【新審査基準対応版】 Pマーク内部監査チェックリスト(チェックリストの分類:適合監査)

作 成	作 成
202X.XX.XX	202X.XX.XX
○○	○○

このチェックリストは、有償で編集可能なエクセルファイルにて提供しています。
記入されているものは、一部抜粋したものですが、有償版は、新審査基準に対応したすべての要求事項を網羅しています。
詳細は以下になります。
https://www.iso-mi.com/article/16478276.html

監査実施日:202X.X.XX

ーは非該当もしくは今回の監査では確認しなかった事項。評価結果は適合、不適合、観察事項とします。 ○:適合 △:観察事項 ×:不適合

指針項目		チェック内容		確認結果(運用の証拠)	評価結果(○、△、×)	参照項番	是正計画等
J.1 組織の状況	J.1.1組織及びその状況の理解(4.1)	確認事項	個人情報を取り扱う事業に関して、個人情報保護マネジメントシステムに影響を与えるような外部及び内部の課題を特定しているか。	留意事項には、いくつかの観点から洗い出し、外部・内部の課題を特定することが求められているが、実施していない。	×	J.1.2(4.2) J.1.3(A.3.3.2) J.4.1(7.1)	「個人情報保護マニュアル」に手順を追加し、洗い出しができる様式を作成する。
	J.1.2 利害関係者のニーズ及び期待の理解 (4.2)	確認事項	次の事項を特定しているか。 a)個人情報保護マネジメントシステムに関連する利害関係者 b)その利害関係者の、個人情報保護に関連する要求事項	a)具体的に特定していない b)法令、契約事項を特定	△	J.1.3(A.3.3.2)	a)は上記に関連付けて運用する。
	J.1.3法令、国が定める指針その他の規範 (A.3.3.2)	確認事項	個人情報の取扱いに関する法令、国が定める指針その他の規範(以下、「法令等」という。)を特定し参照する手順を内部規程として文書化しているか。	「個人情報保護マニュアル」にて文書化	○	J.2.4(A.3.1.1) J.4.5.4(A.3.3.5)	―
	J.1.4 個人情報保護マネジメントシステムの適用範囲の決定 (4.3)	確認事項	自らの事業の用に供している全ての個人情報の取扱いを個人情報保護マネジメントシステムの適用範囲として定め、その旨を文書化しているか。	「個人情報保護マニュアル」にて文書化	○	―	―
	J.1.5 個人情報保護マネジメントシステム (4.4)	確認事項	「プライバシーマークにおける個人情報保護マネジメントシステム構築・運用指針」(以下、本指針)に従って、個人情報保護マネジメントシステムを確立し、実施し、維持し、かつ、継続的に改善しているか。	―	―	J.1~J.11	―
J.2 リーダーシップ	J.2.1リーダーシップ及びコミットメント(5.1)	確認事項	社長は、次の事項について統率し、その結果について責任を持つことを明確にしているか。 a)事業者の戦略的な方向性と両立した、個人情報保護方針及び個人情報保護目的を確立する。 b)個人情報保護マネジメントシステムの要求事項を事業者の業務手順に適切に組み入れる。 c)個人情報保護マネジメントシステムに必要な資源を確保する。 d)有効な個人情報保護マネジメント及び個人情報保護マネジメントシステム要求事項への適合の重要性を利害関係者に周知する。 e)個人情報保護マネジメントシステムを適切に運用できるようにする。 f)個人情報保護マネジメントシステムが計画通りに実施できるように、従業者を指揮・支援する。 g)継続的改善を促進する。 h)その他の関連する管理者がその職務領域において、統率力を発揮できるよう、その管理者に割り当てられた役割をサポートする。	「個人情報保護マニュアル」に明確化 a)○ b)○ c)○ d)○ e)○ f)○ g)○ h)○	○	J.1.2(4.2) J.1.5(4.4) J.2.2(5.2.1、5.2.2、A.3.2.1、A.3.2.2)J.2.3.1(5.3) J.3.2(6.2) J.4.1(7.1) J.4.3(7.3、A.3.4.5)J.5.1(8.1、8.2、8.3、A.3.4.1) J.7.2(10.2)	―
	J.2.2個人情報保護方針(5.2.1、5.2.2、A.3.2.1、A.3.2.2)	確認事項	社長は、次の事項を考慮して、個人情報保護方針を策定しているか。 a)事業の目的に対して適切であること。 b)J.3.2で定めた個人情報保護目的を含むか、又は個人情報保護目的の設定のため の枠組みを示すこと。 c)個人情報保護に関連して適用される要求事項を実施すること。d)個人情報保護マネジメントシステムの継続的改善を実施すること。	「個人情報保護方針」に明確化 a)○ b)○ c)○	○	J.1.3(A.3.3.2) J.2.4(A.3.1.1) J.3.2(6.2) J.7.1(10.1、A.3.8) J.7.2(10.2) J.9.2(A.3.4.3.2) J.11.1(A.3.6)	―
		確認事項	個人情報保護方針を文書化した情報には、次の事項を含んでいるか。 a)事業の内容及び規模を考慮した適切な個人情報の取得、利用及び提供に関する こと(目的外利用 を行わないこと及びそのための措置を講じること を含む。) b)個人情報の取扱いに関する法令その他の規範の遵守 c)個人情報の漏えい、滅失又はき損の防止及び是正に関する事項 d)苦情及び相談への対応に関する事項 e)個人情報保護マネジメントシステムの継続的改善に関する事項 f)トップマネジメントの氏名 g)制定年月日及び最終改正年月日 h)個人情報保護方針の内容についての問合せ先	「個人情報保護方針」に明確化 a)○ b)○ c)○ d)○ e)○ f)○ g)○ h)○	○		
		確認事項	社長は、個人情報保護方針を文書化した情報を、事業者内に周知するとともに、一般の人が入手可能な措置を講じているか。	社内掲示や教育実施	○		
J.3 計画	J.3.1.1個人情報の特定(A.3.3.1)	確認事項	自らの事業の用に供している全ての個人情報を特定するための手順を内部規程 として文書化しているか。	「個人情報保護マニュアル」に明確化	○	J.1.4(4.3) J.2.4(A.3.1.1) J.4.5.4(A.3.3.5)	
		確認事項	個人情報を管理するための台帳を整備しているか。	「個人情報管理台帳」確認	○		

指針項目		チェック内容		確認結果（運用の証拠）	評価結果（○、△、×）	参照項番	是正計画等
		確認事項	台帳には、少なくとも次の項目を含んでいるか。 ・個人情報の項目 ・利用目的 ・保管場所 ・保管方法 ・アクセス権を有する者 ・利用期限 ・保管期限	「個人情報管理台帳」に明確化 個人情報の項目 ）○ 利用目的 ）○ 保管場所 ）○ 保管方法 ）○ アクセス権を有する者 ）○ 利用期限 ）○ 保管期限 ）○	○		
		確認事項	台帳の内容は少なくとも年一回、適宜に確認し、最新の状態で維持しているか。	「個人情報管理台帳」確認	○		
	J.3.1.2 リスク及び機会に対処する活動（一般）（6.1.1）	確認事項	個人情報保護マネジメントシステムの計画の策定にあたって、J.1.1で把握した課題及び J.1.2で特定した要求事項を考慮し、次の事項を実現できるよ う個人情報保護リスクアセスメント及び個人情報保護リスク対応を行っているか。 a)事業者が意図した成果を達成できるようなマネジメントシステムの策定 b)望ましくない影響の防止 c)個人情報保護マネジメントシステムの継続的な改善 参照項番	「リスクアセスメント結果表」「リスク対応計画書」確認	○	J.1.1（4.1） J.1.2（4.2）	
		確認事項	個人情報保護マネジメントシステムの計画の策定にあたって、次の事項を含んでいるか。 d)リスクに対する対策の内容 e)d)の対策を個人情報保護マネジメントシステムの手順に含めて実施する方法 f)d)の対策の評価	「個人情報保護マニュアル」に明確化	○		
	J.3.1.3 個人情報保護リスクアセスメント（6.1.2、A.3.3.3）	確認事項	個人情報に関するリスクについて、次の事項を踏まえて、個人情報保護リスクアセスメント（リスクを特定、分析及び評価）をするための手順を定め、かつ実施しているか。手順及び実施した内容については、少なくとも年一回及び必 要に応じて適宜に見直しているか。 a)次の観点を、個人情報保護のリスク基準とする。 1)本指針に定める事項 2)法令及び国が定める指針その他の規範に関する事項 3)個人情報の漏えい、滅失又はき損等に関する事項 b)繰り返し実施した個人情報保護リスクアセスメントに、一貫性及び妥当性があ り、かつ、比較可能な結果を生み出すことを確実にする。 c)個人情報保護リスクを特定する。1)事業者において、事業毎に、個人情報の取扱いを特定する。2)個人情報の取得、保管、利用及び消去等に至る各局面において、適正な保護措 置を講じない場合に想定されるリスクを特定する。3)上記で特定したリスクのリスク所有者を特定する。 d)個人情報保護リスクを分析・評価する。1)c)で特定したリスクと、a)のリスク基準とを比較する。2)リスク対応の優先順位を明らかにする。	「個人情報保護マニュアル」に明確化	○	J.2.4（A.3.1.1） J.3.1.1（A.3.3.1） J.3.1.2（6.1.1） J.4.5.4（A.3.3.5）	
		確認事項	個人情報保護のリスクを特定、分析及び評価をするための手順を内部 規程として文書化しているか。	「個人情報保護マニュアル」に明確化	○		
	J.3.1.4 個人情報保護リスク対応（6.1.3、A.3.3.3）	確認事項	次の事項について、個人情報保護リスクへの対応手順を内部規程とし て文書化し、かつ実施しているか。手順及び実施した内容については、適宜見直しているか。 a)個人情報保護リスクへの対応にあたっては、個人情報保護リスクアセスメントの結果を考慮して、必要な対応策（本指針及び事業者が必要であると決定した、個人情報保護に関するリスクを修正する対策を含む。）を策定すること。 b)a)を踏まえて、個人情報保護リスクへの対応計画を策定し、実施すること。 c)個人情報保護リスクへの対応計画及び実施した内容（現状で実施し得る対策を講じた上で、未対応部分を残留リスクとして把握し、管理することを含む。）について、原則として、社長の承認を得ること。	「個人情報保護マニュアル」に明確化	○	J.2.4（A.3.1.1） J.3.1.1（A.3.3.1） J.3.1.2（6.1.1） J.3.1.3（6.1.2、A.3.3.3） J.4.5.4（A.3.3.5）	
		確認事項	a)～c)を実施した記録を保持すること。	「リスクアセスメント結果表」確認	○		
	J.3.2 個人情報保護目的及びそれを達成するための計画策定（6.2）	確認事項	次の事項を含めて、個人情報保護目的を達成するために計画しているか。 a)実施事項 b)必要な資源 c)責任者 d)達成期限 e)結果の評価方法	「情報セキュリティ目標管理表」に明確化	○	J.4.1（7.1）	
	J.3.3計画策定（A.3.3.6）	確認事項	個人情報保護マネジメントシステムを確実に実施するために、次の事項を含めて、少なくとも年一回及び必要に応じて適宜に必要な計画を立案し、文書化しているか。 a)教育実施計画 b)内部監査実施計画	「教育訓練計画書」「内部監査実施計画書」確認	○	J.2.4（A.3.1.1） J.3.2（6.2） J.4.3（7.3、A.3.4.5）J.6.2（9.2、A.3.7.2）	
J.7 改善	J.7.1不適合及び是正処置（10.1、A.3.8）	確認事項	次の事項を含めて、不適合に対する是正処置を実施するための責任及 び権限を定める手順を内部規程として文書化しているか。 a)その不適合に対処し、該当する場合には、必ず、次の事項を行う。 1)その不適合を管理し、修正するための処置をとる。2)その不適合によって起こった結果に対処する。 b)次の事項によって、その不適合の原因を除去するための処置を検討する。1)その不適合を調査及び分析する。2)その不適合の原因を特定する。3)類似の不適合の有無、又はそれが発生する可能性を検討する。 c)是正処置を計画し、計画された処置を実施する。 d)実施された全ての是正処置の有効性を調査、分析及び評価する。 e)必要な場合には、個人情報保護マネジメントシステムの改善を行う。	「個人情報保護マニュアル」に明確化	○	J.2.4（A.3.1.1） J.3.1.3（6.1.2、A.3.3.3） J.3.1.4（6.1.3、A.3.3.3） J.4.4.2（A.3.3.7） J.4.5.4（A.3.3.5） J.6.1（9.1、A.3.7.1） J.6.2（9.2、A.3.7.2） J.6.3（9.3、A.3.7.3） J.11.1	

指針項目		チェック内容		確認結果（運用の証拠）	評価結果（○、△、×）	参照項番	是正計画等
		確認事項	不適合が明らかとなった場合、上記の事項を実施しているか。	「是正処置報告書」確認	○	(A.3.6)	
		確認事項	上記の実施結果について、文書化した情報を保持（保管）するとともに、原則として、社長が承認しているか。	「是正処置報告書」確認	○		
	J.7.2継続的改善（10.2）	確認事項	個人情報保護マネジメントシステムの適切性、妥当性及び有効性を継続的に改善しているか。	「Pマーク推進委員会議事録」確認	○	J.7.1（10.1、A.3.8）	
J.8 取得、利用及び提供に関する原則	J.8.1利用目的の特定（A.3.4.2.1）	確認事項	個人情報の利用目的をできる限り特定し、その目的の達成に必要な範囲内において取扱いを行っているか。	自社ホームページ及び「個人情報の取扱いに関する同意書」確認	○	J.2.4（A.3.1.1） J.3.1.1（A.3.3.1） J.4.5.4（A.3.3.5）	
		確認事項	利用目的は、取得した情報の利用及び提供によって本人の受ける影響を予測できるように、利用及び提供の範囲を可能な限り具体的に明らかにしているか。	○○における個人情報取扱い業務の実態確認	○		
	J.8.2適正な取得（A.3.4.2.2）	確認事項	適法かつ公正な手段によって個人情報を取得しているか。	○○における個人情報取扱い業務の実態確認	○	J.2.4（A.3.1.1） J.4.5.4（A.3.3.5）	
	J.8.3要配慮個人情報（A.3.4.2.3）	確認事項	新たに要配慮個人情報を取得、利用又は提供並びに要配慮個人情報のデータを 提供する場合、あらかじめ書面による本人の同意を得ているか。	「個人情報の取扱いに関する同意書」確認	○	J.2.4（A.3.1.1） J.4.5.4（A.3.3.5）	
		確認事項	要配慮個人情報を取得、利用する際、書面による本人の同意を得ることを要しな いときとは、以下の場合に限定しているか。 a)法令に基づく場合 b)人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意 を得ることが困難であるとき c)公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合で あって、本人の同意を得ることが困難であるとき d)国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務 を遂行することに対して協力する必要がある場合であって、本人の同意を得る ことによって当該事務の遂行に支障を及ぼすおそれがあるとき e)当該要配慮個人情報が、法令等により個人情報取扱事業者の義務などの適用除 外とされている者及び個人情報保護委員会規則で定めた者によって公開され た要配慮個人情報であるとき f)本人を目視し、又は撮影することにより、その外形上明らかな要配慮個人情 報を取得又は利用する場合 g)個人情報保護法二十七条第五項各号に掲げる場合において、個人データである 要配慮個人情報の提供を受けるとき h)個人情報取扱事業者が学術研究機関等である場合であって、当該要配慮個人情 報を学術研究目的で取り扱う必要があるとき（当該要配慮個人情報を取り扱う 目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。） i)学術研究機関等から当該要配慮個人情報を取得し、利用する場合であって、当 該要配慮個人情報を学術研究目的で取得し、利用する必要があるとき（当該要 配慮個人情報を取得する目的の一部が学術研究目的である場合を含み、個人の 権利利益を不当に侵害するおそれがある場合を除く。）（当該個人情報取扱事 業者と当該学術研究機関等が共同して学術研究を行う場合に限る。）	健康診断に関係する個人情報取扱いの実態確認	○		
		確認事項	要配慮個人情報を提供する際、書面による本人の同意を得ることを要しないときとは、J.8.3のa)～d)、又は、以下の場合に限定しているか。 j)個人情報取扱事業者が学術研究機関等である場合であって、個人データの提供 が学術研究の成果の公表又は教授のためやむを得ないとき（個人の権利利益 を不当に侵害するおそれがある場合を除く。） k)個人情報取扱事業者が学術研究機関等である場合であって、個人データを学術 研究目的で提供する必要があるとき（個人データを提供する目的の一部が学 術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがあ る場合を除く。）（個人情報取扱事業者と第三者が共同して学術研究を行う場 合に限る。） l)第三者が学術研究機関等である場合であって、第三者が個人データを学術研究目的で取り扱う必要があるとき（個人データを取り扱う目的の一部が学術研 究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場 合を除く。）	健康診断に関係する個人情報取扱いの実態確認	○		
	J.8.8個人データの提供に関する措置（A.3.4.2.8）	確認事項	個人データを第三者に提供する場合には、あらかじめ、本人に対して、当該個人 データを第三者に提供することに関して、J.8.5のa)～d)に示す事項又はそれと 同等以上の内容の事項、及び取得方法を通知し、本人の同意を得ているか。	「個人情報の取扱いに関する同意書」確認	○	J.2.4（A.3.1.1） J.4.5.4（A.3.3.5）	

指針項目		チェック内容		確認結果 （運用の証拠）	評価結果 （○、△、×）	参照項番	是正計画等
		確認事項	個人データを第三者に提供する場合に、本人に通知し、本人の同意を得ることを要しない場合は、以下の場合に限定しているか。 a)J.8.5の規定によって、個人データを第三者に提供することに関して、既に J.8.5のa)～d)の事項又はそれと同等以上の内容の事項を本人に明示し、本人の同意を得ているとき、またはJ.8.7の規定によって、既に J.8.5のa)～d)の 事項又はそれと同等以上の内容の事項を本人に通知し、本人の同意を得ているとき b)本人の同意を得ることが困難な場合であって、法令等が定める手続に基づいた 上で、次に示す事項又はそれと同等以上の内容の事項を、あらかじめ、本人に通知し、又はそれに代わる同等の措置を講じているとき 1)事業者の氏名又は名称及び住所並びに法人あっては、その代表者の氏名 2)第三者への提供を利用目的とすること 3)第三者に提供される個人データの項目 4)第三者への提供の手段又は方法 5)本人の請求などに応じて当該本人が識別される個人データの第三者への提供を停止すること 6)取得方法 7)本人からの請求などを受け付ける方法 8)その他個人の権利利益を保護するために必要なものとして個人情報保護委 員会規則で定める事項 c)法人その他の団体に関する情報に含まれる当該法人その他の団体の役員及び株主に関する情報であって、かつ、本人又は当該法人その他の団体自らによって公開又は公表された情報を提供する場合であって、法令等が定める手続に基 づいた上で、b)の1)～8)で示す事項又はそれと同等以上の内容の事項を、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき d)特定した利用目的の達成に必要な範囲内において、個人データの取扱いの全部 又は一部を委託するとき e)合併その他の事由による事業の承継に伴って個人データを提供する場合であ って、承継前の利用目的の範囲内で当該個人データを取り扱うとき f)個人データを共同利用している場合であって、共同して利用する者の間で、J.8.7に規定する共同利用について契約によって定めているとき g)J.8.3のa)～d)、又は、J.8.3の j)～l)のいずれかに該当する場合	記載以外の事例はなかった。	○		
		確認事項	上記b)の適用にあたっては、以下の1)～3)を除いているか。 1)要配慮個人情報 2)偽りその他不正の手段により取得された個人データ 3)個人情報保護法二十七条第二項、又は 上記b)により提供された個人 データ（提供されたデータに対して、その全部又は一部を複製し、又は加工 したものを含む）	b)に該当する事案はなかった。	○		
J.8.8.1外国にある第三者への提供の制限（A.3.4.2.8.1）		確認事項	外国にある第三者に個人データを提供する場合、以下のいずれかを満たしているか。ただし、J.8.3のa)～d)、又は、J.8.3の j)～l)のいずれかに該当する場合はこれに限らない。 a)あらかじめ外国にある第三者への提供を認める旨の本人の同意がある場合 b)個人データの取扱いについて個人情報取扱事業者が講ずべきこととされている措置に相当する措置を継続的に講ずるために必要なものとして個人情報保 護委員会規則で定める基準に適合する体制を整備している者への提供をする 場合 c)個人の権利利益を保護する上で我が国と同等の水準にある外国として個人情報保護委員会規則で定める国・地域にある第三者への提供をする場合	該当なし	○	J.4.5.4（A.3.3.5） J.8.8（A.3.4.2.8）	
		確認事項	上記の a)によって外国にある第三者に個人データを提供する場合は、あらかじめ、法令等の定めるところによって、次に掲げる事項について、当該本人に必要な情報を提供しているか。 d)当該外国の名称 e)当該外国における個人情報の保護に関する制度に関する情報 f)当該第三者が講ずる個人情報の保護のための措置に関する情報 g)d)～f)に定める事項が特定できない場合、その旨及びその理由 h)g)に該当する場合であって、d)～f)の事項に代わる本人に参考となるべき情報 がある場合には、当該情報 i)g)及びh)に該当する場合について情報提供できない場合には、g)及びh)に定め る事項に代えて、その旨及びその理由	該当なし	○		
		確認事項	上記の b)によって外国にある第三者に個人データを提供する場合には、あらかじめ、法令等の定めるところによって、次に掲げる事項について、必要な措置を講じているか。 j)当該第三者による相当措置の実施状況並びに相当措置の実施に影響を及ぼすおそれのある当該外国の制度の有無及びその内容について、適切かつ合理的な方法による定期的な確認 k)当該第三者による相当措置の実施に支障が生じたときは、必要かつ適切な措置 を講ずるとともに、当該相当措置の継続的な実施の確保が困難となったときは、個人データの当該第三者への提供の停止 l)本人の求めを受けた場合には、情報提供することにより当該組織の業務の適正な実施に著しい支障を及ぼすおそれがある場合を除き、遅滞なく、以下の情報の提供 1)当該第三者による体制の整備の方法 2)当該第三者が実施する相当措置の概要 3)j)による確認の頻度及び方法 4)当該外国の名称 5)当該第三者による相当措置の実施に影響を及ぼすおそれのある当該外国の制度の有無及びその概要 6)当該第三者による相当措置の実施に関する支障の有無及びその概要 7)前号の支障に関して、k)により講ずる措置の概要	該当なし	○		
		確認事項	上記のl)で、本人の求めに係る情報の全部又は一部について提供しない旨の決定をしたときは、本人に対して、遅滞なく、その旨を通知するとともに、その理由を説明できるか。	該当なし	○		

指針項目	チェック内容		確認結果（運用の証拠）	評価結果（○、△、×）	参照項番	是正計画等
J.8.8.2 第三者提供に係る記録の作成など（A.3.4.2.8.2）	確認事項	個人データを第三者に提供したときは、当該個人データの提供について必要な記録を作成しているか。	実績はなかった。	○	J.4.5.2（7.5.3） J.4.5.3（7.5.2、A.3.5.2） J.4.5.4（A.3.3.5） J.4.5.5（A.3.5.3） J.8.8（A.3.4.2.8）	
	確認事項	個人データを第三者に提供したときに、当該個人データの提供に関する記録の作成を要しない場合を、以下の場合に限定しているか。 a)特定した利用目的の達成に必要な範囲内において、個人データの取扱いの全部又は一部を委託するとき b)合併その他の事由による事業の承継に伴って個人データを提供する場合であって、承継前の利用目的の範囲内で当該個人データを取り扱うとき c)個人データを共同利用している場合であって、共同して利用する者の間で、J.8.7に規定する共同利用について契約によって定めているとき d)法令に基づく場合 e)人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき f)公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき g)国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることによって当該事務の遂行に支障を及ぼすおそれがあるとき h)個人情報取扱事業者が学術研究機関等である場合であって、個人データの提供が学術研究の成果の公表又は教授のためやむを得ないとき（個人の権利利益を不当に侵害するおそれがある場合を除く。） i)個人情報取扱事業者が学術研究機関等である場合であって、個人データを学術研究目的で提供する必要があるとき（個人データを提供する目的の一部が学術 研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場 合を除く。）（個人情報取扱事業者と第三者が共同して学術研究を行う場合に限 る。） j)第三者が学術研究機関等である場合であって、第三者が個人データを学術研究 目的で取り扱う必要があるとき（個人データを取り扱う	実績はなかった。	○		
	確認事項	個人データを第三者に提供したことに関する記録を作成した場合、当該記録を必要な期間保管しているか。	実績はなかった。	○		
	確認事項	個人データを提供したときに、提供先が実施する第三者提供を受ける際の確認等に対し、適切に応じているか。	実績はなかった。	○		
J.8.8.3 第三者提供を受ける際の確認など（A.3.4.2.8.3）	確認事項	第三者から個人データの提供を受けるに際しては、必要な確認を行っているか。	実績はなかった。	○	J.4.5.2（7.5.3） J.4.5.3（7.5.2、A.3.5.2） J.4.5.4（A.3.3.5） J.4.5.5（A.3.5.3） J.8.4（A.3.4.2.4）	
	確認事項	第三者から個人データの提供を受けるに際して、確認を要しないのは、以下の場合に限定しているか。 a)特定した利用目的の達成に必要な範囲内において、個人データの取扱いの全部 又は一部を委託されたとき b)合併その他の事由による事業の承継に伴って個人データを提供される場合で あって、承継前の利用目的の範囲内で当該個人データを取り扱うとき c)個人データを共同利用している場合であって、共同して利用する者の間で、J.8.7に規定する共同利用について契約によって定めているとき d)法令に基づく場合 e)人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意 を得ることが困難であるとき f)公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合で あって、本人の同意を得ることが困難であるとき g)国の機関若しく は地方公共団体又はその委託を受けた者が法令の定める事務 を遂行することに対して協力する必要がある場合であって、本人の同意を得る ことによって当該事務の遂行に支障を及ぼすおそれがあるとき h)個人情報取扱事業者が学術研究機関等である場合であって、個人データの提供 が学術研究の成果の公表又は教授のためやむを得ないとき（個人の権利利益を 不当に侵害するおそれがある場合を除く。） i)個人情報取扱事業者が学術研究機関等である場合であって、個人データを学術 研究目的で提供する必要があるとき（個人データを提供する目的の一部が学術 研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場 合を除く。）（個人情報取扱事業者と第三者が共同して学術研究を行う場合に限 る。） j)第三者が学術研究機関等である場合であって、第三者が個人データを学術研究 目的で取り扱う必要があるとき（個人データを取り扱う目的の一部が学術研究 目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を 除く。）	実績はなかった。	○		
	確認事項	第三者から個人データの提供を受けるに際して確認を行ったときは、必要な記録を作成しているか。	実績はなかった。	○		
	確認事項	第三者から個人データの提供を受けるに際して確認を行った記録は、必要な期間保存しているか。	実績はなかった。	○		
J.8.9匿名加工情報（A.3.4.2.9）	確認事項	匿名加工情報の取扱いを行うか否かの方針を定めているか。	匿名加工情報は取り扱わない	○	J.2.4（A.3.1.1） J.4.5.4（A.3.3.5）	
	確認事項	匿名加工情報を取り扱う場合には、法令等の定めるところによって、以下の事項に関する適切な取扱いを行う手順を内部規程として文書化しているか。 a)適切な加工方法の決定、及び加工の実施 b)加工方法等情報の安全管理措置 c)匿名加工情報を作成、及び提供することに関する公表 d)匿名加工情報の取扱いにおいて識別行為を防止する措置 e)匿名加工情報の安全管理、苦情処理、その他の適正な取扱いのための措置、及び当該措置の公表	匿名加工情報は取り扱わない	○		
	確認事項	匿名加工情報を取り扱う場合には、定めた手順に従っているか。	匿名加工情報は取り扱わない	○		
J.8.10 仮名加工情報	確認事項	仮名加工情報を取り扱う場合には、法令等の定めるところによって、適切な取扱いを行う手順を内部規程として文書化しているか。	仮名加工情報は取り扱わない	○	J.2.4（A.3.1.1） J.4.4.2（A.3.3.7） J.4.5.4（A.3.3.5）	

指針項目		チェック内容		確認結果 （運用の証拠）	評価結果 （○、△、×）	参照項番	是正計画等
		確認事項	仮名加工情報を作成する場合には、他の情報と照合しない限り 特定の個人を識 別することができないようにするために必要なものとして、個人情報保護委員会規則で定める基準に従い、 個人情報を加工しているか。	仮名加工情報は取り扱わない	○	J.8.5（A.3.4.2.5） J.9.4（A.3.4.3.4）	
		確認事項	仮名加工情報を作成したとき、又は仮名加工情報及び当該仮名加工情報に係る削除情報等を取得したときは、削除情報等の漏えいを防止するために必要なも のとして個人情報保護委員会規則で定める基準に従い、削除情報等の安全管理のための措置を講じているか。	仮名加工情報は取り扱わない	○		
		確認事項	仮名加工情報を利用する場合には、以下を実施しているか。 a)利用目的をできる限り特定し、法令に基づく場合を除くほか、その目的の達成 に必要な範囲内において行うこと b)あらかじめその利用目的を公表している場合及び法令に基づく場合を除き、速やかに、その利用目的を公表すること c)仮名加工情報を取り扱うに当たっては、当該仮名加工情報の作成に用いられた 個人情報に係る本人を識別するために、当該仮名加工情報を他の情報と照合し ないこと d)電話をかけ、郵便若しくは信書便により送付し、電報を送達し、FAX若しくは電子メールを用いて送信し、又は住居を訪問するために、当該仮名加工情報に含まれる連絡先その他の情報を利用しないこと	仮名加工情報は取り扱わない	○		
		確認事項	仮名加工情報を提供する場合には、以下の場合を除き、仮名加工情報である個人 データを第三者に提供していないか。 e)仮名加工情報の取扱いの全部又は一部を、J.9.4と同等の措置を講じたうえで 委託する場合 f)仮名加工情報が特定の者との間で共同して利用され、 共同して利用する者が、既に共同して利用する場合（J.8.5のa)～f)に示す事項又はそれと同等以上の 内容の事項を明示又は通知し、本人の同意を得ている場合であって、以下の1) ～6)に示す事項又はそれと同等以上の内容の事項を、あらかじめ、本人に通知 し、又は本人が容易に知り得る状態に置く場合） 1)共同して利用すること 2)共同して利用される仮名加工情報の項目 3)共同して利用する者の範囲 4)共同して利用する者の利用目的 5)共同して利用する仮名加工情報の管理について責任を有する者の氏名又は 名称及び住所並びに法人にあっては、その代表者の氏名 6)取得方法 g)合併その他の事由による事業の継承に伴って仮名加工情報を提供する場合 h)法令に基づく場合	仮名加工情報は取り扱わない	○		
		確認事項	仮名加工情報の取扱いに関する苦情の適切かつ迅速な対応を行っているか。	仮名加工情報は取り扱わない	○		
		確認事項	仮名加工情報である個人データ及び削除情報等を利用する必要がなくなったときは、当該個人データ及び削除情報等を遅滞なく消去しているか。	仮名加工情報は取り扱わない	○		
J.11 苦情及び相談への対応	J.11.1苦情及び相談への対応（A.3.6）	確認事項	個人情報の取扱い及び個人情報保護マネジメントシステムに関して、本人からの苦情及び相談を受け付けて、適切かつ迅速な対応を行う手順が内部規程とし て文書化しているか。	「個人情報取扱い規定」に明確化	○	J.2.4（A.3.1.1） J.4.4.1（7.4） J.4.5.4（A.3.3.5） J.10.3 （A.3.4.4.3）	
		確認事項	苦情及び相談への対応を実施しているか。	実績はなかった。	○		
		確認事項	苦情の申立て先を、本人にとって明確にしているか。	実績はなかった。	○		
		確認事項	認定個人情報保護団体の対象事業者となっている場合は、当該団体の苦情解決の申し出先も明示しているか。	自社ホームページに明確化	○		
		確認事項	本人からの苦情及び相談を受け付けて、適切かつ迅速な対応を行うための体制を整備しているか。	自社ホームページで体制を明示していた。	○		

【新審査基準対応版】 Pマーク内部監査チェックリスト(チェックリストの分類:運用監査)

作 成	作 成
202X.XX.XX	202X.XX.XX
○○	○○

このチェックリストは、有償で編集可能なエクセルファイルにて提供しています。
記入されているものは、一部抜粋したものですが、有償版は、新審査基準に対応したすべての要求事項を網羅しています。
詳細は以下になります。
https://www.iso-mi.com/article/16478276.html

監査実施日:202X.X.XX
対象部門:管理部門
ーは非該当もしくは今回の監査では確認しなかった事項。評価結果は適合、不適合、観察事項とします。 ○:適合 △:観察事項 ×:不適合

監査項目 (対応する文書)		チェック内容		確認結果 (運用の証拠)	評価結果 (○、△、×)	備考	是正計画等
個人情報保護マニュアル J.2.3.1 安全管理規定 Ⅰ	組織の役割、責任及び権限	確認事項	「個人情報保護マニュアル」で定められた手順に従って、資源、役割、責任及び権限が明確化されているか? 手順:社長は、個人情報保護を行うための必要な経営資源を提供し、その提供資源の評価及び決定については、経営会議やマネジメントレビューにより行う (具体的なチェック事項) ・「安全管理規定」において明確化された、役割、責任及び権限は周知されているか? ・役割、責任は自覚しているか? ・運用状況を報告しているか?	「組織図」にて明確化され、社内への周知も行われていた。Pマーク推進委員会で運用状況は報告されていた。	○	―	―
個人情報保護マニュアル J.8.1 個人情報取扱い規定 Ⅱ	利用目的の特定	確認事項	「個人情報保護マニュアル」および「個人情報取扱い規定」で定められた以下の手順に従って行われているか? 手順①:個人情報の取得担当者は、書面によって、利用目的の明示を行う 手順②:各部門における責任者は、自部門の社員が収集する個人情報の使用目的と必要な限度であるかを適切に判断し、管理する 手順③:個人情報の取得担当者は、個人情報の収集を行う前に、利用目的を書面もしくはこれに代わる方法によって本人に通知し、同意を得る (具体的なチェック事項) ・各種利用目的が明示されているものの確認 ・利用目的は適切か? ・可能な限り具体化されているか? ・利用目的の承認は適切か?	自社WEBサイトでの利用目的および「個人情報取扱いに関する同意書」での利用目的を確認。さらに具体化されていた。	○	―	―
個人情報保護マニュアル J.8.2 個人情報取扱い規定 Ⅱ	適正な取得	確認事項	「個人情報保護マニュアル」及び「個人情報取扱い規定」で定められた手順に従って、適正な取得がされているか? 手順:個人情報の取得担当者は、取得をする際に、事前に、同意書面を取って取得する。 (具体的なチェック事項) ・適法かつ公正な手段によって取得しているか? ・本人同意に漏れや抜けはないか? ・提供元又は委託元が適正に行っていることは確認できているか?	個人情報取得におけるクレームはなく、同意漏れもなかった。	○	―	―
個人情報保護マニュアル J.8.3 個人情報取扱い規定 Ⅱ	要配慮個人情報	確認事項	「個人情報保護マニュアル」及び「個人情報取扱い規定」で定められた手順に従って行われているか? 手順:原則、健康診断等、法令で取得が認められているもの以外で、要配慮個人情報は取得しない。 (具体的なチェック事項) ・具体的にどんな要配慮個人情報があるか? ・例外的に要配慮個人情報を取得したものはあるか? ・法令以外に要配慮個人情報を第三者に提供していないか?	健康診断等、法令で取得が認められているもの以外で、要配慮個人情報は取得していなかった。	○	LGBTに関する事項は、個人情報保護委員会によると、要配慮個人情報に該当しないが、法令に定める病歴、障害、診療情報が含まれる場合は、要配慮個人情報に該当する可能性がある。	―
個人情報保護マニュアル J.8.4、J.8.5 個人情報取扱い規定 Ⅱ	個人情報を取得した場合の措置(個人情報の通知)	確認事項	「個人情報保護マニュアル」及び「個人情報取扱い規定」で定められた手順に従って、適正な通知がされているか? 手順①個人情報の取得担当者は、本人との同意を確実にする。同意不要の例外事項については、個人情報管理責任者の承認を得る 手順②個人情報を直接書面以外の方法によって取得した場合、個人情報の取得担当者は、その利用目的をWEB等で公表している場合を除き、直接本人に対して利用目的の通知を行う (具体的なチェック事項) ・通知の方法は適切か ・本人からの同意の署名やその記録はあるか? ・同意不要の例外事項はあるか? ・「個人情報の取り扱いに関する同意書」の項目等は適切か?	自社WEBサイトでの通知事項および「個人情報取扱いに関する同意書」を確認。	○	―	―
個人情報保護マニュアル J.8.6 個人情報取扱い規定 Ⅲ	利用に関する措置	確認事項	「個人情報保護マニュアル」及び「個人情報取扱い規定」で定められた手順に従って、適正な利用がされているか? 手順①利用部門は、個人情報の“目的外利用”を防ぐため、利用目的以外の利用をしてはならない 手順②利用部門以外の部門は、個人情報の利用をしてはならない 手順③利用目的を変更する場合には、個人情報の取扱い担当者は、変更理由を明記し、個人情報管理責任者の承認を得なければならない。承認後、個人情報の取扱い担当者は、本人への通知およびその同意を確実に行う 手順④個人情報の取扱い担当者は、目的外利用に該当するか判断に迷う場合は、自ら判断せず、個人情報管理責任者の判断を仰ぐ (具体的なチェック事項) ・違法又は不当な行為を助長し、又は誘発する恐れはないか? ・目的外利用はないか? ・利用部門以外の利用はないか?	目的外利用や利用部門以外での利用がないかどうかは、Pマーク推進委員会で確認していた。また、暴力団員等により行われる暴力的要求行為に利用されたり、本人に対して差別的な利用を行うこともなかった。	○	―	―

個人情報保護マニュアル J.8.7 個人情報取扱い規定 Ⅲ.5	本人に連絡又は接触する場合の措置	確認事項	「個人情報保護マニュアル」及び「個人情報取扱い規定」で定められた手順に従って、適正な連絡又は接触がされているか？ 手順：該当部門の担当者は、同意が取れているかどうかを確認して、業務開始初回時に「個人情報利用・アクセス承認申請書」を記載し、個人情報管理責任者の承認を得て、アクセスを行う。 （具体的なチェック事項） ・連絡又は接触する方法は適切か？ ・誰が、いつ行っているか？ ・トラブル事例はあるか？	手順に基づき実施され、トラブル事例もなかった。	○		
個人情報保護マニュアル J.8.8 個人情報取扱い規定 Ⅳ	個人データの提供に関する措置	確認事項	「個人情報保護マニュアル」及び「個人情報取扱い規定」で定められた手順に従って、適正な提供（委託する場合も含める）がされているか？ 手順①提供（委託）部門は、提供（委託）の事前の本人同意の確認をする 手順②第三者に提供する場合、「個人情報の提供に関する申請書（第三者提供）」に記入し、上長の承認を得る 手順③担当者は、本人への通知が必要な場合、書面によって行う （具体的なチェック事項） ・給与計算・労務処理の委託は適切か？ ・提供（委託）目的以外の提供（委託）は行っていないか？	給与計算の委託は、社労士事務所に委託しており、目的以外での個人情報の提供はなかった。	○		
個人情報保護マニュアル J.9.1	正確性の確保	確認事項	「個人情報保護マニュアル」で定められた手順に従って、個人情報の正確性の確保がされているか？ 手順①担当者は、誤入力のチェック（再確認）を行い、正確性を保つ 手順②個人データを利用する必要がなくなったときには、該当部門長の承認を得て、当該個人データを遅滞なく消去する 手順③個人データの保存期間は、「個人情報管理台帳」に明記し、正確性が確保されているかどうかの検証は、Pマーク推進委員会にて行う	誤入力があっても、部門内で確認していた。また、直接入力しないなど、誤入力の防止に努めていた。	○		
個人情報保護マニュアル J.9.2 安全管理規定 Ⅲ	安全管理措置	確認事項	「個人情報保護マニュアル」及び「安全管理規定」で定められた手順に従って、安全管理措置が適切にされているか？ 手順①：個人情報に関するリスクに応じて、合理的な安全対策を講じる 手順②：現場は、「日常点検チェックリスト」等に基づき実施する （具体的なチェック事項） 1.人的安全管理事項 ●すべての雇用者と秘密保持誓約書を結んでいるか？ ●個人の机及びキャビネット内がキチンと整理・整頓され、退出時には、機密情報が出しっぱなしになっていないか？ ●「入退出管理台帳」への記入が徹底されているか？	「日常点検チェックリスト」「入退出管理台帳」確認	○		
		確認事項	2.物理的事項 ●パソコン起動時及び離席時には、パスワードロック対策が全てのパソコンにできているか？ ●記録メディア及び機密書類はかぎ付キャビネットに保管されているか？ ●個人データは、指定するサーバーのホルダーに保管されているか？ ●貸与されたスマートフォンの画面ロックは行っているか？ ●紙やデータは、廃棄（削除）のルールに基づき、実施されているか？ ●機器・記録メディア・書類の持ち込み・持ち出しについてやむを得ず持ち出す場合、データの暗号化をかけて情報漏えい対策をしているか？	自部門の担当者のPC確認	○		
		確認事項	3.技術的事項 ●各個人のパスワードは8文字以上・数字記号の混合になっているか？ ●アクセス制限がなされているか？ ●Eメールで個人データを添付ファイルとして送付の際、誤送信対策をしているか？ ●個人情報を含んだ情報をFAX送信する場合は、送付の前後に電話連絡をし、相手先本人が確実に受け取れる配慮をしているか？ ●パソコンについてウイルス対策ソフトはインストールされているか？また定期的にアップデートされているか？ ●不正なソフトウェアは入っていないか？	自部門の担当者のPC確認	○		
個人情報保護マニュアル J.9.4 安全管理規定 Ⅲ	委託先の監督	確認事項	「個人情報保護マニュアル」及び「安全管理規定」で定められた手順に従って、委託先の監督が適切にされているか？ （具体的なチェック事項） ●委託先に関して「秘密保持誓約書」「業務委託契約書」は規定すべき項目を満たして結ばれているか？また不備はないか？ ●「委託先評価表」に従った、実際の評価がなされているか？ ●委託先と個人データの保有期間を合意し、確認しているか？ ●委託先とのEメール誤送信対策や外部メディア・紙は直接手渡しのルールが徹底されているか？ ●FAXを受ける際、送信の連絡を行っているか、また情報をFAXトレーに放置していないか？	具体的な委託先（社労士事務所）とのやり取り確認。	○		