

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	外国人の在留資格に係る許可に関する事務、外国人の出入国又は在留の管理に関する事務及び特別永住者証明書の交付に関する事務

個人のプライバシー等の権利利益の保護の宣言

出入国在留管理庁は、外国人の在留資格に係る許可に関する事務、外国人の出入国又は在留の管理に関する事務及び特別永住者証明書の交付に関する事務において特定個人情報ファイルを取り扱うに当たり、そ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、その他の事案が発生するリスクを軽減させるために適切な措置を講じ、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

評価実施機関名

出入国在留管理庁長官

個人情報保護委員会 承認日【行政機関等のみ】

公表日

項目一覧

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

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	外国人の在留資格に係る許可に関する事務、外国人の出入国又は在留の管理に関する事務及び特別永住者証明書の交付に関する事務
②事務の内容 ※	＜制度内容＞ 出入国在留管理庁は、出入国管理及び難民認定法（昭和二十六年政令第三百十九号）及び日本国との平和条約に基づき日本の国籍を離脱した者等の出入国管理に関する特例法（平成三年法律第七十一号）に基づき、本邦に入国し、又は本邦から出国する全ての人の出入国及び本邦に在留する全ての外国人の在留の公正な管理を図るとともに、難民の認定手続を整備することを目的としている。 ＜事務内容＞ 出入国在留管理庁が行う事務のうち、番号利用法第9条別表31の3の項「出入国管理及び難民認定法による外国人の在留資格に係る許可に関する事務」、同表31の4の項「出入国管理及び難民認定法による外国人の出入国又は在留の管理に関する事務」、同表91の2の項「日本国との平和条約に基づき日本の国籍を離脱した者等の出入国管理に関する特例法による特別永住者証明書の交付に関する事務」において、特定個人情報を用いる以下の範囲で利用する（特定個人情報の流れを明記した事務フロー図を別添1に記載。）。 1. 個人番号登録（在留申請（窓口申請）、在留カードに係る届出等） 地方出入国在留管理官署の受付窓口において、申請者等から在留申請又は在留カードに係る届出等を受け付ける際、個人番号の提供を受け、真正性を確認したうえで個人番号情報管理システム（IMS）に登録する。 2. 個人番号登録（オンライン申請） 在留申請オンラインシステム（RAS）において、申請者等から在留申請（永住許可申請を除く。）を受け付ける際、個人番号の提供を受け、真正性を確認したうえで個人番号情報管理システム（IMS）に登録する。 3. 個人番号登録（在留申請等以外） 住民基本台帳ネットワークシステムから基本4情報に紐づく個人番号を取得し、個人番号情報管理システム（IMS）に登録する。 4. 情報照会 個人番号情報管理システム（IMS）の画面機能を通じて公共サービスメッシュ機関間情報連携サービス（中間サーバー相当機能）（以下、「中間サーバー相当機能」という。）から、個人管理番号と照会条件に紐づけられた照会結果を取得する。取得した情報は、個人番号情報管理システム（IMS）でのみ表示する。 （※）対象事務：在留資格認定証明書の交付の申請に関する事務、在留資格の変更の申請に関する事務、在留期間の更新の申請に関する事務、永住許可の申請に関する事務、在留資格の取得の申請に関する事務、在留資格の取消しに関する事務、特定技能所属機関による届出に関する事務、特別永住許可の申請に関する事務 5. 情報提供 他機関からの情報照会要求に対して、中間サーバー相当機能を通じて副本情報を送信する。
③対象人数	＜選択肢＞ [30万人以上] 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

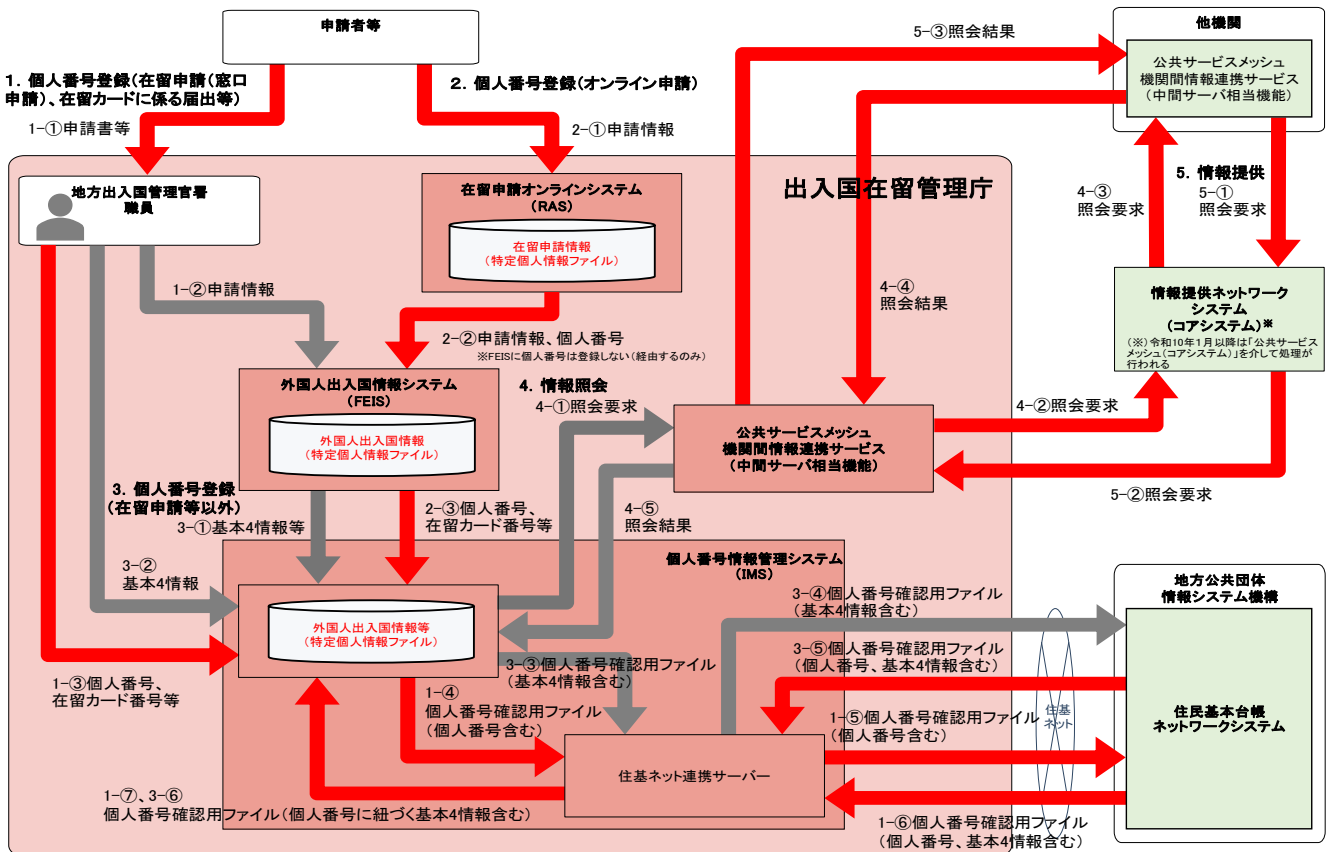
2. 特定個人情報ファイルを取り扱う事務において使用するシステム	
システム1	
①システムの名称	個人番号情報管理システム(IMS)
②システムの機能	個人番号情報管理システム(IMS)は、個人番号利用事務で利用する個人番号を管理するために新たに構築するシステム。 主な機能は以下のとおり。 ①個人番号・情報提供用個人識別符号管理機能 - 在留外国人の基本情報及びその日本人関係者の情報を管理する。 - 個人番号の登録・更新・削除を行う。 - 住基ネット連携サーバーを用いて住民基本台帳ネットワークシステムに連携し、住民基本台帳ネットワークシステム及び外国人出入国情報システム(FEIS)の4情報を突合し、個人番号の真正性を確認する。 - 機関間情報連携サービスへ処理通番の発番及び住基へ符号取得を依頼する。 ②情報照会管理機能 - 照会の状況を確認する。 - 機関間情報連携サービスへ情報照会要求を行い、照会結果を取得する。 ③副本登録・管理機能 - 機関間情報連携サービスに連携する副本情報の管理、登録要求依頼、連携後の登録結果の受領を行う。
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 (外国人出入国情報システム(FEIS))
システム2～5	
システム2	
①システムの名称	外国人出入国情報システム(FEIS)
②システムの機能	外国人出入国情報システム(FEIS)は、出入国審査、在留審査、退去強制、難民認定等、出入国在留管理庁の主要業務を行う基幹システム。 主な機能は以下のとおり。 ・出入国審査機能 出入国審査において、審査支援及び出入国審査データの登録を行う。 ・在留審査機能 在留審査において、審査支援及び在留審査データの登録を行う。 ・退去強制手続き機能 退去強制手続きにおいて、手続き支援及び退去強制手続きデータの登録を行う。 ・難民認定機能 難民認定申請において、業務支援及び難民認定データの登録を行う。 ・データ管理機能 各種業務が登録するデータを個人マスタに紐づけて履歴を含めて管理する。データの照会、補正の実施及び各種外部システムとの連携を行う。
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 (個人番号情報管理システム(IMS)、在留申請オンラインシステム(RAS))

システム3	
①システムの名称	在留申請オンラインシステム(RAS)
②システムの機能	在留申請オンラインシステム(RAS)は、在留審査手続の円滑化・迅速化のための在留管理基盤の強化の施策として、令和元年7月25日から稼働しているオンラインでの在留審査申請手続を行うためのシステム。主な機能は以下のとおり。 ・在留申請機能 オンラインで在留諸申請(在留期間更新許可申請、在留資格変更許可申請、在留資格認定証明書交付申請、在留資格取得許可申請等)を行う。 ・各種通知機能 オンライン申請された案件について、案件状態の変更等必要に応じてメールにて利用者に通知する。 ・利用者管理機能 オンライン申請を行うことが可能な利用者の情報を管理する。 ・データ連携機能 申請データを外国人出入国情報システム(FEIS)に連携する。また、審査結果を外国人出入国情報システム(FEIS)から受領する。
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 (外国人出入国情報システム(FEIS)、マイナポータル(法人設立OSS)、マイナポータル(自己情報取得API)、統合文書管理システム)
システム4	
①システムの名称	公共サービスメッシュ機関間情報連携サービス(中間サーバー相当機能)
②システムの機能	中間サーバー相当機能は、インターフェイスシステムや既存システム等の各システムとデータの受け渡しを行うことで、符号の取得や各情報保有機関で保有する特定個人情報の照会、及び各情報保有機関への情報提供等の業務を実現する。 ・符号管理機能 情報照会、情報提供に用いる個人の識別子である「符号」を保管・管理する。 ・情報照会機能 情報提供ネットワークシステムを介して、特定個人情報(連携対象)の情報照会及び情報提供受領(照会した情報の受領)を行う。 ・情報提供機能 情報提供ネットワークシステムを介して、情報照会要求の受領及び当該特定個人情報(連携対象)の提供を行う。 ・既存システム接続機能 中間サーバー相当機能と既存システム等との間で情報照会内容、情報提供内容、特定個人情報(連携対象)、符号取得のための情報等について連携する。 ・情報提供等記録管理機能 特定個人情報(連携対象)の照会、又は提供があった旨の情報提供等記録を生成し、管理する。 ・情報提供データベース管理機能 特定個人情報(連携対象)を副本として、保持・管理する。データは機関ごとに分散管理する。 ・データ送受信機能 中間サーバー相当機能とインターフェイスシステムとの間で情報照会、情報提供、符号取得のための情報等について連携する。 ・セキュリティ管理機能 情報提供ネットワークシステムに送信する情報について、情報照会者から受領した暗号鍵で暗号化を適切に実施した上で提供を行う(暗号化、復号機能と、鍵情報及び照会許可照合リストを管理する。) ・職員認証・権限管理機能 中間サーバー相当機能を利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報(連携対象)へのアクセス制御を行う。 ・システム管理機能 バッチの状況管理、業務統計情報の集計、稼働状態の通知、保管期限切れ情報の削除を行う。 ・現行I/F互換機能 中間サーバー相当機能を利用する機関と中間サーバー相当機能を利用していない(従来の中間サーバーを利用する)機関との番号連携を可能とする機能。
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 (インターフェイスシステム)

システム6～10	
システム11～15	
システム16～20	
3. 特定個人情報ファイル名	
外国人出入国情報等ファイル	
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	番号利用法に定められた範囲内で、出入国管理及び難民認定法(昭和二十六年政令第三百十九号)及び日本国との平和条約に基づき日本の国籍を離脱した者等の出入国管理に関する特例法(平成三年法律第七十一号)で定められた業務に対応するため、特定個人情報ファイルを保有する。
②実現が期待されるメリット	在留審査等において情報提供ネットワークシステムによる情報連携によって他機関から必要な情報の提供を受けることで、申請時の添付書類の省略による申請者等の利便性の向上、正確な情報による円滑な審査、業務を実現できる。
5. 個人番号の利用 ※	
法令上の根拠	- 番号利用法 第9条第1項、別表31の3の項、31の4の項、91の2の項 - 住民基本台帳法 第30条の9
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	- 番号利用法 第9条第1項、別表31の3の項、31の4の項、91の2の項 - 番号利用法 第19条第8号 (照会)番号利用法第19条第8号に基づく主務省令第2条の表55の2の項、55の3の項、123の2の項 (提供)番号利用法第19条第8号に基づく主務省令第2条の表項番1の項、2の項、3の項、5の項、6の項、7の項、48の項、49の項、57の項、58の項、65の項、67の項、69の項、73の項、83の項、85の項、107の項、115の項、141の項
7. 評価実施機関における担当部署	
①部署	在留管理支援部在留企画室
②所属長の役職名	出入国在留管理庁参事官
8. 他の評価実施機関	
法務大臣	

(別添1) 事務の内容

特定個人情報ファイルを取り扱う事務の流れ



外国人の在留資格に係る許可に関する事務、外国人の出入国又は在留の管理に関する事務及び特別永住者証明書の交付に関する事務における情報の流れを、以下の5つで整理する。

1. 個人番号登録(在留申請(窓口申請)、在留カードに係る届出等)
2. 個人番号登録(オンライン申請)
3. 個人番号登録(在留申請等以外)
4. 情報照会
5. 情報提供

凡例

- 特定個人情報の流れ
- 個人情報の流れ
- 出入国在留管理庁に関する事務に関わる対象者・対象機関
- 出入国在留管理庁に関する事務に関わる対象者・対象機関(出入国在留管理庁)
- 出入国在留管理庁に関する事務で利用するシステム(出入国在留管理庁の所有システム以外)
- 出入国在留管理庁に関する事務で利用するシステム(出入国在留管理庁の所有システム)
- 出入国在留管理庁に関する事務で利用する情報
- 出入国在留管理庁に関する事務で利用するネットワーク

1. 個人番号登録(在留申請(窓口申請)、在留カードに係る届出等)

- 1-① 地方出入国在留管理官署の受付窓口において、申請者等から在留申請又は在留カードに係る届出等を受け付ける際、申請書類等と併せて個人番号の提供を受ける。
- 1-② 地方出入国在留管理官署の職員は、提出された申請書類等の内容を確認し、外国人出入国情報システム(FEIS)に申請情報等を登録する。
- 1-③ 地方出入国在留管理官署の職員は、個人番号情報管理システム(IMS)にログインして、提供を受けた個人番号の登録状況を確認する。当該個人番号が対象者の個人番号として登録済みである場合は、個人番号の真正性を確認できたものとして処理を終了。
- 1-④ 個人番号情報管理システム(IMS)に対象者の個人番号が未登録又は登録済みであるが提供を受けた個人番号と一致しない場合は、提供を受けた個人番号を同システムに仮登録する。仮登録された個人番号の真正性を確認するため、当該個人番号に紐づく基本4情報を住基ネットに照会するための個人番号確認用ファイル(提示された個人番号を含む。)を出力し、住基ネット連携サーバーに転送する。
(※)通信障害等により専用線で個人番号を入手することが困難な場合は、電子記録媒体を用いて入手する場合がある。
- 1-⑤ 地方出入国在留管理官署の職員は、住基ネット連携サーバーから地方公共団体情報システム機構(住基ネット)に個人番号確認用ファイルを送信する。
- 1-⑥ 住基ネット連携サーバーにおいて、地方公共団体情報システム機構(住基ネット)から1-⑤の照会への回答として送信される個人番号確認用ファイル(個人番号に紐づく基本4情報を含む。)を受信する。
- 1-⑦ 個人番号情報管理システム(IMS)において、住基ネット連携サーバーから連携される1-⑥の個人番号確認用ファイルを登録する。個人番号情報管理システムにおいて、システム内で保有する対象者の基本4情報と地方公共団体情報システム機構(住基ネット)から送信された基本4情報を突き合わせ、真正性を確認できれば仮登録中の個人番号を正式に登録する。真正性を確認できない場合、仮登録した個人番号は削除する。

(※)仮登録された番号は、基本4情報が完全に一致する場合は自動で正式に登録され、部分一致の場合は、職員が目視で真正性を確認する。

2. 個人番号登録(オンライン申請)

- 2-① 在留申請オンラインシステム(RAS)において、申請人等から在留申請を受け付ける際、申請情報と併せて個人番号の提供を受ける。
 - 2-② 入力された申請情報及び個人番号は、外国人出入国情報システム(FEIS)内に連携され、登録される(入力された個人番号を除く。)
 - 2-③ 提供を受けた個人番号は、対象者の基本4情報等と併せて外国人出入国情報システム(FEIS)を経由して個人番号情報管理システム(IMS)に連携される。当該個人番号が対象者の個人番号として登録済みである場合は、個人番号の真正性を確認できたものとして処理を終了。
- 以降の流れは、1-④～1-⑦と同様。

3. 個人番号登録(在留申請等以外)

- 3-① 外国人出入国情報システム(FEIS)から個人番号情報管理システム(IMS)に、バッチ処理によって、中長期在留者、特別永住者、経過滞在者、一時庇護上陸許可者及び仮滞在許可者の最新の基本4情報、国籍、在留カード等番号及び組織内個人識別記号を連携する。
- 3-② 出入国在留管理庁職員は、個人番号情報管理システム(IMS)に在留申請の申請者等の日本人関係者の基本4情報を登録する。
(※)通常は、在留申請の受付の際に個人番号と併せて登録する。本処理は、受付後に追加で登録が必要となった場合の処理である。
- 3-③ 住民基本台帳ネットワークシステムに対象者の基本4情報に紐づく個人番号を一括照会して取得するため、個人番号情報管理システム(IMS)において照会用の個人番号確認用ファイル(対象者の4情報を含む。)を出力し、住基ネット連携サーバーに転送する。本処理はバッチ処理にて実施される。
(※)通信障害等により専用線で個人番号を入手することが困難な場合は、電子記録媒体を用いて入手する場合がある。
- 3-④ 地方出入国在留管理官署の職員は、住基ネット連携サーバーから住民基本台帳ネットワークシステムに個人番号確認用ファイルを送信する。
- 3-⑤ 住基ネット連携サーバーにおいて、住民基本台帳ネットワークシステムから3-④の照会への回答として送信される個人番号確認用ファイル(送信した基本4情報と一致又は部分一致する基本4情報及びこれに紐づく個人番号を含む。)を受信する。
- 3-⑥ 個人番号情報管理システム(IMS)において、住基ネット連携サーバーから連携される3-⑤の個人番号確認用ファイルを登録する。個人番号情報管理システムにおいて、システム内で保有する対象者の基本4情報と住民基本台帳ネットワークシステムから送信された基本4情報を突き合わせ、完全に一致する場合は自動で個人番号は登録され、部分一致の場合は、職員が目視で同一人性を確認する。同一人性が確認できない場合は個人番号は登録されずに削除される。

4. 情報照会

- 4-① 個人番号情報管理システム(IMS)は、中間サーバー相当機能に対し、情報照会結果の取得要求(対象者の個人管理番号、照会条件)を送信する。
- 4-② 出入国在留管理庁内の中間サーバー相当機能は、情報提供ネットワークシステム(コアシステム)に対し、情報照会要求を送信する。
- 4-③ 情報提供ネットワークシステム(コアシステム)は、他機関の中間サーバー相当機能に対し、情報照会要求を送信する。
- 4-④ 他機関の中間サーバー相当機能は、出入国在留管理庁内の中間サーバー相当機能に対し、情報照会結果を送信する。
- 4-⑤ 出入国在留管理庁内の中間サーバー相当機能は、個人番号情報管理システム(IMS)に対し、情報照会結果を送信する。
- (※) 4-②、4-③、4-④の中間サーバー相当機能と情報提供ネットワークシステム(コアシステム)間の処理内容は、「公共サービスメッシュ機関間情報連携サービス(中間サーバー相当機能)」外部インターフェイス仕様書(業務システム編)第1.02版(2025年1月31日)をもとに記載。

5. 情報提供

- 5-① 他機関の中間サーバー相当機能は、情報提供ネットワークシステム(コアシステム)に対し、情報照会要求を送信する。
- 5-② 情報提供ネットワークシステム(コアシステム)は、出入国在留管理庁内の中間サーバー相当機能に対し、情報照会要求を送信する。
- 5-③ 出入国在留管理庁内の中間サーバー相当機能は、他機関の中間サーバー相当機能に対し、情報照会結果(副本)を送信する。
- (※) 5-①、5-②、5-③の中間サーバー相当機能と情報提供ネットワークシステム(コアシステム)間の処理内容は、「公共サービスメッシュ機関間情報連携サービス(中間サーバー相当機能)」外部インターフェイス仕様書(業務システム編)第1.02版(2025年1月31日)をもとに記載。

(備考)

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	
外国人出入国情報等ファイル	
2. 基本情報	
①ファイルの種類 ※	[システム用ファイル] <選択肢> 1) システム用ファイル 2) その他の電子ファイル(表計算ファイル等)
②対象となる本人の数	[100万人以上1,000万人未満] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
③対象となる本人の範囲 ※	・個人番号を有する外国人 ・在留資格認定証明書交付申請、在留資格変更許可申請、在留期間更新許可申請、永住許可申請、在留資格取得許可申請又は特別永住者許可申請の申請者の日本人関係者
その必要性	番号利用法に定められた範囲内で、出入国管理及び難民認定法及び日本国との平和条約に基づき日本の国籍を離脱した者等の出入国管理に関する特例法で定められた業務に対応するため、特定個人情報を管理する必要がある。
④記録される項目	[10項目以上50項目未満] <選択肢> 1) 10項目未満 2) 10項目以上50項目未満 3) 50項目以上100項目未満 4) 100項目以上
主な記録項目 ※	・識別情報 [☐] 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 (戸籍関係情報、出入国関係情報、在留カード交付関係情報、特別永住者証明書交付関係情報)
その妥当性	・個人番号:対象者を正確に特定するために保有。 ・その他識別情報(内部番号)個人番号と紐付け、対象者を正確に特定するために保有 ・基本4情報:対象者を正確に特定するために保有。 ・地方税関係情報、医療保険関係情報、雇用・労働関係情報、年金関係情報、戸籍関係情報:在留審査等で使用するために保有。 ・出入国関係情報、在留カード交付関係情報、特別永住者証明書交付関係情報:情報提供ネットワークシステムによる情報連携によって他機関に提供するために保有。
全ての記録項目	別添2を参照。
⑤保有開始日	令和8年4月
⑥事務担当部署	在留管理支援部在留企画室

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 (地方公共団体情報システム機構)
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、在留申請オンラインシステム(RAS))
③入手の時期・頻度	【住民基本台帳ネットワークシステム又は電子記録媒体から入手する場合】 ・出入国在留管理庁における情報提供ネットワークシステムによる情報連携の運用開始(令和9年3月予定)に向けた準備として、運用開始時点で本邦に正規に在留する中長期在留者及び特別永住者の個人番号を一括照会する。 ・運用開始後に本邦に在留することとなる中長期在留者のうち、住所を定めた自治体に転入届出を行った者について、定期的に個人番号を一括照会する。 ・在留資格認定証明書交付許可に関する事務、在留資格変更許可に関する事務、在留期間更新許可に関する事務、永住許可に関する事務、在留資格取得許可に関する事務、在留資格取消し手続に関する事務、特定技能所属機関による届出に関する事務、特別永住許可申請に関する事務において、必要な限度で任意のタイミングで対象者の個人番号を照会する。 ・稼働後の障害発生時に、障害によって未取得となった対象者の個人番号を一括照会する。 【本人又は本人の代理人から入手する場合】 ・在留申請や在留カードに係る届出等において、申請人等から個人番号から提供を受ける。 【情報提供ネットワークシステムから入手する場合】 ・在留資格認定証明書交付許可に関する事務、在留資格変更許可に関する事務、在留期間更新許可に関する事務、永住許可に関する事務、在留資格取得許可に関する事務、在留資格取消し手続に関する事務、特定技能所属機関による届出に関する事務、特別永住許可申請に関する事務において、審査等を行う都度、情報提供ネットワークシステムによる情報連携によって他機関から必要な情報の提供を受ける。
④入手に係る妥当性	【住民基本台帳ネットワークシステム又は電子記録媒体から入手する場合】 ・番号利用法第14条第2項に基づき、対象者の個人番号を照会する。 ・運用前の個人番号の事前取得及び運用開始後の定期的な一括取得によって、事前に個人番号を入手することで、情報提供ネットワークシステムによる情報照会による情報照会者からの特定個人情報の求めに迅速に対応できる。 ・障害発生時の個人番号の一括取得によって、情報提供ネットワークシステムによる情報照会による情報照会者からの特定個人情報の求めに迅速に対応できる。 【本人又は代理人から提供を入手場合】 ・番号利用法第14条第1項に基づき、本人等から個人番号の提供を受ける。 ・運用前の個人番号の事前取得及び運用開始後の定期的な一括取得によって個人番号を入手できなかった場合、在留申請等の際に本人等から提供を受ける必要がある。 【情報提供ネットワークシステムから入手する場合】 番号利用法第19条第8号に基づく主務省令の規定に基づき、同主務省令に規定された事務において、他機関からの情報を提供を受けることができる。
⑤本人への明示	個人番号の利用目的を出入国在留管理庁のWebページで明示する。

⑥使用目的 ※		在留審査等において情報提供ネットワークシステムによる情報連携によって他機関から必要な情報の提供を受けることで、申請時の添付書類の省略による申請人等の利便性の向上、正確な情報による円滑な審査、業務を実現するため。	
	変更の妥当性	－	
⑦使用の主体	使用部署 ※	出入国在留管理庁本庁、地方出入国在留管理局、地方出入国在留管理局の支局、地方出入国在留管理局の出張所、地方出入国在留管理局の支局の出張所	
	使用者数	[1,000人以上]	<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 ※		・在留資格認定証明書交付許可に関する事務、在留資格変更許可に関する事務、在留期間更新許可に関する事務、永住許可に関する事務、在留資格取得許可に関する事務、在留資格取消し手続に関する事務、特定技能所属機関による届出に関する事務、特別永住許可申請に関する事務において、情報提供ネットワークシステムによる情報連携によって他機関から必要な情報の提供を受ける。 ・番号利用法第19条第8号に基づく主務省令に定められた事務において、情報照会者から出入国関係情報、在留カード関係情報及び特別永住者証明書関係情報の求めがあった場合、情報提供ネットワークシステムによる情報連携によって提供する。	
	情報の突合 ※	・本人等から提供を受けた個人番号については、まずは個人番号情報管理システム(IMS)での登録状況を確認する。当該個人番号が対象者の個人番号として登録済みである場合は、当該個人番号の真正性を確認できたものとする。 ・対象者の個人番号が未登録又は登録済みであるが提供を受けた個人番号と一致しない場合は、提供を受けた個人番号を同システムに仮登録し、その真正性を確認するため、当該個人番号に紐づく基本4情報を住民基本台帳ネットワークシステムに照会して取得し、個人番号情報管理システム(IMS)で登録されている基本4情報と突合する。	
	情報の統計分析 ※	特定個人情報を用いた統計分析を行う予定。	
	権利利益に影響を与え得る決定 ※	在留資格認定証明書の交付可否、在留資格の変更の許可、在留期間の更新の許可、永住の許可、在留資格の取得の許可、在留資格の取消しの可否、特別永住許可の許可	
⑨使用開始日		令和9年3月19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		個人番号情報管理システム(IMS)のシステム運用保守
①委託内容		特定個人情報を取り扱う運用・保守業務(バックアップ取得、障害時・異常発生時の確認及び復旧作業等)
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全体]
	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 [100万人以上1,000万人未満]
	対象となる本人の範囲 ※	・個人番号を有する外国人 ・在留資格認定証明書交付申請、在留資格変更許可申請、在留期間更新許可申請、永住許可申請、在留資格取得許可申請又は特別永住者許可申請(入管特例法第5条)の申請者の日本人関係者
	その妥当性	個人番号情報管理システム(IMS)全体に係る保守を適切に実施するためには、専門的かつ高度な知識・技術を要すること等、全体の取扱いを委託することが必要であるため。なお、出入国在留管理庁において保守業務を行うよりも、より高水準のセキュリティを確保することが可能である。
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 (当庁承認を得た上で、当庁サーバ室内でファイルにアクセスさせる。)
⑤委託先名の確認方法		出入国在留管理庁Webページに掲載。
⑥委託先名		令和8年度に調達予定のため、未定。
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	当該業務の主体的部分を除く一部を再委託する場合、再委託先に再委託承認申請書及び安全管理措置を施している証拠を提出させた上で、出入国在留管理庁が事前に承認を行う。
	⑨再委託事項	個人番号情報管理システム(IMS)の運用管理・保守業務における主体的業務を除く実作業の一部

委託事項2～5		
委託事項2		在留申請オンラインシステム(RAS)のシステム運用保守
①委託内容		特定個人情報を取り扱う運用・保守業務(バックアップ取得、障害時・異常発生時の確認及び復旧作業等)
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	[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
	対象となる本人の範囲 ※	在留申請オンラインシステム(RAS)での在留資格認定証明書交付申請、在留資格変更許可申請、在留期間更新許可申請、在留資格取得許可申請の申請者である外国人又はその日本人関係者
	その妥当性	在留申請オンラインシステム(RAS)全体に係る保守を適切に実施するためには、専門的かつ高度な知識・技術を要すること等、全体の取扱いを委託することが必要であるため。なお、出入国在留管理庁において保守業務を行うよりも、より高水準のセキュリティを確保することが可能である。
③委託先における取扱者数		[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
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		出入国在留管理庁Webページに掲載。
⑥委託先名		令和8年度に調達予定のため、未定。
再委託	⑦再委託の有無 ※	[再委託する] <選択肢> 1) 再委託する 2) 再委託しない
	⑧再委託の許諾方法	当該業務の主体的部分を除く一部を再委託する場合、再委託先に再委託承認申請書及び安全管理措置を施している証拠を提出させた上で、出入国在留管理庁が事前に承認を行う。
	⑨再委託事項	在留申請オンラインシステム(RAS)の運用管理・保守業務における主体的業務を除く実作業の一部

委託事項3		個人番号情報管理システム(IMS)への個人番号登録業務
①委託内容		本邦に在留する外国人の個人番号を地方公共団体情報システム機構から一括で入手し、データベースとして登録する業務
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全体 <選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部
	対象となる本人の数	☐ 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
	対象となる本人の範囲 ※	本邦に在留しており、個人番号を有する外国人又はその日本人関係者
	その妥当性	個人番号情報管理システム(IMS)において個人番号の登録業務を適切に実施するためには、専門的かつ高度な知識・技術を要すること等、当システム全体の取扱いを理解していることが必要であるため。なお、当庁において個人番号登録業務を行うよりも、より高水準のセキュリティを確保することが可能である。
③委託先における取扱者数		☐ 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
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 (当庁承認を得た上で、当庁サーバ室内でファイルにアクセスさせる。)
⑤委託先名の確認方法		当庁ホームページに掲載。
⑥委託先名		令和7年度に調達予定のため、未定。
再委託	⑦再委託の有無 ※	☐ 再委託する <選択肢> 1) 再委託する 2) 再委託しない
	⑧再委託の許諾方法	再委託する業務の範囲、再委託の必要性、再委託予定金額、再委託先の業務の履行能力等について記載した申請書及び再委託に係る履行体制図を当庁に提出して申請し、許諾する。
	⑨再委託事項	⑧にて行う許諾申請の中で定義する。
委託事項6～10		
委託事項11～15		
委託事項16～20		

5. 特定個人情報の提供・移転(委託に伴うものを除く。)	
提供・移転の有無	[☐] 提供を行っている (20) 件 [☐] 移転を行っている () 件 [☐] 行っていない
提供先1	厚生労働大臣
①法令上の根拠	番号利用法第19条第8号、情報連携主務省令第2条の表1の項
②提供先における用途	健康保険法第5条第2項の規定により厚生労働大臣が行うこととされた健康保険に関する事務又は同法による保険医若しくは保険薬剤師の登録に関する事務
③提供する情報	・出入国関係情報 ・在留カード関係情報 ・特別永住者証明書関係情報
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	個人番号を有する外国人
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	番号利用法上の情報照会者から照会を受けたとき。
提供先2～5	
提供先2	全国健康保険協会
①法令上の根拠	番号利用法第19条第8号、情報連携主務省令第2条の表2の項
②提供先における用途	健康保険法による保険給付の支給に関する事務
③提供する情報	・出入国関係情報 ・在留カード関係情報 ・特別永住者証明書関係情報
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	個人番号を有する外国人
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	番号利用法上の情報照会者から照会を受けたとき。

提供先3	健康保険組合	
①法令上の根拠	番号利用法第19条第8号、情報連携主務省令第2条の表3の項	
②提供先における用途	健康保険法による保険給付の支給に関する事務	
③提供する情報	・出入国関係情報 ・在留カード関係情報 ・特別永住者証明書関係情報	
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	個人番号を有する外国人	
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	番号利用法上の情報照会者から照会を受けたとき。	
提供先4	厚生労働大臣	
①法令上の根拠	番号利用法第19条第8号、情報連携主務省令第2条の表5の項	
②提供先における用途	船員保険法第4条第2項の規定により厚生労働大臣が行うこととされた船員保険に関する事務	
③提供する情報	・出入国関係情報 ・在留カード関係情報 ・特別永住者証明書関係情報	
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	個人番号を有する外国人	
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	番号利用法上の情報照会者から照会を受けたとき。	

提供先5	全国健康保険協会	
①法令上の根拠	番号利用法第19条第8号、情報連携主務省令第2条の表6の項	
②提供先における用途	船員保険法による保険給付の支給に関する事務	
③提供する情報	・出入国関係情報 ・在留カード関係情報 ・特別永住者証明書関係情報	
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	個人番号を有する外国人	
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	番号利用法上の情報照会者から照会を受けたとき。	
提供先6～10		
提供先6	全国健康保険協会	
①法令上の根拠	番号利用法第19条第8号、情報連携主務省令第2条の表7の項	
②提供先における用途	船員保険法による保険給付又は雇用保険法等の一部を改正する法律附則第39条の規定によりなお従前の例によるものとされた平成19年法律第30号第4条の規定による改正前の船員保険法による保険給付の支給に関する事務	
③提供する情報	・出入国関係情報 ・在留カード関係情報 ・特別永住者証明書関係情報	
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	個人番号を有する外国人	
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	番号利用法上の情報照会者から照会を受けたとき。	

提供先7	市町村長
①法令上の根拠	番号利用法第19条第8号、情報連携主務省令第2条の表48の項
②提供先における用途	地方税法その他の地方税に関する法律及びこれらの法律に基づく条例又は森林環境税及び森林環境譲与税に関する法律による地方税又は森林環境税の賦課徴収に関する事務
③提供する情報	・出入国関係情報 ・在留カード関係情報
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	個人番号を有する外国人
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	番号利用法上の情報照会者から照会を受けたとき。
提供先8	都道府県知事
①法令上の根拠	番号利用法第19条第8号、情報連携主務省令第2条の表第49の項
②提供先における用途	地方税法その他の地方税に関する法律及びこれらの法律に基づく条例による地方税の賦課徴収に関する事務
③提供する情報	出入国関係情報
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	個人番号を有する外国人
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	番号利用法上の情報照会者から照会を受けたとき。

提供先9	日本私立学校振興・共済事業団
①法令上の根拠	番号利用法第19条第8号、情報連携主務省令第2条の表57の項
②提供先における用途	私立学校教職員共済法による短期給付、年金である給付又は一時金の支給に関する事務
③提供する情報	・出入国関係情報 ・在留カード関係情報 ・特別永住者証明書関係情報
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	個人番号を有する外国人
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	番号利用法上の情報照会者から照会を受けたとき。
提供先10	厚生労働大臣(日本年金機構)又は共済組合等(日本私立学校振興・共済事業団、国家公務員共済組合連合会、地方公務員共済組合又は全国市町村職員共済組合連合会)
①法令上の根拠	番号利用法第19条第8号、情報連携主務省令第2条の表58の項
②提供先における用途	厚生年金保険法による年金である保険給付又は一時金の支給に関する事務
③提供する情報	・出入国関係情報 ・在留カード関係情報 ・特別永住者証明書関係情報
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	個人番号を有する外国人
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	番号利用法上の情報照会者から照会を受けたとき。

提供先11～15	
提供先11	国家公務員共済組合
①法令上の根拠	番号利用法第19条第8号、情報連携主務省令第2条の表65の項
②提供先における用途	国家公務員共済組合法による短期給付の支給に関する事務
③提供する情報	・出入国関係情報 ・在留カード関係情報 ・特別永住者証明書関係情報
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	個人番号を有する外国人
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	番号利用法上の情報照会者から照会を受けたとき。
提供先12	
国家公務員共済組合連合会	
①法令上の根拠	番号利用法第19条第8号、情報連携主務省令第2条の表67の項
②提供先における用途	国家公務員共済組合法による年金である給付又は一時金の支給に関する事務
③提供する情報	出入国関係情報
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	個人番号を有する外国人
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	番号利用法上の情報照会者から照会を受けたとき。

提供先13	市町村長又は国民健康保険組合	
①法令上の根拠	番号利用法第19条第8号、情報連携主務省令第2条の表69の項	
②提供先における用途	国民健康保険法による保険給付の支給又は保険料の徴収に関する事務	
③提供する情報	・出入国関係情報 ・在留カード関係情報 ・特別永住者証明書関係情報	
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	個人番号を有する外国人	
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	番号利用法上の情報照会者から照会を受けたとき。	
提供先14	厚生労働大臣	
①法令上の根拠	番号利用法第19条第8号、情報連携主務省令第2条の表73の項	
②提供先における用途	国民年金法による年金である給付若しくは一時金の支給、保険料の納付に関する処分又は保険料その他徴収金の徴収に関する事務	
③提供する情報	・出入国関係情報 ・在留カード関係情報 ・特別永住者証明書関係情報	
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	個人番号を有する外国人	
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	番号利用法上の情報照会者から照会を受けたとき。	

提供先15	地方公務員共済組合
①法令上の根拠	番号利用法第19条第8号、情報連携主務省令第2条の表83の項
②提供先における用途	地方公務員等共済組合法による短期給付の支給に関する事務
③提供する情報	・出入国関係情報 ・在留カード関係情報 ・特別永住者証明書関係情報
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	個人番号を有する外国人
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	番号利用法上の情報照会者から照会を受けたとき。
提供先16～20	
提供先16	地方公務員共済組合又は全国市町村職員共済組合連合会
①法令上の根拠	番号利用法第19条第8号、情報連携主務省令第2条の表第85の項
②提供先における用途	地方公務員等共済組合法による年金である給付又は一時金の支給に関する事務
③提供する情報	出入国関係情報
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	個人番号を有する外国人
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	番号利用法上の情報照会者から照会を受けたとき。

提供先17	市町村長
①法令上の根拠	番号利用法第19条第8号、情報連携主務省令第2条の表107の項
②提供先における用途	児童手当法による児童手当又は旧特例給付の支給に関する事務
③提供する情報	・出入国関係情報 ・在留カード関係情報 ・特別永住者証明書関係情報
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	個人番号を有する外国人
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	番号利用法上の情報照会者から照会を受けたとき。
提供先18	後期高齢者医療広域連合
①法令上の根拠	番号利用法第19条第8号、情報連携主務省令第2条の表115の項
②提供先における用途	高齢者の医療の確保に関する法律による後期高齢者医療給付の支給又は保険料の徴収に関する事務
③提供する情報	・出入国関係情報 ・在留カード関係情報 ・特別永住者証明書関係情報
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	個人番号を有する外国人
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	番号利用法上の情報照会者から照会を受けたとき。

提供先19	独立行政法人日本学生支援機構	
①法令上の根拠	番号利用法第19条第8号、情報連携主務省令第2条の表第141の項	
②提供先における用途	独立行政法人日本学生支援機構法による学資の貸与及び支給に関する事務	
③提供する情報	・在留カード関係情報 ・特別永住者証明書関係情報	
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	個人番号を有する外国人	
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	番号利用法上の情報照会者から照会を受けたとき。	
提供先20	地方公共団体情報システム機構	
①法令上の根拠	住民基本台帳法第30条の9、住民基本台帳法別表第1第40の項、第40の2の項、40の3の項	
②提供先における用途	個人番号に紐づく本人確認情報の検索・提供	
③提供する情報	個人番号	
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	・個人番号を有する外国人 ・在留資格認定証明書交付申請、在留資格変更許可申請、在留期間更新許可申請、永住許可申請、在留資格取得許可申請又は特別永住者許可申請の申請者の日本人関係者	
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 ()	☒ 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	本人等から提供を受けた個人番号の真正性確認を実施するとき。	
移転先1		
移転先2～5		
移転先6～10		
移転先11～15		
移転先16～20		

6. 特定個人情報の保管・消去														
①保管場所 ※		【中間サーバー相当機能における措置】 中間サーバー相当機能はガバメントクラウドに設置する。 ・サーバー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、クラウド事業者は政府情報システムのためのセキュリティ評価制度（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。 ・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。 【出入国在留管理庁内（中間サーバー相当機能以外）における措置】 ・特定個人情報を保管するためのサーバーは、入退室管理を行っている部屋にて保管する。 ・作業のためにサーバー室等へ入退室する際に電子記録媒体等の機器類の持込み又は持出しをする場合には、事前に責任者に申請書を提出し、承認を得る。 ・職員等がサーバー室等へ入退室をする際は、データの漏えい防止のために、電子記録媒体、携帯電話、パソコン類等の不要な機器の持込みがないかを確認する。 ・電子記録媒体は、要管理対策区域内の施錠できる保管庫に保管する。												
②保管期間	期間	<選択肢> <table border="0"> <tr> <td>1) 1年未満</td> <td>2) 1年</td> <td>3) 2年</td> </tr> <tr> <td>4) 3年</td> <td>5) 4年</td> <td>6) 5年</td> </tr> <tr> <td>7) 6年以上10年未満</td> <td>8) 10年以上20年未満</td> <td>9) 20年以上</td> </tr> <tr> <td colspan="3">10) 定められていない</td> </tr> </table> [定められていない]	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		
	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	外国人の出国・死亡後も外部からの情報提供依頼に対応したり、その関係者に係る在留審査等で参考とすることがあるため、保存期間を定めず保有し続ける必要がある。												
③消去方法		【中間サーバー相当機能における措置】 中間サーバー相当機能はガバメントクラウドに設置する。 ・特定個人情報の消去は出入国在留管理庁からの操作によって実施される。出入国在留管理庁の業務データはデジタル庁及びガバメントクラウドのクラウド事業者にはアクセスが制御されているためデジタル庁及びクラウド事業者が特定個人情報を消去することはない。 ・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等にしたがって暗号化消去等により確実にデータを消去する。 【出入国在留管理庁内（中間サーバー相当機能以外）における措置】 ・特定個人情報は消去せず、漏えい等を防止するために職員の特定個人情報に対するアクセスは監視にて検知する等の措置を講じた上で保有し続ける。 ・電子記録媒体上のデータは、利用後速やかに完全消去し、媒体を物理的に破壊する。												
7. 備考														
—														

(別添2) 特定個人情報ファイル記録項目

- ・住民区分
- ・個人管理番号
- ・氏名(英字)
- ・氏名(漢字)
- ・氏名(漢字カナ)
- ・生年月日
- ・性別
- ・国籍
- ・住所
- ・在留カード等番号
- ・個人番号
- ・個人番号登録状況確認結果
- ・符号発行状況
- ・事務名称
- ・事務手続名称
- ・提供の求めの日時
- ・提供の日時
- ・特定個人情報名
- ・情報提供者機関

【情報提供ネットワークシステムによる情報連携によって他機関から入手する情報】

- ・地方税関係情報
- ・市町村民税関係情報
- ・医療保険関係情報
- ・雇用・労働関係情報
- ・年金関係情報
- ・戸籍関係情報

【出入国管理及び難民認定法による外国人の出入国に関する情報(出入国関係情報)】※他機関に提供する特定個人情報として副本登録するもの。

- ・国籍・地域(最新のみ)
- ・出入国年月日
- ・記録区分
- ・出入国港
- ・回次

【出入国管理及び難民認定法による在留カードの交付に関する情報(在留カード関係情報)】※他機関に提供する特定個人情報として副本登録するもの。

- ・国籍・地域
- ・在留資格
- ・在留資格「特定活動」に係る情報
 - － 特定活動告示25号該当の有無
 - － 特定活動告示26号該当の有無
 - － 特定活動告示40号該当の有無
 - － 特定活動告示41号該当の有無
- ・在留期間
- ・在留期限の満了の日
- ・許可の種類
- ・許可の年月日
- ・在留カード番号
- ・交付年月日
- ・有効期間満了の日
- ・就労制限の有無
- ・資格外活動許可に係る情報
 - － 資格外活動許可(包括)の有無
 - － 資格外活動許可(個別)の有無
 - － 許可年月日

【日本国との平和条約に基づき日本の国籍を離脱した者等の出入国管理に関する特例法による特別永住者証明書の交付に関する情報(特別永住者証明書交付関係情報)】※他機関に提供する特定個人情報として副本登録するもの。

- ・国籍・地域
- ・特別永住者証明書番号
- ・交付年月日
- ・有効期間満了の日

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 ※(7. リスク1⑨を除く。)

1. 特定個人情報ファイル名	
外国人出入国情報等ファイル	
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	【在留申請（窓口申請）、在留カードに係る届出等における入手】 ①本人が提出する場合 ・窓口において、申請者に在留カード等を提示させ、本人確認が完了した後に申請を受け付ける。 ・在留申請、特別永住許可申請及び在留カードに係る届出等は、様式を定めた提出方式によるものであり、申請者本人又は関係者に限定した情報のみ記載することとしている。 ②法定代理人が提出する場合 ・窓口において、申請者との関係を証明する資料（住民票等）を提示させ、代理が認められていることの確認が完了した後に申請を受け付ける。 ・在留申請、特別永住許可申請及び在留カードに係る届出等は、様式を定めた提出方式によるものであり、申請者本人又は関係者に限定した情報のみ記載することとしている。 ③親族（配偶者、子、父又は母（法定代理人を除く））、弁護士・行政書士、外国人の所属機関等の職員が提出する場合 ・窓口において、代理（※1）又は取次が認められている者から以下の資料（※2）を提示させ、代理又は取次が認められていることの確認が完了した後に申請を受け付ける。 （※1）在留資格認定証明書交付申請においては、親族（配偶者、子、父又は母（法定代理人を除く））及び外国人の所属機関等の職員の代理申請が認められている。 （※2）親族（配偶者、子、父又は母（法定代理人を除く））：申請者との関係を証明する資料（住民票等）、弁護士・行政書士：地方出入国在留管理官署に届出を行うことで交付される届出済証明書、外国人の所属機関等の職員：在留資格認定証明書交付申請の場合は、当該機関の身分証明書等。取次の場合は、地方出入国在留管理官署に申出を行い適当と認められることで交付される申請等取次者証明書。 ・在留申請、特別永住許可申請及び在留カードに係る届出等は、様式を定めた提出方式によるものであり、申請者本人又は関係者に限定した情報のみ記載することとしている。 【在留申請（オンライン申請）における入手】 ①本人が提出する場合 ・在留申請オンラインシステム（RAS）の利用にあたっては、事前に発行されたID及びパスワード認証による本人確認を行う。 ・利用申出時に利用者のマイナンバーカードの署名用電子証明書及び利用者証明用電子証明書の有効性の確認を行い、在留諸申請時に利用者証明用電子証明書の有効性の確認及び利用申出時のマイナンバーカードとの同一性確認を行う。 ・在留申請は、様式を定めた提出方式によるものであり、申請者本人又は関係者に限定した情報のみ記載することとしている。 ②法定代理人が提出する場合 ・在留申請オンラインシステム（RAS）の利用にあたっては、事前に発行されたID及びパスワード認証による本人確認を行う。 ・利用申出時に利用者のマイナンバーカードの署名用電子証明書及び利用者証明用電子証明書の有効性の確認を行い、在留諸申請時に利用者証明用電子証明書の有効性の確認及び利用申出時のマイナンバーカードとの同一性確認を行う。 ・在留申請は、様式を定めた提出方式によるものであり、申請者本人又は関係者に限定した情報のみ記載することとしている。 ③親族（配偶者、子、父又は母（法定代理人を除く））、弁護士・行政書士、外国人の所属機関等の職員が提出する場合 ・在留申請オンラインシステム（RAS）の利用にあたっては、事前に発行されたID及びパスワード認証による本人確認を行う。 ・親族（配偶者、子、父又は母（法定代理人を除く））については、利用申出時に利用者のマイナンバーカードの署名用電子証明書及び、利用者証明用電子証明書の有効性の確認を行い、在留諸申請時に利用者証明用電子証明書の有効性の確認及び、利用申出時のマイナンバーカードとの同一性確認を行う。 ・弁護士・行政書士については、事前に地方出入国在留管理官署に届出を行ったうえでなければ、利用申出を行うことができない。 ・外国人の所属機関等の職員については、地方出入国在留管理官署に利用申出を行い、同官署の承認を受けなければ、システムを利用することができない。 ・在留申請は、様式を定めた提出方式によるものであり、申請者本人又は関係者に限定した情報のみ記載することとしている。 【住民基本台帳ネットワークシステムからの入手】 ・住民基本台帳ネットワークシステムに対象者の条件等を提示し、その条件に適合した対象者のみの情報の提供を受けているため、対象者以外の情報を入手することはない。

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	【在留申請（窓口申請）、在留カードに係る届出等における入手】 申請は、様式を定めた提出方式によるものであり、申請に必要な情報に限定した情報のみ記載することとしているため、不必要な情報の入手はできない。 【在留申請（オンライン申請）における入手】 申請は、様式を定めた提出方式によるものであり、申請に必要な情報に限定した情報のみ記載することとしているため、不必要な情報の入手はできない。 【住民基本台帳ネットワークシステムからの入手】 住民基本台帳ネットワークシステムから提供される情報は、個人番号及び基本情報のみにシステム制御されているため、不必要な情報の入手はできない。
その他の措置の内容	電子記録媒体を用いて地方公共団体情報システム機構から入手する場合、電子記録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、地方公共団体情報システム機構とは協定書を締結し、電子記録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、当庁における適切な保管及び廃棄を確認している。電子記録媒体内の情報には暗号化処理を施す。
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク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	【在留申請（窓口申請）、在留カードに係る届出等における入手】 在留申請等の際は、使用目的を明示するとともに、不必要な情報の提供を求めないこととする。 【在留申請（オンライン申請）における入手】 申請フォームでは、使用目的を明示するとともに、不必要な情報の提供を求めないこととする。 【住民基本台帳ネットワークシステムからの入手】 ・地方公共団体情報システム機構（住民基本台帳ネットワークシステム）は、使用目的が法令に基づくものである場合に限り提供を行う。また、情報の入手は、地方公共団体情報システム機構及び出入国在留管理庁双方のシステム間で行うため、申請者に負担を生じることはない。 ・電子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	[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	【在留申請（窓口申請）、在留カードに係る届出等における入手】 窓口において申請を受け付ける場合は、原則、本人の在留カード等を確認する。 【在留申請（オンライン申請）における入手】 ・在留申請オンラインシステム（RAS）の利用にあたっては、事前に利用者登録によって発行されたID及びパスワード認証による本人確認を行う。 なお、外国人本人、法定代理人及び親族（配偶者、子、父又は母）については、利用申出時に利用者のマイナンバーカードの署名用電子証明書及び利用者証明用電子証明書の有効性の確認を行い、在留諸申請時に利用者証明用電子証明書の有効性の確認及び利用申出時のマイナンバーカードとの同一性確認を行う。 ・弁護士・行政書士については、事前に地方出入国在留管理官署に届出を行ったうえでなければ、利用申出を行うことができない。 ・外国人の所属機関等の職員については、地方出入国在留管理官署に利用申出を行い、同官署の承認を受けなければ、システムを利用することができない。 【住民基本台帳ネットワークシステムからの入手】 住民基本台帳ネットワークシステムからの入手にあたっては、番号利用法の規定に基づき地方公共団体情報システム機構が個人番号を生成しており、個人番号が本人の情報であることは担保されている。

個人番号の真正性確認の措置の内容	【在留申請(窓口申請、オンライン申請)、在留カードに係る届出等における入手】 ・本人等から提示された個人番号については、まずは個人番号情報管理システム(IMS)での登録状況を確認する。当該個人番号が対象者の個人番号として登録済みである場合は、当該個人番号の真正性を確認できたものとする。 ・対象者の個人番号が未登録又は登録済みであるが提示された個人番号と一致しない場合は、提示された個人番号を同システムに仮登録し、その真正性を確認するため、当該個人番号に紐づく基本4情報を住民基本台帳ネットワークシステムに照会して取得し、個人番号情報管理システム(IMS)で登録されている基本4情報と突合する。 【住民基本台帳ネットワークシステムからの入手】 住民基本台帳ネットワークシステムからの入手にあたっては、番号利用法の規定に基づき地方公共団体情報システム機構が個人番号を生成しており、個人番号が本人の情報であることは担保されている。		
特定個人情報の正確性確保の措置の内容	申請等の際に提示された個人番号・基本4情報と住民基本台帳ネットワークシステムから取得した個人番号・基本4情報を突合することで正確性を確保する。		
その他の措置の内容	住民基本台帳ネットワークシステムからの入手にあたっては、入手経路(専用線または例外的な電子記録媒体)に関わらず、番号利用法の規定に基づき地方公共団体情報システム機構が個人番号を生成しており、個人番号が本人の情報であることは担保されている。		
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている	
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	【在留申請(窓口申請)、在留カードに係る届出等における入手】 窓口において申請を受け付ける場合、申請者のマイナンバーカードから個人番号を読み取るなどして、個人番号情報管理システム(IMS)に直接登録することで、個人番号の漏えい・紛失等のリスクを回避し、機密性を確保している。 個人番号が記載された資料を提示された場合、個人番号情報管理システム(IMS)に当該番号を直接入力し、速やかに資料を返却することで、個人番号の漏えい・紛失等のリスクを回避し、機密性を確保している。 個人番号が記載された資料の提出を受けた場合、個人番号情報管理システム(IMS)に当該番号を直接入力し、当該資料の個人番号部分を黒塗り等することで、個人番号の漏えい・紛失等のリスクを回避し、機密性を確保している。 【在留申請(オンライン申請)における入手】 在留申請オンラインシステム(RAS)は、ユーザ認証機能、アクセス制御機能、ユーザアカウント認証機能、証跡管理機能、システム監視機能等を有しており、情報を送受信する場合は情報を暗号化する等のセキュリティ対策を講じることで機密性を確保している。 【住民基本台帳ネットワークシステムからの入手】 ・住民基本台帳ネットワークシステムとの接続では、通信の暗号化等の高度なセキュリティを維持した専用回線を利用することで機密性を確保している。 ・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	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている	
特定個人情報の入手(情報提供ネットワークシステムを通じた入手を除く。)におけるその他のリスク及びそのリスクに対する措置			
—			

3. 特定個人情報の使用		
リスク1: 目的を超えた紐付け、事務に必要なない情報との紐付けが行われるリスク		
宛名システム等における措置の内容	個人番号情報管理システム(IMS)においては、特定個人情報を取り扱う権限が与えられた者以外はアクセスできないようシステム制御した上で、外国人出入国情報システム(FEIS)の保有情報へのアクセスを制御することにより、目的を超えた情報連携や事務に必要なないデータへのアクセスができないようにする。	
事務で使用するその他のシステムにおける措置の内容	【外国人出入国情報システム(FEIS)】 ・外国人出入国情報システム(FEIS)では、個人番号を保有しない。 ・外国人出入国情報システム(FEIS)と個人番号情報管理システム(IMS)、外国人出入国情報システム(FEIS)と在留申請オンラインシステム(RAS)間には、ファイアウォールを有効化しており、定められた通信以外は連携できない仕組みとしている。 ・外国人出入国情報システム(FEIS)の機能から在留申請オンラインシステム(RAS)の保有する個人番号へのアクセスは、バッチ処理のみによってシステムで制御している。そのため、職員は外国人出入国情報システム(FEIS)の画面等を通じて在留申請オンラインシステム(RAS)の保有する個人番号へアクセスすることはない。 【在留申請オンラインシステム(RAS)】 ・申請者が申請情報の入力～申請完了までの間、在留申請オンラインシステム(RAS)で個人番号が一時保存されるが、外国人出入国情報システム(FEIS)に対し申請情報・個人番号を送信後、速やかに在留申請オンラインシステム(RAS)上から削除される。 ・申請者が在留申請オンラインシステム(RAS)に入力した情報は自動的に外国人出入国情報システム(FEIS)へ連携されるため、出入国在留管理庁の職員が在留申請オンラインシステム(RAS)を介して目的を超えた紐付けや必要の無い情報との紐付けは行えない仕組みとしている。 【住民基本台帳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では、通信の暗号化等の高度なセキュリティを維持した専用回線を利用するため、他のシステムからのアクセスや人為的なアクセスが行われることはない。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2: 権限のない者(元職員、アクセス権限のない職員等)によって不正に使用されるリスク		
ユーザ認証の管理	[行っている]	<選択肢> 1) 行っている 2) 行っていない
具体的な管理方法	【外国人出入国情報システム(FEIS)】 ・ユーザ認証はID、パスワードによる認証を行い、IDは共用ではなく個人ごとにユーザIDを割り当てている。 ・パスワードの最長有効期限を定め、定期的に更新を実施するようシステムで制御している。 【個人番号情報管理システム(IMS)、在留申請オンラインシステム(RAS)】 ・個人番号情報管理システム(IMS)及び在留申請オンラインシステム(RAS)のID、パスワードは、それぞれ外国人出入国情報システム(FEIS)と連携しており、外国人出入国情報システム(FEIS)と共通のID、パスワードを用いている。 ・ユーザ認証は、ID、パスワードによる認証を行い、IDは共用ではなく個人ごとにユーザIDを割り当てている。 ・パスワードの最長有効期限を定め、定期的に更新を実施するようシステムで制御している。 【住基ネット連携サーバー】 ・システム操作や特定個人情報等へのアクセスを行う前にログイン操作を行い、操作者を認証するようシステムで制御している。 ・システムへアクセスできる者を特定し、必要最小限度の範囲でのみ特定個人情報を取り扱うことができるように利用者ごとにIDを割り当てる。 ・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	【外国人出入国情報システム (FEIS)】 (1) 発効管理 (権限発効) ・アクセス権限と事務の対応表を作成する。 ・管理者は、アクセス権限が必要となった利用者に対して、事務に必要な業務権限を確認し、必要なアクセス権限のみを付与する。 (2) 失効管理 ・管理者は、職員の退職により、不要となったユーザIDについては速やかに失効させ、職員の異動により業務上アクセス権限が不要となった職員に対しても、アクセス権限を速やかに失効・停止する。 【個人番号情報管理システム (IMS)、在留申請オンラインシステム (RAS)】 ・個人番号情報管理システム (IMS)、在留申請オンラインシステム (RAS) では、外国人出入国情報システム (FEIS) で一元管理している権限管理の情報を利用している。 ※住基ネット連携サーバーも同様の管理を実施	
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	・アクセス権限と事務の対応表を作成し、外国人出入国情報システム (FEIS) にて管理を行う。職員の退職及び異動については、出入国在留管理庁で管理する人事異動情報から職員情報を取得し、外国人出入国情報システム (FEIS) へ反映する。人事異動情報と外国人出入国情報システム (FEIS) で管理するアクセス権限の対応は定期的に見直しを行う。 ・アクセス権限の管理は、地方出入国在留管理官署の部署ごとに管理者を設置し、管理者が所属する職員のアクセス権限を管理する。 ・管理者はアカウントの棚卸を毎月実施し、不要となったアカウントを失効処理する。 ※住基ネット連携サーバーも同様の管理を実施	
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	・職員が特定個人情報へアクセスした履歴 (アクセスした個人番号、日時、職員ID等) はログとして個人番号情報管理システム (IMS) に保存される。 ・特定個人情報の使用記録の確認については、所属する職員の利用記録を処理結果として作成し、管理者が必要に応じ随時確認を行う。 ・番号利用法第23条及び番号利用法施行令 (平成26年3月31日政令第155号) 第30条により情報提供等の記録の保存期間が7年とされていることを考慮し、ログの保存期間は7年間以上とする。 ※住基ネット連携サーバーも同様に記録	
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	・「出入国在留管理庁保有個人情報等保護管理規程」を定め、業務上の目的以外の目的で、個人情報等へのアクセスを禁止している。また、個人情報等の取扱いに従事する職員に対し、保有個人情報等の取扱いについて理解を深め、個人情報及び特定個人情報等の保護に関する意識の高揚を図るための啓発その他必要な教育研修を行う。 ・個人番号を含むCSVやPDFファイル等をダウンロードする機能 (外部媒体へのダウンロードも含む。) は設けない。 (※) 住民基本台帳ネットワークシステムに本人確認用ファイルを送信するために職員の手動操作が必要となるが、その前処理 (個人番号情報管理システム (IMS) から住民ネット連携サーバーへの連携) は自動であり、職員が当該ファイルを確認することはできない。 ・職員が特定個人情報へアクセスした履歴 (個人番号、アクセスした日時、職員ID等) はログとして個人番号情報管理システム (IMS) に記録する。	
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	・あらかじめ定められた照会方式(ファイル連携方式)以外で特定個人情報ファイルの取得を禁止している。 ・個人番号を含むCSVやPDFファイル等をダウンロードする機能(外部媒体へのダウンロードも含む。)は設けない。 ・職員が特定個人情報へアクセスした履歴(個人番号、アクセスした日時、職員ID等)はログとして記録する。 ・複製の権限は、通常誰にも付与せず、該当操作が必要な場合に限り、システム管理者の監督のもと、承認された作業員に対して一時的に権限を付与する。また、作業終了時は、システム管理者の監督のもと、その権限を削除する。さらに、権限付与操作の監視、定期的な付与権限の棚卸しを行うことで、不正な権限取得や権限の削除漏れを防止する。
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の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	委託先を選定する際、個人情報管理体制を確認するため下記の事項を記載した「情報セキュリティの管理体制」を提出させることとしている。 ・行政機関等からの個人情報の取扱いを含む業務の受託実績 ・プライバシーマーク又はISO/IEC27001の認証取得状況 ・個人情報保護に関する基本方針・取扱い規程等の整備状況 ・個人情報保護に関する管理体制の整備状況 ・個人情報保護に関する教育、訓練の実施状況	
特定個人情報ファイルの閲覧者・更新者の制限	[制限している]	<選択肢> 1) 制限している 2) 制限していない
	具体的な制限方法	・委託先は、委託業務の実施に当たり、特定個人情報にアクセスできる業務委託員を必要最小限に特定し、当該者のみアクセス権限を付与する。また、アクセス権限の設定に当たっては、業務上の責務と必要性を勘案し、必要最小限の範囲に限って許可を与える。 ・通常時運用保守作業で使用するユーザは、データベース製品の機能を使用して、特定個人情報をマスキングして閲覧できないように制御する。なお、運用保守作業で特定個人情報を確認する必要が生じた場合は、委託先から出入国在留管理庁に依頼の上、特定個人情報を閲覧可能なユーザIDを都度払い出す。
特定個人情報ファイルの取扱いの記録	[記録を残している]	<選択肢> 1) 記録を残している 2) 記録を残していない
	具体的な方法	特定個人情報ファイルへのアクセス記録を取得し、作業実施後に委託業務以外の作業を実施していないか確認する。
特定個人情報の提供ルール	[定めている]	<選択肢> 1) 定めている 2) 定めていない
	委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	契約書に、契約の履行において知り得た秘密を他に漏らしてはならない旨定めており、委託先から他者への特定個人情報の提供は認めていない。また、締結した契約書等に基づく特定個人情報の取扱い状況に関して、出入国在留管理庁職員が定期的に現地調査にて確認する。
	委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	委託先に提供する際、使用目的、情報の内容を記載した申請書を使用し、それを出入国在留管理庁の情報セキュリティ責任者が確認する。授受記録については、媒体、利用期限、返却方法を記載した台帳を作成し、翌年度の初日から起算して5年間保管する。また、提供情報は受託業務完了時に全て返却又は消去する。
特定個人情報の消去ルール	[定めている]	<選択肢> 1) 定めている 2) 定めていない
	ルールの内容及びルール遵守の確認方法	・特定個人情報が記録された書面を廃棄する場合には、復元が困難な状態にする。また、特定個人情報が保存された電子計算機及び電子媒体を廃棄する場合は、データ消去ソフトウェア若しくはデータ消去装置の利用又は物理的な破壊若しくは磁気的な破壊により、復元が困難な状態にする。消去作業後に、廃棄等に関する実施結果を出入国在留管理庁に報告する。 ・委託契約終了後、委託先から特定個人情報等の消去・廃棄等に関する報告書を提出させ、消去及び廃棄状況の確認を行う。
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	出入国在留管理庁と委託先との間で、以下の規定を定める。 ・秘密保持義務 ・事業所内からの特定個人情報の持ち出しの禁止 ・特定個人情報の目的外利用の禁止 ・漏えい事案等が発生した場合の委託先の責任 ・委託契約終了後の特定個人情報の返却又は廃棄 ・委託先における情報の複製の禁止 ・従業者に対する監督・教育 ・契約内容の遵守状況について報告を求める規定 ・再委託における条件

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	・個人情報保護のための情報セキュリティの徹底を図る観点から、委託業務の範囲に係るISO/IEC27001又はJIS Q 27001に適合していることの認証を取得していること、又はそれと同等以上の情報セキュリティ管理体制を有することを証明できる資料を提示できることを、応札条件としている。 委託先が業務を再委託する場合は、次の事項を条項に含む契約・誓約書を締結し、特定個人情報の適切な取扱いの確保を図ることとしている。 ・秘密保持義務 ・特定個人情報の持ち出しの禁止 ・特定個人情報の目的外利用の禁止 ・情報の複写複製の禁止 ・漏えい、滅失、毀損の禁止 ・出入国在留管理庁による調査への協力	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		
—		

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		[] 提供・移転しない
リスク1： 不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録	[記録を残している]	<選択肢> 1) 記録を残している 2) 記録を残していない
具体的な方法	住民基本台帳ネットワークシステムと連携する個人番号を含む個人番号確認用ファイルへのアクセス記録を取得し、作業実施後に委託業務以外の作業を実施していないか確認する。	
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	バッチプログラムで操作ログを参照し、暗号化済み、送信済み、復号化済みファイルをバックアップ用フォルダへ移動する。バックアップし一定日時(10日)経過後のファイルは削除する。 バッチプログラムはデスクトップにショートカットを作成する等により手動により実施できるようにする。また、バッチプログラムを定期的に行う(1回/時)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： 不適切な方法で提供・移転が行われるリスク		
リスクに対する措置の内容	通信の暗号化等の高度なセキュリティを維持した専用ネットワークを利用し、安全性を確保する。	
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： 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	通信の暗号化等の高度なセキュリティを維持した専用ネットワークを利用し、安全性を確保する。	
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
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	【中間サーバー相当機能における措置】 ・情報照会機能(※1)により、情報提供ネットワークシステムに情報照会を行う際には、提供許可証の発行と照会内容の照会許可照会リスト(※2)との照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから提供許可証を受領してから情報照会を実施することになる。つまり、番号利用法上認められた情報連携以外の照会を拒否する機能を備えており、目的外入手やセキュリティリスクに対応している。 ・中間サーバー相当機能の職員認証・権限管理機能(※3)では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 (※1) 情報提供ネットワークシステムを使用した特定個人情報の照会及び照会した情報の受領を行う機能。 (※2) 番号利用法の規定による情報提供ネットワークシステムを使用した特定個人情報の提供に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの。 (※3) 中間サーバー相当機能を利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。 【個人番号情報管理システム(IMS)・外国人出入国情報システム(FEIS)における措置】 ・決められた事務の流れの中でシステム的に情報照会が行われるようにすることで、業務と離れた形で個別に照会が行われないようにしている。 ・個人番号情報管理システム(IMS)及び外国人出入国情報システム(FEIS)では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。		
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている	
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	【中間サーバー相当機能における措置】 ・中間サーバー相当機能は、個人情報保護委員会との協議を経て、内閣総理大臣が設置・管理する情報提供ネットワークシステムを使用した特定個人情報の入手のみ実施できるよう設計されるため、安全性が担保されている。 ・中間サーバー相当機能と既存システム、公共サービスメッシュ機関間情報連携サービス(インターフェイスシステム)との間は、通信の暗号化等の高度なセキュリティを維持した専用ネットワーク(政府共通ネットワーク等)を利用し、安全性を確保する。		
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			
リスクに対する措置の内容	【中間サーバー相当機能における措置】 中間サーバー相当機能は、個人情報保護委員会との協議を経て、内閣総理大臣が設置・管理する情報提供ネットワークシステムを使用して、情報提供用個人識別符号により紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。		
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている	

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	【中間サーバー相当機能における措置】 ・中間サーバー相当機能は、情報提供ネットワークシステムを使用した特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応している。 ・既存システムからの接続に対し認証を行い、許可されていないシステムからのアクセスを防止する仕組みを設けている。 ・情報照会が完了又は中断した情報照会結果については、一定期間経過後に当該結果を情報照会機能において自動で削除することにより、特定個人情報漏えい・紛失するリスクを軽減している。 ・中間サーバー相当機能の職員認証・権限管理機能ではログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 ・中間サーバー相当機能と既存システム、公共サービスメッシュ機関間情報連携サービス（インターフェイスシステム）との間には高度なセキュリティを維持した専用ネットワーク（政府共通ネットワーク等）を利用することにより、漏えい・紛失のリスクに対応している。 ・中間サーバー相当機能の運用保守についてデジタル庁が委託した事業者の業務は、中間サーバー相当機能の運用、監視・障害対応等であり、特定個人情報は出入国在留管理庁の鍵でデータの暗号化を行うため、業務上、中間サーバー相当機能の運用保守についてデジタル庁が委託した事業者は特定個人情報へはアクセスすることはできない。 （※）中間サーバー相当機能は、情報提供ネットワークシステムを使用して特定個人情報を送信する際、送信する特定個人情報の暗号化を行っており、照会者の中間サーバー相当機能でしか復号できない仕組みになっている。そのため、情報提供ネットワークシステムでは復号されないものとなっている。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
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	【中間サーバー相当機能における措置】 ①情報提供機能（※）により、情報提供ネットワークシステムにおける照会許可照会リストを情報提供ネットワークシステムから入手し、中間サーバー相当機能にも格納して、情報提供機能により、照会許可照会リストに基づき情報連携が認められた特定個人情報の提供の要求であるかチェックを実施している。 ②情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供ネットワークシステムから情報提供許可証と情報照会者へたどり着くための経路情報を受領し、照会内容に対応した情報を自動で生成して送付することで、特定個人情報不正に提供されるリスクに対応している。 ③特に慎重な対応が求められる情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報不正に提供されるリスクに対応している。 ④中間サーバー相当機能の職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）情報提供ネットワークシステムを使用した特定個人情報の提供の要求の受領及び情報提供を行う機能。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク6: 不適切な方法で提供されるリスク		
リスクに対する措置の内容	【中間サーバー相当機能における措置】 ・セキュリティ管理機能（※）により、情報提供ネットワークシステムに送信する情報は、情報照会者から受領した暗号鍵で暗号化を適切に実施した上で提供を行う仕組みになっている。 ・中間サーバー相当機能の職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 ・中間サーバー相当機能と既存システム、公共サービスメッシュ機関間情報連携サービス（インターフェイスシステム）の間は、高度なセキュリティを維持した専用ネットワーク（政府共通ネットワーク等）を利用することにより、不適切な方法で提供されるリスクに対応している。 ・中間サーバー相当機能の運用保守についてデジタル庁が委託した事業者においては、特定個人情報にはアクセスができないよう管理を行い、不適切な方法での情報提供を行えないよう管理している。 （※）暗号化・復号機能と、鍵情報及び照会許可照会リストを管理する機能。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

リスク7: 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク	
リスクに対する措置の内容	【中間サーバー相当機能における措置】 ・情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供許可証と情報照会者への経路情報を受領した上で、情報照会内容に対応した情報提供をすることで、誤った相手に特定個人情報提供されるリスクに対応している。 ・情報提供データベース管理機能(※)により、「情報提供データベースへのインポートデータ」の形式チェックと、接続端末の画面表示等により情報提供データベースの内容を確認できる手段を準備することで、誤った特定個人情報を提供してしまうリスクに対応している。 ・情報提供データベース管理機能では、情報提供データベースの副本データを既存業務システムの原本と照合するためのエクスポートデータを出力する機能を有している。 (※)特定個人情報を副本として保存・管理する機能。
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置	
【中間サーバー相当機能における措置】 ・情報連携においてのみ、情報提供用個人識別符号を用いることがシステム上担保されており、不正な名寄せが行われるリスクに対応している。 ・中間サーバー相当機能では、特定個人情報を管理するデータベースを機関ごとに区分管理(アクセス制御)しており、中間サーバー相当機能を利用する機関であっても他機関が管理する情報には一切アクセスできない。 ・特定個人情報の管理を出入国在留管理庁のみが行うことで、中間サーバー相当機能の運用保守についてデジタル庁が委託した事業者における情報漏えい等のリスクを極小化する。	

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	【中間サーバー相当機能における措置】 中間サーバー相当機能はガバメントクラウドに設置する。 ・ガバメントクラウドについては政府情報システムのためのセキュリティ評価制度(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。 ・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。 【出入国在留管理庁内(中間サーバー相当機能以外)における措置】 ・サーバー設置場所への入退室については、入退室管理システムで記録・管理する。 ・サーバー設置場所においては、入退室管理を徹底するため出入り口の場所を限定する。 ・特定個人情報は、インターネットと接続された端末(情報系端末)や情報系システムの共有フォルダには保管しない。 ・端末(FEIS端末)が設置されている執務室等の電子錠等による入室制限を実施している。 ・庁舎への出入口に監視カメラを設置しており、端末(FEIS端末)やサーバーの設置場所も含む、庁舎内における関係者以外の立入が禁止されている領域への第三者の侵入を抑止・検知する体制を構築している。

⑥技術的対策	[十分にやっている] <選択肢> 1) 特に力を入れてやっている 2) 十分にやっている 3) 十分にやっていない
具体的な対策の内容	【中間サーバー相当機能における措置】 中間サーバー相当機能はガバメントクラウドに設置する。 ①出入国在留管理庁が管理する業務データは、デジタル庁及びクラウド事業者がアクセスできない契約等とし、アクセス制御等の必要な措置を講じる。 ②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。 ③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。 ④デジタル庁(若しくは、中間サーバー相当機能の運用保守についてデジタル庁が委託した事業者)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。 ⑤デジタル庁(若しくは、中間サーバー相当機能の運用保守についてデジタル庁が委託した事業者)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。 ⑥ガバメントクラウドの特定個人情報保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。 ⑦出入国在留管理庁や出入国在留管理庁が委託した事業者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。 【出入国在留管理庁内(中間サーバー相当機能以外)における措置】 ・個人番号情報管理システム(IMS)、外国人出入国情報システム(FEIS)はインターネットに接続していないため、保有する特定個人情報インターネットに流出することはない。住基ネット連携サーバーは、地方公共団体情報システム機構に対して住基ネット専用線を用いて接続し、地方公共団体情報システム機構から提供されている手順に基づいて連携するため、特定個人情報が流出することはない。また在留申請オンラインシステム(RAS)において保有する特定個人情報がインターネットに流出することのないよう、システム面の措置を講じている。 ・ファイアウォール、URLフィルタリング、ウイルス対策ソフト等を導入し、アクセス制限、侵入検知及び侵入防止を行う。 ・不正アクセス対策については、侵入防止及び侵入検知機能を有した装置を導入し、ネットワークへの不正侵入を検知し、管理者に通知する仕組みとする。また、本システムのネットワーク上に許可のない端末が接続した場合、検知、通信の遮断、管理者へ通知する仕組みとする。 ・ウイルス対策ソフトのパターンファイルの更新、導入しているOS及びミドルウェアについて必要に応じセキュリティパッチの適用を行う。 ・個人番号を含むCSVやPDFファイル等をダウンロードする機能(外部媒体へのダウンロードも含む。)は設けない。 ・職員が特定個人情報へアクセスした履歴(個人番号、アクセスした日時、職員ID等)はログとして記録する。 ・特定個人情報を参照可能なユーザは、ユーザID不正使用や業務情報の不正使用による情報漏えいのリスクに備え、承認/非承認作業に関わらず当該ユーザが使用された際に検知できるよう監査データをリアルタイムで監視する。 ・端末(FEIS端末)入力したパスワードが画面上で伏字で表示される機能を導入している。
⑦バックアップ	[十分にやっている] <選択肢> 1) 特に力を入れてやっている 2) 十分にやっている 3) 十分にやっていない
⑧事故発生時手順の策定・周知	[十分にやっている] <選択肢> 1) 特に力を入れてやっている 2) 十分にやっている 3) 十分にやっていない

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も引き続き生存者の個人番号と同様の方法で保管することとしている。	
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: 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	利用者の申請等により、特定個人情報(在留資格情報等)に変更等が生じた場合はその都度データを更新する。	
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	[定めていない]	＜選択肢＞ 1) 定めている 2) 定めていない
手順の内容	—	
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		
・当庁では「出入国在留管理庁保有個人情報等保護管理規程」第25条において個人情報等の漏えい等の事案が発生した場合の報告義務を規定している。 ＜出入国在留管理庁保有個人情報等保護管理規程＞ (事案の報告等) 第25条 保有個人情報等の漏えい等の事案の発生又は兆候を把握した場合、職員がこの規程等に違反している事実又は兆候を把握した場合その他安全確保の上で問題となる事案が発生した場合に、その事実を知った職員は、直ちに当該保有個人情報等を管理する保護管理者に報告する。 2 保護管理者は、被害の拡大防止又は復旧等のために必要な措置を速やかに講ずる。ただし、被害拡大防止のため直ちに講じ得る措置については、直ちに講ずるものとする。 3 保護管理者は、事案の発生した経緯、被害状況等を調査し、部課等保護管理者に報告する。ただし、特に重大と認める事案が発生した場合には、直ちに部課等保護管理者に当該事案の内容等について報告する。 4 部課等保護管理者は、前項の規定に基づく報告を受けた場合には、当該事案の内容、経緯、被害状況等を総括保護管理者に報告する。 5 総括保護管理者は、前項の規定に基づく報告を受けた場合には、事案の内容等に応じて、当該事案の内容、経緯、被害状況等を出入国在留管理庁長官に速やかに報告する。 6 総括保護管理者は、第4項又は前項の規定に基づく報告が個人情報保護法第68条第1項に規定する場合又は行政機関等匿名加工情報等に係るものであった場合には、当該案件の内容等を個人情報保護委員会に直ちに報告する。 7 部課等保護管理者及び保護管理者は、事案の発生した原因を分析し、再発防止のために必要な措置を講ずる。 8 部課等保護管理者は、前項の規定に基づく再発防止のために講じた措置が行政機関等匿名加工情報に係るものであった場合には、講じた措置の内容等を総括保護管理者に直ちに報告する。 9 総括保護管理者は、前項の規定に基づく報告を受けた場合には、講じた措置の内容等を個人情報保護委員会に直ちに報告する。 ・電子記録媒体を利用する場合においては、電子記録媒体の利用後速やかに媒体上のデータを完全消去し、媒体を物理的に破壊する。		

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) 十分に行っていない
具体的なチェック方法	【中間サーバー相当機能における措置】 運用規則等に基づき、中間サーバー相当機能の運用に携わる職員及び事業者において、定期的に自己点検を実施することとしている。 【出入国在留管理庁内(中間サーバー相当機能以外)における措置】 情報セキュリティポリシー等に規定されている事項について定期的に職員による自己点検を行い、その点検結果について管理者が確認を行う。自己点検の結果、改善が必要な場合は、速やかに改善のための対応策を検討して、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) 十分に行っていない
具体的な内容	【中間サーバー相当機能における措置】 運用規則等に基づき、中間サーバー相当機能について、デジタル庁が定期的に監査を行うこととしている。出入国在留管理庁は、デジタル庁による中間サーバー相当機能の運用に係る監査の結果を確認することにより、中間サーバー相当機能の運用に問題がないかを確認する。 【出入国在留管理庁内(中間サーバー相当機能以外)における措置】 ・個人情報の管理方法等について定めた規程の遵守状況等について、定期的に本庁職員による内部監査を実施する。監査における指摘事項については次回の監査時に改善状況を確認し、PDCAサイクルによる課題又は問題点の把握、改善に努める。 ・特定個人情報の取扱いに関する項目を監査項目に盛り込んでいる。	
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) 十分に行っていない
具体的な方法	【中間サーバー相当機能における措置】 ・中間サーバー相当機能の運用に携わる職員及び事業者に対し、セキュリティ研修等を実施することとしている。 ・中間サーバー相当機能の業務に就く場合は、運用規則等について研修を行うこととしている。 【出入国在留管理庁内における教育・啓発】 ・情報セキュリティポリシー等に規定されている事項について必要な教育・研修を行う。 ・情報セキュリティポリシー等に規定されている事項について定期的に職員による自己点検を行い、その点検結果について管理者が確認を行う。自己点検の結果、改善が必要な場合は、速やかに改善のための対応策を検討して、実施する。	
3. その他のリスク対策		
【中間サーバー相当機能における措置】 中間サーバー相当機能はガバメントクラウドに設置する。 ・ガバメントクラウド上での業務データの取扱いについては、当該業務データを保有する出入国在留管理庁及び出入国在留管理庁が委託した事業者が責任を有する。 ・ガバメントクラウド上でデジタル庁が構築・運用するアプリケーションの運用等に障害が発生した場合等の対応については、原則としてガバメントクラウドに起因する事象の場合は、デジタル庁はクラウド事業者と契約する立場から、その契約を履行させることで対応する。また、ガバメントクラウドに起因しない事象の場合は、中間サーバー相当機能の運用保守についてデジタル庁が委託した事業者又はガバメントクラウド運用管理補助者が対応するものとする。 ・具体的な取り扱いについて、疑義が生じる場合は、出入国在留管理庁とデジタル庁及び関係者で協議を行う。		

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	【出入国在留管理庁の開示請求先】 出入国在留管理庁総務課出入国情報開示係 〒160-0004 東京都新宿区四谷1-6-1 四谷タワー13F 03-5363-3005 (https://www.moj.go.jp/isa/publications/disclosure/kaiji_release.html)
②請求方法	指定様式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。
特記事項	-
③手数料等	[有料] <選択肢> 1) 有料 2) 無料 (手数料額、納付方法: 1件300円、収入印紙の貼付により納付。)
④個人情報ファイル簿の公表	[行っている] <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	外国人出入国記録マスタファイル、日本人出帰国記録マスタファイル、上陸審査における個人識別情報提供記録ファイル、自動化ゲート利用希望者登録記録マスタファイル、電子届出システム利用者登録情報ファイル、乗客予約記録情報マスタファイル、特定登録者情報マスタファイル、回収原票記録、在留申請オンラインシステム利用者情報マスタファイル
公表場所	電子政府総合窓口
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	出入国在留管理庁総務課出入国情報開示係 〒160-0004 東京都新宿区四谷1-6-1 四谷タワー13F 03-5363-3005
②対応方法	室内で必要な調整を行い、担当する部署等において対応する。

VI 評価実施手続

1. 基礎項目評価	
①実施日	令和7年9月30日
②しきい値判断結果	[基礎項目評価及び全項目評価の実施が義務付けられる] <選択肢> 1) 基礎項目評価及び全項目評価の実施が義務付けられる 2) 基礎項目評価及び重点項目評価の実施が義務付けられる(任意に全項目評価を実施) 3) 基礎項目評価の実施が義務付けられる(任意に全項目評価を実施) 4) 特定個人情報保護評価の実施が義務付けられない(任意に全項目評価を実施)
2. 国民・住民等からの意見の聴取	
①方法	e-Govにおいて意見公募手続を行い、電子メール又は書面にて意見を受付。
②実施日・期間	令和7年8月17日から令和7年9月16日までの30日間
③期間を短縮する特段の理由	—
④主な意見の内容	誤字脱字、表記ゆれに関する御意見の御意見が1件、出入国在留管理行政におけるマイナンバーによる情報連携の利用に関する御意見が3件、番号利用法に関する御意見が1件、公共サービスメッシュの利用に関する御意見が1件、個人情報の取扱いに関する御意見が1件
⑤評価書への反映	誤字脱字、表記ゆれについては御意見を踏まえて評価書を修正した。
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9月30日
②個人情報保護委員会による審査	

(別添3) 変更箇所

[illegible]