別紙

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：　社会保険労務士事務所（パターンＤ事務所）が委託契約に基づき、労働社会保険諸法令関係書類に、個人情報を記載して公共職業安定所、日本年金機構及び健康保険組合等に提出する事務に関する評価書

全体的な事項

審査の観点	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	—	—	—	適切	「モデル評価書」としてしきい値判断は行っていないが、特定個人情報の適切な取扱いを目的として全項目評価を実施している。
(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。	—	適切	「モデル評価書」として、社会保険労務士事務所における評価を想定していることから、社会保険労務士事務所を評価実施主体とし、他の評価実施機関はなしとしている。
(3) 公表しない部分は適切な範囲か。	—	—	—	適切	公表しないとしている項目は無い。
(4) 適切な時期に実施しているか。	—	—	—	該当なし	前回の特定個人情報保護評価から 5 年経過する前に再実施している。
(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。	—	—	—	該当なし	特定個人情報保護評価の枠組みを用いて任意に評価を実施するものである。
(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すべての項目について検討し、記載しているか。	—	—	—	適切	社会保険労務士法（昭和 43 年法律第 89 号）第 2 条に規定される事務について、求められる事項がすべて記載されている。
(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。	—	—	—	適切	「モデル評価書」として、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、社会保険労務士事務所における代表者としている。
(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。	Ⅰ1. ②	適切	事務の内容が漏れなく、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。	Ⅰ2. システム 1,2,3	適切	本事務で使用するシステムの機能の名称と概要が具体的に記載されている。
		4. 当該システムと情報をやり取りするシステムをすべて記載しているか。	Ⅰ2. ③	適切	当該システムと接続して情報をやりとりするシステムが記載されている。
		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。	Ⅰ4. ①	適切	評価対象の事務を実施するうえで、特定個人情報ファイルを取り扱うことが必要である旨が説明されている。
		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。	Ⅰ4. ②	適切	行政機関等との手続きに必要な情報を管理することが明記されていることを確認した。
		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	Ⅰ（別添 1）	適切	各事務の流れを別添 1 に具体的に記載していることを確認した。

審査の観点	主な考慮事項	主な考慮事項（細目）	該当箇所	審査結果	所見
		の流れを具体的に記載しているか。			
（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、個人情報保護の対象となる事務の実態に基づき、特定しているか。	―	―		適切	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。 課題（別紙参照） リスク分析手法・プロセスを説明する等を行うことによって、リスク分析の結果を特定個人情報保護評価書に反映することを薦めます。
（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、評価の実態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。	Ⅳ1.①	適切	自己点検については、評価書記載事項の運用状況を 1 年に 1 回以上システムログ又は利用実績の記録により確認すると具体的に記載されている。また、定期的に特定個人情報取扱規程に基づいて特定個人情報の取扱いに関する安全対策及び諸施策を見直し、改善すると記載されている。加えて、特定個人情報の取扱が法令、ガイドライン、規程およびその他の規範と合致していることを定期的（年 1 回以上）に確認する旨が記載されていることも確認した。 課題（別紙参照） 点検項目や点検手法を記載することを薦めます。
		71. 評価書に記載したとおりに運営がなされていることを等について、どのように監査するか具体的に記載しているか。	Ⅳ1.②	適切	監査については、内部監査員が定期的（年 1 回以上）に監査すると記載されている。また、特定個人情報管理責任者は、特定個人情報取扱規程に基づき外部監査結果や経営環境により特定個人情報の取扱いに関する安全対策及び諸施策を定期的に見直し、改善すると記載されている。加えて、モデル評価書として、外部監査に関しても記載されていることを確認した。
		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。	Ⅳ2	適切	少なくとも年 1 回以上、個人情報保護及び情報セキュリティに関する研修を実施すること、入職時に特定個人情報等の適切な取扱いに関する研修の受講を必須としていることを記載している。また、研修を複数回開催することで未受講者への受講機会を与えるだけでなく、すべての取扱い者が確実に受講する旨も記載されており、年 1 回以上の研修は、特定個人情報の取扱いを含むことが記載されていることを確認した。
		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。	別添 3	適切	モデル評価書として、別添 3 に変更箇所の記載例が記載されていることを確認した。
（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。	―	―	表紙	適切	社労士事務所は、委託契約に基づく個人番号関係事務及び委任による個人の手続事務における特定個人情報ファイルの取扱いに当り、特定個人情報ファイルの取扱いが委託者の従業員等及び委任者の個人のプライバシー等の権利利益に影響を及ぼしかねないことを認識し、特定個人情報の漏えいその他の事態を発生させるリスクを軽減させるために適切な措置を講じ、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。

顧問先従業員（被保険者台帳）情報ファイル

審査の観点	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。	II 2.③	適切	事務手続きの対象となる顧問先の従業員及び当該従業員の被扶養者を記録するために必要であると記載されている。
		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。	II 2. ④	適切	
		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。	II 3. ①②④	適切	委託契約業務遂行のためとしている。FAX について、使用を推奨するものではないものの、実態として FAX の取り扱いがあり、記載漏れを防止する意図である旨を確認した。
		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。	II 3. ⑤	適切	「委託者である顧問先にて実施」としている。
		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。	II 3. ⑥	適切	特定個人情報を使用する目的が具体的に記載されている
		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。	II 3. ⑧	適切	個人のプライバシー等の権利利益の観点から、不必要な突合を行わない旨が記載されていることを確認した。
		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。	II 3. ⑧	該当なし	統計分析を行わない。
		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。	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。	II 4. ②	適切	委託事項は 2 つあるが、いずれも特定個人情報ファイルの取扱いを委託する理由が具体的に記載されている。また、委託することに関する妥当性に加え、委託する範囲の妥当性についても記載されていることを確認した。
		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。	II 4. ⑤⑥	適切	「モデル評価書」として、具体的な委託先名がわかる記載（株式会社〇〇等）がされていることを確認した。また、「⑤委託先名の確認方法」は対象読者を想定し、当該読者が契約締結前に確認可能であることを確認した。
		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。	II 4. ⑧	適切	「委託先からの書面による申請に基づき、妥当性を考慮し顧問先企業の許諾を得た上で、書面により許諾を回答する」とされており、「妥当性」の具体的な内容が記載されている。また、自らが果たすべき安全管理措置と同等の措置が講じられるよう必要かつ適切な監督として、委託先の適切な選定、安全管理措置に関する委託契約の締結、委託先における特定個人情報の取扱状況の把握が含まれることが記載されていることを確認した。
		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。	II 5. ②	適切	提供先及び提供先における用途が具体的に記載されている

審査の観点	主な考慮事項	主な考慮事項（細目）	該当箇所	審査結果	所見
		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。	II 5．移転先 1	該当なし	移転先はない。
		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。	II 6．①	適切	端末設置場所、電子記録媒体保管場所、紙媒体保管場所のそれぞれの態様と立入制限、アクセス制限について具体的に記載している。
		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。	II 6．②	適切	保管期間の記載が不要との誤解が生じないよう、モデル評価書として期間の例（複数ある場合は最も長い期間）が記載されていることを確認した。
		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。	II 6．③	適切	リース機器の返却の際等も廃棄と同様の措置を行う旨が記載されていることを確認した。

個人番号情報（特定個人情報）ファイル

審査の観点	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。	II 2.③	適切	事務手続きの対象となる顧問先の従業員及び当該従業員の被扶養者を記録するために必要であることが記載されている。
		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。	II 2．④	適切	識別情報、連絡先等情報のそれぞれについて保有する理由が記載されている。
		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。	II 3. ①②④	適切	委託契約業務遂行のためとしている。FAX については、使用を推奨するものではないものの、実態としてFAX の取り扱いがあり、記載漏れを防止する意図である旨を確認した。
		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。	II 3．⑤	適切	特定個人情報の入手の事実、利用目的は委託者である顧問先が本人へ明示していることが記載されている。
		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。	II 3．⑥	適切	特定個人情報の使用目的として 4 つの事務を記載している。
		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。	II 3．⑧	適切	個人のプライバシー等の権利利益の観点から、不必要な突合を行わない旨が記載されていることを確認した。
		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。	II 3．⑧	該当なし	統計分析を行わない。
		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。	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。	II 4．②	適切	委託事項は 2 つあるが、いずれも特定個人情報ファイルの取扱いを委託する理由が具体的に記載されている。また、委託することに関する妥当性に加え、委託する範囲の妥当性についても記載されていることを確認した。
		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。	II 4. ⑤	適切	「モデル評価書」として、具体的な委託先名がわかる記載（株式会社〇〇等）がされていることを確認した。また、「⑤委託先名の確認方法」は対象読者を想定し、当該読者が契約締結前に確認可能であることを確認した。
		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。	II 4．⑧	適切	「委託先からの書面による申請に基づき、妥当性を考慮し顧問先企業の許諾を得た上で、書面により許諾を回答する」とされており、「妥当性」の具体的な内容が記載されていることを確認した。また、自らが果たすべき安全管理措置と同等の措置が講じられるよう必要かつ適切な監督として、委託先の適切な選定、安全管理措置に関する委託契約の締結、委託先における特定個人情報の取扱状況の把握が含まれることも記載されていることを確認した。
		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。	II 5．②	適切	提供先の 4 件に関して、それぞれ提供先における用途が具体的に記載されている。

審査の観点	主な考慮事項	主な考慮事項（細目）	該当箇所	審査結果	所見
		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。	II 5．移転先 1	該当なし	移転先はない。
		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。	II 6．①	適切	端末設置場所、電子記録媒体保管場所、紙媒体保管場所のそれぞれの態様と立入制限、アクセス制限について具体的に記載している。
		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。	II 6．②	適切	保管期間の記載が不要との誤解が生じないよう、モデル評価書として期間の例（複数ある場合は最も長い期間）が記載されていることを確認した。
		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。	II 6．③	適切	リース機器の返却の際等も廃棄と同様の措置を行う旨が記載されていることを確認した。

賃金計算関係情報ファイル

審査の観点	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。	II 2.③	適切	事務手続きの対象となる顧問先の従業員及び当該従業員の被扶養者を記録するために必要であることが記載されている。
		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。	II 2. ④	適切	識別情報、連絡先等情報、業務関連情報のそれぞれについて保有する理由が記載されている。
		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。	II 3. ①②④	適切	委託契約業務遂行のためとしている。FAX については、使用を推奨するものではないものの、実態としてFAX の取り扱いがあり、記載漏れを防止する意図である旨を確認した。
		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。	II 3. ⑤	適切	特定個人情報の入手の事実、利用目的は委託者である顧問先が本人へ明示していることが記載されている。
		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。	II 3. ⑥	適切	特定個人情報の使用目的として、賃金計算事務が記載されている。
		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。	II 3. ⑧	適切	個人のプライバシー等の権利利益の観点から、不必要な突合を行わない旨が記載されていることを確認した。
		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。	II 3. ⑧	該当なし	統計分析を行わない。
		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。	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。	II 4. ②	適切	委託事項は 3 つあるが、いずれも特定個人情報ファイルの取扱いを委託する理由が具体的に記載されている。また、委託することに関する妥当性に加え、委託する範囲の妥当性についても記載されていることを確認した。
		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。	II 4. ⑤	適切	「モデル評価書」として、具体的な委託先名がわかる記載（株式会社〇〇等）がされていることを確認した。また、「⑤委託先名の確認方法」は対象読者を想定し、当該読者が契約締結前に確認可能であることを確認した。
		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。	II 4. ⑧	適切	「委託先からの書面による申請に基づき、妥当性を考慮し顧問先企業の許諾を得た上で、書面により許諾を回答する」とされており、「妥当性」の具体的な内容が記載されていることを確認した。また、自らが果たすべき安全管理措置と同等の措置が講じられるよう必要かつ適切な監督として、委託先の適切な選定、安全管理措置に関する委託契約の締結、委託先における特定個人情報の取扱状況の把握が含まれることが記載されていることを確認した。
		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。	II 5. 提供先 1	該当なし	提供先はない。

審査の観点	主な考慮事項	主な考慮事項（細目）	該当箇所	審査結果	所見
		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。	II 5．移転先 1	該当なし	移転先はない。
		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。	II 6．①	適切	端末設置場所、電子記録媒体保管場所、紙媒体保管場所のそれぞれの態様と立入制限、アクセス制限について具体的に記載している。
		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。	II 6．②	適切	保管期間の記載が不要との誤解が生じないよう、モデル評価書として期間の例（複数ある場合は最も長い期間）が記載されていることを確認した。
		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。	II 6．③	適切	電子データ、紙媒体に分けて消去する方法が具体的に記載されている。

プロセスにおけるリスク対策

審査の観点	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標に照らし、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。	Ⅲ２．リスク１	適切	「入社連絡票」等により入手根拠となる委託業務及び対象者を明確にし、その対象者のみに係る特定個人情報を顧問先又は従業員本人から入手する方法を用いると共に委託を受ける社会保険労務士が当該連絡票等をチェックすることにより入手時に対象者以外の情報が含まれていないことを確認してい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。	Ⅲ２．リスク１	適切	必要のない情報を記載できない「入社連絡票」を使うことで、顧問先又は従業員本人から必要な情報以外を入手できなくすると共に委託を受ける社会保険労務士が当該連絡票をチェックすることで入手時に必要な情報以外が含まれていないことを確認していること等が具体的に記載されている。
		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。	Ⅲ２．リスク２	適切	顧問先との契約に際して、利用目的の通知と本人確認が確実に励行されていることを確認することにより不適切な方法で入手が行われるリスクを回避していることが具体的に記載されている。
		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。	Ⅲ２．リスク３	適切	顧問先から入手する個人番号は、「個人番号報告書」の様式にて顧問先で本人確認済みであることを確認し、入手している。従業員本人から直接入手する場合は、委託を受ける社会保険労務士がマイナンバーカード又は通知カード及び本人確認資料等の提示を受け、本人確認を行い、個人番号を入手していると記載している。なお、通知カードの使用は実態として存在するため、当面の間記載することを確認した。
		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。	Ⅲ２．リスク３	適切	「個人番号報告書」（又は、「通知カード」、「マイナンバーカード」のコピーの添付）等にて確認出来る手段をとっている。また、通知カードの使用は実態として存在するため、当面の間記載することを確認した。
		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。	Ⅲ２．リスク３	適切	「個人番号報告書」（又は、「通知カード」、「マイナンバーカード」のコピーの添付）等にて確認出来る手段をとっている。また、通知カードの使用は実態として存在するため、当面の間記載することを確認した。
		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。	Ⅲ２．リスク４	適切	入手の手段・方法ごとに特定個人情報が漏えい・紛失するリスク対策が記載されている。
		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。	Ⅲ２．その他のリスク	該当なし	該当なしと記載されている。 課題（別紙参照） モデル評価書として、リスク分析の結果を記載することがわかるような例等を記載することを薦めます。
	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。	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のない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。	Ⅲ３．リスク１	適切	個人番号管理システムへのログイン時の認証による使用者の特定に加えて特定の業務端末だけが特定個人情報ファイルにアクセスすることができるようにアクセス制御していること等が具体的に記載されている。また、個人番号を個人番号管理システムに分離して保存するなどのシステム構成をとることにより、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のない情報と併せて取り扱われないように制御している旨が説明されていることを確認した。

審査の観点	主な考慮事項	主な考慮事項（細目）	該当箇所	審査結果	所見
	記載された対策は、特定個人情報評価の目的に照らし妥当なものか。	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のない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。	Ⅲ３．リスク１	適切	個人番号管理システム以外のシステムにおいても特定個人情報が保存されることから、上記（「宛名システム等における措置の内容」）と同等の対策を講じることが想定される場合は、その内容を記載する旨が説明されていることを確認した。
		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。	Ⅲ3. リスク２	適切	・ユーザＩＤ及びパスワードによる認証を行っている。 ・使用できる端末を特定の業務端末のみに限定している。としている。 課題（別紙参照） ユーザID、パスワード以外の認証方法も普及しつつあることから、その他の方法も検討することを薦めます。
		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。	Ⅲ３．リスク２	適切	職務権限による制限をかけ、ログイン ID とパスワードを発行し、事務取扱担当者のみログインできるように管理をすること、従業者の採用、異動退職時等にユーザ ID の発行、権限の付与及び削除が行われる仕組みとしていること、などが具体的に記載されている。
		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。	Ⅲ3. リスク２	適切	特定個人情報管理責任者が事務取扱責任者に指示してユーザＩＤの発行、権限の付与及び削除を行い、当該内容をアクセス権限管理台帳に記録していること、特定個人情報管理責任者はアクセス権限管理台帳によりユーザIDに関するアクセス制御リストを作成し、業務に対して必要最小限の権限が付与されていることを確認していること、などが具体的に記載されている。
		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、残していなく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。	Ⅲ3. リスク２	適切	・ログインＩＤにより、誰が、いつ、どの端末で、誰の情報を取り扱ったか記録し、その記録は３年間保存している。（保存期間については、１年以上の期間で各事務所にて設定） ・特定個人情報取扱規程に基づき、特定個人情報のアクセスログについて分析・確認をしている。 としている。 また、 １，アクセス失敗時の対応 ２，システム以外の取扱い についても記載されていることを確認した。
		38. 従業者が特定個人情報ファイルを事務外で使用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。	Ⅲ３．リスク３	適切	事務所の職員等に対しては個人情報保護に関する研修で意識啓発を行っていること、システムを使用する際にはログインＩＤ、パスワードが必要であり、ログインＩＤにより、誰が、いつ、どの端末で誰の情報を取り扱ったか分かるよう記録を残し、事務取扱責任者が記録を定期的に確認していること、などが具体的に記載されている。
		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。	Ⅲ３．リスク４	適切	バックアップや外部記憶媒体を用いた役所へのデータ提出のため、特定個人情報ファイルを電子記録媒体に複製する場合やオンプレミスサーバから業務端末にダウンロードする場合の操作ログを取得し、分析・確認をしていることが記載されている。

審査の観点	主な考慮事項	主な考慮事項（細目）	該当箇所	審査結果	所見
		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。	Ⅲ３．その他のリスク	適切	自宅で業務を行う場合、執務室への入室制限等、家族に対するリスクを認識し、事前に同居家族に対するセキュリティ教育（説明等）を行うこと、顧問先に書類等を持参・送付・送信するときは授受記録を残し、肌身離さず携行すること、記録が残る送付手段を利用すること、又は電子データの暗号化・パスワード保護を行うこと等の必要なリスク対策が記載されている。
	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。	Ⅲ４．情報管理体制	適切	委託先を決定する際にプライバシーマークの取得、ISMS 認証取得又は同等の要件を満たすことを確認すること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。	Ⅲ４．閲覧者の制限	適切	委託契約書において保守・管理担当者指名の提出と変更時における報告・更新を義務付けて、特定個人情報ファイルの閲覧者・更新者を制限していること等が具体的に記載されている。
		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。	Ⅲ４．記録	適切	溶解処理の証明書、機器の保守・管理に関する業務完了報告書等の記録を受領することが具体的に記載されている。
		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、特定個人情報評価の目的に照らし、妥当なものか。	Ⅲ4．提供ルール	適切	委託先等から他者への特定個人情報の提供は一切認めないことを契約書上明記して、必要があれば当事務所が現地調査を行うことも可能とすること、遵守の確認を業務報告書及び実施報告書等にて行うことが具体的に記載されている。また、遵守状況の確認を業務報告書等で確認し、必要に応じて現地調査を実施する形での記載順になっていることも確認した。
		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。	Ⅲ４．消去ルール	適切	委託契約時等に、提供資料の返還、 情報の消去、立入検査等を明記した契約を締結して、溶解処理の証明書等の記録を受領して消去されたことを確認すること等が具体的に記載されている。
		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。	Ⅲ４．委託契約書中の規定	適切	委託契約における特定個人情報ファイルの取扱い関する規定が具体的に記載されている。(「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」の「第４－２－(1) 委託の取扱い」で定められた契約条項が記載されている)
		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。	Ⅲ４．再委託	適切	委託契約時に、「再委託」に関するセキュリティ要件を明記した契約を締結し、書面による許諾のない再委託を禁止すると共に委託者である社会保険労務士事務所と最初の委託者である顧問先の許諾を得ること、再委託先においては、委託先と同等の安全管理措置を行うこと、等が具体的に記載されている。
		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記載はあるか。	Ⅲ４．その他のリスク	適切	'クラウドサービス事業者やデータ保管事業者等については、番号法上の「委託」に当たらない場合であっても、委託先として「適切な選定」を実施し、日々の運用状況、再委託の有無等を把握し、必要な監督を実施すると記載されている。

審査の観点	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。	Ⅲ５．リスク１	適切	特定個人情報の提供に関するルールを定め、業務処理簿にて記録をしていることが記載されている。
		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。	Ⅲ５．リスク１	適切	特定個人情報取扱保護規程に定める内容に基づいて、提供を行うこととしている。また、ルールの具体的な内容及び遵守の確認方法が記載されていることを確認した。
		51. 特定個人情報の提供・移転する際に、情報漏えいや紛失のリスク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。	Ⅲ５．リスク２	適切	不適切な方法で提供が行われるリスクについて具体的に記載している。法令に基づく手続きであることから提供先における使途は明白である。利用システムが具体的に記載され、行政機関の定める方法により適切に提供される旨についても記載されていることを確認した。
		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。	Ⅲ５．リスク３	適切	紙媒体、電子記録媒体、通信ネットワーク（e-Govg、gBizID）の提供方法毎に、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措置が具体的に記載されている。
		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。	Ⅲ５．その他のリスク	適切	不適切な方法で提供・移転が行われるリスクと同一の措置が記載されています。不適切な方法で提供・移転が行われるリスク以外に、事務所毎に存在するリスクを記載する旨の説明が記載されていることを確認した。
	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るべき措置を具体的に記載しているか。記載された対策は、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手する際に、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。	Ⅲ６．リスク１	該当なし	―
		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手する際に、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手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。	Ⅲ６．リスク２	該当なし	―
		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。	Ⅲ６．リスク３	該当なし	―
		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手する際に、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、特定個人情報評価の目的に照らし、妥当なものか。	Ⅲ６．リスク４	該当なし	―
		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。	Ⅲ６．リスク５	該当なし	―

審査の観点	主な考慮事項	主な考慮事項（細目）	該当箇所	審査結果	所見
		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。	Ⅲ６．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、特定個人情報評価の目的に照らし、妥当なものか。	Ⅲ６．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。	Ⅲ６．その他のリスク	該当なし	―
	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。	Ⅲ７．リスク1⑤	適切	サーバ設置場所、端末設置場所、電子記録媒体保管場所、紙媒体保管場所のそれぞれについて物理的対策（立入制限、アクセス制限等）が具体的に記載されている。業務環境は様々であることが想定されるが、記載内容が形骸化しないよう、モデル評価書の記載は例であって、実際の業務環境を踏まえた以下の観点のリスク分析を実施して、実際の業務環境に即した内容を記載するよう説明されている。 a 特定個人情報等を取り扱う区域の管理 b 機器及び電子媒体等の盗難等の防止 c 電子媒体等の取扱いにおける漏えい等の防止 d 個人番号の削除、機器及び電子媒体等の廃棄
		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。	Ⅲ７．リスク1⑥	適切	アクセス制御、アクセス者の識別と認証、外部からの不正アクセス等の防止、情報漏えい等の防止等の技術的対策が具体的に記載されている。また、 １、パスワードの定期的な変更が求められるものではないものの、必要に応じて変更する場合があること ２，パスワードは容易に漏えい等が発生しないよう十分な強度を有するものを設定すること ３,「信用のおける事業者」に関して、対象、信用に足りる基準等 ４,「事務所で許可されたソフトウェア以外はダウンロードしていない。」に関して許可する基準等（業務に必要ないものはインストールしないなど、事務所としての対応を記載） ５,「導入したセキュリティ対策ソフトウェア等により、入出力データにおける不正ソフトウェアの有無」に加えて、不正アクセスから保護すること ６,「機器やソフトウェア等に標準装備されている自動更新機能等の活用により、 ソフトウェア等を最新状態としている。」に関し、設置する機器、ソフトウェア等を一覧化し管理すること
		64. 過去３年以内に発生したすべ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。	Ⅲ７．リスク1⑨	該当なし	発生なし。
		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。	Ⅲ７．リスク1⑨	該当なし	発生なし。

審査の観点	主な考慮事項	主な考慮事項（細目）	該当箇所	審査結果	所見
		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。	Ⅲ７．リスク 1⑩	適切	
		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。	Ⅲ７．リスク 2	適切	
		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。	Ⅲ７．リスク 3	適切	期間を経過した情報の削除についてはシステムプログラムを作成して削除処理を行うこと、申請書及び届出書等の紙媒体についてはシュレッダーによる細断もしくは外部業者による溶解処理を行うこと、が記載されている。また、電子記録媒体及び特定個人情報等が記録された機器（サーバやパソコンの HDD 等）を廃棄する際は、復元不可能な手段を採用することが記載されている。加えて、以下の内容についても記載されていることを確認した。 １，システムに保管されている情報を手動で削除することが想定される場合は、定期的に削除すること ２，リース期間が満了した機器等の返却の場合もデータを消去すること ３，消去漏れが生じないよう定期的に確認すること
		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。	Ⅲ７．その他のリスク	適切	消去のリスク対策として、誤って廃棄・消去しないように、務取扱責任者が確認をしてから廃棄・消去の手続きを行うこと、廃棄・消去の際には、いつ、誰が、どのような方法で、何を消去・廃棄したのかを記録し、保存すること、等が具体的に記載されている。 課題（別紙参照） 【外的環境の把握】クラウドサービス事業者やデータ保管事業者等が、データの保管場所としてデータセンターが国外にある場合 ① 顧問先との契約上問題がないか、契約前（業者選定時）に確認している。 ②当該外国の個人情報保護の制度等を把握した上で特定個人情報の安全管理のために必要な措置を講じている。 としていますが、モデル評価書として、データセンターが国外にある場合の記載の有無について検討することを薦めます。（データセンターが国内にあることを記載するなど）

審査の観点	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。		Ⅲ３．	適切	パターンＤ事務所（事務取扱担当者２人以上/特定個人情報ファイルを事務所外で保管）では、事務所職員が複数人いるため固有のリスクとして不正アクセスを想定して、以下の通り対策が具体的に記載されている。 ・クラウドサービスに使用する端末は特定の業務端末に限定する。 ・ユーザ ID とパスワードでユーザを認証し、事務取扱担当者のみがログインできるように管理している。 ・事務取扱責任者がクラウドから特定個人情報のアクセスログをダウンロードし、アクセスログを分析・確認し、その結果を特定個人情報管理責任者に報告する。 ・事務所職員に対しては、データ保護に関する研修を行う。

総　評

・全体的事項

社会保険労務士事務所は、特定個人情報保護評価の実施が義務付けられていないが、顧問先従業員等の特定個人情報ファイルを取扱うことから、その保護の重要性に鑑み、特定個人情報保護評価の枠組みを用いて任意に評価をするものである。この特定個人情報保護評価書は、全国社会保険労務士会連合会が社会保険労務士事務所のモデルを設定して作成した「モデル評価書」であり、社会保険労務士事務所が自社の特定個人情報保護評価を実施するにあたり参考にするものである。本評価書は、社会保険労務士事務所における特定個人情報の取扱い関する水準の確保、関係者からの信頼の確保を目的としている。

この度、前回の評価から 5 年が経過することにより特定個人情報保護評価を再実施しているが、個人情報保護委員会の「特定個人情報保護評価 5 年経過前の評価の再実施に係る留意事項について」において示されているポイントについても本評価書で対応している。

特定個人情報保護評価の対象となる社会保険労務士事務所の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項目について検討し、記載していることを確認した。

・本評価書に固有な事項

本評価書は、パターン D（事務取扱担当者 2 人以上/特定個人情報ファイルを事務所外で保管）のケースであり、事務所職員が複数人いること、また外部のクラウドサービスを使用すること、から固有のリスクとして不正アクセス、不正利用等のリスクを想定して、以下のような対策が記載されていることを確認した。

a)事務取扱担当者、事務取扱責任者を定めて特定個人情報を取扱うことができる者を限定する。(組織的安全管理措置)
b)端末設置場所、執務室、媒体保管庫等の立入制限、アクセス制限（物理的安全管理措置）
c）パソコン及びクラウドサービスを利用するための識別・認証、アクセス制御、アクセスログの分析・確認（技術的安全管理措置）
d)事務所職員に対するデータ保護に関する研修（人的安全管理措置）

・今後の課題について

今後実施が望まれる事項については、別紙「特定個人情報保護評価に関する課題について」参照。

以上