http://www.tokiorisk.co.jp/

TRC EYE Vol. 193

東京海上日動リスクコンサルティング（株）
情報グループ
主任研究員　本多　尚登
リスクコンサルタント　平岡　孝雄

マンネリを解消するマネジメントシステム内部監査とは

はじめに

近年、業種や規模を問わず全ての企業にとって、情報セキュリティや個人情報保護は避けて通れない経営課題の一つです。企業として事業を続ける以上、これらのリスクをゼロにすることは不可能であり、各種の対策を導入してリスクを許容水準以下にコントロールすることも一朝一夕にできることではありません。

こうした継続的な取り組みが必要となる経営課題を、組織的な仕組み作りによって解決していく手法として、ISO や JIS が発行するマネジメントシステム規格の活用があります。情報セキュリティや個人情報保護の分野では ISO/IEC27001[1]や JISQ15001[2]があり、それぞれの規格の適合性に関する第三者認証制度として「ISMS 適合性評価制度」や「プライバシーマーク制度」が広く認知されています。

このようなマネジメントシステム規格は、いずれも PDCA サイクルを運用することで継続的な改善を行なうことが定められており、その中の C（check）では、日常的な点検とマネジメントシステム内部監査を実施することが求められています。これらの活動を通じて課題や問題点が洗い出され、それが経営者の参画するマネジメントレビューのインプットとなって、A（act）の改善へとつながる仕組みになっています。

このように C（check）→A（act）の活動が機能することで、はじめてマネジメントシステムの導入効果が発揮されるのですが、現実にはマネジメントシステムを構築し、P（plan）→D（do）の局面で「息切れ」してしまっている例も少なくありません。特に経営者からのバックアップが十分ではない事務局では、「通常の業務量が多すぎて、内部監査にまで手が回らない。」「忙しい現場部門から協力を得られない。」といった事情で、マネジメントシステム内部監査が形式的に繰り返されるだけで、パフォーマンスが上がらず、結果として有効な改善に結びつかないという悪循環に陥っています。

このような現状を踏まえ、本稿では、主に JISQ15001（個人情報保護マネジメントシステム）を例にとりながら、マネジメントシステム内部監査の有効性および効率性を高めるアイデアを紹介したいと思います。

Ⅰ．効率と効果の両方を上げる内部監査の体制とは

JISQ15001 では、組織の代表者から指名された個人情報保護監査責任者が内部監査チームを率いてマネジメントシステム内部監査の実施を統括することになっています。そして、内部監査チームとして編成された内部監査員は、必要な力量があること、公平かつ客観的に行なえる立場にあることが求められているため、自己の所属する組織の監査をすることができません。

---

[1] ISO/IEC27001:2005 (JISQ27001:2006) 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項

[2] JISQ15001:2006 個人情報保護マネジメントシステム－要求事項

このような規格の要求事項に適合するため、多くの企業は、以下の 3 つのパターンのどれかに該当する内部監査体制を構築しています。

パターン①	マネジメントシステムの事務局メンバーが、内部監査員として自己の所属する部門以外を監査する
パターン②	マネジメントシステム内部監査を担当する部門（例：内部監査部、品質保証部等）が事務局とは別に設置されており、当該部門が自己の所属する部門以外を監査する
パターン③	内部監査員が各部門から指名されており、それぞれが自己の所属する部門以外を監査する

パターン①及び②では、内部監査員が特定の単一部門から編成されているため、当該部門を監査する仕組みが別途必要となります。一般には、個人情報保護監査責任者や他の組織[3]が内部監査員の所属する部門を監査することになります。

一方、パターン③は、複数の部門（通常、全社各部門）に所属する内部監査員によって編成されているため、自己の所属する部門以外を互いに監査することが可能です。このような仕組みを一般に「相互監査」と呼びます。相互監査のメリット・デメリットは以下の通りです。

メリット	デメリット
1. 内部監査員としての事務局の負担が軽減される 2. 多くの部門から内部監査員が指名されることで、被監査側としてだけでなく、監査側として参画することとなり、全社的な取り組みとしての認識が高まる 3. 内部監査員の育成、監査の実施を通じて、現場の意識向上、教育効果が見込める 4. 内部監査員が監査を通じて、自己の所属する部門と被監査部門を比較する機会ができる。その経験を通じて、互いの改善活動の活性化が期待できる	1. 一般に個々の内部監査員の力量のバラツキが比較的大きいため、内部監査員の育成コストが増加する。また、特に専門知識が必要となる監査（例：情報システム部など）を実施するにあたって、必要な力量を確保するのが困難となる可能性がある 2. 部門を超えた編成となるため、内部監査チーム内のコミュニケーションが不足しがちとなる 3. 内部監査員と被監査部門の間で不適切な監査プロセスが行なわれることで、監査の中立性・公平性、被監査部門に関わる情報管理（守秘義務）、内部監査員の身分の保証等が脅かされる可能性がある

相互監査のメリットをうまく引き出すことで、マネジメントシステム内部監査の効率性・有効性を向上させる効果が期待できます。また、デメリットとして挙げられている項目については、実施手順やチェックリストの工夫によってカバーすることが可能です。従って、総合的に考えると多くの企業にとって相互監査の導入メリットは大きいといえます。

[3] 事務局と内部監査担当部門（例：内部監査部、品質保証部等）が相互監査を行なうケースや、事務局に対する監査のみ個人情報保護監査責任者から委託を受けた社外の専門家・コンサルタントが行なうケースがあります。

Ⅱ．内部監査員が陥りがちなインタビュー時の落とし穴

現地監査において各部門の管理責任者や従業員に対してインタビューを実施する際、時間管理は重要です。各部門は通常業務の合間に時間を割いてマネジメントシステム内部監査に臨んでいるので、事前に調整したスケジュール内に監査実務をこなすことが必要です。

内部監査を事務局や内部監査部で行なう場合も同様ですが、特に相互監査において、経験の浅い内部監査員は、インタビューの進行がうまくいかなくなると、時間がどんどん押していくため、終了間際に最後の質問まで辿り着こうとして慌ててしまいがちです。結果として、インタビューが途中で打ち切りになったり、終了予定時刻を大幅に超過したりすることとなります。

以下にインタビューの進行がコントロールできなくなるケースを例示しながら、このような事態の原因を考えてみましょう。

【ケース１】内部監査員がしどろもどろになる

内部監査員の力量不足が原因といえますが、更に整理すると以下の 3 点が考えられます。

原因① 監査経験不足	現地監査の進行が理解できていない。あがってしまい、うまく話が進まない。（特に相手が役員、強面の管理職の場合や相手が監査に非協力的で会議の雰囲気が非常に悪い場合が考えられます）
原因② チェックリストや規程の理解不足	チェックリストや規程を理解できていない。何を質問しようとしているのか、内部監査員本人が正しく理解していない。
原因③ 現地監査にあたっての準備不足	上記、原因②も準備不足の一種といえるが、その他には被監査側についての基本情報を把握しないまま現地監査に赴いている場合が当てはまる。この場合、いくらチェックリストや規程をよく理解していても、スムーズな進行は期待できない。

【ケース２】被監査者が質問の意味を理解できない、回答を持っていない

内部監査員がチェックリストに従って質問をしても、被監査者から全く回答を得られず、場が混乱するばかりで進行しなくなる場合があります。

原因① 質問する相手が違う	管理職から担当者まで、全て同じレベルで業務や作業手順を理解しているわけではないことを忘れてはならない。 例えば、社内の各種申請書の承認プロセスにおいて起票する者と承認印を押す者とは立場が違い、当該プロセスやその前後のプロセスに対する理解度は異なる。従って、質問の主旨（何を確認したいのか）と相手の立場の違いをよく理解した上で質問する必要がある。 また、質問する相手を間違えると、回答者の思い込みや勘違いから、誤った情報がインプットされて、後で事実誤認として訂正しなければならなくなる可能性も高くなることに注意する。
原因② 質問の仕方	チェックリストを見ながら質問を棒読みするだけでは、こちらの質問の意図が相手に伝わりにくい。 特に、時間が限られている中で、矢継ぎ早に質問するような状況では、質問が唐突過ぎて、相手が話についていけなくなる場合がある。 上記、原因①でも触れたように、適切な相手に対して、相手が理解しやすい質問を投げかけることが重要である。
原因③ 言葉使い、用語の定義の違い	同じ組織の中でも部門が違うと言葉も違うことがある。 特に、情報システムに関しては、情報システム部門とユーザ部門では技術的な理解度が異なるため、用語のすれ違いがあることに注意する。 例えば、コンピュータに詳しくない被監査者は「ファイルサーバ」「ローカルディスク」と言ってもピンとこないが、「Ｎドライブ」（ファイルサーバの共有フォルダがマップされているドライブ名）や「Ｃドライブ」といえばどこを指すのかわかる、といった具合である。

【ケース３】被監査者の話が発散する、論点がずれる、すり替わる

内部監査員の立場としては、被監査者が積極的に発言してくれることを歓迎すべきことですが、行き過ぎるとコントロールできなくなる場合があるので注意が必要です。

原因① 質問の仕方	上記、【ケース２】原因②と同様に、質問の仕方によっては、こちらの意図しない反応が返ってくる場合がある。 質問の仕方が具体性に欠けていたり、被監査部門の状況とはマッチしなかったりすると、積極的な被監査者は、自分なりに解釈し、何とか自分の知っている範囲で答えようとする。 この事態を回避するためには、インタビュー全体を通して、常に相手の理解している業務範囲を確認しつつ、もし意図しない反応が返ってきたら、必要に応じて補足説明をする、別の人に質問しなおす等、速やかに軌道修正していくとよい。軌道修正にあたっては、回答者の心証を害さないよう、十分配慮する必要がある。
原因② 被監査者の個人的興味や性格	上記、原因①に当てはまらなくても、被監査者が話好きであったり、特定のテーマ（例：インターネット、ウイルス等）に強い興味があったりすると、話がどんどん脱線し、進行の妨げとなる場合がある。 また、ここぞとばかり、日頃の不平不満をぶちまけられる場合

	もある。 このようなケースを切り抜けるには、やはり相手が不快に感じないよう、うまく話を切り上げて次の質問へ進むしかないが、時間が許す限り、相手に話をさせるのも一つのアプローチである。 なぜなら、積極的に話をするという姿勢はそれだけでも現場の関心度、モチベーションの高さの表れであるし、不平不満は現場だからこそ見えている問題点である可能性が高い。そういった潜在的な問題点をうまく拾い上げて是正・予防措置につなげていけば、マネジメントシステムの改善に大きく貢献する可能性がある。

Ⅲ．内部監査を成功に導くチェックリストの作り方

チェックリストの内容としては、チェック項目と質問文を記載することが一般的です。チェック項目は規格や規程の文言そのままで、それを噛み砕いた文を質問欄に記載しているチェックリストが多くみられます。そのようなチェックリストを使用する場合は、質問の順序がインタビューの流れに合わないため、会話が「行ったり来たり」にならないか、内容が重複している質問が続くため、何度も同じような回答を求めていないかを事前によく確認しましょう。

チェックリストをこれから作る場合は、まず監査テーマに従ってチェック項目を洗い出し、その全項目を被監査者から効率よく聞きだすための質問を整理して、質問欄に記載しましょう。順序良く、そして重複無く質問することが目的ですので、チェック項目と質問が１対１になる場合もあれば、１対ｎ、つまり複数のチェック項目をひとつの質問でまとめて聞いてしまうという場合もあります。

内容にもよりますが、チェック項目数と質問数の関係は内部監査員の力量によっても変わります。マネジメントシステムを導入してまだ日が浅く、内部監査員の力量も十分ではない場合は、チェック項目と質問は１対１の形として、定型的な質問によって、広く網羅的に規格への適合性及び規程の運用状況をみることをお勧めします。特に深く切り込みたいチェック項目については、一つのチェック項目に対して複数の質問を投げかける必要も出てくるかもしれません。（チェック項目数≦質問数）

内部監査員の力量が向上していくにつれて、複数のチェック項目を効率よく質問することが可能となり、また、マネジメントシステムの成熟によって質問の内容が高度化していくことで、定型的な質問文としてチェックリストに記載しておく必要性が下がりますので、結果として、チェック項目数に比して質問数が減少することとなります。（チェック項目数＞質問数）

チェックリスト作成時のポイント

どの程度詳しいチェックリストを用意するかは、監査プログラムの規模や内部監査員の平均的な力量に合わせて（場合によっては最も力量の低い内部監査員に合わせて）検討します。その際、内部監査責任者および内部監査チーム（事務局）において、チェック項目の優先度を決めておくことをお勧めします。その優先度に沿って、チェックリスト上で時間が無くてもこれだけは必ず確認する、という重点項目を設定するとよいでしょう。特に記録をきっちりとっておきたい項目や、現場の実態を調査するための項目については、インタビューの最初に聞くか、あるいは別途そのための時間をとっておく（例：ラスト５分間はこの質問をする、など）と時間管理がしやすくなります。

質問パターン（５Ｗ１Ｈというけれど・・・）

よく紹介されている質問方法として、「はい」または「いいえ」で答えられるような質問（y/n 形式）ではなく、なるべく５Ｗ１Ｈ（who、what、when、where、why、how）で質問（wh 形式）することが推奨されています。しかし、y/n 形式で質問した後に、wh 形式で二の矢、三の矢の質問を用意してお

くと、議論が発散せずに有効であることも覚えておきましょう。

また、内部監査ではチェックリストに列記した項目だけでなく、関連事項についての現場の問題意識や意見の集約も重要です。なぜなら、それらは改善の糸口としてマネジメントレビューへの重要なインプットとなる可能性があるからです。そのような意見・要望を出しやすくするため、質疑応答だけでなく議論の時間を設けることも時には効果的な場合があります。ただし、そのままでは話が発散してしまうので、テーマをよく理解してもらうこと、時間を区切ること、質問する相手をよく考えておくことを忘れないようにしましょう。

チェックリストの呪縛

チェックリストの作成は重要な準備作業ですが、現地監査当日は視線をしっかりと被監査者に向け、チェックリストから自分をフリーにしましょう。逆説的に聞こえるかもしれませんが、準備に時間をかけて、よく練り込まれたチェックリストほど、当日は参考程度で利用するにとどめ、全体の流れを大切にした方がインタビューはうまくいきます。

チェックリストにこだわりすぎると、柔軟性を失うだけでなく、視野が固定されて、想定していたストーリーから外れた途端、話の全体像が見えなくなる危険があります。そのような想定外の場面に遭遇した時こそ、マネジメントシステム改善への意外な発見があるかもしれません。視野を広く持ち、被監査者の話に耳を傾けてください。

Ⅳ．改善につながる効果的な指摘とは

前向きな気持ちでつける「不適合」

マネジメントシステム内部監査の中で、規程の不備や運用の不徹底等が事実として明らかになり、それが規格等の要求事項に適合していない場合は「不適合」となります。マネジメントシステムの導入初期は、比較的多くの不適合が検出されることでしょう。しかし、内部監査の回数を重ねて、運用も定着していくにつれて、記録漏れやうっかりミスのような軽微な不適合が散発的に検出されるだけで、本質的な改善につながるような「良い指摘」がなかなか出てこなくなります。いわゆるマンネリ化といわれる状態ですが、これにはいくつかの原因が考えられます。

一つ目は、内部監査員の力量が低迷したままで、より高度な内部監査を実施できるだけの力量に達していないという点です。毎年同じような社内研修や説明会に参加しているだけでは、なかなか力量は向上しません。また、企業規模や事業内容によっては、隣の部門の業務内容がわからないということも珍しい話ではありません。そのような場合は、被監査部門の業務について、事前に基本情報としてインプットするか、チェックリストの項目にあらかじめ質問を用意しておくなど、内部監査員の理解を助ける配慮をしてください。

二つ目は、内部監査の実施内容に変化が乏しく、新しい監査テーマに切り込めずにいる場合です。被監査部門は良くも悪くも監査に慣れてきます。毎年同じような質問を繰り返していても、取り組みが遅れているところや弱いところが見えてきません。監査テーマの決定に際しては、「広さ」だけでなく「深さ」も考える必要があります。しかし、広さ（＝網羅性）の確保に偏り過ぎると、どうしても深く切り込む余力が無くなります。場合によっては、絞り込まれた監査テーマについて重点的に実施する年度（PDCA の１サイクル）があってもよく、「広さ」と「深さ」の両立を図るために複数年度の内部監査計画を立てることも検討してみましょう。

三つ目として、これらを包含する根本的な原因として存在するのが、不適合をつける（つけられる）という行為に対する社内全体の心理的な障壁です。マネジメントシステムの内部監査においては、あくまでも組織全体の改善のために不適合をつけるのですが、現実は自部門の内部監査で不適合がつくと、それを不服として強硬に反発したり、部下を叱りつけたりする部門の長が少なくありません。そうなると、不適合をつける行為が各部門から編成されている内部監査員にとっても酷く重い決断となり、結果として、不適合をつけずに何も検出されない内部監査が繰り返されることとなります。このような企業

は、「問題がない（ように見える）代わりに、何も改善されない組織」となります。

この傾向は、指摘の段階にも現れます。通常なら不適合となるところが、「観察事項（不適合ではないが改善が望まれる事項）」にトーンダウンして、結果として是正処置の優先度やその後のフォローアップの取り扱いが軽くなる等があげられます。また、「口頭指摘」を有効としている企業では、口頭指摘が多くなって文書として記録に残らず、多くの問題が現場の中で処理されてしまうといった事態となります。

一方で、「不適合」という言葉に心理的な障壁があるとして、「要改善事項」や「指摘事項」といった別の用語を定義する企業もあります。名前だけ変えても実質的には変わらないという意見もあるかもしれませんが、どのような言葉を使うにせよ、内部監査員は前向きな気持ちで不適合をつけること、そして、被監査者もまた前向きな気持ちでその不適合を受け入れることが重要といえるでしょう。

「観察」をつけることは意外に難しい

観察事項には、改善を促す場合と後述の Good Point として取り上げる場合と二つのパターンがありますが、時折、どちらをつけるべきか迷うことがあります。一見、矛盾しているように思えますが、例えば、現場の取り組みが事務局の意図していない方向ではあるものの、現場なりに課題意識を持ち、真剣に考えて独自の解を導き出しているような場合が当てはまります。

どちらにすべきという決まった答えはありませんが、独自の取り組みを好意的に受け止めることもできますし、全社ルールからの逸脱行為として受け止めることもできるでしょう。また、全社ルールが現場の個々の事情に対応し切れていないという視点から、事務局の問題と位置づけることも可能かもしれません。

筆者の私見としては、こういった「出る杭」を積極的に受け入れる姿勢は組織全体の参加意識の向上、および改善活動の活性化という視点で有効と考えますが、どういう指摘の仕方をするにせよ、観察事項として取り上げて、マネジメントレビューの場で活発に議論してほしいと思います。

「Good Point」のつけ方

規程に定められているルールより更にレベルの高い取り組みを行っている場合や、ルールを守るために独自のアイデアで運用上の工夫を行っている場合に模範的事例として Good Point をつけます。積極的な行いや模範的な行いを褒めることで組織のモチベーションが向上する効果と、良い取り組みを他組織へ水平展開していくよう促すという効果が期待できます。

また、例えば取引先や親会社といった外部組織から日常的に厳しいチェックを受けているような組織にとって、マネジメントシステム内部監査でポジティブな面を積極的に取り上げることは、現場の疲弊（いわゆる、「監査疲れ」と呼ばれるもの）や閉塞感に対する良い刺激となるかもしれません。

しかし、その対象組織の良い面を探して、的確な Good Point をつけることは簡単ではありません。人間関係と同様に、相手の悪いところを非難するより、良いところを褒めることの方が難しいのです。例えば、ある部門で行われている表面的で「ウケ狙い」の行為に対して Good Point をつけたら、組織全体にどのような影響が出るでしょうか。その部門の長や担当者からすれば「してやったり」かもしれませんが、事情を知っている当該部門や他部門の関係者にとっては不公平感も感じるでしょうし、内部監査の仕組みに対する不信感にもつながりかねません。また、表面的な取り組みを助長するというミスリードにつながる可能性もあります。

一方で、内部監査チームの実感として、目に見えるような独創的な取り組みはないものの、決められたことを決められた通りに遂行する非常に真面目な部門を評価したいと感じることがあります。このような部門に対して Good Point の根拠として有効な客観的事実がない場合は、取り組みの有効性評価や目標達成度評価を指標として、その評価の高さや継続性（評価を安定的に維持している）に対して Good Point を出すというのも一案です。

以下に、良い Good Point、つまり、組織全体にとって良い影響を及ぼす Good Point をつける判断基準を考えてみましょう。

①公平感はあるか？全社的に納得を得られるか？

Good Point をつける理由を明らかにすることが第一です。全社的な納得感を醸成するため、定量的な評価でなければならないという考え方は、常に正しいとは限りません。マネジメントシステムの目的やトップマネジメントの意思と整合していることを説明できれば、定性的な判断だとしても十分納得感のある指摘ができます。逆に、過度に定量的な評価に傾倒すると、図らずも点数稼ぎに長けている部門が有利となり、結果として企業全体の納得感が下がってしまう可能性もあります。

②他部門にとって模範となる考え方か？水平展開する価値があるか？

独創的な取り組みの背景として、その部門固有の事情が動機付けとなっている場合があります。そういう取り組みに Good Point をつけると「あの部門は特殊な事情があるから・・・」という他部門の声が聞こえてくるかもしません。しかし、その取り組みの手法や考え方が他部門にも応用できる（＝水平展開が可能である）ならば Good Point をつける価値があるといえます。

例えば、ある部門が取引している特定の顧客の要請を受け、全社ルールより厳しいローカルルールを策定・運用しているケースを考えてみましょう。この場合、ローカルルールをそのまま他部門へ水平展開することが、必ずしも全社的な改善となるとは限りません。Good Point は、厳しいルールそのものに対してではなく、「顧客満足を向上させるため（＝顧客からの要求事項に適合することを確実にするため）に自部門の取り組みとしてローカルルールを設定したこと」に対してつけるのです。

このような視点でつけられた Good Point は、他部門においても、それぞれのステークホルダーのニーズを理解し、自部門の取り組みに反映させる姿勢として、考え方を応用することが可能となります。

③Good Point を得た部門が喜ぶか？実務担当者のモチベーションアップにつながるか？

意外かもしれませんが、Good Point をつけられた部門の全ての人が必ず喜ぶとは限りません。実務担当者が上司や取引先等から無理なルールを強要されて、仕方なくやっているような場合もあるからです。また、部門の長が誇らしげに喜んでいるものの、実務担当者の間ではしらけたムードという場合もあることに注意しましょう。

同じ褒めるにしても、実務担当者のモチベーションが向上するような観点で褒めることが重要ですので、Good Point のコメントの書き方にも気を使ってください。

まとめ

情報セキュリティマネジメントシステムや個人情報保護マネジメントシステムを構築し、第三者認証も取得しているが、どうも最近閉塞感がある、マンネリ化していると感じている企業は、過去の実施記録とこれから実施される内部監査の進行状況を注意深く観察してください。

実施手順に非効率な部分はないか、内部監査員の力量は年を重ねるごとに向上しているか、任命を受けた内部監査員から不満は出ていないか、指摘内容は質的に変化しているか（毎回同じ不適合が繰り返されていないか）等、色々な観点で評価することによって問題点・課題が見えてくるはずです。

特に、今まで内部監査のパフォーマンス向上への取り組みが十分でなかった企業は、必要以上に重厚な手順を持て余していたり、内部監査員の力量を正しく評価できていなかったりするかもしれません。それらの問題点・課題を一つ一つ改善し、より軽く、より良く効く（＝効率良く、効果的な）内部監査を実現すれば、マネジメントシステム全体のパフォーマンス向上にも大きな改善効果が期待できます。企業がマネジメントシステムを運用するにあたって、内部監査はその成熟度が如実に現れる部分といえるでしょう。

以上

（第 193 号　2008 年 7 月発行）