52－R007

システム監査の現状と問題点

情報化社会の健全なルール確立をもとめて

昭和53年5月

JIPDEC

財団法人　日本情報処理開発協会

この資料は，日本自転車振興会から競輪収益の一部である機械工業振興資金の補助を受けて昭和52年度に実施した「システム監査に関する調査研究」の成果をとりまとめたものであります。

序

当協会は，昭和49年に情報化社会の基本的なルールの1つとしてシステム監査を提唱いたしました。そして，翌50年度には，システム監査委員会（委員長・故金子佐一郎氏）を設置し，理論および技術の両面から調査研究をつづけてまいりました。

まず，50年度は，システム監査のフレームワークを示し，今後の調査研究の方向を明確にいたしました。

つぎに，51年度は，システム開発・運用段階における詳細なシステム監査上のチェックポイントを明確にいたしました。そして，システム監査体制が確立されていない時点での過渡期的な措置として，監査部門やコンピュータ部門等の関係部門が連携を保ち，プロジェクト・チームを編成してシステム監査にあたるチーム・アプローチを提唱いたしました。

本年度は，これら過去の実績をベースとして，調査研究をさらに一歩前進させるべく，わが国および米国のシステム監査の実態面に焦点を合せました。そして，その問題点を堀り下げると同時に，日米の現状比較をも試みました。

これらの調査研究の結果が，関係各位のご参考に資することができることを願うとともに，本報告書をシステム監査の研究に偉大な足跡を残された故金子佐一郎先生に捧げるものであります。

昭和53年5月

財団法人　日本情報処理開発協会

会長　上　野　幸　七

目　　次

第１章　システム監査調査研究の概要

第1章　システム監査調査研究の概要

当協会は，昭和49年にシステム監査を提唱すると同時に，調査研究体制を整えて活動を続けてきた。とくに，49年秋には，第1次システム監査研修団を米国に派遣し，翌50年にはシステム監査委員会を設置して本格的な調査研究に取り組んできた。

本年度は，第2次システム監査研修団を派遣するとともに，独自の調査研究活動を実施し，米国のシステム監査の実態とわが国の現状を把握して，システム監査の現状と問題点をとりまとめた。

1．1　調査研究の目的

本調査研究は，システム監査の理論的な位置づけや方法論等について調査研究を行い，コンピュータ・ユーザにおいてシステムの信頼性，安全性，効率性等の監査を可能にするためのガイドラインを示すことを目的としている。

この点については，昭和50年度報告書「わが国におけるシステム監査のあり方」で，つぎのように調査研究の趣旨を明確にしている。

わが国において，コンピュータを対象としたシステム監査が必要になってきた背景には，数多くの原因が考えられる。これらを簡単にとりまとめるとつぎのようになる。

① コンピュータ・システムには大規模な投資がともなうため，企業収益にも関連して何らかの投資基準が必要と指摘されていたが，低成長下において，その声がさらに強くなってきており，採算面からの評価を実施することが必要になってきている。

② 安全対策，個人データ保護等の観点から，コンピュータ・システムの備える

べき対策が検討されつつあり，近い将来において，対策項目およびその基準が作成されることになろう。したがって，早晩これらの基準が満たされているかどうかの監査が必要になってくる。

③ 従来から会計監査，業務監査等の監査業務が行われているが，コンピュータ・システムを含めたシステム監査を確立することにより，総合的かつ効率的な監査が可能になると思われる。

しかし，これらの監査業務は，個々の対策項目ごとに十分な体制を固めることが必要であるから，システム監査として一つの概念を構築することについては，まだ検討すべき問題点を多々含んでいると考えられる。

これらの問題点は，今後の検討課題として残すこととし，当面考えるべき検査・監査を広くまとめてシステム監査の範囲に入れれば，第1.1表のようになるであろう。

第1.1表　　システム監査の範ちゅう

要　　因	システム監査の内容	監査の観点
コンピュータ部門のマネジメント	マネジメント監査 (1) リソース・マネジメント (2) コスト・マネジメント (3) リスク・マネジメント	採算性中心
過失・事故・不正からの保全	セキュリティ監査（安全性監査） (1) エラー (2) フィジカル・セキュリティ (3) コンピュータ悪用	安全性中心
ＥＤＰ会計システム	会計システムの監査	信頼性中心
高度システムの登場	オンライン・リアルタイム・システム監査	信頼性中心
	コンピュータ・ネットワーク・システム監査	信頼性中心
プライバシー保護	個人データ監査	基本的人権中心

なお，新しい動きとしては，監査役による取締役の業務執行の監査や，労働組合の経営参加などが，これからの問題点としてクローズアップされている。

システム監査の対象となるのはコンピュータ部門中心であるが，監査目的は多様化しており，したがって監査サイドは複数という形になっている。図に示すと第1.1図のようになる。

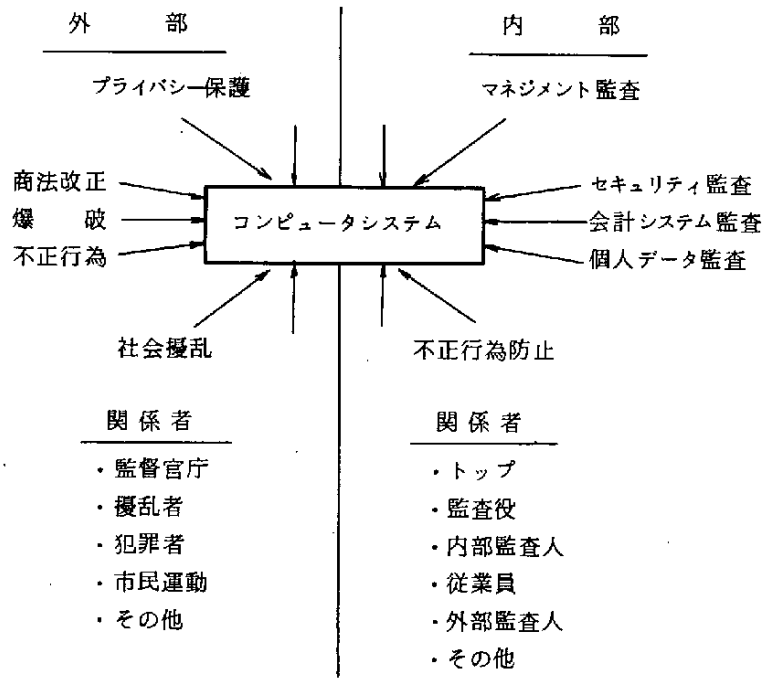
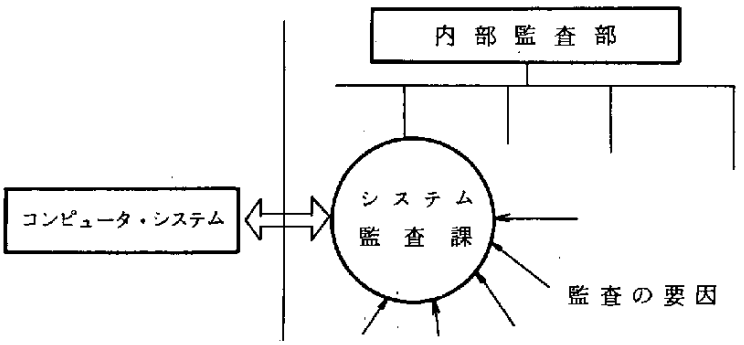


図1.1　コンピュータ・システムをめぐる諸問題

米国では，システム監査を行うために，内部監査部門にシステム監査課を設置している企業が多く，今後ともこの傾向は増加していくものと見られている。これを図に示すと第1.2図のようになる。



第1.2図　システム監査の担当部門

以上のようなことから，わが国においてはコンピュータ・システムをめぐる監

査をどのように整理し，どのような形でシステム監査を体系づけるか，基本的な問題から検討しなければならない。

なお，詳細については，「わが国におけるシステム監査のあり方」のP52~71を参照されたい。

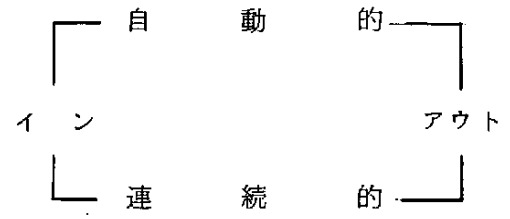
1．2　過去2年間の調査研究の要点

システム監査に関する調査研究について，過去2年間の成果の基本的部分を簡単にとりまとめるとつぎのとおりである。なお，これらの詳細については，昭和50年度報告書「わが国におけるシステム監査のあり方」，および昭和51年度報告書「システム監査体制確立への道」を参照されたい。

1.2.1　システムの定義

システムとは，一般的に相関連する機能の有機的集合と定義される。この意味から，ここでは企業経営目的を達成するためのコンピュータに関連した機能の有機的集まりと定義して考えることにしたい。

まず，システムには"イン"と"アウト"とがあり，インからアウトに至るプロセスが自動的・連続的につらなる構成体としてとらえてみたい。



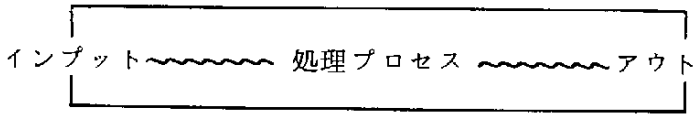
第1.3図　　システムの構成

自動的・連続的というのは，何も技術的な面に限らず，法律あるいは規定やルールにより構成される人間の介在したプロセスも当然この範疇に入ることはいうまでもない。

そこで，コンピュータ・システムの場合の構成体を考えてみると，ハードウェア，ソフトウェアおよび要員の有機的結合体系ということができる。

(a) **狭義のシステム**

上記のような考え方に立ってシステムをとらえる場合，狭義にはコンピュータ・システムということになる。すなわち，インプットからアウトプットに至る情報処理システムが該当する。



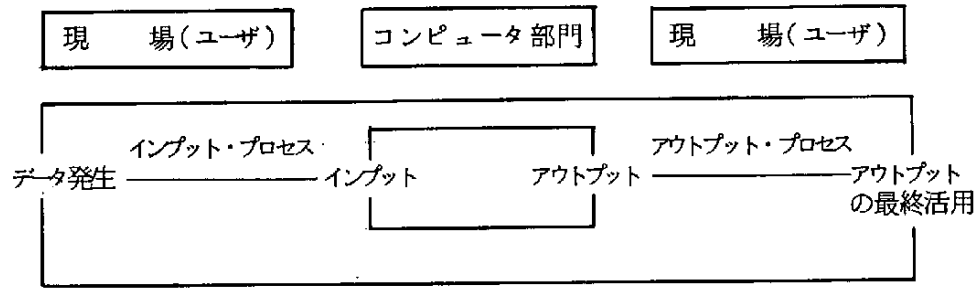
第1.4図　狭義のシステム

狭義のシステムは，直接マシンにインプットする段階からアウトプットまでのプロセスであるから，いかにインプット・データへの変換が正確に行われようとも，データ発生時あるいはインプット・データへの変換に至るまでの過程でミスが生じていたとしたら，この場合は誤データを誤データのままで正確にインプットしたことになる。したがって，狭義のシステムが完全だからといって，そこで処理されている業務が正確で信頼性がおけると即座に断定することもできない。

(b) **広義のシステム**

以上のように，各現場でデータが発生してコンピュータにインプットされるまでのプロセスが存在し，インプットを正確に行うためにはデータ発生現場での処理がきわめて重要なことがわかる。われわれはこれをインプット・プロセスとよぶことにする。同様にアウトプットについてもプロセスが存在し，これをアウトプット・プロセスとよぶことにする。

ここでは，データ発生からアウトプットのユーザにおける最終活用および保管または破棄までを含めて，広義のシステムとしてとらえることにした。したがって，すべての業務がコンピュータ処理されている場合，生産・営業その他の第一線現場における業務すべてが当人の意識にかかわらずコンピュータとの接点をもっており，この場合の広義のシステムは企業活動全体に関連することになる。



第1.5図　広義のシステム

さらに広義のシステムは，伝統的なタテ系列・ヨコ系列の管理の枠内に整然とおさまっているものではなく，逆に双方に横断して存在する活動体であるといわなければならない。このように把握しなければならない点が，従来の業務処理の場合と異なる一面である。

1.2.2　システム監査の定義

システム監査を定義づけるにあたって，まず「監査」という言葉のもつ意味から検討してみたい。監査（Audit）という言葉がもっている意味で，われわれにとってきわめて重要な要素は2つある。ひとつは，監査人が監査対象から独立した客観的な立場でなければならないことであり，もう1つは，監査結果を表明しなければならないことである。そして，この2つの要件を満たさなければ，厳密な意味では監査として成立しない。したがって，監査という言葉には，他の言葉で表現できない意味があるといえよう。

システム監査の定義については，過去に，本協会が昭和50年2月，つぎのように定義した。

「システム監査とは，独立した第三者の立場で，コンピュータ・システムの安全性・信頼性・採算性等をチェックし，①マネジメント面からの評価および改善勧告，②悪用の防止，③個人データの濫用防止，その他，システムの健全化をはかるための施策をいう」。

本委員会では，この定義に検討を加えた結果，若干の補強・修正をする必要が

あると認められた。そこで，幅広く各面から検討を重ね，本委員会として，つぎのように定義することとした。

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，そ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。

1.2.3　システム監査の実施基準

システム監査を実施する場合の基準を設定するにあたっては，システムの企画から開発・稼動レベルに至るまでの全体の業務について実施する基準と，開発・稼動レベルにおけるシステムの品質を保障するための基準との二本立を想定した。そして前者を一般基準，後者を品質基準と呼ぶことにした。それぞれの基準の内容はつぎに述べるとおりである。

(a) **一　般　基　準**

システムを全般的に監査する実施基準で重要なものとしては，①準拠性，②採算性，③適時性，④生産性の4つをとりあげた。なお，採算性と生産性は「効率性」を把握しやすくするために2つにわけたものである。これらは企業活動そのものに適用される項目であり，当然システム監査の場合にも基準としなければならない。

ⓐ　準拠性：すべての業務活動は，そのレベルに応じてポリシー・法律・規定その他のルール等に準拠して行われなければならない。

ⓑ　採算性：企業は採算の上に成立する。したがって，採算面からコンピュータ・システムを検討・評価することは最も基本的な監査活動ということができる。

ⓒ　適時性：コンピュータ・システムを開発し運用するにあたっては，タイムリーであることを要求される業務が非常に多いので，1つの基準としなければならない。

ⓒ 生産性：ソフトウェアの開発，メンテナンス，オペレーション等は，他の業務と比し，管理性にも困難がともない，リソースの無駄が発生する恐れがある。したがって，ソフトウェアの開発やメンテナンス，オペレーションをいかに効率よく行うかが重視されなければならない。

(b) 品 質 基 準

コンピュータ・システムそれ自体の内容，すなわち，品質または性能を保障するためには何が満たされたらよいかを検討し，その結果，①安全性，②信頼性，③機密性が確保されなければならないという結論を得た。これらを監査サイドの観点からながめるとつぎのようになる。

ⓐ 安全性：コンピュータ・システムの破壊は，それが人為的行為であれ自然現象であれ，企業あるいは組織に対して大きな経済的打撃を与える。しかも，事故発生時においても間断なく業務を遂行することが要求されるので，安全性の保障はきわめて重視されなければならない。

ⓑ 信頼性：業務が正しく処理されるためには，とくにハードウェア，ソフトウェアおよびオペレーションの信頼性が保障されなければならない。

ⓒ 機密性：個人データを処理する際の機密性の保障は今後さらに重視されるようになる。また，情報処理を受託する企業にとっては企業機密が保障されなければならない。

1.2.4 チェックポイント

(a) システム機能上の重要なポイント

システムの重要な機能は，同時にシステム監査の対象としても重要である。このような観点からは，①コントロールそのもの，②セキュリティの確保，③プライバシー保護の三点がとくに重視されなければならない。これらを監査の観点からとらえるとつぎのようになる。

ⓐ コントロール：監査サイドからはとくにソフトウェアに限定し，その信頼性を確保するためのチェック機能としてとらえるべきである。

一方では，それは法律や規定に準拠したコントロールでなければならない。

ⓑ セキュリティ：ハードウェアを中心としたリソースは，過失・事故・不正等から保全されなければならない。いいかえれば，電磁的電子的エラーの防止・物理的破壊・悪用・エラー・機密漏洩からの保全ということになる。

ⓒ プライバシー：個人データに関する機密保護問題であるが，プライバシー保護法の立法化の動きなどもある折から重大な問題として認識しなければならない。

(b) マネジメント上の重要なポイント

システム開発レベルおよび稼動レベルにおいて，質の高い管理が要求される。とくに，その中でも各段階ごとに，①ドキュメンテーション，②標準化，③スケジューリング，④承認が体系立って管理されていることが必要である。これらを監査の観点からながめるとつぎのとおりである。

ⓐ 承　　認：正当な権限をもつ者の承認は不可欠であり，業務の重要性に応じて承認のレベルが決められている承認制度が存在すべきである。したがって重要なステップは，その計画ないしは結果が必ず評価され，承認をうけなければならない。事後においても，この承認は責任の所在を明確にするものである。

ⓑ 標　準　化：開発および稼動レベルにおける標準化は，システムの信頼性や生産性に大きな影響を与えるものである。システム開発の各ステップの作業内容が標準化されなければ，システム開発が属人的となり分業することも困難がともなう。そうなれば，システムの質の向上も望めないしオペレーションの効率化もおぼつかない。

ⓒ ドキュメンテーション：開発および稼動レベルにおけるドキュメンテーションは，システムの信頼性を証明し，かつ，ソフトウェア開発の生産性

に大きな影響を与えるものであり，社内規定にもとづき整然と行わなければならない。とくに，開発レベルにおけるプロセスを把握できることが必要である。

ⓓ スケジューリング：開発および稼動レベルにおいて，当初予定された通りに作業が進むよう配慮されなければならない。もし，当初の予定通り作業が進行していないときは原因究明が要求されるべきである。しかも，それらの遅れによりタイミングを失するということになれば重大な問題であると認識しなければならない。

1.2.5 監査基準とチェックポイントの関連

これまで述べてきたシステム監査の実施基準と，機能上，マネジメント上の重要なチェックポイントとの関連性を示すと第1.2表のようになる。

第1.2表　実施基準とチェックポイントの関連

チェックポイント ＼ システム監査の実施基準		品質基準			一般基準			
		安全性	信頼性	機密性	準拠性	採算性	適時性	生産性
ファンクション	コントロール（プログラムのチェック機能）		◎	○	○			
	セキュリティ（物理的安全）	◎	○		○			
	プライバシー（個人データ保護）		○	◎	○			
マネジメント	承認	○	◎	○	○	○	○	
	標準化		○		○			◎
	ドキュメンテーション		○		○			◎
	スケジューリング						◎	○

◎最も重要な関連を示す
○二重マルに次ぐ重要性を示す

この表は，たとえばコントロールの場合をみると，信頼性，機密性，準拠性の見地からチェックされなければならないということを表現しているものである。

1.2.6 システム監査の対象業務

これまでシステムを定義し，監査基準を設定し，システムのファンクションおよびマネジメント上できわめて重要な項目をピックアップしてきた。そこで，これらを適用してシステムを監査するための監査対象業務を明確にし，整理しなければならない。すなわち，業務のどの段階で何をどのような視点から監査すればよいのかの解明が必要である。

従来，監査とは業務活動の結果を調査して，これに基づく意見を表明するものであり，業務の事後評価としての認識が一般的であった。もし監査をそのような意味でとらえるならば，システム監査も事後段階で行えばよいということになる。しかしながら，コンピュータ・システムには莫大な投資が行われているため，従来の手作業とは異なり，事後段階で監査人が問題点を指摘して，現行システムの変更・改善等を助言・勧告しても，それを実行するにはあまりにも経済的・時間的に多大の損失を与えることが明白である。

そこで，システム監査の場合には，企画レベル ― 開発レベル ― 稼動レベルの3段階でとらえる必要があり，それぞれのプロセスごとに監査されることが望ましいといえるであろう。

まず，企画レベルで重視されなければならない項目として，①経営方針，②組織計画，③要員計画，④調査研究，⑤評価計画，以上の5点を強調した。

つぎに，開発レベルでは，業務の流れを順に追って，①予備設計，②基本設計，③詳細設計，④プログラミング，⑤システム・テスト，以上5段階にブレークダウンした。

さらに，稼動レベルについては，①インプット・プロセス，②オペレーション，③アウトプット・プロセスの3つに区分した。

そして，以上のように細分化した業務の各レベルごとに，実施基準とチェック

第1.3表　システム監査の着眼点

◎　最も重要な項目
○　二重マルに次ぎ重要な項目

システム監査の内容 / 対象業務の範囲			チェックポイント							システム監査の実施基準							関係者の参加	
			ファンクション			マネジメント				一般基準				品質基準				
			コントロール	セキュリティ	プライバシー	承認	標準化	ドキュメンテーション	スケジューリング	準拠性	採算性	適時性	生産性	安全性	信頼性	機密性	トップ	ユーザ
企画レベル	経営方針									○	◎	◎					◎	
	組織計画					○				◎		○						
	要員計画					○				◎		○						
	調査研究					○				○	○	○						
	評価計画					○				○	◎		◎				◎	○
開発レベル	予備設計					◎		○		◎	◎	○					○	○
	基本設計		○	○		○	○	○	○	○		○			○		○	◎
	詳細設計		◎		◎	○	◎	◎	○	○		○			◎	◎		○
	プログラミング		◎		○	○	◎	○	○			○	◎		◎	◎		
	システム・テスト		○			◎			○			○			◎			
稼動レベル	入力プロセス	現場処理	◎			◎	○	○		○					◎			
		センタ処理	◎	○		○			○	○		○		○	◎			
	オペレーション	マシン・オペレーション	○	◎		○	○	○	○	○	○	○	○	◎	○			
		ライブラリ	○	◎		○		○		○				◎	○	○		
	出力プロセス	出力管理			◎	○	○		○			○			○	◎		

ポイントとの関連づけを明確にしてとりまとめたものが第1.3表である。

1.3 システム監査をめぐる最近の動向

当協会がシステム監査を提唱して以来，コンピュータ・ユーザおよび監査側の双方に大きな反響を呼び，これを契機として関連各界の動きが活発になった。

とくに，昭和51年秋には，EDPユーザー団体連合会および日本公認会計士協会から，通産大臣に対してシステム監査に関する要望書が提出された。一方，通産省では，これに応えるように，昭和52年度よりシステム監査をユーザ対策として位置づけ政策として取りあげている。

また，各企業においては，とくに金融機関を中心として，コンピュータ専門家を内部監査部門に配置してシステム監査人の養成に乗り出すところが増加するなど，着実にシステム監査の実施体制が整いつつある。

なお，現時点におけるコンピュータ・ユーザおよび公認会計士のシステム監査に対する考え方は，上述の要望書にかなり明確に表現されているので紹介してみたい。

1.3.1 ユーザからの要望

昭和51年10月14日，EDPユーザー団体連合会は，通産大臣に対して「システム監査の実施に関する要望書」を提出した。

この要望書では，「コンピュータ・システムに対する多額の投資が果してそれに対応する成果を生んでいるか否かに関する反省が，自主的にシステム監査を実施して，システムの正確性と信頼性を守り，利用水準の高度化を推進する動きとなってあらわれつつある」としている。

しかしながら，現在のわが国におけるシステム監査への意見の多くが，日本公認会計士協会の内部統制質問書等に見られるごとく，「会計監査の立場から会計情報システムの正確性，信頼性を追求することのみに重点がおかれ，必ずしもコ

ンピュータ・システム全体の効率的運用という面に配慮を加えていないのが実情である」とも述べている。

そして，「システム監査の実施に関して，国が明確なガイドラインを示され，企業の合理化，健全化の促進と情報化の推進を遅らせることのない施策をとられることを望むものである」としている。

1.3.2　公認会計士からの要望

昭和51年11月9日，日本公認会計士協会は，通産大臣に対して「企業内部におけるＥＤＰシステム監査に関する要望書」を提出した。

この要望書では，「ＥＤＰ監査人の拠るべき指針としての一般に認められたシステム監査マニュアルの整備が，目下の急務である」としている。

また，「監査人が行うＥＤＰシステムの内部統制の検討・評価には，ＥＤＰシステム監査人の存在が大きな影響をもつものであるだけに，ＥＤＰシステム監査人が実施する監査の範囲・程度・時期等についての監査手続上の諸問題は，公認会計士にとって重大な関心事である」ともしている。

そして，「ＥＤＰシステムの内部監査実施上の拠るべき指針としてのガイドライン策定に当っては，日本公認会計士協会の意見を十分汲みとっていただき，各企業におけるＥＤＰシステムの内部監査の充実に特に配慮するよう」要望している。

1．4　昭和52年度における調査研究のハイライト

本年度の調査研究については，主として事務局ベースの活動を行い，本報告書をとりまとめたものである。

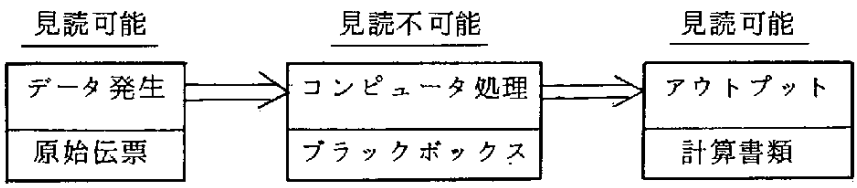
とりまとめ方針としては，第1に，各企業で現在問題とされているシステム監査における公認会計士の役割を明確にするために，会計監査の位置づけを検討した。

第2に，わが国よりは実態面で一歩進んでいる米国の状況を，発展の経緯とセキュリティ面について，できるだけ詳細に，かつ，体系的にとりまとめるよう努力した。

第3に，現段階では，日米ともに実態を詳細に把握するには資料に乏しいが，既存の資料から可能な限り日米比較を試みた。

1.4.1　システム監査における公認会計士の役割

会計処理がコンピュータを利用して行われている場合，公認会計士の行う財務諸表監査にどのような影響があるかを考えてみたい。まず，コンピュータにより処理される部分，すなわち計算書類の作成過程が，従来の手作業による処理と異り，ブラックボックスになっていると公認会計士側から指摘されている。これを図に示すと第1.6図のようになる。



第1.6図　会計処理システムの問題点

このようなことから，公認会計士が行う財務諸表監査との関連性は，会計処理システムに限定されることになる。そして，企業が自らシステム監査を実施している場合においては，公認会計士が会計処理システムに対して注目すべき点は会計コントロールということになろう。

さらに，正確な会計処理を行うために直接的に影響を与える会計コントロールとしては，インプット・コントロール，プログラム・コントロール，アウトプット・コントロールをあげることができる。

したがって，企業としては，会計処理システムについて，これら3つのコントロールに関して公認会計士と調整をはかることが望ましいといえよう。そして，公認会計士が，これらのポイントを十分に信頼できると判断すれば，その会計処

理システムで処理された計算書類は正確であると判定できるであろう。

詳細については第2章で述べる。

1.4.2 米国のシステム監査

米国におけるシステム監査の展開は，各企業ごとに，個々の部分についての積上げとして進められているのが実情である。したがって，統一的な手法が一般的にとられているというような状況ではない。

このような中で，システム監査人は，システム側の技術的進歩に何とか遅れをとるまいと模索しているといってよい。そして，このような状況下にあることからも，システム監査人の責任分野は次第に広がりつつあり，若干のとまどいも見受けられる。

すなわち，システム監査の場合，システムが稼動段階に入ってから監査人が問題点を指摘し，システムの変更・改善等を助言あるいは勧告しても，実際にはその通りに行うことは不可能というのが現状である。そこで，事後に変更や改善を行わなくてもよいように，システム開発段階から監査人が関与しはじめたものである。その結果，システム監査人の責任分野として，システムの品質管理等までが加わってくることになってきた。

また，セキュリティ面については，学生運動が吹き荒れた昭和44年頃から数年間，全米各地で大学を中心としてコンピュータ・センタが数多く破壊された。これについては，学生運動が下火になったこと，セキュリティ対策が徹底したこと，およびセキュリティ監査が実施されるようになったことなどから，現在は落ち着きをとりもどしている。

詳細については，第3章および第4章で述べる。

1.4.3 システム監査の日米比較

システム監査については，日米ともに，昭和50年に大きな動きがあった。わが国では，当協会のシステム監査委員会が発足し，米国では米国内部監査人協会

のSystems Auditability and Control Reserch Projectが発足し,双方とも非常に世間の注目をあびた。

しかしながら，システム監査へのアプローチについては，日米がまったくといってもよいほど異った方向をたどっている。わが国の場合は，理論づけや総論づくりに手をつけ，通産政策へと発展してきている。一方，米国では，各企業における具体的な取組みの積上げという方向で発展しつつある。

このような相違点はあるが，日米のシステム監査について実情を比較してみると，実施状況，システム監査人の設置などでかなりの格差が見られる。しかし，わが国の場合は，通産省が民間企業に対して，システム監査の普及，指導に乗り出していることなどから，今後，加速度的に米国へ近づくものと思われる。

詳細については第5章で述べる。

1．5　システム生産性概念の導入

今後の研究課題の1つとしては，システムの効率性の監査がある。これは，最近マネジメント側からとくに求められている事柄でもある。しかし，そのためには，まずシステムの効率性あるいは有効性についての測定基準が存在しなければならない。

これらの点について，技術的な側面からは，ハードウェア・モニタ，ソフトウェア・モニタ等々をはじめとして，各方面でシステムの性能評価に関する調査研究が進められている。しかしながら，マネジメント・サイドからの，経営効率を向上させるためのコンピュータ活用という観点からは，効率性の測定基準についても評価基準についても，一般的に通用している概念は存在しない。

そこで，1つの案として，他の多くの分野で普及している生産性をコンピュータ・システムにも適用することを考えてみたい。すなわち，新たに「システム生産性」という概念を構築することを提唱するものである。

たとえば，以下に述べるようなことについて，英知を結集し，一般的に通用す

る１つの指標を求めることが今後の研究課題であろう。

1.5.1　マクロ指標としてのシステム生産性

生産性とは，基本的には投入に対する産出の割合いである。したがって，投入に対して産出の割合いが高いか低いか，いいかえれば効率が良いか悪いか等を測る尺度として，生産性が高いあるいは低いといういい方をしている。

そこで，システム生産性を考える場合も同様に，システムの効率が良いか悪いかの測定を可能にしなければならない。そして，一般的に，かつ，簡単に利用できる方式が確立されれば，共通の方法で他との比較も出来ることになる。

まず，システム生産性を総合的にとらえることから考えてみたい。これは，前述の生産性＝$\frac{\text{産出}}{\text{投入}}$ をあてはめると，システムの総コストに対し，システムの総メリットの金額換算をすれば，つぎのようにとらえることができる。

$$\text{システム総生産性} = \frac{\text{システム総効果}}{\text{システム総コスト}}$$

この場合に問題となるのは，効果の把握の方法である。とくに効果を数量的に把握するためには，定量的な効果のみを金額換算することになり，定性的効果はプラス・アルファということにならざるを得ない。しかも，各業種によっても異るが，定量的効果の金額換算方法が明確にされなければならない。

効果の把握についてもう１つの問題は，これから開発しようとするシステムは企画段階で効果の予測をし，それを評価し，そのシステムを開発するかどうかの決定を下すための資料とされるべき点であろう。そして，運用段階においては，企画段階での予測と実績との対比がなされる必要がある。このように考えると，マクロ指標としてのシステム総生産性のほかに，個別指標としてのシステム生産性が必要になる。以下，これらの点について述べてみたい。

1.5.2　システム開発生産性

システム開発の生産性を測定する場合，いわゆる開発作業の効率についてはプ

ログラミング生産性を考慮することとして，ここでは，開発しようとする当該システムのコストや要員数と効果との関係でとらえてみるとつぎのようになる。

ⓐ　システム開発生産性（コスト）$=\dfrac{\text{システム効果}}{\text{開発コスト}}$

ⓑ　システム開発生産性（労　働）$=\dfrac{\text{システム効果}}{\text{開発要員数}}$

ⓒ　システム開発生産性$=\dfrac{\text{システム効果}}{\text{開発コスト}}+\dfrac{\text{システム効果}}{\text{開発要員数}}$

1.5.3　プログラミング生産性

プログラミングの生産性を高める方法としては，多々考え方があると思う。しかも，最近では生産性の問題だけでなく，プログラミング時におけるエラーや不正防止策等について，会計監査サイドからの要請などもあることから，一概に生産性向上のみを追求するわけにはいかないだろう。

そこで，一般的な目安ということにとどめれば，プログラミングの作業効率を測る単純な方法としては，プログラム・ステップ数に対する延プログラマ数という考え方がなりたつ。

$$\text{プログラミング生産性}=\frac{\text{ステップ数}}{\text{延プログラマ数}}$$

しかし，この場合でさえも，業務内容や使用言語などによっても異るので，いづれにしろ各企業別の基準を設ける必要がある。

1.5.4　オペレーション生産性

オペレーションの生産性については，考え方も多々あろう。まず，コストと効果との関連でみれば，すでに効率が悪くなり新システムを開発した方が良いとか，改善を要するとかの判断材料とすることができよう。

しかし，ここでは，あまり複雑なことを考えるよりも，現状を把握し，かつ，

改善の必要性や生産性向上の可能性等を，システム監査人が判断するのに役立つような観点からオペレーション生産性を考えてみたい。

(a) **生産性の回復**

システムの企画段階で予測された通りの生産性があがっているかどうかの評価が必要である。そして，もし予定の生産性があがっていなければ，原因を追求し，欠陥を発見して補修しなければならない。

(b) **生産性の維持**

システムは，状況の変化に常に対応し，生産性の水準を保つとともに，システム自体の陳腐化を防がなければならない。

(c) **生産性のアップ**

現行のシステムについて，もっと良い方法があれば，システムを改善して生産性をアップさせるように努めなければならない。

以上，簡単にオペレーション生産性の回復，維持，アップについて考え方のみを示したが，このように考えてみると，オペレーション段階においてはメンテナンスがきわめて重要なことになる。

そして，オペレーションの現状をコスト面から把握するためには，原価計算を実施することが必要となってこよう。

いずれにせよ，今後，ぜひともシステム生産性についての研究が関係各方面で進められることを願いたい。

第２章　システム監査と公認会計士監査の接点

第２章　システム監査と公認会計士監査の接点

２．１　会計処理システムをめぐる諸問題

公認会計士が行う監査は会計監査であるが，会計処理が従来の手書きからコンピュータ処理に変わることによって，新しい問題点が出て来た。つまり，公認会計士としては，コンピュータ処理過程がブラックボックスになり，監査証跡が得られなくなるので，何らかの措置が必要であるということである。

そして，これらの問題点を解消する１つの方策として，企業がシステム監査体制を確立し，自からシステム監査を実施することを望んでいる。

また，システム監査をめぐる公認会計士監査との調整問題については，昨年度の報告書「システム監査体制確立への道」でつぎのように述べている。

「公認会計士のおこなう会計監査は，端的にいえば，計算書類が法令や定款に従って適法に作成されているかどうかについて監査を行い，意見を表明することであるといえよう。

そして，システム監査との関連については，会計がコンピュータにより処理されている場合に，計算書類の作成過程，すなわち，会計処理システムにもとづく処理過程について，監査証跡が見読不可能な形に変ってしまうということが問題点として指摘されている。したがって，公認会計士としては，この部分についての信頼性を確認できるようにすることを望んでいるわけである。

企業としては，これに対応する必要があるから，システム監査人は，会計処理システムについては公認会計士との意思疎通をはかり，公認会計士の意図するところを十分に理解するように努め，調整をはかりながら監査の実施にあたることが望まれる。」

2.1.1　会計監査の位置づけ

システム監査における会計監査の位置づけについて考察してみたい。この場合，システム監査が実施されていることを前提とする。

たとえば，会計がコンピュータで処理されている企業で，自からシステム監査を実施しているとした場合，公認会計士は，当然システム監査の結果に興味を示すであろう。そして，満足であれば，コンピュータ処理過程での不正や誤謬がないことを前提として，原始伝票や計算書類にもとづき，従来どおりの会計監査が行われるということになるであろう。

もし，企業が実施したシステム監査の結果に公認会計士が不満である場合は，企業側と話し合ってシステム監査方法の改善あるいは充実がはかれることになろう。なぜなら，公認会計士としては，コンピュータによる会計処理過程が信頼でき，そこにおいて不正や誤謬の発生はないという確信を得られることが重要なポイントであるはずだからである。

このような場合，いずれにしても，公認会計士が財務諸表監査を行う際の危惧は，計算書類の作成過程である会計処理システムに限定されることになる。

すなわち，システム監査は，システム全般にわたって，マネジメント面，セキュリティ面，効率面等，有機的な監査を実施するわけであるから，ブレークダウンしていくと，個々のアプリケーション特有の問題は，それぞれアプリケーションごとに解決されなければならない。そして，とくに重視されるべきものの1つとして会計処理システムがあるといえよう。

したがって，システム監査人は，個々のシステム特有の問題点については自からのチェックポイントを明確にしておき，システム開発段階において必要なコントロールが組み込まれるように関与することが重要になってくる。

このようにしておけば，公認会計士が会計処理システムの信頼性を確認する場合にも，これらの点を重点にレビューすれば良いことになる。いいかえれば，会計処理システムについては，公認会計士が会計監査を実施して，財務諸表について正しい意見を表明できるようにするため，内部統制が確立され，システムの信

頼性を確認できるような手続きができていることが要求されているといえよう。

2.1.2 会計コントロール

会計がコンピュータで処理されている場合，正しい会計処理が行われるためには，どのようなコントロールが必要になるかを検討してみたい。

(a) 主要コントロール

まず，すべての条件を捨象して，主要なコントロールを日本公認会計士協会の内部統制質問書からとりまとめてみると，つぎの7つに大分類することができる。

①システム部門の諸管理

②プログラム・コントロール

③インプット・コントロール

④アウトプット・コントロール

⑤データ保護

⑥物理的セキュリティ

⑦システム監査体制

以上の①～⑥については，内容の差こそあれ，コンピュータを活用する企業は独自の必要性からコントロールしている事項である。したがって，コントロールの内容が十分であるか，あるいは不十分かという問題がある。

そこで，これらコントロールを徹底させるために，客観的な立場での評価を重視し，システム監査体制を整える必要があるとの考え方が表現されているといえよう。

コンピュータで会計処理を行う企業が，もし，仮に何らのコントロールもしていないとすれば，これらの主要コントロールはすべて，程度の差こそあれ，何らかの形で会計処理システムの信頼性に影響を与える性格のものである。したがって，万一，このようなケースがあるとすれば，これらの主要コントロールすべてを会計コントロールとして捉えられても仕方あるまい。

しかしながら，これらの主要コントロールは，コンピュータを活用する企業に

とって，必要欠くべからざるコントロールであり，かつ，現に存在するコントロールでもある。しかも，企業が自からシステム監査を実施している場合を想定すれば，公認会計士の行う財務諸表監査の際に必要となる会計処理システムの信頼性を確認するための会計コントロールは，きわめて限定されても良いということがいえよう。

(b) 会計コントロール

以上のような観点から，会計処理上のルールを十分に踏まえた上で，通常設定されているコントロールに加えて，会計処理システム特有のコントロールとしては何が必要かを検討してみたい。

前述の主要コントロールについて検討してみると，正確な会計処理を行うために直接的に影響を与えるコントロールとしては，インプット・コントロール，アウトプット・コントロール，プログラム・コントロールがあげられる。これらについては，会計処理のための十分なコントロールはいかにあるべきかを検討してみる余地がある。しかし，他のコントロールについては，コンピュータ・システム全般についての管理・運営上で必要とされるコントロールであり，会計処理のための特別な手当ての必要性は感じられない。

以下，この3つのコントロールについて述べる。

① プログラム・コントロール

会計業務の処理過程で，不正や誤謬が発生する余地をなくすため，いろんな会計処理上のコントロールをプログラムに組み込み，会計処理システムが稼動している時は常にこのコントロールが働くようにするのが，この場合のプログラム・コントロールの基本である。いいかえれば，会計データが処理され，計算書類が作成されるプロセスが，常に自動的に検証されている状態に保つことが中心になるといえよう。

具体的な個々のテクニックは別として，基本的には，システム・デザイン段階で必要なコントロールとして明確にされたものが確実に組み込まれていること，それが勝手に変更できないような管理下に置かれていること。もし，これ

らのコントロールが無視されたり出し抜かれたりした場合には，例外報告がなされるようになっていること。このようなことに十分に留意して，プログラム・コントロールが考えられなければならない。

② インプット・コントロール

インプットの正確性をチェックし確認するコントロールであり，インプット・データの取扱い手続き等も含まれる。コンピュータ処理の場合のエラーの大部分は，インプットにまつわって発生しているといわれており，とくに注意を要する点である。

したがって，技術的な面のチェック方法の採用と同時に，インプット・データの取扱い手続きが十分であるかどうか，それが遵守されているかどうか等の検証が必要となる。

③ アウトプット・コントロール

会計処理システムからのアウトプットに関するコントロールは，そのアウトプットが正確であるかどうか，アウトプットの取扱い手続きが確立され，遵守されているかどうか，必要な期間完全な形で保存されるようになっているか等が重視されることになろう。

以上，これら3つのコントロールについて，公認会計士が十分に信頼できると判断すれば，そこで作成された計算書類は不正や誤謬の入り込む余地がなくなり，正確であると判定することができることになる。

2．2　公認会計士の対応

日本公認会計士協会は，昭和51年9月，「電子計算機を使用した会計組織に対する内部統制質問書（改訂案）」，および「EDPシステムの監査基準および監査手続試案」を公表した。

これは，コンピュータ利用の普及にともなって，各企業で会計処理のコンピュータ化が進んできたこと。ならびに，金融機関等をはじめとして，オンライン・リアルタイム・システムが急速に普及し始めたこと，などのためにとられた対応策であるといえよう。以下，ポイントについて，批判を加えずに紹介してみたい。

2.2.1　内部統制質問書

この質問書は，全般統制，業務処理統制，安全統制，EDPシステム監査人制度の4つに大分類されているもので，質問は全部で130項目である。そして，質問に対する回答がイエスの場合，ノーの場合について，それぞれ補充質問が準備されている。

(a)　内部統制質問書の意義

この質問書は，昭和50年10月に公表された「電子計算機を使用した会計組織に対する内部統制質問書（案）」を改訂したものである。改訂案の特色としては，質問項目の分類体系を整理し直していることと，EDPシステム監査人制度を大きな柱の1つとしてとりあげていることであろう。

この質問書が公表されたことは，つぎの2つの点でコンピュータ・ユーザにインセンティブを与えた。1つは，現段階ではシステム監査に十分使用できる統一的な内部統制質問書的な性格のものが，監査する側にも監査を受ける側にも存在しない状況のもとで公表されたこと。もう1つは，明確にシステム監査に焦点を当て，公認会計士側から被監査会社に対して，素材として提示されたという点である。

(b)　内部統制質問書のねらい

この質問書については，“まえがき”にて単なる参考資料ではないとつぎのように述べている。

いうまでもなく，当「電子計算機を使用した会計組織に対する内部統制質問書（改訂案）」は単なる参考資料ではないので，監査人は積極的にその利用をはかり，また，EDPシステムを導入している企業は，EDPシステムに関する健全に

して良好な内部統制組織の確立のための参考に供していただくことを切望する。

以上述べられていることを簡単にいい直せば，公認会計士はこの質問書を積極的に使えということと，企業はこれを参考にして内部統制の充実をはかれということである。

(c) 内部統制質問書の性格

この質問書の使用上の留意点について，つぎの3点に注意しなければならないとし，その性格づけを明確にしている。

① この質問書は監査人が監査にあたって実施すべき監査手続の選択適用範囲を決めるために使用するものであり，会計監査基準懇談会より公表されている「内部統制の質問書」を補足するためのものであるが，言うまでもなくＥＤＰシステムとその適用はそれぞれ多様な内容をもっており，各被監査会社毎に異なっているので，この質問書の適用に際しては十分なる理解と適切な判断をもって当る必要がある。

② ＥＤＰシステムを利用している被監査会社がそれについて良好な内部統制組織を整備確立することは財務諸表監査の前提であり，監査人はその存在を本質問書を利用して確かめることになろう。しかし監査人は被監査会社の電子計算機の利用を阻害しないよう慎重な注意を払う必要があることは言うまでもないことであり，健全にして良好な内部統制組織の整備確立が促進されるよう積極的なアドバイス・指導に努めなければならない。

③ 本質問書は，質問（本文）とその補充質問から成りたっている。前者は，内部統制組織を評価する上で基本的に重要な質問であり，原則として調査・評価すべき問題を対象としている。後者は，前者の質問の対象となっている内部統制組織を評価する際の具体的質問内容の例示であり，補充質問である。従って補充質問については，監査人は適当に取捨選択し，また追加質問を設定する必要がある。補充質問のＹ，Ｎの記号は，前者の質問に対する解答が肯定・否定にそれぞれ対応するものである。

なお，前者の質問に対する答がすべて肯定であることが望ましいが，答が否

定であるからといって直ちに当該内部統制組織が悪いあるいは問題ありと性急に評価してはならない。被監査会社のフォローが適切になされているかを適当な補充質問によって十分に吟味した上で適確な評価をすべきである。

2.2.2 EDPシステムの監査基準等試案

前述の内部統制質問書と同時に公表された「EDPシステムの監査基準および監査手続試案」は，会計処理のコンピュータ化に公認会計士が積極的に対応していくための拠るべき基準を明らかにする必要があるために作成したとしている。

(a) 試案のねらい

従来の手作業による会計処理の場合の内部統制が人間の目に依存して行えたのに対し，コンピュータ処理の場合には，加えて機械化・自動化され，組織的計画的に行わねばならなくなる部分が多くなるので，EDPシステムの内部統制の評価が監査において重要となり，この試案が作成されるところとなったものであるとしている。

そして，つぎのようにものべている。ここでとりあえず当協会独自の「試案」の形で公表し，関係各位のご意見をいただき，監査実務での実際の適用の中から，一般に公正妥当と認められるものに昇華させ，さらに大蔵省企業会計審議会の「監査実施準則」との係り合いへの検討にまで進むことを期待している。

(b) 試案の性格

この試案では，“はじめに”でつぎのように述べ，その性格をかなり明確にしている。

企業の会計組織に電子計算機が使用されることによって，公認会計士ならびに監査法人が実施する財務諸表監査は，著しい影響を受けている。監査人は，変化する監査環境に積極的に対応し，財務諸表に対して正しい意見を表明することにより，監査人としての社会的責務を果さなくてはならない。

このためには，まずEDPシステムが企業の会計組織に如何なる影響を及ぼしているかを明確にすることを要す。かかる点につき概観すれば，

第1は，内部統制の態様の変化の問題であり，

第2は，会計記録の構造の変化と会計処理のEDP化に伴う監査証跡の問題であり，

第3は，監査手続ならびに監査証拠の実証力に与える影響からして，内部統制の重要性がますます増大しており，またシステムの信頼性を実証する上で確証的証拠による直接的実証が重要である。

これらの点に，監査人が積極的に対応していくためには，その拠るべき基準を明らかにする必要があるとの結論に達したことから，日本公認会計士協会は，ここに「EDPシステムの監査基準および監査手続試案」を作成した。

(c) システム監査人制度

この試案の内容は，第1章EDPシステムの監査基準，第2章EDPシステムの内部統制，第3章EDPシステムの監査手続，から構成されているが，第2章第5項にEDPシステム監査人制度がとりあげられている。

そして，同制度の整備確立が必要であるとし，同制度を欠いておれば，EDPシステムの内部統制に関する信頼性は保証されなくなると述べている。以下，この第2章第5項を紹介するとつぎのとおりである。

EDPシステム監査人は，内部監査制度の一環として，EDPシステムを監査対象とする内部監査人である。

EDPシステムにあっては，相互牽制機能の結合という問題ならびに監査証跡が必然的に残される保証がないという問題があり，かつ個々の適用業務を実行するEDPアプリケーションは常に流動的であることから，内部統制の諸項目に変更が加えられることが頻発している。それにもかかわらず，反復継続的に大量のデータ処理を行っているのであるから，内部統制の各統制に加えてEDPシステム監査人がEDP部門から独立しておかれ，EDPシステムの諸統制ならびにデータ処理の正確性について有効適切な内部監査を実施するEDPシステム監査人制度が整備・確立されていることが必要である。

とくに，会計手続をはじめ生産やマーケティングその他の経営情報までを統合

したEDPアプリケーション・システムの場合あるいはオンライン・システムの場合には，EDPシステム監査人制度を欠いているならば，EDPシステムの内部統制に関する信頼性は保証されないことになる。従って，かかる場合は，監査人は自己が満足するまで監査手続を拡張して，十分な証拠を求めなければならない。

以上のように述べており，企業がシステム監査人制度を確立し，独自にシステム監査を実施している場合は，公認会計士が行う試査の範囲が狭くなることを示唆している。

2．3　問題点と対応策

以上のべてきた会計処理システムをめぐる諸問題，ならびに公認会計士の対応から，問題点を整理してみたい。

2.3.1　公認会計士の懸念

昭和48年に米国で発覚したイクイティ・ファンディング事件は，大規模なコンピュータ犯罪として世間を驚かすと同時に，世界中の公認会計士に大きなショックを与えた。以後，日米をはじめとして，公認会計士のコンピュータ犯罪対策が急ピッチで進められたといっても過言ではない。

この事件の概要を述べると，イクイティ・ファンディング生命保険会社の役員と従業員23人が，3年間にわたって総額20億ドルにのぼる架空の保険証書を作成し，これを他の保険会社に再保険として譲渡し，自社の運転資金を調達しようとした大規模な詐欺事件である。

しかも，この事件をはじめとして，コンピュータ犯罪が，公認会計士の会計監査や内部監査で発見されるというケースはほとんどないことなどから，いきおいコンピュータ犯罪の元凶としてコンピュータ・システムの不備な面に一般の目が向けられるようになってきた傾向も見逃せない。

わが国の公認会計士の中には，これらの傾向をEDP会計が野放しにされてきたために起った弊害と指摘する向きも多い。そして，これらを正常な状態にもどすことが公認会計士の社会的責任であるとする意見が聞かれるようにもなってきた。

このような背景のもとに，前述の内部統制質問書等が公表されたわけであるが，公認会計士としては，コンピュータ処理の場合でも内部統制の確立が何よりも重要であるとの立場から，企業に対してコンピュータ・システムについての考え方を改めてほしいとの要請がこめられていると解釈することができよう。

2.3.2 公認会計士のアプローチ

会計処理がコンピュータ化されている場合の公認会計士の対応を，前述の内部統制質問書等から簡単にとりまとめるとつぎのようにいうことができよう。

まず，公認会計士の行う財務諸表監査は，内部統制が存在することを前提としているが，会計処理がコンピュータで行われたとしてもこの前提は変わらないこと。つぎに，コンピュータ処理過程がブラックボックスになっているが，何らかの手段でこれを把握できるようにする必要があること。さらに，コンピュータ・システム全般にわたる信頼性を確認するための1つの方法としてシステム監査人制度を確立して徹底させること。

そして，内部統制の充実度と公認会計士監査との間には，つぎのような関連性があることが明確になってくる。

① 内部統制が行われていない場合には，公認会計士が直接これらの監査を行う必要がある。

② 内部統制が不備の場合は，公認会計士の行う試査の範囲が広くならざるを得ない。

③ 内部統制が整備されている場合には，公認会計士の行う試査の範囲が狭くてすむ。

2.3.3　企業の対応

各企業が行うシステム監査は，企業経営のニーズにもとづいて，マネジメント面，セキュリティ面，効率面等，コンピュータ活用をめぐる総合的な監査である。したがって，その一部分として会計処理システムは当然含まれている。ただし，企業のシステム監査人は，会計処理システムについては公認会計士と調整をはかって問題解決にあたる必要があろう。

しかしながら，わが国の現状としては，1部の金融機関を除いて，ほとんどの企業がこれからシステム監査人を養成しなければならない状態であり，今後かなりの時間を要するところである。したがって，まず可能な部分から手をつけていくという対処の仕方が現実的であるといえよう。

第３章　米国における
システム監査の展開

第3章　米国におけるシステム監査の展開

米国では，1970年前後まで，コンピュータ業務に関する監査の必要性を売り込むのが非常に困難であった。その理由は，監査人に知識が欠けていたことと，システムを監査するという関心が低かったことをあげることができる。しかも，とくに問題だったことは，マネジメント層がシステム監査に対するニーズをあまり感じていなかったからである。

ところが，コンピュータ処理上において，非常に多額の損害を与えたエラーが発見されたり，イクイティ・ファンディグ事件のようなコンピュータを利用した大規模な詐欺事件が発生したことなどから，マネジメント側でもシステム監査に関心を示すようになってきた。

しかし，この詐欺事件は，システム監査の重要性を認識させたという点で大きな意味をもっているが，システム監査という観点からは詐欺というのはあまり大きな意味をもたない。すなわち，確率的にひん度が多く，しかも金額的にも大きな損害を与えることになる可能性が高いプログラミング上のエラーとか，あるいはＩ／Ｏコントロールがうまくいかないとか，ユーザ側で処理の誤りを発見できないとか，これらのことの方がシステム監査としては重要である。

アメリカの法律では，役員と監査人が株主に対して責任をもっており，もし職務怠慢があれば株主から責任を問われる。だから，イクイティ・ファンディング事件の発生で，とくに，独立したコンピュータ・システム全体を監査するグループが必要であると感じられたわけである。

ＡＩＣＰＡ（アメリカ公認会計士協会）では，イクイティ・ファンディング事件が発生したのち，いろんなスタンダードを変更している。簡単に述べれば，各種の計算書類を承認するにあたっては，システム監査を義務づけようとする立場をとっているといえる。

このように，イクイティ・ファンディング事件を契機として，システム監査が大きくクローズアップされてきた。この事件が発生する以前はどうであったかといえば，公認会計士も内部監査人も，システム監査についてはあまり関心もはらわなければ重視もしていなかった。当時の監査人の監査の重点は，財務諸表監査に置かれ，コンピュータで処理された計算を，監査人が加算機を使って正しく計算されているかどうかを確かめるというようなことがあった。

3．1　システム監査人の責任

アメリカでもカナダでも同様であるが，内部監査人は，基本的には内部統制に関する専門家であると考えられてきた。しかし，本質は，内部統制の評価をすることについての専門家というべきである。

3.1.1　1960年頃の主要な3つの責任分野

(a)　設計段階における責任

システム監査人は，プログラマなどコンピュータ部門の人と接触しながら仕事をするが，その責任は，トップ・マネジメントに監査結果を報告することにある。

プログラマと一緒になり，各システムごとの問題点や，プログラム上のコントロールについてレビューする。また，欠点はないか，一貫性があるか，継続性があるか等についてレビューする。

その場合，システム監査人とプログラマとの間で，コントロールについて意見が一致しなかった場合は，その上の段階のマネジメントに問題をあずけ，たとえば，システム監査人の主張しているコントロールをシステムに組み込むかどうか等を上級管理者が決定するということになる。

システム監査人としては，コントロールの設計には責任がなく，設計されたコントロールの評価に責任がある。そして，必要なコントロールをつけ加えるとか，場合によっては取り除くとかの勧告をすることに責任をもっている。

つまり，システム監査人は評価者であって設計者ではない。かりに，システム監査人がコントロールを設計したとしたら，システムが稼動段階に入った時点では，自分のつくったものを監査するという立場になってしまう。システム部門としても，そういうことを受入れることは困難である。

システム監査人とシステム部門との意見がくい違った場合，当初は，コントローラが決定していた。しかし，コントローラは，企業において非常に重要なポジションであり，これらのことに全て携わってはおれない。そこで，財務，ユーザ，システム各部門とシステム監査人とで構成する委員会が設けられるようになり，委員会レベルで意見の一致をはかるようになってきた。

委員会では，コンピュータに関する知識のない人の意見がよく聞かれたり，その逆の場合の問題等も生じる。しかし，いつも問題が生じるわけでもないし，委員会のメンバ全員に，コンピュータの専門家であれというのも無理がある。

他の問題としては，システム監査人が“これは絶対に必要である”とか，“これについてはコントロールが多すぎる”というように判断した場合，委員会を飛び越えて，直接，上級管理者へ問題を持ち込むことがある。こういうやり方をすると，結局，そのシステム監査人は，人間として嫌われてしまう。

委員会方式での最初の誤ちは，システム監査人が，あまりにもプログラム上のコントロールに重点を置きすぎたため，インプット，アウトプット，エラー・コントロールが無視されるようなことがあった。

このようなことから，システム監査の責任範囲が広がり，システム全体を責任範囲として含むようになってきた。つまり，インプット・ドキュメントの作成から，アウトプットに至るまで，システム全体がシステム監査の対象とされるようになった。たとえば，ユーザが，そのアウトプットを本当に必要としているのか，あるいは実際に活用しているのか等も監査対象に含むようになった。

(b)　システム・テストに関する責任

システム監査人は評価者の立場であり，システム・テストのための手続きをチェックし，しかも，それが実際に守られているかどうかを調べる。システム監査

人の任務は，テストそのものにはなく，システムが十分テストされたかどうかを確認するところにその責任がある。

そこで，システム監査人としては，主に，テスト・データの作成，およびパラレル・テストについて関与していた。したがって，個々の具体的なテスト，およびデバッギング等については関与しなかった。また，インプット装置やテレコミュニケーションについても監査の対象となっていなかったが，これは，当時あまり利用されていなかったので含まれていなかったものである。現在では，これらの分野も含まれるようになり，監査対象が拡大している。

(c) データ・コンバージョンに関する責任

システム監査人は，データのコンバージョンに関するコントロールを評価する。ここでの主要な観点は，すべてデータが，1回だけコンバートされるということにある。

アメリカで非常に多い例として，データが全部コンバートされず，しかも，数カ月も発見されず，データそのものが破壊され，企業が大きな損害を蒙るということがある。

極端な例としては，670万ドルに及ぶ売掛金口座データのコンバージョンをわすれ，その分，会社が全部損をしたというのがある。しかし，この例については，税金を考えれば実際の損害は230万ドル位だから大したことはないという意見もある。

3.1.2 新たに加わってきた責任分野

アメリカで監査という言葉を使う場合は，定期的な検査，つまり，コントロールやポリシー，あるいは手続きに関しての定期的な検査ということを意味している。これに対して，日々おこなわれている場合には，監査とはいわず品質管理であると考えられている。

アメリカの企業では，システム監査人があまりにも日常業務に関与しすぎることがある。そのため，システム監査人が，内部監査部門所属というよりも，品質

管理グループのような形でオペレーションのコントロールをやってしまうという例が多い。ところが，監査というのは，あくまでも定期的な検査，チェックであるということをわすれてはならない。

1959年，南ニューイングランドの電話会社で，本来の意味でのシステム監査の最初の試みがなされた。つまり，当時は，何をやっているのか，あるいは実際に正しい処理が行われているのかが明確でない段階であった。

そこで，独立したシステム監査機構を置く主要な目的は，システムに関して，実際に独立した立場で評価をする機能を与えることにあった。経営者が求めるコントロール，手続き，あるいはポリシーが，確実にシステムに組み込まれているかどうかを客観的に評価させようということである。

しかしながら，企業のポリシーをシステム中にも取り入れて実現することは，ユーザおよびシステム部門の基本的な責任である。システム監査人の責任は，経営者が求めるポリシーや手続き等が，実際に，確実に実現されているかどうかを観察し確認することにある。

最近では，ますます内部監査人は企業内のコンサルタント的立場になると考えられるようになってきている。すなわち，コンサルタントとして，監査の対象部門に対してサービスを提供するという考え方である。

そこで，いろいろサービスを提供する場合，内部監査人は，経営者がどういうことに関心をもっているか十分に理解しておく必要がある。たとえば，全般的にコストがアップしているような状況の中で，経営者がコスト削減に主眼を置いているような場合には，内部監査人としても，とくにコスト削減に注意をはらう必要がある。つまり，内部監査人としては，企業の当面のニーズが何であるかを良く知ることが，良い仕事をすることにつながる。

そして，内部監査人を一種のコンサルタント的に考えるように変わってきたのは，システム監査人がシステム開発段階に関与するようになってきたことから発生してきたことである。

1950年代後半から60年代前半にかけて，システム監査人のそれまでの経験

にもとづいて，新しい責任分野が付け加わってきた。

(a) 品質管理への関与

とくに主要な傾向として，非常に多くのシステム監査人が，システム開発段階に関与することを通じて，従来は関与していなかった品質管理に関与するようになってきた。

しかし，システムの品質管理は，非常に重要な機能であり，監査機能に含まれるのではなく，他の独立したグループが独立の機能をはたすべき性格のものと考えられる。したがって，あくまでも品質管理監査の枠を踏みはずさないようにしなければならない。

(b) ポリシー，法律等への準拠

つぎに，設計中のシステムが，企業のポリシー，手続き等に合致しているかどうか，また，税務関係などの要件を満たしているかどうか，全体的な立場での確認をする必要が出てきた。

たとえば，企業のポリシーとして，品物を納品してから10日以内に現金払いをする場合には，一定率で割引きをするという方針をとっていれば，そのようにプログラムで自動化されることになる。システム監査人は，これらのポリシーがシステムの中に組み込まれているかどうかを確かめる機能をはたさなければならない。

また，外部の要件としては，たとえばIRS（内国歳入庁）の要件として，会計資料の保管義務があり，税務監査を可能にしておくことが必要である。

結局，準拠性についてのシステム監査人の責任は，システム部門に対して独立した立場からの援助，つまり評価を与え，確かにポリシー，手続き，その他の要件が満たされているということを明確にさせる役割りである。

(c) 監査性の向上

監査性（Auditability）とは，設計されたシステムが稼動段階で監査可能であるかどうかの問題である。つまり，システム監査人は，システム設計段階で，システムが稼動段階に入った場合に監査できるようになっているかどうかを確認する必要がある。

したがって，このための手続きとしては，システム部門がドキュメンテーションをやるのと同様に，システム監査人もドキュメンテーションをやる必要がある。そして，稼動段階でシステム監査をする場合に，当初設計されたコントロールが除去されることのないように確かめる機能などが出てくる。

すなわち，システム開発段階での監査性を考えてみると，監査のための道具建てが出来ているかどうかということになろう。たとえば，ソフトウエアがあるかどうか，テスト・デックがあるかどうか，もしある場合にはそれをいかにして使うか等も含まれる。

3．2　システム監査をめぐる諸問題

システム監査人の失敗の多くは，システム開発に対するアプローチの際のデータ分析や，これまで経験したことのない新しい分野の監査をいかに実行するか等に起因するものである。

現在，アメリカで使われている監査技術は，ほとんどが1960年代の初期までに開発されたものであり，それ以降に新技術の開発は見られない。

その理由としては，IIA（米国内部監査人協会）やAICPA（米国公認会計士協会）などのリーダーシップが弱いことがあげられる。これらの組織は，誰れかが何かやってくれるのではないかと考えているらしい。その後，2つの専門家の組織ができた。1つは，EDPオーディターズ・アソシエーションであり，他はアソシエーション・オブ・バンク・オーディタである。後者は，BAI（Banking Adominis tration Institute）に統合された。

とくに，イクイティ・ファンディング事件が発生して以来，これらの協会やコンピュータ・メーカでは，セキュリティについての関心が非常に高まってきた。そして，何らかの形でこの分野に関係する人が多くなってきているが，実際にやられていることはあまりない。

システム監査について，現在アメリカで行われている1つの方向としては，シ

ステム監査人がシステム設計段階から関与して，評価をし，コントロールの弱点や監査証跡の問題などをシステム部門に教えるというようなことをやっている。このアプローチは，システム部門に対するサービス，つまりインプットを与えて，システム設計のための情報を提供するというサービス機能にあたる。

もう１つのアプローチは，フィジビリティ・スタディ段階で，その妥当性を監査する方法がとられている。このようなやり方で発見されることは，システム部門が導入しようとする機能が経済的に妥当でなかったり，予測される経費節減などのメリットが水増しされていることがしばしばある。

また，ユーザがシステム開発段階に十分関与していないような問題や，当該システムに対してシステム部門要員の技術的能力が不足していることなどもある。

さらに，新規導入のためのスケジュールが非現実的である場合が多々ある。これは，スケジュールが固定的なため，最終段階になって日数がたりなくなっても，予定したスケジュールどおりに開発作業を終了させなくてはならないために，テストが十分なされなかったり，バグがたくさんあったり，インプット手続きが不十分であるなど，スケジュールに柔軟性が欠けているため生じる問題がある。

これは，システム部門のみに責任があるとは限らないわけで，たとえば，社長が１２月中に稼動させると発表したりすると，本来は翌年の６月中が妥当であるにもかかわらず，社長がいった非現実的なスケジュールである１２月中稼動に固執するというような問題が起こる。

このような場合は，非常に解決が困難になる。なぜなら，社長を相手に説得しなければならないからである。効果的な方法としては，システムのデバッグやテストが十分でないため，何らかの損失が発生して株主から訴訟を起された場合には，役員がシステムのコントロールを十分に果たしていなかったという責任を負わされるであろうことをレポートとしてトップへ提出することである。

その他，最近の顕著な傾向としては，パフォーマンス・エバリエーションをシステム監査の対象に加えていることである。しかし，これは今後の研究課題であり，現段階で一般的な方法が確立しているというものではない。

3.2.1 組織問題

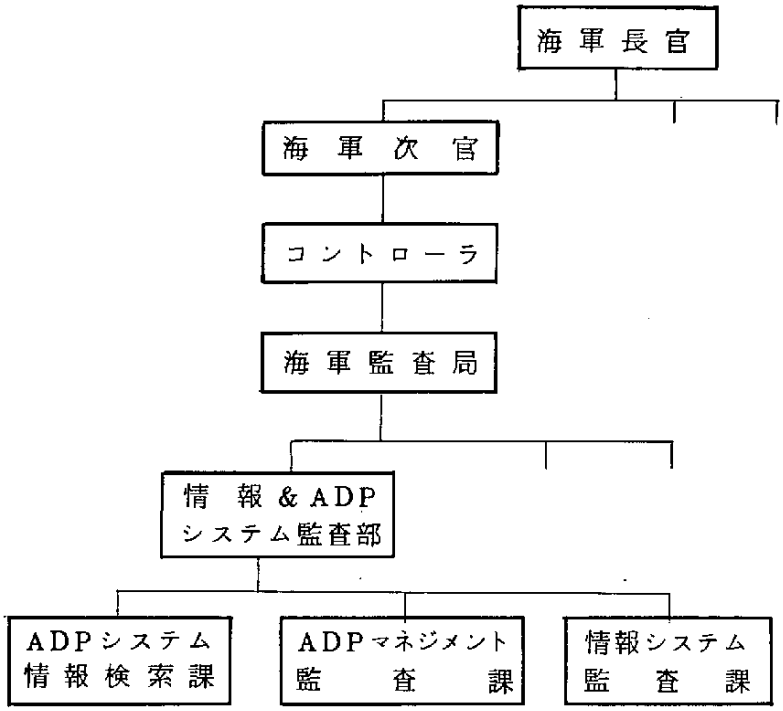
アメリカの海軍監査局（Naval Audit Service）は，1973年，コンピュータ・スペシャリストで構成する情報＆ADPシステム監査部（Information and ADP Systems Audit Division）を発足させ，システム監査で効果をあげている。

同局は，海軍関係の1,000以上のコンピュータ・システムを監査しなければならない立場にあるが，現在，すべて監査を終えたという状況ではない。しかしながら，これまでに行われた監査の結果で，成果をあげているケースもある。たとえば，3台のコンピュータが設置されていたが，システム監査の結果，1台で十分との結論が得られ，そのような勧告を出して，実際に2台のコンピュータが撤去された例がある。

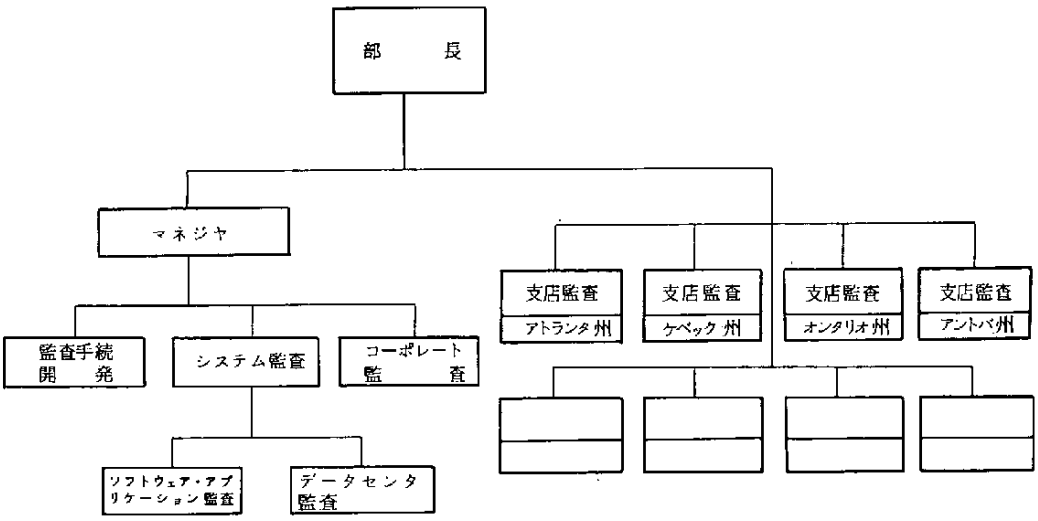
この海軍監査局の場合，監査人は監査の専門家であってコンピュータの専門家ではない。一方，情報＆ADPシステム監査部のスタッフは，コンピュータの専門家であって監査の専門家ではない。したがって，システム監査の際には，監査人があくまでも監査を行うが，コンピュータの専門的知識や技術，あるいは監査ソフトウエアを使う場合に，同部のスタッフがサポートするという形式をとっている。

このような方法は，海軍が大規模なためにとれるものであり，民間企業の場合は同様に考える訳にはいかないと思われる。そこで，海軍監査局の情報＆ADPシステム監査部，および，民間企業の例としてロイヤル・バンク・オブ・カナダの内部監査部門の組織をつぎに示す。（3－1図，3－2図）

とくに，ロイヤル・バンク・オブ・カナダの例は，アメリカのビック・ビジネスでもよく見られる形式で，内部監査部門のスタッフが，①監査手続開発グループ，②システム監査グループ，③会計および業務監査グループ，に大別できる例である。



第3.1図　海軍監査局の組織



第3.2図　ロイヤル・バンク・オブ・カナダの内部監査部門組織

3.2.2 報告制度

システム監査の結果は，報告書にとりまとめ，トップへ提出することになるが，その場合にも業種によって，あるいは企業によって報告のルートが異なる。また，報告の内容については，システム部門の意見が正しいと考えたら，それをとり入れた形の報告内容になり，その場合にはマネジメント側を説得することになる。したがって，監査人の資格としては，非常にしっかりした考えを持ち，場合によっては戦いも辞さないという姿勢のとれる人ということになる。

内部監査部門のマネジャが誰れに報告するかについては，通常の場合はコントロール担当の副社長，財務担当の副社長，あるいは会計担当の副社長などに報告している。しかし，銀行の場合は，内部監査部門のマネジャが内部監査担当の副社長である例が多く，したがって，この副社長が報告する相手は社長，筆頭副社長，あるいは役員会などである。

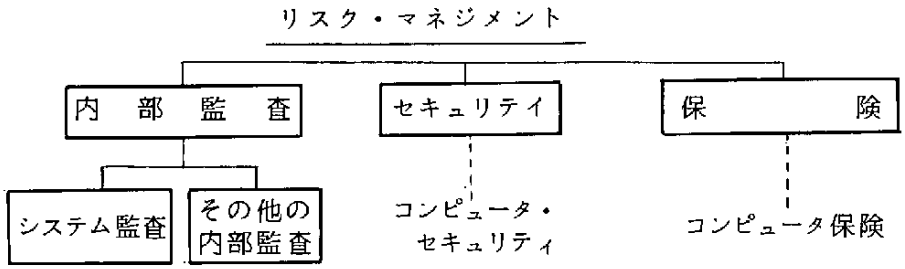
また，財務担当の副社長に報告するような場合，実際には，財務担当者に監査結果を報告し，その担当者が自分の上司である財務担当副社長に報告するようなケースが多い。

3.2.3 リスク・マネジメント

リスク・マネジメントには3つのファンクションがある。すなわち，内部監査，セキュリティ，および保険のマネジメントの問題ということができる。保険については，データ処理，データ・セキュリティ等の保険ではなく，災害における保険を買うという考え方である。

このような形態をとる利点は，まず，システム監査の独立性を保つことが出来るし，セキュリティの分野，保険の分野等のリスクとして考えられる項目を，独立して見出すことができることにある。

リスク・マネジメントをめぐって，アメリカの企業が現在直面している問題は，コンピュータ・システムのリスクがうまく計算できないことと，トップ・マネジメントが情報の価値を十分に認識していないことである。



第 3.3 図　リスク・マネジメントの形態

システム部門の管理者が，もしコンピュータ・システムの価値を十分に認識していないとしたら，どのようにしてコントロールやセキュリティを十分設計できるのか，これはきわめて重要なことである。

たとえば，自動車に保険をかける場合に，自動車の値段がわかっていて，保険でいくらの保障を得られるかということになる。これは，コンピュータ・システムのコントロールやセキュリティを設計する場合にも同様である。すなわち，その価値がわかっていて，保険に加入する際には，何か事故が起った場合に，その保険でどれ位の保障が得られるかを比較検討しなければならない。

これらの実際の価値を決めるのは，システム監査人そのものの役割りではないが，コンピュータ・システムの評価がやられてなく，その価値がわからないという場合には監査人としてトップ・マネジメントに指摘する必要がある。

3.2.4　監査部門の規模

アメリカの企業における内部監査部門の規模は，大体１人から３０～４０人程度までである。この場合，監査人の数を決めるのにルール的なものは何もない。ただ，ベル・システムでは，電話設置４万台について内部監査人１人という規定を持っている。

したがって，通常，内部監査部門の規模を決定するためには，１年間を通じてどの程度の範囲の監査と，具体的なプログラムを持っているかによるであろう。

内部監査部門におけるシステム監査グループの規模を決める場合に考慮すべき

要素は，アプリケーションの数，開発中のアプリケーションの数，インストラクションの数，新しい監査技術を開発するための研究開発の量，他の監査人に提供すべき情報収集の量，などである。

アメリカにおいて最も深刻な問題になるのは，システム監査人が１人しかいない場合でも，彼は他に給料の良い職場があれば転職してしまい，その企業にシステム監査人が１人もいないという状態になることがある。

アメリカでは，日本の従業員のように企業に対する忠誠心はない。アメリカ式の忠誠度は企業が自分にどの程度の給料をくれるかで決まるといってもよい。したがって，システム監査グループの規模も，システム監査人がどれだけ仕事をしたいかという意欲によって決まってくるともいえる。

3.2.5　システム監査人の養成

アメリカでは，1960年代の初めから，最も良いシステム監査人はどのようにして得られるかという問題が論議されている。つまり，内部監査人にコンピュータの訓練をするのか，システム部門の要員をシステム監査人に育てるのかということである。

基準というようなものはないが，内部監査人をシステム監査人に育てる場合には，その適性がなければならないことと，システム監査をやってみたいという意欲を持ち，意志堅固でなければならない。

一方，システム部門の要員をシステム監査人に対する場合には，監査をやりたいという欲求を持ち，その適性のある人でなければならない。システム部門要員の１つの問題点は，ユーザに売込めるようなシステムをつくるという方向に走り，客観的な評価者であることを忘れてしまう点である。

以上のようなことから，システム監査人を養成するにあたっては，システム監査の仕事をしたいという欲求があることと，監査技術についてもコンピュータについても能力を持っていることが基本的に必要であるといえる。

内部監査人の訓練は，これまで１対１の関係で，年輩の経験豊富な監査人が経

験の浅い若い監査人を訓練してきた。これは，アメリカにおける伝統的な監査人の訓練方法ともいえるもので，経験をもつ者が自分の知恵を若い者に授けるということである。しかし，このような方法では，全部教え終った頃には，若い方の監査人も年をとってしまい，同じことの繰りかえしになってしまう。したがって，もっと早く経験が伝えられるように望まれるところである。

従来，システム監査人の機能は，きわめて重要であるという認識はあったが，監査人の側がマネジメントに対してそれを売り込めなかったという問題があった。アメリカでシステム監査がマネジメント側に重視されたのは，不幸にもイクイティ・ファンディング事件が発覚した後である。

したがって，このようなことからシステム監査人が学ぶべきことは，自分達が監査で発見したこと，および勧告等について，もっとマネジメント側へ売り込めるようにすることであろう。

3．3　コントロール・ギャップをいかに埋めるか

非常に単純・簡単な部分で，どのような問題が出てきているかについて述べる。

3.3.1　処理手続き

アメリカでは，インプットの操作で主な不正が起っている。すなわち，これまでシステム設計段階で基本的なミスがあった主な部分は，データ準備，およびインプットのコントロールが十分に準備されていなかったからである。

不正や情報の紛失，および不必要なデータの混入を防ぐ唯一の方法は，データのインプット段階での準備にかかわっていると思われる。

したがって，まず，すべてのデータが受け入れられること，そして，すべてルールに従って処理されるようにすることが必要である。また，そのためには，その情報を受け取る側で積極的にコントロールの方式を持っていることが必要である。

3.3.2　データの承認

すべてのデータが承認されていることが必要である。そして，この部分で詐欺が起りやすい。

たとえば，ニューヨークのあるデパートの社員が，自分のクレジットのデータを調整し，自分の買った物については請求書が出されないようにしてしまった事件があった。これはアメリカでよく発生する形態の詐欺事件である。そして，これらによる金銭的なロスは膨大な額になるものと思われる。

これらの分野では，新しい規制方法というものは何もない。これまでと同様に，きわめて基本的なコントロール方法で防止しなければならない。つまり，権限，仕事を分離すること，データの流れるプロセスを管理すること，品質管理を行うこと等々，なんら新しいテクニックはない。システム監査人としては，この分野に十分な注意をはらい，不正が行われないようにしなければならない。

3.3.3　データの再生能力

予期せぬ出来事が起った場合にそなえ，データを再生できる能力を備えていなければならない。たとえば，銀行取引きに関しては，小切手がある支店から他の支店へ渡されるような場合にマイクロフィルムで情報を保存している。

この分野に含まれる問題点としては，エラーの訂正がインプット・グループ内部のみで行われ，そのレポートが出てこないため，誰れがどのようなエラーを犯したかがわからないケースが多い。したがって，このようなエラーに関しては報告システムをつくり，ソース・データを準備する人々を管理できるようにしなければならない。

これらは，きわめて基本的なことであるが，各企業はこれらの基本的なことをもう一度チェックし，それらがなされているかどうか，なされているとしたら適正になされているかどうかチェックする必要がある。

このようなチェックをやってみると，不正が起るのは，基本的なことがうまくやられてなかったり，だらしなくやられていたり，あるいはコントロールに誰れ

も目を光らせていなかったり，というようなことに多くの原因があることを発見できる。

3.3.4. コントロールの方法

コントロールについて，現在，可能な方法について述べる。

(a) 自己監査（Self Audit）

アメリカでは，自己監査ということが良くいわれる。つまり，システム部門が自らシステムをチェックあるいは評価することである。

(b) 文書化

マニュアル部分についてのコントロールは，その手続きが十分に文書化されていることが必要である。しかも，それは実際に使用する人のレベルで十分理解できるものでなければならない。

(c) フォームの統一化

たとえば，プレコードするなど，フォームを標準化することによって，エラーを減少させ，かつ，処理スピードをあげることができる。

エラーが発見された場合には，標準方式との関連でどうなのかまで検討する必要がある。つまり，正確度を上げるために方式を変更すべきかどうか，についての検討も必要である。

(d) シリアル・ナンバ

データの紛失等を防ぐために，フォームには一連番号をつける必要がある。とくにアメリカ人は，何にでも連続番号をつけるのが好きである。ところが，やたらと番号をふりかざしてコントロールが全然なされていない場合がある。この連続番号をつけるべき書類は，データの性質によって異るものである。

(e) コントロール・トータル

コントロール・トータルには，まったく意味を持たないものもあるので，これは，有意なコントロール・トータルということである。つまり，意味のある分野からとった価値あるコントロール・トータルを使うことが必要である。

(f) 品質管理

アメリカの場合，品質管理グループがあり，データの管理についてチェックする。場合によっては，インプット・プロセスについてもチェックするので，部門から部門へのデータの流れるプロセスにおけるコントロールもチェックすることになる。

アメリカでは，キーパンチ・システムをなるべくやめて，キー・ツー・ディスク，キー・ツー・テープなど，もっとコントロールしやすい方法に変ってきている。

(g) ＯＣＲ

ＯＣＲ（Optical Character Readers）は，残高等の情報を調べるのに非常に簡単な方法である。これは，ソース→カード→テープのカードが省略されて，ソース→テープという形の処理形態である。

アメリカの銀行では，預金の預入れ伝票にＯＣＲを多く使って合理化をはかっているが，一方では，ＯＣＲをうまく活用した詐欺事件も発生している。

ある男がニューヨークの銀行に行き，高額の小切手を振込み，振込用紙をたくさん欲しいと依頼した。そこで，銀行の担当副社長が，依頼に見合う振込み用紙を新しい顧客であるその男に渡した。その男は，副社長に対して，自分の預金残高がどうなっているのか毎日チェックするようにたのんだ。その理由は，毎日，多額の預金を引出すことになるだろうからということであった。

この男は，振込み用紙を持ち帰り，口座番号欄に自分の口座番号を記入し，同銀行のいろんな支店へ行って，その振込み用紙を置いてまわった。

一般の顧客は，預金用の振込み用紙が置いてあるので自分の預金をするつもりで，その用紙に口座番号を書き，現金といっしょに窓口係に渡した。ところが，振込み用紙の口座番号欄には，光学的に読み取れる犯人の口座番号が刷り込んであるので，その通りに処理され，多くの顧客の預金が犯人の預金口座に集められた。

犯人であるこの男は，毎日，副社長に電話を入れ，預金残高を確かめ，入金し

た預金を現金で引き出すということを繰り返していた。4日後，銀行側でこれはおかしいということになったが，その時には犯人はすでに消え去っていた。被害総額は10万ドルにも及んだ。

アメリカでは，このような事件が何度も発生している。しかも，最初の事件の全貌が明らかにされたにもかかわらず，他の銀行が適切な処置をとらなかったために，各地で同様な事件が多発した。ただ，同一人物が全部の犯罪を犯したのか，それとも，新聞等で事件を知った他の誰れかが，まねをして犯した事件なのかについては明らかではない。

(h) バッチ・コントロール

バッチ・コントロールについて，システム監査人は，とくにバッチのサイズに十分注意しなければならない。

たとえば，バッチ処理の際に，小切手とカードを確かめるとした場合，その件数が2,000以上であれば，その間のバランスをとることが非常に難かしい。したがって，バッチのサイズを80トランザクションに減らし，その調整がとれるようにすること等が必要になってくる。

(i) プログラム・コントロール

プログラム・コントロールに関して，システム監査人に期待されていることは，現在あることになっているプログラム・コントロールが実際に存在するかどうか，それが適切であるかどうか，コントロールのやりすぎはないかどうか，重複はないかどうか，などを監査することである。

実際にプログラム化されているコントロールの正当性や正確性を，とくにエラーが沢山みつかった場合に見るためには，インプットの質を見るのがよい。

プログラムの正当性あるいは論理性等をチェックするためには，基本的にはデザイン段階で十分なテストがなされたかどうかを見ることが第1である。つぎに，現行のシステムとパラレルに処理してチェックすること，および沢山のトランザクションを入れてテストしてみること等が考えられる。

(j) エラーの検出と報告

第二世代のハードウェアでは，システム内のエラー検出のコントロールが非常に悪かった。実際にエラー検出のためのコントロールをデザインしてうまくいかなかった場合には，マシンを止めてしまうということも起り得た。問題は，システム中のエラーの量が大きかったために，何とかしてエラーをコントロールするシステムをさがさなければならなかったわけである。

理想的な形としては，たとえば，システム自体で1日に5,000件のエラーを検出したとしたら，コントロール・グループがその5,000枚のカードを書き直して，それをシステムにもどして再処理すれば問題はない。ところが，問題なのは，エラーのすべてが簡単に訂正できるとは限らないし，場合によっては訂正が不可能なエラーもある。同時に，実際になぜこのようなエラーが発生したのか，誰れがそのようなエラーを起したのか，というような有意な統計が出てこないという問題もある。

ベル・システムで開発されたエラー・コントロールの例では，毎月，エラーのテープがつくられ，それに関するコレクションのカードやレコードがプリントされ，エラー訂正グループに送られて，エラーのマスター・ファイルがつくられる。

このマスター・ファイルによって，すべてのエラーに対するコントロールを確保したわけである。すなわち，エラーの訂正がなされて，マスター・ファイルに送られ，その分のレコードが消され，メインのプロセスにもどって再処理をし，エラーを訂正するという形である。

つぎに，エラーがシステムの中で，どの程度の時間エラーとして留まっていたかを読み出し，レポートする機能を付加した。たとえば，エラーが40日間訂正されないまま残っていたとすれば，そのようなレポートが出るようにしてある。

カードが何かの理由で紛失したり，意図的に壊されたりした場合には，どの程度の数のエラーがあったかを再確認して新しいカードにつくり変えることができた。

このシステムは，どこから，いくつのエラーが検出されたかわかるレポートが

出るようになっている。しかし，誰れがエラーを起したかということまではわからなかった。

そこで，誰れがエラーを発生させたかを記録する報告機能を付け加えた。つまり，ソース・ドキュメントを準備すると同時に，それを準備する人がカードを準備して自分の従業員番号を記入するようにした。これですべてのレコードの一部分として，そのソース・ドキュメントをつくった人の従業員番号が記録されるようになった。

以上により，各人がどれ位のドキュメントを準備したか，どの程度のエラーを発生させたか，どの分野でエラーが発生したか，などがわかるようになった。

結局，これはＭＩＳという形になった。もし何かエラーが発生したような場合に，誰れがその従業員に対して責任があるのか，彼は再訓練の必要があるのか，教育・訓練が適当であったかどうか，などの情報が出てくるようになり，教育・訓練のやり方にフィードバックされるようになった。

このようなシステムを開発することによって学んだことがある。第１は，標準化されたフォームに固定的な弱点があることによって，その部分で非常にエラーが多くなるということであり，フォームを変えたことでエラーがかなり減少した。第２は，クラークの教育・訓練プログラムの弱点がわかった。第３は，知識的なメリットという意味で，誰れが企業にとって良い人間，役に立つ人間になるかということがわかった。

このシステムは，通常のオペレーションにおいて大量のエラーが発生する可能性があるようなシステムのタイプに活用することができる。エラーの量が少ない場合，このようなことをやるのは無意味である。

このシステムを最初に導入したのは，電話料金の徴収システムで，トランザクション量が１日２万件，そしてエラー率が初期において１７％と非常に高かった。このシステムを導入してからは，エラー率が 2.1 %まで低下した。

(k)　エラーの修正

誰れがエラーを修正するかについては，アメリカの場合，コントロールがうま

くいっている企業では，エラー・コレクション・グループをつくり，エラーを修正することだけが責任というやり方をとっているところがある。

そして，この修正グループだけが，エラー修正についての権限を持つようにしてあり，システム部門要員が修正することを禁じている。なぜなら，その要員が何か悪いことをしようとする場合に弱点をさらけ出すからである。

ニューヨークのある銀行でつぎのような詐欺事件が発生した。この銀行では，顧客の口座にエラーが発生した場合は，その支店のヘッド・テラー（窓口係の長）が修正するという方法をとっていた。このような立場にあるヘッド・テラーが，いわゆる睡眠口座から預金を全部，新しい口座に振り込み，さらに金額を増し，それで競馬，バスケット，野球などに賭けていたという事件が発生した。

このヘッド・テラーが，なぜこのようなことができたかというと，彼はインプットについても，アウトプットについても，修正についても，全部自分でやるという立場に置かれたわけである。

アメリカの新聞などは，この事件をとりあげて，わずかの給料しかもらっていないヘッド・テラーが，高価なコンピュータを出しぬいたというような報道をした。しかし，これはもっと単純な問題であり，コンピュータそのものには関係のない，基本的なコントロールの問題であった。すなわち，内部統制がうまくいっていない，基本となる責任分割がやられていない，というところに問題がある。

この場合も，全然コントロールがないというのではなく，1つはあった。それは，テラーとして何か非常に例外的な事態が発生した場合には，マネジャに報告しなければならないという規定である。しかし，2万ドルや3万ドルの調整は，この支店では通常やられていたので報告がなされなかったわけである。

第4章　米国における
セキュリティ対策

第4章　米国におけるセキュリティ対策

米国におけるセキュリティ問題の高まりは，昭和44年，カナダはモントリオールのサー・ジョージ・ウイリアムズ大学のコンピュータ・センタが，学生により破壊されるという事件に端を発していると言ってもよい。

その後，全米各地の大学で，学生運動の高まりと同時に，学生によるコンピュータ・センタ破壊事件が多発した。一方では，コンピュータ利用の発展にともなって，コンピュータ犯罪が発生するところとなり，コンピュータ・システムをめぐるセキュリティ問題が大きくクローズアップされ，その対策が各企業で具体的に進められるところとなった。

このセキュリティ問題を，システム監査の観点からとらえると，セキュリティ自体については，その対策を講じるのはシステム部門の仕事であるが，その対策がうまくいっているかどうかを客観点に評価するのはシステム監査人の仕事ということになる。

4.1　リスクのタイプ

リスクにはどのようなタイプがあるかといえば，最も多いのがエラーである。これまで発生した事例の数からいっても，悪意の介在しないエラーによるリスク問題が例としては多い。

つぎのリスクは，悪意によるもので，コンピュータあるいはデータ等に対して，何らかのダメージや損害を与えようとする意図によってもたらされる破壊行為等である。

第3のリスクは，利得を目的とするもので，当人あるいは第三者に利得を得させるために行われる行為である。

第4のリスクは事故である。これは，地震，洪水などの自然現象が中心で，企業自身ではコントロール出来ないリスクである。

以上のように，大別して4種類のリスクがあるが，これらのリスクをいかに分析し，いかに管理して，その顕在化を防止するかという問題が出てくる。

4．2　リスク・アナリシス

このようなリスクは，あらゆるコンピュータ・センタに共通して存在するが，やみくもに心配する前に，一体どのような可能性でこれらが顕在化するのか，その確率はどうか等について検討しておく必要がある。

まず，どの程度の可能性をもってこのようなリスクがあるのかを検討し，それを評価して，潜在的リスクを検討する。そして，それに対する対策を検討することになる。

つぎに，リスクの発生する可能性の検討から，実際に発生した場合の結果はどのようになるかを予測し，どういう損害が発生し得るかを検討する。

さらに，その影響の度合は，どの程度の深刻な問題になるかを検討し，そのようなケースの発生する可能性を全体的な立場から評価する。

最後に，このようなリスク，それにともなう損害という観点から，それに対する保護対策を検討する。以上が，リスク・アナリシスの手順の概略である。

そこで，つぎはリスクをさけるための保護手段を講じることになる。まず，どの程度のコストがかかるかを評価し，保護措置を講じることによってリスクがどの程度減少するかを検討する。この場合の基本的な考え方は，保護措置を講じることによって得られる価値と，そのために要するコストを対比して評価し，保護措置のレベルを決定するということになる。

4.3 サイト・セキュリティ

サイト・セキュリティとは，主として天災や事故からコンピュータ・システムの場所を保護することである。まず，場所に関するリスクにはどのようなものがあるか，そして，それを最小化するためにはどのようにしたらよいか，などが問題になってくる。

4.3.1 コンピュータ施設に関するリスク

コンピュータ・システムおよび関連する諸設備を，天災や事故から守るわけであるが，まず，どのようなリスクが考えられるかを明確にしなければならない。

(a) 扉・窓

建物の構造で，扉，窓，壁などは，外部からの浸入口ともなるため，通常の建物とちがって物理的に保護する必要がある。

(b) 水

水の問題としては，建物内でのパイプの破裂，スプリンクラの故障，下水の逆流，洪水などが考えられる。

たとえば，コンピュータ・センタの2階にマシンが設置してあると仮定した場合，2階と3階との間で，マシンの直接上をトイレのための水道管が通っていることも考えられる。この場合，もし地震が起ったら，その継手がゆるんでマシンの上に水がもれてくる可能性がある。

それから，洪水あるいは下水が逆流してくる可能性があれば，排出するためのポンプの設備がないと，水がたまってマシンに損害を与えることが考えられる。これは，高いビルの場合，とくに問題である。なぜなら，ポンプは地下には設置してあっても，上層部にはないのが普通である。

(c) 雷

雷の問題については，通常は避雷針があるので，建物そのものが損害を受けるということはない。しかし，避雷針を通じて電流が流れる場合に，瞬間的にでも

強力な磁場が形成されると，コンピュータが非常に影響を受ける可能性がある。それに，空調，電気，通信関係などが故障する可能性もあり，それによる損害が考えられる。

(d) 煙

空気を正常に保つ必要がある。たとえば，他から出た煙を吸い込んで，部屋中に煙が充満し，コンピュータをストップせざるを得ない事態になる可能性がある。

(e) 爆　発

これはガス爆発，ダストによる爆発，および悪意をもった者が意図的に爆弾を仕掛けるなどが考えられる。

たとえば，暖房関係のガスの配管が各階につながっている場合がある。また，マシン室の床に小さな紙屑等がたまっていると，非常に爆発性を帯びた空気になることがある。さらに，悪意を持った者が，爆弾をビルの外側に仕掛けたり，窓から投げ込んだり，部屋に侵入してマシンのそばに仕掛けたりというようなことがある。

(f) 火　災

床下の配線の不備から漏電をおこし，火災が発生して，データや機器類が燃える可能性がある。また，放火の危険性なども考慮しなければならない。

(g) 侵　入

建物には必ず入口があるが，いかなる場合にも，集団で，中にいる人間を圧倒して侵入してくる場合には，これを防ぐことが非常に困難になる。エントリ・コントロールをすれば，１人で侵入しようとすることを阻止できるかも知れないが，１００人が暴徒となって入ってくる場合には役に立たない。

すなわち，緊急事態が発生した場合には，従来やっていたような標準的な手続きは無視されてしまうということを考慮しておかなければならない。したがって，リハーサルしていないような事態が発生すると，対応策がないために，非常にリスクが大きくなるということがいえる。

4.3.2 リスクの最小化

以上のべてきたようなコンピュータ関連施設にまつわるリスクを，どのようにして最小化するか，まず，建物の設計から検討する必要がある。

(a) 建物の構造

考慮すべきことは，まず，ガラス窓をなるべく少なくすること，扉の構造を変えること，建物を補強構造にすることなどがある。また，給水パイプが機器の真上を通らないように設計したり，ビル内に特別な装置を設けて安全性を高めるようにするなどで検討の余地がある。

(b) 金　庫

水にも火にも耐え得る金庫を設けて，そこにテープやディスクパックを入れるようにすることも1つの方法である。

このような金庫を設計する場合には，とくに熱伝導に注意しなければならない。もちろん耐火性にはつくってあるが，熱が伝わると紙やテープにダメージを与える可能性があるので，その点を注意する必要がある。

(c) ポンプ

水が浸入したり，漏れたりしたような場合にそなえて，それを汲み出すポンプを適当な場所に備え付けておくことが検討の対象になる。

(d) サービス・ソース

電力その他のサービス・ソースを二重につくっておくことによって，サービスの切断によるダメージを最小限度に食い止めることができる。

アメリカの場合は，第2の電力源を別の方向からビルに入るような形にしたり，変電所や電力会社を別にするようなこともできる。また，自家発電装置の設置については，ディーゼル・エンジンを使って，スチーム・タービンでもガス・タービンでも動かすことができる。

停電の場合には，バッテリでコンピュータを動かせるように，バッテリを十分にストックしておくこともできる。

電流を均一に供給するため，あるいは急な停電や急に電圧が上ったりしたよう

な場合の緊急時には，はずみ車のようなものでも十分に発電機を廻すことができる。

エアコンについても，代替的なソースを持っており，緊急時でもマシン室だけは冷却できるような設備になっていることが多い。

(e) 通信施設

通信用の施設は，最近のコンピュータ利用にとって欠かせないサービスであり，しかも移動させることが難かしい。

その場合，代替的な第2の通信源を別のビルに置き，マイクロウェーブかレーザで伝達し，そこからは通常の通信回線に継ぐということができる。

(f) エアコン

エアコン装置については，たいてい自動ダンパがあり，もし火災が発生した場合にはダクトを自動的に締めるような装置がついている。しかし，自動ダンパは，熱に感じて作動するようになっているので，煙の場合には締まらず，これだけでは十分でない。

(g) モニタ

建物内の煙その他を検出するために，いろんなモニタ装置を付けることができる。モニタ装置でよく使われるのは，煙，熱，イオン化に関するものである。

通常，モニタ装置はマシン室の天井についており，たとえば，絶対温度がどの程度あがったか，どのくらいの上昇率であったかなどをモニタできるようになっている。また，煙に関しては，煙の粒子がどの程度か，どの位の大きさの粒子が存在するかなどを検出できる。

このようなモニタ装置は，パターンのように組まれ区域化されている。たとえば，Aの区域で何か警報装置に引っかかっても，それだけでは大きな警報は出ない。AとBの両区域で警報装置にふれるようなことが起った時に大きな警報が出るというような区画別になっている。

なぜ，このような作動の仕方が必要かというと，たとえば，探知器の真下に立ってタバコを吸った場合に装置が作動するかも知れないが，それだけでは危険性

はないので，別々に区画し，両方が作動した時に大きな警報を出すような方式がとられている。

(h) 緊急装置

通常，モニタ装置と一緒に緊急装置が設置されている。たとえば，CO_2ガスやハロンガスを使うような自動消火装置がそうである。

これらのガスは，天井や床に貯蔵してあり，警報装置のセンサがいくつか作動すると警報が発せられ，ガスが撒かれ消火するという形式になっている。通常，警報装置が音で鳴ったり，あるいはフラッシュのような形でピカピカ光ってから後，少し時間の余裕があるが，これはカウント・ダウンの時間である。その時間内に，オペレータが何が起ったかをすばやく発見し，もし緊急装置を作動させなくてもよい場合には，それを止めることが出来るような形式になっている。その時間内に緊急装置を手動で止められなかった場合には，自動的に作動してガスが出るということになる。

このような装置には，いくつかの問題がある。たとえば，CO_2ガスを使って消火すると酸素不足となり，中にいる人間が呼吸できなくなる。この場合，酸素マスクを設置しておくとか，装置が作動する前に全員避難させるなど，慎重な対応が必要である。

一方，ハロンガスについてはCO_2ガスのような問題はなく，人間に影響を及ぼさない。しかも，化学反応を起こして火を消すため，非常に有効な消火剤である。しかし，ハロンガスは非常に高価なため，誤って作動してハロンガスを使用してしまうと，非常に高価なエラーということになる。

つぎに，警報装置には，内部的なものと外部的なものとがある。もし，センサが動いて警報装置が作動すると，それによって耳に聞こえるような警報が発せられ，そこにいる人間が避難する。また，避難体制が決まっていれば，それに従うような形で警報を発する。これが内部的な警報装置である。

この場合の問題点は，具体例をあげると，たとえば，CO_2ガス装置がアクシデントで作動し，部屋中にガスが広がった事故がある。そして，警報装置がマシン

室でしか聞こえなかったため，下の部屋にいる者には事故の発生が全然わからなかった。しかも，CO_2ガスは空気より重いため，下の部屋に柱その他を伝わって下降し，匂いもないため誰れも気づかず，死にそうになるという事故が起ったことがある。

外部警報装置については，たとえば，当ビルとセントラル・ステーションを通信回線で結んでいる場合を仮定すると，何らかの理由で通信回線が切断されたり，セントラル・ステーションから特別なシグナルが送られて切断されたりすると，セントラル・ステーションから警察や消防署に連絡がなされるという形式になる。

(i) 緊急時の対策

緊急事態が発生した場合に，どのような手続きに従うかについては，発生後に何かを決定しようとしても遅いので，事前に決めておかなければならない。

たとえば，機器はどのようにするか，電力はどのようにするか，どのデータを金庫に入れるか，どういう経路で避難するのか，などを各人に徹底しておかなければならない。同時に，緊急装置は常にテストし，人については普段から訓練しておくことが重要である。

4.4 アクセス・コントロール

アクセス・コントロールは，人および物の双方を含むコンピュータ施設への出入についてのコントロールであり，当然，通信回線を介してのアクセスも含まれる。

いいかえれば，アクセス・コントロールとは，コンピュータ・システムの操作，ならびにコンピュータ関連諸設備への接近の制御ということができよう。

4.4.1 コンピュータ施設へのアクセス

(a) 出入口

出入口の問題は，扉だけではなく，窓，通信回線，エスカレータなど，コンピュータ・システムにつながる一切の開かれた口のコントロールが必要である。

(b) 人の確認

従業員か，外来者か，業者か等々，コンピュータ・センタに入って来る人の確認をする必要がある。

(c) 物の確認

データ，消耗品，その他のマテリアル等，物理的に搬入されてくる物，および通信回線で入ってくるもののコントロールが必要である。

(d) 出の確認

出ていく方も，物理的な形で出ていく場合もあれば，通信回線で人手を介せずに直接出ていく場合もある。

通信回線を介する場合の問題としては，ターミナルを操作しているのが誰れかということを明確にさせる必要がある。なぜなら，誰れかが情報を盗むために傍受しているかも知れないし，ユーザを擬装して情報を盗もうとして操作している可能性もあるからである。

4.4.2. コントロールの方法

(a) ガードマン

まず最初は，ガードマンを入口に置き，入館者をチェックすることである。裏側の出入口があまり使用されていない場合には，テレビを使って正面玄関のガードマンが監視するという方法がとれる。

その他，建物は消防法の規則により，非常口を設けなければならないし，非常口には鍵をかけてはならない。したがって，何重にも監視設備を置かなければならない。たとえば，非常口が開けられた場合には警報装置が鳴り，なぜ開けられたかはガードマンがテレビで見れるようにしておくなどの対策がとられている。

(b) 出入制限

出入を制限するのも１つの方法である。回転式の扉にすることによって，多数で押しかけてきても，１人づつしか入ることが出来ないようにすることができる。

(c) トラップ

迷路のようなものをつくって，マシン室には直接入れないようにする方法もある。たとえば，二重扉になっていて，最初の扉を閉めないと次の扉が開かないというやり方も使われている。

このトラップのやり方については，火事などの場合に直ちに現場に行けないとの理由で，防災上の規則から問題にされることがある。

(d) 本人の確認

アクセス・コントロールのもう１つの側面は，確かに本人であるかどうかを確認することである。最ものぞましいのは，ガードマンが入館する人の顔を全部知っていて入れるということがある。

非常にうまくいっている例としては，ガードマンがその建物で働いている人を全部知っているだけでなく，彼らの当番まで知っているというシステムをとっている企業がある。しかし，これは特殊な例である。

(e) バッジ

バッジや通行証を持っている人は入る権利があるということを前提としてコントロールする。それを持っている者は誰れでも入れるという前提になっているため，トラブルを避けるためにも写真を焼きつけて，名前と顔を確かめてから初めて入れるというふうにする。

バッジの問題点は，紛失した場合に，それが後で何らかの目的のために使用される可能性があるということである。この問題を避けるためには，定期的に新しいものに切り替える必要がある。

もう１つのやり方は，ミニコンピュータを使う方法で，バッジの中に，読めないような形で番号を印刷しておくやり方がある。もし，従業員がバッジを紛失し

たり，退職したような場合には，そのこともミニコンピュータに記憶させておく，そうすることにより，そのバッジが使用された際にも排除することができる。

(f) 個人の特性

他には，手形のようなものを使うなど，それぞれ個人の特性に応じた方法がある。

たとえば，手形を使う方法の場合，機械の上に手を置き，指の長さなどを認識して本人かどうかを確かめるという具合である。これは，1,000人程度までと限られる場合には効果的な方法とされている。

これと同じ考え方の範ちゅうとしては，指紋や声紋により識別する方法が研究されている。

(g) 問題点

以上のような方法論にも問題点がある。たとえば，ガードマンを置いても，月日がたつにつれ，ガードマンがコントロールに従って厳重に決められた手続きをとるということがなくなってくる傾向がある。毎日，同じようなことを繰り返していると，3人一緒に入ってきたような場合に，シフトでない者が1人加わっていても通してしまう危険性がある。

これに対しては，バッジ・リーダやミニコンピュータなど，機械を使うコントロールが出てきた。しかし，機械は，バッジを認識するのであって人間を認識するのではない。他人のバッジを使っても機械は通してくれる。いいかえれば，バッジさえ持っていれば，すべての扉が開くという危険性がある。

鍵の場合には，簡単にスペアをつくることができるのが問題である。しかも，鍵は，いつも取り替えるということが非常にむずかしい。エレクトロニクスによる方法を使う場合には，変更するのが割と簡単になる。

サインを使う方法があるが，サインは研究すれば形は十分まねることができる。しかし，書き方や書くスピードまでまねることはできない。

建物内で，一定区域には特定の担当者しか入れないようにする場合，入室を許可するバッジは特定の色にするとか，特定の区域には誰れか必ず同行するなど

のルールをつくる必要がある。

バッジの場合で，とくに重要なことは，何のためのバッジかを明記してはならないということである。たとえば，マシン室への入室用のバッジだとわかるようになっていれば，これを拾った人には一種の招待状の役割をはたすことになりかねない。

そして最後に，誰れが入ったか，出たか，何が動かされたか，などについて記録をとるということが重要である。

4.4.3 ターミナル

オンライン・リアルタイム・システムの場合，ターミナルからのアクセス，およびターミナルへのプリント・アウトをめぐる問題がある。まず，ターミナルを使用する場合に，どのような処理のために使うのかがわかっているだけでなく，コンピュータ・システム側で誰れがターミナルを使用しているかが認識できるようにする必要がある。

(a) ハードウエア

ターミナルが使われている場合，信号のやりとりを通じて確認するようハードウエアに組み込む方法がある。

もう1つは，IDコードを通じてユーザを確認し，初めて使用を許可する方法がある。

(b) パスワード

パスワードをつくり，パスワードが使用された場合にのみ，アクセスを認める方法であるが，パスワードを不注意にあつかって，それが漏れてしまえば，パスワードによるコントロールは簡単に駄目になってしまう。

(c) 暗号化

暗号化は，磁気テープやディスクに記憶されている場合でも，伝送している場合でも，そのままでは簡単に情報として使えないというところにメリットがある。

(d) シュレッダ

非常に重要なことの1つに，用紙を粉砕するシュレッダがある。重要な情報の場合，そのまま捨てたのでは拾った人が読めるため，読めないような形にして情報を捨てることが大切である。しかも，これはターミナル側だけの問題ではない。

4.5 人 事 管 理

人の問題は，人選，教育訓練その他によって，エラー，事故，犯罪等を防止すると同時に，効率的な処理をするために有効である。

具体的には，まず，人間的なエラーの防止。そして，同じようなコントロールを重複して何人もがやらないようにしなければならない。

つぎは，コンピュータ犯罪の防止。これは必ずしも単独犯というのではなく，共謀の率が高いので注意しなければならない。

さらに，単なる不注意によるエラーの防止。仕事がルーチン化してしまうと，どうしても注意力が散漫になり，見過ごしたままで仕事を流してしまうようになるので，この不注意を防止しなければならない。

最後に，意図的に有害な行為をする者からの防衛。これは，自分達の要求が受入れられなかったり，あるいは解雇された等の恨みから，何か有害なことをするわけで，きわめて危険である。

これらの諸問題について，何とかコンピュータ関連施設や情報等を守ろうとするためには，いくつかの方法がある。しかし，これらは何とかして守ろうとする努力の方向であって，これらを根絶させることはできない。

(a) 経歴調査

被雇用者の経歴を調べるが，これは通常3回行われる。最初は雇用前，そして雇用直後，それから定期的にチェックするという意味で3回である。

アメリカでは，よく仕事を変えるので，雇用前にどこで働いていたのか，そこでの勤務状態はどうであったか，その上司から推薦状をとるなどして，本人の能

力や性格を判断するための資料をそろえ，チェックしなければならない。

雇用後は，本人が提出した資料や情報が正しいかどうか確かめてみる必要がある。たとえば，学歴等についても，本当であるかどうか検証する必要がある。

(b) 状況チェック

各人の状況をチェックする必要がある。たとえば，ある従業員がギャンブル等で非常に借金が多くなっているという状況にあると，それが圧力となって犯罪を唆かされるような環境が出来あがる。したがって，定期的にチェックすることが非常に有効になる。

しかし，いろんな個人的状況を調査することは，雇用規定にふれ非常に難しい。むしろ，管理者が，部下のことをよく知るように目を光らせ，状況が変わったかどうかに注意をはらうことが必要である。

どの程度に目を光らせておくかについて，その度合を決めておくことが有効である。必要なところに力点を置いてチェックするということでよい。

たとえば，必要な補給部品を搬入する者が，建物の奥まで入って，エスコートもなしに歩きまわることなどあまり考えられないので，このコントロールのためには，入口に近い所で何らかの措置を講じておけばよい。また，プログラマがマシン室に入って行く必要はないので，それは認めないという方針にもとずいてチェックすればよい。つまり，人によってコントロールの仕方を考える必要がある。

(c) 教育訓練

エラーや不注意な行為をなるべく少なくするために，十分な訓練が必要になる。内容的には，各人の仕事や責任分担に関する訓練のみでなく，セキュリティ問題についての訓練や，緊急事態の発生にともなう避難訓練なども含めなければならない。

(d) 雇用契約

特定の従業員に対して，これだけの信用を与えるが，それについては，これだけの責任をもってその信用に応えるよう仕事を進めるように，というような雇用契約にサインさせることによって，一定の機密データへのアクセス権を与えると

いうやり方もある。

しかし，どのような契約を結んだところで，悪いことをしてやろうと決意している人間には何の効力もない。ただ，契約を結ぶことによって，自分がどのような信用をおかれているかわかるようになるので，そんなことには全然気がつかなかったというような状態はなくなる。

(e) 責任分割

他の業務と同様に，コンピュータ分野においても，仕事の分割，責任の分割を行うことがマネジメント上有効である。

たとえば，磁気テープをあつかうライブラリアンとプログラマは同一人物であってはならない，別々に分けるべきである。同様にプログラマとオペレータを別にすること，プログラマが端末機から操作することがないように，はっきりと分けておくことが必要である。

また，要員の仕事を交代させること，たとえば，3交替制をとっている場合，スタッフが夜番から昼番と廻っている時には，監督者はその逆まわりにシフトすることによって，スタッフと監督者の共謀による不正を減少させることが可能となる。

(f) 監 督 者

非常に効率のよい監督者を得ることが必要である。活発に役割を果たし，自分が抱えている部下が何をしているか常に把握して，自分の立場ならびにやっていることが何かをはっきりと認識しているような監督者を得ることが重要である。

(g) レビュー

他の有効な手段はレビューである。たとえば，新しいコードができた時，それをシステムに組み込む前に，別のグループまたは担当者がレビューし承認しなければ使用してはならないというやり方をとる。

プログラミングについては，バディ・システムというのがある。これは，2人が一緒になってプログラム開発にたずさわり，相互に修正しあうという形式で，片方の担当者しか知らないようなことが出来ないように，お互にお目付役的な役

割をはたすわけである。

このような，チームを組んで仕事をするやり方は，元来，そのような方式をとった方が効率が良いので行われるわけで，セキュリティ上の問題から出てきたものではない。たまたま，このような方式がセキュリティ上の問題解決に非常に役に立つということである。

4．6　災害からの回復

災害からの復旧をめぐる問題で考慮しなければならないことは，どれくらいで回復できるかというスピードの問題，復旧するために必要なリソースがどれだけ利用可能か，正常なセーフガードがどの程度ダメージを受け別の方法で動かす必要が出てくるか，最後に復旧のためにどの程度の資金が必要になるかである。

個々の対応策については，すでにふれてきたので，ここでは基本的な問題についてのみ検討する。

(a)　緊急時対策のプラン

まず必要な対策としては，プランをよく立案しておくことである。災害が発生した後でいろんな決定をしても遅いので，事前にプランをたてておくことが必要である。

つぎに，そのプランを使って要員を良く訓練しておくこと。緊急事態が発生した時には，どのような手続きがあるかを良く知らしめ，実際に演習をさせ，同時に機器等についても訓練しておく必要がある。

(b)　バックアップ体制

2次的な動力源その他，サービス・ソースのサポート体制をつくっておくことおよび，万一，コンピュータが完全にダウンしてしまった時のことを考え，別の施設のコンピュータを利用するなどのサポートも必要になってくる。

この場合のコンピュータ構成は，同一メーカであるばかりでなく，メモリ・サイズがほぼ同じであるとか，テープのドライブ数が同じであるとかまで考慮し，

ダウン時に十分代替して稼動できるようにしておかなければならない。また,OSが特定システム用に構成されている場合，自社の業務処理ができるようにOSを準備しておく必要がある。

(c) テスト

コンピュータがダウンした時，他のシステムに切換えるという事については，あまりテストがされていない。したがって，その時になって構成が合わないことが初めてわかったり，あわててOSを組んだり，切換えにともなう諸手続きをあわててつくったり，というようなことが往々にしてあるので注意しなければならない。

(d) 施設の再建

災害が発生した後，施設を再建しなければならないが，その時重要になるのがデータ・ファイルである。たとえば，三世代前までのデータ・ファイル等が，別の施設にきちんと保管されておかねばならない。

また，災害が発生した時には，いろんな必要資料を他の場所に移さなければならないという問題が出てくる。その時に，運搬をめぐってセキュリティ上の問題がからんでくる。そのような移動に関しては，とくに標準的な手続きもないし，経験も積んでいないので，いろんな弱点が暴露されることになる。

(e) リスタート

リスタートの保証，およびチェックポイントが必要である。つまり，ランが完全に終る前に，何か異常が発生した場合，かりに，それが非常に長い業務で，途中で終ってしまったような時には，リスタートのポイントをはっきりさせておかなければならない。

このように，非常に長い業務処理の場合，リスタートの能力を与えておくことが，コンピュータ・リソースの上手な使い方のために必要となる。

(f) 保　険

最後は保険の問題である。保険は，あくまでも事後的な救済にしかならないもので，事故などのために機器類，データ類，その他のいろんな収益をあげ得る機

会が失われてしまうということは避けることが出来ない。そして，そのために処理がストップしたり，顧客へのサービスが出来なくなるという事実が残る。

第５章　システム監査・日米比較研究

第５章　システム監査・日米比較研究

コンピュータ処理をめぐる監査については，日米ともに，かなり以前から研究が進められてきた。しかし，今日のように情報処理が各分野で普及し，かつ，高度化・複雑化した段階での研究体制が本格化したのは，わが国では当協会のシステム監査委員会の発足，米国では米国内部監査人協会（The Institute of Internal Auditors, Inc.略称ＩＩＡ）のSystems Auditability and Control Research Projectの発足を契機としていると見てよい。そして，この両者は，昭和５０年にほとんど同時にスタートした点も興味深い。

内容的には，わが国の場合は理論づけや体系づけ，そして通産政策へと発展しているのに対し，米国では個々の企業における具体的なアプローチの積上げという形で推移している。

また，米国では，EDP Auditsと称するのが一般的であるが，ここでは名称に関する論議は避け，システム監査と称することにする。

いずれにしても，その研究は緒についたばかりであり，現段階では資料も限られるが，可能な点についてのみ日米比較を試みたい。

5．1　システム監査の実態

システム監査の実態については，日米ともに明確には把握されていない。したがって，内部監査の実態調査の中から，コンピュータ関連部分のみを抽出し，日米の比較検討をしてみたい。

まず，日本の資料としては，日本内部監査協会が実施した「昭和５１年度内部監査実施状況調査」を基にし，米国については，米国内部監査人協会の「1975年度内部監査実態調査」を中心として比較検討してみたい。

なお，米国の調査は，米国・カナダを中心に世界１２か国にわたる実態調査であり，その集計は米国・カナダとその他諸外国の２つに分類している。したがって，ここで使用する数字は，米国とカナダを加えた数字であるが，内部監査あるいはシステム監査といった場合，米国における催物や研究グループ等には通常カナダは参加しており，米国とカナダを加えた数字を米国のみに当てはめて見ても大きな誤差を生じない。逆に，それをカナダのみに当てはめることは問題が多い。ここでは，一応，米国とカナダを加えた数字を米国とすることにする。

5.1.1 実施状況

(a) 日本

わが国の状況は，調査に回答した主要企業190社のうち，31社がＥＤＰ業務を監査の対象としている。比率としては16.3％であり，監査対象業務の中でも普及率は第１１位とかなり低い。（第5.1表）

第5.1表　監査対象業務（日本）

今回順位（51年度）	監査対象	実施会社数	実施比率	前回順位（50年度）	前々回順位（49年度）
1　位	販売業務	136社	71.6％	1　位	1　位
2　位	棚卸資産管理業務	102	53.7	2　位	3　位
3　位	経理業務	94	49.5	3　位	2　位
4　位	子会社関連会社	84	44.2	4　位	4　位
5　位	購買業務	80	42.1	7　位	5　位
6　位	固定資産管理業務	78	41.1	4　位	6　位
7　位	製造業務	61	32.1	9　位	10　位
8　位	総務・人事・厚生業務	59	31.1	7　位	7　位
9　位	外注管理業務	58	30.5	10　位	8　位
10　位	全般管理・組織・制度	54	28.4	6　位	8　位
11　位	ＥＤＰ業務	31	16.3	11　位	11　位
	その他	71	37.4		

〔出所〕　日本内部監査協会調べ

(b) 米　　国

これに対し，米国の場合は，大企業で実に92％がＥＤＰを監査対象としており，監査対象業務の中で最も比率が高い。中および小企業の場合でも，72％，71％と購買業務に次ぐ高い率を示している。全企業合計で見ても78％で，購買業務の81％に次ぐ実施状況となっている。（第5.2表）

第5.2表　監査対象業務

	アメリカ・カナダ				その他諸外国				合計	1968調査
	小企業	中企業	大企業	計	小企業	中企業	大企業	計		
広告宣伝	32%	37%	60%	43%	43%	71%	67%	63%	48%	47%
設備計画	36	64	71	56	36	62	63	57	56	56
ＥＤＰ	71	72	92	78	68	79	90	81	79	64
在庫計画・管理	53	66	67	62	68	85	87	82	67	80
会社財産に対する保険	48	58	73	59	59	68	60	64	60	66
経営情報システム	53	47	60	53	59	79	90	78	60	48
組織管理	56	58	59	57	68	82	90	81	63	44
製　造	39	49	57	48	64	71	67	68	53	46
購　買	78	82	84	81	82	94	93	91	84	89
輸　送	28	45	51	41	50	71	63	64	47	51
その他	41	48	39	43	32	29	43	35	41	?
回答会社数	90	83	82	255	22	34	30	88	343	308

〔出所〕米国内部監査人協会（ＩＩＡ）調べ

(c) 比　　較

これは，あくまでもＥＤＰを監査対象としているかどうかの調査であり，これで内容のレベルを類推することは出来ない。しかしながら，内容はともあれ実施状況に歴然たる格差があることは事実である。

この日米格差が生じた原因の１つとしては，米国では従来から内部監査体制が確立し，当然のこととしてＥＤＰ業務が監査の対象とされてきたからであろう。その点，わが国では１部の企業を除いて，内部監査体制そのものが弱体であるといえよう。

そして，内部監査体制そのものに格差があることについては，日米のトップ・

マネジメントの内部監査に対する認識の差といえなくもない。しかし最近の傾向としては，わが国でもトップ・マネジメントがシステム監査に注目しはじめており，トップ・マネジメントの意向でシステム監査の実施に踏み切った企業もあらわれるなど，将来については大きく期待できる面もある。

5.1.2 システム監査人

(a) 日　本

内部監査人で，過去に機械計算部門に籍を置いたことのある人は11.5％である。最も多いのは経理の経験者で86.1％，つぎに営業経験が51.9％等であり，入社時より監査を相当しているのは5.8％しかいない。したがって，通常，内部監査人は，複数の業務を経験した後，監査部門に配属されているといえる。

しかも，これは内部監査人の社内経歴であり，ここでの機械計算部門の経験者11.5％がシステム監査人ということにはならない。わが国にシステム監査人が皆無とはいえないが，きわめて少数といわざるを得ない。（第5.3表）

第5.3表　内部監査人の主要出身部署（日本）

	経理	営業	総務・人事・労務	管理	企画・調査	資材・購買	生産	機械計算	入社時より監査	その他
合　計（社）	179	108	73	56	50	47	31	24	12	12
比　率（％）	86.1	51.9	35.1	26.9	24.0	22.6	14.9	11.5	5.8	5.8

〔出所〕　日本内部監査協会調べ

このような状況のもとで，新しい傾向としては，金融機関を中心とした動きであるが，コンピュータ専門家を内部監査部門に配置し，システム監査の実施体制を整えつつある企業も徐々に増えてきている。

これらのことから，現時点でシステム監査人を置いている企業は，東証一部，二部上場企業のうちで，金融機関を中心とした約１％程度と推定される。しかし，今後は，通産省がシステム監査を政策としてとりあげていることなどから，加速度的に普及する可能性が大であるといえよう。

(b) 米　　国

内部監査人の中に，少くともシステム監査人が１人以上いる企業が45％ある。しかも，大企業では実に８２％がシステム監査人を置いており，一般的にシステム監査がかなり普及していることを示している。（第5.4表）

第5.4表　システム監査人の存在

	アメリカ・カナダ				その他諸外国				
	小企業	中企業	大企業	計	小企業	中企業	大企業	計	合計
回答会社数	88	82	78	248	19	31	26	77	325
コンピュータ監査の専門家がいると回答した会社の比率	16%	39%	82%	45%	5%	39%	77%	42%	44%

〔出所〕　ＩＩＡ調べ

また，ＩＩＡでは，委員会を設置して活発な調査研究活動を行っている。他にシステム監査人による専門家集団であるEDP Auditors Association, Inc .は，いわばシステム監査人協会ともいえるもので，昭和48年に３支部100名という組織であったものが，５２年には23支部で2,000人以上という大規模な構成にまで成長している。これを見てもわかるように，システム監査は，米国においてもごく最近になって著るしい発展をとげている分野といえよう。

(c) 比　　較

システム監査人の面から日米を比較すると，わが国の場合は，現在システム監査人と称することの出来る人々は金融機関を中心としてごくわずかである。また，システム監査についての専門団体は存在せず，システム監査人の養成が著るしく

立ち遅れている。

米国では，大企業の８０％以上がシステム監査人を置いており，システム監査人の専門団体が存在するなど，ここ数年間にすさまじい発展をとげている。

これらの状況からして，この面での日本の立ち遅れが目立っているというのが現状である。

5.1.3　システム監査の内容

(a)　日　　本

システム監査の内容に関する系統だった調査が行われているわけではないので，軽々しく論評することはさけなければならない。そして，現段階では部分的には行われているが，その内容は企業ごとにまちまちである。（第5.5表）

また，昭和５１年に大蔵省が実施した"金融機関の内部検査に関する実態調査"によれば，金融機関でコンピュータ関連部門の検査を実施しているのは12.9％と低率である。個別にながめてみると，都市銀行以外は，まだまだこれからの問題であるといえよう。内容的にも，きわめて断片的であり，今後の進展が期待されるところである。（第5.6表）

第5.5表　　監査実施例（日本）

業　種	会社例	監査テーマ・内容（着眼または要点）
建　　設	例　1	＊ＥＤＰ関連業務のいっさいとその組織，手続，規程
食品・水産	例　2	＊ＥＤＰシステムの稼動実績
繊　　維	例　3	＊(1)ＥＤＰの組織，制度，手続　(2)ＥＤＰの日常管理の状況
化　　学	例　4	＊(1)適用業務の運営管理状況と問題点の内容把握　(2)諸費用の管理状況の点検　(3)機械処理の開発と実施状況　(4)事故防災ならびに保守状況
	例　5	＊計数作表監査 (1)計数作表１件別利用実態の把握　(2)類似作表の統合　(3)陳腐化作表の廃止，削減　(4)システム自体の見直し，合理化
薬　　品	例　6	＊アウトプットの適否
	例　7	＊研究開発部門におけるＥＤＰの利用状況 (1)ＥＤＰＳの能力増強計画に対する実施状況　(2)現在実施中の各システムの状況と問題点　(3)データならびにアウトプットの管理状況　(4)ＥＤＰ部門の管理組織および運営

業　種	会社例	監査テーマ・内容（着眼または要点）
石油・石炭	例　8	*購買・資材管理システム監査 (1)請求書省略と自動支払制度にともなうシステム上の補完手続　(2)データの受渡（チェック・ルーチン等）内部牽制面の適否　(3)プログラム・ドキュメンテーションの整備　(4)システム・メンテナンス委員会設置に関する勧告
	例　9	*管理機構
ゴ　ム	例１０	*リアルタイム・システム *データコントロール・システム *アウトプット・データ利用状況
ガラス土石	例１１	*会計組織のコンピュータ処理実施にともなう問題点
	例１２	*ＥＤＰ管理体制全般
鉄鋼・金属	例１３	*ＥＤＰシステムに投入するインプット・データの信頼性（販売単価のチェック状況）
	例１４	*「現品の流れ」と伝票の合致
機　械	例１５	*ＥＤＰ業務の現況と問題点 (1)システム部門の同業他社比較　(2)電算機の稼動状況と余力　(3)電算機室の面積と保安状況　(4)システム開発体制とオンライン化の状況　(5)職種別，人員と勤務状況，システム部門の費用
	例１６	*生産用直接材料在庫記録維持システムのPIR(Post Inplementation Review) (1)当システムの機械化開発計画予測効果の適否 *機械化システム開発時のチェック（対象はサービス工事精算，棚卸資産会計，材料分譲，金属素材・ストックステータスのシステム） (1)ＥＤＰ利用システム要件の妥当性　(2)アウトプットの信頼性，正確性を保証するコントロール機構の妥当性　(3)各種ドキュメント・マニュアル等の整備状況
電気機器	例１７	*機械化方針，データＩ／Ｏチェックならびに保管状況，データファイルの信頼性，正確性，ドキュメンテーションおよびプログラム管理
	例１８	*会計監査（Ｂ／Ｓ，Ｐ／Ｌの正確性，信頼性，経営分析） *業務監査（ＥＤＰ導入の実情とその適否，価格管理制度運用の適否）
輸送用機器	例１９	*電算機データ管理状況 (1)オンライン・リアルタイム方式，データベース方式へ移行に際してのデータ管理上の問題点　(2)オペレータの社内要員化
精密機器	例２０	*ＥＤＰ担当部門についての安全管理 (1)原料の整備保全　(2)ＥＤＰシステムの効率状況，インプットとアウトプット整票，ＳＥの養成，外注業務
商　業	例２１	*ＥＤＰアウトプット帳票の追跡調査（利用状況）
	例２２	*従業員預金
	例２３	*インプットデータのバッチ・システムとプログラム・チェックについて
金融保険証券	例２４	*電算処理事務体制の再検討
	例２５	*ＥＤＰ部門の組織ならびに運営の適切性 *E.DPシステムの安全管理の適否

業　種	会社例	監査テーマ・内容（着眼または要点）
金融保険証券	例２６	*コンピュータ・システムの現状調査
	例２７	*営業課・支社配布の機械作成諸表の利用の実態とその改善
	例２８	*端末機，パイデックス等の配置状況
鉄道・運輸	例２９	*電子計算機部門業務監査 (1)情報ファイルの管理状況　(2)各種契約の現状
	例３０	*コンピュータ・アウトプット・データの利用状況 (1)管理態勢　(2)業務とデータの適応性　(3)データ取扱状況
	例３１	*インプットと未収管理の正確性：コンテナ・デイテンション・チャージ

〔出所〕　日本内部監査協会調べ

第5.6表　金融機関のコンピュータ関連部門検査（日本）

項目＼金融機関	都銀	信託	長銀	地銀	全銀計	相銀	信金	合計	%
コンピュータ関連部門の検査について									
(1)検査部等の検査は									
(イ)実施している	9		1	11	21	12	48	81	12.9
(ロ)実施していない	3	6	2	49	60	56	351	467	74.4
(ハ)その他		1		2	3		38	41	6.5
(ニ)無回答	1			1	2	4	33	39	6.2
(2)検査の範囲は									
(イ)ハードウェアの管理状況	7		1	5	13	4	12	29	
(ロ)ソフトウェアの内容	3			1	4	1	3	8	
(ハ)データ等のファイルの管理状況	9		1	9	19	7	35	61	
(ニ)オペレーションの管理状況	9		1	7	17	7	25	49	
(ホ)その他	4	1		3	8	3	10	21	

〔出所〕　大蔵省調べ

(b)　米　　国

通常コンピュータ・システムの開発に関与している企業が３４％ある。大企業のみを見ると５０％がシステム開発に関与している。（第5.7表）

また，システム監査人が監査の際に関係をもつ分野としては，保全，コンピュータ室，業務の効率性等が非常に高い率を示している。したがって，システム監

査人は，これらの点について非常に高い関心を示していると判断することができる。（第5.8表）

第5.7表　コンピュータ・システムの開発に関与しているか

	アメリカ・カナダ				その他諸外国				
	小企業	中企業	大企業	計	小企業	中企業	大企業	計	合計
	%	%	%	%	%	%	%	%	%
通常はする	24	30	50	34	27	29	57	38	35
ほとんどしない	47	40	29	39	41	41	30	37	39
全くしない	24	26	14	22	27	21	7	17	20
回答なし	5	4	7	5	5	9	6	8	6
回答会社数	90	83	82	255	22	34	30	88	343

〔出所〕　ＩＩＡ調べ

第5.8表　監査の際に関係をもつ分野

	アメリカ・カナダ				その他諸外国				
	小企業	中企業	大企業	計	小企業	中企業	大企業	計	合計
	%	%	%	%	%	%	%	%	%
内国歳入庁規則への準拠性	9	8	12	10	—	—	—	—	7
EDP業務の効率性	42	45	62	49	36	38	67	48	49
コンピュータ室	42	54	79	58	18	47	77	50	56
プログラムの効率性	20	30	50	33	27	32	43	35	34
保　　全	68	65	84	72	45	62	83	65	70
データの機密保持	30	33	56	39	27	35	50	39	39
回答会社数	90	83	82	255	22	34	30	88	343

〔出所〕　ＩＩＡ調べ

5．2　政策の動向

(a)　日　　本

通産省では，コンピュータ・システム導入の増加にともない顕在化してきているデータ流出，プライバシー保護問題等種々の弊害に対し，ユーザの立場からの施策が求められているとの認識の下，これまでのメーカ・サイドからの情報関連振興策に加えて，ユーザ対策にも取り組む姿勢をみせている。

この中でも，システム監査はとくに大きな役割を果たすことになると予想されており，昭和５２年度よりシステム監査の方法を明確にし，その指導および普及も目指して本格的に検討を始めている。

このように政府がユーザ対策の一環としてシステム監査に取り組み，その指導，普及をはかるという動きは他に例を見ず，注目されるところである。（第5.9表）

第5.9表　通産省のシステム監査関係予算

年度	項　　目	予　算　額
５２	システム監査に関する調査研究	６００万円
５３	システム監査士制度創設のための調査研究	５００万円

(b)　米　　国

商務省標準局は，昭和４９年，情報処理に関する物理的安全性とリスク・マネジメントのためのガイドライン"Guidelines for Automatic Data Processing Physical Security and Risk Management"を連邦政府内情報処理標準（Federal Information Processing Standers）として公表した。

同年１２月，プライバシー法（The Privacy Act of 1974）が成立すると，翌５０年５月には，同法の施行にともなうセキュリティ・ガイドライン（Computer Security Guidelines for Implementing The Privacy Act of 1974）を公表している。

このガイドラインの取りまとめにあたったのは，標準局のInstitute for

Computer Sciences and Technologyであり，連邦政府関係のコンピュータ運営の効率化等の活動を行っている機関である。したがって，このガイドラインは，連邦政府機関の情報処理を対象とする性格のものである。

ガイドラインの内容には，フィジカル・セキュリティの内部監査（Internal Audit of Physical Security）が含まれており，監査準備，監査計画，監査実施等について述べている。

5．3　公認会計士の対応

(a)　日　　本

日本公認会計士協会は，昭和５１年，「電子計算機を使用した会計組織に対する内部統制質問書（改訂案）」，および「ＥＤＰシステムの監査基準および監査手続試案」を発表した。

まず，内部統制質問書の性格については，監査人が監査にあたって実施すべき監査手続きの選択適用範囲を決めるために使用するものとしている。また，良好な内部統制組織を整備確立することは，財務諸表監査の前提であり，監査人はその存在を質問書を利用して確かめるとしている。

つぎに，ＥＤＰシステムの監査基準および監査手続試案については，会計処理がコンピュータで行われることにより，公認会計士の実施する財務諸表監査が著るしい影響を受けており，それに対応していくために拠るべき基準を明確にする必要があるため作成したとしている。

そして，51年11月，通産大臣へ「企業内部におけるＥＤＰシステム監査に関する要望書」を提出した。

(b)　米　　国

アメリカ公認会計士協会は，昭和４９年，監査基準書第３号「ＥＤＰが監査人の行う内部統制の調査と評価に与える影響」を発表した。また，昭和５２年には「Audit and Accounting Guide」を発表している。

このAudit and Accounting Guideは，第1章序論，第2章会計コントロールの調査と評価，第3章ゼネラル・コントロール，第4章アプリケーション・コントロール，第5章ＥＤＰシステムのドキュメンテーションから構成されている。

また，カナダでは，すでに昭和５０年に，カナダ勅許会計士協会が「Computer Audit Guidelines」を発表している。

5．4　内部監査人の研究体制

(a) 日　　本

昭和５０年度以来，コンピュータ・サイドおよび監査サイドの双方を含めて，当協会で委員会を設置し，研究体制の一元化をはかってきたため，当協会以外の組織による目立った活動は見受けられない。しかし，その中において，日本内部監査協会は，従来よりＥＤＰ監査委員会を設置して地道な活動をつづけている。

(b) 米　　国

米国内部監査人協会では，国際ＥＤＰ監査委員会（International EDP Auditing Committee）を常設して研究活動を行っている。また，特筆に値する調査研究活動としては，昭和５０年，５０万ドルの予算で，Systems Auditability and Control Reserch Project（ＳＡＣ）を発足させ，実態調査をＳＲＩに委託した。

昭和５２年初頭，このＳＡＣレポートが３分冊にまとめられた。全体のサマリともいえるExecutive Report，およびData Processing Control Practices Report，Data Processing Audit Practices Reportの３冊である。

5．5　情報関連機関における研究体制

(a) 日　　本

当協会は，昭和５０年度，システム監査委員会を設置し，本格的な研究活動を

開始した。

同委員会は，システム部門の代表をはじめとして，内部監査人，公認会計士，監査役等の代表を網羅しており，システム監査をめぐる利害関係者全員を同一テーブルにつけた構成となっている。

同委員会の発足後，関連各界とも，同委員会における意見調整ならびに基準の設定を求めることになった。これにより，わが国では，同委員会がシステム監査に関してリーダーシップを発揮し，監査サイド，被監査サイドの協力を受けて強力な研究体制がとられてきた。

(b) 米　　国

情報処理サイドにおけるシステム監査の調査研究体制は見受けられない。

第5.10表　システム監査日米比較（要旨）

	日　　本	米　　国
企　　業	普及率　16.3% システム監査人の存在　1 %（推定）	普及率　78 % （大企業のみでは92 %） システム監査人の存在　45 % （大企業のみでは82 %）
政　　府	通産省機械情報産業局 民間企業に対するシステム監査の普及促進をはかるため，ユーザ対策としてとりあげている。	商務省標準局 連邦政府機関の情報処理に対するセキュリティ・ガイドラインでセキュリティ監査をとりあげている。
公認会計士	日本公認会計士協会 電子計算機を使用した会計組織に対する内部統制質問書公表 ＥＤＰシステムの監査基準および監査手続試案公表	米国公認会計士協会 監査基準書第3号公表 Audit and Accounting Guide公表
内部監査人	日本内部監査協会 ＥＤＰ監査委員会設置	米国内部監査人協会本部 国際ＥＤＰ監査委員会設置
情報関連団体	日本情報処理開発協会 システム監査委員会設置	とくに活動なし
システム監査専門団体	な　　し	EDP Auditors Association, Inc.

付属資料1
コントロール・ガイドライン

付属資料 1

コントロール・ガイドライン

将来のコンピュータ・システム開発および利用のために

原題：Control Guidelines
…for use in the development and implementation
of future computerized systems

マサチュセッツ相互生命保険会社
総合監査部EDP監査グループ　1977年1月発行

コントロール・ガイドライン

本文書起草の目的は，将来の標準化に備えてシステムズ・コントロールやコントロール手続きのガイドラインを設定することである。このガイドラインにそって，先々システムズ・コントロールは総合監査部の手で実施されよう。個別的にせよ。あるいは組合せにせよ，これらのコントロールが実施の運びとなれば，実際的な運用ベースにおける最良のシステム・セキュリティが確保できるに違いない。

コントロールの定義

「コントロール」とは，コンピュータ・システム内部の一貫性と正確さに一定の基準を与える手段である。これは，つぎのような機能をもつ。

- ○企業資産のセーフガード
- ○会計データの正確さおよび信頼性の検証
- ○運用効率の促進
- ○経営政策との密着性を確保
- ○監査証跡の提供

コントロールの設計はアプリケーションにより異なるが，その基本的な目的および必要性は一定不変のものである。

資産および負債の金額を正確に把握することは，全てのコントロール手続きでは第一義に属することであり，コントロールは常に財務報告や総勘定元帳の収支およびこうした収支残高を示す数字に関係した金額取扱欄に置かれねばならない。

コントロールの設定コストとコントロールなしですますコスト／リスクのバランスは，コントロール設計・評価においてシステム設計者が絶えず考慮せねばならないテーマである。また時間，材料，資産等の損失リスク，ユーザおよび保険契約者の満足，経営者の信用等も，コントロールを開発・利用する際必要な時間

や素材を考える時，コントロール・コストの対として重視される必要がある。もしこの間に適切なバランスがなければ，そのコントロールは，当初の意図を超すか，あるいは及ばないという結果になる。

フォーマット

このガイドラインの論理的立場を強化するため，コントロールの発想概念は，12の主要なカテゴリに分けられた。また各カテゴリは，ＩＳＤやユーザ分野の責任により，さらに細分化されている。大抵の場合，コンピュータ・システムに関連しユーザ利用に向けたコントロールの設計や提供は，ＩＳＤの責任に入る。

① 入力コントロール
② 処理コントロール
③ 出力コントロール
④ 直接更新手法を使用するシステムのコントロール
⑤ データ保存
⑥ エラー・コントロール
⑦ データ変更コントロール
⑧ ファイル・セキュリティ
⑨ プログラム／システム・ドキュメンテーション
⑩ プログラム変更コントロール
⑪ 責任の分担
⑫ マネジメント・トレイル

論理的解釈の立場を一層明快にするため，12の主要カテゴリは，各々対応するコントロール・タイプに分化された。

① 手続きコントロール ― データ準備，受領，処理，蓄積，出力などのためのコントロールは，データの正確さ，一貫性，継続性を保つものである。
② 管理的コントロール ― このコントロールは，システム・プログラムの正確さと継続性を保証するため設計される。
③ 組織的コントロール ― 責任の存する正当かつ適切な部位を確かならしめる

意図をもったコントロール。

内容目次

Ⅰ．手続きコントロール

A．入力コントロール

ISD（Information Systems Department）の責任

1. 転送フォーム(注1)は，データが不正確あるいは不完全に記録される機会を最小限

に抑えるよう設計されなければならない。

2. 機械読取可能なフォームへのデータ変換（カード入力，直接エントリ）は，間違った変換により発生するエラーを極力抑えるようにコントロールされなければならない。

a．データ検査

b．ユーザまたはコントロール・グループによる検討，あるいはトランザクションの調節制御

3. バッチの場合，ＩＳＤはバッチ・コントロール記録からのコントロールおよびハッシュ・トータルが入力から取られたトータルに対し検査されるよう保障すべきである。

4. バッチにおけるエラー量やユーザの訂正速度にもよるが，全てのエントリが編集された後，全バッチを除去することが望ましい。

5. エラーは，修正や再付託のためユーザ分野別のエラー・リストにのせるべきである（「エラー・コントロール」の項参照）。

6. データが磁気ファイルから入れられつつある時，ファイルのラベルは，システム・ソフトウェア（例えばＴＭＳ）や正しいファイルがランされ得る他の何らかの手段によって検証されるべきである。

a．正しい日付け

b．正しいサイクル

c．正しいファイル／バッチ・ナンバ

d．正しいファイル識別子

7. オンラインまたはリアルタイムのシステムを使用する場合，コントロールはつぎのような内容を確実にしなければならない。

a．端末が有効な伝送装置である。

b．ユーザは，アクセスする合法性と権限を有する。

c．いかなるメッセージも失なわれない。

1）メッセージ・カウント

2）メッセージ再生

3）エコー・チェック

d．メッセージが有効である（これは通常の入力コントロール，編集ルーチン等により実行できる）。

e．ログ（トランザクション・コントロール・ログ）に記載される問合せ，更新等はつぎの事柄を忘れてはならない。

1）誰がどのターミナルから

2）時刻と日付け

3）行われたトランザクションまたはオペレーション

4）影響をうけたファイル

8. 入力コントロールのタイプはつぎの通りである。(注2)

a．トランザクション・カウント

b．データ予測

c．キーパンチによる，またはキーパンチとは別なカード検査

d．機械読取可能ドキュメント入力

e．分離入力妥当性検査ラン

f．入出力コントロール・グループ

g．入力データセットのチェック

h．入力妥当性検査

（注1）：転送ドキュメントは，このガイドラインにあっては，ソース・ドキュメントからデータを利用するユーザにより用意されるフォームと定義される。またソース・ドキュメントは，データが取られたオリジナル文書として定義される。

（注2）：付録Bの「コントロール説明およびその実例」を参照。

ユーザの責任

1. トランザクションの適当な許可，開始，点検の責任は，つぎの方法により明確にされるべきである。

a．責任の明確化

b．高度な責任レベルを確保するための許可業務の点検

c．任務の分割

1）記録保管

2）資産保護

3）検討／許可

2. 転送書類は，その作成，点検，許可の責任について，フォーム上の識別コード，あるいは作成者，点検者，許可者のイニシャルを当該書類上に記入させることによって責任の所在を明らかにしなければならない。

3. 最近のドキュメントを識別・チェックできるよう文書に日付けを添付する。

4. トランザクションが膨大であったり，異常または稀にしか現れないタイプの場合，転送ドキュメントやそのトランザクション用のログ・エントリに監督者は署名すべきである（この時使用されるのは，トランザクション・コントロール・ログ(注3)である）。

5. 転送フォームの稼動は，作成とシステム・エントリのプロセスの間で何も失なわれないようコントロールされねばならない。

a．事前に番号を付与したフォーム ― もし可能なら，このフォームの採用により，全転送フォームの算定が可能となり，行方不明のフォームの指摘が容易となる。

b．何が，誰から，誰に転送されているかを示すルート・スリップ。

c．でき得るならば，共通取引グループに区分する。

6. バッチは，つぎの方法でコントロールされる必要がある。

a．コントロール・トータルは，キーとなる識別子や金額の欄か（算定数のハッシュは金額のトータルと同程度に重要），バッチ・レコードの数の上に置かれるべきである。

b．もしバッチ・コントロール・グループがあるなら，それは，全入力を受信し，バッチし，コントロール・トータルを決定し，コントロール・カードを

生成し，バッチをＩＳＤの処理に提供するために用いられるべきである。

c．バッチ・コントロール・グループが存在しないなら，バッチ・コントロール・トータルを算出し，コントロール・カードを作成し，そして作成者はバッチ・コントロール・ログ・エントリを実行しなければならない。その際責任ある監督者は，そのバッチを取りあげ，コントロール・カードを検査し，コントロール・ログ・エントリを検証しサインするとともに，バッチをＩＳＤに提出する必要がある。

d．コントロール記録の共通認識を得るため，汎用的な識別子が用いられなければならない（例，保険証券ナンバ＝9's）。

（注３）：コントロール・ログは本ガイドラインにおいては，ユーザによりシステムに投入されたトランザクション／バッチの統計を内容としてもつ帳簿（あるいは書類，書式）を指している。追跡調査とか参照用に用いられることが主目的となっている。

B．処理コントロール

ＩＳＤの責任

1. 処理コントロールには，つぎの意図がある。

a．システムからの出力＝システムへの入力。

b．プログラム・インタフェースは，送付されたプログラム出力と受け取られたプログラム入力を合致させる必要がある。

c．さらにシステム・インタフェースに要求される役割はつぎの２つである。

1）送付されたシステム出力＝受け取られたシステム入力。

2）共用ファイルは，送受両システムのコントロール要件を満足させなければならない。

2. トランザクション・ソースに密着して開発された平衡コントロールは，出来得る限り実際的な処理を通じて行われるべきである。

3. プロセシングのコントロール手法

a．ランごとにコントロール・トータルを集計する。

1) ハッシュ・トータル

2) 金額コントロール・トータル

3) 記録カウント

b. 極めて重大な異動およびコンピュテーションの結果をチェックする。

1) 限　界

2) 合理性

3) 欄からのはみ出し

4) 内部ファイル・ラベル

4. もし入力がバッチ・フォームで，そのフォームのまま維持できるなら，バッチ・コントロール・トータルは，プロセシングの全体を通して集計されるべきで，詳細な点まで帳尻の合ったものでなければならない。

5. 1つのラン／モジュールや1つのシステム内部でプロセシングがかなり容易に再開できるポイント（例，ジョブ・ステップの間）は，再開部位として「マーク」される必要がある。

6. プロセシングが再開点に達した時，処理中のデータは，指定ファイルに書き込まれなければならず，この情報こそが，失敗以前の最も近い再開点までシステムを再ロードするために用いられる。

7. 全データのバックアップは，「データ保存」の項で示されているレベルまで完全性と十分性を持たなければならない。

ユーザの責任

1. ユーザは，つぎのような作業項目に従い，コントロール・プロセスで進行中の事務管理に関心を払わなければならない。

a. 入力から出力までの取引の定期的追跡またはエラー・リストの作成。不一致は調和解消されなければならない。

b. 出力レポート上のトータルを定期的に手作業により横計算（クロスフット）する。可能ならレポートの品目記載行でも同様の作業を行う。

c. 別個のレポート間で共通するデータに偏差がないようチェックする。

d．機械生成値の定期的な有効性チェック。

2. ユーザ・サイドの点検により生じた処理コントロールに対する彼等の不満は，直ちにＩＳＤに通告される必要がある。

（注）ユーザ・チェックの頻度は，当該システムの複雑さやインパクトの大きさに左右されることが多い。

C．出力コントロール

ＩＳＤの責任

1. 処理および入力のコントロール・トータルは，出力が準備される際，全てのレコードが一時に算定できるよう，出力コントロール・トータルと結果に一致を見なければならない。

2. 出力コントロール・トータルは，出力データセット・ファイルの後書き，およびそれが出力の検査に使用できるあらゆる場所に書き込むべきである。後書きレコードに含まれるものはつぎの通り。

a．識別子（例，保険証書ナンバ＝9's）

b．ファイル／バッチ・ナンバ

c．レコード・カウント

d．重要欄のコントロール・トータル／ハッシュ

3. 出力設計では情報の誤解や誤用を防ぐため，印刷書式を指定すべきである。

a．タイトルは全て，無意味なものであってはならない。

b．作成された全レポートには，処理されたデータ，そのデータの日付け（あるいは処理日時）が記載される必要がある。

c．レポートの各ページに必ずページ・ナンバを入れる。

d．コンピューテーションに含まれる全ての変動要因は，チェックを容易にするためにも印刷されなければならない。

e．プリントアウトの最後は，標準的なメッセージ（例，「レポート末尾」）で表示する。

4. 出力の正確度を高めるため，選択的にシステム・チェックを行う方法もある。

このようなチェックには，つぎのようなものがある。

a．関連欄の横計算（クロスフット）チェック

b．残高（バランス）チェック

c．既定限度との比較

d．サイズ，ブランク，アルファベット，数字等の有効性チェックのための欄内容点検

5. 出力配布先管理リストは，配布が認可先に限定されるよう出力管理要員により保存される必要がある。

6. 出力の配布先と時期を適切にするため，その配布手順を確かなものとする。遅滞が予想される場合，ユーザは早急にその旨通告すべきである。

7. ユーザは，各レポートの必要性が依然継続しているか否か，周期的に自答すべきである。

8. 事前に印刷されたフォームが出力として用いられる時，ナンバリング済みなら管理が事の外容易となる。

9. 出力コントロール・グループは，完全さ，合理性，均整を対象に出力を精査すべきである（必ずしも正確度はこの場合要求されない）。

ユーザの責任

1. ユーザは各レポートに対する必要性を定期的に点検し，不必要なものは中断すべきである。

2. 出力の配布管理リストは，ユーザにより作成維持されなければならない。出力管理要員はこのリストを利用して，配布予定の出力の全部をタイムリに受け取ったかを確認し，当該レポートの配布許可を受けた人物にのみ手渡っているかチェックする。

3. ユーザは，トータルの正確さだけでなく，その品目の合理性についても適宜出力を点検する。

4. 出力結果を入力と比較し，手作業によるコンピュータ処理をチェックするため，個々のドキュメントまたはリストを選択的に点検する方法もある。

5. ユーザは，問題に直面すれば直ちに適当なＩＳＤの接触先に通報すべきである。

6. 微妙なデータに対しては，特別な配布手順を設定する（例えば給与支払データ）。

7. 事前に印刷されたフォームが使用される場合，定期点検を行い廃止フォームの全てを除去破壊する必要がある。

D．直接的更新手法を用いたシステムのコントロール

ＩＳＤの責任

1. システムのアクセスは，認知されたターミナルとオペレータに限られる。

2. アクセス・セキュリティ・マトリクスを使用する際，ファイルに対する行為レベル（例えば，インクワィアリ，更新）は，許可レベルと常に対応しなければならない。

   a．必要でかつ適当な場合，この方法は，所定レコードの欄にも選択的に拡大使用することができる。

3. 成功あるいは目的の如何にかかわらず，全てのアクセスはシステムによってログされる必要がある。

4. 一定時間何の活動もおこさなかったアクセスは，全て自動的にシステム側で中断されるべきである。耐え得るレベルとして，われわれは２～３分の非活動時間を勧告する。

5. ファイルの直接的更新は，つぎのような結果をもたらす。

   a．レコードが生成されバックアップ・ファイルに追加される。このレコードは，更新対象とされるレコードの前後のピクチャーをも含むべきである。

   b．エントリの日付けおよび時刻を伴なったトランザクションと開始者のコードが取引ファイルに投入される。

      1）このファイルからトランザクション・ログは，コスト・センタ別にリストされ，点検のためユーザ分野のリーダに定期的に配布される。

   c．最後のシステム・バックアップ・ダンプから算出されたコントロール・ト

ータルと，最後のバックアップで生じたプロセシングのためのコントロール・トータルの累計を内包するコントロール・ファイルは，当面する作業のために，これらの累計を更新させなければならない。

d．上述したアプリケーションの理論的システム・ダイアグラムは，図1に示す通りである。

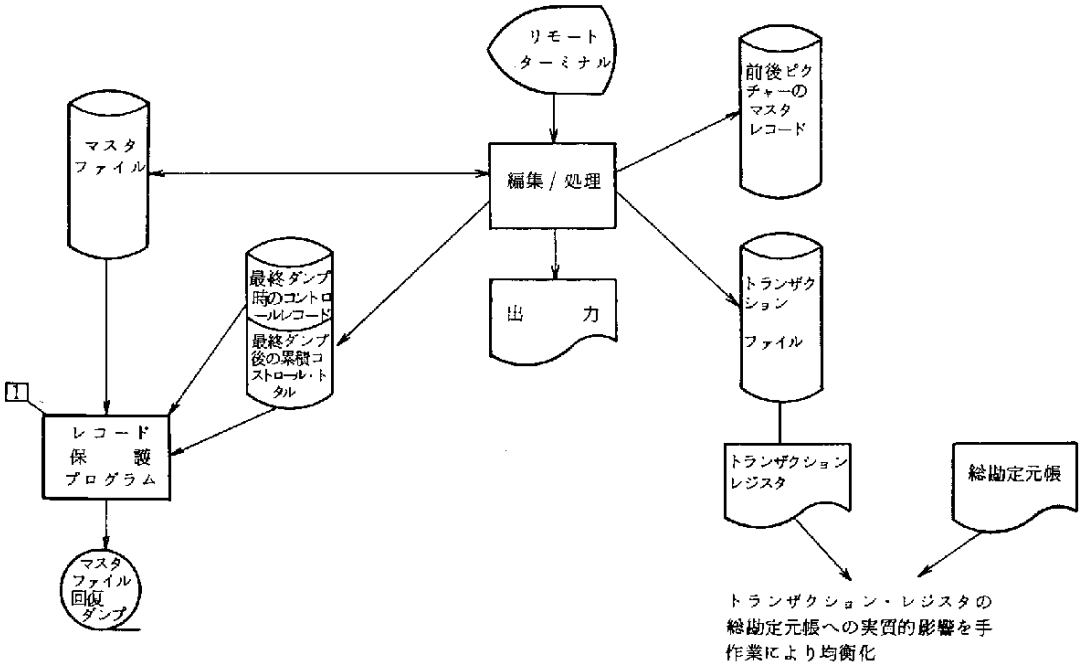


図1. 記録保護プログラムにおいては，古いコントロール記録やコントロール累計は，ダンプ中にマスタ・ファイルから抽出されたトータルと帳尻を合せられる。

ユーザの責任

1. 責任あるユーザの管理者レベルは，ファイルを直接更新する必要があり，かつ，またその能力を有する人のみが行い得ることを保証すべきである。

2. トランザクション・ログ・リストは，責任あるユーザの部門リーダにより徹底的に検査され，異常な，過剰な，不合理な，そして不許可の行為がないかどうかチェックされなければならない。

3. 疑問の残る品目は即座に精査を行い，ファイルのインテグリティに支障がないようにすべきである。

E．データ保存

ＩＳＤの責任

1. データ保存のフォーマットおよびその期間に対する規制機関の要求は，全て満たされるべきである。情報源として，つぎのものがあげられる。

a．適当なユーザ部門

b．レコード・マネジメント・サービス

c．法律担当部門

d．全社的コントローラ部門

2. データは，生産ファイルのバックアップとユーザの担当部門の活動へのサポートのために必要な時間だけは，少くとも保持されなければならない。

ユーザの責任

1. システム設計時にユーザは，システム出力の有効性チェックに必要な時間数をあらゆる努力を払って決定すべきである。この長さがどうであろうと，こうして決定された所要時間は，出力およびその出力の生成に必要なデータにとって最少の保存期間となることが大部分である。

2. ユーザは，その最低保存期間について，ＩＳＤと緊密に連絡をとるべきである。この期間の決定要因はつぎのとおりである。

a．バックアップと調整用に公刊されている洗練された数値。

b．法律。

c．外部調査機関（例，内国歳入庁（ＩＲＳ），州監査官）のデータに対する必要性。

F．エラー・コントロール

ＩＳＤの責任

1. システムはエラーの十分な識別手段をもたなければならない。

a．除去項目は全て，除去理由を示す意味とともに相応なエラー・リストに掲

載されなければならない。

b．共通のデータを使用しているシステムは，クロスチェックが容易となるようエラー・リスト上の当該データの識別に画一性をもたせるべきである。

c．除去理由を示す文字またはコードとともに，誤りのあるレコードの全体を別のエラー・データ・セットに書き込むことは，良いアイデアである。

2. 金銭的エラーの目録も必ず用意されなければならない（例，仮勘定）。これは，未修正のエラー追跡を可能とするからである。上述した1(c)のデータセットが利用できる。

a．ISDは，仮勘定リストのような未解決エラーのリストを作成し，備忘録として関係ユーザに提出すべきである。品目のエージングもまた良い手段といえる。

b．訂正は，トランザクションを意図通りマスタに照らして修正・処理することであり，ファイルや仮勘定・エラー・リストからトランザクションを除去することでもある。どちらの場合も，手直しした行為はトランザクション・レジスタかそれと同様のリストに現われ，その後点検のためユーザやユーザのコントロール・グループへ返送される。

3. エラーはユーザに戻され訂正されなければならない。この訂正においても，それだけの能力を有する高レベルのスタッフに戻すべきなのはいうまでもない。

4. 全ての欄の正確さを期すため，修正項目の再記帳（リエントリ）は必ずチェックする。以前に誤りのあった項目だけでなく，レコード全体の再チェックが必要である。

ユーザの責任

1. ユーザ側の管理では，つぎの事柄を確実にしなければならない。

a．仮勘定リストの点検と修正のスピードアップでエラー訂正の適時性を確保する。

b．エラー・リストの注視と過度のエラーをフォロー・アップすることによってエラー数を最低限に抑える。

c．修正手順は，最も迅速で，正確で，かつよくコントロールされた作業でなければならない。

2. エラー・リストの作成では，ユーザがつぎの項目について各エラーを修正するごとに，その旨表示が必要である。

a．訂正の日時

b．訂正の担当者

c．訂正されるトランザクションの取引ナンバまたはそれに代る識別記号

3. ユーザは，エラーの発生源をできる限り突きとめ，そのエラーの訂正に努めなければならない。

4. エラーは，ハードウェアまたはソフトウェアで発生したことが明らかである場合にのみ，ＩＳＤに照会される。

G．データ変更コントロール

ＩＳＤの責任

1. 製品ファイルやデータ・レコードに内容に影響を与えるどのような変更も，関係ユーザ部門の事前の文書による承認なしで，ＩＳＤによって行われるべきではない。

a．もし適切な時点で関係ユーザ部門の承認が得られないならば，その限りにおいて変更はあり得るが，その場合直ちに変更が行われた旨当該ユーザ部門に文書で通知されなければならない。

2. 製品データの変更は，意図した修正だけが実行されるよう制御されるべきである。

3. 製品データの変更は，変更されたデータ項目（できるならば，生じた変更自体も）を明確に表示するため，トランザクション・リストに反映させなければならない。このリスト作業の結果はユーザやユーザのコントロール・グループに送達され，変更の影響が当初の意図通りであるか否か検証される必要がある。

ユーザの責任

1. データ項目の変更は，そのシステム全体へのインパクトの見地から評価され

るべきである。もしユーザが，その変更の正当性と有害を及ぼさないという確信をもつことができたなら，ユーザは入力コントロールに従ってそれを承認することになる。

2. ユーザは，システムが作成したトランザクション・リストを点検し，望むべき変更のみがなされたかを確認すべきである。

H. ファイル・セキュリティ・コントロール

ＩＳＤの責任

1. 全てのテープ，ディスク・パックおよびデータセルは，容易に処理プログラムによりチェックできる適切な識別子（例，ファイル・ラベル）を備えなければならない。

2. 全てのファイル媒体は，レコード・カウントと批評欄（クリティカル・フィールド(注4)）を持ち，同時に処理プログラムにより対照されるトータルをもつようにすべきである。

3. 磁気媒体のファイルは全て，処理中の事故や災害で破壊された場合を考慮し，そのファイルの再生を可能とする十分なバックアップを備える必要がある。バックアップは，ファイル中のエラーの検知を可能とするだけの期間は確保されねばならない（例，ユーザ出力検査手順）。

4. 全ての製品データセットは，さかのぼって保護されるべきである。

ユーザの責任

1. ユーザが管理するファイル（例，パンチ・カードやある種の磁気テープ）には，つぎの事項に留意すべき必要性がある。

ａ．つぎの項目の使用により，即座の識別を可能とするマークを添付すべきである。

1）ラン・ナンバ

2）ラン日時

3）システム

4）場所の順序（例，４の１）

b．許可の無いアクセスや不注意による破壊から防護されるようファイルは蓄積されなければならない。

（注４）：本ガイドライン中で定義されている批評欄は，つぎの特長を有している。

- 総勘定元帳の収支残高による裏付け
- 処理あるいは処理結果の重視
- コントロールの実用性

Ⅱ．管理的コントロール

A．プログラム／システム・ドキュメンテーション

ＩＳＤの責任

1. アプリケーション・ラン・ブックやコンピュータ・センタ・ラン・ブックの標準は，ＩＳＤ標準および情報マニュアル（Ｓ＆ＩＭ4.04－02および4.07－01）にそって最低限遵守されなければならない。
2. ＩＳＤは，ユーザ・マニュアルの作成に必要なレイアウト，フローチャート，機能表示の全てが時機を得て供給されるよう保証すべきである。
3. 全てのドキュメンテーションは，常に最新のものでなければならず，オリジナル・システムに起った変化の全てを反映したものでなければならない。

ユーザの責任

1. 当該システム向けの「ユーザ・マニュアル」の存在およびその完全さに，ユーザは絶えず関心を払う必要がある。これにはつぎの項目が含まれる。

a．コントロールおよびインプットの機能的効果を含む作成用の入力レイアトと完全なインストラクション。

b．出力レポートの定義および包括的な解釈の説明。

c．エラーの修正ができるだけ速やかとなるようなエラー解釈・訂正手順。

d．システム概要の表示に含まれるものはつぎの通り。

1）その用途

2) システム機能の作動の仕方

3) ソース・ドキュメンテーション

4) その能力

5) 総合的なシステム運用の詳細表示(インタフェース目的，ファイル結果など)

B．プログラム変更コントロール

ＩＳＤの責任

1. 変更がなされる以前に，適切な許可がユーザから得られなければならない。
2. ＩＳＤは，変更されたプログラムの徹底的なテストを確実にし，そのプログラムが再び生産現場に投じられる以前に，テスト結果についてのユーザの正式な承認が得られるようにする。
3. プログラムの変更により影響を受けたドキュメンテーションの全て(システム，ユーザ，プログラム)は，その変更を反映するよう改変されなければならない。
4. 会計手法の全ての変更は文書化され，ユーザと会計部門の双方より正式の承認をうける必要がある。

ユーザの責任

1. ユーザの要求するあらゆる変更は，責任あるユーザからの文書による許可要請に基づかなければならない。
2. プログラム変更にまつわる品質管理の一方法として，ユーザは既存システムに重大な変化が発生したか否かをテストすることもあり得る。
3. ＩＳＤのプログラム変更テストの結果は，生産現場に導入される以前に，他の影響を受けるシステムのユーザだけでなく，中心システムのユーザからも正式の承認をとりつける必要がある。
4. 全てのユーザ・マニュアルは，プログラム変更によりもたらされた変化を反映するよう更新されなければならない。

Ⅲ．組織的コントロール

A．責任の分担

ＩＳＤの責任

1. 全てのコンピュータ・システムにおいてＩＳＤの介入は，それをランし展開させる機能に分離されなければならない。

   a．コンピュータ・システムの開発者は，それをランさせる者と同一人物であってはならない。アプリケーションやオペレーションも機能ごとに分割されるべきである。

2. ＩＳＤは，当該システムへのユーザの要求にそって，システムの運用スケジュールに責任をもつものとする。

ユーザの責任

1. 全てのコンピュータ・システムにおけるユーザの介入は，エントリ・データを提供する機能，それに許可を与える機能，戻り出力の受領・点検を担当する機能等に分離されなければならない。

   a．入力データの作成者は，入力の許可者と同一であってはならない。

   b．入力データに許可を与えた者は，そのデータの作成者と重複してはならない。

   c．システム出力の受領・検査を行う者は，入力の作成者と同一人物であってはならない。

2. 対象システムをいつランさせるかを決定するのはユーザである。

B．マネジメント・トレイル

ＩＳＤの責任

1. 直接間接を問わず，企業の会計簿に影響を与える全てのシステムにとって，つぎの要件が満たされなければならない。

   a．記帳のサポート ― システムは，それが生成した合計の記帳のために詳細なサポートを作成するか，要請に応じて作成する能力をもたなければならない。

b．収支のサポート ― システムは，企業の帳簿で資産と負債の帳尻をサポートするため，ハードコピーの詳細な試算表を作成するか，要請に応じて作成する能力をもたなければならない。

2. 監査証跡は，トランザクションの最初から最後までの追跡を可能とするため，全てのシステムに組み込まれる必要がある。その逆方向あるいは往復型の追跡もできれば用意したい。

a．監査証跡は，最初のソースからコンピュータ環境における記帳，そして処理結果のプリントアウトおよび帳簿への最終的な転記までのトランザクション追跡能力をもつ。

b．反対に，証跡は，マスタ・レコードの更新前の状態を再構成することも可能である。

1）現状のプリントアウト，マスタ・レコード，トランザクション・レジスタ等に「最終取引期日／最終取引形態」を記入することにより，この方法が実施される。

3. トランザクション処理後，十分なサポーティング・ドキュメンテーションが適切な期間利用できるようにすべきである。

4. ＥＤＰシステムにおけるデータの集約は，監査証跡を妨害したり，その価値を減じるものではない。

5. ネットワークにおけるような直接入力は，監査証跡の不可欠要素としてのソース・ドキュメントや認可要件の必要性を軽視しはしない。

6. マスタ・ファイルの収支残高は，常にその構成部分と関連づけられなければならない。

ユーザの責任

1. トランザクション処理後，十分なサポーティング・ドキュメンテーションが適切な期間利用できるようにすべきである。

2. ソース・ドキュメントは，以後の検索が容易となるようファイルされなければならない。

3. 出力ドキュメントは，以後の検索が容易となるようファイルされなければならない。

付録A　様々なコントロールが証明すべき事柄の概要

入力コントロール

- データは合法的である。
- データは正確でかつ完全である。
- データは正確かつ完全に転送されている。

処理コントロール

- 許可されたファイルの利用。
- ファイルは正しい。
- データはプログラムとシステム間で正確かつ完全に転送されている。
- 出力は入力に正確かつ完全に基づいたものである。

出力コントロール

- 出力は入力＋（プラス）トランザクション，または入力－（マイナス）トランザクションに等しい。
- 出力は完全で正確である。
- 出力は均整がとれている。
- 出力はその理解が容易なように設計されている。
- 出力は必要である。
- 出力は許可を与えられた受け取り手に渡っている。

直接的更新手法を使用したシステムのコントロール

- 許可されたユーザだけがアクセスを許されている。
- 無許可の更新は最大限に困難である。
- 無許可の更新は手順の均衡で出来る限りキャッチされている。

データ保存

- 保存は全ての要件（法律，ＩＲＳ，システム・バックアップなど）を満たし

ている。

エラー・コントロール

- エラーは完全かつ正確に発見され訂正されている。
- エラーは速かに修正される。
- エラーの量は過大ではない。

データ変更コントロール

- 変更は許可をうけたものである。
- 変更は完全である。

ファイル・セキュリティ

- ファイルは適切に識別されている。
- ファイルは十分保護されている。
- ファイルは十分なバックアップをもっている。
- 意図的でかつ許可をうけたアクセスだけが許されている。

ドキュメンテーション

- （最低の要件である）標準および情報マニュアルの要件が満たされている。
- ドキュメンテーションは最新のものである。
- ユーザ・マニュアルは完全でかつ正確である。

プログラム変更コントロール

- 変更は許可されたものである。
- 変更は完全である。
- 変更のドキュメント化は十分である。
- テストは完全であり，関係者の満足を得ている。
- コンバージョンのインパクトは非常に少ない。
- ユーザは事前に準備できている。
- ドキュメンテーションは更新されている。

責任の分担

- コントロールが維持できるほど完全である。

マネジメント・トレイル

- 証跡は完全でかつ正確である。
- 証跡は双方向型である。

付　録　B

入力コントロールの定義

入力コントロール	定　　義	例
コントロール・トータル	ファイル・レコードの特定欄に記載された価格の金額および件数の合計。 ファイルの管理に用いられる。	ある時点までの給与支払ファイルに記入された通年給与合計は 784,964.5ドル
バッチ平衡	全項目が処理済みか否かを確認するため，確定している照査合計と実際に処理された項目を比較すること。	入　力　　コントロール 20　レコード　20 112925638　保険証券番号ハッシュ　112925638 2565.99　保険料合計　2565.99
バッチ・コントロール・ログ	バッチまたはトランザクションの照査数値および関係詳細を内容とするログ	7／22／76 ― バッチ＃41-100 レコード ― 保険料合計 921,475.37ドル 保険証券ハッシュ・トータル 894,371,711
バッチ・コントロール・トータル	特定の組合せのトランザクションに適用されるコントロール，ハッシュまたはレコード・カウントの合計。トランザクションはこのトータルと均衡している。	20レコードの最初のバッチは，保険証券のハッシュ合計が112,925,638で，保険料合計は2,747ドルであった。
バッチ番号チェック	全項目が処理中のバッチに属するものであることを確認するため行う個々のバッチ項目上のバッチ番号とコントロール・バッチ番号の比較対照。	
チェック・ディジット	欄の内容を検査するため使用される数字。欄内では数学的な機能の数字であり，特殊数字として添加される。その値は，欄の有効性をチェックするため算定・比較し得る。	欄　276924 乗因数　21212 4+7+12+9+4＝36 -40 チェック・ディジット　4
完全性チェック	データを事実上含んでいるか，データを含まねばならない欄を検証するチェック	チェックは，受取人または金額の欄が空白の場合，プリントされてはならない。

入力コントロール	定　　義	例
一貫性テスト	特定欄の内容が他の関連欄の内容と一致しているかを確認する検査。 一貫性テストは，また同じデータを使用している別のプログラムが共通の形でそのデータを扱っているかを確認するのに用いる。	支払済みの保険証券は，保険料支払日に記入があってはならない。プログラムAの月間保険料がプログラムBに移された途端，年間保険料として扱われてはならない。
データ予測	ある時点またはある条件における特定のトランザクションやデータ項目を予測すること。	給与支払システムは，どの給料未支払従業員も週40時間と計算していると予測する。
フォーマット・チェック	特定欄のデータのフォーマットが適切かどうかをチェックすること（数字あるいはアルファベット）。	一連の文字72P×192は，正しい保険証券番号ではない。
ハッシュ・トータル	非金銭欄の数値量の合計でファイルまたはバッチのコントロールに用いられる（金額照査合計と対応）。	ファイル・レコードの保険証券番号のハッシュ合計は， 7,829,771,592,346である。
見出しラベル	ソース，アプリケーション，日付け，あるいはその他の識別指標に対するファイルまたはバッチの内部識別物。	
入出力コントロール・グループ	入力，そのバッチ，コントロールの完全性，出力の完全性，出力の配布を確実にする責任を負う個人またはグループ。これは明確に入力準備と分離されねばならない。	
キーストローク検証	パンチカードへの最初の入力が正確か否かをチェックするため，データを再びキーパンチでエントリすること。偏差は機械的にキーパンチャに通知される。	
限界テスト	指定された上下限値をもとに，特定の数値欄が適合しているか否かチェックするテスト。	保険証券の貸付利率が1ドル以下なら記載する必要がない。
ライン・コントロール・トータル	印刷された出力の行数のトータル数。	5月の保険証券貸付ジャーナルは47,000件のエントリを含んでいた。
機械読取可能ドキュメント	磁気的にドキュメント上にコード化されているデータ。このデータはコンピュータ周辺機器で直接読み取れる。	小切手末尾の口座番号は磁気的にコード化されている。
オーバフロー・チェック	欄の容量をもとに，その中のデータのサイズをチェックすること。	10×499.50の積は5桁欄には入りきれない。

入力コントロール	定　　義	例
レンジ・テスト	一定の上下限数値をもとにある数値欄をチェックすること。	5％の保険証券貸付利率は，証書番号1350470から4549999の間にのみ適用される。
合理性テスト	レコードやトランザクションの他の欄に含まれているデータと比較してデータ欄をチェックすること。	額面1万ドルの保険証券は，月間保険料7,995.97ドルとはならない。
レコード・カウント	ファイルまたはバッチ中の個々のレコード数の算定。	給与支払ファイルは7,043件のレコードを有している。
インプット正当性チェック・ラン	入力が処理にまわされる前に，その有効性をチェックするためシステム内に含まれているプログラム。一般には多数の有効性チェックを組合せたものが多い。	これらのプログラムは入力編集プログラムと呼ばれるのが普通である。
シーケンス・チェック	処理されるレコードまたはトランザクションの識別子またはキー欄内の数値順序をチェックすること。	保険証券番号4 216 961は，順序として5 096 712に先行し，4 216 942の後にしなければならない。
通し番号	ドキュメントやバッチは，そのコントロールを容易にするため，順序立てて番号を与えられるべきである。	小切手に記載されたチェック・ナンバ
視覚確認	ドキュメントの完全性や合理性を視覚で点検すること。	
視覚確認－ＣＲＴ	データがＣＲＴ端末から入力される時，そのデータはすぐにその端末のディスプレイ上に現われ，送り手自身が目でチェックできる仕組みとなっている。データは送り手がこの検査を終えた後はじめてシステムにより受け付けられる。	
後書きラベル	ファイル上のレコードのカウント合計とコントロール・トータルを含むファイル・レコードで，レコード処理中の累積値と比較される。	
単一構造テスト	単一構造を必要とするか，正にそういう構造をもっている欄（または欄のセット）を確認するテスト。	日付け欄は，年（２文字），月（２文字），日（２文字）から構成されている。
正当性テスト	フォーマット，数値，コード等の要件をデータ欄が満たしているかをチェックすること。数値は表や算定ルーチンを使っても検査できる。	現在の日付け項目は6桁であり，7621は是認できるが760201は認められない。

（注）この表の主要情報提供源は，Tauche, Ross & Co. の Computer Control and Audit である。

Bibliography

1. Security, Accuracy, and Privacy in Computer Systems
   by James Martin of the IBM Systems Research Institute
   1973

2. Security for Computer Systems
   by The National Computing Center, Ltd.
   1973

3. Security Standards for Data Processing
   Wooldridge, Corder, and Johnson
   1973

4. Computer Control and Audit
   Touche, Ross & Co.
   1976

5. Management Controls in Data Processing
   IBM Manual

6. Basic System Controls
   by Aetna's Data Processing Educational Program (ADPEP)

7. "Auditing Aspects of Data Processing"
   Data Management, July 1972, page 17

8. "Auditing Control and Systems Design"
   by Eoster Brown; presented in the Journal of System Management, April 1975

9. Data Control Guidelines
   by J.R. Sharralt, National Computing Center, Ltd. as reviewed by the Automation Training Center in EDPACS, October 1975, page 12

10. Systems Analyst Training Program
    by DELTAK

11. "Why Document"
    Data Management, January 1975, page 6

12. Computer Control Guidelines
    The Canadian Institute of Chartered Accountants
    1972

13. Computer Audit Guidelines
The Canadian Institute of Chartered Accountants, 1975

14. "EDP Security Control"
The Internal Auditor, July/August 1974, page 16

15. "EDP Controls to Check Fraud"
Management Accounting, October 1974, page 43

16. "The EDP Technician, The Accountant, and Internal Control"
Management Accounting, September 1975, page 38

17. The Practice of Modern Internal Auditing
by Lawrence Sawyer, The Institute of Internal Auditors, 1973

18. The Handbook for Auditors
James Cashin, editor-in-chief, 1971

19. The Effects of EDP on the Auditors Study of Evaluation of Internal Control
Statement on Auditing Standards #3, by the Auditing Standards Committee, AICPA, December 1974

20. "An Audit Perspective of Operating System Security"
The Journal of Accountancy, September 1975, page 97

付属資料2
コンピュータ・セキュリティの監査と評価

付属資料2

コンピュータ・セキュリティの

監査と評価

原題：Audit and Evaluation of Computer Security

（本報告書は，全12章で構成されているものであるが，都合により第6章までを紹介し，残りは別途紹介することと致したい。）

米国商務省標準局

コンピュータ・セキュリティの監査と評価

概　　要

1977年3月22～24日，コンピュータ・セキュリティの監査・評価に関する研究集会がフロリダ州マイアミで米国標準局（National Bureau of Standards, NBS）の主催により開かれた。この研究集会は，米国会計検査院（General Accounting Office, GAO）の後援を得，連邦政府内情報処理標準（Federal Information Processing Standards, FIPS）計画第15作業部会が策定したコンピュータ・セキュリティ監査関連作業の第1段階を構成するものである。集会の目標は，この分野の最新情報を集約し，将来の研究課題を確定することである。また第2段階の目標は，専門の作業グループによりこうした情報を編集し連邦政府内情報処理ガイドラインの形で政府機関に提供することである。

NBS側連絡責任者Zella G. Ruthbergの協力を得てGAOのRobert G. McKenzieは，第15作業部会の中に非公式のチームを設置し，研究集会の開催要項とテーマを企画させた。その結果，研究集会はコンピュータ・セキュリティ監査の領域における10項目をカバーすることになった。

また米国内部監査人協会（The Institute of Internal Auditors, Inc., IIA），米国公認会計士協会（American Institute of Certified Public Accountants, AICPA），カナダ勅許会計士協会（Canadian Institute of Chartered Accountarts, CICA）および上記チームから提出された資料で，監査・コンピュータ両分野から議長，書記，参加者が選出された。研究集会のまず最初の3日間で彼らは，議事に含まれる10件の報告書に目を通し理解を深めた。以下はその報告書を要約したものである。各レポートは独立したもので，議事の初めにとりあげられているのはマネジメント関係，後半にとりあげられているのは技術色の強いものとなっている。

内部監査基準セッション

コンピュータ・セキュリティの監査基準に関する勧告案を起草するため，このグループはまずコンピュータ・システムの内部監査という大枠を定義し，つぎにコンピュータ・セキュリティ監査の定義に移った。この監査は，承認やプログラム結果の範疇の責務もカバーするものとして特長づけられている。結論として，ＧＡＯ発行パンフレット「政府関係の機関，計画，活動，機能等の監査基準」がＥＤＰ監査の内部監査基準に適切な基盤を提示しており，監査人がコンピュータ・セキュリティ監査において，これらの基本的な基準を遵守するに必要な副次作業を明確にするため，AICPAの監査基準第３号のごとき補完的基準が不可欠とされている。こうした補完的基準が必要な領域としてはつぎの３つがあげられている。

(1)　システム開発

(2)　運用システム（アプリケーション・コントロール）

(3)　物理的セキュリティおよび全般統制

システム開発の場合，監査関係者は，プランが盗難やエラーに対する管理，適切な監査証跡，マネジメント目的や法律との整合性，十分なドキュメンテーション，適切な設計承認機構および全般的効率，経済性等を配慮したものであるよう保証すべきであろう。さらに運用システムにあっては，監査はそのアプリケーションが基準や最新の設計仕様に適合し，かつデータの内部管理と信頼性が健全であることをチェックするものとなろう。また物理的セキュリティと全般的管理の面では，組織体系，物理的設備，要員管理，支援態勢，ソフト／ハード管理等の全てが運用目的にそっているかどうか検証される。

このセッションの活動勧告の骨子はつぎの通り。

(1)．ＧＡＯはこれら補完的基準を再検討し他の基準とのだき合せを考慮する。

(2)　再検討された補完的基準に，連邦監査推進会議（Federal Audit Executive Council）の承認をとりつける。

(3)　ＮＢＳは，補完的基準をＦＩＰＳガイドラインの一部としてとり入れ，コン

ピュータ・セキュリティ監査の領域を強化拡充する。

資格・訓練セッション

コンピュータ・セキュリティ監査の実行に必要な資格ならびにトレーニングとは何かという問いに対し，このグループは，監査に不可欠な広汎な知識のアウトラインをまとめた。

(1) コンピュータ・セキュリティとは，情報の取得，処理，蓄積，分散等に関わる総合性，正確性，信頼性を保証する全てのコントロールを含んでいる。

(2) 監査担当者は，会計，ビジネス，エンジニアリング，ＯＲ，コンピュータ工学，経済等の基本的学位を持ち，同時にマネジメント，監査，データ処理，通信等に確かな素養を保持していなければならない。

(3) 複雑なシステムの監査は，実に多岐にわたる専門知識を必要とするので，学際的チームの活用が望ましい。

(4) 教育訓練は，全ての標準的教育機関でうけられるようにすべきである。

(5) コストは組織ごとに様々な変動要因があるので，推定不可能である。

(6) 監査に必要な最低限の知識はつぎのとおり。

a) 一般的なマネジメント・監査の概念

b) データ処理および通信の専門知識

c) 経験および教育から得たa)およびb)の包括的統合

基本的知識のアウトラインが含むカテゴリは，つぎのように列挙することができる。

(1) コンピュータ・システム，オペレーションおよびソフトウェア

(2) データ処理技術

(3) データ処理業務のマネジメント

(4) データ処理業務のセキュリティ

(5) リスク・アナリシスおよび脅威の予測評価

(6) マネジメント概念およびその実務

(7) 監査概念およびその実務

(8) コンピュータ・セキュリティの評価に必要なその他の資格

これらのカテゴリの各々についても討議がなされ，アウトラインの最終案には，各カテゴリごとの主要学科一覧が添付されている。

セキュリティ管理セッション

このセッションは，「監査のアプローチおよび技法でセキュリティ管理業務の評価に効果なものは何か」という設問に答えるものである。当初このグループは，連邦政府機関におけるセキュリティ管理業務法，つまりブルックス法（PL−89−306）と1974年プライバシー法の法的基盤を討議したが，さらにセキュリティ管理業務を，監査が標準的な検査となるよう詳細に規定すべきであるとの提案も行っている。本節の以下の部分は，このセキュリティ管理業務の定義にあてられている。

レポートの前半で触れられているもう1つの重要なテーマは，プライバシー法の国際的な共通基盤に対する必要性である。プライバシー法案がすでに立法化されているのは，スウェーデン，西ドイツで，ノルウェー，デンマーク，フランス等では審議中である。国際的な諸機関は，日ならずしてこの問題の重要性を認識するようになるだろう。本レポートの付録の1つは，西独プライバシー法の概念である。

セキュリティ管理業務の主要な論点はつぎの通りである。

(1) ある組織のデータおよび情報源の保護責任は，それらを物理的に保管し，かつ責任を持つ個人，つまり各レベルの管理者層に属する。

(2) セキュリティ管理計画は，幹部の職務領域に入り，総合的なポリシーの策定，全体的な効率の監視から構成されねばならない。

(3) セキュリティ管理のプランニングは，3つのマネジメント・レベルで行われる必要がある。

a) 首脳陣の情報を使用する全体政策レベル

b) 運用上の指示を与える中間的政策レベル

c) 計画および資源配分を立案する運用レベル

(4) セキュリティ目標を達成するため管理者のコントロールは，3つのカテゴリを対象に行き渡らなければならない。すなわち，トップ・レベルで形成される政策，管理的物理的かつ技術的なセキュリティ手段の各種手順，標準的な管理業務の実行がそれである。

(5) ＡＤＰセキュリティ・コントロールには，a）事故対策，セキュリティ・ドキュメンテーション，許可管理リスト，プログラム・アクセス・コントロール，就業規則等の形をとる運営上のセーフガード，b）用地規制，災害対策，記録保管ライブラリ，配置手順等の物理的セキュリティ・セーフガード，c）データ・ファイル，プログラム・ライブラリ，ＯＳ，テレプロセシング，暗号化等を取扱うセキュリティ・システムの形での技術的セキュリティが含まれるべきである。

(6) 教育訓練は，ユーザだけでなくシステム関係者にも必要である。

オンライン・システムを例にとったセキュリティ・システムの一例が取りあげられている。本グループが示唆した最後の要件は，監査やセキュリティ管理の各業務が各々独立したものであるべき点，監査業務は組織の長に常時報告されなければならない点である。

様々なシステム環境における監査要因セッション

「さまざまなシステム環境にあってコンピュータ・セキュリティ監査で考慮されるべき事柄は何か」というのがこのグループの命題である。まず，こうしたセキュリティ監査の柔軟性構造モデルを開発するため，4種の概念的モジュールが指定された。その要旨はつぎの通りである。

(1) 実際的な監査の3構成要素（アクセス・コントロール，正確性，可用性）の定義。

(2) システムおよび環境の形態，つまり物理的要素，システム構造，要員の確認。システムは5つの特長，すなわちユーザ数，サービス・タイプ，システム組織，ユーザ・アクセス，アプリケーション組み合せによって描き出せる。

(3) 方法論，つまり監査対象となり得る各パラメータのスコアカード値を設定するコンピュータ監査モデルの定義づけ。

(4) 4例を対象としたモデルのテストで当該モデルの有効性をチェックする。

このグループは，監査人が設計チームの辿った一連のステップをそのまま並行的に踏襲すると断定している。そして設計チームの活動を概括して，要件，目的，鋭敏さの定義，物理的，システム的，管理的なパラメータの決定，適用可能なコントロール技術の指定，4種類のコントロールに対する判定……とまとめている。

(1) コスト

(2) アクセス・コントロール維持の効率

(3) 正確性維持の効率

(4) 可用性維持の効率

(2)～(4)の効率については理論値（1～10）を与え，当該コントロール利用の是非を決定する際には(1)～(4)の全部を使用している。つぎの設計チームの活動は，望ましい保護レベルを確保するためのコントロール・サブセットの選択，これらのコントロールの所要環境への適用，システムの再評価，全要件が満足されるまでの反復である。監査担当者が並行して行う作業は，目的，要件，鋭敏さの検討，現実的環境の決定，使用すべきコントロール技術の選定，コスト効果分析である。この時，各コントロールに総合値を与え調査結果のレポートを作成するためハード／ソフトの両技術が利用される。同グループは結果を記録するための作表シートを開発し，4システムを実例としたシートを作りあげてコンピュータ・セキュリティに対するこのアプローチを図表化している。またコントロール評価に対しては現時点で標準的な方法はないと指摘し，今後かなりの努力が払われねばならないとしている。

管理面および物理的コントロール・セッション

このグループの命題は，「ＡＤＰ環境における管理的物理的コントロール（偶発事故対策等）の評価に対する監査のアプローチや技術とは何か」ということで

ある。このグループは，まずデータ・セキュリティの重要性ならびに監査人の責務はともにデータ処理の枠内でリソースの保護を扱うものゆえ相互補完的なものであるとの前提を立て，監査人にとって重要な分野をつぎのようにまとめている。

(1) 実際的なセキュリティ定義の必要性

(2) セキュリティ政策明示の必要性

(3) 実証ずみの実務基準の必要性

(4) 適切なテストおよび試験を認識すべき必要性

(5) システムが被る可能性のある災害を認識する必要性

レポートの残り部分は，監査人への示唆を記載している。

まず監査人の一般的関係4分野が討議され，つぎに5種類のデータ処理セキュリティ・アプローチが詳細に論じられている。4つの一般的分野とはつぎの通り。

(1) 監査の焦点と具体性 — セキュリティ保護手段には，「リスクの許容し得る範囲」を想定すべきであり，監査人はとくに鋭敏なアプリケーションではこの範囲を重視しなければならない。

(2) 実施およびドキュメンテーションの標準 — 5つの参考文献の意義が調査され，貢献度の高い文献としてカナダ勅許会計士協会の「コンピュータ・コントロール・ガイドライン」と「コンピュータ監査ガイドライン」がとりあげられた。

(3) セキュリティ監査レポート — このレポートの内容は2つの部分に大別でき，1つは上級管理者，また，もう1つは被監査人およびその管理者にあてたものである。

(4) 第一級の既存監査手法 — 重要なリソースの保護を検閲する選択的保護，可能な局面で利用される実際的テスト，従業員と管理層の全関係者を対象とするインタビュー，他の組織の能力を活用する技術的協力……である。

5種類の監査アプローチは，重要性，目的，アプローチ，将来性を検討項目として各々討議された。

(1) システム開発・保守業務監査

(2) アプリケーション調査

(3) インストレーション・セキュリティ調査

(4) セキュリティ機能（データベース／通信環境）調査

(5) 折衷的試み

レポートは最後に，ＤＰをめぐる問題点は新しいテクノロジーへの対応（記憶媒体のポータビリティ改善，大容量記憶装置，分散処理システム），監査項目や技法を網羅した単一のリストの必要性，マネジメント層のアプリケーションやシステムの開発における進歩や態度の変更等に起因すると結論づけている。

プログラム・インテグリティ・セッション

「ＡＤＰ環境にあってプログラム・インテグリティの評価に対する監査アプローチおよび技法とは何か」というのがこのセッションのテーマである。グループは，プログラムの全ライフ・サイクルを考慮する必要があると強調し，プログラム・インテグリティと関係する領域をつぎのようにまとめている。1）所要条件を満たしたり何も実行しない場合の正確さ，２）訓練を受けたユーザの期待を満足させること，３）意図された役割を遂行する際の有用性，４）プログラムに一定のレベルの信頼性を持たせるための被評価能力。

プログラム・インテグリティの評価は多面的なテーマである。ライフ・サイクル中に監査実施の決定をすることと，セキュリティに対する脅威の厳しさおよび開発中にインテグリティを確保するため採用する手段等は別次元の問題である。

プログラム・インテグリティの達成手段は，つぎの３つのカテゴリに分けられる。

(1) 当該プログラムの正確さを証明するもの。

(2) 現在的に健全であり，今後の予期せぬ出来事にも十分対応能力を持っていることを証明するもの。

(3) そのプログラムが信頼するに足り，円滑な業務の流れにそって展開され得ることを示すもの。

同グループの勧告はつぎの通りである。

＜既存のソフトウェアに対し＞

(1) プログラム・インテグリティが存在すると仮定する際慎重を期すこと。

(2) 注意深いリスク・マネジメント分析に従って既存のツールを利用する。

(3) 物理的・管理的なコントロールを改善し，プログラム・インテグリティの欠如がもたらす影響を減じる。

(4) アクセス・コントロールにより利用者数を抑制する。

(5) 非使用時のシステムから各種資産を除去し，資産の放置を防ぐ。

＜将来のソフトウェアに対し＞

(1) プログラム作成プロセスの改良。

(2) 全ライフ・サイクルを通したプログラム・インテグリティの確保。

＜利用組織に対し＞

(1) 使用プログラムのライフ・サイクル中における脅威および困難に対し自己評価を実施。

(2) プログラム・インテグリティの監査対象となるソフトウェアの開発・取得のため，ガイドラインを設定。

データ・インテグリティ・セッション

このグループのテーマは，「ＡＤＰ環境におけるデータ・インテグリティの評価にあたって，その監査アプローチおよび技法とは何か」ということである。同グループは，物理的管理的手段やソフトウェア手段，すなわちデータ・インテグリティに必要な全ての事柄は他のセッションで取扱われるものと仮定し，データ・インテグリティ監査に直接関連を持つセーフガードに対象を絞った。またデータ・インテグリティ，つまりデータの保全を，当該データが（規定の信頼性レベル内で）正確で一貫性を持ち，認定ずみで，有効で，完全無欠であり，そして時に応じて仕様通り処理され得る時の状態だと定義した。インテグリティ監査の目的は，現行の政策および手順の十分性およびそれとの一致を評価し，矯正手段を勧告することである。

この目的を達成するため，つぎの項目の評価が必要となる。

(1) データ・ソースの信頼度

(2) ソース・データの準備

(3) データ・エントリ・コントロール

(4) データ入力受諾コントロール

(5) データ妥当性検査およびエラー修正

(6) 処理仕様

(7) 出力および分散コントロール

(8) 監査能力

同グループは，データ・インテグリティ監査の各種方法を討議し，包括的な監査作業プランに含まれる活動を摘出した。

(1) ユーザにおける正確性，完全性，一貫性のチェック

(2) 採用可能な抽出手法

(3) 並行処理

(4) ITF(Integrated Test Facility)

(5) システム・コントロール・テスト・レビュー・ファイル(SCARF)

(6) タグ・トランザクションの追跡

(7) テスト・デック

(8) アンケート調査

(9) 手続き，現場検査

(10) 活動記録

コミュニケーション・セッション

このグループは，「ADP環境におけるコミュニケーション評価の監査アプローチおよびその技法とは何か」という設問に取組んだ。討議対象は，データ通信ネットワークを利用しているコンピュータ・システムのデータ通信セキュリティ監査ガイドラインに絞り，結論として，この種の監査は，頻度がアプリケーションやシステムの感知性に直接影響を持っている鋭敏なアプリケーションや総合デ

ータ通信システムになされるべきものであると勧告している。一般的な監査アプローチは，入力端末からネットワークを介してコンピュータに連なる（あるいはその逆の）トランザクションを追跡するトランザクション・フロー分析の形態をとる。

このタイプの監査を実行する道具として同グループは，リソース／エクスポージャ／セーフガード・マトリクスを開発した。マトリクスには，左側に一連の10システム・リソースが配され，上段にはエクスポージャ・カテゴリ6種が横に並び，そしてリソースとエクスポージャの各組み合せに適したセーフガードが列挙されている。監査人はまず当該コンピュータ・システムのリソースが何であるか（端末，分散処理機能，モデム，ローカル・ループ，回線，マルチプレクサ／コンセントレータ／スイッチ，フロント・エンド・プロセッサ，コンピュータ，ソフトウェア，要員）を決定し，つぎに予期し得るエクスポージャ（エラー，脱落，災害，妨害，インテグリティの欠如，漏洩，不正流用，盗難）に対しこれらリソースを保護する適切なセーフガードは何か見出す。レポートに記載された17のセーフガードは明確に規定されているだけでなく，監査人が各セーフガードで考慮すべき事柄についても個別にステートメントが用意されている。

報告書はセーフガードの限界についても指摘しており，本質的な包括的なものとなり得ないこと，セキュリティ向上の一助となり得ても保障措置とはなり得ないこと，最新技術や手法を反映しているが全アプリケーションをカバーするものではないことを明らかにしている。

処理後監査手段・技法セッション

このグループの命題は，「コンピュータ・セキュリティ監査においては，多様なシステム・ジャーナルやログを効果的に利用するに必要な処理後の監査手段や技法とは何か」というものである。同グループは最初に，監査作業の一般的目標として，所要保護レベルを対象としたコントロールの存在，範囲，十分性の決定をあげ，つぎに特殊な目標として，トランザクションの独自性，トランザクション・インテグリティ（完全，正確，許可の管理），処理インテグリティ，配布コ

ントロール，回復管理，妨害対策コントロール等の諸機能の存在を確立することを掲げている。「コンピュータ・セキュリティ」，「コンピュータ・セキュリティ監査」，「処理後監査」，「ログ」，「手段および技法」「トランザクション」等の用語は，このグループでも，レポート内容の明瞭性を強化するため改めて定義されている。

処理後セキュリティ監査の基本要素と考えられているのは，

インプット，プロセス，アウトプットおよびこの3要素へのアクセス……

である。

セキュリティ監査の目的は，上述した4要素のログが記載する詳細情報を追及することで達成される。ログの内容としては，5種類の基本的な情報タイプがあげられる。

(1) 誰が — 活動を開始した者を区別

(2) 機能 — 処理活動を表示

(3) 何を — 処理活動の対象を識別

(4) 状態 — 機能，それに付随する行為開始者および影響を受けた対象

(5) 時刻 — 日時のスタンプを付与

この後，EFTSシステムのセキュリティ情報の必要項目例が載せられている。

つぎに処理後技法が4つの基本監査構成要素ごとに説明されている。アクセスおよびインプットでは，成功のログ，失敗のログそしてログ継続チェックが用いられ，プロセスの場合，マニュアル・チェック，コントロール・トータル，テスト・データ，ＩＴＦ，タグ付け，拡張記録保管，追跡，マッピング，再編集，並行シミュレーション，検索プログラムが含まれる。またアウトプットでは，配分リストおよび認可リストのアウトプットがある。

同グループの結論と勧告はつぎの通りである。

(1) 既存のソフトウェア・ツールは多くの機能を提供し得るが，より利用が容易となるためには，つぎの2点への取り組みが必要である。

a) 監査人を対象としたツール，カタログの発行

b） ツールの複数組み合せを可能とする手段の創出

(2) 今後必要となる技法としてはつぎの通り。

a） セキュリティ・ログのセキュリティ維持法（可能な手段としては，既存ＯＳの活用，全活動を記録する非干渉型特殊記録装置の使用，航空機のフライト・レコーダと同質の完全なハードウェア・モニタの使用）

b） ログにアクセスまたはログを操作する高水準ソフトウェア

インタラクティブ監査ツールおよび技術セッション

このグループは，「コンピュータ・セキュリティのオンライン監査で必要なインタラクティブ監査ツールおよび技法は何か」というテーマに取り組んだ。その全体目的を，「コンピュータ・システムのパフォーマンス保証を最大限達成するためのオンラインまたはインタラクティブ技術に対する監査アプローチの開発」と定義し，具体的目標としてつぎの４点をあげている。

(1) インタラクティブ技術の領域および要件の定義。

(2) コンピュータ・システムの監査能力およびコントロール能力の検討および明確化。

(3) 現時点で利用できるツールおよび技術の洗い出し，今後必要となるそれらの指定。

(4) 特定のシステム環境におけるこれらツールの使用基準の設定と必要なインタフェースの選定（例，データベース，ＯＳ）。

これら目標達成のため，同グループはまずさまざまな用語の定義付けに着手し，とりわけ重要な用語として，会話型監査プログラミングと会話型監査プロセシングで構成される「インタラクティブ監査」活動を中軸に据えた。そしてコンピュータ・セキュリティのインタラクティブ監査は，より一段大きな枠のパフォーマンス保証（ＰＡ）の一部として位置づけられた。ＰＡとは，あるコンピュータ・システムが既定の正確性，適時性，データ・セキュリティ内で企図された諸機能を実行し，所定外の機能は実行していないことを保証することと定義されている。このＰＡは元来，数分野の人々，すなわち公認会計士，上級管理者，内部監査人，

品質管理担当者，現場管理者等により実施される職務と想定されるものだが，同グループは4種の活動を中心にＰＡ作業を検討した。

(1) つぎの2項に関するＰＡ目標の設定。

a) テストの性格および目的

b) テストされるコンピュータ・システムの性格

(2) システム，手順，コントロールを検討し評価し，あるいは確立するに必要な情報の収集。

(3) システム・アプリケーションの性格および複雑さに適合するＰＡ分析と評価の実施。

(4) 上記分析および評価の結果からＰＡテスト手順を設計し実行する。

ＰＡ作業に使用される既存の監査ツールや技法は，その長所短所からバッチとインタラクティブに大別される。バッチツールとして利用できるのは，ユーティリティ・プログラム，テスト・デック，監査モジュール，ＩＴＦ，テスト・データ・ジェネレータ，スナップショット（タグ付き），追跡，SCARF，監査ソフトウェア・パッケージ並行シミュレーションである。またインタラクティブ・ツールには，監査コマンド言語（ACL），National Automated Accounting Research System(NAARS)がある。レポートでは後者の利点が言及され，また実施されたＰＡごとに全監査ツールおよび技法が図表化されている。

その後必要とされるツールおよび技法の包括的検討が行われているが，対象が5つのカテゴリに分割されている。

(1) リアルタイムに近いエラー検知・修正

(2) コントロールの十分性監視

(3) 設計の正確性の測定

(4) プログラム修正コントロール

(5) システム・トラブル表示の監視

レポートのこの部分では，インタラクティブ監査の実現に是非とも開発されねばならない各種多様のツールが概説されている。これらについては実施されたＰ

A結果ごとに一覧表が作成されている。

今後検討・調査すべき領域として以下の項目が勧告されている。

(1) 会話型ツールおよび技法における設計とパフォーマンス要件の仕様。

(2) ＯＳならびにDBMSとのインタフェース向け会話型監査ツールおよび技法の設計。

(3) インタラクティブなマン・マシン・オペレーション・モードにおける監査行動を研究する監査行動リサーチ。

(4) 監査ツールや技法の開発に従事するソフトウェア設計者や，ＰＡ専門家向けの包括的な監査・コントロール理論の展開。

PARTI 序

1．主催者歓迎の辞

標準局，S. Jeffery

標準局主催の「コンピュータ・セキュリティ監査・評価に関する研究集会」に諸氏をお招きでき誠に嬉しい。参会者の代表する諸団体および専門分野の広さはいうまでもなく，その絢爛たる資格が一堂に会したという意味でも本集会は記念すべきものとなりましょう。

参会者の33％が12の連邦政府機関を代表している事実にも言及すべきでしょう。主な所として，米国会計検査院（ＧＡＯ），保健教育厚生省，国防総省，連邦調達庁（ＧＳＡ），農務省，商務省をあげることができます。

これら政府諸機関の参列者の中でも，とりわけつぎの方々の参加を私は歓迎したいと思います。Frank S. Sato（国防省監査相当次官補代理），Donald L. Scantlebury（ＧＡＯ財政および一般管理研究部長），Howard R. Davia（ＧＳＡ監査局長），Donald L. Eirich（ＧＡＯ兵站通信部副部長），C. William Getz（ＧＳＡ第9地域コミッショナー）。

参加者の残る67％は，会計士事務所，ソフト／ハード関係，その他の民間企業，大学の関係者である。会計関係からは6社，ソフトウェア・ハウス7社，メインフレーマー2社，3大学の他，金融，公共事業，石油，保険，調査，出版，信販，カメラの分野から民間22社とカナダ騎馬警察が参加している。

一方，本研究集会参加者の知識および経験にも注目すべきである。監査に強い関係を持つ米国公認会計士協会，内部監査人協会，ＥＤＰ監査人協会，政府関係会計検査官，民間の6公認会計士事務所，様々な官民組織に席を置く監査人などの参加が注目される。

またコンピュータ分野でも，官民，教育機関のためにコントロール，ソフトウェアやその技術の開発に従事している多くの専門家の参画を得た。

つまり本集会は，異例ともいうべき多くの有能の士を迎えたものとなった。恐らくコンピュータ・セキュリティの監査・評価をテーマに開催される会議で，これほどの広汎な分野からこれほど才能ある多くの人々を集めたものは初めてであろう。

つぎに本集会開催までに絶大な努力を払われたＧＡＯのRobert G. McKenjie議長に御礼を申し述べたい。様々なセッションのテーマとその司会者の選択，そして参加者の選定等に手腕を発揮された。またZella G. Ruthberg女史にも感謝の意を表したい。彼女はMcKenzie氏と協力してプランニングにあたり，本集会の御膳立てに全責任を負われた。

われわれの本集会の中心課題は，コンピュータ・セキュリティの監査・評価の領域で連邦政府内情報処理標準（ＦＩＰＳ）とガイドラインの基礎を形成すべく十分な情報を蓄積することである。ＮＢＳのコンピュータ科学技術研究所（Institute for Computer Sciences and Technology）は，ＤＰ標準およびガイドラインを連邦政府機関に提示する責任を有しており，本集会の成果は必ずやこうしたガイドラインの先駆的役割を果すものと思う。

さらに参加者の持つ広範かつ深い学識経験を考えると，議事録はそれ自身貴重な文書であると同時に内部監査を担当しておられる人々にも活用され得るものだと断言できる。

最後に参会者が示された集会への深い関心に謝し，成功裡に集会を終えられることを希望して挨拶にかえたい。

2．セッションおよびレポートに対するエディタのコメント

2.1　用語の定義について

各参加者は，各セッションの起草するレポートで技術的専門用語に統一性を持

たせるため，まずＦＩＰＳ　ＰＵＢ39すなわち「コンピュータ・システム・セキュリティのためのグロサリー」を配布された。多くのセッションで幾つかの用語再定義が試みられ，またグロサリーに含まれない用語の使用も散見された。このような場合，当該セッションと参加者により使用された定義はレポートの基幹部を構成することが多く，その内重要な事例を２，３とりあげてみたい。

コンピュータ・セキュリティ監査

(1)　ＡＤＰシステムで維持あるいは生成されるデータの正確性および信頼性，(2)　全ての予期し得る脅威または災害から，ハード，ソフト，データを含む当該組織の資産を守る保護機能の十分性，(3)ＡＤＰシステムの運用上の信頼性およびパフォーマンス保証（ＰＡ）等を決定する独立した評価行為。

内部監査

経営への寄与として運営の点検を内部的に行う独立した評価行為。その主要目的は，経営者の責務・目標に関係した情報，分析，評価ならびに勧告を提供し，彼等に助力を与えることである。連邦政府機関に効果的な内部監査を行うべき必要性は，種々立法化されたものであることでも自明である。とりわけ1950年予算会計手続法は重要で，「当該組織の責に帰する全ての資産を効率よく運用するため，内部監査を含む適切な内部コントロールを確立・維持すること」がその組織の長に求められている。

外部監査

この用語は，公認会計士による財務監査の類義語として考えられることが多い。財務監査は財務諸表の客観的な点検で，財務諸表の示す内容の公正さに対し適切な見解が添付されるのが通例である。しかし，広義の外部監査は，「対象とされる組織から独立した個人により実施されるある種の監査」といえるだろう。

2.2　若干の考察

コンピュータ・セキュリティの監査および評価は，システムをトータルに把握すべき非常に複雑なテーマである。これは，前節で定義されたコンピュータ・セ

キュリティを確保するに必要な全てのコントロールに対する評価行為を含んでいる。

確実なトータル・セキュリティ・システムは，様々なカテゴリつまり物理的側面，手順，運用，技術等の領域に区分できるコントロールから構成されるが，一部のコントロールが弱かったり信頼性が低く容易に改変され得るものならば，たとえ他の部分に強力なコントロールが存在しても無意味となる。その結果は崩壊ということだ。このように様々な領域のコントロールの関係を考察すれば，ＡＤＰシステム内部のコンピュータ・セキュリティの十分性に意見を述べる以前に，全てのコントロールが評価されねばならないことがわかる。したがって本議事録中の各レポートは，監査計画の展開に際し，同等のウェイトで評価される必要がある。

2.3　議事録を読むにあたって

全10セッションの各レポートは，各個独立したものであり，読む順序に制限はない。ただ留意すべきは，議事録の前半には，マネジメント中心のレポートが多く，後半には技術的レポートが多い点である。詳細な索引も用意されているので希望する項目の検索には有効である。各セッションの主要な勧告および結論は総論の部にまとめられている。またなぜこの集会が開催され，いかに実施の運びとなり，どのように各セッションのレポートが作成されたかについては，付録Ｂを参照されたい。

ＰＡＲＴⅡ　基調講演

Donald L. Adams

米国公認会計士協会

プロフィール

Donald L. Adams 氏は，米国公認会計士協会専務理事で，協会内のコンピュータ・アプリケーションを含む会計および監査業務でのコンピュータ利用の発展に深い関心をもっている。その職責は，人事，購買，事務管理，出版など多岐にわたり，ＡＩＣＡＰの古いメンバとしてコンピュータ分野の様々な委員会に参加している。もちろんＥＤＰ監査委員会の議長であったこともよく知られている。また，ＡＩＣＰＡニューヨーク州の支部のコンピュータ委員会のメンバでもあった。

1973年6月にＡＩＣＰＡ入りする以前は，投資銀行 Salomon Brothers のＤＰ副部長として3年間その職にあり，その前はピート・マーウィック・ミッチェル会計士事務所のコンピュータ監査部長であった。彼は1960年以来コンピュータ監査に係りを持ち，関係著書も多い。また米国内だけでなく，カナダ，ヨーロッパでも講演歴をもっている。彼は現在，ＥＤＰＡＣＳ（ＥＤＰ　Audit Control & Security，月刊誌）の編集者でもある。マサチューセッツ工科大学およびミラキューズ大学に学び，1959年には後者から優等で工学士を受けている。

1．　序

研究集会各セッションの意義は誠に大きい。時間的制約はあるが，これは各テーマの達成にあたり積極的要因に転化し得るものである。討議の回数にも自ずと制約が生まれると思うが，これは避け難いことである。他の多くの会議でテーマ

を長期にわたり検討できるかも知れない。だが時間的制約は良い結果を生むチャンスでもある。下検分する時間も恐らくないと思われる。ある会議がある問題を扱う時，まず事前の調査を参加者が望む，どこに隠れているか判らぬ真実を追い求めるわけである。幸いにして下調査で知恵の宝石を探り当てることがあるかも知れない。だが私はこうした幸運を見聞したことはこれまで一度もない。

われわれのほとんどは，科学的手法の全盛期に教育を受け，その結果問題解決に科学的アプローチを利用することが肌に滲みついている。だが会計や監査は科学ではない。せいぜい技術，それも不完全な形のそれといえよう。したがって科学的手法の応用自体無理がある。この研究集会参加者のようなグループは，粒よりの集まりであり，各界の最高峰を集めた代表ともいい得るものである。コンピュータ・セキュリティの監査，評価の領域で重要な論点は，すべて全参加者の眼前にさらされ，そして解明されるに違いない。これこそが今回の研究集会の真価といえよう。各界の英知が結集し，情報を集積し，他の人々を啓蒙するドキュメントができるであろう。これが十分活用されれば，知識を配分する上で最もコスト効果の高い方法となるに違いない。

2．研究集会へのアプローチ

集会がカバーするトピックスは，基本的に10分野から構成される。これは非常に野心的な試みと言えよう。1年前，私は，データベース管理の研究会議に参加した。われわれの集会の目標を達成するうえで，この時のアプローチを想起することは有益だと考える。

まず，ブレーン・ストーミングが行われ，最後に提起されたテーマを対象に投票がなされ，重要性の高い5テーマが選ばれた。そして各テーマごとの時間配分が決められ，あるテーマに5時間が割当てられたとすると，その討議に5時間費すと次の課題に移るといったパターンをたどった。このアプローチは成功裡に機能した。今後数日間に，この方式の有益さが証明されることと信じる。

3．提起されたテーマに対する所見

各セッションのテーマについて若干のコメントを申し述べたい。

3.1　内部監査基準

公認会計士が監査基準を確立することは難しい。内部の監査人の場合さらに難しい。だが外部の監査人なら共通の目標を共有することができる。それは，ある組織の財務諸表を素材に各人の見解が生かせるからである。内部監査人は，やはり契約に拘束されるし，その役割りや活動範囲はともに経営者の意向に規定される。だが，一方，外部のグループの場合，内部監査業務の基準を押しつけることは困難である。こうした背景のもとで，本セッションが基準確立でとるアプローチは，セキュリティをいかに定義するかにより大きく左右される。事前に手元に配布された資料から見ると，広義の解釈が採用されているようである。有効な基準を本グループが開発できるまで，この定義は建設的な礎石となろう。

3.2　資格および訓練

このテーマも挑戦すべき価値が高い。だがコンピュータ・セキュリティに必要な資格やトレーニングについて確立した知識体系があるはずもないので，輪郭を明確化するにも骨折るだろう。恐らく厳密な定義を設けるには時機尚早だろう。専門的な資格や基準は実にゆっくり定着して行くものである。コンピュータ・セキュリティの様な特殊分野の専門的資格に有効な基準が何時実現するか，その予測は難しい。本グループが彼等の勧告を実施レベルまで高めようと努力するのはかまわないが，私自身は，この時期に厳密な資格や教育の基準を定めようとすることは間違いだと思う。ゆっくり着手し，まずその基礎を固めるべきである。

3.3　セキュリティ管理

この分野は，ＥＤＰ関連では比較的新しい概念である。徹底的討議により，そ

の全体像が明らかとなろう。また，このセキュリティ管理業務の義務，責任，組織体系の定義も必要である。このテーマは，巨大組織のみが関心を示すものかも知れないが，将来性は確かなものである。われわれは，セキュリティ管理機能の点検に応用し得る監査アプローチおよび技法を開発する必要がある。とくにこの分野のガイドラインのもつ今後の意義は大きい。

3.4 様々なシステム環境における監査要因

環境が監査に決定的影響を与えることは自明だが，では，そのインパクトとはどういうものか。この問題は容易に解答が出るものではない。担当グループは非常なタフさを要求されるだろう。現状では指針を提示することすら難しい。とにかく過去の蓄積が皆無に等しいので，このグループの討議内容は，踏み出した第一歩として意義深いものとなろう。

3.5 管理面と物理面のコントロール

管理と物理的側面の組み合せは一見奇妙に見える。内外の監査人は，その結合環を見い出せないだろうが，コンピュータ・セキュリティを中軸に据えれば不自然さはない。だが，この両者のコントロールは広汎な課題を内包し，非常に時間のかかる作業となるだろう。グループは現在定義の不明確な領域に力を入れようとしている訳で，新しい独特のコントロールを見出すのは至難のわざといえよう。

3.6 プログラム・インテグリティ

この分野では，ＯＳ，ＤＢＭＳ，アプリケーション・プログラム等のセキュリティを評価する監査アプローチが問題とされる。これらのインテグリティを確立する課題を取りあげることは容易であるが，インテグリティを評価するため監査技法を具体化するのは極めて難しい作業である。その討議の成果が注目される。

3.7　データ・インテグリティ

このテーマはかなり一般化している。監査人，とりわけ外部の監査人はデータ・インテグリティの検査や評価にかなり深くかかわってきているはずである。このグループは，現在の枠以上の技法を展開するよう求められているが，やはり労多い作業となろう。参考文献の非常に多い領域でもあるので，全く新しい成果を生み出すのは容易ではない。

3.8　コミュニケーション

監査人にはなじみのない課題であるが，ＥＦＴＳや分散処理システムが重視されつつある現在，決して無視できないテーマとなっている。効果的なセキュリティが他のあらゆる側面で確保できても，データ通信面のセキュリティが欠落すれば全体が無に帰してしまう。適切なガイダンスが導入されれば，この分野の将来の問題を解決するうえで監査界に多大の貢献をなすであろう。

3.9　処理後監査ツールおよび技法

既存のコンピュータ・システムのジャーナルやログには膨大な情報が蓄積されている。したがって監査人は監査の実施にあたってこれら情報を如何に取捨選択すべきかという問題に直面している。求められている新技術の開発は不要との決論になるかも知れないが，ツール自体は現時点でも監査人の利用可能な形となっている。ただし，それらはシステム要員向けに製作されたものだけに，同グループが監査人も使用できる形のガイダンスを準備し，監査人の活躍できる局面を提示できれば，課題の大半は解決されたといえるだろう。

3.10　インタラクティブな監査ツールと技法

この分野に限れば，内部監査人と外部のそれらとの必要性は極めて違ったものとなる。内部監査人は経営面に重点を置きデータのオンライン分析の必要性を強調するだろうが，一方，公認会計士は，ある時点のむしろ静的な素材に必要性を

感じるはずである。だが，こうした事情も変るかも知れない。ＥＦＴＳと分散処理の普及は会話型監査の存在を一層クローズアップさせ，このグループの成果に内外双方の監査人の目を集める結果となろう。

結　び

コンピュータ・セキュリティの監査並びに評価というテーマは実にタイムリーなものである。また討議対象とされている諸項目も，監査界にとって重要かつ時宜を得たものといえよう。データ・セキュリティの欠落による財政的損失は，目に見えるところではいかにも小さい。だが論理的には増大の一途をたどるはずである。この研究会での討議内容は，現在的な課題を浮き彫りにし，さらにテクノロジーの進展に対処し得る技法を開発するうえで，貴重な素地を形成するものといえよう。

PART Ⅲ　内部監査基準

議長　William E. Perry

米国内部監査人協会

参加者

Howard R. Davia

連邦調達庁

S. Jeffery

標準局

Fred L. Lilly

Lilly & Harris社，公認会計士

Gerald E. Meyers

CNA Insurance 社

Kenneth A. Pollock

米国会計検査院

Frank S. Sato

国防総省

Donald L. Scantlebury

米国会計検査院

T. Q. Stevenson（書記）

農務省

編集者注

議長の経歴紹介

William E. Perry氏は，米国内部監査人協会（ＩＩＡ）のＥＤＰおよび調査担当の理事であり，国際ＥＤＰ監査・調査委員会のメンバでもある。ＩＩＡに奉

職する前は，イーストマン・コダック社のコンピュータ監査責任者の地位にあり，その他アーサーヤング会計士事務所，Ft. Richie，プライス・ウォータハウス会計士事務所等にも関係していた。彼はクラークソン・カレッジの卒業生で，経営学および教育学の修士をロチェスター工科大学とロチェスター大学から得ている。公認会計士（ニューヨーク州）と公認内部監査士の資格をもっている。現在，ＡＩＣＰＡのコンピュータ・サービス委員会ならびにＥＤＰシステム監査作業部会のメンバとＡＦＩＰＳ（米国情報処理学会）の理事会メンバを兼ねており，以前にＧＵＩＤＥ　International PL／1 委員会の委員長を務めたこともある。またモンロー・コミュニティ・カレッジで情報処理工学教授の職に着いたこともあった。最近の著述に，「事前監査－監査プログラムへのコントロールの組み込み」（Bank Administation, 1975年1，2月号）があり，ＥＤＰ監査とコントロールの分野ではＥＤＰＡＣＳへの貢献も大である。

＜本会議の議題＞

本セッションに与えられた課題は，内部監査基準である。すなわち，内部監査人の役割と旧来の監査基準のアプリケーションを考慮して，コンピュータ・セキュリティ監査基準に関する計画草案をまとめることである。

コンピュータ・セキュリティは，システムをトータルにとらえねばならない複雑な主題である。(1)ＥＤＰシステムにより生成維持されるデータの正確さと信頼性，および(2)ハード，ソフト，データを含む組織の資産を予期し得る全ての脅威・災害から保護すること，この２点を確実ならしめるあらゆるコントロールが含まれる必要がある。

本セッションは，また，ＡＤＰシステムの開発・運用のライフ・サイクルを通じて内部監査人がコンピュータ・セキュリティを評価する責任にも配慮を及ぼさねばならない。ＡＩＣＰＡ監査基準第３号に関する声明「監査人の内部統制に対する調査・評価に及ぼすＥＤＰの影響」も，本セッションの基本的資料として取りあげる必要があろう。

次のレポートは，セッション・メンバの合意のもとに検討作成されたものである。

「コンピュータ・システムとその展開に伴なう内部監査人の役割増大に対する補足的基準」

William E. Perry, Fred L. Lilly, D. L. Scantlebury, Ken Pollock, T. Q. Stevenson, Frank S. Sato

1. 序

1.1 ＡＤＰシステムの環境への影響

コンピュータは，データ処理システムの運用法やそれに対する管理，監査の方法を根本的に変えてしまった。データの収集と利用が一変したのでスタッフによる点検や事務的チェックの機会すら減少してしまった。こうした変化は，データや会計プロセスに通じた個々人による手作業の手順が，こうした分野に不案内な人々による大規模な自動処理技法に取って替えられたことを意味する。

ＤＰ装置の導入は，しばしばデータの発生部門とは別の所に記録・処理機能を集中することになり，以前は分散していた記録保管責任の集中化も促している。また経営や財務のデータが企業規模のデータベースを抱える情報システムに統合される傾向も目立ち，独立した記録というものの存在を減少させている。もちろん狙いはこうした総合情報システムにより，より有効かつタイムリな経営意思決定が実現されることである。

コンピュータリゼーションは，会計記録となる前の取引面の点検をより短かい時間で可能としている。だが同時に，コントロールが稚拙なシステムにあっては，エラーを発見するチャンスが減る結果ともなっており，リアルタイム・システム(注1)やデータベース・システムではこの実例が多い。したがって，内部の管理手順の重要性が増し，監査人の仕事にも影響を与えている。とくに表面化している大事な作業は，コンピュータ・セキュリティの十分性を点検することである。

1.2　コンピュータ・セキュリティの定義

コンピュータ・セキュリティはシステムをトータルに把握すべき複雑な主題である。それは，(1)ＡＤＰシステムにより生成維持されるデータの正確性と信頼性，(2)ハード，ソフト，データを含む当該組織の資産を，予期し得る全ての脅威・災害から適切に保護すること，(3)コンピュータ・オペレーションの経済性と効率等を保証するあらゆるコントロールが含まれねばならない。

コンピュータ・セキュリティには，(1)コンピュータ・システム運用の正当性，(2)全ての経営目標の達成，ある組織にとって許容できるリスク・レベルの決定－等は問題とならないが，監査となると別問題である。

1.3　コンピュータ・セキュリティで監査が関与する局面

会計責任の概念は，政府・民間にかかわらず，その監査に固有のものである。いかなる監査も会計責任をめぐる3要素を内包している。

(1)　財務およびその承認行為

(2)　経済性および効率

(3)　プログラムの結果

セキュリティを点検する監査人の立場からすると，承認行為とプログラム結果は，ともに守備範囲内の要素である（効率と経済性は反対にコンピュータ・セキュリティ側からの制約の方がずっと強いといえる）。承認を求める必要のあるオペレーションの様々なセキュリティを支配する特定の基準や規定要件の存在も考えられるし，あるオペレーションのプログラム結果を評価する際には，セキュリティは重要なファクタとなり得る。同様に，ＣＰＡ事務所やＧＡＯの監査では，資産に対するコントロールの十分性に注意が払われる。したがって，当該組織の所有する情報のセキュリティ・コントロールもこの範疇に属するわけである。内部監査人は，こうした組織内情報のコントロールの十分性に十分な関心を払うべきである。

監査人の業務をカバーする個別の監査基準自体は保証されていない。だが，コ

ンピュータ・セキュリティの問題に監査人の注意を引きつけ，彼の責任を自覚させるためには，別なメカニズムが必要である。このメカニズムには，既存基準の説明や解釈のような項目が含まれることだろう。

ＡＩＣＰＡは，監査基準第３号「監査人による内部統制の調査・評価におけるＥＤＰの影響」を出した時点で，そのやり方を用いている。長い間，何の修正もなしに適用されてきた基本的なＣＰＡ監査基準は，コンピュータの出現によっても変更されなかったし，ＥＤＰ関連の課題に対しては，それらを拡大解釈してきた。われわれは，この分野の内部監査人の役割増大を論ずるにあたって，やはり「補足的基準」という用語を選択し使用している。

1.4　変容する監査人の要件

内部監査人がコンピュータ化された環境で業務を執行する時，監査責任として，つぎのような局面が新たに登場している。

(1) 監査対象システム向けの体系を創りあげるため，ＤＰやユーザの要員にガイダンスを提供する。

(2) コンピュータ・アプリケーションにおける内部統制が機能しているか，そして効果的かを，これらのコントロールの検証により判断する。

2．コンピュータ内部監査業務のための補足的基準

2.1　総　　論

コンピュータ化された環境は，必ずしも新規の監査基準の創設に結びつかない。ＧＡＯのパンフレット「政府関係の組織，プログラム，活動および業務における監査基準」に示された現行の内部監査基準は，基本的にはＤＰ機能の監査にも適応している。必要とされるのは，監査人がコンピュータ化された環境において，この基本的基準を満足させるため行わねばならない追加業務をカバーする補足的基準である。この基準追加の対象となる領域は，つぎの３分野である。

(1) システム開発

(2) 稼動システム（アプリケーション・コントロール）

(3) 物理的セキュリティおよび全般管理

2.2 システム開発のための補足基準

内部監査人は，つぎのようなシステムを対象とする時，新ＤＰシステムの開発や既存システムの大幅な改変に直面するだろう。

(1) 盗難や重大なエラーに対する保護コントロールを含むシステム

(2) 経営者，監査人，運用点検に必要な監査証跡を提供するシステム

(3) 経営者が当該システムに期待した政策を忠実に実行するシステム

(4) 効率的経済的システム

(5) 法的な要件を満たすシステム

(6) 当該システムの維持や監査に必要な理解を与えるため相応の文書が用意されているシステム

2.2.1 注釈説明

システム開発のプロセスには，コンピュータが履行する処理アプリケーションの定義，処理ステップの設計，必要とされる入力データやファイルの決定，個々のプログラムの入出力データの仕様等が含まれる。

監査人の関与は，アプリケーションの設計において重要である。というのは，設計は，コントロール手順を提示し，システム稼動後の監査に必要なレポートやデータ・ファイルを生成しなければならないからである。

また，ＥＤＰシステムの要件は，経営者により決定されるべきものだが，これらの政策が設計にそって実行されているか，あるいは，これらの設計が法的な適用要件に一致しているかは監査人の責任となる。したがって監査人は，経営者が設定した要件の性格やその要件が適切なものであるかを検証しなければならない。

監査人は，さらに，新システム開発や既存システムの修正で適切な承認プロセ

スがとられているかも検証すべきである。この際，監査人は，システム設計の承認がＤＰ管理者，ユーザ・グループ，データやレポートにより影響を受けるその他のユーザ・グループ等のいずれから必要か判断せねばならない。

そして監査人は，経営者がつぎのような必要性をもっているか否か決定することになろう。システム・プログラムにより実行されるプロセシングを明確にしたドキュメンテーション，処理されるデータ・ファイル，ユーザ向けのレポート，コンピュータ・オペレータが使うオペレーティング・インストラクション，データの準備・制御用のユーザ・インストラクション。その上，システムが実稼動に使われる以前に，経営方針が当該システムの信頼性確保に十分なテストを用意したものであるかどうかも判定しなければならないはずである。

監査人は，不正なアクセスや修正を防ぐために，経営者が要請したセキュリティ・レベルが十分か否か検査し，システム利用の効果がコスト的にひきあうかどうか考慮する必要がある。あらゆるケースを通じていえることだが，監査人は，システムの効率，経済性がより一層発揮され得るシステム設計を追求する責務を負わされているといえよう。

経営方針をのみこんだ後は，監査人は，どの程度それが実現しているか判断するため，許容の程度，ドキュメンテーション，テスト結果，コスト等のデータを検討すべきである。（注２）監査人は開発段階のシステムに密接に関与するが，しかし設計チームの一員とはなり得ない。ただ客観性を確保するため，コントロールの方策については勧告を与えることもあろう。

監査人は，経営政策実現の十分性ならびに，これらの政策が監査人の点検によりどの程度フォローされているか報告書の形で連絡すべきである。また，手直しを必要とする項目や適切な行動がとられるべき勧告案は逐一提示すべきことはいうまでもない。

2.3　稼動システムの補足的基準（アプリケーション・コントロール）

内部監査人は，導入されたＤＰアプリケーションを調査し，データ処理の適時

性，正確性，完全性を判断しなければならない。

監査目標はつぎの2点に絞られる。

(1) 稼動しているアプリケーションが基準に合致しているか，また最新の設計仕様にマッチしているかを判定する。

(2) 定期的監査で内部統制を生成されたデータの信頼性をテストし，運用アプリケーションの弱点を明らかにする。

2.3.1 注釈説明

機械的なデータ処理からＥＤＰへの移行は，従来の監査基準にも変革をもたらした。ＥＤＰシステムの複雑さとそのカバーする領域の広大さは，データだけではなく，そのデータを処理するシステムにも内部監査の目が向けられねばならないことを意味している。理論的にも，「もしそのシステムが安全かつ完全なら，処理され生成されるデータも信頼が置ける」という前提が第一義となる。

コンピュータ・セキュリティの確保（リスク・アナリシスを含む）と既存のＤＰ内部統制の強化を対象に，内部監査人がシステム仕様の開発において取り扱うべき補足的基準は十分論議された。

2つの補足的基準により，監査人は，内部統制を含んだ仕様修正の促進や運用アプリケーションの改善を念頭に置き，当該アプリケーションの欠陥や環境の変化を精査するため定期的な内部監査に着手できる。こうした定期監査では，監査人の内部統制に対する配慮がとくに重要となる。またシステムが最新の仕様に従ってオペレートしているという保証がどこにもないことを監査人は銘記すべきだろう。

生成データの信頼性テストの一環として，監査人は，任意に選択したトランザクションのサポーティング・ドキュメンテーションを検討し，コントロール手順との一致をテストするため，トランザクションの実行様式の事務的な正確さを確かめることになる。加えて監査人は，例外条件やデータ変換，収集の正確度を判断するうえで，データ・ファイルの点検も必要となろう。もしデータ・レコード

が機械読取の可能な状態なら，コンピュータを利用した監査技法をこのテストで応用すべきである。

コンピュータ・システムの不正使用やその他の非合法行為の可能性を考慮に入れ，内部監査人は常に注意を払わねばならない。不正手段摘発の監査が必ずしも主要目的ではないが，現状から判断すると，こうした不正の検知が内部監査の目標の一つとなるのは仕方ないことである。

2.4 物理的セキュリティおよび全般管理のための補足的基準

ＤＰシステムの存在やオペレーションが経営方針および法的要件に合致し，処理データのセキュリティが効果的に確保されているかどうかを確認するためには，内部監査人による全般的コントロールの調査が必要となる。

2.4.1 注釈説明

監査人は，あらゆるプロセシング・アプリケーションに適用される全般的なＥＤＰコントロールと，個々のアプリケーションごとに異なるアプリケーション・コントロール（第2.3項参照）とを区別しなければならない。全般的コントロールの検証にあっては，監査人は，数分野のコントロールを評価判定し，アプリケーション・コントロール調査時の全般的コントロールの効用について判断する。

権限や責任は，当該組織の目的が効果的に満足され得る形でその組織内部において分担されねばならない。監査人は，組織，権限の委任，責任，その分担等を調査して，権限が組織目的にあうよう機能分化されているか，あるいは，責任の分担が内部統制の強化に役立っているか判断すべきである。任務分担の単位は，プログラム・システム開発，コンピュータ・オペレーション，データ入力制御，アプリケーション・コントロールの保守を担当する制御グループが基本となろう。

任務分担の点検で監査人は，コントロールの度合いの評価，不適切な分担によるマイナス効果の報告を行わねばならない。任務分担の円滑運用は，職務の定期的なローテーションや休暇の指定に依拠するが，監査人はこうした面にも意を配

る必要がある。

十分な物理的施設や他のリソース（熟練要員，備品，パワー）は，処理目的の完遂には不可欠である。監査人は，当該組織がこうした面で不足をきたしていないか確認すべきである。

人事管理，勤労意欲の向上，専門的要員の供給なども，ＤＰ機能を円滑に運営する上で欠くことはできない。人事管理全体を視野に置き，監査人はこうした局面に注意を向ける必要がある。

監査人は，セキュリティ向上のため，コンピュータ・ハードウェア，プログラム，データ・ファイル，要員等の物理的セキュリティを精査すべきである。もちろんＣＰＵ周辺だけでなく，端末周辺機器の部位までこうした監査の目を注ぐ必要がある。ハードウェアの物理的セキュリティを検査する際，監査人が注意すべきことは，データ処理の中断を克服しプロセシングの継続を確保する偶発事故対策のレベルである。ハードウェアのバックアップだけでなく，支援機器の活用，要員，プログラム，フォーム，データ・ファイル等の代替処理場所への運搬も含める必要がある。さらに監査人は，こうした偶発事故対策プランの検証程度もチェックすべきである。

ファイルの物理的セキュリティの点検では，データやプログラム・ファイル・ライブラリがコンピュータおよびプログラムにアクセスしないスタッフにより保管されているか否か，あるいはライブラリ自体が安全な状態にあるか，オペレータや他の要員がライブラリにアクセスしているか，ファイル・バックアップ（オフ・サイトのバックアップも含む）は完全か，といった項目が監査人のチェックポイントになる。ファイルがオンラインで維持されている際は，監査人は，ＯＳ内の許可コントロールによりどの程度ファイルが保護されているか，またファイルのバックアップ・コピーが通常通り保管されているか検査しなければならない。このバックアップ・ファイル・コピーの維持手順を検査するには，監査人は，バックアップ・ファイルを識別する手順やラベルを確かめ，バックアップの完全性や正確性を確保する内容のチェックも行うべきである。

コンピュータ・システムは，システムズ・ソフトウェアとりわけＯＳによって最もよくコントロールされ，しかもシステムズ・ソフトウェアは，ファイル取扱能力，マルチプログラミング，ファイル・ラベルのチェック機能，その他の数多くの許可制御手段を提供するので，コンピュータ処理のコントロールの最重要部分だといえる。監査人は，ＯＳやその他のシステムズ・ソフトがカバーできるコントロールのタイプを認識し，これらのコントロールがなし得る能力の範囲をよくわきまえるべきである。またシステムズ・ソフトウェアの保守にあたる要員や，こうしたソフトウェアの修正権限を与えられている人々が，ソフトウェア内部の特定コントロール部分に手を加えて故意の如何にかかわらずダウンさせ得る可能性もよく認識すべきである。

コンピュータ・ハードウェアは，プログラムの故障より，むしろハードウェアのそれに関連したエラー検知設計をもっていることが多い。監査人は，設置システムがどの程度これらのハードウェア・コントロールに依存しているか，またＯＳがこれらコントロールをいかに活用しているか，システム内で検知されたハードウェア・エラーがどのようにレポートされ矯正手段がとられるかに，十分注意を払わねばならない。

2.5　その他の監査要件

監査人はＤＰ装置の調達に関し，当該組織の経済効果測定や利用分析に意を用いるべきである。これは，運用予定システムのユーザと協力し，ＤＰスタッフにより開発された対費用効果分析の徹底的解明が含まれる。また経営陣が導入コストを正当化させるためには，その装置が表面にさらされたり逸脱したりする可能性があることをリスク・アナリシスによって十分確認する必要がある。たとえば，プライバシー法に見合う諸要件は，故意または偶発によるデータの暴露を防ぐため，特殊な技法の採用を必然としている。これには多種多様の手段をとり得るだろうが，選択すべき方式は，意図にかない最大のコスト効果をもつものであるべきである。

3．活動勧告

監査人は，その基準に従い，当該組織のＡＤＰシステム取得書類の点検を行うべきであり，その際，対象となる仕様を，組織内で利用できる他の仕様や既存の運用装置およびソフトウェアと比較対照すべきであろう。何らかの逸脱があれば，必ずそれは書類に明記されねばならない。

つぎにあげる３つの活動は，前述した３種の内部監査補足基準の運用・定着を推進するため示唆したものである。

(1) ＧＡＯはこれら基準を検討し，基準パンフレットの改訂，追加基準の補足資料発行を考慮すべきである。

(2) 補足的基準は，連邦監査推進会議に回付され，その検討と承認を受けねばならない。

(3) ＮＢＳは，システム開発，運用システム，物理的セキュリティならびに全般管理を対象とするＦＩＰＳガイドラインを準備する時，これら補足的基準を考慮に入れる必要がある。

4．参考文献

（注１）「ＳＡＳ No．３および内部統制の評価」，Elise G. Jancura および Fred L. Lilly, The Journal of Accountancy. 1977年3月号，69ページ

（注２）連邦政府内情報処理標準（ＦＩＰＳ）Pub．38，コンピュータ・プログラムと自動データ・システムのドキュメンテーション。連邦政府印刷局，ＳＤカタログNo．Ｃ13．52：38

PART IV　資格と訓練

議　長　C. O. Smith

米国会計検査院

参加者

Sid Baurmash

Seidman & Seidman

Adolph Cecule

地質調査局

C. W. Getz

連邦調達庁

Walter Kennevan

アメリカ大学

Kathleen Kolos（記録係）

米国中央情報局

Haman Mc Daniel

米国人事委員会

編集者注

議長の経歴紹介

C. O. スミス氏は米国会計検査院（ワシントンD. C. ）のロジスティックコミュニケーション部次長で，過去20数年間にわたり連邦，州，地方の各政府機関および民間企業のあらゆる階層の業務担当者および管理者と共に活躍している。現に，事務管理，科学，軍事の各方面におけるコンピュータ・アプリケーションを含む情報処理活動の世界的規模における評価の計画，指導，調整，実施の責任者である。同氏の仕事は全世界的なベースに立脚したシステムとプログラム

のプロジェクト計画，経営分析，設計，実施，運用を含む情報処理のすべての面の評価に中心がおかれており，過去10年間は，指揮／統制，給与，会計，ロジスティック，経営情報のアプリケーションに限らず，これらをも含めた多種多様なシステムとプログラムに焦点がしぼられてきたが，同氏のかつての専門は個々のデータ処理設備の導入実績の評価である。氏は会計学（カリフォルニア州立大学ーフレノス　理学士）と経営管理および経営情報システム（アメリカ大学B.A修士）で学位を得ている。同氏はまた，公認内部監査士（Certified Internal Auditor,略称ＣＩＡ，米国内部監査人協会の認定資格）であると同時に，米国内部監査人協会（The Institute of Internal Auditors, Inc.），経営情報システム学会（ Society for Management Information Systems),軍用ＯＲ学会（Military Operations Research Society），およびＥＤＰ監査人協会（EDP Auditers Association, Inc. ）の会員でもある。最近の関係出版物にはH. Jポール氏およびB.ノールズ 氏との共著，コンピュータ・オペレーションのマネジメント監査：個別指導（ニューヨーク　ＩＥＥＥ，1976 ）がある。

＜本会議の議題＞

資格と訓練

コンピュータのセキュリティ監査を行うための資格と訓練はなにか。

ＡＩＣＰＡ（米国公認会計士協会）の最初の一般監査基準は下記のとおりである。

"検査は監査人としての十分な技術的訓練と熟練をもった人，または人々によって行われなければならない。"（ＳＡＳ　№1第150，20節）ＳＡＳ№3の第4項はこの基準を詳述しており，"さらに複雑なＥＤＰアプリケーションが含まれる状況下では，監査人は必要な監査手続の実行に際して，特定の専門知識を適用する必要がある"と述べている。

本会議の任務は適切なレベルの専門知識を得るために必要な訓練と経験とともに，コンピュータのセキュリティの評価に必要な専門知識を確認して定義することである。このためには，簡単な物理的セーフガードの評価からシステム・ソフ

トウェアの機密保持特性の分析に至るまですべての範囲にわたるコントロールにについての考察が必要である。

本会議の全メンバーによって，下記の全員一致の報告書が作成，審議された。

序

コンピュータは急速に我々の最も有用な道具の1つになりつつあるが，出現以来20年ちよっとの間に，我々の生活の多くの面で重大な変化をもたらしてきた。コンピュータは我々の選挙結果の予測の手伝いをし，宇宙飛行士のために人間の比較的緩慢な反応力を補い，道路，鉄道，航空における交通の流れをコントロールするし，病気の診断の手伝い，天気の予報，銀行残高の計算，その他，その出現以前には我々では手もつけられなかった無数の退屈な雑用的な仕事に使用されている。

コンピュータ利用の将来予測は，数も多く，多岐にわたっている。なぜなら人間の知識欲は，未知の領域を圧縮する可能性とのかかわりにおいて際限がないからである。

予想されるコンピュータ活用の成長は今後も驚異そのものであり，管理者やユーザは，以前よりますますコンピュータに頼ることになろう。これらの人々がコンピュータにたよればたよるほど，その誤用，悪用の機会もまた増加し，そうなればなるほど管理者やコンピュータのオペレーション，とくにコンピュータのセキュリティの監査と評価にたずさわる人々は高度の資格をもち，かつ，よく訓練されていなければならないことになる。これらの人々は，さらに，そのコンピュータ・システムが悪夢のようなエラーで財務的な損失をきたす前に効率的で効果的な修正計画を立案，実行維持できるように，潜在的な危険の前兆をよく知る必要があり，その上，予想される兆候や危険からデータを保護するための方法についてもよく知る必要がある。

以上のような理由から，研究集会の本会議中に提出された根本的な問題は"コンピュータ・セキュリティの信頼できる監査を行うための人材の資格と訓練の必要事項は何であるか"であった。本質的には，この仕事はコンピュータ・セキュ

リティの評価を適切に実行するために必要な専門知識の認識と定義，およびこの専門知識の必要レベルを得るために必要な訓練とからなる。さらに簡単にいえば，この仕事を行うために必要な知識の共通内容はなにかということである。

知識の共通内容開発のための考察

今回の目的にかんがみて，委員会はトータル・システム的な観点からコンピュータ・セキュリティを考察した。すなわち，コンピュータ・セキュリティのためには，自動データ処理システムの統合部分であるデータの完全性と正確性，信頼性を保証するために必要なあらゆるコントロールが含まれ，この観点には情報の取得，処理，貯蔵，および普及に関しての既定のすべての管理が含まれるものである。委員会の考察によると，委員会の知る限りでは悪意の専門家や技術力のある侵入者による自動データ処理システムの無断，または不法な介入を防止するコンピュータ・セキュリティを評価する簡単なシステムは存在しない。

このような監査の実施に必要な専門知識の適切なレベルの考察に際して，委員会はまず，当事者が仕事に入る前に持っていなければならない知識の共通内容を確認し，しかる後に，この仕事を行う環境の複雑性を徹底的に考慮した。委員会としては，これらの評価を実施する人々は会計学，経営管理，工学，オペレーションズ・リサーチ，コンピュータ科学，あるいは経済学などに限られるわけではないが，このような科目の基礎教育とその経験をもっていればよいと考えた。これらの科目では，すでにそれぞれの知識の内容は特定化され，それらに関連する知識も固まっている。

これらの評価活動は色々なバックグランドと経験を持つ人々によっても行うことができそうなので，この仕事を行っている人すべてが完全な資格を有する専門的な監査人であるとは考えない。各人が所有するそれぞれの基礎教育と経験には関係なく，コンピュータ・セキュリティの監査には，ハードウェアとソフトウェアの両方の能力と制約の評価を含めたデータ処理とテレコミュニケーションのしっかりした基本的知識を加えた管理・監査の概念と実際のがっちりした基礎が必要である。監査の種類，性質，範囲によって，各監査人に要求されるコンピ

ュータ・オペレーション，ソフトウェアの機能，自動データ処理機能中の，入ったり出たりする情報フローに関する知識と経験の程度は異り，評価しようとするシステムが複雑であるほど，より広い技術知識が必要になる。

たとえば監査の主要項目が１つのコンピュータ・プログラムの，あるいは一連のコンピュータ・プログラムの完全性の確認にあるならば，この場合の監査人は他の要素に加えて，これにからむ潜在，顕在の危険性の重大さを完璧に承知しなければならない。議事録のＰＡＲＴⅧに概説してあるように，これらの危険性にはつぎのようなものが含まれるが，これだけと明言できるものではない。

A　事故による開示

1. ハードウェアかソフトウェアかいづれかの，またはその双方の自然故障
2. 人間のエラー

B　偶発的な未承認のアクセス

1. 拾い読みで発見された弱点や欠陥
2. 悪意の侵入者が弱点や欠陥を発見する

C　意図的な攻撃

1. 賊が欠陥をつくる（わなをかけたり，コードを変える）
2. 陰謀（計画的な攻撃）
3. 無分別な従業員

この種の監査を行うために必要な熟練というものは１人の人間では持ち合せないことは明かで，このときには多角的監査チームを編成すればよい。この多角的チームには特定の監査に必要なすべての熟練と経験を網羅する。この多角的チームはすでに政府機関や非政府機関で活用されて成功している。

委員会としては"だれが監査を行うか"ということについてはあまり関心を持つべきではなく，そのために必要な知識の共通内容の確認に努力を集中すべきであるという見解を示し，さらに，"だれが訓練するか"についても関心をみせなかった。委員会の意見によれば，大学でもカレッジでも，あるいは国家公務員任用委員会（Civil Service Commission），Interigency Auditor Train-

ing Center，Institute for Professional Education Inc. でも，その他の多無数の施設や職業集団のいづれでも知識の共通内容に含まれる訓練・教育の必要事項を満足させるコースやセミナー，研究集会をもつことができるし，すでにもっているところもある。

最後に，委員会は専門知識の必要レベルの開発に要する費用の問題については，考慮すべき要素が多すぎるため，結論を出そうとはしなかった。たとえば，専門知識の必要レベルの開発に関係する費用は，その組織がその組織内で自己の職員を訓練するか，少数の者を訓練して部分的な能力を開発して，外部から臨時的に専門知識を雇用して補足するか，あるいはまた，コンサルタント会社のような外部組織から必要な専門知識を一時的にあるいは継続的に使用するかによって，本質的に異ってくる。訓練の必要性は，それぞれの組織，各人によって異るから，組織としては，コンピュータ・セキュリティを効果的に監査するために必要な知識の共通内容を修得・保持するための計画を立てる必要がある。おそらく，ここでの主要な関心事は専門知識の必要レベルの開発にいくらかかるという問題ではなくて，コンピュータの誤用・悪用が発見されたり，報告されたりするケースが増加している事態のなかで，組織がこの開発をしないですむかどうかということである。

コンピュータ・セキュリティ監査に必要な知識の共通内容の開発に際して，委員会は2つの根本的な問題に直面した。第1の問題は監査を担当する人々の基本的な知識と経験を拡大することであり，第2の問題は監査に従事する人々に必要な技術的訓練の範囲を決定することである。経験上から判断すると，この仕事に必要な知識には少くとも3つのレベルがある。

まず第1は，管理と監査の概念および実際で要求される知識の一般的なレベルであって，通常の大学やカレッジの卒業生で経営管理か会計学の学位をとっている人々ならば，普通はこのレベルに達している。これらの人々は，一般的にはデータ処理やテレコミュニケーションの基礎知識の素養を欠いており，このための追加訓練が必要である。

第2のレベルは各人がハードウェアおよびソフトウェアの機能と限界の評価を含めてデータ処理とテレコミューニケーションの基礎知識をもっていることである。通常の大学やカレッジでコンピュータ科学などの学位を得ている人々はこのレベルに達しているのが通例だが，これらの人々は管理と監査の概念および実際についての基礎を欠いていることがあり，この場合は追加訓練を必要とする。

知識の第3レベルでは，さらに複雑なコンピュータ・システムの監査を行うための包括的な技術知識と関連する経験が要求される。たとえば，このレベルの知識はオペレーティング・システム（モニタ，エグゼグティブ・システム等）の弱点を捜そうと垣間見る者や悪意の探索者による無許可のアクセスに対する弱点を評価するときに必要である。

以上の必要事項にもとづいて，委員会は，コンピュータ・セキュリティの信頼できる監査を実行するために必要と確信した知識の共通内容とその関連資格と訓練の概略を示した。後述アウトラインの前には；知識の内容の各部分の重要性の簡単な説明がつけられている。

読者への案内のために，アウトラインは下記の8つの部分に分割されている。

(1) コンピュータ・システム，オペレーション，およびソフトウェア

(2) データ処理技術

(3) データ処理機能の管理

(4) データ処理機能のセキュリティ

(5) リスク・アナリシス

(6) 管理の概念と実務

(7) 監査の概念と実務

(8) コンピュータ・セキュリティの監査に必要な追加資格

1．コンピュータ・システム、オペレーションおよびソフトウェア

この章にのべられている論題は，各人がコンピュータ・システムのあらゆる部

分の相互関係と相互作用を理解するために必要な広範な理論的基礎を与えることを目的としている。

これらの論題によって与えられる基礎知識によって，コンピュータの作動方法，ソフトウェアの相互関連，および基本機能を知ることができる。これらの一般論は，バッチ，相互作用，オンライン，あるいは分散処理のいづれのシステムであろうと関係なく，あらゆる種類のシステムに適用できるものである。

2．データ処理技術

データ処理技術は過去20年の間に劇的な発展をとげ，しかも毎年，データ処理の速度はますます高速化され，その方法はますます効率的になっている。プログラム言語の数も増え，データ管理は一層効率化され，ファイル処理は膨大な量のデータの貯蔵，取出しが可能になっている。このようなデータ処理の急速な革新にともなって，人々はデータ処理技術の基礎知識をもつだけでは十分ではなく，この分野の急激な変化について行かなければならない。

この章の論題はデータ処理技術の基本に一般的な方法でふれており，この分野で現在利用されている技術を包括しているが，新しい開発の速度に基づいて，たえず教育計画を前進させていかなければならない。

3．データ処理機能の管理

データ処理機能のよき管理は，コンピュータ・オペレーションの信頼性のあるセキュリティを実現するための重要な要素の1つである。これらの管理者は，日々のオペレーションの責任者であると同時に，それらのオペレーションの物理的レイアウトからデータ処理に使用するソフトウェアの信頼性に至るまでの全範囲における詳細事項に関心をもっていなければならない。この種の仕事の重大性は，いくら強調しても強調し過ぎることはない。監査人は，これらの仕事の相互関係

と進歩するプログラムの管理に対してそれのもつ意義を理解しなければならない。

本章の論題は"監査人"にデータ処理機能の管理に関連する責任の基本領域を紹介するものであり，また同時に，"監査人"がデータ処理機能を全体の組織内で適切に見通すことを助けるものである。この点において，コンピュータは情報の生産者ではなく，また少くとも管理的な感覚においては情報の使用者でもなくて，情報の処理機構である。最後に，これらの論題はこの機能が進歩するプログラムの管理で果す貢献度に対する監査人の理解を助けるものである。

4．データ処理機能のセキュリティ

意図的な熟練技術者がコンピュータ・システムを侵害することを防止することができるほどとりあつかいが簡単な保護技術は存在しないが，これを邪魔することのできるある種の方策はある。これらの機密防止は，たとえばデータの取扱いの慎重度あるいは格付け，従業員の身元調査の度合，および周辺コントロールなどの要素の多少によって，施設ごとに異り，担当者はデータの保護状態の信頼できる評価ができるためには，コンピュータ・システムにおけるデータの敏感性はもちろんのこと，セキュリティ技術に精通する必要がある。効果的なセキュリティを維持することの困難性に，さらに，コンピュータ・システムのリモート・アクセス能力の発達が加わっており，担当者の仕事のある部分はコンピュータ・システムのすべてのコンポーネントのセキュリティの完全性を評価することになろう。

アウトラインに含まれている論題は，出発点，使用されるべきセキュリティ対策を羅列してみることであるが，このリストはそれらの対策を網羅するのが目的ではなく，それらの説明を目的とするもので，新しいさらに効果的な方法を考察して，本題のより強力な知識を築き上げる基礎として使用されるべきものである。

5．リスク･アナリシスと危険兆候の評価

管理者とコンピュータ処理を評価する人々は，潜在的な災害の前兆を識別する能力がなければならない。異常な危険の発生の可能性を知ることは，それに対抗する最も効果的なセキュリティ手続きの種類と性質を評価するための主要な要素である。脅威は自然の災害（洪水や火災）やあるいは，コンピュータ・システムの適切なオペレーションを偶然に，あるいは故意に妨害する人間の側からもやってくる可能性があり，セキュリティの技術と手続きの評価が可能であるためには，各人は災害からの損害の程度を評価できなければならない。このため，各人は潜在性の損害を現実的に評価するためにリスク・アナリシス技術の基本を理解する必要がある。

アウトラインのこの章にかかげた論題はこの仕事を効果的に行うために必要なリスク・アナリシスの技術の基本を理解させるためのものである。

6．管理の概念と実際

ほとんどの権威者達は，やや違った管理業務の見方をしている。恐らく，この異論は彼等が働いてきた環境の違いや，彼等自身の気質上の性格によってある種の管理法を考察し，しかもそれらが効果的な結果をもたらした事に原因しているからであろう。

また異論の一部は，管理の技術と科学が今世紀中頃からかなりの変化をみせていることに起因しているのかも知れない。たとえば数字的，統計的概念，コンピュータ，および行動科学の発展は，管理の概念と方法に絶大な影響を及ぼした。管理のための単純な公式や即効的な解答などはない。管理の仕事はそれにはあまりにも複雑すぎる。しかしながら，権威者達は管理の仕事に対して異った見解をもっていると云っても，彼等とてこの仕事に関連する論題には一人として異論はもっていない。それらの論題については，コンピュータ・セキュリティの監査に

必要な知識の共通内容に関する委員会の概念で述べてある。

7．監査の概念と実際

監査の技術とこれに関連する論題はコンピュータ・セキュリティの評価を行うための基礎になるものである。監査は，それ自体は文明と同じ位古いものであり，古代エジプトやローマ帝国でも，また，中世の商業組織でも，もちろん行われていたものである。監査行為の共通的な内容範囲は，歴史を通じて，審査，実証と報告であった。

監査があらゆる種類の組織体のコントロールでの主要要素になり，その重要性が増大したのはコンピュータの出現以後である。たとえば，下院政府活動委員会のジャック・ブルック委員長は，最近，利用状況の見直しが行われないことが連邦政府の根本問題の1つであると述べている。（注1）

コンピュータの出現以来，情報が蒙る可能性がある潜在的な脅威は，事故による露見によるものであろうと，偶然性による未承認のアクセスによるものであろうと，あるいはまた故意の攻撃によるものであろうと，いづれも驚く程増加しており，コンピュータ・セキュリティを継続的に監査する必要性はいくら強調しても，強調し過ぎることはない。

本章に含まれている知識の共通内容に関する論題は，会計分野に最も共通するものであるが，監査人およびそれ以外の人にも基本的な原理を与え，コンピュータ・セキュリティの評価を実施するチームに根本的な監査実務を教えるものである。

（注1）

Administration of public Law 83-306 連邦政府ＡＤＰ資源調達，38回政府活動委員会報告追加見解付，議会報告№94-1746，1976年10月1日

8．コンピュータ･セキュリティの評価に必要な基本的資格

委員会で確認された資格は，管理，監査の概念と実務，データ処理に関連するテレコミュニケーションの基礎知識に加えて，もたなければならない経験的な諸要素である。

委員会では，各人の基礎教育と経験は，この仕事に必要な知識の共通内容の根本的な構成と考えられる科目の約1年間の学業あるいは同等の教育を追加して補足する必要があるという点で意見の一致を見た。

この追加教育は，約400-500授業時間の努力を意味する。比較上，各授業時間は，期間中50分として考慮されている。1学期－3単位，カレッジ・コースで14−16週間，週3回になり，このコースで42−48 授業時間の学業になる。また，この仕事を効果的に効率よく行うまでには，1年から5年の職場教育か，またはコンピュータ・セキュリティ監査での経験が必要になろう。

要　約

コンピュータが急速にわれわれの最も有効な道具の1つになりつつあり，その将来の使用については多種多様なものが予想されるので，管理者やその他のユーザ達がコンピュータの成果に依存することができるという事実がますます重要になってきている。これらの人々のコンピュータ依存度が高くなるにつれて，人々は，彼等のコンピュータ・オペレーションがエラーや費用倒れの悪夢になることなく，鎮痛剤になるようにコンピュータ・セキュリティの監査にたずさわる人々のもたらす情報を重視するようになるだろう。

したがって，このような監査を行う人々は，高度の資格をもち，かつ，よく訓練されていなければならない。以下にかかげた知識の共通内容は，専門知識の必要レベルを開拓するための基礎になるものである。

アウトライン

コンピュータ・セキュリティ監査に必要な知識の共通内容

1. コンピュータ・システム，オペレーション，およびソフトウェア

A　システム理論（情報システム）

B　コンピュータ理論

C　データ・コミュニケーション理論

2.　データ処理技術

A　情報の構造

B　プログラム言語

C　分類，探索の技法

D　ファイルの生成，維持と問合せ

E　記憶装置

F　データ管理システム

G　統合システム

H　コンピュータ・ソフトウェアの開発，修正，保守工学

3.　データ処理機能の管理

A　組織構造

B　要員の選択，訓練，管理

C　運営，組織の方針，手続き

D　コンピュータ・オペレーション

E　分析，設計，とプログラミング機能

4.　データ処理機能のセキュリティ

A　コンピュータ・センタ

B　遠隔サイト

C　システム（オペレーション，アプリケーションおよびテレコミュニケーション・ソフトウェアを含む）

D　方針と手続き

E　要員

F　データの取扱い

G　回復能力

H　内部制御のテスト

5.　リスク・アナリシス

A　物理施設

B　遠隔サイト

C　ソフトウェア

D　情報

6.　管理の概念と実務

A　管理業務，責任，実施，および倫理綱領

B　経営管理

C　組織構造の原則

D　一般管理の概念

E　人的資源の管理

7.　監査の概念と実務

A　初級会計

B　中級会計

C　上級会計

D　原価計算

E　政府および地方行政体の会計

F　監査

8.　コンピュータ・セキュリティ監査に必要な追加資格

コンピュータ・セキュリティ監査人は，上記の知識の共通内容のほか，さらに下記の資格を備えていなければならない。

1.　大規模・複雑な機能，活動，プログラムの監査の計画，指導，調整ができるだけの十分な経験

2.　チームの各要員に仕事を割当て，作業に必要な特定科目と専門知識を確認する能力

3.　会議を主宰し，作業結果の報告書を作成，提出，処理する能力

BIBLIOGRAPHY

Allen, Brandt R. "Computer Security." Data Management 10 (February 1972): 24-30.

American Institute of Certified Public Accountants Auditing Standards Executive Committee. Effects of EDP on the Auditor's Study and Evaluation of Internal Control. New York: American Institute of Certified Public Accountants, 1974.

Campbell, Voin R. "Privacy and Security in Local Government Infosystems." Infosystems 23 (December 1976): 31,34.

Canadian Institute of Chartered Accountants. Computer Audit Guidelines; Guidelines on the Minimum Standards and Accepted Techniques Which Should be Observed in the Audit of Organizations Using a Computer. Toronto: Canadian Institute of Chartered Accountants, 1975.

Canadian Institute of Chartered Accountants. Computer Control Guidelines; Guidelines on the Minimum Standards of Internal Control Which Should be Maintained by Organizations Using a Computer. Toronto: Canadian Institute of Chartered Accountants, 1970.

Canning, Richard. "The Internal Auditor and the Computer." EDP Analyzer 13 (March 1975): 1-13.

Cardenas, Alfonso F.; Presser, Leon; and Marin, Miguel, eds. Computer Science. New York: John Wiley & Sons, 1972.

Cutting, Richard W.; Guiltinan, Richard J.; Lilly, Fred L.; Mullarkey, John F. "Technical Proficiency for Auditing Computer Processed Accounting Records." Journal of Accountancy 132 (October 1971): 74-82.

Gildersleeve, Thomas R. Data Processing Project Management. New York: Van Nostrand Reinhold Co., 1974.

Gray, Max, and London, Keith. Documentation Standards. Princeton: Brandon/Systems Press, 1969; revised ed., New York: Petrocelli Books, 1974.

Hamphill, Charles F., Jr., and Hamphill, John M. Security Procedures for Computer Systems. Homewood, Ill: Dow-Jones-Irwin, 1973.

Kanter, Jerome. Management-Oriented Management Information Systems. Englewood-Cliffs, N.J. Prentice-Hall: 1972.

Krauss, Leonard J. Computer-Based Management Information Systems. New York: American Management Association, 1970

Leibholz, Stephen W., and Wilson, Louis D. User's Guide to Computer Crime; Its Commission, Detection & Prevention. Radnor, Pa: Chilton Book Co., 1974.

Linde, Richard R. "Operating System Penetration." National Computer Conference Proceedings 44 (1975): 361-368.

Mair, William C.; Wood, Donald R.; Davis, Keagle W. Computer Control and Audit. 2nd ed. Altamonte Springs: Institute of Internal Auditors, 1976.

Martin, James. Security, Accuracy, and Privacy in Computer Systems. Englewood Cliffs, N.J.: Prentice-Hall, 1973.

Martin, James. Telecommunications and the Computer. 2nd ed. Englewood Cliffs, N.J.: Prentice-Hall, 1976.

Martin , James. Teleprocessing Network Organization. Englewood Cliffs, N.J.: Prentice-Hall, 1970.

Menkus, Belden. "Management Responsibilities for Safeguarding Information." Journal of Systems Management 27 (June 1976): 6-14.

Methodius, Ioannis. "Internal Controls and Auditing." Journal of Systems Management 27 (November 1976): 6-14.

Milligan, Robert H. "Management Guide to Computer Protection." Journal of Systems Management 27 (November 1976): 14-18.

Parker, Donn B. Crime By Computer. New York: Scribner & Sons, 1976.

Parker, Donn B. "Computer Security: Some Easy Things To Do." Computer Decisions 6 (January 1974): 17-18.

Porter, W. Thomas. EDP: Controls and Auditing. Belmont: Wadsworth Press, 1974.

Rosove, Perry E. Developing Computer-Based Information Systems. New York: John Wiley & Sons, 1967.

Roy, Robert H., and MacNeill, James H. Horizons For a Profession. New York: American Institute of Certified Public Accountants, 1967.

Scoma, Louis, Jr. "Data Center Security." Data Management 13 (September 1975): 19-21.

Tharp, Marvin O. "Auditor and the Systems Audit." Journal of Systems Management 27: 29-33.

U.S. National Bureau of Standards. Approaches to Privacy and Security in Computer Systems; Proceedings of a Conference Held at the National Bureau of Standards, March 4-5, 1974. National Bureau of Standards Special Publication 40, 1974.

U.S. National Bureau of Standards. Guidelines for Automatic Data Processing, Physical Security and Risk Management. Federal Information Processing Standards Publication 31, June 1974.

Van Tassel, Dennis. Computer Security Management. Englewood Cliffs, N.J.: Prentice-Hall, 1972.

Weber, Ron. "An Audit Perspective of Operating Systems Security," Journal of Accountancy 140 (September 1975): 97-103.

Weiss, Harold. "Computer Security, An Overview." Datamation 20 (January 1974): 42-47.

Wofsey, Marvin M. Management of ADP Systems. Philadelpha: Auerbach Publishers, 1973.

PARTV　セキュリティ管理

議　長　Malcolm Blake Greenlee

シティバンク

参加者

David L. Costello

バンク・オブ・アメリカ

Linwood M. Culpepper

海軍省

Donald L. Eirich

米国会計検査院

Thomas Fitzgerald

マニファクチャーラーズ・ハノーバー・トラスト（銀行）

Wallace R. McPherson, Jr（記録係）

保健・教育・厚生省

編集者注

議長の経歴紹介

マルコム・ブレーク・グリーンリー氏は，シティバンクの監査部次長補佐で，データ・センタの設立，運営上のリスク・アナリシス，物理的ならびにコミュニケーションのセキュリティ，およびプライバシーのための総合政策と基準開発の責任者である。同時にまた，リスクの評価と運営上の新しいリスクを相殺する方法・手順の開発と具体化の責任者でもある。

同氏の経歴は，1956年，パーデュ大学における研究と講義にはじまり，1957～1968年には，ジョン・ポプキンス大学で上級物理学者として，また，ポラリス潜水艇の衛生航法施設のプログラム・マネジャ，各種システムのための応用物

理実験室のプログラム・マネジャなどを歴任，マイター・コーポレーション(Mitre Corp.)のスタッフ，Advanced Management Reserch の指導員を務めた。

1969年にシティバンクに所属してからは，世界的規模の自動支払システム設定のプログラム・マネジャとしてその全局面を担当するかたわらシティバンクの子会社のトランザクション・テクノロジィ（東部）の技術活動のマネジャを務めた。同氏は，パーデュとメリーランドでの物理修士課程で学び，パーデュから物理と数学の学位（ＢＳ）を得ているほか，ジョージ・ワシントン大学からも財政と管理の修士（ＭＢＡ）を受けている。著書は数種あり，いくつかのパテントを所有している。

本会議の議題

セキュリティ管理：

セキュリティ管理機能の評価にはどんな監査方法と技術が使用できるか

情報処理システム内における物理面，手続き面，技術面におけるコントロールの効率と効果を確保するために多くの組織内にセキュリティの管理機能が設けられ，このような機能は種々の組織レベルで設置されていて，割当てられている責任も異っている。集中主義の観念が採られるか，分散主義の考え方が採られるかによってあるものはスタッフの形をとり，またあるものはラインの形態をとっている。

本会議の目的は，大きな組織におけるそのような機能の義務と責任と，その最も効果的な組織構造を定めることであり，さらに進んでは，そのような機能の評価に使用さるべき監査の方法と技術の確認を行う必要がある。

本会議が全グループによって，つぎのような報告書が満場一致で作成され，審議された。

セキュリティ管理

総合報告書

デビッド　L．コステロ

リンウッド　M．カルペパー

ドナルド・L．アイリッヒ

トーマス・フィッツジェラルド

M．ブレーク・グリーンリー

ウォレス　R．マクファーソン．Jr．

1．　序

1.1　総　則

米連邦政府（および関連機関）内の情報処理システムに対して，下記のような面における指導を行うために，ブルックス法（ＰＬ89－306)の規定に従って，連邦政府内情報処理基準（Federal Information Processing Standerds＝ＦＩＰＳ）が作成されて発行されている。

－システムのセーフガード

－活動の継続を維持するための準備をする

－システムによって処理される情報のセーフガード

個人情報の取扱いに関しては，1974年のプライバシー法によって法律上の規制が課せられている。この法律は市民のプライバシーに関する暗黙の権利を守るために，なんらかの慎重な手段が欲しいという米国市民の希望の具体化されたものとみることができる。この法律の条項に該当する組織は非常に大きく，分散されている傾向が大きい。

本報告書は，この法律によって表明されているかかる世論の希望に対処する1つの方策としてのセキュリティ管理機能の実施について述べるものであり，ここに述べる実施要領は，標準的なＡＤＰ監査事項に基いており，ＦＩＰＳの定める技術ベースを利用する。

セキュリティ管理機能の定義が明示されれば，その機能の監査は基準に盲従的な標準的な審査を行うことになる。

1.2　プライバシーに関する立法

1.2.1　1974年のプライバシー法

ますます大量に収集されている個人情報のプライバシーを守るため，1974年のプライバシー法として知られている公法93－579が施行された。この種の情報は，拡大する政府機構の技術的改良とデータ要求によって個人情報の利用性がますます増大しており，活発に収集されている。

この法律の範ちゅうに入る機構は，適当な管理，技術，および物理的なセーフガードを設置する必要があり，これを実施するための機構の規則は1974年のプライバシー法（5USC 552a)に定められている。多くの部／局の場合，これらの規則の実施は管理機構をデータ・センタのユーザか，それ以上の組織レベルで追加することによって実現しつつあり，この管理機構によってセキュリティ管理機能が実施される。

1.2.2　外国の法律

米国以外でも，多くの国々が公共および／または民間企業のプライバシー関係の立法を行ったり，考慮しており，個々にあげれば，

○スウェーデンおよび

○ドイツ（連邦とヘッセン州）ですでに立法化され，

○デンマークと

○フランスでは審理中である。

これらの法律が地理的な領土内にとどまらないため，システム設計において次の事項を考慮する必要がある。

○国境を越えての情報の流通

○国家主権の問題

○戦時，あるいは戦争が予想される場合，

○情報の流れの中断が起り易いこと

1.2.3　国際プライバシー法の適合性

欧州委員会は（米国務省と通信政策局と共に）これらの対立する法律の要求を調整するための努力を開始しており，現在（未解決）の環境下でのシステムへの含蓄的な依存度を軽減するために，近い将来において，条約による調整が成功することが望まれている。

セキュリティ管理機能は，多くの国の法律で暗に含まれているものであるが（1974年現在），ドイツの場合は，"データのセーフガードのための連邦監督官"の署名が明示されており，セキュリティ管理を組織し，管理，実行，報告するスタッフが定められている。民間企業も同様な機構を持つべきである。ドイツ法も1974年のプライバシー法もその要求する内容は同様であるし，また監督官の機能，義務などの定義を明確にするため，本報告書に監督官の義務の概要を添付する。

1.3 本章の構成

この章は3つの部分と1つの付録で構成されている。

第1の序に続いて，第2のセキュリティ管理プログラムでは，計画，マネジメント・コントロール，およびセキュリティ管理者のＡＤＰセキュリティ義務と機能について検討し，第3のセキュリティ管理機能の監査で，使用さるべき監査機能と監査方法についての機構上の要求事項を推薦する。付録にはドイツ連邦プライバシー法に含まれている要求事項の一部が含まれている。

2．セキュリティ管理プログラム

2.1 序

前述した諸般の事情から，連邦機関の内部にセキュリティ管理のための組織機能を設ける必要が生じた（これは多くの機関にとって比較的新しいかも知れない）。セキュリティ管理は，一方では従来からのデータの完全性の問題と機関の情報資源を変形や消失，破壊から守るということを含むかたわら，また一方では，情報

を漏洩や不当使用から保護することにも注意しなくてはならない。

したがって，セキュリティ管理は，機関が管理するデータを保護するための総合計画を立てなければならない。こゝで，ＡＤＰシステムに適用できるセキュリティ管理の原則にふれておくと，一般的には，別個のセキュリティ管理機能が実際的であり得るのは大きな組織だけである。小さな組織では，この機能は他の機能や仕事と組合せた形で処理することができる。

本セッションのメンバーは，機関のデータ・情報資源を保護する責任は物理的に管理する者と，これの責任者の個人責任であると信じている。

1974年のプライバシー法も不当な意図的な漏洩に対して，すべての幹部，職員に個人的な責任を課して，罰金刑を規定している。このように，われわれは，情報のセキュリティは指揮系統を上下するラインの責任とするのが適当であると信じている。この責任を他の管理，処理，監督などの責任から分離して別個のセキュリティ管理体に一任することは，異常な還境でない限りは，明かに実際的ではないと思われる。

つぎに，セキュリティ管理（注１）は，適当な組織上のレベルと本部において管理補佐をするスタッフ機能（ＤＰライン部門から独立）であるべきで，セキュリティ管理は全体政策と監視，それに継続することをベースとしたセキュリティ計画の全般的な有効性に対して責任をもたなければならない。

（注１）この文脈からみると，この報告書全体を通じて使われている“セキュリティ管理”は恐らく誤称で，セキュリティ計画管理と呼称するほうが良いと思われる。

2.2　マネジメントによる計画

セキュリティ管理の計画は，組織内で３つの段階に分けて立案される。すなわち，最高段階では，包括的な方針が立案され，これにはつぎのような問題が提起される。

○　ＡＤＰの設置を承認する前に，とられるべきステップはなにか。

○　確立された方針に対する例外をいかに認めるか。

○　確定方針が守られているかどうかを最初はどのようにして判定するか，またその後いかにして判断するか。

○　運営経験の結果として，方針をいかにして維持し，更新してゆくか。

組織内の中間段階では，方針を実現するためのさらに詳細な指令が考えられ，これらの指令には下記のような問題が提起される。

○　ＡＤＰシステムのためのリスク・アナリシスの実行にあたって考慮すべき要素はなにか。これらの要素のうち，いづれをインプット，すなわち，不変としてとるか，いづれをアウトプットとしてとることができるか。

○　システムの導入に際して，チェックポイントはどこにおくのか。各チェックポイントにおけるドキュメンテーションはどうするか。

○　どのような種類のレポートが必要か。また誰がレポートを作成するか。レポートを受けとるのは誰か。セキュリティ侵害のレベルごとにレポートが必要であろう。たとえば，それぞれの侵害のレベルによって，組織内でレポートの提出されるレベルが異るかもしれない。

○　セキュリティの各問題の責任者は誰にするか。これらの問題には，身元調査，監査証跡の分析，セキュリティ侵害レポートなどが含まれる。

一番低い段階では，これらの指令が実際に実行される。この段階で実行されるべき機能には下記の事項の作成が含まれる。

○　指令の実施計画

○　実施に必要な資源の見積り

2.3　マネジメント・コントロール

マネジメント・コントロールは，その組織のセキュリティ目標の達成を保証するために従来から必要とされてきた種々のコントロールを実行することにあり，つぎの事項からなる。

方針 ― 管理目標

○　組織の利益保護

○　組織的なデータの保護

○　ＡＤＰ資源の保護

と効率的でかつ費用対効果の優れた方法によるこれら資源の濫用防止の明示である。これらは，下記の事項に対する明確な方向を与えるものでなければならない。

○　どの情報を保護すべきか

○　遵守すべき保護のレベル

○　誰が誰に情報を発表・公開する権限をもっているか

○　違反に対する懲戒の基準，その他

このような方針は，通常セキュリティ管理機能より上位の組織的レベルか，あるいは少くともトップ・マネジメントの完全参加の下で，正式に形式化され，セキュリティ計画の基礎になるものである。

手続 ― 管理目標を達成するための処理，指令の記述である。これらの記述は，下部の管理レベルにおいて，以下の各項で述べる管理的，物理的，技術的なセキュリティの基準とコントロールを実行するために十分な記述が詳細に行われていなければならない。このほかには，レポートの性質，タイミング，受取人とその例外事項も含める必要があり，手続きはＡＤＰ機能の実行に限るべきではなく，組織内のユーザ自身が使用するデータとＡＤＰ資源のセキュリティ手続きも含めるべきである。手続きの公布前には，セキュリティ管理スタッフの審査と同意が必要である。

実行 ― 従来からの管理原則によって指示されているその他の諸活動として，下記のものがあげられる。

○　十分な監督，評価，コントロール

○　従業員の行動の監視

○　品質管理

○　システム上の明確なあるいは疑わしい違反の調査

○　懲戒行為の設定と施行

2.4　ADPセキュリティ

2.4.1　管理面のセキュリティ

セキュリティ管理機能には，下記の事項を含めた管理面のセーフガード基準の開発と維持の責任が含まれる。

○　セキュリティの実施計画

現在の物理的，技術的，管理的なセーフガードの分析と，

- データおよび資源の弱点
- これらの弱点のセーフガードに必要な保護措置についてのシステム管理者の判定にもとずく

計画は必要なセーフガードを追加するために必要な活動，資源，スケジュールの詳細にわたっていなければならない。

○　非常時対策

プライバシー保護手続が許可なく開示されたり，その違反が発見された場合にとらるべき行動を明示する。この対策には告知，適切な回復，訂正行為も含まれる。

○　災害 — 緊急処理計画

施設がそのセーフガードとバックアップの責任をもつすべての個人データの保護と回復の能力を含み，すべてのセキュリティ・セーフガードが常に守られるための準備をする。

○　施設に関するセキュリティの概要

単一のファイルに下記事項を収容する。

- 施設で働く人々・機関，またはこれと接続する人々や機関が守るべき手続き
- ログ，監査証跡など，セキュリティ記録の場所と形式
- 内外部のセキュリティ検査の結果
- 実行されたすべてのリスク・アナリシスの結果

－ 施設のセキュリティ実施計画の写し

－ あらゆる非常時のバックアップと災害対策の写し

○ 許可管理リスト

－ 施設への出入を許可されている人員のリスト

－ 許可されている端末ユーザ

－ 認可されている端末

を含み，リストはすべて最新のものであること。

○ プログラムの修正，テストおよび確認の管理

これには下記の事項が必要である。

－ データとシステムの仕様は＂知る必要のある＂人だけに制限する

－ プログラムの変更が実施段階に入る前にテストする必要のある修正をコントロールする手続き

－ 模擬テスト，データを使用するシステムの修正，または新システムのテスト

－ システムの稼動前のシステム機能の完全性ならびに信頼性確認

－ アナリスト，プログラマの任務のモジュール化（人員的に可能な場合）

○ 要員管理規則

－ 権限と責任を確立する

－ セキュリティの自覚，その他，積極的勤労を生む要員参加の計画を立案する

－ 将来性のある要員の評価が十分なされているかどうかを評果する

管理面からのセーフガードの根本的な役割は人間の権威，判断，決定過程の機能である諸活動を設定することである。

2.4.2 物理的セキュリティ管理

2.4.2.1 物理的な接近

データ処理施設や個々を構成する資源への接近をコントロールすることがセキュリティの実現のための第1歩ではあるが，これはセキュリティの第1段階であると考えるべきで，その上にさらにレベル／フォームを設定してゆく基底になるものである。

人間の接近を制限するセキュリティ手続きの作成に際しては，つぎのような考慮が必要である。

○　制限地域

－ 建物全体

－ データ処理センタ

－ すべての付属機器と施設（キーパンチ，キーテープ，プリンタ，出力装置など）

－ リモート・ジョブ － 入力または出力装置

－ リモート・ターミナル

－ 補助電源，燃料，用水貯蔵地区

－ 通信回線，集信装置地区，その他

○　多重制限

データ処理施設の１地域へ接近する必要のある人が必ずしも施設の全地域，あるいは他の地域へ接近する必要があるわけではない。可能な場合には，個々の地域への接近は区別して，別々にコントロールされるべきである。

○　接近制限の方法

接近を制限する方法の選択には下記のものが含まれる。

－ ドアの施錠（鍵またはコンビネーション）

－ ドアのガードと個人の認識チェック

－ ドアのガードとバッジまたは身分証明書

－ 個人がナンバーコードを使用して開閉する電気ドア

－ 磁気コード，パスかバッジで作動する電気ドア

－ 個人識別（サイン，手のひらか指紋（簡単にはできない）チェックによって作動する電気ドア

－ 上記の数種の組合せ

接近制御の方法を決めるときには，これらの装置が制限地域の内側から働くような方法を考える必要がある（とくに緊急の場合）。これらの装置は緊急の場合

には，人員の安全のために至近の自由出口になる必要がある。（所定の火災／生命安全法規に従う）。

2.4.2.2　災害防止

データ処理の資源を機器の物理的な損傷の影響から守らなければならないが，一方また，オペレーションの継続に関する規定も優先して考えなければならない問題で，潜在的な事象をその可能性からランクづけして，適当な防止策を講ずべきである。より起りそうな事象の一部には，つぎのようなものがある。(注2)

○　電源消失（全般，不足）

○　用水消失（空調などの機器）

○　火災

○　洪水などの水害（天災，施設内外のパイプの破裂，火災による）

○　爆発，その他

認識できる可能性を最小限に止めるための方策としては，種々の方法が考えられるが，下記に，考えられる代替策のいくつかをあげる。

○　代替用の公共電力ルート

○　自家発電（電気的起動連続特性をもつもの，あるいは，もたないもの）

○　自家貯水施設，または取入計画

○　適切な防火資材

○　発火／発熱式火災防止器（ハロン，スプリンクラ），その他

(注2) NBS FIPS PUB 31, Guidelines for Automatic Data Processing Physical Security and Rish Management（1974年6月）

2.4.2.3　バックアップ施設

ＡＤＰ施設の処理能力の全体，または重要な部分が失われた場合には，継続計画かあるいは緊急処理計画（2.4.1項参照）のいづれかを発動する必要がある。バックアップ施設との間の必要な用紙，データ・ファイル，出力，要員，その他，移動中は勿論，このバックアップ施設にもまた，物理的なセキュリティが講じられなければならない。

2.4.2.4　格納ライブラリ

下記の物件を保護するために，十分な物理的な格納地区を離れた地域に確保する必要がある。

○　テープ，ディスク，カード，ファイル／記録

○　オペレータ・ラン記録，プログラマ／アナリストの設計および保守を含むプログラム・ドキュメンテーション

○　各種の管理面からのセキュリティ・コントロール記録／計画で下記を含む

－ 許可リスト

－ セキュリティ概要／レベル・ドキュメンテーション

－ 緊急用バックアップ／処理計画

これらの地域は許可のない人の接近を排除し，かつ災害を防止できるように建設されなければならない。これらのライブラリは，一般に他のＡＤＰ資源と比較してより高度の接近・災害のセキュリティ策を講じるべきである。データ・ファイルの多くはオフ・サイトのバックアップであるから，オフ・サイト施設にも同様，またはこれに近いレベルのセキュリティ保護策が必要である。これらのファイルを移動する際にも適切な予防策を講じる必要がある。

2.4.2.5　データの取扱いと処置

ＡＤＰ施設内でのデータの取扱いに，ある種の物理的なセキュリティ技術が適切なことがある。もし，多重のセキュリティ・レベルが採用されている場合は，この情報の取扱いを必要な地域に制限するか，あるいは情報を移動する途中で見られないようにする方法（たとえば，密封／施錠した容器／運搬具／トラックなど）を考えるべきである。限定情報や個人情報を含むデータには，なにか物理的に容易にこれを識別できる方法を考えるべきで，外部ラベル，ラベルやリールの色別け，それらのファイルの格納場所を別にする方法などが利用できる。しかしまた，このような方法は，逆に不当に接近しようとする場合の識別法にもなる点を忘れてはならない。

また陳腐化したファイルや入出力の適当な処置方法を決めておくことも必要

である。情報を保存しないときは，ファイルが再使用される前に，消磁，別用途に使用して消去，あるいは破壊するかしておかなければならない。プリンタの整合時やジョブの再処理時に使用した書類のようなコンピュータからのスクラップは陳腐化した入出力と同様に処置する必要がある。通常の処置方法としては，所定の手続きによる寸断，焼却（環境問題の恐れがある）などがある。

2.4.3　技術的セキュリティ

○　セキュリティ・システム

セキュリティ担当者は，セキュリティ・システムのプログラムとすべての関連ファイルの保守に関する責任を持っている。ユーザ・プロフィールにおける変更の要求は，しかるべきマネジメントとセキュリティの認可を得てその地域の管理者が行う。（地域のセキュリティ管理者に対する変更ができるのは，セキュリティ管理者だけである）。

○　データとファイル

セキュリティ管理者は，すべてのファイルの内容とその物理的安全を保護する責任をもち，セキュリティ・システムを使用して，システムが全データの保護に万全であることを確認しなければならない。

○　プログラム・ライブラリ

セキュリティ管理者は，プログラム・ライブラリの確実性を確認する責任を持っており，この点に関するその職務内容にはつぎのものが含まれる。

－ 自己のコントロール下にあるすべてのプログラムとテスト・ファイルへのアクセスを制限するアクセス・コントロール・プログラムが作動することを確認する。

－ しかるべき管理者からの文書による要求がある場合にのみ，認可された要員に対してプログラムのコピーと適当なテスト・データを提供する。

－ プログラムの変更を行うための方法を提供し，適正な並行テスト期間を確認する。

－ 処理の継続性を確保するために，プログラム・ライブラリとデータ・ファイ

ルのバックアップ施設を用意する。

○　オペレーティング・システム

ＡＤＰのライン管理には，オペレーティング・システムの保守責任があり，ハードウェア業者との"調整"をシステム・プログラマの承認を得た上で実施しなければならない。このなかには，システム変更の保守とテストの責任も含まれる。セキュリティ・コントロールのセキュリティの変更とオペレーティング・システムの安定は，セキュリティ管理者の責任である。

○　テレプロセシング

セキュリティ管理者は下記の責任を負うものとする。

－ ユーザ・テーブルとテレプロセシングのセキュリティ（ＴＰシステム内のセキュリティ・モジュールの保守を含む）

－ ＴＰシステムのバックアップと回復（バックアップ機能〔たとえば，ダイアル・アップ〕，ライン・コントロール，およびセキュリティ違反の調査を含む）

○　暗号化

セキュリティ管理者は下記の責任を負う。

－ 暗号化アルゴリズムの維持

－ アルゴリズム用キイの作成，配布・使用のコントロール

2.4.4　訓練

セキュリティ機能のための訓練には２種類ある。

○　システムを実施，維持，運用する要員の訓練

○　システムを利用する人々の訓練

第１のグループの場合には，ＡＤＰセキュリティ管理の既定の専門コースと組合せた正式な訓練用カリキュラムが必要である。ＡＤＰのハードウェアとソフトウエアの設計・使用法に関する技術面からプライバシー法の規定に至る範囲にわたる多彩な項目を正規な方法で教えなければならない。

一方，システムの使用者に対しては，セキュリティに違反した場合の結果などに関する訓練を行うことが必要であり，これらの使用者は適当な訓練をうけてい

ることの確認のため，定期的にチェックする必要がある。

2.4.5　オンライン・システムの場合のセキュリティ・システムの一例

大型のオンライン・システムのためのセキュリティ・システムは広範囲なものになり，各端末とアプリケーション・プログラム／ファイルとの間で有効なバッファとして十分に働けるものでなければならない。システムの規模と複雑性が小さい程，高度な知識も必要でなくなる。しかしながら，ある種の自動システムは必要である。ここにあげたシステムは下記の３つのファイルからなる。

○　端末ファイル

このファイルは端末のステータスに関するすべての必要情報を格納するもので，つぎの項目をもつ。

－ 端末ＩＤ－特定の端末と同義のユニークな識別。この識別は各端末のハードウェア特色で，この端末から送信されるすべてのメッセージに入れられる。

－ ユーザＩＤ－ログ・オンの成功後にこのファイルへ捜入されるユニークな識別である。この項目はトランザクションのロギング前に，トランザクション・メッセージに付けられ，これによって各メッセージには送信端末とメッセージの送信人の識別があることが確実になる。

－ 端末のステータス － この項には端末のステータスが入る。

－－ 休止　－未だ端末がログ・オンしていない。

－－ ログ・オン処理中　－ログ・オン・メッセージは受信されたが，パスワードが証明されない。

－－ アクティブ　－ログ・オンが完了して，ユーザＩＤ項目が更新された

－－ 違反　－セキュリティの違反行為が発見された。調査が完了するまで端端はログ・アウトされる。

－ 違反カウンタ　－この項は誤まったパスワードかトランザクションを入れようとして失敗（無効）した回数を記録する。この数がプレセットした数，たとえば３，に等しくなると，端末ステータスは〝違反〟にセットされる。

－ 最終トランザクション時 － 端末において，各トランザクションごとにログ

・オンが必要でない場合は，この項目が"アイドル"チェック用に最終トランザクションの時間を保持する。メッセージ間の経過時間がプリセットしたアイドル・タイムをオーバーすると，端末は休止ステータスにセットされて，再び最初にもどってログ・オンする必要がある。

○　ユーザ・プロフィール

このファイルには，端末オペレータに関する全情報が格納されており，以下の項目が保持されている。

－ ユーザＩＤ　特定の個人と同義のユニークな識別で，この項目は大抵の場合，端末オペレータの従業員番号である。

－ パスワード　端末オペレータが入力するユニークなコードで，これによってシステムに端末オペレータであることを識別させる。"プリント禁止"モードでオペレータが入力する（パスワードは端末で表示されない）。確認の後端末ステータスが"アクティブ"にセットされる。パスワード・コントロールは数段にすることも可能である。

－ トランザクション・コード　端末オペレータが実行を許可されているトランザクションとアプリケーション・モジュールの名称を識別する１組のコードである。ログ・オンが成功すると，セキュリティ・システムは特定のトランザクション・コードが認可されているかどうかを決定するために，この項目を調べる。これで突き合せが得られると，アプリケーション・プログラム・モジュールがコールされて，アプリケーション・モジュールへコントロールが渡される。もし，この突き合せがうまくいかないときは，違反カウンタが１増加されて，トランザクションは拒否される。

○　トランザクション・ファイル

さらに複雑なシステムでは，下記のようにユーザ・プロフィールとの組合せでトランザクション・ファイルを使用することができる。

－ トランザクションＩＤ　このファイルのキーとして使用されるユニークなコードで，端末オペレータが入力する。

－ サブ・コード　形式にもとづいてファイル内の特別のデータ・ファイルへのアクセスをさらに制限するために使用できる項目である。ファイルをさらに小さいユニットに分割する場合には，この項目によって，特定の端末と／またはオペレータにアクセスが許されるユニットを指示することができる。

－ ファイルＩＤ　この項目はマスター・ファイルと特別のトランザクション・タイプによって実行可能な機能を識別する。

○　監査証跡

一般的には，監査証跡はセキュリティ管理がデータとデータの保全を取締まるシステムのセキュリティ機能を監視できるように利用されなければならない。監査証跡，個々の組織や活動において知覚できる恐威に対して適当であるとされるセキュリティ・レベルにユニークな必要事項を満足させる種々の特性をもつようにデザインされてよく，一般には，誰が何のデータへアクセスしたかを記録するようにデザインされるべきである。求める詳細の程度に従って，アクセスされたファイル・レコード，あるいはデータ要素でさえも識別できるし，また，何のトランザクションが実行されたかを識別することも可能である。

セキュリティ・システムの機能は，バッファとして働き，偶然による違反の可能性を減少，故意の違反に対して必要な専門知識のレベルを上げることである。システムは各地域のセキュリティ担当者に負うところが多く，すべての違反はセキュリティ担当者が毎日点検することになっているログとセキュリティ管理者が審査する特別ログに記録される。セキュリティ担当者は，また，個々の多重違反について直ちに連絡してくるオンライン・ハードコピー・ターミナルを持っていなければならない。これによって，担当者はその識別された端末へ出向いて，違反の原因を判定する必要があり，端末の機能再開を許可するためには，その特別のセキュリティ・コードを使用して，その端末をリセットしなければならない。さらに，担当者はセキュリティ管理の各責任者に違反に関しての報告書を提出する義務がある。

3．セキュリティ管理機能の監査

3.1　組織的条件

セキュリティ管理機能の監査計画を立案するに際しては，つぎの2つの機構上の問題を考慮する必要がある。

○　監査機能はセキュリティ管理機能から独立したものであること。

○　監査機能は分散してよいが，監査のスタッフは，直接その機関の長に対して，または監査の長を通じて機関の長へ報告しなければならない。

3.2　監査プロセス

セキュリティ管理機能の監査は，簡単な適合性監査で，監査人の任務は表示された方針が尊重されていることを確認して，その意見を個々に報告することである。

組織における基準や手続きは，その規模の大小，処理環境，責任の委任などの相違によって異なり，このために監査人は，それぞれに相応するセキュリティ管理機能の完成に適切な監査計画を設定，組織する必要がある。いづれのレベルにおいても，監査計画はセキュリティ管理機能とは独立に，下記の事項を完全に実施しなければならない。

○　監査人はセキュリティ管理機能の設立に際して定められた方針と基準を評価しなければならない。方針と基準は，

－　包括的であり，

－　文書化されており，

－　よく理解され，

－　守られている……必要がある。

○　監査計画は，一般的な監査基準と監査技術を使用して既定のコントロール手続きがどの程度守られているかを評価し，また，新たに設定される手続きを審査，評価する必要がある。

○　監査人は，自主的にセキュリティ管理機能内部の，その他の重要なコントロ

ール・ポイントおよび手続きを調査しなければならない。

○　監査人は，セキュリティ管理機能をより効果的にするためのコントロールの追加の必要性を発見する必要がある。

○　監査人は，発見したこと，および意見を指定のマネジメントに対して報告しなければならない。

監査で審査される特殊な手順やコントロールは，たとえば前述のように，採用されている手続きと特定の責任の委任によって決まる。

付　　録

ドイツ連邦プライバシー法の特長の一部

1．公共部門データ・セキュリティ管理ー組織

1.1　連邦監督官の役割

データを保護するために連邦監督官が任命されなければならない。

監督官は

- 5年の任期をもち，
- 連邦内務省に所属し，その監督下にあって，政府最高部へ報告の義務を有する独立した役割であり，
- スタッフをもち，支援をうけ，
- 厳密に規定された法的地位を有するものとする。

1.2　連邦監督官の任務

連邦監督官の任務は下記のとおりである。

- 合法性の確認
- 勧告の作成
- 報告書の発行
- 他部局からの援助の要請
- 個人データ（公共記録）のデータバンクの24時間記録
- 聴問とその処理

2．非公共部門データ･セキュリティ管理

2.1　非公共機関のデータ・セキュリティ監督官

個人データを自動的に処理し，原則として最低５人の人員を永続的に雇用する個人／法人／団体はデータ・セキュリティ監督官を任命しなければならない。

監督官は下記を満足するものでなければならない。

- 書面によって任命される
- その任務を達成する十分な能力を有する
- その任務の遂行によって不利を来すことがない。
- 外部からの指示に従う必要はない
- 支援スタッフを指名，雇用することができる

2.2　非公共機関データ・セキュリティ監督官の任務

データ・セキュリティ監督官の任務は下記のとおりである。

- 合法性の確認
- 必要時におりる政府監督当局の援助の要請，企業／団体の認可は不要
- 下記記録の保持
  - －記憶データの性質
  - －その目的
  - －アクセス要求をする者
  - －使用するＡＤＰ装置の性質
- 個人データ処理プログラムの“適切”な利用の監督
- 従業員の法的責任の教育
- 個人データ処理要員のコンサルタント

3．データ保護に必要なコントロール

法によって要求されるコントロール

- アクセス・コントロール
  - －施設（機器）への無許可のアクセスを禁止し
  - －データ・アクセスを必要なデータにのみ限定する
- 記憶装置コントロール
  - －記憶装置への無許可の入力
  - －記憶装置からのデータの収集
  - －記憶データの変更／取消

  を禁止する。
- 使用コントロール
  - －許可なき者のデータ・システム使用を禁止する（リモート・アクセスによる使用を含む）
- 転送コントロール
  - －自動化された装置によって個人情報を授受できるのは認可された者のみであることを保証する（認証）
- 入力コントロール
  - －何に関する個人データを
  - －いつ，または
  - －だれがシステムに入れたか

  を確認する能力を維持する。
- 監視コントロール
  - －指令の監視：個人データを処理する許可
  - －個人データの転送に際して，
    - －－読取り
    - －－変更，または

－－監督なしの取消

を防止するための監視

－データの適切な保護を確保する組織／内部構造，委員会の監視。

PART VI 様々なシステム環境における監査要因

議　長　Carl Hammer

スペリー・ユニバック社

参加者

Sheila Brand（記録係）

社会保障局

P. J. Corum

モントリオール銀行

Ike Dent

クレジット・ビューロ社（ジョージア）

Peter D. Gross

コンピュータ・サイエンス社

Thomas L. Hamilton

イーストマン・コダック社

James F. Morgan

GEインフォメーション・サービス

Gerald J. Popek

カリフォルニア大学ロサンゼルス分校（UCLA）

Stephen T. Walker

国防総省高等調査プロジェクト局（ARPA）

Ronald L. Winkler

サザーランド・アシュビル・ブレナン

編集者注

議長の経歴紹介

カール・ハンマー博士は，ワシントンD．C．にあるアメリカ大学の助教授，軍の工業大学の客員教授を兼ねるだけでなく，現にスペリー・ユニバックのコンピュータ科学担当の取締役である。氏は過去において，ＲＣＡのミニットマン通信システムの初期設計の責任者，ドイツのフランクフルトにあるユニバック・ヨーロッパ・コンピュータ・センタの取締役，フィラデルフィアのフランクリン研究所のコンピュータ部門の上級スタッフ・エンジニア，ニューヨーク市のコロンビア大学およびハンター大学の教師を歴任した。氏は現在，米国情報処理学会（ＡＦＩＰＳ）の理事であるが，1973年に行われたその最初の全米コンピュータ会議（ＮＣＣ）の科学・技術部門の議長，1976年のＮＣＣの議長を務めた。また同氏はAssociation of Computing Machinery(ＡＣＭ)のワシントン支部のかつての議長であり，米国サイバネティクス学会(American Society for Cybernetics)の会長でもあった。現在は，大統領府の任命によって，National Defense Executive Reserveのメンバであると同時に，また，ニューヨーク科学アカデミー，ＡＡＡＳ，ＩＥＥＥ，Reseach Society of America，およびコンピュータ・プログラマ／アナリスト協会の会員である。イリノイ州シカゴ生れで，数理統計学でミューニッヒ大学から学位を受けている（哲学博士）。

＜本会議の議題＞

様々なシステム環境における監査要因

（ａ）分散処理，（ｂ）専用システム，（ｃ）タイムシェアリング，（ｄ）マルチ・プロセシング，（ｅ）ミニ／マイクロ・コンピュータ等，種々のシステム環境におけるコンピュータ・セキュリティ監査に必要な考慮すべき事項はなにか。

コンピュータ・セキュリティは，一般にはシステムが行動する環境の機能であると考えられる。おだやかな安定した環境で，バッチ・モードで移動する専用システムでは，セキュリティのための必要事項はオンライン・リアルタイム・システムとは全然違ってくる。

本会議は各種のシステム環境をとりあげて，コンピュータ・セキュリティの評価を実施するに際して，監査人が考慮しなければならない主要な局面を認識する

ためのものである。

本会議の全メンバによって下記の報告書が全員一致で作成され審査された。

1. 序

ワークショップに先だっての2カ月間，現状の業務内容の説明書や意見書の提出を依頼し，収集され，関連する参考文献も収集，配布された。このドキュメンテーションは，3月22日（火曜日）午前の部の第1セッション開催中に，チームの全員によって審査された。また，チームの任務の慎重な解釈検討も未組織のままの広範囲な検討方式で開始された。

トップ・ダウン方式による問題の検討は，第1日程の終り頃から始まって，3月23日（水曜日）の第2セッション中も継続され，コンピュータ・セキュリティ監査の柔軟構造モデルの開発のための基礎となる4つの概念的モジュールが集約された。

(i) 3つの重要な監査要素の定義：アクセス・コントロール，正確性，有用性。

(ii) システムおよび環境の形態論，物理的要素，システム構造，要員 — 5つのシステム特性：ユーザの数，サービスのタイプ，システム構成，ユーザのアクセス，アプリケーション・ミックス。

(iii) 監査可能でパラメータ的に識別されるすべてのコントロールの個々に対するスコア・カード値を設定する方法論，またはコンピュータ監査モデル。

(iv) 4つの例を用いてモデルの完全性はもちろん，その能力を経験上から確めるシミュレーションによるモデルの確認

われわれが発見したことの概要は，この報告書に記載されている。われわれの最終目標の達成に尽された全メンバの助力に対して，議長は感謝の意を表している。本報告書の資料は彼等の鋭敏な思考力，集約能力，それに表現力のたまものであり，議長はとくに，シーラ・ブランド女史がメンバの一員であることに加えて，本報告書作成のための監督調整の任に当ったことを感謝している。しかしな

がら，この編集過程における脱落エラーや仕事については，議長が全責任を負うものである。

2．定　義

本報告書中で使用されているコンピュータ・システムのセキュリティに関する主な用語の定義は下記のとおりである。

環境 ― 監査されるＡＤＰシステムを構成する物理的施設，システムの構造，および管理機能。

セキュリティ監査 ― 管理（マネジメント）によって定められた環境の継続と完全性を保証するコントロール・システムの評価。これらのコントロールの適合性の評価はシステム・アクセス，精度，および有用性を検査，評価することによって行われる。

システム・アクセス ― データを取得，貯蔵，検索する能力と方法，すなわちＡＤＰシステムの資源との連絡やその利用である。

システム精度 ― いかなる要求条件の下でもＡＤＰシステムが(i)システムの総合的なロジカル上の正確性と信頼性，(ii)保護機構を実行しデータの完全性を保証するために必要なハードウェアとソフトウェアのロジカルな正確性と完全性をもっている時の状態をいう。

システムの可用性 ― ユーザの主要機能を達成するためにユーザが必要と定めたサービスのレベル，すなわち品質。

3．方 法 論

3.1　監査と設計

セキュリティ監査の実施手順は，セキュリティの対象になるシステム開発の初期段階で行われるセキュリティに関する決定検討と密接な関係がある。この結論

は，われわれがいろいろなシステム環境でのコンピュータ・セキュリティ監査に適用すべき一連の考察を基礎にした方法論を展開しようと試みた際に得たものであり，コンピュータの特性，物理的ならびに管理的な環境等の説明書を厳密に調べる必要があるとの決定がなされた。これらはいづれも相互関連をもつものであって，容易に分離することはできないものである。われわれは最終的に，始めは設計チームが担当し，後に監査担当者が少々，変更しながら担当するステップの一覧表を作成してみた。このことは，効果的な設計チームの構成を調べてみれば，そんなに驚くべきことではない。

費用的に見合う包括的かつ効果的なセキュリティをシステムに組み込むためには，そのチームの少くとも一人は監査人としての見解をもっているべきであり，出来れば，実際に資格のある監査人であることが望ましい。すなわち，監査の仕事には2つの任務があることがわかる。第1は，監査人はシステムの入力を準備する設計チームのアドバイザである必要があり，つぎには，システムの稼動期間中，監査人は従来のＥＤＰ監査機能を実行して，コンピュータ・システムのセキュリティ設計の有効性を再評価する必要がある。

以下，最初は設計チーム，その後は監査チームが，システムのセキュリティの有効性を評価するために必要なステップを例記する。

3.2　設計チームのとるべきステップ

ステップ(1)　全体システムとしての要求事項，目的，敏感性を定義する。

ステップ(2)　ステップ(1)にもとづいて，要望される環境の仕様を決定する。

○　下記の物理的パラメータの仕様：

－　システムの場所

－　"入れ物"（建物）の構造

－　洪水，火災，爆破などの災害時におけるシステムの存続性

○　下記のシステム・パラメータの仕様：

－　情報の分割使用の程度（単一ユーザまたは複数ユーザ）

－　バッチまたは相互作用処理

－　集中または分散方式データベース／処理

－　ローカルまたはリモート・アクセス

－　アプリケーション・ミックス

○　下記の管理パラメータの仕様

－　リスク分析

－　人事手続

－　組織構造

－(a)　アクセス・コントロール

(b)　精度

(c)　可用性に対するセキュリティの要求

－　保険

－　システム開発手続

ステップ(3)　ステップ(2)で指定した環境を実施するために使用されるべきコントロール技法の仕様を決定する。

ここで，セキュリティの目的，方針，および手続の相違を指摘しておいた方がよさそうである。指定された稼動中のコントロールの目的は，アクセス，精度および可用性の規制であり，アクセス・コントロールの目的は慎重な処理に対する個人の責任の形で引きつがれる。この方針はパスワードによるシステムへの登録，あるいは保証地区への出入りに際しての手書きログの形で手続へ引きつがれる。

ステップ(4)　1つずつ個別にコスト／保護分析を実施する。その環境内でシステムを保護するための一連のコントロールを設定する作業でこのステップが最も重大な作業である。このステップでは，ステップ(3)で記述されているシステムの何れかの面を保護するために使用できる各コントロールを分析する。詳細なコスト／保護マトリックスになると，システムの複雑さによるが，数百，数千の同類項目が含まれる。

必要とされるコントロールの各々について，下記の4項目の判定がなされる。

(a) コントロールの実施，開発，オペレーションの費用

(b) アクセス・コントロールの保持に関する効果

(c) 精度の維持に関する効果

(d) システムの可用性の保持に関する効果

(b)，(c)，(d)に関する効果判定は，最終的には0～10の数値（0＝無効果，10＝最高効果）に評価（主観的）される。これは現在の状態に見合うものである。しかし，客観的な効果測定方法の工夫が極力望まれる。

便宜的な方法として，設計者は速記的な評点法を使用しても差支えない。

等級の格づけ＝ＡＣ／Ａ／ＡＶ

ＡＣ＝アクセス・コントロールの効果レベルに割当てる数値

Ａ＝精度の効果レベルに割当てる数値

ＡＶ＝可用性の効果レベルに割当てる数値

これらの格付けは，システム・ドキュメンテーションの一部にとり入れられて，ステップ(5)と監査人が使用する。

ステップ(5)　総合評価を実施する。ステップ(4)の個別分析のあとで，広域のセーフガードの基礎になるものとしてこれらのコントロールの特定なサブセットを選び出す。管理部門はこのサブセットで環境のすべての面 — 物理面，システム面，管理面の保護に必要な深さ，広さ，オーバーラップが最も費用対効果の効率よく与えられることを確認する必要がある。言葉を換えていえば，このステップは，先に定義されたセキュリティの目的を満足させるために"リスク・アセスメント"がなされ，"セキュリティ"システムが設計される段階である。

ステップ(6)　承認されたセキュリティ・コントロールを組み入れる。この新しい全般環境を3つの環境パラメータ（物理面，システム面，管理面）に投入された特質に照らして再評価する。もし，これらの付加特質によって全体システムとしての効果（ステップ(1)で規定された要求事

項と目的の達成）を低下されることがなければ，設計者は実施段階へ進むが，新しい全体システムの分析後，目的が効果的に達成できなくなることが発見されれば，反復処理が必要になり，設計者はステップ(2)へ戻ってステップ(1)で記述されたすべての要求事項が効果的に満足されるまで環境の仕様その他を練り直すことになる。

3.3 監査人のとるべきステップ

システムが設計されて完成すると，オペレーションの段階へ進み，稼動状態でのセキュリティ・コントロールの効果を評価するためにここで監査人の出番になる。先に述べたとおり，初期設計チームのステップと監査人のステップは非常に似ており，一部のステップではただ動詞を変えるだけで事足りる。たとえば，ステップ(1)では，設計者はシステムの要求事項を定義するが，監査人は述べられた要求事項を管理の規定どおりに審査する。

ステップ(1)　監査対象のシステム用にマネジメントが文書化した目的，要求事項，敏感度を審査する。

ステップ(2)　システムの実稼動の間における環境の性質を組織上の記述とは関係なく決定する。物理面，システム面，管理面に対する監査人の感覚は設計段階で指定されたものとは全く違っているかも知れない。

ステップ(3)　ステップ(2)での監査人が認めた環境のコントロールに使用されるコントロール技法を確認する。

ここに，設計アプローチとの明らかな違いを見ることができる。設計者は多数の可能性のあるコントロールを認め得たかも知れないが，監査人は実際に採用されたコントロール・サブセットだけを検査するわけであり，独自の検査を行い，システムのセキュリティの要素識別の出発点にシステムのドキュメンテーションを使用しても，しなくても差支えない。

ステップ(4)　きめの細かいコスト／保護分析を実施する。ステップ(3)における

ように，監査人は可能なセーフガードの全部を扱うことはなく，監査で決定したとおり，システム内で実施され適切に機能しているものだけに関係する。設計者は，ＡＣ／Ａ／ＡＮ等級の要素に対する値を非客観的根拠によって決定しているかも知れないが，監査人は規定のセキュリティの目的を達成するために，これらの決定をハードウェア，ソフトウェア，それに各評価要素の効果をテストするその他の複雑な技法（利用できれば）を使って拡大していくことになる。

ステップ(5)　総合評価を実施する。ここで監査人はマネジメントによって設定された目的が満足されるかどうかを判定するために，セキュリティ・システムの総合効果を評価する。すなわち，設計者の等級格付けと監査人が発見したものとの間での比較が行われる。設計者と監査人の測定標準が恐らくは違うだろうから，これはたとえ鋭いものであっても，単なる質的な比較に過ぎないことになろう。

ステップ(6)　弱点が発見された場合，たとえば，設計者の格付けのほうが監査を通して決定されたものを上廻るようなときはセキュリティを改善する勧告も含めた監査結果報告書を作成する。また，環境が初期設計時点の仮定から変ったり前回の監査後に変化しているときは，全体的なセキュリティ・コントロールの要求事項を変えるように勧告することも監査人の責任である。

4．環境とコントロール

設計者と監査人のお互の義務は明確に区別されなければならないが，システム的な監査方法の重要な要素は，設計作業と監査業務の間の密接な連繋である。設計に関係している要素を十分に理解したうえで，監査に際しては同じ要素を適切に配慮することを忘れてはならない。これに関しては，主要な要素として２つが

あげられる。その第1は，システムが稼動する環境であり，第2は，その環境を実現するために使用するコントロールの技法である。肝心なことは，システム稼動の環境は設計段階で定義され，監査でこの環境の記述を指針として使用することである。もしオペレーションの環境が，設計時に仮定されたものからシステム・セキュリティの面に影響を及ぼすような方向に変っているときは，監査の一部分の仕事として，このような影響を分析し，設計チームが最初にとったと同じような手続でセキュリティ・コントロールの要求事項を再評価しなければならない。

ここで提唱するアプローチでは，2種類のやや複雑なチェックリストと参考資料を使用する。第1のチェックリストは，システムを稼動させる環境をかなり詳細に設定するのに使用される。新システムの設計の場合には，このリストは希望されるシステム特性のリストであり，評価対象の現存システムのケースでは，既に存在するシステム特性のリストである。前述した処理手続は，新システムの設計でも，現存システムを拡張強化する場合でも，これを単に監査するときでも活用できるものである。監査のときには，環境の記述は与えられている。監査人は，環境になんらかの矛盾性を発見した場合には積極的にこれを指摘すべきであるが，しかし，環境チェックリストは，設計者が指定したコントロール技法が与えられた環境を実施するのに十分なものであるかどうかを評価するための基準点である。

第2のチェックリストは，システムを稼動させる環境を実現するために，設計者が採用できるコントロール技法の一般的な種類を記載したものであり，後述のようにその種類は物理的な施錠や囲いから，内部的なハードウェア，ソフトウェアによるアクセス・コントロール・チェック，さらには管理手続にまで及んでいる。設計の過程で，設計者はシステム環境の設定後，そのシステムの保護のために利用したいと思う方法をコントロール技法チェックリストから選択する。このコントロール技法のチェックリストの各記入項目は，連続体の1セグメントを表わしており，各項とも2つの変数の相関関係で程度が異なる。すなわち，保護の程度とコストの関係で，保護の範囲が狭まれば，普通にはコストは最低ですみ，程度が高く保護が大規模になれば，それにつれてコストも上昇する。ドアにつけ

る物理的な施錠を例にとれば，簡単なナンキン錠と複雑精巧な電子制御でしかも中央監視方式のドア・ロック・システムでは，費用の範囲も異ってくる。システムのもつ情報の敏感性が（環境記述によって）与えられたならば，設計者はセキュリティ・コントロールのために必要な方法を全体として総合的に決定するために，採用しようとするコントロール技法と保護／コストに関する適切な見解を選定しなければならない。

セキュリティの点から見た場合，環境の決定とその環境の実現のためのコントロール技法の妥当性を評価するには，３つの基準，すなわちアクセス・コントロールと精度，および可用性がある。これらの要素のいずれも環境評価で扱われるべきものであり，採用されているコントロール技法は，いずれもこれら３つの要素全部に対しての格付けが必要である。ある種のコントロール技法は，これらの尺度のあるものには適用しないこともあろう。たとえば，施錠は情報の精度には影響はしないが，しかし，システムの可用性とアクセス・コントロールには重大な影響をもっている。環境の記述には，これらの領域の各々に必要な保護の程度を述べ，コントロール技法の総合評価では，これらの方法の各々についての設計者と監査人による格づけが計算されて，環境要求事項との比較がなされなければならない。

コントロール技法チェックリストに記載されている多くは補足的な性質があって，ある１つの方法を採用すると，他の方法が不要になる可能性がでてくる。１つのコントロール技法の投資額によって，その補充技法への投資額が決定されよう。コントロール技法チェックリストの各項目間の相互関係は複雑なものであり，環境を実現するために十分な方策が完全に，しかも過重にならないようにとられているかを確認するためには，種々の環境におけるコントロールの相互作用の関係を解説したガイドブックをチェックリストに添付する必要がある（ＰＡＲＴⅤ参照）。ガイドブックには，各種コントロール技法の効果レベルとコストの関係の解説と実行可能なトレード・オフの相関的評価が記載されている。

設計者は，システムを運営する環境と適切なコントロール技法の両者を設定する。監査人が，十分なコントロール技法が適用されているかどうかを決定する際

に使用する方法も全く同じものである。設計者は，先ずコントロール技法チェックリストを入念に調査して，使用する適当な項目を選出する。それから，各記入事項ごとに選定された有効性評価基準を論理的に集計することによって，システムの総合的なセキュリティの評価を行う。この場合，もし総合分析の結果，保護が十分でないとか，あるいは費用的な限度を超えてしまうときは，設計者はコントロール技法を，恐らくは環境自体を再評価して，適当な費用で必要なセキュリティを完成するために必要な変更を行うことになる。

監査人は，環境チェックリストが与えられたならば，先ず現実の稼動環境が設計段階で仮定されたものであるかどうかの判定を行い，そのあとで，その環境の遂行に適切であると思われるコントロール技法を決定する。監査人は，自分のコントロール技法，チェックリストと設計者のそれとを比較して，その相違について考察し，詳細分析を実行する。チェックリストの記入項目ごとの評価を行ってから，設計者と同様な総合分析を実施し，この総合分析が終ったならば，もう一度元に戻って，全体システムを完璧に知ったうえで，個々のコントロール技法に対する自身の評価を調整する。この監査過程で得られる結果は設計によって，稼動環境に対するセキュリティ要求事項がどの程度満たされているかの総合評価である。この監査の過程によって十分な保護であると評価されれば，そのシステムは使用を承認されてもよい。これが不十分ということになれば，ここで設計者はもう一度コントロール技法チェックリスト，あるいは環境チェックリストへ戻って，システムの必要とされるセキュリティを確保するために適当な修正を行うことになる。

この過程での問題点は，設計者と監査人が同一のチェックリスト情報を使用することである。このことによって，関連し合う事項を討議する共通のベースが得られ，これがわれわれの方法論の決定的な要素になっている共通出発点となる。コントロール技法チェックリストから要素を選択することと，各々の要素に与えられる保護の程度は，しばしば主観的であり，設計者としては，これらの方法に対して監査人が与えた特定の評価には異論があることもある。重要な点は，設計

の全要素を設計者と監査人が共通の前後関係において把握することである。設計者と監査人の両者で使用する方法に関するこのような完全な共通リストが，今までの監査に不足していた要素である。

4.1 チェックリスト

チェックリストは，環境チェックリストもコントロール技法チェックリストも，いずれも3つのサブ・カテゴリに分類されている。すなわち，物理面，システム，管理の3つである。物理面の環境チェックリストの場合は，システムのセキュリティに物質的に影響を与える物理的環境の諸要素があり，このなかには，洪水や犯罪のような自然または人為による災害，その他特別の動力や空調などを考慮に入れたシステムの地理的立地条件も含まれる。

システム環境リストには，システムの内部構造を表わす手段が含まれる。とくに，ここにはシステムのセキュリティを実現するために内部的なハードウェア／ソフトウェア的手段に頼る必要性に影響する諸要素が含まれている。管理方法には，システムの保持する情報の敏感性と正確性，想定されるシステムへの恐威等の要素が含まれる。

システム環境は，つぎの5つの物理的／論理的要素，すなわち，主要カテゴリからなっている。

① 分割の程度：多数ユーザ対単一ユーザ

② サービスのタイプ：インタラクティブ対バッチ

③ 編成組織：分散対集中

④ ユーザ・アクセス：リモート対ローカル

⑤ アプリケーション：多目的対専用

コントロール技法チェックリストも同様に3つのカテゴリからできている。すなわち，物理面，システム面，管理面である。物理的コントロールは伝統的な"システムを金庫室へ入れる"方法で，周辺コントロール，危険防止，および支援機構を含む。システム・コントロールはハードウェア／ソフトウェア，アクセス・

コントロール技術，プログラム保全方法，監査証跡技術，および故障応答手続からなり，管理コントロール技術は通常は変更コントロール手続と呼ばれているものから成っている。それぞれのコントロール技法はアクセス・コントロール，精度，および可用性の各要素に対して評価する必要があり，それらの各要素に対して総合スコアを出す必要がある。

4.2 ガイドブック

ここに述べる方法論の重要な要素は，チェックリストを支援するバックグラウンドとなる資料である。このガイドラインは2つの部分からなる。第1は，環境チェックリストとコントロール技法チェックリストの要素の個々の解説であり，後者は，各項目についての保護費用の範囲が与えられる。特定の環境要素が指定された場合，ある範囲のコントロール技法が適用できるようにするためには，環境チェックリストはコントロール技法チェックリストと相互参照できることが必要である。

またガイドブックでは，コントロール技法間の相互関係を扱わなければならない。これによって，設計者も監査人も，あるコントロール技法を採用した場合この技法によって他のコントロール技法が不要になるかどうかの決定を下すことが可能でなければならない。たとえば，もし十分な物理面のコントロール方法がとられ，しかもシステムに関係する全員がシステム情報に対して同等のアクセスを許されているものとすると，内部的なソフトウェアによるアクセス・コントロールへの依頼度は相当ゆるいものでよいことになる。この評価のためのガイドラインは，技術の状態に対しては非常に敏感で，たえず更新する必要がある。とくに，特定形式の保護の費用と効果の関係はしばしば変更する必要があり，また新しい技法が開発され実行可能になり次第，とり入れることも必要である。

この総合的な方法論は，コンピュータのセキュリティ施設の監査という問題に対してのシステマチックなアプローチである。設計者も監査人も共に，システムが稼動する環境とその環境を実現するために使用されるべきコントロール技法の

完全なリストをもとに作業を行う。共通リストで仕事をすることによって，設計者と監査人はお互の評価の相違を容易に伝えることができ，これらを調整することも可能である。

このようなチェックリストはすでに数多く存在している。それらは，いずれも環境チェックリストとコントロール技法チェックリストの基礎の形成に使用されている。

個々の解説と要素の相互関係を示す完全で正確なガイドブックの作成がこれから完成するこの総合的な方法論の重大な要素になる。例として下記を参照されたい。

Data Processing Security Evaluation Guidelines：Peat, Marwick, and Mitchell & Co.，Certified Public Accountants；345Park Avenue, New York NY 10022.

5．ガイドライン

ＰＡＲＴⅢにおいて，われわれは監査方法論とここに取上げられているその監査機能の実行に先立ち，監査人が従うべき一連のステップについて述べた。したがって，本章の目的は，監査人が各種のシステム環境におけるデータ・セキュリティを比較，測定する対象になる＂理想＂を構成する考察について検討することである。

＂理想＂は①監査人がその仕事に使用する情報と経験，②監査対象のシステムをより完全に理解するため自ら努力して収集した情報と観察を含む諸種のソースから造成されるものである。

本章は，監査の実際のガイドブックを作るのが目的ではなく，そのような参考資料は数種のものが既に存在している。さらに，この研究集会に許されている僅かの時間では，そのような（徹底的な）努力をすることは許されない。しかしながら，付録に添付した図にみられるように，一部のさらに特定的なセキュリティ

手段（選定された場合）だけではなく，コントロール技法の重要なカテゴリを識別しようとする努力は試みられた。関連作業に含まれる材料の活用（や監査人自身の知識と経験）によってコントロール技法のカテゴリでは種々の取捨選択が拡大展開できるが，ここでは選定システム環境例題間の相違の分析の機会も持てる主流的なセキュリティ・オプション（一般的に）を反映するコントロール技法のカテゴリを選択している。

われわれの検討の結果，理論的には，物理面，管理面，およびシステム設計面からの見解の組合せによってはたくさんのシステム環境が可能であることが明瞭である。このグループに与えられた任務に答えるため，われわれは，お互に重要な相違点をもちながら，かつ今日のコンピュータ処理環境で存在する最も普及している4種類のシステム例題を選定した。

これらの4つの例題システムの各々の環境の説明は付録に記載されている。"環境"の構成要素を確認する方法はＰＡＲＴⅣの環境とコントロールで述べられており，この4例題システムに関する可能な保護手段としてわれわれが選定したコントロール技法の種類も同じ章に簡単に解説されている。しかしながら，われわれのグループは一歩進んで，3つのカテゴリのコントロール技法に主観的な数値（低0から高10）を割当ててみた。これらの数値は，例題システムの場合，そのようなコントロール技法が重要かどうかについてのグループの意見が一致したものである。この重要度のファクタは，われわれの定義による"セキュリティ監査"によってＡＡＡ（ＡＣ／Ａ／ＡＶ）基準：①アクセス・コントロール，②精度，③可用性が与えられた3つの基本的保護カテゴリの各々に対して考慮された。

特定のシステムの弱点を判定するに際して，監査人が利用する一般的なある種の監査的考察が存在することは明瞭であるが，これらは監査人が与えられた仕事を成功裡に完遂するために自ら持たなければならない経験的な事項である。

したがって，われわれが考慮したのは，4つの例題システムのある種の特定面だけであり，システムとシステムを特色別に区分するような方向でセキュリティ

考察に影響するものにハイライトが当てられた。セキュリティの完全な監査の際に，監査人はもっと遥かに広範囲に亘る分析を期待されるのは勿論であるが，グループに与えられた任務の目的は，監査人が特別の注意を払うべき異なるシステム環境下での特定な問題領域に焦点をしぼることであると考えている。著名な教科書の説明にあるようなもっと一般的なケースは読者への課題としたい。

6．結　論

コンピュータ・コントロールと監査の共著者であるウィリアムC．メイア氏は最近，"ＤＰ監査人は警察官ではなく，そうあることも出来ない"と語ったことがある。氏の言によれば，ＤＰ監査人の第１の責任は，適当に文書化されて連絡の要のある基準の必要性を強調するために，管理のアドバイザとして行動することである。基準はすべてをつくる根拠となるものであり，評価のための範囲，対処の仕方，基準を与えるものであって，これらの基準を介して監査人は，やがては基本的に対立する環境において遭遇する不利な効果の減少に役立つシステム・コントロールを設定する。事実，監査人はこれらのコントロールの一部分である。

リスクを受け入れ可能なレベルまで引き下げるためには，弱点部分が摘出されなければならない。ＥＤＰシステムが直面する危険性は，結局のところ間違った管理の決定であるが，横領，詐欺，資産の喪失，破壊，過大な費用，不十分な収入も含まれる。これらによる影響は甚大なものがあり，結果的には，競争上の不利益，法による強制，罰則，さらには経済的，政治的，軍事的な災害をももたらすことすらある。

われわれは"敵"の力や才能，しぶとさを過少評価してはならない。コントロールの開発を潜在的可能性の発覚，露見に結びつけるときは，むしろ単純志向のアプローチが必要である。われわれが考えることは，ほかの誰かもまた考えることができる。すなわち，監査人は巧みに詳細な基本的情報を収集し，システムの長所と弱点を評価し，その設計と性能をテストして，特定の目的のために設計さ

れた構造モデルに従って，その構成要素全部を個々に，そして集合的に審査しなければならない。

最終的にはいろいろなシステム環境で，コンピュータ・セキュリティ監査の最初の内部設計とフォローアップ（外部）の双方についての柔軟構造モデルが開発された。このモデルは，システムが定義の明確な（定義可能）環境内で実行可能であるためには，システムへのアクセス・コントロールが確実に維持され，正確なサービスが可能で，かつ，これらのサービスのユーザへのタイムリな可用性が確保しなければならないという概念にもとづいている。

監査の実施に際しては，すべての識別可能なシステム項目のアクセス・コントロール，精度，および可用性に関しての格づけのための標準ガイドラインの可用性は当然のことと考えられる。したがって，セキュリティ監査の総合的な測定は，各項目の個々の部分評価から得ることができる。"部分"評価を"総合"評価に変換する方法は数多く示されているが，しかしセキュリティ環境で受け入れられるのは設計仕様の評価と完全に一致しているときだけのように思われる。

要約すれば，あらゆるコンピュータ・セキュリティ監査の重要な要素は人間であり，したがって完璧なセキュリティを得るためにわれわれに許されることは，明白な選択つまりコンピュータを捨てるか人間を捨てるか……であるように思われる。

付属資料：４つの例題

提案された方法論の効果を判定するために，システム環境の諸々の面を網羅する４つの代表的タイプのシステムを部分的に分析して，その結果をここで検討する。

１．システムの選定

ここで選ばれた４つのシステム・タイプは，少くとも可能と思われるシステム環境の広いスペクトルの各カテゴリの１つの例を示すものである。

① 大学の計算センタ

② 航空会社の座席予約システム

③ 電子預金振替システム（ＥＦＴＳ）

④ 福祉小切手送達システム

各システムの目的／要求事項の検討が行われ，関係する制約や仮定が指示された。分析の進行につれて，さらに，システムの目的と制約についての仮定の説明の必要が生じた。たとえば，大学の計算センタは，厳密に教育への目的とノンセンシティブな研究にのみ使用され，ノンセンシティブな情報（たとえば，成績，給料支払いなど）と危険でないアプリケーション（たとえば，クラスのスケジューリング）がシステムの対象になるものと考えられた。同様に，航空会社の座席予約システムは非常な頻度で利用されるが，一定の〝リーズナブル〟な範囲までのエラーは許容されると仮定された。電子預金振替システムは，遠隔の金融機関や小売店などの１つの機能として，他地域との間で預金を振替えるために，それらの個々のプロセッサを暗号化して保護された回線で結合された１つのネットワークであるとされた。福祉小切手送達システムは，法人の給料支払いの専用シス

テムに非常によく似た大型の専用資金支払いシステムの代表例であると考えられた。また，入力は磁気テープに記録し，チェックのためのランは月一回と仮定された。

2．環境の決定

2.1　物理面

監査の範囲に入るべき物理的環境の代表的問題として2つの要素，すなわちシステムの設置場所と処理の継続性が選ばれた。

2.2　システム

システム環境がこの研究の主要焦点であった。考慮されるべきシステムの5つの面はつぎのとおりである。

- 分割の程度（単一または多数ユーザ）
- サービスのタイプ（バッチあるいはインタラクティブ）
- システム構成（集中または分散）
- ユーザ・アクセス（ローカルあるいはリモート）
- アプリケーション・ミックス（単一専用，あるいは多重）

先に示したように，4つの選択システムはシステム環境の各面を少くとも一度は一斉に求められる。

2.3　管理面

管理的環境要素の2つの代表的な領域がここでは考慮された。すなわち，システムの敏感性とシステムの仮定された恐威である。

分析する要素を選定してから，研究会のメンバはこれらを一諸に検討して，4つのシステムの各々との一致する密接な関係を決定した。明らかに実際の監査では，もっと多くの環境要素を考慮する必要がある。標準としては，あらゆるセキュリ

ティ関係の要素から考慮すべき適切な要素が選定される。

3．コントロール技法の識別

各システムに対して，環境要素のサンプルを設定した後，コントロール技法の代表サンプルをグループ一致で開発した。ここでも再び徹底的なリストを使って作業は代表的に行われた。そして，各カテゴリ（物理面，システム面，および管理面）に対する数種の技法が評価のために選定された。

3.1　物理面

- 周辺コントロール ― これは人間と"物"の両方をベースにした合成（この例では）になろう。周辺コントロールの種々の"層"が考慮されよう（場所，建物，室，壁の厚さ，ドア，施錠，囲い，その他），および種々の面（ダクト，フィルタ，火災防止，空調，ＴＶモニタ，ガード，その他）。
- 支援地区 ― 場所，セキュリティ，可用性など。
- 処分コントロール ― 出力のコントロールや細裂など。
- 通信保護 ― リンク・バイ・リンクの暗号化，遮蔽導線など。

3.2　システム

- 内部アクセス・コントロール ― 識別／証明，アクセスの承認，実施方式などのためのハードウェア／ソフトウェア・コントロール。
- プログラム保全方法 ― 自己チェック，正確性，信頼性などのコントロール。
- エラー検出／訂正 ― 周期的リダンダンシィ・チェック，リダンダンシィ，モニタ，自己テストなど。
- 監査証跡
- 故障応答 ― ソフトウェアとハードウェア。
- 通信連絡 ― エンド・ツー・エンド暗号化方式。

3.3　管理面

- 周辺アクセス手続
- 保守手続 ― ソフトウェアとハードウェア。
- 支援手続 ― オフラインとオンライン。
- 人事手続 ― 訓練，教化，契約，その他。
- 開発手続 ― 基準，コンフィギュレーション管理，承認，その他。

4．コントロール分析

コントロール技法のサンプルの例挙に続いて，各システムを0（皆無）から10（最大）のスケールで評価した。おのおのの評価には3つの基準が使用された。その環境でのコントロールが下記に関しての保護を果した相対的な程度である。

システムへのアクセス・コントロール

システムの精度

システムの可用性

各項目の検討には全メンバが参加し，ここに示す結果は全体の意見が一致したものである。一部の結果は実際のシステムの印象を反映しているが，他のものは可能性のある"設計目的"を反映している。以下の数字は，われわれのサンプル分析の結果を示すものである。

5．総合評価

つぎのステップは，システムが可用性，精度，およびアクセス・コントロールに関する保護の程度についての総合的な評価を引き出すことと，それをシステム管理者が決定したセキュリティの目的と比較してみることである。この比較には，各種のコントロール間のトレード・オフの分析も含めなければならない（すなわち，物理的コントロールが良い場合は，システム・コントロールをゆるやかにで

きるし，あるいはこの逆になることもあり得る）。また同時に，＂最も弱い部分＂の評価も必要である。このための満足すべき技法が，今後，開発されなければならない。

われわれに奨められるアプローチは，各々のコントロール技法の項目に評価される特定のシステム環境の１つの関数としての＂範囲＂または＂最大限＂のパラメータ的な値を準備することである。これらの評価値をサブシステムによって集積して，それらの評価用の評価値を作成する。たとえば，サブシステムに受入れられる評価値をこのサブシステムの項目を構成する全パラメータ・セットから選択される最高の数値パラメータとすることもできる。概念的には，（最低の）項目のレベルに対しては十分なミクロなコントロール・レベルのすべてを上位サブシステム・レベルのマクロなパラメータに変形し終えるまで，この集成処理を段階的に続けることができる。この予備的な調査段階においてすら考えられることは，システム・セキュリティのための＂標準＂尺度は結局ここで定義されたような未完成なことを手始めに展開されてゆくものであるということである。

例題1

汎用・多数ユーザ用　プログラミング・システム(例：大学計算センタ)

	環境	コントロール	評価*
物理面	場所：大学構内 存続性：低	周辺コントロール 支援地区 処分コントロール 通信保護	2／－／2 －／0／0 0／－／－ 0／－／0
システム面	分割の程度：多数ユーザ サービスのタイプ：インタラクティブ システムの構成：集中式 ユーザ・アクセス：リモート アプリケーション・ミックス：多重	内部アクセス・コントロール プログラム保全方法 エラー検出／訂正 監査証跡 故障応答 通信保護	2／－／－ －／0／－ －／0／－ 0／0／－ －／4／4 0／－／0
管理面	タイプ：ノンセンシティブ 脅威：サービス拒否 サービスの盗用 騙し ローカル	周辺アクセス手続 保守アクセス手続 支援手続 人事手続 開発手続	2／－／2 2／2／4 －／－／0 1／1／1 2／2／4

＊
アクセス・コントロール／精度／可用性

例題 2

専用データベース・マネジメント・システム（例：航空会社座席予約システム）

	環境	コントロール	評価*
物理面	場所：多重 存続性：高	周辺コントロール 支援地区 処分コントロール 通信保護	5／－／5 －／3／7 4／－／－ 0／－／6
システム面	分割の程度：多数ユーザ サービスのタイプ：インタラクティブ システム構成：分散方式 ユーザ・アクセス：リモート アプリケーション・ミックス：専用	内部アクセス・コントロール プログラム保全方法 エラー検出／訂正 監査証跡 故障応答 通信保護	7／－／4 －／7／－ －／5／－ 1／6／－ －／4／8 0／－／0
管理面	タイプ：センシティブ 脅威：サービス拒否 データの不認可露見 リモート	周辺アクセス手続 保守アクセス手続 支援手続 人事手続 開発手続	4／－／4 6／6／8 －／－／8 2／8／5 4／7／9

＊アクセス・コントロール／精度／可用性

例題 3

分散型多数ユーザ・リモート・アクセス（例：ＥＦＴＳ）

	環　　境	コントロール	評　価＊
物理面	場所：多重 存続性：高 特殊：暗号通信	周辺コントロール 支援地区 処分コントロール 通信保護	6／－／7 6／3／6 5／－／－ 9／－／7
システム面	分割の程度：多数ユーザ サービスのタイプ：インタラクティブ システム構成：分散方式 ユーザ・アクセス：リモート アプリケーション・ミックス：多重	内部アクセス・コントロール プログラム保全方法 エラー検出／訂正 監査証跡 故障応答 通信保護	9／－／5 －／8／－ －／8／－ 8／8／－ 8／8／4 8／－／3
管理面	タイプ：ハイ・センシティブ 脅威：誤用 サービス拒否 リモート	周辺アクセス手続 保守アクセス手続 支援手続 人事手続 開発手続	8／－／8 8／8／6 6／3／7 8／9／7 8／9／7

＊アクセス・コントロール／精度／可用性

例題 4

専用バッチ ― 支払い（例：福祉システム）

	環　　境	コントロール	評　価*
物理面	場所：単一場所 存続性：中	周辺コントロール 支援地区 処分コントロール 通信保護	4／－／4 －／－／5 5／－／－ 0／－／0
システム面	分割の程度：単独ユーザ サービスのタイプ：バッチ システム構成：集中方式 ユーザ・アクセス：ローカル アプリケーション・ミックス：単一	内部アクセス・コントロール プログラム保全方法 エラー検出／訂正 監査証跡 故障応答 通信保護	0／－／－ －／5／－ －／8／－ 0／8／－ －／0／0 0／－／0
管理面	タイプ：センシティブ 脅威：誤用 ローカル	周辺アクセス手続 保守アクセス手続 支援手続 人事手続 開発手続	4／－／4 3／5／3 －／－／5 3／6／3 3／8／3

＊ アクセス・コント ロール／精度／可用性

昭和53年5月発行

発行所　財団法人　日本情報処理開発協会
東京都港区芝公園3丁目5番8号
機械振興会館内
TEL（434）8211（代表）

印刷所　三協印刷株式会社
東京都渋谷区渋谷3丁目11番11号
TEL（407）7316

52－R007