愛知工業大学研究報告
第23号B　昭和63年

経営情報システムのセキュリティ管理

工藤市兵衛・鈴木　達夫・近藤　高司

Computer Security Mangement for Information Systems

Ichibei KUDO, Tatsuo SUZUKI and Takashi KONDO

The need to provide security protection of business information held on computer systems has to balanced against the cost of providing and maintaining security, and its damage to the system users. In this paper, concepts of data security and results of a small survey of the security states on the computer centers are discussed.

1．緒言

我が国の企業において経営合理化，生産性向上のため，ＯＡ，ＦＡと呼ばれて，その膨大な管理情報処理計算に複雑なコンピュータ・システムが急激に広範囲に普及してきている。しかし経済性を最重視するあまり無秩序に広範囲に普及してきているように感じられる。この事は，様々な危険性を含みつつ広がり，例えば自然災害，地震，落雷，火災などによるシステムの損害，停止，機能低下または管理不良によるシステムの事故など新たな問題が増加しつつある。さらに操作する作業者あるいはシステム管理者など，システムのデータを操作できうる人間が悪意を持ちいたずら，犯罪を企てるかもしれない。そこで，コンピュータ・システム，特に企業経営管理においてその管理情報処理の中核機能部門のシステムを対象としてシステム安全管理（セキュリティ）の在り方とアンケートによる実態調査結果の詳細な検討を試みる。

2．コンピュータ・システムの危険性

「高度情報化社会＝コンピュータ社会」と言われるほど，社会機構の様々な方面にコンピュータが導入されている。たとえば，コンピュータ産業の実績を見ても，●汎用コンピュータの実働推移は1986年３月末現在実働台数は24万4,148台（前年度比32.2%増）であり，1985年度を基準として，５カ年ごとにさかのぼって比較して見ると，1980年度比（台数2.8倍，金額1.8倍），1975年度比（同７倍，3.4倍），1970年度比（同25.7倍，8.6倍），1965年度比（同122倍，45倍）となっている[1]。

●オフィス・コンピュータは1985年度の出荷台数10万5,385台（前年度比35.7%増）となり，稼働台数も43万842台（同27.7%増）となっている[2]。

●パーソナル・コンピュータの1985年度出荷実績を見ても総出荷台数198万4,000台（前年度比5.8%増，国内118万8,000台，輸出79万6,000台）[3]となっている。

この事実からして，

① 劇的なる情報通信処理技術の発展

② 産業社会が高度化して大量で高速にデータを処理する要求の増加

③ 遠隔地から通信（システムの国際化）

がますます要求され，収集・伝達・蓄積・加工という情報処理業務にコンピュータ・システムが広範囲にあらゆる部門に利用され，ますます，データ通信ネットワークと融合したオンライン処理形態の高度化傾向が強まって行くことは明白である。高度情報化社会のニーズに合うコンピュータ・システムの管理方式の確立が重要となろう。

しかし，こうしたコンピュータ化の効用とは裏腹に，数々の危険性を内在してしまい，大きな損失を生じる可能性を秘める。そして，それに付随する副作用や悪影響の問題が今日，きわめて，重要な問題とされている。

特に次の問題は社会の有り方の根本にも拘わる問題と言われている[4][5]。

(1) 情報網の支配力に大きな差ができ，情報を支配する側と情報を集められる側，その二つに社会が分極する。これは国際間でも起こり得ることであり，いわゆる管理社会の危険にもつながる。

(2) 社会のコンピュータへの依存度が高まることの結果，コンピュータの事故，破壊，悪用，そういったものによる影響が社会にとって致命的にまで大きくなるという危険性。

(3) 労働者の人減らし・配転といった労働者への影響，あるいは労働条件，労働環境に与える影響の問題。

(4) コンピュータが導入されることによって，様々な面で仕事のやり方が変わり，それによって生じる社会的，あるいは文化的なインパクトといった問題。したがって，企業や行政機関において，社会の機構の一部を構成するたぐいの情報処理システムには，常にその機能を正常に果たすことが要求され，万一そのシステムに何らかの支障が起きて機能を果たせなくなってしまうようなことがあれば，それと連動して機能している企業活動や社会活動に大きな支障を及ぼすことになるのである[6]。

3．コンピュータ症候群

コンピュータを中心とした情報処理システムの支障には，様々な安全をおびやかす要素が上げられるが，こうした，コンピュータが及ぼす悪影響を「コンピュータ症候群」として捉えられている。一般に「コンピュータ症候群」とは，コンピュータにおける災害，障害，犯罪，プライバシーの侵害を総称するものであり，それはコンピュータ利用に伴うリスク（危険性）と言えるだろう。

ここでコンピュータ利用をめぐるリスクについて簡単に述べる[7]。

① エラー（障害）

エラーは人間の犯す過失であり，したがって，意図的なものではなく，そこに悪意は介在していない。エラーは決して悪意なものではないとされるが，一方において，コンピュータ利用をめぐるリスクが実際に表面化する場合，その件数においても，また，損失額においても大部分はエラーによるものだとされている。

② 犯罪

コンピュータの犯罪は利得を目的とするものと，相手にダメージを与えることを目的とするものとの二つに大別され，前者は情報および情報関連資産の盗み，あるいは金銭にまつわる詐欺，横領などが見られ，後者にはコンピュータ・センターや特定の情報関連設備などに対する爆破その他の破壊行為が該当する。

③ 事故（災害）

事故・災害には自然現象によって発生する災害，たとえば，地震，風水害など不可抗力の事態によってもたらされるものが多い。特に我が国の場合は世界でも有数の地震国であり，地震対策は極めて重要な意味を持つ。また，これらは排除するという対策ではなく，それに耐え得るような構造上あるいはシステム上の対策を講ずることが必要である。

④ プライバシー侵害

プライバシーの侵害は故意にも，あるいは過失によっても発生する可能性がある。しかもエラー・事故・犯罪等の発生に付随してプライバシーが侵害されることもありうる。いずれにしてもプライバシー問題は基本的人権にかかわる問題であるだけに慎重かつ万全な対策が望まれる。

このようにコンピュータを利用するに伴って発生する可能性のあるリスク（危険性）はコンピュータの犯罪だけでなく，エラーや事故等もある。

しかし，前述のようにエラー（障害）および事故（災害）については過失および自然に発生するものであり，その防止策（セキュリティ）も既知なるものである。したがって，コンピュータ・センターの建設やシステム開発の際に，これらのリスク（危険性）に対する対応策を検討して行くことが最善であろう。

ところがコンピュータの犯罪およびプライバシー侵害に関しては前者は故意によるものであり，後者は故意・過失にかかわらず発生するということで防止策（セキュリティ）も一貫したものがない。

特にコンピュータの犯罪においてはその手口も日増しに高度化し，緻密なものとなっているため，こうした問題に対して，多角多面的に検討し，万全を期した防止策（セキュリティ）を講ずる必要がある。

4．コンピュータ・システム・セキュリティ

4・1 セキュリティ必要性の背景

前述したように急速な高度情報化社会の進展過程において，安全をおびやかす要素にコンピュータの事故，破壊，悪用等による損失の問題がある。

アメリカをはじめ，諸外国においてもこのコンピュータに関する問題が大きくクローズ・アップされて，この問題はコンピュータが様々な方面で使われ，コンピュータの社会に対する依存度が高まれば高まるほど，それに伴うデメリットという影の及ぼす影響が大きなものとなる。これは情報の価値の高まりと共に情報に対する社会のニーズも大きく影響しており，今後，コンピュータ技術の発達により，ますます，問題化することは明らかである。

中でも，コンピュータ・システムの運用にまつわるセキュリティ問題やコンピュータ・ソフトの法的保護が重要な課題となっている。大規模化するコンピュータ・システムが稼働し円滑な企業活動を営むためにはその安全性・信頼性に対する十分な管理行動が重要不可欠である。

コンピュータ・システムを使う業務に対し，どの部分が弱点であるか認識・評価し，安全対策を措置するセキュリティ体制の機能強化をしなければならない。この様な観点から，我が国では1977年４月に制定され1984年７月改訂された「電子計算機システム安全基準」[8]，1982年に郵政省告示の「データ通信ネットワーク安全・信頼性基準」[9]，が存在し守るべきものを網羅している。

また，日本情報処理開発協会では情報化の基盤整備の一環として，「システム監査」[10]を提唱しており，システムの有効性・採算性・信頼性データの安全性をその枠組みとしている。日本公認会計士協会から「ＥＤＰシステムの内部統制質問書」[11]が公表されており，会計システムの信頼性監査を主眼点とし，会計記録の適性の程度を確かめることを目的としている。

以上，高度情報化社会の進展に伴う技術的・法的保護におけるコンピュータ・セキュリティ対策，あるいは情報化技術に対応する法的保護の在り方について，また，これまでの情報化社会におけるコンピュータの及ぼす悪影響（一般にコンピュータ症候群と言われている）のうち，故意によるものを「コンピュータ犯罪」として捉え，その実態を究明するとともに，どのように対処していかなければならないか。また，今後，ますます発展していくであろう情報化社会に，コンピュータがどのような危険性を生み，どう対処していくべきかを推測することが必要となってきているのである。

４・２　セキュリティとは

セキュリティという用語は危険・脅威などからの解放，そして，安全に保つことである。

コンピュータ・システムのセキュリティとはシステムに対する様々な危険や脅威[12]によって受ける自然的または人的な要因によって引き起こされる損害・損失（災害・事故・障害・エラー・犯罪等）に対して，法的・技術的に未然防止するか，あるいは発生した損害を最小にするために防止・除去・回復する対策措置を施すことである。

コンピュータ・システムのセキュリティには次の二面を持つものと考えられる。

(1)　コンピュータ・セキュリティ

企業における重要な情報を取り扱う情報処理機能を損なわなくする管理行動の一面

(2)　データ・セキュリティ

情報あるいはソフトウエアやデータの機密性の保持管理の一面である。

５．セキュリティ管理のあり方

ここではデータ・セキュリティ管理のあり方について述べる。

データ保護については

①　データを権限外の人が故意に，偶然にさらけ出すことから保護する

②　権限外の変更を加えることから保護する

③　情報処理システムの機能停止・サービス低下を発生防止する

ことが重要である。

そのためデータ・セキュリティ管理が必要であり，図１はセキュリティ管理の体系図を示したものである。企業の外部から客観的に，そして，科学的にシステムに対する各種の危険・脅威を事前に評価・認識し，分析して被害から回避，または未然に有効で適切に防止する対策を検討し，選択して，コンピュータ・システムの管理者・企業の経営者へ勧告，助言することであろう。そして，その対策措置が実行されたならば，その後のフォローアップが必要であり，再度有効に機能しているか確認することであり，セキュリティ管理は広範囲の事象を取り扱い，様々な観点から総合的に評価分析することが必要である。したがって，セキュリティ管理をする場合は方針・理念から手順，対象，対策措置に大別して，その体系をより明確にする必要がある。

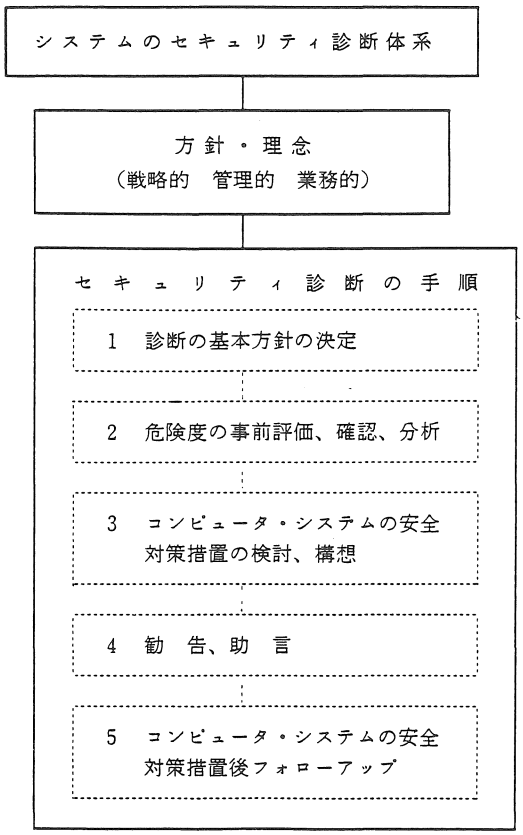

図1　セキュリティ管理の体系図

5・1　セキュリティ管理の方針・理念

コンピュータ・システムに対する危険の防止・回避し，損害発生を未然に防ぐために第1番目にセキュリティの方針を明確にしなければならない。

方針を設定する場合，

① システムの機能が停止する。遅延時間の許容限度。機能停止による業務の遂行がどの範囲まで許されるか。

② システムに蓄積されているデータの重要性。データ破壊，または無くなった場合，復元再生に要する費用と時間分析。

③ システムに蓄積されている機密性。データが漏洩した場合の企業経営に与える影響の分析を行うことが必要である。

特に機密性は戦略的レベルや管理的レベルや業務的レベル等の経営組織の上層で重要である。そして，目標安定度を確立するために経済性，効率性，安全性がなければならない。

5・2　セキュリティ管理の手順

セキュリティ管理の手順は大きく分けて，次の5つのステップになる。

(1)　管理の基本方針の決定

費用対効果あるいはシステムの経営的レベルでの安全目標を明確にしておく。

(2)　危険度の事前評価，確認，分析

システムに対する危険・脅威の度合いを事前に評価し，何が危険であるか確認し，総合的に分析することである。

(3)　コンピュータ・システムの安全対策措置の検討，構想

前ステップの分析結果の資料をもとに対策措置を検討する。主要な安全対策は危険・脅威の低減，抑制対策である。それは管理的対策，物理的対策，技術的対策から構成される。

(4)　セキュリティ管理実施

管理実施は企業経営管理の一部門として認識し，管理の対象としてはシステムの技術，物理的装置設備建物を含むもの。実際の業務遂行には責任の所在と権限を明確にする。

(5)　コンピュータ・システムの安全対策措置後のフォローアップ

仕事の状態を評価する管理ポイントを設ける仕組みを組織に持たせ，フォローアップする。

5・3　セキュリティ管理の対象・範囲

セキュリティ管理の対象・範囲はコンピュータ・システムの構成要素であり，①ハードウエア，②ソフトウエア，③データ，④通信回線，⑤人，⑥用品等，⑦建物，付帯設備等の広範囲な要素から構成されている。

これらが複雑に結合融合され，大規模システムになればなるほど，脆弱な点が生じてくる。セキュリティ管理では脆弱性を検出認識すべく潜在的危険要因を評価することになる。システムに対する危険・脅威・損害を大別すれば，図2の体系図に示されているようになる。

(1)　一般的危険脅威：自然災害，非自然災害・故障，エラー等

(2)　システム運用管理における危険脅威：人的災害（意図的，非意図的）等

(3)　システムの損害形態：腐食，システム，ダウン，煙害，浸水冠水，破壊等

5・4　セキュリティ管理による対策措置

コンピュータ・システムのセキュリティ管理により，安全対策措置が検討構想されて，システムの改善強化復旧が実施されるが基本的には3つの段階から成立すると考えられる。

セキュリティ診断の対象・範囲

（システムに対する危険・脅威・損害）

1．一般的危険要因

（自然的災害）
　火災・水害・台風・洪水・地震・風害・氷雪害・塩害・落雷・動物害
爆発・人為的破壊
建築物施設・附帯設備機器障害・静電気影響
供給電源設備障害
　電圧電流変化　停電　瞬電　周波数変動
（故障・エラー）
システム（ハードウエア）障害・不良
　演算装置・記憶装置・入出力装置
　周辺端末機器・データ通信回線機器
　オフライン機器
システム（ソフトウエア）障害・エラー・バグ

2．システム運用管理における危険要因
（人的災害 → 意図的・非意図的）
↓
事故　不正　犯罪　怠慢

　運用管理制度不備
　教育訓練不足
　運用管理規定不備
　システム取り扱い不良
　ハードウエア管理不良
　ソフトウエア管理不良
　データ・ファイル管理不良
　ドキュメント管理不良
　システム開発設計不良
　設備設計施工不良

3．システムの損害形態

焼失・熱分解・煙害・汚損・腐蝕・浸水冠水・塵挨障害・損傷砂壊・構内、建物への侵入
コンピュータ室・ファイル保管室などへの侵入
データ消滅・漏洩・変形・破壊・盗用・改ざん
システム不正使用
システム・ダウン
コンピュータ・エラー
データ・エラー
盗聴・漏話・通信システムへの侵入
損傷破壊・障害回復時間延長
損害の拡大・信用失墜

図2　システムに対する危険脅威損害

(1)　未然防止策・拡大防止策

防止対策措置であり，損失損害の未然防止であり，または損害を最小限に抑える拡大防止である。

(2)　迅速応急策

応急対策措置で早期に検知して迅速に対応すること。

(3)　復旧策・再開処理

復旧対策措置で損失被害が発生し，早期に対応しても後々まで種々の問題を残すことがあるので事後処理そしてシステムの再開処理が必要となってくる。

対策措置の内容を類型化すれば，次の様になる。（図3）

①　物理的対策

コンピュータ・システムが一般的危険要因から安全に保護する対策で建物等の構造の改善強化であり，自然災害からの損害を回避してシステムに付随している設備あるいは施設の強化改善である。

②　管理的対策

セキュリティ管理の最も基本となるコンピュータ・システムを取り扱う人間の要素が大きく，企業経営管理の一部門としても対策措置実施の効果が高く，広範囲の危険要因に対応が可能である。

セキュリティ診断による対策措置

①　未然防止策・拡大防止策
②　迅速応急策
③　復旧策・再開処理

物理的対策	管理的対策	技術的対策
緩衝地帯	運用管理	ソフトウエア
構造の改善	組織計画	構造化設計
耐火構造	教育訓練	テスト法
耐震構造	入退室管理	ハードウエア
耐水構造	環境整備	二系統化
施設設備改善	保管管理	診断機能
消火設備強化	保守点検	通信回線
移転分散化	緊急管理体制	識別技術
バックアップ	暗号化	
開発作業管理		

図3　セキュリティ対策措置

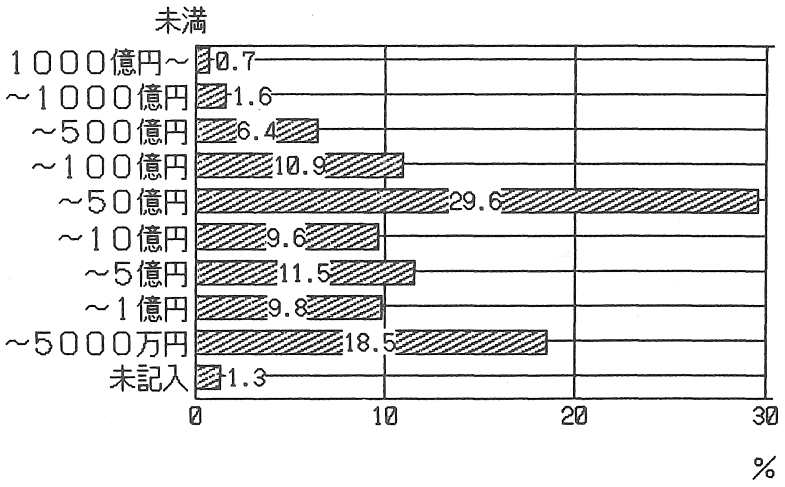

図4　調査対象企業資本金別頻度分布図

表1　ＤＰシステムの主業務

	汎用	オフコン	ミニコン	ﾊﾟｿｺﾝ
無解答	1.3 % (13)	3.3 % (26)	2.0 % (3)	10.1 % (111)
販売管理	15.4 % (149)	17.4 % (138)	5.3 % (8)	5.0 % (55)
受・発注	6.1 % (59)	5.6 % (44)	3.3 % (5)	2.2 % (24)
在庫管理	7.8 % (76)	9.3 % (74)	4.0 % (6)	1.6 % (18)
事務全般	26.7 % (259)	24.9 % (197)	12.6 % (19)	21.8 % (241)
売掛管理	1.0 % (10)	2.3 % (18)	0.0 % (0)	0.5 % (5)
買掛管理	1.0 % (10)	1.0 % (8)	0.0 % (0)	0.3 % (3)
原価計算	1.4 % (14)	1.8 % (14)	0.0 % (0)	0.5 % (6)
人事管理	5.9 % (57)	2.4 % (19)	0.0 % (0)	1.8 % (20)
給与計算	4.9 % (48)	6.7 % (53)	1.3 % (2)	0.9 % (10)
生産管理	10.7 % (104)	10.4 % (82)	5.3 % (8)	4.2 % (46)
技術計算	4.3 % (42)	2.5 % (20)	25.2 % (38)	14.7 % (162)
CAD/CAM	4.5 % (44)	0.5 % (4)	13.9 % (21)	3.5 % (39)
ＮＣ管理	0.1 % (1)	0.5 % (4)	5.3 % (8)	0.5 % (5)
貿易業務	0.0 % (0)	0.9 % (7)	0.0 % (0)	0.3 % (3)
銀行証券	2.7 % (26)	1.4 % (11)	5.3 % (8)	1.5 % (16)
ワープロ	0.3 % (3)	0.9 % (7)	1.3 % (2)	7.0 % (77)
端末	0.7 % (7)	3.0 % (24)	4.6 % (7)	10.7 % (118)
通信制御	2.0 % (19)	0.9 % (7)	4.6 % (7)	2.3 % (25)
新聞印刷	0.1 % (1)	0.1 % (1)	0.0 % (0)	0.0 % (0)
情報管理	2.5 % (24)	3.3 % (26)	4.0 % (6)	8.0 % (88)

③　技術的対策

コンピュータ・システムのハードウエアそしてソフトウエアの技術の問題点を改良改善強化し，損害を防止復旧することである。

6．セキュリティ対策の現況

1986年10月にセキュリティ管理の実態調査を実施し，対策の現況を把握した。

◎調査対象

東京（大阪）証券取引所上場企業　1,650社

中部圏優良企業　350社

◎調査方法：郵送によるアンケート調査（回収率28.6%），資本金別企業分布は図4である。

6・1　コンピュータの主業務

表1に示されているようにシステムの主業務は汎用コンピュータとオフコンは事務管理に，ミニコン

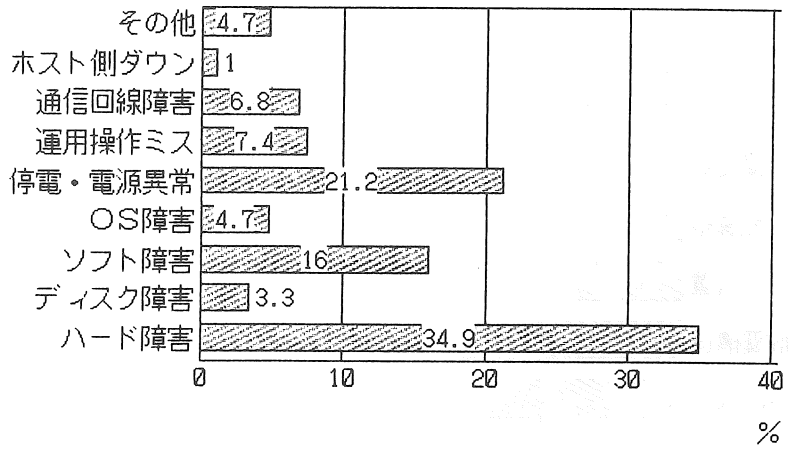

図5　システム・ダウン（15分以上停止）の原因

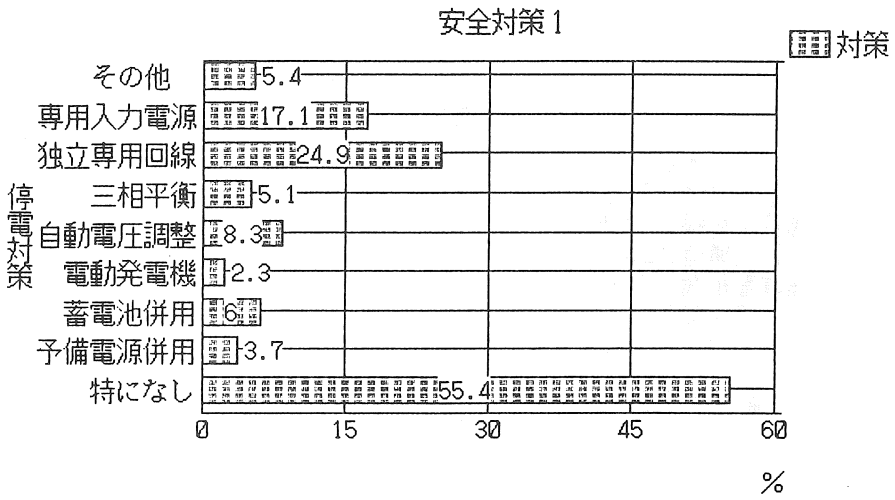

図6　システムの停電対策

は工場管理によく使われ，パソコンは多目的に使われている。

6・2　DP業務中断回数・原因

「事故や障害による業務中断（15分以上のシステムダウン）の年間回数」は1～5回が62%と最も多く，0回が18.9%，6～10回が9.4%，11～20回が4.7%で約8割の企業が何等かのシステムダウンを経験している。

「システムダウンの原因」も図5に示されているように「ハード障害」34.9%，「停電・電源異常」21.2%，「ソフト障害」16%の順になっている。

6・3　物理的安全対策

いつ発生するか分からない災害に対して，どのような対策を行っているか，停電，地震，火災，水害の4項目の調査結果は次のようである。

(1)　停電対策

図6は一般企業の結果であるが「特になし」の55.4%以外は「独立専用回線」24.9%である。銀行結果では「蓄電地併用」77.8%である。システムダウンの原因では「停電・電源異常」と答えた企業が多かったのに停電対策では「電動発電機」,「蓄電地併用」,「予備電源併用」と極めて低いのは現状の危険要因の認識はもっているが即座の対策を施す所までいかない。一般企業と銀行では対策の実施度でかなりの差があるが必要性に対する意識の違いが生じるものと思われる。

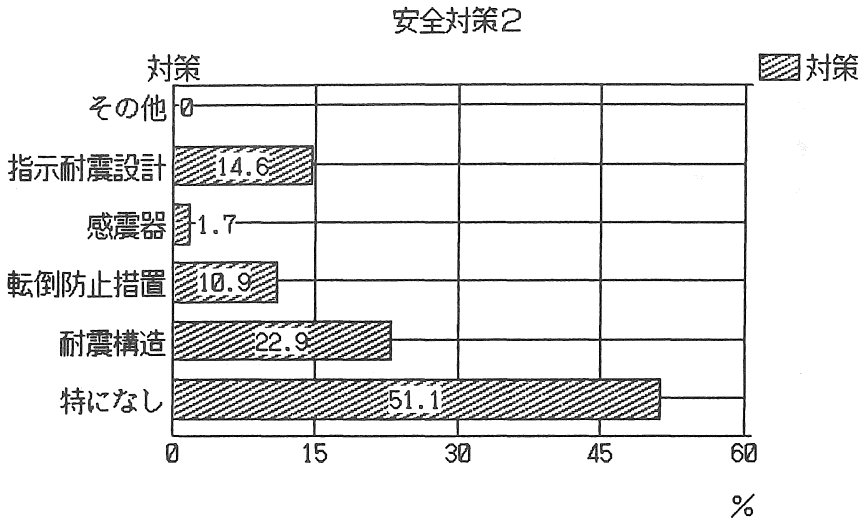

図7　システムの地震対策

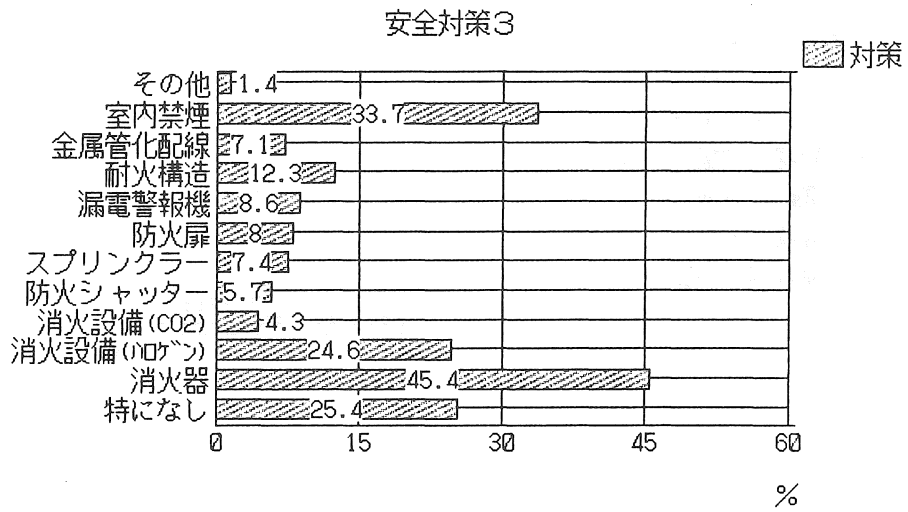

図8　システムの火災対策

(2)　地震対策

図7は一般企業の結果であるが「特になし」の51.1%以外は「耐震構造」22.9%，「転倒防止を行っている」企業が10.9%とかなり低い値となった。銀行結果は100%「耐震構造」で「転倒防止措置」も77.8%実施されている。

(3)　火災対策

図8は一般企業の結果であるが「消火器」45.4%であるが銀行結果では「ハロゲンガス系の消化設備」が100%普及されている。一般企業でも「ハロゲンガス系消化設備」は24.6%である。「室内禁煙」は33.7%に対し，銀行結果でも66.7%と予想以上に低い値である。

(4)　水害対策

図9は一般企業の結果であるが「2階以上に設置」が48.5%であり，銀行結果は77.8%である。全体を見ると水害対策に関してはかなり実施度が低い。水害に対する実感のなさ，地形，立地条件などの面から必要性の意識が薄いと考えられる。

6・4　DPシステムの運用管理

運用管理は安全のための投資を無駄にしないためにも維持，改善，陳腐化しないよう細かい配慮が必

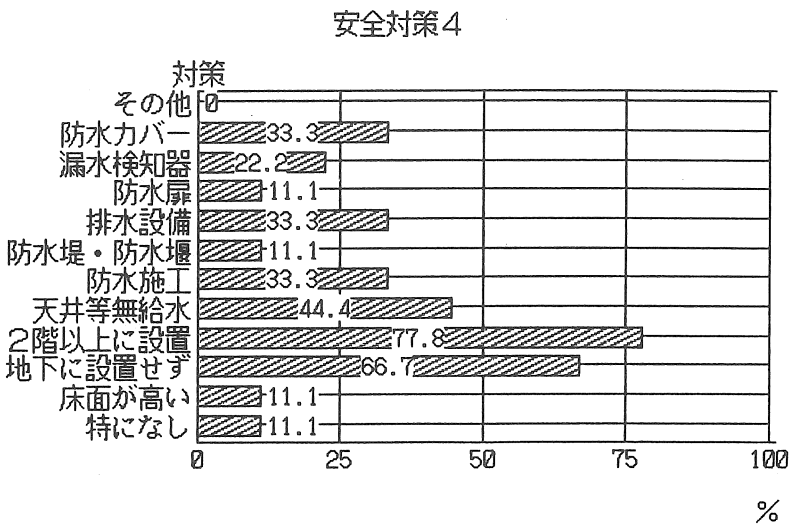

図9　システムの水害対策

要である。物理的な環境の変化，コンピュータ・アプリケーションの変化，コンピュータ・セキュリティに関する新技術の開発や新しいハードウエアの出現などに注意して，安全計画の変更を行わなければならない。

また，コンピュータ・セキュリティの根底にあるのは人間の問題であり，コンピュータ・システムに携わる各個人のモラルを高めていくのも各企業の役割である。

(1)　ＥＤＰ室の運用管理責任者の人数

一般企業で「１人」が46.7%，「２～３人」が30.4%である。銀行の結果でも「１人」が43.7%である。

(2)　データ・ソフトウエアの機密管理

一般企業でデータの機密管理は「普通」40.9%，「やや不十分」26.5%，「やや十分」は６%である。銀行の結果でも「やや十分」44.4%，「普通」33.3%である。「ソフトウエア」は「普通」41.7%，「やや不十分」27.1%，「やや十分」８%である。銀行結果は「やや十分」55.6%，「普通」22.2%である。機密管理の問題は企業内の重要な事項であるのに管理への注意が不足していることがわかる。

(3)　教育訓練および人事管理

●システムの安全対策の教育・訓練については一般企業では「不十分」37.1%，「普通」28%，「やや不十分」27.4%を占めている。銀行結果は「やや十分」55.6%，「普通」44.4%を越しており，システムの対策がしっかりしていることがわかる。

●防災・防犯対策についての教育・訓練については一般企業では「やはり不十分」40.3%，「やや不十分」26.9%，「普通」26%である。銀行結果では「普通」44.4%，「やや十分」22.2%である。定期的に教育・訓練を行うなどして意識の高揚を図ることが必要である。

●コンピュータ・システム要因の配置・交換等の人事管理については一般企業では「普通」39.1%，「不十分」29.1%，「やや不十分」25.1%と答えており，同じ仕事を特定の人だけに限定せずに定期的に勤務交替を図ることが必要である。

銀行結果については「十分」22.2%，「やや十分」11.1%，「普通」33.3%とかなり高いことがわかる。

(4)　運用管理規定

●コンピュータ・システムの操作手順を明確にした手引書を作成していると答えについては銀行100%，一般企業では69.1%と高い水準である。

●システムの運転日誌を常備し，運転状況を把握しているという答えは一般企業49.4%，銀行結果では88.9%と高い。正確なシステムの運転状況を把握して防犯に備える必要がある。

●不正使用防止のための適切な処置を行っているかの答えは一般企業が76.6%がNOと答えている。銀行結果ではYesが77.8%と全く反対の結果であった。一般企業ではそこまでやる必要がないという考えがあり，銀行はささいな不正行為も見逃さない綿密さがある。

(5)　システム監査

●システム監査制度は一般企業では53.4%，銀行結果では100%必要性を感じている。

●外部者によるシステム監査の実施は一般企業では9.8%，銀行結果では50%であった。内部者によるシステム監査の実施は一般企業13.2%，銀行結果では75%となっている。外部監査は一般に結果の点検であり，内部監査は予防的意味合いと能率，効率の向上の資料を得るためである。

(6)　データの保管管理

データの重要度・機密度に応じて厳密に保管・管理し，いかに漏洩を防ぐかが重要である。

6・5　技術的安全対策

(1)　システムダウンに対する技術

一般企業ではデュアル・システム（常時2系統のコンピュータにより同時処理を行うシステムであり，一方が故障しても全く支障なく処理を継続できる）が「必要である」が64.9%，「必要性は感じる」32.4%である。デュプレックス・システム（2系統のコンピュータのうち一方を予備機に切り替えて処理を続行できる）については「必要でない」49.7%，「必要性は感じる」は33.4%である。銀行結果はデュアル•システムは「必要でない」55.6%，「必要性は感じる」33.3%である。デュプレックス・システムは100%使用している。一般企業では専門技術の対策をあまり重視していないことが解る。

(2)　データの漏洩，破壊およびシステムの不正使用の防止対策

●内部関係者による犯罪防止対策であるが，ＥＤＰ室への入室管理やアクセス管理についてはＩＤカード・声紋・指紋などによる運用者・利用者の識別および承認を行う本人確認技術の実施を行っているかであるが一般企業では「使用している」が17.7%である。「必要性は感じている」が49%である。銀行結果では「使用している」が56.3%と高く，「必要性を感じる」が37.5%であり，9割以上銀行は本人確認技術の必要性を唱えている。

●外部者による不正アクセスの防止対策であるが通信回線との不正接続防止技術（回線2重化）を「行っている」一般企業は5.7%に過ぎない。「必要性は感じる」は47.1%である。銀行結果では「行っている」50%を越えており，「必要性を感じる」も50%と高い。内部関係者による犯罪対策においては高いレベルで行われていることが解る。一般企業の対策は十分とは言えない。

6・6　ソフトウエア開発保守

(1)　ソフトウエア品質管理部門の形態

正式組織を「設置している」一般企業は15社に過ぎない。「グループや委員会として設置している」も9社である。「責任担当者あり」は99社である。銀行結果は「正式組織を設置」は35.7%，何等かの形でソフトウエア品質管理者がいるを含めると全体の80%を占めている。派遣要員が多いのが理由と思われる。

(2)　品質管理部門の要員

品質管理部門の要員をどの部門から補充しているかの結果は一般企業では「システム開発」部門から53.5%補充している。「エンドユーザー」部門からは18.3%程度である。銀行結果では66.7%「社外専門家」を採用している。

(3)　コンピュータ部門でのＴＱＣ活動の実施

一般企業では「実施している」28.3%，「必要性は感じる」55.7%，「必要ない」13.7%である。銀行結果では「実施している」44.4%，「必要性を感じる」44.4%である。

(4)　ソフトウエア開発の外注レベル

「基本設計，詳細設計，プログラミング」とシステム開発工程全体を外注している企業は全体の16.1%あり，「基本設計は自社で行い，詳細設計，プログラミング」を外注している企業は23.4%である。「設計を完成させ，プログラミングだけを外注している」企業は20%である。何等かの形で60%の企業が外注を利用している。

(5)　作業委託管理

派遣要員の委託の実施状況は一般企業では「委託している」26.5%である。銀行結果では68.8%派遣要員に委託している。銀行の信頼を重んじ，より専門の人員で，しかもユーザーとなり得ない外部要員を利用している。

7．結言

コンピュータ・システム，特に経営管理において広範囲に利用されている経営情報処理部門のセキュリティ管理のありかたにつき詳細に述べた。究極的には，そのシステムに拘わる人間の倫理観の問題であろう。今日の企業経営管理にはコンピュータ・システムは不可欠な情報処理ツールであり，企業組織にかかわる人々，経営者，管理者，一般社員，それ

に，利害関係者，消費者などシステムから出てくる情報を完全に真理であるかのごとく信じて行動しているが，様々な計算エラーがあり，事故が付き物である事を十分認識して活用すべきであろう。科学技術の進歩は急激であり，コンピュータの分野でもしかり，一般のユーザーは，ＯＡ，ＦＡ，情報通信などの最新鋭の装置の欠点，利点を十分理解することなしに利用している。システムの欠点，あるいは，弱点を補う管理法，システム・セキュリティを中心として様々な分野の知見の結集，充実が今後必要である。

参考文献

1．日本情報処理開発協会編：情報化白書1987，コンピュータエージ社，68，1987
2．前掲書(1)，p.82
3．前掲書(1)，p.90
4．ジュリスト，有斐閣，No.707，13，1980
5．日本科学者会議編：コンピュータ時代を考える，大月書店，15，1982
6．学習コンピュータ，学研，28，1982
7．鳥居壮行著：検証．日本のコンピュータ犯罪，コンピュータエージ社，10-13，1982
8．通商産業省機械情報産業局：電子計算機システム安全基準，1977，1984
9．郵政省：データ通信ネットワーク安全・信頼性基準，1982
10．日本情報処理開発協会：システム監査実施への道路標，1980
11．日本公認会計士協会編：ＥＤＰシステムの内部統制，19，1981
12．旭リサーチセンター編：コンピュータ社会情報政策，日刊工業新聞社，１，1983

（受理　昭和63年１月25日）