JIPDEC ジャーナル

NO.74
1990/DEC

- 春　夏　秋　冬：システム監査におけるリスク分析の重要性
- 寄　稿　・　解　説：通商産業省のセキュリティ関連施策
- JIPDEC REPORT：コンピュータウイルス対策基準について

目　次

No.74　1990/DEC.

春　夏

システム監査におけるリスク分析の重要性

明治大学商学部教授
リスク分析委員会委員長
森宮　康

現代の情報化社会においては，情報システムの利用状況から様々な脆弱性が予想でき，リスクへの対応を重要課題とすべき段階にきている。とりわけ，こうした特徴は，システムを利用する企業の生産・流通等に関わる部門の統合化や，ネットワークの広域化・国際化などを前提とした資金や情報の流れに目を向けるとき，特に象徴的に認識できよう。それというのも，現代の情報化社会において，我々が情報システムへの依存度を増すにしたがい，便利さに比例してリスクが拡大・増大・複雑化するからである。ここで問題となるのは，システムの利用を前提とする社会的な枠組より早いスピードでシステムが導入され，ネットワーク化されたシステムが我々の社会なり経営組織において神経細胞ないし血液の役割を演じてきていることである。

この点，アメリカでも，データ処理，通信，OAが企業経営の中で統合されて来ているが，こうした統合の経験がまだ十分でなく，約15年ほどとされ，しかもこれらが，伝統的な管理体制の中におかれているといわれる(Cash, McFarlan, &McKenney著，小澤，南共訳『情報システム企業戦略論』日経マグロウヒル社，P. 28)。ここがまさに問題の核心となる処である。こうした状況をベースにおいてリスク問題を考える必要がある。企業がコンピュータを単に机上の計算だけに利用していた段階では，コンピュータ関連のリスクについての注意は，いわば「点」という視点から見るだけでよかったわけである。それが，ホスト・コンピュータと接続されるにしたがい「線」となり，ネットワーク化されるに至って，情報システムの脆弱性は「面」(そして立体)にまで拡大されてきているからである。

とりわけ，リスクの問題は，例えば，アメリカン航空の座席予約のセイバーシステムにおけるように，システム化することにより競争における優位を勝ち取り，利益に結実する側面から「事業経営に関するリスク」をみているきらいがある。むしろリスクには，システムの停止・誤作動・縮退，さらには操作者のエラーや悪意・故意の犯罪等が

秋　　冬

原因となり，組織に予期せぬ損失をもたらす側面があるため，この点を軽視してはならないのである。しかも，今後のリスクに関する動向には，システムそれ自体もさることながら，システムと「人」が関係する部面(特にコンピュータ犯罪)こそ重要な問題発生の場となろう。もしも，組織のトップ・マネジメントに後者のリスクの認識がないとすれば，経営目標・方針の達成すら不可能となる場合もないではない。それだけに，情報システムへの依存度に応じて，システム監査を実施する重要性が指摘されるわけである。

ところで，どのようなリスクがシステム利用の組織のどこにあり，それがどんな影響を組織にもたらすのか，この点をなおざりにして現代の経営は成り立たないはずである。この問題の鍵を握っているのが，リスク分析である。システムなりプログラムをわずかなりともいじれば，そこに変化なり変動が生じ，それだけリスクが発生し易くなる。たとえば，プログラムを変える場合でも，税法の変化による税金部分の書き直し，減価償却費率の変更，さらに組織内部の部門の統廃合による組織変更，生産ラインの新設・廃止等により，リスクが発生してくるかもしれないのである。それだけに，リスクを分析することにより，「リスク」の点から，組織の「どこに」問題(脆弱性，リスク発生原因等)があるのか，したがって，システム利用の組織にとり，「どこを監査すべきなのか」，この点についての優先順位の決定も可能となるのである。それにより，「組織の意思決定の際の不確実性を減少させる」のである。

特に，情報システムへの依存度の高いコンピュータ・ユーザでは，団体内部に専門委員会等を設け，システム監査に関する研究活動を多年にわたり継続的に進めており，これも情報化社会の脆弱性についての状況認識を反映してのことと思われる。すでにシステム監査については，通産省が1985年1月25日に「システム監査基準」を公表し，翌年より情報処理システム監査技術者試験を実施に移すほか，システム監査学会も，1987年3月31日に設立され，システム監査に対する社会的認知を高めるべく研究体制の場が広げられてきている。

このシステム監査については「セキュリティ産業研究委員会」の報告書『21世紀へ飛躍するセキュリティ産業—2010年におけるセキュリティ産業市場』(財)日本情報処理開発協会(平成2年3月)を散見すると，セキュリティの観点からみた2010年情報社会の基本理念のひとつに「システム監査の実施」が指摘されており，また産業予測の動向に関する「教育」，「コンサルティング」の部分で，システム監査が包含され，今後10年間のそれぞれの成長率を10%とし，それ以降は年率30%としている。こうした推定の根拠には，汎用コンピュータ台数(1987年9月現在)(『情報化白書1990』(財)日本情報処理開発協会)が34万台を超えているといった他，今後のコンピュータ利用状況に基づいていると思われるが，そこに示されている成長率の高さそれ自体，逆に現在のシステム監査への意識の低さを物語っているといえなくもない。それだけに，システム監査の必要性を理解し，リスク分析をベースに，コンピュータ・セキュリティを含め，費用対効果の点ですぐれたリスク処理方法を導入すべきなのである。

通商産業省のセキュリティ関連施策

通商産業省機械情報産業局
情報処理振興課長　中村　薫

通商産業省のコンピュータ関連あるいは情報サービス産業全体の施策の中で，どのようにセキュリティ問題，ウイルス対策を位置づけ，取り組んでいくかを理解していただくために，そのバックグラウンドについて，説明させていただきます。

Ⅰ．わが国の情報産業の現状

今から約20年前にコンピュータライゼーションといいますか，情報化がスタートしたわけですが，最近5年間は特に目を見張る変化，進展があったのではないかと感じています。

この劇的な変化の要因を考えてみると，

(1)半導体技術の進歩

単位当たりの情報処理コストが急激に低減し，ますます商品サイクルが早くなるという形で，半導体の技術が進んできたこと。

(2)通信コストの逓減

通信面でも，光ファイバーから通信衛星へというように，通信コストが大幅に下がってきたこと。

(3)利用技術面の進展

ネットワーク化というようなネットワーク利用技術の進展が見られたこと。

という3つが挙げられるかと思います。

また，現在情報化の進展が特に目につく分野としては，

①戦略的情報システムのような高度情報システムの構築を進めている企業の分野。

②ファミコンやパソコン利用者が増加している個人や家庭の分野。

③マイコン利用が進む電気機器の分野。

こういった3つの分野で情報化が進んできているように思います。

その結果，情報処理ネットワークが社会のインフラとしての位置を確立したという意味で，この数年の間に質的な変化があったと思います。他方，これを産業のサイドで見てみると，中核になる情報サービス産業の伸びは急速なものがあります。ちなみに，通商産業省が実施しています特定サービス産業実態調査の平成元年度の結果によると，情報サービス産業の売上は4兆3500億円で，前年度比32％増という伸びになっています。その前年，あるいは前々年も20～40％強の伸びですから，特殊要因を除いたとしても年々3割の勢いで成長を遂げているわけです。

このような急速な動きの中で，社会での情報化の位置づけ，あるいは拡大する情報サービス産業が，これから先90年代はどうなるかということを考えてみると，まず90年代の大きな経済のフレー

ムワークから考えると，経済全体のサービス産業化が着実に進むことがアメリカなどの流れを見ても予想されます。その中で日本の経済に期待されているのは，内需中心の経済構造，産業構造にシフトしていくことであると考えられています。また，90年代の大きな課題として，労働時間の短縮を始めとする総投入労働量の低減，さらには，老齢化に伴う労働人口の減少傾向への対応があります。

つまり90年代は，こうしたサービス産業化，あるいは内需中心の経済構造，あるいは労働時間の低減といった流れがフレームワークをつくると思われます。

その中で考えると，企業単位では，労働力の低減に対応して経営を進めていくためにも当然1人当たりの生産性(特にサービス部門，あるいは製造業のサービス関連部門)を上げていくことに力を入れていかざるを得ません。そうなると，やはり現在進められているSISのようなコンピュータ利用を採用する企業が，90年代にはさらに増加していくのは必然です。また，個人単位でも，ファミコンやパソコンが家庭や教育現場に普及し，今後さらに利用者が増加していくことは確実です。

一方，前述した半導体の技術の進展に伴う情報処理コストの低減や通信コストの低減などは90年代を通じて続くと思われるので，情報部門にそういう利用を可能にするような素地は充分にあります。また，それらを利用すれば，例えばマルチメディアの対応とか，あるいはニューロ，ファジイといった新しい技術を，企業や家庭あるいは機器の面に生かすことができるので，社会全体の需要あるいは情報の中のこれら種々の技術の革新ということを考え合わせると，やはり90年代，この傾向は一層続くと考えられます。

そういった意味で，情報サービス産業の規模でいうと，現在4兆3500億円の規模が，毎年20%前後の伸びで推移し，2000年には16兆円程度あるいは20兆円といった規模になるだろうと予想されるわけです。また，情報サービスネットワークも現在の広がりをさらに超えて，単にローカルなネットワークからグローバルなネットワークへと，さらに拡大していくことが考えられます。

II. 情報産業の拡大と問題点

情報サービス産業は，現在までこのように順調に伸びてきており，2000年に向かいさらなる拡大が予想されている分野ですが，他方このような拡大の過程で種々問題もあります。それらの主なものとして2つを挙げると，

第1点がいわゆるソフトウエア・クライシス対応

第2点がセキュリティ問題

ではないかと感じています。

まず，ソフトウエア・クライシス問題について簡単にいいますと，我々が数年前に研究したところでは，先ほど触れたような需要の拡大に伴い，2000年には100万人弱の情報処理技術者が不足します。現在，既に人材不足ということが言われていますが，この人材不足という問題は90年代を通じての大きなテーマになっていくということです。この基本的な問題は，需要の増加がそのまま必要となる人材，人員の数に比例してしまう現在の構造を変えていかなければ解決しないので，欧米並みにパッケージソフトを効果的に使用したり，ソフトウエアの生産体制といったものを根本的に組み替えて，より効率的な，例えばコンピュータを利用したようなソフトウエアの作成といった形に生産体制を移行していく必要性があります。

そのために我々は従来からシグマシステムの開発を行い，本年4月からは会社方式による事業化を進めつつあります。その結果，この5年間にソフトの生産プロセスをコンピュータライズしていくというコンセプトは確立し，そのツールとして，ワークステーションなりUNIXなりを使っていくという流れも着実に広がってきています。今後，この4月から発足した事業会社の成果が活用され，大きな流れになればと考えています。

また，こうした構造の変化と合わせて，人材育成についても正面から取り組んでいるところです。20年来実施している情報処理技術者試験に加え，専門学校のレベルアップを目指した情報大学校構想，あるいは東京以外の地域におけるシステムエンジニアの育成を目的として，昨年からスタートした地域ソフトウエアセンターの指定などを現在進めているところです。これで十分かどうかは別にしても，それなりの体制は整いつつあると思っています。

もう一つの大きな課題であるコンピュータセキュリティ対策については，やはり50年代前半から安全対策基準の制定，あるいは安全対策実施事業所認定制度，システム監査などを中心に進めてきました。しかしながら，前述したように社会全体，あるいはグローバルな情報システムがさらに出現してくるという前提で考えると，そのエラーや事故，犯罪が与える影響の範囲というものはますます拡大し，常に新たな問題への対応が求められる分野です。

また，コンピュータセキュリティ対策の性格として，グローバルなネットワークシステムが対象となるので，非常に多くの人々の協力を必要とし，また，そのシステムによって当然注意すべき範囲や程度，あるいはそれに伴うリスクも違ってくるので，システムの違いを念頭に置いて進めなければならず，なかなか難しい面があります。従来だと，単に企業内だけのシステムでその影響も企業内に留まっていたため，安全対策の必要性についてもその程度の認識をされていたものが，今後はVANで結びつき，流通段階やファイル管理その他のシステムを通じて外にも影響を与えてしまうようなシステムに変化しているので，常に新たなリスクに対応できるような対策を進めていくことが必要になるかと思います。

Ⅲ．通商産業省におけるコンピュータセキュリティ対策

従来，我々が進めてきた施策についていいますと

1．基本となっているのが，「電子計算機システム安全対策基準」という基準で，昭和52年に制定し，59年に大幅に改正しています。これは，運輸省や大蔵省などの関連各省が，その主管である業態の安全基準を作成する際のベースにもなっており，広く社会に受け入れられた安全基準であると思っています。しかしながら，技術の進展，あるいは社会的な影響度の拡大といったようなものは着々と進み，ウイルスもその一つですが，例えば，フロン系の消火器をどの様に考えるのかとか，あるいは安全対策を前提としたビルの基準を明確にしてほしいというような新しい要望も出てきているので，それらを踏まえて見直していく必要があると思っています。

2．また，この安全対策基準を受けて，情報処理サービス業を対象にした「安全対策実施事業所認定制度」という制度があります。これは昭和56年に創設されて，現在までに163事業所がこの安全対策を行っているということで認定を得ています。今後，いわゆる情報サービス産業の拡大に伴い，

我々としては本制度がより一層活用されるよう，必要に応じて手直しをしていこうと考えています。

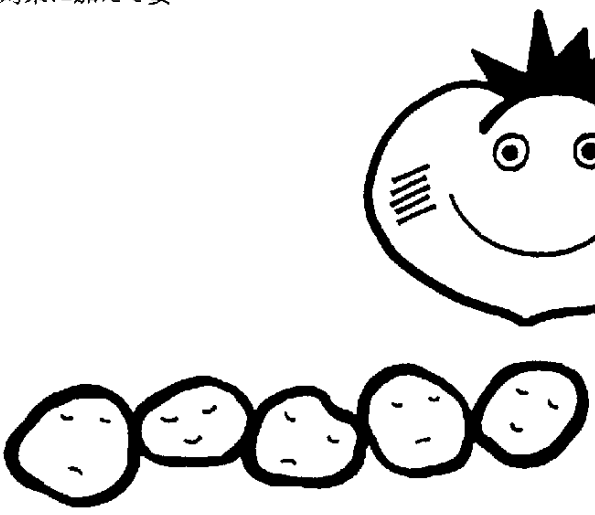
3．次に，「システム監査基準」ですが，コンピュータシステムを第三者の公正な立場から総合的に点検評価をする，あるいはセキュリティ対策の実効性を担保させるといった意味で，システム監査は非常に大きな役割が期待されています。このため通商産業省としては，昭和60年にシステム監査基準を策定し，具体的なシステム監査の対象，システム監査人の要件，あるいは具体的な実施内容などをガイドラインとしてまとめました。また，監査を実施する者の資格に関連して，昭和61年度から情報処理技術者試験の科目にシステム監査という項目を入れて，システム監査技術者試験をスタートさせました。

システム監査については，昨今非常に重要性が指摘されていますが，実際の実施状況を見てみると，必ずしも広く行われている，あるいはその試験に合格した専門家によってきちっと行われているわけでもありません。

そのためにも，今後さらに拡大するネットワーク社会の中で，システム監査の一層の定着ということが必要ではないかと思っております。

4．最後に，今後，個々の安全対策に加えて安全対策を講じてもなおかつ事故が起きた場合の保険制度，あるいは事故が起きた場合の「バックアップセンター」なりバックアップ体制の整備といった総合的なセキュリティ対策も考えていく必要があります。例えば，バックアップセンターについては，前々から，税制上，あるいは融資等の助成措置を講じてきているわけですが，今後，先日のサンフランシスコ地震，あるいは次第に広がってきているウイルス等々の問題から考え，より一層の対応の必要性が感じられます。ですから，ユーザはそれぞれのシステムの性質を考慮しながらリスクを分析して，最適の対応を取っていくことが必要ですし，また，我々としてはそのための共通のリスク分析の方法といったフレームワークを提示することが重要かと思っています。その点については，現在日本情報処理開発協会の方でいろいろ研究をしており，近々それがまとまれば，またいろいろな形でご報告できるのではないかと思っています。

以上，我々が考えるコンピュータセキュリティ対策の概要，及びその前提になっている情報化，あるいは情報サービス産業に対する我々の認識というものを簡単に説明させていただきました。



コンピュータウイルス
対策基準特別講演会

通商産業省では，最近情報化社会の新たな脅威となりつつあるコンピュータウイルスに対する対策として平成２年４月に「コンピュータウイルス対策基準」を策定し，本格的な予防対策の指導に乗り出しました。

当協会では，行政支援の一環として，同基準の普及と効果的な運用方法の確立のため，４月25，26日の両日にわたって，「コンピュータウイルス対策基準特別講演会」を開催致しました。

本誌では，２日間行なわれた講演会プログラムの中から，

①コンピュータウイルス対策基準

②パネルディスカッション

について内容を要約し，以下に掲載致します。

「コンピュータウイルス対策基準」について

通商産業省機械情報産業局情報処理振興課

安全指導係長　佐藤 直一

通商産業省では，平成2年4月にコンピュータウイルス対策基準を策定しましたが，本項ではコンピュータウイルス対策基準について，大きく分けて次の4点を中心に説明いたします。

Ⅰ．コンピュータウイルス対策基準策定に至る背景。

Ⅱ．ワーキンググループ及び情報化対策委員会電子計算機システム安全対策部会の検討内容。

Ⅲ．コンピュータウイルス対策基準及び解説書の特徴と留意点。

Ⅳ．これからの対策。

Ⅰ．基準策定に至る背景

通商産業省では，従来からコンピュータの普及とともに，安全対策についても積極的に取り組んできましたが，具体的には，昭和52年の電子計算機システム安全対策基準に始まり，56年の情報処理サービス業，電子計算機システム安全対策事業所認定制度，それから昭和60年のシステム監査基準などがあります。

このような中にありまして，一昨年，日本電気が主催するパソコン通信ネットワーク，通称PC-VANにコンピュータウイルスが入ったとか，また昨年末には，東大原子核研究所，阪大理学部高エネルギー物理学研究所にコンピュータウイルスが入った等，最近，多くのコンピュータウイルスの被害が報道されています。幸いにして大きな被害は無かったようですが，ウイルスがわが国でも現実に発生してきています。

一方，海外に目を向けて見ますと，クリスマスツリーウイルスとか，インターネットワームウイルスとか，パキスタンウイルス，イスラエルウイルス，フルショット4ウイルスなどさまざまなウイルスが出ており，中には1万台以上に被害を出したというウイルスもあって，大きな問題になっています。

アメリカのコンピュータウイルス産業協会の調査によると，昨年の11月末で，IBMパソコン関係で51種類，マッキントッシュ関係で13種類，ネットワーク関係で2種類のウイルスがあると報告されています。日本ですと，同じ時期の，去年の11月ごろには5種類程度しか発見されていませんので，海外では既に相当数のウイルスが出ているということがいわれています。

いずれ，わが国におきましてもコンピュータウイルスの被害は，今までのパーソナルコンピュータシステムのみならず，ホストコンピュータシス

テムにまで被害を及ぼし，ひいては社会全般の活動にも大きな影響を及ぼすであろうことが懸念されています。

通商産業省といたしましては，こういう新しいリスクとしてのコンピュータウイルスに対しては，前に述べたような基準では十分に対応できないという判断に立ち，またその影響の大きさ，スピードの早さ，といったことを考慮して早急に対応策を示す必要があるという観点から，コンピュータウイルス対策基準を策定しなければいけないという判断に至った次第です。

基準を作る前に，基準の柱として5つの基本線を考えました。

第1の柱は，まず基準の文章自体をなるべく簡潔にして，汎用性をもたせるようにする。これは，ウイルス自体が変化することが考えられるので，なるべく変化に対応できるような形を取りたいと考えました。

第2の柱は，基準が簡潔であるため，理解しにくい点が出てくる可能性があるので，別に解説書をつくって詳細な補足説明をする。

第3の柱は，コンピュータウイルスは波及速度が早く，その及ぼす影響が大きいので，大至急対策をとらなければいけないと考えました。そこで，目標として，本年の4月13日がたまたま金曜日だということもあり，13日の金曜日ウイルスというものがありますから，それが出るまでの間には基準を完成させたいということで最終のまとめの期日を決めました。

第4の柱は，暗号等，理論上コンピュータウイルス対策として有効なものはありますが，現在はあまり使われていないものは，削除するという観点に立ちました。

第5の柱は，コンピュータウイルスはネットワークを通して広範囲に影響を及ぼすので，今回の基準に関しては他の基準と異なり，官報告示をして広く国民に知らしめる必要があるという観点に立ちました。

以上の5つが基準の柱となる基本線です。

II．ワーキンググループおよび電子計算機システム安全対策部会の検討内容

前述の基本線に沿って一応基準を作成することになりましたが，具体的な作業は，コンピュータウイルスに特に詳しいと思われる専門家の方々にお集まりいただき，昨年の12月に開始いたしました。

ワーキンググループでは，NIST(National Institute Standard of Technology)の『マネージメントガイド』と情報処理振興事業協会が平成元年4月にまとめた報告書『電子ウイルスの現状と課題』と，昨年11月に警察庁から出された指針等について内容を検討するとともに，各委員からコンピュータウイルスに対する考え方，あるいは実際にコンピュータウイルスの被害を受けた会社のメンバーの報告等を聞き，多面的に検討を行いました。その後，対策項目を各委員に作成していただき，委員間での検討を経て，通商産業省の5つの線に沿った形で基準を作成しました。

ワーキンググループの議論では

(1) 基準の切り口をどのようにするか。

(2) コンピュータウイルスの定義自体をどのように考えるか。

(3) 基準案の中の項目で大きくとらえられているものと，小さくとらえられているもののバラツキについてどうするのか。

(4) 基準の中の項目を実施する場合には，ある程度使い勝手が面倒になる。システムが小さいようなものまで，守らなければいけないことにするのか。

といった4つの問題が出ました。

まず，(1)の基準の切り口をどうするかという問題が一番大きな問題だったのですが，具体的には，

基準の分類案として，

①PCレベル，UNIXレベル，汎用レベルといったハード面からの分け方。

②オペレーション，独立系，ネットワーク系というシステムの形態による分け方。

③機密性，完全性，可用性といった項目の性格からの分け方。

④予防，検知，事後対応といった対策の機能別の分け方。

⑤ユーザ，管理者，開発者といった担当業務による分け方。

という5つの案が出ました。

まず，①のPCレベル，汎用レベルについては，技術進歩が非常に激しい中でこういった分け方をしてもすぐに陳腐化してしまうので難しいだろうということでした。

②のオペレーション，独立系，ネットワーク系については，ただレベルが違うだけということで不採用となりました。

③機密性，完全性，可用性という分類については，海外では実際に情報セキュリティの目的をこのように分けていることもあり，日本でも同様に扱おうという考えもありますが，日本ではまだ，概念というものが固定しておらず，定義づけも難しいということもあり，基準自体を非常にわかりやすい形にしたいということから，これも不採用になりました。

④予防，検知，事後対策についてですが，実際には予防と検知というのはほとんど同じようなものなので，分ける意味が無いということで，結論として5番目の，今回まとまったような基準になった訳です。

(2)のコンピュータウイルスの定義をどのようにするかという問題は，具体的には，ハッカーとかワームをどのように扱うかということでした。まずワームについては，一般的なコンピュータウイルス同様他のプログラムに侵入してくるものですが，システム機能を利用して侵入してくるという点で相違があります。しかし，被害を与えるという意味では同じであり，この基準では，コンピュータウイルスの中にワームも含めて考えるという結論に達しました。

ハッカーについては，他人のものを無断で見ているというだけですから，コンピュータウイルスの予防をしていれば，ハッカー対策にもなるということで，別に考える必要はないとの結論に達しました。

(3)の基準の項目で，大きくとらえられているものと，非常に狭い範囲でとらえられているものとのバラツキについては，非常に重要なものは細かくても示す必要がある，その方が実際には効果が出るということから，基準の中では，若干細かいものと，大きなものとに分かれているものがあります。

(4)の基準の中の項目を実施する際に，ある程度使い勝手が面倒になるが，システムの小さいものでは守らなくてもいいのかという点については，この基準自体が強制力があるわけではないので，基準を利用する人がウイルス対策に必要かどうか判断し，自分が必要ないと思う場合には，それは使わなくても良いという結論に達しました。

この様な議論を踏まえ，ワーキンググループでは基準案と解説書の原案を作成し，基準案については電子計算機システム安全対策部会に提出しました。

解説書原案の作成については，基準項目ごとに趣旨と対策のポイント，具体例を記し，基準でわかりづらい点をできるだけカバーすることを念頭において作業を進めました。

ワーキンググループの活動はひき続き進められたわけですが，その間に，通産省内に機械情報産業局長の私的諮問機関として，情報化対策委員会

電子計算機システム安全対策部会を設置し，検討のうえ基準案の報告を公式に部会から通商産業省に提出していただきました。

部会の中では，

(1) 基準の項目がパーソナルコンピュータでしか使えないもの，あるいは汎用コンピュータレベルでしか使えないものが混在しており，整理をする必要がある。

(2) 用語の定義で，コンピュータウイルスの機能を自己伝染機能，潜伏機能，発病機能と書いてあるが，人によっては一般的な病気ととる人もいるので，なるべく病気の表現をしない方がよい。

(3) コンピュータシステムの相違，機種の相違，ソフトウェアの設計等によって使えない項目があるが，それをどのように扱うか。

(4) システム監査を基準に入れるべきかどうか。

(5) 基準自体の，使う人にある程度選択させるという趣旨からすると，システム管理者基準，ソフトウェア開発管理者基準の事後対応の項で明記されている，「コンピュータウイルスが発見された場合，公的機関に届け出をする」という項目は意味があるかどうか。

という5点について特に議論がなされ，それぞれの項目について以下のような結論に達しました。

(1) 基準の項目がパーソナルコンピュータでしか使えないもの，あるいは汎用コンピュータレベルでしか使えないものが混在しているので整理すべきであるとの意見については，基準に汎用性を持たせたいという意味もあり，基準には入れないで，解説書の方で明記をする。

(2) 用語の定義でコンピュータウイルスを，病気と取ってしまう人がいるということについては，コンピュータウイルスが怖いものであるという認識を持たせる必要性からも，このままの表現にしておいた方が良い，また海外でも実際にこういう表現を使っているということで合意された。

(3) コンピュータシステムの相違，機種の相違，ソフトウェアの設計等によって使えない項目の扱い方については，基準の正しい使い方をしてもらうという意味で非常に重要であるため，留意事項である程度詳細に表現をするということで合意した。

(4) システム監査を基準に入れるべきかどうかという問題は，コンピュータウイルスに対しては直接的には有効ではないがシステム監査の信頼性，安全性を確保するという点では重要なので，留意事項の中に入れ，システム監査をする際に，ウイルス対策基準に準じた監査方法を進めたらどうかという結論に達した。

(5) 基準の趣旨からすると，コンピュータウイルスが発見された場合に公的機関に届け出をさせることに，どれだけ意味があるかということに対しては，基準はある程度選択して使用することには問題ないが，事後対応，特に届け出については，被害の拡大，再発を防止するという観点から，また，コンピュータウイルスの正しい情報を収集し，ワクチン情報等を第3者に知らせるためにも非常に重要であるため，強制ではないが，機会があるごとに協力を呼びかけるということで合意された。

III. 基準及び解説書の特徴と留意点

コンピュータウイルス対策基準については，部会の報告を3月28日に通商産業省にいただき，「省内で所定の手続きを経て，4月10日に，「通商産業省告示第139号」で官報告示をしました。

基準の具体的中身ですが，まず基準の考え方と，具体的な対策項目からなるコンピュータウイルス対策基準からなっています。

基準の考え方は，基本的事項と留意事項，用語の定義という3つからなっており，

(1) 基本的事項では，基準の構成について述べられています。基準はユーザ基準，システム管理者基準，ソフトウェア開発管理者基準の3つから構成されており，

①ユーザ基準には，システム利用者のためのソフトウェア管理，運用管理，ウイルスに汚染された場合の事後対応について記してあり，全部で19項目。

②システム管理者基準は，システム管理者のためのソフトウェア管理，運用管理，ネットワーク管理，事後対応の対策について記してあり，全部で27項目。

③ソフトウェア開発管理者基準は，ソフトウェア開発管理の責任者のための開発環境管理，製品管理，事後対応についての対策について記してあり，全部で13項目。

からなっており，これらは基準の骨格について説明をしています。

さらに，本基準はコンピュータウイルスに対する予防，検知，事後対応についての実効性の高い対策を取りまとめたということで，基準の基本的概念を示しています。

(2) 留意事項は，基準を使う際に特に注意してもらいたい点，基準以外でもセキュリティを強化するものがあるので，そういう点を記してあります。

①基準を適用する場合に，使用しているコンピュータシステムの規模や形態や業務の実態に即して行う。

②ユーザ基準，システム管理者基準，ソフトウェア開発管理者基準はそれぞれ独立しているので，利用者はそれぞれの立場から基準を活用していただきたい。

③コンピュータウイルスということではないが，入退室管理とかの一般的コンピュータセキュリティについても非常に重要であるので通商産業省でとりまとめた「電子計算機システム安全対策基準」を活用することが望ましい。

④システムの安全性，信頼性を確保するという観点から，システム監査を実施することはコンピュータウイルスにも有効で，そのための方法として「システム監査基準」がある。ただし，現行の「システム監査基準」では，特にコンピュータウイルスに対する項目はないから，監査に当たっては「コンピュータウイルス対策基準」を活用することが望ましい。

(3) 用語の定義は，7つの用語からなっており

①コンピュータウイルス：第三者のプログラムやデータベースに対して，意図的に何らかの被害を及ぼすようにつくられたプログラムであり，以下その機能を1つ以上有するもの。

・自己伝染機能：自らの機能によって他のプログラムに自らをコピーし，またはシステム機能を利用して自らを他のシステムにコピーすることにより，他のシステムに伝染する機能。

・潜伏機能：発病するための特定時刻，一定時間，処理回数等の条件を記憶させて発病するまでの症状を出さない機能。

・発病機能：プログラムやデータ等のファイルの破壊を行ったり，設計者の意図しない動作をする機能。この基準では，ファイルの破壊だけでなく，設計者の意図しない動作についても発病機能として捉える。

②ユーザ：各種のコンピュータを利用する者ということで，実際には，パーソナルコンピュータから大型汎用コンピュータまで全ての利用者を意味する。

③システム管理者：コンピュータの資源を運用管理する者。

④ソフトウェア開発管理者：ソフトウェアの

開発管理を直接に担当する者。

⑤特権ユーザ：ユーザのうちで，そのシステムの維持，運用のための特定された機能にアクセスできる資格を与えられた者。

⑥ソフトウェア：システムプログラム，アプリケーションプログラム，ユーティリティプログラム等を全部含める。

⑦ネットワーク管理：ネットワーク内の機器，接続方法，接続相手に関する情報管理。

の7つであります。

次に，基準の中の，通商産業大臣が別に指定する公的機関への届け出に関してですが，

(1) システム管理者基準の中の事後対応の最後に「被害の拡大及び再発を防止するために必要な情報を，通商産業大臣が別に指定する公的機関に届け出ること」

(2) ソフトウェア開発管理者基準の中の事後対応の最後に「製品にウイルスが発見された場合には，被害の拡大及び再発を防止するために必要な情報を，通商産業大臣が別に指定する公的機関に届け出ること」

という2つの項目があります。

まず，届け出をする人ですが，届け出の義務が生じるのは，システム管理者とソフトウェア開発管理者の二人で，ユーザについてはありません。ユーザの場合には，異常が発生した場合にシステム管理者に連絡することになっています。コンピュータウイルスといっても，ほとんどの場合，九十何パーセントがバグというケースであるといわれていることから，システム管理者が調査をした方が望ましく，ユーザが調査をするとしても，実際のところ，時間的にも調査能力という面からも難しいということで，ユーザには届け出の義務は課していません。

ソフトウェア開発管理者に対しては，製品にウイルスが発見された場合に特定していますが，これについては，開発段階であれば試行錯誤の繰り返しをしているわけで，実際のところバグなのかコンピュータウイルスなのか，判断が非常に難しく，また仮にコンピュータウイルスが入っていたとしても，ソフトウェア開発管理者であればすぐに除去してしまうケースが多いだろうということで，この中には載っていません。ただし，製品に万が一コンピュータウイルスが発見された場合には，その影響が非常に大きいので，公的機関に届け出をすることが望ましいということです。

次に，なぜ届け出という項目を入れたかについてですが，コンピュータウイルスが発見された場合，今までは，

- 被害を内密にするケースが非常に多かったので正しい情報が伝えられていなかったケースが多い。
- 同じようなコンピュータウイルスの被害があったとしても，情報が不足していたので，ワクチン等をつくる場合でも，自分のところでつくる必要があった。
- 内密にしているため，実際にどの程度の被害があったのかが不明であり，コンピュータウイルスが悪いものであるという認識自体確立もされていない。

ということが現状なので，まずコンピュータウイルスに対する正しい情報をどこかに収集させ，そこから正しい情報をコンピュータシステムを使っている人たちに提供することが非常に重要ではないか，ということから設けました。また，届け出機関については，通商産業大臣によって情報処理振興事業協会，通称IPAを指定(平成2年4月25日付通商産業省告示176号)しました。

次に届け出をする際の手続きですが，

①コンピュータウイルスが発見された場合，まずIPAに電話等で連絡をする。

②実際にウイルスだとわかった場合には，所

定の書類を提出する。

ということです。ただし，バグの可能性が非常に高いので，複数の関係者によって判断した上で，連絡をとっていただきたいと思います。

IPAでは，届け出があった場合には，必要に応じてIPAの中にコンピュータウイルス対策委員会を開催して，届け出の内容を調査検討し，緊急を要すると委員会が判断した場合には，至急公表をすることを考えています。緊急性のないものというのは，類似のウイルスというケースですが，その場合には，ある程度まとまった段階で公表する方向で検討中です。

届け出のあったものの中には，類似のウイルスもあるかと思われますが，その場合にはIPAでできるだけワクチン情報を入手しておき，「どこどこに行けばこのワクチンはあります」という様な情報を提供できるようにしたいと考えています。

この基準は強制規定ではないので，届け出に当たっては強制力はないのですが，コンピュータウイルスの被害の拡大，再発を避けるために，また個々の企業の対応だけでは対応し切れないものについて有効な手段だと考えています。

次に解説書ですが，「解説についての留意点」として

(1) 解説の内容として，基準の解説は，全項目について「基準の主旨」「対策のポイント」「具体例・その他」の3つの側面から説明を加えています。

(2) 基準とコンピュータ種別の対応としては，OSの種類により大きく2つに分けています。AとBに分け，Aは，シングルユーザ，シングルタスクを基本としたOSで，一応パーソナルコンピュータを意識しています。Bは，マルチユーザ，マルチタスクOSで，この中ではワークステーションとかミニコンピュータ　汎用コンピュータ，パーソナルコンピュータの上位クラスの部類が含まれます。このA，B分けを意識して，基準では付けられませんでしたが，解説書では一応の目安として，適用できるものは◎，基本的には適用できるが，一部に例外があるものについては○，適用できないものは×と明示しました。◎，○，×については，一応1990年現在における分類です。

なお，コンピュータウイルス対策基準解説書は，日本情報処理開発協会から発刊されております。

Ⅵ. 今後のコンピュータウイルス対策について

最後に，今後コンピュータウイルス対策を実施していく上で留意して頂きたい点として

1. 使い勝手等が非常にめんどうだということで，すでに個々のシステムに備わっているセキュリティ機能を省いて使わないでもらいたい。備わっているセキュリティ機能はフルに活用してほしい。
2. コンピュータウイルスが発見された場合には，必要な情報をIPAに届け出をしていただきたい。
3. コンピュータウイルス対策基準を正しく使ってもらいたい。
4. 他人のものに対して害を与えるコンピュータウイルスは，被害を受けた人だけの問題ではなくて，コンピュータシステムを利用する人すべての問題だという意識を持っていただきたい。
5. コンピュータウイルスを実際に発生させないということは非常に難しいわけで，現在のところ，一般的な学校教育とか企業内の教育等で，個人の倫理観を高める以外に手段はないと思われるので，企業内の教育を一層充実させていただきたい。

という5点を挙げておきたいと思います。

パネルディスカッション

「コンピュータウィルスをいかに防止するか」

コーディネータ　田中正憲（富士通㈱　情報システム事業本部　企画部　標準推進室　部長付）

パネリスト　生田英機（日本電気㈱　ＶＡＮ技術本部　本部長代理）

岡本栄司（情報処理振興事業協会　技術センター　研究員）

佐藤直一（通商産業省　機械情報産業局　情報処理振興課　安全指導係長）

古瀬幸広（㈱プロファイル　編集長）

吉村　伸（東京大学　教養学部　助手）

服部武司（ＮＴＴデータ通信㈱　開発本部　第１製品開発部　第５開発担当部長）

田中　まず最初に，コンピュータウイルスに対応する際にどの様な課題があるのか，また，どの様な問題が隠されているのかといった点についてパネラーの方々のご意見をおうかがいしていきたいと思います。

最初に，生田さんからその辺のところをお話しいただけますでしょうか。

生田　御存じのように，ウイルスは世界的にかなり以前から騒がれていますが，日本国内でも去年ぐらいから具体例が見つかったということで，平成元年がいわばウイルス発生元年と言えるかと思います。そういった意味では非常に話題性があるので，残念ながらこれからしばらくいろいろな形でウイルスが発生する可能性は高いのではないかと考えています。

ただ，ウイルスそのものは発展していけば経済活動を著しく混乱させる程の要素を持っていますが，今現在はいたずら的な要素にとどまっているので，この時期に世間にウイルスに対する知識が普及し，対策がなされれば，これは非常に望ましいことだといえます。

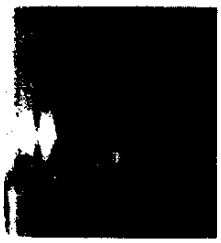
ウイルス対策としては技術的な観点からの対策というものが考えられますが，技術には限界がありますので，作る側はもちろんサービスや機能ばかりでなく安全性をも考慮して提供していかなければなりませんが，利用する側も安全はただでは買えないといった認識を持つなど作る側，利用する側双方が注意していかなければならないと思います。

また，ウイルスがメインフレームの様な大型コンピュータにまで侵入するのではという不安は当然出てくると思いますが，大型コンピュータはOSを中心にいろいろなセキュリティ機能が用意されているので，それを本当に上手に使えば，現在生

まれているようなウイルスはそう簡単には入り込めません。今までウイルスの被害にあっているのは，そういったセキュリティ機能をうまく使えていなかったり，もともと機能を持たないパーソナル・コンピュータだったので，今後一般利用者が使えるようなセキュリティ技術が普及していけば，少なくとも現在のようなウイルスはかなり防げると考えられます。

田中　ありがとうございました。次にIPAで実際にワクチンを研究なさっている岡本さんに，今後の技術的な対応の方向についてご意見をうかがいたいと思います。

岡本　ワクチンに関していいますと，ワクチンには，予防，検出，回復の3つの機能がありまして，予防と検出についてはどんなウイルスにも対応できますが，回復機能を持つものについては個々のウイルスに合わせたワクチンを作らなければならないので，現在出ているワクチンを利用するための情報提供をしていくというような形になろうかと考えております。



いずれにしても，ソフトのみでウイルス対策をするのは限界があるので，ハード面からも対策を考えていく必要が出てきていると思います。

IPAで現在検討中の技術としては暗号技術が挙げられます。これは，デジタル署名などによりソフトウエアを改ざんした場合に検出できるようにする技術で，特に公開鍵暗号系のRSA暗号が有名です。マサチューセッツ工科大学のリベースト・シャミア・エーデルマンという人がつくったRSA暗号を使うとデジタル署名が容易にできるというもので，このデジタル署名がCRCのパリティーチェックのような働きをして，途中で改ざんされると合わなくなるので検出や予防に役立つのではないかと考えています。ただし，ただ作るだけではそういった機能をパスするウイルスがまた出てきてしまうので，運用方法についても慎重に検討していかなければならず，今はまだ研究調査段階です。

私自身は，ウイルスは日本ではあまり広まらないだろうとタカをくくっていたのですが，最近マスメディアを見てますと結構あるようですし，実際に調査してみても思ったよりはあるんだなという気がしました。したがって，やはり技術的な対策システムを作らなくてはならないと考えて努力しているところであります。

田中　どうもありがとうございました。今，ご説明があった暗号技術というのは理論面ではかなり進んでいますが，これを実際のパソコンレベルで実現するにはまだ課題があるようなので，やはり情報の迅速な提供というのが当面，一番効果的な手段ではないかと思います。

次に，服部さんにやはり将来的なところを一言お願いいたします。

服部　将来的ということになるかどうかわかりませんが，従来官公庁向けの専用端末類は，どちらかというとノンインテリジェントの端末であったり，インテリジェンシィがあったとしても専用のモニターを使って動いていたのでなかなかその仕組みがわからずウイルスも作りにくかったのですが，現在では官公庁からも汎用的なOSを使った端末の需要がかなりでてきています。

こういう汎用のOSはいろいろなところでウイルスが作られているので，ウイルスが侵入する可能性も高くなります。一見ウイルスに侵入されにくい専用線を使用している閉じられたシステムであっても，家庭用の汎用OSパソコンで使ったフロッピィを会社に持ってきたり，会社の仕事をちょっと家に持って帰ったりすれば当然ウイルスが

入り込む危険性は高くなってきます。そのためにも，企業内でのルール作りだけでなく個人ベースでの対策も考えていかなくてはなりません。

田中　どうもありがとうございました。それでは佐藤さんは将来的なところをどのようにお考えでしょうか。

佐藤　私どもとしましては，今後もウイルスの被害は増えてくるだろうという前提に立ってコンピュータウイルス対策基準を作ったわけです。ですが，この基準があればよいというものではないので，利用者が自分のシステムは自分で守るという態度でウイルスに対処していただきたいと思います。

田中　ジャーナリストの古瀬さんとしてはどの様にお考えですか。

古瀬　ウイルスの記事を最初に書いた頃，非常にまずいときにまずいものがはやり出したなと思いました。ウイルスを防ぐためには正規のソフトウエアを使うのが一番よいのですが，日本のコンピュータ市場，特にパーソナル・コンピュータ市場がまだ成熟していないためハードウェア，ソフトウェア双方ともアメリカなどに比べるとまだまだ価格が高く，そう簡単には買えません。そこで不正コピーという問題が出てきてしまうのですが，ただ，ある意味では今はソフト代の中には何が含まれているのかということを広く認識してもらう良い機会であるとも言えるでしょう。ソフトを不正コピーして使うと，一見得をしたようにみえますが，万一，ハードディスクの内容が飛んだらそれどころではないのですから，実際にはソフト代で安全も一緒に買っているのだということです。また逆に言うと，みんなが正規のソフトを買うようになればソフト代も安くなるはずなんです。

田中　どうもありがとうございました。最後に吉村さんはいかがでしょうか。

吉村　将来ということですけれども，コンピュータのパフォーマンスというのは1年にMIPS値が倍になるようなペースで年々爆発的に向上してきています。ですから，1人のユーザーが使えるコンピュータファシリティも，数年前に比べると飛躍的に増えたわけです。かつてパフォーマンスが非常に低かったときは，自分の仕事以外のことにCPUが使われるというのは，仕事が遅くなってしまうので非常に困ったわけですが，これだけCPUが早くなってコンピュータのパフォーマンスが向上してきたのですから，ただ，早くなった，早くなったと喜ぶだけでなく，その一部をセキュリティ確保に割くことを考えたらよいのではないかと思います。

もう1つは，理論と実装という面ではどうしても若干のずれが生じるので，理論どおり実装できないケースも出てきます。そういった点を考えると，テクノロジーの進歩や標準化ということを追求するのもいいんですけれども，テクノロジーというのは，ユーザにとってはいい意味で枯れているということも必要です。次々と新しい標準，基準が出てきますが，ユーザが非常に多くて十分にバグが取れていること，セキュリティホールが寄ってたかってつぶしてあるということは，大変貴重なことであるということを認識してはどうかと思います。

田中　どうもありがとうございました。今の吉村さんのご説明にあったように，情報システムの世界ではあちこちで標準化をやってくれという話が持ち上がっています。しかしセキュリティという点からいうと，隠すことによってシステム全体の安全性が守られるということも事実ですから，どの辺までをオープンにして，どこからを隠すか

というその兼ね合いの難しさがあるという感じがいたしております。また，個人レベルとしては，安全はただではない，たとえどんなにコストがかからない手段であっても不正コピーはしないということがルールであると考えられます。それと対策面では当面のものとしては情報提供が，将来的なものとしてはメッセージ認証機能，あるいはプログラムのロム化やフォームウエア化などが対策として考えられますが，いずれにしろこれからの方向を決めてしまうのは時期尚早ですので，当分はこういった問題を抱えながら暗中模索していかなくてはならないのではないかと思います。

それでは次に，会場の方からご質問をいただいていますので，それに対してそれぞれの立場からお考えをお聞きしたいと思います。

最初のご質問の内容は「将来的にみて，パソコンを超えてホストコンピュータにウイルスが入ってくることが考えられるが，ホストのセキュリティ機能は整ってるのか。」ということと，「今後，日本でもハッカーのような存在は増えていくのだろうか。」という2点です。生田さんはこの点についてどのようにお考えでしょうか。

生田　パソコンとホストコンピュータとどこが違うかということの1つのポイントは，セキュリティ機能が整ってるか整ってないかという点だと思います。ただ，その機能がうまく使われていなければ，効果はあげられません。少なくとも現在まで現れているようなウイルスは，入りやすいところ，例えばセキュリティ機能を持ってはいるけどそういうガードをかけていない環境に入ってきています。つまり，セキュリティ機能があれば入らないということではなく，その使い方次第だということです。ただし，これも対外部についてのことで，内部でいたずらをしたらどうなるかということがあります。ウイルスだけでなく，過去新聞ダネになったようなコンピュータに関わる被害は，多くの場合，内部の人間が関与しているのが事実です。こういった点を考えますと。セキュリティ機能を備えた大型コンピュータも決して安全ではないと考えるべきだと思います。

田中　服部さんいかがですか。

服部　今後，ホストコンピュータが単独で動くのではなく，ネットワーク化が進んで端末と連動して処理を行うようになれば，ホストコンピュータ自体は汚染されなくても，ホストコンピュータがウイルスを媒介してしまうような事態も考えられます。そういう意味でホストコンピュータについては，自分自身が侵されるという意味と，それから，自分自身ではなくて媒介してしまうという，そういう2つの面を考えなくてはならないと思います。

田中　どうもありがとうございました。古瀬さんはどういうご意見でしょうか。

古瀬　私個人の意見としては，現在各方面で注目されて，いろいろな形で使われようとしている

UNIXなどは狙われやすいシステムではないかと思いますが，そのかわりきちんとセキュリティ機能もあるので，それを適切に使えばウイルスの侵入はかなり防げるだろうと思います。

ハッカーについては，日本では今までハッカーを生み出す環境がなかっただけではないかと思います。1960年代に，アメリカでは既にマサチューセッツ工科大学でオンライン処理の研究が行われ，良質のハッカーを沢山生んでいますし，パーソナル・コンピュータなども随分ヒッピー文化と結びついていて，ジーンズしかはかないような人がむしろ担い手であったわけです。それに比べ，日本

では1970年代の後半に東京大学の教育計算機センターではパンチカードを使ってみんなで学んでいたというような状態ですから，ハッカーになろうにも育つ環境がなかったと私は理解しています。しかし，わが国でもこれだけコンピュータが普及してきたので，いつハッカーが出てきてもおかしくないだけの環境は整っていると言えるでしょう。また，今後増えていくかどうかは分かりませんが，それくらい詳しい人たちが出てこないと日本のソフトウェア文化も成長しないのではないかという気もします。

田中　どうもありがとうございました。吉村さんはいかがでしょうか。

吉村　どうしても日本では，ハッカー，イコール悪いことをする人というイメージが非常に強いのですが，いい意味で言えばシステムの端から端までなめるようによく知っている存在ですから，そういう人もいないと困るのも事実です。ですから，金銭や機密データを盗むなど犯罪行為を目的としたハッカーは論外ですが，いい意味でのハッカーは育つべきだと思っています。

パスワードを破るというのは簡単なことです。設定してはいけないパスワードというものが何種類かあります。同じ文字列，例えばQWERTYというふうにキーボードを端から順々に打ってくだけのものとか本名などです。実際には大体それで50％は破れます。例えば東大の教育計算機センターなどもかつてはパンチカードぐらいしか使えなかったし，ファシリティが非常に少なく使いたくても使えない時，知識欲が猛烈に旺盛な人間は他人のパスワードを盗んできてでも使おうとするわけです。ですから，そういった人たちの知識欲をなるべく制限しないように，その辺の環境をもう少しよくするべきではないでしょうか。

ホストコンピュータのセキュリティ機能と言う点では，私としては世界中のハッカーが寄ってきたかってセキュリティホールをつぶしているUNIXよりも，今までベールに包まれていたIBMのコンパチブルのOSの方が危険だと思っています。

田中　どうもありがとうございました。ただいま4名の方からご意見をうかがいましたが，ハッカーやウイルスを作る人が出てくるような環境は整ってきているのが現実なので，あとはそれをどのようにすれば発生させずにすむかというところが大きな課題かと思います。

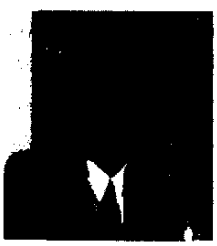
よく新聞報道等では，コンピュータ犯罪の場合に「愉快犯」などという呼び方をしていますが，最近のいくつかのウイルスの発生例を見てみますと，何の目的もなく単にウイルスを作って広く配布し，人が困っているのを見て喜んでいるという事件は意外と少なくて，もっと別の深い目的を持っているように感じます。例えば，イスラエルの独立40周年記念日にシステムのファイルを全部破壊するようにプログラムが仕掛けられていたイスラエルウイルス事件では，従来のテロや爆弾といった手段に代わる知的な武器としてウイルスが使われたと十分考えられます。従来は，拳銃や爆薬などによって破壊活動を行っていたわけですが，今度はコンピュータウイルスのように簡単なソフトを仕掛けるだけで，軍事の一番重要な情報系のシステムを1発で破壊してしまうわけです。こうなるともう愉快犯どころではなくて，はっきりとした目的を持った動きなんですね。そういった意味で，こういうものをつくる人の目的というのは，ますます多種多様化していくことが考えられますし，ハッカーの出現は避けられないということが結論かと思います。

続きましては，コンピュータウイルス対策基準解説書が作られた背景や，基準を活用していく上で役に立つ事柄などについて私の方で質問させて

いただきたいと思います。

アメリカのEDP関係のアンケート調査の結果によりますと，例えばゲームソフトやおもしろいソフトウェアが世の中に出回ると，真っ先にトライするのはEDP関係の人だそうです。ということは，そういったソフトがもしウイルスに汚染されていたとすると，真っ先にシステム側のソフトウェアがやられてしまうという結果になります。その辺のところを今回の基準書では，利用者のための基準，あるいはシステム管理者のための基準の中で，「身元不明なソフトは使わない」としていますが，こういった現状に対し現在どのような対策がとられているのかを，東京大学の計算機センターの運用管理者兼研究者でいらっしゃる吉村さんにおうかがいしたいと思います。

吉村　まず，そういうことをやってはいけないかということになると，やはりそれくらい知識欲



の旺盛な人がいてくれないと困るんですね。ユーザへのサービスということを考えると，ユーザの要求に対処するためには，やはり旺盛な知識欲のある人がマネージメントサイドにいて，ユーザに適切なサービスを提供する必要があると思います。

それで実際に東大ではどうなってるかというと，いわゆる業務LANと研究開発LANは分離しています。ですから，研究開発LANで起こったことが業務LANの上に拡散することはありません。ですが，それが完全かというと，実はまだ完全ではありません。もう一段階LANを分離すると完全になると思っているんですが，コスト面で非常に問題があります。ただ，やはりいろいろなソフトを知らない人がユーザサービスをすることはできませんので，なるべく早く分離していろいろなことができる環境を作るように現在最大限の努力をしているところです。

田中　コストが許せば，論理的あるいは物理的にそのシステムを分けることが望ましいということですね。現実に，マッキントッシュでは業務用と研究用のシステムを混在させていたために，フリーハンドというウイルス入りのグラフィックソフトを出荷してしまいユーザにひどい迷惑をかけたという事件がありました。この場合実害はなかったといわれていますが，「信頼できるメーカからのソフトウエアを使いなさい」といっていたそのメーカからウイルス入りのソフトを買わされてしまったのですから，メーカの信用というのは，一挙に落ちてしまうわけです。その点からも，ソフトウェアの開発者というのは，一般の開発者に比べて数段上のモラルとその開発管理体制の確立を要求されているといえます。

服部さんのところでは，社会的に影響のある大規模なネットワークシステムを開発なさっています。その開発にあたっては，いろいろな意味で信頼度の向上という対策がとられているかと思いますが，実際にはどのような点に注意してソフトウェアの信頼度の向上に努めていらっしゃるのかをご説明願えますか。

服部　私の今の仕事はソフトとはちょっと離れているので，実際の業務の中でどうこうという話

ではなく，まあこんなことをやった方がいいのではないかというレベルになってしまいますが，特にウイルスに関してまずやらなければならないのは，いかにしてウイルスの入っていないものを作るかということです。ウイルスが入り込む可能性がある段階としては，まず開発の段階，次に実際に開発したものを製品化し

て出荷する段階，それから最後に製品をお客様のところに届ける時が考えられます。開発時点で混入させないということについては，その開発環境を汚染させないということが絶対条件ですが，ただ，ここで区別しなくてはならないのは，開発環境が汚染されることと，製品が汚染されることは別であるということです。たまたまターゲットマシンと開発マシンが同じであると，同じように混入してしまう場合はありますが，基本的にはそれぞれについて対策を立てなくてはならないと思います。

製品化の段階について言えば，受託ソフトなどの場合には自分自身で開発から製品化まで全部できるわけですが，市販用のソフトになりますと，どうしてもコピー業者に出さざるを得ないので，この過程で混入することも十分考えられます。コピー業者では，開発側が渡したFDから直接コピーするのではなく，それをもとにしてコピーをするためのマスターファイルを複数作り，そのうちの1つを依頼側に返してきます。これについてチェックをして，よければそのまま製作に入るわけです。そういう過程の中のちょっとした手違いですぐにウイルスは入り込んでしまうので，コピー業者との間でうまく連携をとり，実際にコピーされる原本が汚染されてないという保証をどの様に取るかを明確にしたり，そのルートを確実にチェックしていく必要があるだろうと思います。

あとはお客さんに渡ったときに汚染されるということが考えられます。この点については，インストールのやり方に対して，ライトプロテクトできるような製品を出すとか，コピープロテクトをしないといった方法を提供側は考えていかなければならないと思います。

田中　どうもありがとうございます。今ベンダーサイドからウイルス入りのソフトを出荷するなどということはあってはならないことだと申しましたが，実は2－3日前に大阪の方で，実際にこういったことが起きてしまったようなんですね。佐藤さんにその辺のところを教えていただきたいと思います。

佐藤　一昨日ですが，新聞で報道されたので，朝一番でそのゲームメーカーから話を聞いたんですが，その話によると，数日前に小売店，ユーザから，ソフトに何かウイルスが入ってるという連絡を受け調査したところ，7月まで潜伏して7月以降に使用した場合にはフロッピィが破壊されるという内容のウイルスが，昨年1月に入れられていたそうです。原因についてはまだ調査中だそうですが，非常に協力的な会社で基準に基づいて届け出を出していただけるということでしたので，多分届け出の第1号の企業になると思っております。

田中　ありがとうございました。次に生田さんにお聞きしたいのですが，やはり生田さんのところのPC-VANネットワークでウイルスが出たそうですが，実際こういう変なソフトというのがシステムに紛れ込みますと，私たちメーカとしては自分たちのソフトにバグがあるんじゃないかということでそちらの調査ばかり行い，ユーザを疑うということはまずしないわけです。そういう意味で原因追求には時間もかかり，非常にご苦労なさったと思いますが，その辺のところはいかがでしょうか。

生田　やはり異常が発見されてまず考えることは，自分たちの中に欠陥があるのではないか，伝送路上に何か変なものがあるのではないかということです。ですからそういった側面から分析はしていたのですが，かといってシステム全体に大きな影響を与えるものではありませんので，あまり危機感を持っていなかったというのが実態です。

また，パソコン通信では送られた情報を保証するということが1つの目的なので，こちらからは消したくても消せないわけです。ところが私どものところにも欠陥はなさそうだったので，この情報を送っているらしい方々をIDパスワードで調べて連絡をとっていくうちにウイルスではないかと疑うようになったわけです。ただ，この場合はIDパスワードが盗まれていたので，犯人と思われた人も実際は被害者であり，真犯人を特定することはできませんでした。ですから，論理的な囲い込みだけでなく，指紋や声紋といった物理的な囲い込みをも行わなければ犯人を特定することは難しいと思います。つまり，残念ながら技術的な観点からだけでは限界があるので，もっと総合的な観点からウイルスだけでなくセキュリティを考えていく必要があります。啓蒙といった点では解説書も1つの手段ですし，あるいは社会規範みたいな問題や，保険というような問題もあると思います。そういったものを全てひっくるめた総合的なセキュリティ対策が求められているのではないでしょうか。

田中　どうも有難うございました。最後に古瀬さんにお聞きしたいんですが，こういったウイルスなどの問題について広く事実を伝えるというのは重要ですが，正しく伝えないと，逆に問題が大きくなるといった側面もあると思います。そういった意味で正しく伝えるため，ジャーナリストである古瀬さんはどういうところに注意されているのかお聞かせ願えますか。

古瀬　コンピュータウイルスに関しては，非常に神経を使います。あんまり危ないと騒いでもパニックに陥るし，一般の読者にわかるような形で説明しようとするのは大変難しいことです。最近，僕らジャーナリズムの現場で一番困っているのは，「どうも何とかの何々というソフトにウイルスが入っているようだから調べてほしい。」という情報が寄せられることです。こちらとしてはウイルスがあると書いてみたいけれども，社会的に影響が大き過ぎるのできちんと調べなければ書けません。ただ，たとえ本当にウイルスがあったということがわかっても，それをすぐに報道することには疑問が残るので，どこか第三者的な消費者相談窓口のような機関がきちんと対処していく必要があると思います。そこのところを今のうちにきちんと特定しておかないと，ジャーナリズムも詳しい人たちばかりではありませんので，混乱した報道が多発する可能性はあると思っています。

田中　それでは次に，個別の質問に回答をいただきたいと思います。

まず，今回の解説書ではウイルスを「第三者のシステムを破壊する目的」と定義づけていますが，自分の会社内，あるいは通信相手，取引先を破壊した場合この第三者に該当するのかどうかという言葉の定義の問題です。もう1点は，今回のウイルス対策基準解説書がシステム監査と併せて使いなさいという言い方になっていないのはなぜですかというご質問です。

佐藤　第三者の定義という問題ですが，自分が作っているシステム以外のシステムに何かを入れた場合，それは全てウイルスであると解釈していただきたいと思います。ですから，例えそれが通信回線を通して入った場合も当然ウイルスであるということです。

それから，システム監査とウイルス対策基準を併用した方がよいのではないかというご質問ですが，これについては，時期は明確にはいえませんが，なるべく早い段階でシステム監査基準自体を見直していきたいと考えていますので，その中でコンピュータウイルスについても検討を加えていきたいと思います。

田中　次は，コンピュータウイルスがどのような仕組みになっているかという構造についての質問と，基準書の中で届け出制というのが謳われてるわけですが，では届け出たときの企業側への見返りはあるのかという，2点の質問でございます。

岡本　ワームというものは，自分のところからパスワードを破ったり，センドメールのデバッグ機能を使ってほかのマシンを起動させることができるのですが，ウイルスというのは中に入り込むだけで，後で親のプログラムを実行したときにそのウイルスも一緒に動き出すということです。入り込んだところが悪いと，変な動作を起こして壊れることもありますが，大体は最初のあたりを書きかえて，ジャンプ命令でどこかへ跳んでいくという形をするみたいです。広まるウイルスというのはシステムを壊したりしないでうまくほかに伝染していき，動作がうまくいかないのは自然的に淘汰されるという傾向があると思います。

佐藤　届け出に対する見返りということですが，コンピュータウイルスというのは，自分だけの問題ではなくて全体で考えるべき問題だと思います。例えば，届け出をすることによって多くの情報が集まれば，結果としてほかの人の情報やワクチンの情報などいろいろな情報がはいってくるわけで，それを見返りだというふうに解釈してもらいたいと思います。

田中　どうもありがとうございました。それでは次の質問を古瀬さんにお願いします。

古瀬　「ファイルのサイズその他の変化を調べるユーティリティとか，ファイルの内容を比較するワクチン機能は，今現在どの程度実用性がありますか」ということですが，実用性はかなりあると思いますが，当然これをくぐり抜ける方法が考えられるでしょうから，万能薬はないというふうに認識しておいた方がいいでしょう。

田中　どうもありがとうございました。万能薬がないということは理論的にも実証されていますが，もう1つの方法として，現在のアーキテクチャを変えることも考えられます。データとプログラムが明確に区分けされているパラレルコンピュータ，パラレルプロセッシングであれば，現在いわれているようなコンピュータウイルスをある程度防御できるのではないかということがよくいわれているかと思います。

それでは時間もなくなってまいりましたので，次を最後の質問とさせていただきます。今後いろんな部分がファームウェア化されてくるが，そのファームウェアも検査対象にするのかということです。服部さんの方からお願いいたします。

服部　ウイルスに汚染される時，ファームウェアとしてウイルスを入れられる場合が一番怖いのではないかと思います。ロムなどに焼きつけてきっちりした状態で出荷されてしまうと，単にソフトウェアを入れ替えるだけでは修復できないし，ひどい場合には，一般のユーザがそれをどうこうするというわけにいかない状況になってしまうのではないかと思います。ですから，システムソフトウェアという意味ではファームウェアも当然検査対象に入ります。

田中　どうもありがとうございました。これで「コンピュータウイルス対策基準講演会」パネルディスカッションを終了したいと思います。

海外情報産業の動向

〈情報産業界の動向〉

アメリカのハードウェアとソフトウェアを合計した総売上高は，年率10％前後で成長しており，これは全産業の成長率の約３倍，GNP５兆2,400億ドルの２％である。全産業レベルで比較すると好調のようであるが，主要コンピュータ・メーカの業績は最近あまり良くない。例えば，世界最大のコンピュータ・メーカであるIBMの1989年の純利益は前年比35.3％減と大幅に落ち込み，DECも同年の純利益は前年比17.8％減となった。

この不振の原因は，アメリカの景気の停滞，産業界の設備投資の鈍化，およびメーカ間の値下げ競争の激化である。技術革新により，高性能なコンピュータを市場へ安く提供するようになったため，メーカは収益の悪化を招きやすくなっている。

これらの業績の伸び悩みを解消するために各コンピュータ・メーカでは，人員の削減，工場の統廃合，再編成等の合理化を実行している。例えば，IBMでは1990年末までにアメリカ国内で１万人以上を削減する計画である。

〈政策・制度〉

EC著作権法案の行方が注目される。この法案はリバースエンジニアリングをも強力に制限するもので，データ入出力部のソフトウェアインタフェースの互換製品の開発に特に影響を与えると考えられている。IBMやDECなど，すでに支配的な立場にあるベンダはこの法案を支持しているが，その他のベンダ約50社はソフトウェアインタフェースを著作権保護対象から外すことおよびインタフェース情報に関するリバースエンジニアリングが認められることの明文化を求め，ロビー活動を展開している。

〈環境整備〉

現在，アメリカでは，政府が主体となってコンピュータとLANのセキュリティ対策の開発がさかんに行われている。例えば，SRIが海軍のために開発しているシステムは，“Intrusion Detection Expert System(IDES)”と呼ばれている。ユーザのワークステーション・ネットワーク上の行動を通常業務の“Profile”とリアルタイムに比較し，その相違の重要性を分析するために人工知能(AI)を利用するもので，まだ実験段階にもかかわらず，Rockwell International社やFBIなどが導入を予定している。

また，Citicorpでは，AIを利用して顧客へのインボイスを処理する行員を監視するシステムを独自に開発している。同システムは，週および月のどの時期に，どの顧客宛のインボイスを入力すべきかという“Profile”と行員の日常業務を比較するもので，業務内容を監視していることは，行員にもあらかじめ知らされている。システムの開発者たちは，AI技術の併用によって，“Profile”のデータの有効期限や業務項目，休暇のスケジュールなど変動性の高い要素にも対応できるシステムの構築をめざしている。

〈エンドユーザ環境〉

イギリスのSouthern Pacific Transportation社は新開発の手書き文字認識可能な携帯型パソコンを導入した。500人にわたる鉄道労働者はキーボードよりも操作のわかり易いこのペン入力パソコンを使って作業しているが，記憶された情報をモデムを経由してホスト上に直接送ることにより，伝票処理上のエラーを大幅に減らすことができた。Best Foods Baking Groupでは配送用トラックに

置いており，伝票エラーの防止や食品の流通の迅速化により，年間150万ドルのコスト削減になると期待している。

ペン入力可能なノート型パソコンの市場は広がりつつある。セースルマンは契約と同時にデータを入力でき，警官は交通違反のキップをその場で切ることができる。短いメモを作る感覚で入力できるあらゆる仕事に応用が期待される。またホワイトカラー層においてもハンディなコンピュータは需要があると考えられるし，さらに電子ペン技術の進歩はいつの日かキーボードにとって代わる可能性も大きい。この種のコンピュータは，キーボード入力の伝統的ハンドヘルド型の市場の25%を奪うと予測され，規模としては2000年までに30億ドルの市場が見込まれている。

〈ソフトウェア〉

エキスパートシステムは，予期しなかったような所で利用され始めており，その一つとして小売業での利用がある。小売業は現場における知識とセンスが売上に大きく影響するため，こうした知識をエキスパートシステムに入れることにより，未経験のマネジャーでもトップレベルのマネジャーと同じような決定や計画を立てることができるようになる。

700のクッキー売場と100のデリカテッセンを持つMrs. Fields社は，クッキーの無料販売等を通してマーケットを調べ，それを販売に役立ててきたが，店舗が数100になるともはやこの手は使えなくなり，エキスパートシステムの利用を思い立った。同社のエキスパートシステムは店員スケジューラ，採用インタビューイング，デイリー生産プランナー等から成っている。

店員スケジューラは雇用関係の法律，店の特殊事情，労働意欲等を基に最適な，店員の労働時間割りを作る。採用インタビューイングは，採用の面接時により良い候補者を選ぶのに役立ち，デイリー生産プランナーは生産調整計画を立てるのに役立っている。

ファッション小売業のBroadway社もエキスパートシステムを用いて売上を伸ばしている。

〈ネットワーキング〉

自営網において，現在の回線をそのまま使用してトラヒック量を増加させることのできる技術が，ヨーロッパでも実現できそうである。高速パケット交換方式と呼ばれるこの技術は，既に数年前から，アメリカの大規模な自営網で利用されている。

高速パケット交換方式は，リースした回線上で通常の約2倍のトラヒック量を実現できるが，ヨーロッパではPTTの強固な反対により利用できなかった。反対の理由は，表向きは公衆網の音声伝送の品質を保証するためというものである。

しかしECが，イギリスの電気通信庁(OFTEL)によって提案された実用ネットワークコード(Network Code of Practice: NCOP)を認可することになれば，この状況は一変する。NCOPは，イギリスの自営網と公衆網の接続の規制を緩和するものであり，同様の緩和をヨーロッパ全域まで拡げるよう提案している。

これに対してECでは，PTTにとって競争が不利にならないような一定のルールをNCOPに付加するよう提案している。

〈電気通信政策〉

ヨーロッパの18の公衆通信事業体は，その主要法人顧客に対し，ワン・ストップ・ショッピング

を提供する協定に合意した。この協定は，主要法人顧客がヨーロッパ内で国境を超えた専用線網を設定する際，注文から料金請求，要求，メンテナンスサービス等一切を，単一事業体を通じてできるようにするものである。

これらの18の事業体は，ワン・ストップ・ショッピングにより，今までのヨーロッパ経済共同体(EEC)の境界線をさらに超えたより大きなヨーロッパ単一市場を作るとしている。この協定は，今ユーザをイライラさせる原因となっている各国それぞれの通信事業体との別々の交渉や隣国同士の回線接続の保証など官僚的な問題を取り除くことができるとされる。

しかし，この協定は企業ネットワーク・ユーザにとってのもう一つの悩みのタネである専用線料金については触れていない。

'90米国情報産業視察団報告

当協会では，1970年以来団員公募による海外情報産業視察団を数多く派遣してきており，本年度は，'90米国情報産業視察団を6月4日～17日までの14日間派遣した。参加者は総勢19名で，コーデネータは当協会山鳥調査部長が務めた。訪問先は，COMDEX/Spring'90，EDS(Electronic Data Systems)，Sterling Software，TI(Texas Instruments)，Nynex，Quantum Group International，INPUT，Apple Conputerの8ケ所である。以下に訪問先の概要を述べる。

(1)COMDEX/Spring'90

COMDEX/Spring'90は，情報機器ディーラを主に対象とした世界的な展示会であるが，ここ数年はディーラのみならずユーザを含む幅広い参加者を得ている。同展示会は，6月3日～6日の4日間ジョージア州アトランタ市の中心にあるジョージア・ワールド・コングレス・センターで開催され，「PC Solutions for the90s」というメイン・テーマでディスクトップ型PCをはじめ，ラップトップまで広範な展示が行われた。

(2)EDS

同社は，1962年に設立された情報サービス企業であり，1984年にはGMの子会社になり，GMの情報処理のかなりの部分を担当することになった。現在の同社の主要な業務としてはシステム・インテグレーションがあげられる。顧客のニーズを分析して，最適のファシリティ・マネジメントを構築している。

(3)Sterling Software

同社は，1981年に設立された情報サービス企業であり，社員数は約2,000名である。同社の事業は，大きく分けてアプリケーション・ソフトウェア，システム・ソフトウェア，政府関係ソフトウェアから構成されており，売上高はそれぞれ3,500万ドル，6,300万ドル，8,300万ドルである。最近では，特にEDI(Electronic Data Interchange)に力を入れており，1990年におけるこの部門の売上高は2,500万ドルに達すると予測している。

(4)TI

同社は，約50年前に石油探索会社として創業されたが，1958年にICを開発して以来，半導体分野で世界的な企業となった。今回の訪問では，同社が開発・販売しているCASE(Conputer Aided Software Engineering)プロダクツIEF(Information Engineering Facility)についての説明を受けた。IEFは，分析から設計，実行までの過程を一貫してサポートする統合化CASEプロダクツである。

(5)Nynex

Nynexは，1983年に設立された地方電話会社で，従業員数は約95,000人，サービス地域はニューヨーク州とニューイングランド諸州である。同社は電話事業以外にも積極的に進出しており，高度なアプリケーション・システムの開発も行っている。例えば，病院，医師，医療記録バンク等を統合的にネットワーク化した健康管理保険事業を行っている。

(6)Quantum Group International

同社は，情報産業分野における調査コンサルタント専門企業で，特にコンピュータや通信分野で高い評価を得ている。1990年代と2000年における情報産業におけるキーワードとしては，①グローバリゼーション　②ニーズの多様化　③自由化と規制緩和　④新しいインフラ(光ファイバ，衛星通信)等があげられる。また，画像を中心としたイメージ記憶に対するニーズが高くなり，記憶媒体としては，光ディスクが有力であると予測している。

(7)INPUT

同社は，情報サービス産業や最近話題のEDIを含めたコンピュータ利用動向等を専門とする調査コンサルタント企業である。情報サービス産業の1990年代のキートレンドとしては，①プロダクトとサービスの融合　②市場構造の変化　③国際化　④標準化　⑤ベンダの統合化等があげられる。アメリカにおけるシステム・インテグレーション市場は，今後年率20%以上で成長し1994年には172億ドルに達し，またEDI市場は年率30%以上で成長し1994年には14億ドルに達すると予測している。

(8)Apple Computer

同社は，1976年に設立され，1989年には売上高50億ドルを越える企業となっており，ユーザと市場のニーズに適合した製品を提供している。最近，日本市場に対する売込みが，非常に積極的で，この地域の担当役員によると日本語処理だけでなく，日本の文化をも考慮したシステムを開発し提供していきたいと述べている。

会員サロン

パラダイムシフトへの対応

三菱自動車工業㈱経営企画室情報システム部

計画グループ長　渡辺　豊

自動車業界は，一般的に自動化，コンピュータ化が進んでいる産業と言われている。生産分野では，組立てラインのコンピュータ制御(ALC[*1])，部品生産用の型製作の数値制御化(NC化，CAM[*2])等により製造業務の合理化・製造コスト低減を図っている。また開発分野では，設計業務における製図作業のコンピュータ化(CAD[*3])，振動解析・衝突解析等技術計算の高度な活用(CAE[*4])により設計・開発業務の合理化及び精度の向上を図っている。これらのコンピュータ化は他産業に先駆けて各自動車メーカが独自に取組んできたもので，車を生産する為の個々の固有技術として益々高度化しつつある。一方，販売分野でも車を効率良くお客様に届けるための物流管理システム，販売会社で必要となる補用部品を供給するデポ管理システム等があり，煩雑な物流業務をがっちりとサポートしている。

これらの固有技術を実現する為，或は固有技術同士の連携をとる為には，最適なコンピュータ資源を必要な時に必要な量だけ投入する必要があり，当社でも各部門で必要となるコンピュータ機器を検討し導入しているが，更に全社レベルでの整合性をとる為，各部門で検討した計画を当部で調査・調整をしている。

ところで，コンピュータ技術動向に目を向けてみると最近の情報システムは機器の処理速度の向上，軽量化及び低価格化，AI等ソフトの高機能化により従来とは全く異なる利用形態が実現可能となってきている。これは，一つのパラダイムショックと言えるのではなかろうか。パラダイムとは，『その時代における大半の人間が正しいと考えて

いる規範』であり，その規模が情報システムにより大きく変貌しようとしている。例えば，従来実車でしか検証できなかった衝突試験でのコンポーネント部位の変形をスーパーコンピュータ上で再現できるようになった。コンピュータで処理する為，変形した箇所をあらゆる角度から，また顕微鏡のように拡大したり縮小して見ることが可能となり，更に繰り返し見ることも可能となる。これにより過渡的な現象の検討も可能となり，今まで捉えることの出来なかった観点からより詳細な検討が可能となった。我々は，情報システムを活用することにより，今まで考えもしなかったことを容易に実現できるようになったのである。

こうして見ると，情報システムは今真に新しいパラダイムを創造する母体であり，今後も各分野で新しいパラダイムが次々と創造されてくるだろうと思われる。

最近，戦略情報システム(SIS)とか統合生産システム(CIM)が世の風潮となり，どこの企業も重点推進事項として積極的に推進している。これも一つの新しいパラダイムの創造ーパラダイムシフトと考えてよいと思う。

戦略情報システムの定義を専門家に聞くと，『同業他者に対し，競合優位に立てるよう情報システムを戦略的に活用すること』という説明が返ってくる。しかし，どのような戦略情報システムを構築すべきかについては，『業種業態により差別化の要素は異なり，決まったものは無い。』という説明ばかりで，具体的なものは何も提示されない(戦略情報システムは一定の形を持たない)。他社の真似ばかりしていては，競争優位には立てなく，他社が考えそうもない奇想天外なアイデアで業務システムを構築することにより競争優位に立てるといったところだろうか。しかし，競合企業間では概ね最終ゴールが同じである場合が多い為，アプローチは最終的には一つに収斂すると思われる。つまり，各企業が取組んだアイデアの内，幾つかは生き残るがその他は淘汰され，多くの企業は，生き残った最良のアプローチを採用し，先行する企業に追随することになる。ここで新しい規範ーパラダイムが成立する。つまり，競合他社に対して競争優位に立つ為には，業務の本質をついた生き残れるアプローチを如何に早く見極め，他社に先行してシステム構築するかが肝要となる。

コンピュータ技術を含めた技術革新により人々の生活は益々豊かになり，生活スタイルも大きく変わりつつあるように思われるが，それのみならず経済構造，社会構造さえも大きく変貌するだろう事を多くの人が指摘している。堺屋太一著の「知価革命」もそのような変貌を指摘する本の一つであるが，堺屋氏によるとコンピュータ技術の発展が石油ショック以降の資源有限感に対する省資源化と商品の多様化・情報化に大きな役割を果たしたが，これにより人々の商品に対する価値観も大きく変わってきている。つまり，人々は，もはや商品の製造コストには価値を見出さず，商品

を作り出すアイデアに対価を支払うようになっている。この価値観の変貌により，商品の多様化が進むと同時にそのアイデアを提供する個人への依存が高まり，結果として個人への情報の集中が益々高まっていく。さらに，これら多様化する商品を製造する企業自身も製造を目的とした機能的組織からアイデアを創出する属人的組織に変化していくというのである。

つまり，情報システムという技術革新は，人間の価値観を変貌させ，組織のあり方までも変えてしまう可能性を持っているのではなかろうか。

とにかく，今や情報システムはこれからの企業戦略を立案する上で中核を担っており，新しいパラダイムを創造する上で無くてはならないものとなってきた。そこには奇想天外な発想があり，既存の概念にとらわれている人間には到底判断できないものとなってきている。では，新しいパラダイムを全社的な見地から評価する為にはどうすれば良いのか。

一つの見方であるが，情報システムが如何に高度化しようとそれ自身のみでは企業に貢献できない。なんらかの業務と結び付いて初めて貢献できる。つまり，業務のニーズを情報システムという手段により高度に実現し企業の利益に貢献していると考えることができる。従って，新しいパラダイムを評価する為には，先ず業務が持つ真の目的を捉えることであり，次に個々の業務の目的を全社的見地で集約し，あるべき企業の姿をイメージしてみる。つまり，その企業独自の戦略情報システム計画を立案してみるのである。その中で個々の業務のアプローチを評価し，方向がおかしければ調整する。このようにして，全社的に見て整合性のとれた計画としてオーソライズが可能となる。

今後，全社的見地から戦略情報システムを構築するニーズが高まれば高まる程，全社的立場で評価することの重要性が高まってくると思う。先行している部分は良いが，遅れている部分は推進を促す等積極的に提言していく必要がある。誠に担当者としては，頭の痛い話である。何か指針となるものが出てくることを切望してやまない。

＊1：ALC(Assembly Line Control)：組立てライン上で，コンピュータから自動機(ロボット)の制御，作業者へ部品組み付け指示や部品手配をする。

＊2：CAM(Computer Aided Manufacturing)：生産で必要となる型，治具や生産設備の設計，製作をコンピュータの数値制御(NC)により実施する。

＊3：CAD(Computer Aided Design)：製図，デザイン等の描画作業をコンピュータの画面上で実施する。

＊4：CAE(Computer Aided Engineering)：実験等で検証していた衝突試験等の解析作業をコンピュータ・シミュレーション等により，コンピュータ上で実施する。

平成二年度春期情報処理技術者試験

実施試験区分　第一種情報処理技術者試験
　　第二種情報処理技術者試験

試験期日　平成２年４月15日(日)

合格発表　第二種　平成２年５月30日(水)
　　第一種　平成２年６月29日(金)

応募者数/受験者数/合格者数

第二種　153,130人/89,489人/13,733人
(受験率58.4％)(合格率15.3％)

第一種　87,565人/50,359人/ 9,153人
(受験率57.5％)(合格率18.2％)

年齢別状況(平均年齢)

第二種　応募者　23.4歳　合格者　23.2歳

第一種　応募者　26.9歳　合格者　26.5歳

最年少・最年長合格者

第二種　最年少合格者　14歳　櫻井一俊さん
　　最年長合格者　59歳　北村直明さん

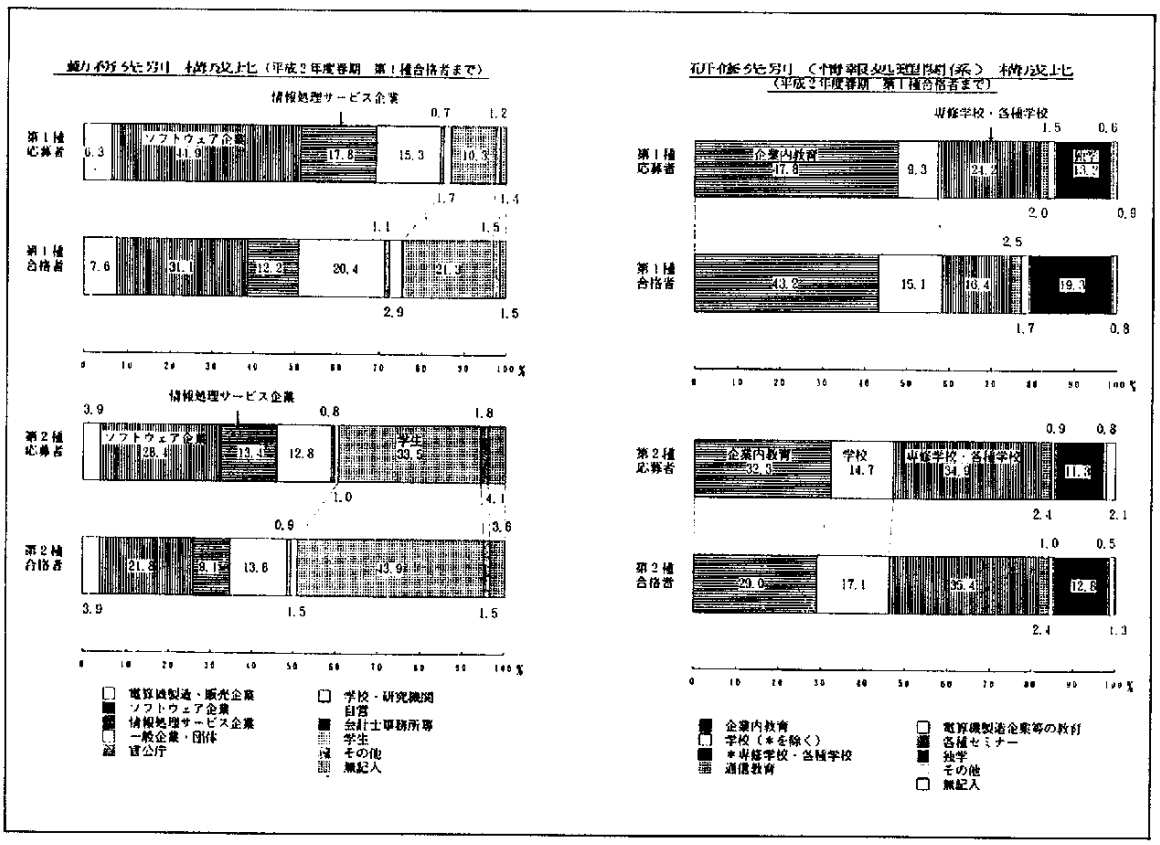
第一種　最年少合格者　16歳　高橋　誠さん
　　最年長合格者　65歳　大野　元さん

試験地別状況(表)

受験率上位３位　第二種　帯広　新潟　青森
　　第一種　帯広　新潟　大分

合格率上位３位　第二種　新潟　高知　静岡
　　第一種　京都　新潟　鹿児島

勤務先別状況(図)：第二種は，前々回から徐々に学生の合格比率が上昇している。



平成２年度　春期情報処理技術者試験　試験地別一覧表

試験地別	Ⅰ種			2種（春期）			春期合計		
	応募者数	受験者数	合格者数	応募者数	受験者数	合格者数	応募者数	受験者数	合格者数
札幌	1,719 (23.3)	1,023 (59.5)	218 (21.3)	3,870 (11.1)	2,467 (63.7)	443 (18.0)	5,619 (14.6)	3,490 (62.1)	661 (18.9)
青森	93 (89.8)	69 (74.2)	9 (13.0)	366 (21.9)	290 (81.5)	35 (12.1)	449 (34.7)	359 (80.0)	44 (12.3)
岩手	102 ( )	100 (61.7)	17 (17.0)	627 ( )	462 (73.7)	62 (13.4)	789 ( )	562 (71.2)	79 (14.1)
盛岡	292 (24.7)	189 (64.7)	45 (23.8)	686 (25.8)	468 (70.3)	86 (17.1)	958 (25.4)	657 (68.6)	125 (19.0)
仙台	1,773 (20.0)	1,052 (59.3)	140 (13.3)	4,115 (10.6)	2,648 (64.3)	254 (9.6)	5,888 (13.3)	3,700 (62.8)	394 (10.6)
秋田	206 (28.0)	120 (58.3)	18 (15.0)	526 (37.3)	374 (71.1)	44 (11.8)	732 (34.6)	494 (67.5)	62 (12.6)
水戸	1,462 (8.6)	820 (56.1)	108 (13.2)	3,112 (7.6)	1,624 (52.2)	221 (13.6)	4,574 (8.0)	2,444 (53.4)	329 (13.5)
宇都宮	585 (8.7)	329 (56.2)	72 (21.9)	1,900 (20.2)	1,385 (72.9)	196 (14.2)	2,485 (17.8)	1,714 (69.0)	268 (15.6)
前橋	819 (33.4)	519 (63.4)	74 (14.3)	2,122 (31.2)	1,477 (69.6)	207 (14.0)	2,941 (31.8)	1,996 (67.9)	281 (14.1)
埼玉	2,523 (18.6)	1,428 (56.6)	281 (19.7)	4,844 (14.0)	2,698 (55.7)	392 (14.5)	7,367 (50.0)	4,126 (56.0)	673 (16.3)
千葉	2,885 (28.0)	1,603 (55.6)	384 (19.0)	4,030 (15.1)	2,089 (51.8)	291 (13.9)	6,915 (1.3)	3,692 (53.4)	585 (16.1)
東京	28,075 (7.1)	14,970 (53.3)	2,795 (18.7)	46,810 (25.5)	23,150 (49.5)	3,617 (15.7)	74,885 (17.9)	38,120 (50.9)	6,432 (16.9)
横浜	2,228 (16.9)	1,161 (52.1)	233 (20.1)	3,240 (8.2)	1,611 (49.7)	245 (15.2)	5,468 (9.6)	2,772 (50.7)	478 (17.2)
神奈川	8,642 (10.7)	4,581 (53.0)	858 (18.7)	9,329 (40.9)	4,810 (51.6)	754 (15.7)	17,971 (23.8)	9,391 (52.3)	1,612 (17.2)
小計	44,353 (10.0)	23,743 (53.5)	4,471 (18.8)	68,253 (6.4)	34,358 (50.3)	5,319 (15.5)	112,606 (7.8)	58,101 (51.6)	9,790 (16.8)
新潟	1,268 (12.6)	912 (71.9)	224 (24.6)	8,826 (13.6)	1,428 (78.2)	413 (28.9)	3,094 (13.2)	2,340 (75.6)	637 (27.2)
長野	664 (16.1)	382 (57.5)	83 (21.7)	1,287 (13.0)	758 (58.9)	91 (12.0)	1,951 (14.0)	1,140 (58.4)	174 (15.3)
静岡	1,496 (10.7)	978 (65.4)	146 (14.9)	3,082 (27.5)	2,147 (69.7)	414 (19.3)	4,578 (21.5)	3,125 (68.3)	560 (17.9)
名古屋	6,050 (15.7)	3,866 (63.8)	662 (17.2)	11,359 (15.4)	7,622 (67.1)	1,196 (15.7)	17,409 (15.5)	11,482 (66.0)	1,858 (16.2)
岐阜	597 (25.2)	358 (60.1)	71 (19.8)	1,143 (26.3)	665 (58.2)	104 (15.6)	1,740 (25.9)	1,024 (58.8)	175 (17.1)
愛知	803 (21.5)	469 (58.4)	62 (13.2)	1,502 (13.2)	925 (61.6)	106 (17.9)	2,305 (15.9)	1,394 (60.5)	228 (16.4)
福井	409 (23.6)	272 (66.5)	39 (14.3)	765 (13.2)	520 (68.0)	83 (16.0)	1,174 (16.6)	792 (67.5)	122 (15.4)
三重	1,628 (6.5)	1,032 (63.4)	255 (24.7)	3,217 (10.9)	2,001 (62.2)	345 (17.2)	4,845 (9.4)	3,033 (62.6)	600 (19.8)
大阪	11,770 (16.9)	7,081 (60.2)	1,253 (17.7)	18,046 (8.2)	10,943 (60.6)	1,548 (14.1)	29,816 (11.5)	18,024 (60.5)	2,801 (15.5)
滋賀	1,596 (1.0)	1,060 (66.3)	161 (15.2)	3,820 (39.4)	2,382 (62.4)	341 (14.3)	5,416 (25.4)	3,302 (62.6)	502 (14.8)
京都	14,994 (13.8)	9,123 (60.8)	1,669 (18.3)	25,083 (12.4)	15,326 (61.1)	2,234 (14.6)	40,077 (12.9)	24,449 (61.0)	3,903 (16.0)
兵庫	257 ( )	174 (67.7)	33 (19.0)	709 ( )	522 (73.6)	78 (14.9)	966 ( )	696 (72.0)	111 (15.9)
岡山	1,075 (5.2)	673 (62.6)	118 (17.5)	2,191 (2.4)	1,487 (67.9)	212 (14.3)	3,266 (3.3)	2,160 (66.1)	330 (15.3)
広島	1,876 (25.8)	1,210 (64.5)	213 (17.6)	3,465 (3.6)	2,332 (67.3)	397 (17.0)	5,335 (10.4)	3,542 (66.4)	610 (17.2)
山口	239 (28.5)	158 (66.1)	29 (18.2)	889 (44.3)	643 (72.3)	78 (12.1)	1,128 (40.6)	802 (71.1)	107 (13.3)
香松	532 (5.5)	320 (60.2)	70 (21.9)	1,250 (2.0)	782 (62.6)	107 (13.7)	1,782 (3.0)	1,102 (61.8)	177 (16.1)
徳島	484 (22.8)	290 (59.9)	46 (15.9)	996 (28.7)	714 (71.7)	111 (15.5)	1,480 (26.7)	1,004 (67.8)	157 (15.6)
高知	167 ( )	89 (53.3)	21 (23.6)	424 ( )	282 (66.5)	76 (27.0)	591 ( )	371 (62.8)	97 (26.1)
福岡	2,966 (26.1)	1,711 (57.7)	274 (16.0)	5,829 (28.2)	3,703 (63.5)	576 (15.6)	8,795 (27.5)	5,414 (61.6)	850 (15.7)
佐賀	176 (12.8)	113 (64.2)	17 (15.0)	436 (9.9)	311 (71.3)	50 (16.1)	612 (4.4)	424 (69.3)	67 (15.8)
長崎	259 (44.7)	165 (63.7)	19 (11.5)	726 (16.7)	489 (67.4)	61 (12.5)	985 (23.0)	654 (66.4)	80 (12.2)
熊本	583 (27.0)	355 (60.9)	53 (14.9)	1,240 (2.5)	829 (66.9)	117 (14.1)	1,823 (9.2)	1,184 (64.9)	170 (14.4)
大分	509 (25.4)	362 (71.1)	59 (16.3)	979 (32.7)	701 (71.6)	96 (13.7)	1,488 (30.1)	1,063 (71.4)	155 (14.6)
宮崎	197 (38.7)	133 (67.5)	18 (13.5)	814 (8.8)	654 (80.3)	63 (9.6)	1,011 (13.6)	787 (77.8)	81 (10.3)
鹿児島	235 (24.3)	147 (62.6)	36 (24.5)	856 (12.5)	626 (73.1)	79 (12.6)	1,091 (14.8)	773 (70.9)	115 (14.9)
那覇	241 (19.9)	139 (57.7)	19 (13.7)	732 (29.1)	478 (64.2)	70 (14.9)	973 (26.7)	609 (62.6)	89 (14.6)
全国	87,565 (13.8)	50,359 (57.5)	9,153 (18.2)	153,130 (11.7)	89,489 (58.4)	13,733 (15.3)	240,695 (12.5)	139,848 (58.1)	22,886 (16.4)

(注)　応募者数欄の下段（ ）内数字は対前年度比増加率(%)，受験者数欄の下段（ ）内数字は受験率（受験者数／応募者数：%）
合格者数欄の下段（ ）内数字は合格率（合格者数／受験者数：%）
なお，青森・高知に関しては平成元年秋期から，松江は平成二年春期から試験地となりましたので，応募者数の対前年度比増加率は未記入です。

平成２年度　秋期情報処理技術者試験

10月21日(日)に行われた平成２年度秋期情報処理技術者試験の応募状況がまとまった。今回は、全国で総数303,555人の応募があり，前年に対し12.8％の増加率であった。種別・試験地別の応募状況は別表の通りである。

平成２年度　秋期情報処理技術者試験　試験地別応募状況一覧

		システム監査	特　種	オンライン	２　種	秋期合計
札　幌		114	446	885	6,158	7,603
帯　広		3	8	59	489	559
青　森		7	33	84	921	1,045
盛　岡		17	57	192	972	1,238
仙　台		116	319	639	6,117	7,191
秋　田		13	51	85	949	1,098
郡　山		20	44	113	983	1,160
水　戸		132	551	585	4,125	5,393
宇都宮		54	187	313	2,672	3,226
前　橋		53	212	342	2,990	3,597
東京	埼　玉		1	1	6,226	6,228
	千　葉				8,458	8,458
	東　京	6,098	17,185	21,284	54,276	98,843
	八王子				5,465	5,465
	横　浜		3	1	14,896	14,900
	厚　木				4,000	4,000
	小　計	6,098	17,189	21,286	93,321	137,894
新　潟		60	234	629	3,066	3,989
長　野		50	199	246	1,948	2,443
甲　府		22	87	123	828	1,060
静　岡		98	287	516	3,975	4,876
名古屋		503	1,756	2,973	16,551	21,783
豊　橋		35	106	226	1,762	2,129
富　山		77	244	247	1,575	2,143
金　沢		77	245	346	2,169	2,837
福　井		29	129	186	1,091	1,435
大阪	京　都	219	581	689	4,579	6,068
	大　阪	1,806	5,102	5,545	24,865	37,318
	神　戸				5,958	5,958
	小　計	2,025	5,683	6,234	35,402	49,344
米　子		15	89	98	1,329	1,531
岡　山		81	404	413	3,128	4,026
広　島		167	492	994	5,644	7,297
山　口		28	83	109	1,368	1,588
高　松		50	162	235	1,915	2,362
松　山		43	132	246	1,607	2,028
高　知		7	32	108	627	774
福　岡		265	831	1,567	8,995	11,658
佐　賀		7	37	107	614	765
長　崎		6	56	73	1,138	1,273
熊　本		38	147	226	1,832	2,243
大　分		23	170	259	1,435	1,887
宮　崎		5	49	85	1,173	1,312
鹿児島		16	47	134	1,234	1,431
那　覇		6	53	146	1,132	1,337
合　計		10,360 (9.7)	30,851 (9.8)	41,109 (11.8)	221,235 (13.6)	303,555 (12.8)

合計欄(　　)内数字は対前年度比増加率（％）

1990年コンピュータ利用状況調査集計結果

当協会で行っている「コンピュータ利用状況調査」は，89年度の時点で22年間継続している調査であり，この種の調査では最も歴史があるものとして定着し，少なからぬ評価を利用者の方々からいただいている。

さて，89年度までの22回の本調査の中でもコンピュータ部門要員に関する問題は常にユーザの最も悩む事項であったといえる。慢性的な技術者不足に直面される担当者は，どの業種のユーザの方でも同様の悩みを抱えておられる。近年は特にその傾向が著しいようである。そこで本欄では，過去10年間をふりかえり5年ごとの調査結果を取り出し，コンピュータ部門要員の問題をいくつかの視点から捉え，傾向を探っていくこととした。

なお，ここではコンピュータ部門要員の問題に対する視点は次の項目を取り上げることとする。

(1)コンピュータ部門社内要員に関する問題点
(2)コンピュータ部門社内要員数
(3)コンピュータ部門要員教育費
(4)コンピュータ部門要員給与
(5)要員派遣費用

(1)要員の問題はSE，プログラマが足りないということである。

図1にみられるとおり，SE，プログラマの「絶対数の不足」を訴えている企業は10年前でもかなり多かったが，急激に増えて89年度では第1位の高さである。特にSEは，全体の7割近くの企業が同じ意識をもっていると考えられる。また，「他部門からの配置転換」，「教育」にあたっての困難

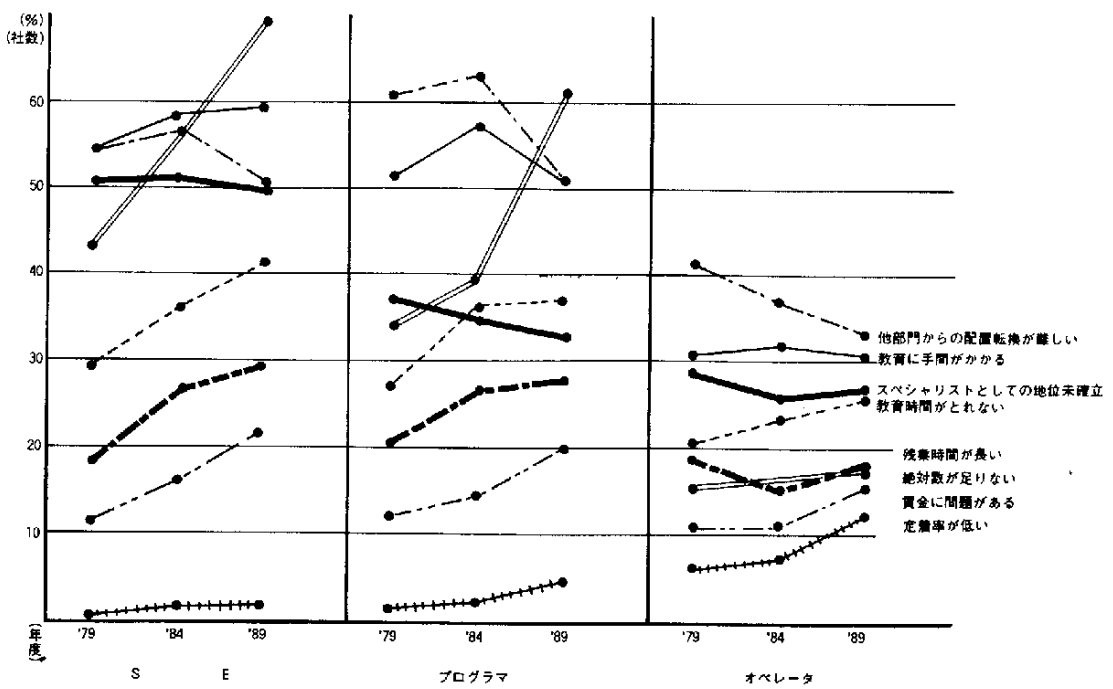


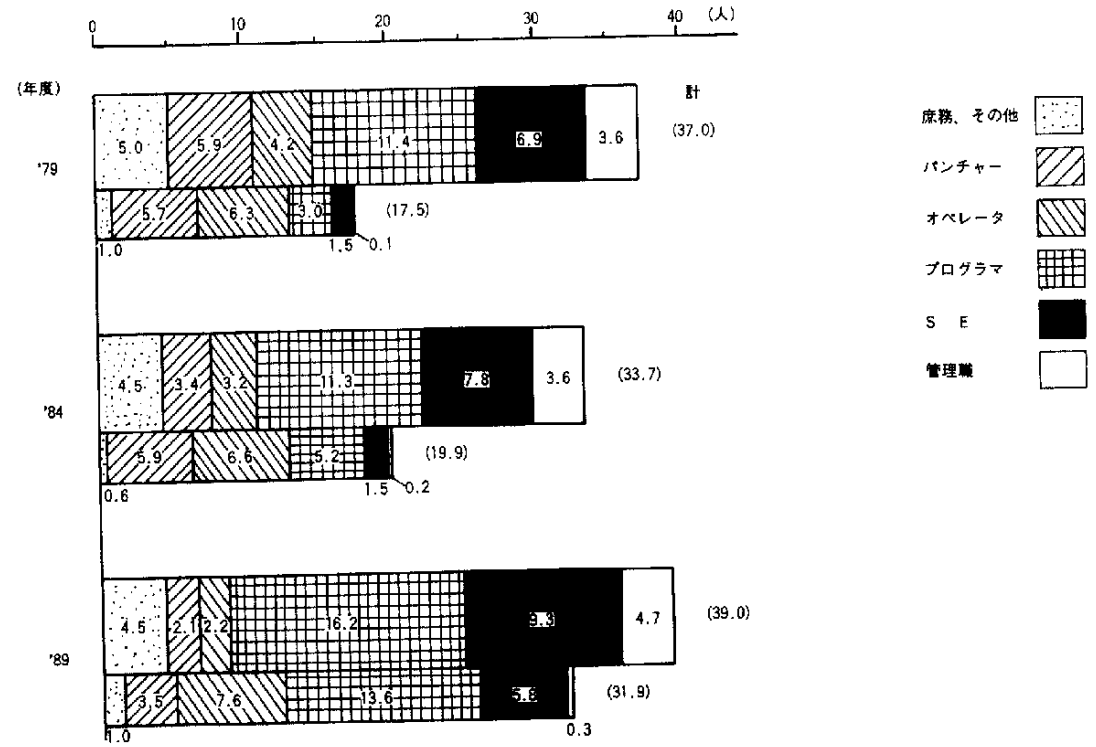
図1　職種別要員問題の変化

さが叫ばれており，この3点はいずれも企業の半数以上が挙げている。

反対にオペレータについての「定着率」の低さに問題があるとする意識は，SE，プログラマよりも高いという結果になっている。

(2)要員の数では1社当りの社内要員はあまり増加していないが，被派遣要員(外部要員)は急増している。

図2を見ると，この10年間では社内要員数は途中減少しているが1社当り平均37人から39人とほとんど変らないが，外部要員数は17.5人から31.9人と2倍近くに伸びており，社内，外部要員の差が急激に縮まっている。また，SE(管理職も含めて)，プログラマの要員の構成比率が高まってきており，いわゆる組織上の「頭でっかち」現象が著しくなってきていると思われる。



(上段：社内要員，下段：被派遣要員)

図2　職種別コンピュータ部門要員構成の変化

(3)要員に対する教育の費用は最近著しく増加している。

図3ではコンピュータ部門要員に対する教育にかかる費用の推移を示しているが，78年度は全体では1社当り平均108万円であったものが，88年度では262万円と約2.5倍に膨んできている。しかも，'78～'83ではゆるやかな伸びに対して，'83～'88では急上昇しているのが特徴的である。また，要員1人当りの教育費用では，全産業平均で28千円から58千円と，これは2倍以上の伸びを示している。産業別でみると，当初は二次産業と三次産業とを比較して要員1人当りではあまりひらきはなかったが，88年度になって二次産業(要員1人当り79.3千円)が三次産業(同47.2千円)の教育費の平均

を大きく上まわっている。(調査年度は'79,'84,'89であるが調査年度の前年の教育費の額を集計しているため，それぞれ'78,'83,'88の実績値とした。)

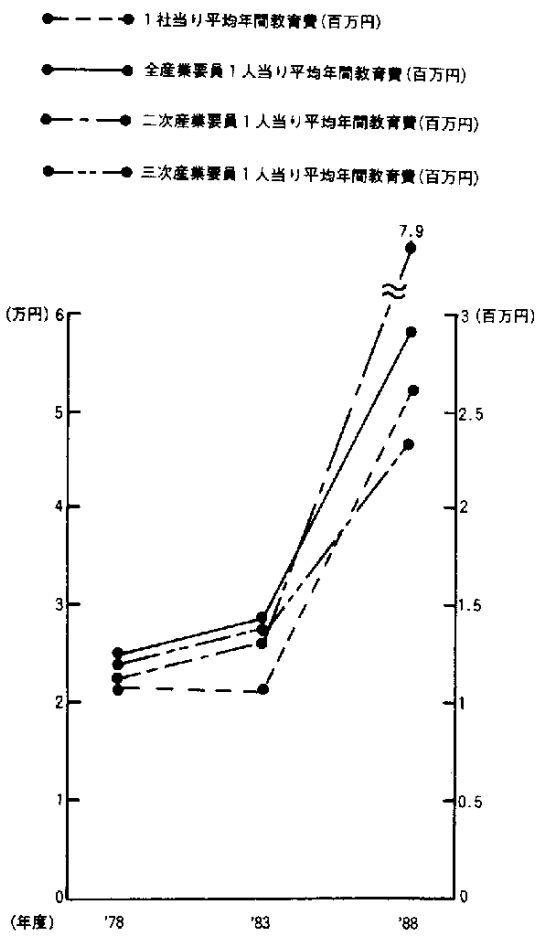


図3　産業別コンピュータ部門要員教育費(年間)の変化

(4)要員の給与は，毎年ほぼ同率で上ってきている。

図4の要員給与の変化を見ると職種別にSE，プログラマ，オペレータ，パンチャーの4職種ともこの10年間では同じような傾向で推移してきている。89年度では月額でSE292.1千円，プログラマ229.9千円，オペレータ190.0千円，パンチャー153.2千円でそれぞれ79年度のほぼ1.5倍に達している。この額は，賞与，残業手当等を含まない，いわゆる「基本給」に近いものと考えられる。10年間で1.5倍というのは平均の年率では約4％程度の上昇率であり，感覚的には世間相場よりも若干低く感じられるが，他の手当類についての調査を省略しているのでなんともいえないのが実情である。

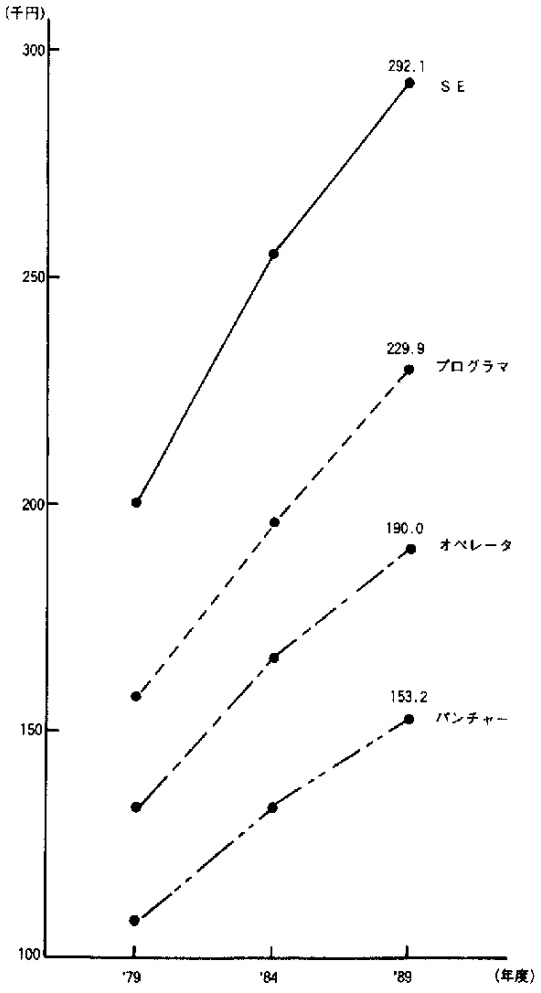


図4　職種別要員給与(月額)の変化

(5)被派遣要員1人当りの費用は1日に換算するとSE，プログラマは順調に伸び，オペレータ，パンチャーは横ばい状態である。

派遣元に要員の派遣費用として1日，1人当りいくら支払っているのかを10年の期間で示したも

のが図5であるが，結果はSE，プログラマとオペレータ，パンチャーの2つのグループで費用の上昇率に極端な差が出ている。SE，プログラマが10年前の約1.5倍と社内要員の給与の上昇率(図4)とほとんど同じ水準を示しているのに対し，オペレータ，パンチャーは同1.2倍強にしか達していない。これは(2)と図2のところで述べたように，社内要員の構成の変化によってプログラマ，SEが増加しているのとは逆にオペレータ，パンチャー層が減少している現象と関連があるのではないか。さらに被派遣要員の構成についても同様のことが起こっており，オペレータ，パンチャーを外部の要員でまかなうということが少なくなってきているのではないか，すなわち，オペレータ，パンチャーの職種については需要が減ってきていると見られる。また，派遣元では開発部隊である「プログラマ」として要員を派遣した方が有利なのではないかとも推測されるが，そこまでの実態は把握していない。

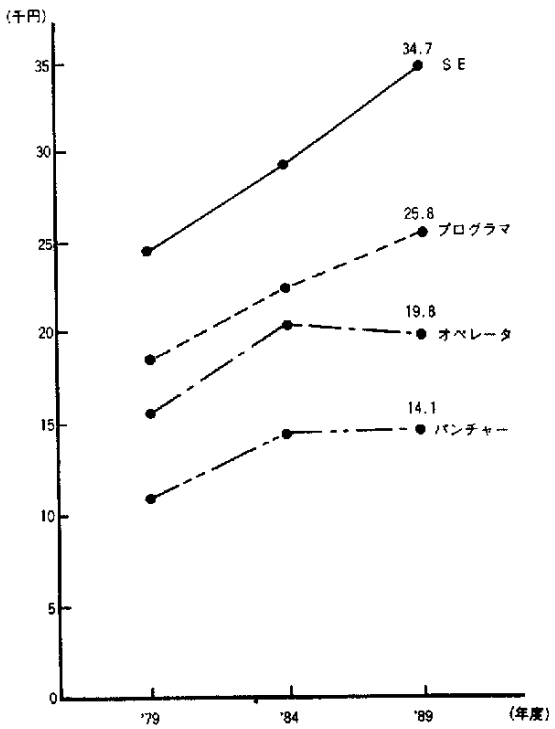
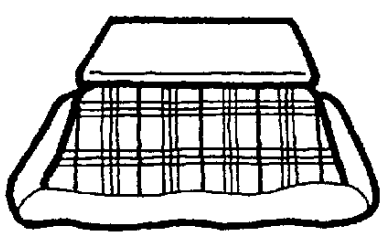


図5　派遣元に対する派遣要員1人当り日額換算支払費用平均の推移

おわりに

以上，要員に関する10年間の調査結果を5項目を挙げて簡単に紹介したが，もとより本調査は全数(悉皆)調査ではなく，年毎にサンプル数も違い，また，サンプルの企業規模等も変化しているので，一概に結果を時系列データとして見ることは無理なところもあるが，本調査が20年以上にもわたってほぼ同じ内容，項目で，調査を継続していることに多少なりとも意義を感じていただき，今後も本調査に対しご理解とご協力をお願いする次第である。



JIPDECだより

CASEシンポジウム'90報告

当協会では，通商産業省，㈳情報サービス産業協会，日刊工業新聞社の後援を得て，7月12日，13日の両日「CASEシンポジウム'90」を開催した。参加者は，招待者を含めて360名であった。

このシンポジウムは，当協会で進めているCASE (Computer Aided Software Engineering)に関する調査研究の一環として実施したものである。第一日目は，影山会長の主催者挨拶，広沢通商産業省機械情報産業局電子政策課長殿の来賓挨拶などの開会式後，米国から招待したインデックステクノロジー社筆頭取締役アール・ホスキンス氏が，「CASEの適用とその効果」について講演された。つづいてソニーテクトロニクス㈱立田種宏氏より「構造化手法による設計」について，また，㈱日立製作所堀内一氏より「データ中心手法」について各々講演が行われた。

第二日目は，米国ストラテジック・フォーカス社社長ジェイ・プラカッシュ氏より「米国におけるCASEの現状と動向」について，CASE調査研究委員会委員長原田実氏(青山学院大学)から「日本におけるCASEの現状と動向」について，報告があった。その後，川鉄システム開発㈱富沢実氏および日産自動車桂元親氏よりCASE適用事例が発表された。パネル討論会は，「CASE体験論」と題し，原田委員長をコーディネータに，新日鉄情報通信システム㈱岡本健二氏，㈱シーエスケー斉藤行雄氏，三菱信託銀行㈱三田明氏，㈱安川電機製作所元村直行氏，当協会向山博の各パネリストにより報告討論があり，次いで会場内の参加者との間で質疑応答が行われた。

また，シンポジウム期間中，CASEベンダー8社によるツール展示とデモンストレーション及びツール説明会を同時に開催し，多数の参加者が熱心に説明を受けていた。

このシンポジウムには，予想を越える多数の参加者を得ることができ，ソフトウェア開発における生産性と信頼性の向上に対する関心の高さが改めて認められた。今後とも，この種の問題への更なる取り組みの必要性を痛感した次第である。

AI振興センター

1．AIオープンハウス設置機器の入れ換え(報告)

AIツールの共同利用センター「AIオープンハウス」は，開設して以来3年目に入ったのを機会に下記のとおり機器やソフトウェアの入れ換えを行った。併せて，ツールの相互利用を容易にするため，設置機器をローカルエリアネットワーク(LAN)で接続した。また，高速処理用ワークステーションに対応可能な大型プロジェクタを設置し，AIオープンハウス内でのツールの操作説明やデモンストレーションの際にディスプレイの出力結果を拡大して容易に見ることができるようにした。

2．「人工知能総合展(AI'90)」への出展(報告)

ICOT-JIPDEC AIセンターは，本年7月2日～5日に日本経済新聞社が主催して東京流通センターで開催された。「人工知能総合展」に協賛するとともに，主催者共通コーナーに出展した。出展内容は，AIセンターの事業の紹介，第五世代コンピュータ開発プロジェクトの後期計画などについてパネルとビデオにより紹介した。なお期間中の入場者は4万3千人であった。

3．AI講演会の開催(報告)

管理者やビジネスマンを対象に斯界の第一人者

の方を講師にAIの技術や利用の動向について解説していただく「AI講演会」を次のとおり開催した。

第14回(平成2年5月15日開催)

演題：最近のハイパーメディア等に関する動向

講師：田中　譲　北海道大学工学部教授

第15回(平成2年6月27日開催)

演題：情報検索と人工知能

講師：有川　節夫　九州大学理学部教授

4．今後の予定(ご案内)

「平成元年度知的ハイパーテキストに関する調査研究報告書」の頒布

知的オフィスオートメーションのキィテクノロジイと期待されているハイパーテキストとAI技術の融合による「知的ハイパーテキスト」について，調査研究委員会(委員長：田中　譲　北海道大学工学部教授)を設置して調査研究を行っている。なお昨年度の調査研究報告書を実費(賛助会員価格4,000円)で頒布している。

出展社名（五十音順）	ハードウェア（稼働環境）	AIプログラミング言語	エキスパートシステム開発支援ツール
伊藤忠テクノサイエンス	SUN-3/260C	SUN Common Lisp	＊G2
岩崎技研工業	(PC9801VX)		AI PLAN TELL
インタフェイスコンピュータジャパン	(AV310C)	＊IF Prolog	
エー・アイ・ソフト	(PC9801VX)		創玄、大創玄
NTTインテリジェントテクノロジ	＊ELIS 8242	Common Lisp	
NTTソフトウェア	(PC9801VX)		KBMS/PC
シーアイテクノセールス	(SUN-3/260C)	IXLA	
シーイーシー	(PC9801VX)	GC Lisp 286 Developer	
センチュリリサーチセンタ	EXPLORER-II	Common Lisp	Knowledge Graft
	(PC9801VX)		Personal Consultant
知識工学研究所	(PC9801VX)		GURU
東洋情報システム	Symbolics 3650	Common Lisp ＊Statice オブジェット指向	Super BRAINS
日商岩井	(EXPLORER-II)		GEST
日本データゼネラル	＊AV310C	Common Lisp	
日本ユニシス	＊U6000/51C	Common Lisp	＊KES-II
日立製作所	日立クリエイティブワークステーション2050/32	Prolog	ES/KERNEL/W
富士通	FM-G150A/20	Common Lisp	ESHELL/X
三菱電機	MELCOM PSI-II	ESP	EXT-KERNEL-II

上記のほか、パーソナルコンピュータの稼働環境として、日本電気PC9801VX、マッキントッシュII及びSE、三菱電機MAXY、NeXTシステムの5機種を導入,運用しています。

インフォメーション

〈イベント名〉①開催日②開催場所③主な内容④問合せ先

3年1月

〈基盤技術研究促進センター創立5周年記念研究報告会〉①3/1/21②経団連ホール③出融資プロジェクト報告，出資4件，融資2件。特別講演　唐津　一④基盤技術研究促進センター☎03-3505-6811

3年2月

〈情報管理専門研修会〉①3/2/7～3/2/8，3/3/7～3/3/8（東京）3/2/21～3/2/22（大阪）②JICST　7Fホール（東京），大阪科学技術センター（大阪）③メインテーマ「情報の戦略的活用」について6名の講師が講演する。④日本科学技術情報センター☎03-3581-6411

〈パソコン通信ネットワークに関する特別研修〉（岡山）①3/2/20～3/2/21②山光荘③パソコン通信ネットワークの現状を明確にし，活用の可能性基本的考え方及び課題等について認識を深める。④(財)地方自治情報センター☎03-3261-8922

〈第3回コンピュータ・ソフトウェアの法的保護に関する国際シンポジウム〉①3/2/19～3/2/20②京王プラザホテル③「ソフトウェアの発展と法との緊張関係」をメインテーマに，基調講演および3つのセッションを行う。セッション1「プログラムの保護範囲に関する最新動向―今，日米欧で何が起きているか―」。セッション2「ソフトウェア技術の進歩と法的対応―どうなる，プログラムの創作性，類似性，権利帰属―」。セッション3「プログラム関連発明に関する特許保護の国際的動向―特許と著作権の保護範囲―」。④(財)ソフトウェア情報センター☎03-3437-3071

〈書籍名〉①発行日②内容③発行者

新刊案内

〈情報システム分野における「人材教育・育成調査報告書」〉①3/1/中旬②総論，データ編，実例編，資料編からなる。実例編ではSE教育，EUC教育について先進企業の54事例を紹介。また，資料編は教育機関案内となっている。③(社)日本オフィスオートメーション協会☎03-3434-6677

通商産業省よりのお願い
「特定サービス産業実態調査」にご協力を！

通商産業省では毎年，サービス産業の実態を把握しサービス産業統計の整備拡充を図るため，「特定サービス産業実態調査」を実施しています。この調査結果は，サービス産業の事業活動や経営の実態を明らかにし，サービス産業の発展を目指した各種行政施策の検討を行うための基礎資料となるだけでなく，皆様の経営上の参考資料としても大変貴重なものとなります。また，調査結果は統計以外の目的に使用されることは絶対になく，ご協力いただいた方々の秘密は厳守されます。

調査実施は12月ですので，皆様のお手元に調査票が届けられました際には是非ともこの調査の趣旨を御理解いただき，調査票の記入，提出にご協力下さいますようお願いいたします。

12月1日特許庁新システム(電子出願)稼働開始！

通商産業省特許庁では，かねてより導入準備中であった『電子出願』システムを平成2年12月1日より稼働させた。

従来，工業所有権の出願・受付，審査等の業務及び工業所有権情報提供サービスは書面によって行われていたが，その数は膨大な量であり平成5年には5,000万件もの特許情報が特許庁内に蓄積されると見込まれる。これを従来の方法で処理していたのでは効率的な業務遂行が困難であり，業務効率向上のための対策を立てることが急務となっていた。

そこで特許庁は，①工業所有権の審査期間の短縮，②工業所有権情報サービスの拡充，③事務処理の効率化，④国際的な工業所有権情報交換等の協力の推進，の4つを目的として昭和59年より『ペーパーレスシステム計画』を推進し，本年12月1日よりオンライン，FDによる『ペーパーレスシステム(電子出願)』を本格稼働するに至った。このシステムの導入により，今後書面だけでなくオンライン，FDによる出願が可能となる。

12月1日は，通商産業大臣，政務次官出席のもと記念式典が開かれ，特許庁長官の挨拶のあと，1F出願課窓口においてテープカットと共に通商産業大臣によってオンラインのスイッチが入れられた。また，式典では功績のあった関係者に対し感謝状が授与された。

特許庁では今後，閲覧・送達，通知，審査事務処理，審判手続等の電子化及び意匠・商標の電子出願制度の導入について，技術的課題，各手続の電子化の進捗状況等を見つつ，平成5年度以降段階的に実施していく考えである。

平成2年12月　発行

JIPDEC ジャーナル No. 74

発行人・照山正夫／編集人・日高良治

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
郵便番号105　　電話 03(3432)9384

※本誌送付宛先の変更等については当協会調査部 (03-3432-9384) までご連絡下さい。

通商産業省機械情報産業局監修

コンピュータウイルス対策基準解説書

通商産業省策定の「コンピュータウイルス対策基準」
(官報告示第139号)の解説書

Ⅰ　基準の構成

①ユーザ基準

大型汎用コンピュータからパーソナルコンピュータまで，全てのユーザを対象として，ソフトウエア管理・運用管理およびウイルスに汚染された場合の事後対応の観点から19項目の基準を定めています。

②システム管理者基準

コンピュータシステム管理者（様々なレベルにおけるホストの管理者）を対象として，ソフトウエア管理・運用管理・ネットワーク管理および事後対応の観点から27項目の基準を定めています。

③ソフトウエア開発管理者基準

ソフトウエア開発環境における管理責任者を対象として，開発環境管理・製品管理および事後対応の観点から13項目の基準を定めています。

Ⅱ　解説の内容

解説は，基準の１項目ごとにその主旨，対策のポイント，具体例・その他という３つの観点に統一して，理解しやすく記述しています。

①基準の主旨

各基準がなぜ設定されたのか，その理由や背景をわかりやすく説明しています。

②対策のポイント

当該基準に対して考えられる対策のポイントを箇条書で示しています。

③具体例・その他

当該基準を実施するための具体的な方法論など，参考になると思われる情報を収録しています。

定　　価：一般2,200円　会員1,800円（税込。送料別。）

――システム監査シリーズ　全３冊――

多くの方々からご好評をいただいております本シリーズは，通商産業省によって昭和60年に「システム監査基準」が公表されたのに伴い，システム監査の重要性を広く認識し，効果的にシステム監査を実施していただくことを目的に編集されております。

システム監査基準解説書　システム監査基準，基準の概要，基準の逐条解説および参考資料から構成されております。システム監査を知る上での基本の１冊と言えます。

システム監査Ｑ＆Ａ110　当協会が開設したシステム監査相談室に寄せられた相談内容の中から110項目を選び，システム監査実施上の様々な問題点に対して，Ｑ＆Ａ形式で回答いたしております。

システム監査実施の手引　「情報システムとシステム監査」「システム監査Ｑ＆Ａ」「事例紹介」の３部構成となっております。これからシステム監査を実施なさる方，現在システム監査を実施している中で問題点を抱えてお困りになっている方に最適の書。

定　　価：各　一般2,900円　会員2,300円（税込。送料別。）

お申込み：〒105 東京都港区芝公園3-5-8（機械振興会館内）

財団法人　日本情報処理開発協会　　調査部　普及振興課

☎03-3432-9384 / FAX03-3432-9389

JIPDEC
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
郵便番号105　　電話 03(3432)9384

Japan Information Processing DEvelopment Center