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
2	情報提供ネットワークシステムの運営に関する事務 全項目評価書

個人のプライバシー等の権利利益の保護の宣言

情報提供ネットワークシステムにおける特定個人情報ファイルの取扱いに当たり、同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すものであることを認識し、情報漏えいその他の事態を発生させるリスクを軽減させることが必要である。このため、本システムにおいて不正な情報取得が行われないようシステムを設計し、特定個人情報の一元管理・把握が不可能な仕組みの導入等、特定個人情報の保護に係る適切な措置を講じることをもって、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	番号制度導入の目的である迅速かつ安全な情報連携を実現するため、情報提供ネットワークシステムは特定個人情報の照会・提供の媒介を行う。情報提供ネットワークシステムで保持する特定個人情報については、業務上必要最小限のものとすることで、特定個人情報の一元管理・把握を回避する。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（平成25年法律第27号。以下「番号法」という。）上認められた情報連携以外はシステム上連携しないなど、不正な情報連携の防止を図る。

評価実施機関名

内閣総理大臣

個人情報保護委員会　承認日 【行政機関等のみ】

令和6年10月9日

公表日

令和6年10月18日

［令和6年10月　様式4］

項目一覧

Ⅰ　基本情報

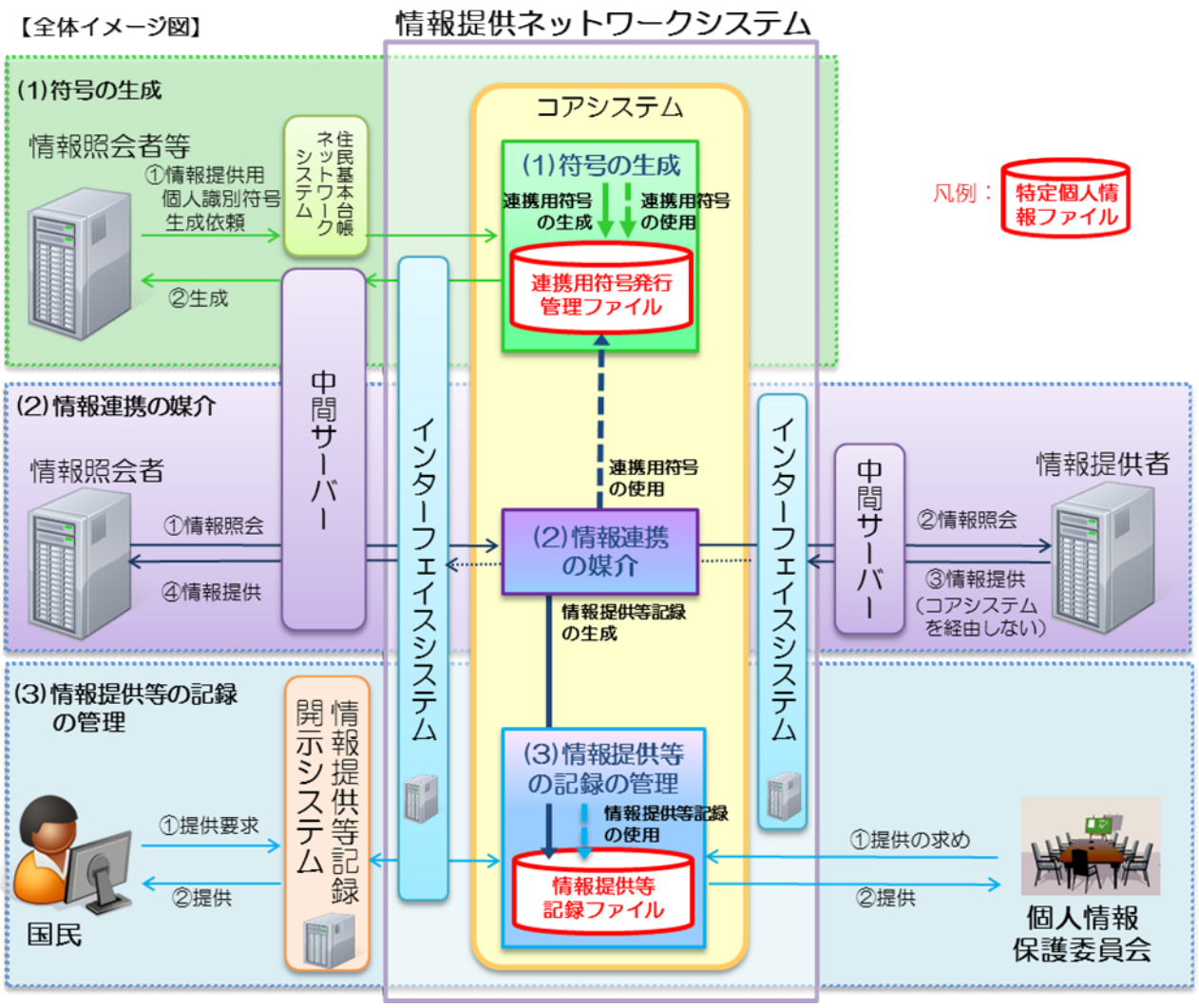
1. 特定個人情報ファイルを取り扱う事務	
①事務の名称	情報提供ネットワークシステムの運営に関する事務
②事務の内容　※	社会保障・税番号制度は、複数の機関に存在する個人の情報を同一人の情報であることの確認を行うための基盤であり、社会保障・税制度の効率性・透明性を高め、国民にとって利便性の高い公平・公正な社会を実現することを目的とした制度である。個人番号の利用は、より公平・公正な社会、社会保障がきめ細やかかつ的確に行われる社会、行政に過誤や無駄のない社会、国民にとって利便性の高い社会、国民の権利を守り、国民が自己情報をコントロールできる社会の実現を旨として行うものである。情報提供ネットワークシステムは、番号法に基づき特定個人情報の正確かつ安全な連携を行うために設置されるシステムである。個人情報についてはこれまでどおり、行政機関や地方公共団体等の情報照会者又は情報提供者（以下「情報照会者等」という。）がそれぞれの事務を遂行するために必要な情報を分散して管理することとし、情報照会者等が保有していない個人情報を必要とする場合には、情報提供ネットワークシステムを介した情報連携を行うこととする。これにより、個人情報を特定の情報照会者等へ集約したり、情報提供ネットワークシステムにて一元管理しないものとする。情報提供ネットワークシステムにより実現する事務は、次のとおりである。 (1)符号の生成（根拠法令：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施行令（平成26年政令第155号。以下「番号法施行令」という。）第27条） 情報の分散管理を実現するため、情報提供ネットワークシステムにおいては個人番号を一切用いず、個人を特定するために、個人番号に代えて符号を用いることとしている。すなわち、情報提供ネットワークシステムにおいて情報連携を行う際に符号を用いることにより、万が一、符号が漏えいした場合でも、符号が個人番号を含む個人情報と紐付けされることを防止することとしている。これを実現するため、情報提供ネットワークシステムは、情報照会者等からの依頼を受け、各種符号（連携用符号、情報提供用個人識別符号）を生成する。 (2)情報連携の媒介（根拠法令：番号法第21条） 情報照会者からの情報照会を情報提供者に対し連絡し、情報照会・提供の媒介を行う。情報の一元管理を防止するため、本機能においては、情報提供用個人識別符号を用いて特定個人情報の照会・提供に係る情報連携を媒介するのみとし、特定個人情報ファイルの保存は行わない。 また、番号法で認められた範囲（番号法第21条第2項）を超えて情報連携を行うことを防止するため、情報保有機関が情報提供ネットワークシステムとの接続開始時に、接続申請により特定個人情報保護評価が適切に実施されていることを確認する。また、情報照会者等が情報連携を行う都度、情報照会の内容と情報提供ネットワークシステム内で管理するファイルとを照合して当該情報連携が番号法で認められた事務等の範囲であることを確認する。なお、番号法で認められる範囲を超えている場合は情報連携を行わない。 (3) 情報提供等の記録の管理（根拠法令：番号法第23条） 番号法第23条の規定においては情報提供等の記録の記録・保存が義務付けられていることから、情報提供ネットワークシステムを介した情報照会・提供に係る事項については情報提供等の記録として保存する。情報提供等の記録を参照することで、いつどこで誰の特定個人情報が照会・提供されたのかを把握することができる。情報提供等の記録として保存するのは、情報照会・提供を行った日時や特定個人情報名などの記録のみであり、提供された情報の内容が記録されることはない。 情報提供等記録開示システムを介した本人からの情報提供等の記録の提供要求がなされた場合には、情報提供等の記録を提供する。また、番号法第35条第1項の規定により、個人情報保護委員会から報告を求められた場合には、番号法第19条第13号の規定により、特定個人情報を提供することとされており、この規定に基づき、個人情報保護委員会から情報提供等の記録の提供の求めがあった場合には、情報提供等の記録を提供する。 番号法第35条第1項の規定に基づく個人情報保護委員会への報告については、犯罪捜査を目的としたものではない。 （※）平成29年7月から情報提供等記録開示システムが稼働している。当該システムにより、自らの特定個人情報がどのように利用されたのか確認すること等ができる。
③対象人数	[　30万人以上　] ＜選択肢＞ 1) 1,000人未満　2) 1,000人以上1万人未満 3) 1万人以上10万人未満　4) 10万人以上30万人未満 5) 30万人以上

2. 特定個人情報ファイルを取り扱う事務において使用するシステム	
システム1	
①システムの名称	情報提供ネットワークシステム
②システムの機能	情報提供ネットワークシステムは、コアシステムとインターフェイスシステムにて構成されている。 コアシステムは、情報提供ネットワークシステムの中核的な機能を担い、(1)符号の生成、(2)情報連携の媒介、(3)情報提供等の記録の管理の3つの機能を有する。 (1)符号の生成 ・連携用符号及び情報提供用個人識別符号は、情報連携の媒介開始前にあらかじめ生成しておく必要があり、次の手順により生成する。 ・情報照会者等から情報提供用個人識別符号生成の依頼を受ける。 ・情報照会者等から、住民基本台帳ネットワークシステムを介して、情報提供用個人識別符号生成の対象者の住民票コードを受領する。 ・住民票コードを基に、暗号演算により、対象者ごとに異なり、情報提供用個人識別符号等の生成の基となる全ての情報照会者等に共通の連携用符号を生成し、連携用符号発行管理ファイルに保存する。住民票コードは連携用符号生成後に直ちに削除する。 ・連携用符号に暗号演算による変換を行うことにより、情報照会者等ごとに異なる情報提供用個人識別符号を生成し、依頼元の情報照会者等へ送信する。情報提供用個人識別符号は情報提供ネットワークシステムに保存しない。情報提供用個人識別符号の生成は、一連のシステム処理で自動的に行われており、連携用符号発行管理ファイルにより確認を行うことで、誤った情報照会者等へ提供されない仕組みとしている。 ・また、情報連携が行われる際にはその情報連携の記録を情報提供等記録ファイルに保存することとしているが、その際も、個人を特定するために、連携用符号に暗号演算による変換を行うことにより、情報提供等記録用符号を生成し、情報提供等記録ファイルに保存する。 (2)情報連携の媒介 ・情報照会者から、情報提供用個人識別符号による情報照会要求を受信する。 ・情報照会が、番号法で認められる範囲(番号法第21条第2項)かどうかの確認を行い、情報提供用個人識別符号及び照会内容等を情報提供者へ送信する。 ・情報提供者は、情報照会者に対し、特定個人情報の提供を行う。情報提供は、コアシステムを介さず、インターフェイスシステムを介して行われる。これにより、コアシステムにおいて特定個人情報が蓄積されることを防止する。情報提供の媒介は、一連のシステム処理にて自動的に行われることにより、誤った情報が提供されない仕組みとしている。 (3)情報提供等の記録の管理 ・番号法第23条の規定に基づき、情報連携における情報照会・提供に係る一連の過程に関する記録を自動的に作成し、情報提供等記録ファイルに保存する。その際、情報提供等の記録に関する提供要求等において個人を識別するものとして、個人番号(マイナンバー)を用いずに、情報提供等記録用符号を用いる。情報提供ネットワークシステムを使用して情報照会・提供が行われる都度、当該システム内で自動的に連携用符号から情報提供等記録用符号を生成し、情報提供等記録ファイルに保存する。 ・情報提供等記録開示システムを介して本人から提供要求を受信した際に、該当する情報提供等の記録を抽出し、インターフェイスシステムを介して情報提供等記録開示システムへ送信する。 ・番号法第35条第1項の規定により、個人情報保護委員会から報告を求められた場合には、番号法第19条第13号の規定により、特定個人情報を提供することとされており、この規定に基づき、個人情報保護委員会から情報提供等の記録の提供の求めがあった場合には、情報提供等の記録を提供する。 ・情報提供等の記録を基に、各種統計処理を実施する。 インターフェイスシステムは、情報提供ネットワークシステムの一部として情報照会者等となる国や地方公共団体等及び情報提供等記録開示システムの設置機関ごとに配置され、情報照会者等側のシステムとコアシステム等との接続の役割を担うシステムである。 情報連携を行う場合において、情報照会者はコアシステムを通じて照会を行うこととなるが、情報提供者が情報照会者に特定個人情報を提供する際は、コアシステムを介さず、インターフェイスシステムを介して行われる。これにより、コアシステムに特定個人情報が蓄積されないようにし、情報の一元管理が行われない仕組みとしている。また、情報提供等記録開示システムを介した本人からの情報提供等

	の記録の提供要求がなされた場合には、コアシステムに保存されている記録を、インターフェイスシステムを介して情報提供等記録開示システムに送信する。インターフェイスシステムは、情報を送信・受信するのみであり、特定個人情報は蓄積されない仕組みとしている。 また、令和8年1月以降においては、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）を含むものとする。 公共サービスメッシュは、コアシステムと機関間情報連携サービス（インターフェイスシステム）にて構成され、番号法第21条に規定される情報提供ネットワークシステムに相当するシステムである。 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）は、情報提供ネットワークシステムを構成するインターフェイスシステムと機能、役割等が同一であるため、評価書上は両システムをインターフェイスシステムとして扱う。 ※現行の情報提供ネットワークシステムは、令和7年1月から第三期情報提供ネットワークシステムへ移行する。 特定個人情報は第三期情報提供ネットワークシステムで継続して使用するためデータ移行を行う。 特定個人情報のデータ移行は専用回線で行うため安全である。 追加の対策として、①移行データの暗号化、②移行用一時ファイルのアクセス制限及び③ログ情報等の監査による不正の監視を行う。 利用しなくなった環境の破棄は、ディスクの物理破壊、廃棄証明書の提示などの厳格な対応を行う。
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　（情報提供等記録開示システム、各情報照会者等のシステム、個人情報保護委員会の監視・監督システム）
システム2～5	
システム6～10	
システム11～15	
システム16～20	

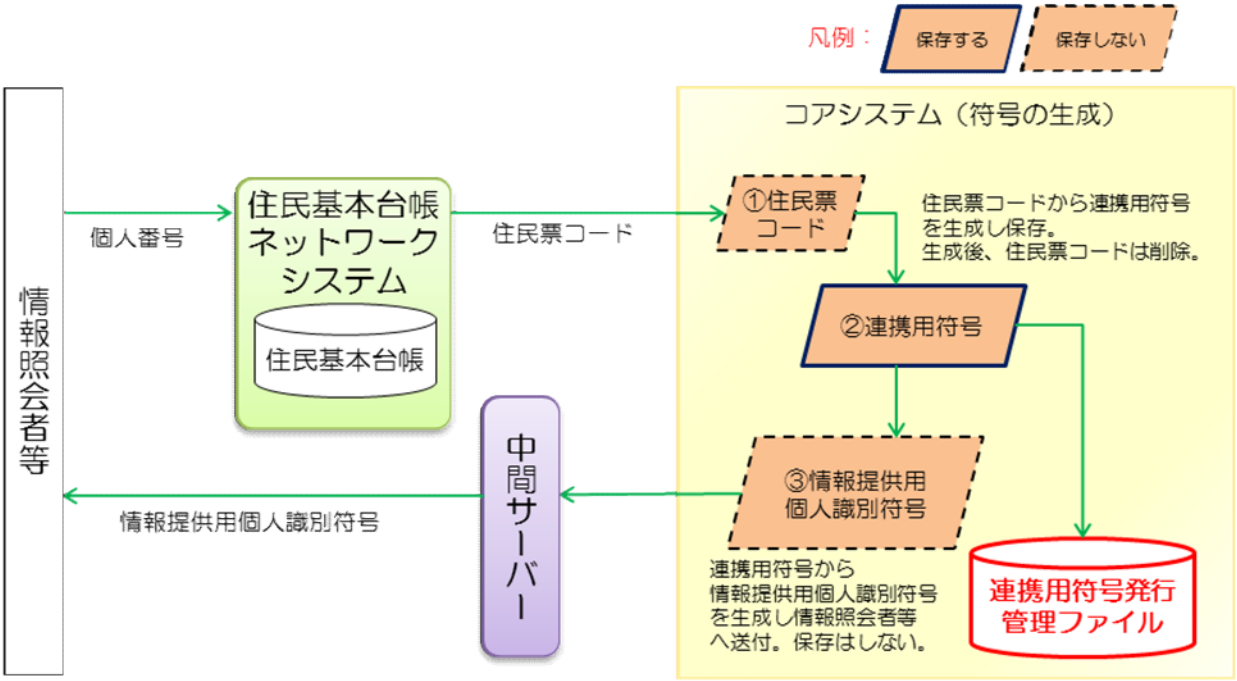
3. 特定個人情報ファイル名	
1. 連携用符号発行管理ファイル　2. 情報提供等記録ファイル	
4. 特定個人情報ファイルを取り扱う理由	
①事務実施上の必要性	情報提供ネットワークシステムの符号の生成機能及び情報提供等の記録の管理機能については、次の必要性から、特定個人情報ファイルとして連携用符号発行管理ファイル及び情報提供等記録ファイルを保有する。 (1)連携用符号発行管理ファイル 情報の分散管理を実現するため、情報提供ネットワークシステムにおいて個人番号を一切用いず、個人を特定するために、個人番号に代えて符号を用いることとしている。このため、情報提供ネットワークシステムは各種符号（連携用符号、情報提供用個人識別符号）を生成することとしており、①連携用符号の重複生成防止、②情報提供用個人識別符号の発行の有無の判定、③障害時等の調査を行うことを目的として、符号の生成・変換に必要な連携用符号管理情報を特定個人情報ファイルとして保有する必要がある。 (2)情報提供等記録ファイル 番号法第23条の規定において、情報提供等の記録の記録・保存が義務付けられていることから、情報提供ネットワークシステムを介した情報照会・提供に係る事項についての情報提供等の記録を特定個人情報ファイルとして保有する必要がある。
②実現が期待されるメリット	1. 国民の行政手続負担の軽減 　社会保障・税に係る行政手続における添付書類の削減が期待できる。 2. 公正・公平な行政の実現 　所得のより正確な捕捉により、きめ細やかな新しい社会保障制度の設計に資すると期待できる。 3. 行政の効率化 　情報を電子的に迅速に授受することにより、行政事務の効率化が見込まれ、効率化された人員や財源を国民サービスにより振り向けることが期待できる。 4. 開示請求者等からの開示請求等への対応 　開示請求者等は、いつ誰が情報提供ネットワークシステムを使用して本人の特定個人情報を照会・提供したのか確認できる。
5. 個人番号の利用　※	
法令上の根拠	1. 番号法 ・第19条第8号・第9号（特定個人情報の提供の制限） ・第21条第2項（情報提供ネットワークシステム） ・第23条第3項（情報提供等の記録） ・第24条（秘密の管理） 2. 番号法施行令 ・第26条第1項・第2項・第4項・第5項・第6項（特定個人情報の提供の求めがあった場合の内閣総理大臣の措置） ・第27条第5項・第6項（情報提供用個人識別符号の取得）
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	[　　実施しない　　]　　＜選択肢＞ 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	
7. 評価実施機関における担当部署	
①部署	デジタル庁デジタル社会共通機能グループ
②所属長の役職名	デジタル庁統括官（デジタル社会共通機能担当）付参事官（基準・標準担当）
8. 他の評価実施機関	

（別添1）事務の内容

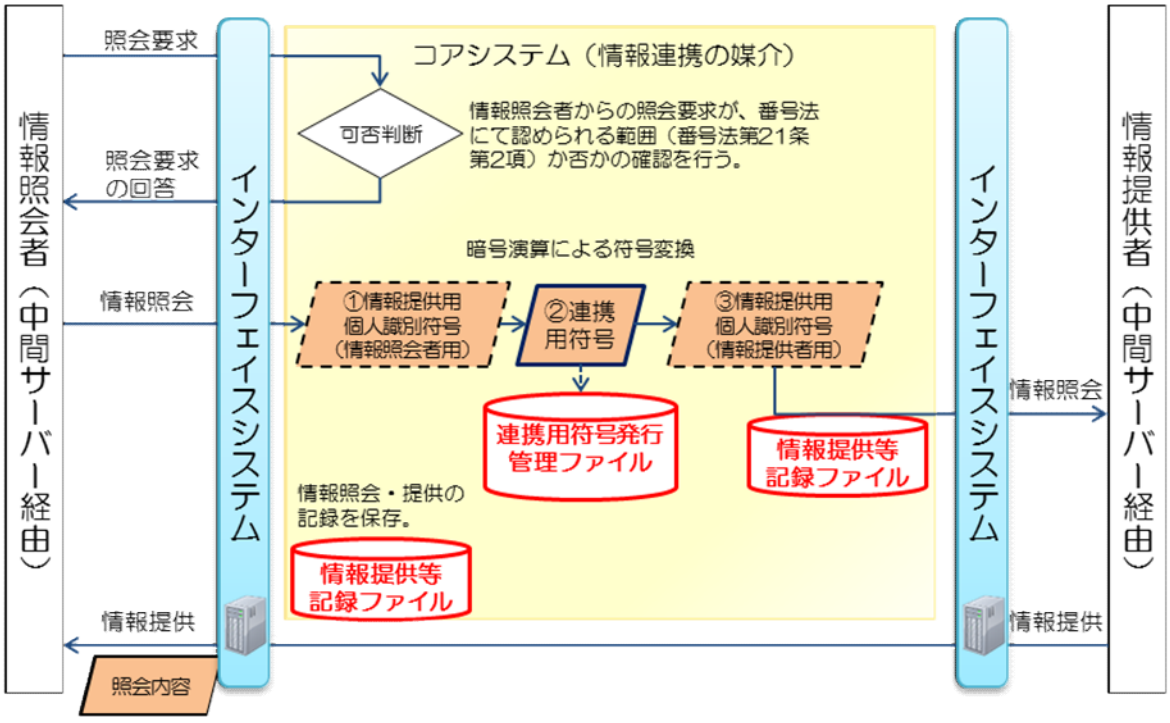


図中の（1）符号の生成、（2）情報連携の媒介、（3）情報提供等の記録の管理の詳細を、以下それぞれ示す。

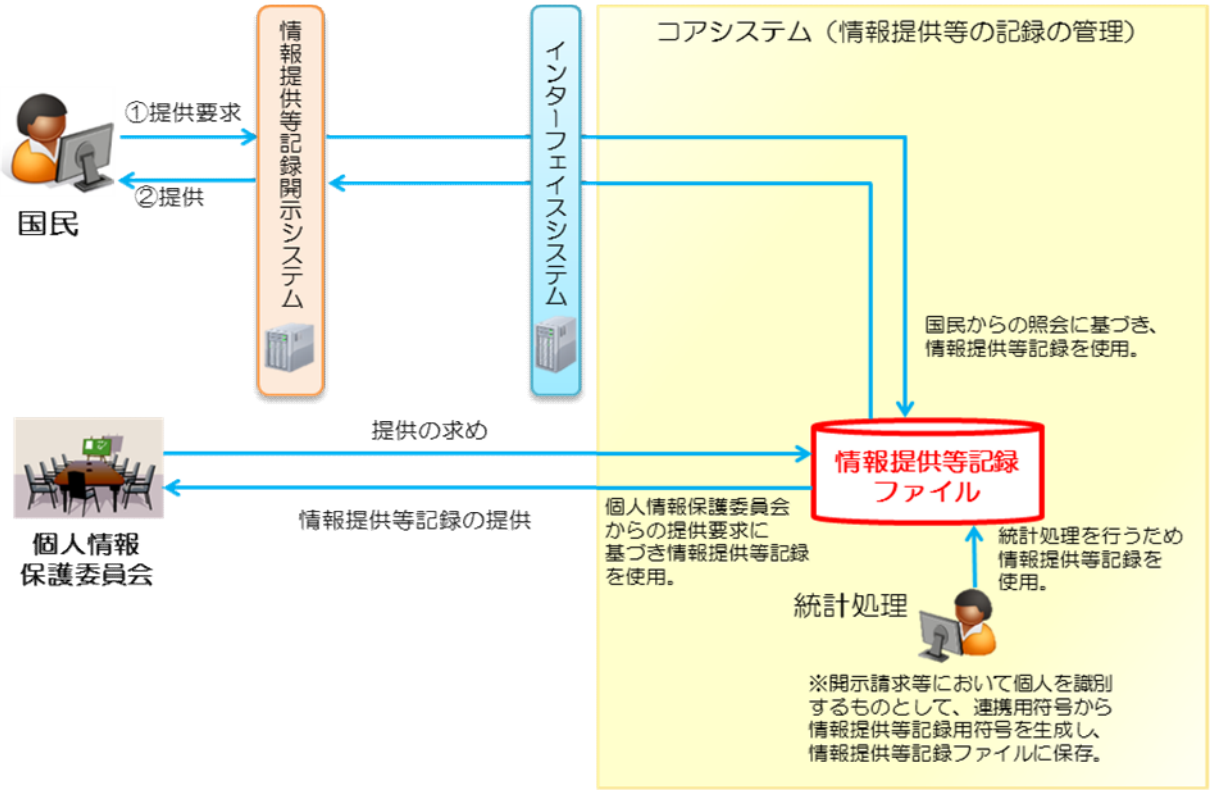
(1) 符号の生成



(2) 情報連携の媒介



(3) 情報提供等の記録の管理



（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		
1. 連携用符号発行管理ファイル		
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 ※		情報提供ネットワークシステムを使用して行われる特定個人情報の照会・提供の対象となる者
	その必要性	番号法第19条第8号及び第9号の規定により、情報提供ネットワークシステムを使用して行われる特定個人情報の照会・提供の対象となる者の全ての連携用符号や連携用符号から変換される情報提供用個人識別符号を生成する必要があるため。
④記録される項目		[　　10項目未満　　] ＜選択肢＞ 1）10項目未満　2）10項目以上50項目未満 3）50項目以上100項目未満　4）100項目以上
	主な記録項目 ※	・識別情報 [　] 個人番号　[○] 個人番号対応符号　[　] その他識別情報（内部番号） ・連絡先等情報 [　] 4情報（氏名、性別、生年月日、住所）　[　] 連絡先（電話番号等） [　] その他住民票関係情報 ・業務関係情報 [　] 国税関係情報　[　] 地方税関係情報　[　] 健康・医療関係情報 [　] 医療保険関係情報　[　] 児童福祉・子育て関係情報　[　] 障害者福祉関係情報 [　] 生活保護・社会福祉関係情報　[　] 介護・高齢者福祉関係情報 [　] 雇用・労働関係情報　[　] 年金関係情報　[　] 学校・教育関係情報 [　] 災害関係情報 [○] その他　（　連携用符号発行管理情報　）
	その妥当性	・個人番号対応符号（連携用符号） 個人番号を使用せずに、連携用符号及び情報提供用個人識別符号により、本人を特定して情報提供ネットワークシステムを運用していくために、システム管理上必要な項目として保有する。 ・その他 連携用符号生成時に、既に生成済みの連携用符号との重複生成を防止し、連携用符号を一意とする必要があるため保有する。
	全ての記録項目	別添2を参照。
⑤保有開始日		令和3年9月1日
⑥事務担当部署		デジタル庁デジタル社会共通機能グループ

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　（連携用符号の生成については、特定個人情報ファイルの入手には該当しないため、⑧使用方法の欄に記載）
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　（連携用符号の生成については、特定個人情報ファイルの入手には該当しないため、⑧使用方法の欄に記載）
③入手の時期・頻度		連携用符号の生成については、特定個人情報ファイルの入手には該当しないため、⑧使用方法の欄に記載
④入手に係る妥当性		－
⑤本人への明示		特定個人情報の使用に関しては、番号法第19条第8号、第19条第9号及び第21条第2項において、情報提供ネットワークシステムにより情報連携を行う旨が規定されている。
⑥使用目的 ※		・新たに生成する連携用符号が、生成済みの連携用符号と重複することを防止するための機能として使用（住民票コード変更の際の重複の確認を含む。）。 ・情報連携の媒介において、連携用符号から情報提供用個人識別符号を生成する際に、生成済の判定及び暗号演算に必要な情報を取得するために使用。 ・障害時や異常発生時等に暗号鍵等が危殆化し、連携用符号を再生成する必要が生じた場合に使用。 ・符号生成に関する統計処理の元データとして使用。
	変更の妥当性	
⑦使用の主体	使用部署 ※	デジタル庁デジタル社会共通機能グループ
	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 ※		・情報照会者等から符号生成の依頼を受け、情報照会者等から住民基本台帳ネットワークシステムを介して符号生成の対象者の住民票コードを受領する。住民票コードを基に、暗号演算により、対象者ごとに異なり、情報提供用個人識別符号等の生成の基となる全ての情報照会者等に共通の連携用符号を生成し、連携用符号発行管理ファイルに保存する。住民票コードは連携用符号生成後に直ちに削除する。
	情報の突合 ※	① 住民基本台帳ネットワークシステムから受領した住民票コードから生成した連携用符号が、既に生成している連携用符号と同一でないか突合する。 ② 情報照会を受けた際、照会対象者の連携用符号を基に、情報提供者へ情報提供用個人識別符号が発行済みかを確認するため、連携用符号発行管理ファイル（発行履歴）と突合する。
	情報の統計分析 ※	符号生成処理状況の把握のため、必要な統計処理を行う。
	権利利益に影響を与え得る決定 ※	ない。
⑨使用開始日		令和3年9月1日

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※		[委託する] <選択肢> 1）委託する 2）委託しない （ 4 ） 件
委託事項1		情報提供ネットワークシステムの移行に伴う第二期システムからのデータ抽出
①委託内容		情報提供ネットワークシステムの移行に伴うデータ抽出
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	[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 ※	情報提供ネットワークシステムを使用して行われる特定個人情報の照会・提供の対象となる者
	その妥当性	情報提供ネットワークシステムの移行に向けたデータの抽出を適切に実施するためには、専門的かつ高度な知識・技術を要することなど、全体の取扱いを委託することが必要であるため。
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		調達結果（委託先名）は官報公示及びホームページ公表により、国民等が確認可能。
⑥委託先名		株式会社エヌ・ティ・ティ・データ
再委託	⑦再委託の有無 ※	[再委託する] <選択肢> 1）再委託する 2）再委託しない
	⑧再委託の許諾方法	・原則として再委託は行わないこととするが、再委託を行う場合には、委託先から再委託先の商号又は名称、住所、再委託する理由、再委託する業務の範囲、再委託先に係る業務の履行能力、再委託予定金額等及びその他のデジタル庁が求める情報について記載した書面による再委託申請及び再委託に係る履行体制図の提出を受け、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を確認し、決裁等必要な手続を経た上で、再委託を承認する。
	⑨再委託事項	上記委託事項と同じ。
委託事項2～5		

委託事項2		情報提供ネットワークシステムの移行に伴う第三期システムへのデータ投入
①委託内容		情報提供ネットワークシステムの移行に伴うデータ投入業務
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	[　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　※	情報提供ネットワークシステムを使用して行われる特定個人情報の照会・提供の対象となる者
	その妥当性	情報提供ネットワークシステムの移行において、現行の情報提供ネットワークシステムから抽出したデータの投入を適切に実施するためには、専門的かつ高度な知識・技術を要することなど、全体の取扱いを委託することが必要であるため。
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		調達結果（委託先名）は官報公示及びホームページ公表により、国民等が確認可能。
⑥委託先名		株式会社エヌ・ティ・ティ・データ
再委託	⑦再委託の有無　※	[　再委託する　]　＜選択肢＞ 1）再委託する　2）再委託しない
	⑧再委託の許諾方法	・原則として再委託は行わないこととするが、再委託を行う場合には、委託先から再委託先の商号又は名称、住所、再委託する理由、再委託する業務の範囲、再委託先に係る業務の履行能力、再委託予定金額等及びその他のデジタル庁が求める情報について記載した書面による再委託申請及び再委託に係る履行体制図の提出を受け、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を確認し、決裁等必要な手続を経た上で、再委託を承認する。
	⑨再委託事項	上記委託事項と同じ。

委託事項3		情報提供ネットワークシステムの移行後の廃棄等
①委託内容		情報提供ネットワークシステムの移行後の廃棄等業務
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	[　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　※	情報提供ネットワークシステムを使用して行われる特定個人情報の照会・提供の対象となる者
	その妥当性	情報提供ネットワークシステムの移行前のデータを保存している機器の廃棄を適切に実施するためには、専門的かつ高度な知識・技術を要することなど、全体の取扱いを委託することが必要であるため。
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　（ 機器の廃棄　）
⑤委託先名の確認方法		調達結果（委託先名）は官報公示及びホームページ公表により、国民等が確認可能。
⑥委託先名		エヌ・ティ・ティ・コミュニケーションズ株式会社
再委託	⑦再委託の有無　※	[　再委託する　]　＜選択肢＞ 1）再委託する　2）再委託しない
	⑧再委託の許諾方法	・原則として再委託は行わないこととするが、再委託を行う場合には、委託先から再委託先の商号又は名称、住所、再委託する理由、再委託する業務の範囲、再委託先に係る業務の履行能力、再委託予定金額等及びその他のデジタル庁が求める情報について記載した書面による再委託申請及び再委託に係る履行体制図の提出を受け、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を確認し、決裁等必要な手続を経た上で、再委託を承認する。
	⑨再委託事項	上記委託事項と同じ。

委託事項4		第三期情報提供ネットワークシステムの運用・保守業務
①委託内容		連携用符号発行管理ファイルに関する運用・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	［ 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 ※	情報提供ネットワークシステムを使用して行われる特定個人情報の照会・提供の対象となる者
	その妥当性	システム全般に係る運用・保守等を適切に実施するためには、専門的かつ高度な知識・技術を要することなど、全体の取扱いを委託することが必要であるため。
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　（データはISMAPのリストに登録されたクラウドサービス上で管理されている。運用者が運用施設にて運用するが、特定個人情報へのアクセスは障害時など例外的である。）
⑤委託先名の確認方法		調達結果（委託先名）は官報公示及びホームページ公表により、国民等が確認可能。
⑥委託先名		株式会社エヌ・ティ・ティ・データ
再委託	⑦再委託の有無 ※	［ 再委託する ］ ＜選択肢＞ 1）再委託する　2）再委託しない
	⑧再委託の許諾方法	・原則として再委託は行わないこととするが、再委託を行う場合には、委託先から再委託先の商号又は名称、住所、再委託する理由、再委託する業務の範囲、再委託先に係る業務の履行能力、再委託予定金額等及びその他のデジタル庁が求める情報について記載した書面による再委託申請及び再委託に係る履行体制図の提出を受け、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を確認し、決裁等必要な手続を経た上で、再委託を承認する。
	⑨再委託事項	上記委託事項と同じ。
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　（　　）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	
提供先2～5	
提供先6～10	
提供先11～15	
提供先16～20	

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	
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 ※		運用者の運用端末からのアクセスはできない仕組みとなっている。 ＜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	[20年以上] ＜選択肢＞ 1）1年未満 2）1年 3）2年 4）3年 5）4年 6）5年 7）6年以上10年未満 8）10年以上20年未満 9）20年以上 10）定められていない
	その妥当性	連携用符号の重複生成を防ぐため、及び、各情報照会者等から情報提供用個人識別符号を用いた照会要求に対応するために生成済みの符号に関する情報を恒久的に保管する必要があるため、原則として消去しない。例外的に事務処理誤りを考慮して、物理削除要求電文による削除が可能である。
③消去方法		原則として消去しない。例外的に事務処理誤りを考慮して、住民基本台帳ネットワークシステムを介した物理削除要求電文による削除が可能である。 ＜ガバメントクラウドにおける措置＞ ①特定個人情報の消去はデジタル庁及び委託事業者からの操作によって実施される。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特定個人情報を消去することはない。 ②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。 ③現行システムからの移行については、2期運用保守事業者及び3期設計・開発事業者が実施する。移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。 【情報提供ネットワークシステム移行の際に実施する措置】 ・ディスクの物理破壊が終了して搬出が許可されるまで、現行システムのデータセンター内にて機器を保持する。電源をオフするまでは運用中と同様のアクセス制限を実施する。データセンターへの入館、マシンルームの入室に関する手続は継続して行う。 ・データ消去に当たっては、同値性確認を行って確実に必要なデータ移行を実施した後、データの破棄を行う。また、データの破棄は、データを復元できないよう、記憶装置に対し論理的消去処理を行った上で、当該装置の物理破壊の措置を講じるとともに、消去完了の証跡の提示により確実な履行を担保する。 ・消去操作に用いる機器については、ネットワークに接続できないものを用いて、データの流出を防止する。

7. 備考

・運用施設において本番環境にアクセスできる端末は、専用端末を固定して設置しており、アクセス端末を限定している。
・運用施設にPCを持ち込む場合には、事前での持ち込み申請を必須とし、入室時にシリアル番号を確認することにより、持ち込み機器の制限を実施している。
・不正ソフト対策として、運用施設にPCを持ち込む場合には、最新のパターンファイルにてウイルスチェックを実施したかを確認している。

（別添2）特定個人情報ファイル記録項目

コアシステム

連携用符号発行管理ファイル

連携用符号	住民票コードを基に生成する個人ごとに異なる符号 住民票コードへの不可逆性をシステムで担保
連携用符号管理情報	連携用符号生成時に、既に生成済みの連携用符号との重複生成を防止し、連携用符号を一意とするための暗号情報
連携用符号のバージョン	連携用符号のバージョン情報。暗号鍵等が危殆化し、連携用符号を再生成する必要が生じた場合を考慮し保存
機関別パラメータ	情報提供用個人識別符号を変換する際に付与する情報照会者等ごとのパラメータ
情報提供用個人識別符号生成方式等のバージョン	情報提供用個人識別符号の生成方式等のバージョン。暗号鍵等が危殆化し、連携用符号を再生成する必要が生じた場合を考慮し保存
機関コード	情報提供用個人識別符号を生成した情報照会者等のコード
発行日時	情報提供用個人識別符号の発行日時

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. 情報提供等記録ファイル		
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 ※		情報提供ネットワークシステムを使用して行われる特定個人情報の照会・提供の対象となる者
	その必要性	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の照会・提供があったときは、当該照会・提供に係る事項を情報提供ネットワークシステムに記録・保存しなければならないものとされている（番号法第23条）。これにより、情報提供ネットワークシステムを使用して行われた特定個人情報の照会・提供のやり取りを対象者ごとに、情報提供等記録ファイルに記録・保存する必要がある。
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 [　] 4情報（氏名、性別、生年月日、住所）　[　] 連絡先（電話番号等） [　] その他住民票関係情報 ・業務関係情報 [　] 国税関係情報　[　] 地方税関係情報　[　] 健康・医療関係情報 [　] 医療保険関係情報　[　] 児童福祉・子育て関係情報　[　] 障害者福祉関係情報 [　] 生活保護・社会福祉関係情報　[　] 介護・高齢者福祉関係情報 [　] 雇用・労働関係情報　[　] 年金関係情報　[　] 学校・教育関係情報 [　] 災害関係情報 [○] その他　（　特定個人情報名等の照会・提供の記録に関する事項　）
	その妥当性	・個人番号対応符号（情報提供等記録用符号） 情報提供等記録ファイルは、本人等からの開示請求による閲覧、個人情報保護委員会への資料提供等に使用されるが、その場合の対象者を一意に特定する識別情報として情報提供等記録用符号を生成し、記録している。 ・その他 番号法第23条に規定されている項目及びシステム管理のために必要な項目を選定して記録している。
	全ての記録項目	別添2を参照。
⑤保有開始日		令和3年9月1日
⑥事務担当部署		デジタル庁デジタル社会共通機能グループ

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　（情報提供等記録用符号の生成については、特定個人情報ファイルの入手には該当しないため、⑧使用方法の欄に記載）
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　（情報提供等記録用符号の生成については、特定個人情報ファイルの入手には該当しないため、⑧使用方法の欄に記載）
③入手の時期・頻度		情報提供等記録用符号の生成については、特定個人情報ファイルの入手には該当しないため、⑧使用方法の欄に記載
④入手に係る妥当性		－
⑤本人への明示		特定個人情報の使用に関する法令の規定として、番号法第23条第3項において、特定個人情報の提供の求め又は提供があったときは情報提供ネットワークシステムに記録を保存する旨が規定されている。
⑥使用目的 ※		・開示請求者等からの開示請求等に対して、対象となる情報提供等の記録を開示し、いつ誰がどのような本人の特定個人情報を情報提供ネットワークシステムを使用して照会・提供したのか開示することを可能にする。 ・情報提供等の記録を情報提供ネットワークシステムに記録・保存することにより、不正な情報連携の有無を確認することを可能とする。 ・情報提供ネットワークシステムを円滑かつ安定的に運用していくため、情報連携の処理件数等を集計し、統計資料として使用する。
	変更の妥当性	
⑦使用の主体	使用部署 ※	デジタル庁デジタル社会共通機能グループ
	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 ※		・番号法第23条の規定に基づき、情報連携における情報照会・提供に係る一連の過程に関する情報を自動的に記録し、情報提供等記録ファイルに保存する。その際、特定の個人を識別するものとして個人番号（マイナンバー）は利用せずに、連携用符号から情報提供等記録用符号を生成し、情報提供等記録ファイルに保存する。 ・情報提供ネットワークシステムを使用して行われる特定個人情報の照会・提供について、個人情報の保護に関する法律（平成15年法律第57号。以下「個人情報保護法」という。）第76条の規定に基づき、開示請求できることとなっており、本人等からの開示請求に基づき情報提供等記録ファイルを使用して、開示することとなっている。 ・情報提供等記録開示システムを介して本人から提供要求を受信した際に、該当する情報提供等の記録を抽出し、インターフェイスシステムを介して情報提供等記録開示システムへ送信する。 ・番号法第35条第1項の規定により、個人情報保護委員会から報告を求められた場合には、番号法第19条第13号の規定により、特定個人情報を提供することとされており、この規定に基づき、個人情報保護委員会から情報提供等の記録の提供の求めがあった場合には、情報提供等の記録を提供する。 ・情報提供ネットワークシステムにおける運用実績の把握、情報提供ネットワークシステムの利用範囲の拡大の検討、及び行政機関等の正確な業務量の把握等のため、必要な集計・統計処理を行う。
	情報の突合 ※	突合は行わない。
	情報の統計分析 ※	・情報提供ネットワークシステムにおける運用実績の把握、情報提供ネットワークシステムの利用範囲の拡大の検討、及び行政機関等の正確な業務量の把握等のため、必要な集計・統計処理を行う。
	権利利益に影響を与え得る決定 ※	個人情報保護法第82条の規定により、情報提供等の記録の開示又は不開示の決定を行う。
⑨使用開始日		令和3年9月1日

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※		[委託する] <選択肢> 1）委託する 2）委託しない （ 4 ） 件
委託事項1		情報提供ネットワークシステムの移行に伴う第二期システムからのデータ抽出
①委託内容		情報提供ネットワークシステムの移行に伴うデータ抽出
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	[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 ※	情報提供ネットワークシステムを使用して行われた特定個人情報の照会・提供の対象となる者
	その妥当性	情報提供ネットワークシステムの移行に向けたデータの抽出を適切に実施するためには、専門的かつ高度な知識・技術を要することなど、全体の取扱いを委託することが必要であるため。
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		調達結果（委託先名）は官報公示及びホームページ公表により、国民等が確認可能。
⑥委託先名		株式会社エヌ・ティ・ティ・データ
再委託	⑦再委託の有無 ※	[再委託する] <選択肢> 1）再委託する 2）再委託しない
	⑧再委託の許諾方法	・原則として再委託は行わないこととするが、再委託を行う場合には、委託先から再委託先の商号又は名称、住所、再委託する理由、再委託する業務の範囲、再委託先に係る業務の履行能力、再委託予定金額等及びその他のデジタル庁が求める情報について記載した書面による再委託申請及び再委託に係る履行体制図の提出を受け、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を確認し、決裁等必要な手続を経た上で、再委託を承認する。
	⑨再委託事項	上記委託事項と同じ。
委託事項2～5		

委託事項2		情報提供ネットワークシステムの移行に伴う第三期システムへのデータ投入
①委託内容		情報提供ネットワークシステムの移行に伴うデータ投入業務
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	[　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　※	情報提供ネットワークシステムを使用して行われる特定個人情報の照会・提供の対象となる者
	その妥当性	情報提供ネットワークシステムの移行において、現行の情報提供ネットワークシステムから抽出したデータの投入を適切に実施するためには、専門的かつ高度な知識・技術を要することなど、全体の取扱いを委託することが必要であるため。
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		調達結果（委託先名）は官報公示及びホームページ公表により、国民等が確認可能。
⑥委託先名		株式会社エヌ・ティ・ティ・データ
再委託	⑦再委託の有無　※	[　再委託する　]　＜選択肢＞ 1）再委託する　2）再委託しない
	⑧再委託の許諾方法	・原則として再委託は行わないこととするが、再委託を行う場合には、委託先から再委託先の商号又は名称、住所、再委託する理由、再委託する業務の範囲、再委託先に係る業務の履行能力、再委託予定金額等及びその他のデジタル庁が求める情報について記載した書面による再委託申請及び再委託に係る履行体制図の提出を受け、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を確認し、決裁等必要な手続を経た上で、再委託を承認する。
	⑨再委託事項	上記委託事項と同じ。

委託事項3		情報提供ネットワークシステムの移行後の廃棄等
①委託内容		情報提供ネットワークシステムの移行後の廃棄等業務
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	[　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　※	情報提供ネットワークシステムを使用して行われる特定個人情報の照会・提供の対象となる者
	その妥当性	情報提供ネットワークシステムの移行前のデータを保存している機器の廃棄を適切に実施するためには、専門的かつ高度な知識・技術を要することなど、全体の取扱いを委託することが必要であるため。
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　（ 機器の廃棄　）
⑤委託先名の確認方法		調達結果（委託先名）は官報公示及びホームページ公表により、国民等が確認可能。
⑥委託先名		エヌ・ティ・ティ・コミュニケーションズ株式会社
再委託	⑦再委託の有無　※	[　再委託する　]　＜選択肢＞ 1）再委託する　2）再委託しない
	⑧再委託の許諾方法	・原則として再委託は行わないこととするが、再委託を行う場合には、委託先から再委託先の商号又は名称、住所、再委託する理由、再委託する業務の範囲、再委託先に係る業務の履行能力、再委託予定金額等及びその他のデジタル庁が求める情報について記載した書面による再委託申請及び再委託に係る履行体制図の提出を受け、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を確認し、決裁等必要な手続を経た上で、再委託を承認する。
	⑨再委託事項	上記委託事項と同じ。

委託事項4		第三期情報提供ネットワークシステムの運用・保守業務
①委託内容		情報提供等の記録に関する運用・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、統計処理の業務）
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	［ 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 ※	情報提供ネットワークシステムを使用して行われる特定個人情報の照会・提供の対象となる者
	その妥当性	システム全般に係る運用・保守等を適切に実施するためには、専門的かつ高度な知識・技術を要することなど、全体の取扱いを委託することが必要であるため。
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　（ データはISMAPのリストに登録されたクラウドサービス上で管理されている。運用者が運用施設にて運用するが、特定個人情報へのアクセスは障害時など例外的である。 ）
⑤委託先名の確認方法		調達結果（委託先名）は官報公示及びホームページ公表により、国民等が確認可能。
⑥委託先名		株式会社エヌ・ティ・ティ・データ
再委託	⑦再委託の有無 ※	［ 再委託する ］ ＜選択肢＞ 1）再委託する　2）再委託しない
	⑧再委託の許諾方法	・原則として再委託は行わないこととするが、再委託を行う場合には、委託先から再委託先の商号又は名称、住所、再委託する理由、再委託する業務の範囲、再委託先に係る業務の履行能力、再委託予定金額等及びその他のデジタル庁が求める情報について記載した書面による再委託申請及び再委託に係る履行体制図の提出を受け、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を確認し、決裁等必要な手続を経た上で、再委託を承認する。
	⑨再委託事項	上記委託事項と同じ。
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 （ 2 ）件 [ ] 移転を行っている （ ）件 [ ] 行っていない
提供先1	開示請求を行った者（書面にて開示請求を受け付ける。） 又は情報提供等記録開示システムにより提供要求を行った者（情報提供等記録開示システムを介して提供要求を受け付ける。）
①法令上の根拠	＜開示請求を行った者＞ 個人情報保護法第76条 ＜情報提供等記録開示システムにより提供要求を行った者＞ 番号法附則第6条第3項
②提供先における用途	情報提供等の記録を閲覧し、自身の特定個人情報の取扱いが適切であることを確認する。
③提供する情報	・情報照会者の名称 ・情報提供者の名称 ・提供の求めの日時 ・提供の日時 ・特定個人情報の項目 ・提供の求め又は提供の事実が不開示情報に該当する場合はその旨 ・番号法第23条第1項第4号のデジタル庁令で定める事項
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	情報提供等の記録に係る本人のうち、開示請求又は提供要求を行う者
⑥提供方法	[ ] 情報提供ネットワークシステム [ ] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [○] 紙 [○] その他 （ 情報提供ネットワークシステムと接続された情報提供等記録開示システム ）
⑦時期・頻度	開示請求又は提供要求を受け付けた都度
提供先2～5	
提供先2	個人情報保護委員会
①法令上の根拠	番号法第19条第13号
②提供先における用途	番号法第35条第1項の規定に基づき、情報提供等の記録等を基に調査を行い、特定個人情報の取扱いに関する監視又は監督を行う。
③提供する情報	情報提供等記録ファイルのうち、個人情報保護委員会が求める情報
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	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・提供の対象となった者
⑥提供方法	[ ] 情報提供ネットワークシステム [ ] 専用線 [ ] 電子メール [○] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [○] 紙 [ ] その他 （ ）
⑦時期・頻度	提供を求められた都度

提供先6～10	
提供先11～15	
提供先16～20	
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	
移転先2～5	
移転先6～10	
移転先11～15	
移転先16～20	

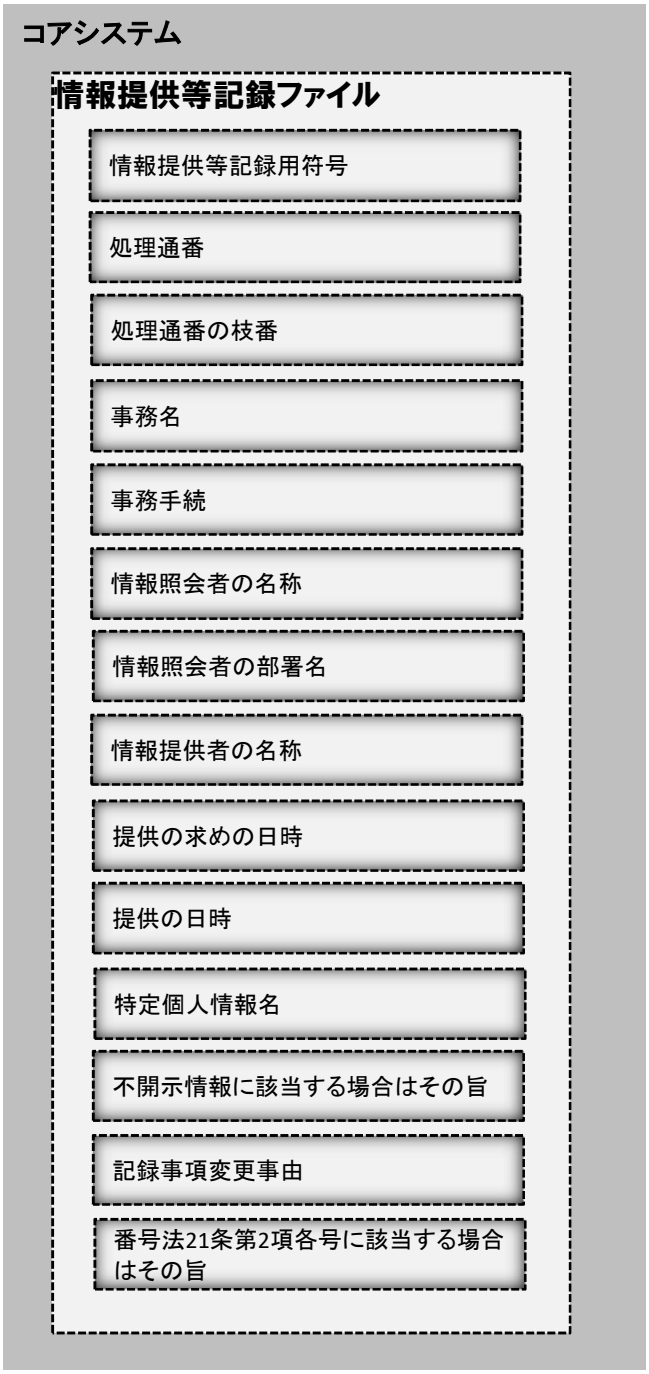
6. 特定個人情報の保管・消去

①保管場所 ※		運用者の運用端末から画面操作によるファイルアクセスは可能であるが、情報提供等記録用符号を参照できないようにしており、特定個人情報としてのアクセスはできない仕組みとなっている。 ＜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	[　6年以上10年未満　] ＜選択肢＞ 1）1年未満　2）1年　3）2年 4）3年　5）4年　6）5年 7）6年以上10年未満　8）10年以上20年未満　9）20年以上 10）定められていない
	その妥当性	過去に行われた情報連携の確認を行う必要性を踏まえ、刑法第235条（窃盗）及び同第246条の2（電子計算機使用詐欺）の公訴時効が刑事訴訟法第250条で7年となってることに鑑み、番号法第23条第3項に基づく施行令第29条にて、7年間保存する旨が規定されている。
③消去方法		保管期間経過後は、適切に廃棄等を行う。 ＜ガバメントクラウドにおける措置＞ ①特定個人情報の消去はデジタル庁及び委託事業者からの操作によって実施される。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特定個人情報を消去することはない。 ②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。 ③現行システムからの移行については、2期運用保守事業者及び3期設計・開発事業者が実施する。移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。 【情報提供ネットワークシステム移行の際に実施する措置】 ・ディスクの物理破壊が終了して搬出が許可されるまで、現行システムのデータセンター内にて機器を保持する。電源をオフするまでは運用中と同様のアクセス制限を実施する。データセンターへの入館、マシンルームの入室に関する手続は継続して行う。 ・データ消去に当たっては、同値性確認を行って確実に必要なデータ移行を実施した後、データの破棄を行う。また、データの破棄は、データを復元できないよう、記憶装置に対し論理的消去処理を行った上で、当該装置の物理破壊の措置を講じるとともに、消去完了の証跡の提示により確実な履行を担保する。 ・消去操作に用いる機器については、ネットワークに接続できないものを用いて、データの流出を防止する。

7. 備考

・運用施設において本番環境にアクセスできる端末は、専用端末を固定して設置しており、アクセス端末を限定している。
・運用施設にPCを持ち込む場合には、事前での持ち込み申請を必須とし、入室時にシリアル番号を確認することにより、持ち込み機器の制限を実施している。
・不正ソフト対策として、運用施設にPCを持ち込む場合には、最新のパターンファイルにてウイルスチェックを実施したかを確認している。

（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 ※（7. リスク1⑨を除く。）

1. 特定個人情報ファイル名	
1. 連携用符号発行管理ファイル	
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	（留意事項） 連携用符号は、情報提供ネットワークシステム内で住民票コードから生成されるため、「特定個人情報の入手」には該当しないが、特定個人情報である連携用符号の生成におけるリスク対策について、「3. 特定個人情報の使用　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」の欄に記載することとする。
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	
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	
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	
個人番号の真正性確認の措置の内容	
特定個人情報の正確性確保の措置の内容	
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
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	[　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、事務に必要のない情報との紐付けが行われるリスク	
宛名システム等における措置の内容	情報提供ネットワークシステムでは、地方公共団体の宛名システムに相当する個人番号（符号含む。）と他の個人情報とを紐付けるよう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	情報提供ネットワークシステムの運営に関する事務においては、情報提供ネットワークシステムが存在するのみで、その他のシステムは存在しない。なお、連携用符号はシステム内で暗号化されて管理されており、また、連携用符号から情報提供用個人識別符号への変換はシステム上で自動的に暗号演算により実施されるため、特定個人情報が使用目的を超えて取り扱われることや事務に必要のない情報と併せて取り扱われることはあり得ない。
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	情報提供ネットワークシステムとしては、以下のユーザ認証の管理を行っている。 ・情報資産の重要度に応じて、ID・パスワード認証、生体認証、多要素認証など適切な認証方式を選択するよう設計を行う。また、デュアルロック機能等も活用する。 ・文字種の混在やパスワードの長さ等に関するポリシーを策定し、ポリシーに合致しないパスワードの設定を防止する。 ・システムへのログイン画面に前回のログイン日時を表示し、不正ログインの有無を確認できるようにする。 ・OSやデータベースで初期設定されているIDのパスワードは、システム管理者が初期設定時に変更又は無効化する。 ・定めた運用手順に基づき、定期的にパスワード変更を実施する。 ・OSや管理ソフトにより運用端末へのアプリケーションのインストールを制限する。 ・システムにアクセスできる端末を制限する。
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	情報提供ネットワークシステムとしては、以下のアクセス権限発行・失効の管理を行っている。 ・システム運用者の役割に従って権限を設定し、ユーザと権限の対応表を作成する。 ・運用者の異動等に伴い、必要な権限を確認し、迅速に発効・失効を実施する。 ・定期的に対応表を見直し、アクセス権限の発行・失効管理が正しく実施されていることの確認を行う。 ・定期的に全てのユーザと権限の棚卸しを実施している。
アクセス権限の管理	［　行っている　］　＜選択肢＞ 1）行っている　2）行っていない
具体的な管理方法	情報提供ネットワークシステムとしては、以下のアクセス権限の管理を行っている。 ・IDやアクセス権限の発行・失効処理の権限を持つ者を制限し、発行・失効を行った際はその旨の記録を残す。 ・運用者によるID・パスワードの共有利用は行わない。 ・定期的に対応表を見直し、アクセス権限が正しく付与されているか確認を行う。
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	連携用符号は、人が識別できない形態（規則性を備えていない数字・文字列の羅列）で生成・保存し、運用端末から運用者がアクセスできないよう制御を行っている。連携用符号発行管理ファイルには生成済みの符号に関する情報を恒久的に保管することとしており、連携用符号発行管理ファイル自体が使用の記録であるとともに、アクセスに関するログの記録を行う。
その他の措置の内容	・無線LAN経由でのアクセスを許可しない。 ・システムにログインするパスワードは、システム上不可逆な形式で暗号化され保管される。
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： 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	・年次で当該全ての業務従事者に対し、個人情報保護及び情報セキュリティに関する教育・啓蒙活動を行う。 ・システムの監査権限を持った者が、操作ログ等で操作者別のシステム利用状況の記録を残し、定期的に異常作業等の監視を行う。
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
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	・運用者が使用する端末は、許可されてないUSB等の媒体接続を禁止する。 ・許可されていない外部媒体への書き出しをシステム的に禁止する。 ・運用着手に当たり、システム運用者に対しバックアップ権限を付与し、システム運用者のみバックアップを実施できるようにする。 【情報提供ネットワークシステム移行について】 特定個人情報のデータ移行は、ガバメントクラウド環境と第二期拠点間を移行用回線(閉域網)で接続を行い、第三者はアクセスできない。 【情報提供ネットワークシステム移行の際に特に想定されるリスクに対する措置】 ①移行用回線上を暗号化することで第三者による盗聴や改ざんができない仕組みとする。データベース接続時のパスワードは職員のみが把握し、事業者には開示されない。 ②移行用一時ファイルとそのフォルダへのアクセスを制限する。移行に関与する運用者以外からのアクセスは不可として設定する。 ③データ移行時において、作業者等によるデータの詐取や外部へのデータ漏えいの予防のために、第二期システムにおいてはログ情報等の統合分析・監査を行うシステム（SIEM）、第三期システムにおいてはガバメントクラウド環境のデータ分析・可視化サービス（SIEM）を用いて、各種ログによる監査及びファイル、フォルダ、NWのアクセス状況の監視（モニタリング）・分析を行い、移行元・移行先双方での不正の兆候や不正アクセスの検知を行う。
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	
＜連携用符号の生成について＞ ・連携用符号は、情報照会者等からの依頼に基づき、住民基本台帳ネットワークシステムを介して受領する住民票コードを基に、システム内にて暗号演算により生成・保存する。住民票コードは、住民基本台帳ネットワークシステムを通じ、情報照会者等から符号生成の対象者に関するもののみを受領する仕組みとしている。対象者の住民票コードの受領は、地方公共団体情報システム機構から暗号化された状態で専用線にて受領しており目的外の生成が行われることはない。 ・情報提供ネットワークシステムにおいて、住民票コードを受領してから連携用符号を生成するまでの処理及び情報提供用個人識別符号への暗号演算による変換は、一連のシステム処理により自動的に行うため不適切な方法で生成されることはない。 ・連携用符号の生成は、暗号化技術を用いて実施される。その際に用いる鍵は、物理的・論理的に内部情報を読み取られることに対する耐性の高い機能を備え、鍵の生成・管理における高い安全性を確保するものとしてガバメントクラウドが提供する鍵管理サービスを用いて厳密な管理を行い、鍵の不正利用等を防止する。 ・連携用符号の生成の際は、連携用符号発行管理ファイルと突合し、既に生成済みの連携用符号と重複がないか等の確認を行い正確性を確保する。	

4. 特定個人情報ファイルの取扱いの委託		[　　]委託しない
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク		
情報保護管理体制の確認		・会計法令等に基づく総合評価落札方式により委託者を選定する。 ・委託者の選定を行う際は、プライバシーマークやISMS(ISO/IEC 27001)等の認証取得事業者であること等、特定個人情報の保護を適切に行えることを確認する。
特定個人情報ファイルの閲覧者・更新者の制限		[　制限している　] ＜選択肢＞ 1）制限している　2）制限していない
	具体的な制限方法	通常業務では、受託者が運用端末から連携用符号にアクセスすることを禁止している。
特定個人情報ファイルの取扱いの記録		[　記録を残している　] ＜選択肢＞ 1）記録を残している　2）記録を残していない
	具体的な方法	連携用符号発行管理ファイルに関する運用業務（バックアップ取得、障害時・異常発生時の確認及び復旧業務）の委託については手順書・指示書等によって作業内容を明確にし、作業を行う都度、事績の報告を求める。また、職員が必要に応じて報告された内容を確認する。さらに、システムにおいてもアクセスログや操作ログを全て記録する。
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	連携用符号は、情報提供ネットワークシステムの内部管理のためにのみ利用し、その他の目的に利用したり、情報提供ネットワークシステムから外部に出すことはないため、委託先から他者への提供は行わない。
	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	・連携用符号は、情報提供ネットワークシステムの内部管理のためにのみ利用し、その他の目的に利用したり、情報提供ネットワークシステムから外部に出すことはないため、委託先へ特定個人情報の提供は行わない。 ・再委託も含めて、番号法第１１条の趣旨を踏まえ、必要かつ適切な監督を行う。
特定個人情報の消去ルール		[　定めていない　] ＜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	・情報提供ネットワークシステムの運用は委託先の者により行われるが、連携用符号の重複生成を防ぐ等、情報提供ネットワークシステムの内部管理に利用するため、特定個人情報は消去しないこととしている。 ・委託契約終了後の特定個人情報の消去については、ISMS（情報セキュリティマネジメントシステム）に準拠した廃棄プロセスを確保する。デジタル庁の情報システム責任者等は委託先事業者から提出される報告書の内容を確認するとともに、報告書に基づいてシステム管理者に聴取を行い、必要に応じて立入検査を実施することで、委託契約終了後の消去が適切に行われていることを確認する。
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	・秘密保持義務 ・事業所内からの特定個人情報の持出しの禁止 ・特定個人情報の目的外利用の禁止 ・再委託における条件 ・漏えい事案等が発生した場合の委託先の責任 ・委託契約終了後の特定個人情報の返却又は廃棄 ・従業者に対する監督・教育 ・契約内容の遵守状況について報告を求める規定 等 特定個人情報の取扱いに関する以下の管理を強化する。 ・契約に基づき委託先に報告を求める。 ・委託先に対して実地の監査、調査等を行う。 ・委託契約で盛り込んだ内容の実施の程度を把握した上で、委託の内容等の見直しを検討することを含め、適切に評価する。

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		[　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　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、再委託契約に次の事項を盛り込むこととする。 ・秘密保持義務 ・事業所内からの特定個人情報の持出しの禁止 ・特定個人情報の目的外利用の禁止 ・漏えい事案等が発生した場合の再委託先の責任の明確化 ・再委託契約終了後の特定個人情報の返却又は廃棄 ・従業者に対する監督・教育 ・契約内容の遵守状況について報告を求める規定 等 また、再委託先がデジタル庁と同等の安全管理措置を講じていることを確認する。 特定個人情報の取扱いに関する以下の管理を強化する。 ・契約に基づき再委託先に報告を求める。 ・再委託先に対して実地の監査、調査等を行う。 ・再委託契約で盛り込んだ内容の実施の程度を把握した上で、再委託の内容等の見直しを検討することを含め、適切に評価する。
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
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　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		
リスクへの対策は十分か		[　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3： 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク		
リスクに対する措置の内容		
リスクへの対策は十分か		[　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置		

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

7. 特定個人情報の保管・消去		
リスク1： 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[特に力を入れて遵守している]	＜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	[特に力を入れて整備している]	＜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	[特に力を入れて整備している]	＜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	[特に力を入れて周知している]	＜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	[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	・運用端末が置かれた部屋では、個人ごとのICカードと生体認証を併用した入退室管理を実施する。 ・運用端末が置かれた部屋に監視カメラを設置し、端末や媒体の持ち出し・持ち込みの監視を行う。 ＜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。 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	・ガバメントクラウド上で、情報提供ネットワークシステムをプライベートな空間として確保し、インターネットと論理的に分離している。 ・運用施設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。 ・FW（ファイアウォール）等を導入し、必要な通信のみ制御する。 ・ガバメントクラウドが提供するデータ分析・可視化サービス(SIEM)を利用して侵入検知を行う。 ・端末にウィルス対策ソフトを導入し、ウィルスパターンファイルを適宜更新する。 ・OSやデータベースに関するセキュリティ情報の情報収集を行い、セキュリティパッチを適宜適用する。 ＜ガバメントクラウドにおけるその他の措置＞ 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。 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システムが管理する特定個人情報を含むデータは、クラウド事業者がアクセスできないようシステムにおいて制御を講じる。	
⑦バックアップ	[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
⑧事故発生時手順の策定・周知	[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
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	[発生あり]	＜選択肢＞ 1）発生あり 2）発生なし
その内容	令和5年5月23日に誤登録事案（他人の口座情報等の漏えいのおそれ）が判明した旨公表。 その後の総点検や、新たな検出手法を通じて、令和4年3月28日から令和5年6月23日にかけて、自治体支援窓口においてマイナポータル経由で公金受取口座を登録する際、ログアウトを忘れたため他人のマイナンバーと預貯金口座情報を誤って紐付けてしまうことで誤登録された可能性が高い事例が、計1,186件あることが判明した。	
再発防止策の内容	・ログアウトの徹底をはじめ、公金受取口座の登録支援に係るマニュアル遵守の徹底などについて、自治体向けに通知 ・口座登録開始時だけではなく、口座登録完了時にもマイナンバーカードを改めて読み込むことで、ログアウト忘れ防止のためのシステム改修を実施（令和5年6月23日） ・登録申請時に重複確認を行い、口座の重複登録を防止するシステムを整備・導入（令和6年1月16日）	

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	システムでは生存者か死者かを区別することなく安全管理を実施する。	
その他の措置の内容	ー	
リスクへの対策は十分か	[　　特に力を入れている　　]	＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
リスク2：　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	連携用符号の重複生成を防ぐため、及び、各情報照会者等から情報提供用個人識別符号を用いた情報照会要求に対応するために、生成済みの連携用符号に関する情報を恒久的に保管している。	
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
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	連携用符号の重複生成を防ぐため、及び、各情報照会者等から情報提供用個人識別符号を用いた情報照会要求に対応するために、生成済みの符号に関する情報の保管が恒久的に必要であり、原則として情報は削除しない。例外的に事務処理誤りを考慮して、物理削除要求電文による削除が可能である。 ＜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	ー	
リスクへの対策は十分か	[　　特に力を入れている　　]	＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
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		
・運用施設において本番環境にアクセスできる端末は、専用端末を固定して設置しており、アクセス端末を限定している。 ・運用施設にPCを持ち込む場合には、事前での持ち込み申請を必須とし、入室時にシリアル番号を確認することにより、持ち込み機器の制限を実施している。 ・不正ソフト対策として、運用施設にPCを持ち込む場合には、最新のパターンファイルにてウイルスチェックを実施したかを確認している。		

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. 情報提供等記録ファイル	
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	（留意事項） 情報提供等記録用符号は、情報提供ネットワークシステム内で連携用符号から生成されるため、「特定個人情報の入手」には該当しないが、特定個人情報である情報提供等の記録の生成におけるリスク対策について、「3. 特定個人情報の使用　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」の欄に記載することとする。
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	
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	
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	
個人番号の真正性確認の措置の内容	
特定個人情報の正確性確保の措置の内容	
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
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	[　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、事務に必要のない情報との紐付けが行われるリスク		
宛名システム等における措置の内容	情報提供ネットワークシステムでは、地方公共団体の宛名システムに相当する個人番号（符号含む。）と他の個人情報とを紐付けるよう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	情報提供ネットワークシステムの運営に関する事務においては、情報提供ネットワークシステムが存在するのみで、その他のシステムは存在しない。なお、情報提供等記録用符号はシステム内で暗号化されて管理されており、また、連携用符号から情報提供等記録用符号への変換はシステム上で自動的に暗号演算により実施されるため、特定個人情報が使用目的を超えて取り扱われることや事務に必要のない情報と併せて取り扱われることはあり得ない。	
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	情報提供ネットワークシステムとしては、以下のユーザ認証の管理を行っている。 ・情報資産の重要度に応じて、ID・パスワード認証、生体認証、多要素認証など適切な認証方式を選択するよう設計を行う。また、デュアルロック機能等も活用する。 ・文字種の混在やパスワードの長さ等に関するポリシーを策定し、ポリシーに合致しないパスワードの設定を防止する。 ・システムへのログイン画面に前回のログイン日時を表示し、不正ログインの有無を確認できるようにする。 ・OSやデータベースで初期設定されているIDのパスワードは、システム管理者が初期設定時に変更又は無効化する。 ・定めた運用手順に基づき、定期的にパスワード変更を実施する。 ・OSや管理ソフトにより運用端末へのアプリケーションのインストールを制限する。 ・システムにアクセスできる端末を制限する。	
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	情報提供ネットワークシステムとしては、以下のアクセス権限発行・失効の管理を行っている。 ・システム運用者の役割に従って権限を設定し、ユーザと権限の対応表を作成する。 ・運用者の異動等に伴い、必要な権限を確認し、迅速に発効・失効を実施する。 ・定期的に対応表を見直し、アクセス権限の発行・失効管理が正しく実施されていることの確認を行う。 ・定期的に全てのユーザと権限の棚卸しを実施している。	
アクセス権限の管理	[行っている]	＜選択肢＞ 1）行っている 2）行っていない
具体的な管理方法	情報提供ネットワークシステムとしては、以下のアクセス権限の管理を行っている。 ・IDやアクセス権限の発行・失効処理の権限を持つ者を制限し、発行・失効を行った際はその旨の記録を残す。 ・運用者によるID・パスワードの共有利用は行わない。 ・定期的に対応表を見直し、アクセス権限が正しく付与されているか確認を行う。	
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	・システムへのアクセスログ、システムでの操作ログの記録を行い、操作者個人を特定できるようにする。 ・ログは電子署名の付与等を行い、改ざんが検出できるようにする。 ・定期的に操作ログをチェックし、不正とみられる操作があった場合、操作内容を確認する。	
その他の措置の内容	・無線LAN経由でのアクセスを許可しない。 ・システムにログインするパスワードは、システム上不可逆な形式で暗号化され保管される。	
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： 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	・情報提供等記録用符号は暗号化され保存されている。 ・年次で当該全ての業務従事者に対し、個人情報保護及び情報セキュリティに関する教育・啓蒙活動を行う。 ・操作ログ等で操作者別のシステム利用状況の記録を残し、システムの監査権限を持った者が、定期的に異常作業等の監視を行う。
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
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	・運用者が使用する端末は、許可されていないUSB等の媒体接続を禁止する。 ・許可されていない外部媒体への書き出しをシステム的に禁止する。 ・個人情報保護委員会へ電子記録媒体形式で開示する場合は、媒体接続する端末を必要最小限にする。 ・運用着手に当たり、システム運用者に対しバックアップ権限を付与し、システム運用者のみバックアップを実施できるようにする。 ・データ抽出等はログを残し、定期的にチェックする。 【情報提供ネットワークシステム移行について】 特定個人情報のデータ移行はガバメントクラウド環境と第二期拠点間を移行用回線(閉域網)で接続を行い、第三者はアクセスできない。 【情報提供ネットワークシステム移行の際に特に想定されるリスクに対する措置】 ①移行用一時ファイルを暗号化することで、ファイルが漏えいしてもそのまま利用できない仕組みとする。暗号化パスワードは職員のみが把握し、事業者には開示されない。 ②移行用一時ファイルとそのフォルダへのアクセスを制限する。移行に関与する運用者以外からのアクセスは不可として設定する。 ③データ移行時において、作業者等によるデータの詐取や外部へのデータ漏えいの予防のために、第二期システムにおいてはログ情報等の統合分析・監査を行うシステム（SIEM）、第三期システムにおいてはガバメントクラウド環境のデータ分析・可視化サービス（SIEM）を用いて、各種ログによる監査及びファイル、フォルダ、NWのアクセス状況の監視（モニタリング）・分析を行い、移行元・移行先双方での不正の兆候や不正アクセスの検知を行う。
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	
＜情報提供等記録用符号の生成について＞ ・情報提供等記録用符号は、外部から入手されるものではなく、情報提供ネットワークシステムを使用して情報照会・提供が行われる都度、当該システム内で自動的に生成されるものであり、目的外の生成が行われることはない。 ・情報提供等記録用符号の生成は、一連のシステム処理により自動的に行うため不適切な方法で生成されることはない。 ・情報提供等記録用符号の生成は、暗号化技術を用いて実施される。その際に用いる鍵は、物理的・論理的に内部情報を読み取られることに対する耐性の高い機能を備え、鍵の生成・管理における高い安全性を確保するものとしてガバメントクラウドが提供する鍵管理サービスを用いて厳密な管理を行い、鍵の不正利用等を防止する。 ・情報提供等記録用符号の生成の際は、連携用符号発行管理ファイルにおいて重複が無いことを確認することで、正確性を確保する。	

4. 特定個人情報ファイルの取扱いの委託		[　　] 委託しない
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク		
情報保護管理体制の確認		・会計法令等に基づく総合評価落札方式により委託者を選定する。 ・委託者の選定を行う際は、プライバシーマークやISMS(ISO/IEC 27001)等の認証取得事業者であること等、特定個人情報の保護を適切に行えることを確認する。
特定個人情報ファイルの閲覧者・更新者の制限		[　制限している　] ＜選択肢＞ 1）制限している　2）制限していない
	具体的な制限方法	委託契約書に以下の規定を設ける。 ・アクセス権限を付与する従業員数を必要最小限に制限する。 ・従業員に付与するアクセス権限を必要最小限にする。 ・アクセス権限の管理状況を定期的に報告する。
特定個人情報ファイルの取扱いの記録		[　記録を残している　] ＜選択肢＞ 1）記録を残している　2）記録を残していない
	具体的な方法	システムへのアクセスログ、システムでの操作ログの記録を行い、操作者個人を特定できるようにする。 記録したログについては、ガバメントクラウド環境のデータ分析・可視化サービス(SIEM)にて相関分析を行っており、不正ログイン等を検知できるようにしている。また、SIEMの分析結果をもとに、運用業者が操作者による内部不正がなかったかを自己点検し、月次にて職員にセキュリティ監査報告を実施している。
特定個人情報の提供ルール		[　定めている　] ＜選択肢＞ 1）定めている　2）定めていない
	委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	情報提供等記録用符号は、情報提供ネットワークシステムの内部管理のためにのみ利用され、その他の目的に利用されたり、情報提供ネットワークシステムから外部に出ることはないため、委託先から他者への提供は行わない。
	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	・情報提供等記録用符号は、情報提供ネットワークシステムの内部管理のためにのみ利用され、その他の目的に利用されたり、情報提供ネットワークシステムから外部に出ることはないため、委託先へ特定個人情報の提供は行わない。 ・再委託も含めて、番号法第11条の趣旨を踏まえ、必要かつ適切な監督を行う。
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	番号法第23条第3項に基づく施行令第29条にて、情報提供等記録の保存期間は7年間とされており、保存期間の過ぎたファイルは、バッチ処理等自動処理にて適切に消去する。 ・委託契約終了後の特定個人情報の消去については、ISMS（情報セキュリティマネジメントシステム）に準拠した廃棄プロセスを確保する。デジタル庁の情報システム責任者等は委託先事業者から提出される報告書の内容を確認するとともに、報告書に基づいてシステム管理者に聴取を行い、必要に応じて立入検査を実施することで、委託契約終了後の消去が適切に行われていることを確認する。

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	・秘密保持義務 ・事業所内からの特定個人情報の持出しの禁止 ・特定個人情報の目的外利用の禁止 ・再委託における条件 ・漏えい事案等が発生した場合の委託先の責任 ・委託契約終了後の特定個人情報の返却又は廃棄 ・従業者に対する監督・教育 ・契約内容の遵守状況について報告を求める規定 等 特定個人情報の取扱いに関する以下の管理を強化する。 ・契約に基づき委託先に報告を求める。 ・委託先に対して実地の監査、調査等を行う。 ・委託契約で盛り込んだ内容の実施の程度を把握した上で、委託の内容等の見直しを検討することを含め、適切に評価する。
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		[　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　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、再委託契約に次の事項を盛り込むこととする。 ・秘密保持義務 ・事業所内からの特定個人情報の持出しの禁止 ・特定個人情報の目的外利用の禁止 ・漏えい事案等が発生した場合の再委託先の責任の明確化 ・再委託契約終了後の特定個人情報の返却又は廃棄 ・従業者に対する監督・教育 ・契約内容の遵守状況について報告を求める規定 等 また、再委託先がデジタル庁と同等の安全管理措置を講じていることを確認する。 特定個人情報の取扱いに関する以下の管理を強化する。 ・契約に基づき再委託先に報告を求める。 ・再委託先に対して実地の監査、調査等を行う。 ・再委託契約で盛り込んだ内容の実施の程度を把握した上で、再委託の内容等の見直しを検討することを含め、適切に評価する。
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
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	・情報提供等記録開示システムを介して行われた提供要求者からの情報提供等記録の提供要求については、提供を行う際に、いつどの提供要求者が提供要求し、どの情報提供等記録を提供したのかの記録を情報提供ネットワークシステムにて全て記録・管理する。 ・書面により行われた本人等からの情報提供等記録の開示請求については、職員が特定の端末を操作して開示することとなるが、その際受付の記録と共に、どの職員がいつどの情報提供等記録について抽出したのか情報提供ネットワークシステムにて記録・管理する。 ・個人情報保護委員会からの報告若しくは資料の提出の求めについては、所定の書面等にて受け付け、職員が特定の端末を操作して提供することとなるが、その際受付の記録と共に、どの職員がいつどの情報について抽出したのか情報提供ネットワークシステムにて記録・管理する。 ・情報提供等記録については、番号法第23条第3項に基づく施行令第29条の規定に従い、7年間保存する。
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	・情報提供ネットワークシステムを使用して行われる特定個人情報の照会・提供について、個人情報保護法第76条の規定に基づき、開示請求できることとなっており、本人等からの開示請求に基づき情報提供等記録ファイルを使用して、開示することとなっている。 ・開示請求は、書面で行い、開示は書面によって行われる。 ・提供要求は、情報提供等記録開示システムを介して行うことができるようになっており、提供は情報提供等記録開示システムによって行われる。 ・本人等からの開示請求、提供要求又は個人情報保護委員会からの報告若しくは資料の提出の求めがあった場合には、システム処理又は定められた手続に則り処理が行われ、当該開示又は提出等に関する記録が情報提供ネットワークシステムに記録・保管される。 ・定期的に書面による開示請求又は報告若しくは提出の求めと操作ログ等を管理者が突き合わせ確認を行う。 ・情報提供等記録については、番号法第23条第3項に基づく施行令第29条の規定に従い、7年間保存する。
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： 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	・情報提供ネットワークシステムを介して行われる特定個人情報の照会・提供については、個人情報保護法第76条の規定に基づき、本人等が開示請求できることとなっている。 ・書面により行われた本人等からの開示請求又は個人情報保護委員会からの報告若しくは資料の提出の求めがあった場合には、定められた手続に則り処理を行う。 ・定期的に書面による開示請求又は報告若しくは提出の求めと操作ログ等を管理者が突き合わせ確認を行う。
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

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	【誤った情報を提供してしまうリスク】 ・情報提供等記録開示システムを介して行われた提供要求者からの提供要求については、情報提供等記録開示システムにおいて要求者である本人又は代理人から指定された内容のみが開示されるようシステムにより担保されている。 ・書面により行われた本人等からの開示請求又は個人情報保護委員会からの報告若しくは資料の提出の求めについては、定められた手続に則り処理を行い、指定された内容であることを確認の上、回答することとしている。 【誤った相手に提供してしまうリスク】 ・情報提供等記録開示システムを介して行われた提供要求者からの提供要求については、情報提供等記録開示システムにおいて要求者である本人又は代理人の真正性の確認が行われており、提供要求された本人の内容のみが提供されるようシステムにより担保されている。 ・書面により行われた本人等からの開示請求又は個人情報保護委員会からの報告若しくは資料の提出の求めについては、定められた手続に則り本人確認書類等により請求者（本人又は代理人、個人情報保護委員会）の真正性の確認を行う。開示する情報については、書面又はパスワードを付して情報を格納した電子記録媒体により開示する。
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
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置	
―	

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

7. 特定個人情報の保管・消去		
リスク1： 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[特に力を入れて遵守している]	＜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	[特に力を入れて整備している]	＜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	[特に力を入れて整備している]	＜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	[特に力を入れて周知している]	＜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	[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	・運用端末が置かれた部屋では、個人ごとのICカードと生体認証を併用した入退室管理を実施する。 ・運用端末が置かれた部屋に監視カメラを設置し、端末や媒体の持ち出し・持ち込みの監視を行う。 ＜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。 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	・ガバメントクラウド上で、情報提供ネットワークシステムをプライベートな空間として確保し、インターネットと論理的に分離している。 ・運用施設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。 ・FW（ファイアウォール）等を導入し、必要な通信のみ制御する。 ・ガバメントクラウドが提供するデータ分析・可視化サービス(SIEM)を利用して侵入検知を行う。 ・端末にウィルス対策ソフトを導入し、ウィルスパターンファイルを適宜更新する。 ・OSやデータベースに関するセキュリティ情報の情報収集を行い、セキュリティパッチを適宜適用する。 ＜ガバメントクラウドにおけるその他の措置＞ 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。 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システムが管理する特定個人情報を含むデータは、クラウド事業者がアクセスできないようシステムにおいて制御を講じる。	
⑦バックアップ	[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
⑧事故発生時手順の策定・周知	[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
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	[発生あり]	＜選択肢＞ 1）発生あり 2）発生なし
その内容	令和5年5月23日に誤登録事案（他人の口座情報等の漏えいのおそれ）が判明した旨公表。 その後の総点検や、新たな検出手法を通じて、令和4年3月28日から令和5年6月23日にかけて、自治体支援窓口においてマイナポータル経由で公金受取口座を登録する際、ログアウトを忘れたため他人のマイナンバーと預貯金口座情報を誤って紐付けてしまうことで誤登録された可能性が高い事例が、計1,186件あることが判明した。	
再発防止策の内容	・ログアウトの徹底をはじめ、公金受取口座の登録支援に係るマニュアル遵守の徹底などについて、自治体向けに通知 ・口座登録開始時だけではなく、口座登録完了時にもマイナンバーカードを改めて読み込むことで、ログアウト忘れ防止のためのシステム改修を実施（令和5年6月23日） ・登録申請時に重複確認を行い、口座の重複登録を防止するシステムを整備・導入（令和6年1月16日）	

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	システムでは生存者か死者かを区別することなく安全管理を実施する。	
その他の措置の内容	ー	
リスクへの対策は十分か	[特に力を入れている]	＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク2： 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	情報提供等記録ファイルには、いつ誰と誰の間で特定個人情報の照会・提供があったかを記録する必要があるため、過去の情報であっても更新せずに、事実をそのまま記録する必要があるので、このリスクは該当しない。	
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
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	番号法第23条第3項に基づく施行令第29条の規定において、保存期間は7年間とされており、保存期間経過後は、適切に廃棄等を行う。 ＜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	ー	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置		
・運用施設において本番環境にアクセスできる端末は、専用端末を固定して設置しており、アクセス端末を限定している。 ・運用施設にPCを持ち込む場合には、事前での持ち込み申請を必須とし、入室時にシリアル番号を確認することにより、持ち込み機器の制限を実施している。 ・不正ソフト対策として、運用施設にPCを持ち込む場合には、最新のパターンファイルにてウイルスチェックを実施したかを確認している。		

Ⅳ　その他のリスク対策 ※

1. 監査		
①自己点検	［　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
具体的なチェック方法	「デジタル庁情報セキュリティポリシー」に基づき、年度自己点検計画を策定し、デジタル庁の全職員を対象として、情報セキュリティ対策の自己点検を実施している。 自己点検の手法としては、各職員が研修システムにアクセスして自己点検票（チェックリスト形式）に回答することにより年1回実施している。この結果、情報セキュリティ対策の取組不足が認められた項目については改善措置を講じている。 運用業者においてもセキュリティ自己点検を毎月実施しており、その結果を関係者と共有している。例えば、作業申請のないログインがないか等を点検している。 また、不正なアクセスがないこと等、定常又は定期的に監査を実施している。	
②監査	［　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
具体的な内容	「デジタル庁情報セキュリティポリシー」に基づき、年度監査計画を策定し、情報セキュリティ対策に係る自己点検結果の監査など、運用業者に対する情報セキュリティ対策の監査を実施している。 監査手法としては、以下の項目について、運用管理支援業者に委託して実施している。 ・運用作業マニュアルのデジタル庁情報セキュリティポリシー等との準拠性監査 ・内部不正監査 ・調達仕様書に規定された役務の準拠性監査 ・セキュリティ自己点検結果の確認 ・情報提供ネットワークシステムの脆弱性対応確認 ・ガバメントクラウド環境のデータ分析・可視化サービスによるセキュリティインシデント予兆の確認 なお、デジタル庁職員については、特定個人情報を取り扱う業務は原則として行わないが、ログインや操作等のログについてはガバメントクラウド環境のデータ分析・可視化サービス(SIEM)を利用した監査の対象となっており、内部不正などの検知が行われる。 ＜ガバメントクラウドにおける措置＞ 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、ISMAPにおいて、クラウドサービス事業者は定期的にISMAP監査機関リストに登録された監査機関による監査を行うこととしている。	

2. 従業者に対する教育・啓発		
従業者に対する教育・啓発	［　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
具体的な方法	「デジタル庁情報セキュリティポリシー」に基づき、情報セキュリティ対策の教育に係る計画を策定し、デジタル庁の全職員を対象として、情報セキュリティ対策の教育を実施している。 教育手法としては、各職員が最低年1回は研修システムにアクセスしてコンテンツを閲覧することにより実施している。コンテンツの作成に当たっては、昨年度の自己点検の結果を基に、結果が良くなかった点検事項を重点的に教育できる内容としている。 運用業者においても、全従事者へのセキュリティ教育を毎年度実施している。教育に関する受講者を管理しており、未受講者がないようにしている。要員の交代が発生した場合には新しい要員にもセキュリティ教育を必ず実施している。	

3. その他のリスク対策
情報提供ネットワークシステムは、情報連携のための個人を識別する符号（個人番号ではない）と、情報連携の結果（提供された情報は含まない）のみを保持しており、個人の具体的な情報は保持していない。 情報提供ネットワークシステムにおける内部不正やマルウェア検知のために、ガバメントクラウド環境のデータ分析・可視化サービス(SIEM)を利用している。分析結果を常に関係者間で共有することにより、セキュリティ事故を未然に防止する取組みを継続している。 特定個人情報の漏えいを含むセキュリティインシデントの発生を想定し、異常時運用実施要領とインシデントレベル判定表を作成している。発生事象とその重大性をレベル1～5に分類しており、レベル別の対応事項を整理して運用している。事象の確認、報告、影響調査、原因の特定と対処、再発防止策の検討、事実の公表などの対応準備が整っている。 情報提供ネットワークシステムを使用した情報連携が番号法などの関係法令に基づき適切に実施されるよう、データ標準レイアウト関連様式（※）の改版において、作業スケジュールの設定及び管理を行うとともに、制度所管府省に対してデータ標準レイアウト作成支援環境及びチェックツールを提供することにより、情報連携の対象となる事務や当該事務を処理するために必要な特定個人情報

の項目について、十分な確認を行うことができる環境を整備することとしている。

＜ガバメントクラウドにおける措置＞
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、デジタル庁及びその業務データの取扱いについて委託を受ける運用保守事業者が責任を有する。
ガバメントクラウド上での業務アプリケーションの運用等に障害が発生する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、国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、運用保守事業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、デジタル庁及び関係者で協議を行う。

（※）データ標準レイアウト
情報連携における共通的なフォーマットで、ある事務手続において、どの情報が提供できるかを表形式でまとめたもの。情報連携を実施するシステムに共通して適用し、必要な情報のみを取得できるようにしている。

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	デジタル庁個人情報受付窓口 住所：〒102-0094　東京都千代田区紀尾井町1-3（東京ガーデンテラス紀尾井町20階） 電話番号：03-4477-6775
②請求方法	・郵送による開示請求 ・電子申請による開示請求 ・来庁による開示請求
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：　保有個人情報が記録されている行政文書1件つき、開示請求書に300円の収入印紙を貼付、窓口に来所して現金を納付又は電子納付する　方法　）
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	連携用符号発行管理ファイル、情報提供等記録ファイル
公表場所	・事務所への備付け ・デジタル庁ホームページ（https://www.digital.go.jp/privacy）から個人情報ファイル簿の検索が可能
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	デジタル庁個人情報受付窓口 住所：〒102-0094　東京都千代田区紀尾井町1-3（東京ガーデンテラス紀尾井町20階） 電話番号：03-4477-6775
②対応方法	個人情報開示請求等事務マニュアルを作成しており、来所又は電話等による相談等に対して、必要な情報提供等を行っている。

Ⅵ　評価実施手続

1. 基礎項目評価	
①実施日	令和6年10月18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パブリックコメントのホームページに意見募集公告を掲載し、ダウンロード資料として「特定個人情報保護評価書（全項目評価書）（案）」及び「意見募集要項」を掲載した。意見はインターネット上の意見募集フォームにより受け付けた。
②実施日・期間	令和6年8月19日から令和6年9月18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	・ガバメントクラウドにおける措置について ・特定個人情報の一元管理に関する対策について ・特定個人情報の情報漏えいに関する対策について
⑤評価書への反映	寄せられた意見及び意見に対する考え方と対応方針を回答として一覧形式で取りまとめた。回答はe-Govパブリックコメントのホームページにて公表する。
3. 第三者点検	
①実施日	ー
②方法	ー
③結果	ー
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6年10月7日
②個人情報保護委員会による審査	(1)情報提供ネットワークシステムの運営に関する事務の内容、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、情報提供ネットワークシステムをインターネットから論理的に分離する旨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・見直しを行い、今後リスクを相当程度変動させ得る事実関係の変更が生じ、当該変更に応じたリスク対策を講ずる際などには、必要な特定個人情報保護評価を適切に実施する体制を、有効に機能させることが重要である。 (4)情報提供ネットワークシステムのガバメントクラウドへの移行に伴う特定個人情報ファイルのデータ移行の際には、委託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ことが重要である。また、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29年5月30日	「Ⅰ．1．②」等 評価書全般	（略）	情報提供等記録開示システムによる情報提供等記録の確認行為を「提供要求」または「提供」として記載し、書面による開示請求と区別した	事後	時点修正（重要な変更に当たらない）
平成29年5月30日	「Ⅰ．1．②」等 評価書全般	特定個人情報保護委員会	個人情報保護委員会	事後	時点修正（重要な変更に当たらない）
平成29年5月30日	「Ⅰ．1．②」等 評価書全般	（略）	平成29年5月30日施行の改正番号法の条番号に変更	事後	時点修正（重要な変更に当たらない）
平成29年5月30日	「Ⅰ．1．②」等 評価書全般	平成29年1月から情報提供等記録開示システムが稼働する予定である旨を記載	平成29年7月から情報提供等記録開示システムが稼働する予定である旨を記載	事後	時点修正（重要な変更に当たらない）
平成29年5月30日	Ⅰ．1．②	情報提供ネットワークシステムの運用業務に係る項目については、想定で記載している旨を記載	項目が確定したため削除	事後	時点修正（重要な変更に当たらない）
平成29年5月30日	Ⅰ．4．②	4．開示請求者からの開示請求への対応 開示請求者は、いつ誰が情報提供ネットワークシステムを使用して本人の特定個人情報を照会・提供したのか確認できる。	4．開示請求者等からの開示請求等への対応 開示請求者等は、いつ誰が情報提供ネットワークシステムを使用して本人の特定個人情報を照会・提供したのか確認できる。	事後	時点修正（重要な変更に当たらない）
平成29年5月30日	Ⅰ．7．①	総務省大臣官房企画課個人番号企画室	総務省大臣官房個人番号企画室	事後	時点修正（重要な変更に当たらない）
平成29年5月30日	Ⅰ．7．②	個人番号企画室長　望月明雄	官房参事官（個人番号企画室長）　下仲宏卓	事後	時点修正（重要な変更に当たらない）
平成29年5月30日	「Ⅰ．8」等 評価書全般	システム開発の主体として内閣官房社会保障改革担当室	該当しなくなったため削除	事後	時点修正（重要な変更に当たらない）
平成29年5月30日	Ⅱ．2．⑤ （連携用符号発行管理ファイル）	平成28年4月1日 （現時点の予定として記載。）	平成28年10月18日	事後	時点修正（重要な変更に当たらない）
平成29年5月30日	Ⅱ．3．⑨ （連携用符号発行管理ファイル）	平成28年4月1日	平成28年10月18日	事後	時点修正（重要な変更に当たらない）
平成29年5月30日	Ⅱ．2．⑤ （情報提供等記録ファイル）	平成29年1月4日	平成29年7月18日	事後	時点修正（重要な変更に当たらない）

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5月30日	Ⅱ．3．⑨ （情報提供等記録ファイル）	平成29年1月4日	平成29年7月18日	事後	時点修正（重要な変更に当たらない）
平成29年5月30日	Ⅱ．4．⑥	平成27年度以降に調達を実施予定	エヌ・ティ・ティ・コミュニケーションズ株式会社	事後	時点修正（重要な変更に当たらない）
平成29年5月30日	Ⅱ．5 （情報提供等記録ファイル・提供先1）	開示請求を行った者（情報提供等記録開示システムを介して又は書面にて開示請求を受け付ける。）	開示請求を行った者（書面にて開示請求を受け付ける。） 又は情報提供等記録開示システムにより提供要求を行った者（情報提供等記録開示システムを介して提供要求を受け付ける。）	事後	時点修正（重要な変更に当たらない）
平成29年5月30日	Ⅱ．5．① （情報提供等記録ファイル・提供先1）	番号法第30条第2項の規定により読み替えられた行政機関個人情報保護法第12条	＜開示請求を行った者＞ 番号法第31条第2項の規定により読み替えられた行政機関個人情報保護法第12条 ＜情報提供等記録開示システムにより提供要求を行った者＞ 番号法附則第6条第3項	事後	時点修正（重要な変更に当たらない）
平成29年5月30日	Ⅱ．5．② （情報提供等記録ファイル・提供先2）	特定個人情報の取扱いに関する監視又は監督及び苦情の申出についての必要なあっせんを行う。	特定個人情報の取扱いに関する監視又は監督を行う。	事後	時点修正（重要な変更に当たらない）
平成29年5月30日	Ⅲ．5 （情報提供等記録ファイル・リスク1）	・開示請求は、書面又は情報提供等記録開示システムを介して行うことができるようになっており、開示は書面・電子記録媒体・情報提供等記録開示システムによって行われる。	・開示請求は、書面で行い、開示は書面・電子記録媒体によって行われる。 ・提供要求は、情報提供等記録開示システムを介して行うことができるようになっており、提供は情報提供等記録開示システムによって行われる。	事後	時点修正（重要な変更に当たらない）
平成29年5月30日	Ⅲ．7．⑥	・FW（ファイアウォール）、WAF（アプリケーションファイアウォール）等を導入し、必要な通信のみ制御する。	・FW（ファイアウォール）等を導入し、必要な通信のみ制御する。	事後	時点修正（重要な変更に当たらない）
平成29年5月30日	Ⅲ．7．⑨	発生なし	発生あり、内容について記載	事後	時点修正（重要な変更に当たらない）
平成29年5月30日	Ⅳ．1．①	「総務省情報セキュリティポリシー」（平成23年総務省行政情報化推進委員会決定）に基づき、年度自己点検計画を策定し、総務省の全職員を対象として、情報セキュリティ対策の自己点検を実施している。（注）	「総務省情報セキュリティポリシー」に基づき、年度自己点検計画を策定し、総務省の全職員を対象として、情報セキュリティ対策の自己点検を実施している。	事後	時点修正（重要な変更に当たらない）
平成29年5月30日	Ⅴ	連携用符号発行管理ファイル（仮）、情報提供等記録ファイル（仮）	連携用符号発行管理ファイル、情報提供等記録ファイル	事後	時点修正（重要な変更に当たらない）

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5月30日	（別添2）	*要件定義段階の記録項目及び項目名	項目が確定したため削除	事後	時点修正（重要な変更に当たらない）
平成29年5月30日	（別添2）	（略）	記録項目を追加等するとともに、一部の情報名称を変更。	事後	時点修正（重要な変更に当たらない）
平成31年4月26日	Ⅰ．1．②	平成29年7月から情報提供等記録開示システムが稼働する予定である旨を記載	平成29年7月から情報提供等記録開示システムが稼働している旨を記載	事後	時点修正（重要な変更に当たらない）
平成31年4月26日	Ⅰ．7．②	官房参事官（個人番号企画室長） 下仲宏卓	官房参事官（個人番号企画室長）	事後	特定個人情報保護評価に関する規則等の改正に伴う変更
平成31年4月26日	Ⅱ．2．⑤ （連携用符号発行管理ファイル）	平成28年10月18日特定個人情報の使用開始日において同じ。）	平成28年10月18日	事後	時点修正（重要な変更に当たらない）
平成31年4月26日	Ⅱ．2．⑤ （情報提供等記録ファイル）	平成29年7月18日（現時点での予定として記載。特定個人情報の使用開始日において同じ。）	平成29年7月18日	事後	時点修正（重要な変更に当たらない）
平成31年4月26日	Ⅲ．7．⑨ （連携用符号発行管理ファイル）	（略）	平成30年7月3日（火）に発生した事象を記載	事後	時点修正（重要な変更に当たらない）
平成31年4月26日	Ⅲ．7．⑨ （情報提供等記録ファイル）	（略）	平成30年7月3日（火）に発生した事象を記載	事後	時点修正（重要な変更に当たらない）
平成31年4月26日	Ⅴ．1．①	平成29年7月から情報提連携が開始する予定である旨を記載	平成29年7月から情報提連携を開始しているため、注釈の記載を削除	事後	時点修正（重要な変更に当たらない）
令和2年2月19日	Ⅰ．5．	1．番号法 ・第19条第7号（特定個人情報の提供の制限）	1．番号法 ・第19条第7号・第8号（特定個人情報の提供の制限）	事後	特定個人情報保護評価の再実施
令和2年2月19日	（別添1）	提供要求者	国民	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅱ．3．⑤ （連携用符号発行管理ファイル）	特定個人情報の使用に関しては、番号法第2条第14項、第19条第7号、第19条第8号及び第21条第2項において、情報提供ネットワークシステムにより情報連携を行う旨が規定されている。	第2条第14項を削除	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅱ．3．⑦ （連携用符号発行管理ファイル）	10人未満	10人以上50人未満	事後	特定個人情報保護評価の再実施

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2月19日	Ⅱ．4．④ （連携用符号発行管理ファイル）	システムが設置されるデータセンター内にて取扱いを行う。	システムが設置されるデータセンター内にて データは管理されている。 運用者が運用施設にて運用するが、特定個人情報へのアクセスはできない。	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅱ．6．① （連携用符号発行管理ファイル）	個人ごとのICカードや生体認証を用いた	個人ごとのICカードと生体認証を併用した	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅱ．6．① （連携用符号発行管理ファイル）	－	運用者の運用端末からのアクセスはできない仕組みについて補記	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅱ．6．② （連携用符号発行管理ファイル）	連携用符号の重複生成を防ぐため、及び、各情報照会者等から情報提供用個人識別符号を用いた照会要求に対応するために生成済みの符号に関する情報を恒久的に保管する必要があるため、消去しない。	連携用符号の重複生成を防ぐため、及び、各情報照会者等から情報提供用個人識別符号を用いた照会要求に対応するために生成済みの符号に関する情報を恒久的に保管する必要があるため、原則として消去しない。例外的に事務処理誤りを考慮して、物理削除要求電文による削除が可能である。	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅱ．6．③ （連携用符号発行管理ファイル）	消去しない	原則として消去しない。例外的に事務処理誤りを考慮して、住民基本台帳ネットワークシステムを介した物理削除電文による削除が可能である。	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅱ．7 （連携用符号発行管理ファイル）	－	災害対策、アクセス端末の限定、持ち込み機器の制限、不正ソフト対策について記載	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅱ．3．⑧ （情報提供等記録ファイル）	－	行政機関個人情報保護法に基づき開示請求できることについて記載	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅱ．3．⑧ （情報提供等記録ファイル）	番号法第19条第12項	番号法第19条第12号	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅱ．4．④ （情報提供等記録ファイル）	システムが設置されるデータセンター内にて取扱いを行う。	システムが設置されるデータセンター内にて データは管理されている。 運用者が運用施設にて運用するが、特定個人情報へのアクセスはできない。	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅱ．5．⑥ （情報提供等記録ファイル）	（略）	提供方法から「電子記録媒体（フラッシュメモリを除く。）」を削除	事後	特定個人情報保護評価の再実施

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2月19日	Ⅱ．5．提供先2．② （情報提供等記録ファイル）	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の再実施
令和2年2月19日	Ⅱ．6．① （情報提供等記録ファイル）	個人ごとのICカードや生体認証を用いた	個人ごとのICカードと生体認証を併用した	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅱ．6．① （情報提供等記録ファイル）	－	運用者が特定個人情報としてのアクセスはできない仕組みについて補記	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅱ．7 （情報提供等記録ファイル）	－	災害対策、アクセス端末の限定、持ち込み機器の制限、不正ソフト対策について記載	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅲ．3 （連携用符号発行管理ファイル）	（略）	職員はアクセス権を保持していないため、対象から削除	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅲ．3 （連携用符号発行管理ファイル）	－	全てのユーザと権限の棚卸しについて記載	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅲ．3 （連携用符号発行管理ファイル）	連携用符号は、人が識別できない形態（規則性を備えていない数字・文字列の羅列）で生成・保存し、運用端末からアクセスできないよう使用の制御を行っている。	連携用符号は、人が識別できない形態（規則性を備えていない数字・文字列の羅列）で生成・保存し、運用端末から運用者がアクセスできないよう制御を行っている。	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅲ．3 （連携用符号発行管理ファイル）	－	「全ての」業務従事者を対象とするため補記	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅲ．3 （連携用符号発行管理ファイル）	（略）	「クローズドの」を削除	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅲ．4 （連携用符号発行管理ファイル）	－	特定個人情報の取扱いについて補記	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅲ．4 （連携用符号発行管理ファイル）	十分に行っている	特に力を入れて行っている	事後	特定個人情報保護評価の再実施

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2月19日	Ⅲ．4 （連携用符号発行管理ファイル）	十分である	特に力を入れている	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅲ．7．⑤ （連携用符号発行管理ファイル）	個人ごとのICカードや生体認証を用いた	個人ごとのICカードと生体認証を併用した	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅲ．7．⑨ （連携用符号発行管理ファイル）	平成30年7月3日（火）に、外部の関係団体及び自治体に対し、国の機関の職員の141名分の個人情報（氏名116件及びメールアドレス77件）を電子メールで誤送信した。 個人情報の厳重かつ適正な管理を徹底する。	発生事象の内容と再発防止策を補記	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅲ．7 （連携用符号発行管理ファイル）	（略）	消去手順の内容について補記	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅲ．7 （連携用符号発行管理ファイル）	－	災害対策、アクセス端末の限定、持ち込み機器の制限、不正ソフト対策について記載	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅲ．3 （情報提供等記録ファイル）	（略）	職員はアクセス権を保持していないため、対象から削除	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅲ．3 （情報提供等記録ファイル）	－	全てのユーザと権限の棚卸しについて記載	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅲ．3 （情報提供等記録ファイル）	－	「全ての」業務従事者を対象とするため補記	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅲ．3 （情報提供等記録ファイル）	開示請求者	個人情報保護委員会	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅲ．3 （情報提供等記録ファイル）	（略）	「クローズドの」を削除	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅲ．4 （情報提供等記録ファイル）	－	SIEMによる不正ログイン等検知、相関分析実施について補記	事後	特定個人情報保護評価の再実施

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2月19日	Ⅲ．４ （情報提供等記録ファイル）	－	特定個人情報の取扱いについて補記	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅲ．４ （情報提供等記録ファイル）	十分に行っている	特に力を入れて行っている	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅲ．４ （情報提供等記録ファイル）	十分である	特に力を入れている	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅲ．５ （情報提供等記録ファイル）	－	「開示」を削除	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅲ．５ （情報提供等記録ファイル）	開示請求者	本人等	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅲ．５ （情報提供等記録ファイル）	開示請求は、書面で行い、開示は書面又は電子記録媒体によって行われる。	開示請求は、書面で行い、開示は書面によって行われる。	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅲ．７．⑤ （情報提供等記録ファイル）	個人ごとのICカードや生体認証を用いた	個人ごとのICカードと生体認証を併用した	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅲ．７．⑨ （情報提供等記録ファイル）	平成30年7月3日（火）に、外部の関係団体及び自治体に対し、国の機関の職員の141名分の個人情報（氏名116件及びメールアドレス77件）を電子メールで誤送信した。 個人情報の厳重かつ適正な管理を徹底する。	発生事象の内容と再発防止策を補記	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅲ．７ （情報提供等記録ファイル）	－	災害対策、アクセス端末の限定、持ち込み機器の制限、不正ソフト対策について記載	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅳ．１．①	－	運用業者について補記	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅳ．１．②	－	監査の具体的な内容について補記	事後	特定個人情報保護評価の再実施
令和2年2月19日	Ⅳ．２	－	運用業者について補記	事後	特定個人情報保護評価の再実施

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2月19日	Ⅳ．３	－	その他のリスク対策について記載	事後	特定個人情報保護評価の再実施
令和3年10月8日	表紙 評価実施機関名	総務大臣	内閣総理大臣	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅰ．１．②	(1)符号の生成（根拠法令：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施行令（平成26年政令第155号。以下「番号法施行令」という。）第20条）	(1)符号の生成（根拠法令：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施行令（平成26年政令第155号。以下「番号法施行令」という。）第27条）	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅰ．１．②	特定個人情報の項目	特定個人情報名	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅰ．１．②	番号法第19条第12号	番号法第19条第13号	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅰ．２．②	番号法第19条第12号	番号法第19条第13号	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅰ．２．②	－	第二期情報提供ネットワークシステムの移行に伴う記載	事前	重要な変更
令和3年10月8日	Ⅰ．５	第19条第7号・第8号	第19条第8号・第9号	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅰ．５	・第27条第1項・第2項・第4項・第5項・第6項（特定個人情報の提供の求めがあった場合の総務大臣の措置）	・第26条第1項・第2項・第4項・第5項・第6項（特定個人情報の提供の求めがあった場合の内閣総理大臣の措置）	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅰ．５	・第20条第6項・第7項（情報提供用個人識別符号の取得）	・第27条第5項・第6項（情報提供用個人識別符号の取得）	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅰ．７．①	総務省大臣官房個人番号企画室	デジタル庁デジタル社会共通機能グループ	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅰ．７．②	官房参事官（個人番号企画室長）	デジタル庁統括官（デジタル社会共通機能担当）付参事官（基準・標準担当）	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅱ．２．③ （連携用符号発行管理ファイル）	番号法第19条第7号及び第8号	番号法第19条第8号及び第9号	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅱ．２．④ （連携用符号発行管理ファイル）	個人番号（マイナンバー）	個人番号	事後	時点修正（重要な変更に当たらない）

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10月8日	Ⅱ．2．⑤ （連携用符号発行管理ファイル）	平成28年10月18日	令和3年9月1日	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅱ．2．⑥ （連携用符号発行管理ファイル）	総務省大臣官房個人番号企画室	デジタル庁デジタル社会共通機能グループ	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅱ．3．⑤ （連携用符号発行管理ファイル）	番号法第19条第7号、第19条第8号	番号法第19条第8号、第19条第9号	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅱ．3．⑦ （連携用符号発行管理ファイル）	総務省大臣官房個人番号企画室	デジタル庁デジタル社会共通機能グループ	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅱ．3．⑨ （連携用符号発行管理ファイル）	平成28年10月18日	令和3年9月1日	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅱ．4 （連携用符号発行管理ファイル）	委託事項1	第二期情報提供ネットワークシステムの移行に伴い、委託事項1～4に記載を変更	事前	重要な変更
令和3年10月8日	Ⅱ．6．③ （連携用符号発行管理ファイル）	－	第二期情報提供ネットワークシステムの移行に伴う記載	事前	重要な変更
令和3年10月8日	Ⅱ．7 （連携用符号発行管理ファイル）	LTOによるデータの長期保管について	第二期情報提供ネットワークシステムでは、LTOを使用しないため記載を変更	事前	重要な変更
令和3年10月8日	Ⅱ．2．④ （情報提供等記録ファイル）	特定個人情報の項目等の	特定個人情報名等の	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅱ．2．⑤ （情報提供等記録ファイル）	平成29年7月18日	令和3年9月1日	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅱ．2．⑥ （情報提供等記録ファイル）	総務省大臣官房個人番号企画室	デジタル庁デジタル社会共通機能グループ	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅱ．3．⑦ （情報提供等記録ファイル）	総務省大臣官房個人番号企画室	デジタル庁デジタル社会共通機能グループ	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅱ．3．⑧ （情報提供等記録ファイル）	番号法第30条第2項の規定に読み替え	番号法第31条第2項の規定による読替え	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅱ．3．⑧ （情報提供等記録ファイル）	番号法第19条第12号	番号法第19条第13号	事後	時点修正（重要な変更に当たらない）

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10月8日	Ⅱ．3．⑨ （情報提供等記録ファイル）	平成29年7月18日	令和3年9月1日	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅱ．4 （情報提供等記録ファイル）	委託事項1	第二期情報提供ネットワークシステムの移行に伴い、委託事項1～4に記載を変更	事前	重要な変更
令和3年10月8日	Ⅱ．5．③ （情報提供等記録ファイル）	・特定個人情報の項目	記載を削除	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅱ．5．③ （情報提供等記録ファイル）	総務省令	デジタル庁令	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅱ．5．① （情報提供等記録ファイル）	番号法第19条第12号	番号法第19条第13号	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅱ．6．③ （情報提供等記録ファイル）	－	第二期情報提供ネットワークシステムの移行に伴う記載	事前	重要な変更
令和3年10月8日	Ⅱ．7 （情報提供等記録ファイル）	LTOによるデータの長期保管について	第二期情報提供ネットワークシステムでは、LTOを使用しないため記載を変更	事前	重要な変更
令和3年10月8日	Ⅱ．（別添2） （情報提供等記録ファイル）	特定個人情報の項目	記載を削除	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅲ．3 （連携用符号発行管理ファイル）	パスワードには有効期限を設ける。また、	記載を削除	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅲ．3 （連携用符号発行管理ファイル）	－	第二期情報提供ネットワークシステムの移行に伴う記載	事前	重要な変更
令和3年10月8日	Ⅲ．4 （連携用符号発行管理ファイル）	－	第二期情報提供ネットワークシステムの移行に伴う記載	事前	重要な変更
令和3年10月8日	Ⅲ．4 （連携用符号発行管理ファイル）	総務省	デジタル庁	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅲ．7．⑥ （連携用符号発行管理ファイル）	－	・インターネットとは物理的に分離している。 （Ⅳ．3から記載を移行）	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅲ．7．⑨ （連携用符号発行管理ファイル）	重大事故	発生から3年が経過したため削除	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅲ．7 （連携用符号発行管理ファイル）	LTOによるデータの長期保管について	第二期情報提供ネットワークシステムでは、LTOは使用しないため記載を変更	事前	重要な変更

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10月8日	Ⅲ．３ （情報提供等記録ファイル）	パスワードには有効期限を設ける。また、	記載を削除	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅲ．３ （情報提供等記録ファイル）	－	第二期情報提供ネットワークシステムの移行に伴う記載	事前	重要な変更
令和3年10月8日	Ⅲ．４ （情報提供等記録ファイル）	－	第二期情報提供ネットワークシステムの移行に伴う記載	事前	重要な変更
令和3年10月8日	Ⅲ．４ （情報提供等記録ファイル）	総務省	デジタル庁	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅲ．５ （情報提供等記録ファイル）	番号法第30条第2項の規定に読み替え	番号法第31条第2項の規定による読替え	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅲ．５ （情報提供等記録ファイル）	番号法第31条第2項の規定に読み替え	番号法第31条第2項の規定による読替え	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅲ．７．⑥ （情報提供等記録ファイル）	－	・インターネットとは物理的に分離している。 （Ⅳ．３から記載を移行）	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅲ．７．⑨ （情報提供等記録ファイル）	重大事故	発生から3年が経過したため削除	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅲ．７ （情報提供等記録ファイル）	LTOによるデータの長期保管について	第二期情報提供ネットワークシステムでは、LTOは使用しないため記載を変更	事前	重要な変更
令和3年10月8日	Ⅳ．１．①	総務省に関する記載	デジタル庁に関する記載	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅳ．１．②	総務省に関する記載	デジタル庁に関する記載	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅳ．２	総務省に関する記載	デジタル庁に関する記載	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅳ．３	インターネットに接続していない記載	Ⅲ．７．⑥に記載を移行したため削除	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅳ．３	総務省	デジタル庁	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅳ．３	平成30年４月	削除	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅴ．１．①	総務省個人情報受付窓口　（注） 住所：〒100-8926　東京都千代田区霞が関2-1-2（中央合同庁舎第2号館2階） 電話番号：03-5253-5111（代表）。	デジタル庁個人情報受付窓口 住所：〒102-0094　東京都千代田区紀尾井町1-3（東京ガーデンテラス紀尾井町20階） 電話番号：03-4477-6775	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅴ．１．②	来省	来庁	事後	時点修正（重要な変更に当たらない）

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10月8日	Ⅴ．1．④	・総務省ホームページ （http://www.soumu.go.jp/menu_sinsei/kojin_jyouhou/index.html）	・デジタル庁ホームページ （https://www.digital.go.jp/privacy）	事後	時点修正（重要な変更に当たらない）
令和3年10月8日	Ⅴ．2．①	総務省個人情報受付窓口 住所：〒100-8926　東京都千代田区霞が関2-1-2（中央合同庁舎第2号館2階） 電話番号：03-5253-5111（代表）	デジタル庁個人情報受付窓口 住所：〒102-0094　東京都千代田区紀尾井町1-3（東京ガーデンテラス紀尾井町20階） 電話番号：03-4477-6775	事後	時点修正（重要な変更に当たらない）
令和6年10月18日	Ⅰ．2．②	（略）	令和8年1月以降において、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)を含む旨追記	事前	重要な変更
令和6年10月18日	Ⅰ．2．②	※現行の情報提供ネットワークシステムは、令和4年1月から第二期情報提供ネットワークシステムへ移行する。 特定個人情報は第二期情報提供ネットワークシステムで継続して使用するためデータ移行を行う。 特定個人情報のデータ移行は同一データセンター内のLAN接続で行うため安全である。 追加の対策として、①移行データの暗号化、②移行用一時ファイルのアクセス制限及び③ログ情報等の統合分析・監査を行うシステム（SIEM）による不正の監視を行う。	※現行の情報提供ネットワークシステムは、令和7年1月から第三期情報提供ネットワークシステムへ移行する。 特定個人情報は第三期情報提供ネットワークシステムで継続して使用するためデータ移行を行う。 特定個人情報のデータ移行は専用回線で行うため安全である。 追加の対策として、①移行データの暗号化、②移行用一時ファイルのアクセス制限及び③ログ情報等の監査による不正の監視を行う。 利用しなくなった環境の破棄は、ディスクの物理破壊、廃棄証明書の提示などの厳格な対応を行う。	事前	重要な変更
令和6年10月18日	Ⅱ．4．委託事項1 （連携用符号発行管理ファイル）	情報提供ネットワークシステムの移行に伴うデータ抽出及びテストデータ生成	情報提供ネットワークシステムの移行に伴う第二期システムからのデータ抽出	事前	重要な変更
令和6年10月18日	Ⅱ．4．委託事項1①委託内容 （連携用符号発行管理ファイル）	情報提供ネットワークシステムの移行に伴うデータ抽出及びテストデータ生成業務	情報提供ネットワークシステムの移行に伴うデータ抽出	事前	重要な変更
令和6年10月18日	Ⅱ．4．委託事項3④ （連携用符号発行管理ファイル）	機器の廃棄（倉庫保管のLTOを含む）	機器の廃棄	事前	重要な変更
令和6年10月18日	Ⅱ．4．委託事項4④ （連携用符号発行管理ファイル）	システムが設置されるデータセンター内にてデータは管理されている。	データはISMAPのリストに登録されたクラウドサービス上で管理されている。	事前	重要な変更
令和6年10月18日	Ⅱ．6．① （連携用符号発行管理ファイル）	（略）	ガバメントクラウドにおける措置を追記	事前	重要な変更

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10月18日	Ⅱ．6．③ (連携用符号発行管理ファイル)	(略)	ガバメントクラウドにおける措置を追記	事前	重要な変更
令和6年10月18日	Ⅱ．6．③ (連携用符号発行管理ファイル)	(略)	システム移行の際のデータの消去方法を見直したため記載を変更	事前	重要な変更
令和6年10月18日	Ⅱ．7 (連携用符号発行管理ファイル)	(略)	ガバメントクラウドに移行し、データセンターには特定個人情報を保管しなくなるため記載を見直し。	事前	重要な変更
令和6年10月18日	Ⅱ．3．⑥ (情報提供等記録ファイル)	・開示請求者等からの開示請求等に対して、対象となる情報提供等の記録を開示し、いつ誰がどのような情報を情報提供ネットワークシステムを使用して本人の特定個人情報を照会・提供したのか開示することを可能にする。	・開示請求者等からの開示請求等に対して、対象となる情報提供等の記録を開示し、いつ誰がどのような本人の特定個人情報を情報提供ネットワークシステムを使用して照会・提供したのか開示することを可能にする。	事前	重要な変更
令和6年10月18日	Ⅱ．3．⑧ (情報提供等記録ファイル)	情報提供ネットワークシステムを使用して行われる特定個人情報の照会・提供について、行政機関の保有する個人情報の保護に関する法律（平成15年法律第58号。以下「行政機関個人情報保護法」という。）第12条（番号法第31条第2項の規定による読替え）の規定に基づき、開示請求できることとなっており、本人等からの開示請求に基づき情報提供等記録ファイルを使用して、開示することとなっている。	情報提供ネットワークシステムを使用して行われる特定個人情報の照会・提供について、個人情報の保護に関する法律（平成15年法律第57号。以下「個人情報保護法」という。）第76条の規定に基づき、開示請求できることとなっており、本人等からの開示請求に基づき情報提供等記録ファイルを使用して、開示することとなっている。	事前	重要な変更
令和6年10月18日	Ⅱ．3．⑧ (情報提供等記録ファイル)	行政機関個人情報保護法第18条の規定により、情報提供等の記録の開示又は不開示の決定を行う。	個人情報保護法第82条の規定により、情報提供等の記録の開示又は不開示の決定を行う。	事前	重要な変更
令和6年10月18日	Ⅱ．4．委託事項1 (情報提供等記録ファイル)	情報提供ネットワークシステムの移行に伴うデータ抽出及びテストデータ生成	情報提供ネットワークシステムの移行に伴う第二期システムからのデータ抽出	事前	重要な変更
令和6年10月18日	Ⅱ．4．委託事項1①委託内容 (情報提供等記録ファイル)	情報提供ネットワークシステムの移行に伴うデータ抽出及びテストデータ生成業務	情報提供ネットワークシステムの移行に伴うデータ抽出	事前	重要な変更
令和6年10月18日	Ⅱ．4．委託事項3④ (情報提供等記録ファイル)	機器の廃棄（倉庫保管のLTOを含む）	機器の廃棄	事前	重要な変更
令和6年10月18日	Ⅱ．4．委託事項4 (情報提供等記録ファイル)	第二期情報提供ネットワークシステムの運用・保守業務	第三期情報提供ネットワークシステムの運用・保守業務	事前	重要な変更

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10月18日	Ⅱ．4．委託事項4④ （情報提供等記録ファイル）	システムが設置されるデータセンター内にてデータは管理されている。	データはISMAPのリストに登録されたクラウドサービス上で管理されている。	事前	重要な変更
令和6年10月18日	Ⅱ．5．提供先1．① （情報提供等記録ファイル）	番号法第31条第2項の規定により読み替えられた行政機関個人情報保護法第12条	個人情報保護法第76条	事後	時点修正（重要な変更に当たらない）
令和6年10月18日	Ⅱ．5．提供先1．③ （情報提供等記録ファイル）	（略）	「特定個人情報の項目」を追加	事前	重要な変更
令和6年10月18日	Ⅱ．5．提供先1．⑤ （情報提供等記録ファイル）	情報提供等の記録に係る本人、未成年者又は成年被後見人の法定代理人、本人の委任による代理人のうち、開示請求又は提供要求を行う者	情報提供等の記録に係る本人のうち、開示請求又は提供要求を行う者	事前	重要な変更
令和6年10月18日	Ⅱ．5．提供先2．② （情報提供等記録ファイル）	番号法第35条第1項の規定に基づき、個人情報保護委員会から提供の求めがある場合、情報提供等の記録等を基に調査を行い、特定個人情報の取扱いに関する監視又は監督を行う。	番号法第35条第1項の規定に基づき、情報提供等の記録等を基に調査を行い、特定個人情報の取扱いに関する監視又は監督を行う。	事後	時点修正（重要な変更に当たらない）
令和6年10月18日	Ⅱ．5．提供先2．⑤ （情報提供等記録ファイル）	全ての対象者	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・提供の対象となった者	事前	重要な変更
令和6年10月18日	Ⅱ．6．① （情報提供等記録ファイル）	（略）	ガバメントクラウドにおける措置を追記	事前	重要な変更
令和6年10月18日	Ⅱ．6．③ （情報提供等記録ファイル）	（略）	ガバメントクラウドにおける措置を追記	事前	重要な変更
令和6年10月18日	Ⅱ．6．③ （情報提供等記録ファイル）	（略）	システム移行の際のデータの消去方法を見直したため記載を変更	事前	重要な変更
令和6年10月18日	Ⅱ．7 （情報提供等記録ファイル）	（略）	ガバメントクラウドに移行し、データセンターには特定個人情報を保管しなくなるため記載を見直し。	事前	重要な変更
令和6年10月18日	Ⅲ．3．リスク4　リスクに対する措置の内容 （連携用符号発行管理ファイル）	【情報提供ネットワークシステム移行について】 特定個人情報のデータ移行は同一センター内のLAN接続で行い、第三者はアクセスできない。	【情報提供ネットワークシステム移行について】 特定個人情報のデータ移行は、ガバメントクラウド環境と第二期拠点間を移行用回線(閉域網)で接続を行い、第三者はアクセスできない。	事前	重要な変更

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10月18日	Ⅲ．3．リスク4に対する措置の内容 （連携用符号発行管理ファイル）	データ移行時において、作業者等によるデータの詐取や外部へのデータ漏えいの予防のために、ログ情報等の統合分析・監査を行うシステム（SIEM）を用いて、作業ログ、ファイル、フォルダ、NWのアクセス状況を監視（モニタリング）・分析し、移行元・移行先双方での不正の兆候や不正アクセスの検知を行う。	データ移行時において、作業者等によるデータの詐取や外部へのデータ漏えいの予防のために、第二期システムにおいてはログ情報等の統合分析・監査を行うシステム（SIEM）、第三期システムにおいてはガバメントクラウド環境のデータ分析・可視化サービス(SIEM)を用いて、各種ログによる監査及びファイル、フォルダ、NWのアクセス状況の監視（モニタリング）・分析を行い、移行元・移行先双方での不正の兆候や不正アクセスの検知を行う。	事前	重要な変更
令和6年10月18日	Ⅲ．3．リスク4　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 （連携用符号発行管理ファイル）	その際に用いる鍵は、物理的・論理的に内部情報を読み取られることに対する耐性の高い機能を備え、鍵の生成・管理における高い安全性を確保するハードウェア機器（HSM：Hardware Security Module）を用いて厳密な管理を行い、鍵の不正利用等を防止する。	その際に用いる鍵は、物理的・論理的に内部情報を読み取られることに対する耐性の高い機能を備え、鍵の生成・管理における高い安全性を確保するものとしてガバメントクラウドが提供する鍵管理サービスを用いて厳密な管理を行い、鍵の不正利用等を防止する。	事前	重要な変更
令和6年10月18日	Ⅲ．7．リスク1．⑤ （連携用符号発行管理ファイル）	（略）	ガバメントクラウドにおける措置を追記	事前	重要な変更
令和6年10月18日	Ⅲ．7．リスク1．⑥ （連携用符号発行管理ファイル）	・インターネットとは物理的に分離している。 ・FW（ファイアウォール）等を導入し、必要な通信のみ制御する。 ・ネットワークを介した侵入検知や保護を行えるIDS（侵入検知システム）・IPS（侵入保護システム）を設置する。	・ガバメントクラウド上で、情報提供ネットワークシステムをプライベートな空間として確保し、インターネットと論理的に分離している。 ・運用施設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。 ・FW（ファイアウォール）等を導入し、必要な通信のみ制御する。 ・ガバメントクラウドが提供するデータ分析・可視化サービス(SIEM)を利用して侵入検知を行う。	事前	重要な変更
令和6年10月18日	Ⅲ．7．リスク1．⑥ （連携用符号発行管理ファイル）	（略）	ガバメントクラウドにおける措置を追記	事前	重要な変更
令和6年10月18日	Ⅲ．7．リスク1．⑨ （連携用符号発行管理ファイル）	－	令和5年5月23日に判明した誤登録事案（他人の口座情報等の漏えいのおそれ）の内容及び再発防止策について記載。	事後	時点修正（重要な変更に当たらない）
令和6年10月18日	Ⅲ．7．リスク3 （連携用符号発行管理ファイル）	（略）	ガバメントクラウドにおける措置を追記	事前	重要な変更

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10月18日	Ⅲ．7．その他のリスクに対する措置 （連携用符号発行管理ファイル）	（略）	ガバメントクラウドに移行し、データセンターには特定個人情報を保管しなくなるため記載を見直し。	事前	重要な変更
令和6年10月18日	Ⅲ．3．リスク4に対する措置の内容 （情報提供等記録ファイル）	【情報提供ネットワークシステム移行について】 特定個人情報のデータ移行は同一センター内のLAN接続で行い、第三者はアクセスできない。	【情報提供ネットワークシステム移行について】 特定個人情報のデータ移行はガバメントクラウド環境と第二期拠点間を移行用回線(閉域網)で接続を行い、第三者はアクセスできない。	事前	重要な変更
令和6年10月18日	Ⅲ．3．リスク4に対する措置の内容 （情報提供等記録ファイル）	データ移行時において、作業者等によるデータの詐取や外部へのデータ漏えいの予防のために、ログ情報等の統合分析・監査を行うシステム（SIEM）を用いて、作業ログ、ファイル、フォルダ、NWのアクセス状況を監視（モニタリング）・分析し、移行元・移行先双方での不正の兆候や不正アクセスの検知を行う。	データ移行時において、作業者等によるデータの詐取や外部へのデータ漏えいの予防のために、第二期システムにおいてはログ情報等の統合分析・監査を行うシステム（SIEM）、第三期システムにおいてはガバメントクラウド環境のデータ分析・可視化サービス(SIEM)を用いて、各種ログによる監査及びファイル、フォルダ、NWのアクセス状況の監視（モニタリング）・分析を行い、移行元・移行先双方での不正の兆候や不正アクセスの検知を行う。	事前	重要な変更
令和6年10月18日	Ⅲ．3．リスク4　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 （情報提供等記録ファイル）	その際に用いる鍵は、物理的・論理的に内部情報を読み取られることに対する耐性の高い機能を備え、鍵の生成・管理における高い安全性を確保するハードウェア機器（HSM：Hardware Security Module）を用いて厳密な管理を行い、鍵の不正利用等を防止する。	その際に用いる鍵は、物理的・論理的に内部情報を読み取られることに対する耐性の高い機能を備え、鍵の生成・管理における高い安全性を確保するものとしてガバメントクラウドが提供する鍵管理サービスを用いて厳密な管理を行い、鍵の不正利用等を防止する。	事前	重要な変更
令和6年10月18日	Ⅲ．3．リスク4　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 （情報提供等記録ファイル）	・情報提供等記録用符号の生成の際は、連携用符号発行管理ファイルと突合し既に生成済みの情報提供等記録用符号と重複がないか等の確認を行い正確性を確保する。	・情報提供等記録用符号の生成の際は、連携用符号発行管理ファイルにおいて重複が無いことを確認することで、正確性を確保する。	事前	重要な変更
令和6年10月18日	Ⅲ．4．特定個人情報ファイルの取扱いの記録 （情報提供等記録ファイル）	記録したログについては、ログ情報等の統合分析・監査を行うシステム（SIEM）にて相関分析を行っており、不正ログイン等を検知できるようにしている。	記録したログについては、ガバメントクラウド環境のデータ分析・可視化サービス(SIEM)にて相関分析を行っており、不正ログイン等を検知できるようにしている。	事前	重要な変更
令和6年10月18日	Ⅲ．5．リスク1（特定個人情報の提供・移転に関するルール）（情報提供等記録ファイル）	行政機関個人情報保護法第12条（番号法第31条第2項の規定による読替え）	個人情報保護法第76条	事後	時点修正（重要な変更に当たらない）
令和6年10月18日	Ⅲ．5．リスク2 （情報提供等記録ファイル）	行政機関個人情報保護法第12条（番号法第31条第2項の規定による読替え）	個人情報保護法第76条	事後	時点修正（重要な変更に当たらない）

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10月18日	Ⅲ．7．リスク1．⑤ （情報提供等記録ファイル）	（略）	ガバメントクラウドにおける措置を追記	事前	重要な変更
令和6年10月18日	Ⅲ．7．リスク1．⑥ （情報提供等記録ファイル）	・インターネットとは物理的に分離している。 ・FW（ファイアウォール）等を導入し、必要な通信のみ制御する。 ・ネットワークを介した侵入検知や保護を行えるIDS（侵入検知システム）・IPS（侵入保護システム）を設置する。	・ガバメントクラウド上で、情報提供ネットワークシステムをプライベートな空間として確保し、インターネットと論理的に分離している。 ・運用施設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。 ・FW（ファイアウォール）等を導入し、必要な通信のみ制御する。 ・ガバメントクラウドが提供するデータ分析・可視化サービス(SIEM)を利用して侵入検知を行う。	事前	重要な変更
令和6年10月18日	Ⅲ．7．リスク1．⑥ （情報提供等記録ファイル）	（略）	ガバメントクラウドにおける措置を追記	事前	重要な変更
令和6年10月18日	Ⅲ．7．リスク1．⑨ （情報提供等記録ファイル）	－	令和5年5月23日に判明した誤登録事案（他人の口座情報等の漏えいのおそれ）の内容及び再発防止策について記載。	事後	時点修正（重要な変更に当たらない）
令和6年10月18日	Ⅲ．7．リスク3 （情報提供等記録ファイル）	（略）	ガバメントクラウドにおける措置を追記	事前	重要な変更
令和6年10月18日	Ⅲ．7．その他のリスクに対する措置 （情報提供等記録ファイル）	（略）	ガバメントクラウドに移行し、データセンターには特定個人情報を保管しなくなるため記載を見直し。	事前	重要な変更
令和6年10月18日	Ⅳ．1．①	（略）	監査について定常又は定期的に実施していることを追記	事前	重要な変更
令和6年10月18日	Ⅳ．1．②	ログ情報等の統合分析・監査システムにおけるセキュリティインシデント予兆の確認	ガバメントクラウド環境のデータ分析・可視化サービスによるセキュリティインシデント予兆の確認	事前	重要な変更
令和6年10月18日	Ⅳ．1．②	（略）	デジタル庁職員に対する監査及びガバメントクラウドにおける措置を追記	事前	重要な変更
令和6年10月18日	Ⅳ．1．③	ログ情報等の統合分析・監査を行うシステム（SIEM）を稼働させている。	ガバメントクラウド環境のデータ分析・可視化サービス(SIEM)を利用している	事前	重要な変更
令和6年10月18日	Ⅳ．1．③	（略）	ガバメントクラウドにおける措置を追記	事前	重要な変更