

【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	確認(承認)
202X.XX.XX	202X.XX.XX
〇〇	〇〇

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。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/category/2091601.html>

※赤字は、新基準における改訂箇所
 ※記載事項はサンプルとなります。

監査実施日: 202X.X.XX

対象部門: 個人情報管理責任者

— 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 ○: 適合(有効である) △: 観察事項(検討が望まれる) ×: 不適合(有効でない)

指針項目 ※カッコはJISQ15001:2023の要求事項	チェック内容	確認結果 (適合の証拠)	適合性評価 結果 (○、△、×)	有効性の評価 (○、△、×)	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	×	×	内部規程(文書化)は要求事項ではないが、明確化するために「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	△	△	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 (4.1)	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。また、法令は特定され、参照(順守を含む)されているか。	「個人情報保護マニュアル」にて文書化。「法規制登録台帳」確認	○	△ 完全に法令を理解しているかどうかは一部不明であった	外部の専門家等のフォローを受けることを検討する
	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.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、従業員を指揮・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.2.2 個人情報保護方針 (5.2.1、5.2.2)	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.2.1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)○ d)○	○	○	—
		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、国が定める指針その他の規範の遵守 c)個人情報の漏えい、滅失又ははぎ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	○	○	—	

指針項目 ※カッコはJISQ15001:2023の要求事項	チェック内容	確認結果 (適合の証拠)	適合性評価 結果 (○、△、×)	有効性の評価 (○、△、×)	是正計画等	
J.2.3.1 組織の役割、責任及び権限 (5.3.1)	確認事項 社長は、個人情報保護に関連する役割に対して、責任及び権限を従業者へ割り当てるとともに、その結果を利害関係者に周知しているか。□	「個人情報保護マニュアル」に明確化	○	○	-	
	確認事項 責任及び権限を、次の事項を実施するために割り当てているか。 a)個人情報保護マネジメントシステムを、本指針の要求事項に適合させる。 b)個人情報保護マネジメントシステムの運用の成果をトップマネジメントに報告させる。□	「個人情報保護マニュアル」に明確化	○			
	確認事項 役割及び役割に対する責任及び権限を、内部規程として文書化しているか。	「安全管理規定」に明確化	○			
J.2.3.2 個人情報保護管理者と個人情報保護監査責任者 (5.3.2)	確認事項 社長は、本指針の内容を理解し実践する能力のある個人情報保護管理者を事業者内部に属する者の中から指名し、個人情報保護マネジメントシステムの実施及び運用に関する責任及び権限を他の責任にかかわりなく与え、業務を行わせているか。□	個人情報管理者、A氏の実務の現状確認	○	○	-	
	確認事項 個人情報保護管理者は、個人情報保護マネジメントシステムの見直し及び改善の基礎として、社長に個人情報保護マネジメントシステムの運用状況を報告しているか。	「マネジメントレビューに関する記録」確認	○			
	確認事項 社長は、公平、かつ、客観的な立場にある個人情報保護監査責任者を事業者内部に属する者の中から指名し、監査の実施及び報告を行う責任及び権限を他の責任にかかわりなく与え、業務を行わせているか。□	監査責任者、B氏の実務の現状確認	○			
	確認事項 個人情報保護監査責任者は、監査を指揮し、監査報告書を作成し、社長に報告しているか。	「内部監査報告書」確認	○			
	確認事項 監査員の選定及び監査の実施においては、監査の客観性及び公平性を確保しているか。	「内部監査実施計画書」「内部監査チェックリスト」確認	○			
J.2.4 管理目的及び管理策 (一般) (4.4)	確認事項 管理策について、社長又は社長によって権限が与えられた者によって、組織が定めた手段に従って承認しているか。	「Pマーク推進委員会議事録」確認	○	○	-	
J.3 計画	J.3.1.1 個人情報の特定 (6.1)	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	○	○	-
		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	○		
	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・管理する個人情報の件数(概数でも可)	「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) ○ 個人情報の件数) ○	○			
	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) (6.2.1)	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	「リスクアセスメント結果表」「リスク対応計画書」確認	○	○	-	
	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	○			

指針項目 ※カッコはJISQ15001:2023の要求事項	チェック内容	確認結果 (適合の証拠)	適合性評価 結果 (○、△、×)	有効性の評価 (○、△、×)	是正計画等
J.3.1.3 個人情報保護リスク アセスメント (6.2.1、6.2.2)	<p>確認事項 個人情報保護リスクについて、次の事項を踏まえて、個人情報保護リスクアセスメント(個人情報保護リスクを特定、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。 定めた手順及び実施した内容については、少なくとも毎年一回及び必要に応じて適宜に見直しているか。</p> <p>a)次の観点を、個人情報保護のリスク基準とする。 1)本人の権利利益の侵害 2)本指針に定める事項 3)法令及び国が定める指針その他の規範に関する事項 4)個人情報の漏えい、紛失、滅失・毀損、改ざん、正確性の未確保、不正・不適正取得、目的外利用・提供、不正利用、開示等の求め等の拒否に関する事項 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。</p>	「個人情報保護マニュアル」に明確化	○	○	-
	<p>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。</p>	「個人情報保護マニュアル」に明確化	○		
	<p>確認事項 文書化した情報を利用可能な状態にしているか。</p>	「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 (6.2.1、6.2.3)	<p>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。 定めた手順及び実施した内容については、適宜見直しているか。</p> <p>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。</p>	「個人情報保護マニュアル」に明確化	○	○	-
	<p>確認事項 a)~c)を実施した記録を 利用可能な状態にしているか。</p>	「リスクアセスメント結果表」確認	○		
J.6 パフォーマンス 評価	<p>確認事項 各部門及び階層の管理者が定期的に、及び適宜に 個人情報保護マネジメントシステムが適切に運用されていることを確認する手順を内部規程として文書化しているか。□</p>	「個人情報保護マニュアル」に明確化	○		
	<p>確認事項 個人情報保護マネジメントシステムが適切に運用されているかどうかを確認するために、次の事項を決定しているか。 a)対象とする個人情報保護マネジメントシステムの運用状況 b)a)で対象とした運用状況の監視、測定、分析及び評価の方法 c)a)で対象とした運用状況の監視及び測定の実施時期 d)a)で対象とした運用状況の監視及び測定の実施者 e)a)で対象とした運用状況の分析及び評価の時期 f)a)で対象とした運用状況の分析及び評価の実施者</p>	「個人情報保護マニュアル」に明確化	○	○	-
	<p>確認事項 各部門及び各階層の管理者は、定期的に、及び適宜にマネジメントシステムが適切に運用されているかを確認し、不適合が確認された場合は、その是正処置を行っているか。□</p>	「Pマーク推進委員会議事録」確認	○		
	<p>確認事項 監視及び測定の結果の証拠となる文書化した情報を利用可能な状態にしているか。</p>	「日常点検チェックリスト」確認	○		
	<p>確認事項 個人情報保護管理者は、定期的に、及び適宜に社長に運用の確認の状況を報告しているか。□</p>	「Pマーク推進委員会議事録」確認	○		
J.6.2 内部監査 (9.2.1、 9.2.2)	<p>確認事項 内部監査の計画及び実施、結果の報告並びにこれに伴う記録の保持に関する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。</p>	「内部監査規定」に明確化	○		
	<p>確認事項 個人情報保護マネジメントシステムが次の事項の状況にあるか否かについて、少なくとも毎年一回及び必要に応じて適宜に内部監査を実施しているか。 a)自社の内部規程(文書)が、プライバシーマーク構築・運用指針の要求事項に適合している。 b)個人情報保護マネジメントシステムが有効に実施され、維持されている。□</p>	「内部監査実施計画書」「内部監査チェックリスト」「内部監査報告書」確認	○	○	-
	<p>確認事項 個人情報保護監査責任者は、次の事項を行っているか。 c)内部監査実施計画を策定、確立、実施及び維持する。その内部監査実施計画は、関連するプロセスの重要性及び前回までの内部監査の結果を考慮する。 d)各内部監査について、監査目的、監査基準及び監査範囲を明確にする。 e)内部監査プロセスの客観性及び公平性を確保する監査員を選定し、内部監査実施計画に従って、監査を実施する。 f)内部監査の結果を内部監査報告書としてまとめ、管理層及び社長に報告する。 g)内部監査実施計画及び監査結果の証拠として、文書化した情報を 利用可能な状態にする。□</p>	「内部監査実施計画書」「内部監査チェックリスト」「内部監査報告書」確認	○		

指針項目 ※カッコはJISQ15001:2023の要求事項	チェック内容	確認結果 (適合の証拠)	適合性評価 結果 (○、△、×)	有効性の評価 (○、△、×)	是正計画等		
J.6.3 マネジメントレビュー (9.3.1、9.3.2、9.3.3)	確認事項	マネジメントレビューを実施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」に明確化	○			
	確認事項	社長は、事業者の個人情報保護マネジメントシステムが、引き続き、適切、妥当かつ有効であることを確実にするために、少なくとも年一回及び必要に応じて適宜にマネジメントレビューを実施しているか。□	「マネジメントレビューに関する記録」確認	○			
	確認事項	マネジメントレビューの実施にあたっては、次の事項を考慮しているか。 a)前回までのマネジメントレビューの結果を踏まえた見直しの状況 b)個人情報保護マネジメントシステムに関連する外部及び内部の問題点の変化 c)以下の状況を踏まえた、現在の個人情報保護マネジメントシステムの運用状況の評価 1)不適合及び是正処置 2)監視及び測定の結果 3)内部監査結果 4)個人情報保護目的の達成 d)利害関係者からのフィードバック e)リスクアセスメントの結果及びリスク対応計画の状況 f)継続的改善の機会 □	「マネジメントレビューに関する記録」確認	○	○	-	
	確認事項	マネジメントレビューからのアウトプットには、継続的改善の機会及び個人情報保護マネジメントシステムのあらゆる変更の必要性に関する決定を含めているか。	「マネジメントレビューに関する記録」確認	○			
	確認事項	マネジメントレビューの結果の証拠となる文書化した情報を 利用可能な状態 にしているか。	「マネジメントレビューに関する記録」確認	○			
J.7 改善	J.7.1 不適合及び是正処置 (10.2)	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	○	○	-
		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	○		
		確認事項	上記の実施結果の 証拠 となる文書化した情報を 利用可能な状態 にするとともに、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.8 取得、利用及び提供に関する原則	J.7.2 継続的改善 (10.1)	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.8.1 利用目的の特定 (A.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	○	○	-
		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。	〇〇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.4)	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。	〇〇における個人情報取扱い業務の実態確認	○	○	-
J.8.3 要配慮個人情報などの取得 (A.5)	確認事項	要配慮個人情報の取得に際しては、要配慮個人情報の取得、利用又は提供(要配慮個人情報のデータの提供を含む)する旨について、あらかじめ書面によって明示し、書面によって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	○			
	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)本人を自視し、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)特定した利用目的の達成に必要な範囲内において、要配慮個人情報の取扱いの全部又は一部を委託することに伴って、当該要配慮個人情報の提供を受けるとき h)合併その他の事由による事業の継承に伴って要配慮個人情報の提供を受けるときであって、承継前の利用目的の範囲内で当該要配慮個人情報を取り扱うとき i)J.8.7のd)によって、特定の者との間で共同して利用される要配慮個人情報を当該特定の者から提供を受けるとき	健康診断に係る個人情報取扱いの実態確認	○	○	-	

指針項目 ※カッコはJISQ15001:2023の要求事項		チェック内容	確認結果 (適合の証拠)	適合性評価 結果 (○、△、×)	有効性の評価 (○、△、×)	是正計画等
		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、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) k)学術研究機関等から当該要配慮個人情報を取得する場合であって、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)。なお、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。				
		確認事項 個人情報に、性生活、性的指向又は労働組合に関する情報が含まれる場合には、当該情報を要配慮個人情報と同様に取り扱っているか。	個人情報取扱いの実態確認	○		
J.8.4個人情報を取得した場合の措置 (A.6)		確認事項 個人情報を取得した場合は、あらかじめ、その利用目的を公表している場合を除き、速やかにその利用目的を本人に通知し、又は公表しているか。	「個人情報の取扱いに関する同意書」確認	○		
		確認事項 本人に利用目的を通知し、又は公表を要しないのは、以下の場合に限ること。 a)利用目的を本人に通知し、又は公表することによって本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合 b)利用目的を本人に通知し、又は公表することによって自社の権利又は正当な利益を害するおそれがある場合 c)国の機関又は地方公共団体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、利用目的を本人に通知し、又は公表することによって自社の事務の遂行に支障を及ぼすおそれがある場合 d)取得の状況からみて利用目的が明らかであると認められる場合	記載以外の事例はなかった。	○	○	—
J.8.10 仮名加工情報 (A.27)		確認事項 仮名加工情報を取り扱いを行うかの方針は定めているか。	仮名加工情報は取り扱わない	○		
		確認事項 仮名加工情報を取り扱う場合には、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	○		
		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	○		
		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、又はJ.8.4の(a)～(d)のいずれかに該当する場合を除き、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、以下の場合に限定しているか。 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、適法かつ公正な手段によって共同利用されている場合であって、以下の1)～5)に示す事項をあらかじめ公表するとともに、共同して利用する者との間で共同利用についての契約を定めているとき 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 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.9 適正管理	J.9.1 正確性の確保 (A.9)	確認事項 利用目的の達成に必要な範囲内において、個人データを、正確、かつ、最新の状態で管理しているか。	指定されたサーバーで管理されていた	○	○	—
		確認事項 個人データの管理(利用する必要がなくなった場合の消去を含む。)は、定めた手順に基づいて適切に行っているか。	個人情報取扱い業務の実態確認	○		
	J.9.2 安全管理措置 (A.10)	確認事項 取り扱う個人情報の個人情報保護リスクに応じて、漏えい、滅失又は毀損の防止その他の個人情報の安全管理のために、法令に基づき必要かつ適切な措置を講じているか。	「安全管理規定」に明確化	○	○	—

指針項目 ※カッコはJISQ15001:2023の要求事項		チェック内容	確認結果 (適合の証拠)	適合性評価 結果 (○、△、×)	有効性の評価 (○、△、×)	是正計画等	
		確認事項 外部サービスを利用する場合であって、当該サービス提供事業者が当該個人データを取り扱わないことになっているサービスを利用する場合には、適切な安全管理措置が図られるよう、あらかじめサービス内容の把握、評価等を行ったうえで選定しているか。		○	○	—	
J.9.3	従業者の監督 (A.11)	確認事項 個人データを取り扱う従業者に対して必要かつ適切な監督を行っているか。	該当部門の責任者にヒアリングを実施	○	○	—	
J.9.4	委託先の監督 (A.12)	確認事項 個人データの取扱いの全部又は一部を委託する場合、十分な個人データの保護水準を満たしている者を選定するための委託先選定基準を確立し、委託先を選定しているか。	「安全管理規定」に明確化し、選定された委託先は、「委託先管理台帳」に登録されていた	○	○	—	
		確認事項 個人データの取扱いの全部又は一部を委託する場合、特定した利用目的の範囲内で委託契約を締結しているか。	契約書確認	○			
		確認事項 次に示す事項が盛り込まれた契約を締結しているか。 a)委託者及び受託者の責任の明確化 b)個人データの安全管理に関する事項 c)再委託に関する事項 d)個人データの取扱状況に関する委託者への報告の内容及び頻度 e)契約内容が遵守されていることを委託者が、定期的に、及び適宜に確認できる事項 f)契約内容が遵守されなかった場合の措置 g)事件・事故が発生した場合の報告・連絡に関する事項 h)契約終了後の措置 □	契約書確認	○			
		確認事項 全ての委託先を漏れなく特定しているか。	「委託先管理台帳」確認	○			
		確認事項 委託契約書は当該個人データの保有期間にわたって保存しているか。	契約書確認	○			
		確認事項 委託契約に基づき、委託先を適切に監督しているか。	「委託先継続評価表」確認	○			
J.10.7	保有個人データの利用又は提供の拒否権 (A.22、A.23)	確認事項 本人から当該本人が識別される保有個人データの利用停止等(利用の停止、消去 又は第三者への提供の停止)の請求に応じているか。	「個人情報保護マニュアル」及び「個人情報取扱規程」で明確にしているが、実績はなかった	○	実績がないので、有効性は判断できない	—	
		確認事項 本人からの当該本人が識別される保有個人データの利用停止等の請求に応じた場合、遅滞なくその旨を本人に通知しているか。□	「個人情報保護マニュアル」及び「個人情報取扱規程」で明確にしているが、実績はなかった	○			
		確認事項 本人からの当該本人が識別される保有個人データの利用停止等の請求に応じなかった場合は、以下のいずれかに該当する場合に限り、本人に遅滞なくその旨を通知するとともに、理由を説明しているか。 a)当該保有個人データの利用停止等に方法に多額の費用を要する場合等の理由により、利用停止等を行うことが困難な場合であって、本人の権利利益を保護するために必要なこれに代わるべき措置をとるとき b)本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合 c)当社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 d)法令に違反する場合	「個人情報保護マニュアル」及び「個人情報取扱規程」で明確にしているが、実績はなかった	○			
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 (7.4.2、A.26)	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を内部規程として文書化しているか。	「個人情報取扱規程」に明確化	○	実績がないので、有効性は判断できない	—
		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。	「個人情報取扱規程」に明確化	○			
		確認事項 苦情及び相談の申出先(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出先も含む)について、本人の知り得る状態(本人の請求などに応じて遅滞なく回答する場合を含む)に置いているか。	自社ホームページに明確化	○			
		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	○			