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
4	給水装置工事主任技術者免状の交付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

国家資格である給水装置工事主任技術者の免状の交付に関する事務における特定個人情報ファイルの取扱いに当たり、同ファイルの取扱いが個人のプライバシー等の権利利益に影響を及ぼすものであることを認識し、特定個人情報の漏洩その他の事態を発生させるリスクを軽減させるために適切な措置を講じることをもって、個人のプライバシー等の権利利益の保護に取り組んでいることを宣言する。

特記事項	

評価実施機関名

国土交通大臣

個人情報保護委員会　承認日 【行政機関等のみ】

令和7年7月31日

公表日

令和7年8月1日

［令和7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	給水装置工事主任技術者免状の交付に関する事務
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（マイナポータル電子申請については特定個人情報ファイルの取扱有、e-Gov電子申請及び紙申請については特定個人情報ファイルの取扱無） i.資格情報の登録 　オンライン（マイナポータル及びe-Gov）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（マイナポータル）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）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）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。 ■免状事務（特定個人情報ファイルの取扱無） i.デジタル資格情報表示（オンライン） 　資格保有者が自身の保有する資格情報を第三者へ対面で自身のスマホやタブレット上に表示する。 ii.免状の交付・書換え・再交付（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、免状の作成処理を行う。書換え・再交付については、オンライン（マイナポータル及びe-Gov）又は紙での申請を受けて、審査を行う。審査の結果、問題が無ければ免状の作成処理を行う。 ※オンライン（e-Gov）は、登録の際には戸籍妙本又は住民票の抄本を利用し、資格保有者本人であることを確認するものであり、マイナンバーカードを保有しない資格保有者においても電子申請を行うことを可能とするもの。
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	【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）】 ■「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.国土交通省が資格登録者名簿等をクラウド上において保存・管理すること等を可能とする。 ii.国土交通省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（マイナポータル）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、国土交通省にオンラインで申請・提出を行うことを可能とする。 iii.国土交通省はオンラインで申請等を行った資格登録申請者等の本人確認やオンライン申請の受付、申請データの受領等を可能とする。 iv.オンライン申請の際に作成される個人番号を含む資格情報については国家資格等情報連携・活用システムへ連携された後にマイナポータルからは削除される。（国家資格等情報連携・活用システムでログデータを一定期間保存した後に削除。） ■「オンライン決済関連機能」（特定個人情報ファイルの取扱無） i.資格登録のオンライン手続の際に、手数料等の支払いのオンライン化等を可能とする。 ■「資格情報提供関連機能」（特定個人情報ファイルの取扱無） i.資格保有者がオンラインでマイナンバーカードによる本人認証・同意を行い、自己情報としての資格に関する情報を電子的な形式で表示を可能とする。 ii.国土交通省において、資格保有者がオンラインでマイナンバーカードによる本人認証・同意を行った際に電子的な形式で資格証と同等の情報を資格保有者等へ提供を可能とする。 iii.資格保有者等がオンラインでマイナンバーカードによる本人認証・同意等を行い、自己情報としての資格に関する情報を電子的な形式で第三者に提供することを可能とする。 iv.国土交通省において、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。 ■「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.国土交通省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 符号管理機能では、情報照会、情報提供に用いる個人の識別子である「符号」を保管・管理する。 ii. 情報照会機能 情報照会機能では、情報提供ネットワークシステムを介して、特定個人情報（連携対象）の情報照会及び情報の受領を行う。 iv. 情報提供等記録管理機能 特定個人情報（連携対象）の照会、又は提供があった旨の情報提供等記録を管理する。 v. データ送受信機能 中間サーバー機能と情報提供ネットワークシステム（インターフェイスシステム）との間で情報照会、符号取得のための情報等について連携する。 vi. セキュリティ管理機能 vii. 職員認証・権限管理機能 中間サーバー機能を利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報（連携対象）へのアクセス制御を行う。 viii. システム管理機能 バッチ処理の状況管理、業務統計情報の集計、稼働状態の通知、保管切れ情報の削除を行う。 ■「オンライン通知機能」（特定個人情報ファイルの取扱無） i.資格登録申請者等は申請結果等の通知をオンラインで受取ることを可能とする。 ii.国土交通省は、手続結果や各種お知らせ等をオンラインで送付することを可能とする。
③他のシステムとの接続	[○] 情報提供ネットワークシステム　　[　　] 庁内連携システム [○] 住民基本台帳ネットワークシステム　　[　　] 既存住民基本台帳システム

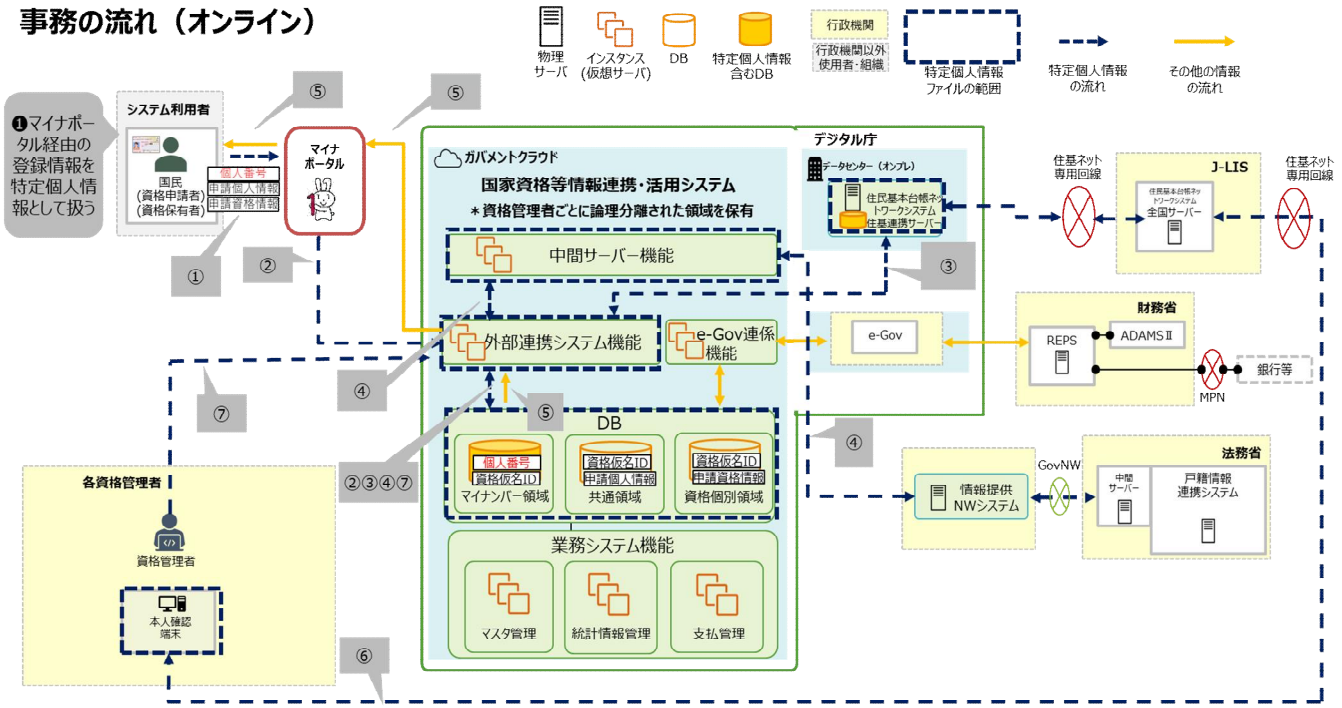
⑨他のシステムとの接続	[　] 宛名システム等　　[　] 税務システム [○] その他　（ e-Gov、マイナポータル　　）

システム2～5	
システム2	
①システムの名称	住民基本台帳ネットワークシステム
②システムの機能	【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. 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もしくは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	【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)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、国土交通省に申請・提出を行うことを可能とする。 ・国土交通省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表示等を可能とする。 ・国土交通省において、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。 ・国土交通省において、資格保有者等がマイナンバーカードによる本人認証・同意等を行った際に電子的な形式で資格証と同等の情報を第三者へ提供することを可能とする。 (3)オンライン通知機能（特定個人情報ファイルの取扱無） ・申請者は申請結果等の通知をオンラインで受取ることを可能とする。 ・国土交通省は、手続結果や各種お知らせ等をオンラインで送付することを可能とする。
③他のシステムとの接続	[　] 情報提供ネットワークシステム　　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　　[　] 既存住民基本台帳システム [　] 宛名システム等　　[　] 税務システム [○] その他　（ 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	
システム5	
①システムの名称	
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	
給水装置工事主任技術者ファイル	
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	【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）】 ・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	【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、国土交通省にとっては登録原簿の正確性を保つことが可能となる。
5. 個人番号の利用　※	
法令上の根拠	・番号法第9条第1項（利用範囲） 別表　項番39の3 ・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101の2
6. 情報提供ネットワークシステムによる情報連携 ※	
①実施の有無	[　　実施する　　] ＜選択肢＞ 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	番号法第19条第8号（特定個人情報の提供の制限）に基づく主務省令第2条の表　項番62
7. 評価実施機関における担当部署	
①部署	国土交通省水管理・国土保全局水道事業課
②所属長の役職名	水道事業課長
8. 他の評価実施機関	
なし	

（別添1）事務の内容


事務の流れ（オンライン）
物理サーバ
インスタンス（仮想サーバ）
DB
特定個人情報含むDB
行政機関
行政機関以外使用者：組織
特定個人情報ファイルの範囲
特定個人情報の流れ
その他の情報の流れ
❶マイナポータル経由の登録情報を特定個人情報として扱う
システム利用者
国民（資格申請者）（資格保有者）
個人番号
申請個人情報
申請資格情報
マイナポータル
ガバメントクラウド
国家資格等情報連携・活用システム
＊資格管理者ごとに論理分離された領域を保有
中間サーバー機能
外部連携システム機能
e-Gov連係機能
DB
個人番号
資格仮名ID
マイナンバー領域
資格仮名ID
申請個人情報
共通領域
資格仮名ID
申請資格情報
資格個別領域
業務システム機能
マスタ管理
統計情報管理
支払管理
デジタル庁
データセンター（オンプレ）
住民基本台帳ネットワークシステム
住基連携サーバー
e-Gov
住基ネット専用回線
J-LIS
全国サーバー
住基ネット専用回線
財務省
REPS
ADAMSⅡ
MPN
銀行等
GovNW
情報提供NWシステム
法務省
中間サーバー
戸籍情報連携システム
各資格管理者
資格管理者
本人確認端末
①
②
③
④
⑤
⑥
⑦
②③④⑦

（備考）

【事務の流れ】
〇資格管理事務(マイナポータル電子申請については個人番号利用有、e-Gov電子申請及び紙申請については個人番号利用無)
・資格情報の登録
オンライン(マイナポータル)若しくはe-Gov電子申請及び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)若しくはe-Gov電子申請及び紙での申請のほか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一年に一回照会を行う。審査の結果、問題が無ければ結果情報を登録する。
・資格の削除
オンライン(マイナポータル)若しくはe-Gov電子申請及び紙での申請のほか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一年に一回照会を行う。審査の結果、資格の削除が決定した場合、登録者名簿からの削除を行う。
〇決済事務(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、オンラインで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従来通りの収入印紙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、更新)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。
〇交付事務(個人番号利用無し)
・デジタルでの資格情報表示
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、タブレット上に表示する。
・免状の交付・書換え・再交付
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、免状の作成処理を行う。書換え・再交付については、オンライン(マイナポータル)若しくはe-Gov電子申請及び紙での申請を受けて、審査を行う。審査の結果、問題が無ければ免状の作成処理を行う。

【特定個人情報の流れ】
〇マイナポータル電子申請の場合
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照会を行い、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、一年に一回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から取得することができる。
⑥国土交通省は資格登録情報について、本人確認端末(国家資格等情報連携・活用システム専用端末)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。

注1)外部連携システム機能を介し、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情報と一度紐づけした後に、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、個人番号と紐づ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		
給水装置工事主任技術者ファイル		
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 ※		給水装置工事主任技術者免状の登録者
	その必要性	【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情報の表示を行うため。
④記録される項目		[　10項目以上50項目未満　] ＜選択肢＞ 1）10項目未満　2）10項目以上50項目未満 3）50項目以上100項目未満　4）100項目以上
	主な記録項目 ※	・識別情報 [○] 個人番号　[　] 個人番号対応符号　[　] その他識別情報（内部番号） ・連絡先等情報 [○] 5情報（氏名、氏名の振り仮名、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	【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）】 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		令和8年2月1日
⑥事務担当部署		国土交通省水管理・国土保全局水道事業課

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		【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		【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 別表の39の3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 ※		【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 ※	国土交通省水管理・国土保全局水道事業課
	使用者数	[10人未満] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
⑧使用方法 ※		【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）】 ・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 ※	【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）】 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 ※	【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）】 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 ※	【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）】 該当なし
⑨使用開始日		令和8年2月1日

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※		[委託する] <選択肢> 1）委託する 2）委託しない （ 1 ） 件
委託事項1		【国家資格等情報連携・活用システムに係る部分（共通して記載）】 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 ※	給水装置工事主任技術者資格登録者
	その妥当性	【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）】 システム全体に係る運用保守を適切に実施するためには、専門的かつ高度な知識・技術を要することから全体の取扱を委託することが必要であるため。
③委託先における取扱者数		[50人以上100人未満] <選択肢> 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[ ]専用線 [ ]電子メール [○]電子記録媒体（フラッシュメモリを除く。） [ ]フラッシュメモリ [ ]紙 [○]その他 （ システム直接操作 ）
⑤委託先名の確認方法		【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		【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）】 株式会社 NTTデータ
再委託	⑦再委託の有無 ※	[再委託する] <選択肢> 1）再委託する 2）再委託しない
	⑧再委託の許諾方法	【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	【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）】 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6～10		
委託事項11～15		
委託事項16～20		

5. 特定個人情報の提供・移転（委託に伴うものを除く。）	
提供・移転の有無	[　] 提供を行っている　（　　）件　[　] 移転を行っている　（　　）件 [○] 行っていない
提供先1	
①法令上の根拠	
②提供先における用途	
③提供する情報	
④提供する情報の対象となる本人の数	[　　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤提供する情報の対象となる本人の範囲	
⑥提供方法	[　] 情報提供ネットワークシステム　[　] 専用線 [　] 電子メール　[　] 電子記録媒体（フラッシュメモリを除く。） [　] フラッシュメモリ　[　] 紙 [　] その他　（　　）
⑦時期・頻度	
提供先2～5	
提供先6～10	
提供先11～15	
提供先16～20	
移転先1	
①法令上の根拠	
②移転先における用途	
③移転する情報	
④移転する情報の対象となる本人の数	[　　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤移転する情報の対象となる本人の範囲	
⑥移転方法	[　] 庁内連携システム　[　] 専用線 [　] 電子メール　[　] 電子記録媒体（フラッシュメモリを除く。） [　] フラッシュメモリ　[　] 紙 [　] その他　（　　）
⑦時期・頻度	
移転先2～5	
移転先6～10	
移転先11～15	
移転先16～20	

6. 特定個人情報の保管・消去

①保管場所 ※		【国家資格等情報連携・活用システムに係る部分（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。
②保管期間	期間	[定められていない] ＜選択肢＞ 1）1年未満　2）1年　3）2年 4）3年　5）4年　6）5年 7）6年以上10年未満　8）10年以上20年未満　9）20年以上 10）定められていない
	その妥当性	【国家資格等情報連携・活用システムに係る部分（共通して記載）】 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）】 ・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。

7. 備考

（別添2）特定個人情報ファイル記録項目

（給水装置工事主任技術者ファイル）
1 資格仮名ID
2 マイナポータル仮名ID
3 資格情報
4 本籍情報
5 合格者番号
6 免状番号
7 漢字氏名
8 カナ氏名
9 郵便番号
10 電話番号
11 住所
12 生年月日
13 免状交付日
14 再交付日
15 再交付回数
16 返納理由
17 警告
18 備考

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	
給水装置工事主任技術者ファイル	
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	【マイナポータル電子申請からの入手】 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。 【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。 ・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。 ・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いないことの確認を行うため、対象者以外の情報を入手することはない。
必要な情報以外を入手することを防止するための措置の内容	【マイナポータル電子申請からの入手】 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。 【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	免状交付事務において個人番号を要することはないため、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。）の制限を行う。
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	【マイナポータル電子申請からの入手】 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。 【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 マイナポータル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	【マイナポータル電子申請からの入手】 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。 【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	【マイナポータル電子申請からの入手】 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。 【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	【マイナポータル電子申請からの入手】 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。 【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	【マイナポータル電子申請からの入手】 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、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。 ①国家資格等情報連携・活用システムから入手する場合 地方公共団体情報システム機構との接続においては通信の暗号化等の高度なセキュリティを維持した専用回線を利用することで機密性を確保している。 ②本人確認端末（専用端末）から入手する場合 本人確認情報については、専用端末において権限のある者のみ処理を行うことができる。また通信の暗号化等の高度なセキュリティを維持した専用回線を利用することで機密性を確保している。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置	

3. 特定個人情報の使用	
リスク1： 目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク	
宛名システム等における措置の内容	【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）】 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。
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、従事者が利用する端末に顔認証機能を設け、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。 ※給水装置工事主任技術者資格を扱う情報システム責任者及び情報システム管理者を指す。 【住基連携サーバー及び本人確認端末（専用端末）に係る部分】 ・システム操作や特定個人情報等へのアクセスを行う前にログイン操作を行い、操作者を認証するようシステムで制御している。 ・システムへアクセスできる者を特定し、必要最小限度の範囲でのみ特定個人情報を取り扱うことができるように利用者ごとにIDを割り当てる。 ・なりすましによる不正を防止する観点から、共用IDの利用を禁止する。
アクセス権限の発効・失効の管理		[　行っている　] ＜選択肢＞ 1）行っている　2）行っていない
	具体的な管理方法	【国家資格等情報連携・活用システムに係る部分（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)発効の管理 ・情報システム責任者等及び事務従事者ユーザーの役割とアクセス権限との対応表を作成する。 ・事務従事者用ユーザーアカウントは、情報システム責任者等に対してユーザ登録を事前申請した者に限定して発行される。 ・情報システム責任者等はそれぞれの従事者ごとにそれぞれの役割に応じた別々のユーザーアカウントを割り当てる。 (2)失効の管理 ・情報システム責任者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アカウントを消去する。

アクセス権限の管理		[　行っている　] ＜選択肢＞ 1）行っている　2）行っていない
	具体的な管理方法	【国家資格等情報連携・活用システムに係る部分（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アカウントの割り当て状況等を随時確認するとともに、必要に応じて、利用者ユーザーIDの登録や変更、削除等の操作を行い、アクセス権限の発効・失効等の管理を行う。 【住基連携サーバー及び本人確認端末（専用端末）に係る部分】 ・情報システム責任者等が作成するアクセス権限と事務の対応表により、実施できる事務の範囲を限定している。また、対応表は随時見直しを行う。 ・パスワードの最長有効期間を定め、定期的に更新を実施する。
特定個人情報の使用の記録		[　記録を残している　] ＜選択肢＞ 1）記録を残している　2）記録を残していない
	具体的な方法	【国家資格等情報連携・活用システムに係る部分（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。
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。
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を必要とする。 【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。 ・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。
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	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。 【国土交通省、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】 国土交通省、デジタル庁、当該システムの運用保守事業者の三者の関係を規定した「国家資格等情報連携・活用システムの利用にあたっての確認事項（規約）」に同意することにより、当該確認事項に基づき、国家資格等情報連携・活用システムに係る特定個人情報の取扱いを当該システムの運用保守事業者に委託することとする。なお、次の内容については、当該確認事項に規定されている。 ・ 特定個人情報ファイルの閲覧者・更新者の制限 ・ 特定個人情報ファイルの取扱いの記録 ・ 特定個人情報の提供ルール/消去ルール ・ 委託契約書中の特定個人情報ファイルの取扱いに関する規定 ・ 再委託先による特定個人情報ファイルの適切な取扱いの確保	
特定個人情報ファイルの閲覧者・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を確認をする。	
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を確認をする。	
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。	

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	・国家資格管理事務に係る資格情報等は、資格情報等の抹消申請、行政処分又は登録者の死亡を契機とし、システムの名簿情報から抹消される。なお、データの物理削除は行わず当該抹消情報を記録した上で管理する。 ・システムから消去を行う際には、適切に消去等を行い、消去等に係る記録を作成し、管理する。 ・データの復元がなされないよう、クラウド事業者においてISO/IEC27001に準拠した廃棄プロセスを確保する。 ・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、その内容を確認する。 ・委託契約終了後の特定個人情報の消去については、ISMS（情報セキュリティマネジメントシステム）に準拠した廃棄プロセスを確保する。 ・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。
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		[　　再委託していない　　] ＜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り検査の実施を依頼する。
その他の措置の内容		
リスクへの対策は十分か		[　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		[○] 提供・移転しない
リスク1： 不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録	[ ]	<選択肢> 1）記録を残している　2）記録を残していない
具体的な方法		
特定個人情報の提供・移転に関するルール	[ ]	<選択肢> 1）定めている　2）定めていない
ルールの内容及びルール遵守の確認方法		
その他の措置の内容		
リスクへの対策は十分か	[ ]	<選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2： 不適切な方法で提供・移転が行われるリスク		
リスクに対する措置の内容		
リスクへの対策は十分か	[ ]	<選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
リスク3： 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク		
リスクに対する措置の内容		
リスクへの対策は十分か	[ ]	<選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置		

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

リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	・中間サーバー・ソフトウェアにおける措置 ①中間サーバー機能（国家資格等情報連携・活用システム）は、情報提供ネットワークシステムを使用した特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応している（※）。 ②既存システムからの接続に対し認証を行い、許可されていないシステムからのアクセスを防止する仕組みを設けている。 ③情報照会が完了又は中断した情報照会結果については、一定期間経過後に当該結果を情報照会機能において直ちに自動で削除することにより、特定個人情報が漏えい・紛失するリスクを軽減している。 ④中間サーバー機能（国家資格等情報連携・活用システム）の職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）中間サーバー機能（国家資格等情報連携・活用システム）は、情報提供ネットワークシステムを使用して特定個人情報を送信する際、送信する特定個人情報の暗号化を行っており、照会者の中間サーバー機能（国家資格等情報連携・活用システム）でしか復号できない仕組みになっている。 そのため、情報提供ネットワークシステムでは復号されないものとなっている。 ・中間サーバー･プラットフォームにおける措置 ①中間サーバー機能（国家資格等情報連携・活用システム）と情報提供ネットワークシステムとの間は、高度なセキュリティを維持したGSSネットワークを利用することにより、漏えい･紛失のリスクに対応している。 ②中間サーバー機能（国家資格等情報連携・活用システム）と団体についてはGSSネットワークや総合行政ネットワーク等の高度なセキュリティを維持した回線による接続とするとともに、通信を暗号化することで漏えい･紛失のリスクに対応している。 ③中間サーバー･プラットフォーム事業者の業務は、中間サーバー・プラットフォームの運用、監視・障害対応等であり、業務上、特定個人情報へはアクセスすることはできない。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク5： 不正な提供が行われるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク6： 不適切な方法で提供されるリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
リスク7： 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク	
リスクに対する措置の内容	
リスクへの対策は十分か	[ ] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている

情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置
＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバー機能（国家資格等情報連携・活用システム）の職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 ②情報連携においてのみ、情報提供用個人識別符号を用いることがシステム上担保されており、不正な名寄せが行われるリスクに対応している。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー機能（国家資格等情報連携・活用システム）と情報提供ネットワークシステムとの間は、高度なセキュリティを維持したGSSネットワークを利用することにより、安全性を確保している。 ②中間サーバー機能（国家資格等情報連携・活用システム）と団体についてはGSSネットワークや総合行政ネットワーク等の高度なセキュリティを維持した回線による接続とするとともに、通信を暗号化することで安全性を確保している。 ③中間サーバー・プラットフォームでは、特定個人情報を管理するデータベースを団体ごとに区分管理（アクセス制御）しており、中間サーバー・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 ④特定個人情報の管理を資格管理団体のみが行うことで、中間サーバー・プラットフォームの事業者における情報漏えい等のリスクを極小化する。

7. 特定個人情報の保管・消去		
リスク1： 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[十分に遵守している]	<選択肢> 1）特に力を入れて遵守している 2）十分に遵守している 3）十分に遵守していない 4）政府機関ではない
②安全管理体制	[十分に整備している]	<選択肢> 1）特に力を入れて整備している 2）十分に整備している 3）十分に整備していない
③安全管理規程	[十分に整備している]	<選択肢> 1）特に力を入れて整備している 2）十分に整備している 3）十分に整備していない
④安全管理体制・規程の職員への周知	[十分に周知している]	<選択肢> 1）特に力を入れて周知している 2）十分に周知している 3）十分に周知していない
⑤物理的対策	[十分に行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
具体的な対策の内容	【国家資格等情報連携・活用システムに係る部分（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。 ・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。	

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国土交通省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		[　発生なし　] <選択肢> 1）発生あり　2）発生なし
	その内容	
	再発防止策の内容	
⑩死者の個人番号		[　　保管している　　] <選択肢> 1）保管している　2）保管していない
	具体的な保管方法	死者の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。	
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。 ・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、消去等に係る記録を報告書等により提出させる。 ・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。 ・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。	
その他の措置の内容		
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置		

Ⅳ　その他のリスク対策 ※

1. 監査		
①自己点検	[　　十分に行っている　　]	＜選択肢＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
具体的なチェック方法	【国家資格等情報連携・活用システムに係る部分（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。 【その他事務に係る部分】 国土交通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情報システム責任者等が確認を行う。	
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。 【その他事務に係る部分】 国土交通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。	

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。 【その他事務に係る部分】 ・国土交通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。 ・国土交通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。	

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。

特定個人情報の漏えい等事案が発生した場合は、「特定個人情報の適正な取扱いに関するガイドライン」にて示されている以下の安全管理措置を実施する。
<特定個人情報の漏えい等事案が発生した場合の対応>
①組織内における報告及び被害の拡大防止
②事実関係の調査及び原因究明
③影響範囲の特定
④再発防止策の検討・実施
⑤影響を受ける可能性のある本人への連絡等
⑥事実関係、再発防止策等の公表
⑦個人情報保護委員会への報告

Ⅴ　開示請求、問合せ

1. 特定個人情報の開示・訂正・利用停止請求	
①請求先	〒100－8918 東京都千代田区霞が関2-1-2 中央合同庁舎第2号館14階 国土交通省総合政策局情報政策課 （https://www.mlit.go.jp/report/file000018.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。 https://www.mlit.go.jp/report/file000018.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	
③手数料等	[　　有料　　]　　＜選択肢＞ 1) 有料　　2) 無料 （手数料額、納付方法：　　）
④個人情報ファイル簿の公表	[　　行っている　　]　　＜選択肢＞ 1) 行っている　　2) 行っていない
個人情報ファイル名	給水装置工事主任技術者ファイル
公表場所	電子政府総合窓口 （https://personal-info.e-gov.go.jp/servlet/Ksearch?CLASSNAME=KJNMSTSEARCH）
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	国土交通省水管理・国土保全局水道事業課 〒100-8918 東京都千代田区霞が関2-1-3 中央合同庁舎第3号館 03-5253-8111（内線34420,34406）
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7月17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	パブリックコメント
②実施日・期間	令和7年6月10日～令和7年7月9日
③期間を短縮する特段の理由	
④主な意見の内容	意見無
⑤評価書への反映	反映無
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7月17日
②個人情報保護委員会による審査	(1) 給水装置工事主任技術者の免状の交付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) 情報漏えい等に対するリスク対策について、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、また、電子記録媒体は情報の暗号化を行うとともに、管理区域内から電子記録媒体を持ち出す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が重要である。 (5) 委託先事業者による特定個人情報ファイルの適正な取扱いに関して、クラウドサービスに係る安全管理措置も含め、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。 (6) 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

国土交通省内における漏えい事案（令和4年度～6年度、重大事案）

	事案の概要	個人情報の本人数	再発防止策
令和4年度	関係行政機関及び一般の方向けに送信するメールにおいて、本来BCCで送信するべきところ、宛先に入れて送信したことにより、受信者全員が関係行政機関及び一般の方のメールアドレスを見られる状況となった。	128人	外部へメールを送信する際、事前にチェックするべき項目を整理し、関係者間にて共有した。
	行政文書開示請求があった旅客自動車運送事業の事業計画に関する一部の文書（H28～29年度頃）について、保存期間満了前に誤って廃棄したものと思われる。	600人（最大）	・文書管理システムに登録している情報、令和2年度及び令和3年度に廃棄協議の同意を受けた文書リスト、現在書庫にある行政文書の突合を行い、近似の文書に同種の事案（行政文書の誤廃棄）は無いことを確認した。 ・該当支局において文書管理システムに登録している行政文書が、全て保管されていることを確認した。
	大容量転送システムで法令遵守講習会参加者に会議資料を添付して送信するところを、誤って参加者182者のメーリングリストを添付・送信した。	182人	課内職員に、個人情報を含む外部へのメールを送信する際は、宛先及び内容について、送信者以外の職員とのダブルチェックを徹底するよう、あらためて周知。 局内職員に、外部へのメールを送信する際の注意点など、個人情報等の適切な管理の徹底について、メールにて周知。 今年度及び次年度における局内職員への研修等の教育の場を通じて、個人情報等の適切な管理について促し、ルールの徹底を図る。
	大雪による国道の通行止めの実施・解除、集中除雪のための報道機関に送信した記者発表資料について、報道機関104名の宛先を「bcc」に入力して送信しなくてはいけないところを、「to」に入力してメールアドレスが確認できる状態で送信してしまった。	104人	今後、このような事態が生じないよう、メール送信において確認の再徹底を図るなど、個人情報の厳重かつ適正な管理を徹底し、再発防止に万全を期する。
令和5年度	令和5年12月11日に主催する公共交通シンポジウム参加申込者のメールアドレス計217件に対して、開催案内及び当日の動画配信に関する案内を令和5年12月5日付けで電子メール（以下、「メール」という。）で送付した際、参加者のメールアドレスを見えないようにBCCに設定すべきところ、宛先（To）に設定したことで参加申込者のメールアドレスが流出した。	155人	受託者に対し、個人情報保護の重要性の再確認と、個人情報漏えいの再発防止を指示した。 受託者においては、参加申込者に次にメールを送信する（令和5年12月11日）前までに、送信前における複数人によるチェックの徹底、申込者ごとに個別に送信する方法の採用等により、再発防止を図った。 事案公表後速やかに、委託している全ての事業について、個人情報が記載されたメールの送信時の適切な対応について注意喚起を行った。 個人情報の取扱いを含む委託事業については、事業者が選定要件を満たしているかどうかの事前チェックを徹底するとともに、単発の契約においてもメール送信を伴う業務委託の際には送付方法の事前確認を行い、事後的な報告を求め確実な履行が行われたことを確認することで、受託者においても業務における個人情報の取扱いに関する一層の意識向上が図られるようにする。
	上記と同じシンポジウムの同年1月17日開催分において公共交通シンポジウム参加申込者のメールアドレス計217件（※）に対して、開催案内及び当日の動画配信に関する案内を令和5年12月5日付けで電子メール（以下、「メール」という。）で送付した際、参加者のメールアドレスを見えないようにBCCに設定すべきところ、宛先（To）に設定したことで参加申込者のメールアドレスが流出した。	122人	受託者に対し、個人情報保護の重要性の再確認と、個人情報漏えいの再発防止を指示した。 事案公表後速やかに、委託している全ての事業について、個人情報が記載されたメールの送信時の適切な対応について注意喚起を行った。 個人情報の取扱いを含む委託事業については、事業者が選定要件を満たしているかどうかの事前チェックを徹底するとともに、単発の契約においてもメール送信を伴う業務委託の際には送付方法の事前確認を行い、事後的な報告を求め確実な履行が行われたことを確認することで、受託者においても業務における個人情報の取扱いに関する一層の意識向上が図られるようにする。 なお、上記に適さないケースについては、個人情報の取扱いに関する業務を委託しないこととする。
	過去に職場メールアドレスから私用メールアドレスへ送受信履歴が残っている状態でのサポート詐欺被害。	162人	12月12日に発生原因課内の職場内ミーティングにおいて、以下について徹底するよう指導した。 ・個人端末での業務作業については行わない。また、要保護情報を持ち出す場合は、必ずセキュリティ担当者からの許可を受けるよう徹底する。 ・業務に関する情報を持ち出す（送信）場合は、パスワード及び暗号化などファイルを第三者が安易に開けないようセキュリティを強化するよう徹底させる。 ・過去事案や警察庁のネット詐欺情報などを課内で共有し、日頃の個人端末使用に潜むリスク理解の深化を図り、個人端末での業務作業の禁止を徹底する。 12月15日に開発局職員全員に対して、業務における私用パソコン使用の禁止や個人情報を含むファイルのパスワード設定について周知を行った。 12月22日に本省から私有端末を業務に利用しないこと等の徹底に関する注意喚起文書が発出され、26日に職員全員に対して、同文書の周知を行った。
	河川公園の公園施設予約システムのOSリプレイス及びシステム移行作業を行う中で、テストサーバーに対して不正アクセスが確認された。	34000人	・プログラムの脆弱性を解消した新サーバーを再構築し、受託者による再診断を実施したところ、脆弱性解消が確認されたので7月5日(金)に予約システムを再開した。
	新規採用予定者に対し、開発監理部職員研修室から新規採用者研修の案内を対象者141名にメール（bcc）にて送信した際に1名分のアドレスに誤りがあり、第三者に誤って送信された。送信された資料に、令和6年1月採用者を含む新規採用者148名の配属部局、所属・役職、官職、氏名が記載された「研修員名簿」が含まれていた。	148人	（誤送信対策） 従前は新規採用予定職員から当局に対して送信してもらう連絡票に記載のメールアドレスをリスト化していたが、今後は送信してもらった差出人アドレスそのものをリスト化し、関係課所と共有することとする。 また、新規採用予定者に関するメールの誤送信が疑われる情報が寄せられた場合は関係する職員間で速やかに共有することを徹底する。 （機密情報対策） 新規採用者研修の事前送付資料から研修員名簿を分離し、研修員には当該名簿は研修初日に配布する。 上記いずれの対策も今後実施する新規採用者研修から実施することとした。 また、職員向け教育の一環として、局内イントラネットに掲載済の個人情報保護に関する資料の中で本件事案を受けた留意事項を追記し周知した。

国土交通省内における漏えい事案（令和4年度～6年度、重大事案）

	事案の概要	個人情報の本人数	再発防止策
令和6年度	自宅駐車場に駐車していた本人の自動車の窓ガラスが何者かに割られ、車内にあった鞄が盗まれた。鞄には所属の緊急連絡先（紙）が入っていた。	9人	本人に対して個人情報の管理徹底を指示。 所内会議において情報共有と注意喚起を実施。 講習会において事例紹介と注意喚起を実施。
	受注業者においてデータを管理するサーバにおいて6月30日に不正アクセス（ランサムウェア）があり、その後の外部調査の結果で令和元年度～5年度にかけて特定部局管内の事務所から受注していた業務の関係者の個人情報が含まれていた旨の報告を受けた。	109人	（委託業者による対応） ランサムウェアに感染した可能性が高いことから、ウィルスがネットワークに入った場合でも被害を拡大させない仕組みとして、専門業者による24時間365日体制で組織のセキュリティ監視を行うサービスMDR（Managed Detection and Respouse）を導入済み。 （発注者における対応） 補償コンサルタント協会を通じ、会員向けに以下の点について周知・注意喚起を実施予定（令和6年10月） 〇今回の事案について発生状況等の共有（原因など） 〇発注者からの貸与資料・データの取扱いに関する周知・徹底（業務完了後の返却、抹消など） 〇引き続きデータ管理が必要な場合は、ネットワーク接続のない外部媒体等に移動するよう注意喚起
	全国道路基盤地図等データベースで公開している道路台帳図面において、個人情報（氏名）が記載された図面が公開された	1，871人	個人情報の厳重かつ適正な管理を徹底し、附図データの公開にあたり個人の氏名を確実に削除するため、複数人での確認作業を徹底するなど体制を確保することにより、再発防止を図る。
	令和6年2月に公告した業務の閲覧資料の登録に際し、担当部局の職員が、資料閲覧業務を委託している事業者に対し、閲覧資料を登録した際に、本来個人情報等をマスキングすべきところ未処理のファイルを送付したため、個人情報の漏えいが生じた。	150人	担当部局においては、ただちに担当部局の管理職等へ事案の内容、原因、対策等について周知し、再発することが無いよう二重チェックを徹底するよう措置を講じた。 個人情報漏洩事案が発生した場合の報告についての注意喚起を各部・各事務所に改めて発出、事務連絡を管内各事務所に発出し、再発防止に努めた。 情報セキュリティに関する職員向けの研修を実施するとともに、継続的に、全職員に対し、eラーニング等を通じて個人情報保護および情報セキュリティに関する教育を実施する。 担当職員が公開用ファイルについて、個人情報をマスキングしなければならないことについての認識が不足していたことから、所属全職員に対して、改めて公開用ファイルの情報管理の徹底（個人情報のマスキング）を定期的（四半期毎を目途）に周知する。 併せて、これまで公開用ファイル送信前の二重チェックが徹底できていないかったことから、担当課長・担当職員による二重チェック後に公開ファイルを送信することを徹底する。 更なる再発防止策として、下記内容の事務連絡を管内各事務所に発出した。 ①これまで概略・予備・詳細設計のみ公開用（墨入り）成果品を作成していたが、今後は、原則として全ての業務を対象とし、公開用成果品を業務受注者に作成させる。 ②閲覧時には、公開用設計書以外の閲覧をおこなっていないかの確認を、複数の職員で行うことを徹底する。 事務連絡の発出後、会議等により関係部局に情報共有を行う。
	・測量成果検定機関の登録業務を担当する職員から、検定機関A社2名あてに、別の検定機関（B社）の「測量成果検定機関変更登録通知書」をメール添付により誤って送付した。 ・「測量成果検定機関変更登録通知書」には、個人情報が記載された「測量成果検定機関（技術管理者等）名簿」が含まれている。 ・「測量成果検定機関（技術管理者等）名簿」には、B社135名分の氏名、実務経験年数、測量士・測量士補登録No、CPDの取得状況が記載されていた。	135人	個人情報を含む資料等をメール添付で送信する際は、 ・添付ファイルの内容を必ず複数人で確認する。 ・送信時速やかに送信メールの確認が行えるようCC等の宛先への送信者個人アドレスを入力する。 その他、 ・添付ファイルの名称に機関毎の特定の番号等を付して、送信先に適したファイル添付がされているかを視認できるようにする。 について対応をするよう所属長から口頭及びメールにて注意喚起を行った。 当院で作成した個人情報漏えい防止のポイント資料の活用を定期的に周知し、職員の行為による個人情報漏えいの再発防止のための日頃の意識づけの徹底に取り組む。

保護評価に係る重大事故の定義（特定個人情報保護評価指針（令和6年5月27日改正））
6 特定個人情報に関する重大事故評価実施機関が法令に基づく安全管理措置義務を負う特定個人情報に関する事態であって、次の（1）又は（2）のいずれかに該当するもの（配送事故等のうち当該評価実施機関の責めに帰さない事由によるものを除く。）をいう。
（1）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第二十九条の四第一項及び第二項に基づく特定個人情報の漏えい等に関する報告等に関する規則（平成 27 年特定個人情報保護委員会規則第5号）第2条第1号から第3号までの各号に掲げる事態（当該事態における当該特定個人情報に係る本人が当該評価実施機関の従業者であるものを除く。）のいずれかに該当するもの
（2）同条第4号に掲げる事態のうち、当該特定個人情報に係る本人（当該評価実施機関の従業者を除く。）の数が 100 人を超えるもの
7 個人情報に関する重大事故 評価実施機関が法令に基づく安全管理措置義務を負う個人情報に関する事態であって、次の（1）から（3）までのいずれかに該当するもの（配送事故等のうち当該評価実施機関の責めに帰さない事由によるものを除く。）又は特定個人情報に関する重大事故に該当するものをいう。
（1）個人情報の保護に関する法律施行規則（平成 28 年個人情報保護委員会規則第3号）第7条第1号から第3号までの各号又は第 43 条第1号から第3号までの各号若しくは第5号に掲げる事態（当該事態における当該個人情報に係る本人が当該評価実施機関の従業者であるものを除く。）のいずれかに該当するもの
（2）同規則第7条第4号に掲げる事態のうち、当該個人情報に係る本人（当該評価実施機関の従業者を除く。下記（3）において同じ。）の数が 1,000人を超えるもの
（3）同規則第 43 条第4号に掲げる事態のうち、当該個人情報に係る本人の数が 100 人を超えるもの
（なお、上記の定義は令和6年度以降のものであり、令和5年度以前の事案については7（1）及び（2）は記載不要）