解　説

コンピュータ・システムの保全対策（セキュリティ）について*

高　田　　武**

1. はじめに

日本のコンピュータ設置台数は約 35,000 台といわれ，産業構造審議会によれば，昭和60年には 107,000 台に目標を置いてコンピュータの導入を計るとされている．日本にコンピュータが導入されて以来約20年，昨今ではようやく各分野での利用技術も大巾に進歩し，ハードウェア，ソフトウェアの進歩と相まって，コンピュータなしでは業務処理が考えられない分野も出てきている．特に金融業においてはこの傾向が著しい．本部事務・支店事務のいずれをとっても，コンピュータと無関係ではあり得ない状態である．従来はこのようなコンピュータの華々しい一面だけが強調されてきた．いはば“表”の部分である．

しかし，ひるがえって，一旦コンピュータが，機能を中止したり，信頼性を保てなくなったら，その影響は計り知れないものがある，いはば“裏”の部分である．コンピュータを有効に利用することはもちろん，安全に利用することが益々重要になってきている．本稿はこの“裏”の部分に光をあてて見ようと思う．

2. 安全対策の必要性

（1） EDP の定着

社会のあらゆる分野でコンピュータが利用され，システム自体は一企業のものであっても，その EDP 機能は社会的にも認知され，日常性活において，多くの第三者がその機能を利用している状態では，システムの運用主体がその安全性を維持することは，社会的責任を全うすることになる．国鉄のみどりの窓口やバンキングオンラインが何時間もストップすれば，非常に大きな混乱を巻き起こす．しかも，このようなシステムは益々大型化しており，システムの複元，継続も破壊度如何では非常に長時間を要する．あるいは，これから益々利用が拡大される医療用コンピュータの場合は，一歩誤ると生命を奪うこともある．第三者がその機能を利用しなくとも，化学制御用のコンピュータの場合には，近隣に大きな被害をもたらし，公害をもたらすような事故も考えられる．また運用主体からみても，システムが高度化し大型化するに従い，システムの安全化を計ることが経営上からも要請される．

（2） 社会的背景

ここ数年来過激な刑事犯が頻発している．従来の犯罪パターンとは異なり，体制に対する反抗が社会的不安をもたらしている．従来の犯罪パターンの場合は，動機と加害者と被害者が明確に結びついているが，体制に対する反抗の場合には，これらの関係が抽象化されているだけに，被害者から見れば全く予想もしない被害を受けることになる．EDP が重要度を増す程，これらの犯罪の対象となり易い．

テロ行為とは大分趣を異にするが，法制上コンピュータ時代にマッチした法的な保護が遅れている部分がある．コンピュータ時間の窃取・情報の窃取や複写などに対しては現行法上では非常に問題となる．刑法の一大原則である罪刑法定主義からいえば，現行法での処罰は難しいのではないかと考えられる．基本的人権を守る立場からいえばやむを得ないことであり，法制面の整備が望まれるのであるが，それを待つまでもなく，運用主体での自衛が要請される．

（3） 担当部門内外の意識

EDP が合理化・効率化の担い手として脚光をあびているため，ややもすると省力化・コスト削減に走りすぎ，EDP 部門内でその安全性に対しては充分な施策がとられない傾向がある．あるいは地震対策のように，何時起こるか起こらないか判らないものに対して経費をかけ難い点がある．また EDP 部門外では，EDP アレルギーはまだまだ強く，EDP 部門まかせになっていないであろうか．しかし近時 EDP 監査や外

* Approach for the secured computer systems by Takeshi TAKADA (Assistant General Manager, Methods & Systems Planning Dep., The Sanwa Bank Ltd.)

** (株)三和銀行事務企画部

表-1

事故年月	ユーザ	損害(万円)	使用cpu	原因
45. 1	非鉄金属業	7,020	中型	エアコンダクト附付から出火，一部焼失一部冠水.
46. 6	重機械製造業	6,910	〃	エアコン出火，ダクトからの強粘着性ガスによる電算機汚染.
46. 3	地方公共団体	5,540	〃	エアコン電源盤ショート，消火剤重炭酸ナトリウムによる電算機汚染.
46.12	商業	62,730	大型	加湿機バルブ故障により湿度95%，電算機に水滴浸入.
45. 8	食品製造業	1,090	ミニ	台風9号によりトタン屋根破壊・水浸し.
50. 2	土木建設業	24,841	大型	テロ行為.

部監査により EDP も監査の対象として捉えられてきたために，EDP の安全性についてもこの監査内容の一部となっている．この点からも対処が要請される．

（4） 事故例

EDP の事故も，他の事故と同じく一般に知られることは少ない．事故発生側でできるだけ世間に知られたくないのは人情である．従ってそのほとんどがもぐっていると思われるが，JECC の調査のうち金額的に大きいものは表-1 の通りである．米国の事故例としては，利息端数を横領した銀行員の横領プログラム，コンピュータ時間の盗用，ベトナム反戦グループによるファイルの磁気抹消，見学団が持っていた磁石によるデータ消失などがある．

私の職場でも，残念ながらこの 18 年間に，プログラムやオペレーションのミスはもちろん，空調機からの溢水，天井の雨もり，配水管のジョイント部不良，M/T デッキのショートによる発煙，鼠によるケーブル破損などがあったが，幸いなことには，いずれも大事に至る前に発見対処して事なきを得ている．

3. 安全対策の対象

EDP の安全を計るには単にコンピュータだけを対象と考えてはならない．EDP をファンクションとして捉え，このファンクションを阻害する要因全てに対して安全対策を講ずる必要がある．ハードウェア，ソフトウェア，付帯設備，建物，室，更にはデータやドキュメントや，従事する要員そのものも対象として捉えることになる．また一次災害だけでなく二次災害や復旧のことも念頭において対策を講ずる．余り出入を厳重にして火災時の避難路に障害となるとか，火災に対して水は有効だけれども，コンピュータが使いものにならなくなったのでは良い対策とはいえない．対策にはバランスが必要である．

4. 安全対策のポイント

（1） 環境

コンピュータが設置されている周囲の環境に気をくばる必要がある．この環境の中には，大は自然環境から，建物の設置環境，建物自体の利用のされ方，あるいはコンピュータ室そのものの中での収容状態などに分かれる．自然環境についていえば，台風コースの地域，落雷多発地域，低地で出水し易い場所によってそれぞれ対策のたて方が異なるし，建物の設置環境について言えば密集地の場合とか，周囲に石油タンクがあったり，塵埃が多いか否か，あるいは強力な磁力線を出すものがあるかによって打つ手は異なってくる．また雑居ビルの場合などは特に火災とか，出入管理などに重点を置く必要がある．収容状態について言えば，ケーブルの配線上誘導を起こさないよう注意しなければならないし，運搬車の衝突などにより，ノイズ発生（静電気）や，衝撃による接触不良やショートの防止にレイアウト上の工夫も必要となる．

（2） 事故例のケーススタディ

コンピュータシステムを機能として捉えると，その機能を全うするためには，非常に広い範囲にわたって関連する処がある．これら全てが完全に機能することが必要である．単にコンピュータ本体だけが問題なのではない．先にも述べた通り，容れものとしてのコンピュータ室，そのまた容れものとしての建物，電源設備，空調設備，通信設備，これらを連絡する配線・配管，運用管理，ありとあらゆる処に事故原因・誘因がある．それら全てに対して安全性・正確性が計られなければ，コンピュータは機能しない．ところが，これらが余りにも広い範囲にまたがるために，余程注意しないと危険の存在を見落しがちである．できるだけ多くの事故例を参考にしながら万遍なく丁寧に自社内の危険の存在を再チェックすることである．

（3） 対策の基本

対策の基本の第一は何と言っても用心である．用心のない処に危険の認識も対策のアイディアも生まれてこない．その気になると危険な箇所はいくらでも目につく．また必ずしもコストのかからない対策のアイディアも出てくる．原因としてどんな小さなことであっても事故が起こってしまうと結果は同じである．ちょっとしたアイディアで防止できるものを気づかずに放置して，重大な結果を招くほどばかばかしいことはない．また対策のために設備を整えても，運用・維持に

ついて充分管理することが重要になってくる．

第二は，事故を早期に発見し，所定の部署に通報できるようにすることである．早期に発見できるか否かで結果は大きく異なってくるのが常である．タワリング・インフェルノの様に火災が発生しているのに，フレッシュエアーを供給するなど，文字通り火に油を注ぐことになる．

（4） 監視体制と非常時行動規準

大きなコンピュータ設備を持つ処では，防災センターを設置する．ここでは出入管理の補助機能を果たすITV の受像機，ID カード・システムの記録機，電源設備や空調設備に組込まれたセンサーからの指標の表示盤，備蓄してあるオイルや水のレベル表示，火災や漏水感知機がどの場所で作動したかの表示盤，あるいはこれらセンサーからの警報機を備え集中かつ専門化された監視体制をとる．そこまで設備を整えない処でも，巡視による侵入者の警戒，各種表示盤の読取りとチェックを行なうことは最低限必要である．問題は思いついた時に巡視するのではなく，ルーチンとして巡視することが大切である．何時でもやれることは，得てして何時もやらないことになり勝ちだからである．そして一旦事故が発生した場合，その事故を巧く最小限の損害で済ませられるか否かのキーを握るのは，指導者である．強力な指導者による適確・迅速な指示と伝達系統の確立は不可欠である．この指示に従い，各々の要員が，それぞれの役割を果たすことが重要である．これもその場で急にやろうとしてもできないことである．日頃から非常時の場合の役割と行動基準を作り，しばしば訓練して始めてできることである．

5. 物理的災害と対策

（1） 火 災

JECC の調査によれば，事故例中火災によるものが52%を占めている．火災は天災・人災・故障から二次的にも発生する．特にコンピュータ室は湿度も低く，空調もあるため，空気の流れも速い．火災の拡がり易い条件を備えているので一層の注意をすることである．室内の可燃物を除去することはもちろん，隣りのビルや隣室からの延燃を防ぐシャッターを窓や室内，出入口に設ける．検知機は天井だけではなく，天井裏，空調ダクトの中，フリーアクセスの下等にも取付ける．また検知と同時に空調を停止できるようにしておかなければならない．検知と同時にエアダクトのダンパーを働かせる方法もある．通報機はコンピュータ室内にも設置する．消火設備としては，ハロン 1301 が一番良い．これは空中濃度 4～6% で消火能力を有し，使用により機器の絶縁性も損わない．但し高圧ガスのため，噴出口の位置には工夫が要ることと，高温では腐蝕性のガスとなるので，使用後できるだけ早く排気することが肝要である．炭酸ガス消化も電気機器に対しては二次災害を惹起しないので良いが，30%以上の濃度となると人体に有害となるので防毒マスクを併置すると共に，リモート・コントロールで噴出せしめるときは，現場との密接な連携が要る．これらに対し粉抹消火器（B.C 剤）は，火災が消えても接触不良を起こすし，スプリンクラーも絶縁不良を起こすので使用しない方が良い．避難に当っては機器に防水カヴァーをかけて避難することが望ましい．日頃の訓練にもよるが，磁気テープ，ディスクがかなり多い大型システムでもコンピュータを計画停止し磁気テープ，ディスクを所定の耐火保管庫に収納し，防水カヴァーをかけて避難するのに約 10 分あれば可能である．

（2） 水 災

洪水，台風雨のことを考えて2階以上のフロアーにコンピュータを設置する．これ以外に建物内だけでも水災はある．雨もり，天井裏の配水管の破れや継ぎ目の不良，他のフロアー，部屋の溢水，空調機のドレンの溢水などである．日頃から天井の僅かのシミにも注意を怠ってはならない．配管などは定期的に点検する．できればコンピュータ室の天井には配管しない方が良い．検知器もこれらの危険な箇所に配置する．床下，天井裏，空調機廻りなどである．出水時に備えて，防潮板，排水ポンプ，土のう，排水溝を設ける．また大きな出水ではないが，結露によるショートを起こさないよう温湿度制御には注意を要する．

（3） 地震災害

最近，大地震発生の予想が新聞紙上によく出る．69年周期説でいう 69 年 ±13 年の周期の中に入ったからか，中国での地震予知の成功もあったからかも知れない．もっとも科学としての地震予知も段々進歩してきていることもある．しかしそれでも仲々正確には予測できない．過去の大地震の例をあげると次のようになる．

関 東	1923 年	M 7.9
福 井	1948	7.2
十勝沖	1952	8.2
チ リ	1960	8.5
アラスカ	1964	8.5
新 潟	1964	7.3
河 北	1976	8.5?

地震のマグニチュードはエネルギーの大きさを示すものであるから，実際にはマグニチュードの大きさよりも震源地にどれだけ近いかが問題となる．いわゆる直下型地震が危険となる．いくらマグニチュードが大きくてもイタリアや米国の地震は関係のない理屈である．この意味で地震が起こった時，ある場所での震度が問題となる．地震に対しては地下階のある建物ではかなりエネルギーを弱めることができる．機器・什器の滑動・転倒，フリーアクセスの倒壊に対して対策することが必要となる．日本での地震で，コンピュータ機器が20～30cm 移動した例を聞いている．幸いケーブルを切断するところまでには至らず，転倒もしなかったようである．

この対策として耐震据付工法が開発されている．一つは，機器を特殊なカプラーを用いて床のスラブに直接固定する方法である．この方法ではフリーアクセスのパネルとは離されているので，フリーアクセスが倒壊しても機器には影響がない．水平方向に1Gぐらいまでは充分耐えられる．ちなみに機器自体は0.3Gぐらいまでなら大丈夫といわれている．ただし床に固定する処からレイアウトの変更に難があるが，ケーブルの配線には影響がない．次の方法は免震床である．この方法は，いわばつり床方式で，床全体を油圧機とスプリングで宙づりにする方法である．これだと建物に入力された震動がスプリングに吸収され，コンピュータに伝わる震動は非常に小さくなる．レイアウトの変更も自由ではあるが，コストが若干割高となる．試みに震動台に乗った感じではかなり評価できるのではないかと考えている．このような耐震据付まで行かなくとも，フリーアクセスの倒壊防止は是非考えておく必要がある．フリーアクセスの支柱は床に糊付されているケースが多い．得てして床の塵などで完全に接着していないとか，ケーブルが当って接着がはずれていることがある．またケーブル孔のために震動方向によっては力が均等にかからなくなり，一枚がはじき飛ばされると将棋倒しとなりかねない．接着を確認すると共に，支柱同志を横につないで補強することが必要である．

什器類についても，運搬車にストッパー付きのものを選ぶとか，キャビネット類はロック付のものを選ぶ．またキャビネット類を相互につないで安定性をよくする等の工夫が要る．コンピュータ室内だけではなく，空調設備・電源設備等も転倒防止策を施す．空調配管・配線についても震動により力のかからないようにする．特に，配水管のジョイント部に注意が要る．現在はまだ実施しているところはないと思われるが，地震計をセンサーとして，一定限度以上の地震の発生の場合には，地震計から信号を貰いコンピュータに入力することによって計画停止をし，電源を自動切断してファイルの摺動による破損やショートによるコンピュータの損壊を阻止できるのではないかと考えている．

ほとんどの建物が倒壊するような場合は致し方ないとしても，その際でも，データファイルやプログラムやドキュメントの安全だけは確保することは可能であり必要でもある．

6. 動物害と対策

蟻と鼠がある．特に鼠による被害は案外多い．あるアンケートによると約200社中 10% の事業所で鼠の被害を受けている．現象としてはケーブルの損傷，腐蝕，絶縁不良の形で現れる．鼠は 2cm あれば出入りするといわれており，その対策も仲々難しい．食料となるようなものをできるだけコンピュータ室に持込まないことである．薬品としてはシクロヘキシミドがある．

7. 人的災害と対策

人的災害には大きく分けて二つある．故意による事故と不注意・ミスによる事故とである．

（1） 入 室 管 理

ここ数年来の爆破事件のために，企業の自衛策として入室(館)管理が厳重になされるようになってきた．従来は受付的意味のみしかなかったが今ではむしろ警備に重点が置かれており，専用の警備会社も育ってきている．外部からの侵入者に対して体制としての警備を敷く必要がある．ここでの主なことは，出入の制限，警備と監視，異常の発見と通報である．とにかく疑わしきは建物・室内に入れないことである．また室内ではそれぞれ名札を着用して在室者による相互確認ができるようにしておくことである．入口の配置などにも気をつけ，受付や警備セクションを経由せずに，外部から直接入室できないようにする．入館証などで出入制限をしておきながら，一方で顔パスなど許してはならない．例外だと思って顔パスを許しているうちに警戒心が緩み，不法侵入に対してスキができることになるからである．

入室管理にハードウェアも利用できる．ID カード

によりドアの開閉をするのは比較的多い事例である．最近では声紋とか手形(人間の手の特徴)によりドアを開閉することもできる．前者は研究中であるが後者は既に実用化されている．いずれにしても立入る権限の有無により，同じ ID カードでもアクセスできる処とできない処を区別することが必要である．例えば，ある ID カードホルダーはオペレーション室には入れるけれどもファイル室のドアーは開かないようにする．

昭和45年から50年6月までに，676 件の爆破事件があった．入室管理を厳重にすると共に，搬入物・搬出物のチェックもしなければならない．不幸にして第一次警戒線を突破されても，不審物を発見できるようにしておくことも考えねばならない．そのためには巡回の励行と，巡回時に異常物を発見しやすくするための日常の整理・整頓もなされていなければならない．

(2) 内 部 統 制

外部からの故意に基づく事故への対策だけでは不充分であり，社内における自己統制が要る．内部統制は二つの観点から実施されるべきである．一つはミスまたは偶発事故の防止であり，二つ目は内部で発生する故意に基づく不正事故の防止である．このためには，システムの設計・開発部門と運用部門を明確に区分する必要がある．更にファイルの管理部門も分けた方が良い．部門の独立性を計ると共に，組織の権限を明確にし，いやしくも自前で全てのことがやれないように相互牽制することである．そして，そこには手続が制定されていなければならない．プログラムの設計・変更・作成手続，システムの承認手続，オペレーションの手続などである．特にインプットコントロールとしてデータの受渡しが記録されていなければならず，アウトプットコントロールとして，アウトプットの正確性と受渡しが確認・記録される手続になっていなければならない．重要印刷物（例えば配当金領収証の印刷済分・未印刷分）などの管理規定，廃棄物の管理規定なども含まれていなければならない．

オペレーションコントロールとしては，中央 cpu，端末機が権限のない者により使用されることのないようハード的，ソフト的に防御されていることが必要である．オペレーションの計画と実績との記録は作業指示書と共に保存するよう規定されていなければならない．これらにより不正事故に対して牽制を計ると共に，ミスを含めて事故が起こった時の原因と結果のトレースをやり易くし，次の対処策を迅速にたてることができる．

内部統制としてはこの他にもいろいろなことが含まれる．教育・健康管理，モラールの維持・昂揚，作業能率の向上や信頼度の向上のための諸施策も内部統制の範疇に入る．いずれにしても，内部統制を裏打ちするものとして，部内・部外者による監査が必要となる．企業内の監査部門にも，EDP 知識を持った人を配置する必要があり，最近このようなアプローチをする企業が増えつつある．外部による監査の場合でも，単に会計的な意味からだけでなく，業務の適正な執行，安全な執行の観点から，今後は EDP もその重要な対象範囲に入ってくる．第三者の評価に耐えられるよう内部統制も益々重要となってくる．

8. ユーティリティの障害対策

(1) 電 源 対 策

停電の頻度は余り高くはないが，アプリケーション如何では停電に対する対策をたてておく必要がある．電源の引込系統を二重化するとか，自家用発電機を設置するが前者については電力会社と相談すると良い．停電ではないとしても良質の電源を確保するためには電圧調整機 (AVR) や定周波電圧装置 (CV・CF) がある．高度のシステムでは自家用発電機と CV・CF を組み合わせ，通常は商用電源を一旦 CV・CF に落として，システムに安定電源を供給する．停電時には自家用発電機と CV・CF をつなぐ．これだけでは，瞬断（静止形 CV・CF の場合）や停電時の切り替えの時に電力供給がストップするのでバッテリーを更に組み合わせ，これらのときのつなぎをやらせる．バッテリーは大容量の電力を長時間持たせることに難があるので一定時間内に自家用発電機を作動させることになるが，この時間内に，もし自家用発電機が作動しない場合には，信号を cpu に送り，この割込処理によりシステムを計画停止せしめ，再開始をし易くすると共に，ショックによるシステムの損傷を避ける．これらの制御は全て自動的に行われるようになっている．電源のバックアップはいろいろな様式・組み合わせがあるが，非常にコストのかかる部分でもあり，必要性に応じてそのレヴェルを選ぶことになる．なお自家用発電機のように，使用頻度の少ないものは，日頃のメンテナンスと試験駆動が特に重要であり，非常時に備えなければならない．

(2) 通信回線障害対策

センター側では引込経路を二系化し，道路工事や浸水などで全回線がストップすることを防止できるが電

電公社と相談すると良い．回線そのものを二重化すれば安全度は上るが，遠距離回線が多いとコスト的に大変である．このような場合，普段は専用回線を用い，専用回線に異常のある時は，端末機を加入回線に接続する方法がある．二系化であり，特殊なデヴァイスが要るがコスト的には安価な場合が多い．

（3） 備　蓄

空調機用の水，自家用発電機用の油，飲料水・非常食など非常時に備え蓄える．主として大災害対策である．何日分位を備蓄するかは難しい問題であるが最低3日分ぐらいは欲しいところである．これだけあれば非常時の特殊対策のためのコンピュータの運転は大体まかなえるのではないかと思われる．大災害時の復旧に何日かかるかは起こってみないと判らない点もあるが，ちなみに，新潟地震の場合の電力についていえば5日後に 90% が復旧している．

9. 情報メディアの管理と保護

（1） ファイル管理・運用

ファイルは専用の耐火構造の保管庫に入れる．保管庫の庫内は温湿度共コンピュータ室と同じが良い．大体 20℃±3℃，50%±5% ぐらいである．保管の状況により，リード／ライトエラーを起こすことがある．特にテープリールを斜にして長時間放置することは良くない．はなはだしいときには，層づれによりシンチングを起こすからである．

保管庫からの出入は専用のライブラリアンを置く．権限のある者のみに取り扱わせることによって不正事故を防止しなければならない．どの仕事にどのファイルを必要とするかは，データファイル管理システムをつくれば良い．このシステムでは，その日の作業内容，必要なインプットファイル，保管を要するアウトプットファイルがリストとしてアウトプットされ，これとファイル保存規定とによってライブラリアンが出入庫することになる．もっともシステムの開発部門でテストのために必要なファイルの出入も，手続に基づいた権限者の承認印ある申請書により出庫されることになる．

ソフトウェアライブラリイについても，データファイルと同じような保管を要するが，ヴァージョン・アップの手続を制定し，権限のある者による更新をさせ，バグに備えて二世代保管することと，バックアップのためにコピーファイルを作成することを付け加えたい．

（2） 別保管体制

米国などでは何マイルも離れた処にファイルを保管している．大震災の場合，建物や設備が倒壊してもファイルだけは救いたい．データやプログラムを復元することは極めて困難である．否，不可能かも知れない．このことから第一次重要ファイル，第二次重要ファイル，その他ファイルと区分けし，第一次重要ファイルは別地域へ，第二次重要ファイルは同地域でも別の建物へ，それぞれコピーして保管する．プログラムライブラリイ，ドキュメントも第一次重要ファイルと同じ扱いとする．データファイルは毎日のことであるのでコストもかかるが止むを得ない．

10. 事故時の対応

（1） フォール・バック

何か事故が発生した時に，そのことだけで全システムの機能を停止しないで，サービスグレードは低下しても稼動はするよう種々の手段を考えて置く．J・マーチンのいう graceful degradation である．バック・アップシステム，障害ユニットの切離し，空調機や CV・CF を大容量のものを一つ造るよりもいくつかに分割しておくなどハードウェアやソフトウェアでの工夫が必要である．

最近，分散化の議論が盛んである．集中か分散かはそれだけ取り上げて議論しても仕方がない．私の感じたところでは，もう一つ論点がはっきりしていないように思われるが，どうもリスクの分散から分散化論が出てきているのではないだろうか．コストからいえば分散化はやはり高くつくように思える．ここで注意を要するのは危険分散のためにシステムを分散化しても守るべき対象も分散して増えるということである．要は具体的な条件の中で何を狙いとするかによって分散化か集中化かの議論があるはずである．

（2） 復旧時間の短縮

復旧時間や事故の影響を最小限に抑え得るか否かは，指揮者と要員の動員体制の如何にかかっている．もちろん，日常において非常時の手続を定め，訓練をしておくことは大切である．しかし事故は千差万別であり，多くのことがその場で決定され遂行されなければならない．指揮者の任務は，損害を明らかにし，優先度を判断し，迅速に指示命令することである．余り細かいことに拘泥していると取りかえしがつかなくなったり，復旧が大巾に遅れる．ある程度での割り切りに勇気と決断が要る．逆に言えば，このような資質の

ある人を管理者として任命しておかなければならない．決定されたことが忠実に実行されるためには，指揮・命令系統が明確化されておかなければならないが，これは事前に決めておける．また要員不足では何もできない．いざの場合にオペレータ，CE，SE を動員できなければならない．寮をできるだけセンターの近くに持つとか，SE の連絡網を日頃から確立しておくことを忘れてはならない．

（3） 情報化保険

紙面の都合もありここでは触れないが，あくまでも二義的に考えるべきである．銀行の元帳（ファイル）が全て消失すれば，いくら保険に加入していてもどうにもならない．安全対策の必要性が減少するわけではないことを強調しておきたい．

11. 安全対策を成功させるために

以上に安全対策についてざっと一通り眺めてきた．しかし安全対策を実施していくことは実は案外難しい．当行も上述のことはほとんど実施しているが，それでもまだまだ充分だとは考えていない．今後も引続いて進めて行く考えである．

筆を置く前に，安全対策を実施して行く上でのキーポイントとなると思えることを取りまとめて述べておく．

（1） まず第一に安全対策を意識の上に置くことである．安全性についての意識がなければ危険の存在も気がつかない．対策やアイディアも出てこない．

（2） 安全対策を担当する者を任命することである．プロジェクト・チームを組めたら一番良い．ハード，ソフト，オペレーション，付帯設備などそれぞれの専門家で構成する訳である．しかしそれができない処は一人でも良い，とにかく担当者を任命することである．これが第一歩となる．

（3） 大きく構想をねるのも良いが計画倒れに終ると何にもならない．手をつけられる処，やり易い処から対策を計画し，実行に移して行くことである．そして段階的にコストのかかるもの，難しいものへと拡げて行った方が良い．

（4） 必ず決めたことは文書化し，手続き化することである．口答だけの指示では，いつの間にか元に戻ってしまう．

（5） 安全対策担当者は仮りに一人であっても，これは計画担当者であり，実行段階は職場の一人々々が実行するのだということを全員に徹底させる必要がある．QC と同じで全員に実行者としての自覚をもたせることである．参画意識を持たせることにより，決めたことも守られ易くなるし，提案も出てくるし，危険の存在も目につき改善も進む．

（6） 常に見直しが必要である．環境や条件は常に変って行っている．それに追随した対策が要求されるし見落しも拾える．仮りに他の条件が変らなくても，経年劣化するものもある．

（7） ある対策が他の対策の障害とならないようバランスをとる必要がある．何が重要かをよく見極めることである．

（8） 安全対策の対象を EDP ファンクションと考えることである．コンピュータだけではコンピュータは動かない．

（9） 安全対策にはコストがかかるということを認識すべきである．米国では EDP コストの 10% が安全に対するコストとして支払われているといわれている．ある程度まではコストのかからない安全対策を実行できることも確かだが，全然コストをかけずというのは虫がよすぎる．日本人は従来から空気と水と安全はタダのように考えていた．最近では，公害問題などで空気と水はタダではないとの認識ができたように思われる．イザヤ・ベンダサンの「日本人とユダヤ人」にあるように安全はタダではないことを認識すべきである．

参 考 文 献

1) J. Martin：コンピュータ安全管理マニュアル，リアル・タイム・システム．海外技術資料研究所 (1972. 11).
2) NBS Technical Note.
3) JECC：情報処理の安全対策 (50. 6).
4) 堀内恭一：コンピュータ犯罪，日本工業新聞社．

（昭和 51 年 11 月 9 日受付）