（６）規程の遵守状況等の日常的点検・確認の方法

本節では、規程などの遵守状況について、日常業務の中で適切に点検・確認を行う上でどのような取組がなされているのか、ということについて取り上げている。定期的に実施され、網羅性の高い監査に加え、日常的に個人情報保護に関する取組の実効性担保のために何がなされているか、ということについて事例を紹介している。

例えば、実際に日常的に担当者や管理職員が個人情報保護に関する規程の遵守状況について業務の現場を巡回等し検査を行うなどの事例を紹介しているが、事業者の規模や考え方などによって、毎日点検を実施している事例（②）や、1ヶ月に1度などの定期的な点検を実施している事例（④）も紹介している。

また、パソコン等の個人情報保護対策の進展状況について直感的にわかりやすいシールを貼付することで、職員の誰でもが分かるように対策状況の「見える化」を行っている事例（⑥）や、巡回の際に個人情報保護の面から見て望ましくない行動を取っている職員の席などに“レッドカード”を置いていくというゲーム感覚を取り入れて点検を実施しているようなユニークな事例（⑧）についても紹介している。

自己点検ができるモニタリングシートの作成（⑨）や、管理体制チェックシートの使用で紛失を未然に防止する事例（⑬）など、シートを有効活用している事例もある。

その他、監査前にアンケートを行って、可視的に職員の個人情報保護に関する意識や現状、管理職と一般職層のギャップなどをチェックしている事例（⑫）も紹介している。

本節で紹介している取組事例

4-(6)-①：個人パソコンを定期的に点検し、個人情報が含まれている場合には削除
4-(6)-②：抜き打ちで毎日の放置検査を実行
4-(6)-③：毎月、部署ごとに報告を義務付けている。最終的には査定評価に反映
4-(6)-④：月に１日をコンプライアンスデーと定め、項目別に実施を促進
4-(6)-⑤：１日１回以上現物点検・周知徹底
4-(6)-⑥：３つのシールで対策の「見える化」を実現
4-(6)-⑦：毎日朝礼時に「情報管理の誓い」を唱和
4-(6)-⑧：「レッドカード」を導入し、ゲーム感覚の中で従業者のモチベーションを高める
4-(6)-⑨：自己点検ができるモニタリングシートの作成・配布
4-(6)-⑩：イントラネットで事故事例を紹介、ポップアップ画面の使用で注意を引く
4-(6)-⑪：情報セキュリティマネジメントシステムを回すための監査等を複層的に実施
4-(6)-⑫：監査の実効性を高めるための従業員への事前アンケートを実施
4-(6)-⑬：管理体制チェックシートの定期実施でミスの削減を実現
4-(6)-⑭：実践的な携行ハンドブックの携行を全従業者に義務付け

4-(6)-⑮：年3回の全社総点検を切れ目無くフォローアップ

4-⑹-①【個人パソコンを定期的に点検し、個人情報が含まれている場合には削除】

（電気・ガス・水道業：約 60 人）

・C 社では従来は見積もりに関する情報も個人で管理していたが、サーバですべて保管するように規程を定め、IT 委員会の活動によって周知を図った。個人のパソコンを定期的にチェックし、サーバに入れていない情報は削除するという取組を始めたところである。サーバの導入は社内の IT 化と情報セキュリティの取組を並行して進めた結果だが、サーバの導入で 100 万円近くの費用がかかっている。

4-⑹-②【抜き打ちで毎日の放置検査を実行】

（小売業（通販等）：約 520 人）

・H 社では情報放置整理点検シートがあり、3 時間ごとに FAX や出力物の放置を点検する。このチェックシートで 3 回以上放置があった場合には、指導を受けることになっており、場合によってはプリンタを使用できなくするなどの措置をとる。

4-⑹-③【毎月、部署ごとに報告を義務付けている。最終的には査定評価に反映】

（小売業（通販等）：約 520 人）

・H 社では個人情報管理月報があり、各部署に毎月提出を義務付けている。

・個人情報の保管に関して、「管理者が保管庫の鍵を適切に管理し施錠しているか」、などの項目をチェックする。

・適切な管理がなされていない場合には是正計画書を提出させる。“不適合”の評価を 2 回受けると情報セキュリティ委員会から呼び出しがあり、指導を受ける。

・更に改善が見られない場合には、査定評価に反映することになっている。

4-⑹-④【月に 1 日をコンプライアンスデーと定め、項目別に実施を促進】

（信用業：約 700 人）

・J 社ではコンプライアンスについて、各項目別に実施を指示してもなかなか行動に結びつかなかった。そのため、毎月 7 日をコンプライアンスデーと定め行動を促進するようにした。

・実施項目は複数あり、内容によって毎月実施のものと 3 ヶ月、6 ヶ月に一度のものがある。

・年間でいつ何を実施するのかを分かりやすくするため、実施日を記録できる用紙を用意した。各部署の責任者は、実施日を入力し管理している。コンプライアンス統括部もそのデータでどの部署がいつ実施したかをすぐに分かるようになっている。

図表　実施日を記録できる用紙イメージ

取組確認シート

部門名　　責任者

実施項目	実施日または実施完了日											
	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
勉強会の実施	月 日	月 日	月 日	月 日	月 日	月 日	月 日	月 日	月 日	月 日	月 日	月 日
パスワード変更の実施	月 日	月 日	月 日	月 日	月 日	月 日	月 日	月 日	月 日	月 日	月 日	月 日
個人情報一覧表のメンテナンス	－	月 日	－	－	月 日	－	－	月 日	－	－	月 日	－
リスク評価と対策一覧表の見直し	－	月 日	－	－	月 日	－	－	－	－	－	－	－
個人情報破棄の定期点検の実施	－	－	月 日	－	－	－	－	－	月 日	－	－	－
委託先調査の実施	月 日	－	－	－	－	月 日	－	－	－	－	月 日	－
自主監査チェックシート	月 日	－	－	月 日	－	－	月 日	－	－	月 日	－	－
アンケート回答	－	－	－	－	月 日	－	－	－	－	－	月 日	－
	月 日	月 日	月 日	月 日	月 日	月 日	月 日	月 日	月 日	月 日	月 日	月 日

・前述のコンプライアンスに関する勉強会もコンプライアンスデーに設ける部署が多い。

4-⑹-⑤【1 日 1 回以上現物点検・周知徹底】（信用業：100 人未満）

・K 社では主に朝礼時に、IC カードや鍵等の現物の確認、個人情報の授受記録、出力や作成の管理簿等の確認を行って、個人情報保護の日常的な点検・確認を実施。

4-⑹-⑥【３つのシールで対策の「見える化」を実現】（情報サービス業：約 1,600 人）

・O 社では、セキュリティ区画レベル２で扱う従業者のパソコンに対して、重要な対策が行われていることを一目で分かるように点検結果のシールを貼付している。

・具体的には HD の暗号化や、電子メール添付ファイルの暗号化をしている「暗号化対応済シール」、ノート PC などのモバイルの持ち出し許可を受けている「持出し許可済シール」、PC に顧客データ（個人情報）を記録していない「個人情報なしシール」の 3 種類である。「個人情報なしシール」と「暗号化対応済シール」は番号管理されている。

・「個人情報なしシール」については、使用期間が半年間（1～6 月／7～12 月）に限定されている。個人情報なしチェックは半年に一度、従業者のパソコンに顧客データ（個人情報）が入っていないことをチェックし、顧客データ（個人情報）が記録されていないことが証明できた場合に「個人情報なしシール」を貼付する。

・「持ち出し許可済シール」の貼付（持ち出し）は「個人情報なしシール」及び「暗号化対応済シール」が貼られているパソコンで、持ち出し目的が明確な PC に最長 3 ヶ月を限度で認められる。

・これらのシールは、誰が見ても一目で必要な対策が終わっているかどうかを確認できるようにするために貼付しており、貼付がないパソコンは持ち出しが許可されない。また、他事業所へ持ち込む際も同様で、貼付がなければ持ち込めない。

図表　「見える化」のためのシール（３種）

4-⑹-⑦【毎日朝礼時に「情報管理の誓い」を唱和】

（情報サービス業（コールセンター等）：約 2,500 人）

・Q 社では個人情報保護に関して、毎日の作業開始（朝礼）時に「情報管理の誓い」を唱和して注意喚起をしている。作業場の責任者が作業通知の後全員で読み上げている。

・スクリーンセーバーも「情報管理の誓い」が表示されるようにしている。ポスターも掲示している。

・「情報管理の誓い」を唱和することにより、日常業務の中で注意しやすい環境作りができる。毎日全員で唱えているので、説得力がある。

4-⑹-⑧【「レッドカード」を導入し、ゲーム感覚の中で従業者のモチベーションを高める】

（複合（情報システム／製造）：約 500 人）

・R 社では役員や担当がセキュリティ上の危険事項を発見した際に、「レッドカード」を発行している。発行は課単位で集計され、半年毎に優秀な課には報奨金（1 人 3,000 円程度）が支給される。

4-⑹-⑨【自己点検ができるモニタリングシートの作成・配布】（卸売業：約 1,480 名）

・D 社では、モニタリングシート「自己点検付きマニュアル」を作成配付した。
冊子形式で、遵守すべきルールが見開き左、自己点検チェック項目が見開き右に記載されており、ルールの確認とセルフチェックが同時に出来るよう工夫してある。

・社内イントラネットで公開し、各自がダウンロードして出力する。B5 版 20 ページの構成である。

4-⑹-⑩【イントラネットで事故事例を紹介、ポップアップ画面の使用で注意を引く】

（情報サービス(コールセンター等)：約 2,500 名）

・Q 社では、全従業者に宛てたイントラネットを通じて個人情報漏洩事件・事故の事例を紹介し、個人情報保護への取組みの重要性について周知・啓発を行っている。特に、トップのポップアップ画面に、マスコミに発表された個人情報漏洩事件・事故の概要を掲載し、常に新しいニュースを社員に発信している。朝礼などで発表し、教育のテーマとして活用している。

・自主点検表を作り、現場の機密管理者が日常的に状況をチェックしており、オペレータの入れ替わりがあってもセキュリティを保てるように注意している。

4-⑹-⑪【情報セキュリティマネジメントシステムを回すための監査等を複層的に実施】

（その他サービス業(印刷・広告)：約 11,000 人）

・X 社では、以下のように監査等を複層的に実施している。

①事業部内の内部監査

②事業部が行うファミリー会社、協力会社への監査

監査ツールを複数タイプ整備し、委託先の規模やプライバシーマークの取得の有無に応じて監査を実施。

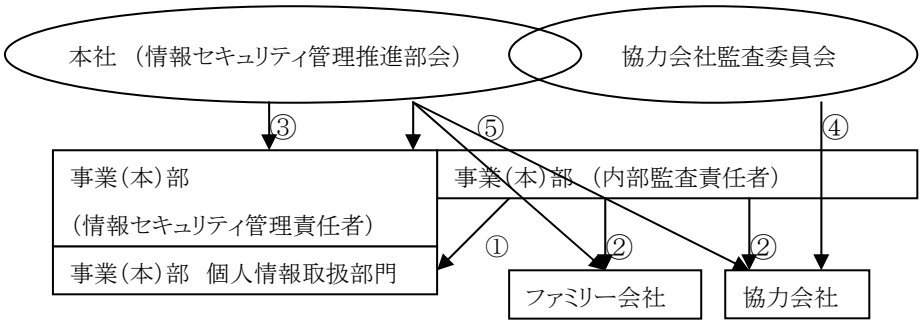
③本社（情報セキュリティ管理推進部会）が事業部に対して行う内部監査

事業部内の内部監査と同時並行で実施

④協力会社監査委員会が行う協力会社への監査

⑤本社の品質管理部が総合品質保証の観点で行う、事業部・ファミリー会社・協力会社への監査

図表　監査関連図



4-⑹-⑫【監査の実効性を高めるための従業員への事前アンケートを実施】

（その他サービス業(印刷・広告)：約 11,000 人）

・X 社では、平成 18 年度、監査時の回答と実態とのギャップ、サンプリングによる問題点の見落とし等の問題を解消するため、被監査部門の従業者（派遣社員等を含む）から、日常的な管理運用に関する事前アンケート調査を実施した。

・多岐にわたるアンケート項目により、評価軸に照らして管理レベルを視覚的に捉えられるだけでなく、管理者と一般層に分けることによって、そのギャップを捉えることも可能となった。

・監査員が被監査部門の業務内容に精通していない場合であっても、同アンケートが運用状況を指摘する上で有力な監査ツールとなった。

4-⑥-⑬【管理体制チェックシートの定期実施でミスの削減を実現】

（小売業(百貨店・スーパー)：約 10,000 名）

・エ社では、事故の発生の原因が郵送時の誤送付、封入ミス、伝票の持ち運び中の紛失などである場合が多かったため､チェックシートを事務局が作成し各部門の部長代理クラスに毎月チェックしてもらうようにしている。

・伝票等の紛失を防ぐため、クリアファイルに入れて持ち運ぶように定めている。

・これらによって紛失事故がゼロに近づいたという実感がある。

図表　個人情報管理体制緊急チェックシート

2008部・Div別 個人情報保護管理体制 月別チェックシート

（提出日）

部

検査責任者

チェック内容

必須項目	1	個人情報が無くなれば判る状態か	各職場、ショップ等の個人情報が無くなればすぐ判るよう整理整頓とナンバリング、区分け等出来ていること。
	2	個人情報の受渡し確認と記録はあるか	個人情報の受渡しの際、確認し記録をしているか。(必ずしも授受簿作成が目的ではない)
選択項目	1	個人情報のＦＡＸは厳禁	個人情報のFAX送信は厳禁です。　※顧客の強い要望や業務上必要な場合は、上司の確認を得、相互確認の上送信する。
	2	送付時の相互確認	個人情報を郵送等する際、第三者が宛名等のチェックを行い、封筒の裏に担当者と第三者が押印したうえで郵送する。
	3	移送時のクリアケース使用	個人情報を記載した伝票を館内で移送する際、必ずクリアケースに入れて持ち運ぶ。また、原則、他業務と兼務しない。
	4	並行作業時のバインダー使用	売場のカウンター等で、並行して作業する場合、伝票等が紛失しないようにバインダーに挟んで作業する
	5	個人情報を区別する赤いクリアホルダー使用	個人情報が個人情報以外の書類と区別するため赤いクリアホルダーを使用する(赤いクリアホルダーは10枚単位で用度にて物品購入のこと)
検査責任者必須		個人情報保護活動報告書記入	毎月「個人情報活動報告書」に実施記録を必ず記入すること。

チェック実施月		3月						4月						5月						6月						7月						8月				
		1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5
チェック内容 / 課・Div・担当名		無くなれば直ぐ判る状態か	個人情報はあるかの受渡し確認と記録					無くなれば直ぐ判る状態か	個人情報はあるかの受渡し確認と記録					無くなれば直ぐ判る状態か	個人情報はあるかの受渡し確認と記録					無くなれば直ぐ判る状態か	個人情報はあるかの受渡し確認と記録					無くなれば直ぐ判る状態か	個人情報はあるかの受渡し確認と記録					無くなれば直ぐ判る状態か	個人情報はあるかの受渡し確認と記録			
①																																				
②																																				
③																																				
④																																				
⑤																																				
⑥																																				
⑦																																				
⑧																																				
※　検査責任者必須項目																																				

チェック基準

○　全てルール通り行われており、全く問題ない

×　期間中にルール違反があった

△　ルールを知らない者がいたが、指導でルールを守らせた

―　該当する業務が無い

＊毎月のチェック結果を、翌月初(5日迄)に法務担当までメールで送付して下さい。

4-⑹-⑭【実践的な携行ハンドブックの携行を全従業者に義務付け】

（情報サービス業(アウトソーシング等)：約 2,700 人）

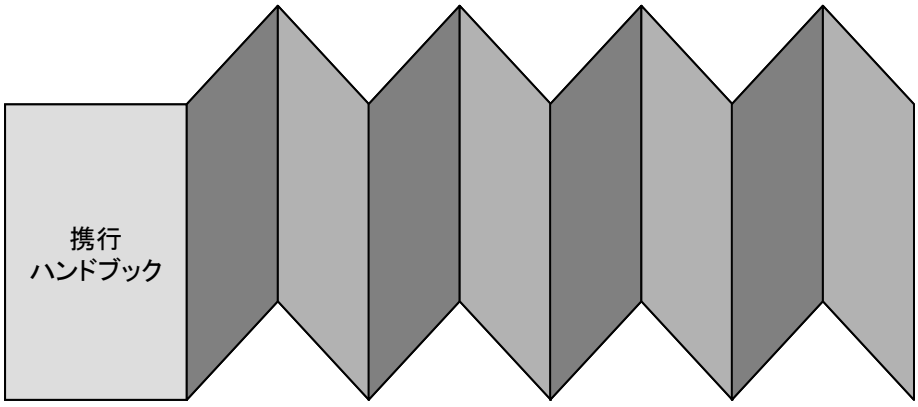
・キ社では、「携行ハンドブック」を作成し、全従業者に携行を義務付けている。毎月、携行ハンドブックが実際に所持されているか、チェックしている。

・携行ハンドブックには、表面が情報セキュリティ、裏面が個人情報保護に関する内容となっており、全体で 18 ページにわたって、手順及び要点を解説している。

・携行ハンドブックは半年近くの検討を重ねて作成した。見開きで閲覧できるよう、配置を工夫している。

・携行ハンドブックは、定期的に見直し、最新情報を掲載している。

図表　携行ハンドブックのイメージ



［主な記載内容］

- 情報セキュリティ推進体制
- セキュリティ対策の項目別の原則、及び実施要領
- 他社秘密情報管理体制
- 個人情報に関する社内手続
  - ✓ 行為別の社内手続、受付窓口、備考
  - ✓ 罰則
  - ✓ ライフサイクル別の手続（商談発生～受託個人情報受領、利用、管理、外部委託、業務終了後（廃棄・返還）

図表　ハンドブック記載事項のイメージ（各見開きで２ページ分）

実施項目		原則	ﾁｪｯｸ	実施要領
データ保護〈アクセス制限〉	ＰＣの保護	・全PC にBIOSパスワード設定 ・全PCにパスワード付スクリーンセーバ設定 ・ノートパソコンを机上に放置しない		
	サーバ アクセス	秘密情報/個人情報の格納サーバ（イントラ用） ・ＩＤ／パスワード設定 ・アクセスコントロール		
	ファイルの データ保護	暗号化		
	可搬記憶媒体	・USBメモリ、メモリカード等使用禁止 （顧客都合の場合に限り申請により許可） ・ポータブルHDDは使用可 ・使用時はドライブ全体を暗号化		
	ＰＣの持込み /持出し	原則持込み/持出し禁止 （特別な場合のみ条件付きで許可）		
	外出時	**「手放すな　とにかく絶対　手放すな」** **「飲むなら持つな、持つなら飲むな」**		
	情報の保管	電子媒体や紙媒体は鍵付ロッカーに保管する		
協力会社	秘密情報 管理義務	水準を満たす業者の選定		
		適正管理義務		
		外部委託		
ネットセキュリティ	ウィルス対策ソフト	全てのPCにウィルス対策ソフトをインストール		
	PCのﾈｯﾄﾜｰｸ接続	業務作業開始前に十分なセキュリティチェックを行う		
		危険な社外アクセス行為の禁止		

実施項目		原則	ﾁｪｯｸ	実施要領
ネット セキュリティ	社外との接続	他の社外ネットワークに接続しない		
データの受渡し	情報の 受渡し方法	許可申請		
		顧客との取り決め		
		直接手渡す		
		次善策はセキュアなネットワーク経由		
		授受データの暗号化・搬送後の媒体からの削除		
		登録申請		
		機微情報は鍵付きトランクで専用デリバリで運搬		
特別注意事項		私的利用の禁止		
		デモデータ、テストデータ適正管理		
		電子メール送受信の注意点		
		ＦＡＸ送受信時の注意点		
		パスワードの適正管理		
		情報の破棄		
		携帯電話の取り扱い		
		紛失・盗難事故発生時は、直ちに報告		

4-⑥-⑮【年 3 回の全社総点検を切れ目無くフォローアップ】

（情報サービス業(アウトソーシング等)：約 1,000 名）

・ク社では、全社総点検プログラムのひとつとして、年 3 回（7 月、11 月、3 月）情報保護月間を定め、各部で点検を実施して結果を報告している。

・全社総点検は、1 年間を 4～7 月、8～11 月、12 月～3 月の 3 つの期間に区切り、それぞれの期間終了時に点検結果の報告を求めているが、毎月情報保護推進委員会において、対応の進捗状況の報告を行っている。このため実質的には一年中切れ目無く自主点検をしていることになる。

・ただし、現場の負荷軽減のため全項目に対する点検は 7 月のみで、残り 2 回はテーマを絞って実施することとしている。

図表　自主点検結果の報告書イメージ

A（一般）

２００８年度情報保護推進状況(第１回総点検)　　最終報告

2008 年 4 月 1 日新規作成
ク社 情報保護推進委員会（事務局）

◆第１回総点検は、各部４～６月に計画、実施。７／３１までに事務局が報告書類を全て受領、内容を確認（「●」がその表示）。

実施項目	自己点検チェックリストによる、点検結果報告書作成	２００８年度第１回総点検項目内訳														<参考> JIS 規格不適合事象への対応（管理強化履歴）
		PMS 文書１（体制、計画、規程、対象整備）			PMS 文書２（ﾘｽｸｱｾｽﾒﾝﾄ整備）				PMS 文書３（教育記録）			PMS 文書４（再委託先）		PMS 文書５（その他点検）	
		体制図 実行計画	内部規定の最新化	個人情報管理台帳 最新化	業務ﾌﾛｰ	潜在ﾘｽｸ管理台帳	残留ﾘｽｸ管理台帳	発生ﾘｽｸ管理台帳	一斉教育(最終)	随時研修	誓約書の再取付け	実査対象	評価 アンケート① 実査 ② 自己評価 ③	※１	
実施期限	4~5 月	5~6 月	5~6 月	5~6 月	5～6 月			5~6 月	5~6 月	随時	5~6 月	5~6 月		5~6 月	
A部	● ●	● ●	●	●	●	●	●	●	最終 最終	⑥⑦	(実施) (実施)	5	①、②、③	①、②、③、④	
B部	● ●	● ●	●	●	●	●	●	●	最終		(実施)	3	①、② ③	①、－、－、④	
C部	● ●	● ●	●	●	●	●	●	●	最終	④⑤⑥	(実施)	－		①、－、－、④	20080718Ⅱ 改定
D部	● ●	● ●	●	●	●	●	●	●	最終	⑤⑥	(実施)	－		－、－、－、④	
E部	● ●	● ●	●	●	●	●	●	●	最終	⑥	(実施)	－		①、－、－、④	20080430Ⅰ 改定
F部	● ●	● ●	●	●	●	●	●	●	最終	④⑤⑥⑦	(実施)	－		①、②、－、④	20080620Ⅱ 7/14 解除
G部	● ●	● ●	●	●	●	●	●	●	最終	④	(実施)	－		①、②、③、④	
H部	● ●	● ●	●	●	●	●	●	●	最終	⑥	(実施)	－		①、②、③、④	
I 部	● ●	● ●	●	●	●	●	●	●	最終	④⑤⑥	(実施)	3→1	①、②、③	①、②、③、④	20080430Ⅰ 改定
J 部	● ●	● ●	●	●	●	●	●	●	最終		(実施)	－		－、－、③、④	
K部	● ●	● ●	●	●	●	●	●	●	最終	－	(実施)	3	①、②、③	①、②、③、④	
LMN部	● ●	● ●	●	●	●	●	●	●	最終	④⑤⑥⑦	(実施)	6	①、②、③	①②③④⑤⑥	

※1．①ＦＤＫ管理、②サーバー管理、③コンティンジェンシープラン、④外来者受付票改定、⑤ウイルス対策、⑥暗号化対策、（各部対応は①～④、事務局対応⑤～⑥）