

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
16	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

埼玉県は、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、適切な措置を講じ、もって個人のプライバシー等の権利利益の保護に取り組んでいることを宣言する。

特記事項

住民基本台帳ネットワークに関する事務では、事務の一部を外部業者に委託するが、委託する業務は、都道府県サーバの運用及び監視に関する業務とし、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。

評価実施機関名

埼玉県知事

個人情報保護委員会 承認日【行政機関等のみ】

公表日

令和5年12月28日

項目一覧

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

I 基本情報

1. 特定個人情報ファイルを取り扱う事務

①事務の名称	住民基本台帳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 県は、住民基本台帳法(以下「住基法」という。)に基づき、住民基本台帳のネットワーク化を図り、全国共通の本人確認システム(住基ネット)を市町村と共同で構築している。</p> <p>住民基本台帳は、住基法に基づき作成され、住民に関する記録を正確かつ統一的行う制度であり、住民の利便を増進するとともに、行政の合理化に資することを目的としている。</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地方公共団体情報システム機構(以下「機構」という。)への通知 ③埼玉県知事から本人確認情報に係る埼玉県の他の執行機関への提供又は他部署への移転 ④住民からの請求に基づく当該個人の本人確認情報の開示及び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(コミュニケーションサーバ)、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。以下「4情報」という。)、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埼玉県知事から附票本人確認情報に係る埼玉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><選択肢> 1) 1,000人未満 2) 1,000人以上1万人未満 3) 1万人以上10万人未満 4) 10万人以上30万人未満 5) 30万人以上</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	住民基本台帳ネットワークシステム(以下「住基ネット」という。) ※「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、住基ネットの構成要素のうち、都道府県サーバで管理されているため、以降は、住基ネットのうち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. 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、住基ネットの市町村CS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. 埼玉県他の執行機関への情報提供又は他部署への移転 埼玉県他の執行機関又は他部署による住基法に基づく情報照会に対応するため、照会のあった当該個人の個人番号又は4情報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> <p>3. 本人確認情報の開示 法律に基づく住民による自己の本人確認情報の開示請求に対応するため、当該個人の本人確認情報を都道府県知事保存本人確認情報ファイルから抽出し、帳票に出力する。</p> <p>4. 機構への情報照会 全国サーバに対して住民票コード、個人番号又は4情報の組合せをキーとした本人確認情報照会要求を行い、該当する個人の本人確認情報を受領する。</p> <p>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。</p> <p>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。</p>
----------	---

③他のシステムとの接続	<table style="width: 100%; border: none;"> <tr> <td style="width: 50%; border: none;">[] 情報提供ネットワークシステム</td> <td style="width: 50%; border: none;">[] 庁内連携システム</td> </tr> <tr> <td style="border: none;">[] 住民基本台帳ネットワークシステム</td> <td style="border: none;">[] 既存住民基本台帳システム</td> </tr> <tr> <td style="border: none;">[] 宛名システム等</td> <td style="border: none;">[] 税務システム</td> </tr> <tr> <td style="border: none;">[] その他 (</td> <td style="border: none;">)</td> </tr> </table>	[] 情報提供ネットワークシステム	[] 庁内連携システム	[] 住民基本台帳ネットワークシステム	[] 既存住民基本台帳システム	[] 宛名システム等	[] 税務システム	[] その他 ()
[] 情報提供ネットワークシステム	[] 庁内連携システム								
[] 住民基本台帳ネットワークシステム	[] 既存住民基本台帳システム								
[] 宛名システム等	[] 税務システム								
[] その他 ()								

システム2～5

システム2									
①システムの名称	<p>附票連携システム</p> <p>※「3. 特定個人情報ファイル名」に示す「都道府県知事保存附票本人確認情報ファイル」は、住基ネットの構成要素のうち、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、附票連携システム内の附票都道府県サーバ部分について記載する。</p>								
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を經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. 埼玉県他の執行機関への情報提供又は他部署への移転 埼玉県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情報等に対応する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、埼玉県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>								
③他のシステムとの接続	<table border="0"> <tr> <td>[] 情報提供ネットワークシステム</td> <td>[] 庁内連携システム</td> </tr> <tr> <td>[] 住民基本台帳ネットワークシステム</td> <td>[] 既存住民基本台帳システム</td> </tr> <tr> <td>[] 宛名システム等</td> <td>[] 税務システム</td> </tr> <tr> <td>[] その他 (</td> <td>)</td> </tr> </table>	[] 情報提供ネットワークシステム	[] 庁内連携システム	[] 住民基本台帳ネットワークシステム	[] 既存住民基本台帳システム	[] 宛名システム等	[] 税務システム	[] その他 ()
[] 情報提供ネットワークシステム	[] 庁内連携システム								
[] 住民基本台帳ネットワークシステム	[] 既存住民基本台帳システム								
[] 宛名システム等	[] 税務システム								
[] その他 ()								
システム6～10									
システム11～15									
システム16～20									

3. 特定個人情報ファイル名

- (1)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

4. 特定個人情報ファイルを取り扱う理由

<p>①事務実施上の必要性</p>	<p>(1)都道府県知事保存本人確認情報ファイル 県では、都道府県知事保存本人確認情報ファイルを、下記に記載のと通りの必要性から取り扱う。</p> <p>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> <ul style="list-style-type: none">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(住基ネットに係る本人確認情報の管理及び提供等に関する事務)の処理を行うため、区域内の住民に係る最新の本人確認情報を管理する。②市町村からの本人確認情報の更新情報の通知を受けて都道府県知事保存本人確認情報ファイルを更新し、当該更新情報を機構に対して通知する。③埼玉県以外の執行機関又は他部署からの照会に基づき、本人確認情報を提供・移転する。④住民からの請求に基づき、当該個人の本人確認情報を開示する。⑤住基ネットに係る本人確認情報の管理及び提供等に関する事務において、本人確認情報を検索する。⑥市町村において保存する本人確認情報との整合性を確認する。 <p>(2)都道府県知事保存附票本人確認情報ファイル 県では、都道府県知事保存附票本人確認情報ファイルを、下記に記載の通りの必要性から取り扱う。</p> <p>・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> <ul style="list-style-type: none">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埼玉県以外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、埼玉県以外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>②実現が期待されるメリット</p>	<p>住民票の写し等にかえて本人確認情報を利用することにより、添付書類の省略が図られ、住民の負担軽減(各行政機関を訪問し、書類を入手する金銭的、時間的コストの節約)及び行政の合理化につながる。</p> <p>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>

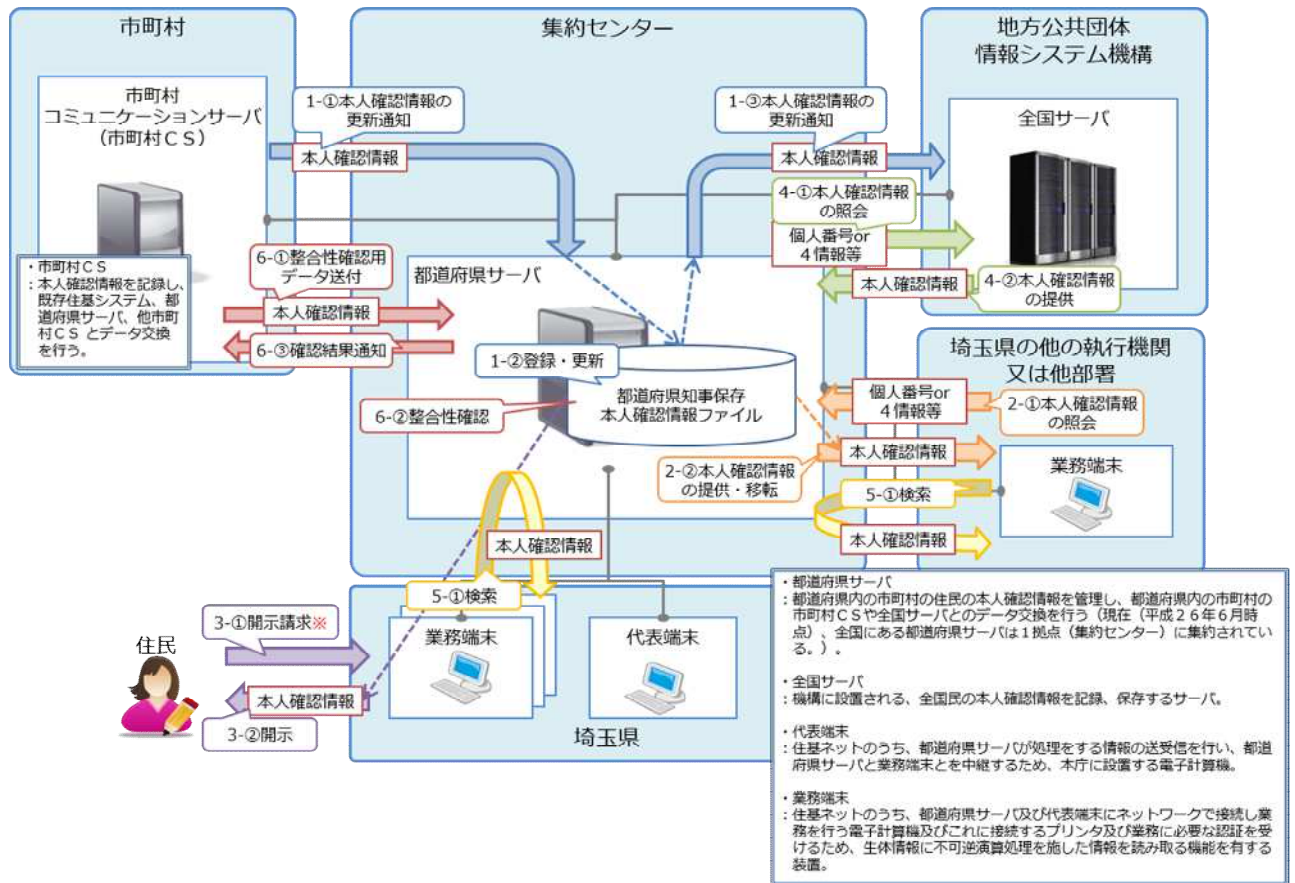
5. 個人番号の利用 ※

<p>法令上の根拠</p>	<p>住民基本台帳法(住基法)(昭和42年7月25日法律第81号)</p> <ul style="list-style-type: none">・第7条(住民票の記載事項)・第12条の5(住民基本台帳の脱漏等に関する都道府県知事の通報)・第30条の6(市町村長から都道府県知事への本人確認情報の通知等)・第30条の7(都道府県知事から機構への本人確認情報の通知等)・第30条の8(本人確認情報の誤りに関する機構の通報)・第30条の11(通知都道府県以外の都道府県の執行機関への本人確認情報の提供)・第30条の13(都道府県の条例による本人確認情報の提供)・第30条の15(本人確認情報の利用)・第30条の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(都道府県知事保存附票本人確認情報(住民票コードに限る。)の利用)
---------------	---

6. 情報提供ネットワークシステムによる情報連携 ※	
①実施の有無	[実施しない]
②法令上の根拠	—
<p style="text-align: right;"> <選択肢> 1) 実施する 2) 実施しない 3) 未定 </p>	
7. 評価実施機関における担当部署	
①部署	企画財政部 情報システム戦略課
②所属長の役職名	課長
8. 他の評価実施機関	
—	

(別添1) 事務の内容

(1) 本人確認情報の管理及び提供に関する事務



(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、住基ネットを介して、本人確認情報の更新を通知する。

2. 埼玉県の他の執行機関への情報提供又は他部署への移転

- 2-①.埼玉県の他の執行機関又は他部署において、個人番号又は4情報等をキーワードとした本人確認情報の照会を行う。
- 2-②.埼玉県知事において、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。
※埼玉県の他の執行機関又は他部署に対し、住基ネット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、埼玉県の他の執行機関又は他部署において、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)により行う。
(注1)埼玉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。

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. 機構への情報照会に係る事務

- 4-①.機構に対し、個人番号又は4情報等をキーワードとした本人確認情報の照会を行う。
- 4-②.機構より、当該個人の本人確認情報を受領する。

5. 本人確認情報検索に関する事務

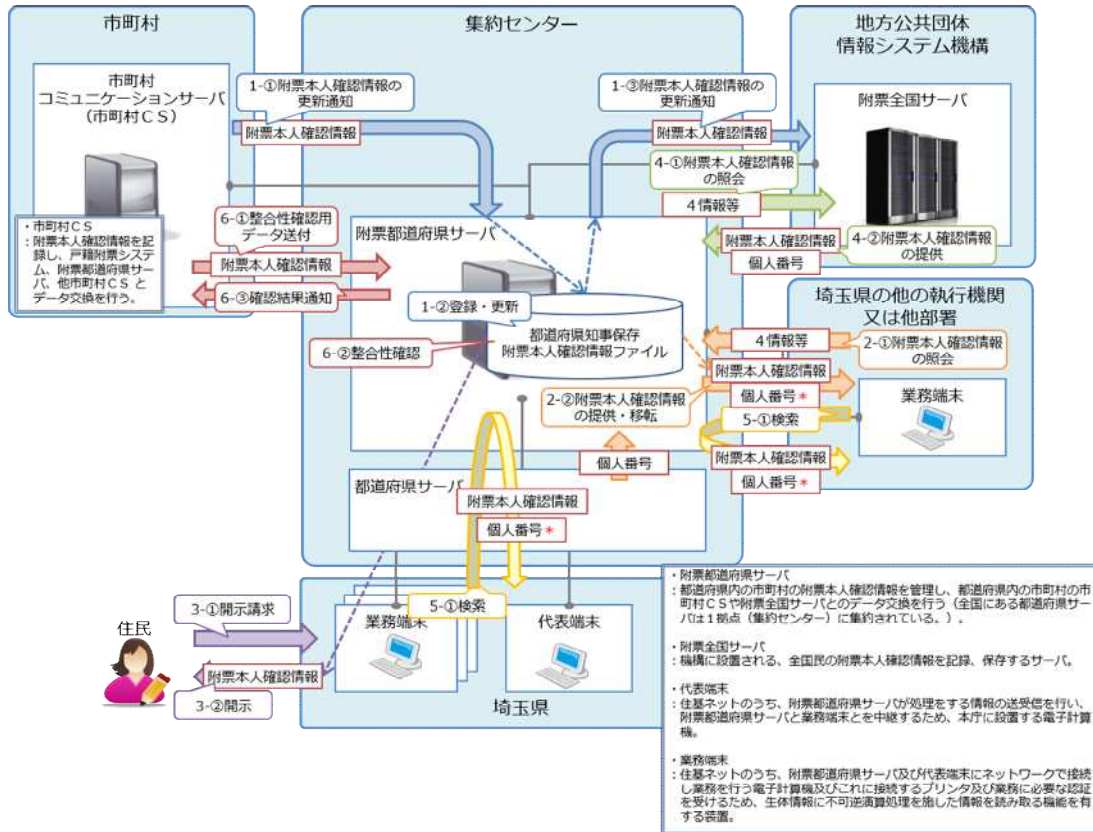
- 5-①.4情報の組み合わせを検索キーに、都道府県知事保存本人確認情報ファイルを検索する。

6. 本人確認情報整合

- 6-①.市町村CSより、都道府県サーバに対し、整合性確認用の本人確認情報を送付する。
- 6-②.都道府県サーバにおいて、市町村CSより受領した整合性確認用の本人確認情報を用いて都道府県知事保存本人確認情報ファイルの整合性確認を行う。
- 6-③.都道府県サーバより、市町村CSに対して整合性確認結果を通知する。

(別添1) 事務の内容

(2) 附票本人確認情報の管理及び提供等に関する事務



(備考)

- 附票本人確認情報の更新に関する事務
 - 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を通じて附票都道府県サーバに通知する。
 - 附票都道府県サーバにおいて、市町村より受領した附票本人確認情報を元に都道府県知事保存附票本人確認情報ファイルを更新する。
 - 機構に対し、住民基本台帳ネットワークを介して、附票本人確認情報の更新を通知する。
- 埼玉県の他の執行機関への情報提供又は他部署への移転
 - 埼玉県の他の執行機関又は他部署において、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。
 - 埼玉県知事において、提示されたキーワードを元に都道府県知事保存附票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、埼玉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。

※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。
 ※埼玉県の他の執行機関又は他部署に対し、附票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、埼玉県の他の執行機関又は他部署において、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用する。)を操作し、媒体連携(注2)により行う。
 (注1) 埼玉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。
- 附票本人確認情報の開示に関する事務
 - 住民より附票本人確認情報の開示請求を受け付ける。
 - 開示請求者(住民)に対し、都道府県知事保存附票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。
- 機構への情報照会に係る事務
 - 機構に対し、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。
 - 機構より、当該個人の附票本人確認情報を受領する。
- 附票本人確認情報検索に関する事務
 - 4情報の組み合わせを検索キーに、都道府県知事保存附票本人確認情報ファイルを検索する。
- 附票本人確認情報整合
 - 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。
 - 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。
 - 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。

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	住基ネットを通じて全国共通の本人確認を行うため、本特定個人情報ファイル(都道府県知事保存本人確認情報ファイル)において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 ※	<ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・個人番号、4情報、その他住民票関係情報 住基ネットを通じて本人確認を行うために必要な情報として、住民票の記載等に係る本人確認情報(個人番号、4情報、住民票コード及びこれらの変更情報)を記録する必要がある。
全ての記録項目	別添2を参照。
⑤保有開始日	平成27年6月
⑥事務担当部署	企画財政部 情報システム戦略課

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、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(市町村長から都道府県知事への本人確認情報の通知等)、第30条の7(都道府県知事から機構への本人確認情報の通知等)により、住民に関する情報に変更があった又は新規作成された際は、市町村から都道府県へ、都道府県から機構へと通知することとされている。	
⑤本人への明示	都道府県知事が当該市町村の区域内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)で明示されている。	
⑥使用目的 ※	住基ネットを通じて全国共通の本人確認を行うため、本特定個人情報ファイル(都道府県知事保存本人確認情報ファイル)において区域内のすべての住民の情報を保有し、住民票に記載されている住民全員の記録を常に正確に更新・管理・提供する。	
	変更の妥当性 ー	
⑦使用の主体	使用部署 ※	企画財政部 情報システム戦略課
	使用者数	[10人未満] <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上
⑧使用方法 ※	<ul style="list-style-type: none"> ・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)。 ・埼玉県他の執行機関又は他部署からの本人確認情報の照会要求を受け(埼玉県の他の執行機関又は他部署→都道府県サーバ)、照会のあった住民票コード、個人番号又は4情報の組合せを元に都道府県知事保存本人確認情報ファイルを検索し、該当する個人の本人確認情報を照会元へ提供・移転する(都道府県サーバ→埼玉県の他の執行機関又は他部署)。 ・住民からの開示請求に基づき(住民→都道府県窓口→都道府県サーバ)、当該住民の本人確認情報を都道府県知事保存本人確認情報ファイルから抽出し、書面により提供する(都道府県サーバ→帳票出力→住民)。 ・4情報の組合せをキーに都道府県知事保存本人確認情報ファイルの検索を行う。 ・都道府県知事保存本人確認情報ファイルの正確性を担保するため、市町村から本人確認情報を受領し(市町村CS→都道府県サーバ)、当該本人確認情報を用いて都道府県知事保存本人確認情報ファイルに記録された本人確認情報の整合性確認を行う。 	
	情報の突合 ※	<ul style="list-style-type: none"> ・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、住民票コードを基に突合する。 ・埼玉県の他の執行機関又は他部署からの照会に基づいて本人確認情報を提供・移転する際に、照会元から受信した対象者の4情報等との突合を行う。 ・請求に基づいて本人確認情報を開示する際に、開示請求者から受領した本人確認情報との突合を行う。 ・市町村CSとの整合処理を実施するため、4情報等との突合を行う。
	情報の統計分析 ※	住基法第30条の15第1項第4号(本人確認情報の利用)の規定に基づいて統計資料の作成を行う場合、情報の統計分析を行うことがある。また、本人確認情報の更新件数や提供件数等の集計を行う。
	権利利益に影響を与え得る決定 ※	該当なし
⑨使用開始日	平成27年6月1日	

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※	[委託する] <選択肢> 1) 委託する 2) 委託しない (1) 件	
委託事項1	都道府県サーバの運用及び監視に関する業務	
①委託内容	全国の都道府県サーバを1拠点(集約センター)に集約化したことに伴い、都道府県サーバの運用及び監視に関する業務を、集約センター運用者に委託する。 委託する業務は、直接本人確認情報に係わらない(直接本人確認情報にアクセスできず、閲覧・更新・削除等を行わない)業務を対象とする。	
②取扱いを委託する特定個人情報ファイルの範囲	[特定個人情報ファイルの全体] <選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部	
	対象となる本人の数 [100万人以上1,000万人未満] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上	
	対象となる本人の範囲 ※ 「2. ③対象となる本人の範囲」と同じ	
その妥当性	本特定個人情報ファイル(都道府県知事保存本人確認情報ファイル)が保存される都道府県サーバの運用及び監視業務を委託することによる。 なお、「①委託内容」のとおり、委託事項は、直接本人確認情報に係わらない事務を対象としているため、委託先においては、特定個人情報ファイルに記録された情報そのものを扱う事務は実施しない。	
③委託先における取扱者数	[10人未満] <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上	
④委託先への特定個人情報ファイルの提供方法	[<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	埼玉県企画財政部情報システム戦略課のホームページにて確認できる。	
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	書面による承諾。 なお、承諾に当たっては、再委託先がプライバシーマーク等を取得していることを確認する。
	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、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。
委託事項2～5		
委託事項6～10		
委託事項11～15		
委託事項16～20		

5. 特定個人情報の提供・移転(委託に伴うものを除く。)	
提供・移転の有無	[<input type="radio"/>] 提供を行っている (3) 件 [<input type="radio"/>] 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	都道府県知事から受領した本人確認情報を元に機構保存本人確認情報ファイルを更新する。
③提供する情報	住民票コード、氏名、生年月日、性別、住所、個人番号、異動事由、異動年月日
④提供する情報の対象となる本人の数	[100万人以上1,000万人未満] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤提供する情報の対象となる本人の範囲	「2. ③対象となる本人の範囲」と同じ
⑥提供方法	[] 情報提供ネットワークシステム [] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [] 紙 [<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	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の更新を行った都度、随時。
提供先2～5	
提供先2	埼玉県の他の執行機関(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)
②提供先における用途	住基法別表第6に掲げる、埼玉県の他の執行機関への情報提供が認められる事務(例:教育委員会における特別支援学校への就学のため必要な経費の支弁に関する事務等)の処理に用いる。
③提供する情報	住民票コード、氏名、生年月日、性別、住所、個人番号、異動事由、異動年月日 ※住民票コードについては、行政手続における特定の個人を識別するための番号の利用等に関する法律の施行に伴う関係法律の整備等に関する法律(平成25年5月31日法律第28号)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」と同じ
⑥提供方法	[] 情報提供ネットワークシステム [] 専用線 [] 電子メール [<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 [<input checked="" type="radio"/>] 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	埼玉県の他の執行機関からの情報照会の要求があった都度、随時。

提供先3	住基法上の住民
①法令上の根拠	住基法第30条の32(自己の本人確認情報の開示)
②提供先における用途	開示された情報を確認し、必要に応じてその内容の全部又は一部の訂正、追加又は削除の申出を行う。
③提供する情報	住民票コード、氏名、生年月日、性別、住所、個人番号、異動事由、異動年月日
④提供する情報の対象となる本人の数	[100万人以上1,000万人未満] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤提供する情報の対象となる本人の範囲	「2. ③対象となる本人の範囲」と同じ
⑥提供方法	[] 情報提供ネットワークシステム [] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [<input checked="" type="checkbox"/>] 紙 [] その他 ()
⑦時期・頻度	開示請求があった都度、随時。
提供先4	
提供先5	
提供先6～10	
提供先11～15	
提供先16～20	
移転先1	埼玉県その他の部署(税務局など)
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)
②移転先における用途	住基法別表第5に掲げる、都道府県知事において都道府県知事保存本人確認情報の利用が認められる事務(例:地方税の賦課徴収又は地方税に関する調査に関する事務等)の処理に用いる。
③移転する情報	住民票コード、氏名、生年月日、性別、住所、個人番号、異動事由、異動年月日 ※住民票コードについては、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」と同じ
⑥移転方法	[] 庁内連携システム [] 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 [<input checked="" type="checkbox"/>] 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	埼玉県その他の部署からの情報照会の要求があった都度、随時。
移転先2～5	
移転先6～10	
移転先11～15	
移転先16～20	

6. 特定個人情報の保管・消去		
①保管場所 ※		<ul style="list-style-type: none"> ・セキュリティゲートによって入退室管理をしている都道府県サーバの集約センターにおいては、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、端末及び記録媒体を施錠管理された部屋に保管する。
②保管期間	期間	<p style="text-align: center;"><選択肢></p> <div style="display: flex; justify-content: space-between;"> <div style="text-align: center;">[20年以上]</div> <div style="text-align: center;"> 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 </div> </div>
	その妥当性	<ul style="list-style-type: none"> ・住民票の記載の修正後の本人確認情報は、新たに記載の修正の通知を受けるまで保管する。 ・住民票の記載の修正前の本人確認情報(履歴情報)及び消除者の本人確認情報は、住基法施行令第30条の6(都道府県における本人確認情報の保存期間)に定める期間保管する。
③消去方法		都道府県知事保存本人確認情報ファイルに記録されたデータをシステムで自動判別し消去する。
7. 備考		
—		

II 特定個人情報ファイルの概要

1. 特定個人情報ファイル名	
(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 ※	区域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者 ※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)において区域内の戸籍の附票に記録された全ての者の情報を保有し、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"> ・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。))
その妥当性	<ul style="list-style-type: none"> ・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(本籍及び筆頭者の氏名)は含まない。 <ul style="list-style-type: none"> ・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、埼玉県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。
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	企画財政部 情報システム戦略課

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。 ※番号法別表に掲げる事務につき、埼玉県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>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)において区域内の戸籍の附票に記録された全ての者の情報を保有し、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、埼玉県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>企画財政部 情報システム戦略課</p>
	<p>使用者数</p> <p>[10人未満]</p> <p><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 ※		・埼玉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(埼玉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→埼玉県の他の執行機関又は他部署)。 ※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・移転する可能性がある。
	情報の突合 ※	・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。
	情報の統計分析 ※	該当なし。
	権利利益に影響を与え得る決定 ※	該当なし。
⑨使用開始日		「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。
4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※	[委託する]	<選択肢> 1) 委託する 2) 委託しない (1) 件
委託事項1	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、直接附票本人確認情報に係わらない(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。)業務を対象とする。	
②取扱いを委託する特定個人情報ファイルの範囲		<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	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)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、直接附票本人確認情報に係わらない事務を対象としているため、委託先においては、特定個人情報ファイルに記録された情報そのものを扱う事務は実施しない。
③委託先における取扱者数	[10人未満]	<選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上
④委託先への特定個人情報ファイルの提供方法	[<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	埼玉県企画財政部情報システム戦略課のホームページにて確認できる。	
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	書面による承諾。 なお、承諾に当たっては、再委託先がプライバシーマーク等を取得していることを確認する。	
	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、直接附票本人確認情報に係わらない(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。)業務を対象とする。	
委託事項2～5			
委託事項6～10			
委託事項11～15			
委託事項16～20			
5. 特定個人情報の提供・移転(委託に伴うものを除く。)			
提供・移転の有無	[<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 [] 行っていない		
提供先1	埼玉県以外の執行機関(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) 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	住基法別表第六に掲げる、埼玉県以外の執行機関への情報提供が認められる事務(例:教育委員会における特別支援学校への就学のため必要な経費の支弁に関する事務等)の処理に用いる。		
③提供する情報	住民票コード、氏名、住所、生年月日、性別、個人番号(番号法に基づく埼玉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	[] 情報提供ネットワークシステム [] 専用線 [] 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 [] 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	埼玉県の他の執行機関からの情報照会の要求があった都度、随時。		
提供先2～5			
提供先6～10			
提供先11～15			
提供先16～20			

移転先1	埼玉県への他の部署(税務局など)		
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) 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	住基法別表第五に掲げる、都道府県知事において都道府県知事保存附票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、住所、生年月日、性別、個人番号(番号法に基づく埼玉県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。		
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"/> 庁内連携システム <input type="checkbox"/> 電子メール <input type="checkbox"/> フラッシュメモリ <input type="checkbox"/> その他 (住民基本台帳ネットワークシステム)	<input type="checkbox"/> 専用線 <input checked="" type="checkbox"/> 電子記録媒体(フラッシュメモリを除く。) <input type="checkbox"/> 紙	
⑦時期・頻度	埼玉県の他の部署からの情報照会の要求があった都度、随時。		
移転先2～5			
移転先6～10			
移転先11～15			
移転先16～20			
6. 特定個人情報の保管・消去			
①保管場所 ※	・セキュリティゲートにて入退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、端末及び記録媒体を施錠管理された部屋に保管する。		
②保管期間	期間	[1年未満]	<選択肢> 1) 1年未満 2) 1年 3) 2年 4) 3年 5) 4年 6) 5年 7) 6年以上10年未満 8) 10年以上20年未満 9) 20年以上 10) 定められていない
	その妥当性	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、埼玉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。		
7. 備考			
—			

(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

1. 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、埼玉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。)

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1⑩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、システムの仕様によって市町村CSからの本人確認情報更新要求の際に通知される本人確認情報に限定される。この場合、市町村CSから対象者以外の情報が通知されてしまうことがリスクとして想定されるが、制度上、対象者の真正性の担保は市町村側の確認に委ねられるため、市町村において厳格な審査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、システム上で担保する。
その他の措置の内容	—
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2： 不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	本人確認情報の入手元をシステムの仕様により市町村CSに限定する。
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3： 入手した特定個人情報ที่ไม่正確であるリスク	
入手の際の本人確認の措置の内容	住民の異動情報の届出等を受け付ける市町村の窓口において、対面で身分証明書(個人番号カード等)の提示を受け、本人確認を行う。
個人番号の真正性確認の措置の内容	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仕組みとする(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など。)。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	システムでは対応できない事象が発生した際に、本人確認情報の正確性を維持するため、要領・手順書等に基づいて本人確認情報の入力、削除及び訂正が行われていることを定期的に確認する。
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	<ul style="list-style-type: none"> ・機構が作成・配付する専用のアプリケーション(※)を用いることによって、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、情報の暗号化を実施する、操作者の認証を行う等の措置を講じる。 ・特定個人情報の入手は、システム上自動処理にて行われるため、操作者は存在せず人為的なアクセスが行われることはない。 ※都道府県サーバのサーバ上で稼動するアプリケーション。 都道府県内の市町村の住民の本人確認情報を管理し、都道府県内の市町村の市町村CSや全国サーバとのデータ交換を行う。 データの安全保護対策、不正アクセスの防止策には、最新の認証技術や暗号化技術を採用し、データの盗聴、改ざん、破壊及び盗難、端末の不正利用及びなりすまし等を防止する。
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

特定個人情報の入手(情報提供ネットワークシステムを通じた入手を除く。)におけるその他のリスク及びそのリスクに対する措置	
3. 特定個人情報の使用	
リスク1: 目的を超えた紐付け、事務に必要な情報との紐付けが行われるリスク	
宛名システム等における措置の内容	都道府県サーバと宛名管理システム間の接続は行わない。
事務で使用するその他のシステムにおける措置の内容	<p>庁内システムと都道府県サーバとの接続は行わない。</p> <p>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。</p> <p>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。</p> <p>(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、埼玉県へ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> <p>(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、埼玉県へ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。)</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2: 権限のない者(元職員、アクセス権限のない職員等)によって不正に使用されるリスク	
ユーザ認証の管理	[行っている] <選択肢> 1) 行っている 2) 行っていない
具体的な管理方法	生体認証による操作者認証を行う。
アクセス権限の発効・失効の管理	[行っている] <選択肢> 1) 行っている 2) 行っていない
具体的な管理方法	<ul style="list-style-type: none"> 必ず個人に対して操作権限を発効し、共用IDの発行は行わない。 新たに操作権限を発効する際には、事前に書面で届出を行い、システム管理者からのID発行がない限り、登録しない。 異動、退職等により、操作権限を失効させる際には、セキュリティ管理者がシステム管理者に書面で届出を行い、システム管理者が権限の削除を行う。削除履歴についてはシステム上に記録する。
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	<ul style="list-style-type: none"> 操作者の権限に応じてアクセス権限が付与されるように管理する。 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	<ul style="list-style-type: none"> 本人確認情報を扱うシステムの操作履歴(アクセスログ・操作ログ)を記録する。 不正な操作がないことについて、操作履歴により適時確認する。 操作履歴の確認により不正な操作の疑いがある場合には、本人への聞き取り調査等により確認する。
その他の措置の内容	—
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

リスク3: 従業者が事務外で使用するリスク		
リスクに対する措置の内容	<ul style="list-style-type: none"> ・システム管理者も含め、システムの操作履歴(操作ログ)を記録する。 ・担当者へのヒアリングを実施し、業務上必要のない検索又は抽出が行われていないことを確認する。 ・システム利用職員へのセキュリティ研修を定期的に行い、事務外での利用禁止等について周知する。 ・職員以外の委託先等の従業者については、当該事項についての誓約書を提出させ、確認することとする。 	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク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"> ・システム上、管理権限を与えられた者以外は、情報の複製を行えない仕組みとする。 ・定期運用に基づくバックアップ以外にファイルを複製しないよう、職員・委託先に対し指導する。 	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置		
<p>その他、特定個人情報の使用に当たり、以下の措置を講じる。</p> <ul style="list-style-type: none"> ・業務端末は、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及び業務端末のディスプレイを、来庁者から見えない位置に置く。 ・業務端末のディスプレイには、覗き見防止フィルタを装着する。 ・業務端末は、移転・提供先の業務における必要性を踏まえて設置を検討する。 ・本人確認情報が表示された画面の印刷は事務処理に必要な範囲とし、印刷した記録を管理し、廃棄、保管を適正に行う。 ・統計処理を行う場合、その必要性について十分検討を行い、作業内容を記録する。 ・大量のデータ出力に際しては、事前にシステム管理者に届出を行い、システム管理者が操作を行う。 ・システムの稼働確認など、端末操作でのエラーやトラブル等についての記録を残し、必要な検証を行う。 ・本人確認情報の開示・訂正の請求及び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。 ・特定個人情報を取り扱うシステムは、インターネットから分離されたネットワーク及び専用パソコンで利用する。 		
4. 特定個人情報ファイルの取扱いの委託 [] 委託しない		
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク		
情報保護管理体制の確認	<ul style="list-style-type: none"> ・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、住基法に基づき住基ネット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。 	
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	<ul style="list-style-type: none"> ・都道府県サーバの運用及び監視に関する業務に関して、委託先である機構には、特定個人情報ファイルの閲覧／更新権限を与えていない。 ・委託先(再委託先を含む。)に、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、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。)で、災害等におけるデータの損失等に対する対策として、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。 	

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	<ul style="list-style-type: none"> ・委託先(再委託先を含む。)に、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、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。)で、災害等におけるデータの損失等に対する対策として、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、月次で書面により報告を受けている。 	
特定個人情報の提供ルール	[定めている]	<選択肢> 1) 定めている 2) 定めていない
委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	<ul style="list-style-type: none"> ・県の指示又は承認があるときを除き、委託先から第三者への特定個人情報の提供を一切禁止し、委託先から個人情報の取扱状況等について、適時書面により報告をさせることを契約書上明記している。 ・委託先は、目的外利用及び提供についてのチェックを含むセキュリティチェックを行い、委託元である当県は、チェックリストの結果について、月次で書面により報告を受けている。 ・必要と認めれば、本県職員が実地に調査を行い、必要な指示を行うことを契約書上明記している。 	
委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	<ul style="list-style-type: none"> ・委託先(再委託先を含む。)に送付する特定個人情報ファイルは暗号化されているため、委託先(再委託先を含む。)がファイル内の特定個人情報にアクセスできないシステム設計としている。 	
特定個人情報の消去ルール	[定めている]	<選択肢> 1) 定めている 2) 定めていない
ルールの内容及びルール遵守の確認方法	<ul style="list-style-type: none"> ・本県の指示があった場合を除き、廃棄を行う場合は、物理的破壊、裁断、溶解を行うものとし、適切に廃棄した旨の報告書を本県に提出させることを契約書上明記している。 	
委託契約書中の特定個人情報ファイルの取扱いに関する規定	[定めている]	<選択肢> 1) 定めている 2) 定めていない
規定の内容	<ul style="list-style-type: none"> ・個人情報の取扱状況等についての書面報告 ・必要と認める場合の個人情報の取扱状況等についての実地調査 ・本県の書面による承諾を除く再委託の禁止 ・目的外利用、第三者への提供の禁止 ・複写又は持ち出しの禁止 ・業務完了後の資料の返還又は廃棄 ・業務従事者への個人情報保護に関して必要な事項の周知 等 	
再委託先による特定個人情報ファイルの適切な取扱いの確保	[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない 4) 再委託していない
具体的な方法	<ul style="list-style-type: none"> ・再委託する業務は、直接本人確認情報に係らない(直接本人確認情報にアクセスできず、閲覧・更新・削除等を行わない)業務を対象としている。 ・委託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。 ・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。 	
その他の措置の内容	本県の書面による承諾があった場合を除き、再委託を禁止している。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報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		
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	特定個人情報の提供・移転を行う際に、提供・移転記録（日時、操作者等）をシステム上で管理し、記録を保存する。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保存する。	
特定個人情報の提供・移転に関するルール	[定めている]	<選択肢> 1) 定めている 2) 定めていない
ルールの内容及びルール遵守の確認方法	特定個人情報の提供・移転は、番号法、住基法及び個人情報の保護に関する法律の規定により認められる事項のみとし、住基ネットを使用して提供・移転を行うものとする。操作権限の付与に際しては、利用課所からシステム管理者への利用事務の内容も含めた申請が必要となり、システム管理者は、定期的にシステム内の権限付与の状況を確認する。	
その他の措置の内容	「サーバ室等への入室権限」及び「本特定個人情報ファイルを扱うシステムへのアクセス権限」を有する者を厳格に管理し、情報の持ち出しを制限する。 媒体を用いて情報を連携する場合には、必要に応じて媒体へのデータ出力（書き込み）の際に職員が立会う。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2： 不適切な方法で提供・移転が行われるリスク		
リスクに対する措置の内容	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基ネット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。 なお、全国サーバと都道府県サーバとの間の通信では相互認証を実施しているため、認証できない相手方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、埼玉県以外の執行機関への提供及び他の部署への移転のため、媒体へ出力する必要がある場合には、逐一出力の記録が残る仕組みを構築する。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3： 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク		
リスクに対する措置の内容	<ul style="list-style-type: none"> ・誤った情報を提供・移転してしまうリスクへの措置 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・移転することがシステム上担保される。 ・誤った相手に提供・移転してしまうリスクへの措置 相手方（全国サーバ）と都道府県サーバとの間の通信では、相互認証を実施しているため、認証できない相手先への情報の提供はなされないことがシステム上担保される。 	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置		
外部媒体を用いた移転の際には、事前に使用する媒体のウイルスチェックを行う。また、移転する情報にはパスワードを設定する。また、外部媒体にフラッシュメモリを使用する場合は、暗号化機能、ウイルス対策機能のある機器を使用する。		

6. 情報提供ネットワークシステムとの接続		[○] 接続しない(入手)	[○] 接続しない(提供)
リスク1: 目的外の入手が行われるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク2: 安全が保たれない方法によって入手が行われるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク3: 入手した特定個人情報 that 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"> ・都道府県サーバの集約センターにおいて、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。また、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。 ・埼玉県においては、代表端末の設置場所、記録媒体の保管場所を施錠管理する。 ・特定個人情報を取り扱うシステムは、インターネットから分離されたネットワーク及び専用パソコンで利用する。 	
⑥技術的対策	[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
具体的な対策の内容	<ul style="list-style-type: none"> ・都道府県サーバの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。 ・埼玉県においては業務端末等でウイルス対策ソフトのパターンファイルの更新を定期的に行う。また、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。 	
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)に定める期間保管する。	
その他の措置の内容	-	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2: 特定個人情報が古い情報のまま保管され続けるリスク		
リスクに対する措置の内容	市町村の住民基本台帳で本人確認情報の変更があった場合には、住基ネットを通して本人確認情報の更新が行われる仕組みとなっているため、古い情報のまま保管されることはない。また、市町村CSとの整合処理を定期的の実施し、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"> ・住民票の記載の修正前の本人確認情報(履歴情報)及び消除者の本人確認情報は住基法施行令第30条の6に定める保存期間を経過した後に系統的に消去する。 ・磁気ディスクの廃棄時は、内容の消去、破壊を行うとともに磁気ディスク管理簿を作成しその記録を残す。 	

その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置		
—		

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

1. 特定個人情報ファイル名	
(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からの附票本人確認情報更新要求の際に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、システム上で担保する。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	附票本人確認情報の入手元を市町村CSに限定する。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、埼玉県内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ที่ไม่正確であるリスク	
入手の際の本人確認の措置の内容	住民の異動情報の届出等を受け付ける市町村の窓口において、対面で身分証明書（個人番号カード等）の提示を受け、本人確認を行う。個人番号については、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。
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が市町村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、既に削除されている者に対して、削除を要求する通知があっ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、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附票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なりすまし等を防止する。
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置	
—	

3. 特定個人情報の使用

リスク1: 目的を超えた紐付け、事務に必要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と宛名管理システム間の接続は行わない。
事務で使用するその他のシステムにおける措置の内容	庁内システムと附票都道府県サーバ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、埼玉県以外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、埼玉県以外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	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	・必ず個人に対して操作権限を発効し、共用IDの発行は行わない。 ・新たに操作権限を発効する際には、事前に書面で届出を行い、システム管理者からのID発行がない限り、登録しない。 ・異動、退職等により、操作権限を失効させる際には、セキュリティ管理者がシステム管理者に書面で届出を行い、システム管理者が権限の削除を行う。削除履歴についてはシステム上に記録する。
アクセス権限の管理	[行っている] <選択肢> 1) 行っている 2) 行っていない
具体的な管理方法	・操作者の権限に応じてアクセス権限が付与されるように管理する。 ・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	・本人確認情報を扱うシステムの操作履歴(アクセスログ・操作ログ)を記録する。 ・不正な操作がないことについて、操作履歴により適時確認する。 ・操作履歴の確認により不正な操作の疑いがある場合には、本人への聞き取り調査等により確認する。
その他の措置の内容	—
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

リスク3: 従業者が事務外で使用するリスク		
リスクに対する措置の内容	<ul style="list-style-type: none"> ・システム管理者も含め、システムの操作履歴(操作ログ)を記録する。 ・担当者へのヒアリングを実施し、業務上必要のない検索又は抽出が行われていないことを確認する。 ・システム利用職員へのセキュリティ研修を定期的に行い、事務外での利用禁止等について周知する。 ・職員以外の委託先等の従業者については、当該事項についての誓約書を提出させ、確認することとする。 	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク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"> ・システム上、管理権限を与えられた者以外は、情報の複製を行えない仕組みとする。 ・定期運用に基づくバックアップ以外にファイルを複製しないよう、職員・委託先に対し指導する。 	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置		
<p>その他、特定個人情報の使用に当たり、以下の措置を講じる。</p> <ul style="list-style-type: none"> ・業務端末は、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。 ・都道府県サーバの代表端末及び業務端末(都道府県サーバと共用する。)のディスプレイを、来庁者から見えない位置に置く。 ・業務端末のディスプレイには、覗き見防止フィルタを装着する。 ・業務端末は、移転・提供先の業務においての必要性を踏まえて設置を検討する。 ・附票本人確認情報が表示された画面の印刷は事務処理に必要な範囲とし、印刷した記録を管理し、廃棄、保管を適正に行う。 ・大量のデータ出力に際しては、事前にシステム管理者に届出を行い、システム管理者の承認を得る。 ・システムの稼働確認など、端末操作でのエラーやトラブル等についての記録を残し、必要な検証を行う。 ・特定個人情報を取り扱うシステムは、インターネットから分離されたネットワーク及び専用パソコンで利用する。 		
4. 特定個人情報ファイルの取扱いの委託 [] 委託しない		
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク		
情報保護管理体制の確認	<ul style="list-style-type: none"> ・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、住基法に基づき住基ネット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。 	
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	<ul style="list-style-type: none"> ・附票都道府県サーバの運用及び監視に関する業務に関して、委託先である機構には、特定個人情報ファイルの閲覧／更新権限を与えていない。 ・委託先(再委託先を含む。)に、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、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。)で、災害等におけるデータの損失等に対する対策として、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。 	

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	<ul style="list-style-type: none"> ・委託先(再委託先を含む。)に、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、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。)で、災害等におけるデータの損失等に対する対策として、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、月次で書面により報告を受けている。 	
特定個人情報の提供ルール	[定めている]	<選択肢> 1) 定めている 2) 定めていない
委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	<ul style="list-style-type: none"> ・県の指示又は承認があるときを除き、委託先から第三者への特定個人情報の提供を一切禁止し、委託先から個人情報の取扱状況等について、適時書面により報告をさせることを契約書上明記している。 ・委託先は、目的外利用及び提供についてのチェックを含むセキュリティチェックを行い、委託元である当県は、チェックリストの結果について、月次で書面により報告を受けている。 ・必要と認めれば、本県職員が実地に調査を行い、必要な指示を行うことを契約書上明記している。 	
委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	<ul style="list-style-type: none"> ・委託先(再委託先を含む。)に送付する特定個人情報ファイルは暗号化されているため、委託先(再委託先を含む。)がファイル内の特定個人情報にアクセスできないシステム設計としている。 	
特定個人情報の消去ルール	[定めている]	<選択肢> 1) 定めている 2) 定めていない
ルールの内容及びルール遵守の確認方法	<ul style="list-style-type: none"> ・本県の指示があった場合を除き、廃棄を行う場合は、物理的破壊、裁断、溶解を行うものとし、適切に廃棄した旨の報告書を本県に提出させることを契約書上明記している。 	
委託契約書中の特定個人情報ファイルの取扱いに関する規定	[定めている]	<選択肢> 1) 定めている 2) 定めていない
規定の内容	<ul style="list-style-type: none"> ・個人情報の取扱状況等についての書面報告 ・必要と認める場合の個人情報の取扱状況等についての実地調査 ・本県の書面による承諾を除く再委託の禁止 ・目的外利用、第三者への提供の禁止 ・複写又は持ち出しの禁止 ・業務完了後の資料の返還又は廃棄 ・業務従事者への個人情報保護に関して必要な事項の周知 等 	
再委託先による特定個人情報ファイルの適切な取扱いの確保	[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない 4) 再委託していない
具体的な方法	<ul style="list-style-type: none"> ・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。 ・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。 	
その他の措置の内容	本県の書面による承諾があった場合を除き、再委託を禁止している。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報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		
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	特定個人情報の提供・移転を行う際に、提供・移転記録(日時、操作者等)をシステム上で管理し、記録を保存する。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保存する。	
特定個人情報の提供・移転に関するルール	[定めている]	<選択肢> 1) 定めている 2) 定めていない
ルールの内容及びルール遵守の確認方法	特定個人情報の提供・移転は、番号法、住基法及び個人情報の保護に関する法律の規定により認められる事項のみとし、住基ネットを使用して提供・移転を行うものとする。操作権限の付与に際しては、利用課所からシステム管理者への利用事務の内容も含めた申請が必要となり、システム管理者は、定期的にシステム内の権限付与の状況を確認する。	
その他の措置の内容	「サーバ室等への入室権限」及び「本特定個人情報ファイルを扱うシステムへのアクセス権限」を有する者を厳格に管理し、情報の持ち出しを制限する。 媒体を用いて情報を連携する場合には、必要に応じて媒体へのデータ出力(書き込み)の際に職員が立会う。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2： 不適切な方法で提供・移転が行われるリスク		
リスクに対する措置の内容	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。 なお、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、埼玉県内の他の執行機関への提供及び他部署への移転のため、媒体へ出力する又は回線連携を行う必要がある場合には、逐一出力の記録が残される仕組みを構築する。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3： 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク		
リスクに対する措置の内容	<ul style="list-style-type: none"> ・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。 ・誤った相手に提供・移転してしまうリスクへの措置 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担保される。 	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の提供・移転(委託や情報提供ネットワークシステムを通じた提供を除く。)におけるその他のリスク及びそのリスクに対する措置		
外部媒体を用いた移転の際には、事前に使用する媒体のウイルスチェックを行う。また、移転する情報にはパスワードを設定する。また、外部媒体にフラッシュメモリを使用する場合は、暗号化機能、ウイルス対策機能のある機器を使用する。		

6. 情報提供ネットワークシステムとの接続		[○] 接続しない(入手)	[○] 接続しない(提供)
リスク1: 目的外の入手が行われるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク2: 安全が保たれない方法によって入手が行われるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク3: 入手した特定個人情報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	<ul style="list-style-type: none"> ・附票都道府県サーバの集約センターにおいて、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。また、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。 ・埼玉県においては、代表端末の設置場所、記録媒体の保管場所を施錠管理する。 ・特定個人情報を取り扱うシステムは、インターネットから分離されたネットワーク及び専用パソコンで利用する。
⑥技術的対策	[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
	具体的な対策の内容	<ul style="list-style-type: none"> ・附票都道府県サーバの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。 ・埼玉県においては業務端末等でウイルス対策ソフトのパターンファイルの更新を定期的に行う。また、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。
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	<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、埼玉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。</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: 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"> ・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、内容の消去、破壊を行うとともに磁気ディスク管理簿を作成しその記録を残す。
その他の措置の内容	—
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置	
—	

IV その他のリスク対策 ※

1. 監査	
①自己点検	[十分に行っている] <選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
具体的なチェック方法	年に1回、物理的なセキュリティの確保、帳票、記録媒体、規定等の適切な管理、障害発生時の対応手順の整理など自己点検を行い、特定個人情報が適切に取り扱われていることを確認する。
②監査	[十分に行っている] <選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
具体的な内容	<ul style="list-style-type: none"> ・内部監査 住基ネットの利用課所に対して、セキュリティ管理責任者が任命する内部監査員が内部監査を実施する。 監査は機器のセキュリティの状況や媒体、書類の保管状況等を確認の上、聞き取り、実地検証、記録等の検証を行い、監査結果を文書で通知し、必要に応じて改善要求を行う。 改善要求があった場合、利用課所はセキュリティ管理責任者に内部監査改善計画書を提出し承認を得るとともに、改善結果を報告する。 セキュリティ管理責任者は監査対象課所に対して必要に応じてフォローアップ監査を実施し、改善状況を確認する。改善結果に対して不適切な事項がある場合は、利用課所に対して再度改善要求を行う。
2. 従業者に対する教育・啓発	
従業者に対する教育・啓発	[十分に行っている] <選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
具体的な方法	住基ネットの管理業務を行う職員及び利用課所の職員(非常勤職員等を含む。)を対象に、業務遂行に必要な知識及び能力の習得のため、研修計画を作成の上、研修を行う。 新任のシステム運用管理担当者にはOJTによる訓練を行う。
3. その他のリスク対策	
<ul style="list-style-type: none"> ・予防措置 監査結果、障害記録の定期的な分析、システム性能監視結果、他のシステムの事例等からセキュリティ対策において改善すべき点が認められる場合は、原因に応じた予防処置を実施し、記録を行う。 ・是正措置 重大なシステム障害や情報セキュリティに関する事件、事故が発生し、再発の可能性が認められる場合は、原因に応じた是正措置を実施し、記録を行う。 ・操作者が不正にシステムを利用したことを発見した場合には、直ちに、利用権限を無効化するものとする。なお、不正なシステム利用については、懲戒処分の対象となる。 	

V 開示請求、問合せ

1. 特定個人情報の開示・訂正・利用停止請求	
①請求先	埼玉県企画財政部情報システム戦略課 住基ネット・マイナンバー担当 〒330-9301 さいたま市浦和区高砂3-15-1 電話 048-830-2686
②請求方法	埼玉県の規則で定める様式により本人確認情報開示請求書又は本人確認情報訂正等申出書を提出する。なお、申請は埼玉県電子申請サービスでも受け付ける。
特記事項	請求方法、様式については、埼玉県のホームページで案内し、利用しやすいようにしている。 ・開示請求 https://www.pref.saitama.lg.jp/a0105/juki-net/kaiji.html ・訂正等申出 https://www.pref.saitama.lg.jp/a0105/juki-net/teisei2.html
③手数料等	[無料] <選択肢> 1) 有料 2) 無料 (手数料額、納付方法:)
④個人情報ファイル簿の公表	[行っている] <選択肢> 1) 行っている 2) 行っていない
個人情報ファイル名	住民基本台帳ネットワークシステム本人確認情報ファイル
公表場所	埼玉県のホームページ https://www.pref.saitama.lg.jp/a0304/kj-f-jouhousystem.html
⑤法令による特別の手続	—
⑥個人情報ファイル簿への不記載等	—
2. 特定個人情報ファイルの取扱いに関する問合せ	
①連絡先	埼玉県企画財政部情報システム戦略課 住基ネット・マイナンバー担当 〒330-9301 さいたま市浦和区高砂3-15-1 電話 048-830-2686
②対応方法	問い合わせの受付時に記票し、対応内容を記録に残す。

VI 評価実施手続

1. 基礎項目評価	
①実施日	令和5年12月28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	以下の方法で公表し、郵送、FAX、電子メール等の手段により評価書案に対する意見募集を実施した。 (公表方法) ・報道機関への記者発表 ・県広報誌(彩の国だより)での周知 ・県ホームページへの掲載
②実施日・期間	令和5年10月12日から令和5年11月13日まで
③期間を短縮する特段の理由	—
④主な意見の内容	意見なし
⑤評価書への反映	—
3. 第三者点検	
①実施日	令和5年12月14日
②方法	情報セキュリティに関する学識経験者、個人情報の保護に関する学識経験者等の複数の有識者で構成される「埼玉県特定個人情報保護評価委員会」において点検を行った。
③結果	適合性及び妥当性の観点から点検を行った結果、評価書に記載している内容については、妥当であるとの意見を受けた。
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28年2月1日	I 基本情報 7. 評価実施機関における担当部署 ②所属長	課長 加藤 信次	課長 黒坂 和実	事後	人事異動
平成28年2月1日	II 特定個人情報ファイルの概要 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	時点修正
平成29年3月30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 3. 特定個人情報の使用 特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置	その他、特定個人情報の使用に当たり、以下の措置を講じる。 ・業務端末は、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。 ・都道府県サーバーの代表端末及び業務端末のディスプレイを、来庁者から見えない位置に置く。 ・業務端末のディスプレイには、覗き見防止フィルタを装着する。 ・業務端末は、移転・提供先の業務における必要性を踏まえて設置を検討する。 ・本人確認情報が表示された画面の印刷は事務処理に必要な範囲とし、印刷した記録を管理し、廃棄、保管を適正に行う。 ・統計処理を行う場合、その必要性について十分検討を行い、作業内容を記録する。 ・大量のデータ出力に際しては、事前にシステム管理者に届出を行い、システム管理者が操作を行う。 ・システムの稼働確認など、端末操作でのエラーやトラブル等についての記録を残し、必要な検証を行う。 ・本人確認情報の開示・訂正の請求及び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。	その他、特定個人情報の使用に当たり、以下の措置を講じる。 ・業務端末は、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。 ・都道府県サーバーの代表端末及び業務端末のディスプレイを、来庁者から見えない位置に置く。 ・業務端末のディスプレイには、覗き見防止フィルタを装着する。 ・業務端末は、移転・提供先の業務における必要性を踏まえて設置を検討する。 ・本人確認情報が表示された画面の印刷は事務処理に必要な範囲とし、印刷した記録を管理し、廃棄、保管を適正に行う。 ・統計処理を行う場合、その必要性について十分検討を行い、作業内容を記録する。 ・大量のデータ出力に際しては、事前にシステム管理者に届出を行い、システム管理者が操作を行う。 ・システムの稼働確認など、端末操作でのエラーやトラブル等についての記録を残し、必要な検証を行う。 ・本人確認情報の開示・訂正の請求及び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。 ・特定個人情報を取り扱うシステムは、インターネットから分離されたネットワーク及び専用パソコンで利用する。	事後	対策強化 ・リスクを軽減させる変更であり、重要な変更にあたらないため
平成29年3月30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 7. 特定個人情報の保管・消去 ⑥技術的対策 具体的な対策の内容	・都道府県サーバーの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。 ・埼玉県においては業務端末等でウイルス対策ソフトのパターンファイルの更新を定期的に行う。また、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。	・都道府県サーバーの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。 ・埼玉県においては業務端末等でウイルス対策ソフトのパターンファイルの更新を定期的に行う。また、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。 ・特定個人情報を取り扱うシステムは、インターネットから分離されたネットワーク及び専用パソコンで利用する。	事後	対策強化 ・リスクを軽減させる変更であり、重要な変更にあたらないため
平成30年3月29日	I 基本情報 7. 評価実施機関における担当部署 ②所属長	課長 黒坂 和実	課長 横田 淳一	事後	人事異動
平成31年3月28日	I 基本情報 7. 評価実施機関における担当部署 ②所属長の役職名	課長 横田 淳一	課長	事後	記載事項修正
令和2年3月30日	I 基本情報 5. 個人番号の利用 法令上の根拠	住民基本台帳法(昭和42年7月25日法律第81号) (平成25年5月31日法律第28号施行時点) ・第7条(住民票の記載事項) ・第12条の5(住民基本台帳の脱漏等に関する都道府県知事の通報) ・第30条の6(市町村長から都道府県知事への本人確認情報の通知等) ・第30条の7(都道府県知事から機構への本人確認情報の通知等) ・第30条の8(本人確認情報の誤りに関する機構の通報) ・第30条の11(通知都道府県以外の都道府県の執行機関への本人確認情報の提供) ・第30条の15(本人確認情報の利用) ・第30条の32(自己の本人確認情報の開示) ・第30条の35(自己の本人確認情報の訂正)	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) ・第30条の7(都道府県知事から機構への本人確認情報の通知等) ・第30条の8(本人確認情報の誤りに関する機構の通報) ・第30条の11(通知都道府県以外の都道府県の執行機関への本人確認情報の提供) ・第30条の15(本人確認情報の利用) ・第30条の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)	事後	番号整備法(平成25年法律第28号)施行に伴う変更、システムの機能「本人確認情報整合」の根拠として、第30条の22を追加したものであり、重要な変更にあたらないため
令和2年3月30日	(別添1)事務の内容	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	特定個人情報を含まない手続きを明記したものであり、重要な変更にあたらないため
令和2年3月30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 提供先2 ③提供する情報	住民票コード、氏名、生年月日、性別、住所、個人番号、異動事由、異動年月日 ※住民票コードについては、行政手続における特定の個人を識別するための番号の利用等に関する法律の施行に伴う関係法律の整備等に関する法律(平成25年5月31日法律第28号)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、生年月日、性別、住所、個人番号、異動事由、異動年月日 ※住民票コードについては、行政手続における特定の個人を識別するための番号の利用等に関する法律の施行に伴う関係法律の整備等に関する法律(平成25年5月31日法律第28号)第22条第7項に基づく経過措置である。	事後	番号整備法(平成25年法律第28号)施行に伴う変更であり、重要な変更にあたらないため

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和2年3月30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 移転先1 ③移転する情報	住民票コード、氏名、生年月日、性別、住所、個人番号、異動事由、異動年月日 ※住民票コードについては、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、生年月日、性別、住所、個人番号、異動事由、異動年月日 ※住民票コードについては、行政手続における特定の個人を識別するための番号の利用等に関する法律の施行に伴う関係法律の整備等に関する法律(平成25年5月31日法律第28号)第22条第7項に基づく経過措置である。	事後	番号整備法(平成25年法律第28号)施行に伴う変更であり、重要な変更にと当たらないため
令和2年3月30日	(別添2)特定個人情報ファイル記録項目	都道府県知事保存本人確認情報ファイル 1. 住民票コード、2. 漢字氏名、3. 外字数(氏名)、4. ふりがな氏名、5. 生年月日、6. 性別、7. 住所、8. 外字数(住所)、9. 個人番号、10. 異動事由、11. 異動年月日、12. 保存期間フラグ、13. 清音化かな氏名、14. 市町村コード、15. 大字・字コード、16. 操作者ID、17. 操作端末ID、18. タイムスタンプ、19. 通知を受けた年月日、20. 外字フラグ、21. 削除フラグ、22. 更新順番号、23. 氏名外字変更連番、24. 住所外字変更連番	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	事後	住民基本台帳法施行令等(平成31年4月17日政令第152号)施行に伴う変更であり、重要な変更にと当たらないため
令和2年3月30日	IIIリスク対策 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	・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、前身である財団法人地方自治情報センターにおいて平成14年8月5日から平成26年3月31日まで、指定情報処理機関として住基ネット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。	・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、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。	事後	住民基本台帳法(昭和42年法律第81号)改正に伴う住民基本台帳ネットワークシステムが機構の業務となったことによる変更であり、重要な変更にと当たらないため
令和3年3月30日	I 基本情報 5. 個人番号の利用 法令上の根拠	住民基本台帳法(昭和42年7月25日法律第81号) ・第7条(住民票の記載事項) ・第12条の5(住民基本台帳の脱漏等に関する都道府県知事の通報) ・第30条の6(市町村長から都道府県知事への本人確認情報の通知等) ・第30条の7(都道府県知事から機構への本人確認情報の通知等) ・第30条の8(本人確認情報の誤りに関する機構の通報) ・第30条の11(通知都道府県以外の都道府県の執行機関への本人確認情報の提供) ・第30条の15(本人確認情報の利用) ・第30条の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(住民基本台帳の脱漏等に関する都道府県知事の通報) ・第30条の6(市町村長から都道府県知事への本人確認情報の通知等) ・第30条の7(都道府県知事から機構への本人確認情報の通知等) ・第30条の8(本人確認情報の誤りに関する機構の通報) ・第30条の11(通知都道府県以外の都道府県の執行機関への本人確認情報の提供) ・第30条の13(都道府県の条例による本人確認情報の提供) ・第30条の15(本人確認情報の利用) ・第30条の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)	事後	法律の施行に伴う記載の変更であり、重要な変更にと当たらないため
令和3年12月27日	I 基本情報 7. 評価実施機関における担当部署 ①部署	企画財政部 情報システム課	企画財政部 情報システム戦略課	事後	記載事項修正
令和3年12月27日	II 特定個人情報ファイルの概要 2. 基本情報 ⑥事務担当部署	企画財政部 情報システム課	企画財政部 情報システム戦略課	事後	記載事項修正
令和3年12月27日	II 特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ⑦使用の主体	企画財政部 情報システム課	企画財政部 情報システム戦略課	事後	記載事項修正
令和3年12月27日	II 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 ⑤委託先名の確認方法	埼玉県企画財政部情報システム課のホームページにて確認できる。	埼玉県企画財政部情報システム戦略課のホームページにて確認できる。	事後	記載事項修正
令和3年12月27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 ①請求先	埼玉県企画財政部情報システム課 住基ネット・マイナンバー担当 〒330-9301 さいたま市浦和区高砂3-15-1 電話 048-830-2686	埼玉県企画財政部情報システム戦略課 住基ネット・マイナンバー担当 〒330-9301 さいたま市浦和区高砂3-15-1 電話 048-830-2686	事後	記載事項修正
令和3年12月27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 ②請求方法 特記事項	請求方法、様式については、埼玉県のホームページで案内し、利用しやすいようにしている。 ・開示請求 http://www.pref.saitama.lg.jp/a0105/juki-net/kaji.html ・訂正等申出 http://www.pref.saitama.lg.jp/a0105/juki-net/teisei2.html	請求方法、様式については、埼玉県のホームページで案内し、利用しやすいようにしている。 ・開示請求 https://www.pref.saitama.lg.jp/a0105/juki-net/kaji.html ・訂正等申出 https://www.pref.saitama.lg.jp/a0105/juki-net/teisei2.html	事後	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和3年12月27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 ④個人情報ファイル簿の公表公表場所	埼玉県のホームページ http://www.pref.saitama.lg.jp/a0304/kj-f-jouhousystem.html	埼玉県のホームページ https://www.pref.saitama.lg.jp/a0304/kj-f-jouhousystem.html	事後	
令和3年12月27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	埼玉県企画財政部情報システム課 住基ネット・マイナンバー担当 〒330-9301 さいたま市浦和区高砂3-1-5-1 電話 048-830-2686	埼玉県企画財政部情報システム戦略課 住基ネット・マイナンバー担当 〒330-9301 さいたま市浦和区高砂3-1-5-1 電話 048-830-2686	事後	記載事項修正
令和5年12月28日	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	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	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	表紙 個人のプライバシー等の権利利益の保護の宣言	埼玉県は、住民基本台帳ネットワークに係る本人確認情報の管理及び提供等に関する事務における特定個人情報ファイルの取扱いに当たり、特定個人情報ファイルの取扱いが個人のプライバシー等の権利利益に影響を及ぼしかねないことを認識し、特定個人情報の漏えいその他の事態を発生させるリスクを軽減させるため、適切な措置を講じ、もって個人のプライバシー等の権利利益の保護に取り組んでいることを宣言する。	埼玉県は、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態を発生させるリスクを軽減させるため、適切な措置を講じ、もって個人のプライバシー等の権利利益の保護に取り組んでいることを宣言する。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	表紙 個人のプライバシー等の権利利益の保護の宣言 特記事項	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では、事務の一部を外部業者に委託するが、委託する業務は、都道府県サーバーの運用及び監視に関する業務とし、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。	住民基本台帳ネットワークに関する事務では、事務の一部を外部業者に委託するが、委託する業務は、都道府県サーバーの運用及び監視に関する業務とし、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。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	I 基本情報 1. 特定個人情報ファイルを取り扱う事務 ①事務の名称	住民基本台帳ネットワークに係る本人確認情報の管理及び提供等に関する事務	住民基本台帳ネットワークに関する事務	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	I 基本情報 1. 特定個人情報ファイルを取り扱う事務 ②事務の内容	県は、住民基本台帳法（以下「住基法」という。）に基づき、住民基本台帳のネットワーク化を図り、全国共通の本人確認システムを市町村と共同で構築している。 住民基本台帳は、住基法に基づき作成され、住民に関する記録を正確かつ統一的に行う制度であり、住民の利便を増進するとともに、行政の合理化に資することを目的としている。 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） ①磁気ディスクによる特定個人情報ファイルの管理 ②市町村からの本人確認情報に係る変更の通知に基づく特定個人情報ファイルの更新及び地方公共団体情報システム機構（以下「機構」という。）への通知 ③埼玉県知事から本人確認情報に係る埼玉県の他の執行機関への提供又は他部署への移転 ④住民からの請求に基づく当該個人の本人確認情報の開示及び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	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。 1. 本人確認情報の管理及び提供等に関する事務 県は、住民基本台帳法（以下「住基法」という。）に基づき、住民基本台帳のネットワーク化を図り、全国共通の本人確認システム（住基ネット）を市町村と共同で構築している。 住民基本台帳は、住基法に基づき作成され、住民に関する記録を正確かつ統一的に行う制度であり、住民の利便を増進するとともに、行政の合理化に資することを目的としている。 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） ①磁気ディスクによる特定個人情報ファイルの管理 ②市町村からの本人確認情報に係る変更の通知に基づく特定個人情報ファイルの更新及び地方公共団体情報システム機構（以下「機構」という。）への通知 ③埼玉県知事から本人確認情報に係る埼玉県の他の執行機関への提供又は他部署への移転 ④住民からの請求に基づく当該個人の本人確認情報の開示及び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	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年12月28日	I 基本情報 1. 特定個人情報ファイルを取り扱う事務 ②事務の内容		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(コミュニケーションサーバ)、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。以下「4情報」という。)、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。 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埼玉県知事から附票本人確認情報に係る埼玉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	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	I 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1 ①システムの名称	住民基本台帳ネットワークシステム(以下「住基ネット」という。) ※「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、住基ネットの構成要素のうち、都道府県サーバで管理されているため、以降は、住基ネットのうち都道府県サーバ部分について記載する。	住民基本台帳ネットワークシステム(以下「住基ネット」という。) ※「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、住基ネットの構成要素のうち、都道府県サーバで管理されているため、以降は、住基ネットのうち都道府県サーバ部分について記載する。	事前	語句の修正(事後で足りるものの任意に事前提出)
令和5年12月28日	I 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1 ②システムの機能	1. 本人確認情報の更新 都道府県知事保存本人確認情報ファイルを最新の状態に保つため、住基ネットの市町村CS(コミュニケーションサーバ)を経由して通知された本人確認情報の更新情報を元に当該ファイルを更新し、全国サーバに対して当該本人確認情報の更新情報を通知する。 2. 埼玉県の他の執行機関への情報提供又は他部署への移転 埼玉県の他の執行機関又は他部署による住基法に基づく情報照会に対応するため、照会のあった当該個人の個人番号又は基本4情報(氏名、住所、性別及び生年月日。以下「4情報」という。)等に対応する本人確認情報を都道府県知事保存本人確認情報ファイルから抽出し、照会元に提供・移転する。 3. 本人確認情報の開示 法律に基づく住民による自己の本人確認情報の開示請求に対応するため、当該個人の本人確認情報を都道府県知事保存本人確認情報ファイルから抽出し、帳票に出力する。	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、住基ネットの市町村CS(コミュニケーションサーバ)を経由して通知された本人確認情報の更新情報を元に当該ファイルを更新し、全国サーバに対して当該本人確認情報の更新情報を通知する。 2. 埼玉県の他の執行機関への情報提供又は他部署への移転 埼玉県の他の執行機関又は他部署による住基法に基づく情報照会に対応するため、照会のあった当該個人の個人番号又は4情報等に対応する本人確認情報を都道府県知事保存本人確認情報ファイルから抽出し、照会元に提供・移転する。 3. 本人確認情報の開示 法律に基づく住民による自己の本人確認情報の開示請求に対応するため、当該個人の本人確認情報を都道府県知事保存本人確認情報ファイルから抽出し、帳票に出力する。	事前	語句の修正(事後で足りるものの任意に事前提出)
令和5年12月28日	I 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1 ②システムの機能	4. 機構への情報照会 全国サーバに対して住民票コード、個人番号又は4情報の組合せをキーとした本人確認情報照会要求を行い、該当する個人の本人確認情報を受領する。 5. 本人確認情報の検索 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。	4. 機構への情報照会 全国サーバに対して住民票コード、個人番号又は4情報の組合せをキーとした本人確認情報照会要求を行い、該当する個人の本人確認情報を受領する。 5. 本人確認情報の検索 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。	事前	語句の修正(事後で足りるものの任意に事前提出)
令和5年12月28日	I 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 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、住基ネットの構成要素のうち、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、附票連携システム内の附票都道府県サーバ部分について記載する。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年12月28日	I 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 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. 埼玉県への他の執行機関への情報提供又は他部署への移転 埼玉県へ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、照会があった当該個人の4情報等に対応する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、埼玉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>	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	I 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 ②システムの機能		<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>	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	I 基本情報 3. 特定個人情報ファイル名	都道府県知事保存本人確認情報ファイル	(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	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	I 基本情報 4. 特定個人情報ファイルを取り扱う理由 ①事務実施上の必要性	<p>県では、都道府県知事保存本人確認情報ファイルを、下記に記載のとおり必要性から取り扱う。</p> <p>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(住基ネットに係る本人確認情報の管理及び提供等に関する事務)の処理を行うため、区域内の住民に係る最新の本人確認情報を管理する。 ②市町村からの本人確認情報の更新情報の通知を受けて都道府県知事保存本人確認情報ファイルを更新し、当該更新情報を機構に対して通知する。 ③埼玉県の他の執行機関又は他部署からの照会に基づき、本人確認情報を提供・移転する。 ④住民からの請求に基づき、当該個人の本人確認情報を開示する。 ⑤住基ネットに係る本人確認情報の管理及び提供等に関する事務において、本人確認情報を検索する。 ⑥市町村において保存する本人確認情報との整合性を確認する。</p>	<p>(1)都道府県知事保存本人確認情報ファイル 県では、都道府県知事保存本人確認情報ファイルを、下記に記載のとおり必要性から取り扱う。</p> <p>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(住基ネットに係る本人確認情報の管理及び提供等に関する事務)の処理を行うため、区域内の住民に係る最新の本人確認情報を管理する。 ②市町村からの本人確認情報の更新情報の通知を受けて都道府県知事保存本人確認情報ファイルを更新し、当該更新情報を機構に対して通知する。 ③埼玉県の他の執行機関又は他部署からの照会に基づき、本人確認情報を提供・移転する。 ④住民からの請求に基づき、当該個人の本人確認情報を開示する。 ⑤住基ネットに係る本人確認情報の管理及び提供等に関する事務において、本人確認情報を検索する。 ⑥市町村において保存する本人確認情報との整合性を確認する。</p>	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年12月28日	I 基本 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>(2)都道府県知事保存附票本人確認情報ファイル 県では、都道府県知事保存附票本人確認情報ファイル、下記に記載の通りの必要性から取り扱う。</p> <p>・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埼玉県以外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、埼玉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・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>	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	I 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	住民票の写し等にかえて本人確認情報を利用することにより、添付書類の省略が図られ、住民の負担軽減(各行政機関を訪問し、書類を入手する金銭的、時間的コストの節約)及び行政の合理化につながる。	住民票の写し等にかえて本人確認情報を利用することにより、添付書類の省略が図られ、住民の負担軽減(各行政機関を訪問し、書類を入手する金銭的、時間的コストの節約)及び行政の合理化につながる。 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。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	I 基本情報 5. 個人番号の利用 法令上の根拠	住民基本台帳法(昭和42年7月25日法律第81号) ・第7条(住民票の記載事項) ・第12条の5(住民基本台帳の脱漏等に関する都道府県知事の通報) ・第30条の6(市町村長から都道府県知事への本人確認情報の通知等) ・第30条の7(都道府県知事から機構への本人確認情報の通知等) ・第30条の8(本人確認情報の誤りに関する機構の通報) ・第30条の11(通知都道府県以外の都道府県の執行機関への本人確認情報の提供) ・第30条の13(都道府県の条例による本人確認情報の提供) ・第30条の15(本人確認情報の利用) ・第30条の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(住基法)(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) ・第30条の7(都道府県知事から機構への本人確認情報の通知等) ・第30条の8(本人確認情報の誤りに関する機構の通報) ・第30条の11(通知都道府県以外の都道府県の執行機関への本人確認情報の提供) ・第30条の13(都道府県の条例による本人確認情報の提供) ・第30条の15(本人確認情報の利用) ・第30条の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(都道府県知事保存附票本人確認情報(住民票コードに限る。))の利用)	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	I 基本情報 (別添1)事務の内容	本人確認情報の管理及び提供等に関する事務	(1)本人確認情報の管理及び提供等に関する事務	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	I 基本情報 (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		図の修正	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	I 基本情報 (別添1)事務の内容 (備考) (1)本人確認情報の管理及び提供等に関する事務	<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ーに通知する。 1-②都道府県サーバーにおいて、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、住基ネットを介して、本人確認情報の更新を通知する。</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ーに通知する。 1-②都道府県サーバーにおいて、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、住基ネットを介して、本人確認情報の更新を通知する。</p>	事前	語句の修正(事後で足りるものの任意に事前提出)

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年12月28日	I 基本情報（別添1）事務の内容（備考）(1)本人確認情報の管理及び提供等に関する事務	2. 埼玉県への他の執行機関への情報提供又は他部署への移転 2-①.埼玉県への他の執行機関又は他部署において、個人番号又は4情報等をキーワードとした本人確認情報の照会を行う。 2-②.埼玉県知事において、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、全国サーバーに対して検索の要求を行う。 ※埼玉県への他の執行機関又は他部署に対し、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、埼玉県への他の執行機関又は他部署において、都道府県サーバーの代表端末又は業務端末を操作し、媒体連携（注2）により行う。 （注1）埼玉県へ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ーに照会し、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。	2. 埼玉県への他の執行機関への情報提供又は他部署への移転 2-①.埼玉県への他の執行機関又は他部署において、個人番号又は4情報等をキーワードとした本人確認情報の照会を行う。 2-②.埼玉県知事において、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、全国サーバーに対して検索の要求を行う。 ※埼玉県への他の執行機関又は他部署に対し、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、埼玉県への他の執行機関又は他部署において、都道府県サーバーの代表端末又は業務端末を操作し、媒体連携（注2）により行う。 （注1）埼玉県へ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ーに照会し、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。	事前	語句の修正（事後で足りるものの任意に事前提出）
令和5年12月28日	I 基本情報（別添1）事務の内容（備考）(1)本人確認情報の管理及び提供等に関する事務	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. 機構への情報照会に係る事務 4-①.機構に対し、個人番号又は4情報等をキーワードとした本人確認情報の照会を行う。 4-②.機構より、当該個人の本人確認情報を受領する。 5. 本人確認情報検索に関する事務 5-①.4情報の組み合わせを検索キーに、都道府県知事保存本人確認情報ファイルを検索する。 6.本人確認情報整合 6-①.市町村CSより、都道府県サーバーに対し、整合性確認用の本人確認情報を送付する。 6-②.都道府県サーバーにおいて、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.都道府県サーバーより、市町村CSに対して整合性確認結果を通知する。	3. 本人確認情報の開示に関する事務 3-①.住民より本人確認情報の開示請求を受け付ける（※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. 機構への情報照会に係る事務 4-①.機構に対し、個人番号又は4情報等をキーワードとした本人確認情報の照会を行う。 4-②.機構より、当該個人の本人確認情報を受領する。 5. 本人確認情報検索に関する事務 5-①.4情報の組み合わせを検索キーに、都道府県知事保存本人確認情報ファイルを検索する。 6.本人確認情報整合 6-①.市町村CSより、都道府県サーバーに対し、整合性確認用の本人確認情報を送付する。 6-②.都道府県サーバーにおいて、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.都道府県サーバーより、市町村CSに対して整合性確認結果を通知する。	事前	語句の修正（事後で足りるものの任意に事前提出）
令和5年12月28日	I 基本情報（別添1）事務の内容		(2)附票本人確認情報の管理及び提供等に関する事務	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したもの
令和5年12月28日	I 基本情報（別添1）事務の内容 (2)附票本人確認情報の管理及び提供等に関する事務		図の挿入	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したもの
令和5年12月28日	I 基本情報（別添1）事務の内容 (2)附票本人確認情報の管理及び提供等に関する事務（備考）		1. 附票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を通じて附票都道府県サーバーに通知する。 1-②.附票都道府県サーバーにおいて、市町村より受領した附票本人確認情報を元に都道府県知事保存附票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、附票本人確認情報の更新を通知する。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したもの

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年12月28日	I 基本情報（別添1）事務の内容（2）附票本人確認情報の管理及び提供等に関する事務（備考）		<p>2. 埼玉県内の他の執行機関への情報提供又は他部署への移転</p> <p>2-①.埼玉県内の他の執行機関又は他部署において、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。</p> <p>2-②.埼玉県知事において、提示されたキーワードを元に都道府県知事保存附票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、埼玉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・移転する必要がある。</p> <p>※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。</p> <p>※埼玉県内の他の執行機関又は他部署に対し、附票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、埼玉県の他の執行機関又は他部署において、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用する。）を操作し、媒体連携（注2）により行う。</p> <p>（注1）埼玉県内の他の執行機関又は他部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。</p> <p>（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。</p>	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したもの
令和5年12月28日	I 基本情報（別添1）事務の内容（2）附票本人確認情報の管理及び提供等に関する事務（備考）		<p>3. 附票本人確認情報の開示に関する事務</p> <p>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。</p> <p>3-②.開示請求者（住民）に対し、都道府県知事保存附票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. 機構への情報照会に係る事務</p> <p>4-①.機構に対し、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。</p> <p>4-②.機構より、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</p> <p>5-①.4情報の組み合わせを検索キーに、都道府県知事保存附票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</p> <p>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。</p> <p>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。</p> <p>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>	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したもの
令和5年12月28日	II ファイルの概要 1. 特定個人情報ファイル名	都道府県知事保存本人確認情報ファイル	(1)都道府県知事保存本人確認情報ファイル	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したもの

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年12月28日	II ファイルの概要 3. 特定個人情報の入手・使用 ⑧使用方法	<ul style="list-style-type: none"> ・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→都道府県サーバー)、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(都道府県サーバー→全国サーバー)。 ・埼玉県への他の執行機関又は他部署からの本人確認情報の照会要求を受け(埼玉県への他の執行機関又は他部署→都道府県サーバー)、照会のあった住民票コード、個人番号又は4情報の組合せを元に都道府県知事保存本人確認情報ファイルを検索し、該当する個人の本人確認情報を照会元へ提供・移転する(都道府県サーバー→埼玉県の他の執行機関又は他部署)。 ・住民からの開示請求に基づき(住民→都道府県窓口→都道府県サーバー)、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(都道府県サーバー→帳票出力カー→住民)。 ・4情報の組合せをキーに都道府県知事保存本人確認情報ファイルの検索を行う。 ・都道府県知事保存本人確認情報ファイルの正確性を担保するため、市町村から本人確認情報を受領し(市町村CS→都道府県サーバー)、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。 	<ul style="list-style-type: none"> ・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→都道府県サーバー)、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(都道府県サーバー→全国サーバー)。 ・埼玉県への他の執行機関又は他部署からの本人確認情報の照会要求を受け(埼玉県への他の執行機関又は他部署→都道府県サーバー)、照会のあった住民票コード、個人番号又は4情報の組合せを元に都道府県知事保存本人確認情報ファイルを検索し、該当する個人の本人確認情報を照会元へ提供・移転する(都道府県サーバー→埼玉県の他の執行機関又は他部署)。 ・住民からの開示請求に基づき(住民→都道府県窓口→都道府県サーバー)、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(都道府県サーバー→帳票出力カー→住民)。 ・4情報の組合せをキーに都道府県知事保存本人確認情報ファイルの検索を行う。 ・都道府県知事保存本人確認情報ファイルの正確性を担保するため、市町村から本人確認情報を受領し(市町村CS→都道府県サーバー)、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。 	事前	語句の修正(事後で足りるものの任意に事前提出)
令和5年12月28日	II ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1	都道府県サーバーの運用及び監視に関する業務	都道府県サーバの運用及び監視に関する業務	事前	語句の修正(事後で足りるものの任意に事前提出)
令和5年12月28日	II ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 ①委託内容	<p>全国の都道府県サーバーを1拠点(集約センター)に集約化したことに伴い、都道府県サーバー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。</p> <p>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)業務を対象とする。</p>	<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。</p> <p>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)業務を対象とする。</p>	事前	語句の修正(事後で足りるものの任意に事前提出)
令和5年12月28日	II ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 ②取扱いを委託する特定個人情報ファイルの範囲その妥当性	<p>本特定個人情報ファイル(都道府県知事保存本人確認情報ファイル)が保存される都道府県サーバーの運用及び監視業務を委託することによる。</p> <p>なお、「①委託内容」とおり、委託事項は、直接本人確認情報に係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。</p>	<p>本特定個人情報ファイル(都道府県知事保存本人確認情報ファイル)が保存される都道府県サーバの運用及び監視業務を委託することによる。</p> <p>なお、「①委託内容」とおり、委託事項は、直接本人確認情報に係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。</p>	事前	語句の修正(事後で足りるものの任意に事前提出)
令和5年12月28日	II ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 再委託 ⑨再委託事項	都道府県サーバーの運用及び監視に関する業務。再委託する業務は、直接本人確認情報に係らない(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。	都道府県サーバの運用及び監視に関する業務。再委託する業務は、直接本人確認情報に係らない(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。	事前	語句の修正(事後で足りるものの任意に事前提出)
令和5年12月28日	II ファイルの概要 5. 特定個人情報の提供・移転 提供先1 ①法令上の根拠	住民基本台帳法第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)	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)	事前	語句の修正(事後で足りるものの任意に事前提出)
令和5年12月28日	II ファイルの概要 5. 特定個人情報の提供・移転 提供先2 ①法令上の根拠	住民基本台帳法第30条の15第2項(本人確認情報の利用)	住基法第30条の15第2項(本人確認情報の利用)	事前	語句の修正(事後で足りるものの任意に事前提出)
令和5年12月28日	II ファイルの概要 5. 特定個人情報の提供・移転 提供先2 ②提供先における用途	住民基本台帳法別表第6に掲げる、自都道府県への他の執行機関への情報提供が認められる事務(例:教育委員会における特別支援学校への就学のため必要な経費の支弁に関する事務等)の処理に用いる。	住基法別表第6に掲げる、埼玉県の他の執行機関への情報提供が認められる事務(例:教育委員会における特別支援学校への就学のため必要な経費の支弁に関する事務等)の処理に用いる。	事前	語句の修正(事後で足りるものの任意に事前提出)
令和5年12月28日	II ファイルの概要 5. 特定個人情報の提供・移転 提供先3	住民基本台帳法上の住民	住基法上の住民	事前	語句の修正(事後で足りるものの任意に事前提出)
令和5年12月28日	II ファイルの概要 5. 特定個人情報の提供・移転 提供先3 ①法令上の根拠	住民基本台帳法第30条の32(自己の本人確認情報の開示)	住基法第30条の32(自己の本人確認情報の開示)	事前	語句の修正(事後で足りるものの任意に事前提出)
令和5年12月28日	II ファイルの概要 5. 特定個人情報の提供・移転 提供先1 ①法令上の根拠	住民基本台帳法第30条の15第1項(本人確認情報の利用)	住基法第30条の15第1項(本人確認情報の利用)	事前	語句の修正(事後で足りるものの任意に事前提出)
令和5年12月28日	II ファイルの概要 5. 特定個人情報の提供・移転 提供先1 ②移転先における用途	住民基本台帳法別表第5に掲げる、都道府県知事において都道府県知事保存本人確認情報の利用が認められる事務(例:地方税の賦課徴収又は地方税に関する調査に関する事務等)の処理に用いる。	住基法別表第5に掲げる、都道府県知事において都道府県知事保存本人確認情報の利用が認められる事務(例:地方税の賦課徴収又は地方税に関する調査に関する事務等)の処理に用いる。	事前	語句の修正(事後で足りるものの任意に事前提出)

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年12月28日	II ファイルの概要 6. 特定個人情報の保管・消去 ①保管場所	・セキュリティゲートによって入退室管理をしている都道府県サーバーの集約センターにおいては、施錠管理及び入退室管理(監視カメラを設置してサーバー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ー内に保管する。サーバーへのアクセスはID/パスワードによる認証が必要となる。 ・県においては、端末及び記録媒体を施錠管理された部屋に保管する。	・セキュリティゲートによって入退室管理をしている都道府県サーバーの集約センターにおいては、施錠管理及び入退室管理(監視カメラを設置してサーバー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ー内に保管する。サーバーへのアクセスは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、端末及び記録媒体を施錠管理された部屋に保管する。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 6. 特定個人情報の保管・消去 ②保管期間 その妥当性	・住民票の記載の修正後の本人確認情報は、新たに記載の修正の通知を受けるまで保管する。 ・住民票の記載の修正前の本人確認情報(履歴情報)及び消除者の本人確認情報は、住民基本台帳法施行令第30条の6(都道府県における本人確認情報の保存期間)に定める期間保管する。	・住民票の記載の修正後の本人確認情報は、新たに記載の修正の通知を受けるまで保管する。 ・住民票の記載の修正前の本人確認情報(履歴情報)及び消除者の本人確認情報は、住民基本台帳法施行令第30条の6(都道府県における本人確認情報の保存期間)に定める期間保管する。	事前	・語句の修正(事後で足りるものの任意に事前提出)
令和5年12月28日	II 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	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 2. 基本情報 ①ファイルの種類		システム用ファイル	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 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	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 2. 基本情報 ③対象となる本人の範囲		区域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者 ※消除者を含む。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 2. 基本情報 ③対象となる本人の範囲 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)において区域内の戸籍の附票に記録された全ての者の情報を保有し、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	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 2. 基本情報 ④記録される項目		10項目以上50項目未満	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 2. 基本情報 ④記録される項目 主な記録項目		[○]個人番号 [○]14情報(氏名、住所、性別、生年月日) [○]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。))	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 2. 基本情報 ④記録される項目 その妥当性		・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(本籍及び筆頭者の氏名)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、埼玉県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ー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。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 2. 基本情報 ④記録される項目 全ての記録項目		別添2を参照。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 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。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 2. 基本情報 ⑥事務担当部署		企画財政部 情報システム戦略課	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 3. 特定個人情報の入手・使用 ①入手元		[○]地方公共団体・地方独立行政法人(市町村) [○]その他(都道府県サーバー(※入手には該当しないが、都道府県サーバーから個人番号を抽出する場合がある))	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年12月28日	II ファイルの概要 3. 特定個人情報の入手・使用 ②入手方法		[○]専用線	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 3. 特定個人情報の入手・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、埼玉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。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 3. 特定個人情報の入手・使用 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。 ※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。 ※※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。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 3. 特定個人情報の入手・使用 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44の6第3項に明示されている。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 3. 特定個人情報の入手・使用 ⑥使用目的		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)において区域内の戸籍の附票に記録された全ての者の情報を保有し、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、埼玉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	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 3. 特定個人情報の入手・使用 ⑦使用の主体 使用部署		企画財政部 情報システム戦略課	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 3. 特定個人情報の入手・使用 ⑦使用の主体 利用者数		10人未満	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 3. 特定個人情報の入手・使用 ⑧使用方法		・埼玉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(埼玉県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→埼玉県の他の執行機関又は他部署)。 ※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。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 3. 特定個人情報の入手・使用 ⑧使用方法 情報の突合		・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	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 3. 特定個人情報の入手・使用 ⑧使用方法 情報の統計分析		該当なし。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 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得る決定		該当なし。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年12月28日	II ファイルの概要 3. 特定個人情報の入手・使用 ⑨使用開始日		「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。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託の有無		1) 委託する(1件)	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1		附票都道府県サーバの運用及び監視に関する業務	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 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、直接附票本人確認情報に係わらない(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。)業務を対象とする。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 ②取扱いを委託する特定個人情報ファイルの範囲		1) 特定個人情報ファイルの全体	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 ②取扱いを委託する特定個人情報ファイルの範囲 対象となる本人の数		4) 100万人以上1,000万人未満	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 ②取扱いを委託する特定個人情報ファイルの範囲 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	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 ②取扱いを委託する特定個人情報ファイルの範囲 その妥当性		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)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、直接附票本人確認情報に係わらない事務を対象としているため、委託先においては、特定個人情報ファイルに記録された情報そのものを扱う事務は実施しない。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 ③委託先における取扱者数		1) 10人未満	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 ④委託先への特定個人情報ファイルの提供方法		[○]専用線	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 ⑤委託先名の確認方法		埼玉県企画財政部情報システム戦略課のホームページにて確認できる。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 ⑥委託先名		地方公共団体情報システム機構(機構)	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 ⑦再委託の有無		1) 再委託する	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 ⑧再委託の許諾方法		書面による承諾。 なお、承諾に当たっては、再委託先がプライバシーマーク等を取得していることを確認する。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 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、直接附票本人確認情報に係わらない(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。)業務を対象とする。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II 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・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	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II 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1		埼玉県の他の執行機関(教育委員会など)	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年12月28日	II 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。) 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) 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	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II 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。) ②提供先における用途		住基法別表第六に掲げる、埼玉県他の執行機関への情報提供が認められる事務(例:教育委員会における特別支援学校への就学のために必要な経費の支弁に関する事務等)の処理に用いる。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II 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。) 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(番号法に基づく埼玉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。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II 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。) ④提供する情報の対象となる本人の数		4) 100万人以上1,000万人未満	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II 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。) 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	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II 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。) 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(住民基本台帳ネットワークシステム)	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II 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。) ⑦時期・頻度		埼玉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。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II 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		埼玉県の他の部署(税務局など)	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II 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。) 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) 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	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II 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。) ②移転先における用途		住基法別表第五に掲げる、都道府県知事において都道府県知事保存附票本人確認情報の利用が認められた事務の処理に用いる。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II 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。) 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(番号法に基づく埼玉県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	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II 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。) ④提供する情報の対象となる本人の数		4) 100万人以上1,000万人未満	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II 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。) 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	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II 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。) 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(住民基本台帳ネットワークシステム)	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II 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。) ⑦時期・頻度		埼玉県の他の部署からの情報照会の要求があった都度、随時。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 6. 特定個人情報の保管・消去 ①保管場所		・セキュリティゲートにて入退館管理をしている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、端末及び記録媒体を施錠管理された部屋に保管する。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年12月28日	II ファイルの概要 6. 特定個人情報の保管・消去 ②保管期間 期間		1)1年未満	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 6. 特定個人情報の保管・消去 ②保管期間 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、埼玉県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。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	II ファイルの概要 6. 特定個人情報の保管・消去 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。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	(別添2)特定個人情報ファイル記録項目	都道府県知事保存本人確認情報ファイル 1. 住民票コード 2. 漢字氏名 3. 外字数(氏名) 4. ふりがな氏名 5. 生年月日 6. 性別 7. 住所 8. 外字数(住所) 9. 個人番号 10. 異動事由 11. 異動年月日 12. 保存期間フラグ 13. 清音化かな氏名 14. 市町村コード 15. 大字・字コード 16. 操作者ID 17. 操作端末ID 18. タイムスタンプ 19. 通知を受けた年月日 20. 外字フラグ 21. 削除フラグ 22. 更新順番号 23. 氏名外字変更連番 24. 住所外字変更連番 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	(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	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	(別添2)特定個人情報ファイル記録項目		(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 1. 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、埼玉県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。)	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 1. 特定個人情報ファイル名	都道府県知事保存本人確認情報ファイル	(1)都道府県知事保存本人確認情報ファイル	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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、システムの仕様によって市町村CSからの本人確認情報更新要求の際に通知される本人確認情報更新要求の際に通知される本人確認情報に限定される。	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、システムの仕様によって市町村CSからの本人確認情報更新要求の際に通知される本人確認情報に限定される。この場合、市町村CSから対象者以外の情報が通知されてしまうことがリスクとして想定されるが、制度上、対象者の真正性の担保は市町村側の確認に委ねられるため、市町村において厳格な審査が行われることが前提となる。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年12月28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 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が入力されたシステムが不正であるリスク その他の措置の内容	システムでは対応できない事象が発生した際に、本人確認情報の正確性を維持するため、要領・手順書等に基づいて、市町村からの連絡によって、本人確認情報の削除等を行う。	システムでは対応できない事象が発生した際に、本人確認情報の正確性を維持するため、要領・手順書等に基づいて本人確認情報の入力、削除及び訂正が行われていることを定期的に確認する。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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4: 入手の際に特定個人情報が入力されたシステムが不正であるリスク 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(※)を用いることによって、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、情報の暗号化を実施する、操作者の認証を行う等の措置を講じる。 ・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。 ※都道府県サーバーのサーバー上で移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や全国サーバーとのデータ交換を行う。 データの安全保護対策、不正アクセスの防止策には、最新の認証技術や暗号化技術を採用し、データの盗聴、改ざん、破壊及び盗難、端末の不正利用及びなりすまし等を防止する。	・機構が作成・配付する専用のアプリケーション(※)を用いることによって、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、情報の暗号化を実施する、操作者の認証を行う等の措置を講じる。 ・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。 ※都道府県サーバーのサーバー上で移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や全国サーバーとのデータ交換を行う。 データの安全保護対策、不正アクセスの防止策には、最新の認証技術や暗号化技術を採用し、データの盗聴、改ざん、破壊及び盗難、端末の不正利用及びなりすまし等を防止する。	事前	語句の修正(事後で足りるものの任意に事前提出)
令和5年12月28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 3. 特定個人情報の使用 リスク1: 目的を超えた紐付け、事務に必要な情報との紐付けが行われるリスク 宛名システム等における措置の内容	都道府県サーバーと宛名管理システム間の接続は行わない。	都道府県サーバーと宛名管理システム間の接続は行わない。	事前	語句の修正(事後で足りるものの任意に事前提出)
令和5年12月28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 3. 特定個人情報の使用 リスク1: 目的を超えた紐付け、事務に必要な情報との紐付けが行われるリスク 事務で使用するその他のシステムにおける措置の内容	庁内システムと都道府県サーバーとの接続は行わない。	庁内システムと都道府県サーバーとの接続は行わない。 都道府県サーバーは、集約センター内において、附票都道府県サーバーと接続する。 なお、都道府県サーバーと附票都道府県サーバー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)都道府県サーバー⇒附票都道府県サーバーへのアクセス 番号法で認められた場合に限り、埼玉県他の執行機関又は他部署等からの求めに応じ、国外転出に係る個人番号を連携する場合。 (2)附票都道府県サーバー⇒都道府県サーバーへのアクセス 国外転出に係る事務処理に関し、番号法で認められた場合に限り、埼玉県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。)	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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 アクセス権限の発効・失効の管理 具体的な管理方法	・新たに操作権限を発効する際には、事前に書面で届出を行い、システム管理者からのID発行がない限り、登録しない。 ・異動、退職等により、操作権限を失効させる際には、事前に書面で届出を行い、システム管理者が権限の削除についてチェックを行う。削除履歴についてはシステム上に記録する。	・必ず個人に対して操作権限を発効し、共用IDの発行は行わない。 ・新たに操作権限を発効する際には、事前に書面で届出を行い、システム管理者からのID発行がない限り、登録しない。 ・異動、退職等により、操作権限を失効させる際には、セキュリティ管理者がシステム管理者に書面で届出を行い、システム管理者が権限の削除を行う。削除履歴についてはシステム上に記録する。	事前	時点修正(事後で足りるものの任意に事前提出)
令和5年12月28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 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 具体的な管理方法	・必ず個人に対して操作権限を発効し、共用IDの発行は行わない。 ・操作者の権限に応じてアクセス権限が付与されるように管理する。 ・不正アクセスを分析するために、都道府県サーバー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。	・操作者の権限に応じてアクセス権限が付与されるように管理する。 ・不正アクセスを分析するために、都道府県サーバー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	時点修正(事後で足りるものの任意に事前提出)
令和5年12月28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 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 特定個人情報の使用記録 具体的な管理方法	・システムの操作履歴(アクセスログ・操作ログ)を記録する。 ・不正な操作がないことについて、操作履歴により適時確認する。 ・操作履歴の確認により不正な操作の疑いがある場合には、本人への聞き取り調査等により確認する。	・本人確認情報を扱うシステムの操作履歴(アクセスログ・操作ログ)を記録する。 ・不正な操作がないことについて、操作履歴により適時確認する。 ・操作履歴の確認により不正な操作の疑いがある場合には、本人への聞き取り調査等により確認する。	事前	時点修正(事後で足りるものの任意に事前提出)

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年12月28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 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	<ul style="list-style-type: none"> ・システム管理者も含め、システムの操作履歴(操作ログ)を記録する。 ・システム利用職員へのセキュリティ研修を定期的に行い、事務外での利用禁止等について周知する。 ・職員以外の委託先等の従業者については、当該事項についての誓約書を提出させ、確認することとする。 	<ul style="list-style-type: none"> ・システム管理者も含め、システムの操作履歴(操作ログ)を記録する。 ・担当者へのヒアリングを実施し、業務上必要のない検索又は抽出が行われていないことを確認する。 ・システム利用職員へのセキュリティ研修を定期的に行い、事務外での利用禁止等について周知する。 ・職員以外の委託先等の従業者については、当該事項についての誓約書を提出させ、確認することとする。 	事前	時点修正(事後で足りるものの任意に事前提出)
令和5年12月28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 使用 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>その他、特定個人情報の使用に当たり、以下の措置を講じる。</p> <ul style="list-style-type: none"> ・業務端末は、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。 ・都道府県サーバーの代表端末及び業務端末のディスプレイを、来庁者から見えない位置に置く。 ・業務端末のディスプレイには、覗き見防止フィルタを装着する。 ・業務端末は、移転・提供先の業務における必要性を踏まえて設置を検討する。 ・本人確認情報が表示された画面の印刷は事務処理に必要な範囲とし、印刷した記録を管理し、廃棄、保管を適正に行う。 ・統計処理を行う場合、その必要性について十分検討を行い、作業内容を記録する。 ・大量のデータ出力に際しては、事前にシステム管理者に届出を行い、システム管理者が操作を行う。(※要確認) ・システムの稼働確認など、端末操作でのエラーやトラブル等についての記録を残し、必要な検証を行う。 ・本人確認情報の開示・訂正の請求及び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。 ・特定個人情報を取り扱うシステムは、インターネットから分離されたネットワーク及び専用パソコンで利用する。 	<p>その他、特定個人情報の使用に当たり、以下の措置を講じる。</p> <ul style="list-style-type: none"> ・業務端末は、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。 ・都道府県サーバーの代表端末及び業務端末のディスプレイを、来庁者から見えない位置に置く。 ・業務端末のディスプレイには、覗き見防止フィルタを装着する。 ・業務端末は、移転・提供先の業務における必要性を踏まえて設置を検討する。 ・本人確認情報が表示された画面の印刷は事務処理に必要な範囲とし、印刷した記録を管理し、廃棄、保管を適正に行う。 ・統計処理を行う場合、その必要性について十分検討を行い、作業内容を記録する。 ・大量のデータ出力に際しては、事前にシステム管理者に届出を行い、システム管理者が操作を行う。 ・システムの稼働確認など、端末操作でのエラーやトラブル等についての記録を残し、必要な検証を行う。 ・本人確認情報の開示・訂正の請求及び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。 ・特定個人情報を取り扱うシステムは、インターネットから分離されたネットワーク及び専用パソコンで利用する。 	事前	語句の修正(事後で足りるものの任意に事前提出)
令和5年12月28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 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	<ul style="list-style-type: none"> ・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、都道府県サーバー集約化の実施および集約化された都道府県サーバー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、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。 	<ul style="list-style-type: none"> ・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、都道府県サーバー集約化の実施および集約化された都道府県サーバー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、住基法に基づき住基ネット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。 	事前	時点修正(事後で足りるものの任意に事前提出)
令和5年12月28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 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	<ul style="list-style-type: none"> ・本県の承認があるときを除き、業務を処理するために引き渡された個人情報が記録された資料等の複写等を一切禁止し、施錠又は入退室管理の可能な保管庫に保管する等適正な管理を行わせることを契約書上明記している。 ・委託先(再委託先を含む。)に送付する特定個人情報ファイルは暗号化されているため、委託先(再委託先を含む。)がファイル内の特定個人情報にアクセスできないシステム設計としている。 ・必要と認めれば、本県職員が実地に調査を行い、必要な指示を行うことを契約書上明記している。 	<ul style="list-style-type: none"> ・委託先(再委託先を含む。)に送付する特定個人情報ファイルは暗号化されているため、委託先(再委託先を含む。)がファイル内の特定個人情報にアクセスできないシステム設計としている。 	事前	時点修正(事後で足りるものの任意に事前提出)
令和5年12月28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 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 ルールの内容及びルール遵守の確認方法	<ul style="list-style-type: none"> ・個人情報が記録された資料は、業務完了後直ちに本県に返還するか、本県の承諾を得て廃棄することを契約書上明記している。 ・本県の指示があった場合を除き、廃棄を行う場合は、物理的破壊、裁断、溶解を行うものとし、適切に廃棄した旨の報告書を本県に提出させることを契約書上明記している。 	<ul style="list-style-type: none"> ・本県の指示があった場合を除き、廃棄を行う場合は、物理的破壊、裁断、溶解を行うものとし、適切に廃棄した旨の報告書を本県に提出させることを契約書上明記している。 	事前	時点修正(事後で足りるものの任意に事前提出)
令和5年12月28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 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>再委託先の選定については、都道府県サーバー集約に伴う調達評価委員会(都道府県の各ブロックから推薦された新潟県、長野県、富山県、和歌山県、香川県、愛媛県、岡山県および福岡県により構成)が、入札の評価基準の作成に参加し、適切な再委託先となるようにした。</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及び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>	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したもの

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年12月28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 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: 不正な提供・移転が行われるリスク 特定個人情報の提供・移転に関するルール ルールの内容及びルール遵守の確認方法	特定個人情報の提供・移転は、番号法及び住民基本台帳法並びに埼玉県個人情報保護条例の規定により認められる事項のみとし、住民基本台帳ネットワークシステムを使用して提供・移転を行うものとする。操作権限の付与に際しては、利用課所からシステム管理者への利用事務の内容も含めた申請が必要となり、システム管理者は、定期的にシステム内の権限付与の状況を確認する。	特定個人情報の提供・移転は、番号法、住基法及び個人情報の保護に関する法律の規定により認められる事項のみとし、住基ネットを使用して提供・移転を行うものとする。操作権限の付与に際しては、利用課所からシステム管理者への利用事務の内容も含めた申請が必要となり、システム管理者は、定期的にシステム内の権限付与の状況を確認する。	事前	時点修正(事後で足りるものの任意に事前提出)
令和5年12月28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 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: 不正な提供・移転が行われるリスク その他の措置の内容	—	「サーバ室等への入室権限」及び「本特定個人情報ファイルを扱うシステムへのアクセス権限」を有する者を厳格に管理し、情報の持ち出しを制限する。 媒体を用いて情報を連携する場合には、必要に応じて媒体へのデータ出力(書き込み)の際に職員が立会う。	事前	時点修正(事後で足りるものの任意に事前提出)
令和5年12月28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 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: 不適切な方法で提供・移転が行われるリスク リスクに対する措置の内容	全国サーバーと都道府県サーバーとの間の通信では相互認証を実施しているため、認証できない相手方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、埼玉県の他の執行機関への提供及び他の部署への移転のため、媒体へ出力する必要がある場合には、逐一出力の記録が残る仕組みを構築する。	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基ネット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。 なお、全国サーバーと都道府県サーバーとの間の通信では相互認証を実施しているため、認証できない相手方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、埼玉県の他の執行機関への提供及び他の部署への移転のため、媒体へ出力する必要がある場合には、逐一出力の記録が残る仕組みを構築する。	事前	時点修正(事後で足りるものの任意に事前提出)
令和5年12月28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 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: 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 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・移転することがシステム上担保される。 ・誤った相手に提供・移転してしまうリスクへの措置 相手方(全国サーバー)と都道府県サーバーとの間の通信では、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。	・誤った情報を提供・移転してしまうリスクへの措置 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・移転することがシステム上担保される。 ・誤った相手に提供・移転してしまうリスクへの措置 相手方(全国サーバー)と都道府県サーバーとの間の通信では、相互認証を実施しているため、認証できない相手先への情報の提供はなされないことがシステム上担保される。	事前	語句の修正(事後で足りるものの任意に事前提出)
令和5年12月28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 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 ⑤物理的対策 具体的な対策の内容	・都道府県サーバーの集約センターにおいて、監視カメラを設置してサーバー設置場所への入退室者を特定し、管理する。また、集約センターにおいては、サーバー設置場所、記録媒体の保管場所を施錠管理する。 ・埼玉県においては、代表端末の設置場所、記録媒体の保管場所を施錠管理する。 ・特定個人情報を取り扱うシステムは、インターネットから分離されたネットワーク及び専用パソコンで利用する。	・都道府県サーバーの集約センターにおいて、監視カメラを設置してサーバー設置場所への入退室者を特定し、管理する。また、集約センターにおいては、サーバー設置場所、記録媒体の保管場所を施錠管理する。 ・埼玉県においては、代表端末の設置場所、記録媒体の保管場所を施錠管理する。 ・特定個人情報を取り扱うシステムは、インターネットから分離されたネットワーク及び専用パソコンで利用する。	事前	語句の修正(事後で足りるものの任意に事前提出)
令和5年12月28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 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 ⑥技術的対策 具体的な対策の内容	・都道府県サーバーの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。 ・埼玉県においては業務端末等でウイルス対策ソフトのパターンファイルの更新を定期的に行う。また、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。	・都道府県サーバーの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。 ・埼玉県においては業務端末等でウイルス対策ソフトのパターンファイルの更新を定期的に行う。また、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。	事前	語句の修正(事後で足りるものの任意に事前提出)
令和5年12月28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 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 ⑩死者の個人情報 具体的な保管方法	生存する個人の個人番号とともに、死亡による消除後、住民基本台帳法施行令第30条の6(都道府県における本人確認情報の保存期間)に定める期間保管する。	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)に定める期間保管する。	事前	語句の修正(事後で足りるものの任意に事前提出)
令和5年12月28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 7. 特定個人情報の保管・消去 リスク3: 特定個人情報の漏えい・滅失・毀損リスク ⑪磁気ディスクの廃棄時、内容の消去、破壊を行うとともに磁気ディスク管理簿を作成しその記録を残す。	・住民票の記載の修正前の本人確認情報(履歴情報)及び消除者の本人確認情報は住民基本台帳法施行令第30条の6に定める保存期間を経過した後に系統的に消去する。 ・磁気ディスクの廃棄時は、内容の消去、破壊を行うとともに磁気ディスク管理簿を作成しその記録を残す。	・住民票の記載の修正前の本人確認情報(履歴情報)及び消除者の本人確認情報は住基法施行令第30条の6に定める保存期間を経過した後に系統的に消去する。 ・磁気ディスクの廃棄時は、内容の消去、破壊を行うとともに磁気ディスク管理簿を作成しその記録を残す。	事前	語句の修正(事後で足りるものの任意に事前提出)
令和5年12月28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 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	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年12月28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 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からの附票本人確認情報更新要求の際に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。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したもの
令和5年12月28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 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		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、システム上で担保する。 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。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したもの
令和5年12月28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 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 リスクへの対策は十分か		2) 十分である	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したもの
令和5年12月28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 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		附票本人確認情報の入手元を市町村CSに限定する。 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、埼玉県等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。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したもの
令和5年12月28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 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 リスクへの対策は十分か		2) 十分である	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したもの
令和5年12月28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 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が入手の際の本人確認の措置の内容		住民の異動情報の届出等を受け付ける市町村の窓口において、対面で身分証明書(個人番号カード等)の提示を受け、本人確認を行う。 個人番号については、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。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したもの
令和5年12月28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 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が入手の際の本人確認の措置の内容		市町村において真正性が確認された情報が市町村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。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したもの
令和5年12月28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 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が入手の際の本人確認の措置の内容		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、既に削除されている者に対して、削除を要求する通知があっ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。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したもの
令和5年12月28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 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が入手の際の本人確認の措置の内容		システムでは対応できない事象が発生した際に、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。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したもの
令和5年12月28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 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が入手の際の本人確認の措置の内容		2) 十分である	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したもの

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年12月28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 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4: 入手の際に特定個人情報情報が漏えい・紛失するリスク リスクに対する措置の内容		<ul style="list-style-type: none"> ・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、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附票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なりすまし等を防止する。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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4: 入手の際に特定個人情報情報が漏えい・紛失するリスク リスクへの対策は十分か		2) 十分である	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 3. 特定個人情報の使用 リスク1: 目的を超えた紐付け、事務に必要な情報との紐付けが行われるリスク 宛名システム等における措置の内容		附票都道府県サーバと宛名管理システム間の接続は行わない。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 3. 特定個人情報の使用 リスク1: 目的を超えた紐付け、事務に必要な情報との紐付けが行われるリスク 事務で使用するその他のシステムにおける措置の内容		庁内システムと附票都道府県サーバ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、埼玉県内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、埼玉県内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。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 3. 特定個人情報の使用 リスク1: 目的を超えた紐付け、事務に必要な情報との紐付けが行われるリスク リスクへの対策は十分か		2) 十分である	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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 ユーザー認証の管理		1) 行っている	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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 ユーザー認証の管理 具体的な管理方法		生体認証による操作者認証を行う。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年12月28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 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 アクセス権限の発効・失効の管理		1)行っている	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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 アクセス権限の発効・失効の管理 具体的な管理方法		・必ず個人に対して操作権限を発効し、共用IDの発行は行わない。 ・新たに操作権限を発効する際には、事前に書面で届出を行い、システム管理者からのID発行がない限り、登録しない。 ・異動、退職等により、操作権限を失効させる際には、セキュリティ管理者がシステム管理者に書面で届出を行い、システム管理者が権限の削除を行う。削除履歴についてはシステム上に記録する。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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		1)行っている	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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 具体的な管理方法		・操作者の権限に応じてアクセス権限が付与されるように管理する。 ・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。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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 特定個人情報の使用の使用の記録		1)記録を残している	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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 特定個人情報の使用の使用の記録 具体的な方法		・本人確認情報を扱うシステムの操作履歴(アクセスログ・操作ログ)を記録する。 ・不正な操作がないことについて、操作履歴により適時確認する。 ・操作履歴の確認により不正な操作の疑いがある場合には、本人への聞き取り調査等により確認する。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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 リスクへの対策は十分か		2)十分である	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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		・システム管理者も含め、システムの操作履歴(操作ログ)を記録する。 ・担当者へのヒアリングを実施し、業務上必要のない検索又は抽出が行われていないことを確認する。 ・システム利用職員へのセキュリティ研修を定期的に行い、事務外での利用禁止等について周知する。 ・職員以外の委託先等の従業者については、当該事項についての誓約書を提出させ、確認することとする。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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 リスクへの対策は十分か		2)十分である	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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		・システム上、管理権限を与えられた者以外は、情報の複製を行えない仕組みとする。 ・定期運用に基づくバックアップ以外にファイルを複製しないよう、職員・委託先に対し指導する。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年12月28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 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 リスクへの対策は十分か		2) 十分である	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 3. 特定個人情報の使用 特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置		その他、特定個人情報の使用に当たり、以下の措置を講じる。 ・業務端末は、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。 ・都道府県サーバの代表端末及び業務端末（都道府県サーバと共用する。）のディスプレイを、来庁者から見えない位置に置く。 ・業務端末のディスプレイには、覗き見防止フィルタを装着する。 ・業務端末は、移転・提供先の業務における必要性を踏まえて設置を検討する。 ・附票本人確認情報が表示された画面の印刷は事務処理に必要な範囲とし、印刷した記録を管理し、廃棄、保管を適正に行う。 ・大量のデータ出力に際しては、事前にシステム管理者に届出を行い、システム管理者の承認を得る。 ・システムの稼働確認など、端末操作でのエラーやトラブル等についての記録を残し、必要な検証を行う。 ・特定個人情報を取り扱うシステムは、インターネットから分離されたネットワーク及び専用パソコンで利用する。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 4. 特定個人情報ファイル取扱いの委託 情報管理体制の確認		・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、住基法に基づき住基ネット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。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 4. 特定個人情報ファイル取扱いの委託 特定個人情報ファイルの閲覧者・更新者の制限		1) 制限している	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 4. 特定個人情報ファイル取扱いの委託 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		・附票都道府県サーバの運用及び監視に関する業務に関して、委託先である機構には、特定個人情報ファイルの閲覧／更新権限を与えていない。 ・委託先（再委託先を含む。）に、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、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。）で、災害等におけるデータの損失等に対する対策として、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。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 4. 特定個人情報ファイル取扱いの委託 特定個人情報ファイルの取扱いの記録		1) 記録を残している	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年12月28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 4. 特定個人情報ファイル取扱いの委託 特定個人情報ファイルの取扱いの記録 具体的な方法		<ul style="list-style-type: none"> ・委託先(再委託先を含む。)に、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、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。)で、災害等におけるデータの損失等に対する対策として、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、月次で書面により報告を受けている。 	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 4. 特定個人情報ファイル取扱いの委託 特定個人情報の提供ルール		1) 定めている	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 4. 特定個人情報ファイル取扱いの委託 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遵守の確認方法		<ul style="list-style-type: none"> ・県の指示又は承認があるときを除き、委託先から第三者への特定個人情報の提供を一切禁止し、委託先から個人情報の取扱状況等について、適時書面により報告をさせざることを契約書上明記している。 ・委託先は、目的外利用及び提供についてのチェックを含むセキュリティチェックを行い、委託元である当県は、チェックリストの結果について、月次で書面により報告を受けている。 ・必要と認めれば、本県職員が実地に調査を行い、必要な指示を行うことを契約書上明記している。 	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 4. 特定個人情報ファイル取扱いの委託 特定個人情報の提供ルール 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		<ul style="list-style-type: none"> ・委託先(再委託先を含む。)に送付する特定個人情報ファイルは暗号化されているため、委託先(再委託先を含む。)がファイル内の特定個人情報にアクセスできないシステム設計としている。 	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 4. 特定個人情報ファイル取扱いの委託 特定個人情報の消去ルール		1) 定めている	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 4. 特定個人情報ファイル取扱いの委託 特定個人情報の消去ルール ルールの内容及びルール遵守の確認方法		<ul style="list-style-type: none"> ・本県の指示があった場合を除き、廃棄を行う場合は、物理的破壊、裁断、溶解を行うものとし、適切に廃棄した旨の報告書を本県に提出させることを契約書上明記している。 	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 4. 特定個人情報ファイル取扱いの委託 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		1) 定めている	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 4. 特定個人情報ファイル取扱いの委託 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の内容		<ul style="list-style-type: none"> ・個人情報の取扱状況等についての書面報告 ・必要と認める場合の個人情報の取扱状況等についての实地調査 ・本県の書面による承諾を除く再委託の禁止 ・目的外利用、第三者への提供の禁止 ・複写又は持ち出しの禁止 ・業務完了後の資料の返還又は廃棄 ・業務従事者への個人情報保護に関して必要な事項の周知 等 	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 4. 特定個人情報ファイル取扱いの委託 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		2) 十分に行っている	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年12月28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 4. 特定個人情報ファイル取扱いの委託 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 具体的な方法		<ul style="list-style-type: none"> 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。 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。 	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 4. 特定個人情報ファイル取扱いの委託 その他の措置の内容		本県の書面による承諾があった場合を除き、再委託を禁止している。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 4. 特定個人情報ファイル取扱いの委託 リスクへの対策は十分か		2) 十分である	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 4. 特定個人情報ファイル取扱いの委託 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		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。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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: 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		1) 記録を残している	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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: 不正な提供・移転が行われるリスク 特定個人情報の提供・移転の記録 具体的な方法		特定個人情報の提供・移転を行う際に、提供・移転記録(日時、操作者等)をシステム上で管理し、記録を保存する。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保存する。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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: 不正な提供・移転が行われるリスク 特定個人情報の提供・移転に関するルール		1) 定めている	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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: 不正な提供・移転が行われるリスク 特定個人情報の提供・移転に関するルール ルールの内容及びルール遵守の確認方法		特定個人情報の提供・移転は、番号法、住基法及び個人情報の保護に関する法律の規定により認められる事項のみとし、住基ネットを使用して提供・移転を行うものとする。操作権限の付与に際しては、利用課所からシステム管理者への利用事務の内容も含めた申請が必要となり、システム管理者は、定期的にシステム内の権限付与の状況を確認する。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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: 不正な提供・移転が行われるリスク その他の措置の内容		「サーバ室等への入室権限」及び「本特定個人情報ファイルを扱うシステムへのアクセス権限」を有する者を厳格に管理し、情報の持ち出しを制限する。 媒体を用いて情報を連携する場合には、必要に応じて媒体へのデータ出力(書き込み)の際に職員が立会う。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの

(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
令和5年12月28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 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：不正な提供・移転が行われるリスク リスクへの対策は十分か		2) 十分である	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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：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。 なお、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、埼玉県他の執行機関への提供及び他部署への移転のため、媒体へ出力する又は回線連携を行う必要がある場合には、逐一出力の記録が残される仕組みを構築する。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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：不適切な方法で提供・移転が行われるリスク リスクへの対策は十分か		2) 十分である	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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：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。 ・誤った相手に提供・移転してしまうリスクへの措置 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担保される。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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：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 リスクへの対策は十分か		2) 十分である	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年12月28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 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。） 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		外部媒体を用いた移転の際には、事前に使用する媒体のウイルスチェックを行う。また、移転する情報にはパスワードを設定する。 また、外部媒体にフラッシュメモリを使用する場合は、暗号化機能、ウイルス対策機能のある機器を使用する。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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）	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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		4) 政府機関ではない	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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 ②安全管理体制		2) 十分に整備している	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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 ③安全管理規程		2) 十分に整備している	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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 ④安全管理体制・規程の職員への周知		2) 十分に周知している	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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 ⑤物理的対策		2) 十分に行っている	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年12月28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 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 ⑤物理的対策 具体的な対策の内容		・附票都道府県サーバの集約センターにおいて、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。また、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。 ・埼玉県においては、代表端末の設置場所、記録媒体の保管場所を施錠管理する。 ・特定個人情報を取り扱うシステムは、インターネットから分離されたネットワーク及び専用パソコンで利用する。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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 ⑥技術的対策		2) 十分に行っている	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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 ⑥技術的対策 具体的な対策の内容		・附票都道府県サーバの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。 ・埼玉県においては業務端末等でウイルス対策ソフトのパターンファイルの更新を定期的に行う。また、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。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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 ⑦バックアップ		2) 十分に行っている	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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 ⑧事故発生時手順の策定・周知		2) 十分に行っている	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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 ⑨過去3年以内に、評価実施期間において、個人情報に関する重大事故が発生したか		2) 発生なし	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 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 ⑩死者の個人番号		2) 保管していない	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年12月28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 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 リスクへの対策は十分か		2) 十分である	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 7. 特定個人情報の保管・消去 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		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、埼玉県等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。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 7. 特定個人情報の保管・消去 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 リスクへの対策は十分か		2) 十分である	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 7. 特定個人情報の保管・消去 リスク3: 特定個人情報消去されずいつまでも存在するリスク 消去手順		2) 定めている	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 7. 特定個人情報の保管・消去 リスク3: 特定個人情報消去されずいつまでも存在するリスク 消去手順 手順の内容		・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、内容の消去、破壊を行うとともに磁気ディスク管理簿を作成しその記録を残す。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28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 7. 特定個人情報の保管・消去 リスク3: 特定個人情報消去されずいつまでも存在するリスク リスクへの対策は十分か		2) 十分である	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの
令和5年12月28日	Ⅳ その他のリスク対策 ② 監査 具体的な内容		・内部監査 住基ネットの利用課所に対して、セキュリティ管理責任者が任命する内部監査員が内部監査を実施する。 監査は機器のセキュリティの状況や媒体、書類の保管状況等を確認の上、聞き取り、実地検証、記録等の検証を行い、監査結果を文書で通知し、必要に応じて改善要求を行う。 改善要求があった場合、利用課所はセキュリティ管理責任者に内部監査改善計画書を提出し承認を得るとともに、改善結果を報告する。 セキュリティ管理責任者は監査対象課所に対して必要に応じてフォローアップ監査を実施し、改善状況を確認する。改善結果に対して不適切な事項がある場合は、利用課所に対して再度改善要求を行う。	事前	令和6年1月に予定される業務アプリケーション適用前に評価を実施したものの