

(定期・臨時) 内部監査チェックリスト

監査年月日 : ※※※※年※※月※※日
 被監査部門 : ※※※※部
 被監査者 : ※※ ※※、※※ ※※
 監査員名 : ※※ ※※、※※ ※※

【監査基準】 適合 ○ : 要求事項どおりに実施されている
 不適合(重大) × : 要求事項が全く、実施されていない
 不適合(軽微) △ : 要求事項が一部、実施されていない
 観察 観 : 推奨事項、こうした方がよいとされるもの

承認	審査	作成
/ /	/ /	/ /

規格要求事項 (JISQ15001)		監査事項 (監査前に記述)			監査記録(監査中に記述)		
		質問事項	関連文書	項	監査所見及び確認した文書	判定	
3. 要求事項							
3.1 一般要求事項							
1	3.1	事業者は、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文書(規程書、手順書、様式集)の構築を行い実施し、維持し、かつ、改善を行う手順を明確にし、文書化し実施されていますか。	【手順】 ①個人情報保護マネジメントシステム文書一式 【様式】 ①関連様式一式	全項	個人情報マネジメントシステム文書として確立し、実施し、維持しています。文書としては「内部文書記録管理台帳」に記載されている文書になります。	○
3.2 個人情報保護方針							
2	3.2	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	個人情報保護の理念を明確にした上で、JISQ15001(3.2-a)~f)で示す事項を含む個人情報保護方針を定め、実行し、かつ、維持する手順を明確にし、文書化し実施されていますか。	【手順】 ①個人情報保護方針 【様式】 (1)個人情報保護方針	3.2	個人情報保護方針は定められています。口頭で従業員などに伝えているだけでなく、文書化はしていません。	×
3	3.2	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、従業員に周知させるとともに、一般の人が入手可能な措置を講じなければならない。	個人情報保護方針を一般の人が入手可能となるように当社ホームページや社内案内に掲示されていますか。また、従業員に周知徹底するため事務所内などへも掲示する手順を明確にし、文書化し実施されていますか。	【手順】 ①個人情報保護方針 【様式】 (1)個人情報保護方針		社内案内に記載されている個人情報保護方針の制定日は他の制定日と異なっている。(誤記?)	△
3.3 計画							
3.3.1 個人情報の特定							
4	3.3.1	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。	個人情報を特定するための手順を確立し、かつ、維持されていますか。	【手順】 ①個人情報管理規定 【様式】 (1)個人情報管理台帳		手順は文書化され、また、実施、維持はされているが、「個人情報管理台帳」の見直しの間隔が1年毎であり、長いように思います。もう少し、短い間隔での見直しを実施された方がよいと思われます。	観
3.3.2 法令、国が定める指針その他の規範							
5	3.3.2	事業者は、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。	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できる手順を確立し、かつ、維持されていますか。	【手順】 ①適合性管理規程 【様式】 (1)法令チェック表 (2)外部文書記録管理台帳	全項		
3.3.3 リスクなどの認識、分析及び対策							
6	3.3.3	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。					
7	3.3.3	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ための手順を確立し、かつ、維持しなければならない。		【手順】 ①個人情報取扱い管理規定 ②情報主体の権利管理規定 ③教育・研修管理規定 【様式】 (1)同意書 (2)通知書 (3)年間教育・研修計画表	全項		
7	3.3.3	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個人情報の漏えい、滅失又はき損、関連する法令、国が定める指針その他の規範に対する違反、想定される経済的不利益及び社会的信用の低下、個人の権利利益の侵害などのおそれ(以下、「リスク」という。)を認識し、分析し、必要な対策を講じるための手順を確立し、かつ、維持しなければならない。	個人情報の取扱いの各局面におけるリスクを認識し、分析し、必要な対策を講じるための手順を確立し、かつ、維持されていますか。	【手順】 ①リスクアセスメント理規定 【様式】 (1)業務フロー (2)リスク対応シート (3)リスク分析・評価表	4		
3.3.4 資源、役割、責任及び権限							
8		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。	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するための手順を明確にし、文書化し実施されていますか。	【手順】 ①個人情報保護運営管理規程 【様式】 (1)プライバシーマーク推進体制図	全項		
9		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。	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、従業員に周知するための手順を明確にし、文書化し実施されていますか。	【手順】 ①個人情報保護運営管理規程 【様式】 (1)業務分掌・職務権限表	3		