情報セキュリティ監査人の責任

石　井　夏　生　利

〔目次〕

１．情報セキュリティ監査人と保証型監査

情報技術(Information Technology)が社会基盤となった現代社会において、情報セキュリティの確保は欠かせない存在となっている。それを担保する重要な制度の１つとして「情報セキュリティ監査」がある。

「情報セキュリティ監査」とは、「情報セキュリティに係るリスクのマネジメントが効果的に実施されるように、リスクアセスメントに基づく適切なコントロールの整備、運用状況を、情報セキュリティ監査を行う主体が独立かつ専門的な立場から、国際的にも整合性のとれた基準に従って検証又は評価し、もって保証を与えあるいは助言を行う活動」をいう。この定義は、経済産業省商務情報政策局長の諮問委員会である「情報セキュリティ監査研究会」が、2003年３月26日に公表した「情報セキュリティ監査研究会報告書」によっている。同研究会は、情報の電子化に伴い、情報システムへの不正侵入、機密情報・個人情報の外部漏えい、情報システムに保存されているデータの破壊、ホームページの改ざんや情報システムのダウンといった、情報セキュリティ事故が生じるようになったことを受け、独立かつ専門的知識を持った者によって、当該組織の情報セキュリティ対策の有効性を評価してもらう制度整備が喫緊の課題であるという問題認識に基づき、設置された。

研究会は、2002年９月から検討を開始し、前記報告書によって、「情報セキュリティマネジメント」を確立するための情報セキュリティ監査制度の設置を提言した。経済産業省は、この提言を受け、2003年４月１日、情報セキュリティ監査制度の運用を開始した。この制度は、「情報セキュリティ監査基準」及び「情報セキュリティ管理基準」等に基づき運用されている。情報セキュリティ監査を受けた企業は、2003年度は4714件、2004年度は6032件、2005年度は9093件となっており、飛躍的に増加している(1)。

また、情報セキュリティ監査制度を着実に浸透させていくための運営組織として、特定非営利活動法人日本セキュリティ監査協会(Japan Information Security Audit Association, JASA)が設立された。JASAは、2005年１月、「公認情報セキュリティ監査人」制度を発足させ、情報セキュリティ監査制度の普及を図っている。

(1) 特定非営利活動法人日本セキュリティ監査協会のウェブ・サイトのうち、「情報セキュリティ監査制度」のページ(http://www.jasa.jp/kansa/jyoho.html)参照。

そして、最近の政府の動きの中で着目すべきは、「保証型監査」の推進である。内閣官房情報セキュリティセンター(National Information Security Center, NISC)は、情報セキュリティ政策に係る基本戦略の立案等を行っており、その一環として、中長期計画の「情報セキュリティ基本計画」、年度計画の「セキュア・ジャパン」をそれぞれ策定している。「第1次情報セキュリティ基本計画」(2006年２月１日付)では、「第３章　今後３年間に取り組む重点政策－「新しい官民連携モデル」の構築－」の中で、地方公共団体の取るべき対策として「情報セキュリティ監査実施の推進」、企業の取るべき対策として「情報セキュリティ人材の確保・育成」が掲げられた。そして、「セキュア・ジャパン2007－ITを安全・安心に利用できる環境づくりのための情報セキュリティ対策の底上げ－」(2007年６月14日付)では、2008年度の重点政策の方向性として、「情報セキュリティ人材の育成・確保に向けた集中的な取組み」の中で、「保証型情報セキュリティ監査の普及(経済産業省)　監査人が一定の保証を与える保証型情報セキュリティ監査の普及のため、保証型監査ガイドラインを作成等するとともに、その普及方策について検討を行う」ことなどが掲げられた。

監査の形態には助言型監査と保証型監査があり、「セキュア・ジャパン2007」が推進するのは後者である。保証型監査の考え方は、会計監査などの他の監査業務から取り入れられており、将来的には情報セキュリティによる市場の評価、格付け制度なども見据えたものである。また、他の関連する制度(会計監査、システム監査、内部統制にかかわる監査、ISMS適合性評価制度など)との整合性や相乗効果などを考慮した制度であると説明されている。(2)

ところで、助言型・保証型を含めた監査業務は、「保証業務」の一内容である。「保証業務」とは、「主題に責任を負う者が一定の規準によって当該主題を評価又は測定した結果を表明する情報について、又は、当該主題それ自体について、それらに対する想定利用者の信頼の程度を高めるために、業務実施者が自ら入

(2)　大木栄二郎監修・日本セキュリティ監査協会編『情報セキュリティ監査公式ガイドブック』(日科技連出版、2007年)８頁。

手した証拠に基づき規準に照らして判断した結果を結論として報告する業務」をいう。この言葉は、国際会計士連盟の国際監査・保証基準審議会が「国際監査基準」を策定する過程において、従来の監査業務のみならず、レビュー業務などを包摂した“Assurance Engagements”として登場したものである。(3)

保証業務には、財務諸表監査、内部統制の有効性検証業務、コンプライアンス検証業務、環境マネジメントシステム認証などが該当し、合意された手続(4)、財務諸表の作成・編集、税務業務、コンサルティングは含まれない(5)。

財務諸表監査を例に取ると、「主題に責任を負う者」は当該会社経営者、「一定の規準」は会計基準、「主題」は財務情報、「主題情報」は四半期財務情報、「想定利用者」は株主、「業務実施者」は監査法人、「業務実施者が準拠する規準」は監査基準、「判断結果の報告」は、企業の財政状態、経営成績及びキャッシュ・フローの状況をすべての重要な点において適正に表示しているかどうかに関する意見表明であると考えられる。情報セキュリティ監査の場合は、判断結果の報告形態として「助言型」と「保証型」に分類されることになる。保証業務のいう「保証」と保証型監査のいう「保証」は意見表明である点で共通するが、前者が後者を包摂する概念である。

また、レビューとは、諸外国において、「財務諸表には会計基準に照らして特に修正を要する重要な事項は見当たらなかったことを、限定した手続により消極的に証明する業務」であるとされている。しかし、財務諸表全体が適正であるか否かについての意見を表明する監査とは、保証水準を明確に異にするという理由により、レビュー業務は、監査基準の対象から除外されている(6)。

---

(3)　企業会計審議会2004年11月29日付「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」(http://www.fsa.go.jp/news/newsj/16/singi/f-20041129-1/01.pdf) 2 頁及び 4 頁。

(4)　合意された手続とは、業務実施者が業務依頼者との間で合意された手続を実施し、その実施結果を報告するものである。意見表明は伴わないため、保証業務には含まれない。

(5)　和貝享介「財務諸表監査以外の保証業務等に関する実務指針について」会計情報第348号 (2005年) 8 頁以下。

(6)　企業会計審議会2002年 1 月25日付「監査基準の改訂に関する意見書」(http://www.fsa.go.jp/singi/singi_kigyou/tosin/f-20020125-1.pdf) 4 頁。

一方で、保証型監査の与える法的効果、及び、情報セキュリティ監査人の法的責任を考えた場合、それは必ずしも明確とはいいがたい。日本において、「お墨付き」の与える社会的効果は非常に高く、例えば、2007年12月時点のデータによれば、日本のISMS認証取得事業者数は、世界全体の認証取得事業者数のうち、約57パーセントを占めている(7)。この背景には、客観的なセキュリティレベルを担保できるとの期待が存在すると考えられる。しかし、ISMS適合性評価制度は、当該組織の情報セキュリティマネジメントシステムについて、ISMS認証基準に準拠していることを認定するにすぎず、必ずしも社会の期待に応えた制度であるとはいいがたい。また、後述するように、監査にはそもそも機能的な限界があり、会計監査の世界では、財務諸表監査に対する社会の「期待ギャップ」(expectation gap)の問題が指摘されている。このようなことから、「お墨付き」を与えるような形態の監査については、インシデントが発生しないことの担保が得られたという誤解を与えることが懸念される。「情報セキュリティマネジメント」を実効性あるものにするためには、社会的に信頼されるような制度設計が必要であり、公認情報セキュリティ監査人制度についても同様である。

そこで、本稿では、保証型監査に着目しつつ、会計監査との比較において、とりわけ虚偽証明の場合における情報セキュリティ監査人の責任を検討してみることとしたい。

２．公認会計士の会計監査

２.１．公認会計士とは

(7)　International Register of ISMS Certificates, http://www.iso27001certificates.com/ (last visited Jan. 26, 2008). このサイトによれば、4140件のうち2354件が日本の事業者で占められている。なお、2008年１月18日現在における日本のISMS認証取得事業者数は2472件である。

公認会計士は、その専門的能力を基礎として、広く他人の依頼に応じて報酬を得て監査と会計に関する専門的なサービスを提供することを専門の業務とする者である[8]。1948年に制定された公認会計士法[9]によって創設された制度であり、財務諸表の真実性の確保と投資家の保護を目的とする。

公認会計士になるためには、公認会計士試験に合格し、2年以上の業務補助等の期間を経験し、実務補修団体等における実務補修を修了し、内閣総理大臣から実務補修を修了した旨の確認を受け、かつ、公認会計士名簿の登録を受けなければならない(公認会計士法第3条、同法第15条第1項、同法第16条第1項、同法第17条)。公認会計士名簿は、日本公認会計士協会に備え付けられる(同法第18条)。

公認会計士は、法律上、独立性・専門性を持つ(同法第1条)。

また、公認会計士法については、特に1963年から1965年にかけて、会社の倒産や破綻が相次ぎ、会社の巨額な粉飾決算が社会問題化したため、公認会計士制度の実効性を高めるべく、1966年の改正法によって、監査法人制度が創設された[10]。

その後の大きな改正は、2003年である。アメリカでは、エンロン社、ワールドコム社等の不正会計事件を背景として、2002年7月30日、「2002年上場企業会計改革及び投資家保護法、2002年サーバンス・オクスリー法」(Public Company Accounting Reform and Investor Protection Act of 2002, Sarbanes-Oxley Act of 2002)[11]が成立した。日本も、企業の粉飾決算や、バブル経済崩壊後の証券会社や銀行等の経営破たんをきっかけに、監査の公正性と信頼性を確保する必要性等から、公認会計士法の抜本改正に着手し、2003年5

(8) 羽藤秀雄『改正 公認会計士法 日本の公認会計士監査制度』(同文舘出版、2004年)6頁。
(9) 昭和23年7月6日法律第103号。
(10) 羽藤・前掲『改正 公認会計士法』10頁。
(11) Pub. L. No. 107-204, 116 Stat. 745 (codified as amended in scattered sections of 11, 15, 18, 28, and 29 U.S.C.).

月30日、公認会計士の使命及び職責の明文化、監査法人等に対する監視・監督の機能及び体制の充実・強化、公認会計士試験制度の見直し等を盛り込んだ改正法を成立させた(2003年６月６日公布、2004年４月１日一部施行、2006年１月１日全部施行[12])。

また、後述するとおり、2007年にも重要な改正がなされた。きっかけは、カネボウの粉飾決算に加担した中央青山監査法人の公認会計士が逮捕・起訴されたこと、ライブドア事件で港陽監査法人の公認会計士が在宅起訴されたことにある。これによって、監査法人に対する批判や規制強化の機運が高まり、2007年６月27日、改正公認会計士法が成立した[13]。同法は2008年４月１日に施行される予定である。

２.２. 監査証明業務

公認会計士は、他人の求めに応じ報酬を得て、財務書類の監査又は証明をすることのほか(公認会計士法第２条第１項)、財務書類の調製、財務に関する調査若しくは立案、又は財務に関する相談に応ずることを業とする(同条第２項)。前者は「監査証明業務」、後者は「非監査証明業務」と呼ばれている。前者の「監査」及び「証明」はいずれも保証業務、後者は非保証業務である。独占業務として位置づけられるのは、監査証明業務であり、最も重要な業務とされている(同法第47条の２[14])。

ここで、監査とは、「ある行為あるいはある行為の結果を示す情報等について、独立の立場にある第三者が検査することによって、その真実性、妥当性などを確かめ、その結果を関係者に報告すること」をいう。監査主体となる第三者は監査人、監査対象は、行為又はその結果を示す情報等、監査行為は、「検

(12)　平成15年６月６日法律第67号。羽藤・前掲『改正　公認会計士法』15～17頁。
(13)　平成19年６月27日法律第99号。
(14)　羽藤・前掲『改正　公認会計士法』37頁以下、73頁以下。

査すること」、「確かめること」、「報告すること」である。(15)

監査の語源は２つの系統からなると説明されている。１つは、英語で“audit”、フランス語では“audition”といい、その語源はラテン語の“audire”からきている。その意味は「聞くこと、聴聞すること、理解すること、従うこと、弟子であること、注意すること、是認すること」である。(16)もう１つは、ドイツ語、スペイン語の“revision”であり、その語源はラテン語の“revisere”からきている。意味は「再び尋ねること、帰って見ること、見に帰ること、再び行って見ること、もう一度訪ねること」である。(17)いずれの行為(聴く、再び見る)も、他人の行為に対して聴取し、それを監察、調査する行為からなる用語である。(18)

監査証明業務がいかなる場合に求められるかについては、金融商品取引法や会社法等を根拠法とする「法定監査」、及び、法律に根拠はなく、監査の目的も内容も当事者の契約によって任意に定められる「任意監査」に分けることができる。

会社法上、会計監査人は、株式会社の計算書類及びその附属明細書、臨時計算書類並びに連結決算書類を監査し、会計監査報告を作成することが義務付けられている(会社法第396条～第399条、第436条第２項)。大会社及び委員会設置会社は会計監査人を置かなければならない(同法第327条第５項、同法第328条)。会計監査人は、公認会計士又は監査法人でなければならない(同法第337条第１項)。

金融商品取引法は、金融商品取引所に上場されている有価証券の発行会社等に対し、計算書類等及び内部統制報告書について、原則として特別の利害関係を持たない公認会計士又は監査法人の監査証明を受けることを義務付けている

(15)　石田三郎『監査論の基礎知識　五訂版』(東京経済情報出版、2005年)５頁。
(16)　柴田光蔵『法律ラテン語辞典』(日本評論社、2004年)37頁。
(17)　國原吉之助『古典ラテン語辞典』(大学書林、2005年)656頁。
(18)　石田・前掲『監査論の基礎知識　五訂版』４頁。

（金融商品取引法第193条の２）。

ところで、監査については、従来から「期待ギャップ」の問題が存在していた。従来の考え方では、会計監査の主たる目的は、財務諸表が財政状態や経営成績などを適正に表示しているかどうかの表明であり、不正・誤謬の摘発は二次的目的に過ぎなかった。しかし、企業の証券・金融における不祥事や経営者不正による経営の破綻などに見られる企業の反社会的行動が社会問題になり、経営者等の不正摘発に対する監査責任が問われるようになった。このように、不正・誤謬の摘発に関して、監査の主目的と社会の期待の間にギャップが存在することを、「期待ギャップ」と呼んでいる[(19)]。これに対応する形で、金融庁の企業会計審議会は、2002年１月25日付「監査基準の改訂に関する意見書」の中で、次のように監査の目的を明確にしている。

「⑴　監査の目的は、経営者の作成した財務諸表に対して監査人が意見を表明することにあり、財務諸表の作成に対する経営者の責任と、当該財務諸表の適正表示に関する意見表明に対する監査人の責任との区別（二重責任の原則）を明示した。

⑵　監査人が表明する意見は、財務諸表が一般に公正妥当と認められる企業会計の基準に準拠して、企業の財政状態、経営成績及びキャッシュ・フローの状況をすべての重要な点において適正に表示しているかどうかについて、監査人が自ら入手した監査証拠に基づいて判断した結果を表明したものであることを明確にした。

⑶　改訂基準では、基本的な構成からなる財務諸表に対する監査を前提として、財務諸表が企業の財政状態、経営成績及びキャッシュ・フローの状況を適正に表示しているかどうかについて意見を表明するとしているが、監査の対象となる財務諸表の種類、あるいは監査の根拠となる制度や契約事項が異なれば、それに応じて、意見の表明の形式は異なるもの

(19)　石田・前掲『監査論の基礎知識　五訂版』11頁以下。

となる。

⑷　適正意見と虚偽の表示との関係について、監査人が財務諸表は適正に表示されているとの意見を表明することには、財務諸表には全体として重要な虚偽の表示がないことの合理的な保証を得たとの自らの判断が含まれていることを明確にした。

⑸　合理的な保証を得たとは、監査が対象とする財務諸表の性格的な特徴(例えば、財務諸表の作成には経営者による見積りの要素が多く含まれること)や監査の特性(例えば、試査で行われること)などの条件がある中で、職業的専門家としての監査人が一般に公正妥当と認められる監査の基準に従って監査を実施して、絶対的ではないが相当程度の心証を得たことを意味する。

なお、監査報告書における適正意見の表明は、財務諸表及び監査報告書の利用者からは、結果的に、財務諸表には全体として重要な虚偽の表示がないことについて、合理的な範囲での保証を与えているものと理解されることになる。」

要するに、①監査の最終目的は意見表明であること、②意見とは、財務諸表の適正性について、監査人が自ら入手した監査証拠に基づく判断結果を表明すること、③適正意見の中には、財務諸表には全体として重要な虚偽の表示がないことの合理的な保証を得たとの自らの判断が含まれること、④合理的な保証とは、職業専門家としての監査人が、絶対的ではないが相当程度の心証を得たこと、を意味する。③の「全体として重要な虚偽の表示がない」ことを捉え、肯定的不正摘発責任を明確にしたという評価がなされている。(20)

しかし、保証とはいえ絶対的なものではなく、あくまで職業専門家の心証に基づく意見表明にすぎない。また、冒頭で触れた保証業務に関しては、公認会計士法をはじめとして、法制度上の定義づけや法的効果が明示的に与えられて

(20)　石田・前掲『監査論の基礎知識　五訂版』14頁。

いるわけではないことにも注意が必要である。[21]

３．公認会計士の法的責任

公認会計士は、監査及び会計の専門家として、独立した立場において、財務書類その他の財務に関する情報の信頼性を確保することにより、会社等の公正な事業活動、投資家及び債権者の保護等を図り、もって国民経済の健全な発展に寄与することを使命とする（公認会計士法第１条）。

しかし、公認会計士が職務上果たすべき義務を怠った場合には、民事責任、刑事責任の追及を受けるほか、公認会計士法上の行政処分を受けることもある。これらの責任は、公認会計士個人の責任と監査法人の責任に分けることができる。主体による責任の違いは、民事責任の場面ではさほど大きくは取り上げられないが、刑事責任及び行政処分の場面では重要性を持つ。

３.１．公認会計士・監査法人の民事責任

民事の場面では、契約違反ないしは不法行為責任が問題となり、会社法及び金融商品取引法には、会計監査人の責任に関する規定が存在する。

まず、会計監査人と株式会社との関係は委任に関する規定に従う（会社法第330条）[22]ことから、会計監査人としての公認会計士は、会社に対して善管注意義務を負う（民法第644条）。

会計監査人は、その任務を怠ったときは、会社に対し、これによって生じた損害を賠償する責任を負う（会社法第423条第１項）。また、会計監査人は、職務を行うについて悪意又は重大な過失があったときは、これによって第三者に生じた損害を賠償する責任を負う（同法第429条第１項）。ただし、会計監査報告に記載し、又は記載すべき重要事項についての虚偽の記載又は記録を行った

(21)　羽藤・前掲『改正　公認会計士法』91頁。
(22)　準委任契約と解するのが通説である。

ことについて、当該会計監査人が注意を怠らなかったことを証明したときは、責任を免れる(同条第３項)。一般の不法行為の場合は、原告が被告の過失を立証しないと不法行為責任を問うことはできないが、この規定によって会計監査人が無過失を立証しなければならない。

金融商品取引法上、有価証券届出書のうちに重要な事項についての虚偽記載等があった場合に、当該監査証明に関する書類に虚偽記載等がないものとして証明した公認会計士・監査法人は、当該有価証券の募集又は売出しに応じて取得した者に対し、それによって生じた損害を賠償する責めに任ずる(金融商品取引法第21条第１項第３号)。ただし、当該会計士・監査法人が故意又は過失の不存在を証明したときは、責任を免れる(同法同条第２項第２号)。また、虚偽記載等を知らずに、当該有価証券を募集又は売出しによらないで取得した者に対しても、損害賠償の責任を負う(同法第22条第１項)。免責規定も準用される(同法同条第２項)。第22条の規定は、内部統制報告書等についても準用されている(同法第24条の４の６)。

会計監査人がいかなる場合に過失を免れることができるかという点については見解が分かれており、①会計監査人が監査基準にしたがって監査を行い、それを監査調書に記載しておけば、過失のないことが立証されるとするもの、②①に加えて、一連の粉飾決算事件や企業倒産事件を契機に公認会計士協会が公表した実務指針に基づき、被監査会社の内部統制組織の整備状況等を個別的具体的に検討し、会計処理の適法性・適正性を図る観点から、その実態に適合した監査手続を取るべきと解釈するもの[(23)]などがある。また、現行の監査基準第２の第３項には、「監査人は、職業的専門家としての正当な注意を払い、懐疑心を保持して監査を行わなければならない」との規定が存在し、これは、善管注意義務よりも高度なものと解釈するものがある[(24)]。

(23)　根田正樹「公認会計士の責任」川井健・塩崎勤編『新・裁判実務体系８　専門家責任訴訟法』(青林書院、2004年)98頁以下。
(24)　羽藤・前掲『改正　公認会計士法』31頁。

公認会計士の責任が認められた裁判例としては、東京地方裁判所2003(平成15)年４月14日判決がある[25]。この事件では、公認会計士が労働組合の会計監査(法定監査)を行うに当たって、預金通帳の原本を実査せず、組合員の横領行為に気づかずに適正意見を表明した行為について、債務不履行に当たるか否かが問題となった。東京地裁は、「公認会計士が計算書類の監査を行うにあたっては、計算書類の適正性・適法性を確かめる前提として、不正・誤謬があり得ることを当然念頭に置いて監査を行う必要があることを考えると、『預金の実在性』という監査要点については、特段の事情がない限り、少なくとも預金先に対し直接預金残高を確認するか又は預金通帳の原本を実査することは通常実施すべき監査手続として要求されており、このような監査手続を実施することが監査契約上の注意義務の内容をなしているというべきである」と判示し、監査を依頼した原告の請求を一部認容した。

他方、責任の否定された事例としては、大阪地方裁判所2005(平成17)年２月24日判決がある[26]。これは、旧山一證券株式会社の株主であった原告が、山一證券の自主廃業によって、保有する株式を１株１円で売却することとなり、損害を被ったとして、中央青山監査法人及び国を相手取って損害賠償を請求した事案である。監査法人に関しては、有価証券報告書の重要事項に虚偽記載があったにもかかわらず、それがないものとして監査証明した行為について、旧証券取引法第24条の４等の違反が問題となった。大阪地裁は、監査は不正の発見・摘発を直接の目的とするものではないこと、不正や誤謬による重要な虚偽記載が全くないという絶対的な保証を得ることまでを求めてはいないこと、被監査

(25)　東京地判平成15年４月14日判時第1826号97頁。解説は、湯川益英「監査契約に基づく労働組合の財務諸表の法定監査において、預金通帳の実査を行わず、組合内部の横領行為を発見できないままに適正意見を表明した公認会計士の債務不履行責任(注意義務違反)の有無」判時第1846号(2004年)183頁以下。また、最近の裁判例の傾向をまとめたものとしては、志谷匡史「公認会計士の任務懈怠とその責任－主要判例を素材に－」月刊監査役第524号（2007年）18頁以下、秋坂朝則「公認会計士の責任」民事法情報第220号（2005年）74頁以下。

(26)　大阪地判平成17年２月24日判時第1931号152頁。

会社の任意の協力により監査手続を実施することが前提とされていること、また、監査手続が原則として試査によらざるを得ないことなどから、次のように判示した。

「監査法人が、重要な事項について虚偽の記載のある有価証券報告書について、「監査基準、監査実施準則及び監査報告準則の改訂について」(企業会計審議会平成３年12月26日報告)に定める監査基準及び監査実施準則に従い、通常実施すべき監査手続(監査実施準則２項)を実施し、その過程において、監査人として通常要求される程度の注意義務(職業的監査人としての正当な注意を払う義務)を尽くして監査に当たったにもかかわらず、当該虚偽記載があることを発見するに至らなかった場合には、当該有価証券報告書について記載が虚偽であるものを虚偽でないものとして証明したことについて、当該監査法人に過失があるということはできず、当該監査法人は、上記損害賠償責任を負わないものと解するのが相当である。」

そして、大阪地裁は、中央青山監法人において、財務諸表の監査に際し、その都度、山一證券の経営状況、財務内容等に応じてあらかじめ監査計画を定め、これに基づいて種々の監査手続を選択・適用し、監査を実施していたことから、おおむね通常実施すべき監査手続が実施されていたとして、原告の請求を棄却した。

大阪地方裁判所2006(平成18)年3月20日判決[(27)]では、同様の事案において、「監査人としては、財務諸表の監査に当たり、善良なる管理者としての注意義務をもって、主として監査基準に基づき通常実施すべき監査手続を実施する義務を負っており、この通常実施すべき監査手続とは、監査実施準則の定めに従い、公正な監査慣行を踏まえ、十分な監査証拠を入手し、財務諸表に対する意見表明の合理的な基礎を得るために必要と認められる手続を中心とすると解するのが相当である」とし、監査に関する職業的専門家として一般的に要求される程

(27)　大阪地判平成18年３月20日判時第1951号129頁。

度の注意義務をもって、通常実施すべき監査手続等を実施していれば過失は存在しない旨を判示した。

これらの判断の分かれ目は、会計監査の性質をいかにとらえるかによる。不正や誤謬があり得るということを常に念頭に置いて監査に望む必要があると考えれば、会計監査人は、重要な虚偽記載等の不正を発見すべく努めなければならない、ということになる。他方、監査人の任務にも限界が存在することを考慮すれば、監査基準に従い、通常実施すべき監査手続を実践することにより必要な注意義務を果たした、ということになる[(28)]。判例は、監査に対する社会の期待よりも、監査に内在する限界から注意義務のレベルを導き出しているようである。

ところで、監査法人が賠償責任を負う場合の内部負担については、公認会計法が定めを置いている。以前は、監査法人は、５人以上の公認会計士によって組織され、無限連帯責任を負うこととなっていた（公認会計士法第34条の７、第34条の10の５）。しかし、2007年改正法によって、①内閣総理大臣への登録、②最低資本金、③供託金、④計算書類の開示といった要件を満たすことにより、有限責任監査法人（社員の全部を有限責任社員とする定款の定めのある監査法人）の設立が認められた。ただし、虚偽証明事案に関する業務執行社員については、無限連帯責任が課せられる[(29)]。これは、諸外国でも有限責任形態の監査事務所が一般化していること、日本でも社員が数百人規模の監査法人が出現している現状等に鑑み、非違行為に関係しない社員については有限責任化の途を開いていくことを目的とする[(30)]。

(28)　前掲志谷匡史神戸大学大学院法学研究科教授の分析によれば、裁判例の傾向は、最低限度の注意さえ尽くさなかったと判断し得るだけの会計士側の大きな落ち度があったとされない限り、会計士が賠償責任を問われる可能性は相当低いとのことである。

(29)　金融庁金融研究研修センター2007年９月７日付「公認会計士法等の一部を改正する法律の概要」（http://www.fsa.go.jp/frtc/kenkyu/20070907/06.pdf）参照。

(30)　金融審議会公認会計士制度部会2006年12月22日付「公認会計士・監査法人制度の充実・強化について」（http://www.fsa.go.jp/singi/singi_kinyu/tosin/20061222.pdf）12頁。

3.2. 公認会計士・監査法人の刑事責任

3.2.1. 監査法人の刑事責任

刑事責任の場面では、法人処罰の議論に着目しなければならない。

2007年の公認会計士法の改正に先立ち、内閣総理大臣の諮問機関である金融審議会の公認会計士制度部会(部会長・関哲夫新日本製鉄株式会社常任監査役)が、約3年ぶりに再開され、2006年4月26日(通算第5回目)から11回にわたる会合を開いた。この中で、法人処罰に関する議論が登場した。初回の会合では、証券取引等監視委員会が、旧証券取引法第197条第1項第1号の定める有価証券報告書等虚偽記載罪について、「監査法人に刑事罰を適用できるようにすべき」との建議を金融庁長官に提出していることが紹介された。背景には、カネボウ事件に絡み、中央青山監査法人自体の虚偽記載罪を立件できなかったことがある。これに対し、刑事罰の導入は、監査法人にとって「死刑宣告」に等しく、日本公認会計士協会は、実質的に解散命令に近い結果が生じるとして強く反対した。(31)

結局、2006年12月22日付金融審議会公認会計士制度部会の報告「公認会計士・監査法人制度の充実・強化について」では、法人処罰の是非について、①まずは行政的な手法の多様化等により対応すべきこと、②法的に見ても、法人の犯罪能力そのものが認められているわけではないこと、③虚偽記載罪の名宛人は有価証券報告書を作成する企業であり、監査法人に両罰規定を設けるためには、公認会計士個人についての虚偽記載罪等を新設する必要があるが、これの妥当性についてはさらなる検討が必要である、という理由で、1つの検討課題に位置づけられるにとどまった。

確かに、刑事法の分野では、犯罪の主体について、自然人である個人を前提とし、法人に対しては両罰規定を設けるにとどまっていた。それは、(a)法人には意思に基づく身体の動静がない以上、「行為」は考えられない、(b)主体

(31) 種村大基『監査難民』(講談社、2007年)164頁以下。この書籍の中では、2007年の法改正をめぐる諸事情が分析・紹介されている。

的・倫理的自己決定もなく、倫理的な責任非難ができない、(ｃ)現行刑法は生命刑・自由刑が中心である以上法人には適用し得ない、(ｄ)法人には刑罰感受能力が欠けているということが根拠とされてきた。しかし、(ａ)’法人に自然人と全く同様の、意思に基づく身体の動静はあり得ないが、それでも犯罪の主体となり得る、(ｂ)’刑罰にとって倫理的な非難は本質的な問題ではなく、処罰を国民が納得し得ればそれで足りる、(ｃ)’現行刑法典は自然人を念頭に刑罰の種類を設定したため自由刑が多いが、罰金刑も存在し、それは法人に科し得ることから、最近では、企業(法人)自体の責任を問うべきという考え方が有力化している[(32)]。

したがって、この議論を踏まえれば、公認会計士制度部会の掲げる法的な問題をクリアすることは可能である。今後も大型粉飾決算事件が多発するなどの事態が生ずれば、監査法人の処罰をめぐる議論が再燃する可能性がある。

３.２.２. 公認会計士の刑事責任

一方、公認会計士個人が有価証券報告書等の虚偽記載罪に問われた事件では、初の実刑判決が下されている。

東京地方裁判所は、2007(平成19)年３月23日、公認会計士２名が、ライブドアの粉飾決算事件で、有価証券報告書に虚偽の内容が記載されているのを知りながら、監査で問題がないとする適正意見を付けた行為に対し、有価証券報告書の虚偽記載罪に基づき、それぞれ、懲役10月の実刑、及び、懲役1年・執行猶予４年の有罪判決を言い渡した[(33)]。小坂敏幸裁判長は、判決理由の中で、「犯行の隠ぺい行為に積極的に関わった」と認定し、「公認会計士として社会から託された職責を果たさず、堀江被告らの粉飾を是認した。ライブドアが一般投

(32)　前田雅英『刑法総論講義』(東京大学出版会、第４版、2006年) 98～100頁。法人処罰をめぐる思考的枠組みを専門的に分析したものとしては、樋口亮介「法人処罰・特集・刑法典の百年」ジュリスト第1348号 (2008年)69頁。

(33)　東京地判平成19年３月23日公刊物未登載。

資家を欺くのを阻止できたにもかかわらず、それを助長した責任は重い」と判断している。また、この２人が、不正の発覚を防ぐために粉飾の仕組みを複雑化させた点についても、「専門知識を悪用しており悪質だ」と述べている。(34)

このように、法人処罰は見送られたが、公認会計士個人については、厳しい判断が下されるケースもある。

３.３. 公認会計士・監査法人に対する行政処分

３.３.１. 2007年改正前の懲戒処分

2007年改正前の公認会計士法は、公認会計士に対する懲戒処分として、戒告、２年以内の業務停止、登録抹消(公認会計士法第29条)、監査法人に対するものとして、戒告、２年以内の業務停止、解散命令に関する規定を置いていた(同法第34条の21第２項)。

公認会計士の懲戒事由は、(ａ)故意に、虚偽、錯誤又は脱漏のある財務書類をそうでないものとして証明した場合(同法第30条第１項)、(ｂ)相当の注意を怠り、重大な虚偽、錯誤又は脱漏のある財務書類をそうでないものとして証明した場合(同法第30条第２項)、(ｃ)監査法人が虚偽、錯誤又は脱漏のある財務書類をそうでないものとして証明した場合において、当該証明に係る業務を執行した社員である公認会計士に故意又は相当の注意を怠った事実があるとき(同法第30条第３項)、(ｄ)公認会計士法に基づく命令に違反したとき、又は、第34条の2に基づく内閣総理大臣の指示に従わないとき(同法第31条)、である。

(ａ)～(ｃ)は、虚偽又は不当な説明についての懲戒、(ｄ)は一般の懲戒とされている。(ａ)は２年以内の業務停止又は登録抹消、(ｂ)は戒告又は２年以内の業務停止、(ｃ)は(ａ)ないしは(ｂ)の処分、(ｄ)は懲戒の種類に挙げた３つの処分をすることができる。いずれも処分を下すのは、内閣総理大臣で

(34) 読売新聞2007年３月23日夕刊１面、同22面。朝日新聞2007年３月23日夕刊19面。

ある。また、懲戒処分がなされた場合は、その旨が公告される（同法第34条第３項）。カネボウの粉飾決算事件では、金融庁によって、2006年５月10日、１名の公認会計士に対する１年間の業務停止、２名の公認会計士に対する登録抹消、中央青山監査法人に対する２ヶ月間の業務停止処分が下されており、記憶に新しい。

監査法人の懲戒事由は、①社員の故意により、虚偽、錯誤又は脱漏のある財務書類を虚偽、錯誤及び脱漏のないものとして証明したとき、②社員が相当の注意を怠ったことにより、重大な虚偽、錯誤又は脱漏のある財務書類を重大な虚偽、錯誤及び脱漏のないものとして証明したとき、③公認会計士法若しくは同法に基づく命令に違反し、又は運営が著しく不当と認められるとき、④内閣総理大臣の指示に従わないとき、である。

3.3.2　行政処分の多様化

前記公認会計士制度部会の報告書は、法人処罰の導入を見送った理由の１つに、行政処分の多様化を掲げたことから、それを穴埋めするかのように、2007年改正法によって、次のような行政処分が新設された。

①　監査法人に対して

・業務管理体制の改善命令（改正法第34条の21第２項）

・違反行為に重大な責任を有すると認められる社員について、２年以内の期間を定めて、当該監査法人の業務又は意思決定の全部又は一部に関与することの禁止命令（同法第34条の21第３項）

②　個人に対して

・公認会計士が著しく不当と認められる業務の運営を行った場合に、内閣総理大臣による必要な戒告又は２年以内の業務停止（同法第31条第２項）

③　監査法人・公認会計士に対して

・財務書類の虚偽証明にかかる課徴金納付命令（同法第31条の２、第34条の21の２）

故意の場合：監査報酬相当額の1.5倍

相当の注意を怠った場合：監査報酬相当額

3.4　小括

以上のとおり、会計監査人・監査法人の責任論をめぐる傾向を簡単に整理してみた。全体的に見ると、①虚偽証明については、民事責任、刑事責任、行政処分のいずれについても法律上の手当てがなされている、②民事責任をめぐる判例、法人処罰の見送りの点を除けば、責任の厳格化の傾向が見られる、③とりわけ、行政処分の強化が目立つ、とまとめることができる。

4．情報セキュリティ監査人の責任

4.1．情報セキュリティ監査とは

冒頭でも紹介したとおり、情報セキュリティ監査は、「情報セキュリティに係るリスクのマネジメントが効果的に実施されるように、リスクアセスメントに基づく適切なコントロールの整備、運用状況を、情報セキュリティ監査を行う主体が独立かつ専門的な立場から、国際的にも整合性の取れた基準に従って検証又は評価し、もって保証を与えあるいは助言を行う活動」と定義されている。情報セキュリティ監査を行う主体は、内部の場合は組織体の内部監査部門、外部の場合は、監査法人、情報セキュリティ関連のシステム構築を行うベンダー、一般のシステム構築を行うベンダー、システム監視等を行う情報セキュリティ専門企業、システム監査企業などがある[(35)]。監査目的は「情報セキュリティマネジメントの効果的な実施」、監査対象は「情報資産」に対する「リスクアセスメントに基づく適切なコントロールの整備、運用状況」である。

そして、「国際的に整合性の取れた基準」として、経済産業省は、情報セキュリティに係るマネジメントサイクルの確立のための国際標準規格であるISO/

(35)　経済産業省2003年３月26日付「情報セキュリティ監査研究会報告書」(http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Report.pdf)12頁。

IEC17799：2000(JISX5080：2002)[36]に準拠した形で、「情報セキュリティ管理基準」を公表している。管理基準は、情報セキュリティ監査を行う際の判断尺度である。これとは別に、監査の際に監査主体が従うべき行為規範を定めたものを「情報セキュリティ監査基準」という。監査基準は、①監査人としての適格性及び監査業務上の遵守事項を規定する「一般基準」、②監査計画の立案及び監査手続の適用方法を中心に監査実施上の枠組みを規定する「実施基準」、③監査報告に係る留意事項と監査報告書の記載方式を規定する「報告基準」で構成される。

監査人は、前記基準に従って「検証又は評価し、もって保証又は助言」を与える。そして、情報セキュリティ監査の普及によって、ISMS適合性評価制度による認証取得組織の裾野を広げ、認証取得事業者数の増加との相乗効果を生むことが期待されている[37]。

会計監査との比較でいえば、①会計監査は情報監査、情報セキュリティ監査は実態監査である[38]、②情報セキュリティ監査には助言型監査と保証型監査がある、③公認会計士の会計監査は外部監査であるが、情報セキュリティ監査(助言型)には内部監査を含む、という点で異なっている。

４.２．公認情報セキュリティ監査人

JASAは、2005年１月、「公認情報セキュリティ監査人」(Certified Auditor for Information Security, CAIS)制度を発足させた。この資格は、情報セキュリティ監査主体の質を確保することを目的とする。当該資格を得るためには、知識、経験、実証された能力が必要とされ、資格認定要件の緩やかな順から、

(36)　ISO/IEC17799：2000は、2005年６月に改訂され、ISO/IEC17799：2005となった。その後、2007年４月には、ISO/IEC 27002:2007へとさらに改訂された。
(37)　経済産業省・前掲「情報セキュリティ監査研究会報告書」８頁。
(38)　情報監査は、行為や活動の結果の陳述ないしは主張を対象とする監査をいい、実態監査は、ある特定の人間ないし実体の行為や活動それ自体を対象とする監査をいう。石田・前掲『監査論の基礎知識　五訂版』23頁より。

情報セキュリティ監査アソシエイト、情報セキュリティ監査人補、公認情報セキュリティ監査人、公認情報セキュリティ主任監査人の４つに分けられる。資格を得るためには、情報技術分野で少なくとも４年以上の業務経験があること、そのうち、情報セキュリティ関連分野で少なくとも２年以上の業務経験があることが必須とされる[39]。これらは、個別の情報セキュリティ監査を実際に行うための資格であり[40]、それぞれの役割は次のようになっている[41]。

・情報セキュリティ監査アソシエイト(CIAS-Associate)：監査チームリーダーの要請によりチームの一員として専門知識にもとづく助言を行う。

・情報セキュリティ監査人補(CIAS-Assistant)：情報セキュリティ監査制度に対する知識と経験を有し、OJT(On the Job Training)として監査に参加する。監査経験を積んで、公認情報セキュリティ監査人をめざすことができる。

・公認情報セキュリティ監査人(CIAS-Auditor)：情報セキュリティ監査制度に対する知識と経験を有するとともに、実証された能力として、監査計画を立案し、監査計画に基づいて監査を実施し、報告書を作成し、監査結果を被監査主体に報告する役割を行う。また、上位の監査人の指導のもとで、OJTとして監査チームリーダーを務め、経験を積んで、公認情報セキュリティ主任監査人をめざすことができる。加えて、情報セキュリティ監査人補がOJTとして監査に参加している場合は、これを指導し評価する。

・公認情報セキュリティ主任監査人(CIAS-Lead Auditor)：情報セキュリティ監査制度に対する知識と経験を有するとともに、実証された能力とし

(39)　2007年５月に資格制度が改正され、監査人補の専門分野要件は廃止された。

(40)　社会全体の見地から公正かつ公平な情報セキュリティ監査の実施に寄与し、情報セキュリティ監査制度の普及促進・発展を担保するためのものとして、公認情報セキュリティ主席監査人(CIAS-Principal Auditor)制度も存在する。

(41)　日本セキュリティ監査協会編・前掲『情報セキュリティ監査公式ガイドブック』243頁以下。

て、監査チームを編成し監査を実施する場合に監査チームリーダーとなって、監査計画を立案し、監査計画に基づいて監査を実施し、報告書を作成し、監査結果を被監査主体に報告する役割を行う。また、公認情報セキュリティ監査人がOJTとして監査チームリーダーを務める場合は、これを指導し評価する。

資格を得るためのプロセスは、①研修受講（２日間）、②研修修了試験(60分)、③トレーニング受講(3日間)、④トレーニング修了試験(60分)、⑤経験確認試験(90分)、⑥面接審査となっている。監査アソシエイトは①及び②、監査人補は①～④まで、監査人は①～⑤、主任監査人は①～⑥までの合格によって認定資格を得ることができる。

資格維持の有効期間は３年であり、期限が到来すると、資格及び専門性の更新を行うこととなる。2007年12月12日現在、主任監査人の登録者は67名、監査人は129名、監査人補は109名、監査アソシエイトは143名となっている。

公認会計士と情報セキュリティ監査人の共通点は、独立・専門の立場から監査を行うことにある。しかし、現状では相違点の方が多い。一番大きな違いは、法律に基づく国家資格であるか否かである。公認会計士試験は、国家試験であり、合格者が増加したとはいえ、医師国家試験や司法試験と並ぶ難関の資格試験である。公認情報セキュリティ監査人は民間の資格であり、取得する要件も研修やトレーニングが中心となっている。その一方で、公認会計士には資格の有効期限が存在せず、公認情報セキュリティ監査人には有効期限が存在する。また、公認会計士の場合は、会社法や金融商品取引法に基づく法定監査が存在し、独占業務となっているが、情報セキュリティ監査人にはそのような制度は存在しない。

４.３．保証型監査と期待ギャップ

情報セキュリティ監査には、２つの形態が存在する。１つは、助言型監査と呼ばれるものであり、不備な点(「基準」とのギャップ)を指摘するものである。

これは、従来から行われてきたシステム監査と関連・類似する制度であり、システム監査は、情報システムの信頼性、安全性及び効率性の向上を図る目的の内部監査を前提としている。[(42)] もう１つは、保証型監査と呼ばれるものであり、被監査主体の情報セキュリティマネジメントについての、いわば「お墨付き」を与える形式である。

助言型の監査意見では、「情報セキュリティ管理基準」などに照らした欠陥及び懸念事項を検出事項として提示するにとどまらず、当該検出事項に対応した改善を提言する。

保証型の監査意見では、「情報セキュリティ管理基準」その他の適切な管理基準などを監査上の判断尺度として利用する場合、当該管理基準などに照らして慎重に監査手続を実施した限りにおいて、情報セキュリティ対策において重大な欠陥がないこと(又はあること)を保証する。[(43)] しかし、「インシデントが発生しない」という絶対的な保証ではなく、入手した監査証拠に基づき、「基準」に従って監査手続を行った範囲における合理的な根拠に基づく保証である。[(44)]

助言型監査と保証型監査を比較してみると、助言型監査は、①保証は与えない、②意見は述べる、③提言は行う、④客観的基準は存在することが前提、⑤実施者の独立性は必須、⑥監査結果報告先は経営者若しくはそれに該当する役職者、⑦提言のフォローアップは行う。保証型監査は、①保証は与える、②意見は述べる、③提言は行わない、④客観的基準は存在することが前提、⑤実施者の独立性は必須、⑥監査結果報告先は経営者若しくはそれに該当する役職者、⑦提言は行わないため、そのフォローアップも行わない。[(45)]

両者の違いは、①③⑦にある。助言型監査は、保証は行わないが、対象事項

(42)　システム監査基準は、2004年10月に改訂され、この中では保証型監査の考え方が示されている。
(43)　日本セキュリティ監査協会編・前掲『情報セキュリティ監査公式ガイドブック』35頁。
(44)　同上13頁、98頁。
(45)　同上49頁。

と基準のギャップを検出し、参考意見としての改善提言、及び、そのフォローアップを行う。保証型監査は、信頼性の付与がキーワードであり、保証は与えるが、提言やそのフォローアップは行わない。

情報セキュリティ監査では、多くの場合に助言型監査が行われており、保証型監査は、範囲を限定した一部の保証が一般的である。(46)

そして、保証型監査のメリットとしては、次のような点が挙げられている。(47)

(a) ISMS認証取得企業又は同程度以上の水準の情報セキュリティマネジメントシステムを行っている企業が、より精緻なリスク低減を顧客から要求され、実施している場合など、高度なリスク管理を保証する場合である。顧客が期待する情報セキュリティの要求基準に対して、被監査主体が適正に管理策を実装し、運用しているかを保証する。

(b) ISMS認証は不要だが、顧客と必要な情報セキュリティ対策を約束し、その実施の保証を求める場合など、特定の管理策の実装と実施を保証する。

このような保証型監査は、会計監査における監査証明業務の考え方から登場した。しかし、保証型監査を発展させようとした場合には、会計監査の分野と同様に、社会の「期待ギャップ」の問題を考えておかなければならない。前記のとおり、会計監査の分野では、不正・誤謬の発見をめぐって、監査の主目的と社会の期待の間に齟齬が存在してきた。一方、情報セキュリティ監査基準について、この点はあまり議論されていないようである。

そもそも監査には機能的な限界が存在する。第１に、監査には時間的な制約があり、精査ができず試査(重点的な抜取り検査)になってしまうことが多い。第２に、監査で入手できる証拠は、そのほとんどが結果に関連する間接的な証拠であり、絶対的なものにはなり得ず、監査人の立場の推論として合理的と思われる程度の基礎しか得られない。そのため、監査人の出す結論は、絶対的な

(46)　同上53頁､58頁。
(47)　同上58～59頁。

保証でもなく、強制力や拘束力を持った助言でもなく、あくまで職業専門家としての「意見」にとどまる。第3に、調査できる範囲はすべて過去のデータであり、将来予測したり確証を与えたりすることはできない。

これに対し、「お墨付き」や「信頼性の付与」を強調した場合、どうなるであろうか。

保証型監査によって、社会は、当該組織はインシデントが存在しないことのお墨付きを得たと期待する。しかし、保証型監査は、その時点における情報セキュリティの強度を監査するものではなく[(48)]、あくまでも、「基準」に従って監査手続を行った範囲で合理的な保証を与えるにすぎない。要するに、結果を保証するものではなく、手続を保証するにとどまる。そして、保証とはいえ、それは職業専門家としての意見である。

また、ISMS適合性評価制度自体においても、セキュリティレベルが担保されているとの社会の期待に対し、実際は要求手順に準拠していることを認証するにすぎないという「期待ギャップ」が既に存在している。にもかかわらず、認証取得者数は急速な伸びを示している。

このような状況下で、ISMS適合性評価制度と保証型監査が抱き合わせで発展すれば、二重の意味で「期待ギャップ」の拡大されることが懸念される。合理的な範囲の保証であれば責任を果たしたというのであれば、インシデント発生時に責任逃れの根拠を与えることにもなりかねない。この点は、保証型監査の肯定意見を記載する際に、「監査意見としての保証は絶対的な保証ではなく、入手した監査証拠を評価した結果得られた合理的な根拠に基づく保証である。情報セキュリティ対策の欠陥が皆無であることを保証するものではないため、「合理的な」という字句を含めておくことが有益である」との解説が付されていることにも表れているようである[(49)]。

(48)　経済産業省・前掲『情報セキュリティ監査研究会報告書』7頁。
(49)　日本セキュリティ監査協会編・前掲『情報セキュリティ監査公式ガイドブック』98頁。

４.４．情報セキュリティ監査人の法的責任

情報セキュリティ監査自体が新しいものであって、この分野の監査人の法的責任についての議論は未整理である。また、情報セキュリティ監査人は、民間の資格であるため、法律上の規定は存在しない。そのため、情報セキュリティ監査人を主体とした刑事罰は存在せず、法人処罰の議論も登場しない。そこで、今回は、民事責任及び懲戒処分について、一応の整理を行う。

４.４.１．民事責任

被監査企業が情報漏えい事故を発生させ、情報セキュリティ監査人が故意又は過失により虚偽証明を行っていた場合、当該監査人は、被監査企業に対しては不法行為責任ないしは債務不履行責任、監査結果を信頼した第三者に対しては不法行為責任を問われることになる。

情報セキュリティ監査人と被監査企業との間は、一般的に、有償委任契約が締結されるが、保証型監査の場合、どこまでが意思表示の内容に含まれるかが問題になる。この点、会計監査では、「財務諸表」に対する「適正な表示の有無」を監査するが、情報セキュリティ監査では、「情報資産」に対する「リスクアセスメントに基づく適切なコントロールの整備、運用状況」を監査する。前者の範囲は比較的明確であるが、後者については、企業や組織などが保有する情報全般に対する、適切なコントロールの状況であるため、範囲の特定は容易ではない。したがって、とりわけ保証型監査の場合は、何に対するどこまでの監査が意思表示の内容に含まれるかを明確にする必要がある。

また、保証型監査の「保証」の意味内容について、監査人は、職業専門家として、被監査企業に対して十分な説明を行わなければならない。情報セキュリティ監査に類似した制度としてシステム監査というものが存在するが、これに関しては、「誤謬や不正の潜在的な可能性」が問題点として挙げられている。具体的には、「コンピュータ・システムでは、事前承認されていない個人が資産又は関連する会計記録にアクセスしたり、目に見える証拠を残すことなく

データを改ざんする可能性が増加する。また、手作業システムに比べて処理プロセスへの人間の係わり合いが減少するために、誤謬や不正が長期間発見されないことがある」ということを意味する(50)。情報セキュリティ監査にも同様の性質を伴っているといえることから、「お墨付き」や「信頼性」を強調して契約を締結すると、説明義務違反を問われる可能性がある。

次に、注意義務については、監査人は被監査企業に対して、善管注意義務を負う。そして、情報セキュリティ監査基準は、「4.　業務上の義務」の「4.1　注意義務」の中で、「情報セキュリティ監査人は、専門職としての相当な注意をもって業務を実施しなければならない」と定める。また、同報告基準の「4.　監査報告についての責任」では、「監査報告書の記載事項については、情報セキュリティ監査人がその責任を負わなければならない」と規定する。

会計監査で虚偽証明が行われた場合、会社法や金融商品取引法によって過失の立証責任が転換されており、対被監査企業・対第三者を問わず、監査人側が無過失を証明しなければならない。裁判例は、会計監査の性質をいかに解するかによって判断を異にしているが、全体的に見れば、監査基準に従って通常実施すべき監査手続を実践すれば足りるとして、責任を限定する傾向にある。一方、情報セキュリティ監査人について、無過失責任を定める規定は存在せず、助言型監査、保証型監査を問わず、一般の民法の規律に服する。

この場合の注意義務のレベルについて、会計監査における判例の傾向を参考にすれば、監査規準に従った手順を踏むことが重要になる。しかし、情報セキュリティ監査の場合、会計監査と比して監査基準は簡略であり、企業会計基準に相当するものも存在しない。また、前記のような二重の「期待ギャップ」が懸念される以上、会計監査の議論をそのまま援用すべきではない。注意義務の内容については、より詰めた議論が必要である。

ところで、JASAは、被監査企業向けの情報の中に、情報セキュリティ監査

(50)　石田・前掲『監査論の基礎知識　五訂版』186頁。

を用いた情報セキュリティマネジメントの確立は、訴訟リスクを軽減する可能性があるという表現を用いている。しかし、それは、信頼に値する情報セキュリティ監査であることが前提でなければならない。

４.４.２．懲戒処分

公認情報セキュリティ監査人は、民間の資格であるため、行政処分は存在しない。JASAは、2004年11月４日、監査人倫理規定を制定し、情報セキュリティ監査人の職業倫理規範を設けた。その中には、監査人の基本的責務（第３条）、法令遵守（第４条）、品質管理（第７条）等の定めが置かれている。また、監査人がこの倫理規定に違反した場合、協会は、審査委員会の判定を経た上で、監査人資格の剥奪又は監査人に対する戒告を行うことができる（第10条）。

また、経済産業省は、情報セキュリティ監査企業台帳制度を設けており、ウェブ・サイトで公表している[(51)]。これは、任意登録制の台帳であり、登録要件は、①他人の求めに応じて、「情報セキュリティ管理基準」と「情報セキュリティ監査基準」に従って「情報セキュリティ監査」を行う企業又はそれを業として行う個人であること、②独立かつ専門的な立場から「情報セキュリティ監査」を行う企業であることを自己宣言していること、である。そこでは、当該企業の概要、監査実績（監査概要、監査形態）、監査従事者の概要、資格などが公表されている。2007度までの登録分は、全国で410件である。登録は毎年度行うこととし、その際には前年度の監査実績等を申告し、申告内容に虚偽があった場合等は、登録を抹消される（情報セキュリティ監査企業台帳に関する規則第７条第２項）。

ただし、JASAの倫理規定自体、抽象的な文言で構成されており、懲戒の実績も公表されていない。また、監査企業台帳は任意の制度であり、同じく登録抹消の実績は公表されていない。独占事業ではないため、懲戒や登録抹消の効

(51)　経済産業省のウェブ・サイトのうち、「情報セキュリティ監査企業台帳」のページ（http://www.meti.go.jp/policy/netsecurity/is-kansa/index.html）参照。

果は不透明である。

5．むすびにかえて

情報セキュリティ監査の分野では、NICTの政策、それを受けた経済産業省の方針によって、保証型監査が推進されており、専門資格としての公認情報セキリティ監査人制度が運用されている。しかし、情報セキュリティ監査自体、歴史が浅く、資格を取得した監査人の地位を含め、法的関係が不明確である点が多い。信頼ある制度を構築するには、多くの課題が存在する。

とりわけ、日本では、「お墨付き」の与える効果が高いことを考慮すれば、会計監査と比して監査対象の特定が容易ではない情報セキュリティ監査において、「保証型」と称する監査制度を推し進めることに対しては、慎重に考えるべきである。仮に「お墨付き」制度を推進するのであれば、監査人の独立性や独占性、専門性を十分に担保できる制度的枠組みを作るべきであり、法的制度も視野に入れる必要が生じてくる。少なくとも、信頼ある制度を構築するためには、法的責任論を詰めて議論しなければならない。

※本稿は、社会技術研究開発センター・研究開発プログラム「ユビキタス社会のガバナンス」の2006度採択課題「企業における情報セキュリティの実効性あるガバナンス制度のあり方」(研究代表者：林紘一郎情報セキュリティ大学院大学副学長)における研究成果の一環として発表するものである。