６．個人情報の点検・監査の場面

本節では、規程等の遵守状況や、管理状況を確認するために定期的に実施される監査に関する取組について取り上げている。

特に個人情報保護のための監査として、ユニークな事例としては、例えば単に監査を実施するだけでなく、社内の異なる部門や部署が相互に監査を実施することで業務についての一定の理解を持ちながら実効性のある監査を実現している事例（⑪）も紹介している。

監査の中身としては、個人情報保護に関する教育・研修方法の効果測定を監査時に実施しているような事例（⑭）や、監査時にルール自体が守りにくいことなどについても指摘を受け、実際にルールも随時見直しを行っている事例（⑮）などがユニークである。

また、一定以上の職歴のある従業者を中心に監査を実施しているような事例（②）、さらには外部の弁護士や学識経験者等による外部委員会を設置して厳格な監査を実施してもらっているような特徴的な事例（⑤）も紹介している。

本節で紹介している取組事例

6-①：社長が従来から行っていた社内点検に個人情報保護の観点を付加
6-②：監査は一定の役職以上のベテラン職員が担当。問題が見られた場合は短期間で是正計画の策定と再監査を実施することで実効性を高める
6-③：各店部で検査員を選任して店部内検査を実施し、これを取り纏め部が指導・モニタリング
6-④：監査は業務監査部門が実施
6-⑤：外部有識者による委員会の設置
6-⑥：監査室による監査とリスク管理室による確認・監視
6-⑦：プロジェクト単位で、顧客企業を訪問して常駐しているチームに監査を実施
6-⑧：プロジェクトごとにチェックシートを作成。ヒアリングに基づく実態把握を実施
6-⑨：テレビ会議を利用した監査を実施
6-⑩：トップの指示により、年に 4 回の監査を実施
6-⑪：監査は異なる部門の監査担当者が複数で実施
6-⑫：監査手法をとった品質指導を実施
6-⑬：用途やチェックの視点に応じて 3 種類の点検・監査を複層的に実施
6-⑭：教育・研修方法の効果測定を監査の際に実施。部署ごとにフィードバック
6-⑮：監査時にルール自体も指導を受け、実際に改善される
6-⑯：内部監査員は地区別の偏りが出ないように内部で育成し、負担の平準化に配慮

6-①【社長が従来から行っていた社内点検に個人情報保護の観点を付加】

（電気・ガス・水道業：約 60 人）

・C 社では月に 1 度、社長が社内を点検している。もともとは社内清掃のチェックの目的で行っていた見回りを、個人情報保護の視点を取り入れて行っている。

・この点検は抜き打ちではなく、事前に通達をしている。それによって従業者の取組を促進すると考えている。

6-②【監査は一定の役職以上のベテラン職員が担当。問題が見られた場合は短期間で是正計画の策定と再監査を実施することで実効性を高める】（卸売業：約 110 人）

・E 社では年に 1 回、内部監査を実施している。15 部署について、2/15～2/26 までの期間を要して実施した。職場の点検だけでも 1 部署 2.5 時間程度掛けて点検を行った。

・監査チームのリーダーは一定の役職以上（部長等）のベテラン社員が担当し、実際に監査員が現場まで立ち入りを行ってチェックをした。

・監査結果については、即日で「適合」、「不適合」、「観察」の評価を下している。「不適合」になった場合には、10 日以内に「是正計画書」を提出し、その計画書を受けて監査員が 18 日以内に「フォローアップ監査」を実施する。また、フォローアップ監査の結果については、23 日以内に「不適合報告書兼是正処置報告書」を提出することになっており、問題点を単なる注意で終わらせないようにしている。

・「観察」は不適合とは言えないが、改善したほうが個人情報保護のためにより望ましいと考えられる場合に出される。

・平成 19 年の監査では、7 件の不適合と 5 件の観察が報告された。

図表　E社で使用されている監査のための書式

個人情報保護の点検に関する規定

［様式-2］

内部監査チェックリスト

確認	作成
監査責任者	内部監査員

頁:2

株式会社[redacted]

監査実施日　2008 年 02 月 19 日
被監査部門　[redacted]
監査チームリーダー　[redacted]

監査基準　JIS Q 15001:2006

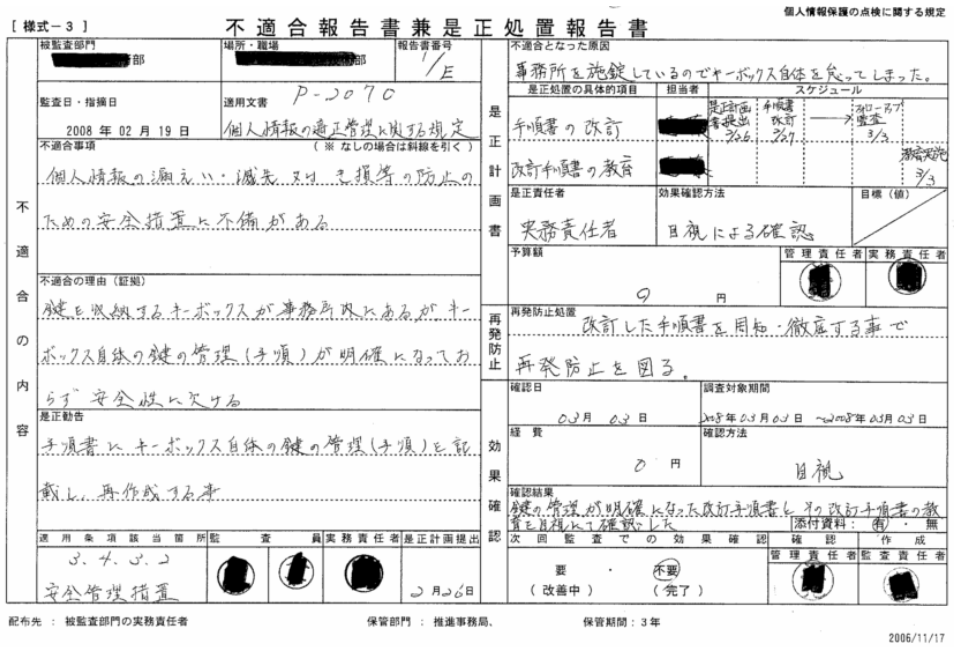
要求事項	チェック項目	対象 本部	対象 部門	判定	質問	コメント
3.3.1 個人情報の特定	☑個人情報を特定する手順は確立され維持されているか		○	○	☑個人情報を特定するとはどういう意味ですか。なぜ特定することが必要ですか	個人情報を保護するため
					☑この部門の「個人情報特定表」を見せてください。	特定表も確認
3.3.2 法令、国が定める指針その他の規範	☑法令、国が定める指針その他の規範を参照するための手順は定められて維持されているか	○	○	○	☑この部門に必要な法令等を言ってください。	個人情報保護法、刑法、就業規則
					☑その法令はこの部門のどんな業務に関係していますか	
					☑その法令が改訂された場合、その改訂されたことをどのようにして知りますか	ホームページ
3.3.3 リスクなどの認識、分析及び対策	☑3.3.1で特定した個人情報について目的外利用を行わないために必要な対策を講じる手順は確立され維持されているか		○	○	☑目的外利用とはどういう意味ですか	
					☑目的外利用を行なわないための手順を説明してください	
	☑3.3.1で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を認識し分析し必要な措置を講じる手順は確立され維持されているか		○	○	☑リスクとはどういう意味ですか	漏えい、紛失
					☑リスクを認識し分析する手順を説明してください	
					☑この部門の「リスク評価表」を見せてください	リスク評価表も確認

判定欄　適合:○　軽微な不適合:×　観察:①、②
（不適合の場合は証拠事実を記入）

保管期間:3年

配布先　被監査部門の実務責任者　保管部門　推進事務局

2007/06/10



個人情報保護の点検に関する規定

［様式－３］

不適合報告書兼是正処置報告書

被監査部門　[redacted]部
場所・職場　[redacted]部
報告書番号　1/E

監査日・指摘日　2008 年 02 月 19 日
適用文書　P-2070　個人情報の適正管理に関する規定

不適合事項　（※ なしの場合は斜線を引く）
個人情報の漏えい・滅失、または毀損の防止のための安全措置に不備がある

不適合の理由（証拠）
鍵を収納するキーボックスが事務所内にあるが、キーボックス自体の鍵の管理（手順）が明確になっておらず安全性に欠ける

是正勧告
手順書にキーボックス自体の鍵の管理（手順）を記載し、再作成する事

適用条項該当箇所：3.4.3.2 安全管理措置
監査員：[redacted]
実務責任者：[redacted]
是正計画提出：2月26日

是正計画書

不適合となった原因
事務所を施錠しているのでキーボックス自体を施錠してしまった。

是正処置の具体的項目	担当者	スケジュール
手順書の改訂	[redacted]	是正計画書提出 2/26 → 手順書改訂 2/27 → フォローアップ監査 3/3
改訂手順書の教育	[redacted]	教育実施 3/3

是正責任者：実務責任者
効果確認方法：目視による確認
目標（値）：
予算額：0 円
管理責任者：[redacted]
実務責任者：[redacted]

再発防止処置
再発防止
改訂した手順書を周知・徹底する事で再発防止を図る。

効果確認

確認日：03月 03日
調査対象期間：2008年03月04日 ～2008年03月03日
経費：0 円
確認方法：目視
確認結果：鍵の管理が明確になった改訂手順書と、その改訂手順書の教育を目視にて確認しました。
添付資料：有 ・ 無

次回監査での効果確認：要（改善中） ・ 不要（完了）
確認：管理責任者 [redacted]
作成：監査責任者 [redacted]

配布先 ： 被監査部門の実務責任者　　保管部門 ： 推進事務局、　　保管期間 ： 3年

2006/11/17

6-③【各店部で検査員を選任して店部内検査を実施し、これを取り纏め部が指導・モニタリング】（信用業：約 700 人）

・J 社では各店部で検査員を選任し、検査項目（全社共通の検査項目と店部独自の検査項目がある）・検査頻度（検査頻度は検査項目毎に定めている）を定めて検査を行なう。

・管理・保管状況に社内ルール違反や問題点が発見されれば、是正を求める。是正措置については、被検査部署から対応策と実施期限について文書で回答をもらった上で、検査員は対応完了の見届けまで行なっている。

・各店部の店部内検査を指導する取り纏め部を儲け、取り纏め部において、店部内検査のモニタリングや検査項目・頻度・検査方法の追加および修正を行なっている。

6-④【監査は業務監査部門が実施】（信用業：約 700 人）

・J 社では監査は社内の業務監査部が実施する。項目が多いため 1 支店 1 週間ほどかかる。2 チーム体制で全国を回っている。

6-⑤【外部有識者による委員会の設置】（情報サービス業：約 1,600 人）

・O 社では個人情報保護に関する第一人者を委員長として、個人情報保護専門の弁護士、生活評論家、情報セキュリティのアドバイザーなど、外部有識者 5 名により構成される「情報セキュリティアドバイザボード」を設置し、同社の個人情報保護の取組について評価と提言をいただいている。

・委員会は、３ヶ月に 1 度開催され、個人情報保護の取組、セキュリティ対策の取組状況や対策の問題点などについて報告を行い、取組や対策についてアドバイスをもらう形式で運営している。また、年に 1 回、情報セキュリティアドバイザリボードから提言書が社長宛に提出され、個人情報保護や情報セキュリティ対策の評価及び提言を受け次期の対応に活用している。

6-⑥【監査室による監査とリスク管理室による確認・監視】（情報サービス業：約 1,600 人）

・O 社では監査室は、社長から承認を得た監査基本計画に基づいて、全部門の情報セキュリティ対策、個人情報保護に関する監査を実施している。

・リスク管理室は、情報セキュリティ対策の確認、インターネット Web 等の利用監視、メールの発信監視を定期的にチェックしている。

6-⑦【プロジェクト単位で、顧客企業を訪問して常駐しているチームに監査を実施】

（情報サービス業：約 380 人）

・P 社では幾つかのプロジェクトを選定し、顧客企業に常駐している場合であっても立ち入り監査を実施している。特に問題があったプロジェクトや、扱う情報のセキュリティレベルが高いプロジェクトが対象となることが多い。

6-⑧【プロジェクトごとにチェックシートを作成。ヒアリングに基づく実態把握を実施】

（情報サービス業：約 380 人）

・P 社ではプロジェクトごとに『顧客の要求する水準を維持できているのか』という視点で監査を行う。まず顧客企業に話を聞きに行き、要求されるセキュリティ水準やポイントとなる管理の方法などを確認した上で監査を実施する。

・監査の際には、事前に、プロジェクトごとの個別チェックシートを作成した上で、実施している。また、現場を見回るだけでなく、プロジェクトメンバーの数人を選んで個別ヒアリングを実施して事情を確認している。

6-⑨【テレビ会議を利用した監査を実施】

（情報サービス業（コールセンター等）：約 2,500 人）

・Q 社では 1 年に一度、社内、コールセンター、入館許可がとれた顧客先で監査を実施している。定められた記録や教育がなされたかどうかを確認している。

・フォローアップ監査については後日書面で実施している。実際の運用状況については半年ごとに点検を行い確認している。

・ 現在、テレビ会議を利用した監査も行なっている。すべての項目について現地で監査を行うことより、事前にテレビ会議で監査項目を開示し、実施に支障のない項目の監査はテレビ会議で終えてしまう方が効率的である。同社では、テレビ会議を積極的に業務に活用しているため、抵抗が小さい。

・「個人情報保護マネジメントシステム要求事項　JISQ15001：2006」に準拠した監査ハンドブックを作成し、教育資料としている。

6-⑩【トップの指示により、年に 4 回の監査を実施】

（複合（情報システム／製造）：約 500 人）

・R 社では専任の監査部門がある。ISMS に詳しい者が監査を行っている。

・この他に内部監査人として社内 33 名、グループ会社 14 名が担当している。内部監査人は、ISO14001 と 9001 の監査ができる人が任命される。

・社長の指示により、監査を年に 2 回から 4 回に増やした。

・個人情報保護の担当者が、今までに 2 回抜き打ちで全事業所を点検している。朝の誰もいない時間帯に訪問し、問題があればレッドカードを発行する。

・自己チェックとして従業者が互いにチェックし合う制度がある。

6-⑪【監査は異なる部門の監査担当者が複数で実施】

（その他サービス業（印刷・広告）：約 11,000 人）

・X 社では各事業部内に各種責任者（法令及びその他の規範調査、教育、苦情及び相談窓口、委託契約内容確認、委託業者管理）と監査責任者をそれぞれ任命している。

・日本情報処理開発協会（JIPDEC）によると、監査には客観性が求められ自部門の監査ができない。しかし、同社の業務内容は多様であり、監査を受ける部門の業務内容にある程度通じている者が監査に入らなければ、業務内容が分からず適切な監査ができない。そのため、同社では監査を受ける部門に近い部門に所属する監査担当者とそれ以外の部門の監査担当者が複数で監査している。

6-⑫【監査手法をとった品質指導を実施】

（その他サービス業（印刷・広告）：約 11,000 人）

・X 社では監査手法で品質事故防止のための指導をしている。従来は「品質事故」とされていたものが、「個人情報保護法違反」になるケースがあるため、品質を向上させることは個人情報保護の推進のためにも重要であると考えている。

・この監査は、書類が整っているかどうかだけの監査ではない。品質管理の担当者が現場に出向き、1 部署あたり最大 15 人日ほど実際の作業に立会いながら個人情報の管理方法をチェックするものであり、製造実務に係わる監査である。例えば品質保証のルールとその遵守状況、機械停止時の操作、目の動き、ゴミ箱の形、服装、といった細かいことまでチェックし、不適切な点があればその場で指導する。

・協力会社に対しても監査を毎年 1 回行っている。結果によっては認定の取消をする場合もある。

・また、従業者、パート、アルバイトにアンケートで、現在実施している作業の中での不安や工夫している点を聞き、監査項目を抽出した。

6-⑬【用途やチェックの視点に応じて 3 種類の点検・監査を複層的に実施】

（その他サービス業（ダイレクトメール等）：約 600 人）

・Z 社では点検・監査は以下の 3 種類を行っている。

・早朝抜き打ち監査：施錠のチェック、個人情報が記録された書面や媒体が机の上に放置されていないかなどを半年に 1 度程度の頻度で早朝にチェックする。不適合があった場合は改善報告書を提出させ、その 1 ヶ月後にフォローアップとして再び点検を行う。点検で 2 回不備が発見されると、部長が始末書を提出する。上期の点検で問題がない場合は、下期の点検は免除している。

・オフサイトモニタリング：WEB の使用状況のログをチェックしている。休日にわけも

なくネットワークを利用していないか、利用禁止のサイトを閲覧していないか、などを監査する。
・事前通告の点検：データの授受が適切にできているか、データの受け渡し時に顧客の証印をもらっているか、アンケートの枚数確認をしているか、などをチェックする。
・半期に一度、社長出席の下、監査報告会をしている。

6-⑭【教育・研修方法の効果測定を監査の際に実施。部署ごとにフィードバック】
（情報サービス業(コールセンター等)：約 2,500 人）
・Q 社では、教育内容の浸透度を確認するために、各拠点のオペレータに直接監査を実施している。「オペレータ個人の理解度を確認する」というよりも、教育・研修方法の効果測定が第一の目的である。同じ教育・研修を受けたオペレータは同様の回答をすることが多く、管理者の意識レベルがそのまま影響することがうかがえる。
・監査結果については、当該部署別にフィードバックし、全社的な傾向分析結果をコンプライアンス委員会で発表している。

6-⑮【監査時にルール自体も指導を受け、実際に改善される】（信用業：約 2,000 人）
・カ社では、監査実施の際に、規程遵守の不徹底の部署が多く認められる場合には、被監査部署が指導を受けるのみでなく、ルールを作った事務局側も指導を受けることになる。これはルール自体が業務フローに適していないなど、「守れない仕組み」を構築したことに対する指導であり、それによってルールを変更することもある。
・監査室は「監査における指摘事項への対応未済リスト」を持っており、監査の指摘事項は全体的に周知される。

6-⑯【内部監査員は地区別の偏りが出ないように内部で育成し、負担の平準化に配慮】
（その他サービス業(印刷・広告)：約 1,400 人）
・コ社では、内部監査員の養成が必要になっている。個人情報に関しては昨年から養成を開始した。今年度から営業店勤務職員の一部に、内部監査員になってもらった。
・部署、部門や支店・営業店間では、内部監査員がたすきがけで監査を実施するようにしている（A 支店の内部監査員がB支店の監査を行い、逆に B 支店の内部監査員が A 支店の監査を行うような体制)。
・内部監査員は社内資格として取得してもらうようにしている。課長・係長クラスの人が担当されている。地区別に何名か出してもらうようにした。これは、あまりに特定の地域に監査員が固まると、そのような地域の監査員が、監査員が全くいない遠くの地域にある支店等まで監査に行かなくてはならなくなる状況を懸念したことが理由である。