資料1

特定個人情報保護評価書（全項目評価書）

評価書番号	評価書名
1	住民基本台帳ネットワーク及び番号制度関連事務 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

地方公共団体情報システム機構（以下「機構」という。）は、住民基本台帳ネットワーク（以下「住基ネット」という。）及び番号制度関連事務における特定個人情報ファイルの取扱いにあたり、特定個人情報ファイルの取扱いが個人のプライバシー等の権利利益に影響を及ぼしかねないことを認識し、特定個人情報の漏えいその他の事態を発生させるリスクを軽減させるために適切な措置を講じ、もって個人のプライバシー等の権利利益の保護に取り組んでいることを宣言する。

特記事項	・機構は、住民基本台帳法に基づき、住民の利便の増進と国及び地方公共団体の行政の合理化に資するため、全国共通の本人確認を行うために必要最小限の情報のみを保有する。具体的には、4情報（氏名、住所、生年月日、性別）、個人番号、住民票コード及びこれらの変更情報であり、所得額や社会保障給付情報などの税・社会保障・災害対策業務情報は保有しない。 また、市町村長（特別区の区長を含む。以下同じ。）から法令上の委任を受けて行うこととなる個人番号カード発行のため、上記に掲げる以外の情報（送付先情報）を保有するが、使用目的を厳格に定めている。 ・内部による不正利用の防止のため、システム操作者に守秘義務を課し、生体認証やパスワードにより操作者を限定、追跡調査のためにコンピュータの使用記録を保存、照会条件を限定する等の対策を講じている。 ・外部との接続にあたっては、専用回線を利用、機構が管理するファイアウォールによる厳重な通信制御、侵入検知システム（IDS）による侵入検知、通信相手となるコンピュータとの相互認証、通信データの暗号化、通信プロトコルに独自のアプリケーションを用いる等の厳格な不正アクセス対策を講じている。

評価実施機関名

地方公共団体情報システム機構

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26年4月　様式4］

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及び番号制度関連事務
②事務の内容　※	住民基本台帳ネットワーク及び番号制度関連事務は、以下の、「1．個人番号の生成・通知に係る事務」、「2．本人確認情報の提供及び保存等に係る事務」、「3．個人番号カードに係る事務」に分かれる。 1．個人番号の生成・通知に係る事務（※詳細は、「（別添1）業務の内容」を参照） (1)個人番号の生成・通知 ・個人番号は市町村長が指定することとされている（番号法第7条第1項）が、付番対象者は各市町村をまたがり、それぞれ重複のない番号を指定すべきことから、機構にて、個人番号とすべき番号を生成することとされている（番号法第8条第2項）。 ・そのため機構では、市町村長からの要求に基づき、個人番号とすべき番号を生成するため、市町村長から受領した住民票コードを元に個人番号とすべき番号を生成し、当該住民の住民票コードと対応付けて管理する。 ・市町村長からの要求に基づき、住民票コードに対応付く個人番号とすべき番号を通知する。 (2)個人番号の変更 ・番号法第7条第2項に基づき住民からの請求又は市町村長の職権（当該市町村において個人番号の漏えい等が発生し、本人の請求を待たず個人番号を変更する必要がある場合に行使する）により個人番号を変更するため、市町村長からの要求により、個人番号生成システムで新しい個人番号とすべき番号を生成し、住民票コードと個人番号の対応付けを更新する。 (3)住民票コードの変更 ・住基法第30条の4第1項に基づく住民からの住民票コードの変更申請に基づき、変更前後の住民票コードと個人番号の対応付けを更新する。 2．本人確認情報の提供及び保存等に係る事務（※詳細は、「（別添1）業務の内容」を参照） 機構は、市町村における市町村CS、都道府県における都道府県サーバ及び機構における住基全国サーバ等により構成される「住民基本台帳ネットワークシステム」において、全国共通の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）、個人番号、住民票コード及びこれらの変更情報で構成される「機構保存本人確認情報ファイル」を作成し、住民に関する記録を正確に行う責務がある。そのため、本人確認情報の提供及び保存等に係る以下の事務を実施する。 (1)本人確認情報の更新 ・機構保存本人確認情報ファイルを最新の状態に保つため、都道府県知事から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する。 (2)市町村長等への本人確認情報の提供 ・市町村長、都道府県知事、国の機関等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機構保存本人確認情報ファイルから抽出し、照会元に提供する。 (3)情報提供ネットワークシステムへの住民票コードの通知 情報提供ネットワークシステムでは個人番号を情報連携のキーとせず、個人番号とは異なる「情報提供用個人識別符号」を情報連携のキーとする。 ・情報照会者・情報提供者又は情報提供等記録開示システムから要求を受け、情報提供ネットワークシステムに住民票コードを通知する。情報提供ネットワークシステムは機構から受領した住民票コードを元に符号を生成し、情報照会者・情報提供者又は情報提供等記録開示システムに通知する。 ・過去に通知した住民票コードに変更が生じた場合、変更前後の住民票コードを情報提供ネットワークシステムに通知する。 (4)本人確認情報開示 ・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機構保存本人確認情報ファイルから抽出し、開示請求者に提示する。 (5)本人確認情報整合 ・機構保存本人確認情報ファイルの正確性を担保するため、市町村長から本人確認情報を受領し、当該本人確認情報を用いて機構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。

	3. 個人番号カードに係る事務(※詳細は、「(別添1)業務の内容」を参照) (1)通知カードの印刷・住民への送付／個人番号カードの発行・市町村への送付 個人番号カードは、各種手続における個人番号の確認及び本人確認の手段として国民生活の利便性向上に資することを目的に、番号法第17条により市町村長が交付することとされている。 機構は、個人番号カードの交付主体である市町村長からの法令に基づく委任を受け、個人番号カード発行に係る以下の事務を行うことを予定している。 ・全住民に対して通知カード及び個人番号カード交付申請書(以下「交付申請書」という。)を送付するため、市町村長より送付先に係る情報(以下「送付先情報」という。)を受領し、通知カード及び交付申請書の印刷に係る情報を作成して委託事業者(印刷・送付事務)に提供する。 ・委託事業者(申請受付事務)より受領した申請書情報及びその他個人番号カードに搭載される情報をもとに個人番号カード発行に係る情報を作成し、委託事業者(カード発行事務)に個人番号カード発行を委託する。 (2)カード管理情報の連携 ・委託事業者(コールセンター事務)にて、住民から個人番号カードの紛失・盗難等に基づく一時停止の連絡を受け付けた際に、本人確認を行った上で、個人番号カード管理システムに対して一時停止申請を行う(あわせて、公的個人認証サービスに対し、電子証明書の一時保留要求を行う)。 ・個人番号カード管理システムにおいて個人番号カードの利用を一時停止するための処理を行い、一時停止した旨の情報を市町村長に通知する。
③対象人数	[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	個人番号生成システム
②システムの機能	(「1. 個人番号の生成・通知に係る事務」に対応) ・住基全国サーバから連携される、個人番号の生成に必要となる住民票コードのリストに基づいて個人番号とすべき番号を生成し、住民票コードと対応付けた個人番号とすべき番号のリスト(個人番号管理ファイル)を作成する(初期導入時)。 ・市町村CSより住基全国サーバを経由して受信した個人番号生成要求に基づき、住民票コードに対応する個人番号とすべき番号を生成し、要求元に通知する。 ・市町村CSより住基全国サーバを経由して受信した個人番号変更要求に基づき、住民票コードに対応する新しい個人番号とすべき番号を生成し、個人番号管理ファイルの対応付けを更新した後に要求元に通知する。 ・住基全国サーバから住民票コードの変更通知を受け取り、個人番号管理ファイルの対応付けを更新する。
③他のシステムとの接続	[ ] 情報提供ネットワークシステム　[ ] 庁内連携システム [○] 住民基本台帳ネットワークシステム　[ ] 既存住民基本台帳システム [ ] 宛名システム等　[ ] 税務システム [ ] その他 ( )

システム2	
①システムの名称	住民基本台帳ネットワークシステム ※機構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、「住基全国サーバ」において管理がなされているため、以降、住基全国サーバについて記載する。
②システムの機能	(「2. 本人確認情報の提供及び保存等に係る事務」に対応) ・都道府県サーバから本人確認情報の更新データを受信し、機構保存本人確認情報ファイルを更新し、通知元都道府県サーバに本人確認情報更新結果を送信する。 ・市町村長等からオンライン又は媒体で本人確認情報照会要求を受け取り、住民票コード、個人番号又は4情報の組合せにより機構保存本人確認情報ファイルを検索する。本人確認情報照会要求により検索した、本人確認情報を市町村長等へ提供する。 ・番号法上の情報照会者・情報提供者又は情報提供等記録開示システムからの情報提供用個人識別符号要求の際に通知された個人番号又は利用者証明用電子証明書のシリアル番号(※)で最新の本人確認情報を検索し、情報提供ネットワークシステムに住民票コードを提供する。 ・開示請求内容に相当する情報を機構保存本人確認情報ファイルから抽出し、結果を帳票へ出力する。 ※情報提供等記録開示システムへログインする際に個人番号カードを用いて認証を行った場合、個人番号カードの利用者証明用電子証明書のシリアル番号を用いる。なお、住基カードを用いてログインした場合、住基カードの署名用電子証明書の4情報を用いる。
③他のシステムとの接続	[○] 情報提供ネットワークシステム　　[ ] 庁内連携システム [ ] 住民基本台帳ネットワークシステム　　[ ] 既存住民基本台帳システム [ ] 宛名システム等　　[ ] 税務システム [○] その他 (個人番号生成システム、個人番号カード管理システム、情報提供等記録開示システム、公的個人認証サービス)
システム3	
①システムの名称	個人番号カード管理システム
②システムの機能	(「3. 個人番号カードに係る事務」に対応) ・通知カード及び交付申請書を住民に送付するために、市町村長より既存住基システムから市町村CSを経由して送付先情報を受領し、委託事業者(印刷・送付事務)に提供する。 ・利用者から提出された交付申請書に基づき個人番号カード発行情報を作成し、カード発行システムに連携する。 ・盗難・紛失時に個人番号カード向けコールセンターから連絡を受け、個人番号カード及び電子証明書を一時的に利用停止する。
③他のシステムとの接続	[ ] 情報提供ネットワークシステム　　[ ] 庁内連携システム [○] 住民基本台帳ネットワークシステム　　[ ] 既存住民基本台帳システム [ ] 宛名システム等　　[ ] 税務システム [○] その他 (委託事業者における個人番号カード発行システム、公的個人認証サービス)

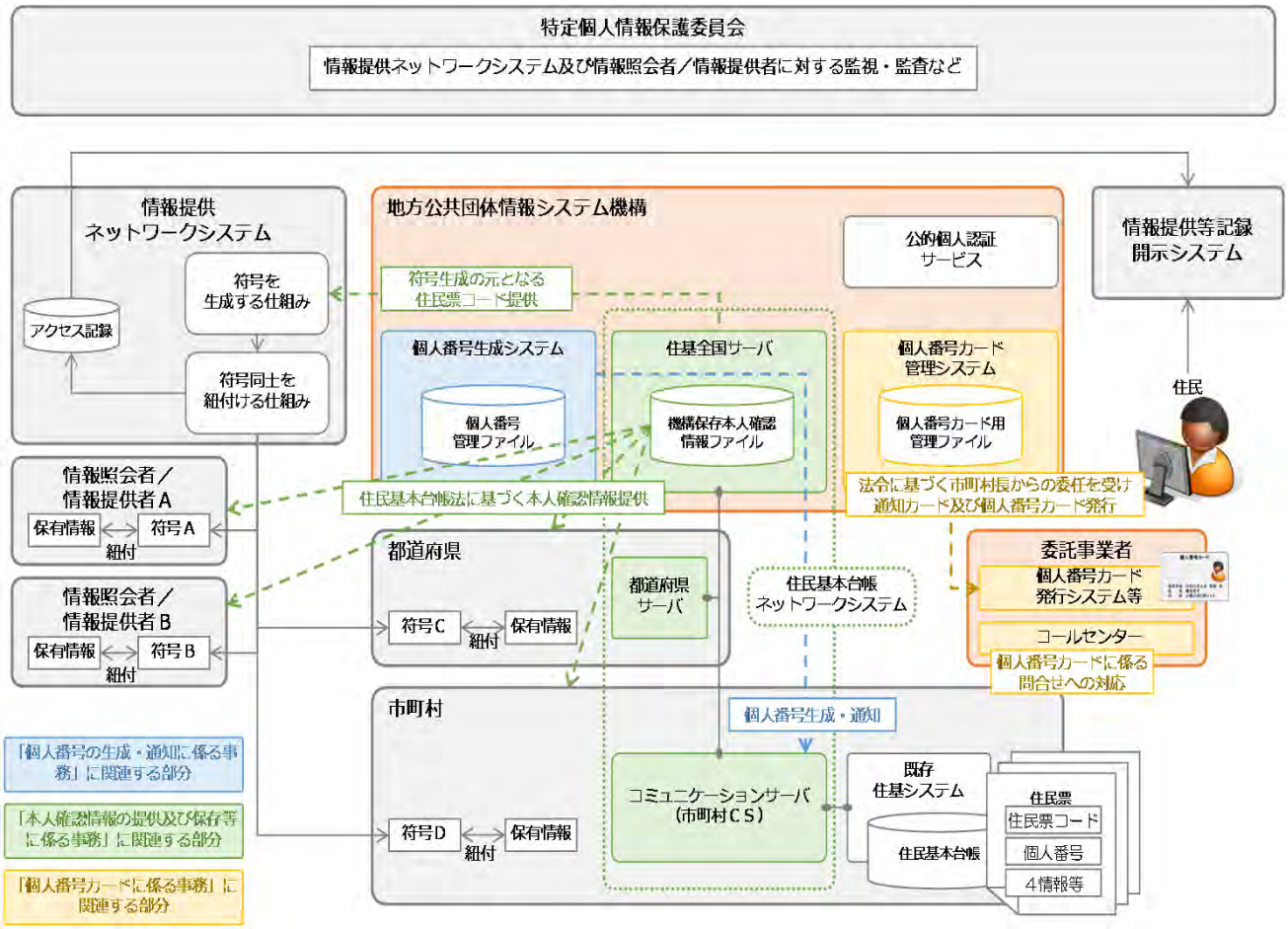
3. 特定個人情報ファイル名

(1) 個人番号管理ファイル
(2) 機構保存本人確認情報ファイル
(3) 個人番号カード用管理ファイル

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	機構では、以下の3ファイルを下記に記載の通りの目的遂行のため取り扱う。 (1) 個人番号管理ファイル ①個人番号とすべき番号を生成し市町村長に通知する ②個人番号が変更される際に、新しい個人番号とすべき番号を市町村長に通知するとともに、個人番号とすべき新旧の番号及び住民票コードとの紐づけを管理する ③住民票コードが変更される際に個人番号とすべき番号と住民票コードとの紐づけを管理する (2) 機構保存本人確認情報ファイル ①全国共通の本人確認を行うための社会的基盤として住民に関する記録を正確に行う ②市町村長、都道府県知事、国の機関等に対し本人確認情報を提供する ③情報提供用個人識別符号生成を行う情報提供ネットワークシステムに対し、符号の元となる住民票コードを提供する 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 (3) 個人番号カード用管理ファイル ①住民に対し、通知カード及び交付申請書を送付する ②個人番号カードを発行し、市町村へ送付する ③個人番号カードの発行状況を管理する ④住民からの個人番号カードに関する問合せ等に対応する
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。 また、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。
5. 個人番号の利用 ※	
法令上の根拠	1. 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 (平成25年5月31日法律第27号)(以下「番号法」という。) ・第8条(個人番号とすべき番号の生成) ・第17条第1項、第3項、第6項(個人番号カードの交付等) 2. 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)(以下「住基法」という。) ・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9(国の機関等への本人確認情報の提供) ・第30条の9の2(総務省への住民票コードの提供) ・第30条の10 (通知都道府県の区域内の市町村の執行機関への本人確認情報の提供) ・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12 (通知都道府県以外の都道府県の区域内の市町村の執行機関への本人確認情報の提供) ・第30条の15第4項(本人確認情報の利用) ・第30条の32第2項(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	[　　実施する　　] ＜選択肢＞ 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	住基法第30条の9の2(総務省への住民票コードの提供)
7. 評価実施機関における担当部署	
①部署	個人番号プロジェクト推進部
②所属長	総括部長　下仲　宏卓
8. 他の評価実施機関	
―	

（別添1）事務の内容

【前提】番号制度における機構の役割（概要）

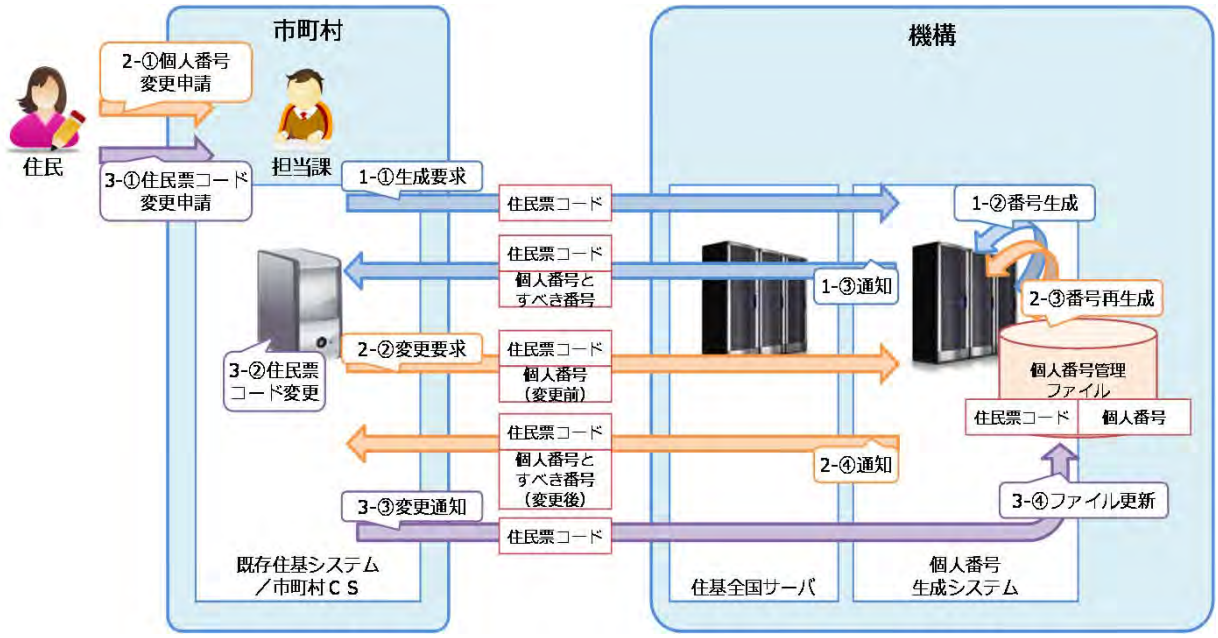


（備考）

番号制度全体における機構が担う役割の概要を、上図に示す。

（別添1）事務の内容

(1) 個人番号の生成・通知に係る業務（該当する特定個人情報ファイル：個人番号管理ファイル）



（備考）

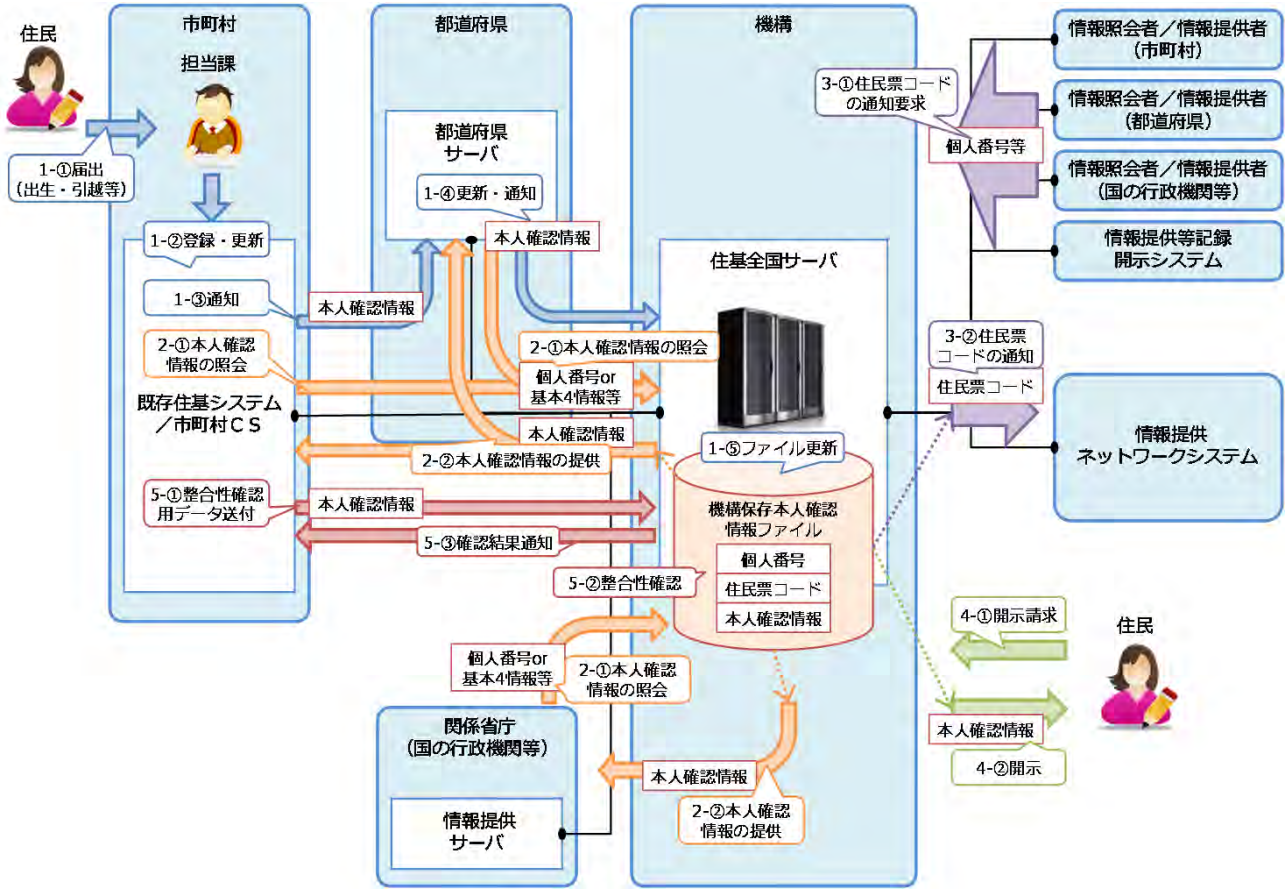
(1)-1.個人番号の生成・通知
1-① 市町村長より、当該市町村の住民の住民票コードに対応付く、個人番号とすべき番号の生成要求を受ける。
1-② 受領した住民票コードを元に個人番号とすべき番号を生成し、住民票コードと対応付けた「個人番号管理ファイル」に登録する。
1-③ 市町村長に対し、生成要求を受けた住民票コードに対応付く個人番号とすべき番号を通知する。

(1)-2.個人番号の変更
2-① 市町村長において、住民より個人番号の変更申請を受け付ける。
2-② 市町村長より、申請のあった個人番号及び当該個人番号に対応付く住民票コードを元に、個人番号の変更要求を受ける。
2-③ 受領した住民票コードを元に個人番号とすべき番号を再生成し、「個人番号管理ファイル」の住民票コードと個人番号の対応付けを更新する。
2-④ 市町村長に対し、再生成した個人番号とすべき番号を、受領した住民票コードに対応付けて通知する。

(1)-3.住民票コードの変更
3-① 市町村長において、住民より住民票コードの変更申請を受け付ける。
3-② 市町村長の既存住基システムにおいて、住民票コードを更新する。
3-③ 市町村長より、申請のあった住民票コードの変更通知を受ける。
3-④ 受領した住民票コードを元に、「個人番号管理ファイル」の住民票コードと個人番号の対応付けを更新する。

（別添1）事務の内容

(2) 本人確認情報の提供及び保存等に係る業務（該当する特定個人情報ファイル：機構保存本人確認情報ファイル）



（備考）

(2)-1.本人確認情報の更新
1-① 住民より、住民異動に関する届出を受け付ける。
1-② 異動情報を既存住基システムに登録する。
1-③ 既存住基システムより、市町村CSを経由して、都道府県サーバに対し本人確認情報の変更情報を通知する。
1-④ 都道府県サーバは、市町村CSから受信したデータを元に保存する本人確認情報を更新した後、住基全国サーバ（機構）に対し本人確認情報の変更情報を通知する。
1-⑤ 都道府県サーバ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。

(2)-2.市町村長、都道府県知事、国の機関等への本人確認情報の提供
2-① 市町村長、都道府県知事、国の機関等より、個人番号又は基本4情報等をキーワードとした本人確認情報の照会を受ける。
2-② 当該個人の本人確認情報を「機構保存本人確認情報ファイル」から抽出し、照会元に提供する。

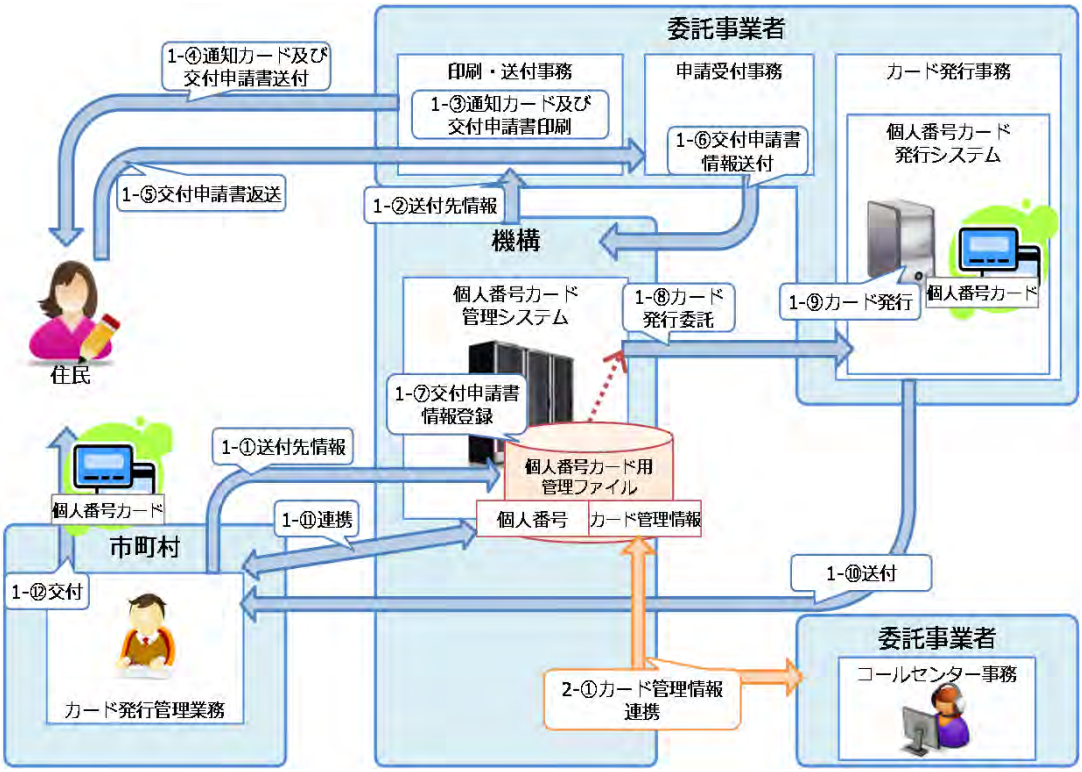
(2)-3.情報提供ネットワークシステムへの住民票コードの通知
3-① 番号法上の情報照会者／情報提供者又は情報提供等記録開示システムより、個人番号等に基づく符号取得要求を受ける。
3-② 符号取得対象者の個人番号に対応する住民票コードを「機構保存本人確認情報ファイル」から抽出し、情報提供ネットワークシステムに通知する。

(2)-4.本人確認情報開示
4-① 住民より本人確認情報の開示請求を受け付ける。
4-② 開示請求者（住民）に対し、当該個人の本人確認情報を開示する。

(2)-5.本人確認情報整合
5-① 市町村CSより、住基全国サーバに対し、整合性確認用の本人確認情報を送付する。
5-② 住基全国サーバにおいて、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機構保存本人確認情報ファイルの整合性確認を行う。
5-③ 住基全国サーバより、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

(3) 個人番号カードに係る業務（該当する特定個人情報ファイル：個人番号カード用管理ファイル）



（備考）

(3)-1.通知カードの印刷・住民への送付／個人番号カードの発行・市町村への送付
1-① 市町村長より、個人番号カードの送付先情報を受領し、「個人番号カード用管理ファイル」に登録する。
1-② 委託事業者（印刷・送付事務）に対し、送付先情報を送付する。
1-③ 委託事業者（印刷・送付事務）において、通知カード及び交付申請書を印刷する。
1-④ 委託事業者（印刷・送付事務）において、受領した送付先住所に対し、通知カード及び交付申請書を送付する。
1-⑤ 委託事業者（申請受付事務）において、住民より、個人番号カードの交付申請書（記入済）を受領する。
1-⑥ 委託事業者（申請受付事務）より、個人番号カードの交付申請書情報を受領する。
1-⑦ 受領した交付申請書情報を、「個人番号カード用管理ファイル」に登録する。
1-⑧ 委託事業者（カード発行事務）に対し、「個人番号カード用管理ファイル」を元に、個人番号カード発行を委託する。
1-⑨ 個人番号カード発行システムにおいて、個人番号カードを発行する。
1-⑩ 発行された個人番号カードを、送付先住所地市町村長に対し送付する。
1-⑪ 個人番号カードの交付及び失効等に係る情報を個人番号カード管理システムと連携する。
1-⑫ 個人番号カードを住民に交付する。
※個人番号カードの発行・市町村への送付については上記の事務フローを想定しているが、国民にとってより利便性の高い交付申請方法も引き続き検討する。本評価書においては上記の事務フローを想定し評価を実施している。

(3)-2.カード管理情報の連携
2-① 盗難・紛失等による個人番号カードの一時利用停止の対応のため、委託事業者（コールセンター事務）に個人番号カードの運用状況、電子証明書の状態等のカード管理情報を連携する。

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) 個人番号管理ファイル		
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		[　　1,000万人以上　　] ＜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 ※		住民（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・死亡等の事由により住民票が消除された者（以下「消除者」という。）を含む
	その必要性	法令に基づいて、住民票コードを有する上記の「対象となる本人の範囲」全員に個人番号を付番することとなっており、個人番号とすべき番号の生成・管理の事務を実施する上で、本特定個人情報ファイル（個人番号管理ファイル）で個人番号の付番対象者全員の個人番号を保有する必要があるため。
④記録される項目		[　　10項目未満　　] ＜選択肢＞ 1) 10項目未満　2) 10項目以上50項目未満 3) 50項目以上100項目未満　4) 100項目以上
	主な記録項目 ※	・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、その他住民票関係情報 ：個人番号は住民票コードを元に生成されることが法令上規定されていることから、住民票コードと対応付けて管理する必要があり、その際に、個人番号を生成した日時（生成日時）及び当該個人番号を通知した日付（払出日付）を合わせて記録する。 また、住民票コード又は個人番号の変更により、ファイル中の個人番号と住民票コードの対応付けが更新されることが想定されるため、当該データが最新のものか履歴なのかを判別するための項目（最新／履歴）が必要となる。
	全ての記録項目	別添2を参照。
⑤保有開始日		平成27年5月予定
⑥事務担当部署		住基全国センター

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　（　） [　] 民間事業者　（　） [○] その他　（住民票コードは市町村長から住基全国サーバを経由して入手し、個人番号は住民票コードを元に個人番号生成システムにて生成する）
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　（住民票コードは市町村長から住基全国サーバを経由して入手し、個人番号は住民票コードを元に個人番号生成システムにて生成する）
③入手の時期・頻度			番号法施行日（平成27年10月予定）までに、個人番号の付番対象者全員の住民票コードに対応する個人番号とすべき番号を一括して生成し、ファイルに格納する。 施行日以降は、個人番号の生成要求や、個人番号の変更要求等を契機として、都度入手・生成し、ファイルに格納する。
④入手に係る妥当性			法令に基づいて個人番号とすべき番号の生成・管理の事務を実施する上で、本特定個人情報ファイル（個人番号管理ファイル）で個人番号の付番対象者全員の個人番号を住民票コードに対応付けて保有する必要があるため。
⑤本人への明示			機構が個人番号の生成のため住民票コードを市町村長から入手することは、住基法第30条の15第4項（本人確認情報の利用）及び番号法第8条第2項（個人番号とすべき番号の生成）に明示されている。
⑥使用目的 ※			個人番号の付番及び通知並びに管理（住民票コード又は個人番号の変更、対応付けの更新を含む）を行う。
	変更の妥当性		―
⑦使用の主体	使用部署 ※		住基全国センター
	使用者数		[　10人以上50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 ※			・市町村長からの個人番号生成要求(既存住基システム→市町村CS→住基全国サーバ)を受け、住民票コードに対応する個人番号とすべき番号を生成し、市町村長に通知する。 ・市町村長からの個人番号変更要求(既存住基システム→市町村CS→住基全国サーバ)を受け、住民票コードに対応する新しい個人番号とすべき番号を生成し、個人番号管理ファイルの対応付けを更新した後に市町村長に通知する。 ・住民票コードが変更された場合は、個人番号管理ファイルの対応付けを更新する。
	情報の突合 ※		・市町村CSからの個人番号生成要求又は個人番号変更要求の際に提示された住民票コードとの突合を行う。 ・住基全国サーバからの住民票コードの変更通知の際に提示された変更前住民票コードとの突合を行う。 ※なお、上記のいずれについてもファイル単位での突合は行わず、特定個人情報ファイルに記録される特定個人情報について他の個人情報との統合（データマッチング）や解析（データマイニング）は行わない。
	情報の統計分析 ※		個人番号管理ファイルに記録される個人情報を用いた統計分析は行わない。 なお、システムの機能としては実装されないが、今後、番号制度の運用において必要とされた場合、個人番号の生成件数や変更件数等の集計を行うことが見込まれる。
	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5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 ※		[　　委託しない　　]　　＜選択肢＞ 1）委託する　　2）委託しない （　　）件
委託事項1		
①委託内容		
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 ※	
	その妥当性	
③委託先における取扱者数		[　　]　　＜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
④委託先への特定個人情報ファイルの提供方法		[　]専用線　　[　]電子メール　　[　]電子記録媒体（フラッシュメモリを除く。） [　]フラッシュメモリ　　[　]紙 [　]その他　（　　）
⑤委託先名の確認方法		
⑥委託先名		
再委託	⑦再委託の有無 ※	[　　]　　＜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	
	⑨再委託事項	

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　（　　）件 [　]行っていない
提供先1	市町村長
①法令上の根拠	番号法第8条第2項（個人番号とすべき番号の生成）
②提供先における用途	個人番号の付番対象者に対し、個人番号を通知する。
③提供する情報	住民票コード、個人番号
④提供する情報の対象となる本人の数	[　　1,000万人以上　　]　　＜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	特定個人情報ファイルの対象者の範囲と同様
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 [○]その他　（ 住民基本台帳ネットワークシステム　　）
⑦時期・頻度	番号法施行日（平成27年10月予定）までの各市町村における個人番号の通知の準備行為のため、対象者全員の個人番号を住所地市町村（1，741団体（平成26年4月5日現在））ごとにまとめて提供する。 制度導入後は、市町村長からの個人番号の生成要求又は個人番号の変更要求を契機として、都度提供する。

移転先1		
①法令上の根拠		
②移転先における用途		
③移転する情報		
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		
⑥移転方法	[　] 庁内連携システム [　] 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。） [　] 紙
⑦時期・頻度		

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建物の中で、さらに入退室管理（※）を行っている部屋（サーバ室）に設置したサーバ内に保管する。 また、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。 ※サーバ室内への入室権限を持つ者を限定し、入退室管理カード等によりサーバ室に入退室する者が権限を有することを確認する等の管理を行う。
②保管期間	期間	[　定められていない　]　＜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	・個人番号の生成に関する問い合わせ対応のため、過去の記録を保存する必要がある。 ・生成済みの個人番号と同一の番号を生成しないために恒久的に保存する必要がある。
③消去方法		上記理由から消去しない

7．備考
特になし。

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) 機構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		[　　1,000万人以上　　] ＜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 ※		住民（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） ※消除者を含む
	その必要性	本特定個人情報ファイル（機構保存本人確認情報ファイル）において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 ※	・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 ：法令に基づき住民に関する記録を正確に行う上で、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ため。
	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		住基全国センター

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　（ 都道府県知事、市町村長　　） [　] 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　（ 住民基本台帳ネットワークシステム　　）
③入手の時期・頻度		住民票の記載事項において、本人確認情報の変更（転入等）又は新規作成（出生等）が発生した都度入手する。
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、全国共通の本人確認を行う上で、市町村の住民基本台帳の記載事項に変更が生じた都度、当該市町村を取りまとめる都道府県を経由して変更後の情報を入手する必要がある。 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。 ※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日の稼働後約10年間、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。
⑤本人への明示		機構が都道府県知事より当該都道府県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7（都道府県知事から機構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 ※		本特定個人情報ファイル（機構保存本人確認情報ファイル）において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 ※	住基全国センター
	使用者数	[　10人以上50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　※		・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→住基全国サーバ)、機構保存本人確認情報ファイルを更新する。 ・市町村長等からの本人確認情報の照会要求を受け(例:市町村CS→住基全国サーバ)、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機構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する(例:住基全国サーバ→市町村CS)。 ・番号法上の情報照会者・情報提供者又は情報提供等記録開示システムからの情報提供用個人識別符号要求を受け(情報照会者・情報提供者等→住基全国サーバ)、通知された個人番号等を元に機構保存本人確認情報ファイルを検索し、該当する個人の住民票コードを情報提供ネットワークシステムに提供する(住基全国サーバ→情報提供ネットワークシステム)。 ・住民からの開示請求に基づき(住民→機構窓口→住基全国サーバ)、当該住民の本人確認情報を機構保存本人確認情報から抽出し、書面により提供する(住基全国サーバ→帳票出力→住民)。 ・機構保存本人確認情報ファイルの正確性を担保するため、市町村長から本人確認情報を受領し(市町村CS→住基全国サーバ)、当該本人確認情報を用いて機構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　※	・機構保存本人確認情報ファイルを更新する際に、都道府県サーバから受信した本人確認情報の更新データの住民票コードとの突合を行う。 ・市町村長等からの照会に基づい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。 ・情報提供ネットワークシステムに住民票コードを提供する際に、符号取得対象者の個人番号との突合を行う。 ・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。 ・都道府県サーバとの整合処理を実施するため、4情報等との突合を行う。 ※特定個人情報ファイルに記録される特定個人情報について他の個人情報との統合(データマッチング)や解析(データマイニング)は行わない。
	情報の統計分析　※	機構保存本人確認情報ファイルに記録される個人情報を用いた統計分析は行わない。 なお、住基法第30条の16(報告書の公表)に基づき、機構保存本人確認情報の提供状況及び住民票コードの提供状況について官報に掲載する必要があることから、当該情報の提供件数等を集計する。 また、本人確認情報更新の通知元である都道府県知事から報告される更新件数と、機構において更新した本人確認情報の件数が整合すること確認するため、本人確認情報の更新件数等を集計する。
	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 ※		[委託しない] ＜選択肢＞ 1）委託する 2）委託しない （ ）件
委託事項1		
①委託内容		
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 ※	
	その妥当性	
③委託先における取扱者数		[ ] ＜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
④委託先への特定個人情報ファイルの提供方法		[ ]専用線 [ ]電子メール [ ]電子記録媒体（フラッシュメモリを除く。） [ ]フラッシュメモリ [ ]紙 [ ]その他 （ ）
⑤委託先名の確認方法		
⑥委託先名		
再委託	⑦再委託の有無 ※	[ ] ＜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	
	⑨再委託事項	

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 （ 3 ）件 [ ] 移転を行っている （ ）件 [ ] 行っていない
提供先1	住基法に基づき機構保存本人確認情報の提供が認められている地方公共団体、行政機関等
①法令上の根拠	（住基法） ・第30条の9（国の機関等への本人確認情報の提供） ・第30条の10（通知都道府県の区域内の市町村の執行機関への本人確認情報の提供） ・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12（通知都道府県以外の都道府県の区域内の市町村の執行機関への本人確認情報の提供）
②提供先における用途	住基法別表に掲げる、各地方公共団体、行政機関等における利用が認められた事務（例：市町村又は都道府県における地方税の賦課徴収又は地方税に関する調査に係る事務、日本年金機構における年金の給付又は一時金の支給に関する事務）の処理に用いる。
③提供する情報	住民票コード、氏名、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	[1,000万人以上] ＜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	特定個人情報ファイルの対象者の範囲と同様
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 [○] その他 （ 住民基本台帳ネットワークシステム ）
⑦時期・頻度	定期的（1ヶ月に1度程度）に一括して又は照会の要求があった都度 （提供先：24件（平成24年8月～平成25年7月実績））
提供先2	情報提供ネットワークシステム
①法令上の根拠	・住基法第30条の9の2（総務省への住民票コードの提供）
②提供先における用途	受領した住民票コードを元に、情報提供ネットワークシステムを通じた情報連携に用いる符号を生成する。
③提供する情報	住民票コード
④提供する情報の対象となる本人の数	[1,000万人以上] ＜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	特定個人情報ファイルの対象者の範囲と同様
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 [ ] その他 （ ）
⑦時期・頻度	番号法上の情報照会者、情報提供者又は情報提供等記録開示システムから符号生成要求があった都度

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、追加又は削除の申し出を行う。
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	[　　1,000万人以上　　] ＜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	特定個人情報ファイルの対象者の範囲と同様
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 [　]その他　（　　）
⑦時期・頻度	開示請求があった都度（平成25年度実績：3件）
移転先1	
①法令上の根拠	
②移転先における用途	
③移転する情報	
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	
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 [　]その他　（　　）
⑦時期・頻度	

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建物の中で、さらに入退室管理(※)を行っている部屋(サーバ室)に設置したサーバ内に保管する。 また、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。 ※サーバ室内への入室権限を持つ者を限定し、入退室管理カード等によりサーバ室に入退室する者が権限を有することを確認する等の管理を行う。
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	・住民票に記載された本人確認情報は、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(最終改正:平成24年3月31日時点)第30条の11(指定情報処理機関における本人確認情報の保存期間)に定める期間(履歴の情報:5年間、消除者の情報:原則5年間(最長80年間))保管する。
③消去方法		機構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		
特になし。		

Ⅱ　特定個人情報ファイルの概要

1. 特定個人情報ファイル名		
(3) 個人番号カード用管理ファイル		
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		[　　1,000万人以上　　] ＜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 ※		住民（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）
	その必要性	番号法第7条第2項（指定及び通知）に基づき、通知カードを個人番号の付番対象者全員に送付する必要がある。 また、同法第17条第1項（個人番号カードの交付等）に基づき、住民からの申請により、その者に係る個人番号カードを発行する必要がある。 機構は、これらの事務を市町村長から委任を受けて実施することを予定している。
④記録される項目		[　　100項目以上　　] ＜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　（送付先の情報、送付先情報を作成した市町村の情報、交付場所の情報、個人番号カード送付場所の情報、通知カードの印刷情報、交付申請書の情報、カード発行委託情報、カード管理台帳情報等）
	その妥当性	法令に規定された個人番号カードの券面記載事項のほか、通知カード及び個人番号カードの送付先に係る情報、交付主体（市町村）に係る情報及びその他カード発行状況の管理等に必要な情報を保管する必要がある。
	全ての記録項目	別添2を参照。
⑤保有開始日		平成27年10月予定
⑥事務担当部署		個人番号カード担当部署

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 （ 市町村長 ） [ ] 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 （ 住民基本台帳ネットワークシステム ）
③入手の時期・頻度			・市町村（電子記録媒体又は住民基本台帳ネットワークシステムにて入手） ：通知カード及び交付申請書の送付先に係る情報は、保有開始日から一定の期間にまとめて入手する（以降、新たに個人番号の通知対象者が生じた都度入手する）。 ・本人（紙にて入手） ：個人番号の通知対象者へ送付した通知カード及び交付申請書の到着以降、個人番号カードの交付希望者により返送された交付申請書（記載済み）より随時入手する。
④入手に係る妥当性			①送付先情報（市町村より入手） ：番号法第7条第2項（指定及び通知）に基づき、通知カードを個人番号の付番対象者全員に送付するため、通知カードの送付先情報が必要となる。 ②交付申請書(申請者本人より入手） ：番号法第17条（個人番号カードの交付等）に基づき、交付希望者に対して個人番号カードを交付する際に、交付に必要な情報（交付申請書に不備があった場合の連絡先、交付を希望する場所、顔写真等）をあらかじめ入手する必要がある。
⑤本人への明示			市町村長より法令に基づく委任を受ける予定。
⑥使用目的 ※			法令による権限委任に基づき、個人番号カードの交付等に係る事務の処理を行う。
	変更の妥当性		―
⑦使用の主体	使用部署 ※		個人番号カード担当部署
	使用者数		[10人以上50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 ※			・全住民に対して通知カード及び交付申請書を送付するため、市町村長より送付先情報を受領（既存住基システム→市町村CS→個人番号管理システム）し、通知カード及び交付申請書の印刷に係る情報を作成して委託事業者（印刷・送付事務）に提供する。 ・委託事業者（申請受付事務）より受領した申請書情報及びその他個人番号カードに搭載される情報（電子証明書情報等）をもとにカード発行に係る情報を作成し、委託事業者（カード発行事務）にカード発行を委託する（住民→委託事業者（申請受付事務）→個人番号カード管理システム→個人番号カード発行システム）。 ・委託事業者（コールセンター事務）にて、住民からの個人番号カード一時停止申請を受け付ける際の本人確認用の利用者情報の提供及び一時停止要求を市町村長に連携する。また、一時停止事前準備として、一時停止申請受付に必要な情報の取得・更新を行う。
	情報の突合 ※		・個人番号カードの発行状況等を管理するため、当該個人の4情報等との突合を行う。 ・個人番号カードに関する問合せの対応のため、当該個人の4情報等との突合を行う。 ※なお、上記のいずれについてもファイル単位での突合は行わず、特定個人情報ファイルに記録される特定個人情報について他の個人情報との統合（データマッチング）や解析（データマイニング）は行わない。
	情報の統計分析 ※		個人番号カード管理ファイルに記録される個人情報を用いた統計分析は行わない。 なお、カード発行の委託状況及び発行状況の進捗を把握するため、送付先情報又は申請書情報の処理状況（現在どの状態にあるか）や、個人番号カードの発行枚数及び有効枚数等の集計は行う。
	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 （ 2 ） 件
委託事項1		番号通知書類の印刷及び受付並びに個人番号カードの発行・送付に係る事務
①委託内容		・個人番号通知対象者に対して送付する通知カード及び交付申請書の印刷に係る事務（印刷・送付事務） ・交付申請書の受付に係る事務（申請受付事務） ・個人番号カードの交付申請に基づく個人番号カードの発行及び市町村への送付に係る事務（カード発行事務）
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一部] ＜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	[1,000万人以上] ＜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 ※	特定個人情報ファイルの対象者の範囲と同様
	その妥当性	番号法第7条第2項（指定及び通知）に基づき、通知カードを個人番号の付番対象者全員に送付する必要がある。 また、同法第17条第1項（個人番号カードの交付等）に基づき、住民からの申請により、その者に係る個人番号カードを発行する必要がある。
③委託先における取扱者数		[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
④委託先への特定個人情報ファイルの提供方法		[○] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [ ] その他 （ ）
⑤委託先名の確認方法		委託先が決定した際には、機構ホームページにて公表する。
⑥委託先名		未定
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	再委託を行う場合は、機構において、委託先より書面による再委託申請を受け付け、委託先と再委託先が秘密保持に関する契約を締結していること等、再委託先における安全管理措置などを確認し、内部における決裁及び必要に応じて所管省庁の承認手続きを経た後に承認する。
	⑨再委託事項	・通知カード及び交付申請書の印刷 ・交付申請書の受付 ・個人番号カードの発行

委託事項2		コールセンター事務
①委託内容		通知カード及び個人番号カードに関する各種問合せ対応に係る事務
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一部]　＜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	[1,000万人以上]　＜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 ※	個人番号カードの交付対象者
	その妥当性	通知カード及び個人番号カードに関する各種問合せへの対応のため、個人番号カード交付対象者全ての情報を取り扱う必要があるため。
③委託先における取扱者数		[100人以上500人未満]　＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[○]専用線　[ ]電子メール　[ ]電子記録媒体（フラッシュメモリを除く。） [ ]フラッシュメモリ　[ ]紙 [ ]その他　（　）
⑤委託先名の確認方法		委託先が決定した際には、機構ホームページにて公表する。
⑥委託先名		未定
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	再委託を行う場合は、機構において、委託先より書面による再委託申請を受け付け、委託先と再委託先が秘密保持に関する契約を締結していること等、再委託先における安全管理措置などを確認し、内部における決裁及び必要に応じて所管省庁の承認手続きを経た後に承認する。
	⑨再委託事項	通知カード及び個人番号カードに関する各種問合せ対応

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 （ ）件 [ ] 行っていない
提供先1		市町村長
①法令上の根拠		総務省令に記載予定
②提供先における用途		市町村の窓口における個人番号カードの運用に関する事務（個人番号カードの交付前設定、交付、更新、一時停止、廃止、回収）において用いられる。
③提供する情報		個人番号、住民票コード、市町村コード、申請書ID、カード発行番号、カード有効期限、 処理結果コード、その他技術的情報
④提供する情報の対象となる本人の数		[1,000万人以上] ＜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		特定個人情報ファイルの対象者のうち、個人番号カードの交付申請を行った者
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 [○] その他 （ 住民基本台帳ネットワークシステム ）
⑦時期・頻度		市町村において個人番号カードに係る申請又は届出を受け付けた都度
移転先1		
①法令上の根拠		
②移転先における用途		
③移転する情報		
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		
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 [ ] その他 （ ）
⑦時期・頻度		
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建物の中で、さらに入退室管理（※）を行っている部屋（サーバ室）に設置したサーバ内に保管する。 また、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。 ※サーバ室内への入室権限を持つ者を限定し、入退室管理カード等によりサーバ室に入退室する者が権限を有することを確認する等の管理を行う。
②保管期間	期間	[10年以上20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	法令で定められる個人番号カードの有効期間を考慮し、有効期間内の個人番号カード保有者からの問合せや一時停止等の対応のために当該管理情報を保管する必要がある。
③消去方法		個人番号カード管理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		
特になし。		

（別添2）特定個人情報ファイル記録項目

（1）個人番号管理ファイル
1. 住民票コード、2. 個人番号、3. 最新／履歴、4. 生成日時、5. 払出日付

（2）機構保存本人確認情報ファイル
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、8. 住所　外字数、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. 氏名　清音ふりがな、14. 住所コード市町村コード、15. 住所コード大字・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

（3） 個人番号カード用管理ファイル
1. 送付先管理番号、2. 送付先郵便番号、3. 送付先住所　漢字項目長、4. 送付先住所　漢字、5. 送付先住所　漢字　外字数、6. 送付先氏名　漢字項目長、7. 送付先氏名　漢字、8. 送付先氏名　漢字　外字数、9. 市町村コード、10. 市町村名　項目長、11. 市町村名、12. 市町村郵便番号、13. 市町村住所　項目長、14. 市町村住所、15. 市町村住所　外字数、16. 市町村電話番号、17. 交付場所名　項目長、18. 交付場所名、19. 交付場所名　外字数、20. 交付場所郵便番号、21. 交付場所住所　項目長、22. 交付場所住所、23. 交付場所住所　外字数、24. 交付場所電話番号、25. カード送付場所名　項目長、26. カード送付場所名、27. カード送付場所名　外字数、28. カード送付場所郵便番号、29. カード送付場所住所　項目長、30. カード送付場所住所、31. カード送付場所住所　外字数、32. カード送付場所電話番号、33. 対象となる人数、34. 処理年月日、35. 操作者ID、36. 操作端末ID、37. 印刷区分、38. 住民票コード、39. 氏名　漢字項目長、40. 氏名　漢字、41. 氏名　漢字　外字数、42. 氏名　かな項目長、43. 氏名　かな、44. 郵便番号、45. 住所　項目長、46. 住所、47. 住所外字数、48. 生年月日、49. 性別、50. 個人番号、51. 第30条の45に規定する区分、52. 在留期間の満了の日、53. 代替文字変換結果、54. 代替文字氏名　項目長、55. 代替文字氏名、56. 代替文字住所　項目長、57. 代替文字住所、58. 代替文字氏名位置情報、59. 代替文字住所位置情報、60. 外字フラグ、61. 外字パターン、62. 印刷依頼番号、63. 印刷事業者コード、64. 印刷情報作成年月日、65. 申請書ID、66. 申請書情報連携管理番号、67. 申請書受付事業者コード、68. 処理年月日、69. 顔写真、70. 申請書イメージ、71. 申請年月日、72. 点字有無、73. 点字カナ氏名　項目長、74. 点字カナ氏名、75. 依頼管理番号、76. 操作者ID、77. 操作端末ID、78. カードセキュリティ情報区分、79. 処理結果コード、80. 提供元市町村コード、81. 異動事由、82. 異動年月日、83. 予備領域1、84. 予備領域2、85. カード状況区分、86. 公開鍵長、87. 公開鍵、88. 外字フラグ、89. 外字パターン、90. 発行委託番号、91. 事業者コード、92. カード発行番号、93. コマンド、94. 有効期限、95. 個人番号カード情報、96. カード運用状況、97. カード有効期限、98. 一時停止日、99. 一時停止理由、100. カード廃止日、101. カード廃止理由、102. カード回収日、103. 操作者ID、104. 操作端末ID、105. 操作端末ID、106. タイムスタンプ、107. 所管フラグ、108. 転入処理日、109. 転出予定経過日、110. 本人確認情報有無、111. 前住地市町村コード、112. 住基AP識別情報、113. 暗号識別情報、114. カード製造者識別情報、115. カードイメージ番号、116. 被証明者識別子

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

1. 特定個人情報ファイル名	
(1) 個人番号管理ファイル	
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	個人番号とすべき番号は、個人番号生成システムにおいて住民票コードを元に生成される。 生成元となる住民票コードは、住基全国サーバから入手することとなるが、住基全国サーバ側において個人番号付番対象者の住民票コードのみを抽出することをシステム上で担保する。 また、個人番号の変更は、住民の請求又は市町村長の職権に基づき、市町村長から住基全国サーバを経由して受信した個人番号の変更要求を契機として行われるが、変更要求時に市町村CSから提示される個人番号（変更前）を入手する場合においても、住基全国サーバ側において当該個人番号が最新の住民票コードに対応付くものであることのチェックを行い、個人番号生成システムに適切に提供する（有効性が確認できない個人番号は提供しない）ことをシステム上で担保する。
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	個人番号生成システムにおいて住基全国サーバから入手する情報は、システム上、個人番号とすべき番号の生成元となる住民票コード及び個人番号に限定する。
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	法令に基づいて、住民票コード及び個人番号の入手元を、住基全国サーバに限定する。 このため、個人番号とすべき番号の生成にあたり、住民票コード及び個人番号を住民から直接入手することはない。
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3： 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	新たに住民票に住民票コードを記載した住民の個人番号とすべき番号の生成を求められた場合には対象者の住民票コードを、住民の請求又は市町村長の職権により個人番号を変更する場合には対象者の住民票コードと従前の個人番号を正確に入手することをシステム上で担保する。 なお、機構は、番号法第16条（本人確認の措置）において特定個人情報の提供を受ける際の本人確認の措置を義務付けられる機関には該当しない。
個人番号の真正性確認の措置の内容	新たに住民票に住民票コードを記載した住民の個人番号とすべき番号の生成時を求められた場合には対象者の住民票コードと生成した個人番号とすべき番号を正確に対応付けること、また、住民の請求又は市町村長の職権により個人番号を変更する場合には、従前の個人番号が対象者の個人番号であったことをチェックし、対象者の住民票コード、従前の個人番号及び新たに生成した個人番号とすべき番号とを正確に対応付けることを、システム上で担保する。
特定個人情報の正確性確保の措置の内容	個人番号管理ファイルでは、住民票コードと個人番号とを対応付けて管理するが、住民票コード又は個人番号に変更が生じた場合は、システムにより対応付けを適切に更新する。また、失効した個人番号と同一の番号が生成されないようにシステム上管理する。
その他の措置の内容	―
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク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	特定個人情報を回線を通じて入手する場合は、他のシステムからのアクセスが行えない専用回線を用いることにより、情報漏えい防止措置を講じる。 磁気ディスク等の電子記録媒体により入手する場合には、取り扱いをサーバ室内に限定し、運用要員による厳格な管理を行う。また、受け渡し時は複数人で対応し、受け渡し簿等に受け渡しの記録を残す、外部への持ち出しを禁止する等の漏えい・紛失防止措置を講じる。また、廃棄の際には廃棄履歴を作成し保存する。
リスクへの対策は十分か	[　特に力を入れている　] ＜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	
個人番号とすべき番号の生成に係るリスク対策としては、以下の措置を講じる。 ・重複する個人番号が付番されないよう、システム上、生成された個人番号とすべき番号が生成済みの個人番号と重複しないことをチェックする仕組みを設ける。 ・生成された個人番号とすべき番号から、生成元の住民票コードが推測できない変換方式を用いる。 ・生成された個人番号とすべき番号にチェックディジットを付加し、個人番号の改ざん等を検知可能とする。	

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		機構において、地方公共団体の宛名システムに相当する、本人確認情報を共通参照することが可能なシステムは存在しない。
事務で使用するその他のシステムにおける措置の内容		個人番号生成システムは、機構内において住基全国サーバとのみ接続し、その他のシステムとは接続しない。 また、個人番号生成システムは、個人番号管理ファイル以外に情報を保有せず、また、システム上、個人番号管理ファイル以外の情報へのアクセスは行えない。 ・個人番号生成システム⇒住基全国サーバ ：住基全国サーバへの情報の参照、更新（情報の紐付けを含む）等は行えないよう、システムによりアクセスを制限する。 ・住基全国サーバ⇒個人番号生成システム ：住基全国サーバからのアクセスは、個人番号の生成要求又は変更要求を行う場合、住民票コードの変更を通知する処理に限られる（情報の紐付けは住民票コード及び個人番号に限られる）よう、システムによりアクセスを制限する。
その他の措置の内容		－
リスクへの対策は十分か		[特に力を入れている] ＜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	システムを利用する必要がある職員を特定し、個人ごとにユーザーIDを割り当てるとともに、IDと生体認証（又はパスワード）による認証を行う。 また、なりすましによる不正を防止する観点から、共用IDの利用を禁止する。
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	本人確認情報の管理について定めた規程に基づき、以下の管理を行う。 （1）ID/パスワードの発行管理 ・アクセス権限と事務の対応表を作成する ・アクセス権限が必要となった場合、オペレーション管理者が事務ごとに更新権限の必要があるか、照会権限のみでよいかの別を確認し、事務に必要なアクセス権限のみを申請する。 ・申請に基づき、オペレーション管理責任者が対応表を確認の上、承認（アクセス権限を付与）する。 （2）失効管理 ・定期的又は異動／退職等のイベントが発生したタイミングで、権限を有していた職員の異動／退職情報を確認し、当該事由が生じた際にはアクセス権限を更新し、当該IDを失効させる。
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	アクセス権限の管理は、本人確認情報の管理について定めた規定に基づいて実施する。特権IDについては毎月証跡（ログ）と使用記録の目視確認を行い、また一般利用者IDについては半期毎にユーザ一覧をシステムより出力し、ユーザ管理台帳と目視による突合を行ってアクセス権限の確認及び不正利用の確認を行う。 また、業務上不要となったIDやアクセス権限を変更または削除する。
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	本人確認情報の管理について定めた規定に基づき、特定個人情報のアクセスについて毎月、担当者による証跡（ログ）と申請書による目視確認を実施する。 また、規定を遵守し運用していることを第三者（外部機関）が監査し正当性の確認を行う。
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		・情報セキュリティポリシー等で情報の事務外利用の禁止について規定。 ・プライバシーマーク維持活動の一環として行うeラーニング（年に1回実施を義務付け）や、全職員を受講対象とした個人情報保護及び情報セキュリティに関する研修会（年に1回開催）において、業務外利用の禁止等について徹底する。
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	・媒体への出力情報について毎月システムから証跡（ログ）を出力し、外部媒体使用簿と突合して目視確認を実施する。 ・バックアップ以外にファイルを複製しないよう、職員に対し周知徹底する。 ・特定個人情報ファイルにアクセスする作業は二人で行う相互牽制の体制で実施する。
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	
－	

4. 特定個人情報ファイルの取扱いの委託 [○] 委託しない

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

情報保護管理体制の確認		
特定個人情報ファイルの閲覧者・更新者の制限	[ ]	<選択肢> 1）制限している 2）制限していない
具体的な制限方法		
特定個人情報ファイルの取扱いの記録	[ ]	<選択肢> 1）記録を残している 2）記録を残していない
具体的な方法		
特定個人情報の提供ルール	[ ]	<選択肢> 1）定めている 2）定めていない
委託先から他者への提供に関するルールの内容及びルール遵守の確認方法		
委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法		
特定個人情報の消去ルール	[ ]	<選択肢> 1）定めている 2）定めていない
ルールの内容及びルール遵守の確認方法		
委託契約書中の特定個人情報ファイルの取扱いに関する規定	[ ]	<選択肢> 1）定めている 2）定めていない
規定の内容		
再委託先による特定個人情報ファイルの適切な取扱いの確保	[ ]	<選択肢> 1）特に力を入れて行っている 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		
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		

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	生成した個人番号とすべき番号を市町村長へ通知する際に、個人番号の提供記録（提供日時、操作者、操作端末等）をシステム上で管理し、住基法又は番号法の罰則規定に該当する行為又はその他犯罪行為（詐欺、窃盗等）がなされた際の刑事訴訟手続き上の証拠保全のため、刑事訴訟法第250条第2項第4号（長期15年未満の懲役又は禁錮に当たる罪）の公訴時効である7年分保存する。 また、システム上、提供が認められなかった場合についても記録を残す。
特定個人情報の提供・移転に関するルール	[　定めている　] ＜選択肢＞ 1）定めている　2）定めていない
ルールの内容及びルール遵守の確認方法	番号法第3条第1項（基本理念）及び第8条（個人番号とすべき番号の生成）等の規定に基づき、厳格な運用を行う。 なお、特定個人情報の提供・移転に係るルール（規程類）の詳細については、今後公布される政省令等の内容を踏まえて策定することを予定している。
その他の措置の内容	サーバ室等への入室権限及び個人番号管理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。 ※サーバ室等への入退室管理方法については「7-リスク1-⑤物理的対策」、アクセス権限管理方法については「3-リスク2-アクセス権限の管理」を参照。
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2： 不適切な方法で提供・移転が行われるリスク	
リスクに対する措置の内容	連携手段として通信の記録が逐一保存され、また、連携するデータが暗号化される仕組みが確立した住民基本台帳ネットワークシステムを用いることにより、不適切な方法による特定個人情報の提供の防止に努める。 なお、相手方（市町村CS等）と住基全国サーバの間の通信では相互認証を実施するため、認証できない相手先への情報の移転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	[　特に力を入れている　] ＜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、個人番号とすべき番号の生成要求等の際に提示された住民票コードに対応付く個人番号とすべき番号を誤りなく提供できることをシステムで担保する。 ・誤った相手に提供・移転してしまうリスクへの措置 ：提供先は市町村CSに限定されており、また、市町村CSと住基全国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	[　特に力を入れている　] ＜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　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	[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	・サーバ室と、データ、プログラム等を含んだ記録媒体及び帳票等の可搬媒体を保管する保管室は、他の部屋とは区別して専用の部屋とする。 ・出入口には機械による入退室を管理する設備を設置する。 ・入退室管理を徹底するため出入口の場所を限定する。 ・監視設備として監視カメラ等を設置する。	

⑥技術的対策		[特に力を入れて行っている] <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	・不正プログラム対策 ：コンピュータウイルス監視ソフトを使用し、サーバ・端末双方でウイルスチェックを実施する。また、新種の不正プログラムに対応するために、ウイルスパターンファイルは定期的に更新し、可能な限り最新のものを使用する。 本人確認情報の管理について定めた規程に基づき、コンピュータウイルス等の有害なソフトウェアへの対策を行う場合の手順等を整備する。 また、同規程に基づき、オペレーション管理に係る手順等を整備し、当該手順に従って、情報セキュリティホールに関連する情報（コンピュータウイルス等の有害なソフトウェアに関連する情報を含む）を定期的（コンピュータウィルス関連情報は毎日、その他の情報は少なくとも半年に一度）に入手し、機器の情報セキュリティに関する設定の内容が適切であるかどうかを確認する。 ・不正アクセス対策 ：本人確認情報の管理について定めた規程に基づき、ネットワーク管理に係る手順等を整備し、ファイアウォールによるネットワーク制限並びに監視要員及び侵入検知システム（IDS）によるネットワーク監視を行う。
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	死者の個人番号と生存する個人の個人番号とを分けて管理しないため、「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」において示す、生存する個人の個人番号と同様の管理を行う。
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： 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		個人番号管理ファイルは、個人番号の二重発行を防止する（新規に個人番号を生成する際に、発行済みの個人番号ではないことをシステム上でチェックする）目的で、これまでに生成した全ての個人番号とすべき番号を管理する必要がある。そのため、消去の時期を迎える、情報が古くなるといった性質を持たないため、本設問に係るリスクは存在しない。 なお、個人番号管理ファイルの項目の中に、当該情報が最新のものか履歴情報かを明示的に判別できる区分を設け、適切に管理を行う。
リスクへの対策は十分か		[十分である] <選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている
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	【※未選択の理由】 「リスク2：特定個人情報が古い情報のまま保存され続けるリスク」と同上。
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) 機構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	市町村CSからの本人確認情報更新要求に伴い本人確認情報を更新するため、市町村CSから対象者以外の情報が連携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、市町村における厳格な審査が行われることが前提となる。 このため、年に1度機構が開催する地方公共団体の担当者向け研修会の機会等を活用し、市町村において厳格かつ適切な審査が行われるよう周知を行う。
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	本人確認情報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	特定個人情報の入手元である都道府県知事及び市町村長は、提供先である機構における使用目的が法令に基づくものであること(住基法に基づいて全国的に正確な本人確認情報を管理するために使用すること)を理解した上で特定個人情報を提供する。 なお、法令に基づいて、市町村CSから都道府県サーバを経由してなされた本人確認情報の更新通知により機構保存本人確認情報ファイルを更新するため、住民から直接情報を入手することはない。
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3： 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	市町村側にて届出申請内容や身分証明書等を確認し、厳格な審査を行われることが前提となる。 なお、機構は、番号法第16条(本人確認の措置)において特定個人情報の提供を受ける際の本人確認の措置を義務付けられる機関には該当しない。
個人番号の真正性確認の措置の内容	市町村CSから都道府県サーバを経由して本人確認情報の更新通知を受領した際に、通知された個人番号が最新の住民票コードに対応付くものであることをチェックする仕組みをシステムにより担保する。
特定個人情報の正確性確保の措置の内容	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。
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	・システム内におけるサーバ間通信においては、相互認証を実施した上で、情報を暗号化する。 ・他システムとの連携においては、情報の詐取・奪取等の防止及び情報の正確性担保のため、専用回線である住基ネットを用いる、情報の暗号化を実施する等の措置を行う。
リスクへの対策は十分か	[　特に力を入れている　] ＜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	機構において、地方公共団体の宛名システムに相当する、本人確認情報を共通参照することが可能なシステムは存在しない。
事務で使用するその他のシステムにおける措置の内容	住基全国サーバは、機構内において、個人番号生成システム、個人番号カード管理システム、公的個人認証サービスと接続するが、特定個人情報の連携先は、①個人番号生成システム及び②個人番号カード管理システムに限られるよう、アクセス制御を行う。 なお、個人番号カード管理システムと①、②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）住基全国サーバ⇒他のシステムへのアクセス ①個人番号生成システム ：個人番号の生成要求又は変更要求を行う場合、住民票コードの変更を通知する場合 ②個人番号カード管理システム ：市町村CSより都道府県サーバを経由して受領した住民の異動情報を連携する場合 （2）他のシステム⇒住基全国サーバへのアクセス ①個人番号システム ：情報の参照、更新等は行わない ②個人番号カード管理システム ：情報の参照、更新等は行わない
その他の措置の内容	ー
リスクへの対策は十分か	[　　特に力を入れている　　] ＜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	①機構内の端末について ・システムを利用する必要がある職員を特定し、個人ごとにユーザーIDを割り当てるとともに、IDと生体認証（又はパスワード）による認証を行う。 ・また、なりすましによる不正を防止する観点から、共用IDの利用を禁止する。 ②情報提供先の端末について ・機構が提供するアプリケーションを任意で使用している機関では、ユーザ認証を実施し、情報利用に係る証跡（ログ）を取得するため、不正利用があった場合の操作者の特定を容易にする。 ・機構が提供するアプリケーションを使用せず、機構が提供するAPI（※）を元に独自開発を行い利用する団体に対しては、ユーザー認証を実装するよう要求する。 ※API：プログラムの機能やデータなどを、外部のプログラムから呼び出して利用するための手順やデータ形式などを定めた規約のこと。
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	本人確認情報の管理について定めた規程に基づき、以下の管理を行う。 （1）ID/パスワードの発行管理 ・アクセス権限と事務の対応表を作成する ・アクセス権限が必要となった場合、オペレーション管理者が事務ごとに更新権限の必要があるか、照会権限のみでよいかの別を確認し、事務に必要なアクセス権限のみを申請する。 ・申請に基づき、オペレーション管理責任者が対応表を確認の上、承認（アクセス権限を付与）する。 （2）失効管理 ・定期的又は異動／退職等のイベントが発生したタイミングで、権限を有していた職員の異動／退職情報を確認し、当該事由が生じた際にはアクセス権限を更新し、当該IDを失効させる。
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	アクセス権限の管理は、本人確認情報の管理について定めた規定に基づいて実施する。特権IDについては毎月証跡（ログ）と使用記録の目視確認を行い、また一般利用者IDについては半期毎にユーザー一覧をシステムより出力し、ユーザ管理台帳と目視による突合を行ってアクセス権限の確認及び不正利用の確認を行う。 また、業務上不要となったIDやアクセス権限を変更または削除する。
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	本人確認情報の管理について定めた規定に基づき、特定個人情報のアクセスについて毎月、担当者による証跡（ログ）と申請書による目視確認を実施する。 また、規定を遵守し運用していることを第三者（外部機関）が監査し正当性の確認を行う。
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		・情報セキュリティポリシー等で情報の事務外利用の禁止について規定。 ・プライバシーマーク維持活動の一環として行うeラーニング（年に1回実施を義務付け）や、全職員を受講対象とした個人情報保護及び情報セキュリティに関する研修会（年に1回開催）において、業務外利用の禁止等について徹底する。
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		・媒体への出力情報について毎月システムから証跡（ログ）を出力し、外部媒体使用簿と突合して目視確認を実施する。 ・バックアップ以外にファイルを複製しないよう、職員に対し周知徹底する。 ・特定個人情報ファイルにアクセスする作業は二人で行う相互牽制の体制で実施する。
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		
－		

4. 特定個人情報ファイルの取扱いの委託			[○] 委託しない
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク			
情報保護管理体制の確認			
特定個人情報ファイルの閲覧者・更新者の制限	[ ]	<選択肢> 1）制限している	2）制限していない
具体的な制限方法			
特定個人情報ファイルの取扱いの記録	[ ]	<選択肢> 1）記録を残している	2）記録を残していない
具体的な方法			
特定個人情報の提供ルール	[ ]	<選択肢> 1）定めている	2）定めていない
委託先から他者への提供に関するルールの内容及びルール遵守の確認方法			
委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法			
特定個人情報の消去ルール	[ ]	<選択肢> 1）定めている	2）定めていない
ルールの内容及びルール遵守の確認方法			
委託契約書中の特定個人情報ファイルの取扱いに関する規定	[ ]	<選択肢> 1）定めている	2）定めていない
規定の内容			
再委託先による特定個人情報ファイルの適切な取扱いの確保	[ ]	<選択肢> 1）特に力を入れて行っている 3）十分に行っていない	2）十分に行っている 4）再委託していない
具体的な方法			
その他の措置の内容			
リスクへの対策は十分か	[ ]	<選択肢> 1）特に力を入れている 3）課題が残されている	2）十分である
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置			

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）	[　] 提供・移転しない
リスク1： 不正な提供・移転が行われるリスク	
特定個人情報の提供・移転の記録	[　記録を残している　] <選択肢> 1）記録を残している　2）記録を残していない
具体的な方法	住基法に基づき機構保存本人確認情報の提供が認められている地方公共団体、行政機関等へ特定個人情報（個人番号、4情報等）の提供を行う際に、個人番号の提供記録（提供日時、提供先、提供理由（住基法）、提供対象者、操作者（※））をシステム上で管理し、住基法又は番号法の罰則規定に該当する行為又はその他犯罪行為（詐欺、窃盗等）がなされた際の刑事訴訟手続き上の証拠保全のため、刑事訴訟法第250条第2項第4号（長期15年未満の懲役又は禁錮に当たる罪）の公訴時効である7年分保存する。 なお、システム上、提供が認められなかった場合についても記録を残す。 （※）「操作者」は人手を介するオペレーションを行った場合に記録
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	番号法第3条第1項（基本理念）、第14条第2項（提供の要求）及び第19条第4号（特定個人情報の提供の制限）等の規定に基づき、厳格な運用を行う。 なお、特定個人情報の提供・移転に係るルール（規程類）の詳細については、今後公布される政省令等の内容を踏まえて策定することを予定している。
その他の措置の内容	サーバ室等への入室権限及び機構保存本人確認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、媒体へのデータ出力（書き込み）の際に職員の立会いを必要とする。 また、媒体内の情報には暗号化処理を施し、連携先機関以外で復号できないような仕組みをシステム上で担保する。 ※サーバ室等への入退室管理方法については「7-リスク1-⑤物理的対策」、アクセス権限管理方法については「3-リスク2-アクセス権限の管理」を参照。
リスクへの対策は十分か	[　十分である　] <選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2： 不適切な方法で提供・移転が行われるリスク	
リスクに対する措置の内容	連携手段として通信の記録が逐一保存され、また、連携するデータが暗号化される仕組みが確立した住民基本台帳ネットワークシステムを用いることにより、不適切な方法による特定個人情報の提供を防止する。 なお、相手方と住基全国サーバの間の通信では相互認証を実施するため、認証できない相手先への情報の移転はなされないことがシステム上担保される。 また、外部記録媒体による情報の受け渡し時は複数人の立会いの下で行い、受け渡し簿等に受け渡しの記録を残す。
リスクへの対策は十分か	[　特に力を入れている　] <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 ：情報提供を行う際に、照会元から指定された検索条件に対応する本人の情報を適切に提供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 ：制度上、情報連携の相手方は法令に定められた機関に限定されており、また、相手方（市町村CS等）と住基全国サーバの間の通信では相互認証を実施するため、認証できない相手先への情報の移転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	[　特に力を入れている　] <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 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	法令（番号法）の規定により認められる機関以外からの符号生成要求を受け付けないよう、システムにより制御する。 また、情報提供の記録（提供が認められなかった場合、その記録）を残す。
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	提供の記録が逐一保存される仕組みが整備された情報提供ネットワークシステムを用いて連携することで、不適切な方法で特定個人情報が提供・移転されることを防止する。
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
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	・誤った情報を提供してしまうリスク ：番号法上の情報照会者・情報提供者又は情報提供等記録開示システムからの符号取得要求時に通知された個人番号等に対応する住民票コードを、情報提供ネットワークシステムに対して適切に提供することを、システムにより担保する。 ・誤った相手に提供してしまうリスク ：符号生成を行う情報提供ネットワークシステムにしか提供できないことを、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
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	
機構における情報提供ネットワークシステムを通じた情報連携は、住基法第30条の9の2（総務省への住民票コードの提供）に基づき、符号生成対象者の住民票コードを情報提供ネットワークシステムに提供する事務に限られる。 そのため、情報提供ネットワークシステムを通じた情報の入手は行われない。	

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	・サーバ室と、データ、プログラム等を含んだ記録媒体及び帳票等の可搬媒体を保管する保管室は、他の部屋とは区別して専用の部屋とする。 ・出入口には機械による入退室を管理する設備を設置する。 ・入退室管理を徹底するため出入口の場所を限定する。 ・監視設備として監視カメラ等を設置する。	
⑥技術的対策	[特に力を入れて行っている]	<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	・不正プログラム対策 ：コンピュータウイルス監視ソフトを使用し、サーバ・端末双方でウイルスチェックを実施する。また、新種の不正プログラムに対応するために、ウイルスパターンファイルは定期的に更新し、可能な限り最新のものを使用する。 本人確認情報の管理について定めた規程に基づき、コンピュータウイルス等の有害なソフトウェアへの対策を行う場合の手順等を整備する。 また、同規程に基づき、オペレーション管理に係る手順等を整備し、当該手順に従って、情報セキュリティホールに関連する情報（コンピュータウイルス等の有害なソフトウェアに関連する情報を含む）を定期的（コンピュータウィルス関連情報は毎日、その他の情報は少なくとも半年に一度）に入手し、機器の情報セキュリティに関する設定の内容が適切であるかどうかを確認する。 ・不正アクセス対策 ：本人確認情報の管理について定めた規程に基づき、ネットワーク管理に係る手順等を整備し、ファイアウォールによるネットワーク制限並びに監視要員及び侵入検知システム（IDS）によるネットワーク監視を行う。	
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	死者の個人番号と生存する個人の個人番号とを分けて管理しないため、「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」において示す、生存する個人の個人番号と同様の管理を行う。	
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： 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	4情報や個人番号に変更が生じた場合、市町村長からの本人確認情報更新通知に基づき、機構保存本人確認情報を随時更新している。また、定期的に市町村長が保有する本人確認情報との整合性確認処理を実施することにより、いずれかの市町村の住民基本台帳に記載されている個人について、保存する特定個人情報が最新の情報であることを担保できる。 一方で、更新前の本人確認情報についても、機構保存本人確認情報ファイルにて履歴として管理しているため、消去のタイミングが到来するまで（法令により定められた期間保管している間）は、古い情報を保管することとなる。	
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	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する。 また、磁気ディスク等の電子記録媒体を廃棄する際は廃棄履歴を作成し保存する。 帳票等の紙媒体については、細断又は外部業者による溶解処理を行った後に廃棄する。	
その他の措置の内容	ー	
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		
ー		

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	
(3) 個人番号カード用管理ファイル	
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	本特定個人情報ファイルにおける「特定個人情報の入手」の手段としては、①市町村からの通知カード等の「送付先情報」の受領及び②個人番号カードの交付対象者からの「交付申請書」の受領によるものが挙げられる。 ①送付先情報 ：現存する住民の送付先情報のみを抽出できることを、機構が提供する市町村CSのアプリケーションにより担保する。 ②交付申請書 ：交付申請書は一人につき一通ずつ記載する書面様式として、申請者が申請者本人以外の同居親族等の交付申請を誤って行うことがないようにする。また、本人により記載される必要がある項目(申請に不備等があった際の連絡先、個人番号カードの点字加工の有無、顔写真等)以外の情報(確認のための4情報、個人番号等)はあらかじめ印字することで、成りすまし等による本人以外からの交付申請が行われることを防止する。 なお、国民にとって利便性の高い交付申請方法をとる場合であっても、交付申請手続きの中で本人確認を行う等の措置を講じることにより本人以外からの申請が行われることを防止する。
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	①送付先情報 ：市町村から受領する際のデータ様式を定める。 ②交付申請書 ：本人が必要な情報以外を誤って記載することがないような様式とする。また、記載要領を充実し、必要最小限の情報の記載となるようにする。
その他の措置の内容	住民からの個人番号カード交付申請に基づき個人番号カード用管理情報を作成しているが、カード交付申請が本人の同意なく申請されることも考えられる。この場合、機構側では対象者か否かの判断ができないため、市町村でカード交付時に厳格な審査を行って頂くことが前提となる。
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	・法令に基づき、個人番号カード管理情報の更新を行う。 ・特定の権限者以外は情報照会できず、また情報照会・情報更新の記録が保存される仕組みとする。 ・また、情報の詐取・奪取等の防止及び情報の正確性担保のため、市町村から送付先情報をネットワークを通じて入手する場合は専用回線である住基ネットを用いる。 ・なお、個人番号カードの交付対象者からの「交付申請書」を受領することになるが、本人以外からの交付申請が行われることを防止する上でも必要最低限なものである。
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	①送付先情報は市町村長からシステムを通じて受領し、②交付申請書は郵送により受領するため、特定個人情報の入手の際に、対面での本人確認（窓口で身分証等の提示を受ける等）は行わない。 なお、機構は、番号法第16条（本人確認の措置）において特定個人情報の提供を受ける際の本人確認の措置を義務付けられる機関には該当しない。
個人番号の真正性確認の措置の内容	①送付先情報 ：送付先情報の入手元である市町村CSにおいて、既存住基システムから受領した送付先情報に含まれる個人番号が最新の住民票コードに対応付くものであることをチェックすることにより、個人番号カード管理システムでは個人番号と住民票コードの組み合わせが適切であることを確認された情報のみを受領することを担保する。 ②交付申請書 ：交付申請書の個人番号は、交付対象者の確認用にあらかじめ機構側で記載するものであり、機構側では、返送された交付申請書（記載済）の個人番号をその後の事務に用いないため、個人番号の入手に係るリスクは存在しない。

特定個人情報の正確性確保の措置の内容	①送付先情報 :制度上、4情報等以外の情報(居所等)については、機構において把握する方法が存在しないため、送付先情報の正確性の担保は提供元となる市町村に委ねられる。 ②交付申請書 :交付申請書の送付後に異動等により4情報等に変更が生じた場合、従前の交付申請書は無効とし、異動届出先の市町村窓口において交付申請書を再発行する。
その他の措置の内容	ー
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	・システム内におけるサーバ間通信においては、相互認証を実施した上で、情報を暗号化する。 ・他システムとの連携においては、専用回線を用いる、情報の暗号化を実施する等の措置を行う。
リスクへの対策は十分か	[特に力を入れている] ＜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	
ー	
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	機構において、地方公共団体の宛名システムに相当する、本人確認情報を共通参照することが可能なシステムは存在しない。
事務で使用するその他のシステムにおける措置の内容	個人番号カード管理システムは、機構内(委託先を含む)において、住基全国サーバ、個人番号カード発行システム、コールセンター、公的個人認証サービスと接続するが、特定個人情報の連携先は、①住基全国サーバ、②個人番号カード発行システム、③コールセンターに限られるよう、アクセス制御を行う。 なお、個人番号カード管理システムと①～③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)個人番号カード管理システム⇒他のシステムへのアクセス ①住基全国サーバ :情報の参照、更新等は行わない ②個人番号カード発行システム :個人番号カード発行情報を提供する場合、利用者に依存しない(特定個人情報を含まない)運用情報(鍵情報等)を連携する場合 ③コールセンター :住民からの依頼に基づきコールセンターの操作者が通知カード又は個人番号カード等に係る問合せ対応を行うために必要な情報を提供する場合 (2)他のシステム⇒個人番号カード管理システムへのアクセス ①住基全国サーバ :市町村CSより都道府県サーバを経由して受領した住民の異動情報を連携する場合 ②個人番号カード発行システム :個人番号カードの発行結果を受信する場合 ③コールセンター :通知カード又は個人番号カード等に係る問合せ対応を行う際に必要となる情報を参照する場合
その他の措置の内容	ー
リスクへの対策は十分か	[特に力を入れている] ＜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	システムを利用する必要がある職員を特定し、個人ごとにユーザID(又は生体認証)を割り当てるとともに、ユーザIDの場合には、パスワードによるユーザ認証を実施する。 また、なりすましによる不正を防止する観点から、共用IDの利用を禁止する。

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	本人確認情報の管理について定めた規程に基づき、以下の管理を行う。 （1）ID/パスワードの発行管理 ・アクセス権限と事務の対応表を作成する ・アクセス権限が必要となった場合、オペレーション管理者が事務ごとに更新権限の必要があるか、照会権限のみでよいかの別を確認し、事務に必要なアクセス権限のみを申請する。 ・申請に基づき、オペレーション管理責任者が対応表を確認の上、承認（アクセス権限を付与）する。 （2）失効管理 ・定期的又は異動／退職等のイベントが発生したタイミングで、権限を有していた職員の異動／退職情報を確認し、当該事由が生じた際にはアクセス権限を更新し、当該IDを失効させる。
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	アクセス権限の管理は、本人確認情報の管理について定めた規定に基づいて実施する。特権IDについては毎月証跡（ログ）と使用記録の目視確認を行い、また一般利用者IDについては半期毎にユーザー一覧をシステムより出力し、ユーザ管理台帳と目視による突合を行ってアクセス権限の確認及び不正利用の確認を行う。 また、業務上不要となったIDやアクセス権限を変更または削除する。
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	本人確認情報の管理について定めた規定に基づき、特定個人情報のアクセスについて毎月、担当者による証跡（ログ）と申請書による目視確認を実施する。 また、規定を遵守し運用していることを第三者（外部機関）が監査し正当性の確認を行う。
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		・情報セキュリティポリシー等で情報の事務外利用の禁止について規定。 ・プライバシーマーク維持活動の一環として行うeラーニング（年に1回実施を義務付け）や、全職員を受講対象とした個人情報保護及び情報セキュリティに関する研修会（年に1回開催）において、業務外利用の禁止等について徹底する。
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		・媒体への出力情報について毎月システムから証跡（ログ）を出力し、外部媒体使用簿と突合して目視確認を実施する。 ・バックアップ以外にファイルを複製しないよう、職員に対し周知徹底する。 ・特定個人情報ファイルにアクセスする作業は二人で行う相互牽制の体制で実施する。
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		
－		

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		下記の委託事業者に対し特定個人情報に係る委託を行う際には、ISMS、プライバシーマーク等の認証取得を要求するなど、特定個人情報の保護を適切に行える委託先であることを確認する。 また、委託事業者の社会的信用と能力を確認するとともに、委託する業務の内容、分担範囲の明確化を行い、機構内でその妥当性の承認を行う。 (1)印刷・送付事務、申請受付事務、カード発行事務 (2)コールセンター事務 なお、委託先名の公開については、機構のホームページに掲載する。
特定個人情報ファイルの閲覧者・更新者の制限		[　制限している　] <選択肢> 1) 制限している　2) 制限していない
	具体的な制限方法	委託先においても、電子計算機室及び磁気ディスク等保管室の常時利用する出入口を限定すること等により、侵入を防止する。また、端末機の操作者ごとにフォルダへのアクセス権限を設定し、利用可能なファイルを制限する等の方法を定める。
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	委託先における特定個人情報を取り扱う職員を限定し、取扱い情報を記録する。 必要に応じて機構の職員が直接現場で監督することを想定している。
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	委託先における委託元以外への特定個人情報の提供は認められず、その旨、委託契約書にも明記する。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提供について書面にて報告させる。 必要があれば、当機構職員が現地調査することも可能とする。
	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	・委託元は、委託先において入手する個人番号カードの交付申請書に係る委託契約の報告条項に基づき、四半期に1度、特定個人情報の取扱いについて書面にて報告を受ける。 ・委託元と委託先の間でやり取りされる特定個人情報は、システム上で操作履歴を取得するものとし、住基法又は番号法の罰則規定に該当する行為又はその他犯罪行為（詐欺、窃盗等）がなされた際の刑事訴訟手続き上の証拠保全のため、刑事訴訟法第250条第2項第4号（長期15年未満の懲役又は禁錮に当たる罪）の公訴時効である7年分保存する。 ・必要があれば、機構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。
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	委託契約上、以下の措置をとる旨を規定 ・委託先における特定個人情報の保管期間を、目的に応じて必要最小限の期間に設定 ・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 ・委託契約終了時に専用線は切断し、特定個人情報を全て消去する 委託契約の報告条項に基づき、四半期に1度、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、機構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		[　　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	・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 ・障害発生時等のリカバリーのためのバックアップデータを適切に取得する ・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、機構職員が委託先の視察・監査を行うことができる ・再委託の原則禁止。再委託を行う場合は、事前に申請し、承認を受けることを契約書に明記する。
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	・委託先に対して、本件業務に従事する再委託先従事者の名簿提出を義務付ける。 ・委託先と再委託先が秘密保持に関する契約を締結していることを確認する。 ・再委託事業者に、本件業務に従事する者に対して、必要な法規・遵守事項の教育を実施させ、委託先に報告させる。 ・必要があれば、機構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。
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		
通知カード及び交付申請書の誤送付・誤配達等のリスクが低減されるような送付方法を検討する。		
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	市町村長へ特定個人情報（個人番号カード管理情報）の提供を行う際に、個人番号の提供記録（提供日時、提供者情報、操作者等）をシステム上で管理し、住基法又は番号法の罰則規定に該当する行為又はその他犯罪行為（詐欺、窃盗等）がなされた際の刑事訴訟手続き上の証拠保全のため、刑事訴訟法第250条第2項第4号（長期15年未満の懲役又は禁錮に当たる罪）の公訴時効である7年分保存する。 また、システム上、提供が認められなかった場合についても記録を残す。
特定個人情報の提供・移転に関するルール		[　　定めている　　] ＜選択肢＞ 1）定めている　2）定めていない
	ルールの内容及びルール遵守の確認方法	番号法第3条（基本理念）第3項及び第18条（個人番号カードの利用）等の規定に基づき、厳格な運用を行う。 なお、特定個人情報の提供・移転に係るルール（規程類）の詳細については、今後公布される政省令等の内容を踏まえて策定することを予定している。
その他の措置の内容		サーバ室等への入室権限及び個人番号カード用管理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、媒体へのデータ出力（書き込み）の際に職員の立会いを必要とする。 また、媒体内の情報には暗号化処理を施し、連携先機関以外で復号できないような仕組みをシステム上で担保する。 ※サーバ室等への入退室管理方法については「7-リスク1-⑤物理的対策」、アクセス権限管理方法については「3-リスク2-アクセス権限の管理」を参照。
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機能を有する専用線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、相手方と個人番号カード管理システムの間の通信では相互認証を実施するため、認証できない相手先への情報の移転はなされないことがシステム上担保される。 また、外部記録媒体による情報の受け渡し時は複数人の立会いの下で行い、受け渡し簿等に受け渡しの記録を残す。
リスクへの対策は十分か	[　　特に力を入れている　　] ＜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 ：住民基本台帳ネットワークシステムでは個人番号カード用管理ファイルで保有する情報すべてを連携することはできない（送付先情報（個人番号、4情報等を含む）に限られる）。 また、情報提供先における事務で必要となる情報のみを提供する（必要以上の情報は提供しない）ことを、システム上担保する。 ・誤った相手に提供・移転してしまうリスクへの措置 ：相手方（市町村CS等）と個人番号カード管理システムの間の通信では相互認証を実施するため、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	[　　特に力を入れている　　] ＜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　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	[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	・サーバ室と、データ、プログラム等を含んだ記録媒体及び帳票等の可搬媒体を保管する保管室は、他の部屋とは区別して専用の部屋とする。 ・出入口には機械による入退室を管理する設備を設置する。 ・入退室管理を徹底するため出入口の場所を限定する。 ・監視設備として監視カメラ等を設置する。	

⑥技術的対策		[　特に力を入れて行っている　] <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	・不正プログラム対策 :コンピュータウイルス監視ソフトを使用し、サーバ・端末双方でウイルスチェックを実施する。また、新種の不正プログラムに対応するために、ウイルスパターンファイルは定期的に更新し、可能な限り最新のものを使用する。 本人確認情報の管理について定めた規程に基づき、コンピュータウイルス等の有害なソフトウェアへの対策を行う場合の手順等を整備する。 また、同規程に基づき、オペレーション管理に係る手順等を整備し、当該手順に従って、情報セキュリティホールに関連する情報（コンピュータウイルス等の有害なソフトウェアに関連する情報を含む）を定期的（コンピュータウィルス関連情報は毎日、その他の情報は少なくとも半年に一度）に入手し、機器の情報セキュリティに関する設定の内容が適切であるかどうかを確認する。 ・不正アクセス対策 :本人確認情報の管理について定めた規程に基づき、ネットワーク管理に係る手順等を整備し、ファイアウォールによるネットワーク制限並びに監視要員及び侵入検知システム（IDS）によるネットワーク監視を行う。
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	死者の個人番号については、一定期間保管した後、個人番号カード用管理ファイルから消去する。 当該情報を保有している間においては、「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」において示す、生存する個人の個人番号と同様の管理を行う。
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：　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		個人番号カード交付済みの住民の異動等が発生した場合、市町村CSより都道府県サーバ、住基全国サーバを経由して、当該住民の異動情報が個人番号カード管理システムに連携される。 個人番号カード管理システムでは、受領した異動情報を元に個人番号カード用管理ファイルを更新することにより、保有する情報を最新の状態で管理する。
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	・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する。また、消去の際は消去履歴を作成し保存する。 ・保管期間の過ぎたバックアップファイルを消去する。消去の際は消去履歴を作成し保存する。 ・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について外部業者による溶解処理を行う。 ・媒体の別（電子記録媒体、紙媒体）を問わず、廃棄の際は廃棄履歴を作成し保存する。
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
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	住基全国センターの規程類に規定されている事項から自己点検項目のチェックリストを作成し、当該チェックリストを用いて、定期的（年１回）に職員による自己点検項目の遵守状況の確認を実施している。
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	本人確認情報の管理方法等について定めた規程に基づき、毎年度、第三者機関による外部監査を実施している。 また、内部監査の一環として、外部監査の際に指摘された事項の改善状況を確認し、PDCAサイクルによる課題又は問題点の把握、改善に努めている。
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	新規配属時に実施されるオリエンテーション及び規程改正時の集合研修において本人確認情報の管理方法等について定めた規程の概要について説明、周知徹底している。 また、毎年実施する地方公共団体向けのセキュリティ研修会において、当機構の職員が持ち回りで講師として登壇することにより、各職員のセキュリティ意識の醸成及び自己研鑽に繋がっている。
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	郵便番号102-8419 東京都千代田区一番町25番地　全国町村議員会館6階 地方公共団体情報システム機構　本人確認情報開示請求受付窓口 （https://www.j-lis.go.jp/juki-net/kaiji/kaiji_seikyu/cms_1453662.html） ※郵送の場合の宛先についても同上
②請求方法	指定様式（下記URLを参照）による書面の提出により開示・訂正・利用停止請求を受け付ける。 （https://www.j-lis.go.jp/data/open/cnt/3/237/1/kaiji_20140401.pdf https://www.j-lis.go.jp/data/open/cnt/3/235/1/teisei_20140401.pdf） また、請求方法について、上記「①請求先」で示すURLのページにおいて要領を記載し、わかりやすい説明に努めている。
特記事項	機構ホームページ上に、請求先、請求方法、諸費用等について掲載する。
③手数料等	［　　有料　　］　＜選択肢＞ 1）有料　　2）無料 （手数料額、納付方法：手数料額：情報開示手数料として、20円／本人確認情報確認書1通 納付方法：来所の場合は現金、郵送の場合は郵便切手　　）
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	「1．①請求先」と同上
②対応方法	・問い合わせの受付時に受付票を起票し、対応について記録を残す。 ・情報漏えい等の重大な事案に関する問い合わせについて、関係先等に事実確認を行うための標準的な処理期間を設ける。

Ⅵ　評価実施手続

1. 基礎項目評価	
①実施日	平成26年7月30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	機構ホームページにおいて意見募集公告を掲載。 ダウンロード資料として「特定個人情報保護評価書（全項目評価書）（案）」及び「意見提出様式」を併せて掲載し、意見提出様式に記載された意見を電子メールにより受け付けた。
②実施日・期間	平成26年6月10日から平成26年7月10日まで
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	・「独自のアプリケーション」が厳格な不正アクセス対策として有効であることは、どのように担保されるのか。 ・個人番号カード発行に係る国民への負荷は、できる限り軽減すべきである。 ・コールセンターについては、国民が混乱しないよう、機能の違いを明確にし、マイナンバー制度が利便性の高い社会基盤であることを、国民が早い時期に実感し、利用してもらうための十分な事前周知が必要ではないか。 ・番号制度は、民間利用も前提とされていることから、弊害となる外字を当該システムのファイルに記録するべきではない。 ・従業者が事務外で使用するリスクに対する措置の内容として、年1回の研修会等では「十分である」とはリスク的に妥当とは言えず、「特に力をいれている」位な意識が欲しい。 ・アクセス権限の確認期間の妥当性及び確認手法がわかりにくい。 ・不正アクセスのリスクが高い場合は内部担当者による監視やログレビュー等のインシデントをいち早く発見する取組みが求められると考える。　等
⑤評価書への反映	寄せられた意見への回答として、全ての意見について機構としての考え方を一覧形式で取りまとめ、機構ホームページにて公表した。 当該一覧において、「意見内容を評価書へ追記・反映する」旨の回答をしたものについては、意見内容を踏まえて本評価書に追記・反映を行った。
3. 第三者点検	
①実施日	ー
②方法	ー
③結果	ー
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	

（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