EDPシステムの信頼性に関する一考察

田中　弘

1. はじめに

現在の産業活動，経済活動，社会活動はコンピュータ・システムに依存して成り立っているといっても過言ではなかろう。1946（昭和21）年に完成されたENIAC（Electronic Numerical Integrator And Computer）に始まるコンピュータの歴史は[1]，すなわち信頼性技術の発達の歴史でもある。

コンピュータが当初もっぱら軍事用として用いられていた時期から，その高速演算機能が注目され，次第に科学技術計算のほか，統計事務などの大量データ処理に活用されるようになってきた。その後，現在に発展するまでの過程を，その中心となる利用形態から分類すれば，①一括処理（batch processing）②即時処理（real time processing）③遠隔処理（on-line processing）④時分割（time sharing）へと発展してきている。

この過程は，利用範囲が拡大され，有用性が増大してきているということの他に，より重要な意味をもっていると考えられる。コンピュータ利用の初期の段階においては，統計事務処理に典型がみられるように，その正確性・迅速性が評価され，対象業務も事後処理的なものが中心であった。それが発展した段

階においては，特に通信技術と結合した段階においては，企業または各種組織の本来的な諸活動が，コンピュータの機能を利用する型で行なわれるように設計されるに至っている。この一例を鉄道業についてみるならば，当初は経営管理目的の路線別あるいは駅別などの各種集計処理といった事後処理的な業務が中心であったが，今日では座席予約をはじめ，時々刻々の列車の運行管理といったその企業で最も本質的であると考えられる業務まで，コンピュータを不可欠の要素としてシステム化している。これらはコンピュータを中心とする周辺技術の発達にともなう信頼性の向上が前提となっていることは論を待たないが，以下信頼性の概念について若干の考察を試みたい。

注(1) ENIAC は演算と記憶に真空管が使用されているものの，現在コンピュータの本質的な要件となっているプログラム内蔵方式ではない。その意味では1949年の EDSAC，また実用化の意味では1951年のUNIVAC-Ⅰ型にコンピュータの歴史が始まるとする定説である。

2. ハートウェアの信頼性

コンピュータを中核とするＥＤＰシステム（Electronic Data Processing Systems）の信頼性向上に，直接的に最も寄与してきたものは電子技術，特に半導体の進歩である。すなわち，演算素子が真空管からトランジスター，ＩＣ（Integrated Circuit），ＬＳＩ（Large Scale Integration）へと発展し，並行して記憶素子，入出力装置などのいわゆるハードウェア（hardware）の発達である。

コンピュータ・システムが単純であった場合は，演算速度が主な性能評価指数であり，部品性能が決定的な影響をもっていた。この進歩の過程は表１に示されるように，演算時間（加算時間），記憶サイクル，記憶素子（コア・メモリ）の価格とも，５年毎にほぼ１桁以上の進歩がみられる。演算速度を中心とする，いわゆるＣＰＵ（Central Processing Unit）の高速化の実現にともなって，周辺装置，特に入出力装置の速度が問題となってきた。すなわち，入出

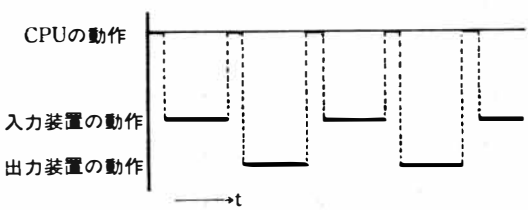
表1　ハードウェア性能の進歩[1]

	1960年	1965年	1970年	1975年
加算時間（アクセス時間を除く）	4μs	0.8μs	8ns	1ns
記憶サイクル	4μs	0.5μs	100ns	30ns
コア・メモリ（1ビット当りの価格）	0.85ドル	0.20ドル	0.05ドル	0.005ドル

備考：μs（マイクロセカンド）は100万分の1秒，ns（ナノセカンド）は10億分の1秒

力の速度がＣＰＵのそれに比較して遅いため，ＣＰＵに遊休時間が生じ（図1参照），ＣＰＵの高速化の割には データの入力から結果の出力までの所要時間，ターン・アラウンド・タイム（turn-around time）が短かくならないという問題である。この対策として考えられたのが，①入出力装置の高速化，②ＣＰＵの遊休時間を少なくするため，複数の処理（プログラム）を並行して実行させ

図1　CPUと入出力装置の動作の関係



太線が動作中を示す。

る，ということである。前者の場合，入出力装置にはどうしても電気的接点や機械的動作部分を含む関係上，その高速化には限界がある。そこで後者，すなわちコンカレント・オペレーション（concurrent operation）の考え方が研究されてきた。コンカレント・オペレーションの初歩の段階では，SPOOL（Simultaneous Peripheral Operation On-Line），ＣＰＯ（Concurrent Peripheral Operation）と呼ばれる手法で，主処理と周辺処理を同じコンピュータで実行させるという形式で試みられており，その後，この概念が今日のＯＳ（Operating Systems）に包含されるに至っている。このような発展に応じて，

コンピュータ処理の能率に対する考え方も，ある一つの処理（job）をいかに短時間で実行するか（ターン・アラウンド・タイムの短縮）と合わせて，一定時間内にいかに多くのジョブを消化するか，すなわちスループット（throughput）の向上という考え方が重要視されてきている。ＯＳは明らかにソフトウェア（software）の範疇に入るものである。今日のコンピュータの性能評価は，ハードウェアに関する事項より，むしろそのシステムが備えているソフトウェア，そしてそのソフトウェアを使用する費用と効率によって決定される。

このように性能についての考え方が変化してきた背景には「動くかどうかが問題であった初期のコンピュータ」から，その安定性，信頼性が飛躍的に向上したということがある。コンピュータの安定性，信頼性という用語は一般的に次のような意味で使用される。

① 誤動作発生の確率

② ＭＴＢＦ（Mean Time Between Failures——平均故障間隔）

③ 可用性（availability）

コンピュータの利用分野が拡大し，利用形態もバッチ処理からリアルタイム処理へと発展するにともない，故障や誤動作による損失も増大する。誤動作が生じると重要なファイルを使用不能にしたり，間違った命令を実行したりすることになる。銀行システムであれば，入出金を行なう口座を間違えたり，座席予約システムであれば，一つの座席を二重に予約したり，逆に空席が余っているにもかかわらず満席として予約を中止したりすることになる。また故障となると，修理中は業務を中断しなければならない。ハードウェアの技術がいかに進歩しても，故障や誤動作を皆無にすることはできない。これらに対して，大別して，①コンピュータ設計時に考慮，②運用に当って考慮，の２つの対策が考えられている。前者としてはデータの転送や処理結果をチェックする機能，演算など同一の処理について二重三重の回路を設けるなど，故障や誤動作をすぐ発見できるような論理の組み込み，後者としては，電源を二重にしたり，一

つの入力データを別々のＣＰＵで処理を行なってその結果を照合し，同一でなければ誤りとするデュアル・システム（dual system——図２），片方を予備機

図２　デュアル・システム

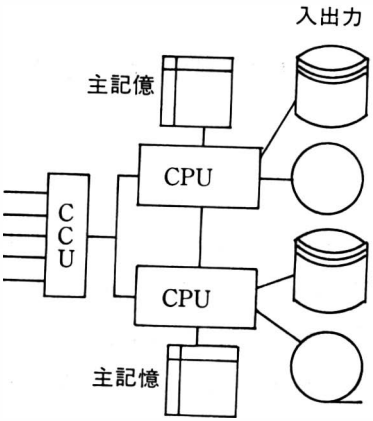
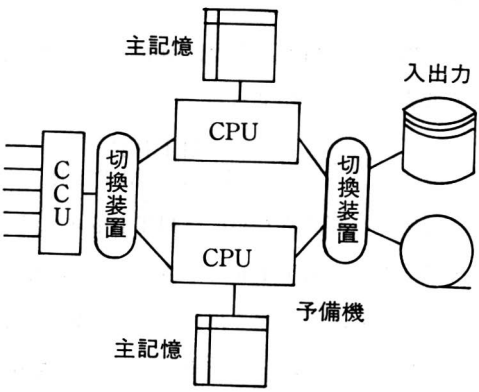


図３　デュプレックス・システム



備考：ＣＣＵ（Communication Control Unit）

として別の処理に使用していて本機の故障のときに切り換えるデュプレックス・システム（duplex system——図３）などがそれである[2]。

コンピュータを構成する各部品や装置類の故障率を表わすのにフィット（fit）という単位が用いられる。１個の部品や装置が10^9時間に１回故障する確率を１フィットという。たとえば，ＩＣは10フィットの故障率，すなわち10万個のＩＣを1,000時間使用すると数個の故障が発生することになる。コンピュータ・システムとしての故障率は，各部品や装置類の故障率をもとにして，その構成に応じた確率計算を行なうことによって理論的な故障率を求めることができる。現在のコンピュータのＭＴＢＦは，そのシステムの大きさや構成部品の種類によって大きく異なってくるが，電気的接点や機械的な可動部分のある装置で数百時間，電子部品から成る装置で数千時間である[3]。

信頼性を評価する別の尺度にＭＴＴＲ（Mean Time To Repair——平均修理時間）がある。いかにＭＴＢＦが向上しても，機械であるからには必ず故障

する。一旦故障した場合に，それが正常稼動できる状態に回復するのに要する平均時間がＭＴＴＲである。またＭＴＴＲは，設計の段階でどの程度保守性が考慮されているかの尺度ともなる。現在，大体数分～数時間というのが実情である。

可用性（可用率）とは，コンピュータが正常に稼動する割合であって，次の式で表わすことができる。

$$\text{可用性}=\frac{\text{MTBF}}{(\text{MTBF}+\text{MTTR})}$$

可用性を高めるためにはＭＴＢＦを大きく，すなわち信頼度の高い部品を使用すること，ＭＴＴＲを小さくする努力，すなわち「その装置に一連の入力データを加え，対応する出力データを観測し，観測結果を調べて故障があると判断される場合は，その結果を利用して故障位置を指摘する」(4) という故障診断（diagnosis）能力が強化されてきている。

可用性を高める別の方法として，前述のデュアル・システムがある。この場合，それぞれのコンピュータの可用性を R_1 とすれば，システム全体の可用性Ｒは，

$$R = 1 -(1 -R_1)\cdot(1 -R_1)$$

となり，相当向上することになる。

注(1) 経済審議会情報研究委員会著「日本の情報化社会」 p.26 ダイヤモンド社
(2) このようなシステムは当然価格が高くなるため，非常に高い信頼性が要求される場合以外用いられない。国鉄の座席予約はデュアル・システムである。
(3) 情報処理学会編「情報処理ハンドブック」p.7－40オーム社
(4) 猪瀬博編著「コンピュータ・システムの高信頼化」p.233 情報処理学会

3. EDPシステムの信頼性の概念

コンピュータのハードウェアについての信頼性は，先に述べたように近年著しく向上し，ＥＤＰシステム監査に当っても，「現代のコンピュータは高度の信頼性を備えているので，通常の場合，監査人はコンピュータが確実に稼動

し，機械に基づくエラーが発生してもそれを検出できるものとみることができる。処理上の欠陥が機械エラーの結果であるとわかった場合を除き，監査人は，通常，そのコントロールの効果に信頼してさしつかえない……」[1] といわれるまでになっている。この小論では以下，このようなハードウェアの信頼性を前提として，広義のソフトウェアについて考察するものである。

ＪＩＳによればハードウェアとは，「データ処理システムを構成する装置の総称，ソフトウェアの対照語」[2]，ソフトウェアとは，「計算機のプログラムの総称，計算機の使用法に関する書類化された情報を含めていうこともある」[3] と規定されている。ＥＤＰシステムの設計・運用の見地からする場合，このソフトウェアの規定では，そこで取り扱われねばならない諸問題を包含するには困難であると考えられる。ＥＤＰシステムをとりあげる場合，ハードウェア，ソフトウェア以前に，まず対象となる問題がよく理解されていなければならず，さらに広義に考慮すれば，この問題はとりあげるべきか否か，あるいはコンピュータに何を行なわせるか，ということが研究されなければならない。運用に当っては，プログラムやファイルの管理，さらにＥＤＰ部門の組織，全体の組織でのＥＤＰ部門の位置などが問題となる。先に広義のソフトウェアと述べたのは，このようなアプリケーション・ウェア（application ware）[4] ともいうべき分野も含めて考えている。

ＥＤＰシステムの信頼性を向上させるための要因は，きわめて多岐にわたっている。これを従来から研究されてきている分野との関係で分類すれば，次のように示される。

ＥＤＰシステムの信頼性
- コンピュータ・ハードウェアの信頼性（既述）
  コンピュータ本体，周辺機器，通信回線などの信頼性。
  MTBF，MTTR，可用性の向上。
- セキュリティ（security）対策
  コンピュータ室警備，利用チェック，コンピュータ室防護，事故対策，プライバシー保護など。
- ＥＤＰシステム監査
  システム設計への監査人の参画，各種標準化，内部牽制組織，各種監査技術など。

(1) セキュリティ対策

物理的対策

コンピュータおよび関連機器は，自然災害や故意または過失による物理的破壊の脅威から保護されなければならない。すなわち，台風，地震，落雷，爆発，火災，ストライキ，電力・通信・水の停止などを指すもので，可能性のある脅威は数限りない。特殊な例として，コンピュータがピストルで撃たれたり（アメリカ）猟銃で撃たれた例（オーストラリア）すらも報告されている[5]。我国でもＣＰＵ内にねずみが巣を作ったため，修理に１週間以上も費やしたという例[6]もある。「脅威とその確率および危険の３つの要素はすべて割引いて考えられやすいから，脅威を評価し，確率を推定し，危険を定量化することに意味がある」[7]のである。

こうした状況のもとで，我国では通商産業省が，コンピュータ利用者が安全対策を講ずる際のチェック基準として，昭和52年４月「電子計算機システム安全対策基準」を策定・公表している。これには，安全対策上必要と考えられる68の基準が網羅されている。また，コンピュータ白書[8]ではセキュリティ対策として次のような事項が考えられている。

セキュリティ対策
- コンピュータ室警備
  - 建屋警備設備（要員配置），外来者入室チェック，一般社員入室チェック，コンピュータ要員入室チェック
- 利用チェック
  - 利用者身元チェック，利用者権限チェック，出力配布先チェック
- コンピュータ室防護
  - 火災対策設備，煙害対策設備，水害（含湿害）対策設備，磁気障害対策設備
- 事故対策
  - 二重データ保管システム，二重ファイル保管システム，システム・バックアップ準備

機密保護

ＥＤＰシステムの本質的な機能は，システムに対する入力を処理し，出力することであったが，近年，ＤＡＳＤ（Direct Access Storage Device）など，

大容量で高速の記憶装置の進歩によって，情報蓄積機能の比重が高まってきている。すなわち，従来のデータ・ファイルの概念から発展して，データ・ベース（data base），さらにデータ・バンクの考え方が現われ始めている。

データ・ベースとは，１つまたは複数のアプリケーションにより処理可能な相互関係のあるデータ項目の重複のない集合と定義[9]され，それが企業といった単一組織を超えて，社会的に利用可能になった状態がデータ・バンクと考えられる。そして，通信回線の利用の増大にともなって，ＴＳＳ（Time Sharing System）によって多数の利用者が遠隔地の端末からデータ・ベースを共用する機会が増してくる。蓄積される情報もしだいに価値の高いものとなり，その漏洩・破壊の問題が惹起されてくる。たとえば，故意にしろ偶然にしろ，不当なアクセスのために，ファイルが破壊されたり，企業の経営内容に関する機密情報が利害関係者に引き出されたり，また個人の医療に関する情報が引き出されてプライバシーを犯す，といった可能性が増してくる。このような事態が生じないように「情報の保護」をいかに行なうかがＥＤＰシステムの重要な条件となりつつある。

情報の保護対策として，最も一般的でかつ有効であると考えられているのが，そのファイル・アクセスが正当かどうかをチェックするパスワード（password）による方法であるが，これが完全なものでないことは指摘されている[10]。対策の中核となるものはＯＳであると考えられるが，ＯＳは従来スループットの向上を主目的として発達してきた経過からして，この面での機能を十分備えているとはいい難い。それに，「ＯＳの機密保護問題について議論することはやさしいが，必要な機密保護機能のユーザ引渡し方法はむずかしい。ひとたびソフトウェアが設計された後で，機能を付加させることはメーカーにとって困難なことであり，ユーザにとっても自分のリソースを使って機能を付加させることは実際上不可能である。かりに，機密保護に関する機能が存在したとしても，それらの機能があらゆる関連場面で働いていたことを，有能な技術面の観察者に立証することはむずかしい」[11]のである。

(2) ＥＤＰシステム監査

ＥＤＰシステムにおいても，他の企業活動と同様に，近代的内部監査がその発展と並行的に行なわれる必要があることはいうまでもない。内部監査と外部監査では，その目的に相違があるが，それらが適切に実施されるということは「ＥＤＰシステムの信頼性を高める」ために不可欠のことである。

監査基準の「監査は，過去においては，不正事実の有無を確かめ，帳簿記録の正否を検査することをもって主たる目的としたものであったが，企業の内部統制組織即ち内部牽制組織及び内部監査組織が整備改善されるにつれて，この種の目的は次第に重要性を失いつつある。……」[12] という記述も，ＥＤＰシステムに関する限り必ずしも妥当でないと考えられる。むしろ，Mr. Zzwick事件[13] に典型をみるような，従来とまったく異なる新しい不正の機会が開かれつつあるといえる。表２はアメリカにおける報告例であるが，この種の事件は企業の社会的信用を失墜させるなどの理由で表面化しない傾向があることを

表2　コンピュータ乱用報告例[14]

年	破壊	情報または物的盗難	金銭的詐欺・盗難	用役の不正使用または売買	合計
1958			1		1
62	2				2
63	1				1
64	1	2	3		6
65		1	4	3	8
66	1		1		2
67	2			2	4
68	2	3	7	1	13
69	4	6	3	2	15
70	8	5	10	10	33
71	6	19	23	6	54
72	15	18	16	17	66
73	11	20	26	11	68
74	7	15	25	2	59
75	6	7	26	4	43
合計	66	96	145	68	375

考えると，その発生は，表わされた数字よりかなり多いと考えなければならない。

このような不正行為のみならず，間違ったプログラム・ロジックとか，不注意なオペレーションなどのために生じるエラーは，結果として非常に高価な作業のやり直し（rerun）となり，ＥＤＰシステムの信頼性にも直接係わってくることになる。

監査の見地からする場合，ＥＤＰシステムは多くの問題を含んでいる[15]が，その対策は，(1)一般的な留意事項，(2)ＥＤＰシステム監査技術に大別して，それぞれ次のように表わすことができる。

監査上の留意事項
- システム設計への監査人の参画
  機械化計画の早い段階に計画ならびにシステム設計に参画する。後日になって，ＥＤＰシステムの全体を理解しようとすると非常に困難をともなう。監査のためのコントロール・ポイントの設定などにも役立つ。
- 標準化の推進
  製造部門にくらべて，ＥＤＰ分野の標準化は大巾に遅れている。システム設計段階から，プログラミング，オペレーションに至るまでの広範囲について標準化を推進する必要がある。
- 内部けん制組織
  ＥＤＰシステムにおける基本的な業務の分離は，①システム設計の機能，②機械操作の機能，③データ管理の機械，と考えられる。

システム監査技術
- コンピュータ周辺監査（auditing around the computer）
  ＥＤＰ担当者との面接・質問書の利用。各種フローチャートの検査。エラーリスト，バッチ・コントロール記録，コントロール・トータル，原始証憑などの相互照合。前記の内部けん制，標準化なども合わせて評価する。ドキュメンテーションの整備状況。
- コンピュータを通じての監査（auditing through the computer）
  スナップショット・ルーチン（snapshot routine）などを利用したプログラム検査，テストデータによる方法，監査プログラムによる方法。

（注）

(1) Gordon B. Davis, 染谷恭次郎訳「会計監査とコンピュータ」p.45 日本生産性本部

(2) JIS C6230 番号0113

(3) JIS C6230 番号0128

(4) 太田文平，味村重臣著「日本の電子計算機」 p.33 日本能率協会 にアプリケーション・ウェアの提唱がされている。

(5) Donn B. Parker, 羽田三郎訳「コンピュータ犯罪」p.25 秀潤社

(6) 大阪のＴ社（一部上場）で，昭和40年ＩＢＭ7040コンピュータについて発生している。

(7) American Federation of Information Processing Societies, 横山・萬代監訳「セキュリティ」p.59 秀潤社
(8) '76コンピュータ白書 p.378 日本情報処理開発協会編
(9) 日本事務能率協会編「ＭＩＳハンドブック」p. 614 日本経営出版会
(10) 猪瀬博編著「コンピュータ・システムの高信頼化」p. 218 情報処理学会
(11) American Federation of Information Processing Societies, 横山・萬代監訳「セキュリティ」p.87 秀潤社
(12) 監査基準・準則の第２項（監査の必要性）の一部
(13) Zzwick とは仮空の人名であり，「少額の横領を数多く繰り返す」という手口でコンピュータの機能を利用した典型的な事件である。その詳細については，大塚経営研究シリーズ・第68号（不正行為の用具としてのＥＤＰ）に記載されている。
(14) Donn B. Parker, 羽田三郎訳「コンピュータ犯罪」p.44 秀潤社。同書では，乱用という語を「犯罪」,「反社会的使用」の意味で使用している。
(15) 拙稿「ＥＤＰシステム監査技術の考察」企業診断 Vol.17 No.11 同友館参照

4. 現状調査に当って

ＥＤＰシステムが単純でその適用も部分的である場合は，信頼性の問題もハードウェアのそれが中心で，解決も比較的容易であった。しかし，システムが複雑化し関連分野が拡大するにつれて，システムとしての信頼性を維持することがきわめて重要となり，そのために大きな努力を注がなければならなくなってきている。信頼性の問題は非常に複雑で，多くの要因をもっている。いずれの要因も克明に検討しなければならないが，完全な解決は至難である。

この調査は，ＥＤＰシステムの信頼性確保（または向上）に必要と考えられる多くの要因について，その対策の現状を調べる目的で，下記の要領で実施するものである。

1. アンケート用紙の発送企業は，電子計算機ユーザー調査年報（情報処理会編，日本経営科学研究所発行），日本データプロセシング協会々員名簿，日本内部監査協会々員名簿よりランダムに500社抽出。
2. アンケート回収予定は６月末日。

この現状調査については，「わが国におけるＥＤＰ内部監査に関する現状調

査及び分析（大塚俊郎，田中弘)」として，昭和52，53年度の学内研究助成（No. 5）を受けている。

以下は，調査票の内容（一部省略）である。

Ⅰ．貴社の概要についてお答えください。

A．業種

1．電力・ガス	2．鉄道・運輸	3．繊維	4．食品・水産
5．製紙・パルプ	6．セメント・窯業	7．石油・石炭・鉱業	8．鉄鋼
9．輸送用機械	10．機械・精密機械	11．電気機器	12．化学・薬品
13．百貨店・スーパー	14．貿易・商事	15．保険・証券・銀行	16．その他

B．資本金

1．1億円未満	2．1億円以上	3．10億円以上
4．50億円以上	5．100億円以上	6．500億円以上

C．従業員数

1．500人以下	2．500人以上	3．1,000人以上
4．5,000人以上	5．10,000人以上	

D．初めてＥＤＰ（またはＰＣＳ）を導入された時期

1．昭和20年まで	2．昭和21～30年	3．昭和31～35年
4．昭和36～40年	5．昭和41～45年	6．昭和46～50年
7．昭和51年以降	8．不明	

Ⅱ．貴社の監査部門とＥＤＰ部門の関係についておたずねします。

E．ＥＤＰ導入（または最近のシステム設計）の際，監査担当者がその計画に参画しましたか。

1．委員会などのリーダーまたはメンバーとして参画した。
2．委員会などのオブザーバーとして参画した。
3．必要に応じ助言者として参画した。
4．上記2，3として参画した。
5．参画しなかった。
6．その他（　　）

F．監査担当者がＥＤＰ教育（社内，社外を含む）を受けたことがありますか。

1．システム設計，プログラミングに関する教育を受けたことがある。
2．システム設計に関する教育を受けたことがある。
3．プログラミング教育を受けたことがある。
4．オペレーション教育を受けたことがある。
5．その他のＥＤＰ関係の教育を受けたことがある。
6．ＥＤＰ教育を受けたことはない。
7．不明

G．貴社の監査担当者はＥＤＰ部門の監査を行なっていますか。

1．行なっている（G11～G13の質問にお答えください）
2．行なっていない（G21の質問にお答えください）
3．不明

G11．（ＥＤＰ部門の監査を行なっている場合）主としてどのような方法で監査を実施されていますか。

1．文書報告による書面監査　　2．インタビュー形式による監査
3．現場視察による実地監査　　4．フローチャートによる監査
5．監査用のデータまたはプログラムによる監査
6．システム設計に当初より参加　　7．その他（　　）

G12．（ＥＤＰ部門の監査を行なっている場合）監査の手段としてＥＤＰを利用されていますか。

1．利用している　　2．利用していない　　3．不明

G13．（ＥＤＰ部門の監査を行なっている場合）その頻度は年間どの程度ですか。

1．6回以上　　2．3回以上　　3．1～2回
4．数年に1回　　5．必要に応じ随時　　6．その他

G21．（ＥＤＰ部門の監査を行なっていない場合）将来どのようにお考えですか。

1. 必ず監査するであろう	2. 監査せざるをえないいだろう
3. 監査するかもしれない	4. 監査しないであろう
5. 監査の必要はないだろう	6. 監査できないだろう
7. 不明	8. その他

H. 外部監査人（公認会計士またはその関係者）が監査の目的でＥＤＰ部門を訪れたことがありますか。

1. 年間1回以上訪れる	2. 数年に1回訪れる
3. 訪れたことはない	4. 不明

Ⅲ. 貴社のＥＤＰシステムの安全性，信頼性対策についておたずねします。

I. 貴社のコンピュータ室は，他の部屋と比較して特に災害・人災から保守されるように設計・考慮されていますか。

1. 特別に設計されている
2. 設計はされていないが，何らかの配慮がされている
3. 特に考慮されていない
4. その他（　　）

J. 過去，ハードウェア（情報機器および関連設備）が故意に破損されたことがありますか。

1. ある
2. 故意と思われる破損を受けたことがある
3. 故意・過失は不明だが破損を受けたことがある
4. ない
5. その他（　　）

K. 情報化保険（コンピュータ総合保険，情報処理業者賠償責任保険など）についておたずねします。

K1. ハードウェア（情報機器および関連設備）について保険に加入されていますか。

1. 加入している	2. 検討中	3. 加入していない

K2. 情報メディア（磁気テープ，ディクス等）について保険に加入され

ていますか。

1．加入している　　2．検討中　　3．加入していない

K3．情報処理業を対象とした保険（情報処理業者利益保険，情報処理業者賠償責任保険など）に加入されていますか。

1．加入している　　2．検討中　　3．加入していない

L．重要な磁気ファイルなどの管理状況についておたずねします。

L1．重要な磁気ファイルなどはどのような場所に格納されていますか。

1．耐火金庫などに格納している
2．金庫など施錠できる格納庫を使用している
3．特に厳重な格納庫は使用していない
4．倉庫業者などに委託している
5．その他（　　）

L2．重要なファイルに対して，どのような機密保護対策を講じておられますか。

1．データそのものを暗号によって記録している
2．特殊な操作，キー番号などによらなければ使用できないようにしている
3．上記1，2は採用していないが，管理面で厳重にしている
4．特に対策は講じていない
5．その他（　　）

L3．重要なファイルの更新に際して，旧ファイルどの程度の期間または世代保存されていますか。

1．半永久的に保存している
2．5世代以上保存している
3．3，4世代保存している
4．2世代以下しか保存していない
5．その他（　　）

IV．貴社におけるドキュメントなどの整備・標準化についておたずねします。

M．新規業務のシステム設計について，その手順の設定とか使用する用紙類

を統一するなど，何らかの標準化をされていますか。

1. ほとんど標準化している
2. 一部標準化している
3. 担当者の自由意志にまかせている
4. その他（　　）

N. プログラム作成について，定型的な処理パターンについてはそのフローを定めておられますか。

1. 定めており，保有プログラムの半分以上はそれに従って作成されている
2. 定めており，おおむね守られている
3. 定めているがあまり守られていない
4. 定めていない
5. その他（　　）

O. プログラムの変更について，いつ，誰が，どのような理由で行なったかわかるようなしくみになっていますか。

1. すべてのプログラムについてわかるようになっている
2. ほとんどのプログラムについてわかるようになっている
3. 重要なプログラムについてのみわかるようになっている
4. プログラマーの自由意志にまかせている
5. その他（　　）

P. プログラムの修正・変更には責任者の承認が必要ですか。

1. すべてのプログラムについて承認が必要である
2. 重要なプログラムについてのみ承認が必要である
3. 担当者の自由意志にまかせる
4. その他（　　）

Q. 現在，稼動中のシステムに関する設計書およびプログラム関係書類は保存されていますか。

1. すべての関係書類が保存されている
2. 主なシステムについてのみ関係書類が保存されている
3. 最近完成したシステムについてのみ関係書類が保存されている
4. 担当者の自由意志にまかせている
5. その他（　　）

R．オペレーション・マニュアルは完備されていますか，またその形式は統一されていますか。

1．統一された型式ですべてのオペレーションについてのマニュアルが完備している
2．統一された型式で主要なオペレーションについてのマニュアルが完備している
3．形式は統一していないが，ほぼ完備している
4．担当者の自由意志にまかせている
5．その他（　　）

V．ＥＤＰ部門の組織，業務分担などについておたずねします。

S．ＥＤＰ部門の２つ上位の部門からその名称をご記入ください。
（たとえば，管理本部，経理部，電子計算課）

T．（内部）監査部門の２つ上位の部門からその名称をご記入ください。

U．システム設計（プログラミングを含），オペレーション，ファイル管理の職務は組織的に区分されていますか。

1．課，係などの単位ではっきり区分されている
2．おおむね区分されている
3．特に区分されていないが，それぞれ別の人間が担当している
4．同じ人間が上記の２つまたは３つの職務に携わっている
5．その他（　　）

Ⅵ．コンピュータ室警備についておたずねします。

W1．コンピュータ室専門の警備要員を配置されていますか。
1．している
2．していない

W2．コンピュータ要員の入室チェックをされていますか。
1．している
2．していない

W3. 一般社員の入室チェックをされていますか。

1. している
2. していない

W4. 外来者の入室チェックをされていますか。

1. している
2. していない

V. 重要なファイルの使用に関して，使用手続を定められていますか。

1. 文書類で責任者の承認を得る必要がある
2. 口頭で　〃
3. 承認は必要でないが，何らかの報告は必要である
4. 自由である
5. その他（　　）