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
6	国家資格等の登録等に関する事務（医師等7資格、管理栄養士、薬剤師、介護福祉士） 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

国家資格等の登録等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

厚生労働大臣

個人情報保護委員会　承認日 【行政機関等のみ】

令和5年4月26日

公表日

令和5年4月26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	国家資格登録関係事務
②事務の内容　※	【国家資格等情報連携・活用システムに係る部分（共通して記載）】 ■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収入印紙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。 【各資格管理者ごとに記載する部分（独自に記載）】 ※各資格ごとの事務内容については別紙参照。
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。 ■「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。 ■「住民基本台帳ネットワークシステム連携機能」（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。また、本人確認情報を基に個人番号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 中間サーバーと既存システム及び住民基本台帳ネットワーク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 中間サーバー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」、「免許登録管理システム」、「登録情報連携システム」）
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　）

システム4	
①システムの名称	免許登録管理システム【医籍等ファイル、薬剤師名簿ファイル】
②システムの機能	■「管理機能（データベース管理機能）」 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.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。 ■「外部連携関連機能」 i.国家資格等情報連携・活用システムと連携を可能とする。（資格情報のデータ連携機能） ii.その他、資格管理者が保有する資格確認検索システムとの連携を可能とする。 ■「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.資格保有者に発行する資格証の印刷機能を有する。
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、薬剤師資格確認検索システム、資格確認検索システム）
システム5	
①システムの名称	登録情報連携システム【介護福祉士登録名簿ファイル】
②システムの機能	■「オンライン申請データの受付機能」（特定個人情報の取扱無） 資格仮名ID及び申請データを国家資格等情報連携・活用システムとAPI等で連携する情報連携システムでデータを受領し、USB等を使用して登録システムにデータの取り込みを行う。 ■「登録情報連携システムデータの送信機能」（特定個人情報の取扱有） 個人番号の提出があった紙による申請受付を特定個人情報管理PCに登録し、当該データをUSB等を使用して国家資格等情報連携・活用システムとAPI等で連携する情報連携システムにデータを移行し、国家資格等情報連携・活用システムに情報連携を行う。 個人番号は、申請書と別様に記載した個人番号等と本人確認書類の突合審査を行い、個人番号及び申請データを国家資格等情報連携・活用システムに連携する。連携後は国家資格等情報連携・活用システムで採番された資格仮名IDのみ登録情報連携システムに登録し、個人番号の記載のある紙、個人番号データは保持せず、復元出来ない方法で削除する。連携以後は資格仮名IDを利用し、国家資格等情報連携・活用システムとの連携を図る。
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	
医籍等ファイル、管理栄養士名簿ファイル、薬剤師名簿ファイル、介護福祉士登録名簿ファイル	
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	【医籍等ファイル】 （医師） ・番号法第9条第1項（利用範囲） 別表第1　項番15 ・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2 （歯科医師） ・番号法第9条第1項（利用範囲） 別表第1　項番16 ・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3 （看護師） ・番号法第9条第1項（利用範囲） 別表第1　項番17 ・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4 （保健師） ・番号法第9条第1項（利用範囲） 別表第1　項番17 ・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4 （助産師） ・番号法第9条第1項（利用範囲） 別表第1　項番17 ・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4 （理学療法士） ・番号法第9条第1項（利用範囲） 別表第1　項番69 ・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10 （臨床検査技師） ・番号法第9条第1項（利用範囲） 別表第1　項番41 ・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9 【管理栄養士名簿ファイル】 ・番号法第9条第1項（利用範囲） 別表第1　項番13 ・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 【薬剤師名簿ファイル】 ・番号法第9条第1項（利用範囲） 別表第1　項番54 ・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59の2 【介護福祉士登録名簿ファイル】 ・番号法第9条第1項（利用範囲） 別表第1　項番87 ・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71の7 ※未施行

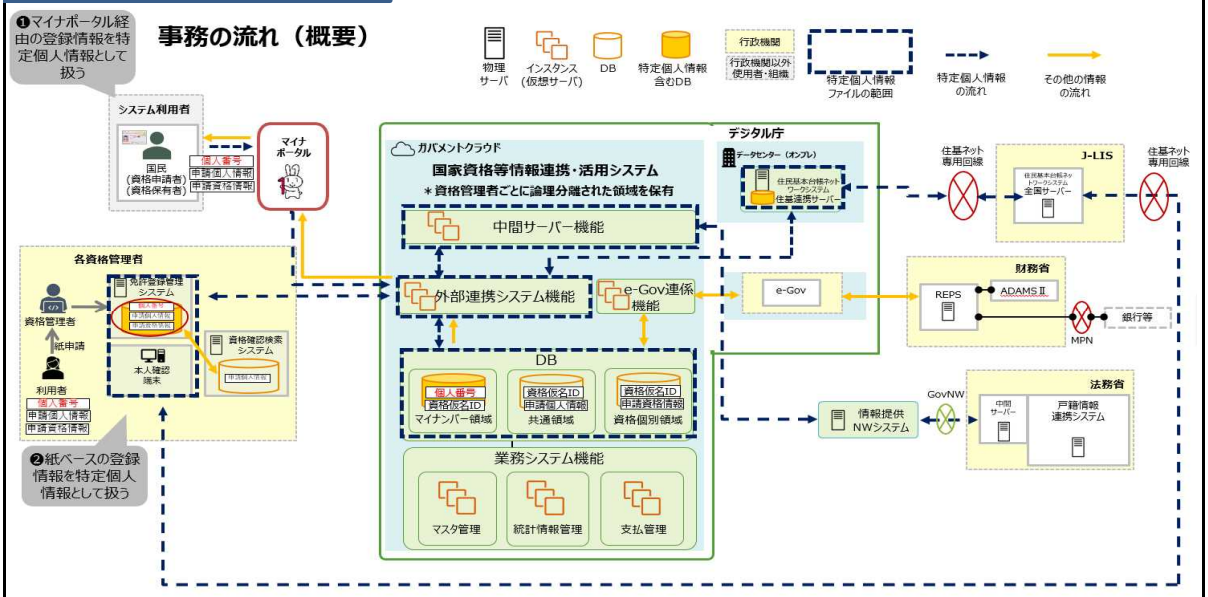
6. 情報提供ネットワークシステムによる情報連携 ※	
①実施の有無	[　　実施する　　]　　＜選択肢＞ 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	【医籍等ファイル】 （医師） ・番号法第19条第8号（特定個人情報の提供の制限） 別表第2　項番27 （歯科医師） ・番号法第19条第8号（特定個人情報の提供の制限） 別表第2　項番28 （看護師） ・番号法第19条第8号（特定個人情報の提供の制限） 別表第2　項番29 （保健師） ・番号法第19条第8号（特定個人情報の提供の制限） 別表第2　項番29 （助産師） ・番号法第19条第8号（特定個人情報の提供の制限） 別表第2　項番29 （理学療法士） ・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87 （臨床検査技師） ・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52 【管理栄養士名簿ファイル】 ・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 【薬剤師名簿ファイル】 ・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71 【介護福祉士登録名簿ファイル】 ・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110 ※未施行
7. 評価実施機関における担当部署	
①部署	【医籍等ファイル】（医師、歯科医師、看護師、保健師、助産師、理学療法士、臨床検査技師） 厚生労働省医政局医事課、歯科保健課、看護課 【管理栄養士名簿ファイル】 厚生労働省健康局健康課 【薬剤師名簿ファイル】 厚生労働省医薬・生活衛生局総務課 【介護福祉士登録名簿ファイル】 厚生労働省社会・援護局福祉基盤課
②所属長の役職名	【医籍等ファイル】（医師、歯科医師、看護師、保健師、助産師、理学療法士、臨床検査技師） 医事課長、歯科保健課長、看護課長 【管理栄養士名簿ファイル】 健康課長 【薬剤師名簿ファイル】 総務課長 【介護福祉士登録名簿ファイル】 社会・援護局福祉基盤課長
8. 他の評価実施機関	
【介護福祉士登録名簿ファイル】 公益財団法人社会福祉振興・試験センター	

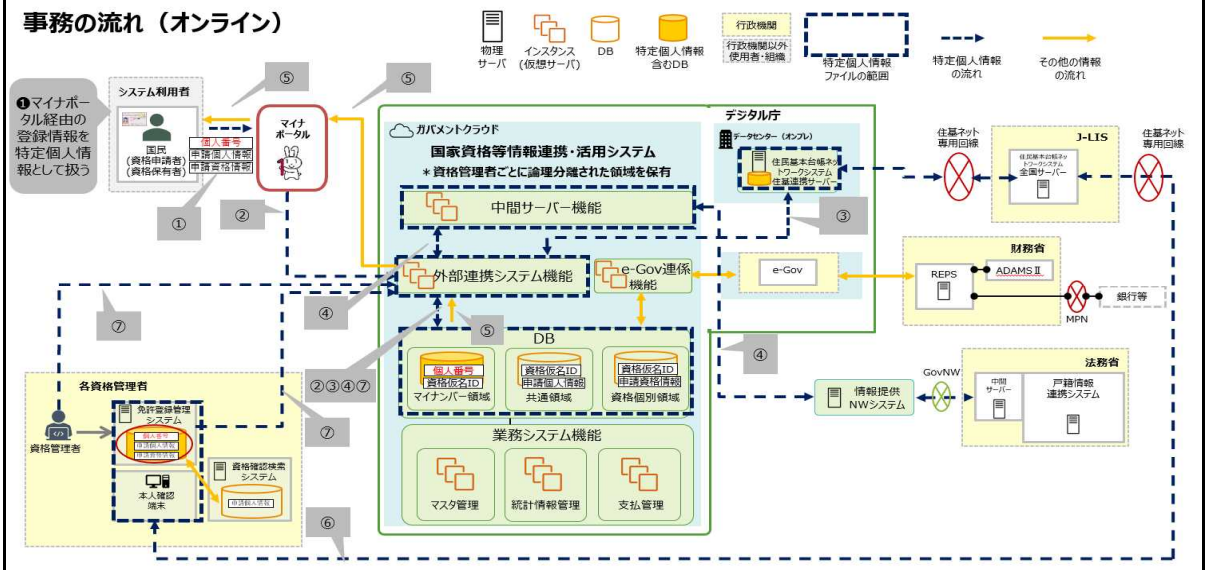
Ⅰ　基本情報（別紙）

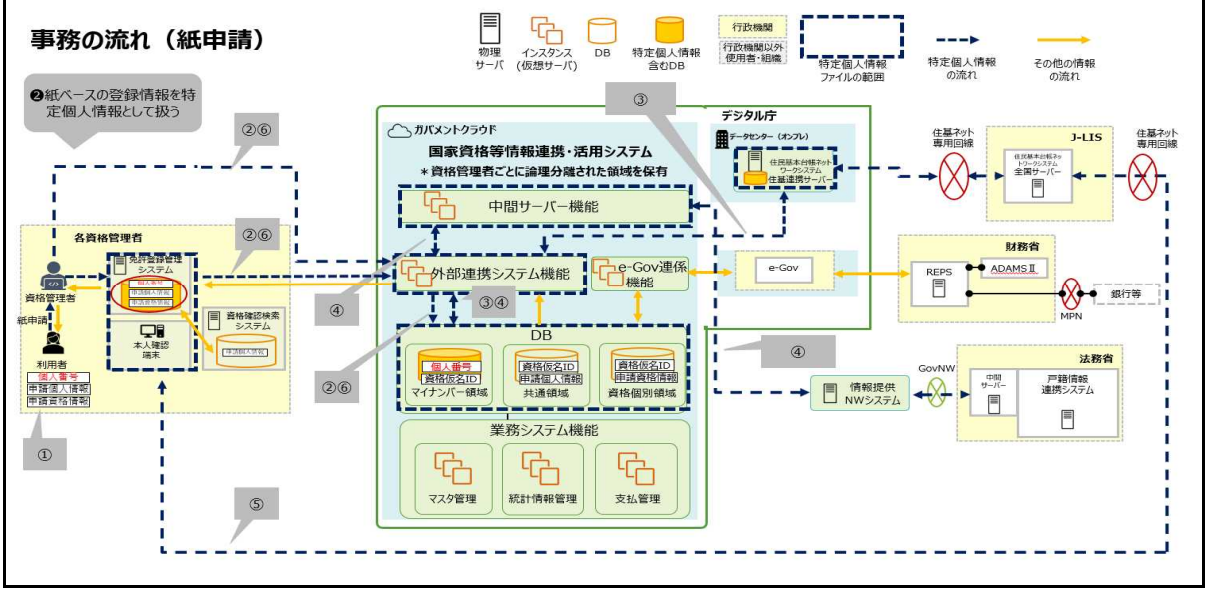
1．特定個人情報ファイルを取り扱う事務	
②事務の内容　※	※各資格ごとの事務内容 【医籍等ファイル】（医師、歯科医師、看護師、保健師、助産師、理学療法士、臨床検査技師） 医師法（昭和23年法律第201号）等の規定に基づき、資格の管理、資格の登録、また登録後の資格情報の維持管理、登録手数料等の収入金の管理などの事務を行う。 ■資格情報の既存システムとの連携（特定個人情報ファイルの取扱有） 　厚生労働省が保有する免許登録管理システムと国家資格等情報連携・活用システムに登録された特定個人情報を含む資格情報データを連携し登録情報の同期を行い正確な資格情報の管理を行う。 【管理栄養士名簿ファイル】 ■既存システムなし。評価書記載のとおり。 【薬剤師名簿ファイル】 ■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） 　厚生労働省が保有する免許登録管理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。 【介護福祉士登録名簿ファイル】 ■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） 　（公財）社会福祉振興・試験センターが保有する登録情報連携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。 【登録情報連携システムに係る部分】 ■「オンライン申請データの受付事務」（特定個人情報の取扱無） 　資格仮名ID及び申請データを国家資格等情報連携・活用システムとAPI等で連携する情報連携システムでデータを受領し、USB等を使用して登録システムにデータの取り込みを行う。 【概要】オンライン申請分の申請データを随時（API連携）もしくは定期（ファイル連携）により情報連携システムへ連携（特定個人情報を含まない資格仮名ID及び別添2の項目3～80のデータ）する。なお、連携後は資格仮名IDをキーに情報連携を行う。 ■「登録情報連携システムデータの情報連携事務」（特定個人情報の取扱有） 　個人番号の提出があった紙による申請受付を特定個人情報管理PCに登録し、当該データはUSB等を使用して国家資格等情報連携・活用システムとAPI等で連携する情報連携システムにデータを移行し、国家資格等情報連携・活用システムに情報連携を行う。 【概要①】試験合格者の別添2の項目（項目3～80のデータ）について、情報連携システムから国家資格等情報連携・活用システムへ合格者情報を連携する。 【概要②】本人より窓口等で紙による申請があり、申請情報を情報連携システムへ登録し、随時（API連系）もしくは定期（ファイル連携）に情報連携システムから国家資格等情報連携・活用システムへ資格情報を連携（個人番号及び別添2の項目3～80のデータ）する。なお、連携後は、特定個人情報は復元できないよう削除し、連携後は資格仮名IDをキーに情報連携を行う。 　個人番号は、申請書と別様に記載した個人番号等と本人確認書類の突合審査を行い、個人番号及び申請情報を国家資格等情報連携・活用システムに連携する。連携後は国家資格等情報連携・活用システムで採番された資格仮名IDのみ登録情報連携システムに連携し、個人番号の記載のある紙、個人番号データは保持せず、復元できない方法で削除する。連携以後は資格仮名IDを利用し、国家資格等情報連携・活用システムとの連携を図る。

（別添1）事務の内容

医籍等ファイル







（備考）

【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（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。

【特定個人情報の流れ】

■オンライン申請の場合
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（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、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、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、資格管理者が保有する免許登録管理システム経由若しくは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。

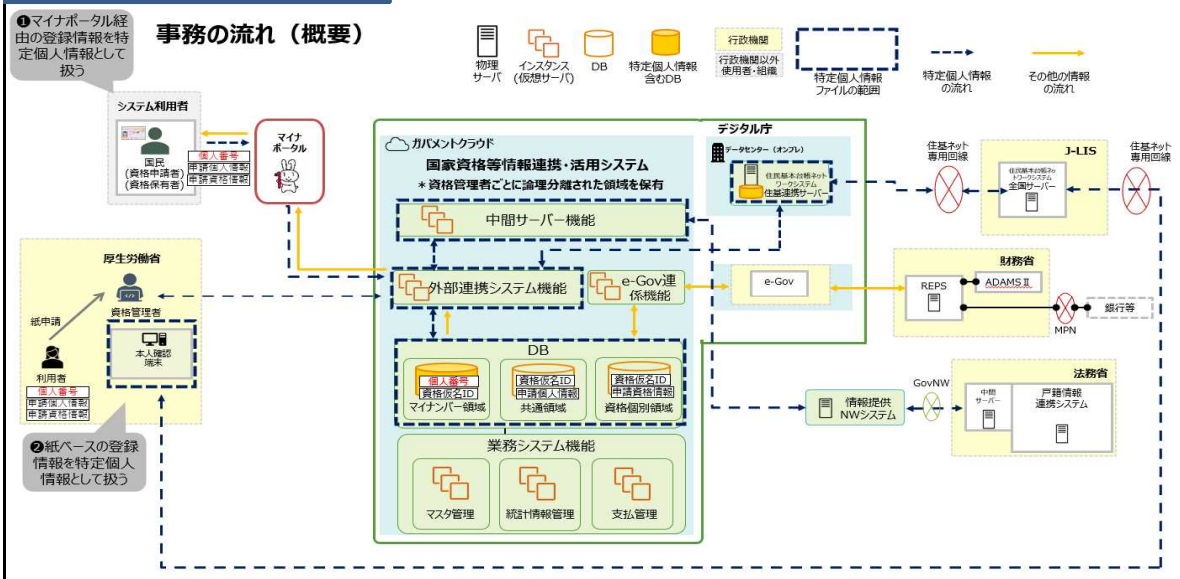
■紙による申請の場合
①紙の申請書において提出された資格情報について、資格保有者本人であることの確認及び個人番号の確認を行う。
②申請された資格情報（個人番号含む）は外部連携システム機能と連携し、資格管理者が保有する免許登録管理システム経由若しくは直接国家資格等情報連携・活用システムに登録を行う。
③登録された情報については、住基法に定められた範囲内において一括方式による住民基本台帳ネットワークシステムを利用した情報連携を行い、本人確認情報等の確認を行う。また、外部連携システム機能において住民基本台帳ネットワークシステムに対して定期に実施する照会処理により取得した照会結果を連携をすることで正確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、資格管理者が保有する免許登録管理システム経由若しくは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。

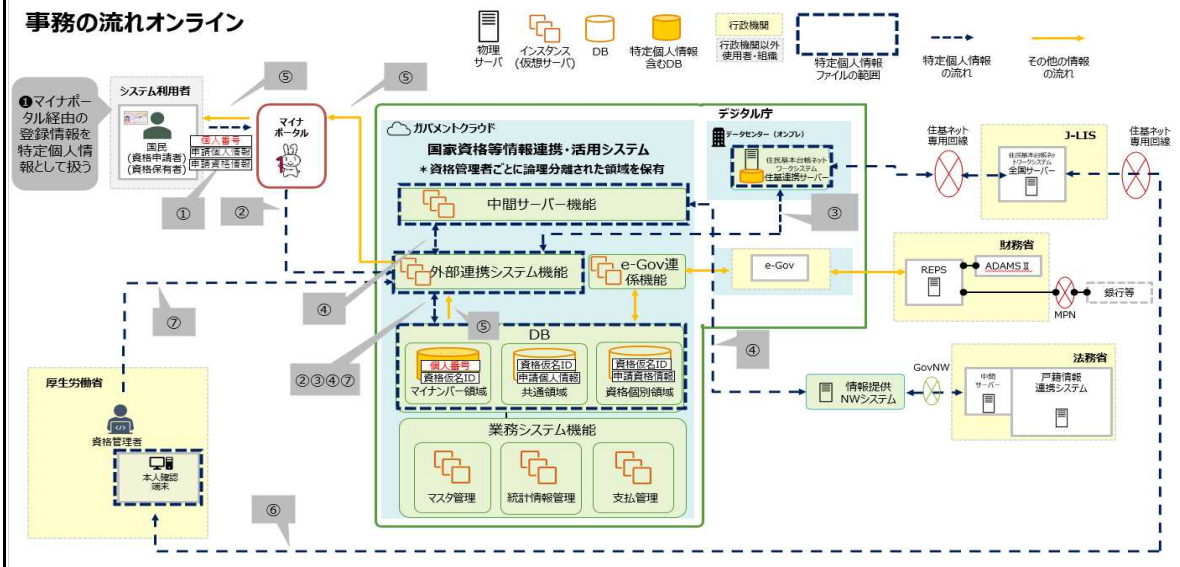
（別添1）事務の内容

管理栄養士名簿ファイル

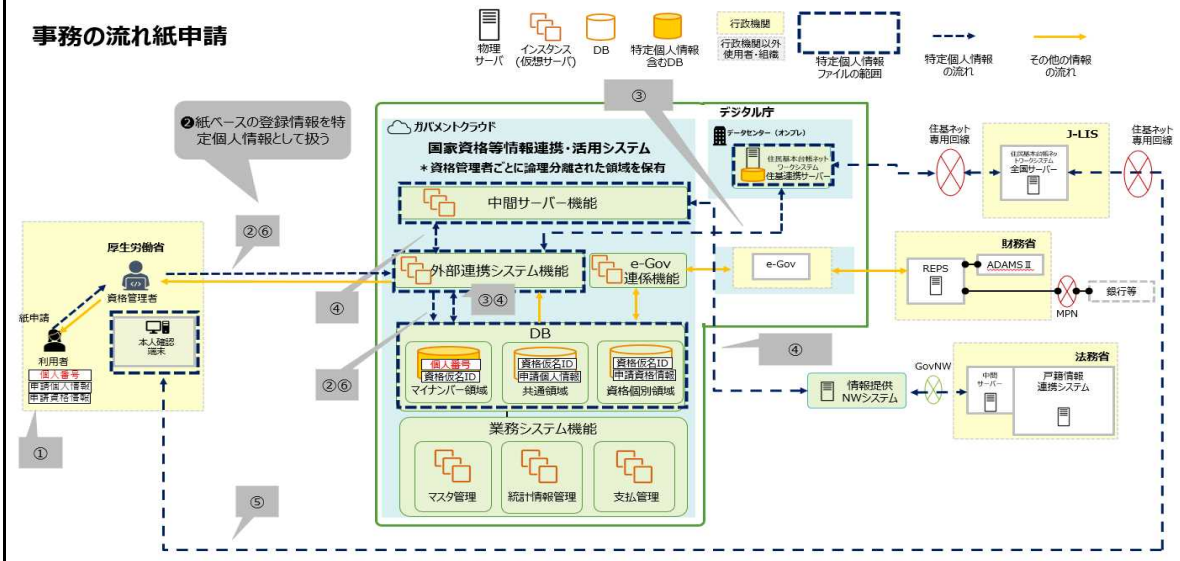
事務の流れ（概要）



事務の流れオンライン



事務の流れ紙申請



（備考）

【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（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。

【特定個人情報の流れ】

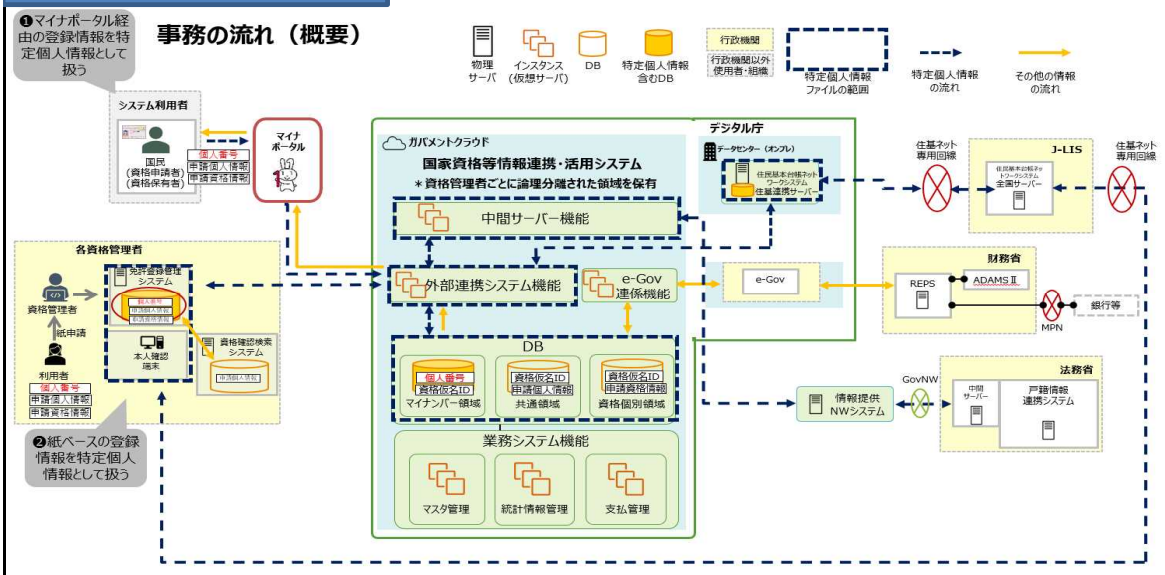
■オンライン申請の場合
①マイナポータルにログイン後、マイナンバーカードの電子証明書を利用し、資格保有者本人であることを確認する。
②入力された資格情報（個人番号含む）は外部連携システム機能と連携し、資格登録情報として国家資格等情報連携・活用システムに登録される。
③資格登録情報は、住基法に定められた範囲内において一括方式による住民基本台帳ネットワークシステムを利用した情報連携を行い、本人確認情報等の確認を行う。また、住民基本台帳ネットワークシステムに対して定期に実施する照会処理により取得した照会結果を連携をすることで正確な資格情報を把握することができる。
④資格登録情報は番号法に定められた範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、直接国家資格等情報連携・活用システムに登録（更新）を行う。

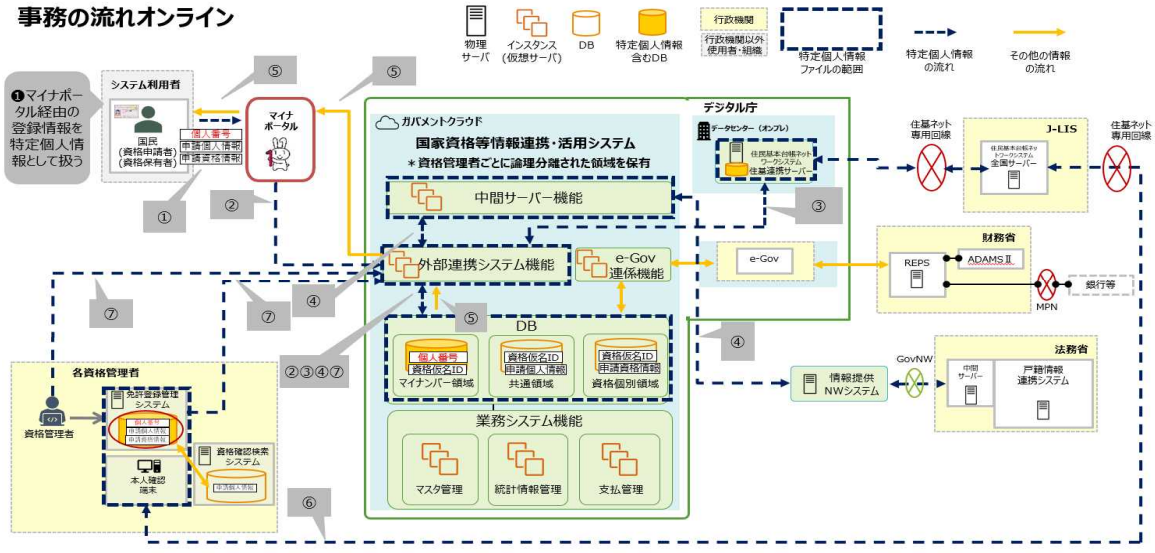
■紙による申請の場合
①紙の申請書において提出された資格情報について、資格保有者本人であることの確認及び個人番号の確認を行う。
②申請された資格情報（個人番号含む）は外部連携システム機能と連携し、直接国家資格等情報連携・活用システムに登録を行う。
③登録された情報については、住基法に定められた範囲内において一括方式による住民基本台帳ネットワークシステムを利用した情報連携を行い、本人確認情報等の確認を行う。また、外部連携システム機能において住民基本台帳ネットワークシステムに対して定期に実施する照会処理により取得した照会結果を連携をすることで正確な資格情報を把握することができる。
④登録された資格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。

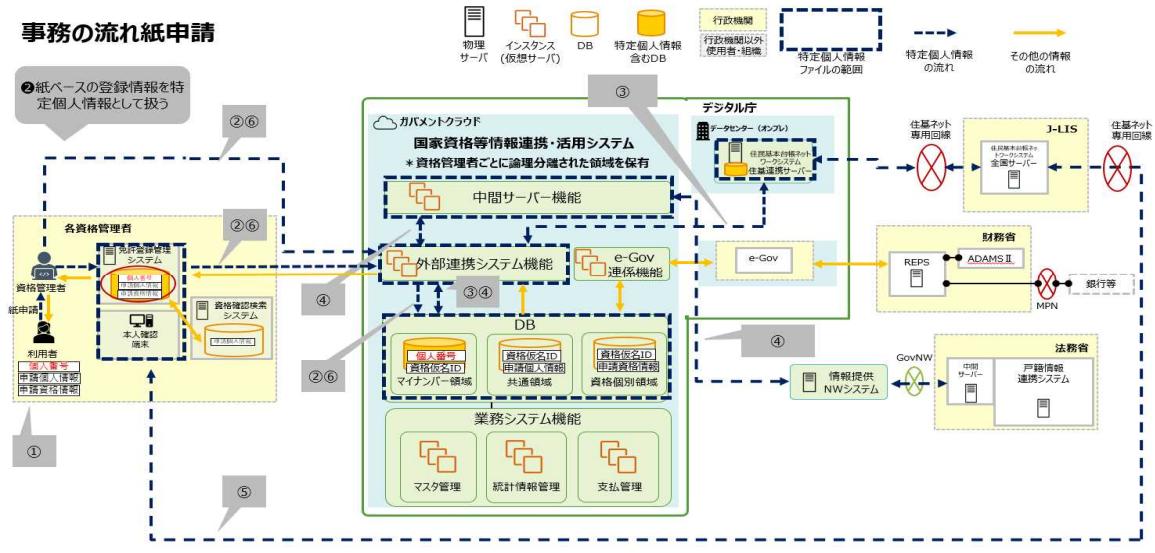
注１）外部連携システム機能を介して連携された資格情報のうち、個人番号は資格情報と直接紐づけるのではなく、資格仮名IDと呼ばれる資格保有者等を一意に識別するためのID情報と一度紐づけた後に、資格情報と紐づける。個人番号と資格仮名IDを結びつけるテーブルは、他のテーブルとは独立して設ける。
注２）戸籍情報については国家資格等情報連携・活用システムに設置する中間サーバー機能において情報提供ネットワークシステムを介して連携し取得する。戸籍情報の要求については個人番号と紐付く機関別符号を用いて行う。

（別添1）事務の内容

薬剤師名簿ファイル







（備考）

【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（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。

【特定個人情報の流れ】

■オンライン申請の場合
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（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、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、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、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、各資格管理者が保有する免許登録管理システム経由若しくは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。

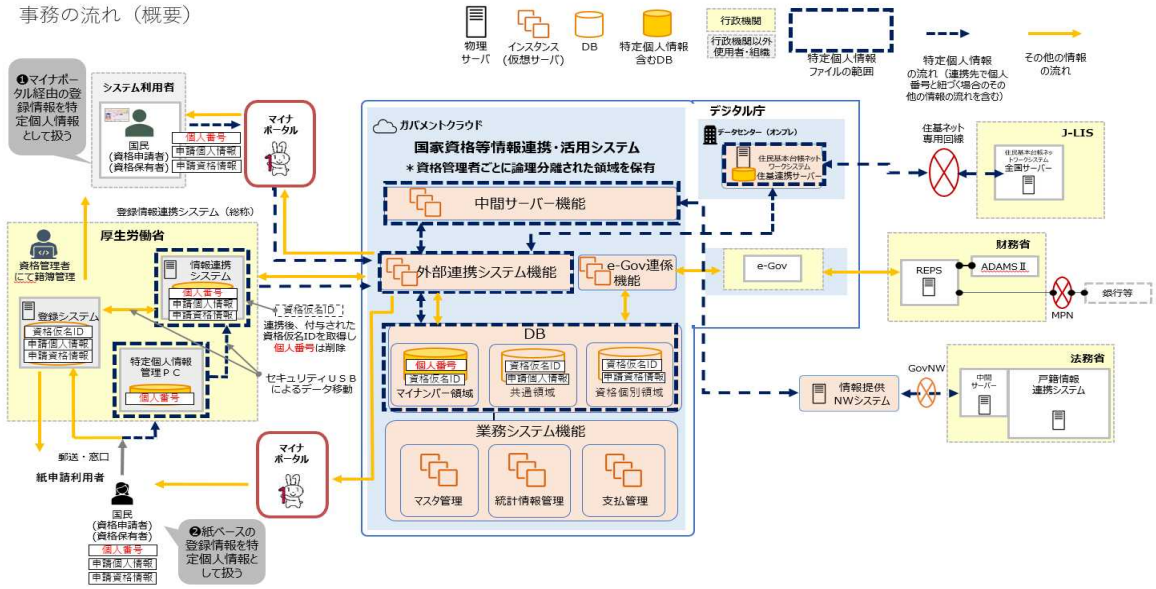
■紙による申請の場合
①紙の申請書において提出された資格情報について、資格保有者本人であることの確認及び個人番号の確認を行う。
②申請された資格情報（個人番号含む）は外部連携システム機能と連携し、各資格管理者が保有する免許登録管理システム経由若しくは直接国家資格等情報連携・活用システムに登録を行う。
③登録された情報については、住基法に定められた範囲内において一括方式による住民基本台帳ネットワークシステムを利用した情報連携を行い、本人確認情報等の確認を行う。また、外部連携システム機能において住民基本台帳ネットワークシステムに対して定期に実施する照会処理により取得した照会結果を連携をすることで正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、各資格管理者が保有する免許登録管理システム経由若しくは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等情報連携・活用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。

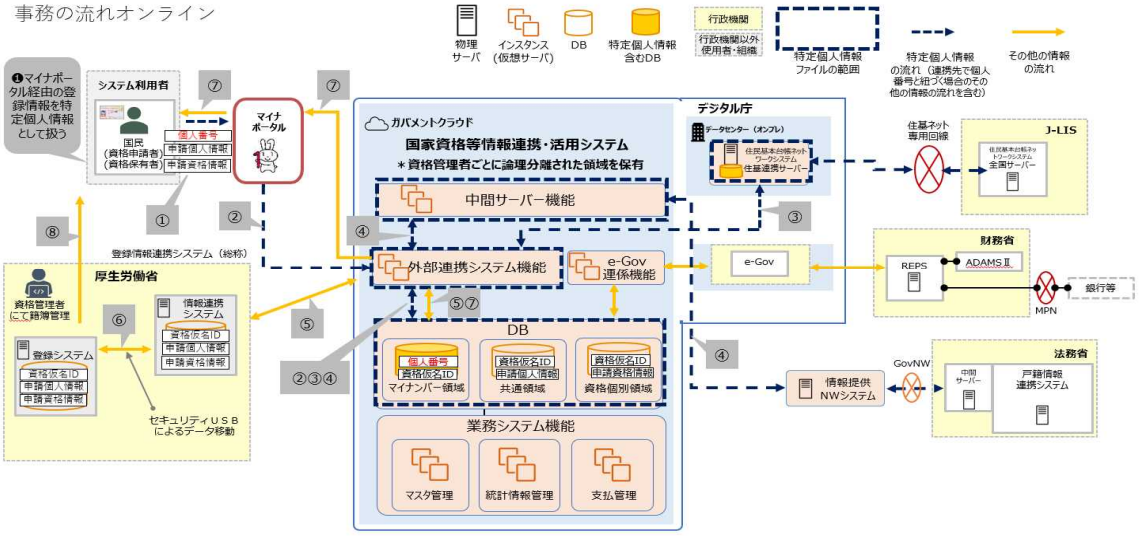
（別添1）事務の内容

介護福祉士登録名簿ファイル

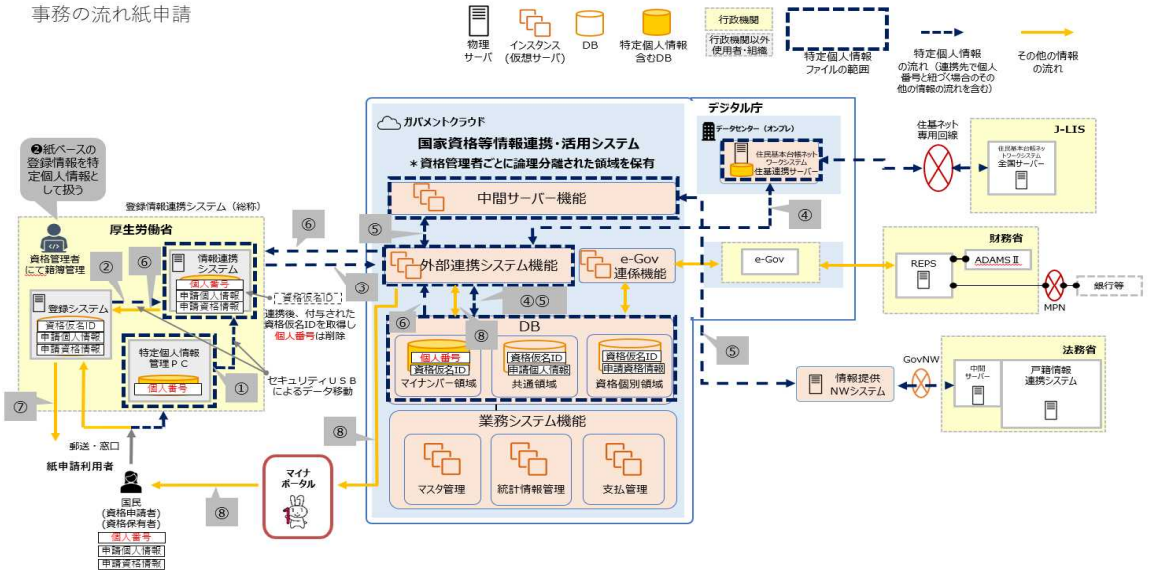
事務の流れ（概要）



事務の流れオンライン



事務の流れ紙申請



（備考）

【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（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。

【特定個人情報の流れ】

■オンライン申請の場合
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（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、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、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、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国家資格等情報連携・活用システムで採番された資格仮名ID及び特定個人情報を含まない資格登録情報を登録情報連携システムに情報連携を行う。
　また、⑥を経て資格仮名IDをキーとして、登録番号が付番された資格登録情報を国家資格等情報連携・活用システムに情報連携を行う。
⑥資格管理者において登録番号を採番し、籍簿に登録（更新）を行う。
⑦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。
⑧紙の資格証の発行を行う。

■紙による申請の場合
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本人確認書類で個人番号の確認を行い、特定個人情報管理PCで入力し、セキュリティUSBを用いて登録情報連携システムにデータ移動を行う。
②申請された資格情報（個人番号含まない）は、登録システムにおいて登録番号を採番し、籍簿に登録し、セキュリティUSBを用いて登録情報連携システムにデータ移動を行う。
③登録情報連携システムで登録システムのデータと特定個人情報管理PCのデータを紐づけ、外部連携システム機能と連携し、国家資格等情報連携・活用システムに登録を行う。
④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、外部連携システム機能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。
⑤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。
⑥国家資格等情報連携・活用システムで採番された資格仮名ID及び特定個人情報を含まない資格情報を登録情報連携システムに情報連携を行う。
⑦紙の資格証の発行を行う。
⑧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。

注1）外部連携システム機能を介して連携された資格登録情報のうち、個人番号は資格登録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、資格登録情報と紐づける。
　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等情報連携・活用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。

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		
医籍等ファイル		
2. 基本情報		
①ファイルの種類 ※		[　　システム用ファイル　　] ＜選択肢＞ 1）システム用ファイル 2）その他の電子ファイル（表計算ファイル等）
②対象となる本人の数		[　100万人以上1,000万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
③対象となる本人の範囲 ※		医師免許、歯科医師免許、保健師免許、助産師免許、看護師免許、理学療法士免許及び臨床検査技師免許の登録者
	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		[　　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　（　資格仮名ID、マイナポータル仮名ID、資格情報、本籍情報　）
	その妥当性	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		医政局医事課試験免許室、歯科保健課、看護課

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 （ 地方公共団体情報システム機構、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　別表第一の15,16,17,41,69（未施行）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 ※		医政局医事課試験免許室、歯科保健課、看護課
	使用者数	[1,000人以上]	＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
⑧使用方法 ※			・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			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

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
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体] <選択肢> 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	[100万人以上1,000万人未満] <選択肢> 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲 ※	医師資格登録者、歯科医師資格登録者、看護師資格登録者、保健師資格登録者、助産師資格登録者、理学療法士資格登録者、臨床検査技師資格登録者
	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		[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		免許登録管理システムの運用等業務
①委託内容		免許登録管理システムの運用保守等業務
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一部]　＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	[100万人以上1,000万人未満]　＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲 ※	医師資格登録者、歯科医師資格登録者、看護師資格登録者、保健師資格登録者、助産師資格登録者、理学療法士資格登録者、臨床検査技師資格登録者
	その妥当性	システム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		株式会社セック
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 [　] 電子メール [　] フラッシュメモリ [　] その他　（	[　] 専用線 [　] 電子記録媒体（フラッシュメモリを除く。） [　] 紙 ）
⑦時期・頻度		
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（共通して記載）】 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。 【免許登録管理システムに係る部分】 ・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。 ・ソフトウェア・情報資産は関係者以外はアクセスできないよう制限し、適切にバックアップ、バージョン管理を行う。
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（共通して記載）】 ・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。 「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。 「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。 【免許登録管理システムに係る部分】 ・作成したデータ等について、不要となった場合又は廃棄を指示した場合には、回復が困難な方法により速やかに廃棄するとともに、廃棄の実施方法については、情報抹消に係る作業実施報告書を提出させ、廃棄方法に問題ないか確認する。
7. 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		
管理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 ※		管理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		[　　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　（　資格情報（登録番号、登録年月日、管理栄養士国家試験の合格の年月、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	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		厚生労働省健康局健康課

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 （ 地方公共団体情報システム機構、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 ※	厚生労働省健康局健康課・各都道府県・各保健所
	使用者数	[1,000人以上] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
⑧使用方法 ※		・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		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

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
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 ※	管理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		免許証作成電算処理業務
①委託内容		入力作業・免許証出力
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　※	管理栄養士資格の登録者
	その妥当性	業務の効率化及び合理化を図る観点から、免許証作成電算処理業務を外部に委託するもの。
③委託先における取扱者数		[　100人以上500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		委託業務の調達結果については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 [　] 電子メール [　] フラッシュメモリ [　] その他　（　）	[　] 専用線 [　] 電子記録媒体（フラッシュメモリを除く。） [　] 紙
⑦時期・頻度		
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　※	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。	
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。 「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。
7. 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		
薬剤師名簿ファイル		
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 ※		薬剤師資格の登録者
	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		[　　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　（　資格仮名ID,マイナポータル仮名ID,資格情報,本籍情報　）
	その妥当性	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		厚生労働省医薬・生活衛生局総務課

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 （ 地方公共団体情報システム機構、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　別表第一の53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 ※	厚生労働省医薬・生活衛生局総務課試験免許係
	使用者数	[1,000人以上] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
⑧使用方法 ※		・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		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

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
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 ※	薬剤師資格登録者
	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		[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		免許登録管理システムの運用等業務
①委託内容		免許登録管理システムの運用保守等業務
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 ※	薬剤師資格登録者
	その妥当性	システム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		株式会社セック
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 [　] 電子メール [　] フラッシュメモリ [　] その他　（　）	[　] 専用線 [　] 電子記録媒体（フラッシュメモリを除く。） [　] 紙
⑦時期・頻度		
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（共通して記載）】 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。 【免許登録管理システムに係る部分】 ・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。 ・ソフトウェア・情報資産は関係者以外はアクセスできないよう制限し、適切にバックアップ、バージョン管理を行う。
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（共通して記載）】 ・国家資格管理事務に係る資格情報等は、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。免許を返納した者や行政処分により資格が喪失となった者といった生者の個人番号についてはデータの物理削除を行う。 ・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。 「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。 【免許登録管理システムに係る部分】 ・作成したデータ等について、不要となった場合又は廃棄を指示した場合には、回復が困難な方法により速やかに廃棄するとともに、廃棄の実施方法については、情報抹消に係る作業実施報告書を提出させ、廃棄方法に問題ないか確認する。
7．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		
介護福祉士登録名簿ファイル		
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		[　100万人以上1,000万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
③対象となる本人の範囲 ※		介護福祉士資格の登録者 （個人番号は国家資格等情報連携・活用システムに連携後は保有なし）
	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		[　　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　（ 資格仮名ID、マイナポータル仮名ID、資格情報、本籍情報 ）
	その妥当性	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		厚生労働省社会・援護局福祉基盤課

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 （ 地方公共団体情報システム機構、法務省 ） [ ] 地方公共団体・地方独立行政法人 （ ） [ ] 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87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 ※		厚生労働省社会・援護局福祉基盤課
	使用者数	[10人以上50人未満]	＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
⑧使用方法 ※			・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			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

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
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体] <選択肢> 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	[100万人以上1,000万人未満] <選択肢> 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲 ※	介護福祉士資格登録者
	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		[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		登録情報連携システムの運用等業務
①委託内容		登録情報連携システム運用環境に係るシステムの運用保守・入力等業務
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	[100万人以上1,000万人未満] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲 ※	介護福祉士資格登録者
	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。 ・業務の効率化及び合理化を図る観点から、申請データ等の入力業務を外部に委託する。
③委託先における取扱者数		[10人以上50人未満] ＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[ ]専用線　[ ]電子メール　[ ]電子記録媒体（フラッシュメモリを除く。） [ ]フラッシュメモリ　[○]紙 [ ]その他　（　　）
⑤委託先名の確認方法		委託業務の調達等に関して、電話、メール、文書等の照会により確認可能
⑥委託先名		日本情報産業株式会社
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
再委託	⑧再委託の許諾方法	
再委託	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 [　] 電子メール [　] フラッシュメモリ [　] その他　（　）	[　] 専用線 [　] 電子記録媒体（フラッシュメモリを除く。） [　] 紙
⑦時期・頻度		
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（共通して記載）】 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。 【登録情報連携システムに係る部分】 電子記録媒体は、情報の暗号化を行うとともに、入退室の記録を取得し、入退室制限等の物理的なアクセス制御手段により、特定者以外の入室を制限し、管理区域内で保管する。
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	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（共通して記載）】 ・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。 「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。 「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。 【登録情報連携システムに係る部分】 ・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。
7．備考	

（別添2）特定個人情報ファイル記録項目

（医籍等ファイル）
【医師】
1 資格仮名ID
2 マイナポータル仮名ID
名簿情報
3 登録ID
4 登録番号
5 職種コード
6 進達県コード
7 受付年月日
8 登録年月日
9 受験番号
10 国家試験回数
11 国家試験実施年
12 受験地コード
13 国家試験合格年月日
14 旧登録県コード
15 旧登録番号
16 旧登録年月日
17 本籍地コード
18 姓
19 名
20 フリガナ（姓）
21 フリガナ（名）
22 通称（姓）
23 通称（名）
24 フリガナ（通称：姓）
25 フリガナ（通称：名）
26 生年月日
27 性別コード
28 籍訂正年月日
29 籍訂正理由コード
30 籍訂正理由（記事）
31 再交付年月日
32 再交付理由コード
33 再交付理由（記事）
34 まっ消年月日
35 まっ消理由コード
36 まっ消理由（記事）
37 登録換年月日
38 登録換理由コード
39 登録換理由（記事）
40 歴代大臣コード
41 歴代局長コード
42 出身校コード
43 件数
44 処理区分コード
45 エントリー区分コード
46 罰金刑区分
47 備考1
48 備考2
49 備考3
50 備考4
51 備考5
52 合格職種コード
53 メモ
54 歴代医務技監コード
55 旧姓
56 フリガナ（旧姓）
57 認定年月日
58 申請厚生局
59 認定番号
60 住所
61 電話番号
62 メールアドレス
63 メールアドレス（利用同意）
64 従事している業務の種別

64 従事している業務の種別
65 主たる従事先(名称)
66 主たる従事先(電話)
67 主たる従事先(所在地)
68 勤務状況(勤務日数)
69 勤務状況(宿直・日直回数)
70 就業形態
71 主たる業務内容
72 休業の取得
73 従たる従事先(名称)
74 従たる従事先(電話)
75 従たる従事先(所在地)
76 勤務状況(勤務日数)
77 勤務状況(宿直・日直回数)
78 従たる従事先の件数
79 従事する診療科名等
80 取得している広告可能な医師の専門性に関する資格名及び麻酔科の標榜資格
81 分娩の取扱いの有無
82 出身地
83 医学課程を修めた外国の医学校のある国
84 地域枠等(従事要件有無)
85 地域枠等(従事年数)
86 地域枠等(終了しているか)
87 地域枠等(要件となる従事場所)
88 地域枠等(奨学金貸与元)
89 地域枠等(選抜方式)
90 医師届出票の活用に関する確認
91 備考
92 再教育研修終了登録日
93 再教育研修命令登録日
職種マスタ情報
94 職種コード
95 籍名簿コード
96 課長コード
97 職種名(和名)
98 職種名(英名)
99 法律名(英名)
100 シーケンス名
101 備考
102 登録端末No
103 登録日時
104 更新端末No
105 更新日時
本籍地マスタ情報
106 本籍地コード
107 本籍地(和名)
108 本籍地(和名(表示用))
109 本籍地(英名)
110 略号
111 外国フラグ
112 備考
113 登録端末No
114 登録日時
115 更新端末No
116 更新日時
受験地マスタ情報
117 受験地コード
118 受験地名
119 備考
120 登録端末No
121 登録日時
122 更新端末No
123 更新日時
記事マスタ情報
124 理由コード
125 処理区分コード
126 理由
127 理由(略称)
128 備考
129 登録端末No
130 登録日時

131 更新端末No
132 更新日時
歴代大臣マスタ情報
133 歴代大臣コード
134 大臣名(和名)
135 大臣名(英名)
136 在位期間(開始)
137 在位期間(終了)
138 大臣種別コード
139 備考
140 登録端末No
141 登録日時
142 更新端末No
143 更新日時
歴代局長マスタ
144 歴代局長コード
145 局長名(和名)
146 局長名(英名)
147 在位期間(開始)
148 在位期間(終了)
149 局長種別コード
150 備考
151 登録端末No
152 登録日時
153 更新端末No
154 更新日時
出身校マスタ情報
155 出身校コード
156 出身校名
157 備考
158 登録端末No
159 登録日時
160 更新端末No
161 更新日時
歴代医務技監マスタ情報
162 歴代医務技監コード
163 医務技監名(和名)
164 医務技監名(英名)
165 在位期間(開始)
166 在位期間(終了)
167 医務技監種別コード
168 備考
169 登録端末No
170 登録日時
171 更新端末No
172 更新日時
本人確認情報照会結果ファイル
173 要求レコード番号
174 提供事務区分
175 個人番号提供事務区分
176 対象者識別情報
177 照会対象期間(開始年月日)
178 照会対象期間(終了年月日)
179 照会基準日
180 消除者の要否
181 対象者住民票コード
182 対象者氏名(漢字)
183 対象者氏名(かな)
184 対象者生年月日
185 対象者性別
186 対象者住所
187 対象者住所(市町村コード)
188 対象者個人番号
189 予備
190 処理結果コード
191 照会結果レコード数
192 照会結果レコード連番
193 照会一致項目
194 異動有無
195 生存状況
196 変更状況

196 変更状況
197 住民票コード
198 氏名（漢字）
199 氏名（かな）
200 生年月日
201 性別
202 住所
203 個人番号
204 異動事由
205 異動年月日
206 外字情報（氏名外字数）
207 外字情報（住所外字数）
208 外字データレコード数
209 市町村コード
210 不参加団体対象フラグ
211 検索パターン番号
212 旧氏（漢字）
213 旧氏（かな）
214 旧氏外字数
215 予備
戸籍関係情報
216 情報提供起点日
217 戸籍異動日
218 戸籍異動事由区分
219 本籍コード
220 出生地
221 国籍取得日
222 取得事由区分
223 国籍喪失日
224 喪失事由区分
225 国籍の得喪の取消し・無効日
226 国籍の得喪の取消し・無効区分
227 死亡日
228 死亡事由区分
229 死亡の取消し・無効日
230 死亡の取消し・無効区分
231 死亡日の不詳・推定区分
個人番号関係情報
232 個人番号
233 機関別符号

（別添２） 特定個人情報ファイル記録項目

（医籍等ファイル）
【歯科医師】
1 資格仮名ID
2 マイナポータル仮名ID
名簿情報
3 姓
4 名
5 フリガナ（姓）
6 フリガナ（名）
7 生年月日
8 性別コード
9 登録番号
10 登録年月日
11 住所
12 電話番号
13 メールアドレス
14 メールアドレス（利用同意）
15 従事している業務の種別
16 主たる従事先（名称）
17 主たる従事先（電話）
18 主たる従事先（所在地）
19 就業形態
20 主たる業務内容
21 休業の取得
22 従たる従事先（名称）
23 従たる従事先（電話）
24 従たる従事先（所在地）
25 従事する診療科名等
26 取得している広告可能な歯科医師の専門性に関する資格名
27 歯科医師免許取得の際に歯学課程を修めた大学名等
28 出身地
29 歯科医師届出票の活用に関する確認
30 備考
31 登録ID
32 登録番号
33 職種コード
34 進達県コード
35 受付年月日
36 登録年月日
37 受験番号
38 国家試験回数
39 国家試験実施年
40 受験地コード
41 国家試験合格年月日
42 旧登録県コード
43 旧登録番号
44 旧登録年月日
45 本籍地コード
46 姓
47 名
48 フリガナ（姓）
49 フリガナ（名）
50 通称（姓）
51 通称（名）
52 フリガナ（通称：姓）
53 フリガナ（通称：名）
54 生年月日

55 性別コード
56 籍訂正年月日
57 籍訂正理由コード
58 籍訂正理由(記事)
59 再交付年月日
60 再交付理由コード
61 再交付理由(記事)
62 まっ消年月日
63 まっ消理由コード
64 まっ消理由(記事)
65 登録換年月日
66 登録換理由コード
67 登録換理由(記事)
68 歴代大臣コード
69 歴代局長コード
70 出身校コード
71 件数
72 処理区分コード
73 エントリー区分コード
74 罰金刑区分
75 備考1
76 備考2
77 備考3
78 備考4
79 備考5
80 合格職種コード
81 メモ
82 歴代医務技監コード
83 旧姓
84 フリガナ(旧姓)
85 認定年月日
86 申請厚生局
87 認定番号
88 再教育研修終了登録日
89 再教育研修命令登録日
職種マスタ情報
90 職種コード
91 籍名簿コード
92 課長コード
93 職種名(和名)
94 職種名(英名)
95 法律名(英名)
96 シーケンス名
97 備考
98 登録端末No
99 登録日時
100 更新端末No
101 更新日時
本籍地マスタ
102 本籍地コード
103 本籍地(和名)
104 本籍地(和名(表示用))
105 本籍地(英名)
106 略号
107 外国フラグ
108 備考
109 登録端末No
110 登録日時
111 更新端末No

112 更新日時
受験地マスタ
113 受験地コード
114 受験地名
115 備考
116 登録端末No
117 登録日時
118 更新端末No
119 更新日時
記事マスタ
120 理由コード
121 処理区分コード
122 理由
123 理由(略称)
124 備考
125 登録端末No
126 登録日時
127 更新端末No
128 更新日時
歴代大臣マスタ
129 歴代大臣コード
130 大臣名(和名)
131 大臣名(英名)
132 在位期間(開始)
133 在位期間(終了)
134 大臣種別コード
135 備考
136 登録端末No
137 登録日時
138 更新端末No
139 更新日時
歴代局長マスタ
140 歴代局長コード
141 局長名(和名)
142 局長名(英名)
143 在位期間(開始)
144 在位期間(終了)
145 局長種別コード
146 備考
147 登録端末No
148 登録日時
149 更新端末No
150 更新日時
出身校マスタ
151 出身校コード
152 出身校名
153 備考
154 登録端末No
155 登録日時
156 更新端末No
157 更新日時
歴代医務技監マスタ
158 歴代医務技監コード
159 医務技監名(和名)
160 医務技監名(英名)
161 在位期間(開始)
162 在位期間(終了)
163 医務技監種別コード
164 備考

165 登録端末No
166 登録日時
167 更新端末No
168 更新日時
本人確認情報照会結果ファイル
169 要求レコード番号
170 提供事務区分
171 個人番号提供事務区分
172 対象者識別情報
173 照会対象期間(開始年月日)
174 照会対象期間(終了年月日)
175 照会基準日
176 消除者の要否
177 対象者住民票コード
178 対象者氏名(漢字)
179 対象者氏名(かな)
180 対象者生年月日
181 対象者性別
182 対象者住所
183 対象者住所(市町村コード)
184 対象者個人番号
185 予備
186 処理結果コード
187 照会結果レコード数
188 照会結果レコード連番
189 照会一致項目
190 異動有無
191 生存状況
192 変更状況
193 住民票コード
194 氏名(漢字)
195 氏名(かな)
196 生年月日
197 性別
198 住所
199 個人番号
200 異動事由
201 異動年月日
202 外字情報(氏名外字数)
203 外字情報(住所外字数)
204 外字データレコード数
205 市町村コード
206 不参加団体対象フラグ
207 検索パターン番号
208 旧氏(漢字)
209 旧氏(かな)
210 旧氏外字数
211 予備
戸籍関係情報
212 情報提供起点日
213 戸籍異動日
214 戸籍異動事由区分
215 本籍コード
216 出生地
217 国籍取得日
218 取得事由区分
219 国籍喪失日
220 喪失事由区分
221 国籍の得喪の取消し・無効日

222 国籍の得喪の取消し・無効区分
223 死亡日
224 死亡事由区分
225 死亡の取消し・無効日
226 死亡の取消し・無効区分
227 死亡日の不詳・推定区分
個人番号関係情報
228 個人番号
229 機関別符号

（別添２） 特定個人情報ファイル記録項目

（医籍等ファイル）
【看護師】
1 資格仮名ID
2 マイナポータル仮名ID
名簿情報
3 登録ID
4 登録番号
5 職種コード
6 進達県コード
7 受付年月日
8 登録年月日
9 受験番号
10 国家試験回数
11 国家試験実施年
12 受験地コード
13 国家試験合格年月日
14 旧登録県コード
15 旧登録番号
16 旧登録年月日
17 本籍地コード
18 姓
19 名
20 フリガナ（姓）
21 フリガナ（名）
22 通称（姓）
23 通称（名）
24 フリガナ（通称：姓）
25 フリガナ（通称：名）
26 生年月日
27 性別コード
28 籍訂正年月日
29 籍訂正理由コード
30 籍訂正理由（記事）
31 再交付年月日
32 再交付理由コード
33 再交付理由（記事）
34 まっ消年月日
35 まっ消理由コード
36 まっ消理由（記事）
37 登録換年月日
38 登録換理由コード
39 登録換理由（記事）
40 歴代大臣コード
41 歴代局長コード
42 出身校コード
43 件数
44 処理区分コード
45 エントリー区分コード
46 罰金刑区分
47 備考1
48 備考2
49 備考3
50 備考4
51 備考5
52 合格職種コード
53 メモ
54 歴代医務技監コード

55 旧姓
56 フリガナ(旧姓)
57 認定年月日
58 申請厚生局
59 認定番号
60 再教育研修終了登録日
61 再教育研修命令登録日
62 住所
職種マスタ
63 職種コード
64 籍名簿コード
65 課長コード
66 職種名(和名)
67 職種名(英名)
68 法律名(英名)
69 シーケンス名
70 備考
71 登録端末No
72 登録日時
73 更新端末No
74 更新日時
本籍地マスタ
75 本籍地コード
76 本籍地(和名)
77 本籍地(和名(表示用))
78 本籍地(英名)
79 略号
80 外国フラグ
81 備考
82 登録端末No
83 登録日時
84 更新端末No
85 更新日時
受験地マスタ
86 受験地コード
87 受験地名
88 備考
89 登録端末No
90 登録日時
91 更新端末No
92 更新日時
記事マスタ
93 理由コード
94 処理区分コード
95 理由
96 理由(略称)
97 備考
98 登録端末No
99 登録日時
100 更新端末No
101 更新日時
歴代大臣マスタ
102 歴代大臣コード
103 大臣名(和名)
104 大臣名(英名)
105 在位期間(開始)
106 在位期間(終了)
107 大臣種別コード
108 備考

109 登録端末No
110 登録日時
111 更新端末No
112 更新日時
歴代局長マスタ
113 歴代局長コード
114 局長名(和名)
115 局長名(英名)
116 在位期間(開始)
117 在位期間(終了)
118 局長種別コード
119 備考
120 登録端末No
121 登録日時
122 更新端末No
123 更新日時
出身校マスタ
124 出身校コード
125 出身校名
126 備考
127 登録端末No
128 登録日時
129 更新端末No
130 更新日時
歴代医務技監マスタ
131 歴代医務技監コード
132 医務技監名(和名)
133 医務技監名(英名)
134 在位期間(開始)
135 在位期間(終了)
136 医務技監種別コード
137 備考
138 登録端末No
139 登録日時
140 更新端末No
141 更新日時
本人確認情報照会結果ファイル
142 要求レコード番号
143 提供事務区分
144 個人番号提供事務区分
145 対象者識別情報
146 照会対象期間(開始年月日)
147 照会対象期間(終了年月日)
148 照会基準日
149 消除者の要否
150 対象者住民票コード
151 対象者氏名(漢字)
152 対象者氏名(かな)
153 対象者生年月日
154 対象者性別
155 対象者住所
156 対象者住所(市町村コード)
157 対象者個人番号
158 予備
159 処理結果コード
160 照会結果レコード数
161 照会結果レコード連番
162 照会一致項目
163 異動有無

164 生存状況
165 変更状況
166 住民票コード
167 氏名（漢字）
168 氏名（かな）
169 生年月日
170 性別
171 住所
172 個人番号
173 異動事由
174 異動年月日
175 外字情報（氏名外字数）
176 外字情報（住所外字数）
177 外字データレコード数
178 市町村コード
179 不参加団体対象フラグ
180 検索パターン番号
181 旧氏（漢字）
182 旧氏（かな）
183 旧氏外字数
184 予備
戸籍関係情報
185 情報提供起点日
186 戸籍異動日
187 戸籍異動事由区分
188 本籍コード
189 出生地
190 国籍取得日
191 取得事由区分
192 国籍喪失日
193 喪失事由区分
194 国籍の得喪の取消し・無効日
195 国籍の得喪の取消し・無効区分
196 死亡日
197 死亡事由区分
198 死亡の取消し・無効日
199 死亡の取消し・無効区分
200 死亡日の不詳・推定区分
個人番号関係情報
201 個人番号
202 機関別符号

（別添２） 特定個人情報ファイル記録項目

（医籍等ファイル）
【保健師】
1 資格仮名ID
2 マイナポータル仮名ID
名簿情報
3 登録ID
4 登録番号
5 職種コード
6 進達県コード
7 受付年月日
8 登録年月日
9 受験番号
10 国家試験回数
11 国家試験実施年
12 受験地コード
13 国家試験合格年月日
14 旧登録県コード
15 旧登録番号
16 旧登録年月日
17 本籍地コード
18 姓
19 名
20 フリガナ（姓）
21 フリガナ（名）
22 通称（姓）
23 通称（名）
24 フリガナ（通称：姓）
25 フリガナ（通称：名）
26 生年月日
27 性別コード
28 籍訂正年月日
29 籍訂正理由コード
30 籍訂正理由（記事）
31 再交付年月日
32 再交付理由コード
33 再交付理由（記事）
34 まっ消年月日
35 まっ消理由コード
36 まっ消理由（記事）
37 登録換年月日
38 登録換理由コード
39 登録換理由（記事）
40 歴代大臣コード
41 歴代局長コード
42 出身校コード
43 件数
44 処理区分コード
45 エントリー区分コード
46 罰金刑区分
47 備考1
48 備考2
49 備考3
50 備考4
51 備考5
52 合格職種コード
53 メモ
54 歴代医務技監コード

55 旧姓
56 フリガナ(旧姓)
57 認定年月日
58 申請厚生局
59 認定番号
60 再教育研修終了登録日
61 再教育研修命令登録日
62 住所
職種マスタ
63 職種コード
64 籍名簿コード
65 課長コード
66 職種名(和名)
67 職種名(英名)
68 法律名(英名)
69 シーケンス名
70 備考
71 登録端末No
72 登録日時
73 更新端末No
74 更新日時
本籍地マスタ
75 本籍地コード
76 本籍地(和名)
77 本籍地(和名(表示用))
78 本籍地(英名)
79 略号
80 外国フラグ
81 備考
82 登録端末No
83 登録日時
84 更新端末No
85 更新日時
受験地マスタ
86 受験地コード
87 受験地名
88 備考
89 登録端末No
90 登録日時
91 更新端末No
92 更新日時
記事マスタ
93 理由コード
94 処理区分コード
95 理由
96 理由(略称)
97 備考
98 登録端末No
99 登録日時
100 更新端末No
101 更新日時
歴代大臣マスタ
102 歴代大臣コード
103 大臣名(和名)
104 大臣名(英名)
105 在位期間(開始)
106 在位期間(終了)
107 大臣種別コード
108 備考

109 登録端末No
110 登録日時
111 更新端末No
112 更新日時
歴代局長マスタ
113 歴代局長コード
114 局長名(和名)
115 局長名(英名)
116 在位期間(開始)
117 在位期間(終了)
118 局長種別コード
119 備考
120 登録端末No
121 登録日時
122 更新端末No
123 更新日時
出身校マスタ
124 出身校コード
125 出身校名
126 備考
127 登録端末No
128 登録日時
129 更新端末No
130 更新日時
歴代医務技監マスタ
131 歴代医務技監コード
132 医務技監名(和名)
133 医務技監名(英名)
134 在位期間(開始)
135 在位期間(終了)
136 医務技監種別コード
137 備考
138 登録端末No
139 登録日時
140 更新端末No
141 更新日時
本人確認情報照会結果ファイル
142 要求レコード番号
143 提供事務区分
144 個人番号提供事務区分
145 対象者識別情報
146 照会対象期間(開始年月日)
147 照会対象期間(終了年月日)
148 照会基準日
149 消除者の要否
150 対象者住民票コード
151 対象者氏名(漢字)
152 対象者氏名(かな)
153 対象者生年月日
154 対象者性別
155 対象者住所
156 対象者住所(市町村コード)
157 対象者個人番号
158 予備
159 処理結果コード
160 照会結果レコード数
161 照会結果レコード連番
162 照会一致項目
163 異動有無

164 生存状況
165 変更状況
166 住民票コード
167 氏名（漢字）
168 氏名（かな）
169 生年月日
170 性別
171 住所
172 個人番号
173 異動事由
174 異動年月日
175 外字情報（氏名外字数）
176 外字情報（住所外字数）
177 外字データレコード数
178 市町村コード
179 不参加団体対象フラグ
180 検索パターン番号
181 旧氏（漢字）
182 旧氏（かな）
183 旧氏外字数
184 予備
戸籍関係情報
185 情報提供起点日
186 戸籍異動日
187 戸籍異動事由区分
188 本籍コード
189 出生地
190 国籍取得日
191 取得事由区分
192 国籍喪失日
193 喪失事由区分
194 国籍の得喪の取消し・無効日
195 国籍の得喪の取消し・無効区分
196 死亡日
197 死亡事由区分
198 死亡の取消し・無効日
199 死亡の取消し・無効区分
200 死亡日の不詳・推定区分
個人番号関係情報
201 個人番号
202 機関別符号

（別添２） 特定個人情報ファイル記録項目

（医籍等ファイル）
【助産師】
1 資格仮名ID
2 マイナポータル仮名ID
名簿情報
3 登録ID
4 登録番号
5 職種コード
6 進達県コード
7 受付年月日
8 登録年月日
9 受験番号
10 国家試験回数
11 国家試験実施年
12 受験地コード
13 国家試験合格年月日
14 旧登録県コード
15 旧登録番号
16 旧登録年月日
17 本籍地コード
18 姓
19 名
20 フリガナ（姓）
21 フリガナ（名）
22 通称（姓）
23 通称（名）
24 フリガナ（通称：姓）
25 フリガナ（通称：名）
26 生年月日
27 性別コード
28 籍訂正年月日
29 籍訂正理由コード
30 籍訂正理由（記事）
31 再交付年月日
32 再交付理由コード
33 再交付理由（記事）
34 まっ消年月日
35 まっ消理由コード
36 まっ消理由（記事）
37 登録換年月日
38 登録換理由コード
39 登録換理由（記事）
40 歴代大臣コード
41 歴代局長コード
42 出身校コード
43 件数
44 処理区分コード
45 エントリー区分コード
46 罰金刑区分
47 備考1
48 備考2
49 備考3
50 備考4
51 備考5
52 合格職種コード
53 メモ
54 歴代医務技監コード

55 旧姓
56 フリガナ(旧姓)
57 認定年月日
58 申請厚生局
59 認定番号
60 再教育研修終了登録日
61 再教育研修命令登録日
62 住所
職種マスタ
63 職種コード
64 籍名簿コード
65 課長コード
66 職種名(和名)
67 職種名(英名)
68 法律名(英名)
69 シーケンス名
70 備考
71 登録端末No
72 登録日時
73 更新端末No
74 更新日時
本籍地マスタ
75 本籍地コード
76 本籍地(和名)
77 本籍地(和名(表示用))
78 本籍地(英名)
79 略号
80 外国フラグ
81 備考
82 登録端末No
83 登録日時
84 更新端末No
85 更新日時
受験地マスタ
86 受験地コード
87 受験地名
88 備考
89 登録端末No
90 登録日時
91 更新端末No
92 更新日時
記事マスタ
93 理由コード
94 処理区分コード
95 理由
96 理由(略称)
97 備考
98 登録端末No
99 登録日時
100 更新端末No
101 更新日時
歴代大臣マスタ
102 歴代大臣コード
103 大臣名(和名)
104 大臣名(英名)
105 在位期間(開始)
106 在位期間(終了)
107 大臣種別コード
108 備考

109 登録端末No
110 登録日時
111 更新端末No
112 更新日時
歴代局長マスタ
113 歴代局長コード
114 局長名(和名)
115 局長名(英名)
116 在位期間(開始)
117 在位期間(終了)
118 局長種別コード
119 備考
120 登録端末No
121 登録日時
122 更新端末No
123 更新日時
出身校マスタ
124 出身校コード
125 出身校名
126 備考
127 登録端末No
128 登録日時
129 更新端末No
130 更新日時
歴代医務技監マスタ
131 歴代医務技監コード
132 医務技監名(和名)
133 医務技監名(英名)
134 在位期間(開始)
135 在位期間(終了)
136 医務技監種別コード
137 備考
138 登録端末No
139 登録日時
140 更新端末No
141 更新日時
本人確認情報照会結果ファイル
142 要求レコード番号
143 提供事務区分
144 個人番号提供事務区分
145 対象者識別情報
146 照会対象期間(開始年月日)
147 照会対象期間(終了年月日)
148 照会基準日
149 消除者の要否
150 対象者住民票コード
151 対象者氏名(漢字)
152 対象者氏名(かな)
153 対象者生年月日
154 対象者性別
155 対象者住所
156 対象者住所(市町村コード)
157 対象者個人番号
158 予備
159 処理結果コード
160 照会結果レコード数
161 照会結果レコード連番
162 照会一致項目
163 異動有無

164 生存状況
165 変更状況
166 住民票コード
167 氏名（漢字）
168 氏名（かな）
169 生年月日
170 性別
171 住所
172 個人番号
173 異動事由
174 異動年月日
175 外字情報（氏名外字数）
176 外字情報（住所外字数）
177 外字データレコード数
178 市町村コード
179 不参加団体対象フラグ
180 検索パターン番号
181 旧氏（漢字）
182 旧氏（かな）
183 旧氏外字数
184 予備
戸籍関係情報
185 情報提供起点日
186 戸籍異動日
187 戸籍異動事由区分
188 本籍コード
189 出生地
190 国籍取得日
191 取得事由区分
192 国籍喪失日
193 喪失事由区分
194 国籍の得喪の取消し・無効日
195 国籍の得喪の取消し・無効区分
196 死亡日
197 死亡事由区分
198 死亡の取消し・無効日
199 死亡の取消し・無効区分
200 死亡日の不詳・推定区分
個人番号関係情報
201 個人番号
202 機関別符号

（別添２） 特定個人情報ファイル記録項目

（医籍等ファイル）
【理学療法士】
1 資格仮名ID
2 マイナポータル仮名ID
名簿情報
3 登録ID
4 登録番号
5 職種コード
6 進達県コード
7 受付年月日
8 登録年月日
9 受験番号
10 国家試験回数
11 国家試験実施年
12 受験地コード
13 国家試験合格年月日
14 旧登録県コード
15 旧登録番号
16 旧登録年月日
17 本籍地コード
18 姓
19 名
20 フリガナ（姓）
21 フリガナ（名）
22 通称（姓）
23 通称（名）
24 フリガナ（通称：姓）
25 フリガナ（通称：名）
26 生年月日
27 性別コード
28 籍訂正年月日
29 籍訂正理由コード
30 籍訂正理由（記事）
31 再交付年月日
32 再交付理由コード
33 再交付理由（記事）
34 まっ消年月日
35 まっ消理由コード
36 まっ消理由（記事）
37 登録換年月日
38 登録換理由コード
39 登録換理由（記事）
40 歴代大臣コード
41 歴代局長コード
42 出身校コード
43 件数
44 処理区分コード
45 エントリー区分コード
46 罰金刑区分
47 備考1
48 備考2
49 備考3
50 備考4
51 備考5
52 合格職種コード
53 メモ
54 歴代医務技監コード

55 旧姓
56 フリガナ(旧姓)
57 認定年月日
58 申請厚生局
59 認定番号
職種マスタ
60 職種コード
61 籍名簿コード
62 課長コード
63 職種名(和名)
64 職種名(英名)
65 法律名(英名)
66 シーケンス名
67 備考
68 登録端末No
69 登録日時
70 更新端末No
71 更新日時
本籍地マスタ
72 本籍地コード
73 本籍地(和名)
74 本籍地(和名(表示用))
75 本籍地(英名)
76 略号
77 外国フラグ
78 備考
79 登録端末No
80 登録日時
81 更新端末No
82 更新日時
受験地マスタ
83 受験地コード
84 受験地名
85 備考
86 登録端末No
87 登録日時
88 更新端末No
89 更新日時
記事マスタ
90 理由コード
91 処理区分コード
92 理由
93 理由(略称)
94 備考
95 登録端末No
96 登録日時
97 更新端末No
98 更新日時
歴代大臣マスタ
99 歴代大臣コード
100 大臣名(和名)
101 大臣名(英名)
102 在位期間(開始)
103 在位期間(終了)
104 大臣種別コード
105 備考
106 登録端末No
107 登録日時
108 更新端末No

109 更新日時
歴代局長マスタ
110 歴代局長コード
111 局長名(和名)
112 局長名(英名)
113 在位期間(開始)
114 在位期間(終了)
115 局長種別コード
116 備考
117 登録端末No
118 登録日時
119 更新端末No
120 更新日時
出身校マスタ
121 出身校コード
122 出身校名
123 備考
124 登録端末No
125 登録日時
126 更新端末No
127 更新日時
歴代医務技監マスタ
128 歴代医務技監コード
129 医務技監名(和名)
130 医務技監名(英名)
131 在位期間(開始)
132 在位期間(終了)
133 医務技監種別コード
134 備考
135 登録端末No
136 登録日時
137 更新端末No
138 更新日時
本人確認情報照会結果ファイル
139 要求レコード番号
140 提供事務区分
141 個人番号提供事務区分
142 対象者識別情報
143 照会対象期間(開始年月日)
144 照会対象期間(終了年月日)
145 照会基準日
146 消除者の要否
147 対象者住民票コード
148 対象者氏名(漢字)
149 対象者氏名(かな)
150 対象者生年月日
151 対象者性別
152 対象者住所
153 対象者住所(市町村コード)
154 対象者個人番号
155 予備
156 処理結果コード
157 照会結果レコード数
158 照会結果レコード連番
159 照会一致項目
160 異動有無
161 生存状況
162 変更状況
163 住民票コード

164 氏名（漢字）
165 氏名（かな）
166 生年月日
167 性別
168 住所
169 個人番号
170 異動事由
171 異動年月日
172 外字情報（氏名外字数）
173 外字情報（住所外字数）
174 外字データレコード数
175 市町村コード
176 不参加団体対象フラグ
177 検索パターン番号
178 旧氏（漢字）
179 旧氏（かな）
180 旧氏外字数
181 予備
戸籍関係情報
182 情報提供起点日
183 戸籍異動日
184 戸籍異動事由区分
185 本籍コード
186 出生地
187 国籍取得日
188 取得事由区分
189 国籍喪失日
190 喪失事由区分
191 国籍の得喪の取消し・無効日
192 国籍の得喪の取消し・無効区分
193 死亡日
194 死亡事由区分
195 死亡の取消し・無効日
196 死亡の取消し・無効区分
197 死亡日の不詳・推定区分
個人番号関係情報
198 個人番号
199 機関別符号

（別添２） 特定個人情報ファイル記録項目

（医籍等ファイル）
【臨床検査技師】
1 資格仮名ID
2 マイナポータル仮名ID
名簿情報
3 登録ID
4 登録番号
5 職種コード
6 進達県コード
7 受付年月日
8 登録年月日
9 受験番号
10 国家試験回数
11 国家試験実施年
12 受験地コード
13 国家試験合格年月日
14 旧登録県コード
15 旧登録番号
16 旧登録年月日
17 本籍地コード
18 姓
19 名
20 フリガナ（姓）
21 フリガナ（名）
22 通称（姓）
23 通称（名）
24 フリガナ（通称：姓）
25 フリガナ（通称：名）
26 生年月日
27 性別コード
28 籍訂正年月日
29 籍訂正理由コード
30 籍訂正理由（記事）
31 再交付年月日
32 再交付理由コード
33 再交付理由（記事）
34 まっ消年月日
35 まっ消理由コード
36 まっ消理由（記事）
37 登録換年月日
38 登録換理由コード
39 登録換理由（記事）
40 歴代大臣コード
41 歴代局長コード
42 出身校コード
43 件数
44 処理区分コード
45 エントリー区分コード
46 罰金刑区分
47 備考1
48 備考2
49 備考3
50 備考4
51 備考5
52 合格職種コード
53 メモ
54 歴代医務技監コード

55 旧姓
56 フリガナ(旧姓)
57 認定年月日
58 申請厚生局
59 認定番号
職種マスタ
60 職種コード
61 籍名簿コード
62 課長コード
63 職種名(和名)
64 職種名(英名)
65 法律名(英名)
66 シーケンス名
67 備考
68 登録端末No
69 登録日時
70 更新端末No
71 更新日時
本籍地マスタ
72 本籍地コード
73 本籍地(和名)
74 本籍地(和名(表示用))
75 本籍地(英名)
76 略号
77 外国フラグ
78 備考
79 登録端末No
80 登録日時
81 更新端末No
82 更新日時
受験地マスタ
83 受験地コード
84 受験地名
85 備考
86 登録端末No
87 登録日時
88 更新端末No
89 更新日時
記事マスタ
90 理由コード
91 処理区分コード
92 理由
93 理由(略称)
94 備考
95 登録端末No
96 登録日時
97 更新端末No
98 更新日時
歴代大臣マスタ
99 歴代大臣コード
100 大臣名(和名)
101 大臣名(英名)
102 在位期間(開始)
103 在位期間(終了)
104 大臣種別コード
105 備考
106 登録端末No
107 登録日時
108 更新端末No

109 更新日時
歴代局長マスタ
110 歴代局長コード
111 局長名(和名)
112 局長名(英名)
113 在位期間(開始)
114 在位期間(終了)
115 局長種別コード
116 備考
117 登録端末No
118 登録日時
119 更新端末No
120 更新日時
出身校マスタ
121 出身校コード
122 出身校名
123 備考
124 登録端末No
125 登録日時
126 更新端末No
127 更新日時
歴代医務技監マスタ
128 歴代医務技監コード
129 医務技監名(和名)
130 医務技監名(英名)
131 在位期間(開始)
132 在位期間(終了)
133 医務技監種別コード
134 備考
135 登録端末No
136 登録日時
137 更新端末No
138 更新日時
本人確認情報照会結果ファイル
139 要求レコード番号
140 提供事務区分
141 個人番号提供事務区分
142 対象者識別情報
143 照会対象期間(開始年月日)
144 照会対象期間(終了年月日)
145 照会基準日
146 消除者の要否
147 対象者住民票コード
148 対象者氏名(漢字)
149 対象者氏名(かな)
150 対象者生年月日
151 対象者性別
152 対象者住所
153 対象者住所(市町村コード)
154 対象者個人番号
155 予備
156 処理結果コード
157 照会結果レコード数
158 照会結果レコード連番
159 照会一致項目
160 異動有無
161 生存状況
162 変更状況
163 住民票コード

164 氏名（漢字）
165 氏名（かな）
166 生年月日
167 性別
168 住所
169 個人番号
170 異動事由
171 異動年月日
172 外字情報（氏名外字数）
173 外字情報（住所外字数）
174 外字データレコード数
175 市町村コード
176 不参加団体対象フラグ
177 検索パターン番号
178 旧氏（漢字）
179 旧氏（かな）
180 旧氏外字数
181 予備
戸籍関係情報
182 情報提供起点日
183 戸籍異動日
184 戸籍異動事由区分
185 本籍コード
186 出生地
187 国籍取得日
188 取得事由区分
189 国籍喪失日
190 喪失事由区分
191 国籍の得喪の取消し・無効日
192 国籍の得喪の取消し・無効区分
193 死亡日
194 死亡事由区分
195 死亡の取消し・無効日
196 死亡の取消し・無効区分
197 死亡日の不詳・推定区分
個人番号関係情報
198 個人番号
199 機関別符号

（別添２） 特定個人情報ファイル記録項目

（管理栄養士名簿ファイル）
1 資格仮名ID
2 マイナポータル仮名ID
3 試験回（数値）
4 試験実施年度（西暦）（数値）
5 受験希望地（数値）
6 整理番号（数値）
7 氏名（カナ）
8 漢字氏名
9 性別
10 生年月日（元号）
11 生年月日（年）
12 生年月日（月）
13 生年月日（日）
14 年齢
15 本籍地（国籍）のコード（数値）
16 学校区分コード（数値）
17 学校コード（数値）
18 卒業区分
19 卒業（見込）年月（元号）（数値）
20 卒業（見込）年月（年）（数値）
21 卒業（見込）年月（月）（数値）
22 卒業（見込）年月（日）（数値）
23 現住所
24 電話番号（数値）
25 栄養士免許取得状況（既取得：1、取得見込：2）
26 〃栄養士免許取得年月日（元号）（数値）
※既取得者のみ〃
27 〃栄養士免許取得年月日（年）（数値）
※既取得者のみ〃
28 〃栄養士免許取得年月日（月）（数値）
※既取得者のみ〃
29 〃栄養士免許取得年月日（日）（数値）
※既取得者のみ〃
30 〃管理栄養士養成課程履修の有無
※学校区分コード1該当者のみ〃
31 〃学位授与機構の認定する栄養学に関する専攻科の履修
※該当者のみ〃
32 〃実務期間（開始）（元号）
（実務施設1箇所ごとに作成）
※学校区分コード2～9該当者のみ〃
33 〃実務期間（開始）（年）
（実務施設1箇所ごとに作成）
※学校区分コード2～9該当者のみ〃
34 〃実務期間（開始）（月）
（実務施設1箇所ごとに作成）
※学校区分コード2～9該当者のみ〃
35 〃実務期間（開始）（日）
（実務施設1箇所ごとに作成）
※学校区分コード2～9該当者のみ〃
36 〃実務期間（終了）（元号）
（実務施設1箇所ごとに作成）
※学校区分コード2～9該当者のみ〃
37 〃実務期間（終了）（年）
（実務施設1箇所ごとに作成）
※学校区分コード2～9該当者のみ〃
38 〃実務期間（終了）（月）

（実務施設1箇所ごとに作成）
※学校区分コード2～9該当者のみ″
39 ″実務期間（終了）（日）
（実務施設1箇所ごとに作成）
※学校区分コード2～9該当者のみ″
40 ″実務期間合計（終了、見込）（数値）
※学校区分コード2～9該当者のみ″
41 ″実務期間合計（年）（数値）
※学校区分コード2～9該当者のみ″
42 ″実務期間合計（ヶ月）（数値）
※学校区分コード2～9該当者のみ″
43 前回受験時の氏名
44 前回受験時の試験回（数値）
45 前回受験時の試験地（数値）
46 前回受験時の受験番号（数値）
47 登録番号
48 登録日（元号）
49 登録日
50 漢字氏名（姓）
51 漢字氏名（名）
52 カナ氏名（姓）
53 カナ氏名（名）
54 旧姓（漢字）
55 通称名（姓）
56 通称名（名）
57 生年月日（元号）
58 生年月日
59 本籍コード
60 性別
61 登録資格種別
62 資格取得（元号）
63 資格取得年月日
64 交付日（元号）
65 交付日
66 進達県コード
67 申請区分
68 理由コード
69 理由発生日（元号）
70 理由発生日
71 履歴区分
72 職種コード
73 籍名簿コード
74 課長コード
75 職種名（和名）
76 職種名（英名）
77 法律名（英名）
78 シーケンス名
79 備考
80 登録端末No
81 登録日時
82 更新端末No
83 更新日時
84 本籍地コード
85 本籍地（和名）
86 本籍地（和名（表示用））
87 本籍地（英名）
88 略号
89 外国フラグ
90 備考

91 登録端末No
92 登録日時
93 更新端末No
94 更新日時
95 受験地コード
96 受験地名
97 備考
98 登録端末No
99 登録日時
100 更新端末No
101 更新日時
102 歴代大臣コード
103 大臣名（和名）
104 大臣名（英名）
105 在位期間（開始）
106 在位期間（終了）
107 大臣種別コード
108 備考
109 登録端末No
110 登録日時
111 更新端末No
112 更新日時
113 行政処分内容コード
114 行政処分内容
115 備考
116 登録端末No
117 登録日時
118 更新端末No
119 更新日時
120 養成施設コード
121 養成施設の名称（漢字）
122 要求レコード番号
123 提供事務区分
124 個人番号提供事務区分
125 対象者識別情報
126 照会対象期間（開始年月日）
127 照会対象期間（終了年月日）
128 照会基準日
129 消除者の要否
130 対象者住民票コード
131 対象者氏名（漢字）
132 対象者氏名（かな）
133 対象者生年月日
134 対象者性別
135 対象者住所
136 対象者住所（市町村コード）
137 対象者個人番号
138 予備
139 処理結果コード
140 照会結果レコード数
141 照会結果レコード連番
142 照会一致項目
143 異動有無
144 生存状況
145 変更状況
146 住民票コード
147 氏名（漢字）
148 氏名（かな）
149 生年月日

150 性別
151 住所
152 個人番号
153 異動自由
154 異動年月日
155 外字情報（氏名外字数）
156 外字住所（住所外字数）
157 外字データレコード数
158 市町村コード
159 不参加団体対象フラグ
160 検索パターン番号
161 旧氏（漢字）
162 旧氏（かな）
163 旧氏外字数
164 予備
165 情報提供起点日
166 戸籍異動日
167 戸籍異動事由区分
168 本籍コード
169 出生地
170 国籍取得日
171 取得事由区分
172 国籍喪失日
173 喪失事由区分
174 国籍の得喪の取消し・無効日
175 国籍の得喪の取消し・無効区分
176 死亡日
177 死亡事由区分
178 死亡の取消し・無効日
179 死亡の取消し・無効区分
180 死亡日の不詳・推定区分
181 死亡日の不詳・推定区分
182 機関別符号
183 受験番号

（別添２） 特定個人情報ファイル記録項目

（薬剤師名簿ファイル）
1 資格仮名ID
2 マイナポータル仮名ID
3 受験番号
4 国家試験回数
5 登録区分コード
6 受験地コード
7 国家試験実施年
8 本籍地コード
9 名称区分（氏名）
10 姓
11 名
12 フリガナ（姓）
13 フリガナ（名）
14 通称（姓）
15 通称（名）
16 フリガナ（通称：姓）
17 フリガナ（通称：名）
18 生年月日
19 性別コード
20 国家試験合格年月日
21 受付番号
22 罰金刑区分
23 退避フラグ
24 合格年月日有無コード
25 同時申請回数
26 印刷対象取込コード
27 備考
28 合格証書番号
29 試験地コード
30 出身校コード
31 エントリーID
32 親エントリーID
33 受付番号
34 登録区分コード
35 登録ID
36 進達県コード
37 受付年月日
38 登録番号
39 登録年月日
40 受験番号
41 国家試験回数
42 国家試験実施年
43 受験地コード
44 国家試験合格年月日
45 旧登録県コード
46 旧登録番号
47 旧登録年月日
48 本籍地コード
49 姓
50 名
51 フリガナ（姓）
52 フリガナ（名）
53 通称（姓）
54 通称（名）
55 フリガナ（通称：姓）
56 フリガナ（通称：名）

57 生年月日
58 性別コード
59 仮登録年月日
60 名簿訂正年月日
61 名簿訂正理由コード
62 名簿訂正理由（記事）
63 再交付年月日
64 再交付理由コード
65 再交付理由（記事）
66 消除年月日
67 消除理由コード
68 消除理由（記事）
69 登録換年月日
70 登録換理由コード
71 登録換理由（記事）
72 歴代大臣コード
73 歴代局長コード
74 出身校コード
75 件数
76 処理区分コード
77 エントリー区分コード
78 罰金刑区分
79 保留フラグ
80 保留日時
81 仮完了フラグ
82 エラーフラグ
83 はがき有無
84 データ移行フラグ
85 合格年月日有無コード
86 同時申請回数
87 印刷対象取込コード
88 備考
89 合格登録区分コード
90 合格証書番号
91 誤謬訂正年月日
92 誤謬訂正理由コード
93 誤謬訂正理由（記事）
94 試験地コード
95 旧姓
96 フリガナ（旧姓）
97 登録ID
98 登録番号
99 登録区分コード
100 進達県コード
101 受付年月日
102 登録年月日
103 受験番号
104 国家試験回数
105 国家試験実施年
106 受験地コード
107 国家試験合格年月日
108 旧登録県コード
109 旧登録番号
110 旧登録年月日
111 本籍地コード
112 姓
113 名
114 フリガナ（姓）
115 フリガナ（名）

116 通称(姓)
117 通称(名)
118 フリガナ(通称:姓)
119 フリガナ(通称:名)
120 生年月日
121 性別コード
122 名簿訂正年月日
123 名簿訂正理由コード
124 名簿訂正理由(記事)
125 再交付年月日
126 再交付理由コード
127 再交付理由(記事)
128 消除年月日
129 消除理由コード
130 消除理由(記事)
131 登録換年月日
132 登録換理由コード
133 登録換理由(記事)
134 歴代大臣コード
135 歴代局長コード
136 出身校コード
137 件数
138 処理区分コード
139 エントリー区分コード
140 罰金刑区分
141 合格年月日有無コード
142 同時申請回数
143 印刷対象取込コード
144 備考
145 合格登録区分コード
146 合格証書番号
147 誤謬訂正年月日
148 誤謬訂正理由コード
149 誤謬訂正理由(記事)
150 試験地コード
151 旧姓
152 フリガナ(旧姓)
153 レコード識別番号
154 登録ID
155 行政処分年月日
156 行政処分コード
157 行政処分内容(開始期間)
158 行政処分内容(終了期間)
159 行政処分期間(年)
160 行政処分期間(月)
161 行政処分内容(発簡番号)
162 合格年月日有無コード
163 同時申請回数
164 印刷対象取込コード
165 備考
166 再教育研修終了登録日
167 再教育研修命令登録日
168 行政処分ステータスコード
169 登録ID
170 登録番号
171 登録区分コード
172 進達県コード
173 受付年月日
174 登録年月日

175 受験番号
176 国家試験回数
177 国家試験実施年
178 受験地コード
179 国家試験合格年月日
180 旧登録県コード
181 旧登録番号
182 旧登録年月日
183 本籍地コード
184 姓
185 名
186 フリガナ(姓)
187 フリガナ(名)
188 通称(姓)
189 通称(名)
190 フリガナ(通称:姓)
191 フリガナ(通称:名)
192 生年月日
193 性別コード
194 名簿訂正年月日
195 名簿訂正理由コード
196 名簿訂正理由(記事)
197 再交付年月日
198 再交付理由コード
199 再交付理由(記事)
200 消除年月日
201 消除理由コード
202 消除理由(記事)
203 登録換年月日
204 登録換理由コード
205 登録換理由(記事)
206 歴代大臣コード
207 歴代局長コード
208 出身校コード
209 件数
210 処理区分コード
211 エントリー区分コード
212 罰金刑区分
213 ソート順
214 合格年月日有無コード
215 同時申請回数
216 印刷対象取込コード
217 備考
218 合格登録区分コード
219 合格証書番号
220 誤謬訂正年月日
221 誤謬訂正理由コード
222 誤謬訂正理由(記事)
223 試験地コード
224 旧姓
225 フリガナ(旧姓)
226 登録日付
227 登録区分コード
228 処理件数
229 エントリーID
230 帳票コード
231 レコード識別NO
232 行政処分識別番号
233 再教育交付年月日

234 処理コード
235 交付表示順
236 ステータスコード
237 ID
238 登録区分コード
239 登録番号
240 画像パス
241 職種コード
242 籍名簿コード
243 課長コード
244 職種名（和名）
245 職種名（英名）
246 法律名（英名）
247 シーケンス名
248 備考
249 登録端末No
250 登録日時
251 更新端末No
252 更新日時
253 本籍地コード
254 本籍地（和名）
255 本籍地（和名(表示用)）
256 本籍地（英名）
257 略号
258 外国フラグ
259 備考
260 登録端末No
261 登録日時
262 更新端末No
263 更新日時
264 受験地コード
265 受験地名
266 備考
267 登録端末No
268 登録日時
269 更新端末No
270 更新日時
271 理由コード
272 処理区分コード
273 理由
274 理由(略称)
275 備考
276 登録端末No
277 登録日時
278 更新端末No
279 更新日時
280 歴代大臣コード
281 大臣名（和名）
282 大臣名（英名）
283 在位期間（開始）
284 在位期間（終了）
285 大臣種別コード
286 備考
287 登録端末No
288 登録日時
289 更新端末No
290 更新日時
291 歴代局長コード
292 局長名（和名）

293 局長名(英名)
294 在位期間(開始)
295 在位期間(終了)
296 局長種別コード
297 備考
298 登録端末No
299 登録日時
300 更新端末No
301 更新日時
302 出身校コード
303 出身校名
304 備考
305 登録端末No
306 登録日時
307 更新端末No
308 更新日時
309 歴代医務技監コード
310 医務技監名(和名)
311 医務技監名(英名)
312 在位期間(開始)
313 在位期間(終了)
314 医務技監種別コード
315 備考
316 登録端末No
317 登録日時
318 更新端末No
319 更新日時
320 行政処分内容コード
321 行政処分内容
322 備考
323 登録端末No
324 登録日時
325 更新端末No
326 更新日時
327 要求レコード番号
328 提供事務区分
329 個人番号提供事務区分
330 対象者識別情報
331 照会対象期間(開始年月日)
332 照会対象期間(終了年月日)
333 照会基準日
334 消除者の要否
335 対象者住民票コード
336 対象者氏名(漢字)
337 対象者氏名(かな)
338 対象者生年月日
339 対象者性別
340 対象者住所
341 対象者住所(市町村コード)
342 対象者個人番号
343 予備
344 処理結果コード
345 照会結果レコード数
346 照会結果レコード連番
347 照会一致項目
348 異動有無
349 生存状況
350 変更状況
351 住民票コード

352 氏名（漢字）
353 氏名（かな）
354 生年月日
355 性別
356 住所
357 個人番号
358 異動事由
359 異動年月日
360 外字情報（氏名外字数）
361 外字情報（住所外字数）
362 外字データレコード数
363 市町村コード
364 不参加団体対象フラグ
365 検索パターン番号
366 旧氏（漢字）
367 旧氏（かな）
368 旧氏外字数
369 予備
370 情報提供起点日
371 戸籍異動日
372 戸籍異動事由区分
373 本籍コード
374 出生地
375 国籍取得日
376 取得事由区分
377 国籍喪失日
378 喪失事由区分
379 国籍の得喪の取消し・無効日
380 国籍の得喪の取消し・無効区分
381 死亡日
382 死亡事由区分
383 死亡の取消し・無効日
384 死亡の取消し・無効区分
385 死亡日の不詳・推定区分
386 個人番号
387 機関別符号

（別添２） 特定個人情報ファイル記録項目

（介護福祉士登録名簿ファイル）
1　資格仮名ID
2　マイナポータル仮名ID
名簿情報
3　登録コード
4　登録番号
5　登録年月日（元号）
6　登録年月日（年月日）
7　カナ氏名（姓）
8　カナ氏名（名）
9　漢字氏名（姓）
10　漢字氏名（名）
11　旧姓
12　旧姓（長名）
13　通称
14　通称（長名）
15　通称（旧姓）
16　通称（旧姓）（長名）
17　カナ氏名（長名）
18　漢字氏名（長名）
19　アルファベット氏名
20　本籍地コード
21　現住所コード
22　郵便番号
23　固定電話
24　携帯電話
25　住所
26　メールアドレス
27　生年月日（元号）
28　生年月日（年月日）
29　性別
30　EPA
31　留学
32　期限付登録
33　合格証書番号
34　合格年月(元号)
35　合格年月（年月）
36　養成施設コード
37　有効期限（元号）
38　有効期限（年月日）
39　有効期限解除日（元号）
40　有効期限解除日（年月日）
41　有効期限解除理由
42　合計休業日数
43　休業可能日数
44　訂正日（元号）
45　訂正日（年月日）
46　再交付（元号）
47　再交付（年月日）
48　消除日（元号）
49　消除日（年月日）
50　消除理由
51　消除取消日（元号）
52　消除取消日（年月日）
53　停止日（元号）
54　停止日（年月日）
55　停止理由

56	停止解除日（元号）
57	停止解除日（年月日）
58	登録可能日（元号）
59	登録可能日（年月日）
60	指定研修課程修了
61	指定研修課程修了（元号）
62	指定研修課程修了（年月日）
63	付記資格１
64	付記資格年月日１（元号）
65	付記資格年月日１（年月日）
66	付記資格２
67	付記資格年月日２（元号）
68	付記資格年月日２（年月日）
69	付記資格３
70	付記資格年月日３（元号）
71	付記資格年月日３（年月日）
72	付記資格４
73	付記資格年月日４（元号）
74	付記資格年月日４（年月日）
75	付記資格５
76	付記資格年月日５（元号）
77	付記資格年月日５（年月日）
78	旧姓フラグ
79	通称名フラグ
80	旧姓通称名フラグ
本人確認情報照会結果ファイル	
81	要求レコード番号
82	提供事務区分
83	個人番号提供事務区分
84	対象者識別情報
85	照会対象期間（開始年月日）
86	照会対象期間（終了年月日）
87	照会基準日
88	消除者の要否
89	対象者住民票コード
90	対象者氏名（漢字）
91	対象者氏名（かな）
92	対象者生年月日
93	対象者性別
94	対象者住所
95	対象者住所（市町村コード）
96	対象者個人番号
97	予備
98	処理結果コード
99	照会結果レコード数
100	照会結果レコード連番
101	照会一致項目
102	異動有無
103	生存状況
104	変更状況
105	住民票コード
106	氏名（漢字）
107	氏名（かな）
108	生年月日
109	性別
110	住所
111	個人番号
112	異動事由
113	異動年月日

114　外字情報（氏名外字数）
115　外字情報（住所外字数）
116　外字データレコード数
117　市町村コード
118　不参加団体対象フラグ
119　検索パターン番号
120　旧氏（漢字）
121　旧氏（かな）
122　旧氏外字数
123　予備
戸籍関係情報
124　情報提供起点日
125　戸籍異動日
126　戸籍異動事由区分
127　本籍コード
128　出生地
129　国籍取得日
130　取得事由区分
131　国籍喪失日
132　喪失事由区分
133　国籍の得喪の取消し・無効日
134　国籍の得喪の取消し・無効区分
135　死亡日
136　死亡事由区分
137　死亡の取消し・無効日
138　死亡の取消し・無効区分
139　死亡日の不詳・推定区分
個人番号関係情報
140　個人番号
141　機関別符号

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

医籍等ファイル

2．特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）

リスク1：　目的外の入手が行われるリスク

対象者以外の情報の入手を防止するための措置の内容	【国家資格等情報連携・活用システムに係る部分（共通して記載）】 【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。 【免許登録管理システムに係る部分】 ・申請書の提出があり、医籍等へ登録して問題ない者のみ免許登録管理システムへデータを連携させるため、医師免許等を持っている者以外の情報は免許登録管理システムで保有しないため、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	【国家資格等情報連携・活用システムに係る部分（共通して記載）】 【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。 【免許登録管理システムに係る部分】 申請書の様式で定められた必要な情報のみを管理することにより、必要な情報以外を入手することを防止している。
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	【国家資格等情報連携・活用システムに係る部分（共通して記載）】 【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、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。 【郵送による入手】 経由機関からの申請書類等、情報の郵送については、原則として、簡易書留等の追跡可能な郵送手段により漏洩・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。 【免許登録管理システムとの接続】 免許登録管理システムと国家資格等情報連携・活用システムとの接続についてはLGWAN回線又はVPNによる接続のみを認め、通信の暗号化等の高度なセキュリティを維持することで機密性を確保している。また、当該通信は、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。 国民向けの検索機能を有する資格確認検索システムと同期を予定しているが、専用回線を用いて氏名、登録年、性別のみのデータを同期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	【国家資格等情報連携・活用システムに係る部分】 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。 ・システムにアクセスする職員について、権限のある者が必要な情報のみ閲覧ができるようアクセス制御を行い、当該職員が所掌する資格以外の資格情報を閲覧できない仕組みとしている。 【免許登録管理システムに係る部分】 ・免許登録管理システムとの連携は、権限のある者が必要な情報のみ連携ができるようアクセス制御を行い、目的を超えた紐付けや必要の無い情報との紐付けが行えない仕組みとしている。 ・住民基本台帳ネットワークシステム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。 ・システムにアクセスする職員について、権限のある者が必要な情報のみ閲覧ができるようアクセス制御を行い、当該職員が所掌する資格以外の資格情報を閲覧できない仕組みとしている。

その他の措置の内容		
リスクへの対策は十分か	[　　十分である　　]	＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
リスク2：　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。 ※免許登録管理システム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。 【免許登録管理システムに係る部分】 ・システム操作や資格者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。 情報システム責任者及び情報システム管理者は、「免許登録管理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)従事者による免許登録管理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)免許登録管理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。	

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。 【免許登録管理システムに係る部分】 （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当該事務に従事する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利用者をユニークにする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又は無効化する。
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、アクセス権限の発行・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。 【免許登録管理システムに係る部分】 ・免許登録管理システムへのログイン用のユーザーIDは、当該事務に従事する者に限定して発行される。 ・それぞれの従事者ごとに個人を特定可能な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、アクセス権限の発行・失効等の管理を行う。 ・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。 【免許登録管理システムに係る部分】 ・システムの利用範囲を利用者の職務に応じて制限するために、アクセス権を利用者に応じて制御する機能を備えるとともに、アクセス権を適切に設定する。 ・免許登録管理システムへのアクセスログ、免許登録管理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。
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（共通して記載）】 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。 【免許登録管理システムに係る部分】 ・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できるよう制御している。 ・アカウントは当該業務に従事する者のみに割り当て、操作ログを記録し、不正なアクセス等がないか確認を行う。 ・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。 ・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。 ・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。 ・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。

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。 【免許登録管理システムに係る部分】 ・システムの利用範囲を利用者の職務に応じて制限するため、アクセス権を利用者に応じて制御している。 ・共用アカウントを採用せず利用者をユニークにするアカウント管理を実施し、各作業に必要最低限の権限を付与するとともに、適切にアカウント管理が実施されていることを第三者が定期的に確認する運用体制としている。 ・バックアップ以外にファイルの複製を行うことは禁止とし、バックアップ媒体は施錠可能な金庫等に保管するよう指導する。 ・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。 ・既存システムと国家資格等情報連携・活用システム間のデータ連係については、データ及び通信の暗号化を実施する。また、通信回線について、高度なセキュリティが維持されたLGWAN回線又はVPN回線において実施することで安全性を確保し不正に複製されることを防止する。 ・国家資格等情報連携・活用システム、住基連携サーバー及び本人確認端末（専用端末）に係る部分と同等のリスク対策を講じる。
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】 ・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。 【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 【免許登録管理システムに係る部分】 ・委託先事業者の選定を行う際は、プライバシーマーク、ISO/IEC27001認証（国際規格）、JIS Q 27001認証のいずれかを取得している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	【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。 【免許登録管理システムに係る部分】 委託先事業者は管理責任者及び情報取扱管理者等の保護を要する情報を取り扱う可能性のある者の氏名、住所、生年月日、所属部署、役職等を記載した情報取扱者名簿を提出することとし、あらかじめ確認を受けなければならない。また、台帳等を設け個人情報の管理状況を記録することとする。
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	【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。 【免許登録管理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、管理台帳等により適切に管理をし、情報システム責任者等がこれらの情報の取扱いについて適切な措置が講じられていることを確認するため、遵守状況の報告や実地調査を求めた場合には応じなければならない。また、調査の結果、セキュリティ対策の履行が不十分である場合、速やかに改善策を提出しなければならない。
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	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	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。
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。 「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。 【免許登録管理システムに係る部分】 ・免許登録管理システムに係る資格情報等は、医籍等も兼ねているため、医籍等は永年保存であり、死亡等により資格が喪失となった場合でも、システムからすべての情報の消去を行うことはない。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。 ・システムから特定個人情報の消去を行う際には、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。 【免許登録管理システムに係る部分】 ・秘密保持義務 ・委託者施設内の作業実施場所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	【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。 【免許登録管理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。 ・あらかじめ再委託先事業者の名称、再委託を行う業務の範囲、再委託の必要性等を記載した承認申請書を提出し、承認を受ける。 ・知的財産権、情報セキュリティ（機密保持及び遵守事項）、ガバナンス等に関する委託契約書で定める委託先事業者の債務を、再委託先事業者も負うような必要な措置を実施する。 ・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。 ・再委託先事業者の対応について最終的な責任を委託先事業者が負うこととする。
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	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。 ・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。 【免許登録管理システムに係る部分】 ・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を利用している。 ・情報資産を管理するデータセンターの物理的所在地を日本国内とし、電子ロック等で施錠され、許可された関係者のみが入退室できるようにすることとし、入退室の記録がログで確認できるようにすることとしている。また、事前に登録された機器や端末のみが接続できるようにし、接続された機器や端末を特定する情報が記録される仕組みとなっている。 ・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、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。 ・本人確認端末のある部屋には、入退室制限等の物理的なアクセス制御手段により、許可された利用者のみが入退室できるようにし、入退室記録簿等により、入退室の記録を管理することとしている。 ・国家資格等情報連携・活用システム及び免許登録管理システムへの接続端末のある部屋では、特定個人情報等を取り扱う事務を実施する区域を明確にし、入退室管理を徹底するため出入口の場所を限定している。事務取扱担当者等以外の者が特定個人情報等を容易に閲覧等できないように特定個人情報等を取り扱う機器、電子媒体又は書類等を、施錠できるキャビネット、書庫又は必要に応じて耐火金庫等へ保管する。 ・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。	
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。 【免許登録管理システムに係る部分】 ・権限を有する者以外個人情報にアクセスできないように制御している。 ・情報セキュリティ監査を年1回程度実施し、脆弱性等が発見された場合には速やかに対応策を検討し、セキュリティパッチの適用、設定の変更及びシステムの改修等、必要な対応を行う。 ・データベース及びシステムで作成されるデータファイルを日次バックアップし、障害等の発生により、データが破損・消失した場合には最新のバックアップ時点まで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。 ・不正な変更が情報システムのハードウェアやソフトウェア等に加えられないための管理体制が整備されている。 ・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。 ・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	【令和4年度】 厚生労働省が収集している診断書情報について、研究者から、利用申出を受けて提供したデータファイルに、本来、削除されるべき個人情報（氏名・生年月日・住所等、延べ5,640名分）が含まれていた。
	再発防止策の内容	所管の国立研究開発法人及び厚生労働省での複数の者によるダブルチェックの徹底などの基本的な対策に加え、人為的な理由による削除漏れの防止、所管の国立研究開発法人における確認体制の強化、厚生労働省における最終チェック体制の整備、所管の国立研究開発法人における職員・研究者の個人情報保護に係る教育等の具体的な再発防止策を策定し、その徹底を図る。

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		【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。 ・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。 【免許登録管理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。
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	・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。 ・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。 ・紙媒体は保管期間ごとに分けて保管し、保管期間が過ぎているものについては、細断又は外部業者による溶解処理等により廃棄を行う。廃棄の際は廃棄履歴を作成し保存する。また職員は、廃棄が確実に実施されたか否かについて、外部業者の提出する廃棄証明書等により確認を行う。
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
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		

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】 窓口等において申請を受け付ける場合、紙媒体の資料は、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。 【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。 【管理栄養士に係る部分】 経由機関からの情報の郵送については、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洩・紛失を防止する。

リスクへの対策は十分か	[　　十分である　　]	<選択肢> 1）特に力を入れている　　2）十分である 3）課題が残されている

特定個人情報の入手（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	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。 ※管理栄養士（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	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	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、アクセス権限の発行・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	・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	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	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		【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。 【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 【管理栄養士に係る部分】 ・会計事務手引に基づき、委託先業者を選定する。 〇情報保護管理体制 ・情報の取扱いに関して、適切な保護措置を講ずる体制を整備していること。一般財団法人日本情報経済社会推進協会が認定するプライバシーマーク付与認定、ISO/IEC 27001認証、JISQ27001認証のうち、いずれかを取得している事業者であること。また、社員教育等により、社員全員に対してその取扱いを周知徹底しており、かつ、情報漏洩に対して懲戒処分等の制裁措置についての社内規定を設けていること。 ・本件全ての受託業務の一部または全部を他の業者に再委託することなく全ての機械処理及び作業事務を自社社員により自社内(本・支社限定)で行い、納品ができること。また入力・電算処理業務の全てを国内で行うことができること。 ・作業場所は、全て防災、防犯等の対策が講じられていること。またシステム及びデータに関して、堅牢なセキュリティで保護措置を講ずる体制を整備していること。また、データ入力場所の入口に生体認証システムを導入してあること。
特定個人情報ファイルの閲覧者・更新者の制限		[　制限している　] ＜選択肢＞ 1）制限している　2）制限していない
	具体的な制限方法	委託先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	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	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。
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。 【管理栄養士に係る部分】 ・会計事務手引に基づき、委託先業者を選定する。 〇消去ルール ・請負者は、契約終了時に全てのデータを電子媒体にて発注者に提出後、速やかに当省から貸与したデータ等は返却し、それ以外の電子媒体、紙媒体等は全て回復困難な方法で廃棄すること。なお、実施方法等については、当省の承認を得た上で速やかに実施すること。実施後においては、作業完了報告書を当省へ速やかに提出すること。 ・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。
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	(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。 ・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。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。 ・電子記録媒体のデータについては、暗号化している。 (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、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ことにより、漏えいや紛失を防止する。 ・本人確認端末を利用する場所は、入退室制限等の物理的なアクセス制御手段により、許可された利用者のみが入退室できるようにし、入退室記録簿等により、入退室の記録を管理することとしている。 ・国家資格等情報連携・活用システムに接続できる端末の使用は、特定個人情報等を取り扱う事務を実施する区域を明確にし、入退室管理を徹底するため出入口の場所を限定している。事務取扱担当者等以外の者が特定個人情報等を容易に閲覧等できないように特定個人情報等を取り扱う機器、電子媒体又は書類等を、施錠できるキャビネット、書庫又は必要に応じて耐火金庫等へ保管する。 ・電子記録媒体のデータについては、暗号化している。	

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	【令和4年度】 厚生労働省が収集している診断書情報について、研究者から、利用申出を受けて提供したデータファイルに、本来、削除されるべき個人情報（氏名・生年月日・住所等、延べ5,640名分）が含まれていた。
	再発防止策の内容	所管の国立研究開発法人及び厚生労働省での複数の者によるダブルチェックの徹底などの基本的な対策に加え、人為的な理由による削除漏れの防止、所管の国立研究開発法人における確認体制の強化、厚生労働省における最終チェック体制の整備、所管の国立研究開発法人における職員・研究者の個人情報保護に係る教育等の具体的な再発防止策を策定し、その徹底を図る。

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	・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。 ・厚生労働省における紙媒体の廃棄については、公文書管理の規程に基づき、処理するとともに、管理簿等に記録する。 ・委託先事業者の紙媒体の廃棄については、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。
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		

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

薬剤師名簿ファイル

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	【国家資格等情報連携・活用システムに係る部分（共通して記載）】 【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。 【免許登録管理システムに係る部分】 ・申請書の提出があり、薬剤師名簿へ登録して問題ない者のみ免許登録管理システムへデータを連携させるため、薬剤師資格を持っている者以外の情報は免許登録管理システムで保有しないため、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	【国家資格等情報連携・活用システムに係る部分（共通して記載）】 【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。 【免許登録管理システムに係る部分】 申請書の様式で定められた必要な情報のみを管理することにより、必要な情報以外を入手することを防止している。
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	【国家資格等情報連携・活用システムに係る部分（共通して記載）】 【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、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。また、経由機関から郵送で受け取る場合、厳封封筒で、簡易書留等の追跡が可能な郵送手段を推奨することにより、漏えい等を防止する。 【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。 【免許登録管理システムとの接続】 免許登録管理システムと国家資格等情報連携・活用システムとの接続についてはLGWAN回線又はVPNによる接続のみを認め、通信の暗号化等の高度なセキュリティを維持することで機密性を確保している。 また、当該通信は、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。 国民向けの検索機能を有する薬剤師資格確認検索システムと同期を予定しているが、専用回線を用いて氏名、登録年、性別のみのデータを同期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	【国家資格等情報連携・活用システムに係る部分（共通して記載）】 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。 【免許登録管理システムに係る部分】 ・免許登録管理システムとの連携は、権限のある者が必要な情報のみ連携ができるようアクセス制御を行い、目的を超えた紐付けや必要の無い情報との紐付けが行えない仕組みとしている。 ・住民基本台帳ネットワークシステム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。 ・システムにアクセスする職員について、権限のある者が必要な情報のみ閲覧ができるようアクセス制御を行い、当該職員が所掌する資格以外の資格情報を閲覧できない仕組みとしている。

その他の措置の内容		
リスクへの対策は十分か	[　　十分である　　]	＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている
リスク2：　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（共通して記載）】 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。 ※免許登録管理システム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。 【免許登録管理システムに係る部分】 ・システム操作や資格者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。 情報システム責任者及び情報システム管理者は、「免許登録管理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)従事者による免許登録管理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)免許登録管理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。	

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（共通して記載）】 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。 【免許登録管理システムに係る部分】 （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当該事務に従事する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利用者をユニークにする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又は無効化する。
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（共通して記載）】 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、アクセス権限の発行・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。 【免許登録管理システムに係る部分】 ・免許登録管理システムへのログイン用のユーザーIDは、当該事務に従事する者に限定して発行される。 ・それぞれの従事者ごとに個人を特定可能な別々のユーザーアカウントを割り当てる。 ・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。 ・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、アクセス権限の発行・失効等の管理を行う。
特定個人情報の使用の記録		[　記録を残している　] ＜選択肢＞ 1）記録を残している　2）記録を残していない

	具体的な方法	【国家資格等情報連携・活用システムに係る部分（共通して記載）】 ・情報システム責任者等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、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。 ⑵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。 ⑶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。 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。 【免許登録管理システムに係る部分】 ・システムの利用範囲を利用者の職務に応じて制限するために、アクセス権を利用者に応じて制御する機能を備えるとともに、アクセス権を適切に設定する。 ・システムの操作履歴を記録する。 ・免許登録管理システムへのアクセスログ、免許登録管理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。
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（共通して記載）】 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。 ⑴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。 ⑵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。 ⑶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。 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。 ⑸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。 【免許登録管理システムに係る部分】 ・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できるよう制御している。 ・アカウントは当該業務に従事する者のみに割り当て、操作ログを記録し、不正なアクセス等がないか確認を行う。 ・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。 ・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。 ・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。 ・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。

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（共通して記載）】 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。 【免許登録管理システムに係る部分】 ・システムの利用範囲を利用者の職務に応じて制限するため、アクセス権を利用者に応じて制御している。 ・共用アカウントを採用せず利用者をユニークにするアカウント管理を実施し、各作業に必要最低限の権限を付与するとともに、適切にアカウント管理が実施されていることを第三者が定期的に確認する運用体制としている。 ・バックアップ以外にファイルの複製を行うことは禁止とし、バックアップ媒体は施錠可能な金庫等に保管するよう指導する。 ・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。 ・既存システムと国家資格等情報連携・活用システム間のデータ連係については、データ及び通信の暗号化を実施する。また、通信回線について、高度なセキュリティが維持されたLGWAN回線又はVPN回線において実施することで安全性を確保し不正に複製されることを防止する。 ・国家資格等情報連携・活用システム、住基連携サーバー及び本人確認端末（専用端末）に係る部分と同等のリスク対策を講じる。
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（共通して記載）】 ・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。 【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 【免許登録管理システムに係る部分】 ・委託先事業者の選定を行う際は、プライバシーマーク、ISO/IEC27001認証（国際規格）、JIS Q 27001認証のいずれかを取得している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	【国家資格等情報連携・活用システムに係る部分（共通して記載）】 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。 【免許登録管理システムに係る部分】 委託先事業者は管理責任者及び情報取扱管理者等の保護を要する情報を取り扱う可能性のある者の氏名、住所、生年月日、所属部署、役職等を記載した情報取扱者名簿を提出することとし、あらかじめ確認を受けなければならない。また、台帳等を設け個人情報の管理状況を記録することとする。
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	【国家資格等情報連携・活用システムに係る部分（共通して記載）】 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。 【免許登録管理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、管理台帳等により適切に管理をし、情報システム責任者等がこれらの情報の取扱いについて適切な措置が講じられていることを確認するため、遵守状況の報告や実地調査を求めた場合には応じなければならない。また、調査の結果、セキュリティ対策の履行が不十分である場合、速やかに改善策を提出しなければならない。
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	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	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。

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（共通して記載）】 ・国家資格管理事務に係る資格情報等は、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。免許を返納した者や行政処分により資格が喪失となった者といった生者の個人番号についてはデータの物理削除を行う。 ・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。 【免許登録管理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、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。免許を返納した者や行政処分により資格が喪失となった者といった生者の個人番号についてはデータの物理削除を行う。 ・死亡等により薬剤師名簿から消除を行う際には、適切に消除を行い、消除に係る記録を作成し、管理する。 「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（共通して記載）】 ・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。 【免許登録管理システムに係る部分】 ・秘密保持義務 ・委託者施設内の作業実施場所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	【国家資格等情報連携・活用システムに係る部分（共通して記載）】 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。 【免許登録管理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。 ・あらかじめ再委託先事業者の名称、再委託を行う業務の範囲、再委託の必要性等を記載した承認申請書を提出し、承認を受ける。 ・知的財産権、情報セキュリティ（機密保持及び遵守事項）、ガバナンス等に関する委託契約書で定める委託先事業者の債務を、再委託先事業者も負うような必要な措置を実施する。 ・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。 ・再委託先事業者の対応について最終的な責任を委託先事業者が負うこととする。
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 3）課題が残されている	2）十分である
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 3）課題が残されている	2）十分である
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 3）課題が残されている	2）十分である
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）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（共通して記載）】 (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。 ・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。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。 【免許登録管理システムに係る部分】 ・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を利用している。 ・情報資産を管理するデータセンターの物理的所在地を日本国内とし、電子ロック等で施錠され、許可された関係者のみが入退室できるようにすることとし、入退室の記録がログで確認できるようにすることとしている。また、事前に登録された機器や端末のみが接続できるようにし、接続された機器や端末を特定する情報が記録される仕組みとなっている。 ・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、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。鍵は担当者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。 ・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。 （本人確認端末） 入退室制限等の物理的なアクセス制御手段により、許可された利用者のみが入退室できるようにし、入退室記録簿等により、入退室の記録を管理することとしている。 （国家資格等情報連携・活用システム及び免許登録管理システムへの接続端末） 特定個人情報等を取り扱う事務を実施する区域を明確にし、入退室管理を徹底するため出入口の場所を限定している。事務取扱担当者等以外の者が特定個人情報等を容易に閲覧等できないように特定個人情報等を取り扱う機器、電子媒体又は書類等を、施錠できるキャビネット、書庫又は必要に応じて耐火金庫等へ保管する。また、電子記録媒体を使用する場合は、データの暗号化を行う。	
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（共通して記載）】 ・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。 【免許登録管理システムに係る部分】 ・権限を有する者以外個人情報にアクセスできないように制御している。 ・情報セキュリティ監査を年１回程度実施し、脆弱性等が発見された場合には速やかに対応策を検討し、セキュリティパッチの適用、設定の変更及びシステムの改修等、必要な対応を行う。 ・データベース及びシステムで作成されるデータファイルを日次バックアップし、障害等の発生により、データが破損・消失した場合には最新のバックアップ時点まで復元できるようにする。 ・不正な変更が情報システムのハードウェアやソフトウェア等に加えられないための管理体制が整備されている。 ・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	【令和4年度】 厚生労働省が収集している診断書情報について、研究者から、利用申出を受けて提供したデータファイルに、本来、削除されるべき個人情報（氏名・生年月日・住所等、延べ5,640名分）が含まれていた。
	再発防止策の内容	所管の国立研究開発法人及び厚生労働省での複数の者によるダブルチェックの徹底などの基本的な対策に加え、人為的な理由による削除漏れの防止、所管の国立研究開発法人における確認体制の強化、厚生労働省における最終チェック体制の整備、所管の国立研究開発法人における職員・研究者の個人情報保護に係る教育等の具体的な再発防止策を策定し、その徹底を図る。

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	【国家資格等情報連携・活用システムに係る部分（共通して記載）】 ・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。 【免許登録管理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。	
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	・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、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。免許を返納した者や行政処分により資格が喪失となった者といった生者の個人番号についてはデータの物理削除を行う。 ・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。 ・厚生労働省内で保管する特定個人情報が記載された紙媒体の資料を廃棄する場合は、シュレッダー又は外部業者による溶解処理等の復元不可能な手段で廃棄を行う。廃棄の際は廃棄履歴を作成し保存する。また職員は、廃棄が確実に実施されたか否かについて、外部業者の提出する廃棄証明書等により確認を行う。	
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
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		

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

介護福祉士登録名簿ファイル

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	【国家資格等情報連携・活用システムに係る部分（共通して記載）】 【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。 【登録情報連携システムに係る部分】 申請書の提出があり、登録要件を満たしている者のみ国家資格等情報連携・活用システムへデータを連携させるため、登録要件を満たしている者以外の情報は、情報連携システム、登録システムで保有しないため、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	【国家資格等情報連携・活用システムに係る部分（共通して記載）】 【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。 【登録情報連携システムに係る部分】 申請書の様式で定められた必要な情報のみを管理することにより、必要な情報以外を入手することを防止している。
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。
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	【国家資格等情報連携・活用システムに係る部分（共通して記載）】 【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、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。 【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。 【登録情報連携システムに係る部分】 ・国家資格等情報連携・活用システムとの接続については、VPN等による接続により、通信の暗号化等の高度なセキュリティを維持することで機密性を確保する。また、当該通信は、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。 ・電子記録媒体は、情報の暗号化を行うとともに、入退室制限等の物理的なアクセス制御手段により、特定者以外の入室を制限し、管理区域内から電子記録媒体を持ち出すことを禁止している。 ・電子記録媒体でのデータ連係は、あらかじめ定められたファイル形式（個人番号を含まない）によるパスワード設定され、暗号化されたファイルの入出力のみ可能となるようシステム（情報連携システム、登録システム）にて制御を行う。 また、事前登録したPC以外では使用できないよう制限し、接続時には暗証番号の入力を必要とし、ウイルススキャン機能付とする。 ・紙媒体は、専用の厳封封筒を配付し、更に提出する際は、簡易書留を利用させる。

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		【国家資格等情報連携・活用システムに係る部分（共通して記載）】 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。 ・登録情報連携システムとの情報連携については、あらかじめ定められた情報についてのみ連携を可能とするよう国家資格等情報連携・活用システムにて内部制御を行う。 【登録情報連携システムに係る部分】 登録情報連携システムは、国家資格等情報連携・活用システムとの情報連携する際に、その他のシステムとは接続せず、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。また、特定個人情報が記録された電子記録媒体については取扱者を限定し、利用目的を報告した上で利用させ、また、利用終了時には当該電子記録媒体にデータが残っていないことを報告・確認することにより、事務に必要のない情報と紐付かないようにする。特定個人情報管理PC及び登録システムにおいても同様に事務に必要のない情報と紐づかないようにする。
その他の措置の内容		
リスクへの対策は十分か		[十分である] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2： 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（共通して記載）】 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。 ※介護福祉士等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。 【登録情報連携システムに係る部分】 ・登録情報連携システムでは、共通ID、元職員、アクセス権限のない職員等は、ログインできない運用をしている。また、パスワードは利用者本人と特定管理者で管理しており、なりすましによる不正利用の防止を図っている。 ・「国家資格等情報連携・活用システムに係る部分」と同等程度の対策を講じる。

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（共通して記載）】 情報システム責任者等は以下の作業を行う。 ⑴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。 ⑵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。 ⑵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。 【登録情報連携システムに係る部分】 ・登録情報連携システムのアクセス権限の発行・失効の管理は、特定管理者で管理しており、なりすましによる不正利用の防止を図っている。 ・「国家資格等情報連携・活用システムに係る部分」と同等程度の対策を講じる。 ・なお、情報セキュリティ責任者は、組織全体の責任者であり、記載の特定管理者は、既存システムを運用する部署の長が部セキュリティ管理者として、情報セキュリティポリシーの遵守に関する意見の集約、当該部の職員に対する教育、訓練、助言及び指示を担っている。
アクセス権限の管理		[　行っている　] ＜選択肢＞ 1）行っている　2）行っていない
	具体的な管理方法	【国家資格等情報連携・活用システムに係る部分（共通して記載）】 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、アクセス権限の発行・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。 【登録情報連携システムに係る部分】 ・登録情報連携システムのアクセス権限の発行・失効の管理は、特定管理者で管理しており、なりすましによる不正利用の防止を図っている。 ・「国家資格等情報連携・活用システムに係る部分」と同等程度の対策を講じる。 ・なお、情報セキュリティ責任者は、組織全体の責任者であり、記載の特定管理者は、既存システムを運用する部署の長が部セキュリティ管理者として、情報セキュリティポリシーの遵守に関する意見の集約、当該部の職員に対する教育、訓練、助言及び指示を担っている。

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（共通して記載）】 ・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。 【登録情報連携システムに係る部分】 ・登録情報連携システムでは、国家資格等情報連携・活用システムに情報連携を行う以外に特定個人情報が使用出来ない仕様としている。 ・「国家資格等情報連携・活用システムに係る部分」と同等程度の対策を講じる。
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		【国家資格等情報連携・活用システムに係る部分（共通して記載）】 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。 【登録情報連携システムに係る部分】 ・登録情報連携システムでは、国家資格等情報連携・活用システムに情報連携を行う以外に特定個人情報が使用出来ない仕様としているため、従事者が事務外で使用することはない。 ・「国家資格等情報連携・活用システムに係る部分」と同等程度の対策を講じる。
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	【国家資格等情報連携・活用システムに係る部分（共通して記載）】 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。 【登録情報連携システムに係る部分】 ・「国家資格等情報連携・活用システムに係る部分」と同等程度の対策を講じる。
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（共通して記載）】 ・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。 【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 【登録情報連携システムに係る部分】 ・「国家資格等情報連携・活用システムに係る部分」と同等程度の対策を講じる。	
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（共通して記載）】 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。 【登録情報連携システムに係る部分】 特定個人情報を取り扱うエリア、及び取扱者を限定します。入退室名簿を使用し、入退室を管理、使用するPCは全てローカル環境とする。また、管理及び実施体制を書面で報告し、確認を受けなければならない運用とする。	
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	【国家資格等情報連携・活用システムに係る部分（共通して記載）】 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。 【登録情報連携システムに係る部分】 特定個人情報を取り扱うエリアで使用するPCは、ログ取得ツールを用いて履歴を記録する。入退室名簿を使用し、入退室を管理、使用するPCは全てローカル環境とする。また、取得したログを書面により報告し、情報セキュリティ責任者等が必要に応じて調査を行う運用とする。	
特定個人情報の提供ルール	[　　定めている　　]	<選択肢> 1）定めている　　2）定めていない
委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	【国家資格等情報連携・活用システムに係る部分（共通して記載）】 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。 【登録情報連携システムに係る部分】 ・「国家資格等情報連携・活用システムに係る部分」と同等程度の対策を講じる。	
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	【国家資格等情報連携・活用システムに係る部分（共通して記載）】 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する。 【登録情報連携システムに係る部分】 ・「国家資格等情報連携・活用システムに係る部分」と同等程度の対策を講じる。	
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（共通して記載）】 ・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。 「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。 【登録情報連携システムに係る部分】 特定個人情報について、紙媒体の場合は、機密保持契約を締結する廃棄・溶解処理業者に復元できない方法で依頼し、廃棄証明書を委託元へ提出する。電子記録媒体（特定個人情報が記録された機器を含む）の場合は、完全に消去するツールを使用し復元できない方法で消去し、消去証明書を委託元へ提出する。また、情報システム責任者等に廃棄する場合のリスク対策について、書面により報告する。必要に応じて立入検査を実施する。
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（共通して記載）】 ・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。 【登録情報連携システムに係る部分】 ・「国家資格等情報連携・活用システムに係る部分」と同等程度の対策を講じる。
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	【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。 【登録情報連携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。
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）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）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）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（共通して記載）】 (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。 ・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。また、事前に申請し承認されていない物品、記憶媒体、通信機器など不正に所持し、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。 【登録情報連携システムに係る部分】 紙媒体は、入退室制限等の物理的なアクセス制御手段により、特定者以外の入室を制限し、管理区域内から紙媒体を持ち出すことを禁止する。国家資格等情報連携・活用システムに情報連携後は、機密保持契約を締結する廃棄・溶解処理業者に復元出来ない方法で依頼し、廃棄証明書を受領する。 電子記録媒体は、情報の暗号化を行うとともに、入退室制限等の物理的なアクセス制御手段により、特定者以外の入室を制限し、管理区域内から電子記録媒体を持ち出すことを禁止する。国家資格等情報連携・活用システムに情報連携後は、データを完全に消去するツールを使用し復元出来ない方法で行い、消去証明書を受領する。 なお、入退室管理のログを取得し、取得したログを定期及び随時確認する。		

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（共通して記載）】 ・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。 【登録情報連携システムに係る部分】 登録情報連携システムは、外部と切り離された環境で運用し、特定の管理者以外アクセスできないよう制限をしている。また、国家資格等情報連携・活用システムへの情報連携はセキュリティが保たれたUSB等を使用し、API等で連携する情報連携システムに移行して情報連携を行う。また、国家資格等情報連携・活用システムの通信はVPN等による接続のみを認め、通信の暗号化等の高度なセキュリティを維持することで機密性を確保する。 また、データファイルを日次バックアップし、障害等の発生により、データが滅失・毀損した場合には、最新のバックアップ時点まで復元ができ、不正な変更が加えられない管理体制を確保する。
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		[　発生あり　] ＜選択肢＞ 1）発生あり　2）発生なし
	その内容	【令和4年度】 厚生労働省が収集している診断書情報について、研究者から、利用申出を受けて提供したデータファイルに、本来、削除されるべき個人情報（氏名・生年月日・住所等、延べ5,640名分）が含まれていた。
	再発防止策の内容	所管の国立研究開発法人及び厚生労働省での複数の者によるダブルチェックの徹底などの基本的な対策に加え、人為的な理由による削除漏れの防止、所管の国立研究開発法人における確認体制の強化、厚生労働省における最終チェック体制の整備、所管の国立研究開発法人における職員・研究者の個人情報保護に係る教育等の具体的な再発防止策を策定し、その徹底を図る。

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（共通して記載）】 ・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。 ・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。 【登録情報連携システムに係る部分】 登録情報連携システムでは、国家資格等情報連携・活用システムに情報連携後、電子記録媒体のデータ消去は、データを完全に消去するツールを使用し復元出来ない方法で行い、消去証明書を受領する。紙媒体の消去は、機密保持契約を締結する廃棄・溶解処理業者に復元出来ない方法で依頼し、廃棄証明書を受領する。また、電子記録媒体を媒体記録簿で管理し、消去・廃棄した際は管理簿に記録を残す。	
その他の措置の内容	【登録情報連携システムに係る部分】 （公財）社会福祉振興・試験センターにおいて、国家資格等情報連携・活用システムへ情報連携後は、紙・データとも廃棄し、消去されずいつまでも存在するリスクを軽減させる。	
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（共通して記載）】 「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。 【医籍等ファイル、薬剤師名簿ファイル】 「免許登録管理システムに係る部分及びその他事務に係る部分」 厚生労働省情報セキュリティポリシー及び関係規程に規定されている事項について定期的に職員による自己点検を行い、その点検結果について管理者が確認を行う。 【管理栄養士名簿ファイル】 厚生労働省情報セキュリティポリシー及び関係規程に規定されている事項について定期的に職員による自己点検を行い、その点検結果について管理者が確認を行う。 【介護福祉士登録名簿ファイル】 「登録情報連携システムに係る部分及びその他事務に係る部分」 （公財）社会福祉振興・試験センターにおいて、社内で定める情報セキュリティに関する規程（政府の基準と同等程度）、情報セキュリティ基本方針、情報セキュリティ対策基準、情報取扱手順書、情報セキュリティに係る電磁的記録媒体等の取扱要領に則り、適切な運用を遵守させ、管理者は利用者の管理、必要な監督を行う。
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（共通して記載）】 「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。 【医籍等ファイル、薬剤師名簿ファイル】 「免許登録管理システムに係る部分及びその他事務に係る部分」 厚生労働省情報セキュリティポリシー及び関係規程の遵守状況等について、定期に及び必要に応じて内部監査を実施する。 【管理栄養士名簿ファイル】 厚生労働省情報セキュリティポリシー及び関係規程の遵守状況等について、定期に及び必要に応じて内部監査を実施する。 【介護福祉士登録名簿ファイル】 「登録情報連携システムに係る部分及びその他事務に係る部分」 （公財）社会福祉振興・試験センターにおいて、社内で定める情報セキュリティ委員会運営要領に則り、適切な運用がなされているか定期に及び必要に応じて監査を行う。
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（共通して記載）】 「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。 【全ファイル共通】 厚生労働省情報セキュリティポリシー及び関係規程並びに特定個人情報の適正な取扱いに関するガイドラインで求められる必要な教育・研修を行う。 【医籍等ファイル、薬剤師名簿ファイル】 「免許登録管理システムに係る部分」 ・厚生労働省情報セキュリティポリシー及び関係規程に規定されている事項について定期的に職員による自己点検を行う。また、自己点検以外に管理者が前述のセキュリティポリシー及び関係規程を用いて、新たに事務取扱担当者になる者に対する研修を行うこととする。 【介護福祉士登録名簿ファイル】 「登録情報連携システムに係る部分」 （公財）社会福祉振興・試験センターにおいて、社内で定める情報セキュリティに関する規程（政府の基準と同等程度）、情報セキュリティ基本方針、情報セキュリティ対策基準、情報取扱手順書、情報セキュリティに係る電磁的記録媒体等の取扱要領に則り、適切な運用を遵守ができるよう必要な教育（研修）を行う。

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（共通して記載）】
「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。
【全ファイル共通】
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
【介護福祉士登録名簿ファイル】
「登録情報連携システムに係る部分」
（公財）社会福祉振興・試験センターにおいて、社内で定める情報セキュリティ対策基準に則り、適切に対策を行う。

Ⅴ　開示請求、問合せ

1. 特定個人情報の開示・訂正・利用停止請求	
①請求先	〒100－8916 東京都千代田区霞ヶ関1－2－2　中央合同庁舎第5号館2階 厚生労働省大臣官房総務課公文書監理・情報公開室 (http://www.mhlw.go.jp/jouhou/hogo05/index.html) ※郵送の場合の宛先についても同上
②請求方法	指定様式（下記URLを参照）による書面の提出により開示・訂正・利用停止請求を受け付ける。 (http://www.mhlw.go.jp/jouhou/hogo06/index.html) また、請求方法について、上記「①請求先」で示すURLのページにおいて流れを記載し、わかりやすい説明に努めている。
特記事項	厚生労働省ホームページ上に、請求特記事項 先、請求方法、諸費用等について掲載する。
③手数料等	[　　有料　　]　　＜選択肢＞ 1) 有料　　2) 無料 （手数料額、納付方法：　手数料額： 開示請求手数料として1件300円（書面）又は200円（オンライン）　　） 納付方法：収入印紙の貼付（書面）又はオンライン納付（オンライン）
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	医籍ファイル、歯科医籍ファイル、保健師籍ファイル、助産師籍ファイル、看護師籍ファイル、理学療法士籍ファイル、臨床検査技師籍ファイル、管理栄養士名簿ファイル、薬剤師名簿、介護福祉士登録名簿ファイル
公表場所	電子政府総合窓口
⑤法令による特別の手続	
⑥個人情報ファイル簿への不記載等	

2. 特定個人情報ファイルの取扱いに関する問合せ	
①連絡先	【医籍等ファイル】（医師、歯科医師、看護師、保健師、助産師、理学療法士、臨床検査技師）】 厚生労働省医政局医事課、歯科保健課、看護課 100-8916　東京都千代田区霞が関1－2－2 03-5253-1111（内線2575、2583、4175） 【管理栄養士名簿ファイル】 厚生労働省健康局健康課 〒100-8916 東京都千代田区霞が関1-2-2 中央合同庁舎第5号館 03-5253-1111（内線2972、2953） 【薬剤師名簿ファイル】 厚生労働省医薬・生活衛生局総務課 100-8916　東京都千代田区霞が関1－2－2 03-5253-1111（内線2715） 【介護福祉士登録名簿ファイル】 厚生労働省社会・援護局福祉基盤課 〒100-8916 東京都千代田区霞が関1－2－2 03-5253-1111（内2845）
②対応方法	【医籍等ファイル】（医師、歯科医師、看護師、保健師、助産師、理学療法士、臨床検査技師）】 内部で必要な調整等を行い、担当する部署等において対応する。 【管理栄養士名簿ファイル】 内部で必要な調整等を行い、担当する部署等において対応する。 【薬剤師名簿ファイル】 内部で必要な調整等を行い、担当する部署等において対応する。 【介護福祉士登録名簿ファイル】 内部で必要な調整等を行い、担当する部署等において対応する。

Ⅵ　評価実施手続

1. 基礎項目評価	
①実施日	令和5年4月25日
②しきい値判断結果	[　　基礎項目評価及び全項目評価の実施が義務付けられる　　] ＜選択肢＞ 1) 基礎項目評価及び全項目評価の実施が義務付けられる 2) 基礎項目評価及び重点項目評価の実施が義務付けられる（任意に全項目評価を実施） 3) 基礎項目評価の実施が義務付けられる（任意に全項目評価を実施） 4) 特定個人情報保護評価の実施が義務付けられない（任意に全項目評価を実施）
2. 国民・住民等からの意見の聴取	
①方法	e-Govパブリックコメントのホームページに「特定個人情報保護評価書（全項目評価書）（案）」の意見募集公告を掲載した。意見は所定の意見提出様式により、インターネット上の意見募集フォーム及び郵送により受け付けた。
②実施日・期間	令和5年3月10日（金）～令和5年4月8日（土）
③期間を短縮する特段の理由	短縮期間なし
④主な意見の内容	「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」と記載されているが、法文等と同様のルールで「もしくは」ではなく、「又は」と記載すべきではないか。4箇所程度ある。 等
⑤評価書への反映	意見のとおり、以下4か所の「もしくは」を「又は」に修正した。 Ⅰ１．②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） 1）i.資格情報の登録 2）ii.登録情報の訂正・変更 3）iv.資格の削除 ■資格証事務（特定個人情報ファイルの取扱無） 4）ii..資格証の発行・再発行（紙） 等
3. 第三者点検	
①実施日	
②方法	
③結果	

4. 個人情報保護委員会の承認 【行政機関等のみ】	
①提出日	令和5年4月25日
②個人情報保護委員会による審査	(1)国家資格等の登録等に関する事務(医師等7資格、管理栄養士、薬剤師、介護福祉士)の内容、特定個人情報ファイルの内容、特定個人情報の流れ並びにリスク及びリスク対策が具体的に記載されており、特段の問題は認められないと考えられるが、特定個人情報保護評価書に記載されているとおり確実に実行する必要がある。 (2)特定個人情報のインターネットへの流出を防止する対策については、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等の措置が記載されているが、特定個人情報保護評価書に記載されているとおり確実に実行する必要がある。 (3)組織的及び人的安全管理措置については、適切な組織体制の整備、職員への必要な教育・研修、実効性のある自己点検・監査等を実施し、実務に即して適切に運用・見直しを行うことが重要である。 (4)情報漏えい等に対するリスク対策については、免許登録管理システムと国家資格等情報連携・活用システムとの接続はLGWAN回線又はVPN、登録情報連携システムと国家資格等情報連携・活用システムとの接続はVPN等とするとともに、各システム間の通信の暗号化等を行うことにより、通信のセキュリティを維持すること、電子記録媒体は情報の暗号化を行うとともに、入退室制限等の物理的なアクセス制御手段により、特定者以外の入室を制限し、管理区域内から電子記録媒体を持ち出すことを禁止していること等が記載されている。特定個人情報保護評価書に記載されているとおり確実に実行することに加え、不断の見直し・検討を行うことが重要である。

（別添3）変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明