報　告

パネル討論会
システム監査
昭和57年後期第25回全国大会†報告

パネリスト
上園　忠弘[1]，岸　紅児[2]，行武　郁博[3]
平田　正敏[4]，湯野　勉[5]，**司会**　山本　欣子[6]

システム監査のある側面

山本　欣子

1. その発想

コンピュータシステムが正当にかつ有効にその目的を果たしているか否かということをなんらかの形で私的・公的に評価しようという考え方は，すでに10数年以前から存在していた．米国で生れたこの発想は，当初は例えばコンピュータを利用した選挙システムというようなものが，不正なく正当に運用されているか否かを客観的に監視評価する，あるいは軍事システムにおいて安全かつ正確にコンピュータシステムが動作し得るか否かを厳重にチェックするなどの，社会的あるいは非常にクリティカルなシステムに対する監視機能という立場からの1つのアプローチがまずあったと思う．

一方，従来から法的に定められている会計監査あるいは監査役制度の立場からも，ここ10数年来，急速に浸透してきたコンピュータの影響を無視しては，本来の監査目的自体がもはや達成できぬという環境の変化によって，従来の監査業務の拡張としてコンピュータシステム監査の機能を包含せざるを得なくなったという第2のアプローチも存在する．

2. 定義の試みと枠組

今日“システム監査”(EDP システム監査の意)という言葉自体はかなりポピュラなものとなった．しかしその具体的実践という面からはまだまだ社会に定着したとは言えない．ただわが国においてもここ数年来，幾つかの啓蒙的活動が行われてきた．その1つとしてJIPDECが数年間の検討結果にもとづき，企業内システムに対する“システム監査基準”の試案を昭和55年に作成し，1つの定義付けをおこなった．ここではシステム監査の意義・目的を

“システム監査とは，監査対象から独立した客観的な立場で，コンピュータを中心とする情報処理システムを総合的に点検・評価し，関係者に助言・勧告することをいい，システムの有効利用の促進と弊害の除去とを同時に追求して，システムの健全化をはかるものである”

と定義付け，加えて監査の対象，監査人の職務権限・立場，監査体制などにつき基本的な明文化を試みている．

この基準試案およびその他の活動の成果を総合すると，企業内システム監査の枠組はある程度明確になり，その要点は以下の通りである．

(1)　システム監査の視点は，
①EDP システムの有効性・採算性
②EDP システムの信頼性
③コンピュータの悪用，機密漏洩等に対する安全性
の3点である．

(2)　システム監査の対象は，システムの企画・開発・運用のすべてにわたる．

(3)　システム監査人は監査対象，例えば EDP 部門とは独立した立場でなければならず，客観的な評価を行わねばならない．

(4)　システム監査人は，システムの設計・開発の経験があり，ハードウェア，ソフトウェア，システム分析，プログラミングなどに関し十分な知識を持つとともに，監査についての専門知識と実務経験とを持たねばならない．

(5)　監査結果にもとづく改善勧告を，被監査部門は十分検討し，それに対する改善結果をシステム監査人

† 日時　昭和57年10月19日，15：00～17：00
場所　九州大学
1) 日本アイ・ビー・エム(株)，2) 東陶機器(株)，3) 福岡銀行，4) 西南学院大，5) 電電公社，6) (財)日本情報処理開発協会

に回答しなければならない.

3. あるデータ

現在，わが国には企業内の監査制度に3つのレベルがあり，そのうち監査役制度，公認会計士監査制度の2つは法的にその実施が義務付けられているが，システム監査はまだ各企業の自主性にゆだねられている.

やや古いデータではあるが，昭和54年にわが国の主要大手企業約400社を対象としたアンケートによると，なんらかの形でシステム監査を実施している企業はそのうちの28%であった．またそのうち公認会計士によるもののみを除くと，本来の意味でのシステム監査の実施企業は18%に過ぎない．その後3年間に，どの程度これが改善されたかを調べてみる必要があると思うが，米国では5年前に大企業の78%がシステム監査を実施中であるというデータと比較すると，恐らく現在でも日米間の差は大きいものと想像される.

一方同じく上記のデータでわが国で行われている監査の対象としては，システムの信頼性に対し，75%の企業が監査を実施しており，次いで安全性に対し50%，採算性あるいは有効性に対しては20%と最も少ない.

4. その重要性

今さらシステム監査の重要性を云々する必要はないかも知れないが，特にセキュリティの観点から，以下の3点に留意したい.

第1はコンピュータの持つブラックボックス性である．コンピュータ社会といわれるものの理想は，人々がコンピュータ自身の存在を無視し得る状態となることであろう．すなわちこれはそのブラックボックス性を100%容認し得る状態と言える．しかしながら現状はこの理想には程遠い．システム監査の役割の1つは，この理想に可能な限り近づくため，ハードウェア，ソフトウェアを含めたシステムのベリフィケーションを行うことにある.

第2はコンピュータの脆弱性の影響を可能な限り軽減する役目を果たすということである．極度に精密化・複雑化した装置の複合体の上に，さらに繊細な網の目のごときソフトウェアがからまった今日のコンピュータシステムは，物理的にも論理的にも極めて脆弱であると言わざるを得ない．折しもコンピュータセキュリティへの世間の関心が高まり，この脆弱性がシステム監査によって可能な限りカバーされ得ることへの期待は大きい.

第3は今後の社会的システム増大への対処である．現在コンピュータは社会のあらゆる分野に浸透し，人間の社会生活全般に対するコンピュータへの依存度は今後ますます増大する．これは言うまでもなく，コンピュータシステムの健全性なしにはもはや人間生活の基盤が保てぬことを意味する.

以上いずれの面からみても，システム監査は少なくとも現在の巨大なリスクを負ったコンピュータ化社会に住むすべての人間に対する精神安定剤的役割を，まず果たしてくれねばならない.

5. 解決すべき問題点

システム監査を効果ある形で実現することは言うべくして極めてむずかしい．少なくとも現時点では以下のような問題点をとりあえず指摘できるであろう.

（1） 現在のコンピュータシステムは監査性(Auditability)が極めて乏しい．例えばソフトウェアに関して言えば，現在の技術ではそのソースコードレベルはもちろんのこと，スペックレベルに関してさえも，その正当性を検証することが困難である.

（2） 監査ツールの不足

現在までに幾つかの監査ツールと呼ばれるものが開発され，一部で利用されてもいる．しかし決して満足できる状態とは言えない．特に近年大幅に普及しているオンラインシステムに対処し得るものはほとんど皆無と言ってよい.

（3） 技術革新への追従が困難

コンピュータ技術は日進月歩である．システム監査はその技術変化にタイミングよく追従してゆかねばならない.

（4） 監査人の不足

前述のごとくシステム監査人の資格はきわめて厳しい．少なくとも現状では有資格者の絶対数はかなり限定される．もちろん教育の問題もあるが，恐らく今後はなんらかの公的資格制度がとり入れられる必要があろう.

以上簡単にシステム監査のある側面からのアウトラインを述べた．コンピュータ社会におけるシステム監査の位置付けは現在その軽重に対する個人差が大きいようだ．しかしコンピュータ技術に携わる人間に課せられた社会的責任は，まず健全に機能するコンピュータシステムを世の中に提供することであろう．そしてシステム監査はその証しを客観的に行う手段であると言えよう.

システム監査の手法とツール

上園　忠弘

1. システム監査の視点

システム監査担当者（以下監査人）が実施しようとする点検・評価の項目は，

（1）　システムの完全性（Integrity）の評価

（2）　システムの予防力（Protectability）の検証

（3）　システムの復元性（Recoverability）の査定

（4）　システムの効率性（Effectiveness）の評価

の4つに分類することができる．

これらを「視る」ことができるためには，監査人は次のような能力を具備したいと望むことであろう．

（1）　データの検索と分析

所要のデータの選択（例えば高額取引の抽出）の能力とある程度の四則演算/統計計算の能力．

（2）　トランザクションの追跡

各トランザクションがシステム内を流れて行く径路を追及できる機能．

（3）　システムの諸機能の検査

リアルタイム処理を含めて，コンピュータ処理がシステム仕様に合致していて信頼でき，繰り返し可能かどうか，悪用の入りこむ余地はないかを視る．

（4）　アクセス・コントロールの能力の評価

データ，プログラム，コマンドなどが変更，破壊あるいは改ざんされる危険性に対する対策を視る．

（5）　原始入力の正確性の確認

データの正確度，エラーの検知能力を評価し，逆に検知できないエラーがないかを視る．

（6）　文書類の検証

システム文書（例えばフローチャートやプログラム・コーディング・シート）の正確性と適切な保管の有無を検査する．

2. 監査のツール

さきに述べたような6項目の能力を具体化するものが監査のツールであるが，現在のところそれらをすべて具備したオールインワンの道具は存在しない．目的ごとに種々使いわける必要があるのが実情である．

極めて大まかに言うなら，システム監査のためにコンピュータを利用する方法としない方法とに分けられるであろう．

コンピュータを利用しないで EDP システムの監査を行うには，現場部門でのインタビュウの実施や，チェックリストあるいは質問書を使うなど旧来の手法が使われる．

一方コンピュータを用いる方法では，大なり小なりそのためのプログラムが要求される．

コンピュータの安全や効率を監査するために，コンピュータを用いるのでは自己矛盾を起こしそうであるが，監査用プログラムを，その他のソフトウェアと独立にすることによって解決することができる．

監査用プログラムは次の4種類に分類できる．

（1）　汎用監査プログラム

会計事務所あるいはソフトウェアハウスが作成販売あるいは自己の業務用に用いるもの．

（2）　汎用ユーティリティ・プログラムの流用

コンピュータ・メーカあるいはソフトウェアハウスが提供するプログラムで，例えばソート，マージ，挿入，削除等のユーティリティ・プログラム．

（3）　テーラード・プログラム（1）

被監査部門（主としてコンピュータ部門）が監査人のために作成するプログラム．

（4）　テーラード・プログラム（2）

監査人自身が，または監査人が仕様を設定して，作成するプログラム．

汎用監査プログラムは，その性質上バッチ・モードで働くものが大部分で，リアルタイム的に監査人が望む時点でデータを取出すというわけにはいかない．また特定のコンピュータを想定して仕様が設定されているため，必ずしもどのコンピュータにも使えるとは限らない．このような短所はあるものの，レディメードのプログラムを利用できる便利さがあることは否定できず，かなり多くの本数のプログラムが販売されている．価格は1回の使用料が数万円，買取で数百万円（米国で1万～2万ドル）といったところである．これらのプログラムが共通に備えている機能は，データの選択/抽出，分類，四則演算，サマリ，テスト・データ生成，レポート作成などで，これらにより監査人は目指すフィルムから所要のデータを抽出し，分析を行ってその結果を作表することができるのである．

次に，ユーティリティ・プログラムは，監査人が所要のデータを取出し評価/分析を行うために利用するもので，補助的な役割を果すものである．

（3）と（4）のプログラムは，いわば自家製の監査プログラムで，自分のシステムにフィットするように設計できるし，リアルタイム的な監査プログラムも作成できる．例えば50万円を越える取引はすべて監査の対象とするのが内部規程であるとすれば，そのトラン

ザクションがシステムに入力されると同時に，監査用データ・ファイルに記録が行われるようなサブルーティンを組込んでおくというようなことが考えられる．これにより監査人は望むときに監査ジョブを始動させることも可能になる．

この形のプログラムを実用化して使っているケースはまだそれほど多くはない．それはなにを監査するかについて必ずしも企業体内で明確な結論が出ていないためにプログラム化しづらいことと，費用対効果の点で——システム設計の原点まで戻る必要がある——そこまですることに踏み切れていないためと思われる．

3. 将来の動向

数年前からコンピュータ・システムの設計基準として RASIS という言葉が時折使われている．最後の2字は Integrity と Security の略である．さらにこれに，Auditability を加えて RASISA という6つの要素を提供することが，システムの提供者の責任であると考えられるようになるかも知れない．ここに Auditability とは「データの妥当性を検証するとともにデータ処理の結果の正確性と完全性を検証するに必要な機能および性能」(SAC レポート*) と定義される．これは RASIS の基準が確保されているかどうかの検証を，システム自身にビルトインされた能力によって行わせようとするものである．

このようなビルトイン・ファンクションが有効であるかどうかは，個々の適用業務にそれらの機能が活用されるかどうかによって決まってくる．その意味では，将来適用業務のシステム設計の時点で監査をどうするか考えることが必須事項になってくるであろう．また適用業務システムに対して，監査人が設計の時点から意見を述べる機会を持つ必要があろう．

それと同時に監査証跡を記録するメディアの検討もなされねばならない．例えば現在のところ更新が不可能であることが欠点とされているレーザ・ディスクも，かえってその性質のゆえに監査証跡用メディアとして有効であると言えるかもしれない．

なお今後の技術課題として，OA，分散処理，通信回線の自由化という互いにからみ合いながら発展しつつある3つの方向へのシステム監査の対応という問題があるが，ここでは時間の都合上問題の指摘のみに止めておきたい．

---

* SAC レポート：Systems Auditability Control アメリカ内部監査協会のシステム監査に関するレポート．

製造・販売業におけるシステム監査の現状について

岸 紅児

企業における監査は従来より財務会計を主体とする会計監査・業務内容に及ぶ内部監査とがあり，われわれの属する製造・販売業では商法・有価証券取引法・納税のための税法等，主として法律の定めに基づいた規則をバックボーンとした監査方法を確立してきた．

特に戦後，株式市場の一般大衆への公開によって有価証券取引法をはじめディスクロージャの公開といった面で商法も数次に及ぶ改正を重ねてきた．

会計監査面も昔ながらの監査役の監査（商法 274 条・275 条・281 条・282 条等）に戦後は株式上場企業には公認会計士監査制度（証券取引法 193 条の 2，監査特例法2条等）が採り入れられ，さらに商法では「会計監査人」による第3者監査を含め，監査役・会計監査人（公認会計士）・内部（業務）監査人，と2重3重の監査が行われている現状である．これを3様監査制度と呼んでいる．制度面でみれば厳重かつ完備しているようであるが最近は別の問題が起ってきている．

企業は人・金・物の集りでありその中での企業活動は伝票一枚一枚，人間1人1人の仕事の積み上げである．伝票の計算や起票にしても僅かな誤記誤算を避けることができず，一方では省力化や合理化と称して製造・事務を問わず作業工程を減少させ人を減らそうとする結果，正確迅速熟練度を機械処理に置換えて OA とかコンピュータの導入が採用され，生産・販売・経理・人事等，およそ企業の中であらゆる分野に及んできた．最近は OA のほか産業ロボットも登場し，製造工程の中味もプログラム化されてきた．

このようなコンピュータ化時代の監査に対して，今日まで培われてきた監査技術は大変無力である．今まで人間の犯した誤りや作為を発見することを中心にして監査技法を磨いてきたが，あらゆる作業がコンピュータに移行してきた現在では，演算実行の結果の検証よりプログラム論理の組立て方やデータベースの維持管理の整合性をチェックしたり，オペレーション上（コンピュータ操作の）の錯誤やスケジュールのタイミングを証査することが監査に必須となったからである．いわゆる EDP 監査を避けることのできない社会環境の中に置かれているといっても過言でないのが現状ではないだろうか？

一般にコンピュータ監査（EDP 会計監査）のステップとして

1) 周辺監査 Auditing Around the Computer.
2) 処理過程監査 Auditing Through the Computer.
3) 活用監査 Auditing With the Computer.

の3段階があり，第1段階の周辺監査はできても第2段階以降はなかなか実施が難しい．

特に従来の経理・原価のベテラン級はコンピュータアレルギの人が多く，一方のシステムエンジニアやプログラム層の人たちは経理・商法などに弱い人が多く，また監査に即使用可能な汎用プログラムやツールが少なく，またあったとしても各企業の使用するシステム，特にコンピュータ機種・容量や使用するオペレーティングシステムのバージョンやレベルの差によって汎用プログラムの導入が難しい．

企業独自でプログラムを組もうとしてもさきに述べた，経理会計実務とプログラミング実務の2足の草鞋を履ける人が少なく，依頼すればでき上るまでの時間がかかりすぎる．

これからは監査人自身がシステム分析手法を身につけることによって企業独自のプログラムを試査したり，データベースのファイル内容を検証しファイルとプログラムの適合性を確める技法を修得しなければならないのではなかろうか？

監査する立場と監査される側とは常にイタチゴッコである．システムの信頼性や安定性についても完璧を最初から期すことは難しい．システムも最初から完成されるものではないし監査テクニックもシステムの成長につれて具備されていくものであろう．

私どもではまだ初歩段階でしかないが監査部門にも端末機を配置して DB の中味を検索しながら原票照合したり，DB ファイル構造を確かめた上で現場試査を行うなど，理論より実地にコンピュータに接近してゆこうとしている．

監査の精度を高めるためには実務部門と監査部門が切磋琢磨（ブラッシュ・アップ）しながら正確性・安全性・信頼性の精度向上のフォーナイン（99・99）を目指してゆくべきではないだろうか．

昔，釜ゆでにされた石川五衛門が「浜の真砂が尽きるとも世に盗人の種は尽きまじ」と辞世したとか……，いかにコンピュータ万能になろうと次々と新手のミスやエラー，そして不正や犯罪は新しい手口を生んでいる．監査の手段方法も負けることなく新な手法を工夫しなければならない．

銀行におけるシステム監査事例

行武　郁博

1. 経　緯

当行では，54年2月の総合オンラインシステム稼動を機に，システム監査実施の機運が高まり，54年4月に実施準備担当者が発令された．約6か月の準備作業を行った後，54年11月から実施し，今日に至っている．システム監査の呼称であるが，当行では，「EDP システム検査」と称している．監査担当者の所属が，検査部であり，検査諸規定の下で実施しているからであるが，このような例は他行でも多いようである．以下システム検査と略称する．

準備作業の主なものは，システム検査要綱とシステム検査要領の作成である．システム検査要綱は，システム検査の意義目的，対象，基準，方法といった，基本事項であり，システム検査要領は，担当者がシステム検査を行う際の具体的指針となるものである．以下システム検査要綱の項目に沿い当行のシステム検査の概要を述べる．

2. システム検査の定義，目的

日本情報処理開発協会，システム監査研究委員会のシステム監査の定義，目的に沿ったものであるが，公共性が強く要求される金融業として，当然のことながら安全対策，事故防止，不正防止に重点をおいている．

3. システム検査組織

検査部内にシステム検査班を設置し，現在，専任者2名で担当している．検査対象部門は，本部の EDP 部門であって，営業店の EDP 関連事項は営業店検査班が担当する．他行においても，このような例が多いようである．

システム検査組織を EDP 部門内に設置する例もあるが，検査対象部門から独立性を保つということは，重要かつ基本的なことであると思う．

システム検査は，営業店検査と異なって，組織上の問題がある．本部は，営業店に対しては管理部門であるので，営業店検査は問題ないが，システム検査の場合は検査部と EDP 部門は同じ本部の一部門であり，管理部門である．いわば並び大名である．しかも，EDP 部門には優秀な人材が投入されてきており，かつスペシャリストとしてプライドをもって作業している部門である．検査担当者として，十分な配慮と

EDP 処理内容に精通すべく絶えざる自己研鑽が要求される.

4. システム検査対象部門

EDP システムの企画開発運用を所管業務としている本部各部で，事務管理部，電子計算部および事務集中部である．なお，当行の関連会社である福岡コンピュータサービス(株)への当行の委託業務を検査対象としている.

ここで，当行の EDP 部門の組織上の特長をのべると，当行では，システムの開発段階を2分割し，それぞれ異なった部で担当し，相互牽制を行っていることである．システム設計は事務管理部（事務開発課）で担当し，プログラム仕様，プログラムは電子計算部（電子計算第一課）で担当する．そして，システム稼動前に，システム設計担当者による確認を行わせている．運用は電子計算部（電子計算第二課）で行う．福岡コンピュータサービス(株)のシステム検査は，業務委託契約書により立入調査を行うこととしており，これにもとづきおこなっている．立入調査という名目であるが，EDP 部門のシステム検査に準じておこなっている．現状では，当行の OB および出向者が管理層のほとんどであり，スムースに行われている.

5. システム検査の対象項目

対象項目は，当然のことながら，EDP 処理業務全分野にわたる．大項目のみをあげると，システム開発改善，プログラム，電子計算機運用，データ管理，施設管理，人事管理，経費管理等である，項目ごとの検査ポイント等の説明は紙面の都合上割愛せざるをえないが，要するに，定められた手続きが正しく守られているか，相互牽制が有効に機能しているかをドキュメントを中心に点検してゆくことに主眼をおいており，手続検査が主体である．一部内容に立入って点検しているものとしては，システム設計上でのエラー，障害対策，プログラムテスト，運用上発生したエラー，障害とその対策，重要プログラムの内容検証等である.

6. システム検査基準

システム検査の基準は，検査諸規定のほか所管部の内部規定によることとしている．本部はなかなか内部規定が整備されていないということがある．内部規定がなくても，システム検査は行わねばならないし，また行えるものである．その場合の基準としているのが，各種公的機関等の電子計算機管理基準である．通産省の「電子計算機システム安全対策基準」，システム監査委員会の「システム監査実施への道標」，日本公認会計士協会の「EDP システムの内部統制」などである.

7. システム検査の方法

（1） 検査の種類と周期

システム検査は，定例検査，特別検査および随時検査に分けられる．定例検査は月次検査であって，検査対象部門の前月中の EDP 作業実績について検査するもので，検査項目は前述のとおりである．特別検査は年次検査であり，保存磁気テープ，プログラムファイル，施設について管理状況の検査を行う．随時検査は検査立入日以外にも随時検査するもので，システム設計書の内容検査等である.

（2） 検査実施計画

定例検査，特別検査とも前月中に検査立入日を決めて検査対象部門へ通知する．いわゆる予告検査である．検査立入期間は，定例検査で計7日間程度であり，特別検査は1～3日間である.

（3） 検査結果報告

検査終了後，現地で講評を行い，改善要望事項等については，検査対象部門の意見を聞き調整をはかる．講評内容については，後日文書化して検査対象部門へ送付するとともに，次回検査時に進捗状況の報告をうけることとしている．その他，常務会あての報告として，システム検査概要報告があり，頭取あてのシステム検査報告書を作成して，システム検査の総まとめとしている.

8. おわりに

以上が当行のシステム検査の概要である．特別な監査ツールを用いて行っているわけではない．検証用プログラムの作成を行うことがあるが，ほとんどは，EDP 部門のドキュメント精査，現場調査といった伝統的な手法に頼っているのが現状である．それでおおよそはカバーできる．今後の問題として，システムの内容検査を深めるには自から限界があり，汎用監査プログラム等の監査ツールの使用を検討課題としている．システム検査の重点は，前述のとおり，安全対策，事故防止，不正防止にあり，それはまず EDP 部門の内部統制なかんずく相互牽制で達せられるところが大きい．したがって，システム検査は，相互牽制がどこまで徹底しているか，正常に機能しているかをきめ細かく点検してゆくことである．その意味で，月次検査を主体とした当行のシステム検査は有効な方法であると確信している.

コンピュータ・セキュリティと EDP システム監査

平田　正敏

最近コンピュータ・セキュリティへの認識が高まり，これに対応して EDP システム監査の内容を見直そうとする蠢きが起っている．これに対しては，わが国でも日本情報処理開発協会を中心とした積極的な取り組みがあるが，この中でとくに注目されているのは「システム監査研究委員会」の活動であろう．昭和 53 年 3 月に公表された委員会報告書『システム監査実施への道標』(以下『道標』とする）では，EDP システム監査の内容について以下のように説明している．

「システム監査というのは，監査対象から独立した客観的立場でコンピュータを中心とする情報処理システムを総合的に点検・評価し，関係者に助言・勧告することをいい，その有効利用と弊害の除去とを同時に追求し，システムの健全化をはかるものである」と．そしてその具体的な内容は，内部監査の一環として与えられるというのである．

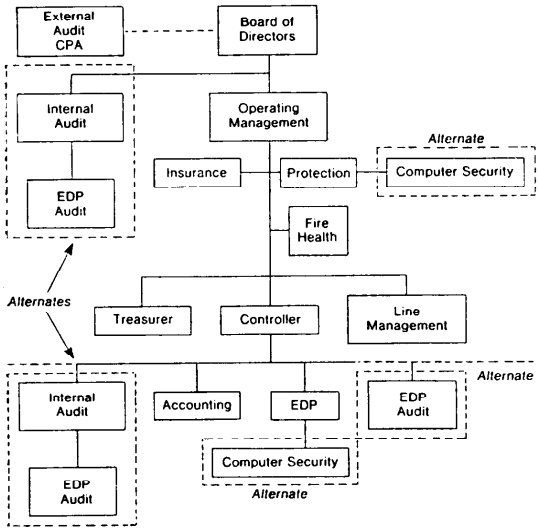
この内容規定においてはっきりとしていることは，EDP システム監査の目的が「健全なシステム」の確立であるということであろう．ここで健全なシステムというのは，『道標』の説明によれば，効率性，信頼性，安全性が保たれているシステムを指す．この場合に信頼性は，「チェック・コントロールによって業務が正しく処理されていること」であり，安全性は「過失，事故，不正から保護されていること」であるので，この二者はいわゆるコンピュータ・セキュリティという範疇に入る．さらに，このようにコンピュータ・セキュリティが確保されたシステムは，物質的には一定の品質基準を備えたシステムであるということができるであろうから，かかる観点からすれば，健全なシステムというのはその効率と品質のトレードオフするフロンティア上において定められるというべきであろう．もちろんこのようなフロンティアがどのようにして求められるかはなお議論の余地があるが，しかしいずれにしても，内部監査の一環としての EDP システム監査の目標は，ここに求められるべきであろう．

しかしながら『道標』の規定によると，必ずしもこのようにいいきれないのである．なぜならば，上述のコンピュータ・セキュリティの他の表現であるところの「弊害の除去」という概念の中にはいつのまにか「プライバシの保護」という社会的な立場からの観点が滑り込んでおり，この限りでは EDP システム監査の基本的視点が内部監査のみで説明しきれないものを内蔵しているからである．だが，『道標』はこれを「機密性の保護」として捉えて，EDP システム監査を内部監査と論理的に斉合せしめようとしているが，これは牽強付会といわざるをえないであろう．この考え方には，セキュリティ・コンフィデンシャリティ（機密性）とプライバシの混同がみられるのである．

Donn B. Parker によると，これらの三つは明確に区別されるべきである．まずプライバシは人権を含む社会問題に関するものであり，これはセキュリティと混同されるべきではない．次に機密性はプライベート，あるいはシークレットな状態にあることをいい，そしてそれは特定のデータの分類とそれに対応する一連の規則によって定められるものと解すべきである．最後に，プライバシは個人データの使用に機密性の規則を課すことによって保証されるが，それが保護されるのはセキュリティ活動および機能によってである．

この解釈は極めて明解であり，十分に納得しうるが，しかしこのような見方をすれば，コンピュータ・セキュリティという概念は EDP システム監査とはちがった次元の独自の概念であり，必ずしも EDP システム監査という範疇に閉じ込めることはできないであろう．このことは，当然のことながら，コンピュータ・セキュリティに対する組織上の責任について考えざるをえなくするのである．それは EDP システム監査部門にあるであろうか．そうではない．むしろ，それは EDP システム監査から助言・勧告を受けるところの情報処理システム関係者にあるともいえよう．かかる関係者と EDP システム監査部門を含めて，われわれはそれを「コンピュータ・セキュリティ担当者」と呼ぶのが適切であろう．

かかる立場から，資産に対する危険発生度をベースとした職種レベルを吟味するならば，EDP システム監査人が最大のリスクをもっていることを否めない．と同時に，システム監査人の立場からみれば，他のコンピュータ・セキュリティ担当者のリスク・レベルは彼自身のリスク・レベルと同じなのである．ということは，コンピュータ・セキュリティにおいてもっとも重要なものは，システム監査部門とコンピュータ専門家，さらにそれに付随する保安サービス部門との相互牽制的な内部統制システムということになるであろう．



出典: Donn B. Parker, *Computer Security Manegement*, Roston Publishing Co., 1981, p. 86.

図-1

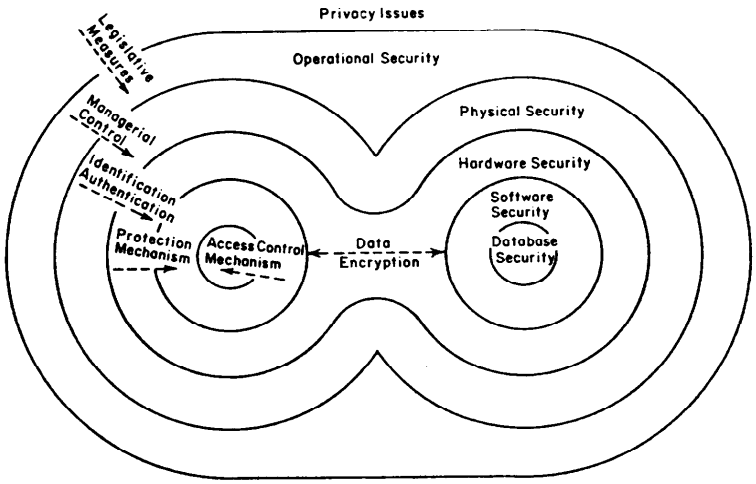
このようにみてくると，コンピュータ・セキュリティの責任は EDP 部門を中心として，他の関連部門を組織的に巻き込むという形でシステム化され，発展せしめられていくのである．Parker は，かかる組織開発の過程は以下のようになるとする．

第1段階；EDP 部門にコンピュータ・セキュリティの機能をもたせる．

第2段階；コンピュータ・セキュリティを組織全体の保護サービスの一部として機能せしめる．この段階では，コンピュータ・セキュリティが EDP 組織の一部に属する場合にくらべて，その独立性と客観性とを高めてくれるであろう．このことによってコンピュータ・セキュリティと組織の他の部門の安全性とがインタフェースせしめられ，一貫性が高められるのみならず，伝統的なセキュリティ技術と経験とをより強く結びつけることができるのである．

第3段階；コンピュータ・セキュリティが組織全般の保護機能の一部として，すべての EDP 機能と関連機能に対して必要な制約を課す段階．この段階のセキュリティ組織は，その専門的機能の遂行のため，EDP 組織内のセキュリティ担当者，保安組織の中の物理的コンピュータ・セキュリティ専門員，セキュリティの確保を責務とする DB システムの管理者，および情報保護担当取締役が含められることになるであろう．かかる段階の組織機構図を Parker は図-1のようにえがいている．

このようなコンピュータ・セキュリティ組織の一貫として，EDP システム監査は内部監査組織の中における新しい機能として開発されるとともに，EDP 組織の中にも，新しい機能として設置されなければならないであろう．そしてこの両者は，図-2 のようなコンピュータ・セキュリティの技術構造に対応して，体系化されなければならないのである．この場合，前者の機能に属するのがオペレーショナル・セキュリティと物理的セキュリティであり，後者の機能に属するのがハードウェア・セキュリティ以下 DB セキュリティ



出典: David K. Hsiao, Dougles S. Kerr, and Stuart E. Madnick, *Computer Security*, Academic Press, 1979, p. 2.

図-2

に至る3つのレベルであろう．

いずれにしても，EDP システム監査技術がこれから開発されなければならないが，しかしかかる技術の源流は，従来の内部監査の役割であったところの業務監査と不正の摘発法とが合体せしめられ，これがEDP 化されることによって果されるであろう．また，コンピュータ・プライバシと従来の外部監査との関係も問い直され，これがいわゆるオペレーショナル・セキュリティのレベルでどのように技術化されるかも考え直してみる必要があるのである．まさに，EDP システム監査は，現段階の新しい課題であるといえよう．

システム開発時におけるシステム監査

湯野　勉

1. まえがき

わが国におけるコンピュータ設置台数は，1981 年12月現在で約 10 万台を越え，今後もかなりの伸びが見込まれている．日常生活を振り返っても，航空機・国鉄の座席予約システムや，全国をカバーしたバンキングシステムなどがあり，これらのシステム抜きでは現代社会は成りたたないとまで言われている．また，コンピュータシステムの一時的サービス中断や，不正・異常処理による社会への影響は，従来と比較にならないほど大きなものとなる．一方，長期にわたる低成長時代において企業は，投資効果に対して，より敏感となり，特に多額の投資を必要とするコンピュータシステムに対して厳格なチェックを要求している．

このような環境をふまえ，最近システム監査の重要性が認識されつつある．ここでは，システム開発担当者としての立場から，システム開発時におけるシステム監査について述べる．

2. システム監査の目的

日本情報処理開発協会では，『システム監査とは，監査対象から独立した客観的な立場でコンピュータを中心とする情報システムを総合的に点検・評価し，関係者に助言することをいい，その有効利用と弊害の除去とを同時に追求してシステムの健全性を図るものである』と定義している．このような意味からシステム監査の目的は，効率性，信頼性，安全性の観点からシステムをチェックするといえる．

（1） 効 率 性

システムが目的とする処理を，投資費用に見合った形態で効率よく設計・運用されているか．

（2） 信 頼 性

入出力データを含めたシステム全体が信頼のおける品質の良いものか．

（3） 安 全 性

不正使用，盗難，破壊，プライバシ保護等の観点からみて，十分に対策がとられているか．

3. システム開発時におけるシステム監査の重要性

システムの有効利用と弊害の除去を図るためのシステム監査は，運用中のシステムだけでなく開発中のシステムも対象とする．システム運用時における効率性，信頼性，安全性を決める多くの要素が，この開発時点において決定されることを考慮しなければならない．また，一旦運用に入ると，運用後発見された不具合を改良する場合において莫大な費用と年月を必要とすることがある．このため，システム開発時においては，運用後のあらゆる状況を想定した設計や試験が行われるのであり，このような意味からも，システム開発時点で，効果的なシステム監査を行っていくことが，重要になる．

4. 望ましいシステム開発体制

効率性，信頼性，安全性の高いシステムを開発するために望ましいシステム開発体制は，システム監査を容易にするシステム開発体制と同一であり，概略以下のように考えられる．

（1） 機 能 分 離

業務を組織上分離することにより，責任の明確化と相互チェックを図るものであり，例えば，開発部門と運用部門との分離や，開発部門における設計部門と製造部門との分離などである．

（2） 開発手順，ソフトウェア等の標準化

開発工程における組織的な承認手続，試験手順，開発工法，実施基準等一定のルールを決めておく必要がある．プログラム作成については，標準言語の採用，プログラムのパッケージ化等の標準化を図ることが有効である．

（3） 文 書 化

各種ドキュメント，開発工法書，オペレーション指示書，システム管理用資料等が決められたとおりに文書化されていることが必要である．

5. システム監査の方法

システム開発時におけるシステム監査の具体的な方法としては，次のものがある．

（1） 委員会方式

この方式は，トップ層を混じえた委員会形式により

開発方針の決定・承認，工事進捗状況の管理・チェックを行う方式である．

（2） ドキュメント方式

チェックシートや質問書による開発状況を監査したり，各種ドキュメント，報告書類等により監査する方式である．

（3） ソフトウェアツール方式

システム監査用のソフトウェアとしては，テストデータ法，監査ソフトウェア法などがあり，ブラックボックス化したシステムの処理内容について監査する場合有効である．

6. システム開発時におけるシステム監査の問題点

システム開発を進めていく過程では，当初予想できなかった仕様追加等の要因により，工程増，線表変更が生じ易い．このようなシステム開発の変動性，ならびに，システムごとの多種多様な要求等により，開発工程において標準化を行う上で，多くの解決しなければならない問題がある．システム監査人については，システム開発部門と独立した部門であることが望ましいが，限られた開発線表で，かつ，変更要素の多い工程で，開発部門と独立した部門の監査人が関与できる範囲は，おのずと限定される．一方，ソフトウェアによる監査については，開発しようとしているシステムが，本来目的としていないルーチンやツールを組みこむことにより，システムに与える経費面，品質面の影響も無視することはできない．

7. おわりに

システム開発工程における標準化は，今後ソフトウェア人口の大幅な増加が望めないことを考慮すると，システム監査面からだけでなく，今後ますます必要とされよう．現在各方面で標準化に向かって努力されているが，具体的にはソフトウェア部品レベルの標準化から開発方法の標準化，開発管理方法の標準化へと進んでいくものと思われる．システム監査人については，システム設計経験が豊富で，かつ，監査知識を有する人を長期にわたって育成していく必要がある．しかし，システム開発を今後行っていく上でもっとも重要なことは，システム関係者性善説をとってきた従来の考え方を性悪説に転換することであろう．コンピュータシステムが現代社会における両刃の剣であることを，なによりもシステム開発に携わるわれわれ自身がまず認識することが重要と思われる．