

特定個人情報保護評価書(全項目評価書)

評価書番号	評価書名
1	島根県が行う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

島根県知事は、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の管理及び提供等に関する事務における特定個人情報ファイルの取扱いにあたり、特定個人情報ファイルの取扱いが個人のプライバシー等の権利利益に影響を及ぼしかねないことを認識し、特定個人情報の漏えいその他の事態を発生させるリスクを軽減させるため適切な措置を講じ、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システムにおいて、島根県は、住民基本台帳法(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、島根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システム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を行うなど厳格な不正アクセス対策を講じている。また、内部による不正利用の防止のため、システム操作者に住基法に基づく守秘義務を課し、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。
- ・島根県サーバは全都道府県分と共に1カ所(都道府県サーバ集約センター)に集約しており、その運用・監視を機構に委託している。
- ・島根県において、住民基本台帳ネットワークシステムの運用にあたり、運用管理規程等を定めており、住民基本台帳ネットワークシステムの運用が始まって以来、適切に個人情報を取り扱っている。住民基本台帳ネットワークにおいて、平成27年度から保有する情報に個人番号が加わったが、基本的な業務やシステムは個人番号を保有する前と大きな変更は無い。今後も住民基本台帳ネットワークシステムを利用する職場への実地監査の実施や、情報セキュリティポリシーの変更への対応等、引き続き厳格な運用に努める。

評価実施機関名

島根県知事

個人情報保護委員会 承認日【行政機関等のみ】

公表日

令和4年3月14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>島根県では、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住民基本台帳ネットワークシステムを用いて市町村の区域を越えた住民基本台帳に関する事務(住民基本台帳ネットワークシステム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島根県の他の執行機関又は他部署からの照会に基づき、本人確認情報を提供・移転する。 ④住民からの請求に基づき、当該個人の本人確認情報を開示する ⑤住民基本台帳ネットワークに係る本人確認情報の管理及び提供等に関する事務において、本人確認情報を検索する。 ⑥市町村において保存する本人確認情報との整合性を確認する。</p>
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/住民の負担軽減(各機関を訪問し、証明書等を入手する金銭的、時間的コストの節約)につながるが見込まれる。</p>
5. 個人番号の利用 ※	
法令上の根拠	<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)
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;"><選択肢> 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	島根県地域振興部市町村課
②所属長の役職名	島根県地域振興部市町村課長
8. 他の評価実施機関	

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	[10万人以上100万人未満] <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 ※	島根県内の住民(島根県内のいずれかの市町村において、住基法第5条(住民基本台帳の備付け)に基づき住民基本台帳に記録された住民を指す) ※住民基本台帳に記録されていた者で転出等の事由により住民票が消除(死亡による消除を除く。)された者(以下「消除者」という。)を含む
その必要性	住民基本台帳ネットワークシステムを通じて全国共通の本人確認を行うため、都道府県知事保存本人確認情報ファイルにおいて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システムを通じて本人確認を行うために必要な情報として、住民票の記載等に係る本人確認情報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10月5日
⑥事務担当部署	島根県地域振興部市町村課

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 [<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"/> 電子メール [<input type="checkbox"/> 専用線 [<input type="checkbox"/> 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を通して入手する。)
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、市町村がそれをまず探知した上で、全国的なシステムである住民基本台帳ネットワークシステムで管理する必要があるため、市町村から島根県へ、島根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	島根県知事が当該市町村の区域内の住民の本人確認情報を入手することについて、住基法第30条の6(市町村長から都道府県知事への本人確認情報の通知等)に明示されている。
⑥使用目的 ※	住民基本台帳ネットワークシステムを通じて全国共通の本人確認を行うため、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 ー
⑦使用の主体	使用部署 ※ 地域振興部市町村課
	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→島根県サーバ)、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(島根県サーバ→全国サーバ)。 ・島根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を受け(島根県の他の執行機関又は他部署→島根県サーバ)、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、該当する本人確認情報を照会元へ提供・移転する(島根県サーバ→島根県の他の執行機関)。 ・住民からの開示請求に応じ(住民→島根県窓口→島根県サーバ)、開示請求をした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、書面により当該住民に提供する。(島根県サーバ→帳票出力→住民)。 ・4情報(氏名、住所、性別、生年月日)の組合せをキーに都道府県知事保存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→島根県サーバ)、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を確認する。
	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係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とを、住民票コードをもとに突合する。 ・島根県の他の執行機関又は他部署からの照会に応じて本人確認情報を提供する際に、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。
	権利益に影響を与え得る決定 ※ 該当無し
⑨使用開始日	平成27年10月5日

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※	[委託する] <選択肢> 1) 委託する 2) 委託しない (3) 件	
委託事項1	島根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拠点に集約したことに伴い、島根県サーバの運用及び監視に関する業務を、集約センター運用者に委託する。 委託する業務は、本人確認情報に直接係わらない(本人確認情報に直接アクセスできず、閲覧・更新・削除等を行わない)業務を対象とする。	
②取扱いを委託する特定個人情報ファイルの範囲	[特定個人情報ファイルの全体] <選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部	
対象となる本人の数	[10万人以上100万人未満] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上	
対象となる本人の範囲 ※	「2. ③対象となる本人の範囲」と同上	
その妥当性	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)が保存されている島根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、島根県サーバでは特定個人情報ファイルの全体を保有しているが、委託内容は、直接本人確認情報に係わらない業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業務は実施せず、権限も付与しない。 また、委託業者が利用する端末の定義等については以下のとおり。 (運用端末:島根県サーバへのバッチ処理の開始/終了指示等の運用処理を行う)	
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 type="checkbox"/>] 専用線 [<input type="checkbox"/>] 電子メール [<input type="checkbox"/>] 電子記録媒体(フラッシュメモリを除く。) [<input type="checkbox"/>] フラッシュメモリ [<input type="checkbox"/>] 紙 [<input type="checkbox"/>] その他 ()	
⑤委託先名の確認方法	島根県のホームページに掲載	
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
	⑨再委託事項	島根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2	住民基本台帳ネットワークシステムの運用管理に関する業務	
①委託内容	県で設置するファイアウォール、代表端末及び業務端末等機器について、利用ログ採取等の運用管理業務を委託する。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	[10万人以上100万人未満]	<選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
	対象となる本人の範囲 ※	「2. ③対象となる本人の範囲」と同上	
	その妥当性	住民基本台帳ネットワークシステムの運用を安全かつ適切に実施するため、本県が設置する庁内ファイアウォール、代表端末、業務端末等機器について、利用ログ採取等の運用管理業務を委託する。 なお、島根県サーバでは特定個人情報ファイルの全体を保有しているが、委託内容は、直接本人確認情報に係わらない業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業務は実施せず、権限も付与しない。 また、委託業者が利用する端末の定義等については、以下のとおり。 (代表端末:業務アクセスログ等確認、統計情報を取得、業務端末:本人確認情報の検索等を行う端末、ネットワーク監視装置:市町村のネットワークを確認、FW管理端末:FWログ確認)	
③委託先における取扱者数	[10人未満]	<選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上	
④委託先への特定個人情報ファイルの提供方法	[] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [] 紙 [○] その他 (運用管理上必要がある場合は、職員立会の上、代表端末又は業務端末により確認するが、委託先が特定個人情報を直接扱うことはない。)		
⑤委託先名の確認方法	島根県のホームページに掲載		
⑥委託先名	(株)ペンタスネット		
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	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、事前に書面により委託者の承諾を得ることとしている。	
	⑨再委託事項	本県が設置する庁内ファイアウォール、代表端末、業務端末等機器について、利用ログ採取等の運用管理業務を委託する。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業務を対象としているため、再委託先においても、特定個人情報ファイルに記録された情報そのものを扱う業務は実施しない。	
委託事項3			代表端末、業務端末等機器の保守業務
①委託内容	島根県住民基本台帳ネットワークシステムにおける代表端末、業務端末等の構成機器の保守業務を委託する。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	[10万人以上100万人未満]	<選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
	対象となる本人の範囲 ※	「2. ③対象となる本人の範囲」と同上	
	その妥当性	住民基本台帳ネットワークシステムの運用を安全かつ適切に実施するため、代表端末、業務端末等の機器について保守業務を委託する。 なお、島根県サーバでは特定個人情報ファイルの全体を保有しているが、委託内容は、直接本人確認情報に係わらない業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業務は実施せず、権限も付与していない。	
③委託先における取扱者数	[10人未満]	<選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上	
④委託先への特定個人情報ファイルの提供方法	[] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [] 紙 [○] その他 (保守業務上必要がある場合は、職員立会の上、代表端末又は業務端末により確認)		

⑤委託先名の確認方法		島根県のホームページに掲載
⑥委託先名		山陰総合リース株式会社
再委託	⑦再委託の有無 ※	[再委託する] <選択肢> 1) 再委託する 2) 再委託しない
	⑧再委託の許諾方法	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、事前に書面により委託者の承諾を得ることとしている。
	⑨再委託事項	代表端末、業務端末等機器の保守業務を委託する。 なお、「①委託内容」の通り、委託事項は、直接本人確認情報に係わらない業務を対象としているため、再委託先においても、特定個人情報ファイルに記録された情報そのものを扱う業務は実施せず、権限も付与していない。
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 (3) 件 [<input type="checkbox"/>] 移転を行っている (1) 件 [] 行っていない	
提供先1	地方公共団体情報システム機構(機構)	
①法令上の根拠	住基法第30条の7(都道府県知事から機構への本人確認情報の通知等)	
②提供先における用途	都道府県知事により受領した本人確認情報を元に機構保存本人確認情報ファイルを更新する。	
③提供する情報	住民票コード、氏名、生年月日、性別、住所、個人番号、異動事由、異動年月日	
④提供する情報の対象となる本人の数	[10万人以上100万人未満]	<選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤提供する情報の対象となる本人の範囲	「2. ③対象となる本人の範囲」と同上	
⑥提供方法	[] 情報提供ネットワークシステム [] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [] 紙 [<input type="checkbox"/>] その他 (住民基本台帳ネットワークシステム)	
⑦時期・頻度	市町村長からの通知に基づいて都道府県知事保存本人確認情報ファイルの更新を行った都度、随時。	
提供先2～5		
提供先2	島根県の他の執行機関	
①法令上の根拠	住基法第30条の15第2項(本人確認情報の利用)	
②提供先における用途	住基法別表第6に掲げる、島根県の他の執行機関への情報提供が認められる事務の処理及び住基法施行条例に定める事務の処理に用いる。	
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	[10万人以上100万人未満]	<選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤提供する情報の対象となる本人の範囲	「2. ③対象となる本人の範囲」と同上	
⑥提供方法	[] 情報提供ネットワークシステム [] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [] 紙 [<input 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	島根県の他の執行機関から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	[10万人以上100万人未満] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤提供する情報の対象となる本人の範囲	「2. ③対象となる本人の範囲」と同上
⑥提供方法	[] 情報提供ネットワークシステム [] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [<input checked="" type="radio"/>] 紙 [] その他 ()
⑦時期・頻度	開示請求があった都度、随時。
提供先6～10	
提供先11～15	
提供先16～20	
移転先1	島根県の他の部署
①法令上の根拠	住基法第30条の15第1項(本人確認情報の利用)
②移転先における用途	住基法別表第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た事務の処理及び住基法施行条例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	[10万人以上100万人未満] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤移転する情報の対象となる本人の範囲	「2. ③対象となる本人の範囲」と同上
⑥移転方法	[] 庁内連携システム [] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [] 紙 [<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	島根県の他の部署から検索要求があった都度、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て入退館管理をしている島根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。 ・島根県においては、代表端末及び記録媒体を施錠管理及び入退室管理を行っている部屋に保管し、業務端末はワイヤーロックを施工した上で、職員が退庁する際に執務室を施錠するなど必要な措置を講じている。 ・紙媒体については、島根県情報セキュリティポリシーに基づき、施錠管理ができる場所に保管している。
②保管期間	期間 [20年以上] <選択肢> 1) 1年未満 2) 1年 3) 2年 4) 3年 5) 4年 6) 5年 7) 6年以上10年未満 8) 10年以上20年未満 9) 20年以上 10) 定められていない
	その妥当性 <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）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。紙媒体については、島根県情報セキュリティポリシーに基づき、シュレッダ等により裁断している。
7. 備考	

(別添2) 特定個人情報ファイル記録項目

都道府県知事保存本人確認情報ファイル

1. 住民票コード、2. 漢字氏名、3. 外字数(氏名)、4. ふりがな氏名、5. 生年月日、6. 性別、7. 住所、8. 外字数(住所)、9. 個人番号、10. 異動事由、11. 異動年月日、12. 保存期間フラグ、13. 清音化かな氏名、14. 市町村コード、15. 大字・字コード、16. 操作者ID、17. 操作端末ID、18. タイムスタンプ、19. 通知を受けた年月日、20. 外字フラグ、21. 削除フラグ、22. 更新順番号、23. 氏名外字変更連番、24. 住所外字変更連番、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市町村CSに限定する。
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3: 入手した特定個人情報が不正確であるリスク	
入手の際の本人確認の措置の内容	住民の異動情報の届出等を受け付ける市町村の窓口において、対面で身分証明書(個人番号カード等)の提示を受け、本人確認を行う。
個人番号の真正性確認の措置の内容	市町村において真正性が確認された情報を市町村CSを通じて入手できることを、システムで担保する。
特定個人情報の正確性確保の措置の内容	システム上、本人確認情報更新の際に、論理チェックを行う(例えば、現存する住民に対して転入を異動事由とする更新が行われようとした場合や、転居を異動事由とする更新の際に住所以外の更新が行われようとした場合に当該処理をエラーとする)仕組みとする。 また、入手元である市町村CSにおいて、項目(フォーマット、コード)のチェックを実施する。
その他の措置の内容	—
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク4: 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	・機構が作成・配付する専用のアプリケーションを(※)用いることにより、入手の際の特定個人情報の漏えい・紛失の防止に努める。 ・市町村CSと接続するネットワーク回線に専用回線を用いる、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無い。 ※島根県サーバのサーバ上で稼動するアプリケーション。 島根県内の市町村の住民の本人確認情報を管理し、島根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	島根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	庁内システムと島根県サーバとの接続は行わない。
その他の措置の内容	—
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2: 権限のない者(元職員、アクセス権限のない職員等)によって不正に使用されるリスク	
ユーザ認証の管理	[行っている] <選択肢> 1) 行っている 2) 行っていない
具体的な管理方法	生体認証による操作者認証を行う。
アクセス権限の発効・失効の管理	[行っている] <選択肢> 1) 行っている 2) 行っていない
具体的な管理方法	職員の異動や退職等が発生した際に、ネットワーク管理者が権限の発効及び失効について、管理簿により管理を行っている。 年に一度、アクセス権限の再設定を行っている。
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	・操作者の権限等に応じたアクセス権限が付与されるよう管理する。 ・不正アクセスを分析するために、島根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	・本人確認情報を取り扱うシステムの操作履歴を取得し、保管する。 ・不正な操作が無いことについて、操作履歴の記録により随時確認する。
その他の措置の内容	—
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3: 従業者が事務外で使用するリスク	
リスクに対する措置の内容	・システムの操作履歴を取得し、保管する。 ・定期的に監査を行い、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。 ・操作者研修、事務外利用の禁止等について指導する。
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク4: 特定個人情報ファイルが不正に複製されるリスク	
リスクに対する措置の内容	システム上、管理権限を与えられた者以外、情報の複製は行えない仕組みとなっている。
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あたり、以下の措置を講じる。</p> <ul style="list-style-type: none"> ・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 ・離席時は、パソコンをログオフする ・業務端末のディスプレイは来庁者から見えない位置に置く ・本人確認情報が表示された画面のハードコピーの取得はできない仕様となっている ・大量のデータ出力に際しては、事前に管理責任者の承認を得る ・原則、出力帳票の持ち出しは禁止している ・本人確認情報の開示・訂正の請求に対し、適切に対応する ・本人確認情報の提供状況の開示請求に対し、適切に対応する ・業務端末については、ワイヤーロックにより盗難防止等を図ると共に、島根県セキュリティポリシーに基づき、業務端末の設置してある事務室を適正に管理する。 	

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	社会的信用、過去の履行実績等により確認している。 委託契約書において、秘密保守義務、個人情報保護の徹底、情報資産の管理方法等を明記し、受託者に対して遵守させることを義務づけている。	
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	・当日委託業務に従事する者の名簿を提出させている。 ・委託業務に従事する者に都道府県知事保存本人確認ファイルに直接アクセスする権限を付与しない。	
特定個人情報ファイルの取扱いの記録	[記録を残している]	<選択肢> 1) 記録を残している 2) 記録を残していない
具体的な方法	業務上、特定個人情報を委託先へ提供することはないが、特定個人情報の持ち出し禁止について契約書に明記している。 特定個人情報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(監視カメラ等)を講じ、不正作業が行われないようにしている。	
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	業務上、特定個人情報を委託先へ提供することはないが、特定個人情報の持ち出し禁止について契約書に明記している。 特定個人情報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(監視カメラ等)を講じ、不正作業が行われないようにしている。	
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	委託先には特定個人情報の閲覧・更新権限を付与しておらず、特定個人情報をやりとりすることもない。	
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
ルール内容及びルール遵守の確認方法	委託先には特定個人情報の閲覧・更新権限を付与しておらず、特定個人情報を消去できない仕組みとなっている。	
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	・秘密の保持 ・目的外利用の禁止 ・複製の禁止 ・安全管理措置を講じる義務 ・委託業者ごとの作業場所、使用するネットワーク及び情報機器について特定し、作業内容を管理している。	
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	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し、再委託先が、特定個人情報ファイルを取り扱えないように、特定個人情報の更新/閲覧権限を付与しない。	
その他の措置の内容	-	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		
-		

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。） [] 提供・移転しない

リスク1： 不正な提供・移転が行われるリスク

特定個人情報の提供・移転の記録	[記録を残している]	<選択肢> 1) 記録を残している	2) 記録を残していない
-----------------	--------------	----------------------	--------------

具体的な方法	特定個人情報(個人番号、4情報等)の提供・移転を行う際に、提供・移転の記録(提供・移転日時、操作者等)を住民基本台帳ネットワークシステム上で管理し、7年分保存する。 なお、住民基本台帳ネットワークシステム上、提供・移転に係る処理を行ったものの提供・移転が認められなかった場合についても記録を残す。
--------	---

特定個人情報の提供・移転に関するルール	[定めている]	<選択肢> 1) 定めている	2) 定めていない
---------------------	-----------	-------------------	-----------

ルール内容及びルール遵守の確認方法	住基法、番号法、個人情報保護条例において定められた事項についてのみ行う。
-------------------	--------------------------------------

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： 不適切な方法で提供・移転が行われるリスク

リスクに対する措置の内容	相手方(全国サーバ)と島根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、島根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している。 出力した紙媒体は、施錠管理ができる場所に適切に保管し、廃棄の際はシュレッダ等により裁断して廃棄している。
--------------	---

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	
--	--	--------------	--

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している。 ・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)と島根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	
--	--	--------------	--

特定個人情報の提供・移転(委託や情報提供ネットワークシステムを通じた提供を除く。)におけるその他のリスク及びそのリスクに対する措置

-

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

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。 ・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、内容を読み出すことができないようにする。 ・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。 廃棄時には、要領・手順書等に基づき、裁断、溶解等を行うとともに、帳票管理簿等にその記録を残す。
その他の措置の内容	-
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置	
-	

IV その他のリスク対策 ※

1. 監査		
①自己点検	[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
具体的なチェック方法	年に1回、住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、セキュリティ対策規程等の項目に係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	住民基本台帳ネットワークシステムを利用する所属に対して、現地監査を実施する。 現地監査では、以下の内容を確認する。 ・本人確認情報の利用業務に係る業務端末の管理状況 ・情報資産の管理状況 ・2年間で全所属の監査を行う。	
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	<ul style="list-style-type: none"> ・住民基本台帳ネットワークシステムを利用する職員に対して、年に1回、必要な知識の習得に資するための研修を実施するとともに、その記録を残す。 ・年度途中に利用開始を希望する職員に対しては、その都度個別に研修を実施する。 	
3. その他のリスク対策		
-		

V 開示請求、問合せ

1. 特定個人情報の開示・訂正・利用停止請求	
①請求先	〒690-8501 島根県松江市殿町1番地 島根県総務部総務課(県政情報センター) 0852-22-6139
②請求方法	法令等で定める様式による書面の提出により開示・停止・利用停止請求を受け付ける。
特記事項	-
③手数料等	[無料] <選択肢> 1) 有料 2) 無料 (手数料額、納付方法：請求・閲覧は無料。写しの交付は実費負担。)
④個人情報ファイル簿の公表	[行っていない] <選択肢> 1) 行っている 2) 行っていない
個人情報ファイル名	-
公表場所	-
⑤法令による特別の手続	-
⑥個人情報ファイル簿への不記載等	-
2. 特定個人情報ファイルの取扱いに関する問合せ	
①連絡先	〒690-8501 島根県松江市殿町1番地 島根県地域振興部市町村課 0852-22-5063
②対応方法	問合せの際に、対応について記録に残し、関係法令等に照らし、適切に回答する。

VI 評価実施手続

1. 基礎項目評価	
①実施日	令和4年2月7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	島根県「政策への県民参加制度(パブリックコメント)実施要綱」に基づき実施
②実施日・期間	令和元年12月11日 ~ 令和2年1月10日
③期間を短縮する特段の理由	—
④主な意見の内容	意見なし
⑤評価書への反映	—
3. 第三者点検	
①実施日	令和2年2月14日 ~ 令和2年4月17日
②方法	島根県個人情報保護審査会において点検を受けた。
③結果	第3者点検により以下の答申を受けた。 特定個人情報保護評価指針(平成26年4月18日特定個人情報保護委員会告示第4号。以下「指針」という。)第10の1(2)に定める審査の観点を参考に点検を行ったところ、指針に定める実施手続等に適合しており、当該評価書案の内容は、指針に定める評価の目的等に照らし妥当であると認められる。 今後も、特定個人情報の保護に最大限の注意を払い、社会情勢の変化や技術の進歩等を踏まえ、より有効なリスク対策の実施に向けて、適宜必要な見直しを行いながら適正な管理運用について引き続き積極的に取り組むよう要望する。
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	

