

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、5情報（氏名、氏名の振り仮名、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、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に規定する個人番号、個人番号カード、特定個人情報の提供等に関する命令（平成26年11月20日総務省令第85号。以下「個人番号カード省令」という。）に基づき、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。

・外部との接続に当たっては、専用回線の利用、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

個人情報保護委員会 承認日【行政機関等のみ】

令和7年1月29日

公表日

令和8年6月22日

項目一覧

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

I 基本情報

1. 特定個人情報ファイルを取り扱う事務

①事務の名称	住民基本台帳ネットワーク及び番号制度関連事務
	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」、「4. 附票本人確認情報の提供及び保存等に係る事務」及び「5. カード代替電磁的記録に係る事務」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）事務の内容」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（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 ・住民基本台帳法（昭和42年7月25日法律第81号）（以下「住基法」という。）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）事務の内容」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、5情報（氏名、氏名の振り仮名、住所、性別、生年月日）、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、5情報又はその他機構保存本人確認情報ファイル記録項目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。 ※国外転出者に係る事務処理に関し、番号法で認められた場合に限り、国の機関等からの求めに応じ、当該個人の住民票コードを用いて、機構保存本人確認情報ファイルから個人番号を抽出し、附票全国サーバに連携する場合がある。

(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。

※本人確認情報の利用（個人番号カード管理システムへの本人確認情報の提供）

個人番号カードの交付申請後に機構保存本人確認情報をもってカードの発行に用いられる送付先情報が最新かどうかを比較・突合し、古い住所や氏名でカードが発行され住民へ交付されるリスクを低減させる。

交付後のタイミングにおいても、申請から交付までの間の異動情報を個人番号カードの一時停止時の本人性確認に用いられる利用者情報に反映させることにより、交付後直ちに異動後の最新の住所等で一時停止業務を行えるようにするため、個人番号カード管理システムから照会要求を受け（個人番号カード管理システム→住基全国サーバ）、住民票コード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（住基全国サーバ→個人番号カード管理システム）。

②事務の内容 ※

3. 個人番号カードに係る事務（※詳細は、「（別添1）事務の内容」を参照）

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、個人番号カード省令第23条から第23条の3まで及び第35条第1項に基づき、個人番号通知書及び個人番号カードに係る以下の事務を行う。また、番号法第18条の5第2項により、機構は、特定在留カード等について、個人番号の記載及びその電磁的方法による記録その他個人番号カードとしての機能を付加するための措置を講ずることとされている。

(1)個人番号通知書の印刷・住民への送付

・住民に対して個人番号通知書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、個人番号通知書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。

(2)個人番号カードの交付申請受付・発行・市町村又は住民への送付

・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元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。

(3)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、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（あわせて、公的個人認証サービスに対し、電子証明書の一時的保留要求を行う。）を行う業務を委託する。
・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。

4. 附票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）事務の内容」を参照）

機構は、市町村における市町村CS、都道府県における附票都道府県サーバ及び機構における附票全国サーバ等により構成される「附票連携システム」において、国外転出者に係る本人確認を行うための社会的基盤としての役割を担うため、5情報（氏名、氏名の振り仮名、住所、性別、生年月日）、住民票コード及びこれらの変更情報で構成される「機構保存附票本人確認情報ファイル」を作成し、戸籍の附票に関する記録を正確に行う責務がある。そのため、附票本人確認情報の提供及び保存等に係る以下の事務を実施する。なお、機構保存附票本人確認情報（以下「附票本人確認情報」という場合もある。）には、個人番号は含まれない。

(1)附票本人確認情報の更新

・機構保存附票本人確認情報ファイルを最新の状態に保つため、都道府県知事から通知された附票本人確認情報の更新情報を元に当該ファイルを更新する。

(2)市町村長等への附票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、国外転出者に係る事務処理に関し、照会のあった当該個人の5情報等に対応付く附票本人確認情報を機構保存附票本人確認情報ファイルから抽出し、照会元に提供する。その際、番号法で認められた場合に限り、附票本人確認情報の提供に併せて、当該個人の住民票コードを用いて機構保存本人確認情報ファイルから個人番号を抽出し、照会元に提供する場合がある。

(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・情報提供者から要求を受け、情報提供ネットワークシステムに住基全国サーバを経由して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に住基全国サーバを経由して情報提供ネットワークシステムに通知する。

(4)附票本人確認情報開示

・法律に基づく本人による自己の附票本人確認情報の開示請求に対応するため、当該個人の附票本人確認情報を機構保存附票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)附票本人確認情報整合 ・機構保存附票本人確認情報ファイルの正確性を担保するため、市町村長から附票本人確認情報を受領し、当該附票本人確認情報を用いて機構保存附票本人確認情報ファイルに記録された附票本人確認情報の整合性確認を行う。また、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と機構保存附票本人確認情報ファイルに記録された附票本人確認情報の整合性確認を行う。 ※附票本人確認情報の利用（個人番号カード管理システムへの附票本人確認情報の提供） 個人番号カードの交付申請後に機構保存附票本人確認情報をもってカードの発行に用いられる送付先情報が最新かどうかを比較・突合し、古い住所や氏名でカードが発行され住民へ交付されるリスクを低減させる。 交付後のタイミングにおいても、申請から交付までの間の異動情報を個人番号カードの一時停止時の本人性確認に用いられる利用者情報に反映させることにより、交付後直ちに異動後の最新の住所等で一時停止業務を行えるようにするため、個人番号カード管理システムから照会要求を受け（個人番号カード管理システム→附票全国サーバ）、住民票コードを元に機構保存附票本人確認情報ファイルを検索し、該当する個人の附票本人確認情報を照会元へ提供する（附票全国サーバ→個人番号カード管理システム）。 5. カード代替電磁的記録に係る事務（※詳細は、「（別添1）事務の内容」を参照） ・個人番号カードの交付を受けている者は、自己に係るカード代替電磁的記録をその者が使用する移動端末設備（スマートフォン）に記録して利用するため、その者の申請により当該カード代替電磁的記録の発行を受けることができることとされている（番号第18条の2第1項）。 ・番号法第18条の2に定めるカード代替電磁的記録に係る発行等の手続、有効期間に係る失効通知等について、デジタル庁が運用するmdoc発行管理システムの各機能を用いて、以下の事務を実施する。 (1)カード代替電磁的記録の発行 ・申請者から個人番号カードに記録された5情報（氏名、氏名の振り仮名、住所、性別、生年月日）、個人番号及び本人の写真に係る電磁的記録の送信を受け、カード代替電磁的記録を発行し、申請者のスマートフォンに送信する。 (2)カード代替電磁的記録の失効 ・番号法第18条の2第9項に定める事由が発生したとき、mdoc発行管理システム上で、上記(1)で発行したカード代替電磁的記録を失効させ、当該申請者に係るカード代替電磁的記録が格納されたスマートフォンに対し、カード代替電磁的記録の失効通知を送信する。 (3)カード代替電磁的記録の更新 ・カード代替電磁的記録の有効期間が満了する場合は、新たなカード代替電磁的記録を自動発行し、カード代替電磁的記録が格納されたスマートフォンに送信する。 ※カード代替電磁的記録の有効期間中に、個人番号カードの有効期間が満了する場合は、当該満了の日がカード代替電磁的記録の有効期間となり、自動発行されない。 (4)カード代替電磁的記録の一時利用停止 ・利用者から上記(1)で発行したカード代替電磁的記録が格納されたスマートフォンの紛失・盗難等に基づく一時停止の連絡を受け付けた場合、もしくは利用者からスマートフォンの紛失申請（オンライン申請）を受けた場合、当該利用者のカード代替電磁的記録に一時利用停止処理を行う。		
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な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5情報等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。 ※国外転出者に係る事務処理に関し、番号法で認められた場合に限り、国の機関等からの求めに応じ、当該個人の住民票コードを用いて、機構保存本人確認情報ファイルから個人番号を抽出し、附票全国サーバに連携する場合がある。 ・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。 ・個人番号カード管理システムから利用者情報の照会要求を受け、該当する個人の本人確認情報を照会元へ提供する。 ※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。
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、附票連携システム)
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) ・個人番号通知書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、個人番号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。

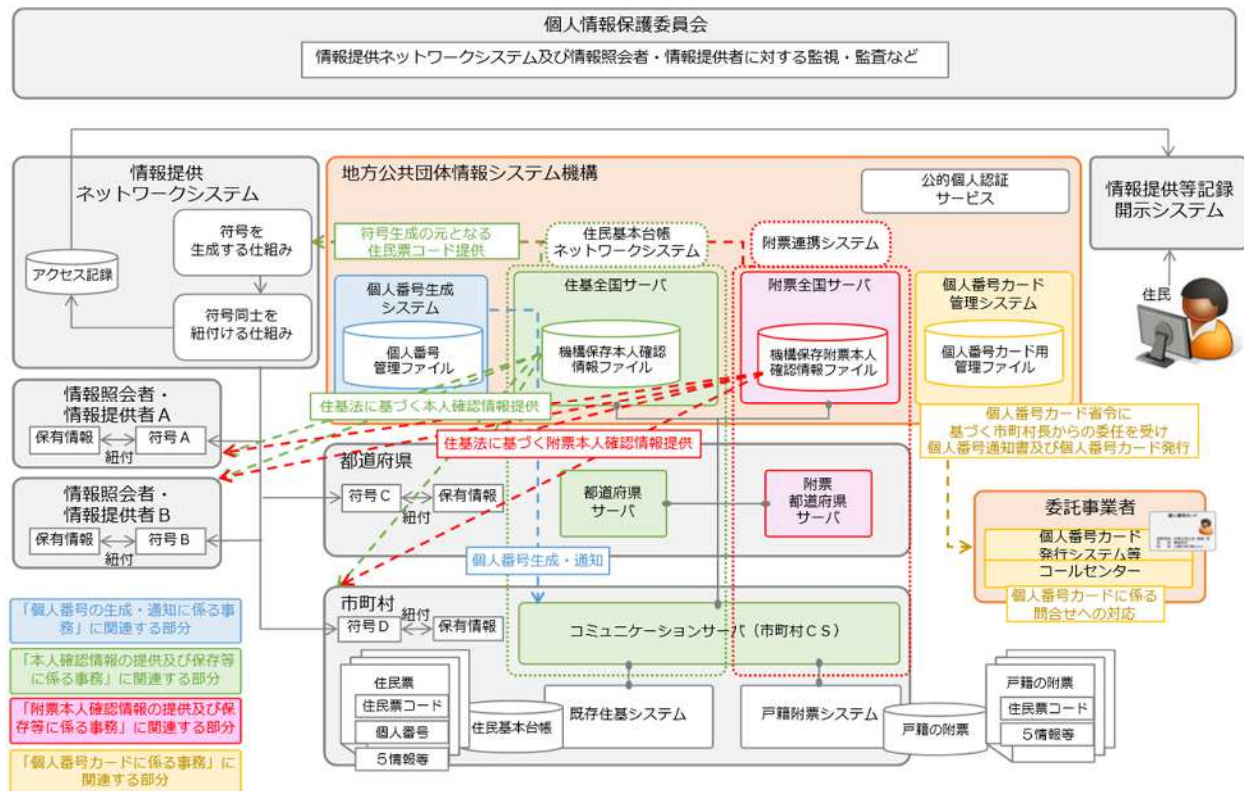
③他のシステムとの接続	☐ 情報提供ネットワークシステム ☐ 庁内連携システム ☐ 住民基本台帳ネットワークシステム ☐ 既存住民基本台帳システム ☐ 宛名システム等 ☐ 税務システム ☐ その他 (委託事業者における個人番号カード発行システム、 公的個人認証サービス、附票連携システム)
システム4	
①システムの名称	附票連携システム ※機構保存附票本人確認情報ファイルは、附票連携システムの構成要素のうち、「附票全国サーバ」において管理がなされているため、以降、附票全国サーバについて記載する。
②システムの機能	(「4. 附票本人確認情報の提供及び保存等に係る事務」に対応) ・附票都道府県サーバから附票本人確認情報の更新データを受信し、機構保存附票本人確認情報ファイルを更新し、通知元附票都道府県サーバに附票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国外転出者に係る附票本人確認情報照会要求を受け取り、住民票コード又は5情報の組合せにより機構保存附票本人確認情報ファイルを検索する。附票本人確認情報照会要求により検索した、附票本人確認情報を市町村長等へ提供する。その際、番号法で認められた場合に限り、国の機関等からの求めに応じ、附票本人確認情報の提供に併せて当該個人の住民票コードを用いて、機構保存本人確認情報ファイルから個人番号を抽出し、照会元に提供する場合がある。 ・番号法上の情報照会者・情報提供者からの国外転出者に係る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等で最新の本人確認情報及び附票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附票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。 ・個人番号カード管理システムから利用者情報の照会要求を受け、該当する個人の附票本人確認情報を照会元へ提供する。
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 (個人番号カード管理システム)
システム5	
①システムの名称	mdoc発行管理システム
②システムの機能	(「5. カード代替電磁的記録に係る事務」に対応) ・申請者のスマートフォンからカード代替記録事項に係る電磁的記録を受信し、当該申請に係るカード代替電磁的記録を発行し、これを当該申請者のスマートフォンに送信する。 ・番号法上で定められた要件に従って、カード代替電磁的記録の再発行・失効を行う。 ・カード代替電磁的記録が格納されたスマートフォンの盗難・紛失時に、個人番号カード向けコールセンターから公的個人認証サービスシステムを介して、もしくはスマートフォンの紛失申請(オンライン申請)を行い、カード代替電磁的記録を一時的に利用停止する。 なお、カード代替電磁的記録には氏名(氏名の振り仮名含む)・住所・性別・生年月日・個人番号・本人の写真の情報が含まれる。
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 (公的個人認証サービスシステム、スマートフォン用公的個人認証機能管理システム、情報提供等開示システム、ぴったりサービス、ウォレット事業者サーバー)

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) 機構保存附票本人確認情報ファイル (5) カード代替電磁的記録用ファイル	
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5ファイルを下記に記載のと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、新しい個人番号とすべき番号、従前の個人番号及び住民票コードとの紐付けを管理する。 ③住民票コードが変更される際に個人番号と住民票コードとの紐付けを管理する。 (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。 ⑤個人番号カードの交付申請時に個人番号カード管理システムが保持する送付先情報と住基全国サーバが保持する本人確認情報が一致しているかを確認し、また個人番号カードの一時停止業務を最新の情報に基づき実施するため、個人番号カード管理システムから利用者情報の照会要求を受け、該当する個人の本人確認情報を提供する。 (3) 個人番号カード用管理ファイル ①住民に対し、個人番号通知書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。 (4) 機構保存附票本人確認情報ファイル ※機構保存附票本人確認情報には個人番号は含まれない。 ①国外転出者に係る本人確認を行うための社会的基盤として記録を正確に行う。 ②市町村長、都道府県知事、国の機関等に対し国外転出者に係る附票本人確認情報を提供する。その際、番号法で認められた場合に限り、国の機関等からの求めに応じ、附票本人確認情報の提供に併せて当該個人の住民票コードを用いて、機構保存本人確認情報ファイルから個人番号を抽出し、照会元に提供する場合がある。 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本人からの請求に基づき、当該個人の附票本人確認情報を開示する。 ⑤個人番号カードの交付申請時に個人番号カード管理システムが保持する送付先情報と附票全国サーバが保持する附票本人確認情報が一致しているかを確認し、また個人番号カードの一時停止業務を最新の情報に基づき実施するため、個人番号カード管理システムから利用者情報の照会要求を受け、該当する個人の附票本人確認情報を提供する。 (5) カード代替電磁的記録用ファイル ①カード代替電磁的記録を発行し、利用者のスマートフォンに送信する。 ②カード代替電磁的記録の発行状況を管理する。
②実現が期待されるメリット	住民票の写し等に代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。また、国外転出者を含め個人番号カードによる本人確認、個人番号の真正性確認が可能となり、行政事務の効率化に資することが期待される。

5. 個人番号の利用 ※		
法令上の根拠	1. 番号法 ・第8条(個人番号とすべき番号の生成) ・第16条の2(個人番号カードの発行等) ・第17条第1項、第3項、第6項(個人番号カードの交付等) ・第18条の2(カード代替電磁的記録の発行等) 2. 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) ・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(デジタル庁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15の2第1項(準法定事務処理者への本人確認情報の提供等) ・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) ・第30条の44の6第6項(附票本人確認情報(住民票コードに限る。)の利用) ・第30条の44の7第1項(準法定事務処理者への附票本人確認情報の提供等)	
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(デジタル庁への住民票コードの提供) 住基法第30条の44の2(デジタル庁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	(1)住民基本台帳ネットワークシステム全国センター (2)住民基本台帳ネットワークシステム全国センター (3)個人番号センター、コンタクトセンター (4)住民基本台帳ネットワークシステム全国センター (5)個人番号センター、コンタクトセンター	
②所属長の役職名	(1)センター長 (2)センター長 (3)センター長 (4)センター長 (5)センター長	
8. 他の評価実施機関		
—		

(別添1) 事務の内容

(前提) 番号制度全体における機構の役割 (概要)



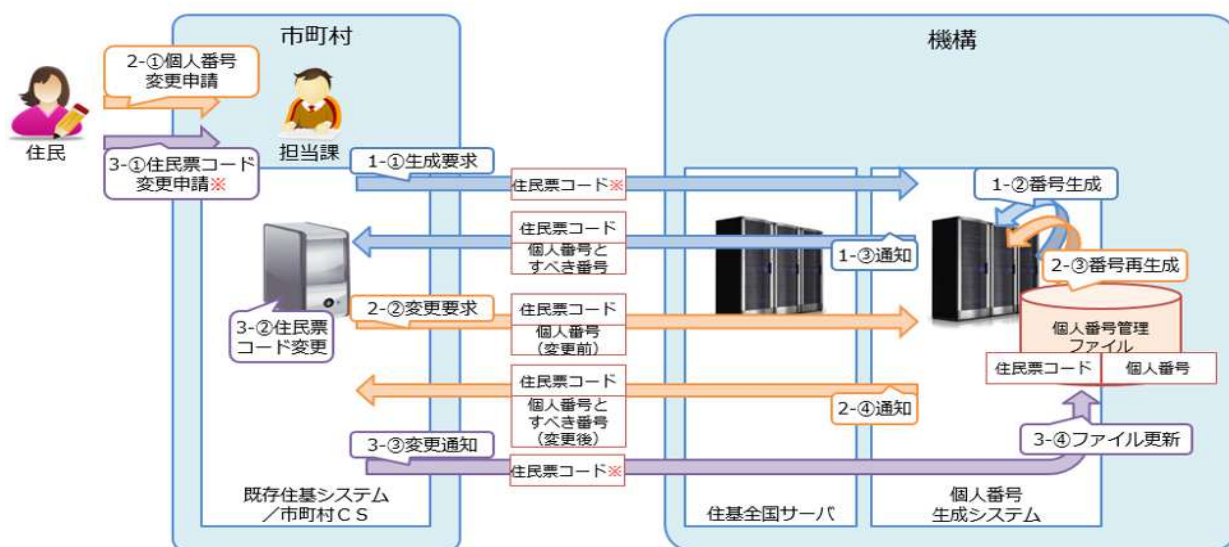
(備考)

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。

(注) カード代替電磁的記録に係る事務については、(5) カード代替電磁的記録に係る事務を参照。

(別添1) 事務の内容

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



(注) 図中に※が付されている箇所は、特定個人情報を含まない事務の流れを指す。

(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（※特定個人情報を含まない）。

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（※特定個人情報を含まない）。

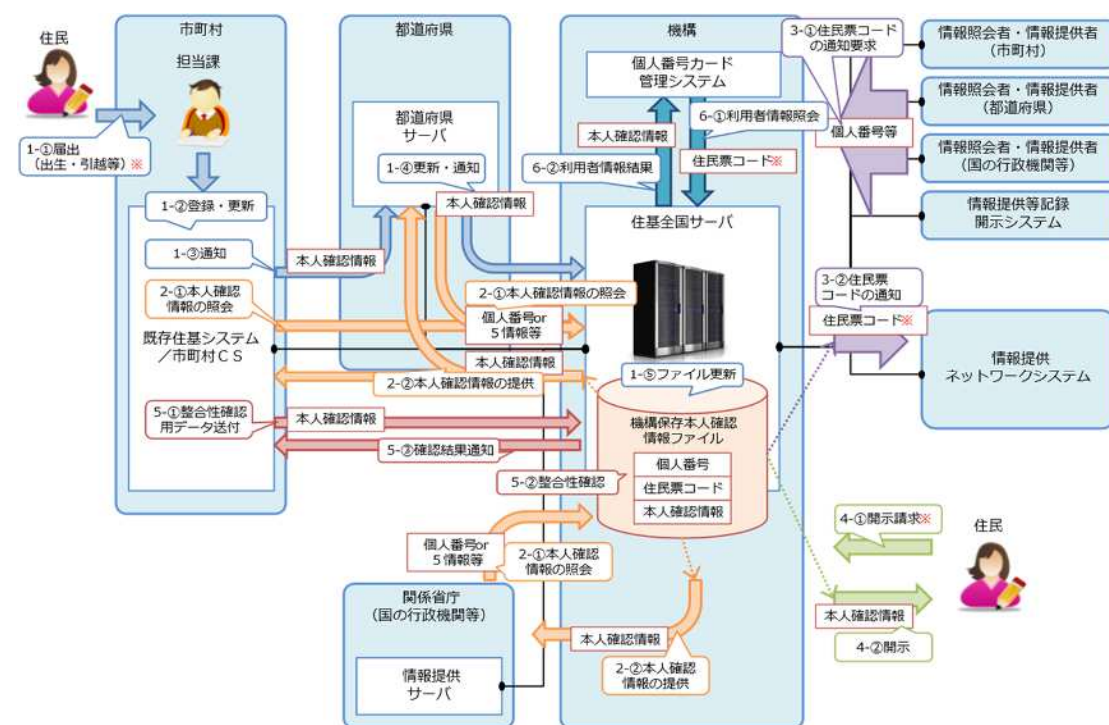
3-② 市町村長の既存住基システムにおいて、住民票コードを更新する。

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（※特定個人情報を含まない）

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に係る事務(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)



(注) 図中に※が付されている箇所は、特定個人情報を含まない事務の流れを指す。

(備考)

(2)-1. 本人確認情報の更新

- 1-① 市町村長において、住民より、住民異動に関する届出を受け付ける(※特定個人情報を含まない)。
 1-② 市町村長において、異動情報を既存住基システムに登録する(更新を含む)。
 1-③ 市町村長において、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信したデータを元に、「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5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。

※国外転出者に係る事務処理に関し、番号法で認められた場合に限り、国の機関等からの求めに応じ、当該個人の住民票コードを用いて、「機構保存本人確認情報ファイル」から個人番号を抽出し、附票全国サーバに連携する場合がある(別添1(4)参照)。

(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(※特定個人情報を含まない)。

(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(※特定個人情報を含まない)。

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。

※本人確認情報整合事務について、正確性確保のため、補完的に以下の事務を行う。

令和元年8月(予定)以降、試行運用を実施し、試行運用の結果を受けて、本番運用へ移行する。

① 機構において、市町村毎に当該市町村の転出漏れ等、不整合の可能性のある住民の情報を

「機構保存本人確認情報ファイル」から抽出する(特定個人情報を含まない)。

② 機構において抽出した結果を確認し、必要なデータのみ抜粋し、市町村に送付する(特定個人情報を含まない)。

③ ②のデータに基づき、市町村において当該データについて修正の必要があるか調査を実施し、必要な場合は修正する(修正する際の流れは(2)-1. 本人確認情報の更新の1-②～1-⑤の流れと同様)。

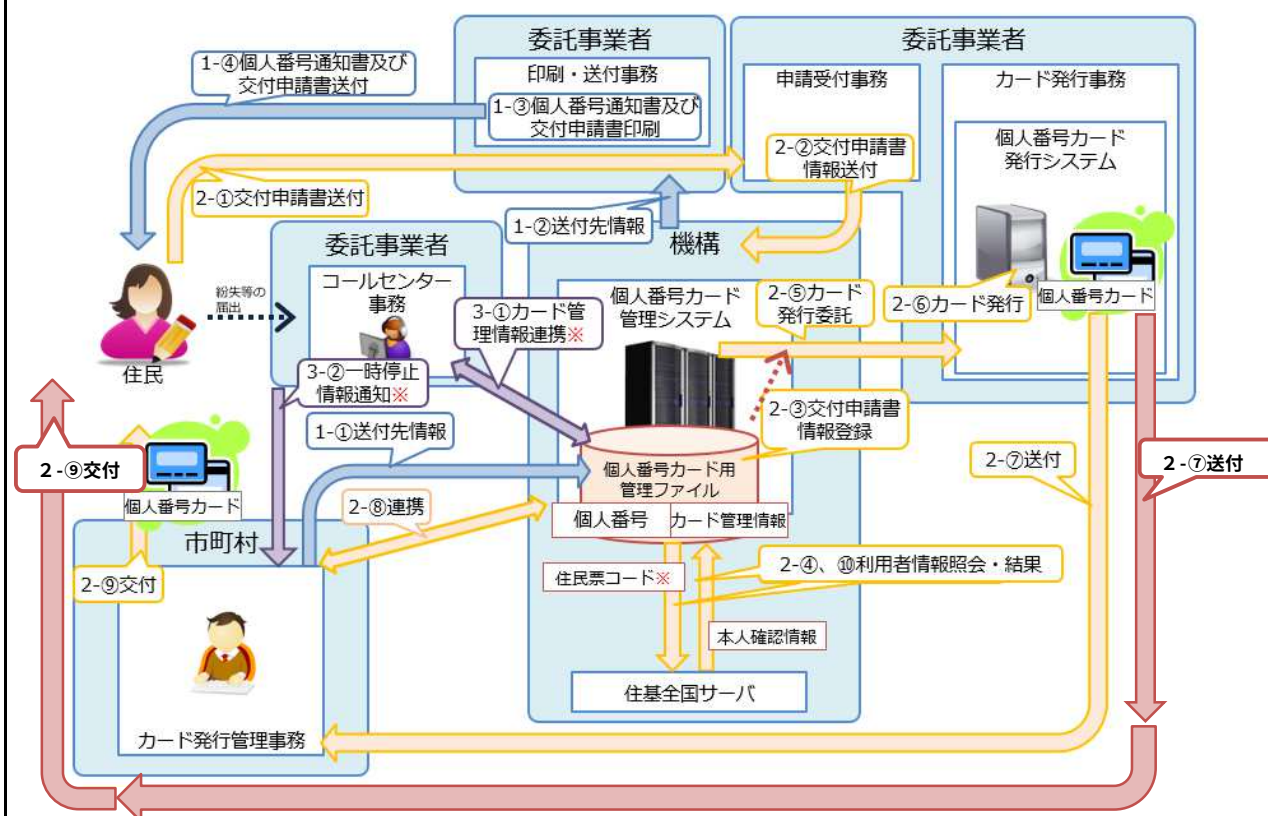
(2)-6. 本人確認情報の利用

6-① 個人番号カードの交付申請後及び交付後に個人番号カード管理システムより、住民票コードをキーとした利用者情報の照会を受ける(※特定個人情報を含まない)。

6-② 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、個人番号カード管理システムへ提供する。

(別添1) 事務の内容

(3) 個人番号カードに係る事務(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)



(注) 図中に※が付されている箇所は、特定個人情報を含まない事務の流れを指す。

(備考)

(3)-1.個人番号通知書の印刷・住民への送付

- 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、個人番号通知書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、個人番号通知書及び交付申請書を送付する。

(3)-2.個人番号カードの交付申請受付・発行・市町村への送付

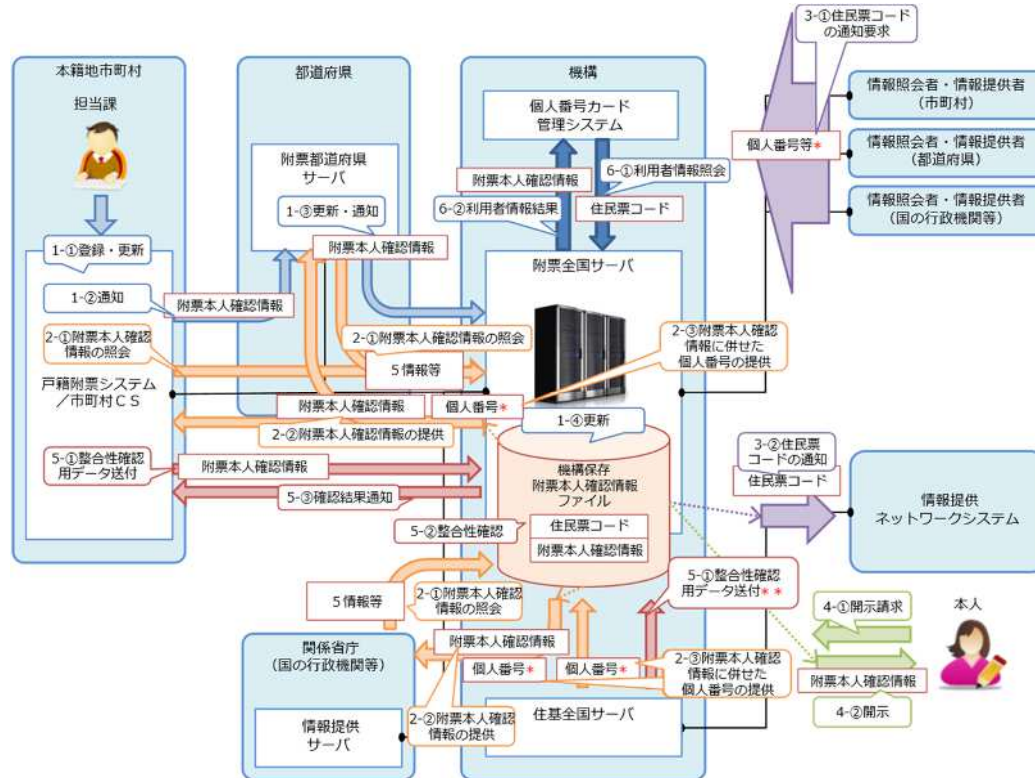
- 2-① 委託事業者(申請受付事務)において、住民より、個人番号カードの交付申請書(記入済)を受領する。
 - 2-② 委託事業者(申請受付事務)より、個人番号カードの交付申請書情報を受領する。
 - 2-③ 受領した交付申請書情報を、「個人番号カード用管理ファイル」に登録する。
 - 2-④ 個人番号カードの交付申請後に住基全国サーバへ住民票コードをキーとした利用者情報の照会を行い(※特定個人情報を含まない)、住基全国サーバより該当する個人の本人確認情報の提供を受ける。
 - 2-⑤ 委託事業者(カード発行事務)に対し、「個人番号カード用管理ファイル」を元に、個人番号カード発行を委託する。
 - 2-⑥ 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。
 - 2-⑦ 発行された個人番号カードを、送付先住所地の市町村長又は住民に対し送付する。
 - 2-⑧ 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。
 - 2-⑨ 市町村長又は機構において、個人番号カードを住民に交付する。
 - 2-⑩ 個人番号カードの交付後に住基全国サーバへ住民票コードをキーとした利用者情報の照会を行い(※特定個人情報を含まない)、住基全国サーバより該当する個人の本人確認情報の提供を受ける。
- ※手書用交付申請書以外の交付申請書には個人番号は記載しない。

(3)-3.カード管理情報の連携

- 3-① 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。
- 3-② 委託事業者(コールセンター事務)は一時停止した旨の情報を市町村長に通知する(※特定個人情報を含まない)。

(別添1) 事務の内容

(4) 附票本人確認情報の提供及び保存に係る事務(該当する特定個人情報ファイル:機構保存附票本人確認情報ファイル)



(注) 図中に*が付されている箇所は、特定個人情報を含む事務の流れを指す。

図中に**が付されている箇所は、特定個人情報(個人番号と紐付けてアクセスできる情報)を

含む事務の流れを指す(個人番号は含まない)。

(備考)

(4)-1.附票本人確認情報の更新

- 1-① 本籍地市町村長において、戸籍の届出、他市町村からの通知等に基づき異動情報を戸籍附票システムに登録する(更新を含む)。
- 1-② 本籍地市町村長において、戸籍附票システムより、市町村CSを経由して、附票都道府県サーバに対し附票本人確認情報の変更情報を通知する。
- 1-③ 附票都道府県サーバは、市町村CSから受信したデータを元に保存する附票本人確認情報を更新した後、附票全国サーバ(機構)に対し附票本人確認情報の変更情報を通知する。
- 1-④ 附票都道府県サーバより受信したデータを元に、機構保存附票本人確認情報を更新する。

(4)-2.市町村長、都道府県知事、国の機関等への附票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、5情報等をキーワードとした国外転出者に係る附票本人確認情報の照会を受ける。
- 2-② 当該個人の附票本人確認情報を機構保存附票本人確認情報から抽出し、照会元に提供する。
- 2-③ 上記2-②の際、番号法で認められた場合に限り、国の機関等からの求めに応じ、附票本人確認情報の提供に併せて当該個人の住民票コードを用いて、機構保存本人確認情報ファイルから個人番号を抽出し、照会元に提供する場合がある(特定個人情報を含む)。

(4)-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・情報提供者より、国外転出者に係る個人番号等に基づく符号取得要求を受ける。
- 3-② 国外転出者に係る符号取得要求を受け、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。個人番号により要求を受けた場合は、機構保存本人確認情報を用いて個人を特定するため、附票全国サーバで個人番号は取り扱わない。

(4)-4.附票本人確認情報開示

- 4-① 本人より附票本人確認情報の開示請求を受け付ける。
- 4-② 開示請求者に対し、当該個人の附票本人確認情報を開示する。

(4)-5.附票本人確認情報整合

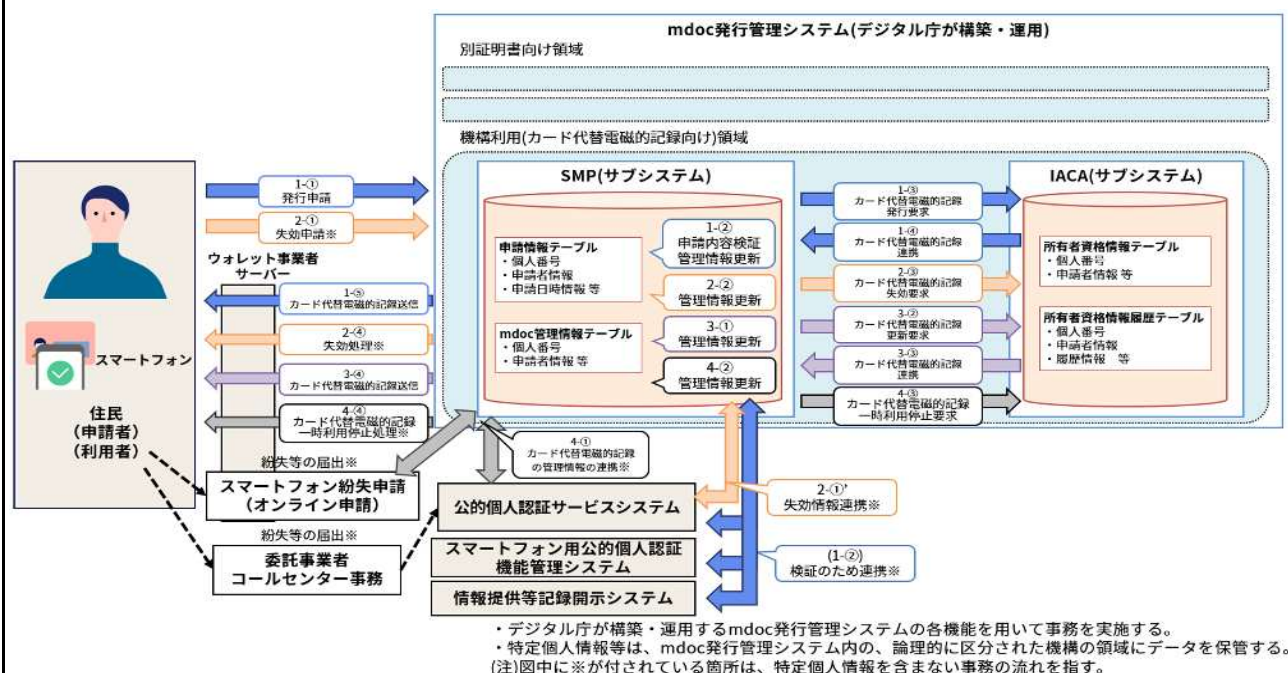
- 5-① 市町村CS又は住基全国サーバより、附票全国サーバに対し、整合性確認用の附票本人確認情報又は機構保存本人確認情報(個人番号を除く)を送付する(特定個人情報を含む(個人番号は含まない))。
- 5-② 附票全国サーバにおいて、市町村CS又は住基全国サーバより受領した整合性確認用の附票本人確認情報又は機構保存本人確認情報(個人番号を除く)を用いて機構保存附票本人確認情報の整合性確認を行う。
- 5-③ 附票全国サーバより、市町村CSに対して整合性確認結果を通知する。

(4)-6.附票本人確認情報の利用

- 6-① 国外転出者に関し個人番号カードの交付申請後及び交付後に個人番号カード管理システムより、住民票コードをキーとした利用者情報の照会を受ける。
- 6-② 当該個人の附票本人確認情報を機構保存附票本人確認情報から抽出し、個人番号カード管理システムへ提供する。

(別添1) 事務の内容**(5) カード代替電磁的記録に係る事務**

(注) 実際の手続ではカード代替電磁的記録の発行申請と併せてスマホ用電子証明書の利用申請も行われるが、スマホ用電子証明書の利用申請に際しては特定個人情報の取扱いが発生しないため、カード代替電磁的記録の発行に関する流れのみを記載している。



用語解説

- ・ウォレット事業者: スマートフォン上でカード代替電磁的記録を扱うためのプログラムの提供者。
- ・SMP: Secure Mobile Platform。mdoc発行管理システム内のサブシステムで、発行申請を受け付け、申請が不正でないかをチェックしたり、発行状態を管理したりする機能を担う。
- ・IACA: Issuing Authority, Certification Authority。mdoc発行管理システム内のサブシステムで、カード代替電磁的記録の発行局・認証局としての機能を担う。
- ・スマートフォン用公的個人認証機能管理システム: 利用者からの移動端末設備用電子証明書の発行等に係る申請を受け付け、公的個人認証サービスシステムへの発行等依頼等の連携機能を担う。

(備考)**(5)-1.カード代替電磁的記録の発行**

- 1-① SMPが申請者のスマートフォンから、カード代替電磁的記録の発行申請を受け付ける。
- 1-② SMPが当該申請の内容を登録し、検証を行う。その際、公的個人認証サービスシステム等、外部システムとの連携を行う。
- 1-③ SMPがIACAに対して、カード代替電磁的記録発行を要求する。
- 1-④ IACAがカード代替電磁的記録を発行し、SMPに連携する。
- 1-⑤ SMPがウォレット事業者のサーバーを経由し、申請者のスマートフォンにカード代替電磁的記録を送信する。

(5)-2.カード代替電磁的記録の失効

- 2-① SMPが利用者のスマートフォンから、カード代替電磁的記録の失効申請を受け付ける。
又は2-①' SMPは、公的個人認証サービスシステムと連携し、失効の契機を受け付ける。
- 2-② SMPが失効の内容を登録する。
- 2-③ SMPがIACAに対して、失効処理要求を行う。
- 2-④ SMPがウォレット事業者のサーバーを経由し、利用者のカード代替電磁的記録に失効処理を行う。

(5)-3.カード代替電磁的記録の更新

- 3-① SMPが日時処理等で管理情報を更新する。
- 3-② SMPがIACAに対して、更新内容に応じたカード代替電磁的記録の更新を要求する。
- 3-③ IACAが更新したカード代替電磁的記録を発行し、SMPに連携する。
- 3-④ SMPがウォレット事業者のサーバーを経由し、利用者のスマートフォンにカード代替電磁的記録を送信する。

(5)-4.カード代替電磁的記録の一時利用停止

- 4-① 盗難・紛失等によるカード代替電磁的記録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)から公的個人認証サービスシステムを介して、又はスマートフォンの紛失申請(オンライン申請)を行い、SMPにカード代替電磁的記録の管理情報を連携する。(※特定個人情報を含まない)。
- 4-② SMPが一時利用停止の内容を登録する。
- 4-③ SMPがIACAに対して、一時利用停止要求を行う。
- 4-④ SMPがウォレット事業者のサーバーを経由し、利用者のカード代替電磁的記録に一時利用停止処理を行う。

(注) 1-⑤、3-④においてスマートフォンに送信されるカード代替電磁的記録は、SMP上で暗号化処理を行い、申請者のスマートフォン上で復号する。

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	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 [☐] 5情報(氏名、氏名の振り仮名、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る、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)を併せて記録する必要がある。 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の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	2015/02/24	
⑥事務担当部署	住民基本台帳ネットワークシステム全国センター	

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 () 個人番号生成時は、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。 個人番号の変更時は、市町村長から住基全国サーバを経由して、住民票コード及び個人番号(変更前)を入手し、個人番号(変更後)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 () 個人番号生成時は、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。 個人番号の変更時は、市町村長から住基全国サーバを経由して、住民票コード及び個人番号(変更前)を入手し、個人番号(変更後)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		個人番号とすべき番号の生成要求や、個人番号の変更要求を契機として、都度入手・生成し、ファイルに格納する。 なお、番号法施行日(平成27年10月5日)への対応として、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、ファイルに格納した。
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。
⑤本人への明示		機構が個人番号とすべき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 ※		個人番号とすべき番号の生成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 ※	住民基本台帳ネットワークシステム全国センター
	使用者数	☐ 10人以上50人未満 <選択肢> 1) 10人未満 3) 50人以上100人未満 5) 500人以上1,000人未満 2) 10人以上50人未満 4) 100人以上500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。
		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20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 ☐ 委託する ☐ 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		☐ ☐	
対象となる本人の数		☐ ☐	
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		☐ ☐ ☐	
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 ※	☐ ☐ ☐	
	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 ☐ 電子メール ☐ フラッシュメモリ ☐ その他 (住民基本台帳ネットワークシステム) ☐ 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	市町村長からの個人番号とすべき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。 なお、番号法施行日 (平成27年10月5日) における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とすべき番号を住所地市町村ごとにまとめて提供を行った。

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。 サーバのバックアップについても、セキュリティゲートにて入退室管理をしている建物の中で、さらに入退室管理(※)を行っている部屋に設置した施錠可能な場所に保管する。 ※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部屋に入退室する者が権限を有すること及び作業に不要な機器等を持ち込まないことを確認する等の管理を行う。
②保管期間	期間	＜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 [定められていない]
	その妥当性	・個人番号とすべき番号の生成に関する問合せ対応のため、過去の記録を保存する必要がある。 ・生成済みの個人番号(個人番号とすべき番号を含む。)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		・上記理由からサーバ内に保管された個人番号管理ファイルに記録されたデータは消去しない。 ・バックアップは複数世代保管し、古いものから上書きする。 ・バックアップを廃棄する場合は、データが復元できないよう処理を行った上で、廃棄する。併せて、廃棄履歴を作成し、保存する。
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	
(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。) ※削除者を含む。
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 [☐] 5情報(氏名、氏名の振り仮名、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、5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、5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	2015/07/02
⑥事務担当部署	住民基本台帳ネットワークシステム全国センター

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、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区域内における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 ※	住民基本台帳ネットワークシステム全国センター
	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5情報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)。 ※国外転出者に係る事務処理に関し、番号法で認められた場合に限り、国の機関等からの求めに応じ、当該個人の住民票コードを用いて、機構保存本人確認情報ファイルから個人番号を抽出し、附票全国サーバに連携する場合がある。 ・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取得要求を受け(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)。 ・個人番号カード管理システムから利用者情報の照会要求を受け(個人番号カード管理システム→住基全国サーバ)、照会のあった住民票コード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(住基全国サーバ→個人番号カード管理システム)。 ・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ファイルから抽出し、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5情報等との突合を行う。 ・機構保存附票本人確認情報ファイルの住民票コードと機構保存本人確認情報ファイルの個人番号を突合する。 ・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、5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。
	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7月2日

4. 特定個人情報ファイルの取扱いの委託

[illegible]

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 () 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) ・第30条の15の2第1項(準法定事務処理者への本人確認情報の提供等)
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、氏名の振り仮名、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 [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か月に一度程度)に一括して又は照会の要求があった都度

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（デジタル庁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、追加又は削除の申出を行う。
③提供する情報	住民票コード、氏名、氏名の振り仮名、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

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。 サーバのバックアップについても、セキュリティゲートにて入退室管理をしている建物の中で、さらに入退室管理(※)を行っている部屋に設置した施錠可能な場所に保管する。 ※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部屋に入退室する者が権限を有すること及び作業に不要な機器等を持ち込まないことを確認する等の管理を行う。
②保管期間	期間	<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 [20年以上]
	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、住民基本台帳法施行令(昭和42年政令第292号)第30条の7(機構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		・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。 ・バックアップは複数世代保管し、古いものから上書きする。 ・バックアップを廃棄する場合は、データが復元できないよう処理を行った上で、廃棄する。併せて、廃棄履歴を作成し、保存する。
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。) ※削除者を含む。
その必要性	番号法第7条第1項(指定及び通知)及び個人番号カード省令第7条(個人番号の通知)に基づき、個人番号通知書を個人番号の付番対象者に送付する必要があるため。 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ため。 機構は、これらの事務を個人番号カード省令第23条から第23条の3まで及び第35条第1項に基づき、実施する。
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 [☐] 5情報(氏名、氏名の振り仮名、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、個人番号通知書の印刷情報、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、個人番号通知書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	2015/10/05
⑥事務担当部署	個人番号センター運用管理本部個人番号カード業務運用部、個人番号センター個人番号カードシステム開発部、個人番号センター運用管理本部個人番号カードシステム運用部、コンタクトセンター

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 (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) ・個人番号通知書及び交付申請書の送付先に係る情報は、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) ・個人番号カードの交付希望者により送付された交付申請書(記入済)により随時入手する。
④入手に係る妥当性		・送付先情報(市町村より入手) ・番号法第7条第1項(指定及び通知)及び個人番号カード省令第7条(個人番号の通知)に基づき、個人番号通知書を個人番号の付番対象者に送付するため、個人番号通知書の送付先情報が必要となる。 ・交付申請書(交付申請者本人より入手) ・個人番号カード省令第20条において、交付申請書に記載すべき事項として交付申請者の氏名、住所、個人番号が規定されている。
⑤本人への明示		機構が送付先情報及び交付申請書を入手することについて、個人番号カード省令第23条の2(個人番号通知書及び個人番号カードに関し機構が処理する事務)、第36条(機構への通知)に明示されている。
⑥使用目的 ※		個人番号カード省令第23条の2(個人番号通知書及び個人番号カードに関し機構が処理する事務)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 ※	個人番号センター運用管理本部個人番号カード業務運用部、個人番号センター個人番号カードシステム開発部、個人番号センター運用管理本部個人番号カードシステム運用部、コンタクトセンター
	使用者数	[10人以上50人未満] <選択肢> 1) 10人未満 3) 50人以上100人未満 5) 500人以上1,000人未満 2) 10人以上50人未満 4) 100人以上500人未満 6) 1,000人以上

⑧使用方法 ※		・住民に対して個人番号通知書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→個人番号カード管理システム）し、個人番号通知書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）を元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（※一時停止端末の画面上で個人番号は表示されない。）。
	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５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５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 ※	個人番号カード用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 (3) 件)	
委託事項1		番号通知書類の印刷に係る事務	
①委託内容		・個人番号通知対象者に対して送付する個人番号通知書及び交付申請書の印刷に係る事務(印刷・送付事務)	
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 [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 [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1項(指定及び通知)及び個人番号カード省令第7条(個人番号の通知)に基づき、個人番号通知書を個人番号の付番対象者に送付する必要がある。	
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 [10人以上50人未満]	
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		・(株) DNPデータテクノ(印刷・送付事務)	
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 [再委託する]	
	⑧再委託の許諾方法	原則として再委託は行わないこととするが、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を経た後に承認する。	
	⑨再委託事項	・個人番号通知書及び交付申請書の封入・封かん・発送	

委託事項3		コールセンター事務
①委託内容		通知カード、個人番号通知書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、個人番号通知書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		[50人以上100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		富士ソフトサービスビューロ（株）、（株）ベルシステム24
再委託	⑦再委託の有無 ※	[再委託しない] <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16条の2第2項 (個人番号カードの発行等) ・個人番号カード省令第23条の2 (個人番号通知書及び個人番号カードに関し機構が処理する事務)
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 ☐ 電子メール ☐ フラッシュメモリ ☐ その他 (住民基本台帳ネットワークシステム) ☐ 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。

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	
⑤移転する情報の対象となる本人の範囲	
⑥移転方法	
⑦時期・頻度	

6. 特定個人情報の保管・消去

①保管場所 ※		
②保管期間	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。サーバのバックアップを記録した電子記録媒体(バックアップ媒体)及び市町村合併等に伴う大量の送付先情報更新時に使用する電子記録媒体についても、セキュリティゲートにて入退室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)に設置した施錠可能な場所に保管する。 ※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及び作業に不要な機器等を持ち込まないことを確認する等の管理を行う。	
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。 ・バックアップ媒体は複数世代保管し、古いものから上書きする。 ・バックアップ媒体を廃棄する場合は、データが復元できないよう処理を行った上で、廃棄する。併せて、廃棄履歴を作成し、保存する。 ・特定個人情報記録された電子媒体(市町村から入手するもの)のデータは、個人番号カード管理システムに登録した後は、個人番号カード管理システムのサーバ上から消去する。 ・特定個人情報記録された電子媒体(市町村から入手するもの)などを廃棄する場合、業者にて物理的な破壊等によりデータを復元できないように完全消去し、消去証明書を提出させる。	

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	
(4) 機構保存附票本人確認情報ファイル	
2. 基本情報	
①ファイルの種類 ※	[システム用ファイル] ＜選択肢＞ 1) システム用ファイル 2) その他の電子ファイル (表計算ファイル等)
②対象となる本人の数	[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 ※	住基法第16条 (戸籍の附票の作成) に基づき戸籍の附票に記録された者 ※削除者を含む。
その必要性	本特定個人情報ファイル (機構保存附票本人確認情報ファイル) において戸籍の附票に記録された全ての者の情報を保有し、その記録を常に正確に更新・管理・提供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 [☐] 5情報 (氏名、氏名の振り仮名、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 (その他戸籍の附票関係情報 (戸籍の表示に係る情報は含まない。))
その妥当性	・5情報、その他戸籍の附票関係情報 (戸籍の表示に係る情報は含まない。) ・法令に基づき戸籍の附票に記録された者に関する記録を正確に行う上で、戸籍の附票の記載等に係る附票本人確認情報 (5情報、住民票コード及びこれらの変更情報) を記録する必要がある。なお、別添2に記載のとおり、記録項目には戸籍の表示に係る情報 (本籍及び筆頭者の氏名) は含まない。 ・個人番号 ・国外転出者に係る事務処理に関し、番号法で認められた場合に限り、国の機関等からの求めに応じ、当該個人の住民票コードを用いて、機構保存本人確認情報ファイルから個人番号を抽出し、附票全国サーバに連携する場合がある。提供後、個人番号は、機構保存附票本人確認情報ファイルに保有することはない。
全ての記録項目	別添2を参照。
⑤保有開始日	2024/05/27
⑥事務担当部署	住民基本台帳ネットワークシステム全国センター

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 (住基全国サーバ(※入手には該当しないが、住基全国サーバから個人番号を抽出する場合がある))
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 ()
③入手の時期・頻度	戸籍の附票において、附票本人確認情報の変更又は新規作成(出生等)が発生した都度入手する。 ※番号法別表に掲げる事務につき、地方公共団体、行政機関等から国外転出者に係るものに関し求めがあった場合、個人番号をその都度抽出する場合がある。
④入手に係る妥当性	法令に基づき、住民の利便の増進と国及び地方公共団体の行政の合理化に資するため、国外転出者に係る本人確認を行う上で、市町村の戸籍の附票の記載事項に変更が生じた都度、当該市町村を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。 ※なお、住基法第30条の44の6第6項に基づき、機構保存附票本人確認情報(住民票コードに限る。)を利用し、第30条の9、第30条の10から第30条の12まで又は第30条の15の2第1項の規定による事務について個人番号を提供することができるとされている。 ※※附票連携システムは、住基ネットを利用して構築されている。住基ネットは、保有情報・利用の制限、内部の不正利用の防止、外部からの侵入防止など、セキュリティ確保のための様々な措置が講じられており、平成14年8月5日の稼働後、住基ネットへのハッキングや情報漏えいなどの事件や障害は一度も発生していない。
⑤本人への明示	機構が都道府県知事より当該都道府県区域内における附票本人確認情報を入手することについて、住基法第30条の42(都道府県知事から機構への附票本人確認情報の通知等)に明示されている。 ※機構が国外転出者に係る個人番号を抽出する場合があることについて、住基法第30条の44の6第6項に明示されている。
⑥使用目的 ※	本特定個人情報ファイル(機構保存附票本人確認情報ファイル)において戸籍の附票に記録された全ての者の情報を保有し、その記録を常に正確に更新・管理・提供する。 ※番号法別表に掲げる事務につき、地方公共団体、行政機関等から国外転出者に係るものに関し求めがあった場合、個人番号をその都度抽出し、住基法第30条の9、第30条の10から第30条の12まで又は第30条の15の2第1項の規定による事務について提供する場合がある。
変更の妥当性	—

⑦使用の主体	使用部署 ※	住民基本台帳ネットワークシステム全国センター
	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 ※	・市町村長等からの附票本人確認情報の照会要求を受け(例:市町村CS→附票全国サーバ)、国外転出者に係る事務に関し、照会のあった住民票コード又は5情報の組合せを元に機構保存附票本人確認情報ファイルを検索し、該当する個人の附票本人確認情報を照会元へ提供する(例:附票全国サーバ→市町村CS)。 ※その際、番号法で認められた場合に限り、附票本人確認情報の提供に併せて、当該個人の住民票コードを用いて機構保存本人確認情報ファイルから個人番号を抽出し、照会元に提供する場合がある。	
	情報の突合 ※	・機構保存附票本人確認情報ファイルの住民票コードと機構保存本人確認情報ファイルの個人番号を突合する。
	情報の統計分析 ※	該当なし。
	権利利益に影響を 与え得る決定 ※	該当なし。
⑨使用開始日		令和6年5月27日

4. 特定個人情報ファイルの取扱いの委託

[illegible]

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 (2) 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附票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) ・第30条の44(国の機関等への附票本人確認情報の提供) ・第30条の44の3(附票通知都道府県の区域内の市町村の執行機関への附票本人確認情報の提供) ・第30条の44の4(附票通知都道府県以外の都道府県の執行機関への附票本人確認情報の提供) ・第30条の44の5(附票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附票本人確認情報の提供) ・第30条の44の6第6項(附票本人確認情報(住民票コードに限る。))の利用) ・第30条の44の7第1項(準法定事務処理者への附票本人確認情報の提供等)	
②提供先における用途	住基法別表に掲げる、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の処理に用いる。	
③提供する情報	住民票コード、氏名、氏名の振り仮名、住所、生年月日、性別、個人番号(番号法に基づく国の機関等からの求めがあった場合に限り。)	
④提供する情報の対象となる本人の数	☐ 100万人以上1,000万人未満 <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上	
⑤提供する情報の対象となる本人の範囲	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 ☐ 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	定期的(1か月に一度程度)に一括して又は照会の要求があった都度	

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44の2 (デジタル庁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。	

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。 サーバのバックアップについても、セキュリティゲートにて入退室管理をしている建物の中で、さらに入退室管理(※)を行っている部屋に設置した施錠可能な場所に保管する。 ※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部屋に入退室する者が権限を有すること及び作業に不要な機器等を持ち込まないことを確認する等の管理を行う。
②保管期間	期間	＜選択肢＞ 1) 1年未満 2) 1年 3) 2年 4) 3年 5) 4年 6) 5年 7) 6年以上10年未満 8) 10年以上20年未満 9) 20年以上 10) 定められていない
	その妥当性	附票本人確認情報の提供に併せて提供される個人番号は、地方公共団体、行政機関等からの求めにより提供された後は、障害発生等により提供先で情報を受領できなかった場合に備えて、一時的に保存されるのみである。
③消去方法		一時的な保存後にシステムにて自動判別し消去する。
7. 備考		
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

(5) カード代替電磁的記録用管理ファイル

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 ※	個人番号カードの交付を受けている住民 ※削除者を含む。	
その必要性	番号法第18条の2(カード代替電磁的記録の発行等)に基づき、住民(申請者)からの申請により、カード代替電磁的記録を発行し、申請者のスマートフォンに送信する必要があるため。	
④記録される項目	[50項目以上100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 [☐] 5情報(氏名、氏名の振り仮名、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 (日時等を含む申請内容の情報、カード代替電磁的記録の管理情報等)	
その妥当性	法令に規定されたカード代替記録事項に係る電磁的記録のほか、カード代替電磁的記録の管理等に必要な情報を保管するため	
全ての記録項目	別添2を参照。	
⑤保有開始日	「情報通信技術の活用による行政手続等に係る関係者の利便性の向上並びに行政運営の簡素化及び効率化を図るための行政手続等における情報通信の技術の利用に関する法律等の一部を改正する法律(令和6年法律第46号)」附則第1条第2号にて規定される公布の日から起算して1年を超えない範囲内において政令で定める日。	
⑥事務担当部署	個人番号センター	

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 ()	
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 (申請者のスマートフォンからのインターネット回線を通じた送信)	
③入手の時期・頻度	・本人(申請者のスマートフォンからのインターネット回線を通じた送信にて入手) ・カード代替電磁的記録の発行希望者により送信された、カード代替記録事項に係る電磁的記録により、随時入手する。	
④入手に係る妥当性	・個人番号カードに記録されたカード代替記録事項に係る電磁的記録の送信 ・番号法第18条の2第3項において、機構に対し、当該申請者の個人番号カードに記録されたカード代替記録事項に係る電磁的記録を送信して行うものと規定されている。 なお、番号法第2条第8項には、カード代替記録事項とは、番号法第2条第7項第1号から第5号(氏名、住所、生年月日、性別、個人番号)までに掲げる事項本人の写真及び主務省令で定める事項と規定されている。	
⑤本人への明示	機構がカード代替記録事項に係る電磁的記録を入手することについて、番号法第18条の2(カード代替電磁的記録の発行等)に明示されている。	
⑥使用目的 ※	番号法第18条の2(カード代替電磁的記録の発行等)に基づき、カード代替電磁的記録の発行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 ※	・申請者に対してカード代替電磁的記録を発行するため、申請者からカード代替記録事項に係る電磁的記録を受信し、カード代替電磁的記録を発行し、申請者のスマートフォンに送信する。 ・個人番号自体が、カード代替電磁的記録の記載事項であるため、カード代替電磁的記録の発行・送信に当たっては、特定個人情報の使用が発生する。	
	情報の突合 ※	・発行状況等の照会については、署名用電子証明書の署名利用者符号等を用いて突合を行うため、個人番号での突合は行わない。
	情報の統計分析 ※	カード代替電磁的記録用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、カード代替電磁的記録の発行状況の進捗を把握するため、申請情報の処理状況(現在どの状態にあるか)や、カード代替電磁的記録の発行数及び有効数等の集計は行う。
	権利利益に影響を与え得る決定 ※	該当なし。
⑨使用開始日	令和7年6月24日	

4. 特定個人情報ファイルの取扱いの委託

[illegible]

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 () 件 [] 移転を行っている () 件 [○] 行っていない
提供先1	
①法令上の根拠	
②提供先における用途	
③提供する情報	
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	
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	

[illegible]

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	
⑤移転する情報の対象となる本人の範囲	
⑥移転方法	
⑦時期・頻度	

6. 特定個人情報の保管・消去		
①保管場所 ※		<mdoc発行管理システムにおける措置> デジタル庁が政府情報システムとしてmdoc発行管理システムをガバメントクラウド上に構築する。 特定個人情報についても、mdoc発行管理システムの中で保管される。 mdoc発行管理システムについては、政府機関等のサイバーセキュリティ対策のための統一基準群や、デジタル庁情報セキュリティポリシーに準拠したセキュリティ対策が講じられている。 <ガバメントクラウドにおける措置> ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。
②保管期間	期間	<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 [10年以上20年未満]
	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や、電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律(平成14年法律第153号)(以下「公的個人認証法」という。)で定められる個人番号カード用電子証明書失効情報の保管期間を考慮し、当該管理情報を保管する必要がある。
③消去方法		<mdoc発行管理システムにおける措置> ・ガバメントクラウド上に構築し、事前に定義された保管期間の経過後、削除を行う。 ・クラウドサービス事業者からはデータにアクセスできないため、消去することができない。 <ガバメントクラウドにおける措置> ・クラウド事業者がHDDやSSDなどの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等にしたがって確実にデータを消去する。
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、25. 提供年月日、26. 機能区分、27. 利用事由、28. 提供事務区分、29. 個人番号提供事務区分、30. 提供元、31. 提供先、32. 旧氏 漢字、33. 旧氏 外字数、34. 旧氏 ふりがな、35. 旧氏 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. 顔写真、69. 申請書イメージ、70. 申請年月日、71. 点字有無、72. 点字カナ氏名 項目長、73. 点字カナ氏名、74. 依頼管理番号、75. カードセキュリティ情報区分、76. 処理結果コード、77. 提供元市町村コード、78. 異動事由、79. 異動年月日、80. 予備領域1、81. 予備領域2、82. カード状況区分、83. 公開鍵長、84. 公開鍵、85. 発行委託番号、86. 事業者コード、87. カード発行番号、88. コマンド、89. 有効期限、90. 個人番号カード情報、91. カード運用状況、92. カード有効期限、93. 一時停止日、94. 一時停止理由、95. カード廃止日、96. カード廃止理由、97. カード回収日、98. タイムスタンプ、99. 所管フラグ、100. 転入処理日、101. 転出予定経過日、102. 本人確認情報有無、103. 前住地市町村コード、104. 住基AP識別情報、105. 暗号識別情報、106. カード製造者識別情報、107. カードイメージ番号、108. 被証明者識別子、109. 通知カード・個人番号通知書管理状況、110. 旧氏 漢字、111. 旧氏 外字数、112. 旧氏 ふりがな、113. 旧氏 外字変更連番、114. ローマ字 氏名、115. ローマ字 旧氏、116. 一体化情報コード、117. 特定在留カード等の有効期限、118. カードバージョン、119. 住民票コード変更受信フラグ、120. 住民票コード変更年月日

(4) 機構保存附票本人確認情報ファイル

ア 附票本人確認情報

1. 住民票コード、2. 氏名 漢字、3. 氏名 外字数、4. 氏名 ふりがな、5. 生年月日、6. 性別、7. 住所 市町村コード、8. 住所 漢字、9. 住所 外字数、10. 最終住所 漢字、11. 最終住所 外字数、12. 異動年月日、13. 旧住民票コード、14. 附票管理市町村コード、15. 附票本人確認情報状態区分、16. 外字フラグ、17. 外字パターン、18. 通知区分、19. 旧氏 漢字、20. 旧氏 外字数、21. 旧氏 ふりがな、22. 旧氏 外字変更連番

イ その他

1. 個人番号(※国外転出者に係る事務処理に関し、番号法で認められた場合に限り、国の機関等からの求めに応じ、当該個人の住民票コードを用いて、機構保存本人確認情報ファイルから個人番号を抽出し、提供する場合がある。)

(5) カード代替電磁的記録用ファイル

ア 申請情報

1. 申請ID、2. 申請種別、3. 申請ステータス、4. 申請詳細ステータス、5. mdoc申請詳細ステータス、6. JPKI申請詳細ステータス、7. 申請受付日時、8. 所有者ID、9. 発行資格情報ID、10. 発行バンドルID、11. アプラインストールID、12. OS識別子、13. インスタンス共有ID、14. カード発行番号、15. カード有効期限、16. 市町村コード、17. 4情報(氏名、住所、性別、生年月日)、18. 個人番号、19. 顔写真(券面)、20. 顔写真(撮影)、21. mdoc画面表示文言、22. 個人番号・4情報署名、23. 署名検証用公開鍵証明書、24. 券面事項署名データ、25. 券面事項用公開鍵証明書_K、26. 処理対象、27. JPKI画面表示文言、28. 電子署名、29. アルゴリズムID、30. 電子証明書、31. 電子証明書種別、32. 署名用電子証明書シリアル番号、33. カードID、34. 次工程トークン、35. 次工程トークン有効期限、36. ワンタイムパスワードリクエストID、37. イベント通知受信フラグ、38. イベント通知受信ステータス、39. 発行バンドル取得受信フラグ、40. バンドル更新送信フラグ、41. バンドル更新失敗受信日時、42. 待機コマンド送信フラグ、43. 待機コマンド結果受信フラグ、44. 確定コマンド受信結果フラグ、45. サブミットコマンド受信結果受信ステータス、46. パス管理受信フラグ、47. 解除契機申請ID、48. カンパセッションID、49. 発行紐付けタスクID、50. 発行紐付けステータス、51. 待機コマンドタスクID、52. 確定コマンドタスクID、53. APDUレスポンス、54. セキュア領域制御公開鍵証明書、55. 補助セキュア領域鍵ID、56. 補助セキュア領域鍵、57. 補助セキュア領域証明書、58. サービス提供者セキュア領域証明書シリアル番号、59. アプレットバージョン、60. プラットフォームバージョン、61. 暗号化データ、62. 電文ID、63. デバイストークン、64. リクエスト理由コード、65. コミットメントS2、66. 登録日時、67. 更新日時、68. バンドル更新送信ID

イ mdoc管理情報

1. mdociD、2. mdocステータス、3. カード発行番号、4. カード有効期限、5. 4情報(氏名(氏名の振り仮名含む)、住所、性別、生年月日)、6. 市町村コード、7. 個人番号、8. 顔写真(券面)、9. 生年月日(検索用)、10. mdoc最終送信日時、11. MSO有効期限、12. 削除フラグ、13. 登録日時、14. 更新日時

ウ 所有者資格情報

1. レコードID、2. 電文ID、3. 資格情報ID、4. 資格情報バージョンID、5. 資格情報ステータス、6. 氏名、7. 生年月日、8. 現住所、9. 性別、10. 市町村コード、11. 個人番号、12. 発行者名、13. 発行日時、14. 有効期限、15. 最終検証日時、16. 顔写真(券面)、17. 登録日時、18. 更新日時

エ 所有者資格情報履歴

1. レコードID、2. 資格情報ID、3. 資格情報ステータス、4. 氏名、5. 生年月日、6. 現住所、7. 性別、8. 市町村コード、9. 個人番号、10. 発行者名、11. 発行日時、12. 有効期限、13. 最終検証日時、14. 顔写真(券面)、15. 登録日時

オ 別OS申請情報

1. 申請ID、2. 端末参照ID、3. 発行コード、4. 資格情報ID、5. 資格情報バージョンID、6. 電文ID、7. 申請ステータス、8. 申請詳細ステータス、9. mdoc申請詳細ステータス、10. 申請種別、11. 申請受付日時、12. 認可コード、13. OS識別子、14. 端末ID、15. カード発行番号、16. カード有効期限、17. 市町村コード、18. 4情報、19. 個人番号、20. 顔写真(券面)、21. 顔写真(撮影)、22. 画面表示文言、23. 個人番号・4情報署名、24. 署名検証用公開鍵証明書、25. 券面事項署名データ、26. 券面事項用公開鍵証明書_K、27. 電子署名、28. アルゴリズムID、29. 電子証明書、30. 電子証明書種別、31. 署名用電子証明書シリアル番号、32. デバイストークン、33. 登録日時、34. 更新日時

カ CDDL情報

1. mdociD、2. トランザクション鍵連番、3. mdoc、4. 電文ID、5. 登録日時、6. 更新日時

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漏えい・紛失するリスク		
リスクに対する措置の内容	個人番号の変更時、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、受渡し時は複数人に対応し、受渡し簿等に受渡しの記録を残す、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。なお、通常業務においては、電子記録媒体による入手は行わない。	
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	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程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については半期ごと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又は削除する。	

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程に基づき、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。具体的には、特定個人情報への不正アクセスを防止するために、アクセスに係る作業を行う者とは別の者が分析・確認を行う体制を整備し、主に市区町村からの依頼に基づく調査を対象として、当該ログの分析・確認の上、その結果を管理責任者へ報告する。 また、規程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		ユーザ認証、アクセス権限の管理に加えて、個人番号管理ファイルにアクセスできる端末を制限する。	
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： 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リスクアセスメント及びリスク対応や、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（年に一度開催）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。 ・サーバのバックアップを記録した電子記録媒体については、セキュリティゲートにて入退室管理をしている建物の中で、さらに入退室管理（※）を行っている部屋に設置した施錠可能な場所に保管する。 ※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部屋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。	
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、個人番号とすべき番号の提供記録（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年未満の拘禁刑に当たる罪）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・移転に係るルールについては、「地方公共団体情報システム機構個人情報保護規程」においてその具体的なルールを定めている。	
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を防止している。 なお、相手先（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

—

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	[十分に遵守している]	<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。 ・サーバ室等への不要な機器の持ち込みを制限し、入退室時に確認を行う。 ・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(コンピュータウイ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。 :インターネットを通じて外部に本人確認情報が漏えいしないよう、個人番号生成システムをインターネットから物理的に分離する。
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、過去に生成した番号と重複した番号の生成を防止する（新規に個人番号とすべき番号を生成する際に、生成済みの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(住基法第3条において、市町村の責務として、常に、住民基本台帳を整備し、住民に関する正確な記録が行われるように努めるとともに、住民に関する記録の管理が適正に行われるように必要な措置を講ずるよう努めることとされている)。このため、年に一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、厳格な審査が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	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、附票連携システムと接続するが、特定個人情報の連携先は、①個人番号生成システム、②個人番号カード管理システム及び③附票連携システムに限られるよう、アクセス制御を行う。 なお、住基全国サーバと①、②、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) 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。 ：個人番号カード管理システムからの利用者情報照会要求に対して利用者情報照会結果を提供する場合。 ③附票連携システム ：番号法で認められた場合に限り、地方公共団体、行政機関等からの求めに応じ、国外転出者に係る個人番号を連携する場合。 (2) 他のシステム⇒住基全国サーバへのアクセス ①個人番号生成システム ：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 ：利用者情報照会要求を行う場合。ただし、住民票コードのみをキーとし、特定個人情報を使ったアクセスは行わない。 ③附票連携システム ：番号法で認められた場合に限り、地方公共団体、行政機関等からの求めに応じ、国外転出者に係る個人番号を入手する場合。	
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	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情報提供先の端末等について ・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、ユーザ認証を実施するとともに、情報利用に係る証跡(ログ)を取得することにより、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機関に対しては、ユーザ認証を実装するよう要求する。 ・自動連携機能(※※)を利用する機関に対しては、端末のユーザ認証や物理的対策を実施するとともに、自ら管理する庁内システムへのアクセス制限、操作ログ分析などを適切に行うよう要求する。 ※ 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。 ※※ 自動連携機能: 庁内システムに登録した照会ファイルについて、情報提供サーバで行っていた手動の送信操作を省き、自動的に全国サーバへ連携する機能のこと。機構が提供するAPI(※)を元に各機関が当該機能の独自開発を行い、庁内システムに搭載している。	

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程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については半期ごと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又は削除する。	
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程に基づき、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。具体的には、特定個人情報への不正アクセスを防止するために、アクセスに係る作業を行う者とは別の者が分析・確認を行う体制を整備し、主に市区町村からの依頼に基づく調査を対象として、当該ログの分析・確認の上、その結果を管理責任者へ報告する。 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		ユーザ認証、アクセス権限の管理に加えて、機構保存本人確認情報ファイルにアクセスできる端末を制限する。	
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: 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リスクアセスメント及びリスク対応や、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(年に一度開催)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。 ・サーバのバックアップを記録した電子記録媒体(バックアップ媒体)については、セキュリティゲートにて入退室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(データ保管室)に設置した施錠可能な場所に保管する。 ※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部屋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。	
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		
—		

【○】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な	[]	<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	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、5情報等）の提供を行う際に（番号法で認められた場合に限り、当該個人の住民票コードを用いて、「機構保存本人確認情報ファイル」から個人番号を抽出し、附票全国サーバに連携する場合を含む。）、当該情報の提供記録（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年未満の拘禁刑に当たる罪）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する。	
特定個人情報の提供・移転に関するルール	[定めている]	☐ <選択肢> ☐ 1) 定めている ☐ 2) 定めていない
ルールの内容及びルール遵守の確認方法	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5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・移転に係るルールについては、「地方公共団体情報システム機構個人情報保護規程」においてその具体的なルールを定めている。	
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、提供先とは、提供に係る協定書を締結し、媒体の適切な保管及び廃棄を定めるとともに、セキュリティチェックリストにより、提供先機関における適切な保管及び廃棄を確認している。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等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、相手先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渡し時は、業務時間内に施錠可能なケースに格納して運搬した上で、複数人の立会いの下で受渡しを行い、受渡し簿等に相手が署名した受渡しの記録を残す。 国外転出者に係る事務処理に関し、番号法で認められた場合に限り、地方公共団体、行政機関等からの求めに応じ、個人番号を連携することを、システムにより担保する。	
リスクへの対策は十分か	[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。 ：媒体に書き込み後のデータについては、誤った情報が提供されないよう、月次で消去する。 ・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、情報連携の相手先は法令に定められた機関に限定されており、また、相手先（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。 ：媒体での提供時は、顔写真入りの身分証明書の提示を求め、本人確認を行っている。
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	[]	☐ 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	[]	☐ 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	[]	☐ 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	[]	☐ 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]	☐ 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、不適切な方法での特定個人情報の提供・移転の防止に努める。		
リスクへの対策は十分か	[十分である]	☐ 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]	☐ 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(デジタル庁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	[十分に遵守している]	<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。 ・サーバ室等への不要な機器の持ち込みを制限し、入退室時に確認を行う。 ・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(コンピュータウイ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。 :インターネットを通じて外部に本人確認情報が漏えいしないよう、住基全国サーバをインターネットから物理的に分離する。
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	5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ファイル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（消去されたデータは、復元できない）。 なお、媒体による提供の場合には、書き込み後のデータを、作業チェックリストに基づき、月次で手動で消去する（消去されたデータは、復元できない）。 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	—	
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	
(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市町村からの個人番号通知書等の「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。電子記録媒体による送付先情報の入手の際には、市町村から提供される送付先情報を編集を行わず、そのままプログラム（ツール）でカード管理システムへ取り込み、市町村からの受領件数と取り込み件数結果を、市町村職員及び機構職員双方で確認することにより担保する。 ②交付申請書 ：交付申請書は一通につき一人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、手書用交付申請書以外の交付申請書には個人番号は記入させないことにより、必要な者以外の特定個人情報の入手を防止し、手書用交付申請書に仮に誤った個人番号が記載されて申請された場合であっても、他の情報との突合により検知し、誤った個人番号カードが発行されることを防止している。 なお、住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に様式とする。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、個人番号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、機構側では対象者が否かの判断ができないため、市町村における個人番号カード交付時等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。 ・交付申請書は「個人番号カード交付申請書」と明示し、個人番号の記入欄を明確にするなど交付申請者（入手元）への配慮を行っている。
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

リスク3： 入手した特定個人情報 that 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合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 ：手書用交付申請書に記載された5情報等を個人番号カード管理システムにおいて突合することにより個人番号の真正性を担保する。 ※手書用交付申請書以外の交付申請書には個人番号は記載させない。
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、5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 ：手書用交付申請書は交付申請者が任意で記載するものであるため記載内容の正確性は交付申請者に委ねられる。 ※手書用交付申請書以外の交付申請書には個人番号は記載させない。
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4： 入手の際に特定個人情報 that 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。 ・電子記録媒体による送付先情報の入手の際には、市町村では送付先情報を暗号化して電子記録媒体へ格納し、2名以上の市町村職員で機構に持ち込む。機構側では2名以上の職員で受領した後、当該媒体のウイルスチェックを実施する。その後、復号化してカード管理システムへ取り込むことにより担保する。
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	
—	

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	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、④（株）DNPデータテクノ、⑤附票連携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①～⑤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 ：利用者情報照会を行う場合。ただし、住民票コードのみをキーとし、特定個人情報を使ったアクセスは行わない。 ②個人番号カード申請受付・発行システム ：個人番号カード発行情報等を提供する場合、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、個人番号通知書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。 ④（株）DNPデータテクノ ：個人番号通知書発行情報等を提供する場合。 ⑤附票連携システム ：国外転出者に係る利用者情報照会を行う場合。ただし、住民票コードのみをキーとし、特定個人情報を使ったアクセスは行わない。 （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。 ：個人番号カード管理システムからの利用者情報照会に基づき、本人確認情報を連携する場合。 ②個人番号カード申請受付・発行システム ：個人番号カードの発行結果等を受信する場合。 ③コールセンター ：通知カード、個人番号通知書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。 ④（株）DNPデータテクノ ：個人番号通知書発行結果等を受信する場合。 ⑤附票連携システム ：市町村CSより附票都道府県サーバを経由して受領した国外転出者の異動情報を連携する場合（特定個人情報を含まない）。 ：個人番号カード管理システムからの国外転出者に係る利用者情報照会に基づき、附票本人確認情報を連携する場合（特定個人情報を含まない）。	
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	特定個人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、特定個人情報の管理について定めた規程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については半期ごと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又は削除する。	
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	特定個人情報の管理について定めた規程に基づき、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。具体的には、特定個人情報への不正アクセスを防止するために、アクセスに係る作業を行う者とは別の者が分析・確認を行う体制を整備し、主に市区町村からの依頼に基づく調査を対象として、当該ログの分析・確認の上、その結果を管理責任者へ報告する。 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		ユーザ認証、アクセス権限の管理に加えて、個人番号カード用管理ファイルにアクセスできる端末を制限する。	
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： 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リスクアセスメント及びリスク対応や、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(年に一度開催)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。 ・サーバのバックアップを記録した電子記録媒体（バックアップ媒体）及び市町村合併等に伴う大量の送付先情報更新時に使用する電子記録媒体についても、セキュリティゲートにて入退室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）に設置した施錠可能な場所に保管する。 ※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。	
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		
—		

「 」委託しない

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)番号通知書類の印刷に係る事務 (2)個人番号カードの交付申請受付・発行・市町村への送付に係る事務 (3)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。

[制限している] **＜選択肢＞**
1) 制限している 2) 制限していない

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。

記録を残している

1) 記録を残している 2) 記録を残していない

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。

[定めている] ＜選択肢＞
1) 定めている 2) 定めていない

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、四半期に一度、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年未満の拘禁刑に当たる罪）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。

[定めている] <選択肢>
1) 定めている 2) 定めていない

委託契約上、以下の措置をとる旨を規定する。

- ・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を外部業者にて溶解処理を行う。
- ・データが紙かを問わず、廃棄の際は廃棄履歴を作成し保存する。
- ・特定個人情報と同様、保管期間の過ぎたバックアップデータを、システムにて自動判別し消去する。
- ・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、四半期に一度、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		・目的外利用を禁止する。 ・特定個人情報の閲覧者・更新者を制限する。 ・特定個人情報の提供先を限定する。 ・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データを完全に消去する。 ・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		原則として再委託は行わないこととするが、再委託を行う場合は、以下の措置を取ることとする。 ・委託先に対して、本委託事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、本委託事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			
・個人番号通知書及び交付申請書の差出前に外観検査・員数検査・重量検査・厚み検査を実施することを委託契約の仕様書に定める等の現行措置に加え、個人番号通知書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随時検討する。 ・機構は、委託を受けた者に対して、機構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うこととする。また、原則として再委託は行わないこととするが、再委託を行う場合は、機構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うこととする。			

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、当該情報の提供記録（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年未満の拘禁刑に当たる罪）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・移転に係るルールについては、「個人番号カード等に関する技術的基準」（平成27年9月18日総務省告示第314号）においてその具体的なルールを定めている。		
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る専用線を用いること、連携するデータが暗号化される機能をシステムに実装することにより、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、相手先と個人番号カード管理システムと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渡し時は複数人の立会いの下で行い、受渡し簿等に受渡しの記録を残す。		
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全てを連携することはできない(送付先情報(個人番号、5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 ・相手先(市町村C S等)と個人番号カード管理システムと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 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 3) 課題が残されている	2) 十分である
リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク5： 不正な提供が行われるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク6： 不適切な方法で提供されるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク7： 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置			

7. 特定個人情報の保管・消去		
リスク1: 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[十分に遵守している]	<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。 ・サーバ室等への不要な機器の持ち込みを制限し、入退室時に確認を行う。 ・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。 特定個人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(コンピュータウイ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 ・特定個人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。 ・インターネットを通じて外部に特定個人情報を漏えいしないよう、個人番号カード管理システムをインターネットから物理的に分離する。
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データを消去する。消去の際は消去履歴を作成し保存する。 ・特定個人情報が記録された電子媒体（市町村から入手するもの）のデータは、個人番号カード管理システムに登録した後は、個人番号カード管理システムのサーバ上から消去する。 ・特定個人情報が記録された電子媒体（市町村から入手するもの）などを廃棄する場合、業者にて物理的な破壊等によりデータを復元できないように完全消去し、消去証明書を提出させる。 ・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		
—		

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		
(4) 機構保存附票本人確認情報ファイル		
2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）		
リスク1： 目的外の入手が行われるリスク		
対象者以外の情報の入手を防止するための措置の内容	市町村CSから附票都道府県サーバを経由してなされた附票本人確認情報の更新通知により附票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（住基法第3条において、市町村の責務として、常に、住民基本台帳を整備し、住民に関する正確な記録が行われるように努めるとともに、住民に関する記録の管理が適正に行われるように必要な措置を講ずるよう努めることとされている）。このため、年に一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。また、対象者以外の個人番号は入手できないことを、システムにより担保する。	
必要な情報以外を入手することを防止するための措置の内容	附票本人確認情報及び対象者の個人番号以外の個人情報は入手できないことを、システムにより担保する。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2： 不適切な方法で入手が行われるリスク		
リスクに対する措置の内容	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附票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から附票都道府県サーバを経由してなされた附票本人確認情報の更新通知により機構保存附票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。 また、国外転出者に係る事務処理に関し、番号法で認められた場合に限り、地方公共団体、行政機関等からの求めに応じ、個人番号を入手することを、システムにより担保する。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3： 入手した特定個人情報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、厳格な審査が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。 個人番号については、機構保存本人確認情報ファイルから入手するため、該当なし。	
個人番号の真正性確認の措置の内容	機構保存本人確認情報ファイルに保存される段階で真正性が担保されている。	
特定個人情報の正確性確保の措置の内容	附票本人確認情報更新の際に、論理チェックを行う仕組みとする。 また、個人番号については、機構保存本人確認情報ファイルに保存される段階で正確性が確保されている。	
その他の措置の内容	—	
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。 ・入手の際に特定個人情報漏えい・紛失するリスクがないよう、安全が確保された専用線で接続する。
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	
—	

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	機構において、地方公共団体の宛名システムに相当する、附票本人確認情報及び個人番号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	附票全国サーバは、機構内において、住基全国サーバ、個人番号カード管理システムと接続する。 なお、附票全国サーバと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) 附票全国サーバ⇒他のシステムへのアクセス ①住基全国サーバ ：国外転出者に係る事務処理に関し、番号法で認められた場合に限り、地方公共団体、行政機関等からの求めに応じ、個人番号を入手する場合（目的を超えた紐づけが行われないよう、個人番号は附票本人確認情報DBとは別の一時保存領域で処理する。）。 ②個人番号カード管理システム ：市町村CSより附票都道府県サーバを経由して受領した国外転出者の異動情報を連携する場合（特定個人情報を含まない）。 ：個人番号カード管理システムからの利用者情報照会要求に対して国外転出者に係る利用者情報照会結果を提供する場合（特定個人情報を含まない）。 (2) 他のシステム⇒附票全国サーバへのアクセス ①住基全国サーバ ：番号法で認められた場合に限り、地方公共団体、行政機関等からの求めに応じ、国外転出者に係る個人番号を連携する場合。 ②個人番号カード管理システム ：国外転出者に係る利用者情報照会要求を行う場合。ただし、住民票コードのみをキーとし、特定個人情報を使ったアクセスは行わない。
その他の措置の内容	—
リスクへの対策は十分か	[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、ユーザ認証を実施するとともに、情報利用に係る証跡（ログ）を取得することにより、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機関に対しては、ユーザ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（附票本人確認情報の管理に関する規定を含む。以下同じ。）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程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については半期ごと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又は削除する。	
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程に基づき、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。具体的には、特定個人情報への不正アクセスを防止するために、アクセスに係る作業を行う者とは別の者が分析・確認を行う体制を整備し、主に市区町村からの依頼に基づく調査を対象として、当該ログの分析・確認の上、その結果を管理責任者へ報告する。 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		ユーザ認証、アクセス権限の管理に加えて、機構保存附票本人確認情報ファイルにアクセスできる端末を制限する。	
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： 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リスクアセスメント及びリスク対応や、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（年に一度開催）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。 ・サーバのバックアップを記録した電子記録媒体（バックアップ媒体）については、セキュリティゲートにて入退室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（データ保管室）に設置した施錠可能な場所に保管する。 ※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部屋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。	
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開覧者・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な	[]	<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	住基法に基づき機構保存附票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、附票本人確認情報の提供に併せて個人番号の提供を行う際に、当該情報の提供記録（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年未満の拘禁刑に当たる罪）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する。	
特定個人情報の提供・移転に関するルール	[定めている]	<選択肢> 1) 定めている 2) 定めていない
ルール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5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・移転に係るルールについては、「地方公共団体情報システム機構個人情報保護規程」においてその具体的なルールを定めている。	
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附票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、提供先とは、提供に係る協定書を締結し、媒体の適切な保管及び廃棄を定めるとともに、セキュリティチェックリストにより、提供先機関における適切な保管及び廃棄を確認している。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附票連携システムを用いることにより、不適切な方法による特定個人情報の提供を防止する。 なお、相手先と附票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渡し時は、業務時間内に施錠可能なケースに格納して運搬した上で、複数人の立会いの下で受渡しを行い、受渡し簿等に相手が署名した受渡しの記録を残す。	
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。また、情報照会の対象となる本人の情報のみが、一時保存領域に保存されるようにシステムで制御されている。 ・媒体に書き込み後のデータについては、誤った情報が提供されないよう、月次で消去する。 ・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、情報連携の相手先は法令に定められた機関に限定されており、また、相手先（市町村CS等）と附票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。 ・媒体での提供時は、顔写真入りの身分証明書の提示を求め、本人確認を行っている。	
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 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 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	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 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	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、不適切な方法での特定個人情報の提供・移転の防止に努める。		
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 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	・誤った情報の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 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			
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44の2（デジタル庁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	[十分に遵守している]	<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。 ・サーバ室等への不要な機器の持ち込みを制限し、入退室時に確認を行う。 ・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(コンピュータウイ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。 :インターネットを通じて外部に附票本人確認情報が漏えいしないよう、附票全国サーバをインターネットから物理的に分離する。
⑦バックアップ	[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
⑧事故発生時手順の策定・周知	[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	[発生なし]	<選択肢> 1) 発生あり 2) 発生なし
	その内容	—
	再発防止策の内容	—
⑩死者の個人番号	[保管していない]	<選択肢> 1) 保管している 2) 保管していない
	具体的な保管方法	—
その他の措置の内容		—
リスクへの対策は十分か		[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

リスク2： 特定個人情報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	附票本人確認情報の提供に併せて提供される個人番号は、地方公共団体、行政機関等からの求めにより提供された後は、障害発生等により提供先で情報を受領できなかった場合に備えて一時的に保存がされるのみであり、情報が更新される必要はない。
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	障害発生等により提供先で情報を受領できなかった場合に備えた一時的な保存の終了後、特定個人情報を、システムにて自動判別し消去する（消去されたデータは、復元できない）。 なお、媒体による提供の場合には、書き込み後のデータを、作業チェックリストに基づき、月次で手動で消去する（消去されたデータは、復元できない）。
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	
(5) カード代替電磁的記録用管理ファイル	
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	＜mdoc発行管理システムにおける措置＞ 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、カード代替電磁的記録の発行を希望する申請者のスマートフォンからインターネット回線を通じて送信された、カード代替記録事項（当該申請者の個人番号カードの券面事項入力補助APから取得した氏名（氏名の振り仮名含む）、住所、生年月日、性別、個人番号及び本人の写真に係る事項）に係る電磁的記録により、随時入手する。 この場合においては、当該申請者は、個人番号カード用署名用電子証明書に係る署名利用者符号を用いて電子署名を行う必要がある。送信を受けた機構は、個人番号カード用署名用電子証明書が公的個人認証法第15条第1項の規定により効力を失っていないこと及び署名利用者検証符号に対応する署名利用者符号を用いて電子署名が行われたことを確認することで、申請者本人からの申請であることを確認している。 以上により、対象者以外の情報の入手が行われることが無いよう、措置を講じている。
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	カード代替記録事項に係る電磁的記録に含まれる内容が、必要最小限の情報の記載となるよう、個人番号カードの読み取りにより必要な情報を入手し、申請者に自由入力させることを避けることで、申請者が不要な情報を送信してしまうリスクを防止する措置を講じている。
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においては、デジタル庁が配布するスマートフォンアプリケーションを用いて行い、その他の手法による入手をシステム上不可能とし、デジタル庁が配布するスマートフォンアプリケーション上も、個人番号カードのインターフェース仕様に沿った手法でカードの読み取りにより必要な情報を入手することで、不適切な方法で入手が行われないよう措置を講じている。
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： 入手した特定個人情報ที่ไม่正確であるリスク	
入手の際の本人確認の措置の内容	＜mdoc発行管理システムにおける措置＞ 特定個人情報の入手においては、申請者は、個人番号カード用署名用電子証明書に係る署名利用者符号を用いて電子署名を行う必要がある。送信を受けた際は、個人番号カード用署名用電子証明書が公的個人認証法第15条第1項の規定により効力を失っていないこと及び署名利用者検証符号に対応する署名利用者符号を用いて電子署名が行われたことを確認することで、本人からの申請であることを確認する措置を講じている。 ＜デジタル庁が配布するスマートフォンアプリケーションにおける措置＞ ・個人番号カードのICチップ読み取り（券面事項入力補助AP）と暗証番号入力 ・（券面事項入力補助APの暗証番号）による二要素認証で本人確認を行うため、本人からの情報のみが送信される。
個人番号の真正性確認の措置の内容	カード代替記録事項に係る電磁的記録は、申請者のスマートフォンで、個人番号カードのICチップを読み取る方式によって取得する。 取得においては、個人番号・4情報署名の署名検証用公開鍵証明書を用いて取得した情報の真正性の確認を行う。また、申請者のスマートフォンから、mdoc発行管理システムまでの経路上での改ざんを防止するため、当該申請者は、個人番号カード用署名用電子証明書に係る署名利用者符号を用いて電子署名を行う必要があり、送信を受けた機構は署名利用者検証符号に対応する署名利用者符号を用いて電子署名が行われたことを確認する。以上により、真正性確認の措置を講じている。
特定個人情報の正確性確保の措置の内容	＜mdoc発行管理システムにおける措置＞ 特定個人情報に含まれる個人番号以外のデータについても、個人番号カードから取得を行う。取得した特定個人情報はmdoc発行管理システムに自動連携されることにより正確性確保の措置を講じている。
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 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	<mdoc発行管理システムにおける措置> 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。 また、下記の通信経路に関しても情報を暗号化する。 ・(申請) 申請者-mdoc発行管理システム間 ・(発行) mdoc発行管理システム-ウォレット事業者サーバ-申請者		
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 3) 課題が残されている	2) 十分である
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	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	<mdoc発行管理システムにおける措置> ・mdoc発行管理システムは、利用者のスマートフォン、ウォレット事業者サーバーとインターネット接続するが、mdoc発行管理システム上の情報（個人番号含む）にはアクセスできないように制御している。 ・スマートフォンへのカード代替電磁的記録送信のために、ウォレット事業者サーバーと接続を行う際には、mdoc発行管理システムとスマートフォンの間で特定個人情報を含むデータの暗号化処理を行い、仲介するウォレット事業者サーバー上で、個人番号が復号されないように措置する。	
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: 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	<mdoc発行管理システムにおける措置> mdoc発行管理システムを運用するデジタル庁において、以下の管理を実施する。 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	<mdoc発行管理システムにおける措置> mdoc発行管理システムを運用するデジタル庁において、以下の管理を実施する。 (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、運用保守主管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	<mdoc発行管理システムにおける措置> mdoc発行管理システムを運用するデジタル庁において、以下の管理を実施する。 アクセス権限の管理は、特定個人情報の管理について定めた規程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については半期ごと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又は削除する。	

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	<mdoc発行管理システムにおける措置> mdoc発行管理システムを運用するデジタル庁において、以下の管理を実施する。 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。 具体的には、特定個人情報への不正アクセスを防止するために、アクセスに係る作業を行う者とは別の者が分析・確認を行う体制を整備し、分析・確認の上、その結果を運用保守管理者へ報告する。 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リスクアセスメント及びリスク対応や、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(年に一度開催)において、業務外利用の禁止等について徹底する。 ・デジタル庁は特定個人情報の取扱いは行わないが、mdoc発行管理システムの運用保守管理者として、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(年に一度開催)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		デジタル庁がmdoc発行管理システムの運用保守管理者として、以下の管理を実施する。 ・監視・保守を行う区画については、電子的に扉の開閉が可能な鍵を備え生体認証を用いる。また、相互牽制として二人一組で入退する。ICカードによる入退室の記録を取得し、加えて監視カメラによるセキュリティ対策を実施し、入退室者及び作業の過程を映像として記録する。 ・情報の持込・持出に際して、運用保守管理者は、作業実施者から作業申請書を、作業内容を確認の上、受け付ける。 ・媒体への出力に際しては、不正な複製、持ち出し等を防止するために、区画への持ち込みが許可された専用の外部記録媒体を使用する。また、媒体管理簿等にて、使用の記録を記載する等、利用履歴を残し、当該管理簿に対する定期的な監査も行い、不正な媒体利用がないか、許可されていない情報の持ち出しがないかを確認する。 ・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。	
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			
—			

「 」委託しない

情報保護管理体制の確認	・機構、デジタル庁、当該システムの運用保守事業者（デジタル庁と委託契約書を締結）の三者の関係を規定した「mdoc発行管理システムの利用にあたっての確認事項」に同意することにより、当該規約に基づき、mdoc発行管理システムに係る特定個人情報の取扱いを機構（委託元）から当該システムの運用保守事業者（委託先）に委託することとする。なお、次の内容については、当該確認事項に規定されている。 ・ 特定個人情報ファイルの閲覧者・更新者の制限 ・ 特定個人情報ファイルの取扱いの記録 ・ 特定個人情報の提供ルール/消去ルール ・ 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 ・ 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
--------------------	---

[制限している]	<選択肢> 1) 制限している	2) 制限していない
------------	--------------------	------------

委託先において、電子計算機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。

[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

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。

[定めている] ＜選択肢＞
1) 定めている 2) 定めていない

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。

特定個人情報の提供が発生する際、委託先は、使用目的及び情報の内容を記載した申請書を使用し、それを当機構職員が確認する。

また、委託先は授受記録について、媒体、利用期限、返却方法を記載した台帳を作成する。

委託元となる機構は、特定個人情報等の管理状況に関する報告により遵守状況を確認をする。

委託元となる機構は、委託契約書の報告条項に基づき、四半期に一度、特定個人情報の取扱いについて書面にて報告を受ける。

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。

[定めている] ＜選択肢＞
1) 定めている 2) 定めていない

委託契約上、以下の措置をとる旨を規定する。

- ・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を外部業者に溶解処理を行う。
- ・データが紙かを問わず、廃棄の際は廃棄履歴を作成し保存する。
- ・特定個人情報と同様、保管期間の過ぎたバックアップデータを、システムにて自動判別し消去する。
- ・委託契約終了時に他システムとの間に敷設する回線は切断し、特定個人情報を全て消去する。
- ・委託元から受けた提供情報は、受託業務完了時に全て返却又は消去する。

委託契約の報告条項に基づき、四半期に一度、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			
規定の内容		・目的外利用を禁止する。 ・特定個人情報の閲覧者・更新者を制限する。 ・特定個人情報の提供先を限定する。 ・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データを完全に消去する。 ・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			
具体的な方法		原則として再委託は行わないこととするが、再委託を行う場合は、以下の措置を取ることとする。 ・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。 ・委託先に対して、特定個人情報にアクセスできる再委託先従事者の名簿作成を義務付ける。 ・本番環境での操作作業は必ず2名1組で実施し、作業手順は委託先側でチェックを行う。 ・委託先において、再委託先従事者による特定個人情報への不要なアクセスがないか確認できるように作業時のログを収集・保管する。 ・再委託事業者に、本委託事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、所管省庁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			
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	[]	<選択肢> 1) 記録を残している	2) 記録を残していない
具体的な方法			
特定個人情報の提供・移転に関するルール	[]	<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			
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
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			
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： 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			
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 3) 課題が残されている	2) 十分である
リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク5： 不正な提供が行われるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク6： 不適切な方法で提供されるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
リスク7： 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置			

7. 特定個人情報の保管・消去		
リスク1: 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[十分に遵守している]	<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	<ガバメントクラウドにおける措置> ①ガバメントクラウドについては政府情報システムのセキュリティ制度 (ISMAP) のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。 ②事前に許可されていない装置等に関しては、外部に持出できないこととしている。
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	<mdoc発行管理システムにおける措置> ・事前に許可された者以外が、特定個人情報にアクセスできないよう、物理的区画による制限やユーザー権限による制限により制御している。 ・個人情報が含まれる領域／環境 (本番環境) はインターネットからアクセスできないよう制御している。 <ガバメントクラウドにおける措置> ①クラウド事業者は利用者のデータにアクセスしない契約等となっている。 ②mdoc発行管理システムに係る特定個人情報の取扱いを受託している運用保守事業者は、ガバメントクラウドが提供するマネージドサービスにより、ネットワークアクティビティ、データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに、ログ管理を行う。 ③クラウド事業者は、ガバメントクラウドに対するセキュリティの脅威に対し、脅威検出やDDos対策を24時間365日講じる。 ④クラウド事業者は、ガバメントクラウドに対し、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ⑤mdoc発行管理システムに係る特定個人情報の取扱いを受託している運用保守事業者は、導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ⑥mdoc発行管理システムが保有しているデータは、クラウド事業者がアクセスできないよう制御を講じる。
⑦バックアップ	[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
⑧事故発生時手順の策定・周知	[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	[発生なし]	<選択肢> 1) 発生あり 2) 発生なし
	その内容	—
	再発防止策の内容	—

⑩死者の個人番号	[保管している]	<選択肢> 1) 保管している 2) 保管していない
具体的な保管方法	・生存者の個人番号と死者の個人番号を区別しないため、生存者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	<mdoc発行管理システムにおける措置> 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、公的個人認証サービスシステムから当該住民の異動情報がmdoc発行管理システムに連携される。 mdoc発行管理システムでは、異動情報をもとに、当該住民のカード代替電磁的記録を失効させ、一定期間保管した後、カード代替電磁的記録用管理ファイルから消去する。	
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	<mdoc発行管理システムにおける措置> ・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データを消去する。消去の際は消去履歴を作成し保存する。 ・USBメモリ等の電子記録媒体に保存された特定個人情報は、保存された情報が復元できないように完全に消去する。 ・紙媒体に記載された特定個人情報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は復元ができないようにシュレッダー等を用いたうえで廃棄する。 ・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。 <ガバメントクラウドにおける措置> データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去する。	
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	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にしていない
具体的なチェック方法	NISC政府機関統一基準群への準拠性の確認のため、全部門を対象に自己点検を実施している。特に、住基全国センターにおいては、NISC政府機関統一基準群、本人確認情報管理規程等に規定され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（年に一度）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。また、個人番号センター運用管理本部個人番号カード業務運用部、個人番号センター個人番号カードシステム開発部、個人番号センター運用管理本部個人番号カードシステム運用部及びコンタクトセンターにおいては、NISC政府機関統一基準群、機構処理事務管理規程等に規定され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（年に一度）に職員による自己点検項目の遵守状況の確認を実施する。	
②監査	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にしていない
具体的な内容	本人確認情報の管理方法及び特定個人情報の管理方法等について、毎年度、地方公共団体情報システム機構本人確認情報管理規程及び地方公共団体情報システム機構機構処理事務管理規程に基づき、内部監査及び第三者機関による外部監査等を実施している。また、外部監査等で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	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にしていない
具体的な方法	入職時の導入研修として集合研修等により実施している。また、年に1回以上、全職員を対象に、集合研修又はeラーニング等による研修を実施している。また、個人情報保護のための活動として、各部門の個人情報の種類及び取扱いを取りまとめたマニュアルを整備し、各部門の業務運営における個人情報の適切な取扱いについて周知徹底を図っている。またこれに加え、各部門において、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等により、本人確認情報の管理方法及び特定個人情報の管理方法を定めた規程の概要について説明し、周知徹底を図っている。特に、集合研修については複数回開催することで、関係する全職員が受講するよう努めている。このほか、毎年度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		
・理事長を委員長とした内部統制委員会等を開催し、個人情報保護、情報セキュリティ管理及び危機管理など、リスク管理に係る諸活動の実施計画及び実施状況について審議することにより、リスク管理活動の運用・改善を図っている。 緊急時対応訓練の実施、インシデント報告会（毎月、全常勤役員参加）の開催等により、危機管理態勢の着実な運用と改善を図っている。 ・特定個人情報をはじめとする個人情報等が漏えいした場合の対策として、業務継続計画及び緊急時対応計画等に基づき、緊急体制により次の事項について必要な措置を講ずる。 (1) 機構内部における報告、被害の拡大防止 責任ある立場の者に直ちに報告するとともに、被害の拡大を防止する。 (2) 事実関係の調査、原因の究明 事実関係を調査し、その原因の究明を行う。 (3) 影響範囲の特定 (2)で把握した事実関係による影響の範囲を特定する。 (4) 再発防止策の検討・実施 (2)で究明した原因を踏まえ、再発防止策を検討し、速やかに実施する。 (5) 影響を受ける可能性のある本人への連絡及び関係する機関等へ連絡等 事案の内容等に応じて、二次被害の防止、類似事案の発生回避等の観点から、事実関係等について、速やかに、本人へ連絡し、又は本人が容易に知り得る状態に置く。また、個人情報保護委員会、総務省等の関係する国の行政組織及び地方公共団体等に報告する。 (6) 事実関係、再発防止策等の公表 事案の内容等に応じて、二次被害の防止、類似事案の発生回避等の観点から、事実関係及び再発防止策等について、速やかに公表する。 ・特定個人情報を取り扱うシステムの調達・構築・運用等に当たっては、サプライチェーンリスクの管理に努める。 ・カード代替電磁的記録が格納されたスマートフォンの紛失・盗難等の発生に備え、委託事業者（コールセンター事務）又はオンライン申告による、速やかにカード代替電磁的記録を一時的に停止するための手続を設けており、また、当該手続の内容について周知をしている。 ・利用者が行政機関や民間事業者等が提供するサービスを利用するためにスマートフォンからカード代替電磁的記録を送信する場合、利用者本人の生体認証等を利用するため、第三者のなりすましは不可となっている。		

V 開示請求、問合せ

1. 特定個人情報の開示・訂正・利用停止請求	
①請求先	郵便番号102-8419 東京都千代田区一番町25番地 全国町村議会会館7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)
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/kaijiseikyusyo.pdf https://www.j-lis.go.jp/data/open/cnt/3/235/1/teiseishinsei.pdf)
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	・問合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合せについて、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	令和7年1月16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
②実施日・期間	令和6年12月9日から令和7年1月8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	寄せられた意見はなし。
⑤評価書への反映	—
3. 第三者点検	
①実施日	—
②方法	—
③結果	—
4. 個人情報保護委員会の承認【行政機関等のみ】	
①提出日	令和7年1月16日
②個人情報保護委員会による審査	(1) 住民基本台帳ネットワーク及び番号制度関連事務の内容、特定個人情報ファイルの内容、特定個人情報の流れ並びにリスク及びリスク対策が具体的に記載されており、特段の問題は認められないと考えられるが、特定個人情報保護評価書に記載されているとおり確実に実行する必要がある。 (2) 特定個人情報のインターネットへの流出を防止する対策については、インターネットを通じて外部に特定個人情報が漏えいしないよう、ISMAPのリストに登録されたクラウドサービスから調達したガバメントクラウドにmdoc発行管理システムを構築し、セキュリティ管理策が適切に実施されていること等が記載されているが、特定個人情報保護評価書に記載されているとおり確実に実行する必要がある。 (3) 組織的及び人的安全管理措置については、適切な組織体制の整備、職員への必要な教育・研修、実効性のある自己点検・監査等を実施し、実務に即して適切に運用・見直しを行うことが重要である。 (4) 委託先事業者による特定個人情報ファイルの適正な取扱いを確保するとともに、クラウドサービスに係る安全管理措置も含め、情報漏えい等に対するリスク対策全般について、特定個人情報保護評価書に記載されているとおり確実に実行する必要がある。 (5) 上記について、不断の見直し・検討を行うことに加え、事務フローの変更や新たなリスク対策が生ずることとなった場合は、必要に応じて評価の再実施を行うことが重要である。

(別添3) 変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
平成27年1月29日	表紙 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。 ・外部との接続に当たっては、専用回線の利用、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。	・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、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規定による通知カード及び個人番号カード並びに情報提供ネットワークシステムによる特定個人情報の提供等に関する省令に基づき、市町村長（特別区の区長を含む。以下同じ。）から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。 ・外部との接続に当たっては、専用回線の利用、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。	事後	特定個人情報保護評価指針（平成26年4月20日特定個人情報保護委員会）に定める重要な変更にあたらないため。
平成27年1月29日	Ⅰ－1 ②事務の内容	・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） （略） ・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） （略） ・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。 （略）	細は、「（別添1）事務の内容」を参照） （略） ・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）事務の内容」を参照） （略） ・3. 個人番号カードに係る事務（※詳細は、「（別添1）事務の内容」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規定による通知カード及び個人番号カード並びに情報提供ネットワークシステムによる特定個人情報の提供等に関する省令（平成26年11月20日総務省令第85号）（以下「通知カード及び個人番号カード省令」という。）第35条（通知カード・個人番号カード関連事務の委任）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。 （略）	事後	特定個人情報保護評価指針（平成26年4月20日特定個人情報保護委員会）に定める重要な変更にあたらないため。
平成27年1月29日	（別添1）事務の内容 イラスト内のコメント	・住民基本台帳法に基づく本人確認情報提供・法令に基づく市町村長からの委任を受け通知カード及び個人番号カード発行	・住基法に基づく本人確認情報提供 ・通知カード及び個人番号カード省令に基づく市町村長からの委任を受け通知カード及び個人番号カード発行	事後	特定個人情報保護評価指針（平成26年4月20日特定個人情報保護委員会）に定める重要な変更にあたらないため。
平成27年1月29日	Ⅱファイルの概要（2） 機構保存本人確認情報ファイル Ⅱ－6 ②保存期間 その他妥当性	（2ポツ目） ・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。	（2ポツ目） ・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7（機構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。	事後	特定個人情報保護評価指針（平成26年4月20日特定個人情報保護委員会）に定める重要な変更にあたらないため。
平成27年1月29日	Ⅱファイルの概要（3） 個人番号カード用管理ファイル Ⅱ－2 基本情報 ③対象となる本人の範囲 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ため。 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ため。 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。	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ため。 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ため。 機構は、これらの事務を通知カード及び個人番号カード省令第35条（通知カード・個人番号カード関連事務の委任）に基づき、市町村長から委任を受けて実施する。	事後	特定個人情報保護評価指針（平成26年4月20日特定個人情報保護委員会）に定める重要な変更にあたらないため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
平成27年1月29日	II ファイルの概要 (3) 個人番号カード用管理ファイル II-3 特定個人情報の入手・使用 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。	機構が送付先情報及び交付申請書を入手することについて、通知カード及び個人番号カード省令第35条(通知カード・個人番号カード関連事務の委任)、第36条(通知カード・個人番号カード関連事務に係る通知)に明示されている。	事後	特定個人情報保護評価指針(平成26年4月20日特定個人情報保護委員会)に定める重要な変更にあたらないため。
平成27年1月29日	II ファイルの概要 (3) 個人番号カード用管理ファイル II-3 特定個人情報の入手・使用 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。	通知カード及び個人番号カード省令第35条(通知カード・個人番号カード関連事務の委任)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。	事後	特定個人情報保護評価指針(平成26年4月20日特定個人情報保護委員会)に定める重要な変更にあたらないため。
平成27年1月29日	II ファイルの概要 (3) 個人番号カード用管理ファイル II-5 提供先1 ①法令上の根拠	総務省令に記載予定	通知カード及び個人番号カード省令第36条第3項(通知カード・個人番号カード関連事務に係る通知)	事後	特定個人情報保護評価指針(平成26年4月20日特定個人情報保護委員会)に定める重要な変更にあたらないため。
平成27年4月30日	II ファイルの概要 (3) 個人番号カード用管理ファイル II-4 委託事項1 ⑥委託先名	未定	・独立行政法人国立印刷局(印刷・送付事務) ・株式会社エヌ・ティ・ティ・データ、株式会社DNPデータテクノ、凸版印刷株式会社(申請受付事務及びカード発行事務)	事後	特定個人情報保護評価指針(平成26年4月20日特定個人情報保護委員会)に定める重要な変更にあたらないため。
平成27年4月30日	II ファイルの概要 (3) 個人番号カード用管理ファイル II-4 委託事項2 ⑥委託先名	未定	株式会社ベルシステム24	事後	特定個人情報保護評価指針(平成26年4月20日特定個人情報保護委員会)に定める重要な変更にあたらないため。
平成28年4月1日	I-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	①部署:住民基本台帳ネットワークシステム全国センター ②所属長:センター長 米田 順彦	事後	特定個人情報保護評価指針(平成28年1月1日個人情報保護委員会)に定める重要な変更にあたらないため。
平成29年3月31日	I-7 評価実施機関における担当部署 ②所属長	センター長 米田 順彦	センター長 加松 正利	事後	特定個人情報保護評価指針(平成28年1月1日個人情報保護委員会)に定める重要な変更にあたらないため。
平成29年3月31日	II-2 ③対象となる本人の範囲 その必要性 II-3 ④入手に係る妥当性	番号法第7条第2項(指定及び通知)	番号法第7条第1項(指定及び通知)	事後	特定個人情報保護評価指針(平成28年1月1日個人情報保護委員会)に定める重要な変更にあたらないため。
平成29年3月31日	III-2 リスク1 対象者以外の情報の入手を防止するための措置の内容	(前略) なお、国民にとって利便性の高い交付申請方法(後略)	(前略) なお、住民にとって利便性の高い交付申請方法(後略)	事後	特定個人情報保護評価指針(平成28年1月1日個人情報保護委員会)に定める重要な変更にあたらないため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
平成29年3月31日	III-2 リスク1 その他の措置の内容	(前略) 市町村における個人番号カード交付時に厳格な審査を行っていただくことが前提となる。 (後略)	(前略) 市町村における個人番号カード交付時等に厳格な審査を行っていただくことが前提となる。 (後略)	事後	特定個人情報保護評価指針(平成28年1月1日個人情報保護委員会)に定める重要な変更にあたらないため。
平成30年3月30日	I-7 評価実施機関における担当部署 ①部署	住民基本台帳ネットワークシステム全国センター	(1)地方公共団体情報システム機構事務局 (2)住民基本台帳ネットワークシステム全国センター (3)個人番号センター	事後	特定個人情報保護評価指針(平成29年5月30日個人情報保護委員会)に定める重要な変更にあたらないため。
平成30年3月30日	I-7 評価実施機関における担当部署 ②所属長	センター長 加松 正利	(1)理事(兼)事務局長事務取扱 山口 英樹 (2)センター長 宮田 昌一 (3)センター長 藤原 通孝	事後	特定個人情報保護評価指針(平成29年5月30日個人情報保護委員会)に定める重要な変更にあたらないため。
平成30年3月30日	(別添1) 事務内容	特定個人情報保護委員会	個人情報保護委員会	事後	特定個人情報保護評価指針(平成29年5月30日個人情報保護委員会)に定める重要な変更にあたらないため。
平成30年3月30日	IIファイルの概要(1) 個人番号管理ファイル II-3 ⑧使用方法 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、個人番号とすべき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。	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。	事後	特定個人情報保護評価指針(平成29年5月30日個人情報保護委員会)に定める重要な変更にあたらないため。
平成30年3月30日	IIファイルの概要(2) 機構保存本人確認情報ファイル II-3 ⑧使用方法 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を確認するため、本人確認情報の更新件数等を集計する。	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。	事後	特定個人情報保護評価指針(平成29年5月30日個人情報保護委員会)に定める重要な変更にあたらないため。
平成30年3月30日	(別添2) ファイル記録項目 (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…(中略)…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. 略号識別情報、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	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…(中略)…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. 略号識別情報、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、117. 通知カード管理状況	事後	特定個人情報保護評価指針(平成29年5月30日個人情報保護委員会)に定める重要な変更にあたらないため。
平成30年3月30日	IIIリスク対策(1) 個人番号管理ファイル III-7 ①NISC政府機関統一基準群	政府機関ではない	十分に遵守している	事後	特定個人情報保護評価指針(平成29年5月30日個人情報保護委員会)に定める重要な変更にあたらないため。
平成30年3月30日	IIIリスク対策(2) 機構保存本人確認情報ファイル III-7 ①NISC政府機関統一基準群	政府機関ではない	十分に遵守している	事後	特定個人情報保護評価指針(平成29年5月30日個人情報保護委員会)に定める重要な変更にあたらないため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
平成30年3月30日	IIIリスク対策(3) 個人番号カード用管理ファイル III-7 ①NISC政府機関統一基準群	政府機関ではない	十分に遵守している	事後	特定個人情報保護評価指針(平成29年5月30日個人情報保護委員会)に定める重要な変更にあたらないため。
平成30年3月30日	V-1 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	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/kaijiseikyusyo.pdf https://www.j-lis.go.jp/data/open/cnt/3/235/1/teiseishinsei.pdf	事後	特定個人情報保護評価指針(平成29年5月30日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	I-1 ②事務の内容	1. 個人番号の生成・通知に係る事務 (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(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)。	1. 個人番号の生成・通知に係る事務 (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(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)。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	I-1 ②事務の内容	1. 個人番号の生成・通知に係る事務 (3)住民票コードの変更 ・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。	1. 個人番号の生成・通知に係る事務 (3)住民票コードの変更 ・住民基本台帳法(昭和42年7月25日法律第81号)(平成30年7月6日法律第71号施行時点)(以下「住基法」という。))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。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	I-1 ②事務の内容	3. 個人番号カードに係る事務 (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規定による通知カード及び個人番号カード並びに情報提供ネットワークシステムによる特定個人情報の提供等に関する省令(平成26年11月20日総務省令第85号)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元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。	3. 個人番号カードに係る事務 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、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規定による通知カード及び個人番号カード並びに情報提供ネットワークシステムによる特定個人情報の提供等に関する省令(平成26年11月20日総務省令第85号)(以下「通知カード及び個人番号カード省令」という。))第35条第1項に基づく委任を受け、通知カード及び個人番号カードに係る以下の事務を行う。 (1)通知カードの印刷・住民への送付 ・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。 (2)個人番号カードの交付申請受付・発行・市町村への送付 ・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元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。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	I-1 ②事務の内容	(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、電子証明書の一時的保留要求を行う。))。 ・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)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、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(あわせて、公的個人認証サービスに対し、電子証明書の一時的保留要求を行う。))を行う業務を委託する。 ・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。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
平成31年3月31日	1-7 ②所属長の役職名	(1)理事(兼)事務局長事務取扱 山口 英樹 (2)センター長 宮田 昌一 (3)センター長 藤原 通孝	(1)理事(兼)事務局長事務取扱 (2)センター長 (3)センター長	事後	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	(別添1) 事務内容 (3) 個人番号カードに係る事務	(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。	(備考) (3)-1.通知カードの印刷・住民への送付 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。	事後	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	(別添1) 事務内容 (3) 個人番号カードに係る事務	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、送付先住所の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 市町村長において、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.個人番号カードの交付申請受付・発行・市町村への送付 2-① 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。 2-② 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。 2-③ 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。 2-④ 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。 2-⑤ 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。 2-⑥ 発行された個人番号カードを、送付先住所の市町村長に対し送付する。 2-⑦ 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。 2-⑧ 市町村長において、個人番号カードを住民に交付する。 ※手書用交付申請書以外の交付申請書には個人番号は記載しない。	事後	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	(別添1) 事務内容 (3) 個人番号カードに係る事務	(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。 (3)-2 委託事業者 (コールセンター事務) は一時停止した旨の情報を市町村長に通知する。	(3)-3.カード管理情報の連携 3-① 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。 3-② 委託事業者 (コールセンター事務) は一時停止した旨の情報を市町村長に通知する。	事後	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
平成31年3月31日	Ⅱファイルの概要(1) 個人番号管理ファイル Ⅱ-2 ⑥事務担当部署	住基全国センター	住民基本台帳ネットワークシステム全国センター	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	Ⅱファイルの概要(1) 個人番号管理ファイル Ⅱ-3 ⑦使用の主体	住基全国センター	住民基本台帳ネットワークシステム全国センター	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	Ⅱファイルの概要(1) 個人番号管理ファイル Ⅱ-5 ⑦時期・頻度	番号法施行日(平成27年10月5日)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。	番号法施行日(平成27年10月5日)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31年3月31日現在))ごとにまとめて提供する。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	Ⅱファイルの概要(2) 機構保存本人確認情報ファイル Ⅱ-2 ⑥事務担当部署	住基全国センター	住民基本台帳ネットワークシステム全国センター	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	Ⅱファイルの概要(2) 機構保存本人確認情報ファイル Ⅱ-3 ④入手に係る妥当性	※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。	※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15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。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	Ⅱファイルの概要(2) 機構保存本人確認情報ファイル Ⅱ-3 ⑦使用の主体	住基全国センター	住民基本台帳ネットワークシステム全国センター	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	Ⅱファイルの概要(2) 機構保存本人確認情報ファイル Ⅱ-3 ⑧使用方法	・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)。	・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取得要求を受け(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)。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	Ⅱファイルの概要(3) 個人番号カード用管理ファイル Ⅱ-2 ③対象となる本人の範囲 その必要性	機構は、これらの事務を通知カード及び個人番号カード省令第35条(通知カード・個人番号カード関連事務の委任)に基づき、市町村長から委任を受けて実施する。	機構は、これらの事務を通知カード及び個人番号カード省令第35条第1項(通知カード・個人番号カード関連事務の委任)に基づき、市町村長から委任を受けて実施する。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	Ⅱファイルの概要(3) 個人番号カード用管理ファイル Ⅱ-2 ⑥事務担当部署	個人番号カード担当部署	個人番号センター個人番号カード部	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	Ⅱファイルの概要(3) 個人番号カード用管理ファイル Ⅱ-3 ③入手の時期・頻度	・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(記入済)より随時入手する。	・本人(紙にて入手) :個人番号カードの交付希望者により送付された交付申請書(記入済)より随時入手する。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
平成31年3月31日	II ファイルの概要 (3) 個人番号カード用管理ファイル II-3 ④ 入手に係る妥当性	・送付先情報 (市町村より入手) ・番号法第7条第1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。 ・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。	・送付先情報 (市町村より入手) ・番号法第7条第1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。 ・交付申請書 (交付申請者本人より入手) ・通知カード及び個人番号カード省令第21条において、交付申請書に記載すべき事項として交付申請者の氏名、住所、個人番号が規定されている。	事後	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める重要な変更にあたらないため。
平成31年3月31日	II ファイルの概要 (3) 個人番号カード用管理ファイル II-3 ⑦ 使用の主体	個人番号カード担当部署	個人番号センター個人番号カード部	事後	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める重要な変更にあたらないため。
平成31年3月31日	II ファイルの概要 (3) 個人番号カード用管理ファイル II-3 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。	・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→個人番号カード管理システム) 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。	事後	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める重要な変更にあたらないため。
平成31年3月31日	II ファイルの概要 (3) 個人番号カード用管理ファイル II-3 ⑧ 使用方法 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。	個人番号カード用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。	事後	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める重要な変更にあたらないため。
平成31年3月31日	II ファイルの概要 (3) 個人番号カード用管理ファイル II-4 委託の有無	2件	3件	事後	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める重要な変更にあたらないため。
平成31年3月31日	II ファイルの概要 (3) 個人番号カード用管理ファイル II-4 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	番号通知書類の印刷に係る事務	事後	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める重要な変更にあたらないため。
平成31年3月31日	II ファイルの概要 (3) 個人番号カード用管理ファイル II-4 委託事項1 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)	・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)	事後	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める重要な変更にあたらないため。
平成31年3月31日	II ファイルの概要 (3) 個人番号カード用管理ファイル II-4 委託事項1 ② 取扱いを委託する特定個人情報ファイルの範囲 その妥当性	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。	番号法第7条第1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。	事後	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める重要な変更にあたらないため。
平成31年3月31日	II ファイルの概要 (3) 個人番号カード用管理ファイル II-4 委託事項1 ③ 委託先における取扱者数	500人以上1,000人未満	10人以上50人未満	事後	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める重要な変更にあたらないため。
平成31年3月31日	II ファイルの概要 (3) 個人番号カード用管理ファイル II-4 委託事項1 ⑥ 委託先名	・独立行政法人国立印刷局 (印刷・送付事務) ・株式会社エヌ・ティ・ティ・データ、株式会社DNPデータテクノ、凸版印刷株式会社 (申請受付事務及びカード発行事務)	・独立行政法人国立印刷局 (印刷・送付事務)	事後	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める重要な変更にあたらないため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
平成31年3月31日	Ⅱファイルの概要(3) 個人番号カード用管理ファイル Ⅱ-4 委託事項1 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	・通知カード及び交付申請書の印刷	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	Ⅱファイルの概要(3) 個人番号カード用管理ファイル Ⅱ-4 委託事項2	コールセンター事務	個人番号カードの交付申請受付・発行・市町村への送付に係る事務	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	Ⅱファイルの概要(3) 個人番号カード用管理ファイル Ⅱ-4 委託事項2 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	・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)	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	Ⅱファイルの概要(3) 個人番号カード用管理ファイル Ⅱ-4 委託事項2 ②取扱いを委託する特定個人情報ファイルの範囲 対象となる本人の範囲 その妥当性	個人番号カードの交付対象者 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。	特定個人情報ファイルの対象者の範囲と同様 番号法第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。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	Ⅱファイルの概要(3) 個人番号カード用管理ファイル Ⅱ-4 委託事項2 ⑥委託先名	株式会社ベルシステム24	・株式会社エヌ・ティ・ティ・データ、株式会社DNPデータテクノ、凸版印刷株式会社(申請受付事務及びカード発行事務)	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	Ⅱファイルの概要(3) 個人番号カード用管理ファイル Ⅱ-4 委託事項2 ⑦再委託の有無	再委託する	再委託しない	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	Ⅱファイルの概要(3) 個人番号カード用管理ファイル Ⅱ-4 委託事項2 ⑧再委託の許諾方法	原則として再委託は行わないこととするが、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を経た後に承認する。	削除	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	Ⅱファイルの概要(3) 個人番号カード用管理ファイル Ⅱ-4 委託事項2 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。	削除	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	Ⅱファイルの概要(3) 個人番号カード用管理ファイル Ⅱ-4 委託事項3		コールセンター事務	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	Ⅱファイルの概要(3) 個人番号カード用管理ファイル Ⅱ-4 委託事項3 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	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
平成31年3月31日	II ファイルの概要 (3) 個人番号カード用管理ファイル II - 4 委託事項3 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	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	II ファイルの概要 (3) 個人番号カード用管理ファイル II - 4 委託事項3 ②取扱いを委託する特定個人情報ファイルの範囲 対象となる本人の数		1,000万人以上	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	II ファイルの概要 (3) 個人番号カード用管理ファイル II - 4 委託事項3 ②取扱いを委託する特定個人情報ファイルの範囲 対象となる本人の範囲		個人番号カードの交付対象者	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	II ファイルの概要 (3) 個人番号カード用管理ファイル II - 4 委託事項3 ②取扱いを委託する特定個人情報ファイルの範囲 その妥当性		個人番号カードの交付対象者	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	II ファイルの概要 (3) 個人番号カード用管理ファイル II - 4 委託事項3 ③委託先における取扱者数		50人以上100人未満	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	II ファイルの概要 (3) 個人番号カード用管理ファイル II - 4 委託事項3 ④委託先への特定個人情報ファイルの提供方法		[○]専用線	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	II ファイルの概要 (3) 個人番号カード用管理ファイル II - 4 委託事項3 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。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	II ファイルの概要 (3) 個人番号カード用管理ファイル II - 4 委託事項3 ⑥委託先名		(株)NTTマーケティングアクト、NTTコミュニケーションズ(株)	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	II ファイルの概要 (3) 個人番号カード用管理ファイル II - 4 委託事項3 ⑦再委託の有無		再委託しない	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
平成31年3月31日	(別添2) 特定個人情報ファイル記録項目	(3) 個人番号カード用管理ファイル 1～67省略 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、117. 通知カード管理状況	(3) 個人番号カード用管理ファイル 1～67省略 68. 顔写真、69. 申請書イメージ、70. 申請年月日、71. 点字有無、72. 点字カナ氏名、項目長、73. 点字カナ氏名、74. 依頼管理番号、75. カードセキュリティ情報区分、76. 処理結果コード、77. 提供元市町村コード、78. 異動事由、79. 異動年月日、80. 予備領域1、81. 予備領域2、82. カード状況区分、83. 公開鍵長、84. 公開鍵、85. 発行委託番号、86. 事業者コード、87. カード発行番号、88. コマンド、89. 有効期限、90. 個人番号カード情報、91. カード運用状況、92. カード有効期限、93. 一時停止日、94. 一時停止理由、95. カード廃止日、96. カード廃止理由、97. カード回収日、98. タイムスタンプ、99. 所管フラグ、100. 転入処理日、101. 転出予定経過日、102. 本人確認情報有無、103. 前住地市町村コード、104. 住基AP識別情報、105. 暗号識別情報、106. カード製造者識別情報、107. カードイメージ番号、108. 被証明者識別子、109. 通知カード管理状況	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	Ⅲリスク対策(1) 個人番号管理ファイル Ⅲー3 リスク1 特定個人情報の使用の記録 具体的方法	本人確認情報の管理について定めた規程に基づき、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。	本人確認情報の管理について定めた規程に基づき、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、規程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。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	Ⅲリスク対策(1) 個人番号管理ファイル Ⅲー5 リスク2 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。	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している。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	Ⅲリスク対策(2) 機構保存本人確認情報ファイル Ⅲー6 リスク6 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提供・移転されることを防止する。	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、不適切な方法での特定個人情報の提供・移転の防止に努める。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	Ⅲリスク対策(3) 個人番号カード用管理ファイル Ⅲー2 リスク1 対象者以外の情報の入手を防止するための措置の内容	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、な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、住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。	②交付申請書 : 交付申請書は一通につき一人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、手書用交付申請書以外の交付申請書には個人番号は記入させないことにより、必要な者以外の特定個人情報の入手を防止し、手書用交付申請書に仮に誤った個人番号が記載されて申請された場合であっても、他の情報との突合により検知し、誤った個人番号カードが発行されることを防止している。 なお、住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。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
平成31年3月31日	IIIリスク対策(3) 個人番号カード用管理ファイル III-2 リスク2 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。	・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。 ・交付申請書は「個人番号カード交付申請書」と明示し、個人番号の記入欄を明確にするなど交付申請者(入手元)への配慮を行っている。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	IIIリスク対策(3) 個人番号カード用管理ファイル III-2 リスク3 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。	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し、③本人確認情報は住基全国サーバからシステムを通じて受領するため、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。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	IIIリスク対策(3) 個人番号カード用管理ファイル III-2 リスク3 個人番号の真正性確認の措置の内容	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(記入済)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。	②交付申請書 :手書用交付申請書に記載された4情報等を個人番号カード管理システムにおいて突合することにより個人番号の真正性を担保する。 ※手書用交付申請書以外の交付申請書には個人番号は記載させない。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	IIIリスク対策(3) 個人番号カード用管理ファイル III-2 リスク3 特定個人情報の正確性確保の措置の内容	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。	②交付申請書 :手書用交付申請書は交付申請者が任意で記載するものであるため記載内容の正確性は交付申請者に委ねられる。 ※手書用交付申請書以外の交付申請書には個人番号は記載させない。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	IIIリスク対策(3) 個人番号カード用管理ファイル III-3 リスク1 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。	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、④国立印刷局に限られるよう、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①～④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。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
平成31年3月31日	IIIリスク対策(3) 個人番号カード用管理ファイル III-3 リスク1 事務で使用するその他のシステムにおける措置の内容	(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 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 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。	(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 ②個人番号カード申請受付・発行システム :個人番号カード発行情報等を提供する場合、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。 ④国立印刷局 :通知カード発行情報等を提供する場合。 (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 ②個人番号カード申請受付・発行システム :個人番号カードの発行結果等を受信する場合。 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。 ④国立印刷局 :通知カード発行結果等を受信する場合。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	IIIリスク対策(3) 個人番号カード用管理ファイル III-3 リスク2 アクセス権限の発効・失効の管理 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。	特定個人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。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	IIIリスク対策(3) 個人番号カード用管理ファイル III-3 リスク2 アクセス権限の管理 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程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については半期ごと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又は削除する。	アクセス権限の管理は、特定個人情報の管理について定めた規程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については半期ごと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又は削除する。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	IIIリスク対策(3) 個人番号カード用管理ファイル III-3 リスク2 特定個人情報の使用の記録 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、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。	特定個人情報の管理について定めた規程に基づき、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。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	IIIリスク対策(3) 個人番号カード用管理ファイル III-3 リスク3 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(年に一度実施を義務付け。)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(年に一度開催)において、業務外利用の禁止等について徹底する。	・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リスクアセスメント及びリスク対応や、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(年に一度開催)において、業務外利用の禁止等について徹底する。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
平成31年3月31日	Ⅲリスク対策(3) 個人番号カード用管理ファイル Ⅲー4 情報保護管理体制の確認	(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 (2)コールセンター事務	(1)番号通知書類の印刷に係る事務 (2)個人番号カードの交付申請受付・発行・市町村への送付に係る事務 (3)コールセンター事務	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
平成31年3月31日	Ⅲリスク対策(3) 個人番号カード用管理ファイル Ⅲー4 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。	・通知カード及び交付申請書の差出前に外観検査・員数検査・重量検査・厚み検査を実施することを委託契約の仕様書に定める等の現行措置に加え、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随時検討する。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。

(別添3) 変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
平成31年3月31日	IIIリスク対策(3) 個人番号カード用管理ファイル III-7 リスク1 ⑥技術的対策 具体的な対策の内容	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。	特定個人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。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更に当たらないため。
平成31年3月31日	IVリスク対策(その他) IV-1 ①自己点検 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(年に一度実施)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。	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(年に一度)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。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更に当たらないため。
平成31年3月31日	IVリスク対策(その他) IV-1 ②監査 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。	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、内部監査及び第三者機関による外部監査を実施している。 また、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。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更に当たらないため。
平成31年3月31日	IVリスク対策(その他) IV-2 従事者に対する教育・啓発 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。	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、毎年度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。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更に当たらないため。
平成31年3月31日	V開示請求、問合せ V-1 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	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7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	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更に当たらないため。
令和1年7月23日	I-1 ②事務の内容	2. 本人確認情報の提供及び保存等に係る事務 (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。	2. 本人確認情報の提供及び保存等に係る事務 (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。 ※本人確認情報の利用(個人番号カード管理システムへの本人確認情報の提供) 個人番号カードの交付申請後に機構保存本人確認情報をもってカードの発行に用いられる送付先情報が最新かどうかを比較・突合し、古い住所や氏名でカードが発行され住民へ交付されるリスクを低減させる。 交付後のタイミングにおいても、申請から交付までの間の異動情報を個人番号カードの一時停止時の本人確認に用いられる利用者情報に反映させることにより、交付後直ちに異動後の最新の住所等で一時停止業務を行えるようにするため、個人番号カード管理システムから照会要求を受け(個人番号カード管理システム→住基全国サーバ)、住民票コード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(住基全国サーバ→個人番号カード管理システム)。	事後	リスクの軽減につながる変更であることから、特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更に当たらないため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和1年7月23日	Ⅰ-2 システム2 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。	〔「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。 ・個人番号カード管理システムから利用者情報の照会要求を受け、該当する個人の本人確認情報を照会元へ提供する。 ※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。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更に応じないため。
令和1年7月23日	Ⅰ-4 ①事務実施上の必要性	(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。	(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。 ⑤ 個人番号カードの交付申請時に個人番号カード管理システムが保持する送付先情報と住基全国サーバが保持する本人確認情報が一致しているかを確認し、また個人番号カードの一時停止業務を最新の情報に基づき実施するため、個人番号カード管理システムから利用者情報の照会要求を受け、該当する個人の本人確認情報を提供する。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更に応じないため。
令和1年7月23日	(別添1) 事務の内容 (1) 個人番号の生成・通知に係る事務 図中の表記		(注) 図中に※が付されている箇所は、特定個人情報を含まない事務の流れを指す。 (図中に※を追記)	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更に応じないため。
令和1年7月23日	(別添1) 事務の内容 (1) 個人番号の生成・通知に係る事務	(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。	(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(※特定個人情報を含まない)。 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。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更に応じないため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和1年7月23日	(別添1) 事務の内容 (1) 個人番号の生成・通知に係る事務	(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。	(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(※特定個人情報を含まない)。 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(※特定個人情報を含まない)。 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。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にとらならないため。
令和1年7月23日	(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事務 図中の表記		(注) 図中に※が付されている箇所は、特定個人情報を含まない事務の流れを指す。 (図中に※を追記)	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にとらならないため。
令和1年7月23日	(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事務	(備考) (2)-1.本人確認情報の更新 1-① 市町村長において、住民より、住民異動に関する届出を受け付ける。 1-② 市町村長において、異動情報を既存住基システムに登録する(更新を含む)。 1-③ 市町村長において、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信したデータを元に、「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。	(備考) (2)-1.本人確認情報の更新 1-① 市町村長において、住民より、住民異動に関する届出を受け付ける(※特定個人情報を含まない)。 1-② 市町村長において、異動情報を既存住基システムに登録する(更新を含む)。 1-③ 市町村長において、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信したデータを元に、「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(※特定個人情報を含まない)。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にとらならないため。
令和1年7月23日	(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事務	(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。 ※本人確認情報整合事務について、正確性確保のため、補完的に以下の事務を行う。 令和元年8月(予定)以降、試行運用を実施し、試行運用の結果を受けて、本番運用へ移行する。 ① 機構において、市町村毎に当該市町村の転出漏れ等、不整合の可能性がある住民の情報を「機構保存本人確認情報ファイル」から抽出する(特定個人情報を含まない)。 ② 機構において抽出した結果を確認し、必要なデータのみ抜粋し、市町村に送付する(特定個人情報を含まない)。 ③ ②のデータに基づき、市町村において当該データについて修正の必要があるか調査を実施し、必要な場合には修正する(修正する際の流れは(2)-1.本人確認情報の更新の1-②～1-⑤の流れと同様)。	(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(※特定個人情報を含まない)。 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。 ※本人確認情報整合事務について、正確性確保のため、補完的に以下の事務を行う。 令和元年8月(予定)以降、試行運用を実施し、試行運用の結果を受けて、本番運用へ移行する。 ① 機構において、市町村毎に当該市町村の転出漏れ等、不整合の可能性がある住民の情報を「機構保存本人確認情報ファイル」から抽出する(特定個人情報を含まない)。 ② 機構において抽出した結果を確認し、必要なデータのみ抜粋し、市町村に送付する(特定個人情報を含まない)。 ③ ②のデータに基づき、市町村において当該データについて修正の必要があるか調査を実施し、必要な場合には修正する(修正する際の流れは(2)-1.本人確認情報の更新の1-②～1-⑤の流れと同様)。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にとらならないため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和1年7月23日	(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事務		(2)-6.本人確認情報の利用 6-① 個人番号カードの交付申請後及び交付後に個人番号カード管理システムより、住民票コードをキーとした利用者情報の照会を受ける(※特定個人情報を含まない)。 6-② 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、個人番号カード管理システムへ提供する。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
令和1年7月23日	(別添1) 事務の内容 (3) 個人番号カードに係る事務 図中の表記	2-④カード発行委託 2-⑤カード発行 2-⑥送付 2-⑦連携 2-⑧交付	2-④、⑩利用者情報照会・結果 2-⑤カード発行委託 2-⑥カード発行 2-⑦送付 2-⑧連携 2-⑨交付	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
令和1年7月23日	(別添1) 事務の内容 (3) 個人番号カードに係る事務 図中の表記		(注) 図中に※が付されている箇所は、特定個人情報を含まない事務の流れを指す。 (図中に※を追記)	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
令和1年7月23日	(別添1) 事務の内容 (3) 個人番号カードに係る事務	(備考) (3)-2.個人番号カードの交付申請受付・発行・市町村への送付 2-① 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。 2-② 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。 2-③ 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。 2-④ 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。 2-⑤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。 2-⑥ 発行された個人番号カードを、送付先住所地の市町村長に対し送付する。 2-⑦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。 2-⑧市町村長において、個人番号カードを住民に交付する。 ※手書用交付申請書以外の交付申請書には個人番号は記載しない。	(備考) (3)-2.個人番号カードの交付申請受付・発行・市町村への送付 2-① 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。 2-② 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。 2-③ 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。 2-④ 個人番号カードの交付申請後に住基全国サーバへ住民票コードをキーとした利用者情報の照会を行い(※特定個人情報を含まない)、住基全国サーバより該当する個人の本人確認情報の提供を受ける。 2-⑤ 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。 2-⑥ 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。 2-⑦ 発行された個人番号カードを、送付先住所地の市町村長に対し送付する。 2-⑧ 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。 2-⑨ 市町村長において、個人番号カードを住民に交付する。 2-⑩ 個人番号カードの交付後に住基全国サーバへ住民票コードをキーとした利用者情報の照会を行い(※特定個人情報を含まない)、住基全国サーバより該当する個人の本人確認情報の提供を受ける。 ※手書用交付申請書以外の交付申請書には個人番号は記載しない。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
令和1年7月23日	(別添1) 事務の内容 (3) 個人番号カードに係る事務	(3)-3.カード管理情報の連携 3-① 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。 3-② 委託事業者(コールセンター事務)は一時停止した旨の情報を市町村長に通知する。	(3)-3.カード管理情報の連携 3-① 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。 3-② 委託事業者(コールセンター事務)は一時停止した旨の情報を市町村長に通知する(※特定個人情報を含まない)。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和1年7月23日	II ファイルの概要 (2) 機構保存本人確認情報ファイル II-3 ⑧使用方法	・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取得要求を受け(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ファイルから抽出し、書面により提供する(住基全国サーバ→帳票出力→住民)。	・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取得要求を受け(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)。 ・個人番号カード管理システムから利用者情報の照会要求を受け(個人番号カード管理システム→住基全国サーバ)、照会のあった住民票コード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(住基全国サーバ→個人番号カード管理システム)。 ・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ファイルから抽出し、書面により提供する(住基全国サーバ→帳票出力→住民)。	事後	リスクの軽減につながる変更であることから、特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
令和1年7月23日	(別添2) 特定個人情報ファイル記録項目	(2) 機構保存本人確認情報ファイル ・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…(中略)…、28. 提供事務区分、29. 個人番号提供事務区分、30. 提供元、31. 提供先	(2) 機構保存本人確認情報ファイル ・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…(中略)…、28. 提供事務区分、29. 個人番号提供事務区分、30. 提供元、31. 提供先、32. 旧氏 漢字、33. 旧氏 外字数、34. 旧氏 ふりがな、35. 旧氏 外字変更連番	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
令和1年7月23日	(別添2) 特定個人情報ファイル記録項目	(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…(中略)…、106. カード製造者識別情報、107. カードイメージ番号、108. 被証明者識別子、109. 通知カード管理状況	(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…(中略)…、106. カード製造者識別情報、107. カードイメージ番号、108. 被証明者識別子、109. 通知カード管理状況、110. 旧氏漢字、111. 旧氏 外字数、112. 旧氏 ふりがな、113. 旧氏 外字変更連番、114. ローマ字 氏名、115. ローマ字 旧氏	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
令和1年7月23日	IIIリスク対策 (1) 個人番号管理ファイル III-3 リスク3 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(年に一度実施を義務付け。)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(年に一度開催)において、業務外利用の禁止等について徹底する。	・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リスクアセスメント及びリスク対応や、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(年に一度開催)において、業務外利用の禁止等について徹底する。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
令和1年7月23日	IIIリスク対策 (2) 機構保存本人確認情報ファイル III-3 リスク1 事務で使用するその他のシステムにおける措置の内容	(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個人番号生成システム :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。	(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。 :個人番号カード管理システムからの利用者情報照会要求に対して利用者情報照会結果を提供する場合。 (2) 他のシステム⇒住基全国サーバへのアクセス ①個人番号生成システム :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 :利用者情報照会要求を行う場合、ただし、住民票コードのみをキーとし、特定個人情報を使ったアクセスは行わない。	事後	リスクの軽減につながる変更であることから、特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
令和1年7月23日	IIIリスク対策 (2) 機構保存本人確認情報ファイル III-3 リスク3 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(年に一度実施を義務付け。)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(年に一度開催)において、業務外利用の禁止等について徹底する。	・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リスクアセスメント及びリスク対応や、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(年に一度開催)において、業務外利用の禁止等について徹底する。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和1年7月23日	IIIリスク対策 (3) 個人番号カード用管理ファイル III-3 リスク1 事務で使用するその他のシステムにおける措置の内容	(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。 ②～④ (略) (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。 ②～④ (略)	(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 : 利用者情報照会を行う場合。ただし、住民票コードのみをキーとし、特定個人情報を使ったアクセスは行わない。 (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 個人番号カード管理システムからの利用者情報照会に基づき、本人確認情報を連携する場合。	事後	リスクの軽減につながる変更であることから、特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める重要な変更にあたらないため。
令和1年7月23日	IIIリスク対策 (3) 個人番号カード用管理ファイル III-7 リスク1 ⑥技術的対策 具体的な対策の内容	・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。	・不正アクセス対策 : 特定個人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。	事後	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める重要な変更にあたらないため。
令和1年8月23日	II ファイルの概要 (1) 個人番号管理ファイル II-3 ①入手元	[] 地方公共団体・地方独立行政法人	[○] 地方公共団体・地方独立行政法人	事前	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める特定個人情報保護評価の再実施のため。
令和1年8月23日	II ファイルの概要 (1) 個人番号管理ファイル II-3 ①入手元	[○] 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。)	[○] その他 (個人番号生成時は、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。個人番号の変更時は、市町村長から住基全国サーバを経由して、住民票コード及び個人番号 (変更前) を入手し、個人番号 (変更後) 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。)	事前	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める特定個人情報保護評価の再実施のため。
令和1年8月23日	II ファイルの概要 (1) 個人番号管理ファイル II-6 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。	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。 サーバのバックアップを記録した電子記録媒体 (バックアップ媒体) についても、セキュリティゲートにて入退室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 (データ保管室) に設置した施設可能な場所に保管する。 ※ 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部屋に入退室する者が権限を有すること及び作業に不要な機器等を持ち込まないことを確認する等の管理を行う。	事前	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める特定個人情報保護評価の再実施のため。
令和1年8月23日	II ファイルの概要 (1) 個人番号管理ファイル II-6 ③消去方法	・上記理由から消去しない。	・上記理由からサーバ内に保管された個人番号管理ファイルに記録されたデータは消去しない。 ・バックアップ媒体は複数世代保管し、古いものから上書きする。 ・バックアップ媒体を廃棄する場合は、データが復元できないよう処理を行った上で、廃棄する。併せて、廃棄履歴を作成し、保存する。	事前	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める特定個人情報保護評価の再実施のため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和1年8月23日	II ファイルの概要 (2) 機構保存本人確認情報ファイル II-6 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。	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。 サーバのバックアップを記録した電子記録媒体 (バックアップ媒体) についても、セキュリティゲートにて入退室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 (データ保管室) に設置した施設可能な場所に保管する。 ※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部屋に入退室する者が権限を有すること及び作業に不要な機器等を持ち込まないことを確認する等の管理を行う。	事前	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める特定個人情報保護評価の再実施のため。
令和1年8月23日	II ファイルの概要 (2) 機構保存本人確認情報ファイル II-6 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。	・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。 ・バックアップ媒体は複数世代保管し、古いものから上書きする。 ・バックアップ媒体を廃棄する場合は、データが復元できないよう処理を行った上で、廃棄する。併せて、廃棄履歴を作成し、保存する。	事前	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める特定個人情報保護評価の再実施のため。
令和1年8月23日	II ファイルの概要 (3) 個人番号カード用管理ファイル II-6 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。	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。 サーバのバックアップを記録した電子記録媒体 (バックアップ媒体) 及び市町村合併等に伴う大量の送付先情報更新時に使用する電子記録媒体についても、セキュリティゲートにて入退室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) に設置した施設可能な場所に保管する。 ※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及び作業に不要な機器等を持ち込まないことを確認する等の管理を行う。	事前	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める特定個人情報保護評価の再実施のため。
令和1年8月23日	II ファイルの概要 (3) 個人番号カード用管理ファイル II-6 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。	・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。 ・バックアップ媒体は複数世代保管し、古いものから上書きする。 ・バックアップ媒体を廃棄する場合は、データが復元できないよう処理を行った上で、廃棄する。併せて、廃棄履歴を作成し、保存する。 ・特定個人情報が記録された電子媒体 (市町村から入手するもの) のデータは、個人番号カード管理システムに登録した後は、個人番号カード管理システムのサーバ上から消去する。 ・特定個人情報が記録された電子媒体 (市町村から入手するもの) などを廃棄する場合、業者にて物理的な破壊等によりデータを復元できないように完全消去し、消去証明書を提出させる。	事前	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める特定個人情報保護評価の再実施のため。
令和1年8月23日	III リスク対策 (1) 個人番号管理ファイル III-2 リスク4 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、受渡し時は複数人で対応し、受渡し簿等に受渡しの記録を残す、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。	個人番号の変更時、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、受渡し時は複数人で対応し、受渡し簿等に受渡しの記録を残す、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。なお、通常業務においては、電子記録媒体による入手は行わない。	事前	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める特定個人情報保護評価の再実施のため。
令和1年8月23日	III リスク対策 (1) 個人番号管理ファイル III-3 リスク2 特定個人情報の使用の記録 具体的な方法	本人確認情報の管理について定めた規程に基づき、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、規程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。	本人確認情報の管理について定めた規程に基づき、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。具体的には、特定個人情報への不正アクセスを防止するために、アクセスに係る作業を行う者とは別の者が分析・確認を行う体制を整備し、主に市区町村からの依頼に基づく調査を対象として、当該ログの分析・確認の上、その結果を管理責任者へ報告する。 また、規程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。	事前	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める特定個人情報保護評価の再実施のため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和1年8月23日	IIIリスク対策(1) 個人番号管理ファイル III-3 リスク2 その他の措置の内容	—	ユーザ認証、アクセス権限の管理に加えて、個人番号管理ファイルにアクセスできる端末を制限する。	事前	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める特定個人情報保護評価の再実施のため。
令和1年8月23日	IIIリスク対策(1) 個人番号管理ファイル III-3 リスク4 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。	・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。 ・サーバのバックアップを記録した電子記録媒体(バックアップ媒体)については、セキュリティゲートにて入退室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(データ保管室)に設置した施錠可能な場所に保管する。 ※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部屋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。	事前	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める特定個人情報保護評価の再実施のため。
令和1年8月23日	IIIリスク対策(1) 個人番号管理ファイル III-7 リスク1 ⑤物理的対策 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。	・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。 ・サーバ室等への不要な機器の持ち込みを制限し、入退室時に確認を行う。 ・監視設備として監視カメラ等を設置する。	事前	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める特定個人情報保護評価の再実施のため。
令和1年8月23日	IIIリスク対策(1) 個人番号管理ファイル III-7 リスク1 ⑥技術的対策 具体的な対策の内容	・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。	・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。 :インターネットを通じて外部に本人確認情報が漏えいしないよう、個人番号生成システムをインターネットから物理的に分離する。	事前	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める特定個人情報保護評価の再実施のため。
令和1年8月23日	IIIリスク対策(2) 機構保存本人確認情報ファイル III-3 リスク2 特定個人情報の使用の記録 具体的な方法	本人確認情報の管理について定めた規程に基づき、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。	本人確認情報の管理について定めた規程に基づき、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。具体的には、特定個人情報への不正アクセスを防止するために、アクセスに係る作業を行う者とは別の者が分析・確認を行う体制を整備し、主に市区町村からの依頼に基づく調査を対象として、当該ログの分析・確認の上、その結果を管理責任者へ報告する。 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。	事前	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める特定個人情報保護評価の再実施のため。
令和1年8月23日	IIIリスク対策(2) 機構保存本人確認情報ファイル III-3 リスク2 その他の措置の内容	—	ユーザ認証、アクセス権限の管理に加えて、機構保存本人確認情報ファイルにアクセスできる端末を制限する。	事前	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める特定個人情報保護評価の再実施のため。
令和1年8月23日	IIIリスク対策(2) 機構保存本人確認情報ファイル III-3 リスク4 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。	・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。 ・サーバのバックアップを記録した電子記録媒体(バックアップ媒体)については、セキュリティゲートにて入退室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(データ保管室)に設置した施錠可能な場所に保管する。 ※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部屋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。	事前	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める特定個人情報保護評価の再実施のため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和1年8月23日	IIIリスク対策(2) 機構保存本人確認情報ファイル III-7 リスク1 ⑤物理的対策 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。	・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。 ・サーバ室等への不要な機器の持ち込みを制限し、入退室時に確認を行う。 ・監視設備として監視カメラ等を設置する。	事前	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める特定個人情報保護評価の再実施のため。
令和1年8月23日	IIIリスク対策(2) 機構保存本人確認情報ファイル III-7 リスク1 ⑥技術的対策 具体的な対策の内容	・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。	・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。 :インターネットを通じて外部に本人確認情報が漏えいしないよう、住基全国サーバをインターネットから物理的に分離する。	事前	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める特定個人情報保護評価の再実施のため。
令和1年8月23日	IIIリスク対策(3) 個人番号カード用管理ファイル III-2 リスク1 対象者以外の情報の入手を防止するための措置の内容	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。	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。	事前	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める特定個人情報保護評価の再実施のため。
令和1年8月23日	IIIリスク対策(3) 個人番号カード用管理ファイル III-2 リスク4 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。	・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。 ・電子記録媒体による送付先情報の入手の際には、市町村では送付先情報を暗号化して電子記録媒体へ格納し、2名以上の市町村職員で機構に持ち込む。機構側では2名以上の職員で受領した後、当該媒体のウイルスチェックを実施する。その後、復号化してカード管理システムへ取り込むことにより担保する。	事前	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める特定個人情報保護評価の再実施のため。
令和1年8月23日	IIIリスク対策(3) 個人番号カード用管理ファイル III-3 リスク2 特定個人情報の使用の記録 具体的な方法	特定個人情報の管理について定めた規程に基づき、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。	特定個人情報の管理について定めた規程に基づき、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。具体的には、特定個人情報への不正アクセスを防止するために、アクセスに係る作業を行う者とは別の者が分析・確認を行う体制を整備し、主に市区町村からの依頼に基づく調査を対象として、当該ログの分析・確認の上、その結果を管理責任者へ報告する。 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。	事前	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める特定個人情報保護評価の再実施のため。
令和1年8月23日	IIIリスク対策(3) 個人番号カード用管理ファイル III-3 リスク2 その他の措置の内容	—	ユーザ認証、アクセス権限の管理に加えて、個人番号カード用管理ファイルにアクセスできる端末を制限する。	事前	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める特定個人情報保護評価の再実施のため。
令和1年8月23日	IIIリスク対策(3) 個人番号カード用管理ファイル III-3 リスク4 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。	・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。 ・サーバのバックアップを記録した電子記録媒体(バックアップ媒体)及び市町村合併等に伴う大量の送付先情報更新時に使用する電子記録媒体についても、セキュリティゲートにて入退室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)に設置した施錠可能な場所に保管する。 ※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。	事前	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める特定個人情報保護評価の再実施のため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和1年8月23日	IIIリスク対策(3) 個人番号カード用管理ファイル III-7 リスク1 ⑤物理的対策 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。	・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。 ・サーバ室等への不要な機器の持ち込みを制限し、入退室時に確認を行う。 ・監視設備として監視カメラ等を設置する。	事前	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める特定個人情報保護評価の再実施のため。
令和1年8月23日	IIIリスク対策(3) 個人番号カード用管理ファイル III-7 リスク1 ⑥技術的対策 具体的な対策の内容	・不正アクセス対策 :特定個人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。	・不正アクセス対策 :特定個人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。 :インターネットを通じて外部に特定個人情報を漏えいしないよう、個人番号カード管理システムをインターネットから物理的に分離する。	事前	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める特定個人情報保護評価の再実施のため。
令和1年8月23日	IIIリスク対策(3) 個人番号カード用管理ファイル III-7 リスク3 消去手順 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データを消去する。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。	・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データを消去する。消去の際は消去履歴を作成し保存する。 ・特定個人情報記録された電子媒体(市町村から入手するもの)のデータは、個人番号カード管理システムに登録した後は、個人番号カード管理システムのサーバ上から消去する。 ・特定個人情報記録された電子媒体(市町村から入手するもの)などを廃棄する場合、業者にて物理的な破壊等によりデータを復元できないように完全消去し、消去証明書を提出させる。 ・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。	事前	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める特定個人情報保護評価の再実施のため。
令和1年8月23日	IV その他のリスク対策 IV-1 ①自己点検 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(年に一度)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。	NISC政府機関統一基準群への準拠性の確認のため、全部門を対象に自己点検を実施している。 特に、住基全国センターにおいては、NISC政府機関統一基準群、本人確認情報管理規程等に規定され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(年に一度)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。また、個人番号センター個人番号カード部においては、NISC政府機関統一基準群、機構処理事務管理規程等に規定され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(年に一度)に職員による自己点検項目の遵守状況	事前	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める特定個人情報保護評価の再実施のため。
令和1年8月23日	IV その他のリスク対策 IV-1 ②監査 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、内部監査及び第三者機関による外部監査を実施している。 また、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。	本人確認情報の管理方法等及び特定個人情報の管理方法等について、毎年度、地方公共団体情報システム機構本人確認情報管理規程及び地方公共団体情報システム機構機構処理事務管理規程に基づき、内部監査及び第三者機関による外部監査等を実施している。 また、外部監査等で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。	事前	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める特定個人情報保護評価の再実施のため。
令和1年8月23日	IV その他のリスク対策 IV-2 従業者に対する教育・啓発 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を定めた規程の概要について説明、周知徹底している。 また、毎年度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。	入職時の導入研修として集合研修等により実施している。また、年に1回以上、全職員を対象に、集合研修又はeラーニング等による研修を実施している。 また、個人情報保護のための活動として、各部門の個人情報の種類及び取扱いを取りまとめたマニュアルを整備し、各部門の業務運営における個人情報の適切な取扱いについて周知徹底を図っている。 またこれに加え、各部門において、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等により、本人確認情報の管理方法等及び特定個人情報の管理方法等を定めた規程の概要について説明し、周知徹底を図っている。特に、集合研修については複数回開催することで、関係する全職員が受講するよう努めている。 このほか、毎年度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。	事前	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める特定個人情報保護評価の再実施のため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和1年8月23日	IV その他のリスク対策 IV-3 その他のリスク対策	—	・理事長を委員長としに内部統制委員会等を開催し、個人情報保護、情報セキュリティ管理及び危機管理など、リスク管理に係る諸活動の実施計画及び実施状況について審議することにより、リスク管理活動の運用・改善を図っている。 緊急時対応訓練の実施、インシデント報告会(毎月、全常勤役員参加)の開催等により、危機管理態勢の着実な運用と改善を図っている。 ・特定個人情報をはじめとする個人情報等が漏えいした場合の対策として、業務継続計画及び緊急時対応計画等に基づき、緊急体制により次の事項について必要な措置を講ずる。 (1) 機構内部における報告、被害の拡大防止 責任ある立場の者に直ちに報告するとともに、被害の拡大を防止する。 (2) 事実関係の調査、原因の究明 事実関係を調査し、その原因の究明を行う。 (3) 影響範囲の特定 (2)で把握した事実関係による影響の範囲を特定する。 (4) 再発防止策の検討・実施 (2)で究明した原因を踏まえ、再発防止策を検討し、速やかに実施する。 (5) 影響を受ける可能性のある本人への連絡及び関係する機関等へ連絡等 事案の内容等に応じて、二次被害の防止、類似事案の発生回避等の観点から、事実関係等について、速やかに、本人へ連絡し、又は本人が容易に知り得る状態に置く。また、個人情報保護委員会、総務省等の関係する国の行政組織及び地方公共団体等に報告する。 (6) 事実関係、再発防止策等の公表 事案の内容等に応じて、二次被害の防止	事前	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める特定個人情報保護評価の再実施のため。
令和1年8月23日	IV その他のリスク対策 IV-3 その他のリスク対策	—	(上の続き) ・特定個人情報を取り扱うシステムの調達・構築・運用等に当たっては、サプライチェーンリスクの管理に努める。	事前	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める特定個人情報保護評価の再実施のため。
令和2年5月11日	表紙 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、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規定による通知カード及び個人番号カード並びに情報提供ネットワークシステムによる特定個人情報の提供等に関する省令に基づき、市町村長(特別区の区長を含む。以下同じ。)から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。	・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、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に規定する個人番号、個人番号カード、特定個人情報の提供等に関する省令(平成26年11月20日総務省令第85号。以下「個人番号カード省令」という。)に基づき、市町村長(特別区の区長を含む。以下同じ。)から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。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更当たらないため。
令和2年5月11日	I-1 ②事務の内容	3. 個人番号カードに係る事務(※詳細は、「(別添1)事務の内容」を参照) 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、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規定による通知カード及び個人番号カード並びに及び情報提供ネットワークシステムによる規定する個人番号、個人番号カード、特定個人情報の提供等に関する省令(平成26年11月20日総務省令第85号)(以下「通知カード及び個人番号カード省令」という。)第35条第1項に基づく委任を受け、通知カード及び個人番号カードに係る以下の事務を行う。 (1) 通知カードの印刷・住民への送付 ・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。	3. 個人番号カードに係る事務(※詳細は、「(別添1)事務の内容」を参照) 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、個人番号カード省令第35条第1項に基づく委任を受け、個人番号通知書及び個人番号カードに係る以下の事務を行う。 (1) 個人番号通知書の印刷・住民への送付 ・住民に対して個人番号通知書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、個人番号通知書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。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更当たらないため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和2年5月11日	I-2 システム3 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、個人番号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. 個人番号カードに係る事務」に対応) ・個人番号通知書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、個人番号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。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
令和2年5月11日	I-4 ①事務実施上の必要性	(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。	(3) 個人番号カード用管理ファイル ①住民に対し、個人番号通知書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。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
令和2年5月11日	(別添1) 事務の内容 [前提] 番号制度全体における機構の役割(概要) 図中の表記	通知カード及び個人番号カード省令に基づく市町村長からの委任を受け通知カード及び個人番号カード発行	個人番号カード省令に基づく市町村長からの委任を受け個人番号通知書及び個人番号カード発行	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
令和2年5月11日	(別添1) 事務の内容 (3) 個人番号カードに係る事務 図中の表記	1-③通知カード及び交付申請書印刷 1-④通知カード及び交付申請書送付	1-③個人番号通知書及び交付申請書印刷 1-④個人番号通知書及び交付申請書送付	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
令和2年5月11日	(別添1) 事務の内容 (3) 個人番号カードに係る事務	(備考) (3)-1. 通知カードの印刷・住民への送付 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。	(備考) (3)-1. 個人番号通知書の印刷・住民への送付 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、個人番号通知書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、個人番号通知書及び交付申請書を送付する。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
令和2年5月11日	II ファイルの概要(3) 個人番号カード用管理ファイル II-2 ③対象となる本人の範囲 その必要性	番号法第7条第1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ため。 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ため。 機構は、これらの事務を通知カード及び個人番号カード省令第35条第1項(通知カード・個人番号カード関連事務の委任)に基づき、市町村長から委任を受けて実施する。	番号法第7条第1項(指定及び通知)及び個人番号カード省令第7条(個人番号の通知)に基づき、個人番号通知書を個人番号の付番対象者に送付する必要があるため。 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ため。 機構は、これらの事務を個人番号カード省令第35条第1項(個人番号通知書・個人番号カード関連事務の委任)に基づき、市町村長から委任を受けて実施する。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
令和2年5月11日	II ファイルの概要(3) 個人番号カード用管理ファイル II-2 ④記録される項目 主な記録項目	[○] 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、個人番号通知書の印刷情報、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)	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
令和2年5月11日	II ファイルの概要(3) 個人番号カード用管理ファイル II-2 ④記録される項目 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。	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、個人番号通知書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。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和2年5月11日	II ファイルの概要 (3) 個人番号カード用管理ファイル II - 3 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) ：個人番号カードの交付希望者により送付された交付申請書 (記入済) により随時入手する。	・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) ：個人番号通知書及び交付申請書の送付先に係る情報は、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) ：個人番号カードの交付希望者により送付された交付申請書 (記入済) により随時入手する。	事後	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める重要な変更にあたらないため。
令和2年5月11日	II ファイルの概要 (3) 個人番号カード用管理ファイル II - 3 ④ 入手に係る妥当性	・送付先情報 (市町村より入手) ：番号法第7条第1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。 ・交付申請書 (交付申請者本人より入手) ：通知カード及び個人番号カード省令第21条において、交付申請書に記載すべき事項として交付申請者の氏名、住所、個人番号が規定されている。	・送付先情報 (市町村より入手) ：番号法第7条第1項 (指定及び通知) 及び個人番号カード省令第7条 (個人番号の通知) に基づき、個人番号通知書を個人番号の付番対象者に送付するため、個人番号通知書の送付先情報が必要となる。 ・交付申請書 (交付申請者本人より入手) ：個人番号カード省令第21条において、交付申請書に記載すべき事項として交付申請者の氏名、住所、個人番号が規定されている。	事後	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める重要な変更にあたらないため。
令和2年5月11日	II ファイルの概要 (3) 個人番号カード用管理ファイル II - 3 ⑤ 本人への明示	機構が送付先情報及び交付申請書を入手することについて、通知カード及び個人番号カード省令第35条 (通知カード・個人番号カード関連事務の委任)、第36条 (通知カード・個人番号カード関連事務に係る通知) に明示されている。	機構が送付先情報及び交付申請書を入手することについて、個人番号カード省令第35条 (個人番号通知書・個人番号カード関連事務の委任)、第36条 (個人番号通知書・個人番号カード関連事務に係る通知) に明示されている。	事後	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める重要な変更にあたらないため。
令和2年5月11日	II ファイルの概要 (3) 個人番号カード用管理ファイル II - 3 ⑥ 使用目的	通知カード及び個人番号カード省令第35条 (通知カード・個人番号カード関連事務の委任) 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。	個人番号カード省令第35条 (個人番号通知書・個人番号カード関連事務の委任) 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。	事後	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める重要な変更にあたらないため。
令和2年5月11日	II ファイルの概要 (3) 個人番号カード用管理ファイル II - 3 ⑧ 使用方法	・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→個人番号カード管理システム) 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) を元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。	・住民に対して個人番号通知書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→個人番号カード管理システム) し、個人番号通知書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) を元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 (※一時停止端末の画面上で個人番号は表示されない。)	事後	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める重要な変更にあたらないため。
令和2年5月11日	II ファイルの概要 (3) 個人番号カード用管理ファイル II - 4 委託事項1 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)	・個人番号通知対象者に対して送付する個人番号通知書及び交付申請書の印刷に係る事務 (印刷・送付事務)	事後	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める重要な変更にあたらないため。
令和2年5月11日	II ファイルの概要 (3) 個人番号カード用管理ファイル II - 4 委託事項1 ② 取扱いを委託する特定個人情報ファイルの範囲その妥当性	番号法第7条第1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。	番号法第7条第1項 (指定及び通知) 及び個人番号カード省令第7条 (個人番号の通知) に基づき、個人番号通知書を個人番号の付番対象者に送付する必要がある。	事後	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める重要な変更にあたらないため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和2年5月11日	II ファイルの概要 (3) 個人番号カード用管理ファイル II-4 委託事項1 ⑥委託先名	・独立行政法人国立印刷局 (印刷・送付事務)	・(株) DNPデータテクノ (印刷・送付事務)	事後	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める重要な変更にあたらないため。
令和2年5月11日	II ファイルの概要 (3) 個人番号カード用管理ファイル II-4 委託事項1 再委託 ⑨再委託事項	・通知カード及び交付申請書の印刷	・個人番号通知書及び交付申請書の封入・封かん・発送	事後	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める重要な変更にあたらないため。
令和2年5月11日	II ファイルの概要 (3) 個人番号カード用管理ファイル II-4 委託事項3 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	通知カード、個人番号通知書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	事後	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める重要な変更にあたらないため。
令和2年5月11日	II ファイルの概要 (3) 個人番号カード用管理ファイル II-4 委託事項3 ②取扱いを委託する特定個人情報ファイルの範囲 子の妥当性	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。	通知カード、個人番号通知書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。	事後	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める重要な変更にあたらないため。
令和2年5月11日	II ファイルの概要 (3) 個人番号カード用管理ファイル II-5 提供先1 ①法令上の根拠	通知カード及び個人番号カード省令第36条第3項 (通知カード・個人番号カード関連事務に係る通知)	個人番号カード省令第36条第3項 (個人番号通知書・個人番号カード関連事務に係る通知)	事後	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める重要な変更にあたらないため。
令和2年5月11日	(別添2) 特定個人情報ファイル記録項目	(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… (中略) …、106. カード製造者識別情報、107. カードイメージ番号、108. 被証明者識別子、109. 通知カード管理状況、110. 旧氏漢字、111. 旧氏 外字数、112. 旧氏 外字ふりがな、113. 旧氏 外字変更連番、114. ローマ字 氏名、115. ローマ字 旧氏	(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… (中略) …、106. カード製造者識別情報、107. カードイメージ番号、108. 被証明者識別子、109. 通知カード・個人番号通知書管理状況、110. 旧氏漢字、111. 旧氏 外字数、112. 旧氏 外字ふりがな、113. 旧氏 外字変更連番、114. ローマ字 氏名、115. ローマ字 旧氏	事後	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める重要な変更にあたらないため。
令和2年5月11日	III リスク対策 (3) 個人番号カード用管理ファイル III-2 リスク1 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。	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市町村からの個人番号通知書等の「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。	事後	特定個人情報保護評価指針 (平成30年5月21日個人情報保護委員会) に定める重要な変更にあたらないため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和2年5月11日	IIIリスク対策(3) 個人番号カード用管理ファイル III-3 リスク1 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、④国立印刷局に限られるよう、アクセス制御を行う。 (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 :利用者情報照会を行う場合。ただし、住民票コードのみをキーとし、特定個人情報を使ったアクセスは行わない。 ②個人番号カード申請受付・発行システム :個人番号カード発行情報等を提供する場合、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。 ④国立印刷局 :通知カード発行情報等を提供する場合。	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、④(株)DNPデータテクノに限られるよう、アクセス制御を行う。 (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 :利用者情報照会を行う場合。ただし、住民票コードのみをキーとし、特定個人情報を使ったアクセスは行わない。 ②個人番号カード申請受付・発行システム :個人番号カード発行情報等を提供する場合、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、個人番号通知書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。 ④(株)DNPデータテクノ :個人番号通知書発行情報等を提供する場合。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
令和2年5月11日	IIIリスク対策(3) 個人番号カード用管理ファイル III-3 リスク1 事務で使用するその他のシステムにおける措置の内容	(上の続き) (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。 :個人番号カード管理システムからの利用者情報照会に基づき、本人確認情報を連携する場合。 ②個人番号カード申請受付・発行システム :個人番号カードの発行結果等を受信する場合。 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。 ④国立印刷局 :通知カード発行結果等を受信する場合。	(上の続き) (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。 :個人番号カード管理システムからの利用者情報照会に基づき、本人確認情報を連携する場合。 ②個人番号カード申請受付・発行システム :個人番号カードの発行結果等を受信する場合。 ③コールセンター :通知カード、個人番号通知書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。 ④(株)DNPデータテクノ :個人番号通知書発行結果等を受信する場合。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
令和2年5月11日	IIIリスク対策(3) 個人番号カード用管理ファイル III-4 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差出前に外観検査・員数検査・重量検査・厚み検査を実施することを委託契約の仕様書に定める等の現行措置に加え、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随時検討する。	・個人番号通知書及び交付申請書の差出前に外観検査・員数検査・重量検査・厚み検査を実施することを委託契約の仕様書に定める等の現行措置に加え、個人番号通知書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随時検討する。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。
令和2年5月11日	IIIリスク対策(3) 個人番号カード用管理ファイル III-5 リスク1 特定個人情報の提供・移転に関するルール ルールの内容及びルール遵守の確認方法	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・移転に係るルールについては、「通知カード及び個人番号カードに関する技術的基準」(平成27年9月18日総務省告示第314号)においてその具体的なルールを定めている。	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・移転に係るルールについては、「個人番号カード等に関する技術的基準」(平成27年9月18日総務省告示第314号)においてその具体的なルールを定めている。	事後	特定個人情報保護評価指針(平成30年5月21日個人情報保護委員会)に定める重要な変更にあたらないため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和3年9月1日	表紙 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、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に規定する個人番号、個人番号カード、特定個人情報等の提供等に関する省令（平成26年11月20日総務省令第85号、以下「個人番号カード省令」という。）に基づき、市町村長（特別区の区長を含む。以下同じ。）から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。 ・外部との接続に当たっては、専用回線の利用、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。	・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、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に規定する個人番号、個人番号カード、特定個人情報の提供等に関する省令（平成26年11月20日総務省令第85号、以下「個人番号カード省令」という。）に基づき、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。 ・外部との接続に当たっては、専用回線の利用、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。	事後	特定個人情報保護評価指針（令和3年9月1日個人情報保護委員会）に定める重要な変更にあたらないため。
令和3年9月1日	Ⅰ 基本情報 Ⅰ－1 ②事務の内容	3. 個人番号カードに係る事務 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、第35条第1項に基づく委任を受け、個人番号通知書及び個人番号カードに係る以下の事務を行う。	3. 個人番号カードに係る事務 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、個人番号カード省令第23条から第23条の3まで及び第35条第1項に基づき、個人番号通知書及び個人番号カードに係る以下の事務を行う。	事後	特定個人情報保護評価指針（令和3年9月1日個人情報保護委員会）に定める重要な変更にあたらないため。
令和3年9月1日	Ⅰ 基本情報 5. 個人番号の利用 法令上の根拠	1. 番号法 ・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. 住基法 ・第30条の9の2（総務省への住民票コードの提供）	1. 番号法 ・第8条（個人番号とすべき番号の生成） ・第16条の2（個人番号カードの発行等） ・第17条第1項、第3項、第6項（個人番号カードの交付等） 2. 住基法 ・第30条の9の2（デジタル庁への住民票コードの提供）	事後	特定個人情報保護評価指針（令和3年9月1日個人情報保護委員会）に定める重要な変更にあたらないため。
令和3年9月1日	Ⅰ 基本情報 6. 情報提供ネットワークシステムによる情報連携 ②法令上の根拠	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9の2（デジタル庁への住民票コードの提供）	事後	特定個人情報保護評価指針（令和3年9月1日個人情報保護委員会）に定める重要な変更にあたらないため。
令和3年9月1日	(別添1) 事務の内容 (前掲) 番号制度全体における機構の役割 (概要) 図中の表記	個人番号カード省令に基づく市町村長からの委任を受け通知カード及び個人番号カード発行	個人番号カード省令に基づく個人番号通知書及び個人番号カード発行	事後	特定個人情報保護評価指針（令和3年9月1日個人情報保護委員会）に定める重要な変更にあたらないため。
令和3年9月1日	Ⅱ ファイルの概要 (2) 機構保存本人確認情報ファイル Ⅱ－5 提供先2 ①法令上の根拠	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9の2（デジタル庁への住民票コードの提供）	事後	特定個人情報保護評価指針（令和3年9月1日個人情報保護委員会）に定める重要な変更にあたらないため。
令和3年9月1日	Ⅱ ファイルの概要 (3) 個人番号カード用管理ファイル Ⅱ－2 ③対象となる本人の範囲 その必要性	番号法第7条第1項（指定及び通知）及び個人番号カード省令第7条（個人番号の通知）に基づき、個人番号通知書を個人番号の付番対象者に送付する必要があるため。 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ため。 機構は、これらの事務を個人番号カード省令第35条第1項（個人番号通知書・個人番号カード関連事務の委任）に基づき、市町村長から委任を受けて実施する。	番号法第7条第1項（指定及び通知）及び個人番号カード省令第7条（個人番号の通知）に基づき、個人番号通知書を個人番号の付番対象者に送付する必要があるため。 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ため。 機構は、これらの事務を個人番号カード省令第23条から第23条の3まで及び第35条第1項に基づき実施する。	事後	特定個人情報保護評価指針（令和3年9月1日個人情報保護委員会）に定める重要な変更にあたらないため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和3年9月1日	II ファイルの概要 (3) 個人番号カード用管理ファイル II-3 ⑤本人への明示	機構が送付先情報及び交付申請書を入手することについて、個人番号カード省令第35条 (個人番号通知書・個人番号カード関連事務の委任)、第36条 (個人番号通知書・個人番号カード関連事務に係る通知) に明示されている。	機構が送付先情報及び交付申請書を入手することについて、個人番号カード省令第23条の2 (個人番号通知書及び個人番号カードに関し機構が処理する事務)、第36条 (機構への通知) に明示されている。	事後	特定個人情報保護評価指針 (令和3年9月1日個人情報保護委員会) に定める重要な変更にあたらないため。
令和3年9月1日	II ファイルの概要 (3) 個人番号カード用管理ファイル II-3 ⑥使用目的	個人番号カード省令第35条 (個人番号通知書・個人番号カード関連事務の委任) 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。	個人番号カード省令第23条の2 (個人番号通知書及び個人番号カードに関し機構が処理する事務) 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。	事後	特定個人情報保護評価指針 (令和3年9月1日個人情報保護委員会) に定める重要な変更にあたらないため。
令和3年9月1日	II ファイルの概要 (3) 個人番号カード用管理ファイル II-5 ①法令上の根拠	・個人番号カード省令第36条第3項 (個人番号通知書・個人番号カード関連事務に係る通知)	・番号法第16条の2第2項 (個人番号カードの発行等) ・個人番号カード省令第23条の2 (個人番号通知書及び個人番号カードに関し機構が処理する事務)	事後	特定個人情報保護評価指針 (令和3年9月1日個人情報保護委員会) に定める重要な変更にあたらないため。
令和3年9月1日	機構保存本人確認情報ファイル III-5 リスク1 特定個人情報の提供・移転に関するルール ルール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・移転に係るルールについては、「地方公共団体情報システム機構個人情報保護規程」においてその具体的なルールを定めている。	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5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・移転に係るルールについては、「地方公共団体情報システム機構個人情報保護規程」においてその具体的なルールを定めている。	事後	特定個人情報保護評価指針 (令和3年9月1日個人情報保護委員会) に定める重要な変更にあたらないため。
令和3年9月1日	IIIリスク対策 (2) 機構保存本人確認情報ファイル III-6 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。	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 (デジタル庁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。	事後	特定個人情報保護評価指針 (令和3年9月1日個人情報保護委員会) に定める重要な変更にあたらないため。

(別添3) 変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和4年8月8日	II ファイルの概要 (3) 個人番号カード用管理ファイル II - 2 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 (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。	事後	特定個人情報保護評価指針 (令和4年4月1日個人情報保護委員会) に定める重要な変更にあたらないため。
令和4年8月8日	II ファイルの概要 (3) 個人番号カード用管理ファイル II - 2 ③対象となる本人の範囲 その必要性	番号法第7条第1項 (指定及び通知) 及び個人番号カード省令第7条 (個人番号の通知) に基づき、個人番号通知書を個人番号の付番対象者に送付する必要があるため。 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ため。 機構は、これらの事務を個人番号カード省令第23条から第23条の3まで及び第35条第1項に基づき、実施する。	番号法第7条第1項 (指定及び通知) 及び個人番号カード省令第7条 (個人番号の通知) に基づき、個人番号通知書を個人番号の付番対象者に送付する必要があるため。 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ため。 機構は、これらの事務を個人番号カード省令第23条から第23条の3まで及び第35条第1項に基づき、実施する。	事後	特定個人情報保護評価指針 (令和4年4月1日個人情報保護委員会) に定める重要な変更にあたらないため。
令和4年8月8日	II ファイルの概要 (3) 個人番号カード用管理ファイル II - 2 ⑥事務担当部署	個人番号センター個人番号カード部	個人番号センター運用管理センター個人番号カードシステム部、個人番号センター運用管理センター運用部個人番号カードシステム運用担当	事後	特定個人情報保護評価指針 (令和4年4月1日個人情報保護委員会) に定める重要な変更にあたらないため。
令和4年8月8日	II ファイルの概要 (3) 個人番号カード用管理ファイル II - 3 ⑦使用の主体	個人番号センター個人番号カード部	個人番号センター運用管理センター個人番号カードシステム部、個人番号センター運用管理センター運用部個人番号カードシステム運用担当	事後	特定個人情報保護評価指針 (令和4年4月1日個人情報保護委員会) に定める重要な変更にあたらないため。
令和4年8月8日	II ファイルの概要 (3) 個人番号カード用管理ファイル II - 4 委託事項1	・ (株) DNPデータテクノ (印刷・送付事務)	・ (株) DNPデータテクノ (印刷・送付事務)	事後	特定個人情報保護評価指針 (令和4年4月1日個人情報保護委員会) に定める重要な変更にあたらないため。
令和4年8月8日	II ファイルの概要 (3) 個人番号カード用管理ファイル II - 4 委託事項3 ⑥委託先名	(株)NTTマーケティングアクト、NTTコミュニケーションズ(株)	(株)NTTマーケティングアクトProCX、NTTコミュニケーションズ(株)	事後	特定個人情報保護評価指針 (令和4年4月1日個人情報保護委員会) に定める重要な変更にあたらないため。
令和4年8月8日	IVその他のリスク対策 IV - 1 ①自己点検 具体的なチェック方法	NISC政府機関統一基準群への準拠性の確認のため、全部門を対象に自己点検を実施している。 特に、住基全国センターにおいては、NISC政府機関統一基準群、本人確認情報管理規程等に規定され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 (年に一度) 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。また、個人番号センター個人番号カード部においては、NISC政府機関統一基準群、機構処理事務管理規程等に規定され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 (年に一度) に職員による自己点検項目の遵守状況の確認を実施する。	NISC政府機関統一基準群への準拠性の確認のため、全部門を対象に自己点検を実施している。 特に、住基全国センターにおいては、NISC政府機関統一基準群、本人確認情報管理規程等に規定され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 (年に一度) 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。また、個人番号センター運用管理センター個人番号カードシステム部及び個人番号センター運用管理センター運用部個人番号カードシステム運用担当においては、NISC政府機関統一基準群、機構処理事務管理規程等に規定され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 (年に一度) に職員による自己点検項目の遵守状況の確認を実施する。	事後	特定個人情報保護評価指針 (令和4年4月1日個人情報保護委員会) に定める重要な変更にあたらないため。

(別添3) 変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和4年10月11日	I 基本情報 I-1 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」及び「3. 個人番号カードに係る事務」に分かれる。	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」及び「4. 附票本人確認情報の提供及び保存等に係る事務」に分かれる。	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更に当たるため。
令和4年10月11日	I 基本情報 I-1 ②事務の内容	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) 事務の内容」を参照) (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。	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) 事務の内容」を参照) (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。 ※国外転出者に係る事務処理に関し、番号法で認められた場合に限り、国の機関等からの求めに応じ、当該個人の住民票コードを用いて、機構保存本人確認情報ファイルから個人番号を抽出し、附票全国サーバに提供する場合がある。	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更に当たるため。
令和4年10月11日	I 基本情報 I-1 ②事務の内容		4. 附票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) 事務の内容」を参照) 機構は、市町村における市町村CS、都道府県における附票都道府県サーバ及び機構における附票全国サーバ等により構成される「附票連携システム」において、国外転出者に係る本人確認を行うための社会的基盤としての役割を担うため、4情報(氏名、住所、生年月日、性別)、住民票コード及びこれらの変更情報で構成される「機構保存附票本人確認情報ファイル」を作成し、戸籍の附票に関する記録を正確に行う責務がある。そのため、附票本人確認情報の提供及び保存等に係る以下の事務を実施する。なお、機構保存附票本人確認情報(以下「附票本人確認情報」という場合もある。)には、個人番号は含まれない。 (1)附票本人確認情報の更新 ・機構保存附票本人確認情報ファイルを最新の状態に保つため、都道府県知事から通知された附票本人確認情報の更新情報を元に当該ファイルを更新する。 (2)市町村長等への附票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、国外転出者に係る事務処理に関し、照会のあった当該個人の4情報等に対応付く附票本人確認情報を機構保存附票本人確認情報ファイルから抽出し、照会元に提供する。その際、番号法で認められた場合に限り、附票本人確認情報の提供に併せて、当該個人の住民票コードを用いて機構保存本人確認情報ファイルから個人番号を抽出し、照会元に提供する場合がある。	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更に当たるため。
令和4年10月11日	I 基本情報 I-1 ②事務の内容		(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・情報提供者から要求を受け、情報提供ネットワークシステムに住基全国サーバを経由して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に住基全国サーバを経由して情報提供ネットワークシステムに通知する。 (4)附票本人確認情報開示 ・法律に基づく本人による自己の附票本人確認情報の開示請求に対応するため、当該個人の附票本人確認情報を機構保存附票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)附票本人確認情報整合 ・機構保存附票本人確認情報ファイルの正確性を担保するため、市町村長から附票本人確認情報を受領し、当該附票本人確認情報を用いて機構保存附票本人確認情報ファイルに記録された附票本人確認情報の整合性確認を行う。また、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と機構保存附票本人確認情報ファイルに記録された附票本人確認情報の整合性確認を行う。	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更に当たるため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和4年10月11日	Ⅰ 基本情報 Ⅰ－1 ②事務の内容		※附票本人確認情報の利用（個人番号カード管理システムへの附票本人確認情報の提供） 個人番号カードの交付申請後に機構保存附票本人確認情報をもってカードの発行に用いられる送付先情報が最新かどうかを比較・突合し、古い住所や氏名でカードが発行され住民へ交付されるリスクを低減させる。 交付後のタイミングにおいても、申請から交付までの間の異動情報を個人番号カードの一時停止時の本人性確認に用いられる利用者情報に反映させることにより、交付後直ちに異動後の最新の住所等で一時停止業務を行えるようにするため、個人番号カード管理システムから照会要求を受け（個人番号カード管理システム→附票全国サーバ）、住民票コードを元に機構保存附票本人確認情報ファイルを検索し、該当する個人の附票本人確認情報を照会元へ提供する（附票全国サーバ→個人番号カード管理システム）。	事前	特定個人情報保護評価指針（令和4年4月1日個人情報保護委員会）に定める重要な変更にあたるため。
令和4年10月11日	Ⅰ 基本情報 Ⅰ－2 システム2 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。	（「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。 ※国外転出者に係る事務処理に関し、番号法で認められた場合に限り、国の機関等からの求めに応じ、当該個人の住民票コードを用いて、機構保存本人確認情報ファイルから個人番号を抽出し、附票全国サーバに連携する場合がある。	事前	特定個人情報保護評価指針（令和4年4月1日個人情報保護委員会）に定める重要な変更にあたるため。
令和4年10月11日	Ⅰ 基本情報 Ⅰ－2 システム2 ③他のシステムとの接続	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）	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、附票連携システム）	事前	特定個人情報保護評価指針（令和4年4月1日個人情報保護委員会）に定める重要な変更にあたるため。
令和4年10月11日	Ⅰ 基本情報 Ⅰ－2 システム3 ③他のシステムとの接続	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）	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、附票連携システム）	事前	特定個人情報保護評価指針（令和4年4月1日個人情報保護委員会）に定める重要な変更にあたるため。
令和4年10月11日	Ⅰ 基本情報 Ⅰ－2 システム4 ①システムの名称		附票連携システム ※機構保存附票本人確認情報ファイルは、附票連携システムの構成要素のうち、「附票全国サーバ」において管理がなされているため、以降、附票全国サーバについて記載する。	事前	特定個人情報保護評価指針（令和4年4月1日個人情報保護委員会）に定める重要な変更にあたるため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和4年10月11日	Ⅰ 基本情報 Ⅰ－2 システム4 ②システムの機能		〔「4. 附票本人確認情報の提供及び保存等に係る事務」に対応〕 ・附票都道府県サーバから附票本人確認情報の更新データを受信し、機構保存附票本人確認情報ファイルを更新し、通知元附票都道府県サーバに附票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国外転出者に係る附票本人確認情報照会要求を受け取り、住民票コード又は4情報の組合せにより機構保存附票本人確認情報ファイルを検索する。附票本人確認情報照会要求により検索した、附票本人確認情報を市町村長等へ提供する。その際、番号法で認められた場合に限り、国の機関等からの求めに応じ、附票本人確認情報の提供に併せて当該個人の住民票コードを用いて、機構保存本人確認情報ファイルから個人番号を抽出し、照会元へ提供する場合がある。 ・番号法上の情報照会者・情報提供者からの国外転出者に係る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等で最新の本人確認情報及び附票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附票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。 ・個人番号カード管理システムから利用者情報の照会要求を受け、該当する個人の附票本人確認情報を照会元へ提供する。	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更に当たるため。
令和4年10月11日	Ⅰ 基本情報 Ⅰ－2 システム4 ③他のシステムとの接続	[]住民基本台帳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 [○]その他(個人番号カード管理システム)	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更に当たるため。
令和4年10月11日	Ⅰ 基本情報 Ⅰ－3	(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	(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) 機構保存附票本人確認情報ファイル	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更に当たるため。
令和4年10月11日	Ⅰ 基本情報 Ⅰ－4 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とおりの目的遂行のため取り扱う。	機構では、以下の4ファイルを下記に記載のとおりの目的遂行のため取り扱う。 (4) 機構保存附票本人確認情報ファイル ※機構保存附票本人確認情報には個人番号は含まれない。 ①国外転出者に係る本人確認を行うための社会的基盤として記録を正確に行う。 ②市町村長、都道府県知事、国の機関等に対し国外転出者に係る附票本人確認情報を提供する。 その際、番号法で認められた場合に限り、国の機関等からの求めに応じ、附票本人確認情報の提供に併せて当該個人の住民票コードを用いて、機構保存本人確認情報ファイルから個人番号を抽出し、照会元へ提供する場合がある。 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本人からの請求に基づき、当該個人の附票本人確認情報を開示する。 ⑤個人番号カードの交付申請時に個人番号カード管理システムが保持する送付先情報と附票全国サーバが保持する附票本人確認情報が一致しているかを確認し、また個人番号カードの一時停止業務を最新の情報に基づき実施するため、個人番号カード管理システムから利用者情報の照会要求を受け、該当する個人の附票本人確認情報を提供する。	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更に当たるため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和4年10月11日	Ⅰ 基本情報 Ⅰ－4 ②実現が期待されるメリット	住民票の写し等に代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。	住民票の写し等に代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、国外転出者を含め個人番号カードによる本人確認、個人番号の真正性確認が可能となり、行政事務の効率化に資することが期待される。	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更にあたるため。
令和4年10月11日	Ⅰ 基本情報 Ⅰ－5 法令上の根拠	2. 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) ・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(デジタル庁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)	2. 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) ・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(デジタル庁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) ・第30条の44の6第6項(附票本人確認情報(住民票コードに限る。)の利用)	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更にあたるため。
令和4年10月11日	Ⅰ 基本情報 Ⅰ－6 ②法令上の根拠	住基法第30条の9の2(デジタル庁への住民票コードの提供)	住基法第30条の9の2(デジタル庁への住民票コードの提供) 住基法第30条の44の2(デジタル庁への住民票コードの提供)	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更にあたるため。
令和4年10月11日	Ⅰ 基本情報 Ⅰ－7 ①部署	(1)地方公共団体情報システム機構事務局 (2)住民基本台帳ネットワークシステム全国センター (3)個人番号センター	(1)住民基本台帳ネットワークシステム全国センター (2)住民基本台帳ネットワークシステム全国センター (3)個人番号センター (4)住民基本台帳ネットワークシステム全国センター	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更にあたるため。
令和4年10月11日	Ⅰ 基本情報 Ⅰ－7 ②所属長の役職名	(1)理事(兼)事務局長事務取扱 (2)センター長 (3)センター長	(1)センター長 (2)センター長 (3)センター長 (4)センター長	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更にあたるため。
令和4年10月11日	(別添1) 事務の内容 [前提] 番号制度全体における機構の役割(概要)		概要図の修正	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更にあたるため。
令和4年10月11日	(別添1) 事務の内容 (2) 本人確認情報の提供及び保存に係る事務(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)	2-② 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。	2-② 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。 ※ 国外転出者に係る事務処理に関し、番号法で認められた場合に限り、国の機関等からの求めに応じ、当該個人の住民票コードを用いて、「機構保存本人確認情報ファイル」から個人番号を抽出し、附票全国サーバに連携する場合がある(別添1(4)参照)。	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更にあたるため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和4年10月11日	(別添1) 事務の内容 (4) 附票本人確認情報の提供及び保存等に係る事務 (該当する特定個人情報ファイル・機構保存附票本人確認情報ファイル)		概要図及び事務の流れを記載	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更に当たるため。
令和4年10月11日	II 特定個人情報ファイルの概要 (1) 個人番号管理ファイル II-6 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。サーバのバックアップを記録した電子記録媒体(バックアップ媒体)についても、セキュリティゲートにて入退室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(データ保管室)に設置した施設可能な場所に保管する。	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。サーバのバックアップについても、セキュリティゲートにて入退室管理をしている建物の中で、さらに入退室管理(※)を行っている部屋に設置した施設可能な場所に保管する。	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更に当たるため。
令和4年10月11日	II 特定個人情報ファイルの概要 (1) 個人番号管理ファイル II-6 ③ 消去方法	・バックアップ媒体は複数世代保管し、古いものから上書きする。 ・バックアップ媒体を廃棄する場合は、データが復元できないよう処理を行った上で、廃棄する。併せて、廃棄履歴を作成し、保存する。	・バックアップは複数世代保管し、古いものから上書きする。 ・バックアップを廃棄する場合は、データが復元できないよう処理を行った上で、廃棄する。併せて、廃棄履歴を作成し、保存する。	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更に当たるため。
令和4年10月11日	II 特定個人情報ファイルの概要 (2) 機構保存本人確認情報ファイル II-3 ④ 入手に係る妥当性	※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15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。	※住基ネットは、保有情報・利用の制限、内部の不正利用の防止、外部からの侵入防止など、セキュリティ確保のための様々な措置が講じられており、平成14年8月5日の稼働後、住基ネットへのハッキングや情報漏えいなどの事件や障害は一度も発生していない。	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更に当たるため。
令和4年10月11日	II 特定個人情報ファイルの概要 (2) 機構保存本人確認情報ファイル II-3 ⑧ 使用方法	・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)。	・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)。 ※国外転出者に係る事務処理に関し、番号法で認められた場合に限り、国の機関等からの求めに応じ、当該個人の住民票コードを用いて、機構保存本人確認情報ファイルから個人番号を抽出し、附票全国サーバに連携する場合がある。	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更に当たるため。
令和4年10月11日	II 特定個人情報ファイルの概要 (2) 機構保存本人確認情報ファイル II-3 ⑧ 使用方法 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。	・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。 ・機構保存附票本人確認情報ファイルの住民票コードと機構保存本人確認情報ファイルの個人番号を突合する。 ・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。	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更に当たるため。
令和4年10月11日	II 特定個人情報ファイルの概要 (2) 機構保存本人確認情報ファイル II-6 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。サーバのバックアップを記録した電子記録媒体(バックアップ媒体)についても、セキュリティゲートにて入退室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(データ保管室)に設置した施設可能な場所に保管する。	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。サーバのバックアップについても、セキュリティゲートにて入退室管理をしている建物の中で、さらに入退室管理(※)を行っている部屋に設置した施設可能な場所に保管する。	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更に当たるため。
令和4年10月11日	II 特定個人情報ファイルの概要 (2) 機構保存本人確認情報ファイル II-6 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。 ・バックアップ媒体は複数世代保管し、古いものから上書きする。 ・バックアップ媒体を廃棄する場合は、データが復元できないよう処理を行った上で、廃棄する。併せて、廃棄履歴を作成し、保存する。	・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。 ・バックアップは複数世代保管し、古いものから上書きする。 ・バックアップを廃棄する場合は、データが復元できないよう処理を行った上で、廃棄する。併せて、廃棄履歴を作成し、保存する。	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更に当たるため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和4年10月11日	II 特定個人情報ファイルの概要 (4) 機構保存附票本人確認情報ファイル		機構保存附票本人確認情報ファイルについて、以下の項目を記載 1. 特定個人情報ファイル名 2. 基本情報 3. 特定個人情報の入手・使用 4. 特定個人情報ファイルの取扱いの委託 5. 特定個人情報の提供・移転(委託に伴うものを除く。) 6. 特定個人情報の保管・消去 7. 備考	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更に当たるため。
令和4年10月11日	(別添2) 特定個人情報ファイル記録項目		(4) 機構保存附票本人確認情報ファイル ア 附票本人確認情報 1. 住民票コード、2. 氏名 漢字、3. 氏名 外字数、4. 氏名 ふりがな、5. 生年月日、6. 性別、7. 住所 市町村コード、8. 住所 漢字、9. 住所 外字数、10. 最終住所 漢字、11. 最終住所 外字数、12. 異動年月日、13. 旧住民票コード、14. 附票管理市町村コード、15. 附票本人確認情報状態区分、16. 外字フラグ、17. 外字パターン、18. 通知区分 イ その他 1. 個人番号(※国外転出者に係る事務処理に関し、番号法で認められた場合に限り、国の機関等からの求めに応じ、当該個人の住民票コードを用いて、機構保存本人確認情報ファイルから個人番号を抽出し、提供する場合)	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更に当たるため。
令和4年10月11日	III 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 (2) 機構保存本人確認情報ファイル III-2 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、年に一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。	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(住基法第3条において、市町村の責務として、常に、住民基本台帳を整備し、住民に関する正確な記録が行われるように努めるとともに、住民に関する記録の管理が適正に行われるように必要な措置を講ずるよう努めることとされている)。 このため、年に一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。	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更に当たるため。
令和4年10月11日	III 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 (2) 機構保存本人確認情報ファイル III-3 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、住基全国サーバと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	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、附票連携システムと接続するが、特定個人情報の連携先は、①個人番号生成システム、②個人番号カード管理システム及び③附票連携システムに限られるよう、アクセス制御を行う。 なお、住基全国サーバと①、②、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) 住基全国サーバ⇒他のシステムへのアクセス ③附票連携システム : 番号法で認められた場合に限り、地方公共団体、行政機関等からの求めに応じ、国外転出者に係る個人番号を連携する場合。 (2) 他のシステム⇒住基全国サーバへのアクセス ③附票連携システム : 番号法で認められた場合に限り、地方公共団体、行政機関等からの求めに応じ、国外転出者に係る個人番号を入手する場合。	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更に当たるため。
令和4年10月11日	III 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 (2) 機構保存本人確認情報ファイル III-5 特定個人情報の提供・移転の記録 具体的方法	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、当該情報の提供記録(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。	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(番号法で認められた場合に限り、当該個人の住民票コードを用いて、「機構保存本人確認情報ファイル」から個人番号を抽出し、附票全国サーバに連携する場合を含む。)、当該情報の提供記録(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。	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更に当たるため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和4年10月11日	III 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 (2) 機構保存本人確認情報ファイル III-5 特定個人情報の提供・移転の記録 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。	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、提供先とは、提供に係る協定書を締結し、媒体の適切な保管及び廃棄を定めるとともに、セキュリティチェックリストにより、提供先機関における適切な保管及び廃棄を確認している。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。	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更に当たるため。
令和4年10月11日	III 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 (2) 機構保存本人確認情報ファイル III-5 リスク2 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、相手先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渡し時は複数人の立会いの下で行い、受渡し簿等に受渡しの記録を残す。	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、相手先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渡し時は、業務時間内に施錠可能なケースに格納して運搬した上で、複数人の立会いの下で受渡しを行い、受渡し簿等に相手が署名した受渡しの記録を残す。 国外転出者に係る事務処理に関し、番号法で認められた場合に限り、地方公共団体、行政機関等からの求めに応じ、個人番号を連携することを、システムにより担保する。	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更に当たるため。
令和4年10月11日	III 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 (2) 機構保存本人確認情報ファイル III-5 リスク3 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、情報連携の相手先は法令に定められた機関に限定されており、また、相手先(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。	・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。 : 媒体に書き込み後のデータについては、誤った情報が提供されないよう、月次で消去する。 ・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、情報連携の相手先は法令に定められた機関に限定されており、また、相手先(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。 : 媒体での提供時は、顔写真入りの身分証明書の提示を求め、本人確認を行っている。	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更に当たるため。
令和4年10月11日	III 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 (2) 機構保存本人確認情報ファイル III-7 リスク3 消去手順 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。	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(消去されたデータは、復元できない)。 なお、媒体による提供の場合には、書き込み後のデータを、作業チェックリストに基づき、月次で手動で消去する(消去されたデータは、復元できない)。 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。	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更に当たるため。

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和4年10月11日	III 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 (3) 個人番号カード用管理ファイル III-3 リスク1 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、④(株)DNPデータテクノに限られるよう、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①～④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。	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、④(株)DNPデータテクノ、⑤附票連携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①～⑤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 ⑤附票連携システム : 国外転出者に係る利用者情報照会を行う場合。ただし、住民票コードのみをキーとし、特定個人情報を使ったアクセスは行わない。 (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 ⑤附票連携システム : 市町村CSより附票都道府県サーバを経由して受領した国外転出者の異動情報を連携する場合(特定個人情報を含まない)。 : 個人番号カード管理システムからの国外転出者に係る利用者情報照会に基づき、附票本人確認情報を連携する場合(特定個人情報を含まない)。	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更に当たるため。
令和4年10月11日	III 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 (4) 機構保存附票本人確認情報ファイル		機構保存附票本人確認情報ファイルについて、以下の項目を記載 1. 特定個人情報ファイル名 2. 特定個人情報の入手 3. 特定個人情報の使用 4. 特定個人情報ファイルの取扱いの委託 5. 特定個人情報の提供・移転 6. 情報提供ネットワークシステムとの接続 7. 特定個人情報の保管・消去	事前	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更に当たるため。

(別添3) 変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年10月1日	II 特定個人情報ファイルの概要 (3) 個人番号カード用管理ファイル II - 2 ⑥事務担当部署	個人番号センター運用管理センター個人番号カードシステム部、個人番号センター運用管理センター運用部個人番号カードシステム運用担当	個人番号センター運用管理本部個人番号カード業務運用部、個人番号センター個人番号カードシステム開発部、個人番号センター運用管理本部個人番号カードシステム運用部	事後	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更にあたらないため。
令和5年10月1日	II 特定個人情報ファイルの概要 (3) 個人番号カード用管理ファイル II - 3 ⑦使用の主体 使用の部署	個人番号センター運用管理センター個人番号カードシステム部、個人番号センター運用管理センター運用部個人番号カードシステム運用担当	個人番号センター運用管理本部個人番号カード業務運用部、個人番号センター個人番号カードシステム開発部、個人番号センター運用管理本部個人番号カードシステム運用部	事後	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更にあたらないため。
令和5年10月1日	II 特定個人情報ファイルの概要 (3) 個人番号カード用管理ファイル II - 4 委託事項2 ⑥委託先名	・株式会社エヌ・ティ・ティ・データ、株式会社DNPデータテクノ、凸版印刷株式会社(申請受付事務及びカード発行事務)	・(株)NTTデータ、(株)DNPデータテクノ、TOPPAN(株)(申請受付事務及びカード発行事務)	事後	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更にあたらないため。
令和5年10月1日	II 特定個人情報ファイルの概要 (3) 個人番号カード用管理ファイル II - 4 委託事項3 ⑥委託先名	(株)NTTマーケティングアクトProCX、NTTコミュニケーションズ(株)	富士ソフトサービスビューロ(株)、エヌ・ティ・ティ・コミュニケーションズ(株)	事後	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更にあたらないため。
令和5年10月1日	IVその他のリスク対策 IV - 1. ①自己点検 具体的なチェック方法	NISC政府機関統一基準群への準拠性の確認のため、全部門を対象に自己点検を実施している。 特に、住基全国センターにおいては、NISC政府機関統一基準群、本人確認情報管理規程等に規定され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(年に一度)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。また、個人番号センター運用管理センター個人番号カードシステム部及び個人番号センター運用管理センター運用部個人番号カードシステム運用担当においては、NISC政府機関統一基準群、機構処理事務管理規程等に規定され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(年に一度)に職員による自己点検項目の遵守状況の確認を実施する。	NISC政府機関統一基準群への準拠性の確認のため、全部門を対象に自己点検を実施している。 特に、住基全国センターにおいては、NISC政府機関統一基準群、本人確認情報管理規程等に規定され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(年に一度)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。また、個人番号センター運用管理本部個人番号カード業務運用部、個人番号センター個人番号カードシステム開発部及び個人番号センター運用管理本部個人番号カードシステム運用部においては、NISC政府機関統一基準群、機構処理事務管理規程等に規定され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(年に一度)に職員による自己点検項目の遵守状況の確認を実施する。	事後	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更にあたらないため。
令和6年5月22日	表紙 特記事項	(省略) また、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に規定する個人番号、個人番号カード、特定個人情報の提供等に関する省令(平成26年11月20日総務省令第85号、以下「個人番号カード省令」という。)に基づき、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。	(省略) また、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に規定する個人番号、個人番号カード、特定個人情報の提供等に関する命令(平成26年11月20日総務省令第85号、以下「個人番号カード省令」という。)に基づき、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。	事後	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更にあたらないため。
令和6年5月22日	I 基本情報 1. 特定個人情報ファイルを取り扱う事務 2. 事務の内容 3. 個人番号カードに係る事務	(2)個人番号カードの交付申請受付・発行・市町村への送付 ・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元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)個人番号カードの交付申請受付・発行・市町村又は住民への送付 ・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元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。	事後	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更にあたらないため。
令和6年5月22日	(別添1) 事務の内容 (3) 個人番号カードに係る事務(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)	図のとおり。	図に矢印(赤色)を追加し、吹き出しを2つ「2-⑦送付」及び「2-⑨交付」を追加。	事後	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更にあたらないため。

(別添3) 変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年5月22日	(別添1) 事務の内容 (3) 個人番号カードに係る事務(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)-2.個人番号カードの交付申請受付・発行・市町村への送付 (省略) 2-⑦ 発行された個人番号カードを、送付先住所地の市町村長に対し送付する。 (省略) 2-⑨ 市町村長において、個人番号カードを住民に交付する。	(備考) (3)-2.個人番号カードの交付申請受付・発行・市町村への送付 (省略) 2-⑦ 発行された個人番号カードを、送付先住所地の市町村長又は住民に対し送付する。 (省略) 2-⑨ 市町村長又は機構において、個人番号カードを住民に交付する。	事後	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更にあたらないため。
令和6年5月22日	II 特定個人情報ファイルの概要 (3) 個人番号カード用管理ファイル 3. 特定個人情報の入手・使用 ④ 入手に係る妥当性	・交付申請書(交付申請者本人より入手) ・個人番号カード省令第21条において、交付申請書に記載すべき事項として交付申請者の氏名、住所、個人番号が規定されている。	・交付申請書(交付申請者本人より入手) ・個人番号カード省令第20条において、交付申請書に記載すべき事項として交付申請者の氏名、住所、個人番号が規定されている。	事後	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更にあたらないため。
令和6年5月22日	II 特定個人情報ファイルの概要 (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の取扱いの委託 委託事項2	個人番号カードの交付申請受付・発行・市町村への送付に係る事務	個人番号カードの交付申請受付・発行・市町村又は住民への送付に係る事務	事後	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更にあたらないため。
令和6年5月22日	II 特定個人情報ファイルの概要 (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の取扱いの委託 委託事項2 ① 委託内容	・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)	・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又は住民への送付に係る事務(カード発行事務)	事後	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更にあたらないため。
令和6年5月22日	II 特定個人情報ファイルの概要 (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の取扱いの委託 委託事項2 ② 取扱いを委託する特定個人情報ファイルの範囲 その妥当性	番号法第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。	番号法第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。また、改正番号法第16条の2第3項及び第17条第3項(令和6年12月2日施行予定)に基づき、住民からの申出により、その者に対し、当該個人番号カードを送付する必要がある。	事後	特定個人情報保護評価指針(令和4年4月1日個人情報保護委員会)に定める重要な変更にあたらないため。
令和6年11月8日	I 基本情報 1. 特定個人情報ファイルを取り扱う事務 ② 事務の内容	(略) 1. 個人番号の生成・通知に係る事務(※詳細は、「(別添1) 事務の内容」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(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。 (略) (3) 住民票コードの変更 ・住民基本台帳法(昭和42年7月25日法律第81号)(平成30年7月6日法律第71号施行時点)(以下「住基法」という。))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。 (略)	1. 個人番号の生成・通知に係る事務(※詳細は、「(別添1) 事務の内容」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(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。 (略) (3) 住民票コードの変更 ・住民基本台帳法(昭和42年7月25日法律第81号)(以下「住基法」という。))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。 (略)	事後	特定個人情報保護評価指針(令和6年5月27日個人情報保護委員会)に定める重要な変更にあたらないため。

(別添3) 変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年11月8日	Ⅰ 基本情報 1. 特定個人情報を取り扱う事務 ②事務の内容	(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。 ※本人確認情報の利用(個人番号カード管理システムへの本人確認情報の提供) 個人番号カードの交付申請後に機構保存本人確認情報+A7をもってカードの発行に用いられる送付先情報が最新かどうかを比較・突合し、古い住所や氏名でカードが発行され住民へ交付されるリスクを低減させる。 (略)	(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。 ※本人確認情報の利用(個人番号カード管理システムへの本人確認情報の提供) 個人番号カードの交付申請後に機構保存本人確認情報をもってカードの発行に用いられる送付先情報が最新かどうかを比較・突合し、古い住所や氏名でカードが発行され住民へ交付されるリスクを低減させる。 (略)	事後	特定個人情報保護評価指針(令和6年5月27日個人情報保護委員会)に定める重要な変更にあたらないため。
令和6年11月8日	Ⅰ 基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム システム4 ③他のシステムとの接続	表中で該当(○)となるもの ・住民基本台帳ネットワークシステム ・その他(個人番号カード管理システム)	表中で該当(○)となるもの ・情報提供ネットワークシステム ・住民基本台帳ネットワークシステム ・その他(個人番号カード管理システム)	事後	特定個人情報保護評価指針(令和6年5月27日個人情報保護委員会)に定める重要な変更にあたらないため。
令和6年11月8日	Ⅰ 基本情報 5. 個人番号の利用※法令上の根拠	2. 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) ・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(デジタル庁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) ・第30条の44の6第6項(附票本人確認情報(住民票コードに限る。))の利用	2. 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) ・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(デジタル庁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15の2第1項(準法定事務処理者への本人確認情報の提供等) ・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) ・第30条の44の6第6項(附票本人確認情報(住民票コードに限る。))の利用) ・第30条の44の7第1項(準法定事務処理者への附票本人確認情報の提供等)	事後	特定個人情報保護評価指針(令和6年5月27日個人情報保護委員会)に定める重要な変更にあたらないため。
令和6年11月8日	Ⅱ 特定個人情報ファイルの概要(1) 3. 特定個人情報の入手・使用 ③入手の時期・頻度	番号法施行日(平成27年10月5日)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。	個人番号とすべき番号の生成要求や、個人番号の変更要求を契機として、都度入手・生成し、ファイルに格納する。 なお、番号法施行日(平成27年10月5日)への対応として、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、ファイルに格納した。	事後	特定個人情報保護評価指針(令和6年5月27日個人情報保護委員会)に定める重要な変更にあたらないため。
令和6年11月8日	Ⅱ 特定個人情報ファイルの概要(1) 5. 特定個人情報の提供・移転(委託に伴うものを除く。) ⑦時期・頻度	番号法施行日(平成27年10月5日)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31年3月31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とすべき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。	市町村長からの個人番号とすべき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。 なお、番号法施行日(平成27年10月5日)における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とすべき番号を住所地市町村ごとにまとめて提供を行った。	事後	特定個人情報保護評価指針(令和6年5月27日個人情報保護委員会)に定める重要な変更にあたらないため。
令和6年11月8日	Ⅱ 特定個人情報ファイルの概要(2) 5. 特定個人情報の提供・移転(委託に伴うものを除く。) 提供先1 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)	(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) ・第30条の15の2第1項(準法定事務処理者への本人確認情報の提供等)	事後	特定個人情報保護評価指針(令和6年5月27日個人情報保護委員会)に定める重要な変更にあたらないため。

(別添3) 変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年11月8日	II 特定個人情報ファイルの概要(4) 2. 基本情報 ⑤保有開始日	「情報通信技術の活用による行政手続等に係る関係者の利便性の向上並びに行政運営の簡素化及び効率化を図るための行政手続等における情報通信の技術の利用に関する法律等の一部を改正する法律(令和元年法律第16号)」附則第1条第10号にて規定される公布から起算して5年を超えない範囲内の政令で定める日。	令和6年5月27日	事後	特定個人情報保護評価指針(令和6年5月27日個人情報保護委員会)に定める重要な変更にあたらないため。
令和6年11月8日	II 特定個人情報ファイルの概要(4) 3. 特定個人情報の入手・使用 ④入手に係る妥当性	法令に基づき、住民の利便の増進と国及び地方公共団体の行政の合理化に資するため、国外転出者に係る本人確認を行う上で、市町村の戸籍の附票の記載事項に変更が生じた都度、当該市町村を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。 ※なお、住基法第30条の44の6第6項に基づき、機構保存附票本人確認情報(住民票コードに限る。)を利用し、第30条の9又は第30条の10から第30条の12までの規定による事務について個人番号を提供することができる。とされている。 ※※附票連携システムは、住基ネットを利用して構築されている。住基ネットは、保有情報・利用の制限、内部の不正利用の防止、外部からの侵入防止など、セキュリティ確保のための様々な措置が講じられており、平成14年8月5日の稼働後、住基ネットへのハッキングや情報漏えいなどの事件や障害は一度も発生していない。	法令に基づき、住民の利便の増進と国及び地方公共団体の行政の合理化に資するため、国外転出者に係る本人確認を行う上で、市町村の戸籍の附票の記載事項に変更が生じた都度、当該市町村を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。 ※なお、住基法第30条の44の6第6項に基づき、機構保存附票本人確認情報(住民票コードに限る。)を利用し、第30条の9、第30条の10から第30条の12まで又は第30条の15の2第1項の規定による事務について個人番号を提供することができる。とされている。 ※※附票連携システムは、住基ネットを利用して構築されている。住基ネットは、保有情報・利用の制限、内部の不正利用の防止、外部からの侵入防止など、セキュリティ確保のための様々な措置が講じられており、平成14年8月5日の稼働後、住基ネットへのハッキングや情報漏えいなどの事件や障害は一度も発生していない。	事後	特定個人情報保護評価指針(令和6年5月27日個人情報保護委員会)に定める重要な変更にあたらないため。
令和6年11月8日	II 特定個人情報ファイルの概要(4) 3. 特定個人情報の入手・使用 ⑥使用目的	(略) ※番号法別表に掲げる事務につき、地方公共団体、行政機関等から国外転出者に係るものに関し求めがあった場合、個人番号をその都度抽出し、住基法第30条の9又は第30条の10から第30条の12までの規定による事務について提供する場合がある	(略) ※番号法別表に掲げる事務につき、地方公共団体、行政機関等から国外転出者に係るものに関し求めがあった場合、個人番号をその都度抽出し、住基法第30条の9、第30条の10から第30条の12まで又は第30条の15の2第1項の規定による事務について提供する場合がある。	事後	特定個人情報保護評価指針(令和6年5月27日個人情報保護委員会)に定める重要な変更にあたらないため。
令和6年11月8日	II 特定個人情報ファイルの概要(4) 5. 特定個人情報の提供・移転(委託に伴うものを除く。) 提供先1 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) ・第30条の44(国の機関等への附票本人確認情報の提供) ・第30条の44の3(附票通知都道府県の区域内の市町村の執行機関への附票本人確認情報の提供) ・第30条の44の4(附票通知都道府県以外の都道府県の執行機関への附票本人確認情報の提供) ・第30条の44の5(附票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附票本人確認情報の提供) ・第30条の44の6第6項(附票本人確認情報(住民票コードに限る。))の利用	(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) ・第30条の44(国の機関等への附票本人確認情報の提供) ・第30条の44の3(附票通知都道府県の区域内の市町村の執行機関への附票本人確認情報の提供) ・第30条の44の4(附票通知都道府県以外の都道府県の執行機関への附票本人確認情報の提供) ・第30条の44の5(附票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附票本人確認情報の提供) ・第30条の44の6第6項(附票本人確認情報(住民票コードに限る。))の利用 ・第30条の44の7第1項(準法定事務処理者への附票本人確認情報の提供等)	事後	特定個人情報保護評価指針(令和6年5月27日個人情報保護委員会)に定める重要な変更にあたらないため。
令和6年11月8日	II 特定個人情報ファイルの概要(4) 3. 特定個人情報の入手・使用 ⑨使用開始日	「情報通信技術の活用による行政手続等に係る関係者の利便性の向上並びに行政運営の簡素化及び効率化を図るための行政手続等における情報通信の技術の利用に関する法律等の一部を改正する法律(令和元年法律第16号)」附則第1条第10号にて規定される公布から起算して5年を超えない範囲内の政令で定める日。	令和6年5月27日	事後	特定個人情報保護評価指針(令和6年5月27日個人情報保護委員会)に定める重要な変更にあたらないため。

(別添3) 変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年11月8日	II 特定個人情報ファイルの概要 (4) 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	提供を行っている 2件	事後	特定個人情報保護評価指針 (令和6年5月27日個人情報保護委員会) に定める重要な変更にあたらないため。
令和6年11月8日	II 特定個人情報ファイルの概要 (2) 6. 特定個人情報の保管・消去 ②保管期間 その妥当性	・住民票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) 及び削除者の本人確認情報は、住基法施行令第30条の7 (機構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。	・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) 及び削除者の本人確認情報は、住民基本台帳法施行令 (昭和42年政令第292号) 第30条の7 (機構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。	事後	特定個人情報保護評価指針 (令和6年5月27日個人情報保護委員会) に定める重要な変更にあたらないため。
令和6年11月8日	III 特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 (1) 3. 特定個人情報の使用 リスク4: 特定個人情報ファイルが不正に複製されるリスク	・サーバのバックアップを記録した電子記録媒体 (バックアップ媒体) については、セキュリティゲートにて入退室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 (データ保管室) に設置した施錠可能な場所に保管する。	・サーバのバックアップを記録した電子記録媒体については、セキュリティゲートにて入退室管理をしている建物の中で、さらに入退室管理 (※) を行っている部屋に設置した施錠可能な場所に保管する。	事後	特定個人情報保護評価指針 (令和6年5月27日個人情報保護委員会) に定める重要な変更にあたらないため。
令和6年11月8日	III 特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 (2) 3. 特定個人情報の使用 リスク2: 権限のない者 (元職員、アクセス権限のない職員等) によって不正に使用されるリスク ユーザ認証の管理 具体的な管理方法	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する機関では、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、ユーザ認証を実施するよう要求する。 ※ 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。	・機構が提供するアプリケーションを任意で使用する機関では、ユーザ認証を実施するとともに、情報利用に係る証跡 (ログ) を取得することにより、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機関に対しては、ユーザ認証を実施するよう要求する。 ・自動連携機能 (※※) を利用する機関に対しては、端末のユーザ認証や物理的対策を実施するとともに、自ら管理する庁内システムへのアクセス制限、操作ログ分析などを適切に行うよう要求する。 ※ 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。 ※※ 自動連携機能: 庁内システムに登録した照会ファイルについて、情報提供サーバで行っていた手動の送信操作を省き、自動的に全国サーバへ連携する機能のこと。機構が提供するAPI (※) を元に各機関が当該機能の独自開発を行い、庁内システムに搭載している。	事後	特定個人情報保護評価指針 (令和6年5月27日個人情報保護委員会) に定める重要な変更にあたらないため。
令和6年11月8日	III 特定個人情報ファイルの取り扱いプロセスにおけるリスク対策 (2) 5. 特定個人情報の提供・移転 (委託や情報提供ネットワークシステムを通じた提供を除く。) リスク2: 不適切な方法で提供・移転が行われるリスク リスクに対する措置の内容	連携手段として通信の記録が逐一保存され、また、連携するデータが暗号化される仕組みが確立した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、相手先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渡し時は、業務時間内に施錠可能なケースに格納して運搬した上で、複数人の立会いの下で受渡しを行い、受渡し簿等に相手が署名した受渡しの記録を残す。 国外転出者に係る事務処理に関し、番号法で認められた場合に限り、地方公共団体、行政機関等からの求めに応じ、個人番号を連携することを、システムにより担保する。	連携手段として通信の記録が逐一保存され、また、連携するデータが暗号化される仕組みが確立した住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、相手先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渡し時は、業務時間内に施錠可能なケースに格納して運搬した上で、複数人の立会いの下で受渡しを行い、受渡し簿等に相手が署名した受渡しの記録を残す。 国外転出者に係る事務処理に関し、番号法で認められた場合に限り、地方公共団体、行政機関等からの求めに応じ、個人番号を連携することを、システムにより担保する。	事後	特定個人情報保護評価指針 (令和6年5月27日個人情報保護委員会) に定める重要な変更にあたらないため。

(別添3) 変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年11月8日	III 特定個人情報ファイルの 取り扱いプロセスにおけるリ スク対策 (4) 3. 特定個人情報の使用 リスク2: 権限のない者 (元職 員、アクセス権限のない職員 等) によって不正に使用され るリスク ユーザ認証の管理 具体的な管理方法	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、ユーザ認証 を実装するよう要求する。	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、ユーザ認証を実施する とともに、情報利用に係る証跡 (ログ) を取得 することにより、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 を行い利用する機関に対しては、ユーザ認証 を実装するよう要求する。	事後	特定個人情報保護評価指針 (令和6年5月27日個人情報 保護委員会) に定める重要な 変更にあたらないため。
令和6年11月8日	(別添2) ファイル記録項目	(1) ~ (3) (略) (4) 機構保存附票本人確認情報ファイル ア 附票本人確認情報 1. 住民票コード、2. 氏名 漢字、3. 氏名 外 字数、4. 氏名 ふりがな、5. 生年月日、6. 性別、7. 住所 市町村コード、8. 住所 漢 字、9. 住所 外字数、10. 最終住所 漢字、 11. 最終住所 外字数、12. 異動年月日、1 3. 旧住民票コード、14. 附票管理市町村 コード、15. 附票本人確認情報状態区分、1 6. 外字フラグ、17. 外字パターン、18. 通知 区分	(1) ~ (3) (略) (4) 機構保存附票本人確認情報ファイル ア 附票本人確認情報 1. 住民票コード、2. 氏名 漢字、3. 氏名 外 字数、4. 氏名 ふりがな、5. 生年月日、6. 性別、7. 住所 市町村コード、8. 住所 漢 字、9. 住所 外字数、10. 最終住所 漢字、 11. 最終住所 外字数、12. 異動年月日、1 3. 旧住民票コード、14. 附票管理市町村 コード、15. 附票本人確認情報状態区分、1 6. 外字フラグ、17. 外字パターン、18. 通知 区分、19. 旧氏 漢字、20. 旧氏 外字数、2 1. 旧氏 ふりがな、22. 旧氏 外字変更連番	事後	特定個人情報保護評価指針 (令和6年5月27日個人情報 保護委員会) に定める重要な 変更にあたらないため。

(別添3) 変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年1月31日	Ⅰ 基本情報 1. 特定個人情報ファイルを取り扱う事務 ②事務の内容	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」及び「4. 附票本人確認情報の提供及び保存等に係る事務」に分かれる。	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」、「4. 附票本人確認情報の提供及び保存等に係る事務」及び「5. カード代替電磁的記録に係る事務」に分かれる。	事前	特定個人情報保護評価指針(令和6年5月27日個人情報保護委員会)に定める重要な変更に当たるため。
令和7年1月31日	Ⅰ 基本情報 1. 特定個人情報ファイルを取り扱う事務 ②事務の内容		「5. カード代替電磁的記録に係る事務」について、以下の項目を記載 5. カード代替電磁的記録に係る事務 (1)カード代替電磁的記録の発行 (2)カード代替電磁的記録の失効 (3)カード代替電磁的記録の更新 (4)カード代替電磁的記録の一時利用停止	事前	特定個人情報保護評価指針(令和6年5月27日個人情報保護委員会)に定める重要な変更に当たるため。
令和7年1月31日	Ⅰ 基本情報 1. 特定個人情報ファイルを取り扱う事務 ③対象人数		30万人以上	事前	特定個人情報保護評価指針(令和6年5月27日個人情報保護委員会)に定める重要な変更に当たるため。
令和7年1月31日	Ⅰ 基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム システム5		「5. カード代替電磁的記録に係る事務」に対応するmdoc発行管理システムについて以下の項目を記載 ①システムの名 ②システムの機能 ③他のシステムとの接続	事前	特定個人情報保護評価指針(令和6年5月27日個人情報保護委員会)に定める重要な変更に当たるため。
令和7年1月31日	Ⅰ 基本情報 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) 機構保存附票本人確認情報ファイル	(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) 機構保存附票本人確認情報ファイル (5) カード代替電磁的記録用ファイル	事前	特定個人情報保護評価指針(令和6年5月27日個人情報保護委員会)に定める重要な変更に当たるため。
令和7年1月31日	Ⅰ 基本情報 4. 特定個人情報ファイルを取り扱う理由 ①事務実施上の必要性		「5. カード代替電磁的記録に係る事務」について以下の項目を記載 (5) カード代替電磁的記録用ファイル ①カード代替電磁的記録を発行し、利用者のスマートフォンに送信する。 ②カード代替電磁的記録の発行状況を管理する。	事前	特定個人情報保護評価指針(令和6年5月27日個人情報保護委員会)に定める重要な変更に当たるため。
令和7年1月31日	Ⅰ 基本情報 5. 個人番号の利用法令上の根拠	1. 番号法 ・第8条(個人番号とすべき番号の生成) ・第16条の2(個人番号カードの発行等) ・第17条第1項、第3項、第6項(個人番号カードの交付等)	1. 番号法 ・第8条(個人番号とすべき番号の生成) ・第16条の2(個人番号カードの発行等) ・第17条第1項、第3項、第6項(個人番号カードの交付等) ・第18条の2(カード代替電磁的記録の発行等)	事前	特定個人情報保護評価指針(令和6年5月27日個人情報保護委員会)に定める重要な変更に当たるため。
令和7年1月31日	Ⅰ 基本情報 7. 評価実施機関における担当部署		「5. カード代替電磁的記録に係る事務」の担当部署を記載 ①部署 (5)個人番号センター ②所属長の役職名 (5)センター長	事前	特定個人情報保護評価指針(令和6年5月27日個人情報保護委員会)に定める重要な変更に当たるため。

(別添3) 変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年1月31日	(別添1) 事務内容(前提) (別添1) 事務の内容 (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。	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。 (注) カード代替電磁的記録に係る事務については、(5) カード代替電磁的記録に係る事務を参照。	事前	特定個人情報保護評価指針(令和6年5月27日個人情報保護委員会)に定める重要な変更に当たるため。
令和7年1月31日	(別添1) 事務内容(5)		(5)カード代替電磁的記録に係る事務について以下の項目を記載 システム構成図 (備考)	事前	特定個人情報保護評価指針(令和6年5月27日個人情報保護委員会)に定める重要な変更に当たるため。
令和7年1月31日	II ファイルの概要(5)		(5)カード代替電磁的記録用管理ファイルについて以下の項目を記載 1. 特定個人情報ファイル名 2. 基本情報 3. 特定個人情報の入手・使用 4. 特定個人情報ファイルの取扱いの委託 5. 特定個人情報の提供・移転(委託に伴うものを除く。) 6. 特定個人情報の保管・消去 7. 備考	事前	特定個人情報保護評価指針(令和6年5月27日個人情報保護委員会)に定める重要な変更に当たるため。
令和7年1月31日	(別添2) ファイル記録項目 (別添2) 特定個人情報 ファイル記録項目		(5) カード代替電磁的記録用ファイルについて以下の項目を記載 (5) カード代替電磁的記録用ファイル ア 申請情報 イ mdoc管理情報 ウ 所有者資格情報 エ 所有者資格情報履歴	事前	特定個人情報保護評価指針(令和6年5月27日個人情報保護委員会)に定める重要な変更に当たるため。
令和7年1月31日	III リスク対策(プロセス) (5)		(5) カード代替電磁的記録用ファイルについて以下の項目を記載 1. 特定個人情報ファイル名 2. 特定個人情報の入手 3. 特定個人情報の使用 4. 特定個人情報ファイルの取扱いの委託 5. 特定個人情報の提供・移転 6. 情報提供ネットワークシステムとの接続 7. 特定個人情報の保管・消去	事前	特定個人情報保護評価指針(令和6年5月27日個人情報保護委員会)に定める重要な変更に当たるため。
令和7年1月31日	VI その他のリスク対策 3. その他のリスク対策	(略) ・特定個人情報を取り扱うシステムの調達・構築・運用等に当たっては、サプライチェーンリスクの管理に努める。	(略) ・特定個人情報を取り扱うシステムの調達・構築・運用等に当たっては、サプライチェーンリスクの管理に努める。 ・カード代替電磁的記録が格納されたスマートフォンの紛失・盗難等の発生に備え、委託事業者(コールセンター事務)又はオンライン申告による、速やかにカード代替電磁的記録を一時的に停止するための手続を設けており、また、当該手続の内容について周知をしている。 ・利用者が行政機関や民間事業者等が提供するサービスを利用するためにスマートフォンからカード代替電磁的記録を送信する場合、利用者本人の生体認証等を利用するため、第三者のなりすましは不可となっている。	事前	特定個人情報保護評価指針(令和6年5月27日個人情報保護委員会)に定める重要な変更に当たるため。

(別添3) 変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年6月10日	I 基本情報 7. 評価実施機関における 担当部署 ①部署	(1)住民基本台帳ネットワークシステム全国センター (2)住民基本台帳ネットワークシステム全国センター (3)個人番号センター (4)住民基本台帳ネットワークシステム全国センター (5)個人番号センター	(1)住民基本台帳ネットワークシステム全国センター (2)住民基本台帳ネットワークシステム全国センター (3)個人番号センター、コンタクトセンター (4)住民基本台帳ネットワークシステム全国センター (5)個人番号センター、コンタクトセンター	事後	特定個人情報保護評価指針(令和7年4月1日個人情報保護委員会)に定める重要な変更にあたらないため。
令和7年6月10日	II 特定個人情報ファイルの概要 (3) 個人番号カード用管理ファイル II - 2 ⑥事務担当部署	個人番号センター運用管理センター個人番号カードシステム部、個人番号センター運用管理センター運用部個人番号カードシステム運用担当	個人番号センター運用管理本部個人番号カード業務運用部、個人番号センター個人番号カードシステム開発部、個人番号センター運用管理本部個人番号カードシステム運用部、コンタクトセンター	事後	特定個人情報保護評価指針(令和7年4月1日個人情報保護委員会)に定める重要な変更にあたらないため。
令和7年6月10日	II 特定個人情報ファイルの概要 (3) 個人番号カード用管理ファイル II - 3 ⑦使用の主体 使用部署	個人番号センター運用管理センター個人番号カードシステム部、個人番号センター運用管理センター運用部個人番号カードシステム運用担当	個人番号センター運用管理本部個人番号カード業務運用部、個人番号センター個人番号カードシステム開発部、個人番号センター運用管理本部個人番号カードシステム運用部、コンタクトセンター	事後	特定個人情報保護評価指針(令和7年4月1日個人情報保護委員会)に定める重要な変更にあたらないため。
令和7年6月10日	II 特定個人情報ファイルの概要 (3) 個人番号カード用管理ファイル II - 4 委託事項3 ⑥委託先名	富士ソフトサービスビューロ(株)、エヌ・ティ・ティ・コミュニケーションズ(株)	富士ソフトサービスビューロ(株)、(株)ベルシステム24	事後	特定個人情報保護評価指針(令和7年4月1日個人情報保護委員会)に定める重要な変更にあたらないため。

(別添3) 変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年6月10日	IVその他のリスク対策 IV- 1. ①自己点検 具体的なチェック方法	NISC政府機関統一基準群への準拠性の確認のため、全部門を対象に自己点検を実施している。 特に、住基全国センターにおいては、NISC政府機関統一基準群、本人確認情報管理規程等に規定され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(年に一度)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。また、個人番号センター運用管理本部個人番号カード業務運用部、個人番号センター個人番号カードシステム開発部及び個人番号センター運用管理本部個人番号カードシステム運用部においては、NISC政府機関統一基準群、機構処理事務管理規程等に規定され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(年に一度)に職員による自己点検項目の遵守状況の確認を実施する。	NISC政府機関統一基準群への準拠性の確認のため、全部門を対象に自己点検を実施している。 特に、住基全国センターにおいては、NISC政府機関統一基準群、本人確認情報管理規程等に規定され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(年に一度)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。また、個人番号センター運用管理本部個人番号カード業務運用部、個人番号センター個人番号カードシステム開発部、個人番号センター運用管理本部個人番号カードシステム運用部及びコンタクトセンターにおいては、NISC政府機関統一基準群、機構処理事務管理規程等に規定され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(年に一度)に職員による自己点検項目の遵守状況の確認を実施する。	事後	特定個人情報保護評価指針(令和7年4月1日個人情報保護委員会)に定める重要な変更にあたらないため。
令和7年6月10日	(別添2) ファイル記録項目 (別添2) 特定個人情報 ファイル記録項目	(3) 個人番号カード用管理ファイル (略)、115. ローマ字 旧氏	(3) 個人番号カード用管理ファイル (略)、115. ローマ字 旧氏、116. 一体化情報コード、117. 特定在留カード等の有効期限	事前	特定個人情報保護評価指針(令和7年4月1日個人情報保護委員会)に定める重要な変更にあたらないため。
令和7年6月10日	I 基本情報 1. 特定個人情報ファイル を取り扱う事務 ②事務の内容 3. 個人番号カードに係る 事務	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、個人番号カード省令第23条から第23条の3まで及び第35条第1項に基づき、個人番号通知書及び個人番号カードに係る以下の事務を行う。	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。また、番号法第18条の5第2項により、機構は、特定在留カード等について、個人番号の記載及びその電磁的方法による記録その他個人番号カードとしての機能を付加するための措置を講ずることとされている。 機構は、個人番号カード省令第23条から第23条の3まで及び第35条第1項に基づき、個人番号通知書及び個人番号カードに係る以下の事務を行う。	事前	特定個人情報保護評価指針(令和7年4月1日個人情報保護委員会)に定める重要な変更にあたらないため。
令和8年6月22日	表紙 個人のプライバシー等の 権利利益の保護の宣言 特記事項	・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。 (略)	・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、5情報(氏名、氏名の振り仮名、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。 (略)	事後	特定個人情報保護評価指針(令和7年7月15日個人情報保護委員会)に定める重要な変更にあたらないため。
令和8年6月22日	I 基本情報 1. 特定個人情報ファイル を取り扱う事務 ②事務の内容 2. 本人確認情報の提供 及び保存に係る事務	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、性別、生年月日)、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に係る以下の事務を実施する。 (略)	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、5情報(氏名、氏名の振り仮名、住所、性別、生年月日)、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に係る以下の事務を実施する。 (略)	事後	特定個人情報保護評価指針(令和7年7月15日個人情報保護委員会)に定める重要な変更にあたらないため。

(別添3) 変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和8年6月22日	① 基本情報 1. 特定個人情報ファイルを取り扱う事務 ② 事務の内容 2. 本人確認情報の提供及び保存に係る事務	(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。 ※国外転出者に係る事務処理に関し、番号法で認められた場合に限り、国の機関等からの求めに応じ、当該個人の住民票コードを用いて、機構保存本人確認情報ファイルから個人番号を抽出し、附票全国サーバに連携する場合がある。	(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、5情報又はその他機構保存本人確認情報ファイル記録項目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。 ※国外転出者に係る事務処理に関し、番号法で認められた場合に限り、国の機関等からの求めに応じ、当該個人の住民票コードを用いて、機構保存本人確認情報ファイルから個人番号を抽出し、附票全国サーバに連携する場合がある。	事後	特定個人情報保護評価指針(令和7年7月15日個人情報保護委員会)に定める重要な変更にあたらないため。
令和8年6月22日	① 基本情報 1. 特定個人情報ファイルを取り扱う事務 ② 事務の内容 4. 附票本人確認情報の提供及び保存に係る事務	機構は、市町村における市町村CS、都道府県における附票都道府県サーバ及び機構における附票全国サーバ等により構成される「附票連携システム」において、国外転出者に係る本人確認を行うための社会的基盤としての役割を担うため、4情報(氏名、住所、性別、生年月日)、住民票コード及びこれらの変更情報で構成される「機構保存附票本人確認情報ファイル」を作成し、戸籍の附票に関する記録を正確に行う責務がある。そのため、附票本人確認情報の提供及び保存に係る以下の事務を実施する。なお、機構保存附票本人確認情報(以下「附票本人確認情報」という場合もある。)には、個人番号は含まれない。 (略)	機構は、市町村における市町村CS、都道府県における附票都道府県サーバ及び機構における附票全国サーバ等により構成される「附票連携システム」において、国外転出者に係る本人確認を行うための社会的基盤としての役割を担うため、5情報(氏名、氏名の振り仮名、住所、性別、生年月日)、住民票コード及びこれらの変更情報で構成される「機構保存附票本人確認情報ファイル」を作成し、戸籍の附票に関する記録を正確に行う責務がある。そのため、附票本人確認情報の提供及び保存に係る以下の事務を実施する。なお、機構保存附票本人確認情報(以下「附票本人確認情報」という場合もある。)には、個人番号は含まれない。 (略)	事後	特定個人情報保護評価指針(令和7年7月15日個人情報保護委員会)に定める重要な変更にあたらないため。
令和8年6月22日	① 基本情報 1. 特定個人情報ファイルを取り扱う事務 ② 事務の内容 4. 附票本人確認情報の提供及び保存に係る事務	(2)市町村長等への附票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、国外転出者に係る事務処理に関し、照会のあった当該個人の4情報等に対応付く附票本人確認情報を機構保存附票本人確認情報ファイルから抽出し、照会元に提供する。その際、番号法で認められた場合に限り、附票本人確認情報の提供に併せて、当該個人の住民票コードを用いて機構保存本人確認情報ファイルから個人番号を抽出し、照会元に提供する場合がある。	(2)市町村長等への附票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、国外転出者に係る事務処理に関し、照会のあった当該個人の5情報等に対応付く附票本人確認情報を機構保存附票本人確認情報ファイルから抽出し、照会元に提供する。その際、番号法で認められた場合に限り、附票本人確認情報の提供に併せて、当該個人の住民票コードを用いて機構保存本人確認情報ファイルから個人番号を抽出し、照会元に提供する場合がある。	事後	特定個人情報保護評価指針(令和7年7月15日個人情報保護委員会)に定める重要な変更にあたらないため。
令和8年6月22日	① 基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム システム2 ② システムの機能	(「2. 本人確認情報の提供及び保存等に係る事務」に対応) (略) ・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。 ※国外転出者に係る事務処理に関し、番号法で認められた場合に限り、国の機関等からの求めに応じ、当該個人の住民票コードを用いて、機構保存本人確認情報ファイルから個人番号を抽出し、附票全国サーバに連携する場合がある。 (略)	(「2. 本人確認情報の提供及び保存等に係る事務」に対応) (略) ・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5情報等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。 ※国外転出者に係る事務処理に関し、番号法で認められた場合に限り、国の機関等からの求めに応じ、当該個人の住民票コードを用いて、機構保存本人確認情報ファイルから個人番号を抽出し、附票全国サーバに連携する場合がある。 (略)	事後	特定個人情報保護評価指針(令和7年7月15日個人情報保護委員会)に定める重要な変更にあたらないため。

(別添3) 変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和8年6月22日	Ⅰ 基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム4 ②システムの機能	(「4. 附票本人確認情報の提供及び保存等に係る事務」に対応) (略) ・市町村長等からオンライン又は媒体で国外転出者に係る附票本人確認情報照会要求を受け取り、住民票コード又は4情報の組合せにより機構保存附票本人確認情報ファイルを検索する。附票本人確認情報照会要求により検索した、附票本人確認情報を市町村長等へ提供する。その際、番号法で認められた場合に限り、国の機関等からの求めに応じ、附票本人確認情報の提供に併せて当該個人の住民票コードを用いて、機構保存本人確認情報ファイルから個人番号を抽出し、照会元に提供する場合がある。 (略)	(「4. 附票本人確認情報の提供及び保存等に係る事務」に対応) (略) ・市町村長等からオンライン又は媒体で国外転出者に係る附票本人確認情報照会要求を受け取り、住民票コード又は5情報の組合せにより機構保存附票本人確認情報ファイルを検索する。附票本人確認情報照会要求により検索した、附票本人確認情報を市町村長等へ提供する。その際、番号法で認められた場合に限り、国の機関等からの求めに応じ、附票本人確認情報の提供に併せて当該個人の住民票コードを用いて、機構保存本人確認情報ファイルから個人番号を抽出し、照会元に提供する場合がある。 (略)	事後	特定個人情報保護評価指針(令和7年7月15日個人情報保護委員会)に定める重要な変更にあたらないため。
令和8年6月22日	Ⅰ 基本情報 (別添1) 事務の内容 [前提] 番号制度全体における機構の役割(概要)	概要図中 「4情報等」	概要図中 「5情報等」	事後	特定個人情報保護評価指針(令和7年7月15日個人情報保護委員会)に定める重要な変更にあたらないため。
令和8年6月22日	Ⅰ 基本情報 (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事務	概要図中 「個人番号or4情報等」	概要図中 「個人番号or5情報等」	事後	特定個人情報保護評価指針(令和7年7月15日個人情報保護委員会)に定める重要な変更にあたらないため。
令和8年6月22日	Ⅰ 基本情報 (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事務	(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。 (略)	(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5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。 (略)	事後	特定個人情報保護評価指針(令和7年7月15日個人情報保護委員会)に定める重要な変更にあたらないため。
令和8年6月22日	Ⅰ 基本情報 (別添1) 事務の内容 (4) 附票本人確認情報の提供及び保存等に係る事務	概要図中 「4情報等」	概要図中 「5情報等」	事後	特定個人情報保護評価指針(令和7年7月15日個人情報保護委員会)に定める重要な変更にあたらないため。
令和8年6月22日	Ⅰ 基本情報 (別添1) 事務の内容 (4) 附票本人確認情報の提供及び保存等に係る事務	(4)-2.市町村長、都道府県知事、国の機関等への附票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、4情報等をキーワードとした国外転出者に係る附票本人確認情報の照会を受ける。 (略)	(4)-2.市町村長、都道府県知事、国の機関等への附票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、5情報等をキーワードとした国外転出者に係る附票本人確認情報の照会を受ける。 (略)	事後	特定個人情報保護評価指針(令和7年7月15日個人情報保護委員会)に定める重要な変更にあたらないため。

(別添3) 変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和8年6月22日	II 特定個人情報ファイルの概要(2) 2. 基本情報 ④記録される項目 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。	・個人番号、5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、5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。	事後	特定個人情報保護評価指針(令和7年7月15日個人情報保護委員会)に定める重要な変更にあたらないため。
令和8年6月22日	II 特定個人情報ファイルの概要(2) 3. 特定個人情報の入手・使用 ⑧使用方法 ※	(略) ・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)。 (略)	(略) ・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5情報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)。 (略)	事後	特定個人情報保護評価指針(令和7年7月15日個人情報保護委員会)に定める重要な変更にあたらないため。
令和8年6月22日	II 特定個人情報ファイルの概要(2) 3. 特定個人情報の入手・使用 ⑧使用方法 情報の突合 ※	(略) ・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。 (略) ・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。	(略) ・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5情報等との突合を行う。 (略) ・都道府県サーバとの整合処理を実施するため、5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。	事後	特定個人情報保護評価指針(令和7年7月15日個人情報保護委員会)に定める重要な変更にあたらないため。
令和8年6月22日	II 特定個人情報ファイルの概要(2) 5. 特定個人情報の提供・移転(委託に伴うものを除く) 提供先1 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	住民票コード、氏名、氏名の振り仮名、住所、生年月日、性別、個人番号、異動事由、異動年月日	事後	特定個人情報保護評価指針(令和7年7月15日個人情報保護委員会)に定める重要な変更にあたらないため。
令和8年6月22日	II 特定個人情報ファイルの概要(2) 5. 特定個人情報の提供・移転(委託に伴うものを除く) 提供先3 ③提供する情報	住民票コード、氏名、住所、生年月日、性別、個人番号、異動事由、異動年月日	住民票コード、氏名、氏名の振り仮名、住所、生年月日、性別、個人番号、異動事由、異動年月日	事後	特定個人情報保護評価指針(令和7年7月15日個人情報保護委員会)に定める重要な変更にあたらないため。
令和8年6月22日	II 特定個人情報ファイルの概要(4) 2. 基本情報 ④記録される項目 その妥当性	・4情報、その他戸籍の附票関係情報(戸籍の表示に係る情報は含まない。) :法令に基づき戸籍の附票に記録された者に関する記録を正確に行う上で、戸籍の附票の記載等に係る附票本人確認情報(4情報、住民票コード及びこれらの変更情報)を記録する必要がある。なお、別添2に記載のとおり、記録項目には戸籍の表示に係る情報(本籍及び筆頭者の氏名)は含まない。 (略)	・5情報、その他戸籍の附票関係情報(戸籍の表示に係る情報は含まない。) :法令に基づき戸籍の附票に記録された者に関する記録を正確に行う上で、戸籍の附票の記載等に係る附票本人確認情報(5情報、住民票コード及びこれらの変更情報)を記録する必要がある。なお、別添2に記載のとおり、記録項目には戸籍の表示に係る情報(本籍及び筆頭者の氏名)は含まない。 (略)	事後	特定個人情報保護評価指針(令和7年7月15日個人情報保護委員会)に定める重要な変更にあたらないため。

(別添3) 変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和8年6月22日	II 特定個人情報ファイルの概要 (4) 3. 特定個人情報の入手・使用 ⑥使用目的 ※	本特定個人情報ファイル(機構保存本人確認情報ファイル)において戸籍の附票に記録された全ての者の情報を保有し、その記録を常に正確に更新・管理・提供する。 (略)	本特定個人情報ファイル(機構保存附票本人確認情報ファイル)において戸籍の附票に記録された全ての者の情報を保有し、その記録を常に正確に更新・管理・提供する。 (略)	事後	特定個人情報保護評価指針(令和7年7月15日個人情報保護委員会)に定める重要な変更に当たらないため。
令和8年6月22日	II 特定個人情報ファイルの概要 (4) 3. 特定個人情報の入手・使用 ⑧使用方法 ※	・市町村長等からの附票本人確認情報の照会要求を受け(例:市町村CS→附票全国サーバ)、国外転出者に係る事務に関し、照会のあった住民票コード又は4情報の組合せを元に機構保存附票本人確認情報ファイルを検索し、該当する個人の附票本人確認情報を照会元へ提供する(例:附票全国サーバ→市町村CS)。 (略)	・市町村長等からの附票本人確認情報の照会要求を受け(例:市町村CS→附票全国サーバ)、国外転出者に係る事務に関し、照会のあった住民票コード又は5情報の組合せを元に機構保存附票本人確認情報ファイルを検索し、該当する個人の附票本人確認情報を照会元へ提供する(例:附票全国サーバ→市町村CS)。 (略)	事後	特定個人情報保護評価指針(令和7年7月15日個人情報保護委員会)に定める重要な変更に当たらないため。
令和8年6月22日	II 特定個人情報ファイルの概要 (4) 5. 特定個人情報の提供・移転(委託に伴うものを除く。) 提供先1 ③提供する情報	住民票コード、氏名、住所、生年月日、性別、個人番号(番号法に基づく国の機関等からの求めがあった場合に限り。)	住民票コード、氏名、氏名の振り仮名、住所、生年月日、性別、個人番号(番号法に基づく国の機関等からの求めがあった場合に限り。)	事後	特定個人情報保護評価指針(令和7年7月15日個人情報保護委員会)に定める重要な変更に当たらないため。
令和8年6月22日	II 特定個人情報ファイルの概要 (5) カード代替電磁的記録用管理ファイル 4. 特定個人情報ファイルの取扱いの委託 ③委託先における取扱者数	*調達結果が判明次第お示しする。	100人以上500人未満	事前	特定個人情報保護評価指針(令和7年7月15日個人情報保護委員会)に定める重要な変更に当たらないため。
令和8年6月22日	II 特定個人情報ファイルの概要 (5) カード代替電磁的記録用管理ファイル 4. 特定個人情報ファイルの取扱いの委託 ⑥委託先名	*調達結果が判明次第お示しする。	株式会社NTTデータ、パナソニック コネクト株式会社	事前	特定個人情報保護評価指針(令和7年7月15日個人情報保護委員会)に定める重要な変更に当たらないため。
令和8年6月22日	II 特定個人情報ファイルの概要 (5) カード代替電磁的記録用管理ファイル 4. 特定個人情報ファイルの取扱いの委託 ⑦再委託の有無	再委託しない	再委託する	事前	特定個人情報保護評価指針(令和7年7月15日個人情報保護委員会)に定める重要な変更に当たらないため。
令和8年6月22日	II 特定個人情報ファイルの概要 (5) カード代替電磁的記録用管理ファイル 4. 特定個人情報ファイルの取扱いの委託 ⑧再委託の許諾方法		原則として再委託は行わないこととするが、再委託を行う場合は、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を経た後に承認する。	事前	特定個人情報保護評価指針(令和7年7月15日個人情報保護委員会)に定める重要な変更に当たらないため。

(別添3) 変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和8年6月22日	II 特定個人情報ファイルの概要 (5) カード代替電磁的記録用管理ファイル 4. 特定個人情報ファイルの取扱いの委託 ⑨再委託事項		mdoc発行管理システムの運用保守	事前	特定個人情報保護評価指針(令和7年7月15日個人情報保護委員会)に定める重要な変更にあたらないため。
令和8年6月22日	(別添2) ファイル記録項目 (別添2) 特定個人情報ファイル記録項目 (5) カード代替電磁的記録用ファイル ア 申請情報	41. 待機コマンド送信フラグ、42. 待機コマンド送信フラグ、43. 解除契機申請ID、44. カンパセーションID、45. 発行紐付けタスクID、46. 発行紐付けステータス、47. 待機コマンドタスクID、48. 確定コマンドタスクID、49. APDUレスポンス、50. セキュア領域制御公開鍵証明書、51. 補助セキュア領域鍵ID、52. 補助セキュア領域鍵、53. 補助セキュア領域証明書、54. サービス提供者セキュア領域証明書シリアル番号、55. アプレットバージョン、56. プラットフォームバージョン、57. 暗号化データ、58. 電文ID、59. デバイストークン、60. リクエスト理由コード、61. コミットメントS2、62. 登録日時、63. 更新日時	41. バンドル更新失敗受信日時、42. 待機コマンド送信フラグ、43. 待機コマンド結果受信フラグ、44. 確定コマンド受信結果フラグ、45. サブミットコマンド受信結果受信ステータス、46. バス管理受信フラグ、47. 解除契機申請ID、48. カンパセーションID、49. 発行紐付けタスクID、50. 発行紐付けステータス、51. 待機コマンドタスクID、52. 確定コマンドタスクID、53. APDUレスポンス、54. セキュア領域制御公開鍵証明書、55. 補助セキュア領域鍵ID、56. 補助セキュア領域鍵、57. 補助セキュア領域証明書、58. サービス提供者セキュア領域証明書シリアル番号、59. アプレットバージョン、60. プラットフォームバージョン、61. 暗号化データ、62. 電文ID、63. デバイストークン、64. リクエスト理由コード、65. コミットメントS2、66. 登録日時、67. 更新日時、68. バンドル更新送信ID	事前	特定個人情報保護評価指針(令和7年7月15日個人情報保護委員会)に定める重要な変更にあたらないため。
令和8年6月22日	(別添2) ファイル記録項目 (別添2) 特定個人情報ファイル記録項目 (5) カード代替電磁的記録用ファイル イ mdoc管理情報	(略) 9. 生年月日、10. 生年月日(検索用)、11. mdoc最終送信日時(略)	(略) 9. 生年月日(検索用)、10. mdoc最終送信日時、11. MSO有効期限(略)	事前	特定個人情報保護評価指針(令和7年7月15日個人情報保護委員会)に定める重要な変更にあたらないため。
令和8年6月22日	(別添2) ファイル記録項目 (別添2) 特定個人情報ファイル記録項目 (5) カード代替電磁的記録用ファイル ウ 所有者資格情報	(略) 4. 資格情報ステータス、5. 氏名、6. 生年月日、7. 現住所、8. 性別、9. 市町村コード、10. 個人番号、11. 発行者名、12. 発行日時、13. 有効期限、14. 最終検証日時、15. 顔写真(券面)、16. 登録日時、17. 更新日時	(略) 4. 資格情報バージョンID、5. 資格情報ステータス、6. 氏名、7. 生年月日、8. 現住所、9. 性別、10. 市町村コード、11. 個人番号、12. 発行者名、13. 発行日時、14. 有効期限、15. 最終検証日時、16. 顔写真(券面)、17. 登録日時、18. 更新日時	事前	特定個人情報保護評価指針(令和7年7月15日個人情報保護委員会)に定める重要な変更にあたらないため。
令和8年6月22日	(別添2) ファイル記録項目 (別添2) 特定個人情報ファイル記録項目 (5) カード代替電磁的記録用ファイル オ 別OS申請情報		1. 申請ID、2. 端末参照ID、3. 発行コード、4. 資格情報ID、5. 資格情報バージョンID、6. 電文ID、7. 申請ステータス、8. 申請詳細ステータス、9. mdoc申請詳細ステータス、10. 申請種別、11. 申請受付日時、12. 認可コード、13. OS識別子、14. 端末ID、15. カード発行番号、16. カード有効期限、17. 市町村コード、18. 4情報、19. 個人番号、20. 顔写真(券面)、21. 顔写真(撮影)、22. 画面表示文言、23. 個人番号・4情報署名、24. 署名検証用公開鍵証明書、25. 券面事項署名データ、26. 券面事項用公開鍵証明書K、27. 電子署名、28. アルゴリズムID、29. 電子証明書、30. 電子証明書種別、31. 署名用電子証明書シリアル番号、32. デバイストークン、33. 登録日時、34. 更新日時	事前	特定個人情報保護評価指針(令和7年7月15日個人情報保護委員会)に定める重要な変更にあたらないため。

(別添3) 変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和8年6月22日	(別添2) ファイル記録項目 (別添2) 特定個人情報 ファイル記録項目 (5) カード代替電磁的記録 用ファイル カ. CDDL情報		1. mdocID、2. トランザクション鍵連番、 3. mdoc、4. 電文ID、5. 登録日時、6. 更 新日時	事前	特定個人情報保護評価指 針(令和7年7月15日個人 情報保護委員会)に定める 重要な変更にあたらない ため。
令和8年6月22日	III 特定個人情報ファイル の取扱いプロセスにおける リスク対策(1) 5. 特定個人情報の提供・ 移転(委託や情報提供ネッ トワークシステムを通じた 提供を除く。) リスク1 特定個人情報の提供・移 転の記録 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、個人番号とすべき番 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つ た場合についても記録を残す。	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、個人番号とすべき番 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年未満の拘禁刑に当たる罪)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つ た場合についても記録を残す。	事後	特定個人情報保護評価指 針(令和7年7月15日個人 情報保護委員会)に定める 重要な変更にあたらない ため。
令和8年6月22日	III 特定個人情報ファイル の取扱いプロセスにおける リスク対策(2) 5. 特定個人情報の提供・ 移転(委託や情報提供ネッ トワークシステムを通じた 提供を除く。) リスク1 特定個人情報の提供・移 転の記録 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(番号法で認め られた場合に限り、当該個人の住民票 コードを用いて、「機構保存本人確認情報 ファイル」から個人番号を抽出し、附票全 国サーバに連携する場合を含む。)、当該 情報の提供記録(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つ た場合についても記録を残す。 (略)	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、5 情報等)の提供を行う際に(番号法で認め られた場合に限り、当該個人の住民票 コードを用いて、「機構保存本人確認情報 ファイル」から個人番号を抽出し、附票全 国サーバに連携する場合を含む。)、当該 情報の提供記録(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年未満の拘禁刑に当たる罪)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つ た場合についても記録を残す。 (略)	事後	特定個人情報保護評価指 針(令和7年7月15日個人 情報保護委員会)に定める 重要な変更にあたらない ため。
令和8年6月22日	III 特定個人情報ファイル の取扱いプロセスにおける リスク対策(2) 7. 特定個人情報の保管・ 消去 リスク2 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ファイルを 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。 (略)	5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ファイルを 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。 (略)	事後	特定個人情報保護評価指 針(令和7年7月15日個人 情報保護委員会)に定める 重要な変更にあたらない ため。
令和8年6月22日	III 特定個人情報ファイル の取扱いプロセスにおける リスク対策(4) 5. 特定個人情報の提供・ 移転(委託や情報提供ネッ トワークシステムを通じた 提供を除く。) リスク1 特定個人情報の提供・移 転の記録 具体的な方法	住基法に基づき機構保存附票本人確認情 報の提供が認められている地方公共団 体、行政機関等へ、附票本人確認情報の 提供に併せて個人番号の提供を行う際 に、当該情報の提供記録(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つ た場合についても記録を残す。 (略)	住基法に基づき機構保存附票本人確認情 報の提供が認められている地方公共団 体、行政機関等へ、附票本人確認情報の 提供に併せて個人番号の提供を行う際 に、当該情報の提供記録(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年未満の拘禁刑に当たる罪)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つ た場合についても記録を残す。 (略)	事後	特定個人情報保護評価指 針(令和7年7月15日個人 情報保護委員会)に定める 重要な変更にあたらない ため。

(別添3) 変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和8年6月22日	III リスク対策 (プロセス) (5) 4. 特定個人情報ファイル の取扱いの委託 再委託先による特定個人 情報ファイルの適切な取扱 いの確保	再委託していない	十分に行っている	事前	特定個人情報保護評価指 針 (令和7年7月15日個人 情報保護委員会) に定める 重要な変更にあたらない ため。
令和8年6月22日	III リスク対策 (プロセス) (5) 4. 特定個人情報ファイル の取扱いの委託 再委託先による特定個人 情報ファイルの適切な取扱 いの確保 具体的な方法		原則として再委託は行わないこととする が、再委託を行う場合は、以下の措置を取 ることとする。 ・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。 ・委託先に対して、特定個人情報にアクセ スできる再委託先従事者の名簿作成を義 務付ける。 ・本番環境での操作作業は必ず2名1組で 実施し、作業手順は委託先側でチェックを 行う。 ・委託先において、再委託先従事者による 特定個人情報への不要なアクセスがない か確認できるよう作業時のログを収集・保 管する。 ・再委託事業者に、本委託事務に従事す 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、所管省庁などの第三者 が現地調査し、適正に運用されているか 確認する。	事前	特定個人情報保護評価指 針 (令和7年7月15日個人 情報保護委員会) に定める 重要な変更にあたらない ため。