個人情報保護監査チェックリスト（PMSとJISQ15001：2017適合性監査）

監査責任者	監査人

被監査部門：—

監査人：線﨑 千里

監査実施日：2022年11月22日

■判定：○＝適合（要求事項が規定されている）、△＝記述が不十分、×＝不適合（規定されていない）

		チェック項目	関連する個人情報保護規程等の項番	判定	コメント
A.3.1.1一般	(1)	この管理策に規定するA.3.2からA.3.8は、トップマネジメントによって権限を与えられた者によって、組織が定めた手段に従って承認されなければならない。	個人情報保護規程　A.3.1.1		
A.3.2.1内部向け個人情報保護方針	(1)	内部向け個人情報保護方針を文書化した情報に、次の事項が含まれていること。 a)事業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[特定された利用目的の達成に必要な範囲を超えた個人情報の取扱い（以下、“目的外利用”という）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を遵守すること。 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こと。 d)苦情及び相談への対応に関すること。 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こと。 f)トップマネジメントの氏名	個人情報保護方針（PA00）		
A.3.2.2外部向け個人情報保護方針	(1)	外部向け個人情報保護方針を文書化した情報に、A.3.2.1に規定する内部向け個人情報保護方針の事項が含まれていること。	個人情報保護方針（PA00）		
	(2)	外部向け個人情報保護方針を文書化した情報に、次の事項を明記していること。 a)制定年月日及び最終改正年月日 b)外部向け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（PA00）		
	(3)	トップマネジメントは、外部向け個人情報保護方針を文書化した情報について、一般の人が入手可能な措置を講じるよう規定していること	個人情報保護方針（PA00） 個人情報保護規定A.3.2.2		
A.3.3.1個人情報の特定	(1)	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が内部規程として文書化されていること。	個人情報保護規程　A.3.3.1		
	(2)	台帳には、少なくとも以下の項目が含まれていること。 ・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(PC01)		
	(3)	特定した個人情報については、個人データと同様に取り扱わなければならないよう規定していること。	個人情報保護規程　A.3.3.1		
A.3.3.2法令，国が定める指針その他の規範	(1)	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。)を特定し参照できる手順が内部規程として文書化されていること。	個人情報保護規程　A.3.3.2		
A.3.3.3リスクアセスメント及びリスク対策	(1)	A.3.3.1によって特定した個人情報について、利用目的の達成に必要な範囲を超えた利用を行わないため、必要な対策を講じる手順を確立し、かつ、維持するよう規定していること。	個人情報保護規程　A.3.3.3		
	(2)	A.3.3.1によって特定した個人情報の取扱いについて、個人情報保護リスクを特定し、分析し、必要な対策を講じる手順が内部規程として文書化されていること。	個人情報保護規程　A.3.4.3		
	(3)	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、管理するよう規定していること。	個人情報保護規程　A.3.3.3		
	(4)	個人情報保護リスクの特定、分析及び講じた個人情報保護リスク対策を少なくとも年一回、適宜に見直すよう規定していること。	個人情報保護規程　A.3.3.3		
	(5)	EU域内から十分性認定に基づき提供を受けた個人情報」がある場合、これを特定し、リスクアセスメント及びリスク対策を行うための手順があること。			
A.3.3.4資源，役割責任及び権限	(1)	各担当者の役割・権限が内部規程として文書化されていること。	個人情報保護規程(A.3.3.5.d))		
	(2)	トップマネジメントは、この規格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組織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、業務を行わせなければならないよう規定していること。	個人情報保護規程　A.3.3.4		
	(3)	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、トップマネジメント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する旨が内部規程として文書化されていること。	個人情報保護規程(A.3.3.5d))		
	(4)	トップマネジメントは、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組織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、業務を行わせなければならないよう規定していること。	個人情報保護規程　A.3.3.4		
	(5)	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、トップマネジメントに報告する旨が内部規程として文書化されていること。	個人情報保護規程(A、3.3.5d))		
	(6)	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する旨が内部規程として文書化されていること。	個人情報保護規程(A.3.3.5 d))		
	(7)	個人情報保護監査責任者と個人情報保護管理者とは異なる者であることを規定していること。	個人情報保護規程　A.3.3.4		

	チェック項目		関連する個人情報保護規程等の項番	判定	コメント
A.3.3.5内部規程 次の事項を含む内部規程が文書化されていること。	(1)	以下の規定があること。 a)個人情報を特定する手順に関する規定	個人情報保護規程 A.3.3.1		
	(2)	b)法令、国が定める指針その他の規範の特定、参照及び維持に関する規定	個人情報保護規程 A.3.3.2		
	(3)	c)個人情報保護リスクアセスメント及びリスク対策の手順に関する規定	個人情報保護規程 A.3.3.3		
	(4)	d)組織の各部門及び階層における個人情報を保護するための権限及び責任に関する規定	個人情報保護規程 A.3.3.4 個人情報保護体制図(PB01)		
	(5)	e)緊急事態への準備及び対応に関する規定	個人情報保護規程 A.3.3.7		
	(6)	f)個人情報の取得、利用及び提供に関する規定	個人情報保護規程 A.3.4.2		
	(7)	g)個人情報の適正管理に関する規定	個人情報保護規程 A.3.4.3		
	(8)	h)本人からの開示等の請求等への対応に関する規定	個人情報保護規程 A.3.4.4		
	(9)	i)教育などに関する規定	個人情報保護規程 A.3.4.5		
	(10)	j)文書化した情報の管理に関する規定	個人情報保護規程 A.3.5		
	(11)	k)苦情及び相談への対応に関する規定	個人情報保護規程 A.3.6		
	(12)	l) 点検に関する規定	個人情報保護規程 A.3.7		
	(13)	m)是正処置に関する規定	個人情報保護規程 A.3.8		
	(14)	n)マネジメントレビューに関する規定	個人情報保護規程 A.3.7.3		
	(15)	o)内部規程の違反に関する罰則の規定	個人情報保護規程 A.3.4.3.3		
	(16)	事業の内容に応じて、個人情報保護マネジメントシステムが確実に適用されるように内部規程を改正しなければならないよう規定していること。	個人情報保護規定A3.3.5		
A.3.3.6計画策定	(1)	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、少なくとも年一回、次の事項を含めて、必要な計画を立案するよう規定していること。 a)教育実施計画 b)内部監査実施計画	個人情報保護規定A3.3.6 個人情報保護教育計画書(PC14) 内部監査計画書(PC19)		
	(2)	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必要な計画に、次の事項を含んでいること。 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	個人情報保護教育計画書(PC14) 内部監査計画書(PC19)		
A.3.3.7緊急事態への準備	(1)	緊急事態を特定するための手順、及び、特定した緊急事態にどのように対応するかの手順が内部規程として文書化されていること。	個人情報保護規程 A3.3.7		
	(2)	緊急事態への準備及び対応に関する規定には、個人情報保護リスクを考慮し、その影響を最小限とするための手順が含まれていること。	個人情報保護規程 A3.3.7		
	(3)	緊急事態への準備及び対応に関する規定には、緊急事態が発生した場合に備え、次の事項を含む対応手順が含まれていること。 a)漏えい、滅失又はき損が発生した個人情報の内容を本人に速やかに通知するか、又は本人が容易に知り得る状態に置くこと。 b)二次被害の防止、類似事案の発生回避などの観点から、可能な限り事実関係、発生原因及び対応策を、遅滞なく公表すること。 c)事実関係、発生原因及び対応策を関係機関に直ちに報告すること。	個人情報保護規程 A3.3.7		
A.3.4.1運用手順	(1)	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、運用の手順が内部規程として文書化されていること。	個人情報保護規程 A.3.4.2、A.3.4.3、A.3.4.4、A.3.4.5、A.3.4.3.3		
A.3.4.2.1利用目的の特定	(1)	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わなければならない旨が規定されていること。	個人情報保護規程 A3.4.2.1		
	(2)	個人情報の取得に当たっては、利用目的をできる限り特定し、その目的の達成に必要な限度において行わなければならない旨が規定されていること。	個人情報保護規程 A3.4.2.1		
A.3.4.2.2適正な取得	(1)	個人情報の取得は、適法、かつ、公正な手段によって行われなければならないという原則を規定していること。	個人情報保護規程 A3.4.2.2		
A.3.4.2.3要配慮個人情報	(1)	新たに要配慮個人情報を取得する場合、あらかじめ書面による本人の同意を得ないで、要配慮個人情報を取得してはならないという原則を規定していること。	個人情報保護規程 A3.4.2.3		
	(2)	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こと。 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)その他、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、又は政令で定められた要配慮個人情報であるとき	個人情報保護規程 A3.4.2.3		
	(3)	あらかじめ書面による本人の同意を得て、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、本人から書面により同意を得る手順を定めていること。	個人情報保護規程 A3.4.2.3		
	(4)	「EU域内から十分性認定に基づき提供を受けた個人情報」に「労働組合」、「性生活」、「性的指向」に関する情報が含まれている場合、要配慮個人情報として取り扱うルール・手順があること。	-	-	

		チェック項目	関連する個人情報保護規程等の項番	判定	コメント
A.3.4.2.4個人情報を取得した場合の措置	(1)	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、本人に通知するか、又は公表しなければならないよう規定していること。	個人情報保護規程 A.3.4.2.4		
	(2)	個人情報を取得する場合は、あらかじめその利用目的を公表する手順、又は取得後に速やかにその利用目的を、本人に通知し、又は公表する手順が定められていること。	個人情報保護規程 A.3.4.2.4		
	(3)	本人への利用目的の通知又は公表を要しないのは、以下の場合に限定していること。 a)利用目的を本人に通知するか、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するか、又は公表することによって当該組織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するか、又は公表す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	個人情報保護規程 A.3.4.2.4		
	(4)	委託、提供、共同利用により取得した場合、委託元、提供元又は他の共同利用者が個人情報保護法及び個人情報保護委員会ガイドライン等に沿って適切に個人情報を取り扱っていることを確認するよう規定していること。	個人情報保護規定A3.4.2.2		
	(5)	「EU域内から十分性認定に基づき提供を受けた個人情報」については、当該個人情報の提供を受ける際に特定された利用目的を含め、その取得の経緯を確認し、記録するルール・手順があること。	–	–	
A.3.4.2.5 A.3.4.2.4のうち本人から直接書面によって取得する場合の措置	(1)	A.3.4.2.4の措置を講じた場合において、本人から、書面（電子的方式、磁気的方式など人の知覚によっては認識できない方式で作られる記録を含む。以下、同じ。）に記載された個人情報を直接取得する場合には、少なくとも、次のa)～h)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、書面によって本人に明示し、書面によって本人の同意を得る手順を取得する手段毎に定めていること。 a）当社の名称 b）個人情報保護管理者（若しくはその代理人）の氏名又は職名，所属及び連絡先 c）利用目的 d）個人情報を第三者に提供することが予定される場合の事項 － 第三者に提供する目的 － 提供する個人情報の項目 － 提供の手段又は方法 － 当該情報の提供を受ける者又は提供を受ける者の組織の種類，及び属性 － 個人情報の取扱いに関する契約がある場合はその旨 e）個人情報の取扱いの委託を行うことが予定される場合には，その旨 f）A.3.4.4.4～A.3.4.4.7 に該当する場合には，その請求等に応じる旨及び問合せ窓口 g）本人が個人情報を与えることの任意性及び当該情報を与えなかった場合に本人に生じる結果 h）本人が容易に知覚できない方法によって個人情報を取得する場合には，その旨	個人情報保護規程 A.3.4.2.5		
	(2)	あらかじめ書面によって本人に明示し、書面によって本人の同意を得ないのは、以下の場合に限定していること。 ・人の生命、身体若しくは財産の保護のために緊急に必要がある場合 ・A.3.4.2.3のa)～d)のいずれかに該当する場合	個人情報保護規程 A.3.4.2.5		
A.3.4.2.6利用に関する措置	(1)	特定した利用目的の達成に必要な範囲内で個人情報を利用しなければならないという原則を明確に規定していること。	個人情報保護規程 A.3.4.2.6		
	(2)	特定した利用目的の達成に必要な範囲を超えて個人情報を利用する場合は、あらかじめ、少なくとも、A.3.4.2.5のa)～f)に示す事項又はそれと同等以上の内容の事項を本人に通知し、本人の同意を得る手順が定められていること。	個人情報保護規程 A.3.4.2.6		
	(3)	本人の同意を得ることを要しないのは、A.3.4.2.3のa)～d)のいずれかに該当する場合に限定していること。	個人情報保護規程 A.3.4.2.6		
A.3.4.2.7本人に連絡又は接触する場合の措置	(1)	個人情報を利用して本人に連絡又は接触する場合には、本人に対して、A.3.4.2.5のa)～f)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、本人の同意を得る手順が規定されていること。	個人情報保護規程 A.3.4.2.7		
	(2)	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こと。 a)A.3.4.2.5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、既に本人の同意を得ているとき b)個人情報の取扱いの全部又は一部を委託された場合であって、当該個人情報を、その利用目的の達成に必要な範囲内で取り扱うとき c)合併その他の事由による事業の承継に伴って個人情報が提供され、個人情報を提供する組織が、既にA.3.4. 2.5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、承継前の利用目的の範囲内で当該個人情報を取り扱うとき 該個人情報を取り扱うとき d)個人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A.3.4.2.5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、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、本人に通知するか、又は本人が容易に知り得る状態に置いているとき(以下、－共同して利用すること“共同利用”という。) －共同して利用される個人情報の項目 －共同して利用する者の範囲 －共同して利用する者の利用目的 －共同して利用する個人情報の管理について責任を有する者の氏名又は名称 －取得方法e)A.3.4.2.4のd)に該当するため、利用目的などを本人に明示、通知又は公表することなく取得した個人情報を利用して、本人に連絡又は接触するとき f)A.3.4.2.3のただし書きa)～d)のいずれかに該当する場合	個人情報保護規程 A.3.4.2.7		
	(3)	共同して利用する者から個人情報を取得する場合であって、共同して利用する者がA.3.4.2.7d)の措置を講じない場合、本人に対して、A.3.4.2.5のa)～f)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、本人の同意を得る手順を定めていること。	個人情報保護規程 A.3.4.2.7		
	(4)	ただし書きd)を適用する場合、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手順が定められていること。	個人情報保護規程 A.3.4.2.7		

	チェック項目		関連する個人情報保護規程等の項番	判定	コメント
A.3.4.2.8個人データの提供に関する措置	(1)	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、A.3.4.2.5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、本人の同意を得る手順を定めていること。	個人情報保護規程 A.3.4.2.8		
	(2)	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こと。 a)A.3.4.2.5又はA.3.4.2.7の規定によって、既にA.3.4.2.5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又は通知し、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、本人に通知するか、又はそれに代わる同等の措置を講じているとき 1)第三者への提供を利用目的とすること 2)第三者に提供される個人データの項目 3)第三者への提供の手段又は方法 4)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 5)取得方法 6)本人からの請求などを受け付ける方法 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、b)の1)～6)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、本人に通知するか、又は本人が容易に知り得る状態に置いているとき	個人情報保護規程 A.3.4.2.8		
		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、A.3.4.2.7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)A、3.4.2.3のただし書きa)～d)のいずれかに該当する場合			
	(3)	ただし書きb)を適用する場合、必要な措置を講じる手順が定められていること。	個人情報保護規程 A.3.4.2.8		
	(4)	ただし書きc)を適用する場合、b)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く手順が定められていること。	個人情報保護規程 A.3.4.2.8		
	(5)	個人データを共同利用している場合、共同して利用する者の間で、A.3.4.2.7に規定する共同利用について契約によって定めるよう規定していること。	個人情報保護規程 A.3.4.2.8		
	(6)	ただし書きf)を適用する場合、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手順が定められていること。	個人情報保護規程 A.3.4.2.8		
A.3.4.2.8.1外国にある第三者への提供の制限	(1)	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、A.3.4.2.5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、本人の同意を得る手順を定めていること。	個人情報保護規程 A.3.4.2.8.1		
	(2)	本人の同意を要しないのは、A.3.4.2.3のa)～d)のいずれかに該当する場合及びその他法令等によって除外事項が適用される場合に限定していること。	個人情報保護規程 A.3.4.2.8.1		
	(3)	ただし書きb)を適用する場合、必要な措置を講じる手順が定められていること。	–	–	
	(4)	ただし書きc)を適用する場合、b)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く手順が定められていること。	–	–	
A.3.4.2.8.2第三者提供に係る記録の作成など	(1)	個人データを第三者に提供した場合、(法令等の定めるところによって)記録を作成、保管する手順を定めていること。	個人情報保護規程 A.3.4.2.8.2		
	(2)	記録を作成しなかったのは、A.3.4.2.3のa)～d)のいずれかに該当する場合、又は以下の場合に限定していること。 a)個人情報取扱事業者が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ことに伴って当該個人データが提供される場合 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が提供される場合 c)特定の者との間で共同して利用される個人データが当該特定の者に提供される場合であって、その旨並びに共同して利用される個人データの項目、共同して利用する者の範囲利用する者の利用目的及び当該個人データの管理について責任を有する者の氏名又は名称について、あらかじめ、本人に通知するか、又は本人が容易に知り得る状態に置いているとき。	個人情報保護規程 A.3.4.2.8.2		
A.3.4.2.8.3第三者提供を受ける際の確認など	(1)	第三者から個人データの提供を受けるに際しては、法令等の定めるところによって確認を行った記録を作成し、保管する手順を定めていること。	個人情報保護規程 A.3.4.2.8.3		
	(2)	確認の記録を作成、保管していないのは、A.3.4.2.3のa)～d)のいずれかに該当する場合、又はA.3.4.2.8.2のa)～c)のいずれかに該当する場合に限定していること。	個人情報保護規程 A.3.4.2.8.3		
A.3.4.2.9匿名加工情報	(1)	匿名加工情報の取扱を行うか否かの方針が存在すること。	個人情報保護規程 A.3.4.2.9		
	(2)	匿名加工情報を取り扱う場合、匿名加工情報の取扱いの手順を内部規程として文書化していること。	個人情報保護規程 A.3.4.2.9		
	(3)	EU域内から十分性認定に基づき提供を受けた個人情報」については、加工方法等情報を削除することにより、匿名化された個人を再識別することを何人にとっても不可能とした場合に限り、匿名加工情報とみなすルール・手順があること。	–	–	

	チェック項目		関連する個人情報保護規程等の項番	判定	コメント
A.3.4.3.1正確性の確保	(1)	個人データを、正確、かつ最新の状態で管理する手順を定めていること。	個人情報保護規程 A.3.4.3.1		
	(2)	利用する必要がなくなった個人データを遅滞なく消去する手順を定めていること。	個人情報保護規程 A.3.4.3.1		
A.3.4.3.2安全管理措置	(1)	個人情報保護のための体制の一環として、安全管理体制が整備されていること。	個人情報保護規程 A.3.4.3.2		
	(2)	入退管理の措置が規定されていること(社員や来訪者の記録、入退制限の措置、全事業所についての規定等)。	個人情報保護規程 A.3.4.3.2		
	(3)	盗難等の防止の措置が規定されていること(携帯可能なコンピュータ等の盗難防止、スクリーンセーバーの起動、媒体の施錠保管・廃棄等)。	個人情報保護規程 A.3.4.3.2		
	(4)	機器・装置等の物理的な保護について規定されていること(盗難、破壊、破損、漏水、火災、停電、地震等)。	個人情報保護規程 A.3.4.3.2		
	(5)	機器・装置等の物理的な保護について規定されていること(電子化された個人情報のバックアップ)。	個人情報保護規程 A.3.4.3.2		
	(6)	アクセス権限の管理について規定されていること(ID・パスワードの発行・更新・廃棄の管理、アクセス権限等)。	個人情報保護規程 A.3.4.3.2		
	(7)	アクセスの記録について規定されていること(アクセスの監視とアクセスログの取得・点検)。	個人情報保護規程 A.3.4.3.2		
	(8)	不正ソフトウェア対策について規定されていること(ウィルス対策、セキュリティパッチの適用等)。	個人情報保護規程 A.3.4.3.2		
	(9)	個人情報の移送・通信時の対策の措置がを規定されていること(授受の記録、リモートアクセスにおけるアクセス制限、インターネット・無線LAN等における暗号化等)。	個人情報保護規程 A.3.4.3.2		
	(10)	個人情報の持ち出し手段の制限の措置が規程されていること(個人情報をみだりに外部記憶媒体へ記録することの禁止、パソコンの持ち出しに関する規定を定めてあること、社内と社外の間の電子メールの監視について規定を定めてあること等)	個人情報保護規程 A.3.4.3.2		
A.3.4.3.3従業者の監督	(1)	従業者に対し必要かつ適切な監督を行わなければならない旨を規格に従い規定していること。	個人情報保護規程 A.3.4.3.3		
	(2)	従業者との雇用契約時または派遣社員等の受入れ時における派遣事業者との委託契約時に、個人情報の非開示契約を締結するよう規定していること。	個人情報保護規程 A.3.4.3.3		
	(3)	雇用契約または派遣社員等の受入れ時における派遣事業者との委託契約等を締結する場合、非開示条項は、契約終了後も一定期間有効であるようにするよう規定していること。	個人情報保護規程 A.3.4.3.3		
	(4)	個人情報保護マネジメントシステムに違反した場合の措置に関する規定が整備されていること。	個人情報保護規程 A.3.4.3.3		
	(5)	ビデオ及びオンラインによる従業者のモニタリングを実施する場合、その措置の実施について規定していること。	個人情報保護規程 A.3.4.3.3		
A.3.4.3.4委託先の監督	(1)	個人データの取扱いの全部又は一部を委託する場合、委託先と特定した利用目的の範囲内で委託契約を締結する旨を規定していること。	個人情報保護規程 A.3.4.3.4		
	(2)	委託先選定基準により委託先を評価するよう規定していること(定期的な再評価を含む)。	個人情報保護規程 A.3.4.3.4		
	(3)	委託先選定基準を定める手順及び見直しの手順が定められていること。	個人情報保護規程 A.3.4.3.4		
	(4)	委託先選定基準により委託先を評価するよう規定していること(定期的な再評価を含む)。	個人情報保護規程 A.3.4.3.4		
	(5)	次のa)～h)の内容が盛り込んだ契約書を締結する手順が定められていること。 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	個人情報保護規程 A.3.4.3.4		
	(6)	委託契約に基づき、委託先を適切に監督する手順を定めていること。	個人情報保護規程 A.3.4.3.4		
	(7)	当該契約書などの書面を当該個人データのの保有期間にわたって保存する手順を定めていること。	個人情報保護規程 A.3.4.3.4		
A.3.4.4.1個人情報に関する権利	(1)	保有個人データに当たらないものとして、次に掲げるいずれかに限定していること。 a)当該個人データの存否が明らかになることによって、本人又は第三者の生命、身体又は財産に危害が及ぶおそれのあるもの b)当該個人データの存否が明らかになることによって、違法又は不当な行為を助長する、又は誘発するおそれのあるもの c)当該個人データの存否が明らかになることによって、国の安全が害されるおそれ、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれのあるもの d)当該個人データの存否が明らかになることによって、犯罪の予防、鎮圧又は捜査その他の公共の安全及び秩序維持に支障が及ぶおそれのあるもの	個人情報保護規程 A.3.4.4.1		
	(2)	保有個人データに該当しないが、本人から求められる利用目的の通知、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止の請求などの全てに応じることができる権限を有する個人情報についても、保有個人データと同様に取り扱わなければならない旨が規定されていること	個人情報保護規程 A.3.4.4.1		

	チェック項目		関連する個人情報保護規程等の項番	判定	コメント
A.3.4.4.2開示等の請求等に応じる手続	(1)	保有個人データの開示等の請求等に応じる手続として、次の事項が 文書化されていること。 a)開示等の請求等の申出先 b)開示等の請求等に際して提出すべき書面の様式その他の開示等の請求等 の方式 c)開示等の請求等をする者が、本人又は代理人であることの確認の方法 d)A.3.4.4.4又はA.3.4.4.5による手数料(定めた場合に限る。)の徴収方法	個人情報保護規程 A.3.4.4.2		
	(2)	規格のc)の事項について、次の具体的手順を、それぞれ規定していること。 ⅰ)申請者が本人である場合。ⅱ)申請者が本人の法定代理人である場合。 ⅲ)申請者が本人の委任した代理人である場合。	個人情報保護規程 A.3.4.4.2		
	(3)	保有個人データの開示等の請求等に応じる手続を定めるに当たっては、本人 に過重な負担を課するものとならないよう配慮しなければならない旨を規定し ていること。	個人情報保護規程 A.3.4.4.2		
	(4)	本人からの請求などに応じる場合に、手数料を徴収するときは、実費を勘案し て合理的であると認められる範囲内において、その額を定める旨を規定して いること。	個人情報保護規程 A.3.4.4.2		
A.3.4.4.3保有個人データに関する事項の周知など	(1)	保有個人データに関し、次の事項を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。)に置いていること。 a)組織の氏名又は名称 b)個人情報保護管理者(若しくはその代理人)の氏名又は職名、所 属及び連絡先 c)全ての保有個人データの利用目的(A.3.4.2.4のa)～c)までに 該当する場合を除く。) d)保有個人データの取扱いに関する苦情の申出先 e)当該組織が認定個人情報保護団体の対象事業者である場合にあっては、 当該認定個人情報保護団体の名称及び苦情の解決の申出先 f)A.3.4.4.2によって定めた手続	個人情報保護規程 A.3.4.4.3		
A.3.4.4.4保有個人データの利用目的の通知	(1)	本人から、当該本人が識別される保有個人データについて利用目的の通知を 求められた場合、遅滞なくこれに応じるように規定していること。	個人情報保護規程 A.3.4.4.4		
	(2)	利用目的を通知しないのは、規格が定めるただし書きの場合に限定している こと。	個人情報保護規程 A.3.4.4.4		
	(3)	ただし書きにより利用目的を通知しない場合、本人に遅滞なくその旨を通知す るとともに、理由を説明するよう定められていること。	個人情報保護規程 A.3.4.4.4		
A.3.4.4.5保有個人データの開示	(1)	本人から、当該本人が識別される保有個人データの開示を求められた場合 に、法令の規定により特別の手続が定められている場合を除き、本人に対し、 遅滞無く応じるよう規定していること。	個人情報保護規程 A.3.4.4.5		
	(2)	開示の求めに応じないのは、規格が定めるただし書きの場合のみに限定して いること。	個人情報保護規程 A.3.4.4.5		
	(3)	ただし書きにより利用目的を通知しない場合、本人に遅滞なくその旨を通知す るとともに、理由を説明するよう定められていること。	個人情報保護規程 A.3.4.4.5		
A.3.4.4.6保有個人データの訂正、追加又は削除	(1)	本人から、当該本人が識別される保有個人データの訂正等を求められた場 合、法令の規定により特別の手続が定められている場合を除き、利用目的の 達成に必要な範囲内において、遅滞なく必要な調査を行い、その結果に基づ いて、当該開示対象個人情報の訂正等を行わなければならない旨を規定して いること。	個人情報保護規程 A.3.4.4.6		
	(2)	本人から保有個人データの訂正等の請求を受けて訂正等を行った場合は、そ の旨及びその内容を本人に遅滞なく通知しなければならない旨を規定してい ること。	個人情報保護規程 A.3.4.4.6		
	(3)	本人から保有個人データの訂正等の請求を受けたが応じなかった場合、その 旨及びその内容を本人に遅滞なく通知しなければならない旨を規定してい ること。	個人情報保護規程 A.3.4.4.6		
A.3.4.4.7保有個人データの利用又は提供の拒否権	(1)	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を求められた 場合、これに応じなければならないと共に、措置を講じた後は、遅滞なくその 旨を本人に通知しなければならない旨を規定していること。	個人情報保護規程 A.3.4.4.7		
	(2)	本人への回答内容(求めに応じない場合を含む)の承認手順が定められてい ること。	個人情報保護規程 A.3.4.4.7		
	(3)	利用停止等の求めに応じないのは、次の場合のみに限定していること。 a)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)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 c)法令に違反する場合	個人情報保護規程 A.3.4.4.7		
	(4)	次のa)～c)のいずれかに該当する場合、本人に遅滞なくその旨通知するとと もに、理由を説明しなければならない旨を規定していること。 a)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)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 c)法令に違反する場合	個人情報保護規程 A.3.4.4.7		
A.3.4.5認識	(1)	全ての従業者に対して、少なくとも年一回、適宜に教育を実施する手順が内 部規程として文書化されていること。	個人情報保護規程 A.3.4.5		
	(2)	教育などに関する規定には、受講者の理解度を確認する手順が含まれてい ること。	個人情報保護規程 A.3.4.5		
	(3)	全ての従業者に対して、次のa)～d)の内容を認識させるよう規定していること。 a)個人情報保護方針(内部向け個人情報保護方針及び外部向け個人情報保 護方針) b)個人情報保護マネジメントシステムに適合することの重要性及び利点 c)個人情報保護マネジメントシステムに適合するための役割及び責任 d)個人情報保護マネジメントシステムに違反した際に予想される結果	個人情報保護規程 A.3.4.5		
A.3.5.1文書化した情報の範囲	(1)	個人情報保護マネジメントシステムの基本となる次のa)～f)の要素を書面で記 述する旨を規定していること。 a)内部向け個人情報保護方針 b)外部向け個人情報保護方針 c)内部規程 d)内部規程に定める手順上で使用する様式 e)計画書 f) JISQ15001が要求する記録及び組織が個人情報保護マネジメントシステム を実施する上で必要と判断した記録	個人情報保護規程 A.3.5.1		

		チェック項目	関連する個人情報保護規程等の項番	判定	コメント
A.3.5.2文書かした情報（記録を除く。）の管理	(1)	規格が要求する全ての文書化した情報（記録を除く。）を管理する手順が、次のa)～c)の事項を含む内部規程として文書化されていること。 a）文書化した情報（記録を除く。）の発行及び改正に関すること b）文書化した情報（記録を除く。）の改正の内容と版数との関連付けを明確にすること c）必要な文書化した情報（記録を除く。）が必要なときに容易に参照できること	個人情報保護規程　A.3.5.2		
A.3.5.3文書化した情報のうち記録の管理	(1)	個人情報保護マネジメントシステム及びこの規格の要求事項への適合を実証するために必要な記録の管理についての手順が内部規程として文書化されていること。	個人情報保護規程　A.3.5.3		
A.3.6苦情及び相談への対応	(1)	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されていること。	個人情報保護規程　A.3.6		
	(2)	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の整備を行わなければならない旨を規定していること。	個人情報保護規程　A.3.6		
A.3.7.1運用の確認	(1)	各部門及び階層の管理者が定期的に、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ことを確認する手順、及び次の事項を含む是正処置の手順が内部規程として文書化されていること。 a)不適合の内容を確認する。 b)不適合の原因を特定し、是正処置を立案する。 c)期限を定め、立案された処置を実施する。 d)実施された是正処置の結果を記録する。 e)実施された是正処置の有効性をレビューする。	個人情報保護規程　A.3.7.1		
	(2)	運用の確認において、不適合が確認された場合は、是正処置を行わなければならない旨を規定していること。	個人情報保護規程　A.3.7.1		
	(3)	個人情報保護管理者は、定期的に、及び適宜にトップマネジメントに運用の確認の状況を報告しなければならない旨を規定していること。	個人情報保護規程　A.3.7.1		
A.3.7.2内部藍査	(1)	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が内部規程として文書化されていること。	個人情報保護規程　A.3.7.2		
	(2)	個人情報保護マネジメントシステムのこの規格への適合状況及び個人情報保護マネジメントシステムの運用状況を少なくとも年一回、適宜に監査しなければならない旨を規定していること。	個人情報保護規程　A.3.7.2		
	(3)	内部監査員は、自ら所属する部門を内部監査しないよう規定されていること。	個人情報保護規程　A.3.7.2		
A.3.7.3マネジメントレビュー	(1)	マネジメントレビューを実施する手順が内部規程として文書化されていること。	個人情報保護規程　A.3.7.3		
	(2)	少なくとも年一回、適宜にマネジメントレビューを実施するよう規定されていること。	個人情報保護規程　A.3.7.3		
	(3)	マネジメントレビューを実施するにあたり、次のa)～g)の事項がインプットされるよう規定していること。 a）監査及び個人情報保護マネジメントシステムの運用状況に関する報告 b）苦情を含む外部からの意見 c）前回までの見直しの結果に対するフォローアップ d）個人情報の取扱いに関する法令，国の定める指針その他の規範の改正状況 e）社会情勢の変化，国民の認識の変化，技術の進歩などの諸環境の変化 f）組織の事業領域の変化 g）内外から寄せられた改善のための提案	個人情報保護規程　A.3.7.3		
A、3.8是正処置	(1)	不適合に対する是正処置を確実に実施するための責任及び権限を定める手順が次の事項を含む内部規程として文書化されていること。 a)不適合の内容を確認する。 b)不適合の原因を特定し、是正処置を立案する。 c)期限を定め、立案された処置を実施する。 d)実施された是正処置の結果を記録する。 e)実施された是正処置の有効性をレビューする。	個人情報保護規程　A.3.8		

個人情報保護監査チェックリスト(運用状況の監査・保護管理者用)

監査責任者	監査人

被監査部門:個人情報保護管理者

監査人:部署名　業務　　氏名　線﨑 千里

監査実施日:　2022年11月22日

○:適合、×:不適合、—:該当なし

チェックポイント(質問事項)	確認方法・エビデンス	評価	監査記録・コメント	JISの要求事項	部門外の関連証憑等
A3.1.1 一般					
(1) A.3.2からA.3.8の管理策について定めた手段に従って承認していること又は承認のために定めた手段が説明できること	・個人情報保護管理者等による承認を得たことが確認できる記録 ・承認のために定めた手段の説明 - 個人情報保護運用チェックリスト - 内部監査計画書 - 個別監査計画書 - 内部監査報告書			A3.1.1　一般	
A.3.2.1 内部向け個人情報保護方針					
(1) トップマネジメントは個人情報保護目的を説明できること	・トップマネジメントによる説明 - 個人情報保護方針 - 個人情報に関する公表文 - 従業者個人情報の取扱いについて - 採用応募者の個人情報保護の取扱いについて			A.3.2.1　内部向け個人情報保護方針	
(2) トップマネジメントは内部向け個人情報保護方針を文書化した情報を組織内に伝達し必要に応じて利害関係者が入手可能にするための措置を講じていること	・トップマネジメントによる説明 - 個人情報保護方針 - 個人情報に関する公表文 - 採用応募者の個人情報保護の取扱いについて ・措置 - 就業規則 - 従業者個人情報の取扱いについて				
A.3.2.2 外部向け個人情報保護方針					
(1) トップマネジメントは外部向け個人情報保護方針を文書化した情報について一般の人が入手可能な措置を講じていること	・トップマネジメントによる説明 ・措置 - 個人情報保護方針 - 個人情報に関する公表文			A.3.2.2　外部向け個人情報保護方針	
A.3.3.1 個人情報の特定					
(1) 個人情報を管理するための台帳を整備していること	・個人情報の特定に関する記録(A.3.5.3a))			A.3.3.1　個人情報の特定	
(2) 個人情報の特定に関する記録(A.3.5.3a))	・個人情報の特定に関する記録(A.3.5.3a))				
A.3.3.2 法令、国が定める指針その他の規範					
(1) 法令等を特定し参照していること	・法令国が定める指針その他の規範の特定に関する記録(A.3.5.3b)) - 個人情報保護に関する法令規範一覧			A.3.3.2　法令、国が定める指針その他の規範	
A.3.3.3 リスクアセスメント及びリスク対策					
(1) 個人情報保護リスクを特定し分析していること	・個人情報保護リスクの認識分析及び対策に関する記録(A.3.5.3c)) - 個人情報リスク分析対策表			3.3.5　内部規程	
(2) 特定した個人情報保護リスクに対して現状で実施し得る対策が講じられていること	・運用の確認の記録(A.3.5.3i)) - 個人情報保護運用チェックリスト				
(3) 未対応部分を残留リスクとして把握し管理していること	・個人情報保護リスクの認識分析及び対策に関する記録(A.3.5.3c)) - 個人情報リスク分析対策表				
(4) 個人情報保護リスクの特定分析及び講じた個人情報保護リスク対策を少なくとも年一回適宜に見直していること	・個人情報保護リスクの認識分析及び対策に関する記録(A.3.5.3c)) - 個人情報リスク分析対策表				
A.3.3.4 資源役割責任及び権限					
(1) トップマネジメントが個人情報保護のための人的資源を説明できること	トップマネジメントによる説明 - 個人情報保護体制図 - 緊急連絡網			A.3.3.4　資源役割責任及び権限	
(2) 個人情報保護幣杏責任者と個人情報保護管理者とは異なる者であること	・体制 - 個人情報保護体制図				
A.3.3.5 内部規程					
(1) 事業の内容に応じて個人情報保護マネジメントシステムが確実に適用されるように内部規程を改正していること	・内部規程の更新履歴 - 内部監査報告書			A.3.3.5　内部規程	
A.3.3.6 計画策定					
(1) 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少な〈とも年一回次の事項を含めて必要な計画を立案し文書化していること a)教育実施計画 b)内部監査実施計画	・計画書(A.3.5.3d)) - 内部監査計画書 - 個別監査計画書 - 個人情報保護教育計画書			A.3.3.6　計画策定	
A.3.3.7 緊急事態への準備					
(1) A.3.3.7緊急事態への準備	・運用の確認の記録(A.3.5.3i)) (例) ・緊急事態に対応した記録 - 個人情報保護体制図 - 緊急連絡網 - 緊急事態対応記録			A.3.3.7　緊急事態への準備	

○:適合、×:不適合、—:該当なし

チェックポイント(質問事項)		確認方法・エビデンス	評価	監査記録・コメント	JISの要求事項	部門外の関連証憑等
A.3.4.2.1 利用目的の特定						
(1)	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こと	個人情報の特定に関する記録(A、3.5.3a)) – 個人情報管理台帳 ・利用目的の特定に関する記録(A.3.5.3e)) – 個人情報管理台帳 ・通知又は公表の記録(A.3.4.2.4) ・本人に明示した書面(A.3.4.2.5)			A.3.4.2.1 利用目的の特定	
(2)	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こと	・利用目的の特定に関する記録(A、3.5.3e)) – 個人情報管理台帳 – 個人情報リスク分析対策表 ・通知又は公表の記録(A.3.4.2.4) ・本人に明示した書面(A.3.4.2.5) – 個人情報保護方針				
A.3.4.2.2 適正な取得						
(1)	定めた手順に従って個人情報を適正に取得していること	・個人情報の取得利用及び提供に関する規定(A.3.3.5f)) – 保有個人データ開示等請求書 ・通知又は公表の記録(A.3.4.2.4) ・本人に明示した書面(A、3.4.2.5) – 個人情報保護方針 – 個人情報に関する公表文 ・個人情報の特定に関する記録(A.3.5.3a)) – 個人情報管理台帳			A.3.4.2.2 適正な取得	
A.3.4.2.3 要配慮個人情報						
(1)	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こと	・本人の同意書面 – 従業者個人情報の取扱いについて例外事項により同意は得ていない			A.3.4.2.3 要配慮個人情報	
A.3.4.2.4 個人情報を取得した場合の措置						
(1)	個人情報を取得する場合個人情報の取得の場面に応じてあらかじめその利用目的を公表している又は取得後速やかにその利用目的を本人に通知又は公表していること	・通知又は公表の記録(A.3.4.2.4) – 個人情報保護方針 – 個人情報に関する公表文 – 新規個人情報取得申請書 – 個人情報取扱変更等申請書			A.3.4.2.4 個人情報を取得した場合の措置	
A.3.4.2.5 A.3.4.2.4のうち本人から直接書面によって取得する場合の措置						
(1)	本人から直接書面によって取得する場合A.3.4.2.4の措置を講じていること	・通知又は公表の記録(A、3.4.2.4)等 – 個人情報保護方針 – 個人情報に関する公表文 – 新規個人情報取得申請書			A.3.4.2.5 A.3.4.2.4のうち本人から直接書面によって取得する場合の措置	
(2)	本人から書面に記載された個人情報を直接取得する場合には少なくとも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書面によって本人に明示し書面によって本人の同意を得ていること a)組織の名称又は氏名 b)個人情報保護管理者(若しくはその代理人)の氏名又は職名所属及び連絡先 c)利用目的 d)個人情報を第三者に提供することが予定される場合の事項 －第三者に提供する目的 －提供する個人情報の項目 －提供の手段又は方法 －当該情報の提供を受ける者又は提供を受ける者の組織の種類及び属性 －個人情報の取扱いに関する契約がある場合はその旨 e)個人情報の取扱いの委託を行うことが予定される場合にはその旨 f)A、3.4.4.4～A.3.4.4.7に該当する場合にはその請求等に応じる旨及び問合せ窓口 g)本人が個人情報を与えることの任意性及び当該情報を与えなかった場合に本人に生じる結果 h)本人が容易に知覚できない方法によって個人情報を取得する場合にはそ	・本人に明示した書面(A.3.4.2.5) – 個人情報保護方針 – 個人情報に関する公表文 ・本人の同意書面 – 従業者個人情報の取扱いについて				
A.3.4.2.6 利用に関する措置						
(1)	特定した利用目的の達成に必要な範囲内で個人情報を利用していること	・通知又は公表の記録(A.3.4.2.4)又は本人に明示した書面(A.3.4.2.5) – 個人情報保護方針 – 個人情報に関する公表文 ・個人情報の特定に関する記録(A.3.5.3a)) – 個人情報管理台帳			A.3.4.2.6 利用に関する措置	
	特定した利用目的の達成に必要な範囲を超えて個人情報を利用する場合はあらかじめ少なくともA.3.4.2.5のa)～f)に示す事項又はそれと同等以上の内容の事項を本人に通知し本人の同意を得ていること	・本人への通知書面(A.3.4.2.6) – 個人情報保護方針 – 個人情報に関する公表文 ・本人の同意書面 – 従業者個人情報の取扱いについて				

○:適合、×:不適合、—:該当なし

チェックポイント(質問事項)		確認方法・エビデンス	評価	監査記録・コメント	JISの要求事項	部門外の関連証憑等
A.3.4.2.7 本人に連絡又は接触する場合の措置						
(1)	個人情報を利用して本人に連絡又は接触する場合には本人に対してA.3.4.2.5のa)～f)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こと	・本人への通知書面(A.3.4.2.7) ・本人の同意書面			A.3.4.2.7 本人に連絡又は接触する場合の措置	
(2)	共同して利用する者から個人情報を取得する場合であって共同して利用する者がA.3.4.2.7d)の措置を講じない場合本人に対してA.3.4.2.5のa)～f)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こと	・本人への通知書面(A.3.4.2.7) ・本人の同意書面				
A.3.4.2.8 個人データの提供に関する措置						
(1)	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A.3.4.2.5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こと	・本人への通知書面(A.3.4.2.8) ・本人の同意書面 - 個人情報保護方針 - 個人情報に関する公表文 - 保有個人データ開示等請求書			A.3.4.2.8 個人データの提供に関する措置	
(1)	個人データを共同利用している場合共同して利用する者の間でA、3.4.2.7に規定する共同利用について契約によって定めていること	・共同利用についての契約(A.3.4.2.8f)) - 個人情報保護方針 - 個人情報に関する公表文				
A.3.4.2.8.1 外国にある第三者への提供の制限						
(1)	外国にある第三者に個人データを提供する場合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を得ていること	・本人の同意書面	-		A.3.4.2.8. 外国にある第三者への提供の制限	
A.3.4.2.8.2 第三者提供に係る記録の作成など						
(1)	個人データを第三者に提供した場合記録を作成保管していること	・作成した記録(書面又は電子データ・記録すべき事項がログIPアドレスなどの一定の情報を分析することによって明らかになる場合にはその状態) - 保有個人データ開示等請求書			A.3.4.2.8. 第三者提供に係る記録の作成など	
A.3.4.2.8.3 第三者提供を受ける際の確認など						
(1)	第三者から個人データの提供を受けるに際しては確認を行った記録を作成し保管していること	・作成した記録 - 新規個人情報取得申請書 - 個人情報取扱変更等申請書			A.3.4.2.8. 第三者提供を受ける際の確認など	
A.3.4.3.1 正確性の確保						
(1)	個人データを正確かつ最新の状態で管理していること	個人情報の適正管理に関する規定(A.3.3.59))に定めた記録 - 個人情報管理台帳 - 新規個人情報取得申請書 - 個人情報取扱変更等申請書			A.3.4.3.1 正確性の確保	
(2)	利用する必要がなくなった個人データを消去していること	・個人情報の特定に関する記録(A.3.5.3a)) ・個人情報の適正管理に関する規定(A.3.3.59))に定めた記録 - 個人情報管理台帳				
A.3.4.3.2 安全管理措置						
(1)	取り扱う個人情報の個人情報保護リスクに応じた安全管理措置を講じていること	個人情報保護リスクの認識分析及び対策に関する記録(A.3.5.3c)) - 個人情報管理台帳 - 個人情報リスク分析対策表 ・内部規程(A.3.3.5a)～o)含む) ・内部規程に定めた記録 ・内部規程に定めた措置の実施状況 - 内部監査計画書 - 個別監査計画書 - 個人情報保護教育計画書 - 個人情報保護運用チェックリスト - 内部監査報告書 - マネジメントレビュー記録 - 是正処置実施記録			A.3.4.3.2 安全管理措置	
A.3.4.3.3 従業者の監督						
(1)	個人データを取扱う従業者に対して必要かつ適切な監督を行っていること	個人情報の適正管理に関する規定(A.3.3.59))に定めた管理手段 - 就業規則 - 個人情報保護教育計画書 - 個人情報保護教育受講者名簿 - 個人情報保護教育実施記録			A.3.4.3.3 従業者の監督	

○:適合、×:不適合、—:該当なし

	チェックポイント(質問事項)	確認方法・エビデンス	評価	監査記録・コメント	JISの要求事項	部門外の関連証憑等
A.3.4.3.4 委託先の監督						
(1)	委託先選定基準に基づいて委託先を選定している	・委託先の選定記録 – 個人情報委託先審査票 – 個人情報委託先管理台帳 – 委託先が公表している個人情報保護方針			A.3.4.3.4 委託先の監督	
(2)	委託先と特定した利用目的の範囲内で委託契約を締結していること	・委託した個人情報の利用目的が確認できる記録 – 個人情報委託先審査票 – 個人情報委託先管理台帳 – 個人情報取扱の委託に関する覚書				
(3)	次に示す事項が盛り込まれた契約を締結していること 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	・委託契約書など – 個人情報委託先管理台帳 – 個人情報取扱の委託に関する覚書 – 個人情報管理台帳 – 個人情報リスク分析対策表 – 委託先が公表している個人情報保護方針				
(4)	全ての委託先が漏れなく特定されていること	・個人情報の取扱いを委託している事業者を確認できる記録 – 個人情報委託先管理台帳				
(5)	委託契約書が当該個人データの保有期間にわたって保存されていること	・委託した個人情報の利用目的が確認できる記録 – 個人情報委託先管理台帳 – 個人情報管理台帳				
(6)	委託契約に基づき委託先を適切に監督していること	委託契約書・委託先の監督に関する記録 (例) ・A.3.4.3.4のa)～h)の実施の記録 – 個人情報委託先審査票 – 個人情報委託先管理台帳				
A.3.4.4.1 個人情報に関する権利						
(1)	本人から開示等の請求等を受け付けた場合政令で定める期間以内に消去する個人情報も含めてA.3.4.4.4～A.3.4.4.7の規定によって遅滞なくこれに応じていること	保有個人データに関する開示等(利用目的の通知開示内容の訂正追加又は削除利用の停止又は消去第三者提供の停止)の請求等への対応記録(A.3.5.3f)) – 個人情報保護規程 – 個人情報保護体制図 – 保有個人データ開示等請求書			A.3.4.4.1 個人情報に関する権利	
A.3.4.4.2 開示等の請求等に応じる手続						
(1)	保有個人データの開示等の請求等に応じる手続を定めるに当たっては本人に過重な負担を課するものとならないよう配慮していること	・配慮している事項の説明 – 個人情報保護規程			A.3.4.4.2 開示等の請求等に応じる手続	
(2)	本人からの請求などに応じる場合に手数料を徴収するときは実費を勘案して合理的であると認められる範囲内においてその額を定めていること	・手数料の額を定めた根拠の説明 – 個人情報保護規程				
A.3.4.4.4 保有個人データの利用目的の通知						
(1)	本人から当該本人が識別される保有個人データについて利用目的の通知を求められた場合遅滞なくこれに応じていること	保有個人データに関する開示等(利用目的の通知開示内容の訂正追加又は削除利用の停止又は消去第三者提供の停止)の請求等への対応記録(A.3.5.3f)) – 個人情報保護規程 – 個人情報保護体制図 – 保有個人データ開示等請求書			A.3.4.4.4 保有個人データの利用目的の通知	
(2)	本人から当該本人が識別される保有個人データについて利用目的の通知を求められた場合であって利用目的の通知を必要としないのは以下の場合に限定していること A.3.4.2.4のただし書きa)～c)のいずれかに該当する場合 A.3.4.4.3のc)によって当該本人が識別される保有個人データの利用目的が明らかな場合	・保有個人データに関する開示等(利用目的の通知開示内容の訂正追加又は肖リ除利用の停止又は消去第三者提供の停止)の請求等への対応記録 (A.3.5.3f)) ・利用目的の通知を求められたが通知をしていない保有個人データがある場合A.3.4.4.4のただし書きに該当していることの説明 – 個人情報保護規程 – 個人情報保護体制図				
(3)	A, 3.4.4.4のただし書きのいずれかに該当する場合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こと	・保有個人データに関する開示等(利用目的の通知開示内容の訂正追加又は削除利用の停止又は消去第三者提供の停止)の請求等への対応記録 (A.3.5.3f)) – 個人情報保護規程 – 個人情報保護体制図				
A.3.4.4.5 保有個人データの開示						
(1)	本人から当該本人が識別される保有個人データの開示の請求を受けた場合法令の規定によって特別の手続が定められている場合を除き本人に対し遅滞なく書面によって開示していること	・保有個人データに関する開示等(利用目的の通知開示内容 の訂正追加又は削除利用の停止又は消去第三者提供の停止)の請求等への対応記録(A.3.5.3f))			A.3.4.4.5 保有個人データの開示	
(2)	A.3.4.4.5のただし書きのいずれかに該当する場合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こと	保有個人データに関する開示等(利用目的の通知開示内容の訂正追加又は削除利用の停止又は消去第三者提供の停止)の請求等への対応記録(A.3.5.3f))				

○:適合、×:不適合、—:該当なし

チェックポイント(質問事項)		確認方法・エビデンス	評価	監査記録・コメント	JISの要求事項	部門外の関連証憑等
A.3.4.4.6 保有個人データの訂正，追加又は削除						
(1)	本人から当該本人が識別される保有個人データの訂正等(訂正追加又は削除)の請求を受けた場合法令の規定により特別の手続が定められている場合を除き利用目的の達成に必要な範囲内において遅滞なく必要な調査を行いその結果に基づいて当該保有個人データの訂正等を行っていること	・保有個人データに関する開示等(利用目的の通知開示内容の訂正追加又は削除利用の停止又は消去第三者提供の停止)の請求等への対応記録(A.3.5.3f)) - 個人情報保護規程 - 個人情報保護体制図 - 保有個人データ開示等請求書			A.3.4.4.6 保有個人データの訂正，追加又は削除	
(2)	本人から保有個人データの訂正等の請求を受けて訂正等を行った場合はその旨及びその内容を本人に遅滞なく通知していること	保有個人データに関する開示等(利用目的の通知開示内容の訂正追加又は削除利用の停止又は消去第三者提供の停止)の請求等への対応記録(A.3.5.3f)) - 個人情報保護規程 - 個人情報保護体制図				
(3)	本人から保有個人データの訂正等の請求を受けたが応じなかった場合その旨及びその理由を本人に遅滞なく通知していること	保有個人データに関する開示等(利用目的の通知開示内容の訂正追加又は削除利用の停止又は消去第三者提供の停止)の請求等への対応記録(A.3.5.3f)) - 個人情報保護規程 - 個人情報保護体制図				
A.3.4.4.7 保有個人データの利用又は提供の拒否権						
(1)	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こと	保有個人データに関する開示等(利用目的の通知開示内容の訂正追加又は削除利用の停止又は消去第三者提供の停止)の請求等への対応記録(A.3.5.3f)) - 個人情報保護規程 - 個人情報保護体制図 - 保有個人データ開示等請求書			A.3.4.4.7 保有個人データの利用又は提供の拒否権	
(2)	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こと	・保有個人データに関する開示等(利用目的の通知開示内容の訂正追加又は削除利用の停止又は消去第三者提供の停止)の請求等への対応記録(A.3.5.3f)) - 個人情報保護規程 - 個人情報保護体制図				
(3)	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A.3.4.4.5のa)～c)に該当する場合に限定していること	・保有個人データに関する開示等(利用目的の通知開示内容の訂正追加又は削除利用の停止又は消去第三者提供の停止)の請求等への対応記録(A.3.5.3f)) ・保有個人データの利用停止等の請求を受けていない保有個人データがある場合A.3.4.4.5のただし書きに該当していることの説明 - 個人情報保護規程 - 個人情報保護体制図				
(4)	A.3.4.4.5のa)～c)のいずれかに該当する場合本人に遅滞なくその旨通知するとともに理由を説明していること	保有個人データに関する開示等(利用目的の通知開示内容の訂正追加又は削除利用の停止又は消去第三者提供の停止)の請求等への対応記録(A.3.5.3f)) - 個人情報保護規程 - 個人情報保護体制図				
A.3.4.5 認識						
(1)	教育実施計画(A.3.3.6a))に従って教育を実施していること	計画書(A.3.5.3d)) ・教育などの実施記録(A.3.5.39)) - 個人情報保護教育計画書 - 個人情報保護教育受講者名簿 - 個人情報保護教育実施記録			A.3.4.5 認識	
(2)	全ての従業者に対してa)～d)の内容を認識させていること a)個人情報保護方針(内部向け個人情報保護方針及び外部向け個人情報保護方針) b)個人情報保護マネジメントシステムに適合することの重要性及び利点 c)個人情報保護マネジメントシステムに適合するための役割及び責任 d)個人情報保護マネジメントシステムに違反した際に予想される結果	・使用した教材等 - 個人情報保護教育計画書 - 個人情報保護教育受講者名簿 - 個人情報保護教育実施記録				
(3)	受講者の理解度確認を実施していること	・教育などの実施記録(A、3.5.39)) - 個人情報保護教育実施記録				

○:適合、×:不適合、—:該当なし

チェックポイント(質問事項)		確認方法・エビデンス	評価	監査記録・コメント	JISの要求事項	部門外の関連証憑等
A.3.5.1 文書化した情報の範囲						
(1)	個人情報保護マネジメントシステムの基本となる次の要素に対応する書面があること a)内部向け個人情報保護方針 b)外部向け個人情報保護方針 c)内部規程d)内部規程に定める手順上で使用する様式 e)計画書 f)この規格が要求する記録及び組織が個人情報保護マネジメントシステムを実施する上で必要と判断した記録	個人情報保護マネジメントシステムの基本となる要素を記述したa)～f)に関する書面 ・内部向け個人情報保護方針を文書化した情報 - 個人情報保護方針 - 就業規則 - 従業者個人情報の取扱いについて ・外部向け個人情報保護方針を文書化した情報 - 個人情報保護方針 - 個人情報保護規程 - 個人情報に関する公表文 ・内部規程(A.3.3.5a)～o)を含む)を文書化した情報及び当該内部規程で規定された様式一式 - PMS文書体系表 - PMS記録管理シート ・計画書(A.3.5.3d)) - 内部監査計画書 - 個別監査計画書 ・記録各種 - 内部監査報告書 - マネジメントレビュー記録 - 是正処置実施記録			A.3.5.1 文書化した情報の範囲	
A.3.5.2 文書化した情報(記録を除く)の管理						
(1)	文書化した情報(記録を除く)の管理を実施していること	・文書化した情報の更新履歴・文書化した情報の管理状況 ・文書化した情報を従業者が参照する環境			A.3.5.2 文書化した情報(記録を除く)の管理	
(2)	文書化した情報(記録を除く)は次の事項を確実にするよう管理されていること a)文書化した情報が必要な時に必要な所で入手可能かつ利用に適した状態である b)文書化した情報が十分に保護されている(例えば機密性の喪失不適切な使用及び完全性の喪失からの保護)	・文書化した情報の管理状況 - PMS文書体系表				
A.3.5.3 文書化した情報のうち記録の管理						
(1)	次の事項を含む必要な記録を作成していること a)個人情報の特定に関する記録 b)法令国が定める指針及びその他の規範の特定に関する記録 c)個人情報保護リスクの認識分析及び対策に関する記録 d)計画書 e)利用目的の特定に関する記録 f)保有個人データに関する開示等(利用目的の通知開示内容の訂正追加又は削除矛|用の停止又は消去第三者提供の停止)の請求等への対応記録 g)教育などの実施記録 h)苦情及び相談への対応記録 i)運用の確認の記録 j)内部監査報告書 k)是正処置の記録 l)マネジメントレビューの記録	a)～l)の記録 - 個人情報管理台帳 - 個人情報保護に関する法令規範一覧表 - 個人情報リスク分析対策表 - 内部監査計画書 - 個別監査計画書 - 個人情報保護教育計画書 - 新規個人情報取得申請書 - 個人情報取扱変更等申請書 - 保有個人データ開示等請求書 - 苦情・相談等受付処理票 - 個人情報保護教育受講者名簿 - 個人情報保護教育実施記録 - 苦情・相談等受付処理票 - 個人情報保護運用チェックリスト - 入退受付票 - 内部監査計画書 - 個別監査計画書 - 内部監査報告書 - 是正処置実施記録			A.3.5.3 文書化した情報のうち記録の管理	
(2)	記録は次の事項を確実にするよう管理されていること a)記録が必要な時に必要な所で入手可能かつ利用に適した 状態である b)記録が十分に保護されている(例えば機密性の喪失不適切な 使用及び完全性の喪失からの保護)	a)～l)の記録の管理状況 - PMS記録管理シート - 個人情報保護運用チェックリスト - 入退受付票 - 内部監査計画書 - 個別監査計画書 - 内部監査報告書				
A.3.6 苦情及び相談への対応						
(1)	苦情及び相談への対応を実施していること	苦情及び相談への対応記録(A.3.5.3h)) - 苦情・相談等受付処理票			A.3.6 苦情及び相談への対応	
(2)	苦情の申立て先が本人にとって明確であること	保有個人データに関する事項を周知している措置(A.3.4.4.3) - 個人情報に関する公表文				
(3)	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こと	保有個人データに関する事項を周知している措置 (A.3.4.4.3) - 個人情報保護規程 - 個人情報に関する公表文 - 保有個人データ開示等請求書	—			
(4)	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の整備を行っていること	体制 (例) ・体制図 - 個人情報に関する公表文 - 個人情報保護体制図				

○:適合、×:不適合、—:該当なし

チェックポイント(質問事項)		確認方法・エビデンス	評価	監査記録・コメント	JISの要求事項	部門外の関連証憑等
A.3.7.1 運用の確認						
(1)	運用の確認を実施していること	・運用の確認の記録(A.3.5.3i)) - 内部監査計画書 - 個別監査計画書 - 個人情報保護教育実施記録 - 個人情報保護運用チェックリスト - 内部監査報告書			A.3.7.1 運用の確認	
(2)	運用の確認において不適合が確認された場合は是正処置を行っていること	・運用の確認の記録(A、3.5.3i)) - 是正処置実施記録				
(3)	個人情報保護管理者は定期的に及び適宜にトップマネジメントに運用の確認の状況を報告していること	・運用の確認の記録(A、3.5.3i)) - マネジメントレビュー記録				
A.3.7.2 内部監査						
(1)	内部監査実施計画(A.3.3.6b))に従って個人情報保護マネジメントシステムのこの規格への適合状況及び個人情報保護マネジメントシステムの運用状況の監査を少なくとも年一回適宜に実施していること	・計画書(A、3.5.3d)) - 内部監査計画書 ・内部監査報告書(A.3.5.3j)) - 内部監査報告書			A.3.7.2 内部監査	
(2)	内部監査の実施にあたっては内部規程とこの規格との適合状況を監査していること	監査項目 ・監査チェックリスト - 個人情報保護運用チェックリスト				
(3)	内部監査の実施にあたっては運用状況の監査を実施していること	監査項目 ・監査チェックリスト - 個人情報保護運用チェックリスト				
(4)	監査員は自己の所属する部署の内部監査を実施していないこと	・計画書(A.3.5.3d)) - 内部監査計画書 ・内部監査報告書(A.3.5.3j)) - 内部監査報告書				
(5)	個人情報保護監査責任者は監査報告書を作成しトップマネジメントに報告していること	・計画書(A.3.5.3d)) - 内部監査計画書 ・内部監査報告書(A.3.5.3j)) - 内部監査報告書				
A.3.7.3 マネジメントレビュー						
(1)	少なくとも年一回適宜にマネジメントレビューを実施していること	・マネジメントレビューの記録(A.3.5.31)) - マネジメントレビュー記録			A.3.7.3 マネジメントレビュー	
(2)	マネジメントレビューを実施するにあたり次の事項がインプットされていること a)監査及び個人情報保護マネジメントシステムの運用状況に関する報告 b)苦情を含む外部からの意見 c)前回までの見直しの結果に対するフォローアップ d)個人情報の取扱いに関する法令国の定める指針その他の規範の改正状況 e)社会情勢の変化国民の認識の変化技術の進歩などの諸環境の変化 f)組織の事業領域の変化 g)内外から寄せられた改善のための提案	・マネジメントレビューの記録(A.3.5.31)) - 内部監査報告書 - 是正処置実施記録 - マネジメントレビュー記録 - 苦情・相談等受付処理票 - 個人情報保護に関する法令規範一覧表 - 個人情報保護規程 - 就業規則				
(2)	マネジメントレビュー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が含まれていること	・マネジメントレビューの記録(A、3.5.31)) ・トップマネジメントによる説明 - マネジメントレビュー記録				
A、3.8 是正処置						
(1)	不適合が明らかになった場合a)～e)の事項を実施していること	・是正処置の記録(A.3.5.3k)) - 是正処置実施記録			A、3.8 是正処置	
(2)	是正処置の立案にあたっては発見された不適合が他の所でも発生しないようにするための措置を検討していること	・是正処置の記録(A.3.5.3k)) - 是正処置実施記録				
(3)	個人情報保護マネジメントシステムを継続的に改善していること	・トップマネジメントによる説明 ・マネジメントシステムの改善履歴 ・マネジメントレビューの記録(A.3.5.31)) - マネジメントレビュー記録 ・是正処置の記録(A.3.5.3k)) - 是正処置実施記録 ・内部規程の改廃履歴 - 内部監査計画書 - 個別監査計画書 - 内部監査報告書				

個人情報保護監査チェックリスト(運用状況の監査・部門用)

被監査部門: 管理　　監査人: 線﨑 千里

監査実施日: 2022年11月22日　　個人情報内部監査責任者: 線﨑 千里

○:適合、×:不適合、—:該当なし

チェックポイント(質問事項)	監査手続	評価	監査記録・コメント	個人情報保護規程 関連項番
個人情報の特定				
(1) 特定漏れはありませんか (他部門で、〇〇が漏れていました)	【閲覧】個人情報管理台帳			
安全管理措置(リスク分析から)				
取得・入力				
(1) FAX受信後、原稿は速やかに回収(周知徹底)	FAX			個人情報保護規程 A.3.4.3.2 b) 4)⑤
(2) ポストに施錠	郵送・宅配			個人情報保護規程 A.3.4.3.2 b) 4)②
(3) 本人確認の徹底	ﾏｲﾅﾝﾊﾞｰ			個人情報保護規程 A.3.4.2.2
利用・加工				
(1) アクセス権の設定、ID/PWの管理	電子			個人情報保護規程 A.3.4.3.2 c) 9)
(2) PWの管理および定期的な変更	電子			個人情報保護規程 A.3.4.3.2 c) 8)
(3) 複製は最小限にとどめる、複製の管理				個人情報保護規程 A.3.4.3.2 b) 2)
(4) クリアデスクの徹底	紙			個人情報保護規程 A.3.4.3.2 b) 1)
(5) クリアスクリーンの徹底				個人情報保護規程 A.3.4.3.2 c) 13)
(6) 入力結果のチェック手順策定と実施				個人情報保護規程 A.3.4.3.1
(7) 取扱担当者の限定	ﾏｲﾅﾝﾊﾞｰ			個人情報保護規程 A.3.3.4 i)
(8) 取扱いPC・エリアの限定	ﾏｲﾅﾝﾊﾞｰ			個人情報保護規程 A.3.4.3.2 b) 3)①
移送・送信				
(1) 移動中は手放さないよう徹底	手渡し			個人情報保護規程 A.3.4.3.2 b) 4)1)
(2) 無用な立ち寄りをしないよう徹底	手渡し			個人情報保護規程 A.3.4.3.2 b) 4)1)
(3) 書留等の利用	郵送・宅配			個人情報保護規程 A.3.4.3.2 b) 4)2)
(4) 短縮ダイヤルの登録 FAX番号のWチェック	FAX			個人情報保護規程 A.3.4.3.2 b) 4)④
(5) FAX送信後、原稿は速やかに回収(周知徹底)	FAX			個人情報保護規程 A.3.4.3.2 b) 4)④
(6) 暗号化またはパスワード付与	電子ﾒｰﾙ			個人情報保護規程 A.3.4.3.2 c) 16) ②
保管・ﾊﾞｯｸｱｯﾌﾟ				
(1) 施錠管理、入退制限				個人情報保護規程 A.3.4.3.2 a) 4)
(2) 施錠保管の徹底	紙			個人情報保護規程 A.3.4.3.2 b) 3)③
(3) 火気を取り扱わない、禁煙、消火器の設置				個人情報保護規程 A.3.4.3.2 b) 3)⑥
(4) ウィルス対策ソフトの導入	電子			個人情報保護規程 A.3.4.3.2 c) 3)①
(5) 定期的ﾊﾞｯｸｱｯﾌﾟ	電子			個人情報保護規程 A.3.4.3.2 c) 1)①
(6) 記憶媒体の利用制限	記憶媒体			個人情報保護規程 A.3.4.3.2 c) 17)
消去・廃棄				
(1) 保管期間を確認する				個人情報保護規程 A.3.4.3.2 b) 3)⑤
(2) シュレッダー利用	紙			個人情報保護規程 A.3.4.3.2 b) 6)①
(3) データ消去簿を作成し、記録	ﾏｲﾅﾝﾊﾞｰ			個人情報保護規程 A.3.4.3.2 b) 6)⑤
委託				
(1) 委託先管理台帳で確認する				個人情報保護規程 A.3.4.3.4 k)
共通				
(1) 担当者個人の判断で対応をしない。				個人情報保護規程 A.3.6 b) 2)

個人情報保護監査チェックリスト(運用状況の監査・部門用)

被監査部門: 業務　　監査人: 曽田 健嗣

監査実施日: 2022年11月22日　　個人情報内部監査責任者: 曽田 健嗣

○:適合、×:不適合、—:該当なし

チェックポイント(質問事項)	監査手続	評価	監査記録・コメント	個人情報保護規程 関連項番
個人情報の特定				
(1) 特定漏れはありませんか (他部門で、〇〇が漏れていました)	【閲覧】個人情報管理台帳			
安全管理措置(リスク分析から)				
取得・入力				
(1) FAX受信後、原稿は速やかに回収(周知徹底)	FAX			個人情報保護規程 A.3.4.3.2 b) 4)⑤
利用・加工				
(1) アクセス権の設定、ID/PWの管理	電子			個人情報保護規程 A.3.4.3.2 c) 9)
(2) PWの管理および定期的な変更	電子			個人情報保護規程 A.3.4.3.2 c) 8)
(3) 複製は最小限にとどめる、複製の管理				個人情報保護規程 A.3.4.3.2 b) 2)
(4) クリアデスクの徹底	紙			個人情報保護規程 A.3.4.3.2 b) 1)
(5) クリアスクリーンの徹底				個人情報保護規程 A.3.4.3.2 c) 13)
(6) 入力結果のチェック手順策定と実施				個人情報保護規程 A.3.4.3.1
移送・送信				
(1) 移動中は手放さないよう徹底	手渡し			個人情報保護規程 A.3.4.3.2 b) 4) 1)
(2) 無用な立ち寄りをしないよう徹底	手渡し			個人情報保護規程 A.3.4.3.2 b) 4) 1)
(3) 書留等の利用	郵送・宅配			個人情報保護規程 A.3.4.3.2 b) 4) 2)
(4) 短縮ダイヤルの登録 FAX番号のWチェック	FAX			個人情報保護規程 A.3.4.3.2 b) 4)④
(5) FAX送信後、原稿は速やかに回収(周知徹底)	FAX			個人情報保護規程 A.3.4.3.2 b) 4)④
(6) 暗号化またはパスワード付与	電子ﾒｰﾙ			個人情報保護規程 A.3.4.3.2 c) 16) ②
保管・ﾊﾞｯｸｱｯﾌﾟ				
(1) 施錠管理、入退制限				個人情報保護規程 A.3.4.3.2 a) 4)
(2) 施錠保管の徹底	紙			個人情報保護規程 A.3.4.3.2 b) 3)③
(3) 火気を取り扱わない、禁煙、消火器の設置				個人情報保護規程 A.3.4.3.2 b) 3)⑥
(4) ウィルス対策ソフトの導入	電子			個人情報保護規程 A.3.4.3.2 c) 3)①
(5) 定期的ﾊﾞｯｸｱｯﾌﾟ	電子			個人情報保護規程 A.3.4.3.2 c) 1)①
(6) 記憶媒体の利用制限	記憶媒体			個人情報保護規程 A.3.4.3.2 c) 17)
消去・廃棄				
(1) 保管期間を確認する				個人情報保護規程 A.3.4.3.2 b) 3)⑤
(2) シュレッダー利用	紙			個人情報保護規程 A.3.4.3.2 b) 6)①
委託				
(1) 委託先管理台帳で確認する				個人情報保護規程 A.3.4.3.4 k)
共通				
(1) 担当者個人の判断で対応をしない。				個人情報保護規程 A.3.6 b) 2)