情報システム監査の保証型監査は如何にあるべきか
What should be the audit assurance in the information systems audit.

大井　正浩
Masahiro Ohi
†中央大学　研究開発機構
† Research and Development Initiative, Chuo Univ.

要旨
情報セキュリティ監査基準において「保証型監査」が推奨された。一つの前進ではあるが、内容的には公認会計士監査の形式に則ったガイドラインが示されただけであり、十分に検討されたものとは言い難く、有効な監査モデルの構築は今後の課題である。監査基準と併せて策定された報告基準ガイドラインにおける保証型監査の問題点を明らかにし、更なる前進の第一歩としたい。

1. はじめに

2003.4、情報セキュリティ管理基準、情報セキュリティ監査基準[１]策定によって、「保証型監査」が提唱された。その後システム監査基準[２]も追随したのであるが、その意義は認められ、進歩とは言えるが、具体的内容は必ずしも細部納得性があるものとは言い難く、各所で議論は行われているが、勝れて今後どのような監査モデルを構築できるかにかかっている。既往の説明では、従来の助言、勧告を旨としたシステム監査よりも、保証型監査が上位にあるかのように認識し、公認会計士決算監査と同様な内容を考えているように見える。これでは、運用を誤ると、従来から経営のための総合的な情報システムの監査を目指してきたシステム監査の内容を、形式的な単なる認証業務に追い込むような方向が懸念される。基本的な課題を考えて見たい。そこで、「情報セキュリティ監査基準・報告基準ガイドライン」[３]の内容に検討を加え、システム監査の本質から見た問題点を明らかにしたい。

なお、システム監査と情報セキュリティ監査をそれぞれ別個独立のものと捕らえ、それらの一部が重複するに過ぎないと定義する動きがあるが、筆者は、システム監査が総合的な情報システム全体を対象とした監査を目指すものなので、情報セキュリティ監査はシステム監査の重要な一部を構成するものと捕らえているのでその前提で議論を進める。

2. 監査と保証業務

監査業界には、従来から保証業務についての関心があった。1997 年には米国公認会計士協会（AICPA）の「保証業務特別委員会」によって、「意思決定者のために、情報の質、あるいは情報の内容を向上させる、独立の職業専門家の業務」のように情報業務に係る保証の定義がなされている。日本では 1998 年に、日本公認会計士協会（JICPA）に「次世代会計士保証業務研究会」が設置された。公的基準としては、企業会計審議会、「財務情報等に係る保証業務の概念的枠組みに関する意見書」、2004.11.29[４]が公表されている。内容的には、公認会計士監査、決算監査を意識したもので、保証の主題として、「内部統制や IT システム」も例示掲載されてはいるが、情報システムの本質を踏まえた十分な吟味が果たされている訳ではない。

3. 情報セキュリティ監査基準などに示された「保証型監査」

情報セキュリティ監査基準はその前文で次のように述べている。「情報セキュリティ監査は、独立かつ専門的な立場から、組織体の情報セキュリティの状況を検証又は評価して、情報セキュリティの適切性を保証し、情報セキュリティの改善に役立つ的確な助言を与えるものだからである。」

更に、別途行われた説明会資料では、「保証型監査」を最終的姿と規定して、市場の創設を目的としている。市場とは、資格を付与された外部監査人が監査報酬を求めて実施する監査、即ち公認会計士の決算監査と同様のものと想定しているようである。

これを受けて、2004 年 7、10 月改訂の「システム監査基準」も保証型監査を受入れた。

4. 基準に示された「保証型監査」の方向性

システム監査が目指すべき「保証型監査」は、情報システムにおいて、社会と経営が信頼関係を持って発展するための重要な位置付けになければならない。2003 年、情報セキュリティ監査基準の策定に続いて公表された「報告基準ガイドライン」を見ると、新たな保証業務のモデルを創るための根本的な検討を加えた内容というよりは、当面、公認会計士監査の決算保証に準じた雛形を提供することに主眼が置かれているように見える。このことは、保証型報告書雛形と公認会計士の監査報告書の文言を比べてみると明らかになる（表参照)。「保証型監査にして監査報酬を得たい」という願望によって公認会計士の決算監査と同様に考えたのであろう。決算監査とは、財務会計、管理会計などと呼ばれる企業の幅広い会計業務の中から、特定期間の決算に的を絞ったもので、経営監査の中の極めて狭い分野でしかない。

[表]保証報告書雛形と会計監査人の監査報告書の比較

項目	保証報告書の雛型・肯定意見	会計監査人の監査報告書
表題	情報セキュリティ監査報告書	独立監査人の監査報告書
期間と対象	200ｘ年ｘ月ｘ日から 200ｘ年ｘ月ｘ日までの期間に係る XXX を対象として、情報セキュリティの状況について監査を実施した。	ｘ株式会社の平成ｘ年ｘ月ｘ日から平成ｘ年ｘ月ｘ日までの第ｘ回営業年度の連結計算書類、すなわち、連結貸借対照表及び連結損益計算者について監査を行った。
責任	われわれの責任は、監査手続を実施した結果に基づいて意見を表明することにある。	この連結計算書類の作成責任は経営者にあり、当監査法人の責任は独立の立場から連結計算書類に対する意見を表明することにある。
準拠基準	われわれの監査は、「情報セキュリティ監査基準」に準拠して行われた。採用した監査手続は、われわれが必要と認めたものを適用しており、	当監査法人は、我が国において一般に公正妥当と認められる監査の基準に準拠して監査を行った。
意見表明根拠	監査の結果として意見表明のための合理的な根拠を得たと確信している。	当監査法人は、監査の結果として意見表明のための合理的な基礎を得たと判断している。
期間及び対象と意見表明	われわれの意見によれば、200ｘ年ｘ月ｘ日から 200ｘ年ｘ月ｘ日までの期間に係る XXX を対象とした情報セキュリティ対策の実施状況は、「情報セキュリティ管理基準」に照らして適切であると認める。	監査の結果、当監査法人は、上記の連結計算書類が、法令及び定款に従いｘ株式会社及びその連結子法人等からなる企業集団の財産及び損益の状態を正しく示しているものと認める。

5. 情報セキュリティ監査基準の報告基準ガイドライン[３]

保証型監査の具体的な内容を示した重要な文献なので、その「保証」に関連する部分を中心にその特徴と思われる事項を整理、解説し、問題点を指摘する。

5.1. 対象期間

監査に当っては、対象として特定期間又は特定時点を定めることを原則としている（Ｖ－１－1.4 他、報告基準ガイドラインの章立表示、以下同じ)。

会計監査の場合は極めて明確である。過去の、特定の決算期間について確定した事象を保証すれば足りる、従って監査の期間特定・限定は当然のこととして受入れられる。

しかし、システム監査の場合はこのような前提はない。勿論実査の物理的限界からして、試査の範囲を期間で限定して監査することは一般的に行われているが、これはあくまでも全体的状況を類推評価するために十分な期間として位置付けられるものであって、決算監査における決算期間とは根本的に意味が異なる。システム監査において問題指摘について望まれる対象期間は、前回監査終了後から今回監査終了日までである。そして、適切に選定した試査対象期間の結果を踏まえて今後のあるべき姿に対して助言､改善勧告を行うことがシステム監査の目的である。

また、筆者の内部監査人としての経験からしても、経営にとって過去の期間限定は大きな意味を持たない。経営トップに対して、「過去の一定期間を対象として監査した結果良好であった」と報告しても、必ず飛んでくる質問は「現在不都合は起きていないのだな」、「今後も安心して居てよいのだな」という確認であって、これに応えようとしない内部監査人は全く評価されない。即ち、システム監査を保証型として完成するために対象期間を決算期間な

どと同様に限定するとすれば本末転倒であると思われる。

5.2. 監査対象

情報セキュリティ監査の保証目的を十分に達成するためには、「情報セキュリティ管理基準」のすべての項目について監査対象とすることが望ましいとしながらも、一部の項目に限定することを認めている。その例示として、「外部委託」、「運用段階」、「機密性」、「Web システム」などをあげている（Ⅴ－１－1.5 他）。これは外部の利害関係者の求める保証内容として考えると微妙なものを含んでいる。例えば「運用段階」の保証は、相前後して戦略、企画、開発、保守などの監査が行われることを前提とすれば、過渡的、部分的保証としての意味があることは分かる。しかし、これが不明であれば、保証効果は疑問である。要は全体感として、監査に注力している企業であり、今回も一部が保証されたという市場理解が成り立つことが重要であるという意義付けが可能であろうか。企業が抱えている情報システムに係る多くの課題を整理すれば、ある程度独立的に評価し保証する対象を選定することは可能なように思われる。具体的な監査モデルの構築が待たれる所以である。

5.3. 責任の範囲

保証の責任については極めて慎重な配慮がなされている。雛形では、「保証する」又は「保証を付与する」などの文言は使われていない。

①「保証意見は情報セキュリティ対策に対して一定の保証を付与するものであるため、情報セキュリティ監査人が負うかもしれない責任に充分に留意し、あいまいな表現を避け、助言意見と混同されることがないようにしなければならない。」（Ⅳ－３－3.1）。

②先ず雛形で「われわれの責任は、監査手続を実施した結果に基づいて意見を表明することにある。」とし、解説において「情報セキュリティ対策に対して直接的かつ第一次的に責任を負うのはあくまでも被監査側であって、情報セキュリティ監査人は自らが実施した監査の方法と結論についてのみ責任を負うという責任区分の原則を徹底するために記載される。」としている（Ⅴ－１－1.7 の後半）。これは、公認会計士の決算に対する態度と全く同様である。

先ず文言として、「適切であると認める」、「正しく示しているものと認める」などは、保証の表現としては限りなく「あいまい」である。長い歴史と慣行に裏打ちされた会計監査用語としては定着しているのであろうが、新しい保証を求める企業・社会に対して十分な表現とは思われない。「保証する」又は「保証を付与する」などの明瞭な表現を使用すべきであろう。数々の限定条件の下で、監査人が「過度の責任を問われないように」との配慮によるものであれば、期待される保証効果どころか、責任逃れの表現としか受取られないであろう。

本来の内部監査としてのシステム監査において重要なことは、監査の対象、範囲の定め方（試査の範囲）、方法・技法の選定など及び結論について責任を負うということである。対象の選定を誤って他の分野で不都合が起これば、何故その分野に目が行かなかったのかと責任を問われ、範囲の決定を誤って後日他の範囲に問題があったことが発見されれば、これまた責任を問われる。方法・技法が拙く十分でなかったとすれば、能力不足を認めざるを得ない。「一般的に公正妥当」だと主張しても、組織は一般論で動いているわけではないと言われるだけである。現在の我社にとって適切かつ効果的であったかどうかが問われるのである。

5.4. 監査の基準

ここでは、「情報セキュリティ管理基準」を基本的判断尺度としている。勿論他の基準を参照することも想定してはいるが、公的基準による監査を前提としている。システム監査にとって、公的基準は最も尊重すべき基準であるが、企業の経営方針、監査対象・目的によって、多様な基準が参照される。公的な個別基準には、「情報システム安全対策基準」、「コンピュータウィルス対策基準」、「ソフトウェア管理ガイドライン」、「コンピュータ不正アクセス対策基準」などがある。業界基準として代表的なものは金融業における金融庁基準、金融情報システムセンターの諸基準がある。国際企業においては諸外国の基準も参照されることは当然である。そして何よりも大切なものは自社・個別企業の基準であり、前記の全ては自社基準を策定する材料であると言っても過言ではない。本来のシステム監査では、当該企業に取って必要かつ適切な基準に照らして監査するのであるが、ここでは企業中心という考え方はなく、保証のために公的基準前提の定型的監査を想定しているように思われる（Ⅱ－１－1.1 他、）。

5.5. 目的及び報告先

監査の目的及び報告先を、組織内に限定せず、外部利害関係者への開示を想定している（Ⅰ－１－1.2 他）。これは、従来のシステム監査が組織体の長に報告することを旨としていたことに対しては大きな変化であり、前進でもあると評価できる。しかし、公認会計士の決算監査では上場企業の株主に的が絞られていることに対して、システ

ム監査の対外的意義は企業の情報開示であり、先ずは経営者に対して保証し、必要に応じて外部に開示されるのが筋である。システム監査の結果が、保証されたのか、助言を受けたのかによって開示の意義、重要性そのものに変化、格差があると考える必要は無い。公認会計士監査の「無限定」、「限定意見」とは根本的に異なる。広範囲で奥行きが深く、時々刻々変化発展する情報システムにおいて、助言を受けることは必要なことであり、積極的なベストプラクティスに向けての助言であれば、その企業の信頼性が揺らぐ筈も無く、高度な目標追求が評価されることもあり得て、システム監査の社会的目標にも合致することは理解できよう。

5.6. 「確認書」の役割

監査人が意見を表明する「直接報告方式」の他に、被監査側が確認書（言明書）を提出する「言明方式」を認めている。「情報セキュリティに関わるリスクマネジメントが効果的に実施されるよう、リスクアセスメントに基づいて適切なコントロールを整備し運用している」旨の経営者又は情報システム管理責任者による確認書（言明書）を得て、当該確認書について情報セキュリティ監査人が意見を表明する方法である。この方式は、「通例、意見表明に関わる情報セキュリティ監査人の責任を明確にしやすい。」ものとして推奨されている（Ｖ－１－１.７前半)。公認会計士監査における統制環境、内部統制や報告書に対する代表者宣誓・確認の例に倣ったものと思われる。

監査の「保証を付与する」については、経営者の責任が大きいことが分かる。経営者は確認書提出に当っては、業務管理、内部統制の信頼性などに対して情報システム部門長と内部監査人の意見を最大の拠りどころとするであろう。外部監査人がこのような監査簡略化、責任軽減を求めれば、経営者は外部監査人の保証を単なる形式としか評価せず、内部監査などの地位を高める効果しかない。良心的な公認会計士諸兄には我慢がならないことであろうが、世の経営者の中には、公認会計士の監査証明を株主総会、証券取引委員会、監督当局のためとしかその意義を認めないと本音を漏らす人もいる。外部監査人のシステム監査をこのような評価に近づけることが無いように留意しなければならない。

6. おわりに

本論では、システム監査の本質から判断して、報告基準ガイドラインなどに示された保証型監査の問題点を明確にした。資料紙数、発表時間の制約から単なる主要な問題指摘に止まっていることをお詫び申上げる。本来の目的は、より詳細な分析と、新しい監査モデルの提示にあるが、別の機会に譲ることをお許し頂きたい。

本論における詳細検討は不十分であるが、現時点で保証型監査に必要な一般的な条件は次の通りと考えられる。

①監査人のための不自然な限定を行わず、企業の抱える問題点に正対して監査を行うこと
②保証する以上、監査の過程と結果に責任を持つこと
③そのために、会計監査ジャーゴンによらず、明瞭なビジネス用語を使用すること
④監査人のための基準に拘らず、当該企業に適切な基準に準拠すること
⑤情報システムおよびセキュリティにとって、基本的なコンポーネントを選定・抽出して保証対象とすること

何よりも心から願うことは、システム監査を矮小化して形式的な保証業務に追い込むこと無く、真に経営の高度化に役立つ情報システム監査として発展させることである。今後皆様のご批判を得て、有効な保証型監査モデル構築を進めて行きたい。

参考文献

[1] 経済産業省、「情報セキュリティ監査基準」、平成 15 年 4 月 1 日.
[2] 経済産業省、「システム監査基準」、平成 16 年 10 月 8 日.
[3] 経済産業省、「情報セキュリティ監査基準、報告基準ガイドライン」、平成 15 年 4 月 1 日.
[4] 企業会計審議会、「財務情報等に係る保証業務の概念的枠組みに関する意見書」、平成 16 年 11 月 29 日.