＜研究論文＞

情報セキュリティ内部監査の品質向上に向けた提言

The Proposals for the Corporate Internal-Audit Quality of Information Security

黒川信弘
Nobuhiro Kurokawa
情報セキュリティ専門監査人

概要

最初に多くの企業において実施されている情報セキュリティの内部監査に関しての実態と内在する諸問題を示す。次に内部監査の目的と効果を再確認し、それを実現する内部監査の品質とは何か、その実体を具体的に示し、品質評価のため５段階の指標を提言する。

また内部監査の品質を確保する施策として、品質管理的な手法、および監査人の教育訓練プロセスも含めた内部監査プロセスに対する品質マネジメント的な手法を論じる。最後に内部監査本来の目的を達成するために、兼任内部監査人を想定した内部監査手法と専門監査部門の強化による高位品質レベルを目標とした内部監査プロセスとしての次のステップへの移行を提言する。なお、本稿では事前に有識者に対して行ったアンケートの回答を随所に参考として挙げる。

キーワード：情報セキュリティ、内部監査、品質、監査人、内部監査プロセス

はじめに

企業における情報セキュリティの取組みの大きな柱として、内部監査がある。ISMS[1] 適合性評価制度（以降、「ISMS」と言う。）やプライバシーマーク制度（以降、「P マーク」と言う。）の認証取得企業が増えるに従い、マネジメントシステムにおける内部監査というものが多くの企業で実施されるようになった。企業内における情報セキュリティに関する取組みを自己評価するプロセスである。

ところが企業が多くの資源を費やし内部監査を実施している割には、最近、この内部監査の品質に関して問題があるという声を多く聞くようになった。ISMS や P マークの審査だけのために形式的に内部監査を実施しているとか、毎年同じメンバーが訪れては同じ質問をして帰っていく、隣の職場の従業員が即席栽培の内部監査人となり、形だけの確認をして監査を実施したという実績つくりをしている。そんな話を聞くと、最近の内部監査はマンネリ化し、形骸化し、儀式化してきているのではないかと危惧する。

そもそも企業が内部監査に求めるものとは何であろうか。内部監査の目的は、内部監査の効果は、何であろうか。それらを達成するための内部監査の品質をどう確保しているのであろうか。内部監査の品質に関してもう少し深堀する必要があると考えた。内部監査に

2012/5/21 受付、2013/1/11 受理

はどのような品質を求めたらよいのだろうか。求められるレベルはどの程度のものであろうか。また現実に内部監査を実施した結果、情報セキュリティ事故は減っているのであろうか。内部監査の効果を企業はどう評価しているのであろうか。

そのような疑問を持って早速内部監査の品質とは何かを調べてみた。しかし内部監査の品質そのものを言い表した文献や文書というものはあまり存在しない。内部監査の品質を確保するための施策を記述した文書はISO19011[2][3]等[1][2]に見られるが、肝心の監査の品質とは何であるかについては明確ではない。

本稿は、それら疑問の解明のため、内部監査の品質に焦点を当て、内部監査の品質とは何か、品質確保のためにどのような対策をすべきか、ということを中心に論じる。尚、本稿の論述の中心は定常の内部監査部門を保有する中規模以上の企業組織を対象としているが、内部監査部門を定常化できない小規模組織においても十分に参考となるものである。

また本稿は事前にそれらの疑問に対して、有識者へのアンケート[3]を試みた。そのアンケート結果も参考にしながら論述を進める。

1. 企業内内部監査の実態

1.1　企業における内部監査の実態

ISMS認証取得組織4,172、Pマーク付与事業者12,799社（いずれも2012.11.29時点）をはじめ、情報セキュリティに関する他の認証を取得した事業者も含め、かなりの事業者が情報セキュリティ対策活動を進めている。こういった企業の中では情報セキュリティ事故の抑止、および組織内の情報セキュリティレベルの向上を狙って、内部監査を実施している。

Pマークの内部監査への要求事項では、JIS Q15001[4][5]の「3.7 点検」の項目で、“代表者が個人情報保護監査責任者を指名し、PMS[5]がJIS Q15001の要求事項と合致していることとPMSの運用状況の二つを定期的に監査させること”を要求している。併せて監査の計画、実施、報告のプロセスの手順に関しても若干の要求がある。

ISO27001[6][4]の内部監査への要求事項は、「6. ISMS内部監査」の項目で”ISMSの管理目的、管理策、プロセス、手順について定期的に監査すること“となっている。監査にて確認すべきこととして、”規格の要求事項に適合していること、関連法例・規制に適合していること、明確にされた情報セキュリティの要求事項（自社の規格）に適合していること、有効性の評価／計画したように実施されていること“と規定している。またPマーク同様に計画、実施、報告のプロセスに対する若干の要求事項が存在する。

しかし、いずれの規定にも、誰が内部監査を実施するのか、および内部監査の品質についての直接的な明示はない。

一方、企業の中では実際に内部監査はどのように実施されているのであろうか。筆者は、システム監査学会・情報セキュリティ研究プロジェクト（情報セキュリティ専門監査人部会含む）、及び情報システムコントロール協会・東京支部調査研究委員会内システム監査・保証研究会に協力を得て、2010年12月17日から2011年1月31日にかけて“内部監査の品質に関してのアンケート”を実施した。本稿ではこのアンケートの結果も参考にしながら本テーマを論じて行く。

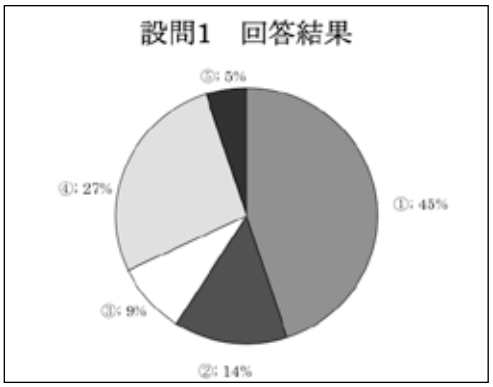
まず、企業内の内部監査を実施する実体に関して、アンケートでは以下のような設問があり、その結果を考察する。

[設問1]

その企業内で内部監査を実施しているのは、どのような組織及び形態ですか？

①定常的な内部監査部門が実施（専任・専

門の内部監査人）
②定常的な内部監査部門主導で他部門要員を活用して実施（兼任・素人の内部監査人）
③定常的な情報セキュリティ推進事務局が実施（推進役と内部監査人を兼任）
④定常的な推進事務局主導で他部門要員を活用して実施（兼任・素人の内部監査人）
⑤その他（具体的に書いてください）

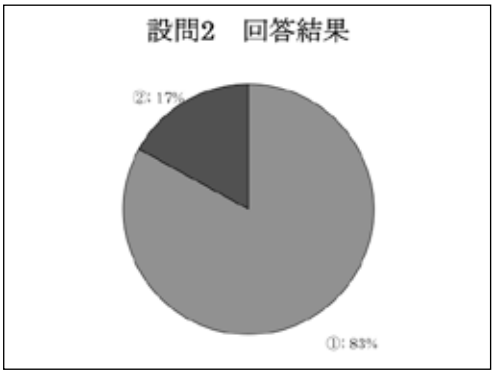


[考察 1]

①“専門の監査部門が実施（上記設問①＋③)”（54％)、“他部署の従業員を活用して実施（上記設問②＋④＋⑤)”（46％）で、専任監査人[7]と兼任監査人[8]が半々の結果となった。監査部門及び監査人の属性・定義は、監査に求められるレベル・内容、組織の規模、業態、対象業務の内容などにより異なると思えるが、兼任監査人の割合が大きいことは確認できた。また専門監査部門が 54％ということは、本アンケートの回答者は比較的中規模以上の企業組織を想定していることがわかる。

[設問 2]

その企業内の「内部監査のレベル」に問題があると思ったことはありますか？
①ある（それは、どのような問題ですか？）
②ない



[考察 2]

①83% の高い割合で内部監査のレベルに課題があるという実態が現れた。
②具体的には、“規程類に書かれている内容通りに運用できているかの監査であり改善のための内部監査ではない”、“監査報告書の内容が指摘事項の単なる羅列だけで経営者へのレポートとしてはきわめて貧弱”など監査の深堀が足りないという意見、“適合／不適合の判断基準があいまいなまま実施しているため監査人により判断のばらつきがある”、“評価結果が属人的になっている”など監査が形骸化／ばらつきがあるという意見、“内部監査人が情報システム及びセキュリティの知識に乏しい”という力量不足の意見などがあった。

以上のように企業内で実施されている内部監査については、専任監査人、兼任監査人が半々の割合であること、実施された内部監査の品質は企業の経営に貢献する内部監査のレベルには未だ達していないと認識されている。

1-2 内部監査に内在する課題

以上の設問 2 のアンケート記述回答の内容を整理すると、企業で行われている内部監査の品質に関する課題は以下のようにまとめられる。

①内部要員の活用による限界の存在

毎年、毎年、同じ人が決まった時期に訪れては、前回と同じことを聞いて帰っていく。監査人と被監査部門とは顔なじみであり、日常的に仕事のやり取りをしている人である。チェックすることも確認することも毎回同じではマンネリ、馴れ合いといわれてもしかたない。監査というものは客観的、公平、公正に行われなければならないが、内部監査は、大きく見れば同じ組織の内部の人間が行うものである。そこには客観性、公平性、公正性、信頼性と言う面では自ずと限界が存在する。

②兼任監査人の限界の存在

企業の資源の制約から内部監査は兼任監査人によって行われる場合がある。本来は別の本業を持っている従業員を監査期間だけ監査人として出稼ぎをしてもらう形態である。監査の素人である同僚を臨時の内部監査人に即席に仕立て上げ、相互監査をするというスタイルでは、その内部監査人に監査人としての多大な研鑽を求めることも憚られる。

その結果、内部監査人は全般的に教育・訓練不足となり、専門スキルに欠ける部分があり正しく妥当な指摘がしにくい。あるいは内部監査人の発言内容・指摘内容が恣意的であり、全体に一貫していない点が見受けられる。また内部監査人の均質性がなく、人による監査品質のバラツキが大きい。監査結果はいわゆる属人的であり、人によって監査対象事項や指摘内容やアドバイスが大きく異なる。

また、あまり監査経験もないし、情報セキュリティの専門知識もない同僚、仲間である内部監査人の言うことが本当に信頼できるのかと言う不信感が被監査部門にある。内部監査人の指摘に対して素直に受け入れられないところが出てくる。

③内部監査品質に対する認識不足

組織自体が内部監査にどこまでの品質を求めるのかが明確でない。ISMS や P マークで内部監査の実施を求められているから実施している。内部監査を実施したという形式的実績が必要と言う中での内部監査である。いつの間にか監査をやること自体が目的化し、形式化し、指摘内容も深堀の足りない表面的なものになっていく。重箱の隅をつつくような指摘ばかりに終始してしまい、被監査部門の業務改善に結びつく指摘や真に経営に役立つ所見も少ない。

2. 企業内内部監査の目的と効果

2.1　内部監査の目的と効果

「調査報告書 ISO9001・ISO14001 に対する適合組織の取組み状況」[9] によると組織が内部監査を行う目的は、「マネジメントシステムのレベルアップを図るため 70.9%」、「規格に要求されているため（第三者審査の準備のため）58.3%」の好対照な二つの目的が上位を占めた。認証の取組みの枠を外して考えると、内部監査の本質的な目的は、情報セキュリティ・マネジメントシステムのレベルアップのため、すなわち経営面からの情報セキュリティの有効性を判断すること、被監査部門の情報セキュリティ上の重要課題を改善すること、さらには、従業員に対して情報セキュリティ事故が発生しないような抑止効果を持たせ意識づけをすること、のためであろう。

一方、実際の内部監査の効果として特筆すべきことの一つは、内部監査を担当した内部監査人自身の啓発である。実際に監査を実施するといろいろなところに気づきがある。人の振り見て我が振り直せともいうが、監査の実務を担当した内部監査人自身が最も触発意識づけされているのではなかろうか。その理屈を押し通すと、できるだけ多くの従業員が内部監査人の役割を担って内部監査を実施することが求められる。

二つ目は、被監査部門の責任者の動機づけである。実際に監査を受けるということは少しばかりでも準備をし、それなりの意識と配

慮をする。それが組織全体の意識づけにつながっていく。

三つ目は、内部監査を主導する側（監査責任者や事務局などの監査実施主体者）の自主性の高揚である。内部監査を主導する側も、それなりの準備をし、情報セキュリティ管理の一端を担っている自負と責任を持たせることで、情報セキュリティの大きな推進力を得ることになる。

2.2 アンケート結果

[設問 11]

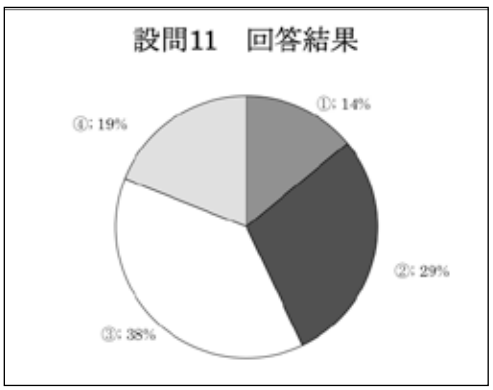
企業の内部監査に求めるレベルについて、あなた自身のお考えはどれですか？

①組織的活動として内部監査が実施 (PDCA) できていれば、それでいいのではないか

②内部監査プロセスについての課題を改善し続ける何らかの取組みが欲しい

③「内部監査のレベル維持・向上」についての明確な仕組み・施策が必要

④その他（具体的に書いてください）



[考察 11]

内部監査のレベル維持・向上のために何らかの施策が必要（上記設問②＋③）（67％）という結果であり、内部監査、及び監査人にかなり高いレベルを要求しているように見え、さらなる対策が必要と感じている。

[設問 14]

「内部監査のレベル維持・向上」について、その他のご意見があれば何なりとご記入ください。

[考察 14]

①内部監査のレベルアップについて回答の代表的なものをあげると次のようなものであった。“トップの意識次第”、“監査の実施経験から得られる”、“内部監査人の力量に負わない手法を構築すべき”、“外部の力を借りること”。

② “内部監査人の力量に負わない手法を構築すべき”については、兼任監査人による内部監査はルール通りにやっているかを見るレベルで十分、逆にいえば兼任監査人でもできる内部監査プロセスにしなければならないということだと受け止められる。多くの組織では人もお金も十二分に割くわけに行かない状況で、内部監査の実効性を上げないといけない。したがって内部監査人を育成することも重要ではあるが、兼任監査人でもできる内容にして、あとは監査部門や事務局で内部監査の精度と品質をあげることである。

3. 内部監査に求められる品質とは何か

内部監査の品質そのものを規定している文書はほとんど見当たらない。ISO9001[10]によれば、“品質とは要求されたことを達成した程度”とあるので、内部監査の品質も同様に考え、本稿では内部監査の品質を、“経営者の要求に応えた程度”と定義する。何故なら、内部監査は経営者から要求・指示されるものであるからである。

経営者が内部監査に求めているものは、本質的には現状の情報セキュリティ推進の有効性と適切性の評価であろう。例えて言えば、ISMS を導入している組織であれば、ISMS そのものの有効性とその運用の適切性の確証を内部監査に求めている。内部監査の品質とは次のように言い表せられる。

ア）経営への貢献度合い

経営者に対して情報セキュリティ推進の有効性と適切性を的確に報告・提言すること。

イ）情報セキュリティ管理の有効性の判断度合い

企業内で運用されている情報セキュリティ管理の有効性を正しく評価すること。

ウ）助言・指導内容の適切性、妥当性と信頼性

内部監査で指摘・助言した内容が適切で妥当であり信頼の置ける内容であること。

エ）内部監査プロセスの効率性と効果性

すべての内部監査プロセスが効率的、効果的に運用実施されていること。

以上のような観点で内部監査の品質を評価することが求められる。本来であれば、上記の項目ごとに品質レベルを定義すべきであるが、本稿では簡便のために上記アからエまでをまとめた総括的な品質レベルとして次のような指標を提言する。

アンケート結果にある内部監査に関する課題（1-2. 内部監査に内在する課題）の解決に対して要求される監査人のスキルレベルの難度を大きく、管理策運用面、職場課題面、経営課題面という切り口から設定する。それらを運用における基準への適合性評価、運用面への助言提示、職場重要課題への助言提示、基準自体の適切性の評価、経営課題としての評価という以下の５段階の序列に整理した。

レベル１：情報セキュリティ・ルールの職場運用の不備を正しく指摘できる

レベル２：職場運用の不備に対して最良の対策を助言できる

レベル３：職場の情報セキュリティに関する重要課題を指摘し、的確に指導、助言できる

レベル４：情報セキュリティ・ルールの適切性を的確に評価できる

レベル５:経営者に対して情報セキュリティ推進の有効性と適切性を的確に報告できる

上位レベルはそれぞれ下位レベルの内容を包含し、レベル５が最上位である。

①レベル１

（情報セキュリティ・ルールの職場運用の不備を正しく指摘できる）

内部監査（内部監査人）に求められる最低限の要求事項は、職場における情報セキュリティ運用状況の評価ということであろう。企業内の運用ルールに対して、その通りに運用されているかどうかを判定する。その際に内部監査人には三つのことが求められる。一つは自社内の情報セキュリティ運用ルールを知っていること、二つ目は情報セキュリティの内部監査人としての基本スキルを持っていること、三つ目は職場の業務概要を知っていることである。

ここで、情報セキュリティの内部監査人としての基本スキルとは、“情報セキュリティ”に関するスキルと“監査”に関するスキル[11]である。内部監査人は、これらのスキルに基づいて職場の運用状況を確認し、ルール通りに実施していない場面・事実を発見し、正しく指摘する。これが内部監査に求められる基本レベルである。

②レベル２

（職場運用の不備に対して最良の対策を助言できる）

内部監査（内部監査人）に求められるのは、運用の状況の不備を発見することだけではない。企業内の内部監査人が行う監査であるから、運用の不備の状況に対して的確な対策案などの助言・アドバイスが欲しい。本来の内部監査の目的はそこにある。不備を指摘するだけではなく、その不備を改善するためにはどうすればいいかを助言することが重要な役割であろう。そのためには内部監査人にはレベル１で記載したスキル以上の部分が必要になる。それは、自らの情報セキュリティ管理

の実体験であり、監査人としての多様な監査経験である。そういった多様な実体験があるからこそ、監査対象組織に対して的確で説得力ある対策アドバイスができる。

③レベル 3

（職場の情報セキュリティに関する重要課題を指摘し、的確に指導、助言できる）

情報セキュリティ管理策の一つ一つの不備の発見をするだけにとどまらず、監査対象職場の本質的な課題を指摘することが求められる。管理策一つ一つに対する運用状況の不備を発見・指摘しても、それでその職場の本質的な改善に結び付くかどうかわからない。もぐら叩きに終始しても仕方がない。いろいろな不備が発見された結果、その職場にはどういった本質的な課題があるのかを見出すことが重要である。いわゆるマネジメントシステムとしてのプロセスの課題と対策を指摘することが求められている。

④レベル 4

（情報セキュリティ・ルールの適切性を的確に評価できる）

レベル 3 までは社内ルールありきであったが、レベル 4 になるとその社内ルール自体の適切性を評価することが求められる。企業内で策定され、運用されている情報セキュリティ・ルールそのものが本当に適切なのか、CIA[12] の実現に効果があるのか、現場業務の実態に合っているのか、などを評価することである。よく情報セキュリティとは利便性とトレードオフの関係にあると言われる。全てがそうではないが、ある面、そのような相反性を有することもあり、あるいは、もっと行き過ぎると組織にとって“百害あって一利なし”と言われかねないルールも無きにしもあらずである。そこまで行かなくとも組織にとって役に立たないルールを運用することほど無駄なことはない。内部監査では、こういった情報セキュリティ管理策自体の有効性についても評価する必要がある。ISO27001 にも管理策の有効性測定という要求事項が存在する通り、時間と経験の経過の中で情報セキュリティ・ルールを適宜見直すことは重要であるし、内部監査はその任の一端を担う。

⑤レベル 5

（経営者に対して情報セキュリティ推進の有効性と適切性を的確に報告できる）

レベル 5 の内容は、内部監査の依頼者である経営者が最も必要としていることである。本質的にはレベル 5 が内部監査への究極的な要求事項というべきものであり、このアウトプットこそが内部監査の品質というべきものであろう。

個々の職場の中の情報セキュリティ運用状況を評価し、情報セキュリティ・ルールを評価し、その結果、企業内の情報セキュリティ管理についての課題と対策を経営者に報告・提言することが求められる。その際、個々の情報セキュリティ管理策の実装状況はさておき、企業内の情報セキュリティ管理の有効性について的確な評価をすることが肝要である。情報セキュリティに関する経営者の方針や目的への適合度合、管理策の運用状況、事故の発生状況、顧客・取引先などのステークホルダーからの要求や提案などを総合勘案して、現在の情報セキュリティ管理が自社にとって有用なのか、事業や環境の実態と合っているのか、問題があるとすればどういう手を打てばいいのか、そういった内容を経営者に的確に報告・提言することこそ、内部監査に要求されていることであり、これこそが内部監査の本来の品質である。

4. 内部監査品質確保のための施策

4.1 アンケート結果

本章では内部監査の品質を確保するための施策について論じる。まずは、アンケート結果から示す。

[設問 3]

「内部監査のレベル維持・向上」のためにその企業ではどのような活動をしていますか？（上記設問 2. で「①ある」と答えた方のみ答えてください）

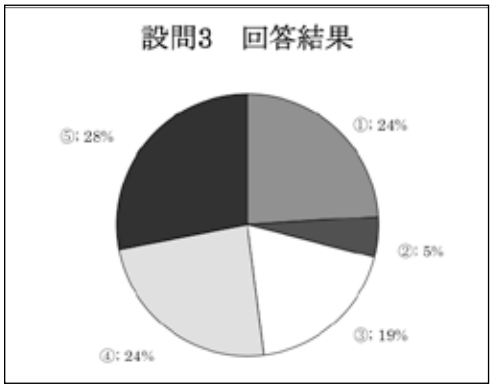
①内部監査主導組織内で定期的に”内部監査の実施状況を確認”している

②内部監査主導組織とは別の部門が定期的に”内部監査の実施状況を確認”している

③その企業から別の企業に定期的に”内部監査の実施状況の確認”を依頼している

④その他（具体的に書いてください）

⑤特に何もしていない



[考察 3]

①回答はばらついた。内部監査のレベル問題に対して、その対応は様々に考えられるということであろうか（特に何もしていないというケースもかなりある）。

②監査品質を確保するために内部自己評価や外部評価という手法をとっているところもあるが、時間とお金がかかることでもあり、その必要性は認識されているものの、まだ一般的に実施されていないと見るべきであろう。監査品質を確保するためには、監査人の教育という手法が必要という回答が既に本設問にて出てきているのは、監査品質の確保のためには監査人の質の確保が大きなウェイトを占めると考える有識者が多いということであろう。

[設問 4]

”内部監査の実施状況の確認”ではどのようなことを実施していますか？

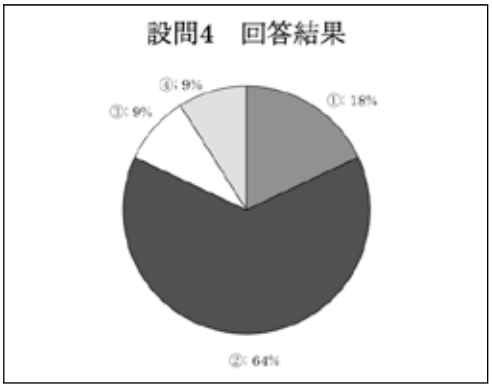
（上記設問 3. で「①～③」を選択された方が答えてください）

①監査基準通りに内部監査プロセスが実施されていることを確認

②内部監査プロセスからアウトプットされた証跡（計画書、報告書など）の内容を評価

③既に実施された内部監査と同じ監査対象を別途に監査して、監査結果を照合する

④その他（具体的に書いてください）



[考察 4]

①上記設問①の回答が少なく、上記設問②が 64％でかなり多いのは意外である。通常の確認手順としては、内部監査プロセスが適切に実施されていること、その次に内部監査プロセスからのアウトプットの評価であろう。

②内部監査の実施状況の確認をすることで内部監査のレベルを維持するケースでは、内部監査プロセスからアウトプットされた証跡を確認する手法が最もポピュラーである。監査計画書や監査報告書の内容を精査すれば、自ずとその内部監査のレベルが見えてくる。但し、内部監査のレベルを把握することはできても、そ

れに対しての対策をどうすればいいかは別の問題である。

[設問 5]

「内部監査のレベル維持・向上」のために、上記設問 3. で記載してある活動以外に考えられる対策を記入してください。(他で見聞きした、或いはご自分の考えとして)

[考察 5]

①アンケートの記述回答を整理すると「内部監査のレベル維持・向上」の施策として、“組織体のポリシーの徹底”、“監査人の教育実施”、“外部からの支援”、“内部監査プロセス自体の工夫”という四つに分類できた。

②内部監査のレベルの向上のためにはお金も人も時間もかなりの資源が必要となる。組織が本当に内部監査を必要としているのかどうかというところに本質があり、その必要性に見合った対策が採用されるのであろう。結局、経営者が内部監査に何を求めているかによるところが大きい。

4.2 品質管理と品質マネジメント

品質を管理するには、品質管理 (Quality Control) と品質マネジメント (Quality Management) という考え方がある。品質管理とは製品・サービスの不具合の発生の予防、品質検査の実施、品質不良に対する適切な処置および再発防止など一連の活動であり目標として設定された品質を達成するための実施技法をいう。

一方、品質マネジメントとは、製品・サービスに関連するプロセスの品質を確保することで要求された品質を達成しようとする総合的・組織的な品質管理のマネジメント手法のことである。ISO9001 やプロジェクトマネジメントの世界では、製品・サービスの品質を確保するためにこのようなプロセス品質を確保するという考え方を導入している。

内部監査の品質確保についても同様に二面的な考え方を導入したい。一つは、品質管理の考え方である。内部監査品質の不具合の発生を予防し、品質検査を実施し、品質不良に対する適切な処置および再発防止をする一連の活動を行う必要がある。

その一方、内部監査プロセスの品質を確保するという面で、計画、実行、報告の各プロセスに対する品質確保の取り組みを行う必要がある。

4.3 内部監査品質管理の取り組み

内部監査の品質を保つためには、個々の内部監査ごとの測定・評価・是正が欠かせない。そういう面ではアンケート結果にもあったが、外部監査人や熟達した内部監査人を常に同席させて一緒に監査させるということも手である。あるいは、内部監査の推進事務局が常に同席して実施状況を確認し、監査終了後は関係者を集めて内部監査での反省点や工夫点などを議論し情報共有する取り組みなども品質確保につながる。監査報告書を確認チェックする手法も同様である(考察 4 ②内部監査プロセスからアウトプットされた証跡(計画書、報告書など)の内容を評価)。この取り組みの課題は、測定・評価・是正のための指導ができる専門家が少ないこと、あるいは、そのためのコストが高くつくということである。

4.4 内部監査プロセスの品質マネジメントの取り組み

「内部監査品質評価ガイド」[1] によると監査品質確保のために 3 段階の内部監査プロセスの監視を行うことを提起している(「図 1. 内部監査プロセスの品質評価の枠組み」参照)。一つは、内部監査部門の業務管理の内部評価として継続的に品質評価のモニタリングを実施し、改善を行うことである。組織の監査業務の内部監査基準への適合度を評価する。図 1 の「①内部評価、継続的モニタリン

グ」に該当する。定常的に存在する内部監査実体があればこの品質マネジメント手法も考えられるが、定常的監査組織を持たず、兼任監査人のみで内部監査を実施するケースが多い場合は、結局、前記の品質管理と同様の取り組みと同じになる。

二つ目は、定期的に内部監査部門の内部監査基準への適合度を判定評価するというものである。内部監査の計画、実施、報告プロセスが監査基準通りに適切に実施されていることを定期的に評価するということである。図1の「②内部評価、定期的レビュー」に該当する。ISO27001の内部監査に対する要求事項もそのような内容を含んでいると思われる。ただし、この手法での課題は、評価者は誰かということである。「内部監査品質評価ガイド」では内部監査の自部門内で選定する場合と、他部門から選定する場合を挙げているが評価者適格性の要件が重要な意味を持つことに変わりない。

三つ目は、組織から独立した外部の評価者により最低でも5年ごとに評価を実施することを挙げている。その中でも外部者が内部監査の内容をフルに評価する直接評価の場合と、企業内部で自己評価した証跡を外部の評価者が検証する間接評価の方法がある。図1の「③外部評価のフル外部評価と自己評価と独立した検証」に該当する。いずれの手法も評価者適格性の要件がポイントとなることに変わりはない。なお、フル外部評価とは内部監査の定義、基準、倫理要綱への適合性評価、有効性と効率性の評価、ベストプラクティスの適用を含む改善の機会を明らかにすることから構成されるフルメニューの品質評価を言う。

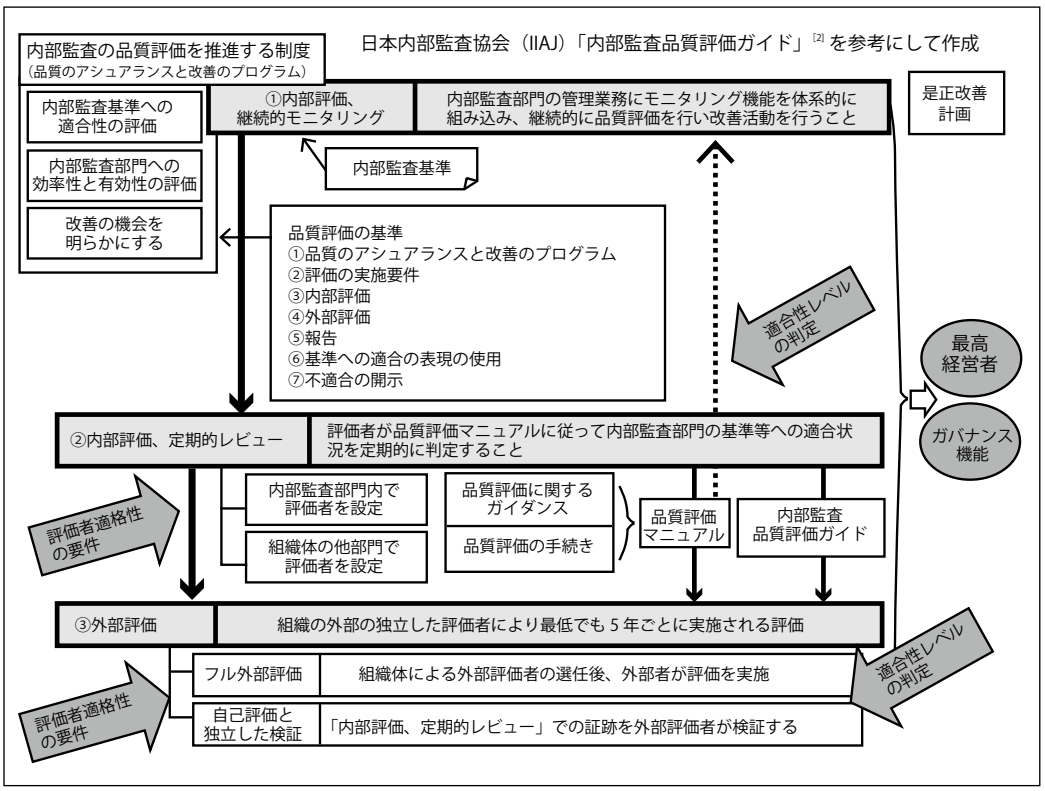


図1　内部監査プロセスの品質評価の枠組み

ここで挙げた手法は、いずれも一つのプロセスの実施状況とアウトプットの適切性を別のプロセスで評価するというものであり、評価した側のプロセスの適切性をどう評価するかという永遠の課題があるとともに、現実には、時間、コスト、評価者の問題が大きく存在する。

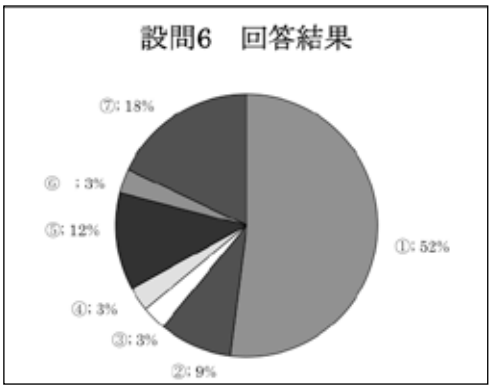
4.5 内部監査人の教育訓練に対する取り組み

内部監査品質の確保のための施策として内部監査人のスキル保証の取り組みがある。品質管理という面からは、内部監査人のスキルを確認することが考えられる。たとえば、スキル面について実際に試験をするとか、保有する専門資格で監査人に認定するなどである。

品質マネジメントの観点からは、内部監査人を教育訓練するプロセスの品質を確保するという手法が一般的に考えられる。一連の内部監査プロセスの評価と同じ枠組みである。これについてアンケート結果を見てみる。

[設問 6]

「内部監査のレベル維持・向上」の施策の一つとして、内部監査人の質の維持・向上が考えられます。企業がそのために実施しているものがあれば選択してください。
（複数選択可。内部監査人とは、設問 1 で選択した監査要員を想定してください）



①内部監査人の教育・訓練の実施
②内部監査人の資格認定制度の導入
③内部監査人のランク付け
④内部監査人の社内人事制度とのリンク付け（昇格、給与）
⑤内部監査人の社外資格取得の奨励（具体的にどういった資格ですか）
⑥内部監査人として専門家の新規採用
⑦その他（具体的に書いてください）

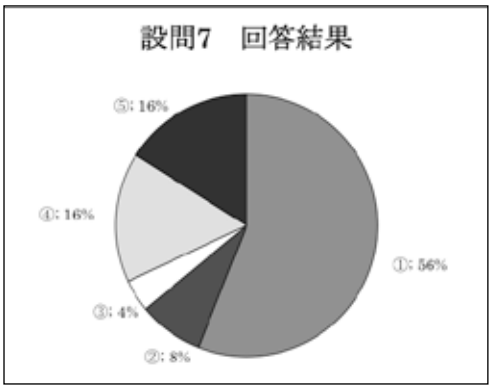
[考察 6]

①教育・訓練の実施が 52%
②内部監査人の質の維持・向上のためには、教育・訓練という項目が第一に挙がる。それももちろん重要であり、直感的にわかりやすい。それとともに、組織の経営方針・ポリシー、或いは風土・カルチャーの中にある内部監査を必要としている度合いというものが重要であるという意見も説得力がある。

[設問 7]

その企業における内部監査人の教育・訓練において、最も重要視しているのはどれですか？

①知識（監査の知識、情報セキュリティの知識、業務の知識など）



②技能（インタビュー技法・コミュニケーション技法、証拠の確認と確保の技法、ICT 関連の技能、不正検出や証跡チェックの技法など）
③監査文書作成スキル（計画書・チェックリスト・報告書の作成など）

④モラル・倫理、態度（倫理観、監査人としての心得）
⑤その他（具体的に書いてください）

[考察 7]

①知識 56％
②内部監査人の質の維持・向上のための教育・訓練では、知識の教育に重点があることがわかる。逆に言えば、内部監査人の教育・訓練としては知識教育しかできない現状が見えてくる。企業が求める内部監査人のレベルをどこに置くかがポイントであるが、それは企業ごとに異なるものであろう。内部監査人の育成についての課題が見える。
③とかく疎かになりがちである倫理・モラル面の教育、及び経営に対するアンテナ感という回答を合わせると 32％ある（上記設問④＋⑤）。

[設問 8]

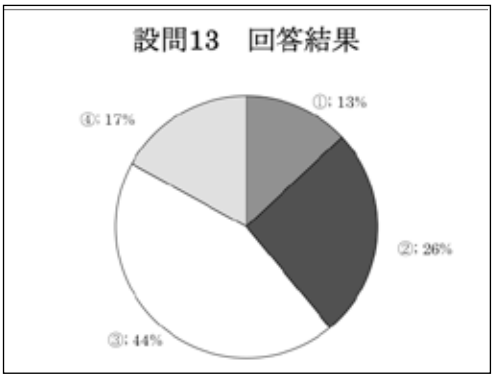
その企業での内部監査人の教育・訓練における現状の課題は何ですか？

[考察 8]

①教育・訓練における課題は、育成方針・指導教育体系、指導者、兼任、その他という四つに分類できた。
②内部監査人の育成については専任・兼任を問わず普遍的な方程式が世の中に存在しない。現状では“何をどのように教育・訓練すればよいのか”一般的で明確な指針が無い。監査関連知識に加えて、何を誰がどのように指導するのか、指導できるのか、など多くの課題が存在する。それを一企業の方針の問題に帰着させることもできないであろう。これらの課題は、兼任というしくみが何時まで持つのか、という将来的な課題まで示しているのではなかろうか。

[設問 13]

企業の内部監査人に対して求めるレベルについて、あなた自身のお考えはどれですか？（兼任・素人の監査人の場合）



①あまり細かな要求は必要ないのではないか
②内部監査人としての資格認定くらいは必要
③内部監査人の質の維持・向上のための明確な仕組み・施策が必要
④その他（具体的に書いてください）

[考察 13]

①兼任監査人に対しても明確なレベルアップのための施策が必要という意見が多い（上記設問④）（44％）。質の向上のためにどうしたらいいか、教育・訓練だけでもないし、経営者のポリシーだけでは組織的な取り組みとして弱い。兼任監査人に切磋琢磨を要求するのも辛い。兼任監査人へのレベルアップ要求度合いが強い割には、設問 6、設問 7 で明確な解決策が見いだせていない実態が見える。
②兼任監査人の位置づけというものは中途半端であり、そういった兼任監査人に任せる内部監査というものはそれなりのレベルにあればいいというものもあった。
③兼任監査人に任せる内部監査、及びそのマネジメントシステム自体が将来にわたって安定したしくみとしては定着しないのではないかとも考えられる。
④ちなみに、設問 12（本稿では割愛）では

専任監査人のレベルへの同様の質問があるが、本問と同様にもっとレベルアップが必要という回答が多い。専任監査人だからと言って高いレベルにあるとは限らず、組織ノウハウの蓄積・継承などの課題も多い。

アンケート結果からも伺えるが、現在の内部監査人の教育訓練プロセスが十分であるとは思えない。“内部監査人に求めるスキルが明確でない”、“指導者がいない”、“監査人の力量を評価できる人がいない”などがアンケート結果にも表れている。また、特に兼任監査人に限って言えば、本業がありながら、どこまでの研鑽を求めるのかという課題もある。

ISO19011「7. 監査員の力量及び評価」では内部監査人のスキル及び評価の枠組みを提供している。これは監査品質確保のための取組みの一つであるが、監査人の専任／兼任の切り口があるわけではない。現実はその点が大きな分水嶺であるので、内部監査の品質を確保するための兼任内部監査人のスキルをどう定義するのか、教育訓練カリキュラム・教育内容及びスキル評価の枠組みをどうするのか、という課題は残る。

4.6 専任監査部門への集約・強化の提言

現状の多くの企業内内部監査について、その品質には様々な問題があることがわかった。その対策として、品質管理的な取り組み、品質マネジメント的な取り組みを挙げてきた。それ以外にアンケート回答にあったものは次のようなものである。

- 経営者が内部監査を重要視する姿勢・方針が大切である
- 相互監査をすることで知見が得られる
- 監査役との連携による情報交換、意識高揚、知見の取得

いずれも示唆に富む内容であり、もっと掘り下げれば今後の内部監査活動においては参考すべきことが多い。このように内部監査のレベルを維持向上するためには、理論上は様々な手法が考えられるが、本稿では内部監査というものを兼任監査人から専任の監査部門へ段階的に集約・強化すべきことの二つを提言する。

一つは、内部監査は兼任内部監査人でもできる内容・レベルにするということである。あらかじめ決まった質問事項を準備し、確認証跡を指定し、順番に機械的にチェックできるものとする。チェックしたポイントを積算すれば自動的に評価結果も出てくる。こうすれば人による違いも出にくいし客観的な評価ができる。このケースは、内部監査の目的を達成するというよりも内部監査の効果（監査人自身の啓発）に重点があると考えたい。

したがって内部監査のレベルを維持向上するためには、兼任監査人を前提として、ルール通りに実施していることを確認するレベル（監査品質レベル 1）の内部監査と、それをサイドから確認評価し監査品質を確保する監査部門（事務局）によるプロセス・マネジメントが重要になってくる。

このことは［考察２］で挙げられた問題点および「1.2 内部監査に内在する課題」に対して、それらの現状の問題点を受け止めたうえで、その限界内での解決策として示すものである。

二つ目には、専任の監査部門の強化である。本来の内部監査に求められている部分については、専門の監査部門による内部監査の深堀をする。兼任監査人の中にも力量・スキル面で有用な人材がいる場合は、専門部署への補強を考えるべきである。専門の監査部門を仕組みや人材面からより強化し、監査品質の向上と専門人材の育成を徹底すべきである。企業の規模にもよるが少数精鋭の監査人で監査品質レベル 5 を達成できる内部監査を目指す。必要により適宜外部の専門家による外部監査なり認証審査で監査品質を補完するとい

うプロセス・マネジメントが重要である。

このことは［考察２］で挙げられた問題点および「1.2 内部監査に内在する課題」に対して、それらの現状の問題点を解消するための解決策として示すものである。

このように従業員への啓発を狙った兼任監査人による内部監査、及び専門的に徹底した深堀をする専任監査人による内部監査の縦横の網の目の二重三重の重層的プロセスのシナジー効果により企業の情報セキュリティは有効に保たれる。中長期的には、専門家の精鋭を揃えた専任監査部隊による内部監査に収斂していくことが必要である。

おわりに

企業における内部監査の経営への貢献度合いを定量的に示すことは難しい。情報セキュリティ事故の件数が減らないからと言って内部監査一人の責に帰すこともできない。内部監査の本質は、指摘件数の問題ではなく、指摘内容の問題であり、所謂、量よりも質の問題だからである。

情報セキュリティが社会的に注目を浴び、企業への浸透を始めてから 10 年を経過した。内部監査は企業の情報セキュリティ推進にとって、無くてはならないプロセスであり、重要かつ企業統治の根幹をなす仕組みだからである。情報セキュリティを下支えするという大きな役割を持つがゆえに、企業内内部監査のあり方はそろそろ次のステップに進む段階にきたのではなかろうか。

＜参考資料＞

[1] 日本内部監査協会「内部監査品質評価ガイド」2010.3.31

[2] 日本内部監査協会（訳）「内部監査の品質評価マニュアル」－有効性と価値の向上のために－　平成 15 年 4 月 15 日　同文館出版

[3] 財団法人日本規格協会「ISO 19011:2011 -Guidelines for auditing management systems-」（マネジメントシステム監査のための指針）2011.11.11

[4] 財団法人日本規格協会「ISO/IEC27001 Information technology-Security techniques-Information security management systems-Requirements」2005.11

[5] 財団法人日本規格協会「JIS Q15001:2006 個人情報保護マネジメントシステム要求事項」2006.5.20

＜注＞

1 Information Security Management System

2 マネジメントシステムにおける監査のガイドライン

3 アンケート依頼数 51 人､有効回答者 22 人、設問は全 14 問、本稿ではその一部を紹介している

4 個人情報保護マネジメントシステム - 要求事項

5 Personal information protection Management Systems：個人情報保護マネジメントシステム

6 ISMS 適合性評価制度の要求事項

7 内部監査を本来の業務ミッションとしている従業員

8 内部監査以外の本来の業務ミッションを他に持つ従業員

9 財団法人　日本適合性認定協会 (JAB)2010 年 2 月

10 品質マネジメントシステム（Quality Management System）要求事項

11「情報セキュリティに関わる人材の体系化とキャリアパスの提言」情報セキュリティ専門監査人部会ＷＧ（システム監査 第 21 巻第 2 号 2008.3）に詳細な内容を発表

12 Ｃ : Confidentiality（機密性） Ｉ : Integrity（完全性） Ａ : Availability（可用性）