

別紙「特定個人情報保護評価書点検」結果表

1 概要

評価実施機関	全国社会保険労務士会連合会
担当部署	
対象評価書種別	全項目評価
対象事務	<p>社会保険労務士事務</p> <p>評価書番号 1 (事務取扱担当者 1 人/特定個人情報ファイルを事務所内で保管)</p> <p>社会保険労務士事務所 (パターン A 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、個人番号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</p>
授受資料	<p>●評価書</p> <p>1 社会保険労務士事務所・特定個人情報保護モデル評価書 A</p> <p>2 社会保険労務士事務所・特定個人情報保護評価 モデル評価書パターン説明書</p> <p>●ハンドブック (社労士版ガイドライン) 令和 2 年版</p> <p>1 ハンドブック～概要～</p> <p>2 ハンドブック (「本編」)</p> <p>●規程等 (雛形)</p> <p>1 特定個人情報等の適正な取扱いに関する基本方針</p> <p>2 (修正) 特定個人情報取扱規程 (小規模事務所用)</p> <p>4 業務委託契約書</p> <p>5 特定個人情報等の取扱いに関する覚書</p> <p>6 就業規則</p> <p>●様式等 (雛形)</p> <p>1 特定個人情報ファイル管理台帳</p> <p>2 (修正) 特定個人情報保護のための体制図</p> <p>3 情報セキュリティ教育計画書</p> <p>4 情報セキュリティ教育実績一覧 (実施報告書)</p> <p>7 (修正) 特定個人情報・個人情報の取扱いに関する事故等の報告書 (外部用)</p> <p>8 特定個人情報・個人情報保護事件・事故対応報告書 (社内用)</p> <p>9 特定個人情報および個人情報の開示等請求書</p>

評価書番号 : 1

	10 特定個人情報・個人情報問合せ・相談受付票 11 入室管理台帳 12 入室管理台帳（管理区域） 13 退室時確認事項 14 アクセス権限管理台帳 15 個人番号報告書 16 個人番号利用目的通知書 17 業務処理簿 18 入社連絡票 19 異動（変更）連絡票 20 退社連絡票 21 自己点検計画書 22 自己点検報告書
審査実施期間	令和2年9月7日から令和2年10月30日までの間
備考	—

2 点検について

以下の観点で点検を行った。

観点	内容	備考
適合性	提出された特定個人情報保護評価の実施が、特定個人情報保護評価指針に定める実施手続等に適合して行われているか	平成30年5月21日特定個人情報保護委員会事務局「特定個人情報保護評価指針（特定個人情報保護委員会）」の第10「委員会の関与」における「審査の観点」に基づき実施
妥当性	特定個人情報保護評価書に記載されている内容は、この指針に定める特定個人情報保護評価の目的等（本人のプライバシー等権利利益の保護）に照らし妥当と認められるか	

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 A 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	—	—	—	—	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、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当たり参考にするものである。
(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。	—	—	同上
(3) 公表しない部分は適切な範囲か。	—	—	—	適切	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。	—	—	—	適切	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。	—	—	—	—	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。	—	—	—	—	この評価書は、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、実施主体は個々の社会保険労務士事務所である。
(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。	I 1. ②	適切	労働者災害補償保険法に基づく請求に関する事務の内容が追記され、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。	I 2. ②	適切	システム3（賃金計算関係システム）の「②システム」にシステム1及び2と連携する旨が明記された。
		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。	I 2. ③	適切	関係するシステムが全て記載されている。
		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	I 4. ①	適切	顧問先従業員の住所、氏名及び生年月日、個人番号等の情報を取得して、特定個人情報ファイルを

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
		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。			作成して管理することにより必要な事務手続きが発生した際に書類を作成すると事務の流れが具体的に記載されている。
		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。	I 4. ②	適切	手続きに必要な情報を管理することにより、効率的に事務を進めることができるとメリットが具体的に記載されている。
		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。	I (別添1)	適切	指摘後修正で別添1（事務の内容）に労働者災害補償保険法に基づく請求に関する事務の内容と使用するシステムが追記された。これにより社会保険労務士事務所の事務の内容と情報の流れ及びシステムが漏れなく記載された。
(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。	—	—	III, IV	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。また、「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対応している。
(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。	⑨特定個人情報ファイルの取扱いについて自己点検・監査や従業員に対する教育・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。	IV 1. 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。
(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。		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。	IV 1. ②	適切	監査については、2年又は3年に1回外部監査を受審すると記載されている。また、外部監査結果や特定個人情報取扱規程等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。
		72. 特定個人情報を取り扱う従業員等に対する教育・啓発や違反行為をした従業員等に対する措置について具体的に記載しているか。	IV 2	適切	従業員がいないため研修は実施していないが、特定個人情報管理責任者は、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等を受講すると記載されている。
		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。	IV 2. ⑤	該当なし	—
(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。	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扶養親族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	識別情報、連絡先等情報、業務関係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	①公共職業安定所、年金事務所、健康保険組合等から入手する確認通知・決定通知等は、顧問先従業員(被保険者台帳)情報ファイルの社員番号で個人番号情報(特定個人情報)ファイルと紐づいていることから、これらの機関を「行政機関・独立行政法人等」に記載されており適切である。 ②上記の理由により、「その他」の()内にデータストレージサービス、FAX が記載されているが、上記の理由により、e-Gov、gBizID も記載されており適切である。 ④委託契約業務を遂行するためと記載しており適切である。
		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と記載されている。
		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3つを記載している。指摘後修正で3つ目の使用目的（労働者災害補償保険法に基づく請求に関する事務）が追記された。
		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	入手した情報をシステムに入力・登録して、間違っていないか突合すると記載されている。
		14. 特定個人情報を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。
		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	該当なし	—
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	委託先から書面による申請に基づき、妥当性を考慮して顧問先の許諾を得た上で書面により許諾を回答すること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
		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	提供先として労働基準監督署が追加され、提供先は4か所になったが、いずれも提供先における用途が具体的に記載されている。
		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. ②	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	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の態様と立入り制限、アクセス制限について具体的に記載されている。
		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	法定保存期間、委託契約により定められると記載されている。
		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。

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扶養親族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. ①④	適切	①顧問先の従業員等の依頼に応じて労働者災害補償保険法に基づく手続が追加されたことを受けて、本人又は本人の代理人からも個人番号を入手しているため「本人又は本人の代理人」に○印を付けており適切である。 ④委託契約業務を遂行するためと記載しており、適切である。
		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3つを記載している。指摘後修正で3つ目の使用目的（労働者災害補償保険法に基づく請求に関する事務）が追加された。
		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	入手した情報をシステムに入力・登録して、間違っていないか突合することが記載されている。
		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。
		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	該当なし	—
		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	委託事項 1, 2 いずれも委託先から書面による申請に基づき、妥当性を考慮して顧問先の許諾を得た上で書面により許諾を回答することが具体的に記載されている。
		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	提供先として労働基準監督署が追加され、提供先は4か所になったが、いずれも提供先における用途が具体的に記載されている。
		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. ②	該当なし	移転先はない。

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
		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	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の態様と立入り制限、アクセス制限について具体的に記載されている。
		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	法定保存期間、委託契約により定められることが記載されている。
		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。

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。	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扶養親族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	①入手元は「本人又は本人の代理人」としており、適切である。 ②入手方法は、データストレージサービス、FAXとしており、適切である。 ④委託契約業務を遂行するためと記載しており、適切である。
		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	入手した情報をシステムに入力・登録して、間違っていないか突合することが記載されている。
		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。
		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	該当なし	—
		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	委託事項 1, 2 のいずれも委託先から書面による申請に基づき、妥当性を考慮して書面により許諾を回答すると具体的に記載している。また、いずれも顧問先の許諾を得ることが記載されており適切である。
		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	該当なし	提供先はない。
		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. ②	該当なし	移転先はない。

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
		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	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の態様と立入り制限、アクセス制限について具体的に記載されている。
		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	法定保存期間、委託契約により定められることが記載されている。
		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
<p>(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</p> <p>(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。</p>	<p>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。</p>	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。	III 2. 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。	III 2. 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。	III 2. 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。	III 2. 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、入手する。また、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等の提示を受け本人確認を行い、個人番号を入手すると記載されている。また、通知カードの場合は他に本人の写真が掲載されている運転免許証、旅券等の写真付身分証明書を併せて確認する。
		28. 入手した個人番号が本人の個人番号で間違いの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。	III 2. 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等にて個人番号の真正性確認が出来る手段をとっていることが具体的に記載されている。
		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。	III 2. リスク 3	適切	顧問先にて、定期的（年1回程度）に確認が行われ、変更があった場合は「個人番号報告書」にて、変更後の個人番号等を入手出来る手段をとり、また入力誤りを防止するため入力した内容を出力してチェックを行うこと等が具体的に記載されている。
		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。	III 2. 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。また、入手する確認通知や決定通知に個人番号が含まれていなくても、それらを登録した「被保険者台帳情報ファイル」が社員番号をキーにして「個人番号情報ファイル」と結び付いているため、e-Gov、gBizID についても同様の措置を講ずることとしている。
		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。	III 2. その他のリスク	該当なし	該当なしと記載されている。

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
	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、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。	III 3. 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。
		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。	III 3. リスク 1	適切	当該事務に不要な内容は保持していないため必要のない情報との紐付けは行われないことが具体的に記載されている。
		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。	III 3. リスク 2	適切	ユーザID及びパスワードによる認証、6か月に1回パスワード変更を行うこと、使用できる端末を特定の業務端末のみに限定していること等なりすましが行われないために講じている対策が具体的に記載されている。
		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。	III 3. リスク 2	適切	特定個人情報を操作できる担当者は自分1人しかいないため発効・失効の管理は行っていない。
		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。	III 3. リスク 2	適切	同上
		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。	III 3. 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年間保存すると記載されている。また、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・確認し、その結果は特定個人情報管理責任者に報告していると記載されている。
		38. 従業員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。	III 3. リスク 3	適切	従業員が存在しないため、リスクの発生はしないが、家族のリスクを認識し、機器や書類に、容易に使用できない様に、入室制限やアクセス制御等を実施していること等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
		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。	Ⅲ 3. リスク 4	適切	従業者が存在しないが、念のために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等が具体的に記載されている。
		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。	Ⅲ 3. 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。	Ⅲ 4. 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か確認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。	Ⅲ 4. 閲覧者の制限	適切	委託契約書において要員名簿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。	Ⅲ 4. 記録	適切	溶解処理の証明書、マニフェスト、業務完了報告書の記録を受領すること等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。	Ⅲ 4. 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、遵守状況の確認については、業務報告書、実施報告書にて行うこと等が具体的に記載されている。
		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。	Ⅲ 4. 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、マニフェスト、業務完了報告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。

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
		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。	Ⅲ 4. 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に関する規定に「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(1) 委託の取扱い」で定め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。	Ⅲ 4. 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。	Ⅲ 4. その他のリスク	該当なし	該当なしと記載している。
	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。	Ⅲ 5. 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。ルールは、「マイナンバー対応ハンドブック」、「特定個人情報取扱規程」に規定されている。なお、移転はしていない。
		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。	Ⅲ 5. リスク 1	適切	特定個人情報保護規程に基づいて、提供・移転を行うこととしている。
		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用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。	Ⅲ 5. リスク 2	適切	利用システムごとに ID とパスワードによる認証及びアクセス制御を実施し、不適切な方法で特定個人情報がやり取りされることを防止していること、また書類を行政機関等へ提出する際には、書類が外部から見えないように、ファスナー付き鞆等で移動するなどして、安全に移送していること等が具体的に記載されている。なお、提供先は行政機関であり、用途は法令に基づくものであることが明白である。
		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。	Ⅲ 5. 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。	Ⅲ 5. その他のリスク	適切	書類を行政機関等へ提出する際には、書類が外部から見えないようにファスナー付き鞆等で移動すること、肌身離さず携行すること、など安全に移送す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		
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、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う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。	Ⅲ 6. 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。	Ⅲ 6. 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。	Ⅲ 6. 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、特定個人情報保護評価の目的に照らし、妥当なものか。	Ⅲ 6. 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。	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。	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。	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。	Ⅲ 6. 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		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。	Ⅲ 7. 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。

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
	<p>す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。</p>	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。	Ⅲ 7. 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。
		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。	Ⅲ 7. 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。	Ⅲ 7. リスク 1⑨	該当なし	発生なし。
		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。	Ⅲ 7. リスク 1⑩	適切	生存者の情報と同様に、安全管理措置を実施していると記載されている。
		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。	Ⅲ 7. リスク 2	適切	住所や氏名等の変更については届出の都度、新たな情報を上書きし最新の情報で管理していると記載されている。
		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。	Ⅲ 7. 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。
		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。	Ⅲ 7. その他のリスク	適切	自宅兼事務所の場合、家族が間違っ書類を廃棄しないように、執務室内は、整理整頓し、書類を放置しないようにすること等が記載されている。

その他のリスク対策

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	⑨特定個人情報の取扱いについて自己点検・監査や従業員に対する教育・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。	IV 1. 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ことが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、改善することが記載されている。
		71. 評価書に記載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。	IV 1. ②	適切	監査については、2年又は3年に1回外部監査を受審することが記載されている。また、外部監査結果や特定個人情報取扱規程等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、改善することが記載されている。
		72. 特定個人情報を取り扱う従業員等に対する教育・啓発や違反行為をした従業員等に対する措置について具体的に記載しているか。	IV 2.	適切	従業員がいないため研修は実施していないが、特定個人情報管理責任者は、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等を受講することが記載されている。
		その他のリスク対策	IV 3.	適切	「影響範囲の特定」の以下の手順が追記された。 i.被害拡大防止策の検討 ii.事実関係の調査及び原因の究明 iii.影響範囲の特定 iv.再発防止策の検討・実施
		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。	VI 2.	該当なし	—
(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。	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。		III 3.	適切	パターン A 事務所（事務取扱担当者1人）における固有のリスクと対策が以下の通り記載されている。 ・従業員が存在しないため、リスクの発生はしないが、家族のリスクを認識し、機器や書類に、容易に使用できない様に、入室制限やアクセス制御等を実施している。 ・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、事前に家族に対するセキュリティ教育（説明等）を行っている。

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特定個人情報保護評価を実施している。この度、前回の平成 27 年の評価から 5 年が経過するので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。また、平成 28 年 1 月から労災年金の請求にマイナンバーの記載が必要になったことから労働者災害補償保険法に基づく請求に関する事務も評価の対象にした。

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 A（事務取扱担当者 1 人/特定個人情報ファイルを事務所内で保管）のケースであるが、従業者は一人であり、自宅で業務を行う場合は、執務室への入室制限のほか機器や書類が容易に使用できないようにアクセス制限すること、家族に対するセキュリティ教育（説明等）を行うこと、など必要な安全管理措置が記載されていることを確認した。

・特記事項

特に、個人情報として入手し、評価対象の事務の実施において個人番号と結び付き特定個人情報となる場合についても、その個人情報を特定個人情報と同等に取扱うことが求められているので、注意して頂きたい。個人情報保護委員会の「特定個人情報保護評価書 記載要領」の「II 特定個人情報ファイルの概要」「3. 特定個人情報の入手・使用」を確認していただくことをお勧めします。

・今後の課題

本評価書で記載されたリスク対策は、実施が求められるので、「マイナンバー対応ハンドブック」、「特定個人情報取扱規程」等に漏れなく反映され、自己点検でも実施状況を確認する必要がある。別紙「規程類の改定について」に必要な事項を一部記載しているので、参考にして頂きたい。

以上