「システム監査の実態とその推進」別冊資料

コンピュータ・セキュリティの
監　査　と　評　価

昭 和 54 年 3 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53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。

コンピュータ・セキュリティの監査と評価

目　　次

コンピュータ・セキュリティの

監査と評価

本資料は，米国商務省標準局が1977年にとりまとめたAudit and Evaluation of Computer Securityの全訳です。

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。

PART I 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。

PART Ⅱ　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，エグゼクティブ・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.

PART V 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，異常な環境でない限りは，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）

（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

－一監督なしの取消

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

PART Ⅶ 管理的・物理的コントロール

議　長　William Hugh Murray

ＩＢＭ

参加者　W. Gregory McCormack Ⅱ

ウエスターン・サウザーン・ライフ

Eldred Nelson

ＴＲＷシステムズ・グループ

Kenneth T. Orr

ラングストン・キッチ・アソシェィツ

Susan K. Reed（記録係）

米国標準局

Barry Wilkins

ＩＢＭ

編集者注

議長の経歴紹介

ウイリアム　H. マレイ氏は，ＩＢＭ社ＤＰＤ（データ処理ディビジョン）のデータ・セキュリティ・サポート・プログラム部門のマーケティング・サポート担当上級管理者である。彼は以前，ＩＢＭ社の拡張管理システム(Advanced Administrative System)向けのセキュリティ・サブシステム開発を統轄していた。また彼は，５巻構成のデータ・セキュリティに関する教育用ビデオテープ「データ・セキュリティ・コントロールおよびその手順」の著者であり，「コンピュータ環境における物理的セキュリティの考察」のような他の幾つかのＩＢＭ社刊行物にも寄稿している。そしてデータ・セキュリティをテーマとして数々の講演も行っており，ＡＩＣＰＡ，ＥＤＰ監査人協会，ＩＮＦＯ76，Data Comm77 等

の全国規模の催しに登場している。米国ではＳＨＡＲＥ（ＩＢＭ科学計算ユーザ・グループ）やＧＵＩＤＥ（ＩＢＭ商業計算ユーザ・グループ）の前に姿を現わすかと思えば，欧州でのDiebold Researchプログラムにも参画した。1974年，ＮＢＳ／ＡＣＭのワーク・ショップ「共有リソース・コンピュータ・システムにおける統御されたアクセシビリティに関する研究集会」の監査作業グループで議長を努めた。彼はルイジアナ州を大学から経営管理の学士号をうけている。

このセッションに与えられた任務は，次の通りである。

管理的・物理的コントロール。偶発事故対策プランニング等を含むＡＤＰ環境下の管理的・物理的コントロールを評価する監査アプローチおよび技法とはどういうものであるか。

管理的コントロールは，以下に説明する如く手続と要員両面のセキュリティを含むものとして定義される。手続面のセキュリティ ― 重要データの保護でその許容レベルを提示するため確立される経営上の制約，運用手順，責任能力（アカウンタビリティ）手順，補助的コントロール。要員面のセキュリティ ― 何らかの重要データに接触し得る全要員が，全てのチェックを済ませその上所要資格を持っていることを保証するために確立される手順。

物理的コントロールには，コンピュータ，関連機器および情報媒体へのアクセスをコントロールするためのロック，ガード，バッジならびに同種の管理手段の利用が含まれる。さらに，このコントロールには，コンピュータや関連機器およびその内容物を収容する構造物を，偶発事故，火災，環境異変等から保護に必要な手段も含まれる。

本セッションは，従来文献で余り取り扱かわれていない分野に重点を置きつつ，管理的・物理的コントロールを評価する監査アプローチおよび技法を対象としている。このセッションの出発点としてＦＩＰＳ・ＰＵＢ31を利用してもらうと良い。

本論稿は，作業グループの合意に基づき作成されたレポートである。

管理的・物理的コントロールに関する
作業グループ・レポート
コンセンサス・レポート

ウイリアム H. マレイ
バリー　ウイルキンス

1. 任　務　の　検　討

コンピュータ・セキュリティの監査および評価に関する招待研究集会は，「コンピュータ・セキュリティの監査問題に対する真の解決策を展開させるために」召集された。現在，テクノロジーは，「問題のない問題」や「疑似的問題」に余りにも囲まれているので，本作業グループは，「真の問題に真の解決を」与えられる指示にのみ焦点を絞ることを決意し作業にかかった。

本作業グループは，管理的コントロールの評価に対する監査アプローチおよび技法と，このようなコントロールのセキュリティへの貢献に関心を置くよう求められた。また文献類で余り触れられていないテーマを含む分野に重点を置き，既に触れている文献については適切であるかどうかコメントするよう要請された。このレポートでは，こうした任務に応えるべく，われわれが取り組んだ文脈あるいは環境を再検討してみようと思う。任務の対象となったものとしては，伝統的な監査人の役割およびセキュリティとの関連性等の例があげられる。グループ内でまず合意をみたのは，この領域で数多くの問題が存在しているという認識であり，こうした問題の輪郭を明らかにすることから着手した。問題の中の幾つかは，監査人のためのそれであり，こうした問題に反応する上で監査人にとって有意義であるとの示唆を提起するよう努めた。またその他の問題は，習慣の範疇に属するものであったり，文献やテクノロジーの前途に関するものであったりした。これらは，より広汎なデータ処理界の人々により取り扱われるべき性質のものである。われわれは，こうして論点を明確にし幾つかの勧告をまとめ上げるべく協力した。

2．監査人とコンピュータ・セキュリティ

監査人の責任とは，従来次のような事柄を含むものと考えられている。

1) 組織の資産を保護すること

2) 政策との密着性を保証すること

3) コントロールおよび手順の充実度を保証すること

3．問　　題　　点

われわれが取り組むべき領域には実に沢山の問題が転っており，このレポートでは，それらに対する解決となり得るような示唆並びに勧告を提起することに意見の一致をみた。

グループのあるメンバーによって，コンピュータ・セキュリティの監査の分野で，監査人達は二元論的でかつ絶対的なセキュリティの定義に悩まされることが指摘された。このような定義は，あるコントロールの存在が常に良いなら，それが存在しないことは必然的に悪いという結論を導き出してしまう可能性が強い。本グループ内では，組織というものは極めてしばしば，明確なセキュリティ政策を持たないだけでなく，セキュリティ責任の明確な所存をも決定していないことがあるというコンセンサスを得た。この場合には，監査人は，よい実施慣例の基準に従って監査するかも知れないが，良き慣例の集積は，その組織によって採用され得る特定の方法の集積より大きいのが普通であり，かえって余分なリソースを費消するとともに効率面でもロスを生じている可能性が強い。

グループの経験から言えば，良い実施慣例の基準と調和させることによって，監査人は次のような様々な問題に直面することが多いであろう。

① 良い実施慣例の基準を文書により証明することは，監査人の目的からは不充分かあるいは無用である。例えば，「コンピュータ・コントロール・ガイドライン」[注1)]は，良い実施例の一般基準を裏付けているが，セキュリティに関してはほ

とんど詳細に述べていない。他方，「ＦＩＰＳ31」[注2]は，セキュリティに特化したものであるが，これは経営者を対象としたもので，監査人に向けたものではない。

② 監査人は，実際的な業務と良き慣例との間に横たわる予盾に気づくことが多いであろう。この種の不一致に直面した時，監査を受ける側は，「誰にも独特な流儀がある」といって，自らの正しさを前面に追し出そうとするはずである。データ処理における標準的な慣行は，伝統的な良い実施慣例の標準に適合したものというより，むしろ初期のデータ処理システムに適した慣行の反映であることの方が多い。データ処理の管理者層は，しばしばユーザに適した良き慣例の厳密な基準が自分達にもあてはまるという事実を認めたがらない。この「基準」と「良き」慣例との間にみられる不一致は，システム開発の領域において特に顕著である。たとえ相違が大きく，問題が重要なものであっても，まず重要なのは，監査人が何も良い方法はないと信じ込んでしまっている点である。

さらに，監査人が，セキュリティ手順の監査に効果的な焦点を定める時間を十分に持っていないという現状についても，グループで意見の一致をみた。この問題は，部分的には，チェックリスト自体の名辞的問題にかかずらわっている文献に帰因している。セキュリティの二元論的定義のように，こうしたチェックリストは，コントロールの存在が常に良くて，その不在が必然的に悪であることを示唆しがちである。それらは，保護されるべきリソースの価値に適切なウェイトを与えることができず，その価値の欠落した結果にも正しい判断を下せない。こうしたリソースがさらされる可能性のある異変や，その推定発生率，システムの利用法やそのシステムに係わるアプリケーション等にも目が行き届かないだろう。

最後に作業グループは，監査人の報告書は，しばしば経営陣の認可を受けられず，そしてその成果に見合う評価も受けていないという結論に達した。上述して来た項目に加えて，こうした現象を起こしている幾つかの理由を次のようにまとめてみた。

① 監査報告書は，適用されている基準について論じていない。会計監査の基

準は，「一般的に受容し得る」ものとして存在し，明確に説明される必要はない。しかしながら，セキュリティの監査においては，「一般的に受容し得る」基準などは存在しない。したがって，適用されている基準やそれにまつわる権限は，明快に規定され言及される必要がある。

② 監査報告書は，見出された一致のレベルに対し正当なウエイトと評価を与えていない。報告書は総じて，一致のレベルについては1節程度言及してすませ，不一致の部分に数ページをさいている傾向が強い。

本作業グループは，監査人がその能率と効果を向上させる上で有効だと認識してほしい示唆をかなり多く具体化した。

4．監査人への示唆

指摘を受けた問題点に即して，グループは，監査の焦点と具体性，実施の基準およびそのドキュメンテーション，セキュリティ監査レポート，監査の領域と技法等についての提言をまとめた。最初の3つの分野は，本章でとりあげているが，最後の領域と技法については，5～10章に分散して説明した。

4.1 監査の焦点と具体性

監査人の効力を最大限発揮させるため，本グループは，完全なセキュリティが生産性ゼロに等しいとの前提に立って，監査人がどのようなセキュリティの定義にもとづこうと「リスクの許容し得るレベル」の概念を導入するよう勧告した。この概念のもとでは，保護手段の全てを採用することよりも，むしろそれらの中から選択的に採用することが許容されている。ある特定の手段が導入されていなくとも，リスクの許容し得るレベルを保持していれば，経営陣はその手段の無いことに対し非難される必要はない。

つぎに作業グループの見解が一致したのは，システムの鋭敏さを決定する最重要な唯一の要因は，そのシステムのアプリケーション即ち利用法であるという点

である。この観点からわれわれは，あるシステムのセキュリティを判断する上で有用な視点は，アプリケーションによって異なるという点を指摘したい。具体性を極大化する最も効果的な方法は，より鋭敏なアプリケーションに集中することである。 Ⅶ－1表はこうしたタイプの幾つかをリストアップしたものである。

Ⅶ－1表 アプリケーションの鋭敏さを表示する基準

- 他のアプリケーションの開発またはコントロール（例，プログラム開発システム，セキュリティ・サブシステム）
- 小切手の記入（例，給与支払，支払勘定，配当金）
- 信用の設定（例，受取勘定）
- 改変し得るリソースのコントロール（例，在庫管理）
- 従業員，資産あるいはその他の極めて重要な事項に関するデータのコントロールまたは包含
- サービスの提供またはオペレーションの継続に不可欠なデータのコントロールまたは包含
- その他

会計監査の場合同様，セキュリティの監査においても，監査のための具体的なアプリケーションを明確にするには，「Sutton テスト」が有効である。彼が何故銀行を襲うのかと尋ねられた時，Willie Sutton は，「そこは金がある場所だから」と答えた。つまり，Sutton テストの示すところを援用すれば，セキュリティ監査人は，その範囲内に非常に貴重なデータを含むか，あるいは貴重なリソースを随伴させているアプリケーションに注意を集中させるべきである。

4.2 実施基準とそのドキュメンテーション

5種類の刊行物が作業グループのメンバーにより引用され，セキュリティ監査人に極めて有用であるとの評価を受けた。それらは以下に示す通りである。

① コンピュータ・コントロール・ガイドライン

② コンピュータ監査ガイドライン

③ ＡＤＰの物理的セキュリティおよびリスク管理のためのガイドライン

④ データ・セキュリティのコントロールおよびその手順

⑤ コントロール目標

「コンピュータ・コントロール・ガイドライン」と「コンピュー監査ガイドライン」は，データ処理の良き運用基準とその効果的監査について，最も明確なそして最も権威あるものとして認められた。これらは，監査人のために監査人の手により上梓されたもので，構成といい使い易さといい申し分ない。その取扱かう領域はセキュリティだけにとどまらず，セキュリティにも適用し得る実施例やテストも含まれている。

「ＡＤＰの物理的セキュリティおよびリスク管理のためのガイドライン」は，物理的セキュリティに良い実施基準をもたらす好適資料として引用された。この刊行書は，特別な尺度が必要であるか否かを決定する際役立つ，自然現象の発生率に関するデータも提供している。内容は包括的でしかもきちんと書かれてあるので，経営者にも有益である。このマニュアルの徹底的研究により監査人は多大の恩恵を享受できるはずである。

「データ・セキュリティのコントロールおよびその手順」は，データ処理の限定的リスクに対する実施基準の良い素材として推薦されている。このマニュアルはまた，偶発事故対策プランニングとセキュリティのためのシステム設計も取扱っている。経営管理者層を意図してまとめられたものだが，監査人にも勿論役立つものである。

最後の「コントロール目標」は，データ処理管理を成功裡に行う基準について説明したものである。とくに重点が置かれているのは，物理的セキュリティ向けの標準である。ＤＰ業務全般とセキュリティを中心としたオペレーション管理の監査に有効であるとの評価を得ている。この刊行物は，ＥＤＰ監査人自らの手でまとめられたものであるが，セキュリティ専門に監査を実施している監査人の場

合，部分的な引用にとどまるかも知れない。

4.3 セキュリティ監査報告書

コンピュータ・セキュリティの監査報告書のスタイルは，その効率に著しい影響を持つというのが，作業グループの結論である。作業グループは，以下の様なフォーマットが有効であると考えている。

実施概要（エグゼクティブ・サマリ）

目的

範囲

環境

結論

採用基準

実施されたテスト

一致レベル

注目すべき相違

勧告

その他のリスク

実施概要は上級管理者に提出されるべきものである。当該監査の領域について触れるとともに，どのようなアクションが必要であるかを読み手に判らせるような形で重要なテーマについての結果を知らせるものでなければならない。場合によっては，報告書全部を精読し，有効な修正活動をとる必要が生まれよう。また，被監査人に当該報告書を手わたし彼が検討しフォローアップする素材とするだけで事足りる場合もあろう。経営者は，取るべき行動を決定する際，このサマリに外のものを見る必要はないはずである。

監査報告書の提出先として主たる位置を占めるのは，被監査人とその管理者である。その監査により必要と判明する修正行動の大部分は，被監査人自身の手で実行されることになるからである。したがって報告書は彼に対して先ずあてたも

のでなければならない。被監査人が正当なそして第一義的な報告書の読者だという認識が定着すれば，被監査人に有用かつ受容し得るスタイルや内容が作り出されるはずである。

ＥＤＰセキュリティを確保するための「一般的にうけいれられる」基準というものは存在しないので，報告書は，採用した基準について必ず言及しなければならない。この場合，外部の採用基準だけでなく，当該組織の全政策，基準，ガイドライン等も勿論触れられる必要がある。外部の基準は，文書化されているかあるいは出所が明らかなはずである。外部の基準については全てその典拠が指摘されねばならない。

監査結果を適切に評価するためには，経営者は，まずその結果をもたらすに至った時間と努力について認識する必要がある。報告書にはまた，当該監査の実施様態，実行されたテストの価値，費やされたリソースについての記述が含まれねばならない。４人が４週間かけて行った監査は，当然１人が１週間使って行ったそれより高い信頼性を持つからである。セキュリティ監査において，「われわれが適当と判断したテスト」のような消極的な権利放棄ともとれる表現は使うべきでない。

一致（コンプライアンス）のレベルおよび性格については，詳細に記載される必要がある。これは経営陣が監査結果や勧告を適切に判断できるか否かに係わる基本的前提である。相違は，それだけを検討する場合よりも，むしろ見出された一致の総体的レベルの視点から検討される時により大きな威力を発揮する。報告書中で，こうした一致にしかるべきウェイトを置かないと，報告書の総合評価を減ずるだけでなく，その信頼性にも傷がつき被監査人の不必要な抵抗を生む結果をもたらすことにもなりかねない。

監査により発見された相違点や勧告が，こうした文脈のもとで報告書中に記載されたならば，高い評価をうける好結果に結びつくと信ずる。

しかしながら，報告書には，経営者が勧告を受け容れるか否かに拘らず，その他のリスクに関する記述も含まれねばならない。もし監査人がこうした残余リス

クの輪郭を明らかにし難いならば，勧告を再度検討し直した方が良いであろう。

5．監　査　の　タ　イ　プ

5.1　まえがき

データ処理セキュリティをレビューするための5種類の監査アプローチが以下に述べられている。この5つのアプローチは互いに独立したものであるが，5種類の区別の明らかなモジュールは，監査される環境に応じて，独立した監査としても，あるいは組み合せた形の監査としても利用できるものである。5つの監査アプローチは次の通りである。

システム開発および保守業務の監査

アプリケーション調査

インストレーション・セキュリティ調査

セキュリティ機能（データベース／通信環境）調査

折衷的試み

これらの監査アプローチは，とくに優先順を与えてこういうふうに列挙したものではない。各監査モジュールの相対的重要性は，監査されるべきＤＰ環境により決定されるだろう。監査スタッフは大抵利用できるリソースに制約を持っているので，レビューされるＤＰ組織やＤＰ施設の輪郭を把握する事前監査のステップに十分な時間を費すことが大切だろう。調査すべき環境が基本的に理解できていれば，どのモジュールを採用するか，監査範囲はどの程度のものか，重点を置くべき項目は何か等について決定が下しやすいはずである。

監査の対象分野，監査目的，監査アプローチ，推薦されたテストの対象となる領域等は，前述の5種類の監査アプローチごとに記してある。

5.2　チェックリスト／リファレンス

本論稿の意図は，各監査アプローチのチェックリストを提供することではない。

チェックリストを含む様々な主題分野に利用し得るリファレンスが数多く存在することがまず確認された。だが作業グループで合意をみたのは，単独のリファレンスとしては，カナダ勅許会計士協会発行の「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」が最良であるという点である。

また個別テーマに関する汎用リファレンスあるいはチェックリストは，調査を受ける環境に合せて作成しなければならない。この認は実に重要である。誰にも等しく適用できる回答や包括的ガイドは存在しない。

本論の目的は，チェックリストおよびその他のリファレンスにより補完し得る統合的なアプローチを提示することである。

5.3 アプローチ

これらの分野のセキュリティ監査にあたって，従来の全ての監査技術を最も有機的に構成したものがアプローチとならねばならない。また次のような技法に重点を置くことも重要である。

選択的保護 — 主要な協力対象となるリソースを区別し，それらのリソースが如何に保護されているかについて調査努力を集中する。

テスト — 実際的なテストを通じて検証手続や討議が可能な場合（例，コントロールレポートとの調和）

インタビュー — コンピュータ・オペレーション，プログラミング，ユーザ，セキュリティ，法的事項，要員問題等に係わる全ての従業員および経営管理者とのインタビューを行う。これは特筆すべき領域であり，十分なフォローアップ・テストによりサポートされたインタビュー技術は，短時間により多くの成果を生み出し得るので，監査を円滑に進めるには不可欠のものである。

技術的協力 — 他の組織或は他の職場からスタッフを選び，その専門的識見を見込んで当該監査のチームに組み込むことは，非常に効果的であり，かつ一般的に認知された方法である。ただ一つ注意しなければならないのは，監査人が常に責任を取る立場を明確にしなければならない点である。

これらはＤＰセキュリティの監査を実施する上で，グループが実に効果的だと感じたアプローチや技法の一部である。

6．システム開発および保守業務

6.1　関心の対象

現在監査界で論議の的になっているのは，監査人がシステム設計やシステム開発に首を突込むべきか否かということである。賛否両陣営のどちらもが意見の一致をみているのは，(1)セキュリティおよびコントロールの両観点から，新しいシステムやアプリケーションは適切に開発されねばならないという点につき多大の関心が現に存在し，(2)導入後の強化は非常に困難であり，しかも(3)監査人はこの重要な領域における責任を無視できなくなっているという諸点である。

大抵の場合，システムやアプリケーションに非常に堅固なセキュリティ・ルーチンを組み込むことが必要であるし，したがって，ＤＰセキュリティの全側面は設計段階で考慮されねばならない。もし適当なセキュリティが付与されなければ，そのプロジェクトは，より良いテクノロジーやコントロールが出現するまで頓座してしまうかも知れない。このことは極めて重要な監査項目である。もしセキュリティが設計段階で組み込まれていないなら，セキュリティの存在は無いということになってしまうかも知れない。

このような監査のアプローチは，現実的には，「システム設計論争」の両極端に代るべきものであり，内部監査人サイドの係わりを最少限に抑制する形となろう。また別ないい方をすれば，監査人が実際にシステム設計の内容に深く関わるというよりむしろ，システム開発プロセスをレビューできるアプローチだといえよう。意識的にシステム開発の内容に参画しないと決意している監査スタッフや，リソース上の制約故に（大組織の場合）全ての新しい開発プロジェクトに注意が行き届かない事実を自覚している監査スタッフには，こうしたアプローチはとくに有用である。

また，システム設計のマネジメント・プロセスをレビューすることが，監査人が参画している場合以外でもシステムに確かなコントロールが施されているのを検証する効果的な方法であるという点でも意見の一致をみた。

6.2 目　的

本監査の目的は，安全なシステムおよびアプリケーションだけが開発されているかを確認するため，現場の管理が確立手順に一致しているかどうか，あるいは明確な手順が用意されていない場合は現場の管理者が十分な基準と手順を確立・導入しているかどうかを判断することにある。こうした点検をする目的は，開発過程で必要とされるセキュリティの全側面が考慮され，そしてコントロールが確保されているか否かを判断することである。監査人は，開発サイクルでなされる全ての決定の一部として，当該セキュリティ課題が組み込まれていることに眼を光らせねばならない。

6.3 アプローチ

監査のアプローチとは，現場の要員および管理者にインタビューし，現行および最近完了したばかりの開発プロジェクトとその付属ドキュメンテーションを実地に検証し（サンプル調査），さらに手順との一致をテストすることである。また，もしこの種の手順が存在しない場合は，独自の判断およびシステム設計のため一般に実証済みの慣例にしたがい，危険にさらされる可能性があるか否かを判断することになる。

6.4 範　囲

6.4.1 設計基準

この種の性格を持つ監査は，まず全体的および局部的な設計基準の点検と，現場組織の手順と確立された企業基準との比較の2つをスタートさせて開始される。監査人が常に念頭に置かねばならないことは，非能率が指摘出来る場合，単に現

場の方針の改善にとどまらず，企業全体の基準にも改善が施されるべきことを勧告すべき立場にあることである。

監査のこの段階で，監査人は，企業の政策と現場の運用手順の十分性を知悉するようになろう。そして現場の運用手順を検討することによって，実際的な慣例がそこに反映されていることに気づくことも多いはずである。

もし管理者が，開発手順の明確化やセキュリティ・コントロールの責任所在を正式に指定することで十分な時間を費していないならば，よくコントロールされた安全な環境，あるいは製品は望むべくもないだろう。

設計基準には，セキュリティ監査のテーマとなる以下の全ての領域における物理的，管理的，そして技術的コントロールが考慮されねばならない。

組織的コントロール

アクセス・コントロール

段階的調査（フェーズ・レビュー）

テスティング／システムの保証

プロモーション・プロセス

ドキュメンテーション

監査人／独立団体の関与

構成マネジメント

緊急対策手順

監査人はこうした全ての領域における手順の十分性を判断すべきである。監査作業の残る部分は，確定した，あるいは勧告された手順が開発サイクルに導入された時，その手順との一致をテストすることに費されるだろう。

6.4.2　組織的コントロール

全てのコントロールの基礎は組織である。監査人は，当該組織がよいセキュリティ・コントロールや，充実した開発業務の延長線上にあるか否かを判断して，その組織を評価しなければならない。雇用活動，任務分担，マンパワー・リソース，熟練者の配置および要員訓練等は，本監査で点検されるべき課題である。監

査のこの部門では，監査人は，利用機能，プログラミングおよびコンピュータ・オペレーションの責任と義務が明確に定義・区分されているかを検証しなければならない。また，マンパワーが主要コントロール機能に適切に充当されているか，これらの機能が必要とされる専門的知識に裏打ちされたものであるから，さらに，従業員は十分な現場教育を与えられているか等の問題についても判断を下さねばならない。

監査人は，組織的コントロールの各テーマが開発サイクルの中で十分に消化されつつあるかを評価することも大事である。

6.4.3　アクセス・コントロール

所有する全てのＤＰリソースへのアクセスを認容されるのは，絶対的必要性を備えた要員だけに限定されるべきであり，これを保証するのは監査の中心的課題の一つである。この領域でのコントロールが欠如すると，専有データが不正なアクセスにさらされ，コンピュータ詐欺，データ・インテグリティやドキュメンテーションの弱体化等が生起することにもなる。

以下のようなＤＰリソースへのアクセスを制約するため，管理的・物理的コントロールが点検されねばならない。

施設（ファシリティ）

コンピュータ設備

ハードウェア

プログラム

ＪＣＬ

データ

出力レポート

全てのＤＰ媒体

監査人は，補足的なアクセスまたは他のコントロールを，必要に応じて開発時に導入出来るよう，システム設計にアクセス・コントロールが考慮されるのを保証しなければならない。

監査人はまた，ＤＰリソースへの従業員の実際のアクセスを管理者作成の有資格要員リストと対比させる方法で，アクセス・コントロール手順をテストする必要がある。管理者が有資格者リストを絶対的な必要性のある人物だけに局限しているか否かも判断しなければならないだろう。

6.4.4　段階的調査／プロジェクト・コントロール

管理者がシステム設計全体に行き届いたコントロールを定着させたいならば，正式の，詳細なドキュメント化された段階調査の手順が必要となる。このフェーズ・レビューは，上級管理者にプロジェクト現況の情報を提供する有力な手段である。このレビュー・サイクルを通して，開発関連のデリケートな問題が存在する地点に，有効なチェックポイントを設定することが出来る。

セキュリティ・コントロールは，様々な理由から，段階的調査中にしばしば見落される重要な問題の一つである。

セキュリティの観点から，監査人は，段階的調査のプロセスを点検し，セキュリティが全開発プロジェクトの不可欠部分として配慮されているかどうか確認しなければならない。回答を必要とする質問が多いはずである。たとえば，セキュリティ部門が関係しているか？，ＤＰセキュリティの調整担当者が加わっているか？，ユーザはセキュリティとの関連を持っているか？，セキュリティ・システムはテストされたか？……

監査人が注目すべき主なポイントは，全開発サイクルの初期段階で，セキュリティ政策と文書化プランが確立され承認を受けているか，またそのプランの達成度が開発サイクル中監視されているかという２点である。セキュリティが軽く取扱われていない状態を実体化するため，十分なドキュメンテーションが必要とされるはずだ。管理者の参与およびアプローチは，文書で明確にしておかねばならない。

6.4.5　テスティング／システムの保証

監査人は，当該システム用に設定された全てのセキュリティ・コントロールが，広範囲にテストされるよう持っていかねばならない。包括的なテスト・プランお

よび文書化された結果，この2つが検討に供される必要がある。セキュリティは，テスト・プランの中で識別し得るカテゴリとして存在しなければならない。

また，テスト・サイクル中，もし適切な管理的・物理的コントロールが，生データへのアクセスをコントロールするため適正配置されていないならば，セキュリティ面の破綻が生じることもある。監査人は，最も極端な環境下以外で生のデータが使用されないよう，そしてもし使用されるなら誤った使用を防止出来るコントロールを設定するよう保証しなければならない。

6.4.6　プロモーション・プロセス

プロモーション・プロセスは，一つのプログラムをテスト状態から稼働態勢に移行させるプロセスのことである。うまくコントロールされた環境においては，コンピュータ・オペレーションは全ての稼働プログラム，ＪＣＬおよび付随するドキュメンテーションの所有権を維持し，プログラミング機能は，プログラムがテスト下にある間そのコントロールを維持する。それ故，あるプログラムをプロモートすることは，コントロールをプログラミング機能からオペレーション機能に移行させることを意味する。

このプロセスの間に，プログラム自体のセキュリティを確保する多くの有効な管理的・手続的コントロールが設定でき，しかもセキュリティはプログラムに組み込まれる。以下に列挙したのは，監査人が追求すべきコントロールの部分的なリストである。

- 機能要求および文書許可の利用
- プログラミング管理の承認／許可およびプログラマへの委任
- プログラムのオペレーション・リリースおよび権限に基づくドキュメンテーション
- エラーを検知しプログラマの不正行為を防止するための独立団体によるコードの再点検
- テストおよび開発業務とオペレーションの分離
- プロモーションの後，オペレーションによりコントロールされるドキュメン

テーション，プログラム，ＪＣＬ，データ等。

プロモーション・プロセスは，保守と開発のサイクルにおいて重要な部分を占めている。このプロセス中の手順とコントロールは，必ず検討されねばならない。

6.4.7　ドキュメンテーション

監査人は，しばしばまずいドキュメンテーションに出くわし，しかもドキュメンテーションは，監査人のためではなくプログラマのために書かれたものであることを知らされる。貧弱なドキュメンテーションは，機能，効率，安全性のどの側面においても劣り，その上，強化拡張が難しく理解や監査の対象とならないようなアプリケーションやシステムを生み出す。

劣悪なドキュメンテーションは，与える影響の範囲も大きく，監査人は決してこれを無視してはいけない。システムやアプリケーションの開発努力により作られたプロダクトには，問題点や必要性に応じた充実したドキュメントによる解決手段としての性格がなければならない。またプログラムやコード自体は，解決手段のごく一部ではあるが，その想定された読者，即ちマシンが，融通のきかないそして最も非妥協的なものであるだけに，最大の関心を呼ぶことがしばしばある。ある問題に対する文書化された解決策の想定読者としては，管理者，ユーザ，運用保守要員，マシン，監査人等が含まれる。

監査人は，その定義からも適切な読者である。それ故，監査人は，ドキュメンテーションを理解出来なければならないし，理解出来ぬ場合でも批評が下せるぐらいでなければならない。また監査人は，ドキュメンテーション基準が確かなものであることを保証し，かつ，ありきたりの貧弱な例をもはや受け容れてはならない。

監査人は常に，適切なドキュメンテーションの欠如を点検し非難する立場を堅持しなければならない。

6.4.8　監査人／独立の第三者の関与

重要かつ鋭敏な(センシティブ)プログラムやシステムは，独立した検証やチェックを受ける必要がある。もし監査人がシステム設計に直接関与していないなら，一定の

職能は独立の第三者に委ねられる。監査人は，システム設計時の独立の第三者の関与に注目しその十分性を点検しなければならない。

6.4.9　コンフィギュレーション・マネジメント

監査人は，あるシステムの特殊の統合やコピーに各コンポーネントのどのバージョンが含まれているかを統制する管理システムあるいは管理機構を見出すよう努力すべきだろう。このマネジメント・システムは，ある特殊の統合やコピーに対しコンポーネントのどのバージョンが含まれているかを決定し得る監査証跡を含まねばならない。またテストは，システムの存在，つまりアプリケーションの十分性を対象にして実施され，意図通り使用されているか，監査証跡が存在ししかも十分であるか等について確かめなければならない。また要望に応じて，監査証跡の内容は，システムの構成内容と対比される必要がある。

6.4.10　緊急対策手順

管理者は，異常事態に対応する必要がある場合，通常手順に代えて緊急手順を用いる柔軟性を保持しなければならない。この緊急手順は，管理機能を追加させることによって，臨時の柔軟な対応に付随するリスクを埋め合わせるはずである。確立されたコントロールの回避を防止するため，緊急事態でプログラムが苦境に陥った場合，手順並びに実際的活動を精査することは，システム開発監査の不可欠の要素である。

監査人は，あらゆる緊急時の苦境に際しても，以後ずっと同じコントロールを受け，しかも通常の更新がそれまでと同じコントロールを受けられるような手順を見い出すべく努力すべきである。

7．アプリケーション・レビュー

7.1　重要性

これまで実用化されて来た全てのアプリケーションには，持続的なセキュリティを具備するため管理，手順，システムの各面で重要なコントロールが適宜用意

されている。これらのコントロールの運用がまるでなかったり，あるいは不十分な場合，当然様々な外部からの脅威にさらされることになる。

7.2 目　的

アプリケーション・レビューは，特定のアプリケーションを対象としてデータ処理セキュリティのコントロールおよび手順を調査する導入後の分析を意味する。また，このレビューは，コンピュータを背景とするあらゆるアプリケーションに共通のデータ処理セキュリティのコントロールおよび手順とは，明らかに一線を画する。

レビューの目的は，当該アプリケーションが十分な内部セキュリティ・コントロールを備えた設計になっているか，そして，これらのコントロールが一貫性を持って運用管理されているかを調査し確認することである。

7.3 アプローチ

アプリケーション・レビューは，財務と営業両分野を対象とした全機能的監査の不可欠な要素として，内部の監査人により実施されるべきである。もし機能的分野にデータ処理に依存する部分がある場合は，当該機能の監査には，データ処理関連のコントロールに対するレビューも含まれねばならない。

ＤＰアプリケーションのレビュー抜きでは，完全な機能的分野の監査とは言い難い。両分野に対する総合的監査は同時に行われる必要がある。

7.4 対象領域

アプリケーション・レビューの対象とする領域には，つぎのような８種の分野があげられる。

入出力コントロール

システム内部コントロールの効率

任務分担

取扱いに慎重を要するプログラムの識別

ユーザの満足度／関与

レポートの活用

システム・ドキュメンテーション

重要レコード

各アプリケーションごとに，これら全ての項目があてはまる訳ではない。以下各分野の内容を要約すると次のようになる。

7.4.1　入出力コントロール

システムあるいはアプリケーションは，十分なコントロールを備え，許容されたものだけが一括して処理されるよう仕組まれていなければならない。処理対象は，それ以上でも以下であってもいけない。監査人は，コントロール技法が十分なものかどうか評価し，それらが適切に使用されているか判断する。

7.4.2　システム内部コントロールの効率

監査人は，内部の編集・監査ルーチンの十分性を評価・テストし，疑問視される，あるいは不適当な状況の発生を検知・予防しなければならない。

監査人は，システム・ドキュメンテーションを点検し,テスト・トランザクションを入力し，ユーザと質疑応答を交し，例外とコントロールに関するレポートを調査することによって，十分な内部コントロールが存在しているか否か判断しなければならない。ここで重要なことは，テストがどの時点でも行ない得ることである。

7.4.3　任務分担

どのようなアプリケーションにおいても，そのセキュリティが，通常ユーザにより実施される業務とプログラミングおよびオペレーションの両面の機能とに適切に分離されていなければ，確保できないことはいうまでもない。たとえば，ある買掛金アプリケーションでは，ユーザは当該アプリケーションのプログラムやその実行を行ってはならない。そしてプログラマは，生のデータの入力やマスター・ファイルへのアクセスを許容されてはならない。またオペレータは，コントロール・トータルを無理に調和させてはならない。この任務の分担については，

第8.4.2.2項に詳しく述べているので参照されたい。

7.4.4　取扱いに慎重を要するプログラムのコントロール

企業資産の構領を目的としてプログラム・コードを不正に操作するおそれのある場合，補足的なプログラム・コントロールが必要とされるかも知れない。補足的なコントロールの例としては，買掛金チェックライター・プログラムで生じたコーディング・ラインの変更だけを独立して調査することがあげられる。この種のレビューは，買掛金アプリケーション内部の他のプログラムに適用できるとは限らない。監査人は，あるアプリケーションの「取扱いに注意を要するプログラム」をまず判断し，それらが「選択的な保護」を受けられるように仕向ける必要がある。

7.4.5　ユーザの満足度／関与

監査実施中，ユーザが過去未解決であったセキュリティの不十分性に気づいているか否かを確認するため，彼等に質問が発せられねばならない。監査人は，ユーザがそのシステムを理解し，その変更にも熱意を持っているかどうか判断しなければならない。

7.4.6　レポートの活用

監査人は，プログラミング・ドキュメンテーションとは別に，そのシステムで利用できるコントロール・レポートを決定し，それらが利用されているかどうかを判断する。

7.4.7　システム・ドキュメンテーション

監査人は，ドキュメンテーションの十分性を点検し，建設的かつ現実的な示唆を行わねばならない。行き届いたドキュメンテーションが無い場合，そのシステムは，強化，理解，監査のどの面でも困難性を生ずる，監査人がドキュメンテーション標準との一致を強調することは重要なことである。ドキュメンテーションについての詳しい討議は，第6.4.7項を参照してほしい。

7.4.8　重要レコード

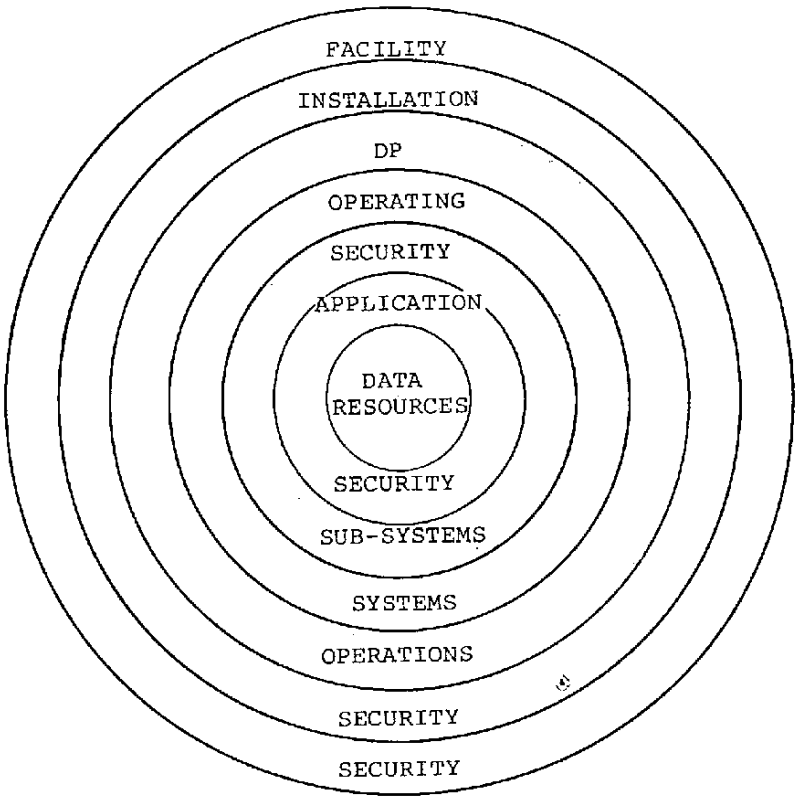
この部分の監査では，当該アプリケーションに特有のファイル，プログラム，

ブランク・フォームなどが，導入時の偶発事故対策プランに組み込まれているかどうかを吟味すべきである。

8．インストレーション・セキュリティ

8.1　重要性

ＤＰ環境で良いセキュリティ状態を維持するためには，そのセキュリティのレベルあるいはリング（Ⅶ－１図参照）に様々な段階があることを銘記すべきである。これらのどの分野においてもコントロールの弱い所があると，セキュリテ



Ⅶ－１図　セキュリティのレベル
Figure 2 System Levels of Security

ィの危機が招来する恐れが生じる。この監査の重要な視点には，①データの不正な修正あるいはアクセス，②データ処理リソースの無資格利用，③認定されたリソースの誤用があげられる。

8.2 目 的

この監査の目的は，調査対象となっている導入設備や組織のセキュリティ状況の評価を経営陣に提供するため，これら全てのレベルにおける管理的，システム的および物理的コントロールを精査することである。

8.3 アプローチ

1組織が何か所かに分散している時は，監査人はまず，最も脅威にさらされやすい導入設備なり組織なりを選定すべきである。監査の事前計画段階で，監査人は，対象とされるインストレーションを注意深く把握し，重要な監査領域を欠落させないようにするとともに，当該インストレーションに固有の技術面に見合った監査チームの選定をこころがけねばならない。可能な限り必要とされるＤＰ専門知識の豊かなメンバーが選ばれるべきである。このことは，単に監査作業を容易にするだけでなく，ＤＰ専門要員に対し貴重な教育的素地を提供することになる。監査アプローチは具体的には，従業員，管理者双方へのインタビュー，ドキュメンテーションの点検，インタビュー結果の正否を証明する詳細なテスト等で構成されるだろう。実際上のテストを抜きにして，インタビューだけを行うのでは不十分さは否めない。

8.4 対象領域

大規模なインストレーションにおけるＤＰインストレーションのセキュリティ調査領域は，非常に複雑に見えるかもしれないが，実質的には，4つの機能的監査技法に集約できる。

① 手順（プロセデュア）のレビュー

② 組織的コントロールのレビュー

③ アクセス・コントロールのレビュー

④ 偶発事故対策プランのレビュー

このように4分した意図は，全ての監査し得る領域を識別し，なおかつ文献でまだ十分定義されていない領域についても敷衍出来るようにするためである。

この監査領域をさらに分類すると次の様にまとめられる。

手順のレビュー

標準的運用（オペレーティング）手順

自己評価（性能及び結果）

組織的コントロール

責任

任務分担

雇用業務

作業ローテーション

休暇スケジュール

アクセス・コントロール

ＤＰリソース

空間（スペース）

媒体（メディア）

装置

プログラム

ドキュメンテーション

手順

保護技法

物理的セキュリティ，位置，設備

ＤＰインストレーション

分類体系

メディア・コントロール

ＤＰオペレーション

リモート・コンピューティング

大量データ伝送

プログラム・コントロール

暗号化

偶発事故対策プラン

緊急事態プラン

支援プラン

復旧プラン

重要レコード・プラン

8.4.1　手順のレビュー

インストレーション・セキュリティの点検は，まず，現場の手順と標準およびガイドラインとの調和から着手されるべきである。もし現場の手順が標準やガイドラインと一致しているならば，そのオペレーションが容認された慣行に合致している証拠とみなせるだろう。しかしながら，監査人はさらに，実際の業務と容認された慣例とを調和させねばならない。また，もし現場の手順が標準やガイドラインと一致していないならば，それは現場管理者がＤＰセキュリティに十分な配慮を下していない証左と考えられる。

監査人は，現場の運用手順を点検して，それらが十分なものであるか，またそれらが責任を明確に規定したものであるかの判断を下すべきである。加えて監査人は，ＤＰセキュリティをテーマとした自己評価を経営管理者に要請すべきである。もっとも関係管理者が，既に自己評価プランやそれに匹敵する検査プログラムに着手している場合も当然あると思う。

8.4.2　組織的コントロール

8.4.2.1　セキュリティ責任の所在

レビュー初期の段階で監査人は，全てのリソースの保護責任が明確に割り振りされているかどうかを判断しなければならない。そして各従業員は，彼が保有あ

るいは保管しているリソースの保護責任を指定されていて，それらのリソースに変動があればそれを指摘し，適切かつタイムリな修正行動をとれるような態勢でなければならない。リソースあるいはオペレーションの範囲や取扱上の微妙さに応じて，スタッフのセキュリティ責任は，指定される必要がある。

8.4.2.2　任務分担

任務の分担は，ＤＰとそのユーザとの間で行われなければならないし，そしてＤＰおよびそのユーザ内部でも明確にする必要がある。この分担のあり方として次のような事項に注意を払うべきである。①どの個人も，慎重な取扱いを要するリソース群にアクセスしない，②どの個人も，そのリソースの取扱いに失敗したり隠したりできる立場に置かれてはならない，③各個人の主要な行動は，割り当てられた仕事に専念している他の個人によりチェックされる，④各個人は，その行為に対して責を負っていると判断され得る状態にある。

監査人は，組織系統図，業績計画および適切な任務分担が実施されているか否かの判断材料となるその他の事項を調査すべきである。そして，その態勢が一貫して維持されているかを確認するため，監査証跡も点検する必要がある。

8.4.2.3　雇用業務，作業ローテーション，休暇スケジュール

これらに関連した組織的コントロールも点検されねばならない。ただ監査人にとって，こうした事柄は，馴れ親しんだものであるだけに，ＤＰ環境でもやはり重要性をもつという指摘をするにとどめる。

8.4.3　アクセス・コントロール

8.4.3.1　ＤＰリソース

現場あるいは設備，ＤＰ設備および全てのＤＰリソースへのアクセス・コントロールは調査されねばならない。具体的には，スペース，メディア，装置，ドキュメンテーション手順，プログラム等が含まれる。これらのリソースの一部については，そのアクセス・コントロール技法を個別に後で取りあげている。監査人はＤＰインストレーションの輪郭からどのようなＤＰリソースが重要であるかを判別し，そこに点検努力を集中する必要がある。アクセスの経過を記載したログ

やジャーナルは，責任の所在を明らかにする必要があるので，適切な場所に配置されねばならない。またこの種のログやジャーナルの内容が予想していたものと調和しているかどうかを判断するため適宜テストが重ねられるべきである。

8.4.3.2　保護技法

8.4.3.2.1　物理的セキュリティ，サイト，設備，ＤＰインストレーション

設備およびインストレーションに対するアクセス・コントロールは，まず最初に問題とすべき保護の２段階である。当該設備あるいはインストレーション内に仕事を有する要員だけが，正式のアクセスを許容される。他の全ての人々は，何らかの補則に合致した場合にのみ許される。監査人は，有資格者リストをもとに，実際のアクセスを点検すべきである。

8.4.3.2.2　分類体系

アクセス・コントロールおよびその他のＤＰセキュリティ・コントロールを維持するために重要な要件の一つに，取扱いに要注意のリソースを識別するシステム（体系）がある。リソースの相対的重要性を示す分類体系がないと，ＤＰセキュリティ計画に良いコスト効果を期待できない。監査人はその分類体系をテストし，それが理解されそして機能しているか，リソースが正しく分類されているか，その分類の満了期限が指定され遵守されているか等の点を十分確かめねばならない。

8.4.3.3.3　メディア・コントロール

メディア（テープ，ディスク等）を確実に保護するため，その分類に応じたラベルが添付される必要があり，またこの分類法の各々には，必要最低限のコントロールが用意されていなければならない。たとえば，「機密」のラベルがあるメディアは半期毎に，また「極秘」とされたメディアは毎週，その在庫調べがなされるといった具合である。メディアの蓄積にあたっては，ＤＰインストレーション内のアクセスを個別的な形に分離すべきである。アクセス有資格者リストが役立つはずだし，個々のメディアへのアクセスを監査することも有効な手だてである。また監査人は，アクセスの監査証跡と上記有資格者リストを対照する方法の

採用も可能である。

8.4.3.3.4　ＤＰオペレーション ― 入出力コントロール

①責任の所在，②認定されたＤＰジョブだけが処理されていること，③結果としての出力が有資格の受容者のみに配布されていることなどを確実にするため，十分なコントロールが用意されねばならない。この種のコントロールを提供し得る手段は数多あるが，コントロールの存在，十分性，調和を視座に置いてＤＰオペレーション機能を点検することも，この分野の監査には不可欠である。

8.4.3.3.5　リモート・コンピューティング

リモート・コンピューティングあるいは会話型の処理環境において，セキュリティ・コントロールは，物理的なロックやキーだけでは十分な責任を付与し得ず，しかも不正なアクセスを排除できないと思われるので，とくに重要となってくる。ＤＰインストレーション監査の対象とされる最少限のコントロールは，つぎのような事項を含む。

ユーザ識別

データ・アクセス・コントロール

端末機器識別

システム・セキュリティ管理

監査証跡

端末機器セキュリティ

特権サイン・オン・コード

出力コントロール

（９セキュリティ機能のレビュー参照）

8.4.3.3.6　大量データ伝送

データは，しばしば郵便や電子的手段で大量に送られる。この場合データの重要度や分類に応じてある種のコントロールが必要となろう。米国郵政公社の手で「機密データ」が送られる場合，内部の分類表示を隠すため二重封筒を用いたり，受領証を返信として要求する書留にする必要があろう。

機密データの大量伝送は常に，書面での承認を必要とし，維持される監査証跡には，日付け，時刻，送信者，承認者，受信者，そして時に応じて肯定応答が示されねばならない。

8.4.3.3.7　暗号化

非常に機密レベルの高いデータを，所有者のコントロールから離れて外部へ送らねばならない時，数式化や暗号化は有効な手だてとなろう。ただデータ暗号化標準（Data Encryption Standard）アルゴリズムのような，よくその特長が知られたアルゴリズムだけを採用すべきである。こうしたアルゴリズムの導入は，そのアプリケーションに合せたものでなければならない。暗号の使用を点検する際，監査人は，システム性能の点で犠牲があることを考慮に入れるべきである。

監査人は，さらに，データが必要な個所で暗号化されているか，またキー処理を含む良い暗号化手順が採用されているか等についてもテストしてみるべきである。

8.4.3.3.8　プログラム・コントロール

プログラム，ＪＣＬ（ジョブ・コントロール・ランゲージ）および関連ドキュメンテーションを不正なアクセスから防護するためにも，アクセス・コントロールは必要である。プログラムというものは，その内在的価値については専右的な面があるが，不正な変更によって企業資産の横領を容易にしたりあるいは隠したり出来ることを考慮すると，「脆弱なもの」ともいえるのである。いずれにせよ，プログラムとそれに関連するＪＣＬ，ドキュメンテーションが，不正なアクセスから保護されることには，重要な意義がある。変更作業記録（チェンジ・ヒストリ）の完全性を確保するために，コントロールは十分なものでなければならない。

8.4.4　偶発事故対策プラン

本レビューにおいて監査人は，当該インストレーションが，通常のビジネス活動を著しく阻害させるような天災，人災あるいは何らかの事件の発生に対し，どのように準備されているか判断せねばならない。監査人はまた，火災や不法侵入のような突発事態を検知・制限するプラン（緊急事態プラン），危機に瀕したジ

ョブをタイムリに完了させるプラン（支援プラン），任務の遂行能力を回復させるプラン（復旧プラン），顧客，従業員および株主の資産に係わるデータや国益に関係のあるデータを識別・保護するプラン（重要レコード・プラン）などが見出されるよう期待すべきであろう。

偶発事故対策を成功裡に打ち立てる鍵は，定期的な検査である。この種の対策計画が検査されなかったり，毎年更新されなかったりすると，その有効性は非常に急ぶまれる。この偶発事故の領域は，決して成り行きまかせであってはならない。監査人は，当該プランが検査・更新されている確証を得るよう努めるべきである。

9．セキュリティ機能のレビュー

9.1　重要性

セキュリティ部門あるいは機能は，セキュリティ政策に明確な表現を与え，セキュリティ・リソースを割り振り，セキュリティ規則の定義・発表・管理を行い，修正活動について勧告するなどの任務を持っている。全てのレベルのマネジメント，そして全てのマネジメント機能に奉仕するのが，スタッフの役目である。運用しているシステムの性格や分野にもよるが，この役目は，広汎なコンピュータ化されたデータや，その責任をまっとうする手順に対して責を負うことになろう。またそのデータには，許可，システムあるいはアプリケーションのアクセス規則，変動発生の通告等に関するステートメントが含まれる。そして手順には，アクセス規則の適用・維持に関するプログラム，現行規則を伝達・分析するためのプログラム，あるいは現行規則の変更通知等が含まれる。

セキュリティ部門のスタッフは，アプリケーションやオペレーション全般に普及している全てのセキュリティ・コントロールの導入および運用に責務を負う。彼等はまた，アプリケーションへのアクセス・コントロール，監視，助言サービス等の提供者とみなすことが出来，アプリケーションの提供者兼顧客としてみる

こともできる。

この部門あるいはスタッフの適切な活動や，データおよびプログラムのインテグリティは，全てのセキュリティ・コントロールおよびその手順が，均質かつ時機にかない一貫した適用を受けることに依拠しているといえるだろう。

9.2 目 的

セキュリティ機能をチェックする目的は，つぎのような事項が確保されている状態を創成することにある。すなわち，その設備および組織が，良き慣行，そしてインストレーション並びにアプリケーションの必要性に合致している。そのリソースが経営管理者の意図にかなった形で消費されていて，使用部門が満足のゆくサービスを受容している。その活動が，経営管理者の意図や使用部門への認可内容に一致している。許可内容，責任，正確さおよび完全性を証明し得る監査証跡である。変更は時機をはずさず処理されている……といった状態である。

重要度の高いセキュリティ機能あるいはサービスが，利用部門やタイムシェアリング，データベース，会話型ＤＰ環境のようなアプリケーションで広く一般化しているような場合，こうしたレビューがとくに望まれる。

9.3 アプローチ

監査対象のインストレーションやシステムの規模にもよるが，セキュリティ機能のレビューは，他の監査，たとえばＤＰインストレーション監査の基本単位（モジュール）ともなるし，独立した監査として実施することも可能である。一方セキュリティは，一つのアプリケーションとして，つまり監査されるアプリケーションとしてみることもできる（7.アプリケーション・レビュー参照）。この監査においては，これまでの監査で述べたのと同じアプローチおよび技法を用いるべきである。

9.4 対照領域

この監査領域の概要は次の通りである。

一　般

責任の規定

標準オペレーティング手順／ユーザ・マニュアル

ＤＰセキュリティの自己点検

教育

従業員の自覚

セキュリティ管理（対話型環境）

セキュリティ・コードの管理

モニタリング

レポーティング

違反

極めて重要なトランザクション利用

端末機器許可

ユーザ許可

ユーザの限界

アクセス・コントロール

ＤＰリソース

空間（スペース）

媒体（メディア）

装置

ドキュメンテーション

コミュニケーション

偶発事故対策プラン

緊急事態プラン

9.5 一 般

9.5.1 責任

セキュリティ機能は，一般的にはＤＰセキュリティの監視・監督に責を負うスタッフ機能を意味する。監査人は，この機能が明確に規定されているよう仕向けなければならない。

セキュリティ機能は，当該システム内部のアクセス規則を管理することによりユーザ・マネジメントを助け，一方監査人は，全ての管理的活動が承認通り行われるよう十分な監査ツールを用意しなければならない。

9.5.2 標準オペレーティング手順／ユーザ・マニュアル

現場のセキュリティ・ガイドライン，オペレーティング手順およびユーザ・マニュアルが文書化され，そして適切に維持される状態を確保することは，セキュリティ機能の責任である。監査人は，必要に応じてこれらのドキュメントを調査し，その利用状況をテストしなければならない。

9.5.3 ＤＰセキュリティの自己点検

監査人は，ＤＰセキュリティをテーマとした何らかの自己点検結果，それに基づく活動計画および現在までの進展状況等の提出を要請すべきである。こうした自己点検情報の分析によって，監査人は問題となっている組織やテーマに対する考案を深められるだろう。だがこれで監査の全責任がまっとうされたことにはならない。監査人は，この種の情報源が承認し得るものであり，しかも結果として出されている論評が正しい展望に立つものである限り，自己点検結果を尊重し利用すべきであろう。

9.5.4 教 育

セキュリティ機能のもう一つの責務として，業務分野別（ライン）機能に合せた特別仕立ての教育コースを運営し，これらの機能がＤＰセキュリティに関する全てのセキュリティ応用コースをフルに活用するよう仕向けることがあげられる。クラスの授業スケジュール，授業細目，名簿などこの種の責任履行の成果が現われているものは，全て点検すべきである。

9.5.5　従業員の自覚

この問題は，セキュリティ機能にまつわるジョブとしては極めて重要な側面をなしている。ＤＰセキュリティという主題は，否定的あるいは消極的に受けとられがちなので，監査人は，このテーマに積極的意味を持たせ，そして従業員の自覚や関心を維持・向上させるために，セキュリティ機能がどのようなことをなしているか判断する必要がある。この分野の責任は無限であるといえよう。ポスター，提案制度，非公式の賞与，朝食，昼食，ゲストによる講演，経営陣のスピーチなど，利用できる機会や方法はいくらでもあろう。こうした手段は単に侵入に対するガードの重要性を指摘するにとどまらず，データの保全とともに何らかの感謝の念も残すことができる。自覚増進計画の内容は，資産価値を反映するとともに，それらの保護において従業員の果し得る役割の重要性をも指摘したものとなろう。

何はともあれ，この領域の重要性は測りがたい。効果的なＤＰセキュリティ計画は，従業員の強い関心や参画なしでは達成出来ないのだから……。

9.6　セキュリティ管理（対話型環境）

通常どのような対話型システムにおいても，幹部としての資格で誰か一人あるいはグループが，セキュリティ管理者に任命されている。効果的なシステム・セキュリティが維持されるためには，こうしたスタッフに付与された職責が適切に果されねばならない。セキュリティ管理の責務には次のような項目が含まれる。

- システム・リソース使用の許可
- セキュリティ・コードの管理
- ユーザ活動の監視

  侵入あるいは変異

  重要トランザクションの利用
- 端末機器許可
- ユーザ許可

- データ・アクセス・コントロール
- ユーザ・セキュリティ教育
- 偶発事故対策プラン

監査人は，上述した全ての領域に対してセキュリティ管理者の能力と成果をテストすべきである。監査人はまた，このような検証作業を容易ならしめるため，できる限り文書化された実績資料の入手に努めるほうが良い。

セキュリティ管理者の責任の中でよく見落されがちなのが，ユーザの関与である。セキュリティ管理者は，ユーザの関与，理解そして最も重要なフィードバックを促進するよう努めるべきであり，同時に，ユーザのセキュリティ活動を絶えず監視しなければならない。

9.7 アクセス．コントロール

セキュリティ管理者が，アクセス・コントロールおよびそのコントロールの監視において果す役割は，常時評価されねばならない。より詳しくは第6.4.3項を参照してほしいが，セキュリティ管理者は一般的に，コントロールの不十分性があればそれを経営管理者に助言する責任を負っているといえよう。

9.8 偶発事故対策プラン

偶発事故対策プランを作成，実施，評価するセキュリティ管理者の役割は，点検されねばならない（第8.4.4項参照）。監査人は，セキュリティ機能の適正な取扱いが全ての偶発事故対策プランに含まれるよう仕向けるべきである。

9.9 要　約

セキュリティ管理者の仕事は，セキュリティ手順を作成，導入し，その運用と原理の一致を点検するものとして把えることができる。したがってセキュリティ監査中に指摘された何らかのコントロールの不十分性は，もしそれらが以前に指摘を受けていなかったり，あるいは解決のため適当なレベルの管理者に通告され

ていない場合は，セキュリティ管理者の職責に対する成果が直接反映したものと見ることができる。つまり職責達成度不良ということになる。

10. 制御されたテスト／浸透調査

10.1 重要性

この監査の目的は，監査人がこれまで経営管理者層に幾度も指摘し，なおかついまだに解決されていない基本的なそして繰り返し起っている問題やエクスポージャ（様々な脅威にさらされること）を解消させることである。第3節に示したようなタイプの問題であるだけに，マネジメント層が監査人の関心事に注意を向けない事態がしばしば発生する。また経営者達は，「自分の所に起こるべくも無いことだ」という態度を示すこともある。

10.2 目 的

このテスト手法の目的は，不正な行為を敢えて登場させることによってＤＰセキュリティの必要性を経営者層に強く印象づけることである。

10.3 アプローチ

監査人は，ＤＰコントロールのエクスポージャ（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）に関する知識を利用してもよいが，監査特権を用いてはならない。このテストを成功裡に終らせるためには，監査人は何らかの脅威が他の従業員や外部の人間により加えられる可能性があることを強く印象づける必要がある。監査人はさらに，監査特権がそうした侵犯の一要因では決してないことも証明できねばならない。

この場合，もし試みた侵害が発見されると，監査人に対する作業上の障害だけでなく当初の意図とは反対の効果が出てしまうので，検知できない侵害が成功する確率は 90 %以上でなければならない。

このように意図的に侵害をおこすプランは，監査側と現場の管理者達との合意の上で実行に移されるべきである。またテストは，監査人が検知されずに不正手段を行使し得る状況に置かれることのないよう十分コントロールされねばならない。

作業グループは，この技法の効用を大いに認める結論を出したが，しかし制御・企画の両面で注意深い配慮が必要であり，危険性をはらんだアプローチだけに，最後の手段とすべきであるという点で意見の一致をみた。

だが，専門的な注意の行き届いた方法で実施されるなら，実に効果的な技法であることに変りはない。

10.4　対象領域

この場合で対象となる領域は，個人の想像力に全面的に依拠する。浸透調査が行える代表的な分野は以下のようなものである。この分野の各々については，順次簡単な説明を加えてあるが，浸透調査は，当該環境に固有のものでありその局面に従ってその結果は判定されるべきである。

①アプリケーション・プログラミング

②ＤＢ／ＤＣシステム

③情報セキュリティ

10.4.1　アプリケーション・プログラミング

プログラム・コードの操作により侵害を検知されずに起こそうとする指示に従って，ＥＤＰ監査人はアプリケーション・プログラミングに対処させられる。選ばれるアプリケーションは，給与支払のようなこのテストの成功率の高いものでなければならない。またこのアプローチは，バッチや対話型の環境にも適用し得るものである。

10.4.2　データベース／データ通信環境

ユーザのふりをしたり，あるいは鋭敏なユーザの領域に実際に入り込むことによって，監査人は企業資産を横領すべく見つからぬ方法でシステム・コントロー

ルの回避を試みるべきである。このアプローチは，当該アプリケーションやそれにまつわる種々のコントロールを徹底的に理解するための十分な時間が必要である。

10.4.3　情報セキュリティ

このアプローチは，情報自体が高度に資産価値のある場合（例えばR＆D環境のもの）適用出来る。その目的は，検知し得ない方法でコントロールを回避し資産価値の高い企業データを入手することにある。同様なアプローチは，不正な手直しや破壊に対しこの種のデータが持つ脆弱性を立証する際にも用いることができる。このアプローチの簡単なそして効果的な実例として，勤務時間後に監査人が端末機器室に入り不注意に放置されているパスワードやユーザ・マニュアルを探し出す方法が考えられる。こうして入手したユーザ・マニュアルやサインオン・パスワードを使用してリモート端末からアクセスを試みれば，きっと興味深い結果が得られるだろうし，セキュリティに対し一層の必要性があることも実証されるはずだ。

このアプローチの鍵は，監査特権を用いずに，ある重要情報に検知し得ないそして認承されないアクセスを行うことにある。その建物に接近する従業員や掃除夫が，当該情報に不正なアクセスを行い得たことを立証するのが最重要課題である。

10.4.4　要　　約

監査人が対象としている業務が，根本的問題でしかも反復して起こるものであるのに，経営管理者層が何の行動もおこさないような場合，正統な手続きを踏まないこうした不正な侵入は，注意を喚起する有効な方法である。しかしながら，この種のアプローチには広汎なプランニングが必要であり，そしてその上リソースを多大に提供しなければならないのに見返りが保証されないという側面がある。また浸透する試みが，一定の危険性をはらんでいると同時に，不成功に終ると監査人の立場でなく被監査人の立場を立証してしまうという結果にもなる。こうした結果になると，相互の信頼が失なわれることにもなりかねないのはいうまでも

ない。

11. D P 界 の 課 題

本作業グループは，今後ＤＰ界が取り組むべき主題が少くとも３項目ある点で合意した。これらの主題は，その影響力の大きさに違いはあったとしても，システムのセキュリティや監査能力に重要な意義を持つものと考えられる。これらのテーマとは，テクノロジー進歩との関係，文献の十分性そしてデータ処理慣行の現状である。

11.1 将来テクノロジーとの関係

将来データ処理分野のセキュリティや監査能力に影響を与え得るテクノロジーには，幾つかの明白な方向性が見てとれる。その中には，メディアの密度および携帯性の向上，大容量記憶装置，分散処理システムが含まれる。

メディア上に情報を記録する密度が向上するにつれて，データの携帯性（ポータビリティ）も増大する。このことは同時に，盗難や改変の機会も増大することを意味している。またより小さなボリュームという面も表面化してきている。(たとえばIBM Mass Starage System(注))大量のデータが，身につけて容易に秘匿し得るほど小さなボリュームに記録できるようになっているのが現状である。

だがこうした傾向は，大容量記憶システムの導入で部分的に相殺されている。というのも，より一層大量のデータをハードウェアの制御領域に移行させることが可能になっているからである。その結果，エラーをおかす可能性のある付帯的な機会に手操作による介入が少くなり，コントロールの画一性，一貫性，適時性が増大するものと思われる。だが単一のケースに従属するデータが増々ふえてくるので，データベース・バックアップ手順がその重要性をさらに増していくことになるだろう。

地理的なシステムの分散は，単一のイベントに従属するリソースの量を削減す

るはずである。

また通信コストの低下およびレスポンス・タイムの向上も期待できる。一方分散システムの場合，マネジメント・コントロールの画一性や効率の面では余り期待できない。

これらの技術的方向の幾つかは，明らかに建設的な本質を持つものである。本作業グループが一様に抱いている感想は，こうした技術的進歩の意義や可能性に対して経営者はもっと関心を持つよう警告されるべきだということである。

（注）編集者注：市場には，他のボリュームの小さな記憶装置も出ている。このＭＳＳを取りあげたのは，何もＮＢＳ（連邦政府国家標準局）による勧告或は保証を意味するものでは決してない。

11.2　文献の十分性

データ処理セキュリティの監査に関する文献は，そのどの領域についてもどこかで書かれているという意味で十分だといえる。だが新しい物指では，やはりこうした文献は，スタイルおよび方向性，読者の感受性，分量，権威の不在などの面で問題をはらんでいる。

文献のスタイルや方向性は，時としてその内容をあいまいにする場合がある。また文献の組織や構成は，各ソースによって異っているのに，その他のソースで使用されているモデルや構成に関するリファレンスが完備しているのは稀である。このような実状は，別々のソースの素材を有機的に関連づけることを困難にしているだけでなく，完全を期して行うソースの検証を殆ど不可能としている。

さらに目的，原則，ガイドラインなどより，むしろ実例，導入，手順に重点が置かれることがよくある。当然このようなケースでは，目標や原則の判断および明確化が読者の責任にされる。したがって素材が結局陳腐化することもあるし，新しいメディアあるいはテクノロジーへの可用性をぼかしてしまうことにもなる。

この分野の素材の大部分は，監査人というよりむしろ経営者，管理者向けに書かれている。したがって監査人に役立たないケースも出てくる。素材のなかには，

最大公約数的な読者を意識したものもある。この種のものは，個々の読者に役立つということはまずないであろう。監査人を特に対象として書かれたものはこのような懸念がないのだろうが，有用かつ適切な内容の素材はなかなか見出せないのが実状である。

公刊されているデータは非常に多い。この状態は一見問題がないようだが，読者にとってはその中から，読むに値し，有益でかつ実際に適用し得るものを選別しなければならないので大変な労苦となる。このプロセスは，著者の資格，経験典拠の是非などが不十分であったり不分明であることが多いので，非常に煩雑なものである。

本作業グループは，権威あるそして名声を得ている機関により，単一の一覧表が作成される必要があると考える。この作業には勿論監査人側からも参加を仰ぐべきである。そして要約欄には，目的と代り得べき解決法の２つに重点が置かれねばならない。また同一の素材が各々の関係読者に数回眼に触れるか，及至は少くとも１回相互参照（クロス・リファレンス）されるよう構成されるべきであろう。

11.3　データ処理慣行の現状

作業グループは，データ処理分野における慣行の水準については非常に批判的である。現在データ処理の監査あるいはセキュリティ問題だと考えられているものの多くは，悪習の制度化にほかならない。この種の悪しき慣行はオペレーションでは重大な影響やリスクを与えないかも知れないが，システム開発では間違いなく容易ならざる結果を及ぼす。

この問題は，技術的問題というより，むしろ管理上の失敗に帰されるべきだろう。管理者が製品や質を軽視しつつプロセスやスケジュールをこなしてきたものと見なされる。

今日こうした不十分な慣行がはびこっているのは，伝統や惰性，ツールの影響，プログラマは変更を望んでいないという管理者側の固定した現状認識などが原因

だと考えられる。現在の慣行は，短かいプログラミングの歴史を反映させたものともいえる。この歴史の半分は，一度に一つのジョブしか処理しない比較的遅い，そして高くつくマシンに費されてきた。こうしたマシンに適合する慣行では，現今のリソース共有システムでは不十分な成果しか得られない。

管理者達は，プログラマが仕事の遂行パターンの変更に抵抗するのではないかという危惧を常に抱いているため，新しいコントロールの導入に余り関心を示さない。ユーザに変更を容認させる能力がその成功の鍵となるテクノロジーが，現在，変更を受け容れるべき専門家の抵抗により脅やかされていることは実に皮肉な現象である。

データ処理管理者は，慎重かつ迅速にプログラミング・アプリケーションの開発およびシステム開発の現状を改善するよう動き出すべきであるという点で作業グループの意見は一致した。彼等は直ちにいわゆる「効果的プログラム開発技法（ＩＰＴ技法）」の導入に踏み切るべきである。これらの技法は管理ツールであって，プログラミング・ツールではないことを銘記すべきである。こうした背景を考えると，この技法はプログラマでなく管理者により採用されるべきであろう。

新しい管理手法の利用は，新しいツールの開発を必要とし，この開発によってプログラマのサポートは容易になろう。新しいエディタ，コンパイラ，ライブラリ・マネジャは，プログラムの許可，指定，点検，調和などで管理者の役割を援助するものでなければならない。そして寛容かつ柔軟なものであるより，制限的でコントロールし得る性格のものである必要がある。

プログラマは，その上司である管理者が考えているほど仕事上の変更を嫌うものではない。彼等は少くともユーザ程度には柔軟性を持っている。ユーザ同様プログラマも，新しいそして期待の持てる管理形態や改善されたツールに反応し適合するであろう。

データ処理界の最優先課題は，監査し得るような方法で監査可能なシステムを構築できるようになることである。

REFERENCES

[1] Computer Control Guidelines, Toronto, Canada: Canadian Institute of Chartered Accountants, 1970.

[2] Guidelines for Automatic Data Processing Physical Security and Risk Management, U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., Federal Information Processing Standard Publication (FIPS PUB) 31, September 1974.

[3] Study Group on Computer Control and Audit Guidelines, Computer Audit Guidelines, Toronto, Canada: Canadian Institute of Chartered Accountants, 1970.

[4] Data Security Controls and Procedures (G320-5649), White Plains, New York: IBM Corporation.

[5] EDP Auditors Association, Inc., Control Objectives

PART Ⅷ プログラム・インテグリティ

議　長　Clark Weissman

システム・ディベロプメント・コーポレーション

参加者　Richard Canning

キャニング・パブリケーションズ

Don C. Lundberg

ＩＢＭ

Harold J. Podell

米国会計検査院

Carl B. Spencer

Glendal Federal Savings and Loan Association

Douglas Webb

ＥＤＰ　オーディット・コントロールス

Edmund L. Burke

マイター・コーポレーション

Theodore A. Linden（記録係）

米国標準局

編集者注

議長の経歴紹介

クラーク・ワイスマン氏は，システム ディベロップメント社（ＳＤＣ）の技術主任であり，かつＲ＆Ｄ部門の副部長も務めている。彼は，同社の独立研究開発（ＩＲ＆Ｄ）計画の責任者であり，過去20年の同社勤務期間中に，プログラミング言語技術，ＯＳ設計，タイムシェアリング，コンピュータ・システム・セキュリティなどの多くの先進テクノロジー分野にＳＤＣを進出させた実情を持つ。

1969年秋のＡＦＩＰＳコンピュータ合同会議で卓越した論文として高い評価を受けた彼の「ＡＤＥＰＴ－50タイムシェアリング・システムにおけるセキュリティ・コントロール」は，コンピュータ・システム・セキュリティの理論と方法論の領域で創成期の貢献と認められている。彼は過去3年間，ＳＤＣのシステムズ・セキュリティ部門を統轄し，ほとんど全ての商用コンピュータ・システムを対象としたセキュリティ侵入分析，および米国標準局（ＮＢＳ）から委託されたＮＢＳデータ暗号化標準のアプリケーション調査を指導した。またそれ以前には，ＡＲＰＡ後援のＲ＆Ｄ活動を主宰し，コンピュータ・ネットワークの設計並びにアプリケーションに関する数字の調査を実施している。彼は航空工学の学位（マサチュセッツ工科大学）を持ち，1967年にはＬＩＳＰ 1.5 Primer を著わしている。これは1970年に日本語版も出版された。西部の神士録にも登場し，ＡＣＭでずっと活動してきた。ＡＣＭのＯＳ部門の編集者を務めたこともある。

本セッションに与えられた課題は，「プログラム・インテグリティ」である。すなわち，ＡＤＰ環境におけるプログラム・インテグリティ評価にはどのような監査アプローチあるいは監査技法があるかを考察し，オペレーティング・システム（ＯＳ），データベース・マネジメント・システム（ＤＢＭＳ）およびアプリケーション・プログラムにも十分な配慮を与えることと要約できよう。

プログラム・インテグリティは，ソフトウェアが論理的に完全であり，それ自体のために設計されたタスクを一貫して正確に達成している状態として定義されている。この文脈内で本セッションは，プログラム・インテグリティの評価に伴なう諸問題を考慮することになろう。

本セッションは，次の2つの領域に対する評価を効率的になすにあたって，現在利用し得るあるいは必要とされる監査アプローチおよび技法を見出すことを中心課題とする。(1)ソフトウェア開発中のプログラム・インテグリティを確実にするため経営管理者により実行されるコントロール，(2)ソフトウェア設計およびそのインプリメンテーションにおける運用面の信頼性とパフォーマンス保証。

プログラム・インテグリティ評価

コンセンサス・レポート

クラーク・ワイスマン

1．プログラム・インテグリティとは何か

プログラム・インテグリティに取組む場合，まず，プログラムおよびインテグリティの定義と評価が必要となる。広義に解釈すれば，プログラムは，一連のプログラムを全て含み，コントロール・ソフトウェア，オペレーティング・システム（ＯＳ），データベース・マネジメントシステム，アプリケーション・プログラム等を指すことになる。さらにプログラムは，所要条件，仕様，設計からソース，目的コードに至る全ライフ・サイクルを通じてそれぞれ違った形で存在するという意味では「有機的」といえる。

一方，インテグリティはまず第一に，(1)そのプログラムが要件を満たし，仕様を完備した場合の正確さおよび何も実行しない場合の正確さを重要視する。だがインテグリティはこうした正確さだけにとどまるものではない。それはまた，(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にも大きな関係を持ち，その上，(4)当該プログラムがその中に一定レベルの信頼を打ちたてられるよう評価出来るものでなければならない。こうしたインテグリティの４つの側面全部が，そのプログラムの全ライフ・サイクルを通じて保持されるべきである。

システム・インテグリティは，プログラム区画のインテグリティの一機能である。通常システム・インテグリティは，そのコンポーネント・プログラムのインテグリティより低いが，余分の独立モジュールが，他の演算をチェックするため採用されているなら，システム・インテグリティの方がコンポーネント・プログラムのそれより幾分上廻ることもある。

要約すれば，プログラム・インテグリティは，ある脅威が存在する環境で一定

レベルのインテグリティを容認するリスクを管理者に判断させることになろう。リスクを視点としてプログラム・インテグリティを評価する際のこうした要因は，この領域の調和の中で拡張されるものである。提起された問題点は，セッション参加者の合意をみて採択されたものである。

2．プログラム・インテグリティの脈絡

コンピュータ・システムのセキュリティは，(1)システムの欠陥，(2)システム資産に対する脅威，(3)開発担当者の数，などが少ないほど増すことはいうまでもない。全ての保護戦略はこうした目標を追求しているからである。プログラム・インテグリティは，まずこの第一の目標，すなわちシステムの欠陥の削減を狙ったものである。

しかしながら，管理者はその保護政策の決定において，一定の脅威や予算レベルとの兼ね合いで，インテグリティの減少とまた別の目標とを交換する場合も出てくるだろう。以下に論述しているのは，インテグリティに付随する様々な問題点である。

2.1　プログラムは時間（ライフ・サイクル）とともに変化する

われわれが通常プログラムについて考える時，その最終コードや最終オペレーションの段階で把えることが多い。だがプログラム・インテグリティは，開発の当初からプログラム中に組み入れられねばならない。プログラムは，6段階を移行して行く。

① 組織的役割：システムの目的が明確化され，責任が各コンポーネント組織ごとに分担される。

② 所要条件：各役割に付与された責任は，特定のシステム要件に翻案される。例えば何がなされるべきかといった風にである。また機能，パフォーマンス，コストおよびその他の制約条件（リミット）も規定される。

③ 仕様：所要条件は，各システムごとに，つまりハードウェア，ソフトウェア，通信，要員，設備等についてシステム仕様の形に翻訳される。この仕様は，所要条件がどのように満たされるかを詳細に定義するものである。また仕様は，機能的レベルとコンポーネント・レベルで存在する。ソフトウェア・コンポーネントの場合，それらは「コーディング・スペック」と呼ばれる。このコーディング・スペックの文書化は，流れ図，デシジョン・テーブル，テーブルおよびメモリーのレイアウト，数学的アルゴリズム，Parnas 様式のモジュールなどが含まれ，最近では公式仕様言語も構成要素の一部として入り込んできている。

④ コード：仕様は，ＰＡＳＣＡＬ，ＰＬ／１，ＦＯＲＴＲＡＮ，ＣＯＢＯＬのような知名度の高いプログラミング言語や，機械アセンブリ言語では，ソース・コードに翻訳される。その後，言語コンパイラやアセンブリ・ツールによって，走行時間目的コードあるいはマイクロ・コードに翻訳される。

⑤ テストおよびインテグレーション：プログラムは稼働前に，単体で，そして総合システムの一部としてテストされる。この段階は，当初のコードを作成したプログラマによる通常の「単体」テストや「デバッギング」とともに実行される。

⑥ オペレーションおよびメインテナンス（Ｏ＆Ｍ）：ソースおよび目的コード・プログラムのライブラリは，コンピュータ設備の利用に供するため貯蔵される。時々Ｏ＆Ｍ要員によりこれらのプログラムにマイナー・チェンジが加えられ，エラーの修正，パフォーマンス改善，機能および能力の拡充，新装置への適応などが実施される。これらの変更のコントロールは，Ｏ＆Ｍ構成管理（コンフィギュレーション・マネジメント）の一部である。このＯ＆Ｍは，容易に片付け得るものだが，プログラムの再設計や大幅な修正がこの段階で試みられるような場合プログラム・インテグリティがそこなわれることがある。主要なプログラムの変更は，既存のモジュールと置きかえられる新規ソフトウェアとしてチェックされる必要があり，これらの新しいモジュールは，役割りと所要条件のライフ・サイクル段階を始める際，当初のプログラム程度に圧縮されねばならない。

2.2　関係の可視性は段階を経過する中で失なわれる

プログラム・インテグリティで最も重大な問題は，ソフトウェア生産の各段階を終るなかで，複雑さが増大し，段階間の可視的なリンクが見失なわれてしまうことである。たとえば，あるコード・モジュールを，役割の目標や，システム要件，さらには機能的な仕様とさえ関係づけることが不可能になる場合がある。とにかく，機能が分散化され，レベルの表示（ノーティション）が低位言語に翻訳され，そしてプログラムが複数の要件を満たすよう作成されるに従って，この結合が希薄化してしまう。

当初の要件と結果として生じるコードとの間に脈絡がなくなってしまう事実は，何らかの目的でコードが変更されねばならない時，とくに重大な影響を及ぼす。改変の程度が大きくなれば，それだけ役割や要件を満たす上での各部の相互関係に対する理解が必要性を増してくる。コードのつぎはぎは，インテグリティの喪失の主要な原因となる。というのも「戦術的」な調整がしばしば，眼に見えぬ「戦略的」な役割の設定を土台から崩してしまい，大きな災事を引き起こすことがあるからである。

2.3　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

プログラムのライフ・サイクル中の変成をいつ監査・評価するかを決定することは，インテグリティ評価のテーマの一面にすぎない。セキュリティの脅威の関連やその厳しさ，およびインテグリティ確保のため開発中に採用される手段などは別次元の問題である。これらの各次元については，以下の章節でより詳しく触れてみたい。

3．関連する脅威およびその厳しさ

脅威は，人為的なものもあるし，自然現象に帰因するものもある。自然災害，物理的故障，作成者或はユーザによる人為的エラー等の結果は，サービスの中断

あるいは突発的な情報漏洩という形で現出するだろう。意識的な不法侵入者が加える脅威の場合，その影響はより重大となる。人為的脅威は，偶発的なものと，故意の攻撃に大別される。前者には，偶然欠陥を見出したり，彼等が利用出来る欠陥を積極的に探し求める個人が中心となり，後者のグループの場合，攻撃のリソース，計画性，方法でより精緻な姿勢を示すだろう。これらの故意の攻撃による脅威は，共謀した一団が，システム，アプリケーション・プログラム，ライブラリ・プログラムなどに含まれる運用コードを改変したり，あるいは破壊的な「トラップ」機能を仕組んで実行に移す注意深さが特長となる。恐らく最悪の意図的な攻撃は，雇用条件に不満を抱く従業員の無分別な行為であろう。漏洩や入手出来る利益などをめぐって攻撃側には何の抑制もないわけだから，この種の無分別なアタックには有効な阻止手段が殆ど見出せないのが実状だ。

攻撃の厳しさの程度や，必要とされる対抗手段を基軸に脅威をランクづけすると，次のような順序になる。

① 無分別な攻撃
② 共同謀議チーム
③ 積極的に欠陥を追求する人
④ 偶然欠陥を見出した人
⑤ 人為的エラー
⑥ 自然の障害

4．プログラム・インテグリティの達成手段

本セッションの合意として，プログラムは，正確さ，堅固さ，信頼性を持たねばならないとの結論で一致している。正しいプログラムは，それが役割（ミッション），所要条件，仕様のどれをも満たす証しを提示するものである。企業の監査になぞらえるならば，プログラムの正確さを監査した場合，企業の「財務諸表」に相当する証左が必要となる。

堅固なプログラムには，予期せぬ環境の変動に直面しても一定の十分なパフォーマンスが維持できるメカニズムが備っていなければならない。こうした変動には，ユーザのキー・ストローク，手続プログラムの欠陥，オペレータの失策などがあげられる。こうした強固なメカニズムを企業監査の例にあてはめると，「内部財務管理体系」がそれに相当する。

信頼し得るプログラムとは，上手に文書化され，機能的に煩雑でなく，モジュラー・タイプで，長さも比較的短かく，構造化されたアーキテクチャに統合され，良きプログラム慣行や鋭敏な標準の所産であるものを指す。プログラムの信頼性を企業組織になぞらえると，「高い評価を受けた会計原則」を持っていることに相当する。

4.1　正確さの証左

プログラムの妥当性検査（バリディション）や検証（ベリフィケーション）は，静的にもまた動的にも実施され得る。つまり前者ではソース・コードで，一方，後者では走行目的コードで行われるからである。

4.1.1　静的評価

次にのべるようなソース・コード検査アプローチの組み合せが，現在，民間企業やR＆D研究所などで採用されている。

① 設計調査：この方法は，役割りと所要条件を基礎としてその設計を吟味するため，設計者と検査者合同の正式の会議をその一環としている（修復相当者は含まず）。設計には，説話調のドキュメント，論理ダイアグラム，機能仕様およびコーディング仕様を含むべきである。重要度の高いコンポーネントにはソース・コードを含むことも考慮されて良い。この設計調査は，各サブシステムと主要なコンポーネントの里程標としてスケジュールを組むべきであろう。また調査結果は，文書化して全参加者に配布されねばならない。

② 仔細点検：この古典的とも言うべき科学手法は，関係専門家の詳細に亘る点検調査が中核をなし，プログラム・ライフ・サイクルの種々の段階についてそ

の製品を批評するものである。設計調査も，この仔細点検の一つの重要な例といえよう。

③ 品質管理（ＱＣ）：顧客や開発者ではなく，第三者が，ライフ・サイクルで生じる全ての形態のプログラム品質をチェックする。この手法は，上述の１および２を組み合せたもので，正式な形でそして時には外部発注で行われる。この場合ＱＣ契約者は，経験，保有するツール，技倆等をよく考慮して選定されるべきである。

④ コンパイラ・チェッキング：ソース・コードを目的コードに変換する翻訳プログラム（例，コンパイラ）は，従来からＱＣツールとしてプログラム・エラーの検出に使用されてきた。また最近のＲ＆Ｄで，良いプログラミング慣行を養するメカニズムとして，この技法が再び注目をあびている。新しい言語は，プログラマの意図を明確にそして詳細に示す宣言（デクラレーション）を要求しており，構造化プログラミングを支える力強いデータ・タイピング，限定的なプログラム領域，厳密にモジュール化された呼び出し手順を重要視している。こうした言語のコンパイラは，言語の構文や意味論を強固にするための広汎かつ包括的なチェックを行い，場合によっては，プログラムの意図を走行時に強調するコードを生み出す機能も果たす。

⑤ 自動アナライザ：コンパイラを構文および意味論の両面から分析するソース・コード・ツールは現在数多く利用されているが，それらは目的コードを生成することはない。この種のツールは，流れ図の作成，ドキュメンテーションを補助するためのコード再書式化，クロス・リファレンス用リストの作成，改良されたライブラリ・コントロールおよびその利用のためのインデックスの生成，そして動的評価向けのテスト・ケースの設定等に用いられている。最新の利用形態としては，その正確さを正式に立証するため当該プログラムの事実断定を自動的に生み出すパターンがある。

⑥ 形式証明：プログラムの正確さに対する形式的証明は，現在の技術水準の先端に係わる問題である。基本的にはこの手法は，インプットとして，「正確さ

の基準」と「プログラム」を受け容れ，アウトプットとして正確さの基準を当該プログラムが満足している正規の証明（あるいは反証）を生み出す。実際面では，この手法は各ライフ・サイクルの段階で反復される。トップ・レベルに於ては，この正確さの基準は，一組みの事実断定とプログラム要件の数学モデルで示される。プログラムは数学的仕様を持つもので，いずれも「仕様言語」で表現されている。また最下位レベルでは，正確さの基準は，前のレベルの出力仕様であり，そのプログラムは高水準言語（ＨＯＬ）のソース・コードである。どのレベルにあっても，これらのインプット，すなわち基準とプログラムは，一組みの検査されるべき条件を作り出す「検査条件生成プログラム（ベリフィケーション・コンディション・ジェネレータ）を通じて処理される。このソース・プログラムや事実断定を内容とする＂検査条件＂は，正確さの数学的形式証明，つまりそのソース・プログラムが事実断定を満たしているという証明を与える＂定理証明式（Theorem Prover）＂を介して処理される。この処理過程は，手操作，自動のいずれの形態をもとり得る。数多くの制限度の高い＂プログラム＂が，この両パターンで処理され得ることが判明しているので，このプロセスが安易に考えられがちだが，問題は大きくしかも十分な理解度に達していないのが実状である。さらに進歩も遅々とし論争の種がつきないし，ツールも限定的で商用化されたものがない状態である。

4.1.2　動的評価

根本的にはこのアプローチは，プログラムをランさせ，それが機能するか否かを判断する。静的評価とは違って，動的評価は，コンパイラ，ローダ（loader），ＯＳ，ライブラリとサポート・パッケージ，物理的手順，通信エレメント，ＣＰＵハードウェア等によりもたらされるエラーをテストするものである。静的評価が全てのプログラム条件を対象にしようとしたのに対し，動的評価は，リアルタイムの状態を含み，選別されたテスト・ケースにのみ有効である。したがってテストには，基本的な技術問題，つまり最良のテスト・ケースの選定という作業が含まれる。そして多くの機構が存在している。国防総省（ＤＯＤ）のテスト手法

は3段階を必要としており，(1)分離型モジュールのユニット・テスト，(2)統合されたモジュール群のサブシステム・テスト，(3)サブシステム，実際のハードウェア，実データの統合体に対するシステム・テストと分けられる。この様式は他のアプローチでも恰好の参考例となるはずだ。

4.2 強固さの立証

正確さの場合とは異なり，強固さのメカニズムについては，ほとんど形式論理は存在しない。今日実施し得る最善の方法は，既存システムで有効だと判明している手法をリストアップすることである。

4.2.1 現行テスト

システムの引渡し後，あるいはオペレーションやメンテナンスが開始された後も，テストは続行されねばならない。

① Exercising：システムは，操作のシミュレーションの形でテストされ，テスト結果と対比される既知のレスポンスが用いられる。この手法は，国防総省のシステムをテストするアプローチとして周知のものである。この修正版が最近になって商用化され，ミニカンパニーへの入力をテストする際，監査人が容易にシステムのレスポンスを観察できるよう，企業の財務管理体系に合わせてシミュレートされたミニカンパニーが設定できるようになっている。このミニカンパニー・アプローチは，インテグレーティッド・テスト・ファシリティ（ＩＴＦ）メソッドとして知られている。

② Flaw Hypothesis Method：このアプローチでは，他のシステムに見出される欠陥例を前提としシステムの欠陥が仮定されており，対象システムにおけるその欠陥の有無がテストされる。テスト・ケースの選定という面からは，コスト効果の高いアプローチだといえよう。

③ 抜きうちテスト：これは軍隊の Inspector General の行う企画に範をとっており，検査班が突如到着して，運用システムのテストを行う。様々の計画アプローチが既存システムを対象として試みられているが，無資格の改変や無認可

の運用手順が摘発されている。

④ 合理性チェック：システムは，印刷ミス，文脈を無視した行動，無意味なコマンド（例，カード・リーダを巻き戻せ）等の代表的な人為的エラーを検知・修復する能力をテストされる。

⑤ エラー回復：システムは，ハードウェアや通信，電源等の故障，サージ（電流の動揺），プログラム・エラーなどを検出・回復する能力をテストされる。再始動点，チェックポイント，ロールバック・オプション等にとくに関心が払われる。

4.2.2 オンライン・モニタリングおよびコントロール

ＤＯＤ（国防総省）アプリケーションで有用なサービスに，システム・セキュリティ・オフィサ（ＳＳＯ）によるオンライン・コントロールがある。ＳＳＯはシステム誤操作の防止，すなわちその監視にあたる。システム・インテグリティに対するこうした侵害を検出する助けとして，ＳＳＯは，組み込まれた監視機構，モニタリング，故障，およびソフトウェア・ジャーナルのコントロール機能をもつ。こうしたプログラムにより，ＳＳＯはシステム環境のテストを通じて，適正な作業手順の確立，活動現況の経過記録，例外状況の個別調査をおこなうことができる。この概念は，国防総省の国家の安全保障という問題をこえて，さらにシステム・インテグリティ全般にも適用できる。とくに重要なのは，サブジェクト・クリアランス，目的分類，暗号化キー，ユーザ識別子（ＩＤｓ），およびパスワードのシステム・セキュリティ・データベースの管理である。

4.2.3 冗長度

ハードウェアの面からするインテグリティへのアプローチが従来おこなわれていたが，ソフトウェアでは，有効性に限度のあるアプリケーションであることがわかった。ある１つの結果を計算するのに，異ったアルゴリズムがいくつもある場合，演算ソフトウェアの１部として独立した異なるモジュールを用いて，これらアルゴリズムを計算でき，計算結果の比較および例外事項の報告（ＳＳＯに）が可能となる。

4.2.4　サポート・コントロール

システムの健全な働きに対する信頼は，機能管理とO＆Mプロセデュアによるものであろう。これらは次のように分類される：

1) コード・コントロール：プログラム・ライブラリは，システムおよびユーザ・コードへの選択的アクセス，エラー訂正，ソフトウェア更新のための合理的な変更プロセデュアを可能にするものでなければならない。

2) エラー・コントロール：エラーはおこるものであり，その報告および適正な措置がなされなければならない。

3) ドキュメンテーション・コントロール：ソース・プログラム・ライブラリは，ドキュメントから得るものである。日付を記した記述およびプロセデュアによるエラーを防止するためには，ユーザおよびシステムのマニュアル，その他の形態の英語版ドキュメンテーションを絶えず使用中のソフトウェアのレベルに合わせておく必要がある。

4.3　信頼性の証明

信頼性の高ソフトウェアでは，つぎの要因がうまくミックスされている：①経験者，②ソフトウェア開発活動の組織化，および③ツール。各要因は各種の方法で開発できる。

4.3.1　人間

作成するコードの品質についてみると，熟練者の方が未熟練者の20倍も効率がよい。人間の選択および訓練を適正にし，また経験を深めることにより，コードの信頼性を向上させることができる。国防総省では，各種レベルの業務感覚に対する適性に応じて要員の選別をするため，経歴調査を行っている。

4.3.2　ソフトウェアの開発

よくできたプログラムに信頼をおくのは当然である。製作品としてのソフトウェアは，その製作管理の質を反映する鏡なのだから，製作法がよければ良い製品ができることになる。すなわち，信頼性評価法（開発方法の吟味）を用いて，製

品の信頼性を見抜くことができる。下記ステップによって，プログラム作成の全体を概観することができる：

① 標準規格，品質管理法，マネジメント・コントロールの評価。ドキュメンテーションは適正か，読みやすいか，使用は適正か。

② 製作状況を管理者が視覚的にとらえることのできるような方法をもとめる。データは意味のあるものか。

③ 上記のマネジメントおよびプログラミング法を実施にうつすための採用する自動化の度合いの決定。

④ 監査チームを設け，上記のマネジメントおよびプログラミング手法と合致するかどうかプログラムを徹底的に検討する。ドキュメンテーションは適正か。

⑤ 従前の監査，審査，およびテストで見つかった問題点に対するプロセデュアおよび補正措置の経歴を検討する。問題点の補正に対する措置は有意義であったか，製作状況は改善されたか。

4.3.3 ツール

ツールがよければ，熟練度の効果は増幅され，さらに，品質，適時性，プログラム開発コントロールに対する信頼感を増すことによって信頼性評価を高める。重要なツールとしては下記のものがある：

① 生産用ツール：言語プロセッサおよびコンパイラテストケース・ジェネレータ，プログラム作成ライブラリ，ベリファイア，定理証明，アサーション・ジェネレータ。

② マネジメント・ツール：構成制御，状況モニタ，スタンダード，品質管理手順，エラーおよび変更コントロール，コスト・コントロール，モジュールと機能との結合環。

③ ドキュメンテーション・ツール：フローチャーター，ワード・プロセッサ，ドキュメント・ライブラリ，変更コントロール。

④ 監査ツール：欠陥リスト，浸透分析，テストケース，フローチャーター，

およびテスト反復用の冗長かつ独立した生産ツール（例：任意に選択したモジュールを監査コンパイラでコンパイルし，システム中で置換して得た対象コードをテストする）。

5．他のセッションに及ぼすプログラム・インテグリティのインパクト

プログラム・インテグリティを多面的な問題としてとらえてきたが，これは他のワークショップでの議論に大きなインパクトを与えた。セッションごとに要約してみたい。

5.1　内部監査標準

内部監査標準が本セッションにおけるガイダンスを反映していることがまず重要である。とくに，各機関ごとの独自の評価（6.3の指摘を参照）を重視する。

5.2　資格および訓練

プログラム・インテグリティは複雑な技術的問題なので，監査人は，独立した，経営豊かな，有能な，そしてコンピュータ工学を知悉した専門家の助力を受ける必要がある。

5.3　セキュリティ管理

プログラム・インテグリティの依存度が高いシステム制御データの管理は，しばしば看過される領域の1つである。この問題は，セキュリティ管理に分類され，システム・セキュリティ・オフィサ（ＳＳＯ）の形態をとるものだろう。関係するデータについては，4.2.2項のオンライン・モニタリングおよびコントロールで述べた。また4.2項，強固さの立証で我々が検討した内容も，セキュリティ管理に関係したものである。

5.4　様々なシステム環境における監査考察

本セッションが提起しているプログラム・インテグリティに関するコメントは，分散処理システム，通信プロセッサ，スマート・ターミナル，コントローラ，マイクロコードなどそのアプリケーションの形態に拘らず，全てのソフトウェアに適用できるものであろう。

5.5　管理的・物理的コントロール

オフラインで蓄積されたソフトウェアへのアクセスおよび改変をコントロールする全てのファシリティ・マネジメント機構は，信頼され得るソフトウェアの土台をなすものである。さらに，オンライン・システム・セキュリティ・オフィサ（ＳＳＯ）の問題や，バックアップと回復のためとられる救済活動は，すべからく物理的コントロールに影響を与える。一方，開発要員の数を削減し物理的アクセス・コントロールを増大させることによって，たとえプログラムに欠陥があっても，容認できるリスク・レベルにシステム・インテグリティを維持できることを指摘しておきたい。自然災害や人為的エラーについても，このことはいえる。

5.6　プログラム・インテグリティ

該当せず。

5.7　データ・インテグリティ

システム制御データは，プログラム・インテグリティの一部と見なし得るので，データ・インテグリティは定義上，プログラム・インテグリティにはインパクトを及ぼさない。他方，データ・インテグリティは，プログラム・インテグリティ抜きでは存在し得ない。既存ソフトウェアのインテグリティに疑しい部分がある場合，直ちに関心を振り向け，リスクを低減させる手段がとられねばならない（参照，第6.1項勧告）。

5.8 通信

上述した第5.4項参照。

5.9 処理後監査ツールおよびその技法

第4節プログラム・インテグリティの達成手段の全文が関係する。

5.10 対話式監査ツールおよびその技法

第4節プログラム・インテグリティの達成手段の全文が関係する。

6. 勧　　告

以下に示す勧告案は，プログラム・インテグリティの監査・評価に関し本セッションで合意をみたものである。

6.1 既存ソフトウェア

• 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。とくに鋭敏なアプリケーションにおいては要注意。

• プログラム・インテグリティの監査・評価に用いるツールおよび技法は，限定的ではあるが存在する。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および技法を利用する。

• 物理的，手続的，管理的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。オペレーションおよびメインテナンス（O&M）組織を上位レベルへ改編する。

• アクセス・コントロールおよびユーザ資格のチェックにより利用者数を抑制する。

• 非使用時には当該システムから資産を除去し，資産の放置を防ぐ。同様な効果を得るため，暗号化手法を用いることもできる。

6.2 将来のソフトウェア

• 良好なプログラミング慣行を樹立して，プログラムの全ライフ・サイクルを通じてその生産プロセスを改良する。

• 任務目録，機能的要件，システム仕様，ＨＯＬコード，Ｏ＆Ｍからの開発段階で，プログラム・インテグリティの調和を確保する。

6.3 利用組織

• 利用する各組織は，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て，自己評価を実施しなければならない。セキュリティの脅威に関する関心の程度にもよるが，この取り組みは早ければ早いほど良い。

• 各組織は，既存または将来導入するソフトウェアの開発・取得に際し，プログラム・インテグリティの監査能力を考察しながら詳細なガイドラインを設定すべきである。

7. BIBLIOGRAPHY

Abbott, R.P. et al., "Security Analysis and Enhancements of Computer Operating Systems,"
NBS, NBSIR 76-1041, April 1976.

Branstad, D.K., "Privacy and Protection in Operating Systems,"
IEEE Computer, Jan. 1973, pp 43-46.

Bushkin, A.A., S. I. Scheen, "The Privacy Act of 1974: A Reference Manual for Compliance,"
SDC, May 1976, 183p, $15.00.

Committee on Govt. Operations, U.S. Senate, "Problems Associated with Computer Technology in Federal Programs and Private Industry,"
U.S. Govt. Printing Office, June 1976, 448 p, $3.95.

Committee on Govt. Operations, U.S. Senate, "Computer Security in Federal Programs,"
U.S. Govt. Printing Office, Feb. 1977, 298 p, $2.80.

Engelman, C., "Audit and Surveillance of Multi-Level Computing Systems,"
MITRE Corp., MTR-3207, June, 1975.

Fagan, M.E., "Design and Code Inspections to Reduce Errors in Program Development,"
IBM Systems Journal, Vol 15, No. 3 1976, PP 152-211.

Goodenough, J.B., "Exception Handling: Issues and a Proposed Notation,"
CACM 18, 12, Dec. 1975, pp 683-696.

Gwinn, C.J., "A Concept of Operations for the WWMCCS ADP Security Officer (WASO),"
SDC, TM-WD-7828, Jan. 1977.

Hecht, H., "Fault-Tolerant Software for Real-Time Applications,"
Computing Surveys, 8, 4, Dec. 1976.

Hollingworth, D., S. Glaseman,, M. Hopwood, "Security Test and Evaluation Tools: An Approach to Operating System Security Analysis,"
The Rand Corporation, P-5298, Sept. 1974.

Linde, R.R., "Operating System Penetration,"
AFIPS Conf. Proc., Vol. 44, 1975, pp 361-368.

Linden, T.A., "A Summary of Progress Toward Proving Program Correctness,"
AFIPS Conf. Proc. FJCC, Vol. 41, Part 1, 1972, pp 201-211.

Linden, T.A. "Operating System Structures to Support Security and Reliable Software,"
Computing Surveys, 8, 4, Dec. 1976.

Mair, W.C., D. R. Wood, and K. W. Davis,
Computer Control & Audit, The Institute of Internal Auditors, 2nd Edition, 1976.

Nielson, N.R., et al., "Computer System Integrity Safeguards - System Integrity Maintenance,"
NSF-SRI Project 4059, Grant # DCR 74-23774, Oct. 1976.

Ruder, B. and J.D.MADDEN, "Development of Technical Specifications to Serve as a Basis for Federal Guidelines to Prevent Intentional Computer Misuse,"
NBS-SRI Project 5798, Jan. 1977.

Webb, D., W. Frickel (Ed.), "Proceedings of the NSF Software Auditing Workshop,"
NSF-LLL Conf-760116, Jan. 1976.

Weissman, C., "System Security Analysis/Certification Methodology and Results,"
SDC SP-3728, Oct. 1973.

PART Ⅸ　データ・インテグリティ

議　長　Leonard I. Krauss

Ernst & Ernst

参加者　Robert P. Abbott

EDPオーディット・コントロールズ

N. D. Babic

アトランティック・リッチフィールド・カンパニー

Dwight Catherwood

Ernst & Ernst

Stuart W. Katzke（記録係）

米国標準局

Aileen MacGaham

チェース・マンハッタン銀行

Hubert S. Obstgarten

Ernst & Ernst

Barry S. Silverman

ガルフ・アンド・ウエスターン・インダストリ社

編集者注

議長の経歴紹介

レオナルドI．クラウス氏は，Ernst & Ernst のニューヨーク事務所におけるマネジメント・コンサルティング・サービスのマネジャで，計画とコントロール・システム，データ処理管理，および情報システム・セキュリティのコンサルタントである。システム計画／開発の経験としては，金融機関，製造業者，サービス会社，その他の組織における各種のコンピュータ・アプリケーションがある。

クラウス氏は，かってはＩＢＭおよびユニオン・カーバイト社に関係しており，いくつかの会社の幹部，役員を務め，管理システムの管理者，高級管理システムのプロジェクト・マネジャを歴任したこともある。専門のＩErとして，ＣＤＰ（データ処理資格認定）を受けており，評判の書，Cnmputer Based Management Information Systems, Adminsteringng and Controlling the Company Data Processing Funetion，およびＳＡＦＥ：Security Audit and Field Evaluation for Computer Facilities and Information Systems の著者である。クラウス氏はフェアレイ・ディキンソン大学からビジネス・マネジメント・システムでＭＢＡを，ペンシルバニア州立大学からＩＥでＢＳを与えられており，国際的なマネジメント会議でしばしば講演を行っている。

＜本会議の議題＞

データの完全性：ＡＤＰ環境においてのデータの完全性を評価するために必要な監査アプローチと技法はなにか。

データの完全性は，コンピュータ化されたデータがソース・ドキュメントのデータと同一であり，かつ，偶発的な変更や破壊の危険にさらされていない場合に得られる状態であり，これにはデータの精度とデータの防衛の両方が含まれる。自動意思決定過程に入ってくるコンピュータ作成のデータもまた，考慮されなければならない。

データの完全性は，伝統的に監査の世界で扱われてきた領域である。本会議はＡＤＰ環境に独特なその監査アプローチと技法を確認することを目的とし，その語句の表わす広範な領域にまで及ぶことはしていない。

以下の報告書は，当グループ全員の審査による全会一致のもので，Ｌ．Ｉ．クラウスならびにＳ．Ｗ．カック両氏の筆になるものである。

データの完全性監査

標準開発のための基本構成

1. 序

ＡＤＰセキュリティを監査し評価するためには，望ましくない事象の影響を防止，阻止，検知，限定する安全システムを検査することが必要である。

適切な安全システムとは，リスクの重さと好ましからざる事象に関連する危険性に対応するだけの設計，実施，および一致性の上での特性をもっているものである。望ましからざる事象としては，たとえば，ＡＤＰセンタ・ファイル，データベース・レコードの無許可更新，データ通信ラインの不法盗聴があり，危険性の例としては，資産の破壊，資金の間違った支出，横領，詐欺，人事や専有情報の露出，政治／軍事／競争上の不利益，誤った決定，余分な運転資金，法的／契約上の違約金，重要なＡＤＰサービスの中断，生命の喪失が上げられる。

ＡＤＰのための安全システムの監査，評価には，データの安全性に直接影響する要素と間接に影響する要素があるが，本報告書の目的は，データの安全性の安全策の監査と評価に直接的な影響をもち，かつ，検査のために選定した特定のＡＤＰアプリケーションに関係する要素に限定する。（データの完全性の監査はアプリケーションごとに行われる。）

本報告書の目的から，間接的な影響をもつ要素には，一般的な安全システムの一部で，かつ通常の場合はいかなる１つのＡＤＰアプリケーションにも特定されない物理面，操作面，管理面，ソフトウェア面のセキュリティの手段が含まれる。これらの一般的なセキュリティ手段は，絶対的な重要性をもつものとされており，一般的な安全システムがひどく不十分なところではＡＤＰアプリケーションに対して適切なデータの安全性の安全策は実際上，不可能であることさえある。

データの安全性の安全システム内に不適切な点があることは，ちょうど人間の血圧や細胞カウントの異常が体の他の部分の故障不全を示すように，総合セキュリティ・システム内の弱点を表わすことがよくある。監査人は，たとえデータの安全性の検査範囲にそれらの詳細な研究が入っていなくとも，このような可能性

には注意して，これらを指摘しなければならない。

とくに，データの完全性監査では，審査されるアプリケーション・システム内のあらゆる形式のデータ（たとえば，ソース，入力，処理，出力）の品質に直接，影響を与える方針や手続を評価する必要がある。データの完全性監査の前提条件としては，監査人はデータの完全性と監査の対象，範囲の定義を明確に理解していなければならない。監査の実行では，監査人が最初になすべきことは，アプローチや作業計画を系統だてることであり，その後に監査を実施するため，適当な受け入れられる方法を使用する。監査の過程においては，データの完全性および監査対象の定義を常に心に止めておくことが必要である。

第2章は，データの完全性の定義であり，以後の各章において，データの完全性監査実施のための対象，範囲，アプローチ，および方法を検討する。

2．データの完全性の定義

データの完全性とは，データが（信頼性の定義範囲内で）正確であり，一貫しており，認可されていて，有効，完全である上，あいまいでなく，かつ，時機を得た方法によって指定どおりに処理される時の状態であり，データの完全性監査中，たえずこの定義を参照してみることが大切である。

3．データの完全性監査の目的

データの完全性の定義からして，特室のアプリケーション・システムのデータの完全性監査の目的は，有資格者による下記事項の評価にもとづいて客観的な意見を下すことである。

① データの完全性維持のための既存の方針および手続の一致性

② 既存の方針および手続の妥当性

さらに，一致性ならびに妥当性の評価の結果として，アプリケーション・シス

テムのデータの完全性を強化するための訂正作業を推薦されることもある。さらにまた，監査の完了年月日は特定な基準点になるので，これを記録しておくことも不可欠である。この日付以後のシステムのデータの完全性の状態に関する仮定は，すべて，時が過ぎる程，有効性が欠けてくる。

データの完全性監査を実行する際は，監査目的に常に留意することが肝要である。

4．データの完全性監査の範囲

アプリケーション・システムに関連するデータは，種々の形式をもち，システムの異る部分およびデータを用意し使用する組織における方針，手続によって影響されるので，データの完全性監査の範囲は必然的に広くなる。しかしながら，データの完全性監査にデータの完全性に影響を与える関連システム領域全部の検査を含めることは，一般的には，実際的でなく，その他の監査手続の部として含まるべき機能には下記の事象の検証がある。

- データ要素によって表わされる根元的な物理的行為（たとえば，カウント，確認，観察など）
- ソフトウェアの完全性コントロール，およびソフトウェア・メインテナンス・コントロール
- 物理面，管理面，および操作面のセキュリティ

前述のデータの完全性監査の目標を達成するためには，既存の方針，手続の妥当性，一致性に関して，下記の領域の評価が必要であり，データの完全性の向上に役立つ場合には適切な推薦を行う必要もある。

データ・ソースの信頼性　自動化されたアプリケーション・システムのデータ・ソースは，そのアプリケーションによって異る。その範囲は手作業によって収集されたデータから自動テラー・マシンやＰＯＳターミナルのような自動データ収録装置で収集されたデータまであり，時としては，ソース・データをフィー

ダ・システムによってアプリケーション・システムへ送信することもある。

ソース・データは，その収集方法がどうであろうと，信頼できるものであることの確証が必要であり，このため，監査人は個々のデータ・ソースが指定された認可済のものであること，取得されたデータは現在時点のタイムリなものであること，出来る限りソースに近く収集されたデータであること，ソース・データの作成／収集／認可の責務分担が十分に確立されていることを検証する必要がある。

ソース・データの準備　生のソース・データの入手後は，ＡＤＰシステムへ投入するための準備がなされなければならないが，この準備には，場合によってはコード系を使用しての，変換とともに他のソース・ドキュメントへの転記が必要である。この変換と転記に続いて，データはＡＤＰシステムへの投入に先立って，マシンが読むことができる形式（たとえば，キーパンチ）に変換されることもある。ソース・データが自動形式で収集される場合や，オンライン・システムへ直接キーインされるケースでは，データ準備のための機能は最小限でよい。データ準備の段階はヒューマン・エラーのチャンスが非常に高く，かつまた，不正目的のためのデータの操作が行われる可能性があるところである。

データ準備作業の管理を評価するためには，データ準備手続と教育プログラムのほかにデータ準備の方針を審査することが必要である。ソース・データ・レコードの精度，認可，完全性を決定する適切なコントロール記録の実体の検証が必要であり，さらに，異るソースからのデータ，または，ソース・ドキュメント間の一貫性と変換精度を確認するためにデータのコード化の構造を審査してみる必要がある。

データ・エントリ管理　データをＡＤＰシステムへ投入する方法は，アプリケーションによって色々と違っている。ある種のシステムでは，自動テラー・マシンやＰＯＳ，光学文字読取り装置のような装置を介してデータの取得と投入が同時に行われ，また一部のシステムでは，オンラインでキーインされたり，あるいはキー・ツー・テープやキー・ツー・ディスクが使用されたりしているが，データがほかのシステムを通してアプリケーション・システムへ投入される場合も

ある。データの準備の段階と同様に，このデータの投入もエラーのチャンスが高く，不正な目的のためのレコード操作が入りやすい。ＡＤＰシステムへのエラー・データの投入を防止し，その不信化を防止するためには，可能な限り，検知・訂正手続を使用しなければならない。

データの投入管理手続の評価では，監査人はまず，精度，完全性，および認可の基準を含めて，使用中の手続を審査してみる必要がある。データの投入要員に与えられている命令だけでなく，教育に関するプログラムと計画も審査する必要があり，エラーの検知・訂正手続を審査し，これがよく守られていることを確認することが絶対条件である。

データ入力の受付け管理　ソース・データが収録され，準備されて，ＡＤＰシステムへ投入される際には，入力データ（トランザクション，マスタ・ファイル／データベースの維持，テーブル，その他）はいくつかの組織領域を通過することがある。ある種のケースでは，データは組織の分散計算ポイントや外部ソースからフィーダ・システムを介してＡＤＰシステムへ入ってくる。入力データがアプリケーション・システムへ投入されるところも含めて，入力データの管理権が変る場合は，入力データのアクセス，認証，精度についての責任を定義する受付け管理手続きがなされなければならない。

データの完全性監査の一部として，入力データの管理権が変る各コントロール・ポイントにおいて，入力データ受入れ管理手続きを評価することが必要であり，この評価には，責任についての入力データ受入れ手続きの審査と，入力データのアクセスと認証管理の審査が含まれなければならない。さらにまた，入力データ記録の精度と完全性を決定する適切なコントロール，記録の実体を検証する必要がある。

データの有効性検査とエラーの訂正　入力データのＡＤＰシステムでの使用に先立って，エラー・データを発見するために，データは慎重にその有効性の確認（編集，チェックなど）が行われなければならない。もし，エラーが発見されたときは，訂正した後，再投入する必要がある。したがって，データの完全性監

査に際しては，データの有効性の確認とエラー訂正手続きを評価することが必要であり，これには現存の手続きの完全な審査が必要になる ── 必要な場合には訂正作業についての推薦事項も含む。

データの有効性確認のための手作業手続きが自動制御に変っている場合は，所期の有効性確認機能が実行されているかどうかを確認するために，この自動制御を審査しなければならない。最後に，エラー・リジェクト，訂正，データ再投入の各処理の管理を審査する必要がある。

処理仕様　アプリケーション・システムにおけるデータの完全性に影響する重要な要素は，仕様どおりの公式や規則に従って処理が行われている保証である。理想的には，このような処理仕様は形式化して，システム文書とともに記録しておくべきであるが，これらの仕様は形式化されておらず，いかなる形の文書化もされてなくて，僅かの人々が知っているに過ぎないことがよくあり，また，そのどっちつかずの状態におかれているケースもある。

処理仕様はどのような形式であるにせよ，データの完全性監査の一部として評価されなければならないものであり，この評価にはすべての処理仕様の審査とＡＤＰシステム内および処理に影響を及ぼすシステム・コンポーネント間の処理コントロールの審査が含まれる。この評価は固有ファイル，内部発生データ，プログラム・シーケンス，内密の変形，アクセス（ユーザの認別／認証／認可）の処理に関係する種類の管理，手続き，および安全性にまたがるものであり，さらに加えて，アプリケーション・システムの処理仕様の評価の一部として，バックアップ，回復，および再開の手続きも審査されなければならない。

安定したデータ・システムは，意外な動作をすることはなく，予定されたとおりに仕様に従って行動するが，仕様どおりに失敗事故も起すもので，失敗事故のときだけでなく，期待どおりに機能しているときでも予言可能なレスポンスを示すものであることに留意する必要がある。

出力管理と配分手続　コンピュータ化された出力の精度，信頼性および適時性と認可されている各人への出力へのアクセスとその配分は，データの完全性に

影響を与える要素である。データの完全性の監査の一部として，出力リポートと作成された磁気媒体の品質を保証する内部（すなわち，自動化）コントロールも出力のアクセス／配分手続同様に評価さるべきであり，さらに，出力形式のコントロール手続きの審査も必要である。

監査性　データの完全性の監査の目的を達成できる可能性は，審査するアプリケーション・システムの監査性によって大きく左右される。監査性には，データの完全性の監査の実施に必要な情報と文書が利用可能であり，かつタイムリで十分であることを保証するための手続きと方針が整備されていることが必要である。したがって，データの完全性の監査の一部として，ＡＤＰシステムの監査性を評価する必要がある。

この評価には，監査，バックアップ，および回復のために保持されるデータの質と量の審査，それらの保存期間の長さの審査，およびシステム文書の通用性と完全さの審査が含まれなければならない。さらに，監査証跡メカニズムの存在が必要であるし，その文書は現行の完全なものである必要がある。一般的には，監査性の評価には監査目的をサポートする情報を維持するためは方針と手続きが含まれなければならない。

5．データの完全性監査へのアプローチ

データの完全性監査の成功は，アプリケーション・システムを監査するためのアプローチや作業計画の完璧な作成にかかっている。作業計画の立案に際しては，データの完全性の定義，およびデータの完全性監査の目的と範囲から焦点を外さないことが重要であり，これらに留意しながら，作業計画の作成には下記の諸作業をもり込むことが必要である。

- 審査対象のアプリケーション・システムに関する編成組織，方針，手続，および実行を理解する。
- 予定の目的や機能，ユーザ団体からの要求，入力データのソースと流れ，処

理の必要条件，出力の要求事項，関係のある時間的拘束のような要素を含めてのアプリケーション・システム一般を理解する。

- アプリケーションを通して使用される特定のデータ・ファイル，入力，処理ステップ，他のアプリケーションとのインターフェイス，および出力を確認する。
- データの完全性に影響する特定のコントロール特性やポイントを確認する。
- アプリケーションを審査する場合に強調すべきデータの完全性への潜在的な脅威を確認する。
- 監査の実行時に使用する方法論（すなわち，監査ツールと方法）を決定する。
- 雇用と契約期間，従業員のモラル，休暇，仕事のローテーションのような人事面だけでなくユーザ・インターフェースの人間工学的な面も含めて，アプリケーション・システムに影響を与える人間関係の要素を理解する。
- アプリケーション・システムで使用されるハードウェア，ソフトウェア，およびシステム技術を理解する。
- 組織側の訓練計画と継続教育プログラムを理解する。
- アプリケーション・システムの開発，実施，および保守の管理を理解する。
- 発見事項，結論の報告形式と監査勧告を決定する。
- 技術的に高質な監査を保証できる監査に必要な審査手続を決定する。
- 監査スタッフとプロジェクトのコントロール方式を決定する。

特定のアプリケーション・システムのデータの完全性監査のための目標，範囲，アプローチ，および作業計画の設定後は，適当な監査ツールと方法を使用して監査を実行する。監査の後は，監査人が勧告を作成し，これを適当な管理者が審査した後に最終形式で提出される。もし，修正方法が推薦されている場合には，最終的にデータの完全性に責任を持つ管理者が作業計画に関する回答を文書で提出するようにすべきである。

6．データの完全性の監査方法

監査の実施段階では，審査対象のアプリケーション・システムにおけるデータの完全性の保証を目的とする方針と手続きの妥当性と，これが守られている事実を確認するために多種多様な監査ツールと方法(注)を利用することができる。以下，その数例について述べる。

- データの正確度，完全性，および一貫性を保証するためのユーザ，カストマ，ベンダー，その他，十分にデータに精通している人々による確認。（現場検査の技法として実行される場合以外は，確認は他の監査手続の一部となる。しかしながら，監査の目的と範囲を決定する際には，確認によって，データの完全性監査の結果を慎重に考慮しなければならない。）
- サンプリング技法，データの状態を判定するためにデータ集団の一部，通常はランダムに選択されたアイテムを検査する。発見サンプリングの目的はエラーの存在を明らかにすることである。エラーが発見された場合は，さらにサンプルをとって，測定サンプリングを適用する。測定サンプリングは汚染度を予測する目的のためのサンプル・データに統計的技法を応用することによって，データベース中のエラーの範囲を測定するために使用される。属性サンプリングは，レコード自体の特質の矛盾性（たとえば，信用限度額を10パーセント以上超過している受取り勘定残）にもとづいてレコードを選択するために使用することができるし，また，母集団中の特定な特質の存在をテストするためにも使用することが可能である。

(注)　1977年，Institute of Internal Auditors(Altamonte Springs，Florida 32701）発行のAudit Practicesリポートに25種類以上の監査技法の検討が記載されている。これはＳＡＣ（Systems Auditability and Control)Studyのレポートのうちの１つである。

- 並行処理，アプリケーション・システムによるデータ処理の正確さをチェックするための技法で，これを使用すると，アプリケーション・システムによって処理されるデータが，同一の機能を実行する独立プログラムによって処理される。その後に，２つの結果が比較される。
- インテグレーティッド・テスト・ファシリティ（ＩＴＦ），監査人はデータベース中にダミーのマスタ・レコードを投入することによって，アプリケーション・システムの動作を連続的に監視することが可能になる。このようなレコードを配置した後は，通常の処理サイクルの間に，テスト・トランザクションを実用データに包含することによって，これらのレコードに対してテスト・トランザクションの処理を行うことができる。監査人はその後で，処理結果を予め定めた結果と比較する。
- システム・コントロール・オーディット・レビュー・ファイル（ＳＣＡＲＦ）監査人の設計によるテスト機能をアプリケーション・システムのプログラム・コード中に投入し，これによって，通常の処理の間に，処理データで監査テストが実行される。希望のレコードの抽出とその審査ファイルへの書き出しには，例外処理か，あるいは予め決定しておいたサンプル解答基準が使用される。その後，監査人が審査ファイルを検査して，適当な結論を引き出す。
- トレーシング，この機能によって，監査人は特別にマークをつけた，つまり，タグをつけた入力トランザクションをアプリケーション・システムによって処理される際に，追跡することが可能になる。これには，アプリケーション・システムにコードを追加し，トランザクションにはタグのフィールドを付加することが必要である。このコードによって，監査人が処理の正確性を判定するために分析するマーク付きトランザクションの処理記録，または証跡が作成される。
- 要員の観察，目視，電子装置，あるいは写真を利用して要員を観察することは，監査人が現在の方針，手続きの妥当性とそれらが守られているかどうかを，また，誤った動作や不正な行動を判定する際に有効である。

- 現存データの照会による分析，矛盾した関係が存在するかどうか（たとえば，データとソース・ドキュメントや他のレコードの間の不符合）を判定するために行われる勘定，残高，あるいはその他の示唆的なヒストリー・データの検査である。
- テスト・デック／テスト・データ，新しい，または修正後のアプリケーション・プログラムの稼働前のテスト，および，アプリケーション・システムの処理の完全性のテストに使用することができる。いずれの場合も，一連のテスト入力トランザクションをアプリケーション・システムで処理し，結果を予め定めた結果と比較する。
- インタビュー，管理層やユーザ，システム要員との公式・非公式の面接を利用して，システムのドキュメンテーションを補足し，現存の方針，手続きの理解を深め，かつ，これらの方針，手続きとの一致性を調べることができる。
- プログラム・ソース・コードの審査，データの完全性監査が目的の場合は，最後の手段としてのみに使用すべきである。ファイル形式やプロセス，ステップ，コントロールの解説に関する情報が必要なときは，レコード・レイアウトやシステム・フローチャート，プログラム・ロジック・フローチャート，プログラム解説書のような他の資料を使用する方がよい。プログラム・リストの分析には，非常な時間がかかり，かつ普通は，プログラミングの練度と特定のプログラミング言語の詳細な知識が要求される。ほかの書類が不十分であるか，あるいは，存在しないときは，プログラム・リストが最も最新な情報を提供できる。したがって，ソース・コードのある程度の審査は必要なこともある。
- 質問表による調査，アプリケーション・システムに関する情報を入手し，コントロールの妥当性とその一致性を評価判定するための伝統的な監査ツールである。給与とか購買，棚卸しなど，特定タイプのアプリケーション用に作成されている場合が最も効果的であり，これによって，さらに完全な評価のための予備情報が得られる。

○ コード分析とマッピング，これを実行するには，おのおののプログラム・ステートメントが何回実行されたかを判定するために，プログラムを実行中に分析するソフトウェア測定ツールが必要である。マッピングは，最初はプログラムの開発を助けることが目的だったが，監査人のプログラム動作の評価にも使用することができる。しかしながら，これを使用するためには，監査人がアプリケーション・システムの構造とアプリケーション・プログラムの両方を理解できるだけの基礎をもっていることが必要である。

○ 自動フローチャーティング・ソフトウェア，プログラム・ソース・ステートメントを，プログラム・ロジックを図表で説明するフローチャートに変換するソフトウェア・ルーチンで構成されている。フローチャーティング・ソフトウェアを使用すると，プログラム・ロジックの理解が容易になると同時に，監査人はアプリケーション・システムの審査の際に現行のフローチャートを間違いなく使用できるわけである。しかしながら，フローチャートを読むには，通常はある程度のプログラミング知識が要求される。フローチャートが最も有用になるのは監査人が特定の問題領域を調査するときであり，ソース・コードの審査と同様に，データの完全性の監査ではロジック・フローチャートを読むということの価値に一定の限度がある。

○ 手順の通読，監査人がそのソースから処理の完了まで，システムの全般を通して特定のトランザクションの流れを追ってみることであり，監査人はこれによって，自身のシステム動作の理解の正しさを検証し，システムが現存のドキュメンテーションに記載されているとおり機能しているかをチェックできるし，また，ドキュメンテーションが不十分だったり，存在しない場合には実際のシステム活動を判定することができる。この方法をコード分析，マッピング，およびフローチャーティング・ソフトウェアと連結して使用すれば，監査人はシステムの手作業機能と自動化機能の両方の全体を理解することが可能である。

○ 秘密観察，システム要員に観察していることを気づかれずに，通常のシステ

ム・オペレーションを観察するチャンスが得られる。これによって，監査人は，所定の方針と手続きが常に守られているかどうかを判定し，もしシステム要員が観察されていることを知ったなら行わないであろう行動を検知することが可能である。この種の行動には，従業員による不正手段や横領も含まれる。

- 不意の訪問，秘密観察と同じく，監査人はこれによって，通常のオペレーション状態のシステムを観察することができる。監査を予告した場合には，要員の懸念をかもして，非常によい行動をまねき易くなる。
- システムの行動ログの分析，トランザクションやアクセス，ライブラリ，オペレーション・ログ，コンソール・ログなどは現在の方針と手続きの一致性の評価に有用なものである。これらのログの分析によって，監査人は，その意図する目的にはログが不十分である事実，あるいは，分析にもとづいて現在の方針と手続きが不十分であったり，守られていないことの決定を下すことが可能である。
- 連続モニタと監視ソフトウェア，ソフトウェアのモニタは，資源の利用とシステムのボトルネックを判定する目的でアプリケーション・システムと並行に実行されるプログラムであり，監視ソフトウェアは処理の間にエラーまたは例外的な事象を検知する目的でアプリケーション・システムのリアルタイム・モニタを可能にするものである。監視ソフトウェアの特殊な例には，前に述べたＩＴＦとＳＣＡＲＦがある。

PART X コミュニケーション

議　長　Jerry Fitz Gerald

SRI

参加者　Dennis K. Branstad（記録係）

米国標準局

Lynne E. Devnew

IBM

Milton Lieberman

Merrill, Lynch, Pierce, Fenner, and Smith

Robert Morris

ATT

Fred A. Stahl

コロンビア大学

Ren Sussman

ベル・ラボラトリ

編集者注

議長の経歴紹介

ジェリー・フィッツジェラルド博士は，以前にはスタンフォード研究所で管理システムのシニア・コンサルタントを努めたことがあるが，現在はジェリー・フイッツジェラルド&アソシエーツを主宰している。博士はまた，ビジネス・データ処理／EDP監査に関する州立大学の准教授，大医療センタのシステム・エンジニア，コンピュータ・メーカの上級システム分析者，薬品会社のIErを歴任している。

氏は専門職として，財政／産業組織，病院／医療センタ，教育施設用のコンピ

ュータ・ベースおよび手作業システムの計画と開発に造詣が深く，ＥＤＰ監査，ＥＤＰセキュリティ，データ通信の専門家でもある。氏はＩＥ（ミシガン大学，ＢＳ）と業務管理（サンタクララ大学，ＭＢＡ）の学位を持ち，さらに，クレアモント大学院から経済学のＭＡと業務のＰｈ．Ｄを受けている。氏の最近の著書には下記のものがある。

Fundamentals of Data Communications　　Wiley/Hamilton(印刷中)

"In-House Staff Versus Outside Consultants"

Proc. of Academy of Management, 35回年次総会，ニューオリンズ La, 1975年

"Auditing EDP System; Eight Areas of Control", Data : Its Use, Organization, and Management, Proc. of Pacific '75ACM Conf.

教科書，Fundamentals of Systems Analyses

John wiley and sons 1973年

氏はAcademy of Managementの会員である。

＜本会議の議題＞

通信：ＡＤＰ環境における通信を評価するには，どんな監査アプローチと技法があるか。ハードウェア，ソフトウェア，およびプロトコルの考察を含む。

データ通信は，通信チャネルを介してのあるポイントから他のポイントへのデータ・メッセージの交換であると簡単に定義することができる。種々のネットワーク構成で専用，またはダイヤル－アップ施設が使用できる。

本会議の目的は，各種の通信環境を分析して，監査人が効果的な評価を行うために考慮すべき主要事項を確認することであり，このような評価活動のための監査アプローチと技法の開発が必要である。

以下は，本会議の全員によって作成，審査された全会一致の報告書である。

データ通信ネットワークの監査とコメントロールに関する報告

ジェリー・フィッツジェラルド（議長）

デニス　K．ブランスタッド

リン　E．デブニュウ

ミルトン・リー・ペルマン

ロバート・モリス

フレッド　A・スタール

ケン・サスマン

1．　序

本章では，データ通信のセキュリティ監査の実施に際して利用することができる一連の規準よりは，むしろガイドラインについて述べる。委員会の意図する目的は，この報告書によって，政府機関，私企業を問わず，ＥＤＰ監査人達がそれぞれの組織のデータ通信ネットワークの監査方法を開発する際に，準拠することができる基礎を設定することであり，この領域においてさらに研究を続けることによって，これらのガイドラインを拡大増補し，政府機関や私企業のデータ通信ネットワークの監査に利用できる一連の規準を開発することができよう。

特別データ通信監査の定義

実行可能な監査には多数のタイプがある。この報告書は，データ通信ネットワークを利用するコンピュータ・システムのみを対象にする特殊なタイプの監査に関するもので，さらに，このようなシステムのデータ通信部門の審査に限定されている。特別データ通信監査には，エンド・ツー・エンド・ネットワーク，その関連ハードウェアとソフトウェア，およびそれらの要員が含まれる。ネットワークを介して送信された情報の安全性がその発生点から最終目的地点まで，適切に防御されているかを判定するためには，この種の監査が定期的に行われることが必要であり，その頻度はネットワークを利用するデータとアプリケーションの機密性にもとづいて決定する必要がある。また，ネットワーク全体の完全性にそれ

らしき疑が生じたときはいつでも，データ通信監査を行わなければならない。

危険性

データ通信ネットワークは，他のすべてのビジネス・インフォメーション・システムが同様に直面する内容も含んで，いくつかの危険性にさらされることがある。この監査の目的からして，この研究集会では，これらの危険性を下記のように類別した。（これらの定義づけは本報告の3にある。）

- エラーと脱落
- 被害と破壊
- 完全性の喪失
- 露出
- 背信
- 資源の盗用

データ通信ネットワークの監査方法

データ通信監査を実施するＥＤＰ監査人は，データ通信システムのオペレーション，すなわち，メッセージが通信リンクを介してどのように送信されるかについての一般的な知識をもっていることが前提である。

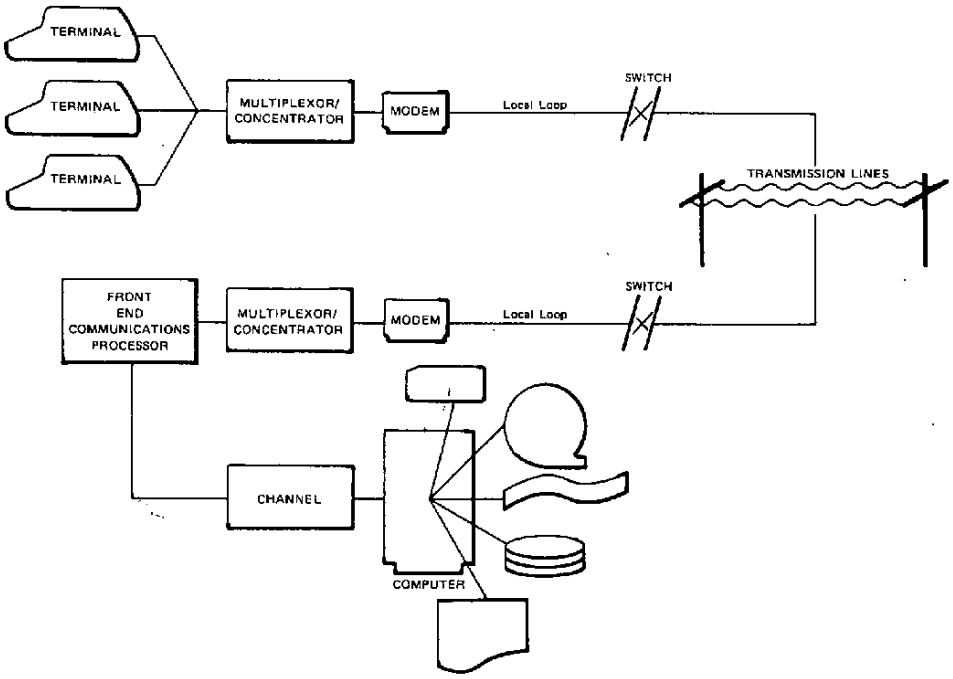
委員会の意見では，データ通信監査は，トランザクション・フロー分析の方式で行われるべきである。トランザクション・フロー分析は，１つのトランザクションまたは一群のトランザクションが，最初の投入点（ターミナル）からデータ通信ネットワークを通ってコンピュータに至るまでを追跡する技法であり，この技法を使用すれば，監査人はトランザクションの流れ，ハードウェア／ソフトウェア，送信媒体，さらにある場合にはネットワークを操作する要員を含めた手作業のインタフェース・コントロールの評価を行うことが可能である。委員会の考えでは，ネットワークの両端（ターミナルとコンピュータ）からトランザクションの流れをトレースして，発見事項を整理してゆく方法が賢明である。監査はデータ通信ネットワークを使用する個々の秘密性の高いアプリケーションだけでなく，データ通信システム全般についても実施さるべきものである。

本報告書には，監査の１つの補助手段として，各種の資源（ターミナル，分散インテリジェンス，通信ライン，その他）と前に述べた危険性（エラーと脱落，災害／破壊，完全性の喪失，その他）を関連づけるマトリックスが記載されているので，これによって，監査人はどの資源がどんなタイプの危険性をもち易いかの判断をすることができる。資源は下記のとおりであり本報告書の第３章に定義されている（Ｘ－１図には，ターミナルからコンピュータに至るまでの資源が記載されている）。

- ターミナル
- 分散インテリジェンス
- モデム
- ローカル・ループ
- ライン・ダイアル式，ポイント・ツー・ポイント，マルチポイント，およびループ
- マルチプレクサ，集信装置，スイッチ
- フロント・エンド
- コンピュータ
- ソフトウェア
- 要員

安全対策マトリックス（Ｘ－１表）の左側の縦列には資源，上部の横列には危険性が記入されており，マトリックの各セルには監査人がネットワークのセキュリティをレビューする場合に考慮すべき各種の安全対策が入っている。安全対策には下記のものがあり，本報告書の第３章におのおのの定義が示されている。

(1) 物理的セキュリティ・コントロール
(2) 監査の手がかり
(3) バックアップ
(4) 回復手続
(5) エラー検出／訂正



X－1図　エンド・ツー・エンド・データ通信ネットワーク

(6)　認　　証

(7)　暗号化

(8)　オペレーション手続き

(9)　予防保全

(10)　フォーマット・チェック

(11)　保険

(12)　法的契約

(13)　故障分離／診断

(14)　訓練／教育

(15)　ドキュメンテーション

(16)　テスト

(17)　報告と統計

監査の実施においては，１つの危険性をもっている資源はいずれも監査人が考慮すべき何らかの安全対策を必ず持つべきであり，これを実行するためには，監

X－1表　データ通信ネットワーク監査のための安全対策マトリックス

危険性 / 資源	エラー，脱落	災害破壊	安全性の喪失	露出	背信	資源の盗用
ターミナル	2, 3, 5, 9, 13	1, 3. 4, 8, 11	1, 2, 5, 6, 8, 13	1, 2, 6. 11, 13, 17	1, 2, 6, 8	1, 2, 6, 17
分散型インテリジェンス	2, 3, 5, 6, 9, 10 13, 16	1, 3, 4, 8, 11	1, 2, 5, 6, 8, 13, 16	1, 11, 13, 16	1, 2, 8	1
モデム	3, 5, 9, 13	1, 3, 8, 11	1, 13	1, 11. 13	1	1
ローカル・ループ	3, 5, 9, 13	1, 3, 8,	1, 5, 6, 7, 13	1, 7, 11, 13		
ライン：ダイヤル・アップ，ポイント・ツー・ポイント，マルチポイント・ループ	3, 5, 9, 13	3, 4, 8, 17	5, 6, 7, 13	1, 7, 11 13		
MUX／CONC／スイッチ	3, 5, 9, 13, 16	1, 3, 8, 11	1, 2, 3, 4, 5, 6, 7, 8, 13 16	1, 7, 11, 13	1, 2, 6, 8	1, 2, 6,
フロント・エンド	2, 3, 4, 5, 9,10, 13, 16, 17	1, 3, 8, 11	1, 2, 3, 4, 5, 6, 8, 10, 13, 16	1, 7, 13, 16	1, 2, 6, 8	1, 2, 6,
コンピュータ	2, 3, 4, 5, 8, 9, 10, 13, 14, 15, 16, 17,	1, 3, 4, 8, 11	1, 2, 3, 4, 5, 6, 8, 10, 13, 16	1, 7, 13, 16	1, 2, 6, 8	1, 2, 6, 17
ソフトウェア	3, 4, 5, 8, 13, 15, 16, 17	1, 3, 4, 11, 15	1, 2, 3, 4, 5, 6, 8, 10, 13, 16	1, 7, 13, 16	6, 8, 12, 15, 16, 17	1, 2, 6, 12, 17,
人	1, 2, 3, 4, 6, 8, 10, 11, 13, 14, 15, 17	1, 3, 8, 11, 12, 15	1, 2, 5, 6, 8, 11, 12, 14, 15, 16, 17	1, 2, 6, 8, 12, 13, 14, 17	1, 2, 6, 8, 11, 12, 17,	2, 14, 15, 17,

査人はデータ通信ネットワークを"視察"して，個々の資源のその危険性に対する安全対策を特定のアプリケーション・システムとの関連で評価すればよい。ここが重要な点である。通信のセキュリティのレビューのためには，マトリックスはデータ通信ネットワークを利用する個々のアプリケーションに照らして利用されなければならない。

制　約

この報告書の目的は，データ通信監査を実施するための企業／政府機関用の規準の設定に通じる今後の研究の基礎を提供することである。資源対危険性のマトリックスは現にデータ通信ネットワークを使用中の各アプリケーション・システムのレビューに利用さるべきものであるが，これには認識すべき若干の制約があることに注意する必要がある。制約はつぎのとおりである。

- マトリックスに記載されている安全対策は，単なるガイドラインであって規準ではなく，また，特定のアプリケーション・システムに関して，そのすべてを含むものであると考えてはならない。
- 記載の安全対策は，データ通信システムの安定を計るための一助であり，セキュリティは相対的なものであって絶対的なものではない点が強調されなければならない。
- 記載の安全対策は，あらゆるアプリケーションの状態に適用されるものではなく，データ通信の一般的な知識が前提になっている。
- ここで考慮されている安全対策は，本報告書の作成時点（1977年）で使用されている技術の状態にもとづいた方法である。

2．監査マトリックスの使用法

監査マトリックスを使用してデータ通信の安全対策監査を行うには，まず最初に，資源，危険性，および安全対策についての委員会の定義に精通することが必要である。

監査人はその後で，それぞれ機密性が必要なアプリケーションによって使用される個々の資源ごとに，下記の4段階の手順を踏む。

- 左側の縦軸上に資源を求める。
- 横に，各潜在的な危険性を読み出す。
- 特定のアプリケーションがネットワークを使用するとなると，可能性のある安全対策のおのおのの適用性を考える。
- 適用可能なおのおのの安全対策ごとに，現在の実施が十分であるかどうかを評価する。

マトリックスはまた，データ通信システム全般の監査にも使用できる。この場合，手続きは基本的に変化はないが，システム資源と危険性の適用対象をトータル・システムとして評価するように実行されることになる。

3．資源，危険性，および安全対策の定義

資源

下記の10種類の資源によってエンド・ツー・エンドのデータ通信ネットワーク（X－1図）が構成される。この章では，マトリックス（X－1表）の資源のおのおのを定義する。

- ターミナル――コンピュータが識別することができる情報の入力／出力に使用される装置。
- 分散インテリジェンス――エラー検出／訂正，認証，メッセージの形式化，データの有効性検査とチェック・サム，プロトコル，およびターミナルから送信されたデータの完全性を確認するための論理的・算術的機能の能力をもつ設備。
- モデム――モデム（Modem）は変調器／復調器（MOdulator ／ D E Modulatar）の頭字語である。この機能は，ターミナルからのデータ・シグナルを使用する特定の通信リンク用の電気的形式への変換，あるいは，その逆の変

換をすることである。

- ローカル・ループ――カストマとキャリアとの間の通信施設で，金属対線であるものとする。
- ライン――通信ネットワーク内でリンクとして使用されるコモン・キャリアの施設で，地上施設も衛星施設も含まれる。

－ダイヤル－アップ：スイッチされた電気通信ネットワークとそれに含まれる各種のサービス，たとえば，市外，ＷＡＴＳ，ＣＣＳＡ(Common Control Switching Arrangement)。

－ポイント・ツー・ポイント専用ライン：２点間の専用線施設。

－マルチポイントまたはループ構成専用ライン：２か所以上の点で共用される専用施設。

- マルチプレクサ，集信装置，およびスイッチ――

－マルチプレクサ：独立のエンド・ポイントからのデータ信号を，１つのデータの流れに結合する装置。

－集信装置：インテリジェント・マルチプレクサ。

－スイッチ：スイッチに接続されているいずれかの２本のラインを相互接続する装置。

- フロント－エンド・プロセッサー－コンピュータへの通信ラインを相互接続する装置で，下記の機能の組合せを実行する。

－コードおよび速度の変換

－プロトコル

－エラー検出と訂正

－フォーマット・チェック

－認証

－データの有効性の確認

－統計データの収集

- コンピューター－電子データ処理装置であるが，ここでは，その通信処理能

力のみを指す。

- ソフトウェア――通信アプリケーション処理機能を実行させるコンピュータ命令。
- 要員――データの入力，施設の運転と保守，ソフトウェアの作成，およびデータ通信の環境管理に責任をもつ人々。

危険性

下記の6つの項目は，マトリックスの上部に記入されている危険性の基本領域を示すもので，この章ではデータ通信ネットワークがさらされる基本的な危険性を定義する。

- エラーと脱落――不注意によるか，あるいは自然に発生する問題で，故意や悪意による行動の結果発生するものは除かれる。下記のものがあるが，これに限るわけではない。
  - －不正確なデータ
  - －不完全なデータ
  - －動作不良の装置，ライン，またはソフトウェア
- 災害と破壊（自然と人為）――通信システムが機能するために必要な要員，または施設の破壊や一時的なダウン。これは下記のような自然／人為による災害が原因になる。
  - －コモン・キャリアの故障
  - －公共施設の故障
  - －ハードウェア／ソフトウェアの故障
  - －いずれも破局的な損失の可能性の低い一連の事象の発生
- 完全性の喪失――システムが，そのハードウェア，ソフトウェア，データ，および構成を含めて，意図された状態ではないとき，すなわち事故，不正，悪意の行動にさらされているときに存在する状態であり，単なる露出はこの定義には含まれない。（このマトリックスではエラーと脱落は別に扱われる。
- 露出――情報の無認可の露出。

- 背信－－信用のある立場の人，または担当作業を実施する人やそのグループによるシステム，またはそのデータの完全性の故意による侵害。
- 資源の盗用－－システムの施設，サービスの所定の目的以外の使用。

安全対策

監査人がデータ通信ネットワークのセキュリティをレビューするとき考慮すべき主な安全対策は，下記の17種類である。この章では，おのおのの安全対策の定義を行う。注意しなければならないことは，データ通信ネットワークに適用されるセキュリティ対策は費用が高くつくこともあるということであり，これらの安全対策の適用上の費用対効果を保証するために，脅威に対抗する可能な安全対策についてだけでなく潜在的な脅威についても現実的かつ実際的な評価をすることが非常に重要である。監査人としては，脅威の査定は該当するアプリケーションの潜在的なロスとそのロスの可能性，十分な保護を行うための費用との関連において実施しなければならない。

① 物理的セキュリティ・コントロール－－物理的施設，コンピュータ，データ通信，および関連装置を保護するための施錠，ガード，バッジ，センサー，警報，管理的手段を使用する。これらの安全対策は，コンピュータに対するアクセスの監視とその物理的保護，ならびにデータ通信施設の作為，無作為による事故にもとずく損傷，火災，環境障害からの保護のために必要なものである。これらの安全対策は，セキュリティ上の危険を検知，防止，報告するために使用される。これらの監査は，特定の物理的セキュリティ対策の存在判定とそれらの機能効果，信頼性のテストからなる。

② 監査の手がかり－－おのおのの事象をとりまく，または，これに至る一連の環境と活動を再現，レビュー，検査するに十分なシステム活動の年代記録。選択されたジャーナル，リポートには下記のものが含まれる。

－コンピュータ　ログ・オン／ログ・オフ

－物理的アクセス　ログ・イン／ログ・アウト

－資源の割当てと使用

－入力と出力の一致

－特定事象の頻度

－フォワード／バックワード・トレース

－ネットワークの使用

この安全対策は，セキュリティの危険性を検知，回復，訂正，報告するために利用される。監査では妥当性，完全性，および範囲を判定する。

③ バックアップ――通常オペレーションで使用される資源の交替，二重化に使用される資源が利用できることとその保護。これには，バックアップ資源の定期点検，更新，テストのための文書化された手続きも含まれる。この安全対策は，ロスの防止，訂正，エラーの回復援助のために利用される。監査は，危険に対するバックアップ技法の妥当性を確認する必要がある。

④ 回復手続き――資源をタイムリに費用対効果の効率のよい方法で回復するために使用される動作，手続き，またはシステムで，監査は回復手続きの効力，実行力を判定する。

⑤ エラー検出／訂正――エコー，フォワード・エラー訂正，自動検出，再送のような方法でエラーを検出，訂正するために使用される技法，手続／またはシステム。これには，選択アルゴリズム，パリティ・チェック，チェック・サムなどを介して行われる有効性の確認も含まれる。この安全対策は，エラーの検出と訂正に使用され，監査人は技法，手続き，あるいはシステムの限界を確認する必要がある。

⑥ 認証――ターミナル，ユーザまたはコンピュータの識別，確実性，および適格性の識別と検証。危険性の検知，防止，阻止には確認装置が使用される。下記のものが含まれるが，これに限られているわけではない。

－ユーザのパスワード

－キー

－バッジ

－メッセージの順序づけ

－ターミナル／コンピュータのコールバック

－ネットワーク・プロトコル

－暗号化

監査人は安全対策の存在と完全性を判定する。

⑦ 暗号化――データの本来の内容を隠したり，気づかない修正を防止するためのデータの変形で，考慮すべき事項は下記のとおりである。

－ある種の規準，たとえば，ＮＢＳデータ暗号化規準に正確に合致するように規定される。

－その通信システムとデータの弱性と特性にマッチする。

－暗号化する種々の方法，たとえば，リンク・バイ・リンクやエンド・ツー・エンド。

－使用キーの選定，その変更時の指示，配布のコントロールのための管理手続きが必要である。

－適当な費用／危険分析で正当化されるときは将来のアプリケーションのシステム設計との統合を計る。

－キーの配分，装置の初期化と同期化，通信エラーからの回復のための間接費を加える。

監査人は，まずシステムとデータの弱性を評価し，暗号化システムの目的をレビューした後，暗号化のための物理的，管理的手続の有効性を測定する必要がある。

⑧ オペレーション手続き――下記のような，データ通信システムのセキュリティ対策のための管理諸規則や方針，ならびに日常の活動。

－１つの組織に対するＡＤＰセキュリティの目的，とくにデータ通信に関係するものの仕様。

－不測のセキュリティ＂事象＂に対する計画。すべての例外状態と活動の記録を含む。

－管理面でほかの安全対策が実施，維持され，かつ監査も行われていることを

確認する。セキュリティ面の資格を十分に持った人々の背景チェック，セキュリティ・クリアランス，雇用，職務の分担，必須休暇が含まれる。

－好ましくないセキュリティ事象を阻止，検出，防止，修正するために効果的な安全対策の開発。

－費用対効果，効率の改善，信頼性の向上，経済性などの関連利益が期待できる。

監査人は現行の管理諸規則，セキュリティ計画，不測計画，危険性分析の存在，管理目的の各人の理解を調査し，しかる後に，これらを満足させるための特定な手続きの適時性と妥当性をレビューする。

⑨ 予防保全――計画的診断テスト：

清掃，交換，および精度，信頼性，完全性を評価するための装置検査，下記の事項が含まれる。

－テストと修理の予定表を作成する。

－保守要員に対して装置の故障を阻止，防止するだけの時間と資源を確保する。

－各装置の平均故障時間（ＭＴＢＦ）のような故障統計にもとずいて，交換部品を在庫する。

－保守記録を保存して，問題の再発，統計的に予測不能なセキュリティ上の危険の場合，これを分析する。

－無許可の変更（"バギング"など）を検知するために特定の装置に対して，予定外の交換やテストを実施する。これによって，重要な期間での故障の可能性が減少し，また副産物として，資源の無許可変更が検出される。

監査人は保守予定表，記録，部品在庫，"作業休止時間"，費用／修理・交換チャートをレビューし，これらを類似のシステムのものと比較してみる。

⑩ フォーマット・チェック――チェックとバランスを介してデータの妥当性を検証する方法。限界チェック（数字フィールド），レコード・カウント，数字フィールドの英文字，フィールド区切りなどの方法によってデータの入力エラーを検出する自動検証システムを開発する。

監査人は，フォーマット・チェックを利用できる領域を調査し，十分なチェックがなされているかどうかを検査する。

⑪ 保険――重大な損失に対する財政的な防衛。潜在または現実の損失を分担し，長期間，予算措置によって大災害に備え，かつ回復するために保険が利用される。

監査人は他の安全対策によってもっと容易に保護できないか，大災害によって組織が受け入れ難いリスクにさらされることがないかを調査する。

⑫ 法的契約――特定の費用ベースで特定のサービスを実施する契約で，一般的には，特定の責任が生じる。たとえば，保証，利害協約の不一致，クリアランス，非公開協約，その他があるが，ほかにも下記のようなものがある。

－一定のセキュリティ事象に対して責任が発生する協約。

－ある種の行為を実施しない，またはペナルティが発生する契約。

監査人は，法的書類の適性と保護手段をレビューする。

⑬ 故障分離／診断――データ通信の全体を構成している各種のハードウェア／ソフトウェア・コンポーネントの完全性を確認するために使用される技法。これらの技法は定期的ベースか，あるいは故障の発見時に，環境全体を監査して不具合な要素を隔離するために使用される。下記のようなものがある。

－診断ソフトウェア・ルーチン

－電気的ループバック

－テスト・メッセージの作成

－管理，人事手続き

監査人は，故障分離に使用されている技法の妥当性をレビューする必要がある。

⑭ 訓練／教育――従業員の訓練／教育は，問題の防止とその発生時における訂正動作に効果があると同時に，また，責任を明確にし，かつ，従業員に認可された手続きを徹底させるために有用である。

監査人は，実施中の教育方針をレビューしてみる必要がある。

教育には，Whyの説明の場合の訓練教育も含まれている。――なぜセキュリテ

ィとコントロールが組織には重要なのかの問題も含まれる。失敗の潜在的な反動と手続きに従い，コントロールを遵守する必要性にもふれる必要がある。

監査人は，管理者層が教育の必要性と有用性を認識しており，かつ，継続ベースで訓練が実施されていることを確認する必要がある。

⑮ ドキュメンテーション――ドキュメンテーションは，問題の予防，問題の原因の識別，問題からの回復を援助することを目的としたプログラム，ハードウェア，システム構成，および手続きの詳細な記述であり，システムをその各部分から再建する場合に有用であり得るだけの十分な詳細さで書かれていなければならない。

監査人は，合理的に予測される必要性を満足させる程度のドキュメンテーションがなされているかどうかを判定する。

⑯ テスト――完全性を確認するためのハードウェアとソフトウェアの動作確認に使用される技法で，人員テストも含めて，特定されたオペレーションからの離脱を発見するものでなければならない。

監査人は，必要なだけのテストが行われているかどうかの判定をする。

⑰ 報告と統計――データ通信のすべての面の使用状況を明示する情報の収集と報告であり，管理層への例外報告には下記のものがある。

－トラフィック統計

－保守統計

－エラー動作

－時間と活動別のターミナル使用状況

監査人は，将来の計画立案に必要なだけの報告と統計が存在することを確認する必要がある。

PART XI 処理後監査手段および技法

議 長 Richard D. Webb

トーシュ・ロス会計事務所

Leo Deege

国防総省監査サービス

Philip M. Mclellan

王室カナダ騎馬警察隊

Albrecht J. Neumann（記録係）

米国標準局

Michael J. Sopko

GTEサービス・コーポレーション

Norman Statland

プライス・ウォーターハウス会計事務所

Robert Stone

ユニロイヤル・コーポレーション

編集者注

議長の経歴紹介

リチャード D. ウェッブ氏はトーシュ・ロス会計事務所の役員室の幹事であり，EDP監査方針，EDP監査技法，およびEDP監査教育の責任者である。氏は，イクイティ・ファンディング生命保険会社の粉飾事件で破産管財人のために調査を実施したEDP監査チームの重要な責任者だった人で，監査用ソフトウェア・パッケージの設計・導入の経験をもち，会計・原価計算システムのコンサルタントを努めたこともある。氏は公認会計士（イリノイ州）の資格をもち，米国公認会計士協会（AICPA）の会員であると同時に，同協会の監査ソフトウェ

ア仕様タスクフォースの議長を努めている。またさらに，コンピュータ監査小委員会，ならびにコンピュータ監査技法・アプローチ監査ガイド・プロジェクトチームのメンバーであり，ＡＩＣＰＡ監査ガイド，＂サービス・センタ作成記録の監査＂および＂ＥＤＰシステムの内部監査に関する監査人の教育と評価＂を草案したタスクフォースの委員でもあった。現在はＥＤＰ監査人協会ニューヨーク支部役員でＣＰＡのニューヨーク協会のメンバーである。なお，氏は会計学でミネソタ大学から理学士号（ＢＳ）を受けている。

＜本会議の議題＞

処理後監査のツールと技法：

コンピュータ・セキュリティ監査において各種のシステム・ジャーナルおよびログを有効に使用するために利用可能な，また，必要な監査用ツールと技法はなにか。

コンピュータ・セキュリティを評価しようとする監査人に，重要な情報を提供する多種多様なログやジャーナルが作られており，また，作ることも可能であるが，監査人がしばしば遭遇する２つの大きな問題は情報の圧倒的な量と分析用のツールが十分でないことである。

本会議の目的は，必要な情報の種類とその取得のための最も効果的かつ効率的な方法，および分析のためのツールと技法を検討することであり，開発する必要があるツール，技法はもちろんであるが，現に使用可能なものはなにかの検討がなされなければならない。

以下は，グループ全員によって審査された全会一致の報告書である。

処理後監査のツールと技法

Ａ．Ｊ．ニューマン

Ｎ．スタットランド

Ｒ．Ｄ．ウェッブ

1. 序

この報告書は，処理後監査のためのツールと技法に関して行われた討論と，その結論を要約したものである。この討論は，外部および内部の監査人とセキュリティの専門家，およびコンピュータ志向のジェネラリストが参加して行われたものであり，討論の開始早々に，討論の内容と概念を設定し，これに止まること，基本的な定義事項を検討すること，セキュリティ監査の範囲を決定すること，に定める点についての合意が行われた。

問題の範囲をお互に了解した上で，トータル・システムを，システム・アクセス，入力，処理，および出力の各領域に分割して，利用できるデータの考察を行った。われわれは，まず標準的なセキュリティ監査に必要な情報，すなわちセキュリティ監査を行うために，処理後の場合には監査人としてはどんな情報が必要か，また，今日の環境では通常は入手できないどのような情報が入用かを決定し，つぎに，現存するツールと技法を評価・検討して，必要になる技法を決定することにした。

執筆に当り，マイアミ集会での多くの助言や寄稿，ならびに本報告書の数次にわたる草稿の審査に際して寄せられた。L．ディーグ，P．M．マクレラン，R．ストーン，およびM．J．ソプコ諸氏の建設的な評論に感謝する。

はじめての会議を準備したH．ロビンソン氏は，直前になって緊急事が発生したため，会議には出席できなかったが，氏もまた，本報告書の草案に尽力された一人である。

2．標準的なセキュリティ監査の目的

監査人が行うべき処理後活動の範囲は，セキュリティ監査に関連して述べられるが，これにはデータの機密性，完全性，および可用性も含まれ，また承認済の

手続きがどの程度守られているかの一致性もこれに含まれる。われわれの討論の意図はほとんどセキュリティを必要としないような環境から国家安全保障のレベルにおける諸環境までも包含するものであり，鑑定・意見を目的とする監査，たとえば財務諸表やシステム効力，システム能力，あるいはシステム結果の効率的な活用のようなものでも，とくに意識的に言及したり，除外したりすることはしていない。

こゝでは，システムの性格によって必要とされる情報保護レベルに照らしての管理の存在とその範囲，適切さを判定することがセキュリティ監査の目的であるということに意見が一致した。

特定目的の一部：

a．すべてのトランザクションが完全に処理され，かつ，1度だけの処理であることを確認する（トランザクションのユニーク性）。

b．おのおののトランザクションは完全，正確，かつ，認可されていることを確認する(トランザクションの完全性，正確性および認可管理，すなわちトランザクションの完璧性である）。

c．処理は完全，正確，かつ，認可されたものであったことを確認する（処理の完全性，正確性および認可管理，すなわち処理の完璧性である）。

d．処理結果が許可された受領者にのみ配布されていることを確認する（配布管理）。

e．データ，およびシステム資源の使用は回復可能であったことを確認する（回復管理）。

f．セキュリティ違反の探知，分析能力を確認する（探知，分析能力，すなわち違反管理）。

これらの目的を達成するためには，監査人はまず監査対象になるシステムを"理解"しなければならないことは無論のことであり，セキュリティ監査に関する討論の結果として，下記の定義が定められた。

3．定　　義

コンピュータ・セキュリティ ― 秘密性，完全性および可用性に対する偶発的，または故意の危険からのシステムのデータおよび資源の保護。

コンピュータ・セキュリティ監査 ― コンピュータ・セキュリティ手続きとその適切性，および設定方針がどの程度守られているかの一致性を評価するための方法の検査。

注：この定義は，データ・セキュリティよりはむしろ，概念を拡大して，コンピュータ・セキュリティを扱うものであり，データ・セキュリティを扱ったＦＩＰＳ　ＰＵＢ　３９のセキュリティ監査の定義のみがこゝに述べられている定義に拡大解釈できるように思われる。

処理後監査 ― セキュリティに関する要求事項を含む予め決定されたシステムの必要事項が守られていることを確認するための入力，処理，および出力情報の事後分析。

ログ ― システムのオペレーション中に，特定の目的のためにとられた特定動作をあらわすデータ要素の歴年記録。こゝでは，"データ要素"はそのもっとも広義な意味で使用され，システムの動作に関するデータその他だけでなく，アプリケーション・データも含むものとする。

ツールと技法 ― 技法とは希望の目的を達成する方法である。したがって，技法はいくつかのツールを含んだ手続きからなる場合もあるし，あるいは，いくつかのツールを交替に使用することもあり得る。たとえば，監査ソフトウェアは多くの技法で使用することができる１つのツールである。

トランザクション ― 事象に関するデータの集合。処理されても，リジェクトされた場合でも，監査の立場からは，常に記録される必要がある。この用語はこゝではコンピュータにサービスされる端末のオペレータの動作記録から財務トランザクションやメッセージ本文に至るまで，最も広義な意味で使用される。

4．処理後監査の範囲

処理後監査の範囲は，ＥＤＰシステムの範囲をこえて，手作業と自動化された管理作業のレビューも含むことになるが，こゝでの討論はＥＤＰシステムそのものに関しての技法とツールに限られる。すなわち，データの最初の変換時点から，中間の処理段階，テレコミュニケーションを通じて，出力の配布に至るまでのトランザクション処理に関するものである。処理の形態（すなわち，オンラインとバッチ）は，検討対象のログの一部はいずれか片方の形態にのみ該当するものであっても，形態そのものは制約要素とみなされることはない。監査人はシステムの行動によってもたらされるセキュリティへの影響を判断でき，かつ，変換前と出力後の手作業領域を効果的にレビューできる十分なシステム知識を持っているものと仮定される。 Ⅺ－1図は，処理セキュリティ監査の範囲を示すダイアグラムである。

5．必　要　な　情　報

セキュリティ監査の諸目的を達成するには，一般的にアクセス，入力，処理，および出力の各領域に関する情報が必要であり，監査人はこれらの各領域のレビューを行って，情報の５つの基本タイプ ― 誰，機能，何，状態，時間（表１～表４）を示すログから詳細な情報をさがし出さなければならない。

誰れ ― トランザクションの根拠，すなわち，トランザクションを起動する力を識別するもので，この根拠は人間でも処理でも，手作業のタスク，あるいはプログラムでもよい。

機能 ― ＂エントリ＂，＂読取り要求＂，＂確認＂，＂カウント＂などのような処理動作の記述である。

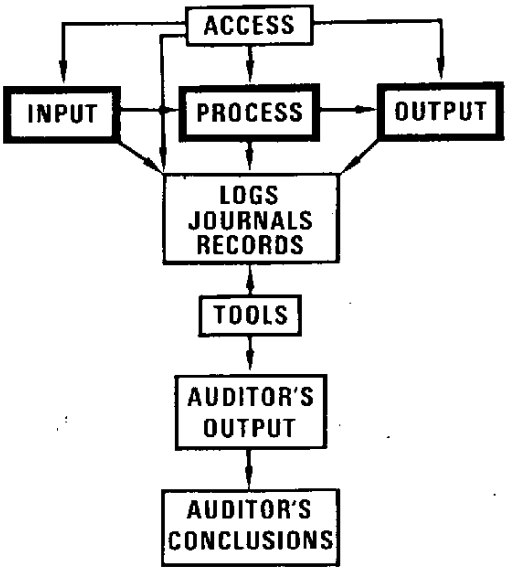
何を ― 処理の対象を識別するもので，対象になるものはファイル，装置，プロ

グラム，あるいはデータ要素である。

状態 ― 機能と関連する根拠および対象に関する情報であり，動作は完全か不完全，正しいか正しくないか，その他である。

時間 ― 記録された動作と情報に関連する日時スタンプで，監査証跡の判定と，一般的には，システムの連続性の追跡に使用可能な基本日時情報を提供するものである。ある場合には，トランザクションまたはレコードの一貫番号が日時スタンプに関連づけられる。

XI－1表から4表までは，代表的な必要情報を表の形で示したものであるが，これらの表はすべてを含むものではなく，いかなる意味でも完全なものと考えてはならない。これらの諸表は，思考の順序手続きを示し，現存システムで入手できる必要なセキュリティ情報と将来のシステムに対して指定すべきもののみチェックに使用できる方法論を示唆するものである。それぞれの表における横列の位置には，時間的なシーケンスはなにもないが，表中の各行は記録，ログして後刻，セキュリティ監査のために処理できるセキュリティ関係情報の基本記録を構成する。



XI－1図　処理後セキュリティ監査

XI－1表　システム・ログ・アクセス・インフォメーション

WHO	FUNCTION	WHAT	STATUS	TIME
USER ID	ENTRY	SYSTEM ID & DEVICE ID	SUCCESSFUL/ UNSUCCESSFUL	D–T
USER ID	EXIT/ RELEASE	SYSTEM ID & DEVICE ID	〃	D–T

D=DATE
T=TIME

XI－2表　インプット・ログ・インフォメーション

WHO	FUNCTION	WHAT	STATUS	TIME
TASK ID	REQUEST TO OPEN FOR READ	RESOURCES I.E. FILES, DEVICES, PROGRAMS DATA	SUCCESSFUL/ UNSUCCESSFUL	D–T
TASK ID	READ	FILE, DATA ELEMENTS	〃	D–T–SN
USER ID	ENTER	TASK ID	〃	D–T

D=DATE　SN=SERIAL #
T=TIME

XI－3表　プロセシング・ログ・インフォメーション

WHO	FUNCTION	WHAT	STATUS	TIME
TASK ID	VALIDATE	TRANSACTION TYPE CONTENT	N/A	N/A
TASK ID	FORMAT LOG RECORD	TRANSACTION	VALID/ INVALID	D–T–SN EACH TRANSACTION
TASK ID	COUNT & SUMMARIZE	〃	N/A	N/A
TASK ID	FORMAT LOG RECORD	TASK COUNTS & SUMS	N/A	D–T–SN
TASK ID	UPDATE	MASTER	N/A	N/A
TASK ID	SAVE	MASTER FILE LOG	NORMAL/ ABNORMAL	D–T–SN OF TRANSACTION
TASK ID	SAVE	PERIODIC BACKUP FILE	N/A	D–T–SN
TASK ID	COUNT & SUMMARIZE	DATA BASE LOGICAL FILE FOR EACH TASK	N/A	D–T–SN

D=DATE　SN=SERIAL #
T=TIME

XI－4表　アウトプット・ログ・インフォメーション

WHO	FUNCTION	WHAT	STATUS	TIME
TASK/ USER ID	REQUEST WRITE (UPDATE)	FILE ID DEVICE ID	SUCCESSFUL/ UNSUCCESSFUL DEVICE/STATUS CHANGE	D–T
TASK ID	WRITE (UPDATE)	DEVICE ID FILE ID MACHINE OR HUMAN READABLE	COMPLETE/ INCOMPLETE	D–T

D=DATE
T=TIME

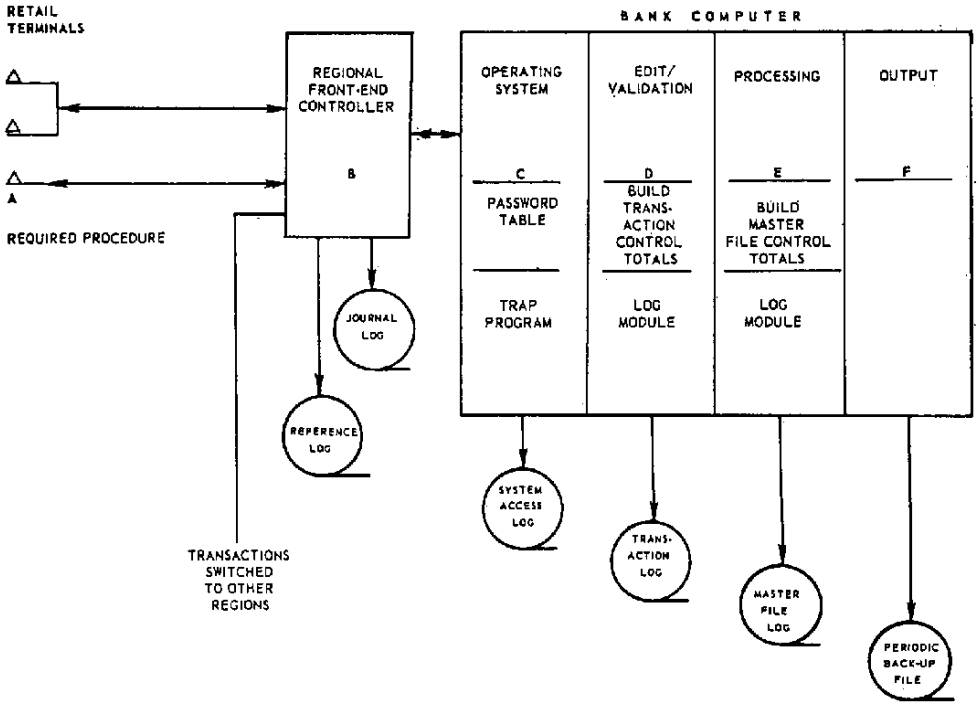
6．代表的な利用可能情報

ほとんどすべての現存システムには，処理後監査に利用できるいろいろな情報がある。会計業務やシステム・メンテナンス，システム・モニタリングのために，各種のログが経常的にとられている。コンソール・ログは，システムの誤動作をコードでエラー・メッセージの項目としてその発生時間と共に記録し，プリント出力することができるし，事象ログでは，成功したエントリの端末およびユーザのＩＤを記録でき，さらに，不成功に終ったエントリとその際に使用されたパスワードの記録をとることも可能である。すべてのユーザ・コマンド，コマンドの時間，端末およびユーザのＩＤもまた記録できる。ＥＤＰ部門会計の立場からすれば，プログラムまたはジョブのラン記録，ビリングで使用された各種の方法（接続時間，ＣＰＵ時間，資源ユニット，その他），ユーザまたは組織のＩＤなどの記録もとっておく必要がある。このような順序のあるものは，セキュリティ監査に利用することが可能であるが，セキュリティ関係情報には動作の時間とタイプ，使用された不認可パスワードの記録，資源管理，違反時に使用されたその手段・方法が含まれなければならない。

7．例題：同時決済システム(ＥＦＴＳ)

ＥＦＴＳ(Electronic Funds Transfer System)における場合のセキュリティ必要情報を以下の各項で説明する。Ⅺ－２図はシステムのブロック・ダイアグラムで，主要なシステム・コンポーネントとセキュリティのために使用される各種のログを示している。１つの地区通信コントローラには，多数の小売端末が接続され，いくつかの地区通信コントローラを銀行のコンピュータへ，あるいは，相互のコントローラと連結することができる。記録とログは，通信コントローラと中央の銀行コンピュータで維持される。

コントローラでは，基準ログとジャーナルが維持され，中央コンピュータには４つの主要ソフトウェア機能 ── オペレーティング・システム，入力機能，処理機能，および出力機能 ── が必要とされるが，これらのすべてに，セキュリティに必要なそれぞれのログと記録が維持される。



Ⅺ－２図　ＥＦＴＳシステム構造におけるセキュリティ考察

7.1 リモート・ターミナル手続き

リモート・ターミナルにおける諸手続きは，各種のログからセキュリティ情報が構成できるように設計されている。該当のファイル・セグメントへのアクセスを制限するために，カストマは個人識別番号で識別される。トランザクションのタイプが投入され，その特定タイプのトランザクションに対するその端末の使用の有効性が確認される。端末の識別には，さらにチェックを追加することもでき，ハードウェア配線でも可能である。信用状況チェック，調整すなわち返済，および高額借入れの承認には，さらに認可コードが要求されることもある。トランザクションの受領確認はすべて，端末で作成される一貫番号で行われる。

7.2 交換用コンピュータにおけるメッセージ・セキュリティ

メッセージは，メッセージ・ヘッダとメッセージの内容で形成される。

7.2.1 メッセージ・ヘッダ

ヘッダには，通常，下記の情報が含まれる。

発動端末のＩＤ

メッセージ・タイプ規制子

優先コード

メッセージ一貫番号（各端末で割当てる）

経路指定子

メッセージの文字カウント

7.2.2 メッセージの受領確認とリリース

メッセージの文字カウントの確認後は，すべてのメッセージは受領ユニット，たとえば，端末，ホスト・コンピュータ，またははかの交換コンピュータがそのメッセージの受領を確認するまで，その交換コンピュータの責任になり，メッセージ・カウントや，発信元コード，宛先コードが不法のものであるときは，同一のメッセージ一貫番号を使って再送要求が行われる。

7.2.3 元帳の均衡

各メッセージごとの入力／出力リストを維持することによって，元帳類は均衡状態が保持される。

7.3　通信プロセッサ・ログ

メッセージの内容は，ジャーナル・ログに記録されるが，メッセージ・ヘッダのデータはすべて基準ログに保持される。

7.4　銀行コンピュータの機能とログ

入力機能は主としてトランザクションの有効性の確認と編集を取扱い，トランザクション・ログが維持される。オペレーティング・システムでシステム・アクセス・ログが維持され，処理機能ではマスターファイル，ログが維持されるが，一方，出力モジュールでは定期的なバックアップ・ファイルが維持されており，システムの故障時にレコードやファイルを再生するために使用することができる。XI－5表は，システム・ログに必要なデータを示すものである。サイン・オンとファイル・エントリには，どのファイルと装置，プログラムが使用されるかを示す関連指示子をもった暗号パスワードが必要である。XI－6表は，入力トランザクションの編集と有効性確認に必要なデータであり，XI－7表と8表はそれぞれ，処理／更新と出力に必要なデータを示す。

8．処理後テクニック

ワーキング・グループによって，いくつかの処理後技法が確認された。特定の技法を使用する場合，監査人はタイミングやコストのような要素をいくつか考慮しなければならないから，こゝでは領域による提示にとどめ，特定な環境においての使用上のガイドラインは与えられない。

8.1 アクセス

8.1.1 成功しないアクセス

誰れがアクセスを行って，なぜ成功しなかったかを判定するために，すべての成功しなかったアクセスをセキュリティ・レベルでリストする。回数と数量を測定する。特定なパターンを確認して，認可表と比べる。これによって，未認可ユーザの発見が容易になる。

XI－5表　オペレーティング・システム

――セキュリティ・アクセス・コントロール・ログ・データ

WHO	FUNCTION	WHAT	STATUS	TIME
SUBSCRIBER ID	SIGN-ON	SYSTEM DEVICE ID	SUCCESSFUL/ UNSUCCESSFUL	D–T
SUBSCRIBER ID	RELEASE	SYSTEM DEVICE ID	SUCCESSFUL/ UNSUCCESSFUL	D–T
SUBSCRIBER ID	ENTER	TASK ID TRANSACTION TYPE	SUCCESSFUL/ UNSUCCESSFUL	D–T
TASK ID	REQUEST TO USE (ACCESS FOR READ)	RESOURCES I.E. FILES, DEVICES, PROGRAMS, JCL PROCEDURES	SUCCESSFUL/ UNSUCCESSFUL	D–T

D=DATE
T=TIME

タスク1と3の完了には，このタスクが使用できるファイルと装置，プログラムなどを示す指示子をもった記憶されている暗号パスワードが使用されることになる。通常でない転送パターンを書止めるには，“トラップ”プログラムを使用する必要がある。

8.1.2 成功したアクセス

使用パターンを決定するためにすべての成功したエントリをリストし，認可表と比べる。

XI－6表　入力トランザクション編集／確認中のセキュリティ関連必須事項

WHO	FUNCTION	WHAT	STATUS	TIME
TASK ID	VALIDATE	TRANSACTION CONTENT	N/A	N/A
TASK ID	FORMAT/ WRITE LOG RECORD	TRANSACTION	VALID/ INVALID	D–T– TRANSACTION SN (INCLUDING TERMINAL)
TASK ID	COUNT & ADD TO CONTROL TOTALS MAINTAINED FOR EACH TERMINAL BY TRANSACTION TYPE	TRANSACTION & SELECTED DATA ELEMENTS	N/A	N/A

D=DATE T=TIME SN=SERIAL #

XI－7表　データ処理／更新中のセキュリティ関連必要事項

WHO	FUNCTION	WHAT	STATUS	TIME
TASK ID	UPDATE	MASTER FILES	N/A	N/A
TASK ID	SAVE	MASTER FILE BEFORE/AFTER IMAGE ON LOG	NORMAL/ ABNORMAL	D–T– TRANSACTION SN
TASK ID	COUNT & ADD TO CONTROL TOTALS	MASTER FILE RECORDS SELECTED DATA ELEMENTS	N/A	D–T– MASTER FILE VN

D=DATE SN=SERIAL #
T=TIME VN=VERSION #

8.1.3　ログの連続性チェック

システム使用中をシステムが指示しなかった時を判定して処理スケジュールとつき合せるために，ログの連続チェックを設定する。システム活動のスケジュール外の中断はすべて解明されなければならない。

8.2　入　力

技法1，2および3の適用はアクセスの項に示されるとおりである。

XI－8表　データ出力時のセキュリティ関連必要事項

WHO	FUNCTION	WHAT	STATUS	TIME
TASK ID	FORMAT SUMMARY RECORDS FOR TRANSACTION & MASTER FILE LOGS	RECORD COUNTS & CONTROL TOTALS OF SELECTED DATA ELEMENTS	N/A	D–T–SN–VN
TASK/ USER ID	REQUEST WRITE/ UPDATE	FILE ID DEVICE ID	SUCCESSFUL/ UNSUCCESSFUL DEVICE STATUS	D–T
TASK ID	WRITE/ UPDATE-IN-PLACE	DEVICE ID FILE ID FOR MACHINE OR VISUAL READ	COMPLETE/ INCOMPLETE	D–T
TASK ID	WRITE	PERIODIC BACKUP FILE	N/A	D–T–SN–VN

D=DATE　SN=SERIAL #
T=TIME　VN=VERSION #

8.3　処　理

処理の完全性とセキュリティをチェックするためには，様々な技法を使用することが可能である。

8.3.1　手作業によるチェック

前に処理された一連のトランザクションを選んで，これを手作業チェックすることによって，１つの実際の，前の処理サイクルの結果を検査することができる。

8.3.2　コントロール・トータル

監査プログラムによって実ファイルのコントロール・トータルを独自に確認することによって，システムが報告したトータルとの照合チェックが可能である。

8.3.3　テスト・データ

予め定められたトータルと照合すべきコントロール・トータルや結果の作成には，システム・テスト・データが使用できる（ベースケース／テストデック）。

8.3.4　ＩＴＦ

監査人が，その管理するファイル・セグメントまたはレコードに対して処理を行う特別のトランザクションを選定する。この方法は，オンライン処理システムの選択された処理パスのテストによく使用される。これは定期的に行っても，あるいは臨時的に予定外に行ってもよく，このＩＴＦ(Integrated Test Facility)は，プログラミングおよびオペレーションの要員に明確な設計も可能なので不正手段の障壁になる。彼等はセキュリティ監査テストが進行していることに気がつかないだろう。

8.3.5 タグ

処理の中間結果を検査するために，本番ラン中にタグをつけたトランザクション（すなわち，監査人が特殊なコードをつけたトランザクション）をトレースする。

8.3.6 拡張レコード・メインテナンス

拡張レコード・メインテナンスは，マスターファイル内にトランザクション・レコードを追加・保持するために使用することができ，マスターファイルの処理歴を得るために利用できる。インライン・データ収集は，データのサンプルを供給し，アプリケーション・プログラムの拡張としての階層を構成する。

8.3.7 トレース

トレースは特定のトランザクションを処理するために使用するプログラム・モジュールやプログラム命令の文書化に利用することができ，これは処理論理の検査とコンピュータ・プログラムの不使用部分の確認に使用される。

8.3.8 マッピング

プログラム・アナライザを使用することによって，どんな条件のときに，おのおののプログラム・モジュールが実行されるかを判定するために必要なロード・イメージ・ライブラリ中に格納されているオブジェクト・プログラム・モジュールのマッピングが可能である。

8.3.9 再コンパイル

ソース・プログラムをコンパイルし直して，その結果のオブジェクト・プログ

ラムで最近のトランザクションのセットを処理することができ，２組の結果を比較してみれば，不適切な処理が検証される。

さらに，現在のソース・プログラムの再コンパイルによるオブジェクト・モジュールはライブラリに格納されている現在の作成モジュールと機械的に比較することが可能であり，この技法によって，ソース・コードには反映されていないオブジェクト・モジュールの修正を確認できる。一たびソース・コードの論理を確認したあとは，監査人が管理するコピーを保持しておいて，以後は作成バージョンと比較することによってプログラムの修正を発見することができよう。

8.3.10　並行シミュレーション

特定の監査テストに関係するアプリケーション・ロジック，計算およびコントロールを選定して使用する並行シミュレーション・プログラムを使って，選択した実際のトランザクションを再処理することができる。重要な計算は別の言語で処理することによって検査できる。

システムの複雑さと柔軟性の程度によることであるが，システムのオペレーションと並行して，汎用的なソフトウェア・パッケージを使用できることもできよう。

8.3.11　検査プログラム

レコード検索プログラムによって，特定の選択基準を満足するか，あるいは統計サンプリング基準の結果として選択されるトランザクションを選択する。将来の分析，調査のためのプリントを作成することも可能である。

8.4　出　力

システム出力のチェックには，つぎの技法が使用される。

8.4.1　出力リスト

出力をリストアップして，予定との一致も含めて出力の処置を検査する。

8.4.2　認可リスト

（入力の場合と同様に）認可リストを作成する。

XI－3図は，前各項の処理後技法とセキュリティ監査対象との関連を示すものであり，トランザクションおよび処理のユニーク性／完全性と比較すると，配分管理や回復性，違反管理のために利用できる技法のほうが少ないことがわかる。

RECORD SELECTION	SIMULATION	RECOMPILING	PROGRAM ANALYZER	MAPPING	TRACING	EXTENDED RECORD MAINTENANCE	TAGGING	INTEGRATED TEST FACILITY	TEST DATA	CONTROL TOTALS	MANUAL CHECKING	TECHNIQUES / SECURITY AUDIT OBJECTIVES
●	●					●	●	●	●	●	●	UNIQUENESS
●	●			●	●	●	●	●	●		●	TRANSACTION INTEGRITY
●	●	●	●	●	●	●	●	●	●	●	●	PROCESSING INTEGRITY
								●	●			DISTRIBUTION CONTROL
						●		●	●			RECOVERABILITY
●	●	●						●	●			VIOLATION CONTROL

XI－3図　監査サポート技法

9．必　要　な　技　法

セキュリティ監査データのロギングとログの分析，操作の2つの領域での技法の開発，改良が考えられる。

9.1　ロギングの方法

セキュリティ・ログのセキュリティを確立する必要がある。セキュリティ・データは暗号化の必要があり，たとえば，パスワードと重要なログは未認可アクセスから防護されていなければならない。

セキュリティ・ロギングの方法としては，下記の方法のいづれか，または組合せが考えられる。

最も簡単な方法は，現在のオペレーティング・システムのソフトウェアを使用

することである。しかし，この方法は，オペレーティング・システムと，これをコントロールする人間に依存することになるので，最低の防衛手段になるに過ぎない。

また，すべてのプログラム中に入れられた特別の命令によって起動される不正な変更のできない完全な記録用マイクロコンピュータのような特殊目的の装置を利用することも可能である。このような装置は，特殊なコントロール・プログラム（たとえば，"スーパ・ザップ"）を含むすべての動作を記録するが，通常は，システム・ログにはなんの痕跡も残さない。

同様に，プログラム・ライブラリの呼出しも全部記録される。

また，別の方法としては，システム中の重要なコントロール・ポイントにプローグを配置したコックピットのフライト・レコーダに似たような，完全ハードウェア・モニタがある。

これを使用すれば，モニタされるシステムからは独立して，適当な防衛レベルでの完全なセキュリティ・ログを入手することが可能である。

9.2 ソフトウェア・ツール

既存の技法によって，多くのことが実行可能であり，新しい技法の開発は必要ないということで多くの人々の意見が一致している。

現在の監査用ソフトウェアは，使用法をさらに容易化することができるし，ある程度の改良も可能であろう。また，ソフトウェアの能力の存在性をもっと一般に知らしめる必要がある。— 多くの監査人達は，"どこで"，"なにが"利用できるかがわかっていない。

利用可能なツールも使用が面倒すぎるように思えるし，また，しばしば原始的であり過ぎる。たとえば，前述したある種の手続きは，共通する対象をもっていても，通常の場合，今日のツールを使って目的を達成するためには複雑なプログラミングを必要とする。監査目的のためのログ・アクセス用のもっと高度なソフトウェアを開発する余地がある。

各種のツールにおける要素，たとえば，トレースとマッピッングなどは，えてして組合せがなされていない。これらの技法は，一般には一緒に使用したほうが適切で，これらが一緒に使用できるような機能が開発されてしかるべきであろう。

10. 結　果　と　提　言

監査人の便宜のために，"どんな"監査ツールが，"どこ"で利用可能であるか，を示す情報を公表すべきである。すなわち，セキュリティ監査用ツールのカタログを作るべきであり，このカタログには，コンポーネントの詳細を記載し，ツールの使用に必要な技法，ハードウェア，およびソフトウェアに従って索引できるようにする。また，困難さの程度についての注釈も記載されることになろう。

新しいシステムの開発に際しては，新システムにセキュリティ・ログ・データも組入れることが必要であり，監査性を確実にするために，そのシステムの計画開発，設計に監査方面の要員を参加させる必要がある。

セキュリティ監査用に，不正変更のできない記録能力を設定するため，完全なロギング・ハードウェア・コンポーネントを調査することが必要である。

11. 参　考　文　献

1. Computer Control and Audit.
   Wiliam C. Mair, Donald R. Wood, Keagle W. Davis.
   The Institute of Internal Auditors, Inc.
   Second Edition Revised and Enlarged, 1976.
2. Features of Seven Audit Software Packages－－
   Principles and Capabilities. A. J. Neumann.
   Special Publication NBS 500 － 13.
   National Bureau of Standards, July 1977.

3. Management Controls for Data Processing.
International Business Machines Corporation.
GF 20−0006−1, Second Edition, April 1976.
4. Stanford Research Institute,
Systems Auditability and Control Study,
− Executive Report.

PART XII インタラクティブ監査ツールと技法

議　長　Hart J. Will

ブリティッシュ・コロンビア大学

参加者　Robert P. Blanc

米国標準局

Henk Brussel

ブリティッシュ・コロンビア大学

Peter S. Browne（記録係）

コンピュータ・リソース・コントロールズ

Robert S. Roussey

アーサー・アンダーセン会計事務所

Joseph J. Wasserman

J. J. Wasserman社

Donald R. Wood

トーシュ・ロス会計事務所

編集者注

議長の経歴紹介

ハートJ. ウィル博士は，会計および経営情報システム（ＭＩＳ）の，始めは助教授，現在は准教授として，1969年以来，ブリティッシュ・コロンビア大学の商業経営学部に在席している。氏の授業と研究の関心は，ＭＩＳの分析，設計，監査，管理とセキュリティ，データベース管理，および監査用ソフトウェア全般，とくにＡＣＬ（監査コマンド言語）に注がれている。博士は，コンサルティングに，教育に，あるいは出版に，欧州，北米において広汎な活躍をしており，コンピュータ監査に関するU. E. C. 国際シンポジウム：法と技法の問題 ── セン

トオーガスティン，ドイツGMD，1975年6月18日～20日 — の議長，協議会会報－コンピュータ監査の法と技法の問題の編集責任者，客員研究教授 — Gesellschaft fuer Mathematik and Datenverarbeitung(GMD) — セントオーガスティン，ドイツ，1974～75年，および非公式DBMS研究集会 － 1976～77年の創設委員長を努め，現在はオペレーショナル・リサーチ／情報処理－1977年のカナディアン・ジャーナル，INFORの准編集者である。博士はDiplom－Kaufmann(ベルリン自由大学）の学位をもち，かつ哲学博士（アーバナ・キャンペインのイリノイ大学）である。

＜本会議の議題＞

インタラクティブ監査ツールと技法　コンピュータ・セキュリティのオンライン監査を可能にするためには，どのようなインタラクティブ・ツールと技法が利用でき，また，必要であるか。

米国内部監査人協会は，内部監査は各種のコントロールの有効性を測定，評価することによって機能する管理コントロールだと考えているが，ADPの環境下では，監査人が反応的な方法でこの責任を果たし，事後ベースで監査を続けて行くことは益々難かしくなっている。処理のスピードを考えるだけでも，違ったアプローチが必要になっている。

この会議の目的は，データの完全性のオンライン評価を可能にするために，今日，適用できる監査ツールと技法，さらに開発が望まれているものを調査することである。

以下は本会議の全員によって作成，審査された全会一致の報告書である。

インタラクティブ監査ツールと技法

グループ報告

ハートJ．ウィルおよびグループ・メンバ

1．エグゼグティブ・サマリ

1.1 序

1.1.1 インタラクティブ（相互作用）

監査に関しては，インタラクティブ監査プログラムが利用できるのは比較的僅かなシステムしかないが，インタラクティブであるという事は通常は監査プログラムのオンライン・コーディングの意味に解釈されている。インタラクティブのまた別の次元としては，コンピュータ化情報システムの自由形式監査調査ともいえるマン・マシン言語によるオンライン監査処理がある。コンピュータ・セキュリティに関しては，リアルタイムに近いモニタとコントロール用にオンライン・システムの活動情報（ＳＭＦ，タイムシェアリング中のデータなど）の収集が，一部使用されたが，しかし，システム自体が高度にインタラクティブであり，かつ，データベースの技法が広く使用されるコンピュータ・コミュニケーションでは，コンピュータをインタラクティブ監査ツールとしても使用できる能力が要求されている。

1.1.2 研究と開発

現在でも，部分的インタラクティブ・ベースで使用されているコンピュータ監査ツールと技法はたくさんあるが，インタラクティブであることは機能の開発と維持において望ましいものであり，研究グループとしては，真のインタラクティブ・ツールと技法に関する研究と開発が必要であると信じている。この報告書では，将来の研究の可能領域を数例あげる。

1.1.3 対象領域

グループの関心の対象は下記の領域である。

－監査効率向上のために，現存する監査ツールと技法をインタラクティブに使用する。

－実行保証処理全般の便宜を計り，とくに監査を容易化するための新しいツールと技法を開発する。

－コンピュータ・システムの監査性を強化するための技法の開発と使用。

1.2 概　要

1.2.1 実行保証

この概要は，コンピュータ・システムが指定された精度，適時性，データ・セキュリティの範囲内で意図された機能を実行しており，かつ意図されていない機能は実行されていない，という保証であると定義される実行保証の骨格について述べたものである。実行保証は，いろいろの異る職種の人々が参加すべき領域で，これには公認会計士，上級組織管理者，内部監査人，品質保証管理者，および運営管理者が含まれる。基本的な定義事項と目的は第2章で述べるが，実行保証機能は，第3章につぎの4つの活動に分けて記述されている。

－プロジェクト・コントロールの対象

－情報収集

－分析と評価

－テスト

1.2.2 現存するツールと技法

インタラクティブに使用することができる現存のツールと技法は，第4章で検討される。

1.2.3 必要なツールと技法

システムの手続きやコントロールの誤動作の検知に新たに追加される非常に有用な必要ツールと技法は第5章で検討される。データやプログラムのエラー，変則的な動作，アクセス・コントロール違反，予め設立された境界をこえる活動は，その兆候を知ることが可能であり，下記の種類のツールによって判断される。

－リアルタイムに近いエラー検出と訂正

－コントロールの妥当性の監視

－プログラム修正の管理

－システムのトラブル，動作の監視

1.3　インタラクティブ・ツールと技法の使用法

この研究グループでは，インタラクティブ・コンピューティングの2つの主要な使用法を確認した。すなわち，インタラクティブ監査プログラミングとインタラクティブ監査処理であり，これらの定義は第2章に示す。インタラクティブ監査プログラミングの場合，監査人がその監査プログラムの開発に際して受ける恩恵はすべてのコンピュータ・プログラムの開発とデバッグの場合と変りはないが，インタラクティブ監査処理では，リポート・データ／ファイルへのインタラクティブ・アクセスと監査プログラムのインタラクティブな実行が可能になる。

リポート・データ／ファイルへのインタラクティブ・アクセスは，この目的のためにシステムのファイル・コントロールによって格納されているリポート・データ／ファイルに関する監査人による照会で，たとえば，セキュリティ機能を貫通してみる企図での特定データに対する各種トランザクションの回数カウントがある。

監査プログラムのインタラクティブ実行は，監査プログラムを1ステップごとに実行する意味で，これによって監査人はインラインで中間結果を検査し，これらの中間結果にもとづいてプログラムの次のステップを実行してゆくことができる。

ワーキング・グループの結論によると，監査のためのインタラクティブ技法はまだ広くは行きわたっておらず，その理由としては，つぎのような事実が確認された。①インタラクティブ監査プログラムは広範囲に利用可能であるというわけではなく，監査人はこのモードでのオペレーションに慣れていない。②リポート・データ／ファイルへのインタラクティブ・アクセスには，これらのデータを収集し，レコード・ファイルを作成するためのコントロールをシステムに組込むことが必要である。③監査プログラムのインタラクティブ実行には監査人が使用するための新しいソフトウェアの設計が必要である。そのようなプロセッサはほとんど存在せず，存在するものも十分には知られていないし，発表もされていない。

1.4　インタラクティブ・ツールと技法の恩恵

インタラクティブ・ツールおよび技法を使用すれば，実行保証機能を容易にするための多くの恩恵が得られるが，その費用対効果が未だ十分に調査されていないので，当然のことであるが，さらに研究と評価が進められなければならない。

インタラクティブ・ツールと技法を使用すれば，システムまたはコントロール機能へ容易にいくらでも詳細なピント合せができる。（ズーム・レンズ効果）これらのツール技法によれば，監査証跡と記録された事象の継続更新をとおしてほとんどリアルタイムで事象を審査することが可能になり，これによって下記の能力が与えられる。

－ファイルのステータスを審査する

－例外を判定する

－関連データまたは状態を要約する

－異常状態を表示する。

また，各種のコントロールの特性と使用を決定する能力が与えられることによって，監査効率が向上される。

監査努力の結果が一層早く戻されることによって監査効率が増大，改善される。

直ちにフィードバックが行われることによって，監査の適時性が向上し，また，訂正動作が遅滞なく行われ，したがって摘発事項が減少する。

また，事務作業と監査準備が減少して，監査人は専門の仕事と分析により多くの時間をかけることが可能になる。

1.5　その他の考察と研究

グループでは，下記の領域でさらに審議と研究を進める必要があると考えている。

－インタラクティブ監査ツールと技法のための設計ならびに能力に関する必要事項の仕様。

－オペレーティング・システムおよびデータベース管理システムとのインターフ

ェース用のインタラクティブ監査ツールと技法の設計。

－オペレーションのインタラグティブ・マン・マシン・モードにおける監査行動を研究するための行動監査研究。

－実行保証（ＰＡ）専門家の活動，およびソフトウェア設計者の適切なツールならびに技法の開発のガイドになる包括的な監査ならびにコントロール理論の開発。

2．目標，目的，定義

2.1　目　標

コンピュータ・システムにおける実行保証のためのオンライン，すなわちインタラクティブ技法の使用に関する監査アプローチの開発。

2.2　目　的

－インタラクティブ・ツールと技法の範囲とこれに関する要求事項を定義する。

－コンピュータ・システムにおける監査性とコントロールの特性をレビューし，定義する。

－使用可能ツールと技法を解説し，必要なツール・技法を指定する。

－特定なシステム環境におけるこれらツールの使用基準を定め所要のインターフェース（たとえば，データベース，オペレーティング・システムとの間）を定義する。

2.3　定　義

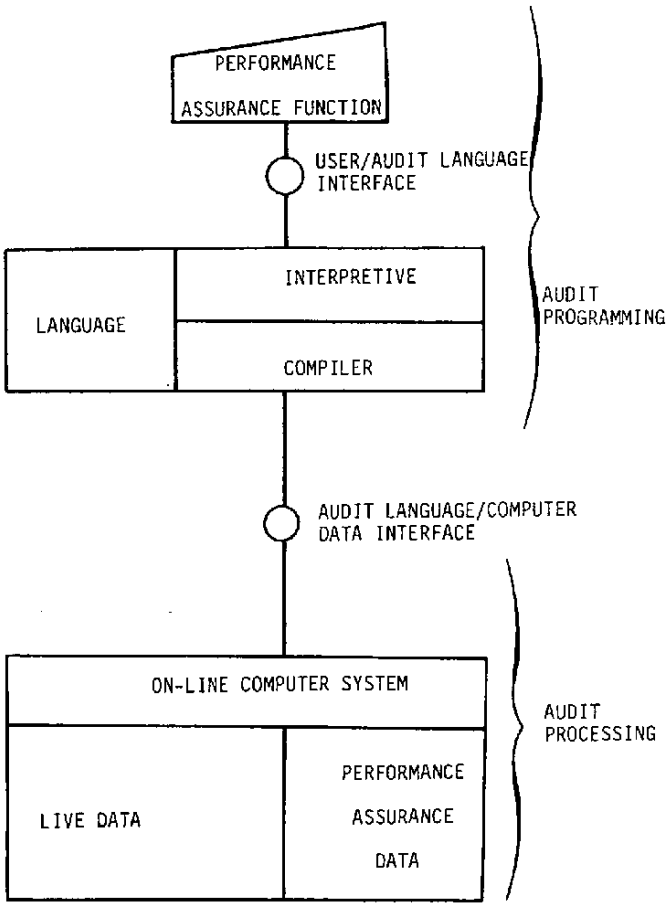
2.3.1　実行保証

コンピュータ・システムが指定の精度，適時性，およびデータ・セキュリティの範囲内で予定の機能を実行し，かつ，予定外の機能は実行していないという保証。精度のレベルは，管理基準によって決定されるアプリケーションおよびファ

ィル（マスターファイル，トランザクション，およびプログラム）のクリティカル特性による。

2.3.2　インタラクティブ・ツールを技法

インタラクティブ監査プログラミングと，インタラクティブ監査処理の双方をサポートするツールと技法。これによって，活動ファイル（マスターファイル，トランザクションおよびプログラム）への即時アクセスとその使用，ならびに，実行保証データへの即時アクセスが容易になる。これには，人間システムとコンピュータ・システム間の連続対話だけでなく，アプリケーションおよびコントロール・ファイルへのインタラクティブ・アクセスも含まれる。（Ⅻ－1図参照）



Ⅻ－1図　インタラクティブ監査

2.3.3　インタラクティブ監査プログラミング

言語を通じてのコンピュータ監査プログラムの開発。すなわち，監査人は構文エラーと，むしろ語義エラーに関して言語から直ちにフィードバックされる。―したがって，監査プログラムは瞬間的にデバッグされて，即時（あるいは故意に遅延）テスト／実行に使用できる。反意語：ジュネレーティブ（コンパイラによる）プログラミング，ホスト言語プログラミング。

2.3.4　インタラクティブ監査処理

インタラクティブ監査処理は，簡単な，しばしば端末で発動されるコマンドによってオンライン・ファイルに対するコンピュータ監査プログラムのステップと全監査プログラムをインタプリタ方式で即時に実行する。反意語：バッジ監査処理，オフライン・ファイル処理。

2.3.5　インタラクティブ監査

インタラクティブ監査は，様々に設計された依頼情報システムとインターフェースが可能な"それだけで完全な"監査ソフトウェア・システムの部分としてのインタラクティブ監査プログラミングとインタラクティブ監査処理の機能に依存する。反意語：バッチ監査

2.3.6　オンライン監査

インタラクティブ方式の監査能力を参照のこと。

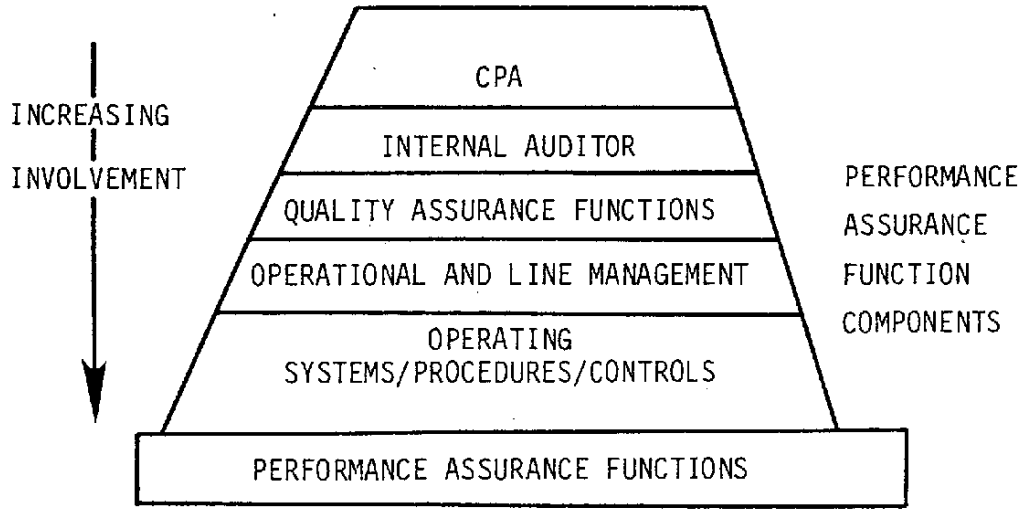
2.3.7　オンライン・システムの監査

処理が，主としてオンラインで行われるシステム（たとえば，航空会社の座席予約システム，リアルタイム・プロセス・コントロール，データ・エントリ・システム，その他）自身と，そのコントロールのいずれも監査する能力を意味する。

2.4　実行保証機能

2.4.1　モデル

"監査"という術語を一般化するために，当グループでは前に定義した"実行保証機能"をⅫ－2図に示すように説明することに決定した。



XII－2図　実行保証

2.4.2　ＣＰＡ機能

財務諸表に関する見解を発表するための客観的な独自の検査の実行に際して，情報システムとその内容のレビュー，評価，テストを行う。

2.4.3　内部監査人の機能

データ処理が正確に行われ，かつ，資産が適切に防衛されていることを保証する。

2.4.4　品質保証機能

コンピュータ資源の効率的，かつ，有効な管理と利用を保証するための基準を監視し，開発する。

2.4.5　オペレーションおよびライン管理機能

諸種の経営管理の開発とその有効性，ならびにそれらがどの程度守られているかを継続的に評価する。それぞれの管理は下記の点についてレビューさるべきである。

－有効性

－完全性

－一貫性

3. 実 行 保 証 活 動

3.1 序

実行保証（ＰＡ）機能の目的は，前の定義のとおり，コンピュータ・システムが指定された精度，適時性，データ・セキュリティの範囲内で所定の機能のみを実行し，予定外の機能は実施しないことを判定することである。また，定義の別の部分では，精度のレベルは管理基準によって決定されるアプリケーションとデータのクリティカル特性によるものであると述べられている。

実行保証機能に関係する諸グループの諸活動を，われわれは，審議の都合上，下記の諸活動に定めて説明することにする。

－ＰＡ対象の設定

－データの収集

－ＰＡ分析と評価の実施

－ＰＡテスト手続の設計と実行

これらの活動は次の２つの章で，現存および必要なＰＡツールと技法との相互分類に利用されている。これによって，実行保証活動に関係する専門家達が種々のツールと技法をどのように使用できるかの説明が可能になる。

3.2 ＰＡ対象の設定

実行保証で考慮さるべき対象としては２つのタイプがある。その第１のタイプは，実行保証テストの性格と目的（監査対象またはテスト対象）に関係し，第２のタイプはテストされるシステムに適用される。すべてのシステム要素（アプリケーション）に対するシステム，手続き，コントロールの開発に使用される基礎や枠組として，システム・コントロールの対象が設定され，システム・コントロールの対象はシステムがなすべき事，すなわち実際には，達成すべき目標を表わす。対象はその特定領域に対する管理によって設定される基準から設定される。

開発チームは，たとえば，システムの設計，詳細手続き設定，システムに組み込む内部コントロールのタイプと範囲の決定において，その手続き，とくに内部コントロールを対象と関連づけて考えることができる。

システム・コントロールの対象が定義されていれば，これらの対象はまた実行保証グループにとっても，特定のシステム・アプリケーションで使用されるコントロールの評価に使用することができる。

システム，手続き，およびコントロールの設計，実施においては，すべての場合，その最終結果にはその特定アプリケーションに組込まれているコンピュータ化された内部コントロールの技法とユーザの詳細に関する文書化が必要である。この"内部コントロール技法の記述"は実行保証機能にとって非常に重要なものであり，あらゆるシステムの場合に標準になるものである。

3.3 情報の収集

実行保証機能の情報収集段階は，システム，手続き，コントロールのレビューと評価，または設定のために必要な情報・データを取得することであるということができる。収集される資料には，たとえば，内部コントロール技法の記述，詳細，要約文書，システムと手続きの口述記録，フローチャート，認可リスト，その他，類似のデータが含まれる。もしこのタイプの情報・データが利用できないと，実行保証グループとしては，分析，評価のための資料を作成，準備しなければならないことになり，実行保証を実施するグループがその必要データをたとへ一部でも作成する必要があるということになると，事実上は，システムの開発グループが実行しておかなければならなかった機能を実施することになる。上記の資料は実行保証機能にとっては，非常に重要なもので，すべてのシステムの場合の標準になるものである。

3.4 ＰＡ分析と評価の実施

分析と評価は，システムと手続き，およびコントロールに関する設計とテスト

の実施において開花するわけで，これらのテストの結果，また，さらに分析，評価に戻ることもあり得る。

分析と評価の活動は２つの要素，すなわち，アプリケーションの複雑性とクリティカル特性（物質性と重要性）によって影響される。アプリケーションのテストは，アプリケーションがクリティカルで複雑であると，一層，広範に，かつ複雑になり，このような場合には，実行保証に関係する各種グループがオンライン・テストとオンライン・システムのテストに使用できるインタラクティブ・ツールと技法を承知していることが重要になる。これらのツールと技法をテスト過程のどこで，どのように利用できるかを知っていることによって，監査プログラムをインタラクティブに作成して，実行することが可能になる。柔軟性が得られることによって，テストの焦点を重要なコントロール領域，危険区域，一致テストと実在テストの適当なバランスに合せることが可能になる。また，テスト・プログラムは適切な場合には，ノン・インタラクティブなツールと技法を利用するように作成することも可能である。

3.5　ＰＡテスト手続の設計と実行

システムとその手続き，コントロールの分析，評価にもとづく結果として，中心となるべきキー・コントロールの設計とテストが必要になる。この活動はつぎのステップで実行することができる。

－検証技法の選択

－コンピュータを利用する技法が使用されるかの判定。

－テスト手続きの準備と実行。

－テスト結果のレビューとさらにテストが必要であるかどうかの判定。

3.5.1　検証技法の選択

一般に，コントロールと処理の検証には２つのアプローチが適用できる。

－結果のテスト：１つ以上のキー・ファイル，または処理の出力を選択して，結果を確認する。

－処理のテスト：クリティカル・プロセスとコントロールの特定テストを直接，実行する。

3.5.1.1　結果のテスト

結果の検証とテストは通常は，結果の独立ファイル，組織または物理的項目との比較，あるいは妥当性テストによって実行される。前者の例としては，個人支払レートおよびインベントリ・バランスのコンピュータ記録と独立の人事ファイルとフィジカル・インベントリ・カウントとの比較，後者の例としては，値の予定範囲によるテスト，あるいは，予算や前期の結果のような類似情報との比較があげられる。

3.5.1.2　処理のテスト

処理の検証には，特定の手作業／コンピュータ・コントロールおよび処理ステップを処理するために，次の2章にわたって述べられる特定のツールと技法が必要である。たとえば，スナップ・ショット技法では，コンピュータ・プログラムの各ステップが，あたかも処理中であるかのように，また，キー・データ要素の状態が修正されるとおりにリストされる。

3.5.2　コンピュータを利用する技法が使用されるかの判定

コンピュータの使用は下記の条件による。

－コントロールの性格。たとえば，監督管理は主として監督作業の文書化されたものを観察，レビューすることによってテストされるコントロールであり，データベースの完全性のテストには，逆論的に，コンピュータの使用が必要である。

－コンピュータ・ファイル，および処理時間の利用性。

－費用の正当性。

－必要な場合にコンピュータ・プログラムを開発するコンピュータ使用の熟練度。

3.5.3　テスト手続きの準備と実行

テスト手続きを準備し実行するには，種々のコントロールが条件になる。コントロールは，プログラムが希望のテスト目的を達成するように設計されているこ

と，また，手続きとファイルが指定どおりに使用されていることを保証する必要がある。一致性テストと実在テストは，重複されがちで，同一のテストをシステムのテストとデータのテストの双方に適用できることもあるが，通常は区別される。

実在監査は主として，会計年度末における財務諸表に関係するものである。実在テストは，内部コントロールの検証よりはむしろ，金額（ドル値）や財務バランスの検証に適用され，その範囲は一致性テストによって決まる内部コントロールへの依存度によって左右される。

3.5.4　テスト結果のレビューとさらにテストが必要であるかどうかの判定

このステップは，テスト結果が有効なものであることを確認するための分析，評価機能である。テストの方法，手続き，および結果はコントロールとその信用，摘発の最終評価におけるその後の独立のレビューのために文書化されるものと考えられる。

実行保証の最終結果は，システムとシステムの処理結果が信用できるのか，どこまで信用できるかを判定するものであって，結論はそれぞれのグループによってある程度は異るにしても，各グループとも，それぞれの結論を出すためにはシステムの信頼性を見積るためのテスト結果をレビューする。

4．現存する実行保証ツールと技法

4.1　序

前の定義によるＰＡ機能に関連しての現存の実行保証（ＰＡ）ツールと技法の調査，検討では，バッチとインタラクティブのツール／技法を別々に区分したが，その要約は図3に示すとおりである。

完ぺきな分類が行われたわけではないが，おのおののツールと技法には，有利か不利かの表現範囲で簡単な注釈が付されている。この重要目的は，第5章の必要なＰＡツールと技法とのギャップを確認することに置かれている。

TECHNIQUES AND TOOLS	PERFORMANCE ASSURANCE FUNCTIONS				
	Control Objectives	Information Gathering	Analysis & Evaluation	Testing	
				Compliance	Substantive
1. Batch PA Tools & Techniques					
a. Utility Programs Documentation	X	X	X		
Flow Charting		X	X	X	
Access Authorization Table		X		X	
Data Dictionary	X	X	X	X	
Program Dictionary	X	X	X	X	
Compare-Source/ Object Programs		X	X	X	
Check Sum		X	X	X	
SMF		X		X	X
b. Test Deck				X	
c. Audit Modules		X	X	X	X
d. ITF				X	
e. Test Data Generator		X		X	
f. Snapshot		X		X	
g. Tracing		X		X	
h. SCARF		X		X	X
i. Parallel Simulation				X	X
j. Audit Software Packages	X	X	X	X	X
2. Interactive Tools & Techniques					
a. ACL	X	X	X	X	X
b. NAARS		X	X		

XII－3図　ＰＡ機能上のＰＡツールと技法

4.2　バッチＰＡツールと技法

4.2.1　ユーティリティ・プログラム

効率，利用性，モニタリング，および文書化を容易にするために，ハードウェア・メーカやソフトウェア会社から入手されるプログラムである。

これらは膨大な量であるので，簡単なリストでこれらのシステムの種類を示す。

－ＳＭＦ（Systems Management Facility）

－自動フローチャーティング・システム

－データ便覧

－プログラム便覧

－データ／プログラムのライブラリ・システム

－ＨＭＢＬＩＳＴ（ＩＢＭ　Ｏ／Ｓの修正を検知するユーティリティ）

－比較システム（ソース対オブジェクト）

a．有利な点

①無償または低コストで利用できる。

②監査人にとっては，追加的な事実を提供し，データ・ファイルとトランザクションのオリエンテーションを超えたコンピュータ・システムの探索を可能にする。

b．不利な点

①専門的な技術が余計に必要になる（オペレーティング・システム，ＤＢＭＳ，その他）。

②"監査ツール"としてテスト，実施されていない。

4.2.2　テスト・デック

コントロールとプログラム・ロジックの正確性をテストするように作成された仮のトランザクションとワーク・ファイル・レコードである。

a．有利な点

①　個々のコントロールの特性と例外の高度な特定テストが可能になる。

b．不利な点

①　プログラムの修正のために，ラスト・データの開発と維持が困難である。

②　ラスト・モードが利用できない限り，特別のコンピュータ・ランが必要になる。

③　レポートや統計を十分にテストできる程包括的であることはめったにない。

4.2.3　監査モジュール

勘定の年令調べのような特殊な監査機能を実行したり，プリントされたレポートへのテスト・データの影響を除去するための特別の監査用サブルーチンがアプリケーション・プログラムに組込まれることがある（ＩＴＦ参照）。

a．有利な点

① 必要な場合には特別な監査作業が可能である。

② いつでも"トリガー"することができる。

b．不利な点

① 専門的なプログラミングが必要であり，設計によっては特別な操作手続きも必要になる。

② 許可されていない者でも呼び出しが可能である。

4.2.4 ＩＴＦ(Integrated Test Facility)

実用ファイルや出力に悪影響を与えることなく，実用トランザクションと同時に，テスト・トランザクションをコンピュータ・システムへ流す方法である。統計ならびにレポートも含む別口の出力が作成される。これによって，テスト資料が実際のデータに関するいかなる出力も防害されない保証が得られるだけでなく，監査人は統計およびレポートが正しく作成されていることをチェックすることが可能になる。

a．有利な点

① 実際の環境のもとでのルーチン的なテスト。

② 特別のラン・タイムが不要。

③ 実用レコードには無影響。

④ 統計，レポートの入手。

b．不利な点

① 完全なテスト・データ・セットの作成と維持が困難。

② テスト用サブシステムを実用システムへ統合するための特別なプログラミングが必要。

4.2.5 テスト・データ・ジェネレータ

コンピュータによって，テスト目的のための仮のトランザクションを作成する方法である。

a．有利な点

① テスト・トランザクションとワーク・ファイル・レコードの自動開発。

b．不利な点

（テスト・デック参照）

4.2.6　スナップショット

たとえば，"タグ"（タギング）によって識別される特定なトランザクション・タイプによってトリガーされて，作成サイクル中の特定な時点でデータのステータスを把握する技法である。

a．有利な点

①　極めて特定な目的のための優れた方法である。

②　"ロギング"の必要を減らすことができる。

b．不利な点

①　"オーバー・タグ"をさけるために，監査人による頻繁なモニタが必要である。

②　一般的な監査アプリケーションには制約が多過ぎる場合があり，かつまた，適当な"ロギング"手続きに否定的な影響を与えることがある。

4.2.7　トレース

スナップショットと同じ条件で，"タグ"で識別される特定のトランザクション・タイプでトリガーされて，プログラム・コードの現実の除外部分を識別する技法。

a．有利な点

（スナップショットと同じ）

b．不利な点

（スナップショットと同じ）

4.2.8　ＳＣＡＲＦ（System Control Audit Review File）

タグをつけたり，監査ファイルへ例外データを抜き書きするために，通常のデータ処理アプリケーションに監査人の決定による妥当性テストを挿入する。

a．有利な点

①　継続例外レポート（監査モジュール参照）。

b．不利な点

① 処理時間。

4.2.9 監査ソフトウェア・パッケージ

年令調べや確認，サンプリングなどのような特殊な監査機能のほか，さらにデータ・アクセスと計算操作を可能にするための高級なデータ処理言語である。各種のソフトウェア・パッケージの実行機能は，下記の点ですべてが同じではない。

－能力，すなわち計算，サンプリング，比較，その他。

－データとのインターフェース（すなわち，ＤＢＭＳとファイル構造）。

－実行効率（すなわち，ランニング・タイム，監査準備，その他）。

a．有利な点

① 独立したデータ収集とデータ・ファイルの分析が可能になる。

② 監査時間の効率を改善し，監査範囲の拡大に貢献する。

③ データの全領域のアクセスができる。

b．不利な点

① 標準のプログラミング言語を使用するより処理時間が長くなる。

標準としては，監査用ソフトウェア・パッケージは読み出し専用モードに限定すべきである。

4.2.10 並行シミュレーション

アプリケーション・システムと同一の，入力データとファイルを使用して，同一の結果を得ることによって，コンピュータのアプリケーションの処理をテストする方法である。シミュレーションの結果が＂実用＂の結果と比較されて，コンピュータのアプリケーション処理結果の確認が行われる。あるいは．さらに分析を必要とするくい違いのある領域を確認する。

a．有利な点

① ファイルの破壊などの心配は全くなしに，実用データでアプリケーション・プログラムの適合性のテストを行える。

② テストされたアプリケーション・プログラム機能は主として，非技術的な

ユーザの文書（エラー，調整手続き）を通じて分析することが可能である。

b．不利な点

① 実行される機能についてよく知っている必要がある。

② シミュレーション・プログラムの開発に時間がかかる。

4.3 インタラクティブＰＡツールと技法

グループの検討の結果，データに適用できる2つのインタラクティブ監査ツールが確認されたが，これらのツールは引続いて研究，評価さるべきとあると考える。さらに，そのほかに現存する監査ツールの可能性について2つの検討を行ったが，この成果は得られなかった。

4.3.1 ＡＣＬ（監査コマンド言語）

ＡＣＬは，バンクーバのブリティッシュ・コロンビア大学で，2つのバージョンが利用できる。はじめのバージョンは，ミシガン・ターミナル・システム（ＭＴＳオペレーティング・システム）でランされているもので，教育（ＣＩＣＡを介して学問と職業の両面）を研究に幅広く使用されている。ＩＢＭバージョンは，ＩＢＭ／ＯＳ／ＶＳ１システムでランされるもので，コンサルタントのほか，内，外部の監査人も使用している。完全にインタラクティブな最初の監査言語として，ＡＣＬは各種の実行監査機能を単一の専門ユーザ言語にまとめようとするパイオニア的な存在である。

4.3.2 ＮＡＡＲＳ（National Automated Accounting Reserch System）

ＮＡＡＲは，ＡＩＣＰＡとMead Data Central，Inc.の共同開発によるもので，3,500社以上の株主に配布される年次報告書の財務諸表の全内容，注釈，および監査報告をインタラクティブに（コンピュータ端末を通じて）探索することが可能である。そのほか，連邦証券法，連邦通商規則だけでなく，ＡＩＣＰＡの各種刊行物のファイルもアクセスすることができる。

5．必要な実行保証ツールと技法

5.1　序

前述した現在時点で存在する実行保証（ＰＡ）ツールと技法は，多くの場合，監査という面では非常に有用なものである。しかしながら，このようなツールは多くの場合，監査人にも，また品質保証の担当者にもほとんど利用されていない。これらのもつ潜在能力が知られていなかったり，それらの実行保証に対する適用性が明確でないこともある。ある場合には，これらのツールは他の目的（たとえば，ハードウェアやソフトウェアのモニタ）のために設計されていて，セキュリティや実行保証への適用性は直観的にははっきりわからない。

以下の各項に亘って，必要なツールの種類を述べ，その設計と開発に関する必要事項を指定する。

5.2　必要なツールと技法

下記に述べるツールと技法は，２つの大きな領域で利用することが可能である。誤動作や，システム，手続き．またはコントロールの不完全性はモニタリングやトレース，テストの機能によってインタラクティブに完全に検出される。また，過度のエラーや，高度の注意を要するファイルへの変則的なアクセス，あるいは特定プログラムの過度の変更のような兆候をさぐるためのシステムの＂健康診断＂も可能である。これは，医師が病気を診察するために行うテストや探針，データの収集と全く同じことで，これと同じ診断をＰＡの専門家が下さなければならない。

5.2.1　リアルタイムに近いエラー検出と訂正

この種のツールは，コンピュータ・システムにおけるエラーの発生時に，＂損害＂が起きてしまわないうちに，発見して，実際面では，これを訂正する作業に有用なものである。損害の例としては，資金支払システムにおける大量資金の自

動支出の間違や，プロセス・コントロール・システムにおける偽フィードバックが上げられる。このようなコントロールは，"全体として"のオペレーション・システムを指向するものである。ハードウェアや個々のシステム・モジュールは，すでにテストされて，検証済みであっても，各種のサブシステムを1つの大きなシステムとして一緒に作動させると故障が発生することがあるものである。下記のツールが必要であると考えられる。

－インタフェース・データのモニタとテスト ― 範囲，限界，および項目の有効性に関して，システム中のモジュール間の各インタフェースにおけるデータをテストするためにあるルーチン。

－手がかりの検出 ― 異常な使用パターンの場合に，これを発見して直ちに停止するために，システムの可変／不変の特性を測定するハードウェアおよびソフトウェアの監視。

5.2.2　コントロールの妥当性の監視

この種のツールは，システムのなかに組込まれている予め決定，指定されたコントロールのオンラインによるテストを可能にするものであり，監査人はこれらのツールによって，潜在的な故障箇所を発見するためのオペレーション・システム・テストを実施することができる。下記のツールが必要であると考えられる。

－ソフトウェア行動モニタ ― これらのルーチンは，システムのなかに停止状態でおかれていて，監査人から呼び出されると，アクセス，入力，出力，および使用回数に関して，指定されたソフトウェア・モジュールの行動のモニタを開始する。

－構成監査 ― このルーチンへのアクセスによって，監査人は，大型のテレプロセシング・システム中の特定的な使用のためのオペレーション・システムの現在の構成に関する情報を即座に入手することができる。

－インタラクティブ・トレース ― 普通のデバッグ・パッケージに似たルーチンで，これらを使用することによって，監査人は，システムのオペレーション・サイクルへ立ち入って，データ値の変化と事象の同期化をモニタし，かつ，モ

ジュールのインタフェースにおけるコントロールの妥当性の検証のために，データ値を修正することが可能である。

－人為的なロード・ジェネレータ ― これらのルーチンの使用によって，監査人はローディング条件が変化するシステムのテストのために，コントロールされた量のトランザクションをジェネレートすることができる。

5.2.3　設計精度の測定

この章では，システムとコントロールの仕様と文書化のためのツールと技法の検討を行う。システム・コントロールだけでなく，システムに対する機能的な必要事項に対する仕様を検査することも可能である。

下記のツールが必要であると考えられる。

－要求事項仕様言語 ― 機能上の要求事項の検証が可能な，システム要求仕様コンピュータ言語。

－コントロール特性仕様 ― 監査人が，"容易"にその適用，機能，予想性能を理解できるような，コントロール特性仕様のためのプログラマ用形式方法。

5.2.4　プログラム修正管理

この種のツールは，監査人がプログラム修正管理手続きの妥当性をオンライン・テストによって検査することができるようにするものである。

下記のツールが推奨される。

－プログラム修正検知 ― システム・アプリケーション，およびコントロール・ソフトウェアの修正を発見するには，チェック・サムや，これに類似するルーチンが使用できる。

－プログラム（修正）監査証跡 ― 個々のオンライン・ファイルの照会によって，監査人はすべてのプログラムに関する安全な情報を入手することができる。さらに，個々のプログラムに対する変更も知ることも当然可能であり，これには，誰れが変更したか，いつ変更されたか，変更の原因となった問題はなにか，修正されたプログラムは何時，オペレーションされるようになったかも含まれる。

5.2.5　システム・トラブル・インディケータの監視

この種のツールによって，監査人は各種のセキュリティの実行とシステム・コントロールに関する情報を格納しているファイルの照会が可能になる。推奨できる必要ツールはつぎのとおりである。

－利用回数の監視 ― あらゆる特権モジュール，装置，データ，およびトランザクションへのアクセスに関する回数情報が，オンラインで与えられる。

－コントロールおよびセキュリティ特性の利用 ― 監査人は，このファイルを照会することによって，使用回数と実行結果を含むシステムの，あらゆるセキュリティ・コントロール，エラー検出，エラー訂正特性の利用に関する情報を入手することが可能になる。例としては，自動エラー検出特性の実行前後のデータに関する情報があげられる。

各種の実行保証機能を達成するために必要であると思われる，ツールと技法の要約をⅫ－4図に示す。図の"コントロール"欄でこれらのツールと技法のあるものは，内部コントロールの目的にも使用できる（すでに使用されている）ことを示しており，監査人はこれらのツール／技法を承知して，とくに情報収集機能における潜在的な有用性を認識する必要がある。

6．要約と推薦される追跡検討

6.1　序

この最後の章は，インタラクティブ監査ツールと技法の必要性の，簡単な一般的要約と，これに関しての適切な追跡検討についてのいくつかの勧薦事項である。

6.2　インタラクティブ・ツールと技法の必要性

実行保証機能のための，インタラクティブ・ツールと技能についての認識が不足していることは明瞭だが，当グループは，このようなツールの必要を認識し，それらの有用性をエグゼグティブ・サマリ（1.4章参照）に要約した。

4.3章に述べられている現存のツールは，実行保証の分野で活躍している専門

家のすべての関心に価するものであり，より深く，より詳細に検討，研究さるべきものである。

当グループとしては，必要ツールと技法（第5章参照）を確認し，すべてのＰＡ専門家の視野の拡大を試み，かつ，近代式な情報システムの適用性と包括的なＰＡ監査のための方法に関する一層の検討を鼓舞することを願うものである。

6.3　推薦される追跡検討

当グループは一層の検討，研究が必要であると考え，下記の事項を可及的速かに完成することを願っており，その検討のための支援をこうものである。

－インタラクティブＰＡツールと技法に関する基準の構想。

－インタラクティブＰＡツールと技法のオペレーティング・システム（ＯＳ）ならびにデータベース管理システム（ＤＢＭＳ）とのインタフェースの設計。

－実行保証を背景としたインタラクティブ・マン・マシン行動を研究するための行動監査の研究。

－ＰＡ専門家の業務とソフトウェア設計者のＰＡツール／技法の開発の指針となる包括的な監査とコントロールの開発。

6.3.1　基準の構想

現存するインタラクティブＰＡツールと技法は僅かで，これらは実行保証の分野で活動している多くの専門家達によって，さらに研究，評価される価値のあるプロトタイプであると考えることができ，現存ツールのあるものを採用することが可能であるかも知れないし，将来のシステムのための設計，実施上の必要事項を指定することも可能になろう。

6.3.2　インタフェース

あらゆるＰＡツールと技法には，システムが実行するデータベース機能とのインタフェースが必要であるが，ＯＳとＤＢＭＳの設計・標準化にはＰＡ専門家はほとんど参加していない。ＯＳとＤＢＭＳにおける相違，あるいは，そのいずれの個有の弱点によってもＰＡと監査の機能の効率，効果がそこなわれる可能性が

ある。したがって，当グループとしては，すべての専門家達が可能性のあるインタフェース設計の必要性を認識するよう勧告するとともに，また，これらの重要なインタフェースに関する検討に参加することを望むものである。

6.3.3　行動研究

どの監査ソフトウェア機能が，インタラクティブ特性としての価値があるかを判定するためには，行動研究が必要である。監査の必要事項は，プロジェクトにより，また時間とともに変化するものであるから，ある種のインタラクティブ・ツールは，ある種の場合にのみ関係することがあり得る。さらに，ある場合には，使用される監査ツールが手続きに影響を与えることがあり得るし，また，監査人の結論に影響することもある。したがって，監査アプローチが使用ツールに従属してしまうこと，および逆の可能性を認識することが必要である。ＰＡ機能は，監査人とツールとの連携動作が認識されて，今までに可能であった以上によほど深く研究されないと，非常に容易になる可能性もあるが，はるかに難しくなる可能性もあり得る。

	PERFORMANCE ASSURANCE FUNCTIONS				
TOOLS AND TECHNIQUES	Control Objectives	Information Gathering	Analysis & Evaluation	Test-ing	Con-trol
Interface testing		X	X	X	X
Threshold detection		X	X		X
Software behavior monitoring		X			X
Configuration auditing		X	X	X	X
Interactive Trace Routine				X	
Artificial load generation		X	X	X	
Requirements specification	X		X	X	
Program modification detection		X		X	X
Program modification audit trails		X			X
Program Modification Documentation	X	X			X
Utilization frequency monitor		X			X
Control specification	X	X			

Ⅻ－４図　ＰＡ機能別のＰＡツールと技法

6.3.4　理論

現在では，ＰＡの分野においてのインタラクティブなマン・マシン行動を監視することが可能であるので，実行保証機能の包括的監査／コントロール理論の開発が可能になっている。その結果，ＰＡ専門家の業務を指導すること，"インテリジェント"なＰＡツールと技法を開発することもできるようになるだろうし，かくて，本報告書に述べられた各種のＰＡ機能の働きはますます便利に，効果的になる。

昭和54年3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