名古屋文理大学紀要　第2号（2002）

情報システムに関する監査基準の動向

Trends of Auditing Standards on Information Systems

吉　田　　洋
Hiroshi YOSHIDA

本稿は，代表的な情報システムに関する監査基準である，わが国の経済産業省が公表する「システム監査基準」，情報システムコントロール協会（ISACA）が公表する「情報システムに関する一般基準及び情報システム監査基準書」，国際会計士連盟（IFAC）の国際監査実務委員会（IPAC)が公表する国際監査基準(ISA)§401「コンピュータ情報システム環境下の監査」に検討を加え，その性格を明らかにした．わが国のシステム監査基準は職業的専門家集団によって認められた一定の枠組みであることを明確にする必要があることを主張した．一方，わが国のシステム監査基準は，実際の監査に対する利用を考えると有用性は高いと言える．

キーワード：監査基準，システム監査基準，情報システムに関する一般基準及び情報システム監査基準書，国際監査基準
Auditing Standards,Systems Auditing Standards,General Standards for Information Auditing and Statements on Information Systems Auditing Standards,International Standards on Auditing

1．はじめに

監査基準は,監査実務の品質を評価する尺度であり，監査の枠組みを総称したものと考えられる．さしあたり，財務諸表監査の基準であれば，「監査実務の中に慣習として発達したもののなかから，一般に公正妥当と認められたところを帰納要約した原則であって，職業的監査人は，財務諸表の監査を行うに当り，法令によって強制されなくとも，常にこれを遵守しなければならない」とされている．

これに対して情報システムに関する監査基準の比較はどのような性格を持つのであろうか．現在，情報技術に適用される主要な専門的基準については数多く存在する[注1]．わが国でも経済産業省（旧通商産業省，以下同じ）が公表するシステム監査基準の他に，金融情報センターが公表している「金融機関等のシステム監査指針」（1987年，1991年），日本公認会計士協会が公表した「EDP システムの監査基準および監査手続試案」（1976年）などがある．

そこで本稿では，代表的な情報システムに関する監査基準である，わが国の「システム監査基準」，情報システムコントロール協会（ISACA）が公表する「情報システムに関する一般基準及び情報システム監査基準書」，国際会計士連盟（IFAC）の国際監査実務委員会（IPAC)が公表している国際監査基準(ISA)§401「コンピュータ情報システム環境下の監査」に検討を加え，その性格を明らかにし，情報システム監査基準の利用

[注1] 情報技術に適用される主要な専門的基準については次に詳しい．
Frederick Gallegos,Daniel P. Manson,Sandra Allen-Senft, *Information Technology Control and Audit,* Auerbach, 1999, pp.429-495.

法について考察したい.

なお，わが国のシステム監査基準と情報システムコントロール協会のシステム監査基準は，内部監査のための基準であるのに対し，国際監査基準は財務諸表監査に関する基準であるので，本来の性格は異なるが，情報システムを監査の対象としていることから比較対象とした.

2．システム監査基準の概要

1）システム監査基準策定の経緯

システム監査は，組織体が自発的に実施する内部監査の一環として発展してきたものであり，通商産業省（現経済産業省，以下同じ）の監査関連施策を歴史的に見ると，その出発点は1951年７月の「企業における内部統制の大綱」に端を発している.通商産業省では，1985年１月，システム監査に関するガイドラインとして，「システム監査基準」を策定・公表した．これは通商産業省が1983年12月に発表した産業構造審議会情報産業部会の中間答申に基づくものである．システム監査基準では「システム監査は，コンピュータシステムの信頼性，安全性，効率性等を確保するため，監査対象から独立した監査人が一定の基準に基づいて，コンピュータシステムを総合的に点検・評価し，関係者に助言，勧告するものである」と定義付けている.

引き続き，1986年には第１回システム監査技術者試験が実施された．その後，後述する情報環境の変化，国際化，災害対策等への対応するため，1996年1月，システム監査基準を改訂し，現在に至っている．システム監査基準にかかわる通商産業省の監査関連施策は表１のようである.

表１　「通商産業省の監査関連施策」

年　月	内　　容
1951年７月	企業における内部統制の大綱
1953年２月	内部統制の実施に関する手続き要領
1983年12月	産業構造審議会情報産業部会中間答申でシステム監査基準の策定を提言
1985年１月	システム監査基準策定
1986年10月	第１回システム監査技術者試験実施
1991年３月	システム監査企業台帳制度創設
1996年１月	システム監査基準改訂

出所：通商産業省機械情報産業局監修，システム監査学会/㈶日本情報処理開発協会編『システム監査白書97-98』コンピュータエージ社，1997年，15頁.

2）旧システム監査基準の概要

「旧システム監査基準」（1985年）は，情報システム監査のためのガイドラインであって，「強制力がないこと」，「実務基準であること」が特徴となっている．したがって，指導的性格の強い基準であると考えられる．また，その構成は，システム監査の対象，監査人の要件など総括的事項を示した一般基準（13項目），システム監査の具体的な実施内容を示した実施基準（105項目）及びシステム監査の結果の取りまとめ事項を示した報告基準（９項目）から構成されている．実施基準は，企画業務，開発業務，運用業務に分けて記述されている.

システム監査基準の特徴はチェックリスト方式にある.「実施基準」については，記述方法はすべて「しているか」というチェックリスト方式で構成されている．厳密には，監査要点が示されたにすぎず，それをどのように立証するかという監査手続を規定しているものではない．また，「報告基準」については，内部報告用の監査報告書を想定しているため，監査意見の表明による情報システムの保証機能よりも，むしろ改善勧告事項とそのフォローアップに重点を置いているのが特徴である[注2].

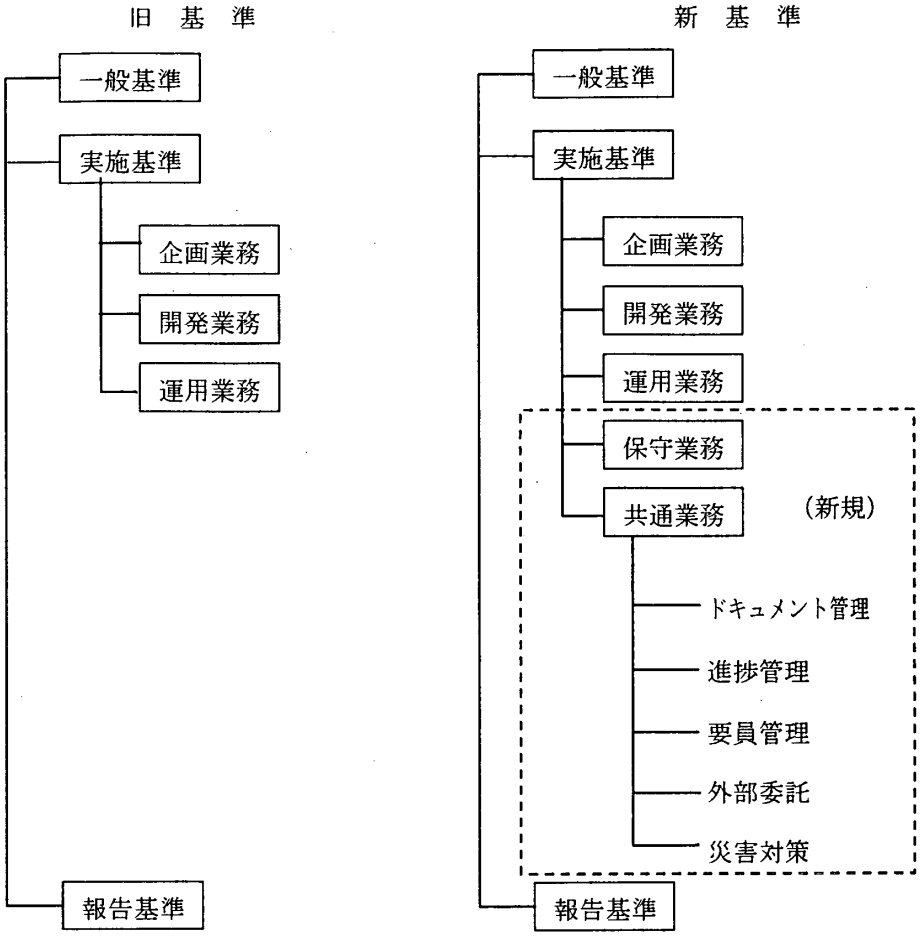
また，「システム監査基準」は，企業会計審議会の「監査基準」の構成と酷似していることも指摘できる．つまり，「システム監査基準」の構成が企業会計審議会の「監査基準」の構成（一般基準，実施基準，報告基準）と酷似しているにもかかわらず，「監査基準」との関連や「基準」の作成者である経済産業省の「情報化対策委員会システム監査部会」の部会長である宮川公男教授の書かれた部会での審議経過を読んでも，特に問題として取り上げられた様子はないことを問題点として指摘している[注3].

この点も企業会計審議会の「監査基準」と比べ，「システム監査基準」の性格を曖昧なものにしていると思われが，後述するようにスタンスや構成については今回の改訂（1996年）においても大きな変更は見られなかった.

注2 堀江正之「「システム監査基準」の制度的意味と立証構造の問題点」，山本　繁(編著)『現代会計基準と会計制度』同文舘，1993年，196～197頁.

注3 翁長良禎「システム監査に関する一考察」，『沖縄国際大学商経論集』第19巻第1号，1991年３月，1～2頁.

表２　「システム監査基準の構成」



出所：通商産業省機械情報産業局監修，システム監査学会/(財)日本情報処理開発協会編『システム監査白書97-98』コンピュータエージ社，1997年，14頁.

３）改訂システム監査基準

さて，改訂システム監査基準（1996年）では，表２のように基準の構成や性格に大きな変化が見られないが，次の点が検討されている[注4].

(1)　情報環境の変化への対応

近年のダウンサイジング化，アウトソーシング化等々の進展により，情報システムは従来のメインフレームによる集中処理システム中心から，クライアント/サーバーなどによる分散処理システムの導入へと大きく転換している点やインターネットの普及に見られるネットワークの利用・応用の多様化といった，ダイナミックな情報環境の変化に対応した.

(2)　国際化への対応

OECDが1992年に公表した「情報システムのセキュリティガイドライン」の第一の原則である「責任原則」の精神をシステム監査基準に反映させるため，システム監査人の責任・権限を明確にした.

(3)　災害対策への対応

阪神・淡路大震災を教訓として，災害対策やバックアップ対策のあり方を重視した.

(4)　他の施策との整合性

経済産業省が施策している他のセキュリティ関連基準等[注5]との整合性をとり，相互関連を明確にし，より効果を高めるようにする必要があるとした.

注4 通商産業省機械情報産業局監修，システム監査学会/（財）日本情報処理開発協会編『システム監査白書97-98』コンピュータエージ社，1997年，12～13頁.

注5 セキュリティ関連基準等とは「情報システム安全対策基準」（1977年4月策定（旧名称：電子計算機システム安全対策基準），1995年8月改訂），「コンピュータウイルス対策基準」（1990年4月策定，1995年7月改訂），「ソフトウエア管理ガイドライン」（1995年11月策定），「コンピュータ不正アクセス対策基準」（1996年8月策定）を指している.

4）新旧システム監査基準の比較

新旧のシステム監査基準を比較してみると次のような点に変化が見られる[注6].

(1) 用語の定義

新基準では，この基準で使用する主な用語の定義をしている．いままで曖昧なまま使用されていた用語の定義が定まった．

(2) 一般基準

一般基準は，システム監査において基本となる監査計画およびシステム監査人の要件等の原則を定めたものである．

改定システム監査基準では，OECDのセキュリティガイドラインの主旨を受け入れて「システム監査人の責任・権限」という項目とともに，「職業倫理」，「守秘義務」いう項目も定め，システム監査人の位置づけをより強固にしている．したがって，システム監査人の責任が重くなったといえる．

(3) 実施基準

実施基準は，システム監査の対象である情報システムの企画，開発，運用ならびに保守業務ならびに共通業務に対する監査項目を定めている．

実施基準の構成には，大きな変化が見られる．旧システム監査基準では，「企画業務」，「開発業務」，「運用業務」の3つに分類していたが，改定基準では，これらに「保守業務」をくわえ，さらに各業務に共通する内容については，「共通業務」として独立させている．

「保守業務」では，最近特に重要性を増しているシステムやプログラムの保守について触れている．

「共通業務」では，ドキュメント管理，進捗管理，要員管理，外部委託，災害対策が取り上げられている．旧システム監査基準では，企画，開発，運用業務といった情報システムの業務の流れに沿って策定されていたが，情報システム全体等を対象とする項目に欠落があった．これは情報システムの内部統制で言うところの全般統制であるといえる[注7].

(4) 報告基準

報告基準は，システム監査の結果の取りまとめるにあたっての必要事項および結果に基づく措置を定めている．

報告基準に関しては，内容的な変更はないが旧システム監査基準に比べ整理されている．

5）基準の関連性

セキュリティ関連，コンピュータウイルス対策，ソフトウェアの利用状況については他に基準があり，相互に関連性を持たせている．したがって，システム監査を実施する場合は，システム監査基準のみならず，他の基準やガイドラインを活用することが必要である．

(1) セキュリティ関連

物理的セキュリティなど，セキュリティに関する項目は「情報システム安全対策基準」を活用することを定めている．

(2) コンピュータウイルス対策

コンピュータ対策基準の監査については「コンピュータウイルス対策基準」を活用することを定めている．

(3) ソフトウェアの利用状況

ソフトウェアの利用状況の監査については「ソフトウェア管理ガイドライン」を活用することを定めている．

3．ISACAの情報システム監査基準

情報システムコントロール協会(ISACA)では，1985年から基準審議会を設置し，情報システム監査人の業務を支援するための基準の作成に着手した．1987年に「情報システム監査に関する一般基準」が公表され，その後改訂がくり返されている．あわせて，「情報システム監査に関する一般基準」に関係する情報システム監査実務のさまざまな問題を解決するために「情報システム監査基準書」が公表されている[注8].

1）情報システム監査における一般基準

最新の監査基準は，1997年に公表されたものであって，すべての情報システム監査に適用される．

その序文では，次のように述べられている．

「情報システムコントロール協会は，情報システム監査業務の特別な性質，監査を実施するのに必要な技能から，情報システム監査に適用される一般基準を制定し，公表する必要があると判断した．」

さらに，「情報システム監査は，関連する自動化されていない処理，及びそれらとのインターフェイスを含む，自動化された情報処理システムのすべての局面(ま

注6 通商産業省機械情報産業局監修，システム監査学会/(財)日本情報処理開発協会編，前掲書，13～15頁.

注7 情報システムの内部統制に関しては次が詳しい．宇佐美　博，吉田　洋「情報システムの内部統制に関する研究」，『経営総合科学』第74号，愛知大学経営総合科学研究所，2000年2月，51~97頁.

注8 Ron Weber, *Information Systems Control and Audit,* Prentice-Hall, 1999, pp.985-987.

たはその一部分）について調査し，評価する監査」と定義する．

情報システムコントロール協会が公表した情報システム監査基準は，情報システムコントロール協会の会員及び公認情報システム監査人（ＣＩＳＡ）の資格保持者が行う情報システム監査業務に適用される．

つまり，情報システム監査業務は会計監査とは異なる特別な性質を有する監査であって，自動化される，されないに係わらず情報システムのすべての局面を監査対象とする．そして，協会の会員やCISAの資格保持者の情報システム監査業務に適用される基準なのである．

この基準の全文を示せば次のようである．

情報システム監査における一般基準

010 監査規程

010.010 職責，権限及び報告説明義務

情報システム監査の機能の職責及び権限並びに報告説明義務は，監査規程または契約書に，適切に文書化されなければならない．

020 独立性

020.010 専門家としての独立性

監査に関連するすべての事柄について，情報システム監査人は，態度及び外観において監査対象から独立していなければならない．

020.020 組織的関係

情報システム監査の機能は，監査を客観的に遂行するために，監査対象領域から十分に独立していなければならない．

030 専門職の倫理と基準

030.010 職業倫理規程

情報システム監査人は，情報システムコントロール協会の定める職業倫理規程を遵守しなければならない．

030.020 専門家としての注意義務

適用される監査基準の遵守を含め，情報システム監査人のすべての業務において，情報システム監査人は，専門家としての注意を払わなければならない．

040 能力

040.010 技能及び知識

情報システム監査人は，技術的に有能であり，監査人の業務を実施するのに必要な技能及び知識を保有していなければならない．

040.020 専門家としての継続教育

情報システム監査人は，適切な継続教育により，技術的能力を保持しなければならない．

050 計画

050.010 監査計画

情報システム監査人は，情報システム監査業務を計画して，監査目的を記述し，適用される監査基準を遵守しなければならない．

060 監査の実施

060.010 監督

情報システム監査の要員は，監査の目的が達成され，適用される監査基準に適合することを保証するために，適切に監督されなければならない．

060.020 証拠

監査の実施にあたって，情報システム監査人は，十分に信頼性があり，関連した，有用な証拠を入手し，効果的に監査目的を達成しなければならない．この証拠を適切に分析し，解釈して，監査発見事項及び結論の根拠としなければならない．

070 報告

070.010 報告書の内容と形式

情報システム監査人は，監査業務の終了後，報告書の受領者に適切な形式の報告書を提出しなければならない．監査報告書には，範囲及び目的，対象期間，並びに実施した監査業務の性質と範囲について，述べられなければならない．監査報告書には，組織名及び受領者，並びにあらゆる制約が明らかにされていなければならない．監査報告書には，発見事項，結論及び勧告，並びに当該監査に関する留保及び限定事項について述べられなければならない．

080 フォローアップ作業

080.010

情報システム監査人は，前回の関連する発見事項及び結論，並びに勧告に関して，適切な情報を要求して，これを評価し，適切な措置が適時に実施されたかどうか判断しなければならない．

2）情報システム監査基準書

情報システム監査基準とその各項目の概要を述べれば次のようである．

1.独立性：態度及び外観；組織的関係

情報システム監査人は，監査にあたって独立した態度を保持しなければならない(No.1,03)．監査人は，監査対象から組織上独立していなければならない(No.1,06)．

2.独立性：システム開発プロセスへの関与

コントロールの設計及び導入を含む，アプリケーションシステムの開発において，プロジェクトチームは，定められたシステム開発プロセスを適用する責任がある．監査人は，プロジェクトチームから独立していなければならない．監査人は，独立した立場でアプリケーション開発レビューの実施に適用する手続を決定しなければならない．監査人は，自らの独立性を損なわず，コントロールおよびその他のシステムの強化策を勧告できる(No.2,08)．監査人が，プロジェクトチームの一員として監査ツールや監査技法の設計及び導入に関与したとしても，監査人の独立性を損なうことにはならない(No.2,11)．

3.監査の実施：証拠の要件

情報システム監査人は，監査の実施過程において監査証拠を収集する．監査証拠は，適切でかつ信頼性のあるものでなければならない(No.3,03)．監査人が収集した証拠は，監査人の発見事項および結論を裏付けるように適正に文書化して整理しておかなければならない(No.3,09)．

4.監査の実施：専門家としての注意義務

専門家としての注意義務は，その専門分野の実務家が通常保有しているとされる水準の技能を行使することを要求する(No.4,03)．

5.監査の実施：監査計画におけるリスクの評価の適用

情報システム監査人は，基本監査計画の策定及び個別監査計画において，リスク評価技法を適用すべきである(No.5,07)．監査人は，個別の監査に当たって適用したリスク評価技法あるいは方法を監査調書に記録しておかなければならない(No.5,08)．

6.監査の実施：監査調書

情報システム監査の監査調書は，実施した監査作業の記録であり，監査人の発見事項及び結論を裏付ける証拠である(No.6,03)．監査調書には，少なくとも，監査範囲と監査目的に関する計画と準備，監査手続書，実施した監査手順と収集した証拠，監査の発見事項，結論および改善勧告，監査の結果発行されたすべての報告書，改善勧告についての被監査側の対応が記録されなければならない(No.6,04)．

7.報告：監査報告書

報告書は，監査目的，適用した監査基準，監査範囲，発見事項，および結論を報告するための正式な手段である(No.7,03)．報告書の形式は，論理的かつ体系化されていなければならない(No.7,09)．報告書には監査対象を明確にし，かつ発行日を明示しなければならない(No.7,11)．

8.監査の実施：不正行為に関する監査考慮事項

情報システム監査人は，監査対象領域における不正行為の発生するリスクを考慮しなければならない(No.8,05)．監査人は，このリスクの評価に基づき，組織や監査対象に対して重大な影響を与える可能性のある不正行為を合理的に発見し得るような監査を計画し，実施する責任を負う(No.8,06)．監査人の不正行為を発見した場合，それらの行為が監査目的や収集した監査証拠の信頼度にどのような影響を与えるかを評価しなければならない(No.8,9)．発見された不正行為は，組織の適切な責任者に遅滞なく報告しなければならない(No.8,10)．

9.監査の実施：監査ソフトウェア・ツールの使用

監査人は，監査ソフトウェア・ツールのインティグリティと有用性に関する合理的な保証を得るために，監査ソフトウェア・ツールを適切に計画し，設計し，テストし，ドキュメンテーションをレビューしなければならない(No.9,04)．監査ソフトウェア・ツールを使用して本番データにアクセスする場合，監査人は，情報システム及びデータのインティグリティを保護するために適切な手順をふまなければならない(No.9,05)．

4．国際監査基準

1）EDPに対する監査の国際的ガイドラインの対応

国際会計士連盟は，1977年各国の会計士団体の合意によって創設された．その下部機関である国際監査実務委員会(International Auditing Practices Committee:IAPC)により，1980年代を通じて「監査の国際的ガイドライン」(International Auditing Guidelines:IAG)が公表された．

ＥＤＰ環境下の監査に関連して，IAPC の作業部会は３つの監査の国際的ガイドラインを次のように公表した．

- IAG-15「ＥＤＰ環境下の監査」(1984年2月発行)
- IAG-16「コンピュータ利用監査技法」(1984年10月発行)
- IAG-20「ＥＤＰ環境が会計組織および関連する内部統制の検討と評価に及ぼす影響」(1987年10月発行)

さらに IAG-20を補足する監査の国際的ステートメントを次のように公表している．

- IAG-20補足第１号「EDP 環境-スタンド・アロンのマイクロコンピュータ」

・IAG-20補足第２号「EDP 環境-オンライン・コンピュータ・システム」
・IAG-20補足第３号「EDP 環境-データベース・システム」

これは，ＥＤＰシステムにより処理されている会計情報の正確性，信頼性を会計士が監査する場合を想定したものである．

2）CIS に対する国際監査基準の対応

IAPC では，各国の監査基準の統一性を高めるために，1994年，監査の国際的ガイドラインの呼称を国際監査基準に変更し，公表した．国際監査基準では，§401「コンピュータ情報システム環境下の監査」(Auditing in a CIS(Computer Information Systems) Environment)（以下，§401とする）において情報システムの監査問題が触れられている．

一連の EDP 監査に関する「監査の国際的ガイドライン」と比較して，技術的な内容よりも監査人にとっての行為の指針が明確に記述されていることは評価に値する．

このISAの主旨は，監査がコンピュータ情報システム(CIS)環境下で遂行される際に適用されるべき手続に関する基準を確立し，指針を提供することであるとされている(para.1)．

技術的進展の観点から見れば，組織体は電子的な情報の開発，蓄積，交換に関して新しい技術に個別に対応している．そこで，監査のプロフェッションを支援するために，監査基準委員会はＣＩＳ問題を扱うため一連の監査基準を今後，公表したのである．§401は，「主旨」，「技術と能力」，「計画」，「リスク評価」，「監査手続」から構成されており，基本原則や必要不可欠な手続を識別したブラック・レタリング（大文字の字体）を中心にその内容を概観すれば次のようになる[注9]．

(1) 主旨

ＣＩＳ環境では，監査にとって重要な事業体の財務情報が何らかの種類や規模のコンピュータで処理され，それは事業体や第三者による運営もあることをいう（para.1）．**監査人はＣＩＳ環境が監査にいかに影響を与えるかを考えるべきである**（para.2）．監査の目的はＣＩＳ環境でも変わらないが，コンピュータの利用は財務情報の処理，蓄積，伝達を変化させ，事業体で用いられる会計・内部統制に影響する．したがって，ＣＩＳの影響は会計・内部統制の把握の手続，固有リスクと統制リスクの考察，統制テストと実証性手続の立案と実行に影響を与える(para.3)．

(2) 技術と能力

監査人は実施される業務を計画し，指揮し，監督し，レビューするためにＣＩＳに関する十分な知識を持つべきである．監査人は特別なＣＩＳ技術が監査で必要かどうかを検討すべきである．もし特別な技術を必要とする場合，専門家の助言を仰ぐべきである．**かかる専門家の利用を計画するのであれば，監査人はISA620「専門家の業務の活用」に準拠しながら，その業務が監査目的上，適切であるとの十分かつ妥当な監査証拠を得るべきである**（para.4）．

(3) 計画

ISA400「リスク評価と内部統制」に準拠し，監査人は監査を計画し，効果的な監査アプローチを展開するために会計・内部統制組織を十分に把握すべきである(para.5)．**依頼人のＣＩＳ環境により影響されるかもしれない監査の部分を計画するにあたっては，監査人はＣＩＳ活動の重要性や複雑性と監査で用いられるデータの入手可能性を把握すべきである**（para.6）．**ＣＩＳが重要な場合，監査人はＣＩＳ環境と，それが固有のリスクならびに統制リスクの評価に影響を及ぼすべきか否かを把握すべきである．**その際の，リスクの性質，内部統制の性格は以下から影響を受ける．

監査証跡の欠如，取引の統一的処理，職務の分離の欠如，人間の誤謬（ごびゅう）や不正の潜在性，取引の開始と実行が承認なしで自動的に行われること，手記で行われる統制手続の有効性自体がコンピュータ処理の完全性や正確性に依存すること，経営者の監督機能を高められること，コンピュータ支援監査技法の利用の可能性（para.7）．

(4) リスク評価

監査人は ISA400「リスク評価と内部統制」に準拠し，重要な財務諸表の主張に対して固有リスクと統制リスクの評価を行うべきである（para.8）．ＣＩＳ環境下における固有リスクと統制リスクは重大な誤表示の蓋然性に全体的かつ個別勘定ごとの両方で影響を与える．（para.9）．新しいＣＩＳ技術はＣＩＳ全体の精巧化と複雑性をもたらし，その結果リスクが増大し，さらなる検討を必要とする（para.12）．

(5) 監査手続

監査人は ISA400「リスク評価と内部統制」に準拠して監査リスクを受容可能な程度の水準に下げるために監査手続の立案に際し，ＣＩＳ環境を検討すべきである(para.11)．監査目的は変わらないが監査手続はコン

注9 日本監査研究学会国際監査基準委員会編『国際監査基準』第一法規，1996年，179～180頁．

ピュータ処理により影響を受ける(para.12).

3) 国際的情報技術のガイドライン

IFAC の情報技術委員会(Information Technology Committe)では，国際的情報技術のガイドライン(International Information Technology Guidelines)として「情報セキュリティの管理」(Managing Security of Information)と「ビジネスインパクトに関する情報計画の管理」(Managing Information Planning for Business Impact)などを公表している.

5. 情報システムに関する監査基準の比較と利用法

(1) 情報システムに関する監査基準の比較

わが国の「システム監査基準」は，ガイドラインとされているように指導的性格が強い．表3「情報システムに関する監査基準の比較」に見られるように，この基準は，システム監査の主体として，内部監査人および外部の職業的専門家によるシステム監査を想定した包括的かつ一般的な基準であって，必ずしも専門家集団の基準であることを明確に謳いあげているわけではない．これはシステム監査を実施する排他的特権を認める資格は現状では存在しないため，基本的には誰でもシステム監査を実施することは可能であることに起因するかもしれない.

しかし，このことは米国でも同様な状況であるにも関わらず，情報システムの監査とコントロールを専門家集団である ISACA の情報システム監査基準は，ISACAの会員及びCISAに適用される基準であると明確に謳いあげている．国際監査基準では公認会計士が行う財務諸表監査がコンピュータ情報システム(CIS)環境下で遂行される際に適用されるべき手続に関する基準を確立し，指針を提供している．いずれも社会的規範性が強い基準といえる.

監査基準とはその監査に関係する専門家集団によって認められた一定の枠組みであり，監査人にとっての行為の指針であって，責任基準である[注10].

たとえば，監査報告書に公認情報システム監査人が「ISACA 監査基準に準拠して監査を実施した旨」あるいは公認会計士が「国際監査基準に準拠して監査を実施した旨」を記載すれば，それは専門家集団が認めた一定水準以上の監査が実施されたことを意味すると考えられる．このように考えた場合，システム監査基準がガイドラインであることには非常に問題がある.

記述方法については，「システム監査基準」がチェックリスト方式で，他は条文方式である．後述するがチェックリスト方式であれば実際の監査への利用価値は高い.

構成については，「システム監査基準」と「情報システムに関する一般基準及び情報システム監査基準書」はほぼ変わらない．すなわち，「システム監査基準」の「一般基準」部分が「情報システムに関する一般基準」に該当し，「システム監査基準」の「実施基準」，「報告基準」部分が「情報システム監査基準書」に該当する．§401については国際監査基準の一部であるので，単純に比較することはできないが，「主旨」，「技術と能力」部分が「システム監査基準」や「情報システムに関する一般基準及び情報システム監査基準書」の「一般基準」に該当し，「計画」，「リスク評価」，「監査手続」部分が「実施基準」や「情報システム監査基準書」に該当する．なお，§401には報告基準に該当する項目はない.

焦点については，いずれもコンピュータシステムや情報システムに焦点を当てている.

他の基準やガイドラインについては，いずれも基準をサポートする他の基準やガイドラン等が存在する.

(2) 情報システムに関する監査基準の利用法

まず，システム監査規程への活用である．システム監査規程はシステム監査を制度化したことを宣言するものである．したがって，システム監査を制度化し，実施する前に必ずシステム監査規程を作成しておかなければならない．すでに，財団法人日本情報処理開発協会では，システム監査規程（モデル）を公表しているので，大いに参考になる．さらに「システム監査基準」の一般基準と報告基準を参考に作成するとともに，各監査項目については，実施基準に組織体の実態を反映して作成できる[注11]．また，ISACA の「情報システム監査に関する一般基準及び情報システム監査基準書」は全般にわたりシステム監査規程作成に際し，大いに参考になる.

注10 ISACA 東京支部システム監査研究会『「ISACA システム監査基準」の研究』ISACA 東京支部，1997年，はじめの部分.

注11 日本セキュリティ・マネジメント学会編『セキュリティハンドブック　情報セキュリティとシステム監査Ⅱ』日科技連出版社，1998年，155頁.

次にシステム監査手続書への利用である．監査手続とは一般に，監査人が証拠を収集したり評定したりする手続をいう．つまり監査手続書では詳細かつ具体的な監査活動を記述するものであるから，「システム監査基準」を参考に監査項目，監査対象部門，監査の着眼点，リスク，コントロールの識別，チェックポイント，関連資料などを記載した手続書を作成することも考えられる．例えば，財団法人金融情報システムセンターが公表している「金融機関等のシステム監査指針」（1987年公表，2000年改訂）などはよい例かもしれない．さらには，ISACA が公表している COBIT，IFAC が公表している国際情報技術ガイドラインなども監査手続だけでなく，システム管理規程やシステム監査人の評価基準（価値判断）にも利用できるだろう．

6．むすび

システム監査基準が単なるガイドラインでよいのかどうかは今後の議論が待たれるところである．わが国のシステム監査基準は必ずしも専門家集団の基準であることを明確に謳いあげているわけではない．システム監査基準が国家機関から公表されようが，民間団体から公表されようが，職業的専門家集団によって認められた一定の枠組みであることを明確にする必要がある．

基準のチェックリスト化はシステム監査規程への活用やシステム監査手続書への利用には役立つかもしれない．しかし，監査基準である限り，システム監査において，一般基準をシステム監査の事前準備に関する要件として位置付けるのではなく，監査人にとっての行為の指針がまず明確化されるべきである．その点では，ISACA の情報システム監査における一般基準は，その意味からすれば利にかなったものといえるだろう．

逆に，システム監査基準の実際の監査に対する利用を考えると，システム監査人は，特定の監査目的に応じ，システム監査基準のなかから適当な項目を取捨選択し，監査手続に応用できることから有用性は高いといえる．

表３「情報システムに関する監査基準の比較」

１．公表団体	経済産業省	情報システムコントロール協会（ISACA）	国際会計士連盟
２．名称	システム監査基準	「情報システム監査に関する一般基準及び情報システム監査基準書」	国際監査基準 §401「コンピュータ情報システム環境下の監査」
３．公表年	１９８５年，１９９６年	１９９4年	１９８４年，１９９４年
４．主な利用者	内部監査人，外部のコンサルタント，システム監査技術者	情報システム監査人 ISACAの会員	公認会計士
５．記述方法	チェックリスト方式	条文方式	条文方式
６．構成	「一般基準」，「実施基準」，「報告基準」	「情報システム監査に関する一般基準」，「情報システム監査基準書」	「主旨」，「技術と能力」，「計画」，「リスク評価」，「監査手続」
７．焦点	コンピュータシステム	情報システム	CIS環境下の財務諸表監査
８．他の基準，ガイドライン	「情報システム安全対策基準」 「コンピュータウイルス対策基準」 「ソフトウェア管理ガイドライン」	「コントロールオブジェクティブ」 「COBIT」	国際的情報技術のガイドライン 「情報セキュリティの管理」 「ビジネスインパクトに関する情報計画の管理」