

特定個人情報保護評価書の特定個人情報保護評価指針への適合性・妥当性の審査

評価書名
国家資格等の登録等に関する事務 (海技資格、小型船舶操縦資格) 全項目評価書
評価実施機関名
国土交通大臣
提出日
令和6年9月10日
概要説明日
令和6年9月11日

(目次)

○ 全体的な事項	1
○ 特定個人情報ファイル(海技士ファイル)	4
○ 特定個人情報ファイル(小型船舶操縦士ファイル)	11
○ 評価実施機関に特有の問題に対するリスク対策	18
○ 総評	19
○ 個人情報保護委員会による審査記載事項	19

全体的な事項

※ 評価実施手続に関する事項及び特定個人情報
ファイルに共通する事項

審査の観点 (指針第10(2))	主な考慮事項	主な考慮事項(細目)	該当箇所		審査 結果	所見
(1)しきい値判断に誤りはないか。	—	—	—	—	問題は認められない	対象人数が30万人以上に該当するため、全項目評価を実施することは、指針に適合している。
(2)適切な実施主体が実施しているか。	—	1. 評価実施機関が複数存在し、取りまとめの評価実施機関が評価書を作成・提出する場合に、取りまとめ以外の全ての評価実施機関について記載しているか。	—	—	問題は認められない	特定個人情報ファイルは、国土交通省が国家資格等の登録等に関する事務(海技資格、小型船舶操縦資格)において保有するものであることから、実施主体は適切である。
(3)公表しない部分は適切な範囲か。	—	—	—	—	問題は認められない	評価書の内容は全て公表することとしている。
(4)適切な時期に実施しているか。	—	—	—	—	問題は認められない	国土交通省が国家資格等の登録等に関する事務(海技資格、小型船舶操縦資格)を実施するために使用する海技資格制度事務処理システムの改修は令和6年10月以降に予定されており、適切な時期に評価を実施している。
(5)適切な方法で広く国民の意見を求め、得られた意見を十分考慮した上で必要な見直しを行っているか。	—	—	—	—	問題は認められない	国民への意見募集については、e-Gov(電子政府の総合窓口)において、34日間実施した。 なお、寄せられた意見はなかった。
(6)特定個人情報保護評価の対象となる事務の実態に基づき、特定個人情報保護評価書様式で求められる全ての項目について検討し、記載しているか。	—	—	—	—	問題は認められない	国家資格等の登録等に関する事務(海技資格、小型船舶操縦資格)について、求められる事項が具体的に記載されている。
(7)記載された特定個人情報保護評価の実施を担当する部署は、特定個人情報保護評価の対象となる事務を担当し、リスクを軽減させるための措置の実施に責任を負うことができるか。	—	—	—	—	問題は認められない	国家資格等の登録等に関する事務(海技資格、小型船舶操縦資格)における番号制度への対応は、海事局海技課が行っており、特定個人情報保護評価の対象となる事務の実施に当たって、リスクを軽減させるための措置の実施等については、責任を負うことができる部署である。

審査の観点 (指針第10(2))	主な考慮事項	主な考慮事項(細目)	該当箇所		審査 結果	所見
(8)特定個人情報保護評価の対象となる事務の内容の記載は具体的か。当該事務における特定個人情報の流れを併せて記載しているか。	①特定個人情報ファイルを取り扱う事務やその事務において使用するシステムについて、基本情報を具体的に分かりやすく記載しているか。	2. 評価対象の事務全体の概要及びその中で特定個人情報ファイルを使用して実施する事務の内容を具体的に記載しているか。	P.3	I 1. ②	問題は認められない	国家資格等の登録等に関する事務(海技資格、小型船舶操縦資格)において、それぞれ特定個人情報ファイルを使用することが事務の流れに即し具体的に記載されている。 また、別添1の事務の内容において、資格保有者からマイナポータルを通して提出された個人番号を国家資格等情報連携・活用システムに登録し、固有の識別子と紐付けること等、事務において取り扱う特定個人情報の流れが事務の内容に即して具体的に記載されているほか、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り、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等、実現が期待されるメリット等についても具体的に記載されている。
		3. 当該システムが実現する機能の名称とその概要を具体的に記載しているか。	P.4	I 2. ②	問題は認められない	
		4. 当該システムと情報をやり取りするシステムを全て記載しているか。	P.4 ～ P.6	I 2. ③	問題は認められない	
		5. 特定個人情報ファイルを取り扱うことが評価対象の事務を実施する上で必要であることを、事務の流れに即して具体的に説明しているか。	P.7	I 4. ①	問題は認められない	
		6. 評価対象の事務において特定個人情報ファイルを取り扱うことにより、期待されるメリットについて幅広く具体的に記載しているか。	P.7	I 4. ②	問題は認められない	
		7. 事務に関わる者、事務において使用するシステム、事務において取り扱う情報の流れを具体的に記載しているか。	P.8 ～ P.9	I (別添1)	問題は認められない	
(9)特定個人情報ファイルを取り扱うプロセスにおいて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、特定個人情報保護評価の対象となる事務の実態に基づき、特定しているか。	—	—	P.24 ～ P.36	Ⅲ、Ⅳ	問題は認められない	全項目評価書に例示されている各リスクにどのように対応しているかが具体的に記載されている。

審査の観点 (指針第10(2))	主な考慮事項	主な考慮事項(細目)	該当箇所		審査 結果	所見
(10) 特定されたリスクを軽減するために講ずべき措置についての記載は具体的か。 (11) 記載されたリスクを軽減させるための措置は、個人のプライバシー等の権利利益の侵害の未然防止、国民・住民の信頼の確保という特定個人情報保護評価の目的に照らし、妥当なものか。	⑨ 特定個人情報ファイルの取扱いについて自己点検・監査や従業者に対する教育・啓発を行っているか。	70. 評価書に記載したとおりに運用がなされていること等について、評価の実施を担当する部署自らが、どのように自己点検するか具体的に記載しているか。	P.36	IV 1. ①	問題は認められない	自己点検については、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管理者が確認を行うこと、監査については、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こと等が具体的に記載されている。 従業者に対する教育・啓発については、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・研修を行うこと等が具体的に記載されている。
		71. 評価書に記載したとおりに運用がなされていること等について、どのように監査するか具体的に記載しているか。	P.36	IV 1. ②	問題は認められない	
		72. 特定個人情報を取り扱う従業者等に対しての教育・啓発や違反行為をした従業者等に対する措置について具体的に記載しているか。	P.36	IV 2.	問題は認められない	
		73. 国民・住民等からの意見聴取により得られた意見を踏まえて評価書のどの箇所をどのように修正したかを具体的に記載しているか。	P.38	VI 2. ⑤	問題は認められない	
(12) 個人のプライバシー等の権利利益の保護の宣言は、国民・住民の信頼の確保という特定個人情報保護評価の目的に照らし、妥当なものか。	—	—	P.1	表紙	問題は認められない	国土交通省は、国家資格等の登録等に関する事務(海技資格、小型船舶操縦資格)における、特定個人情報ファイルの取扱いに当たり、その取扱いが個人のプライバシー等の権利利益に影響を及ぼすものであることを認識し、特定個人情報の漏えいその他の事態を発生させるリスクを軽減させるために適切な措置を講ずることをもって、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している。

審査の観点 (指針第10(2))	主な考慮事項	主な考慮事項(細目)	該当箇所		審査 結果	所見
(8) 特定個人情報保護評価の対象となる事務の内容の記載は具体的か。当該事務における特定個人情報の流れを併せて記載しているか。	②特定個人情報ファイルの取扱いプロセスの概要(特定個人情報の入手・使用、特定個人情報ファイルの取扱いの委託、特定個人情報の提供・移転、特定個人情報の保管・消去)について、具体的に分かりやすく記載しているか。	8. 対象となる国民・住民の特定個人情報を特定個人情報ファイルにおいて保有することが事務を実施する上で必要な理由を具体的に記載しているか。	P.10	Ⅱ 2. ③	問題は認められない	特定個人情報を取り扱う理由について、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及び必要な者には当該登録により資格証の提供を行うために必要であることが具体的に記載されている。 特定個人情報の入手・使用について、専用線を利用して入手すること、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・更新・変更を行う際に、本人を特定するためなどに使用すること、特定個人情報ファイルの取扱いの委託について、システムに係る運用保守を適切に実施するためには、専門的かつ高度な知識・技術を要することから委託することが必要であること等、特定個人情報ファイルの取扱いプロセスの概要(入手・使用、委託、保管・消去)について具体的に記載されている。
		9. 主な記録項目について、保有する理由をそれぞれ具体的に記載しているか。	P.10	Ⅱ 2. ④	問題は認められない	
		10. 特定個人情報の入手に係る妥当性を具体的に記載しているか。	P.11	Ⅱ 3. ④	問題は認められない	
		11. 特定個人情報の入手の事実及び使用目的が本人に示されていることを具体的に記載しているか。	P.11	Ⅱ 3. ⑤	問題は認められない	
		12. 特定個人情報を使用する理由を具体的に記載しているか。	P.11	Ⅱ 3. ⑥	問題は認められない	
		13. 特定個人情報ファイルに記録される情報を他から入手する際の突合の内容、特定個人情報ファイルに記録された情報と他の情報との突合の方法や突合の理由を具体的に記載しているか。	P.11	Ⅱ 3. ⑧	問題は認められない	
		14. 特定個人情報を用いた統計分析を行う場合は、その内容を具体的に記載しているか。	P.11	Ⅱ 3. ⑧	該当なし	
		15. 特定個人情報を使用することにより国民の権利利益に影響を与え得る決定を行う場合は、その内容を具体的に記載しているか。	P.11	Ⅱ 3. ⑧	該当なし	
		16. 委託先に当該特定個人情報ファイルを取り扱わせることが必要な理由を具体的に記載しているか。	P.12	Ⅱ 4. ②	問題は認められない	
		17. 委託先を国民・住民等が確認できるか否か、確認できる場合はどのように確認できるか、確認できない場合はそのような取扱いが評価対象の事務を実施する上で必要な理由を具体的に記載しているか。	P.12	Ⅱ 4. ⑤	問題は認められない	
		18. 特定個人情報ファイルの取扱いを再委託するに当たって、どのような手続・方法によるかを具体的に記載しているか。	P.12	Ⅱ 4. ⑧	問題は認められない	
		19. 提供した特定個人情報が、提供先において、いかなる目的で、どのように使用されることになるかを具体的に記載しているか。	P.13	Ⅱ 5. ②	該当なし	
		20. 移転した特定個人情報が、移転先において、いかなる目的で、どのように使用されることになるかを具体的に記載しているか。	P.13	Ⅱ 5. ②	該当なし	
		21. 特定個人情報の保管場所の態様及び保管場所への立入り制限・アクセス制限について具体的に記載しているか。	P.14	Ⅱ 6. ①	問題は認められない	
		22. 特定個人情報の保管期間は妥当であるか。また、その理由を具体的に記載しているか。	P.14	Ⅱ 6. ②	問題は認められない	
		23. 保管期間を経過した特定個人情報を消去する方法を具体的に記載しているか。	P.14	Ⅱ 6. ③	問題は認められない	

審査の観点 (指針第10(2))	主な考慮事項	主な考慮事項(細目)	該当箇所		審査 結果	所見
(10) 特定されたリスクを軽減するために講ずべき措置についての記載は具体的か。 (11) 記載されたリスクを軽減させるための措置は、個人のプライバシー等の権利利益の侵害の未然防止、国民・住民の信頼の確保という特定個人情報保護評価の目的に照らし、妥当なものか。	③特定個人情報の入手について、特定されたリスクを軽減するために講ずべき措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし妥当なものか。	24. 評価対象の事務を遂行する上で必要な者以外の者の特定個人情報を入手しないよう講じている対策を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.24	Ⅲ 2. リスク1:	問題は認められない	目的外の入手が行われるリスク対策として、オンライン申請からの入手では、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こと等が具体的に記載されている。 入手の際に特定個人情報が漏えい・紛失するリスク対策として、オンライン申請からの入手では、マイナポータル経由でシステムへ登録情報等を登録するが、当該通信は、TSL/SSLによる暗号化された通信経路を使用すること、地方公共団体情報システム機構からの入手では、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等が具体的に記載されている。
		25. 事務を遂行する上で必要な情報以外の特定個人情報を入手しないよう講じている対策を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.24	Ⅲ 2. リスク1:	問題は認められない	
		26. 特定個人情報の入手に際して、適切な方法で入手するために講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.24	Ⅲ 2. リスク2:	問題は認められない	
		27. 特定個人情報を入手する際に、その特定個人情報が本人の情報であることを確認する方法を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.24	Ⅲ 2. リスク3:	問題は認められない	
		28. 入手した個人番号が本人の個人番号で間違いないことを確認する方法を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.25	Ⅲ 2. リスク3:	問題は認められない	
		29. 特定個人情報を入手した後、その情報の正確性を保つために講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.25	Ⅲ 2. リスク3:	問題は認められない	
		30. 特定個人情報を入手する際に、情報の安全確保の観点から講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.25	Ⅲ 2. リスク4:	問題は認められない	
		31. 特定個人情報の入手において、その他のリスク及びそれらのリスクへの対策についての記載はあるか。	P.25	Ⅲ 2. その他のリスク	該当なし	

審査の観点 (指針第10(2))	主な考慮事項	主な考慮事項(細目)	該当箇所		審査 結果	所見
	④特定個人情報 の使用について、特定さ れたリスクを軽減するた めに講ずべき措置を具 体的に記載しているか。 記載された対策は、特定 個人情報保護評価の目的 に照らし、妥当なものか。	32. 宛名システム等において、特定個人情報 ^が 、使用目的を超えて取り扱われないよう、また、評価対象の事務に必要な情報と併せて取り扱われないよう、講じている対策を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.26	Ⅲ 3. リスク1:	問題は認められない	目的を超えた紐付け、事務に必要な情報との紐付けが行われるリスク対策として、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を用いて、情報を紐付けて確認すること、マイナポータルにおいては、個人番号と固有の識別子を紐付けず、個人番号へはアクセスできない仕組みとしていること、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こと等が具体的に記載されている。 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対策として、原則、IDとパスワードを用いた認証方法とすること、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こと、アクセスログ、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こと等が具体的に記載されている。 特定個人情報ファイルが不正に複製されるリスク対策として、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こと等が具体的に記載されているほか、特定個人情報の使用におけるその他のリスク対策として、海技資格制度事務処理システムと国家資格等情報連携・活用システムとの連携は定められたデータ項目とその通信のみに制限されており、一方のシステムから他システムが保有するデータを検索・参照できないように制御していること等が具体的に記載されている。
		33. 事務で使用するその他のシステムにおいて、特定個人情報 ^が 、使用目的を超えて取り扱われないよう、また、評価対象の事務に必要な情報と併せて取り扱われないよう、講じている対策を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.26	Ⅲ 3. リスク1:	問題は認められない	
		34. 特定個人情報にアクセスする際の認証を行う場合は、特定個人情報にアクセスするユーザの認証方法、なりすましが行われないために講じている対策について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.26	Ⅲ 3. リスク2:	問題は認められない	
		35. 特定個人情報ファイルを取り扱う者が正当なユーザであることを確認するための情報の発効・失効の管理について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.27	Ⅲ 3. リスク2:	問題は認められない	
		36. アクセス権限の発効・失効の管理を行う者による当該管理の適正性についてチェックをしている内容を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.27	Ⅲ 3. リスク2:	問題は認められない	
		37. 特定個人情報の入手から消去までの各過程において、特定個人情報ファイルの取扱い記録やアクセスの失敗の記録等を残していることを具体的に記載しているか。記録を残していない場合は、残していても権限のない者による不正な使用を防止できる理由を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.27	Ⅲ 3. リスク2:	問題は認められない	
		38. 従業者が特定個人情報ファイルを事務外で使わないよう講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.28	Ⅲ 3. リスク3:	問題は認められない	
		39. 特定個人情報ファイルを取り扱う者が特定個人情報ファイルを不正に複製しないよう講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.28	Ⅲ 3. リスク4:	問題は認められない	
		40. 特定個人情報の使用において、その他のリスク及びそれらのリスクへの対策についての記載はあるか。	P.28	Ⅲ 3. その他の リスク	問題は認められない	

審査の観点 (指針第10(2))	主な考慮事項	主な考慮事項(細目)	該当箇所		審査 結果	所見
	⑤特定個人情報の委託について、特定されたリスクを軽減するために講ずべき措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし妥当なものか。	41. 委託先を決定する際に特定個人情報ファイルを適切に取り扱う委託先であることを確認する手続等について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.29	Ⅲ 4. 情報管理体制	問題は認められない	国家資格等情報連携・活用システムの運用等業務を委託することとしているが、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こと等が具体的に記載されている。 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こと、管理及び実施体制を書面により報告し確認を受けること、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こと、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、是正を指示すること、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こと、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、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こと、必要に応じて再委託先事業者への立入検査の実施を依頼すること等が具体的に記載されている。
		42. 委託先において特定個人情報ファイルの閲覧者・更新者を必要最小限に制限していることを具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.29	Ⅲ 4. 閲覧者の制限	問題は認められない	
		43. 委託先における特定個人情報ファイルの取扱いについて記録を残している場合は、その方法や保存期間等を具体的に記載しているか。また、記録を残していない場合は権限のない者による不正な使用を防止できる理由を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.29	Ⅲ 4. 記録	問題は認められない	
		44. 委託に伴う特定個人情報の提供に関するルールを定めている場合、ルールの内容やルール遵守の確認方法を具体的に記載しているか。また、委託先から他者への提供を認めていない場合、提供されていないことを確認する方法を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.29	Ⅲ 4. 提供ルール	問題は認められない	
		45. 委託先における特定個人情報の消去のルールを定めている場合は、ルールの内容やルール遵守の確認方法を具体的に記載しているか。また、委託契約終了後に消去されていることを確認する方法を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.30	Ⅲ 4. 消去ルール	問題は認められない	
		46. 委託先と締結する委託契約における特定個人情報ファイルの取扱いに関する規定について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.30	Ⅲ 4. 委託契約書中の規定	問題は認められない	
		47. 特定個人情報ファイルの取扱いを再委託している場合、再委託先での適正な取扱いの確保のために行っている措置について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.30	Ⅲ 4. 再委託	問題は認められない	
		48. 特定個人情報ファイルの取扱いの委託において、その他のリスク及びそれらのリスクへの対策についての記載はあるか。	P.30	Ⅲ 4. その他のリスク	該当なし	

審査の観点 (指針第10(2))	主な考慮事項	主な考慮事項(細目)	該当箇所		審査 結果	所見
	⑥特定個人情報の提供・移転について、特定されたリスクを軽減するために講ずべき措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	49. 特定個人情報の提供又は移転の記録を残している場合は、その記録の内容や記録方法、保存期間等を具体的に記載しているか。また、記録を残していない場合は特定個人情報不正に提供又は移転されることを防止できる理由を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.31	Ⅲ 5. リスク1:	該当なし	—
		50. 特定個人情報の提供・移転に関するルールを定めている場合は、ルールの内容やルール遵守の確認方法を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.31	Ⅲ 5. リスク1:	該当なし	
		51. 特定個人情報を提供・移転する際に、情報漏えいや紛失のリスクを軽減するための措置や提供先・移転先における特定個人情報の使途が法令に基づく適切なものであることを確認するための措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.31	Ⅲ 5. リスク2:	該当なし	
		52. 誤った特定個人情報を提供・移転することや誤った相手に提供・移転することを防止する措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.31	Ⅲ 5. リスク3:	該当なし	
		53. 特定個人情報の提供・移転において、その他のリスク及びそれらのリスクへの対策についての記載はあるか。	P.31	Ⅲ 5. その他の リスク	該当なし	

審査の観点 (指針第10(2))	主な考慮事項	主な考慮事項(細目)	該当箇所		審査 結果	所見
	⑦情報提供ネットワークシステムとの接続について、特定されたリスクを軽減するために講ずべき措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	54. 情報提供ネットワークシステムを通じて特定個人情報を入力する際に、目的外の入手が行われないために講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.32	Ⅲ 6. リスク1:	問題は認められない	目的外の入手が行われるリスク対策として、ログイン時の利用者認証のほかに、ログイン・ログアウトを実施した利用者、時刻及び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こと等が具体的に記載されている。 入手の際に特定個人情報が漏えい・紛失するリスク対策として、中間サーバーと団体については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こと等が具体的に記載されている。 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対策として、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こと等が具体的に記載されている。
		55. 情報提供ネットワークシステムを通じて特定個人情報を入力する際に、特定個人情報の安全が保たれない不適切な方法で特定個人情報を入力しないために講じている対策を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.32	Ⅲ 6. リスク2:	問題は認められない	
		56. 情報提供ネットワークシステムを通じて特定個人情報を入力した後、その情報の正確性を保つために講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.32	Ⅲ 6. リスク3:	問題は認められない	
		57. 情報提供ネットワークシステムを通じて特定個人情報を入力する際に、情報漏えいや紛失のリスクを軽減するために講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.33	Ⅲ 6. リスク4:	問題は認められない	
		58. 情報提供ネットワークシステムを通じて提供する際に、特定個人情報の不正な提供が行われるリスクを軽減するために講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.33	Ⅲ 6. リスク5:	該当なし	
		59. 情報提供ネットワークシステムを通じて提供する際に、特定個人情報の提供方法が不適切とならないよう講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.33	Ⅲ 6. リスク6:	該当なし	
		60. 情報提供ネットワークシステムを通じて提供する際に、誤った特定個人情報を提供することや、誤った相手に提供することを防止するために講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.33	Ⅲ 6. リスク7:	該当なし	
		61. 情報提供ネットワークシステムとの接続に伴うリスクについて、その他のリスク及びそれらのリスクへの対策についての記載はあるか。	P.33	Ⅲ 6. その他のリスク	問題は認められない	

審査の観点 (指針第10(2))	主な考慮事項	主な考慮事項(細目)	該当箇所		審査 結果	所見
	⑧特定個人情報の 保管・消去について、 特定されたリスクを軽減 するために講ずべき措置を具 体的に記載しているか。記 載された対策は、特定個人 情報保護評価の目的に照ら し妥当なものか。	62. 特定個人情報の漏えい・滅失・毀損を防ぐため に行っている物理的な対策について具体的に記 載しているか。記載された対策は、特定個人情報 保護評価の目的に照らし、妥当なものか。	P.34	Ⅲ 7. リスク1: ⑤	問題は認 められな い	物理的対策として、国家資格等情報連携・活用システムの パブリッククラウド環境については、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又は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、オンプレミス環境については、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、情報セキュリティマ ネジメントシステム(ISMS)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等が具体的に記載され ている。 技術的対策として、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 グの解析を行うこと、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 秘匿や漏えい防止が可能なパブリッククラウドサービスを使 用すること、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えい防止が可能なネットワーク回線 を使用すること等が具体的に記載されている。 特定個人情報が消去されずいつまでも存在するリスク対策 として、マイナポータル内に情報等は保管されないこと、オン プレミス環境では、特定個人情報等が記録された機器や電 子記録媒体等を廃棄する場合、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こと、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 ロセスを確保すること等が具体的に記載されている。
		63. 特定個人情報の漏えい・滅失・毀損を防ぐため に行っている技術的な対策について具体的に記 載しているか。記載された対策は、特定個人情報 保護評価の目的に照らし、妥当なものか。	P.34	Ⅲ 7. リスク1: ⑥	問題は認 められな い	
		64. 過去3年以内に発生した全ての重大事故の内 容、原因、影響、重大事故発生時への対応等につ いて具体的に記載しているか。記載された対策 は、特定個人情報保護評価の目的に照らし、妥 当なものか。	P.21 ～ P.23 P.35	Ⅲ 7. リスク1: ⑨	問題は認 められな い	
		65. 重大事故を受けて策定・実施した再発防止策 の内容について具体的に記載しているか。記載さ れた対策は、特定個人情報保護評価の目的に照 らし、妥当なものか。	P.21 ～ P.23 P.35	Ⅲ 7. リスク1: ⑨	問題は認 められな い	
		66. 死者の個人番号を保管している場合は保管方 法を具体的に記載しているか。記載された対策 は、特定個人情報保護評価の目的に照らし、妥 当なものか。	P.35	Ⅲ 7. リスク1: ⑩	問題は認 められな い	
		67. 特定個人情報を最新の状態 で保管するため に行っている措置を具体的に記載しているか。記 載された対策は、特定個人情報保護評価の目的 に照らし、妥当なものか。	P.35	Ⅲ 7. リスク2:	問題は認 められな い	
		68. 保管期間を経過した特定個人情報を適切な 時に安全かつ確実に消去できる手続・体制・手 法になっているか等について具体的に記載して いるか。記載された対策は、特定個人情報保護 評価の目的に照らし、妥当なものか。	P.35	Ⅲ 7. リスク3:	問題は認 められな い	
		69. 特定個人情報の保管・消去において、その 他のリスク及びそれらのリスクへの対策につ いての記載はあるか。	P.35	Ⅲ 7. その他の リスク	該当なし	

特定個人情報ファイル
(小型船舶操縦士ファイル)

審査の観点 (指針第10(2))	主な考慮事項	主な考慮事項(細目)	該当箇所		審査 結果	所見
(8) 特定個人情報保護評価の対象となる事務の内容の記載は具体的か。当該事務における特定個人情報の流れを併せて記載しているか。	② 特定個人情報ファイルの取扱いプロセスの概要(特定個人情報の入手・使用、特定個人情報ファイルの取扱いの委託、特定個人情報の提供・移転、特定個人情報の保管・消去)について、具体的に分かりやすく記載しているか。	8. 対象となる国民・住民の特定個人情報を特定個人情報ファイルにおいて保有することが事務を実施する上で必要な理由を具体的に記載しているか。	P.15	Ⅱ 2. ③	問題は認められない	特定個人情報を取り扱う理由について、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及び必要な者には当該登録により資格証の提供を行うために必要であることが具体的に記載されている。 特定個人情報の入手・使用について、専用線を利用して入手すること、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・更新・変更を行う際に、本人を特定するためなどに使用すること、特定個人情報ファイルの取扱いの委託について、システムに係る運用保守を適切に実施するためには、専門的かつ高度な知識・技術を要することから委託することが必要であること等、特定個人情報ファイルの取扱いプロセスの概要(入手・使用、委託、保管・消去)について具体的に記載されている。
		9. 主な記録項目について、保有する理由をそれぞれ具体的に記載しているか。	P.15	Ⅱ 2. ④	問題は認められない	
		10. 特定個人情報の入手に係る妥当性を具体的に記載しているか。	P.16	Ⅱ 3. ④	問題は認められない	
		11. 特定個人情報の入手の事実及び使用目的が本人に示されていることを具体的に記載しているか。	P.16	Ⅱ 3. ⑤	問題は認められない	
		12. 特定個人情報を使用する理由を具体的に記載しているか。	P.16	Ⅱ 3. ⑥	問題は認められない	
		13. 特定個人情報ファイルに記録される情報を他から入手する際の突合の内容、特定個人情報ファイルに記録された情報と他の情報との突合の方法や突合の理由を具体的に記載しているか。	P.16	Ⅱ 3. ⑧	問題は認められない	
		14. 特定個人情報を用いた統計分析を行う場合は、その内容を具体的に記載しているか。	P.16	Ⅱ 3. ⑧	該当なし	
		15. 特定個人情報を使用することにより国民の権利利益に影響を与え得る決定を行う場合は、その内容を具体的に記載しているか。	P.16	Ⅱ 3. ⑧	該当なし	
		16. 委託先に当該特定個人情報ファイルを取り扱わせることが必要な理由を具体的に記載しているか。	P.17	Ⅱ 4. ②	問題は認められない	
		17. 委託先を国民・住民等が確認できるか否か、確認できる場合はどのように確認できるか、確認できない場合はそのような取扱いが評価対象の事務を実施する上で必要な理由を具体的に記載しているか。	P.17	Ⅱ 4. ⑤	問題は認められない	
		18. 特定個人情報ファイルの取扱いを再委託するに当たって、どのような手続・方法によるかを具体的に記載しているか。	P.17	Ⅱ 4. ⑧	問題は認められない	
		19. 提供した特定個人情報が、提供先において、いかなる目的で、どのように使用されることになるかを具体的に記載しているか。	P.18	Ⅱ 5. ②	該当なし	
		20. 移転した特定個人情報が、移転先において、いかなる目的で、どのように使用されることになるかを具体的に記載しているか。	P.18	Ⅱ 5. ②	該当なし	
		21. 特定個人情報の保管場所の態様及び保管場所への立入り制限・アクセス制限について具体的に記載しているか。	P.19	Ⅱ 6. ①	問題は認められない	
		22. 特定個人情報の保管期間は妥当であるか。また、その理由を具体的に記載しているか。	P.19	Ⅱ 6. ②	問題は認められない	
		23. 保管期間を経過した特定個人情報を消去する方法を具体的に記載しているか。	P.19	Ⅱ 6. ③	問題は認められない	

審査の観点 (指針第10(2))	主な考慮事項	主な考慮事項(細目)	該当箇所		審査 結果	所見
(10) 特定されたリスクを軽減するために講ずべき措置についての記載は具体的か。 (11) 記載されたリスクを軽減させるための措置は、個人のプライバシー等の権利利益の侵害の未然防止、国民・住民の信頼の確保という特定個人情報保護評価の目的に照らし、妥当なものか。	③特定個人情報の入手について、特定されたリスクを軽減するために講ずべき措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし妥当なものか。	24. 評価対象の事務を遂行する上で必要な者以外の者の特定個人情報を入手しないよう講じている対策を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.24	Ⅲ 2. リスク1:	問題は認められない	目的外の入手が行われるリスク対策として、オンライン申請からの入手では、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こと等が具体的に記載されている。 入手の際に特定個人情報が漏えい・紛失するリスク対策として、オンライン申請からの入手では、マイナポータル経由でシステムへ登録情報等を登録するが、当該通信は、TSL/SSLによる暗号化された通信経路を使用すること、地方公共団体情報システム機構からの入手では、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等が具体的に記載されている。
		25. 事務を遂行する上で必要な情報以外の特定個人情報を入手しないよう講じている対策を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.24	Ⅲ 2. リスク1:	問題は認められない	
		26. 特定個人情報の入手に際して、適切な方法で入手するために講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.24	Ⅲ 2. リスク2:	問題は認められない	
		27. 特定個人情報を入手する際に、その特定個人情報本人の情報であることを確認する方法を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.24	Ⅲ 2. リスク3:	問題は認められない	
		28. 入手した個人番号が本人の個人番号で間違いないことを確認する方法を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.25	Ⅲ 2. リスク3:	問題は認められない	
		29. 特定個人情報を入手した後、その情報の正確性を保つために講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.25	Ⅲ 2. リスク3:	問題は認められない	
		30. 特定個人情報を入手する際に、情報の安全確保の観点から講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.25	Ⅲ 2. リスク4:	問題は認められない	
		31. 特定個人情報の入手において、その他のリスク及びそれらのリスクへの対策についての記載はあるか。	P.25	Ⅲ 2. その他のリスク	該当なし	

審査の観点 (指針第10(2))	主な考慮事項	主な考慮事項(細目)	該当箇所		審査 結果	所見
	④特定個人情報 の使用について、特定さ れたリスクを軽減するた めに講ずべき措置を具 体的に記載しているか。 記載された対策は、特定 個人情報保護評価の目的 に照らし、妥当なものか。	32. 宛名システム等において、特定個人情報 ^が 、使用目的を超えて取り扱われないよう、また、評価対象の事務に必要な情報と併せて取り扱われないよう、講じている対策を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.26	Ⅲ 3. リスク1:	問題は認められない	目的を超えた紐付け、事務に必要な情報との紐付けが行われるリスク対策として、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を用いて、情報を紐付けて確認すること、マイナポータルにおいては、個人番号と固有の識別子を紐付けず、個人番号へはアクセスできない仕組みとしていること、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こと等が具体的に記載されている。 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対策として、原則、IDとパスワードを用いた認証方法とすること、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こと、アクセスログ、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こと等が具体的に記載されている。 特定個人情報ファイルが不正に複製されるリスク対策として、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こと等が具体的に記載されているほか、特定個人情報の使用におけるその他のリスク対策として、海技資格制度事務処理システムと国家資格等情報連携・活用システムとの連携は定められたデータ項目とその通信のみに制限されており、一方のシステムから他システムが保有するデータを検索・参照できないように制御していること等が具体的に記載されている。
		33. 事務で使用するその他のシステムにおいて、特定個人情報 ^が 、使用目的を超えて取り扱われないよう、また、評価対象の事務に必要な情報と併せて取り扱われないよう、講じている対策を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.26	Ⅲ 3. リスク1:	問題は認められない	
		34. 特定個人情報にアクセスする際の認証を行う場合は、特定個人情報にアクセスするユーザの認証方法、なりすましが行われないために講じている対策について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.26	Ⅲ 3. リスク2:	問題は認められない	
		35. 特定個人情報ファイルを取り扱う者が正当なユーザであることを確認するための情報の発効・失効の管理について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.27	Ⅲ 3. リスク2:	問題は認められない	
		36. アクセス権限の発効・失効の管理を行う者による当該管理の適正性についてチェックをしている内容を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.27	Ⅲ 3. リスク2:	問題は認められない	
		37. 特定個人情報の入手から消去までの各過程において、特定個人情報ファイルの取扱い記録やアクセスの失敗の記録等を残していることを具体的に記載しているか。記録を残していない場合は、残していても権限のない者による不正な使用を防止できる理由を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.27	Ⅲ 3. リスク2:	問題は認められない	
		38. 従業者が特定個人情報ファイルを事務外で使わないよう講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.28	Ⅲ 3. リスク3:	問題は認められない	
		39. 特定個人情報ファイルを取り扱う者が特定個人情報ファイルを不正に複製しないよう講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.28	Ⅲ 3. リスク4:	問題は認められない	
		40. 特定個人情報の使用において、その他のリスク及びそれらのリスクへの対策についての記載はあるか。	P.28	Ⅲ 3. その他の リスク	問題は認められない	

審査の観点 (指針第10(2))	主な考慮事項	主な考慮事項(細目)	該当箇所		審査 結果	所見
	⑤特定個人情報の委託について、特定されたリスクを軽減するために講ずべき措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし妥当なものか。	41. 委託先を決定する際に特定個人情報ファイルを適切に取り扱う委託先であることを確認する手続等について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.29	Ⅲ 4. 情報管理体制	問題は認められない	国家資格等情報連携・活用システムの運用等業務を委託することとしているが、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こと等が具体的に記載されている。 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こと、管理及び実施体制を書面により報告し確認を受けること、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こと、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、是正を指示すること、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こと、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、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こと、必要に応じて再委託先事業者への立入検査の実施を依頼すること等が具体的に記載されている。
		42. 委託先において特定個人情報ファイルの閲覧者・更新者を必要最小限に制限していることを具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.29	Ⅲ 4. 閲覧者の制限	問題は認められない	
		43. 委託先における特定個人情報ファイルの取扱いについて記録を残している場合は、その方法や保存期間等を具体的に記載しているか。また、記録を残していない場合は権限のない者による不正な使用を防止できる理由を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.29	Ⅲ 4. 記録	問題は認められない	
		44. 委託に伴う特定個人情報の提供に関するルールを定めている場合、ルールの内容やルール遵守の確認方法を具体的に記載しているか。また、委託先から他者への提供を認めていない場合、提供されていないことを確認する方法を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.29	Ⅲ 4. 提供ルール	問題は認められない	
		45. 委託先における特定個人情報の消去のルールを定めている場合は、ルールの内容やルール遵守の確認方法を具体的に記載しているか。また、委託契約終了後に消去されていることを確認する方法を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.30	Ⅲ 4. 消去ルール	問題は認められない	
		46. 委託先と締結する委託契約における特定個人情報ファイルの取扱いに関する規定について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.30	Ⅲ 4. 委託契約書中の規定	問題は認められない	
		47. 特定個人情報ファイルの取扱いを再委託している場合、再委託先での適正な取扱いの確保のために行っている措置について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.30	Ⅲ 4. 再委託	問題は認められない	
		48. 特定個人情報ファイルの取扱いの委託において、その他のリスク及びそれらのリスクへの対策についての記載はあるか。	P.30	Ⅲ 4. その他のリスク	該当なし	

審査の観点 (指針第10(2))	主な考慮事項	主な考慮事項(細目)	該当箇所		審査 結果	所見
	⑥特定個人情報の提供・移転について、特定されたリスクを軽減するために講ずべき措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし妥当なものか。	49. 特定個人情報の提供又は移転の記録を残している場合は、その記録の内容や記録方法、保存期間等を具体的に記載しているか。また、記録を残していない場合は特定個人情報が不正に提供又は移転されることを防止できる理由を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.31	Ⅲ 5. リスク1:	該当なし	—
		50. 特定個人情報の提供・移転に関するルールを定めている場合は、ルールの内容やルール遵守の確認方法を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.31	Ⅲ 5. リスク1:	該当なし	
		51. 特定個人情報を提供・移転する際に、情報漏えいや紛失のリスクを軽減するための措置や提供先・移転先における特定個人情報の使途が法令に基づく適切なものであることを確認するための措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.31	Ⅲ 5. リスク2:	該当なし	
		52. 誤った特定個人情報を提供・移転することや誤った相手に提供・移転することを防止する措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.31	Ⅲ 5. リスク3:	該当なし	
		53. 特定個人情報の提供・移転において、その他のリスク及びそれらのリスクへの対策についての記載はあるか。	P.31	Ⅲ 5. その他の リスク	該当なし	

審査の観点 (指針第10(2))	主な考慮事項	主な考慮事項(細目)	該当箇所		審査 結果	所見
	⑦情報提供ネットワークシステムとの接続について、特定されたリスクを軽減するために講ずべき措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	54. 情報提供ネットワークシステムを通じて特定個人情報を入力する際に、目的外の入手が行われないために講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.32	Ⅲ 6. リスク1:	問題は認められない	目的外の入手が行われるリスク対策として、ログイン時の利用者認証のほかに、ログイン・ログアウトを実施した利用者、時刻及び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こと等が具体的に記載されている。 入手の際に特定個人情報が漏えい・紛失するリスク対策として、中間サーバーと団体については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こと等が具体的に記載されている。 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対策として、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こと等が具体的に記載されている。
		55. 情報提供ネットワークシステムを通じて特定個人情報を入力する際に、特定個人情報の安全が保たれない不適切な方法で特定個人情報を入力しないために講じている対策を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.32	Ⅲ 6. リスク2:	問題は認められない	
		56. 情報提供ネットワークシステムを通じて特定個人情報を入力した後、その情報の正確性を保つために講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.32	Ⅲ 6. リスク3:	問題は認められない	
		57. 情報提供ネットワークシステムを通じて特定個人情報を入力する際に、情報漏えいや紛失のリスクを軽減するために講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.33	Ⅲ 6. リスク4:	問題は認められない	
		58. 情報提供ネットワークシステムを通じて提供する際に、特定個人情報の不正な提供が行われるリスクを軽減するために講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.33	Ⅲ 6. リスク5:	該当なし	
		59. 情報提供ネットワークシステムを通じて提供する際に、特定個人情報の提供方法が不適切とならないよう講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.33	Ⅲ 6. リスク6:	該当なし	
		60. 情報提供ネットワークシステムを通じて提供する際に、誤った特定個人情報を提供することや、誤った相手に提供することを防止するために講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.33	Ⅲ 6. リスク7:	該当なし	
		61. 情報提供ネットワークシステムとの接続に伴うリスクについて、その他のリスク及びそれらのリスクへの対策についての記載はあるか。	P.33	Ⅲ 6. その他のリスク	問題は認められない	

審査の観点 (指針第10(2))	主な考慮事項	主な考慮事項(細目)	該当箇所		審査 結果	所見
	⑧特定個人情報の 保管・消去について、 特定されたリスクを軽減 するために講ずべき措置を具 体的に記載しているか。記 載された対策は、特定個人 情報保護評価の目的に照ら し妥当なものか。	62. 特定個人情報の漏えい・滅失・毀損を防ぐため に行っている物理的な対策について具体的に記 載しているか。記載された対策は、特定個人情報 保護評価の目的に照らし、妥当なものか。	P.34	Ⅲ 7. リスク1: ⑤	問題は認 められな い	物理的対策として、国家資格等情報連携・活用システムの パブリッククラウド環境については、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又は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、オンプレミス環境については、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、情報セキュリティマ ネジメントシステム(ISMS)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等が具体的に記載され ている。 技術的対策として、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 グの解析を行うこと、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 秘匿や漏えい防止が可能なパブリッククラウドサービスを使 用すること、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えい防止が可能なネットワーク回線 を使用すること等が具体的に記載されている。 特定個人情報が消去されずいつまでも存在するリスク対策 として、マイナポータル内に情報等は保管されないこと、オン プレミス環境では、特定個人情報等が記録された機器や電 子記録媒体等を廃棄する場合、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こと、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 ロセスを確保すること等が具体的に記載されている。
		63. 特定個人情報の漏えい・滅失・毀損を防ぐため に行っている技術的な対策について具体的に記 載しているか。記載された対策は、特定個人情報 保護評価の目的に照らし、妥当なものか。	P.34	Ⅲ 7. リスク1: ⑥	問題は認 められな い	
		64. 過去3年以内に発生した全ての重大事故の 内容、原因、影響、重大事故発生時への対応等につ いて具体的に記載しているか。記載された対策 は、特定個人情報保護評価の目的に照らし、妥 当なものか。	P.21 ～ P.23 P.35	Ⅲ 7. リスク1: ⑨	問題は認 められな い	
		65. 重大事故を受けて策定・実施した再発防止策 の内容について具体的に記載しているか。記載さ れた対策は、特定個人情報保護評価の目的に照 らし、妥当なものか。	P.21 ～ P.23 P.35	Ⅲ 7. リスク1: ⑨	問題は認 められな い	
		66. 死者の個人番号を保管している場合は保管方 法を具体的に記載しているか。記載された対策 は、特定個人情報保護評価の目的に照らし、妥 当なものか。	P.35	Ⅲ 7. リスク1: ⑩	問題は認 められな い	
		67. 特定個人情報を最新の状態 で保管する ために行っている措置を具体的に記載している か。記載された対策は、特定個人情報保護評 価の目的に照らし、妥当なものか。	P.35	Ⅲ 7. リスク2:	問題は認 められな い	
		68. 保管期間を経過した特定個人情報を適切 な時に安全かつ確実に消去できる手続・体制・手 法になっているか等について具体的に記載して いるか。記載された対策は、特定個人情報保 護評価の目的に照らし、妥当なものか。	P.35	Ⅲ 7. リスク3:	問題は認 められな い	
		69. 特定個人情報の保管・消去において、その 他のリスク及びそれらのリスクへの対策につ いての記載はあるか。	P.35	Ⅲ 7. その他の リスク	該当なし	

審査の観点 (指針第10(2))	主な考慮事項	主な考慮事項(細目)	該当箇所		審査 結果	所見
(10) 特定されたリスクを軽減するために講ずべき措置についての記載は具体的か。 (11) 記載されたリスクを軽減させるための措置は、個人のプライバシー等の権利利益の侵害の未然防止、国民・住民の信頼の確保という特定個人情報保護評価の目的に照らし、妥当なものか。	⑩その他、評価実施機関に特有な問題や懸念に対し、特定されたリスクを軽減するために講ずべき措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし妥当なものか。	74. 資格情報を含む特定個人情報を国家資格等情報連携・活用システムを用いて管理する際のリスク対策について具体的に記載されているか。記載された対策は特定個人情報保護評価の目的に照らし、妥当なものか。	P.24 ～ P.36	Ⅲ 3. リスク2 等	問題とは認められない	入手した特定個人情報と不一致であるリスクへの対策として、 ・申請者がマイナポータルから申請を行う際に、マイナンバーカードの券面事項入力補助機能を活用することにより、個人番号を含む申請情報の正確性を確保すること ・定期的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及び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うこと、 ・不正アクセスや委託先事業者による不正のリスクへの対策として、 ・特定個人情報等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こと 等が具体的に記載されており、特定個人情報保護評価の目的に照らし、妥当である。
		75. 評価実施機関が国家資格等情報連携・活用システムの利用場面以外で実施するリスク対策について具体的に記載されているか。記載された対策は特定個人情報保護評価の目的に照らし、妥当なものか。	P.24 ～ P.36	Ⅲ 3. リスク2 等	問題とは認められない	特定個人情報ファイルの情報が不一致であるリスクへの対策として、 ・利用者の申請等により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こと、 ・権限のない者によって不正に使用されるリスクへの対策として、 ・本人確認端末について、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を割り当てること、 ・リスク対策の実効性担保のための措置として、 ・システム・端末の操作ログを取得し、定期的に分析すること ・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的に自己点検・内部監査を実施すること 等が具体的に記載されており、特定個人情報保護評価の目的に照らし、妥当である。

【総評】

- (1) 国家資格等の登録等に関する事務(海技資格、小型船舶操縦資格)においては、特定個人情報ファイルを取り扱うことについて、一連の事務の内容や流れが具体的に記載されており、特段の問題は認められないものと考えられる。
- (2) 事務で取り扱われる特定個人情報ファイルの取扱いについての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ものと考えられる。
- (3) 資格情報を含む特定個人情報を入手し、国家資格等情報連携・活用システムを用いて管理する際のリスク対策等、本評価対象事務において懸念されるリスク及びリスク対策についても、具体的に記載されており、特段の問題は認められないものと考えられる。

【個人情報保護委員会による審査記載事項】

(Ⅵ 評価実施手続 4. 個人情報保護委員会の承認)

- (1) 国家資格等の登録等に関する事務(海技資格、小型船舶操縦資格)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・見直しを行い、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は、従事者が特定個人情報ファイルを事務外で使用しないようアクセス権限の管理や操作ログの記録・分析を行うこと、国家資格等情報連携・活用システムの運用保守事業者には報告書を提出させ、必要に応じて立入検査を実施すること等のリスク対策が記載されている。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) 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、システムに登録される資格の拡大に伴い、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。