人情報の入手・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(加理通番、個人番号)を団体内統合宛名システム側の変換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。	・中間サーバで生成された符号取得要求ファイルを受渡し専用装置に保存する。 ・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、受渡し専用装置内の符号取得要求ファイルを取り込む。	事前	重要な変更となるため事前に報告
令和2年3月17日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 (都道府県知事保存本人確認情報ファイル) 3. 特定個人情報の使用リスク 1. 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、これまで用いてい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変換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。	・本人確認情報の一括提供機能の利用について、これまで用いてい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変換し専用装置を設けて、要求ファイル等の受け渡し連携を行う。	事前	重要な変更となるため事前に報告

令和2年3月17日	<p>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(都道府県知事保存本人確認情報ファイル) 5. 特定個人情報の提供・移転(リスク2)リスクに対する措置の内容</p>	<p>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。</p> <p>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ち会う。</p> <p>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。</p>	<p>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。</p> <p>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ち会う。</p> <p>また、都道府県サーバの代表端末または業務端末と受渡し専用装置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。</p>	事前	重要な変更となるため事前に報告
令和2年3月17日	<p>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(都道府県知事保存本人確認情報ファイル) 5. 特定個人情報の提供・移転(リスク3)リスクに対する措置の内容</p>	<p>《新った情報を提供・移転してしまうリスクへの措置》</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> </ul> <p>《新った相手に提供・移転してしまうリスクへの措置》</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> <li>・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。</li> </ul>	<p>《新った情報を提供・移転してしまうリスクへの措置》</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> </ul> <p>《新った相手に提供・移転してしまうリスクへの措置》</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・都道府県サーバの代表端末または業務端末と受渡し専用装置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。</li> <li>・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。</li> </ul>	事前	重要な変更となるため事前に報告
令和2年3月17日	<p>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(符号取得要求ファイル) 2. 特定個人情報の入手(リスク4)リスクに対する措置の内容</p>	<p>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変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または代表端末側から、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。</p>	<p>住民基本台帳ネットワークシステムの業務端末または代表端末側から受渡し専用装置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。</p>	事前	重要な変更となるため事前に報告
令和2年3月17日	<p>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(符号取得要求ファイル) 3. 特定個人情報の使用(リスク2)リスクに対する措置の内容</p>	<p>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もとに付与された照会ID及び照会情報(特例による生体認証)による操作者認証を行う。</p>	<p>符号取得要求ファイルの受け渡しを行う受渡し専用装置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会ID及び照会情報(特例による生体認証)による操作者認証を行う。</p>	事前	重要な変更となるため事前に報告
令和2年3月17日	<p>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(符号取得要求ファイル) 5. 特定個人情報の提供・移転(リスク2)リスクに対する措置の内容</p>	<p>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。</p> <p>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ち会う。</p> <p>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。</p>	<p>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。</p> <p>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ち会う。</p> <p>また、都道府県サーバの代表端末または業務端末と受渡し専用装置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。</p>	事前	重要な変更となるため事前に報告
令和2年3月17日	<p>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(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を通じて入手を除く。)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</p>	<p>&lt;団体内統合宛名システムにおける措置&gt;</p> <p>業務所管課において届出内容や本人確認書類(身分証明書等)の確認を厳格に行い、対象者以外の情報の入手の防止に努める。</p>	-	事前	重要な変更となるため事前に報告
令和2年3月17日	<p>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(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を通じて入手を除く。)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</p>	<p>&lt;団体内統合宛名システムにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> </ul>	-	事前	重要な変更となるため事前に報告
令和2年3月17日	<p>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(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を通じて入手を除く。)リスク3 入手の際の本人確認の措置の内容</p>	<p>&lt;団体内統合宛名システムにおける措置&gt;</p> <p>特定個人情報の入手の際には、業務所管課の事務で確認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。</p>	-	事前	重要な変更となるため事前に報告
令和2年3月17日	<p>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(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を通じて入手を除く。)リスク3 個人番号の真正性確認の措置の内容</p>	<p>&lt;団体内統合宛名システムにおける措置&gt;</p> <p>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。</p>	-	事前	重要な変更となるため事前に報告
令和2年3月17日	<p>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(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を通じて入手を除く。)リスク3 特定個人情報の正確性確保の措置の内容</p>	<p>&lt;団体内統合宛名システムにおける措置&gt;</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・ウイルス対策ソフトウェアを導入し、常に最新のウイルス定義ファイルを更新する。セキュリティ上の有効性を確認している。</li> <li>・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及び必要性等を検証した上で適用し、その動作の安定性を確認している。</li> <li>・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。</li> </ul>	-	事前	重要な変更となるため事前に報告

<p>令和2年3月17日</p>	<p>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（都道府県知事保存本人確認情報ファイル）3. 特定個人情報の使用リスク1 宛名システム等における措置</p>	<p>・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、当該事務に必要な情報との紐付けは物理的に不可能である。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>令和2年3月17日</p>	<p>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（都道府県知事保存本人確認情報ファイル）3. 特定個人情報の使用リスク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</p>	<p>&lt;団体内統合宛名システムにおける措置&gt;        ・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。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>令和2年3月17日</p>	<p>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（都道府県知事保存本人確認情報ファイル）3. 特定個人情報の使用リスク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 アクセス権限の発行・失効の管理</p>	<p>&lt;団体内統合宛名システムにおける措置&gt;        ・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。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>令和2年3月17日</p>	<p>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（都道府県知事保存本人確認情報ファイル）3. 特定個人情報の使用リスク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 アクセス権限の管理</p>	<p>&lt;団体内統合宛名システムにおける措置&gt;        ・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。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>

令和2年3月17日	<p>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 (都道府県知事保存本人確認情報ファイル) 3. 特定個人情報の使用リスク3従業者が事務外で使用するリスク</p>	<p>&lt;団体内統合宛名システムにおける措置&gt; ・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、法令の前掲規定により措置を講じる。</p>	-	事前	重要な変更となるため事前に報告
令和2年3月17日	<p>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 (都道府県知事保存本人確認情報ファイル) 3. 特定個人情報の使用リスク4 特定個人情報ファイルが不正に複製されるリスク</p>	<p>&lt;団体内統合宛名システムにおける措置&gt; ・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、法令の前掲規定により措置を講じる。</p>	-	事前	重要な変更となるため事前に報告
令和2年3月17日	<p>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 (都道府県知事保存本人確認情報ファイル) 3. 特定個人情報の使用 特定個人情報ファイルにおける他のリスク及びそのリスクに対する措置</p>	<p>&lt;団体内統合宛名システムにおける措置&gt; ・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。</p>	-	事前	重要な変更となるため事前に報告
令和2年3月17日	<p>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 (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の取扱いの委託 情報管理体制の確認</p>	<p>&lt;団体内統合宛名システムにおける措置&gt; ・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。</p>	-	事前	重要な変更となるため事前に報告



令和2年3月17日	<p>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 (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の取扱いの委託 特定個人情報ファイルの閲覧者・更新者の制限 具体的な制限方法</p>	<p>&lt;団体内統合宛名システムにおける措置&gt;          ・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契約書を提出させる。          ・契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らる。</p>	-	事前	重要な変更となるため事前に報告
令和2年3月17日	<p>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 (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の取扱いの委託 特定個人情報ファイルの閲覧者・更新者の制限 特定個人情報ファイルの取扱いの記録 具体的な方法</p>	<p>&lt;団体内統合宛名システムにおける措置&gt;          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。</p>	-	事前	重要な変更となるため事前に報告
令和2年3月17日	<p>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 (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の取扱いの委託 特定個人情報の提供ルール 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順守の確認方法</p>	<p>&lt;団体内統合宛名システムにおける措置&gt;          ・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。</p>	-	事前	重要な変更となるため事前に報告
令和2年3月17日	<p>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 (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の取扱いの委託 特定個人情報の提供ルール 委託先と委託先間の提供に関するルールの内容及びルール順守の確認方法</p>	<p>&lt;団体内統合宛名システムにおける措置&gt;          ・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。</p>	-	事前	重要な変更となるため事前に報告

令和2年3月17日	<p>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 (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の取扱いの委託 特定個人情報の提供ルール 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記号 規定の内容</p>	<p>&lt;団体内統合宛名システムにおける措置&gt; 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。 ・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 ・複製等の返還等 ・取扱いについての指示等 ・事故発生時における報告</p>	-	事前	重要な変更となるため事前に報告
令和2年3月17日	<p>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 (都道府県知事保存本人確認情報ファイル) 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・既存リスク ⑤物理的対策 具体的な対策の内容</p>	<p>&lt;団体内統合宛名システムにおける措置&gt; ・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、監視及び施設管理する。</p>	-	事前	重要な変更となるため事前に報告
令和2年3月17日	<p>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 (都道府県知事保存本人確認情報ファイル) 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・既存リスク ⑥技術的対策 具体的な対策の内容</p>	<p>&lt;団体内統合宛名システムにおける措置&gt; ・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。 ・コンピュータウイ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。</p>	-	事前	重要な変更となるため事前に報告
令和2年3月17日	<p>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 (都道府県知事保存本人確認情報ファイル) 7. 特定個人情報の保管・消去 リスク2 特定個人情報がな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</p>	<p>&lt;団体内統合宛名システムにおける措置&gt; 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。</p>	-	事前	重要な変更となるため事前に報告

<p>令和2年3月17日</p>	<p>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 (都道府県知事保存本人確認情報ファイル) 7. 特定個人情報の保管・消去 リスク3特定個人情報情報が消去されずいつまでも存在するリスク</p>	<p>&lt;団体内統合宛名システムにおける措置&gt; 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、焼却等を作成し、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。</p>	<p>—</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>令和2年3月17日</p>	<p>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 (都道府県知事保存本人確認情報ファイル) 7. 特定個人情報の保管・消去 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</p>	<p>&lt;団体内統合宛名システムにおける措置&gt; 団体内宛名統合システムにおいて、単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。</p>	<p>—</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>令和2年3月17日</p>	<p>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 (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</p>	<p>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内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。</p>	<p>・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内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。 &lt;団体内統合宛名システムにおける措置&gt; ・業務所管課において届出内容や本人確認書類(身分証明書等)の確認を厳格に行い、対象者以外の情報の入手の防止に努める。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>令和2年3月17日</p>	<p>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 (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 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</p>	<p>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。</p>	<p>・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。 &lt;団体内統合宛名システムにおける措置&gt; 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。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>

<p>令和2年3月17日</p>	<p>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（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3入手した特定個人情報不正確であるリスク 入手の際の本人確認の措置の内容</p>	<p>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ます。</p>	<p>・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ます。</p> <p>&lt;団体統合宛名システムにおける措置&gt; ・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。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>令和2年3月17日</p>	<p>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（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3入手した特定個人情報不正確であるリスク 個人番号の真正性確認の措置の内容</p>	<p>団体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ないことをシステム上で論理チェックを行う仕組みとする。</p>	<p>・団体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ないことをシステム上で論理チェックを行う仕組みとする。</p> <p>&lt;団体統合宛名システムにおける措置&gt; ・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のみを連携する。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>令和2年3月17日</p>	<p>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（符号取得要求ファイル）3. 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3入手した特定個人情報不正確であるリスク 特定個人情報の正確性確保の措置の内容</p>	<p>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。</p>	<p>・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。</p> <p>&lt;団体統合宛名システムにおける措置&gt; ・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。 ・ウイルス対策ソフトウェアを導入し、常に最新のバージョ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及び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。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>令和2年3月17日</p>	<p>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（符号取得要求ファイル）3. 特定個人情報の使用 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 具体的な管理方法</p>	<p>符号取得要求ファイルの受け渡しを行う団体統合宛名システム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会D及び照会情報（特許による生体認証）による操作者認証を行う。</p>	<p>&lt;住民基本台帳ネットワークシステムにおける措置&gt; 符号取得要求ファイルの受け渡しを行う受渡し専用装置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会D及び照会情報（特許による生体認証）による操作者認証を行う。</p> <p>&lt;団体統合宛名システムにおける措置&gt; ・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。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>

<p>令和2年3月17日</p>	<p>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(符号取得要求ファイル) 3. 特定個人情報の使用リスク2 権限のない者(元職員、アクセス権のない職員等)によって不正に使用されるリスク アクセス権限の発効・失効の管理 具体的な管理方法</p>	<p>・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。</p>	<p>&lt;住民基本台帳ネットワークシステムにおける措置&gt;          ・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。          &lt;団体内統合宛名システムにおける措置&gt;          ・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。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>令和2年3月17日</p>	<p>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(符号取得要求ファイル) 3. 特定個人情報の使用リスク2 権限のない者(元職員、アクセス権のない職員等)によって不正に使用されるリスク アクセス権限の管理 具体的な管理方法</p>	<p>・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。</p>	<p>&lt;住民基本台帳ネットワークシステムにおける措置&gt;          ・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。          &lt;団体内統合宛名システムにおける措置&gt;          ・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。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>令和2年3月17日</p>	<p>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(符号取得要求ファイル) 3. 特定個人情報の使用リスク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</p>	<p>・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、法令の前記規定により措置を講じる。</p>	<p>&lt;住民基本台帳ネットワークシステムの措置&gt;          ・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前記規定により措置を講じる。          &lt;団体内統合宛名システムにおける措置&gt;          ・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わ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、法令の前記規定により措置を講じる。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>令和2年3月17日</p>	<p>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(符号取得要求ファイル) 3. 特定個人情報の使用リスク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</p>	<p>・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、法令の前記規定により措置を講じる。</p>	<p>&lt;住民基本台帳ネットワークシステムにおける措置&gt;          ・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、法令の前記規定により措置を講じる。          &lt;団体内統合宛名システムにおける措置&gt;          ・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、法令の前記規定により措置を講じる。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>

<p>令和2年3月17日</p>	<p>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 (符号取得要求ファイル) 3. 特定個人情報使用のリスク4. 特定個人情報ファイルが不正に複製されるリスク 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</p>	<p>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設管理された安全な場所に設置するとともに、来庁者から見えにくい位置に設置する ・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</p>	<p>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設管理された安全な場所に設置するとともに、来庁者から見えにくい位置に設置する ・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にくい位置に設置する。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>令和2年3月17日</p>	<p>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 (符号取得要求ファイル) 7. 特定個人情報の保管・消去 リスク2 特定個人情報の古いまま保管され続けるリスク リスクに対する措置の内容</p>	<p>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時に、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。</p>	<p>・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時に、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。 ＜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。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>令和2年3月17日</p>	<p>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 (符号取得要求ファイル) 7. 特定個人情報の保管・消去 リスク3 特定個人情報の古いまま保管され続けるリスク 消去手順 手順の内容</p>	<p>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時に、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。</p>	<p>・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時に、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。 ＜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、廃棄等を作成し、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。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>令和2年3月17日</p>	<p>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 (符号取得要求ファイル) 7. 特定個人情報の保管・消去 リスク3 特定個人情報の古いまま保管され続けるリスク 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</p>	<p>—</p>	<p>＜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。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>

令和2年3月17日	表紙 特記事項	<p>・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、社会保険給付情報や所得額などの社会保険・税・災害対策業務情報は保有しない。</p> <p>・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。</p> <p>・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。</p> <p>・都道府県サーバ(又は全都道府県分を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。</p> <p>・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受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。</p>	<p>・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、社会保険給付情報や所得額などの社会保険・税・災害対策業務情報は保有しない。</p> <p>・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。</p> <p>・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。</p> <p>・都道府県サーバ(又は全都道府県分を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。</p> <p>・番号制度の運用において発生する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。</p>	事後	その他の項目の変更であり事前の提出・公表が義務付けられないため事後に報告
令和2年3月17日	II 特定個人情報ファイルの概要(都道府県知事本人情報ファイル) 5. 特定個人情報の提供・移転委託に伴う者を除く。提供先 ⑥ 提供方法	[ ] 電子記録媒体(フラッシュメモリを除く。)	[O] 電子記録媒体(フラッシュメモリを除く。)	事後	その他の項目の変更であり事前の提出・公表が義務付けられないため事後に報告
令和2年3月17日	VI 評価実施手続 2. 国民・住民からの意見の聴取 ② 実施日・期間	平成27年1月14日～平成27年2月13日	令和1年8月23日(金)～令和1年9月24日(火)	事後	その他の項目の変更であり事前の提出・公表が義務付けられないため事後に報告
令和2年3月17日	VI 評価実施手続 3. 第三者点検	<p>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)</p> <p>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。</p> <p>③結果:第三者点検により以下の答申を受けた。</p> <p>「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。」</p> <p>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。」</p>	<p>①実施日:令和1年12月2日</p> <p>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。</p> <p>③結果:第三者点検により以下の答申を受けた。</p> <p>「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。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してください。」</p>	事後	その他の項目の変更であり事前の提出・公表が義務付けられないため事後に報告
令和3年3月19日	I 基本情報 7. 評価実施期間における担当部署 ① 部署	地域振興都市町村振興課	知事公室市町村振興課	事後	その他の項目の変更であり事前の提出・公表が義務付けられないため事後に報告
令和3年3月19日	II 特定個人情報ファイルの概要(都道府県知事本人情報ファイル) 2. 基本情報 ⑥ 事務担当部署	地域振興都市町村振興課	知事公室市町村振興課	事後	その他の項目の変更であり事前の提出・公表が義務付けられないため事後に報告
令和3年3月19日	II 特定個人情報ファイルの概要(都道府県知事本人情報ファイル) 3. 特定個人情報の入手・使用 ⑦ 使用の主体	地域振興都市町村振興課	知事公室市町村振興課	事後	その他の項目の変更であり事前の提出・公表が義務付けられないため事後に報告
令和3年3月19日	II 特定個人情報ファイルの概要(符号取得要求ファイル) 2. 基本情報 ⑥ 事務担当部署	地域振興都市町村振興課	知事公室市町村振興課	事後	その他の項目の変更であり事前の提出・公表が義務付けられないため事後に報告

令和3年3月19日	Ⅱ 特定個人情報ファイルの概要(符号取得請求ファイル) 3. 特定個人情報の入手・使用⑦使用の主体	地域振興都市町村振興課	知事公室市町村振興課	事後	その他の項目の変更であり事前の提出・公表が義務付けられないため事後に報告
令和3年3月19日	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 ③請求先	総務部法務文書課県政情報係 〒630-8501 奈良市登大路町30番地 TEL.0742-27-8348 FAX.0742-27-1323	総務部法務文書課県政情報公開係 〒630-8501 奈良市登大路町30番地 TEL.0742-27-8348 FAX.0742-27-1323	事後	その他の項目の変更であり事前の提出・公表が義務付けられないため事後に報告
令和3年3月19日	Ⅴ 開示請求、問合せ 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	・地域振興都市町村振興課 〒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	・知事公室市町村振興課 〒630-8501 奈良市登大路町30番地 TEL.0742-27-8422 FAX.0742-23-8439 ・総務部ICT推進課 〒630-8501 奈良市登大路町30番地 TEL.0742-27-2052 FAX.0742-23-4196	事後	その他の項目の変更であり事前の提出・公表が義務付けられないため事後に報告
令和4年3月24日	Ⅵ 評価実施手続 1. 基礎項目評価 ①実施日	令和1年7月31日	令和4年2月1日	事後	その他の項目の変更であり事前の提出・公表が義務付けられないため事後に報告
令和4年3月24日	Ⅴ 開示請求、問合せ 2. 特定個人情報ファイルの取扱いに関する問合せ ③連絡先	・知事公室市町村振興課 〒630-8501 奈良市登大路町30番地 TEL.0742-27-8422 FAX.0742-23-8439 ・総務部ICT推進課 〒630-8501 奈良市登大路町30番地 TEL.0742-27-7004 FAX.0742-23-4196	・知事公室市町村振興課 〒630-8501 奈良市登大路町30番地 TEL.0742-27-8422 FAX.0742-23-8439 ・総務部デジタル戦略課 〒630-8501 奈良市登大路町30番地 TEL.0742-27-7003 FAX.0742-23-4196	事後	その他の項目の変更であり事前の提出・公表が義務付けられないため事後に報告
令和5年3月31日	Ⅵ 評価実施手続 1. 基礎項目評価 ①実施日	令和4年2月1日	令和5年2月1日	事後	その他の項目の変更であり事前の提出・公表が義務付けられないため事後に報告
	表紙 評価書名	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	住民基本台帳ネットワークに関する事務 全項目評価書	事前	重要な変更となるため事前に報告



<p>表紙 個人のプライバシー等の権利利益の保護の宣言</p>	<p>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象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。</p>	<p>奈良県は、住民基本台帳ネットワーク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象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。</p>	<p>事前 重要な変更となるため事前に報告</p>
<p>表紙 特記事項</p>	<p>・奈良県知事は、住民基本台帳法(以下「住民法」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民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。 ・外部との接続にあつては、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(DS)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・監視を機体に変更している。 ・番号制度の運用において発生する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と団体内統合宛名システムに変更し専用装置を設けて、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。</p>	<p>・奈良県知事は、住民基本台帳法(以下「住民法」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民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。 ・外部との接続にあつては、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(DS)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。 ・都道府県サーバ及び附帯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・監視を機体に変更している。 ・番号制度の運用において発生する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、都道府県サーバ及び附帯都道府県サーバの代表端末または業務端末と団体内統合宛名システムに変更し専用装置を設けて、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。</p>	<p>事前 重要な変更となるため事前に報告</p>
<p>1 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</p>	<p>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</p>	<p>住民基本台帳ネットワークに関する事務</p>	<p>事前 重要な変更となるため事前に報告</p>
<p>1 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</p>	<p>奈良県(以下「県」という。))は、住民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、住民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届出等を図り、その住民の地位を記録する各県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に行うものであり、市町村において、住民の居住関係の公益、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。</p> <p>県では、住民法の規定に基づき、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)</p> <ol style="list-style-type: none"> <li>①磁気ディスクによる特定個人情報ファイルの管理</li> <li>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</li> <li>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</li> <li>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</li> <li>⑤機構への本人確認情報の照会</li> </ol>	<p>住民基本台帳ネットワークに関する事務は、「1. 本人確認情報の管理及び提供等に関する事務」及び「2. 附帯本人確認情報の管理及び提供等に関する事務」に分かれる。</p> <p>1. 本人確認情報の管理及び提供等に関する事務 奈良県(以下「県」という。))は、住民法に基づいて住民基本台帳のネットワーク化を図り、全国共通の本人確認システム(住民ネット)を市町村と共同して構築している。</p> <p>なお、住民基本台帳は、住民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の地位を記録する各県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に行うものであり、市町村において、住民の居住関係の公益、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。</p> <p>県では、住民法の規定に従い、特定個人情報(を以下の事務で取り扱う。(別添1を参照)</p> <ol style="list-style-type: none"> <li>①磁気ディスクによる特定個人情報ファイルの管理</li> <li>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機構への通知</li> <li>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又は他部署への移転</li> <li>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</li> <li>⑤機構への本人確認情報の照会</li> </ol>	<p>事前 重要な変更となるため事前に報告</p>
<p>1 基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム システム②) システムの名称</p>	<p>団体内統合宛名システム</p>	<p>附帯連携システム ※3. 特定個人情報ファイル名に示す「都道府県知事保存附帯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、附帯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、附帯連携システム内の附帯都道府県サーバ部分について記載する。</p>	<p>事前 重要な変更となるため事前に報告</p>

	<p>1 基本情報 2 特定個人情報ファイルを取り扱う事柄において使用するシステム②③システムの機能</p>	<p>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</p> <p>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</p> <p>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</p> <p>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</p> <p>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</p> <p>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</p> <p>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</p> <p>8. 共通変換機能 既存システムと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</p> <p>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</p> <p>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</p> <p>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の機能</p>	<p>1. 附票本人確認情報の更新 都道府県知事保存附票本人確認情報ファイルを最新の状態で保つため、市町村の登録して通知された附票本人確認情報の更新情報元に当該ファイルを更新し、附票全国サーバに対して当該附票本人確認情報の更新情報を通知する。</p> <p>2. 県以外の執行機関への情報提供又は他部署への転記 県以外の執行機関又は他部署による住民基本台帳に基づく情報照会に対応するため、照会があった当該個人の4情報等に対応付く附票本人確認情報を都道府県知事保存附票本人確認情報ファイルから抽出し、照会元に提供・転送する。</p> <p>その際、番号法で認められた場合に限り、県以外の執行機関又は他部署からの求めに対し、附票本人確認情報の提供・転記に併せて当該個人の住民基本台帳コードを用いて、都道府県知事保存附票本人確認情報ファイルから個人番号を抽出し、照会元に提供・転送する場合があります。</p> <p>3. 附票本人確認情報の開示 法律に基づき(注)による自己の附票本人確認情報の開示請求に対応するため、当該個人の附票本人確認情報を都道府県知事保存附票本人確認情報ファイルから抽出し、帰票に出力する。</p> <p>4. 照会への情報照会 附票全国サーバに対して住民基本台帳コード又は4情報の組合せをキーとした附票本人確認情報照会要求を行い、該当する個人の附票本人確認情報を受領する。</p> <p>5. 附票本人確認情報検索 附票都道府県サーバの代表端末又は業務端末(都道府県サーバ)と共用する。)において入力された4情報(氏名、住所、性別、生年月日)の組合せをキーに都道府県知事保存附票本人確認情報ファイルを検索し、検索条件に該当する附票本人確認情報の一覧を画面上に表示する。</p> <p>6. 附票本人確認情報整合 都道府県知事保存附票本人確認情報ファイルの正確性を担保するため、市町村から附票本人確認情報を受領し、当該附票本人確認情報を用いて当該ファイルに記録された附票本人確認情報の整合性を確認を行う。</p> <p>7. 個人番号制度の運用に伴う情報連携 中間サーバ上で作成される符号取得依頼ファイルと、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と団体内統合宛名システムの間に変換し専用装置を設けて、本人確認情報ファイル等の受け渡しを行う。</p>	事前	重要な変更となるため事前に報告
	<p>1 基本情報 2 特定個人情報ファイルを取り扱う事柄において使用するシステム③④システムの名称</p>	団体内統合宛名システム		事前	重要な変更となるため事前に報告
	<p>1 基本情報 2 特定個人情報ファイルを取り扱う事柄において使用するシステム②③システムの機能</p>	<p>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</p> <p>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</p> <p>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</p> <p>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</p> <p>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</p> <p>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</p> <p>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</p> <p>8. 共通変換機能 既存システムと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</p> <p>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</p> <p>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</p> <p>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の機能</p>	<p>〔 〕情報提供ネットワークシステム 〔 〇 〕府内連携システム 〔 〇 〕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 〔 〇 〕宛名システム等 〔 〕税務システム 〔 〇 〕その他(附票連携システム、中間サーバ)</p>	事前	重要な変更となるため事前に報告
	<p>1 基本情報 3 特定個人情報ファイル名</p>	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	<p>(1) 都道府県知事保存本人確認情報ファイル (2) 都道府県知事保存附票本人確認情報ファイル (3) 符号取得要求ファイル</p>	事前	重要な変更となるため事前に報告

<p>1 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 実施上の必要正</p>	<p>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、下記に掲げる必要性から取り扱う。</p> <ul style="list-style-type: none"> <li>・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。</li> <li>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。</li> <li>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、当該更新情報を機関に対して 通知する。</li> <li>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、当該個人に係る都道府県知事保存本人 確認情報を開示する。</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul> <p>・番号制度の運用において、県の中継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シ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、中継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。</p>	<p>県では、都道府県知事保存本人確認情報ファイル、都道府県知事保存 附票本人確認情報ファイル及び符号取得要求ファイル、下記に記載 の通りの必要性から取り扱う。</p> <p>(1) 都道府県知事保存本人確認情報ファイル ・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。</p> <p>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(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。</p> <p>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、当該更新情報を機関に対して 通知する。</p> <p>③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。</p> <p>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。</p> <p>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、本人確認情報を検索する。</p> <p>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。</p> <p>(2) 都道府県知事保存附票本人確認情報ファイル ・都道府県知事保存附票本人確認情報ファイルは、転出転入に係る 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、附票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。</p> <p>①附票連携システムに係る附票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附票本人確認 情報を管理する。</p> <p>②市町村からの附票本人確認情報の更新情報の通知を受けて都道府 県知事保存附票本人確認情報ファイルを更新し、当該更新情報を機関 に対して通知する。</p> <p>③県の他の執行機関又は他部署からの照会に基づき、附票本人確認 情報を提供・移転する。</p> <p>その際、番号法で認められた場合に限り、県の他の執行機関又は他部 署からの求めに応じ、附票本人確認情報の提供・移転に併せて当該個 人の住民基本台帳コードを用いて、都道府県知事保存本人確認情報ファイル から個人番号を抽出し、照会元へ提供・移転する可能性がある。</p> <p>④本人からの請求に基づき、当該個人の附票本人確認情報を開示す る。</p> <p>⑤附票本人確認情報の管理及び提供等に関する事務において、附票 本人確認情報を検索する。</p> <p>⑥市町村において保存する附票本人確認情報との整合性を確認する。</p> <p>(3) 符号取得要求ファイル ・番号制度の運用において、県の中継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シ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、中継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。</p>	<p>事前</p>	<p>重要な変更となるため事前に 報告</p>
<p>1 基本情報 4. 特定個人情報 ファイルを取り扱う理由 ② 実現 が期待されるメリット</p>	<p>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、証明書等を入力する金銭的、時間的コストの節約)につながる ことが見込まれる。</p>	<p>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、証明書等を入力する金銭的、時間的コストの節約)につながる ことが見込まれる。</p> <p>また、転出転入を含め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。</p>	<p>事前</p>	<p>重要な変更となるため事前に 報告</p>
<p>1 基本情報 5. 個人番号の利 用 法令上の根拠</p>	<p>住民基本台帳法(昭和42年7月25日法律第81号) ・第7条(住民票の記載事項) ・第12条の5(住民基本台帳の脱離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関への本人確認情報の通知等) ・第30条の8(本人確認情報の取りに関する機関の通報) ・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22(市町村間の連絡調整等) ・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)</p>	<p>住民基本台帳法(昭和42年7月25日法律第81号) ・第7条(住民票の記載事項) ・第12条の5(住民基本台帳の脱離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関への本人確認情報の通知等) ・第30条の8(本人確認情報の取りに関する機関の通報) ・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22(市町村間の連絡調整等) ・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) ・第30条の44の6第3項(都道府県知事保存本人確認情報(住民 票コードに限る。))の利用)</p>	<p>事前</p>	<p>重要な変更となるため事前に 報告</p>
<p>1 基本情報 (別添1) 事務の内 容(1)</p>	<p>【図】</p>	<p>(1) 本人確認情報の管理及び提供等に関する事務</p> <p>【図】</p>	<p>事前</p>	<p>重要な変更となるため事前に 報告</p>
<p>1 基本情報 (別添1) 事務の内 容(2)</p>	<p>—</p>	<p>(2) 附票本人確認情報の管理及び提供等に関する事務</p> <p>【新規に作成】</p>	<p>事前</p>	<p>重要な変更となるため事前に 報告</p>

<p>I 基本情報 (別添1事務の内容(2)(備考))</p>		<p>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 機関に対し、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。</p> <p>2. 県の他の執行機関又は他部署又は他都署への移転  2-① 県の他の執行機関又は他都署において、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附票全国サーバに対して検索の要求を行う。  ※県の他の執行機関又は他都署に、附票本人確認情報を一括して提供する場合は(一括提供の方式(注1)により行う場合)には、県の他の執行機関又は他都署において、附票都道府県サーバの代表端末又は業務端末(都道府県サーバと共有する。)を操作し、媒体連携(回線連携)を用いる場合は、「媒体連携又は回線連携」と記載(注2、注3)により行う。  (注1)県の他の執行機関又は他都署においてファイル化された附票本人確認情報照会対象者の情報(検索条件のリスト)を元に附票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附票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附票本人確認情報の提供を行う場合に、情報連携に通信回線(市内LAN等)を用いる方法を指す。具体的には、附票都道府県サーバの代表端末又は業務端末(都道府県サーバと共有する。)と市内システム(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。</p> <p>3. 附票本人確認情報の開示に関する事務  3-① 住民より附票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附票本人確認情報を開示する。</p> <p>4. 機関への情報照会に係る事務  4-① 機関に対し、4情報等をキーワードとした附票本人確認情報の照会を行う。  4-② 機関より、当該個人の附票本人確認情報を受領する。</p> <p>5. 附票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。</p> <p>6. 附票本人確認情報整合  6-① 市町村CSより、附票都道府県サーバに対し、整合性確認用の附票本人確認情報を送信する。  6-② 附票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附票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 附票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。</p> <p>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側と代表端末または業務端末側との間に受渡し専用装置を設けて、附票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(処理通書、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間に受渡し専用装置を介して受領し、附票全国サーバに送信する。  ※附票全国サーバは、個人番号を住民コードに置き換えて、情報提供ネットワークシステムに(処理通書、住民コード)を送信する。情報提供ネットワークシステムは、受領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。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>II 特定個人情報ファイルの概要(都道府県知事保存本人情報ファイル)1. 特定個人情報ファイル名</p>	<p>都道府県知事保存本人情報ファイル</p>		<p>(1) 都道府県知事保存本人情報ファイル</p>	<p>事前</p> <p>重要な変更となるため事前に報告</p>
<p>II 特定個人情報ファイルの概要(都道府県知事保存本人情報ファイル)15. 特定個人情報の提供・移転(委託に伴うものを除く。)</p>	<p>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</p>		<p>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2条</p>	<p>事前</p> <p>重要な変更となるため事前に報告</p>
<p>II 特定個人情報ファイルの概要(都道府県知事保存本人情報ファイル)16. 特定個人情報の保管・消去</p>	<p>&lt;住民基本台帳ネットワークシステムにおける措置&gt;  ・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、施設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設管理及び入退室管理を行っているサーバ室内に保管し、業務端末にはセキュリティファイヤを施し、当該端末を設置した執務室は職員が退庁する際は施設するなど必要な措置を講じる。</p> <p>&lt;団体内統合宛名システムにおける措置&gt;  ・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。</p>	<p>&lt;住民基本台帳ネットワークシステムにおける措置&gt;  ・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、施設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と生体認証(又はパスワード)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設管理及び入退室管理を行っているサーバ室内に保管し、業務端末にはセキュリティファイヤを施し、当該端末を設置した執務室は職員が退庁する際は施設するなど必要な措置を講じる。</p> <p>&lt;団体内統合宛名システムにおける措置&gt;  ・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。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>

	Ⅱ 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル) 1. 特定個人情報ファイル名		(2)都道府県知事保存附票本人確認情報ファイル	事前	重要な変更となるため事前に報告
	Ⅱ 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル) 2. 基本情報 ①ファイルの種類		システム用ファイル	事前	重要な変更となるため事前に報告
	Ⅱ 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル) 2. 基本情報 ②対象となる本人の数		100万人以上1,000万人未満	事前	重要な変更となるため事前に報告
	Ⅱ 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル) 2. 基本情報 ③対象となる本人の範囲		県内のいずれかの市町村において、住基法第16条(戸籍の附票の作成)に基づき戸籍の附票に記録された住民。 ※消除者を含む。  本特定個人情報ファイル(都道府県知事保存附票本人確認情報ファイル)において県内の戸籍の附票に記録された全ての住民の情報を保有し、その記録を常に正確に更新・管理・提供・移転する必要があるため。	事前	重要な変更となるため事前に報告
	Ⅱ 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル) 2. 基本情報 ④記録される項目		10項目以上50項目未満  [○] 個人番号 [○] 4情報(氏名、性別、生年月日、住所) [○] その他(その他戸籍の附票関係情報(戸籍の表示に係る情報は含まない。))  -4情報、その他戸籍の附票関係情報(戸籍の表示に係る情報は含まない。) -法令に基づき戸籍の附票に記録された者に関する記録を正確に行う上で、戸籍の附票の記載等に係る附票本人確認情報(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。なお、別添2に記載のとおり、記録項目には戸籍の表示に係る情報(本籍及び筆跡者の氏名)は含まない。 -個人番号 -国外転出者に係る事務処理に関し、番号法で認められた場合に限り、県の執行機関等からの求めに応じ、当該個人の住民票コードを用いて、都道府県知事保存附票本人確認情報ファイルから個人番号を抽出し、附票都道府県サーバに連携する場合がある。提供又は移転後、個人番号は、都道府県知事保存附票本人確認情報ファイルに保有することはない  別添2を参照。	事前	重要な変更となるため事前に報告
	Ⅱ 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル) 2. 基本情報 ⑤保有開始日		「情報通信技術の活用による行政手続等に係る関係者の利便性の向上並びに行政運営の効率化及び効率化を図るための行政手続等における情報通信の技術の利用に関する法律等の一部を改正する法律(令和元年法律第18号)」附則第1条第10号にて規定される公布から起算して5年を超えない範囲内の政令で定める日。	事前	重要な変更となるため事前に報告
	Ⅱ 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル) 2. 基本情報 ⑥事務担当部署		知事公室市町村振興課	事前	重要な変更となるため事前に報告
	Ⅱ 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル) 3. 特定個人情報 ③ 入手・使用 ① 入手元		[○] 地方公共団体・地方独立行政法人 [○] その他(都道府県サーバ※入手には該当しないが、都道府県サーバから個人番号を抽出する場合がある)	事前	重要な変更となるため事前に報告
	Ⅱ 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル) 3. 特定個人情報 ③ 入手・使用 ② 入手方法		[○] 専用線	事前	重要な変更となるため事前に報告
	Ⅱ 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル) 3. 特定個人情報 ③ 入手・使用 ③ 入手の時期・頻度		戸籍の附票において、附票本人確認情報の変更又は新規作成(出生等)が発生した都度入手する。  ※番号法別表に掲げる事務につき、県の他の執行機関等から国外転出者に係るものに関し求めがあった場合、個人番号をその都度抽出する場がある。	事前	重要な変更となるため事前に報告
	Ⅱ 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル) 3. 特定個人情報 ④ 入手に係る妥当性		法令に基づき、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、国外転出者に係る本人確認を行う上で、市町村の戸籍の附票の記載事項に変更が生じた都度、当該市町村を通じて入手し、機関に通知する必要がある。 また、入手の手段として、法令に基づき構築された専用回線である、住基ネット(※※)を用いることで、入手に係るリスクを軽減している。  ※なお、住基法第30条の4の6第3項に基づき、都道府県知事保存附票本人確認情報(住民票コードに限る。)を利用し、第30条の15第1項又は第2項の規定による事務について個人番号を提供することができる。  ※※附票連携システムは、住基ネットを利用して構築されている。住基ネットは、保有情報・利用の制限、内部の不正利用の防止、外部からの侵入防止など、セキュリティ確保のための様々な措置が講じられており、平成14年9月5日の以降、住基ネットのハッキングや情報漏えいなどの事件や障害は一度も発生していない。	事前	重要な変更となるため事前に報告
	Ⅱ 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル) 3. 特定個人情報 ⑤ 本人への明示		都道府県知事が当該市町村の区域内における附票本人確認情報を入力することについて、住基法第30条の41(市町村長から都道府県知事への附票本人確認情報の通知等)に明示されている。  ※都道府県知事が国外転出者に係る個人番号を抽出する場合があることについて、住基法第30条の4の6第3項に明示されている。	事前	重要な変更となるため事前に報告
	Ⅱ 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル) 3. 特定個人情報 ⑥ 使用目的		都道府県知事保存附票本人確認情報ファイルにおいて県内の戸籍の附票に記録された県内の全ての住民の情報を保有し、その記録を常に正確に更新・管理・提供・移転する。  ※番号法別表に掲げる事務につき、県の他の執行機関等から国外転出者に係るものに関し求めがあった場合、個人番号をその都度抽出し、第30条の15第1項又は第2項の規定による事務について提供する場合がある。	事前	重要な変更となるため事前に報告
	Ⅱ 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル) 3. 特定個人情報 ⑦ 使用の主体		知事公室市町村振興課  [ 10人未満 ]	事前	重要な変更となるため事前に報告

<p>II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)3. 特定個人情報 の入手・使用 ⑧使用方法 情報の突合</p>		<p>県の他の執行機関又は他部署からの附票本人確認情報の照会要求を受け(県の他の執行機関又は他部署一附票都道府県サーバ)、照会のあった住民票コード又は4情報の組合せを元に都道府県知事保存附票本人確認情報ファイルを検索し、該当する個人の附票本人確認情報を照会元へ提供・移転する(附票都道府県サーバ一県の他の執行機関又は他部署)。</p> <p>※その際、番号法で認められた場合に限り、附票本人確認情報の提供に併せて、当該個人の住民票コードを用いて都道府県知事保存本人確認情報ファイルから個人番号を抽出し、照会元へ提供・移転する場合がある。</p>	事前	重要な変更となるため事前に報告
<p>II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)3. 特定個人情報 の入手・使用 ⑧使用方法 情報の突合</p>		都道府県知事保存附票本人確認情報ファイルの住民票コードと都道府県知事保存本人確認情報ファイルの個人番号を突合する。	事前	重要な変更となるため事前に報告
<p>II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)3. 特定個人情報 の入手・使用 ⑧使用方法 情報の統計分析</p>		該当なし	事前	重要な変更となるため事前に報告
<p>II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)3. 特定個人情報 の入手・使用 ⑧使用方法 権利利益に影響を与える決定</p>		該当なし	事前	重要な変更となるため事前に報告
<p>II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)3. 特定個人情報 の入手・使用 ⑨使用開始日</p>		「情報通信技術の活用による行政手続等に係る関係者の利便性の向上並びに行政運営の簡素化及び効率化を図るための行政手続等における情報通信技術の活用に関する法律等の一部を改正する法律(令和元年法律第16号)附則第1条第10号にて規定される公布から起算して3年を超えない範囲内の政令で定める日。	事前	重要な変更となるため事前に報告
<p>II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)4. 特定個人情報 ファイルの取扱いの委託 委託 の有無</p>		[ 委託する ] [ ( 1 )件 ]	事前	重要な変更となるため事前に報告
<p>II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)4. 特定個人情報 ファイルの取扱いの委託 委託 事項</p>		附票都道府県サーバの運用及び監視に関する業務	事前	重要な変更となるため事前に報告
<p>II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)4. 特定個人情報 ファイルの取扱いの委託 委託 事項 ①委託内容</p>		全国の都道府県サーバを1拠点(集約センター)に集約化することとしたことに伴い、都道府県サーバと同様に附票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。この委託する業務は、附票本人確認情報に直接関係がない(附票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。	事前	重要な変更となるため事前に報告
<p>II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)4. 特定個人情報 ファイルの取扱いの委託 委託 事項 ②取扱いを委託する特定 個人情報ファイルの範囲</p>		[ 特定個人情報ファイルの全体 ]	事前	重要な変更となるため事前に報告
<p>II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)4. 特定個人情報 ファイルの取扱いの委託 委託 事項 ②取扱いを委託する特定 個人情報ファイルの範囲 対象となる本人の数</p>		[ 100万人以上1,000万人未満 ]	事前	重要な変更となるため事前に報告
<p>II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)4. 特定個人情報 ファイルの取扱いの委託 委託 事項 ②取扱いを委託する特定 個人情報ファイルの範囲 対象となる本人の範囲</p>		[ 2. ③対象となる本人の範囲 ]と向上	事前	重要な変更となるため事前に報告
<p>II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)4. 特定個人情報 ファイルの取扱いの委託 委託 事項 ②取扱いを委託する特定 個人情報ファイルの範囲 その他受託者</p>		都道府県知事保存附票本人確認情報ファイルが保存される附票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、附票本人確認情報に直接関係の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。	事前	重要な変更となるため事前に報告
<p>II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)4. 特定個人情報 ファイルの取扱いの委託 委託 事項 ③委託先における取 扱者数</p>		[ 10人未満 ]	事前	重要な変更となるため事前に報告
<p>II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)4. 特定個人情報 ファイルの取扱いの委託 委託 事項 ④委託先への特定 個人情報ファイルの提供方法</p>		[ ○ ]専用線	事前	重要な変更となるため事前に報告
<p>II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)4. 特定個人情報 ファイルの取扱いの委託 委託 事項 ⑤委託先名の確認方法</p>		委託先が決定した際に県ホームページにて公開する。	事前	重要な変更となるため事前に報告
<p>II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)4. 特定個人情報 ファイルの取扱いの委託 委託 事項 ⑥委託先名</p>		地方公共団体情報システム機構(機構)	事前	重要な変更となるため事前に報告
<p>II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)4. 特定個人情報 ファイルの取扱いの委託 委託 事項 ⑦委託先の有無</p>		[ 再委託する ]	事前	重要な変更となるため事前に報告

	II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)4. 特定個人情報ファイルの取扱いの委託 委託事項 再委託 ⑦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。	事前	重要な変更となるため事前に報告
	II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)4. 特定個人情報ファイルの取扱いの委託 委託事項 再委託 ⑧再委託事項	-	附票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、附票本人確認情報に直接関係しない(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、「③委託内容」の通り、委託事項は、附票本人確認情報に直接関係しない事務を対象としているが、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。	事前	重要な変更となるため事前に報告
	II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)5. 特定個人情報の提供・移転(委託に伴うものを除く) 特定個人情報の提供・移転の有無	-	[ ○ ] 提供を行っている ( 1 )件 [ ○ ] 移転を行っている ( 1 )件	事前	重要な変更となるため事前に報告
	II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)5. 特定個人情報の提供・移転(委託に伴うものを除く) 提供先1	-	県その他の執行機関(教育委員会など)	事前	重要な変更となるため事前に報告
	II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)5. 特定個人情報の提供・移転(委託に伴うものを除く) 提供先1 ①法令上の根拠	-	住基法第30条の15第2項(本人確認情報の利用) 奈良県住基基本台帳法施行条例第3条 住基法第30条の44の6第3項(都道府県知事保存附票本人確認情報(住民票コードに限る。))の利用	事前	重要な変更となるため事前に報告
	II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)5. 特定個人情報の提供・移転(委託に伴うものを除く) 提供先1 ②提供先における用途	-	住基法別表第六及び奈良県住基基本台帳法施行条例別表第二に掲げられた県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、県そ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。)	事前	重要な変更となるため事前に報告
	II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)5. 特定個人情報の提供・移転(委託に伴うものを除く) 提供先1 ③提供する情報	-	住民票コード、氏名、住所、生年月日、性別、個人番号(番号法に基づく県その他の執行機関からの求めがあった場合に限る。) ※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)第22条第7項に基づく経過措置である。	事前	重要な変更となるため事前に報告
	II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)5. 特定個人情報の提供・移転(委託に伴うものを除く) 提供先1 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 ]	事前	重要な変更となるため事前に報告
	II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)5. 特定個人情報の提供・移転(委託に伴うものを除く) 提供先1 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	事前	重要な変更となるため事前に報告
	II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)5. 特定個人情報の提供・移転(委託に伴うものを除く) 提供先1 ⑥提供方法	-	[ ○ ] 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 [ ○ ] その他(住基基本台帳ネットワークシステム )	事前	重要な変更となるため事前に報告
	II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)5. 特定個人情報の提供・移転(委託に伴うものを除く) 提供先1 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。	事前	重要な変更となるため事前に報告
	II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)5. 特定個人情報の提供・移転(委託に伴うものを除く) 移転先1	-	県その他部署(税務課など)	事前	重要な変更となるため事前に報告
	II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)5. 特定個人情報の提供・移転(委託に伴うものを除く) 移転先1 ①法令上の根拠	-	住基法第30条の15第1項(本人確認情報の利用) 奈良県住基基本台帳法施行条例第2条 住基法第30条の44の6第3項(都道府県知事保存附票本人確認情報(住民票コードに限る。))の利用	事前	重要な変更となるため事前に報告
	II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)5. 特定個人情報の提供・移転(委託に伴うものを除く) 移転先1 ②移転先における用途	-	住基法別表第五及び奈良県住基基本台帳法施行条例別表第一に掲げられた県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、県そ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。)	事前	重要な変更となるため事前に報告
	II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)5. 特定個人情報の提供・移転(委託に伴うものを除く) 移転先1 ③移転する情報	-	住民票コード、氏名、住所、生年月日、性別、個人番号(番号法に基づく県その他部署からの求めがあった場合に限る。) ※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)第22条第7項に基づく経過措置である。	事前	重要な変更となるため事前に報告
	II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)5. 特定個人情報の提供・移転(委託に伴うものを除く) 移転先1 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 ]	事前	重要な変更となるため事前に報告
	II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)5. 特定個人情報の提供・移転(委託に伴うものを除く) 移転先1 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	事前	重要な変更となるため事前に報告
	II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)5. 特定個人情報の提供・移転(委託に伴うものを除く) 移転先1 ⑥移転方法	-	[ ○ ] 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 [ ○ ] その他(住基基本台帳ネットワークシステム )	事前	重要な変更となるため事前に報告
	II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル)5. 特定個人情報の提供・移転(委託に伴うものを除く) 移転先1 ⑦時期・頻度	-	県その他部署からの検索要求があった都度、随時。	事前	重要な変更となるため事前に報告

<p>II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル) 6. 特定個人情報の保管・消去 ①保管場所</p>	<p>—</p>	<p>&lt;附票連携システムにおける措置&gt; ・セキュリティゲートにて入退館管理をしている附票都道府県サーバの集約センターにおいて、施設管理及び入退館管理(監視カメラを設置してサーバ設置場所への入退館者を特定・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と生体認証(又はパスワード)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設管理及び入退館管理を行っているサーバに保管し、業務端末にはセキュリティロックを施し、当該端末を設置した執務室は職員が退庁する際は施設するなど必要な措置を講じる。  &lt;団体内統合宛名システムにおける措置&gt; 入退館管理を行っているサーバ上で管理すると共に、監視カメラによる入退館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。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル) 6. 特定個人情報の保管・消去 ①保管期間</p>	<p>—</p>	<p>[ 1年未満 ]  附票本人確認情報の提供に併せて提供される個人番号は、県その他の執行機関又は他部署からの求めにより提供・移転された後は、障害発生等により提供・移転先で情報を受領できなかった場合に備えて、一時的に保存されるのみである。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>II 特定個人情報ファイルの概要 (都道府県知事保存附票本人情報ファイル) 6. 特定個人情報の保管・消去 ③消去方法</p>	<p>—</p>	<p>一時的な保存後にシステムにて自動判別し消去する。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>II 特定個人情報ファイルの概要 (符号取得要求ファイル) 1. 特定個人情報ファイル名</p>	<p>符号取得要求ファイル</p>	<p>(3)符号取得要求ファイル</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>II 特定個人情報ファイルの概要 (別添2) 特定個人情報ファイル記録項目</p>	<p>都道府県知事保存本人確認情報ファイル</p> <ol style="list-style-type: none"> <li>住民票コード</li> <li>漢字氏名</li> <li>外字数(氏名)</li> <li>ふりがな氏名</li> <li>生年月日</li> <li>性別</li> <li>住所</li> <li>外字数(住所)</li> <li>個人番号</li> <li>異動事由</li> <li>異動年月日</li> <li>保存期間フラグ</li> <li>消音化かな氏名</li> <li>市町村コード</li> <li>大文字・小文字コード</li> <li>操作者ID</li> <li>操作端末ID</li> <li>タイムスタンプ</li> <li>通知を受けた年月日</li> <li>外字フラグ</li> <li>削除フラグ</li> <li>更新原番号</li> <li>氏名外字変更連番</li> <li>住所外字変更連番</li> <li>旧氏 漢字</li> <li>旧氏 外字数</li> <li>旧氏 ふりがな</li> <li>旧氏 外字変更連番</li> </ol> <p>符号取得要求ファイル</p> <ol style="list-style-type: none"> <li>処理連番</li> <li>個人番号</li> <li>符号再発行フラグ</li> </ol>	<p>(1)都道府県知事保存本人確認情報ファイル</p> <ol style="list-style-type: none"> <li>住民票コード</li> <li>漢字氏名</li> <li>外字数(氏名)</li> <li>ふりがな氏名</li> <li>生年月日</li> <li>性別</li> <li>住所</li> <li>外字数(住所)</li> <li>個人番号</li> <li>異動事由</li> <li>異動年月日</li> <li>保存期間フラグ</li> <li>消音化かな氏名</li> <li>市町村コード</li> <li>大文字・小文字コード</li> <li>操作者ID</li> <li>操作端末ID</li> <li>タイムスタンプ</li> <li>通知を受けた年月日</li> <li>外字フラグ</li> <li>削除フラグ</li> <li>更新原番号</li> <li>氏名外字変更連番</li> <li>住所外字変更連番</li> <li>旧氏 漢字</li> <li>旧氏 外字数</li> <li>旧氏 ふりがな</li> <li>旧氏 外字変更連番</li> </ol> <p>(2)都道府県知事保存附票本人確認情報ファイル</p> <p>ア 附票本人確認情報</p> <ol style="list-style-type: none"> <li>住民票コード</li> <li>漢字氏名</li> <li>外字数</li> <li>ふりがな氏名</li> <li>生年月日</li> <li>性別</li> <li>住所</li> <li>市町村コード</li> <li>住所</li> <li>外字数</li> <li>最終住所 漢字</li> <li>最終住所 外字数</li> <li>異動年月日</li> <li>旧氏 漢字</li> <li>旧氏 外字数</li> <li>旧氏 ふりがな</li> <li>旧氏 外字変更連番</li> <li>氏名外字変更連番</li> <li>住所外字変更連番</li> <li>旧氏 漢字</li> <li>旧氏 外字数</li> <li>旧氏 ふりがな</li> <li>旧氏 外字変更連番</li> </ol> <p>イ その他個人番号</p> <p>(※国外転出者に係る事務処理に限り、番号法で認められた場合に限り、県その他の執行機関又は他部署からの求めに応じ、当該個人の住民票コードを用いて、都道府県知事保存本人確認情報ファイルから個人番号を抽出し、提供・移転する場合がある。)</p> <p>(3)符号取得要求ファイル</p> <ol style="list-style-type: none"> <li>処理連番</li> <li>個人番号</li> <li>符号再発行フラグ</li> </ol>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>III 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存本人確認情報ファイル) 1. 特定個人情報ファイル名</p>	<p>都道府県知事保存本人確認情報ファイル</p>	<p>(1)都道府県知事保存本人確認情報ファイル</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>III 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存本人確認情報ファイル) 3. 特定個人情報の使用 リスク 1 事務で使用するその他のシステムにおける措置の内容</p>	<p>都道府県サーバと庁内システムとの接続は行わない。</p>	<p>都道府県サーバと庁内システムとの接続は行わない。  都道府県サーバは、集約センター内において、附票都道府県サーバと接続する。  なお、都道府県サーバは附票都道府県サーバのシステム間のアクセスは、以下の場面の処理に限られるよう、システムにより制限する。  (1)都道府県サーバ⇒附票都道府県サーバへのアクセス 番号法で認められた場合に限り、県その他の執行機関又は他部署等からの求めに応じ、国外転出者に係る個人番号を連携する場合。  (2)附票都道府県サーバ⇒都道府県サーバへのアクセス 国外転出者に係る事務処理に限り、番号法で認められた場合に限り、県その他の執行機関又は他部署等からの求めに応じ、個人番号を入手する場合(目的を超えた連携が行われないよう、個人番号は附票本人確認情報DBとは別の一時的保存領域で処理する。)</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>III 特定個人情報の取扱いプロセスにおけるリスク対策 (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の取扱いの委託 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</p>	<p>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、県そ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のある場合には、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ち会う。 また、都道府県サーバの代表端末または業務端末と受渡し専用装置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。</p>	<p>再委託先については、毎年度の契約において、再委託先業者の業務内容や委託先との業務分担を審査した上で承認を行っているほか、随時業務状況を確認する。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>III 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存本人確認情報ファイル) 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) 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</p>	<p>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、県そ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のある場合には、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ち会う。 また、都道府県サーバの代表端末または業務端末と受渡し専用装置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。</p>	<p>連携手段として通信の記録が逐一保存され、また、連携するデータが暗号化される仕組みが確立した住民基本台帳ネットワークシステムを用いることにより、不適切な方法による特定個人情報の提供を防止する。 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、県そ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のある場合には、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ち会う。 また、都道府県サーバの代表端末または業務端末と受渡し専用装置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。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>



<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)1. 特定個人情報ファイル名</p>	-	<p>(2)都道府県知事保存附票本人確認情報ファイル</p>	事前	<p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票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を適した入手を除く。)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</p>	-	<p>都道府県知事保存附票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41第1項に基づき通知)される附票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。 また、対象者以外の個人番号は入手できないことを、システムにより担保する。</p>	事前	<p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)3. 特定個人情報の入手(情報提供ネットワークを適した入手を除く。)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</p>	-	<p>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で担保されている。(都道府県知事保存附票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からの附票本人確認情報更新要求の際に通知(住基法第30条の41第1項に基づき通知)される本人確認情報に限定される。また、対象者の個人番号以外の個人情報は入手できないことを、システムにより担保する。</p>	事前	<p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票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を適した入手を除く。)リスク1 リスクへの対策は十分か</p>	-	<p>[ 十分である ]</p>	事前	<p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票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を適した入手を除く。)リスク2 リスクに対する措置の内容</p>	-	<p>都道府県知事保存附票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からの附票本人確認情報更新要求の際に通知(住基法第30条の41第1項に基づき通知)される附票本人確認情報に限定される。 また、国が転出者に係る事務処理に關し、番号で認められた場合に限り、県の執行機関又は他部署等からの求めに応じ、個人番号を入手すること、システムにより担保する。</p>	事前	<p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票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を適した入手を除く。)リスク2 リスクへの対策は十分か</p>	-	<p>[ 十分である ]</p>	事前	<p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票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を適した入手を除く。)リスク3 入手の際の本人確認の措置の内容</p>	-	<p>都道府県知事保存附票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からの附票本人確認情報更新要求の際に通知(住基法第30条の41第1項に基づき通知)される附票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、届出の旨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。個人番号については、都道府県知事保存附票本人確認情報ファイルから入手するため、該当なし。</p>	事前	<p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票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を適した入手を除く。)リスク3 個人番号の真正性確認の措置の内容</p>	-	<p>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ように、システムで担保する。 また、都道府県知事保存附票本人確認情報ファイルに保存される段階で真正性が担保されている。</p>	事前	<p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票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を適した入手を除く。)リスク3 特定個人情報の正確性確保の措置の内容</p>	-	<p>システム上、附票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。 個人番号については、都道府県知事保存附票本人確認情報ファイルに保存される段階で正確性が確保されている。</p>	事前	<p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票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を適した入手を除く。)リスク3 その他の措置の内容</p>	-	<p>システムでは対応できない事象が発生した際に、附票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附票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。</p>	事前	<p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票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を適した入手を除く。)リスク3 リスクへの対策は十分か</p>	-	<p>[ 十分である ]</p>	事前	<p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票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を適した入手を除く。)リスク4 リスクに対する措置の内容</p>	-	<p>・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。 ※附票都道府県サーバのサーバ上で稼働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や附票全国サーバとのデータ交換を行う。 サーバの安全確保対策、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、データの盗竊、改ざん、破壊及び盗難、開示の不正利用及びなりすまし等を防止する。</p>	事前	<p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)3. 特定個人情報の利用リスク1</p>	-	<p>[ 十分である ]</p>	事前	<p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)3. 特定個人情報の利用リスク1</p>	-	<p>・附票都道府県サーバの代表端末または業務端末と団体内統合宛名システムの間に変換専用装置を設けて、要求ファイル等の受け渡し連絡を行う。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図られる。目的を定めた届け付け、事前に必要な情報の届け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再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。</p>	事前	<p>重要な変更となるため事前に報告</p>

	<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)3. 特定個人情報の使用リスク1 事務で使用するその他のシステムにおける措置の内容</p>		<p>附票都道府県サーバと市内システムとの接続は行わない。 附票都道府県サーバは、集約センター内において、都道府県サーバと接続する。 なお、附票都道府県サーバと都道府県サーバのシステム間のアクセスは、以下の場合の処理に限られるよう、システムにより制限する。 (1) 附票都道府県サーバ⇔都道府県サーバへのアクセス 国外転出者に係る事務処理に関し、番号法で認められた場合に限り、県の他の執行機関又は他部署等からの求めに応じ、個人番号を入手する場合(目的を越えた紐づけが行われないよう、個人番号は附票本人確認情報DBとは別の一時保存領域で処理する。) (2) 都道府県サーバ⇔附票都道府県サーバへのアクセス 番号法で認められた場合に限り、県の他の執行機関又は他部署等からの求めに応じ、国外転出者に係る個人番号を連携する場合。</p>	事前	重要な変更となるため事前に報告
	<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)3. 特定個人情報の使用リスク1 リスクへの対策は十分か</p>		[ 十分である ]	事前	重要な変更となるため事前に報告
	<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)3. 特定個人情報の使用リスク2 ユーザ認証の管理</p>		[ 行っている ] 附票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会ID及び照会情報(種類による生体認証)による操作者認証を行う。	事前	重要な変更となるため事前に報告
	<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)3. 特定個人情報の使用リスク2 アクセス権限の発効・失効の管理</p>		[ 行っている ] -操作者照会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、操作者照会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。	事前	重要な変更となるため事前に報告
	<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)3. 特定個人情報の使用リスク2 アクセス権限の管理</p>		[ 行っている ] -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、附票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。	事前	重要な変更となるため事前に報告
	<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)3. 特定個人情報の使用リスク2 特定個人情報の使用の記録</p>		[ 記録を残している ] -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、安全な場所に施設保管する。	事前	重要な変更となるため事前に報告
	<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)3. 特定個人情報の使用リスク2 リスクへの対策は十分か</p>		[ 十分である ]	事前	重要な変更となるため事前に報告
	<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)3. 特定個人情報の使用リスク3 リスクに対する措置の内容</p>		<p>-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。 -附票連携システムの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、業務上必要のない附票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、「注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。 -システム管理規程、システムセキュリティ基本方針等を策定する。 -違反行為を行った場合は、法令の前則規定により措置を講じる。</p>	事前	重要な変更となるため事前に報告
	<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)3. 特定個人情報の使用リスク3 リスクへの対策は十分か</p>		[ 十分である ]	事前	重要な変更となるため事前に報告
	<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)3. 特定個人情報の使用リスク4 リスクに対する措置の内容</p>		<p>-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、法令の前則規定により措置を講じる。</p>	事前	重要な変更となるため事前に報告
	<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)3. 特定個人情報の使用リスク4 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</p>		[ 十分である ]	事前	重要な変更となるため事前に報告
	<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)3. 特定個人情報の使用リスク4 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</p>		<p>附票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、長時間にわたり附票本人確認情報を表示させない。 -附票都道府県サーバの代表端末を施設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シートを貼付するとともに、来庁者から見えにくい位置に設置する。 -システム操作者は附票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。 -附票本人確認情報の開示・訂正の請求に対し、適切に対応する。 -附票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。</p>	事前	重要な変更となるため事前に報告

<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)4. 特定個人情報ファイルの取扱いの委託 情報保護管理体制の確認</p>		<p>①附票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の前身である財団法人地方自治情報センターへ委託することを議決している。 委託先である機構は、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、住基法に基づき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業務がある。 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。</p> <p>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、委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、遵守することを義務づける。 委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。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)4. 特定個人情報ファイルの取扱いの委託 特定個人情報ファイルの閲覧者・更新者の制限</p>		<p>[制限している]</p> <p>委託業務に従事する者に都道府県知事附票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。</p> <p>①附票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、附票本人確認情報の更新及び附票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は想定されるが、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。</p> <p>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。 システムの稼働履歴(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。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)4. 特定個人情報ファイルの取扱いの委託 特定個人情報ファイルの取扱いの記録</p>		<p>[記録を残している]</p> <p>①附票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、附票本人確認情報の更新及び附票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は想定されるが、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。また、管理簿に理由を明記し、媒体は引き継ぎデータ保管庫に格納することとしているが、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。 委託契約の報告事項に基づき、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。</p> <p>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、直接附票本人確認情報に依存しない(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、委託者から業務報告書の提出を受ける。また、必要に応じて、委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。 システムの稼働履歴(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。 システムの稼働履歴については7年間、安全な場所に施設保管する。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)4. 特定個人情報ファイルの取扱いの委託 特定個人情報の提供ルール</p>		<p>[定めている]</p> <p>①附票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。)は、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、媒体は引き継ぎデータ保管庫に格納することとしているが、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。 委託契約の報告事項に基づき、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。</p> <p>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、附票本人確認情報に直接依存しない(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、委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。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)4. 特定個人情報ファイルの取扱いの委託 特定個人情報の消去ルール</p>		<p>[定めている]</p> <p>①附票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。)は、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、媒体は引き継ぎデータ保管庫に格納することとしているが、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。 委託契約の報告事項に基づき、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。</p> <p>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、附票本人確認情報に直接依存しない(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、委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。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>

<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)4. 特定個人情報ファイルの取扱いの委託 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</p>		<p>[定めている]</p> <p>①附票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 ・再委託における義務 ・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、当票と同様の安全管理措置を義務付ける。</p> <p>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保護の保護(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)</p> <p>【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)</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)4. 特定個人情報ファイルの取扱いの委託 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</p>		<p>[十分にしている]</p> <p>①附票都道府県サーバの運用及び監視に関する業務 ・委託先である組織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、直接附票本人確認情報に依らない(直接附票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。 ・委託先は、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、委託先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。</p> <p>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、附票本人確認情報に直接関わらない(附票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。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)4. 特定個人情報ファイルの取扱いの委託 リスクへの対策は十分か</p>		<p>[十分である]</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)4. 特定個人情報ファイルの取扱いの委託 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リスクに対する措置</p>		<p>再委託については、毎年度の契約において、再委託先業者の業務内容や委託先との業務分担を審査した上で承認を行っているほか、随時業務状況を確認する。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)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。)リスク 特定個人情報の提供・移転の記録</p>		<p>[記録を残している]</p> <p>・都道府県知事保存附票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。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)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。)リスク 特定個人情報の提供・移転に関するルール</p>		<p>[定めている]</p> <p>・都道府県知事保存附票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。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)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。)リスク その他の措置の内容</p>		<p>「サーバ室等への入室権限」及び「操作権限」を有する者を厳格に管理し、情報の持ち出しを制限する。記録を用いて情報を連携する場合には、媒内へのデータ出力(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。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)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。)リスク リスクへの対策は十分か</p>		<p>[十分である]</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)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。)リスク リスクに対する措置の内容</p>		<p>連携手段として通信の記録が同一保存され、また、連携するデータが暗号化される仕組みが確立した附票連携システムを用いることにより、不適切な方法による特定個人情報の提供を防止する。 附票全国サーバと附票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で担保される。 また、票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。 また、附票都道府県サーバの代表端末または業務端末(都道府県サーバ)に実装する。と変更し、専用装置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。</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)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。)リスク リスクへの対策は十分か</p>		<p>[十分である]</p>	<p>事前</p>	<p>重要な変更となるため事前に報告</p>

<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)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。)リスク リスクに対する措置の内容</p>		<p>《新たな情報を提供・移転してしまいうりリスクへの措置》 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。</p> <p>《新たな相手に提供・移転してしまいうりリスクへの措置》 附票全国サーバと附票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で担保される。 附票都道府県サーバの代表端末または業務端末(都道府県サーバと共用する。)と受渡し専用フォルダ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。</p>	事前	重要な変更となるため事前に報告
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)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。)リスク リスクへの対策は十分か</p>		[ 十分である ]	事前	重要な変更となるため事前に報告
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)6. 情報提供ネットワークシステムとの接続</p>		[ <input type="checkbox"/> 接続しない(入手) <input type="checkbox"/> 接続しない(提供) ]	事前	重要な変更となるため事前に報告
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)7. 特定個人情報の保管・消去 リスク1③NISC 政府機関統一基準群</p>		[ 政府機関ではない ]	事前	重要な変更となるため事前に報告
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)7. 特定個人情報の保管・消去 リスク1②安全 管理体制</p>		[ 十分に整備している ]	事前	重要な変更となるため事前に報告
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)7. 特定個人情報の保管・消去 リスク1③安全 管理規程</p>		[ 十分に整備している ]	事前	重要な変更となるため事前に報告
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)7. 特定個人情報の保管・消去 リスク1④安全 管理体制・規程の権限への周知</p>		[ 十分に周知している ]	事前	重要な変更となるため事前に報告
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)7. 特定個人情報の保管・消去 リスク1⑤物理 的対策</p>		<p>[ 十分に行っている ]</p> <p>附票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。 附票都道府県サーバの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設管理する。 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設管理する。 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み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。</p>	事前	重要な変更となるため事前に報告
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)7. 特定個人情報の保管・消去 リスク1⑥技術 的支援</p>		<p>[ 十分に行っている ]</p> <p>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バージョン更新を随時行う。 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。</p>	事前	重要な変更となるため事前に報告
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)7. 特定個人情報の保管・消去 リスク1⑦バック アップ</p>		[ 十分に行っている ]	事前	重要な変更となるため事前に報告
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)7. 特定個人情報の保管・消去 リスク1⑧事故 発生時手順の策定・周知</p>		[ 十分に行っている ]	事前	重要な変更となるため事前に報告
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)7. 特定個人情報の保管・消去 リスク1⑨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</p>		[ 発生なし ]	事前	重要な変更となるため事前に報告
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)7. 特定個人情報の保管・消去 リスク1⑩死者 の個人番号</p>		[ 保管していない ]	事前	重要な変更となるため事前に報告
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)7. 特定個人情報の保管・消去 リスク1 リスクへの対策は十分か</p>		[ 十分である ]	事前	重要な変更となるため事前に報告
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)7. 特定個人情報の保管・消去 リスク2 リスクに対する措置の内容</p>		附票本人確認情報の提供・移転に併せて提供される個人番号は、県の他の執行機関又は他部署等からの求めにより提供・移転された後は、障害発生等により提供・移転先で情報を乗替できない場合に併せて一時的に保存がされるのみであり、情報が更新される必要はない。	事前	重要な変更となるため事前に報告

<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)7. 特定個人情報の保管・消去 リスク2 リスクへの対策は十分か</p>	<p>—</p>	<p>[ 十分である ]</p>	<p>事前 重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)7. 特定個人情報の保管・消去 リスク3 消去手順</p>	<p>—</p>	<p>[ 定めている ]</p> <p>・障害発生等により提供・移転先で情報を受領できなかった場合に備えた一時的な保存の終了後、特定個人情報を、システムにて自動判別し消去する(消去されたデータは、復元できない)。 ・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、その記録を抹す。また、廃棄を外都委託する場合は、委託者に廃棄証明書の提出を義務づける。 ・廃票の廃棄時には、裁断または溶解等を行うとともに、その記録を抹す。</p>	<p>事前 重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県知事保存附票本人確認情報ファイル)7. 特定個人情報の保管・消去 リスク4 消去手順</p>	<p>—</p>	<p>[ 定めている ]</p> <p>・障害発生等により提供・移転先で情報を受領できなかった場合に備えた一時的な保存の終了後、特定個人情報を、システムにて自動判別し消去する(消去されたデータは、復元できない)。 ・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、その記録を抹す。また、廃棄を外都委託する場合は、委託者に廃棄証明書の提出を義務づける。 ・廃票の廃棄時には、裁断または溶解等を行うとともに、その記録を抹す。</p>	<p>事前 重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 2. 特定個人情報の入手(情報提供ネットワークを適した入手を除く) リスク4 リスクに対する措置の内容</p>	<p>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から受渡。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。</p>	<p>住民基本台帳ネットワークシステム及び附票連携システムの業務端末又は代表端末から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。</p>	<p>事前 重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (符号取得要求ファイル) 3. 特定個人情報の使用リスク2 ユーザ認証の管理</p>	<p>[ 行っている ]</p> <p>&lt;住民基本台帳ネットワークシステムにおける措置&gt; ・操作者照会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、操作者照会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。 &lt;団体内統合宛名システムにおける措置&gt; ・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。</p>	<p>[ 行っている ]</p> <p>&lt;住民基本台帳ネットワークシステム及び附票連携システムにおける措置&gt; ・符号取得要求ファイルの受け渡しを行う受渡し専用装置へのアクセスは、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会ID及び照会情報(静脈による生体認証)による操作者認証を行う。 &lt;団体内統合宛名システムにおける措置&gt; ・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。</p>	<p>事前 重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (符号取得要求ファイル) 3. 特定個人情報の使用リスク2 アクセス権限の発効・失効の管理</p>	<p>[ 行っている ]</p> <p>&lt;住民基本台帳ネットワークシステムにおける措置&gt; ・操作者照会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、操作者照会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。 &lt;団体内統合宛名システムにおける措置&gt; ・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。</p>	<p>[ 行っている ]</p> <p>&lt;住民基本台帳ネットワークシステム及び附票連携システムにおける措置&gt; ・操作者照会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、操作者照会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。 &lt;団体内統合宛名システムにおける措置&gt; ・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。</p>	<p>事前 重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (符号取得要求ファイル)3. 特定個人情報の使用リスク2 アクセス権限の管理</p>	<p>[ 行っている ]</p> <p>&lt;住民基本台帳ネットワークシステムにおける措置&gt; ・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。 &lt;団体内統合宛名システムにおける措置&gt; ・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。</p>	<p>[ 行っている ]</p> <p>&lt;住民基本台帳ネットワークシステム及び附票連携システムにおける措置&gt; ・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。 &lt;団体内統合宛名システムにおける措置&gt; ・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。</p>	<p>事前 重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (符号取得要求ファイル)3. 特定個人情報の使用リスク3 特定個人情報の使用リスク3 リスクに対する措置の内容</p>	<p>&lt;住民基本台帳ネットワークシステムにおける措置&gt; ・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、「住民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利用者等が定める事項」「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。 &lt;団体内統合宛名システムにおける措置&gt; ・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、上記と同様の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。</p>	<p>&lt;住民基本台帳ネットワークシステム及び附票連携システムにおける措置&gt; ・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及び附票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、「住民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。 ・システム管理規程、システムセキュリティ基本方針書等を策定する。 ・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。 &lt;団体内統合宛名システムにおける措置&gt; ・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、上記と同様の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。</p>	<p>事前 重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (符号取得要求ファイル)3. 特定個人情報の使用リスク4 リスクに対する措置の内容</p>	<p>&lt;住民基本台帳ネットワークシステムにおける措置&gt; ・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。 &lt;団体内統合宛名システムにおける措置&gt; ・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。</p>	<p>&lt;住民基本台帳ネットワークシステム及び附票連携システムにおける措置&gt; ・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。 &lt;団体内統合宛名システムにおける措置&gt; ・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。</p>	<p>事前 重要な変更となるため事前に報告</p>

<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (符号取得要求ファイル) 3. 特定個人情報の使用リスク 4. 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</p>	<p>本人確認情報の利用にあたり、以下の措置を講じる。 &lt;住民基本台帳ネットワークシステムにおける措置&gt; ・スクリーンセーブ等を利用して、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設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れない。 ・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。  &lt;団体内統合宛名システムにおける措置&gt; ・スクリーンセーブ等を利用して、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。</p>	<p>本人確認情報及び附票本人確認情報の利用にあたり、以下の措置を講じる。 &lt;住民基本台帳ネットワークシステム及び附票連携システムにおける措置&gt; ・スクリーンセーブ等を利用して、長時間にわたり本人確認情報を表示させない。 ・都道府県サーバ及び附票都道府県サーバの代表端末を施設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れない。 ・本人確認情報及び附票本人確認情報の開示・訂正の請求に対し、適切に対応する。 ・本人確認情報及び附票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。  &lt;団体内統合宛名システムにおける措置&gt; ・スクリーンセーブ等を利用して、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。</p>	<p>事前</p> <p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (符号取得要求ファイル) 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。)リスク 1. 特定個人情報の提供・移転に関するルール</p>	<p>[ 定めている ]</p> <p>・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。 ・システムデータの操作履歴(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。</p>	<p>[ 定めている ]</p> <p>・都道府県知事保存本人確認情報及び都道府県知事保存附票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。 ・システムデータの操作履歴(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。</p>	<p>事前</p> <p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (符号取得要求ファイル) 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。)リスク 2. 特定個人情報の提供・移転に関する措置の内容</p>	<p>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確保される。 また、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。 また、都道府県サーバの代表端末または業務端末と受渡し専用装置の接続はファイアウォールを経由することとし、必要な通信以外を行えないように制限する。</p>	<p>全国サーバと都道府県サーバの間の通信及び附票全国サーバと附票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。 また、都道府県サーバ及び附票都道府県サーバの代表端末または業務端末と受渡し専用装置の接続はファイアウォールを経由することとし、必要な通信以外を行えないように制限する。</p>	<p>事前</p> <p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (符号取得要求ファイル) 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。)リスク 3. リスクに対する措置の内容</p>	<p>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、人的な編集作業は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。</p>	<p>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、人的な編集作業は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。</p>	<p>事前</p> <p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (符号取得要求ファイル) 7. 特定個人情報の保管・消去 リスク1⑤ 物理的対策</p>	<p>[ 十分に行っている ]</p> <p>&lt;住民基本台帳ネットワークシステムにおける措置&gt; ・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設管理する。 ・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室管理設備を設置し、代表端末設置場所への入室者を特定・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設管理する。 ・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み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。  &lt;団体内統合宛名システムにおける措置&gt; ・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室管理、監視及び施設管理する。</p>	<p>[十分に行っている]</p> <p>&lt;住民基本台帳ネットワークシステム及び附票連携システムにおける措置&gt; ・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設管理する。 ・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室管理設備を設置し、代表端末設置場所への入室者を特定・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設管理する。 ・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み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。  &lt;団体内統合宛名システムにおける措置&gt; ・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室管理、監視及び施設管理する。</p>	<p>事前</p> <p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (符号取得要求ファイル) 7. 特定個人情報の保管・消去 リスク1⑥ 技術的対策</p>	<p>[ 十分に行っている ]</p> <p>&lt;住民基本台帳ネットワークシステムにおける措置&gt; ・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、住基ネットワーク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なバージョン更新を随時行う。 ・府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。  &lt;団体内統合宛名システムにおける措置&gt; ・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。 ・コンピュータウイ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。</p>	<p>[ 十分に行っている ]</p> <p>&lt;住民基本台帳ネットワークシステム及び附票連携システムにおける措置&gt; ・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、住基ネットワーク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なバージョン更新を随時行う。 ・府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。  &lt;団体内統合宛名システムにおける措置&gt; ・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。 ・コンピュータウイ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。</p>	<p>事前</p> <p>重要な変更となるため事前に報告</p>
<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (符号取得要求ファイル) 7. 特定個人情報の保管・消去 リスク1 リスクへの対策は十分が⑤物理的対策</p>	<p>[ 十分に行っている ]</p> <p>&lt;住民基本台帳ネットワークシステムにおける措置&gt; ・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設管理する。 ・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室管理設備を設置し、代表端末設置場所への入室者を特定・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設管理する。 ・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み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。  &lt;団体内統合宛名システムにおける措置&gt; ・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室管理、監視及び施設管理する。</p>	<p>[十分に行っている]</p> <p>&lt;住民基本台帳ネットワークシステム及び附票連携システムにおける措置&gt; ・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設管理する。 ・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室管理設備を設置し、代表端末設置場所への入室者を特定・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設管理する。 ・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み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。  &lt;団体内統合宛名システムにおける措置&gt; ・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室管理、監視及び施設管理する。</p>	<p>事前</p> <p>重要な変更となるため事前に報告</p>

	<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (符号取得要求ファイル) 7. 特定個人情報の保管・消去リスク1 リスクへの対策は十分に</p>	<p>[ 十分に行っている ]</p> <p>&lt;住民基本台帳ネットワークシステムにおける措置&gt;</p> <ul style="list-style-type: none"> <li>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、ウイルス対策ソフトの定期的バージョン更新を随時行う。</li> <li>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。</li> <li>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。</li> </ul> <p>&lt;団体内統合宛名システムにおける措置&gt;</p> <ul style="list-style-type: none"> <li>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。</li> <li>コンピュータウイルス対策ソフトウェアを導入する。</li> <li>OSには随時パッチ適用を実施する。</li> </ul>	<p>[ 十分に行っている ]</p> <p>&lt;住民基本台帳ネットワークシステム及び附属連携システムにおける措置&gt;</p> <ul style="list-style-type: none"> <li>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、ウイルス対策ソフトの定期的バージョン更新を随時行う。</li> <li>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。</li> <li>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。</li> </ul> <p>&lt;団体内統合宛名システムにおける措置&gt;</p> <ul style="list-style-type: none"> <li>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。</li> <li>コンピュータウイルス対策ソフトウェアを導入する。</li> <li>OSには随時パッチ適用を実施する。</li> </ul>	事前	重要な変更となるため事前に報告
	<p>Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 (都道府県移転保存附票本人確認情報ファイル) 7. 特定個人情報の保管・消去 リスク2 リスクに対する措置の内容</p>	<p>・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。</p> <p>&lt;団体内統合宛名システムにおける措置&gt;</p> <ul style="list-style-type: none"> <li>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。</li> </ul>	<p>・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。</p> <p>&lt;団体内統合宛名システムにおける措置&gt;</p> <ul style="list-style-type: none"> <li>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。</li> </ul>	事前	重要な変更となるため事前に報告
	<p>Ⅳ その他のリスク対策 1. 自己点検</p>	<p>[ 十分に行っている ]</p> <p>&lt;住民基本台帳ネットワークシステムにおける措置&gt;</p> <p>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。</p> <p>&lt;団体内統合宛名システムにおける措置&gt;</p> <p>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。</p>	<p>[ 十分に行っている ]</p> <p>&lt;住民基本台帳ネットワークシステム及び附属連携システムにおける措置&gt;</p> <p>機構(住民基本台帳ネットワークシステム全国センター)及び附属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。</p> <p>&lt;団体内統合宛名システムにおける措置&gt;</p> <p>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。</p>	事前	重要な変更となるため事前に報告
	<p>Ⅳ その他のリスク対策 1. 監査 ② 監査</p>	<p>[ 十分に行っている ]</p> <p>&lt;住民基本台帳ネットワークシステムにおける措置&gt;</p> <ul style="list-style-type: none"> <li>住民基本台帳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。</li> <li>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屬に対して、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職員が、システム利用部署(庶務事務所・建築安全推進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。)</li> <li>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。</li> </ul> <p>&lt;団体内統合宛名システムにおける措置&gt;</p> <p>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。</p>	<p>[ 十分に行っている ]</p> <p>&lt;住民基本台帳ネットワークシステム及び附属連携システムにおける措置&gt;</p> <ul style="list-style-type: none"> <li>住民基本台帳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。</li> <li>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屬に対して、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職員が、システム利用部署(庶務事務所・建築安全推進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。)</li> <li>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。</li> </ul> <p>&lt;団体内統合宛名システムにおける措置&gt;</p> <p>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。</p>	事前	重要な変更となるため事前に報告
	<p>Ⅳ その他のリスク対策 2. 従業者に対する教育・啓発</p>	<p>[ 十分に行っている ]</p> <p>&lt;住民基本台帳ネットワークシステムにおける措置&gt;</p> <ul style="list-style-type: none"> <li>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。</li> <li>「住民基本台帳業務引継書」を作成のうえ組織として記録を管理することにより、引継事項の周知徹底に努める。</li> <li>年1回、機構が実施するトレ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。</li> </ul> <p>&lt;団体内統合宛名システムにおける措置&gt;</p> <ul style="list-style-type: none"> <li>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。</li> <li>委託業者に対しては、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。</li> <li>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。</li> <li>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。</li> </ul>	<p>[ 十分に行っている ]</p> <p>&lt;住民基本台帳ネットワークシステム及び附属連携システムにおける措置&gt;</p> <ul style="list-style-type: none"> <li>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。</li> <li>「住民基本台帳業務引継書」を作成のうえ組織として記録を管理することにより、引継事項の周知徹底に努める。</li> <li>年1回、機構が実施するトレ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。</li> </ul> <p>&lt;団体内統合宛名システムにおける措置&gt;</p> <ul style="list-style-type: none"> <li>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。</li> <li>委託業者に対しては、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。</li> <li>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。</li> <li>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。</li> </ul>	事前	重要な変更となるため事前に報告