

JIS要求事項	審査内容	不備及び確認事項	
<b>1.適用範囲</b> この規格は、個人情報事業のように供している、あらゆる種類、規模の事業者に適用できる個人情報保護マネジメントシステムに関する要求事項について規定する。 事業者は、次の事項を行う場合に、この規格を用いることができる。 a)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、改善する。 b)この規格と個人情報保護マネジメントシステムとの適合性について自ら確認し、適合していることを自ら表明する。 c)外部組織又は本人に、この規格と個人情報保護マネジメントシステムとの適合性について確認を求める。 d)外部機関による個人情報保護マネジメントシステムの認証/登録を求める。	①全従業者を人的範囲に定めていること。		
	②事業の用に供している個人情報を適用対象とするよう定めていること。		
<b>2.用語及び定義</b>	—	—	—
<b>3.個人情報保護マネジメント要求事項</b>	—	—	—
<b>3.1一般要求事項</b>	—	—	—
<b>3.2個人情報保護方針</b> 事業者の代表者は、個人情報保護の理念を明確にした上で、次の事項を含む個人情報保護方針を定めるとともに、これを実行し、かつ、維持しなければならない。 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り扱い(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)個人情報の取り扱いに関する法令、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、滅失また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)代表者の氏名 事業者の代表者は、この方針を文書(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。)化し、従業者に周知させるとともに、一般の	①個人情報保護の理念を明確にしていること。		
	②a)について記述していること。		
	③b)について記述していること。		
	④c)について記述していること。		
	⑤d)について記述していること。		
	⑥e)について記述していること。		
	⑦f)が表示されていること。		
	⑧制定日が表示されていること。		

JIS要求事項	審査内容	不備及び確認事項	
人が入手可能な措置を講じなければならない。	⑨従業員及び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。		
<b>3.3計画</b>	—	—	—
<b>3.3.1個人情報の特定</b> 事業者は、自らの事業の用に供するすべ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。	①全ての個人情報を特定する手順及び承認手順が明確であること。 ②個人情報を特定した台帳等の更新及び定期的な見直しに関する手順が定められていること。		
<b>3.3.2法令、国が定める指針その他の規範</b> 事業者は、個人情報の取り扱いに関する法令、国が定める指針その他の規範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。	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を特定し、参照し、維持する手順が定められていること。		
<b>3.3.3リスクの認識、分析及び対策</b> 事業者は、3.3.1によって特定した個人情報について、目的外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。 事業者は、3.3.1によって特定した個人情報について、その取扱いの各局面におけるリスク(個人情報の漏えい、滅失又はき損、個人情報保護法との対応、国が定める指針その他の規範に対する違反、想定される経済的な不利益及び社会的な信用の失墜、本人への影響などのおそれ)を認識し、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。	①目的外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、維持するように規定していること。 ②洗い出された個人情報について、ライフサイクルに応じてリスクを洗い出し、リスク分析を実施、リスクに応じた対策を講じ、残存リスクを把握する手順が明確であること。 ③定期的な見直し、及び必要に応じた随時の見直しの手順が明確であること。		
<b>3.3.4資源、役割、責任及び権限</b> 事業者の代表者は、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、かつ改善するために不可欠な資源を用意しなければならない。 事業者の代表者は、個人情報保護マネジメントシステムを効果的に実施するために役割、責任及び権限を定め、文書化し、かつ、従業員に周知しなければならない。 事業者の代表者は、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事業者の内部の者から指名し、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らず	①各担当者の役割、責任及び権限が明確に定められ、文書化されていること。 ②個人情報保護管理者は、事業者の内部の物から指名するよう規定していること。		