

情報処理に関するシンポジウム

健全なる情報化社会の構築に向けて

—コンピュータセキュリティ研究報告書要約—

昭和 57 年 10 月

財団法人 日本情報処理開発協会

JIPDEC

57

X011

このシンポジウムは、日本自転車振興会の競輪収益の一部で
ある機械工業振興資金の補助を受けて実施するものです。

目 次

はじめに—情報化の進展とコンピュータセキュリティ	1
(1) 情報化の意義	1
(2) 情報化の進展とコンピュータセキュリティ	1
(3) コンピュータセキュリティ対策の視点	2
 第1章 システムダウン防止対策（高信頼化対策）	5
1. 情報化社会におけるコンピュータシステム の高信頼化の必要性	7
2. 高信頼化技術の現状と課題	9
3. 各応用分野での高信頼化対策の現状と課題	23
4. コンピュータシステムの高信頼化への対応	35
 第2章 コンピュータ犯罪防止対策	45
1. コンピュータリゼーションとコンピュータ犯罪	47
2. コンピュータ犯罪の現状と問題点	52
3. 現状における対策と問題点	66
4. コンピュータ犯罪防止技術の方向	70
5. コンピュータ犯罪防止のための運用管理の方向	77
6. コンピュータ犯罪防止のための法制的検討	81

第3章 データ保護対策	87
1. データ保護の必要性	89
2. データ保護の目的	89
3. 保護すべきデータの範囲	90
4. データ侵害の態様及び主体	91
5. データ保護対策の考え方	91
6. 具体的対策	92
7. ガイドラインの在り方	98
第4章 結 論	101
1. 技術・設備面における対策	103
2. 運用管理面における対策	105
3. 制度的対策（行政の対策）	106
付 属 資 料	109

はじめに — 情報化の進展とコンピュータセキュリティ

(1) 情報化の意義

情報化とは、情報を物質、エネルギーに次ぐ第3の要素として認識し、その生成、加工、伝達、蓄積、利用を意識的に行おうとする活動の総体である。

情報化は、単に産業面における生産性の向上、省資源、省エネルギーに寄与するばかりでなく、教育、医療、環境、行政などの社会的問題の解決にも役立ち、人間の活動領域を広める効果をもつ。さらに、個人々の生活を通じて、人間活動における労働や余暇のあり方、国民の文化的価値意識にまで影響を及ぼすものである。

したがって、情報化の社会全般に及ぼす影響は、産業革命にも匹敵する広がりと深さを持っており、これへの対応如何が、人間社会の明日を決定するといって過言ではない。

情報化は、21世紀の日本を方向づける国民すべての課題である。狭隘な国土に1億余の国民のほか、これといった資源を有しない我が国が今後とも経済大国として国際社会の発展に貢献しつつ、資源、エネルギーの制約を克服し、活力とゆとりのある豊かな社会を築きあげていくためには、情報化の徹底と高度化が不可欠である。我々は、世界的視野に立って、官民の叡智を結集し、実りある人間中心の情報化社会の構築に邁進していかなければならない。

(2) 情報化の進展とコンピュータ・セキュリティ

これまで、情報化は、産業分野、特に製造部門を中心に経済効率の追

求を主軸に拠点的に展開してきた（第1次情報革命）。しかし、今後、情報化の波は、社会へ、また、個々人の家庭生活へと面的広がりをもって及ぶことが予想される（第2次情報革命）。情報化の進展により、多彩な便益が提供され、人間の活動分野に新たなフロンティアが開けていくことが期待されよう。

他方、情報化は、その在り方如何により、逆に大きな問題が生じる怖れがある。

電子計算機利用の高度化、広汎化に対応して、大量のデータの蓄積、迅速な処理、広汎な拡散が可能となってきた。

また、これに応じ、電子計算機システムに企業活動や社会生活が大きく依存している実態が生じつつある。

情報化の進展に伴い、

- (1) 企業秘密等貴重なデータの破壊、悪用やプライバシーの侵害
- (2) コンピュータ犯罪の多発
- (3) システムダウンによる社会的混乱

等の危険が生じている。

情報化は、秩序なく推進されるべきものではなく、それがもたらすマイナス効果を除去ないし回避するためのコンピュータ・セキュリティ対策を十分講じながら、情報化のもたらすプラス面を発揮させ、国民福祉の向上に寄与するよう進めていかなければならない。

(3) コンピュータ・セキュリティ対策の視点

この分野については、プライバシー問題、通信の秘密等の観点から、官民各界から、各種の提言、調査研究が行われているところである。

既存の研究、提言等にきくべきものは極めて多いが、総合的なコンピュータ・セキュリティ対策というよりは、プライバシーの保護、通信の秘密の保護という一面的な切り口によるものがほとんどといえよう。

我々は、コンピュータ・セキュリティ対策の究極的目的が、健全なる情報化の進展にあることにかんがみ、システムダウン、コンピュータ犯罪、データ侵害といった健全なる情報化の進展を阻む諸事象を広く把え、情報産業の振興という視点も加味し、かかる問題についてバランスのとれた総合的な対策を講ずる必要があると考える。

本研究会は、かかる視点に基づき、システムダウン防止対策(コンピュータシステム高信頼化対策)、コンピュータ犯罪防止対策、データ保護対策の三分科会に分かれ、本年6月初めより検討を続けてきた。

システムダウン防止対策(コンピュータシステム高信頼化対策)を担当する第1グループにおいては、公共性の高いシステム、人命に係るシステム等を主な検討対象とし、これらのシステムダウンを防ぐためにハード、ソフト、周辺設備において技術、運用管理、制度各面にわたってどのような対策が考えられるかを中心に検討した。

また、コンピュータ犯罪防止対策を担当する第2グループにおいては、コンピュータシステムを脅かす犯罪に着目し、その態様、システムの脆弱性、それに対する防止対策のポイントを検討した。

さらに、データ保護対策を相当する第3グループにおいては、企業秘密、プライバシーを保護するとともにシステムの安全運行を確保する観点からデータに着目し、これを保護するため技術、制度の各面においてどのような対策が考えられるかを検討した。

検討期間が短かったため、不十分な点も多々あるが、とりあえず検

討結果をまとめることにより本問題に関する世の議論を喚起することができれば、当初の目的は達せられたものといえよう。本問題解決の道程において一助となれば幸いである。

第 1 章 システムダウン防止対策（高信頼化対策）

1. 情報化社会におけるコンピュータシステムの高信頼化の必要性

1.1 コンピュータシステムの高信頼化の必要性

今日、“コンピュータシステム”は社会のあらゆる分野に利用され、社会の中核的役割を果たしている。例えば、銀行のオンラインバンキングシステム、鉄道や航空機などの座席予約システム等にみられるように、国民の日常生活に密接し、それなしではスムーズな日常生活が送れない現状になりつつある。

またコンピュータシステムは、年々、大規模・高機能・高度化する傾向にあり、自然災害、機器故障、ソフトウェア誤り、オペレーションミス等によるシステムダウンや誤動作により社会に与える影響は大きく、場合によっては人命に係わる重大事故を招くことが予想され、コンピュータシステムに対する高信頼化が社会的な要請となってきている。

1.2 コンピュータシステムの高信頼化とは

コンピュータシステムの高信頼化は、一般に「コンピュータシステムの障害発生をできるだけ減らし（信頼性：Reliability）、万一障害が発生してもその影響を最少限に食い止め（可用性：Availability）、できるだけ速く回復させ（保守性：Serviceability）、またハードウェアおよびソフトウェアの誤りやオペレーションのミスなどによりプログラムやデータが変更されたり、破壊されたりするのを防止し、万一破壊されても元の状態に回復でき（完全性：Integrity）、そして権限のないものに情報が知らされたり、また故意にデータが改ざんされたり、破壊されたりするのを防止する（機密保護：Security）」ことと言われており、

これらはR A S I S技術と総称されている。

本研究会で、特に公共性の高いコンピュータシステム、人命に係わるコンピュータシステム等を主な検討対象とし、ハードウェア技術、ソフトウェア技術、システム技術、周辺関連設備及び運用管理面から検討した。

2. 高信頼化技術の現状と課題

コンピュータシステムのシステムダウンを未然に防止し、万一システムダウンが発生しても速やかに障害個所を究明し、修復するため、①ハードウェア面、②ソフトウェア面、③システム面、④周辺関連設備・運用面による技術等がある。これらの技術の現状は、次のとおりである。

- ・ハードウェア面では、信頼性はかなり高くなっているが、新技術に対応した高信頼化技術を開発する必要がある。
- ・ソフトウェア面では、信頼性にまだ問題があり、ソフトウェアの信頼性の向上が必要である。
- ・システム面では、システム構成要素、個々の信頼性向上及びそのバランスのとれた機器構成によるシステム全体としての信頼性の向上が必要である。
- ・周辺関連設備・運用面では、信頼性に係わる安全対策を更に促進する必要がある。

2.1 ハードウェア面の高信頼化技術

コンピュータシステムの高信頼化を達成するには、図1-1の信頼性、可用性及び保守性を高める必要がある。

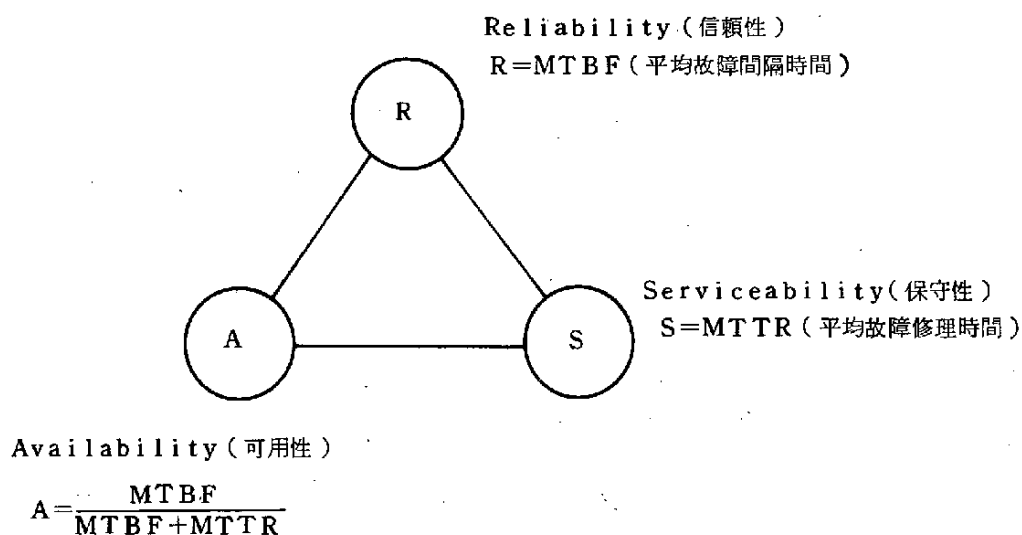


図 1 - 1 高信頼性の三要素

- ① 信 頼 性 ……… 故障がなるべく発生しないようにする。
- ② 可 用 性 ……… 障害が発生してもできるだけシステムダウンを回避し、システムの稼働率を高める。
- ③ 保 守 性 ……… システムダウンした時に速やかに障害個所を究明し、修復できるようにする。

2.1.1 信頼性技術

コンピュータの製造段階では、故障を発生させない対策として、次の各段階において信頼性を高める手段が採られている。

- ① 設計段階では、デザインオートメーション (DA) システムによって論理設計から製造データ作成までの段階を一貫して自動化し信頼性を高めている。

- ② 部品段階では、機構部品は電子化し、電子部品は部品数削減のためより高集積化（LSI、超LSI化）し、部品自体の信頼性を高めている。
- ③ 製造・検査段階では、より自動化を進め、作業ミスや検査もれをなくし、信頼性を高めている。

2.1.2 可用性技術

故障が発生してもできるだけシステムダウンを回避し、システムの稼動率を高めるため、次の各種の回路を組込んでいる。

- ① 故障検出機構としては、費用及びハードウェア量のバランスを考え、次のような故障検出回路が組込まれている。

- ・パリティチェック符号
- ・ハミング符号（SEC-DED^{*1}符号）
- ・拡張ECC^{*2}符号
- ・CRC^{*3}符号
- ・回路の二重化法（例えば加算器の多重化）
- ・ nC_1 コード法
- ・相補的論理法（Two Rail Logic）
- ・時間監視

*1 : Single bit Error Correcting-Double bit Error Detecting

*2 : Error Correction Code

*3 : Cyclic Redundancy Check

② 故障が検出されると、システムダウンを回避するため、当該誤りの訂正、あるいは当該命令の再試行が行われる。

③ 誤り訂正ができず、再試行にも失敗した時には、障害モジュール（例えば、動的アドレス変換機構（DAT）のTLB^{*1}、バッファメモリ）を切離し、縮退して動作を続行する。

2.1.3 保守性技術

システムダウン回避ができず、ダウンした場合には、速やかに障害箇所を指摘し、復旧させるため、次の手段が予め用意されている。

① 障害情報の収集を行うため、

- ・ログアウト
- ・スキャンアウト

がある。

② コンピュータ自身で診断する方法として、

- ・FLT^{*2}法
- ・機能診断法
- ・マイクロ診断法
- ・ログアウト解析法

等がある。

③ 故障部品の交換を迅速に行うため、容易に交換できる構造及び治具が開発されている。

*1 : Translation Lookaside Buffer

*2 : Fault Locating Tests

- ④ 中央の保守センタ側で情報を収集して故障分析を行う遠隔保守診断がある。

2.1.4 今後の課題

ハードウェア面での高信頼化技術の課題としては、次のものがある。

① 素子技術変貌への追従

超LSI化に対するテストビリティの向上とジョセフソン素子等に対するテスト等の技術の対応が必要である。

② 実装技術変貌への追従

超LSI技術、プリント板製造技術等の向上に対応する診断手法の開発が必要である。

③ 間欠障害対策

間欠障害は再現性がないため、解明に時間がかかることが多いが、固定的な障害に比較してずっと多いと言われており、対応が必要である。

2.2 ソフトウェア面の高信頼化技術

ソフトウェアの面からコンピュータシステムの高信頼化を達成するには、

① ソフトウェアの信頼性

② ハードウェア障害およびソフトウェア障害に対する障害回復処理

③ 保守診断機能

の三つについて信頼性を高める必要がある。

2.2.1 ソフトウェアの信頼性

ソフトウェアは、ハードウェアとは異なり、劣化による障害はない。従って、ハードウェアでも同様であるが、特にソフトウェアでは設計及び製造段階での論理的な誤りをいかにして避けるかが最も重要視され、次に設計及び製造段階で盛込まれてしまった誤りを検査段階でいかに発見し、除去するかが重要である。

ソフトウェア自体を高信頼化するため、

- ① デザインレビューの充実
- ② 高信頼化プログラミングの採用
- ③ プログラムテストの充実

等の対策が現在行われている。

2.2.2 障害回復処理

障害の原因には、ハードウェア、ソフトウェア、そしてオペレーションに起因するものがある。いずれの原因であっても、可能な限りユーザに影響を与えないで回復し、できるだけシステムダウンを回避する必要がある。

そのため、OS^{*}では、

- ① 可能な限り回復を試みる。
- ② 回復不可能な場合には、罹障範囲を局所化し、罹障部分の切離し（後に復旧）を行う。

を基本とした処理を行っている。

* : Operating System

最近では、OS障害に対しては、各機能毎に機能回復ルーチンを用意し、障害発生前に実行した処理の取消し、無効化を行い、システムを矛盾のない正常な状態に回復させる確率を増大させている。

またファイル障害に対しては、各種の事前・事後処理の回復手段が一般的であるが、ファイルの大容量化にともなう回復時間の大幅な増大に対処する有効な手段の開発が遅れている。

2.2.3 保守診断機能

ソフトウェアによる保守診断機能は、ハードウェア障害及びソフトウェア障害に対して準備されている。

① オンライン診断

オンライン診断では、固定障害としてシステムから切離された装置に対し、OSの1ジョブとして診断プログラムを実行することによりシステム運転を中断することなしに障害原因を究明する。最近では、本体系装置の診断プログラムは別のサービスプロセッサ等から実行され、オンライン診断は主に周辺装置に対して準備されるのが一般的である。

② ログ編集／ログ分析

障害が発生した時点で収集された障害情報は、ログ編集により保守が容易な形に編集出力される。

最近、この障害情報をプログラムで解析して障害個所を指摘すること（ログ分析）も実用化されつつある。

③ 遠隔保守

遠隔保守は当初ハードウェア障害の診断に限られていたが、最近ではソフトウェア障害も包含した総合システムへと発展してきている。

2.2.4 今後の課題

ソフトウェア面での高信頼化技術の課題としては、次のものがある。

① ソフトウェアの信頼性向上とソフトウェア障害に対する障害処理の充実

ソフトウェアの巨大化により、人手によるソフトウェア誤りの完全除去が難しくなっており、ソフトウェア誤り除去の効果的な支援ツール、またシステム運用中万一ソフトウェア誤りによる障害が発生してもシステムダウンを回避する障害処理が必要である。

② 障害ファイルの回復の迅速化

統合データベース化等の推進により、ファイル障害はシステムダウンと等価になっている。大容量化が進むファイルの障害に対する短時間での回復技術が必要である。

③ 複雑な障害に対する遠隔保守の高度化

コンピュータシステムが数多く設置されるに伴い、高度な保守技術者によるサービスを受けることが難しくなっている。コンピュータシステムの保守・診断作業を単純化すると共に、複雑な障害切分けに対して早く高度な保守技術者によるサービスを受けられるように遠隔保守の充実及びその一層の普及の必要がある。

2.3 システム面の高信頼化技術

コンピュータシステムの社会的な役割が増大し、最近のシステムは大規模化、オンライン化が進み、その影響範囲が大きくなってきている。そのため、コンピュータシステムの信頼性がより重要視されるようになってきた。

システムの信頼性の目標は、

- ① システムが提供すべき機能（サービス）の連続性の確保
- ② システムが保有するファイル内容の完全性（インテグリティ）及び機密保護の確保

の2つである。

高信頼化システム構成技術としてシステムを構成する構成要素をコンピュータ本体、ファイル及び回線・端末に大きく分けて考えてみると次の通りである。

2.3.1 コンピュータ本体

要求信頼度、システムの規模、利用形態、経済性を考慮し、信頼性を高めるためのCPU構成は、次のいずれかの形態がとられている。

- ・デュプレックスシステム
- ・ロードシェアシステム
- ・マルチプロセッサシステム
- ・デュアルシステム

周辺装置に関しても、冗長化構成を主体とした対策が採られている。

オンラインシステムのソフトウェアは数百万ステップにも達しており、ソフトウェアを限られた時間と人的資源で完全なものにするのは、現実には不可能に近い。このため、システム設計上、ソフトウェアの誤りによるシステム異常が検出されても、即座にシステム障害とせず、その罹障部分を切捨て、サービスの連続性を確保するため、次のような手段が講じられている。

- ・アプリケーションプログラムの切離し
- ・端末の切離し（システムの走行環境を変える）
- ・OSモジュールの切離し（一部で実行されている段階である）

2.3.2 ファイル

ファイルで最も重要な点は、システムが保持する大量のファイルをいかに速く、正確に回復するかである。

ファイルの回復処理は、次の2段階に分けて考えることができる。一つはシステム運転中トランザクション情報を記録する事前処理であり、もう一つは、異常発生後、事前に記録しておいた情報を利用し、ファイルを正常に回復する事後処理である。

① 障害事前処理

障害事前処理の技術的なポイントは、回復のための必要最少限の情報をいかに速やかに取得するかの点にしばられる。主要な方式としては、ジャーナル方式とチェックポイント方式がある。

② 障害回復（事後）処理

トランザクション及びファイルの回復は、事前処理で取得された情報を利用して行われる。障害回復処理で最も重要な点は、迅速に行うだけでなく、トランザクションの欠送^{*1}や冗送^{*2}をおこさないようにすることにある。

*1：送信をしわすれること。

*2：同じものを二度以上送信してしまうこと。

2.3.3 回線・端末

回線系では、誤りに対処する伝送制御手段（垂直／水平パリティチェック、CRCチェック、再送等）を採用し、より高い信頼性を確保している。また、最近では、長時間の回線障害を防止するため、図1-2のように、二重に回線を設置したり異なる種類の回線を予備として設置するシステムもある。

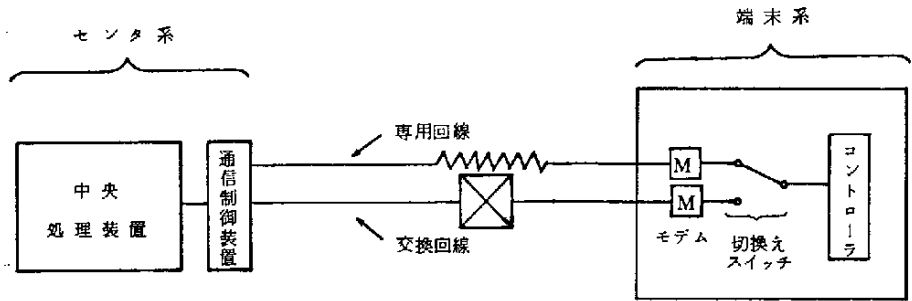


図1-2 回線の二重化

また、TSS* など、データ処理を中心とする全国的なシステムでは、センタダウンの対策として図1-3のように、サービス要求を最寄りのセンタに迂回し、代行処理させる方式を採用して、信頼性の向上を図っている。

端末に関しては、機構部品は電子化し、機械的故障の軽減を図っている。

* : Time Sharing System

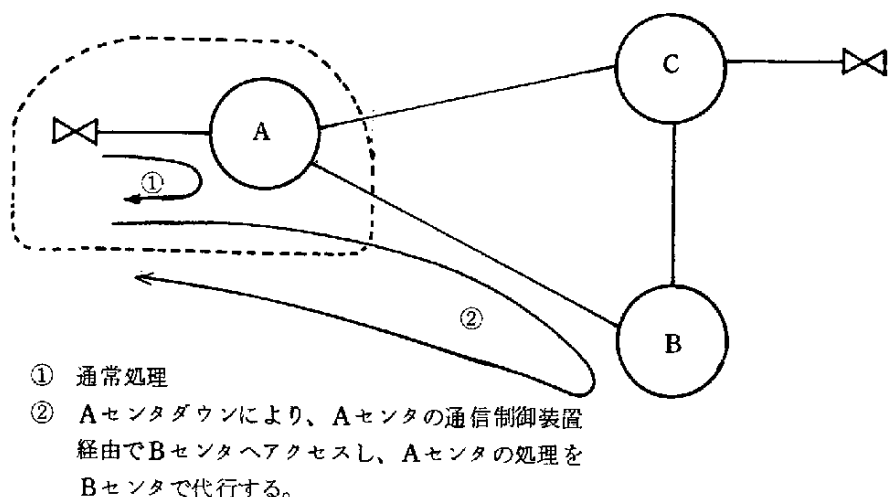


図 1 - 3 センタの代行処理

2.3.5 今後の課題

システム面での高信頼化技術の課題としては、次のものがある。

① 大規模ソフトウェアの品質管理

ソフトウェアのテストを自動化し、残存バグを推定できるようにする必要がある。

② 故障診断技術

ハードウェア及びソフトウェア故障の切分けを迅速化する必要がある。

③ 回線障害対策

故障個所の切分けが難しく、解明に時間がかかることが多いので、対応の迅速化が必要である。

④ 24時間システムへの対応

日夜休みなく稼動する大型システムが増加してくると思われるが、

そのためのシステム構成レベルでのシステムダウン回避の対策がより必要であり、処理対象を考慮した最適システム構成についても研究する必要がある。

2.4 周辺関連設備・運用面の高信頼化対策の現状

我が国のコンピュータシステムの安全対策は、1977年4月に通商産業省において「電子計算機システム安全対策基準」が策定、公表されたことを契機として、意識が急速に高まった。

この基準はコンピュータシステムの高信頼性を直接高めるものではなく、コンピュータシステムが外的要因により停止したり、誤動作しないよう正常に運転するための間接的な信頼性を確保するものである。この基準により、安全対策が一部の企業では経営計画の一環の投資として考えられ、主に次のような設備・運用による対策が採られるとともに、コンピュータシステム運用担当部門の安全意識が高まった。

- ① データの保管、バックアップのための耐火金庫の設置、外部保管業者への保管委託によるデータ保護対策
- ② ハロン消火器及び同消火設備による防火対策
- ③ フリーアクセス床、コンピュータシステム、機器類の耐震対策
- ④ 出入口の監視制御設備等による防犯対策
- ⑤ 電源、空調設備の保守・管理
- ⑥ 緊急時対策マニュアルの整備
- ⑦ 運用体制の整備

等

その後、1978年6月に発生した宮城県沖地震における体験は、コ

ンピュータシステムの耐震対策について数多くの教訓を残し、様々なインパクトを与えている。

しかしながら、これらの対策は、特定の目標や一定のガイドラインのもとに行われるだけではなく、ユーザとメーカの個々の判断のもとに、経済的にできるものから実施しているのが現状である。

3. 各応用分野での高信頼化対策の現状と課題

3.1 各応用分野で要求される信頼性のレベル

コンピュータシステムの信頼性は多額の投資をすることにより向上するが、信頼性を上げるほど信頼性の向上に要する投資額が多額になる。また、こうして高信頼化されたシステムでも必ず故障が生ずるものである。このことを考えれば、一般のコスト有限の状況では、各応用分野ごとに要求されるコンピュータシステムの信頼性のレベルを規定し、そのレベルを達成する最も経済的なシステムを構築することが重要である。

コンピュータシステムにどの程度の信頼性を要求するかを決める時には、何らかの信頼性の尺度を定義しなければならない。信頼性の最も基本的な尺度は信頼度であるが、コンピュータシステムのような総合システムの場合には、稼働率をとるのが普通であろう。

規定された信頼性のレベルが絶対に守らなければならない仕様値なのか、平均としての目標値なのかによって考え方は大幅に異なってくる。一般に、仕様値の場合には、実際に構築するコンピュータシステムには十分な安全率を掛けなければならず、その値はあまり高くすることはできない。人命に係わるコンピュータシステムを除けば、その応用分野ごとに達成すべき目標値を規定することが望ましい。

オンラインバンキングシステム、座席予約システム等の分野では、通常でも客が数分間程度待つのは普通であり、客にとってその待合せが、これより著しくならず、また業務処理上不都合な誤りが生じない程度のシステムダウン時間は許容されるべきであろう。

しかし運送業分野における運転管理システムのように、直接制御対

象（例えば、列車）に接続されたシステムではシステムダウンの許容時間は極めて短い必要がある。

3.2 銀行システムの高信頼化対策

銀行は「金融」を扱うサービス業で顧客との接点が多く、その社会的・公共的役割は大きい。現在では、銀行業務のほとんどが何らかの形でコンピュータシステムに係わっており、顧客対応事務などは、コンピュータなくして円滑な運営が考えられない状況である。特に最近では、CD^{*1}、ATM^{*2}等顧客が直接操作するオンライン端末機も普及しており、短時間のシステムの停止でも社会的な影響はかなりのものとなってきている。

従って、銀行のコンピュータシステム構築時には、その安定性、信頼性に最も重点が置かれ、設計目標値も高い。基本的には、ノンストップシステムを目指し、万が一のシステムダウン時にも10分間以内で復旧するというのを、一般的な基準としているところも多い。

3.2.1 自行システムの現状と課題

(1) 現 状

① システム構成上の信頼性向上策

銀行システムの構成は、ほとんどすべてバックアップのための二重化がはかられている。CPU障害に対処するため、常時複数のCPUを稼働させたデュアルシステムあるいはデュプレクスシステムとなっているか、あるいは静止待機型のバックアップCPUを

*1 : Cash Dispenser

*2 : Automatic Teller's Machine

保有している。CPU障害に対処するもう一つの方法として、分散処理を採用しているシステムもある。即ち、支店をいくつかのグループに分割し、それぞれのグループ毎に処理CPUを特定したシステムである。この方式は、システムダウンの影響を1グループ内の支店に限定できるというメリットがあるが、オンライン預金（どこの支店でも預金出入れ可）のサービスを行うためグループ間のCPU-CPUのデータ授受が必要となっており、効率面、システムの単純化といった面では、問題が残っている。

CPU以外の入出力機器、通信回線、端末、電源、空調等の障害に対処するため、予備機を充分に確保している。

② 障害の早期発見機能

障害発生をできる限り早期に発見し、その影響の拡散を防止することは、銀行システムの重要な機能の一つである。特に入出金の処理に関連する部分は、時間が経過してから異常が発見されても、対処が困難でかつ銀行の信用問題にまで発展しかねない。従って、銀行システムでは、1件のトランザクションの処理が完了するまでに経由する部分部分に様々なセルフチェック機能が組込まれており、異常が発見された場合でも、その取引を保留する等して、システム全体が停止することなく原因究明作業を可能にしている。

③ 機器障害時の自動切替機能

ハードウェアの故障が直ちにシステムダウンに結び付かないように、ソフトウェアでの対処が行われている。銀行システムでは、単に障害機器を切離して縮退運転に入るのではなく、自動的に予

備機へ切替え、サービス機能が低下しないシステムとなっているのが、一般的である。

④ 復旧所要時間の短縮化

銀行システムでは、復旧時間を短縮するため、再立上げの際にバッチジョブ等による準備作業を必要としないようになっている。即ち、オンラインシステムそのものに復旧回復機能が組込まれている。更に復旧に要する処理ステップ削減のため、チェックポイントが有効に活用されており、ダウン直前の状態に戻すことが数分間以内に可能である。

⑤ 運用管理面での信頼性向上

人の介入が多くなるとミスも発生しやすく、信頼性が低下するという観点から、障害発生の把握とその対処などの判断機能もシステムへ組み込み、極力自動化をはかっている。

またシステムオペレータについては、一般的にスキルの高い人を任じ、さらに定期的に異常時対処訓練も行っている。

(2) 今後の課題

自行システムはその安定性を追求するあまり、システム自体が非常に複雑化してきている。このため単純なハードウェア障害でも、その回復ロジックに誤りがあり、増々障害を深くしてしまうという例もある。確かに、回復機能によってシステムダウンの回数は削減されるが、一方では復旧時間を長びかせる要因となっていることは否めない。

この回復機能の必要十分なレベルを明確に設定することは非常に難しいが、現在のようなノーダウンを目指す傾向が続けば、自行シ

システムのソフトウェアの半分以上が異常時対処のためのものとなりかねないので、何らかの社会的な基準が必要であろう。

3.2.2 全銀システムの現状と課題

(1) 現 状

全銀システムは加盟金融機関相互間の為替交換を迅速かつ正確に行い、他行為替事務の合理化及び顧客サービスの向上をはかることを目的に全銀センタ、全銀ターミナル及びこれを結ぶ通信回線で構成されている。

① 全銀システムの構成

全銀センタは信頼性、迅速性、経済性、処理能力等を勘案してオンライン処理用情報処理装置 2 セット（2 系統）と、これをバックアップする待機予備兼オフライン処理用情報処理装置 1 セットにより構成されている。

加盟銀行は全銀ターミナルを 2 セット以上設置し、全銀センタのオンライン処理用処理系 1 及び処理系 2 のそれぞれと特定通信回線で結ばれている。

② 全銀システムの運用

全銀システムの通信の開始は、開始時刻に全銀センタから各自行センタ宛に通信開始通報が送信される。為替通信の終了は、全銀センタから各自行センタ宛に終了通報が送信されるとともに、当日の送受信のカウントが通知されるので、自行センタはカウントの照合を行い、当日の通信を終了する。

③ システム障害管理とその対策

全銀センタの設備及び回線の障害に対して、罹障個所の拡大を

防ぐため、試験プログラムを用意し、罹障装置の識別を行ったうえで、障害装置の種類及び規模に応じた処理を行っている。

更に全銀システムまたは自行システムのいずれかにおいて障害が発生し、オンラインによる発受信が不可能な場合は、障害の発生状況によってはテレバックによる取扱いを行うことができる。テレバックは、仕向行と被仕向行との取引店相互間で、電話により取引1件ごとに為替通知を発受信して取扱い、折返し確認電話をもって為替通知を完了するものである。

(2) 今後の課題

全銀システムの安定化には、様々な対策が講じられており、またシステムとして非常に安定していると言えるが、今後一層の安定化対策として、回線障害時等に公衆回線、DDX等の他回線ルートへ切替える等の対策が必要である。

3.3 医療情報処理システムの高信頼化対策

医療情報処理システムは、現在医事会計業務等、医療のいわば付帯業務的な部分が実用化されているにすぎないが、将来は医療診断をも含む総合的なシステムへと発展して行くものと思われる。

しかし、コンピュータシステムが人間の生命をも直接左右する役割を担って行くことに対して、医師とコンピュータとの役割分担、信頼性に対する不安など、根強い慎重論もあり、この分野でのコンピュータシステムの高信頼化は、今後の解決すべき重要課題の一つである、と言える。

3.3.1 医療情報処理システムのあり方

一般に、医療情報処理システムはその性質上、直接人命に係わる情

報や問題を取扱う。このため、処理データの正確性、信頼性が、人命をも直接左右することすらある。システム開発上、このことを充分に考慮し、正確性及び信頼性の確保を第一とすることが、システム提供者の社会的責務であることを、自覚する必要がある。

次に医療データそのものの取扱いである。医療データ及びその記録である「病歴」の機密性・重要性に深い見識を持つ必要がある。言うまでもなく、「病歴」は個人の健康に関する重要な記録であり、個人のプライバシーにかかわる情報である。従って、悪意を持つ第三者にこれらの情報が漏洩することのないよう、システム設計上及び運用管理面で十分な配慮が必要である。

3.3.2 医療情報処理システムの現状と課題

(1) 救急医療情報システム

救急医療情報システムは、救急医療活動を情報処理の側面から積極的に支援するものであり、最適医療機関の確保、医療資源の効率的活用に寄与している。本システムは、地方自治体を中心に導入されているものが多い。しかし、現在のような信頼性対策では、こうしたシステムの発展には限度がある。今後のこの種のシステムでは、オンラインのファイル回復は勿論、デュアルシステムのような高度な信頼性技術の採用により、機能の質的変革に対処して行く必要がある。

(2) 病院情報処理システム

病院情報処理システムは病院内の業務を対象としたものである。しかし現在のところ、システム化が進んでいるのは、医事会計、診療補助業務等の事務業務であり、病気診断等の診療本来の業務への

適用については、ほとんど例がない。

現在の病院情報処理システムは、臨床検査システム、放射線診断システム、心電図自動解析システム、モニタリングシステム等のような高度かつ専門的な業務機能をサブシステムとして統合しながら、より総合的なシステムへと発展して行くものと思われる。

病院情報処理システムは、その信頼性いかんによっては、人間の生命をも直接脅かす存在にもなりうる。今後、システムのデュアル運転、サブシステム間の機能分担、機能の冗長化など、耐故障設計へ向けた努力が必要となる。

3.4 情報処理サービス業での高信頼化対策

情報処理サービス業では、バッチ処理が主流であった利用形態が、今日では各種のオンライン処理の利用形態の普及がめざましい。このような利用形態での情報処理サービスのシステムダウンによってこうむる利用者の損失（生産性の低下、機会損失、経済的損失等）も大きく、その社会的影響も一層広汎なものとなっており、情報処理サービスの信頼性を高めることが社会的責務となってきた。

3.4.1 情報処理サービス業の現状

情報処理サービス業での高信頼化対策については業界特有の対策は特になく、むしろ一般的な情報処理システムの高信頼化対策を厳守していると言える。

業界での高信頼化対策の一般的な状況は次の通りである。

(1) 設置環境

設置環境の基本となるのは建物とその立地である。理想的な建物等の環境を入手するには莫大な資金を要し、簡単には実現できないのが現状である。

しかし、1981年7月に通産大臣が認定する「情報処理サービス業電子計算機システム安全対策実施事業所認定制度」が創設され、その認定基準を満たすように改善されてきている。

(2) コンピュータシステムの高信頼化

情報処理サービス業はコンピュータメーカの製品を購入し、コンピュータパワーを売る業である。従って、一般のコンピュータ利用企業と同様に信頼性設計・管理の範囲を脱することは難かしく、もっぱら障害対策を重点に信頼性を向上させている場合が多い。

システム障害の主たる原因は、

- ① ハードウェア障害
- ② ソフトウェア障害
- ③ 原因不明の障害
- ④ 過負荷（オーバーロード）による障害

であり、これらいずれの障害に対しても、ユーザの利用に支障とならないよう復旧を図っている。

① ハードウェア障害

情報処理サービス業では、顧客のニーズを満たすため、ハードウェアは必ずしも同一メーカの製品で構成されていない場合もあるため、場合によってはハードウェア障害の原因究明にメーカとの協力が不可欠となる。プラグコンパティブル装置の使用時、各

種の入出力機器、通信機器、端末機器等の障害に関しては、障害原因の切分け作業は自らが行ない、個々の機器に対して該当メーカー側が対処することになる。

② ソフトウェア障害

情報処理サービス業では、メーカー提供のOSをオリジナルのまままで使用せず、運用管理に必要な機能（料金計算、データ保管システム、運転管理・統計等）と、顧客の要求によりオリジナルにない機能を独自に追加するケースがある。これらの追加機能が誤っていることによりOSに障害が起こる場合があり、この場合には情報処理サービス業者が自社で対処する必要がある。

ユーザプログラムの誤りでシステムダウンの直接的原因となることはまずあり得ないが、その動作時に呼ばれるOSのルーチンにバグがある場合、障害を起こすことがある。

③ 原因不明の障害

この種の障害の頻度は意外と多く、またなかなか根絶できていない現状である。直接的なシステムダウン等につながった二次原因は判明できても、更にその原因となった一次原因が不明なしはトレースできないようなケースもある。

この種の障害は、多くの場合、再現性が低く、手掛りを得ることが困難であるため、原因究明には相当な時間と費用が費やされている。

④ 過負荷（オーバロード）による障害

システムの持つ性能限界を超えたトランザクションの集中入力等により、当初システム設計時に設定したターンアラウンドタイム

を維持できなくなることがある。これは、OSの設計思想に依存することもあるが、基本的には、システムの性能設計時の処理量の見積り方法と、運用段階（運転時）の負荷率の監視・管理（とその対策）の問題である。

(3) 運用体制

情報処理サービスの質を決定する要素として、運用は大きな比重を占めている。すなわち、与えられたハードウェア条件、OS構造、適用業務の特質を正確に理解し、運用管理をしなければならないからである。

また最近のコンピュータシステム自体の信頼性の大幅な向上が期待されているため、障害が発生した場合にすぐ対応のとれるよう定期的な障害復旧の訓練をしておく必要がある。

3.4.2 情報処理サービス業電子計算機システム安全対策実施事業所認定制度

本制度は、情報処理サービス企業の安全対策の実施の促進を図り、我が国の情報化および情報処理サービス業の健全な発展を図ることを目的として、通商産業大臣が一定の安全対策を実施している企業を認定するもので、1981年7月20日に創設された。

本制度により、情報処理サービス業の、主として、設置環境および運用面での高信頼化を含めた安全対策が推進されて行くものと考えられる。

3.4.3 今後の課題

情報処理サービス業のもつ社会的責任と重要性に鑑み、利用形態等による規模・性格等に差はあるとしても、サービスに供する設備

（資源）に対して技術面および運用面から高信頼化への対応が必要である。

更に、情報処理サービス業の高信頼化対策を円滑に推進するためには、企業内のシステム監査等の充実も必要であろう。

4. コンピュータシステムの高信頼化への対応

コンピュータシステムの高信頼化に対する今後の対応としては、次のことが必要となっている。

- ・ ハードウェア面では、超LSIのテストビリティの向上、間欠故障対策、遠隔保守の高度化等に対応することが必要である。
- ・ ソフトウェア面では、ソフトウェアの信頼性向上、ファイル回復の迅速化、誤操作対策等に対応することが必要である。
- ・ コンピュータシステム関連設備面では、悪環境条件を避け、耐震対策、防火対策、防犯対策等を強化することが必要である。
- ・ 運用管理面では、障害に対処できる運用体制を確立し、障害を想定した運用訓練を定期的を実施することが必要である。
- ・ システムの高信頼化対策としては、個々の要素技術の開発、改善や企業におけるシステムダウン対策を進めるとともに、処理の内容に合わせたシステム構成のガイドライン作成について検討することが必要である。

4.1 ハードウェア面の対応

4.1.1 信頼性技術

(1) 超LSIのテストビリティ

超小型化・低電力消費化するため、集積度を上げるが、その結果、一般にチップのピンリミット*になる傾向がある。その一方法としてテ

* : 機能(ゲート)をたくさん組込むと、一般にそれに比例して外部接続のためのピン数が増加してしまう。その状態のままチップ化すると、チップ上のピン接続エリアが非常に増大し、従ってパッケージの形状が大きくなり、集積化の意味がなくなるので、ピン数(パッケージの大きさ)に制約がある。

スト用のピンはなるべく少なくし、その分、内蔵されるテスト機能論理で補う対策をたてることになろう。また、テストの組合せ数は、論理素子数の累乗で増加するので、テスト時にチップ内の論理構造を変え、複数のグループに区分できるようにし、1グループ内の素子数を少なくする方式も考えられる。

(2) 間欠障害対策

間欠障害は再現性があまりなく、解明に時間がかかる。解明には、故障検出時よりしばらく前の内部情報が豊富にあることが早道であり、メモリ素子の高集積化が進んでいるので、内部情報のうち重要な情報の履歴を常にとっておく（ある時間間隔で旧情報は消される）ことが考えられる。この方式は、既に部分的に採用されつつある。

4.1.2 可用性技術

(1) 間欠障害対策

間欠障害に対しては、単に命令の再試行を繰返すのではなく、回路に冗長性を持たせ再試行時にはルートを変えて行うような機能が必要となってくる。

(2) 縮退運転

超LSI化が進み、論理素子を節約することに余りコスト的なメリットがなくなっていることを考え、逆に2重化等を行い、切替えあるいは縮退が可能となる設計が必要となろう。

4.1.3 保守性技術

(1) 診断技術の開発

装置を構成する論理素子数が飛躍的に増大し、診断データを作成するのに膨大な工数を要するようになってきている。一方現場での

交換単位は大きくなり、交換枚数は少なくなっている。このことから新しい診断技術の開発が必要となってきた。

(2) 遠隔保守

遠隔保守としては、保守時間を短縮させ、また保守を容易にするソフトウェアの開発が必要である。

さらに、保守は遠隔で行えても、取替え部品はサイト側に持って行く必要があるため、部品センタの設置場所等も今後考えていく必要がある。

4.2 ソフトウェア面の対応

4.2.1 ソフトウェアの信頼性向上

ソフトウェアに誤りを盛込ませないためには、

① デザインレビューの推進

② 最適モジュール分割と構造化プログラミングの適用

を更に徹底するとともに、誤りを除去するためには、工場内で限られたシステム構成、限られた環境下でソフトウェアの品質を高める必要があり、仮想コンピュータシステム、環境シミュレータ等を開発、充実させる必要がある。

そして、ソフトウェアの品質向上のためには、ソフトウェアテスト評価ツールの研究・開発を推進してゆく必要がある。

4.2.2 高度な障害回復処理

ソフトウェア障害の回復手段の範ちゅうとされている機能回復ルーチン等をハードウェア障害の回復をも含めた形でキメ細かく準備してゆく必要がある。

4.2.3 効率のよいファイル回復

現状の技術では、ファイルを2重化しておかない限り、ダンプ情報及びAfter Imageを使ってゼロからファイルを回復する必要がある。このため、例えば2.5ギガバイトのディスク装置が使用不可能になった場合、他のディスク装置に同一ファイルを構築するには数十分間のオーダーの所要時間がかかってしまう。ファイルの2重化によってある程度解決されるが、費用が2倍になってしまうため、今後ソフトウェア面だけでなく、ハードウェア面からの対応も必要である。

4.2.4 効率のよい障害情報の収集と診断

間欠障害は一過性であるため、1回目の障害発生で切分けに必要な全ての障害情報を収集する必要がある。障害切分けに必要な十分な障害情報を素早く収集し、診断を行うには、ハードウェア面及びソフトウェア面を総合した対応が必要である。

4.2.5 誤操作対策

オペレータをいくら訓練しても 10^{-3} 程度のミスを避けることはできないといわれている。これら誤操作対策として自動運転が有効であるが、どうしても人間が判断し、操作しなければならない部分があるため、例えば、その部分についてはシステムダウンを伴うコマンドは受け付けない、また2段階のコマンドにするなど十分なソフトウェア面でのガードを設ける必要がある。

4.2.6 ソフトウェアによる超高信頼化

ソフトウェアによる超高信頼化を実現する研究としては、スタンフォード研究所(SRI)のSIFT(Software Implemented Fault Tolerant)のようにハードウェアを多重化し、ソフトウ

ウェアで結果の照合、出力を行うものとか、フォールトトレラントソフトウェアのようにソフトウェアを多重化（同一仕様で異なるプログラミング）しているものがある。これらは、今後の研究成果を見る必要がある。

4.2.7 ハードウェアとソフトウェアの機能分担

現在のアーキテクチャは、LSI化およびファームウェア化の動向に対し、必ずしも最適でなくなっている。ソフトウェアの機能軽減によるソフトウェアの信頼性向上、負荷分散化によるシステムダウンの回避等を考慮した新アーキテクチャの研究・開発が必要である。

4.3 コンピュータシステム関連設備面の対応

4.3.1 建物の環境

コンピュータシステムの高信頼性を確保するためには、設置する環境が十分に整備されている必要がある。建物の物理的環境条件を良くするためには以下のような悪条件の場所を避けることが必要である。

- ① 地震の多発予想地域や軟弱地盤、液状化地盤など地震時被害の大きい地域や震動障害のおそれのある場所
- ② 危険物集積地など周辺地域の大規模火災や爆発によって被害を受けるおそれのある地域
- ③ 津波、高潮、重塩害、出水、落雷等の多発地域
- ④ 電波塔近辺、マイクロ回線等の強力な電界および磁界のある地域
- ⑤ 塵埃、腐食性ガス、有毒ガス等の空気重汚染地域
- ⑥ 市街地での人の往来の激しい地域（人目につきやすい）や交通

機関の影響を受けやすい地域（例：伊豆半島、東京湾岸工業地帯等）

4.3.2 建物（室）の対策

(1) 耐震対策

建物は多少損傷しても倒壊せず、人命の安全を守るという立場で建設されているが、コンピュータシステムや関連設備の設置の条件により耐震性が変化するため、その設置階がどの程度の加速度と変位をうけるかは、別途専門家による診断を受け、それに基づき、耐震対策を実施する必要がある。

(2) 防火対策

コンピュータシステム等の設置室を1時間以上の耐火壁で囲む等の外部からの火災に備える対策をとるとともに、コンピュータシステム等の設置室から火災の起きないように対策をとることが重要である。

(3) 防犯対策

コンピュータの設置室は勿論であるが、電源、空調等の関連設備のある場所も、

① 不法侵入検知・防止設備

- ・ 無人監視システム
- ・ 出入口開閉コントロールシステム
- ・ 建物開口部侵入検知システム
- ・ マントラップ構造および前室配置

② 破壊工作防止機能

- ・ 出入口の二重化
- ・ 地上（10 m 程度）開口部の閉鎖
- ・ 防爆壁の多用

等の対策をとることが望ましい。

4.3.3 関連設備の対策

関連設備の対策として今後考えて行かなければならないのは、耐震対策及びそれらの保守管理である。

主な耐震対策としては、

- ① 固 定
- ② 補 強
- ③ 脚部改造
- ④ 柔軟構造または免震構造
- ⑤ 緩衝材
- ⑥ 自動運転制御機器

等がある。

4.4 運用管理面の対応

4.4.1 運用管理面からの障害発生防止

ハードウェア、ソフトウェア、そしてシステムの3者が正常に機能していることを前提に運用面からは、次のようなことが必要となる。

① 運用管理に関する規則

コンピュータセンタに出入する人の入退室の管理・監督や、コンピュータセンタの設備の状況監視、防災等の管理・監督に必要

な規則の整備と運用体制を確保することが必要である。

② コンピュータのオペレーション

オペレーションに必要なマニュアルの完備と、変更・修正が行われた場合のマニュアルのメンテナンスが充分に行われているかの管理やこれら運用の監査制度が必要である。更に運転操作のスイッチ類にふれて誤動作を起さぬようカバーを付ける等の設備面での防止対策により補うことも重要である。

③ オペレータの教育・訓練

オペレータにコンピュータシステムの運転に必要な規則や操作手順に関する定期的な教育や訓練、さらに適性検査を行うことも必要である。

4.4.2 障害発生時の運用管理

万一障害が発生した時、迅速で適切な処置が取れることが、障害のもとらす影響を最少限にとどめることになる。

このためには、障害に対処できる運用体制の確立と障害を想定した運用訓練の定期的な実施が重要となる。

4.5 システムの高信頼化のための対応

コンピュータシステムの高信頼化を確保するためには、ハードウェア、ソフトウェア、コンピュータシステム関連設備、運用管理等において総合的にバランスのとれた対策をとることが必要であるが、銀行システム、医療情報処理システム、情報処理サービス業のシステム等のようにコンピュータシステムのダウン、エラー等により社会に与える影響の大きいシステムについては、既に詳述されているような各種技術等で対応する

とともに、コンピュータシステム構成によって信頼性を確保するための対策を講ずる必要がある。

システムダウンを防止するに当たっては、先ず、システムが停止しないようにデュアル、デュプレックス等のシステム構成や回線、関連設備の二重化が考えられる。更に高信頼性を追求すると災害等により地域的にコンピュータシステムが使用できなくなった場合にはコンピュータシステムのバックアップを他の地域で行うことなど様々な方法が考えられるわけである。

しかしながら、これらの対策を講じるに当たって民間企業においてはある程度の採算のとれる範囲で行い、必要とはわかっていながらなかなかこれらのための設備投資を行えない現状にある。従って、これらの対策を講ずべき特定システムについては金融、税制面等による助成を行い、これら対策に対するインセンティブを与える必要があろう。

また、ユーザのデータをコンピュータ処理する情報処理サービス業等にあっては、ユーザと災害発生後、何時間後までに業務を回復させるという一定の契約を締結しておき、予め各種回復手段を用意し、それに合せてバックアップ体制を確保するという対応も考えられる。

上述のごとく民間企業の一部では社会の要請に応じてサービスが存続できる範囲で高信頼化対策が講じられているが、これには企業のリスクマネジメントにより対策の上限が決まるため、コンピュータシステムダウンの際の社会的影響と比し、必ずしもその対策が十分であるとはいえない場合もある。

従って、コンピュータシステムのダウンにより、社会的に悪影響を起すものについては、単に企業の責任に任せず、一定の基準を決めてそ

の基準に合致するように義務付ける等の施策についても検討する必要がある。

なお、本施策を講ずるにあたっては、一定基準の対策が容易になるような補助的助成措置を講ずることも重要である。

第2章 コンピュータ犯罪防止対策

1. コンピュータリゼーションとコンピュータ犯罪

今後、コンピュータ・システムを中心とする情報処理システムは、経済・社会・生活の中枢神経としてあらゆる分野に浸透していくことが予想されるが何らかの要因によってその機能を停止したり、混乱が生じた場合、その経済・社会に与える影響は、はかり知れない広がりや深さをもつことになる。

我々の社会は、いまやコンピュータなしでは成りたちえないほどに多くの便益をコンピュータから享受している。しかし、今後の情報化の進展において問題が生じてくるならば、我々はそのような情報化の意義を厳しく問い直さねばならない。不断に人間とコンピュータの係わりあいについて考察し、健全な情報化社会の構築を目指し、コンピュータを真の幸福のために活用するようチェックしていくことは、情報化時代に生きる我々にとって不可欠の責務と考える。

1.1 コンピュータ利用に伴うリスク

コンピュータ利用に伴うリスクには、多種多様なものがある。しかし大きく分けると、災害と犯罪とに分類することができる。災害としては、地震、風水害、火災、エラー、施設不良、動物害、大気汚染などがある。犯罪としては、破壊、窃取、詐取、横領、機密漏洩、プライバシー侵害などが考えられる（第2-1表）。

第2-1表 コンピュータをめぐるリスク

大 分 類	中 分 類	小 分 類
災 害	地 震	建築物倒壊 ガス管破裂 水道管破裂 各種配線断線 通信回線断線 窓ガラス等破壊 室内機器倒壊 二重床破壊 クーリングタワー等倒壊 各種配管破壊 その他
	風 水 害	台 風 豪 雨 たつ巻
	火 災	コンピュータ室火災 コンピュータ火災 周辺端末火災 附属設備等火災 (配 電 盤 電 源 空 調 エアダクト そ の 他)

大 分 類	中 分 類	小 分 類
災 害	エラー	ビル火災 類 焼 隣接室 / 上下階火災 放 水 取扱不注意 設備点検不備 プログラム・ミス 操作ミス システム設計ミス
	施設不良	停電 電源機器故障 水道管、排水管等破損 排水不良 漏 水 上階出水 加湿機故障
	動物害	鳥 害 鼠 害
	大気汚染	大気汚染

大 分 類	中 分 類	小 分 類
犯 罪	破 壊 窃 取 } 詐 取 } 横 領 } 機密漏洩 プライバシー侵害	破壊行為 データベース、プログラム、 アウトプット・データ等の窃 取、詐取、横領 マシンタイムの盗用、 データベース、プログラム、 磁気記録等のコピー データベース漏洩 アウトプット・データの転写 による漏洩 その他 名誉毀損 人権侵害

1.2 コンピュータ犯罪とは

本研究会では、前述のように、コンピュータ犯罪をコンピュータ利用に伴うリスクの1つとして位置づけた。つぎに、コンピュータ犯罪を取り上げ、その対策を検討していくためには、対象範囲を限定することが必要であり、そのためにそれを定義することが望ましい。

本研究会は、コンピュータ・セキュリティのレベルを高め、健全な情報化社会を築くことを目的としている。そして、その一環としてコンピュータ犯罪をとりあげたものであるから、コンピュータに関連した犯罪を広く対象とし、コンピュータ・システムの脆弱性を克服する必要がある。

以上のような観点から、ここでは、コンピュータ犯罪を次のように定義して、調査研究を進めることとした。

「コンピュータ犯罪とは、コンピュータが直接的あるいは間接的に何らかの形で介在した社会悪行為である。」

このように調査研究対象を明確にして、以下、次の諸点について分析・検討を試みることとする。

- ① 日米のコンピュータ犯罪の現状を分析し、類型化をはかる。
- ② 現状における技術的、運用管理的な対策と、その問題点を考察する。
- ③ コンピュータ犯罪防止技術の今後の方向を模索する。
- ④ コンピュータ犯罪防止のための運用管理について、今後の方向を模索する。
- ⑤ コンピュータ犯罪防止のための法制的対応のあり方を検討する。

2 コンピュータ犯罪の現状と問題点

コンピュータ犯罪は、何らかの形でコンピュータが介在した犯罪であるから、当然、コンピュータ利用の進んでいる国で多く発生する。したがって、米国や日本でコンピュータ犯罪が多く発生するのは、ある意味では必然性があるといえる。

このようなことから、日本と米国のコンピュータ犯罪の現状を分析し、それを基に類型化をはかり、今後の問題点を明らかにする。

2.1 日本のコンピュータ犯罪

最初のコンピュータ犯罪は、1971年に発覚したリーダーズ・ダイジェスト事件である。これまでに発生したコンピュータ犯罪では、キャッシュカード犯罪が圧倒的に多く、今後とも増加する傾向にある。たとえば、80年には212件であったが、81年は288件と35.8%の急増ぶりである。

他方、81年のコンピュータ犯罪は、それ以前と比較して、著しくエスカレートしているといえる。特徴をあげると次のとおりである。

- ① 内部・外部の共謀（三和銀行事件）
- ② グループ犯行（北浜クレジット事件）
- ③ 二重帳簿作成（佐藤工業事件）
- ④ 長期繰り返し犯行（中野市農協事件、北浜クレジット事件）
- ⑤ オフコン犯罪（北浜クレジット事件）
- ⑥ マシンタイム盗用（鉄道建設公団事件、岡山大学事件）
- ⑦ 盗聴（北海道銀行事件）

以下、第2-2表にわが国の主なコンピュータ犯罪事例を示す。

第 2 - 2 表 わが国の主なコンピュータ犯罪

発生（または発覚）年	事 件	内 容	被 害
71年 2月	リーダーズ・ダイジェスト事件	日経ビジネス誌の購読者ファイルが何者かにコピーされ、リーダーズ・ダイジェスト社に売却された。	コピー売価 82万円
73年 3月	コクヨ事件	元社員が飲酒のうえコンピュータ室に侵入し、手あたり次第に暴れて機器類に被害を与えた。	
73年 4月	岡村製作所事件	事務係長が売掛金を架空口座に振り込ませ、取引先には正規の領収書を渡し、会社の経理には未回収のように見せかけて横領した。	4,000万円
74年 8月	オンライン誘拐事件	有名俳優の乳児が誘拐され身代金を第一勧業銀行の架空口座に振り込ませた。	身代金要求額 500万円
74年10月	三井銀行事件	富士銀行蒲田支店の行員が三井銀行で銀行オンラインを利用し預金通帳を偽造、架空口座に振替払込みを行う方法等により詐取した。	300万円
74年12月	キャッシュカード盗用事件	留守中にキャッシュカードが盗まれボーナスがそっくり引き出された。	56万円
74年12月	伏見信用金庫事件	事務本部の係長がサンプルカードを使ってキャッシュカードを偽造した。	200万円
75年 2月	三井銀行事件	堀留支店の行員が預金獲得した新規顧客のキャッシュカードを無断で作成し着服した。	650万円

発生(または発覚)年	事 件	内 容	被 害
75年 2月	間組事件	電算室に爆弾が仕掛けられ爆破された。	20億円(推定)
75年 5月	東天紅事件	人事係長が給与計算について退職者リストを抹消せず退職者分の給与を詐取した。	4,000万円
75年 6月	中国銀行事件	茶屋町支店の行員が3つの架空口座をつくり入金操作し横領した。	7,600万円
76年10月	北海道拓殖銀行事件	女子行員が残金457円の自分の口座に92万円の架空振込みを行い、CDから預金を引出した。	入金操作92万円 40万円引出し
77年12月	墨田区立保育園事件	コンピュータが故障して計算違いが生じたのでやり直すといって23人分のボーナスを持ち去る。	700万円
78年 3月	山形銀行事件	新庄支店の調査役が顧客の忘れたキャッシュカードを着服し暗証番号を調べて預金をおろす。	150万円
78年 5月	新日本製鐵事件	名古屋製鐵所で下請企業の役員が資材管理システムを悪用し、鋼材を横流した。	3,000万円
78年 6月	御牧農協事件	女子職員が夫と共謀して貯金払戻し伝票を偽造したり、架空の振替入金、虚偽解約等の手口で横領した。	8,500万円
78年 6月	チャリティプレート協会事件	銀行の貸金庫に保管していた協力者ファイルがコピーされ他の福祉団体に渡っていた。	
78年 7月	大丸神戸店事件	経理係長が架空の売買契約をでっち上げ契約解消に伴う前受金返却とい	3億3,000万円

発生（または発覚）年	事 件	内 容	被 害
78年10月	親和銀行事件	う手口で横領した。 住吉支店次長が大口預金者の口座から他行に開設した架空口座に振り込んだ。	1,500万円
79年 2月	オンライン誘拐事件	札幌市で児童が誘拐され身代金を、住友銀行の架空口座に振り込ませた。	身代金要求額600万円、20万円引出し
79年 9日	滑川市農協事件	女子職員が給与関係事務担当であることを利用し、架空口座を準備、コンピュータ処理の際エラーとなったものをこの口座に振込まれるよう偽造、架空伝票も偽造してオペレータに回し詐取した。	1,800万円
79年11月	山口銀行事件	徳山東支店の支店長と同代理が端末機をオフラインに切換えてニセ定期預金証書を発行。	発行額47億円
79年11月	西京コクヨ事件	女子社員が入金伝票を偽造し、自らコンピュータを操作して横領した。	1,000万円
81年 3月	宮城第一信用金庫事件	偽造キャッシュカードで4回にわたり預金が引き出された。	49万円
81年 5月	八戸信用金庫事件	偽造キャッシュカードで2人の口座から4回にわたり預金が引き出された。	92万円
81年 7月	常盤村農協事件	女子職員が顧客の口座から自己の口座へ振替入金があったように伝票を偽造して横領した。	800万円
81年 9月	三和銀行事件	オンライン端末機のオペレータが架	入金操作 1億8,000万円

発生(または発覚)年	事 件	内 容	被 害
81年 9月	中野市農協事件	空口座へ入金操作して詐取した。	1億3,000万円 引出し
81年 9月	日本鉄道建設公団事件	経理担当者が資材の代金支払伝票を偽造し兄弟や知人等の口座を借りて振り込んだ。	8,000万円
81年 9月	日本鉄道建設公団事件	係長ほか106名が高校野球をめぐり賭博を行い、カケ金と配当金計算に公団のコンピュータを使用した。	
81年10月	北浜クレジット事件	幹部が店長やプログラマを抱き込み9人のグループで横領。	1億2,000万円
81年10月	近畿相互銀行事件	元行員がキャッシュカードを偽造し顧客の口座から預金を引出した。	2,000万円
81年10月	平和相互銀行事件	電話でテストと称して行員をだまし入金操作を行わせた。	3,000万円
81年10月	岡山大学事件	マイコン・ショップが岡山大学のコンピュータにマイコンを使ってアクセスした。	盗用タイム 45時間
81年10月	キャッシュカード交換事件	銀行員を装いカードの更新に来たと称して交換し預金を引き出した。	31万円
81年11月	富士銀行事件	知らぬ間に預金が引き出された。	195万円
81年11月	佐藤工業事件	出水事故の水没補償費を二重帳簿を作成してごまかす。	1億6,000万円
81年12月	秋田相互銀行事件	女子行員が伝票偽造やコンピュータ不正操作で顧客の預金をつまみ食いついた。	600万円
81年12月	プロミス事件	自社と取引のある顧客データを盗み友人をその顧客に仕立てて融資を	融資申込み 38万円

発生(または発覚)年	事 件	内 容	被 害
82年 1月	羽合町農協事件	申し込んだ。 女子職員が顧客の普通預金口座から勝手に払戻し処理を行ったり、共済満期の掛金払戻金を自分の預金口座に振替える等して横領した。	560万円
82年 1月	大館市農協事件	女子職員が預金申し込みの際し、会計伝票を作成せず預金額を横領した。	1,500万円
82年 2月	北海道銀行事件	電電公社職員が通信回線からデータを盗聴してキャッシュカードを偽造し預金を引き出した。	133万円
82年 6月	郵便貯金事件	貯金口座をつくり入金し、それをオフライン局で引き出し、通帳を改ざんして、引き落としが行われる前に、オンライン局でも引き出した。	2,200万円

2.2. 米国のコンピュータ犯罪

最近、米国公認会計士協会が銀行・保険両業界に対して行った「コンピュータに関連する犯罪調査」によれば、銀行で85件、保険で34件の犯罪事例が報告されている。この調査では、次の諸点について注目すべき結果が出ている。

2.2.1 犯行手口

不正入力、及び入力データの改ざんが非常に多い。つまり、最もやりやすい手口であるといえよう。

犯 行 手 口	犯 罪 件 数	
	銀 行	保 険
不正または許可のない入力を持ち込むこと、操作することまたは許可すること	43	30
入力段階での入力の改ざん	30	2
コンピュータ処理中の改ざん	1	—
リジェクト処理での改ざん	2	—
出力の流用	1	—
データファイルの改ざん	4	1
不正使用のためのプログラムの改ざんまたは開発	3	—
ハードウェアおよびシステムソフトウェアの改ざん	—	—
不正または許可なくして情報にふれたりあるいは照会すること	1	1
合 計	85	34

出所：Report on EDP Related Fraud, AICPA

2.2.2 犯 罪 者

銀行については、一般事務員、事務管理職、データ入力係などが多く、保険では請求処理係、保険証書係などが多い。銀行において、管理職の犯罪が多いことを問題点として指摘できる。つまり、いろいろな場所に出入りでき、全体的な処理システムを知っており、犯行をうまくかくすことも出来る責任ある立場にある者が、その立場を利用した犯行であり悪質である。

銀 行 業		
職 種	件 数	
データ入力係	11	
入力検査係	5	
他の事務員	21	
事務管理職	17	
コンピュータ部門管理職	2	
金銭出納係	8	
データ処理オペレータ	7	
契約等文書処理オペレータ	6	
システムエンジニア、プログラマ	5	
そ の 他	3	
合 計	85	

出所：上に同じ

保 険 業		
職 種	件 数	
請求処理係	12	
請求処理監督者	3	
保険証書係	7	
保険証書係監督者	3	
他の監督者	3	
プロデューサ	3	
上級管理職	1	
コンピュータプログラマ	1	
会 計 係	1	
合 計	34	

出所：上に同じ

2.2.3 犯 行 期 間

大部分が1年以内に発覚しているが、一方では、銀行で23.5%、保険で29.4%が1年以上となっている。内部の者が犯行に及び、長く発覚しないと、繰り返し犯行につながる可能性が高く、被害額が大きくなる。

業 種	期 間	件 数
銀 行	1 カ 月 未 満	15
	1 ～ 3 カ 月	23
	3 ～ 1 2 カ 月	27
	1 年 以 上	20
	合 計	85
保 険	1 カ 月 未 満	4
	1 ～ 6 カ 月	11
	6 ～ 1 2 カ 月	9
	1 2 ～ 2 4 カ 月	6
	2 年 以 上	4
	合 計	34

出 所：上に同じ

2.3. コンピュータ犯罪の類型化

コンピュータ犯罪は、基本的に次の4つのパターンに分類することができる。

① 金銭の不法領得（窃取、詐取、横領）

② コンピュータ・システム及びデータ等の破壊

③ マシンタイムの盗用

④ コンピュータ関連資産の窃取

- ・ 有形資産（ハードウェア等）
- ・ 無形資産（プログラム、情報等）

2.3.1 金銭の不法領得に関する今後の問題点

金融機関のサービスの向上および業務の合理化は、今後ますます進んでいくものと思われる。その中で、一方では、顧客に直接操作させる形式の端末機が普及していき、他方、窓口係は伝票処理するとともに端末機をも操作するという単独処理が進んでいくものと思われる。このように合理化が進めば進むほど、従来の人手による業務処理体制の内部牽制は、次々に崩壊していく恐れがある。したがって、システムに何らかの方法で、これらの失われていく内部牽制に代替する機能あるいは別な方法で内部牽制を強化する機能を組み込んでいく必要がある。たとえば、チェック、監視、監査などの機能でうまく代替させることが望まれる。これは、何も金融機関に限った問題ではない。

同じようなことがオフィスコンピュータについてもいえる。オフコンは、ますます普及するものと思われるが、小規模コンピュータについては1人の担当者がすべてを処理することになる。つまり、コンピュータについて、たった1人のオールマイティをつくりあげてしまう。組織面、管理面からの対策も重視されなければならない。

2.3.2 システムおよびデータ等の破壊に関する今後の問題点

まず、政治的な目的をもって爆破するなどの破壊行為や、不平不満分子による破壊行為などは、将来ともに可能性がのこる。これについ

ては、防御措置を講じる以外にない。最も初歩的には、ビルの入口やエレベータ・ホールなどでのマシン室の表示を消すことから始めなければならない。そして各種の安全装置や設備の充実をはかり、定期的な点検、評価、あるいは見直しを実施する必要がある。

つぎに、端末機からのシステムやデータの破壊については、今後、我が国でも不安が大きくなると思われる。通信回線の開放にともない将来は公衆回線（電話回線）によるオンライン・ネットワークが、米国同様に利用できるようになると予想される。現在、我が国では、オンライン・ネットワークの広がりには緒についたばかりである。したがって、アクセス・コントロール、なかでも不正接続防止技術の開発を至急すすめる必要がある。

2.3.3 マシнтаイムの盗用に関する今後の問題点

これからのマシнтаイムの盗用は、コンピュータ・センタの要員が会社のコンピュータを使って他社の業務を処理しアルバイトをするといった類もあるかも知れないが、むしろこれからは公衆回線を使ったオンライン・ネットワークが増加するに従い、不当アクセスが心配される。しかも、同じ方法で、マシнтаイムの盗用も、情報の盗みも、システムやファイルの破壊も可能になってしまう。

一方では通信回線の開放が進み、他方ではコンピュータに拒絶反応を示す人が減少して行き、かつ、マイコン・ブームの主役を果たした少年層が次々と社会へ流入してくる。そして、コンピュータ・アクセス人口は毎年増加する。もはや、コンピュータを特別視する時代ではなくなった。

このような環境の中で、マシнтаイムの盗用が法律による取締りの

対象外におかれているとすれば、悪意をもって、あるいは面白半分でコンピュータ・システムへの不当なアクセスが頻発する可能性がある。したがって、マシンタイムの盗用を刑法で取締ることができるように法的措置が講ぜられるべきである。

2.3.4 コンピュータ資産の窃取に関する今後の問題点

コンピュータ有形資産の窃取については、これまで事件が発生しなかったが、コンピュータ自体がますますコンパクトになってきており、一方ではOA（オフィス・オートメーション）の進展で関連機器類も増加するであろうから、これからは可能性が高くなるといえよう。

無形資産の詐欺については、今後、最も脅威になると思われるのがプログラムや情報の盗みであろう。これらは、現物が盗まれることもあろうが、通常はコピーして盗まれブラック・マーケットに流れると見る方が妥当であろう。

米国では、すでに16州でコンピュータ犯罪防止法が成立しているが、有体、無体を問わず、コンピュータ・システム、プログラム、情報など、広い範囲で“財産”を定義し、これらの不法領得、破壊、盗用等を処罰の対象としている。また、カリフォルニア州やユタ州などでは、“財産”の定義の中でコピーを明記している。

たとえば、カリフォルニア州のコンピュータ犯罪防止法（刑法第502条）では、財産を次のように定義している。「財産には、人間ならびにコンピュータ・システム双方が読むことのできるデータおよび伝送中のデータを含め、有体であると無体であるとを問わず、商業証券、データ、コンピュータ・プログラム、コンピュータ・システムおよびコンピュータ・プログラムに関連する資料、またはそれらのコピ

ーを包含するが、それらに限定されない。」

つぎに、コピーなどではなく、磁気テープをそっくり盗み出したりコンピュータ室を占拠して脅迫するという大胆な手口も発生しないとはいえない。コンピュータが業務処理の中核神経的な役割を果たすようになった今日、発生すれば致命的ですらある。

ヨーロッパで発生したICI（インペリアル・ケミカル・インダストリーズ）事件では、企業の生命ともいえるべき磁気テープ（業務処理の内容そのものが記録されている。）がごっそり持ち去られ、それを盾に脅迫されたわけである。あたかも“情報”を誘拐して人質にでもしたような形で、情報の身代金でも要求したような光景すら感じられる。つまり、オンライン誘拐が発生するということは、その延長線上にこのようなこともあり得ると考えるべきであろう。

以上のようなことから、コンピュータ資産の窃取については、まず物理的な安全性や運用管理面について、定期的な検討・評価を実施する必要がある。つぎに、米国のコンピュータ犯罪防止法などを研究しわが国においても法律面からの整備に早急に取り組むべきであることが指摘できる。

第2-3表 コンピュータ犯罪の類型化と手口

分類	年	ケース（日本のみ）	不正インプット	不正目的への使用	盗聴	コピー	媒体ごとの盗み	キャッシュカードの盗み	マシンタイムの盗用	破壊行為	キャッシュカードの偽造	データ改ざん	伝票偽造	便益の悪用	架空口座の設定
金銭の不法領得（コンピュータを介した犯罪）	'74	オンライン誘拐事件													○
	'74	伏見信用金庫事件								○					
	'74	キャッシュカード盗用事件					○								
	'75	中国銀行事件													○
	'76	山形銀行事件					○								
	'76	新日鐵名古屋製鉄所事件	○										○		
	'76	大丸神戸店事件											○		
	'79	山口銀行事件		○									○		
	'81	三和銀行事件	○										○		○
	'81	中野市農協事件	○										○		
	'81	北浜クレジット事件		○											○
	'81	近畿相互銀行事件								○					
	'81	平和相互銀行事件	○												○
おとシステム等の破壊	'73	コクヨ事件								○					
	'75	間組事件								○					
マイシムの盗断（無断使用）	'81	鉄道建設公団事件							○						
	'81	岡山大学事件							○						
資産の窃取（コンピュータ関連）	有形資産	なし													
	無形資産	'71	リーダーズ・ダイジェスト事件			○									
		'78	チャリティプレート協会事件			○									
		'81	プロミス事件			○									
	資産	'82	北海道銀行事件		○					○					

3 現状における対策と問題点

コンピュータ犯罪対策は、技術的側面と運用管理的側面とに大別できる。そして基本的には、これらの技術と運用管理とをうまく組み合わせ、弱点をさらけ出さないようにすることが重要である。現状は必ずしも十分ではなく、より一層の充実が望まれる。

3.1 技術的対策

過去に発生したコンピュータ犯罪から、どこに弱点があり、犯罪防止のためにどのような機能が要求されるかなど、前述の手口を参考に代表的な手口を5つに集約し、その技術的な対策と問題点を次に述べる。

3.1.1 破壊およびデータ媒体窃取対策

主にビルや室の管理など、運用の問題がある。最近では、入退室管理システム、TVモニタ、遠隔制御、さらにコンピュータによる総合ビル管理システム等が開発され、運用管理を技術面からサポートできるようになってきている。

3.1.2 コンピュータの不正使用対策

直接、あるいは通信回線を介して、コンピュータを不正に使用する犯罪を防止する必要がある。これについては、アクセス・コントロールが重要な機能を果たす。現在のOSはパスワードなどによる本人確認、ユーザ・プロフィールによるリソースやOS機能の管理、アクセス・モニタリングやコンソール・ログによるアクセス履歴の記録などができる。

これらの機能を十分に活用すれば、コンピュータ犯罪に対してかなり有効に作用するものと思われる。しかし、一方では、パスワードが

盗まれると手の打ちようがないことや、オンライン・システムの通信回線をめぐる盗聴防止・不正接続防止など、課題は多い。

3.1.3 情報窃取、情報破壊対策

コピーして、あるいは通信回線を介して、プログラムや情報が盗まれたり、破壊されたりすることを防止しなければならない。これについては、アクセス・コントロール、データ保護、暗号化などが有効に作用する。しかし、暗号化については、鍵の管理をめぐる問題などがまだ解決されていない。

3.1.4 不正入力対策

偽造伝票などにもとづく不正入力については、それをコンピュータ・システムで正しいか不正かを判断するのが非常に難しい。ある程度は技術的対策も可能であるが、管理面も含めた総合的な対策が必要である。

3.1.5 プログラム改ざん対策

プログラムを不正に改ざんする犯罪は、多発するとは思えないが、仮に発生すれば発見することが非常に難しいと考えられ、長期間にわたる被害の大きな犯罪になる可能性が強い。しかも、現段階においては、全面的に運用に依存せざるを得ない面が問題である。

3.2 運用管理的対策

通産省で策定した「電子計算機システム安全対策基準」の活用や、システム監査の導入などが求められる。具体的には、次のような事例がみられる。

3.2.1 情報処理サービス業における安全対策

A 情報処理サービス会社では、通産省が77年に策定した「電子計算機システム安全対策基準」を参考として、設備および運用管理面の安全対策を実施している。また、通産省が81年に「情報処理サービス業電子計算機システム安全対策実施事業所認定制度」を発足させたのに伴い、従来の安全対策状況に改善を加えて認定を受けた。

同社は、社内に安全対策委員会を設置し、安全対策マニュアルを作成している。このマニュアルは、全部門に配布され、要員の教育訓練や監督のためのガイドラインとしていかされている。安全対策の主な事項は、機密保持、文書管理、ビル入退室管理、マシン室管理、コンピュータ運用と障害対策、入出力データ取扱い、磁気ファイル管理、コンピュータ関連設備の運用、巡回監視、災害対策、委託業務管理などで、それぞれマニュアルで具体的に規定している。

3.2.2 銀行における安全対策

B 銀行では、システム開発段階から運用に至るまでを対象としてシステム監査を実施し成果をあげている。

まず、システム開発監査では、開発部門で作成したシステム設計書をもとに、業務処理の正確化と不祥事防止を中心として、システムの内容調査を行っている。たとえば、ハードウェア、ソフトウェア面については、持つべき機能が充足しているか、データの正確性や不正データ排除のチェック機能が組み込まれているかなど、事務的手続きおよび帳票については、ソフト、ハードでカバーしきれない手作業面のチェック事項が明確にされ、相互牽制機能を持っているかなど、また、異例取引きその他、監査に重要なデータをアウトプットする機能を持っているかどうかなどが、システム開発監査の重要ポイントになっている

る。

システム運用監査については、システムが多種かつ膨大なため、弱点として表面化する誤処理やコンピュータ犯罪事例をもとに、関連するシステムを見直す方法をとっている。

4. コンピュータ犯罪防止技術の方向

コンピュータ犯罪を防止するための技術としては、いろいろなものがある。これらの中には、コンピュータ・システムの安全対策として積極的に導入・普及すべき技術が多い。

しかし、一方では、拡大・高度化しつづけるコンピュータ・システムに対して、さらに、もう一段の前進が要求される技術がある。それは、アクセス・コントロール技術、データ保護技術、暗号化技術などに代表される。今後これらの技術開発を強力に推進する必要がある。

4.1 アクセス・コントロール

アクセス・コントロールは、ユーザがコンピュータ・システムにアクセスする時点で、正しいユーザであるかどうかをコンピュータ・システム自体で検証させる機能である。

4.1.1 本人確認技術

IDナンバーやパスワードのほかに、次のような新しい本人確認技術の研究も進められている。

- ①指紋照合技術：指紋の特徴を照合し確認する技術
- ②声紋判定技術：声の周波数成分を分析し判定する技術
- ③サイン判定技術：サインの特徴を抽出し判定する技術
- ④手形照合技術：手の面積、大きさ、指の長さ、太さなどにより認識する技術

4.1.2 通信回線における不正接続防止技術

専用回線については、接続する端末機が固定されるため、回線への不正接続はかなり難しい。公衆回線（電話回線）の場合は、電話番号

さえわかれば誰でも自由に接続できるため、不正接続が起りやすい。

電電公社のDDX（デジタル通信用に新設したサービス）では、相手先通知（接続しようとしている相手先アドレスを通知する機能）や閉域接続（端末のアドレスをDDXの電子交換機に登録する）により、不正接続などを締め出している。

4.1.3 ユーザ・プロフィール管理技術

これは、ユーザごとのシステムに対する使用权、あるいはリソースの範囲を管理する技術である。すでに商品化されており、ユーザ管理機能（ユーザ名と属性およびシステム使用权の管理）とリソース管理機能（ユーザごとの利用可能なファイルの管理）が含まれる。

4.1.4 アクセス・モニタリング技術

ユーザのコンピュータ・アクセスの記録をとる技術で、不正アクセス・モニタリング、システム・モニタリング（正しいアクセスのモニタリング）、コンソール・ログの3つの機能に分れる。

4.2 データ保護技術

今後、開発を必要とするデータ保護技術としては、次のようなものがある。

4.2.1 データベース領域の縮限

ユーザ・データベースにアクセスする場合、通常は検索言語を使用することが多い。しかし、ユーザが作成する検索文が示すデータベース領域は、そのユーザがアクセスすることを許されている領域と必ずしも一致しない。セキュリティ上からは、許されている領域のみを検索させるコントロールが望ましい。

4.2.2 フロー制御

機密レベルの高いデータほど、不当に外部へ流出してはこまる。一般的には、機密レベルの低いデータほど外部に流出しやすい。このため、コンピュータ・システム内をデータが流れる際に、データが機密レベルの低い方向に流れるのを防ぐコントロールが必要である。

4.2.3 推論の制御

たとえば、データベースをTSSで利用するような場合、正当な検索の質問を組み合わせることにより、本来秘密にされているべきデータが質問者の手に渡る可能性がある。これは、質問で得られた回答から、まったく関連のないデータが推論される場合に起こる。こうした推論を困難にするように質問に規制を設けることなどが必要となる。

4.3 暗号化技術

わが国でも、初の盗聴事件といわれる北海道銀行事件以来、暗号化がにわかに現実の問題としてクローズアップされてきた。しかし現在、暗号方式を導入しているシステムは非常に少なく、米国においても、わが国でいわれているほど普及はしていない。本格的に導入されない理由は暗号方式にはまだ解決されていない問題点が多く残されているからであろう。

主な問題点としては、次のようなことをあげることができる。

- ・暗号方式導入の必要性、効果がより明確にされねばならないこと
- ・高価であること
- ・鍵の配送・管理が繁雑であること
- ・処理能力に影響を与えること

問題点が解決されれば、暗号方式が有効な手段になることは、疑いないところであろう。今後さらに研究が進められ、より効果的な暗号方式が開発されることが望ましい。そのためのポイントとなることは、次の諸点であろう。

- ・暗号強度をより高くし、解読不可能にすること
- ・経済的にユーザが導入できるコストとなること
- ・暗号化、復号化において、システムへの負荷が小さいこと
- ・鍵の管理が容易であること
- ・誤りの影響度が少ないこと
- ・現行システムにスムーズに導入できること

暗号方式の基本は、換字、転字、または双方の組み合わせであり、主な種類を紹介する。

4.3.1 換 字 方 式

文字を別の文字に置き換える方法。置き換え方により次の種類がある。

(a) コードブック方式

各文字ごとに、置換される文字の対応表をあらかじめ作成しておく方法。この対応表が鍵となる。

(b) シーザ方式

文字を一定数だけずらす方法。必然的に鍵の数が少いため、全数検査により完全に解読可能である。

(c) ビジネル方式

シーザ方式の鍵を周期的に変化させる方法。変化させる周期を大きくとることにより、暗号強度を高めることができる。

(d) バーナム方式

ビット対応に排他的論理和をとる方法。ワシントンとモスクワ間のホットラインで使用されている。暗号強度は高いが非効率である。

4.3.2 転置方式

文字の位置を換える方法。暗号化された後も、出現率の高い文字はそのままの出現率を有するが、暗号強度はコードブック方式より高いといわれている。

4.3.3 混合方式

換字方式、転字方式を組み合わせた方法。この方式の代表的な例はDES (Data Encryption Standard) 方式である。DESは、米国商務省標準局が、1973年にデータ暗号規格を公募した際に採用されたもので、IBMの提案した方式である。

DESは、平文を64ビット単位のブロックに分け、これを64ビット (8ビットはパリティビット) の鍵を用いて換字・転字を16回繰り返す。

4.3.4 公開鍵方式

DES方式における鍵管理の繁雑さを解消するために考案された方法。これは、1976年に、Diffie と Hellmanによって考案された概念で、系の加入者に対する暗号鍵は電話帳のようなものに登録・公開しておき、復号鍵は秘密にしておく方式である。

(a) RSA法 (Rivest, Shamir, Adleman)

素数の判定は比較的容易であるが、素因数分解は非常に手間がかかることを利用した方法。

(b) MH法 (Merkle, Hellman)

ナップザックベクトルを利用した方法。ある慎重に選んだナップザックベクトルに関して、その逆を計算することは、仕組まれた落とし戸を知らない限り非常に難しい。

(e) R 法 (Rabin)

二次不定方程式の解を一般的に求めるのは困難であるのに対して、素因数分解した値が明らかならば方程式の解が容易に求められることを利用した方法。

4.3.5 MIX方式

郵政省が1982年6月に発表した方法で、データ暗号鍵を公開鍵方式で暗号化し配送した後、データの暗号化はDES方式で行われる。

4.4. その他の技術

コンピュータ犯罪防止技術で、以上のべたほかにも、次のような分野で各種の技術がみられる。

- ① 接近の防止：赤外線感知器、超音波検知器、モニタテレビカメラ、磁気検知、ビル総合管理システムなど
- ② 隔離：通信回線の埋設、耐火金庫、コンピュータ専用ビルなど
- ③ 鍵：オペレータ・キー、オーディタ・キーなど
- ④ データの無効化：消磁など

これらの中でも、とくに機密性の高い情報については、無効化も有効な対策になり得よう。たとえば、保管している磁気テープに特殊なラベルを貼っておき、その磁気テープが盗み出される場合には、出口に設置してある感知器がラベルを感知し、強力な磁力で内容を消去してしまい情報の流出を避けることができる。

第2-4表 コンピュータ犯罪防止技術一覧表

防止技術 防止対策		ハード	OS	アプリケーション	その他技術
ハードウェア	CPU	鍵、ハードウェア アドレス	PSW, ICP, UP, AM	PSW	PP
	周辺ディスク	IDカード、鍵	PSW, ICP, UP, AM	PSW	PP
	端末末	IDカード、鍵	PSW, ICP, UP, AM	PSW	
	通信機器		PSW, ICP, UP, AM	PSW	埋設(マンホールふた 接着) PP
	媒体				コンピュータバックアップ センター、耐火室、金 庫、電磁遮蔽、PP
ソフトウェア	OS	メモリ保護	PSW, ソフトウェア鍵 ICP, UP, AM	PSW	
	アプリケーション	メモリ保護	PSW, ICP, UP, AM	PSW	
データ	ファイル	暗号	PSW, DB保護, ICP Vol Ser No, UP 暗号, AM, RAC	PSW, 暗号 DB保護, ソフトウェア鍵	
	メモリー	記憶保護ストレージ (主記憶キー)	PSW, ソフトウェア鍵 ICP, 暗号, UP, AM		
	通信回線	暗号		PSW, 暗号	
	出力情報			ユーザ情報の記号化	PP, シュレッダー
付帯設備					ビル総合管理システム ID, 二重化, 予備機 PP

(注) PSW: パスワード

ICP: 不正接続防止

UP: ユーザ・プロフィール管理

AM: アクセス・モニタリング

RAC: リソース・アクセス・コントロール

PP: 物理的保護(防火、防水、防爆、侵入防止等)

Vol Ser No: 媒体通番

5. コンピュータ犯罪防止のための運用管理の方向

コンピュータ犯罪を防止するためには、新技術の開発も重要であるが、あくまでも、コンピュータ・システムの運用管理体制が充実していることが基本である。とくに重視されることは、組織・人事・教育訓練などの社内の管理体制の充実と、システム監査の導入である。そして、これらの充実を促進させるために、制度面で行政の対応が望まれる。

5.1. 運用管理面での対応

5.1.1 組織体制

コンピュータ利用はますます普及し、一方では高度化・大規模化・分散化など、管理面からみてもますます複雑になってきている。このような中であって、現在の組織体制では、コンピュータ・システムの運用管理で、必ずしも十分ではない面が出てきている。システムはダイナミックに変化しているが、組織は固定しているといった状況の弊害が出てきているようにも見受けられる。

コンピュータ犯罪防止の観点からは、とくに職務権限の分割の適正化をはかることが望まれる。合理化をはかり、コンピュータ処理の自動化も進み、処理能力が拡大するにもかかわらず、コンピュータ要員は少くなるという傾向の中では、従来の人手による処理の場合に保たれていた内部牽制が次々と失われつつある。この失われつつある内部牽制をもう一度見直し、その機能を何らかの形態で残すよう再検討する必要がある。効率化をはかることは当然のことであるが、失ってはならない体制まで消滅させている場合には、強い警告を発せざるを得ない。

5.1.2. 人 事 管 理

コンピュータ犯罪防止の観点からは、人事管理の適正化も重要な要素となる。たとえば一つのポジションに同一人物が長期間とどまることにより弊害が出るとすれば、そこにはローテーションが有効である。しかし、ローテーションは、専門化志向とは相反する一面をもっているため企業の特長、方針に照らして慎重な運用が必要なことはいうまでもない。

他の観点からのべれば、コンピュータ犯罪防止対策としては、不平不満分子を生み出さないこと、特定部門においてオールマイティをつくらないことなどを、人事管理面で配慮していくことが必要であろう。

5.1.3 教 育 訓 練

犯罪を犯すのは、あくまでも人間である。しかも、倫理観の欠除が問題にされている。とくにコンピュータ関連については、比較的新しい業務であるから、職業倫理が確立されていないと指摘する向きもある。一方では、業務の重要度に対して、業務が機械化され標準化されることにより単純化し、そのアンバランスが目立つ業務も見受けられる。つまり、重要な業務に対する態度が安易になってしまう傾向にあるようにも思われる。

コンピュータ業務従事者の教育訓練は、コンピュータに関する技術的な専門教育などを実施するのは当然のことながら、それぞれの業務の重要性を教えることや、職業倫理についての教育を施す必要がある。

さらに、今後は学校においてもコンピュータが取り上げられていくことから、学校教育における倫理教育を含むコンピュータ教育の重要

性が増大すると考えられる。

5.2 システム監査での対応

5.2.1 システム監査の導入

今日、システム監査の必要性が叫ばれているが、実際には大企業を中心に導入されているにすぎない。システム監査は、全てのユーザが導入し、実施することが必要である。このためには、まず、トップ・マネジメントがシステム監査の重要性を認識しなければならない。

5.2.2 システム監査人の養成

システム監査を実施するには、システム監査人を置く必要がある。システム監査人の養成には、監査人にコンピュータ教育をする方法とコンピュータ専門家に監査教育をする方法があろう。養成に長い時間をかけられない場合には、コンピュータ専門家に監査教育を施してシステム監査人を養成した方がはるかに早い。

内部監査部門が設置されていない企業については、プロジェクト・チームを編成してシステム監査を実施する等の工夫をすることが必要である。

5.3 行政の対応

コンピュータ犯罪防止のための運用管理については、十分な徹底をはかるため、行政に期待される部分も大きい。必要性が認められることに対しては、あらゆる努力をすべきであろう。

5.3.1 電子計算機システム安全対策基準の見直し

この基準が策定されてすでに5年が経過している。この基準は、ガ

イドラインとして策定されたものであるが、これを見直し、検討するとともに、追加、修正等して、広く一般に活用できるよう普及させることが望ましい。

5.3.2 システム監査のガイドラインの策定、教育、及び技術開発の促進

全てのコンピュータ・ユーザにシステム監査を実施させるよう、政府がシステム監査のガイドラインを策定することが望ましい。内容的には、ユーザがどのように対応したらよいのか、その拠り所となる基準を示すべきである。

つぎに、システム監査を正しく理解させ、広く普及・定着をはかるためには、時間はかかるかも知れないが、大学教育で「システム監査論」講座を開設するのも一方法であろう。

また、コンピュータ・メーカは、コンピュータの提供に際して、各種のシステム監査ツールなども提供可能な状態であることが望ましい。したがって、政府は、コンピュータ・メーカに対してシステム監査ツールの開発に取り組むよう指導し、必要性が認められれば助成すべきである。

5.3.3 コンピュータ犯罪情報センターの設置

コンピュータ犯罪に関する情報を収集・分析し、その防止に役立てるため、コンピュータ犯罪情報センターを設置して、本格的に研究を進め指導にあたることも考えられる。

6. コンピュータ犯罪防止のための法制的検討

6.1 コンピュータ犯罪と現行法制

本研究会において、コンピュータ犯罪をその性質・手口などから

- ① 金銭の不法領得（窃取、詐取、横領）
- ② コンピュータ・システム及びデータ等の破壊
- ③ マシンタイムの盗用
- ④ コンピュータ関連資産の窃取

⑦有形資産、⑧無形資産（コピー含む）

の4つに類型化した。しかし、我が国でこれまでおきたコンピュータ犯罪のほとんどは三和銀行事件に代表されるように、①の金銭の不法領得を意図したものが多く、とりわけその中でもキャッシュカード犯罪が大勢を占めている。警察庁調べによれば1981年の犯罪発生件数は288件を数えている。これらは刑法でいえば、窃盗罪（刑法235条）、詐欺罪（刑法246条）及び横領または業務上横領罪（刑法252、253条）のどれかに、あるいはその2つ以上にまたがって該当するということで法解釈上は問題はない。

次に、我が国では、間組事件で知られる②コンピュータ・システム及びデータ等の破壊については、建造物・器物損壊罪（刑法260、261条）が適用されよう。また、我が国においては摘発の類例がない④コンピュータ関連資産の盗みについては、窃盗罪が適用されよう。しかし、これらの解釈については問題がないわけではない。②における「データ等」④の⑧における「コンピュータ関連資産」の中にはプログラムなどのソフトウェア、磁気テープ、磁気ディスク、磁気ドラムなどの電磁的記録

物が含まれるからである。ソフトウェアの場合ではそれを「財物」と看做しうるか否か、電磁的記録物の場合はその文書性が刑法を解釈、適用するうえで問題となる。ソフトウェアについては、その財産的価値は認められているものの、「財物」としては法的にはまだ認められておらずその直接保護のための一般的な刑罰法規はない。また、個人データなどの保護のための一般的な法規もないが、電磁的記録物についてはそれ自体直接視覚に訴えることができないものの、これをプリントアウトすれば視覚可能な文字や符号となり、一般的な文書と同様に扱うと解される。この場合は、例えば端末から通信回線を通じて、データを抹消する行為に対しては、公用文書毀棄・私文書毀棄罪（刑法258・259条）が適用可能であり、またプログラマが作成依頼人、作成名義人の指示と異なるプログラムを組んでデータを入れたり変えたりする行為やプリントアウトする権限のない者がプリントアウトする行為に対しては、その内容が「権利、義務又は事実証明に関する文書若しくは図画の偽造または変造」にあたる限りにおいて、私文書偽造罪（刑法159条）が適用されると解釈されている。

この考え方は、近畿相互銀行事件のキャッシュカード（キャッシュカードの磁気ストライプのデータの入力、変更も同様に視覚可能な文字、符号に再生できる）偽造を私文書偽造罪と認めた本年9月9日の判決で支持されたと考えてよい。

他方、これらの見解に対しては、私文書偽造罪の客体としての文書は観念または意志の表示物に限られるとし、電磁的記録物は録音テープなどと同様に文書にあたらないとする見解もある。この立場からは電磁的記録物を保護するために新しい立法が必要となる。

4つに類型化された犯罪のうち、以上述べてきた部分については内容の解釈に若干問題があるものの一応刑法によって担保されていることを明らかにした。しかし、問題はまだ解決されていない。③のマシントイムの盗用（無断使用）、④の①の無形資産（コピー含む）の盗みについてはこれを処罰する刑罰法規がないからだ。

後者については代表的なものとして、リーダーズ・ダイジェスト事件、チャリティプレート協会事件があげられる。この2つの事件は両方とも顧客ファイルがコピーされたものであるが、顧客ファイル自体が盗まれたわけではないから、窃盗罪の適用は困難とされ、両事件とも最後は示談で収拾されている。もう一つかなり様相の異なった事件として、電電公社職員が通信回線から情報を盗聴し、その情報を使ってキャッシュカードを偽造して預金を引き出した北海道銀行事件があるが、この犯人は窃盗罪で逮捕されているものの、情報の盗みについては刑事責任を追求されていない。前にも述べたように情報それ自体は刑法的保護の対象とされていないことによる。

結局、無形資産の盗みとマシントイムの盗用については現行法上は処罰規定が存在せず、民法709条における不法行為に対する損害賠償をもって民事的に保障されているものの、コンピュータ犯罪防止の観点からは実質的には無防備の状態といつてよい。

なお、アメリカにおいては、ビル・ネルソン下院議員がコンピュータ犯罪防止法の連邦法案を下院に上程中であり、まだ成立をみていないが州法の方は現時点で16州において法案の成立をみている。これらを見ると、保護対象として、「Property（財産）」ということばを使っており、これは何らかの価値あるものを言い、かつ、有体及び無体財産、

電子的に処理され、製作されもしくは記憶されたデータ形態における情報、またはそれらに関する何らかのデータ処理表示、及び、サービスを包含する。また、イリソイ州法のように、この定義を踏まえた上で、

「所有者の承認なしに、⑦故意にコンピュータ・システムやその一部を利用した場合、及び⑧プログラムまたはデータを故意に改変、損壊した場合、⑨コンピュータ・システムの所有者または第三者から金銭、財産またはサービスを領得せんと目的での欺罔行為（a deception）の一部として、コンピュータ・システムまたはその一部を故意に利用し、改変または損壊した場合」を、すべてコンピュータ犯罪として、処罰の対象とし、マシンタイムの盗用、情報の窃盗、データ破壊など前掲の4つの類型化に対する刑法上の手当をすべて整えているとみられるところもあり、カリフォルニア州やユタ州のように「財産」の定義の中に「コピー」を明記しているところもある。

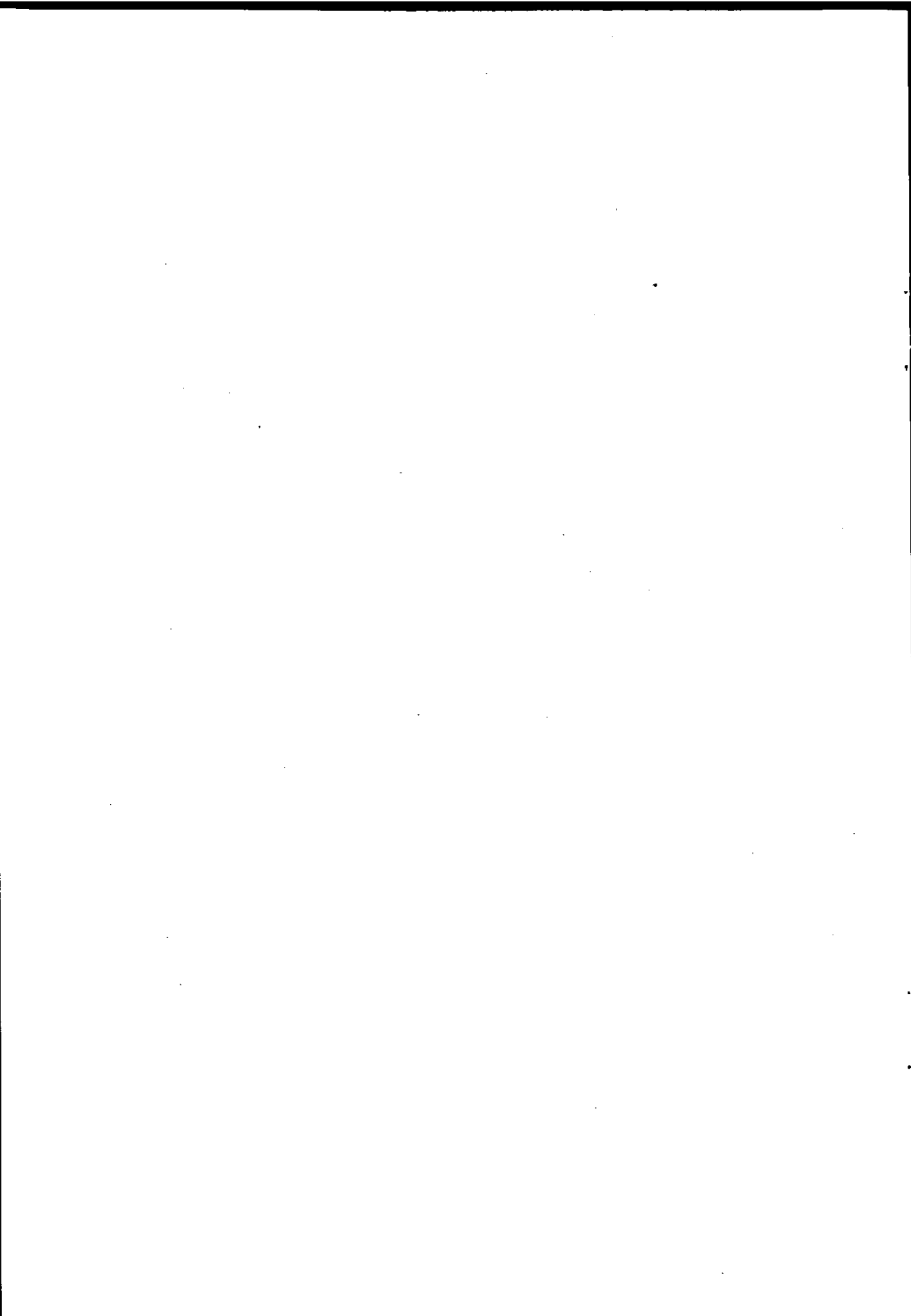
6.2 今後の法制的対応の方向

近年の著しい情報化の進展、特にオンライン情報処理の進展により通信回線の開放が各方面で強く叫ばれ、実現しつつあるが、これにより、コンピュータ処理の分散化も同時に進行しようとしている。これに伴いまた半導体技術の進歩によるハードウェアの小型化、低価格化も手伝ってシステムに占めるソフトウェアの比率は増大し、ここに至ってソフトウェアの増勢を抑え、ソフトウェアの役割をハードウェアで代替させようとする動きさえみられる。これらの事情を反映して、かつて心配されたソフトウェア・プロダクトのソフトウェア市場における流通も次第に促進をみ、ソフトウェアの財産的価値も着実に上昇し、いまや十分財産的取

引の対象となってきた。

また、情報化の進展により、コンピュータが産業・社会・生活のあらゆるところに広く深く浸透している。これにより、従来文書の形態で存在した各種の記録や書類の保存が、磁気テープ、磁気ディスク、磁気ドラムなどの電磁的記録物の形態に変わったが、これについても単に存在形態が変わっただけで財産的価値に変わりはない。

従って今後の方向としては、プログラム・情報（データ）等の財物性を肯定する方向での刑法改正を目標とすべきであろう。しかしこれは、現状として今すぐというのは困難であるため、当面の立法論としては例えば、改正刑法草案 318 条において、企業秘密の保護と併せてこれらの保護を一緒に考える方法がある。現在の草案はあくまでも財産的価値をもつ資産としての秘密を保護するという面が強いので、むしろコンピュータ・システム一般を保護するという、より高次の政策的見地から総合的な法的検討を加えていくことが必要と思われる。さらに将来的には、情報化の今後の進展具合、状況の変化を十分見極めながら、独立法規としてのコンピュータ犯罪防止法を検討していく必要がある。



第3章 データ保護対策



1. データ保護の必要性

① 近時、コンピュータ利用の高度化、広汎化に対応して大量のデータの蓄積、広汎迅速な処理、拡散が可能となってきた。

また、これに応じコンピュータシステムに企業活動や社会生活が大きく依存している実態が生じてきている。

② かかる傾向に伴い、悪意又は過失により、企業秘密に関するデータが破壊、悪用されたり、プライバシーが侵害されたり、さらにデータの侵害あるいは災害等により、社会的に重要なシステムの安全運行上支障を生ずるなどの危険も増大している。

③ また、一般国民の中には、かかる情報化の進展に莫然たる不安感を持つ者も少なくないことも事実である。

④ このような状況にかんがみ、現在制度的に何の対策も行われていないデータ保護について所要の対策を行い、情報化に係る一般国民の不安を除去し、情報処理に係るユーザの保護を図るとともに、広い意味での情報産業の振興を図り、健全な情報化の進展を促進する必要がある。

2. データ保護の目的

以上の観点から、データ保護の目的は、究極的には、健全な情報化の進展にあるが、一義的には、次の3つに整理できよう。

① 企業秘密の保護

② プライバシーの保護

③ 社会的に重要なシステムの安全運行

3. 保護すべきデータの範囲

保護すべきデータの範囲を上記の目的別に整理するならば、次のとおりに考えられよう。

3.1 企業秘密の保護

データのうち、何が保護に値する秘密であるかは、第三者にとっては判断しかねるところである。従って、客観的に判断し得る明確な基準を検討することが重要であるが、当面、保護の態様については強弱あるものの、法人に特定できるデータは全て一義的に保護することが適当であろう。

3.2 プライバシーの保護

データのうち、何が保護に値するプライバシーに関わるものであるかは、第三者にとっては判断しかねるところである。また、プライバシーの定義については、今だコンセンサスが得られていない状況にあり、最も広義に、「自分に関する情報を自分でコントロールする権利」として解釈するものもある。従って、プライバシーの定義、データのうちプライバシーに係るものとして何を保護すべきかという客観的基準を検討する必要はあるが、当面、個人に特定できるデータは全て一義的に保護することが適当であろう。

3.3 システムの安全運行

医療、鉄道、航空等公益的性格をもつシステム、金融等経済活動に直接影響を与えるシステム等社会的に重要なシステムにおいては、システムに係るデータ及びソフトウェアの破壊、改ざん等は、致命的な障害となり得る危険がある。従って、このようなシステムに係るデータ及びそのソフトウェアは、その機密性の有無に係わらず、保護されなければならない。

4. データ侵害の態様及び主体

データの侵害の態様としては、次のようなケースが考えられる。

- ① 故意又は過失に基づく企業秘密に係るデータの破壊、紛失、流用、窃取、改ざん
- ② 故意又は過失に基づくプライバシーに係るデータの窃取、紛失、流用、改ざん
- ③ 故意又は過失さらには災害等に基づく社会的に重要なシステムの安全運行上又は事業運営において重要なデータの破壊、紛失、改ざん

また、侵害の主体としては、オペレーター等データを正規に取扱うことのできる内部の人間、不法にアクセスしてかかる行為を行う外部の人間、更にその両者の共同行為という3通りに整理でき、その他に災害等によるデータ破壊がある。

5. データ保護対策の考え方

以上のようなデータ侵害の態様から、対策については次のような考え方ができる。

データ侵害は、人間により行われるものであり、究極的には、データ保護に関する認識の程度に依存するところも大きい。

従って、その対策は、

- ① 技術面から、
 - (a) 信頼性の向上を図る。
 - (b) 機械化の範囲を広げ、人の接触する部分を極力少なくしていく。
 - (c) 災害等から守る。
- ② 制度面から、

- (a) 社会的にデータ保護に係る認識を覚醒していく。
- (b) データ侵害に関する社会的制裁を制度化する。
- (c) 保護すべきデータを取扱う者にデータ保護のための合理的対策を義務づける。

という方向で整理できる。

6. 具体的対策

6.1 技術面における対策

データ保護に関し、ハードウェア、ソフトウェア両面にわたり、技術開発、普及促進を急ぐ必要がある。

開発を急ぐべき技術について、その詳細を述べることは、第1章および第2章の内容に重複するので、簡単にそのアウトラインのみ紹介することとする。

一応の分類として、システムの信頼性を高める高信頼化技術、システムへのアクセスを制限、管理するアクセス・コントロール技術、情報を伝送する際のデータ侵害を防止する暗号化技術、不正接続防止技術等の分類ができる。

6.1.1 高信頼化技術

(i) ハードウェア

基本的には、部品、設計、製造各段階における信頼性向上策が考えられるところである。

まず、部品段階では、当然のことであるが、信頼度の高い部品を利用することが重要である。

次に、設計段階では、デザイン・オートメーション・システムの導入による機械化の促進が対策の方向として考えられよう。

更に、製造段階では、自動化を一層促進するとともに、検査基準を厳密化し、信頼性を高める必要がある。

(ii) ソフトウェア

ソフトウェアにおける対策としては、デザインレビューの強化、高信頼化プログラミング等が考えられるほか、いったん事故又はデータ侵害が起こった場合に、その原因、侵害者等をトレースすることのできるソフトウェアの開発等が考えられよう。

6.1.2 アクセス・コントロール

現在もかなり普及しつつあるが、IDカード等の二重三重の入退室管理システムの強化、アクセスする際に指数、声紋等で判定を行う本人確認技術の開発・普及、アクセスの記録を自動的に蓄積し、アクセスした人間を判断することが可能なアクセスモニタリング技術の開発、普及が要請される。さらに、そもそもアクセスできる人間を限定する資源アクセス管理技術、ソフトウェア・キーなどの開発、普及促進が考えられよう。

6.1.3 暗号化技術

情報を伝送する際に一定の暗号にかえ、伝送する技術は、発想としては古く、現在までにかなりの方式が考案されている。

かかる技術開発を考えることは、今後とも重要なことであるが、ハードウェアに対する負荷が大きく、処理能力への影響が大きいことなどの問題もある。

以上代表的技術について例示したが、かかる技術開発、普及促進に当

たつては、コスト等種々の問題があり、開発体制を含め検討を要する。

6.1.4 コンピュータシステム設置環境

自然災害、破壊活動からデータを保護するためには、建築物の環境条件、建築物の構造、コンピュータシステム室及びデータの保管室の環境条件等を整備しておく必要がある。

6.2 制度面における対策

6.2.1 データ保護に係る認識の覚醒

データ侵害を防止するため、データ保護に係る認識を覚醒していくとともに、データ保護に止まらず、情報化促進のためのパブリック・アクセプタンスを形成していくことが不可欠である。

そのためには、第一に、国民の情報化に対する正しい認識を涵養するための広報事業が強力に推進されなければならない。

我が国においては、1972年から毎年関係省庁の協力のもとに「情報化週間」が開催されており、本年からは、「情報化月間」として拡充されたところである。かかる行事を利用してデータ保護に対する認識を深めるため、幅広い活動を行うことが望まれる。

第二に、学校教育、社会教育など広汎な教育の場において、データ保護に係る認識を深めるための教育を充実させる必要がある。このひとつの端緒として、「情報処理技術者試験」等の設問としてデータ保護に関する出題を加える等の方策が考えられよう。無論、かかる出題のためには、データ保護に関する技術の標準化等も考えていかなければならない。

更に、情報処理技術者試験の拡充とともに、「システム監査士」、「データ安全管理士」等の資格創設も考えられよう。

6. 2. 2 データ侵害に対する社会的制裁

故意又は重過失に基づくデータ侵害を防止するため、データ保護に関する社会倫理の醸成に伴って、現行刑法では犯罪類型に当たらないものについて、法律的制裁を準備する必要がある。

現行刑法の体系では、企業秘密、プライバシー、社会的に重要な情報システムに対する侵害を防止するための法制的対策は未だなされていない。データ侵害という新たな犯罪類型を法定することが現状において無理にせよ、コンピュータシステムに係るデータの財物的価値を認め、法定することにより、現行刑法における文書毀棄罪、文書偽造罪、窃盗罪等の犯罪類型により、当面、かなりの部分をカバーすることが可能である。更に将来的には、情報化の今後の進展、環境の変化を十分見極めながら、いわゆるコンピュータ犯罪防止のための立法も検討する必要がある。

6. 2. 3 データ保護のための事業者の合理的保護対策

ア) データ保護対策を万全なものとしていくためには、上記の対策に加え、個人及び法人のデータを特に取扱うシステム及び社会的に重要なシステムを運用する事業者自身が、データ侵害に対し合理的な保護対策を講じていく必要がある。

このためには、事業者の指針となるべきガイドラインを定め、これを公表する。

次いで、特にデータ保護対策に優れた事業者に対し、「優良事業者認定」を行う。

更に、特に重要なシステムを運用する事業者に対しては、ガイドラインの遵守義務を法制化する等の方策が考えられよう。

イ) 次に目的別に具体的対策を整理すると次のとおりである。

(i) 企業秘密、プライバシーの保護

考えるべき方向として次のものがあげられよう。

- (a) 不法なアクセス防止のための技術導入
- (b) 不法なアクセス防止のための運用管理
- (c) 目的外使用の禁止
- (d) 秘密の保持

かかる対策のほか、諸外国の立法例では、プライバシー保護の観点から特に、データ収集の目的の明示、データ収集の公正性、データ内容の適正性、データに対する個人のアクセス権の承認等の対策を義務付けているものもある。

しかしながら、我が国のプライバシーに係る社会認識の程度の低さ、(a)～(d)の対策で当面かなりの部分をカバーすることが可能なこと、データ保護対策は必ずしもプライバシーのみを目的としたものではないこと等を考えあわせれば、当面(a)～(d)の対策で必要十分なものではないかと思われる。

(ii) 社会的に重要なシステムの安全運行

考えるべき方向として次のものがあげられよう。

- (a) 不法なアクセス防止のための技術導入
- (b) 不法なアクセス防止のための運用管理
- (c) システムの安全性を高める高信頼化技術の導入
- (d) システムの安全性を高める運用管理

かかる方向の対策をガイドライン化又は法制化していくことが重要であろう。

ウ) さらに、事業者別に対策を整理すると次のとおりである。

(i) 自己の目的のために情報処理を行う者

個人及び法人のデータを取扱う事業者又は社会的に重要なシステムを運用する事業者に対しては、事業の重要性ゆえにガイドラインを提示し、ガイドラインに従った運用管理を要請する。

(ii) 他人の需要に応じ情報処理の事業を行う者

他人の需要に応じ、個人及び法人のデータを取扱う事業者又は社会的に重要なシステムを運用する事業者に対しては、それを業として行っていること、また業者を利用するユーザーの保護を図ること、更に業者のステータスを守るという観点から、事業者に対するガイドラインに従った運用管理を強く要請する。また、特に優良なデータ保護対策を講じている者に対しては、「優良情報処理サービス業者」の認定を行うなどの方策も考えられる。

ガイドラインについては、その内容、社会のニーズを踏まえ、遵守義務を法定することも検討に値しよう。

(iii) 他人の需要に応じ、情報処理及び蓄積をした情報を提供する事業を行う者

基本的には、(ii)に準じた対策が考えられるほか、諸外国の立法例では、プライバシー保護の観点から、前述したようにデータ内容の適正性、アクセス権等の規定がある。しかし、我が国において、かかる産業は今だ黎明期にあり、このような規制をそのまま持ち込むことは、新たな産業の芽を摘むこととなる恐れがある。また、この産業において、現在扱っているデータは、一般的公開データが中心であり、プライバシー、企業秘密に係るものはほとんどない。また、公的機関のプライバシー、対策を民間部門に先行して行うべしとの意見もある。従って、データ内容の適正性、アクセス権等に係る対策は慎重に検討する必要がある。

7. ガイドラインの在り方

7.1 ガイドライン策定のポイント

ガイドラインは、以下のような性格をもったバランスがとれたものでなくてはならない。

- i) 情報化を阻害する要因を排除するものであること。
- ii) 国民の情報化に対する安心を保証するのに必要十分であること。
- iii) 経済効果の優れたものであること。
- iv) 国民全体の利益にかなうものであること。
- v) ガイドラインそのものが、運用し易いものであること。

このような考え方にに基づき、ガイドライン策定に当たって特に留意すべき点は、次のとおりである。

① 現状の把握

i) データ保護の実態把握

コンピュータを中心とする情報処理システム内において、データ保護がどのように行われているか、現状を調査し、データ保護の現状レベルを正しく認識する必要がある。調査に際しては、我が国に設置されている情報処理システムのデータ保護状態を確率高く推定することの出来るサンプリングをすることが肝要である。

ii) 各界動向の把握

データ保護については、プライバシー問題を中心に官民双方から各種の意見が提示されている。これらの意見、調査研究は、さまざまな角度から提示されているが、これらを包含して各動向を把握する必要がある。

iii) データ保護技術動向の把握

データ保護に係る技術は、情報処理技術とともに発展してきた。従来は、ソフト関連の技術が主流であったが、電子機器のコスト・ダウンに伴って、ハードによるデータ保護技術も数多く出現している。また、これらの技術推移もたいへん激しいものであり、その方向を的確に把握する必要がある。

iv) 諸外国動向の把握

データ保護に関する諸外国の動きは、OECDをはじめ、すでに法制化されている国から、現在検討中の国まで、諸々のステータスがある。データの流れは、国際的であり、その意味から我国のデータ保護のあり方については、諸外国のそれを充分把握した上で考える必要がある。データフローの問題は、国益と国際協調とのバランスの上で考えねばならない。

② データ保護のコストパフォーマンス

データ保護を行った場合にも、可能な限り情報処理コストに影響を及ぼすことなく、情報化が円滑に推進されるよう、努力することが必要である。情報化推進という面からみたパフォーマンスが最良となるデータ保護施策を提示することが重要といえよう。

③ データ保護領域のバランス

データ保護について論じられている文献は数多くあるが、コンピュータ・セキュリティという観点からデータ保護を論ずる場合、その保護領域を明確にし、かつ、領域間のバランスがとられていることを確認する必要がある。例えば、システム内にデータを保留している状態別に保護レベルを考えた場合、各状態毎の保護環境が等価になるよう

配慮する必要がある。ファイル系や伝送系にのみ頑強な保護対策を施し、チャンネル系やI/O系はやや手薄となるようなことは避けるべきである。ややもすると、保護手段が先行してしまい、保護システムとしてバランスのとれていないものになる危険性があるので注意を要する。

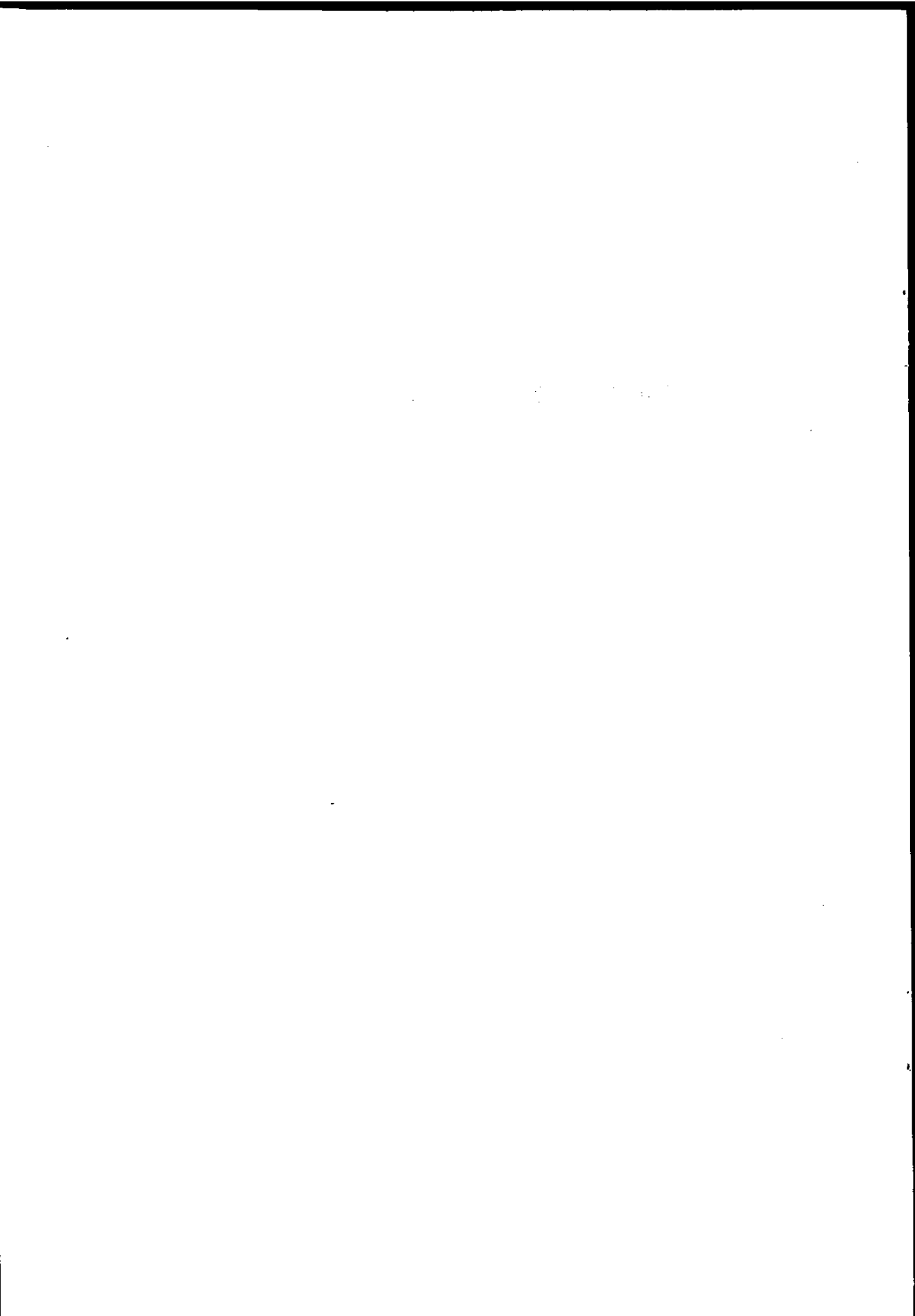
システム内の或るポイントにのみ（例えば通信の領域、ファイルの領域というような）片寄ることのないようデータ保護の指針をガイドすべきである。

7.2 ガイドラインの方向

以上のような留意点を念頭に、ガイドラインの姿を考えるならば、現状において施行されている既存の「電子計算機システム安全対策基準」、
「情報処理サービス業電子計算機システム安全対策実施事業所認定基準」を基本とし、要すればこれに通信回線利用自由化によるネットワーク化の進展という新たな情勢を踏まえたものと考えることができる。

既存の二基準においても、現状の技術レベルにおいて可能な範囲のデータ保護対策が講じられているが、ネットワーク化の進展に対処するとの観点から、特にアクセスコントロール強化の考え方をとり入れる必要があると思われる。その意味で前述した本人確認技術やアクセスモニタリング技術の導入、運営管理面からプロテクションリング等の手法を強化するという方策が考えられよう。また、盗聴対策として技術開発の動向をみつつデータを伝送する際の暗号化技術の導入等も検討する必要がある。

第 4 章 結 論



本研究会は、健全なる情報化社会の構築のため、高信頼性システムの形成、コンピュータ犯罪の防止、データ保護という三つのアプローチにより、情報化の進展とともに益々重要性の高まりつつあるシステムの安全運行、プライバシー等基本的人権にも係るデータの保護を図るため、自然災害、故障、犯罪等の脅威に対し、如何に対応すべきかを検討してきた。

これらの検討の中で、コンピュータに係る適正かつ効果的なセキュリティ対策を実施していくためには、技術の進歩、コンピュータ利用の社会的位置付けを配意しながら、技術・設備面、運用管理面、制度面からのバランスのとれた総合的かつ有機的対策が必要であることが明らかになった。

コンピュータ利用のセキュリティ対策を技術・設備面における対策、運用管理面における対策、制度面における対策の三つに要約すれば、次のとおりである。

1. 技術・設備面における対策

- (1) コンピュータシステムのダウン等により社会的に大きな影響を与えるシステム、特にクイックレスポンスを要求されるオンラインシステムについては、より信頼性の高いシステムが要求される。

コンピュータシステムの高信頼化を確保するためには、ハードウェア、ソフトウェア、コンピュータシステム関連設備、運用管理等において総合的にバランスのとれた対策をとることが必要であるが、このための個別技術としては、①素子を含めた機器の高信頼化、②テストの充実等ソフトウェアの高信頼化技術、③システムダウンを避けるため、誤りを訂正したり故障部分を切り離して動作を継続する可用性技術、④万が一システムがダウンした場合の早期回復技術等がある。

また、特に銀行システム、医療情報処理システム、交通管制システムのようにコンピュータシステムのダウン、エラー等が、多大な社会的影響を与えるシステムについては、このような各種技術等で対応するとともに、コンピュータシステムの構成による信頼性確保対策がある。

具体的には、コンピュータのデュアル、デュプレックス等のシステム構成、回線、関連設備の二重化等の対応があり、更に高信頼性を追求すると災害等により地域的にコンピュータシステムが使用できない場合に対処するバックアップコンピュータセンターの設置等様々な方法が考えられる。

このように現在の技術レベルでもコストを充分にかければ相当の対策が講じられるが、ユーザの過大な負担や二重投資とならないよう上記個別技術の開発、改善、普及及びシステムの実態に適合したシステム構成についての研究開発、ガイドライン作りを進めていく必要がある。

- (2) コンピュータシステムは、今やだれでもが自由に利用できる時代になり、これに伴って、コンピュータ犯罪が我が国においても問題化してきた。

これらの犯罪防止技術としては、①ユーザのコンピュータシステムへのアクセスをコントロールする技術として、本人確認技術（指紋、声紋、サイン、手形等）、通信回線との不正接続防止技術、ユーザごとのシステムに対する使用権あるいはリソースの範囲を管理するユーザプロフィール管理技術、ユーザのコンピュータアクセスの記録を行うアクセスモニタリング技術等がある。また、②犯罪者からデータを保護する技術（企業秘密、個人情報の保護を含む）として、ユーザがデータベースにアクセスすることが許されている領域のみを検索可能とするコントロー

ル技術、TSSでデータベースを利用する場合に全く関連のないデータが推論されないようにする推論の制御、盗聴を防止するための暗号化などの技術がある。特に暗号化技術についてはクローズアップされてきているが、①高価であること。②鍵の配送、管理が繁雑であること。③処理能力に影響を与えること。などの問題もあり、低廉かつ有効な暗号方式が要請されている。

今後は、これら技術の広範な利用を目指し、総合的かつ連けいをとった技術開発、改善が必要となっている。

更に、犯罪を防止するため、コンピュータシステムに近づけないようにする接近の防止技術、接近した場合情報が無効化される技術などコンピュータシステムの周辺の各種技術の改良が行われることが必要である。

2. 運用管理面における対策

システムダウン、コンピュータ犯罪を防止するとともに、データ保護を図っていくためには、コンピュータシステムの運用管理体制を充実させていくことが基本である。

第一に、組織体制の整備である。コンピュータ犯罪防止及びデータ保護の観点からは、特に職務権限の分担の適正化を図り、アクセスできる人間を限定するとともに、責任を明確化し、内部牽制機能が生ずるような体制を組む必要がある。

また、システムダウン防止の観点からは、障害発生時の緊急対策を想定したプロジェクトチームを準備しておくことが望ましい。

第二に、教育訓練及び人事管理である。システムの安全運行やデータ保護のために、操作手順の定型化や内部規程の制定を行うだけでなく、これ

らに関する定期的な教育や訓練を行うことが必要である。この中には緊急時を想定した被害防除、早期復旧訓練等も含まれるべきである。

また、コンピュータ犯罪防止及びデータ保護の観点からは特に、業務の重要度に対して、業務の機械化、単純化に伴い、責任感のアンバランスが目立つ業務も見受けられるので、技術的専門教育は勿論のこと、職業倫理についての教育や適正な人事管理が必要であろう。

この際、職場全体の快適な環境の確保や職員の志気の昂揚を高めることも重要であることは言うまでもない。

第三に、運用管理規程等の制定である。コンピュータセンターに出入りする人の入退室の管理、監督、設備の状況監視、保守点検等の規則は勿論のこと、オペレーションについても、必要なマニュアルの整備、誤動作を防ぐ規則の制定、実施が重要であろう。

最後に、システム監査の導入が重要な方策として上げられよう。監査は、本研究会のテーマ（システムダウン防止、コンピュータ犯罪防止、データ保護）についてチェックをすることとし、制度面からこれを単に監査部門に止めるか、行政の裏づけに基づく一種の資格にまで高めるかは、なお検討を要するが、有力な方策といえる。

3. 制度的対策（行政の対策）

制度的対策、行政側の対策としては、次のような施策が考えられよう。

第一に、コンピュータ・セキュリティに係る技術開発及び導入の促進である。このような技術開発及び導入は、通常莫大なコストを必要とするものであり、民間企業にとって、少なからぬ負担を伴うものである。政府としては、資金の確保等かかる技術開発及び導入のための基盤づくりを行う

必要があろう。

第二に、コンピュータ利用に従事する人々にコンピュータ・セキュリティに対する認識を涵養することも必要である。このための一つの方策として、「情報処理技術者試験」等の設問にコンピュータ・セキュリティに関する出題を加えること等が考えられる。更に、情報処理技術者試験等の拡充とともに、「システム監査士」等の資格創設も考えられよう。

第三に、システムダウン防止及びデータ保護の観点から、事業者の判断の指針となるべきガイドラインの制定が考えられる。通産省においては、既に昭和52年から「電子計算機システム安全対策基準」や昭和56年から「情報処理サービス業電子計算機システム安全対策実施事業所認定制度」を創設し、コンピュータセキュリティ対策を講じているが、情報処理ネットワークの拡大等に伴い現在のままでは必ずしも十分とは言えない面もある。

従って、かかる基準に加えて、社会的に影響の大きい特定のシステム、個人及び法人等のデータを扱う特定の事業者に対し、ガイドラインを提示し、ガイドラインに従った技術導入、運用管理を要請することも必要となっている。このようなガイドラインは、システムを設計するうえでの尺度として広く用いられ、システム設計者の利便に供されるとともに、システム利用者の保護、民間事業者の平準化・レベルアップ・ステータスの向上を図るうえで役立つものと考えられる。

また、ガイドラインに加え、「優良事業者認定」を行う。更に、特定事業者に対しガイドラインの遵守義務を定める等の方策も検討に値しよう。

第四に、特にコンピュータ犯罪を防止する観点から、コンピュータ・セキュリティに係る倫理観の醸成に伴い、刑法の改正や特別立法の制定も検

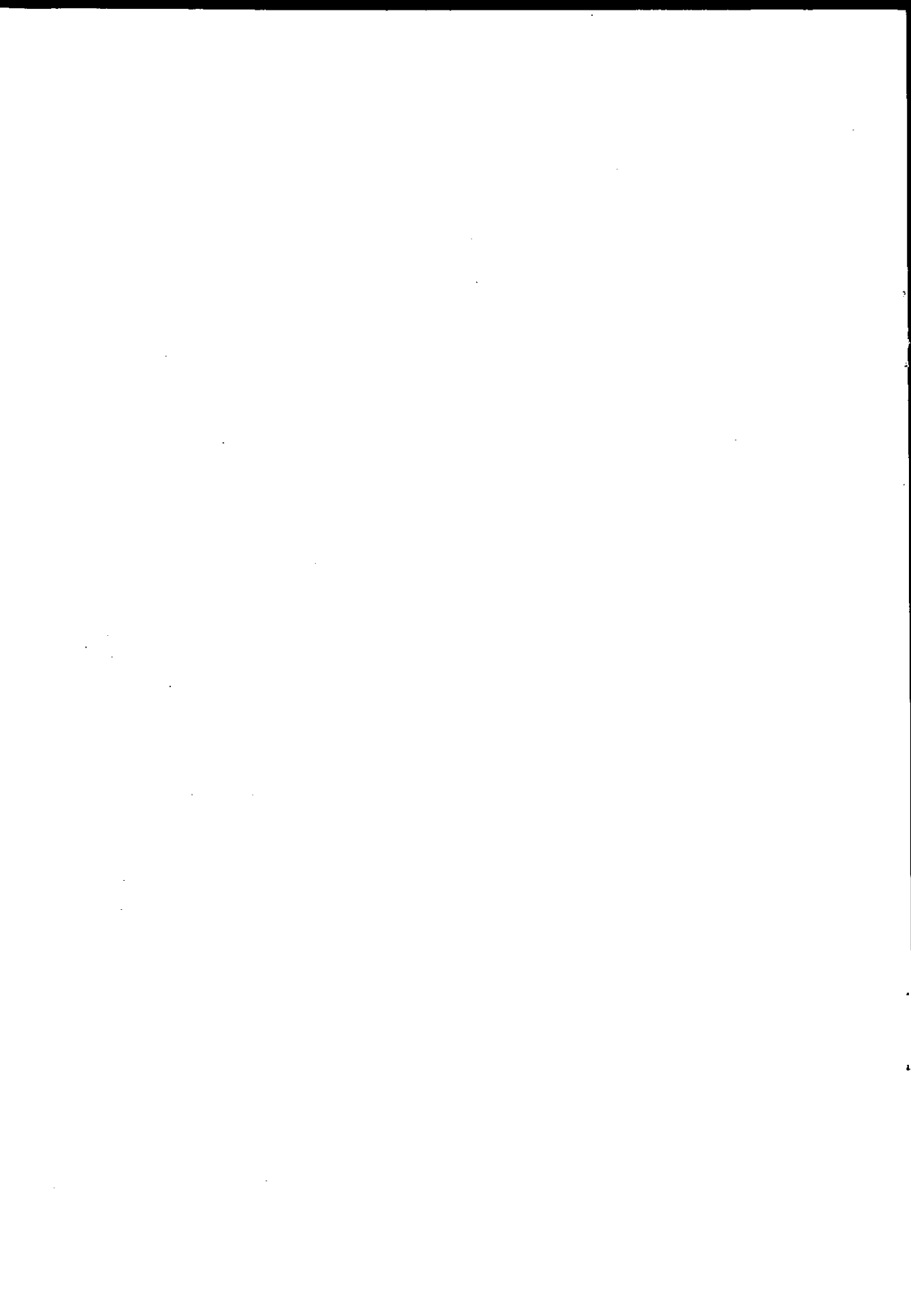
討する必要がある。

以上に加え、民間事業者の対策に係る努力の一助とするため、事故情報、犯罪情報等の収集、資料等の作成が考えられる。また、かかる研究会を恒常的に組織し、新たな問題に対し、研究、調査を積み重ねていくことも肝要である。

以上の諸施策の中には、既に実施に移されているものもあるし、今後直ちに技術開発等に着手すべきもの、将来の倫理観の醸成に待つもの等、短期、長期諸々の課題があり、これらを十分吟味していかなければならないことは言うまでもない。

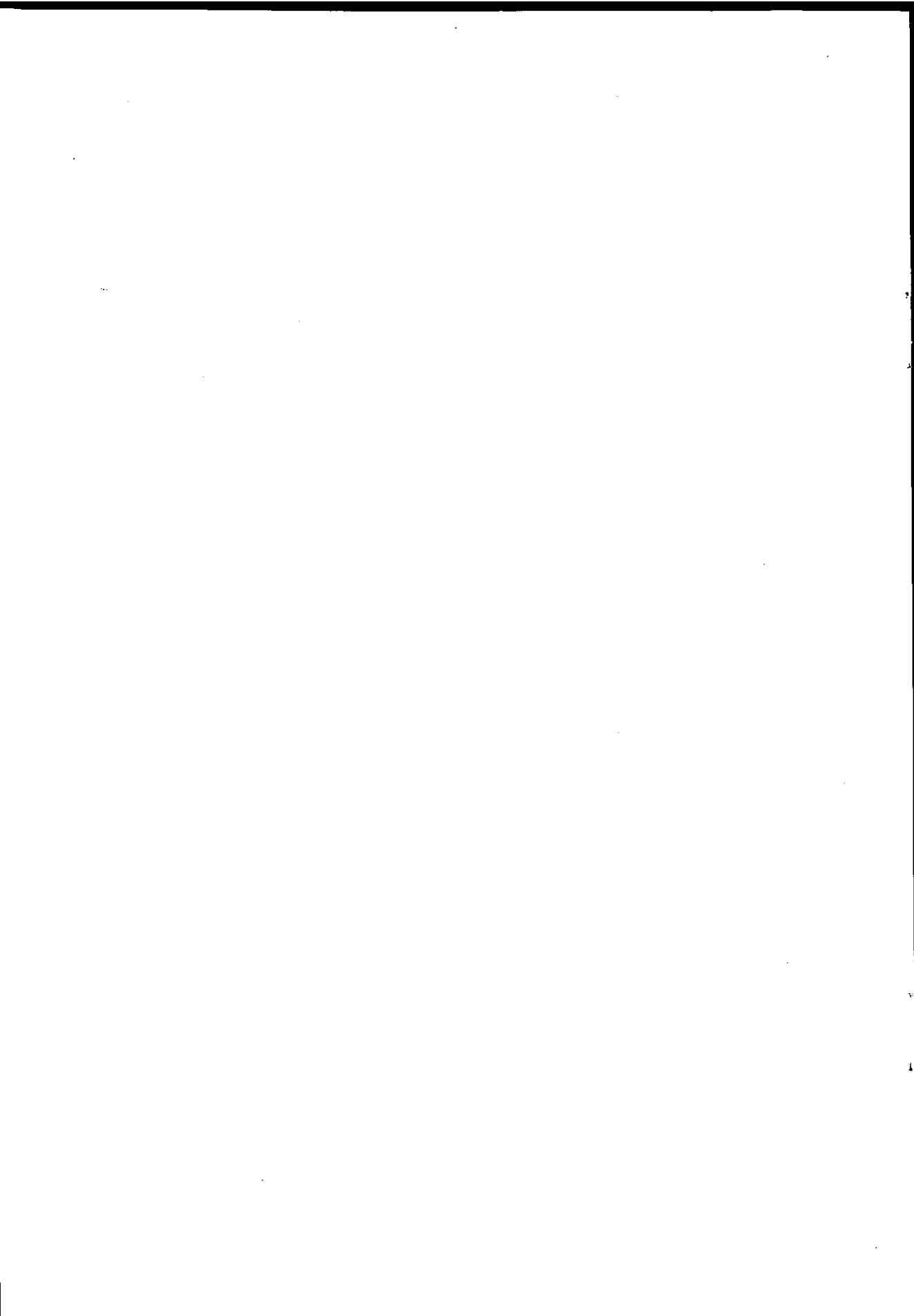
健全なる情報化の進展という大局的観点から、多面的にバランスのとれた総合的な対策に、官民挙げて取り組んでいかなければならない。

付 属 資 料



1. 審 議 経 過

本研究会においては、表1の当初の問題意識により討論グループを3つに分けそれぞれ表2の学識経験者、各方面の専門家・実務家のメンバーの方々から知恵を拝借し、6月から現在まで各グループ6～8回の審議を行ってきた。その内容については表3のとおりである。



(表1)

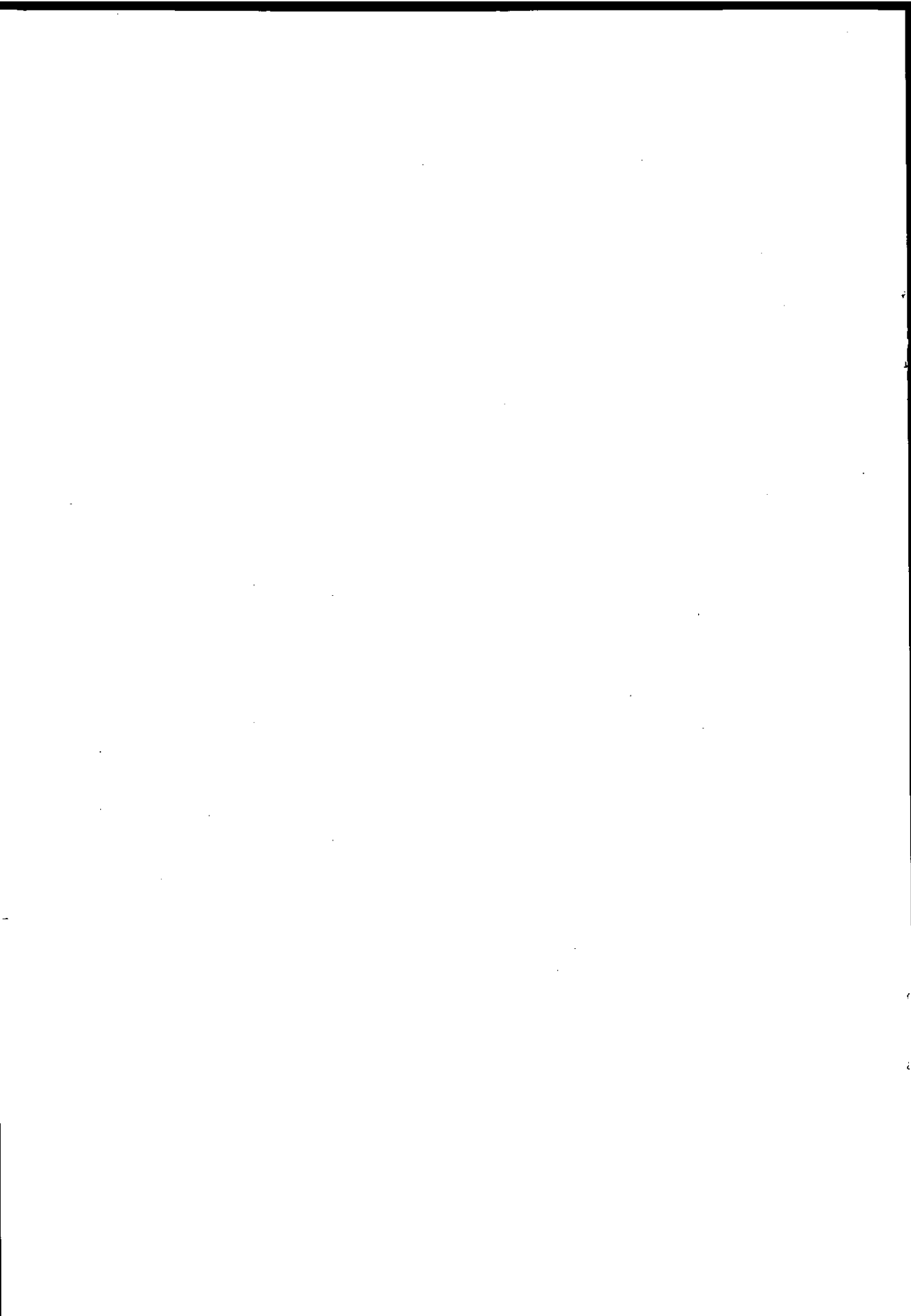
	第 1 グ ル ー プ	第 2 グ ル ー プ	第 3 グ ル ー プ
検討内容	・ 障害（システムダウン、エラー）発生防止対策 ・ 障害範囲の最小化対策 ・ 復旧対策 故障の原因別に類型化し、問題点を整理 ⇒ 技術開発の推進 ガイドライン設定 ガイドライン遵守のための対策 ※ 過失による事故及び自然災害による事故を扱う。 故意に基づくものは検討対象としない。	・ 故意に基づくコンピュータ犯罪防止対策 犯罪の種類別に類型化し、問題点を整理 （破壊、資産の盗み、詐取・横領、コピー、無断借用等、コンピュータに関連した犯罪を扱う。） ⇒ 技術開発の推進 社会的制裁の整備（罰則等） ガイドラインの設定	・ プライバシー保護を含むデータ保護対策 （コンピュータ情報処理システムに係る個人、法人データについて、その利用規制を含むデータ保護対策） ・ 社会的にセキュリティを確保しなければならない範囲を明確化し、規制も含めた制度的、法的な対応策をあきらかにする。 ・ プライバシー保護対策として、特に個人データについて、目的外使用の禁止、本人の閲覧請求、訂正請求等の権利設定等の観点から検討 ⇒ 必要な施策をまとめる。
	システム安全対策基準、システム監査などの整備		コンピュータ利用の制度的検討

2 コンピュータセキュリティ研究会メンバー

(表2)

(順不同、敬称略)

	第1グループ	第2グループ	第3グループ
委 員	齊 藤 忠 夫 鈴 木 弘 道 梅 野 典 隆 押 尾 勝 平 水 野 昌 美 三 谷 保 夫 田 口 孝 弘 宇 多 弘 鍛 治 勝 三	西 田 典 之 湯 野 勉 天 野 武 門 安 住 已久夫 前 田 裕 岡 本 行 二 清 水 光 雄 中 島 基 雄 鷄 内 成 太郎 鳥 居 壮 行	小笠原 謙 蔵 若 山 彰 上 園 忠 弘 森 英 一 勅使河原 可 海 松 村 茂 生 青 木 弘 行 甲 田 篤 信 松 田 宏 鈴 木 茂 樹



3 審 議 概 要

(表3)

	第 1 グ ル ー プ	第 2 グ ル ー プ	第 3 グ ル ー プ
審 議 概 要	6.1 6 第1回会合 (1) 現在考えられているシステム・ダウン対策について報告 (2) 高信頼性システム等について開発状況を報告 (3) システム・ダウンの実際例について報告 (4) 「電子計算機システム安全対策基準」及び「システム監査基準(試案)」について説明 (5) 「システム・ダウン対策とコスト」等のテーマについてフリー・トーキング	6. 9 第1回会合 (1) コンピュータ犯罪の類型について報告 (2) コンピュータ犯罪の事例について報告及び検討 (3) 「システム監査基準」及びこれに係る研究について報告 (4) コンピュータ犯罪防止対策の実例について報告	7.1 6 第1回会合 (1) 趣旨説明 (2) データ保護に係る検討事項について説明
	6.2 5 第2回会合 (1) 銀行システムの信頼性対策について富士銀行の事例を報告 (2) コンピュータシステム・ダウン許容時間に関する業種別調査結果を報告 (3) 信頼性とコストとの関係について報告 (4) 情報処理サービス業での信頼性向上策の例について報告	6.1 7 第2回会合 (1) コンピュータ犯罪の問題点と対応策についてケース・スタディ (2) 銀行業務処理システムの事例とセキュリティ対策について報告 (3) 「データ通信に関する事故防止対策委員会」(電々公社)答申について報告	7.2 1 第2回会合 (1) 情報処理ユーザー、情報処理サービス企業のデータ保護の現状について報告 (2) 海外におけるデータ保護に関する動向について報告
	7. 6 第3回会合 (1) 高信頼性コンピュータシステムの環境につ	6.2 4 第3回会合 (1) 情報処理サービス業電子計算機システム安全対策認定制度について検討 (2) 野村コンピュータシステム安全対策について説明	7.2 9 第3回会合 (1) 海外におけるデータ保護に関する動向について報告(前回のつづき)
			8. 3 第4回会合 (1) 海外におけるデータ保護の現状について報告 (2) 「データ保護に係る検討事項について」の説明
			8.2 4 第5回会合 (1) 「データ保護について」(方向性)の検討

	第 1 グ ル ー プ	第 2 グ ル ー プ	第 3 グ ル ー プ
審 議 概 要	いて報告 (2) ACOSでの信頼性対策について報告 (3) 情報処理サービス業電子計算機システム安全対策実施事業所認定制度について説明 7. 9 第 4 回会合 (1) システムダウンに対する委員の考え方についてフリートーキング (2) 情報処理サービス業電子計算機システム安全対策実施事業所認定制度について説明 (前回のつづき) (3) Mシリーズでの高信頼化対策について報告 (4) スケルトン案についての説明(第1グループ報告書)。 7.1 0 第 5 回会合 (1) 第1グループ報告書スケルトン(案)についてフリートーキング 7.3 0 第 6 回会合 (1) 第1グループ報告書原稿の検討 8. 4 第 7 回会合 (1) 第1グループ報告書原稿の検討	(3) 銀行の安全対策についての事例報告 7. 5 第 4 回会合 (1) 銀行の安全対策についての事例報告(つづき) (2) 欧米のセキュリティ事情についての報告 (3) 第2グループ報告書スケルトン(案)について説明 7. 8 第 5 回会合 (1) 第2グループ報告書スケルトン(案)の検討 7.2 2 第 6 回会合 (1) 第2グループ報告書原稿についての検討 8. 5 第 7 回会合 (1) 第2グループ報告書原稿についての検討	9.1 7 第 6 回会合 (1) 「データ保護について(素案)」「(報告書スケルトン案)の検討

	第 1 グ ル ー プ	第 2 グ ル ー プ	第 3 グ ル ー プ
審議概要	8.1.1 第8回会合 (1) 第1グループ報告書原稿の検討		

