監査チェックシート

個人情報保護マネジメントシステムJIS適合状況監査チェックシート

作成日付	2018/8/25
実施日	
実施者	

大分類	JIS内容	監査部門チェック			
		記載規程	条項	適否	コメント
A.3.1 一般	A3.1.1 一般 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。				
A.3.2 個人情報保護方針	A.3.2.1 内部向け個人情報保護方針 トップマネジメントは，5.2.1 e) に規定する内部向け個人情報保護方針を文書化した情報には次の事項を含めなければならない。 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[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 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なければならない。				
	A.3.2.2 外部向け個人情報保護方針 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は，A.3.2.1に規定する内部向け個人情報保護方針の事項に加えて，次の事項も明記しなければならない。 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 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，一般の人が知り得るようにするための一般の人が入手可能な措置を講じなければならない。				

監査チェックシート

個人情報保護マネジメントシステムJIS適合状況監査チェックシート

作成日付	2018/8/25
実施日	
実施者	

大分類	JIS内容	監査部門チェック			
		記載規程	条項	適否	コメント
A.3.3 計画	A.3.3.1 個人情報の特定 組織は，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確立し，かつ，維持しなければならない。 組織は，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，保管期限などを記載した，個人情報を管理するための台帳を整備するとともに，当該台帳の内容を少なくとも年一回，適宜に確認し，最新の状態で維持されるようにしなければならない。 組織は，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。				
	A.3.3.2 法令，国が定める指針その他の規範 組織は，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を確立し，かつ，維持しなければならない。				
	A.3.3.3 リスクアセスメント及びリスク対策 組織は，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，維持しなければならない。 組織は，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を確立し，かつ，維持しなければならない。 組織は，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，管理しなければならない。 組織は，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，適宜に見直さなければならない。				

監査チェックシート

個人情報保護マネジメントシステムJIS適合状況監査チェックシート

作成日付	2018/8/25
実施日	
実施者	

大分類	JIS内容	監査部門チェック			
		記載規程	条項	適否	コメント
	A.3.3.4　資源，役割，責任及び権限 トップマネジメントは，少なくとも，次の責任及び権限を割り当てなければならない。 a)個人情報保護管理者 b)個人情報保護監査責任者 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。 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しなければならない。 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。 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しなければならない。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なければならない。 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なければならない。				

監査チェックシート

個人情報保護マネジメントシステムJIS適合状況監査チェックシート

作成日付	2018/8/25
実施日	
実施者	

大分類	JIS内容	監査部門チェック			
		記載規程	条項	適否	コメント
	A.3.3.5　内部規程 組織は，次の事項を含む内部規程を文書化し，かつ，維持しなければならない。 a)個人情報を特定する手順に関する規定 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 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 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 e)緊急事態への準備及び対応に関する規定 f)個人情報の取得，利用及び提供に関する規定 g)個人情報の適正管理に関する規定 h)本人からの開示等の請求等への対応に関する規定 i)教育などに関する規定 j)文書化した情報の管理に関する規定 k)苦情及び相談への対応に関する規定 l)点検に関する規定 m)是正処置に関する規定 n)マネジメントレビューに関する規定 o)内部規程の違反に関する罰則の規定 組織は，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。				
	A.3.3.6　計画策定 組織は，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，必要な計画を立案し，文書化し，かつ，維持しなければならない。 a)A.3.4.5に規定する事項を踏まえた教育実施計画の立案及びその文書化 b)　A.3.7.2に規定する事項を踏まえた内部監査実施計画及びその文書化				

個人情報保護マネジメントシステムJIS適合状況監査チェックシート

作成日付	2018/8/25
実施日	
実施者	

大分類	JIS内容	監査部門チェック			
		記載規程	条項	適否	コメント
	A.3.3.7　緊急事態への準備 組織は，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を確立し，実施し，かつ，維持しなければならない。 組織は，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を確立し，かつ，維持しなければならない。 また，組織は，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を確立し，かつ，維持しなければならない。 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。				
A.3.4 実施及び運用	A.3.4.1　運用手順 組織は，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，運用の手順を明確にしなければならない。				
	A.3.4.2　取得，利用及び提供に関する原則				
	A.3.4.2.1　利用目的の特定 組織は，個人情報を取り扱うに当たっては，そ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行わなければならない。 組織は，利用目的の特定に当たっては，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するよう配慮しなければならない。				
	A.3.4.2.2　適正な取得 組織は，適法かつ公正な手段によって個人情報を取得しなければならない。				

個人情報保護マネジメントシステムJIS適合状況監査チェックシート

作成日付	2018/8/25
実施日	
実施者	

大分類	JIS内容	監査部門チェック			
		記載規程	条項	適否	コメント
	A.3.4.2.3　要配慮個人情報 組織は，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。ただし，次に掲げるいずれかに該当する場合には，書面による本人の同意を得ることを要しない。 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 組織は，要配慮個人情報の利用又は提供についても，前項と同様に実施しなければならない。さらに，要配慮個人情報のデータの提供についても，同様に実施しなければならない。				
	A.3.4.2.4 個人情報を取得した場合の措置 組織は，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。ただし，次に掲げるいずれかに該当する場合には，本人への利用目的の通知又は公表は要しない。 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				

監査チェックシート

個人情報保護マネジメントシステムJIS適合状況監査チェックシート

作成日付	2018/8/25
実施日	
実施者	

大分類	JIS内容	監査部門チェック			
		記載規程	条項	適否	コメント
	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 組織は，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なければならない。 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，その旨 ただし，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，又はただし書きA.3.4.2.4のa)～d) のいずれかに該当する場合は，本人に明示し，本人の同意を得ることを要しない。				
	A.3.4.2.6　利用に関する措置 組織は，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。 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，本人の同意を得なければならない。ただし，A.3.4.2.3のa)～d) のいずれかに該当する場合には，本人の同意を得ることを要しない。				

監査チェックシート

個人情報保護マネジメントシステムJIS適合状況監査チェックシート

作成日付	2018/8/25
実施日	
実施者	

大分類	JIS内容	監査部門チェック			
		記載規程	条項	適否	コメント
	A.3.4.2.7　本人に連絡又は接触する場合の措置 組織は，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，本人の同意を得なければならない。ただし，次に掲げるいずれかに該当する場合は，本人に通知し，本人の同意を得ることを要しない。 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 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，“共同利用”という。） －共同して利用すること －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				
	A.3.4.2.8　個人データの提供に関する措置 組織は，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，本人の同意を得なければならない。ただし，次に掲げるいずれかに該当する場合は，本人に通知し，本人の同意を得ることを要しない。				

個人情報保護マネジメントシステムJIS適合状況監査チェックシート

作成日付	2018/8/25
実施日	
実施者	

大分類	JIS内容	監査部門チェック			
		記載規程	条項	適否	コメント
	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 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				
	A.3.4.2.8.1　外国にある第三者への提供の制限 組織は，法令等の定めに基づき，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なければならない。ただし，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は，本人の同意を得ることを要しない。				

個人情報保護マネジメントシステムJIS適合状況監査チェックシート

作成日付	2018/8/25
実施日	
実施者	

大分類	JIS内容	監査部門チェック			
		記載規程	条項	適否	コメント
	A.3.4.2.8.2　第三者提供に係る記録の作成など 組織は，個人データを第三者に提供したときは，法令等の定めるところによって記録を作成し，保管しなければならない。ただし，A.3.4.2.3のa)～d) のいずれかに該当する場合，又は次に掲げるいずれかに該当する場合は，記録の作成を要しない。 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。				
	A.3.4.2.8.3　第三者提供を受ける際の確認など 組織は，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わなければならない。ただし，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は，確認を要しない。 組織は，法令等の定めるところによって確認の記録を作成，保管しなければならない。				
	A.3.4.2.9 匿名加工情報 組織は，匿名加工情報の取扱いを行うか否かの方針を定めなければならない。 組織は，匿名加工情報を取り扱う場合には，本人の権利利益に配慮し，かつ，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確立し，かつ，維持しなければならない。				
	A.3.4.3　適正管理				
	A.3.4.3.1　正確性の確保 組織は，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なければならない。 組織は，個人データを利用する必要がなくなったときは，当該個人データを遅滞なく消去するよう努めなければならない。				
	A.3.4.3.2　安全管理措置 組織は，その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，滅失又はき損の防止その他の個人情報の安全管理のために必要かつ適切な措置を講じなければならない。				

個人情報保護マネジメントシステムJIS適合状況監査チェックシート

作成日付	2018/8/25
実施日	
実施者	

大分類	JIS内容	監査部門チェック			
		記載規程	条項	適否	コメント
	A.3.4.3.3 従業者の監督 組織は，その従業者に個人データを取り扱わせるに当たっては，当該個人データの安全管理が図られるよう，当該従業者に対する必要かつ適切な監督を行わなければならない。				
	A.3.4.3.4 委託先の監督 組織は，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なければならない。 組織は，個人データの取扱いの全部又は一部を委託する場合は，十分な個人データの保護水準を満たしている者を選定しなければならない。このため，組織は，委託を受ける者を選定する基準を確立しなければならない。委託を受ける者を選定する基準には，少なくとも委託する当該業務に関しては，自社と同等以上の個人情報保護の水準にあることを客観的に確認できることを含めなければならない。 組織は，個人データの取扱いの全部又は一部を委託する場合は，委託する個人データの安全管理が図られるよう，委託を受けた者に対する必要かつ適切な監督を行わなければならない。 組織は，次に示す事項を契約によって規定し，十分な個人データの保護水準を担保しなければならない。 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 組織は，当該契約書などの書面を少なくとも個人データの保有期間にわたって保存しなければならない。				
	A.3.4.4 個人情報に関する本人の権利				

個人情報保護マネジメントシステムJIS適合状況監査チェックシート

作成日付	2018/8/25
実施日	
実施者	

大分類	JIS内容	監査部門チェック			
		記載規程	条項	適否	コメント
	A.3.4.4.1 個人情報に関する権利 組織は，保有個人データに関して，本人から開示等の請求等を受け付けた場合は，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なければならない。ただし，次に掲げるいずれかに該当する場合は，保有個人データには当たらない。 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 組織は，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。				
	A.3.4.4.2 開示等の請求等に応じる手続 組織は，開示等の請求等に応じる手続として次の事項を定めなければならない。 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による場合の手数料（定めた場合に限る。）の徴収方法 組織は，本人から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。 組織は，A.3.4.4.4又はA.3.4.4.5によって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，その額を定めなければならない。				

個人情報保護マネジメントシステムJIS適合状況監査チェックシート

作成日付	2018/8/25
実施日	
実施者	

大分類	JIS内容	監査部門チェック			
		記載規程	条項	適否	コメント
	A.3.4.4.3 保有個人データに関する事項の周知など 組織は，当該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。）に置かなければならない。 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				
	A.3.4.4.4 保有個人データの利用目的の通知 組織は，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には，遅滞なくこれに応じなければならない。ただし，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，又は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は利用目的の通知を必要としないが，そのときは，本人に遅滞なくその旨を通知するとともに，理由を説明しなければならない。				
	A.3.4.4.5 保有個人データの開示 組織は，本人から，当該本人が識別される保有個人データの開示（当該本人が識別される保有個人データが存在しないときにその旨を知らせることを含む。）の請求を受けたときは，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，当該保有個人データを書面（開示の請求を行った者が同意した方法があるときは，当該方法）によって開示しなければならない。ただし，開示することによって次のa)～c)のいずれかに該当する場合は，その全部又は一部を開示する必要はないが，そのときは，本人に遅滞なくその旨を通知するとともに，理由を説明しなければならない。 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				

個人情報保護マネジメントシステムJIS適合状況監査チェックシート

作成日付	2018/8/25
実施日	
実施者	

大分類	JIS内容	監査部門チェック			
		記載規程	条項	適否	コメント
	A.3.4.4.6 保有個人データの訂正，追加又は削除 組織は，本人から，当該本人が識別される保有個人データの内容が事実でないという理由によって当該保有個人データの訂正，追加又は削除（以下，この項において“訂正等”という。）の請求を受けた場合は，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，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わなければならない。また，組織は，訂正等を行ったときは，その旨及びその内容を，本人に対し，遅滞なく通知し，訂正等を行わない旨の決定をしたときは，その旨及びその理由を，本人に対し，遅滞なく通知しなければならない。				
	A.3.4.4.7 保有個人データの利用又は提供の拒否権 組織が，本人から当該本人が識別される保有個人データの利用の停止，消去又は第三者への提供の停止（以下，この項において“利用停止等”という。）の請求を受けた場合は，これに応じなければならない。また，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。ただし，A.3.4.4.5のただし書きa)～c) のいずれかに該当する場合は，利用停止等を行う必要はないが，そのときは，本人に遅滞なくその旨を通知するとともに，理由を説明しなければならない。				
	A.3.4.5 認識 組織は，従業者が7.3に規定する認識をもつために，関連する各部門及び階層における次の事項を認識させる手順を確立し，かつ，維持しなければならない。 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 組織は，認識させる手順に，全ての従業者に対する教育を少なくとも年一回，適宜に行うことを含めなければならない。				

監査チェックシート

個人情報保護マネジメントシステムJIS適合状況監査チェックシート

作成日付	2018/8/25
実施日	
実施者	

大分類	JIS内容	監査部門チェック			
		記載規程	条項	適否	コメント
A3.5 文書化した情報	A.3.5.1 文書化した情報の範囲 組織は，次の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書面で記述しなければならない。 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				
	A.3.5.2 文書化した情報（記録を除く。）の管理 組織は，この規格が要求する全ての文書化した情報（記録を除く。）を管理する手順を確立し，実施し，かつ，維持しなければならない。 文書化した情報（記録を除く。）の管理の手順には，次の事項が含まれなければならない。 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				
	A.3.5.3 文書化した情報のうち記録の管理 組織は，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として，次の事項を含む記録を作成し，かつ，維持しなければならない。 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，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 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 組織は，記録の管理についての手順を確立し，実施し，かつ，維持しなければならない。				

個人情報保護マネジメントシステムJIS適合状況監査チェックシート

作成日付	2018/8/25
実施日	
実施者	

大分類	JIS内容	監査部門チェック			
		記載規程	条項	適否	コメント
A.3.6 苦情及び相談への対応	A.3.6 苦情及び相談への対応 組織は，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確立し，かつ，維持しなければならない。 組織は，上記の目的を達成するために必要な体制の整備を行わなければならない。				
A.3.7 パフォーマンス評価	A.3.7.1 運用の確認 組織は，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が組織の各部門及び階層において定期的に，及び適宜に確認されるための手順を確立し，実施し，かつ，維持しなければならない。 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，その是正処置を行わなければならない。 個人情報保護管理者は，トップマネジメントによる個人情報保護マネジメントシステムの見直しに資するため，定期的に，及び適宜にトップマネジメントにその状況を報告しなければならない。				
	A.3.7.2 内部監査 組織は，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。 組織は，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確立し，実施し，かつ，維持しなければならない。 個人情報保護監査責任者は，監査員に，自己の所属する部署の内部監査をさせてはならない。				

個人情報保護マネジメントシステムJIS適合状況監査チェックシート

作成日付	2018/8/25
実施日	
実施者	

大分類	JIS内容	監査部門チェック			
		記載規程	条項	適否	コメント
	A.3.7.3 マネジメントレビュー トップマネジメントは，9.3に規定するマネジメントレビューを実施するために，少なくとも年一回，適宜に個人情報保護マネジメントシステムを見直さなければならない。 マネジメントレビューにおいては，次の事項を考慮しなければならない。 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				
A.3.8 是正処置	A.3.8 是正処置 組織は，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を確立し，実施し，かつ，維持しなければならない。その手順には，次の事項を含めなければならない。 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。				