2014.1

「個人情報保護マネジメントシステム実施ハンドブック」簡易版　第 20 章

個人情報保護監査研究会

第20章　点検

点検とは、事業者自らが構築したＰＭＳの有効性を確認するために行う重要な機能です。
点検には、２通りの手段があります。

運用の確認	個人情報保護管理者以下、全社、各部門、各階層の管理者が、自ら行う日常点検
監査	個人情報保護監査責任者が、組織から独立して第三者的な視点で行う点検

20.1　運用の確認

あらかじめ「3303 年間計画表（兼点検表）」にＰＭＳ運用の確認時期と確認項目を設定し、計画どおり実施されているかどうかを確認します。　上段に予定日、下段に実際に実施した日を記入し、進捗管理をすることになります。実施日は手書きでもかまいません。

201★年度「3303ＰＭＳ年間計画書」

	201★年	１月	２月	３月	４月
①	代表者の見直し（計画表の策定・承認） （状況に変化があった際には随時見直し）				
②	法令・指針・規範の改定確認 （改定を確認した際には随時見直し）				
③	個人情報管理台帳の見直し （取扱に変更があった際には随時見直し）			1 /	
④	リスク分析表の見直し （取扱に変更があった際には随時見直し）				1 /
⑤	従業者定期教育の実施 （採用者には採用初日に教育）		15 /		
⑥	監査の実施 （状況に変化があった際には臨時監査を実施）				
⑦	全社　「343401委託先管理台帳」 （「委託先調査票」が陳腐化していないか点検を含む）				

各記録の点検は、
毎月実施した日付を記入します。

⑧	各部門「3319　個人情報返却廃棄管理表」点検	/
⑨	3432-010「システム機器・ID管理台帳」点検	/
⑩	3432-015 情報機器「持出」許可申請書(OUT)点検	/
⑪	3432-016 情報機器「持込」許可申請書(IN)点検	/
⑫	3432-017「携帯電話使用申請書」点検	/
⑬	3432-211「入退館安全確認記録簿」点検	/
⑭	3432-212「来客入退館カード貸出簿」点検	/

開示請求、苦情などの
件数も記録します。

⑲	開示等請求の件数	計：　件	件	件
⑳	苦情・事故・ヒヤリ・ハットの発生	計：　件	件	件

20.2　監査

監査は、毎年以下の２つの観点から実施します。

監査目的	監査の内容	監査対象
適合性監査	法令、国が定める指針その他の規範および、個人情報保護マネジメントシステム－要求事項（JIS Q 15001:2006）に合致しているかどうかを監査する。	内部規程（ＰＭＳ責任者、事務局など）
運用監査	自社のＰＭＳにおいて、リスク分析の結果講じるとした対策の運用状況の監査	全社、全部門（ＰＭＳ運用、および各部門責任者など）

20.2.1　監査計画

全社を対象にした監査の時期については、大枠を「3303PMS 年間計画書（兼点検表）」に定めます。監査の実施時期は、事業の繁忙期を避ける必要があります。また定期的な全社員教育が実施され、個人情報の特定とリスク分析が実施され、運用が開始された後に行います。

監査計画書には、監査テーマ、部門ごとの実施時期、時間、監査担当者など、具体的な計画を立案します。
監査時間は業務の規模にもよりますが、被監査部門の意見を聴取する場でもあることを認識し、
少なくとも２時間程度は、確保するとよいでしょう。

サンプルの
監査計画書は、
監査報告書を兼ねています。

監査計画書は、代表者の承認が必要です。

201　年度　PMS監査計画書　兼報告書

（201×年4月1日～201×年3月31日）

標題の件、個人情報保護監査規程　第××条に基づき、下記のとおり
実施致したくご承認願います。

監査責任者：取締役　○○○○室長

監査目的	1. JIS等の適合監査	当社ＰＭＳの、JIS Q 15001：2006など利用した	
	2. PMS運用監査	当社ＰＭＳにおいて、リスク分析の結果講ずるとし	
被監査部門 監査日程	1. JIS等の適合監査	個人情報保護管理者	1. 実施予定:
	2. PMS運用監査	全社および全部門	2. 実施予定:
特記事項	（予算、外部からの協力要請等）		

全部門を対象とすること　　監査担当者は被監査部門でないこと　　以下は、監査実施

	被監査部門	監査担当者		監査実施日
☆	ＪＩＳ等の適合性監査	○○○○部	○○○○○	２０１　／
①	ＰＭＳ体制	○○○○部	○○○○○	２０１　／
②	施設・設備の安全管理	○○○○部	○○○○○	２０１　／
③	情報システムの安全管理	○○○○部	○○○○○	２０１　／
④	○○○○部	○○○○部	○○○○○	２０１　／
⑤	○○○○部	○○○○部	○○○○○	２０１　／
⑥	○○○○支店	○○○○支店	○○○○○	２０１　／
監査結果	【監査責任者の所見】 1. JIS等の適合監査について 2. PMS運用監査について			

20.2.2　監査体制

個人情報監査責任者は、全部門の監査を実施する権限を持ちます。
代表者や個人情報保護管理者は、監査責任者を兼務することはできません。自分を監査してはならないというルールがあるからです。ただし、２名しかいない小規模事業者の場合、代表者は個人情報保護管理者を兼務し、監査責任者は他の者を指名します。
同様に、監査担当者は、自部門を監査することはできません。２名しかいない小規模事業者では、相互に監査担当者として監査を実施してください。
なお、企業の監査役は、内部統制上の機能制限により監査責任者だけでなく、個人情報保護体制に参加することはできませんので注意してください。

20.2.3　適合性監査

適合性監査は、規程を更新する時が最も有効な時期です。監査報告書を代表者に提出し、不適合があれば、見直しを経て規程が承認されるという手順で行ってください。

下記の「チェックリスト JISQ15001 適合性監査」のサンプルは、各項目の指摘事項、および全体の【不適合】の概観を記入して代表者に報告する様式になっています。このハンドブックで使用するチェックリストは、すべて報告書を兼ねています。

201y 年度　ＰＭＳ監査チェックリスト[JIS Q 15001 適合性」兼報告書

	代表者	監査責任者	被監査者	監査実施日	201y/mm/dd
				被監査部門	個人情報保護管理者
監査報告に当たっては、手書きのままでよい。 ①適合欄：○× ②規程欄：条項番号まで記載すること。	確認受領	報告	確認	監査担当者	○○部○○課 ○○○○○
				保存期間	３年後年度末
				廃棄予定	201y/mm/dd
	/ /	/ /	/ /	主管	個人情報保護監査責任者

【不適合】の概観

○×（業務がなければ　－）

JIS 要求事項	チェック内容	適合	規程および条文、使用する様式	指摘事項
1.適用範囲	①下記の全従業者を人的範囲に定めているか。（正社員、契約社員、嘱託社員、派遣社員、パート社員、アルバイト社員、取締役、執行役、理事、監査役、監事、等を含む。）		3301 取扱規程 1.1	
	②全社を適用対象としているか。		3301 取扱規程 1.1	

20.2.4　運用監査

被監査部門の職場に出向き、部門長や、業務担当者に対するヒアリングや現場目視を行います。 事業の内容や取り扱いに応じて準備した「監査チェックリスト」を用い、エビデンス（証拠書類）や実態を確認して、「監査チェックリスト」に書き込んでいきます。

	運用監査チェックリストの種類	監査対象
b)	「3726b_予備調査チェックリスト」	被監査部門の事前準備用
c)	「3313c _リスク分析表（兼監査チェックリスト）」	【必須】
d)	「3726d_PMS体制の運用チェックリスト」	個人情報保護管理者および事務局
e)	「3726e_施設・設備の安全性チェックリスト」	施設ごとの管理部門
f)	「3726f_情報システム運用の安全性チェックリスト」	システム運用部門
g)	「3726g_情報システム開発の安全性チェックリスト」	システムのオーナー部門
h)	「3726h_部門ＣＰチェックリスト」	

a)～h)のうち、c)「3313c リスク分析表（兼監査チェックリスト）」を用いての監査は必須です。

部門		管理部	業務名　「従業員管理」								
業務フロー		採用から従業員管理および退職に至る従業員情報管理業務								/ /	
ライフサイクルおよび業務名		台帳	個人情報管理台帳に記載の個人情報名	取得手段入力	媒体	コピー	想定されるリスク	リスク対策	規程・様式	監査○×	監査確認結果
取得	採用業務	1 2 3	履歴書 職務経歴書 成績証明書	本人・直接手渡し	紙	禁止	利用目的の通知漏れ 書面による同意の取得漏れ	1. 面接キット「同意書（応募者用」	「個人情報取扱規程」3.4.2.4		
							漏洩（紛失）	1. 保管管理者の限定	「安全管理規程」4		
								2. 施錠管理	「安全管理規程」4		
		4	応募者からの同意書		紙	禁止	漏洩（紛失）	1. 保管管理者の限定	「安全管理規程」4		
								2. 施錠管理	「安全管理規程」4		
移送		－	（応募書類の返却）	－	紙	－	漏洩（誤送付）	1. 簡易書留で送付	「安全管理規程」9		
								2. 送付表の保管	「安全管理規程」9		
利用		5	応募者リスト 採用結果票	面接者が記入	紙	禁止	目的外利用（期限を超える保管）	「廃棄記録」による確認	「安全管理規程」4		

各部門で取り扱う個人情報について、リスク分析した結果の対策＝規程について監査を実施するため、実務的で、効率的な監査を実施することができます。
他の「監査チェックリスト」は、被監査部門が抱えるリスクに応じ、追加で監査を実施してください。

※　施設や設備は、部門にまたがるため、総務部や支部長などを対象に、「3726e_施設・設備の安全性チェックリスト」で監査します。　　（以下はｅ）の一部）

3.3.7 緊急事態への準備	①緊急事態や、ヒヤリ・ハットしたことはあったか。	施設安全	ヒアリング
	②「緊急事態発生手順書」はすぐに参照できるようになっているか。	施設安全	「緊急事態手順書」
	③「緊急連絡網」はすぐに参照できるようになっているか。	施設安全	「緊急連絡網」

ただし、「3313c リスク分析表（兼監査チェックリスト）」に、上記に類する監査項目が含まれている場合は、e）は、省略可能です。

※　全社の基盤としての情報システムがある場合は、f)「3726_情報システム運用の安全性チェックリスト」によって、システム運用部門の責任者を対象に監査します。　（以下はｆ）の一部）

不正アクセス防止	①ネットワークのログインＩＤは、一人ずつ個別に与えているか。	SYS	「ＩＤ管理表」		
	②人事異動・退職者が発生した際に、速やかにＩＤを削除しているか。	SYS	目視		
	③パスワードは、英数字混合で８文字以上に制限しているか。	SYS	目視		
	④ネットワークのログインパスワードは、６か月以内に（強制的に）パスワードを変更しているか。	SYS	「ＩＤ管理台帳」		
	⑤一般利用者のＰＣログインは、ユーザ権限としているか。	SYS	目視		

※　規程や法律違反とならないよう、また個人の権利を侵害しないために、「3726h_部門ＣＰチェックリスト」で監査します。ただし、「3313c リスク分析表（兼監査チェックリスト）」に、下記に類する監査項目が含まれている場合は、h）は、省略可能です。

3.4.2.2 適正な取得	①あらたな個人情報を取得することとなった場合には、「同意書」を添付して、ＰＭＳ管理責任者の承認を得ているか。	施設安全	「個人情報取扱申請書」
	②監視カメラによって社員および来訪者を録画している場合は、「監視カメラ設置」パネルを掲示しているか。	施設安全	目視

※　サンプルのチェックリストは、事業者の取り扱う個人情報に応じて選択し、社会情勢や事故事例などを参考に適宜、削除、追加して使用します。

20.2.5　運用監査の評価

監査担当者は、ヒアリングや目視した事実に基づき、チェックリストに以下の評価を記入します。

	評価	記述	状況	是正処置
a)	適合	○	問題なし	不要
b)	観察事項	○′	直ちに改善され、再発はしないと評価できる状況	不要
c)	不適合	×	是正しなければ、本人の権利を侵害し、企業の存続に係わるリスクとなる状況	必要

確認結果欄には、確認した記録（エビデンス）の名称、目視したモノやヒアリング内容を明記し、不適合があれば、　“～を実施していない”、“～を記録していない”　など、具体的に記入します。

準備した監査項目のすべてについて、監査結果を記入した後、
チェックリストの１ページ目の「【不適合】の概観」欄に、被監査部門ごとに特徴的な問題点や事情について記述し、代表者が一見してその部門の状況が理解できるようにします。
監査の終了時に「講評会」を実施し、被監査部門に不適合について納得が得られるよう説明し、確認印もしくはサインを得ます。

20.2.6　監査報告

監査責任者は、監査担当者から各部門の監査結果について「チェックリスト」によって報告を受け、結果のサマリーとして「3721 監査計画書（兼報告書）」を作成します。
「3721 監査計画書（兼報告書）」には、監査責任者が，ＰＭＳに対して改善すべき提言が盛り込まれている必要があります。

20.2.7　是正処置

監査において発見した不適合については、「3801 是正・予防処置報告書」を用いて、是正処置を実施します。監査責任者の責務は、不適合の報告迄で、是正処置の責任者は個人情報保護管理者となります。

■

次回は、「第 21 章　是正処置及び予防処置」をご紹介します。＞目次へ

個人情報保護監査研究会　http://www.saaj.or.jp/shibu/kojin.html　　以上