資料1

特定個人情報保護評価書（全項目評価書）
記載要領（都道府県版）

【本記載要領の目的】
　本記載要領は、都道府県における特定個人情報保護評価書の作成を支援することを目的として、地方公共団体情報システム機構（以下「機構」という。）が、特定個人情報保護評価指針第３の２及び特定個人情報保護評価指針の解説第３の２－４に基づき、住民基本台帳ネットワークシステムに関連する項目の記載要領を示すものです。
　各都道府県においては、本記載要領を参考とし、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第２７条に基づき特定個人情報保護評価を実施してください。

【本記載要領の構成、活用方法】
・本記載要領では、各都道府県が住民基本台帳法に基づいて実施する事務を、「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」として一つの評価書で評価を実施し、また、当該事務において保有する特定個人情報ファイルは「都道府県知事保存本人確認情報ファイル」の１ファイルで構成されることを想定して作成しています。
・「都道府県知事保存本人確認情報ファイル」は、機構で開発するシステムの中で管理されることから、仕様に係る項目については回答を、その他の項目については記載例を示しています。
・上記の考え方に基づき、本記載要領では各項目を次の３類型に分けています。
①都道府県サーバの仕様等に係るもので、本記載要領の回答を各都道府県がそのまま評価書へ転記できる項目。（白地項目）
②都道府県サーバ等について、法令や「住民基本台帳ネットワークシステム及びそれに接続している既設ネットワークに関する調査表」（以下「セキュリティチェックリスト」という。）等を参考に機構が記載例を示している項目であり、本記載要領の内容を各都道府県の実情に合わせて適宜修正・追加の上、評価書に記載すべき項目。（橙色で網掛けした項目）
③各都道府県が実情に合わせて回答を作成し、評価書に記載すべき項目。（橙色網掛けで空欄の項目）

【その他留意事項】
・本記載要領は、各都道府県の特定個人情報保護評価の作成支援に資するため、評価書様式の形式を一部変更しています。したがって、本記載要領を編集してそのまま評価書とすることはできません。評価書の作成にあたっては、特定個人情報保護委員会から示される様式を使用してください。（本記載要領の様式を使用した場合、特定個人情報保護委員会への提出の際に不都合が生じる場合があります。）
・なお、本記載要領の赤字部分については特定個人情報保護委員会の了承を得ていることを申し添えます。

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

個人のプライバシー等の権利利益の保護の宣言	
特記事項	

評価実施機関名
（都道府県知事名）

特定個人情報保護委員会　承認日 【行政機関等のみ】
公表日
平成　　年　　月　　日

項目一覧

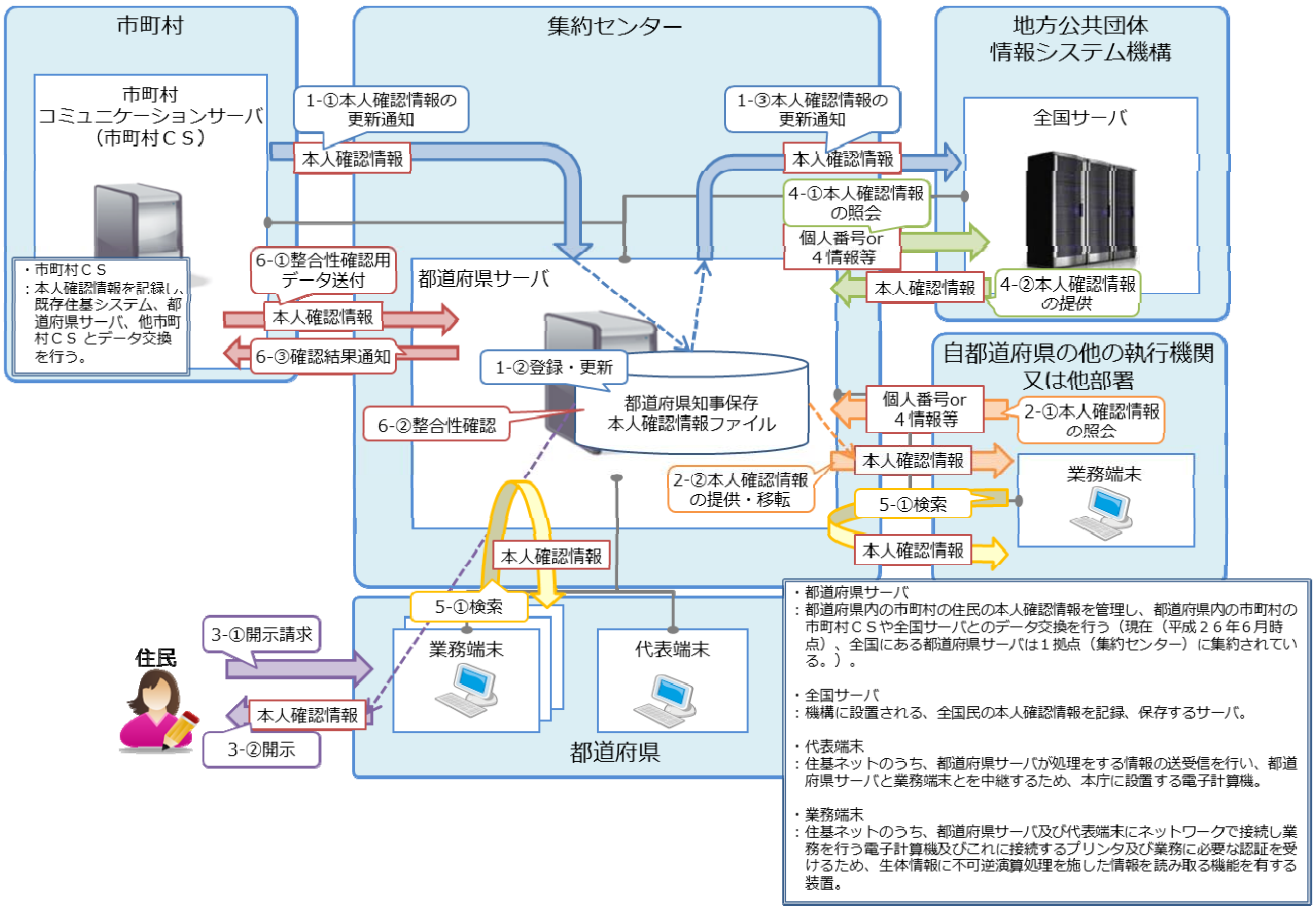
Ⅰ　基本情報

1. 特定個人情報ファイルを取り扱う事務	
①事務の名称	住民基本台帳ネットワークに係る本人確認情報の管理及び提供等に関する事務
②事務の内容　※	下記記載例を参考に都道府県の実態に合わせて記載してください。 なお、条例により本人確認情報の提供等を行っている場合、適宜事務を追加ください。 【記載例】 都道府県は、住民基本台帳法（以下「住基法」という。）に基づいて住民基本台帳のネットワーク化を図り、全国共通の本人確認システム（住基ネット）を市町村と共同して構築している。 なお、住民基本台帳は、住基法に基づき作成されるものであり、市町村における住民の届出に関する制度及びその住民たる地位を記録する各種の台帳に関する制度を一元化し、もって、住民の利便を増進するとともに行政の近代化に対処するため、住民に関する記録を正確かつ統一的に行うものであり、市町村において、住民の居住関係の公証、選挙人名簿の登録、その他住民に関する事務の処理の基礎となるものである。 具体的に都道府県では、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都道府県知事から本人確認情報に係る自都道府県の他の執行機関への提供又は他部署への移転 ④住民による請求に基づく当該個人の本人確認情報の開示並びに開示結果に基づく住民からの 　本人確認情報の訂正、追加又は削除の申出に対する調査 ⑤機構への本人確認情報の照会
③対象人数	[5) 30万人以上]　＜選択肢＞ 1) 1,000人未満　2) 1,000人以上1万人未満 3) 1万人以上10万人未満　4) 10万人以上30万人未満 5) 30万人以上

2. 特定個人情報ファイルを取り扱う事務において使用するシステム	
システム1	
①システムの名称	住民基本台帳ネットワークシステム ※「３．特定個人情報ファイル名」に示す「都道府県知事保存本人確認情報ファイル」は、住民基本台帳ネットワークシステムの構成要素のうち、都道府県サーバにおいて管理がなされているため、以降は、住民基本台帳ネットワークシステムの内の都道府県サーバ部分について記載する。
②システムの機能	１．本人確認情報の更新 ：都道府県知事保存本人確認情報ファイルを最新の状態に保つため、市町村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。 ２．自都道府県の他の執行機関への情報提供又は他部署への移転 ：自都道府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情報等に対応付く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。 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（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．本人確認情報整合 ：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。
③他のシステムとの接続 庁内システム（宛名管理システムを含む。）と回線連携を行う場合、接続するシステムを適宜追加ください。	[ ]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（）

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	都道府県では、都道府県知事保存本人確認情報ファイルを、下記に記載の通りの必要性から取り扱う。 ・都道府県知事保存本人確認情報ファイルは、転出入があった場合等にスムーズな住民情報の処理を行うため、また全国的な本人確認手段として、１つの市町村内にとどまらず、全地方公共団体で、本人確認情報を正確かつ統一的に記録・管理することを目的として、以下の用途に用いられる。 ①住基ネットを用いて市町村の区域を越えた住民基本台帳に関する事務（住民基本台帳ネットワークに係る本人確認情報の管理及び提供等に関する事務）の処理を行うため、区域内の住民に係る最新の本人確認情報を管理する。 ②市町村からの本人確認情報の更新情報の通知を受けて都道府県知事保存本人確認情報ファイルを更新し、当該更新情報を機構に対して通知する。 ③自都道府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。
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、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）につながることが見込まれる。
5. 個人番号の利用 ※	
法令上の根拠 ※住基ネットの条例利用を実施されている場合、法令上の根拠(住基法第30条の13)を追加ください。	住民基本台帳法（住基法）（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）
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	[2) 実施しない]　＜選択肢＞ 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	－
7. 評価実施機関における担当部署	
①部署	
②所属長	
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. 市町村において受け付けた住民の異動に関する情報を、市町村ＣＳを通じて都道府県サーバに通知する。
1-②. 都道府県サーバにおいて、市町村より受領した本人確認情報を元に都道府県知事保存本人確認情報ファイルを更新する。
1-③. 機構に対し、住民基本台帳ネットワークを介して、本人確認情報の更新を通知する。

2．自都道府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. 自都道府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. 都道府県知事において、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。
※自都道府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、自都道府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（回線連携を用いる場合は、「媒体連携又は回線連携」と記載）（注2、注3）により行う。
（注1）自都道府県の他の執行機関又は他部署においてファイル化された本人確認情報照会対象者の情報（検索条件のリスト）を元に都道府県サーバに照会し、照会結果ファイルを提供する方式を指す。
（注2）媒体連携とは、一括提供の方式により本人確認情報の提供を行う場合に、情報連携に電子記録媒体を用いる方法を指す。
（注3）回線連携とは、一括提供の方式により本人確認情報の提供を行う場合に、情報連携に通信回線（庁内LAN等）を用いる方法を指す。具体的には、都道府県サーバの代表端末又は業務端末と庁内システム（宛名管理システムを含む。）のみがアクセス可能な領域（フォルダ）を設け、当該領域内で照会要求ファイル及び照会結果ファイルの授受を行う。

3．本人確認情報の開示に関する事務

3-①. 住民より本人確認情報の開示請求を受け付ける。
3-②. 開示請求者（住民）に対し、都道府県知事保存本人確認情報ファイルに記録された当該個人の本人確認情報を開示する。

4．機構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　※	[1)　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	[　]　＜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	[2)　10項目以上50項目未満]　＜選択肢＞ 1) 10項目未満　2) 10項目以上50項目未満 3) 50項目以上100項目未満　4) 100項目以上
主な記録項目　※	・識別情報 [○] 個人番号　[ ]個人番号対応符号　[ ]その他識別情報（内部番号） ・連絡先等情報 [○]4情報（氏名、性別、生年月日、住所）　[ ]連絡先（電話番号等） [○]その他住民票関係情報 ・業務関係情報 [ ]国税関係情報　[ ]地方税関係情報　[ ]健康・医療関係情報 [ ]医療保険関係情報　[ ]児童福祉・子育て関係情報　[ ]障害者福祉関係情報 [ ]生活保護・社会福祉関係情報　[ ]介護・高齢者福祉関係情報 [ ]雇用・労働関係情報　[ ]年金関係情報　[ ]学校・教育関係情報 [ ]災害関係情報 [ ]その他（）
その妥当性	・個人番号、４情報、その他住民票関係情報 ：住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月予定
⑥事務担当部署	
3. 特定個人情報の入手・使用	
①入手元　※	[ ]本人又は本人の代理人 [ ]評価実施機関内の他部署（） [ ]行政機関・独立行政法人等（） [○]地方公共団体・地方独立行政法人（市町村） [ ]民間事業者（） [ ]その他（）
②入手方法	[ ]紙　[ ]電子記録媒体（フラッシュメモリを除く。） [ ]フラッシュメモリ　[ ]電子メール　[ ]専用線 [ ]庁内連携システム　[ ]情報提供ネットワークシステム [○]その他（市町村ＣＳを通じて入手する。）
③入手の時期・頻度	住民基本台帳の記載事項において、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基ネットで管理する必要があるので、市町村から都道府県へ、都道府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		【記載例】 都道府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。
	変更の妥当性	－
⑦使用の主体	使用部署※	
	使用者数	[ ] ＜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 ※ ※住基ネットの条例利用を実施されている場合、特定個人情報ファイルの使用方法を追加ください。		・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）。 ・自都道府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（自都道府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→自都道府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（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→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。 ・自都道府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 ※		[1) 委託する] （1件）	<選択肢> 1) 委託する　2) 委託しない
委託事項		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		[1) 特定個人情報ファイルの全体]	<選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部
	対象となる本人の数	[ ]	<選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
	対象となる本人の範囲 ※	「2．③対象となる本人の範囲」と同上	
	その妥当性	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」の通り、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		[1) 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　[ ]フラッシュメモリ [ ]電子記録媒体（フラッシュメモリを除く。）　[ ]紙 [ ]その他（）	
⑤委託先名の確認方法		【記載例】 委託先が決定した際には、当県のホームページにて公表している。	
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 ※	[1) 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	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。	

5. 特定個人情報の提供・移転（委託に伴うものを除く。）	提供／移転先の単位の件数を記載します。（条例利用等を行っている場合、適宜提供・移転先を追加ください。）	
提供・移転の有無	[〇]提供を行っている（3件） [ ]行っていない	[〇]移転を行っている（1件）
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	[ ]	＜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 [ ]電子メール [ ]フラッシュメモリ [〇]その他（住民基本台帳ネットワークシステム）	[ ]専用線 [ ]電子記録媒体（フラッシュメモリを除く。） [ ]紙
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	自都道府県の他の執行機関（〇〇など） ※主な提供先機関名を〇〇に記載してください。	
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	住基法別表第六に掲げる、自都道府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２０条第９項及び第２２条第７項に基づく経過措置である。	
④提供する情報の対象となる本人の数	[ ]	＜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 [ ]電子メール [ ]フラッシュメモリ [〇]その他（住民基本台帳ネットワークシステム）	[ ]専用線 [ ]電子記録媒体（フラッシュメモリを除く。） [ ]紙
⑦時期・頻度	自都道府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、住所、生年月日、性別、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	[ ]	＜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 [ ]電子メール [ ]フラッシュメモリ [ ]その他（　　）	[ ]専用線 [ ]電子記録媒体（フラッシュメモリを除く。） [〇]紙
⑦時期・頻度	開示請求があった都度、随時。	

一括提供方式により提供を行う場合、適宜選択ください。

把握している範囲で直近の提供の実績（時期・頻度等）を適宜追記ください。

書面以外の方法により提供を行う場合、適宜選択ください。

把握している範囲で直近の提供の実績（時期・頻度等）を適宜追記ください。

移転先1	自都道府県の他部署（○○など） ※主な移転先部署名を○○に記載してください。
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２０条第９項及び第２２条第７項に基づく経過措置である。
④移転する情報の対象となる本人の数	[ ] ＜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	[ ]情報提供ネットワークシステム　[ ]専用線 [ ]電子メール　[ ]電子記録媒体（フラッシュメモリを除く。） [ ]フラッシュメモリ　[ ]紙 [○]その他（住民基本台帳ネットワークシステム）
⑦時期・頻度	自都道府県の他部署からの検索要求があった都度、随時。
移転先2	

一括提供方式により提供を行う場合、適宜選択ください。

条例により、自都道府県の他部署に本人確認情報の移転を行っている場合、記載を追加ください。

6．特定個人情報の保管・消去		
①保管場所※		【記載例】 ・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。 ・都道府県においては、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	[9）20年以上] ＜選択肢＞ 1）1年未満　2）1年　3）2年 4）3年　5）4年　6）5年 7）6年以上10年未満　8）10年以上20年未満　9）20年以上 10）定められていない
	その妥当性	・住民票の記載の修正後の本人確認情報は、新たに記載の修正の通知を受けるまで保管する。 ・住民票の記載の修正前の本人確認情報（履歴情報）及び消除者の本人確認情報は、住基法施行令第３０条の６（都道府県における本人確認情報の保存期間）に定める期間（１５０年間）保管する。
③消去方法		【記載例】 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。
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

Ⅲ　特定個人情報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	【記載例】 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を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	【記載例】 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	[　] ＜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 【参考】リスク対策状況の選択の目安（以下同じ） 1）特に力を入れている　：セキュリティチェックリストの設問で３点（運用している）を選択するレベル 2）十分である　：セキュリティチェックリストの設問で２点（整備している）を選択するレベル 3）課題が残されている　：セキュリティチェックリストの設問で１点（整備されていない）を選択するレベル
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	【記載例】 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	[　] ＜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	【記載例】 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	【記載例】 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	【記載例】 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	【記載例】 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	[　] ＜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	【記載例】 ・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なりすまし等を防止する。
リスクへの対策は十分か	[　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
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。）におけるその他リスク及びそのリスクに対する措置	

3. 特定個人情報の使用	
リスク1：目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク	
宛名システム等における措置の内容	【記載例】 （媒体連携のみを用いる場合）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。 （回線連携を宛名管理システムにより行っている場合）宛名管理システムに共有フォルダを作成し、都道府県サーバの代表端末又は業務端末を介して、共有フォルダに格納された要求情報を取得して住基ネットに照会を実施する。都道府県サーバの代表端末又は業務端末から宛名システムへのアクセスは、共有フォルダだけにシステム上制限する。なお、当該共有フォルダは部署ごとに作成し、他部署の共有フォルダにはアクセスできないようシステム上制限する。また、システム上、宛名管理システムから都道府県サーバへのアクセスは行えない仕組みとする。 （回線連携を庁内システムにより行っている場合）下欄に記載してください。
事務で使用するその他のシステムにおける措置の内容	【記載例】 （媒体連携のみを用いる場合）庁内システムと都道府県サーバとの接続は行わない。 （回線連携を宛名管理システムにより行っている場合）上欄に記載してください。 （回線連携を庁内システムにより行っている場合）庁内システムに共有フォルダを作成し、都道府県サーバの代表端末又は業務端末を介して、共有フォルダに格納された要求情報を取得して住基ネットに照会を実施する。都道府県サーバの代表端末又は業務端末から庁内システムへのアクセスは、共有フォルダだけにシステム上制限する。なお、当該共有フォルダは庁内システムごとに作成し、他部署の共有フォルダにはアクセスできないようシステム上制限する。また、システム上、庁内システムから都道府県サーバへのアクセスは行えない仕組みとする。
その他の措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている　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	[ ] ＜選択肢＞ 1）行っている　2）行っていない
具体的な管理方法	【記載例】 生体認証（操作者識別カードにより認証を行っている場合はその旨を記載）による操作者認証を行う。
アクセス権限の発行・失効の管理	[ ] ＜選択肢＞ 1）行っている　2）行っていない
具体的な管理方法	【記載例】 ・退職した元職員や異動した職員等のアクセス権限の失効管理（※）を適切に行う。 ・アクセス権限を失効させたことについて、管理簿に記録を残す。 ・記録した管理簿について、失効管理が適切に行われていることを、年1回以上の定期的な棚卸しにより確認し、その記録を残す。 ※退職職員、異動職員のアクセス権限の失効管理の内容については、できるだけ具体的にご記載ください。
アクセス権限の管理	[ ] ＜選択肢＞ 1）行っている　2）行っていない
具体的な管理方法	【記載例】 ・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、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	[ ] ＜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	【記載例】 ・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な操作の疑いがある場合は、申請文書等との整合性を確認する。 ・バックアップされた操作履歴について、定められた期間、安全な場所に施錠保管する。
その他の措置の内容	
リスクへの対策は十分か	[ ] ＜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	【記載例】 ・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研修会において、事務外利用の禁止等について指導する。 ・職員以外の従業者（委託先等）には、当該事項についての誓約書の提出を求める。
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

リスク4：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	【記載例】 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する。 また、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・委託先等に対し指導する。
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

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

【記載例】
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。
・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事務処理に必要となる範囲にとどめる。
・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。
・本人確認情報の開示・訂正の請求に対し、適切に対応する。
・本人確認情報の提供状況の開示請求に対し、適切に対応する。

4. 特定個人情報ファイルの取扱いの委託　[ ]委託しない

委託先による特定個人情報の不正入手・不正な使用に関するリスク
委託先による特定個人情報の不正な提供に関するリスク
委託先による特定個人情報の保管・消去に関するリスク
委託契約終了後の不正な使用等のリスク
再委託に関するリスク

情報保護管理体制の確認	【記載例】 ：委託先の社会的信用と能力を確認する。具体的には、要領・手順書等（※）に基づき、委託業者を選定するとともに、その記録を残す。 また、委託業者が選定基準を引き続き満たしていることを適時確認するとともに、その記録を残す。 ※要領・手順書等について、内容をできるだけ具体的に記載ください。 （「都道府県サーバの運用及び監視に関する業務」に関する記載例） ・平成２４年６月１２日、住民基本台帳ネットワークシステム推進協議会（４７都道府県が構成員）において、都道府県サーバ集約化の実施および集約化された都道府県サーバの運用及び監視に関する業務を機構へ委託することを議決している。 ・委託先として議決された機構は、地方公共団体情報システム機構法（平成２５年５月３１日法律第２９号）に基づき平成２６年４月１日に設立された組織であり、住基法に基づく指定情報処理機関として住民基本台帳ネットワークシステムの運用を行っている実績がある。また、前身の財団法人地方自治情報センターにおいて平成１４年８月５日から平成２６年３月３１日まで、指定情報処理機関であった。 ・そのため、委託先として社会的信用と特定個人情報の保護を継続的に履行する能力があると認められるとともに、プライバシーマークの付与を受けており、情報保護管理体制は十分である。
特定個人情報ファイルの閲覧者・更新者の制限	[ ] ＜選択肢＞ 1）制限している　2）制限していない
具体的な制限方法	【記載例】 ・作業者を限定するために、委託作業者の名簿を提出させる。 ・閲覧／更新権限を持つものを必要最小限にする。 ・閲覧／更新権限を持つ者のアカウント管理を行い、システム上で操作を制限する。 ・閲覧／更新の履歴（ログ）を取得し、不正な使用がないことを確認する。 （「都道府県サーバの運用及び監視に関する業務」に関する記載例） ・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。）には、本人確認情報の更新及び本人確認情報の整合性確認業務のため特定個人情報ファイルを提供する場合が想定されるが、その場合はシステムで自動的に暗号化を行った上で提供することとしており、システム設計上、特定個人情報にアクセスできず閲覧／更新もできない。 ・委託先（再委託先を含む。）は、災害等におけるデータの損失等に対する対策のため、日次で特定個人情報ファイルをバックアップすることが想定されるが、バックアップのために特定個人情報ファイルを媒体に格納する場合は、システムで自動的に暗号化を行うこととしており、システム設計上、特定個人情報にアクセスできず閲覧／更新もできない。

特定個人情報ファイルの取扱いの記録		[ ] ＜選択肢＞ 1）記録を残している　2）記録を残していない
	具体的な方法	【記載例】 ・契約書等に基づき、委託業務が実施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。 ・委託業者から適時セキュリティ対策の実施状況の報告を受けるとともに、その記録を残す。 ・その他、システムによる特定個人情報ファイルの取扱い記録（アクセスログ）や、媒体授受の取扱記録を残す。 （「都道府県サーバの運用及び監視に関する業務」に関する記載例） ・委託先（再委託先を含む。）には、本人確認情報の更新及び本人確認情報の整合性確認業務のため特定個人情報ファイルを提供する場合が想定されるが、その場合はシステムで自動的に暗号化を行った上で提供することとしており、システム設計上、特定個人情報にアクセスできず閲覧／更新もできない。 ・委託先（再委託先を含む。）は、災害等におけるデータの損失等に対する対策のため、日次で特定個人情報ファイルをバックアップすることが想定されるが、バックアップのために特定個人情報ファイルを媒体に格納する場合は、システムで自動的に暗号化を行うこととしており、システム設計上、特定個人情報にアクセスできず閲覧／更新もできない。 ・上記のとおり、委託先（再委託先を含む。）は特定個人情報にアクセスできないが、バックアップ媒体については、記録簿により管理し、保管庫に保管している。週次で管理簿と保管庫の媒体をチェックし、チェックリストに記入している。バックアップの不正取得や持ち出しのリスクに対し、サーバ室に物理的対策（監視カメラなど）を講じ、不正作業が行われないようにしている。 ・チェックリストの結果について、委託先である機構より、月次で書面により「都道府県サーバ集約センターの運用監視等に係る作業報告について　６．セキュリティ確認結果報告」の報告を受けている。
特定個人情報の提供ルール		[ ] ＜選択肢＞ 1）定めている　2）定めていない
	委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	【記載例】 委託先から他者への特定個人情報の提供は一切認めないことを契約書上明記する。 また、委託契約の報告条項に基づき、定期的に特定個人情報の取扱いについて書面にて報告させ、必要があれば当県職員が現地調査することも可能とする。 （「都道府県サーバの運用及び監視に関する業務」に関する記載例） ・委託先である機構に対し、特定個人情報の目的外利用及び提供は認めないことを契約書上明記している。 ・委託先である機構は、日次、月次、年次で目的外利用及び提供についてのチェックを含むセキュリティチェックを行い、委託元である当県は、チェックリストの結果について、機構より、月次で書面により「都道府県サーバ集約センターの運用監視等に係る作業報告について　６．セキュリティ確認結果報告」の報告を受けている。 ・必要があれば、当県職員が委託業務について機構の履行状況を立ち会いまたは報告を受けることを契約書上明記している。
	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	【記載例】 委託先に提供する際、日付及び件数を記録した受け渡しの確認印を押印してもらい、当県の上長がそれを確認する。 （「都道府県サーバの運用及び監視に関する業務」に関する記載例） ・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。
特定個人情報の消去ルール		[ ] ＜選択肢＞ 1）定めている　2）定めていない
	ルールの内容及びルール遵守の確認方法	【記載例】 委託契約書に、以下の措置をとる旨を規定する。 ・保管期間の過ぎた特定個人情報を、システムにて自動判別し消去 ・紙媒体は、保管期間ごとに分けて保管し、保管期間が過ぎているものを外部業者にて溶解処理 ・データか紙かを問わず、廃棄の際は廃棄履歴を作成し保存 ・特定個人情報と同様、保管期間の過ぎたバックアップを、システムにて自動判別し消去 また、委託契約の報告条項に基づき、定期的に特定個人情報の取扱いについて書面にて報告させ、必要があれば当県職員が現地調査することも可能とする。 （「都道府県サーバの運用及び監視に関する業務」に関する記載例） ・委託契約上、委託先である機構に提供された特定個人情報ファイルについては、住基法施行令第３０条の６に規定された本人確認情報の保存期間（１５０年間）が過ぎた際に、システムにて自動判別し消去することを規定している。 ・バックアップ媒体については、「運用設計書」において、「媒体が破損や耐用年数、耐用回数を超過したとき、管理簿に理由を明記し、媒体は引き続きデータ保管庫に格納」することにしているが、委託契約上、委託先である機構に提供された特定個人情報ファイルについては、契約完了時に返還または廃棄することを規定する。 ・委託契約の報告条項に基づき、月次の完了届において、特定個人情報の取扱いについて書面にて報告を受ける。また、必要があれば、当県職員又は監査法人などの第三者が現地調査し、適正に運用されているか確認する。

委託契約書中の特定個人情報ファイルの取扱いに関する規定		[　] ＜選択肢＞ 1）定めている　2）定めていない
	規定の内容	【記載例】 ・目的外利用の禁止 ・特定個人情報の閲覧者・更新者を制限 ・特定個人情報の提供先の限定 ・情報漏洩を防ぐための保管管理に責任を負う。 ・情報が不要となったとき又は要請があったときに情報の返還又は消去などの必要な措置を講じる。 ・保管期間の過ぎた特定個人情報及びそのバックアップを完全に消去する。 ・個人情報の取扱いについて四半期に一度チェックを行った上でその報告をする。 ・必要に応じて、委託先の視察・監査を行うことができる。 ・再委託の禁止 （「都道府県サーバの運用及び監視に関する業務」に関する記載例） ・秘密保持義務 ・事業所内からの特定個人情報の持出しの禁止 ・特定個人情報の目的外利用の禁止 ・再委託における条件 ・漏えい事案等が発生した場合の委託先の責任 ・委託契約終了後の特定個人情報の返却又は廃棄 ・従業者に対する監督・教育 ・契約内容の遵守状況について報告を求める規定 等を契約書において定めるとともに、当県と同様の安全管理措置を義務付ける。
再委託先による特定個人情報ファイルの適切な取扱いの確保		＜選択肢＞ 1）特に力を入れて行っている　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	【記載例】 （「都道府県サーバの運用及び監視に関する業務」に関する記載例） ・委託先である機構と再委託先の契約において、個人情報保護の条項を設けており、従事者への周知を契約で規定している。 ・再委託する業務は、直接本人確認情報に係らない（直接本人確認情報にアクセスできず、閲覧・更新・削除等を行わない）業務を対象としている。 ・委託元は、委託を受けた者に対して、委託元自らが果たすべき安全管理措置と同等の措置が講じられるよう必要かつ適切な監督を行っている。再委託を行う場合は、委託元がその必要性を厳しく審査し、再委託先に対して、委託先と同等の安全管理措置を義務付け、必要かつ適切な監督を行っている。
その他の措置の内容		
リスクへの対策は十分か		[　] ＜選択肢＞ 1）特に力を入れている　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		
【記載例】 （「都道府県サーバの運用及び監視に関する業務」に関する記載例） ・再委託先の選定については、平成２５年１月２４日、都道府県サーバ集約に伴う調達評価委員会（都道府県の各ブロックから推薦された新潟県、長野県、富山県、和歌山県、香川県、愛媛県、岡山県および福岡県により構成）が、入札の評価基準の作成に参加し、適切な再委託先となるよう監督している。		
5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）　[　]提供・移転しない		
リスク1：不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録		[　] ＜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	【記載例】 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、〇年分保存する。 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。
特定個人情報の提供・移転に関するルール		[　] ＜選択肢＞ 1）定めている　2）定めていない
	ルールの内容及びルール遵守の確認方法	【記載例】 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、本業務では具体的に誰に対し何の目的で提供・移転できるかを書き出したマニュアルを整備し、マニュアル通りに特定個人情報の提供・移転を行う。
その他の措置の内容		【記載例】 「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		[　] ＜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	【記載例】 全国サーバと都道府県サーバの間の通信では相互認証を実施しているため、認証できない相手先への情報の提供はなされないことがシステム上担保される。 また、自都道府県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。 （以下は回線連携を用いる場合に追記してください） 回線連携を用いる場合、都道府県サーバの代表端末又は業務端末から庁内システム（宛名管理システムを含む。）へのアクセスは、共有フォルダだけに制限する。また、都道府県サーバの代表端末又は業務端末と庁内のネットワーク間の接続はファイアウォールを経由することとし、必要な通信以外は行えないように制限する。
リスクへの対策は十分か	[ ] ＜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	【記載例】 ・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 ：全国サーバと都道府県サーバの間の通信では相互認証を実施しているため、認証できない相手先への情報の提供はなされないことがシステム上担保される。 （以下は回線連携を用いる場合に追記してください） ：回線連携を用いる場合、都道府県サーバの代表端末又は業務端末から庁内システム（宛名管理システムを含む。）へのアクセスは、共有フォルダだけに制限する。また、都道府県サーバの代表端末又は業務端末と庁内のネットワーク間の接続はファイアウォールを経由することとし、必要な通信以外は行えないように制限する。
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）における その他のリスク及びそのリスクに対する措置	
6. 情報提供ネットワークシステムとの接続	[●]接続しない（入手）　[●]接続しない（提供）
リスク1：目的外の入手が行われるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2：安全が保たれない方法によって入手が行われるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3：入手した特定個人情報が不正確であるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク4：入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク5：不正な提供が行われるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク6：不適切な方法で提供されるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

リスク7：誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク		
リスクに対する措置の内容		
リスクへの対策は十分か	[ ]	＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置		
―		
7．特定個人情報の保管・消去		
リスク1：特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[4）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	[ ]	＜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	[ ]	＜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	[ ]	＜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	[ ]	＜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	【記載例】 ・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。 ・都道府県においては、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	[ ]	＜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	【記載例】 ・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（ほかに侵入検知システム（ＩＤＳ）／侵入防御システム（ＩＰＳ）の導入を予定している場合は追記する。）を導入する。 ・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	[ ]	＜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	[ ]	＜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	[ ]	＜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	[1）　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	[ ]	＜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		【記載例】 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に実施し、保存する本人確認情報が最新であるかどうかを確認する。
リスクへの対策は十分か		[　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3：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		[　] ＜選択肢＞ 1）定めている　2）定めていない
	手順の内容	【記載例】 ・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システム的に消去する。 ・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、物理的粉砕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		[　] ＜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		[　] ＜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	【記載例】 年に１回、担当部署内において実施している自己点検に用いるチェック項目に、「評価書の記載内容通りの運用がなされていること」に係る内容を追加し、運用状況を確認する。
②監査		[　] ＜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	【記載例】 ・内部監査 年に１回、組織内に置かれた監査担当により、以下の観点による自己監査を実施し、監査結果を踏まえて体制や規定を改善する。 ・評価書記載事項と運用実態のチェック ・個人情報保護に関する規定、体制整備 ・個人情報保護に関する人的安全管理措置 ・職員の役割責任の明確化、安全管理措置の周知・教育 ・個人情報保護に関する技術的安全管理措置 ・外部監査 民間機関等より調達する外部監査事業者による監査を実施し、監査結果を踏まえて体制や規定を改善する。
2. 従業者に対する教育・啓発		
従業者に対する教育・啓発		[　] ＜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	【記載例】 ・住基ネット関係職員（任用された派遣要員、非常勤職員、臨時職員等を含む。）に対して、初任時及び一定期間毎に、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。 ・住基ネットの各責任者に対して、その管理に関する必要な知識や技術を習得させる研修を実施するとともに、その記録を残す。
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		
②請求方法		
	特記事項	
③手数料等	[ ]　＜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	[ ]　＜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い合わせ		
①連絡先		
②対応方法		

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	[ ] ＜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	
②実施日・期間	
③期間を短縮する特段の理由	
④主な意見の内容	
⑤評価書への反映	
3. 第三者点検	
①実施日	
②方法	
③結果	
4. 特定個人情報保護委員会の承認【行政機関等のみ】	
①提出日	―
②特定個人情報保護委員会による審査	―