

# 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
25	労働安全衛生法による免許に関する事務 全項目評価書

## 個人のプライバシー等の権利利益の保護の宣言

労働安全衛生法による免許に関する事務における特定個人情報ファイルの取扱いに当たり、同ファイルの取扱いが個人のプライバシー等の権利利益に影響を及ぼすものであることを認識し、特定個人情報の漏えいその他の事態を発生させるリスクを軽減す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7年4月30日

## 公表日

令和7年5月8日

[令和6年10月 様式4]

## 項目一覧

I 基本情報

(別添1) 事務の内容

II 特定個人情報ファイルの概要

(別添2) 特定個人情報ファイル記録項目

III 特定個人情報ファイルの取扱いプロセスにおけるリスク対策

IV その他のリスク対策

V 開示請求、問合せ

VI 評価実施手続

(別添3) 変更箇所

# I 基本情報

## 1. 特定個人情報ファイルを取り扱う事務

①事務の名称	労働安全衛生法による免許に関する事務			
	<p>【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)】</p> <p>■資格管理事務(特定個人情報ファイルの取扱有)</p> <p>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免許交付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を利用した本人確認情報等の確認を行う。</p> <p>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を利用した本人確認情報等の確認を行う。</p> <p>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。</p> <p>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を利用した本人確認情報等の確認を行う。</p> <p>■決済事務(特定個人情報ファイルの取扱無)</p> <p>i.決済 資格の登録、訂正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。</p> <p>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。</p> <p>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。</p> <p>■資格証事務(特定個人情報ファイルの取扱無)</p> <p>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。</p> <p>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。</p> <p>【労働基準行政システムに係る部分】</p> <p>■労働安全衛生法に基づく免許発行業務について 労働安全衛生法(昭和47年法律第57号)の規定に基づく20種類の免許について、免許発行の申請受理、審査、免許発行までの一連の事務に加え、登録後の免許情報の維持管理等の事務を行う。</p> <p>■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労働基準行政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。</p>			
②事務の内容	<p>※</p>			
③対象人数	[ 30万人以上 ]	<選択肢>	1) 1,000人未満 3) 1万人以上10万人未満 5) 30万人以上	2) 1,000人以上1万人未満 4) 10万人以上30万人未満

## 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	<p>■「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)</p> <ul style="list-style-type: none"> <li>i. 資格管理者等が資格登録者名簿等をクラウド上において保存・管理することを可能とする。</li> <li>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を可能とする。</li> <li>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。</li> </ul> <p>■「オンライン申請機能」(特定個人情報ファイルの取扱有)</p> <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> <li>iv. オンライン申請の際に作成される個人番号を含む資格情報については国家資格等情報連携・活用システムへ連携された後にマイナポータルからは削除される。(国家資格等情報連携・活用システムでログデータを一定期間保存した後に削除。)</li> </ul> <p>■「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)</p> <ul style="list-style-type: none"> <li>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。</li> </ul> <p>■「資格情報提供関連機能」(特定個人情報ファイルの取扱無)</p> <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>iii. 資格保有者等がオンラインでマイナンバーカードによる本人認証・同意等を行い、自己情報としての資格に関する情報を電子的な形式で第三者に提供することを可能とする。</li> <li>iv. 資格管理者等において、資格保有者等がオンラインでマイナンバーカードによる本人認証・同意等を行った際に電子的な形式で資格証と同等の情報を第三者へ提供することを可能とする。</li> </ul> <p>■「外部連携関連機能」(特定個人情報ファイルの取扱有)</p> <ul style="list-style-type: none"> <li>i. 資格管理者等が保有する既存の資格登録等に関するシステムとの連携を可能とする。(特定個人情報を含む資格情報のデータ連携機能)</li> <li>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。</li> </ul> <p>■「オンライン通知機能」(特定個人情報ファイルの取扱無)</p> <ul style="list-style-type: none"> <li>i. 資格登録申請者等は申請結果等の通知をオンラインで受取ることを可能とする。</li> <li>ii. 資格管理者等は、手続結果や各種お知らせ等をオンラインで送付することを可能とする。</li> </ul>
③他のシステムとの接続	<p>[ ] 情報提供ネットワークシステム [ ] 庁内連携システム</p> <p>[ ○ ] 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</p> <p>[ ] 宛名システム等 [ ] 税務システム</p> <p>[ ○ ] その他 (「マイナポータル」、「労働基準行政システム」)</p>

### 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	<p>■地方公共団体情報システム機構への情報照会</p> <p>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3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。</p>
③他のシステムとの接続	<p>[ ] 情報提供ネットワークシステム [ ] 庁内連携システム</p> <p>[ ] 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</p> <p>[ ] 宛名システム等 [ ] 税務システム</p> <p>[ ○ ] その他 (労働基準行政システム)</p>

### システム3

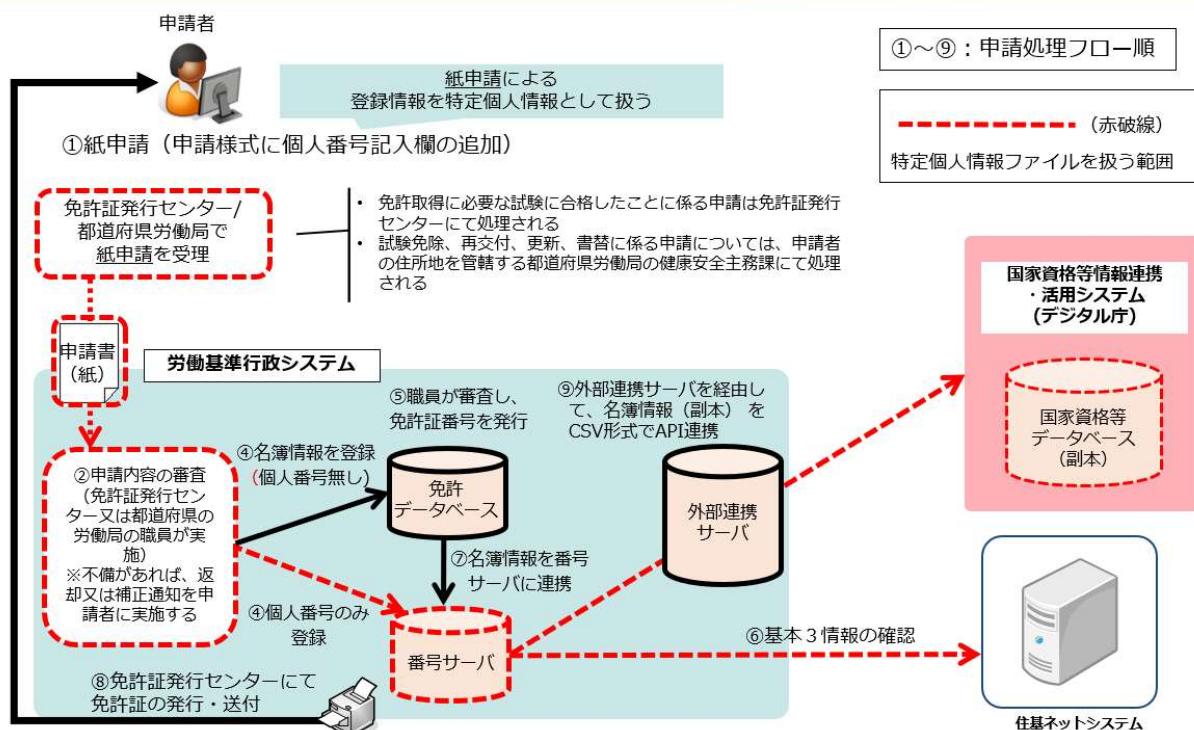
①システムの名称	マイナポータル(情報提供等記録開示システム)					
②システムの機能	<p>(1)申請受付機能(特定個人情報ファイルの取扱有)            ・申請者が資格登録等の手続を行う際に、必要な情報項目の入力、文書ファイルの添付等を可能とする。            ・申請者がマイナンバーカードの電子署名を付与し、資格管理者等に申請・提出を行うことを可能とする。            ・資格管理者等は申請者の本人確認や申請の受付、申請データの受領等を可能とする。</p> <p>(2)資格情報提供関連機能(特定個人情報ファイルの取扱無)            ・資格保有者がマイナンバーカードによる本人認証・同意を行い、自己情報としての資格に関する情報を電子的な形式で取得・表示・提示等を可能とする。            ・資格管理者等において、資格保有者がマイナンバーカードによる本人認証・同意を行った際に電子的な形式で資格証と同等の情報を資格保有者等へ提供することを可能とする。            ・資格保有者等がマイナンバーカードによる本人認証・同意等を行い、自己情報としての資格に関する情報を電子的な形式で第三者に提供することを可能とする。            ・資格管理者等において、資格保有者等がマイナンバーカードによる本人認証・同意等を行った際に電子的な形式で資格証と同等の情報を第三者へ提供することを可能とする。</p> <p>(3)オンライン通知機能(特定個人情報ファイルの取扱無)            ・申請者は申請結果等の通知をオンラインで受取ることを可能とする。            ・資格管理者等は、手続結果や各種お知らせ等をオンラインで送付することを可能とする。</p>					
③他のシステムとの接続	<p>[ ] 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 )</p>					
<b>システム4</b>						
①システムの名称	労働基準行政システム					
②システムの機能	<p>労働基準行政システムでは、労働安全衛生法に基づく免許に関する情報を的確に管理することにより、免許申請業務の簡素化、免許交付期間の短縮を図り、免許交付申請者・免許所持者に対する行政サービス向上させること等を目的としている。</p> <p>免許証発行申請書等の受付、審査を行う労働局等の拠点と、厚生労働本省で管理している労働基準行政システムのサーバを集約したセンタ環境とは、厚生労働省統合ネットワークを介し接続している。なお、労働基準行政システムでは、個人情報が端末を通じてインターネットに流出することのないようシステム面の措置を講じている。</p> <p>■管理機能(特定個人情報の取扱有)            ・資格管理者等による資格登録者名簿等の新規データ登録や既存データの更新を可能とする。            ・資格管理者等による資格登録者名簿等の保存・管理等を可能とする。            ・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を可能とする。</p> <p>■外部連携関連機能(特定個人情報の取扱有)            ・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)</p> <p>■資格情報提供関連機能(特定個人情報の取扱無)            ・資格保有者に発行する資格証の印刷機能を有する。</p>					
③他のシステムとの接続	<p>[ ] 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 )</p>					
<b>システム5</b>						
<b>システム6~10</b>						
<b>システム11~15</b>						
<b>システム16~20</b>						

3. 特定個人情報ファイル名	
安衛法免許名簿ファイル	
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	<ul style="list-style-type: none"> <li>・番号法に基づく国家資格等情報連携・活用システムとの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。</li> <li>・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3情報(氏名、生年月日、住所)を確認する必要がある。</li> </ul>
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	<ul style="list-style-type: none"> <li>・番号法第9条第1項(利用範囲) 別表 項番81の2</li> <li>・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60</li> </ul>
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	<p>[ 実施しない ] &lt;選択肢&gt;</p> <p>1) 実施する 2) 実施しない 3) 未定</p>
②法令上の根拠	
7. 評価実施機関における担当部署	
①部署	厚生労働省労働基準局労働安全衛生部計画課 厚生労働省労働基準局労災保険業務課
②所属長の役職名	計画課長 労災保険業務課長
8. 他の評価実施機関	
なし	

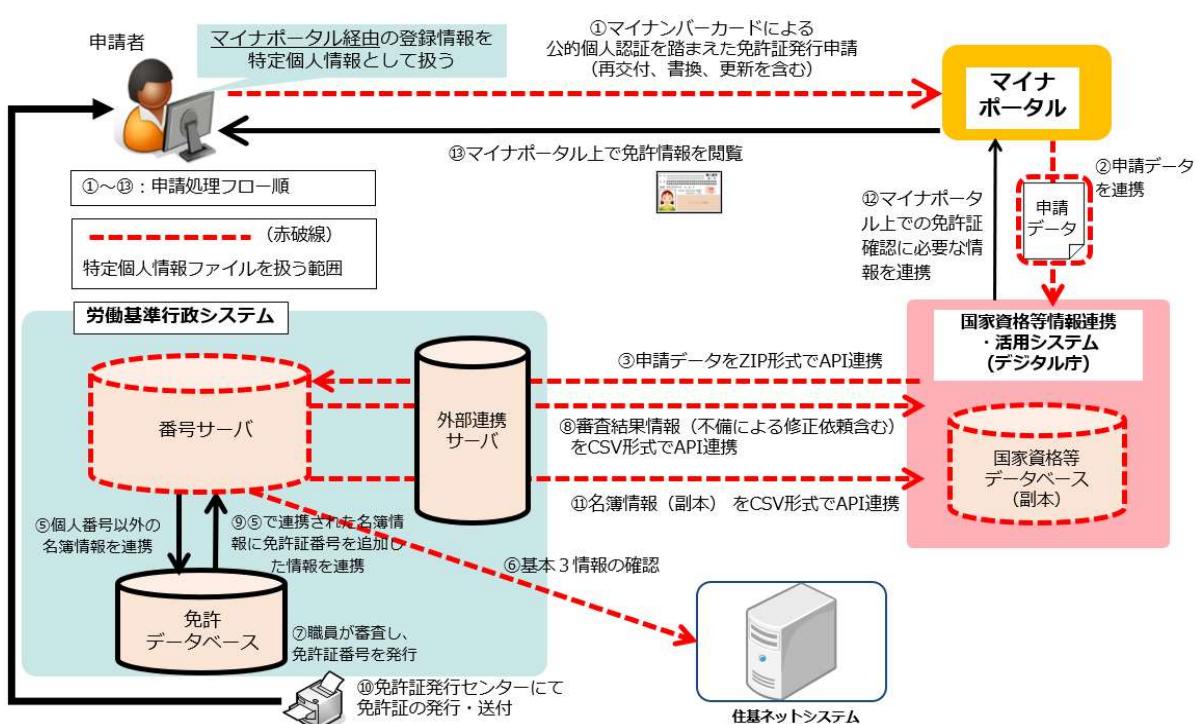
## (別添1) 事務の内容

### 安衛法免許名簿ファイル

#### 事務の流れ（紙申請の場合）



#### 事務の流れ（マイナポータルから申請が行われた場合）



**【事務の流れ】**

**■免許管理事務（個人番号利用有）**

試験合格者に対する免許証の新規発行については東京労働局に配置された「免許センター」において受付から免許証カードの交付までの業務を実施する。試験合格者以外（試験免除者等）の免許証の新規発行及び免許証カードの更新、書換、再発行については、受付から審査までを47都道府県労働局で実施し、免許証カードの発行・交付を免許センターで実施する。以下、各手続きの内容である。

・資格情報の登録

オンライン（マイナポータル）・紙での申請受理後に審査を行い、労働基準行政システムに申請情報の登録を行う。なお、住民基本台帳ネットワークシステムに対して、本人確認情報の真正性について照会・確認を行う。

・登録情報の変更

免許証発行後に、本人申請により本人確認情報の更新がある場合は、登録者名簿の情報の変更を行う。

・資格の取消し

資格保有者について資格の取消しが決定した場合、登録者名簿の情報を更新する。

**■資格証の交付事務（個人番号利用無し）**

審査の結果、免許証の発行を行う場合は、免許証カードの作成・送付を行う。再発行についても上記のとおり実施主体が異なるが、流れは同様である。

**【特定個人情報の流れ】**

**■オンライン（マイナポータル）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入力された申請情報（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国家資格等情報連携・活用システムから労働基準行政システムに申請情報（個人番号含む）が連携される。

④免許センター又は都道府県労働局で審査を行う。

⑤申請者情報の真正性を担保するため、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、基本3情報を確認する。

⑥住民基本台帳ネットワークシステムを利用して取得した本人確認情報の内容に基づき、労働基準行政システムの名簿情報の登録（更新）を行う。

⑦審査結果（不備等の修正依頼を含む）を国家資格等情報連携・活用システムに連携する。

⑧労働基準行政システムに名簿情報として申請情報を登録し、国家資格等情報連携・活用システムに名簿情報を連携する。

⑨国家資格等情報連携・活用システムからマイナポータルに免許確認に必要な情報が連携され、免許保有者はマイナポータルから資格登録情報を取得することができる。

**■紙申請の場合**

①紙で提出された申請情報について、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申請情報（個人番号含む）を資格情報として労働基準行政システムに登録する。

③免許センター又は都道府県労働局で審査を行う。

④申請者情報の真正性を担保するため、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、基本3情報を確認する。

⑤住民基本台帳ネットワークシステム等を利用して取得した本人確認情報の内容に基づき、労働基準行政システムの資格情報の登録（更新）を行う。

⑥審査の結果として免許証を発行する場合は、労働基準行政システムに名簿情報を登録し、国家資格等情報連携・活用システムに名簿情報を連携する。

⑦国家資格等情報連携・活用システムからマイナポータルに免許確認に必要な情報が連携され、免許保有者はマイナポータルから資格登録情報を取得することができる。

**（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			
安衛法免許名簿ファイル			
2. 基本情報			
①ファイルの種類 <b>※</b>	[ <input type="checkbox"/> 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	[ <input type="checkbox"/> 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 <b>※</b>	特級ボイラー技士、一級ボイラー技士、二級ボイラー技士、特別ボイラー溶接士、普通ボイラー溶接士、ボイラー整備士、特定第一種圧力容器取扱作業主任者、クレーン・デリック運転士、揚貨装置運転士、移動式クレーン運転士、ガス溶接作業主任者、林業架線作業主任者、発破技士、第一種衛生管理者、衛生工学衛生管理者、第二種衛生管理者、高圧室内作業主任者、潜水士、エックス線作業主任者、ガンマ線透過写真撮影作業主任者		
④記録される項目	[ <input type="checkbox"/> 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 <b>※</b>	<ul style="list-style-type: none"> <li>・識別情報  <input checked="" type="checkbox"/> 個人番号      [ <input type="checkbox"/> ] 個人番号対応符号      [ <input checked="" type="checkbox"/> ] その他識別情報(内部番号)</li> <li>・連絡先等情報  <input checked="" type="checkbox"/> 4情報(氏名、性別、生年月日、住所)      [ <input checked="" type="checkbox"/> ] 連絡先(電話番号等)</li> <li>・その他住民票関係情報</li> <li>・業務関係情報  <input type="checkbox"/> 国税関係情報      [ <input type="checkbox"/> ] 地方税関係情報      [ <input type="checkbox"/> ] 健康・医療関係情報  <input type="checkbox"/> 医療保険関係情報      [ <input type="checkbox"/> ] 児童福祉・子育て関係情報      [ <input type="checkbox"/> ] 障害者福祉関係情報  <input type="checkbox"/> 生活保護・社会福祉関係情報      [ <input type="checkbox"/> ] 介護・高齢者福祉関係情報  <input checked="" type="checkbox"/> 雇用・労働関係情報      [ <input type="checkbox"/> ] 年金関係情報      [ <input type="checkbox"/> ] 学校・教育関係情報  <input type="checkbox"/> 災害関係情報  <input checked="" type="checkbox"/> その他 ( 資格仮名ID、マイナポータル仮名ID、資格情報 )       </li> </ul>		
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を使用して特定個人情報の真正性を確認する。		
全ての記録項目	別添2を参照。		
⑤保有開始日	<ul style="list-style-type: none"> <li>・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</li> <li>・行政手続における特定の個人を識別するための番号の利用等に関する法律等の一部を改正する法律(令和5年法律第48号)の公布の日から起算して一年三月を超えない範囲内において政令で定める日</li> </ul>		
⑥事務担当部署	厚生労働省労働基準局労働安全衛生部計画課 厚生労働省労働基準局労災保険業務課		

### 3. 特定個人情報の入手・使用

①入手元 <b>※</b>		<input checked="" type="checkbox"/> 本人又は本人の代理人 <input type="checkbox"/> 評価実施機関内の他部署 ( ) <input type="checkbox"/> 行政機関・独立行政法人等 ( ) <input type="checkbox"/> 地方公共団体・地方独立行政法人 ( ) <input type="checkbox"/> 民間事業者 ( ) <input type="checkbox"/> その他 ( )
②入手方法		<input checked="" type="checkbox"/> 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 <input type="checkbox"/> 電子メール [ <input checked="" type="checkbox"/> 専用線 [ ] 庁内連携システム <input type="checkbox"/> 情報提供ネットワークシステム <input type="checkbox"/> その他 ( )
③入手の時期・頻度		新規の免許発行、更新、再交付、書替のための申請の都度、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。
⑤本人への明示		・番号法第9条第1項 別表81の2の項に該当しており、番号法により明示されている。 ・資格保有者からの申請に合わせて本人から入手する。
⑥使用目的 <b>※</b>		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 <b>※</b>	都道府県労働局労働基準部健康安全課、安全課または健康課
	使用者数	<選択肢> [ 100人以上500人未満 ]      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 <b>※</b>		・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を利用した情報連携を行う。
情報の突合 <b>※</b>	情報の統計分析 <b>※</b>	本人からの申請内容(登録、変更)について、システムにおける登録情報と突合する。
	権利利益に影響を与える得る決定 <b>※</b>	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る得る決定 <b>※</b>	該当なし
⑨使用開始日		令和8年3月1日

#### 4. 特定個人情報ファイルの取扱いの委託

委託の有無 <b>※</b>	[ 委託する ] ( 3 ) 件	<選択肢> 1) 委託する 2) 委託しない
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 <b>※</b>	特級ボイラー技士、一級ボイラー技士、二級ボイラー技士、特別ボイラー溶接士、普通ボイラー溶接士、ボイラー整備士、特定第一種圧力容器取扱作業主任者、クレーン・デリック運転士、揚貨装置運転士、移動式クレーン運転士、ガス溶接作業主任者、林業架線作業主任者、発破技士、第一種衛生管理者、衛生工学衛生管理者、第二種衛生管理者、高圧室内作業主任者、潜水士、エックス線作業主任者、ガンマ線透過写真撮影作業主任者	
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いを委託することが必要であるため。	
③委託先における取扱者数	[ 10人以上50人未満 ]	<選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上
④委託先への特定個人情報ファイルの提供方法	[ ] 専用線 [ ] 電子メール [ ○ ] 電子記録媒体(フラッシュメモリを除く。) [ ] フラッシュメモリ [ ] 紙 [ ○ ] その他 ( システム直接操作 )	
⑤委託先名の確認方法	委託業務の調達結果については官報公示及びホームページ公表により確認可能	
⑥委託先名	株式会社 NTTデータ	
⑦再委託の有無 <b>※</b>	[ 再委託する ]	<選択肢> 1) 再委託する 2) 再委託しない
再委託	⑧再委託の許諾方法	<p>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。</p> <p>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。</p> <p>(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</p> <p>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。</p>
	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。

<b>委託事項2</b>		労働基準行政システムの運用等業務
①委託内容		労働基準行政システムの運用保守業務
②取扱いを委託する特定個人情報ファイルの範囲		<p style="text-align: right;">&lt;選択肢&gt;</p> <p>[ 特定個人情報ファイルの全体 ]</p> <p>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</p>
対象となる本人の数		<p style="text-align: right;">&lt;選択肢&gt;</p> <p>[ 100万人以上1,000万人未満 ]</p> <p>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</p>
対象となる本人の範囲 ※		特級ボイラー技士、一級ボイラー技士、二級ボイラー技士、特別ボイラー溶接士、普通ボイラー溶接士、ボイラー整備士、特定第一種圧力容器取扱作業主任者、クレーン・デリック運転士、揚貨装置運転士、移動式クレーン運転士、ガス溶接作業主任者、林業架線作業主任者、発破技士、第一種衛生管理者、衛生工学衛生管理者、第二種衛生管理者、高圧室内作業主任者、潜水士、エックス線作業主任者、ガンマ線透過写真撮影作業主任者
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・技術を要すること等、全体の取扱いを委託することが必要であるため。
③委託先における取扱者数		<p style="text-align: right;">&lt;選択肢&gt;</p> <p>[ 10人以上50人未満 ]</p> <p>1) 10人未満 3) 50人以上100人未満 5) 500人以上1,000人未満 2) 10人以上50人未満 4) 100人以上500人未満 6) 1,000人以上</p>
④委託先への特定個人情報ファイルの提供方法		<p>[ ] 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。)</p> <p>[ ] フラッシュメモリ [ ] 紙</p> <p>[ ○ ] その他 ( システムが設置されるデータセンター内にて取扱いを行う )</p>
⑤委託先名の確認方法		調達結果(委託先名)は官報公示及びホームページ公表により、国民等が確認可能。
⑥委託先名		株式会社 NTTデータ
再委託	⑦再委託の有無 ※	<p style="text-align: right;">&lt;選択肢&gt;</p> <p>[ 再委託する ]</p> <p>1) 再委託する 2) 再委託しない</p>
	⑧再委託の許諾方法	原則として再委託は行わないこととするが、再委託を行う場合には、委託先から再委託先の商号又は名称、住所、再委託する理由、再委託する業務の範囲、再委託先に係る業務の履行能力、再委託予定金額等及びその他の厚生労働省が求める情報について記載した書面による再委託申請及び再委託に係る履行体制図の提供を受け、委託先と再委託先が秘密保持に関する契約を締結していること等、再委託先における安全管理措置を確認し、決裁等必要な手続を経た上で、再委託を承認する。
	⑨再委託事項	上記委託事項と同じ。

<b>委託事項3</b>	免許申請書の記載事項確認業務		
①委託内容	労働安全衛生法に関する免許申請書の記載事項確認業務		
②取扱いを委託する特定個人情報ファイルの範囲	<p style="text-align: center;">&lt;選択肢&gt;</p> <p>[ 特定個人情報ファイルの全体 ]      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</p>		
対象となる本人の数	<p style="text-align: center;">&lt;選択肢&gt;</p> <p>[ 100万人以上1,000万人未満 ]      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</p>		
対象となる本人の範囲 ※	特級ボイラー技士、一級ボイラー技士、二級ボイラー技士、特別ボイラー溶接士、普通ボイラー溶接士、ボイラー整備士、特定第一種圧力容器取扱作業主任者、クレーン・デリック運転士、揚貨装置運転士、移動式クレーン運転士、ガス溶接作業主任者、林業架線作業主任者、発破技士、第一種衛生管理者、衛生工学衛生管理者、第二種衛生管理者、高圧室内作業主任者、潜水士、エックス線作業主任者、ガンマ線透過写真撮影作業主任者		
その妥当性	労働安全衛生法に基づく免許発行業務において申請段階の不備を減らし、免許証発行業務の迅速・円滑化を図るために、申請書類の不備の確認及び必要書類の督促並びに発送用封筒への封入及び郵便局への持ち込みなどの業務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	<p style="text-align: center;">&lt;選択肢&gt;</p> <p>[ 10人以上50人未満 ]      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</p>		
④委託先への特定個人情報ファイルの提供方法	<p>[ ] 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。)</p> <p>[ ] フラッシュメモリ      [ ○ ] 紙</p> <p>[ ] その他 ( )</p>		
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	株式会社綜合キャリアオプション		
再委託	⑦再委託の有無 ※	<p style="text-align: center;">&lt;選択肢&gt;</p> <p>[ 再委託する ]      1) 再委託する      2) 再委託しない</p>	
	⑧再委託の許諾方法	<ul style="list-style-type: none"> <li>契約に係る事務又は事業の全部を一括して第三者に委託することはできない。なお、委託契約金額に占める再委託契約金額の割合は、原則2分の1未満とする。</li> <li>委託業務における総合的な企画及び判断並びに業務遂行管理部分は、再委託してはならない。</li> <li>委託業務の一部を再委託する場合は、事前に再委託する業務、再委託先を東京労働局に申請し、承認を受けること。</li> <li>再委託を行う場合は、その最終的な責任は受託者が負うこと。</li> </ul>	
	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。	
<b>委託事項4</b>			
<b>委託事項5</b>			
<b>委託事項6~10</b>			
<b>委託事項11~15</b>			
<b>委託事項16~20</b>			
<b>5. 特定個人情報の提供・移転(委託に伴うものを除く。)</b>			
提供・移転の有無	<p>[ ] 提供を行っている ( ) 件      [ ] 移転を行っている ( ) 件</p> <p>[ ○ ] 行っていない</p>		
提供先1			
提供先2~5			
提供先6~10			
提供先11~15			
提供先16~20			

移転先1	
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

		<p>【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)】</p> <p>イ) クラウドサービスに係る要件は、主に次のを満たすものとする。</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> <li>・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。</li> <li>・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。</li> <li>・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。</li> <li>・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。</li> </ul> <p>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。</p> <p>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。</p> <p>二) 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。</p> <p>【労働基準行政システムに係る部分】</p> <p>・セキュリティゲートにて入退館管理をしている建物の中で、さらに入退室管理(※)を行っている部屋(サーバ室)に設置したサーバ内に保管する。また、サーバへのアクセスはID及びパスワードによる認証が必要となる。</p> <p>※サーバ室内への入室権限を持つ者を限定し、入退室管理カード等によりサーバ室に入退室する者が権限を有することを確認する等の管理を行う。</p>												
②保管期間	期間	<p>【選択肢】</p> <table style="margin-left: auto; margin-right: auto;"> <tr> <td>1) 1年未満</td> <td>2) 1年</td> <td>3) 2年</td> </tr> <tr> <td>4) 3年</td> <td>5) 4年</td> <td>6) 5年</td> </tr> <tr> <td>7) 6年以上10年未満</td> <td>8) 10年以上20年未満</td> <td>9) 20年以上</td> </tr> <tr> <td colspan="3">10) 定められていない</td> </tr> </table> <p>[ 定められていない ]</p>	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		
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														
③消去方法	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。												
		<p>【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)】</p> <p>・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。</p> <p>「オンプレミス環境の場合」</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> </ul> <p>「クラウド環境の場合」</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> </ul> <p>【労働基準行政システムに係る部分】</p> <p>消去しない。</p>												
<h2>7. 備考</h2>														
特に無し														

(別添2) 特定個人情報ファイル記録項目

別紙1参照

### 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	
安衛法免許名簿ファイル	
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	<p>【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）】  <b>【オンライン申請からの入手】</b>          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。</p> <p>【窓口等（郵送を含む）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。</p> <p>【労働基準行政システムに係る部分】          ・申請書の提出があり、安衛法に基づく免許に係る資格名簿に登録して問題ない者のみ労働基準行政システムに登録しているため、対象者以外の情報を入手することはない。</p>
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	<p>【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）】  <b>【オンライン申請からの入手】</b>          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。</p> <p>【窓口等（郵送を含む）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ます。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・添付書類のみを記載・提出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。</p> <p>【労働基準行政システムに係る部分】          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ます。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・添付書類のみを記載・提出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。</p>
その他の措置の内容	-
リスクへの対策は十分か	<p>[      十分である      ]      &lt;選択肢&gt;</p> <p>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</p>
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	<p>【オンライン申請からの入手】          オンライン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。</p> <p>【窓口等（郵送を含む）における申請からの入手】          ・窓口等（郵送を含む）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。</p>
リスクへの対策は十分か	<p>[      十分である      ]      &lt;選択肢&gt;</p> <p>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</p>

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	<p><b>【オンライン申請からの入手】</b> 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。</p> <p><b>【窓口等(郵送を含む)における申請からの入手】</b> 窓口等(郵送を含む)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等顔写真付きの身分証明書は1点、住民票の写し等顔写真のない身分証明書については2点で確認する。</p>					
個人番号の真正性確認の措置の内容	<p><b>【オンライン申請からの入手】</b> 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。</p> <p><b>【窓口等(郵送を含む)における申請からの入手】</b> 窓口等(郵送を含む)において申請を受け付ける場合は、マイナンバーカード、個人番号の記載された住民票の写し等で、個人番号の真正性確認を行う。</p>					
特定個人情報の正確性確保の措置の内容	<p><b>【オンライン申請からの入手】</b> 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。</p> <p><b>【窓口における申請からの入手】</b> 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。</p>					
その他の措置の内容						
リスクへの対策は十分か	<p>[      十分である      ]      &lt;選択肢&gt;</p> <p>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</p>					
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	<p><b>【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)】</b>  <b>【オンライン申請からの入手】</b> 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、TLS/SSLによる暗号化された通信経路を使用することで漏えい・紛失を防止する。 ※マイナポータル内に情報等は保管されない。 登録画面により入手する情報等は、専用線及びクラウド内部の通信によりシステムへ登録されることで、漏えい・紛失することを防止している。</p> <p><b>【窓口における申請からの入手】</b> 窓口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。</p> <p><b>【郵送による申請等からの入手】</b> 郵送による申請を受け付ける場合、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。また、都道府県労働局間、都道府県労働局と免許証発行センター等の行政機関間で申請書等の郵送でのやりとりを行う場合も同様の扱いとする。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。</p> <p><b>【労働基準行政システムとの接続】</b> 国家資格等情報連携・活用システムとの接続については専用回線による接続により、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。</p>					
リスクへの対策は十分か	<p>[      十分である      ]      &lt;選択肢&gt;</p> <p>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</p>					
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	<p>【国家資格等情報連携・活用システムに係る部分】</p> <p>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。</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> <li>・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。</li> </ul> <p>【労働基準行政システムに係る部分】</p> <ul style="list-style-type: none"> <li>・国家資格等情報連携・活用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な無い情報との紐付けが行えない仕組みとしている。</li> <li>・住民基本台帳ネットワークシステムとの連携についても、権限を有する者のみ連携できるようアクセス制御を行う。</li> <li>・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。</li> </ul>
その他の措置の内容	
リスクへの対策は十分か	<p>[      十分である      ]      &lt;選択肢&gt;</p> <p>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</p>

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>	
具体的な管理方法		1) 行っている	2) 行っていない
	<p>【国家資格等情報連携・活用システムに係る部分】</p> <p>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」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。委託先は以下の作業を行う(以下、リスク2において同様)。</p> <p>(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。</p> <p>情報システム責任者等は以下の作業を行う。</p> <p>(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。            (5)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。            (6)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。</p> <p>※労働基準行政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。</p> <p>【労働基準行政システムに係る部分】</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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利用者ごとにIDを割り当てる。</li> <li>・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。</li> </ul>		
アクセス権限の発効・失効の管理	[ 行っている ]	<選択肢>	
具体的な管理方法		1) 行っている	2) 行っていない
	<p>【国家資格等情報連携・活用システムに係る部分】</p> <p>情報システム責任者等は以下の作業を行う。</p> <p>(1)発行の管理</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> <li>・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。</li> </ul> <p>(2)失効の管理</p> <ul style="list-style-type: none"> <li>・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。</li> </ul> <p>【労働基準行政システムに係る部分】</p> <p>(1)発行の管理</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> <li>・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。</li> </ul> <p>(2)失効の管理</p> <ul style="list-style-type: none"> <li>・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。</li> </ul>		

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	<p>【国家資格等情報連携・活用システムに係る部分】</p> <p>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。</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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帳を割り当てる。</li> <li>・情報システム責任者等は、事務従事者に係るユーザー帳の割り当て状況等を隨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。</li> </ul> <p>【労働基準行政システムに係る部分】</p> <ul style="list-style-type: none"> <li>・アクセス権限は、当該事務に従事する者に限定して付与する。</li> <li>・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帳を割り当てる。</li> <li>・情報システム責任者等は、事務従事者に係るユーザー帳の割り当て状況等を隨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。</li> <li>・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。</li> </ul>		
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	<p>【国家資格等情報連携・活用システムに係る部分】</p> <p>・情報システム責任者等は以下の作業を行う。</p> <ol style="list-style-type: none"> <li>(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。</li> <li>(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、アカウント払出し状況の目視確認を実施する。</li> <li>(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。</li> <li>(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、速やかに委託先に報告する等、必要な対応をとる。</li> </ol> <p>【労働基準行政システムに係る部分】</p> <p>職員が特定個人情報へアクセスした履歴(個人番号、アクセスした日時、職員名等)はログとして労働基準行政システムに保存され、月次で磁気テープ(媒体)に記録を移す。ログは定期的にチェックを行うだけでなく、必要に応じて隨時チェックを行う。</p> <p>番号法第23条に基づく番号法施行令第29条により情報提供等の記録の保存期間が7年とされていることを考慮し、ログの保存期間は7年間以上とする。</p>		
その他の措置の内容	労働基準行政システムへのアクセス権限が付与された他部署の職員等は、当該システムに保存されている特定個人情報へアクセスできないように制御を行い、特定個人情報へアクセスする機能の利用制御や、個人番号の表示の有無の制御等、システムで制御されている。		
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 3) 課題が残されている 2) 十分である	

### 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	<p><b>【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)】</b>          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。</p> <p><b>【労働基準行政システムに係る部分】</b></p> <ul style="list-style-type: none"> <li>・業務外利用の禁止について厚生労働省情報セキュリティポリシーに定めるとともに、年に1回実施する全職員を受講対象とした情報セキュリティに関する研修において業務外利用の禁止等について周知・徹底する。</li> <li>・厚生労働省情報セキュリティポリシーにより、許可されたもの以外のUSBメモリの使用を禁止しており、許可を受けたUSBメモリ以外は使用できないよう、システムで制御されている他、CD、DVD等のUSB以外の磁気媒体への書き込み・保存はできないよう、個々の職員に配置される端末では、CD、DVD等のドライブが使用できないよう、システム的な対策を講じている。</li> <li>・個人番号を含むCSVやPDFファイル等をダウンロードする機能(外部媒体へのダウンロードを含む。)は設けない。</li> <li>・個人番号を含む特定個人情報を取り扱う必要のある職員にのみ、システム内の特定個人情報へのアクセスを許可することで、必要最小限の職員に限定するとともに、ログ等を定期及び必要に応じ隨時に分析し、不適切な使用を防止する。</li> </ul>
リスクへの対策は十分か	<p>[ 十分である ] &lt;選択肢&gt;</p> <p>1) 特に力を入れている 3) 課題が残されている</p> <p>2) 十分である</p>

### 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	<p><b>【国家資格等情報連携・活用システムに係る部分】</b></p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> </ul> <p><b>【労働基準行政システムに係る部分】</b></p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> <li>・運用作業は原則二人で行う相互牽制体制とする。</li> <li>・運用業者、保守業者に対しては、厚生労働省セキュリティポリシーに則り、許可された者以外のUSBメモリの使用を禁止しており、許可を受けたUSBメモリ以外は使用できないよう、システムで制御されている。</li> <li>・アクセスログを取得することで、不適切な端末操作を抑止する。</li> <li>・労働基準行政システムには、個人番号を含むCSVやPDFファイル等をダウンロードする機能(外部媒体へのダウンロードを含む。)は設けない。</li> <li>・許可を受けたUSBを持ち出す際にあっては、責任者に都度申請をして利用することとし、使用の記録等を管理簿(使用簿)に記載することとする。また、使用後は速やかに施錠可能な場所に保管するほか、許可を受けたUSBメモリを廃棄する際は物理的に破壊するなど、不適切な使用を防止する。</li> <li>・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携については、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GSSネットワークや総合行政ネットワーク等の専用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。</li> </ul>
リスクへの対策は十分か	<p>[ 十分である ] &lt;選択肢&gt;</p> <p>1) 特に力を入れている 3) 課題が残されている</p> <p>2) 十分である</p>

### 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

<p><b>【国家資格等情報連携・活用システムに係る部分】</b></p> <ul style="list-style-type: none"> <li>・特定個人情報の管理を含む業務運用の委託を行う際は、プライバシーマークやISMS(ISO/IEC27001)等の認証取得業者であること等特定個人情報の保護を適切に行えることを確認する。</li> </ul> <p><b>【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】</b></p> <p>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。</p> <ul style="list-style-type: none"> <li>・特定個人情報ファイルの閲覧者・更新者の制限</li> <li>・特定個人情報ファイルの取扱いの記録</li> <li>・特定個人情報の提供ルール/消去ルール</li> <li>・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</li> <li>・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</li> </ul> <p><b>【労働基準行政システムに係る部分】</b></p> <p>委託先を選定する際に、個人情報管理体制を確認するため下記の事項を記載した「情報セキュリティの管理体制」を提出させることとしている。</p> <ul style="list-style-type: none"> <li>・行政機関等からの個人情報の取扱いを含む業務の受託実績</li> <li>・プライバシーマーク又はISO/IEC27001の認証取得状況</li> </ul> <p><b>【免許センターから審査依頼を行う委託業者に係る部分】</b></p> <ul style="list-style-type: none"> <li>・委託先の選定を行う際は、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。</li> </ul>			
特定個人情報ファイルの閲覧者・更新者の制限	<p>[      制限している      ]</p>	<p>&lt;選択肢&gt;</p> <p>1) 制限している</p>	2) 制限していない
具体的な制限方法	<p><b>【国家資格等情報連携・活用システムに係る部分】</b></p> <p>委託先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。</p> <p><b>【労働基準行政システムに係る部分】</b></p> <p>委託先は、委託業務の実施に当たり、特定個人情報ファイルにアクセスできる業務委託員を必要最小限に特定し、当該者のみアクセス権限を付与する。また、アクセス権限の設定に当たっては、業務上の責務と必要性を勘案し、必要最小限の範囲に限って許可を与える。</p> <p><b>【免許センターから審査依頼を行う委託業者に係る部分】</b></p> <p>委託先は、委託業務の実施に当たり、特定個人情報ファイルを取り扱うことができる業務委託員を必要最小限に特定し、当該者のみ取り扱い権限を付与する。また、取り扱い権限の設定に当たっては、業務上の責務と必要性を勘案し、必要最小限の範囲に限って許可を与える。</p>		

特定個人情報ファイルの取扱いの記録	<p>[ 記録を残している ]</p> <p style="text-align: right;">&lt;選択肢&gt;</p> <p style="text-align: right;">1) 記録を残している</p> <p style="text-align: right;">2) 記録を残していない</p>
具体的な方法	<p><b>【国家資格等情報連携・活用システムに係る部分】</b> 委託先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。</p> <p><b>【労働基準行政システムに係る部分】</b> 委託先は、特定個人情報ファイルへのアクセス記録を取得・分析し、記録を保存するとともに、作業実施後に委託業務以外の作業を実施していないか確認する。また、アクセス記録、電子計算組織の監視を行うとともに、監視状況に係る監査を定期的に行う。</p> <p><b>【免許センターから審査依頼を行う委託業者に係る部分】</b> 委託元は、特定個人情報ファイルへの取り扱い記録を取得・分析し、記録を保存する。また、委託業務の内容が適切に実施されているか、委託先が定期的に確認を行う。</p>
特定個人情報の提供ルール	<p>[ 定めている ]</p> <p style="text-align: right;">&lt;選択肢&gt;</p> <p style="text-align: right;">1) 定めている</p> <p style="text-align: right;">2) 定めていない</p>
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	<p><b>【国家資格等情報連携・活用システムに係る部分】</b> 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。</p> <p><b>【労働基準行政システムに係る部分】</b> 契約書に、契約の履行において知り得た秘密を、他に漏らしてはならない旨を定めており、委託先から他者への特定個人情報の提供は認めていない。</p> <p><b>【免許センターから審査依頼を行う委託業者に係る部分】</b> 契約書に、契約の履行において知り得た秘密を、他に漏らしてはならない旨を定めており、委託先から他者への特定個人情報の提供は認めていない。</p>
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	<p><b>【国家資格等情報連携・活用システムに係る部分】</b> 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。</p> <p><b>【労働基準行政システムに係る部分】</b> 委託先に提供する際に、使用目的、情報の内容を記載した申請書を使用し、それを厚生労働省の情報セキュリティ責任者が確認する。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、提供情報は委託業務完了時に全て返却又は消去する。</p> <p><b>【免許センターから審査依頼を行う委託業者に係る部分】</b> 契約時、使用目的、情報の内容を記載した申請書を委託先から委託元へ提出させている。授受記録については、委託元が媒体・利用期限、返却方法を記載した台帳を作成する。また、提供情報は委託業務完了時に全て返却又は廃棄する。</p>

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		<p>【国家資格等情報連携・活用システムに係る部分】</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> </ul> <p>「オンプレミス環境の場合」</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> <li>・情報システム責任者等は委託先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。</li> </ul> <p>「クラウド環境の場合」</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・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。</li> <li>・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。</li> <li>・情報システム責任者等は委託先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。</li> </ul> <p>【労働基準行政システムに係る部分】</p> <p>特定個人情報が記録された書面を廃棄する場合には、復元が困難な状態にする。また、特定個人情報が保存された電子計算機及び外部記録媒体を廃棄する場合は、データ消去ソフトウェア若しくはデータ消去装置の利用又は物理的な破壊若しくは磁気的な破壊により、復元が困難な状態にする。消去作業後に、廃棄等に関する実施結果を厚生労働省に報告させる。</p> <p>【免許センターから審査依頼を行う委託業者に係る部分】</p> <p>委託先は、特定個人情報が記録された書面(申請書)について、審査済みとなった申請書を免許センターに都度返却する。</p>	

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	<p>【国家資格等情報連携・活用システムに係る部分】</p> <ul style="list-style-type: none"> <li>・秘密保持義務</li> <li>・事業所内からの特定個人情報の持ち出し禁止</li> <li>・特定個人情報の目的外利用の禁止</li> <li>・再委託における条件</li> <li>・漏えい事案等が発生した場合の委託先の責任</li> <li>・委託契約終了後の特定個人情報の返却または廃棄</li> <li>・従事者に対する監督・教育</li> <li>・契約内容の遵守状況について報告を求める規定</li> <li>・委託内容及び作業場所</li> <li>・管理区域等の明確化</li> <li>・漏えい、滅失、毀損、紛失及び改ざん等の防止策</li> <li>・委託先に対する実地調査</li> <li>・運用状況の記録の提供等</li> </ul> <p>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。</p> <p>【労働基準行政システムに係る部分】</p> <ul style="list-style-type: none"> <li>・秘密保持義務</li> <li>・特定個人情報の目的外利用の禁止</li> <li>・再委託における条件</li> <li>・漏えい事案等が発生した場合の委託先の責任</li> <li>・委託契約終了後の特定個人情報の返却または廃棄</li> </ul> <p>【免許センターから審査依頼を行う委託業者に係る部分】</p> <ul style="list-style-type: none"> <li>・秘密保持義務</li> <li>・特定個人情報の目的外利用の禁止</li> <li>・再委託における条件</li> <li>・漏えい事案等が発生した場合の委託先の責任</li> <li>・委託契約終了後の特定個人情報の返却または廃棄</li> </ul>	
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	<p>【国家資格等情報連携・活用システムに係る部分】</p> <p>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。</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・委託先は、定期的又は必要に応じて、再委託先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。</li> <li>・情報システム責任者等は、委託先から再委託先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への立入検査の実施を依頼する。</li> </ul> <p>【労働基準行政システムに係る部分】</p> <p>原則として再委託は行わないこととするが、再委託を行う場合には、以下の内容を確認した上で、決裁等必要な手続きを経た上で再委託を承認する。</p> <ul style="list-style-type: none"> <li>・秘密保持義務</li> <li>・特定個人情報の目的外利用の禁止</li> <li>・再委託における条件</li> <li>・漏えい事案等が発生した場合の再委託先の責任</li> <li>・再委託契約終了後の特定個人情報の返却または廃棄</li> </ul> <p>【免許センターから審査依頼を行う委託業者に係る部分】</p> <p>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。</p> <ul style="list-style-type: none"> <li>・契約に係る事務又は事業の全部を一括して第三者に委託することはできない。なお、委託契約金額に占める再委託契約金額の割合は、原則2分の1未満とする。</li> <li>・委託業務における総合的な企画及び判断並びに業務遂行管理部分は、再委託してはならない。</li> <li>・委託業務の一部を再委託する場合は、事前に再委託する業務、再委託先を東京労働局に申請し、承認を受けること。</li> <li>・再委託を行う場合は、その最終的な責任は受託者が負うこと。</li> </ul>	
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 3) 課題が残されている	2) 十分である
			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			
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
リスク2: 安全が保たれない方法によって入手が行われるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[ ]	<選択肢>	
		1) 特に力を入れている	2) 十分である
リスク3: 入手した特定個人情報が不正確であるリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[ ]	<選択肢>	
		1) 特に力を入れている	2) 十分である
リスク4: 入手の際に特定個人情報が漏えい・紛失するリスク			
リスクに対する措置の内容			
リスクへの対策は十分か	[ ]	<選択肢>	
		1) 特に力を入れている	2) 十分である
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
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
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
情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置			

## 7. 特定個人情報の保管・消去

### リスク1：特定個人情報の漏えい・滅失・毀損リスク

①NISC政府機関統一基準群 ②安全管理体制 ③安全管理規程 ④安全管理体制・規程の職員への周知 ⑤物理的対策	[ 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
	[ 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
	[ 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
	[ 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
	[ 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
	<p><b>【国家資格等情報連携・活用システムに係る部分】</b></p> <p>(1)パブリッククラウド環境における物理的対策</p> <ul style="list-style-type: none"> <li>委託先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。</li> <li>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。</li> <li>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。</li> </ul> <p>(2)オンプレミス環境における物理的対策</p> <ul style="list-style-type: none"> <li>委託先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。</li> <li>また、具体的な対策の内容としては、例えば、委託先は日本国内にオンプレミス環境を設置し、委託先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。</li> <li>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。</li> </ul> <p><b>【労働基準行政システムに係る部分】</b></p> <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> <li>厚生労働省情報セキュリティポリシーにより、許可されたもの以外のUSBメモリの使用を禁止し、システムの情報が保存されているUSBメモリ等の廻外への持ち出しを禁止している。</li> <li>許可を受けたUSBメモリ以外は使用できないよう、システムで制御されている。</li> </ul>	

⑥技術的対策	<p>[ 十分に行っている ]</p> <p>【選択肢】</p> <p>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</p>
具体的な対策の内容	<p>【国家資格等情報連携・活用システムに係る部分】</p> <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul> <p>【労働基準行政システムに係る部分】</p> <ul style="list-style-type: none"> <li>権限を有する者以外は個人情報にアクセスできないように制御している。</li> <li>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。</li> <li>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。</li> <li>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。</li> <li>ファイアウォール、URLフィルタリング、ウイルス対策ソフト等を導入し、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。</li> <li>申請書等の受付、審査を行う労働局等の拠点と、労働基準行政システム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ネットワーク（厚生労働省統合ネットワーク）を利用し、安全性を確保する。</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul>
⑦バックアップ	<p>[ 十分に行っている ]</p> <p>【選択肢】</p> <p>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</p>
⑧事故発生時手順の策定・周知	<p>[ 十分に行っている ]</p> <p>【選択肢】</p> <p>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</p>
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	<p>[ 発生あり ]</p> <p>【選択肢】</p> <p>1) 発生あり      2) 発生なし</p>
その内容	別紙2参照
再発防止策の内容	別紙2参照

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 3) 課題が残されている 2) 十分である
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	<p>【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。</p> <p>【労働基準行政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。</p>	
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 3) 課題が残されている 2) 十分である

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>	
手順の内容		·マイナポータル内に情報等は保管されない。 ·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。 ·パブリッククラウド環境では、データの復元がなされないよう、パブリッククラウド事業者においてISO/IEC27001に準拠した廃棄プロセスを確保する。 ·特定個人情報の消去ルールに従い、システムから特定個人情報等の消去を行う。なお、クラウド環境ではアカウント誤削除対策としてアカウント削除後も一定期間情報が保持される可能性があるため、アカウント削除前に論理的なデータ消去を行う。 ·委託先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。	1) 定めている 2) 定めていない
その他の措置の内容			
リスクへの対策は十分か	[ 十分である ]	<選択肢>	
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	<p>【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。</p> <p>【安衛法免許名簿ファイル】          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。</p>
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	<p>【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。</p> <p>【安衛法免許名簿ファイル】          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。</p>

### 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	<p>【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。</p> <p>【安衛法免許名簿ファイル】          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。</p>

### 3. その他のリスク対策

<p>【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、適切な対応をとができる体制を構築する。</p> <p>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。</p> <p>&lt;特定個人情報の漏えい等事案が発生した場合の対応&gt;</p> <ul style="list-style-type: none"> <li>①組織内における報告及び被害の拡大防止</li> <li>②事実関係の調査及び原因究明</li> <li>③影響範囲の特定</li> <li>④再発防止策の検討・実施</li> <li>⑤影響を受ける可能性のある本人への連絡等</li> <li>⑥事実関係、再発防止策等の公表</li> <li>⑦個人情報保護委員会への報告</li> </ul>
--

## 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 東京都千代田区霞が関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 ( <a href="http://www.mhlw.go.jp/jouhou/hogo05/index.html">http://www.mhlw.go.jp/jouhou/hogo05/index.html</a> ) ※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。 ( <a href="http://www.mhlw.go.jp/jouhou/hogo06/index.html">http://www.mhlw.go.jp/jouhou/hogo06/index.html</a> ) 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	<p style="text-align: center;">[ 有料 ] &lt;選択肢&gt;</p> <p style="text-align: right;">1) 有料      2) 無料</p> <p>手数料額: (手数料額、納付方法: 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)</p>
④個人情報ファイル簿の公表	<p style="text-align: center;">[ 行っている ] &lt;選択肢&gt;</p> <p style="text-align: right;">1) 行っている    2) 行っていない</p>
個人情報ファイル名	安衛法免許名簿ファイルの登録情報
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	厚生労働省労働基準局労働安全衛生部計画課 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5607,5549)  厚生労働省労働基準局労災保険業務課 177-0044 東京都練馬区上石神井4-8-3 03-3920-3311(内線322)
②対応方法	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7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7年3月22日(土)から同年4月21日(月)までの30日間
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	「反対」というご意見が1件あった。
⑤評価書への反映	反映なし
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7年4月25日
②個人情報保護委員会による審査	(1)労働安全衛生法による免許に関する事務の内容、特定個人情報ファイルの内容、特定個人情報の流れ並びにリスク及びリスク対策が具体的に記載されており、特段の問題は認められないと考えられるが、特定個人情報保護評価書に記載されているとおり確実に実行する必要がある。  (2)特定個人情報のインターネットへの流出を防止する対策については、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。今後リスクを相当程度変動させ得る事実関係の変更が生じ、当該変更に応じたリスク対策を講ずる際などには、必要な特定個人情報保護評価を適切に実施する体制を、有効に機能させることが重要である。  (4)委託先事業者との個人番号が記載された免許申請書の授受及び、特定個人情報ファイルの適正な取扱いの確保等の情報漏えい等に対するリスク対策全般について、特定個人情報保護評価書に記載されているとおり確実に実行する必要がある。  (5)上記について、不断の見直し・検討を行うことに加え、事務の開始やシステム変更に伴い、事務フローの変更や新たなリスク対策が生ずることとなった場合は、必要に応じて評価の再実施を行うことが重要である。

(別添3) 変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明

(安衛法免許名簿ファイル)

- ・個人番号
- ・個人番号更新フラグ
- ・最終更新日時
- ・申請区分コード
- ・申請区分名
- ・資格 ID
- ・資格名（漢字）
- ・事務 ID
- ・事務名
- ・資格取扱単位コード
- ・資格取扱単位名
- ・申請 ID
- ・受付年月日
- ・業務種別コード
- ・業務種別名
- ・資格手続コード
- ・手続名
- ・登録番号
- ・都道府県コード
- ・都道府県名（漢字）
- ・郵送元受付機関コード
- ・郵送元受付機関名
- ・受付機関コード
- ・受付機関名
- ・申請者氏名（漢字）
- ・申請者氏名（かな／カナ）
- ・申請者住所
- ・申請者生年月日
- ・申請者性別コード
- ・申請者電話番号
- ・申請者メールアドレス
- ・マイナンバーカード住所
- ・マイナンバーカード氏名
- ・マイナンバーカード生年月日
- ・マイナンバーカード性別コード

- ・マイナンバーカード情報取得日時
- ・旧姓併記希望
- ・旧姓
- ・外字表記希望
- ・機構保存本人確認情報等照会結果
- ・機構保存本人確認情報等照会日時
- ・戸籍関係情報照会結果
- ・戸籍関係情報照会日時
- ・名簿ステータス
- ・資格仮名
- ・登録年月日
- ・デジタル証発行年月日
- ・デジタル証訂正・変更年月日
- ・デジタル証再発行年月日
- ・取消年月日
- ・一時停止期間（開始）
- ・一時停止期間（終了）
- ・資格別取消・一時停止等処分コード
- ・取消・一時停止処分年月日
- ・取消・一時停止事由
- ・システム登録日時
- ・システム更新日時
- ・削除反映区分
- ・合格者番号
- ・合格年月日
- ・本籍地コード
- ・本籍地（和名）
- ・郵送要否
- ・送付先住所
- ・備考
- ・戸籍照会 ID
- ・デジタル証・署名データ作成状態区分
- ・デジタル証署名データ
- ・デジタル証署名素データ
- ・申請者氏名（姓）
- ・申請者氏名（名）

- ・申請者氏名フリガナ（姓）
- ・申請者氏名フリガナ（名）
- ・郵便番号
- ・住所地
- ・送付先希望
- ・送付先郵便番号
- ・免許証交付回数
- ・新免許交付局C
- ・新免許交付年月日
- ・免許再交付理由C
- ・免許書替理由C
- ・免許有無0 1 F
- ・免許有無0 2 F
- ・免許有無0 3 F
- ・免許有無0 4 F
- ・免許有無0 5 F
- ・免許有無0 6 F
- ・免許有無0 7 F
- ・免許有無0 8 F
- ・免許有無0 9 F
- ・免許有無1 0 F
- ・免許有無1 1 F
- ・免許有無1 2 F
- ・免許有無1 3 F
- ・免許有無1 4 F
- ・免許有無1 5 F
- ・免許有無1 6 F
- ・免許有無1 7 F
- ・免許有無1 8 F
- ・免許有無1 9 F
- ・免許有無2 0 F
- ・免許有無2 1 F
- ・免許有無2 2 F
- ・免許有無2 3 F
- ・免許有無2 4 F
- ・氏名カナ

- ・性別 F
- ・個人本籍 C
- ・登記年月日
- ・免許有無 2 5 F
- ・国籍
- ・備考
- ・登録日時
- ・旧姓・通称
- ・参考事項
- ・都道府県
- ・免許年月日 1
- ・免許年月日 2
- ・免許年月日 3
- ・免許年月日 4
- ・免許年月日 5
- ・免許年月日 6
- ・免許年月日 7
- ・免許年月日 8
- ・免許年月日 9
- ・免許年月日 10
- ・免許年月日 11
- ・免許年月日 12
- ・免許年月日 13
- ・免許年月日 14
- ・免許年月日 15
- ・免許年月日 16
- ・免許年月日 17
- ・免許年月日 18
- ・免許年月日 19
- ・免許年月日 20
- ・免許年月日 21
- ・免許年月日 22
- ・免許年月日 23
- ・免許年月日 24
- ・有効期限 1
- ・有効期限 2

- ・有効期限 3
- ・有効期限 4
- ・有効期限 5
- ・有効期限 6
- ・有効期限 7
- ・有効期限 8
- ・有効期限 9
- ・有効期限 10
- ・有効期限 11
- ・有効期限 12
- ・有効期限 13
- ・有効期限 14
- ・有効期限 15
- ・有効期限 16
- ・有効期限 17
- ・有効期限 18
- ・有効期限 19
- ・有効期限 20
- ・有効期限 21
- ・有効期限 22
- ・有効期限 23
- ・有効期限 24
- ・性別
- ・本籍
- ・交付局
- ・再交付理由
- ・書替理由
- ・免許の種類 1
- ・免許の種類 2
- ・免許の種類 3
- ・免許の種類 4
- ・免許の種類 5
- ・免許の種類 6
- ・免許の種類 7
- ・免許の種類 8
- ・免許の種類 9

- ・免許の種類 1 0
- ・免許の種類 1 1
- ・免許の種類 1 2
- ・免許の種類 1 3
- ・免許の種類 1 4
- ・免許の種類 1 5
- ・免許の種類 1 6
- ・免許の種類 1 7
- ・免許の種類 1 8
- ・免許の種類 1 9
- ・免許の種類 2 0
- ・免許の種類 2 1
- ・免許の種類 2 2
- ・免許の種類 2 3
- ・免許の種類 2 4
- ・免許の種類 2 5
- ・免許有無 0 1
- ・免許有無 0 2
- ・免許有無 0 3
- ・免許有無 0 4
- ・免許有無 0 5
- ・免許有無 0 6
- ・免許有無 0 7
- ・免許有無 0 8
- ・免許有無 0 9
- ・免許有無 1 0
- ・免許有無 1 1
- ・免許有無 1 2
- ・免許有無 1 3
- ・免許有無 1 4
- ・免許有無 1 5
- ・免許有無 1 6
- ・免許有無 1 7
- ・免許有無 1 8
- ・免許有無 1 9
- ・免許有無 2 0

- ・免許有無 2 1
- ・免許有無 2 2
- ・免許有無 2 3
- ・免許有無 2 4
- ・免許有無 2 5
- ・免許証番号
- ・免許証情報
- ・注釈
- ・交付者の役職
- ・作成日時
- ・作成ユーザ
- ・更新日時
- ・更新ユーザ
- ・削除フラグ
- ・登録番号
- ・最終更新日時
- ・資格 ID
- ・事務 ID
- ・資格取扱単位コード
- ・資格仮名
- ・個人番号
- ・初期設定\_申請 ID
- ・初期設定\_資格仮名
- ・作成日時
- ・作成ユーザ
- ・更新日時
- ・更新ユーザ
- ・削除フラグ
- ・申請 ID
- ・最終更新日時
- ・個人番号
- ・個人番号更新フラグ
- ・申請区分コード
- ・申請区分名
- ・資格 ID
- ・資格名（漢字）

- ・事務 ID
- ・事務名
- ・資格取扱単位コード
- ・資格取扱単位名
- ・受付年月日
- ・業務種別コード
- ・業務種別名
- ・資格手続コード
- ・手続名
- ・登録番号
- ・審査ステータス
- ・審査者氏名
- ・審査実施日時
- ・審査結果（重複）
- ・審査メモ（重複）
- ・審査結果（本人確認）
- ・審査メモ（本人確認）
- ・審査結果（戸籍確認）
- ・審査メモ（戸籍確認）
- ・審査結果（申請書確認）
- ・審査メモ（申請書確認）
- ・審査結果（添付確認）
- ・審査メモ（添付確認）
- ・審査結果（決済確認）
- ・審査メモ（決済確認）
- ・審査結果（欠格事由審査）
- ・審査メモ（欠格事由審査）
- ・審査不備理由
- ・審査連絡メモ
- ・資格仮名
- ・システム登録日時
- ・システム更新日時
- ・再申請申請 ID
- ・職権修正備考
- ・作成日時
- ・作成ユーザ

- ・更新日時
- ・更新ユーザ
- ・削除フラグ
- ・個人番号
- ・申請区分コード
- ・申請区分名
- ・資格 ID
- ・資格名（漢字）
- ・事務 ID
- ・事務名
- ・資格取扱単位コード
- ・資格取扱単位名
- ・申請 ID
- ・受付年月日
- ・業務種別コード
- ・業務種別名
- ・資格手続コード
- ・手続名
- ・登録番号
- ・都道府県コード
- ・都道府県名（漢字）
- ・郵送元受付機関コード
- ・郵送元受付機関名
- ・受付機関コード
- ・受付機関名
- ・申請者氏名（漢字）
- ・申請者氏名（かな／カナ）
- ・申請者住所
- ・申請者生年月日
- ・申請者性別コード
- ・申請者電話番号
- ・申請者メールアドレス
- ・マイナンバーカード住所
- ・マイナンバーカード氏名
- ・マイナンバーカード生年月日
- ・マイナンバーカード性別コード

- ・マイナンバーカード情報取得日時
- ・旧姓併記希望
- ・旧姓
- ・外字表記希望
- ・機構保存本人確認情報等照会結果
- ・機構保存本人確認情報等照会日時
- ・戸籍関係情報照会結果
- ・戸籍関係情報照会日時
- ・申請ステータス
- ・資格仮名
- ・システム登録日時
- ・システム更新日時
- ・再申請要否
- ・再申請申請 ID
- ・合格者番号
- ・合格年月日
- ・一部合格番号
- ・一部合格年月日
- ・一部免除番号
- ・一部免除合格年月日
- ・試験免除番号
- ・免除年月日
- ・本籍地コード
- ・本籍地（和名）
- ・送付先住所
- ・備考
- ・受験年月日
- ・受験回
- ・受験地
- ・戸籍照会 ID
- ・申請の区分
- ・新規に申請する免許の種類
- ・宛先局名
- ・申請年月日
- ・申請者氏名（姓）
- ・申請者氏名（名）

- ・申請者氏名フリガナ（姓）
- ・申請者氏名フリガナ（名）
- ・生年月日
- ・住所
- ・住所フリガナ
- ・郵便番号
- ・電話番号
- ・申請者メールアドレス
- ・旧姓を使用した氏名又は通称の併記の希望の有無
- ・併記を希望する氏名又は通称
- ・住所地
- ・送付先希望
- ・連絡先
- ・住所
- ・郵便番号
- ・電話番号
- ・住所
- ・住所フリガナ
- ・郵便番号
- ・電話番号
- ・試験を受けた地域の番号
- ・試験年月日
- ・受験番号
- ・資格内容
- ・資格取得年月日
- ・再交付の理由
- ・変更前の氏名
- ・変更前の氏名フリガナ
- ・申請免許有効期限年月日
- ・新様式免許証番号
- ・免許の種類
- ・交付局
- ・免許証の番号
- ・交付年月日
- ・他の旧様式免許証の有無
- ・他の旧様式免許証の種類

- ・免許の種類
- ・交付局
- ・免許証の番号
- ・交付年月日
- ・既に受けている免許の種類
- ・免許に付されている条件
- ・取消しを申請する免許の種類
- ・備考
- ・データ受付番号
- ・申請区分
- ・保留番号
- ・申請 ID
- ・個人番号
- ・作成日時
- ・作成ユーザ
- ・更新日時

- ・更新ユーザ
- ・削除フラグ
- ・データ受付番号
- ・個人番号
- ・照会対象年月日
- ・住基氏名漢字
- ・住基氏名カナ
- ・住基性別
- ・住基生年月日
- ・住基市町村コード
- ・住基住所
- ・住基生存状況
- ・住基異動事由
- ・住基異動年月日
- ・作成日時
- ・作成ユーザ
- ・更新日時
- ・更新ユーザ
- ・削除フラグ
- ・データ受付番号
- ・個人番号
- ・突合状況確認結果
- ・確認結果備考 1
- ・確認結果備考 2
- ・確認結果備考 3
- ・確認結果備考 4
- ・確認結果備考 5
- ・確認結果備考 6
- ・基準管轄局
- ・基準住居地
- ・基準氏名漢字
- ・基準氏名カナ
- ・基準性別
- ・基準生年月日
- ・基準住所
- ・作成日時

- ・作成ユーザ
- ・更新日時
- ・更新ユーザ
- ・削除フラグ
- ・登録番号
- ・更新回数
- ・個人番号
- ・免許番号
- ・データ受付番号
- ・紐づけステータス
- ・資格仮名
- ・作成日時
- ・作成ユーザ
- ・更新日時
- ・更新ユーザ
- ・削除フラグ
- ・データ受付番号
- ・個人番号
- ・免許番号
- ・保留番号
- ・申請 ID
- ・免許種別
- ・局
- ・機能 ID
- ・アクセス日時
- ・端末 ID
- ・ユーザ ID
- ・ユーザ名
- ・作成日時
- ・作成ユーザ
- ・更新日時
- ・更新ユーザ
- ・削除フラグ
- ・実行 ID
- ・実行ステータス
- ・国家資格エラーコード

- ・条件更新日時 from
- ・条件更新日時 to
- ・条件取得開始行番号
- ・作成日時
- ・作成ユーザ
- ・更新日時
- ・更新ユーザ
- ・削除フラグ
- ・実行 ID
- ・申請 ID
- ・実行ステータス
- ・国家資格エラーコード
- ・作成日時
- ・作成ユーザ
- ・更新日時
- ・更新ユーザ
- ・削除フラグ
- ・申請 ID
- ・ファイル区分
- ・ファイル作成日時
- ・業務種別コード
- ・ファイルパス
- ・ファイル作成ステータス
- ・作成日時
- ・作成ユーザ
- ・更新日時
- ・更新ユーザ
- ・削除フラグ
- ・申請 ID
- ・連携日時
- ・ファイル連携結果ステータス
- ・作成日時
- ・作成ユーザ
- ・更新日時
- ・更新ユーザ
- ・削除フラグ

- ・ファイル ID
- ・レコード ID
- ・データ区分
- ・申請 ID
- ・登録番号
- ・作成日時
- ・作成ユーザ
- ・更新日時
- ・更新ユーザ
- ・削除フラグ
- ・ファイル ID
- ・レコード ID
- ・リトライファイル ID
- ・リトライレコード ID
- ・作成日時
- ・作成ユーザ
- ・更新日時
- ・更新ユーザ
- ・削除フラグ
- ・ファイル ID
- ・レコード ID
- ・データ連携結果ステータス
- ・個別結果コード
- ・個別結果メッセージ
- ・作成日時
- ・作成ユーザ
- ・更新日時
- ・更新ユーザ
- ・削除フラグ
- ・ファイル ID
- ・ファイル区分
- ・ファイルパス
- ・ファイル作成日時
- ・ファイル作成ステータス
- ・作成日時
- ・作成ユーザ

- ・更新日時
- ・更新ユーザ
- ・削除フラグ
- ・ファイル ID
- ・ファイル区分
- ・ファイル連携日時
- ・ファイル連携結果ステータス
- ・国家資格エラーコード
- ・作成日時
- ・作成ユーザ
- ・更新日時
- ・更新ユーザ
- ・削除フラグ

(別添)過去3年以内に発生した個人情報に関する重大事故

該当年度	内容	関係個人情報数	再発防止策
令和4年度	清掃業者が誤って搬出の上、焼却処分してしまった。(地方支分部局)	477	<ul style="list-style-type: none"> <li>幹部職員に対して、本件個人情報誤廃棄事案の概要及び発生原因について説明を行い、文書保存状態の点検及び個人情報誤廃棄防止対策の研修を行った。</li> <li>全職員に対して、幹部職員を通じて以下の指示・徹底を行った。           <ul style="list-style-type: none"> <li>所内の文書管理について、個人で判断することではなく、必ず上司に報告、確認を仰ぐ事を徹底すること</li> <li>行政文書の保管について、作業開始時、終了時には必ず職員による点検を実施すること</li> <li>万一仮置きしている文書を発見した場合には、発見者は速やかに文書管理者に報告・連絡すること</li> <li>定められた場所以外に行政文書が入った箱等を置かないように貼り紙を貼り、職員が明確に認識できることとした。</li> </ul> </li> </ul>
令和4年度	溶解処分のために廃棄業者に引き渡しを行ったはずの個人情報を含む文書が近隣の公園で発見された。(地方支分部局)	371	<ul style="list-style-type: none"> <li>文書廃棄作業を行う場合には、当該作業者以外の者が立入りできない場所(施錠可能な場所)にて複数の職員で行い、第三者が廃棄文書に接触することのないようにする。また、作業者はできる限り作業場所から離れることなく作業を行うこととし、離れる場合は施錠する。</li> <li>文書廃棄作業は廃棄予定リストと(行政文書ファイルの)現物を照合しながら行うが、その際には当該文書の内容等を把握している職員を含めた体制で実施する。</li> <li>これまで文書廃棄作業時においては、廃棄予定リストと(行政文書ファイルの)現物を照合した段階で、廃棄予定リストにチェックを入れていたが、今後は、廃棄文書を段ボールに箱詰めした段階でチェックを入れることとする。</li> <li>溶解処理する文書を廃棄する際、箱詰めして封緘した箱に「溶解」のシールを貼付するが、同時に箱に数字(連番)を記載し保管場所に搬入する。また、契約業者に引き渡す際には、廃棄文書の入った箱の全てが間違なく回収されたことを確認し、それを記録する。</li> <li>原則として、廃棄する文書の入った箱は業者による回収日前日から指定保管場所に移動し、回収するまでの保管場所の鍵の管理は総務課で行うこととする。</li> <li>廃棄業者による廃棄文書の回収作業時の職員立会については、保管場所とトラックへの移動経路、トラックへの積込み場所等において、常時、廃棄業者の作業内容を確認する。</li> </ul>
令和4年度	保有個人情報の開示決定を行うに当たり、請求人の所属する事業所に意見照会の書類を送付すべきところ、別の事業所に誤送付した。(地方支分部局)	142	<ul style="list-style-type: none"> <li>全職員に対し、個人情報の漏えい事案が発生したことを注意喚起し、特に、健康情報など機微な情報が含まれる情報を送付する際には、慎重な取扱いを行うよう指示した。</li> <li>全所属長に対して事案の概要説明を行うとともに、注意喚起及び再発防止の徹底を図るよう指示した。</li> <li>要配慮個人情報が含まれる文書を送付する際には、送付先への電話連絡により、文書を閲覧する権限のある者の役職・氏名を確認し、その者の役職・氏名を宛先に記載した上で、特定記録郵便で親書と記載して送付することを手順として加える。</li> <li>総務部職員が管内全部署を訪問し、個人情報を含む文書の発送時における確認作業を点検し、必要な指導を行う。</li> </ul>
令和4年度	委託事業の受託者(再委託先)が当該事業の利用者の情報が含まれたファイルをメールで誤送付した。(本省課室)	620	<ul style="list-style-type: none"> <li>本省課室より再委託会社も含め個人情報の適切な取扱いと再発防止の徹底を図るよう受託者に対して注意指導を行った。その際、受託者が策定した再発防止策に加え、以下の点についても追加で検討するよう指示し、受託者において対応することとしている。           <ul style="list-style-type: none"> <li>個人情報が含まれるフォルダ及びファイルについて、自社事業で使用するものと厚生労働省事業で使用するものが混在しないよう管理を徹底する。</li> <li>保存の必要ない個人情報が含むファイルを削除するとともに、他のファイルについても保存期間に応じ適切に管理する。</li> <li>業務で頻繁に使うファイルについては、個人情報の含まれていない雛形を様式集として集め所定フォルダに格納し、事業担当者が不必要にファイルの使い回しをしないようにする。</li> </ul> </li> </ul>
令和4年度	研究利用のため審査の結果承認された際は個人情報を除いて提供することとしていた情報について、個人情報が除かれていなかった。(施設等機関)	5640	<ul style="list-style-type: none"> <li>個人情報を含むシートの削除等の自動化ツールの導入。</li> <li>「削除したかの確認」を手順に組み込むこと、所属長が個人情報が含まれていないこと等を確認し書面で記録を残し、それらの記録について定期的に確認すること。</li> <li>個人情報の取扱に関する研修の徹底。</li> <li>提供前に、本省課室でも確認すること。</li> </ul>
令和4年度	医療従事者が勤務場所等の届出を行うシステムにおいて、自機関の登録状況を確認するためにCSV出力した場合に他機関に勤務する者の情報も表示可能な状況になっていた。(本省課室)	396	<ul style="list-style-type: none"> <li>受託者において構築したプログラムについて、受託者と厚生労働省職員のみならず、第三者(受託者以外の事業者)においても確認を実施した。</li> <li>確認する際に、プログラム開発者が想定するような操作だけでなく、システム利用者目線で操作を行い、テストケースを増やした。</li> </ul>
令和4年度	溶解処分のために廃棄業者に引き渡しを行ったはずの個人情報を含む文書が近隣の公園で発見された。(地方支分部局)	503	<ul style="list-style-type: none"> <li>文書ファイルの保管場所等を監視できる防犯カメラの設置を行うこととした。</li> <li>全部署に対して、個人情報を含む行政文書ファイルについては、施錠できる場所に保管することを徹底するよう改めて周知した。</li> <li>文書ファイルの有無についての確認を総務課より全部署に指示し、確認ができない文書がなかったことを確認した。</li> <li>全部署に対して、行政文書ファイルを保管している倉庫等の入退室に使用する鍵の使用簿を設置し、状況を把握するよう指示した。</li> <li>会議を開催して、廃棄処理における情報漏えい防止対策の徹底と、改めて行政文書管理に万全を期するよう指示した。</li> </ul>
令和4年度	個人情報を含む報告書等の継りの所在が不明となっていることが確認された。(地方支分部局)	285	<ul style="list-style-type: none"> <li>全職員に対し、事実経過の概要を説明するとともに、文書廃棄作業時には廃棄対象リストと廃棄文書の背表紙の照合確認を複数人で2回(廃棄文書を段ボールに箱詰める際と段ボールに封をする際)以上確実に行うこととし、行政文書の適正な管理を徹底するよう指示した。</li> <li>緊急会議を開催し、適正な文書管理と個人情報漏えい防止対策の徹底を指示した。</li> <li>今年度廃棄予定の文書と廃棄対象文書リストとの照合確認を、現在の突合作業の進捗にかかるらず、再度、全件行うよう指示した。</li> </ul>

(別添)過去3年以内に発生した個人情報に関する重大事故

該当年度	内容	関係個人情報数	再発防止策
令和4年度	個人情報を含む文書を廃棄手続き完了前に誤廃棄していることが確認された。(地方支分部局)	880	<ul style="list-style-type: none"> <li>●全職員(非常勤職員を含む。)に対し、事実経過の概要を説明するとともに、文書廃棄作業時には廃棄対象リストと廃棄文書の背表紙の照合確認を複数人で2回(廃棄文書を段ボールに箱詰めする際と段ボールに封をする際)以上確実に行うこととし、所内の行政文書の適正な管理を徹底するよう指示した。</li> <li>●メールで本事案を全所属に報告し、情報共有及び再発防止徹底を指示するとともに、文書管理者を含めた管理者が封緘前に最終の照合確認を行い、封緘するよう指示した。</li> <li>●全職員が適正な文書管理への理解を深めるよう研修を行い、行政文書の適正な取扱いを徹底するよう指示した。</li> <li>●会議において、文書管理の留意点を伝えるとともに、行政文書の適正な取扱いを徹底するよう指示した。</li> </ul>
令和5年度	個人情報を含む内容を登録することとしていたシステムについて、標準文書保存期間基準よりも早くシステムから自動削除される仕組みとしていた。(本省課室)	約11000000	<ul style="list-style-type: none"> <li>●本省課室及び関係施設等機関において文書管理に係るe-ラーニングを再度受講し、新規に行政文書を取得する場合は、保存期間表に照らし適切な保存期間が設定されているか確認することを徹底。</li> </ul>
令和5年度	個人情報をマスキングしてHPに公表していた文書について、マスキングが外せる状態だった。(本省課室)	696	<ul style="list-style-type: none"> <li>●関係文書の情報公開に係るガイドラインを作成し、統一的な対応を行えるようにする。</li> <li>●マスキングを行うだけではなく、マスキングの対象となるデータ自体も消去した上で、本省課室に提出するよう依頼。更に、データの消去が行われているかについてチェックリストを用いた確認を経てから掲載することとする。</li> </ul>
令和5年度	個人情報が記載されているデータの送信先を誤って送信。(地方支分部局)	208	<ul style="list-style-type: none"> <li>●部内各課長に対して発生事案の概要説明を行うとともに、部内全職員に対して、以下の事項について指示を行った。           <ul style="list-style-type: none"> <li>●個人情報保護に関する緊急自主点検を速やかに実施すること。</li> <li>●申請書類の様式については、原則として、今後メールで送信せず、労働局HP上からダウンロードする形に変更する。</li> <li>●個人情報を含む・含まないに関わらず、PCのデスクトップ上に行政文書及び個人文書のファイルを保存することを禁止し、定められた場所への保存を徹底する。</li> <li>●外部から個人情報を含むファイルを受け取った場合は、速やかにファイル名を変更の上、パスワードの設定を徹底する。</li> <li>●外部機関等へ個人情報を含むファイルを送信する際は、パスワードを設定する等ファイルの暗号化を徹底する。なお、送信前に必ず宛先と添付ファイルの内容に誤りがないか上司による確認を受ける。</li> <li>●保有個人情報の適正な管理の遵守について、幹部職員が所属職員に対して基本動作の徹底等の意識啓発を図り、再発防止を徹底する。</li> </ul> </li> </ul>