57—S 002

コンピュータ・システムのセキュリティに関する調査研究報告書

昭和58年3月

JIPDEC

財団法人　日本情報処理開発協会

この報告書は，日本自転車振興会から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昭和５７年度に実施した「わが国の情報処理に関する動向調査」の成果をとりまとめたものであります。

はじめに

当財団では，情報処理技術調査研究の一環として，昭和５７年度より２カ年計画で，「コンピュータ・システムのセキュリティに関する調査研究」のプロジェクトに，着手した。

近年，コンピュータ・システムの広範な普及・活用に伴い，その利便性に対する影の面として，コンピュータの悪用，機密データの漏洩等のトラブルの発生が，見受けられ，社会的問題になろうとしている。特に，今後多様化すると考えられる社会的・公共的システムにおいては，犯罪防止およびデータ保護の観点から，セキュリティ対策の充実を図り，コンピュータの悪用や情報の窃取による社会の混乱を未然に防ぐことが，重要になると考えられる。

そこで，本プロジェクトでは，コンピュータ・システムが基本的に具備すべきセキュリティ関連機能，それを実現する上での技術課題および将来の利用形態であるネットワーク・システムでのセキュリティ上の問題点について調査研究することとし，緊急な課題については開発計画の策定を行なうこととした。

今年度は，セキュリティ対策と問題点についての技術面からの調査，および海外の現状と動向を調査した。本報告書は，前者についての成果を，まとめたものである。本報告書が，この方面の関係者の方々に広く利用され，今後の情報処理技術向上の一助として寄与できれば幸いである。

最後に，本調査研究にあたって，ご指導ご協力いただいた，本プロジェクトの研究委員会の委員長各委員を始め関係各位に対し，感謝の意を表します。

昭和５８年３月　財団法人　日本情報処理開発協会

本調査研究で作成した報告書

・コンピュータ・システムのセキュリティに関する調査研究報告書
・コンピュータ・システムのセキュリティに関する調査研究海外調査報告書

コンピュータ・セキュリティ技術研究委員会名簿

（敬称略，順不同）

委員長	斉藤忠夫	東京大学工学部電気工学科助教授
委員	石黒　功	日本電気㈱情報処理第一公共システム事業部第二システム部主任
〃	小笠原謙蔵	日本ＩＢＭ㈱営業企画副部長
〃	川上万寿夫	㈱富士銀行総合事務部システム管理グループ部長代理
〃	寿福利夫	沖電気工業㈱情報処理事業部システム本部開発第一部開発第三課課長
〃	武田　学	国際電信電話㈱技術計画部管理課課長補佐
〃	谷口和道	日本電信電話公社技術局データ宅内部門調査員
〃	千葉恭弘	㈱電通国際情報サービス・システム開発部開発一課長
〃	中島基雄	富士通エフ・アイ・ピー㈱事務システム事業部ＩＰ部技術課長
〃	中村利武	富士通㈱電算機事業本部企画部長
〃	久重剛志	㈱三菱銀行事務本部システム部総括グループ調査役
〃	松田　宏	日本電子計算㈱ＤＰ本部ＤＰ副本部長
〃	水野昌美	㈱日立製作所コンピュータ事業本部本部員
〃	山本欣子	(財) 日本情報処理開発協会開発部長
〃	小関重美	〃　〃　開発部次長
オブザーバ	植松一裕	ファコム・ハイタック㈱ファコム本部システム第一部第三課主任
〃	大川繁喜	日本電気㈱情報処理第一公共システム事業部第二システム部主任
〃	手塚啓一	沖電気工業㈱システム本部開発第３グループ

事務局　(財) 日本情報処理開発協会

目　　次

第Ⅰ部　概　　要

1. 調査研究の背景

1.1 コンピュータ・システムの功罪

１９５０年代に英国において，初めて出現したコンピュータ・システムは，その後３０余年の歳月を経て，今や産業，研究，教育，行政等の社会のあらゆる分野に浸透し，今後，更に人間生活におけるコンピュータ・システムへの依存度は益々増大し続けるものと思われる。

コンピュータ・システムの活用は，社会活動の効率化や利便性の大幅な向上をもたらすのみならず，コンピュータ無くしては不可能と思われる多様な新たな機能の実現を可能とし，それによって人間生活の活動の枠を広げ，併せて人間の能力そのものの拡大にも寄与するものとなる。一方，その広範な普及に伴う多様なニーズへの対応として，コンピュータ・システムの高速，大容量化等の基本機能の向上に加え，入出力，処理方式，記憶方式等を始めとする各種機能の向上と多様化が進み，併せて情報処理と通信の融合によるオンライン処理，分散処理，リアルタイム処理等の広域処理の実現により，時間と距離の克服が現実のものとなった。

あらゆる科学技術は，その華やかな効果の陰に大なり小なりマイナスの面を持つ。そして従来，そのマイナス面を可能な限り抑制すべく，その利用に際しての社会的，制度的ルールの確立と使用者各自の運用上の工夫，あるいは技術的改善の努力等，多角的対策が講じられてきた。コンピュータ・システムもまた例外ではなく，その陰の面の存在を否定する事は出来ない。特に近年，社会的関心を呼ぶものとして，コンピュータの悪用やコンピュータを利用した犯罪，あるいはプライバシの侵害等に関する諸問題がある。

これらの問題がクローズアップされてきた背景としては，幾つかの点が指摘できよう。

① コンピュータ・システムは巨大なブラック・ボックスであり，関係者以外

は，その処理のメカニズムを知る事が出来ない。

② 特にその処理プロセスの細部にわたっては，それぞれのシステムを作成した極く限られた担当者のみしか理解し得ない。

③ コンピュータの処理能力の増大に伴い，官公庁，自治体，企業等における機密に属する情報もコンピュータ処理の対象となってきた。

④ オンライン・システムの普及により，多くの遠隔の端末から，コンピュータ内の情報に容易にアクセス可能となり，データ拡散の危険性が増大した。

⑤ パーソナル・コンピュータの普及により，これらを端末として，種々の社会システムとオンラインで接続しようとする計画もあり，不特定多数のコンピュータ・システムへのアクセスによるトラブル発生の可能性が予見される。

⑥ 現在の技術レベルにおいては，コンピュータ側で，その不正利用を自動的に検出することは極めて難しく，かつ厳重な機密防御のための対策は非常に高価となる。

⑦ 先進国，米国においては，既に１０数年前から種々のコンピュータ悪用や犯罪の事例が報告されていたが，我国においてもここ２・３年間に類似のトラブルが急に増加してきた。

⑧ 従来，少なくとも我国では，性善説に基づいてコンピュータ・システムが運用されてきており，コンピュータ周辺の技術者が悪事を働く事は考慮されていなかった。

⑨ 一方，近年ソフトウェア技術者を中心とするコンピュータ要員の需要は大幅に増大し，これらが一部のエリート集団であった昔とは条件が全く異なってきた。

本来，ある科学技術と，それに基づく弊害を防御，あるいは除去するための技術とは，並行して研究開発されることが理想である。しかしながら，少なく

とも，ことコンピュータに関しては，余りにもその普及が急速であり，加えて，従来はその効率性や経済性に過度の重点が置かれ，それに比較して，コンピュータにまつわる種々のトラブルの防止やその活用上の安全性への配慮は必ずしも充分ではなかった。いうなれば，片手落ちのまま，経過してきてしまったことは否めない。その結果として，上記のような危惧の高まりは，むしろ当然と言うべきであるかもしれない。

今後，コンピュータ技術の一層の向上と，更に広範な普及とを図り，健全な情報化社会の実現を推進するためには，可及的速やかにそのマイナス面を除去すべく，各種の対策が講じられねばならない。

1.2 コンピュータ・セキュリティの考え方

コンピュータ・セキュリティという言葉の定義が現在必ずしも，明確に定まっているわけではない。しかしながら最近になって，その範囲や内容に関して，ほぼ一般的なコンセンサスが得られるようになってきた。当プロジェクトでは，これを以下のように分けて考えることとした。

(1) システム障害に対する安全性

ハードウェア障害，ソフトウェア障害に対する安全性である。

① ハードウェアの故障を防止する。あるいは減少させる。

② ハードウェア故障によるシステム停止やデータ破壊に対処する。

③ プログラム・ミスに起因するプログラムの暴走によるデータ破壊を防止する。

これらの障害に対しては，信頼性の高いハードウェアを用いる，処理系を冗長構成（2.5重系，3重系）し，処理結果の多数決を行なう，処理系のバックアップを完全にし，リカバリ，リスタートに備える，メモリ・プロテクトを行なう等の対策をとる。システム障害に対する安全性とは，システムのインテグリティと，ほぼ等価と考えられる。

(2) 物理的安全性

コンピュータのハードウェアおよびソフトウェアやデータを格納した記録媒体等の，物に対する安全性である。

① 地震，火災，水害等の自然災害から，ハードウェアおよびソフトウェアやデータの記録媒体等を保護する。

② 暴力行為やテロ行為等による人為的破壊行為から，ハードウェアおよびソフトウェアやデータの記録媒体等を保護する。

③ ハードウェアおよびソフトウェアやデータの記録媒体等の物品としての盗難を防止する。

④ コンピュータの出力プリントからの処理内容漏洩，コンピュータが発生する電磁波からの処理内容漏洩等を防止する。

物理的な事故に対する対策としては，例えばコンピュータ室への入退出管理とかコンピュータ室の強固な建造等，やはり物理的対策を主体にすることが多い。従って，物理的安全性とは，むしろその対策の物理性を意味する場合もある。

(3) 誤操作や不当な操作に対する安全性

ミス・オペレーションや不正なオペレーションによるデータやプログラムの変更等に対する安全性である。

① 不注意なオペレーションのミス等によるデータ破壊を防止する。あるいは破壊されたデータを復旧可能にする。

② 正当でない使用者のコンピュータの不正使用を防止する。

③ コンピュータへ権限外のアクセスを行ない，データやプログラムの不当な読み出しや破壊を行なったり，あるいは虚偽データを不当入力し，システムを混乱に落とし入れる等の不正行為からシステムを守る。

これらは，システムの物理的外見には何等の変化も与えないで行なわれる不正や破壊に対する安全性である。例えば，遠隔の端末からデータの不正読み出しを行なっても，記録媒体上のデータが喪失するわけではない。従って，発見が難かしいという特徴もあり，長い間発見されなかった不正が実際にあ

った。後述するように，当プロジェクトの主要な検討テーマである。

1.3 内外の対応

ここでは，主に米国における状況と国内の状況について，概観する。[*1]

1.3.1 米国におけるコンピュータ・セキュリティ

コンピュータ・セキュリティの先進国は，やはり米国であろう。国防省等軍関係のシステムが早くから，機密保護や盗聴防止を目的とした対策を行なっており，それに対応する技術も過去２０年来，多額の費用を投じて研究開発を行なってきた。現在これらの技術成果が徐々に民間へ移転し始めた状態と考えられる。ただ軍関係のセキュリティ技術はその性格上，コンピュータやファイル等へのアクセスの制限（アクセス・コントロール）強化やデータの暗号化に重点が置かれ，民間のシステムとは一味違ったものになっている。

一方，これに対して民間のシステムでは，早くからコンピュータの悪用やコンピュータを利用した犯罪が多発し，これへの対応を迫られてきた。これら犯罪という面に関しても米国は先進国であり，１９６０年代後半から既に事件が発生し，７０年代には大型の事件が多発した。最近の調査によれば，銀行・保険両業界における既発表の件数は約１２０件に上ると言われ，また，これらの事件による損害は年間５０億ドルと見積られている。但し，最近は事件そのものが公表されぬケースも多いと見られており，事実上の損失はこれの数倍にも及ぶという意見もある。

技術的先進性とコンピュータ犯罪の多発という米国の実情は，一見矛盾を含んだ複雑な態様を示しているが，少なくともコンピュータ・セキュリティ問題に対するコンピュータ・ユーザの全般的な関心は，我国に比べ相当高く，かつ

＊１：ここに述べた米国の実情は 1982 年 11 月に約20日にわたり，米国におけるコンピュータ・セキュリティ技術の調査を行なった成果のみによるものであり，その他の詳細な記録に基づくものではないことをお断りする。

歴史的にも長い経緯を伴っている。その結果として，制度面を含め種々の角度からの対応等が実行に移されている。

(1) 国防省のセキュリティ評価センタの設立と評価

１９８１年7月国防省はその関連機関であるＮＳＡ（ National Security Agency ）の中にコンピュータ・システムのセキュリティ・レベルを評価するためのComputer Security Center（ＣＳＣ）を設立した。ＣＳＣの主たる目的は国防省内のコンピュータ・システムのセキュリティ機能を評価するものであるが，その一環としてセキュリティの評価基準（ Trusted Computer System Evaluation Criterion)案を作成し，民間にもこれを公表することによって，その基準の普及と定着とを図っている。この基準はＯＳ機能を中心にしたものであり，AからDの4段階（細かくは8段階）のランク付けが具体的機能との対応によって示されている。

現在，民間の情報処理ベンダにおいてもこの基準が大きな参考となっていると言われる。

(2) 暗号化アルゴリズムの標準化

オンライン・システムの普及に伴い，伝送データの暗号化は通信システムのセキュリティ対策上，強力，かつ重要な位置を占める。また最近は，必ずしも通信のみでなく，コンピュータ内のプログラムやファイルに対しても暗号化を施す計画も出てきた。

暗号化には，その暗号化のアルゴリズムとそれに対する鍵とが存在し，その両者を共に秘密にする方法もあるが，もし充分な強度のアルゴリズムが存在するなら，これを標準として公開し，利用者は独自に鍵のみを機密裡に保護するという発想もある。１９７３年米国のNBS（ National Bureau of Standards ）はこの発想に基づき，標準アルゴリズムの公募を行ない，その結果ＩＢＭの提案が採用され，1977年にＤＥＳ（ Data Encryption Standard ）が民間における標準の暗号化規格として発表された。この標準化は同一アルゴリズムに基づく暗号装置の量産を可能にし，その低価格化を実現

することに貢献している。

(3) コンピュータ犯罪防止法とプライバシ法

米国では現在１４の州で，コンピュータ犯罪防止法が州法として成立している。州により，若干の相違はあるが，コンピュータ処理の対象となるプログラムやファイルをすべて「財産」と見なしており，またそれぞれのコンピュータ犯罪の定義に基づく刑法上の整備を行なっている。また連邦政府においても，現在コンピュータ犯罪防止法が上程されている。

一方，米国のプライバシ法は１９７４年に制定された。これは米国政府内におけるデータの取扱い方法について定めたもので，ヨーロッパのように，民間企業も含めて個人データの取扱いを定めたものとは若干異なっている。

(4) システム監査

システム監査の目的の１つにシステムのセキュリティ機能のチェックがある。米国におけるシステム監査の実施は，１５年余の歴史があり，１９７７年の調査によれば，企業での実施率は既に７８％というデータがある。また米国の国際的な内部監査人協会（ＩＩＡ）が７０年代末にシステム監査手法の体系的な文書化を行なったＳＡＣスタディ（System Auditability and Control）は有名である。

(5) 技術的対応

① セキュリティＯＳの研究開発

国防省が１９７７年より行なっている研究開発の１つにセキュリティＯＳというものがある。これは従来のＯＳに，高度なセキュリティ機能を付加する研究であり，一部にハードウェア・アーキテクチャ上の改造も試みている。現在，なお国防省により幾つかのセキュリティＯＳの研究開発プロジェクトがＳＤＣやハネウェルで推進されており，国防省はこの技術がいずれ民間へ波及することを期待していると言われる。

② 商用セキュリティ・パッケージ等の普及

現在ファイル保護機能を中心とした何種類ものセキュリティ・パッケー

ジが，メーカやソフトウェア・ベンダで開発されて販売されており，既にかなりのユーザが存在すると言われる。また商用のシステム監査ツールも，数多く販売され普及している。

③　商用暗号装置

前述のように，ＤＥＳ標準暗号の発表に伴い，その標準に準拠した多くの暗号化装置が商品化されている。

(6)　セミナー，コンファレンス等の開催

米国ではコンピュータ・セキュリティをテーマとした幾つかのセミナー，シンポジウム，コンファレンス等が盛んに行なわれており，多くの論文やレポートが発表され，また，分野を越えた議論の場も多い。その主催者はメーカ，セキュリテイの専門機関，あるいは学会関連など様々であり，またそれぞれ学術・技術中心か，よりジェネラルな対象をねらうか，教育要素が強いか等の異なる特色があるが，７００名以上もの参加者を集める規模の会合も幾つかあり，既に１０年近い歴史を持つものもある。

(7)　メーカの対応

民間企業に広くセキュリティ機能を普及させるには，コンピュータ・メーカが中心となり，ハードウェア，基本ソフトウェアにわたるベーシックなセキュリティ商品を開発し，標準品に近い形で低価格でユーザに提供する事が最も効果があると言われる。前述のセキュリティＯＳも将来その様な対象となって初めて普及するものと思われる。

現在，米国ではＩＢＭが最も積極的にセキュリティ関連技術の商品化に努めているように見える。またハネウェルも，現在，極めてきめの細かいアクセス・コントロール機能を持つ汎用ＯＳ"MULTICS"を持ち，またＩＣカードの開発も行なっている。その他のメーカも軍関連のプロジェクトにおいて得たセキュリティ技術のノーハウをもとに，徐々に民間用システムにもその効果の普及をはかる役割を果している様に思われる。

(8)　ユーザの対応

米国においても，金融関連企業が最も積極的にセキュリティ対策に取り組んでいる。他の民間企業はまだセキュリティ対策のコスト問題が大きな関心事であり，セキュリティ技術の導入にさほど積極性を持っていないと言われる。当初の期待ほどには暗号装置の販売実績が思わしくないというのもその現われであろう。金融関連の企業では，まずセキュリティ強化のため，システムの運用基準を厳密に規定し，その運用をサポートする機能として，適切な技術的プロダクトがあればそれを導入するという態度である様に見える。しかし中には，極めて積極的に自らの手で新しいセキュリティ関連技術の研究開発を行なうという銀行もある。

一方，官公庁，自治体，あるいは類似の公共的機関においては，その性格上かなり積極的にコンピュータ・システムのセキュリティ対策を行ない，特にデータベースやファイルの機密保護に重点が置かれているようである。

1.3.2　日本におけるコンピュータ・セキュリティ

日本におけるコンピュータ利用の歴史は約２５年を経過し，オンライン・システムを含む多様なコンピュータ・システムが社会の各分野に浸透し，大きな効果をあげている。この間におけるコンピュータ・システムに対する利用者の要求，およびサプライヤの努力は，もっぱらシステムの経済性と効率性に重点が置かれ，システムの安全性やコンピュータの悪用の防止，データ機密保護等のセキュリティ面の対策は，二次的と考えられ勝ちであった。この最大の理由は，幸いなことに，日本では従来，コンピュータ犯罪や機密データの漏洩などの事故が極めて少なかったという事実による。しかしながら，１９８１年に何件かの新しいタイプのコンピュータ犯罪が集中的に発生し，急激に社会の関心がコンピュータ・セキュリティ問題に向けられるようになった。

欧米に比較すると，組織的対応はやや遅れたが，現在までに我国で行なわれてきたコンピュータ・セキュリティへの対応としては，以下のようなものをあげる事ができる。

(1) 諸官庁における対応

① 通産省における活動

ⓐ 「電子計算機システム安全対策基準」の設定と「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」

通産省は１９７７年に「電子計算機システム安全対策基準」を設定した。これは主として，コンピュータ設備の物理的安全性に重点を置いており，３００項目以上にのぼる基準となっている。一方この基準の適用に関して，同省は更に，１９８１年９月から，我国の情報処理サービス業やデータベース・サービス業の各事業所が，この基準を充たしているか否かを認定する制度を設け，現在実施中である。尚，同基準の内容は以下のような項目を含んでいる。

イ. コンピュータ，端末，データ保管庫，空調，電源等の設備の物理的安全基準

ロ. 設備の設置場所に対する基準

ハ. 事業所の組織体制・責任体制に対する基準

ニ. コンピュータ室への入退管理を含むコンピュータ・センタの運用管理基準

ホ. データおよびソフトウェアの管理基準

ヘ. 教育・訓練の実施

ト. システムの安全性に対する内部監査

ⓑ コンピュータ・セキュリティ・ガイドライン策定計画

産業構造審議会の答申の一環として，１９８２年にコンピュータ・セキュリティ対策のためのガイドラインを作成する目的で，運用・技術・法制度面にわたる総合的セキュリティ問題の検討を行ない，ガイドライン策定のための作業を開始した。１９８２年における検討は，以下の3つの視点から行なわれた。

イ. ハードウェア，ソフトウェアを総合したシステムの高信頼化対策

ロ. コンピュータ犯罪の防止，検出のための対策

ハ. データの機密保護対策

② 郵政省における活動

ⓐ 「データ通信セキュリティ基準」の作成

１９８２年中に郵政省はデータ通信のセキュリティ対策として，約９０項目の基準案を作成する予定である。その内容は，信頼性を中心に以下のようなものを含む。

イ. 通信ネットワークの信頼性強化のためのバックアップ回線および迂回ルートの設定に関する基準

ロ. センタ・コンピュータ間のバックアップ機能

ハ. ネットワークの異常検知機能

ニ. トラブル発生時のデグラデーション（ degradation operation ）機能

ホ. コンピュータ・センタや交換センタの地震・火災等の物理的セキュリティ機能

ヘ. 暗号化

ト. アクセス・コントロール

チ. リソース保護

ⓑ ミックス暗号方式の開発

１９８０年から１９８２年にかけて郵政省は，ミックス暗号方式と呼ぶソフトウェアを開発した。これはＤＥＳ暗号系のキーを公開鍵暗号系のＲＳＡ方式で転送するものである。

③ 大蔵省における銀行業務の監査強化

大蔵省は１９８１年に集中的に発生した金融機関におけるコンピュータ犯罪を重視し，１９８２年春に総ての金融機関に対し，それぞれのコンピュータ・システムのセキュリティ対策につき，現状と今後の措置に関する報告書を提出させ，セキュリティの強化を要請した。

④ 警視庁のコンピュータ犯罪対策

警視庁においては，今後多発することが予想されるコンピュータ犯罪に対処するため，専門の部署を新設し，担当者のコンピュータ教育訓練を開始した。

(2) 電電公社によるデータ通信に関する事故防止対策

電電公社では，１９８２年に発生した回線の盗聴事件をきっかけに，データ通信に関する事故防止対策委員会を設け，以下のような対策を検討し，実現に移しつつある。

① 業務上の秘密確保対策の公社内部での徹底

② 保全管理体制の強化改善

③ データ通信システムのセキュリティ機能強化

- アクセス・コントロール機能
- リソース保護機能
- 本人確認技術
- 暗号化
- 無人化運転方式の開発

④ システム監査機能の充実

⑤ 職員のモラルおよび倫理感の向上

(3) 技術的対応

① 研究開発

日本におけるセキュリティ技術の研究開発は，残念ながら，あまり活発ではなかった。従来，コンピュータ関連犯罪の発生が少なかったことが最大の原因であるが，最近の犯罪多発が刺激となり，ようやく対応策の検討が組織的に始まった段階である。もっとも，米国等からの影響もあり，アクセス・コントロール等の技術は，ＩＢＭ等のコピーに近いとは言え，既に製品化され使用されている。また，前述のミックス暗号方式の試作や，マイコン・ソフトウェアの暗号化，ＤＥＳ系の暗号装置の試作等の試みも

ある。

従来，我国では物理的セキュリティ，特に地震，火災等の自然災害への対応に重点が置かれ，システムの悪用防止等に対する新しい研究の芽は，ごく最近まで皆無に等しかった。

② セキュリテイ製品の利用

ＩＢＭのファイル保護用パッケージＲＡＣＦ，あるいは類似のセキュリティ・パッケージ等も我国では，まだほとんど利用されていない。また，暗号装置（輸入品）も現在のところ，我国ではほとんど販売実績がないと言われる。

(4) ユーザの対応

我国で最もセキュリティ対策を積極的に推進しつつあるのは，やはり金融機関である。また，情報処理サービス業や，公共的性格を持つコンピュータセンタ等も，近年セキュリティに対する関心は高まったものの，信頼性強化に専ら重点が置かれ，例えば，暗号化の実施や，新しいセキュリティ技術の導入等に踏み切ったところはほとんどない。

(5) システム監査

システム監査への関心も，ここ２・３年来相当高まってきている。しかしながら，昭和５４年１１月における実施率は２７.６％であり，その後の増加を考慮しても，米国とは大きな差がある。但し，金融機関の実施率は高く，中にはシステム監査支援機能をオンライン・システムの設計段階から有機的に組み込み，成果をあげている銀行もある。

(6) メーカの対応

ＯＳを中心とするアクセス・コントロールやファイル保護機能は，既に標準機能として提供されている。また，最近は金融関連のシステムでは，それなりのセキュリティ機能が要求され，アプリケーション・レベルでのセキュリティ対策の実現例は多いようである。しかしながら，基本機能としての新しいセキュリティ技術の開発や，パッケージの普及等に関しては，まだ積極

的とは言えない。勿論，これはユーザ・ニーズの不足という最大の原因に基づくものである。今後は，ユーザ側でのセキュリティ対策の推進と共に，セキュリティ関連製品の需要が拡大し，これに対応してメーカ側でも新製品の研究開発が活発になると予想される。

2. 調査研究の目標

2.1 位置付及び目的

既に第1章で述べたように，セキュリティ対策は，今日のコンピュータ・システムにおける重要な課題である。かって，セキュリティ対策を強化するための投資に，消極的な経営者が多い時期もあったが，最近では経営者のセキュリティ対策の重要性に対する意識は，かなり改善されたと言われる。

しかしながら，実際に具体的な対策を行なう段階では，様々な問題点が指摘されており，現在，必ずしも各企業で積極的に対策が行なわれているとは言い難い。問題点を大きく集約すれば，次の3点にまとめることができる。

① どんな危険性（リスク）があるのかの分析が難しい。

② 最良の対策方法や手段が見出しにくい。

③ 費用に対する効果を明確にしにくい。

これらは，いづれもセキュリティ対策における特徴的問題である。①の危険性については，過去の事故や事件を参考にして検討する方法も考えられるが，将来起きると思われる事故や事件等は予測しにくい。②の対策については，現在に至るも決定的な方法というものは見出されていない。また③の効果に関しては，コスト／効果を評価する評価基準やデータが不足している。

現在，セキュリティ対策の主な手段は運用（人手）による対策である。これは，効果の大きい技術的対策が，まだ少ないことにもよる。運用による対策は重要で，将来も必要であることには変りがない。しかしながら，応用システムの規模が確実に拡大しており，それに併う対策要員も確実に増加することになる。将来，そのために必要な人材（対策要員）が，大量に確保できるだろうか。仮りに，確保が難しいとするならば，技術的支援を強化しなければならない。その意味で，現在の技術レベルは必ずしも充分とは言えない。むしろ，現状の技術に対して不信を抱く，運用面の関係者も居る。さらに，昭和56年のよう

にコンピュータ・システムの事故[＊1]が続くと，一般の利用者の間に，技術とは災いをもたらすもの，という誤まった概念を植えつけることにも成りかねない。コンピュータ・システムの安全性を強化する技術の進歩が待ち望まれる。

セキュリティ支援技術の開発は，現在まだ活発であるとは言えない。第一の理由は，開発が極めて難しいことであり，第二の理由は，かって後向きの技術（不要な技術）と言われたことからも分かるように，重要性の認識が不充分なことである。後向きという観点では，同じセキュリティ対策でも，信頼性対策と犯罪対策では異なった側面を持つ。人間がすべて善人であっても，機械の故障は発生する可能性があり，機械の信頼性（安全性）を高める技術は，むしろ前向きの優先度の高い技術として認識される。一方，桃源郷では犯罪対策技術などは，ほとんど不要である。現在の社会が桃源郷であると認識する人はほとんどいないと思うが，技術者，研究者等は，日頃身近に犯罪が発生しないと，つい桃源郷と錯覚して，犯罪対策技術の重要性を見逃してしまう。

今日のように，多数のコンピュータ犯罪が報告されるようになっても，依然として，開発が極めて難しいこと，コストが膨大になりそうな可能性があること等が障害となり，研究さえも活発ではない。どうしても，身近で時折発生する故障対策の方に熱が入ってしまう。

さて，ここ１０年間のコンピュータ技術の進歩は目覚しいものであった。特にＩＣ技術の進歩は，安価な高速大量処理を可能にし，センサ技術とインタフェース技術（ＡＤ変換，ＤＡ変換）の発達は，これまでコンピュータ処理が困難であった領域でのコンピュータ処理を可能にした。今後も一層の飛躍が期待されている。このように技術が進歩すると，以前は困難であった新しい犯罪対策技術の実現可能性が出てくる。これらの新しいコンピュータ技術による新し

＊1：宮城第一信用金庫事件（昭５６／３），三和銀行事件（昭５６／９），長野県中野市農協事件（昭５６／９），平和相互銀行事件（昭５６／１０）等のコンピュータ犯罪および富士銀行（昭５６／２），太陽神戸銀行（昭５６／３）等のシステム・ダウンのよる混乱

いセキュリティ支援技術の実現可能性について検討することは，大いに意義あるものとなろう。新しい技術的対策が実現できれば，それによって運用のレベルも向上し，総合的にシステムの安全性を大幅に強化することも可能になるだろう。

当プロジェクトでは，従来，重要であるにもかかわらず注目されなかった技術 — コンピュータ・システムを悪用した犯罪防止，データ保護およびプライバシ保護を支援する技術 — について重点的に調査研究することとし，昭和５７年度から２ケ年計画で，将来の開発を前提にした作業を開始した。

本作業の主な目的は，

① セキュリティ対策の強化のために必要な既存の支援技術の改良とは何か，新しい支援技術とは何かについて検討すること。

② その結果得られた既存技術の改良案および新技術の開発案をまとめ，その実現可能性や有効性についての検討を踏まえたうえで，開発が期待される技術（既存技術の改良を含む）として提案すること。

である。これらの検討結果に基づいて，新技術の開発が行なわれ，セキュリティ対策の強化に役立つことを期待する。

2.2 昭和５７年度の作業内容

今年度は，既存の支援技術の改良および新しい支援技術の方向を見極めるため，下記の４項目について作業を行なった。

- 応用システムの現状のセキュリティ問題や対策についてのまとめ
- 現状のセキュリティ支援技術（関連技術）についてのまとめ
- 対策に有効であると予想される既存技術の改良や新技術の検討
- 将来のコンピュータ・セキュリティについての問題提起

① 現状のセキュリティ問題や対策についてのまとめ

過去に発生したコンピュータ犯罪の分析および金融業や情報処理業を中

心とした実態調査を通して，現状における問題点と対策について検討を行なった。しかしながら，応用システムのセキュリティ問題や対策を調査すること自体が，プライバシ（この場合，企業のプライバシ）の侵害になる恐れがあり，この問題の複雑さを浮彫りにした作業でもあった。従って，本報告書の第Ⅱ部で触れているセキュリティ問題についても，差支えのない範囲で記述されたものであることを，あらかじめ，お断りしておく。

② 現状のセキュリティ支援技術のまとめ

既に実用化されて実際に使用されている支援技術あるいは既に試作を完了した支援技術をまとめ，その問題点や課題について分析を行なった。今年度は，セキュリティ支援技術の範囲について厳密な定義はせずに幅広くとらえ，セキュリティ関連技術として検討した。

③ 既存技術の改良および新技術の検討

前記①，②の検討を踏まえたうえで，既存技術の改良や新技術の可能性について検討した。この結果得られた新しい要素技術を提案の形にまとめた。これらの新技術の有効性および実現可能性につき，今後の検討が必要である。

④ 将来のコンピュータ・セキュリティについての問題提起

１０年後のコンピュータ応用がどのように展開されて行くか正確に予測することは困難である。ただ，より一層応用範囲が拡大し，ネットワーク利用が活発になることだけは，間違いないと思われる。このような状態におけるセキュリティ問題は，現在に増してさらに重要な課題となることは容易に推測される。そこで，仮定の作業ではあるが，将来のシステム形態に基づく新たなセキュリティ上の問題の提起を試みた。

3. 昭和５７年度の検討結果

コンピュータ悪用による不正防止を目標にして進めてきた今年度の検討結果について，簡単にまとめる。詳細は，第Ⅱ部を参照されたい。

3.1 コンピュータ・セキュリティの現状

(1) 応用システムの現状

現状のコンピュータ・システムにおいても必要な対策は行なわれている。特に金融機関では，きめの細い対策が行なわれている。

キャシュ・カード犯罪に対しては，カード発行手順の改善，不正利用に直結する暗証入力ミスの監視，ビデオによるＣＤ，ＡＴＭの監視等の対策が実施されており，さらに顧客に対して，カード管理の重要性をＰＲし，一般の認識を高めるよう努力している。営業店では，端末オペレーション・キーの管理強化，異例取引チェックの徹底，締上げによるチェック等，運用上の対策を中心にして，ミスや不正の防止に努めている。センタでは，入退出管理等の運用上の対策は当然のこととして，ファイルの二重保管，プログラムの改造時のチェック，定期的なマスタとの突合せ等，現在可能な対策はほとんど実行されている。

さらに，比較的安全と考えられる特定通信回線を利用してオンライン・システムが構築されており，システム監査も導入されている。応用システムの中でも最も高いレベルのセキュリティを要求される金融業としては，当然の処置とも言えよう。

しかしながら問題点がないわけではない。例えば，

- 磁気ストライプを誰でも手軽に読取れるようになり，カード内に暗証等の秘密情報を入れられなくなった。
- 暗証による本人確認には一抹の不安が付きまとう。
- 異例取引等のチェックの自動化が難しい。

・通信回線から暗証等の秘密情報を盗聴される危険がある。

・センタにおけるプログラム，重要データの保護が完全とは言えない。

・システムの複雑化，ブラック・ボックス化に対する対応が必要である。

・システムの大規模化，広域化に対する対応が必要である。

等の問題があり，第3次オンラインでの大きな課題となろう。

一方，情報処理業では，業務の性格上，マシンへのアクセス管理とファイルの保護（リソースの保護）に重点が置かれているのは当然である。

第一に，ＴＳＳ等のログオン時には，ユーザＩＤとパスワードにより，ユーザ識別と本人確認が行なわれる。不正ログオンの試みやログオン・ミス等は，すべてログ・ファイルに記録される。ログオンの失敗が数回続いた時，ログオン禁止を設定する方式も使われている。第二に，いわゆるユーザ・プロファイル管理により，各種のファイルへのアクセス権が，ユーザ毎にきめ細かく設定されている。そのため，ログオンに成功したユーザは，自身がアクセス可能なファイルのみ使用できるようになっている。さらに，各ファイルに別途パスワードを付けるような機能もある。ユーザが，ファイルにアクセスした状況は，徹底的にログ・ファイルに記録される。もっとも，これはセキュリティ対策というよりも，課金のための基礎資料作成という意味あいの方が強いかもしれない。データベースでは，それ自身でアクセス・コントロールを行なっている。データベース全体は，ユーザ・プロファイル管理下に置かれているのが普通なので結局，二重のチェックが行なわれることになる。

次に，運用面でも徹底した対策がなされているのが理解できる。例えば，

・磁気ストライプ・カード等による入退出管理と記録

・業務の分割……パスワードを付与する部門とシステム開発部門の分離等のように，業務分割による組織化と責任体制の明確化

・運用手順の明文化

等である。設備面では，通産省の指導基準である「電子計算機システム安全対策基準」に準拠しているのは言うまでもない。これらは，ファイルの保護に寄与している。しかし，問題点もある。例えば，

- グループ・パスワードの変更が簡単にできない。そのため，頻繁に変更するのがつい面倒になる。
- システム・ユティリティによるダンプに対して，ロック機構がない。
- パソコン端末を使用して，データベースのコピーが簡単にできる場合がある。
- 外部に持ち出すファイルの暗号化等が実行されていない。
- ソフトウェアの信頼性向上のために要求仕様言語が効果的と思われるが，操作性の良いものがない。
- 定期保守等の場合に，秘密が漏れる可能性がある。人手による対策が可能ではあるが，大きな手間を要するため，実際は対策不可能である。

等である。その他，安全性を高めるためのコストが，ばかにならないという問題は常に付いてまわる。大量のログ・データは，通常ほとんどチェックされないという問題もある。

以上のように，金融業においても情報処理業においても，それぞれ問題点を抱えていることは事実であるが，それらは別の手段でカバーされ現段階では極めて順調にシステムは稼動している。時々，事故や事件の発生が伝えられるが，いづれも致命的問題を生ずるまでには至っていない。むしろ，現状でのセキュリティ対策は，かなり高いレベルにあると言えよう。

これまで，比較的セキュリティ上の問題は少なかったが，今後に大きな課題を抱えているシステムとして，自治体のそれがある。自治体では，これまでバッチ処理が中心であったため大きな問題が少なかった。もっとも，バッチ処理であっても基本的対策（センタの対策：ファイルの管理，入退出管理等）は必要で，既にほとんどの自治体のシステムで実施されている。現在，

オンライン化が進みつつある段階であり，今後はセキュリティ対策に力を入れる必要があろう。特に情報公開制度開始に併うプライバシ保護は，大きな課題となろう。システム監査の実施も必要になるだろう。

このように，各システムとも何らかのセキュリティ対策が実施されているのは，今日のコンピュータ・システムの大きな特徴であろう。しかしながら，現在の対策で完全というわけではなく，さらに対策の強化が必要なことも確かである。また，現在は人手による対策が中心となっており，いづれ自動化する必要性も生じるであろう。

(2) セキュリティ関連技術の現状

セキュリティ関連技術として，極めて多数の方式やツールが開発，研究されている。ところが，実際に使用されている技術に限定すると，極めて少数になってしまう。その主なものは，

① パスワード，ＩＤカード

② アクセス・コントロール（ＲＡＣＦ等）

③ アプリケーションに内蔵したチェック機能

④ ログ・データ収集機能（ＳＭＦ等）

である。①は，本人確認やファイルにロックをかける（ロックワードとも呼ばれる）時に使用され，②は，ファイルやリソースの保護に，③は不当な業務処理の監視に使われる。④は不正や悪用を後日チェックするための記録である。

新しい技術として，ダイナミック・サインや暗号等のような強力な手段も開発され，実用化しているが，ほとんど使用されていない。このため，技術的なツールは既に充分であり，むしろ，その機能が充分生かされていないとする意見もある。

しかしながら，現在のツールは，実用性という点では問題がある。前述の①～④は，ほとんど市販の商品をユーザは利用しているが，金融業等では，ログ・データ収集機能を自主開発していることが多く，一般に，市販のもの

は操作性が悪いと言われる。暗号装置にしても，キー管理という重要な運用についてのプランが明確でない商品が多く，ダイナミック・サイン装置も，その最適使用法がはっきりしない，コストが高い等の問題があると言う。

このように，これまでの技術は，あまり作業現場のニーズに則しているとは言えないようで，その優秀な機能を無駄にしている例が多く見られる。今後，これらの改善を行なって，システムの安全性向上のために効果的に活用する必要があるだろう。また，印鑑の自動照合のように，まだ実用化されていない技術もあり，今後の研究開発は多いに期待される。

3.2 検討すべき基本技術

今後検討すべき基本技術を表３－１に示す。次にこれらの技術内容について簡単に説明する。

① 本人確認

本人確認は，セキュリティ対策の入口であり，ここで充分なチェックがなされないと，以後のセキュリティ機構の効果が皆無になると言ってもよい程，重要な技術である。現在は，パスワードやＩＤカード等が主に使用されている。新しい技術は２種類ある。一つは，生まれながらに持っている身体的特徴（指紋，声紋等）を利用するものであり，もう一つは，従来の書類システムで用いられているチェック方法（印鑑，サイン等）の自動化である。前者は，理論的にもっとも確度が高いことが特徴であり，後者は，従来の書類システムにもそのまま適用できることが特徴である。技術的には，既にかなりのレベルに達しており，あともう一歩で実用化というところまできている。残された大きな課題は，装置の安定度の確保とコストの低減であろう。

② オペレーティング・システムの強化

オペレーティング・システムには，現在でも各種のセキュリティ機構が付加されており，これらを利用した，かなりのレベルの対策が可能である。

表３－１　検討すべき基本技術（つづく）

目的		技術内容
本人確認		• 指紋照合技術 • 声紋判定技術 • サイン判定技術 • 手形照合技術 • 印鑑照合技術
オペレーティングシステムの強化	アクセス・コントロールの強化	• レコード単位の機密保護機能 • データ項目単位の機密保護機能
	プログラムの保護	• プログラム・ライブラリ管理ツールの強化
	詳細なチェック・データの収集	• ロギング機構の強化・改善 （記録情報の詳細化と操作性の改善）
データベースの保護（不当検索の防止）		• リレーショナル型データベースの関係演算の妥当性チェック機構 • 推論検索防止技術 • データベースの暗号化
ハードウェアの強化	CPUの強化	• ロギング・プロセッサによる効率改善 • ファイル暗号化機構 • 指紋センサ機構付コンソール
	入出力装置の改善	• 残存データー括消去機構付磁気テープ装置 • 残存データー括消去機構付ディスク装置 • フィルド・マスク機構付プリンタ • 暗号化機構付磁気テープ装置
	記録媒体の改良	• 鎖錠付媒体（媒体のケースに物理的キーをつけたもの） • 揮発性メモリによる固体ファイル • 再書き込み不能ファイル（光ディスク等）
ソフトウェアの高信頼化		• 要求仕様定義言語 • システム設計支援ツール • 高信頼化プログラミング言語 • 検査ツール • 保守支援ツール

表３－１　検討すべき基本技術（つづき）

目的		技術内容
通信回線保護	盗聴検出	• 盗聴用搬送電波の検出 • 通信回線回路インピーダンスの変化検出
	盗聴防止	• メッセージ・データの暗号化
	挿入防止	• メッセージ・データの暗号化 • メッセージ発信時間の管理 • メッセージ連続認識番号の管理 • 回線の二重化によるメッセージ二重伝送
	改ざん防止	• メッセージ・データの暗号化 • パケット交換網の適用 • 光通信
	発信端末回線確認	• コール・バック方式による接続 • 相手通知，閉域接続
	自分宛及び相手確認	• デジタル署名
データ暗号化		• 慣用暗号（ＤＥＳ暗号） • 公開鍵暗号（ＲＳＡ暗号） • 暗号鍵管理技術 • 暗号の複合化 • 暗号の標準化 • ソフトウェアによる暗号変換
入出力装置（マンマシン・インタフェース）		• 相互牽制方式の入力 • 入力の冗長化 • 印鑑等の画像データ高精度読取りと知的照合プロセス • 手書き伝票の高度読取り
業務処理の監視		• チェック用データ収集の自動化 • 判断アルゴリズムの研究開発

しかしながら，改善すべき点も多い。レコード単位の機密保護機能やデータ項目単位の機密保護機能は，よりユーザ・ニーズに密着したアクセス・コントロールを提供できる可能性があり，新しいプログラム管理ツールは，ライブラリアンの負担を軽減する可能性がある。また，ロギング機構の改善は，システム・チェックを容易にする。これらは，既存技術で実現可能であり，問題は，これらの機能を，ユーザにどれだけ理解してもらえるかである。

③ データベースの保護

データベース特有の問題としては，リレーショナル型データベース（RDB）のアクセス・コントロールがある。RDBでは関係演算による検索が大きな特徴であるが，これがセキュリティ上の大きな問題点にもなっている。一方，各種の検索を巧みに組み合わせて，本来知ることのできないデータを引き出す推論検索の防止も大きな課題である。いずれも，現状では効果的な防止方法がなく，今後の大きな研究テーマである。

④ ハードウェアの強化

ハードウェアにおける課題は，ロギング専用のサブ・プロセッサ，暗号化機構および入出力装置と媒体の改良である。どの課題にも，基本的な技術的障害はなく，問題はコスト／効果である。これらの新技術は，まだ応用面がはっきりしておらず，その効果も明らかでない。従って，技術開発と共に，その具体的応用方法を研究し，世の中に受け入れ易い環境を整える必要がある。

⑤ ソフトウェアの高信頼化

仕様書どおりのプログラムを作るのが難しいという問題は古くからある。バグをなくすだけでも大変な作業であるが，これに悪意のプロセスが組み込まれては，それらの検出がますます困難になる。仕様とプログラムの間の人間の介在をなくしてしまえば，このような問題は少なくなる。その意味で，要求仕様定義言語は効果的である。同時に，プログラムの検査

ツールも重要である。いづれも現在は満足すべきものがなく，今後の研究が期待される。

⑥　通信回線保護

通信回線については様々な危険性が指摘されているにもかかわらず，対策が進んでいないというのが現状である。決め手は，メッセージ・データの暗号化およびメッセージ確認技術の確立だと言われ，各種の方式が提案されている。しかしながら，既に提案された方式には，まだ解決すべき問題が多数あり，より一層の研究開発が期待される。

⑦　データ暗号化

新しい暗号の中心は，ＤＥＳ暗号であろう。ただし鍵の長さ等，検討の余地は残されている。ＤＥＳ暗号等の慣用暗号と共に公開鍵暗号も重要な開発課題となろう。現在ＲＳＡ暗号がもっとも有望と思われる。これらの暗号は，ハードウェアで変換するのが望ましく，専用ＬＳＩチップ等の開発が望まれる。このような暗号の実用化研究と共に，鍵の管理問題の解決が重要課題である。郵政省の開発したＭＩＸ方式も一つの方法である。

⑧　入出力装置（マンマシン・インタフェース）

内部社員の不正を技術的に防止するのは難しく，むしろ一つの処理を複数名で行ない，互いにチェックし合う方式で防止するのが有効ではないかと思われる。入力時にもこの方式を適用し，相互牽制方式の入力が適当と思われる。印鑑等の自動照合，手書き伝票の直接入力等は古くからある課題であるが，まだ実用上の問題点が多い。しかしながら，これらは本質的にすぐれたセキュリティ技術なので，今後の研究開発に対する期待が大きい。

⑨　業務処理の監視

現在は，人手による監視（事後チェック等）が主体であり，自動化の研究は始まったばかりである。不正を監視するためには，高度な判断機能が必要であり，これまでのコンピュータ・プロセスで実現されてきた判断機

能で実現可能かどうか，よく分っていない。さらに判断アルゴリズムもよく分っていない。従って，判断アルゴリズムやそれを効率よく実現するプログラム言語等，基礎的な部分から研究を始める必要がありそうである。

さて，以上の技術を見渡すと，既存技術の改良が多いことに気が付く。そして，既存技術の大部分は，フィルタ的技術であることも分る。フィルタ的技術は，正当な処理中に混じった不正処理を発見するためには有効であるが，正当な処理と複雑に化合した不正処理の発見には効果が少ない。このような巧妙な不正処理を発見するためには，高度な不正分析技術が必要である。この技術は，処理結果（あるいは処理経過）を分析する技術で，処理結果の高度な加工と判断能力が欠かせない。現在は，主に人手にたよる作業であり，業務処理の自動監視や自動監査と一脈通じる技術である。このアルゴリズムは極めて複雑であることが予想され，単純なロジックにはならないかもしれない。従って，ルール・ベースによる自動診断システムの応用や，さらに人工知能の応用も考えられる。今後の研究が多いに期待される技術である。

3.3 将来システムのセキュリティ問題

(1) ネットワーク高度利用に伴う諸問題

将来，コンピュータ・ネットワーク・システムは異企業間のシステムへと拡大して行くことは確実と思われる。このようになると，ネットワークを統一的に管理することがだんだん難しくなり，セキュリティ対策も高度なものが要求されるようになる。

将来のネットワークで具体的にいかなる危険性があるかを推定するのは難しいが，少なくとも次に示すことは言えよう。

① 現在のネットワークが抱えている危険性（盗聴，介入等）は，将来もある。

② ネットワークに接続している企業自体が不正を行なう可能性がある。

上記②は，将来新たに発生する恐れのある問題である。書類による取引で

は，オリジナル（正）とコピー（副）の区別がはっきりし，法制度も完備しているのに比べ，電子化処理では，取引を統一的にオーソライズする何かがないと，トラブルを発生する。ところが，ネットワークはだんだん統一的管理が難しい方向へ進むため，極めて難しい問題を生じる。

一つの対策方法として，図３－１に示すセキュリティ・ボックスによる通信メッセージのオーソライズおよび高信頼記録（不正も記録される）が考えられるが，その記録技術や管理方法等，解決すべき課題が多く，今後の検討が期待される。

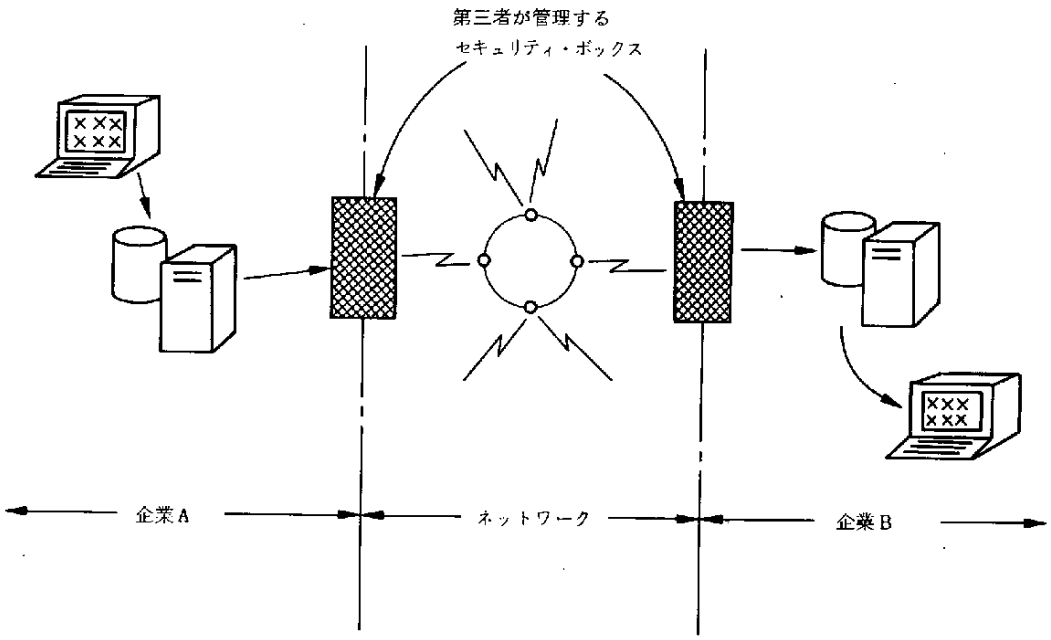


図３－１　セキュリティ・ボックスの概念

(2)　応用システムの諸問題

今後のコンピュータ・システムの利用動向を一言で表すなら，それはコンピュータ・ネットワークの徹底活用ということになるだろう。既に金融業では，その入口に達っしており，情報処理業では，新しい事業としてその応用形態を検討している。また，ニュー・メディア公共システムは，コンピュー

タ・ネットワーク利用を個人レベルまで拡げようとするものである。

第一の問題は，これらは目的の一つとして，すべてを電子的に処理するペーパーレス処理を指向していることである。このことによって，処理の高速化，効率化が達成可能であろうが，電子化処理というのは，充分な対策を講じないと，前述(1)のような問題が発生する恐れがある。現在研究されている個人向システムは，その処理の記録をサービス提供側だけで行なうようになっている。一般的に個人側（ユーザ）の記録はあまり信用されないため，サービス提供側でミスや不正があり記録に問題（料金等）が生じても，個人側（ユーザ）が一方的に損をするケースが多い。現実に，これに似たトラブルが発生している。これの対策にもなり得るセキュリティ・ボックスも，個人レベルでの利用を考えるとコスト的に少々問題がある。将来個人参加が拡大するのは確実であり，この辺りの改善を急がねばならない。

第二の問題として，システムの複雑化，巨大化がある。高度に発達したコンピュータ・システムでは，その全貌を１人の人間が把握するのは困難であり，必然的にブラック・ボックス化が進むだろう。ブラック・ボックス化が極度に進むと，今度はそのブラック・ボックスの全機能さえ把握できなくなるという問題が生ずる。すなわち，設計書どおり入力された時の出力は分っても，設計外の入力があった時の出力は分らないというブラック・ボックスが生ずる。（現在でもモジュール化されたプログラムで同種の問題が発生している。）これは，犯罪の温床になりかねない。数千キロメートルも離れたセンタの詐欺プログラムで，巧妙に不正が行なわれては，その現象だけで不正の実態を把握するのは難しいだろう。

コンピュータを人類のための道具とするために，これら諸問題を一つ一つ解決して行かねばならない。

4. コンピュータ・セキュリティの課題

4.1 セキュリティ問題の背景

企業，官庁などの種々の組織体において，各種のデータを発生し，伝達し，処理し，あるいは蓄積する過程において，誤ったデータが混入しないこと，データが正しく保管され，正しく利用されるようにするためには各種の工夫が行なわれて来た。この問題は，データがコンピュータによって取扱かわれるようになる前に，データが紙に書かれていた時代からもやはり重要な問題であった。

データがコンピュータによって取扱かわれる場合の基本的なちがいのひとつは，コンピュータの中を通して，人の目に見えない形でデータへのアクセスが行なわれるようになったことである。コンピュータで取扱かわれるデータは，またそれ以前の人手によるシステムに比べて格段に集中化されるようになっている。この理由から，コンピュータの故障や，自然災害によってデータが損なわれることによる影響も大きくなって来ている。コンピュータを通して悪意の妨害をする人にとっては，人間を相手にする犯罪行為に比べて，心理的に悪の意識をあまり持たずに犯罪を犯しやすいという点も指摘されている。

今日，企業や官庁においては，数値データの大部分はコンピュータで処理されるようになっており，さらにそれ以外の文書データのコンピュータ化も進められている。コンピュータでデータを処理し，保管する場合それが常に安全であると感じ，安心していられるような状態が求められるのは当然である。

銀行のシステムでは人々の財産が取り扱かわれる。人々の財産の記録は，昔は紙の上に記載されたインクの跡として残され，現代では記録は磁気媒体上の微少面積に磁化の方向として残される。そのどちらがたよりになるかはともかくとして，それが安心できるものであることは何よりも重要であろう。

病院における患者データについては，財産にかかわるものでないにしろ，紙に書いたカルテの秘密が守られたと同じレベルで，不正なアクセスから守られなければならない。

しかしコンピュータ技術の普及によって，人々がコンピュータにアクセスする機会はますます増加して来ている。これは同時にコンピュータに対する不正なアクセスの機会も増加していることを意味している。ネットワーク化の進展もコンピュータへの外部からのアクセスを容易にする。ネットワークも特定通信回線による限定された利用者のシステムから電話交換回線網，パケット交換網などを利用したネットワークに進展して来ると，物理的にネットワークを閉じることによって得られるアクセス制限が実現できなくなる。

このようにコンピュータの普及により，コンピュータのデータの重要性がますます高まると同時に，セキュリティ上の問題がますます困難になる方向に進んでいることは否めない傾向であると言えよう。

コンピュータ・セキュリティに関する技術も，その重要性の認識の増大と共に，急速に発展しつつある。しかしコンピュータ・セキュリティは，コンピュータのハードウェア，ソフトウェア，オペレーションのあらゆる側面に関連し，その開発から運用に至るすべての局面にかかわっている。このためセキュリティ技術は多岐にわたっており，完全にすべての問題が解決されるとは言えないのが現状であり，我国においても，コンピュータ犯罪の事例が報道される例も少なくない。

コンピュータの社会的重要性が今後ますます高まることは明らかであり，コンピュータ・セキュリティは，社会におけるコンピュータ利用の進展の前提条件として確保されなければならない。

4.2　コンピュータ・セキュリティの諸局面

コンピュータの正常な運用に支障を生ずる原因には種々あるが，通常

① コンピュータのハードウェアの故障およびソフトウェアの誤り

② 天災および悪意の妨害によるコンピュータおよび端末の物理的な破壊

③ コンピュータのソフトウェアの改ざん，悪意のデータ入力，悪意のアクセスによるデータの改ざん／乱用

の三種類に分類される。広義のセキュリティ問題はこの三つを含むが，ここでは主として③の局面について検討の対象にしている。

③はコンピュータ犯罪もしくは犯罪には至らなくても，コンピュータの不正な使用にかかわる問題であり，これに関するセキュリティ対策は，こうした悪意からコンピュータをいかにして保護するかという問題である。

コンピュータに対するアクセス経路は種々存在する。図４－１はコンピュータに対する種々のアクセス経路を示したものである。コンピュータに対する入力帳票がオペレータを経由して端末からコンピュータに与えられると考えれば，この間の各要素が悪意によるアクセスの発生源となり得る。

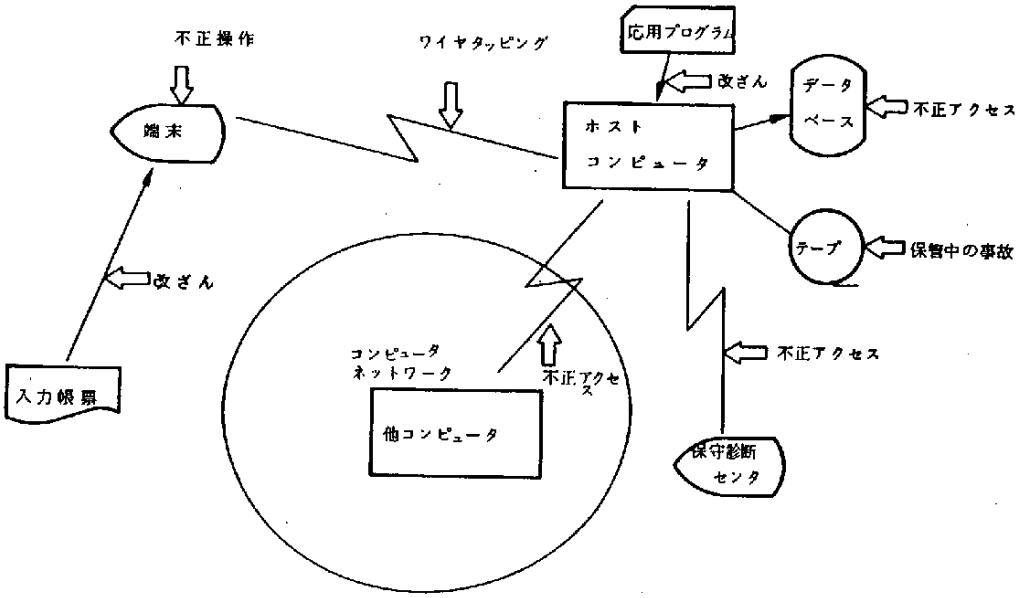


図４－１　コンピュータ・セキュリティの侵害経路

入力帳票の改ざん，オペレータに対して悪意の誤った情報を与えることなどは，コンピュータ・システム外の問題である。コンピュータ化以前にも同様の問題はあったことであり，事務組織における倫理観念の向上と相互牽制の体制

の確立によらなければ防止できない問題である。しかし，コンピュータ化によってその影響も大きくなっており，またコンピュータ化を前提とすれば，その方法にも再検討を必要とする。

端末においては，端末を操作する人間が正当な資格を持った人であるかを確認する本人確認がその対策の中心となる。本人確認の手段としてのカード，パスワードなどについても，それに関連する不正の発生の防止に関して種々の対策が必要となる。

通信回線を通してコンピュータにアクセスする場合には，通信回線が長距離を通ることから，それを通る情報に対して不正を行なう機会が増えることが問題となる。通信回線そのものを保護することも重要である。通信回線上の情報を暗号化することは，通信回線は完全には信用できないものであることを前提としてセキュリティを守ることである。通信回線で盗聴が行なわれていることを何らかの手段で検知する手段も研究されている。しかし通信回線は数が多く，回線ごとにハードウェア的に対処するにはコストが過大になり勝ちな点が問題である。

コンピュータ内部においてはマルチ・ユーザの環境で動作する機械の各種のリソースを，資格のあるユーザにのみ使わせるための，リソース管理が行なわれて来た。データベースのように多様なデータがひとつのシステムの中で扱かわれるようになると，読み書きのできる権利は，ひとつのファイルのデータ項目の各々ごとに管理できるようになって来ている。しかしデータベース管理システムごとの保護方式の考え方の差，本人確認の方法との関連などにおいて，データベースの保護にも残された問題はある。

応用プログラムの開発過程，応用プログラムの改造の過程にも不正の入る余地がある。応用プログラムの開発者が不正を行なっていないかを検査する技術は，プログラムの内容に立ち入るために困難も多い。

コンピュータのハードウェアおよびシステム・プログラムは計算機製造会社によって保守されるのが普通であるが，このレベルでは非常に高い特権でシス

テムのほとんどのデータにアクセスできる。最近ではハードウェアおよびシステム・ソフトウェアの保守のために，通信回線を通して，場合によっては電話交換回線を通して，保守センタへの接続が行なわれていることも多く充分注意を要する。

コンピュータがネットワークを通して他のコンピュータと接続されてコンピュータ・ネットワークが形成されている場合には問題はさらに複雑となる。コンピュータが接続されたときに，他のコンピュータからのアクセス要求を，端末からのアクセス要求と同一に扱かう方法もある。この場合にはアクセス管理は端末からのアクセス管理と同一のレベルで扱かわれることになる。しかしこれではネットワークの機能が限定されるため不都合である場合には，第一のコンピュータでアクセス管理を行なったあとは，コンピュータ間の接続は，よりゆるやかなアクセス管理で接続する必要も生ずる。このような場合に，あるコンピュータが他のコンピュータに不正を働く余地が生ずる可能性も高まる。

コンピュータの運用の実態では，コンピュータ・セキュリティに関するこれらの諸局面は，それぞれ異なった様相で現われて来る。これらについてはそれぞれの局面ごとに対策が考えられているが，事故はそれらの対策のすき間をくぐって生じ得る。コンピュータ・セキュリティの確立のためには，これらの諸局面における個々の対策のみならず，これらを総合的にとらえた全体としての対応技術が重要となろう。

4.3　システム環境とコンピュータ・セキュリティ

コンピュータが計算機室内のオペレータによってだけアクセスされ，ファイルに恒久的に記憶されたデータはなく，またコンピュータでは同時には単一のジョブしか実行されないような環境では，セキュリティの問題は実質的には発生しない。現在ではこのような環境は小規模なパーソナル・コンピュータの中にしか存在せず，通常の大型機の環境ではあり得ないと言って良い。

現在のコンピュータは少なくともマルチ・ジョブの状況で，コンピュータに蓄

積されたファイルを利用して運転される。このような条件で現在の各種システムを考えてみても，コンピュータ利用環境によってセキュリティに対する要求および条件は異なっている。

① 応用が特定しているか汎用であるか

応用が特定しており，特定の種別の伝票の処理だけを端末から行なうシステムと，端末からTSS 等によって種々のプログラムを作成し，それぞれの応用プログラムを任意に開発できるようになっている場合とはセキュリティに対する要求が異なる。利用者が自由に応用を開発できるようになっているシステムでは，計算機を使いやすくするために，リソースの利用に関して高い自由度を持っていることが望ましいが，これはセキュリティの向上とは相反する傾向にある。

② スタンドアロン・システムかネットワーク・システムか

最近の大型機で特定の計算機室内からしかアクセスできないものは少ないとは言え，アクセスする人の範囲あるいはアクセスするときの環境を充分限定することができるシステムと，それを限定しにくいシステムとではセキュリティの条件も異なる。さらに複雑なネットワークで，ネットワークの中に複数個のコンピュータがあり，処理は複数のコンピュータにまたがって実行されるようなシステムではさらに条件が異なる。複数個のコンピュータを持つシステムでも，システム内のリソースの管理を一ヶ所で集中して行なえる場合と行なえない場合では条件が異なる。

③ 利用する通信手段の種別

利用する通信手段が専用回線であるか，交換回線であるかによってもセキュリティの条件は異なる。衛星通信の場合のように原則として自由に盗聴できる通信手段もある。通信回線が交換手段を含んでいても，交換網が特定の目的にのみ用いられ，その利用者が制限されている場合と，交換網をだれもが原則として自由に利用できるようになっている場合とは異なる。

④　利用する端末の種別

ネットワークで利用できる端末が基本的機能のみを持った低レベルのものか，オフィス・コンピュータ，パーソナル・コンピュータのように高度の機能を持つものかによってもセキュリティの条件は異なる。もしパーソナル・コンピュータのようなコンピュータのネットワークとしてシステム全体を構成し，ファイル等の機能も分散しているようになればさらに条件は異なる。

このようにセキュリティに関する条件はシステムの構成形態，応用の形態等によって大幅に異なるのが普通である。現在のコンピュータ応用技術は，一般的により自由なアクセス，より広汎な分散化に向って進んでいるように思われる。このような状況の中でコンピュータ・システムはますます高度なセキュリティを要する重要な情報を取扱かう方向に進んでいると言えよう。

4.4　システム化の進展とセキュリティ

コンピュータ・システムの発展は常にシステムによる能率の向上とシステム機能の高度化を指向している。前節で見たように最近のシステム発展の方向はそれぞれの局面で，セキュリティ確保に困難をもたらす方向に発展しており，セキュリティ技術の課題は，そうして生じた困難を克服しながらいかにセキュリティを確保するかという問題となっている。

こうしたコンピュータ・システムの発展方向はさらに省力化，処理の迅速化を要求している。省力化が端末オペレータに進められれば，組織内における相互牽制の体制を弱くする可能性もある。省力化のためには書によらない書類の決済を要求しており，コンピュータのソフト・コピーだけを見て承認を行なう事務処理の形態も考えられている。ディジタル署名の技術に代表されるように，このような処理も技術的には可能な段階に達しているが，ディジタル署名を用いた応用システムではさらに高い一般的なセキュリティ上の要求が課せられる

と言って良い。

コンピュータ・セキュリティの基本は我々がコンピュータで不安を持たずにデータを取り扱かうことができる状況を確立することにある。現在のコンピュータ技術の目指す方向である，より広汎なシステム化，高能率化が実現できたとしても，それがデータの取り扱かいに不安を残すものであってはならない。この意味でシステム化の進展が社会に受け入れられるかは，セキュリティ技術にかかっていると言うことができよう。

第II部　各　　論

1. 応用システムのセキュリティの現状

本章では，社会的にみて，公共性が高く，セキュリティ面が重要視される代表的な業種である金融業，情報処理業，そして自治体の3つを採り上げ，そこでの応用システムのセキュリティ対策の現状について述べる。

1.1および1.2は，銀行のオンライン・バンキング・システムを対象としたものである。近年，オンライン・バンキング・システムを悪用したコンピュータ犯罪がマスコミに採り上げられ，話題になってはいるが，我国では，バンキング・システムがもっともセキュリティ対策が講じられているシステムである。ここでは現在我国の都市銀行で実施されている運用を含めたセキュリティ対策について述べる。

1.3～1.5の情報処理業は，他人の情報を取り扱い，そして処理することを業とする民間企業である。これらの企業では，現在通産省の「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」のセキュリティ認定基準を確保する対策が採られているが，それらを含め，情報処理業特有のセキュリティ面での対策の現状をまとめ，その問題点や課題を指摘する。

最後の1.6の自治体は，住民に対し，各種のサービスを行う行政機関であり，個人のプライバシ情報が集中的に集められ，蓄積されており，情報公開制度とも関連して，セキュリティ対策がますます重要視されて来た。ここでは現在除々に実現に移されつつある住民情報オンライン・サービスを中心とした地方自治体でのセキュリティ対策について述べる。

1.1　金融業（その１）

金融機関の事務処理のコンピュータ化および金融機関相互間のオンライン提携など，年々機械化が進展する中で，コンピュータ・システムに関連した不祥事件や事故が増加の傾向にある。コンピュータのサポートする領域が広範囲になる状況では，不祥事件，事故が何らかの形でコンピュータとかかわりをもつようになる事は当然である。コンピュータ・セキュリティ，コンピュータ犯罪がマスコミ等で喧伝される中で事務処理がコンピュータ処理されている事だけで，コンピュータ犯罪と騒ぎたてられるケースもあり，本来の意味でのコンピュータ・セキュリティ，コンピュータ犯罪の範疇に入らないものまでも広義のコンピュータ・セキュリティ，コンピュータ犯罪と位置づけられているきらいがある。あまり広義にコンピュータ犯罪をとらえすぎて，その対策を考えると本来の対策がなおざりになったり，焦点がぼける事も考えられ，位置づけを明確にした対策の構築がのぞまれるところである。確かに機械化を進めることで新たな型の犯罪・事件を生みだす可能性はあり，機械化に対応した内部管理体制の確立が必要である。機械化の進展は，

① 取引の即時化，広域化を可能にした。例えば即時に，他行の遠く離れた支店への送金が出来る，あるいは，取引銀行，取引店以外でも自動化機器による支払いが出来る。

② キャッシュ・カード利用が一般化し，少人数に限られていたカードの仕組みが，一般に相当知られるようになってきた。

③ コンピュータ過信で何でもコンピュータ処理は正しいと信じこむ風潮がある。

④ 機械化を効率化のみに重点をおき，内部牽制体制の確立をおこたる傾向がある。

といった状況を生みだし，これらの背景の下でコンピュータ犯罪が発生しているといえる。

金融機関の機械化の現状は第２次総合オンライン・システムの完成期をむかえ，

第3次オンライン・システムの基本構想着手の時期にあるが，通信回線の自由化，店舗行政の緩和により開かれたシステムとして外への拡がりが急速に進展されることが予測され，コンピュータ・セキュリティ対策は従来以上にウェイトをおいて検討すべきテーマとなりつつある。

現時点における金融機関のコンピュータ・セキュリティ対策の現状および問題点と将来における対策，セキュリティ対策上のコンピュータ技術に期待する事項につき以下に述べる。

金融機関におけるコンピュータ犯罪を犯罪を犯す者の側面からみると外部者による犯罪と内部者による犯罪にわかれ，内部者による犯罪はさらに，コンピュータ・システムを利用する立場の者（営業店の操作者等）とコンピュータ・システムに直接関与する者（オペレータ，プログラマ）による犯罪にわかれる。

1.1.1　外部者による犯罪

金融機関コンピュータ・システムの仕組みを知り得た外部者がコンピュータシステムの仕組みを悪用し，金銭の不法領得をする等のケースであり，現状ではキャッシュ・カードに関連した犯罪が大半である。しかしながら今後の展開を考えると通信回線の自由化による回線網を利用した犯罪（データ盗聴・破壊，金銭不法領得），コンピュータ・システムの盲点をついた犯罪等，複雑なテクニックを使った犯罪の可能性も考えられ，これらの対策に真面目に取り組まなければならない。

(1)　キャッシュ・カード対策

キャッシュ・カードは給与振込の拡大，カードによる新種サービスの提供，各銀行における自動化機器の拡充，自動化機器を利用した銀行間提携の支払いシステムの展開，自動化機器の稼動時間の延長等により利便性が増すことで利用客は増加の一途をたどっており，この増加とともにキャッシュ・カードに絡まる事故・事件が多発の傾向にある。特に最近は磁気ストライプの内容を解読する，あるいは回線を盗聴しカードの暗号を知りカードを偽造する

等，犯罪が複雑化している。

① 現状における対策

現状におけるキャッシュ・カードの犯罪防止対策としては，カード発行時点，および，利用時点で主として以下の対策が講じられている。

ⓐ カード発行時点の対策

イ．顧客からのカード発行依頼を受ける際に，暗証の受付は管理者がおこなっている。

ロ．カード発行業務は顧客と直接の接触のない事務集中部門でおこなっており，一連のカード作成工程はコンピュータ処理されており内容につき操作員は知りえない。

ハ．作成後のカードは顧客宛郵送しており，住所の確認出来ない顧客にはカード発行が出来ない。

ニ．同一口座に対してカードの二重発行が出来ないようシステム上の考慮をはらっている。

ⓑ カード利用時点の対策

イ．顧客からのカード盗難，紛失の届けがあると，該当口座に事故登録をおこなうことで支払いが出来ないようガードしている。

ロ．不正にカードを利用した時点で，どの場所の自動化機器が使用されたかを即時に表示できる逆探知システムがオンライン・システムに組込まれている。

ハ．暗証を間違って一定回数以上入力すると，そのカードを無効にしている。

ニ．モニタ・テレビ，ビデオ装置によりカード利用者を特定している。

② 現状システムにおける問題点

イ．カード・システムの一般化，磁気ストライプ内容読取り装置の入手容易化によりカード内容が読み取られる可能性が増している。

ロ．暗証コードを暗号化せず伝送しており盗聴される危険性がある。

ハ．暗証コード4桁で偶然の一致の可能性が考えられる。

③　今後の対策

イ．カードに保有している暗証を廃止しセンタ・ファイルに一本化する。

ロ．暗証登録および暗証入力の操作を顧客側からのみ可能とする。

ニ．暗証コードを複数キーの組み合せとし，偶然一致の機会を少なくする。

ホ．カードによる支払い限度を設定する。

(2)　通信回線利用による犯罪対策

現状は大半の金融機関が特定通信回線を使用し，独自の電文構成で取引処理をおこなっており外部者が犯罪を企てる事は技術的に困難である。しかしながら，通信回線の自由化によるネットワークの拡がり，データ通信手順の標準化，電文の共通化，公衆回線の利用が進む事で今後十分犯罪の発生が予測でき，この進展とあわせて対策をたてる必要がある。

①　現状における対策

イ．特定通信回線の使用と独自の電文構成，通信方法をとることによる盗聴，データ侵入の防止。

ロ．システムと通信可能なターミナルを特定することにより，不特定ターミナルからの取引の防止。

ハ．通信制御プログラムによる応答電文に加えて，業務処理プログラムで入力ターミナルに必ず応答電文を出力することによる正当電文の確認。

ニ．回線単位，ターミナル単位の取引件数，金額のセンタ計と営業店計の勘定突合によるチェックをおこなっている。

ホ．各ターミナル別に通信番号を保有し取引の連続性を管理している。

②　現状システムにおける問題点

イ．電文の暗号化が一部のシステムにしか組み込まれていない。

ロ．電文盗聴に対するチェック機能がない。

③　今後の対策

イ．電文の暗号化を進める必要がある。このためには解読されにくく，か

つ，低コストの暗号化技術の提供がのぞまれる。特に自行内のシステムから外部システムとの接続が普及する状況においては独自の暗号化では対応が限定され，コスト高となるとともにシステム対応が複雑となることから，外部接続システムとの接続には標準化された暗号化技術が必要である。

ロ．重要な電文に関しては（例えば一定金額以上の振込）取引電文と別建てで承認電文を送る仕組みをより簡単な操作で可能なシステムの実現がのぞまれる。

ハ．ホーム・バンキング，ファーム・バンキングの展開で外部のシステムから直接銀行システムへアクセス出来ることになることから，本人確認技術の向上がのぞまれる。

1.1.2　営業店の操作者等の内部者による犯罪の対策

金融機関の機械化の急展開に伴い事務処理の総てが機械処理されており，営業店における不正事件，事故のほとんどがコンピュータ・システムと何らかの関連をもっている。機械処理の進む中で，機械システムによる牽制機能は従来の手作業ベースによる処理に比べ相対的に充実されているのが一般的である。しかしながら，コンピュータ・システムに対する過信，システムの考慮洩れ，効率化偏重によるシステムの欠陥等も一面で否定できず，これらの盲点をついた営業店操作員による犯罪が発生している状況にある。

(1)　現状における対策

①　端末機の操作面

イ．特定のオペレーション・キーでのみ操作を可能にしている。オペレーション・キーの管理は管理者がおこない，毎日始業時に操作員に貸与，終業時に回収している。

ロ．オペレーション・キー別に操作できる取引を特定している。

②　異例取引のチェック

イ．オンライン照会により一定金額以上の取引を照会できる。

ロ．日単位に異例取引の個別の取引明細を還元している。

③　キャッシュ・カード発行

イ．暗証番号届の管理者による管理を行っている。一般の操作員は知ることができない。

ロ．カード発行は事務センタで集中処理している。

④　記帳事務・精査事務

イ．通帳取引については通帳の磁気ストライプ保有の口座番号を使用，誤った通帳への記帳防止をはかっている。

ロ．無通帳の取引については伝票面にコンピュータ保有のカナ氏名を印字し伝票記帳の氏名との確認をおこなっている。

⑤　締上げ

イ．ターミナル単位に取引収支を伝票計とコンピュータ計を突合し，収支一致を確認している。

ロ．毎日の勘定科目別の収入，支払および残高をコンピュータ作成し，営業店全体での収入・支出の一致を確認している。

ハ．重要帳票の発行枚数等の管理をコンピュータ作成の精査表により，おこなっている。

⑥　自店検査・自主点検

本部検査担当者による検査に加え，定期的に営業店サイドで重要項目につき自店検査，自主点検をおこない手続きどおりの事務処理がおこなわれているかを確認している。

⑦　防犯用ビデオ監視装置

店内の営業場を中心に防犯用ビデオ監視装置を取りつけ外部者と併せ内部者の不審な動きを記録にとることで牽制機能を果している。

(2)　現状の問題点と今後の対策

①　取引の即時処理，広域化に伴う対応，営業店で発生する大半の取引がオン

ライン処理され，また，金融機関ネットワークの拡がりにより，端末機で入力した時点で即時に，しかも，距離に関係なく（場合によっては海外まで），多額の資金の移動が可能となっており，現状のチェック・システムに加え，入力した時点での異例取引のきめ細かいチェックが可能なシステム対応がのぞまれる。

② コンピュータ・システムによる顧客チェックの充実

コンピュータ・システムによるチェック機能を高度化し，顧客単位の取引状況に応じた顧客単位の管理システムの導入がのぞまれる。例えば，顧客の取引履歴情報により個別取引の正当性をシステムでチェック出来る仕組みなどがあげられる。

③ 操作者単位の操作可能取引のよりきめ細かな管理

操作者ＩＤをシステムで保有し，操作者別に操作の出来る取引を設定できるシステムとし，操作者単位のオペレーション履歴をよりきめ細かく把握出来る仕組みが必要と考える。特に，地域センタやポータブル端末等操作者が今後ますます多様化する状況では，上記対応は早期システム化がのぞまれる。

④ コンピュータ・システムに対する理解度を高める教育の充実

エレクトロニック・バンキングの展開が進む中で今後ますますコンピュータ処理の範囲が拡大していくことから，営業店の管理者，操作員に対し，正しいコンピュータ・システムの理解を促す教育の充実がのぞまれる。

1.1.3 開発部門／オペレーション部門の内部者による犯罪対策

現在までのところ，この分野における犯罪は日本の金融機関では，ほとんど発生していないため，必ずしも現在までたてられている対策で十分であるか実証できない。しかしながら，この部門において犯罪が計画・実行された場合の被害は予測できない損失をこうむりかねないことから充全な対策を立てておくことがのぞまれる。特に，コンピュータ化の進展に伴い重要な情報は総てコン

ピュータ処理され，またシステムそのものも単なる事務処理にとどまらず高度な情報検索などに利用されており，重要な情報・プログラム等の詐取といった新たな犯罪の発生が考えられる。

(1) 現状における対策

① 重要エリアの入室管理

コンピュータ・ルーム，ＭＴ保管庫等の重要エリアについては，ＩＤカードによる入室チェックをおこなうとともに，モニタ・テレビによる監視をおこなっている。

② 運用部門と開発部門の組織的分離

イ．運用部門はソフトウェアの内容／データの内容を知ることが出来ない。開発部門は本番のデータを操作することは出来ない。

ロ．運用部門において，コンピュータ操作セクションと作業指示セクションとデータ準備セクションが別建てとなっている。

③ オペレーション内容のチェック

承認されていない作業が実行されていないかチェックのため，作業指示書とコンピュータ実行ジョブ・リストとの突合をおこなっている。

④ データベース保護

イ．パスワードにより作業者別にアクセス出来るデータベースの範囲を特定している。

ロ．磁気テープについては，ボリューム番号による管理をおこない，データ内容に関する表示はしていない。

⑤ 検査部によるＥＤＰ部門の検査

営業店検査と同一基準で運用部門，開発部門に対する検査部によるＥＤＰ検査が実施されている。

⑥ 元帳ファイルの残高検証

毎日，科目別の元帳ファイルの口座単位の残高のトータルと，営業店のバランス・シートの科目別残高との突合をおこない，ファイルとバランス

・シートの一致の確認をしている。

⑦ キャッシュ・カード発行の管理

キャッシュ・カード発行業務は営業店の発行登録オペレーションにもとずき事務センタで集中発行されているが，発行の作業工程は総て機械処理され，操作員は暗証等の内容を知り得ない仕組みになっている。ブランク・カードの管理はセンタの特定の管理者を定め厳重な管理をおこなっている。

⑧ 開発プログラムの管理

イ．重要プログラムについては，コード・レベルのチエックを第三者によりおこなっている。

ロ．新・旧バージョンのソース・レベルの突合をおこない余分な修正がおこなわれていないかチェックしている。

ハ．品質管理チームによるテスト・チェックをおこない，第三者によるチェック強化をはかっている。

(2) 現状の問題点と今後の対策

① 重要データの保護機能が不十分

重要データ保護のためのソフトウェアは，いくつか提供されているが，この機能をフルに発揮させるにはシステム環境の整備を伴う。環境整備のために既存システムの大幅修正を要し非現実的であり，新たなシステムを構築する段階で組み入れていくしかない。

② システムに精通した者の不正使用に対するガード機能

システム・プログラマ，システム・オペレータ等システムに精通した者は人数が限られており，彼らの技術レベルで故意におこなわれる犯罪につき現状レベルのチェック・システムでは限界がある。異例オペレーション情報を管理者にレポート出来るようなシステム・サポートがのぞまれる。

③ プログラム改ざん防止対策

プログラムの新・旧バージョン比較の汎用システムの提供がのぞまれる。

④ ＯＳ，ユティリティ・プログラムの管理の強化

メーカ側から提供されるＯＳ，ユティリティ・プログラムについてはユーザによる内容検証は不可能に近く，提供メーカ側による組織的な対応を期待する。特に標準化の推進に伴いメーカ提供のソフトウェアへの依存度がますます高まる状況にあり上記対応がのぞまれる。

⑤　システム監査ツールの充実

現在実施されているシステム監査は手続きどおりの手順が実行されているかどうかのチェックが中心で，監査人によるマニアル・ベースの監査が主体である。今後の期待技術として汎用的に使用できるシステム監査用プログラムの提供が期待されるが，これらの技術を有効に生かすには，システム自体の標準化の推進が前提となろう。

⑥　暗号化技術の向上

データベース，プログラム，電文等，システムに関連する多くの分野で暗号化処理がのぞまれる。現段階の暗号化方式では，システム負荷面，鍵の管理面等解決すべき問題が多く残されている。

1.1.4　金融機関セキュリティ対策の今後のあるべき方向

金融機関における今後のセキュリティ対策で，特に重点をおいて取り組むべき事項として

①　機械化の進展と歩調をあわせた内部牽制システムの確立

②　コンピュータ・システムを標準化し標準化をベースとした各種セキュリティ面の汎用技術の利用

③　システム監査の強化，監査プログラムの活用

④　データの統合化とデータ管理の強化

⑤　コンピュータ・システム関連分野従事者の職業倫理面の強化

等があげられよう。新しい技術の導入は新しい問題を生みだすことからシステム化に併せて常にセキュリティ対策を講じていく必要がある。

1.2　金融業（その２）

バンキング・システムはその公共性の高さ，一旦障害が発生した場合の社会的影響の大きさから，障害対策あるいは犯罪防止対策等のコンピュータ・セキュリティに関しその充実・徹底が要求され，監督官庁・公認会計士等外部からの監査・検査も実施されている。

一方，オンライン・システムにおいては巨大なネットワークを構築し，大規模なファイル保有と多数のトランザクション処理を行なっており，処理能力の確保と効率化が強く要求されている。

こゝでは，バンキング・システムにおけるセキュリティ対策のうち技術的側面に焦点をあてゝ現状と問題点，更には将来期待される技術について述べる。

1.2.1　第一次オンライン・システムにおけるセキュリティ対策

1960年代後半には，銀行の大衆化路線に伴なう事務量の急増に対応して事務処理の省力化を主眼とした第一次オンライン・システムが進展した。

この第一次オンライン・システムは省力化を主目的としており，セキュリティに関しては二義的にしか考えられなかったのは否めない事実であろう。とはいうもののバンキング・システムは，その公共性・社会性の強さから次の様なセキュリティ上の配慮がなされており，大きい問題もなく第二次オンライン・システムへと移行していった。

① 取引毎（トランザクション単位）のチェック機能は従来のオフライン処理に比べ格段に充実した。即ち，支店から文書ベースの顧客元帳がなくなりオンライン・ファイルとしてセンタに集中され，オンライン端末から直接アクセスされることとなり，口座毎の残高チェックあるいは通帳の盗難・紛失等の事故情報に関するチェック等が取引発生の都度即時に可能となったのは画期的なことであった。又ファイルのセンタ集中化により同一銀行内では全国どこの支店でも取引が可能となり，処理の広域化がもたらされたが，種々のチェック機能はシステムで一律処理可能となった。

② 第一次オンライン・システムにおける省力化は内部後方処理を主たる対象としておりセキュリティに関しても銀行内における過誤・犯罪防止対策が主体となっている。即ち，通常オペレーションにおいては端末機の使用者・鍵番号等をジャーナルあるいは取引ログ・ファイルへ記録し，特殊なオペレーション（事故情報登録・解除，異例取引等）に対してはオーディター・キーの使用あるいは上位者による承認操作，更にこれらの特殊な取引については取引結果を事後にチェック・リストで確認する等二重・三重のチエック手段が講じられた。これらは従来のオフライン処理に比べシステムによる自動的なチェック，その場その場でのチェック・承認，より早い時点でのチェックを可能としセキュリティ面でより充実したものとなった。

1.2.2 第二次オンライン・システムにおけるセキュリティ上の問題

1970年代に入って本格化した第二次オンライン・システムは次の様な特徴をもっている。

① 顧客ファイルの統合化あるいは主要業務相互間の複合処理化等を中心とした統合システム化

② 全銀システム等のインターバンク・システムあるいはＳＷＩＦＴシステム（Society for Worldwide Interbank Financial Telecomunication）等の海外通信網との接続をはじめとした対外システム接続の本格化

③ 公共料金・給与データ等外部とのデータ授受の急増

④ CD（自動支払機），AD（自動預金機），ATM（自動入出金機）等の自動化機器の急増

⑤ システム開発の効率化・高信頼化要求の高まりと運用の自動化・省力化の推進

これに伴ない発生ないし認識された，セキュリティ上の問題点及びそれへの対応については以下の様な点が指摘されよう。

(1) システムの統合化

ファイルの集中化・統合化に伴なう複合処理化の推進により，一回の操作で従来の数倍の処理を行なえることとなり，人手の介入が少なくなったことから感違い・ミスによる誤謬の入り込む余地が減少した。この意味でセキュリティ機能の向上が認められる反面，一旦悪意・故意による不正が入り込んだ場合は従来に比べ発見が遅れる可能性が高くなっているといえる。これを検出するために，アプリケーションにおける内部的な整合性チェックを相当組み込んでいるものの限界があり更にこの様なシステムを汎用的な形で提供するのは困難であると考えられる。従ってこの種のチェック・システムはユーザで独自に開発し，管理体制の充実と組み合わせてより高度のセキュリティ機能を実現していくほかない。

又，窓口処理の合理化・効率化を狙った窓口一線体制についても一つの取引を一人の窓口担当者が処理することとなり内部牽制機能が働き難くなる危険があり，システム上の対応と同時に管理体制面でも相応の対応を検討しなければならない。

尚，ファイルのセンタ集中化に対応してはセンタの防災・犯罪対策としての入退室管理システムの利用も含めた警備管理体制の充実を図っており，最近ではファイルの分散保管，重要ファイルの疎開，災害時の遠隔地におけるセンタでのシステム稼動等が検討され一部では実施に移されているといわれている。

(2) システムの広域化

ファイルの集中化を前提とした同一銀行内における他支店顧客分の処理を可能とする全店扱の増加，銀行間の取引を可能とする全銀システム，TOCS[*1]，SICS[*2]，NCS[*3]等のインターバンク・システム，更に海外通信網との接続を行なうSWIFTシステムへの参画等対外システム接続の本格化はシステムの広域化をもたらし，セキュリティの対応にも変化が生じた。

＊1：都銀オンライン・キャッシュ・サービス

＊2：六都銀キャッシュ・サービス

＊3：ナショナル・キャッシュ・サービス

全店扱は第一次オンライン・システムで達成されたファイルの集中化をベースとした即時チェック機能を前提としており，従来の取引毎のチェックに加え統合化されたシステム全体としての勘定突合（中間精査・オンラインによる勘定照合等）を行なうことにより一定レベルのセキュリティ機能を確保している。

インターバンク・システムについては，一種の共用ネットワーク・システムでありソフトウェア面では通番管理・リカバリー機能のほか参加行・店舗のチェック等セキュリティ上の対応が行なわれている。しかしながらハードウェア面では,特段のセキュリティ対策は講じられていないのが実情である。今後通信回線の自由化等周辺環境の変化により接続形態の複雑化・接続端末の多様化が急速に進むことが考えられ，これに対応して接続端末インタフェースの標準化あるいはデータの暗号化等が必須となってこよう。技術的対応としての暗号化については，我国で初めての盗聴事件とされている北海道銀行事件以来具体的検討はかなり進んだものの実施には移されていない。これは暗号化のみですべて解決する問題ではなく，かつコスト上の問題もあり，進展しないものと考えられる。たゞ1982年６月に郵政省が発表した暗号化方式を使えばコスト的にも現実的なものとなる可能性もあり，今後この種の技術開発が進むことが期待される。

(3) データ交換

公共料金・給与データ等外部とのデータ授受は一般企業におけるコンピュータ処理の進展に伴ない急増した。これらのデータ授受は当初の文書ベースの授受から磁気テープあるいはフロッピー・ディスク（ディスケット）等磁気媒体での授受へとシフトしてきた。授受媒体が磁気化したことにより大量のデータが少量の容器・媒体で授受されることとなり運搬の効率上大きい効果を生み，運搬時における種々のリスク回避という面からのセキュリティ機能も格段に向上したといえる。

しかしながら磁気媒体については現物はそのまゝでは判読できないものの，

従来に比べ大量のデータが手軽に持運べかつ機器さえあれば短時間に大量データのコピーも可能であり，この面からセキュリティ対策が必要とされよう。

現状では従来と同様に管理面・体制面での対応が中心とならざるを得ないのが実情である。たゞ物理的な運搬時のリスク回避という意味では最近一部で実施されているオンライン接続によるデータ伝送が有効と考えられる。今後はデータ授受に伴なう資金効率の向上，情報の早期入手等のニーズから，制度上の制約がなくなればオンライン接続によるデータ伝送の普及が予想される。

この場合，セキュリティ面からは回線利用に伴なう新たなリスク（回線あるいはネットワーク上におけるデータ破壊・漏洩等）への対応が必要とされる。一方現状の様な企業と銀行のN対1での接続によるデータ授受は回線効率・一定レベルのセキュリティ機能の確保等の面から問題化してこよう。

これへの対応として，データ交換に関する汎用的なネットワークの構築あるいは業界統一のデータ交換システムの開発が期待される。この様なシステムにおいてはデータ・フォーマットの標準化，変換機能等に加え一定レベルのセキュリティ機能（不正アクセス防止機能・相手先あるいは本人確認機能・データの暗号化等）が必須とされる。

(4) 自動化機器

第二次オンライン・システムにおいて急増したCD（自動支払機）に代表される自動化機器に関しては，従来の端末機が銀行内部に設置され内部者のみが操作していたのに対し，外部の一般顧客が直接操作するということでセキュリティ上画期的な変化をもたらした。即ち，内部者のみが操作するものであればある程度内部手続によりカバーし得るが，外部者では表面的な操作手順の指示のみで対応せざるを得ない。従って，異例操作・オペレーション・ミス等のチェック・対応は従来のシステムに比べ格段に厳密に行なう必要が生じた。更に今後，自動化機器の夜間・休日稼動，代理店・無人化店舗，移動店舗，ポータブル端末等の増加を考えると，防犯対策も含めて総合的なセ

キュリティ機能を強化・徹底していく必要がある。

このためハードウェア上の対応としては頑丈な機器の開発と通信回線上のデータの暗号化装置が考えられる。一方ソフトウェア上の対応としては端末操作時の本人確認が重要なポイントとなる。本人確認のためには現在一般的にパスワード・暗証が用いられているが，覚えやすさと盗難・紛失時の類推のしやすさは相反する面をもっている。又，現状では暗証入力ミスが連続した場合カードそのものを無効にする等の手段が講じられているものの，完璧，なものとはいえず本人確認手段，悪意・故意による不正アクセス防止技術について画期的なものが期待される。

更にこれらの自動化機器は一つの銀行内のみならずTOCS，NCS等のネットワークを通じてほゞ全国どこででも窓口者と相対することなく操作可能となっており，人手による中間段階でのチェック・対応も困難である。このため必然的にセキュリティ上の対応もシステム内部あるいはネットワーク内で処理することが必須とされる。

(5) 開発部門におけるセキュリティ

システムの大規模化・保守負荷の比率増大を踏まえシステム開発の効率化・高信頼化要求が強まっている。これに対応して効率化サポート・ツールの充実とシステム監査の充実が叫ばれ，一部実施に移されその効果も相応に上っているといわれている。

システムの大規模化・統合化によりシステム内での相互チェックが充実し，単純な不正処理は難しくなったものの全体が複雑化しているだけに一旦不正が入り込んだ場合，不正の検出も難しくなっている。これに対して現在実施されているシステム監査は伝統的な人手によるチェックが主体でありシステム的なサポート・ツールの充実が期待されるところである。尚，現在プログラムそのものの信頼性向上・テスト効率向上に重点を置いて利用されているコンペア・プログラム，カバレージ測定プログラム，テスト・データ・ジェネレータ等のツールもセキュリティ機能面から見直すことにより充分利用

可能と考えられるので活用・普及させていくべきであろう。

たゞ，システム開発についてはその性格上プロダクション上のデータ／プログラムのプロテクションと相容れない部分が多く，技術的な対策のみではカバーしきれないと考えられ，開発部門と運用部門の分離あるいは開発部門内における職務分担による相互牽制体制，更にテスト・ジョブとプロダクション・ジョブのライブラリ，処理コンピュータの分離等体制面・管理面の対策と組み合わせ効率・規模とのバランスも配慮しながら充実を図っていくことが必要であろう。

(6) 運用部門におけるセキュリティ

運用部門におけるセキュリティ対策としては，建物及びコンピュータ室への入退室管理システムの導入，ライブラリアン，オペレータ，スケジューラ等の職務分担による相互牽制等がある。

又，オペレーション部門の効率化策として採用されているオペレーションの自動化・省力化システムについても，結果的に処理に携わる要員を減らし，人手の介入を少なくしオペレーション・ミスの減少を図れるという面でセキュリティ充実に効果を上げている。これに加えオペレーション面におけるセキュリティ対策としては重要なオペレーションに対するパスワードの使用，ユーザ・プロファイルあるいはソフトウェア・パッケージ（ RACF等 ）の利用によるオペレーション及びデータ・アクセス制御等が採用されているが必ずしも充分使いこなされているとはいえない。

これらのシステムを有効に活用するためには，これらを適用しやすい運用体制・手順が確立されていることが前提となるので，この面でユーザ側の対応・努力が必須である，と同時にベンダに対してはより使いやすく運用実態にフィットしたツールの提供を要望したい。

1.2.3 今後のシステムにおけるセキュリティ技術

バンキング・システムにおける第三次オンラインを展望すると，次の様な事

項がセキュリティを検討する上でのポイントとなるものと考えられる。

① 1982年10月に施行された第二次回線自由化を契機として，CMS（Cash Management Service）をはじめとした新商品・新サービスの提供，あるいはCAPTAIN(Character And Pattern Telephone Access Information Network system)やCAFIS（Credit And Finance Information Switching system)等現在検討ないし計画されている汎用的・共用的システムの利用が進むものと考えられる。この様なシステムの拡大と多様化に伴ない回線・ネットワークの利用に付随するセキュリティ上の対応が必要とされ，特にこれらが資金決済システムとして利用される場合障害対策，不正・犯罪防止対策につき少なくとも現状の銀行の内部システムと同レベルのセキュリティ機能が要求される。

② システムの拡大・広域化に伴ない不特定多数の人が直接アクセス可能となりかつこれらの人々は従来に比べＯＡ機器・パーソナル・コンピュータ等の普及によりかなり専門的な知識を有しており，システムに対し不当なアクセスを試み，これに成功する可能性が格段に高くなっている。これに対応してデータ保護技術を含めセキュリティ・レベルの一段の高度化が必要とされる。この意味で記憶媒体としてのテープ・ディスク等の不当な読み取りを防止するための技術についても検討することが必要であろう。

③ システムの大規模化・複雑化に対応しての高信頼化要求，ソフトウェア・パッケージの多様化によるブラック・ボックス化の促進等に対応したサポート・ツールの充実，および分散処理，ユーザ部門によるシステム開発等に関連した内部組織・統制上の新たな問題への対応が必要とされる。

④ オフィス・オートメーションの普及，OCR技術・センサ技術の進歩等をふまえたイメージ処理の増加，これは紙幣等の現物を扱う部分も多くセキュリティ面では従来とやゝ異なった観点から検討していく必要があろう。

以上の様なポイントをもとに今後期待されるセキュリティ上の技術としては

次の様なものが考えられる。

(1) 本人確認技術

従来のシステム上の本人確認技術としては，カード上の磁気ストライプ情報と暗証番号の組み合わせが主流となっており，事故・犯罪もこれに関連したものが大半を占めている。

しかしながら，今後のネットワークの拡大，公衆回線の利用，パソコン等インテリジェンシィをもった端末の増加を考えると，本人確認技術については一層のレベル向上が必須となる。このためには暗証番号情報のカード上からの除去，パスワードあるいはハードウェア上の端末ＩＤとの組合せ等によるチェック，更には情報保有量を格段に増加させ得るといわれるＩＣカードの利用等が考えられる。又，声紋・指紋・サイン等本人が属性として保有しているものを利用した本人確認技術が考えられる。この様な技術に関しては，今後イメージ処理技術・音声処理技術等の革新的な進展により利用可能となることが期待されるが，精度の高さ，プライバシーの問題とも絡んで社会的に受け入れられるレベルの見極め，価格の低廉化等がポイントとなろう。

(2) 暗号化

店舗網の拡大，ポータブル端末，対企業間接続等のネットワークの広域化及び回線自由化に伴なう公衆回線の利用拡大に加えパソコン，オフィス・オートメーション機器の爆発的な普及による一般へのコンピュータ知識の普及，安価な機器の普及に対応して従来我国ではやゝもすると軽視されてきた回線上のデータの盗聴・傍受を防止する技術を重視していく必要がある。特にバンキング・システムは資金決済機能を有しており，データの破壊・改ざん・漏洩を防止し機密保持を図ることが必須である。

具体的な盗聴防止技術としては，暗号化とオーセンティケータ（検証子）の利用が考えられる。これらはいづれも技術的には現時点でも可能とされており一部では実用化されているものの本格的な実用化のためにはハードウェア対応・ソフトウェア対応のいづれをとっても問題がある。即ち暗号化にハ

ードウェアで対応する場合，回線あるいは端末毎に装置を設置する必要があり，装置価格の妥当なレベルまでの低下が望まれる。このためにはある程度のまとまった量の装置が利用され普及することが必要であり又暗号化方式につき標準化が前提となろう。現状ではDESをはじめとして数種の方式が普及しているといわれるが，暗号化の機能低下を招かない範囲でどこまで標準化が図れるか，又暗号鍵の管理体制をどうするか等ユーザ側の対応も含めコストと効果を勘案した上で検討すべき点も多い。又ソフトウェアで対応する場合，ハードウェア対応の場合に比べ価格は安くなろうがエンコード／デコードのためのCPU負荷の軽減を含めた一定レベルのパフォーマンス確保がポイントとなる。

(3) 監視機構

現状におけるシステム及びネットワークの監視はオペレーション・ログあるいはシステムへのアクセス・ログ等により事後にチェックすることが主体となっているが，ネットワークの巨大化に伴ないこの監視機能がセキュリティ上重要なポイントとなる。

このため不当なアクセスを事前にチェック・アウトするためのパスワード，プロファイル等の利用に加えオンライン・モニタリングによる即時チェック・アウト機能も要求されてこよう。例えば何回か連続的に誤まったパスワードあるいは暗証でアクセスしているユーザの摘出，ユーザIDによる使用端末の逆探知，受信側における発信番号の検知（現状でもディジタル回線では可能とされている）等がある。但しこれらのチェックはサービス・レベルの低下，プライバシーの侵害につながる可能性もありその判定基準等について慎重な検討を要するものと考えられる。

(4) データ保護

データベースの統合化と，統合化されたデータベースのネットワークを通じてのユーザへの開放が進むに従い，データベース上の情報の窃取・破壊からの保護機能の充実も重要性を増してくる。

このためには本人確認・監視機構を通じてのアクセス制御の他，データベスの内容そのものの暗号化が考えられる。ただデータベースの暗号化に際してはパフォーマンスへの影響が懸念され，当面は簡略化された暗号化方式を用いたり，暗証・パスワード等重要な項目のみに限定して暗号化する等の対応も必要となろう。

又データを保存する磁気媒体については，改ざん防止と不当な読み出し防止のため，更新不可能な媒体の利用，記録後の媒体を更新不可能とする技術，更には一定条件外のアクセスに対しては内容を自動消去する等の技術が要求される可能性もある。但しこれらの技術の利用に際しては運用面での齟齬(そご)が生じない様充分な検討が必要とされよう。

(5) システム監査

システムの大規模化・複雑化に伴ない信頼性の高いソフトウェアを開発しメインテナンスしていくためのサポート・ツール，監査・検証技術のレベル向上は今後更に重要性を増してくる。現在この分野では伝統的に人手によるものが大半を占めておりシステム的対応が遅れている。

これをサポートするため現在でもコンペア，カバレージ測定等のソフトウェアは存在するものの機能的に十分とはいえず，検証・チェック面で活用されているとはいい難く，今後更に使いやすく汎用的なパッケージの開発・普及が望まれる。又，ソフトウェアの正当性検証技術あるいは第三者によるプログラムの正当性チェックが可能なシステムを目指したものとして，システム要求定義言語によるプログラム自動作成・超高級言語があるが，現状ではモデル的・部分的にしか適用できない。これらの技術の改良により一般的なシステムへも適用可能となることが期待される。

更にシステム・ソフトウェアについては，ユーザ側からみた場合，ブラック・ボックス化が進んでおり，今後パッケージの利用拡大等によりこの傾向はますます顕著になってくることが予想される。この意味からもベンダ側におけるシステム・ソフトウェアのバージョン管理・変更管理の充実とその検証

ツール（例えば，システム全体をロード・プログラム・レベルでコンペアすることにより変更部分が明示されるプログラム）の提供が望まれる。

他方ユーザ部門によるシステム開発，オフィス・オートメーションを含めた分散処理の進展に伴ない，初期のEDP部門と同様に一人の人間が何んでも処理する部分が生じ相互牽制機能が弱まる可能性が生じており，これらの管理・統制のための技術と体制についても検討していく必要がある。

(6) OA関連技術

今後のシステムにおいては，オフィス・オートメーションの進展によるイメージ処理の急増が考えられる。このイメージ処理を含んだシステムのセキュリティ対策については従来とはやゝ異った観点から検討してみる必要があると考えられる。

即ちイメージ処理においては，文書そのものが直接コンピュータ・インプットとして使用されるケースが多く，インプット文書そのものの真贋（しんがん）判定，コピーか原本かの判別等の新技術が必要とされよう。この場合インプット時点でのチェック機能の開発と同時にインプット媒体そのもの，あるいにインプット媒体を作成する機器に何らかのセキュリティ・サポート機能をもたせることも含めて検討すべきであろう。

いづれにしろセキュリティの問題は効果について具体的な数値化が難しく，従来から必要性は認識されながらも実際に犯罪が発生ないし表面化しないと対応がなかなか進まない面をもっている。又これらの対応は最終的にはそれに携わる人のスキル・モラルに依存する部分が大きく，技術的な対応のみで全体をカバーすることは困難である。

しかしながら今日の様に大規模化しかつ相互に関連性が強くなったシステム特にバンキング・システムにおいては，その公共性・社会性等を配慮し，体制・管理面も含め可能な限りの対策を講じていくことが要求される。このためのコスト・

ジャスティファイのためには共用化・汎用化・標準化が必須と考えられ，メーカ，ベンダによる効果的な支援システムの開発が期待されるが場合によってはユーザ同士の共同開発を検討するのも有効であろう。

たゞ標準化・画一化は一面からみればセキュリティ機能の弱体化を招くこととともなるので技術開発に当ってはこの面からも検討を加えていく必要があろう。

1.3　情報処理業（その１）

当社は世界35ヶ国，650都市を結ぶネットワークを介してセンタのコンピュータ・パワーを提供する遠隔情報処理サービス（RCS：Remote Computing Service）を主体とする企業である。

利用可能な処理形態には，次のものがある。

① 時分割（TSS）

② 遠隔地ジョブ起動（RJE）

③ 実時間トランザクション処理

④ バッチ処理

アプリケーションの多くは，ネットワークによる多地点制御の利点を活したもので，国際金融オンライン，国際・国内オーダ・サービス，海外店管理システムなど世界的な広がりを持つシステムが特徴である。また近年の回線開放や分散処理の動向に伴って，種々の機能を持ったローカル・プロセサ（オフコン，パソコン，特殊端末etc.）を積極的にネットワークに接続し，情報のトータルな利用を促進している。

このような情況では，セキュリティの保護はネットワーク制御を中心としてシステム運用の最重要問題となっている。

本節では，セキュリティ問題を整理し，現状の問題点，今後の期待される技術を検討する。現状の整理のために，当社の提携先企業が欧米のエンド・ユーザとの間で実施したブレーン・ストーミングの結果を参考にし，一般的にユーザがセキュリティ問題をどう認識しているかを眺めてみた。また特にRCSの立場からの問題点と必要な制御機能を検討する。

1.3.1　セキュリティ問題の現状

(1) 問題の定義と範囲

セキュリティ問題はS（Security），A（Auditability），C（Control）の3つの概念が結合されている。Securityとはアプリケーション・システ

ムが対象としているデータや資源等の利用可能性（availability），整合性（integrity），信頼性（reliability），機密性（confidentiality）を保つための要求であり，Auditability とは Security が要求されたレベルの機能で達成されているか否かを検証するプロセスである。Control とは要求された Security を達成するため，その手段を制御し，効率を測定する行為である。

(2) セキュリティの認識対象

セキュリティの有効的な管理には上の SAC の 3 つの概念がすべて必要である。セキュリティの問題を整理すると，大別して次のような分類になる。

① 物理的セキュリティ

システムの稼動する状況，場所に依存する要素で，要求されるセキュリティのレベルは具体的に種々異なる。

② 操作的セキュリティ

日常のシステム稼動に関する操作や保守に関する操作に依存する要素で，一般に

- 機能の分離
- 事前に定義され，検証されたソフトウェアとプロセスの実行
- 論理的アクセス制御

によって達成される。

③ 人的セキュリティ

システム運用に携わる人的要素に関するセキュリティで，リスク要因として

- ユーザ部門における内部的スタッフ
- システム操作員や管理者
- 内部監査員
- 外部監査員

があり，また問題点として，

・不正アクセス（物理的，論理的）

・データやプログラムの無意識の破壊

・個人的利益のための意識的な破壊

があり，対応策として以下のものがある。

・人事的選択基準の確立

・仕事のローテーション

・高度に組み込まれた制御手順（例外報告，検査）

・機能の分離（相互牽制の原則）

④　データ，プログラムのセキュリティ

データ，プログラムのセキュリティは各々のシステムによりSACのレベルが異なる。制御の実現性はシステムによって提供される技術的能力に依存するが，その手段として，以下のものがある。

・ソフトウェアの検証／確認

・システム・コードもしくはアクセス制限

・自動矯正／誤り修正

・システム・リリース前のソフト／ハードの厳重な検査

⑤　アプリケーション・セキュリティ

前記④の手段に加えて，以下のものがある。

・妥当性検査の規則確立

・保全のための強制的（プロンプト）手続をシステムもしくはアプリケーション用の制御テーブルとして整備

・検証，確認された入力の自動処理

・例外報告機能，ホローアップ機能

⑥　ハードウェア／ネットワーク・セキュリティ

要求として，

・データの整合性確立

・データのプライバシーと機密性確保

・分散されたデータの同期性の確保（ローカル，セントラル・データの論理的一元性）

があり，可能な手段として，

・ネットワーク通信制御

・データの暗号化

・オーセンティケータ／テスター（内部もしくは外部機関による）

がある。一般的にネットワークを通じて入力されるメッセージもしくはトランザクションは次のチェックが完全に実行されるまでは処理されるべきではない。

・端末を含む発信者の確認

・オーセンティケータの承認

・メッセージ入力の完了

・内容の論理的整合性検査

・重複チエック

例外報告が必要な現象として，次のものがある。

・発信／受信不可

・不明確なトランザクション

・不正アクセスの発生

このように整理してみると，コンピュータ・セキュリティの最も中心的な課題は，効果的で使用が容易な論理的アクセス制御システムを構築することであると思える。

(3) 論理的アクセス制御の問題点

現状のシステムで実現されているアクセス制御について次のような問題点が考えられよう。

① パスワードによる保護……機能的には低レベルである。

② セキュリティ担当者はシステム操作とルーチン・ジョブの両方を実行できる。

③ ダンプの多用は危険である。

④ システム操作員用の機能にはすべてのＪＣＬやシステム・ユーティリティの利用ができるような自由度があり過ぎる。

⑤ ドキュメントのない直接的なファイル更新は非常に高いセキュリティ・リスクを伴う。

⑥ パスワードの作成はシステムではなく，セキュリティ担当者によって行なわれる。これは他人のユーザＩＤ／パスワードの無断使用の危険性を常に含んでいる。

⑦ パスワード・ファイルの更新がトレースできない（更新履歴が管理されていない）。

⑧ ユーザＩＤを一時的にブロック（不使用）する機能がない。

⑨ 提供されている資源保護のツールは，多くのシステムであまりに複雑すぎるか，保守のためにあまりに多くの作業を要求するので，有効に用いられていない。

⑩ 現実のシステムでは，アクセス制御を規制するのに「……を含む（include）的な許可の形式が多く，「……を除外して（exclude）他を含める」的な例外的許可の形式がない。

⑪ 通常パスワードはワーク・ステーションのサインオン時に検査されるのみである。

⑫ ジョブ／タスク／メニュー・レベルのパスワード保護は通常システム構築時にオウン・コードで実現しなければならない。

⑬ ワーク・ステーションのアイドル時間が長時間になる場合に自動サインオフもしくは，自動ポーズ・モード切り換えが望ましい。

⑭ 次のような重要でリスク発生の多いジョブには，２ステップ手順もしくは２重パスワード保護が望ましい。

・データベース辞書の更新

・プログラムやシステム・テーブルの更新

・ファイルの削除

・他の重要なシステム操作

1.3.2　遠隔情報処理サービス（ＲＣＳ）における問題点

(1)　RCSの特徴

前項で述べたセキュリティの一般的な問題点は，RCSにおけるシステムについてもすべて適合する。遠隔端末を通じてすべての処理が起動されるRCSの特徴から，セキュリティ保護の完全な達成に対し，次の点が負荷要因として作用する。

①　コスト／効率のトレード・オフ

RCSではシステム運用が，すべて実際に使用した資源による料金で決済される従量制が建前である。従って強力なアクセス制御機能の実現は，常にコストとの比較で検討されなければならない。前提となるマシン系の標準OSが装備するセキュリティ機能に追加して，専用のユティリティやコマンドが開発され，ユーザに提供されているが，その多くはユーザのオプション選択になっている。完全なセキュリティ・システムの運用には，相応するシステム稼動費用が要請される。オプションの範囲は次のものが考えられる。

・アクセス制御の詳細化レベル

・ファイルの暗号化

・障害対策のレベル（バックアップ，トレース，回復機能）

②　アプリケーション空間の拡散

国際間システムのように，ネットワークを通じてオペレーションがグローバルな広がりを持つようになると，アプリケーションの空間が拡散し，これらの統合的な管理機能が要求されるようになる。システム管理機能

（ system administration function ）として次の点が不可欠であろう。

- 資源のアクセス制御
- エンド・ユーザの使用状況把握（費用管理）
- パスワード，ＩＤの管理
- システム整合性の管理
- エンド・ユーザ支援機能
- システム・メッセージの複数言語化

(2) 管理機能の整備（具体例）

当社の提供するRCSの中で具体化されている管理機能（ADM）を紹介する。

① ユーザ番号の構造

個々のユーザはすべて８桁のユーザ番号で識別されるが，これは図１－１のような構造を持っている。

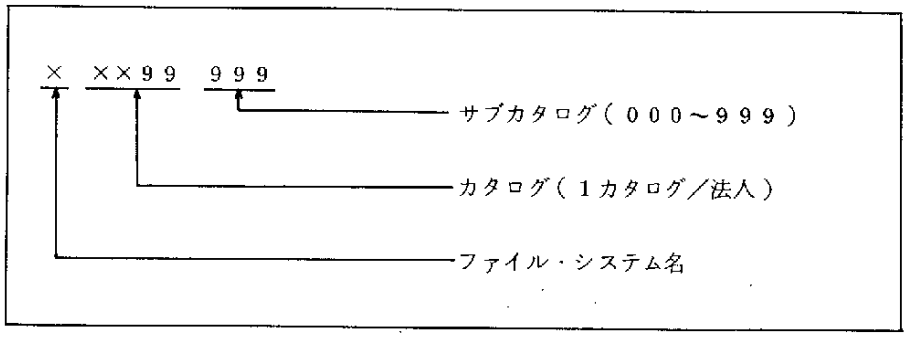


図 １－１ ユーザ番号の形式

カタログとは法人単位に構成できるコミュニティを意味し，その中に最大1000個までのサブカタログ（ユーザ番号）を設けることができる（図１－２参照）。ユーザ番号単位に独自の処理空間を持つことができ，この中の資源（ファイル，プログラム）はカタログ内でアクセス許可を与

えることができる。各サブカタログごとにそれぞれの属性や機能範囲を規定したり制約したりすることができ，これをサブカタログ・プロファイルと呼び，次のようなものがある。

・接続手順の登録

・ＩＲ（接続時即時実行）プログラムの登録

・ブレーク機能停止

・特定コマンド以外のコマンド使用禁止（制限モード）

ADMシステムでは，このカタログ空間を，管理機能に応じて階層化することができる。すなわちサブカタログ（ユーザ番号）間に管理階層を導入することにより，その権限内でのメンバー管理を実現する手段となる。企業組織の階層をADM構造に反映することも可能である。

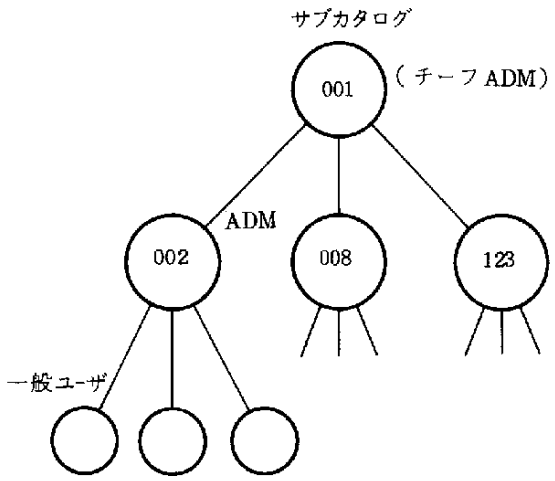


図１－２　カタログの構造

② アクセス権利の管理

サブカタログ内の資源は，そのオーナーの権限で，カタログ全体もしくは特定サブカタログにアクセス権利を与えることができる。アクセス権利には，R(read)，W(write)，E(execute)，A(append)のモードが指定できる。他のサブカタログからはこのアクセス権利が与えられている時にのみ，対象資源をアクセスすることが可能である。また機密保護のために，特定ファイルにパスワードの設定をすることも可能である。

③ アドミニストレータの特権

ADMの階層構造に従って，上位のアドミニストレータは下位のサブカタログのプロファイルを任意に規定したり変更したりすることができる。これらには次のものがある。

- ユーザ番号／パスワードの管理
- メンバーの制限モードの管理
- メンバー管理権の委譲
- 使用料リミットの設定
- 使用状況の情報入手
- メンバー・サブカタログへの移入
- ファイル状況のチエック
- 下位アドミニストレータの任命

④ グループ・カタログの機能

資源の共用は原則として1つのカタログ内に限られている。しかし，業務上緊密な関係を有する法人間や，複数の組織の間では，ファイルやプログラムの共用を実現したいという要求が発生する。特殊のADM機能には，幾つかのカタログをまとめて，仮想的に1つのカタログにする機能があり，これをグループ・カタログと呼ぶ(図1－3参照)。グループ・カタログのメンバー間では，相互の資源へのアクセス権利を与えることが可能であり，データベースの共有，プログラムの共有が実現される。

⑤　まとめ

以上のADM機能は，サブカタログの運用を強力に規制することができるので，地理的に拡散したエンド・ユーザの有効的な管理の手段となり，セキュリティ保護の重要なファクターを実現できる。ただし，チーフ・アドミニストレータやサブ・アドミニストレータはメンバーへの権限が多大となっているので，この運用については，注意深い監視が必要であり，結局，人的セキュリティの問題に帰着することになろう。

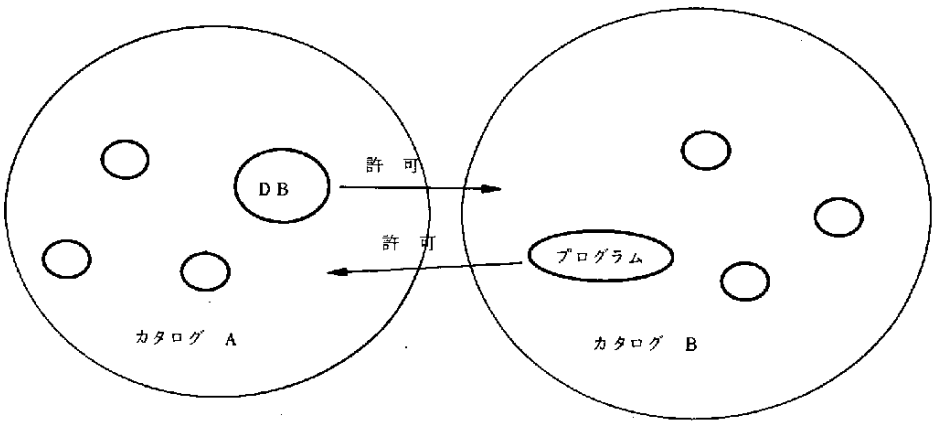


図１－３　グループ・カタログ

1.3.3　技術的展開への期待

今後，実用化が望まれる技術を，ソフトウェアを中心に考えてみよう。

(1)　アクセス制御

アクセス制御には，本人確認技術などの物理的側面での制御と，処理モデル系での資源に対する論理的アクセス制御が考えられる。論理的制御では，現実のアプリケーションを抽象化し資源の形式定義に基づいたアクセス制御の論理モデルを構築する手段が望まれる。これは一部のデータベースの定義言語，要求仕様言語などの方向と一致するが，セキュリティ記述言語の試みである。この言語では，アプリケーション空間（もしくはシステム空間）で

保護対象（sensitive object）を定義し，アクセス権利の構造を明確にする。これらの情報は，データベースやDD／D[*1]と統合され，トータルなセキュリティ・モデルを構築するための手段として用いられよう。

(2) 検証技術

ソフトウェア工学におけるプログラムの検証理論の発展などにより，アプリケーション・プログラムの正当性の検証が実用化されるであろう。プログラムの正当性の他に，トランザクション・データの正当性確認手法の開発も望まれる。データの正当性として①範囲検査，②限界検査，③論理的整合性，④条件充足性，⑤発生時間／発生順序検査などが考えられるが，これも記述言語の発展を期待したい。関係データベースのシステムRでは述語論理を用いたassertionを各事象定義に付加することにより，整合性を定義しているが，今後の方向であると思える。

(3) データベースのセキュリティ

データベースのセキュリティ保護には次のような項目が考えられる。

① アクセスの制御

データベース内の資源アクセス制御には

- パスワード方式
- プロファイル定義
- 述語ロック（predicate lock）
- スキーマ／サブスキーマ

があり，このうち，述語ロックの方式は，保護対象（sensitive object）を条件式（述語）によって記述し，その充足性が動的に評価される。また，サブ・スキーマは，データベースの分割もしくは再構造化により保護領域の定義が可能である。

＊1：DD／D　Data Dictionary & Directory

② 整合性制御

データベースの状態を整合的に保つためには次のような方法が提唱されている。

・主張（assertion）→システムR

・同時アクセス制御→分散データベース

・関数的従属性→関係モデル

・会話理解→推論

これらの手段の実際的な開発は今後の問題であろう。

③ 管理機能（Administration function）

管理機能として次のものが考えられる。

・データ定義言語（ビュー定義）

・データ・アクセス権の制御

・障害回復

・利用状況把握

このような多様なデータベース機能は，アプリケーション・システムに多大な負荷を与えることなく実現して欲しい。最終的には，セキュリティ・データベースの実現はデータベース・マシンの方向であると考えられる。

(3) ネットワーク制御

データ通信の発展によって，今や情報処理は通信機能を切り離して考えることができなくなっている。今後のネットワーク技術の発達に期待したい点は以下のものである。

① 異機種接続の容易性

プロトコルの標準化の進展に従い，近年異機種接続は比較的容易となってきた。今後はより高いレベルでのプロトコル標準化により，アプリケーション・レベルで簡単にネットワークの接続ができることを期待したい（ISOのOpen Systems Interconnection）。

② 回線の効率化

ディジタル・ネットワークにより，回線の有効利用を推進し，回線費用の低減化を期待したい。

1.4　情報処理業（その２）

情報処理業においてセキュリティの現状は，必ずしも十分望ましい状態にあるわけではない。コンピュータ処理におけるミスの発生については多数報告されている。しかしそのことは他のコンピュータ利用業界においても同様のことが言えるようである。一方コンピュータ犯罪の発生件数から比較するならば，情報処理業は，むしろ少ない方であろう。

一方情報処理業は他人のデータの処理を業としてデータの安全に対する社会的責任も重く，将来的に高度なセキュリティの確立が強く望まれる。

本節ではこうした認識に立ち，情報処理業におけるセキュリティの現状と将来必要なセキュリティ技術について述べる。

1.4.1　情報処理業におけるコンピュータ・システムの利用形態

(1)　複数アプリケーションと多様なサービスの共同利用

情報処理業は自社のコンピュータ資源を売ることを業としている。このためコンピュータ資源の極度な効率的利用を指向することとなる。従って複数のアプリケーションと様々なサービス形態が同居した共同利用が行なわれる。

バッチ処理中心だったこれまでのコンピュータ利用においては，スケジューリングによって資源の有効利用を行なっていた。この時代には通常の負荷に合わせて資源を持っておき，最大負荷時には他社システムに外注することでも処理が可能であった。

オンライン処理が普及してきた昨今では，資源は最大負荷に合わせて持つことになる。言うまでもないが，オンライン・システムでは，外注がきかないからである。最大負荷時以外は資源の余剰を有効利用するためにも共同利用が指向されている。

共同利用の実態としては，各種のオンラインあるいは，ＤＢサービス等を同時に提供する。

複数アプリケーション形態（例えばリアルタイム，ＤＢ，ＲＪＥ，ＴＳＳ，

バッチ等のように幾つかのサービスを同時に提供する。)と，複合サービス形態とがある。

特に大型コンピュータを持つ情報処理業においては，様々なアプリケーションが稼動し，複雑な運用が行なわれているのが実態である。

(2) プロダクション・マシンと開発マシンの共用

前記(1)はプロダクション・マシンとしての共同処理形態について述べたものであるが，ここでは，プロダクションと開発でコンピュータを共用することについて述べる。

情報処理業におけるコンピュータ資源の有効利用は，生産用具としてのコンピュータと開発／テスト用としてのコンピュータの共用という実態をも生み出している。近年特にソフトウェア生産の効率化が叫ばれ，従来のように夜間（プロダクション・ラン後）ＳＥのオープン使用による開発では競争力を持たなくなり，日中からプロダクション・ランとの共用でＴＳＳ利用よる開発が主流を占めるに至っている。

(3) メーカ提供のハードウェア，ＯＳの利用

情報処理業は一般にメーカ提供のハードウェア，ＯＳを購入ないし賃借し，アプリケーションを開発し，顧客のデータ処理を行なうため，コンピュータ・パワーを切り売りする形で経営を行なっている。従って一般ユーザと同様にメーカ提供の設計・管理思想の範囲内でしか，資源の有効利用を図れない面がある。

しかし料金計算に付随する独自システム作成のため等に，ＯＳの機能変更等を行なう場合や，異機種結合による複合サービス提供のため，独自のＯＳを持つ場合等，オリジナルなＯＳを持つ情報処理業も出てきている。

またハードウェアでは，特に端末において独自の機能を持った機種の開発例が比較的数多くあり，会計事務所用，漢字入力用等で利用されている。

独自のハード・ソフトを持つのは，まだごく一部であり多くの情報処理業は，押し着せのソフト・ハードを利用している。

1.4.2　情報処理業におけるセキュリティの現状と問題点

前述したとおり情報処理業のコンピュータ利用の特徴は，極端な共同利用にあるといえる。このことからセキュリティにおいては，幾つかの問題点と必要な対策とが浮彫りにされるのである。

情報処理業を対象とした，通産省の「情報処理サービス業電子計算機システム安全対策事業所認定制度」は，スタートして1年余であり，ようやく業界に浸透してきて，前向きに取り組む企業が増えてきた所である。このような実状を踏まえ，ここでは以下の点について，情報処理業におけるセキュリティの現状と必要な対策方法について述べることとする。

① データ処理

② アプリケーション開発

③ 本人確認とアクセス・コントロール

④ 人事組織管理

⑤ 物理的対策

(1) データ処理

情報処理業は顧客のデータを処理することを業とするところから，データ処理における安全については，以前より特別に対応しているところである。次に示す各過程をチェック・ポイントにしている。

- データの受取
- 媒体変換（データ・エントリ）
- データの入力（コンピュータへの入力）
- データ処理と出力
- 製品検査
- 製品納入，データ返却

これら各過程において必要に応じて以下のように何段階ものチェックを行なっている。

- データの受取数量記帳

- レコード件数記録
- コンピュータ入力レコード件数照合
- ジョブステップ毎のレコード件数照合
- 出力レコード件数確認
- 出力帳票における製品検査としてのリミット・チェック，トータル・チェック等
- 納入件数の記帳

これら何段階ものチェックは同一組織，同一人により行なわれるのではなく，複数の組織および人によって行なわれている。

しかし，それでもこのデータ処理に関するトラブルは根絶出来ていない現状にある。情報処理業を利用する顧客の不満も，この辺に集中するのではなかろうか。こうしたトラブルの主要原因は以下のところに求められると考えられる。

① 多くの顧客の非定型的データを取扱う。

情報処理業では，顧客の要望に合わせ様々な種類のかつ非定型フォーマットのデータが処理される。このためどうしても人手に頼る機会の多いコンピュータ入力段階までの間でのトラブルが多発することとなる。このことは，故意に異なるデータを入力させることによる，混乱，資源の無駄使い等の発生を予測させる。

② 人の善意の過信

組織や人による牽制および何段階ものチェックも，他人の善意を過信するとチェックは甘いものとなり，有効性が薄れてしまう。この意味でセキュリティには性悪説で臨むのが妥当のようである。

③ コンピュータに対する過信

コンピュータの処理は完全ではないのであり，最後にはやはり人間に依存したチェックなり確認が必要である。しかしその過程での処理を過信すると，人間同志の牽制が効かなくなるのと同様，コンピュータに対するチェ

ックが極めて甘くなってしまう。

このような人及びコンピュータへの過信はコンピュータ犯罪の温床になりかねないので，十分な対策が望まれるわけである。対策として前述した相互牽制的チェックの他に，次のような方法がある。

ⓐ ジョブ走行ルーチンを通常走行ルーチンと間違いないかコンピュータ監視する。

ⓑ 入力レコード件数が各ジョブステップ順に正しく流れているかコンピュータ監視を行なう。

ⓒ データの受取，製品の納入等のデリバリについては，搬送用具とその鍵について厳重な管理を行なう。

(2) アプリケーション開発

情報処理業におけるアプリケーション開発には二つの目的がある。

一つはアプリケーションの開発そのものが目的の場合であって，開発後そのシステムを顧客に納入することとなる。

もう一つは顧客のデータ処理を請負うためにアプリケーション開発を行なう場合であって，この場合システムは顧客に納入されることなく情報処理業内部で保管運用される。

いずれの場合も開発段階における顧客の要求仕様実現のための技術が問われるところである。特に後者にあっては情報処理業内部でアプリケーションの維持・管理を行なうわけであり，ソース・プログラムの更新記録管理は重要なセキュリティ上の関心事である。

① アプリケーション開発

近年プログラム作成にはＴＳＳ手法が導入され開発コスト削減に大いに効果があった。同時に開発工程管理，開発ライブラリの更新管理にも新手法が導入され，ソフトウェアの品質向上，セキュリティ向上に大いに貢献している。

一方こうした新技術の導入はシステム開発をブラック・ボックス化して

しまうことになる。従って十分なシステム・テストと厳重なライブラリ管理が必要となる。

② ソース・プログラム管理

これには二つの意味がある。一つはソース・プログラムの中身の更新記録管理である。特にプロダクション・ランに入ったプログラムの内容更新は容易に単独の人間の判断で行なってはならない。管理者による事前承認と事後承認（場合によってテスト立合いもある）が是非必要である。

もう一つはプログラムの保管媒体管理である。これは電子計算機システム安全対策基準等で望ましいガイドラインが示されているので大いに採用されるべきであろう。

(3) 本人確認とアクセス・コントロール

情報処理業においてはこれまでのバッチ中心の処理形態から，今やオンライン全盛の時代へと移行しつつある。

バッチ処理においてはデータの投入・処理・出力等が各段階で人の目に入るため管理もしやすかった。またデータ・コントローラ，スケジューラ，オペレータと何人もの手を経由してジョブが処理されるので，チェックも効いていたのである。ところがオンラインになると入力・処理・出力の流れが，大部分ブラック・ボックスとなったコンピュータ・システムの中で行なわれてしまう。従ってこれまでとは大いに異なるセキュリティ技術が求められるわけである。

このような背景から本人確認とアクセス・コントロール技術が生まれてきたのである。

① 本人確認

この場合の本人確認とはそのオンライン・システムに登録した正しい顧客かどうかを判断する手段である。これには最も一般的な手法としてパスワードによるものである。

パスワードはシステムに設定した固有の本人確認記号であり，英数字等

で一定の桁数に決められている。管理方法としては二通りある。一つは特定のコードをシステムに登録しておいて，コンピュータを利用するときは常にそのコードで使用する方法である。もう一つは一定の手法でもって顧客が自由にコードを変更できるものである。後者であれば，もしパスワードを盗用されてもすぐ変更がきくので，比較的手軽に自分の管理下で安全を保てる利便さがある。

またパスワードと同様の機能であるが，二重三重のガードをかける意味で他にユーザ・コード，オーダ・ナンバー等を用いる場合がある。

こうしたパスワードは端末管理が甘い場合や出力リストの管理が正しく行なわれない場合には，極めて弱い保護にしかならない。つまり端末やリストからパスワードを盗まれてしまうことが多くあるからである。このためパスワードの入／出力には印字しないとかダブル印字（異なる記号等による）等によって判読不可能な措置がとられるのが普通である。

② アクセス・コントロール

システムの利用者は，通常は制限された資源や使用範囲でのみ利用できる。この範囲を逸脱していないかどうかを制御する技術をアクセス・コントロールという。

通常は，システム利用権，使用可能ファイル，利用プロシジャー等があらかじめシステム内に登録された管理簿と照合されて，アクセスの可否を判定するのである。

前述したように情報処理業にあっては，極度にシステムの有効利用を追求するために，様々なアプリケーションの複合利用が指向される。従って本人確認とアクセス・コントロールは情報処理業にあっては必須の機能であるといえよう。

(4) 人事組織管理

安全を維持するために組織に必要な要件は，相互牽制が効くことである。一部門の独走を制限できる組織機構になっていることが必要である。バッチ

処理中心の時代には，情報処理業の組織は，相互牽制を効かすため，縦割り組織から横割りの組織へ大きく脱皮した。すなわち縦割りの時代には，業務毎に一人の担当者がデータの受取，処理，出力，納入を全部行なっていた。これではコンピュータ犯罪もさることながら担当者が休んだときのバックアップが効かず，またドキュメントの不備等運用上も様々な問題が発生した。これを解消するため処理の各段階毎に担当をもうけ，担当は，自分の守備範囲の中で複数の業務を受け持つこととしたわけである。これにより前処理段階でのミス等を後の段階で発見でき，相互チェックが有効に働くようになったわけである。

しかし現在のオンライン時代になって，かならずしもこの横割り組織が最適ではなくなってきたのである。すなわちオンライン処理の固有の特徴（顧客が入力・出力を行ない，処理がブラック・ボックスになった）が横割り組織の本来の目的である相互牽制を意味の無いものとしてしまっている。つまり組織形態そのものではブラック・ボックス化したコンピュータ処理のセキュリティを維持できなくなったのである。もう一つは少なくとも内部からコンピュータ犯罪者を出さないための人事管理である。

① システム監査

システム監査は最近各分野で研究されつつあるテーマであるが，まだ定まった概念規定はないようである。このため本格的にシステム監査を導入した情報処理業の例はまだ聞かない。しかし内部監査によるデータを蓄積し，今からシステム監査の本格的導入の準備を進めるべきであろう。

② 人事管理

顧客の多くのデータを扱っている情報処理業にとっては，内部者によるデータの紛失・機密漏洩等を起さないことはまず第一に処置すべき最重要テーマである。コンピュータ犯罪者の動機調査によると，上司や会社への不満や知的挑戦意識が大きな比率を占めている。このことは逆に人事管理の指向すべき方向を暗示しているわけで，内部に不満を蓄積しないような

各職場での人間関係維持及び曲った知的挑戦を起さない内部統制・指導等が大いに望まれるところである。

(5) 物理的対策

物理的対策としては建物，コンピュータ室の位置，入室管理，防火防水耐震設備等での安全対策である。これらは電子計算機システム安全対策基準でも明らかなのでここでは詳述をさける。

昭和５６年よりこの基準をもとに安全対策認定制度が発足した。情報処理業各社はこの制度に合格することで安全維持の責任を果すべく努力しており，５７年度中に２８事業所が合格の予定である。この認定制度の業界への定着は喜ばしいことである。

1.4.3 将来求められるセキュリティ技術

情報処理業におけるセキュリティの現状は前項で述べたとおりである。本項では情報処理業が将来的に提供するサービス形態の中で，それぞれどのようなセキュリティ技術を必要とするかを述べ，開発への期待を明確にする。

(1) 情報処理業が将来的に提供するサービス形態

海外での情報処理業の事業展開分野及び各種統計等を参考にすると，我国の情報処理業が将来進出しようとするか重点を置こうとする事業ないし，サービス形態は次の分野と考えられる。

① ＶＡＮサービス

② ソフトウェア・サービス

③ データベース・サービス

④ リアルタイム・サービス等

以下にこれら各サービス形態の中でとられるべき主要なセキュリティ技術について述べる。

(2) ＶＡＮサービス

ＶＡＮのイメージはまだ社会的に定着したものになっていないが，典型的

な例としては以下のものがある。

- 製造・販売業等における集配信システム
- 信販システムにおける情報交換ネットワーク
- 製造・販売業と小売店の受発注ネットワーク
- 流通業における受発注ネットワーク

これら各システムはいずれも広域ネットワーク網の有効利用を目的とするわけであるが，この特徴により必要となる主要なセキュリティ上の問題は以下のことが考えられる。

① 通信方式の公開・標準化

ネットワーク利用者が多くなれば，様々なメーカのコンピュータあるいは端末とネットワークとの接続の問題が生じる。通信方式を標準化し公開すれば，そのネットワークのセキュリティはどうしても弱くなる。このためネットワーク上のデータの暗号化が必要となる。

ネットワークに接続する機器にはホスト・コンピュータからインテリジェンスのないターミナルまであるので，暗号化機器はそう高価なものでは普及しないであろう。

また多くの機種とのインタフェースを持つことが望まれる。更にターミナルへは，センタ起動でアクセスすることが多いのでセンタからターミナルの暗号器のキー操作ができると，運用上も便利で安全性も増大すると考えられる。

② 高度なアクセス・コントロール

多くの顧客がネットワークに接続してくるとアクセス権の制御も高度で複雑な機能が要求されよう。

アクセス・コントロールそのものは本人確認をも包含する機能であろうが，現状ではアクセス・コントロールの決定打が出ておらず，今後の研究に待つ必要がある。システムないしネットワークでの過大な負荷にならない範囲での有効なコントロールを期待したい。

大規模なネットワークではアクセス・コントロール専用のＦＥＰ（Front End Processor）を設置し処理マシンとの機能分離も一策である。

(3) ソフトウェア・サービス

これは，高級言語等によるシステム開発環境の提供サービスのことで，ＴＳＳと同類であるが，専用化し機能強化したものである。

端末との直接接続の他にネットワークとの接続による利用も当然考えられるので，ＶＡＮと同様のアクセス・コントロールが望まれる。またこのサービス固有の問題としてはオンライン環境が単一サブシステムの下に定義されるため，別々のシステムにもかかわらず影響し合う点がある。これは共同利用が通常の情報処理業にあってはセキュリティ上極めて弱い部分になりかねない。すなわちあるオンライン・プロシジャーのハングアップ等が他に悪影響するとか，他のプロシジャーのファイルをのぞける等の弱さを持つのである。このためオンライン・サブシステムの改造が待たれるところであり，それまではアプリケーション・サイドで配慮しておく必要がある。

(4) データベース・サービス

データベース・サービスにおいては，各ＤＢの保護とアクセス権の制御が問題である。

アクセス制御は別に述べているので，ここではＤＢの保護について述べる。ＤＢの保護については現在までに採用された技術としては，①二重化，②更新処理の同期（二重化ＤＢに対して），③トランザクション用ジャーナルの設置等がある。これらは二重化して，一方のＤＢの破壊に瞬時に対応しようとする配慮と復元の容易さ，短時間の復元を目的とした対策である。

二重化対策には２つの問題がある。一つはＤＡＳＤで二重化すると高価でかつスペースの経費が発生する。しかしこの場合には同時更新が可能となる。もう一つは，ＤＡＳＤは一元化しておき内容をＭＴに退避しておく方法である。この場合には同時更新ではなく，一定の時間差が発生することはいうまでもない。

ＭＴ退避は安価な対策であるが，大規模なＤＢにあっては，退避に要するコンピュータ処理コストがばかにならない。そこでより高記録密度の磁気テープ装置なり記録方式の開発が望まれるところである。

(5) リアルタイム・サービス

これは現在すでに普及期に入ったオンライン処理の更に発展したイメージで述べている。従って必要なセキュリティ技術も，現状解説の中で多くは言及しているところである。

情報処理業ではまだ採用の例を多くは聞かないが，ジョブの実行のダイナミックな記録と監視は，今後必要な機能であろう。これは各ジョブが正しいステップの順に実行されているか，更に正しいモジュール，ファイルを使用しているか等を動的に記録し，管理簿と照合監視しようとするものである。

これはシステム監査に対しても有効な資料を提供することになる。しかしこのようなデータの収集は通常システムの負荷を倍増させることになるため，採用に二の足を踏む企業が多いと思われる。従って余程安価で高性能のツール（ハード・ソフト両面で）が開発されない限り多くの企業に採用されることはないであろう。

以上いくつかの期待される将来技術について述べたが，最後に忘れてはならないのは，システムの開発・運用に携わる人間の管理の問題である。内部者がコンピュータ犯罪を犯す限りにおいてはどんなセキュリティ対策も無力である。従って人間にその気にさせない倫理の確立，環境の維持等の管理面の対策が今後多いに研究されるべきだと考える。

1.5　情報処理業（その３）

本節では，情報処理業における一般的なセキュリティ対策の現状について，標準的な情報処理業者（本文中で当社と記述）をモデルにして記述した。本文中の「当社」が特定の企業を意味するものではないことを，あらかじめお断りしておく。

1.5.1　業務の概況

当社は委託業務を主体とする情報処理サービス会社である。現在は東京と大阪を拠点とする９つのネットワーク網により全国的な情報処理および情報提供サービスを行っている。

また，１９８３年４月，コンピュータ専用ビルを開設し，コンピュータ集中管理による効率化とセキュリティの向上を図る計画である。

(1)　サービスの形態

現在当社の主なサービス形態としてつぎのものがある。

ⓐ　受託計算（バッチ処理）サービス

ⓑ　オンライン・ネットワーク・サービス

- ＴＳＳ
- ＲＪＥ
- リアルタイム

ⓒ　データベース（情報提供）サービス

ⓓ　ＬＡＳＳ（大型科学技術計算）サービス

ⓔ　ソフトウェア開発

ⓕ　オープン・サービス

(2)　ネットワークの形態

当社ネットは，東京・大阪地区に並列設置された大型コンピュータと全国主要都市を高速通信回線で結んだネットワーク・インフォメーション・サービス（ＮＩＳ）である。ユーザは公衆回線または特定回線を介して東京・大

阪の任意のコンピュータを利用できる（図１－４参照）。

またコンピュータ専用ビル開設により，I－TDM（Intelligent Time Division Multiplexer）またはノード・コンピュータにより，回線の有効活用や伝送データのパケット化，伝送上のエラーの自動修正機能によりセキュリティの向上を図る予定である。

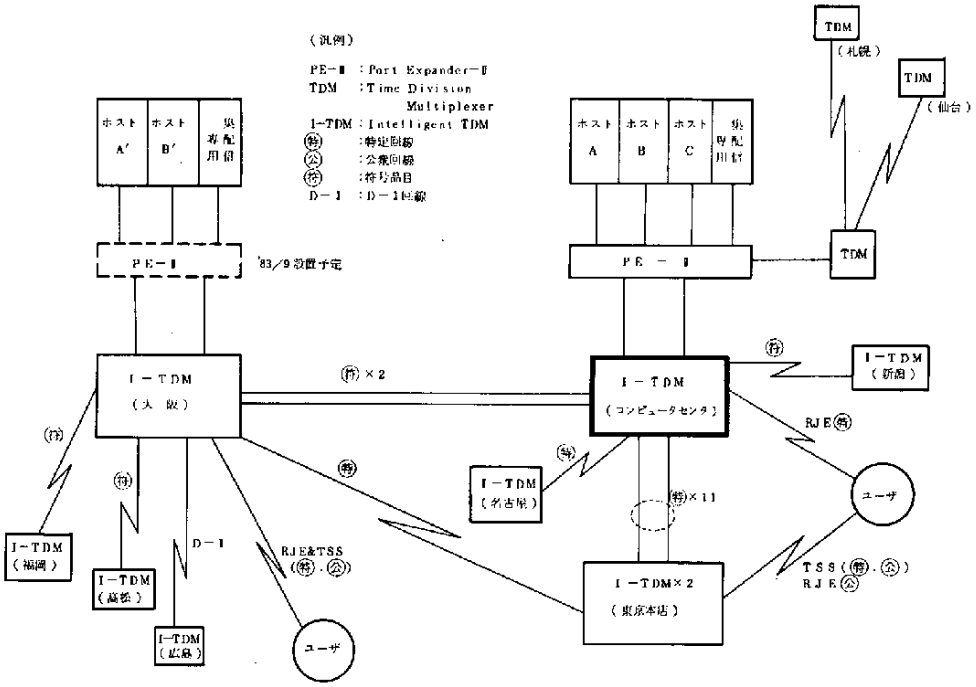


図１－４　ネットワーク構成図

(3)　運用面での安全対策

コンピュータ・セキュリティ対策のうち，主に物理的対策や運用管理面については，１９７６年当社独自の

・電子計算機運用管理規程

・データ保護管理規程

を制定し，全国統一基準として施行，１９７７年通産省の「電子計算機システム安全対策基準」を受け上記規程の一部改定と新たに

・災害対策規程

・入退室管理規程

を制定し，１９７９年より実施，１９８１年通産省による「情報処理サービス業安全対策実施事業所認定制度」の発足に伴い，これ迄の安全対策実施状況の再確認と改善が図られ，一部認定基準に合格した。

これらの安全対策の運用は，主管部署により「安全対策マニュアル」として全部門に配布され，社員に対する教育・訓練のツールとして，また内部監査のガイドラインとして活用している。

(4) 組織面での安全対策

組織面での対策として責任，権限，職務を分割し，組織による内部牽制を指向している。組織は，

・管理部門

・営業部門

・システム開発部門

・研究開発部門

・ＤＰ（データ・プロセシング）部門

に，横割されている。

システム開発部門においては，システム設計とプログラム作成は分離され，業務処理については「業務移管規準」の審査に合格したシステムについてDP部門へ移管され業務運営が行われる。オペレーション，穿孔作業および特殊入出力作業については，それぞれ専門の関連会社へ全面委託している。

(5) オペレーション部門の分離

オペレーションは関連会社に全面委託しており，作業依頼者がホスト・コンピュータ室に入ることはない。専任のオペレータがスケジューラの指示に従いオペレーション指示書にそって，入出力媒体（MT，Removable Disk Pack, etc.）の管理からオペレーションまで一括して処理する。この関連会社に対しても当社と同等のセキュリティ諸規則が適用されている。特にＭＴ

は，テープの絶対番号，記号化されたファイル名で専任のライブラリアンにより厳格に管理されており，部外者が実体に触れることはできない。

また，マシン室への入室も，事前に申請され，管理責任者に許可された者のみ，入室バッヂを付け，番号を登録した磁気ストライプ・カード（ＩＤカード）により入退室を行なうが，すべて記録として保存される。計算結果等成果物は，ユーザ・コード毎にオペレータにより分類され，検品後製品箱に格納される。

(6) オペレーティング・システム（ＯＳでのセキュリティ）

当社は現在設計思想の異なる外国機と国産機の２種類のコンピュータを利用している。この２社に限らず，ＯＳの考え方については，メーカ側にかなり異ったものがあるように感じる。

一つは，一切をＯＳにまかせ，ユーザのＳＥやプログラマの手数を省く，つまりＯＳ設計にあたり，セキュリティ上必要な機能はできるだけ包含していこうという考え方である。他は，ＯＳは身軽であるべきで，オーバヘッドの少ない（効率の良い）ＯＳを提供し，セキュリティ等の問題はユーザ自身のコーディング（Own Coding）で処理すれば良いとの考え方である。

いずれも長短があるが，特に前者では処理スピードの問題があり，後者はユーザＳＥがＯＳに熟知していないと部分的に欠陥が生じる恐れがある。

しかし，オンライン化の増大や企業間ネットワークの普及によりますます高度化・複雑化していく情報化時代において，セキュリティ上の問題の解決策の１つとして，ＯＳに頼らざるをえない部分は大きなものがある。

当社は，これ等２つのＯＳの特徴をうまく結合して，セキュリティ・レベルの向上に努力している。

1.5.2 セキュリティの現状と問題点

現在当社で使用中のコンピュータ・システムには基本的に異った開発思想があり，セキュリティ・レベルも同等ではないが，ここでは両方で使用可能な技

術は統括して述べる。一方のみ使用可能な技術は他方を同等レベルにまで近づけていかなければならない。

(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自身で検証させる機能である。現状ではつぎのことを行っている。

- 本人確認
- ユーザ・プロファイル管理
- アクセス・モニタリング

① 本人確認方法

サービスを提供しているすべての形態について，ユーザ・コード（ユーザＩＤ），パスワード，チャージ・コードにより，システムへのアクセス・コントロールを実施している。システム・アクセスは，ジョブ・タスク・コントロール・モジュールにより，コンピュータ・ユーザ情報ファイル（ユーザ・データ・ファイル）を使って行われる。ユーザ・データ・ファイルには，本人を確認できる個有の情報が入っている。

ⓐ ユーザＩＤ入力方法

イ．カードによる入力

バッチ・プログラムでは，ジョブ・コントロール・カードと呼ばれる実行コントロール用カードの中の１つのパラメータとして，ユーザＩＤを入力する。問題点として，オペレータは簡単にこれらのコードを解読することができるため，運用面での管理が重要である。

ロ．キーボードによる入力

トランザクション処理やＴＳＳのようなオンライン形態では，ＣＲＴキーボードや，キーボード・プリンタ等の端末からユーザＩＤを入力する。この方法では，他人の目に触れることは少ないが，オペレータ・コンソールからアクセスする場合，このアクセス・コントロールの範

囲外となるため，やはりオペレータの管理が重要である。対策としては，オペレータ・コンソールに個有のＩＤカードを渡し，オペレータの識別を可能にする必要がある。

ハ．オンライン起動方式

上記ロ．の方法によりイ．のバッチ・ジョブをスタートさせる方式で，ジョブ投入時にコードが漏れる機会は少なくなる。遠隔地のホスト・コンピュータの利用等に適用される。

ⓑ パスワード方式

パスワードあるいは銀行における暗証番号は，本人のみが記憶している何らかの情報（論理的）をコンピュータに入力することにより本人の確認を行う方法で，パスワードの決定はユーザが行う。パスワードは機種により異なるが，１桁から８桁（外国機は１～１７桁）までの英数字を用い，通常ユーザ・コードと組み合せて使用される。ユーザ・コードは，センタ管理者（特権ユーザ）により指定されたものをユーザは使う必要があるが，パスワードはユーザ本人が管理する。

現状では，ユーザ・コードはユーザ・グループへ与えられているため（複数人が同一コードを使用），社内的にはかなりオープンな状態になっている。そのため，システムへのアクセス・コントロールはパスワードにのみ依存している状態である。外部ユーザに対しては，センタ管理者により厳重に管理されており特に問題はない。パスワードの管理はユーザが個別に行うためセンタ管理者でもユーザのパスワードを知ることはできない。

問題は社内で使用しているグループのパスワードはそのグループのメンバー全員が知っているため漏洩する可能性があることである。特にグループのメンバーの退職等の場合は，すぐに変更する必要が生じる。この変更はかなり大きな作業量であり負担となっている。

いずれにしても，パスワードを使用している場合は，パスワードの保

護が最も重要であり，管理面の強化が当面の課題である。

期待される対策として，特にパスワードをグループで使用している場合，グループに関連するプログラムやデータ・ファイルのパスワードを一斉に変更できる方法の開発が望まれる。

② ユーザ・プロファイル管理

本人確認が行なわれたユーザに対して，コンピュータ・システムは，そのユーザが許された正しい利用の仕方をしているか，また許されたリソースの範囲でコンピュータを利用しているか，これらの検証を行なう必要がある。

ユーザ・プロファイル管理の機能にはユーザ管理の機能 ― ユーザ名と属性およびシステム使用権の管理 ― とリソース管理の機能 ― ユーザ毎の利用可能なファイルの管理 ― が含まれるが，リソース管理については，(2)のリソース保護の項で説明するためここではユーザ管理の機能について述べる。

ⓐ ユーザ登録管理

システムの個々のユーザ（使用者）は，独自のユーザ・コードによって識別されるが，これは通常，センタ管理者によって割当てられる。各ユーザ・コードには，一つまたはそれ以上のパスワードが組になっており，ユーザ・コードが不正に使用されることを防いでいる。

ユーザ・コードは，ある特定のファイルの中で定義され，システムの使用者に関する情報を保持するためにセンタ管理者の手で管理されている。これらの情報をディレクトリと呼び，ディレクトリへのユーザ登録／削除はセンタ管理者によりシステム・ユティリティ，あるいはマスタ端末から行われる。なお前述したユーザ別のパスワードもこのディレクトリ内で管理されている。

ⓑ ユーザ属性とシステム使用権の管理ディレクトリには，ユーザ名の他に各ユーザごとの属性システム使用権が管理されている。

イ．ユーザ属性

使用者は，センタ管理者（システム管理者），一般利用者（グループ管理も可）に分けられる。センタ管理者はディレクトリ管理が行え，一般利用者はディレクトリに登録された後，システムへのアクセス権が得られる。

ロ．システム使用権

コンピュータの利用方法についてはバッチ，オンライン・リアルタイム，TSS等があるが，ディレクトリには各利用者毎に利用方法が登録でき，システム・アクセス（ログオン）時にアクセスの可否がチェックされる（図1－5参照）。

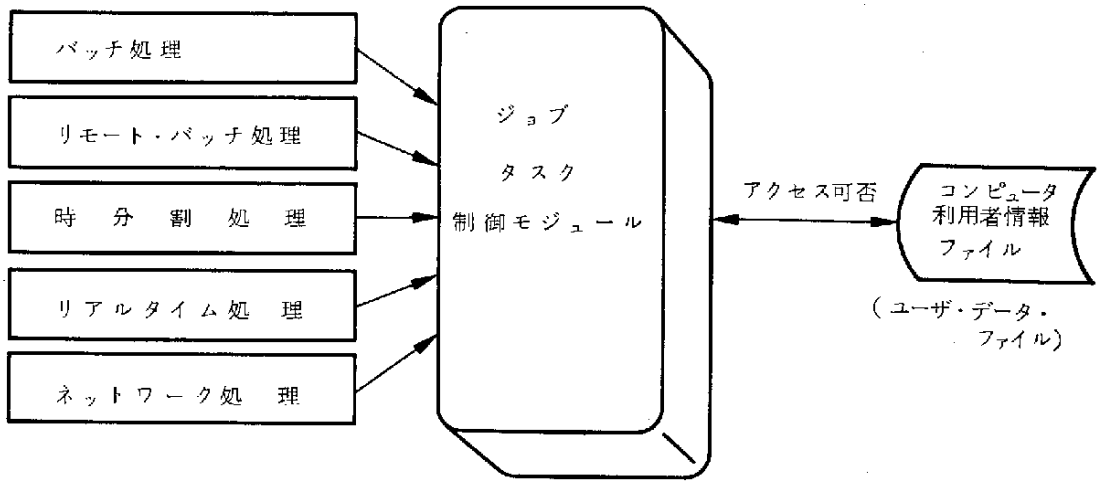


図1－5　システム・アクセス

③　アクセス・モニタリング

アクセス・モニタリングの方法には，つぎのものがある。

- 不正アクセスに対するモニタリング
- 正しいアクセスに対するシステム・モニタリング
- オペレータ・コンソールからのアクセスに対するコンソール・ログ

ⓐ　不正アクセス・モニタリング

ユーザ・コードまたはパスワードが登録されていない利用者によるアクセスや，あるいは誤ったシステム使用権の行使があった場合，システ

ムは利用者の要求を拒否すると共に，そのアクセスの履歴を記録する。この記録はログ・ファイルにとられ，システム管理者が出力してチェックすることができる。

ⓑ システム・モニタリング

各ユーザ毎の利用状況（開始時間から終了時間までのリソース使用状況等課金情報も含む）を記録する。通常は各タスク毎に編集され，別表またはファイル上に出力されているため，特にシステム・モニタリング・ファイルのみ保存することは行っていない。（当社はデータ量が膨大のため，現在は日単位で消去している。）

ⓒ コンソール・ログ

オペレータのコンソールからはユーザ・コードおよびパスワードなしでアクセスできる場合があるが，このアクセスの状況が記録される。コンソール・キーによりアクセスを禁止することは可能であるが，数名のオペレータが操作している場合，オペレータの識別ができない。この問題を解決するために，コンソール自身に，このキーの他に，オペレータ識別のためのＩＤカード読取装置による本人確認機能の付加が必要である。

(2) リソース保護

リソース保護の対策としては，システムを運用するためのソフトウェアやデータの他にディスク，磁気テープ等の記録媒体，データを入出力するための端末機やデータ通信回線等，数多くのものが保護の対象となる。ここでは主に，内部記憶上のデータ保護機能について述べる。

① 資源アクセス管理機能

ファイル・アクセスの態様を表示すると図１－６となる。任意のディスク・ファイルへのアクセスは，そのファイルの３つの属性によって制御される。すなわちSECURITY TYPE，SECURITY USE，SECURITY GUARDである。

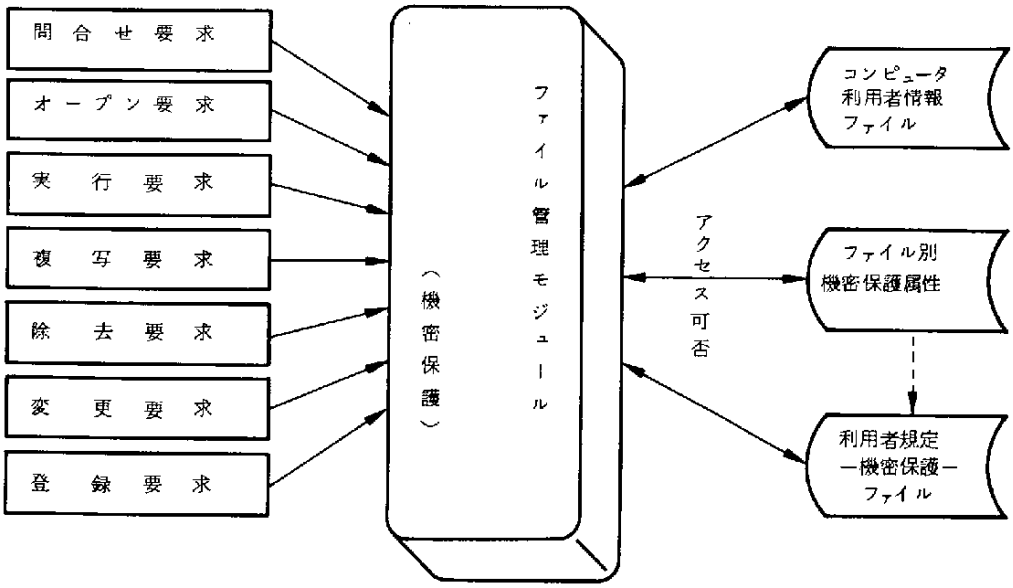


図1－6　ファイル・アクセス

ⓐ　SECURITY TYPEの属性

この属性は，ファイルの所有者は別として誰がそのファイルを使用してよいかを指定する。属性の値はPRIVATE，PUBLIC，GUARDED，CONTROLLEDである。

- PRIVATEは所有者しかアクセスできないことを意味する。
- PUBLICはユーザ・コードとタイトル（FILE-ID）を知っていれば誰でもアクセス可能である。
- GUARDEDはガード・ファイル上で保護されたファイルであることを示す。
- CONTROLLEDはガード・ファイル上で同一ユーザ・コード内の機密をも保護されたファイルであることを示す。このファイルはUSERCODE／PASSWORDとACCESSCODE／PASSWORDの2つのパスワードによりアクセスが制御される。

ⓑ　SECURITY USE属性

ファイルへのアクセスは，さらにその使用法がこの属性によつて制御

される。SECURITY USEはSECURED，IN，OUT，IOの値をとる。

- SECUREDは読み取りも書き込みもできない実行専用ファイル
- INは読み取り専用ファイル
- OUTは書き込み専用ファイル
- IOは読み書き両用ファイル

なおDEFAULT（省略時）はIOである。

ⓒ SECURITY GUARD属性

SECURITY TYPEがGUARDEDあるいはCONTROLLED な

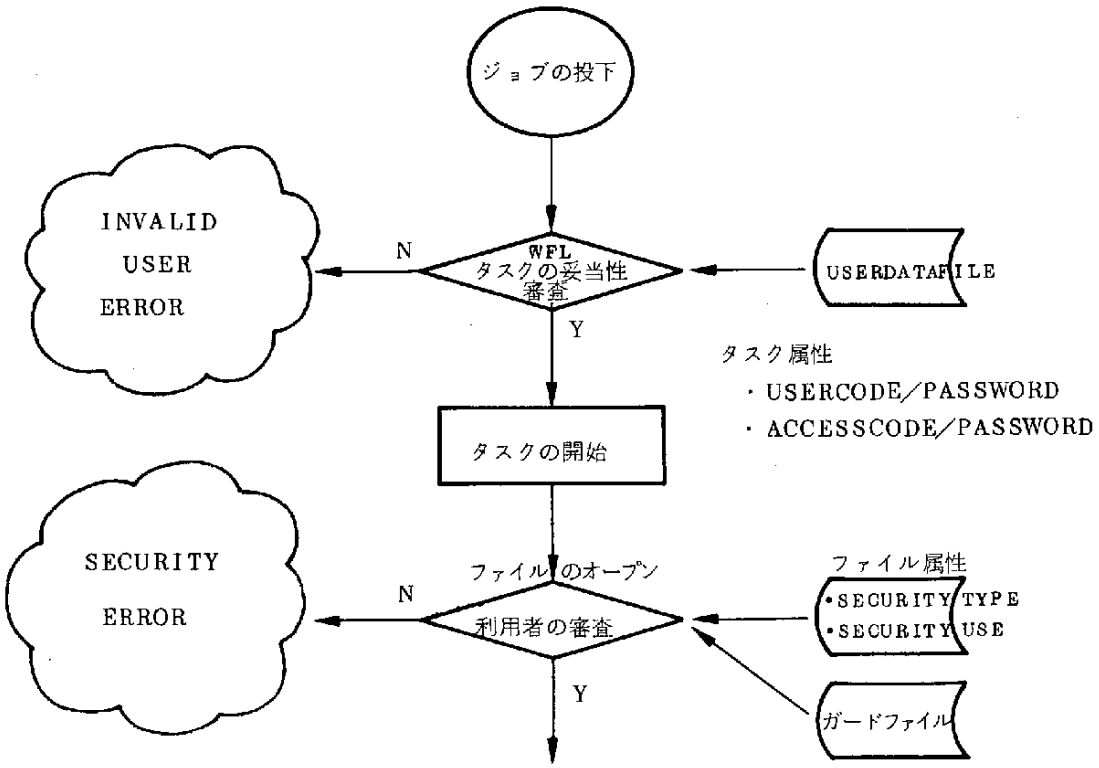


図1－7　機密保護の流れ

らば機密保護タイトルは，属性SECURITY−GUARDによって指定される。指定されていない場合や指定ファイルが存在しない場合は，そのファイルはPRIVATEとして扱われる。ガード・ファイルはSYSTEM/GUARDFILEプログラムを使って構築する。

以上の機密保護の流れを図1−7に示す。

ⓓ 属性の相互作用と属性の指定

利用者コードの下で実行されているプログラムが，その利用者コード・ライブラリのファイルでSECURITY TYPEがCONTROLLEDでないファイルをアクセスしようとすればSECURITY TYPEが無視され，使用の可否はSECURITY USEによって決定される。他の利用者コード・ライブラリのファイルがアクセスされる場合3つのケースが発生する。

- SECURITY TYPEがPRIVATEならばそのプログラムはSECUREDとされる。
- SECURITY TYPEがPUBLICならば使用の可否はSECURITY USEによって決まる。
- SECURITY TYPEがGUARDEDあるいはCONTROLLEDならば使用の可否はSECURITY GUARDによって指定されたガード・ファイルの中の値によって決定され，SECURITY USEは無視される。

ファイルの機密保護属性の指定は，WFL(Work Flow Language)のSECURITY制御文やCANDE(Comand AND Edit)のSECURITY命令によって，あるいはプログラムにより指定される。ファイルの所有者（ファイルのFILE−NAMEで指定されている利用者コードと同じ利用者コードの利用者）と特権利用者だけがファイルの機密保護属性を変更できる。

ⓔ　機密保護違反

入出力動作における機密保護は，初めファイルを開くときに検査される。すべての違反に対し，ミックス番号，違反者のジョブ番号および利用者コードが違反コードおよび違反の原因タイトル（問題のファイル）と共に，システムのサマリー・ログの中に記録され，センタ管理者は経歴をトレースできる。

ⓕ　データ保護機能

使用されたファイルの内容がユティリティなどで不用意にダンプアウトされたりして，その内容が漏洩する危険を防ぐ手段としてSENSTIVE属性がある。属性SENSITIVEはファイルの消去時にデータ

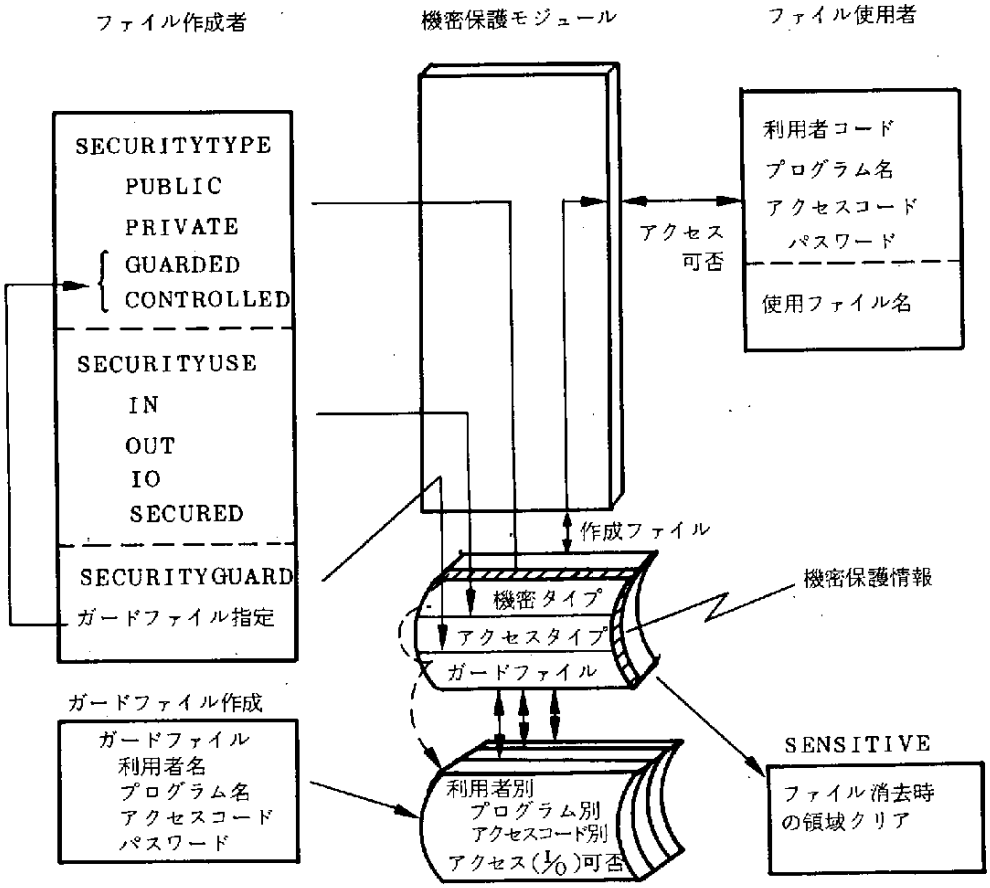


図１－８　ファイルの機密保護機能

が使用したディスクやメモリの領域をクリアすることを指示する。

以上のファイル機密保護機能を図１－８に示す。

② リエントラント機能

プログラムとデータがモジュール単位に作られ，リンクされて１つのロード・モジュールが作られる方式のコンピュータ・システムでは，メモリ保護の点から悪意のユーザによるプログラムの改ざん消去を防止することは困難である。これを防止するには，プログラムとデータを明確に分離しプログラム・コード自身とプログラムによって変更できないような機能をシステムが用意する必要がある。

この解答の１つがプログラムのリエントラント機能である。リエントラントの目的は，本来同一プログラムを同時に共用することによって，メモリ必要量を小さくすることにあるが，副次的な効果として，プログラム自身によるプログラムの破壊を防ぐことができる。たとえ悪意のあるプログラムの変更が可能であっても，その部分を消去するためには再度コンパイルする必要があり経歴として記録に残る。オリジナル・ソース・プログラムに対する変更はパッチ作業で行われるが，当社の外国機の場合はバインド方式で行われその経歴がプログラム上に記録される。

③ コンパートメント制御

ユーザやプログラムおよびファイル等をコンパートメントと呼ばれるグループに区分しておく。この区分はユーザ・コードによって識別している。あるコンパートメント内に含まれるユーザ・ファイルがアクセスを許されるのは，同一ユーザ・コードを持ったファイルやディスクあるいは端末装置に限定する方式を採用している。

④ クリアランス・コンパートメント制御

機密レベルは前述のファイル・アクセスやSAFE(Security Administration Feature：ユーザ情報とデータセット・ボリュームの機密保護

の管理を行う制御プログラム）機能により定義されるが，このクリアランスとコンパーメント制御を組み合せた制御を一部実施している。

クリアランス制御では高いレベルを持つユーザやプログラムは，それより低い機密レベルを持つファイルに原則として無条件にアクセスできる。しかし高位の機密レベルを持つユーザが，その必要性がないにもかかわらず，単に高位であるという理由から，それより低い機密レベルのファイルを読むということのないようコンパートメント制御を併用し乱用を防御している。

⑤ プロシージャ制御

アクセスを許されたファイルであっても，データ内容によって利用を許せない場合が存在する。特にデータベースに対するアクセスにおいて，通常のアクセス・コントロールよりさらにきめ細かい制御が必要になる場合がある。このようなアクセス制御はそのアクセス条件を判定するプロシージャを応用システム内に組み込んで行っている。これは要求されるデータ保護のレベルとそれに投入するコストの費用／効果を考慮して，必要に応じた厳しいアクセス制御を行なうことができる。

(3) データベース保護

アクセス・コントロールは通常のユーザ・コード，パスワード方式とDBMSのアクセス・コントロールを併用した二重のパスワード方式を採用している。特にユーザが限定したいデータベース（会員制サービスおよびプライベート・データベース等）については，ファイル毎にパスワードを設定することができる。

データベースは総て特定のユーザ・コードのもとにおき，データベース管理者以外からの消去や内容変更は不可能にしている。またデータベースの内容を圧縮することにより，他のプログラムで出力された場合にも内容の解読を困難にしている。これはTSSの端末からデータベースの内容をコピーすることが可能であるための措置であるが，大量にコピーされることを防ぐた

め一部のデータベースでは，一文献出力当りのロイヤリティを請求している。この結果大量コピーはコスト高につく。

現状での問題点は，データベース利用のプログラム以外のプログラムから，データベースのコピーが可能なことと，データベースの内容がコピーされた場合その実態をつかむことが難しく，特にマイコン付TSS端末を用いるとかなり容易にマイコン側のプロッピ・ディスクへコピーが可能となることである。

これらの防止策について現在開発中であるがユーザとの信頼関係に頼らざるを得ない面が残る。

(4) セキュリティ上の問題点

情報処理サービス業は，内外の複数ユーザに対してサービスを行っている。したがって個々のユーザあるいはユーザの利用形態により，セキュリティ対策についても自ずと強弱が生じてくる。コンピュータ犯罪と呼ばれるものはその性質・手口などから4つのパターンに類型化されている。

- 金銭の不法領得 ―― コンピュータの不正使用
- システムおよびデータ等の破壊
- マシン・タイムの窃盗
- コンピュータ資源の不法領得

これらの防止対策として，物理的安全対策，運用管理面の対策，技術的対策および制度的対策が考えられる。ここでは現状の技術的対策からみたセキュリティ上の問題について，サービス形態別に考えてみたい。

① オンライン・ネットワーク・サービス

ⓐ 各種端末機の操作は，顧客（社内ユーザも含む）の責任において行われており，アクセス・コントロールはユーザ・コードとパスワードで行っている。ユーザ・コードは殆ど公開された状態にあるものと考える必要があり，コントロールのポイントはパスワード1つに掛っている。ファイルへのアクセスは別に定めることができるために，二重のパスワー

ド方式になっているが，ユーザがこの方式を利用しなければ不正なアクセスは防止しにくい。各端末に特殊固有鍵（キー）を持たせる等の処置が必要である。

ⓑ 通信回線上のセキュリティ対策として暗号化があるが，現在まだ採用していない。

ⓒ 各端末からのホスト・コンピュータ利用状況は現在5分間隔でその接続状況が記録される。またユーザ・コード別に，ログが取られ，事後に追跡できるシステムになっているが，通常は詳細ログのプリントは行っていない（サマリー・ログのみ）。利用回数が多いため現状では詳細ログの出力は困難であるが，詳細ログのチェック方法を検討する必要がある。

② バッチ処理サービス

外部委託のオペレーションを含めて，内部の運用管理が焦点となる。原則としてコンピュータに近づくことができないため，犯罪が発生するとすれば，マシン・タイムの盗用か，コンピュータ資源の不法領得が考えられる。しかし内部の担当者が絡んだ行為は発見が非常に難しく抜本的な対策がないのが現状である。グループ管理者による管理の強化，本人以外の担当者によるシステム・テスト，システム監査によるチェック方法等対策としては考えられるが，数千のソフトウェア・システムに対して実施することは不可能である。

コンピュータ・システムは定期保守，トラブル・シューティング，あるいはＯＳのレベルアップ等のため，一時的にメーカの保守要員や，ＯＳ担当ＳＥに引渡される場合がある。この場合に機密に属するデータやファイルを総てクリアして渡すわけではなく，かなりの重要な情報が入ったまま引渡される。もしこれらの担当者が不正を働く気があればシステムについて一番理解力のある人間であり，例えパスワードがhash化されていたとしても，ユティリティ・プログラムで簡単にダンプ・アウトすることができる。ダンプ・アウトの危険をさけるため，システム管理者が磁気テープ

等にデータを出力し，全データをクリアして渡す方法が考えられるが，この場合当社ではＭＴの数が２００～２６０本となり，時間で２０数時間を必要とするため，現実問題として不可能である（Disk：２７,０００ＭＢ相当）。

③　データベース・サービス

アクセス・コントロールは通常のユーザ・コード，パスワードとＤＢＭＳのアクセス・コード，パスワードで行われている。各データベースに対し，ユーザ毎にかなりきめ細かい規制が必要であるが，その他にユーザ側がマイコンを利用する場合は注意が必要となる。一般にMachine Readableな使用方法は許されておらず，マイコン利用の場合，フロッピー・ディスクやＭＴへの出力は禁止される。これらの管理を強化するとユーザ側の機密を侵害する可能性がでてくる。その他，フロー・コントロール，推理コントロール，データの暗号化等が具体的に行われていない点が問題である。

④　その他セキュリティ上の問題点

ⓐ　アクセス・コントロール

イ．バッチ処理において，カード入力方式で使用する場合，当社の国産機システムの運用では，１枚目にユーザ・コードとパスワードが必要である。これは人目につき易く盗まれる可能性大のため少くとも２枚目以降にセットできるよう改良する必要がある。

ロ．ユティリテイ・プログラム等の使用時または端末機より使用する場合，ユーザ・コードやパスワードが見えてしまう使用方法があるが，これらのオプションは禁止すべきと考える。

ハ．グループでファイルを共用するシステムの場合，ファイルのアクセス権はもう少し厳密に設定すべきであり，メーカより提供されているアクセス・コントロール機能を良く分析し，システムのセキュリティ面を考慮したシステムの再構築が必要なものもある。

ⓑ　リソース保護

イ．ユティリティ・プログラムによるメモリやファイルのダンプ・アウトに対しては運用管理面からの対策は可能であっても技術的対策が弱い。

ロ．外部に持ち出せる記憶媒体のデータに対する暗号化等のセキュリティ対策は具体的に行われていないので，この対策が今後の問題である。

ハ．カタログ管理手法を，もっと活用する必要がある。

ニ．回線の故障等トラブルの早期発見のための自動障害監視システムの構築が必要である。

㈥ その他

イ．オンライン・サービスにおいて，公衆回線上でトラブルが発生した場合，ユーザからの連絡がないと発見が難しい。また端末機の故障を早期発見するためにも，自動障害探索機能をもった監視システムや訂正機能，回復機能を持つシステムの開発および遠隔保守診断機能をもつ機器の設置が必要である。

ロ．システム開発用ツールとして，PRE−COBOLを要求仕様言語として開発し使用しており，さらにPRE−FORTRANを開発中であるが，汎用で多目的な高級要求仕様言語の開発が必要である。

1.5.3 今後のセキュリティ対策と期待される機能

コンピュータの利用は情報化の進展に伴ない，ますます高度化，複雑化してきている。マイコンやパソコンの普及とデータ通信の発展によるコンピュータの大衆化に対し，ＤＰ部門やデータ通信の管理者は入室管理などの物理的対策や，アクセス管理などのソフトウェアを含めたセキュリティ面の総合的対策で対処するとともに，その重要性を再度認識する必要がある。

セキュリティ対策を技術的な面で捉えた場合，ユーザが独自の技術を開発することはかなり難しい。また一般的に，コンピュータ内部の情報を盗難や操作，乱用から完全に保護する手段は存在しない。保護対策が最善であってもそ

れは被害およびリスクを低下させるだけであり，リスクを全面的に消滅させることは不可能である。最善のコンピュータ・セキュリティ対策とは，コンピュータ設備と機器，運用対策，そしてデータ処理，データ通信の方式を理解したうえで，物理的管理とソフトウェアによる管理を組み合せ，これを適切に利用することである。したがって今後のセキュリティ対策としては，既存の対策の線上で，メーカやユーザと協力して対策を強化するとともに，新技術の導入を図る必要がある。

(1) アクセス制御と本人確認

コンピュータ悪用の多くの部分が，物理的設備に合法的に接近しうる内部の人の行為であり，このため保護対策はさらに強化する必要がある。

コンピュータのアクセス権の認可は個人を識別し認証したうえで与えているが，その認証のためにパスワードを使っている。このパスワードが現状では唯一の鍵であり，この管理は一部を除いてコンピュータ・ユーザ自身にまかせているため，総てが厳重に管理されていると言い切れない。これらの危険を防止する対策として以下のことを実施する必要がある。

- 入力されたパスワードは認証後，可能な限り早く消去する。
- システム・サイドでは，必ず一方向性の暗号化形式でこのパスワードを確認テーブル上に記録する。当社の外国機の場合，パスワードは48bitsにhash化されるが国産機の場合は行われていない。
- パスワードの入力回数を減らすため「識別の継続機能」をシステムに持たせる。
- 一定期間ごとにユーザに対して強制的にパスワードを変更させるオプションと，ユーザ側からのパスワード変更権を禁止するオプションを追加する。
- パソコン等の使用による解読を防止するため，パスワードの桁数は少くとも１０桁以上とし，使用文字の範囲を拡大する。
- １つの識別符号が繰り返し破られようとした時，それを検知するアクセス管理システムの開発と，検知した時点でこのシステムはセンタ管理者が調

査する迄，当該の識別符号の利用を停止させる機能を必要とする。

・パスワードの暗号化と確認テーブルの論理的セキュリティによるアクセス・コントロールを開発する必要がある。

(2) データ通信

コンピュータが通信回線に接続されている場合，その利便さに比例して不正なアクセスを許すリスクは増加する。適切な物理的アクセス管理とソフトウェアによるアクセス管理システムを利用すれば，センタ内部にあるデータは保護できる。しかし，データはしばしば電話回線により送受信される。データ通信が電話回線に限定されているとすれば，盗聴の危険性は大いにある。まして衛星やマイクロ・ウエーブによる通信の場合は防止が不可能といえる。この場合盗聴者は回線に物理的に接続する必要すらないため，発見される可能性はないに等しい。

データ通信におけるセキュリティ対策は研究が進められているが，当社では具体的に実施されていない。データの暗号化やユーザのロケーションを入力させるポートの管理および日付，時間による管理技術が今後必要と思われる。

(3) 専用コンピュータ化

コンピュータ利用の高度化，広汎化に対応し，ますます複雑化する情報処理に対処するため，目的別にホスト・コンピュータの機能を分散することが必要と思われる。設置されている各コンピュータに対して，セキュリティ・チェック，オンライン制御，システム開発，プロダクション等を能力に応じて分散し専用化を図ることで，より高度の利用が可能になると思われる。

① オンラインおよびアクセス制御コンピュータ

センタのホスト・マシンにアクセスする総ての利用形態に対して，アクセス・コントロールと使用するコンピュータへの受渡しを行う。よりセキュリティ機能の優れたコンピュータを充てることにより効果を上げることができるが，信頼度の高いノンストップ・コンピュータあるいはマルチ

ＣＰＵコンピュータが必要になる。

② 開発専用コンピュータ

システム設計段階において充分セキュリティ対策が構築されていなければならない。しかし，開発中のシステムは予想されない事故により，通常のプロダクションを混乱に落し入れる可能性がある。このような事故を避けることと開発スピードを上げるため，プロダクション用のコンピュータと分離することが望ましい。当社もこの方向で検討中である。

③ プロダクション専用コンピュータと大容量記憶装置

バッチ処理，オンライン・リアルタイム，ＴＳＳおよびデータベース等のプロダクションについては，大容量ディスク，ＭＳＳ等を装備したプロダクション専用コンピュータにより処理を行い，併せてオペレーションの自動化を実施する。可能な限り人的介入を少なくするため，ＭＴのマシン室への搬出入は磁気テープ収納ロボットで行う。

(4) 複合的分散処理システム

コンピュータ・システムが高度化・広域化してくると，効率向上のためには集中システム化を図った方が良いと思われるが，これは安全という面から考えた場合非常にリスクが大きい。システム・ダウンがゼロにできない以上，適切なバックアップ手段は欠かせない。その一つの手段は，分散処理システムの採用である。それもツリー型の複合バックアップ体制をもった分散システムが望ましい。各端末レベル，ローカル・レベル，通信レベルそして中央のホスト・コンピュータのレベルで，ダウンを自動的にバックアップするような複合的なシステム的保護が必要と思われる。各レベルでのチェック，すなわちバックアップ機能を十分持たせることにより，端末のインテリジェント化等でそこでのオペレーション・ミスや不正使用のチェックを可能にすることである。本人確認が中央のコンピュータを介さずに各端末段階でチェックできるならシステムはもっと簡素になる。今後マイコンの急速な発達で端末のインテリジェント化が進むことは確実である。その際，全体のシステム

の中で端末レベルでのセキュリティ機能をもう少し与え，その範囲を超えたものはローカル段階でさらにセキュリティ・チェックを行うというように，多層状の分散システムを組むならば，ある程度の危機はカバーできるものと思う。

1.6 自治体

自治体（地方公共団体）におけるコンピュータ利用は，昭和５７年４月１日現在で，都道府県は４７団体すべてが，また市町村についても全体の９３％に当る３０５０団体が，何らかの形で利用するに至っている（参考文献１）。このうち，すべての都道府県と，市町村のうち８７５団体が単独又は共同利用であり，残りは委託処理団体となっている。処理形態は依然としてバッチ処理が主体であるが，大・中都市を中心に近年オンライン処理の利用が増加している点が注目される。

都道府県と市町村は，同じ自治体であってもその性格から，コンピュータの利用方法に明らかな相違がみられる。すなわち，都道府県は自動車税等の各種税業務を除くと，給与，人事管理，指定統計等処理対象が多岐に渡るのに対し，市町村は住民に関する事務（住民票に代表される住民記録，税業務，福祉，国民健康保険さらに国民年金など）が中心である。

本節では，今後増加すると予測される，自治体オンラインの現状について，そのセキュリティ上の問題との関連で採り上げるものとして，以下の業務について検討した。

- 市町村の代表的業務として「住民情報オンライン」
- 都道府県主導で実施検討中の「情報公開システム」

住民情報オンラインは，既に実施段階に到達したシステムであり，一方，情報公開システムは，マニアルでの実施は町レベルであるが，今後のコンピュータ・システム利用の検討が課題となっているものである。従って，本節では，住民情報オンラインを中心に述べるものとし，情報公開システムは簡単に触れるのに留めた。

いづれにしても，自治体オンラインにおけるコンピュータ・セキュリティの中心テーマは，

- システムそのものが社会システムであり，その保持する情報をいかに安全に保管管理するか。

・　取扱う個人情報のプライバシー保護をいかに実現するか。

の２点であると言える。

1.6.1　住民情報オンラインについて

(1)　システム化の背景

住民情報オンラインは，市町村における今後の代表的なコンピュータ利用業務であり，近年漢字処理，データベース処理の普及により，著しく利用団体が増加しているものである。

住民情報のシステム化は，バッチ処理による住民記録システムの実施（昭和４１年東京都中野区）以来，利用分野を飛躍的に拡大してきた。その過程で，カナ・システムの限界と漢字化，バッチからオンライン・リアルタイムへのシステム形態の切換え，データベースによるシステムのトータル化の要求が明確になった。また，システム化の進展に伴い，プライバシー保護を中心とするデータのセキュリティへの配慮が必要となってきた。

こうしたニーズに応えて，住民情報オンライン・データベース・システムを，漢字処理により実施するに至った（昭和５５年度：岡山県倉敷市，埼玉県大宮市）。その後，全国的に同様のシステムの実施／計画の団体が相次いで，今日に至っている。

(2)　住民情報オンラインとセキュリティ問題

現在，住民情報オンライン実施中の市役所を例に採って検討してみた。A市は人口４０万余，大都市近郊に位置し，都市化の波に洗われ近年人口増加著しく，市内各所の１４ヵ所に出張所／連絡所を設けていた。市民課窓口の証明書発行枚数は，６９万枚（５６年度実績）であり，その４０％が住民票関係であった。

A市のオンライン化に際し，以下に述べるような各種のセキュリティ対策を講ずることができたのは，システム開発が新庁舎建設の時期と合致した点に負う所が大きい。一般に，庁舎建設は，システムの構築とは非同期に進行

するケースが多いが，今後のオンライン化計画は設備面を含めた十分な対応のために，是非とも庁舎設計時に配慮することが重要であろう。

① 設備面での対応の特徴

電力事情による瞬断や停電に対しては，商用無瞬断装置の設置（２００KVA，５分間対応）と，地下に設備済の庁舎自家発電設備から，電力を供給できる体制をとった。

また，コンピュータ関連の事務室の入室に際しては，電子計算機課の３ケ所の入口すべてにＩＤカードを設置し，ＩＤカードの交付者か，電子計算機課の許可した者以外の入室を禁止した。さらに，コンピュータ室は，特別のカード保有者のみの入室を原則とし，安全対策を強化している。

② データ，プログラムの保管管理

あらかじめ定められたマスタ・ファイル及び使用中のプログラム資産は，すべて完全復元可能な対策を講じた。先ず，コンピュータ室内に磁気テープ保管庫を設け，耐火設備を完備させた。次に，本庁とは別の２ケ所の保管場所に，一定の管理方法に基づき，同一内容の保存テープを管理することとし万全を期している。

③ オペレーションの自動化

コンピュータ室の空調，電源投入，システムの起動や逆の手順による終了処理を自動化可能とした。このために，コンピュータ室の要員の勤務体制が計画化可能となると共に，オペレーション等の正確性も実現した。

④ プライバシー保護への配慮

コンピュータ端末の利用に際しては，端末でのＩＤカード読取と業務開始時のパスワードとの，二重のチェックを行っており，端末利用部門が許可された情報しか利用できぬよう配慮している。さらに，利用記録はジャーナルにとり，後日チェックを可能としている。

運用上の規定は「データ保護管理規定」により行っており，特に問題はないと考えている。従って，現状ではプライバシー保護条例等の制定化の

動きはない。

1.6.2　情報公開システムについて

情報公開は，５７年３月山形県金山町が全国の自治体に先駆けて条例化し，実施時期に入ったと言える。ただし，都道府県や政令指定都市は，現在その準備段階であり，実際の実施にはまだ時間を必要としている。５６年３月の調査（時事通信社と社団法人地方行財政調査会が都道府県と指定都市対象に実施したもの）によれば，２４府県と５都市が検討機関を設けて調査中であると回答してきており，全体として大勢はシステム化の準備段階であると言える。

(1)　コンピュータ・システムの利用

神奈川県作成の「情報公開の制度化をめざして」（参考文献３）によると，公開のためのシステムには，

- 公文書目録の作成開示
- 情報公開コーナーの設置
- 公文書の管理及び検索システム

を検討しているとされている。このうち公文書の管理システムと検索システムは，コンピュータ利用の検討対象となるものと思われる。

(2)　情報公開とプライバシー保護の関係

情報公開はプライバシー保護が図られることが，"公開"の条件となると思われる。行政管理庁のプライバシー保護研究会の「個人データの処理に伴うプライバシー保護対策」に関する研究・検討結果の報告書（以下，「報告書」と略す。）によれば，地方公共団体の動向について触れる中で「最近では，府県段階においても，情報公開制度の検討が進むにつれて，条例によるプライバシー保護の必要性が議論されるようになっている」と言及していることからも，極めて重要な課題であると考える。今後は，プライバシー保護を盛込んだ制度の条例化と共に，システム内部に各種のチェック機構を設けることが必要となろう。

1.6.3　自治体オンラインとセキュリティ対策

(1)　コンピュータ・システムへの配慮

ここでは，コンピュータ・システムの故意の悪用防止と，その検出方法について述べる。内容的には従来から検討してきた事項と大差はないが，いずれにしても一層の徹底化が必要と考える。

①　技術面の対策

- 端末利用者とファイル・アクセスの管理
- 端末利用者のＩＤカード，パスワードによる管理（利用者の特定化と利用可能情報の別扱）
- ファイル内容の不要なリスト出力の防止
- 証明書出力後の用紙の改ざん防止（「改ざん防止用紙」の活用）

②　運用管理面

- システム監査の実施
- コンピュータ室の入室管理
- データ，プログラムの保管方法の改善

③　今後の課題

- オペレーションの一層の自動化により，システム稼動中の故意の悪用防止
- 現在，住民票を可視的な形で保管することが残された課題である。情報ファイルの保管方法の徹底化により，台帳保管の廃止を実現することも重要である。

(2)　プライバシー保護との関係

現在，全自治体３２７８団体のうち，「プライバシー保護条例」を制定した団体は，９０団体であり，今後も徐々に増加する傾向にある。さらに，行政管理庁の前掲「報告書」によっても，個人データの保護に関する関心は高まってきていると言える。

従来，何例かの違法事例が発生したが，自治体におけるプライバシー保護

は，おおむね守られてきたと評価できる。これは，基本的には，地方公務員法や地方税法等にみられる守秘義務により運用されてきた点と，自治省の各種の行政指導により，コンピュータ利用に際し，各種の運用規則や規定を設けるなど，法制度上の対応が即応できた点によることが大きい。

今後とも，公開の原則とプライバシー保護の要請を十分に配慮した施策が必要であろう。

〔参考文献〕

1) 自治大臣官房情報管理官室編，「地方自治コンピュータ総覧」，丸井工文社，１９８２．１２

2) 行政管理庁行政管理局編，「プライバシー保護の現状と将来」，ぎょうせい，１９８２．８

3) 神奈川県情報公開準備室編，「情報公開　制度化をめざして」，ぎょうせい，１９８１．３

4) 今橋盛勝他，「自治体の情報公開」，学陽書房，１９８２．４

5) 堀部政男，「現代のプライバシー」，岩波書店，１９８０．８

6) 「地方自治コンピュータ」，財団法人地方自治情報センター，Vol.１２，№８，№１０，№１２，１９８２．８，１０，１２

7) 「ＦＡＣＯＭジャーナル　特集：行政情報システム（地方自治体）」，富士通株式会社，Vol.７，№４，１９８１．４

2. 現在のセキュリティ関連技術

本章では，既に実用化され，稼働中のコンピュータ・システムや応用システムに採用されているセキュリティ関連技術の現状をまとめ，その問題点や課題を指摘する。現在研究中のセキュリティ技術，今後新たに開発が期待される技術については，第3章で述べる。ここでは，調査・検討した結果を，以下のように分類してまとめてある。

① 本人確認及びアクセス・コントロール技術

② リソース保護技術

③ データベース保護技術

④ 通信ネットワークのセキュリティ関連技術

⑤ 暗号化技術

⑥ その他の関連技術

調査・検討に当っては，内外のコンピュータ・システムすべてを対象とした。しかしながら，コンピュータ・セキュリティには微妙な問題が多く，このような調査自体が調査対象となるシステムの安全性を低下させる恐れがある。キャッシュ・カードのフォーマットが知れ渡ったために，キャッシュ・カードの安全性が低下したというのは好例である。そのため，残念ながら公表できない項目があったことを，つけ加えておく。

2.1 本人確認及びアクセス・コントロール

本人確認とは，利用者がコンピュータや端末を利用する時，あるいは室の入退時等に，利用者の識別（Identification）および承認（Authentication）を行なうことである。また，アクセス・コントロールは，その利用者がコンピュータ利用を許可されているかどうか，また許可されている範囲内で正しくコンピュータを使用しているかどうかを検証するもので，何れもセキュリティには欠かせない機能と言える。本節では，本人確認およびアクセス・コントロールに関して現在実現されている技術，およびそれらの問題点について説明する。

2.1.1 本人確認技術

(1) 本人確認技術の種類

本人確認のためには，その人が確かに識別の本人であることを確認するための情報が必要になるが，この確認情報としては以下の3つの種類がある。

① 本人のみ所有している持ち物

一般的には，バッジ，身分証明書，印鑑等が使用されるが，コンピュータに関連する本人確認手段としては，IDカードやオペレータ識別鍵が一般的である。IDカードは，プラスチック・カードに磁気ストライプが装てんされていて，物理的な規格がJISにより規定されている。IDカードは，端末のオペレータ識別用，室の入退室管理用，あるいは銀行の自動化機器（キャッシュ・ディスペンサ（CD）およびオートマティック・テラーズ・マシン（ATM））利用時の本人確認用等に幅広く利用されている。IDカードの磁気ストライプには本人を識別するための情報（名前やID番号）が記録されていて，IDカードを所有していることが本人であることを証明することになる。しかし，それだけでは，IDカードの他人使用に対する防御が働かないため，より厳しいセキュリティが要求されるシステムでは，後述するパスワードや暗証番号を併用している。

尚，最近では，プラスチック・カードにホログラフィック模様を記録し

たり（三洋電機のホログラム・カード），ＩＣメモリを埋込んだ（ハネウェル社のＣＰ－８）新しいＩＤカードが開発されているが，これらの本格的な利用は今後に期待されている。

一方，オペレータ識別鍵は，端末を操作するオペレータに別々の鍵を渡し，端末が鍵の形状を識別することにより，鍵の所有者（すなわち本人）を識別するもので，金融機関の窓口端末等で利用されているケースがある。この場合も，鍵の他人使用を防ぐ手段はなく，金融機関のように鍵の管理が十分徹底されるようなシステムでないと利用は難しいものと思われる。

尚，印鑑については，我国では古くから重要な本人確認手段として使われてきており，現在でも，各種の証明書や金融機関の通帳・証書類には印鑑が押印されている。このため，地方自治体や金融機関では印鑑簿の管理や印鑑照合のための事務処理に多くの人手を要しており，その機械化が望まれているが，最近のイメージ処理技術の進歩に伴ない，印鑑の入力，記録，出力，伝送，さらには照合を行なう装置が実用化され始めている。

② 本人のみ知っている情報

今日では，パスワードや暗証番号が一般に使用されている。パスワードは，通常８文字以上の英数字で構成され，タイム・シェアリング・システム（ＴＳＳ）やデータベース・システム等の高度なシステムで広く利用されている。一方，暗証番号は金融機関の自動化機器を利用するときの本人確認手段として利用されている。金融機関に於ける暗証番号は数字４桁で構成され，キャッシュ・カードに記録されている。パスワードや暗証番号による本人確認は，本人のみ知っている言葉や数字をコンピュータやキャッシュ・カードに登録し，利用者がコンピュータや自動化機器を利用するときに，その内容を入力し，照合して本人確認を行なう方法である。

パスワード（暗証番号はパスワードの一種であるため以後パスワードで総称する）による本人確認は，現在それに代わる有効な本人確認技術が開発されていないこともあり，現状では，殆んど唯一の本人確認手段と言え

る。ところが，パスワードは一度他人に知れると，保護は効かなくなる。事実，これまでにも，大学の共同利用センタや金融機関システムにおいて，他人のパスワードや暗証番号を使用した犯罪や事故が多く起きている。このため，パスワードの管理が極めて重要になるが，それらについては，パスワード管理の項を別に設け，そこで詳しく説明する。

③ 本人の有する特徴

この本人の有する特徴としては，声，容姿，筆跡，指紋，手形等があるが，この特徴に基づく本人確認が最も確実な方法と言える。現在，声紋，指紋，筆跡（サイン），手形により本人確認する技術が研究されていて，一部実用化されているが，それらの説明は次章の「今後検討すべき基本技術」の章に譲る。

(2) パスワード管理技術

前述したように，パスワードは今日最も重要な本人確認技術であるが，パスワード自体の保護には十分な配慮を必要とする。例えば，通信回線の盗聴やピギーバックと呼ばれる方法（端末装置とコンピュータ間の通信回線を切離して，その端末装置を自分のコンピュータに接続し，利用者に本物のコンピュータに接続されていると誤解させ，ユーザから必要な情報を盗み出す方法）で，パスワードを盗み見したり，あるいはコンピュータのパスワード・マスタからパスワード情報を盗み出したりされる危険性がある。このため，大学や研究機関等では，パスワード管理に各種の工夫を施しているが，以下にいくつかの例を示す。

① パスワードをシステムが生成する方法

パスワードは通常利用者が決めるが，その場合，誕生日や名前，住所，電話番号を利用する場合が多く，容易に類推される欠点を持つ。このためMITのMULTICSシステムでは，システムが5～8文字の発音可能な無意味語をパスワードとして生成し，利用者に提示する方法を採っている。利用者は気に入らないときは拒否でき，気に入った場合はそれがパスワー

ドとして決定する。また変った方法としては，端末の側に品物の絵と2桁の数字を対として掲示しておき，利用者はその品物の中から2つを選んで，その2つの品物に付いている合計4桁の数字をパスワードとして利用する方法もある。この場合，ユーザは4桁の数字の代りに，2つの品物を覚えていれば良く，システムがパスワードを決める場合のパスワードの覚えにくさの欠点が軽減されている。

② パスワードを頻繁に変える方法

同一のパスワードを長期間用いると，漏れたり，しらみつぶしに調べられたりする危険性が高くなる。これを防止するため，利用する毎にパスワードを変更したり，SWIFT（Society for Worldwide Interbank Financial Telecommunication）システムのように，初めに別々に配布された2組のパスワード・リストから毎回異なるパスワードを拾って使う方法などが採られている。また，ローレンス・リバモア研究所のOCTOPUSシステムでは，パスワードにカウンタを付加し，カウンタをセッション毎に1つずつ増加して，もし番号が飛んでいれば不正使用があったことが分かるようにしている。

③ システムと利用者が会話をして本人確認するハンド・シェーク方式

利用者にしか分らない情報（例えば飼い犬の名前等）をシステムに登録し，ログオン（端末接続）時に，システムと利用者が会話をして，本人確認する方法や，システムが乱数をユーザに与え，ユーザはその乱数をあらかじめ定められた計算式に基づいて計算し，その答えをシステムに入力する方法などが考案されている。

④ パスワード・マスタを暗号化する方法

システムに格納されているパスワードのマスタが盗まれると被害が大きい。このため，マスタは暗号化して格納しておくことが望ましい。

2.1.2　アクセス・コントロール

アクセス・コントロールは，利用者がコンピュータを利用するときに，正しく登録されている利用者かどうか，また，許可された正しい範囲内でシステムを使用しているかどうかを検証するためのツールで，元来は大学等のタイム・シェアリング・システムで個別に開発されてきたものが，最近では標準的な機能として整備され，最近の中型以上のＯＳでは，この機能を持つものが多くなってきている。

アクセス・コントロールは一般に，ユーザ管理機能，リソース管理機能，アクセス・モニタリング機能により構成される。

(1)　ユーザ管理機能

ユーザ管理機能には，コンピュータを利用するすべてのユーザ（システム管理者，プログラマ，オペレータ，エンド・ユーザ等のすべての利用者を含む）を登録・管理する機能と，ユーザの属性やシステム使用権を管理する機能が含まれる。

①　ユーザの登録・管理

コンピュータ・システムの利用者は一般に，組織体系に合わせてツリー構造上に体系化できる。例えば，システム全体を管理するシステム管理者を頂点として，利用者も部門別，さらにはグループあるいはプロジェクト別に階層化される。このため，アクセス・コントロールにおけるユーザ管理体系も，ツリー構造で管理される。ユーザ管理における管理体系を図２－１に示すが，これらの情報はディレクトリと呼ばれ，システム・ディスク上に格納される。ディレクトリへの登録・削除は，システム管理者またはグループ管理者により，センタのユティリティを使用したり，あるいはマスタ端末から行なわれる。尚，一般には，本人確認で説明したパスワードもこのディレクトリに管理される。このディレクトリの内容は，ログオン（端末接続）時に端末から与えられるユーザ名やパスワードと照合され，そのユーザが使用可能ユーザとしてシステムに登録されているかどうかが

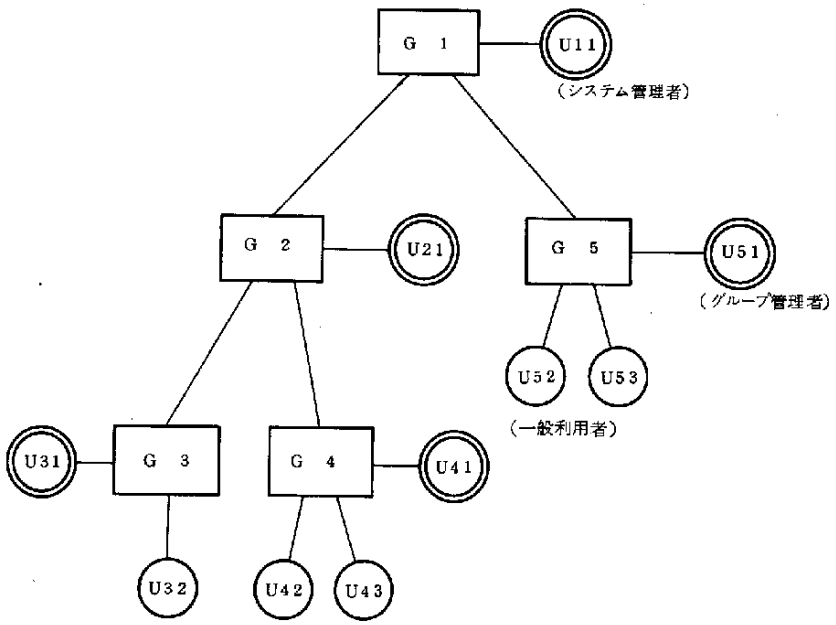


図２－１　アクセス・コントロールにおけるユーザ管理体系

チックされる。従って，アクセス・コントロールのユーザ管理機能の中には本人確認機能も含んでいる。

② ユーザ属性とシステム使用権の管理

ディレクトリにはグループ名とユーザ名の他に，ユーザ毎の属性とシステム使用権を登録できる。

ⓐ ユーザ属性……ユーザはシステム管理者，グループ管理者及び一般利用者にクラス分けされる。システム管理者はディレクトリ全体の管理が行なえ，グループ管理者はグループ内のディレクトリ管理が行なえる。グループ管理者はシステム管理者により登録され，かつグループ管理者としての権限が譲渡されなければならない。また，一般利用者は，システム管理者またはグループ管理者によりディレクトリに登録された後，システムへのアクセス権が得られる。

ⓑ システム使用権……コンピュータの利用方法には，バッチ，オンライン，タイム・シェアリング，エンド・ユーザ言語等があるが，ディレク

トリには各ユーザ毎に利用方法を登録でき，ログオン時には正しい利用を行なっているか否かチェックされる。また，バッチに対してはジョブ・クラス（スケジューリング優先度を決める属性），オンラインに対しては業務別のよりきめ細かな使用権を設定することもできる。

(2) リソース管理機能

アクセス・コントロールのリソース管理機能により保護されるリソースとしては，一般に，ファイルとボリュームが対象になる。プログラムはライブラリ・ファイルに格納されるため，ライブラリ・ファイル単位に保護の対象となる。コンピュータ・システムのリソースとしては，ファイルとボリューム以外にも，CPU，メモリ，端末等があるが，これらのリソースに対する保護は，通常，アクセス・コントロールのリソース管理機能とは別のＯＳ機能により制御される。このため，それらの保護機能に対する説明は，2.2「リソース保護」の節で行なう。

アクセス・コントロールのリソース管理におけるリソース（通常ファイルとボリューム）の保護は，リソース単位にアクセス権を設定することにより行なわれる。アクセス権には，次の4種類があり，ユーザ・プログラムやサービス・プログラムによるファイルへのアクセスは，設定されたアクセス権により決定される。

① ALTER……参照や更新，削除，リネームなどファイルに対するすべてのアクセスが許される。

② UPDATE……参照と更新が許される。

③ READ……参照だけが許される。

④ NONE……一切のアクセスが許されない。従って，アクセス権限はない。

このアクセス権はユーザ単位に独立に設定され，ファイル単位にユーザのアクセス権をまとめたものをアクセス権リストと呼ぶ。アクセス権リストの例を図２－２に示すが，その例では，ファイルA，B，Cに対し，その所有権はユーザＧ１．Ｕ１１であり，所有者には自動的にALTER権が設定され

る。また，ユーザG１．U１２にはUPDATE権が，またユーザG２.U２１とG２．U２２にはREAD権が与えられる。尚，システム管理者には，アクセス権の設定とは無関係に特別の権限（すべてのファイルに対するALTER権及びアクセス権情報が格納されているカタログ・ファイルに対する保守）が与えられる。このように，各ファイルおよびボリュームに対して，各ユーザ単位に独立したアクセス権を設定できるため，きめ細かな保護が可能になる。

```
ファイル ： A, B, C
所有者 ： G1.U11
アクセス権リスト：
  UPDATE ： G1.U12
  READ ： G2.U21, G2.U22
```

図２－２　ファイルに対するアクセス権リスト

(3)　アクセス・モニタリング機能

アクセス・モニタリング機能は，利用者のコンピュータ・アクセスの記録を採る機能で，一般には，不正アクセスに関するモニタリング，正しいアクセスに関するモニタリング（システム・モニタリングと言う）の機能，およびコンソール・ログの機能に分れる。また，標準のＯＳ機能とは別に，アプリケーション・システムの中で業務固有のモニタリングを行なっている例もある。

①　不正アクセス・モニタリング……ユーザ名やパスワードを誤った場合あるいは許可されていないシステム使用権やリソースをアクセスした場合，アクセス・コントロールは利用者の要求を拒否するとともに，そのアクセスの履歴を記録する。この機能により，誤ってあるいは故意にアクセスしようとしたユーザ要求を把握できる。この機能は，通常，アクセス・コントロールの機能として実現される。

② システム・モニタリング……各利用者毎の利用状況（開始／終了時間，経過時間，CPU時間，LP出力枚数，端末使用時間等）及びリソースの稼動状況（メモリ使用状況，ディスク入出力回数，端末使用状況等）に関するデータを収集する機能である。本機能は，本来，利用者に対する課金やシステムの性能評価のためにデータ収集を行なうもので，そのため，セキュリティ機能とは独立したOSの機能として実現されている。しかし，この機能により，どの利用者が（あるいは利用者を騙って），何時システムにアクセスしたかを把握でき，事後検査やシステム監査のデータとして利用できる。

③ コンソール・ログ……オペレータのコンソール上の操作履歴や，システムがコンソールに表示するシステム動作状態履歴が記録される。コンソール・ログを事後検証することで，オペレータの操作履歴を把握できる。

④ アプリケーション・レベルのモニタリング機能……前記3つのOSのモニタリング機能では，アプリケーションに関連した詳細なデータの収集は困難である。このため，OSのモニタリングに加えてアプリケーション・レベルでのデータ収集を行なっている例がある。例えば，金融機関システムでは，1日に行なわれた全取引の内容及び役席者承認扱いの取引の内容を収集し，翌日営業店に還元送付している。

2.2 リソース保護

この節では，汎用コンピュータ・システムのハードウェアおよびソフトウェアで実現しているリソース保護技術の現状について概要を述べる。ここでは，コンピュータ室の入退室ＩＤカード管理等，コンピュータ周辺設備面でのリソース保護技術については割愛する。

また，悪意のあるデータ・アクセス等からのデータの保護（防犯技術），コンピュータ障害等からのデータの保護（保全技術），コンピュータ障害に起因するシステム停止の低減方法（高信頼化技術）に分けて述べる。

2.2.1 保護の対象

ここでは，リソースとしてとらえる範囲について述べる。コンピュータ・システムにおける価値あるリソースとしては，まずデータであるが，それ以外にデータ処理機能自身もとりあげる。

(1) データ

データ（情報）は主としてコンピュータ利用者のリソースである。保護されるべきリソースとして最も重要なものであり，その保護は次の２点に分けて考えられる。

① データ保護

ここでは，狭義に，データの悪意のある公開，盗み，変更，破壊からデータを守ることをいう。コンピュータ・システム内のデータの保存場所として，主記憶上，外部記憶上，回線上の３つに分けて述べる。それら以外に，磁気テープ上，プリンタ用紙上等があり，犯罪対象になり易いが，これらは，コンピュータ・システム外にあると考えられ，物理的な物として対処すべきである。

② データ保全

データ作成後，再読出し可能な状態に保つことをいう。データ破壊が悪意によるかよらないかを問わず，それを防ぐ必要がある。記憶媒体の経年

変化，ハードウェア障害，オペレーション・ミス等がデータ保全を脅かすものである。データのインテグリティとも呼ばれる。

(2) データ処理機能

コンピュータ・システムのハードウェア，ソフトウェアの使用権と，それらの安全対策に分けて述べる。

① プログラム使用権の保護

プログラムは，それ自身データに似た保護対象であるが，読出し権，書込み権以外に実行権の属性があるという点が異なる。事例としては，科学計算用ライブラリ（版権のあるもの）をコピーして，自分のプログラムの一部として組込み，他センタで使用されていたことがある。

② ハードウェア使用権の保護

保護対象のハードウェアとしては，CPU，外部記憶装置，端末等がある。事例としては，大学センタでのTSS課金逃れおよび未登録ユーザの使用がある。

2.2.2 データの保護方法

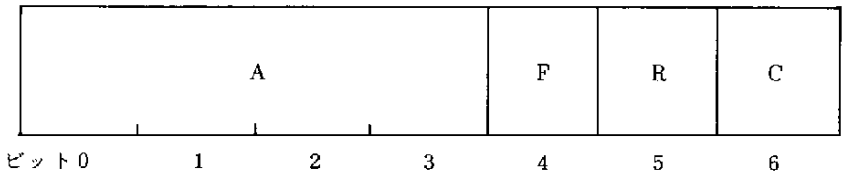
代表的なものについて以下に述べる。

(1) 主記憶上のデータの保護方法

① 主記憶キーによる方法

主記憶の一定領域単位とユーザ・プログラムの各々にキーを与え，それら二つが一致した場合にのみアクセスを許す機構であり，通常ソフトウェアによってキーが設定され，CPUハードウェアによりキーの一致が確認される。これにより，キーの異なる領域はアクセス不可能になり，データの保護能力，保全性が向上する（図２－３，表２－１参照）。

また，ユーザ・プログラムだけでなくオペレーティング・システムの各構成要素にも別のキーを与えることにより，プログラム・ミスによる主記憶上のデータ破壊を防いでいる場合もある。



A ： アクセス制御ビット
F ： 読出し保護ビット
R ： 参照ビット
C ： 変更ビット

図２－３　主記憶キーの形式

表２－１　主記憶キーと保護キーの関係によるアクセスの可否

保護ビット＼キーの関係／アクセス		一　致	不　一　致
0	書　込　み	可	不　可
	読　出　し	可	可
1	書　込　み	可	不　可
	読　出　し	可	不　可

一致：主記憶キーと保護キーが等しい場合か，又は保護キーがゼロである場合である。
可：アクセスは許される。
不可：アクセスは許されない。

② 多重仮想記憶

ユーザごとに独立なアドレス空間を与えることにより，各々のアドレス空間上では同一アドレス値でも主記憶上は常に異なる場所を指定するようにした機構である。ユーザ間の干渉を排除でき，データの保護能力，保全性が向上する。これは優れた機構である一方，主記憶上でのユーザ間のデータの交換や通信が難しくなり，共通アクセス領域を設けているオペレーティング・システムがある。さらには，二つのユーザ固有空間の間でデータの交換や通信が可能な機構も考えられている（図２－４参照）。

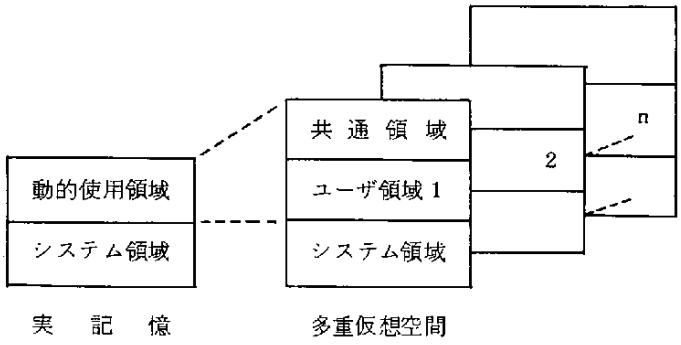


図２－４　実記憶と多重仮想空間

(2)　外部記憶上のデータ保護方法

外部記憶としては，固定ディスク，ドラム等，物理的に取りはずせない装置と，磁気テープ，フロッピー・ディスク，リムーバル・ディスク・パック等，取りはずせる装置がある。前者はパスワード等の論理的手法によりアクセスを制限可能であるが，後者については，他センタへ移動した後読出すことが可能であり，暗号化がデータ保護の一つの手段となる。

①　パスワード保護

これは主記憶キーの方式と似ているがユーザとアクセス対象ファイルの各々にパスワードという識別子を与え，それらの対応状況により，ユーザのファイル・アクセスを制御する方法である。最も単純な方法は，パスワードが一致した場合のみ読出し権と書込み権を与え，一致しなければ与えない方法である（図２－５参照）。この方法は単純かつ有効で汎用性があるが，パスワードを知られないことが重要であり，管理の良いセンタでは同じパスワードを長く使用しているユーザを定期的にチェックし，パスワードを変更するように警告を出している。使い易さの面では，以下の機能がある。

・パスワードのレベル分けが可能なこと（マスタ・パスワードなど）。

・ユーザ・グループとファイル・グループを1対Nまたは N対1に対応づけてアクセス権を付与できること。

・ファイル内のレコードのフィールドごとにきめ細かくアクセス権を設定できること。

また，ファイル以外に端末，プログラムも含んでパスワード保護する場合はリソースの命名規約の作成，一意性保証が必要な場合があり，運用への影響が大きく，徐々に導入できることが大切である。

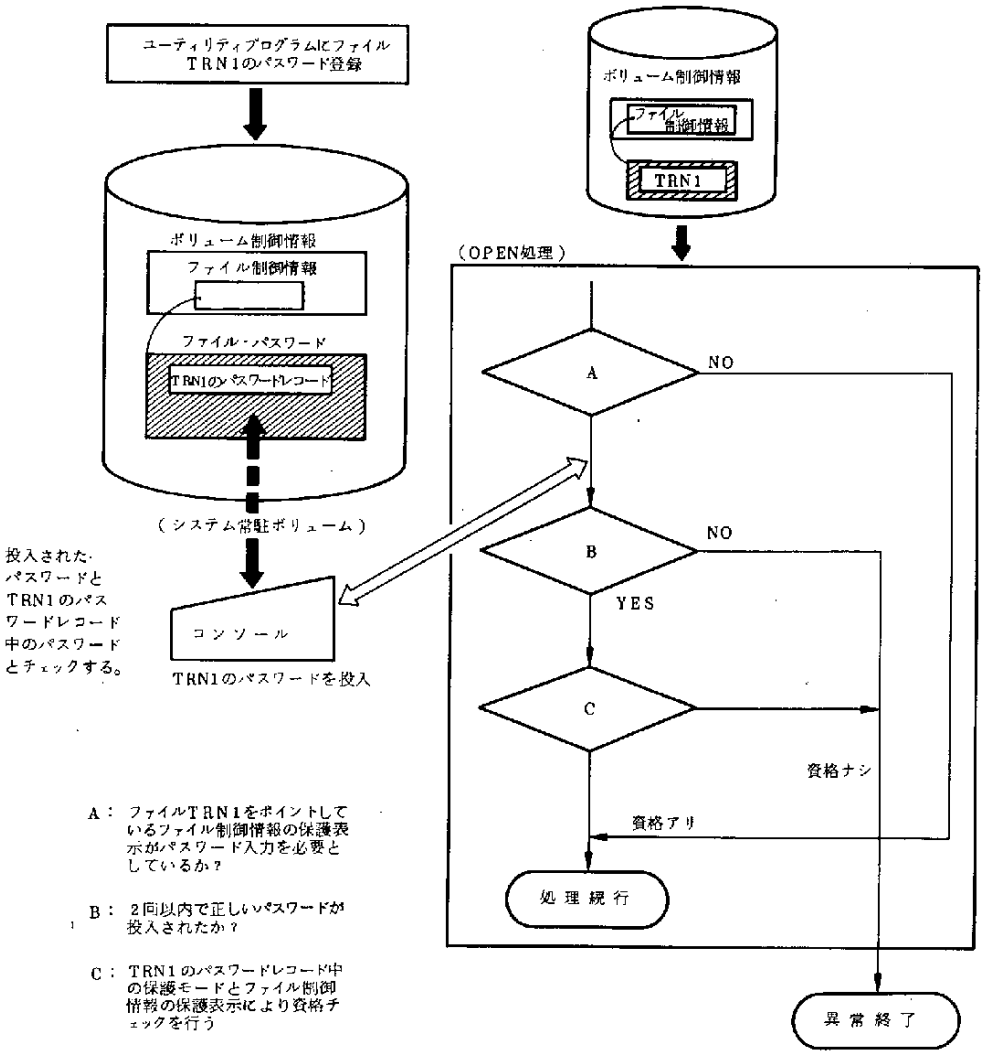


図２－５　パスワード保護と資格チェックの概略

② 暗号化

暗号化はデータが盗まれても，利用されないことにより被害を防ぐことを目的としている。暗号化方法，暗号化キーの管理方法等については以前より研究されており各種の手法がある。ただし，暗号化／復号化処理は一般に負荷が大きく，CPU以外の専用ハードウェアで処理する方が良い。

(3) 回線上のデータ保護方法

回線上を流れるデータの保護方法としては暗号化が重要な手段である。実現手法としては回線の両端に暗号化／復号化装置を設置し，CPU，通信制御装置上では平文で処理する方法と，ホスト間レベルで暗号化／復号化する方法がある。前者はCPU等からは暗号化が見えず導入が簡単な場合もあるが，回線単位に一対の装置を設ける必要があり，回線数の多いシステムではコスト・アップになり易い。また，センタが地理的に離れていてキーの設定や運用が難しいことを考慮し，装置間でキーを自動的に交換する形式の装置も開発されている。

通常，多くの回線使用プログラムはデータ圧縮を行なっており，圧縮手法の高度なものは，暗号化に近いものもある。

2.2.3 データ処理機能の保護方法

(1) プログラム使用権の保護方法

プログラムの実行権を読出し権とは別に与えられるシステムがある。主記憶上のプログラムに対して，CPUアーキテクチャ上，実行権が別になっている場合は，ハードウェア機能を利用し，別になっていない場合は，呼出し時にオペレーティング・システムの介入により判断している。主記憶と外部記憶間のプログラムの移動はオペレーティング・システムによってのみ可能としている。

(2) ハードウェア使用権の保護方法

各センタごとにユーザ識別子が管理され，ジョブの入力，またはTSSの開

始時に識別子がチェックされる。CPUは，ユーザ間で共用されており，各ユーザは使用時間の累積値によって，その後の使用権が判断される。外部記憶については，使用スペース量の総容量で管理され，新しいスペースを要求した時に可否を判断するソフトウェアもある。端末については，パスワードまたはＩＤカードによって使用可否を判断されるのが一般的である。

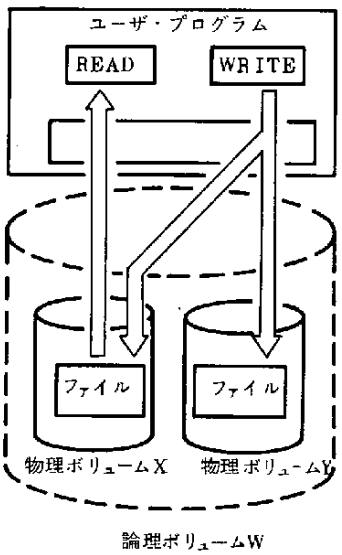
2.2.4　コンピュータ・システムの高信頼化方法

コンピュータ・システムの高信頼化方法としては二重化（冗長化）を中心として以前より多くの手法が開発されている。

ここでは，比較的大きな単位の二重化として，ディスクの二重化と通信制御装置（CCP：Communication Control Processor）の二重化について紹介する。

(1)　ディスクの二重化

ボリューム単位の二重化について述べる。ディスクを二重に用意しておき片系障害時，他系のみで運用する機能である。書込み時は両方に，読出し時は片方からが一般的である。障害の早期発見のため読出しを交互にやる場合もある（図２－６参照）。



・READ処理
負荷分散を考慮して選択した
一方のボリュームに対して
READ処理を行う。

・WRITE処理
両方のボリュームに対して
WRITE処理を行う。

図２－６　　ディスクの二重化

データの二重書きは，ユーザ・プログラムとオペレーティング・システム階層の中でなるべく低レベルでやる方が，一重書きに比較して，性能低下が小さい。ハードウェアで二重書きしているものは無いようだが，入出力制御プログラムで二重書きしているものはある。システム・ダウン後，両系の一致をとるため，ジャーナルを各々でとって比較し最新側に合わせる技術も必要である。

(2) 通信制御装置の二重化

CCPを二重に用意しておき，片系障害発生時，ホストの通信制御プログラムにより自動的に他方に切換える機能である（図２－７参照）。

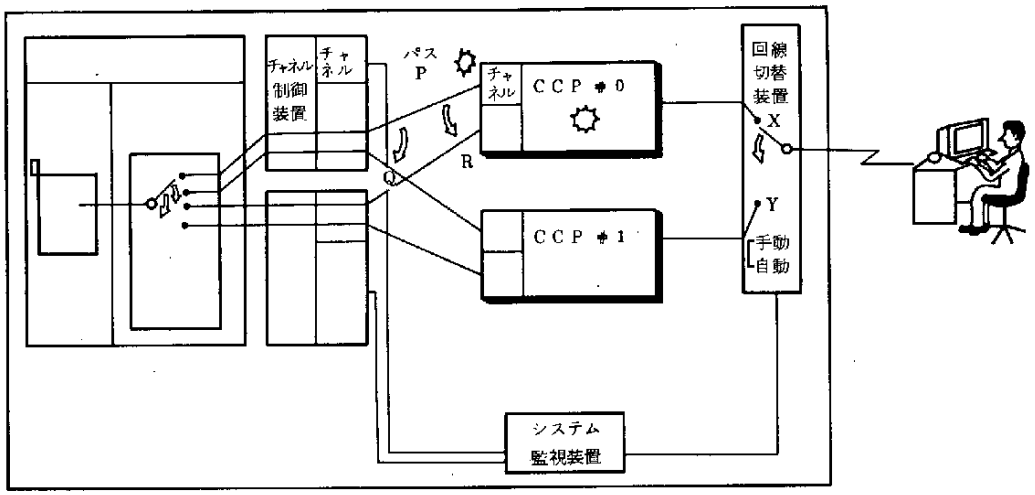


図２－７　　通信制御装置の二重化

CCP又は，チャネルに障害が発生した場合，オンライン・システムの運用に何ら影響を与えず予備CCP，代替チャネルに切換え，自動的に回復処理を行なう。

2.3 データベース保護

2.3.1 データベース保護の必要性

(1) データベース・ファイル

データベース・ファイル（以下データベース）として，現在，磁気テープ，フロッピ・ディスク，磁気ディスク，MSS等が使われている。

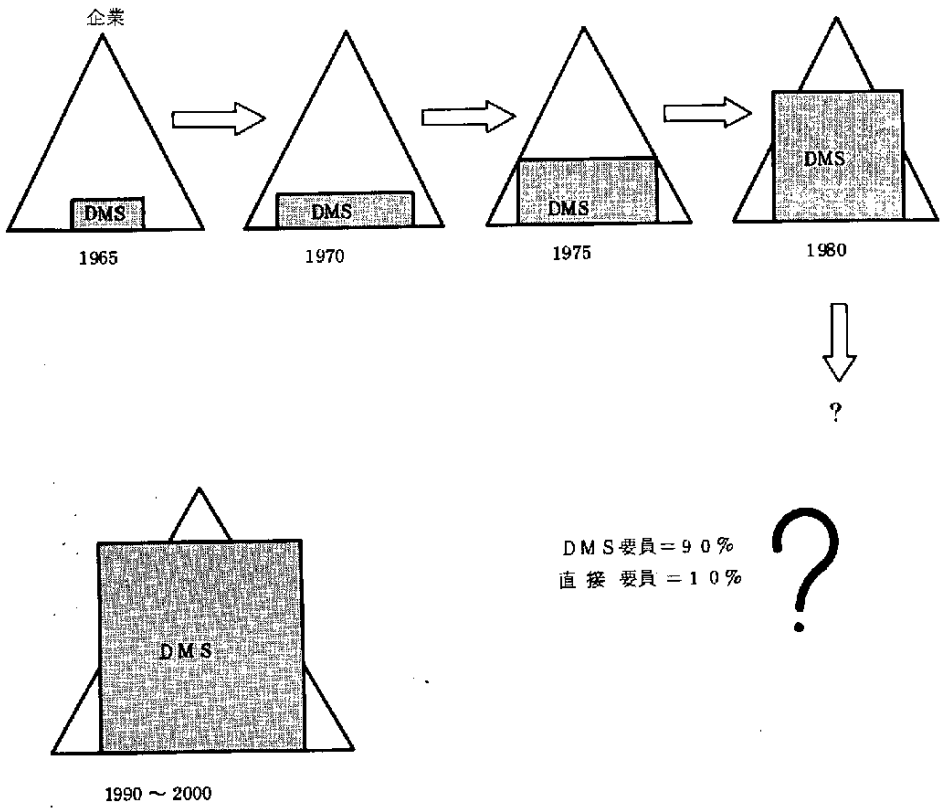
１９８０年代のコンピュータ・システムは，情報量の増大に伴い，情報（データ）が重要となって来ると共に，そのデータの蓄積が，重要な課題となってくる。情報化が進み，データの蓄積，すなわちデータベースが充実し，情報処理技術が進むに従って，１９８０年代は，データベース・ファイルの時代に入り，その用途は，限りなく拡がって行き，誰でも自由に，データ・ファイルを利用するようになって来る。

今までは，特定の関係者が，データ・ファイルを使用していたが，誰でも自由に利用するようになると，データベースの保護が，新しい問題として，課題に上って来た。コンピュータ・システムの利用が進むにつれて，データベースの大きさが，どのように変って来たか，又将来どのようになって行くかを見てみると図２－８のようになる。

１９７０年迄は，磁気テープの管理を，事務センタで行なえばよかった。また１９７０年代は，磁気テープの他，磁気ディスク・パックが加わり，データ・ファイルの管理量が飛躍的に増大し，専任のデータ管理者が必要となって来た。

一方，コンピュータ・システムもバッチ処理から，オンライン処理（閉じたシステム）が主体となり，データベースのデータを取扱う量が飛躍的に増大した。コンピュータ・システムの規模と取扱いデータ量とデータベースの関係を見ると図２－９のとおりである。

コンピュータの用途が拡がり，データが蓄積されて来ると，今迄であれば，簡単に作り直せた一時データが，時の経過を持って累積データとなり，データが歴史を持って重要な意味を持つようになる。また長期のデータ収集によ



DMS : Data Management System

図２－８　データベースの大きさの変遷

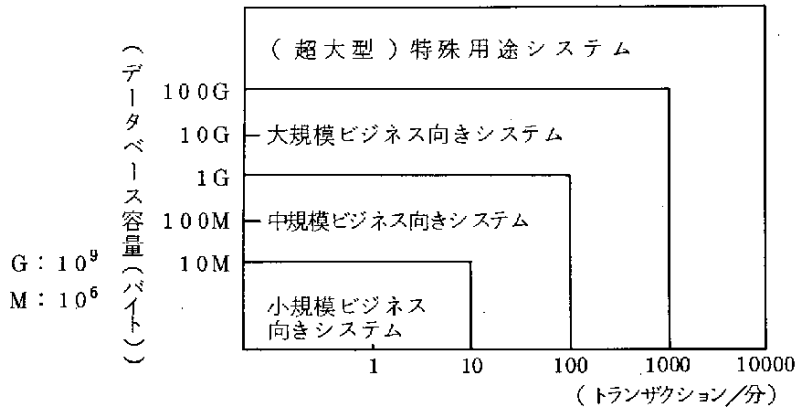


図２－９　　データベースの規模
（出典：Proc. AFIPS 1980 NCC,p.237）

って，データベースとして，資産価値を持つようになる。戸籍，住民データや個人資産等もコンピュータの利用によって，紙から磁気的データベースに変ってきた。ここで，データベースを整理してみる。

① 累積データが経緯を物語るような歴史を持つデータベース

② 長期データ収集によってデータが資産価値を持つような資産データベース

③ 戸籍，住民データ，個人資産データ，人事ファイル等，個人のプライバシーに関するデータベース

④ 顧客に関する収集データ等のデータベース

等がある。改めて作る事が非常に難しいデータ・ファイル，関係者以外に洩れては困るデータが，大規模に多種類所有されるようになって来た。ここでコンピュータ（情報）処理によるデータベースについて，新たな問題が生じて来た。

(2) データベース保護の必要性

データベースが，不意の事故や悪意にもとづく変更，破壊，漏洩することから防御されていなければならない。では情報処理システムの中で，データベースは，セキュリティ上どの位置にあり，どのような問題を持っているか見てみる。

図２－１０に示すように，ユーザから見ると一番奥まった位置に，データベースはあるが，一旦，問題が起ると被害が大きく，又今後ねらわれやすい。

① データベースの問題点の種類

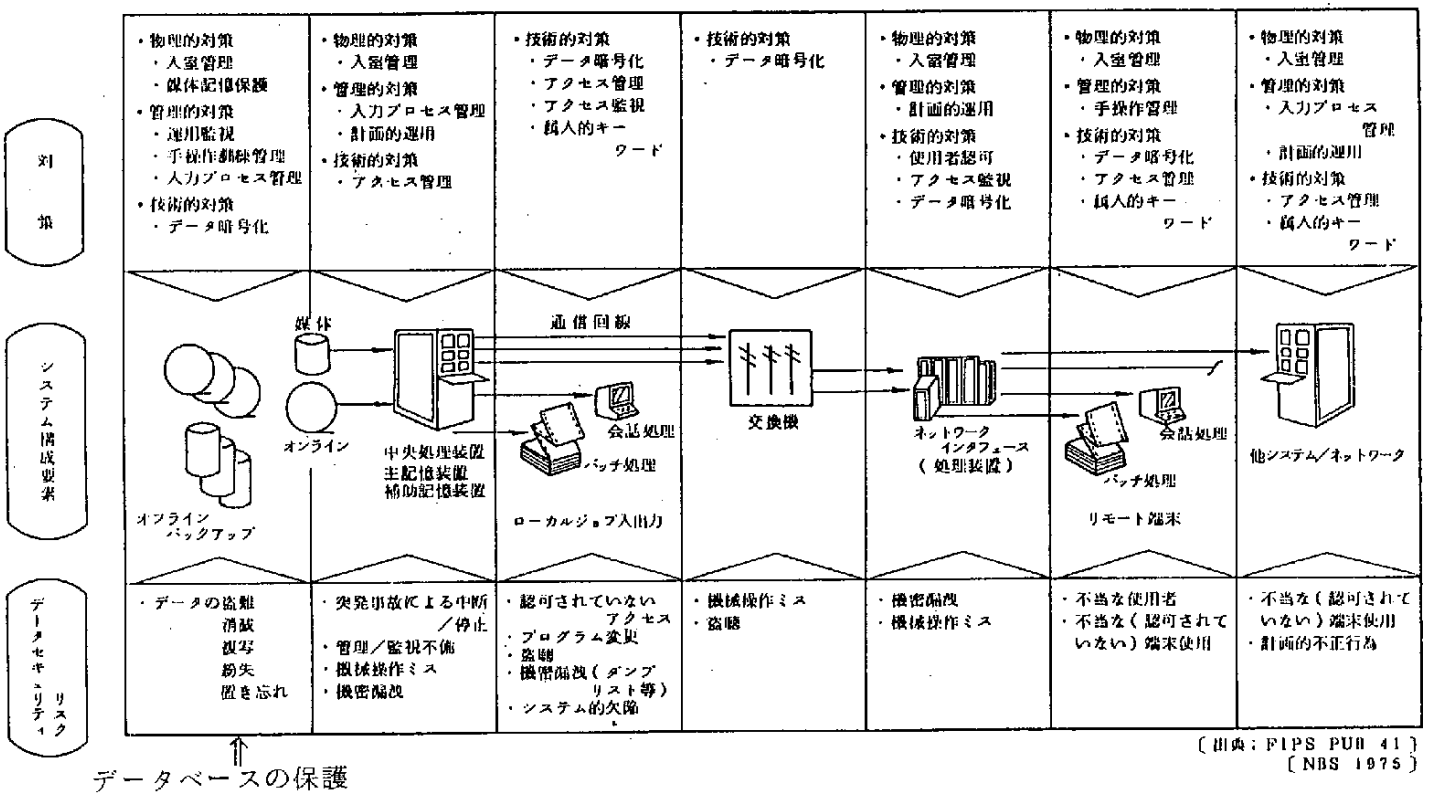
データベースを保護するについて，３つの点から考える必要がある。

ⓐ 悪意によって，データベースが変更，破壊，漏洩する犯罪的なもの。

ⓑ 機械の故障によるデータベースの破壊 ― すなわちハードウェアの信頼性によるもの ― データ自体に関する問題

ⓒ 管理不十分によるデータベースの変更，破壊，漏洩 ― すなわち管理責任によるもの ― データの取扱いに関する問題

この中で，ⓒの管理責任によるものについて，原因を見てみる。



〔出典：FIPS PUB 41〕
〔NBS 1975〕

図２－１０　データ・セキュリティ・リスクとその対策

② データベースの管理責任

ⓐ データベースのユーザ間で，同一のデータに対するデータの仕様（記録形式，長さ等）が異なる事によって問題を起す。

ⓑ データの私有意識がなくなり，無責任体制になることによって問題が起る。

ⓒ データの機密性に対する認識不足によるもの。

ⓓ データの集中，量的物理的な負荷によるもの。

ⓔ データベースの利用規約や統制のルールがないもの。

ⓕ データベースの設計，定義／作成，監視および保守のルール，管理がないもの。

等がある。データを保護するためには，まず次の4点を確保する事である。

イ．データベースの独立性の確保

ロ．データベースの操作性の確保

ハ．データベースの完全性の確保

ニ．データベースの機密性の確保

(3) データベースと犯罪

データベースの犯罪を大別すると次のようになる。

① データの改ざん

内容を故意に変えて，論理不正を起し不正に金額操作を行なう。

② データの破壊

内容を故意に破壊し金額計算不能を誘発させ，経済的ロスに至らせる。または，論理不正を誘発させ，システム停止などの障害に至らせる。

③ データの盗用

内容をコピーなどして転売する。

以下ではデータベースを犯罪から守るため，機械の故障からデータベースを守るため，管理不備によるデータベースの破壊から守るため，どのような技術があるかを見てみる。

2.3.2　データベース機密保護技術

データベースを保護する技術はいろいろあるが，ここでは現在すでにある技術，将来の技術について述べる。

(1)　機密保護技術の分類

保護技術を分類してみると，次の5通りに分けることができる。

①　ハードウェアによる技術

②　ソフトウェアによる技術

③　アクセス技術

④　暗号化による技術

⑤　管理技術によるもの

この分類は，一部だぶったり不合理な面はあるが，わかり易くなるように分けた。

(2)　機密保護の技術

①　ハードウェアによる技術

ⓐ　データベース機密保護機能

リレーショナル・データベースの機密保護方式

ⓑ　再書込み不能ファイル

イ．光ディスク技術

ロ．マイクロ・フィルム

ハ．マイクロ・フィッシュ

ニ．超マイクロ・フィルム

ⓒ　システム運転情報収集高密度化に伴う効率悪化防止技術

イ．記録ファイル

ロ．記録システムのハードウェア内蔵化あるいは外部サブシステム化

ⓓ　ＭＴデータ内容自動消去

ＭＴのカセット化等により，正しいパスワードの入力がない場合あるいはカセットに何等かの物理的破壊が加えられた場合に，ＭＴ内容が自

動的に消去される。

ⓔ 記憶内容の完全消去

従来，ＭＴやディスク・ファイルの消去は，見出しやＶＴＯＣ情報を消去するのみで実体は残ったままとなっている。機密保護のためには，実体を完全にクリアする必要がある。又，メイン・メモリ内の残骸もクリアせねばならない。

ⓕ データベース推論検索防止技術

ⓖ 改ざん防止用再書込み不能ファイル

ロード・モジュール，重要マスタ，あるいは外部持出し不可避のファイル（例えば銀行自振用データ）等の改ざんを防止するため，再書込み（更新）不能な記憶媒体の開発

ⓗ デバイスのキーロックによるデータベースへの不当アクセス防止

ⓘ アクセス・トレース・プログラムによるデータベース・アクセス者のトレース

② ソフトウェアによる技術

ⓐ 対話内容の分析

対話型のデータベース検索において，利用者の質問の組合せによっては，機密性のあるデータが，推測可能になる可能性がある。これを防御するには，システム側で質問の組合せに対するプロテクトを行なう必要がある。

ⓑ 低機密レベルへのデータフローの禁止

高機密レベルのデータをＲＡＥＤする権利のあるユーザが，その内容を低機密レベルのファイルに，ＷＲＩＴＥすると，そこから機密が洩れる可能性がある。この様なＷＲＩＴＥを禁止するのが望ましい。

ⓒ データベース検索文の保護領域チェック機能

データベース検索言語によりユーザが作成する検索文，または検索式に基づくデータ領域は，必ずしもそのユーザに許されている領域内のみ

におさまるとは限らない。

従って，システム側でこの検索文（検索式）を分析し，そのユーザの許可領域以外の部分を検索対象から削除する機能が必要となる。

ⓓ ファイル・ラベル自身に読み出し記録を保持

MTやディスクのファイルそのものの中に，OPENの日時を記録し不正なアクセスやコピーを監視する。

この記録レコードは，責任者の特定パスワードによってのみREADでき，責任者は適宜この内容をチェックする。

③ データの不可視化技術

ⓐ データ圧縮を伴うデータの難読化技術

イ. コダシル型データベースのアクセス・コントロール

- メイン・スキーマの保護方式
- サブ・スキーマによるアクセス・コントロール
- サブ・スキーマの保護方式

ロ. リレーショナル・データベースのアクセス・コントロール

- ビュー管理によるアクセス制限
- ファンクション・レベルのアクセス・コントロール

ⓑ データベース・アクセス領域限定化技術

ⓒ ファイル・アクセス・コントロール技術

イ. READ／WRITE承認方式

ロ. パスワードによるアクセス制限方式

ハ. レコード単位のアクセス制限方式

④ データベース・アクセス領域限定化技術

⑤ 暗号化による技術

ⓐ ファイル上のデータ暗号化

イ. ファイル全体の暗号化

ロ. 部分的暗号化

ハ. キーの管理方式

ニ. 暗号化のアルゴリズム

ホ. 効率のよいシステム体系

ヘ. ハードウェアによる暗号化／ソフトウェアによる暗号化

ⓑ ファイルやプログラムの暗号化

⑥ 管理技術によるもの

ⓐ データ・フロー制御技術（ファイルのコピーのコントロール）

イ. 有資格者のコピー監視技術

ロ. 不正に結びつきやすいコピー処理形態の分析

ⓑ システム運転情報収集高密度化に伴なう効率悪化防止技術

イ. 記録ファイルの改良

ロ. 記録システムのハードウェア内蔵化あるいは外部サブシステム化

2.3.3 データベースのバックアップとリカバリ

(1) データベースの物理的破壊対策

① データベースの物理的完全性のためのバックアップ・コピー

データベースの物理的完全性を維持するためには，データベースの物理的破壊に備えて，ある時点のデータベースの内容を全部コピーして，万一に備える必要がある。これを，バックアップ・コピーと呼ぶ。

② データベースの破壊に備えた更新情報

データベースの破壊があった時，バックアップ・コピーからデータベースを復元するために，データベースに対する更新情報を記録しておく機能と，バックアップ・コピーと更新情報からデータベースの回復を行なう機能が必要である。

③ データベースの物理的破壊からの回復手順

図２－１１に物理的破壊からの回復手順を示す。

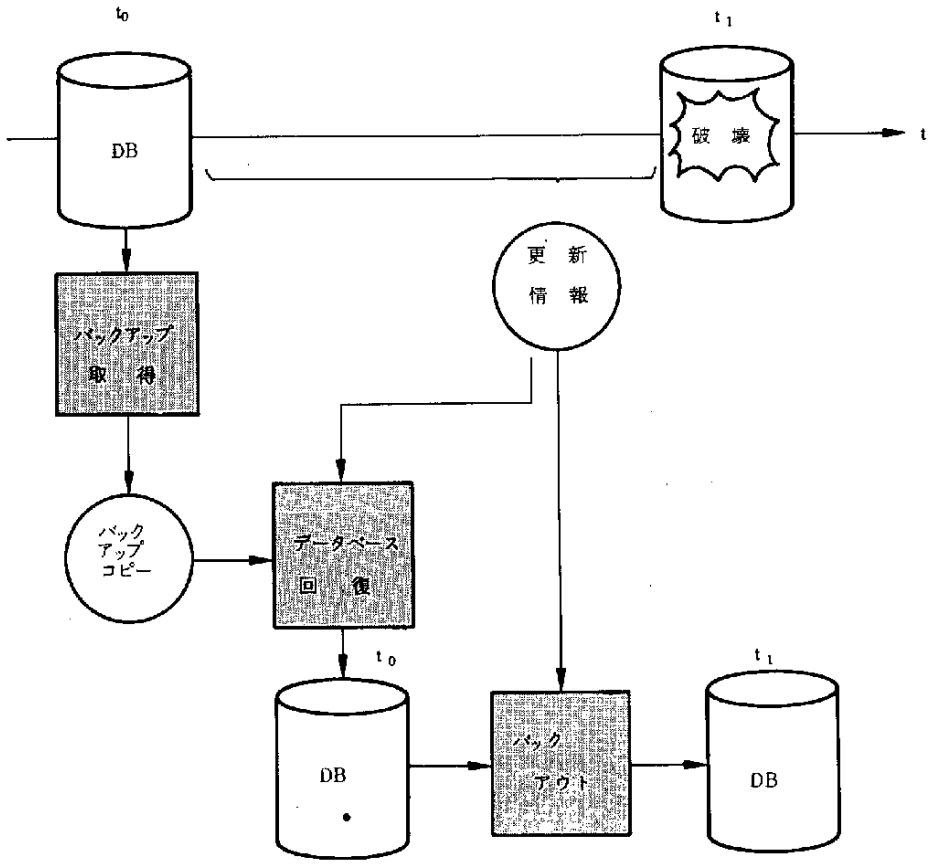


図２－１１　データベース（ＤＢ）の物理的破壊からの回復手順

(2)　２重化によるデータベース破壊からの保護

①　データベースの２重化

データベースのファイルを完全２重化することによって，障害時の破壊からデータベースを守る方法である。しかし，コストが掛るので重要なデータ・ファイル等に用いられる。

②　２重化データベースのバックアップ

２重化データベースの内容を，毎日全部ダンプする方法と，更新される毎の更新内容をダンプする方法の２通りあり，ダンプされた内容を使って，データベース・ファイルを回復させる。

2.3.4　将来のデータベース・セキュリティ

いろいろな情報処理アプリケーションが増えるにつれ，データベースの利用が急速に進み，データベースに関する需要や要求が新たに出てくる。これに伴なって，新技術が必要になり生まれてくる。

これからのアプリケーションである

① EFTS

② オフィス・オートメーション・システム

は，成長と共に新しい問題を起してくる。

現在，数字や文字等のコード化されたデータベースが主たるものであるが，これから問題を起こしそこなうものは，長い文章やグラフ，図，絵などのコード化されないデータのファイル，すなわち，イメージ・データベースがトラブルを起すと推定される。しかし，今この対策技術を開発するのは難しいし，時期早尚であるかもしれない。又，ネットワーク・システム，分散処理におけるデータベース・セキュリティやマルチ・プロセッサによるデータベース・アクセス等も，新たなセキュリティ問題を起すものと思われる。これらに対処するためには，ハードウェアの技術による他，適当なハイレベルのランゲージの開発も必要に迫られてくるものと思う。

新しい情報産業として，商業データベース産業が育ってくるが，商業データベースでも今迄にないセキュリティ上の問題が起ってくるものと思われる。

以上，イメージ・データベース，分散データベースおよび商業データベースの問題点について，簡単に述べたが，これらを実現するために解決すべき課題は多いと思われる。

2.4 通信ネットワーク

通信ネットワークのデータ保護について，最初に考えなければならないことは，バッチ・システムにおけるデータ保護とのちがいであろう。

もちろん通信ネットワークのデータ保護に使われる技術や手法は，バッチ・システムや比較的単純なオンライン・システムに使われるそれらの延長線上にあるとみられるが，しかしテーマを通信ネットワーク・システムとして広義にとらえた場合，地域的広がり，適用業務種別と利用者の多様性，そして介在する各種ノードや通信媒体の多様性や周囲セキュリティ環境のちがいなどの観点から，通信ネットワークのデータ保護はさらに多くの課題を包含することになる。

また，通信ネットワークのデータ保護には，一般にこれまでに使用された，利用者の識別，確認，承認と，追跡や記録の手法が利用されるが，処理ノードと通信ノードの分散化にともなって，新たにそれら手法の分散応用といった局面が発生する。

通信ネットワーク内を通るデータは，ネットワーク・システムに包含される適用業務に応じて，いろいろなデータが流れることになるが，総てのデータが機密性を有するものばかりでなく，金銭や取引に関するデータ，顧客や売上に関するデータ，人事や評価に関するデータなどに限られる。一般に広域ネットワークにおいては，今後のLAN（Local Area Network）や付加価値ネットワーク・サービスも含めて，各種通信媒体を使用することになり，当然公衆電気通信網や衛星通信サービスも含むことになる。

公衆電気通信網の目的は，不特定多数の利用者が自由に各種情報を伝達するために利用するためのものであるところから，共通のインタフェース条件で最少必要限の約束事にしたがって通信できることが要求される。したがって，利用者にとっては電気信号の伝達は本来トランスペアレントなものであり，伝達情報内容の機密保護は最終的に利用者側で実施すべき事柄となる。必要に応じて，暗号化技術やメッセージ認証，相手確認と承認の手順やソフトウェア手法，

それに漏洩や侵害の防止策を講じなければならない。

何にも増して重要なことは，端末装置やパーソナル・コンピュータの広範囲の普及とオンライン利用にともなって，エンド・ユーザのデータ保護教育のより一層の実施と徹底を図ることであり，また通信ネットワークのデータ保護上の問題をよく把握して有効な対策手段を確立することである。

2.4.1　通信ネットワークにおけるデータ保護の考え方

通信ネットワークのデータ保護について，バッチ・システムとの差異を挙げると次のようになる。

- 利用者が遠隔地に分散している。
- 利用者数が多数，端末機の共同使用。
- 保護環境がコンピュータ室程完備していない。
- 現場の利用者（エンド・ユーザ）にはいろいろな人々がいる。
- 利用者の職務分担は必ずしも明確ではない。複数システムへの端末アクセス。
- 利用者はコンピュータ知識やデータ保護知識を十分に持っているとは言えない。
- 通信ネットワーク・システムには，各種，複数の処理ノード，通信ノード，通信媒体が介在する。
- 利用者は，単独で仕事をする場合がある。
- 分散システムにおいては，ローカルの適用業務プログラムを内蔵する処理装置がある。

以上述べたように，通信ネットワークにおけるデータ保護は，バッチ・システムにおけるデータ保護の考え方といろいろな点で異なった特徴と性質をもっている。一般にコンピュータ室とそれに付随するライブラリなどは，要員の室への入退出はもちろん，地震対策などの物理面の対策も含めて，管理手続面や保護環境の点で，ととのっている。また要員はコンピュータに関する教育や訓

練の面でいわゆるエンド・ユーザとはちがった専門的なものを持っており，また職務分担も比較的はっきりしているために相互牽制の機能が作用する。しかしエンド・ユーザの作業環境はセンタから離れており，保護環境が十分でないと同時に，利用者はその上司も含めて十分なデータ保護知識を持っていないのが実状である。したがって，このような状況を考えるならば，エンド・ユーザにコンピュータ室の要員と同じ程度の保護意識を期待し，同様の対策をほどこすことは避けるべきである。通信ネットワーク・システムのかなりの部分はデータ保護面から手薄であり，偶発的または意図的な侵害に対しては弱点を持っているとみるべきであろう。

2.4.2 通信ネットワークのデータ保護対策

通信ネットワーク・システムにおけるデータ保護対策は，オンライン・システムのために考案され使用されてきた対策と基本的には同じであり，それら対策の延長線上にある。

通信ネットワークを通して結合された処理能力やデータベースへのアクセスは，端末機使用者の識別（Identification），確認（Authentication），および確認（Authorization）の手続を通して行なわれる。識別は利用者を文字どおり識別するための手順であって，氏名や従業員番号などで，内容は秘密ではない。これに対して，確認は本人が本人であることの証明を求める手順であり，本人の身体的特徴（例えば，指紋とか声紋など）や本人だけが知っているコード（パスワードとかロックワード[*1]）または暗証番号とか，本人だけが持っているもの（磁気バッチなど）により本人であることを証明する。一般に，パスワードやロックワードは，必要に応じて数週間か数ケ月で更新するのがよい。

＊1：ロックワードは，利用者が作成する合言葉で，リソースと関連付けられている。同一の合言葉と合致した場合に，そのリソースのアクセスまたは利用が可能になる。

パスワードは，本人を確認して許可を与えるのに対し，ロックワードは，利用者が主体的にリソースに鍵をかける意味合いがある。ただし，パスワードとロックワードとは，同意語に使われることが多い。

パスワードの更新に際して他人にそれが漏れることのないよう，通知には細心の注意が必要である。また他人にパスワードが漏れたとみられる場合には，遅滞なくパスワードの更新がいつでもできるようなシステムでなければならない。本人の確認がされたならば，次は利用者に許されたオペレーションの承認を行なうことである。通常，機密性の高い又は改ざんなどに対して保護を必要とするデータやプログラムについては，利用者の実施できるオペレーションを限定して利用者の権限を制限する。このため利用者の権限を登録したユーザ・プロファイルをシステム内に備えておき，システム利用に際して重要データやプログラムへのアクセスは，権限プロファイルを参照して，使用承認が行なわれる。

重要データやプログラムへのアクセスは，利用者別に操作時間と端末番号，操作種別を記録（ロギング／ジャーナリング）しておき，たび重なる不当なアクセスの試みに対しては追跡できる手がかりを得ることができる。

また，本格的なアクセス制御用ソフトウェアを使用しない場合でも，共通なデータベースへのアクセスにおいて，重要部分のデータ読出しや書換えについては，パスワードとコマンドを組合せて，承認と記録を行なうことがある。

反復的なエラーや不当とみられるアクセスの試みに対しては，強制的に端末機の操作をロックする方法があり，端末使用の凍結解除はデータ保護責任者の介入のみによって行なうことにしてもよい。

機密データの取扱いについては，操作可能な端末機の場所を限定しておき，指定された時間にのみに操作を制限することができる。ある利用者がシステムへのログオンを行なったのち，それをログオフすること無しに席を離れることは，端末の悪用に対してチャンスを与えることになり危険である。利用者が保持する磁気バッチを挿入する特殊機器を端末機に付加し，席を離れて他の場所に行く場合は，セキュリティ・エリアへの入室もその磁気バッチで制御して，離席中の端末機操作をロックする方法を採用しているケースがある。

2.4.3　データ保護に関するポリシー

上記のような通信ネットワーク・システムにおけるデータ保護対策を実施した場合に，その根幹となるのは，ネットワーク・システムを利用する企業なり団体のデータ保護上のポリシー決定である。

例えば，技術的に高度なデータ保護対策を実施したとしても，違反行為に対してどのような通報，処置，追跡を行なうかは，マネージメントの意志決定による。

また利用者申請と権限登録の手続の明確化を図るとともに，人事移動などにより利用者がその任を解かれた場合には，たゞちに登録を変更する等の手続が規定にしたがって行なわなければならない。

こゝで重要になるのは，情報処理にかゝわる資源（この場合は特に機密データやプログラム）の所有者制（オーナーシップ）を明確にして，資源の管理責任を持たせるとともに，利用者への使用権限付与の許諾・選択を実施する組織体制の確立である。

また，データ保護対策も含めて高度の技術を駆使したシステムを構築したとしても，要員やオペレータの職務分担をあいまいにし，例えば，プログラマに重要データへのアクセスを許すなどの慣習が残されている場合には，データ侵害の危険性をはらむことになる。

2.4.4　分散処理システムにおけるデータ保護対策

分散処理システムが通信ネットワークを通して結合されている場合は，技術的に複雑であり遠隔地に散在するシステムの状況を把握することは難かしくなる。しかし分散処理システムに対しては，これまでいろいろなデータ保護のための有効な手段が考案され使用されてきている。

複数の分散処理システムを各地に配置して同じ適用業務処理をそれぞれの場所でする場合，最初はシステム開発の目的で1台導入し，テストの後台数を増やすことは一般に採用されている方法である。このような場合，センタでプ

ログラム開発を行ない，アッセンブルされたシステム・プログラムを通信回線を通して遠隔地の分散処理システムにロードするか，またはディスケットにプログラムをコピーして書込み，それを分散処理システムに投入する方法が用いられる。

分散処理システム内の固定型ディスクの接続プラグ部分への物理的なアクセスは必要によりキーロックして不当な介入を許さないようにしている。

一般に，最近の大型コンピュータもそうであるように，分散処理システムでは，スイッチや調節ボタンの類は，装置から無くなりつゝあり，外部から自動的に起動や操作ができない形になっている。数少ないスイッチに対してもキーロックがほどこされ，キーを差し込まないとＩＰＬやシステムの切換えができない。キーロックの設定位置により，電源のオン／オフのみが一般の利用者に許されるようにすることができる。

またシステム・プログラムへの介入や変更は容易にできないようになっているが，必要によりプログラムが修正，変更された場合には，各モジュールに付けられている無変更の印としてのインジケータがアッセンブラ・プログラム・エディタの働きによってリセットされる。さらにリスト・モジュール・コマンドを使うことによって，修正，変更された総てのモジュールを簡単に識別できるので，プログラムが変更されたかどうかはチェックすることができる。

多くの場合，ＩＰＬや装置の初期設定は内蔵されたプログラムにより行なわれるが，手動で，それらを実行したときには，そのことを示す印が内部的に記録される。

分散処理システムの監査のためには，これまで各種の機能が開発されている。センタのホスト内のプログラムにより，遠隔地にどのような適用業務プログラムとデータが存在するかについて，広くリストを収集することができるし，また監査用のプログラムを通信回線を通して分散処理装置にロードすることができる。さらにホスト内の別のプログラムにより，ホスト側に居ながら遠隔地の分散処理システムにサイン・オンして監査プログラムで分散処理システムの適

用業務プログラムをチェックすることができる。

またこれとは反対に，ホスト内のプログラムにより，遠隔地の分散処理装置内の適用業務プログラムをホスト側に吸い上げ，オリジナルの適用業務プログラムと内容を比較検証することができる。

分散・遠隔地でデータ保護上手薄になるのは装置設置場所へのアクセス制御である。大型情報処理システムとちがって，分散処理システムは事務所や現場の一角に置かれることが多いために，入退室の管理は行なわれていない。データ処理の担当者も多くはなく，したがって職務分担も明確ではなく，磁気媒体やライブラリそれに入出力管理のための専任者や機械稼動のスケジュール監視者は通常配置されていない。さらに機械操作の習熟度もセンタ・システムのオペレータ程高くはない。

したがって，上記のように分散処理システムでは，利用者兼オペレータの介入操作が少くてすむようにスイッチ類を省略し，操作を自動化するとともに，操作コンソールも備えないようにしている。またホストとの連携により，ネットワーク制御とともに，監視やシステム監査が容易に行なえるよう，各種の機能が整備されてきている。

もちろん分散処理システムに結合された端末装置は，通信ネットワークを通して，複数の情報処理資源にアクセスすることができる。この場合，各利用者は重要データやプログラムの使用については，オンラインでのデータ保護の基本である識別，確認，承認の手順を通してアクセスが許される。

2.4.5　通信媒体

通信ネットワークには複数，多種類の通信回線が目的に応じて使われる。この中には従来の電話型アナログ回線から，電話型デジタル回線，さらに新しいパケット交換や回線交換デジタル回線，それに将来のLAN，衛星通信回線，VAN，光ファイバなどがあり，その種類は豊富である。特定回線や私設回線（構内）ではデータ保護対策は比較的容易であるが，公衆交換網ではその広域

性や本来の目的からデータ保護上考慮すべき点は多い。

通信回線上の機密保護で有効な手段は，暗号化であるが，実際に盗聴による問題が発生するケースは諸外国の例も含めてそれ程多くない実情からすれば，単なる通信リンク上の機密保護ばかりでなく，データベースと端末機との間のいわゆるエンド・ツー・エンドの暗号化による機密保護を指向することがより効果的であろう。それと同時に，データベース内の重要データの暗号化記録とともに，可搬型磁気媒体の内容の機密保護をも包含した暗号化が理想的である。

最近の暗号化の研究は，暗号アルゴリズムにもとづくメッセージ認証の方向に向けられており，これは特に金融機関などにおける情報伝達に有効に使われることになろう。

暗号化による効用は単に盗聴防止のみならず，いたずら通信を排除できる点にある。パケット交換は，中途の中継ノードにおける盗聴は多ルート伝送のため実行不可能であるとしても，相手先アドレスを知っているときはそこへ向けていたずら通信を発信することは起こり得ることである。クローズ・ユーザ・グループの機能を使えばそのような妨害は防ぐことができるが，そうでない場合は米国における学生によるいたずらと同様な問題が発生しないとも限らない。特にパソコンの機能強化と普及にともなって，そのような危険性は増大する。またパケット交換の加入者線でデータを捕捉された場合は，いぜんとして盗聴の危険性は残る。パケット交換のメッセージ形式から，データ・テキストのみを暗号化する方法は未だ日本において開発されていないが将来必要とされるであろう。

衛星通信については，我国においても実用化が近いものと思われる。米国における実際例においては，衛星通信には音声・データ・画像のいろいろなデジタル化信号が多重化して混在しているために，自然的にスクランブルされており，通常は容易に盗聴ができないようになっている。また，米国連邦通信委員会（FCC）の規定によりトランス・ポンダとの間のバルク・キャリヤはグループ・エンクリプションされている。さらに各ユーザには個有のアドレスが暗号

化された形で割当てられているため，当事者間以外には誰の通信か分からないようにしている。しかし，それでも不安な場合には，暗号装置をユーザ側で設置して通信内容を秘守すればよい。

2.4.6 ま と め

広域通信ネットワークにおいては，バッチ・システムや従来のオンライン・システムに比較して，データ保護上いろいろなちがった局面を持っている。公衆電気通信網の本来の目的がそうであるように，通信ネットワーク・システムが広域化し多目的に使用されるようになると，通信網自体に過大なデータ保護上の期待を持つことは無理となる。

やはり，データ保護の最終的な責任はユーザ側にあるのであるから，目的と必要に応じてネットワーク・システムの特性に照らして有効な防御策をユーザ側が組み入れなければならない。

また複数通信ノードのネットワーク・システムにおいて，一部のノードには万全のセキュリティ対策をほどこしても，一部のノードに手薄な状態が残されている場合は，全体としてのセキュリティ対策は弱いものとなる。多種のデータが機密性の高いものも含めて，ノードを通過する際に，横どりされたり，侵害されたりする危険性があるからである。

2.5 暗号化技術

従来，暗号は政府の軍事，外交上の秘密通信が主であった。しかし，最近はデータ通信が企業活動や国民生活に大きな役割を果たし，そのネットワーク化が急速に発展している。それに伴って各種の犯罪や事故が発生し社会に及ぼす影響は極めて大きい。そこで秘密データを暗号化することはシステムのセキュリティを確保する上で有効な手段である。今後更に分散データ処理やデータベースにおけるデータ保護，衛星通信による秘密データの保護，EFTS（Electronic Funds Transfer System）や電子郵便の保護など暗号化の必要な分野が広がってきている。

このような状況によりアメリカでは標準暗号としてDES（Data Encryption Standard）が公表され実用化が進んでいる。又，一方では新しい暗号系である公開鍵暗号系の概念が発表され実現に向けて研究開発が行なわれている。この公開鍵暗号系では鍵の秘密配送の必要がなくその管理が容易になる。更に，通信相手の認証となるディジタル署名が簡単であるなどの大きな利点を備えている。

2.5.1 古典的な暗号

最も古典的な暗号としてシーザ暗号がある。これは例えば「DOG」を「GRJ」というようにA，B，……，Zの順序を3文字シフトして対応させる。後に，K文字シフトと一般化されたが，鍵Kは26通りしかないのですぐ解読されてしまう。そこで，シフトではなく平文の英文字に任意の置換を行なう単文字換字式暗号が考えられた。鍵の数は$26! \approx 4 \times 10^{26}$となり全数検査による解読は不可能である。しかし，言語の文字出現率の不均一性が残るので文字使用頻度の統計的性質により解読できる。

次に，転置式暗号は平文をn文字のブロックにくぎり，n！通りの順列を鍵としてブロックの中の文字を並べ換えるものである。この方法も文字出現率の不均一性を残すが，単文字換字式暗号と異なり言語の高次の統計的性質を崩す。

文字出現率の不均一性を残さないために多表式暗号が考えられた。これはn個の換字を周期的に用いるもので鍵の数は一般的に$(26!)^n$となる。単純な多表式暗号としてビジネル暗号があり，これは前述したシフト暗号のシフト量を周期的に変えるもので周期nのビジネル暗号の鍵は26^n通りとなる。このnをn→∞とした時，即ち，周期を通信文の長さと同じにした時バーナム暗号の使い捨て乱数表が得られ，鍵がわからない限り暗号の解読は原理的に不可能である。ワシントン・モスクワ間のホットラインはこの使い捨て乱数表を使っているという。しかし，平文と同じ長さの鍵を予め通信相手に配送しておかなければならないので，この方法が有効なのは特殊な場合のみである。

これらの暗号は実用的なnを考慮すると単体では安全性に問題があるが，それらを組み合わせ繰り返すことにより暗号強度を増すことができる。そのような合成暗号は換字や転置のような基本的な方式を用いてDESのような複雑な暗号を構成することができる。

2.5.2　暗号方式の現状

暗号系は慣用暗号系と公開鍵暗号系に分類される。慣用暗号系は従来からの暗号系で暗号鍵と復号鍵が同一であり，各送受信者間で共通の鍵を個々に持たなければならない。それに対して公開鍵暗号系は暗号鍵と復号鍵が異なり，暗号鍵を公開することができ鍵を秘密配送する必要がない。又，両暗号系の欠点を補うために両者を組み合わせた暗号方式も考えられている。以下にその概要を示す。

(1)　慣用暗号系

代表的な慣用暗号系としてDESを取り上げる。DESは1977年にアメリカの商務省標準局が公表したもので実質的にアメリカの標準暗号となっている。

DESは64ビットのデータ・ブロックを64ビットの鍵の下に暗号化，復号化する。但し，鍵64ビットのうち8ビットはパリティで実質的な鍵は2^{56}

≈１０^{16}通りである。暗号アルゴリズムを図２－１２に示す。基本的には転置と換字を高度に組み合わせたものであり，機能的に同一な反復を１６段行なっている。この反復はｎ段目でのブロックの左３２ビットをLn，右３２ビットをRnとして次のように表わされる。

$$\begin{cases} Ln = Rn-1 \\ Rn = Ln-1 \oplus f(Rn-1, Kn) \end{cases} \qquad (1 \leqq n \leqq 16)$$

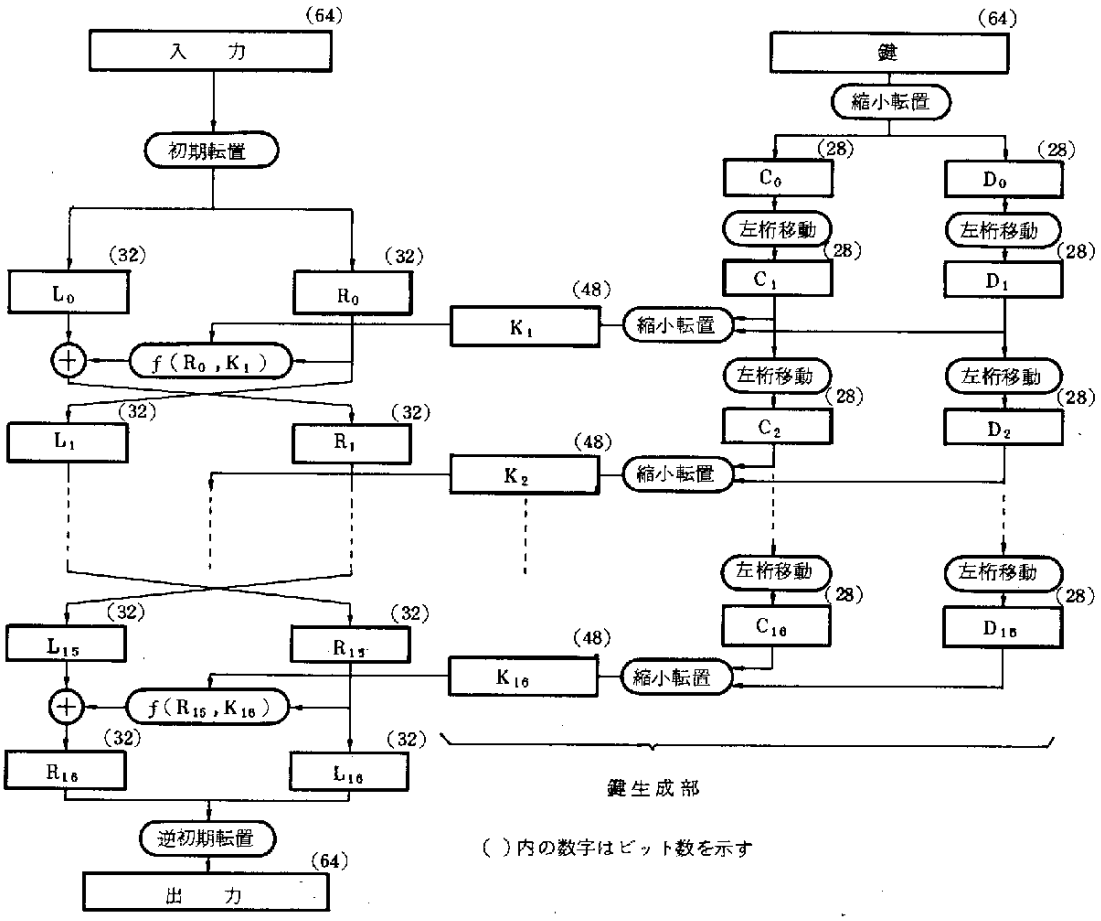


図２－１２　　ＤＥＳアルゴリズム

ここで，Knは各段での鍵で鍵生成部から送られてくる。$f(Rn-1, Kn)$は暗号関数でその内容を図２－１３に示す。この暗号関数の中にＤＥＳの核となるＳ－boxがあり，ＤＥＳの強さもここにある。これは４８ビットを８個の６ビ

ットのブロック $S_1 \sim S_8$ に分割し，換字表を用いて４ビットずつのブロックを出力するもので逆変換が不可能となっている。

DESの基本的な利用形態としては図２－１４に示す３種類がある。①は同

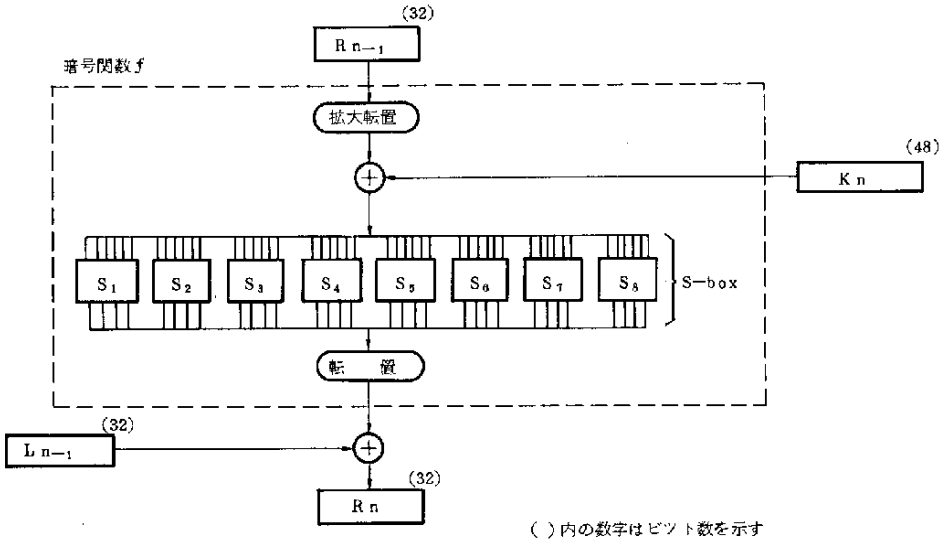


図２－１３　暗号関数 $f(Rn-1, Kn)$

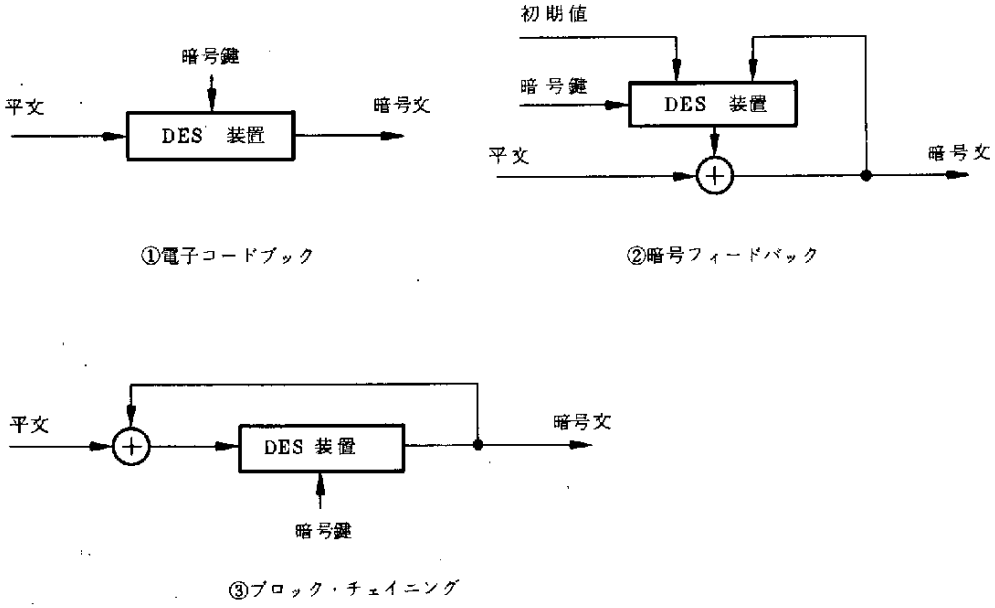


図２－１４　　DESの利用形態

じ暗号鍵の下では，同一の平文ブロックは同一の暗号ブロックに変換されるので，長文の暗号化には適さない。②，③は暗号ブロックを再び入力側に戻すので長文に対する暗号強度が高い。

(2) 公開鍵暗号系

公開鍵暗号系の概念は１９７６年に発表された。これは慣用暗号系と違って暗号鍵と復号鍵が異なり，暗号鍵から復号鍵を求めることができない。従って，暗号鍵を公開することができるため，慣用暗号系で問題となる鍵の秘密配送を行なう必要がない。公開鍵暗号系の実現には暗号鍵から復号鍵を割り出せないようにするために一方向性関数を用いる。その実現法として，ここではRSA法とMH法を取り上げる。

① RSA法（Rivest-Shamir-Adlemanの方法）

RSA法は１９７７年にリベスト（Rivest），シャーミル（Shamir），アドルマン（Adleman）によって発表された。これは一方向性関数として大きな数の素因数分解を利用している。暗号化，復号化は平文をM，暗号文をCとすると次のように表わされる。

$$\begin{cases} \text{暗号化} : C \equiv M^{e} \pmod{n} \\ \text{復号化} : M \equiv C^{d} \pmod{n} \end{cases}$$

ここで，暗号鍵は（ e， n ）であり公開される。復号鍵は（ d， n ）であり秘密に管理する。nは素数p，qの積で与えられる。即ち，

$$n = p \cdot q$$

これが実質的に一方向性関数となりp，qは秘密である。dとしては，（ p－１ ）・（ q－１ ）と互いに素な任意の整数を選ぶ。つまり，

$$\gcd\{d, (p-1)\cdot(q-1)\} = 1$$

eは次のように定める。

$$e \cdot d \equiv 1 \{\bmod (p-1)\cdot(q-1)\}$$

② MH法（Merkle-Hellmanの方法）

MH法は公開鍵暗号系の概念を提案したヘルマン（Hellman）らによって

発表された。これはナップザック問題という一方向性関数を用いる。平文は2進のn次元ベクトルM＝（m_1，m_2，……;m_n）であり，暗号鍵はn次元の落し戸ナップザック・ベクトルA＝（a_1，a_2，……，a_n）である。a_iは正の整数であり，暗号化は次のようになる。

$$c = \sum_{i=1}^{n} a_i \cdot m_i$$

暗号文Cはcを2進数で表わしたものである。復号化は秘密の復号鍵により簡単に解ける特殊なナップザック問題に変換して行なわれる。

(3) 慣用暗号系と公開鍵暗号系の併用

慣用暗号系と公開鍵暗号系の欠点を補うために両者を併用した暗号方式が考えられている。郵政省はMIX方式として提案している。これは通常のデータの暗号化，復号化は処理速度の速い慣用暗号系で行ない，それに必要な鍵の配送は公開鍵暗号系を用いて行なう方式である。暗号アルゴリズムは慣用暗号系にDES，公開鍵暗号系にRSA法を使用している。但し，MIX方式はホスト・ホスト間の通信の場合であり，ホスト・端末間ではRSAアルゴリズムのオーバヘッドが大きいのでDESを推薦している。この暗号システムはエンド・ツー・エンド方式によるソフトウェアで実現しているため通信だけでなくファイル・データの暗号化への拡張も可能である。

2.5.3 暗号の適用

(1) 通信保護

通信データが回線上で盗聴されてもそのデータが暗号化されていれば解読しない限りデータの内容を知ることも有効な変更を加えることもできない。特に，電波通信による機密データの保護に対しては暗号化が唯一の手段である。

ネットワーク・アーキテクチャにおける暗号化を考えると通信プロトコルのどの階層レベルで暗号化を行なうかの問題がある。例としてISO（International Organization for Standardization）の7階層構成ではまず物理層

またはデータリンク層での暗号化が考えられ，これはリンク・バイ・リンクの暗号化である。又，トランスポート層あるいはプレゼンテーション層での暗号化も考えられエンド・ツー・エンドの暗号化ができる。

通信保護の実現手法としてＩBM社によるホスト・端末間通信の例を取り上げる。暗号方式にDESを採用しているのでホストと端末で同じデータ暗号化鍵KS（セッション鍵）を共有しなければならない。このKSは鍵暗号化鍵KMT（端末マスタ鍵）で暗号化して配送される。但し，KMTはシステム導入時にホストと端末の両方にセットしておく必要がある。通信要求があるとまずホストで疑似乱数RNを発生し，RNをマスタ鍵で暗号化されたKSであると見なす。これは裸のKSを見せないためである。RNを暗号機構の中でKSをKMTで暗号化したものに変換し端末へ配送する。それを端末は自己のKMTで復号しＫＳを得る。こうして鍵がホストから端末へ配送され暗号通信が行なわれる。

(2) ファイル保護

ファイルに蓄積されているデータを不当な利用者に知られてもそのデータが暗号化されていれば内容を理解することができない。ＴＳＳにおける利用者ファイルや機密情報ファイルなどの保護に適用される。

ファイル保護の場合，通信と異なりホストからファイルへ送った暗号はファイル・デバイス側で復号する必要はなく，鍵の配送の必要がない。従って，公開鍵暗号系における鍵配送の利点は役立たず，ファイル保護そのものに対する公開鍵暗号系の適用は無意味である。

また，通信保護と異なりファイル・データの保護期間が長く，その間暗号化されたファイル・データの復号鍵を保持しなければならない。ＩBM社によるファイル保護においては各ファイルごとに固有の鍵暗号化鍵KNFを用意し，ファイル・データを暗号化する鍵ＫＦ（ファイル鍵）はそのKNFで暗号化され，それをファイルのヘッダに書き込むようにしている。これによりホストはKFを保護する必要がなくなる。

(3) ディジタル署名

通信においてその相手が正当であることを判断し，送受信の事実を確認できる認証方法がなければならないことは重要である。そこでメッセージの認証であるディジタル署名が考えられている。電子郵便やEFTS などの新しいデータ通信でも署名が望まれる。このディジタル署名は慣用暗号系での実現は難しいが，公開鍵暗号系では容易に実現できると考えられる。その実現方法を次に述べる。

まず，送信者Aは秘密の復号鍵D_Aで平文Mを復号変換する。それを更に，公開されている受信者Bの暗号鍵E_Bで暗号化する。こうして得られた暗号文$C = E_B\{D_A(M)\}$をBへ送る。受信者Bは自分の秘密の復号鍵D_Bで暗号文Cを復号化し$D_A(M)$を得る。更に，公開されているAの暗号鍵を用いれば平文Mが得られる。以上の過程を式で表わせば次のようになる。

送信者A：$C = E_B\{D_A(M)\}$

受信者B：$E_A\{D_B(C)\} = E_AD_BE_BD_A(M)$

$= E_A\{D_A(M)\}$

$= M$

この過程において暗号文CはD_Bを知らないと解読できないのでこれを復号できるのは正当な受信者Bのみである。又，$D_A(M)$を作れるのは秘密の鍵D_Aを持っている送信者Aのみなので送信者がAであるかどうか判断できる。即ち，受信者Bは$D_A(M)$によりD_Aを持っているAを認知できる。しかし，一方向性関数によりE_AがわかっていてもD_Aを知ることはできない。これが，認知はできるが他人には書けない署名の作用に相当する。

2.5.4 暗号方式の評価

(1) 安全性

暗号の安全性には無条件的安全性と計算的安全性がある。前者は原理的に解読不可能なもので2.5.1で述べた一回使い捨て乱数表方式がある。しかし，

その乱数表の頻繁な秘密交換という大きな問題があり暗号方式として一般的でない。後者は，理論的には解読できるがそのために必要な計算処理時間が実用的でない程長大なものである。現代の実用的な暗号はすべてこれに頼っている。

商業用の最近の暗号はその秘密を鍵だけに頼り，暗号アルゴリズムは公開するのが一般的である。DESの場合，鍵の長さは実質的に56ビットであるから検査を2^{56}回行なえば鍵を割り出すことができる。一つの鍵の検査に1μsかかるとすると約2,000年かかる。しかし，そのようなチップを10^6個用いて並列処理を行なえばわずか1日で鍵が求められる。現在の技術ではそれは不可能であるが，計算的安全性による暗号方式は質的に絶対的な安全性を持っているわけではなく，鍵の大きさとコンピュータの能力の競争の上に成り立っている。

しかし，計算的安全性の前に暗号アルゴリズムの安全性は絶対でなければならない。例えば，RSA法の場合nを10進200桁とし,知られている最も速い方法で素因数分解しても3×10^9年以上かかる。しかし，これは素因数分解の有効なアルゴリズムが現在見つかっていないからであって，今後それが発見されればRSA法の安全性はなくなる。また，MH法の場合も一般的なナップザック問題ではなく，簡単なナップザック問題に変換できる特殊なものであり，そこに解読の可能性があるかもしれない。DESにおいても暗号の核となるS-boxの設計思想に論議があるがこれも安全なものでなければならない。

(2) 鍵の配送，管理

最近の暗号の安全性は鍵のみに依存し，暗号の運用では鍵の生成，保管，配送などの操作が多いので鍵の管理が暗号システムを考える上で重要な問題となってきた。

公開鍵暗号系の場合，各ユーザの暗号鍵は公開できるので鍵を秘密に配送する必要がなく，自分の復号鍵のみを秘密に管理しておけばよい。それに対

して慣用暗号系の場合，送受信者間で共通の鍵を持たなければならないので鍵を通信相手に秘密配送する必要がある。また，通信相手ごとに別々の鍵を用意しなければならないので鍵の数が増え，鍵の管理上に大きな問題がある。

そこでＩＢＭはＤＥＳの鍵管理に階層方式を採用している。これは鍵の役割に応じて鍵を階層化し，上位の鍵で下位の鍵を暗号化する。その頂点に立つマスタ鍵だけ暗号化されていなく，管理者はマスタ鍵のみを厳重に守ればよい。暗号の主な操作は暗号機構の中で行なわれ，マスタ鍵はこの中にセットされている。ユーザは暗号機構の中を見ることができず，暗号機構の外では鍵はすべて暗号化されている。

ＤＥＳの鍵配送問題の対処として公開鍵配送方式が考えられている。これは自分の秘密の鍵と相手の公開鍵をつなぎ合わせてＤＥＳに必要な鍵を共有するものであり，次に示す一方向性関数を用いる。

$$Y \equiv \alpha^{X} \pmod{n} \qquad (1 \leqq X \leqq n-1,\ n：素数)$$

各ユーザはＸを任意に選び秘密にし，Ｙを求めて公開する。ユーザＡは自分の秘密鍵X_Aと公開されているユーザＢの鍵Y_Bより

$$K_{AB} \equiv Y_B{}^{X_A} \equiv \alpha^{X_A X_B} \pmod{n}$$

を求める。一方，ユーザＢも同様にして

$$K_{AB} \equiv Y_A{}^{X_B} \equiv \alpha^{X_A X_B} \pmod{n}$$

が得られる。このようにしてユーザＡとＢは共通の秘密鍵K_{AB}を持つことができる。

(3) スループット

暗号化によるスループットの低下はシステム運用の上で重要な要因である。ＲＳＡ法は計算が複雑であり，ＤＥＳに比べて計算処理時間がかなりかかる。処理速度を比較してみると現状のハードウェアではＤＥＳが約１０Ｍｂ／ｓであるのに対してＲＳＡ法は最大で５０Ｋｂ／ｓであるから数百倍の差が生じている。

公開鍵暗号系の実現法としてＲＳＡ法が現状では有力であるが，スループッ

トの問題が最も大きく，処理速度の速いＬＳＩの開発が行なわれている段階である。従って，現状でRSA法を通常のデータの暗号化に用いると問題があるが，ＭＩＸ方式のようにその使い方を限定すると有効なシステムを設計することができる。

しかし，スループットの高い実現法が他に見つかれば公開鍵暗号系のみで暗号システムを構成できるわけであり，そういう意味でまだ最適な公開鍵暗号系の実現法が確立しているわけではない。従って，処理時間の短いもっと簡単な一方向性関数の適用が望まれる。

(4) 実用難易度

ＤＥＳの場合はハードウェアで簡単に実現でき，既にＬＳＩ化され各メーカから種々のチップ，暗号装置が商品化されている。また，ソフトウェアで実現しファイル・データ保護への適用もできる。但し，鍵配送の問題とディジタル署名が困難であるという問題がある。

RSA法の場合はまだ研究開発の段階であり実用化には多くの問題点が残されている。特にスループットの問題が大きい。また，鍵の長さもまだ決まってなく，リベストらはｎは１０進２００桁（６６５ビット）にすることを推奨している。しかし，そのように大きな素数の選択をどのようにするかなどの問題もある。更に，公開鍵暗号系は通信には有効であるがファイル保護そのものに対しては利点がないのも問題である。

2.5.5 暗号ＬＳＩと暗号装置

(1) 暗号ＬＳＩ

ＤＥＳの暗号ＬＳＩは表２－２に示すように各種販売されている。その中で特にAm９５１８は１０Mb／s以上の処理速度を持ち，通信だけでなくディスクのDMA転送にも対応できる。また，暗号通信でも３種類のモードが可能で用途に応じた適用ができる。

公開鍵暗号系のRSA法を実現するハードウェアとしてはリベストが1.2Kb

／sのLSIを試作し，HP(Hewlett Packard)社は10Kb／sを軍用に開発中という。また，日本電信電話公社の横須賀電気通信研究所ではROMを利用した多チップ構成により50Kb／sの処理速度を持つという。

表2－2　DESの暗号LSI

LSI名	メーカ名	処理速度(Kb/s)	暗号モード	ピン数	備考
i8294	インテル	0.64	ECB	40	
WD2001	ウェスタンディジタル	1300	ECB	28	1ポート
WD2002	〃	〃	〃	40	2ポート
MC6859	モトローラ	400	—	24	
9414－1～4	フェアチャイルド	—	—	40×4	4個のLSIで構成
Am 9518	AMD	10400	ECB CFB CBC	40	
AmZ8068	〃	8000	〃	40	
TMS99541	TI	5.12 0.64	ECB CFB	40	発売予定

ECB：電子コードブック　（Electronic Codebook）
CFB：暗号フィードバック　（Cipher Feedback）
CBC：ブロック・チェイニング（Cipher Block Chaining）

(2) 暗号装置

暗号装置は通信回線内に配置されて伝送データの暗号化を行なう。DESを採用した暗号装置としてIBM社，モトローラ社，パラダイン社などの各メーカから販売されている。

IBM3845は鍵管理機能を持ち，最高データ伝送速度は19.2Kb／sとなっている。この装置は送信側から見てモデムの前に配置されリンク・バイ・リンクの通信に適用される。しかし，ファイルの暗号化はできない。そこで，IBMの暗号サブシステムではハードウェアとソフトウェアを組み合わせて通信保護とファイル保護の両方を可能にしている。ソフトウェアを援用することによりデータの機密の程度に合わせてデータを暗号化するかどうか

を切り分け合理的，効果的な暗号の運用ができる。

〔参考文献〕

1) Lempel, A., "Cryptology in Transition", Computing Surveys, Vol. 11, №4, pp. 285－304, (1979).〔西村和夫訳，"暗号学の変遷"，コンピュータ・サイエンス，bit別冊，pp.109－125,(1980).〕

2) 田中善一郎，"鍵なしではまず解けなくなった最近の暗号方式"，日経エレクトロニクス，9月4日号，pp. 68－103，(1978).

3) 山沢昌夫／秋山良太／田中正和，"暗号化技術の動向",ビジネス・コミュニケーション，Vol. 19, №7, pp. 35－39，(1982).

4) 赤木昭夫，"公衆暗号系とアルゴリズム基礎理論"，コンピュータ・サイエンス，bit，Vol. 10，№5，pp. 580－586.

5) 土居範久，"米国のデータ暗号化規格"，コンピュータ・サイエンス，bit，Vol. 13，№2，pp. 102－113.

6) 上園忠弘，"暗号化技術とその応用"，情報処理，Vol. 20，№9，pp. 785－792，(1979).

7) 村川勝彦，"データ通信の暗号化"，日経コンピュータ，11月1日号，pp. 111－118，(1982).

8) 田中善一郎，"コンピュータ犯罪に対する暗号の有効性を探る"，日経エレクトロニクス，10月11日号，pp. 118－136，(1982).

2.6　その他の関連技術

本章で既にとりあげた種々のセキュリティ関連技術に加え，ここではコンピュータ・システムのシステム監査を支援する技術的手法やツールについて述べる。併せて，現在市販されているセキュリティ関連ソフトウェアについても簡単に紹介する。

2.6.1　システム監査とセキュリティ

ここ数年来，システム監査の重要性に対する認識が高まり，日常業務として取り入れる企業も少しづつ増加してきた。

システム監査とは「監査対象から独立した客観的な立場で，コンピュータを中心とする情報処理システムを総合的に点検・評価し，関係者に助言・勧告することをいい，その有効利用の促進と弊害の除去とを同時に追求して，システムの健全化をはかるものである。」と定義されている。従って，コンピュータ・システムのセキュリティ対策がどのようになっているかは，重要なチェック項目である。すなわち，コンピュータ・システムに組み込まれたセキュリティ機構が充分な機能を有し，かつ，その機能が正当に運用されているか否かは，監査担当者によってチェックされなければならない。

システム監査では，システムの企画・設計・製造・運用のすべてのフェーズが対象となり，理想的には，監査担当者がシステム開発グループと一体となって企画段階から参加し，設計・製造の各段階におけるレビュー・チェックや，運用時のシステムの改造や更新のすべてのフェーズにおいても，その結果のチェックを行なうという全面的な介入が望ましいと言われている。

一方，このような細部にわたる監査の実施には，それを支援する手段が必要不可欠のものとなり，従来から幾種類かの技術的手法やシステム監査ツールと呼ばれるソフトウェアが存在していた。これらの技術的手法やツールには，

① コンピュータ・システムの正しさを検査するもの。

② コンピュータ・システムの運用状況の監視・記録あるいはその分析を

行なうもの。

③ 不正変更発見のためプログラムの比較検査を行なうもの。

などがある。システム監査とセキュリティ対策とは，自ら，その範囲も目的も異なるが，これらの技術的手法やツールはやや間接的ながら，コンピュータ・システムのセキュリティを向上させる機能の一種と考えることが出来よう。

以下に代表的な技術的手法やツールにつき，その概要を述べる。

2.6.2 システム監査を支援する技術的手法やツール

(1) コンピュータ・システムの正当さを検査する手法

システムの正しさとは信頼性の高さと同時に，目的に対する正当性の意味をも含む。

① ITF

ITF（Integrated Test Facility）は，名に示すとおり，対象とするコンピュータ・システムの正しさを総合的にテストするものである。この手法は，別名ミニ・カンパニと呼ばれることもある。これは処理対象の中に，架空の取引会社あるいは部門に相当するダミーを故意に挿入し，それに伴うトランザクションをシステムの正規のトランザクションと共に入力する。処理の実行によって，このダミー・トランザクションは他の正規のトランザクションと同等の資格で，対象アプリケーションの全ステップを通過して処理され，予め作成済みの結果と照合され，システムの正当性がテストされる。この手法は一般のテスト・データ法に比べ，ファイル機能やオンライン処理機能等を含むシステムの総合的なテストを可能とすると同時に，正規の処理の最中にテストを行なう事も可能となる。

一方，架空のマスタ・データやトランザクションが混入しているため，正規の経理記録や種々の統計記録等から，その影響を打ち消す手段を講じなければならないという問題がある。

② 平行シミュレーション法

これはテストすべき機能を実現し得るシミュレータを作成し，実際のデータによりシミュレーションを行ない，本物のプログラムによる結果と照合し，正否をテストするものである。即ち，①のＩＴＦとは逆に入力データはすべて本物であり，プログラムは模擬のものである。図２－15にITFと平行シミュレーションの概念図を示す。この方法はテスト・データの作成が不要になる反面，シミュレータの作成という新たな負担が発生することとなる。

しかしながら，このシミュレータはすべての処理内容を含む必要はなく，監査の対象としたい特殊な部分に的をしぼる事が可能である。例えば，給

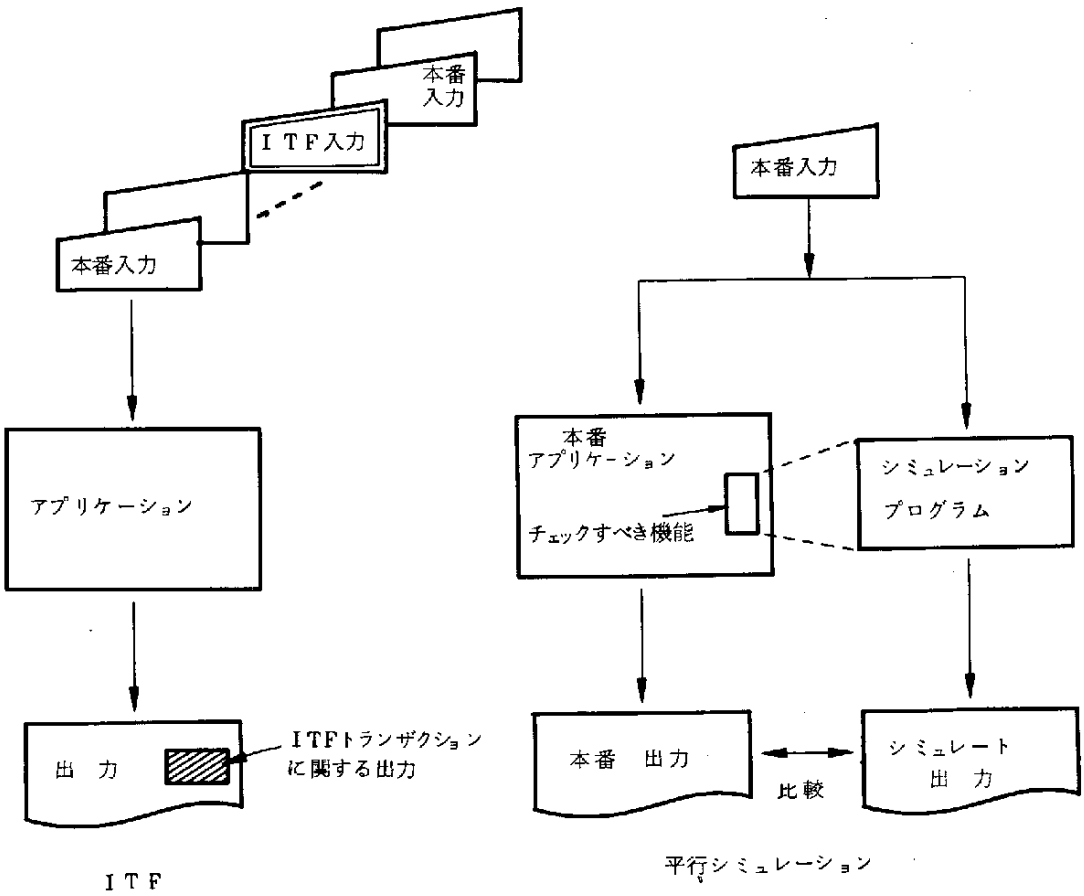


図２－１５　ＩＴＦと平行シミュレーション

与システムの税金計算のような重点的な部分に対し，本番のプログラム・ロジックに不正が施されていないかどうかをチェックするなどに有効である。

③ 基本ケース・システム評価法

基本ケース・システム評価法（Base case system evaluation）では，対象とするコンピュータ・システムのユーザ，監査担当者，開発部門がそのソフトウェアの設計時から協力して，適用アプリケーションの中で，特に監査上，留意すべき基本ケースを抽出し，その部分の処理プロセスに重点を置き，テスト・データを作成しテストする方法である。これは，テスト・データ法の一種であるが，ファイルやオンライン機能を含んだ，より包括的な重点的テストが可能であり，またシステムの変更時にも同様の協力体制で変更結果がチェックされる。

(2) 運用時の監視・記録・分析などを行なうツール

① ロギング機能

コンピュータ・システムの運用時に，使用されたファイル，プログラム，コマンド，メッセージなどが逐一記録され，誰が何時，どういう処理を行なったかが明確にトレース出来ることは，システム監査上極めて重要である。この場合，どの位詳細な記録がとれるかは，そのロギングに使用するファイル容量や処理時間との兼ね合いで制約が出ることとなるが，例えば，重要なファイルはファイル名だけでなく，読み出されたり，更新されたレコードやフィールドまで細かく記録されないと，監査の目的が充分達せられないというような事もある。

一方，このロギング情報をオペレータが勝手に変更してしまうという様なことが出来ては意味がない。通常のオペレーティング・システムには，コンピュータ使用料の計算処理のためにユーザ毎の課金情報をロギングする機能があり，またＩＢＭのＳＭＦ（System Management Facility）のように，システムの処理効率やオーバヘッドを検討する目的で運用状態の記

録をとる機能もあり，これらの機能を利用して，システム監査の目的に合わせたロギングを行なうことが多い。またSMFなどのロギング情報を分析し，見易いレポートに出力するレポート・ジェネレータもパッケージとして多数商品化されている。

② 違反チェック・ルーチン

コンピュータ運用時の例外事項やルールの違反事項等を監視し，その記録をとるものである。例えば，ログオン時のパスワードをチェックするルーチンや，端末入力データの妥当性をチェックするルーチンである。

これらは，ＯＳの機能としてシステムに組み込まれるものと，アプリケーション・プログラムに組み込まれるものに大別される。これらのルーチンで検出された違反に対する処置は，違反の状況により様々である。特に，アプリケーション・プログラムに組み込まれるルーチンは，ユーザが作成するので，極めてバラエティに富んだ処置がとられる。例えば，通常，違反処理は無効となるが，監査キーという特別の手段を用いることにより，違反処理を可能としたシステムがある。

検出した違反は，通常記録される。ＯＳの一部として動作するチェック・ルーチンは，記録もＯＳの持つロギング機能（SMF等）を使用する。一方，ユーザ作成のチェック・ルーチンでは，記録部分もユーザが作成することが多い。ユーザ側で，ＯＳの持つ記録機能を利用するのが一般的に難しいからである。これらの記録は，すべてシステム監査の重要なデータになる。そのため，近年のシステムでは，積極的にユーザ作成のチェック・ルーチン（記録機能を含む）が，アプリケーション・プログラムに組み込まれている。特に金融業のシステムで盛んである。

③ 組み込み監査用データ収集機能

これはアプリケーション・プログラム自身の中に，監査に有用な運用時の情報を収集する機能を組み込んだものである。この機能は，それぞれの目的にあった的確な監査情報をきめ細かくキャッチ出来るという点ですぐ

れた方法であり，オンライン・システムにも有効である。しかしながら，この様な機能を効果あらしめるためには，そのアプリケーション等の設計時点から，データ収集に対する綿密な計画や手段の検討が必要であり，監査担当者とシステム開発者との充分な協力体制が必要不可欠となる。また，実用上は運用後の新たな収集の要求に柔軟に対応出来るようパラメータ指定方式などにより，そのアプリケーション・システムの完成後も，任意のポイントでのデータ収集機能の組み込み（パラメータの変更程度の労力で）が可能になっていることが望ましい。また，収集したデータを後日分析・チェックするという利用方法のみならず，特別なケースでは，リアルタイムの情報表示等のアクションを取り得ることなども要求される。

(3) プログラム／ファイルの比較を行なうもの

コンピュータ・システムのプログラムの変更は，正しい変更手続きを経て，許された人間のみが行なうものである。また，システム監査の立場から言えば，変更の内容が正当であり，不正が行なわれなかったか否かを確認せねばならない。一方，正規の手続きによらぬ不当な変更や権限のないオペレータによる変更などは，原則的には前述の運用記録により，とらえられる筈であるが，監査担当者の立場からすれば，念のため特に重要なプログラムは，例えば，年に1回か2回，不当な変更が施されていないか否かを確かめることが要求される。

プログラムの比較には，マスタ・バージョンとカレント・バージョンとをモジュール毎に比較するという方法がとられる。この場合，ソース・コード・レベルの比較とオブジェクト・コード・レベルの比較とがある。通常の修正変更は，ソース・コードで行なわれるが，その比較のみではオブジェクト・レベルの不正変更は発見出来ない。いずれの場合も比較の結果，両者の差違が出力される。

なお，この比較ツールの応用として，プログラムではなく，データ・ファイルの比較も原理的には可能である。但し，その量からして実用性のない場

合もあろう。

以上，種々の技術的手法やツールの紹介を行なったが，現状ではその機能はまだ限られており，特にオンライン・システムや大規模なシステムには効果的適用が難しく，また使用法が面倒である。あるいは，本番システム運用への信頼性上・効率上の悪影響の恐れ等，種々の問題が多いとされている。また，有効な監査用データの把握のためには，数週間，あるいは数か月間等の長期間にわたるデータの時系列的変化をとらえる事も要求され，よりダイナミックな監査証跡（Audit Trail）を容易に追跡する機能が期待されている。一方，セキュリティの観点からすれば，システム監査ツール自体のセキュリティが問題となり，この様な機能が悪用されることによる脅威についても充分な検討を行ない，その監視と運用上の配慮が必要となろう。

2.6.3　商用ソフトウェアの例

セキュリティ関連の商用ソフトウェアは，ＩBM用のものを主体に１９７０年代から多種類のプログラムが市販されている。表２－３および表２－４にその例を示す。なお，この表はＩCP　DIRECTORY１９８１年版およびDATA-PRO　SOFTWARE１９８２年版を参考に作成した。

表２－３は，ファイル・アクセス・コントロールのためのユーティリティで，ＯＳの基本的なセキュリティ機能を支援するものである。すなわち，各種資源のプロファイルと利用者のプロファイルとを保持し，利用者のログオンを始め，種々のファイルのREAD，WRITE，APPEND，UPDATE，DELETE，EXECUTE等の要求に対してのアクセス資格の逐一チェックおよび記録を行ない，さらに違反に対しては，アクセス不能を表示する。また，要求に応じて種々のレポートを作成する機能を持つものもある。

表２－４は，暗号化のソフトウェアであり，重要なプログラム，データ・ファイル等を暗号化して記憶または伝送し，必要の際に復号化を行なう場合のツールである。またデータ圧縮を同時に行なうものもある。

表２－３　アクセス・コントロール用商用ソフトウェアの例

（ ― はデータ不明）

名　　称	使用開始	ユーザ数	価格 $	対象機種	製造／販売	備　　考
RACF―Resource Access Control Facility	―	―	569／月	IBM360／370，3030	IBM Corp.	
ACF2	78	525	27,000 1150／月	IBM370，3030	Combridge Systems Group	
CICS―PROTECT	―	―	―	IBM370	Ambridge International	CICSの保護
FILE／MANAGER	―	250	―	IBM370，4300	Altergo Software Inc.	
GUARDIAN	―	100	18,000 880／月	IBM370，3030，4300	Online Software International Inc.	CICSの保護監査 レポート出力可能
IMS／VS USER SECURITY	78.7	―	150／月	IBM370	IBM Corp.	IMSの保護
POWER／VS REMOTE JOB ENTRY CONTROL-LED ACCESS MONITOR	―	―	―	IBM370	IBM Corp.	
SAC―SECURITY ACCESS CONTROLLER	76	5	15,000～ 20,000	IBM	Electronic Data Systems（EDS）	監査レポート作成可能
SECURE	―	250	―	IBM360／370，3030	Boole & Babbage	
TOP SECRET	81.9	22	700／月	IBM370，3030，4300	CGA Software Product Group	
PANEXEC	78.2	―	―	IBM360／370，4300	Pansophic Systems，Inc.	実行形式プログラムの保護
SECURE／IMS	―	―	―	IBM，Amdahl	Chicago Data Systems	IMSファイルの保護
SUPER MSI（Multiple Systems Integrity Facility）	78.3	210	10,000 625／月	IBM360／370，3030	CGA Software Product Group	
INFOFLEX	―	20	12,000 400／月	DEC PDP―11，VAX	Interactive Information Systems，Inc.	オンラインネットワークアクセスに対するデータ保護
SENTRY	―	―	635／月	UNIVAC1100	Spery Univac	
COMPUTERIZED LIMI-TED ACCESS SECURI-TY SYSTEM（CLASS）	―	40	4,650	IBM Series 1	Applied Realtine Systems，Inc.	
SDSI（SHARED DATAS-ET INTEGRITY）	78.9	125	12,000～ 15,000	IBM360／370	Software Module Marketing Inc.	
SECURITY MANAGEME-NT SYSTEM	80.6	3	2,500 100／月	Prime Series 50	Q. S. Inc.	
DB SAFE	80.3	8	950	IBM System 34	D／B Services	

表２－４　暗号化用商用ソフトウェアの例

（ — はデータ不明）

名　　称	使用開始	ユーザ数	価 格 $	対　象　機　種	製造／販売	備　　考
CYPHER	—	3	—	IBM360/370,3030,4300	Innovative Management	
CRYPTEX-Keyless Data Cryptography Software	75.2	50	1,250	IBM360/370	Bi-Hex Company	COBOL,PL/I プログラムからコール可能
CRYPTOPAK	—	—	9,750	IBM360/370 UNIVAC1100	Computation Planning Inc.	DESおよびQIK-CRYPT系
DATASECURE	—	—	—	IBM360/370	Applied Data Research Inc.	
DESQIK	—	—	3,250	IBM360/370,4300,Amdahl ITEL,UNIVAC1100 Burroughs B2700/4700	Computational Planning Inc.	DESおよびQIK-CRYPT系
NCODE/DCODE	75.7	50	70/月	IBM360/370,3030	Applied Software Inc.	
SHRINK-FILE COMPRESSION ENCRYPTION SYSTEMS	—	80	—	IBM360/370	Informatics Inc.	データ圧縮と暗号化
ADVANCED DATA CODE(ADC)	77.3	8	2,000	IBM360/370,3030,4300	Hansco Data Processing Inc.	データ圧縮と暗号化
PROGRMMED CRYPTOGRAPHIC FACILITY	—	—	250/月	IBM370	IBM Corp.	
SAFEGARD Ⅱ 同　上　Ⅲ	73.8 77.9	70 20	650	IBM360/370,WANG	Software Solution Inc.	乱数によるキー発生
PSYPHER	80.11	4	—	IBM,DEC,CDC,WANG,Data General	Prime Factors	
SECURE	—	—	500	Data General Eclipse	Gamma Technology Inc.	DES
DESCRYPT	—	—	—	IBM360/370,3030,4030;DEC PDP-11 20, VAX;Data General NOVA,Eclipse;CDC,WANG	Prime Factors	DES
007	77.9	35	495	IBM360/370,3030,4300	Hansco Data Processing Inc.	DES
NBS DATA ENCRIPTION ALGORITHM	79.8	2	500	Data General NOVA,Eclipse	Gamma Technology Inc.	DES

3. 今後検討すべき基本技術

本章では，コンピュータ・システムのセキュリティ機能を強化するため，今後さらに検討すべき基本的要素技術について，概要を述べる。これらの技術は，前述の第1章および第2章で指摘された問題点や新たな要求に対応しようとするものであり，既存技術の改良や新しい技術を下記のように分類し，提案の形にまとめた。

① 本人確認に関する技術

② オペレーティング・システムに関する技術

③ データベースに関する技術

④ ハードウェアに関する技術

⑤ ソフトウェア技術

⑥ 通信回線に関する技術

⑦ 暗号に関する技術

⑧ 入出力装置（端末）に関する技術

⑨ 運用自動監視に関する技術

これらの技術は，その実現可能性や効果等について，まだ充分な検討が行なわれていない。そのため，実際の応用システムに適用した場合，ねらい通りの効果を発揮できるかどうかは明確ではない。実際の応用システムでは，技術以外の要素が多数からむので，実験室で有効な技術が必ずしも役立つとは限らないからである。また，技術は日進月歩であり，ここで提案した技術が可能性のある技術のすべてである，とは言い切れない。さらに，第1章および第2章で指摘された項目は，現在か近未来の問題点や要求であり，将来これまでとはまったく別種の新たな脅威が予測される可能性もある。従って，今後ここで提案された技術の実現可能性や実際の効果と共に，さらに効果の大きい新しい技術の可能性をも含めて，慎重に検討し開発して行く必要がある。

尚，将来新たに起きる可能性のある脅威については，第4章で述べる。

3.1 本人確認

本人確認とは，コンピュータ・システムに対して当事者としての関与の妥当性を検証し，以降に続く行為に許可／不許可を与えるものであり，身近なものとしてはキャッシュ・カードの暗証番号システム，コンピュータ室入出監視システム，あるいはＴＳＳなどで使っているパスワードなどである。

本人確認の方法として，

① 厳密な意味での本人でなくても，所定の手続き，あるいは情報により本人と見なす場合（ＩＤカード，鍵など所定のものを所持していることにより本人と見なすもの，あるいは，パスワードなど所定の情報により本人と見なすものがこれに該当する）

② 厳密な意味での本人を認識するもの（指紋などによる確認がこれに該当する）

に大別できるが，どちらが優れているかについては一概に判断することは不可能で，システムの特徴，本人確認の必要度合いなどにより決められる。

コンピュータの世界で広くとらえるならばコンピュータ・システム間の確認も本人確認と言えるが，本節では相手を人間に限定している。

3.1.1 本人確認の必要性

従来から本人確認に使われているＩＤカード，パスワード，暗証番号等は，他人が不正に使用しない限りかなり安全性の高い保護を期待することができるが，ひとたび不正が発生すると，不備ながら，その方式を前提としたシステムを構築しているだけに問題をより複雑にする。例えば暗証番号を前提としているキャッシュ・カード・システムは，カードと暗証番号が合えば本人が正しく使ったものか，不正に使われたものかまでは追及しない。仮に，以前のシステム（ＣＤやＡＴＭのないバンキング・システム等）であれば，暗証番号とかカードとか言うよりも「顔」という確実な方法で本人を認識していた。しかし経済の発展，技術の進歩などにより直接・間接を問わず全員がコンピュータに，

係わる様になり，それに比例して過失，あるいは不正にコンピュータ・システムをアクセスする事故が増えており，現在犯罪件数の多いのも不正に本人となるケースである。

いずれにせよ，本人確認の技術はコンピュータ・システムを外部からの過失，脅威から防ぐためのセキュリティ上重要なものである。

3.1.2 期待される本人確認技術

磁気カード，暗証，パスワードなどの本人確認は，本人と認識するための媒体，情報のみの妥当性により行なうものであるが，本人確認を高度に推し進めると，他人に盗まれない，あるいは真似のできない方式となり，結局は本人の身体上の特徴をとらえることになる。

(1) 指紋照合技術

指紋とは，指頭の手のひら側にある隆起した汗腺の出口のつながり（隆線）が作る紋理，あるいは紋理を押印してできた像のことを言うが，この紋様は受胎後18週位で形が整い終生変らないことと，更にどの指，どの人にも1つとして同じものがないという特徴を使って本人の確認（識別）を行なうものである。

確認の方法としては，指紋をスキャナで読み取り，その特徴を予め記憶しておき，それと確認する本人の指紋の特徴を比較するものである。ただし，実現に当っては，高速な計算機と高精度な画像装置を必要とし比較的高価なものになっているが，技術的にはすでに確立され，特殊なシステムでは実用化されている。

(2) 声紋判定技術

声の音としての要素は，発生器官が個人によって全く異なることから，1人1人異った特徴をもっている。この特徴はその声を構成している色々な周波数成分を分析することで表現される。そしてこの周波数成分をもとに紋様として表わすことができる。この紋様は同じ単語でも個人差があることから

紋様を使って個人の認識を行うものである。

最近ＬＳＩ技術の進歩，高密度大容量記憶装置の実用化などにより，解析技術も進歩しているが，現在は音声認識（つまり言葉の認識）が商用化の限界で，自動声紋判定の実用化はもうしばらく時間がかかるものと思われる。

(3) サイン判定技術

サインの交差線数，上下左右に動く回数による空間的判定基準法や，速度，加速度，所要時間，筆順の時間的判定基準により特徴を抽出して本人確認を行なうものであり，一部欧米では簡易型ではあるが実用化されている。日本では手書き漢字入力装置として製品化されているが，漢字という事情からサインにより本人確認の技術を実用化するまでには至っていない。

(4) 手形照合技術

人間の手形の特徴（手の大きさ，指の長さあるいは太さなど）により本人確認を行なうもので指紋，声紋に比べ精度の面では若干不安が残るが，比較的容易な技術で実現可能なため既に製品化されているものもある。

(5) 印鑑照合技術

印鑑を本人確認の手段に使う方法は，印鑑を盗用された場合はキャッシュ・カードと同じになるが，画像処理により照合する点で大きく異なる。照合手法は指紋照合と同じ概念であるが，実際問題としては朱肉の質の問題，印鑑の押し方の問題，印鑑の破損の問題など細かい問題は残っている。

3.1.3 本人確認技術の採用拡大による影響

本人確認は，信頼度を高めれば高める程，個人個人のもつ生理的な特徴をもとに行なわれる。そして本人以外アクセスを許可されないという現象が発生する。例えば一般のバンキング・システムで厳密な本人確認技術を採用すると取引契約を結んだ者以外家族でも利用不可能となる。この様な場合，特別な属性を与えて解決することも可能である。今後技術の進歩により高度な本人確認技術が出現することは十分予想される。しかし，その反面不都合が生じることも

考えられるし，プライバシの問題にまで発展することも懸念される。高度な本人確認技術の導入は高い見地からの判断が必要と思われる。

3.2 オペレーティング・システム

3.2.1 アクセス・コントロール

現在のリソース・アクセス・コントロールにおけるアクセス権のチエックは2.1節で述べられている通り，データセット単位のコントロールである。

従って，あるデータセットをアクセスする資格を有する者は，そのデータセットに格納されているすべての情報をアクセスする事が可能となっている。故に，機密レベルが異なる様な情報を同一のデータセットに混在させる事は避けなければならない。

しかしながら，それを完全に実施する事は困難であり，かつ今後パソコン等の普及により，システム利用者は拡大化する傾向にあり，機密レベルの異なる情報が同一のデータセットに混在格納されているケースはますます増加するものと考えられる。

この様な状況の中で，本項では以下の技術的な対応策を提案する。

(1) レコード単位の機密保護機能

レコードに数段階の機密レベル（秘密区分）を設定する事により，データセットのアクセス資格および機密レベルにより，アクセス・コントロールを行なう方式である（図3－1参照）。

例えば，図3－2の場合，以下のようになる。

① 利用者Aは，人事マスタ上のレコード㋐，㋔についてアクセス可能である。

② 利用者Bは，㋐，㋑，㋓，㋔についてアクセス可能である。

③ 利用者Cは，㋐，㋑，㋒，㋓，㋔についてアクセス可能である。

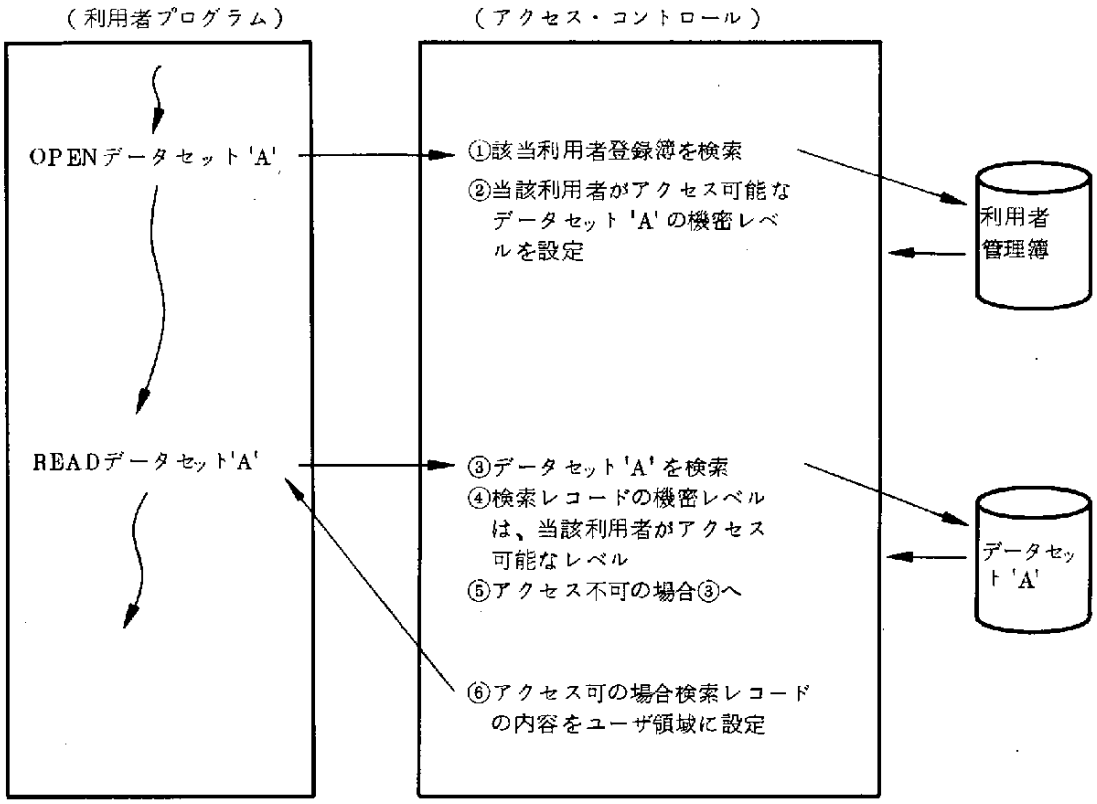


図３－１　レコード・コントロールの方式

〔利用者登録簿〕

利用者ＩＤ	データセット名	機密レベル
A	人事マスタ	1
B	〃	2
C	〃	3

〔人事マスタ〕

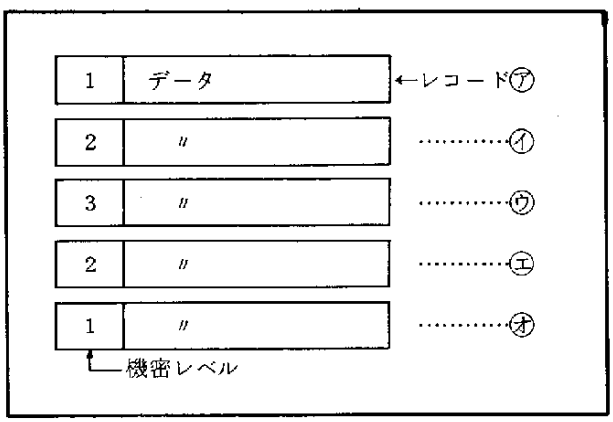


図３－２　レコード・コントロールの機能

(2) データ項目単位の機密保護機能

DBMSのサブスキーマと同様な考え方であり，利用者毎に論理サブファイルを設定し，必要なデータ項目のみをアクセス可能とするコントロール方式である（図３－３参照）。

例えば，図３－４の場合，以下のようになる。

① 利用者Aは，レコード㋐，㋑，㋒，㋓，㋔の社員番号，本給，評価のデータ項目についてアクセス可能である。

② 利用者Bは，レコード㋐，㋑，㋒，㋓，㋔の社員番号，本給のデータ項目についてアクセス可能である。

③ 利用者Cは，レコード㋐，㋔の社員番号，本給についてアクセス可能である。

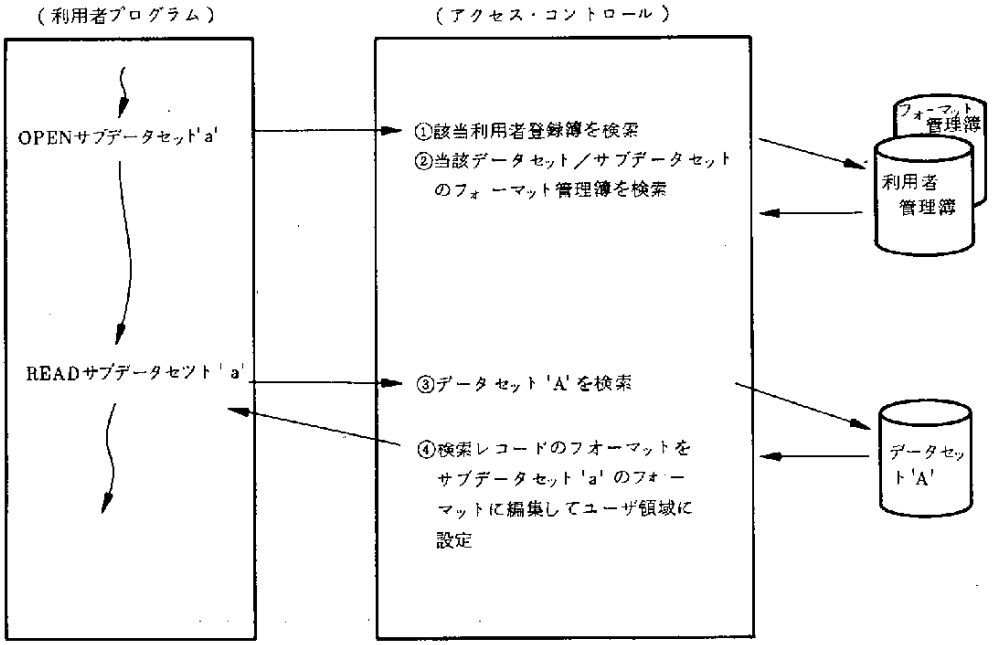
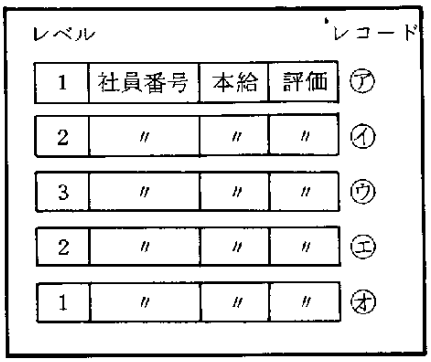


図３－３　データ項目コントロールの方式

〔利用者登録簿〕

利用者ID	データセット名	サブファイルID	レベル
A	人事マスタ	ⓐ	3
B	〃	ⓑ	3
C	〃	ⓑ	1

〔人事マスタ〕



〔サブファイル管理簿〕

サブファイルID	データ項目名
ⓐ	社員番号，本給，評価
ⓑ	社員番号，本給

図３－４　データ項目コントロールの機能

3.2.2　プログラム・ライブラリ

現在，アプリケーション・システムのソース／ロード・モジュールは，運用では一体管理されているが，コンピュータ・システムとしては，別々に管理されている。

本ライブラリ管理機構は，これらソース／ロード・モジュールを一体管理し，その対応付けを明確にする事により，ソフトウェアの信頼性向上を図ると共に，不正な改ざんを防止する事を目的とする。

これを実現するために，図３－５のように，ソース・モジュール，ロード・モジュール，実行用ジョブ・コントロール・データを含む，アプリケーション・システム・コントロール・ファイル（ＡＳＣＦ）を設ける。ＡＳＣＦはアプリケーション・システム毎に存在する。

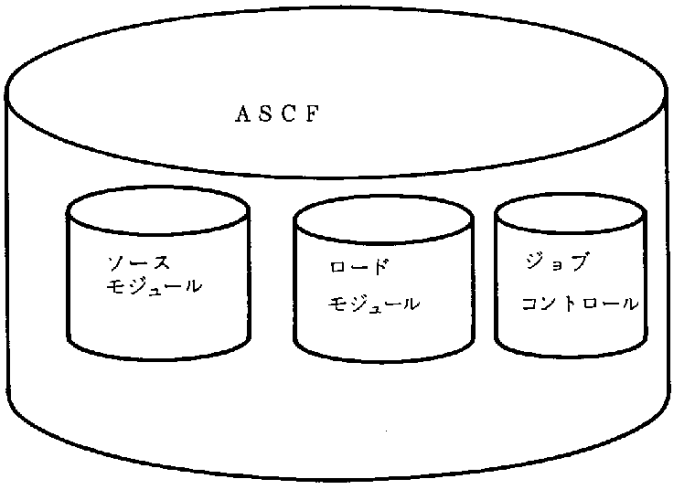


図３－５　ＡＳＣＦの構成

ＡＳＣＦは，本ライブラリ管理機構の核となる重要なファイルであり，原則として固定ディスク上に展開される。

ＡＳＣＦは運転用と開発用の２種類が存在する。

(1)　運転用ＡＳＣＦの機能

①　ソース・モジュールの修正

ソース・モジュールの修正が発生すると，ただちにコンパイルが実行され，ソースおよびロード・モジュールの対応が保たれる。ロード・モジュールに直接修正が実行された場合は，その情報がソースにも書き加えられる。すなわち，いかなる場合もソース，ロード・モジュールは，その論理的関連性が保証される。

②　運転中の修正

ＡＳＣＦ内のアプリケーション・システムが実行中であれば,そのＡＳＣＦは修正不可能とする。

(2)　開発用ＡＳＣＦの機能

ソース・モジュールの修正について説明する。開発用ＡＳＣＦは，ソース・

モジュールのみの修正が可能である（ロード・モジュールの直接修正は不可能）。また，開発用ＡＳＣＦで使用されるファイルは，すべて「ＴＥＳＴ」のマークが付加され，運転用ファイルと区分される。

3.2.3　拡張ロギング機構

本ロギング機構は，従来のロギング機構を，主に記録部分を中心にして，外部に分離独立させ，サブシステム化を図る事により，詳細な情報の記録を行ない，システム自体の安全度を強化するものである。

(1)　記録情報の選択方法と記録項目

①　ジョブ名のユニーク化

従来のシステムでは，ジョブ名の設定は自由であったが，拡張ロギング機構を使用する場合は，ジョブ名をユニーク化する。ユニーク化には次の２つの方式を用いる。

ⓐ　固定ジョブ名方式

本方式は，ユーザＩＤごとに登録制でジョブ名を固定にする方式である。重要ファイルにアクセスする場合は，この方式とする。

ⓑ　自由ジョブ名方式

本方式は，ユーザが自由にジョブ名を決定できるが，１日の間に同一のジョブ名が複数回出現する事は不可であり，かつ重要ファイルのアクセスは禁止される。

②　記録情報の選択

ジョブ名のユニーク化の目的は，記録情報の選択と，事後チエックの容易化である。固定ジョブ名が使用されると，拡張ロギング機構は，例えばアクセスしたレコードの情報まで記録する。自由ジョブ名では，従来のロギングと同様な項目を記録する。

③　記録項目

従来のロギング情報に加えて，レコード・アクセス情報を記録する。シー

ケンシャル・ファイルでは，レコード番号，ランダム・ファイルでは，論理アクセス・キーと，物理アクセス・キー等を記録し，さらにレコード情報そのものを記録する事も可能にする。

3.3 データベース・システム

データベースに対するセキュリティ面から見た脅威を分類すると

① データベースの破壊，消滅

② 内容の漏洩，複写

③ 内容の改ざん，不正更新

である。それに対して，現在あるデータベース・システムのセキュリティ対策は，アクセス管理方式の原始的なパスワードと，それを多重化したもの，および，モニタリングに集約される。

その理由は，

① セキュリティ対策の対象となるデータが多様で，かつ大量である。

② データベース構造がコダシル型の，いわゆるツリーが大部分である。

③ きめ細かいアクセス制御を必要とする階層関係，包含関係のあるデータ構造が多い。

④ 各レベルにおける保護機能を必要とする。

⑤ データベースが特定の応用プログラムと対になっているため，影響範囲も限定されている。

などである。

しかし，データベース・システムを実現するための記憶装置の技術的進歩により，高密度化，大容量化し，また，データベースの構造も従来の固定的なものから可変的なものに変ってきている。その結果，データベースの位置づけも大きく変化している。リレーショナル型データベースの出現がよい例で，リレーショナル型データベースは利用面からみると柔軟性はあるが，セキュリティ面からみると逆行している。それは，すべて応用プログラムに解放し，応用プログラムが必要に応じて選択する方式だからである。

この様に，データベースの利用形態の変化に伴ない，セキュリティ対策も変えていく必要がある。本節では，そういった背景を踏まえて開発が期待される基本技術について述べる。

3.3.1　リレーショナル型データベースにおける関係演算の妥当性チエック

リレーショナル型データベースは，全体構造を単なる表として扱い，必要なデータは応用プログラムが関係式を用いて引き出す方式である。つまり，関係代数によって表わされる関係式がアクセスの手順となり，そして，その関係式も固定的なものでなく応用プログラムがアクセスする都度意味を成すものである。その結果，データベースに対するアクセスの妥当性のチエックはデータベース利用者側の責任において行なうことになる。別の言い方をすると,データベース利用者側（応用プログラム）の作り方次第で，データベースの内容はどの様にも扱えることになる。

システム管理者側であえてデータベースに対するアクセスの妥当性をチエックするとなると関係演算の妥当性をチエックする必要がでてくるが，式の作成がデータベース利用者側にある以上容易ではない。今後，この点について，新方式の開発が望まれる。

3.3.2　推測防止技術の開発

統計処理を目的とするデータベースに，いくつかのパターンで質問を重ねると本来直接的には引き出せない情報を推測することができる。これを防止するためにシステム管理者側が質問の内容をトレースし，システム利用者側が与えられた以外の情報を推測するのを未然に防ぐ手段が必要である。

3.3.3　データベース（ファイル）の暗号化

データベースの内容を直接的，または正規にアクセスを許されたプログラムを介して内容を複写することを防止するためのものである。

最近，特に通信回線からの不正アクセス防止に有効な手段であることから暗号化技術が急速に進んでいるが，この考えをファイルにも適用しようとするのであり，

① 技術的には現在の暗号化方式を採用する。

② 暗号化キーは，応用プログラムごと変え，かつ該当ファイルとは別に保管する。

という方法を用いれば特に難しいものではない。しかし，

① 暗号化，および復号化のための時間がかかり過ぎる。

② 容量が増える。

③ オペレータの不正に対して弱い。

などの欠点があり，有効な暗号化方式，もしくはそれに代る手段の開発が望まれる。

3.3.4 その他の技術

① 書き込み不可能なファイル

一部光ディスクという名称で商品化されているが，更新を許さないファイルに対して有効である。

② ファイル不正使用時の内容自動消却

磁気テープ，あるいは移動可能な磁気ディスク等が不正に使用される場合，自動的に内容を消却するものである。

3.4 ハードウェア

3.4.1 本体装置

(1) ロギング・プロセッサ

本プロセッサは，コンピュータ・システムの運用状況監視のために必要とされる各種の情報を収集するサブ・プロセッサである。

現在，既にオペレーティング・システムにより，各種の情報収集が行なわれているが（SMF等），不正処理，不正アクセス等の防止，追跡のための情報としては不充分である。しかしながら，現在以上の詳細情報をオペレーティング・システムで収集することは，システム効率に与える影響が多大であり，事実上困難である。

本サブ・プロセッサは，それらの情報収集をハードウェアでサポートするものであり，オペレーティング・システムと密接な関係を持ったロギング専用プロセッサである。

① ハード構成

本プロセッサは，CPU，メモリ，ディスク，コンソールにより構成され，メインCPUとは高速チャネルで接続される（図3－6参照）。

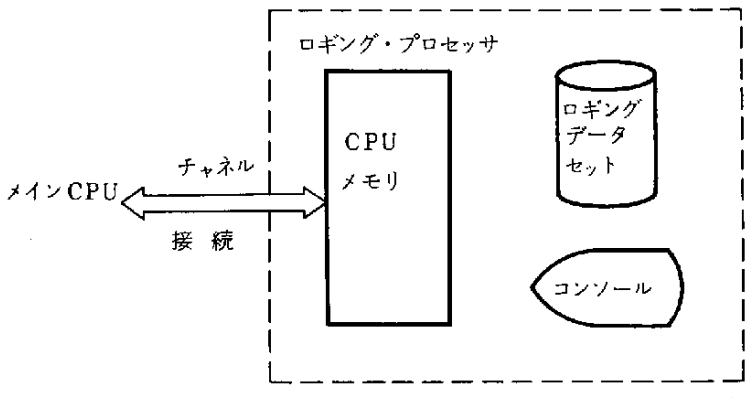


図3－6 ロギング・プロセッサの構成

② 機 能

従来の収集情報機能に加え，

ⓐ 収集情報の選択ロギング機能

収集情報の種別により，ロギング・データセットを区分して格納

ⓑ レコード・アクセス情報のロギング機能

特定データセットのレコード・アクセス情報のロギング

ⓒ 不正アクセス時の表示機能

不正アクセス情報のロギングとコンソールへの表示

等を有する。

(2) ファイルの暗号化機構

ファイルの暗号化については，

① プログラムによる方法

② ハードウェアによる方法（暗号化プロセッサのチャネル接続）

が，既に実用化されている。しかしながら，

- ①については，CPUの負荷
- ②については，価格

の面で問題を抱えている。

本項で提案する方法は，ハードウェアによるものであるが，現行のハードウェアに簡易暗号方式による暗号化命令を追加する方法である。

暗号化命令は，マイクロ・プログラムで実現し，キーはシステムのIPL時にサービス・プロセッサ等により設定されるものとする。従って，キーはシステム毎に固定されたものとなるが，定期的に変更することは可能である。

この暗号化命令を使用するソフトウェアは，前述（3.2.1項）したソース・アクセス・コントロールの機能で保護するものとし，ユーザ・レベルのソフトウェア（プログラム）では，本命令の使用を不可とする。

(3) 指紋センサ機構付コンソール

本装置は，キーボードに指紋センサ機構を有した装置であり，

① センタ・オペレータの本人確認

② オペレータ・コマンド投入者のロギング・データへの反映

を行なうことにより，センタにおける不正オペレーションの防止を図るものである。

3.4.2　周辺装置

(1)　残存消去機構付磁気テープ装置

現在，磁気テープ媒体の初期化はユティリティ・プログラムで行なっており，初期化の範囲もボリューム・ラベルのみである。従って，再使用する媒体には以前のデータがそのまま残っており，初期化後も比較的簡単に参照することが可能である。

本装置は，媒体の初期化時，ボリューム・ラベル部分の初期化を行なうと同時に，媒体全体をイレーズ（消去）する機構を持った装置である。

尚，媒体の初期化は，スタンドアロンで可能とする。

(2)　残存消去機構付ディスク装置

現在，ディスク上のデータセット削除時消去される内容は，VTOC 上の内容のみであり，データセットの内容はそのまま残っている。

本装置は，データセットの削除コマンド発行時，および作業用データセットの解放時，当該データセットの領域をすべて初期化する機構を持った装置である。

(3)　フィールド・マスク機構付プリンタ装置

本装置は，帳票出力時に機密レベルの高い項目を“メカクシ”して印刷する機構を持った装置である。解読は，当該帳票を見る資格を有する者が“メカクシ”項目に特殊加工を施すことにより可能となる。

(4)　暗号化磁気テープ装置

重要ファイルのバックアップとして，磁気テープ媒体を利用する場合，内部保管については，物理的保護（入退室管理等）や前述（3.2.1項）のリソース・アクセス・コントロール等により保護可能であるが，外部に持ち出すデータについては，上記の保護方式は，ほとんど意味をもたない。

外部に持ち出すデータを保護する手段として，データの暗号化が考えられる。本装置は，コマンド種別（SAVE，COPY等）および対象データセット名等により，磁気テープ媒体へ格納するバックアップ用データ等を，暗号化して書き込む機構を持った磁気テープ装置である。

3.4.3 媒　体

(1) 鎖錠付媒体

文字通り記録媒体に物理的な鍵を付ける方法である。この方式のメリットは，安価に実現できる可能性があることである。さらに，物理的な鍵の方が，数字等の組合せによるパスワード的な鍵よりも，管理が容易ではないかと思われる。また，次の(2)で述べる揮発性メモリによる固体媒体と組合せ，アクセス手順として物理的鍵を用いる方法も効果的であると考えられる。

(2) 揮発性メモリの活用

半導体メモリを用いた固体媒体を作り，データ交換用媒体として利用しようという提案である。半導体RAMの欠点の一つに揮発性（電源を切ると内容が失われること）という問題がある。これを利用して通常はバッテリで内容を保存し，不当なアクセスが行なわれた時，電源を切断して内容を消去することにより，不当なアクセスに対応しようとするものである。

不当なアクセスがどうかの判断は，固体媒体にプロセッサを内蔵して行なう。この固体媒体は内容を自動消去することによって，保護を行なうのであるから，当然バックアップ・データを保存しておく必要がある。

固体媒体へのアクセス手順は，秘密にしなければならない事項であり，暗号化におけるキー管理と同様な運用上の問題が存在する。

(3) 再書き込み不能ファイル

光ディスクやヒューズ溶断型ROM等，一度書き込むと再書き込みできないという不便なファイルやメモリがある。これを逆手に利用して，データ保存用のファイルに使用すれば，再書き込みできないだけに安全性が高い（物理

的破壊には効果がない）。光ディスクは，容量が大きいので，バックアップ・データ保存用には最適である。

しかしながら問題点もある。光ディスクは，レーザ光線を使って必要なビットのみON（またはOFF）にするが，一度書き込んだ後，再度すべてのビットをON（またはOFF）にしてデータを破壊することは可能である。ヒューズ溶断型ROM等も，一度書き込んだ後さらにすべてのヒューズを切断すれば，データを破壊できる。これらの点を改善して，マイクロフィルムと同等な再書き込み不能性を持つようにする必要がある。

3.5 ソフトウェア技術

本節では，ソフトウェアのライフサイクル全体でソフトウェア自体のセキュリティ*1を向上させる観点[1]（ソフトウェア工学の立場）および犯罪防止等の観点（システム監査の立場）からソフトウェア技術に対して期待される点を述べる。

ソフトウェアのライフサイクルは，大きく次の5つの段階に分けられる。

① 要求仕様定義段階

ソフトウェアに対して要求される機能・性能を定義する。

② システム設計段階

要求仕様を満足させ，最適に実現するソフトウェア構造，アルゴリズム，抽象データ構造等を設計する。

③ 詳細設計／コーディング／デバック段階

システム設計書に基づき，使用するコンピュータに適合するように，詳細にアルゴリズムや物理データ構造を設計し，それに基づき，プログラムをコーディングし，バグを除去する。

④ 出来上がったソフトウェアを第三者が要求仕様書通りに正しく機能するかを確認する。

⑤ 保守段階

出来上がったソフトウェア製品が使用され，ソフトウェア・エラーが検出されると修理し（修正保守），より機能を完全にするため改良し（完全化保守），あるいはシステム機能拡張のため更新（適応保守）する。

以上の5つの段階，すなわちライフサイクル全体を通してソフトウェアのセキュリティを向上させることが重要である。

以下では，上記のライフサイクルの5つの各段階とシステム監査の立場に分

＊1：本節では，この用語を主として，「信頼性」(reliability)，「正当性」(correctness)，「完全性」(integrity)，「完備性」(completeness)，「無矛盾性」(consistency)，「高品質性」(quality)の総称として使用している。

けて述べる。

3.5.1　要求仕様定義段階

ソフトウェア開発の第1段階は，ソフトウェア・システム全体に対する利用者（発注者）の要求を厳密に記述する段階である。このソフトウェア要求定義が，以後のソフトウェア開発のすべての段階での拠所であり，この要求定義が不完全で，不正確で，あいまいであると，以後の開発段階での高度なセキュリティの達成が不可能となる。

そのためには，ソフトウェアに対する要求定義をもれなく，完全に，正確に，あいまいさなく，容易に記述するのに使用できる要求仕様言語が期待される。

期待される要求仕様言語が具備すべき主な条件・特性は，以下の諸点である。

① 要求仕様書は，利用者がシステムに対して何（what）を要求するかを記述したものであり，利用者にとって作成が容易でなければならない。

② 要求仕様書をあいまいさなく厳密に記述するためには，その記述言語は形式的でなければならない。

③ 要求仕様書はすべての段階での拠所となるもので，関係者すべての人の必読書であり，簡潔・明瞭で，読み易く，構造的で，理解が容易でなければならない。

④ 要求仕様書を完全に，矛盾なく記述するのは困難であるので，ある程度の自動検証ができる必要がある。

⑤ ソフトウェアの品質を向上させる現実的な手段はテストであり，この要求仕様書から出来上がったソフトウェアに対するテスト・データが自動的に生成できる必要がある。

⑥ 使い勝手の良いコンピュータ支援（computer aided）の知識ベース指向の要求仕様記述システムが望まれる。

3.5.2　システム設計段階

システム設計は，出来上がるソフトウェアのセキュリティ・レベルを実質的に決定する最重要段階であり，高セキュリティのシステム設計が行なわれなければならない。過去の大規模ソフトウェアの開発の経験によると，稼動中のソフトウェアのエラーの大半がソフトウェア開発の初期の段階で入り込んでいる。要求エラー，設計エラーが特に多い。設計段階で入り込んだエラーを修正する作業は，後続のコーディング段階でのそれに比べ，格段に困難となる。

また，開発中には，システムのセキュリティ機能について特別な配慮がなされず，ソフトウェア・システムの作成完了後に，ソフトウェアで新たなセキュリティ機能を実現するため，既存のソフトウェアに新しいセキュリティ機能を追加すると，セキュリティ強度が向上するよりも，むしろ，システム全体のセキュリティ強度が低下することが多々あり，更にシステム全体の性能低下の主要原因ともなってしまう。

システム設計段階では，ソフトウェア自体のセキュリティを向上させるには，抽象化と分解を徹底させる必要がある。抽象化と分解は，複雑なシステムをより容易に，高セキュリティに構築する工学での常套手段である。抽象化することによりシステム全体の機能の把握が容易となる。そしてシステムをサブシステムに最適に分解することにより，システムの作成が容易となる。抽象化と分解は，各々逆過程，すなわち，抽象化は下位のモジュールでもって上位のモジュールを合成する過程であり，一方分解は逆に上位のモジュールをより詳細な下位のモジュールに分割していく過程である。

システム設計段階では，抽象化と分解を支援する設計方法論が期待される。トップ・ダウン設計法は，この分解を基本的な技法として採り入れている一例である。設計方法論だけでなく，これをある程度自動支援するCAD（Computer Aided Design）システムがますます期待される。CADを使用してソフトウェア設計が行なえるようになると，ソフトウェア要求定義条件に照らして，コンピュータによる設計内容のセキュリティに対する評価・検証がある程度可能に

なる。コンピュータに設計書が蓄積されるようになると，設計書を常時最新の内容に維持しておくことも可能となる。

またCADを使用することにより，設計書の記述作法の標準化が徹底的に推進され，第三者が設計書の内容を理解するのが容易となる。このことにより，第三者による設計内容のレビューがより容易となり，思い違いによる設計ミスや，設計もれの指摘を効率的に行えるようになる。

3.5.3　詳細設計／コーディング／デバック段階

本段階は，出来上がるソフトウェアのセキュリティ・レベルを直接的に決定する段階であり，高信頼化プログラミング（secure programming）あるいは防御的プログラミング（guarded programming）が行なわれなければならない。

人間の思考や情報能力は限られており，大きく複雑なプログラムはモジュール化し，プログラムの複雑性や一時の作業負荷を軽減する必要がある。そのためには，プログラミング言語には，強力なモジュラ・プログラミング機能，抽象化機能，情報隠蔽機能等が備わっている必要がある。また，プログラミング時の単純なケアレス・ミスを防止する機能も備わっている必要がある。

例えば，

MISTAKE＝MISTEAK＋1

では，プログラマは変数MISTEAKを1だけ増加することを意図している。FORTRAN言語では，このエラーは検出できない。しかし，COBOLやPascal言語では，使用する変数は前もってすべて宣言するので，このエラーはコンパイル時に検出できる。この種のケアレス・ミスはコンパイル時に静的に検出できるように，プログラミング言語が設計されていなければならない。この種のエラーは特性エラー（characteristic error）と呼ばれる。[2] 更にcase文，配列の添字等の値の範囲が正しいか否かを，実行時に効率的にチェックできなければならない。従来は，プログラムのデバッグ時にはこの種のチェックをやり，一方，効率を重視するあまり，本番稼動時にはこの種のチェックを省く傾向に

あるが，むしろ本番時にこそプログラムのセキュリティが要求されるのであって，本末転倒である。

そして，ソフトウェア自身による自己のセキュリティ向上のため positive check，self-check 等の技法[3]を積極的に採用する必要がある。

プログラムの作成や理解を容易にするため，プログラムの構造化，ブロック化，すなわち構造化プログラミング（Structured Programming）が容易でなければならない。

セキュリティ機能を実現するには，複雑なロジックやたくさんの組合せロジックをコーディングしなければならず，時には数１０段以上に及ぶＩＦ文の入れ子構造を実現しなければならない。既存の手続型プログラミング言語では，ＩＦ文が何重にも入れ子になっていると，デバッグがしにくく，かつどんなセキュリティ機能を実現しているかの読解性が悪くなってしまう。複雑なロジックやたくさんの組合せロジックを簡易に記述でき，読解性の高いプログラミング言語が期待される。これに適する言語としては，決定表形式，述語論理形式，知識表現形式を指向したものが候補となろう。

プログラム自身のセキュリティを向上させるには，究極的にはプログラムの正当性が検証できなければならない。検証では，多分，要求仕様に対してプログラムが正しく使われていることを証明するのであるが，検証が可能となった暁にはプログラムの自動合成も完成していると想定されるので，むしろプログラムの自動合成の方が期待される。プログラムの検証を可能にするためには，プログラミング言語自身が，副作用がなく，形式的（数学的構造）でなければならない。これに適する言語としては，関数形式を指向したものが候補となろう。

3.5.4　検査段階

検査段階[4]は，ソフトウェアのセキュリティ，特に品質を確認する段階である。そしてソフトウェアにエラーが存在することが検出された場合には，それ

らのエラーを修正したのち，再び検査をし，それらのエラーが正しく修正されたかを確認する。

大規模ソフトウェアの検証は当分実用化せず，現実には，検査（test）によりエラー（バグ）を完全につぶして，プログラムの正しさを追求することになる。

ソフトウェアの検査ツールとしては，静的解析と検査データの生成が2本柱である。特に後者の検査データの選択は，検査の質を左右する大きな鍵である。起り得るすべてのテスト・ケースについてすべて検査するのは無限の時間を必要として不可能であるので，最適なテスト・データの組合せを選択する必要がある。

もれなく検査を行なうには，要求仕様書から自動的に検査データを生成することが期待される。またソフトウェアは想定された望ましい実行環境（システム構成，OS）でしか走行できないので，検査時には，その実行環境を忠実に再現する使い勝手のよい安価な仮想コンピュータ・システム，環境シミュレータが期待される。仮想コンピュータ・システムは，ソフトウェアにより種々の入出力装置，端末等をシミュレートすることにより，開発用の限られたハードウェア・リソース環境下で，種々のシステム構成を実現するソフトウェア・システムである。一方環境シミュレータは，ハードウェアにより，電源，温度，湿度等の各種環境条件の設定，CPUまたは入出力装置の擬似的な障害を発生させる等の各種事象を発生させるハードウェア・システムである。

ソフトウェアの検査は際限がないので，どの程度まで検査済であるかという経験則が期待される。最近，ソフトウェアの検査がどの程度まで達成されたかを表わす尺度として，網羅率（coverage）が使われるようになってきた。これは，今のところ理論的根拠を持つものではないが，ソフトウェアに対する品質保証の尺度として広く使われることを期待したい。

3.5.5　保守段階

保守段階は，ソフトウェアのライフサイクル内で最も長い期間を占めるようになってきている。[5] そのため，システム全体（ハードウェア，ソフトウェア）のコストの内，大部分がソフトウェア開発に充てられ，そのまた大部分が保守作業に充てられている。この傾向は今後も続くと想定されるので，保守の生産性を向上する必要がある。

保守者は開発部隊とは異なる人であり，ソフトウェア開発に関連するすべての成果物（プログラム，ドキュメント）を通読し，理解しなければならない。現実問題として不可能であるので，保守支援用の各種のツールが期待される。

修正保守は出現したソフトウェア・エラーを正しく機能するように修正する作業である。そのソフトウェア・エラーを修正すると，同時に新たなるソフトウェア・エラーを埋込んでしまう危険性をはらんでいる。これは余波効果（ripple effect）と呼ばれるが，修正・変更による余波効果の影響範囲を解析するツールが期待される。そして，ソフトウェアの修正の履歴を蓄積・管理し，希望する時点に戻し，再現するツールも期待される。またソフトウェアの各種バージョンが存在するので，ソフトウェア・バージョンの自動管理システムも期待される。

3.5.6　システム監査の立場からの期待

システム監査[6] は，ソフトウェア開発の初期の段階から実施される必要がある。なぜなら，稼動段階に入ったシステムを監査し，セキュリティ上の問題点，商法等の関係諸法規に準じてない等を指摘し，現行のシステムの改善・変更等助言・勧告しても，それを実行するにはあまりにも経済的・時間的な損失が大きすぎる。従って基本的には，システム開発の初期の段階からシステム監査人が関与し，セキュリティ問題を解決する必要がある。

現在のソフトウェア開発においては，開発過程をシステム監査人が監査するという点をほとんど考慮しておらず，システム監査人の技量にもよるが，現行

の状況では不可能である。ソフトウェアのライフサイクル全体に渡ってシステム監査が実施できるような状況に持って行く必要がある。そのためには，まずソフトウェア・システムの開発過程が標準化されていなければならない。またソフトウェア開発者は，開発のポイント・ポイントでドキュメント等を整備し，システム監査人にはシステムの中味など解かる筈がないという偏見や縄張り根性をすて，進んでシステム監査に応じる姿勢を持つ必要がある。

要求定義段階でのシステム監査は，新システムのセキュリティ上の弱点がどこにあるか検査することになる。そのためには，要求仕様書の記述形式が標準化され，内容の理解が容易となっていなければならない。

システム設計段階でのシステム監査は，システム設計書と要求仕様書の間に矛盾がないかを確かめる。またシステムの中に，ミス，不正，例外事項のチェック・システムが組み込まれているかも重要な監査項目である。

主としてコーディング段階でのシステム監査は，標準化ルールに従ってプログラムが作成されているか，プログラムの保守を充分に考慮されているかを確かめる。

検査段階でのシステム監査は，必要充分なテスト・データでソフトウェア・システムが検査されたかを確認する。この段階は運用に至る最終段階であり，特に最終的な監査が要求される。

保守段階でのシステム監査は，システム開発と同様な点を確かめ，システムのセキュリティが低下しなかったことを再確認する。

このように，システム監査はソフトウェアのライフサイクル全体に渡って実施することが必要不可欠であり，その実現性および完全性を高めるためにも，高級言語あるいはソフトウェア検証技術等をはじめとするソフトウェア開発技術自体の大幅な向上が期待される。

〔参　考　文　献〕

1) 宮本勲，ソフトウェア・エンジニアリング：現状と展望，ＴＢＳ出版，pp.３５２，１９８１年１月.

2) Tsichritzis, D.,“Reliability,”Lecture Note in Computer Science／Software Engineering: Advanced Course, Springer－Verlag, pp.３１９－３７２，１９７５.

3) Yau, S.S. and Cheung, R.C.,“Design of Self-Checking Software,” Proc.１９７５ International Conference on Reliable Software, pp.４５０－４５７，Apr.１９７５.

4) 田中，石井，「手工業的手法から脱皮を目指すソフトウェア・テスト」，日経エレクトロニクス，№２８６，pp.１２４－１５２，１９８２年３月１５日号.

5) 協同システム開発株式会社，ソフトウェア保守技術開発計画全体構想概説書，pp.２１０，昭和５７年４月.

6) （財）日本情報処理開発協会，システム監査実施への道標，５４－Ｒ００７，pp.２３９，昭和５５年３月.

3.6 通信回線

現在，TSSのように誰でも通信回線を通じてコンピュータにアクセスでき，EFTS（Electronic Funds Transfer System）による電子送金が行なわれ，さらにホーム・バンキング，ファーム・バンキング等の実現を考えたとき，通信回線の脅威はたいへん大きなものとなって来ている。通信回線に関する脅威は主に次のようなものがあげられる。

- 通信回線からの盗聴
- 通信回線への挿入
- 通信メッセージの改ざん
- 不正端末からのアクセス
- 権限が賦与されていないものからの不当アクセス

以下，これらの脅威に関するセキュリティ関連技術について述べる。

3.6.1 通信回線からの盗聴対策技術

現在までにも，競争会社の入札価格を盗聴し競争会社を出し抜く等，通信回線からデータを盗聴してそれを悪用する犯罪が発生している。通信回線を利用してのデータ処理が増加している現在，通信回線の盗聴に対する脅威は大きなものになってきている。

しかし，電話回線からの盗聴を行なうには簡単な電子回路とテープ・レコーダがあれば，音声であれデータであれ，たやすく情報をモニタすることができる。また，ローカル・マイクロ波回線，衛星通信回線に至っては，盗聴を防ぐことは困難であろう。

そこで，盗聴対策の1つとして，盗聴されていることが検出できるような装置が考えられる。例えば，電話回線からの盗聴が行なわれる場合，盗聴装置は構内交換機，コンピュータ・オペレータ室等に仕掛けられ，一般に人目を避けるため無線装置が取付けられる場合が多い。無線装置が伴えば，広帯域の受信機，電界強度測定器，スペクトル・アナライザ等を応用することにより盗聴を

検出することができる。この方法では，無線装置が取付けられていなければ盗聴を検出することはできない。あるいは，盗聴装置の接続による回線の電圧変動を検出することにより盗聴を発見する方式も考えられる。しかし，通信回線全体に渡ってこのような対策を打つことは困難である。まして，マイクロ波回線等の盗聴検出は不可能であろう。

この他の盗聴対策としては，盗聴されたデータの意味が判別できないようにしてしまう方法が考えられる。これに対しては，暗号が有効なものとなる。しかし，暗号は確かに有効であるが，現在暗号装置は高価なものであり，性能，鍵の配送等克服しなければならない問題が多い。

現在，多額の送金，個人のプライバシにかかわるデータ等さまざまな情報が回線を通じて処理されている中で，大部分のデータがむき出しのまま通信されているのが現状である。この対策として暗号が有効な手段として取り上げられているが，果してそれだけでよいのであろうか。郵便システムにおいてさえも，ユーザはハガキ，封書，書留等何種類かのセキュリティに対するレベルを選ぶことができる。通信回線においても同様に，ユーザはセキュリティに対するレベルを何種類か選べる必要があるのではないか。

3.6.2　通信回線への挿入防止技術

高性能のパソコン等が普及している中で，通信回線への偽装メッセージの挿入は容易である。通信回線への挿入防止技術の一つとして暗号がある。確かに暗号化したデータを通信回線に挿入することは難しいであろう。

また，メッセージの発信時間を管理することにより，発信時間以外の挿入を防止することができる。そのとき，一般に一定の時刻に発信するのでなく，その時刻をランダムに変更できればさらに有効であろう。

あるいは，メッセージに連続認識番号を付加しておくことも有効であり，通信プロトコルの上位レベル，下位レベルのいずれにも付加すれば，さらに効果があるであろう。特に，パケット交換によるデータ回線においては，データを

分割し連続番号を付加した上さまざまなルートを経由させて送るため専用回線より偽装メッセージの挿入は難しくなる。専用回線であっても回線を二重化して同様の制御を行なうことにより挿入の防止を行なうことができる。

さらに，メッセージ番号を暗号化する等，これらの技術を組合せて通信回線への挿入を防止していくことも必要である。

3.6.3　通信メッセージの改ざん防止技術

ローカル・マイクロ波回線，衛星通信回線において，盗聴の防止は難しいが，通信メッセージの改ざんという面では強いといえる。ところが，電話回線等の地上回線での通信メッセージの改ざんは，盗聴，挿入ほど容易ではないが，現在の電子回路技術からすればそれ程難しい問題ではない。特にプロテクションされて通常アクセスできないデータであっても，通信回線上ではむき出しのデータとなり，この状態を襲うことにより，他の状態にあるときよりもむしろ容易に改ざんすることができる。

このように，電子送金データ，売買契約にかかわるデータ，学業成績等の改ざんは，電子回路技術により一瞬のうちに行なうことができる。犯罪者にとってその報酬は大きく大変魅力的なものでありその脅威は大きい。

通信メッセージの改ざん防止の技術としても暗号は有効である。暗号が解けなければ改ざんはできない。また前項の挿入防止の項で述べたように，パケット交換のようにメッセージを分割し異なるルートを経由させてデータを転送する方法も改ざんに対して効果のある方法である。

回線上だけでなくターミナル等で暗号データが復号化されて，平文で処理されているために，この状態においても改ざんは行なわれやすい。このような状態での改ざん防止技術もまた重要である。

また，光通信が実現し始めた現在，光通信回線における改ざん，盗聴，挿入は比較的難しいように思われるが，光通信技術の進展とともに新しい目でセキュリティについて考え直さなければならない。

3.6.4　発信端末の確認技術

何らかの形でＴＳＳ等のシステムのパスワードを盗んだあと，自分の端末から回線に侵入しそのシステムを不法にアクセスするという犯罪がこれまでにも発生している。今後，パソコン等のホーム・コンピュータが家庭に普及するとともに，ゲーム気分等での不法アクセスが増加すると思われる。この結果，システムを破壊したり，プライバシにかかわるデータを盗み出したり，ファイルの改ざんを行なう等その脅威もまた大きい。

これらの不当な端末からのアクセスに対して，発信端末を確認する技術が必要となる。

その一つに，コール・バックを行なう方式がある。これは，端末側からセンタを呼び出し，センタ側は端末を識別し，回線が確立したことを知ると一度回線を切断し，あらたに相手端末の回線番号で端末を呼び出し再度確認した後通信を開始するという方式である。この方式は公衆回線においては，より有効である。ここで，センタからのコール・バック時に回線がビジー中であった場合の対策，コール・バックすることによる処理開始の遅れ，回線使用料金の増加，回線使用料金の負担等の問題がある。

また，端末からシステムにアクセスするときに，端末ＩＤをハードウェアで自動発生させ不正端末使用を防止する方式もある。

一般に，同じ端末ＩＤ，同じパスワードをいつまでも使用し続けるのは，盗まれる危険も多く問題である。そこで端末ＩＤ，パスワード等をランダムに自動変更でき，端末使用者とシステムの対応が容易にできるような方式ができればさらに有効であろう。あるいは接続した端末の発信回線番号を自動検出できれば，端末が正しく接続されているか否か確認でき，さらに不正接続であればその回線番号をモニタすることもできる。

一般に公衆回線に接続されたシステムの場合，どの回線からでもアクセス可能であることに問題がある。そこで，接続できる回線が指定でき，権限のない回線は自動的に排除できるようになれば不正接続の可能性は減少する。現

在でもDDX等データ回線での付加サービスとして閉域接続，相手通知機能があるが，データ回線だけでなく広範囲できめの細いサービス技術が必要となると思われる。

3.6.5　通信相手の確認技術

システムに正しく接続された端末において，システムの使用権限がない者が不当にアクセスする場合がある。システムは，このようなアクセスを防がなければならない。

通信相手を確認するために一般に2つのステップを行なう。先ず初めにシステム利用者がシステムに本人であることを提示し，身元照合(Identification)を行なう。次に身元照合した利用者が確かに本人であるか認証（Authentication）する。

確かに本人であるかを認証するためには，本人だけが持っているもの，本人だけが知っているもの，あるいは本人の属性（声紋，指紋等）で確認すればよい。（これについての詳細は，「3.1　本人確認」を参照のこと。）

これらの本人確認技術は，ホーム・バンキング等の端末の普及を考えたとき，単純で経費のかからないものでなければならない。

また，本人確認のため今まで署名というものが使われていた。電子郵便，電子送金等のシステムにおいてデジタル署名が考えられており，公開鍵による方式，DESによる方式等があるが，これらは複雑で高価な暗号装置を必要とする。より簡単で経費のかからないデジタル署名ができる技術も必要であろう。

3.6.1項より各項ごとに各種のセキュリティ関連技術を述べてきたが，それぞれの技術は各項にだけ適用するものではなく，他の項にも有効であり，これらのセキュリティ関連技術を組合せることによりセキュリティ侵害に対してより強固なものとなる。

また，セキュリティ侵害が発生した場合，それをセキュリティ責任者に通知するような技術，あるいは，システム・アクセスしたものすべてについて日時，時刻，

端末ＩＤ等のログを取る技術，特にセキュリティ侵害時のログを取る技術等もまた重要である。

3.6.6　将来の通信ネットワークのセキュリティ管理技術

将来，電話回線，デジタル・データ回線等が相互に接続され，通信ネットワークにおいて異なる企業間のコンピュータが接続され，ホーム・バンキング，ファーム・バンキングが実現し，家庭にいながらにして，航空券の予約といったサービスを受けられるようになったとき，今より増してセキュリティの問題は大きなものになるであろう。

多額の電子送金データを改ざんし，我が物にしたり，画像通信による天気予報サービス等を行なっているところに，不正な地震情報を挿入し社会混乱を起こすことさえ可能である。

このように多様化した通信ネットワークの中でセキュリティの侵害が生じた場合，それをいかにして防ぎ，回避し，回復するか，そしてそれをどこに通知するか等を管理する技術が必要になって来るであろう。このとき，この管理を一箇所で集中管理するのか，分散管理するのか等どこでどのように分担するのか，これから検討しなければならない。

さらに，セキュリティの侵害があったときの責任あるいは保障といったこと等をも考慮してセキュリティ関連技術を考えていかなければならない。

〔参　考　文　献〕

1) 伊藤裕幸，「コンピュータ不正とその対策」，清文社，ＰＰ.91－137，昭和５７年８月。

2) D.Kaufman and K.Auerbach, "A secure, national system for electronic funds transfer," in Proc.1976 AFIPS NCC, Vol.45, AFIPS Press, Arlington, Va., PP. 129－138。

3) 中川由章，「コンピュータ症候群－犯罪・災害・プライバシー対策」，税務経理協会，昭和５７年９月。

4) 鳥居壮行，「検証・日本のコンピュータ犯罪」，コンピュータ・エージ社，昭和５７年５月。

5) 「コンピュータクライム」，インタープレス，Vol.1，№7，昭和５７年１１月。

3.7 暗　　号

3.7.1　暗号の現状

近年暗号技術は従来の秘密のイメージを離れてコンピュータ・セキュリティ技術の柱として研究，技術開発が進んでいる。特にアメリカにおいては通信回線の開放，金融機関に対する規制緩和等により必要性が高く，普及しつつある。一方日本においては暗号はほとんど実用の域に達していない。暗号化が最も要求される為替データにおいても生データが通信回線上を流れている現状である。しかしながら電電公社職員の通信回線盗聴による詐欺事件，通信回線開放を契機に暗号の実用化，普及の気運が高まりつつある。

3.7.2　暗号の方式

(1)　簡易暗号方式および高度な暗号方式

暗号の普及を防げている最大の原因はコストである。特に端末系に暗号を適用する場合，低コスト化が必須条件となる。犯罪者の立場に立つと，簡易でも暗号を採用したシステムに対する犯罪の費用対効果比は著しく悪化し，犯罪の抑止力となる。コンピュータ犯罪の事例によれば，一般の犯罪と異なり犯罪者側よりむしろコンピュータ・システムが犯罪に対し無防備である事が犯罪のきっかけになっている場合が多い。

しかしながら攻撃的な犯罪に対しては簡易な暗号方式では十分でない。重要な情報に対してはコストをかけ高度な暗号方式を採用すべきである。

(2)　ソフトウェアによる暗号方式

ソフトウェアによる暗号方式は最も低コストである。特に一般性のある言語で作成すれば端末一台当りのコストは無視できる。又低コストが目的ではなく，アルゴリズム上ハードウェア化できない暗号方式を採用したためソフトウェアによる場合がある。ソフトウェアによる暗号方式の欠点は以下の通りである。

① 低処理能力

② インテリジェンシーのない端末には適用できない。

しかしながら低コスト暗号の普及，高度な暗号への適用の重要性から開発が急がれる。

(3) ハードウェアによる暗号方式

ハードウェアによる暗号方式は付加型と組込み型が考えられる。

① 付 加 型

現システムを変更することなく付加できる暗号装置で現在商用化されているものもあるが，低コスト，高機能化が望まれる。低コスト化では暗号鍵のみならずアルゴリズムが非公開になってもよい。その場合解読の危険度が増すが，他のセキュリティ対策（例えばキャッシュ・カードの暗証番号のチェック法）を併用し普及を重視すべきである。また一方では強固な暗号方式の暗号装置の開発も望まれる。

② 組込み型

組込み型は標準化システムに採用されるとコスト，スペースを余り必要としない。汎用性を考慮すると標準化されたアルゴリズムが望ましく，当面 DES 方式が主流になるだろう。DES 方式の高速で低コストのＬＳＩの開発が望まれる。

3.7.3 暗号鍵の配送・管理技術

(1) 暗号鍵の配送・管理技術の重要性

いづれの暗号方式においても暗号鍵の配送とその管理には問題点が多い。難易の程度の差はあるが，いづれにしても暗号鍵が漏れてしまうと暗号としては役立たない。さらに致命的な欠点として暗号鍵（正確には復号鍵）が漏れた又は盗まれたという事が発見できない事である。その為に暗号鍵はある程度使用したならば更新する必要があり，暗号鍵の配送，管理を複雑にしている。又それ故強固で簡単な暗号鍵の配送，管理技術の開発が望まれる。

(2) 暗号鍵の配送

暗号鍵を安全に配送する方法としては通常の通信路と異なったルートを使用し，暗号鍵を分割して配送するのが最も安全である。暗号鍵配送ルートとしては電気通信路の他に郵便，人手による配送ルートが用いられている。鍵の分割配送も一部では使用されつつある。

通常の通信路を暗号鍵配送ルートとして使う場合，暗号鍵をマスタ鍵で暗号化するのが安全である。このままでは堂々巡りになってしまうが強固な暗号方式，注意深い運用法によって現実には使用可能と思われる。ただし，この様な場面にこそ処理能力は低いが強固なアルゴリズムを実現できるソフトウェアによる暗号方式が採用されるであろう。強固な暗号アルゴリズムが期待される。

暗号鍵の配送法は運用上，技術上どのレベルまで標準化するかが問題である。

(3) 慣用暗号系

慣用暗号系ではユーザ数がnのとき，暗号鍵の数がn(n−1)／2となり，暗号鍵の配送，管理は，センタ方式が簡単ではある。しかしセンタ故障の場合安全な通信路は確保できなくなる。

センタを複数個分散して配置し，迂回ルートを設ける方式が有力になると思われる。この方式ではセンタ故障もシステム・ダウンとはならず，管理すべき暗号鍵も階層化することにより実質nに比例するものと考えられる。

(4) 公開鍵暗号系

公開鍵暗号系においては慣用暗号系より暗号鍵配送，管理の問題は少ないとされている。しかし次の点で問題があり今後の研究が期待される。

① 暗号鍵を公開するからセンタ方式となる。慣用暗号系と同様にセンタ故障の問題と，暗号鍵の更新時全ユーザに配送する必要がある。

② 暗号鍵を公開しているので偽電文の送信等は自由である。従って暗号化しても相手確認に対しては強化されたことにならず，別途対策が必要である。

③ 慣用暗号系に比較して通信文の挿入が行なわれ易いが，これは相手確認の技術により解決できると思われる。

(5) 暗号鍵の管理責任

前述した様に暗号鍵が漏れてしまうと暗号は役立たないが，暗号システムを現実に導入する場合問題となるのは，暗号鍵が漏れた場合の責任の所在である。

慣用暗号系では送信側，受信側共，共通の暗号鍵を用いるので鍵の管理責任は双方にある。万一暗号鍵が漏れた場合どちらから漏れたのか不明である。将来回線の使用が自由化されるに伴ない，異企業間通信は急速に普及するであろう。システムを全面的に慣用暗号系で構築した場合の安全性について研究が必要である。

一方公開鍵暗号方式やＭＩＸ方式では，暗号鍵（復号鍵）の管理責任者がはっきりしているので，慣用暗号系の様な問題は生じない。暗号鍵管理上，公開鍵暗号系やＭＩＸ方式の方が社会的に受け入れ易いので研究開発の促進が望まれる。

3.7.4 暗号と相手確認

ネットワークにおける相手確認は重要で，暗号の使用法により解決すべきである。相手確認法に欠点があると暗号鍵を盗まれる事にもなるので細心の注意が必要となる。

(1) 慣用暗号系

パスワードによって相手を確認する方法では通信傍受者に暗号を教える様なものである。また自分が受信者の場合，相手が偽の通信相手だとしたら暗号鍵は返事によって盗まれるだろう。この問題に対しては事前の通信文で暗号鍵を互に交換する等が考えられるが，研究が必要である。

(2) 公開鍵暗号系

公開鍵暗号系ではデジタル署名を利用すると相手確認手続が比較的簡単と

思われる。慣用，公開鍵暗号系共相手確認技術は研究途上にあり，これからの成果が期待される。

3.7.5　ファイルの暗号化

ファイルの暗号化は通信系の暗号化程進んでいない。しかしながらコンピュータ犯罪の事例によると通信回線の盗聴，挿入よりファイルの盗難，コピー，不正使用の方が多い。以下ファイルの暗号化の特徴を述べる。

① ファイルの保護期間が長い。
　このためにホストのマスタ鍵の変更があり得る。

② 他のホストが使用する場合がある。

③ ホストで暗号，復号を行なえばファイル装置側では暗号機能を持つ必要がない。

上記①，②からファイル上に暗号鍵を書き込む必要があり，暗号鍵を暗号化するマスタ鍵管理の問題がある。一案として暗号化された暗号鍵を解読する復号鍵を，システム内にあるマスタ鍵とユーザ鍵に分割する方法が考える。マスタ鍵を変更する場合ユーザ鍵も更新し，新マスタ鍵と新ユーザ鍵によって以前の復号鍵が生成できる様にする。ファイルに暗号鍵を書き込む際の問題としてファイルは破損する可能性がある。このため，暗号鍵の書き込みは多重化しておく必要がある。また③からは暗号化鍵の配送の問題はなくなり，従ってファイルの暗号化においては公開鍵暗号方式は適さない。

ファイルは一般にファイル形式が公開されているので，データのヘッダ部のみならず全データを暗号化することが望ましい。このためには暗号化の速度が重要であり，高速ＬＳＩの開発が期待される。

ファイルの暗号化と，他の本人確認手段との併用によりファイルに対する犯罪に対しては，かなりの効果を発揮すると思われる。

3.7.6　暗号の多重化，複合化技術

(1)　暗号の多重化

暗号は一般に多重化することにより強固なものとなる。多重化は単に多重化する方法と他の条件との整合を考慮する方法がある。前者は同一の暗号機構を繰り返し使用できるので安価で実用的であろう。後者はシステムを構築する際各レベルで暗号化を実施し，総合的に強固な暗号体系を実現する方法である。一例としては通信プロトコルの各層において暗号を採用する方法で，他の例としては管理責任を持った者がそれぞれ暗号化を行なう方法である。回線提供者，VAN業者，ユーザ毎に責任分担に応じた暗号を採用するならば，全システムを熟知した犯人でないと破れないので強固な暗号システムとなる。これからの開発が期待される。

(2)　暗号の複合化

暗号方式はアルゴリズム，構築法共に種々あるが上記暗号の多重化において，できる限り種々の暗号方式を組合せた方がよい。さらにコンピュータ・セキュリティの他の技術（例えば本人確認技術）等と組合せると効果がある。またコンピュータ・システムの信頼性に関する部分を暗号化に利用すれば安価で強固なシステムが構築できる。2重化された回線による暗号鍵の分割配送，誤り検出・訂正回路と暗号LSIの複合化，予備機による暗号処理等が開発実用化されるであろう。

3.7.7　暗号の標準化

暗号はその性質上標準化には限界がある事を認識すべきである。標準化の期待できる技術としては，アルゴリズム，ファイルの暗号化，通信プロトコルの低レベルでの暗号化，端末等に使用される暗号，コンピュータ・メーカによって提供される標準暗号システム，回線提供業者の標準暗号システム等がある。暗号の標準化は一通りに絞る必要はなく，適用分野，アルゴリズム毎に標準があってもよい。ユーザはシステムに適した標準システムを採用すると共にアプ

リケーション・レベルの暗号，暗号鍵の配送，管理上の適用方法等は独自の方法を研究，採用すべきである。特に厳重な管理を要するマスタ鍵の取扱い，暗号システムの初期化，更新方法等は運用細則まで決める様な標準化をすべきではない。

しかしながら標準化によって製品は低価格化し，普及していくのであるから標準化すべき技術の範囲を決め標準化を促進すべきである。

3.7.8　今後の暗号政策

暗号は歴史上，軍，政府の意向を受けその研究成果が公開されることはなかった。DESの標準化以来，その重要性と共に研究成果が公開される様になったのは喜ばしい。

しかしながら近年アメリカにおいて，暗号の研究発表，外国への暗号関連製品の販売に規制がある様であり，アメリカ以外の国でも制限があるだろう。従って我国においてはアメリカの後追い研究だけではなく，独自の研究も必要と思われる。今までの暗号の研究はほとんど外国において行なわれている。幸い我国においても暗号の研究は盛んになりつつあり，成果が期待される。

3.7.9　今後の期待

(1)　新アルゴリズムの開発

一般に技術は先端技術が進んでいる程その裾野も広くなり，ますますその技術は向上する。各種の適用形態を考慮すると現状の暗号アルゴリズムでは不十分である。暗号化，復号化が簡単で，強固な暗号アルゴリズムが必要である。

(2)　故障，デバッグに対する対策

暗号システムにおける故障時には通常システムと異なった問題が発生する。例えば予備機の互換性等がある。また導入後プログラムにバグが発生するとデバッグが必要となり，暗号システムが公になる可能性がある。この様に

通常運用時と異った業務の場合，システム介入法を十分検討しておく必要がある。

(3) 高速暗号 LSI の開発

暗号の普及を妨げている原因の一つに処理能力の低下がある。特に公開鍵暗号系においては処理能力が大きな問題である。高速暗号 LSI の開発が期待される。

(4) デジタル化による暗号適用の拡大

近年通信網においてはデジタル化技術は急速に進歩している。今後は従来考えられなかった領域まで暗号が採用される可能性がある。既に警察無線において暗号化の研究が進められており，ホーム・バンキング，キャッシュレス社会，高度通信システム，衛星通信，衛星放送，プライバシー保護等に対する暗号技術の開発も推進する必要がある。さらに，現状では暗号の適用方法は明確ではないが，OA，光通信，ホーム・エレクトロニクス等も考慮しておく必要がある。

3.8 入出力装置

オンライン・システムでは，端末は，基本的データの投入口であり，業務的には極めて重要な部分である。この部分の設計次第で，応用システムの効率・操作性の大半が決まってしまうからである。また，端末は台数が多くなるため，システム全体に占めるコストも無視できない。従って従来は，操作性·効率(コストを含む)を重点にした開発が行なわれてきた。

一方，日本で発生した犯罪には，入力段階における不正がかなり含まれており，何らかの対策が望まれている。操作性がよく処理効率の高い端末は，同時に，不正も効率よく実行できる可能性がある。このような状況のなかでは，操作性と効率を重視した従来の端末を見直す必要があるのではないかとも思われる。入力段階での不正を防止できれば，過去に発生したコンピュータ犯罪のかなりの部分を防止できることとなり，その効果は大きい。本節では，マンマシン・インタフェースとしての入出力装置と不正との関係の分析を試みる。

3.8.1 端末の新技術と不正の関係

従来はキーボード・スイッチ，CRTディスプレイ及びプリンタが主要な端末の構成機器であった。近年，技術の進歩により音声入出力装置，OCR(印刷文字および手書き)，液晶パネル等が実用化され構成機器として普及してきた。音声入力装置の応用として声紋チェック等，不正防止と直接関係する技術も研究されているが，これについては，3.1節を参照されたい。

新しい構成機器の出現により，端末の形態が多様化してきているが，これがすべて，操作性と効率重視のみで構成されるようになれば，不正防止にとってむしろマイナスになる危険性がある。

難しいと言われていた音声認識や文字パターン認識は，使用場所と使用方法を限定すれば，そのいづれも今日では実用レベルにある。しかしながら，認識技術だけでは不正防止に効果があるかないかは，分らない。問題は，不正判断プロセスも含めたその利用方法にありそうである。新しいタイプの端末出現

の機会に，不正防止に効果のある入力方式とは，どのようなものか，研究する必要があるだろう。

3.8.2　入力段階における不正防止の方向

入力段階の不正防止を入力装置そのもので行なおうとする発想には限界がある。あらゆる入力装置は，人間の意志を正確にコンピュータ本体に伝えるためにある。たとえその意志が不正を働こうとする意志であっても，コンピュータに伝えなければならない。不正な意志表示を許可するかしないかは，コンピュータ本体の判断[*1]の問題であって，端末の問題ではない。

端末にとって重要なのは，コンピュータ本体が不正を判断するのに必要な情報をなるべく多く入力させることである。一方，同時に使用される出力装置では，コンピュータの判断結果（あるいは処理結果）を，すべての関係者に正確に伝える機能を持っていることが重要である。

現在までの技術開発は，この目標に向って行なわれてきた。問題点は，機器の実現技術にあるのではなく，使い方にある。使い方のテクノロジー（technology）と言うよりは，テクニック（technic）と言うべきかもしれない。

例えば，入力装置については，先に述べたように，コンピュータが不正を判断するための情報が，漏れなく入力されるように，機器が配置され操作されるような，端末を構成するテクニックを研究する必要があると言うことになる。

3.8.3　入力設計の見直し

従来の入力設計目標は，入力の簡易化と効率化にあった。このために，入力項目は極限まで削減し，さらに同一項目のダブリ入力等は，可能な限り追放し

＊1：マイクロ・プロセッサの開発により端末部で判断される場合もある。しかしながら，マンマシン・インタフェースと直接関係しない項目として，この節では端末のインテリジェント化を無視して検討を進める。

てきた。しかしながら，このような設計思想では，一度正確に入力すれば，以後間違いが発生しないというメリットは生じるものの，コンピュータ本体にとっては，あまりにも情報が少なく不正の判断は不可能となり，単なるデータ処理装置に甘んじてしまうという問題がある。

これに対し，効率を犠牲にしてエラーや不正の発見に努力してきた実例もある。多くのバンキング・システムでは，個々の伝票を入力した後，さらに，人手により別途集計した合計値を入力して，コンピュータによる個々の伝票の集計結果との一致を調べるという方式が従来から使用されてきた。これは，一種のダブリ入力を行なうことにより，エラーや不正の発見をしようとするものである。

このように，不正を防止するためには，入力の簡易化／効率化という従来の目標を修正し，不正発見のための入力方法（同一項目の冗長入力等）を研究する必要があるだろう。

例えば，一枚の伝票のすべての項目を同一人が一度に入力するのではなく，複数人が別々に入力する方法が考えられる。この結果，操作性や効率の悪化が生じる可能性があるが，それは技術でカバーすべきであり，又可能であろう。

3.8.4　入力方式のパターン化

入力方式は実際のシステムでは，システム全体の処理形態と密接に関係している。もし，入力方式を改善して，不正防止を図ろうとするならば，システム全体的な視野で検討する必要がある。従って，最適入力方法は，応用システム毎に異なることになり，一般化は難しい。

例えば，1人しか駐在していない営業所の端末に対し，複数人で入力する方式を用いることは，無意味である。あるいは，コマンドを入力する都度本人確認を行なうTSSでは，いくら不正防止のためとはいっても，利用者は耐えられない。

すなわち，応用システム毎に最適な端末構成を設計する必要があるが，これ

は大変な作業である。そこで標準構成モデルをいくつか設定しておき，業務や処理形態に応じて選択する方法が考えられる。一種のガイドラインである。これまでも，端末供給者によって，モデル構成が発表されてきたが，それは，入出力装置本位のものであった。例えば，「キーボードとCRTで，これだけの業務が可能で，プリンタを付加すれば，さらに業務拡大が可能」という具合である。

ここで言う標準構成とは，入出力装置を基準にするのではなく，業務や処理形態を基準として設定するものである。「入金伝票の入力では，CRTとキーボードを用い，別にチェック用として管理者用のプリンタを設け，次のような操作で行う。」というようなものである。この標準構成モデルは，業務や処理形態によって分類した応用システム本位のものとし，使用機器の備える機能を明確にし，さらに標準的な運用も示したものである。

応用システムの設計者は，この標準構成モデルをそのまま取り入れるのではなく，これを参考に，さらに自分達のシステムに適合するよう修正を施して採用するのである。端末供給者（メーカ）は，この標準構成モデルに使用される機器を，一つの目標として開発を進めることも可能だろう。

3.8.5　標準構成端末モデルの一例

ここで，標準構成端末モデルの一例を示す。このモデルは，まだ充分検討されていないことをあらかじめお断りしておく。ここで取上げる例は，商社等の売上げ伝票の入力を想定したもので，金額が大きく件数が少いという仮定をしている。

図3－7のように起票の後入力を行なうが，この起票は入力のための準備であるので，起票せずに直接入力することも可能である。CRTとキーボードを用いて入力ミスを取り除いた後，これを管理者端末へ送る。管理者は，これをCRT上でチェックした後プリント・アウトし，これに印を押して，正式伝票とする。同時にコンピュータへの入力も完了したことになる。

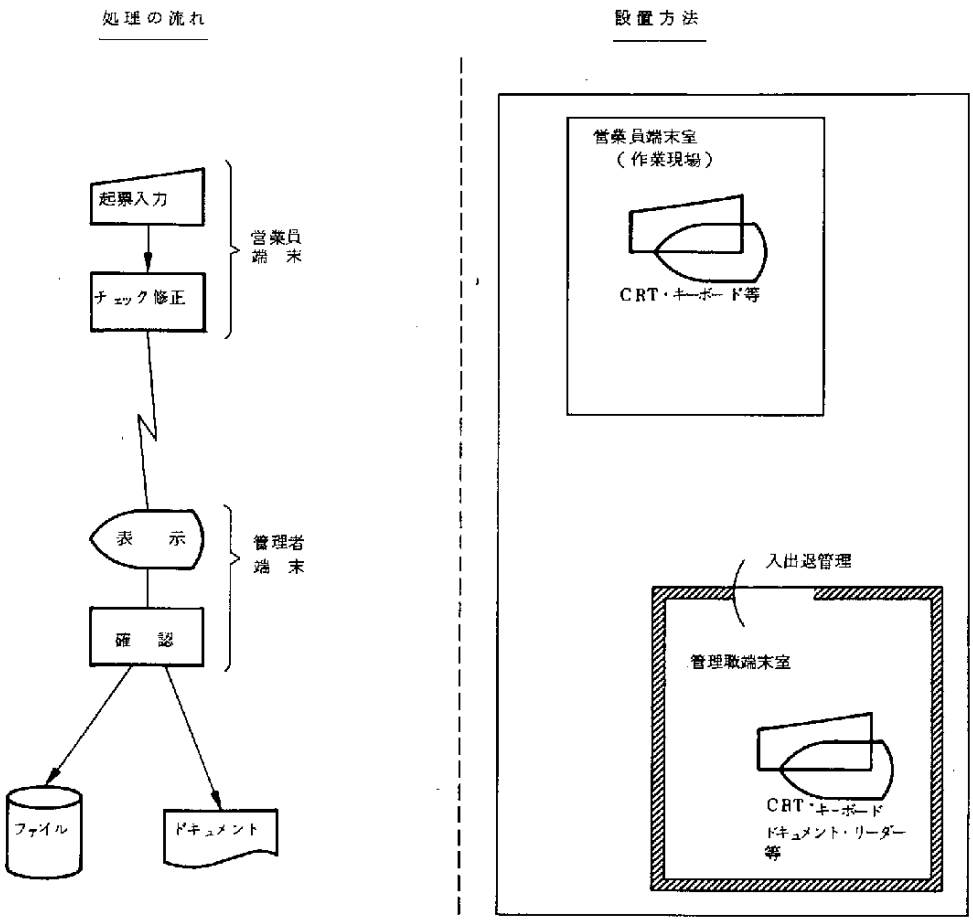


図３－７　　端末構成の一例

① 管理者チェックで問題があれば，営業員端末（原データ入力端末）へもどして，修正を求める。

② 管理者チェック後（確認後）に誤りがあることが判明した場合は，管理者端末で修正する。図３－８のように，この時，ドキュメント・リーダーで，プリント・アウトされた正式伝票を読ませることで，コンピュータ・ファイルから該当伝票を呼び出す。訂正の後，読ませた伝票には，訂正情報がプリントされ，訂正伝票となり２度と使用できないものとなる。さらに訂正後の正式伝票が，図３－９のようなフォーマットでプリ

ントされる。同時に，コンピュータのファイルも訂正される。

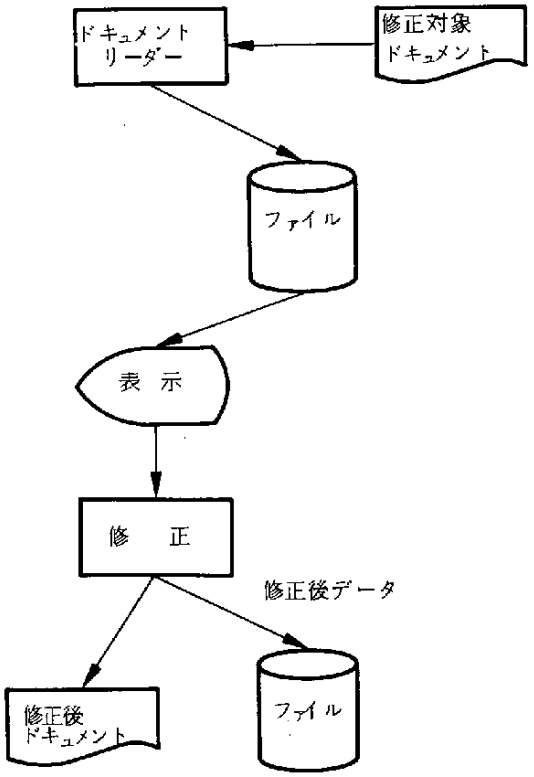


図３－８　　管理者確認後修正

○　○　伝　票

—	150, 000	100	15, 000, 000
—	600, 000	100 ~~50~~	60, 000, 000 ~~30, 000, 000~~
合　計			75, 000, 000 ~~45, 000, 000~~

訂正が表示される。

図３－９　訂正された伝票の印字例

③ この構成では，営業員の端末では，原データの入力はできるが，管理者確認後の修正はできない。一方管理者の端末では，表示とプリント・アウトおよび管理者確認後の訂正のみ可能となっている。（機能分散）

④ 管理者確認後に訂正を行なうと，ハード・コピーに訂正状況が表示される。

このモデルでは，入力完了後の不正な修正が困難なように，たとえ行なっても容易に発見できることを目標にしている。また，コンピュータ・アウトプットを正式書類にすることにより，コンピュータ・ファイルと正式伝票の内容が一致するようにしている。管理者は訂正が自由にできるが，証拠は確実に残る。従来は，端末のジャーナル，センタのジャーナル等，極めて見にくい部分に証拠が残されたが，このモデルの出力様式では，それに加えて伝票そのものに証拠が残るので発見しやすいだろう。

管理者確認後，売上げ伝票に関連する伝票（出庫指示，納品伝票，請求書等）が自動的に発行されてしまうと，これの回収は自動的にはできないため，関連する伝票が発行されたら，修正不可にすべきである。また，原データそのものが不正であり，管理者がそれに気付かない場合，および管理者自身の不正については，防止できない。別の方策を検討する必要がある。

このパターンの入力方式では，管理者の作業量が増えるので，最初に仮定したように，件数が少く取扱金額の大きい処理に適する。

3.8.6 高度な検出機構

この項で提案する技術は，いづれもコンピュータが不正を判断するための有力な情報を検出する機構である。実現上の問題点が多数あり，ただちに実用化することはできない。しかしながら，前述の入力方式の改善では防止できないような犯罪に対して特に効果があると予想される技術であるので，今後，基礎的研究を行ない，実現に努力すべきだと考える。

(1) 印鑑の読取り

コピーのように白黒で無階調に読取る技術は，既に実用化している。今後の課題は，色情報および明度情報の読取りである。但し，これについても実験室で読取る技術はある。問題点は，いかに長期安定性を確保し，安価な機器を開発するかにある。

一方，読取ることはできても，その情報を充分生かすことができないという問題がある。印鑑の自動照合のために読取るのであるが，照合プロセス[*1]（高度パターン・マッチング）の開発が遅れている。この進歩が期待される。

(2) 手書き伝票の読取り

前記(1)と同様に，読取り技術の問題点は比較的少い。問題点は，むしろその情報を解析するプロセス側にある。ここでも高度なパターン・マッチング技術の開発が期待される。手書き伝票リーダー[*2]を用いれば，専任オペレータが不要となり，それだけエラーや不正の機会が減少するし，端末構成の自由度が増大するメリットがある。さらに，製品コードではなく，製品名で入力すること等も可能で，管理者チェック等で有効と思われる。

(3) 偽造伝票の検出

高度な入力機能として，偽造伝票の検出がある。ここでいう偽造とは，改ざん，修正および不当にコピーすることを言う。読取り機構の課題は，前述(1)と同様に，色情報と明度情報の読取りがある。さらに平面的ではなく，立体的に読取る必要がある。これは，切り張りや砂消しゴム使用を検出するために必要である。さらに，表側だけでなく裏側を読取ることも重要であろう。

立体的に読取ると伝票表面の光沢が検出でき，砂消しゴム使用はすぐ発見できる。しかしながら，このような解析を行なうプロセスは発達が遅れている。このようなプロセスは，パターン理解技術もしくはさらに高度な画像

＊1：押印された印鑑の一部が欠けていると自動照合が難かしい。
＊2：このリーダーは，数字だけでなく漢字も入力可能とする。

理解技術＊1 と呼ばれる。この技術においても，問題点の多くはプロセス側にあり，その方面の発達が期待される。

(4) 精神的動揺の検出

不正乗車は，切符の有無よりも改札を通る時の態度の変化で発見される方が多いと言われている。不正を行なう時，微妙な精神的動揺があるからだと言われている。これを科学的に応用した電子機械として，「うそ発見器」がある。端末でも，特殊なセンサを備え精神的動揺をキャッチすれば，不正発見に役立つのではないだろうか。手作業の時代には，人間がこの役割りを持っていた。いわば，人間並みのチェック能力を持った端末である。現状では，まったく夢の話であるが，科学技術の進歩は不可能を次々に可能にしてきた事実もあるので，必ずしも実現不可能とは言えない。もっともプロの犯罪者には役立たないかもしれない。

＊1：3次元画像理解

3.9　運用自動監視

国語辞典には，監視とは「注意して見張ること」と記述してある。見張った結果，異常を発見すれば，警報を発し，さらに異常状態を正常状態に戻す作業を行なう意味である。コンピュータ・システムにおける監視では，一般的に警報を発する機能として定義されており，警報を出した後は，処理を停止させるのが普通である。正常状態に戻す作業はリカバリ処理として定義されている。本節では，監視を次のように定義した。

> 監視……各種の情報から異常状態が起きたかどうか判断し，異常状態であれば，警報を出し，処理を停止させる機能。異常状態とは，あらかじめ予想されていない状態とする。

次に，各種の情報の収集方法および判断方法の違いによって，次の３つの監視方式に分類して，検討を進めることにした。

①　自動監視
②　半自動監視
③　手動監視

①の自動監視は，判断するために必要な情報の収集および判断を自動的に（無人で）行なう方式であり，②の半自動監視は，判断するために必要な情報は自動的に収集し，判断そのものは人間が行なう方式である。③の手動監視は，すべてを手作業で行なう方式である。

本節では，最初に従来の監視方式のまとめを行ない，次に，より高度な監視の実現および自動化の実現のために解決しなければならない問題点および解決案（提案）について分析を試み，その結果をまとめた。

3.9.1　自動監視

自動監視は，防御機構の最終的目標の一つであり，もっとも有効な機能であ

る。自動監視は，人間のような判断ミスがなくパワー（処理能力）が大きく，手作業では不可能な全数チェックも可能である。しかしながら，現存するコンピュータの知能が低いため，高度な判断ができないという問題がある。以下に現在実用化している自動監視について簡単にまとめる。

(1) センタの自動監視

センタのハードウェア障害の監視を行なう。コンピュータ本体に障害監視用のサブプロセッサを付加し，マシンの運転状態をチェックする。障害が発生すると，センタに警報が出されるが，多くの場合，センタとマシンを製作したメーカとを通信回線で結び，メーカの保守管理部門に直接警報が通知される。こうして，障害復旧の迅速化に役立っている（リモート監視・診断と呼ばれる）。

警報の通知と共に，原因追求のための情報が送信されており，メーカ保守員は，この情報を用いて故障原因の分析を行なっている。今後の課題は，故障原因の自動分析である。

(2) ネットワークの自動監視

通信回線の異常を検出し，さらに自動的に対策を行なう。検出できる異常状状態としては，回線故障（切断等）と回線品質低下があり，いづれの場合も，発生と同時に他の回線に切り換えて通信路を確保する。既に実用化されている。現状では，故障原因は障害記録や各種の測定器による測定および実際の回線をチェックする（人間の目で確める）ことによって，分析されている。原因の自動分析には，困難な課題がたくさんあると言われている。

(3) 入出力の自動監視

磁気ディスクや磁気テープ等における入出力エラーの監視である。警報は主にシステム・コンソールに出される。この技術は，かなり以前から実用化されており，近年はかなり高度化されている。例えば，エラーが発生するとただちに警報を出すのではなく，自動復旧処理を何回か行ない，それでも回復できない時警報を出すようになっている。障害記録も，すべてのエラーおよび復旧を

記録する方式，最終的に復旧できなかったエラーのみ記録する方式，品質をチェックするために，発生回数をカウントする方式等，各種の記録方式がある。しかしながら，原因の自動分析には至っておらず，各種の診断コンサルテーション・システム（半自動診断）が提案されており，一部実用化されている。

(4) ジョブ実行の自動監視

最新のオペレーティング・システム（ＯＳ）では，ユーザ・ジョブの実行状態を，いろいろな角度から監視している。

例えば，ジョブの実行時間，使用メモリ，使用する入出力機器，ＯＳへの不当なアクセス等を監視している。警報を発する条件は，①システム的に決定されているものと，②ユーザが警報を発する条件を選択できるものとがある。ＯＳへのアクセス等は，前者の方式で制限され，実行時間の制限等は後者の方式で制限されるのが普通である。

この監視の問題点は，ＯＳ側で考えている監視内容とユーザ側で考えている監視内容が，しばしばずれていることである。例えば実行時間制限は，無限ループ防止策として使用されることがある。しかしながら，この場合実行時間が制限されるだけで，無限ループそのものを防止していることにはならない。今のところ，ジョブ実行の自動監視では，プログラムの実行ロジックそのものを監視する方法はない。

(5) 本人確認とアクセス・コントロールによる自動監視

通常これらを自動監視とは呼ばないが，見方を変えて，ファイルへのアクセス等を監視し，契約違反（システムへ登録した以外のアクセス）があれば，それを阻止する機能として理解すれば，自動監視である。詳細については，3.1節および3.2節を参照されたい。自動監視という観点での問題点は，警報を出した原因が自動分析できないことである。いわゆる不正アクセスが発生しても，「不正アクセスがあり阻止した。」という記録が残るだけで，何故不正アクセスを行なうに至ったかという原因までは自動分析できない。

(6) 処理中断時間の監視

主に端末での処理状態を監視するもので，一定時間以上処理が中断されると，その処理を無効にする。例えば，ＴＳＳ端末では一定時間オペレーションがないと強制的にログオフを行なう。この監視の目的は，オペレータが端末から離れたことを検出することである。ログオフを忘れて食事へ行ったこと等を検出し，オペレータが不在の間に行なわれる不正を阻止するために，強制的にログオフする。

このような一定時間以上新しいアクションがないことを検出して異常をキャッチする方法は，いろいろな分野で利用されている。この方式の問題点は，一定時間以上アクションがない原因を，自動分析できないことである。センタで端末をこの方式で監視した時，端末からの信号が一定時間以上中断しても，端末の故障か回線の故障か多くの場合判断できない。

(7) リミット・チェックによる自動監視

主に数値入力項目の内容を許容基準と比較し，基準を超えた時警報を出す手法である。応用システムに組み込まれて，広く利用されている。これの効果は大きいと言われている。

リミット・チェックの問題点は，許容基準の決定方法である。許容基準は，異常検出の精度に直接関係する重要な値であるが，経験的に決定されているのが実状である。工場等の製品検査では，この許容基準を定量的に（理論的に）決定している。いわゆる商用システムでは，許容基準の理論が作りにくい面もあるが，過去の実績を統計処理する等の方法が考えられる。

次に，時間の要素を加える問題がある。現状では，一処理（１トランザクション）での許容値をチェックしているが，これを一定期間内の総量チェックに拡大する必要があるだろう。このようになると，経験的に許容値を決定するのが難かしくなるので，許容基準自動設定の研究が望まれる。

自動監視に共通した問題点であるが，許容基準を超えた場合，その原因は自動分析できないという問題がある。原因追求が何故重要であるかは，

3.9.4で述べる。

(8) 入出退自動監視

センタあるいは端末室への人間の出入を監視するシステムである。多くの場合，ＩＤカード，パスワード等による本人確認と，自動ドアーおよび記録システムで構成されている。

このシステムの問題点は，本人確認方式とピギーバック*1である。その他，消耗品の搬入やゴミの運び出しという問題もある。

このシステムを導入し，部分的に管理の無人化を行なった例はあるが，全面的な無人化を行なった例はない。入室チェックで自動的に入室禁止になった場合，システムは，その原因を判断できないので，例えばＩＤカードを忘れた者は入場することができない。この救済のために人間が必要である。（本当の社員であるか等をチェックする。）すなわち，ここでも原因を自動分析できないという問題がある。

3.9.2 半自動監視

半自動監視は，自動監視に比べると，はるかに能率は落ちるが，はるかに高度な判断が可能である。警報を出すかどうかの判断を人間が行なうからである。従って原因究明も可能である。半自動監視では，①コンピュータ処理を一時中断して，人間が判断を行ない，その後処理を再開するリアルタイム型と，②すべての処理が完了してから行なうバッチ型（監視というより監査に近い）がある。

(1) リアルタイム型半自動監視

① リミット・チェックとの組合せ

リミット・チェックで正常処理がチェック・アウトされることが実際に

＊1：ピギーバック：室への入室資格を有する者といっしょに出入りしてシステム・チェックを逃れる犯罪手法である。ピギーバック本来の意味は，トレーラートラックを車ごと鉄道貨車に載せて，戸口から戸口まで自動車と鉄道で一貫輸送する輸送システムのことである。米国で発達した。

は起きる。このような処理を救済するため次のような方法を用いる。チェック・アウトされた処理を管理者が判断し，正常であると認められるならば特殊な追加入力（物理的キーやＩＤカードを用いる場合が多く，監査キーと呼ばれる。）を行ない，再処理を行なう。この特殊な追加入力は，通常リミット・チェックのロジックをバイパスさせる効果を持っている。このようにして，リミット・チェックの持つ欠点を人間がカバーするシステムを構成する。この方式では，管理者の不正を阻止できないという新たな問題が発生してくる。

② 管理者による入力データ・チェック

現場の営業員がデータ入力を行なった後，管理者専用端末へ編集出力し，管理者チェックを行なって確認し，正式入力とする方式である。この方式では，管理者端末への出力の時，マスター・ファイル等にある入力データに関連した情報といっしょに入力データを表示できるので，管理者の判断資料を多くできるメリットがある。しかしながら，この方式は，あまり応用システムに組み込まれていないようである。管理者専用端末というコスト上昇要因および管理者への情報過多の問題，さらに効果に対する疑問があるからであろう。管理者の不正をチェックできないという問題もある。

(2) バッチ型半自動監視

判断資料の収集および編集を自動的に行ない，判断は人間が行なう方式で，監視というより，監査に近い性格を持つ。ほとんどのコンピュータ・システムで実施されている監視方法で効果も大きいし，実績もある。問題点は，能率の悪いことである。全処理をチェックするのは不可能に近く（実行しているシステムもある。），通常，サンプリング・チェックが実施されている。コンピュータ的監視と，非コンピュータ的監視がある。

① コンピュータ的監視

ジャーナル・データ，ロギング・データ等の内容を判断材料として，不正処理の検出を行なう。これの最大の利点は，不正の発見だけでなく，原

因の追求も可能な点にある。人間の持つ経験や高度の連想能力が大きく寄与するからである。

第１の問題点は能率の悪さである。自動分析の技術が期待される。第２の問題点は，しばしば重要な情報の記録が欠落していることである。例えば，ファイルへのアクセスは記録されても，そのファイル内のレコードへのアクセスは記録されないという問題がある。第３に，ユーザ作成のロギング収集プロセスは，ＯＳなみに保護されていないことである。例えば，ＳＭＦ（ System Management Facility ）はＯＳと同等に保護されている。しかしながらユーザ作成の業務処理取引記録プロセスは，ユーザ・プロセスと同等の保護しか受けられない。ユーザ作成のロギング収集プロセスを他の業務処理プロセスより，強力に保護するために，効率のよいマルチ・レベルＯＳが期待される。

② 非コンピュータ的監視

テープ・レコーダやビデオ・レコーダによる監視である。航空機では，ボイス・レコーダとして実用化されており，事故原因追求の際の重要な資料となっている。ビデオ・レコーダは，カメラと共に，銀行，スーパー，商店，倉庫および端末室等に設置され，不正防止や犯人逮捕に大きな貢献をしている。今後の課題はコンピュータとの連動であろう。

3.9.3 手動監視

資料の収集から判断まで，すべて人間が行なう監視で，監査との区別はほとんどない。代表例は，プログラムのチェックである。これについては，3.5節で詳述してある。システム監査も現状ではこの分類に入る。従って問題点は，非能率でありデータ収集を自動化して半自動化を達成することが課題であろう。

半自動化を達成する既存のツールとして，例えばＩＴＦ（ Integrated Test Facility ）がある。しかしながら，このツールにはテストを行なう前に慎重な準備が必要でかつテスト終了後に，これまた慎重な後処理が必要という大き

な欠点がある。業務処理に悪影響が出る可能性が極めて大きいという理由で，ほとんど利用されていない。この辺の改善が急務でないかと思われる。

3.9.4 問題点のまとめ

(1) 原因の自動分析

自動監視に共通の課題である。ここで，何故原因の分析が重要かを述べておく。

自動監視では，エラーや不正を自動的に阻止するので結果として，エラーや不正は発生しない。一方，犯罪者は新手を求めて試行錯誤を繰り返す。この時，警報は鳴っても結果として犯罪は起きないので，注目されることはない。ついに，システムの欠陥を発見した時，犯罪は成功してしまう。そこで，警報が出た時の原因分析が重要になる。この分析によって，犯罪者が何を狙っているか，ある程度予測ができるからである。犯罪者が成功する前に，システムの改造ができる可能性さえある。

さて，現状では警報が出るたびに原因追求を行なっていては，人手が足りないので，警報を出さない自動監視もある。ファイルのアクセス等の管理では，不正アクセスが発生しても，処理を停止して記録をとるだけで，警報は出さない。犯罪が発生しなければ，センタ管理者がこの記録を使用して，原因追求を行なうこともない。

(2) 半自動監視の能率改善

これも大きな課題であり，自動化が望まれる。自動化すると，チェック人の不正もなくなる。実際の犯罪でも管理者（チェック人）の不正があり問題になっている。従って，自動化されれば，大きな効果がある。その他，全数チェックが可能になるという効果もある。

(3) 手動監視の能率改善

手動監視の自動化には，大きな未解決の問題が多数あり，早急な自動化は難かしい。従って，半自動化による能率改善が妥当な対策と考えられる。

3.9.5　問題点解決のための課題

(1)　データ収集の効率化

必要な時に必要なデータが短時間で入手できるのが理想的である。コンピュータ処理でこの理想を実現するための条件は，

- 必要なデータの所在がはっきりしていて，すぐアクセスできる。
- データを自由に編集して出力できる。

の２点である。通常，データはファイルの中にある。必要なデータは，その中の一つである場合が多い。ところが，コンピュータによるデータ管理は，ファイル単位であり，アクセスの単位はレコードである。この結果，必要なデータにアクセスするためには，目的のデータが存在するファイルを知ると共に，そのファイルのどのレコードにあるか，およびレコード・フォーマット（ファイル・フォーマット）を知ったうえで，プログラムを作成するか汎用の編集ツールのパラメータを作成しなければならない。問題点は五つある。

①　ファイル名

目的のデータが格納されているファイルを捜す場合，ファイル名を見て捜す。しかしながら手作業時代のファイル（帳簿）の内容と，コンピュータ・ファイル（磁気ディスク等）の内容とは，同じ名前のファイルでもかなりの違いがある。手作業のファイルでは，経理用のファイル等，どの会社でも似たようなものであった。コンピュータ・ファイルでは，このような統一性がなく，ファイル・フォーマットを調べて目的のファイルを捜さなければならなくなった。

②　レコードへのアクセス

目的のレコードへアクセスするのに検索キーが必要である。すべてのファイルに共通の検索キーがあれば，容易にアクセスできるが，実際には，すべてのファイルの検索キーは異なると考えねばならない。

③　データへのアクセス

ファイル・フォーマットは，システム設計書に書かれている。これは，しばしば不完全であったり，記述に誤りがある。プログラムを見て確認する必要がでてくる。

④　プロセスの問題

苦労して捜したデータは，実際は入れ物（データ・エリア）である。そこに入っているデータが有効であることを確認するためには次の作業を必要とする。

- システムのプロセス・フローを調べて，ファイルに有効データが格納されることを確認する。システム設計書のチェックでは不完全な場合がある。
- そのファイルが処理済であることを確認する。

⑤　編集ツール

コンピュータ・ファイルのデータは，目で直接確認できないので，編集出力が必要である。プログラムを作成し，デバックを行ないマシン実行をしなければならない。汎用の編集ツールやＴＳＳを用いても，「ボタン一つで出力」には程遠い。

これらの問題点の解決法として，例えばファイルの統一化がある。ただし，これまでの標準化運動の成果を考慮すれば，近い将来の解決策にはならないように思われる。むしろデータベース的発想の方が実現性がある。各ファイルについてフォーマットを記述した辞書（サブ・スキーマに相当）を作成する。この辞書を用いてアクセスの自動化を行なう。ただし，辞書と実際のファイル内容を一致させるため，何らかの方法で辞書とファイルを連動させなければならない。

監視用データ（監査用と言うべきかもしれない）を出力するプロセスをシステムに組み込む方法もある。しかしながら，実際に監視を実施しないと必

要なデータがはっきりしないという問題があり，応用システム完成後に容易に新たなプロセスを組み込む技術が是非とも必要である。また，この方式は不要なデータを多数出力してしまうという問題もある。詳細にチェックするかどうかを判断するためには，１０のデータが必要であり，詳細にチェックして最終的結論を得るためには，１００のデータが必要であるというのは特に珍しいことではない。しかしながら，このシステムでは常に１００のデータを出力してしまう。

(2) 監視用データのインプット

これまでの監視では，業務処理のために入力されたデータを利用して，判断を行なってきた。しかしながら，監視に必要なデータのすべてが，業務処理のために入力されるデータ中にあるとは限らないので，監視用データの入力が研究課題になると思われる。手作業によるデータ収集では，欠落しているデータを直接作業現場へ行って収集することができる。自動化を進めると，このようなことができなくなるので，重要な問題である。オンライン・システムでは，数万キロメートルも離れた作業現場を設置することが可能である。このようになると，現場へ行ってデータ収集を行なうことは，大きな負担になるという問題が，手作業でも発生する。

別種の問題として，オペレーティング・システムのロギング・データ[*1]詳細化という問題がある。例えば，レコード・アクセス情報が必要になるかもしれない。

(3) オペレーティング・システムのマルチ・レベル化

監視プロセスの自動化を進めると，このプロセス自身を保護しなければならないという新たな問題が起きる。第１にプロセス自身を保護する必要があり，第２に悪用されないようにしなければならない。現在の多くの汎用オペレーティング・システムは，２レベルの保護体系（システムとユーザ）しか

＊１：広い意味で，監視プロセスに対するオペレーティング・システムによる監視用データのインプットと考えられるので，取りあげた。

ない。第3のレベル（場合によっては第4のレベルも）が必要である。悪用に関しては，本人確認技術の高度化（3.1参照）が必要で，さらに運用方法の研究も必要となろう。

(4) 判断プロセスの改善

リミット・チェックにおける許容基準の自動設定および時間要素の追加が検討テーマとなろう。難かしいのは，許容基準の自動設定である。一案として統計手法の応用（経験値の理論化とも言える。）がある。業務処理に直接関連した分野であることも分析を難かしくしている。

(5) その他の課題

警報発生原因の自動分析，および，ビデオ監視あるいは音監視とコンピュータとの連動がある。いづれも当面は解決困難な課題で長期的検討が必要であろう。

① コンサルテーション・システム

警報発生のパターンとその原因を，知識として蓄積しておき，原因分析時のコンサルテーションをさせる方法が考えられる。その他，不正のパターンを知識として蓄積しておき，コンサルテーションさせる等の応用も考えられる。

② 音の活用

画像情報に比較すれば，音情報は情報量が少なく，解析技術も進んでいる。加えて，コストも安価である。ビデオとコンピュータの連動よりも，マイクロフォン（音のセンサー）とコンピュータの連動の方が実現性が高いのではないか。複数のマイクロフォンを利用した音場検出の面で進んでいるし，音声認識，話者検出等の波形解析技術もある。今後の研究が期待される。

4. 将来システムにおけるセキュリティ

本章では，今後のコンピュータ・システムの利用形態である「コンピュータ・ネットワーク・システム」をテーマとして，将来新たに発生が予測されるセキュリティ上の問題点について検討した結果をまとめた。

ＬＳＩを始めとする各種のコンピュータ技術の長足な進歩によって，これまでＳＦ小説の中の空想でしかなかった「夢の文明社会」が現実のものになりつつあり，人類は計り知れない幸福と永遠の繁栄を得ることができるだろうと言われている。しかし，専門家や技術者は，コンピュータ・システムの利点や効果だけを強調する傾向があり，その陰に隠れた暗い部分については，これまであまり議論されなかったようだ。コンピュータ・システムは，良い点ばかりでなく，不都合な点もいっしょに持ち合わせていることは，これまでの経験で充分過ぎる程分っている。将来のシステムでも，大きな効果と共に大きな危険性があることを充分予測でき，解決方法を検討しておかなければならない。

当プロジェクトでは，最初に具体的な問題点を研究することとし，その結果をここにまとめた。4.1では，将来の汎用ネットワークにおける問題点を提起し，4.2ではネットワークを利用して高度なシステムへ発展して行く応用システムにおける問題点を提起した。今後これらの問題点を，さらに詳細に研究し，対策案を策定する必要がある。

4.1　ネットワーク・システムから見た技術

コンピュータ・システムは，事務・電算機（コンピュータ）部門から，販売・製造・総務等の第一線に使用範囲が拡がり，計画／運営に対し発言の中心が第一線の人々に移ってきている。さらに，データ通信の自由化，通信網の発達，コスト・ダウンによって，企業グループや（含む中小企業・子会社）異企業が通信ネットワークによって結ばれる，コンピュータ・ネットワーク・システムの方向へと進んで行きつつある。

また，コンピュータ・システムの中心（コントロールの中心部門）も，事務・電算機部門から，委員会型[*1]に移り，さらに，組合／協会等と変って来ている。

将来は，コンピュータ・ネットワーク・システムも異企業間のシステムへと拡大して行き，システムは，統一的管理が難しくなる方向へ動きつつある。

4.1.1　閉じたシステムから開いたシステムへ

今までのように，事務・電算機部門で，コンピュータ・システムの建設と運用が，しっかりと把握され，コントロールされ，責任者も明確であり，責任者（あるいは所轄部門）がシステムをコントロールできる場合を，例えば現在の特許システム，バンキング・システム，生産管理システムや医療システム等を，われわれは「閉じたシステム（Closed System）」と呼ぶこととした。

一例を図４－１に示す。

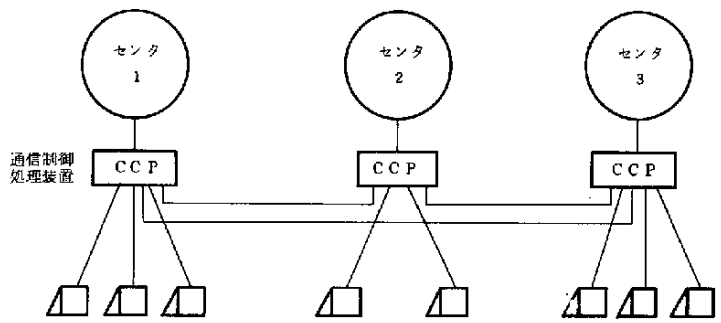


図４－１　単一サービスの複数センタ間の通信

＊１：合議制によって問題解決する集団責任制を表す。電算機利用委員会等

一方，コンピュータ・システムがネットワーク化され，異企業が加わってくると，責任部門を組合や外部団体で持つようになり，誰が責任者なのか責任元が決まっても，コントロールが十分きかなくなってくる。システムが，複雑化，ネットワーク化し，責任体制がはっきりしなくなって，アンコントロール型になって来る。これを，われわれは「開いたシステム（Opened System）」と呼ぶこととした。例えば，ネットワークに接続された端末相互間で自由に仕事を行なったり，電子メール等は開いたシステムの例と言える。

開いたシステムの一例を示すと図４－２のようになる。

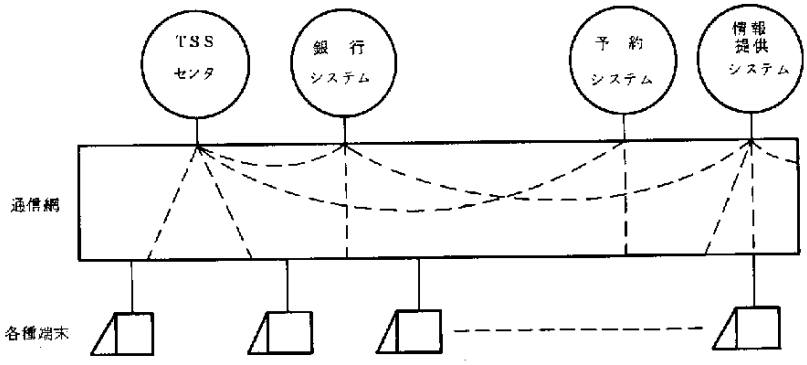


図４－２　統合データ通信網

この閉じたシステムと開いたシステムは，カテゴリーを明確に区別することはできない。

閉じたシステムと開いたシステムは，連続的であり，中間段階にいろいろのレベルのシステムが存在する。システムは，最初の構築後も，新しい企業が参加したり，参加している企業が個々にまたは企業間で，端末間（パソコンを含む）で，新業務を追加することによって，しだいにマンモス化／拡散して行く。

システムが銀河宇宙のように膨張して行くに従って，コントロールのレベルが悪化し，アンコントロールの方向へ進んで行く。このためシステムの安全性，すなわちセキュリティが守りにくくなり問題となってくる。図４－３は発達して行くネットワーク・システムを示す。

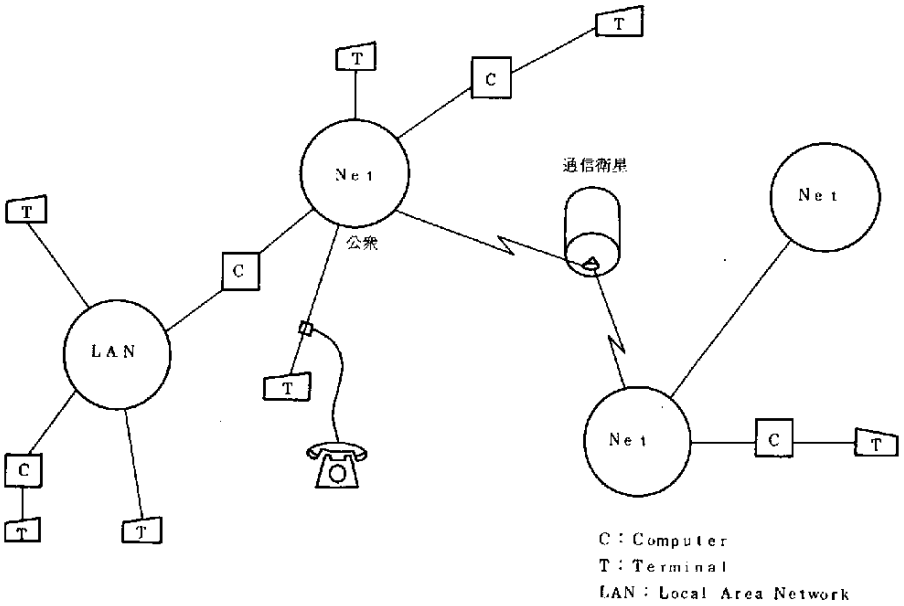


図４－３　発達するネットワーク

しだいに複雑化し膨張して行くコンピュータ・ネットワーク・システムのセキュリティが，これからの重要な課題となってきた。以下，本節では極限まで開いたシステム[*1]について分析を行なった。

4.1.2　想定される脅威

セキュリティ対策の第一歩は，問題点の解明である。ここでは，具体的な問題点の解明を試みる。より進んだ開いたシステムの利用形態は，商取引等をネットワークを通じて，電子的に処理する形態（ペーパーレス処理）が考えられる。ここでは，このようなシステムを，Electric Transaction Transfer System（略してＥＴＴＳ）と呼ぶことにした。

ＥＴＴＳに近い機能を持つ汎用システムは，現在はまだ構築されていない。従って，本項で示す想定犯罪も現状では起り得ない。ここでの分析対象は，かなり先の時点での問題であることを，あらかじめお断りしておく。

＊１：これに近いシステムは，１９８０年代の終り頃に現れると言われている。

(1) 高速処理により拡大する影響範囲

ＥＴＴＳ（Electric Transaction Transfer System）利用目的の一つは，処理の迅速化にあると思われる。ところが処理の迅速化が，事故が起きた場合，影響範囲を拡大させるという問題がある。

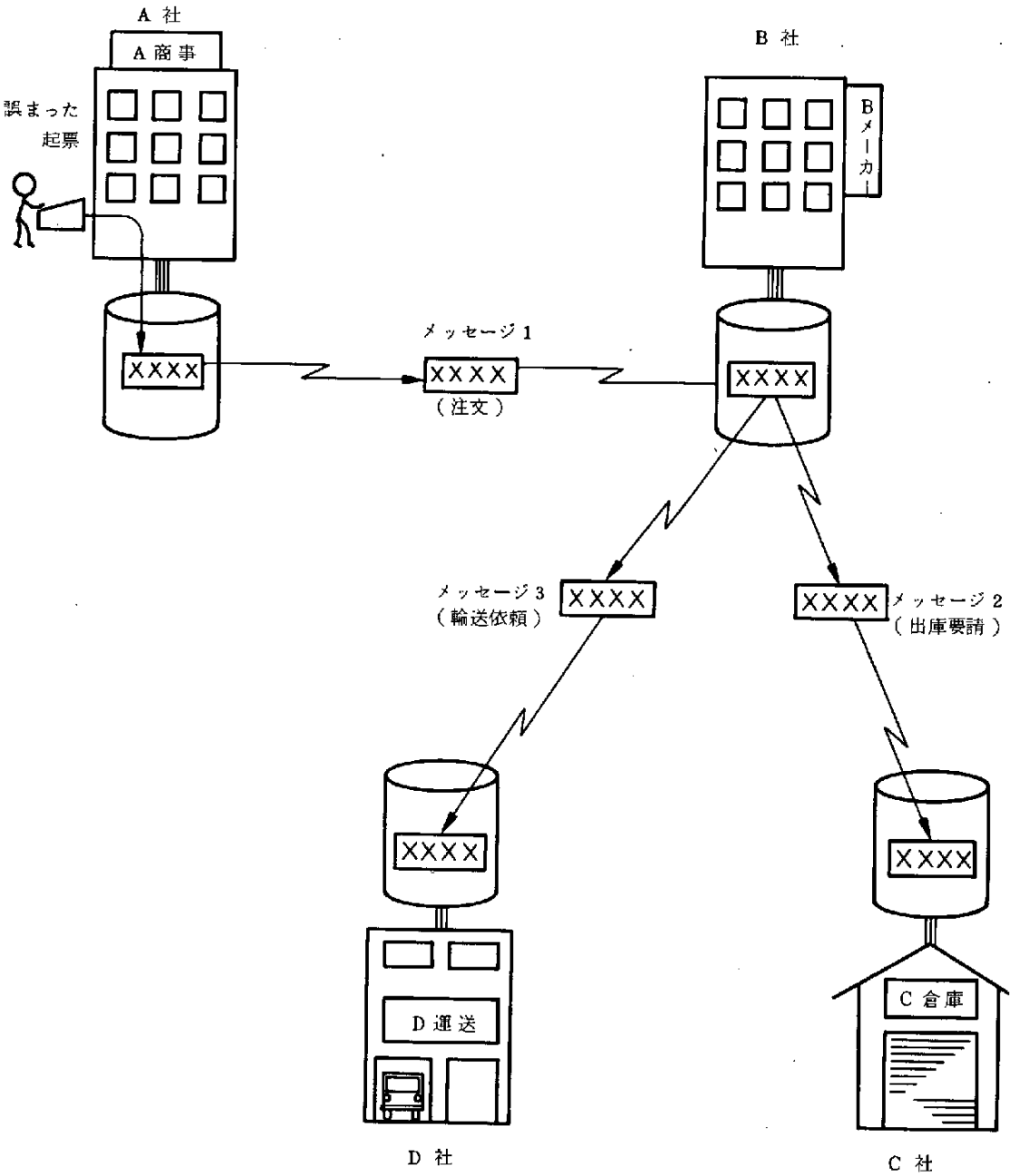
Ａ社のある営業員が，Ｂ社に対する注文伝票の起票を間違え，そして数時間後にその事実に気が付いたと仮定しよう。

手作業の時代なら，恐らく彼は，その伝票をすぐ回収して訂正できただろう。現代のように機械化されていても，多くの場合伝票は社内にあり，容易に訂正できると思われる。

しかしながらＥＴＴＳでは，数時間後には既にＢ社へ送付され，さらに，Ｂ社からＣ社，Ｄ社へ送付されていることが充分考えられる。Ｂ社ではＡ社から受け取った注文メッセージ内容に誤り（例えば商品名等）があるかないかチェックする方策はない。そのため，Ａ社から受け取った注文メッセージは正しいとして，ただちに商品発送の準備をするのは自然であろう。そこで，Ｂ社にそのメッセージが到着すると，ただちにＣ社，Ｄ社に対応するメッセージが送付されることは充分考えられる（以上図４－４を参照）。

このように誤まった起票に基づくメッセージが社外に流出すると，訂正はほとんど不可能になる。なぜなら，ある起票（インプット）を訂正する場合，それに関連するすべてのメッセージおよびファイルを訂正しなければならないが，メッセージは社外に流出し，訂正すべきファイルも社外にあるからである。

図４－４では，Ａ社で行なわれた起票を訂正するために，Ａ社のファイルだけでなく，メッセージ１，２，３およびＢ社，Ｃ社，Ｄ社のファイルを訂正しなければならない。Ｂ社，Ｃ社，Ｄ社はＡ社の被害を受けることになる。これらのことは，もし悪意のメッセージが一通でも流されれば，たちまち数社が被害を受けることをも意味する。



・メッセージ１，２，３は互いに関連している。
・A社のファイルを訂正する場合はＢ，Ｃ，D社のファイルも
同時に訂正しないと、つじつまが合わなくなる。

図４－４　ＥＴＴＳ（Electric Transaction Transfer System）
の業務処理例

(2) 悪徳会社の詐欺

ＥＴＴＳ（Electric Transaction Transfer System）ですぐ思いつく問題は，回線盗聴や介入である。これも大きな問題であるが，さらに大きな問題として，ＥＴＴＳに接続している悪徳会社の存在がある。この会社に対しては，暗号化もメッセージ認証も効果がない。

悪徳会社はＥＴＴＳに接続させなければ良いのだが，これが難かしい。ある日突然，優良会社が悪徳会社に変身することがあるからである。例えば，ちょっとした判断の誤りから多額の負債を抱え，これを取りもどすため詐欺に走ったケースが実際にある。このような当初は信用のあった会社は，容易にＥＴＴＳに接続できる。詐欺が発生しなければ，悪徳会社への衣替えを知る方策はなく，詐欺発生前にＥＴＴＳから締め出すことはできない。

ＥＴＴＳに接続している善良な会社は，詐欺メッセージを受け取った瞬間に詐欺と分ることは，ほとんどなく，ずっと後になって，初めて被害にあったことが分る。悪徳会社は，この時間差とＥＴＴＳの高速処理を活用して詐欺を行なう可能性がある。ＥＴＴＳのセキュリティ対策が不完全であれば，詐欺の事実さえ，はっきりしなくなる可能性もある。

① メッセージの改ざん

悪徳会社Ａ社は，善良なＢ社に大量の商品注文メッセージを送った。運悪く，その直後にその商品の価格が大暴落してしまい，Ａ社は大損失を出した。このような仮定をしよう。現在であれば，Ａ社は泣く泣く大量の在庫（デッド・ストック）を抱えなければならない。しかしながらＥＴＴＳでは，違った展開になる。

すなわち，注文しなかったことにする。そのためＡ社は自社のファイルやジャーナルを改ざんする。一方，Ｂ社には正しい記録（ジャーナル）が残されているが，これはＢ社が自身に都合が良いように改ざんしたことにする（以上図４－５を参照）。

かくして，商品を受け取らず支払もしない悪徳会社Ａ社を，善良なＢ社

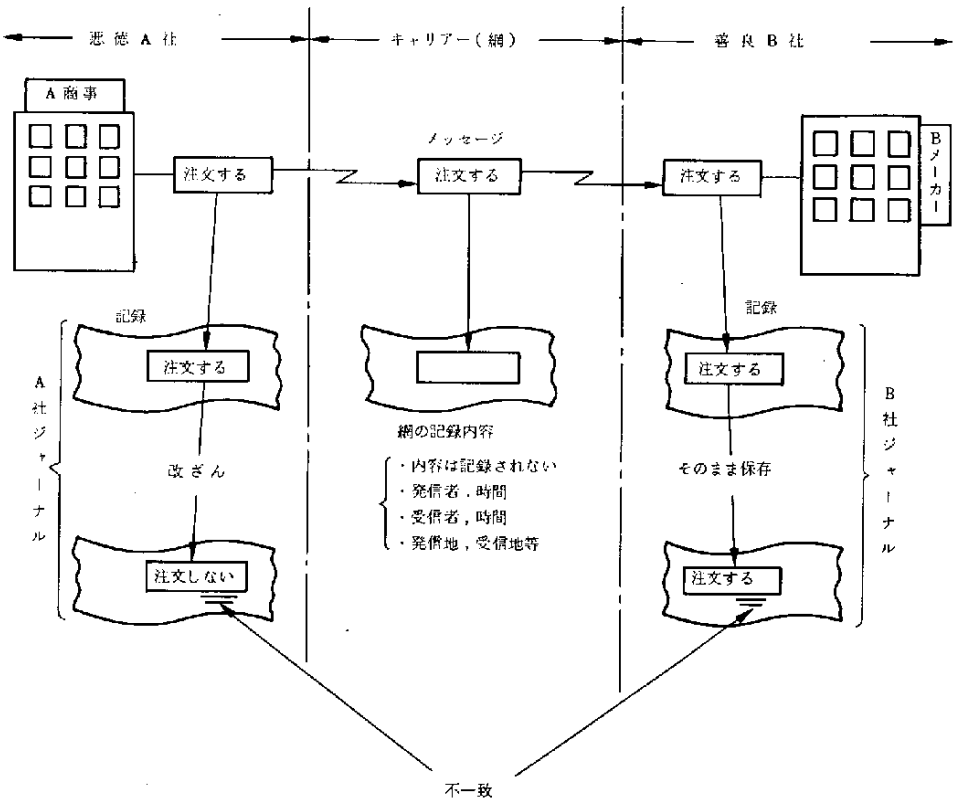


図4－5　メッセージの改ざん

は，裁判所へ告訴するだろう。ここで，A社，B社の言い分をまとめてみよう。

（A社の主張）

・A社のジャーナルは，「注文しない」を記録している。「注文する」というメッセージは送っていない。B社の記録は改ざんによるもので，ありもしない取引を作った。

・通信網の記録は「　　」だけで参考にならない。

（B社の主張）

・A社が，A社のジャーナルを「注文する」から「注文しない」に改ざんした。B社のジャーナルは正しい。取引は存在している。

・通信網の記録は参考にならないというが，メッセージは存在したことを表わしている。その内容がA社は「注文しない」だと言うが，通常こんなメッセージは使用しない。従って，このメッセージは「注文する」の筈だ。

この論争の原因は，信用のおけるメッセージの記録がどこにもないことである。A社，B社のジャーナルは，共に自社に都合の良いように改ざん可能であり，通信網にも内容の記録がない。もし通信網で内容の記録を行なえば，プライバシの侵害になる恐れがある。

ＥＴＴＳにおけるメッセージの記録方法は大きな問題である。

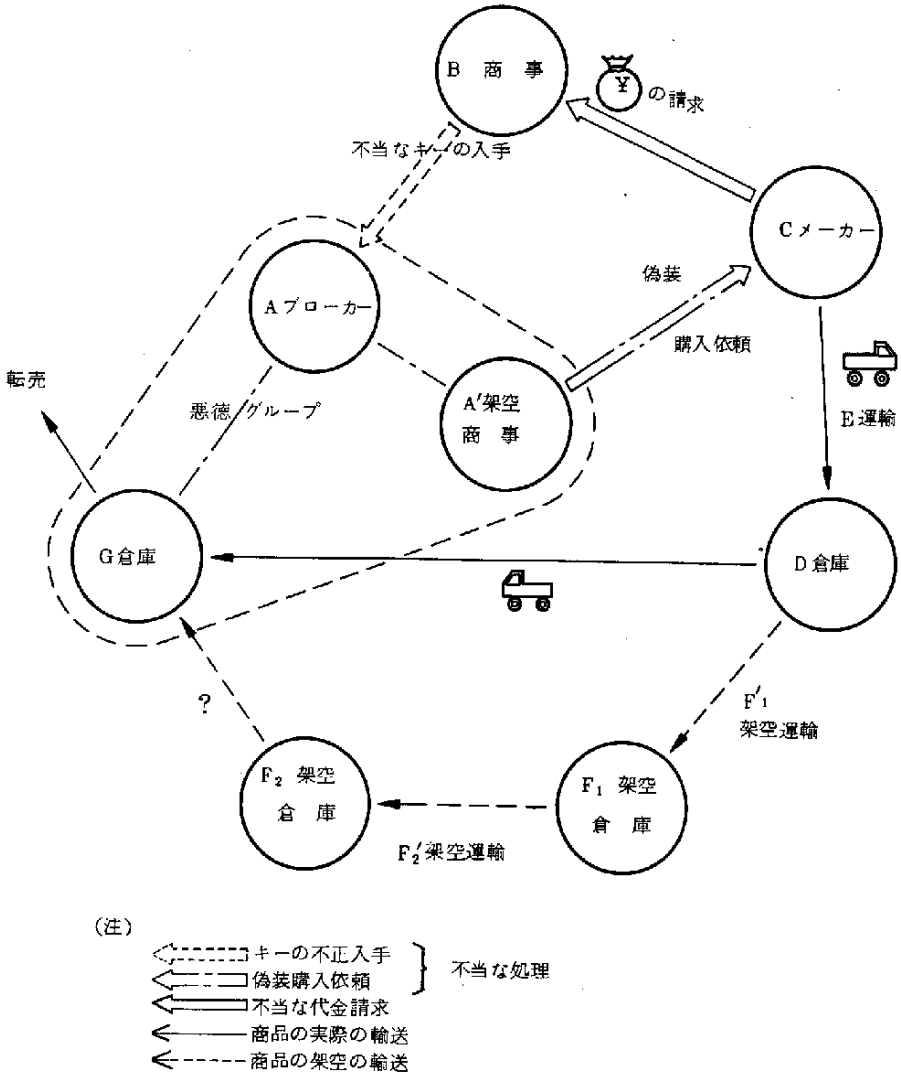
② デジタル署名の悪用

ＥＴＴＳでは，デジタル署名が相手の確認，自分宛の確認のために有効だと思われる。デジタル署名では，キーの管理が重要であるが，ＲＳＡ暗号等を使用するデジタル署名では，論理キー（数字を組み合わせたキー）なので，盗まれても分らない。このためトラブルが発生する可能性がある。

悪徳会社A社は，たまたまB社の秘密キーを入手する機会を得た。そこでB社と偽って，C商事へ商品注文メッセージを送り，D倉庫へ運ばせた。支払はもちろんB社である。さらに架空会社A′社を使用して，商品をF_1倉庫，F_2倉庫，G倉庫へ転送し，転売した。ただし，実際の輸送は，D倉庫からG倉庫へ直接行ない，F_1倉庫およびF_2倉庫へは書類上（ファイル上）で輸送しただけである。ＥＴＴＳでは，このような架空の輸送も簡単にできる（以上図４－６を参照）。

決済期日が来て，B社は買った覚えのない商品の代金請求に驚いた。さて，犯人を割り出すことが可能だろうか。

注文メッセージが公衆網から発信されていれば，ニセ・メッセージがA′社から発信されたのは分らないが，商品がD倉庫へ輸送されたことはすぐ分かる。そこでD倉庫に協力してもらえれば，A′社とF'_1社の存在は分る。



B商事のキーを不当入手し，B商事と偽って，注文メッセージをC社に送り，商品の詐欺を行なう。

図4－6　キー盗難時のトラブルの一例

但し，機密保護を理由に，具体的な社名を教えてもらえない可能性もある。しかしながら，A′商事やF′1 運輸が分ったところで，これらは架空会社なので調査のしようがない。さらにF1 倉庫が発見できても，さらにF2 倉

庫，F'_2 運輸等の架空会社を調査しなければならない。

これらの困難を越えて悪徳ブローカーA社を発見しても，A社がそのような詐欺行為は断じて行なっていないと主張すれば，責任追求はできない。なぜなら，キーがなければデジタル署名ができないからである。従って，キーを盗んだ現場を押さえるか，A社から確かにニセ・メッセージが出たという証拠のどちらかが必要になる。いづれも実証が難かしい。

デジタル署名のキーは，現在の印鑑やサインと同等であるから，盗難に遭ったことがすぐ分る必要がある。従って，論理キーよりも物理的なキーの方がよいのではないか。

次に，書類システムでは，ニセ書類判定のために印鑑以外[*1]に肉筆部分の筆跡鑑定も使える。（タイプの場合は，タイプの字形も手掛りとなる。）ＥＴＴＳでは，このような手掛りがない。

(3) 詐欺の自動化

ＥＴＴＳ（Electric Transaction Transfer System）では，可能な限りのセキュリティ対策は行なわれるので，デジタル署名のキーを盗むことやジャーナルの改ざん等は，そう簡単ではない。

これに対し，日常業務として入出金を行なっている企業の経理課等の社員は，簡単に金を盗むことができる。ただし，すぐ発見されてしまうので通常盗む者はいない。しかしながらＥＴＴＳでは以下のような問題がある。

悪徳経理課員Aは，端末機に詐欺プログラムを仕組んだ。明日，銀行へ1通のメッセージを送るプログラムである。そのメッセージは，会社の金をAが設定した架空口座に振込依頼をするメッセージである。当日，アリバイ作りのためAは会社を休んだ。その間に端末機は自動的にメッセージを発送し，横領を自動的に行なった。あらかじめ連絡してあった悪徳仲間が振込まれた金を，さらにB金融へのサラ金返済という形で転送した。翌日出勤したAは

＊1：厳密に言えば，朱肉の色，タイプのリボンの色，さらに伝票用紙そのものも，判定材料になる。

プログラムを消した（以上図４－７を参照）。

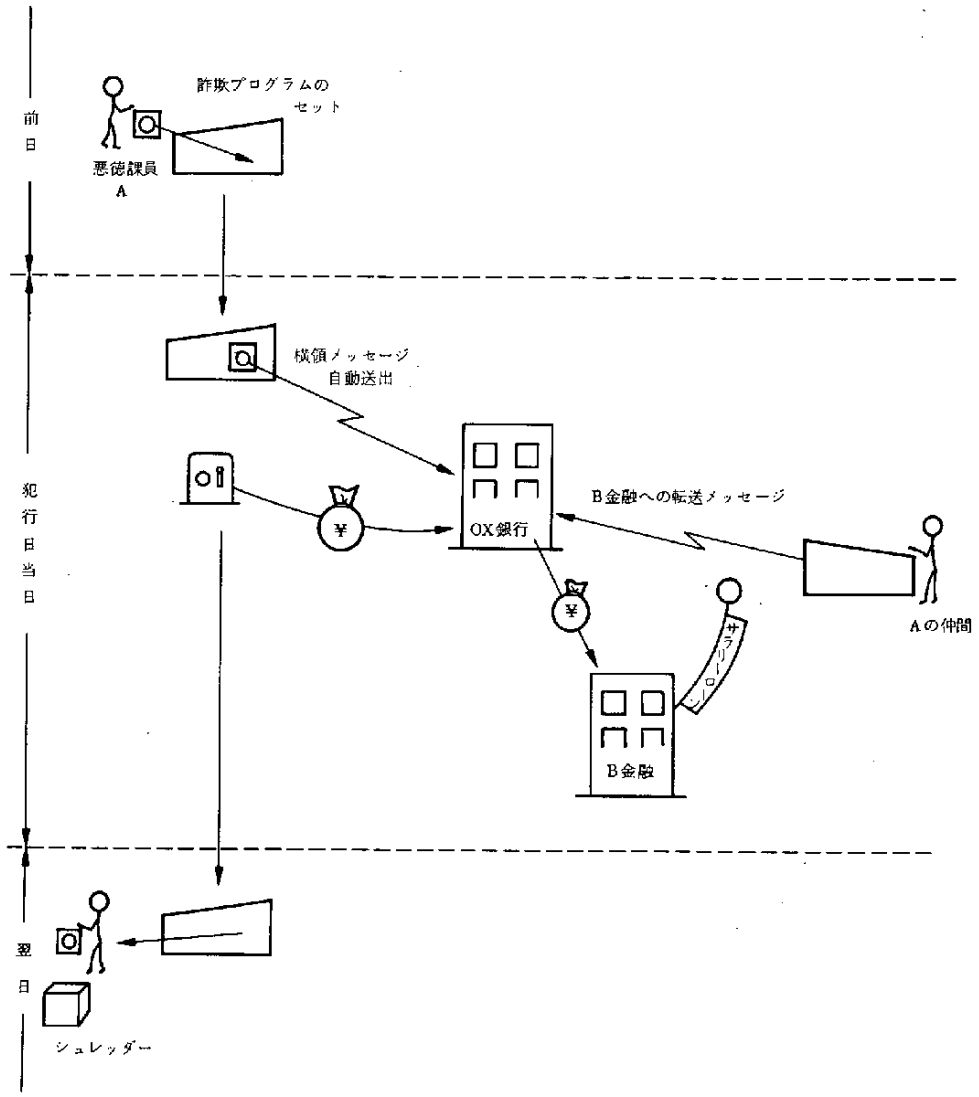


図４－７　詐欺の自動化の一例

横領メッセージは悪徳経理課員Aの名前で発送されたことは明白である。しかしながら，彼にはアリバイがある。このアリバイを崩すためには，詐欺プログラムのセットの事実を証明しなければならない。でなければ，誰かがAの名前を使って横領したことになる。過去に詐欺プログラムが動いたこと

を証明することは難かしいし，それが分っても誰が仕組んだか調べることも難かしい。むしろ，プログラムが簡単に交換できないことが重要である。フロッピー・ディスクでプログラムをロードする方法では問題が多い。

尚，善意の第3者に現金が渡れば，取りもどすことはできない。図4－7のケースでは，B金融から横領金を取りもどすことはできない。

(4) いやがらせ

B社の社員Aは，端末を使って在宅勤務をしていたが，B社の事業縮少のあおりを受けて，解雇されてしまった。怒り心頭にきたAは，B社に対し「いやがらせ」を計画し，プログラムを作った。

そのプログラムは，B社にメッセージを送るものである。ただし1通ではない。何通もくりかえし送るものである。内容は無意味のメッセージである。

B社は，Aを首にした時，彼のＩＤ番号やパスワードは消してしまった。従って，Aの「いやがらせメッセージ」は，すべて無視される。しかしながら，コンピュータは，どんな無意味なメッセージでも受け取って最低1度はチェックしなければならない。ところが，Aの「いやがらせメッセージ」は何通も来る。このため，通信回線がAの「いやがらせメッセージ」で占領されてしまう恐れがある。もしそのようになったら，B社のＥＴＴＳ（Electric Transaction Transfer System）機能が麻痺してしまう。

ＥＴＴＳに，このような端末を接続させない対策が必要ではないか。

4.1.3 問題点と対応策

(1) 問題点の提示

書類をコンピュータ・ファイルに置き換えることは，現在では，大きな疑問もなく行なわれている。そして，書類の代わりに磁気テープを運ぶことも行なわれている。この段階までは，単純に記録媒体を紙から磁気ディスクや磁気テープへ置き換えただけと考えられる。

しかしながら，通信回線を通じて社外へデータを送るようになれば，単純

な置き換えとは言えなくなる。通信回線上で磁気テープそのものを送ることはできないので，その内容のみ送る。いわば，コピーを送ることになる。書類システムではオリジナルそのものを送るのに比べて大きな違いがある。そこで，コピーにオリジナルと同等の機能を与えなければならない（図４－８参照）。

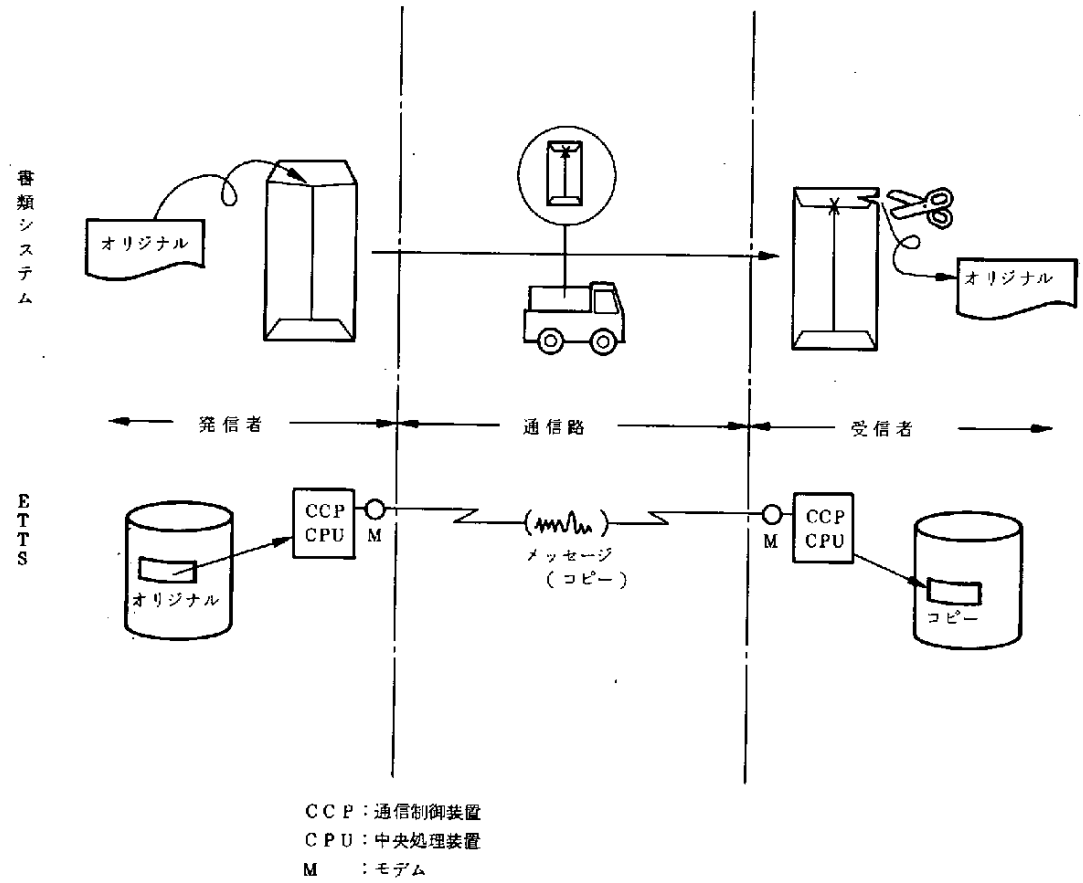


図４－８　書類システムとＥＴＴＳとの対比

① 記録（ジャーナル）の重要性

図４－８の発信側，受信側のファイルの信頼性は，それぞれ両者の良識に任されている。しかし，良識だけで信頼性を確立するのは無理である。前項で述べたように「悪徳会社」が存在するからである。それでは外部か

ら規制可能かというと，これもなかなか難かしい。むしろ，伝送路を通過したメッセージを唯一無二のオリジナル・データとしてはどうかという発想が生まれてくる。すなわち，一瞬しか存在しないメッセージに最高の価値を与えようとするものである。

ただし，一瞬しか存在しないメッセージの価値を保存するため，何かに記録（ジャーナル）しておく必要がある。この記録には，発信者も受信者もアクセスできず，書留郵便のようにプライバシーの保護が可能になっていなければならない。さらに，トラブル発生時は，しかるべき関係者のみ参照可能である必要性もある。つまり，記録方法，管理方法および誰が管理するのかが，大きな問題となる。

② 相手確認の重要性

相手確認方式としては，デジタル署名やチェック・ワード方式等の各種の方式が提案され，実際に使用されているものもある。どの方式も秘密の漏れに弱いという欠点がある。開いたシステムでは，接続している企業や機関の良識だけでセキュリティのレベルを維持するのは無理だと考えられ，新しい方式の開発が望まれる。前項で述べたような論理的なキー（数字やアルゴリズム）の欠点*1が克服できなければ，物理的なキーについても再考する必要があるのではないか。

③ パソコン端末

セキュリティ対策を考える時，パソコン端末は，端末本来の機能である入出力機能（マンマシン・インタフェース部分）とプロセッサ機能とを分離して検討する必要がありそうだ。そして，プロセッサ部分（付属のファイルも含む）のロック機構と運用は，センタのコンピュータと同等の対策がなされている必要がある。パソコン端末は，センタと同等の機能を持っているので，前項で示したようなトラブルが発生する可能性があるからで

＊1：盗難に遭っても当事者が気付かないこと。前項4.1.2の(2)の②「デジタル署名の悪用」を参照のこと。

ある。しかしながら，作業現場や個人持ちのパソコン端末に，前記のような対策を期待するのは無理であろう。それならば，ネットワーク・システムに接続できる端末は，一般に使う端末とは区別する必要があるかもしれない。

(2) 期待される対応策

① 現在技術による対応策

コンピュータ・システムが，閉じたシステムから，開いたシステムになるに従って，そのセキュリティ対策は，複雑かつ困難になっていく。技術面で考えると，開かれたシステムも閉じたシステムと基本的なセキュリティ技術は，同じといえる。相手認識技術，メッセージ認証技術，暗号方式等の暗号技術あるいはリリース保護技術，データベース保護技術など，基本的な概念としては余り変化はない。しかしながら実際面では，上記技術を開いたシステムに適用していくとなると，数多くの問題にぶつかる。

まず第1に，コンピュータ・セキュリティに関するレベルの差の問題である。データ通信回線の自由化，コンピュータ通信技術の進歩等があいまって，コンピュータ・システムのネットワーク化が進みつつある。しかし，セキュリティ・レベルから考えると，現状ではコンピュータ・システムによって，そのレベルが余りにもマチマチ過ぎる。このため，これらのコンピュータ・システムを相互に接続する，あるいは端末から複数のコンピュータ・システムにアクセスするような時には，はなはだ不都合になる。しかもこのような場合，一般には，セキュリティ・レベルの低い方に足を引っ張られてしまう。今後これについては，最低必要なセキュリティ・レベルといったものを決めて，開いたシステムでは，各システムとも最低レベルのセキュリティを守ることを，義務付けることが必要になる。

第2には，セキュリティ方式の標準化の問題である。標準化の問題は，セキュリティ・レベル差の問題とも，相互に関連する問題である。各コンピュータ・システムが，それぞれ努力してセキュリティ対策を施すと，閉

じたシステムの場合は非常に有効的である。しかし異なるシステムが，相互に通信をするような場合，それぞれのセキュリティ方式が異なっていると，ほとんど役立たなくなる。多数の端末が相互に通信を行うような場合，相手認識方法，暗号方式，メッセージ認証方式，アクセス・コントロール方式などの標準化が，必ず必要となろう。

② 新たな対応策

新たな対応策は，第三者によるチェック機構の問題である。前述①の場合は，外部からのセキュリティ侵害に対する場合を主として想定している。しかし開かれたシステムでは，4.1.2で示したように，ネットワークに参加している者の犯罪の可能性も，より一段と強まる。この場合従来のセキュリティ対策では，チェックは不十分となろう。このことを考えるに当って，電子化されていない現在の伝票（紙による）システムとネットワークによる電子化伝票とを見てみる（図4－9参照）。

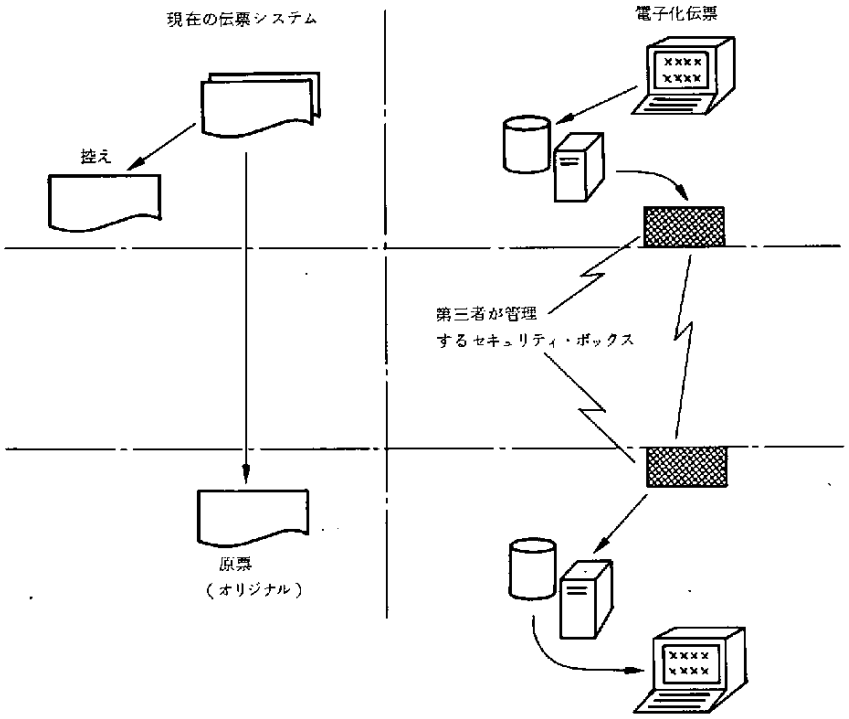


図4－9　紙伝票と電子伝票との対比

現在の伝票システムでは，正伝票，副伝票，控伝票とはっきり区別でき，正伝票によって金銭が動く。これに対し，電子化伝票は，正・副・控等の区別がつかない。ネットワークに流れた電子情報によって，次々と契約・金銭の支払いが進んで行く。このため，どうしても端末・システム等の責任境界線を決め，この境界線での情報の出入りを，公的な第三者によりチェックする機構が必要となって来る。このチェック機構を，我々は「セキュリティ・ボックス」と名付けた。

例えば，異なる企業間等でコンピュータ通信を行なう場合，必ず大容量小型光ディスク等でログ・ファイルを取り，このログ・ファイルは，第三者のみがオープン可能で，誤りや不正が生じた場合，そこで確認・切り分けを行なう方法が考えられる。もちろん，このログ・ファイルはすべての情報を取る必要はなく，約束に従った重要案件のみを取れば良い。開かれたシステムでは，多数の端末を同一のレベルにおくことなく，アクセスの許容レベルに応じて，端末のクラス分けを行なう必要も出てこよう。そのクラス分けに応じて，必要なセキュリティ機能の付与を義務付けることが必要であろう。

例えば，物流や資金転送にかかわるような端末では，公的な機関によるＩＤの付与（もち論，それはオペレータが操作出来ないよう封印等が必要）と定期的なチェック，さらにはオペレータの認識機能の義務付けが必要であろう。また，システムごとに，セキュリティ・レベルの相違が生じるが，異なるシステム相互間にあって，セキュリティ・レベルの整合をとるゲートウェイ機能も必要となる。ゲートウェイ機能の簡単な例として，セキュリティの高いシステムから，低いシステムへのデータ・フローを禁止する等である。

最後に，ネットワーク・システムのセキュリティ対策には，第三者が管理するセキュリティ・ボックスが不可欠である。このセキュリティ・ボックスを実現するうえでのポイントは，

ⓐ どういった公的機関で管理するか。法的な裏付けはどうするか。

ⓑ セキュリティ・ボックスは，どのような機能を必要とするか。その機能を実現する技術はどうするか。

ⓒ セキュリティ・ボックスを義務付けることによって，ネットワークのプロトコル・インタフェースを標準化できないか。

である。以上3点をどのようにしたら良いかは，今後，多方面からの意見を参考にして，慎重に研究すべきである。そして，十分な議論を行なったうえで開発する必要がある。

4.2　応用システムのセキュリティ

本節では，第１章の「応用システムのセキュリティの現状」で採り上げた金融業と情報処理業が将来どのようなサービスを提供しようとしているかを推測し，その将来システムでどのようなセキュリティ侵害が起るかを調査・検討した結果を述べる。

4.2.1の金融関連業では，ネットワーク化の進展に伴うセキュリティ上の問題点，週休２日制に移行し，休日営業時の無人化で新たに発生する問題点，ホーム・バンキングでの安全性の問題点，機械化拡大に伴う問題点等を指摘する。

4.2.2の情報処理業では，情報処理業が今後どの方向，どの分野に進出しようとしているかをできるだけ明確に想定し，そこで発生する可能性のあるセキュリティ侵害を具体的に指摘し，それに対する対策の調査・検討した結果を述べる。

そして最後の4.2.3では，今後膨大な需要が見込まれる，ビデオテックス，双方向ＣＡＴＶ等の画像情報システムをはじめとする新しい情報サービスであるニュー・メディア公共システムで発生すると考えられるセキュリティ問題に対する調査・検討結果を述べる。

4.2.1　金融関連業

金融関連業のオンライン化／ネットワーク化は，今後さらに発展し，将来のコンピュータ・ネットワーク利用の中心的役割を担うことが予想される。一方で，金融関連業は，直接的に貨幣を取扱うため，もっとも高いレベルのセキュリティ対策が必要になり，これがネットワーク化推進の障害になっているとも言われる。本項では，主に銀行を中心とした，金融関連業における将来のセキュリティ問題について考察を試みた。

(1)　ネットワーク化進展に伴う問題

多くの金融業では，自行内のオンライン化がほぼ終り，全銀システムへの加入等を通じて他行との接続が進みつつある。将来は，他業種との接続も行なわれるだろう。このように，ネットワーク化が高密度に進んだ時，発生する可能性のあるセキュリティ上の問題について簡単に触れる。

①　インターバンク・システムの発展

近い将来，都銀・地銀・相銀・信金等，国内の主な金融機関をすべてネットワークで結ぶことが計画されている。これによって，全国のどこからでも，あらゆる金融機関の口座への入出金が可能となり，利用者の利便さは飛躍的に増すことが期待されている。一方で，このような利便さは，数年前に起きた「オンライン誘拐事件」[*1]の犯人に対し，さらに有利な環境を与えることになるので，何らかの対策が必要となろう。

例えば，これまでも，各金融機関は逆探知システムを整備して犯罪発生に備えてきたが，将来は，全国の端末（ＣＤ，ＡＴＭ等）に警官を配置することは不可能になり，これだけで犯人を捕まえることは難かしくなる。逆探知システムとビデオ・モニタを連動させ，現金の引出しが行なわれたら，ただちに犯人の顔や姿をキャッチする等のより進んだ対策が必要となろう。

＊１：身の代金をＣＤ（ＡＴＭ）から引き出そうとする誘拐事件

② 海外支店とのネットワーク化

海外ＥＦＴＳ[*1]としてはＳＷＩＦＴが有名であるが，国内の金融機関が海外支店とオンラインで結合されると，ＳＷＩＦＴとは別の海外ＥＦＴＳが誕生することになる。後者のＥＦＴＳでは，例えば，海外のＣＤ（あるいはＡＴＭ）で日本国内の口座から現金を引き出すことも可能となろう。このような機能を利用した，国内と海外に股がった三和銀行事件[*2]と同種の犯罪が発生すると，法的にもかなり厄介な問題が発生する可能性がある。

③ 他業種とのネットワーク化

現在，自動振替等のデータは磁気テープで輸送することが一般的に行なわれている。今後，これを通信回線上のデータ伝送に置き換えることが計画されている。この場合，他業種と共用ネットワークを組むことが経済的に有望視されており，異業種間での本格的電子化処理の第一歩になるので，注目を集めることとなろう。

このような異業種（異企業）間での電子化処理では，解決すべき大きな課題がある。詳細は，前節で述べたとうりである（4.1「ネットワーク・システムから見た技術」を参照）。

(2) 週休２日制と業務の拡大

① 週休２日制

週休２日制は時代の流れであり，遠からず金融機関でも完全実施されるだろう。さて週休２日制が実施されると，今度は逆に，休日営業が大きなセールス・ポイントになるため，これを主な商品にした金融機関が出現する可能性は充分ある。例えば，現在でも勤労者のために営業時間を延長している銀行がある。このため，金融機関の営業時間の多様化が進み，その

＊１：Electronic Funds Transfer System

＊２：１９８１年３月に発生した事件で，銀行の行員が架空口座に振り込みを行ない，すぐ現金を引き出し，海外へ逃亡した。犯人は捕まり有罪となった。この事件では，現金の引出しは国内で行なわれた。

うえ各金融機関は前述のようにネットワークで結ばれているので，ネットワーク運用が複雑化し，これに起因するトラブルが発生するかもしれない。また，これらの状況を巧みに利用した犯罪も発生するかもしれない。一方，週休２日制になれば，平日の業務密度は高くならざるを得ず，機械化の拡大が進められると思われるが，これについては後述する。

② 業務の拡大

各金融機関では，ほぼオンライン化を完了させ，現在は新しい商品の開拓に力を入れている。例えば，クレジット業務，証券業務，ホーム・バンキング，ファーム・バンキング等である。まだ法的問題の残っている商品もあるが，近いうちに解決されるという。さらに，金利の自由化等もうわさされており，今後，金融機関の業務は多種多様になることが予想される。これが，セキュリティ上どのような問題を引き起こすかは，現在まだよく分らない面が多い。しかしながら，ホーム・バンキングでは安全性への配慮から，当面送金等価値の移転を行なうものはサポートされないと言われている。とはいうものの，実際にホーム・バンキングが始まれば，送金処理を求める顧客の要望がかなり大きくなることが予想され，対策に苦慮することとなろう。

また，業務が多種多様に拡大しても，省力化が今日の普遍的課題である以上，より少ない人数で達成しようという努力が続けられ，結局，機械化のより一層の推進を促し，機械化拡大の方向を辿ることとなろう。機械化に伴う問題については，次に述べる。

(3) 機械化拡大に伴う問題

前述のように，機械化の拡大は今後の金融機関の必須項目とも言える。今後の機械化の特徴は，①顧客による直接オペレーションの増大と，②処理の自動化で，そして，③処理量の増大，質の変化という副作用である。①は，金融機関外部での問題を生み，②，③は金融機関内部の問題を生む。以下に，これらの問題を提起して，本項を締めくくる。

① 顧客直接オペレーションの増大

ＣＤやＡＴＭは省力化の切り札であり，顧客にとっても便利であるため，今後も増大するだろう。新しい商品であるホーム・バンキングも同様である。また，これによって無人営業店も可能になる。しかし，これらの機器には顧客の直接オペレーションに伴う問題，例えばミス・オペレーションや悪用等がある。既に何度も述べられているので，詳述は避ける。

② 処理の自動化

金融機関内部では，各種の自動化の推進が予想される。センタ・オペレーションの自動化，端末での帳票の自動読取り，通信回線による外部との接続，その他，センタや営業店ではロボットの導入も考えられる。磁気テープの自動輸送やＡＴＭへの現金の自動セット等を可能にする。これらは，内部犯罪（必ずしもコンピュータ犯罪だけではない）の減少に効果がある。人が現金に触れる機会が減少するからである。その半面，処理のブラック・ボックス化が進むため，巧妙な犯罪が長期間発見されない恐れもある。この問題は，第１章でも述べられている。詳細はそちらの方を参照されたい。

③ 処理量の増大，質の変化

これまで金融機関では，機械化（オンライン化）が進むごとに，処理量（処理件数）が増大してきた。機械化によって新しい商品が開拓され新しい需要を喚起したからだと説明されている。すると将来は，機械化が徹底的に進むため処理量の増大はかなりのものになると予想される。当然ハードウェアも進歩するため，これだけでは大きな問題にならないが，すべてを機械化できるわけではなく，人間がチェックすべき部分もずっと残る。従って，この人間のチェック能力が，量の増加について行けるかどうかというのは大きな問題となろう。

他方で，量の増加と共に，今後の機械化処理では，センタ処理の質の変化が求められるだろう。その結果，現在でも巨大なシステムは，ますます巨大化複雑化し，開発部門は新開発の作業に追われ，超大型システムのす

べてを知る人が居なくなり，システムの一部はその構造を知っている人さえ居ない等という状況も生まれよう。この時，密かに組み込まれた詐欺プログラムをどうやって発見できるだろうか。誰も知らないことを幸いに行なわれる詐欺オペレーションを，どうやって見破ることができるだろうか。人間による管理といえども限界がある。

しかしながら，現実の課題として世の中が超巨大システムを必要としており，セキュリティ問題の壁を乗り越えてこれを実現するためには，様々なセキュリティ技術の開発が必要で，一日も早く着手すべきである。

4.2.2　情報処理業

(1)　情報処理業の進展方向・進出分野

情報処理業での将来システムのセキュリティ問題を考える時，先ず将来どんなシステムが構築されるかを明確にする必要がある。そのためには，情報処理業が今後どの方向に向って，すなわち，どのような分野に進出しようとしているかを明確に想定しなければ，そこで発生すると考えられるセキュリティ侵害を具体的に指摘し，対策を考えることができない。本項では，情報処理業が今後進出すると想定される分野を考えてみる。

先ず，情報処理業は情報を処理することを生業としており，情報を取り扱うサービス分野すべてに進出すると考えるのが妥当であろう。第一は，情報処理業が既に持っているファシリティを増強し，拡大して行く方向であり，次のサービス分野への進出が考えられる。

① ネットワークをより広域化し，全国網を形成し，全国サービスへの進出

② 国際ネットワーク・サービスへの進出

③ コンピューティング・パワーの販売から情報の販売やコンサルタント・サービス等の分野への進出

・高度なデータベース／データバンク・サービスへの進出

・有料ソフトウエアの時間貸，販売への進出

④ 一括代行サービスへの進出

・企業で必要とする業務処理システムの開発から運用までの一貫したトータル・サービスへの進出

第二は，新規の分野への進出であり，次のサービス分野が考えられる。

ⓐ 通信を主体としたＶＡＮサービスへの進出

ⓑ 情報処理業が主体（主導）による異業種間ネットワーク・サービスへの進出

ⓒ ニュー・メディア・サービスへの進出

①と②は，現在のＴＳＳ等のオンライン・サービスの延長線上にあり，自社のネットワークを拡大し，全国津々浦々，あるいは企業の国際化にともなう海外の主要な国から自社の情報処理サービスを受けられるようにすることを目指すこととなろう。③は，従来はコンピューティング・パワーが主要商品であったが，今後は各社が提供する情報検索サービスを活用するノウハウをコンサルタントしたり，代行検索等をしたりする方向である。すなわち，各社の検索結果を加工・統合して，新たな付加価値を加えた検索結果を導き出す高度なサービスを目指すこととなろう。更に，情報処理業は今後どんなソフトウエアを開発し，販売できるかが，その社の命運を制すると考えられるので，委託ではない，自社独自の目玉商品となるソフトウエアの開発をより重要視することとなろう。④は，企業内にあるコンピュータ・システムの運用を支援するためにオペレータを派遣する，言わゆるＦＭ（Facility Management ）サービスに変って，今後は，一般企業では減量経営の一環としてその社で抱えているコンピュータ要員やコンピュータ設備を削減，あるいはコンピュータ部門を縮少・廃止する方向に向うことが想定されるので，その企業の中枢の業務処理のシステム開発から運用まで一貫して受託する方向を目指すこととなろう。

ⓐは，電電公社から賃借した高速回線を各種の方式で多重化し，より高品質と高信頼通信という付加価値を付けて回線の賃借をする分野を目指すこととなろう。ⓑは，情報処理業者が管理・監督・賠償責任を持つ，例えば，小売業，運送業，銀行／クレジット会社等が加入する異業種間ネットワーク・サービスの分野を目指すこととなろう。ⓒは，今後膨大な需要が見込まれる分野であり，情報処理業の主要なターゲットとなろう。（ⓒについては，4.2.3の「ニュー・メディア公共システム」の節で詳しく述べられるので，本項ではこれ以上言及しない。）

(2) 今後新たに想定される脅威とその対策方向

本項では，(1)で述べた新たな分野へ情報処理業が進出した場合，どんな脅

威が発生する可能性があるか，それに対してどんな対策を取る必要が生じてくるかを，(1)とは異なる観点から見て述べる。

① データ／プライバシの保護

情報処理業が提供するであろう将来システムでは，増々重要な情報がここに集まり，蓄積されるので，社会的責任がより重く，公共性が高まってくるであろう。特にプライバシ情報など機密性の高い情報を取り扱うので，それに参入する企業に対して一定の資格を満たしているかの認定制度，あるいは国家資格制度が必須となるであろう。同時に，そのシステムが正しく構築され，セキュリティ対策が万全に行なわれ，システム運用がなされているか等を定期的に第三者によるシステム監査や立入り検査も必要となるであろう。そして，それに従事する人達に対しても機密のレベルに応じて資格制度を採り入れるとともに，情報の守秘義務などの職業倫理感を確立する必要がある。さらに退職に対しても一定期間守秘を義務付けることも必要となろう。

② ソフトウェアの保護

ソフトウェアが独立した商品として流通・売買されることが急激に多くなってくると想定されるが，そのときソフトウェアの開発者の権利の保護がより重要な課題となろう。著作権法を拡大して，法制的に保護することも考えられるが，一方では自衛手段を講ずることもより重要となろう。自衛手段としては，ソフトウェアを暗号化し，解読を不能にしたり，ＯＳと連携してコピーをできなくしたりする一時しのぎの手段も考えられるが，根本的に解決するには，このソフトウェアはこのマシンでしか動かないという新しいコンピュータ・アーキテクチャを考える必要があろう。

③ ネットワークの保護

情報処理サービスのネットワークが拡大・普及し，コンピュータの大衆化が成熟した暁には，影の面として，最大な脅威の一つと考えられる，強力なパーソナル・コンピュータを駆使して遊びのつもりでサービスを妨害

したり，システム破りを試みる若い人が出てくる不健全な堕落した社会が想定されるので，今後は，パーソナル・コンピュータによる不当アクセスに対して充分な対策を講ずることが増々重要となってくるが，同時に市民に対してセキュリティ侵害の罪の重さを啓蒙する必要があろう。将来のネットワーク・サービスでの最大の弱点の一つとなるであろう回線上のデータの盗聴に対しては，現在暗号化が実現可能な手段として有望視されているが，一般の端末にも組込み可能な安価（数千円程度）な暗号器（あるいはチップ）が出現・市販されることを期待したい。

④ システムの保護

ＦＭサービスでは，オペレータ要員を派遣するのみであり，派遣されたオペレータが業務システムの中味に精通して不正を行なう機会はおのずと少ないが，トータル・サービス，すなわち業務システムの開発から運用までを一貫して受請うと，その業務システムの開発・運用全体に従事し，精通する人もでてくるであろう。セキュリティの面からは，システム全体について精通しているオールマイティを輩出させないように，システム・エンジニア，プログラマ，オペレータ等の職種を明確に分離する必要がある。一方，アベイラビリティの面からは，すなわち，障害が発生した時迅速に復旧するためには，システム全体に精通した人がたくさんいた方がずっとよい。セキュリティとアベイラビリティをいかに両立させるかという問題をどのように解決するかが課題となろう。

4.2.3　ニュー・メディア公共システム

(1)　ニュー・メディア時代の到来

ＬＳＩ技術，光ファイバ技術，衛星技術などのエレクトロニクス技術の進歩，コンピュータとコミュニケーションの融合などを背景として，キャプテン，ＣＡＴＶ，文字多重放送，衛星放送などの他，さまざまなニュー・メディアが出現しつつある。さらには，電子新聞や電子郵便のように，これまで電気通信と直接結ばれていなかったメディアの電子化，電気通信化も進もうとしている。ニュー・メディアの登場によって，情報化の波は企業から社会，家庭へと進展し，情報化社会の到来に大きなインパクトを与えるであろう。そうして，誰でもが居ながらにして，各種情報提供サービスをはじめとして，多彩なサービスを自由かつ簡単に受けられるようになるだろう。

今，ニュー・メディアは夢と期待を持って国民の間に迎え入れられようとしている。たしかに，ニュー・メディアはオフィス業務や社会生活，家庭生活に大きな変革と利便性をもたらすことになろう。しかしながら，反面，プライバシー問題や各種セキュリティ問題などの新たな社会的問題をも生じる可能性があることも忘れてはならないだろう。残念ながら，この問題に関しては今まであまり深く検討されてはいない。

(2)　ニュー・メディア公共システムの具体例

ニュー・メディア・システムにおけるセキュリティ問題を考えるために，具体的なシステムを参考としてとりあげる方がわかり易いだろう。

ここでは，コンピュータの情報処理機能，蓄積機能を活用したニュー・メディア公共システムをとりあげてみることとしたい。

ビデオテックスは「既存の電話回線を介して，家庭用のテレビ受像機等とコンピュータを結び，会話形式で文字と図形情報を提供するシステム」であり，日本ではキャプテン・システム（Captain System）という名称で，昭和５４年１２月末から実験サービスが行なわれており，昭和５９年１１月には商用サービス開始が予定されている。実験システムでは，キャプテン・セ

ンタと呼ばれる単一の情報提供センタ中心のサービスであったが，商用システムではゲートウェイ機能を持たせ，多数の民間オンライン・システムも接続し，多彩なサービスを可能とするよう計画されている。

このように将来のビデオテックス・システムでは，キャプテン情報センタをはじめ，航空会社，デパート，銀行などのオンライン・センタと接続することにより，家庭やオフィスに居ながらにして，各種情報検索をはじめ座席予約，商品注文，残高照会，振込依頼等の多様なサービスの利用が可能となる。図４－１０に将来のビデオテックス・システムのイメージ図を示す。

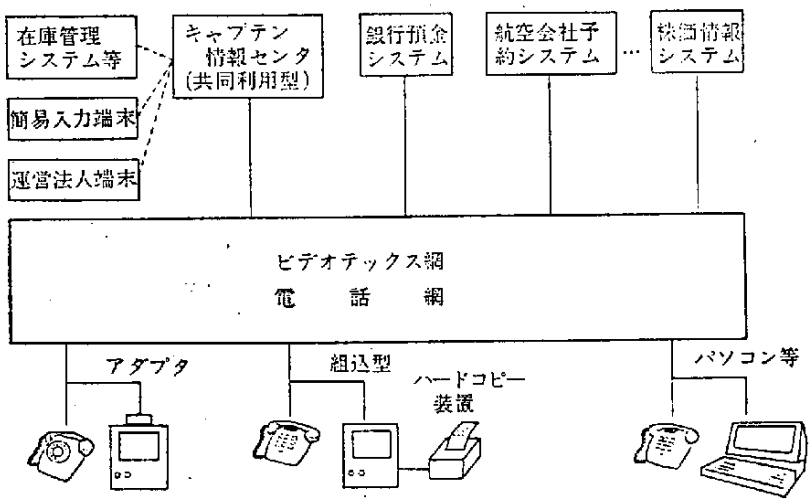


図４－１０　ビデオテックス・システム（出典：電気通信　１９８２．１１）

(3)　ニュー・メディア公共システムにおけるセキュリティ問題

ニュー・メディア・システムの特徴を整理してみると，概略次のとおりであろう。

①　情報通信の社会生活，家庭生活への普及（利用の拡大）

②　情報通信の双方向化

③　多様な情報の流通

④　簡単かつ自由な利用

⑤　不特定多数の利用

このように，ニュー・メディア公共システムは多大な利便性をもたらすが，逆にいうとその分だけセキュリティの問題は難しくかつ複雑になると言える。以下に今後懸念されるセキュリティ問題を幾つか取り上げてみたい。

情報提供側における問題から眺めてみると，まず第一に情報操作の問題である。ビデオテックス，ＣＡＴＶ，文字多重放送などニュー・メディア時代になると，多くの情報提供者から多様な情報が提供されるようになる。それら数多くの情報の中には，悪意を持って作られた情報が含まれないとも限らず，それによって意図的な世論操作も可能となる。勿論，今までもこういう心配はあったが，ニュー・メディア時代になると情報量が増大し多様化するだけに，そのチェックはより一層困難となる。

第二に懸念されるのがプライバシ侵害の問題であろう。これはプライバシに係わる情報を意図的に流す場合もあろうし，偶発的に流れる場合もあろう。

第三に懸念されるのは，利用者から入力された情報の悪用の問題であろう。双方向型のシステムでしかもその利用形態は多岐に渡るとなると，様々な情報が利用者からインプットされる。単なる趣味に関するものから家庭生活に関するもの，さらには政治信条に関するものまで含まれるかもしれない。それらの情報を情報提供者（提供者が逆に収集者にもなるわけだが）が不正に使用する，あるいは第三者に流すということも考えられる。

次に情報利用者の側から眺めてみよう。この場合懸念されるのは，コンピュータ・システムの悪用であろう。単にコンピュータ・システムの利用が，提供される情報の利用にとどまっている場合はそうでもないかもしれないが，ホーム・ショッピングやホーム・バンキングなどのように物流やマネー・フローに係わってくると，その心配は現実的なものとなる恐れがある。しかも，それが家庭等のように第三者の目になかなか触れない場から，自由にどんなセンタでもアクセス可能となるとより一層の問題をおびる。意図的な悪用の

チャンスが増えるばかりでなく，出来心的に悪用を行なうというケースも増えてこよう。

(4) 今後の対応

前項で幾つかのセキュリティ上の問題を取りあげたが，ここでこれらの問題への対応について少し触れてみたい。

① サービス提供者，情報提供者の審査

ニュー・メディア時代になると各種のメディアを利用していろいろなシステム（サービス）が構築される。さらにそのシステムには多種多様のコンピュータ・センタや情報提供者が参加する。ニュー・メディア・システムは，共同利用型でかつ社会生活，家庭生活と密接につながりを持つものであり，その意味で社会的，公共的システムと位置づけられる。このように社会的影響の大きいシステムについては，情報の不正提供，不正収集，プライバシ侵害などを防ぐためにも，サービス提供者，情報提供者に対する事前チェックが必要となろう。勿論これは参加の自由を不必要に阻害するものであってはならないし，その意味からも公的な機関による審査制度の検討が望まれる。

② 端末におけるセキュリティ対策

社会，家庭に普及させるために，端末は安価であること，また取り扱う情報の内容が犯罪に結びつくようなものではなかったことなどから，ニュー・メディア・システムにおいてもセキュリティ対策はあまり真剣な問題としてとりあげられていなかったきらいがある。

しかし，ホーム・ショッピングやホーム・バンキングなどのように物流やマネー・フローの伝達手段として使用されるようになると，情報犯罪が現実の問題として心配される。勿論，この場合のセキュリティ対策は銀行やデパートなどのサービス提供者側で個々に措置すべき問題であろうが，端末については利用者側が購入し多目的に使うものであり，公的な場で検討しておく必要があるだろう。

具体的には，ＩＤ，パスワード，暗号化等の必要性が出てこよう。端末が自由にどこからでも使えるようになると，端末認識以上に利用者認識が重要になる。いずれにしても，ニュー・メディアを普及させるには，端末は安価でなければならず，上記のような対策を施すためには安価で効果的な方式が是非とも必要となろう。

昭和５８年３月発行

発行所　財団法人　日本情報処理開発協会
東京都港区芝公園３－５－８
機械振興会館内
TEL（434）8211（代表）

印刷所　株式会社　三州社
住　所　東京都港区芝大門１－１－21
TEL　（433）1481（代表）

57－S002