改訂されたシステム監査基準・管理基準の解説（第 105 回月例研究会報告）

No.1060　太田　香

日時：2004 年 7 月 27 日（火）　18：30 ～ 20：30
場所：中央大学駿河台記念館　280 号会議室
講師：特定非営利活動法人　日本システム監査人協会理事　本田　実　氏
演題：「改訂されたシステム監査基準・管理基準の解説

●はじめに

この講演が行われた時点ではまだ経済産業省からの発表が行われていないため、演題を「改訂された」から「改訂される」と理解して頂きたいとの説明とともに講演が開始された。講師は当協会の理事であり、また内閣府 ＣＩＯ 補佐官である本田氏である。システム監査基準検討委員会委員として改訂システム監査基準・管理基準の両ワーキンググループにてご活躍された。氏に委員会内部での検討経緯を交えながらご解説頂いた。

●講演内容

以下の項目に従って講演が行われた。

Ⅰ．前段
1. システム監査基準改訂の経緯
2. システム監査基準検討委員会の活動状況、ワーキンググループのメンバー構成

Ⅱ．主題
1. 改訂システム監査基準・管理基準の基本方針
2. 情報セキュリティ監査とシステム監査の位置づけ
3. 現行「システム監査基準」との対比
4. 改訂システム監査基準の概要と内容
5. 改訂システム管理基準の概要と内容

Ⅲ．まとめ
1. 今後の課題

～質疑応答～

Ⅰ－1. システム監査基準改訂の経緯

1985 年 1 月に当時の通産省にて「システム監査基準」が作成され、1996 年 1 月に「改訂」が行われ、現在に至っている。2000 年以降において、当協会にてシステム監査にかかわるさまざまな提言を行ってきている。

Ⅰ－2. システム監査基準検討委員会の活動状況、ワーキンググループのメンバー構成

省略（筆者記：JIPDEC のホームページ等でご参照頂きたい。）

Ⅱ－1. 改訂システム監査基準・管理基準の基本方針

以下の 5 点をシステム監査基準改定の基本方針とした。
1. 新しい技術革新への対応
2. 事業における情報システムの位置付けの変化への対応
3. 社会に対する説明責任の高まりと保証型監査の必要性
4.「情報システム管理の標準」と「監査人の行為規範」の峻別
5. 情報セキュリティ監査制度との関係明確化

また、以下の 3 点については、今回の改訂では行わないこととした。
(1)「用語の定義」は基準に入れず、別途定めることを検討する。
(2) 個別の対象システムの規模、状況等に大きく依存するものは、個別に設定されるものとし、基準では触れない。
(3) 活用範囲を広く保つため、特定の定義はしない。

Ⅱ－2. 情報セキュリティ監査とシステム監査の位置づけ

図 1 をご参照頂けるとより明確となるが、システム監査は「情報システムに対する構築・運用の全体最適化」を目的とし、情報セキュリティ監査は情報システム以外を含めた「情報資産」を範囲としている。また、判断の尺度についてはシステム監査の場合は「効率性・有効性」も尺度に含ま

れるが、情報セキュリティ監査についてはこの判断基準は適用されない。さらにシステム監査において情報セキュリティ確保の観点が必要とされる場合は「情報セキュリティ管理基準」を活用するという位置付けとしている。

Ⅱ－3. 現行「システム監査基準」との対比

大きく改訂されたのは、「システム監査基準」と「システム管理基準」の2本立てで構成したことである。これは基本方針の「4」で挙げられている通りで、「情報セキュリティ監査制度」の構成に合わせたものである。システム監査基準、システム管理基準のそれぞれの章立てについては現行の「システム監査基準」を基本的に踏襲し、そこに新たな項目を追加する形をとっている。(図2、図3を参照)

Ⅱ－4. 改訂システム監査基準の概要と内容

「一般基準」、「実施基準」、「報告基準」に先立ち「前文」と「目的」を掲げ、そこに先ほどの「基本方針」を盛り込んでいる。「前文」についてはシステム管理基準にも同様の観点のものを追加している。この「前文」についてはパブリックコメントでも意見が多く、訂正している所がある。意識して盛り込んだ内容として、内部監査部門による実施だけではなく、組織体の外部者の監査にも利用できるものとしたこと、保証型監査と助言型監査の存在を明記したなどがある。

「目的」に「リスクアセスメントに基づくコントロールの整備･運用状況」と明示することにより、リスクアセスメントの必要性を強調した。リスクの例として「目的・目標が実現できないリスク」「安全･有効・効率的に機能しないリスク」「提供する情報の信頼性が低いリスク」「関連法制度に準拠していないリスク」というものが挙げられる。システム監査はこれらのリスクのコントロールが適切に整備・運用されていることを確認するための有効な手段である。システム監査さえ行えばリスクコントロールがうまく行えるというものではないことにご注意いただきたい。

「一般基準」、「実施基準」、「報告基準」で説明を要する部分として、「監査人の独立性、客観性」についての程度はさまざまな状況が考えられるため、あえて監査基準には明記しなかった。本基準を広範囲に使えることを目指したことにより、文言の厳密性をあえて追求していない。「システム監査人は、職業倫理に従い～」という文章でも内部監査人はシステム監査を職業としているものではないが「職務上の倫理」と読み替えて理解していただくなどの点も同様である。また監査の手順の項を設け「予備調査・本調査」を挙げているが、これらは情報セキュリティ監査基準には存在しない。これは現実に実施されている状況を踏まえ、あえて残したものである。ただし、予備調査と本調査の違いを明確にすべきとの意見がある。これについては基準では定義を行わず、別途定めることを検討中である。

Ⅱ－5. 改訂システム管理基準の概要と内容

「前文」については監査基準のものと同様の観点で記述されている。特に明記する点はこの管理基準を「原則として、監査人が監査上の判断の尺度として用いるべき基準」と明示している点である。また「全体最適化」という考え方は「EA」と共通するものであり、改訂作業において意識はしたが、あえて用語として文言化はしていない。

管理基準の内容についてだが、大きな変更点は「情報戦略」が追加されたことである。この「情報戦略」のかなりの部分で前出の「全体最適化」という文言を用いている。またここで現在の情報技術の潮流(トレンド)を取り込んでいる。「企画業務」については「調達」の項目を追加、「開発業務」についてはほぼ同じ。「運用業務」については一部項目を追加し、今まで「保守業務」に位置づけられていた大規模保守については開発業務へと移動した。「共通業務」については品質管理と変更管理を追加した。また外部委託を「委託・受託」として受託の項目も追加した。

Ⅲ－1. 今後の課題

これは私見をかなり含んでいるが、経済産業省、JIPDEC、IPAとして

①システム監査基準、管理基準の説明･普及
②システム監査基準解説書の作成
③システム監査技術者試験の対応等

また、日本システム監査人協会として

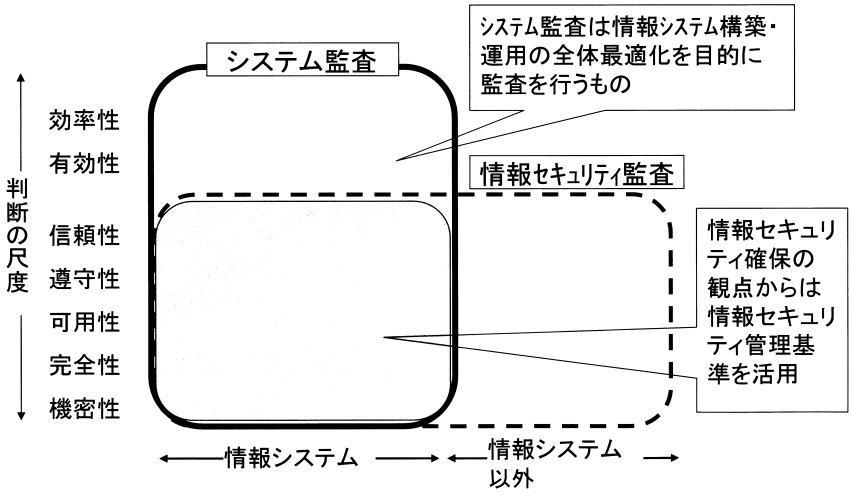
①システム監査基準、管理基準の研究、ガイドラインの作成
②情報セキュリティ監査との連携の研究、ガイドラインの作成

③システム管理基準の各項目ごとのコントロール及びサブコントロールの作成
④業種･業界ごとのシステム管理基準ガイドラインの作成
⑤システム監査事例の蓄積・公開等
以上の点の必要性が感じられる。

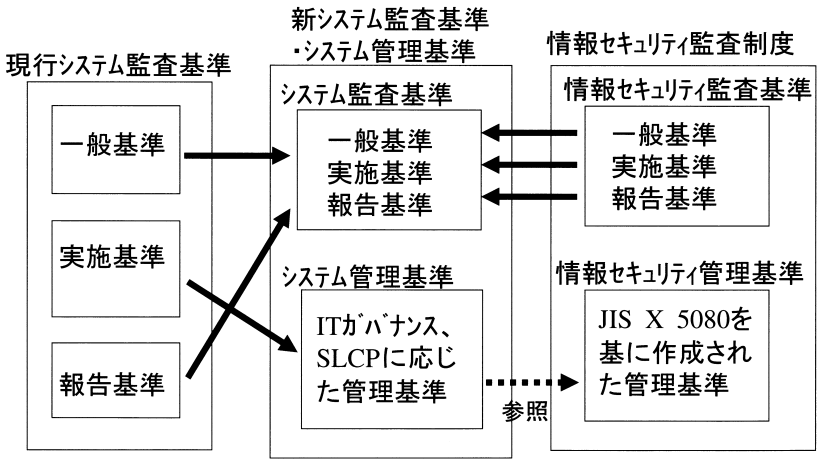
～質疑応答～
一通りご説明いただいた後で、限られた時間ではあったが質疑応答が行われた。質問内容は用語の定義やあいまいさが残るような文章への質問、また改訂の方向性に対する意見なども挙げられた。それらに対する回答の中で、用語の定義を含めなかった経緯などは詳細にご説明され、パブリックコメントにも挙げられた「IT ガバナンス」についての定義を明確化することによる範囲の矮小化への懸念、また全体に「EA」の概念を基礎として取り入れているものの「EA」そのものの用語化は避けることになったなどの説明があった。
また、デファクトスタンダードに準拠しすぎると、それらが改訂された場合には本基準も改訂せざるを得なくなるなど、日本の文化で育てられた「システム監査基準」の独立性を損なう懸念も説明されていた。
新しい概念をどこまで取り入れ、また、用語化するか、他の基準との整合性、デファクトスタンダードへの準拠程度などについての委員の方々の意見の交錯があったことも説明され、決定しづらいことについても成果物として纏め上げなければならないもどかしさも窺い知れた。

●おわりに
当日は 130 余名、会場を埋め尽くすほどの参加者があり、ただでさえ熱気の立ち込める東京都内でも場内の熱気はひとしおのものであった。
講演の端々にて、委員会、ワーキンググループ内部でもパブリックコメントへの対応に対する意見が分かれた事などをご説明され、パブリックコメントを提出した方も参加されているであろう今回の研究会でその経緯をご説明頂き、納得された方も多いのではないだろうか。
今回の研究会は IT 環境の変化の早さと可能な限り齟齬のない改訂にしようと検討を重ね続けられた委員会のメンバーの方々のご苦労が拝察される講演内容であった。

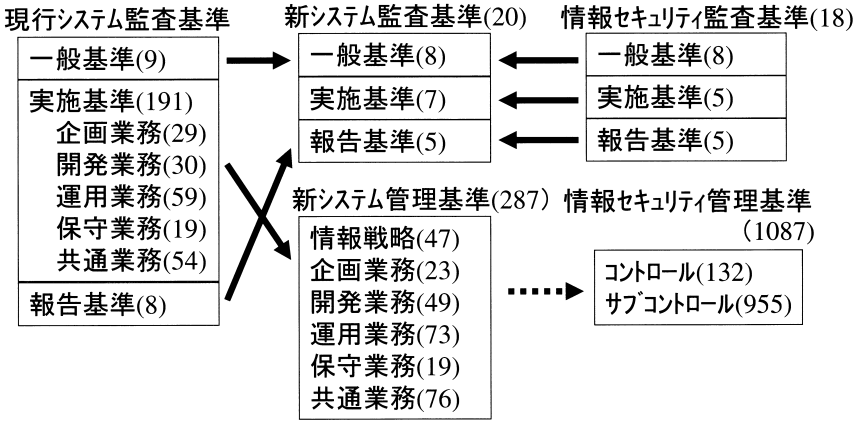
3．2 情報セキュリティ監査とシステム監査



3．3 現行システム監査基準との対比（1）



3．3 現行システム監査基準との対比（2）



（注）ｼｽﾃﾑ監査基準、管理基準の項目数は、発表予定のものである。