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
37	栄養士法による栄養士資格の登録（免許）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

東京都知事は、栄養士資格の登録（免許）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、特定個人情報の漏えいその他の事態を発生させるリスクを軽減させるために適切な措置を講じることをもって、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

東京都知事

個人情報保護委員会　承認日　【行政機関等のみ】

公表日

令和6年3月21日

［平成30年５月　様式４］

項目一覧

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

Ⅰ　基本情報

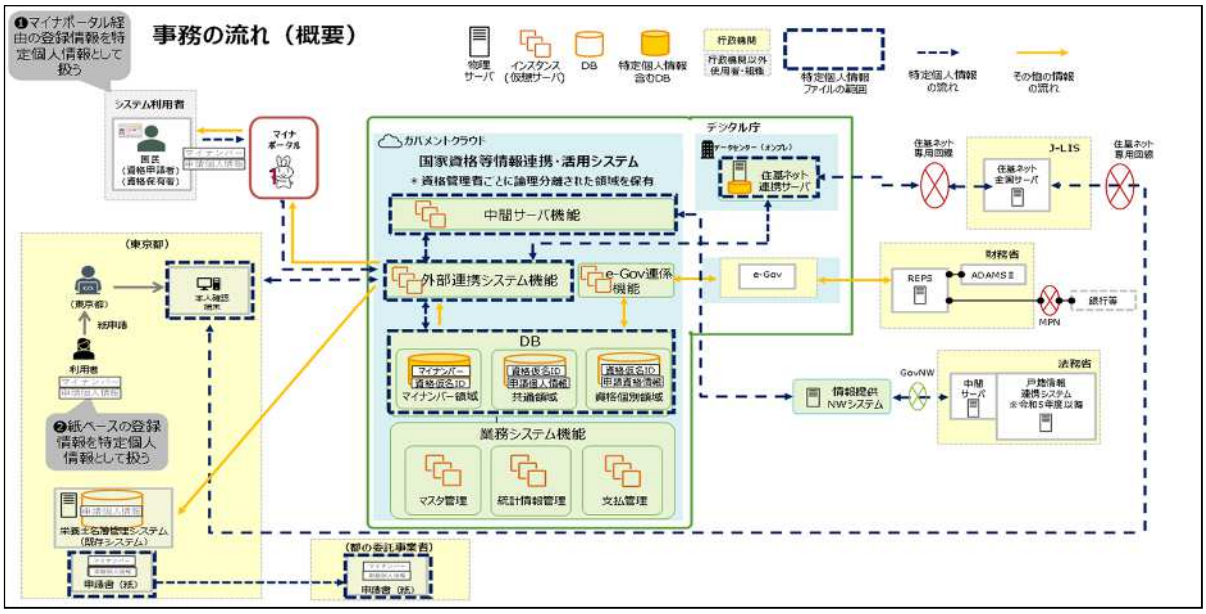
1．特定個人情報ファイルを取り扱う事務	
①事務の名称	栄養士法による栄養士資格の登録（免許）に関する事務
②事務の内容　※	■資格管理事務（特定個人情報ファイルの取扱有） i.資格情報の登録 　オンライン（マイナポータル）又は紙での申請受理後に審査を行い、資格情報の登録を行う。なお、オンライン登録の際にはマイナンバーカードの電子証明書を利用し、資格保有者本人であることを確認する。個人番号については、登録を受けようとする資格保有者のマイナンバーカードに搭載された券面事項入力補助機能を活用し、その改変を不可能ならしめることにより真正性を担保する。登録情報については、住民基本台帳法（昭和42年法律第81号。以下「住基法」という。）、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。）及び「デジタル社会の形成を図るための関係法律の整備に関する法律」に定められた範囲内において住民基本台帳ネットワークシステム、情報提供ネットワークシステムを利用した情報連携を行い、本人確認情報等の確認を行う。 ii.登録情報の訂正・変更 　オンライン（マイナポータル）又は紙での申請について、個人番号を利用し、住基法及び番号法に定められた範囲内において住民基本台帳ネットワークシステム、情報提供ネットワークシステムを利用した情報連携を行い、本人確認情報等の確認を行う。この他に住民基本台帳ネットワークシステムや情報提供ネットワークシステムにおいて、資格登録情報の更新の有無について定期に照会を行う。審査の結果、問題が無ければ結果情報を登録する。 iii.資格の停止・取り消し 　資格保有者について、資格の停止または取り消しが決定した場合、登録者名簿の資格情報を更新する。 iv.資格の削除 　オンライン（マイナポータル）又は紙での申請について、個人番号を利用し、住基法及び番号法に定められた範囲内において住民基本台帳ネットワークシステム、情報提供ネットワークシステムを利用した情報連携を行い、本人確認情報等の確認を行う。この他に住民基本台帳ネットワークシステムや情報提供ネットワークシステムにおいて、資格登録情報の更新の有無について定期に照会を行う。審査の結果、資格の削除が決定した場合、登録者名簿から削除を行う。 ■決済事務（特定個人情報ファイルの取扱無） i.決済 　資格の登録、訂正・削除などに係る費用について、オンラインにて完結可能となるよう決済処理を行う。オンライン決済を望まない利用者についてはシステムを利用せずに従来通りの現金等による手続きが可能なものとする。 ii.入出金管理 　各種申請（登録、訂正等）を完了させるためには、決済処理が完了していることが必須条件となるため、入金情報について管理する。申請の取消し、取り下げ等が発生した際に、申請者が納付すべき額を管理し、状況に応じて利用者に返金等の処理を行う。 iii.統計処理・集計処理 　任意の決済期間、決済区分で収支を集計する。 ■資格証事務（特定個人情報ファイルの取扱無） i.デジタル資格証発行（オンライン） 　資格保有者が自身の保有する資格情報を第三者へ対面で自身のスマートフォンやタブレット上に表示しデジタル資格証として提示する。また、当該資格情報をオンライン上で提供することも可能とする。 ii..資格証の発行・再発行（紙） 　資格情報の登録業務にて登録が完了した資格登録者について、資格証の作成処理を行う。再発行については、オンライン（マイナポータル）又は紙での申請を受けて、審査を行う。審査の結果、問題が無ければ資格証の作成処理を行う。 ■資格情報の既存システムとの連携（特定個人情報ファイルの取扱有） 　東京都保健医療局保健政策部健康推進課が保有する栄養士名簿管理システム（既存システム）と国家資格等情報連携・活用システムに登録された特定個人情報を含む資格情報データを連携し登録情報の同期を行い正確な資格情報の管理を行う。
③対象人数	[　10万人以上30万人未満　] ＜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

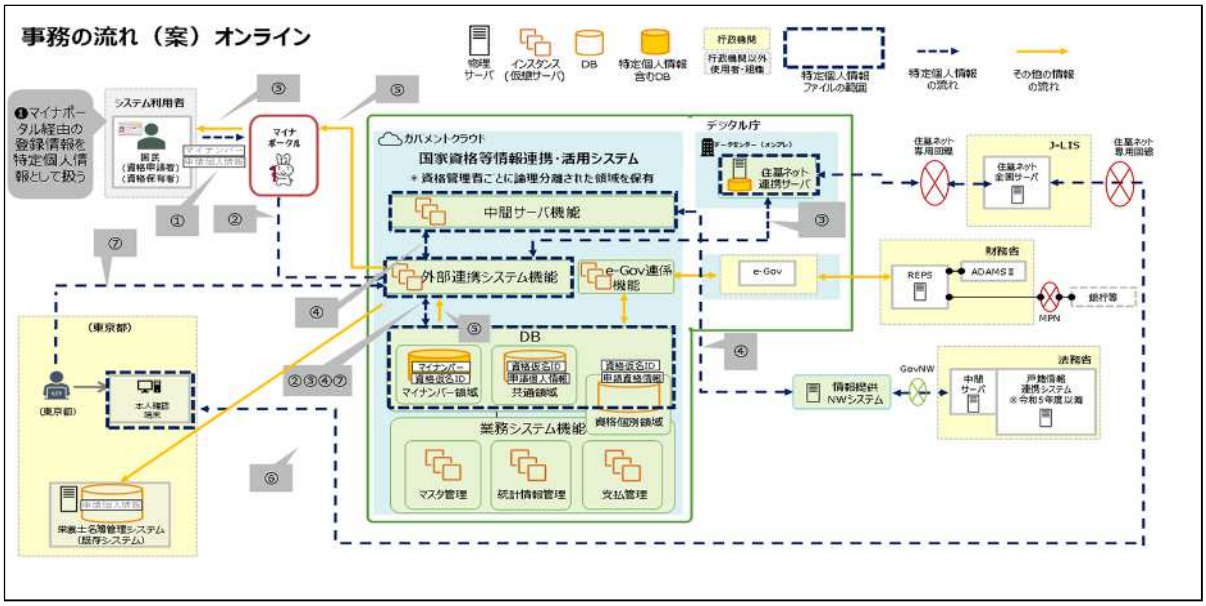
2. 特定個人情報ファイルを取り扱う事務において使用するシステム	
システム1	
①システムの名称	国家資格等情報連携・活用システム
②システムの機能	■「管理機能（データベース管理機能）」（特定個人情報ファイルの取扱有） i.資格管理者等が資格登録者名簿等をクラウド上において保存・管理等を可能とする。 ii.資格管理者等がクラウド上の資格登録者名簿等に新規データの登録や既存データの変更・抹消等を可能とする。 iii.マイナンバーを含む資格情報をデータベースとして管理する。当該データベースについては適切なアクセス権限管理により、権限を付与された限られた者のみ取扱いが可能とする。 ■「オンライン申請機能」（特定個人情報ファイルの取扱有） i.資格登録申請者等がオンラインで資格登録等の手続を行う際に、必要な情報項目の入力、文書ファイルの添付等を可能とする。 ii.資格登録申請者等がマイナンバーカードの電子署名を付与し、資格管理者等にオンラインで申請・提出を行うことを可能とする。 iii.資格管理者等はオンラインで申請等を行った資格登録申請者等の本人確認やオンライン申請の受付、申請データの受領等を可能とする。 iv.オンライン申請の際に作成されるマイナンバーを含む資格情報については国家資格等情報連携・活用システムへ連携された後にマイナポータルからは削除される。 ■「オンライン決済関連機能」（特定個人情報ファイルの取扱無） i.資格登録のオンライン手続の際に、手数料等の支払いのオンライン化等を可能とする ■「資格情報提供関連機能」（特定個人情報ファイルの取扱無） i.資格保有者がオンラインでマイナンバーカードによる本人認証・同意を行い、自己情報としての資格に関する情報を電子的な形式で取得・表示・提示等を可能とする。 ii.資格管理者等において、資格保有者がオンラインでマイナンバーカードによる本人認証・同意を行った際に電子的な形式で資格証と同等の情報を資格保有者等へ提供を可能とする。 iii.資格保有者等がオンラインでマイナンバーカードによる本人認証・同意等を行い、自己情報としての資格に関する情報を電子的な形式で第三者に提供を可能とする。 iv.資格管理者等において、資格保有者等がオンラインでマイナンバーカードによる本人認証・同意等を行った際に電子的な形式で資格証と同等の情報を第三者へ提供を可能とする。 ■「外部連携関連機能」（特定個人情報ファイルの取扱有） i.既存の資格管理者等が保有する資格登録等に関するシステムと連携を可能とする。（特定個人情報を含む資格情報のデータ連携機能） ii.その他、資格管理者以外が保有する外部システムとの連携を可能とする。 ■「住基ネット連携機能」（特定個人情報ファイルの取扱有） i.資格管理者等が住民基本台帳ネットワークシステムに個人番号を利用して照会することで、氏名、住所、性別、生年月日の本人確認情報の取得を可能とする。又本人確認情報を基にマイナンバーの取得を可能とする。 ii.資格登録申請者等はオンラインの手続の際に住民票の写しの添付省略が可能となる。 ■「中間サーバー機能（戸籍連携機能）」（特定個人情報ファイルの取扱有） i. 符号管理機能 符号管理機能は、情報照会、情報提供に用いる個人の識別子である「符号」を保管・管理する。 ii. 情報照会機能 情報照会機能は、情報提供ネットワークシステムを介して、特定個人情報（連携対象）の情報照会及び情報の受領を行う。 iii. 既存システム接続機能 中間サーバと既存システム及び住民基本台帳システム等との間で情報照会内容、情報提供内容、特定個人情報（連携対象）、符号取得のための情報等について連携する。 iv. 情報提供等記録管理機能 特定個人情報（連携対象）の照会、又は提供があった旨の情報提供等記録を管理する。 v. データ送受信機能 中間サーバと情報提供ネットワークシステム（インターフェイスシステム）との間で情報照会、符号取得のための情報等について連携する。 vi. セキュリティ管理機能 vii. 職員認証・権限管理機能 中間サーバを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報（連携対象）へのアクセス制御を行う。 viii. システム管理機能 バッチ処理の状況管理、業務統計情報の集計、稼働状態の通知、保管切れ情報の削除を行う。 ■「オンライン通知機能」（特定個人情報ファイルの取扱無） i.資格登録申請者等は申請結果等の通知をオンラインで受取りを可能とする。 ii.資格管理者等は、手続結果や各種お知らせ等をオンラインで送付可能とする。
③他のシステムとの接続	[○] 情報提供ネットワークシステム　　[　　] 庁内連携システム [○] 住民基本台帳ネットワークシステム　　[　　] 既存住民基本台帳システム [　　] 宛名システム等　　[　　] 税務システム [○] その他　（「e-Gov」、「マイナポータル」、「栄養士名簿管理システム（既存システム）」）

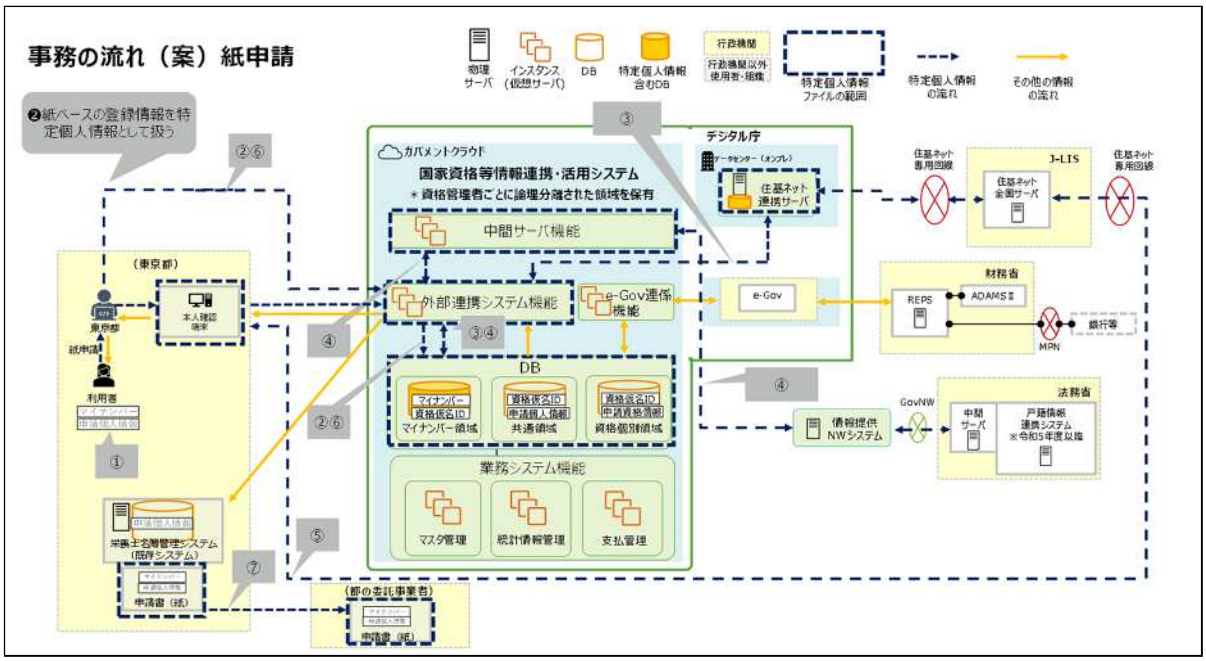
システム2～5	
システム2	
①システムの名称	住民基本台帳ネットワークシステム
②システムの機能	1. 地方公共団体情報システム機構への情報照会 住民基本台帳ネットワークシステム全国サーバに対して住民票コード、個人番号又は4情報の組合せをキーとした本人確認情報照会要求を行い、該当する個人の本人確認情報を受領する。 2. 本人確認情報検索 本人確認端末(専用端末)において入力された個人番号又は4情報(氏名、住所、性別、生年月日)の組合せをキーに本人確認情報の検索を行い、検索条件に該当する本人確認情報の一覧を画面上に表示する。
③他のシステムとの接続	[　] 情報提供ネットワークシステム　[　] 庁内連携システム [○] 住民基本台帳ネットワークシステム　[　] 既存住民基本台帳システム [　] 宛名システム等　[　] 税務システム [○] その他　(国家資格等情報連携・活用システム　)
システム3	
①システムの名称	マイナポータル(情報提供等記録開示システム)
②システムの機能	(1)申請受付機能(特定個人情報ファイルの取扱有) ・申請者が資格登録等の手続を行う際に、必要な情報項目の入力、文書ファイルの添付等を可能とする。 ・申請者がマイナンバーカードの電子署名を付与し、資格管理者等に申請・提出を行うことを可能とする。 ・資格管理者等は申請者の本人確認や申請の受付、申請データの受領等を可能とする。 (2)資格情報提供関連機能(特定個人情報ファイルの取扱無) ・資格保有者がマイナンバーカードによる本人認証・同意を行い、自己情報としての資格に関する情報を電子的な形式で取得・表示・提示等を可能とする。 ・資格管理者等において、資格保有者がマイナンバーカードによる本人認証・同意を行った際に電子的な形式で資格証と同等の情報を資格保有者等へ提供を可能とする。 ・資格保有者等がマイナンバーカードによる本人認証・同意等を行い、自己情報としての資格に関する情報を電子的な形式で第三者に提供を可能とする。 ・資格管理者等において、資格保有者等がマイナンバーカードによる本人認証・同意等を行った際に電子的な形式で資格証と同等の情報を第三者へ提供を可能とする。 (3)オンライン通知機能(特定個人情報ファイルの取扱無) ・申請者は申請結果等の通知をオンラインで受取りを可能とする。 ・資格管理者等は、手続結果や各種お知らせ等をオンラインで送付可能とする。
③他のシステムとの接続	[　] 情報提供ネットワークシステム　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[　] 既存住民基本台帳システム [　] 宛名システム等　[　] 税務システム [○] その他　(国家資格等情報連携・活用システム　)

3. 特定個人情報ファイル名	
栄養士名簿ファイル	
4. 特定個人情報ファイルを取り扱う理由	
①事務実施上の必要性	・番号法に基づく情報提供ネットワークシステムを用いた情報連携を行うためには、資格情報等を個人番号と紐付けて管理する必要がある。 ・資格保有者本人であることを正確に把握するため個人番号により基本4情報（氏名、住所、生年月日、性別）を確認する必要がある。 ・資格保有者が登録した資格情報について定期に本人確認情報（生存情報、氏名、住所など）を照会し正確な資格情報を把握し管理する必要がある。
②実現が期待されるメリット	資格保有者にとって資格取得・更新等の手続時の添付書類の省略することが可能となる他、資格管理者にとっては登録原簿の正確性を保つことが可能となる。
5. 個人番号の利用　※	
法令上の根拠	・番号法第9条第1項（利用範囲） 別表第1　項番12 ・住民基本台帳法　第30条の9（国の機関等への本人確認情報の提供） 別表第1　項番57の22
6. 情報提供ネットワークシステムによる情報連携 ※	
①実施の有無	[　　実施する　　] ＜選択肢＞ 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	・番号法第19条第8号（特定個人情報の提供の制限） 別表第2　項番21
7. 評価実施機関における担当部署	
①部署	東京都保健医療局保健政策部健康推進課
②所属長の役職名	健康推進課長
8. 他の評価実施機関	
－	

（別添1）事務の内容


事務の流れ（概要）
❶マイナポータル経由の登録情報を特定個人情報として扱う
❷紙ベースの登録情報を特定個人情報として扱う
システム利用者
国民（資格申請者）（資格保有者）
マイナポータル
（東京都）
本人確認端末
紙申請
利用者
業務主名簿管理システム（既存システム）
申請書（紙）
（都の委託事業者）
申請書（紙）
カバメントクラウド
国家資格等情報連携・活用システム
＊資格管理者ごとに論理分離された領域を保有
中間サーバ機能
外部連携システム機能
e-Gov連携機能
DB
マイナンバー領域
共通領域
資格個別領域
業務システム機能
マスタ管理
統計情報管理
支払管理
デジタル庁
住基ネット連携サーバ
e-Gov
住基ネット専用回線
J-LIS
住基ネット全国サーバ
財務省
REPS
ADAMS Ⅱ
MPN
銀行等
GovNW
情報提供NWシステム
法務省
中間サーバ
戸籍情報連携システム
※令和5年度以降
物理サーバ
インスタンス（仮想サーバ）
DB
特定個人情報含むDB
行政機関
行政機関以外使用者・組織
特定個人情報ファイルの範囲
特定個人情報の流れ
その他の情報の流れ


事務の流れ（案）オンライン
❶マイナポータル経由の登録情報を特定個人情報として扱う
システム利用者
国民（資格申請者）（資格保有者）
マイナポータル
（東京都）
本人確認端末
業務主名簿管理システム（既存システム）
カバメントクラウド
国家資格等情報連携・活用システム
＊資格管理者ごとに論理分離された領域を保有
中間サーバ機能
外部連携システム機能
e-Gov連携機能
DB
マイナンバー領域
共通領域
資格個別領域
業務システム機能
マスタ管理
統計情報管理
支払管理
デジタル庁
住基ネット連携サーバ
e-Gov
住基ネット専用回線
J-LIS
住基ネット全国サーバ
財務省
REPS
ADAMS Ⅱ
MPN
銀行等
GovNW
情報提供NWシステム
法務省
中間サーバ
戸籍情報連携システム
※令和5年度以降
物理サーバ
インスタンス（仮想サーバ）
DB
特定個人情報含むDB
行政機関
行政機関以外使用者・組織
特定個人情報ファイルの範囲
特定個人情報の流れ
その他の情報の流れ


事務の流れ（案）紙申請
❷紙ベースの登録情報を特定個人情報として扱う
（東京都）
本人確認端末
紙申請
利用者
業務主名簿管理システム（既存システム）
申請書（紙）
（都の委託事業者）
申請書（紙）
カバメントクラウド
国家資格等情報連携・活用システム
＊資格管理者ごとに論理分離された領域を保有
中間サーバ機能
外部連携システム機能
e-Gov連携機能
DB
マイナンバー領域
共通領域
資格個別領域
業務システム機能
マスタ管理
統計情報管理
支払管理
デジタル庁
住基ネット連携サーバ
e-Gov
住基ネット専用回線
J-LIS
住基ネット全国サーバ
財務省
REPS
ADAMS Ⅱ
MPN
銀行等
GovNW
情報提供NWシステム
法務省
中間サーバ
戸籍情報連携システム
※令和5年度以降
物理サーバ
インスタンス（仮想サーバ）
DB
特定個人情報含むDB
行政機関
行政機関以外使用者・組織
特定個人情報ファイルの範囲
特定個人情報の流れ
その他の情報の流れ

【事務の流れ】

■資格管理事務（マイナンバー 利用有）
・資格情報の登録
オンライン（マイナポータル）もしくは紙での申請受理後に審査を行い、資格情報の登録を行う。
・登録情報の訂正・変更
オンライン（マイナポータル）もしくは紙での申請の他に住民基本台帳ネットワークシステムや中間サーバーにおいて、資格登録情報の更新の有無について定期に照会を行う。審査の結果、問題が無ければ結果情報を登録する。
・資格の停止・取消し
資格保有者について資格の停止または取り消しが決定した場合、登録者名簿の資格情報を更新する。
・資格の削除
オンライン（マイナポータル）もしくは紙での申請の他に、住民基本台帳ネットワークシステムや中間サーバーでの資格登録情報の更新の有無について定期に照会を行う。審査の結果、資格の削除が決定した場合、登録者名簿から削除を行う。

■決済事務（マイナンバー利用無し）
・決済
資格の登録、訂正・削除などに係る費用について、オンラインにて支払可能となるよう決済処理を行う。オンライン決済を望まない利用者についてはシステムを利用せずに従来通りの収入印紙等による手続きが可能なものとする。
・入出金管理
各種申請（登録、訂正等）を完了させるためには、決済処理が完了していることが必須条件となるため、入金情報について管理する。申請の取消し、取り下げ等が発生した際に、申請者が納付すべき額を管理し、状況に応じて利用者に返金等の処理を行う。
・統計処理・集計処理
任意の決済期間、決済区分で収支を集計する。

■資格証事務（マイナンバー利用無し）
・デジタル資格証発行（オンライン）
資格保有者が自身の保有する資格情報を台帳へ対面で自身のスマホやタブレット上に表示しデジタル資格証として提示する。よ、、当該資格情報をオンライン上で提供することも可能とする。
・資格証の発行・再発行（紙）
資格情報の登録業務にて登録が完了した資格登録者について、資格証の作成処理を行う。再発行については、オンライン（マイナポータル）もしくは紙での申請を受けて、審査を行う。審査の結果、問題が無ければ資格証の作成処理を行う。

【特定個人情報の流れ】

■オンライン申請の場合
①申請者がマイナポータルにログイン後、マイナンバーカードの電子証明書を利用し、資格保有者本人であることを確認する。
②入力された資格情報（マイナンバー含む）は外部連携システムと連携し、資格登録情報として国家資格管理システムに登録される。
③資格登録情報は、住民基本台帳法（昭和42年法律第81号）（以下、「住基法」という。）に定められた範囲内において一括方式による住民基本台帳ネットワークシステムを利用した情報連携を行い、本人確認情報等の確認を行う。
また、住民基本台帳ネットワークシステムに対して定期に実施する照会処理により取得した照会結果を連携をすることで正確な資格情報を把握することができる。
④資格登録情報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（平成25年法律第27号）（以下、「番号法」という。）に定められた範囲内において情報提供ネットワークシステムを利用した情報連携を行い、本籍情報の確認を行う。また、情報提供ネットワークシステムに対して定期に実施する照会処理により取得した照会結果を連携することで正確な資格情報を把握することができる。
⑤資格登録情報はマイナポータルより取得することができる。
⑥資格管理者は資格登録情報について必要がある場合、本人確認端末（住基ネット専用端末）を用いて即時方式により本人確認情報の確認を行う。
⑦即時方式により確認を行った本人確認情報について、直接国家資格管理システムに登録（更新）を行う。

■紙による申請の場合
①紙の申請書において申請者が提出した資格情報について、資格保有者本人であることの確認及びマイナンバーの確認を行う。
②申請された資格情報（マイナンバー含む）は外部連携システム機能と連携し、直接国家資格管理システムに登録を行う。
③登録された情報については、住基法に定められた範囲内において一括方式による住民基本台帳ネットワークシステムを利用した情報連携を行い、本人確認情報等の確認を行う。また、外部連携システムにおいて住民基本台帳ネットワークシステムに対して定期に実施する照会処理により取得した照会結果を連携をすることで正確な資格情報を把握することができる。
④登録された資格情報は番号法に定められた範囲内において情報提供ネットワークシステムを利用した情報連携を行い、本籍情報の確認を行う。また、情報提供ネットワークシステムに対して定期に実施する照会処理により取得した照会結果を連携することで正確な資格情報を把握することができる。
⑤資格管理者は登録された資格情報について必要がある場合、本人確認端末（住基ネット専用端末）を用いて即時方式により本人確認情報の確認を行う。
⑥即時方式により確認を行った本人確認情報について、直接国家資格管理システムに登録（更新）を行う。
⑦事務処理が完了した申請書類は、都の委託事業者において保管し、保存期間を満了した申請書類は溶解処理により廃棄する。

注１）外部連携システムを介して連携された資格情報のうち、マイナンバーは資格情報と直接紐づけるのではなく、資格仮名IDと呼ばれる資格保有者等を一意に識別するためのID情報と一度紐づけた後に、資格情報と紐づける。
マイナンバーと資格仮名IDを結びつけるテーブルは、他のテーブルとは独立して設ける。
注２）戸籍情報については国家資格管理システムに設置する中間サーバー機能において情報提供ネットワークシステムを介して連携し取得する。戸籍情報の要求についてはマイナンバーと紐付く機関別符号を用いて行う。

（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		
栄養士名簿ファイル		
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		[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
③対象となる本人の範囲　※		栄養士資格の登録者
	その必要性	資格保有者が本人の資格情報を登録することにより、資格登録原簿の正確な管理を行うため。また、必要な者には当該登録によりデジタル資格証の発行を行い、必要な時に提示、提供を行うため。
④記録される項目		[　10項目以上50項目未満　] ＜選択肢＞ 1）10項目未満　2）10項目以上50項目未満 3）50項目以上100項目未満　4）100項目以上
	主な記録項目　※	・識別情報 [○] 個人番号　[　] 個人番号対応符号　[　] その他識別情報（内部番号） ・連絡先等情報 [○] 4情報（氏名、性別、生年月日、住所）　[　] 連絡先（電話番号等） [　] その他住民票関係情報 ・業務関係情報 [　] 国税関係情報　[　] 地方税関係情報　[　] 健康・医療関係情報 [　] 医療保険関係情報　[　] 児童福祉・子育て関係情報　[　] 障害者福祉関係情報 [　] 生活保護・社会福祉関係情報　[　] 介護・高齢者福祉関係情報 [　] 雇用・労働関係情報　[　] 年金関係情報　[　] 学校・教育関係情報 [　] 災害関係情報 [○] その他　（　資格情報（登録番号、登録年月日、養成施設卒業年月日、免許の取消・停止の処分に関する事項、証の書き換え交付・再交付・抹消の理由・年月日）、本籍地都道府県名、資格仮名ID,マイナポータル仮名ID　）
	その妥当性	住基法、番号法及び「デジタル社会の形成を図るための関係法律の整備に関する法律」に定められた範囲内において、本人を正確に特定し、住民基本台帳ネットワークシステム及び情報提供ネットワークシステムを使用して特定個人情報を取得するため。本人確認情報の定期的な照会を行うことで正確な資格情報を保有することができる。
	全ての記録項目	別添2を参照。
⑤保有開始日		デジタル社会の形成を図るための関係法律の整備に関する法律（令和3年法律第37号）の公布の日から起算して四年を超えない範囲内において政令で定める日
⑥事務担当部署		東京都保健医療局保健政策部健康推進課

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 （ 地方公共団情報システム機構、法務省 ） [○] 地方公共団体・地方独立行政法人 （ 都道府県・保健所（本人から入手する際の経由機関として記載） ） [ ] 民間事業者 （ ） [ ] その他 （ ）
②入手方法		[○] 紙 [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 電子メール [○] 専用線 [ ] 庁内連携システム [○] 情報提供ネットワークシステム [ ] その他 （ ）
③入手の時期・頻度		・資格取得、資格更新、登録情報の訂正時に都度、特定個人情報を入手する。 ・定期の住民基本台帳ネットワークシステム、情報提供ネットワークシステムへの情報照会実施の都度、特定個人情報を入手する。
④入手に係る妥当性		・資格登録者の管理を適正に行うために、最新の情報を入手する必要がある。 ・死亡等の事由により、資格情報の抹消処理を行う必要がある。
⑤本人への明示		・番号法第9条第1項　別表第1の13の項に該当しており、番号法により明示されている。 ・資格保有者からの申請に合わせて本人から入手する。
⑥使用目的 ※		資格登録者の適切な管理を行うため。
	変更の妥当性	-
⑦使用の主体	使用部署 ※	東京都保健医療局保健政策部健康推進課
	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 ※		・個人番号は、資格保有者からの申請を受けて、資格情報の登録・変更・抹消を行う際に、本人を特定するために使用する。 ・申請情報の内容確認のために、住民基本台帳ネットワークシステム、情報提供ネットワークシステムを利用した情報連携を行う。
	情報の突合 ※	本人からの申請内容（登録、変更、抹消）について、システムにおける登録情報と突合する。
	情報の統計分析 ※	特定個人情報を用いた統計分析は行わない。
	権利利益に影響を与え得る決定 ※	該当なし
⑨使用開始日		令和6年12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 （ 2 ）件
委託事項1		システムの運用等業務
①委託内容		国家資格等情報連携・活用システム運用環境に係るシステムの運用保守等業務 （委託主体：国）
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	[10万人以上100万人未満] ＜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 ※	栄養士資格の登録者
	その妥当性	システム全体に係る運用保守を適切に実施するためには、専門的かつ高度な知識・技術を要することから全体の取扱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 （ システム直接操作 ）
⑤委託先名の確認方法		委託業務の調達結果については官報公示及びホームページ公表により確認可能
⑥委託先名		＊調達結果が判明次第お示しする。
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	委託先は、受託業務の全部又は一部を第三者に委託することはできない。ただし、受託者があらかじめ書面により再委託の申請を行い、委託者が承認した場合にはこの限りではない。 委託先が、本業務の一部について再委託の承認を求める場合は、以下の（イ）から（ニ）に示す事項を記載した再委託承認申請書を提出するとともに、（ホ）及び（ヘ）を記載した文書、再委託に係る履行体制図についても併せて提出することとしている。 （イ）再委託先名称（商号）、住所 （ロ）再委託する業務の範囲、再委託の必要性及び再委託予定金額 （ハ）再委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報 （ニ）その他委託者が求める情報 （ホ）受託者と同等のセキュリティ水準を再委託先も具備すべきことを受託者との間に定めている内容 （ヘ）再委託先の情報セキュリティに関する対策方針及び管理方法 また、委託先は、委託者が再委託を承認した場合であっても、委託先から業務の再委託を受けた事業者が行った作業について、全責任を負うものとする。
	⑨再委託事項	上記「委託事項」に記載する業務の一部を再委託する。

委託事項2～5		
委託事項2		特定個人情報に係る文書の保管・廃棄委託
①委託内容		処理の完了した個人番号が記載された申請書類等を保管・管理し、保存期間を経過した書類を溶解処理等により廃棄する。
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの一部]　＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	[　10万人以上100万人未満　]　＜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　※	資格取得、資格更新、登録情報の訂正等を書面で申請する申請者
	その妥当性	個人番号に係る申請書類等の保管・管理及び廃棄を適切に行うため、専用の業者に特定個人情報を提供する必要がある。
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		東京都公式ホームページの入札情報サービスにおいて公表する。
⑥委託先名		＊調達結果が判明次第お示しする。
再委託	⑦再委託の有無　※	[　再委託しない　]　＜選択肢＞ 1）再委託する　2）再委託しない
	⑧再委託の許諾方法	
	⑨再委託事項	

5. 特定個人情報の提供・移転（委託に伴うものを除く。）	
提供・移転の有無	[　] 提供を行っている　（　　）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	
移転先1	
①法令上の根拠	
②移転先における用途	
③移転する情報	
④移転する情報の対象となる本人の数	[　　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤移転する情報の対象となる本人の範囲	
⑥移転方法	[　] 庁内連携システム　[　] 専用線 [　] 電子メール　[　] 電子記録媒体（フラッシュメモリを除く。） [　] フラッシュメモリ　[　] 紙 [　] その他　（　　）
⑦時期・頻度	

6. 特定個人情報の保管・消去

①保管場所 ※		【国家資格等情報連携・活用システムに係る部分】 イ） クラウドサービスに係る要件は、主に次を満たすものとする。 ・政府情報システムのためのセキュリティ評価制度（ISMAP）において登録されたサービスか、ISO/IEC27017:2015又はCSマーク・ゴールドのいずれかの認証を取得していること。 ・十分な稼働実績を有し、運用の自動化、サービスの高度化、情報セキュリティの強化、新機能の追加等に対し積極的かつ継続的な投資が行われ、サービス提供期間中に中断するリスクに対して十分な対策が講じられているサービスであること。 ・契約者がサービスを利用して情報資産を管理する領域について、当該契約者以外の者が接続できないように通信制御がされ、資源を専有できるように構成したものであること。 ・情報資産を管理するデータセンターの物理的所在地が日本国内であること。 ・法令や規則に従って、クラウドサービス上の記録を保護すること。 ・上記のほか、「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こと。 ロ)オンプレミス環境においては、入退室制限等の物理的なアクセス制御手段により、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を収集し、入退室の記録を取得することとしている。 ハ） 電子記録媒体は、適切に管理された鍵にて施錠可能な場所に保管し、利用の際には都度、媒体管理簿に記入する。 ニ） 電子記録媒体は、情報の暗号化を行うとともに、管理区域内から管理区域外、又は管理区域外から管理区域内への移動の際は、施錠可能な衝撃防止ケースに入れて持ち運びを行う。 【申請書類】 申請書類はキャビネットにおいて施錠保管を行っている。
②保管期間	期間	［　定められていない　］ ＜選択肢＞ 1）1年未満　2）1年　3）2年 4）3年　5）4年　6）5年 7）6年以上10年未満　8）10年以上20年未満　9）20年以上 10）定められていない
	その妥当性	資格名簿に登録がある限り原則として保有し続ける
③消去方法		【国家資格等情報連携・活用システムに係る部分】 イ） 国家資格管理事務に係る資格情報等は、資格情報等の抹消申請、行政処分又は死亡により資格が喪失となった者の個人番号を含む資格情報等も適切に管理することとする。 ロ） システムから消去を行う際には、適切に消去等を行い、消去等に係る記録を作成し、管理する。 「オンプレミス環境の場合」 ハ） 特定個人情報等が記録された機器を廃棄する場合、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。 ニ） 特定個人情報等が記録された電子記録媒体等を廃棄する場合、物理的な破壊等によりデータを復元できないよう完全に消去するとともに、消去証明書を提出させる。 「クラウド環境の場合」 ホ） 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ISO/IEC27001に準拠した廃棄プロセスを確保していること。 ヘ） 廃棄プロセスの適切な実施について、第三者の監査機関による監査を受け、その内容を確認できること。 【申請書類】 ・保存期間を満了した申請書類については、溶解処理により廃棄している。 ・なお、廃棄に当たっては、仕様書により、委託先により①廃棄文書の回収の際、受託者の社員であることの身分証明書を常時携帯させ、委託者の求めに応じて提示させること、②廃棄文書の飛散・盗難防止のため、施錠又は特殊警報装置等を装備した車両を使用すること、③作業中に車両を離れる場合は、施錠し、又は監視員を配置すること、④廃棄文書が収納された箱を開封することなく、受託者の監視下に置いて回収運搬・溶解処理を行うこと、⑤溶解処理については、荷下ろしから溶解までの録画やモニター監視、不審者の侵入防止のための入退室管理や監視カメラの設置等の安全対策が講じられている施設に搬入し、処理すること及び⑥委託者に溶解処理証明書を提出することを義務付けている。

7. 備考

-

（別添２）特定個人情報ファイル記録項目

1　保有者ID
2　収受日
3　交付方法
4　申請区分
5　発行年月日
6　登録年月日
7　登録番号
8　登録種別（試験合格／養成施設卒業）
9　資格取得年月（試験合格年月／養成施設卒業年月）
10　氏名（姓）
11　氏名（名）
12　カナ氏名（姓）
13　カナ氏名（名）
14　旧姓（姓）
15　通称名（姓）
16　通称名（名）
17　本籍地都道府県又は国籍
18　性別
19　生年月日
20　理由（数値：結婚、離婚、転籍、紛失、死亡、失踪など）
21　備考（外字登録など）

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	
管理栄養士名簿ファイル	
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	【オンライン申請からの入手】 申請機能による入手では、あらかじめマイナポータルにおいて、マイナンバーカード及びパスワード入力による本人確認を完了した後に行うため、対象者以外の情報を入手することはない。 【窓口等における紙での申請からの入手】 ・入手時に本人確認措置を実施するため、対象者以外の情報を入手することはない。 【地方公共団体情報システム機構からの入手】 ①国家資格等情報連携・活用システムから入手する場合 ・オンライン申請の場合、マイナポータルにおいて入手した対象者情報に基づき処理を行うため、対象者以外の情報を入手することはない。 ・窓口等における紙での申請の場合、本人確認措置を実施し、当該対象者の情報について処理を行うため、対象者以外の情報を入手することはない。 ・処理については定期に照会処理の記録を確認し、申請情報について対象者以外の情報が取り扱われてないことの確認を行うため、対象者以外の情報を入手することはない。 ②本人確認端末（専用端末）から入手する場合 ・オンライン申請の場合、マイナポータルにおいて入手した対象者情報に基づき処理を行うため、対象者以外の情報を入手することはない。 ・窓口等における紙での申請の場合、本人確認措置を実施し、当該対象者の情報について処理を行うため、対象者以外の情報を入手することはない。 ・本人確認端末（専用端末）は、権限のある者のみ処理を行うことができる。また、当該処理については定期に照会処理の記録を確認し、提出された申請情報について対象者以外の情報が取り扱われてないことの確認を行うため、対象者以外の情報を入手することはない。
必要な情報以外を入手することを防止するための措置の内容	【オンライン申請からの入手】 申請機能による入手は、必要最小限の情報だけを入手できるように決められたインターフェースを用意し入手することにより、必要な情報以外を入手することを防止している。 【窓口等における紙での申請からの入手】 申請書の様式は定められている。様式に沿って記入することにより必要な情報のみ入手することができる。申請を受け付けする際は、本人確認により対象者を確認し、申請に必要な情報のみを記載するよう説明及び確認を行うことにより必要な情報以外を入手することを防止している。 【地方公共団体情報システム機構からの入手】 ①国家資格等情報連携・活用システムから入手する場合 システムにおいて、決められた形式による照会対象ファイルを作成し処理を行うことにより必要な情報以外を入手することを防止している。 ②本人確認端末（専用端末）から入手する場合 専用端末において、権限のある者のみ処理を行うことができる。また、必要な情報のみ取得できるようにシステムにて制御を行う。
その他の措置の内容	-
リスクへの対策は十分か	[　　十分である　　]　＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
リスク2：　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	【オンライン申請からの入手】 マイナポータルの申請情報登録画面を通じてシステムへ登録されるため、自らの操作により特定個人情報を入手することはなく、不適切な方法では情報を入手できない。 【窓口等における紙での申請からの入手】 ・窓口等において申請を受け付けする際は、本人確認により対象者を確認し、本人の申請に必要な情報のみを記載するよう説明及び確認を行っており、不適切な方法では情報を入手できない。 【地方公共団体情報システム機構からの入手】 ①国家資格等情報連携・活用システムから入手する場合 入手した情報はシステムにおいて処理されるため、自らの操作により特定個人情報を入手することはなく、不適切な方法では情報を入手できない。 ②本人確認端末（専用端末）から入手する場合 オンライン（マイナポータル）又は窓口において本人確認措置を実施し、当該対象者の情報について処理を行う。専用端末において、権限のある者のみ処理を行うことができる。また、当該処理については定期に照会処理の記録を確認し、不適切な方法で情報が入手されてないことの確認を行う。
リスクへの対策は十分か	[　　十分である　　]　＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている

リスク3： 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	【オンライン申請からの入手】 マイナポータルにおいて、マイナンバーカード及びパスワード入力により本人確認を行う。 【窓口等における紙での申請からの入手】 窓口等において申請を受け付ける場合は、原則、本人のマイナンバーカード（番号確認と身元確認）、個人番号の記載された住民票の写しなど（番号確認）と運転免許証など（身元確認）のいずれかの方法で確認する。 【地方公共団体情報システム機構からの入手】 地方公共団体情報システム機構からの入手にあっては、番号法の規定に基づき地方公共団体情報システム機構が個人番号を生成しており、個人番号が本人の情報であることは担保されている。
個人番号の真正性確認の措置の内容	【オンライン申請からの入手】 マイナポータルにおいて、マイナンバーカード及びパスワード入力による本人確認及び真正性確認を行う。 登録を受けようとする申請者のマイナンバーカードに搭載された券面事項入力補助機能を活用することで、その改変を不可能ならしめることにより真正性を担保する。 登録後においても、システムから住民基本台帳ネットワークシステムへの照会による本人確認を定期に実施する。 【窓口等における紙での申請からの入手】 窓口等において申請を受け付ける場合はマイナンバーカードと身分証明書の提示等で、本人確認を実施し、個人番号の真正性確認を行う。 【地方公共団体情報システム機構からの入手】 地方公共団体情報システム機構からの入手にあっては、番号法の規定に基づき地方公共団体情報システム機構が個人番号を生成しており、個人番号が本人の情報であることは担保されている。
特定個人情報の正確性確保の措置の内容	【オンライン申請からの入手】 申請者が登録画面により入力した情報から特定個人情報ファイルを作成し、管理する。情報管理に当たっては、住民基本台帳ネットワークシステムへの照会による本人確認を行い、正確性を担保する。 【窓口等における紙での申請からの入手】 情報管理に当たっては、申請された情報から特定個人情報ファイルを作成し、管理する。また、住民基本台帳ネットワークシステムへの照会による本人確認を行い、正確性を担保する。 【地方公共団体情報システム機構からの入手】 地方公共団体情報システム機構からの入手にあっては、番号法の規定に基づき地方公共団体情報システム機構が個人番号を生成しており、当該個人番号の正確性については地方公共団体情報システム機構において担保されている。
その他の措置の内容	-
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	【オンライン申請からの入手】 本人からマイナポータル経由でシステムへ登録情報等を登録するが、当該通信は、TSL/SSLによる暗号化された通信経路を使用することで漏えい・紛失を防止する。 ※マイナポータル内に情報等は保管されない。 登録画面により入手する情報等は、専用線によりシステムへ登録されることで、漏えい・紛失することを防止している。 【窓口等における紙での申請からの入手】 窓口において申請を受け付ける場合、紙媒体の資料は、速やかに保管場所で施錠管理等を行う。鍵は内部職員のみが知る場所で保管することにより、漏えいや紛失を防止する。また、郵送については、原則として、厳封封筒による郵送や、簡易書留等の追跡可能な郵送手段により漏えい・紛失を防止する。 【地方公共団体情報システム機構からの入手】 ①国家資格等情報連携・活用システムから入手する場合 地方公共団体情報システム機構との接続においては通信の暗号化等の高度なセキュリティを維持した専用回線を利用することで機密性を確保している。 ②本人確認端末（専用端末）から入手する場合 本人確認情報については、専用端末において権限のある者のみ処理を行うことができる。また通信の暗号化等の高度なセキュリティを維持した専用回線を利用することで機密性を確保している。
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		個人番号と直接紐付く情報は必要最低限の情報のみとし他の領域とは別で管理する。またシステム的にアクセス制御を行うことにより、目的を超えて個人番号及び機関別符号と個人情報が紐付かない仕組みとしている。
事務で使用するその他のシステムにおける措置の内容		システム的に以下のアクセス制御等の措置を講じることにより、個人番号が他の事務システム等と紐付かない仕組みとしている。 ・オンライン申請による入手に当たり、マイナポータルの登録画面から連携され、システムへ登録される。申請情報等は、マイナポータルに保管されない。 ・申請者が登録情報を確認する際は、マイナポータルから確認を行うこととなるが、どの利用者が申請を行ったかを識別するための固有の識別子である仮名を用いて、情報を紐付けて確認する。なお、マイナポータルにおいては、個人番号と仮名を紐付けず、個人番号へはアクセスできない仕組みとしている。 ・住民基本台帳ネットワークシステムと連携を行う住基連携サーバーについては、国家資格等情報連携・活用システムとのみ接続し、その他のシステムとは接続しない。また、権限を有する者のみアクセスができるようユーザ管理を行う。 ・住民基本台帳ネットワークシステムとの連携については専用端末（本人確認端末）においてのみ行い、システム操作を行う前にログイン操作を行う操作者認証を行う。
その他の措置の内容		-
リスクへの対策は十分か		［　　十分である　　］　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2： 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	【国家資格等情報連携・活用システムに係る部分】 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、「国家資格等情報連携・活用システム運用環境に係るシステムの運用保守等業務の委託先事業者」（以下「委託先事業者」という。）から払い出される管理者権限を有するアカウントに係るID及びパスワードを管理する。委託先事業者は以下の作業を行う（以下、リスク2において同様）。 (1)情報システム責任者等ごとにその役割に応じた別々の管理者ユーザーアカウントを割り当てる。 (2)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。 情報システム責任者等は以下の作業を行う。 (1)従事者用ユーザーアカウントを作成する。認証方式については、原則としてIDとパスワードを用いた認証方法とする。 (2)従事者ごとにそれぞれの役割に応じた別々の従事者用ユーザー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)従事者による国家資格等情報連携・活用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する。 (5)従事者による不正ログインの有無を定期的に確認することにより、ユーザー認証の管理の適正性を確認し、必要に応じて運用状況の改善を行う。 (6)国家資格等情報連携・活用システムにアクセスできる端末を制限する。 (7)なりすましによる不正を防止する観点から、IDの払出状況について名簿管理を行い不正な利用がなされていないことの確認を行う。 (8)従事者が利用する端末のOS等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。 ※栄養士（各資格管理者）の情報システム責任者及び情報システム管理者を指す。 【住基連携サーバー及び本人確認端末（専用端末）に係る部分】 ・システム操作や特定個人情報等へのアクセスを行う前にログイン操作を行い、操作者を認証するようシステムで制御している。 ・システムへアクセスできる者を特定し、必要最小限度の範囲でのみ特定個人情報を取り扱うことができるように利用者ごとにIDを割り当てる。 ・なりすましによる不正を防止する観点から、共用IDの利用を禁止する。

アクセス権限の発効・失効の管理		[　行っている　] ＜選択肢＞ 1) 行っている　2) 行っていない
	具体的な管理方法	【国家資格等情報連携・活用システムに係る部分】 情報システム責任者等は以下の作業を行う。 (1)発行の管理 ・情報システム責任者等及び事務従事者ユーザーの役割とアクセス権限との対応表を作成する。 ・事務従事者用ユーザーアカウントは、情報システム責任者等に対してユーザ登録を事前申請した者に限定して発行される。 ・情報システム責任者等はそれぞれの従事者ごとにそれぞれの役割に応じた別々のユーザーアカウントを割り当てる。 (2)失効の管理 ・情報システム責任者等及び事務従事者の異動/退職等が生じた際には、速やかにその者のユーザーアカウントを消去する。 【住基連携サーバー及び本人確認端末(専用端末)に係る部分】 (1)発行の管理 ・アクセス権限の管理は、情報システム責任者等が作成するアクセス権限と事務の対応表により適正に行う。 ・事務に必要なアクセス権限を情報システム責任者等に対して申請した者に限定して発行する。 ・情報システム責任者等はそれぞれの役割に応じた別々のユーザーアカウントを割り当てる。 (2)失効の管理 ・情報システム責任者等及びユーザーアカウントを割り当てられた者に異動/退職等が生じた際には、速やかにその者のユーザー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	【国家資格等情報連携・活用システムに係る部分】 情報システム責任者等は以下のとおりアクセス権限の管理を行う。 ・国家資格等情報連携・活用システムへのログイン用のユーザーIDは、情報システム責任者等に対してユーザー登録申請を事前申請した者に限定して発行される。 　情報システム責任者等はそれぞれの従事者ごとにそれぞれの役割に応じた別々のユーザーアカウントを割り当てる。 ・情報システム責任者等は、事務従事者に係るユーザーアカウントの割り当て状況等を随時確認するとともに、必要に応じて、利用者ユーザーIDの登録や変更、削除等の操作を行い、アクセス権限の発効・失効等の管理を行う。 【住基連携サーバー及び本人確認端末(専用端末)に係る部分】 ・情報システム責任者等が作成するアクセス権限と事務の対応表により、実施できる事務の範囲を限定している。また、対応表は随時見直しを行う。 ・パスワードの最長有効期間を定め、定期的に更新を実施する。
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	【国家資格等情報連携・活用システムに係る部分】 ・情報システム責任者等は以下の作業を行う。 (1)特定個人情報の使用の記録として、特定個人情報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、記録簿は事業が終了するまで保管する。 (2)システム利用従事者が情報システム責任者等に提出する特定個人情報ファイルへのアクセス用アカウントの払出しに係る申請書(以下「申請書」という。)と記録簿を突合し、アカウント払出状況の目視確認を実施する。 (3)国家資格等情報連携・活用システムへのアクセスログ、国家資格等情報連携・活用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。 (4)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、速やかに委託先事業者に報告する等、必要な対応をとる。 【住基連携サーバー及び本人確認端末(専用端末)に係る部分】 ・記録簿を作成しアカウントの払い出し状況を管理する。 ・システムの操作履歴(操作ログ)を記録する。 ・不正な操作が行われていないことについて、操作履歴(操作ログ)を適時確認する。 ・操作履歴の確認により、不正な操作が疑われる場合、申請文書等との整合性の確認を行う。
その他の措置の内容		-
リスクへの対策は十分か		[　十分である　] ＜選択肢＞ 1) 特に力を入れている　2) 十分である 3) 課題が残されている

リスク3： 従業者が事務外で使用するリスク	
リスクに対する措置の内容	【国家資格等情報連携・活用システムに係る部分】 情報システム責任者等は、システム利用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、以下の作業を行う。 (1)システム利用従事者に特定個人情報ファイルへのアクセス用のアカウントを払い出す際は、システム利用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、事務に従事する必要がなくなり次第すぐに当該アカウントを無効とすることで、システム利用従事者が特定個人情報ファイルへアクセス可能な期間が必要最小限となるようにする。 (2)定期的に国家資格等情報連携・活用システムへのアクセスログ及び操作ログを確認し、システム利用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。 (3)サーバー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込み又は持ち出しを物理的検査により監視し、厳重に制限する。 (4)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。 (5)システム利用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。 【住基連携サーバー及び本人確認端末（専用端末）に係る部分】 ・システム操作や特定個人情報等へのアクセスを行う前にログイン操作を行うことで、権限のある者のみ利用ができるよう制御している。 ・システム利用時において、割り当てられたユーザーアカウントに対して許可された事務／事務手続のみ取り扱うことができるようシステムで制御している。 ・操作ログを記録し不正なアクセス等がないか分析を行う。
リスクへの対策は十分か	[十分である]　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク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	【国家資格等情報連携・活用システムに係る部分】 リスク3「リスクに対する措置の内容」の(3)(4)に加え、特定個人情報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。 ・特定個人情報を電子記録媒体により移送する場合は、電子記録媒体を施錠可能な保管庫への保管の上、媒体管理簿で管理し、利用する場合は情報システム責任者等の承諾が必要となる。 【住基連携サーバー及び本人確認端末（専用端末）に係る部分】 ・システム操作や特定個人情報等へのアクセスを行う前にログイン操作を行うことで、権限のある者のみ利用ができるよう制御している。 ・システム利用時において、割り当てられたユーザーアカウントに対して許可された事務／事務手続のみ取り扱うことができるようシステムで制御している。 ・あらかじめ定められた照会方式（ファイル連携方式）以外で特定個人情報ファイルの取得を禁止している。 ・権限のあるもの以外、複製は行えない仕組みとする。 ・バックアップ以外にファイルを複製しないよう、取扱者及び委託先等に対して指導する。 ・バックアップ以外の複製の制限は、通常誰にも付与せず、該当操作が必要な場合に限り、システム管理者の監督のもと、承認された作業者に対して一時的に権限を付与する。また、作業終了時は、システム管理者の監督のもと、その権限を削除する。さらに、権限付与操作の監視、定期的な付与権限の棚卸しを行うことで、不正な権限取得や権限の削除漏れを防止する。 ・操作履歴の確認により、不正な操作が行われていないことの確認を行う。 ・許可された電子記録媒体に限定して使用できるようにシステムを実装し制御する。
リスクへの対策は十分か	[十分である]　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置	
-	

4. 特定個人情報ファイルの取扱いの委託		[　　] 委託しない
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク		
情報保護管理体制の確認		【委託事項1：国家資格等情報連携・活用システムに係る部分】 ・会計法令等に基づく総合評価落札方式により委託先事業者を選定する。 ・委託先事業者の選定を行う際は、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。 【委託事項1：各資格管理者、デジタル庁、当該システムの運用保守事業者の三者の関係】 各資格管理者、デジタル庁、当該システムの運用保守事業者の三者の関係を規定した「国家資格等情報連携・活用システム」の利用にあたっての確認事項（規約）」に同意することにより、当該確認事項に基づき、国家資格等情報連携・活用システムに係る特定個人情報の取扱いを当該システムの運用保守事業者に委託することとする。なお、次の内容については、当該確認事項に規定されている。 ・ 特定個人情報ファイルの閲覧者・更新者の制限 ・ 特定個人情報ファイルの取扱いの記録 ・ 特定個人情報の提供ルール/消去ルール ・ 委託契約書中の特定個人情報ファイルの取扱いに関する規定 ・ 再委託先による特定個人情報ファイルの適切な取扱いの確保 【委託事項2：特定個人情報に係る文書の保管・廃棄委託】 ・仕様書により、 ・責任者、作業体制、連絡体制及び作業場所を書面にして提出 ・業務従事者への遵守事項の周知 ・再委託の承諾申請の提出 ・作業担当者の名簿の提出 等を委託先に求める。 ・選定時にプライバシーマーク取得事業者であることを要件とする。 ・委託元が委託先に対して実地調査を定期的に行い、適切な管理体制をとっていることを確認する。
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	【委託事項1：国家資格等情報連携・活用システムに係る部分】 委託先事業者は特定個人情報について、取扱責任者及び事務取扱担当者を定め、定められた者のみ特定個人情報ファイルにアクセスができるよう制限を行う。また、管理及び実施体制を書面により報告し確認を受けなければならない。 【委託事項2：特定個人情報に係る文書の保管・廃棄委託】 ・作業者を限定するため、委託業務従事者名簿を事前に提出させる。 ・文書の引渡しの際、文書を格納した箱にコードを付与した上で、開封防止のシールを貼付し、職員の監視の下、専用のコンテナに封印して運搬する。
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	【委託事項1：国家資格等情報連携・活用システムに係る部分】 委託先事業者は特定個人情報ファイルの取扱いを含む管理の状況について書面により報告をしなければならない。情報システム責任者等は必要に応じて調査を行い、調査の結果、不適切と認められる場合、是正を指示する。 【委託事項2：特定個人情報に係る文書の保管・廃棄委託】 ・委託先との契約に際して、保管庫等での施錠・管理、管理状況の記録等を規定した仕様書により、取扱いに係る必要事項を定める。 ・仕様書により、委託先に、文書の引渡の都度、引渡した文書を格納した箱に付与されたコード及び引渡日が記載された確認書を提出させる。

特定個人情報の提供ルール		[　　定めている　　] ＜選択肢＞ 1）定めている　　2）定めていない
	委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	【委託事項1：国家資格等情報連携・活用システムに係る部分】 提供する際には、使用目的及び情報の内容を記載した申請書を使用し、情報システム責任者等が確認の上、定められた方法により提供する。 特定個人情報等の管理状況に関する報告により遵守状況の確認をする。 【委託事項2：特定個人情報に係る文書の保管・廃棄委託】 業務上、委託先から他者への提供はない。
	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	【委託事項1：国家資格等情報連携・活用システムに係る部分】 提供する際に、使用目的及び情報の内容を記載した申請書を使用し、それを情報システム責任者等が確認する。授受記録については、媒体、利用期限、返却方法を記載した台帳を作成する。また、提供情報は受託業務完了時に全て返却又は消去する。 特定個人情報等の管理状況に関する報告により遵守状況の確認をする。 ・紙媒体の資料は、直接の授受を原則とし、事務処理が完了したら簿冊に綴り、速やかに保管場所で施錠管理等を行う。鍵は内部職員のみが知る場所で保管することにより、漏えいや紛失を防止する。 ・特定個人情報を電子記録媒体により入手した場合は、電子記録媒体を施錠可能な保管庫への保管の上、媒体管理簿で管理し、国家資格等情報連携・活用システムへの登録が完了次第廃棄する。 【委託事項2：特定個人情報に係る文書の保管・廃棄委託】 ・文書の引渡しの際、文書を格納した箱にコードを付与した上で、開封防止のシールを貼付し、職員の監視の下、専用のコンテナに封印して運搬する。また、その際、コード及び引渡日が記載された確認書を提出させる。仕様書により、搬送車の施錠など盗難、紛失等の防止措置を義務付ける。 ・システムにより、入出庫依頼を管理するとともに、保管状況を確認する。
特定個人情報の消去ルール		[　　定めている　　] ＜選択肢＞ 1）定めている　　2）定めていない
	ルールの内容及びルール遵守の確認方法	【委託事項1：国家資格等情報連携・活用システムに係る部分】 ・国家資格管理事務に係る資格情報等は、資格情報等の抹消申請、行政処分又は死亡により資格が喪失となった者の個人番号を含む資格情報等も適切に管理することとする。 ・システムから消去を行う際には、適切に消去等を行い、消去等に係る記録を作成し、管理する。 「オンプレミス環境の場合」 ・特定個人情報等が記録された機器を廃棄する場合、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。 ・特定個人情報等が記録された電子記録媒体等を廃棄する場合、物理的な破壊等によりデータを復元できないよう完全に消去するとともに、消去証明書を提出させる。 ・情報システム責任者等は委託先事業者から提出される消去等に係る報告書の内容を確認するとともに、報告書に基づき委託先事業者に聴取を行い、必要に応じて立入検査を実施することで、消去が適切に行われていることを確認する。 「クラウド環境の場合」 ・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ISO/IEC27001に準拠した廃棄プロセスを確保していること。 ・廃棄プロセスの適切な実施について、第三者の監査機関による監査を受け、その内容を確認できること。 ・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。 ・情報システム責任者等は委託先事業者から提出される消去等に係る報告書の内容を確認するとともに、報告書に基づき委託先事業者に聴取を行い、必要に応じて立入検査を実施することで、消去が適切に行われていることを確認する。 【委託事項2：特定個人情報に係る文書の保管・廃棄委託】 ・仕様書により、保存期限を過ぎた文書について、溶解処理等により、復元不可能な状態とすることを規定し、処理日、処理対象とした文書箱のコード、処理方法、処理結果等を明記した廃棄証明書を取得する。

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	【委託事項1：国家資格等情報連携・活用システムに係る部分】 ・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。 【委託事項2：特定個人情報に係る文書の保管・廃棄委託】 ・契約書により、個人情報の保護に関する法律施行条例の規定を順守し、個人情報の漏洩防止等適正な管理のために必要な体制の確保に万全の措置を講じることを規定する。 ・目的外使用の禁止、複写及び複製の禁止、作業場所以外持出禁止、情報の保管及び管理に係る安全管理措置、再委託の取扱い並びに実地調査及び指導等について仕様書で規定する。 ・文書の引渡しの際、文書を格納した箱にコードを付与した上で、開封防止のシールを貼付し、専用のコンテナに封印して運搬する。また、その際、コード及び引渡日が記載された確認書を提出させる。仕様書により、搬送車の施錠など盗難、紛失等の防止措置を義務付ける。
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　2）十分に行っている 3）十分に行っていない　4）再委託していない
	具体的な方法	【委託事項1：国家資格等情報連携・活用システムに係る部分】 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。 ・委託先事業者は、定期的又は必要に応じて、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。 ・情報システム責任者等は、委託先事業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検査の実施を依頼する。 【委託事項2：特定個人情報に係る文書の保管・廃棄委託】 仕様書により、業務の全部又は主たる部分の再委託を禁止するとともに、再委託する場合には、事前に申請書を提出させ、委託元の承諾を受ける旨を定める。
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
【委託事項2：特定個人情報に係る文書の保管・廃棄委託】 ・取扱区域への入退室はICカードにより制御し、ログを管理する。 ・取扱区域の出入口は固定カメラ等で監視・録画する。 ・取扱区域への私物の電子機器の持込を禁止し、退出時に荷物検査を行う。

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	国家資格等情報連携・活用システムの利用者認証及び権限管理機能では、ログイン時の利用者認証のほかに、ログイン及びログアウトを実施した利用者、時刻並びに操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する。 ＜中間サーバー・ソフトウェアにおける措置＞ ①情報照会機能（※1）により、情報提供ネットワークシステムに情報照会を行う際には、提供許可証の発行と照会内容の照会許可用照合リスト（※2）との照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから提供許可証を受領してから情報照会を実施することになる。つまり、番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応している。 ②中間サーバーの職員認証・権限管理機能（※3）では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※1）情報提供ネットワークシステムを使用した特定個人情報の照会及び照会した情報の受領を行う機能。 （※2）番号法の規定による情報提供ネットワークシステムを使用した特定個人情報の提供に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの。 （※3）中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2： 安全が保たれない方法によって入手が行われるリスク	
リスクに対する措置の内容	・中間サーバー・ソフトウェアにおける措置 中間サーバーは、個人情報保護委員会との協議を経て、内閣総理大臣が設置・管理する情報提供ネットワークシステムを使用した特定個人情報の入手のみ実施できるよう設計されるため、安全性が担保されている。 ・中間サーバー・プラットフォームにおける措置 ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（LGWAN等）を利用することにより、安全性を確保している。 ②中間サーバーと団体についてはVPN（バーチャルプライベートネットワーク）等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3： 入手した特定個人情報が不正確であるリスク	
リスクに対する措置の内容	・中間サーバー・ソフトウェアにおける措置 中間サーバーは、個人情報保護委員会との協議を経て、内閣総理大臣が設置・管理する情報提供ネットワークシステムを使用して、情報提供用個人識別符号により紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	・中間サーバー・ソフトウェアにおける措置 ①中間サーバーは、情報提供ネットワークシステムを使用した特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応している（※）。 ②既存システムからの接続に対し認証を行い、許可されていないシステムからのアクセスを防止する仕組みを設けている。 ③情報照会が完了又は中断した情報照会結果については、一定期間経過後に当該結果を情報照会機能において直ちに自動で削除することにより、特定個人情報が漏えい・紛失するリスクを軽減している。 ④中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）中間サーバーは、情報提供ネットワークシステムを使用して特定個人情報を送信する際、送信する特定個人情報の暗号化を行っており、照会者の中間サーバーでしか復号できない仕組みになっている。 そのため、情報提供ネットワークシステムでは復号されないものとなっている。 ・中間サーバー・プラットフォームにおける措置 ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（LGWAN等）を利用することにより、漏えい・紛失のリスクに対応している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ③中間サーバー・プラットフォーム事業者の業務は、中間サーバー・プラットフォームの運用、監視・障害対応等であり、業務上、特定個人情報へはアクセスすることはできない。
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	
＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 ②情報連携においてのみ、情報提供用個人識別符号を用いることがシステム上担保されており、不正な名寄せが行われるリスクに対応している。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（LGWAN等）を利用することにより、安全性を確保している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ③中間サーバー・プラットフォームでは、特定個人情報を管理するデータベースを団体ごとに区分管理（アクセス制御）しており、中間サーバー・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 ④特定個人情報の管理を資格管理団体のみが行うことで、中間サーバー・プラットフォームの事業者における情報漏えい等のリスクを極小化する。	

7. 特定個人情報の保管・消去		
リスク1： 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[十分に遵守している]	<選択肢> 1）特に力を入れて遵守している 2）十分に遵守している 3）十分に遵守していない 4）政府機関ではない
②安全管理体制	[十分に整備している]	<選択肢> 1）特に力を入れて整備している 2）十分に整備している 3）十分に整備していない
③安全管理規程	[十分に整備している]	<選択肢> 1）特に力を入れて整備している 2）十分に整備している 3）十分に整備していない
④安全管理体制・規程の職員への周知	[十分に周知している]	<選択肢> 1）特に力を入れて周知している 2）十分に周知している 3）十分に周知していない
⑤物理的対策	[十分に行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
具体的な対策の内容	【国家資格等情報連携・活用システムに係る部分】 (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、政府情報システムのためのセキュリティ評価制度（ISMAP）において登録されたサービスか、ISO/IEC27017:2015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。 ・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。また、事前に申請し承認されてない物品、記憶媒体、通信機器などを不正に所持し、持出持込することがないよう、警備員などにより確認している。 ・設置場所はデータセンター内のパブリッククラウド専用の領域とし、他テナントとの混在によるリスクを回避する。 (2)オンプレミス環境における物理的対策 ・委託先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を収集し、入退室の記録を取得することとしている。 【窓口等における申請書類】 ・申請書類は、キャビネットにおいて施錠保管を行っている。 ・審査が完了した申請書類は適宜文書保管・廃棄委託業者に引渡し、保管・管理する。委託業者においては、①取扱区域への入退室はICカードにより制御し、ログを管理すること、②取扱区域の出入り口は固定カメラ等で監視・録画すること、③取扱区域への私物の電子機器の持込みを禁止し、退出時に荷物検査を行うことを義務付ける。	
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	【国家資格等情報連携・活用システムに係る部分】 ・利用者本人がマイナポータルにアクセスする際、マイナンバー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。 ・パブリッククラウド事業者は個人番号を内容に含む電子データを取り扱わない契約とし、個人番号等にクラウド事業者がアクセスできないように、アクセス制御を行う。 ・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。 ・運用保守拠点とパブリッククラウド環境及びオンプレミス環境との通信には、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ネットワーク回線を使用する。 ・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。 ・論理的に区分された各資格管理者ごとの領域にデータを保管し、当該領域のデータは暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・権限を有する者以外特定個人情報にアクセスできないように制御している。 ・当該システムへの不正アクセスの防止のため、外部からの侵入検知・通知機能を備えている。 ・ウイルス対策ソフトを必要に応じて導入し、パターンファイルの更新を行う。 ・導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ・電子記録媒体のデータについては、暗号化している。	

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	[　発生あり　]	＜選択肢＞ 1）発生あり　2）発生なし
その内容	①令和2年8月21日に東京都人権プラザにおいて開催した「心と体を傷つけられて亡くなった大国の子供たちのメッセージ」展のメディア向けカンファレンスの動画配信案内を（公財）東京都人権啓発センターの行事案内希望者に対して送付する際、事務担当者が誤ってメールアドレスをBCC欄ではなく、CC欄に入力して発信したため、個人情報が流出する事故が発生した。 ②令和3年1月に東京都電子調達システムにより印刷物の契約案件を公表した際、印刷物の配布先となる町会名のみを公表するところ、誤って中野区内の町会の代表者の氏名、住所及び電話番号を1月28日から2月3日までの間、公表してしまった。 ③令和3年3月、助成金返還事務のためにワンビシより取り寄せていた平成29年度教育助成金調査票（B表）の返却手続きを行った際、段ボール二箱分がないことが発覚した。当該段ボール箱は執務室内の空きスペースにて保管していた。 ④令和3年7月、都のインターンシップ関連イベントに係る告知メールを送信する際、都が過去に出展した民間企業主催の就職イベント参加者及び当該企業に対して都関連の採用情報の提供を希望した者のメールアドレスを、BCC欄ではなく宛先欄に入力して一斉に送信したため、個人情報が流出する事故が発生した。 ⑤令和3年9月、東日本大震災都内避難者向けに作成する「都内避難者の皆様への定期便」の一部について、送付業務の受託者が誤って本人以外の避難者の宛名を記載して発送してしまい、氏名が流出する事故が発生した。 ⑥令和3年12月、都営住宅の毎月募集の申込者に対して、東京都住宅供給公社において、抽せん番号をお知らせする郵便はがきを発送する準備を行い、料金別納で郵便局に持ち込みを完了したつもりであったが、後日、郵便局に確認したところ、持ち込まれたことを示す書類がないことが判明した。申込者に電話で確認したところ、郵便はがきが届いていることを確認できなかったため、申込者の氏名、住所等が記載されたはがきを紛失する事故が発生した。 ⑦令和4年5月、指定管理者が運営する東京都現代美術館において、ミュージアムショップ運営の受託事業者スタッフが、展覧会図録を予約した顧客へ一斉に案内メールを送信する際、メールアドレスをBCC欄ではなく、宛先欄に入力して発信した。 ⑧令和4年5月、都の技能検定試験に関する業務を行う東京都職業能力開発協会において、技能検定試験に関する通知を外国人技能実習の監理団体に対してメールで送付する際、事務担当者が誤ってメールアドレスをBCC欄ではなく、CC欄に入力し、一斉送信した。 ⑨令和4年5月、就学支援金事務の受託者である東京都私学財団が、就学支援金の基礎データをCD-Rに情報を保存し、対象高等学校等宛て一斉に送付したところ、そのうち1校において、他校の受給者に関する情報が含まれていることが判明した。 ⑩令和4年5月、都の医療機器産業への参入支援事業の受託者が、事業に関するイベントを案内するメールマガジンを送付する際、宛先欄に複数のメールアドレスを入力し、送信してしまった。同社の配信システムは、1名分のメールを送信した後、宛先欄のメールアドレスが自動で次の1名のアドレスに上書き処理されるプログラムが組まれていたが、プログラムの改修ミスにより、メールアドレスが上書きではなく追記されて送信されていた。 ⑪令和4年10月、東京都陽性者登録センターの運営受託者が、医療機関で新型コロナウイルス陽性の診断を受け、センターに登録申請を行った複数の患者への登録完了メールを、送付先アドレスが全て入れ替わったまま送信してしまった。 ⑫令和4年12月、労働力調査の統計調査員に対して連絡事項をメールした際、BCC欄に入力して送るべきところを宛先欄に入力し、一斉送信した。

	再発防止策の内容	①団体に対し、外部へ一斉送信する際は、メールアドレスをBCC欄に入力すべきことと、メール送信前に、複数の職員で宛先の確認作業を必ず行うことを、職員全員に改めて周知徹底するとともに、組織としての検証を行い、再発防止策を検討するよう指導した。 ②（1）事務フローの見直し ・起工部署の事務フローを、別紙1のとおり見直し、周知徹底を図る。 ・契約部署は、着手起案作成時及び発注図書登録時、電子調達システムに、起工部署から提出されたPDFデータを公表前の登録を行ってから印刷した上で、契約依頼文書に添付された仕様書と照合し、一致していることを確認する。また、この確認方法について、令和元年12月19日付経理部契約課長事務連絡「契約事務に係る情報漏えい等の防止策について」により配布されたチェックリストに追記した。 （2）臨時支所コンプライアンス推進委員会の開催 臨時支所コンプライアンス推進委員会を開催し、再発防止に向け、上記事務フローの見直しの周知徹底を図った。 ③（1）個人情報の重要性を再確認し、高い危機意識をもって個人情報の適正な管理・運用を図るよう、改めて基本的な取扱いルールの徹底を図る。 （2）書類の所在及び処理状況が明確に分かるような管理方法の整備や、文書廃棄の際の事務処理手順の整備など、書類管理の徹底に向けた仕組みの構築を図る。 ④（1）局内全職員に対して情報セキュリティ研修を実施し、二度と同様の事故を起こさないよう、情報セキュリティ対策の確認を徹底する。 （2）外部の複数の宛先に対してメールを送信する場合、「BCC」欄に入力するとともに、送信前に複数の職員によるチェックを徹底する。 ⑤これまで実施してきた委託事業者への発送完了時の確認のほか、委託事業者職員による宛名、住所の複数チェック等、発送作業での確認作業を確実に実施させるとともに、都においても個人情報を含む情報の適切な取扱いについて、さらなる徹底を図り、再発防止に努める。 ⑥（1）スケジュールの情報共有と進行管理の徹底 発送に関わる者を含め、課全員が発送スケジュールや作業進捗状況を把握・共有する。また、管理監督職が発送作業の進捗管理を密に行うことで発送遅延や発送漏れを直ちに把握できるようにする。 （2）発送前後の確認体制の見直し 当日発送すべき郵便物が揃っているか、発送を担当している係全体でチェックする。発送担当者は、郵便局からの領収証を運搬業者から受け取った後に、発送物作成担当者に引き渡す。発送物作成担当者は、領収証等に担当課長代理・課長の確認押印を受ける。 （3）紛失リスクの解消 発送予定日前にはがきが納品された場合であっても、その日のうちに郵便局へ持ち込み、はがきを長期間執務室に滞留させないようにする。 ⑦（1）ミュージアムショップにおいて、本社セキュリティインシデント統括部と連携して、個人情報取り扱い、情報管理体制の改善を行う。 （2）特に複数人へのメール送信に際してはダブルチェックを徹底する。 （3）現代美術館全委託業者に、適切な個人情報等の取扱い及び情報管理を徹底するよう指示する。 （4）財団が管理運営する各施設にも本事案を共有し、個人情報を含む情報の適切な管理を徹底する。 ⑧（1）個人情報の取扱い及び情報管理の徹底等について周知するとともに、職員全員に臨時研修を速やかに実施 （2）誤送信防止に向けたシステムの導入（ダイアログの自動表示など） （3）複数人チェックなど基本的対策の徹底 ⑨チェック機能を再検証し、全日制等と同様の仕組みを通信制にも直ちに導入するほか、事務フローの再構築を行い、再発防止に努める。そのうえで、本件を財団内で広く共有させ、個人情報の取扱い

		全般についてハード・ソフトの両面から厳しく見直すとともに、職員の意識向上を図っていく。また、都の実施機関においても個人情報の適正管理とサイバーセキュリティー対策について改めて確認を行う。 ⑩(1)システムの改善 メールマガジンの配信は、これまで「TO」により自動で1件ずつ送信がされる仕組みであったが、一括メール送信においては送信者アドレスを全て「BCC」に入れるようシステム改修を行う。 (2)システム会社における確認体制の強化 開発前にシステム会社が実施する、影響調査・テスト内容等について、これまでの2名体制によるダブルチェックから、システム会社のプロジェクトマネージャーも加えることとし、確認した内容を報告させて承認する運用へ見直す。 (3)受託者における確認体制の強化 システム会社のテスト結果の確認にあたっては、テストの証跡情報の提出を求め、内容の確認を行うとともに、受託者での運用テストでは要件定義とも照らした確認を担当だけでなく管理職も実施することにより徹底する。 ⑪受託事業者に対して厳正に指導し、登録完了メール送信作業のチェック体制を強化させる。 ⑫(1)部コンプライアンス推進委員会の臨時開催 ・メール送信時のダブルチェックを徹底させるため、個人情報等の取扱いに係るチェックリストの全職員での点検により注意を喚起、情報管理を再徹底する。 ・あわせて、最近の事故事案の事例を周知するなど、事故の再発予防を進める。 (2)定期的な事故防止意識の醸成 統計調査員を含む全職員を対象に、各所属長や指導員から情報セキュリティや感染拡大防止等に関する指導を定期・継続的に行い、危機意識の醸成等を図る。
⑩死者の個人番号		[保管している] ＜選択肢＞ 1) 保管している 2) 保管していない
	具体的な保管方法	死者の個人番号は生存者の個人番号と同様の保管方法により保管される。
その他の措置の内容		-
リスクへの対策は十分か		[十分である] ＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている

リスク2： 特定個人情報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	・利用者の申請等により、特定個人情報（資格情報等）に変更等が生じた場合はその都度データを更新する。 ・定期に、住民基本台帳ネットワークシステムへの照会による本人確認を行い、データの更新を行うことで正確性を担保する。 ・定期に、情報提供ネットワークシステムへの照会による本籍情報の確認を行い、データの更新を行うことで正確性を担保する。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク3： 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	【国家資格等情報連携・活用システムに係る部分】 ・マイナポータル内に情報等は保管されない。 ・国家資格管理事務に係る資格情報等は、資格情報等の抹消申請、行政処分又は死亡により資格が喪失となった者の個人番号を含む資格情報等も適切に管理することとする。 ・定められた運用手順に従い、特定個人情報は、国家資格等情報連携・活用システムによる自動的な消去あるいは定期的な運用による消去を行う。 ・特定個人情報を電子記録媒体により入手した場合は、電子記録媒体を施錠可能な保管庫への保管の上、媒体管理簿で管理し、国家資格等情報連携・活用システムへの登録が完了次第廃棄する。 ・オンプレミス環境の電子記録媒体は、専用ソフトによる完全消去又は物理的破壊により、復元不可能な手段で消去・廃棄し、管理簿等に消去・廃棄の記録を残す。 ・オンプレミス環境では、特定個人情報等が記録された機器や電子記録媒体等廃棄する場合、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。 ・パブリッククラウド環境では、データの復元がなされないよう、パブリッククラウド事業者においてISO/IEC27001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及びオンプレミス環境とも、特定個人情報の消去ルールに従い、システムから特定個人情報等の消去を行う。なお、クラウド環境ではアカウント誤削除対策としてアカウント削除後も一定期間情報が保持される可能性があるため、アカウント削除前に論理的なデータ消去を行う。 ・委託先事業者から提出される消去等に係る報告書の内容を確認するとともに、報告書に基づき委託先事業者に聴取を行い、必要に応じて立入検査を実施することで、消去が適切に行われていることを確認する。 【窓口等における申請書類】 ・保存期間を満了した申請書類については、溶解処理により廃棄している。 ・東京都で保管する書類の廃棄に当たっては、仕様書により、委託先により①廃棄文書の回収の際、受託者の社員であることの身分証明書を常時携帯させ、委託者の求めに応じて提示させること、②廃棄文書の飛散・盗難防止のため、施錠又は特殊警報装置等を装備した車両を使用すること、③作業中に車両を離れる場合は、施錠し、又は監視員を配置すること、④廃棄文書が収納された箱を開封することなく、受託者の監視下に置いて回収運搬・溶解処理を行うこと、⑤溶解処理については、荷下ろしから溶解までの録画やモニター監視、不審者の侵入防止のための入退室管理や監視カメラの設置等の安全対策が講じられている施設に搬入し、処理すること及び⑥委託者に溶解処理証明書を提出することを義務付けている。 ・文書保管委託により保管している書類の廃棄に当たっては、委託先における溶解処理等により、復元不可能な状態とする。溶解処理等については、仕様書により、①取扱区域への入退室はICカードにより制御し、ログを管理すること、②取扱区域の出入り口は固定カメラ等で監視・録画すること、③取扱区域への私物の電子機器の持込みを禁止し、退出時に荷物検査を行うこと、④処理日、処理対象とした文書箱のコード、処理方法、処理結果等を明記した書面により報告することを義務付ける。
その他の措置の内容	-
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置	
-	

Ⅳ　その他のリスク対策 ※

1. 監査

①自己点検	[　　十分に行っている　　]	＜選択肢＞ 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
具体的なチェック方法	【国家資格等情報連携・活用システムに係る部分】 「国家資格等情報連携・活用システムの利用にあたっての確認事項（規約）」に同意のうえ、適切に事務従事者等の当該システムの利用を管理し、必要な監督をする。 【東京都における取扱い】 ・個人情報保護については、全職員が職員向けの自己点検表を用いてチェックを実施。 ・情報セキュリティについては、情報セキュリティ責任者（統括）が点検表を用いてチェックを実施。 ・評価書の記載内容どおりの運用ができているか、年１回担当部署でチェックを実施。	
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	【国家資格等情報連携・活用システムに係る部分】 「国家資格等情報連携・活用システムの利用にあたっての確認事項（規約）」に同意のうえ、適切に事務従事者等の当該システムの利用を管理し、必要な監督をする。 【東京都における取扱い】 ・東京都特定個人情報保護監査ガイドラインに従い、４年に一度のサイクルで助言型の内部監査を実施。	

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	【国家資格等情報連携・活用システムに係る部分】 「国家資格等情報連携・活用システムの利用にあたっての確認事項（規約）」に同意のうえ、適切に事務従事者等の当該システムの利用を管理し、必要な指導をする。 【東京都における取扱い】 ・全職員を対象に情報セキュリティ・個人情報保護の研修を実施している。研修の目的は、個人情報保護の重要性及び適正管理等に関する理解を深め、個人情報保護の遵守を徹底することである。具体的には、以下の研修を実施している。 ・個人端末からアクセスするe-ラーニング研修（理解度が基準に達しないと終了できない） ・新規採用職員や他局転入職員等を対象とした研修 ・未研修者に対しては、研修受講者によるフォローアップ研修の実施 【委託事業者】 業務開始に当たり、個人情報の取扱いルールを順守することを確認させている。	

3. その他のリスク対策

【国家資格等情報連携・活用システムに係る部分】
「国家資格等情報連携・活用システムの利用にあたっての確認事項（規約）」に同意のうえ、適切に当該システムを利用し、万が一、障害や情報漏えいが生じた場合、適切な対応をとることができる体制を構築する。
特定個人情報の漏えい事案が発生した場合は、「特定個人情報の適正な取扱に関するガイドライン」にて示されている以下の安全管理措置を実施する。
<特定個人情報の漏えい事案が発生した場合の対応>
①組織内における報告及び被害の拡大防止
②事実関係の調査及び原因究明
③影響範囲の特定
④再発防止策の検討・実施
⑤影響を受ける可能性のある本人への連絡等
⑥事実関係、再発防止策等の公表
⑦個人情報保護委員会への報告

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	東京都保健医療局保健政策部健康推進課 〒163-8001東京都新宿区西新宿二丁目8-1 都庁第一本庁舎29階南側 TEL：03-5320-4357（内線 32－872）
②請求方法	指定様式による書面の提出（原則として持参）により開示、訂正又は利用停止の請求を受け付ける。
特記事項	請求方法、様式等について東京都公式ホームページ上で分かりやすく表示
③手数料等	[　　有料　　]　＜選択肢＞ 1) 有料　2) 無料 （手数料額、納付方法：納付書により、実費相当分（10円／1枚）の手数料を納付する。　　）
④個人情報ファイル簿の公表	[　行っていない　]　＜選択肢＞ 1) 行っている　2) 行っていない
個人情報ファイル名	-
公表場所	-
⑤法令による特別の手続	-
⑥個人情報ファイル簿への不記載等	-

2. 特定個人情報ファイルの取扱いに関する問合せ	
①連絡先	東京都保健医療局保健政策部健康推進課 〒163-8001東京都新宿区西新宿二丁目8-1 都庁第一本庁舎29階南側 TEL：03-5320-4357（内線 32－872）
②対応方法	電話・メールなど

Ⅵ　評価実施手続

1. 基礎項目評価	
①実施日	令和6年1月17日
②しきい値判断結果	［　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）　］ ＜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	東京都ホームページにおいて意見募集の掲載を行い、電子メール、FAX及び郵送にて意見を受け付けた。
②実施日・期間	令和5年9月15日（金曜日）から同年10月16日（月曜日）まで
③期間を短縮する特段の理由	-
④主な意見の内容	意見なし
⑤評価書への反映	なし
3. 第三者点検	
①実施日	令和5年11月22日（水曜日）から同年12月20日（水曜日）まで
②方法	東京都情報公開・個人情報保護審議会特定個人情報保護評価部会において点検を受けた。
③結果	以下の答申を受けた。 特定個人情報ファイルの取扱いの開始時期も未定であり、現時点で未確認の事項があるものの、現時点で把握している情報を基に個人のプライバシー等の権利利益に与える影響を予測した上で、特定個人情報の漏えいその他の事態を発生させるリスクを分析し、そのようなリスクを軽減するための適切な措置を講じることができるよう準備が進められているものと認められる。
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
令和6年3月21日	Ⅰ個人情報 5個人番号の利用 法令上の根拠	・番号法第9条第1項（利用範囲） 別表第1　項番13	・番号法第9条第1項（利用範囲） 別表第1　項番12	事前	