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	情報提供等記録開示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	
情報提供等記録開示システム運営に関する事務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、特定個人情報の漏洩その他の事態を発生させるリスクを軽減させるために適切な措置を講じることをもって、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	

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】
公表日

［平成30年５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	情報提供等記録開示システムの運営に関する事務
②事務の内容　※	・情報提供等記録開示システム（以下「開示システム」という。）は、行政手続における特定の個人を識別するための番号の利用等に関する法律（以下「番号法」という。）第23条第3項に規定される情報提供ネットワークシステムで生成、保存される利用者本人の情報提供等記録（以下「自己情報提供等記録」という。）について、利用者本人からの要求に基づき表示を行うために設置されるシステムである（番号法附則第6条第3項）。開示システムの運営に関する事務では、大きく分けて下記の2種類の事務を実施する。 (1)情報提供ネットワークシステム経由で取得する特定個人情報の表示等 ・開示システムの利用者本人に対し、①自己情報提供等記録の表示、②情報提供ネットワークシステムに接続する機関（以下「情報保有機関」という。）が保有する利用者本人の特定個人情報（以下「自己情報」という。）の表示及びAPIによる外部ウェブサービス（注1）への自己情報の提供並びに③情報保有機関から情報提供ネットワークシステム経由で利用者本人宛に送信された情報（件名、本文及び付随するデータ等が含まれる。以下「お知らせ情報」という。）の表示及びAPIによる外部ウェブサービスへのお知らせ情報の提供を実施する。 (2)開示システムと連携する他のシステム経由で取得する情報のAPIによる外部ウェブサービスへの提供 ・利用者本人の同意の下、開示システムのAPIの利用が許可された外部ウェブサービスに対し、開示システムと連携する他のシステム（以下「連携先システム」（注2）という。）経由で取得する情報（件名、本文及び付随するデータ等が含まれる。なお、付随するデータには特定個人情報が含まれうる。以下「連携先システム経由情報」という。）の提供を実施する。 ・連携先システム経由情報は、連携先システムから取得後まもなく開示システムから消去されるため、本事務に関するリスク対策については Ⅲ　1．に簡潔に記載している。 ※　そのほか、開示システムにおいては、連携先システム経由情報のうち、件名の閲覧及びその他の情報を閲覧するためのリンク先を表示する事務も実施しているが、当該事務においては特定個人情報を取り扱わないため、本評価書記載の対象外としている。 （注1）外部ウェブサービスとは、情報セキュリティ要件等につき、一定の基準を満たしているとして、内閣府から開示システムのAPI利用の許可を受けた民間事業者が提供しているサービスである。 （注2）現時点で、開示システムと連携しているシステムは、国税庁のe-Tax、日本年金機構のねんきんネット、日本郵便のMyPost、野村総合研究所のe-私書箱がある。
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	情報提供等記録開示システム
	1　利用者管理機能 (1)本人確認機能 ・開示システムは、利用者本人または任意代理人にパスワードを入力させ、個人番号カード内に格納されている利用者証明用電子証明書を取り出すとともに、公的個人認証サービスに対し、当該電子証明書の有効性を問い合わせる。 ・開示システムは、当該電子証明書が有効だった場合、本人確認を完了する（その際、当該電子証明書のシリアル番号（以下「シリアル番号」という。）を取得する。）。 (2)ログイン機能 ・利用者本人は、開示システムに対してログインを試みる。 ・開示システムは、本人確認後、シリアル番号に対応する利用者フォルダが存在する場合、ログインを認める。 ・存在しない場合、(3)を実施する。 (3)利用者フォルダ開設等機能 ・利用者本人がログインを試みた際に、当該シリアル番号が格納されている利用者フォルダが存在しなかった場合、そもそも利用者フォルダが存在しないかシリアル番号が更新されている可能性があるため、開示システムは、住民基本台帳ネットワークシステム経由で情報提供ネットワークシステムから利用者を識別するための情報提供用個人識別符号（以下「機関別符号」という。）を取得する。 ・開示システムは、取得した機関別符号に基づき、再度利用者フォルダが存在するか確認する。 ・当該機関別符号に対応する利用者フォルダが存在しない場合、利用者本人から利用者情報の登録を受けた上で、利用者フォルダファイル（本事務で取扱う特定個人情報ファイル）内に利用者フォルダを生成し、シリアル番号を機関別符号と紐づけて格納する。その際、当該利用者フォルダには利用者フォルダ番号が割り振られる。 ・当該機関別符号に対応する利用者フォルダが存在する場合、シリアル番号が更新されているため、利用者フォルダに格納されているシリアル番号を今回取得したシリアル番号に置き換える。 ※　当該機能については、APIによる提供も行う。具体的には、①外部ウェブサービスが開示システムのAPIに対し、利用者フォルダ開設要求を行い、②開示システムは上記処理を実施し、③その結果を外部ウェブサービスに伝える。 2　代理人管理機能 ・代理権の設定及び代理権の削除を行う。 ア）代理権設定機能（被代理人及び代理人が同席し、同一端末で設定する場合） ・利用者本人が個人番号カードを用いてログイン後、開示システムは、任意代理人の個人番号カードで本人確認を行うとともに、代理権設定について利用者本人及び任意代理人より同意を得る。 ・利用者本人が代理権設定画面において、代理の範囲（特定個人情報番号単位）及び有効期限を入力する。 ・開示システムは、利用者本人及び任意代理人のシリアル番号に基づき、利用者フォルダ番号を利用者フォルダから取得する。 ・開示システムは、代理権情報として、利用者フォルダファイル内の代理情報フォルダに利用者本人と任意代理人の利用者フォルダ番号、代理の範囲（特定個人情報番号単位等）及び有効期限等を記録する。 イ）代理権設定機能（遠隔地の別端末で設定する場合） ・外部ウェブサービスにおいて、代理の範囲と有効期限等が記載されたファイルに対し、任意代理人及び利用者本人の個人番号カードに格納されている署名用電子証明書を用いて電子署名を付す。 ・外部ウェブサービスは、開示システムの代理権設定APIを呼び出し、当該ファイル並びに利用者本人及び任意代理人の署名用電子証明書を送信する。 ・開示システムは、当該署名用電子証明書のシリアル番号に基づき、地方公共団体情報システム機構から利用者証明用電子証明書のシリアル番号を入手する。 ・開示システムは、当該シリアル番号に基づき、利用者本人と任意代理人の利用者フォルダから利用者フォルダ番号を取り出す。 ・開示システムは、代理権情報として、利用者フォルダファイル内の代理情報フォルダに本人と任意代理人の利用者フォルダ番号、代理の範囲（特定個人情報番号単位等）及び有効期限等を記録する。 ウ）代理権削除機能 ・利用者本人または任意代理人が開示システムにログインを行い、解除要求を行う。 ・ア）及びイ）で記録された情報が削除される。 3 「情報提供ネットワークシステム経由で取得する特定個人情報の表示等」事務の遂行に必要な機能 (1) 情報取得・表示機能 ア）自己情報提供等記録または自己情報の取得 ・利用者本人がログイン後、自己情報提供等記録または自己情報の取得要求を行う。

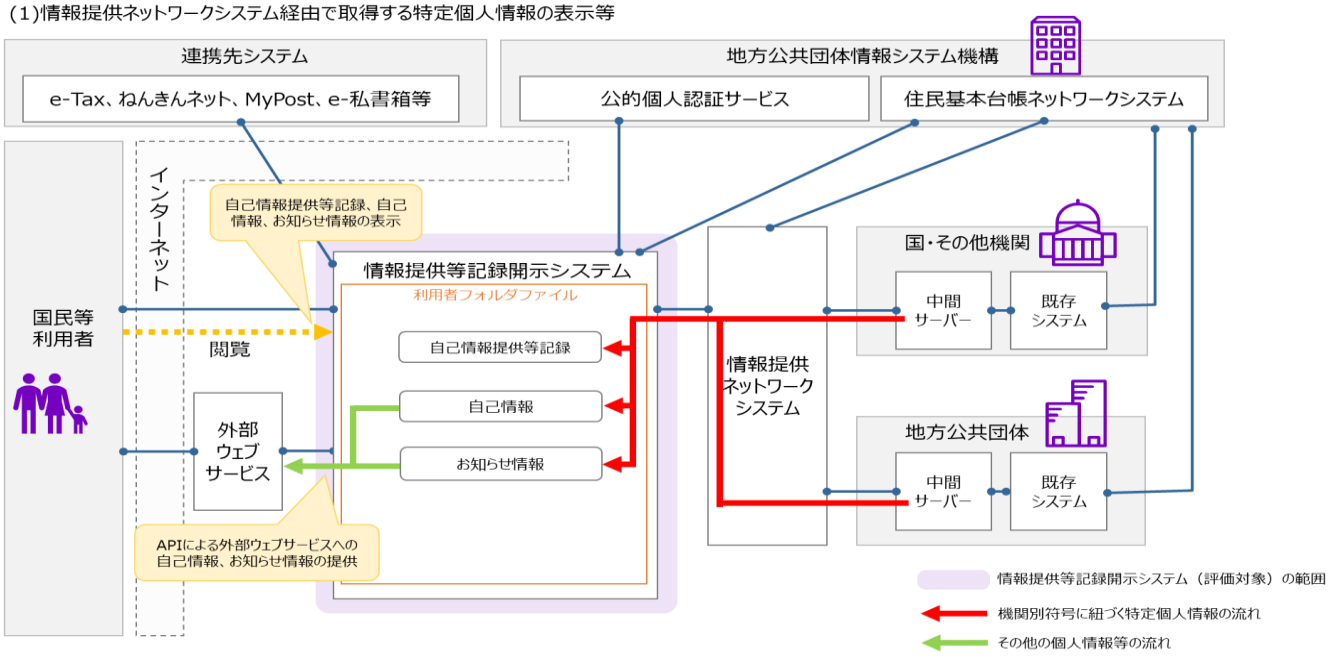
②システムの機能	・開示システムは、シリアル番号に基づき、機関別符号を利用者フォルダから取得する。 ・開示システムは、当該機関別符号に基づき、自己情報提供等記録については情報提供ネットワークシステムから取得し、自己情報については、情報提供ネットワークシステム経由で情報保有機関から取得し、利用者フォルダに格納する。 イ）お知らせ情報の取得 ・情報保有機関は、情報提供ネットワークシステム経由で開示システムに対し、機関別符号に基づき、本人の利用者フォルダが開設されているか確認を行う（その際に情報提供ネットワークシステムは処理通番を生成し、開示システムに対して送付する。）。 ・利用者フォルダが開設されていた場合、開示システムは当該処理通番を利用者本人の利用者フォルダに格納するとともに、情報保有機関に対し、情報提供ネットワークシステム経由で利用者フォルダが開設されている旨を通知し、その通知を受けた情報保有機関は、情報提供ネットワークシステム経由で開示システムに対し、処理通番を付してお知らせ情報を送信する。 ・開示システムは当該処理通番に基づき、お知らせ情報を利用者本人の利用者フォルダに格納する。 ウ）情報の表示 ・利用者本人は、自己情報提供等記録、自己情報またはお知らせ情報の表示要求を行う。 ・開示システムは、シリアル番号に基づき、利用者フォルダに格納されている当該情報を取得し、開示システムに接続された端末に表示する。 (2) 情報提供機能 ア）自己情報 ・外部ウェブサービスが、開示システムのAPIに対し、外部ウェブサービスの認証要求及び自己情報の取得要求を行う。 ・開示システムは、外部ウェブサービスの認証を行った上で、本人確認を行うとともに、自己情報の提供につき、利用者本人の同意を得る。 ・開示システムは、シリアル番号に基づき、機関別符号を利用者フォルダから取得する。 ・開示システムは、当該機関別符号に基づき、情報保有機関から情報提供ネットワークシステム経由で利用者本人の自己情報を取得し、外部ウェブサービスに提供する（当該情報は情報提供ネットワークシステムから取得後、一定時間経過後に削除される。）。 イ）お知らせ情報 ・外部ウェブサービスが、開示システムのAPIに対し、外部ウェブサービスの認証要求及びお知らせ情報件名一覧の取得要求を行う。 ・開示システムは、外部ウェブサービスの認証を行った上で、利用者本人の個人番号カードで本人確認を行うとともに、お知らせ情報の件名一覧並びに本文及び付随するデータの提供につき、利用者本人の同意を得る。 ・開示システムは、シリアル番号に基づき、利用者フォルダから利用者本人の連携用IDを抽出する。 ・開示システムは、連携用IDに基づき、お知らせ情報件名一覧の取得要求を連携先システムに送信し、お知らせ情報件名一覧を取得する。 ・開示システムは、お知らせ情報件名一覧及び件名ごとに一意な処理通番を付して外部ウェブサービスに送付する。 ・外部ウェブサービスは、開示システムのAPIに対し、利用者本人が取得を希望するお知らせ情報の件名に対応する処理通番に基づき、お知らせ情報の取得要求を行う。 ・開示システムは、当該処理通番に基づき、利用者フォルダから当該情報を取得し、外部ウェブサービスに提供する。 ※　任意代理人による情報取得または任意代理人への情報提供の際、開示システムは任意代理人のシリアル番号に基づき、本人のシリアル番号を取得する必要がある。具体的には、任意代理人のログインまたは本人確認の際に取得したシリアル番号に基づき、代理情報フォルダ内の任意代理人の利用者フォルダ番号と紐づいた本人の利用者フォルダ番号を取得し、当該利用者フォルダ番号に基づき、本人のシリアル番号を取得する。 4 「連携先システム経由で取得する情報のAPIによる外部ウェブサービスへの提供」事務の遂行に必要な機能 (1)認証連携機能 ・認証連携設定及び認証連携を行う。 ア）認証連携設定 ・利用者本人が開示システムにログインし、認証連携設定画面において、連携先システムを選択し、認証連携を行う旨の同意を行う。 ・開示システムは、利用者本人の連携用ID（連携先システムごとに異なる。）を生成し、利用者フォルダに保管する。 ・開示システムは、当該連携用IDを認証連携先に送付する。 ・（認証連携先は当該連携用IDと紐づくアカウントを生成・保管する。） イ）認証連携 ・利用者本人が開示システムにログインし、認証連携画面から認証連携先を選択する。 ・開示システムは、利用者フォルダから利用者本人の連携用IDを抽出し、認証連携先に送付する。 ・（認証連携先は当該連携用IDと紐づくアカウントによるログイン処理を行う。） (2) 情報提供機能 ・外部ウェブサービスが、開示システムのAPIに対し、外部ウェブサービスの認証要求及び連携先システ

	ム経由情報件名一覧の取得要求を行う。 ・開示システムは、外部ウェブサービスの認証を行った上で、利用者本人の本人確認を行うとともに、連携先システム経由情報の件名一覧並びに本文及び付随するデータの提供につき、利用者本人の同意を得る。 ・開示システムは、本人確認時に取得したシリアル番号に基づき、利用者フォルダから利用者本人の連携用IDを抽出する。 ・開示システムは、連携用IDに基づき、連携先システム経由情報件名一覧の取得要求を連携先システムに送信し、連携先システム経由情報件名一覧を取得する。 ・開示システムは、連携先システム経由情報件名一覧の件名ごとに一意な処理通番を付して外部ウェブサービスに送付する。 ・外部ウェブサービスは、開示システムのAPIに対し、利用者本人が取得を希望する連携先システム経由情報の件名に対応する処理通番に基づき、連携先システム経由情報の取得要求を行う。 ・開示システムは、当該処理通番に基づき、連携先システムから当該情報を取得し、外部ウェブサービスに提供する（当該情報は連携先システムから取得後、まもなく削除される。）。 ※　任意代理人による情報取得または任意代理人への情報提供の際、開示システムは任意代理人のシリアル番号に基づき、利用者本人の連携用IDを取得する必要がある。具体的には、任意代理人のログインまたは本人確認の際に取得したシリアル番号に基づき、代理情報フォルダ内の任意代理人の利用者フォルダ番号と紐づいた利用者本人の利用者フォルダ番号を取得し、当該利用者フォルダ番号に基づき、利用者本人の連携用IDを取得する。 ※　開示システムについては、現在プライベートクラウド及びオンプレミスで構築されているシステム基盤につき、令和２年４月よりパブリッククラウド環境（情報提供ネットワークシステム及び住民基本台帳ネットワークシステムとの接続点についてはオンプレミス環境）へ移行することとするところ、移行に際しては、委託先事業者がデータ抽出及びテストデータの生成、パブリック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行う。なお、パブリッククラウドサービスの利用にあたっては、パブリッククラウド事業者は個人情報にはアクセスしない。
③他のシステムとの接続	[○] 情報提供ネットワークシステム　　[　　] 庁内連携システム [○] 住民基本台帳ネットワークシステム　　[　　] 既存住民基本台帳システム [　　] 宛名システム等　　[　　] 税務システム [○] その他　（公的個人認証サービス、認証連携先（国税庁のe-Tax、日本年金機構のねんきんネット等））
システム2～5	
システム6～10	
システム11～15	
システム16～20	

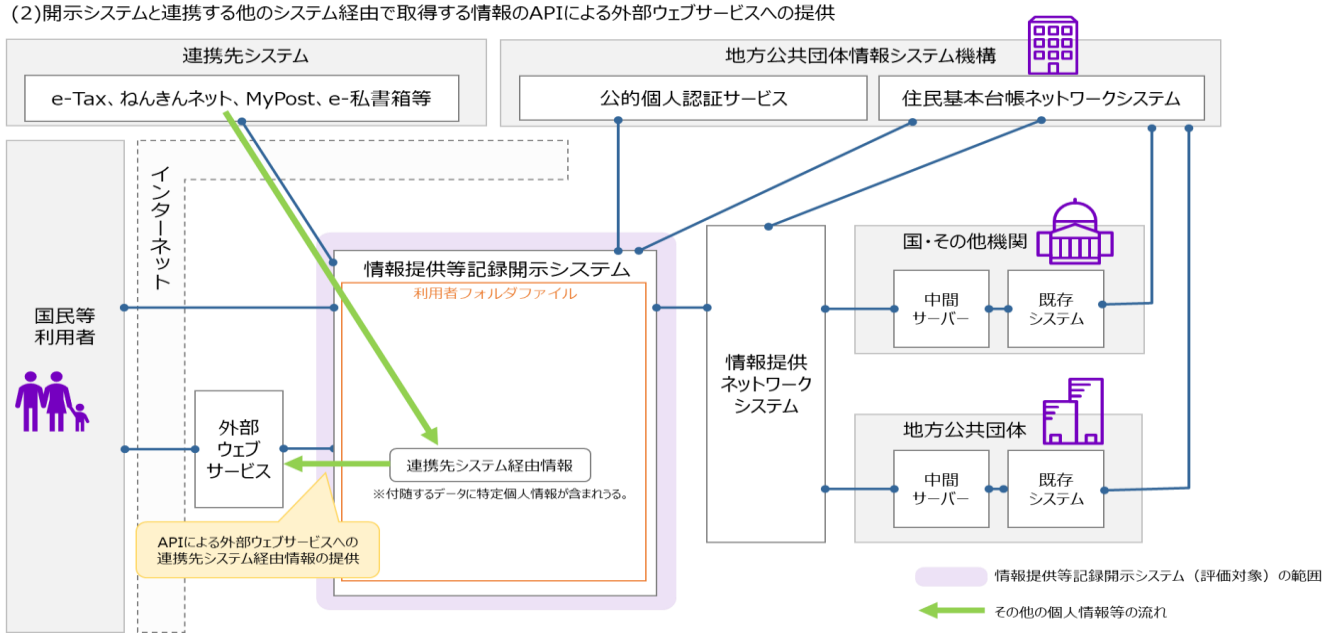
3. 特定個人情報ファイル名	
利用者フォルダファイル	
4. 特定個人情報ファイルを取り扱う理由	
①事務実施上の必要性	1. ②の事務を遂行するために、①開示システムが情報提供ネットワークシステム経由で特定個人情報を取得する場合には、機関別符号に基づき情報取得を行うこととしていること、②特定個人情報を含む各種情報を本人の機関別符号と紐づけて利用者フォルダに保有し、当該情報の利用者本人への表示等を行う必要があること、③任意代理人が利用者本人の情報を表示等するために、代理権設定情報を保有する必要があることの3点により、事務実施上特定個人情報ファイルを取り扱う必要がある。
②実現が期待されるメリット	利用者である国民等は、自己情報提供等記録、自己情報、お知らせ情報の確認ができるようになる。また、外部ウェブサービスが利用者本人の同意の下で自己情報、お知らせ情報及び連携先システム経由情報を取得することが可能となり、行政機関等が保有する情報の民間活用が促進される。
5. 個人番号の利用 ※	
法令上の根拠	番号法附則第6条
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	内閣府大臣官房番号制度担当室
②所属長の役職名	番号制度担当室長
8. 他の評価実施機関	
-	

（別添1）事務の内容

(1)情報提供ネットワークシステム経由で取得する特定個人情報の表示等



(2)開示システムと連携する他のシステム経由で取得する情報のAPIによる外部ウェブサービスへの提供



（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	
利用者フォルダファイル	
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 ※	開示システムを利用する国民等（開示システムのAPIによる外部ウェブサービスへの情報提供に同意した者も含む）
その必要性	・開示システムの利用にあたり、あらかじめ開示システムによる機関別符号の入手・保管が必要であるため。 ・個人番号を含む連携先システム経由情報を開示システムで保管する必要があるため。 ・任意代理人が利用者本人に代わり、開示システムを利用するため。
④記録される項目	[　　100項目以上　　] ＜選択肢＞ 1）10項目未満　　2）10項目以上50項目未満 3）50項目以上100項目未満　　4）100項目以上
主な記録項目 ※	・識別情報 [○] 個人番号　　[○] 個人番号対応符号　　[○] その他識別情報（内部番号） ・連絡先等情報 [　] 4情報（氏名、性別、生年月日、住所）　　[　] 連絡先（電話番号等） [　] その他住民票関係情報 ・業務関係情報 [　] 国税関係情報　　[　] 地方税関係情報　　[　] 健康・医療関係情報 [　] 医療保険関係情報　　[　] 児童福祉・子育て関係情報　　[　] 障害者福祉関係情報 [　] 生活保護・社会福祉関係情報　　[　] 介護・高齢者福祉関係情報 [　] 雇用・労働関係情報　　[　] 年金関係情報　　[　] 学校・教育関係情報 [　] 災害関係情報 [○] その他　（　利用者情報、代理情報、自己情報提供等記録、自己情報、お知らせ情報　）
その妥当性	1　個人番号対応符号（機関別符号） 開示システムが、機関別符号により利用者本人を特定の上、情報提供ネットワークシステム経由で自己情報提供等記録等を取得するため。 2　その他識別情報（内部番号）（機関別符号に紐づく情報） ・ 利用者フォルダ番号 　開示システムが、利用者本人の利用者フォルダを特定し、各種情報を保管するため。また、代理情報フォルダ内に利用者本人及び任意代理人の利用者フォルダ番号を紐づけて保管し、代理権情報の一部として記録するため。 ・連携用ID 　開示システムが認証連携等を実施するため。 3　その他（機関別符号に紐づく情報） (1)利用者情報（ニックネーム、メールアドレス等） ・開示システムが、開示システムの利用者本人にメールを送信等するため。 (2)代理情報 ・開示システムが任意代理人による代理の範囲等を特定するため。 (3) 自己情報提供等記録、自己情報、お知らせ情報 　・利用者本人の要求に基づき、自己情報提供等記録、自己情報及びお知らせ情報を開示システムに接続された端末に表示するため。 ・利用者本人の同意の下、自己情報、お知らせ情報を外部ウェブサービスに提供するため。
全ての記録項目	別添2を参照。
⑤保有開始日	平成29年1月16日
⑥事務担当部署	内閣府大臣官房番号制度担当室

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　（ 総務省、開示システムに接続する行政機関・独立行政法人等 ） [○] 地方公共団体・地方独立行政法人　（ 都道府県知事、市町村長等 ） [○] 民間事業者　（ 民間送達サービス等 ） [　　] その他　（　　）
②入手方法	[　　] 紙　[　　] 電子記録媒体（フラッシュメモリを除く。）　[　　] フラッシュメモリ [　　] 電子メール　[　　] 専用線　[　　] 庁内連携システム [○] 情報提供ネットワークシステム [○] その他　（ インターネット回線（サーバ認証を用いた暗号化通信を実施） ）
③入手の時期・頻度	1　個人番号対応符号（機関別符号） 利用者本人が開示システムへのログインを試みたが、利用者本人の利用者フォルダが存在しないとき 2　その他 (1)利用者情報（ニックネーム、メールアドレス等） ・利用者本人が、利用者情報を登録・変更する都度 (2)代理情報 ・利用者本人及び任意代理人による代理権設定の都度 (3) 自己情報提供等記録、自己情報、お知らせ情報 ・開示システムが、自己情報提供等記録、自己情報及びお知らせ情報を取得する都度 ※ 「2. ④」に記載されているその他識別情報（内部番号）には、利用者フォルダ番号及び連携用IDが含まれるところ、当該情報は内部で生成する番号であるため、「入手」には該当しない。
④入手に係る妥当性	1　個人番号対応符号（機関別符号） ・入手方法の妥当性 情報提供ネットワークシステムにおいて、機関別符号を生成するところ、当該システムから直接取得することが効率的であるため。 ・時期・頻度の妥当性 お知らせ情報は機関別符号に基づき、本人の利用者フォルダに格納されるところ、機関別符号をあらかじめ取得していなければ、当該フォルダを特定できないため。 2　その他 (1)利用者情報（ニックネーム、メールアドレス等） ・入手方法の妥当性 開示システムのみで利用する情報であることから、開示システムで入力を求めることが効率的であるため。 ・時期・頻度の妥当性 開示システムにおいては、利用者本人が利用者情報を登録・変更する際、初めて利用者情報を把握することとなるため。 (2)代理情報 ・入手方法の妥当性 開示システムのみで利用する情報であることから、開示システムで入力を求めることが効率的であるため。 ・時期・頻度の妥当性 開示システムにおいては、利用者本人及び任意代理人が代理権設定をする際、初めて代理情報を把握することとなるため。 (3) 自己情報提供等記録、自己情報、お知らせ情報 ・入手方法の妥当性 　当該情報の取得においては、既に構築されている情報提供ネットワークシステムまたは連携先システムの仕組みを活用することが効率的であるため。 ・時期・頻度の妥当性 　当該情報は、開示システムの外部で生成される情報であることから、情報提供ネットワークシステムまたは連携先システム経由で当該情報を取得する際に初めて当該情報を把握することとなるため。

⑤本人への明示		1　個人番号対応符号（機関別符号） 機関別符号については、入手の事実が利用規約に明示されている。 2　その他 (1)利用者情報（ニックネーム、メールアドレス等） ・利用者本人が利用者情報を登録・変更する際に入手の事実及び利用目的が明示される。 (2)代理情報 利用者本人及び任意代理人が代理権設定をする際に入手の事実及び利用目的が明示される。 (3) 自己情報提供等記録、自己情報、お知らせ情報 ・自己情報提供等記録、自己情報及びお知らせ情報については、入手の事実及び利用目的が利用規約等に明示されている。 ・自己情報及びお知らせ情報を外部ウェブサービスに提供する場合には、提供に係る利用者本人の同意を得る際、入手の範囲、事実及び利用目的が明示される。
⑥使用目的　※		1　個人番号対応符号（機関別符号） 開示システムが、利用者本人に係る自己情報提供等記録等を表示するため。 2　その他識別情報（内部番号） ・ 利用者フォルダ番号 　開示システムが、利用者本人の利用者フォルダを特定し、各種情報を保管するため。また、代理情報フォルダ内に利用者本人及び任意代理人の利用者フォルダ番号を紐づけて保管し、代理権情報の一部として記録するため。 ・連携用ID 　開示システムが認証連携等を実施するため。 3　その他 (1)利用者情報（ニックネーム、メールアドレス等） ・開示システムが、開示システムの利用者本人にメールを送信等するため。 (2)代理情報 ・開示システムが任意代理人による代理の範囲等を特定するため。 (3) 自己情報提供等記録、自己情報、お知らせ情報 　・利用者本人の要求に基づき、自己情報提供等記録、自己情報及びお知らせ情報を開示システムに接続された端末に表示するため。 　・利用者本人の同意の下、自己情報及びお知らせ情報を外部ウェブサービスに提供するため。
	変更の妥当性	－
⑦使用の主体	使用部署　※	内閣府大臣官房番号制度担当室
	使用者数	［　　10人未満　　］　＜選択肢＞ 1）10人未満　　2）10人以上50人未満 3）50人以上100人未満　　4）100人以上500人未満 5）500人以上1,000人未満　　6）1,000人以上
⑧使用方法　※		1　個人番号対応符号（機関別符号） 開示システムが情報提供ネットワークシステム経由で自己情報提供等記録等を取得する際、取得すべき利用者本人の情報を機関別符号を用いて情報提供ネットワークシステムに伝達する。 2　その他識別情報（内部番号） ・ 利用者フォルダ番号 　開示システムが、利用者フォルダを特定するための番号として利用するほか、代理権の設定・確認等の際に、利用者本人及び任意代理人を紐づけるために利用する。 ・連携用ID 　開示システムが連携用IDに基づき認証連携等を実施する。 3　その他 (1)利用者情報（ニックネーム、メールアドレス等） ・開示システムが、利用者情報に基づき開示システムの利用者本人にメールを送信等する。 (2)代理情報 ・開示システムが代理情報に基づき任意代理人による代理の範囲等を特定する。 (3) 自己情報提供等記録、自己情報、お知らせ情報 　・利用者本人の要求に基づき、自己情報提供等記録、自己情報及びお知らせ情報を開示システムに接続された端末に表示する。 　・利用者本人の同意の下、自己情報及びお知らせ情報を外部ウェブサービスに提供する。
	情報の突合　※	行わない。
	情報の統計分析　※	行わない。
	権利利益に影響を与え得る決定　※	該当なし。
⑨使用開始日		平成29年1月16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		パブリッククラウド環境移行に伴うデータ抽出及びテストデータ生成
①委託内容		パブリッククラウド環境移行に伴うデータ抽出及びテストデータ生成業務
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	[1万人以上10万人未満] ＜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 ※	開示システムを利用する国民等（開示システムのAPIによる外部ウェブサービスへの情報提供に同意した者も含む）
	その妥当性	パブリッククラウド環境移行に向けたデータの抽出を適切に実施するためには、職員が有さない専門的な知識・技術を有する者に特定個人情報ファイル全体の取扱いを委託する必要がある。
③委託先における取扱者数		[10人未満] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[ ]専用線 [ ]電子メール [○]電子記録媒体（フラッシュメモリを除く。） [ ]フラッシュメモリ [ ]紙 [ ]その他 （ ）
⑤委託先名の確認方法		委託先名は、官報公示及び内閣府ホームページにより、国民等が確認可能。（案件名：「情報提供等記録開示システムの再構築及び同システム等のサービス提供」 内閣府ホームページURL：https://www.cao.go.jp/chotatsu/kohyo/tekiseika/1nendo/20190905_kohyo_kyoso.pdf）。
⑥委託先名		アクセンチュア株式会社
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内閣府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		パブリッククラウド環境移行に伴うデータ投入
①委託内容		パブリッククラウド環境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	[1万人以上10万人未満] ＜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 ※	開示システムを利用する国民等（開示システムのAPIによる外部ウェブサービスへの情報提供に同意した者も含む）
	その妥当性	パブリッククラウド環境移行において、現行の開示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、職員が有さない専門的な知識・技術を有する者に特定個人情報ファイル全体の取扱いを委託する必要がある。
③委託先における取扱者数		[10人未満] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上

④委託先への特定個人情報ファイルの提供方法		[　　]専用線　　[　　]電子メール　[○]電子記録媒体(フラッシュメモリを除く。) [　　]フラッシュメモリ　　[　　]紙 [　　]その他　(　　)
⑤委託先名の確認方法		委託先名は、官報公示及び内閣府ホームページにより、国民等が確認可能。(案件名:「情報提供等記録開示システムの再構築及び同システム等のサービス提供」 内閣府ホームページURL:https://www.cao.go.jp/chotatsu/kohyo/tekiseika/1nendo/20190905_kohyo_kyoso.pdf)。
⑥委託先名		アクセンチュア株式会社
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
再委託	⑧再委託の許諾方法	原則として再委託は行わないこととするが、再委託を行う場合には、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内閣府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。
再委託	⑨再委託事項	上記委託事項と同じ。
委託事項3		パブリッククラウド環境移行後の破棄等
①委託内容		パブリッククラウド環境移行後の破棄等業務
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	[　　1万人以上10万人未満　　]　　＜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　※	開示システムを利用する国民等(開示システムのAPIによる外部ウェブサービスへの情報提供に同意した者も含む)
	その妥当性	パブリッククラウド環境移行前の現行の開示システムの特定個人情報ファイルについては、その全体を適切に消去する必要がある。
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　(システム直接操作　　)
⑤委託先名の確認方法		委託先名は、官報公示及び内閣府ホームページにより、国民等が確認可能。(案件名:「情報提供等記録開示システムの再構築及び同システム等のサービス提供」 内閣府ホームページURL:https://www.cao.go.jp/chotatsu/kohyo/tekiseika/1nendo/20190905_kohyo_kyoso.pdf)。
⑥委託先名		アクセンチュア株式会社
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
再委託	⑧再委託の許諾方法	原則として再委託は行わないこととするが、再委託を行う場合には、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内閣府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。
再委託	⑨再委託事項	上記委託事項と同じ。
委託事項4		情報提供等記録開示システムのサービス提供
①委託内容		利用者フォルダ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)

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 ※	開示システムを利用する国民等（開示システムのAPIによる外部ウェブサービスへの情報提供に同意した者も含む）
	その妥当性	委託事業者による開示システムのサービス提供を受けるためには、特定個人情報全体の取扱いを委託する必要がある。
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　（ システム直接操作　）
⑤委託先名の確認方法		委託先名は、官報公示及び内閣府ホームページにより、国民等が確認可能。（案件名：「情報提供等記録開示システムの再構築及び同システム等のサービス提供」 内閣府ホームページURL：https://www.cao.go.jp/chotatsu/kohyo/tekiseika/1nendo/20190905_kohyo_kyoso.pdf）。
⑥委託先名		アクセンチュア株式会社
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内閣府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 ※		パブリッククラウド環境及びオンプレミス環境のデータベース内に保管される。 (1)パブリッククラウド環境における立入り・アクセス制限 ・Ⅲ　7. ⑤具体的な対策の内容(1)と同じ。 (2)オンプレミス環境における立入り・アクセス制限 ・Ⅲ　7. ⑤具体的な対策の内容(2)と同じ。
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	1　個人番号対応符号（機関別符号） 　利用者本人が開示システムの利用を希望し、利用者本人の同意に基づき、開示システムが利用者フォルダを開設する際に開示システムが取得するものであり、利用者本人が利用者フォルダの削除を行わない限り、保管され続ける。 ※長期間利用がない（一定期間ログインがない場合など）利用者フォルダ内の特定個人情報の削除については今後検討。 2　その他識別情報（内部番号） ・利用者フォルダ番号 　利用者本人が開示システムの利用を希望し、利用者本人の同意に基づき、開示システムが利用者フォルダを開設する際に開示システムが生成するものであり、本人が利用者フォルダの削除を行わない限り、保管され続ける。 ・連携用ID 　利用者本人が認証連携を希望し、利用者本人の同意に基づき、開示システムが認証連携を行う設定を行う際に開示システムが生成するものであり、本人が認証連携を解除しない限り、保管され続ける。 3　その他 (1)利用者情報（ニックネーム、メールアドレス等） 利用者本人が開示システムの利用を希望し、利用者本人の同意に基づき、開示システムが利用者フォルダを開設する際に利用者本人が設定するものであり、利用者本人が利用者フォルダの削除を行わない限り、保管され続ける。 (2)代理情報 利用者本人及び任意代理人が代理権設定の際に有効期限等を指定するため、利用者本人または任意代理人が代理権を削除しない限り、当該期限経過後に削除する。 (3) 自己情報提供等記録、自己情報、お知らせ情報 　・自己情報提供等記録及び自己情報については、開示システムが、①利用者本人の情報表示要求に基づき、当該情報を表示した際は利用者本人のログアウト後に、②外部ウェブサービスの情報取得要求に基づき、自己情報を提供した際は、情報提供ネットワークシステムから取得後一定時間経過後に削除する。 　・情報提供ネットワークシステムを通じて開示システムに対して送信されたお知らせ情報については、各情報保有機関等が保存期限を設定しているため、当該期限経過後に消去することが妥当である。また、外部ウェブサービスの情報取得要求に基づき、連携先システムを通じて取得した連携先システム経由情報を提供した際は、連携先システムからの取得後まもなく削除する。
③消去方法		・保管期間を経過した特定個人情報は開示システムにより自動的に消去される。 ・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。 【パブリッククラウド環境移行の際に実施する措置】 ・移行後に利用しなくなったオンプレミス環境の機器等は、破棄するまでの間、特定個人情報の漏えいが起きないよう適切に保管する。 ・利用者フォルダファイルが記録された機器を破棄する場合、専用のデータ削除ソフトウェアの利用により、データを復元できないよう電子的に完全に消去するとともに、消去証明書を提出させる。また、当該機器は物理的に破壊し、内閣府の職員が当該措置の完了まで立ち会いを行うなど確実な履行を担保する。

7. 備考

－

（別添2）特定個人情報ファイル記録項目

利用者フォルダファイル(1/2)

情報名			記録項目名		説明
1	利用者フォルダ管理情報	利用者のログインに関する情報を管理する	1	利用者フォルダ番号	開示システム内で利用者フォルダを識別するID
			2	シリアル番号	利用者フォルダの開設時に使用した個人番号カード利用者証明用電子証明書の番号
			3	機関別符号	情報提供ネットワークシステムから取得した開示システム用の符号
			4	登録日時	利用者フォルダの登録を行った日時
			5	登録利用者情報識別子	登録を行った利用者を識別するID
			6	更新日時	利用者フォルダ情報の更新を行った日時
			7	更新利用者情報識別子	更新を行った利用者を識別するID
2	利用者情報	利用者が開示システムを操作するに当たり保持する属性情報	1	ニックネーム	利用者が設定するニックネーム
			2	メール通知有無（回答到着）	要求に対する回答到着時にメール通知を行うか否かを設定する
			3	メール通知有無（お知らせ到着）	お知らせ到着時にメール通知を行うか否かを設定する
			4	メール通知有無（利用者情報の設定）	利用者情報の設定が変更したときにメール通知を行うか否かを設定する
			5	メール通知有無（連携先システム連携）	連携先システムとの連携登録と連携解除の実施にメール通知を行うか否かを設定する
			6	メール通知有無（利用者フォルダ使用量超過）	利用者フォルダの使用量の上限値及びしきい値が超過した時にメール通知を行うか否かを設定する
			7	メール通知有無（ログイン）	ログイン及び連携先システムへの連携時にメール通知を行うか否かを設定する
			8	メールアドレス1	利用者が設定するメールアドレス
			9	メールアドレス2	利用者が設定するメールアドレス
			10	言語指定コード	利用者が設定する情報提供開示システムの画面に表示する言語を指定する
			11	利用履歴表示期間（月）	利用者が設定する利用履歴を画面に表示する期間
			12	最終ログイン日時	利用者が最後にログインした日時
			13	最終ログアウト日時	利用者が最後にログアウトした日時
			14	前回ログイン日時	利用者が前回ログインした日時
3	利用履歴情報	利用者の開示システムの操作履歴を保管する	1	利用履歴通番	利用者単位かつ利用履歴登録ごとに付与される番号
			2	操作者識別子	操作者を特定する内部管理用のID
			3	サービスコード	利用履歴を登録するサービスを識別する
			4	処理通番（利用履歴）	利用履歴を登録した際の情報に紐づく処理通番
			5	操作者IPアドレス	操作者の端末のIPアドレス
			6	利用履歴詳細	利用履歴を登録する契機となった業務において詳細を設定する
			7	利用履歴設定種別コード	利用履歴に設定する操作内容、処理内容を一意に識別する
			8	代理関係番号	操作者が代理人の場合の代理関係番号
4	代理権限情報	代理権限の範囲、期間を管理する	1	代理権限番号	代理権限を識別する番号
			2	代理期間の開始日	代理期間の開始日
			3	代理期間の終了日	代理期間の終了日
			4	代理権限の範囲（サービス）	開示システムの各種サービスに係る代理権限の範囲
			5	代理権限の範囲（特定個人情報番号単位等）	の取り扱いに係る代理権限の範囲
5	代理関係情報	代理人と被代理人の紐付けを管理する	1	任意代理人の利用者フォルダ番号	任意代理人の利用者フォルダ番号
			2	委任者の利用者フォルダ番号	委任者の利用者フォルダ番号
			3	代理権限の有効期間の開始日	代理権限の有効期間の開始日
			4	代理権限の有効期間の終了日	代理権限の有効期間の終了日
			5	代理関係メモ	委任者との代理関係や代理作業に関するメモ
			6	代理人管理メール送信有無情報コード	代理人管理メールの送信有無を管理する
			7	代理関係名	委任者と代理人との関係名
			8	無効化フラグ	代理人関係の無効化状態を管理する
			9	期限切れ事前通知完了フラグ	期限切れ事前通知の完了状態を管理する
6	自己情報提供等記録情報	利用者に開示する自己情報提供等記録情報を管理する	1	処理通番（開示請求）	開示請求を識別する通番（情報提供ネットワークシステムより提供）
			2	処理通番の枝番（開示請求）	処理通番（開示請求）の枝番
			3	処理通番枝番	処理通番の枝番であり、特定個人情報単位に付与する
			4	提供の求めの日時	情報提供の求めの日時
			5	情報照会者機関コード	情報照会者の機関コード
			6	情報提供者機関コード	情報提供者の機関コード
			7	事務コード	情報提供を行った事務コード
			8	事務手続コード	情報提供を行った事務手続コード
			9	情報照会条件	情報照会者が情報提供の求めを実施する際に指定する条件
			10	不開示コード	開示か不開示かを判別する
			11	不開示事由	不開示となった事由
			12	情報照会者部署名	情報照会者の部署名
			13	提供日時	情報提供があった日時
			14	特定個人情報（自己情報）名コード	特定個人情報名のコード
			15	法第21条第2項各号の該当コード	法第21条第2項各号の該当コード
			16	自己情報提供等記録ステータスコード	自己情報提供等記録の状況を示す
			17	決定通知番号	開示決定通知を一意にする番号
7	自己情報提供要求情報	自己情報の提供要求情報や提供要求条件を保管する	1	処理通番	情報ネットワークシステム全体で一意となる通番
			2	処理通番の枝番	処理通番の枝番であり、特定個人情報単位に付与する
			3	提供要求管理番号	自己情報表示業務内で提供要求を管理するために採番する番号
			4	機関一覧取得処理通番	機関別符号発行済情報保有機関リスト取得依頼時の通番（情報提供ネットワークシステムより提
			5	分野コード	指定条件入力時に分野が選択された場合に設定する
			6	分野詳細コード	指定条件入力時に分野詳細が選択された場合に設定する
			7	情報保有機関コード	指定条件入力時に情報保有機関が入力された場合に設定する
			8	自己情報処理状態コード	提供要求の状況を表すコード
			9	要求の日時	提供要求を行った日を設定する
			10	最終回答受領日	回答内容を受領した際に設定する提供の日時
			11	提供要求処理完了日時	提供要求の完了した日時を設定する
			12	任意代理人閲覧日時	任意代理人閲覧フラグが閲覧済になった日時を設定する
			13	利用者本人閲覧フラグ	利用者本人の閲覧状況を管理する
			14	任意代理人閲覧フラグ	代理人の閲覧状況を管理する
			15	代理人権限解除フラグ	代理人の権限解除を管理する
			16	電文種別コード	電文の種別を示すコード
			17	処理結果コード	処理結果を識別するコード
8	自己情報提供要求回答情報	自己情報の提供要求の回答または事後回答の通知を格納する	1	情報保有機関管理連番	情報保有機関を管理する連番
			2	特定個人情報（自己情報）	法別表第一の各項の該当情報（暗号化対象、復号済提供要求の回答情報）
			3	提供の日時	回答内容の受領日を設定する
			4	利用者本人閲覧日時	利用者本人閲覧フラグが閲覧済になった日時を設定する
9	お知らせ情報開封管理	お知らせ情報ごと利用者ごとに未読/既読を管理する	1	操作者開封フラグ	お知らせ画面に表示する「開封状態」を管理する
10	お知らせ管理情報	お知らせ情報ごとの受信情報と状態を管理する	1	お知らせ開封フラグ	情報保有機関からの「お知らせ情報状況確認」に対してお知らせ開封操作を管理する
			2	お知らせ削除フラグ	情報保有機関からの「お知らせ情報状況確認」に対してお知らせ削除操作を管理する
			3	お知らせ取消フラグ	情報保有機関からの「お知らせ情報状況確認」に対してお知らせ取消操作を管理する
			4	お知らせ保存状態コード	利用者フォルダ上限値超え等の理由で、お知らせ情報を保存できなかった状態を識別する
			5	回答方式コード	お知らせ情報の回答方式を示す
			6	回答項目数	利用者の回答で選択された項目数
			7	回答	利用者の回答
			8	回答日時	利用者が回答を実施した日時
			9	代理人フラグ	回答した者が利用者本人／任意代理人を識別する

（別添2）特定個人情報ファイル記録項目

利用者フォルダファイル(2/2)

情報名			記録項目名		説明
11	お知らせ情報	情報保有機関から送付されるお知らせ情報を管理する	1	処理通番	お知らせ情報を一意に識別する値
			2	処理通番の枝番	処理通番の付番時に特定個人情報ごとに発番される値
			3	お知らせ件名	お知らせ情報の件名
			4	お知らせ本文	お知らせ情報の本文
			5	受信日時	お知らせ情報を閲示システムが受信した日時
			6	保存期限	情報保有機関側で設定したお知らせ情報を保存する期限
			7	お知らせ容量	お知らせ本文と添付書類の合計サイズをバイト単位で格納する
			8	回答期限	情報保有機関側で設定したお知らせ情報の回答を行うことのできる期限
			9	選択項目数	情報保有機関側で設定したお知らせ情報の回答で表示する選択項目の数
			10	回答選択肢文言	情報保有機関側で設定したお知らせ情報の回答で画面表示する回答選択肢の文言
			11	本人限定フラグ	情報保有機関側で設定したお知らせ情報の回答を本人のみ実施できるお知らせかどうかを識別す
			12	回答訂正可否フラグ	情報保有機関側で設定したお知らせ情報の回答の訂正が可能かどうかを識別する
			13	破損フラグ	お知らせ情報の回答設定情報が破損しているかどうかを識別する
12	お知らせ情報添付ファイル管理情報	情報保有機関から送付されるお知らせ情報の添付ファイルを管理する	1	お知らせ連番	お知らせ情報ごとの添付ファイルを一意に識別する番号
			2	添付書類名	お知らせ情報に添付されたファイルの名称
			3	添付書類	お知らせ情報に添付されたファイルの実体
13	お知らせ情報関連ページ管理情報	情報保有機関から送付されるお知らせ情報の関連ページを管理する	1	関連ページURL	お知らせ情報に紐づけられた関連ページのURL
			2	関連ページ名称	お知らせ情報に紐づけられた関連ページへのハイパーリンク名称
14	連携先システム経由情報件名情報	APIとの連携において利用する連携先システム経由情報件名情報を管理する	1	民間送達サービス識別子	民間送達サービスを識別するID
			2	件名番号	連携先システム経由情報件名を識別する番号
			3	件名URL	連携先システム経由情報件名のURL
			4	件名	連携先システム経由情報件名
			5	開封状態	未読または既読の状態を管理する
			6	差出人	連携先システム経由情報提供機関名
			7	件名種別	連携先システム経由情報件名の種別を管理する
			8	保管期限	連携先システム経由情報件名の保管期限
			9	データ発行日	民間送達サービスが受領したお知らせ情報の発行された日付
			10	データ種別	お知らせ情報・連携先システム経由情報の種別を識別する情報
			11	連携先システム経由情報ID	連携先システム経由情報を識別するID
15	問い合わせ情報	利用者が登録した問い合わせ情報及び回答内容を管理する	1	問い合わせ日時	問い合わせの登録日時を設定する
			2	問い合わせ案件ID	問い合わせ管理機能側で付与される問い合わせごとに振られるID
			3	問い合わせ種別コード	画面上で選択された問い合わせ種別を設定する
			4	問い合わせ内容	画面上で入力された問い合わせ内容を設定する
			5	問い合わせ回答日時	問い合わせの回答を行った日時を設定する
			6	問い合わせ回答内容	問い合わせの回答を設定する
			7	問い合わせ回答保存日時	問い合わせの回答を利用者フォルダへ保存した日時を設定する
			8	問い合わせ回答開封日時	問い合わせの回答を最初に確認した日時を設定する
			9	問い合わせ開封状態コード	問い合わせの詳細表示を行ったかを判定する
16	本人同意内容	APIにおける外部ウェブサービス利用時の本人同意に係る内容を管理する	1	サービス名	外部ウェブサービスが自己情報を取得する目的（サービスの名称）
			2	本人同意内容	取得する自己情報や利用目的等、同意を取得する内容
			3	有効開始日	情報の利用が有効化される日時
			4	有効終了日	情報の利用が無効化される日時
17	本人同意結果	APIにおける本人同意の結果を管理する	1	本人同意結果	本人同意の実施結果
18	本人確認結果	APIにおける本人確認の実施結果を管理する	1	本人確認結果	本人確認の実施結果
19	情報提供事務進行状況	APIにおける自己情報・お知らせ情報・連携先システム経由情報提供状況を管理する	1	ステータス	事務の進行度合いやエラー等の発生状況を示すコード
20	取得履歴情報	APIにおける自己情報・お知らせ情報・連携先システム経由情報の取得履歴情報を管理する	1	処理結果	自己情報取得の処理結果
			2	照会日時	外部ウェブサービスから自己情報の取得依頼を受けた日時
			3	取得結果	お知らせ情報・連携先システム経由情報取得成否
			4	取得日時	お知らせ情報・連携先システム経由情報取得日時
			5	照会サービス提供者ID	照会した外部ウェブサービスを一意に識別する番号
			6	照会サービスID	照会した外部ウェブサービスが提供するサービスを一意に識別する番号
			7	提供日時	外部ウェブサービスに情報を提供した日時
			8	提供機関コード	自己情報を提供した機関の機関コード
			9	取得した特定個人情報名	自己情報で取得した対象の特定自己情報名
21	アクセストークン管理	APIが自己情報・お知らせ情報・連携先システム経由情報を提供する際に必要なアクセストークンを管理する	1	アクセストークン	自己情報・お知らせ情報取得時に利用するためのアクセストークン
			2	認可コード	アクセストークンの取得時に利用する認可コード

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

利用者フォルダファイル

※ Ⅰ 1. ②⑵の事務においては、開示システムは、外部ウェブサービスに対し、当該データの加工等を行わずにそのまま提供しているところ、当該情報に係る主なリスク対策は以下の通り。
・目的外の特定個人情報の入手・提供を防ぐため、利用者本人の本人確認を行うとともに、利用者本人の同意の下、当該情報の入手・提供を実施する。
・改ざんによる不正確な特定個人情報の入手・提供や当該情報の漏洩を防止するために、開示システムと連携先システムまたは外部ウェブサービスとの間の通信についてサーバ証明書等を用いた認証及び暗号化通信を実施する。

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	
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	[　　] ＜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	[　　] ＜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	[　　] ＜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
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		宛名システム等は存在しない。
事務で使用するその他のシステムにおける措置の内容		事務で使用するその他のシステムは存在しない。
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	・内閣府の情報システム責任者及び情報システム管理者（以下「情報システム責任者等」という。※）は、ユーザ認証の管理を委託先事業者の運用統括責任者に委任し、運用統括責任者は以下の作業を行う（以下、リスク2において同様）。 (1)ユーザアカウントを作成する。また、認証方式については、原則としてID・パスワード及びハードウェアトークンを使用した二要素認証を用いる。 (2)内閣府の情報システム責任者等及び委託先事業者の従事者個人ごとにその役割に応じた別々のユーザアカウントを割り当てる。 (3)パスワードについて、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。 (4)従事者による開示システムへのログイン状況を運用端末で確認できるようにし、従事者による不正ログインの有無を定期的に確認する。 (5)OSやデータベースで初期設定されているIDのパスワードについて、初期設定時に変更または無効化する。 (6)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機械的に制限する。 (7)開示システムにアクセスできる運用端末を制限する。 (8)なりすましによる不正を防止する観点から共有IDの利用を禁止する。 ・内閣府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ユーザアカウントの割当て状況、委託先事業者による開示システムへのログイン状況などに係る報告書の内容を随時確認するとともに、報告書等に基づいて運用統括責任者から聴取を行う。これにより、ユーザ認証の管理の適正性を評価し、必要に応じて運用統括責任者に改善を指示する。また、評価の際には必要に応じて開示システムの運用拠点への立入り検査を実施する。 ※内閣府大臣官房番号制度担当室の情報システム部門の情報システム責任者及び情報システム管理者を指す。
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	・運用統括責任者は以下の作業を行う。 (1)発効の管理 ・内閣府の情報システム責任者等及び委託先事業者の従事者の役割とアクセス権限との対応表（以下「アクセス権限対応表」という。）を作成する。 ・アクセス権限対応表に基づき、内閣府の情報システム責任者等及び委託先事業者の従事者にID及びハードウェアトークンを払い出し、その者の役割に応じたアクセス権限を持つユーザアカウントと当該ID及びハードウェアトークンとを紐づける。なお、ハードウェアトークンは運用拠点に備え付ける鍵付きの金庫に保管し、従事者等が運用拠点内での業務に従事する際に、その都度運用統括責任者が払い出す。 (2)失効の管理 ・内閣府の情報システム責任者等及び委託先事業者の従事者の異動/退職等が生じた際には、速やかにその者のユーザアカウントを消去する。なお、運用統括責任者に異動/退職等が生じた際には、後任の運用統括責任者が前任の運用統括責任者のユーザアカウントを消去する。
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	・運用統括責任者は、ID管理ソフトウェアによりユーザアカウントを管理し、システムに対するユーザIDの登録や変更、削除等の操作を行い、ユーザアカウントの不正利用をシステムで監視する。 ・内閣府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アクセス権限対応表、ユーザアカウントの割り当て状況等に係る報告書の内容を随時確認するとともに、報告書等に基づいて運用統括責任者から聴取を行う。これにより、アクセス権限の発効・失効等の管理の適正性を評価し、必要に応じて運用統括責任者に改善を指示する。また、評価の際には必要に応じて開示システムの運用拠点への立入り検査を実施する。

特定個人情報の使用の記録		[　　記録を残している　　] ＜選択肢＞ 1）記録を残している　　2）記録を残していない
	具体的な方法	・運用統括責任者は以下の作業を行う。 ⑴特定個人情報の使用の記録として、利用者フォルダファイルへアクセスするためのアカウントの払い出し状況の記録簿（以下「記録簿」という。）を作成する。記録簿には、アカウントの払い出し日時、アカウント名、アクセスする必要性等を記載し、アクセスした個人を特定できるようにする。なお、記録簿は委託事業が終了するまで保管する。 ⑵委託先事業者の従事者が運用統括責任者に提出する利用者フォルダファイルへのアクセス用アカウントの払い出しに係る申請書（以下「申請書」という。）と記録簿を突合し、アカウント払い出し状況の目視確認を実施する。 ⑶開示システムへのアクセスログ、開示システムでの操作ログの記録を行うとともに、定期的にログの分析を実施する。また、これらのログの改ざんや滅失を防止するため、不正プロセス検知ソフトウェアにより不正なログの書き込み等を検知する。 ⑷不正プロセス検知ソフトウェアにより不正なログの書き込み等が検知された場合は操作ログをチェックし、速やかに内閣府の情報システム責任者等に報告する等、必要な対応をとる。 ・内閣府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記録簿、申請書の内容を随時確認するとともに、記録簿、申請書等に基づき運用統括責任者から聴取を行う。これにより、特定個人情報の使用の記録方法の適正性を評価し、必要に応じて運用統括責任者に改善を指示する。また、評価の際には必要に応じて開示システムの運用拠点への立入り検査を実施する。
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		・内閣府の情報システム責任者等は、委託先事業者の従事者が特定個人情報を事務外で使用することがないよう、運用統括責任者に以下の作業を実施させる。 ⑴従事者に利用者フォルダファイルへのアクセス用のアカウントを払い出す際は、従事者から申請書を受領した都度アカウントを払い出し、作業終了後すぐに当該アカウントを無効とすることで、従事者が利用者フォルダファイルへアクセス可能な時間が必要最小限となるようにする。 ⑵定期的に開示システムへのアクセスログ、開示システムでの操作ログを確認し、従事者による特定個人情報の事務外での使用がないか監視する。 ⑶サーバや運用端末の置かれた部屋へのカメラ機能を持った携帯端末の持ち込み、持ち出しを物理的検査により監視し、厳重に制限する。 ⑷運用端末等に接続できるUSBメモリ等の外部記憶媒体を物理的に接続できないように制御及び管理する。また、接続を制御及び管理する為のソフトウェアを導入する。 ⑸従事者に対して個人情報保護及び情報セキュリティに関する教育を実施する。 ・内閣府の情報システム責任者等は、運用統括責任者による従事者に対する個人情報保護及び情報セキュリティに関する教育の実施結果を確認するとともに、実施結果等に基づき運用統括責任者から聴取を行う。また、必要に応じて運用統括責任者に社内教育の改善を指示する。 ・内閣府の情報セキュリティ責任者は、全職員を受講対象とした個人情報保護及び情報セキュリティに関する研修を定期的に職員に受講させ、特定個人情報の事務外での使用の禁止を徹底する。
リスクへの対策は十分か		[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
リスク4：　特定個人情報ファイルが不正に複製されるリスク		
リスクに対する措置の内容		・リスク3「リスクに対する措置の内容」の⑶⑷に加え、運用統括責任者は利用者フォルダファイルが含まれるデータベースに暗号化を施し、万が一複製されても復号できない措置を講じる。 【パブリッククラウド環境移行の際に特に想定されるリスクに対する措置】 ・運用統括責任者は、移行作業に用いる電子記録媒体について事前に内閣府の情報システム責任者等から承認を得る。電子記録媒体は暗号化したファイルを格納するとともに、電子記録媒体には追記できない状態とする。 ・運用統括責任者は、ファイルの移行後、ただちに電子記録媒体を破棄し、破棄日時・破棄方法の記録を作成する。 ・運用統括責任者は、利用者フォルダファイルにアクセスする作業は、従事者二人で行う相互牽制の体制で実施させる。 ・運用統括責任者は、定期的に開示システムの操作ログをチェックし、不正なデータ抽出等が行われていないか監視する。 ・内閣府の情報システム責任者等は、運用統括責任者から提出されるパブリッククラウド環境移行に関する報告書の内容を確認するとともに、必要に応じて委託事業者が実施する移行作業に立ち会うことにより、不正な複製が行われていないことを確認する。
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		・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。 ・委託者選定を行う際は、プライバシーマークやISMS（ISO/IEC27001）等の認証取得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	3. リスク2「アクセス権限の管理」「具体的な管理方法」の2項目目、3. リスク3「リスクに対する措置の内容」の(1) の制限に加え、情報セキュリティインシデントの発生時など、委託先事業者が利用者フォルダファイル内の特定個人情報を確認する必要が生じた場合を除き、運用端末から利用者フォルダファイルにアクセスすることを禁止する。
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	3. リスク2「特定個人情報の使用の記録」「具体的な方法」(1)～(4)と同じ。
特定個人情報の提供ルール		[　定めている　] ＜選択肢＞ 1）定めている　2）定めていない
	委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	委託先事業者から他者への特定個人情報の提供は原則禁止している。また、内閣府の情報システム責任者等が委託先事業者におけるユーザ認証、アクセス権限の管理や特定個人情報の使用の記録に関する報告書の内容を確認するとともに、報告書等に基づいて運用統括責任者から聴取を行い、必要に応じて立入り検査を実施することで、委託先事業者から他者への特定個人情報の提供がなされていないことを確認する。
	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	委託先事業者への特定個人情報の提供は行わない。
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	・ルールの内容はⅡ　6. ③と同じ。 ・ルール遵守の確認方法については、特定個人情報の消去が開示システムにより自動化されているため、委託先事業者の運用統括責任者が開示システムが正常に稼働していることを随時監視し、その監視結果に係る報告書の内容を内閣府の情報システム責任者等が確認するとともに、報告書等に基づき運用統括責任者から聴取を行い、必要に応じて立入り検査を実施することで、ルールが遵守されているか確認している。 ・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。内閣府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、報告書に基づいて運用統括責任者に聴取を行い、必要に応じて立入り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ち出し禁止 ・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または廃棄 ・従事者に対する監督・教育 ・契約内容の遵守状況について報告を求める規定 ・委託内容及び作業場所 ・管理区域等の明確化 ・漏えい、滅失、毀損、紛失及び改ざん等の防止策 ・委託先に対する実地調査 ・運用状況の記録の提供等 なお、契約書の規定の他、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、必要に応じて委託内容などの見直しを検討する。

再委託先による特定個人情報ファイルの適切な取扱いの確保		[　　十分に行っている　　] ＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない　4）再委託していない
	具体的な方法	原則として再委託は行わないこととするが、再委託を行う場合は、下記の措置を実施する。 ・再委託契約に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を盛り込む。 ・委託先事業者の運用統括責任者は、定期的または必要に応じて、再委託先事業者に作業の進捗状況等の報告を行わせる等、再委託業務の適正な履行の確保に努める。 ・内閣府の情報システム責任者等は、委託先事業者の運用統括責任者から再委託先事業者の作業状況について報告を受け、ルールが遵守されているか否かを確認する。また、必要に応じて再委託先事業者への立入り検査の実施を依頼する。
その他の措置の内容		－
リスクへの対策は十分か		[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		
－		

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	開示システムが、情報提供ネットワークシステム経由で入手する特定個人情報は原則的には機関別符号のみであり、当該情報を入手する際に利用者本人以外の機関別符号の入手を防止するため、利用者本人の本人確認を行うとともに、その際に開示システムが取得したシリアル番号（個人番号カード内に格納されている利用者証明用電子証明書のシリアル番号）を基に機関別符号の取得要求をすることにより、当該シリアル番号に紐づけられる機関別符号のみを入手する。
リスクへの対策は十分か	[　特に力を入れている　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク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	・漏えいリスクに対する措置 開示システムと情報提供ネットワークシステムとの間の通信については、政府共通ネットワークを通じて実施しているところ、リスクに対する措置については政府共通ネットワークにおけるリスク対策に依拠している。そのほか、暗号化通信も行っている。 ・紛失リスクに対する措置 機関別符号の入手については、システムにより自動化されている。 ・その他の措置 サーバ装置（仮想マシンを含む）及び運用端末には、マルウェア対策ソフトウェアを導入し、マルウェア検出用不正プログラム定義ファイル等の最新化を図るため適宜不正パターンファイルの更新を行うほか、侵入検知及び侵入防止等も実施する。
リスクへの対策は十分か	[　特に力を入れている　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3： 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	情報提供ネットワークシステムから入手する機関別符号は、政府共通ネットワークを通じて実施しているところ、リスクに対する措置については、政府共通ネットワークにおけるリスク対策に依拠している。また、入手後も加工を行っていない。
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2「リスクに対する措置の内容」と同じ。
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	
・利用者本人が偽のサイトへ誘導されることを防止するため、開示システムのサーバについてサーバ認証を実施する。 ・利用者情報の漏洩を防止するため、開示システムと利用者本人との間においてサーバ証明書を用いた暗号化通信を実施する。	

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	[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	[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	(1)パブリッククラウド環境における物理的対策 ・委託先事業者がパブリッククラウド事業者を選定する際の調達要件として、ISO/IEC27017またはCSマーク・ゴールドの認証を取得している者で、かつ、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等による各種条件を満たしている者が、物理的対策を含めたセキュリティ管理策を適切に実施していることを確認できることを定めている。 ・また、具体的な対策の内容としては、例えば、パブリッククラウド事業者は保有・管理するパブリッククラウド環境を日本国内に設置し、委託先事業者が電子錠による入退室制限等の物理的なアクセス制御手段により、パブリッククラウドの運用環境には許可された利用者のみが入退室できるようにし、監視カメラ等による入退室及び室内映像を収集し、入退室の記録を取得することとしている。 (2)オンプレミス環境における物理的対策 ・委託事業者がオンプレミス環境を構築する際の調達要件として、ISMS（情報セキュリティマネジメントシステム）の認証と同等以上の認証を取得しており、物理的対策を含めたセキュリティ管理策が適切に実施されていることが確認できることを定めている。 ・また、具体的な対策の内容としては、例えば、委託先事業者は日本国内にオンプレミス環境を設置し、委託先事業者が電子錠による入退室制限等の物理的なアクセス制御手段により、オンプレミスシステムの運用環境（データセンター等）には許可された利用者のみが入退室できるようにし、監視カメラ等による入退室及び室内映像の収集し、入退室の記録を取得することとしている。	
⑥技術的対策	[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	・利用者本人がインターネット回線を通じて開示システムにアクセスする際、個人番号カードによる本人確認を行っている。 ・クラウドマネージドサービス等を活用し、アクセス制御、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 ・クラウドマネージドサービスを利用する場合においても、パブリッククラウド事業者は個人情報にはアクセスしない。 ・オンプレミス環境においても、パブリッククラウド環境と同等の技術的対策を講ずる。 ・パブリッククラウド環境とオンプレミス環境の通信には、当該環境間のVPN接続等による通信内容の秘匿や漏洩防止が可能なパブリッククラウドサービスを使用する。 ・バックアップは地理的に十分に離れた複数の拠点に保管することで、大規模なシステム障害や震災などの発生によりデータが破損・消失しても、バックアップからデータを復元できるようにする。	
⑦バックアップ	[十分に行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
⑧事故発生時手順の策定・周知	[十分に行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	[発生なし]	<選択肢> 1）発生あり 2）発生なし
その内容	-	
再発防止策の内容	-	
⑩死者の個人番号	[保管している]	<選択肢> 1）保管している 2）保管していない
具体的な保管方法	死者の機関別符号は生存者の機関別符号と同様の保管方法により保管される。 ※死者の機関別符号を含めた特定個人情報の削除については今後検討。	
その他の措置の内容	-	
リスクへの対策は十分か	[十分である]	<選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている

リスク2： 特定個人情報が古い情報のまま保管され続けるリスク	
リスクに対する措置の内容	1　個人番号対応符号（機関別符号） 　機関別符号は原則として更新されないところ、例外的に更新される場合は、開示システムは、利用者フォルダ内に格納されている全ての利用者証明用電子証明書のシリアル番号に基づき、新しい機関別符号を取得し、既存の機関別符号と置き換えるため、古い機関別符号のまま保管されることはない。 2　その他識別情報（内部番号）（機関別符号に紐づく情報） ・利用者フォルダ番号 　利用者フォルダ開設の際のみに生成される番号であり、当該リスクは存在しない。 ・連携用ID 　認証連携を行う際のみに生成されるIDであり、当該リスクは存在しない。 3　その他（機関別符号に紐づく情報） (1)利用者情報（ニックネーム、メールアドレス等） 　利用者本人の要求のみに基づいて更新されるため、当該リスクは存在しない。 (2)代理情報 　利用者本人及び任意代理人の要求のみに基づいて更新されるため、当該リスクは存在しない。 (3)自己情報提供等記録、自己情報、お知らせ情報 　自己情報提供等記録及び自己情報は利用者本人の要求に基づき提供されるものであり、常に最新の情報が提供されることから、当該リスクは存在しない。 　また、お知らせ情報については更新されることはないため、当該リスクは存在しない。
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3： 特定個人情報が消去されずいつまでも存在するリスク	
消去手順	[　定めている　] ＜選択肢＞ 1）定めている　2）定めていない
手順の内容	・保管期間を経過した特定個人情報は開示システムにより自動的に消去される。 ※長期間利用がない（一定期間ログインがない場合など）利用者フォルダ内の特定個人情報の削除については今後検討。
その他の措置の内容	－
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置	
－	

Ⅳ　その他のリスク対策 ※

1. 監査		
①自己点検		[　　十分に行っている　　] ＜選択肢＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
	具体的なチェック方法	・内閣府の情報システム責任者等は委託先事業者を介さずに利用者フォルダファイルを取扱うことはないため、委託先事業者への監査を実施することで自己点検に代えている。
②監査		[　　十分に行っている　　] ＜選択肢＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
	具体的な内容	・内閣府の情報システム責任者等は、本評価書に記載したとおりに利用者フォルダファイルの運用がなされていることを確認するため、委託先事業者における開示システムの運用について下記の通り監査を実施する。 (1)委託先事業者におけるユーザ認証の管理、アクセス権限の管理、特定個人情報の使用の記録の管理等、利用者フォルダファイルの取扱いに関連のある事項を監査事項とする。 (2)監査は委託先事業者による開示システムの運用の履行状況に関する内閣府の情報システム責任者等への報告の内容などから、内閣府の情報システム責任者等が監査の実施が必要であると判断した際に実施する。 (3)監査責任者は内閣府の情報システム責任者とし、内閣府の情報システム管理者及び職員が監査を実施する。 (4)内閣府の情報システム責任者等は監査結果を踏まえ、委託先事業者に開示システムの運用について必要な改善を指示する。
2. 従業者に対する教育・啓発		
従業者に対する教育・啓発		[　　十分に行っている　　] ＜選択肢＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
	具体的な方法	Ⅲ　3.　リスク3　リスクに対する措置の内容の1項目目(5)、2項目目、3項目目と同じ。
3. その他のリスク対策		
―		

Ⅴ　開示請求、問合せ

1. 特定個人情報の開示・訂正・利用停止請求	
①請求先	内閣府大臣官房総務課個人情報受付窓口 住所：〒100-8914 東京都千代田区永田町1-6-1 電話番号：03-5253-2111（大代表）
②請求方法	・郵送による開示請求 ・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	利用者フォルダファイル
公表場所	・事務所への備付け ・内閣府ホームページ（https://www8.cao.go.jp/kojin-jyouhou/index.html）
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	内閣府大臣官房総務課個人情報受付窓口 住所：〒100-8914 東京都千代田区永田町1-6-1 電話番号：03-5253-2111（大代表）
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う。

Ⅵ　評価実施手続

1. 基礎項目評価	
①実施日	平成27年3月10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	
②実施日・期間	
③期間を短縮する特段の理由	
④主な意見の内容	
⑤評価書への反映	
3. 第三者点検	
①実施日	
②方法	
③結果	
4. 個人情報保護委員会の承認 【行政機関等のみ】	
①提出日	
②個人情報保護委員会による審査	

（別添3）変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明