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
40	調理師法による調理師資格の登録（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、調理師資格の登録（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

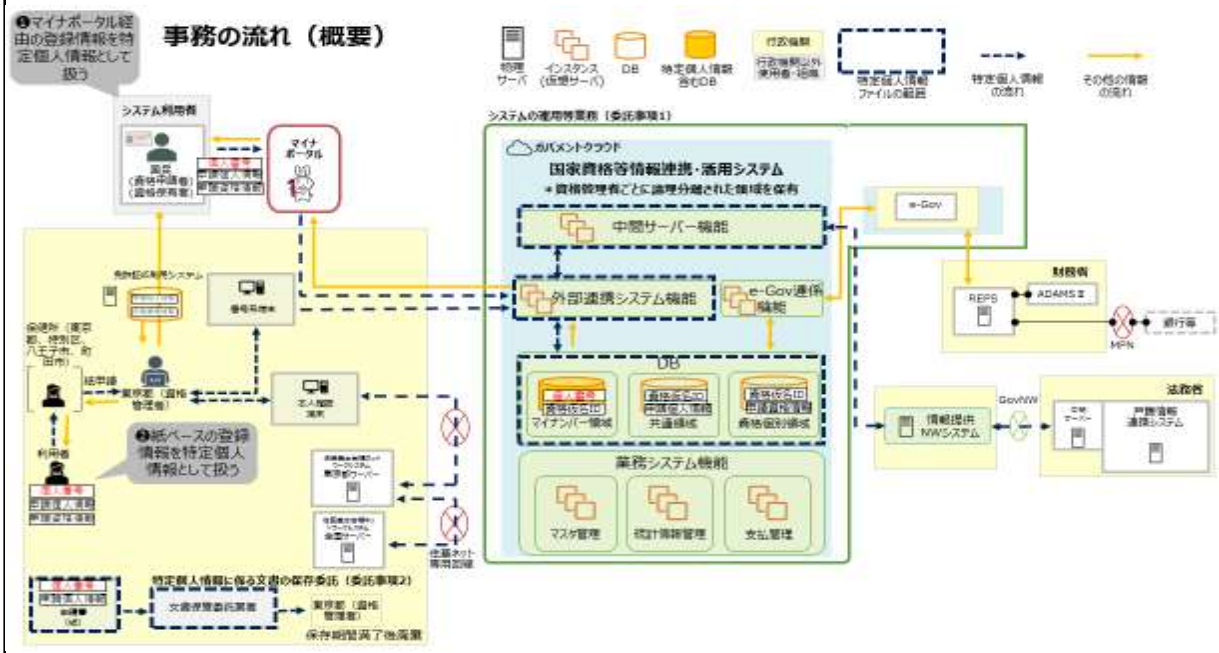
1. 特定個人情報ファイルを取り扱う事務	
①事務の名称	調理師法による調理師資格の登録（免許）に関する事務
②事務の内容　※	■資格管理事務（特定個人情報ファイルの取扱有） i.資格情報の登録 　オンライン（マイナポータル）又は紙での申請受理後に審査を行い、資格情報の登録を行う。なお、オンライン登録の際にはマイナンバーカードの電子証明書を利用し、資格保有者本人であることを確認する。個人番号については、登録を受けようとする資格保有者のマイナンバーカードに搭載された券面事項入力補助機能を活用し、その改変を不可能ならしめることにより真正性を担保する。登録情報については、住民基本台帳法（昭和42年法律第81号）（以下、「住基法」という。）及び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。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 　なし
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	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・管理すること等を可能とする。 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.個人番号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個人番号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。（国家資格等情報連携・活用システムでログデータを一定期間保存した後に削除。） ■「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することを可能とする。 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することを可能とする。 ■「外部連携関連機能」（特定個人情報ファイルの取扱有） i.資格管理者等が保有する既存の資格登録等に関するシステムとの連携を可能とする。（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。 ■「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 符号管理機能では、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 情報照会機能では、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 中間サーバー機能と住民基本台帳ネットワークシステム等との間での情報照会内容、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 中間サーバー機能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 中間サーバー機能を利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報 （連携対象）へのアクセス制御を行う。 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ることを可能とする。 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することを可能とする。
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」　　）

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（全国サーバー）
②システムの機能	1. 住民基本台帳ネットワークシステム（全国サーバー）への情報照会 住所地が都外にある場合は、住民基本台帳ネットワークシステム（全国サーバー）に対して、東京都サーバーを経由して、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　（　）
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することを可能とする。 ・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することを可能とする。 ・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することを可能とする。 (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ることを可能とする。 ・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することを可能とする。
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　（　）

システム4	
①システムの名称	免許証印刷用システム
②システムの機能	調理師免許証印刷機能（特定個人情報ファイルの取扱無）
③他のシステムとの接続	[　　] 情報提供ネットワークシステム　　[　　] 庁内連携システム [　　] 住民基本台帳ネットワークシステム　　[　　] 既存住民基本台帳システム [　　] 宛名システム等　　[　　] 税務システム [　　] その他　（　　）
システム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	
調理師名簿ファイル	
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を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　項番43の2 ・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3　項番6の4　、別表第5　項番7の4
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　項番43の2
7. 評価実施機関における担当部署	
①部署	東京都保健医療局健康安全部健康安全課
②所属長の役職名	健康安全課長
8. 他の評価実施機関	
―	

（別添1）事務の内容

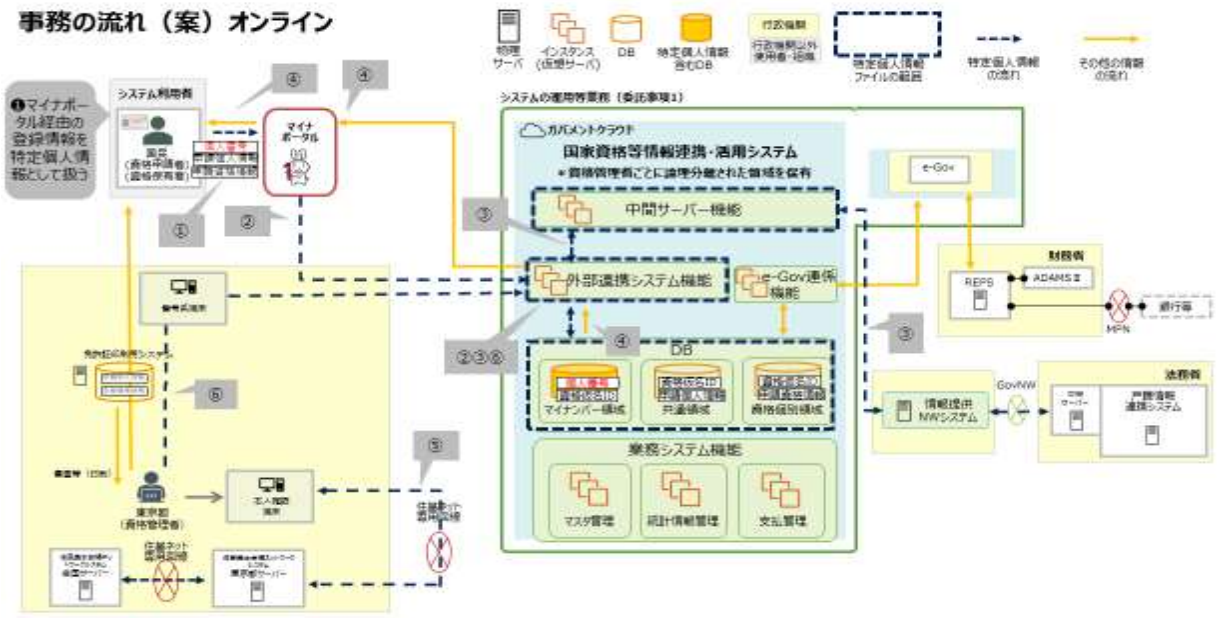


【事務の流れ】

■資格管理事務（個人番号利用有）
・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。
・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（個人番号利用無し）
・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。

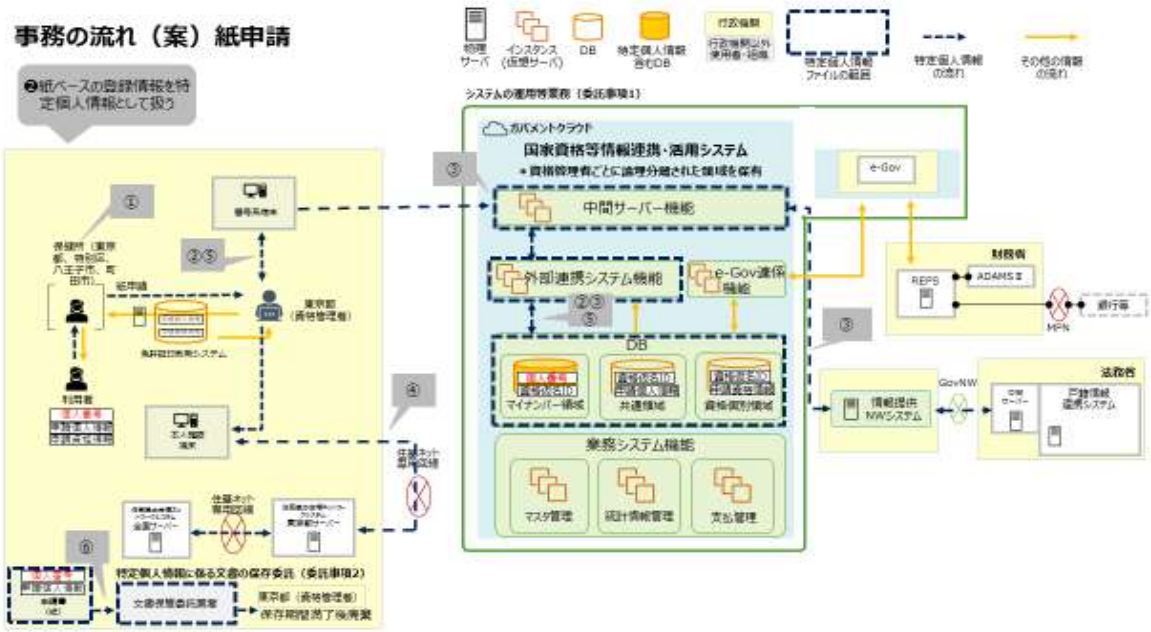
■資格証事務（個人番号利用無し）
・デジタル資格証発行（オンライン）
資格保有者が自身の保有する資格情報を第3者へ対面で自身のスマホやタブレット上に表示しデジタル資格証として提示する。また、当該資格情報をオンライン上で提供することも可能とする。
・資格証の発行・再発行（紙）
資格情報の登録業務にて登録が完了した資格登録者について、資格証の作成処理を行う。再発行については、オンライン（マイナポータル）もしくは紙での申請を受けて、審査を行う。審査の結果、問題が無ければ資格証の作成処理を行う。
作成後、申請者に対して免許証を交付する。



【特定個人情報の流れ（オンライン）】

①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（自動的に取得される個人番号含む）は外部連携システム機能と連携し、資格登録情報として国家資格等情報連携・活用システムに登録される。
③資格登録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。
④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。
⑤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。
⑥即時方式により確認を行った本人確認情報について、番号系端末を介し、資格管理者が直接国家資格等情報連携・活用システムに登録（更新）を行う。

注１）外部連携システム機能を介して連携された資格情報のうち、個人番号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。個人番号と資格仮名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個人番号と紐付く機関別符号を用いて行う。



【特定個人情報の流れ（紙）】

①紙の申請書において提出され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個人番号の確認を行う。
②申請された資格情報（個人番号含む）は外部連携システム機能と連携し、番号系端末から国家資格等情報連携・活用システムに登録を行う。
③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。01_第74回評価部会（総
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。
④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。
⑤即時方式により確認を行った本人確認情報について、番号系端末を介し、資格管理者が直接国家資格等情報連携・活用システムに登録（更新）を行う。
⑥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、保存期間が満了した申請書類は、職員がシュレッダー処理をする。

注１）外部連携システム機能を介して連携された資格情報のうち、個人番号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。個人番号と資格仮名　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個人番号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		
調理師名簿ファイル		
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　※		調理師資格の登録者
	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 ［〇］個人番号　［　］個人番号対応符号　［〇］その他識別情報（内部番号） ・連絡先等情報 ［〇］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 ［〇］その他　（　資格情報（登録番号、登録年月日等）、本籍地都道府県名　）
	その妥当性	【識別情報】 ・調理師資格の登録者及びその申請者を正確に特定するために保有する。 【連絡先等情報】 ・調理師資格の登録者及びその申請者対象者を正確に特定するため保有する。 【業務関係情報】 ・調理師資格の名簿登録事務及び免許証発行事務を実施するため保有する。
	全ての記録項目	別添2を参照。
⑤保有開始日		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等の一部を改正する法律（令和5年法律第48号）の公布の日から起算して一年三月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		東京都保健医療局健康安全部健康安全課

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 （ 総務局（住民基本台帳ネットワーク） ） [○] 行政機関・独立行政法人等 （ 法務省 ） [○] 地方公共団体・地方独立行政法人 （ 都区市保健所（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 （ 住民基本台帳ネットワークシステム ）
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 項番43の2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	ー
⑦使用の主体	使用部署 ※	東京都保健医療局健康安全部健康安全課
	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		未定

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 ※	調理師資格登録者
	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		[50人以上100人未満] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[ ]専用線 [ ]電子メール [○]電子記録媒体（フラッシュメモリを除く。） [ ]フラッシュメモリ [ ]紙 [○]その他 （ 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		株式会社 NTT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	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存委託
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及び管理を適切に行うため、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		未定
⑥委託先名		未定
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	
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 ※		【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。 【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う。 審査が完了した申請書類は、適宜、仕様書で個人情報保護法の他関係法令の規定に従い、個人の権利利益を侵すことのないよう最大限努めることを義務づけた文書保存委託業者に引渡し、保管・管理する。
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	国家資格・情報連携システム内の資格名簿については、登録がある限り原則として保有し続ける。上記「期間」欄に記載の「定められていない」は、システム内の資格名簿に関する記載である。 なお、申請書類の保存期間は1年である。
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】 ・資格情報等は、資格情報等の抹消申請、行政処分又は登録者の死亡を契機とし、システムの名簿情報から抹消される。なお、データの物理削除は行わず当該抹消情報を記録した上で管理する。 ・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。 ・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。 【申請書類】 申請書類の保存期間は1年と定めており、保存期間が満了した申請書類は、職員がシュレッダー処理している。

7. 備考

―

（別添2）特定個人情報ファイル記録項目

1　仮名ID
2　免許番号
3　収受年月日
4　収受番号
5　免許年月日
6　交付年月日
7　本籍地都道府県又は国籍
8　カナ氏名
9　氏名
10　外字登録有無
11　旧姓（姓）
12　旧姓併記の外字登録有無
13　通称名
14　通称名併記の外字登録有無
15　生年月日
16　性別
17　免許資格（養成施設卒業/講習会受講/試験合格）
18　所管場所
19　履歴1（氏名変更、本籍地変更、再交付、併記など）
20　履歴1の年月日
21　履歴2（氏名変更、本籍地変更、再交付、併記など）
22　履歴2の年月日
23　履歴3（氏名変更、本籍地変更、再交付、併記など）
24　履歴3の年月日
25　履歴4（氏名変更、本籍地変更、再交付、併記など）
26　履歴4の年月日
27　履歴5（氏名変更、本籍地変更、再交付、併記など）
28　履歴5の年月日
29　マイナンバー

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	
調理師名簿ファイル	
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】 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（住基ネット専用端末）からの入手】 本人確認端末（住基ネット専用端末）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、住基ネットセキュリティ責任者（健康安全課長）が、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い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。 【本人確認端末（住基ネット専用端末）からの入手】 本人確認端末（住基ネット専用端末）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。 【本人確認端末（住基ネット専用端末）からの入手】 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。本人確認端末（住基ネット専用端末）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、住基ネットセキュリティ責任者（健康安全課長）が、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。
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、必要に応じ、本人確認端末（住基ネット専用端末）において本人確認を実施する。 【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。
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、必要に応じ、本人確認端末（住基ネット専用端末）において本人確認を行い、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。
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、専用線及びクラウド内部の通信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】 窓口等において申請を受け付ける場合、本人から直接書面を受け取ることを原則とし、紙媒体の資料は、窓口担当部署から審査担当部署への送付には、専用の封筒及び重要文書送付簿で管理される重要文書交換制度を用いる。郵送については、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。審査担当部署において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。 【本人確認端末（住基ネット専用端末）からの入手】 本人確認端末（住基ネット専用端末）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（東京都サーバー）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（サイバーセキュリティ管理者及び情報システム管理者）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。 【本人確認端末（住基ネット専用端末）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は以下の作業を行う。 (1)発効の管理 ・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アカウントを消去する。 【本人確認端末（住基ネット専用端末）に係る部分】 （1）発行の管理 ・アクセス権限の管理は、住基ネットセキュリティ責任者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住基ネットセキュリティ責任者に対して申請した者に限定して発行する。 住基ネットセキュリティ責任者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 ・住基ネットセキュリティ責任者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は、事務従事者に係るユーザ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。 【本人確認端末（住基ネット専用端末）に係る部分】 ・情報システム責任者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。 【本人確認端末（住基ネット専用端末）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。 【本人確認端末(住基ネット専用端末)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。 【本人確認端末(住基ネット専用端末)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。 ・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権限は、通常誰にも付与せず、該当操作が必要な場合に限り、システム管理者の監督のもと、承認された作業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	【国家資格等情報連携・活用システムに係る部分】 特定個人情報の管理を含む業務運用の委託を行う際は、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。 【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 【特定個人情報に係る文書の保存委託】 ・仕様書により、以下の事項等を委託先に求める。 ・責任者、従事者、監査者、作業場所及び連絡・対処体制の届出 ・従事者への個人情報保護に関して必要な事項の周知 ・責任者・従業者に対する個人情報保護法に係る教育及び研修の実施 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。 ・必要に応じ委託元が委託先に対して実地調査を行い、必要な措置が講じられ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	【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。 【特定個人情報に係る文書の保存委託】 ・文書記録等の取扱いは、その重要性について専門的な教育を受けた委託先社員が行う。	
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	【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。 【特定個人情報に係る文書の保存委託】 ・保管庫への入出については、限られた者であり、入出の記録を適正な期間保持できる入退室管理システムを整備している。 ・在庫管理、入出庫管理及び期限管理について、システム管理している。	

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	【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を確認をする。 【特定個人情報に係る文書の保存委託】 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	【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を確認をする。 【特定個人情報に係る文書の保存委託】 ・在庫管理、入出庫管理及び期限管理について、システム管理している。 ・集配は文書記録等の重要性について専門的な教育を受けた自社社員が自社の車両を使用して行う。 ・集配車両は積載コンテナの完全な施錠、GPS搭載等防犯装備が完備している。 ・文書等の引き渡しを受けた場合は、委託者に受領書を提出する。
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	【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、行政処分又は登録者の死亡を契機とし、システムの名簿情報から抹消される。なお、データの物理削除は行わず当該抹消情報を記録した上で管理する。 ・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。 ・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	【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。 【特定個人情報に係る文書の保存委託】 ・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2条第1項に定める個人情報等（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「番号利用法」という。）第2条第8号に定める特定個人情報を含む。以下同じ。）を取り扱う場合は、個人情報保護法の他関係法令の規定に従い、個人の権利利益を侵すことのないよう最大限努めなければならない。 ・目的外使用の禁止、複写、複製等の禁止、従事者等の教育及び研修並びに個人情報等の安全管理等。 ・文書等の引き渡しを受けた場合は、委託者に受領書を提出する。 ・集配車両の積載コンテナの完全な施錠、GPS搭載等防犯装備の完備の義務付け。
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	【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り検査の実施を依頼する。 【特定個人情報に係る文書の保存委託】 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		
－		

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・活用システムに係る部分】 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中間サーバー機能（国家資格等情報連携・活用システム）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）中間サーバー機能（国家資格等情報連携・活用システム）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 中間サーバー機能（国家資格等情報連携・活用システム）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中間サーバー機能（国家資格等情報連携・活用システム）と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ガバメントソリューションサービス・ネットワーク（以下「GSSネットワーク」という。）を利用することにより、安全性を確保している。 ②中間サーバー機能（国家資格等情報連携・活用システム）と団体についてはGSSネットワークや総合行政ネットワーク等の高度なセキュリティを維持した回線による接続とするとともに、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 中間サーバー機能（国家資格等情報連携・活用システム）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中間サーバー機能（国家資格等情報連携・活用システム）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中間サーバー機能（国家資格等情報連携・活用システム）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。 （※）中間サーバー機能（国家資格等情報連携・活用システム）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機能（国家資格等情報連携・活用システム）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中間サーバー機能（国家資格等情報連携・活用システム）と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GSSネットワーク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中間サーバー機能（国家資格等情報連携・活用システム）と団体についてはGSSネットワークや総合行政ネットワーク等の高度なセキュリティを維持した回線による接続とするとともに、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中間サーバー機能（国家資格等情報連携・活用システム）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中間サーバー機能（国家資格等情報連携・活用システム）と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GSSネットワークを利用することにより、安全性を確保している。 ②中間サーバー機能（国家資格等情報連携・活用システム）と団体についてはGSSネットワークや総合行政ネットワーク等の高度なセキュリティを維持した回線による接続とするとともに、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。 【窓口等における申請書類】 窓口担当部署から審査担当部署への送付には、専用の封筒及び重要文書送付簿で管理される重要文書交換制度を用いる。 審査担当部署において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。 審査が完了した申請書類は、適宜、仕様書で個人情報保護法の他関係法令の規定に従い、個人の権利利益を侵すことのないよう最大限努めることを義務づけた文書保存委託業者に引渡し、保管・管理する。	
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。	
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、対象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。 ②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た。 ③令和3年12月、都営住宅の毎月募集の申込者に対して抽せん番号をお知らせする郵便はがきを発送する際、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。 ④令和4年5月、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。 ⑤令和4年5月、技能検定試験に関する通知を外国人技能実習の複数の監理団体に対してメールで送付する際、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。 ⑥令和4年5月、就学支援金事務において、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、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。 ⑦令和4年5月、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、配信プログラム改修ミスにより、宛先欄に複数のメールアドレスが入力され、送信されてしまった。 ⑧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。 ⑨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。 ⑩令和5年4月、再委託先の派遣会社職員が、業務で使用するシステムを不適切に使用し、個人情報を閲覧、メモにとり自宅に持ち出した。 ⑪令和5年5月、施設から転院する患者に診断資料を渡した際、別の患者の検査資料を含めて交付した。 ⑫令和5年6月、施設から転院する患者に診断資料を渡した際、別の患者の検査資料を含めて交付した。 ⑬令和5年7月、施設を退所する患者に関して、退所先候補の施設と受入調整を行うため、診療関係書類をFAX送信した際、誤って別のFAX番号宛てに送信した。 ⑭令和5年8月、申請により受け付けた申請書が紛失していることが発覚した。 ⑮令和5年9月、関係施設宛に都民情報をFAX送信した際、誤って別の事業者宛てに送信した。 ⑯令和5年9月、事業の対象者に案内チラシを郵送した際、送付対象者の抽出ツールのプログラム仕様の不備により、誤って事業対象外の方に送付したことで、旧住所宛てに送付し返戻されなかったものが誤送付となった。 ⑰令和5年9月、決定通知書に公印を押印する目的で本庁に出張し、押印後持ち帰ったが、発送の準備をしていた際に、通知書1枚が紛失していることが発覚した。 ⑱令和6年1月、患者A宛てに送付すべき利用者情報を、誤ってB宛てに送付した。 ⑲令和6年1月、入所者の診療関係ファイルが紛失していることが発覚し、その後、退所者の荷物の中に当該ファイルが紛れ込んでいたことが発覚した。 ⑳令和6年2月、児童相談所の職員が、出張中に個人情報が記載されている手帳を紛失し、あわせて手帳に収納されていた、当該職員の証票及び所内職員の緊急連絡網を紛失した。 ㉑令和6年2月、施設を退所した患者Aに関する薬剤情報等を記載した書類を、誤って別の患者の退院時荷物に混入させ交付した。 ㉒令和6年2月、オンライン研修で使用した映像において、患者の情報をマスキング処理していたところ、当該映像をスマートフォンで視聴した場合に、マスキングが外れ、個人が特定できる状態になっていたことが判明した。

	再発防止策の内容	①（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。 ②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。 ③（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。 ④（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。 ⑤（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 ⑥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。 ⑦（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。 ⑧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。 ⑨（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委託先における個人情報の閲覧・使用に当たっての権限の設定や、不適切な閲覧・使用・持ち出しを防止するための体制についてあらためて確認し、適切な運用を徹底させる。 ⑪（1）情報共有をしているホワイトボードの位置、記入欄が分かりにくいとの意見が出たため、位置、記入方法について変更した。 （2）書類封入時のチェック手順中に、患者氏名の確認を明示した。 （3）2者確認を徹底するため、事務員のみでなく看護職員もチェックを行うこととし、2者チェックが終わった段階で封書のチェックボックスに記載する。 （4）責任の所在を明確にするため「転院時退所セット確認書」を新たに作成し、チェックを行った職員が記名する。 ⑫（1）チェックリストを活用し、複数人、複数回のチェックを行うとともに、最終チェック者を統括責任者とすることで、誤封入等を防ぐ体制を整える。 （2）都職員が施設へ直接出向き、個人情報管理の実態確認を実施するとともに、対応が不十分な場合は是正指導を行う。 （3）個人情報保護の研修を実施し、施設全体で個人情報保護の取り組み状況を共有した上で、改善を徹底する。 ⑬（1）委託先に対し、個人情報に関する業務手順を見直し及び徹底を図ることや、全従事者に対する個人情報保護研修を行うことを指導した。また、改善策の確認のため、都が施設へ出向き、個人情報管理の実態を確認した。 （2）再委託先において、送付の際は、まずFAX以外の手段を調整し、止むを得ずFAXを使用する際には、FAX番号の聞き取りの際の復唱や、FAX送信前の送信先への番号の再確認、複数人で複数回のチェックを必ず行うこととした。また、全従業者に対する個人情報保護研修を行った。 ⑭（1）作業環境等を見直し、書類の混入等が起きにくい環境を整備 ①執務室内の作業スペースの確保及び活用 ②引き出し付きの棚をキャビネット内に新設し、書類の分類をよりしやすくした。 （2）委託業者との書類の受け渡し方法の変更（送付する判定機関ごとに数を確認しながら受け渡す）。

		⑮個人情報をFAX送信することを禁止するよう各施設に通知した。 ⑯抽出ツールのプログラム確認は、委託先事業者の運用チームのみが行っていたが、抽出ツールを作成・利用する際には、運用チームに加えて、開発チームと委託元である都の3者で抽出ツールのプログラムの仕様・設定を確認することとした。 ⑰個人情報の持出、返却確認及び受け渡しの際の確認の徹底を行う。また、作業工程等を点検し、作業方法やチェック方法等ミスが起きにくい方法を検討、実施する。 ⑱郵便の発送作業は複数職員でチェックすることを再徹底。また、特に慎重を要する個人情報を取り扱う施設における個人情報の事故の重大性について改めて周知するとともに、書類の発送、保管、業務の進行管理等について、注意喚起や指導を行った。 ⑲（1）ファイルが他の物に紛れてしまわないよう、目立つ色に変更する。 （2）作業スペースに仕切りを立てて、使用スペースを物理的に限定する。 （3）ファイルに記載する名前をイニシャルに表記変更する等、使用する情報から個人情報を削除する。 （4）決まった時間に決まった人員が所在を確認する。 （5）チェックの時間を定刻とし、声をかけ合う。 （6）出したらしまうといった基本的事項を、改めて徹底するよう、注意喚起する。 （7）急いでいたり、忙しい時間帯でも、ダブルチェックをするよう、改めて徹底する。また、退所時にも荷物を確認してから渡すようにする ⑳（個人情報の管理について） （1）相談援助業務上の記録をノート等に記載する場合は、イニシャルを使用するなど個人情報を特定されないようにすること。また、私物のノートや手帳に個人情報を記載しないこと。 （2）庁舎外での会議等に出席した際には、個人端末を活用して記録の作成を行うとともに、作成した文書は暗号化し保存すること。 （3）業務上やむを得ず個人情報が記録された書類を庁舎外に持ち出す場合は、局の保有個人情報安全管理基準に基づき管理職の許可を得ること。 （4）個人情報を含む書類を持ち出すにあたっては、盗難や紛失を防止できる形状・機能を持つ鞄に収納し、肌身離さず持ち運ぶなど十分に注意すること。 （5）その他個人情報の取り扱いについては、局の保有個人情報安全管理基準等を遵守し、適正に行うこと。 （職員の証票の管理について） （1）月1回、各職員の保有状況を点検すること （2）携行する際には、ストラップ付きのケースに収納するなど、常に身体から離さずに携行することを徹底すること （職員の緊急連絡網の管理について） （1）必要な連絡先は公用携帯に保存し、連絡網を記載した紙は庁舎外に持ち出さないこと。 ㉑（1）入所時や退所時の手順確認のチェックリスト様式を変更し、入所時の写真撮影やリストへの正確な情報記載、退所時の荷物確認の手順など守るべきルールを追記するとともに、実施者を記載する欄を追加
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	【国家資格等情報連携・活用システムに係る部分】 ・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。 ・必要に応じ、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。 ・必要に応じ、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。 ・資格情報等は、資格情報等の抹消申請、行政処分又は登録者の死亡を契機とし、システムの名簿情報から抹消される。なお、データの物理削除は行わず当該抹消情報を記録した上で管理する。 ・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。 ・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。 ・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。 【紙媒体の申請書類】 ・保存期間が満了した申請書類は、職員がシュレッダー処理している。
その他の措置の内容	－
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
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】 ・毎年１月を「個人情報安全管理・情報セキュリティ強化月間」と位置付け、自己点検等の取組を実施	
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】 ・情報セキュリティ・個人情報保護について、個人端末からアクセスするe-ラーニング研修を実施し、併せて未受講者に対する研修機会を確保している。 【委託事業者】 　従事者への個人情報保護に関して必要な事項の周知並びに責任者・従業者に対する個人情報保護法に係る教育及び研修の実施を義務付けている。	

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等事案が発生した場合は、「特定個人情報の適正な取扱い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等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	東京都保健医療局健康安全部健康安全課 〒163-8001東京都新宿区西新宿二丁目8-1 都庁第一本庁舎30階北側 TEL:03-5320-4358(内線 34-141)
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:　　)
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	調理師名簿
公表場所	東京都ホームページ
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	東京都保健医療局健康安全部健康安全課 〒163-8001東京都新宿区西新宿二丁目8-1 都庁第一本庁舎30階北側 TEL:03-5320-4358(内線 34-141)
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	
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