

# 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
2	住民基本台帳ネットワークに係る本人確認情報の管理及び提供等に関する事務 全項目評価書

## 個人のプライバシー等の権利利益の保護の宣言

山口県は、住民基本台帳ネットワークに係る本人確認情報を含む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に適切な措置を講じ、もって個人のプライバシー等の権利利益の保護に取り組んでいることを宣言する。

### 特記事項

- ・住民基本台帳ネットワークにおいて、都道府県は、住民基本台帳法(昭和42年7月25日法律第81号(以下「住基法」という。))に基づき、市町村から住民の本人確認情報に関する通知を受け、都道府県サーバに都道府県知事保存本人確認情報として保有する。都道府県知事保存本人確認情報は、4情報(「氏名・住所・生年月日・性別」をいう。以下同じ。)、個人番号、住民票コード及びこれらの変更情報に限定される。
- ・住民基本台帳ネットワークは専用回線を使用し、地方公共団体情報システム機構(以下「機構」という。)が管理するファイアウォールにより、厳重な通信制御、侵入検知システム(IDS)による侵入検知、通信相手となるコンピュータとの相互認証及び通信を行う際のデータの暗号化を行っているほか、独自のアプリケーションを用いる等、厳格に外部からの侵入防止対策を講じている。また、内部による不正利用を防止するため、操作者及びアクセス権限を限定し、システムの操作履歴を保存する等の対策を講じているほか、システムの操作者には住基法に基づく守秘義務が課せられている。
- ・都道府県サーバは全都道府県分を1箇所(集約センター)に集約し、その運用・監視を機構に委託している。

## 評価実施機関名

山口県知事

## 個人情報保護委員会 承認日【行政機関等のみ】

## 公表日

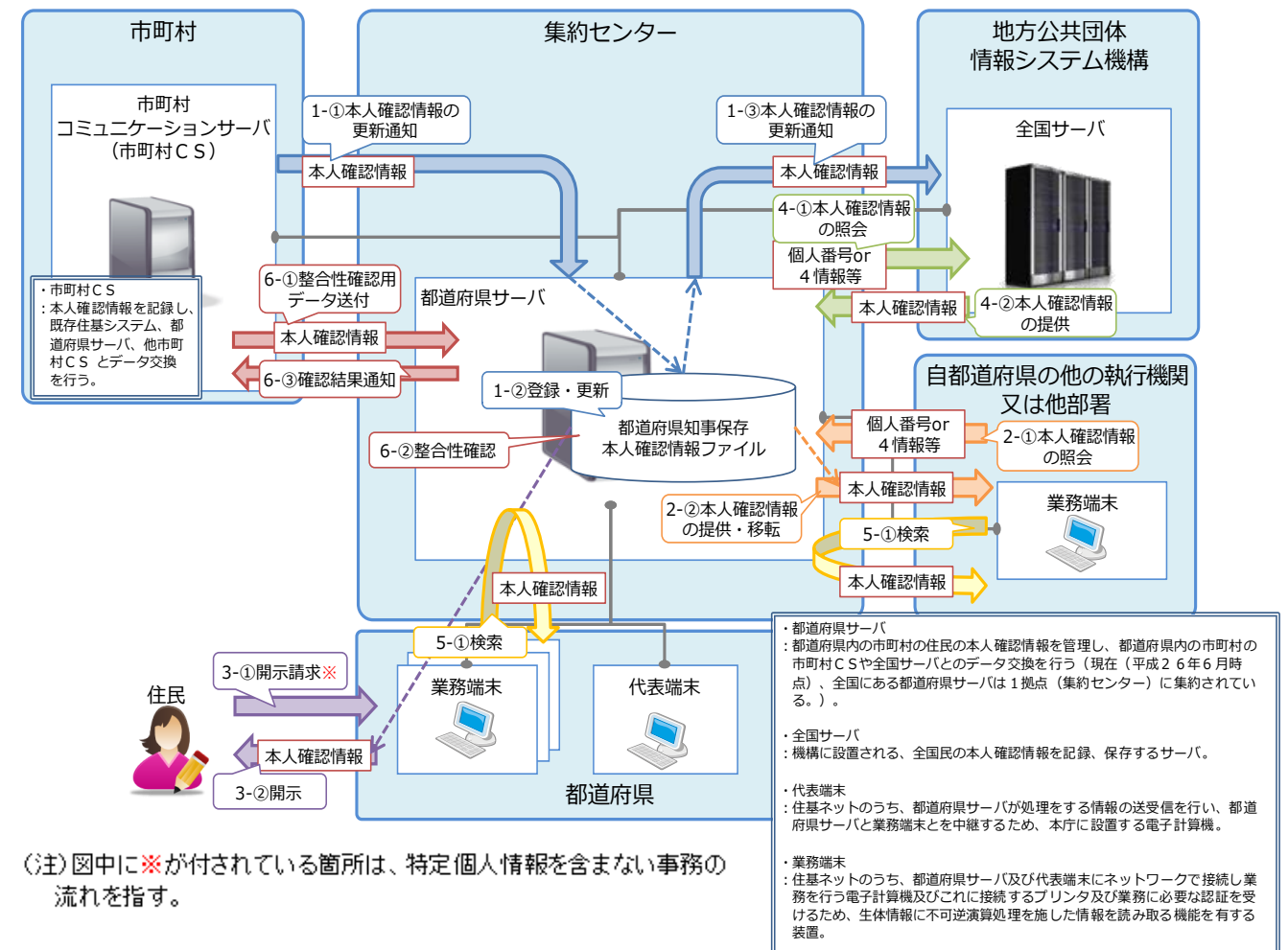
## 項目一覧

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



3. 特定個人情報ファイル名	
都道府県知事保存本人確認情報ファイル	
4. 特定個人情報ファイルを取り扱う理由	
①事務実施上の必要性	<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住民基本台帳ネットワークシステムを用いて市町の区域を越えた住民基本台帳に関する事務「住民基本台帳ネットワークに係る本人確認情報の管理及び提供等に関する事務」の処理を行うため、区域内の住民に係る最新の本人確認情報を管理する。  ②市町からの本人確認情報の更新情報の通知を受けて都道府県知事保存本人確認情報ファイルを更新し、当該更新情報を機構に対して通知する。  ③県の他の執行機関又は他部署からの照会に基づき、本人確認情報を提供・移転する。  ④住民からの請求に基づき、当該個人の本人確認情報を開示する。  ⑤「住民基本台帳ネットワークに係る本人確認情報の管理及び提供等に関する事務」において、本人確認情報を検索する。  ⑥市町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実現が期待されるメリット	<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、これまでに窓口で提出が求められていた行政機関が発行する添付書類(住民票の写し等)の省略が図られ、もって国民の負担軽減(各機関を訪問し、証明書等を入手する金銭的、時間的コストの節約)につながるが見込まれる。</p>
5. 個人番号の利用 ※	
法令上の根拠	<p>住基法</p> <ul style="list-style-type: none"> <li>・第7条(住民票の記載事項)</li> <li>・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)</li> <li>・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)</li> <li>・第30条の7(都道府県知事から機構への本人確認情報の通知等)</li> <li>・第30条の8(本人確認情報の誤りに関する機構の通報)</li> <li>・第30条の11(通知都道府県以外の都道府県の執行機関への本人確認情報の提供)</li> <li>・第30条の15(本人確認情報の利用)</li> <li>・第30条の22(市町村間の連絡調整等)</li> <li>・第30条の32(自己の本人確認情報の開示)</li> <li>・第30条の35(自己の本人確認情報の訂正)</li> </ul>
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	<p>[ 実施しない ]</p> <p style="text-align: right;">&lt;選択肢&gt;  1) 実施する  2) 実施しない  3) 未定</p>
②法令上の根拠	—
7. 評価実施機関における担当部署	
①部署	総合企画部市町課
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



(備考)

1. 本人確認情報の更新に関する事務

- 1-① 市町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、市町より受領した本人確認情報を元に都道府県知事保存本人確認情報ファイルを更新する。
- 1-③ 機構に対し、住民基本台帳ネットワークを介して、本人確認情報の更新を通知する。

2. 県の他の執行機関への情報提供又は他部署への移転

- 2-① 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 県知事において、提示されたキーワードを元に都道府県知事保存本人確認情報ファイルを検索し、照会元に対し、当該個人の本人確認情報を提供・移転する。

※検索対象者が他都道府県の場合は全国サーバに対して検索の要求を行う。

※県の他の執行機関又は他部署に対し、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、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) 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。

## Ⅱ 特定個人情報ファイルの概要

1. 特定個人情報ファイル名	
都道府県知事保存本人確認情報ファイル	
2. 基本情報	
①ファイルの種類 ※	[ システム用ファイル ] <選択肢> 1) システム用ファイル 2) その他の電子ファイル(表計算ファイル等)
②対象となる本人の数	[ 100万人以上1,000万人未満 ] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
③対象となる本人の範囲 ※	区域内の住民(区域内のいずれかの市町において、住基法第5条(住民基本台帳の備付け)に基づき住民基本台帳に記録された住民を指す。) ※住民基本台帳に記録されていた者で、転出等の事由により住民票が消除(死亡による消除を除く。)された者(以下「消除者」という。)を含む。
その必要性	住民基本台帳ネットワークを通じて全国共通の本人確認を行うため、本特定個人情報ファイル(都道府県知事保存本人確認情報ファイル)において区域内の全ての住民の情報を保有し、住民票に記載されている住民全員の記録を常に正確に更新・管理・提供する必要がある。
④記録される項目	[ 10項目以上50項目未満 ] <選択肢> 1) 10項目未満 2) 10項目以上50項目未満 3) 50項目以上100項目未満 4) 100項目以上
主な記録項目 ※	・識別情報 [ <input type="checkbox"/> ] 個人番号 [ <input type="checkbox"/> ] 個人番号対応符号 [ <input type="checkbox"/> ] その他識別情報(内部番号) ・連絡先等情報 [ <input type="checkbox"/> ] 4情報(氏名、性別、生年月日、住所) [ <input type="checkbox"/> ] 連絡先(電話番号等) [ <input type="checkbox"/> ] その他住民票関係情報 ・業務関係情報 [ <input type="checkbox"/> ] 国税関係情報 [ <input type="checkbox"/> ] 地方税関係情報 [ <input type="checkbox"/> ] 健康・医療関係情報 [ <input type="checkbox"/> ] 医療保険関係情報 [ <input type="checkbox"/> ] 児童福祉・子育て関係情報 [ <input type="checkbox"/> ] 障害者福祉関係情報 [ <input type="checkbox"/> ] 生活保護・社会福祉関係情報 [ <input type="checkbox"/> ] 介護・高齢者福祉関係情報 [ <input type="checkbox"/> ] 雇用・労働関係情報 [ <input type="checkbox"/> ] 年金関係情報 [ <input type="checkbox"/> ] 学校・教育関係情報 [ <input type="checkbox"/> ] 災害関係情報 [ <input type="checkbox"/> ] その他 ( )
その妥当性	・個人番号、4情報、その他住民票関係情報:住民基本台帳ネットワーク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1日
⑥事務担当部署	総合企画部市町課

### 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 ( ) <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、市町がそれをまず探知した上で、全国的なシステムである住民基本台帳ネットワークで管理する必要があるため、市町から県へ、県から機構へと通知がなされることとされているため。								
⑤本人への明示	県知事が当該市町の区域内の住民の本人確認情報を入手することについて、住基法第30条の6(市町村長から都道府県知事への本人確認情報の通知等)に明示されている。								
⑥使用目的 ※	住民基本台帳ネットワークシステムを通じて全国共通の本人確認を行うため、本特定個人情報ファイル(都道府県知事保存本人確認情報ファイル)において区域内の全ての住民の情報を保有し、住民票に記載されている住民全員の記録を常に正確に更新・管理・提供する。								
	変更の妥当性	—							
⑦使用の主体	使用部署 ※	総合企画部市町課							
	使用者数	[ 10人未満 ] <table style="display: inline-table; vertical-align: middle; margin-left: 10px;"> <tr> <td colspan="2" style="text-align: center;">＜選択肢＞</td> </tr> <tr> <td style="width: 50%;">1) 10人未満</td> <td style="width: 50%;">2) 10人以上50人未満</td> </tr> <tr> <td>3) 50人以上100人未満</td> <td>4) 100人以上500人未満</td> </tr> <tr> <td>5) 500人以上1,000人未満</td> <td>6) 1,000人以上</td> </tr> </table>	＜選択肢＞		1) 10人未満	2) 10人以上50人未満	3) 50人以上100人未満	4) 100人以上500人未満	5) 500人以上1,000人未満
＜選択肢＞									
1) 10人未満	2) 10人以上50人未満								
3) 50人以上100人未満	4) 100人以上500人未満								
5) 500人以上1,000人未満	6) 1,000人以上								
⑧使用方法 ※	①市町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(既存住民基本台帳ネットワークシステム→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)。 ②県の他の執行機関又は他部署からの本人確認情報の照会要求を受け(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→県の他の執行機関又は他部署)。 ③住民からの開示請求に基づき(住民→県窓口→都道府県サーバ)、当該住民の本人確認情報を都道府県知事保存本人確認情報ファイルから抽出し、書面により提供する(都道府県サーバ→帳票出力→住民)。 ④4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。 ⑤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、市町から本人確認情報を受領し(市町村CS→都道府県サーバ)、当該本人確認情報を用いて都道府県知事保存本人確認情報ファイルに記録された本人確認情報の整合性確認を行う。								
	情報の突合 ※	・都道府県知事保存本人確認情報ファイルを更新する際に、受領した本人確認情報に関する更新データと都道府県知事保存本人確認情報ファイルを、住民票コードをもとに突合する。 ・県の他の執行機関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提供する情報の対象となる本人の数	<input type="checkbox"/> 100万人以上1,000万人未満 ] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤提供する情報の対象となる本人の範囲	「2. ③対象となる本人の範囲」と同上
⑥提供方法	<input type="checkbox"/> 情報提供ネットワークシステム <input type="checkbox"/> 専用線 <input type="checkbox"/> 電子メール <input type="checkbox"/> 電子記録媒体(フラッシュメモリを除く。) <input type="checkbox"/> フラッシュメモリ <input type="radio"/> 紙 <input type="radio"/> その他 (住民基本台帳ネットワークシステム )
⑦時期・頻度	県の他の執行機関から要求があった都度、随時。

<b>移転先1</b>		県の他部署(税務課など)	
①法令上の根拠		住基法第30条の15第1項(本人確認情報の利用)	
②移転先における用途		住基法別表第五に掲げる、都道府県知事において都道府県知事保存本人確認情報の利用が認められた事務の処理及び「本人確認情報の利用及び提供に関する条例」(平成19年3月13日県条例第2号)に定める事務の処理に用いる。	
③移転する情報		住民票コード、氏名、生年月日、性別、住所、個人番号、異動事由、異動年月日 ※住民票コードについては、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		<input type="checkbox"/> 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"/> 専用線 <input type="checkbox"/> 電子メール <input type="checkbox"/> 電子記録媒体(フラッシュメモリを除く。) <input type="checkbox"/> フラッシュメモリ <input type="checkbox"/> 紙 <input checked="" type="checkbox"/> その他 (住民基本台帳ネットワークシステム)	
⑦時期・頻度		県の他部署から要求があった都度、随時。	
<b>6. 特定個人情報の保管・消去</b>			
①保管場所 ※		・セキュリティゲートにて入退館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、施錠管理及び入退室管理(監視カメラを設置してサーバ設置場所への入退室者を特定・管理)を行っている部屋に設置したサーバ内に保管する。サーバへのアクセスはID/パスワードによる認証が必要となる。 ・県においては、端末及び記録媒体を施錠管理された部屋で保管し、ログインは生体認証方式としている。	
②保管期間	期間	<input type="checkbox"/> 20年以上 <選択肢> 1) 1年未満 2) 1年 3) 2年 4) 3年 5) 4年 6) 5年 7) 6年以上10年未満 8) 10年以上20年未満 9) 20年以上 10) 定められていない	
	その妥当性	・住民票の記載の修正後の本人確認情報は、新たに記載の修正の通知を受けるまで保管する。 ・住民票の記載の修正前の本人確認情報(履歴情報)及び削除者の本人確認情報は、住基法施行令第30条の6(都道府県における本人確認情報の保存期間)に定める期間(150年間)保管する。	
③消去方法		都道府県知事保存本人確認情報ファイルに記録されたデータをシステムにて自動判別し、消去する。	
<b>7. 備考</b>			
—			

## (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

(機構が提供する住民基本台帳ネットワークシステムのデータ項目)

- 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

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

1. 特定個人情報ファイル名	
都道府県知事保存本人確認情報ファイル	
2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）	
リスク1： 目的外の入手が行われるリスク	
対象者以外の情報の入手を防止するための措置の内容	都道府県知事保存本人確認情報ファイルにおける特定個人情報の入手手段は、市町村CSからの本人確認情報更新要求の際に通知される本人確認情報に限定される。この場合、市町村CSから対象者以外の情報が通知されてしまうことがリスクとして想定されるが、制度上、対象者の真正性の担保は市町側の確認に委ねられるため、市町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市町村CSIに限定する。
リスクへの対策は十分か	[ 十分である ] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3： 入手した特定個人情報が不正確であるリスク	
入手の際の本人確認の措置の内容	住民の異動情報の届出等を受け付ける市町の窓口において、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	市町において真正性が確認された情報を市町村CSを通じて入手できることを、システムで担保する。
特定個人情報の正確性確保の措置の内容	・システム上、本人確認情報更新の際に、論理チェックを行う（例えば、現存する住民に対して転入を異動事由とする更新が行われようとした場合や、転居を異動事由とする更新の際に住所以外の更新が行われようとした場合に当該処理をエラーとする）仕組みとする。 ・入手元である市町村CSにおいて、項目（フォーマット、コード）のチェックを実施する。
その他の措置の内容	—
リスクへの対策は十分か	[ 十分である ] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	・機構が作成・配付する専用のアプリケーション（※）を用いることにより、入手の際の特定個人情報の漏えい・紛失の防止に努める。 ・市町村CSと接続するネットワーク回線に専用回線を用いる、情報の暗号化を実施する等の措置を講じる。 ・特定個人情報の入手は、システム上自動処理にて行われるため、操作者は存在せず人為的なアクセスが行われることはない。 ※都道府県サーバのサーバ上で稼動するアプリケーション。都道府県内の市町村の住民の本人確認情報を管理し、都道府県内の市町村の市町村CSや全国サーバとのデータ交換を行う。データの安全保護対策、不正アクセスの防止策には、最新の認証技術や暗号化技術を採用し、データの盗聴、改ざん、破壊及び盗難、端末の不正利用及びびなりすまし等を防止する。
リスクへの対策は十分か	[ 十分である ] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置	
—	

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	庁内システムと都道府県サーバとの接続は行わない。
その他の措置の内容	—
リスクへの対策は十分か	[ 十分である ] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2: 権限のない者(元職員、アクセス権限のない職員等)によって不正に使用されるリスク	
ユーザ認証の管理	[ 行っている ] <選択肢> 1) 行っている 2) 行っていない
具体的な管理方法	・生体認証(静脈認証)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	・権限の付与にあたっては、事前にシステム管理者への協議を行い承認を要する。 ・権限の有効期間を翌年度末とする。異動や退職により業務端末を利用する必要がなくなった場合、システム管理者に報告し権限を抹消することとしている。 ・定期的に操作者の所属・氏名・権限を記載した管理簿名簿と職員の在籍状況の確認を行い、整合性が図れない場合、実態確認を行い市町課にて権限の削除を行う。
アクセス権限の管理	[ 行っている ] <選択肢> 1) 行っている 2) 行っていない
具体的な管理方法	・操作者に対しては業務上必要な限度での権限を付与する。 ・権限の付与にあたっては、事前協議を行い、システム管理者の承認を得ることを要する。 ・操作者の所属・氏名・権限を記載した管理簿を作成し、定期的に確認作業を行う。 ・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	・操作者は業務端末の使用にあたって、使用簿に利用日時・所属・氏名・検索回数を記載し、セキュリティ責任者の決裁を受ける。 ・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。 ・不正な操作が無いことについて、操作履歴により適時確認する。 ・操作履歴の確認により本人確認情報の検索に関して不正操作の疑いがある場合には、申請文書等との整合性を確認する。
その他の措置の内容	—
リスクへの対策は十分か	[ 十分である ] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3: 従業者が事務外で使用するリスク	
リスクに対する措置の内容	・システムの操作履歴(操作ログ)を記録する。 ・自己点検時に、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研修会において、操作者へリスクに係る説明を実施し、事務外利用の禁止等について周知を行う。 ・研修を受講していない職員のシステム利用を禁止する。
リスクへの対策は十分か	[ 十分である ] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク4: 特定個人情報ファイルが不正に複製されるリスク	
リスクに対する措置の内容	・システム上、管理権限を与えられた者以外、情報の複製は行えない。 ・検索結果の帳票出力にあたっては、出力日時・使用目的・検索者等の記録を残し、セキュリティ責任者の決裁を受ける。
リスクへの対策は十分か	[ 十分である ] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

#### 特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置

その他、特定個人情報の使用にあたり、以下の措置を講じる。

- ・スクリーンセーバー等を利用して、長時間(10分以上)にわたり本人確認情報を表示させたままにしない。
- ・離席する際には、シャットダウンする。
- ・業務端末のディスプレイを来庁者から見えない位置に置く。
- ・システム操作者は本人確認情報が表示された画面のハードコピーは必要以上に取らない。また、必要性がなくなれば速やかに処分する。





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"> <li>・再委託先との契約で、秘密保持義務を課すことを義務づけている。</li> <li>・再委託する業務は直接本人確認情報に関わらない業務を対象とする。</li> <li>・委託元は、委託を受けた者に対して、委託元自らが果たすべき安全管理措置と同等の措置が講じられるよう必要かつ適切な監督を行っている。再委託を行う場合は、委託元がその必要性を厳しく審査し、再委託先に対して、委託先と同等の安全管理措置を義務付け、必要かつ適切な監督を行っている。</li> <li>・重要機能室での現地作業は、入館前に入館申請を行い、職員の事前了解の下作業を行う。</li> <li>・作業日報及び作業者名簿に基づいた入室管理により確認する。</li> </ul>
その他の措置の内容	—	
リスクへの対策は十分か	[ 十分である ]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		
—		

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		[ ] 提供・移転しない
リスク1: 不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録	[ 記録を残している ]	<選択肢> 1) 記録を残している      2) 記録を残していない
具体的な方法	<ul style="list-style-type: none"> <li>・特定個人情報(個人番号、4情報等)の提供・移転を行う際に、提供・移転の記録(提供・移転日時、操作者等)をシステム上で管理し、7年分保存する。なお、システム上、提供・移転に係る処理を行ったものの提供・移転が認められなかった場合についても記録を残す。</li> <li>・業務端末を利用し、本人確認情報の照会を行う場合は、使用簿に日時・所属・名前・検索件数などを記載する。</li> </ul>	
特定個人情報の提供・移転に関するルール	[ 定めている ]	<選択肢> 1) 定めている      2) 定めていない
ルール内容及びルール遵守の確認方法	番号法及び住基法並びに個人情報保護条例の規定に基づき認められる特定個人情報の提供・移転について、特定個人情報の提供・移転を行う。また、提供・移転先の職員に対しては、定期的に研修を行う。	
その他の措置の内容	<ul style="list-style-type: none"> <li>・「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する。</li> <li>・媒体を用いて情報を連携する場合には、媒体へのデータ出力(書き込み)については市町課職員が行う。</li> </ul>	
リスクへの対策は十分か	[ 十分である ]	<選択肢> 1) 特に力を入れている      2) 十分である 3) 課題が残されている
リスク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	市町村CS・全国サーバと都道府県サーバ間の通信では相互認証を実施しているため、認証できない相手先への情報の提供はなされないことがシステム上担保される。また、県の他の執行機関への提供及び他の部署への移転のため、媒体へ出力する必要がある場合には、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"> <li>○誤った情報を提供・移転してしまうリスクへの措置</li> <li>・システム上、照会元から指定された検索条件に基づき得た結果を適切に提供・移転することを担保する。</li> <li>○誤った相手に提供・移転してしまうリスクへの措置</li> <li>・市町村CS・全国サーバと都道府県サーバ間の通信では相互認証を実施しているため、認証できない相手先への情報の提供はなされないことがシステム上担保される。</li> </ul>	
リスクへの対策は十分か	[ 十分である ]	<選択肢> 1) 特に力を入れている      2) 十分である 3) 課題が残されている
特定個人情報の提供・移転(委託や情報提供ネットワークシステムを通じた提供を除く。)におけるその他のリスク及びそのリスクに対する措置		

6. 情報提供ネットワークシステムとの接続		[○] 接続しない(入手)	[○] 接続しない(提供)
リスク1: 目的外の入手が行われるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク2: 安全が保たれない方法によって入手が行われるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[ ]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク3: 入手した特定個人情報 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		・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。 ・都道府県サーバの集約センターにおいては、サーバ設置場所、記録媒体の保管場所を施錠管理する。 ・県においては、端末設置場所、記録媒体の保管場所を施錠管理する。
⑥技術的対策	[ 十分に行っている ]	<選択肢> 1) 特に力を入れて行っている    2) 十分に行っている 3) 十分に行っていない
具体的な対策の内容		・ウイルス対策ソフトの定期的パターン更新を行う。 ・庁内のネットワークにおいて、ファイアウォールを設置している。 ・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。
⑦バックアップ	[ 十分に行っている ]	<選択肢> 1) 特に力を入れて行っている    2) 十分に行っている 3) 十分に行っていない
⑧事故発生時手順の策定・周知	[ 十分に行っている ]	<選択肢> 1) 特に力を入れて行っている    2) 十分に行っている 3) 十分に行っていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	[ 発生なし ]	<選択肢> 1) 発生あり    2) 発生なし
その内容		
再発防止策の内容		
⑩死者の個人番号	[ 保管している ]	<選択肢> 1) 保管している    2) 保管していない
具体的な保管方法		生存する個人の個人番号とともに、死亡による消除後、住基法施行令第30条の6(都道府県における本人確認情報の保存期間)に定める期間(150年間)保管する。
その他の措置の内容		—
リスクへの対策は十分か	[ 十分である ]	<選択肢> 1) 特に力を入れている    2) 十分である 3) 課題が残されている

リスク2: 特定個人情報古い情報のまま保管され続けるリスク	
リスクに対する措置の内容	市町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: 特定個人情報消去されずいつまでも存在するリスク	
消去手順	[ 定めている ] <選択肢> 1) 定めている 2) 定めていない
手順の内容	<ul style="list-style-type: none"> <li>・住民票の記載の修正前の本人確認情報(履歴情報)及び消除者の本人確認情報は法令(住基法施行令第30条の6)に定める保存期間を経過した後に系統的に消去する。</li> <li>・磁気ディスクの廃棄時は、要領・手順書等に基づき、専用ソフトによる消去、物理的粉碎等でデータ読み取り不可の状態にするとともに、磁気ディスク管理簿にその記録を残す。</li> <li>・帳票については、要領・手順書等に基づき、帳票管理簿等を作成し、受渡し、保管及び廃棄の運用が適切になされていることを適時確認するとともに、その記録を残す。</li> <li>・廃棄時には、要領・手順書等に基づき、裁断、溶解等を行う。</li> </ul>
その他の措置の内容	—
リスクへの対策は十分か	[ 十分である ] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置	
—	

## IV その他のリスク対策 ※

1. 監査	
①自己点検	[ 十分に行っている ] <選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
具体的なチェック方法	年に1回、住民基本台帳ネットワークシステムを利用する全所属に対し、セキュリティに関するチェックリストを配布し、自己点検を実施する。
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	定期的に以下の観点で経済産業省の情報セキュリティ監査企業台帳に登録された企業の有資格者による外部監査を実施する。 ・組織体制 ・情報資産の分類と管理方法 ・物理的セキュリティ ・人的セキュリティ ・技術的セキュリティ ・運用
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	システム利用職員及びセキュリティ責任者に対して、住民基本台帳ネットワークの利用について必要な知識の習得及びセキュリティに関する意識向上のため、毎年度当初に研修を実施している。
3. その他のリスク対策	
—	





## VI 評価実施手続

1. 基礎項目評価	
①実施日	
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	山口県情報公開センター、各地方県民相談室における閲覧及び県HPへの掲載、報道機関への発表にてパブリック・コメント(意見募集)の掲載を行い、電子メール、FAX、郵送の手段にて意見を受け付けることとした。
②実施日・期間	令和3年8月10日～令和3年9月9日
③期間を短縮する特段の理由	期間短縮なし
④主な意見の内容	
⑤評価書への反映	
3. 第三者点検	
①実施日	
②方法	
③結果	
4. 個人情報保護委員会の承認【行政機関等のみ】	
①提出日	
②個人情報保護委員会による審査	

### (別添3)変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
	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	①住基ネットを用いて市町の区域を越えた住民基本台帳に関する事務「住民基本台帳ネットワークに係る本人確認情報の管理及び提供等に関する事務」の処理を行うため、区域内の住民に係る最新の本人確認情報を管理する。	①住民基本台帳ネットワークシステムを用いて市町の区域を越えた住民基本台帳に関する事務「住民基本台帳ネットワークに係る本人確認情報の管理及び提供等に関する事務」の処理を行うため、区域内の住民に係る最新の本人確認情報を管理する。	事後	重要な変更にあたらない変更
	I 基本情報 4. 特定個人情報ファイルを取り扱う理由 ①事務実施上の必要性	③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する。	③県の他の執行機関又は他部署からの照会に基づき、本人確認情報を提供・移転する。	事後	重要な変更にあたらない変更
	I 基本情報 5. 個人番号の利用 法令上の根拠	住基法(平成25年5月31日法律第28号施行時点)	住基法	事後	番号整備法が施行されたことによる修正
	I 基本情報 5. 個人番号の利用 法令上の根拠	・第30条の13(都道府県の条例による本人確認情報の提供)	削除	事後	該当する事務で個人番号の利用は行っていないため
	I 基本情報 5. 個人番号の利用 法令上の根拠	記載なし	・第30条の22(市町村間の連絡調整等)	事後	番号整備法が施行されたことによる修正
	I 基本情報 (別添1)事務の内容 図	記載なし	(注) 図中に※が付されている箇所は、特定個人情報を含まない事務の流れを指す。	事後	記載内容の正確性向上のため
	I 基本情報 (別添1)事務の内容 (備考)2. 県の他の執行機関への情報提供又は他部署への移転 (注2)	具体的には、都道府県サーバの代表端末又は業務端末と庁内システム(宛名管理システムを含む。)のみがアクセス可能な領域(フォルダ)を設け、当該領域内で照会要求ファイル及び照会結果ファイルの授受を行う。	削除	事後	回線連携は行っていないため
	I 基本情報 (別添1)事務の内容 (備考)3. 本人確認情報の開示に関する事務	住民より本人確認情報の開示請求を受け付ける。	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	記載内容の正確性向上のため
	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	平成27年6月1日	事後	記載内容の正確性向上のため

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
	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 ⑥使用目的	住基ネットを通じて全国共通の本人確認を行うため、本特定個人情報ファイル(都道府県知事保存本人確認情報ファイル)において区域内の全ての住民の情報を保有し、住民票に記載されている住民全員の記録を常に正確に更新・管理・提供する。	住民基本台帳ネットワークシステムを通じて全国共通の本人確認を行うため、本特定個人情報ファイル(都道府県知事保存本人確認情報ファイル)において区域内の全ての住民の情報を保有し、住民票に記載されている住民全員の記録を常に正確に更新・管理・提供する。	事後	重要な変更にあたらない変更
	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 委託事項1 ⑤委託先名の確認方法	山口県情報公開条例に基づく開示請求	県のホームページにて業務委託にかかる契約情報を公表している。	事後	重要な変更にあたらない変更
	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 委託事項1 ⑧再委託の許諾方法	書面による許諾	書面による承諾	事後	重要な変更にあたらない変更
	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 委託事項2 ③委託先における取扱者数	10人未満	10人以上50人未満	事後	重要な変更にあたらない変更
	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 委託事項2 ⑤委託先名の確認方法	山口県情報公開条例に基づく開示請求	県のホームページにて業務委託にかかる契約情報を公表している。	事後	重要な変更にあたらない変更
	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 委託事項2 ⑥委託先名	株式会社NTTフィールドテクノ中国支店 山口営業所(YSN運営センタ)	NTTビジネスソリューションズ株式会社 山口ビジネス営業部(YSN運営センタ)	事後	重要な変更にあたらない変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
	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 委託事項2 ⑧再委託の許諾方法	原則として再委託を禁止しているが、やむを得ず再委託を実施する必要がある場合は、再委託する業務内容等について事前に書面により委託者の許諾を得ることとしている。	原則として再委託を禁止しているが、やむを得ず再委託を実施する必要がある場合は、再委託する業務内容等について事前に書面により委託者の承諾を得ることとしている。	事後	重要な変更にあたらない変更
	II 特定個人情報ファイルの概要 5. 特定個人情報の提供・移転(委託に伴うものを除く。) 提供先2 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	「2. ③対象となる本人の範囲」と同上	事後	重要な変更にあたらない変更
	II 特定個人情報ファイルの概要 5. 特定個人情報の提供・移転(委託に伴うものを除く。) 提供先3 ①法令上の根拠	住基法第30条の13(都道府県の条例による本人確認情報の提供)	削除	事後	当該事務の法令上の根拠ではないため
	II 特定個人情報ファイルの概要 5. 特定個人情報の提供・移転(委託に伴うものを除く。) 提供先3 ③提供する情報	※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	経過措置が終了したため
	II 特定個人情報ファイルの概要 5. 特定個人情報の提供・移転(委託に伴うものを除く。) 提供先3 ⑥提供方法	[ <input type="radio"/> ]電子記録媒体(フラッシュメモリを除く。) [ <input type="checkbox"/> ]紙	[ <input type="checkbox"/> ]電子記録媒体(フラッシュメモリを除く。) [ <input type="radio"/> ]紙	事後	重要な変更にあたらない変更 ※一括提供方式は行わないが、帳票出力は行う場合があるため
	II 特定個人情報ファイルの概要 5. 特定個人情報の提供・移転(委託に伴うものを除く。) 移転先1 ①法令上の根拠	住基法第30条の13(都道府県の条例による本人確認情報の提供)	削除	事後	当該事務の法令上の根拠ではないため

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
	II 特定個人情報ファイルの概要 5. 特定個人情報の提供・移転(委託に伴うものを除く。)移転先1 ②移転先における用途	住基法別表第五に掲げる、都道府県知事において都道府県知事保存本人確認情報の利用が認められた事務の処理及び「本人確認情報の利用及び提供に関する条例」(平成19年3月13日県条例第2号)に用いる。 ※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。	住基法別表第五に掲げる、都道府県知事において都道府県知事保存本人確認情報の利用が認められた事務の処理及び「本人確認情報の利用及び提供に関する条例」(平成19年3月13日県条例第2号)に定める事務の処理に用いる。	事後	記載内容の正確性向上のため ※以降は③移転する情報に関する記載であるため削除
	II 特定個人情報ファイルの概要 5. 特定個人情報の提供・移転(委託に伴うものを除く。)移転先1 ③移転する情報	※住民票コードについては、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	経過措置が終了したため
	II 特定個人情報ファイルの概要 5. 特定個人情報の提供・移転(委託に伴うものを除く。)(別添2)特定個人情報ファイル記録項目	12 保存期限フラグ	12 保存期間フラグ	事後	重要な変更にとらならない変更
	II 特定個人情報ファイルの概要 5. 特定個人情報の提供・移転(委託に伴うものを除く。)(別添2)特定個人情報ファイル記録項目	記載なし	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の一部を改正する政令が公布されたことによる修正
	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。	・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。	事後	重要な変更にとらならない変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
	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り漏れ・紛失するリスク リスクに対する措置の内容	記載なし	・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。	事後	記載内容の正確性向上のため
	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	・不正アクセスを分析するために、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。	・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。	事後	記載内容の正確性向上のため
	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記録 具体的な方法	・操作者は業務端末の使用にあたって、使用簿に利用日時・所属・氏名・検索回数を記録する。	・操作者は業務端末の使用にあたって、使用簿に利用日時・所属・氏名・検索回数を記載し、セキュリティ責任者の決裁を受ける。	事後	記載内容の正確性向上のため
	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	・操作者へリスクに係る説明を実施し、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研修会において、事務外利用の禁止等について周知を行う。	・自己点検時に、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研修会において、操作者へリスクに係る説明を実施し、事務外利用の禁止等について周知を行う。	事後	記載内容の正確性向上のため
	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	・検索結果の帳票出力にあたっては、出力日時・使用目的・検索者等を記録を残す。	・検索結果の帳票出力にあたっては、出力日時・使用目的・検索者等の記録を残し、セキュリティ責任者の決裁を受ける。	事後	記載内容の正確性向上のため

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
	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	・規約書において業務により知り得た個人情報の目的外使用及び第三者への提供を禁止している。	・契約書において業務により知り得た個人情報の目的外使用及び第三者への提供を禁止している。	事後	重要な変更にあたらない変更
	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	記載なし	・委託先(再委託先を含む。)に送付する特定個人情報ファイルは暗号化されているため、委託先(再委託先を含む。)がファイル内の特定個人情報にアクセスしないシステム設計としている。	事後	記載内容の正確性向上のため
	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 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	記載なし	・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。	事後	記載内容の正確性向上のため
	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	・業務端末を利用し、本人確認情報の照会を行う場合は、業務端末管理簿に日時・所属・名前・検索件数などを記載する。	・業務端末を利用し、本人確認情報の照会を行う場合は、使用簿に日時・所属・名前・検索件数などを記載する。	事後	重要な変更にあたらない変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
	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する。 ・媒体を用いて情報を連携する場合には、媒体へのデータ出力(書き込み)の際には職員が立ち会う。	・「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する。 ・媒体を用いて情報を連携する場合には、媒体へのデータ出力(書き込み)については市町課職員が行う。	事後	記載内容の正確性向上のため
	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 リスクに対する措置の内容	また、市町CSとの整合処理を定期的実施し、保存する本人確認情報が最新であるかどうかを確認する。	また、市町村CSとの整合処理を定期的実施し、保存する本人確認情報が最新であるかどうかを確認する。	事後	重要な変更にあたらない変更
	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 手順の内容	・磁気ディスクの廃棄時は、要領・手順書等に基づき、内容の消去、破壊等を行うとともに、磁気ディスク管理簿にその記録を残す。また、専用ソフトによるフォーマット、物理的粉碎等を行うことにより、内容を読みだすことができないようにする。	・磁気ディスクの廃棄時は、要領・手順書等に基づき、専用ソフトによる消去、物理的粉碎等でデータ読み取り不可の状態にするとともに、磁気ディスク管理簿にその記録を残す。	事後	重要な変更にあたらない変更
	Ⅳ その他のリスク対策 1. 監査 ①自己点検 具体的なチェック方法	・評価書の記載内容に基づき職員が運用状況の確認を行う。 ・代表端末においては自己点検チェックリスト項目に沿って自己点検を実施する。 ・各業務端末においては、各自が自己点検を実施するとともに、「評価書の記載内容通りの運用がなされていること」に係る内容を新たにチェック項目に加えて、運用状況を確認する。	年に1回、住民基本台帳ネットワークシステムを利用する全所属に対し、セキュリティに関するチェックリストを配布し、自己点検を実施する。	事後	重要な変更にあたらない変更
	Ⅳ その他のリスク対策 2. 従業者に対する教育・啓発 具体的な方法	新たなシステム利用者に対して、住民基本台帳ネットワークの利用について必要な知識の習得及びセキュリティに関する意識向上のため、研修を実施している。	システム利用職員及びセキュリティ責任者に対して、住民基本台帳ネットワークの利用について必要な知識の習得及びセキュリティに関する意識向上のため、毎年度当初に研修を実施している。	事後	記載内容の正確性向上のため