JIPDECジャーナル

NO.77
1992/MAR

- 春　夏　秋　冬：情報化社会とセキュリティ
- 寄　稿　・　解　説：日本のセキュリティ政策
- JIPDEC REPORT：国際情報セキュリティシンポジウム

目　次

No.77 1992/MAR

春夏

情報化社会とセキュリティ

セコム株式会社　常務取締役
セキュリティ対策委員会委員長

安保　二見男

社会がより豊かで便利な生活環境を求めていることは洋の東西を問わず当然なことであり，人間の欲望は限りなく拡大される。しかしこの半面新しいリスクが発生し，これ等を護るためのセキュリティが必要になってくる。

日本の民間警備会社の歴史は今だ30年程度であるが，その急速な発展ぶりは世界でも類を見ない。昨年12月末で東京の警備員の数は59千人，全国では247千人となっている。

昭和30年代の後半には人による常駐警備から始まり，次に巡回警備(即ち数件のお客様を1人が巡回して警備する。)が加わり，昭和40年に入り機械警備が登場する。機械警備システムはお客様と電話回線によって警備会社のセンターマシンと繋がれ，24時間遠隔監視され，事故が発生すると直ちに緊急対処と共に状況によって警察，消防への通報を行うまったく新しい警備システムとして脚光を浴びた。

欧米ではその時期に同様のシステムはあったが，異なる点はユーザーに設置する機械(センサー，発信機等)は売ってしまい，後は監視だけで，緊急対処はやらないシステムとなっていた。日本は機器も運用もすべてレンタルで運用することとした。これはセキュリティのクオリティを確実に保つために絶対に不可欠の条件としてこの方式を採用した。例えば誤報が出た場合，レンタルの機器ならば自分の責任で取り換えが出来るが，売り切りの場合ユーザーの所有物であるから誤報が多いといって勝手に取り換えることは出来ない。従って，緊急対処も誤報であっても何回でも出動しなければならない。これでは本当の火災や犯罪の発生し

た時に的確な対応が取れなくなる。

この機械警備システムは，昭和40年代の高度経済成長の波に乗って急激に拡大され，現在では全国で約52万件に及んでいる。

実は，この機械警備システムのネットワークの構築が情報化社会に於ける究めて大きな役割を果たすことになるのである。専用線または公衆線によって，各個別のユーザーと結ばれたネットワークの大きさは世界最大級のネットワークであり，また現在警備のビジネス用として使用されているのは僅かに数パーセントに過ぎない。従って，今使用されていない90％以上の容量を新しい付加価値として回線を利用すれば，情報化時代に於ける有力な情報ネットワークとして大きな戦力となるのである。

情報化社会に於けるネットワークは，セキュリティビジネスにとって人間の体に譬えるならば「神経」といえる。神経によって末端から伝えられた情報は，センターのコンピュータ(即ち「頭脳」)により判断し，手足に向けて行動を起こすように命令される。そこで手足(即ち「筋肉」)が緊急対処を行う。即ちセキュリティビジネスの基本は，「神経」→「頭脳」→「筋肉」の三つの要素が完全に機能することなのである。

今，我々が日常の生活の中で金を出し入れするのは人との接点ではなく，機械(CD・ATM等)との接点となっている。今後ホームバンキングが各銀行で開始された場合，犯罪或いは事故に対応するセキュリティは社会的に究めて重要なファクターを有することになる。機密の漏洩，プライバシーの保護，本人確認，コンピュータ及びネットワークの安全対策，データ保管，保険等セキュリティは各分野に於いてその責任者が，その重要性を認識し確実に実施して初めて安全な情報化社会が成立するのである。

日本はセキュリティに対する考え方が欧米諸国に較べ非常に甘い。これは基本的な社会組織の差であり，欧米の「鍵社会」と「ドロボーはお上におまかせ」の違いと言えよう。しかし，情報化時代は距離を超えた地球的な相互の情報交換が行われ，特に経済が中心となってきた世界の中に於ける日本の位置付けは日本だけでなく国際的な影響力を持っているのである。

金融市場は，ニューヨークと東京とロンドンが支配していると言われるが，今や情報化社会も同様，国際社会の中での日本としての責任において，官民一体となってセキュリティの対策をすべきである。

日本のセキュリティ政策

——国際情報セキュリティシンポジウム　基調講演より——

通商産業省機械情報産業局
情報処理振興課長　中村　薫

わが国のコンピュータセキュリティ対策について，国際的な比較をベースにこれらの施策がどういう形でなされているかということについて説明致します。

ご承知のように，コンピュータセキュリティ対策というのは国際的な問題になってきておりますが，必ずしも各国が日本と同じような政策を進めているわけではなく，また，日本が各国と同一レベルで政策を講じているわけでもありません。それを踏まえ，わが国の政策について説明致します。まず，わが国のコンピュータセキュリティ問題に対する関心というものは，欧米とは異なり，1978年の宮城県沖地震や1984年の世田谷の電話ケーブル火災事故等，地震，火災などの自然災害に対してコンピュータシステムをいかに守るかという観点から出発してきております。これに加えて，最近のさまざまな事故やコンピュータウイルス，また，ハッカー等の問題に対する対応も注目されてきているところであります。

このような世論の関心の背景となるものではありますが，ちなみにわが国のコンピュータシステムについての事故の原因を原因別に区別してみますと，ハードウェア，ソフトウェア障害によるものが8割近くを占めております。次いで，空調や回線障害によるものがあります。また，人による誤った操作，いわゆる過失による事故というものも大きなウエートを占めてきております。逆に，ハッカー等悪意の人によるものは原因のうちの1％にもなっておりません。

このようにわが国のセキュリティ問題の背景は若干欧米と異なるために，対策もこのような現状を踏まえて講じられてきていると言えます。

近年，コンピュータシステムの大規模化，ネットワーク化に伴い，いくつかの変化が顕れてきております。これは広い意味で欧米と同じような傾向が見えてきているということが言えるかと思います。

1つは，システムダウンの発生率自体は減少してきております。システム自体の数が増えておりますから，件数は膨らんできておりますが，ダウンの発生率自体は改善してきております。これは1システム当たりの，事故が起きてから次の事故までどれくらい時間がかかっているかということを見てみますと，だんだん事故が少なくなっているということからわかるわけですが，逆にシステムが大規模化してきているために，一旦システムダウンが起こると，回復に長い時間を要するようになってきております。

また，もう1つは，ウイルス等に見られるようなコンピュータ犯罪が，欧米より件数は少ないも

のの増加傾向にあります。特に昔はコンピュータのデータをコンピュータにいたずらするというより，コンピュータから情報を盗んで悪いことをするという犯罪が多かったのですが，最近はコンピュータの機能を阻害する犯罪，ファンクションを阻害する犯罪が増加してきております。いわゆるウイルスであるとかそういう類のものが増加しております。

このような背景のもとに，コンピュータ犯罪に対する社会的安心も高まってきております。ちなみに，財日本情報処理開発協会(JIPDEC)が行ったアンケート調査によれば，コンピュータ犯罪に対して現行刑法では不十分と答える人の割合が4割を超えております。ご承知のように，日本の刑法の場合，無権限アクセス，それからいわゆる未遂に対する罰則規定はないわけですが，既遂にならなければ罰せられないという現行刑法に対して不十分と答える人が4割を超えているということは，世論の変化が窺えるかと思います。

他方，同じアンケート結果からですが，データプログラミングののぞき見，会社のコンピュータを私用に使うこと，いわゆる無権限アクセス自体を犯罪として考えるという人は1割に満たない。このようなこと自体を会社内部の訓告の対象にするとか，そういう意味でのモラルとして規制するということについてはかなりの方が賛成しておられるわけですが，これ自体を犯罪として見るということについては1割以下の人しか同意していない。その意味で，コンピュータシステムの無権限アクセスその行為自体を刑罰の対象と考えることには世論は否定的とみているというように考えられると思います。

他方，そのようなこと自体は，会社の内部のいわゆる社内処罰の対象となると考えている人は増えてきておりますし，また，他社のデータに対してそういうことを行った場合はやはり犯罪と見るべきではないかという人は増えております。

次に，このような日本の現状を踏まえて行われている通商産業省のコンピュータセキュリティ対策についてご説明します。

まず，コンピュータによる情報化というのは，産業界から社会，一般家庭へ着実に普及してきております。しかしながら，先ほど申しましたように，日本国内における宮城県沖地震であるとか，ケーブル火災事故であるとかいうような事故もありましたし，また，国際的に見ても―昨年のサンフランシスコ地震であるとか，昨年のニューヨーク停電，また，新聞紙上を賑わせておりますコンピュータウイルス等に見られるようなコンピュータシステムの停止や悪用ということが起こった場合における社会的影響の大きさということも注目をされてきているところです。

このようなコンピュータシステムの脆弱性をできるだけ克服するためにも，コンピュータセキュリティ対策が重要と考えられます。

通商産業省は，1977年に電子計算機システム安全対策基準，1985年にシステム監査基準をそれぞれ公表してきておりますし，また，1990年4月にはコンピュータウイルス対策基準を作成，公表，普及してきております。また，本年に入りましてシステム監査企業台帳の作成，また5月には電子計算機システム安全対策基準の改正作業等を行ってきたところです。

以下，最近の通商産業省のコンピュータセキュリティ対策についてご紹介いたします。

なお，ここでは説明を省略しますが，わが国の場合，通商産業省は一般的なコンピュータセキュリティ対策を行っているわけですが，ほかにも，例えば金融機関に対して大蔵省がセクター別の対策を行ってきておりますし，そういう意味で通商産業省以外にも大蔵省とか郵政省とか自治省とか総務庁とか警察庁とかがそれぞれの特殊分野についての対策を講じてきております。

ただ，日本の場合，諸外国と比べてそれらの対

策はどちらかというとガイドライン中心といいますか，法の強制，罰則規定を持たない形で行われているということは各国比較をする意味で注目に値すると思います。

通商産業省の電子計算機システム安全対策基準というものは，先ほどご説明しましたように，1977年に初めてつくられました。その後，1984年に改定されておりますが，昨年，1990年，全面改定の必要があるということで改定作業に着手し，1991年の5月に新しい電子計算機システム安全対策基準が策定，公表されました。

どのような観点からこの基準が定められているかということですが，新しい基準の特徴点は大きく分けて3点ほどあると思います。

1つは，今までのオーバーオールな基準，画一的な基準で定められていたものを関連スペースごとに対応した基準という形になってきております。要するに今回の改定ではインテリジェントビルであるとか，パーソナルコンピュータ化等，事務所，コンピュータの使われている状況などが異なってきていることから，電子計算機システムに関係するスペースを，計算をするところであるとか，データを保管するところ，端末とか，後処理をするところ，管理室であるとか，電源室であるとかの13のスペースに分けて，それぞれの項目，セクター別に基準を設けております。

第2の特徴点は，ネットワーク化に対応致しまして，電子計算機のシステムの接続形態ごとに基準を分けて，区分を明確にしております。

第3の特徴点としては，システムの重要度に応じて対策項目を示しております。最も重要なシステム，これは人命であるとか他人の財産，プライバシー等の社会に影響を与えるシステム，第2番目に重要なシステム，これは，企業への影響が大きいもの，第3番目としてそれ以外の比較的影響度の小さいものといったカテゴライズに分けて，それぞれ基準に示しております。

これが新しい基準の内容ですが，個別項目についてはいくつかの具体的な基準が定められております。例えば，ハロンガスが規制された場合にどのような対応をとっていかなければならないかとか，そのような新しい技術進歩ないし社会の規制の変化に伴った基準の見直しが行われております。

通商産業省の対策の次の柱として，情報処理サービス業に対する電子計算機システム安全対策実施事業所認定制度というものがあります。これはいわゆる他人の情報を処理する，特に社会的影響の大きいシステムを行っている民間の情報処理サービスは安全対策に注意を払いながら実施する必要があるわけですが，そのような対策を行っている事業所を認定するという制度です。これは強制的な制度ではありませんが，ボランタリーに自己申告で認定を受ける。その場合，通商産業省から認定されて，その企業は——企業というよりは事業所ですが，セキュリティがある一定の水準に達しているということを確保するものです。

この制度自体は1981年7月に設けられた制度です。具体的な実施方法は，ハード面の検査というものを通商産業大臣が指定した指定検査機関，具体的には財機械電子検査検定協会が設備面の検査を行うとともに，通商産業局が運用検査を行い，それに合格したところを認定委員会(これは通商産業省の第三者からなる諮問機関)の審査にかけて合格したところを認定していくという制度です。1991年6月現在時点での認定事業所は170事業所ありますが，全国の主要県，ほとんど各県と主要都市にこのような事業所が増えてきております。

この検査で認定を受けますと，ある程度社会的にセキュリティ対策が充実しているということが認められておりますから，官公庁であるとか金融機関等の公共性の高いデータを扱うところで外部発注をするときに，いわば入札の際に安全対策がよく行われているかどうかを調べる際の1つの手がかりといいますか，入札の際に考慮されるよう

な運用がされてきております。運用がされているというのは，これは別に法律によって義務づけられているわけではないのですが，実態的には関係者がそれを尊重するというか，考慮しながら仕事を行っているというのが実態です。

次に，コンピュータウイルス対策関係についてご説明します。

わが国では，新聞などにも報道されておりますが，3年前からコンピュータウイルスが発見されて，それから順次増えてきております。海外で発見されたウイルスが日本に入ってくるということも増えてきております。

このような現状に鑑みまして，通商産業省では1990年に内部委員会を設置し，同年4月にコンピュータウイルス対策基準を公表いたしました。コンピュータウイルス対策基準自体は，コンピュータウイルスに対する予防，それから検知，要するに調べる。それから事後対策をどうするかということについての必要と思われるガイドラインを定めたものですが，これは現在利用されているシステムの機能で対応できる，現実的な実効性のある対策にはどういうものがあるかということを広く皆さんに知らせたという効果を持っております。

この基準の特徴としては，そのような現実的な対応可能な対応策で構成してあるということと，パソコンから大型機までの全機種に対応している。対策基準自体はかなり汎用性を持たせている。それから，最も大きな特徴点としては，コンピュータウイルスの被害の拡大および再発の防止をするために，必要な情報を公的機関に届け出ることにしております。公的機関というのは，具体的には通商産業大臣告示で情報処理振興事業協会(IPA)を定めております。今まではコンピュータウイルスが発見された場合に，被害を内密にするケースが多いために，正しい情報が広く伝わらない。その結果，被害が拡大するという傾向が多かったために，このような公的情報機関を作ったわけです。また，ワクチンを作る場合等の二重投資を避けるというような効果を期待しているわけです。届出件数もだんだん増えてきているところです。

次に，コンピュータウイルス対策について注目されるべきは国際的視点がこの対策にとって必要であるということです。アメリカを中心にして，日本だけではなく，ヨーロッパ，アメリカなど各国で新しいウイルス，また，それら先進国のみならず，発展途上国でもウイルスが作られる。それが国際的に影響を与えてきている。また，国際的なネットワークの広がりによってウイルスが広まってきているということが大きな問題になっている。その意味で，国際的にはウイルスを作った場合の犯人の特定方法であるとか，犯人引渡しとかいろいろな問題がこれから出てくる。通商産業省としてはこうした問題を国際的にどう対応すべきかということを各国と協調しながら検討していく必要があると考えております。

次に，システム監査対策についてご説明します。

コンピュータシステムというのは利用分野形態が非常に多様であるために，一律的なセキュリティ対策を議論することは難しい。そういう意味で，費用と効果を考慮したそれぞれのシステムごとのコンピュータセキュリティ対策というものが必要になるわけです。これの費用対効果をどのように考慮していくかということと，他方，コンピュータ処理の信頼性の確保，それから効率性の向上というものが経営上重要な問題になっているという観点から，通商産業省はこれらの問題に対応するためにシステム監査というものを広く一般の方々に知ってもらいたいということで，1983年からこの問題についての検討を始めております。1984年に，この議論の結果を踏まえてシステム監査基準というものを設けました。システム監査の基準内容はかなり技術的なものですが，非常にきめ細やかな基準になっております。これは別に法律に基づくものではありません。いわばどういう項目を

どういう観点からチェックするかというような教科書的なものですが，現在システム監査関係者のバイブルというような位置づけで実質的に尊重されているということです。

通商産業省はシステム監査の普及とシステム監査の実効を上げるために，情報処理システム監査技術者試験を情報処理技術者試験の一環として実施してきております。具体的には，1986年から毎年試験が行われているわけですが，現在までに約2,000名の方が合格されており，かなり高い質の試験と認められております。

また，このようなシステム監査対策の一環として，1991年3月にシステム監査企業台帳というものを作成することにしました。わが国の場合，まだ必ずしもシステム監査というものが広く皆さんに知られていないために，どういう企業がシステム監査の能力をどの程度持っているのかということをそれぞれの企業に自分で登録してもらう。登録すれば，逆にユーザーの方は，どういう企業がどの程度，どういうシステム監査を出来る人が世の中にいて，どの程度の技術レベル，能力を持っているかということを調べることが容易であるというような観点でこのような台帳を作ったわけです。(1991年10月作成)

次に，今後のコンピュータセキュリティ対策についてご説明します。

わが国のコンピュータオンライン化というものは現時点で9割近くになっており，また，パソコンの出荷台数も平成元年には165万台というように急速な勢いで増えております。さらに，ネットワーク化というものも，例えば，パソコン通信サービスというものが3年前には9万人であったものが，一昨年の2年後には38万人，約40万人に増えているというようなことで，非常に大きな社会的な広がりを持ってきている。そういう意味で，コンピュータについての問題の重要性が生じてきているとともに，このようなものを1つのセールスとしてとらえていくという動きが生じてきています。既にアメリカなどではこの様な形での産業が起こってきていますけれども，日本においてもいわゆるコンピュータセキュリティ産業というものが片一方で出てきております。

次に，このようなコンピュータ対策関係について，われわれとしては国際的に貢献をしていかなければならないとの認識があります。国際的な範囲で考えなくてはいけないということについては，いくつかのポイントがあります。1つは，基準などの統一，ハーモナイゼーションの問題があります。各国がバラバラに基準を作る，ないし，その基準を満たしているかどうかをチェックするためのいろいろなソフト面の投資であるとか，基準を作るための投資というものはかなり社会的に見てばかにならないものになってきております。また，特にハード面などについてそういうバラバラな基準自体が新しい貿易障害ともなりかねないことも懸念されております。

そのような意味で，われわれとしては国際的なある程度調和のとれた，ヨーロッパにおけるITSECであるとかアメリカのTCSECなどを含めた基準の調和というものが必要になってきていると思います。通商産業省におきましても9月末からオープンシステム環境整備委員会を設け，その中の一つの柱としてセキュリティの技術基準の策定，検討作業を行ってきているところですが，これも当然国際的な動向の中でわれわれとして議論を進めていく必要があると思います。具体的には来年の3月までに中間的な方向を打ち出し，最終的な結果としては，1993年の3月までに最終答申をいただきたいと考えておりますし，そのような技術基準の調整の場としてISOなどの国際的な場を活用しながら進めていく必要があると思います。

当然のことながらそのようないろいろな技術基準を作る場合に，国防上の観点というものは別途の要請として各国が定める分野は残ると思います

が，ある程度それに悪影響を与えない範囲で，また民間でいろいろな基準などを定めるときに統一的な基準の調和というものが必要になってきているとわれわれは認識しております。

それから，国際的に行われる問題として，われわれとしてある程度貢献できる部分もあると思います。海外と比較して，日本の場合，民間のシステム安全対策基準というものがかなり整備されてきていると思いますし，そのため比較的システムダウンというものも相対的には少ないと理解しております。そういう意味でもわが国の民間の取り組みについてのノウハウというものを国際的な場で提供していくことが可能かと思います。

また，われわれとしては刑法の問題というものは考えていかなければならないと思います。刑法の問題については通商産業省があれこれいう立場にはないわけですが，アメリカ，ヨーロッパの各国，大きな国はコンピュータの無限アクセス自体についての処罰規定を整備し，ないし整備し終わったというような方向があるわけです。それについて日本としてどう対応していくかというのが，われわれにとっての大きな課題になってくるものと思います。

他方，国際的にはそのような動きがあると共に，先ほど説明したように，必ずしも日本の現状というのはすぐに無限アクセスについて処罰するということはどうかというような社会的認識が片一方にある。これは現場というか，私のようなある程度情報処理産業に携わっている者から見ても，例えば，会社のコンピュータを使ってゲームソフトを楽しんでいる人とか，少し他人のカードとやり取りしながらコンピュータを動かしたりしているようなケースなど刑法で処罰されるべきものと，社会的に認められるものとの間にかなりグレーな部分，モラルに依存する部分が多いかと思います。これを果して一律に罰則の対象とするということがいいかどうかということが議論の対象になってくると思います。この問題は必ずしも日本だけで決められる問題ではなくて，日本だけが罰則が甘いということになると，国際的にウイルスなりについて日本が非常に甘い国という国際的な調和の問題が片一方で出てくる。非常に問題であると考えています。

それから，技術開発について国際的な協力の場というものが必要であるというように考えております。ワクチン開発技術であるとか，セキュリティ製品の技術であるとか，いろいろなセキュリティ関係の技術について国際的な協力というものが今後必要になってくると考えております。

次に，われわれ日本もそうですが，セキュリティ対策というものは，まず啓蒙普及活動というものが一番初めに重要になっていくだろう。そういう意味で，今回JIPDECが行ったような国際シンポジウムというものが国際的にも持ち回りで毎年行われるとか，国際的にもある一定の日を定めてコンピュータセキュリティの問題について議論し，考えるような日が設けられるとか，いろいろな意味での啓蒙普及活動をこれから進めていく必要があるのではないかと考えております。

4番目としては，発展途上国への援助の問題があると考えております。セキュリティ対策というのは先進国，どんなに広げてもOECD加盟国だけがやればよいという問題ではないと思います。少なくともコンピュータシステムが今や国際的につながってきておりますし，実態からみてもウイルスを作ってきているのは必ずしもOECD加盟国だけではありません。それこそイスラエルで作られたり，アラブで作られたり，東欧で作られたり，アジアで作られたりするというような事態に備えるためには，発展途上国にもこのようないろいろな国際的な活動，支援対策というものを先進国として考えていくことが必要かと思います。OECDがその場合の活動の大きな考慮要素になるとわれわれは考えております。OECDの場そのものであ

るのか，それともOECDの民間部門を担うところであるBIACという団体をベースにするのか，今後検討する必要があると思いますが，このような国際的な強調スキムというものを考えていくことが必要になってきていると思います。

それから，わが国の取り組みについてですが，通商産業省だけでもJIPDECのほかに，例えば，コンピュータのハード及びOSを中心にしてセキュリティ対策を考えている㈳日本電子工業振興協会(JEIDA)それから先ほどご説明したコンピュータウイルスの登録機関及びコンピュータウイルス対策を中心に進めているIPA，そのほかいろいろなチェック機能を持っている㈶機械電子検査検定協会等々がありますし，通商産業省関係以外にも例えば，㈶金融情報システムセンターを始めとする機関が広範なコンピュータセキュリティ問題を扱っております。そういう関係機関の連携，例えば，協議会スタイルでも構わないと思いますが，そのような場を設けていくということは必要だと思います。国際的な協調も必要ですし，国内的な調和の場というものも必要だと思います。

国際的，国内的対策についてわれわれとして考えているところは以上の通りですが，コンピュータセキュリティ産業の育成ということも通商産業省にとって新しい課題になってきていると思っております。

国際情報セキュリティシンポジウム

今日，情報システムは，ネットワークの発展により国境をこえて相互に接続され，情報処理においてもはや国境はない状況を呈しています。その結果，地球上の各地は，時間的に等距離になり，極めて効率的かつ便利な社会となっています。しかし，その反面ひとたび情報システムに障害が発生した場合の影響は，ネットワークの拡大に比例して大きくなっています。

このため，地球時代の情報化においては，最低限のセキュリティ対策を各国がレベルをそろえて実施しなければ，社会の安定は得られません。情報システムをめぐるセキュリティ上の問題は，これまでセキュリティ対策の弱い部分で発生しており，したがって，ネットワークで接続された場合は，その影響はセキュリティ対策の十分な情報システムにまで及ぶことにもなります。

いまや，情報システムのセキュリティについては，局地的な対応では限界があり，地球時代の情報セキュリティを関係各国が共同で検討しなければならない時代に来ています。このような認識のもとに，世界初の試みとして日・米・欧のセキュリティ問題の指導的立場にある専門家が一同に会し，地球時代の情報セキュリティ対策のあり方を検討いたしました。

本シンポジウムは，日・米・欧のセキュリティ問題の実態を政策面，および実務面の双方から明確に把握して問題点を探り，相互に研鑽するとともに，今後の協力関係等を模索して，地球情報化の環境整備および安定化に向けて活発な報告，議論が行なわれました。

本誌では，シンポジウムの各セッションにおける講演等の概要を取りまとめ，ご紹介いたします。

開催日時　1991年10月17日～18日
場　　所　新高輪プリンスホテル
　　国際館パミール
参加人員　約1,000人
主　　催　(財)日本情報処理開発協会
後　　援　通商産業省，総務庁，外務省
　　アメリカ大使館

シンポジウムプログラム

第1日目　10月17日（木）

講　演　テ　ー　マ	講　師
開会挨拶	(財)日本情報処理開発協会 会長　影山　衛司
祝　辞	通商産業大臣　中尾　栄一
基調講演Ⅰ 21世紀へ向けてのセキュリティ戦略	ソロモン　J．バックスバウム
基調講演Ⅱ セキュリティ対策への政府と民間の役割	パトリック　R．ギャラガーJr.
基調講演Ⅲ セキュリティ対策に関する国際協力へのＯＥＣＤの対応	マイケル　D．カービー
基調講演Ⅳ 国際情報化社会とセキュリティ構造の変化	関本　忠弘

第2日目　10月18日（金）

第1セッション	第2セッション	第3セッション
セキュリティ関連政策	コンピュータウイルス	企業におけるセキュリティ対策
日本のセキュリティ政策 中村　薫	日本におけるウイルスの現状と対策 棟上　昭男	セキュリティ対策の新段階 平栗　俊男
米国のセキュリティ政策 ビル コルビン	米国におけるウイルス、ワームの動向と今後の見通し フレデリック B. コーエン	ＩＢＭのセキュリティ方針と対策 ウィリアム A. ホワイトハースト
英国のセキュリティ政策 マイケル R. ジョーンズ	欧州におけるウイルスの動向と新しい傾向 クラウス ブルンスタイン	欧州企業のセキュリティ対策 アラン スタンレイ
パネルディスカッション	パネルディスカッション	パネルディスカッション

第1日目

基調講演 I

「21世紀へ向けてのセキュリティ戦略」

ソロモン　J.バックスバウム
AT&T　Bell研究所　筆頭副社長

1．情報セキュリティの重要性

今日，情報セキュリティは，世界的な重要性を持つようになっている。それは，ネットワークがグローバルになっており，ユーザである企業も国際的な活動をするようになっており，サプライヤもグローバルにリソースを供給しているからである。そして，コンピュータをベースとしたサービスが普及するにつれて，情報セキュリティがわれわれ1人1人に直接影響を与えるようになっている。また，国家レベルにおいても国際通商や安全保障に影響を与えている。

2．アクセスコントロールの困難性

コンピュータが大量に普及し，相互に接続されているという状況の中では，アクセスを十分にコントロールしなければならない。しかし，広域化しているだけコントロールも従来に比べて困難になっている。従来のコンピュータ環境におけるセキュリティと比べた場合，コンピュータやデータなどの，リソースの間に壁をつくることはもはや不可能である。従来とは基本的に全く別の形でセキュリティを考えなければならないということである。すなわち，セキュリティシステムにより，データ通信環境における多くの要素間のアクセスをコントロールしなければならない。

3．何を護るべきか

情報セキュリティで護るものは，情報の機密性，ソフトウェア，コンピュータ，情報とソフトウェアの集合体としてのインテグリティ，コンピュータやネットワークのリソースとしての可能性，およびビジネスの方法論に関する能力などである。そして，護るということは，侵入を防止する，もし防止できなかったときは検知し，事実関係を把握することである。そして，関連する好ましい行動として，侵入から回復を図り，最低の中断でもって機能が継続できるようにすることである。

情報セキュリティは，ネットワークを利用している人々の行動に依存している。これらの人々は，情報セキュリティの手続きを認識する必要がある。彼らには，何ができ，何ができないか，それはなぜか，を知らせなければならないし，そのような手続きを実行させるための動機を与えなければならない。

基調講演 II

「セキュリティ対策への政府と民間の役割」

パトリック　R.ギャラガー　Jr.
ナショナル・コンピュータ・セキュリティ・センター，ディレクタ

1．セキュリティ登場の背景

初期のコンピュータでは，そのユーザは設計者または操作の熟練者であって，しかもスタンドアロンであるため外部からのアクセスに対しては安全であり，仕事の効率向上に有益であると認識されていた。このためユーザの急増，ニーズの多様化，利用形態の変化等，予想もしない事態が発生した。かかる状況においてシステム管理者等に，ある懸念が生じた。1つは，システムにアクセスしている者は誰かであり，また，その者はいかなる特権，権利を保有しているか？である。2つめは，オペレータは暗黙的に信頼できるか？ということである。しかしながら，こういった懸念はごく一部で持たれるにすぎなかった。

2．連邦政府のセキュリティ対策と民間との連携

前述の状況により，政府とりわけ国防総省関係の研究は刺激を受け，コンピュータに対する種々の試みを行った。これによりいくつかの問題が発見されたが，解決は個々にではなく，組織的・系統的になされるべきであることがわかった。これを受け，1982年に現在のNCSCが設立され，基準の作成と評価および他省庁との調整役としての活動が開始された。コンピュータセキュリティという概念を構築する土台としてオレンジブックが作成された。

NCSCはNIST(旧NBS)との連携を開始した。1987年コンピュータセキュリティ法の成立により，この2機関の管轄がはっきりするに従い，この連携は深くなった。この法律は，一方の機関は不特定ユーザーを対象とし，もう一方は特定ユーザーを対象とするよう求めているが，両者同様の部分については，共同で作業を進めている。また，両機関は欧州でも議論を開始した。現在多くの人がセキュリティに関心を持っている。

3．今後の展望と施策

今後の基準には，インテグリティ，アベイラビリティを取り込む予定である。また，ネットワーク化にも対応すべきで，かかる問題を解決するには，技術力，政府および民間並びにユーザの協力が必要である。さらに，国際的な基準の統一，もしくは少なくとも基準に互換性を持たせること，評価方法も各国に互恵的に実施することが必要である。

コンピュータの世界では基準がなければプライバシー，秩序というものは守れない。したがって，われわれ専門家はセキュリティに関してユーザが容易に理解できるよう啓蒙，教育を続ける必要がある。

基調講演III

「セキュリティ対策に関する国際協力へのOECDの対応」

マイケル　D. カービー
OECD・ICCP情報セキュリティ専門家会議
議長

1．国際的な調和への障害

情報セキュリティ問題を扱うとき，次のような障害がある。第1に，情報技術はユニバーサルであるが，社会的な規制制度については全く国レベル，地方レベルである。第2に，多くの動きが国際制度に向けられているが，国際的な制度は非常に弱く，国，地方の問題に対して脆弱である。第3に，国際的な制度については，政治家，官僚がでてきてエゴが表れる。第4に，政治的指導者には，国内的には民主的な圧力がかかる。第5に，政治的なプロセスは，国内的にも国際的にも，流行や，空想や，偏見や，あるいは地域的な問題に対応する。第6に，国際的に情報セキュリティのような問題に対応する場合，まるで氷河の動きのように遅い。第7に，言葉及び文化の問題がある。第8に，富める国と貧困な国の南北問題がある。そして最近の新しい傾向として技術的な貧富の差もでてきている。

現代の情報技術は，官僚，法律家などは恐れをなすところであり，あまりにも専門的な問題である。特に情報セキュリティというテーマは，理解できないところであり，ましてや適切な規制など難しいと考える人が多い。

2．国際ルールづくりの緊急性

情報セキュリティについての国際ルールづくりは，急を要していると思う。ネットワークによる相互作用は，他の事柄よりはもっと大きな影響を及ぼすからである。情報セキュリティがうまくい

かなかった場合，財産，生命，そして生活へのダメージが非常に大きい。

しかし，一筋の光明がある。それは，初期の国際的な努力，すなわち情報化の社会的な側面におけるガイドラインをまとめることに成功していることである。すなわち，プライバシーのガイドラインが，OECDの理事会の勧告という形式をとって，1980年9月に採択されたのである。現在，新たに設置された専門家会議で情報システムセキュリティのガイドラインを策定中である。

3．情報セキュリティの原則

第1の原則は，情報システムがアベラビリティ，コンフィデンシャリティ，インテグリティ，認証の尊重に基づいていることである。

第2の原則は，とられるべき措置はセキュリティのニーズに調和しなければならないことである。

第3は，フリーフロー(情報の自由な流れ)の原則である。

第4の原則は，適用可能なセキュリティ原則の実施に対して誰が責任をとるかという，責任の原則である。

基調講演Ⅳ

「国際情報化社会とセキュリティ構造の変化」

関本　忠弘

㈳日本電子工業振興協会　会長

1．情報化社会の国際化とボーダレス化

産業革命の後，情報革命が起こり，現在の情報化社会が到来しているのであるが，情報はこれからますます重要となるし，企業経営者にとって，人・物・金に続く第4の資源であるのは今や常識である。しかも，これからの社会を俯瞰するとボーダーレス・エコノミーということが言えるわけであり，その基盤に情報があり，情報システムがある。ボーダーレスを促進する通信衛星，国際的な企業展開，さらに家庭の情報化等，その原動力は情報システムである。

2．情報化社会におけるセキュリティ問題

セキュリティは，コンピュータのみでは十分でなく情報を送る通信ネットワークを含んで考える必要がある。情報を処理するコンピュータおよび通信ネットワーク，この2つが有機的に結合したシステムが大変重要となっている。かかるシステムにおける脅威，すなわち，マシン等の故障，過失による障害および故意の障害＝犯罪であるが，これら脅威に対するセキュリティを考慮する際重要なことは，機密性，完全性およびアベイラビリティ＝可用性である。機密性，完全性ではアクセスコントロールが必要である。アクセスに対する識別，アクセスの記録および適切な通報である。問題は可用性の継続であるが，詰まるところ抗堪性向上の施策＝回線の複ルート化etc.になる。加えて重要なことは，セキュリティに対して投資しなければならない，という意識の問題である。

3．今後の対応策

わが国におけるセキュリティ問題に対する取り組みは災害故障対策が重点であった。したがって今後の対応のポイントとしては，体制の整備，特

に監査体制の整備があり，次に研究開発，法制度に関しての国際協力の推進，さらには意識の改革＝倫理の確立が必要である。特に，3つめの人に関する問題が一番重要であり，セキュリティ問題の原点である。

情報社会においてはまさに人間というものが問われている。したがって，情報セキュリティの問題は，個々の権益の問題ではなく社会的な責任である，という認識に立って解決に努めていかなければならない。

第2日目

第1セッション：セキュリティ関連政策

講演I

「日本のセキュリティ政策」

中村　薫

通商産業省機械情報産業局情報処理振興課長

本講演の詳細については，本誌「寄稿・解説」欄に全文を掲載してあります。

第1セッション：セキュリティ関連政策

講演II

「米国のセキュリティ政策」

ビル　コルビン

米国航空宇宙局検査官

1．米国のセキュリティ問題の背景

連邦政府内には，議会，会計検査院(GAO)，行政管理予算局(OMB)，検査局長，商務省標準技術局(NIST)およびコンピュータのシステムセキュリティおよびプライバシーに関する諮問委員会等があり，各々の管轄において政府のコンピュータシステムを監督している。それほど連邦政府の運営は，コンピュータに依存している。このため，各省庁がシステム開発の際に準拠する法律・規制等は多数整備されており，これにはシステムを利用するユーザを規制する法律，プライバシーに関する法律，財務的なプライバシーの権利に関する法律，NISTの提供する各種標準およびNCSCのオレンジブック等がある。

しかしながら，多くの施策および法律等をもってしても，より良いセキュリティを達成しているとは言い難い。セキュリティに関する標準が実質的に少なく，評価・測定ができない。これは政府内のコンピュータシステムの管理者および監督者にとって，根本的な問題である。なぜなら，基準がほとんど無いため，システムの評価ができないからである。

2．セキュリティ環境の改善施策

現状のコンピュータセキュリティの全体環境を改善するための施策として，次のようなものがあろう。

(1) 適切なガイダンスおよびツールの提供

システムのマネージャまたは上位の意志決定者に適時かつ明確に提供する。特に，意志決定する際に具体的に使い得るものとして提供しなければならない。

(2) セキュリティのシステムへの取り込み

セキュリティをシステムのライフサイクル全ての側面に統合させる。セキュリティは担当者だけのものではなく，関係する全ての者に責任がある。

(3) プロセスを重視したセキュリティの強化

個々のセキュリティ上の違反および欠如を問題にするのではなく，組織全体としての施策の有無，各種の手続並びに基準の有無，そして，これら手続等によるリスクの認識の可否等に焦点をおいて，セキュリティを強化しなければならない。

第1セッション：セキュリティ関連政策

講演III

「英国のセキュリティ政策」

マイケル　R. ジョーンズ
英国貿易産業省セキュリティ担当マネージャ

1．英国貿易産業省の施策

貿易産業省(DTI)は，現在および将来の貿易に対するインパクトの観点から，情報セキュリティには国際的なアプローチが重要との認識に立っている。DTIは産業界の潤滑油的存在として，円滑な市場メカニズムのための施策を実行している。この際，円滑なメカニズムを阻害する要因として，基準，法律の未整備および情報不足が挙げられよう。

DTIも基準の確立の必要性からオレンジブックを参照したが，幾多の欠点から民間市場等への適用には支障があった。このため，DTIは新しいアプローチにより1989年，グリーンブックとしてセキュリティ製品の評価基準を公表した。この基準は，ドイツ，フランス，オランダにおけるITSEC策定作業の成果と歩調を合わせている。ITSECバージョン1.2は最近ECから公表された。この基準はプロダクト，システム両方および民間，軍事両部門を対象としている。

また，現在，英仏独蘭4か国によりITセキュリティ評価マニュアル(ITSEM)を開発中である。英国では，英国情報技術セキュリティ評価認証計画が発表された。この計画により市場の開放が促進されるとともに，認証されたセキュリティ製品が出荷され，ユーザおよびベンダー共にメリットが生まれるであろう。

また，ISO傘下の標準化活動であるが，国内を問わず国際レベルでも，標準の策定作業の推進だけでなく，調整作業の支援も行っている。さらにDTIは，セキュリティに関する認識の向上のための活動を行っている。

2．コンピュータ濫用法について

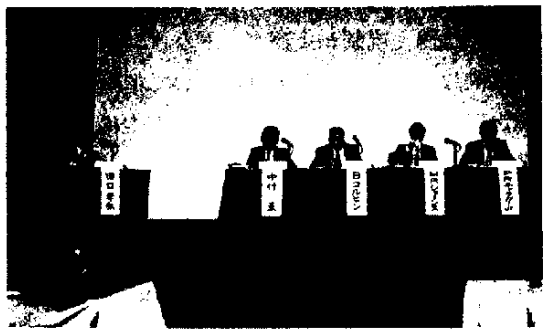
英国ではコンピュータ濫用に対してコンピュータ濫用法が制定されている。この法律の制定により3つの新しい犯罪類型ができた。1つは，興味本意のアクセス，次に認証のないアクセス，しかも意図的に重罪を起こすもの，最後に無許可によるプログラム，データ等の破壊，改ざん等である。

DTIは，この法律の適用状況を追跡しつつ，警察，電話会社，検察等関係部門と共に，コンピュータ濫用において鍵となる問題を明らかにする作業を行っている。立法に関する国際協調があれば，越境犯罪の場合に法の執行がやりやすくなる。

3．ECの活動

DTIは他国の代表と共に，ECによる情報セキュリティに関連する研究，開発及び計画を積極的に支援している。

第1セッション：セキュリティ関連政策
パネルディスカッション
コーディネータ　田口　孝弘
（日本電子計算機㈱　主幹）
パネリスト　中村　　薫
ビル　コルビン
マイケル　R. ジョーンズ
パトリック　R. ギャラガー　Jr.



1．主な論点

(1) 各国のセキュリティの現状と今後の問題点
(2) データインテグリティの評価基準における尺度について
(3) セキュリティに関する国際機関の設立について

2．パネリストの強調した点

(1) 各国のセキュリティの現状と今後の問題点

ギャラガー：従来，セキュリティの分野は秩序が不十分であり，1987年になって非軍事・軍事における責任の明確化がなされ，両者の協力の下，連邦基準の作成が開始された。このようにセキュリティでは，責任の明確化および基準の制定が重要であり，今後は基準を運用するための評価の実施と，そのための国際的な協調，さらには民間の役割の明確化が必要となる。

中村：刑法面における各国のノウハウ，セキュリティに関する基準の制定等，日本と諸外国との違いが明確になってきた。したがって，今後は国際協調の観点から基準の調和と相互認証のための評価基準の制定を行うために情報交換の場の設定，セキュリティの普及と啓蒙・教育が重要である。また，国際化に伴い，今後発展途上国への対策が重要になってくる。

コルビン：米国のセキュリティのインフラには，多数の法律・規制およびガイドラインがあるが，具体的なシステムの安全性について信頼性の高い測定方法はない。しかしながら監査中に多数の不具合が発見されており，それらの責任は明確にしなければならない。また，コンピュータの濫用，これを使った詐欺を防止する責任も明確にしなければならない。技術的な問題というよりは管理に問題がある。問題の解決のためには，国際的なコンセンサスが必要となっているが，ECのITSEC，米のTCSEC等があるが，基準は1つに統一することが望ましく，これらの作業を通してセキュリティのコンセンサスを地球的規模で明確にすべきである。

ジョーンズ：評価基準や標準，研究，開発，立法，啓蒙等の問題を取り扱う，情報セキュリティのための国際センターの設立は，メリットはあるであろう。しかしながら，技術的な対策は別にして，日常の情報システムの運用のためのガイドラインを作成・普及することの重要性を認識することが大事である。

(2) データインテグリティの評価基準における尺度について

コルビン：如何なる評価基準を作るにしてもインテグリティとアベイラビリティが主たる点であり，これを確保するには最初にマネジメント部門の改善が必要である。すなわち，全般的なシステムセキュリティの基準を規定し，マネジメント部門だけでなく，その他の部門でも取り上げ基準を参照し，マネジメント部門の効率性を測定してみることが肝要であり，これにより限定された評価は避けられる。

ジョーンズ：インテグリティを考える前に，十分なリスク分析がなされていなければならない。リスク分析により，脅威，脆弱性，リスクが明らかになり，適正な手段が採用され得る。しかしながら，リスク分析の手法はまだ完全ではない。

ギャラガー：インテグリティ，アベイラビリティどちらも概念の定義が難しく，最終的にはコンピュータをテストして，これがインテグリティを提供している能力である，と言えるようになれば良い。

(3) セキュリティに関する国際機関の設立について

ギャラガー：国際機関の設立は，研究の刺激となり，また相互の国際協調も促進するだろうが，機

関自体官僚的になると思われ，個人的には希望しない。各国内の機関が相互によく連絡をとりあえるようにすれば，国際機関の設置と同様の成果が得られると考える。

コルビン：個人的には国際機関の設立には賛成である。しかしながら，各国ではそれぞれ諮問委員会が政府に助言を行っており，その助言も国際レベルで採用できるか注意しなければならない。このため，1つの国際的諮問委員会の設立より現状の方が良い。

中村：日本がセキュリティに関する基準を設定するとき，欧米の基準が調和されていないことが問題である。したがって，セキュリティの問題は範囲が広く機関を作れば良いというものではないが，なんらかの国際的な情報交換の場は必要である。

3．結　論

情報社会の今後の発展のためには，情報セキュリティに関する評価を国際的な協調で実施することが非常に重要であり，また，かかる場におけるセキュリティ確立のための啓蒙活動・教育も忘れてはならない重要事項である。このため，情報の共有化，話合いの場として，ある種の機関を各国の中に設置するとともに，各国機関の交流が国際的なレベルにまで発展するよう活動しなければならない。今回のシンポジウムは，世界的なものとしては第1回であるが，今後の各国のセキュリティ対策の啓蒙として非常に有益と思うので，何らかの形で実施されることが重要である。

第2セッション：コンピュータウイルス

講演Ⅰ

「日本におけるウイルスの現状と対策」

棟上　昭男

情報処理振興事業協会　理事

1．IPAの活動について

IPA(情報処理振興事業協会)では，通商産業省のウイルス対策基準に基づき，ウイルスの届出機関になっており，ウイルス対策室を設置している。ここでは，主としてウイルスの現状分析，その対策等を検討している。また，ウイルスに感染していないかどうかをチェックするためのシステムの開発も同時に行っている。

2．日本の現状ならびに対策基準

コンピュータウイルスの問題は，日本でも近年パーソナルコンピュータが非常に普及してきたということもあって，徐々に被害が広がりつつある。このような状況に対処するため1990年からいろいろな施策が講じられてきた。日本で最初に大きな話題になったのは，1985年6月のPC-VANのウイルスである。その後，国としてもきちんとした対策基準を検討する必要が生じてきたため，1990年4月，通商産業省の告示としてコンピュータウイルス対策基準が出された。この基準は，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等から構成されている。たとえば，ソフトウェア管理の項では，一番最初には，「ソフトウェアの販売者または配布責任者の連絡先，バージョン，更新情報を入手し，信頼のできるソフトウェアを使用すること」ということが述べられており，一番最後の発生したときの事後対応ということでは，「汚染されたフロッピィは，破棄すること」と書いてあるが，重要なことは，「異常が発生した場合には，その現象を記録して，システム管理者に連絡する」ことである。また，発見されたウイルスは，届出機関に届けることが推奨されており，その届出機関にはIPAが指定されている。

3．コンピュータウイルス対策室

IPAのウイルス対策室は，活動が始まったばか

りで，準備期間を合わせてもまだ1年と少しの歴史であるが，今後は継続的に国内の被害状況の調査・分析を実施し，海外についてもその被害状況を組織的に調査していきたい。また各ウイルスの詳細解析および類型化ということが1つのテーマとなっており，それに基づいて，高度なワクチンを開発すると同時に，ワクチン以前の何かうまい防御システムを研究開発していきたい。

4．今後の課題

これからは，世界的に軍縮が行われ，古典的な意味の兵器があまり役に立たなくなってくる。しかし，情報システムに対するテロや破壊活動というのは，ますます可能性が高くなってきている。そのような意味でも，ウイルスの問題を始めとして，現在よりもさらに，情報システムの安全性と信頼性に対する問題意識とコスト意識を持つことが重要な課題となってくる。

第2セッション：コンピュータウイルス

講演II

「米国におけるウイルス，ワームの動向と今後の見通し」

フレデリック　B.コーエン

レードンプロジェクト社　ディレクタ

1．コンピュータウイルスの経緯

コンピュータウイルスの問題は，1984年に初めて発表された。それ以来各方面で研究がされてきたが，状況はあまり変化しておらず，現在のコンピュータ技術というのは，ウイルスに対して非常に弱いわけで，できるだけ強い防御策をしなければならないが，それでもまだウイルスに対して弱い部分が残る。コンピュータウイルスは，1987年頃から非常に広く伝染を開始し，電子メール等を通じて，アメリカ，ヨーロッパを中心にしてIBMメインフレーム等のネットワークに侵入してきた。そして，世界的にも非常に高スピードで拡散している。1988年には，世界中で何万というユーザが，ウイルスの影響を受けた。その当時，20種類のよく知られたウイルスが存在していたが，89年初頭には，ウイルスの数としては約800種類に増加した。

2．ワクチン

これを防御する1つの手段として，ワクチン接種が考えられる。ウイルスが，侵入しようとしてもワクチン接種によりこれを防ぐことができるが，たとえば100種類のウイルスに対して全てワクチン接種をするということは，非常に大変なことである。もしかするとプログラム自体が動かなくなる恐れもある。ワクチンの方がウイルスの影響よりも大きくて，それでプログラムがだめになってしまうことも考えられる。

3．良性ウイルスと悪性ウイルス

ウイルスには，良性のものと悪性のものの2種類がある。これを区別する場合に大切なことは，悪性ウイルスというのは，他の人に損害を与えるために開発するわけで，自分自身のIDを隠して捕まらないようにしている。しかし，ウイルスを開発するということは，考えてみると非常に知的な行為であり，このような知的エネルギーをうまくコントロールして良い方向に使うこともできる。たとえば，良性ウイルスとして，ビルコレクター，料金徴収者，というウイルスがある。これは，負債者に対して督促状を書いたり，電話をかけたり，あるいは借金の金額を計算したりする。また，メンテナンスウイルスというのもある。これは，システム内のガベージ，ゴミをウイルスが食べるものである。したがって，悪性のウイルスではなく，良性のウイルスをうまく使うためには，人々が自分自身のウイルスを書くという興味をうまく利用

することが大切である。良性ウイルス，役に立つ安全なウイルスを開発した場合には，たとえば表彰するとか，賞金を与えるとか，もちろん悪性ウイルスを開発した場合には，罰則を与えるということをはっきりさせてはどうかと思う。

第2セッション：コンピュータウイルス
講演III
「欧州におけるウイルスの動向と新しい傾向」
クラウス　ブルンスタイン
ハンブルグ大学　教授

1．ハンブルグ大学ウイルステストセンターの活動について

ウイルス被害に関しては，欧州あるいは米国では，いろいろ経験を積んでいるが，幸いにして日本では数百万のPCが有るにもかかわらず，欧米と比較するとはるかにその被害件数は少ない。ハンブルグ大学では，1988年にウイルステストセンターを設立し，ウイルスについての各種の実験を行っている。どのようにウイルスを分析し，どのようにウイルスを探知するかという技術に関しての研究を行っている。1989年には，エマジェンシー・レスポンス・チームがドイツ連邦政府のもとに設置され，それにも参加している。

2．欧州の状況

欧州において，いろいろなウイルスの被害が報告されているが，たとえば，1つのウイルスが，広域ネットワークの中で一度現れて，その後ネットワーク内に潜伏している場合や，メインフレームの中で複製したり，なかにはPCやワークステーション内で複製するものも出現している。また，UNIXのエリアで増殖するものもあり，今後，数年の間にこのケースが増えると思われる。

3．良性ウイルスについて

コーエン氏の良性ウイルスという考え方には反対する。ウイルスが，良性であるはずがないと思う。品質の高いプログラムというものは，著作権で保護されている。しかし，ウイルスで感染されてしまったプログラムに対しては，この著作権というのは存在しなくなる。プログラムの品質が，保証できなくなる。ウイルスが，メーカの権利，ユーザの権利も侵してしまうのである。

4．ウイルス対策

これらウイルスの被害を最小限にとどめる1つのアドバイスとしては，ペーパーコピーを必ずとるということである。一番最後の，一番重要なドキュメントといったものを読める状態で，そして，システムをイニシエーションしたとき，そして，プロパーなデータをきちんと取り出しておくことことである。ペーパーレス社会と言っているが，もしそのフレーズのとおりにしてしまったら，非常にリスキーな事態に陥ることが予想される。きちんとしたバックアップ・システムを常に考慮しておく必要がある。

第2セッション：コンピュータウイルス
パネルディスカッション
コーディネータ　上條　史彦(東海大学　教授)
パネリスト　棟上　昭男
フレデリック　B.コーエン
クラウス　ブルンスタイン
服部　武司
(NTTデータ通信第5開発担当部長)

1．主な論点

(1)　ウイルスの現状と対策
(2)　被害の報告義務ならびに国際的な情報交換の必要性

2．パネリストの強調した点

棟上：日本では，ウイルスに関連する被害の状況が諸外国と比較すると少し異なっている。パーソナルコンピュータが，かなり普及しているわりにはウイルスの被害は，欧米諸国ほどは広がってはいない。原因の1つには，専用ワープロやいわゆるオフコンと呼ばれているシステムの存在が考えられる。このような専用機器は，欧米諸国ではほとんど存在しない。大部分は，パーソナルコンピュータ上にパッケージソフトウェアを載せて処理を行っている。日本では，パッケージソフトウェアをベースにしたビジネスの広がりは，欧米と比べてかなり低い水準にある。その1つの要因はこれらの専用機器が広く利用されているためで，これが結果的にウイルスの爆発的な広がりを押さえているのではないかと考えられる。専用ワープロやオフコンは閉鎖的なシステムを作ることにつながり，その点ではあまり望ましいものではないが，ウイルスの被害を避けるためには役立っているのかもしれない。開放性と安全性を無理なく両立させるための方策を考えないといけない。

しかし今後，日本においてもウイルスは，ある程度増えることは間違いない。技術的な解決策として防御手段，検出手段，修復手段等を開発する必要がある。また，各種の運用基準等を整備することも重要な課題である。しかし，根本的には人の問題であり，教育に戻って初等教育や中等教育における道徳教育のレベルで，「情報倫理的」なことをきちんと教育していくことが，一番の基本になると思う。

コーエン：ウイルスの被害については，国の中に中央組織のような機関を設置し報告を義務付け，それを国際的に被害情報としてシェアすることが有効である。しかし，それと同時に守秘義務を確立する必要がある。そうしないと，必要以上の情報が漏れてしまい，本来の善意が生かされないからである。

ウイルスにおける犯罪性に関しては，慎重に検討すべきである。損害が，査定され，証明されたときに罰を与えるべきである。人権というのはきちんと保護されなければならない。ウイルスを作るのが良いか，悪いのかということであるが，ウイルスは，すぐに悪い方に向いてしまう可能性がある。しかし，あまり近視眼的になっても良くないと思う。

ブルンスタイン：将来，恐らく日本でもコンピュータウイルスは，増加することが予想される。IPAが，コンピュータウイルス対策室を設置したことは，よいタイミングだったと思う。そして，何か事故や被害が生じたとき，できるだけ早く探知して，早くそれを救済することが，重要である。ビジネス分野はもちろんのこと科学・技術分野に対し悪い影響がでない前に探知し，解決することが重要な課題である。

日本の場合は，欧米諸国と比較するとまだウイルスの被害は深刻ではないと思う。ウイルスの対策を講じるには，日本の場合十分時間があると思う。したがって，アーキテクチャの中にしっかりとした予防措置を組み込むことが重要である。その一方で，学校や職場におけるコンピュータ教育の中で道徳とか倫理についても教えるべきである。

服部：コンピュータウイルスが日本で欧米と比較してそれほど増加していない理由は，いろいろ考えられるが，まず第1は，日本と諸外国との文化の相違が上げられる。被害を出すこと自体恥であるという文化的背景がある。また，終身雇用制という会社に対する帰属意識が強いことも挙げられる。第2は，PCのアーキテクチャが非常に多彩であり，ウイルスが広範囲に感染しにくい。最後に，日本語の障壁がある。これは，現在起きている多くの被害が公共機関研究所とか大学とか，どちらかというと英語版のソフトウェアをそのまま

使う機会の多いところで多発している。防止策としては，早期発見，早期治療が原則で，万が一感染したときのために，必ずバックアップをしておくことである。さらに，対企業向けだけではなく，今後一般の家庭向けにもこれらの啓蒙活動が重要になってくると思う。

3．結論

コンピュータウイルスの問題は，確実に世界中に広がりつつある。そして，今回のシンポジウムで，世界のいろいろなグループが，ウイルスに対抗するための活動をしていることが確認できた。将来，これらのグループ間での情報交換を通じて，国際的にこの問題解決に当たることが急務である。

第3セッション：企業におけるセキュリティ対策

講演 I

「セキュリティ対策の新段階」

平栗　俊男

富士通㈱　常務取締役

1．情報セキュリティとは何か

情報セキュリティをめぐる脅威としては，自然災害，故障，過失，故意の4つがある。これらの脅威からハードウェア，ソフトウェア，データという資産を守ることが情報セキュリティ対策であると思う。

2．情報セキュリティにおける日本の特徴

①自然災害

日本と欧米の違いの1つは自然災害である。全世界で発生する地震の10%が日本で発生しており，また台風による風水害が多いのも特徴である。たとえば，1982年の台風における建物の破壊，流出，浸水は32万棟であり，通信回線の切断は1万8,000回線であった。また1986年には，破壊，流出，浸水が12万棟であり，通信回線の切断が9,000回線であった。そして1991年にも，最終的な集計がまだ出ていないが，台風により大きな被害が出ている。

②コンピュータ犯罪

日本ではコンピュータ犯罪の発生件数が少ない。これまでに認知された日本のコンピュータ犯罪件数(キャッシュカード犯罪を除く)は，警察白書(1990年版)によれば130件にすぎない。また，日本は10万人当りの盗難件数が1.4件となっており，一般的に治安の良い国といえる。

③大規模ユーザの実態

富士通の大型機ユーザの集まりでラージシステム研究会というのがあるが，このメンバーに対して1990年9月に実施したアンケート調査では，データバックアップについては(近く実施したいという回答までを含めると)95%が実施するとしている。しかし，データの暗号化については16%に過ぎなかった。

④ダウンからの早期回復

1977年から1983年までの間に，新聞で報道された日本の重要な社会システムのダウン件数は40件である。これら40件の回復までに要した時間は，30分以内が17.5%，30分～1時間以内が25%，1時間～2時間以内が25%，2時間～4時間以内が17.5%，4時間～8時間以内が10%，8時間以上が5%となっている。整理してみると，1時間以内に回復したものが42.5%で，2時間以内に広げると67.5%が回復している。この2時間が長いか短いかは議論のあるところであるが，可用性の確保にかなり力を入れていることを物語っていると思う。

3．今後の課題

情報セキュリティ対策を推進していくための今後の課題としては，次の3点が考えられる。

①コンピュータ製品に対する評価基準の必要性

②国レベルでのセキュリティに関する啓蒙活動の必要性
③リスク分析手法の確立

第3セッション：企業におけるセキュリティ対策講演II

「IBMのセキュリティ方針と対策」
ウイリアム　A.ホワイトハースト
IBMデータセキュリティ担当ディレクタ

1．情報セキュリティ重視への各種圧力

最近の情報システム環境において，セキュリティの重要性の認識が高まってきている。これには，いくつかの事項が挙げられる。

① 第1には，ハッカー，ウイルス，その他のコンピュータ犯罪のマスコミによる報道がある。

② 第2は，マルチユーザおよび企業間システムの成長により，企業が情報資産の価値の安全性に懸念を持ちはじめていることがある。

③ 第3は，監査人の係わりである。米国では，内部監査と，外部の監査人から成る監査委員会があるが，この両者とも情報システムを重視するようになってきている。

④ 第4は，政府の係わりが増えていることが挙げられる。米国では，政府が次の4つの分野で係わりを深めている。まずコンピュータ犯罪防止法の立法化，次に輸出規制，そして信頼性システムの評価基準，さらにプライバシー(個人データ)の保護である。

2．IBM社のセキュリティルール

IBMでは，1973年，「コーポレート・ポリシー・レター」を定め，プライバシー保護とデータセキュリティについてのガイダンスを規定した。これは，従業員および組織の記録についてのプライバシーの保護に関する枠組みを定めたものである。これはまた，基本的主義として，顧客が必要とするデータセキュリティを達成するにあたって支援することをIBMの責任として確立している。このポリシーは，情報マネジメント計画及び社内規定を通じて更に充実される。

3．セキュリティにはマネジメントの関与が不可欠である

技術の進歩はますます強力になり，相互接続されたシステムが増え，セキュリティ機能は，要求されるセキュリティレベルを達成するため，より重要になる。たとえば，認証，アクセスコントロール，データインテグリティ，システムインテグリティ，およびシステム管理などを損なってはならないということである。そして，これらの分野について，技術が重要な役割を果たし得る。しかし，それは情報セキュリティの要求を全て解決するものではない。情報システムは高度に相互依存した人間・装置・コミュニケーション機能の組合せであり，システムのあらゆる側面，たとえば人間・製品・政策・手続きなどの全てがシステムのインテグリティに貢献していることを忘れてはならない。

第3セッション：企業におけるセキュリティ対策講演III

「欧州企業のセキュリティ対策」
アラン　スタンレイ
欧州セキュリティフォーラム　ディレクタ

1．情報技術(IT)セキュリティは重要である

1980年代，多くの組織は変革を経験し，今や高度にITに依存している。しかしながらセキュリティのレベルはそのペースに追いついておらず，高まるリスクに晒されている。多くの組織にとって，ITリスクは他のビジネスリスクよりも大きい。

2．ユーザの意見反映が重要

欧州セキュリティフォーラムは，ITセキュリティの重要な問題点を明確にし解決するための組織であり，ユーザのグループである。もちろん，主要なメーカも含まれている。今日，ITセキュリティは，1つの企業だけで解決できる問題ではなくなっており，広範囲にながめて解決策を講じなければならなくなっている。これまでは，軍事部門がITセキュリティをリードしてきた。しかしビジネスの世界では，要求は様々であり，ユーザニーズを予測する必要がある。当フォーラムではそれを目的としている。具体的なトピックについて，国家や標準化機構に対して影響を及ぼすことも目的の1つに加えている。標準化活動には，ユーザからのインプットが欠けているという問題があるからである。

3．日本は一面で進歩

フォーラムでは，効果的な実施手順を作成することも目的としている。日本では，通産省がセキュリティ分野について基準を定めているが，欧州ではこの種の基準は存在しない。この点では，日本の方が欧州より進んでいるといえる。

4．ほとんどの組織には弱点がある

セキュリティポリシーについて調査をしたことがあるが，その結果は以下のようなものであった。

(1) 欧州では一般的にシニアマネジメントがITセキュリティに関心を示しており，セキュリティポリシーを持っていないと回答した企業はあまりなかった。しかし，取締役レベルでITセキュリティの責任を担っているかどうかについて質問すると，イエスという件数は大幅に減り，全体の約5割が体制を確立していなかった。

(2) セキュリティ管理の全般的なレベルについては，欧州は中間的だといえる。データ保護，セキュリティ監査およびレビューについては強く，セキュリティ管理，個人的なポリシー，セキュリティについての認識については弱いといえる。

(3) 最近，フォーラムではリスク分析についてのプロジェクトを終了した。市場では33の異なるアプローチが利用されていることが分かった。これは，しかしながら，リスク分析は，フォーラムの参加メンバーの17%しか実施していない。その理由は，現在のアプローチが複雑だからであろう。当フォーラムは，簡単に理解でき，容易に実施できるリスク分析手法を開発した。現在，システム開発にいかにリスク分析を適用していくかを研究している。

5．基本的な問題に注意が必要

ビジネスでのセキュリティにおいて基本的な問題として以下の5つがある。

(1)定義及び利点
(2))ユーザーの要求を理解する
(3)広く受け入れられるユーザーの手続
(4)セキュリティ組み込み製品
(5)教育及び訓練

第3セッション：企業におけるセキュリティ対策
パネルディスカッション
コーディネータ　　鵜澤　昌和
（東京家政学院大学　学長）
パネリスト　ソロモン　J.バックスバウム
ウィリアム　A.ホワイトハースト
アラン　スタンレイ
森　　紘一
（富士通㈱情報システム事業本部企画部長代理）

1．主な論点

(1) 評価基準の共通化の必要性について

(2) 情報セキュリティとコストの関連について

2．パネリストの強調した点

(1) 評価基準の共通化の必要性について

バックスバウム：技術面の合意よりも用語についての合意から着手すべきである。すなわち，コンフィデンシャリティ，インテグリティ，アベラビリティについて，第1段階では認識が一致しているが，第2，第3レベルでの定義の理解がどうなっているのか，そこから始めるべきである。

スタンレー：評価基準はそれによって特性を理解しようとするものであり，グローバルな基準がないとベンダーは複数の基準により複数の製品をつくらなければならなくなる。統一基準は，ベンダーにもユーザにも役立つものである。その成功のためには，ユーザーニーズに応えるものでなければならない。ITSECは現在ユーザーニーズを充分に反映しているとは言えない。最初から複雑なものを作るのではなく，まず基本的なものを確立し，徐々に修正し拡張するようすべきである。

ホワイトハースト：オレンジブックは米国で生まれ，ITSECは欧州の4ヵ国の作業によって生まれた。オレンジブックとITSECは相当に異なっているので，統一基準及び評価に対する相互の信頼が必要である。評価基準の策定にあたっては，用語の定義のレベルにおいてさえ合意することが難しい。たとえば，いくつかの作業部会で「インテグリティ」という一つの用語について多くの議論があったが，残念ながら未だに定義はできていない。

森：製品評価基準については情報セキュリティについて，日本は遅れており，米国や欧州に学び，早急に検討を進めていかなければならない。しかし，共通的な評価基準の必要性については，他のパネリストの皆さんと認識は同じである。

(2) 情報セキュリティとコストの関連について

バックスバウム：経験的には，セキュリティコストはオペレーションコストの数％に過ぎない。その数％が2％なのか3％なのか，あるいは10％なのかはわからない。しかし，10％を超えることはほとんど無い。適切なセキュリティコストは10％以下であろう。

ホワイトハースト：望ましいセキュリティコストとして予算の一定割合を固定的に設定するのは危険である。その理由は，アプリケーションは会社ごとに，あるいは会社の中でも部門ごとにそれぞれ違うわけだからである。必要とされるセキュリティは適用業務ごとに違う。適用業務には様々なリスクがあり，セキュリティは保護するためのコストと見合ったものであるべきである。

スタンレー：どれくらいセキュリティにコストをかけるべきか，組織はそれほど理解していないと思う。フランスでのある調査によれば，フランスでは，IT予算全体の20～30％，あるいはそれ以上をセキュリティに費やしている会社もあることがわかっている。ネットワークの二重化もセキュリティコストとして考えられるし，セキュリティをアクセスコントロールに限定して考えるべきではない。まず，アプリケーションが持っているリス

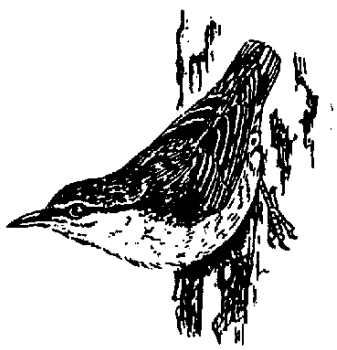
クを理解しなければならない。そして，それに基づいてコントロールを実施するということになる。

バックスバウム：ホワイトハースト氏，スタンレー氏の意見に同意する。セキュリティコストのレベルは，ケースバイケースで設定すべきである。それが設定できれば，オペレーションコストのどれくらいをセキュリティに費やすべきかの測定あるいは判断ができることになるといえる。

森：アプリケーションによりケースバイケースでセキュリティコストを設定するということに全く賛成である。また，富士通でも，そのような数字は持っていない。調査などでいろいろな数字があるようであるが，定義の仕方によっても数字は違ってくると思う。

3．結　論

討論した結果，国際的に統一された評価基準が必要という点においてパネリストの意見は一致した。また，情報セキュリティの概念が，コンフィデンシャリティ，インテグリティ，アベラビリティを確保することという点では完全に一致をみたが，具体的な評価基準づくりについてのアプローチについては若干の相違点がみられた。今後，これらの点について，日米欧で議論をつめていくべきとの認識で一致した。



情報産業界の動向

〈情報産業界の動向〉

自社内に抱えていたデータ処理をすべて外部に委託する企業が増える傾向にある。

例えば，Kodakは1989年に自社のすべてのメインフレームをIBMに売却，以後10年間すべてのデータ処理をIBMに委託する契約を結んだ。このように社内のデータ処理をすべて外部に任す方法は「アウトソーシング」と呼ばれているが，Kodak以外にも，多くの企業がすでにアウトソーシングを実施している。

アウトソーシングの利点としては，データ処理に掛かる莫大な経費の削減ができることが最も大きい。アウトソーシングは，企業と企業の契約であり，企業の系列化を進めることで，日本やドイツとの企業競争における戦略にもなるとも考えられている。

〈環境整備〉

EC委員会は，1993年初旬までにDigital Service Data Protection Directiveと呼ばれるプライバシー保護指令を策定する意向である。この指令は，当人の了解なく個人に関する情報を伝送・利用すること，および適切なプライバシー保護法を持たない国々に対する情報の伝送を禁じるもので，実際に施行されればヨーロッパでビジネスを展開しようとする各国に深刻な影響をもたらすと思われる。

その利点は，これまでヨーロッパ12ヶ国において，それぞれ独自の規制のもとに実施してきたビジネス様式の統一が可能になることである。EC域内の統一基準を決めることにより，相手国ごとの煩雑な業務処理がなくなるため，ミスを減らし，時間も短縮できるようになる。

このプライバシー保護指令のなかでも特に強い拘束力を持つと思われるのが第24条で，『適切な』プライバシー保護規制を持たない国に対し，ECは個人情報の流出を阻止することができるというものである。しかし，何をもって『適切』とするかについてはあいまいな点も多く，自由な物品・情報の流通を阻害し，保護貿易主義傾向に陥る危険性もはらんでいる。

〈エンドユーザ環境〉

ペンベース・コンピュータは携帯に便利であり，またデータ入力も簡単である。2年前アメリカのGrid System社とカナダのMicro Slate社が相次いでペンベース・コンピュータを発表した。これらのシステムはアプリケーションにある程度の制限があったが，セールスマン，配達やメンテナンスで戸外で働く人々には適当であるためよく使われるようになった。

現在のところオフィスワーカーはキーボード入力のパソコンを使っているが，ペンベースのパソコンを併せて使いたいという需要も潜在的に多いと見られている。そのためキーボードを取り外せるノートパソコンも作られている。

〈ソフトウェア〉

TI(Texas Instruments)社では，オブジェクト指向ソフトウェア開発技法を使って，まったく新しい製造プロセスを開発しようとしている。この

プロジェクトは米国国防省と1988年に1億1200万ドルで契約したもので，現在のものよりもずっと短期間かつ低コストで軍用カスタムチップを生産できる革新的な半導体製造設備を建設しようとするものである。

ハイテク兵器用部品の外国依存度の削減を狙う国防省は，最終的にオブジェクト指向を取り入れたチップ製造技術のかなりの部分を非軍事的分野に転換する計画を持っている。

〈教育・訓練〉

アメリカのビジネススクールでは，企業幹部の役員教育コースが人気を集めている。この役員教育コースの費用は高く，また，景気後退でアメリカビジネスは減速しているにもかかわらず，企業の役員教育にかける費用は増加している。

アメリカ企業は1950年頃より，役員教育に力を入れ始めており，現在は，日本，ドイツなどの企業との競争激化によりその必要性が特に高くなっていると考える企業が多い。特に現在人気が高まっているのは，企業とビジネススクールが共同で教育プログラムを作っていく方法で，カスタムプログラムと呼ばれており，高い割合で増加している。

〈電気通信政策〉

BTは，世界規模でのネットワーク・アウトソーシング・サービスの提供を開始した。この初めての新しいサービスは，各国に自社所有の基幹網を持つことによって，ノンストップショッピングを可能にし，また多国籍企業のネットワーク運用コストの削減をもたらすもので，BTの子会社であるSyncordia社(本社アトランタ)を通じ，専用音声・データ・イメージサービスが提供される。すでに契約した企業もある。

このサービスは，当初は28ヶ国70都市を光ファイバーケーブルで結んで提供される。

これに競合するサービスとしては，アメリカの大手通信事業者3社(AT／T，MCI，US Sprint)が提供している国際VPNサービスの一部が考えられる。

International Maritime Satellite Organization (Inmarsat：国際海事衛星機構)は，世界衛星移動通信システム計画(プロジェクト21)を発表した。これはポケットサイズの端末により，地球上のあらゆる場所での2地点間の通信を衛星を介して可能とするもので，Motorola社が発表したIridium計画と直接競合する。

Iridium計画は，低軌道衛星77機により全世界をカバーする予定であり，コストは21億ドルで1994年サービス開始，1997年よりフルサービスと予定されている。Inmarsatは各国コモンキャリアのネットワークのバイパスは考えていない。音声端末には陸上のセルラシステムとの互換性を持たせる考えである。

会員サロン

『コンピュータ社会に思う』

住友セメントシステム開発㈱

課長　酒井　潔

入社以来，既に12年の月日が流れようとしている。私は，学生時代，経営工学を専攻していたが，コンピュータが嫌いでしかたがなかった。大学院に進学してからは，人事・労務管理を専攻し，恩師からはアルコールを通じて，学問というよりも人間の心のあり方，人生哲学を学んだ。それが，新人研修後の配属発表を聞いて，私は愕然とした。当時の人事担当者の話では，3～5年位でローテーションがあるという話だったが，それが今だにコンピュータ関係の仕事をしている。

配属後，最初に担当した仕事は，会計システムのオペレーションだった。この頃は，カードパンチ機がまだ使われており，パンチャーがよく記号の“I”と数字の“1”を間違うので，プログラムが不正10進で異常終了した。私が会社で最初につけられたあだ名は，「アボートの酒井」だった。膨大なデータリストの中から“I”と“1”の違いを探すのが，私に託された最初の大仕事だった。「これが男のする仕事か」とよく腹を立てて，先輩に随分迷惑をかけた。

その私が，この仕事に生きがいを感じるようになったのは，ある書物で「コンピュータは原子力と同じである」という関本忠弘氏(現日本電気社長)の言葉に出会ってからである。こういう仕事をしていると，専門知識の洪水の中で機械の世界にどっぷりと浸ってしまい，自分が機械の一部である様な錯覚を覚える時間がある。コンピュータと言えども，あくまでも人間の使う道具である。時には，専門を忘れる事も必要ではなかろうか。

話は変わるが，私の娘は現在6才で，近所のある保育幼稚園に通っている。ここの教育方針が非常にユニークである。園長先生は東京大学の確か工学部を卒業された方であるが，今流行の英才教育は一切やらない。1才児から真冬でも半袖半ズボンで，子どもはとにかく一生懸命に遊ぶ。たとえ台風が来訪していても遠足(バス旅行)は中止にならないので，親としては心配になる事もあるが，私は入園させて良かったと思っている。それは，ここの教育方針が「子どもの創造性，社会性，独

自性の育成」であり，現代の人間に一番欠けているものを目指していると思うからである。

先日，松田武彦先生の「組織知能とシステム監査」という講演を拝聴させていただいた。「組織知能は，組織の人間知能と機械知能との交絡・集積・統合・複体であり，これを高度化させるのがシステム監査である」というのが松田先生の持論である。この講演の中で強調されていた事は，機械知能は急速な進歩を遂げているが，人間知能はあまり進歩していないという事であった。同感である。

コンピュータの急速な進歩によって，確かに人間社会は便利になったが，反面，人間の能力は退化している様にさえ思える。例えば，私も最近ほとんどの文書をワープロで作成し，便利な道具だと思うのだが，一方では漢字をよく忘れる様になった。今後，人間に計算力や記憶力が不要になる時代は間近である。専門的な分析力も，AIの進展に伴って，人間に不可欠な能力とは言えなくなりそうである。

そこで，先程の保育幼稚園ではないが，これからの社会では，人間の創造力・社会性・独自性の存在価値がますます大きくなっていく様に思えてくるのである。だが，おうむ返しの学校教育が全盛の中で，こうした能力を伸ばしていく事は難しいし，人間の創造力や独自性を伸ばす教育方法などというものがこの世に存在するのだろうか。これらの能力は，能力というよりも，むしろ人間の心に関わる部分が多いようにも思う。

社会性という面からもよく言われる事であるが，今後国際的な感覚の育成がますます重要になろう。衛星通信や海底回線等の普及により，情報ネットワークも国際的な広がりを見せている。日本の経済発展と相まって，コンピュータ関係者が諸外国の方々と関わる時間も飛躍的に増大している。最近の傾向を見ていると，国際社会の中で何か日本人は孤立化している様でさえある(経済支援等の打算的な面では頼りにされている様であるが)。

今後，我々が諸外国の風土・慣習・文化をもっと勉強すべきなのは当然だが，所詮知識を身につけただけでは何の役にも立たない。海外の人達との間で信頼関係を築いていけるかが問題なのであって，この問題はコンピュータ関係者にも不可欠の要素となろう。先日，日本情報処理開発協会主催の国際セキュリティシンポジウムに参加させていただいたが，日本は米国・欧州に比較してやはり立ち遅れている様である。コンピュータセキュリティの問題も行きつく所は，そこに関わる人間がこの問題にどれだけ心を向けられるかにかかっている。

私は以前に，「ニューサイエンスは物質的なものばかりでなく，人間の心をも対象にしている」という話を聞いたことがある。我々コンピュータに携わる人間も機械的・技術的な面ばかりでなく，そこに色々な形で関わってくる人間の心をしっかり見つめていかなければ，コンピュータ社会の発展はありえないのではないだろうか。

システム監査に関するアンケート結果より

Q貴社では，過去1年間(平成2年7月～平成3年6月)にシステムダウンが発生しましたか。

1	した	1,015件	58.6%
2	しない	691	39.9
無回答		25	1.4
計		1,731	100.0

・過去1年間にシステムダウンを経験したことがあるのは，58.6%と非常に多い。そして，発生率は，第二次産業(61.1%)の方が第三次産業(56.2%)よりも高い。

Q過去1年間に貴社で発生したシステムダウンは，障害原因別にそれぞれ何回発生したかご記入ください。(多重回答)

原因	回数	回答件数
自然災害	0.21回	126件
電源障害	0.42	290
空調等障害	0.17	124
回線障害	0.89	208
ハード・OS障害	1.73	611
ソフト障害	1.11	323
火災による事故・障害	0.00	1
人の悪意による事故等	0.01	2
オペミス等人の過失による事故	0.64	232
その他	0.09	27

(注1)システムダウンとは，システムの全面ストップもしくはそれに準じる障害と定義する。

(注2)1回の事故について原因が複数考えられる場合は，主要原因のみ記入

・過去1年間にシステムダウンを経験した1,015社のうち，987社が障害別の発生回数を回答している。この987社における1年間の1社平均総障害発生回数は5.25回になる。

・システムダウンを経験しなかった企業まで含めた回答企業総数1,703社の1年間の1社平均総障害発生回数は3.03回である。

・障害原因別に，昭和63年調査と同じ項目について比較してみると，過去3年間で明らかにシステムダウンの発生回数が減少していることがわかる。

Q貴社には専任のセキュリティ管理者がいますか。

1	いる	202件	11.7%
2	いない	1,519	87.8
無回答		10	0.6
計		1,731	100.0

・専任のセキュリティ管理者を置いているのは，11.7%と少ない。大多数の企業が専任のセキュリティ管理者を置いていないことが，セキュリティの重要性が叫ばれながら，なかなか対策が進まない原因の1つであると思われる。すなわち，セキュリティ対策が1つの業務として確立されていないといえる。

Q貴社には専任のセキュリティ担当者がいますか。

1	いる	288件	16.6%
2	いない	1,433	82.8
無回答		10	0.6
計		1,731	100.0

・専任のセキュリティ担当者を置いている企業も16.6%と少ない。管理者と担当者との関連をみると次のとおりである。

両方いる	171社(9.9%)
管理者のみいる	31社(1.8%)
担当者のみいる	117社(6.8%)
両方いない	1,412社(81.6%)

各部・センター活動状況

総務部

年末懇親会の開催

昨年12月18日(水)17時30分から霞が関ビルの東海大学校友会館において，恒例の年末懇親会を開催いたしました。

この懇親会は，当協会が昭和42年12月20日に設立されましたので，設立記念日にあわせ日ごろ協会にご支援，ご協力を頂いている方々をお招きし，感謝の意を表するために毎年開催しているものです。当日は，監督官庁の通商産業省をはじめ関連団体，企業，学校等から関係者多数のご出席がありました。

開会の挨拶をする影山衛司当協会会長

新技術調査研究室

当財団では，1990年代の第五世代コンピュータの後に来るものとして，21世紀を目指した革新的な情報処理技術について，その技術的シーズ，求められる機能，社会に与える影響など，多角的な立場から「新情報処理技術に関する総合的調査研究」を平成元年度から実施しています。

新情報処理技術のイメージは，従来のコンピュータでは不得意であった人間に近い感覚や，極めてあいまいな状況に対しても適切かつ迅速な対応をとり得る機能をもつものであり，従来のコンピュータの機能が人間の左脳に相当するものであったのに対し，初めて人間の右脳に相当する機能の実現を目指すものといえます。

これまで実施した2年間の調査研究では，新情報処理技術を特徴づけるキーコンセプトとして，「柔らかな情報処理」と「超並列超分散処理」の2つを提案するとともに，これらのコンセプトの内容をより明確化・具体化するための研究課題も明らかにしました。

平成3年度では，通商産業省の新情報処理技術開発調査研究委員会の下部機構として，当協会にワークショップ実行委員会(委員長：甘利俊一東京大学教授)，制度検討ワーキンググループ等を設置し，新情報処理技術推進のための基本計画の策定，新機構の組織や運営方針等についても検討を行っています。

第1回ワークショップ

平成3年11月5日(火)～8日(金)

横浜プリンスホテル(神奈川県横浜市)

参加　100名(うち海外9か国28名)

第2回ワークショップ

平成4年3月2日(月)～3日(火)
ホテルニューオータニ(東京都千代田区)
参加　99名(うち海外9か国14名)

調査部

1．コンピュータ利用状況調査

第24回コンピュータ利用状況調査および第21回オンライン化調査を実施しました。全国の40業種，4,467事業体を対象に，11月初旬にアンケートを郵送し，12月下旬までに1,049件(内オンライン化企業940件)の有効回答を得ました。

本調査は，コンピュータ部門の経費，要員数，派遣要員の費用単価等，長年にわたり，継続して調査しているもので，とくに5年後の規模の予測値，安全対策のレベル化等，当協会独自の調査方式にて分析し，関係者に資料として提供し，高い評価をいただいております。

今回の調査では，コンピュータに接続して利用する通信回線の項目にINSネット64，1500の2種類の回線を加えて，通信回線の全容をさらに把握できるようにしました。

本調査の結果は，5月発刊予定の『情報化白書1992』に例年どおりその概要を載せるとともに，当協会の報告書としても作成する予定です。

2．情報化白書1992年版の編集

発刊以来26冊目にあたる「情報化白書1992年版」の編集作業を現在行っています。

1992年版は総論と各論の2本柱で構成されていますが，その年の情報化の全般的トレンドを捉え，読み物の形で解説する総論の今回のテーマは，「人間そのものを重視した人間のための情報化」，すなわち「人間中心(anthropocentric)の情報化」です。情報化の最近のトレンドとして「人間あるいは生活を重視した情報化」が実感として問われている今日，21世紀を迎える前に考えておきたいテーマであると思います。

各論は，情報化の各分野について最新動向をとりまとめています。

発行は5月中旬の予定です。

3．海外調査，国際交流等

海外調査

当協会では，海外の情報処理の状況を把握するために，調査員を派遣し最新の動向を調査しています。このほど，アジア諸国における情報化の現状等について調査をいたしました。

①タイ，香港
- 期　日：平成3年12月8日～14日
- 訪問先：タイ(タイ電話公社，タイ・日経済技術振興会ほか)
  香港(TRADE LINK，職業訓練局ITトレーニングセンターほか)

②中華民国
- 期　日：平成3年11月27日～12月1日
- 訪問先：I.I.I. (Institute for Information Industory)ほか

③シンガポール
- 期　日：平成3年12月2日～7日
- 訪問先：National Computer Boardほか

日独情報技術フォーラムの開催

第7回日独情報技術フォーラムを次のとおり開催しました。
- 期　日：平成3年11月5日～7日
- 会　場：経団連会館　国際会議場ほか
- 概　要：
  両国政府並びに議長の挨拶
  基調講演Ⅰ　㈱ソルテック筑波研究所
  所長　阿刀田伸夫

基調講演II　University Stuttgart
Prof. Dr. Werner Frank

3分科会　ニューメディア，コンピュータ，半導体における発表と意見交換

ニューロコンピューティング・スペシャル・ワークショップ

・参加者：日本側74名，ドイツ側53名
合計　127名

国際交流

訪問者の受入れ

・平成3年10月14日
大韓民国　韓国電子通信研究所
：日本の情報産業，情報化白書について

・平成3年11月25日
大韓民国　韓国能率協会研修団
：日本の情報産業，データベースの現状について

・平成4年1月13日
中華民国　I. I. I. (Institute for Information Industory)
：日本の情報化の現状，情報処理技術者の育成について

・平成4年2月24日
大韓民国　情報産業標準院
：日本におけるEDIの概況

・平成4年3月6日
ドイツ　シーメンス
：JIPDECの研究開発等

Japan Computer Quarterlyの発行

日本の情報産業をさまざまな角度から取上げ，年4回英語で紹介しています。平成3年度は以下のテーマを取上げ発行しました。

No.86：VANサービス
・日本のVANサービスの現状
・業界VANの事例紹介
①プラネット
②JD－NET
③紙・パルプ流通VAN

No.87：ワークステーション
・日本のワークステーション
・ワークステーションの導入事例
①オムロン㈱における事例
②NTT研究開発部門における事例
③三菱電機㈱における事例

No.88：情報処理関連試験の紹介
・情報処理技術者試験
・マイクロコンピュータ応用システム開発技術者試験
・中小企業診断士試験
・データベース検索技術者試験

なお，No.89は新情報処理技術の動向を紹介する予定です。

4．普及振興

コンピュータ・トップセミナーの開催

平成3年度第2回のトップセミナーを1月29日～31日の3日間にわたって開催しました。23省庁から24名の幹部職員が参加し，パソコンを使用したコンピュータ実習，情報処理の基礎，情報化の動向等について2泊3日の集中研修を行ないました。

AI・ファジイ振興センター

1．次世代知識処理シンポジウム

日　時：平成4年1月31日㈮
9：20～17：00

会　場：機械振興会館B2ホール

テーマおよび講師

・基調講演：「AIパラダイムと知識」

東京大学教授・先端技術研究センター

センター長　大須賀節雄

・招待講演：「論理と知識」

㈶新世代コンピュータ技術開発機構　研究所

所長　淵　一博

・招待講演：「自然言語と知識」

京都大学教授・工学部電気工学第二教室

長尾　真

・報　告：大規模知識ベースに関する調査研究

－語彙知識から世界知識へ－

㈱日本電子化辞書研究所

研究所長　横井　俊夫

・パネルディスカッション

「次世代知識処理技術はいかにあるべきか」

コーディネータ

㈱日本電子化辞書研究所

研究所長　横井　俊夫

パネリスト

京都大学工学部情報工学科

助教授　西田　豊明

㈶新世代コンピュータ技術開発機構　研究所　第7研究室長　新田　克己

㈱東芝　総合研究所情報システム研究所

所長　河田　勉

日本電信電話㈱基礎研究所情報科学部

主幹研究員　後藤　滋樹

通商産業省機械情報産業局電子政策課

課長補佐　佐伯　俊則

2．講演会「ファジイ技術とその応用」

日　時：平成4年1月30日㈭

13：00～17：00

会　場：八丁堀シャンテ(広島市中区八丁堀)

テーマおよび講師：

・ファジイ技術とは：

九州工業大学工学部

教授　村上　周太

・ファジイ技術の応用事例

オムロン㈱ファジイ推進センター

マーケティング課長　高田　邦雄

3．講演会「ファジイ技術とその応用」

日　時：平成4年2月13日㈭

13：00～17：00

会　場：富山市高田

㈶富山技術開発財団富山技術交流センター

テーマおよび講師：

・ファジイ技術とは

金沢大学機械システム工学科

助手　田中　一男

・ファジイ技術の応用事例

－ファジイ技術の家電製品への応用例として－

松下電器産業㈱中央研究所

野村　博義

4．第3回CESP(ComonESP＊注)説明会

日　時：平成4年1月17日㈮

10：00～16：00

会　場：当協会中央情報教育研究所5番教室

講　師：㈱AI言語研究所第一研究室

主任研究員　中澤　修

(＊注　第五世代コンピュータプロジェクトで開発されたAI言語。ESP(Extended Self contained Prolog)をベースに，開発されたプログラミング言語。論理型言語Prologにオブジェクト指向をとり入れてAI言語としての機能を一層強化しており，知識情報処理システムの研究，試作，開発などに最も適しています。)

5．第2回CESPプログラミングセミナー

日　時：平成4年1月21日(火)～23日(木)

会　場：当協会AIオープンハウス

プログラム：

月／日	午　前	午　後
1／21	CESPの概要	CESPの基礎(1)
1／22	CESPの基礎(2)	CESPの応用(1)
1／23	CESPの応用(2)	CESPアプリケーションの拡張

講　師：

㈱ラデックス	黒澤　芳夫
ヒューマンシステム㈱	内藤　裕介
㈱オーキット	中間　正人

第3回は3月10日(火)～12日(木)に開催しました。なお，このセミナーのテキストを別途頒布いたしております。A4判126ページ　頒価3,000円(税込み)，送料260円。入手希望の場合は☎03(3432)9390まで。

6．第22回AI講演会

日　時：平成4年2月17日(月)
14：00～16：00

会　場：中央大学駿河台記念館

テーマおよび講師：

「知識システムのシステム化技術」

筑波大学大学院システム科学専攻
講師　寺野　隆雄

定　員：70名

7．研究用連続音声データベース(CD-ROM)の頒布

AI・ファジィ振興センターでは，連続音声を研究している方のために，㈳日本音響学会と協力し，研究用連続音声データベース(CD-ROM版)を作成いたしました。今回Vol. 1～3(全部で6種類作成予定)ができ，頒布を始めております。入手希望の場合は，☎03(3432)9390まで。

頒価　CD-ROM1枚につき3,090円(税込み)
送料250円

マイコンシステム技術者試験部

平成3年度の試験は，昨年11月17日(日)に全国9都市で実施されましたが，その試験結果が初級は1月15日に，中級は2月15日にそれぞれ発表されました。

初級試験は合格者1,543名，合格率30.2%(平成2年度は38.0%)，中級試験は合格者103人，合格率14.7%(平成2年度は16.6%)

合格者の平均年齢は初級が25.8才，中級が28.5才。最年少は初級が16才，中級19才。最年長は初級が65才，中級が54才でした。業務別，勤務先別，技術分野の傾向等は次表のとおりです。

また，合格者には同日付で合格証書が交付されました。

○勤務先別

勤務先		初級				中級			
		応募者	受験者	合格者	合格率	応募者	受験者	合格者	合格率
電算機・半導体製造又は販売企業		886人	638人	277人	43.4%	325人	233人	48人	20.6%
システムハウス		518	334	122	36.5	256	193	26	13.5
メカトロニクス関連企業		558	410	175	42.7	231	166	30	18.1
情報処理サービス企業等		1,110	664	211	31.8	418	270	20	7.4
上記以外の一般企業団体	製造業	999	753	336	44.6	415	296	45	15.2
	非製造業	456	320	121	37.8	164	107	17	15.9
官公庁		17	7	3	42.9	5	5	1	20.0
学校・研究機関		95	67	32	47.8	47	38	5	13.2
学生・生徒		2,309	1,866	245	13.1	95	70	11	15.7
不明		84	58	21	36.2	11	5	0	0
合計		7,032	5,117	1,543	30.2	1,967	1,383	203	14.7

○業務別

業務	初級				中級			
	応募者	受験者	合格者	合格率	応募者	受験者	合格者	合格率
研究・開発	2,206人	1,575人	699人	44.4%	1,084人	777人	138人	17.8%
情報処理	1,149	670	229	34.2	404	258	25	9.7
製造	621	464	186	40.1	192	132	17	12.9
保守・サービス	180	139	41	29.5	49	34	2	5.9
営業	75	55	18	32.7	29	19	2	10.5
調査・企画	17	10	2	20.0	6	5	1	20.0
教育	101	69	37	53.6	52	43	4	9.3
学生・生徒	2,309	1,866	245	13.1	95	70	11	15.7
その他	305	221	72	33.6	44	37	2	5.4
不明	69	48	14	29.2	12	8	1	12.5
合計	7,032	5,117	1,543	30.2	1,967	1,383	203	14.7

○技術分野の傾向

専門技術	初級				中級			
	応募者	受験者	合格者	合格率	応募者	受験者	合格者	合格率
①ハードウェア技術者	860人	624人	239人	38.3%	293人	214人	39人	18.2%
②ハードウェアよりの技術者	854	639	288	45.1	453	333	62	18.0
③ソフトウェアよりの技術者	929	675	326	48.3	542	379	66	17.4
④ソフトウェア技術者	1,487	901	325	36.1	491	314	22	7.0
小計	4,130	2,839	1,178	41.5	1,779	1,240	189	15.2
その他	2,464	1,939	318	16.4	149	113	10	8.8
不明	438	339	47	13.9	39	30	4	13.3
合計	7,032	5,117	1,543	30.2	1,967	1,383	203	14.7

中央情報教育研究所(CAIT)

中央情報教育研究所では，企業人を対象とした「高度情報処理技術者(SE)研修」およびソフトウェア技術者の主要な供給源であるコンピュータ関連の専修学校の情報処理教育担当者を対象とした「情報処理技術インストラクタ研修」ならびに企業内の情報処理技術者を指導・育成する指導者(リーダ)を養成するための「企業内リーダ養成研修」の3種類の研修事業を実施しています。

このうち「企業内リーダ養成研修」は，特に，地域における情報化の活性化を狙いとして，そのために，まず，地域における企業内の情報処理教育を充実させようというもので，東京並びに全国各都市で実施しています。

当研修コースは，「実践型インストラクタ養成コース」，「コミュニケーション技法コース」，「問題発見・解決技法コース」，「ソフトウェア開発技法コース」，「プロジェクト管理コース」，「SE向け戦略的育成プラン作成技法コース」の6つのコースから構成されており，いずれのコースも課題演習が中心になっており，研修結果あるいは演習の成果物がすぐに実務に役立つように工夫されています。

例えば，SEやプロジェクトリーダのスキルとして，最近特に重要視されてきた「コミュニケーション技法コース」を例にとりますと，当コースは，全体で4日間のコースとなっており，コース内容は，情報収集を的確に行うための「インタビュー技法」，効果的な提案書等をまとめる「文書表現技法」，相手を上手に説得するための「プレゼンテーション技法」がVTR等を活用したグループ別ロールプレイングを通じて体得でき，コミュニケーション技法のノウハウが修得できるように，きめ細かな個別指導を主体としたものになっています。このため，受講後のアンケートでは，受講者の皆様からかなり高い評価をいただいています。

CAITでは，平成4年度におきましては，当研修コースにさらに「コンサルティング技法コース」を新設し，7つのコース体系で実施することにしています。

情報処理技術者試験センター(JITEC)

1．平成3年度秋期情報処理技術者試験の合格者について

平成3年10月20日に実施した秋期情報処理技術者試験は，第2種は12月10日，システム監査，特種，オンラインは1月28日に合格者を発表しました。試験区分別の合格者等は以下のとおりでした。

①合格者数等

	システム監査	特　種	オンライン	第2種
応募者数(人)	11,355	33,293	45,456	246,542
受験者数(人)	6,016	16,881	22,858	157,446
合格者数(人)	422	600	1,757	27,857
合　格　率(%)	7.0	3.6	7.7	17.7
累計合格者数(人)	2,314	12,625	3,923	287,354

②合格者平均年齢

システム監査	35.6歳
特種	30.6歳
オンライン	28.4歳
第2種	22.6歳

③女性合格者数

システム監査	22人
特種	40人
オンライン	66人
第2種	4,765人

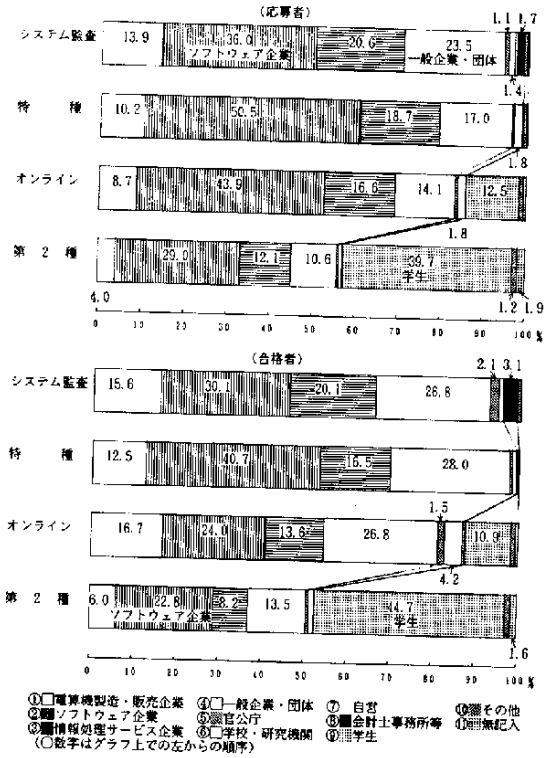
④試験地別合格者数

試験地		システム監査	特種	オンライン	第2種
札幌		4 (6.5)	6 (2.1)	21 (3.2)	831 (17.0)
帯広		0 (0.0)	0 (0.0)	0 (0.0)	47 (11.5)
青森		2 (25.0)	0 (0.0)	3 (5.4)	133 (15.4)
盛岡		0 (0.0)	3 (7.9)	7 (7.1)	100 (10.4)
仙台		2 (3.4)	3 (2.1)	21 (5.9)	696 (15.1)
秋田		0 (0.0)	0 (0.0)	2 (3.2)	94 (13.1)
山形		0 (0.0)	0 (0.0)	0 (0.0)	98 (16.2)
郡山		0 (0.0)	0 (0.0)	3 (4.6)	112 (13.0)
水戸		4 (5.3)	9 (3.4)	18 (6.1)	457 (16.7)
宇都宮		2 (9.5)	3 (3.9)	10 (5.6)	346 (15.4)
前橋		1 (3.3)	4 (3.4)	12 (5.5)	402 (15.6)
東京	埼玉	( )	0 ( )	0 (0.0)	701 (17.7)
	千葉	0 (0.0)	( )	0 ( )	833 (20.2)
	東京	270 (7.9)	338 (3.8)	995 (9.8)	6,323 (19.8)
	八王子	( )	( )	( )	683 (22.3)
	横浜	( )	0 (0.0)	0 (0.0)	2,269 (21.0)
	厚木	( )	( )	( )	435 (19.0)
	小計	270 (7.9)	338 (3.8)	995 (9.8)	11,244 (20.0)
新潟		5 (12.2)	9 (6.0)	31 (7.0)	603 (20.4)
長野		2 (4.9)	6 (5.0)	12 (8.6)	191 (13.1)
甲府		1 (9.1)	1 (2.5)	1 (1.2)	87 (13.4)
静岡		3 (5.8)	6 (3.9)	28 (7.7)	444 (14.8)
名古屋		23 (7.2)	36 (3.5)	115 (5.5)	2,237 (16.7)
豊橋		2 (10.0)	2 (2.5)	13 (7.1)	283 (15.7)
富山		2 (3.7)	2 (1.7)	16 (11.8)	203 (16.1)

試験地		システム監査	特種	オンライン	第2種
金沢		0 (0.0)	7 (4.6)	6 (2.9)	285 (17.7)
福井		0 (0.0)	2 (2.7)	7 (5.4)	126 (13.8)
大阪	京都	10 (7.4)	16 (4.5)	48 (11.7)	616 (19.0)
	大阪	56 (6.2)	87 (3.7)	189 (7.5)	2,985 (16.9)
	神戸	9 (5.2)	20 (3.4)	34 (6.0)	683 (19.8)
	小計	75 (6.2)	123 (3.7)	271 (7.8)	4,284 (17.6)
姫路		( )	( )	( )	127 (10.5)
米子		1 (7.7)	1 (2.1)	8 (8.6)	163 (15.3)
岡山		2 (3.3)	11 (4.2)	13 (4.5)	422 (16.7)
広島		8 (7.7)	7 (2.3)	33 (4.2)	895 (18.2)
山口		1 (6.7)	0 (0.0)	5 (6.6)	152 (14.9)
高松		0 (0.0)	2 (2.3)	14 (9.2)	216 (16.5)
松山		0 (0.0)	3 (3.8)	13 (9.6)	186 (13.5)
高知		0 (0.0)	0 (0.0)	5 (5.3)	92 (15.8)
福岡		6 (4.3)	10 (2.3)	33 (4.3)	894 (17.9)
北九州		2 (6.1)	1 (1.0)	7 (2.8)	295 (13.5)
佐賀		1 (10.0)	1 (4.2)	2 (3.8)	89 (12.0)
長崎		0 (0.0)	0 (0.0)	1 (1.7)	145 (15.6)
熊本		0 (0.0)	1 (1.3)	9 (6.7)	223 (15.8)
大分		1 (3.1)	3 (2.4)	7 (3.2)	217 (18.7)
宮崎		1 (33.3)	0 (0.0)	5 (5.9)	142 (14.9)
鹿児島		1 (11.1)	0 (0.0)	4 (2.8)	209 (17.9)
那覇		0 (0.0)	0 (0.0)	6 (6.5)	87 (10.8)
全国		422 (7.0)	600 (3.6)	1,757 (7.7)	27,857 (17.7)

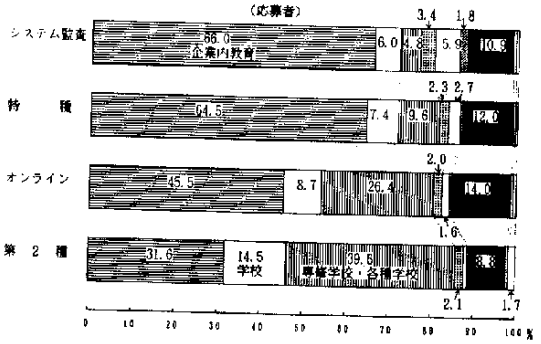
合格者数欄の下段（ ）内数字は合格率（合格者数／受験者数：%）

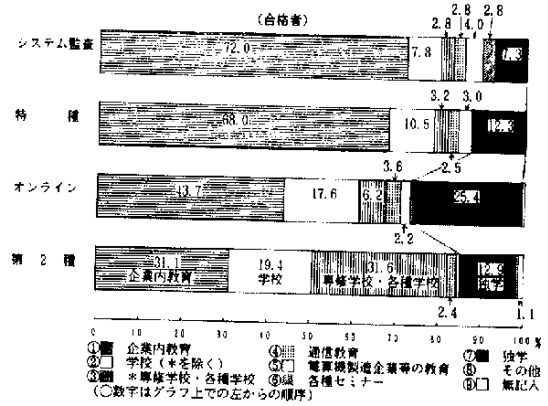
勤務先別 応募者・合格者 構成比（平成3年度 秋期）



①□電算機製造・販売企業 ④□一般企業・団体 ⑦ 自営 ⑩▒その他
②▒ソフトウェア企業 ⑤▒官公庁 ⑧▒会計士事務所等 ⑪▒無記入
③▒情報処理サービス企業 ⑥□学校・研究機関 ⑨ 学生
（○数字はグラフ上での左からの順序）

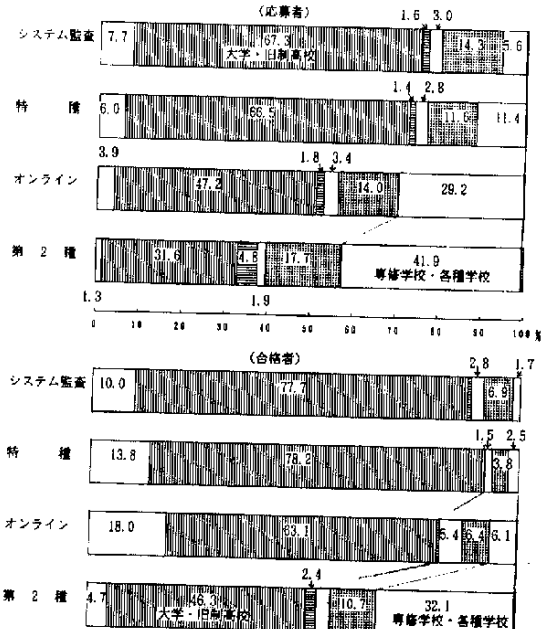
研修先別 応募者・合格者 構成比（平成3年度 秋期）
（情報処理関係）





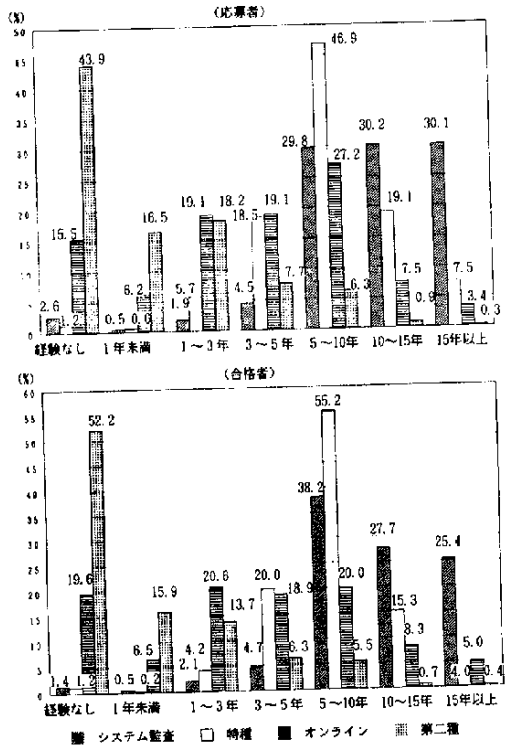
①▒ 企業内教育 ④▒ 通信教育 ⑦▒ 独学
②□ 学校（＊を除く） ⑤□ 電算機製造企業等の教育 ⑧ その他
③▒ ＊専修学校・各種学校 ⑥▒ 各種セミナー ⑨□ 無記入
（○数字はグラフ上での左からの順序）

最終学歴別 応募者・合格者 構成比（平成3年度 秋期）



（注）最終学歴には在学中も含む
①□ 大学院 ④□ 高専 ⑦▒ 小学校
②▒ 大学・旧制高校 ⑤▒ 高校・旧制中学 ⑧□ 専修学校・各種学校
③▒ 短大 ⑥▒ 中学 ⑨▒ その他
（○数字はグラフ上での左からの順序） ⑩▒ 無記入

経験年数別 応募者・合格者 構成比（平成3年度 秋期）
（情報処理関係業務の業務経験年数）



2．平成4年度春期情報処理技術者試験の応募状況について

平成4年度の春期試験の応募状況が明らかになりました。応募者総数は，303,833人(前年比11%増)，うち，1種は109,298人(前年比12%増)，2種は194,585人(前年比10%増)でした。

春期の試験は，4月19日(日)に全国47都市で一斉に実施されます。

産業情報化推進センター(CII)

1．OSIオブジェクトの登録・管理

従来の通信では，端末識別情報，アドレス情報，データ構造，通信方式などの通信に必要な情報を，利用するネットワーク・アーキテクチャで独自に定義し管理していました。OSIによる通信では，通信する当事者間で共通に認識しなければならないこれらの情報をオブジェクトと呼び，オブジェクトの定義や体系化，識別子の付与を一元的に登録・管理(オブジェクトの登録・管理)することが，ISOやCCITTで同意されています。

オブジェクトの登録・管理は，その性格からすべてを国際的に唯一の機関で行うことが最良ですが，それは実際的ではないので国レベルのオブジェクトについては，その登録・管理を各国に委譲する仕組みになっています。わが国では，日本工業標準調査会(JISC)がISO系の国内登録機関として権限を委譲されています。

産業情報化推進センターでは，このOSIオブジェクトの登録・管理に係る国内登録機関としての業務をJISCから移管され，平成3年3月より業務を開始し，組織と国内標準の登録・管理を行っております。現在，組織については，42の会社からの組織の登録申請を受けて組織登録番号とオブジェクト識別子を付与し登録・管理しています。また，国内標準については，登録申請を受けた4件について審査しているところです。

2．業界システム等の調査および構築支援

①情報化動向調査

EDIにおいて重要な役割を果たすVANの実態について，各種業界VANおよび地域VANの実態調査を行ったほか，情報ネットワークサービス事業の実態やEDIの利用状況等についても，主として利用者の立場からアンケート調査を実施しています。

また，業界共同ネットワークの実態と動向について，プラスチック日用品業界，自動車部品業界を対象に調査を行っています。今後は，他業界に

ついても情報化動向調査を行う予定です。

②業界システムの構築支援

中立的な立場から，個別業界，業際間のシステム構築における支援を進めており，平成2年度より本稼働を開始した機械工具業界の機工VANシステムの運営支援を行ったほか，管工機材商業界の業界VAN構築の支援を行っているところです。また，電子機器業界のEDI標準(EIAJ標準)の改善と普及，同業界の電線業界とのEDI検討，石油化学業界と商社とのEDI検討の仲介を務めています。

3．産業界のシステム構築のあり方に関する調査研究

本調査研究では，産業界におけるEDIおよび情報ネットワークの動向，ニーズ等について業種，業態，地域等いくつかの視点からその実態を調査しています。本年度は，最近，中央大手主導の情報系列化に対する危機感を背景に，全国各地に広がっている地方の流通業者が結束して設立する地域VANについての実態を調査しました。この程その調査結果として「地域VANの動向調査報告書」(平成3年11月発行)を取りまとめました。

OSIに係る組織及び国内標準の登録状況について

通商産業省告示第502号に基づき，平成3年3月1日より当協会を正式な国内登録機関としてスタートしたOSIに係る組織及び国内標準の登録状況は次のとおりです。

1．組織の登録

登録を完了した組織は次表のとおりです。

2．国内標準の登録

現時点で登録を完了した国内標準はありません。

但し，以下の情報オブジェクトについて，(財)情報処理相互運用技術協会(INTAP)からの登録申請を受理し，国内標準調整委員会による審査を終了しており，近々正式に国内標準として登録される予定です。

(1) MOTIS　JP1テキスト
(2) FTAM　INTAP－1　レコードファイル
(3) FTAM　INTAP－AS1　抽象構文
(4) FTAM　INTAP－TS1　転送構文

これらの情報オブジェクトについて，仕様の閲覧をご希望の方，あるいは異議・質問のある方は下記までご連絡下さい。

(財)日本情報処理開発協会 産業情報化推進センター
オブジェクト登録管理係　担当　関本，福井
☎　03-3432-9394
FAX　03-3432-4324

組　織　名　称	組織登録番号	オブジェクト識別子構成要素値
財団法人情報処理相互運用技術協会(INTAP)	100000	200000
富士通株式会社	100001	200001
日本アイ・ビー・エム株式会社	100002	200002
日本電気株式会社	100003	200003
シャープ株式会社	100004	200004
日本ユニシス株式会社	100005	200005
エヌ・ティ・ティ・データ通信株式会社	100006	200006
松下電器産業株式会社	100007	200007
沖電気工業株式会社	100008	200008
日本電信電話株式会社	100009	200009
株式会社日立製作所	100010	200010
三菱電機株式会社	100011	200011
株式会社東芝	100012	200012
富士ゼロックス株式会社	100013	200013
住友電気工業株式会社	100014	200014
株式会社アステック	100015	200015
株式会社日立情報システムズ	100016	200016
横河ディジタルコンピュータ株式会社	100017	200017
東京電気株式会社	100018	200018
住友海上火災保険株式会社	101001	201001
共栄火災海上保険株式会社	101002	201002
興亜火災海上保険株式会社	101003	201003
三井海上火災保険株式会社	101004	201004
大成火災海上保険株式会社	101005	201005
大東京火災海上保険株式会社	101006	201006
第一火災海上保険株式会社	101007	201007
千代田火災海上保険株式会社	101008	201008
東京海上火災保険株式会社	101009	201009
同和火災海上保険株式会社	101010	201010
東洋火災海上保険株式会社	101011	201011
日動火災海上保険株式会社	101012	201012
日産火災海上保険株式会社	101013	201013
日新火災海上保険株式会社	101014	201014
日本火災海上保険株式会社	101015	201015
富士火災海上保険株式会社	101016	201016
安田火災海上保険株式会社	101017	201017
朝日火災海上保険株式会社	101018	201018
太陽火災海上保険株式会社	101019	201019
大同火災海上保険株式会社	101022	201022
オールステート自動車火災保険株式会社	101023	201023
ジャパン・インターナショナル傷害火災保険株式会社	101024	201024
アリアンツ火災海上保険株式会社	101025	201025

以上，42組織が正式に登録を完了しています。

通商産業省　編

システム監査企業／安全対策実施認定事業所総覧

情報化の進展に伴い，コンピュータウイルスや個人情報保護，セキュリティ対策などの問題が発生し，システム監査の重要性が高まってきています。

また，このような諸問題を孕んだ状況の中で外部へ情報処理業務を委託する場合，安全対策を万全に行っている事業所かどうかということが選定の目安として挙げられます。

本書は，通商産業省が公表した「システム監査企業台帳」登録企業全44社および「情報サービス業電子計算機システム安全対策実施認定事業所」全170事業所を収録したものです。システム監査を行う際，また情報処理業務を外注する際の業者選定の目安として，ぜひご利用ください。

なお，ご注文は当協会で承っておりますので，ご希望の方は下記までFAXにてお申込みください。

B５版　204ページ　定価　一般 1,500円　会員 1,300円(税込み，送料別)

情報化月間20周年記念誌

わが国の情報化

－35のキーワードに見る現状と動向－

情報化月間は，昭和47年に情報化週間としてスタートしてから，本年で20周年を迎えました。本誌はこれを記念し，10月１日の情報化月間記念式典の折，来賓をはじめ関係者に記念として配布したものです。内容は，わが国の，情報化の現状と動向について35のキーワードを取上げ，わかりやすく解説したもので，読物としても，資料としてもご利用いただけます。

現在，残部を実費(1,110円，税込み，送料別)でお頒けしておりますので，入手をご希望の方は下記までFAXにてお申込みください。

＜お申込み先＞

〒105 東京都港区芝公園３-５-８

(財)日本情報処理開発協会　　TEL 03-3432-9384

調査部普及振興課　行　　FAX 03-3432-9389

平成４年３月　発行

JIPDEC ジャーナル No. 77

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　　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普及振興課(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