58—S 001

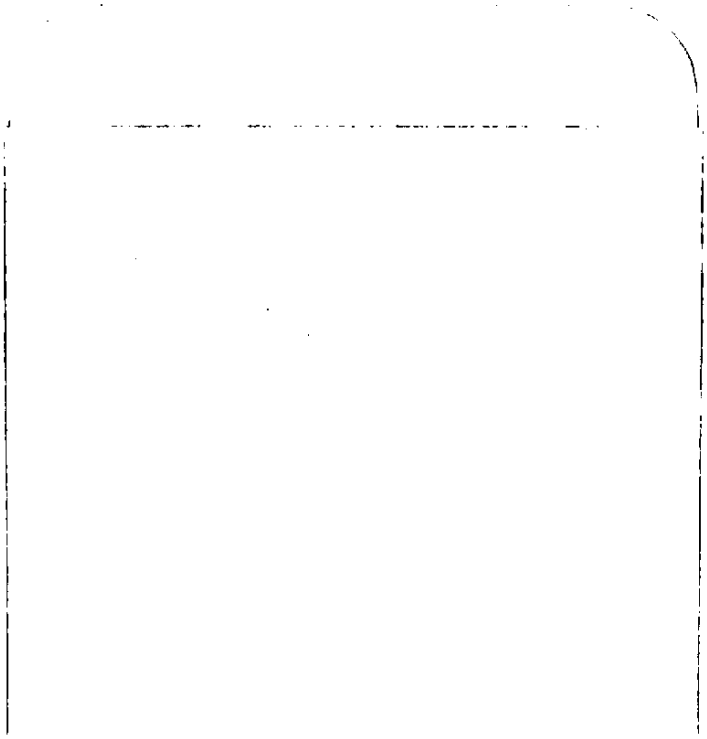
コンピュータ・システムのセキュリティ技術の開発に関する調査研究報告書

昭和59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５８年度に実施した「コンピュータ・システムのセキュリティ技術の開発に関する調査研究」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」のプロジェクトを実施した。

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。

このような背景をふまえ，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につき，調査研究を行なった。

昨年度は，現在のセキュリティ要素技術全般につき，その実現状況および問題点などについての網羅的な調査を行なった。

今年度は，その成果を受けて，要素技術の複合によるシステム化に重点を置き，特に，今後の実現が強く期待される３つのセキュリティ対策機能を取り上げ，その基本構想，実現手段などにつき，詳細な検討を行なった。本報告書は，その成果をまとめたものである。

本報告書が，この分野に関心のある方々に広く利用され，今後の情報処理技術の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，強力な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斉藤委員長をはじめ，各委員およびワーキング・グループのメンバー各位に対し，心から感謝の意を表します。

昭和５９年３月　　財団法人　日本情報処理開発協会

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㈱情報処理金融システム事業部システム部主任
〃	小笠原謙蔵	日本アイ・ビー・エム㈱製品営業推進副部長
〃	川上万寿夫	㈱富士銀行システム開発室次長
〃	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1部開発第3課長
〃	中尾康二	国際電信電話㈱研究所情報処理研究室
〃	谷口和道	日本電信電話公社技術局分散処理担当調査役
〃	千葉恭弘	㈱電通国際情報サービス営業技術部次長
〃	中村利武	富士通㈱情報処理事業本部端末機事業部端末第2技術部長
〃	久重剛志	㈱三菱銀行事務本部システム部調査役
〃	松田　宏	日本電子計算㈱ＤＰ本部運用管理部長
〃	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	(財) 日本情報処理開発協会開発部次長
オブザーバ	押尾勝平	富士通㈱情報処理事業本部企画部調査部調査課長

事務局　(財) 日本情報処理開発協会

コンピュータ・セキュリティ技術調査研究
ワーキング・グループ

（敬称略，順不同）

〔セキュリティ・オペレーティング・システムの検討〕

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長
小林俟史	埼玉工業大学電子工学科助教授
佐薙充	富士通㈱情報処理事業本部企画部計画部第6計画課長
千葉恭弘	㈱電通国際情報サービス営業技術部次長
林伝雄	日本電気㈱情報処理金融システム事業部システム部主任
森正道	日本電子計算㈱名古屋支店計画管理課長

〔システム監査支援ツールの検討〕

小笠原謙蔵	日本アイ・ビー・エム㈱製品営業推進副部長
久重剛志	㈱三菱銀行事務本部システム部調査役
油井直治	アーサー・アンダーセン　システム・コンサルティング・マネージャー

〔ネットワーク・セキュリティの検討〕

川上万寿夫	㈱富士銀行システム開発室次長
谷口和道	日本電信電話公社技術局分散処理担当調査役
手塚啓一	沖電気工業㈱システム本部開発第1部開発第3課
中尾康二	国際電信電話㈱研究所情報処理研究室
水野昌美	㈱日立製作所コンピュータ事業本部本部員

〔事務局〕

鍛治勝三	(財) 日本情報処理開発協会開発部主任部員
三木良治	(財) 日本情報処理開発協会開発部開発第二課

目　　次

第Ⅰ部　総　　論

1. 調査研究の背景

1.1 情報処理の高度化

今や，コンピュータ・システムは社会のあらゆる分野へ広範に普及し，それが果す機能は急速に拡大・多様化している。この進展は技術面における素子の超ＬＳＩ化，スーパー・コンピュータの開発，パーソナル・コンピュータ等低価格コンピュータの出現に加え，光ファイバー，通信衛星の本格的な利用開始など，情報処理と通信の技術の融合によるものである。また，経済・社会的にも産業活動の高度化，高付加価値化，国民生活の一層の質的向上といった要請があり，この要請と技術的進歩とが結びつき，情報処理の高度化につながっているといえる。

ここで我国における情報化の進展を顧みると，１９６０年代後半から７０年代にかけては，産業界におけるコンピュータ導入を中心とする情報化で，いわゆる第一次情報化革命の時代であった。その後，情報処理技術と通信処理技術の飛躍的な発展とその結合によるコンピュータ・ネットワークの進展により，これまでの拠点的な展開から面的な展開へと一層広範に，また内容的にも質的にも，非常に高度な利用の形態，すなわち，第二次情報化革命と呼ぶべき新たな高度情報化の段階を迎えつつある。

面的な展開では，これまで産業界を中心に進展して来た情報化が，現在では社会や家庭にも広がりつつあり，今後は社会のあらゆる分野，局面においても一層広範に，かつ深く情報化が浸透していくものと思われる。

次に内容的・質的面であるが，従来コンピュータは，科学技術計算や事務処理に使われることが多かったが，今後は社会のあらゆる分野を有機的に結合するネットワークが構築され，双方向ＣＡＴＶ，ビデオテックス，衛星通信等，ニューメディアを活用した情報システムによって，ファーム・バンキング，ホーム・バンキング，ホーム・ショッピング等，多様なサービスが全国津々浦々の企業および家庭で受けられるものと思われる。そして利用方法においても，情報を一方的にただ

受け取るだけでなく，きめ細かな個々のニーズに対応した情報を主体的に随時取捨選択して得ることができるようになる。

1.2 コンピュータ・セキュリティについて

前項で述べたような情報処理の高度化によって，経済・社会の多くの分野がコンピュータ・システムに依存する状況に至っており，また，個人情報等の重要でかつ大量のデータが，コンピュータ・システムに蓄積されるなど，国民生活にもコンピュータ・システムは密接なものになって来ている。万一このシステムの機能が停止，あるいは不完全になった場合には，その影響は単に経済活動にとどまらず，身体，生命への危害，財産，プライバシー等の侵害を通じて，国民生活全般に及ぶ恐れがある。

豊かな高度情報化社会を構築するためには，このような情報化社会の有する脆弱性を克服し，情報化のもたらす便益を，あまねく安定的に享受されるように情報化を進展させる必要がある。このため，コンピュータ・システムの安全性，信頼性等を確保するため，それを阻害するマイナス面を除去すべき各種の対策が講じられねばならない。すなわち，コンピュータ・セキュリティ対策の検討が必要である。

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，以下のように分けて考えることとしている。

(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 ハードウェアの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重系，３重系）にし処理結果の多数決を行う，処理系のバックアップを完全にし，リカバリやリスタートに備える，メモリ・プロテストを行う等の対策をとる。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，および記録媒体（ソフトウェアやデータを格納したもの）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記録媒体等を保護する。

③ ハードウェアおよび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および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とすることが多い。したがって物理的安全対策とはむしろその対策の物理性を意味する場合を含む。

(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い，データやプログラムの不当な読み出しや破壊を行ったり，あるいは虚偽データを不当入力し，システムを混乱に陥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っても，記録媒体上のデータが喪失するわけではない。したがって発見が難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。

当プロジェクトでの対象は，この(3)を主要な検討テーマとしている。

1.3 新しい動き

ここでは主に，我国における新しい動きについて概説する。

(1) 産業構造審議会情報産業部会

通商産業大臣から「情報化の健全かつ円滑な進展を図るための基盤整備の具体的方策の在り方いかん。」という諮問を受けて，特に重要かつ緊急性が高い，ニューメディアの出現・発展への対応，コンピュータ・セキュリティの確保およびソフトウェアの開発・流通における基盤の整備，という三つの課題について検討し中間答申を行っている。

特にセキュリティの確保の課題検討の中で，政府が講ずべき措置として次のものをあげている。

① 指針の提示

② 基準の提示

ⓘ セキュリティ対策についての基準の策定

ⓘⓘ システム監査基準の策定

③ セキュリティ対策のインセンティブ措置

ⓘ コスト面の制約の緩和

ⓘⓘ 認定制度の充実

④ 技術開発

また，ニューメディアの出現・発展への対応の課題の検討においても，政府が講ずべき施策の一つに，総合的なコンピュータ・セキュリティ対策の必要性を掲げている。

(2) システム監査人の認定制度の動き

システム監査人の養成等を促進するため，システム監査についての試験を実施し，合格者をシステム監査人として認定しようというものである。

(3) 通商産業省の「電子計算機システム安全対策基準」の見直し

昭和52年に通商産業省から提示された「電子計算機システム安全対策基準」を，コンピュータ・セキュリティ対策の面から見直しを行ない，より充実した基準にしようというものである。

(4) 郵政省の「データ通信ネットワーク安全・信頼性基準」の発表

これはデータ通信ネットワークとして，安全と信頼性を確保するためのガイドラインを提示したもので，郵政省より昭和57年に発表されている。

(5) ファーム・バンキング・サービスの開始およびホーム・バンキング，ホーム・ディーリング・サービスの動き

銀行および証券会社を中心に，委員会や研究会を設置して，サービス内容，時期，問題点など，さまざまな方面からの検討が活発化するとともに，一部銀行においては既にファーム・バンキング・サービスを開始している。

(6) 銀行第3次オンライン・システムの構築活発化に伴ないセキュリティ対策導入の動き

全銀協標準通信プロトコル（ベーシック手順）においては，国際標準化機構（ＩＳＯ）のＯＳＩ（Open Systems Interconnection）参照モデルで定義されている，機能階層化（レイヤ）の考え方を採用し，通信プロトコルを構成する機能のもれや重複がないよう，機能分担を明確にするとともに，ファイル・アクセス・キーやパスワードの暗号化もできるように，セキュリティ対策を講じている。

(7) ビデオテックス通信サービスが本格化

ニューメディアの一つであるビデオテックス通信サービスが計画されており，

昭和５９年１１月よりサービスが開始される予定である。これにより，ホームショッピング，各種予約，情報検索等が家庭で行えるようになり，それにより発生するマイナス面（コンピュータ犯罪等）を防止するコンピュータ・セキュリティ対策が，益々重要になっている。

(8) 通信衛星の実用化

我国最初の「実用通信衛星」ＣＳ－２ａおよびＣＳ－２ｂが昭和５８年２月および８月に打ち上げられ，これにより全国津々浦々まで各種の通信サービスが提供可能になった。それに伴なうセキュリティの問題がクローズアップする可能性があり，その対策の検討が必要と考えられている。

(9) 双方向CATV事業の動き

我国では多摩CCIS（Coaxial Cable Information System）や東生駒Hi-OVIS等で実験が行なわれているが，最近この双方向CATVを建設し，運営しようとする計画が全国各地，特に電鉄会社を中心に進められている。昭和６０年前後に計画のいくつかが具体化され，各種のサービスが開始されるものと思われるが，ここでも(7)，(8)で述べたのと同様な，セキュリティ対策の検討が，重要な課題としてクローズアップされると思われる。

(10) 郵政省において電気通信事業法案がまとまる

「この法律は，電気通信事業の公共性にかんがみ，その適正かつ合理的な運営を確保することによって，電気通信役務の利用者の利益を保護するとともに，電気通信の健全な発達に資することを目的とする」と第一条で定めており，第三条，第四条では検閲の禁止，秘密の保護について定めている。また，第六条においては事業の種類を第一種電気通信事業（電気通信回線設備を設置して電気通信役務を提供する事業）と第二種電気通信事業（第一種電気通信事業以外の電気通信事業）の二つに，明確に区分している。

この法律は，通信の自由化を目指すものであり，この法律の施行により，ＶＡＮ（付加価値通信）サービスの活発化が期待される。その場合，通信ネットワークも非常に複雑化するとともに，多種多様な企業間の情報交換が行なわれるようになり，セキュリティ対策がますます重要になって来ると思われる。

2. 今年度の調査研究目標

2.1 目　的

当プロジェクトでは，昨年度（昭和５７年度）に，応用システムのセキュリティ対策を分析し，今後検討すべきセキュリティ関連基本技術を提案した（表２－１参照）。これらは要素技術なので，どのような局面で，いかなる効果を持つのか，分りにくいところがあった。要素技術は応用システムに組込まれて，初めて目に見えるセキュリティ機能を発揮するからである。そのため，提案した技術が応用システムに組込まれた場合，どのようなセキュリティ機構が実現できるか，確認しておく必要があるだろう。

一方，現実との適合性も重要である。実際のニーズについては，昨年度に充分調査したつもりではあるが，完全と言うことはできない。加えて，ニーズから導き出した結論は，必要条件ではあっても，十分条件にはならない場合もある。従って，昨年度提案した基本技術を現実に写像し，その有効性を確認しておく必要もある。

そこで，当プロジェクトは今年度（昭和５８年度），要素技術の組合わせ（システム化）を試みることとした。要素技術をどのような形に統合するかは重要な検討項目であるが，我々は，先ず応用システムの形に組上げることを検討した。すなわち，コンピュータ・システムを，個々の応用システムとネットワーク・システムに分類し，それぞれのシステムのセキュリティ対策を考慮し，要素技術の有効なシステム化について検討することにした。

一方，我々が問題とするシステムは，コンピュータ・システムであり，現在のコンピュータ・システムでは，例外なくオペレーティング・システム（ＯＳ）が使用されているという事実を，無視することはできない。いかなるセキュリティ機構でも，それが技術的機構であれば，その背後にＯＳが必ず見え隠れしている。もし，ＯＳにセキュリティ上の弱点があれば，どんなに工夫されたセキュリティ機構も無意味になる可能性がある。このように，ＯＳは極めて重要な要素である。

表２－１　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２－１　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 • 人力の冗長化 • 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

（昭和５７年度コンピュータ・システムのセキュリティに関する調査研究報告書より）

しかしＯＳは，応用システムの立場から見れば確かに要素であるが，要素技術の立場からは応用システムのように見える。我々は，このような中間的性格を持つ技術を，基盤技術と定義し，セキュリティ要素技術統合の一形態として，とらえることにした。

以上のような理由で，当プロジェクトは，次に示す３つのテーマを，今年度検討することとした。

① コンピュータ・システムのセキュリティ基盤技術
② 応用システムのセキュリティ対策
③ コンピュータ・ネットワーク・システムのセキュリティ対策

我々の最終的目標は，今後開発すべきセキュリティ新技術を，明らかにすることである。新技術には，要素技術，基盤技術，場合によっては応用システムも含まれる可能性がある。セキュリティ要素技術は，単独で開発するよりは，それが使われる環境――ＯＳあるいは各種の応用システム――に合わせて開発した方が，目標も明確になり効果的であると思われる。我々が今年度，システム的視野で要素技術の組合せを検討しようとしたのは，このような理由もある。この意味では，今年度提案する開発課題は複数になると思われるが，それぞれ独立した技術ではなく，全体で一つのセキュリティ技術体系になる。

第2.2節で，３つの検討テーマの具体的な検討課題を，それぞれ説明する。調査結果の概要は，第2.3節を参照されたい。

2.2 調査研究テーマ

本節では，今年度に検討を行うことになった３つのテーマ

① コンピュータ・システムのセキュリティ基盤技術
② 応用システムのセキュリティ対策
③ コンピュータ・ネットワーク・システムのセキュリティ対策

について，各テーマ毎に具体的検討結果を述べる。

2.2.1　コンピュータ・システムのセキュリティ基盤技術

昨年度（昭和５７年度）は，「検討すべき基本技術」を抽出し，今後の詳細な検討の必要性を指摘したが，第2.1節でも述べたように，コンピュータ・セキュリティ確保の技術的対策の基本はオペレーティング・システムにあることが認識された。また平行して行った「米国におけるコンピュータ・セキュリティの現状と動向」の調査結果から，米国防省がここ数年来先導して「セキュア・オペレーティング・システム」（ＳＯＳ：Secure Operating System）の研究開発を行っており，その重要性が再確認された。しかも我国でこの方面の研究開発は皆無で，緊急を要する研究課題とはまだ認識されていない状況にある。

米国防省では，ＳＯＳに対して主として次の３つの要求事項を満たすことを開発目標として挙げている。

① すべてのファイルに対するアクセスは，例外なくセキュリティ・カーネル（security kernel）と呼ばれるＳＯＳの中核で不正アクセスか否かを検査できること。

② セキュリティ・カーネルを形成しているコンピュータ・プログラムは，いかなるプログラムによっても修正，変更，妨害を受けないこと。

③ セキュリティ・カーネルは，仕様書で指定されたセキュリティ機能に関することのみ行い，指定されない作業は絶対に行わないこと。換言すると，セキュリティ・カーネルは，その機能および実現が正当であることが検証されていること。

特に③の要求事項が最重要と考えられる。③は，セキュリティ・カーネルがプログラムとして正しく機能するための条件であるが，ソフトウェア工学の観点から見ると，ここにＳＯＳの研究・開発の大きな意義がある。

そしてＳＯＳを評価するため，米国防省では，コンピュータ・システムをそのセキュリティ・レベルでＡ（最高）～Ｄ（最低）までのランク付けしている。さらにランク内にも順位があり，全体で８段階のランクに細かくセキュリティ・レベルが分かれている。最高のＡランクは最高機密情報を扱っても安全というものだが，ＳＯＳはＡランクを目標にしている。　ＡランクのＡ－１では，基本ソフ

トウェアに関する仕様が完全に明確であり，かつ最高セキュリティを実現していることが設計レベルで形式的に検証されていることを要件としている。この上のA－2では，仕様に従って作成されたプログラムが仕様書通りに具体化されたものであることが形式的に検証されていることを要件としている。今のところA－2レベルに適合したシステムは，公表された情報で知り得るかぎりでは存在しない。またA－1のレベルのものも現在開発中であり，完成して本番稼動しているシステムはまだない。

いずれにしてもセキュリティの基盤となる機能は可能な限りOSによって実現されることが望ましいことは確実であり，そのような観点から，SOSが今後重要な研究課題であることが明らかとなった。そこで，今年度（昭和58年度）は，SOSを1つのテーマとして採り上げ，特に商用システムにおけるSOSへの要求を中心に調査・検討することになった。

商用システムにおけるSOSを調査・検討するに当って，以下の調査研究目標を立てた。

① 現在までに開発されたSOSの基本概念は何であるかを明確にする。

② 軍用システムにおけるSOSと商用システムのSOSとの差異はどうあるべきかを検討する。

③ 商用システムにおけるSOSの持つべき機能を明確にする。

④ SOSを実現するために必要な条件や関連技術を明確にする（ソフトウェア工学，検証技術等含む。）。

⑤ SOSの開発に向けての計画を立案する。

2.2.2 応用システムのセキュリティ対策

応用システムのセキュリティ対策には，事前防止と事後のチェックがあり，図2－1に示すように相互にフィードバックされるのが理想的である。今年度は，要素技術を組合わせて，有効なセキュリティ機構を構築するのが目的であるが，その対象は事前防止機構と事後チェックの2つである。

昨年度は，事前防止対策を検討し，要素技術を導き出したのであるが，応用シ

ステムは極めて多様であり，特定のシステムをモデルとして，要素技術の統合を試みても，一般性は薄く，要素技術の有効性確認には，適当でないと思われる。そこで，今年度は事後のチェックに的を絞ることにした。

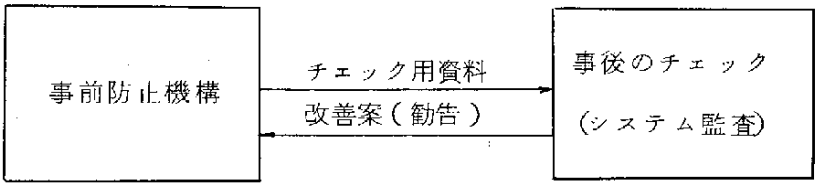


図２－１　応用システムのセキュリティ対策

応用システムの事後チェックは，いわばシステム監査の分野である。

そこで，システム監査とセキュリティ要素技術との関係について考えてみる。システム監査者にとって興味があるのは，要素技術の機能とか応用システム内での有効性であるから，要素技術を監視する立場にあり，要素技術の支援を受ける立場ではない。しかし，これはセキュリティ要素技術が事前防止に使用された場合である。もし，事後のチェック用に使用された場合は，システム監査者は，支援を受ける立場に移行する。この場合，システム監査支援ツールと呼ばれる。この支援ツールは，直接的に（積極的に）不正等の防止を行うものではないので，間接的セキュリティ技術と言うことができる。

本テーマの目標は，セキュリティ要素技術を組合わせて，有効なシステム監査支援ツールを組立てることである。我々は，次の手順で作業を進めることとした。最初に，システム監査そのものの分析と現状調査を行う。次に，既に実用化されているシステム監査支援ツールを調査し，システム監査の問題点および現状ツールの問題点を研究し，さらに両者の相関について検討する。これらの結果を踏まえて，新しいツールを構築することとした。

システム監査の分析では，標準的なシステム監査実施手順の把握に重点を置いた。その結果を考慮して最大公約数的な実施手順を検討し，そこで有効な支援ツ

ールを検討するためである。以下に，今年度の検討課題を示す。

① システム監査の最大公約数的実施手順の把握

② 既に実用化しているツールを適用する場合の問題点

③ 新しいシステム監査支援ツールの検討

2.2.3 コンピュータ・ネットワーク・システムのセキュリティ対策

当プロジェクトは昨年度（昭和57年度），コンピュータ・ネットワーク・システムのセキュリティについて検討し，やや検討不足の面もあったが，セキュリティ・ボックスを対策の決め手として提案した。

さて，このセキュリティ・ボックスが実現できれば，画期的なコンピュータ・ネットワーク・システムが構築できると期待していたのであるが，セキュリティ・ボックスには，その実現可能性という面で，かなり問題のあることが分った。詳細は，第Ⅱ部3章を参照していただきたいが，その後の検討で，かなりの技術革新がなければ，実用化が難しいという結論を得た。

そのため我々は，再度コンピュータ・ネットワーク・システムの分析を行って，セキュリティ要素技術の組合わせによる新しいセキュリティ対策方式を，検討することとした。同時に，コンピュータ・ネットワーク応用の現状調査およびネットワーク・セキュリティの分析を，行うこととした。今年度（昭和58年度）の検討課題を示すと，次のようになる。

① 昨年度のセキュリティ・ボックスは，技術的実現可能性に問題があった。今年度は，より実現性の高い方式を検討しなければならない。

② ネットワーク・システムの利用方法を把握する必要がある。犯罪が起きるためには，犯罪を起こしたくなる程，魅力に富んだ業務処理が，実際にネットワーク・システムを利用して行われるかどうかを，確認しなければならない。

③ 魅力に富んだ業務処理が存在するならば，その業務処理によってどのようにネットワーク・システムが使用されるかの検討が必要である。

④ 上記①～③の問題に対応できるネットワーク・システムの実現形態の検討

と，要素技術の組合わせ方式の検討が必要である。これは，本作業の最終結論でもある。

我々が問題にしているコンピュータ・ネットワーク・システムとは，図２－２のような全体像を持ち，少なくとも５年以上先の構築になる高度情報処理体系である。典型的な未来型ネットワークであり，現在考えられているサービス――ファーム／ホーム・バンキング，ペーパーレス処理，ホーム・ショッピング，在宅勤務，etc――が，そのネットワークを通じて行われる。当プロジェクトは，このような未来型ネットワークこそ，セキュリティ対策が非常に重要だと予測し，調査研究を開始した。

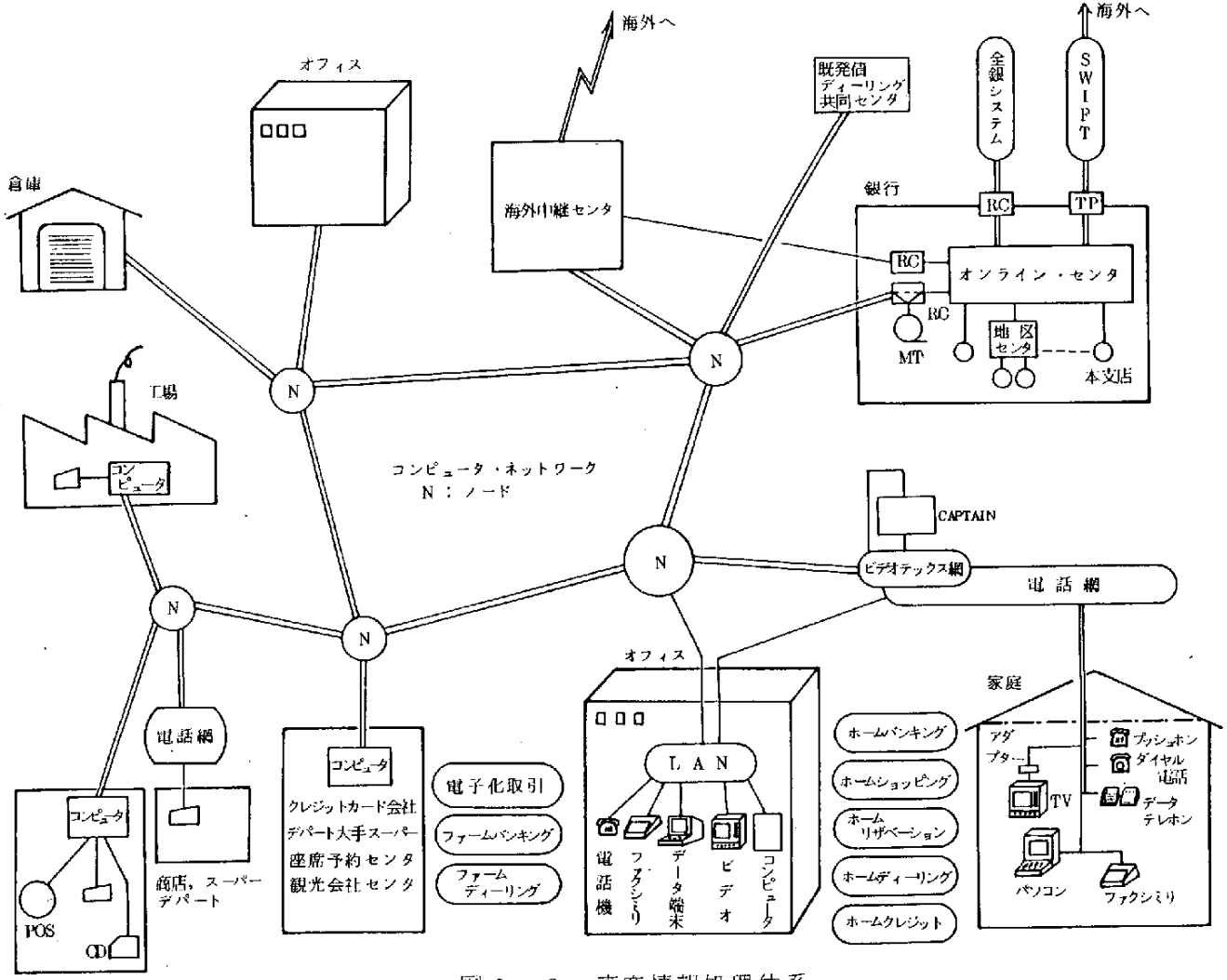


図２－２　高度情報処理体系

3. 今年度の検討結果

第2章で述べたように，当プロジェクトは今年度（昭和58年度），次の3つの課題

① セキュリティ・オペレーティング・システム（ＳＯＳ）
② システム監査支援ツール
③ コンピュータ・ネットワーク・システムのセキュリティ対策

について，現状調査および文献調査等に基づく分析を行った。その結果，新たに開発すべきセキュリティ技術を提案するに至った。

本章では，その調査研究結果の概要を述べる。詳細は，「第Ⅱ部　各論」に，検討テーマ毎に，それぞれ説明してあるので，参照されたい。

3.1 セキュリティ・オペレーティング・システム

(1) 既存のＳＯＳの調査

現状でのセキュリティ・オペレーティング・システム（ＳＯＳ）の開発状況を把握し，技術レベルを確認するために，文献調査を行った。既存のＳＯＳあるいは高信用コンピュータ・システム（trusted computer system）として研究開発中のものを含めると約30システムが存在し，ほとんどすべて軍用のシステムである。この内，重要と考える次の6つのシステムにつき公表されている文献をもとに，その詳細を調査した。

① Multics Security Enhancements
② UCLA Data Secure Unix
③ KVM / 370 （Kernelized VM / 370）
④ KSOS （Kernelized Secure Operating System）
⑤ SCOMP （Secure Communications Processor）

⑥ PSOS （ Provably Secure Operating System ）

その内で，ＨＩＳ社（ Honeywell Information Systems ）で開発したSCOMPは商用の汎用ＳＯＳであり，現在米国防省のCSEC（ Computer Security Evaluation Center ）でＡ－１レベルに適合しているか否かの認定作業中であり，今後の実用化が注目される。

(2) ＳＯＳに対する要求機能とその実現手段

既存のＳＯＳはほとんどすべて軍用のシステムであり，軍のセキュリティ・ポリシーを反映した形式的なセキュリティ・モデルに基づいて構築されている。開発されたシステムは試行的なシステムであり，一部が実際に使用されているといわれているが，性能的に妥当な段階に至っていないし，モデルが軍の要求に基づいていることから，特殊なものと考えられる。

商用システムは，経済性が重要視される。そのため，従来，セキュリティ機能はオプショナルと考えられてきた。その結果，技術的なセキュリティ対策は高価であるという認識が一般的なものとなった。しかし，近年のコンピュータ関連技術の急速な進展の成果を活用することによって，従来は経済性や効率性の点からオプションにせざるを得なかった機能を徐々に標準的なものとして，とり込むことも可能になる。

そこで，商用ＳＯＳをその具体化の例として考え，多様な利用目的に共通したセキュリティ機能を抽出し，商用ＳＯＳの要求とした。

表３－１はその要求機能である。また機能項目毎に若干の配慮を加え，要求度合としてＡ，Ｂ，Ｃのランクを付けてみた。なお要求度合ＢあるいはＣの機能もＳＯＳ完成後に追加されるのではなく，その機能が必要であると判断される場合には，システム設計段階から考慮され，織り込まれていなければならない。

次に表３－２は，ＳＯＳの考慮事項をまとめたものである。表の上段はＳＯＳを構築する際に有用と考えられる実現手段をまとめたものであり，中段はＳＯＳのソフトウェア及びハードウェアに対する前提条件をまとめたものである。特に「ソフトウェアの品質保証」は今後の最重要課題であることを再度指摘し

表３－１　ＳＯＳの要求機能の一覧表

ＳＯＳの要求機能	要求度合＊
(1)　本人確認機能	A
(2)　アクセス制御機能	A
(3)　プロセス隔離機能	A
(4)　使用済記録媒体白紙化機能	A
(5)　ジャーナル／ログ機能	A
(6)　セキュリティ管理者支援機能	A
(7)　システム監査支援機能	B
(8)　シャットダウン防止機能	B
(9)　システム監査用の出口の常設	B
(10)　リモート・プログラミング抑止機能	C

＊　：　要求度合

A　：　核となる機能で必須である。

B　：　周辺機能であるが，重要と考えられる。

C　：　場合によっては必要となる機能である。

表３－２　ＳＯＳの考慮事項の一覧表

	考　慮　事　項
実現手段面	①　主記憶 ②　アドレス表現 ③　ＣＰＵの実行モード ④　汎用レジスタ ⑤　チャネル／ＤＭＡ ⑥　アクセス仲介機構 ⑦　ディシジョン・テーブル機構 ⑧　暗号化機構 ⑨　パトロール機構 ⑩　本人確認手段
品質保証面	①　ソフトウェアの品質保証 ②　ＳＯＳの検定（侵入テスト） ③　環境シミュレータ ④　ソフトウェアの遠隔保守 ⑤　ハードウェアの遠隔保守
運用管理面	①　コンピュータ関連要員の資格区分支援機能 ②　開発と本番の隔離支援機能 ③　インストレーション作業の監査支援機能 ④　プログラム移管支援機能 ⑤　システム・ダウン後の復旧支援機能 ⑥　リモート・プログラミング監査支援機能

ておく。そして，下段は運用管理を円滑に行うためにＳＯＳに要求される支援についてまとめたものである。

(3)　ＳＯＳの開発に向けて

ＳＯＳはコンピュータ・セキュリティ対策の技術的基盤である。すなわち，ＳＯＳによって技術的基盤が強固に構築されていないと，軟弱地盤に建築された建物と同様に，不安で，危険が一杯である。したがってＳＯＳが健全な情報化社会の構築のための欠くことのできない技術的対策であり，緊急を要する研究開発課題である。

ＳＯＳの研究開発では，要求仕様作成技術や検証技術の研究・実用化がキー・ポイントであり，ソフトウェアの基礎研究的色彩の強い長期的研究課題が多く，一研究機関あるいは一企業での研究開発課題の範囲を越えており，官・学・民が一体となって取り組むべきである。したがって，セキュリティの基盤技術であるとともにソフトウェアの先端技術でもあるＳＯＳの研究開発を国家的プロジェクトとして採り上げるべきであると提案する。

3.2　システム監査支援ツール

当プロジェクトでは，システム監査の実施手順を把握するため，最初にシステム監査の分析を行った。分析の結果，実際のシステム監査への要求が極めて多様であることが判明したため，最大公約数的実施手段の検討を行った。その結果，コンピュータ支援が可能な部分として認められたのは，

①　業務処理の記録（すなわちロギング）と，そのデータの検索・編集

②　上記①の結果の判断

である。上記の①，②は，図３－１の①，②に対応する。

図３－１の①の段階は，図３－２に示すように，収集（記録）と検索・編集の２つの機能に分解でき，市販のツールの大半は，図３－２の㊁の部分の支援ツールであることが確認された。

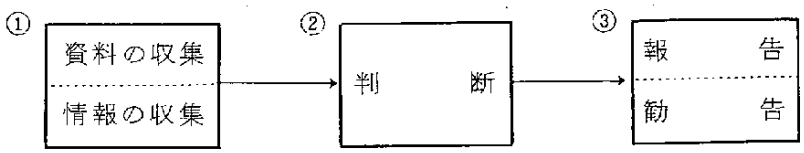


図３－１　システム監査の作業手順

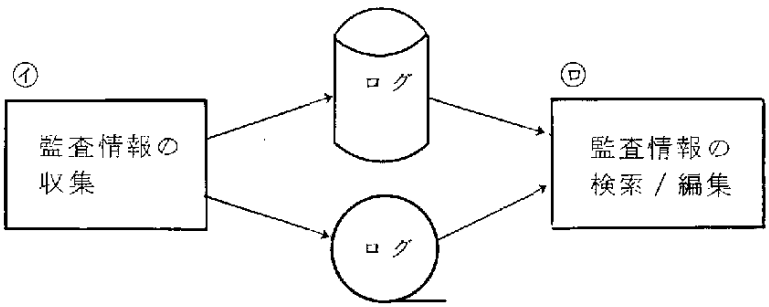


図３－２　資料／情報の収集段階

ここで問題点の検討結果を述べると，次のようになる。図３－２の㋑の段階で使用できるツールが少なく，効率上の問題があり，データ保護の面でのセキュリティ上の問題がある。図３－２の㋺の段階に使用できるツールは多数あるが，その検索・編集機能は必ずしも充分とは言えない。図３－１の②の段階で使用するツールには，現在のコンピュータ・アーキテクチャは向いていない，等である。

以上の結果を考慮し，新しいシステム監査支援ツールを，次の２つの観点から検討した。

① 現状技術の応用 …… ロギングに関する新ツール（短期的に実現できる。）

② 新しい技術である知識工学の応用 …… 判断の段階（図３－１の②）で使用可能なツール（長期的な研究開発が必要）

以下に，新しいシステム監査支援ツールの検討結果を示す。

(1) ロギング・ツール

このツールの目的は，ログ・データの保護対策の強化と，効率の改善である。従来のツール（代表的なのは ＳＭＦ[*1]である）は，この面でかなり問題があっ

＊1：System Management Facility

た。当プロジェクトの提案するツールは，図３－３に示すもので，ロギング・サブ・システムと呼ぶ。その特徴は，

① 専用ハードウェア化

② 大容量ファイルによる無人運転の実現

③ 新記録媒体（再書込不能型光ディスク）の使用

④ サブ・システム自身で検索・編集機能を持つ

等である。このことによって，

- ログ・データ保護の強化（物理面，運用面）
- 効率の改善（その結果，レコード・アクセス情報等のようなきめの細い情報が記録可能となる）
- 操作性向上（ログ・データを何時でも検索編集可能になる）
- 運用の簡易化

等が，同時に達成可能となる。

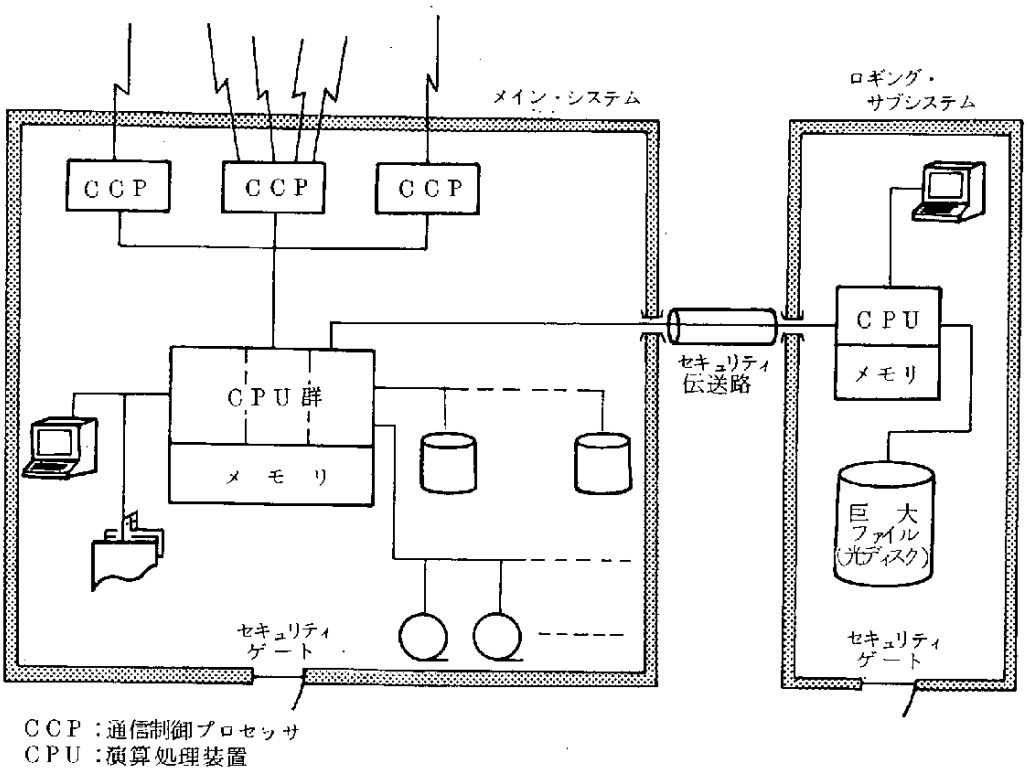


図３－３　ロギング・サブ・システム

ロギング・サブ・システムは，既存の技術で実現可能であるが，下記については，多少の改良が必要である。

① 再書込不能型光ディスク（大容量化，高信頼化）

② 高信頼システムの構築手法

本サブ・システムは，その技術内容から考えて，3～4年の期間で充分開発可能だと思われる。このツールによって，コンピュータに入力された情報はすべて収集できるので，その後の検索・編集を工夫することにより，システム監査の多種多様な作業に役立つ資料が作成可能になる。その意味では，ロギング・サブ・システムは，システム監査ツールの土台となる基本システムと言うことができる。

(2) 知識工学の応用

ロギング・サブ・システムで収集した情報を，さらにコンピュータ処理し，図3－1の②の段階の結果を直接出力できるようになれば，画期的なシステム監査支援ツールが実現できる。さらにこの結果を事前防止機構に直接フィードバックすれば，事後チェックは，システム監査の領域から，事前防止の範ちゅうに移行してしまう可能性さえある。

この夢のような構想を実現するためには，最初に図3－1の②の部分に適用できるツールを作らなければならない。当プロジェクトでは，様々な理由で（詳細は第Ⅱ部2.5.3を参照），現状でのノイマン・アーキテクチャを用いた実現は，ほとんど不可能だと結論した。そして，新しい技術である知識工学に活路を求めるべきだと考えた。知識工学とは，第5世代コンピュータとも呼ばれる，新しいアーキテクチャによるコンピュータの応用であり，現在世界各国で1990年代の実用化を目指した研究開発が活発に行われている。応用例を以下に示す。

① 知的検索・編集

新しい技術は，パターン・マッチングを極めて容易に実現できるだけでなく，さらに一歩進んで，パターン理解も可能なところに大きな特徴がある。これを応用すると画期的な検索ツールが実現できる。

ロギング・サブ・システムの収集したデータは，一種のデータベースとして考えることができる。これを検索するための条件は，従来は厳密に定義しなければならなかった。それでも数値条件であれば，それ程難しいものでもなかった。例えば，「支払額が千万円以上の取引」等のように決められた。しかし論理条件では難しい問題がある。例えば，「機械類の出荷額」という条件はどうであろうか。ファイルが，そのように仕分けしてあれば簡単であるが，そうでなければ，検索ロジックを作成しなければならない。このような検索の必要性はいくらでもある。例えば，「月末日の出荷額」,「欠損発生日」，「異例取引の検索」，……，etc。これらは，多大な労力を投入すれば，すべて可能な検索ではあるが，実用性に欠ける。

知識処理では，これらを容易に実現できる可能性がある。検索のロジックを自動作成できるからである。もちろん，自動作成するための専門知識を，あらかじめ入れて置かなければならない。知識の入力方法は，現在大きな問題になっているが，将来は容易になると言われている。知識の自動獲得も可能になると予想されている。

この検索は見方を変えれば，サンプリングでもある。しかし単純なサンプリングではなく，知的サンプリングと言った方がよいだろう。

② システム監査コンサルテーション・システム

検索システムのもっとも高級な機能は，「不正取引を検索せよ」という条件を投入できることである。ここまでくれば，事後監査は，単なるルーチン・ワークになるかもしれない。前述の知的検索・編集をさらに発展させれば，可能性がないとはいえない。

知的検索・編集は知能が低い段階，コンサルテーションは知能が発達した段階と言うことができる。図３－４は，実現予想図である。必要なのは知識である。不正に関する知識を入れれば不正の検出を，システムの効率に関する知識を入れれば，システム効率の測定を，自動的に行ってくれる。実現時期は，かなり先とだけ述べておく。

以上のように，知識工学の応用は有望であるが，基本となる第５世代コンピュータの実用化が１０年先というように，まだかなり長い年月に渡って，研究開発しなければならないことが難点である。しかし最近は，夢の実現が思いの他早くできることもあるので，研究すべき価値は十分あると考える。特に，システム監査コンサルテーション・システムは，不正検出の最終的形態であり，応用システムのセキュリティ対策に，大きなインパクトを与えるであろう。

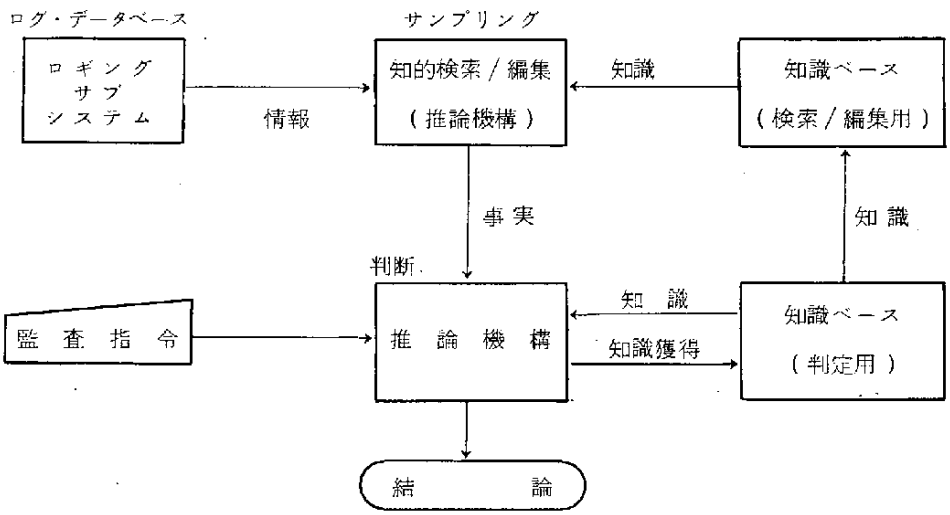


図３－４　システム監査コンサルテーション・システム

3.3　セキュア・ネットワーク

(1)　検討経過

ネットワークのセキュリティとは何かを分析するため，当プロジェクトは最初に，コンピュータ・ネットワークを通じて行われる業務処理（可能性のある業務処理も含む）を調査した。現状調査および机上の検討の結果，特にセキュリティ対策が重要と思われる業務処理として，

①　EFTS[*1]／ファーム・バンキング

＊１：Electric Funds Transfer System

② 電子化取引

③ 高付加価値情報の交換/売買

を想定することができた。これらの業務処理は，いづれも従来の書類（伝票類）をコンピュータ・メッセージ化（電子化伝票）するもので，まとめて電子化取引と呼ぶこととする。これらの業務処理は，流通効率化の促進を目的としており，特に③は商品自体も電子化情報なので，極めて効率が高く効果的な業務処理である。いづれにしても，電子化取引は新時代の情報処理の核となるアプリケーションである。

次に，我々は電子化取引を可能とするコンピュータ・ネットワークのセキュリティ対策を検討した。そのために，先ず，従来の書類をコンピュータ・メッセージに置き換える場合の問題点を検討し，メッセージ（電子化伝票）を交換可能なコンピュータ・ネットワーク・システム[*1]の必要条件を導き出した。その条件とは，

① メッセージの安全確実な転送 …… メッセージが，途中で改ざん，破壊あるいは盗聴されることなく，安全に正確に目的地へ送り届けられること。

② メッセージの安全な保存

転送されて，個々の応用システムに保存されたメッセージが，改ざんあるいは破壊されることなく保存されること。

③ メッセージの承認（オーソライズ）

転送されたメッセージが，責任者によって承認されているか，それとも単なる連絡情報なのかを区別する情報の，安全正確な伝達と安全な保存である。そこで，この対策に応用可能なセキュリティ基本技術を調査検討し，以下のような総合的対策案をまとめるに至った。

(2) 総合的対策案

電子化取引を実現するためには，ネットワークおよびそれに接続した応用シ

＊1 ： ここでは，個々の応用システムを含むコンピュータ・ネットワーク全体を，コンピュータ・ネットワーク・システムと呼んでいる。

ステムを含めた，コンピュータ・ネットワーク・システム全体のセキュリティ対策の確立が重要である。

しかし，これは理想像であって，現実的には，個々の応用システムのセキュリティ・レベルは異なるものとして，セキュリティ機構を検討する必要がある。この場合，あるサイトの応用システムにおけるセキュリティ上の問題が，他のサイトの応用システムに波及しないような歯止めが重要である。当プロジェクトは，この解決策として，

① 応用システムとネットワークとの間に物理的責任分解点を設ける。

② 責任分解点を境として，個々の応用システム内のセキュリティ問題は，その応用システムの管理者の責任とする。

③ 責任分解点を境として，ネットワーク内のセキュリティは，公正中立な第3者の機関（公証機関と呼ぶ）の責任とする。

ことにより，コンピュータ・ネットワーク・システムのセキュリティ管理を，個々の応用システムとネットワークに分割し，ネットワーク内での統一的セキュリティ対策が実現可能な方式を追求した。この方式では，ネットワーク内での統一的セキュリティ対策が防波堤になり，個々の応用システムのセキュリティ問題が，他の応用システムに波及しない利点がある。

さて，このような方式を実現するためには，ネットワークの統一的セキュリティ対策を行うために，公証機関が管理運用するネットワーク・セキュリティ・センタが必要であり，物理的責任分解点として，セキュリティ・ボックス[*1]が必要である。そして，それらによる電子化取引ネットワークは，図3－5に示すようになる。当プロジェクトは，これを，ネットワーク・セキュリティ・センタ構想と呼ぶ。

この構想では，ネットワーク・セキュリティ・センタ（ＮＳＣ）とセキュリティ・ボックス（ＳＢ）との組合せによる，強力な技術的セキュリティ機構が

＊1 ： 昨年度提案のセキュリティ・ボックスはメッセージ・ロギング装置，今年度提案のセキュリティ・ボックスはセキュリティ機構を持ったインタフェース装置でロギング機構を持たない。

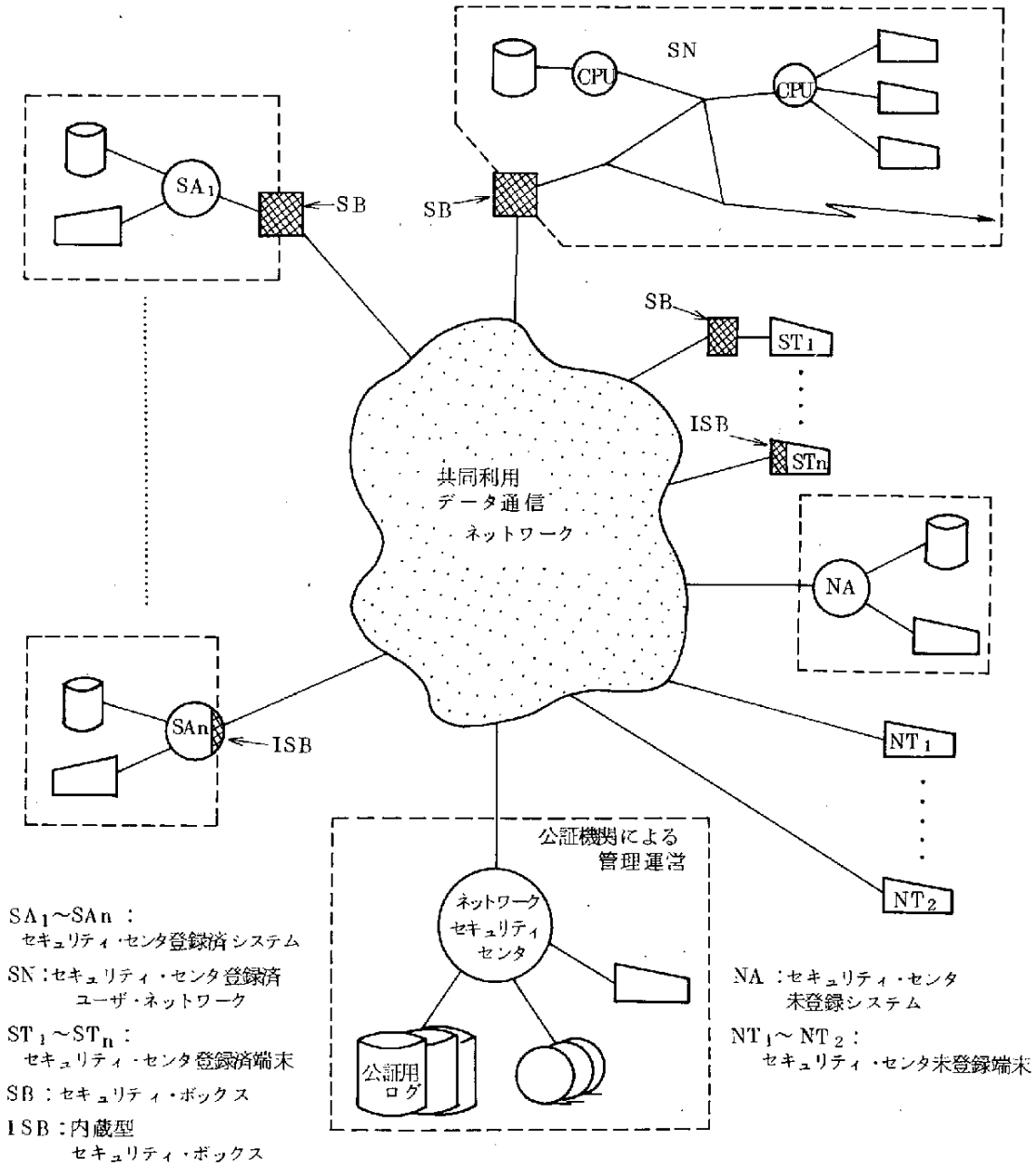


図３－５　ネットワーク・セキュリティ・センタ構想

構築でき，

- メッセージ内容の漏洩防止
- メッセージ内容の改ざん防止
- ネットワークの介入防止
- 送受信先の確認

が可能となり，メッセージを安全に転送できる。加えて，公正中立な公証機関がＮＳＣを管理運用することから，

① ＮＳＣのメッセージ内容の記録は，公証用ログとすることができる。

② ＮＳＣが，メッセージ発信人（受信人）のメッセージに対するオーソライズ状況（押印したかどうかを表す情報）を，記録保存することにより，過去に転送されたメッセージ（電子化伝票）が，発信人（受信人）によって承認されていたかどうかを，証明することができる。

等の機能を生み出すことができる。その結果，ネットワーク・セキュリティ・センタ構想は，電子化取引の基本的条件

① 安全なメッセージの転送

② 応用システム内に保存されているメッセージ内容の保障

③ メッセージ内容の承認機能（書類システムにおける押印）

を，満たすことが可能である。

我々は，国家的課題として，このネットワーク・セキュリティ・センタ構想の開発を提案する。主な開発課題を表３－３に示す。ネットワーク・セキュリティ・センタ構想の一つの特徴は，可能な限り技術的対策を行うことと，セキュリティ機構のハードウェア化である。セキュリティ機構のハードウェア化は，セキュリティ機構を強固にし，効率を改善し，さらに長期的視野では，コスト削減という効果も期待できる。我国の進んだハードウェア技術を生かすのにも都合がよい。

電子化取引は，時代の要請であり，流通の効率化に欠かせぬシステムである。今後の我国の社会・経済の発展に寄与するだけでなく，広く全世界の貿易事務の効率化にも，寄与するであろう。電子化取引をターゲットとするセキュリテ

表３－３　技術面での開発課題

課　　題	内　　容
専用ハードウェアの開発	・セキュリティ・ボックス ・ネットワーク・セキュリティ・センタのコンポーネント ｛暗号化機構 ｛アクセス・コントロール機構 ｛ロギング機構（ロギング・サブ・システム）
理想的基本技術の研究開発	・セキュリティ・オペレーティング・システム（ＳＯＳ） ・公開鍵暗号機構 ・新アルゴリズムの慣用暗号機構 ・パスワードやＩＤカードに依らない本人確認機構 ・高信頼／大容量，再書込不能型光ディスク
ソフトウェア	・高信頼化手法／技術

ィ技術の開発は，緊急を要する開発テーマであると考える。

3.4　開発課題／計画

当プロジェクトは，昭和５７年度より２年間に渡って，コンピュータ・システムのセキュリティについて，技術面から検討を行ってきた。その結果，多くの要検討項目を指摘することができた。昭和５７年度には，主に，セキュリティ機構を構築する時，核となる技術（セキュリティ要素技術）を提案し，昭和５８年度（今年度）には，要素技術を組合わせたセキュリティ機構を提案した。

これらの提案をすべて実現できれば，我国のコンピュータ・システムのセキュリティ・レベルは飛躍的に高まるであろう。しかし，すべての課題を一度に開発するのは，かなり難かしい。一方，要素技術については，個々の要素技術を別々に開発するよりは，互いに関連を持たせて開発した方が効果的である。その例を一つ示そう。本人確認技術とアクセス・コントロール技術は，互いに密接不可分

な技術である。本人確認が実行されなければ，いかに高級なアクセス・コントロール機構であっても，結果的に何をコントロールしているのか分らなくなってしまう。

問題は，どのように関連を持たせるかであるが，最終的なターゲット応用システムを通じて関連付けるのが，最も合理的である。例えば，セキュリティ・オペレーティング・システムの要素技術として，本人確認技術とアクセス・コントロール技術を開発すれば，要素技術の機能目標は，非常にはっきりとしたものになろう。

そこで，当プロジェクトは，表３－４に示すセキュリティ基本システムとそれに関連する要素技術を，開発課題として提案する。

これらの提案が理にかなったものであるかどうか，さらに詳細な検討を要するかもしれないが，実際に開発すること以上に，確実に効果を把握する方法はないだろう。また，新しいセキュリティ機構を開発することは，不幸にして予期した程の成果が得られなくても，我国のセキュリティ技術水準を確実に向上させるであろう。

加えて，強力なセキュリティ機構は，新時代の情報処理技術の中核であり，必須の技術であることは，明らかである。実現は，早ければ早い程よいが，セキュリティ機構の実現のためには，解決しなければならない課題も多数存在する。そこで，セキュリティ基本システムについて，妥当と思われる開発期間を示すと，次のようになる。

① セキュリティ・オペレーティング・システム（ＳＯＳ）
…… ８年（長期）

② システム監査コンサルテーション・システム
…… １０年以上（長期）

③ ロギング・サブ・システム …… ３年（短期）

④ ネットワーク・セキュリティ・センタ／セキュリティ・ボックス
…… ５年（中期）

表３－４　開　発　課　題

	ターゲット応用システム	セキュリティ基本システム	セキュリティ要素技術
個々の応用システム	応用システム　x （例：金融システム等）	• セキュリティ・オペレーティング・システム（ＳＯＳ） • システム監査・コンサルテーション・システム	• 本人確認機構 • アクセス・コントロール機構 • 暗号化機構 • 端末確認機構 • メッセージ認証機構 • ロギング用大容量ファイル（再書込不能型光ディスク） • プロセス隔離機構 • 使用済記録媒体白紙化機構 • セキュリティ管理者支援機能（マンマシン・インタフェース） • 高信頼ハードウェア構築法 • 高信頼ソフトウェア　〃 • 知識工学（不正の判断アルゴリズム研究開発）
コンピュータ・ネットワーク	コンピュータ・ネットワーク・システム　y （例：電子化取引ネットワーク等）	• ロギング・サブ・システム • ネットワーク・セキュリティ・センタ • セキュリティ・ボックス	

(注)　□ 内が，開発課題である。

このように，通常企業レベル等で行われる技術開発に比べて，かなり長期の開発期間が必要である。また，セキュリティ要素技術は，それが関連するセキュリティ基本システムや，ターゲット応用システムの開発に間に合うように，開発しなければならない。電子化取引ネットワークの開発では，当初は，汎用ＯＳのセキュリティ機能強化版（恐らくＳＯＳ開発初期に現れる）を用い，その後，本格的ＳＯＳを使用することになる。

我々の提案する開発課題には，ＳＯＳやシステム監査コンサルテーション・システムのように，基礎研究的色彩の強いテーマもある。そのため，一研究機関あ

るいは一企業内での開発テーマの範囲を，越えている可能性が強い。

加えて，セキュリティ基本システムは，要素技術の組合せで成立っており，いきおい開発規模も開発費も大きく成らざるを得ない。そのため，これらの開発課題が国家的課題としてとりあげられることを期待したい。表３－４のターゲット応用システムは，開発されたセキュリティ基本システムおよびセキュリティ要素技術を用いて，各企業／機関が独自に開発すべきシステムであり，国家的課題ではない。

コンピュータ・セキュリティとナショナル・セキュリティとが同等などとは，思わぬが，昨年度の報告書で，「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。」と指摘したように，応用システムは，セキュリティ技術なしには，成り立たないことは明らかである。あまりに当然のことなので，我々はめったに意識することはない。このように重要なセキュリティ技術の開発を怠り，海外に頼ろうとするならば，将来に大きな禍根を残すことにならないだろうか。我国の銀行等は，他の業種に比べれば，セキュリティ対策に関心が強いとはいうものの，決して充分というわけではない。幸いにも，今日まで，応用システムにとって 致命的なコンピュータ犯罪[*1]は，起きないで済んできた。これは，全く偶然としか言いようがない状況なのである。

しかし，ネットワーク化が進んでいる現在では，セキュリティ対策とは無関係に，ファーム・バンキングも電子化取引も進行する。もちろん，日本人がいつまでも善良だという保証など，どこにもない。やがて必ず，堪え難い犯罪が発生する。これは，決っして脅しではない。これまでの調査結果を総合して推測すれば，むしろ犯罪が起きないという結論の方が，余程不自然なのである。そうならないために，我国独自のセキュリティ対策を構築し，問題を克服しなければならない。

情報処理は，無限に拡大する。人手によるセキュリティ対策は，いづれ限界に近づき，今後の対策の主流は，技術的対策になる。そのための技術開発を，国家的課題として，一刻の猶予もおかず，開始すべきであると結論する以外にない。

＊１ ： 小さい事件は多数発生している。

4. 新時代の情報処理に向けて

4.1 情報処理発展の方向

コンピュータ・システムによる情報処理は，今や事務処理における基本的な手段となっている。コンピュータ以前の事務処理が紙とペンによって行なわれ，連絡が電話や郵送によって行なわれていたのに代わって，コンピュータのファイルのデータ通信がこれに置き代わりつつある。

コンピュータもデータ通信も，紙や電話に代わる事務処理のための手段にほかならない。しかし事務処理の手段が異って来れば，それを使いこなす人間の組織も事務処理の手順も変わって来る。銀行業務，商社業務など，特に情報を仲介することを主たる機能としている業種では，情報を取扱かう手段の変化によって，企業の業務そのものも変化してしまう可能性もある。

従来のコンピュータ・システムの導入は，当初は新らしい手段によってそれまであった業務の省力化，能力向上を目標として行なわれた。これはさらにコンピュータ・システムによってはじめて可能となる新らしいサービス業務を生じた。特にコンピュータ・ネットワークによる企業間接続は，企業間の関係を密接なものとし，企業間の新らしい関係を作り，より強い競争力を持つための道具として推進されている。

一方コンピュータのハードウェア技術の発展によって，パーソナル・コンピュータもしくはデスクトップ・メインフレームと呼ばれるような，小形コンピュータが安価に供給されるようになって来た。このような小形コンピュータを使う場合には，企業内で多数の機械をネットワークによって相互接続することによって，システムを形成する場合が多い。いわゆるＯＡネットワークと呼ばれる概念である。

4.2 セキュリティとシステム構成

このような業務の形態，コンピュータがスタンドアローンになっているのか，

企業間でネットワーク化されているのか，あるいは，企業内でもネットワーク化されているのかと言ったシステムの形態の区別は，セキュリティの考え方にも種種の差をもたらす。

セキュリティとは安心ということである。コンピュータに仕事を任せて安心していられる状態を作るには，どうしたらよいであろうか。この問題は処理の道具がコンピュータではなく，紙とペンであった時代からも本質的には同じ問題である。我々が安心して書類を扱かえるのはどのような条件においてか，我々が安心して取引きできるようになるにはどのような条件が必要かということを，従来の伝統的事務手段とコンピュータによる事務手段について考えるとき，事務手段とセキュリティ確保の関係には多様な要素が介在しているように思われる。

セキュリティの問題は，紙によるファイルを作り人間が情報を処理した時代から，コンピュータが情報を処理し，磁気媒体上にファイルが作られるようになった今日まで，本質的には同様の問題をかかえている。人間が情報を処理している時代でも，担当者がその情報を乱用することによって犯罪が形成されることは，必ずしも希ではなかった。これを防止するために人間の事務組織の中には高度な相互牽制のシステムが組込まれており，このシステムは本来業務の一部と混じりあって，それとは気付かぬ形になっているものもある。

このような人間の事務組織におけるセキュリティの対策は，人間の特性に合わせて作られたものであり，その中でセキュリティに関するコストを計算すれば，無視できない額に達することはまちがいない。ひとつの決裁の書類に対して，何人もの上長が次々に印を押すシステムは，純粋の事務の能率の向上の観点からすれば，全く無駄な行為に思われるが，これも既に習慣として確立した，セキュリティ対策である。しかしこの習慣は，セキュリティ対策であると同時に，人間の犯し易すい善意の誤りに対する対策であると，理解されている場合も多い。

コンピュータ化に際しては，後者の側面が強調されるならば，入力帳票の作成に際しての誤りの検査を行なったあとには，最終的な処理までのチェックの必要はないことになり，無チェック状態での処理が行われるようになっている場合も少なくない。特に，コンピュータ導入の初期においては，その狙いが省力化にお

かれており，必ずしも充分なチェックが行われるということではなかった。

コンピュータがスタンドアローンで，計算機室に閉じている限り，処理用のプログラムさえ正当であれば，コンピュータは正しい結果を生ずる筈である。そこで，セキュリティ対策は，もっぱら計算機室の入退のチェックと，計算機室の保護に重点がおかれた。

しかし，コンピュータがネットワークを介して，より開かれた形になってくると，セキュリティ問題は，より複雑な様相を呈することになる。計算機室を保護するのと同様の保護は，通信回線と端末を含む広い範囲に，及ばなければならなくなる。企業間接続の場合には，異企業間でやり取りされるデータの正しさについて，企業間でどのような責任体制をとるかも，大きな問題である。

企業内のコンピュータ・システムが，小形コンピュータのＯＡネットワークによって実現されている時には，コンピュータに対するアクセスをどのように管理し，それぞれの小形コンピュータの中で実行されるプログラムの正当性を，どのように確保するかには，まだ多くの問題が残っている。

セキュリティに対して考えなければならないことは，どのような処理の道具を使うかによって，それぞれ異っている。今後進展してゆく各種の高度なコンピュータ・システムにおいては，セキュリティ上配慮しなければならないことは増大し，その解析はますます複雑化して来ると，考えなければならない。

4.3　セキュリティ技術

コンピュータ・システムは，多様な応用に用いられる。これを利用する環境も多様であり，またシステムは故障，保守など種々の状態を持ち，それぞれの状態に応じて，異なる人間が異なる方法で，システムにアクセスする。

コンピュータ・セキュリティ技術としては，その正常な運用時において，入力帳票のチェック，端末における本人確認，通信回線上での保護，コンピュータへのアクセス管理，リソース管理，データ管理，さらにはプログラムの監査などがその技術要素となる。

これらの要素技術は，どのような対象者を相手にするかによっても異なる。コ

ンピュータにアクセスする資格には，種々のレベルがあるが，全く資格のない者を対象にして保護する場合から，最高の資格を持った者のアクセスを対象とする場合も，考える必要があり，それぞれの場合で問題が異なることになる。

セキュリティ技術は，こうした多様な場合におけるあらゆる状況において，システムを保護できるようになっていなければならない。セキュリティ技術の各技術要素を，それぞれ完全に作っておいても，それらの要素の組合せのすき間を抜けて，システムに不正アクセスする可能性が，ないとはいえない。

しかし反面，そのような状況ばかりを考えているのでは，それぞれのセキュリティ要素技術の発展が，阻害される可能性が強い。現時点においては，それぞれのセキュリティ技術によって対処しようとする脅威の範囲を明確化し，それによって，どのような効果のある対応ができるのかを，明らかにしておくことが，重要であると考える。

本報告書の第Ⅱ部で述べられているセキュリティ・オペレーティング・システム（ＳＯＳ）は，アクセス管理の条件を明確化し，その条件においては，アクセスが完全に保護されることを，確保しようとするセキュリティ基本システムである。これは反面，規定された条件以外の場合には，セキュリティは確保されないことを示しているのであり，これ自体では，完全なアクセス管理が行われることを保証していないことも，明らかである。

また，ネットワータ・セキュリティ・センタの考え方は，システム間でやり取りされるデータについて，客観性のある証拠を確保することを目的とするものであって，事故が生じた時の回復処置について，あらかじめ準備されていなければ，充分に機能し得ない可能性がある。

しかしここで重要なことは，その有効な範囲を明確化したうえで，セキュリティ要素技術を積み上げてゆくことであろう。

実際のシステムにおいて，実効あるセキュリティ対策を作り上げてゆくには，これらのセキュリティ技術を，その応用の場面に応じて，適切に組合わせてゆく必要がある。この場合に重要なことは，各々のセキュリティ技術の効果が，客観的に明確化されていることである。その効果を明確化した上で，総合的配慮とし

てより安全度の高いシステムを構築できるようになると思われる。

セキュリティに関しては，人間的要素は大きな要素である。各種のアクセス資格を持った者の不正アクセス，特に高いアクセス資格を持つ者のアクセスに対してセキュリティを確保することを考えるときには，所詮は人間の問題であって，限界があるとの考え方も少くない。しかしセキュリティ技術では，高位の資格を持ったユーザの不正利用に対しては完全な防護は不可能であるにしても，システムが破滅的な被害を受けないようにするための，何かの処理が行なわれるようになっていなければならないであろう。セキュリティの問題にはこうした人間的要素も含めての総合的配慮が重要であると考えられる。

現在のところ，こうした総合的配慮とセキュリティの技術要素の区別は必ずしも明確ではない。むしろそれぞれの要素技術によって，セキュリティが確保されるかのような誤解も少なくない。それぞれの応用におけるこうした総合的考え方の方法論の確立は今後の課題である。

4.4　新しいシステムにおけるセキュリティ

コンピュータ・システムの応用は，これからもますます社会の広い領域に浸透してゆく。コンピュータ・システムの使用される態様によって，そのセキュリティについて検討しなければならない課題は，ますます多様化して来ると考えられる。

本報告書におけるセキュリティ上の課題は，実際のシステムのセキュリティ核となるセキュリティ基本システムであり，コンピュータ本体に対するアクセスの保護を行うことを目的としたＳＯＳ，応用ソフトウェアの製造時の正しさの検証と，それによって処理されたデータの正しさを確認することを目的としたシステム監査支援システム，ならびに電子化取引における取引データの記録と証明のための確認システムである。

これらは，スタンドアローン・システムから，それがより開かれたシステムに移行する段階での，セキュリティ上の課題に対処する基本システムであり，これらの基盤技術と従来から知られている他の技術要素を組合せ，総合的配慮を高め

ることによって，これからますます発展するコンピュータ・システムのネットワーク化と分散化の動向に対して，セキュリティ上の有効な手段となり得るものである。

これと同時にこれからの情報システムは，そのシステム形態からも応用からもますます分散化の方向に進むことは明らかである。コンピュータ・システムを常に安心して使える状態にすることは，これからのコンピュータ・システムの発展と社会の安定化のひとつの鍵であり，多様なシステムについてこの状態を作り出すためにセキュリティ技術の新らしい課題と，それぞれの応用における総合的な配慮の方法論について，より広い研究が進められることを期待したい。

第II部　各　　論

1. コンピュータ・システムのセキュリティ基盤技術

本章では，コンピュータ・システムの主としてオペレーティング・システム（ＯＳ）のセキュリティ対策について検討した結果を述べる。昨年度（昭和５７年度）は，主にコンピュータ・セキュリティの要素技術について報告したが，今年度は，それらのセキュリティ要素技術を最適に統合したＯＳについて検討し，報告することとした。

コンピュータ・システムのセキュリティ確保の技術的対策の基本はＯＳにある。ＯＳのセキュリティ機能が強固に構築されていないと，軟弱地盤に建築された建物と同様に，不安で，危険が一杯である。高度なセキュリティ機能を統合したＯＳは健全な情報化社会の構築のための欠くことのできない技術的対策であり，緊急を要する研究開発課題である。ここでは，高度なセキュリティ機能が統合され，強固に構築されているＯＳをセキュリティ・オペレーティング・システムあるいはセキュア・オペレーティング・システム（ＳＯＳ）と呼んでいる。当プロジェクトは，このＳＯＳをセキュリティ基盤技術として採り上げ，技術的に検討した。まず，第1.1節で調査研究の概要を述べ，そして第1.2節～第1.7節で検討結果の詳細を述べる。

1.1 概　　要

1.1.1 検討経過

本プロジェクトでは，昭和５７年度より２年計画で「コンピュータ・システムのセキュリティ」の技術的対策を中心に調査研究を行ってきた。

昨年度（昭和５７年度）は，表１－１に示す「検討すべき基本技術」を抽出し，今後の詳細な検討の必要性を指摘した。そしてコンピュータ・セキュリティ確保の技術的対策の基本はオペレーティング・システムにあることが認識された。また平行して行った「米国におけるコンピュータ・セキュリティの現状と動向」の調査結果から，米国防省がここ数年来先導して「セキュア・オペレーティング・システム」（ＳＯＳ：Secure Operating System）の研究開発を行っており，その重要性が再確認された。しかしながら我が国でこの方面の研究開発は皆無で，緊急を要する研究課題とはまだ認識されていない状況にある。

米国防省では，ＳＯＳに対して主として次の３つの要求事項を満たすことを開発目標として挙げている。

① すべてのファイルに対するアクセスは，例外なくセキュリティ・カーネル（security kernel）と呼ばれるＳＯＳの中核で不正アクセスか否かを検査できること。

② セキュリティ・カーネルを形成しているコンピュータ・プログラムは，いかなるプログラムによっても修正，変更，妨害を受けないこと。

③ セキュリティ・カーネルは，仕様書で指定されたセキュリティ機能に関することのみ行い，指定されない作業は絶対に行わないこと。換言すると，セキュリティ・カーネルは，その機能および実現が正当であることが検証されていること。

特に③の要求事項が最重要と考えられる。③は，セキュリティ・カーネルがプログラムとして正しく機能するための条件であるが，ソフトウェア工学の観点から見ると，ここにＳＯＳの研究・開発の大きな意義がある。

ＳＯＳを評価するため，米国防省では，コンピュータ・システムをそのセ

表１－１　検討すべき基本技術（つづき）

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１－１　検討すべき基本技術（つづく）

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

キュリティ・レベルでA（最高）～D（最低）までのランク付けしている。さらにランク内にも順位があり，全体で8段階のランクに細かくセキュリティ・レベルが分かれている。最高のAランクは最高機密情報を扱っても安全というものだが，ＳＯＳはAランクを目標にしている。AランクのA－1では，基本ソフトウェアに関する仕様が完全に明確であり，かつ最高セキュリティを実現していることが設計レベルで形式的に検証されていることを要件としている。この上のA－2では，仕様に従って作成されたプログラムが仕様書通りに具体化されたものであることが形式的に検証されていることを要件としている。今のところA－2レベルに適合したシステムは，公表された情報で知り得るかぎり存在しない。またA－1のレベルのものも現在開発中であり，完成して本番稼動しているシステムはまだない。

いずれにしてもセキュリティの基盤となる機能は可能な限りＯＳによって実現されることが望ましいことは確実であり，そのような観点から，ＳＯＳが今後重要な研究課題であることが明らかとなった。そこで，今年度（昭和５８年度）は，ＳＯＳを1つのテーマとして採り上げ，特に商用システムにおけるＳＯＳへの要求を中心に調査・検討することになった。

1.1.2　今年度の作業方針

商用システムにおけるＳＯＳを調査・検討するに当って，以下の作業方針を立てた。

① 現在までに開発されたＳＯＳの基本概念は何であるかを明確にする。

② 軍用システムにおけるＳＯＳと商用システムのＳＯＳとの差異はどうあるべきかを検討する。

③ 商用システムにおけるＳＯＳの持つべき機能を明確にする。

④ ＳＯＳを実現するために必要な条件や関連技術を明確にする（ソフトウェア工学，検証技術等含む）。

⑤ ＳＯＳの開発に向けての計画を立案する。

但し，ＳＯＳ自体ではない周辺問題は棚上げし，検討対象外とした。例えば，

正当な人による不正データの作成／入力，ハードウェアの故障によるセキュリティ機構の不完全さ，ハードウェア／ソフトウェアに係わる保守の問題等は検討対象外としたが，今後検討すべき重要な課題であることを指摘しておく。

1.1.3 今年度の作業内容及び検討結果

(1) 既存のＳＯＳの調査

現状でのＳＯＳの開発状況を把握し，技術レベルを確認するために，文献調査を行った。既存のＳＯＳあるいは高信用コンピュータ・システム（trusted computer system）として研究開発中のものを含めると，約３０システムが存在し，ほとんどすべて軍用のシステムである。この内，重要と考えられる次の６つのシステムにつき公表されている文献をもとに，その詳細を調査した。

① Multics Security Enhancements
② UCLA Data Secure Unix
③ KVM/370 （Kernelized VM/370）
④ KSOS（Kernelized Secure Operating System）
⑤ SCOMP（Secure Communications Processor）
⑥ PSOS（Provably Secure Operating System）

調査結果を表１－２に示す。表１－２の性能欄を見るとわかるように実用に供せるＳＯＳはまだ開発されていない。しかし，ＨＩＳ社（Honeywell Information Systems）で開発したSCOMPは商用の汎用ＳＯＳであり，現在米国防省のCSEC（Computer Security Evaluation Center）でＡ－１レベルに適合しているか否かの認定作業中であり，今後の実用化が注目される。

(2) ＳＯＳに対する要求機能とその実現手段

既存のＳＯＳはほとんどすべて軍用のシステムであり，軍のセキュリティ・ポリシーを反映した形式的なセキュリティ・モデルに基づいて構築されている。開発されたシステムは試行的なシステムであり，一部が実際に使用されているといわれているが，性能的に妥当な段階に至っていないし，モデルが軍の要求に基づいていることから，特殊なものと考えられる。

商用システムは，経済性が重要視される。そのため，従来，セキュリティ機能はオプショナルと考えられてきた。その結果，技術的なセキュリティ対策は高価であるという認識が一般的なものとなった。しかし，近年のコンピュータ関連技術の急速な進展の成果を活用することによって，従来は経済性や効率性の点からオプションにせざるを得なかった機能を徐々に標準的なものとして，とり込むことも可能になる。

そこで，商用ＳＯＳをその具体化の例として考え，多様な利用目的に共通したセキュリティ機能を抽出し，商用ＳＯＳの要求とした。

表１－３はその要求機能である。また機能項目毎に若干の配慮を加え，要求度合としてＡ，Ｂ，Ｃのランクを付けてみた。なお要求度合ＢあるいはＣの機能もＳＯＳ完成後に追加されるのではなく，その機能が必要であると判断される場合には，システム設計段階から考慮され，織り込まれていなければならない。

次に表１　４は，ＳＯＳの考慮事項をまとめたものである。表の上段はＳＯＳを構築する際に有用と考えられる実現手段をまとめたものであり，中段はＳＯＳのソフトウェア及びハードウェアに対する前提条件をまとめたものである。特に「ソフトウェアの品質保証」は今後の最重要課題であることを再度指摘しておく。そして，下段は運用管理を円滑に行うためにＳＯＳに要求される支援についてまとめたものである。

(3)　ＳＯＳ開発の波及効果

１９８０年代に入ってもソフトウェア危機に対して一向に解決の兆しが見えない。ＳＯＳの研究開発はソフトウェア危機の解決に対して画期的なブレークスルーをもたらすと期待されている。ソフトウェア・ライフサイクル全体での現在の開発費と保守費の割合をみると，保守費が全体の７割を占めているといわれている。そして今後も保守費の割合が増大すると想定される。ではなぜ保守の割合が増大するかといえば，ソフトウェアにある種の欠陥があるからである。その欠陥はプログラムのバグであったり，あるいは機能不足である。ＳＯＳの研究開発では，これらの欠陥を事前に取り除くことを最重要視している。即ち，

表１－２　調査対象の Secure

プロジェクト名	開発開始年	スポンサー	構築者	セキュリティの目標	方法論
Multics Security Enhancements	70年代初期	空軍 Honeywell	Honeywell Mitre	セキュリティ強化版の汎用TSS	Bell-LaPadulaモデルを励行するため，既存の検査機構を改造する。
UCLA Data Secure Unix	70年代初期	DARPA	UCLA	セキュリティ強化版のUnix	• セキュリティ・カーネル • Unix エミュレータ
KVM / 370	1976	DARPA 空軍 DCA	SDC	セキュリティ強化版の汎用TSS	仮想マシンを改造してセキュリティ・カーネルを組み込む。
KSOS	70年代後期	NSA DARPA 海軍	FACC Logicon	本番用のプロトタイプ：高安全Unix	• セキュリティ・カーネル • Unix エミュレータ • 高信用プロセス
SCOMP	70年代後期	Honeywell DARPA DCA NSA 海軍	Honeywell	本番用のプロトタイプ：高安全Unix	• セキュリティ・カーネル • Unix エミュレータ • 高信用プロセス • ハードウェア支援機構
PSOS	1980	NSA	FACC Honeywell	セキュリティ・ケーパビリティを基盤とするオペレーティング・システム	ＯＳ全体の仕様を形式的に記述して，検証を行なう。

略語

〔　〕：予定

AFDSC : Air Force Data Services Center

DARPA : Defense Advanced Research Projects Agency

DCA : Defense Communications Agency

DoD CSEC : Department of Defense Computer Security Evaluation Center

FACC : Ford Aerospace and Communications Corp.

Operating System（SOS）一覧表

形式的仕様	検証	ハードウェア	プログラミング言語	性能	DoDの *1 運用モード	DoD CSECの *2 評価基準	設置箇所
No	No	Honeywell 618 DPS8/70M	PL/I	Yes	Controlled (Secret 以下の機密データのみ処理対象とする。)	B－2	Pentagon AFDSC〔DoD CSEC〕
Yes	一部	PDP-11	UCLA-Pascal	デモ用	No	A－1	UCLA
Yes InaJo	Yes ITP	IBM4331	Jovial J3	デモ用	〔多重レベル〕	A－1	Mitre SDC
Yes Special	Yes Boyer-Moore	PDP-11	Modula	No	〔多重レベル〕	A－1	Logicon Mitre
Yes Special	Yes Boyer-Moore	Honeywell Level 6	UCLA-Pascal C	未完成	〔多重レベル〕	A－1	Mitre DoD CSEC Logicon
Yes	Yes 人手	Honewell（新型）	Ada	作成されていない	〔多重レベル〕	A－1	—

UCLA : University of California at Los Angeles
NSA : National Security Agency
SDC : System Development Corp.

〔注〕*1 ：運用モードとして，Dedicated, System high, Controlled, Miltilevel の4つのモードが規定されている。

*2 ：B-2=Structured Protection，A-1=Verified Design，A-2=Verified Implementation

表１－３　ＳＯＳの要求機能の一覧表

ＳＯＳの要求機能	要求度合＊
(1)　本人確認機能	A
(2)　アクセス制御機能	A
(3)　プロセス隔離機能	A
(4)　使用済記録媒体白紙化機能	A
(5)　ジャーナル／ログ機能	A
(6)　セキュリティ管理者支援機能	A
(7)　システム監査支援機能	B
(8)　シャットダウン防止機能	B
(9)　システム監査用の出口の常設	B
(10)　リモート・プログラミング抑止機能	C

＊　：　要求度合

Ａ　：　核となる機能で必須である。

Ｂ　：　周辺機能であるが，重要と考えられる。

Ｃ　：　場合によっては必要となる機能である。

表１－４　ＳＯＳの考慮事項の一覧表

	考　慮　事　項
実現手段面	①　主記憶 ②　アドレス表現 ③　ＣＰＵの実行モード ④　汎用レジスタ ⑤　チャネル／ＤＭＡ ⑥　アクセス仲介機構 ⑦　ディシジョン・テーブル機構 ⑧　暗号化機構 ⑨　パトロール機構 ⑩　本人確認手段
品質保証・保守面	①　ソフトウェアの品質保証 ②　ＳＯＳの検定（侵入テスト） ③　環境シミュレータ ④　ソフトウェアの遠隔保守 ⑤　ハードウェアの遠隔保守
運用管理面	①　コンピュータ関連要員の資格区分支援機能 ②　開発と本番の隔離支援機能 ③　インストレーション作業の監査支援機能 ④　プログラム移管支援機能 ⑤　システム・ダウン後の復旧支援機能 ⑥　リモート・プログラミング監査支援機能

要求仕様を厳密に記述し，検証し，できあがったプログラムに対しては形式的検証を課し，さらにシステム全体での欠陥をなくす侵入テストを義務付けている。ＳＯＳの研究開発を行うことによって，これらの技術（要求仕様作成技術，検証技術）の進展が期待できる。現在，ソフトウェアの生産現場で緊急に必要とする技術は，ソフトウェアの品質保証と生産性を画期的に向上させる技術であり，ＳＯＳの研究開発の目的とも合致している。そして，コンピュータ・システムのセキュリティ保持の基盤確保の上でも，ＳＯＳの研究開発が要請される。

(4) ＳＯＳの開発に向けて

ＳＯＳはコンピュータ・セキュリティ対策の技術的基盤である。すなわち，ＳＯＳによって技術的基盤が強固に構築されていないと，軟弱地盤に建築された建物と同様に，不安で，危険が一杯である。したがってＳＯＳは健全な情報化社会の構築のための欠くことのできない技術的対策であり，緊急を要する研究開発課題である。

ＳＯＳの研究開発では，要求仕様作成技術や検証技術の研究・実用化がキー・ポイントであり，ソフトウェアの基礎研究的色彩の強い長期的研究課題が多く，一研究機関あるいは一企業での研究開発課題の範囲を越えており，官・学・民が一体となって取り組むべきである。したがって，セキュリティの基盤技術であるとともにソフトウェアの先端技術でもあるＳＯＳの研究開発を国家的プロジェクトとして採り上げるべきであると提案する。

1.2　ＳＯＳの基本技術の現状

本節では，ＳＯＳ（ Secure　Operating　System ）を構築する際に根幹となる基本技術の現状について述べる。

先ず，1.2.1では，ＳＯＳを理解する上で必須の重要な用語を簡潔に解説する。1.2.2では，高品質・高信頼性のソフトウェアを開発する方法論について解説し，1.2.3では，その内でも高品質・高信頼性を保証する最も期待されている手段である検証技術を採り上げ検討し，最後の1.2.4では，ＳＯＳの構築の際の実世界での強固さを実証するために行われる特異なテストである侵入テストについて解説する。

1.2.1　ＳＯＳの基本用語

本項では，ＳＯＳ（ Secure　Operating　System ）や高信用コンピュータ・システム（ Trused　Computer　System ）を検討する上で，しばしば用いられる重要な基本的用語について定義と簡単な解説を行う。用語としては，次に示す術語を採録し，アルファベット順に並べてあり，本章を読む際に適時参照されたい。特に重要な用語は，1.2.2～1.2.4で詳細に述べられている。

- Bell-LaPadulaモデル（Bell-LaPadual model）
- 資格（ Capability ）
- 封鎖（ Confinement ）
- データベース（ Database ）
- 暗号化（ Encryption ）
- ガード（ Guard ）
- 情報フロー分析（ Information　Flow　Analysis，IFA ）
- 評価尺度（ Measure ）
- ネットワーク・アーキテクチャ（ Network　architecture ）
- 稼動モード（ Operation　mode ）
- 侵入テスト（ Penetration　test ）

・プロトコル(Protocol)
・参照モニタ(Reference monitor)
・リスク評価(Risk assessment)
・セキュリティ・カーネル(Security kernel)
・セキュリティ・モデル(Security model)
・仕様化技法(Specification technique)
・高信用(Trusted)
・検証技法(Verification technique)
・仮想マシン(Virtual machine)
・仮想記憶(Virtual memory)

Bell-LaPadulaモデル（Bell-LaPadual model）

Bell - Lapadulaモデルは，参照モニタ（ reference monitor ）の概念に基づくセキュリティ・モデルであり，DoD（U. S. Department of Defense，米国防省）のコンピュータ・システムの試作品に広く適用されている。このモデルの2つの基本規則は，単純セキュリティ条件（ simple security condition）及び＊性（＊- property ）である。単純セキュリティ条件は，任意のセキュリティ・レベルを保持する主体（ subject ）が，自分と同じかあるいはそれ以下のセキュリティ・レベルを保持する対象（ object ）に対して読取りアクセス操作のみを許す（すなわち，no read up ：上を読むことはできない），という規則である。一方，＊性は任意のセキュリティ・レベルを保持する主体が，自分よりも下位のセキュリティ・レベルを保持する対象に対して書込みアクセス操作を禁止する（すなわち，no write down ：下へは書けない），という規則である。しかし，例外規則として，高信用主体（ trusted subject ）に対しては，＊性に違反してもよいとしている。高信用主体は，システム中ではプロセスとして実現されるので，高信用プロセス（ trusted process ）としても知られている。

資格（ Capability ）

資格とは，偽造不可能な鑑札のことである。この鑑札を保持している主体に対しては，特定の対象に対して特定の型（ mode ）のアクセス操作が許可される。資格は許可されるアクセス・モードを定義する付加ビット付きの仮想アドレスとして実現可能である。資格は，対象へのアクセスを制御する機構であり，セキュリティ・ポリシーを実現する機構ではない。

資格を導入しているシステムの大部分では，アクセス制御の励行は，非集中的に行われている。すなわち，資格がプロセスに付与されると，そのプロセスは自由に自分の資格を他のプロセスに付与することが可能である。そのため鑑札が悪の札になってしまうのを妨ぐのが困難である。資格を実現する適切なハードウェア機構が欠如している場合には，資格を基盤とするコンピュータ・システムは良好に動作しないようである。

資格機構をハードウェアで実現したコンピュータとして，現在，Plessey S/250（英国のBritish Plessey Corporation），IBMシステム38，Intel 432等がある。資格概念を導入したシステムとしては，UCLA Data Secure Unix Kernel，Kernelized VM/370，PSOS（Provably Secure Operating System）等がある。

記述子（descriptor）という概念は，自プロセスの実行環境内でのみ有効であるという点を除いて，資格と同じ概念である。そのため，プロセス間で記述子を付与し合っても意味がない。

封鎖（Confinement）

封鎖とは，プログラムが重要なデータ（sensitive data）を漏洩するのを防止することである。例えば，あるユーザが，機密データ（confidential data）を蓄積しているファイルへのアクセスを許可されたプログラムを使用して，そのデータを内秘に（不正に）複写し，それを他のユーザに転送することが可能である。この時，データを他のユーザに伝えるのに使用される通信路（channel）は微妙でとらえがたい。情報を伝送する手段としては，ファイル名等が付けられたシステムの記憶装置を経由して（storage channelと呼ばれる），システムの負荷状態を刻々変化させて（timing channelと呼ばれる）等があり，この手段を活用して，情報の使用許可権限を持たぬ第3者がその情報を得ることが可能である。

プログラムがデータを漏洩することが不可能である場合には，プログラムは封鎖状態（confined）にあると言える。実際には，ストレージ・チャネルをそのプログラムの形式的仕様書を分析することによって検出し，削除することは可能であるが（「情報フロー分析」の項参照），一方，タイミング・チャネルを制限することは可能ではあるが，削除するには多大な性能低下をもたらすのが普通である。

データベース（Database）

データベースとは，属性と値の組からなるレコードの集りのことである。高信用データベース管理システム（trusted database management system）を設計す

る際の課題は，情報の共用とアクセス権限を持たぬ主体による暴露（開示）の両方を工学的にいかに両立させるかである。

この課題に関して，ＮＲＬ（Naval Research Labaratory），Mitre 社等の研究機関で研究を行っているが，共通データベースを高信用（secure）にするのに，まだ成功していない。

暗号化（Encryption）

暗号は，権限を持たぬ人によるアクセスを防御できないような記憶媒体に蓄積されたり，あるいは，権限を持たぬ人による監視（monitor）を防御できないような伝送媒体上を伝送されたりするデータを保護するために使用される。ある場合には，情報源を確認（authentication）するために使用することもできる。データに対する保護強度は鍵の秘密性に依存しているので，鍵の保護及び分配は致命的因子である。

リンク暗号化（link encryption，あるいは link-by-link encryption とも言われる）は，データが通過するネットワーク内のすべてのノードでそれぞれ暗号化及び複合化処理を行うことを意味し，物理的経路（すなわち，リンク）を流れるデータに対して使用される。エンド・ツー・エンド暗号化の場合には，メッセージはネットワーク内の発信地（source）で一度暗号化されると，最終の目的地（destination）に到着するまで復号化されない。公衆鍵暗号系（public－key cryptosystem）では，メッセージを暗号化する鍵と，そのメッセージを復号化する鍵とは異なる鍵を使用しているので，暗号化鍵を公開することが可能である。

ガード（Guard）

ガードとは，セキュリティ・レベルの異なるモードで稼動している２つのコンピュータ・システム間，あるいはユーザ端末とコンピュータ・システムとの間に設置され，フィルタ機能（filter）を提供する処理装置のことである。ガードの典型的な例としては，重要なデータを保持しているシステムが，より低いレベルの重要なデータをも保持している場合に，全体として，高いレベルの重要なデー

タにアクセスする権限を持たぬユーザにも本システムへのアクセスを可能にするシステムである（「稼動モード」の項参照）。

ガード処理装置は通過するユーザの要求をすべて監視し，それに対するシステムの応答内容を検閲し，必要があればデータをサニタイズ（sanitize）したり，削除したりすることができるが，しかし，監視作業を任務とする人（watch officer）を必要とするかもしれない。（DoDでは，セキュリティ環境の異なるコンピュータ・システム間を転送される情報のすべてを人によるレビューを要求している。）ガードの事例としては，ACCAT Guard（Advanced Command and Control Architecural Testbed，最近では，単にGuardと略記されている），LSI Guard（DEC LSI-11），Forscom Guard（Army's Forces Command），RAP Guard（Restricted-Access Processor），Recom Guard，Message Flow Modulator 等がある。ACCAT GuardとForscom Guardではハネウエル社のScompを使用する予定になっている。

情報フロー分析（Information Flow Analysis，IFA）

情報フロー分析とは，プログラム内の変数に注目し，情報（あるいはデータ）がどの変数を通過するかを分析し，セキュリティの本性に違反しているか否かを検査する手法のことである。

コンピュータ・セキュリティの分野で最も重要な課題の1つは，権限のない人による重要な情報の暴露をいかにして防止するかである。重要な情報をアクセスするプログラム群が事故で，あるいは不正にそのデータをセキュリティ・レベルのより低いファイルに複写したり，あるいはオペレーティング・システムの漏洩チャネル（leakage channel，「封鎖」の項参照）を活用して，他のユーザに間接的にデータを手渡す危険がある。

情報を危険にさらす潜在的なチャネルを検出するために，プログラムやオペレーティング・システムに適用可能な各種の分析手法がある。

これらの分析手法には，プログラムあるいはそのプログラムの形式的仕様書中に現れる変数すべての間での可能な情報のフローを識別する手段が含まれている。

まず，セキュリティ・ポリシーに従って，各変数にセキュリティ・レベルが割り当てられる。セキュリティ・レベルとしては，束（lattice）が良く採用される。束は半順序集合で，次のような条件の時のみ情報のフローを許可する。変数Xのセキュリティ・レベルを$\underline{X}$で表すとすると，変数Xから変数Yへの情報フローは，$\underline{X} \leqq \underline{Y}$の場合，かつその場合にかぎって許可される。

これらの手法を使用して，文（statement）の型に応じて，情報フローを構文的に識別される。例えば，代入文

A ： ＝ B

は，BからAへのフローを意味するし，条件文

if B ＝0 then A：＝0

も同じ意味となる。

プログラムに対する情報フロー分析手法はD.E. Denningによって，形式的仕様書に対するそれはJ.K. Millen（Mitre社）によって，それぞれ提唱された。SRI社でも仕様記述言語Special（SPECIfication and Assertion Language）用に“Multilevel Security Formula Generator”と呼ばれる情報フロー分析システムを開発した。

評価尺度（Measure）

現在，システム・セキュリティの強度を定義する有効な定量的な評価尺度が存在せず，この重要な問題について研究がなされていない。唯一の有効な評価尺度は，侵入（penetration）の困難さの程度である。DoDのCSEC（Computer Security Evaluation Center）では，コンピュータ・システムがDoDのセキュリティ要求仕様のどの範囲を実現し，その実現が，どの程度信用（trusted）できるかの段階を定義した評価基準を確立している。(詳細は，1.3.8項の「米国防省のコンピュータ・セキュリティ評価基準」を参照)。

ネットワーク・アーキテクチャ（Network architecture）

ネットワーク・アーキテクチャとは，リンクとノードの両方を包含した体系の

ことである。軍のセキュリティの観点から見ると，ネットワーク・アーキテクチャの重大な問題点は，以下の通りである。

① ネットワーク・ポートに到着したデータに付けられているセキュリティ・ラベルを正しく中継することができるか。

② ネットワーク・ノードはこれらのラベルを保護し，ラベルが変更されたかを検出できるか。

③ 第3者がリンク上のトラフィックを監視することができるか。

この方面での直ぐに使用できる技術は，主としてリンク暗号化技術を基盤にしている（「暗号化」の項参照）。エンド・ツー・エンドの暗号化を採用して構築されたシステム（例えば，ガード）は，かなり成功している。ネットワーク・アーキテクチャの事例としては，Sacdin（Strategic Air Command Digital Network） RSRE / PPSN（英国防省のRoyal Signals and Radar Establishment / Pilot Packet Switched Network），Autodin II（DoD Automatic Digital Network），COS / NFE（Communications Operating System / Network Front End）等がある。WWMCCS（Word-Wide Military Command and Control System）の情報システム・プロジェクトでは，これらの問題点に対するいくつかの新しい解決策を提案するであろう。

稼動モード（Operation mode）

DoDでは，重要な情報（classified information）を処理するシステムがどのレベルの基準に適合している（accredit）かに応じて，稼動モードとして，次の4つのモードを規定し，採用している。

① 専用モード（Dedicated）

このモードでは，システムのすべての装置が，そのシステムによって排他的・独占的に使用され，かつ，そのシステムのすべてのユーザは，そのシステムが処理しているすべての情報に対する機密区分をクリアし，そのすべての情報に対する知る必要性（need-to-know）をも保持している。

② システム・ハイ・モード（System high）

このモードでは，そのシステムのすべての装置は，そのシステムが処理している情報の内の最も高い機密区分の情報に対して課せられたセキュリティ要件に合致するように保護される。そのシステムのすべてのユーザは，そのシステムが処理している情報の内の最も高い機密区分をクリアしているが，ユーザの内の何人かは，それらの情報の内のある情報に対する知る必要性は保持していない。

③ 統制モード（ Controlled ）

このモードでは，そのシステムのユーザの内の何人かは，そのシステムが処理している情報の内のある情報に対する機密区分もクリアしてないし，また知る必要性をも保持していないが，しかし（統制モードでは，）ユーザと重要文書とを隔離する制御機能は，オペレーティング・システムの必須機能というわけではない。

④ 多重レベル・モード（ Multilevel ）

このモードでは，そのシステムのユーザの内の何人かは，システムが処理している情報の内のある情報に対する機密区分をクリアしてないし，また知る必要性をも保持していないが，ユーザと重要文書との隔離はオペレーティング・システムおよび関連するシステム・ソフトウェアによって達成される。

侵入テスト（ Penetration test ）

侵入テストとは，コンピュータ・システムのセキュリティ制御を破ることができるかどうか，どのようにして破るかを試験することである。特定のコンピュータ・システムに対して徹底的に侵入テストを行って，破ることに成功しなかったことはない。侵入テストの結果はほとんど公表されていないが，仮想マシンである VM / 370 （ CP / 67 ）システムに対する SDC （ System Development Corporation ） のテストでは，このシステムは他のシステムに比べてセキュリティを破るのがより困難であると結論付けている。

プロトコル（ Protocol ）

プロトコルとは，ネットワーク中の2つ以上のノードの間での通信手順のことである。プロトコルにおけるセキュリティに関する重大な問題点は，メッセージの制御フィールド（ルーティング情報，誤り訂正情報等が入っている）が通常，暗号化されないで伝送されるので，制御フィールドの情報の漏洩をどのようにして制限するかである。

参照モニタ（ Reference monitor ）

参照モニタとは，主体（ subject ）（ユーザあるいはプログラム）が対象（object，すなわち客体）（ファイル，装置，ユーザ，あるいはプログラム）を参照（ reference ）するたびに，仲介・検査し，そのアクセスがシステムのセキュリティ・ポリシーに照らして正当であるか否かを決定するコンピュータ・システムの構成要素のことである。そのような機構は参照のたびごとに必ず呼び出されるので，効率的に有効に機能するためには，充分に小さく，その正しさが保証でき，不正な変更がなされてないことが保障できなければならない。

リスク評価（ Risk assessment ）

リスク評価とは，特定の設置箇所でのシステムの資産や，システムの脆弱性（ vulnerability ）について，ある脅威がある確率で発生するものと予想して，そこから生ずると思われる損失を分析することである。リスク評価でのもっとも難しい問題は，データが漏洩したり，破壊された際の被害額を決定する点である。リスク評価は特定の設置箇所での諸条件を考慮するので，開発者が実施可能なもっとも一般的な評価は，システム全体の脆弱性の分析である。脆弱性分析は，利用可能なシステムの欠陥を明示するので，より有効である。

セキュリティ・カーネル（ Security kernel ）

セキュリティ・カーネルとは，参照モニタを実現するハードウェア及びソフトウェアからなる機構ことであるが，この用語は，セキュリティに関連するシステ

ム・ソフトウェアすべてを指すのにも慣用されている。実現された機構は，特定のセキュリティ規則集を励行するカーネルと呼ばれる唯一の構成要素から成るが，高信用プロセス群（ trusted processes ）から成る構成要素郡も含まれているのが普通である。高信用プロセス群はセキュリティ規則全体の制約を受けないが，セキュリティを危くすることがないことが保証（ trusted ）されている。規則を厳格に適用する必要のある業務システムでは，多分，高信用プロセス群をセキュリティ・カーネルの一部として取り込んでおり，その結果，その正当性を形式的に保証するためにカーネルをできるだけ小さく保つ必要があるのに，実際には肥大化し，検証が困難になってしまった。

多くのプロジェクトでセキュリティ・カーネルのアプローチの実用性を実証しようとして研究を行っている。このアプローチを採用したMitre Secure Unix，UCLA Data Secure Unix，KSOS，KVM / 370 等のシステムでは汎用のプログラミング機能を支援し，既存のオペレーティング・システム（例えばUnix ）をエミュレートしているので，ほとんど成功していないが，一方，SDC Communications Kernel （ System Development Corporation ），PPSN / SUE （ Pilot Packet Switched Network / Secure User Environment ），Sacdin （ Strategic Air Command Digtial Network ）等の通信処理装置のように小型の専用システムではかなり成功している。システムの性能がいくつかのシステムでは，重大な問題点となっている。前者のいくつかのシステムでは，高信用化されていない同種のシステムに比べて，その性能は１０～２０％程度しか提供できない。後者のシステムの場合には，十分な性能が実現されており，本番用のシステムとして使用可能である。

これらの問題では，実現のための基盤となる抽象機構として記述子機構（ descriptor ）ではなく，資格機構（ capability ）を選択したことと，プロセス毎に記述子リスト（ descriptor list ）でもってたくさんのセグメントを支援できず，実行空間を充分に提供できないようなハードウェアを採用したことが主要な原因となっている。KSOSの場合には，性能の問題は，Unixエミュレータを１回呼び出すと，セキュリティ・カーネルへの複数回の呼び出しが起り，カーネル・コー

ルのたびごとに実行環境の切換え（ context switch ）のオーバヘッドが発生しているという事実に起因している。性能を改善するために，Scomp（ Secure Communications Processor ）やKSOSでは，Unixエミュレータに代ってカーネルへの単一オペレーティング・システム・インタフェースを提供するように改造されたが，そのインタフェースはUnix との互換性のあるシステム・コール・インタフェースを保持するように定義されるであろう。

セキュリティ・モデル（ Security model ）

セキュリティ・モデルとは，システムを構築する際に厳守しなければならないセキュリティ規則を定義しているモデルのことである。セキュリティ・モデルは，特定の応用環境を反映したセキュリティ・ポリシーの要求を表現している。セキュリティ・モデルは，ユーザがシステムの動作を理解する際の，そして設計者がシステムを設計する際の拠所を提供する。セキュリティ・モデルは仕様書を検討する際の基準として使用されるので，形式的に記述され，システム・セキュリティを厳密に定義してなければならない。

Mitre Brassboard Kernel，Multics Security Enhancements, KSOS，Scomp，Guard（ ACCAT Guard のこと），MME（ Millitary Message Experiment Systems ），Autodin II（ DoD Automatic Digital Network ），KVM/370，そしてSacdin はすべてBell-LaPadula モデルに基づいて構築されている。UCLA カーネルは資格機構を導入し，カーネルの外側にあるポリシー管理モジュールで特定の Bell-LaPadula 規則を定義することを許している。MME やGuard のような応用業務システムでは，Bell - LaPadula モデルを励行するシステムを基盤にして構築されており，その制御下で情報の格下げ（ downgrade ）を行う高信用プロセスを導入している。最近では，例えばNRL SMMS（ Naval Research Laboratory / Secure Millitary Message Systems ），Message Flow Modulator，COS / NFE（ Communications Operating System / Network Front End ）のように特定の応用業務から導かれたセキュリティ・モデルに基づいてシステムを構築する傾向にある。

仕様化技法(Specification technique)

仕様化技法とは，システムの振舞いを記述する手法である。仕様書が数学的な分析が可能となるように構造化されている場合には，形式的仕様書と呼ばれる。いくつかのシステムの仕様の一部分は，形式的に記述されている。典型的な形式的仕様書では，相対的に抽象化され，最上位の仕様書(TLS : Top-level Specification)を段階的に詳細化(洗練化)し，第2段階の仕様書を作成する(必要があれば，さらに詳細化して第3段階の仕様書も作成される。以下同様。)階層構造的アプローチを採用している。プログラム・コードは最下位の仕様書に基づいて作成される。

最上位の形式的仕様書で規定されたセキュリティの諸性質(security properties)を検証する際に使用可能なシステム及びツールとして，現在，仕様記述言語 Special (SPECIfication and Assertion Language), InaJo, Gypsy, Affirm 等がある。プログラミング言語である Euclid, Ada, Pascal 等もまた仕様を記述するのに使用可能である。その証拠として，KSOS や Scomp では，これらのプログラミング言語を使用して，熟練したプログラマが形式的仕様書を作成し，自動ツールを使用してセキュリティ欠陥のいくつかを摘発している。しかし，ほんとうの理由(利点)は，システム開発者，レビアー，あるいは仕様書作成者自身でさえ，仕様記述言語を熟知していないので，プログラミング言語で記述した形式的仕様書ならば理解でき，人手でそれをレビューしてセキュリティの欠陥を見つけることができるという点にある。形式的仕様書を作成し，検証する際に使用可能な諸ツールはまだ未熟で，一層の改良が必要であり，まだ研究用のツールであり，ソフトウェア開発での生産性及び品質向上のエイドとはまだなっていない。

高信用(Trusted)

構成要素が，関連するセキュリティ・ポリシーを励行していると信頼できるならば，その構成要素は高信用であると言える。プロセスが特権を持っている場合でも乱用せず，セキュリティ・ポリシーに違反しない時には，そのプロセスは高

信用プロセスと呼ばれる。プログラムに対して，事実上，信用できる（ trust－worthy）ことを確信する手段がなければならない。DoDのCSEC （ Computer Security Evaluation Center ）の評価基準に従うと，" trusted computing base "とは，コンピュータ・システム中の保護機構の全統合体，すなわちハードウェア，ファームウェア，ソフトウェアの複合体を言い，この統合体によってセキュリティ・ポリシーの励行に責任を持っている。

検証技法（ Verification technique ）

検証技法とは，２つの仕様書が合致していることを決定する手法である。コンピュータ・セキュリティの分野では，システム仕様書があるセキュリティ・モデルに合致している，あるいは励行している，または，下位の仕様書がその上位の仕様書と等価，あるいは正しく詳細化されたものであることを検証したい。２つの仕様書がそれぞれ形式的に記述されている場合には，自動定理証明器のような数学的技法を形式的検証を行うのに使用できる。

検証技法は，仕様化技法と同じようにまだ未熟である。最上位の形式的仕様書に対するセキュリティの諸性質の検証は，現在の技術水準でもかろうじて実施可能ではあるが（例えば，Scomp，KSOSではこのレベルの検証が実施されている。），プログラミング言語で記述されたプログラム・コードをより上位の仕様書に合致しているかの検証は，利用可能なツールを活用しても非常に困難であり，通常は人間のかなりの介入を必要としている。検証の現在の技術水準がMessage Flow Modulatorプロジェクトを見るとよくわかる。

研究の進展にもかかわらず，現在の検証ツールはシステム開発での実際の使用とは遊離しているのが現状である。検証を行う波及効果は，検証過程では設計者及び構築者に対して自分が何をしたいかを厳密に考え，他の人がレビューするために良く構造化された，厳格な文書証跡を残すように課している点にある。

仕様書中のセキュリティの諸性質を検証する際に使用可能なシステムとしては，Boyer-Moore 定理証明器，Gypsy 定理証明器，Affirm定理証明器，Shostak 定理証明器，Stanford 大学の Pascal 検証系，Compion 社の Verus 等がある。

仮想マシン（ Virtual machine ）

仮想マシンでは，各ユーザに対してそれぞれ独立の別々のオペレーティング・システムの下で実行されるようなシミュレートされた仮想的なマシン環境を提供する。各々のユーザは自分専用の仮想マシンに隔離されている。仮想マシン間の通信は，１つの物理的なマシン上に複数個の仮想マシンをシミュレートする仮想マシン・モニタ（ VMM, Virtual Machine Monitor ）によって提供される。 KVM/370はこのアプローチに基づく高信用システムの典型的な例である。別の例として， Share-7がある。各々の仮想マシンは別々のセキュリティ・レベルで稼動可能であり，VMMの一部に別々の仮想マシンにいるユーザ同士の通信を制御する参照モニタの役割りを演じさせることも可能である。この仮想マシンでは，異なるセキュリティ・レベルを保持するユーザ各々を隔離するのを手助けするので，隔離が主要な要件の場合には，仮想マシンのアプローチは最良である。しかし，異なる仮想マシン間で情報をやり取りするのにかかわるオーバヘッドは，特に異なるセキュリティ・レベルにまたがる通信には，大量の通信を必要とするので，システム構築の際の重大な考慮事項となる。

仮想記憶（ Virtual memory ）

仮想記憶では，プログラムが発生した（論理）アドレスを物理アドレスに変換する。アドレス変換機構では，複数のユーザが主記憶に同時に常駐することを許し，相互に干渉し合わないようにしている。アドレス変換装置はすべてのメモリ・アクセスに介入するので，レジスタを操作するアクセスをも制御できるのならば，参照モニタの一部の機能の役割りを演ずることも可能である。新型の高信用システムを開発することを放棄した場合には，仮想記憶はコンピュータ・システムを構成する１つのツールである。しかし，PDP-11で採用した小規模の仮想記憶空間と，装置を仮想化するアプローチには，列挙された研究成果の中にはセキュリティの観点からみて困難な問題点がいくつか含まれている。

1.2.2 セキュア・ソフトウェアの開発方法論

(1) 概　　要

ソフトウェア開発での最大の関心事は，ソフトウェアの品質及び生産性の向上である。本項では，ソフトウェアの品質向上技術についてのみ言及する。

コンピュータ・システムのセキュリティはハードウェア，ファームウェア，そしてソフトウェアの3者の複合体で達成される。[*1] そしてコンピュータ・システムのセキュリティ確保には，言うまでもなく，単に技術的（technical）な対策（固有セキュリティ度[*2]（inherent security）の向上）だけでは不充分で，物理的安全対策（physical safeguard）及び運用管理（administration）が非常に重要であり，技術的に提供されるセキュリティ機能が正しく運用管理されなければ何の意味もなさない（使用セキュリティ度[*2]（use security）の向上に留意する必要がある）。すなわち，技術的な安全対策が充分に威力を発揮し続けるためには，それなりの運用管理面の体制と手続きを確立し，従来のＱＣ（Quality Control）活動と同様に地道に継続的にやっていくことが肝要である。例えば，ソフトウェアのこの面での管理は，ソフトウェア構成管理（Software Configuration Management）と呼ばれる。ソフトウェア構成管理では，ソフトウェアのみのバージョンや変更の管理だけでなく，関連するすべての文書と，当該ソフトウェアに使用したすべてのテスト・データ（以後の回帰テスト[*3]（regression test）に使用される）をも管理対象としている。

＊1 ： コンピュータ・セキュリティの中核を実現しているこの3者の複合体をD.D（米国防省）の"Trusted Computer System Evaluation Criteria"では，特に"Trusted Computing Base"と呼んでいる。

＊2 ： 固有セキュリティ度及び使用セキュリティ度は信頼性工学の用語からの造語である。信頼性工学の分野では，この点を考慮して，運用信頼度（operational reliability）を固有信頼度（inherent reliability）（設計，製作，試験等の過程を経て，アイテムに作り込まれる信頼度）と使用信頼度（use reliability）（運用環境，設備環境，保守環境等の諸条件で変わるアイテムの信頼度）の積と定義している。

＊3 ： 保守（修正）されたプログラムに対して以前実施したテストの全部あるいは一部を行うことにより，新しいエラー（ripple effect）が混入していないことを保証するために行うテストである。

ソフトウェアの固有セキュリティ度を向上させるため，即ち，ソフトウェア自体の品質を高めるため（ secure とか trusted という形容詞で表せられる），セキュア・オペレーティング・システム（ SOS ）の開発過程では，次の５つの段階に区分している。

① コンピュータ・セキュリティのモデル化

② 形式的仕様書の作成

③ 高位言語（HOL）によるコーディング

④ 検証及びテスト

⑤ 侵入テスト（ Penetration Test ）

ソフトウェアの品質は，企画・設計段階（①，②）で作り込まれ，製造・試験段階（③，④）で実現され，検査段階（⑤）で確認・評価（品質保証）されることになる。

以下，各開発段階の概要について述べる。特に重要な開発段階（④，⑤）については別項でやや詳細に検討する。

(2) セキュア・オペレーティング・システムの開発段階

① コンピュータ・セキュリティのモデル化

まず最初に，各企業や機関でのコンピュータ・システム（アプリケーション・システム）に要求されるセキュリティ・ポリシー（機能）を明確にする必要がある。それを基にセキュリティ要求機能を正確に反映した形式的（あるいは論理的）モデルを作成する。コンピュータ・セキュリティのモデル化に当っては，モデルをできるかぎり単純にする必要がある。即ち，セキュリティ・モデルは以後の開発段階でのすべての拠所（基準）となるのみならず，モデル自体の妥当性，完全性等が確認（あるいは証明）できなければならず，複雑なモデルでは充分な確認ができないからである。

米国では，軍の人手による文書の機密保持手続きに則した，コンピュータ上での実現に適したモデルとして，Mitre社で開発した Bell - LaPadula モデルが有名で，よく採用されている。

② 形式的仕様書の作成

セキュリティ・モデルとプログラム作成との間のギャップが非常に大きいので，その間を埋めるために形式的仕様が採用される。「形式的」とは，数学的に厳密な定義が与えられ，検証の基礎となり，機械的な取扱いが可能である，ことである。

最上位の形式的仕様書（TLS : Top-level Specification）には，SOSのすべての入出力特性（インタフェース）が記述される。TLSは，SOSの機能が適切であるか否かを判断するのに使用される。そしてTLSがセキュリティ・モデルを厳守していることを検証する必要がある。TLSがBell-LaPadulaモデルを厳守していることを検証するには，Mitre社で開発された情報フロー分析手法（基本用語参照）がよく使用されている。

TLSの正しいことが検証されると，仕様書が段階的に詳細化され（中間レベルの仕様書，即ち2LS：Second - level Specificationの作成），より抽象化のレベルの低い仕様書に書き換えられ，最後にコーディングが可能な最下位の仕様書に到達する。各レベルごとに，その仕様書が直上レベルの仕様書を正しく具体化したものであることが保証（レビュー，確認，検証等の手段により）されなければならない。

検証を困難にしている最大な要因の1つは，ソフトウェアが果たすべき機能を明確かつ厳密に記述すること，つまりプログラムの仕様を書くのがむずかしいからである。そのためには，形式性，厳密性，記述性，理解性等に富む仕様記述言語及び支援システムの開発が緊急の課題であるが，一方，一階述語論理等を使用できる人材を養成することも必要である。

いずれにしろ，高品質のソフトウェア製品を作成するには，この段階で品質を作り込むことが肝要である。

③ 高位言語によるコーディング

SOSの正当性を示す主要な手段は検証であり，検証に適したプログラミング言語と文体（スタイル）でプログラムがコーディングされなければならない。そして，抽象データ型などの概念を積極的に導入し，プログラムの品質を向上させる必要がある。

Gypsy（テキサス大学で開発），Euclid 等の検証可能な言語を採用する必要があるが，現在はまだ商用化の段階に達していないのが実状である。そして最近注目されている Ada あるいはそのサブセットが検証可能なプログラミング言語であるか否かを検討する必要があろう。

コーディングが完了すると，プログラムが最下位の仕様書と等価であることが示されなければならない。この段階がプログラム検証である。

今後は，高品質のソフトウェア製品の製造には，コーディングの際の人間の不注意の誤りを防止するためにも，当然自動化，あるいは既存の枯れた安定している（エージングされた）ソフトウェア部品の再利用をはかるべきである。

④ 検証及びテスト

プログラムの正しさをプログラムを試験的に実行して確認するテストは，最もよく採用されている。しかしテストはある意味で最も能率の悪い方法であることは確かである。プログラム中の各経路（path）の組合せ数はすぐに爆発し，従ってすべてのケースをつくすようなテスト・データを準備するのは不可能である。仮に準備できたとしても，テストには天文学的な時間を必要とし，実施不可能である。そのため，最近ではプログラム中のすべての文が少くとも1回はテスト中に実行させるようなテスト・ケースを生成するシステムが開発されている（この種のテスト・データでは，C_0 網羅度＊ は 100 %となるが，C_1網羅度＊はせいぜい 50 %程度である）。

しかしいずれにせよ，テスト・データによる網羅的なテストが事実上不可能であることを考えると，プログラムの正しさを，テストによらず確認することが，より本質的な解決策であることは明らかである。これを厳密かつ数学的に，形式的に行うのが検証である。

検証技術はまだ未熟なので，検証しやすさを前提にして，ソフトウェアの

＊：C_0 網羅度は最も簡単な網羅度で，すべての実行文の内どのくらいの割合の文が実行されたかの指標である。C_1網羅度は，C_0に比べ，より厳しい指標で，すべての分岐の内どの位の割合が実行されたかという指標である。

開発を行う必要がある。すなわち，要求仕様書を厳密に形式的に記述し，段階的に詳細化し，各段階毎に検証（あるいはレビュー）を行い，正しさを保証し，コーディングに当っては検証容易な言語及び文体でプログラムを書く必要がある。この様な配慮を行うことによって，始めて誤りの少ないプログラム（ソフトウェア）を実現することができ，ソフトウェアの品質向上に寄与することになる。

プログラムの検証はあくまでも品質を保証する手段であって，プログラム検証自体が目的ではない。1.2.3項で述べるように，プログラム検証には適用限界があり，そしてプログラム検証が困難だからといって，代替手段としてテストを採用するのではなく，両者を相互補完的に使用すべきである。

⑤ 侵入テスト

検証は，その仕様書と直上レベルの仕様書とが等価であることを証明しているにすぎない。最上位の仕様書あるいはセキュリティ・モデルが実社会でセキュアであることを証明しているわけではない。

侵入テストとは，システムの内部に精通した経験者が端末からシステムのセキュリティ破りを敢行して，セキュリティ機能の欠陥（hole）を探すことである。侵入テストによって指摘されたセキュリティ機能の欠陥は是正され，セキュリティがより強化されることになる。

以上，ＳＯＳの開発方法論について述べたが，米国における先進的かつ実用的なシステムでも以下のような技術を導入して，ソフトウェアの品質を向上させている。*

・IBM Federal Systems Division

実時間処理を含むアプリケーションの開発に，従来のIPT（Improved Programming Technologies），HIPO（Hierarchy plus Input - Process - Output）に代わり，段階的詳細化，形式的検証を導入している。

---

*：吉村，『要求仕様作成技術』，情報処理研修センター，RP833-03，昭和58年11月．

・IBM Yorktown 研究所

H. D. Mills らによってＯＳの設計に抽象データ型の概念を導入している。

・Honewell Information Systems 社

大型機のＯＳ設計に当って，Dijkstra の Guarded Command や抽象データ型の概念を導入している。

・NRL （ Naval Research Laboratory ）

Paras教授の指導のもとに，艦載機Ａ７Ｅ用のソフトウェアの開発にあたり，形式的仕様技術，プロセス同期技術，抽象データ型の概念等を導入している。

1.2.3 検証技術

(1) 検証とは

セキュア・オペレーティング・システムの開発でのセキュリティ及びインテグリティを保証する手段として検証が行われている。

検証（verification）とは，「検証対象の仕様書（あるいはプログラム）と一段上のレベルの仕様書が論理的に等価である」ことを確かめることである。つまり，検証は，形式的な直上位の仕様書があって始めて可能なのである。混同される用語に証明（proof）があるが，証明は数学のように無条件に正しいことを示す点にあり，検証とは本質的に異なっている。検証で正しいことが確認されたからと言って，絶対的な正しさが保証されたわけではない点に注意する必要がある。

(2) 検証技術の現状

今日までに開発されたセキュリティ・カーネルの大部分に対してある程度の形式的検証が試みられた。形式的検証に対する初期の公約のいくつかは，誇大であった。現在では，検証は予期された以上の困難な作業であることがわかってきた。

DoD（米国防省）の “Trusted Computer Evaluation Criteria ”では，Ａ基準として保護機構の検証（Verified Protection）を要求し，すなわち細分基準のA-1では設計仕様書の検証（Verified Design）を，A-2ではプログラ

ムの検証（Verified Implementation）を要求している。（詳細は，1.3.8項を参照されたい。）

セキュリティ・カーネルの開発では，最上位の形式的仕様書（formal specification）（通常，要求仕様書あるいはユーザ・インタフェース仕様書に相当する文書）がBell -LaPadulaのセキュリティ・モデルに準拠しているかを自動的に検証する手法は現在発展途上であり，決まり決った手順にはほど遠いのが現状である。（このレベルの検証には，Mitre社で開発され情報フロー分析手法がよく使用されている。詳細は基本用語の項を参照されたい。）開発者は，そのような検証によって何が論証されるかを理解しなければならない。検証では，主として，2つの形式的な文，すなわち，1つはシステム・セキュリティ・モデルの文，もう1つはシステム設計書の文との間での合致を確認する。Bell -LaPadula モデルに基づくすべてのアプリケーションでは，ある種の高信用主体群（trusted subjects）が必要であり，その高信用主体群に対して検証を要求しているが，高信用プロセスが励行すべきセキュリティの諸性質を形式的に記述するのが困難である。結論を言うと，システムがBell -LaPadulaモデルの公理を励行していることを保証するために形式的検証を高信用主体群に適用することはできない。高信用主体群がシステム・セキュリティを維持していることを保証するには，高信用主体用の別の分離されたモデルと仕様書とが合致しているかの検証か，あるいは信頼できる人によるレビューを必要とする。

自動ツール（例えば，JnaJo，Gypsy）を高信用主体群の検証とか，Bell-LaPadula モデル以外のセキュリティ・モデルに基づくシステムに適用して，成果をあげている。しかし，選択されたセキュリティ・モデルがユーザのセキュリティ・ポリシーに対する直観的な観念に一致しているかを論証するのは困難な作業である。

大量のソース・コードに対してセキュリティの諸性質に準拠しているかを自動的に検証するのは，現在の技術レベルを越えている。今日までに検証されたプログラム・コードの最も大きなものの1つは，Gypsy言語（Pascal言語の一派）で記述されたもので，1,000行（非実行文も含む）以下である。これらの

検証法は将来発展する見込みがあるが，しかし，来週にシステム開発を開始するプロジェクトに，検証法を導入するのはかなり危険である。仕様書あるいはプログラム・コードの小さな部分に対して特定の性質に合致しているかを検証するのは人手でも可能ではあるが，それらが適切な言語で記述されていれば機械の支援が利用できるであろう。

検証に対する現状での技術成熟度の悲観的な評価にもかかわらず，形式的な方法論を採用する利点がいくつかある。形式的検証では形式的設計仕様書を必要とし，この仕様書を作成するには，設計者に対して問題を注意深く，厳密に考えることを要求する。こうすることにより，設計の欠陥をインプリメンテーションの前により発見されやすくなる。2･3のセキュリティ欠陥が形式的検証過程で発見されるけれど，形式的仕様書中のかなり多くのセキュリティ欠陥は，設計者が事前に気が付いて訂正されているのが普通である。最後に，設計者は形式的仕様書を読んで更新する能力を備えていなければならない。

システムに対する注意深い設計および作成の必須のパートナーとして充分なテストも必要であり続ける。テスト計画が作成された時には，システムのセキュリティの諸性質をテストするように特別な注意が必要である。もし可能ならば，開発者は侵入テストを計画し，削除することのできない漏洩通路（leakage channel）の帯域幅を評価すべきである。

(3) プログラム検証の限界

最近の文献では，プログラム検証の可能性に対して疑問を呈している。事実，検証はソフトウェア開発の現場では広く受け入れられていないばかりでなく，セキュリティ・カーネルのような複雑なソフトウェアに対して完全には適用されていない。今日までの最も野心的なプロジェクトはUCLAセキュリティ・カーネルでの限定された部分に対する検証である。プログラム検証には潜在的な弱点があり，プログラム検証は絶対的な正当性基準ではなく，代替手段としてのテスティングはシステム開発での重要な役割りを演じつづけるであろう。

プログラム検証がソフトウェア開発で重要な役割りを演じられない点を次に列挙する。

① プログラム検証は数学の証明のように社会的な過程を受けることがない。すなわち，数学の世界では，発表された証明は，別のある一部の数学者が興味を示し，証明過程をチェックするが，プログラム検証の場合には，このようなことを期待することができない。

② 検証の誤りを通常，形式的記号論理では訂正することができない。数学の場合には，別の数学者によって時間をかけてその証明過程が精査され，やがて数学の共同体の中でその証明が正しいらしいとして受け入れられて行く。

③ プログラムの検証は，複雑な記号論理の長い列で行われるので，他の誰もその検証過程を読んでくれないし，まして綿密に調べてくれないであろう。

④ プログラム検証は，検証されたプログラムに対して“Titanic*”効果をもたらすであろう。すなわち，検証済のソフトウェアは，故障に対して適切な予防策がとられていなくても，とられているように信じられてしまう。

以上の弱点を克服するには，プログラム検証は数学の証明と同じように社会的過程を受ける必要がある。検証法と，（セキュリティのBell - LaPadulaモデルのようなプログラムの正当性基準を記述している）モデルは，検証学の共同体の中で綿密に調べられなければならない。

いずれにしろ，検証は高品質ソフトウェアを保証する有力手段であることはまちがいないが，万能ではないので，従来のテスト技法を代替手段とみなすのではなく，より完全性をきすため両者を相互補完的に使用すべきである。

〔参考文献〕

・検証関係のみ

1) Ames, S.R. Jr., “Security Kernels : A Solution or Problem ?,” Proc. 1981 Symp. Security and Privacy, pp. 141 - 150, (Apr.1981).

---

*：当時の英国の最大の豪華客船で，絶対に沈まないと信じられていたが，1912年，処女航海で氷山に衝突・沈没した。

2) Cheheyl, M.H., Gasser, M., Huff, G.A., and Millen, J.K., "Verifying Security," ACM Computing Surveys, Vol. 13, No. 3, pp. 279 - 340, (Sept. 1981).

3) Adrion, W.R., Branstad, M.A., and Cherniavsky, J.C., "Validation, Verification, and Testing of Computer Software," ACM Computing Surveys, Vol. 14, No. 2, pp. 159 - 192, (June 1982). (邦訳:「ソフトウェアの検証とテスト」, 日経コンピュータ, No. 52, (1983.9.12), No. 53, (1983.10.3).)

4) Ames, S.R. Jr., Gasser, M., and Schell, R.R., "Security Kernel Design and Implementation: An Introduction," IEEE Computer, Vol. 16, No. 7, pp. 14 - 22, (July 1983).

5) Landwehr, C.E., "The Best Available Technologies for Computer Security," IEEE Computer, Vol. 16, No. 7, pp. 86 - 100, (July 1983).

6) 鳥居, 二木, 真野,「プログラミング方法論の展望」, 情報処理, Vol. 20, No. 1, pp. 22 - 43, (Jan. 1979).

1.2.4 侵入テスト

侵入テスト(Penetration Test)とは, ユーザが端末機を通してコンピュータ・システムのセキュリティ機構を破ることができるか, またどのようにして破れるかをテストすることである。"検証"が主として仕様書を対象とした机上における論理的なセキュリティ機能の論証であるのに対し, 侵入テストは対象となるコンピュータ・システムが実社会において実際的にセキュアであることを実証するものである。侵入テストはまた, オペレーティング・システム(OS)の設計上の欠陥を発見するための有力な一手段であり, より完全なデータ保護を可能にするコンピュータ・システムを構築する上で, 欠くことのできないものである。事実, 数多くのコンピュータ・システムに対し, 侵入テストが繰り返し行なわれてきているが, そのテスト結果は極く一部の例外(例えば, 1976年に行なわれ

たＶＭ／３７０システムに対するＳＤＣ（ System Development Corporation ）による侵入テスト等）を除き，セキュリティ対策上ほとんど公表されていない。そこで，本項においては一般的な侵入テストのやり方について概説する。

(1) 侵入テストの一般的実施要領

a．テスト・チームの編成

テスト・チームは対象とするコンピュータ・システムの設計や構築には参加しなかったＯＳのスペシャリスト数名で編成される。彼等は当該システムのユーザ群の一員であり，セキュリティ上最も低いランクに位置付けられるものとして扱われる。すなわち，テスト・チームによって発見されたシステムの欠陥は全てのユーザが発見し，そこからシステムに侵入できる可能性を保持させるためである。チームに与えられる侵入テスト用のツールは，システムに接続されている端末機とＯＳの全ての仕様書（プログラム・リストを含む）だけである。

b．侵入の目標

侵入テストの目的は，対象システムのセキュリティ機能が本当に完全かどうかを調べることであるが，その目標とするところは次のとおりである。

① 他のユーザのパスワードやデータのように，自分には取り扱う資格のない情報を入手する。

② 他のユーザへのサービスが不可能または不十分になるように，リソースの多くを占有する。

③ アカウントされることなく，システム内のリソースを使用する。

c．テストの要領

ＯＳは，それ自体が膨大で複雑なソフトウェアであるため，設計ミスやプログラム・ミスによる欠陥が必ず存在する。更にユーザの要望や欠陥の是正のためにひんぱんに修正の手が加えられており，新たな欠陥やロジックの矛盾が発生している可能性が強い。テスト・チームはこのようなセキュリティ上の穴を見つけ出し，ここからシステムに侵入する。このセキュリティ上の穴を見つけるのに，一般的には次のような手順を用いることが多い。

① セキュリティ構造のモデル化

システムへの侵入の可能性を探る上で先ず最初に理解しなければならないことは，ユーザはそのシステムにどのように係りあっているか，ユーザはシステムからどのようなサービスを受けられるのか，ユーザはどのような制限を受けるのか，ということである。更に制御機能（すなわちシステムへのアクセスやリソースの提供を制御する機能）を確認し，制御機能間の相互関連と，それらがどのように利用されるかについて十分に理解する。

② 仮定欠陥の摘出と検討

システムのセキュリティ構造を十分に理解したならば，制御機能が設計者の意図しない方法で変更されたり無効にされたりするような，セキュリティ上の弱点となる可能性のありそうな機能や部分＝仮定欠陥を摘出する。一般的に，セキュリティの弱点が最も現出し易い機能等を次に示す。

- リソース・シェアリング機構
- ＯＳにより管理されているマン・マシン・インタフェース
- ソフトウェア構成管理の制御機能
- 本人（ユーザ）確認の制御機能
- 追加，設計変更，設計拡張された部分
- パラメータ・チェック機能
- セキュリティに関する記述の統制部分
- エラー処理機能
- 副次的機能
- 並列処理機能
- マイクロプログラミング支援ツールへのアクセス機能
- 複雑なインタフェース機能
- 機能の重複している部分
- 制限及び禁止機能
- 設計原則への違背部分

こうして摘出された仮定欠陥に，真に欠陥が存在する確率を見積り，次に

その欠陥が利用されることからくる潜在的なセキュリティ上の弱点について予測する，そして真に欠陥として認められる確率が高く，更に加えて侵入をもたらす確率も高いものに対し，以降の手順を進める。

③ 欠陥の立証と侵入

検討の結果，選別された仮定欠陥は，それが真の欠陥であるか否か詳細に審査する。まず第1段階として，ツールとして与えられた仕様書を基に徹底的な机上テストを行い，欠陥を立証する。机上テストで立証できなかった仮定欠陥については，実働中のシステムにおけるテストを実施し，その欠陥を実証する。

これらの方法によって立証された欠陥は，それらの欠陥をうまく組み合わせればシステムに侵入できることを論理的に論証するだけの場合と，実際に実働中のシステムに侵入してみせる場合とがあるが，後者の場合には更に多大の労力を要することが多い。

なお，これら一連の詳細なテストの結果，当初予期していなかった他の重大な欠陥の発見につながることも多い。

④ 欠陥の一般化

立証された欠陥について，さらにそれらがより一般的な欠陥に汎化できるか否かを分析する。欠陥を一般化することによって同種の気付かなかった欠陥を発見する手掛かりとすることができるとともに，一般的なセキュリティ上の弱点に対して効果的なシステムを設計することが可能となる。

更に一つのシステムにおける欠陥を一般化することにより，他システムに対する侵入テストの手掛かりとすることができる。

(2) 侵入テストの実際

前述のごとく，実際に行なわれた侵入テストの結果はほとんど公表されることがないが，極く例外的に公表された例について述べる。

a．米国防省における侵入テスト

米国の国防省において空軍のタイガー・チームが中心となり，1960年代後半から1970年代前半にかけて当時の全ての商用オペレーション・システ

ムに対する侵入テストを実施した結果，一つ残らず侵入に成功したことが知られている。

b. ＶＭ／３７０に対する侵入テスト

１９７６年，ＳＤＣによって行なわれたＶＭ／３７０に対する侵入テストの結果は，次のように報告されている。

- 摘出された仮定欠陥　　— ８８０件
- 詳細審査された仮定欠陥 — ７６件
- 立証された欠陥　　— ３５件
- 実際に侵入したもの　　— １９件
- 副次的に発見された欠陥 — ２件

これらの欠陥のほとんどは入出力機構で発見されたものである。また，設計を適切に簡潔に行うことが侵入しようとする企てに対する最も強力な防護の根源であると結論付けられている。

1.3 ＳＯＳの事例

1.3.1 概　　要

ＳＯＳの開発は１０年以上にわたり，軍用の保安規準に適合するコンピュータ・ソフトウェア・システムの構築を目指して行なわれてきた。しかし，ここで蓄積されたノウハウは今後来るべき高度情報化社会において主役となるコンピュータのネットワーク利用のための基礎的技術を与えるものでもある。本節では次節以下に取り上げる各種ＳＯＳの概要を述べる。

Miltics Security Enhancements は米空軍がBell - LaPadula モデルをMultics に適用したものである。本来のMultics のリング保護機能をセキュリティに利用し，外部リングよりも内部リングに特権を持たせている。さらに，ユーザのファイル（セグメント）に対するアクセス制御リストもMultics の機能を用いている。アーキテクチャは２状態（スーパバイザとユーザ）マシンをｎ状態マシンに一般化し，１状態が１リングに対応させている。現在の Honeywell 社のDPS 8/70Mはｎ＝８をサポートしている。Multics はセキュリティの検証やモデルを考慮せずに開発されたものだが，その高度な保護アーキテクチャと多層設計は十分ＳＯＳとして使用できると考えられる。

このシステムは米国防省内の空軍データ・サービス・センタに１９７４年に設置され，１９７６年１２月から２レベルで運用を行なっている。システム中には最高機密（Top Secret）分類の情報の一部が格納され，機密（Secret）レベルの審査に適合した一部ユーザをサポートしている。これはＡＩＭ（アクセス分離機構）と呼ばれ，購入者の希望により標準Multics に修正を加えたものである。現在のところ利用者は軍関係に限られている。

Honeywell 社とMitre 社はＡＩＭの開発に続きMultics ＯＳ を改造してセキュリティ・カーネルを作成する予定である。さらにＭＩＴでの研究ではMultics のリング０中の命令コード（プログラム）をかなり減せることも判明している。しかし，予算削減のあおりで，今のところセキュリティ・カーネルは作られていない。

UCLA Data Secure Unix はPDP－11 用のプロトタイプのセキュリティ・カーネルである。PDP－11 の機能を損なわないという配慮からUnix ユーザ用のインターフェースが設けられているが，処理速度が著しく低下してしまった。カーネルをできるだけ小型にしようとしたため，カーネル外にかなりのセキュリティ関係の機能を持たせている。たとえば，Bell－LaPadula モデルを実行させるためのポリシー・マネジャ・モジュールはカーネル外となっている。したがって，他のカーネルと単純に大きさを比較することはできない。

ISI，Xivus セオレム・プルーバにより形式的検証を行なう努力がなされている。高レベルの仕様に対する検証がかなり困難な障害となっているが，カーネルについては４０％までは検証が終っている。

KVM／370 はIBM社のVM／370 用にSDC社が作ったシステムである。現在までにIBM 4331，IBM 4341，Amdahl V7／A 上でデモンストレーションが行なわれている。今のところ当初の標準ＶＭに対する性能低下予測½を下回る¼程度となっている。

ＫＶＭは現在のところ大型ＴＳＳを取り扱える唯一のものであるが，これについては単に小型システムを大型マシン上で走らせているだけに過ぎないという批判もある。設計では複数の仮想マシンが異なるセキュリティ・レベルで，共有ミニディスクにより制約された通信を行なうようにしてある。現在のＫＶＭはサポートできる周辺機器の台数に制限があり，システム・ディレクトリや基本ハードウェア構成を変更するにはシステム・ジェネレーションが必要になってしまう。監査者およびセキュリティ担当者に対するサポートはない。Mitre社で実運用されているが，デモンストレーション用以上にするにはさらに開発努力が必要である。

KSOSはKSOS－11とも呼ばれている。PDP－11／70 上で動作するカーネルに基づく商用のプロトタイプである。カーネル上にはエミュレータを設けユーザ用のUnix インターフェースとしている。カーネルの最上位の仕様はSpecial により記述されており，仕様に対するプログラム・コード（Modula ）の完全な検証を目指していたが，FACC （Ford Aerospace and Communicatins Corp.）の契約は１９８０年１２月に切れている。

Unix エミュレータとユーザ・ソフトウェアのレーヤの性能はよくないが，カーネルの最上位の仕様レベルでの情報フローの諸性質の検証には成功している。プログラム・コードの検証は人手で行っている。カーネル自体は十分応用性があるが，エミュレータにカーネルの一部を二重に持っていることが性能低下の原因となっている。

米海軍ではLogicon社にFACCのものをカーネルの小型化とエミュレータに代るカーネル・インタフェース・パッケージの作成により性能改善するよう命じている。

Scompは Secure Communications Processorの略称でKSOS-6とも呼ぶ。これにはHoneywell社の Level 6 のハードウェアを用いている。米政府の要求により，SPM（セキュリティ保護モジュール）というハードウェアの製作と カーネル・ソフトウェアの仕様とその展開が行なわれた。SPMはCPUの介入なしにバス上でのデータの高速伝送を可能にし，さらに仮想記憶能力を向上させ標準の Level 6 をしのぐものになっている。カーネルとハードウェアは完成しており，ハードウェアに対するカーネル動作の検査が行なわれている。

初めはKSOS－11と同じくUnixエミュレータを入れる予定であったが， 最少のScompインターフェースSKIP のみが設けられることとなった。Unix のシステム・コールをSKIPのコールへ変換するパッケージの製作が現在行なわれている。カーネルは Speial 言語で記述されており，検証は SRI のツールにより行なわれている。最終的な最上位の仕様の検証はほとんど終ってはいるが，SRIツールでは大きすぎるモジュールが残ってしまっている。国防省のCSEC（Conputer Security Evaluation Center）で，この部分について新たな検証が行なわれ成功している。カーネルはUCLA Pascal により記述され，Pascal-to－C コンパイラでコンパイルされた。トラステッド・プロセス部はGypsy言語によって記述されているが，契約範囲にはこの部分の検証は含まれていない。

Scompのハードウェアとソフトウェアは，Los Alamos，Mitre 社，GE社 などに引き渡されている。SPMを32ビットのDPS－6／94に導入する方向が今後有望となっている。

PSOS（Provable Secure Operating System）はSRIで1970 年代後半に

書かれた仕様である。このドクメントは1980年始めに締結されたFACC, Honeywell両社に対する2フェーズの契約に用いられた。

最終目標は中，大型汎用コンピュータ・システムで，仕様に対する適合性を形式的に検証できるものである。第1フェーズはケーパビリティ・ベースのアドレシングとタグ付きのアーキテクチャを用いたＳＯＳの設計である。第2フェーズはその開発である。プログラム・コードの検証がなされたかどうかは不明である。Honeywell 社はSPMを持つ次世代のLevel 6型の32ビット・ミニコンピュータを提案して入札を行なった。この契約は1981年に終ったが，同社は1982年に新たな契約により関連するハードウェアの設計を行なっている。

以上のＳＯＳを合せ，完了，未完了のＳＯＳのプロジェクトはわかっているだけでも２６個存在している。しかし，上記のものを除いてはその詳細が不明なものが多い。次節では各ＳＯＳの内容，その特徴について紹介する。

1.3.2 Multics Security Enhancements

(1) 目　　的

ＴＳＳの汎用オペレーティング・システム（ＯＳ）として厳重な保護策が施されているMulticsは1964年からベル研究所，ハネウェル社（当時はＧＥ），ＭＩＴの3者による共同研究により開発された。６９年に一般利用者用としてＭＩＴで使われるようになった。このＯＳの保護システム部分のプログラムは命令の数にして150,000ライン，カーネルの部分だけでも54,000ラインにものぼる膨大なものであった。

７０年代の初期，スポンサーが米国空軍とハネウェル社で，ハネウェル社とMitre社の共同開発で"よりセキュアなMultics"開発に挑んだ。そのプロジェクトに対してはMulticsに強固な機密保護機能と機能の保全性を持たせることに加えて保全性監査者が理解できるようにスーパーバイザを簡単にすること，理解しやすい形式的モデルによってあらわせるセキュリティ機能を提供することであった。

(2) どんな形式的なセキュリティ・モデルを採用しているか。

Multics に Bell - LaPadula モデルを適用した。

Multics 中の対象に秘密区分（ classification ）を与え，このモデルの規則を励行するための検査機構が組み込まれた。

Bell - LaPadula モデルは次の２つの公理に集約できる。

① 使用者は自分に認可されている使用許可レベルより上にある秘密区分レベルを持つ情報を読むことはできない。

（ " No read-up " ：上は読めない）

② 使用者は情報の秘密区分レベルを下げることができない。

（ "No write-down " ：下に書けない）

(3) セキュリティ・カーネルの構成要素は何か。

Multicsには８つのリング（ ０～７ ）が用意されている。プログラムの実行の際，より低位のリング番号により多くの特権が与えられる。ユーザが新しいファイル（ セグメント ）のアクセスを要求する時，要求が認められるか否かはＡＣＬ（ Access Control List ）とＡＩＭ（ Access Isolation Mechanism ），およびリング階層で決定される。ACL，AIMそしてリング・メカニズムの関係を述べると各メカニズムはアクセスを一応定義しているが，実際のアクセスは３つのメカニズムの連携によって行われる。ユーザが要求したアクセスがＡＣＬやＡＩＭにより許可された場合ファイルをアクセスできる。そして，そのプロセスは適切なリング階層内のあるリングで実行される。

(4) ＳＯＳはどんな階層構造となっているか。

ファイルを何段階にも分けて保護のレベルを作っておく「リング構造」になっている。リング構造では，内側（より小さい値）のリングは外側のリングよりも多くの特権を保持している。あるレベルから外側のレベルへ向けてのファイルのアクセスは許されるが，内側へ向けての参照は，「ゲート」と呼ぶ関門を通してしか許されない。ゲートは内向き呼出しが正当なものかどうか判断して権限のない呼出しは拒絶し，不正なアクセスがあったことを報告する。このようにＡＣＬを使用してファイルへのユーザ・アクセスを規制しており，他人が勝手にアクセスできないようになっている。又，リングの一番内側にあるＯ

Sの核は厳重に保護されている。

(5) どの程度まで検証が行なわれたか。

検証に関しては元々のMulticsの開発で考慮されておらず，行われなかった。

(6) 侵入テストが行われたか。

1970年代の初期に米国防省にタイガー・チームが創設され，種々のコンピュータ・システムを研究し，これらの安全性を評価することが行なわれた。タイガー・チームは困難な末，Multicsに入り込むことができた。この時，タイガー・チームはMulticsのハードウェア上の設計エラーを発見した。システムの他の要素が安全でなければ，最高のソフトウェアをもってしても不十分であることが浮きぼりにされた。一方，Multicsのデータのセキュリティ・メカニズムが優れたものであるかが判明された。

OSのセキュリティ・メカニズムはいかにそれが精巧につくられていたとしても，それを形成しサポートするソフトウェアとハードウェアの品質レベルと同一レベルでしかない。この両者の結合によってOSのセキュリティ・メカニズムを守ることが可能である。

(7) そのSOSの問題点は何か。

① 数多くの複雑なプログラムで構成されている。複雑化されたシステムでは，その変更ごとに正当性を検証することは困難である反面，セキュリティ・メカニズムは変更の頻度と範囲が拡大するのに応じて，その機能が拡大する。

② SOSを考慮する上でOSそのものが大きくなりすぎ，OSによるプロセッサの使用時間がそれ自身で増えてしまい効率が悪くなってしまう。

③ SOSはもともと軍の要請によるものであるが，最近は民間への普及も望まれている。コスト面も含め，民間の浸透はまだ先の事となろう。今後の動向としては，SOSの効率を向上させるために，ハードウェア・アーキテクチュアをSOSの基本思想に含め，改善することが必要である。

(8) プログラムの大きさ，実用性，評価，性能等について

① プログラムの大きさ

初期の時点でカーネルの部分は54,000ラインであった。

リング・ゼロ　　44,000ライン

応答サービス　　10,000ライン

（システムのログ，パスワード，システムの課金管理）

1974年～1977年にかけて，各プロジェクトがカーネルの大きさを減らす研究を行い，カーネルの大きさが半分くらいの26,000ラインの大きさのプログラムになった。減少できた要因は，システムのアルゴリズムを簡単にしたからであった。

② 実用性

このシステムは1974年にPentagonにあるAFDSC（Air Force Data Services Center）に導入され，1976年12月以降，2レベル・モード（Controlledモード）で，即ち，システムがTop-Secretの秘密区分を持つある情報を蓄積し，かつSecret の秘密区分を持つ何人かのユーザを支援しているモードで稼動できることが保証されている。Multics自身はその後の改良も含め，現在もハネウェル社の標準提供ＯＳの1つとしてユーザに提供されている。

③ 性能・評価について

ＳＯＳの歴史はMulticsから始まっている。このデータ・セキュリティ体系は，ＯＳの核に強固なセキュリティ機能（アクセス・コントロール機能）を持たせており，優れた制御機能によって複数ユーザによる共用を可能にしたばかりでなく，信頼性のある大規模汎用ＯＳとして評価されている。

Multicsは，以降に発表されたＳＯＳの基本になったものの，ＯＳが大きくなり過ぎ，パフォーマンスが悪く開発が困難になり，国防省からの予算が打ち切られたのでMulticsセキュリティ・カーネルは作成されなかった。一方，ベル研究所はMulticsの巨大ＯＳに対する反省から，Multics の持つ設計思想を盛り込んだコンパクトで小まわりの効くＯＳの開発に着手し完成したのが，現在使われている“Unix”の基本である。

1.3.3 UCLA Data Secure Unix

(1) 目　　的

ＳＯＳの基本的な機能を，「種々のユーザが保有する情報資源を，権限を持たないアクセスから保護する」ことであると定義する。従来のＯＳが機密保護を実現する方法では，制御の裏をかくユーザの侵略経路を防御するため，コードの改良で対処してきた。しかし，パッチによる方法はそれ自身に誤りを含んでおり，基本的に限界がある。このような受動的なアプローチから前進して，より構成的な手法でＯＳの機密制御の正当性を示す必要が提唱されている。

UCLA Data Secure Unixは，検証可能なデータ保全システムを中規模の汎用コンピュータ・システムで実現することを目的に開発されたもので，開発に際しては，次のような設計原則を設けている。

① 基本カーネル，第二次ポリシー・カーネルの設定

② 既存ＯＳとのインターフェイス

③ 高レベル言語（ Pascal ）での開発

④ カーネルのソース・コードに対し，形式的，自動的プログラム検証手法を適用

実現されたシステムは，基本的にはUnix とのインターフェイスを持ち，DEC PDP-11/45SとPDP-11/70Sで稼動する。

(2) 形式的セキュリティ・モデル

セキュリティの保護とは，保護されるべき対象が権限を持たないアクセスから守られることである。当モデルでは証明されるべき命題として次の3つのセキュリティ命題を掲げている。

Ｓ１：保護対象（ object ）は明示的な要求によってのみ更新できる。

Ｓ２：保護対象は明示的な要求によってのみ参照できる。

Ｓ３：保護対象への特定のアクセスは，記録された保護データが許可する時のみ可能である。

形式的モデルはＳＯＳを有限状態の抽象機械Ｍとして構成し，状態（ state ），

命令集合および状態遷移関数で記述される。

$$M = <S, S〔0〕, I, T>$$

ここで，S：状態の集合

S〔0〕：初期状態

I：命令集合

T：$I \times S \rightarrow S$　状態遷移関数

命令集合IはOSカーネルの呼び出しや，ハードウェア命令等を含む。各状態遷移は単一ステップで完結するものである。状態は，対象，I/O待ちリスト，カレント・プロセスの3つ組で記述される。対象（object）は保護されるべき情報の単位で，それぞれにユニークな識別名，タイプ，アドレスおよび値を持つ。

対象のタイプには次のものがある。

- プロセス …… 実行主体
- セグメント …… 均一の単位に分割された情報の塊（ページ）
- 保護データ …… セキュリティ・ポリシーを記録している対象で，SOSが制御すべき行動を規定し，値として特権（capability）リストを持つ。特権リスト（C－リスト）はどのプロセスが，どの対象をどのアクセス・タイプでアクセスできるかを記録している。

アクセス関係はRef（参照）とMod（更新）がある。Mod関係とは，状態sの時，命令iを実行した場合，特定の対象nが更新される可能性があることを示し，Ref関係とは，状態sの時，命令iを実行した場合，特定の対象nが参照される可能性があることを示す。

セキュリティの定義は，要約すると次のようになる。

「どんな命令も，Mod関係もしくはRef関係でアクセスの可能性を定義されていなければ，当該対象を実際に更新もしくは参照することはできない。」

このことは，どんな命令も規定された以外の副作用を持たず，実際に更新・参照ができる対象とは，実行主体がアクセスを許されているものに限ることを意味しており，具体的にはアクセス許可が保護データとして記録されている

（Ｃ－リスト）。

このようなセキュリティの定義は抽象機械の概念のみで完結しており，具現化（ implementation ）レベルの仮定が何ら含まれていない点が特徴である。

前述のアクセス関係は，アクセスの可能性を定義するもので，潜在アクセス関係と呼ぶ。すなわち，抽象機械の仕様記述の一部を構成するもので，各々の命令の意図的な行動を記述している。ここでRef関係，Mod関係は次のような論理関数である。

Ref ：Ｓ×Ｉ×対象名 → ｛真，偽｝

Mod ：Ｓ×Ｉ×対象名 → ｛真，偽｝

すなわち，ある状態ｓの時，命令ｉの引数リストに対象名ｎが含まれている場合，関数値は真をとる。

潜在アクセス関係とは別に，対象に対し，実際に参照・更新を実行したかを定義する関係がある。これをアクセス実行関係と呼び，状態遷移に関連する。アクセス実行関係には更新実行関係と参照実行関係とがある。

以上のモデル構成の中で，最初に掲げたセキュリティ命題は，次のように規定される。

Ｓ１：更新セキュリティ

状態ｓ′で命令ｉを実行した時，実行後の状態ｓですべての対象が不変であるか，変化した対象がすべてMod関係で定義されている場合，更新セキュリティが満されている。

Ｓ２：参照セキュリティ

状態ｓ′で命令ｉを実行した時，実行後の状態ｓですべての対象が参照されていない（ NoRef ）か，参照された対象がすべてRef関係で定義されている場合，参照セキュリティが満されている。

Ｓ３：特権許可

状態ｓ′で命令ｉを実行した時，Mod関係で定義されている対象があるならば，必ず“write”モードで保護データとして許可が与えられているか，もしくは命令ｉ実行後の状態ｓでその対象が不変で

ある。又，Ref関係で定義されている対象があるならば，必ず“read”モードで保護データとして許可が与えられているか，もしくは命令i実行後の状態sでその対象が参照されていなかった（NoRef）かである。

このようなモデル構成の目的は，セキュリティに関して簡潔・明確で精密な記述をすることであり，現実のハードウェア上でこのモデルを具現化する時には，抽象レベルでの仮定を何ら乱すことなく，実現することができる。

(3) カーネル

カーネル命令は状態遷移関数として考えられ，抽象データ型の実現として見ることができる。すなわち，各データ型上の妥当な操作が定義されているのである。UCLA Data Secure Unix のカーネルは，以下の12個の基本操作で構成されている。

① GRANT …… 特権（capability）を追加
② INITIALIZE PROCESS …… プロセスの初期化
③ ZERO SEGMENT …… セグメントの初期化
④ INVOKE …… プロセスの抑止，他プロセスの起動
⑤ SWAP …… 2次記憶と主記憶間でセグメント・コピーの転送
⑥ REFLECT …… 主記憶の内容にマッチするように2次記憶を更新
⑦ NOTIFY …… 他のプロセスを認識する為の割込み機能（ソフトウェア）
⑧ RECEIVE …… あるプロセス空間から要求されたプロセス空間へメッセージの内容を移す

＊プロセス間通信（Sending process → NOTIFY,
Recipient process → RECEIVE）

⑨ STARTIO …… I/Oの開始，I/O待ちリストにエントリー
⑩ MAP …… 仮想アドレスの制御
⑪ INTERRUPT …… I/O終了等，割込み機能（ハードウェア）

⑫ EXECUTE …… セキュリティに関連しないハードウェア・サポート命令実行

(4) システムの具現化

以上のUCLAカーネルの実現コードは，基本カーネル部分で760行（Pascalコード），I/Oサポート部分の内，デバイス独立な内部インターフェイスが300行，デバイス依存のドライバーが約300行であり，かなりコンパクトな構成となっているが，これらの実現コードの行数は，プログラム検証の可能性と関係している。

UCLA Data Secure Unix のシステム構成を，図1－1に示す。

カーネルはOSの核であり，サイズも最小にし，非常に簡潔に構成されている。従ってカーネルの上で直接に稼動する拡張部分が必要となり，OSインターフェイス，ネットワーク管理，プロセスの初期化，スケジューラー等の機能がそこで実現される。セキュリティに関連した拡張には特権（capability）管理，プロセス間通信，仮想記憶管理，ある種のファイル・システム・インターフェイス等がある。UCLA Unixでは，カーネルとOSインターフェイスの間に中間的なインターフェイスのレベルを設定し，KISS（Kernel Inter-

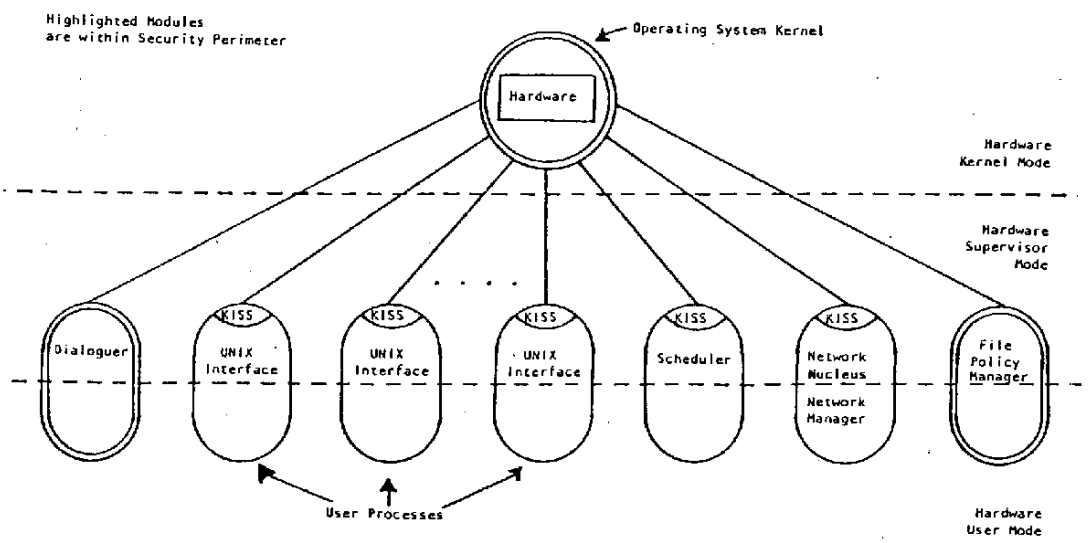


図1－1　UCLA Data Secure Unixのアーキテクチャ

face Sub-System ）と呼ぶ。すべてのプロセスでは，カーネルの直接呼び出しはせず，スケジューラーや後述のポリシー・マネジャーにメッセージとして要求を渡す。これらの要求はKISS を介してカーネル呼び出しに変換される。

ＯＳインタフェイスに関連して，次の３つの特別プロセスが設定されている。

① ポリシー・マネジャー（Policy Manager）

保護データや保護条件の変更を司る。

② ダイアローガー（ Dialoguer ）

ユーザの確認（ Authentification ）を司る。

③ スケジューラー（Scheduler）

資源管理（ CPU，プロセス・スケジューリング，ページ管理等）を司る。

セキュリティに関係する部分は，すべてカーネル命令によって実行される。

特別プロセスの関連は図１－２に示される。

すべての入出力操作（含端末）は他の操作と同様に，特権機構で制御される。Ｉ/Ｏ の完了割込は，他のプロセス間通信と同じように扱われる。

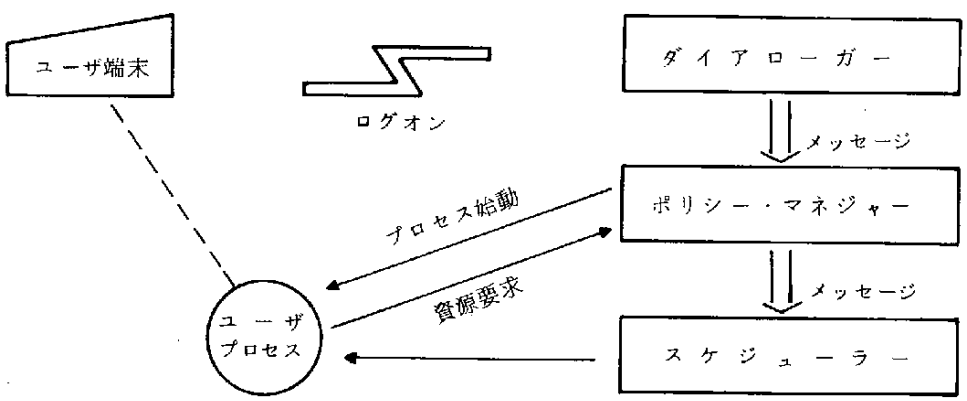


図１－２　ユーザ・プロセスと特別プロセスの関連

セキュリティ管理の中核を占める特権機構（capability）は，保護情報のカーネル表現であり，プロセスがアクセスできる対象を管理する。各プロセスはこれらの特権を記したC－リストに関係づけられる。C－リストは図1－3のように構成される。

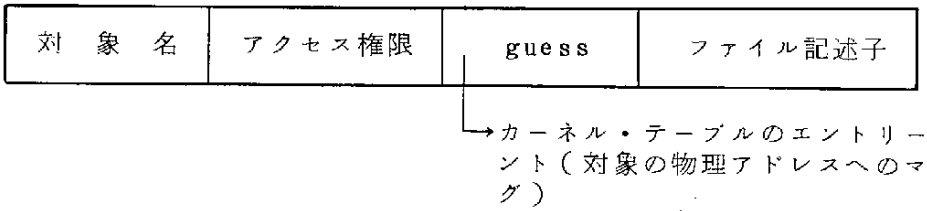


図1－3　C－リストの構成

(5)　検証のステップ

セキュリティ命題を満たす仕様の検証は，次の段階的アプローチで実現された。

①　抽象機械の規定

ユーザ・プログラムで利用可能なハードウェア，ソフトウェアの拡張マシンについての抽象的表現を定義 → セキュリティ定義が適用される意味的環境を与える。

②　抽象機械の解釈

個々のカーネル命令の記述を含む。抽象機械の当初の記述でなされている仮定もしくは制限と無矛盾であることを検証 → 抽象機械が効果的ＯＳ設計の枠組を提供することを示す。

③　基本命令に関する抽象入出力命題の規定

セキュリティ定義と整合的であることを検証

④　意味的定義の規定

Pascal言語を拡張，必要なハードウェア機能を含む。

⑤　抽象命題に対応する具現命題の規定

③に対してPascalで記述する。

⑥ プログラム・コードの検証

帰納的命題証明の手法を用いる。

会話型検証システムの開発

詳細は参考文献〔3〕を参照のこと。

(6) 問題点

当システムでは同期処理の問題を排除している。これはシステム構築の主目的を検証可能性に置いているため，検証が困難となる並列プログラムを排除し，カーネルの待ち問題を回避している。1つのカーネル命令の実行は単位時間で終了し，その間の割込みを排除する（非カーネル命令では並列処理可能）。このためリアル・タイム・アクティビティには適さず，応答タイプのシステムに向いている。

UCLA Data Secure Unix の最終開発が，どの段階まで達成したかは不明であるが，参考文献〔2〕の結論を要約すると，次のようになる。

① ＳＯＳの開発コストは通常のシステムより高い。

② 高信頼で整合性の高いシステムを構成でき，厳格なモジュール構造により，拡張・修正が容易である。

③ 効率に関しては，アーキテクチャ上の制約が多大な影響を及ぼしたとは考えられない。

④ カーネル構造による試みが成功したので，従来のＯＳアーキテクチャを再検討する必要がある。

尚，UCLAのアーキテクチャの特徴である独立分離した命令群，一実行単位に割込みが入らない，命令の結果に影響するＩ/Ｏを発生させないなどの状態遷移の不可分性（indivisible）は，ファームウェアでの具現化の可能性が大きいことを示唆している。

〔参考文献〕

〔1〕 Popek, G.J. and Farber, D.A. "A Model for Verification of Data Security in Operating Systems." Comm. ACM, Vol. 21, No. 9, (Sept. 1978).

〔2〕 Popek, G.J., Kampe, M., Kline, C.S., and Walton, E.J., "UCLA Data Secure Unix," Proc. 1979 NCC, AFIPS Press.

〔3〕 Walker, B.J., Kemmerer, R.A.,and Popek, G.J., "Specification and Verification of the UCLA Unix Security Kernel," Comm. ACM, Vol. 23, No. 2, (Feb. 1980).

1.3.4 KVM／370

(1) 目 的

KVM/370 (Kernelized VM/370) は，IBMの中大型機用の商用ＯＳであるVM/370 を改造し，セキュリティ・カーネルを組み込み,SOS を実現することを目的としたSDC社のプロジェクトである。広く使われている商用のＯＳをベースにしていることが，このプロジェクトの特徴である。

図1－4にKVM/370 のシステム・アーキテクチャを示す。

(2) セキュリティ・モデル

KVM/370 は軍のセキュリティ・モデルを実現するよう設計されている。すなわち，システム内の各主体，対象（すなわち，客体）にセキュリティ・レベルを付与し，主体が対象にアクセスする際に，次の２つの条件を守るよう強制する。

・セキュリティ条件

主体のセキュリティ・レベルが対象のセキュリティ・レベルより低いか等しい場合，read / appendはできない。

・封鎖条件

主体のセキュリティ・レベルが対象のセキュリティ・レベルと等しい場合のみwrite アクセス（read / write の両方を許すアクセス）が許される。

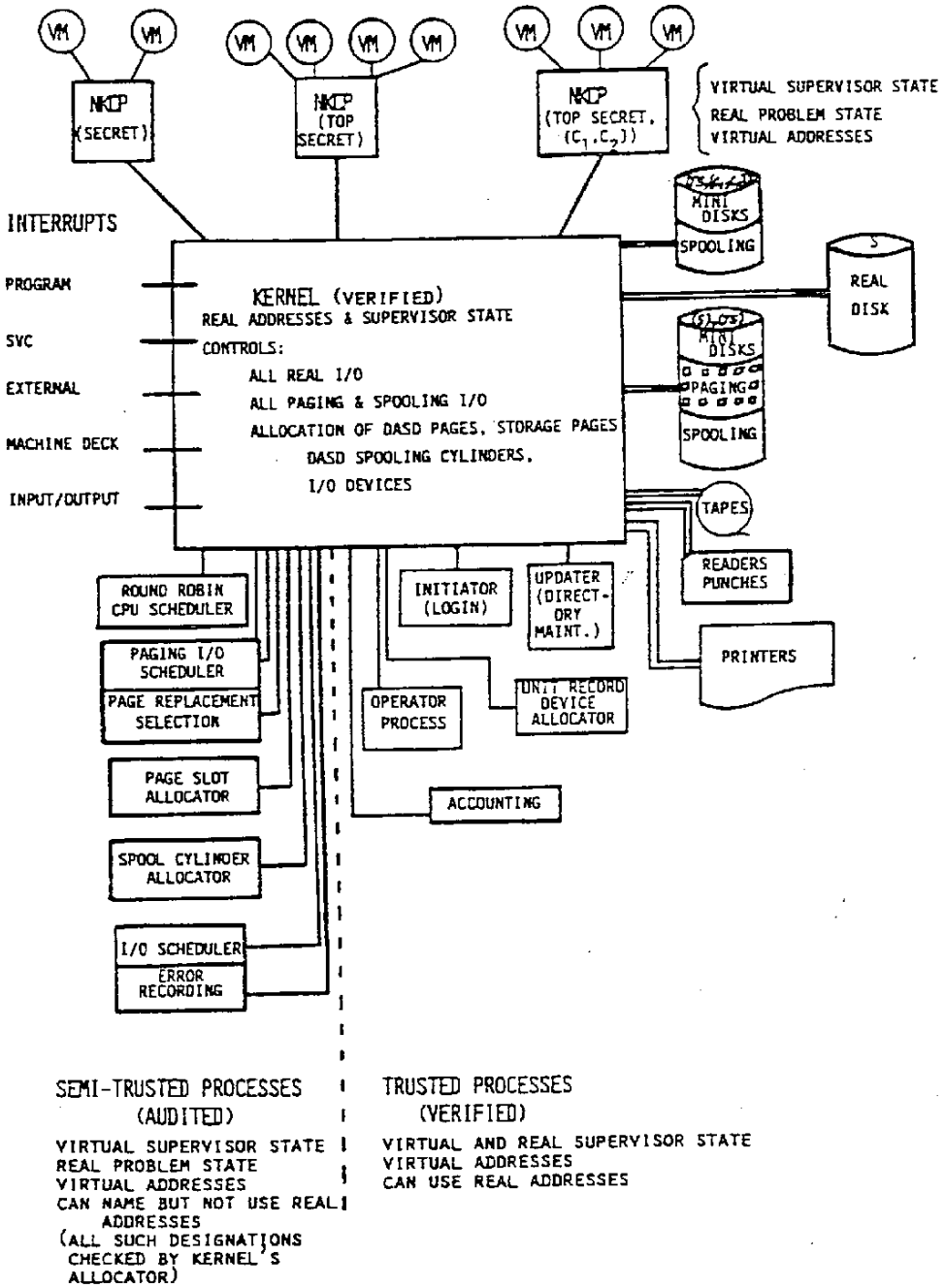


図 1 － 4　KVM/370 のシステム・アーキテクチャ

ここで主体とはユーザ，プロセスなどのシステム内の能動的な要素である。具体的な主体には，NKCP（Non Kernel CP）と呼ばれる各セキュリティ・レベルごとに存在するカーネル外の制御プログラムと,グローバル・プロセスと呼ばれる異なるセキュリティ・レベルの複数のNKCPとインタフェースをもつプロセスとがある。対象とはデータまたはデータの入れものである。具体的な対象にはDASD上のデータ，DASDボリューム，データ・ボリューム，ユニット・レコード装置,実メモリ，プロセス，VMの実行環境（テーブル，作業域，レジスタ）がある。

(3) システムの構成

KVM / 370 システムは次の要素から構成される。

- カーネル
- 高信用プロセス（ trusted process ）
- 半信用プロセス（ semi - trusted process ）
- NKCP（ Non Kernel CP ）
- ユーザ仮想マシン

カーネルはVM/370のCP（ Control Program ）の機能のうちセキュリティに関与する部分をとりだしたものであり，カーネルがセキュリティ・モデルを実現していることは数学的に検証する必要がある。

極端な性能の低下を防ぐために，カーネル以外でもある種のシステム・モジュールには複数のセキュリティ・レベルにまたがるシステム・データへのアクセスを許している。これらのシステム・モジュール（グローバル・プロセスと呼ぶ）についても，カーネルと同じように，セキュリティ・モデルを実現していることを数学的に検証するべきであるが，現実問題としてそれが不可能なものもある。グローバル・プロセスのうち，数学的検証の対象とするものを高信用プロセスと呼び，現実的に数学的検証が不可能なものを半信用プロセスと呼ぶ。半信用プロセスについては，十分な監査を行なう。

カーネルと高信用プロセスは Jovial で記述されており，合計で6,000 行である。高信用プロセスは，LOGIN 処理，ディレクトリ更新，オペレータとの交信，ユニット・レコード装置の割当て，会計情報処理などの機能を実行する。

半信用プロセスはアセンブラで記述され，10,000行である。半信用プロセスは，CPUスケジュール，ページング処理，スプールのスロット割当て，I/Oスケジュール，エラー・レコーディングなどの機能を実行する。

NKCP は VM/370 の CP の機能のうちセキュリティに無関係な部分に相当する。NKCPは各セキュリティ・レベルに1個ずつ存在し，そのセキュリティ・レベルのシステム・データにのみアクセスする。NKCPは仮想マシン上で走行する。すなわち，プロブレム状態で動き，仮想アドレスのみを使用する。NKCPはアセンブラで記述され，70,000行である。

ユーザ仮想マシンはユーザ・プログラムを実行する仮想マシンであり，そのセキュリティ・レベルのNKCPの制御を受ける。

(4) 検　証

セキュリティ・モデルが実現されることを数学的に検証するために，カーネルと高信用プロセスは Euclid で記述することを意図していたが，実用に耐えるコンパイラがないため断念した。このためカーネルと高信用プロセスの仕様（specification）に対し，検証を試みた。これらの仕様はSDCの仕様記述言語である InaJo で記述された。実際に検証がどこまで行なわれたかは報告されてないが，文献〔1〕*には検証された旨記述されている。

(5) 侵入テスト

KVM/370 について侵入テストが行なわれたことは報告されていない。VM/370 そのものに対しては侵入テストが行なわれ，35項目の欠陥が見つかった（文献〔2〕*）。これらの欠陥がKVM/370 では存在してないことは確認された。

(6) 問　題　点

理論的な観点からは，半信用プロセスを検証の対象外としている点に弱点がある。

---

*：文献〔1〕IEEE Computer, Vol. 16, No. 7.

〔2〕"Penetrating an Operating System: A Study of VM/370 Integrity," IBM Systems Journal, No. 1, 1976.

実用上の観点からは性能の低下，リソースの使用効率の低下，サポートしているハードウェア構成が限定されていること，監査およびセキュリティ管理者のためのサービス機能がないことなどの問題点がある。

(7) 現時点での評価

KVM/370はIBM4331, IBM4341,アムダールV7/Aでデモンストレーションが行なわれた。KVM/370の性能は当初は標準のVM/370に比べて½程度であったが，現在では¾程度まで改善されている。KVM/370は大規模タイムシェアリング・システムの複雑さに正面からとりくんだ現在までの唯一のプロジェクトである。性能の点では，前述の報告が事実なら，KVM/370はほぼ実用の域に達している。ただし(6)で述べたように現在のKVM/370はセキュリティの実現の検証が不十分であり，しかも実際の運用のための機能を欠いているため，デモンストレーション用にしか使えないと思われる。

1.3.5 KSOS

(1) 概　　要

KSOSはKernelized Secure Operating Systemの略で，KSOS-11として知られており，PDP-11/70用のカーネルを基盤とするシステムの商用プロトタイプを構築する試みの代表的なものである。カーネルの最上位層にはUnixエミュレータがあり，Unixユーザ・インタフェースを提供している。カーネルの最上位仕様（Special言語で記述してある）全体のセキュリティの諸性質の検証と，プログラム・コード（Modula言語で記述してある）と仕様との間での検証が予定されていた。FACC(Ford Aerospace and Communications Corp.)との契約が1980年12月で切れてしまった。Unixエミュレータとユーザ・ソフトウェアという階層構造で実現されているので性能は悪いが，しかしカーネルの最上位仕様レベルでの情報フローの性質を（SRIで開発したBoyer-Moore定理証明器を使用して）検証することに成功した。プログラム・コードの検証は人手で行なわれた。カーネルは応用業務用の役に立つ基盤であると実証されるかもしれないが，Unixエミュレータは，カーネルの機能のいくつかと重複して

おり，Unixエミュレータとカーネルを結合して使用すると，性能が悪くなる。

米国海軍では，Logicon社に資金を出し，FACCの製品（KSOS）を強化し，カーネルをより小さく，かつ高速にし，元のエミュレータと交替するためのカーネル・インタフェース・パッケージ（SCOMPを参照のこと）を作成させている。Unixのシステム・コールを取り扱うインタフェースの開発はまだ可能性がある。標準システム仕様書（B5仕様と呼ばれる*）と標準詳細仕様書（C5仕様と呼ばれる*）と同様に，形式的仕様書もこれらの変更と一致するように維持・管理されている。

(2) KSOSの設計

KSOSは，次の3つの構成要素からなる。

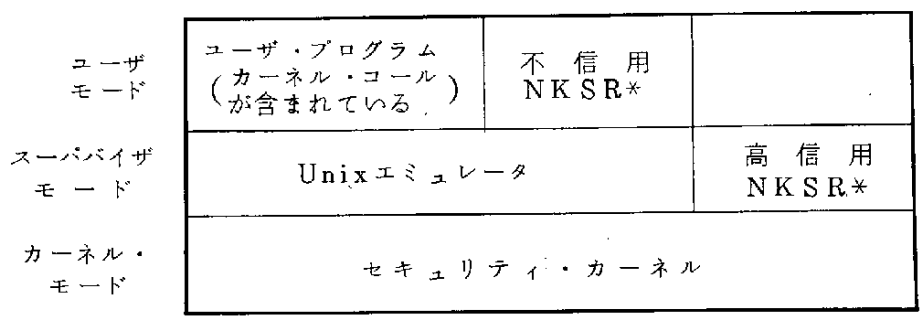
① セキュリティ・カーネル

② Unixエミュレータ

③ 非カーネル・システム・ソフトウェア

これらの構成要素の関係を図1－5に示す。

セキュリティ・カーネルは，完全であることが実証できる範囲での簡単なOS（Operating System）の機能を提供する。セキュリティ・カーネルには，



*：Non-Kernel Security Related Software
（非カーネルのセキュリティ関連ソフトウェア）

図1－5 KSOSのシステム・アーキテクチャ

---

*：Phase A（概念段階，Canceptual Phase），
Phase B（確定段階，Definition Phase），
Phase C（設計段階，Design Phase），
Phase D（製作・建設段階，Construction Phase），
Phase E（運用段階，Operational Phase）
に対応していると思われる。

システム中の全リソースの制御機能が集中している。セキュリティ・カーネルは，ユーザ・プロセスがリソースへアクセスを試みるたびごとに仲介し，そのユーザ・プロセスがアクセス制御ポリシーに則っている場合のみアクセスを許可する。セキュリティ・カーネルは，マシンの特権アドレス空間（PDP-11／70ではカーネル・モードと呼ばれる）に常駐している。このアドレス空間に常駐しているプログラムは生のハードウェアとソフトウェアのすべてをアクセスすることができる。

Unixエミュレータは，スーパバイザ・モードのアドレス空間に常駐する各々のUnixプロセスの一部である。Unixエミュレータは，ユーザ・プロセスからのUnixシステム・コールを相当するカーネル・コールの列に変換する。

非カーネル・システム・ソフトウェアは，システム・サービスを提供する独立のプロセスの集りである。Unixと同様に，KSOSはOS中に組み込まれているログイン（login）のようなシステム・サービスは提供していない。むしろ，これらのシステム・サービスは，セキュリティ・カーネルの外側に常駐する高信用プロセス群（trusted processes）によって提供される。

これらの高信用プロセス群は，セキュリティ・カーネルが厳守させている規則に違反してもいい特権を持っている。Unix エミュレータは検証されていない関係上，信用できない（untrusted）ので，高信用ソフトウェアからは直接使用することはできず，セキュリティ・カーネルを直接使用することになる。

(3) セキュリティ・カーネル

セキュリティ・カーネルの機能を抽象マシンの観点で見ると，システムの基本的ハードウェア・リソースからそのインタフェース用の対象（object）（例えば，プロセス，プロセス・セグメント，ファイル，装置，そしてサブタイプ（subtype））を生成し，これらの対象へのアクセスすべてに介入している。

セキュリティ・カーネルは，3つのアクセス審査規則を励行している。第1番目の規則はDoD（米国防省）のセキュリティ・ポリシーである。この規則では，情報を読む際に適切な使用許可権（clearance）と知る必要性（need-to-know）を保持しているか（単純セキュリティ性（simple security property）と呼ばれる），そして読まれた情報がより低いセキュリティ・レベルのファイ

ルに対して書き込まれ，情報が格上げ（downgrade）されないか（セキュリティの＊性（security ＊−property）と呼ばれる）を検証することを要求している。

第２番目の規則は，インテグリティ・ポリシーである。インテグリティは，システム中のデータベース，プログラム等を，それに対して読み取りアクセスを許された任意のプロセスがそれを変更することを防御する機構である。この規則は，１番目の規則とは数学的には，双対関係（dual）にある。

第３番目の規則は，自由裁量的アクセス制御（discretionary access control）のポリシーである。最初の２つの規則と同様に，自由裁量的アクセス制御はユーザの制御下に完全にある。ユーザは自分の裁量で自分の所有する対象を他のユーザに使用許可することもできるし，使用を拒否することもできる。KSOSはUnixと同様に，自由裁量的アクセス制御ポリシーを励行している。

1.3.6 SCOMP

(1) 目　的

SCOMPは，Guardian Project（Multics システムのセキュリティを調査し，エンハンスすることを目的としたプロジェクト）の一部として，ハネウェルが中心となって，DoD，NAVALEX（Naval Electronics System Command）と共に開発に取組んできたSOSであり，当初はフロント・エンド・プロセッサ用SOSの開発を目的としたものであった。

しかしながら，現在のSCOMPはGuardian Project の中止等に伴ない，もともとのデザインとは異なったものとなっており，フロント・エンド・プロセッサ用SOSというより，汎用コンピュータ・システム用SOSとなっていると言われている。

(2) セキュリティ・モデル

SCOMPは，DoDのセキュリティ・ポリシーを実現するよう設計されており，形式的モデルとしてBell & LaPadulaモデルを採用している。

本モデルの基本的ルールは，Simple Security と Security Property と

呼ばれるものである。

・Simple Security

データのセキュリティ・レベルがリーダ（処理）のセキュリティ・レベルより高い場合，データの読み込みを行なわない。

・Security Property

データを受取る対象がデータの書き手（書く処理）よりもセキュリティ・レベルが低い場合，データを書けないというものである。

以上の様なデータの暴露を防ぐセキュリティ・ルールに加えて，データの破損を防止する同様のセットが存在する。これらはSimple Integrity，Integrity Property と呼ばれ，データの修正をコントロールしている。

(3) ハードウェア

SCOMP をインプリメントするハードウェアは，ハネウェルのレベル6ミニコンピュータ（16ビット）をベースに，SPM（Security Protection Module）と呼ばれる機構を付加したものである。

システムの各コンポーネントは，すべてレベル6のバスにつながっており，各種I/O，プロセッサ，記憶装置をアクセスしている。

SPMは，セントラル・プロセッサと，他のあらゆるシステム要素を結ぶバス上に存在し，全てのプロセッサの要求を捕捉すると共に，メモリやI/O装置をアクセスする前に要求の確認を行なう特別なハードウェア機構であり，パフォーマンスの向上を目的としたものである。図1－6にバスで他のシステム要素と結ばれたSPMの配置を示す。

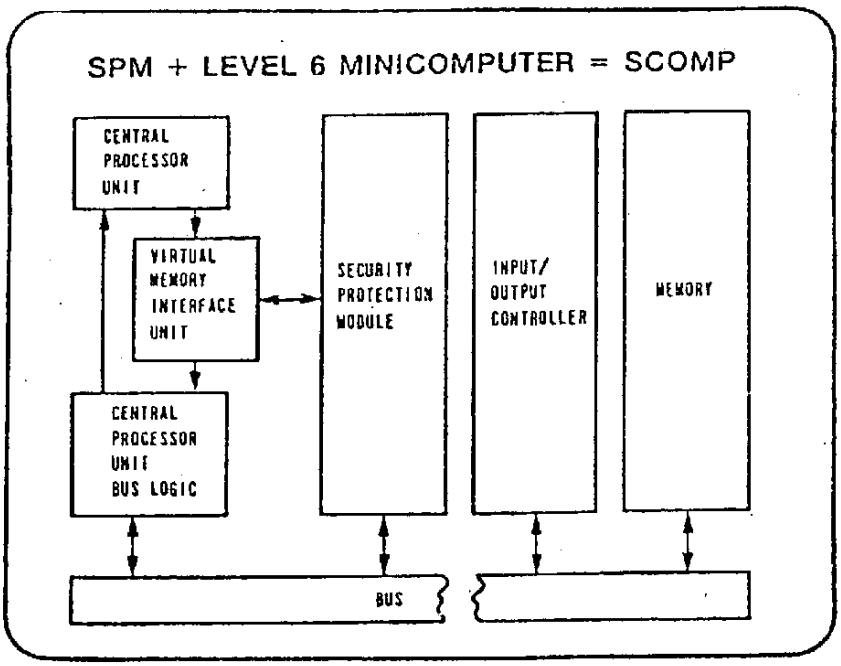


図１－６　SCOMP ハードウェアの内部構成

(4)　ソフトウェア

SCOMP のオペレーティング・システムは，次の３つの主要な機能から構成されている。

・セキュリティ・カーネル

セキュリティ・メカニズムと，すべてのアクセスのコントロールを行なう。

・トラステッド・ソフトウェア

管理者，オペレータ，ユーザがセキュリティ・カーネルを使用する場合に必要なインタフェース・サービスをサポートする。

・SKIP (Scomp Kernel Interface Package)

低レベルのアプリケーション・インタフェースであり，ファイル・システム，イベント・メカニズム，プロセス・コントロールをサポートする。

図１－７に SCOMP ソフトウェアの体系を示す。

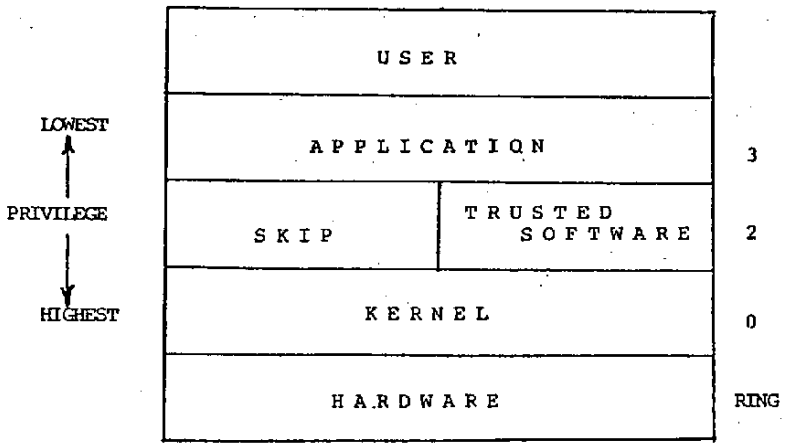


図１－７　SCOMPソフトウェアのアーキテクチャ

① セキュリティ・カーネル

セキュリティ・カーネルは，全ての資源の管理，スケジュール処理，メモリ管理，トラップ・インタラプト管理，オウディティングを実行する基本的なオペレーティング・システムである。

又，オブジェクトとしてセグメント，デバイス，プロセスの３つのタイプをサポートしており，セキュリティ・ポリシーにしたがって各オブジェクトに対するアクセスをコントロールしている。

② トラステッド・ソフトウェア

トラステッド・ソフトウェアは，ユーザ，システム管理者，オペレータとSCOMPシステムとのインタフェースをサポートするものであり，サービスタイプにより，

- トラステッド・ユーザ・サービス
- トラステッド・オペレーション・サービス
- トラステッド・メンテナンス・サービス

の３つに分割されている。

③ SKIP

SKIPは，アプリケーションとセキュリティ・カーネルとのインタフェー

スをサポートするソフトウェアであり，Unixエミュレータの結果の反省から，SCOMP上に開発されたものである。

SKIPで用意されている機能として，

- 階層的な複数レベルのファイル・システム
- 子プロセスの創成
- 処理同期の為のイベント・メカニズム
- 低レベルのインタフェース

等がある。

(5) 検　証

セキュリティ・モデルが実現されていることを形式的に検証するために，カーネルとトラステッド・ソフトウェアは，下記の仕様記述言語を使用して開発を行なっている。

① カーネル

カーネルの仕様は，Special を使用して記述されており，検証はSRIのHDM（Hierarchical Development Methodology）を利用して行なわれている。

尚，プログラムはUCLAパスカルで記述されており，約10Kステートメント，ロード・モジュールの大きさ約63KWである。

② トラステッド・ソフトウェア

トラステッド・ソフトウェアの仕様は，Gypsy を使用して記述されているが，検証については不明である。

(6) 評　価

SCOMPのハードウェア及びソフトウェアは，Los Alamos, Mitre, Logicon, そしてGeneral Electric を含めた数社に現在導入されており，今後実用面での評価が論議を呼ぶものと思われる。又，ハネウェル社のレベル6シリーズの拡張版である32ビットのDPS-6/94用のSPMも実現可能と考えられる。

1.3.7 PSOS

(1) 目　的

PSOS（Provably Secure Operating System＝証明可能なＳＯＳ）は1970年代の中期から後期にかけてSRI社で最初の仕様が記述された。この文書は1980年の初めに主契約者であるFACC（Ford Aerospace and Communications Corp.）と副契約者であるHoneywell社に対する製品仕様の一部として使用された。

PSOSの目標は中規模から大規模の汎用コンピュータをベースに，セキュリティ・カーネルだけでなく，オペレーティング・システム全体が仕様を満たしていることを形式的に検証することである。

(2) セキュリティ・モデル

PSOSは Special 言語により仕様化されており，約２０の階層構造化されたモジュールより成っている。

PSOSのセキュリティ概念は資格（capability）モデルに基づき，対象はこの資格により統制される。

資格は次の２つの部分より構成され，ブール配列で表記される。

① unique identifier（uid）

各uidに対してオリジナルな資格が与えられ，資格の分配統制も可能にしている。

② アクセス権

アクセス権とは，ある資格を有する主体（subject）が対象（object）に対してどの様な操作が許されるかを規定するもので，その対象に責任あるモジュールにより解釈される（図１－８参照）。

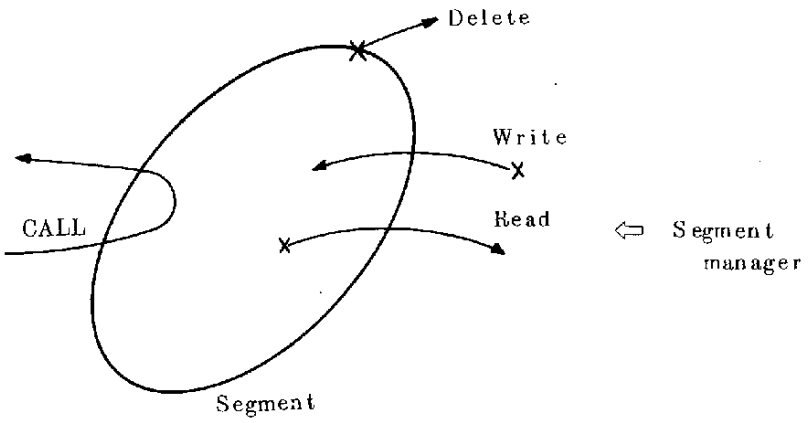


図１－８　Segment Capability のアクセス権

アクセス権の解釈は常に単調性の規則（monotonicity rule）に従っている。

PSOSも基本的にはアクセス行列モデルであり，Bell - LaPadula モデルの修正版である。

(3)　PSOSのプロテクション機構

PSOSの資格は以下に示す様に，非常に単純でかつ柔軟性のあるプロテクション機構により出来ている。

まず，資格そのものはタグ・ビットとして表現され，ハードウェアにより偽造不可性（nonforgeability）あるいは変更不可性（unalterability）の保証が実現できている。また資格上の操作は創成（create）と限定（restrict）の２つより成っている。創成とは資格が全てのアクセス権を所有する全く新しい別の資格を作ることを言い，限定とは，対象へのアクセスにより，ある資格とアクセス権をもつ uid と同一の uid である資格を作るとき，この資格とアクセス権はこれらの最大マスクを取る交わり（intersection）として与えられること

を言う。

一方，格納許可（store permission）とは，PSOSの基本的なstorage object manager（＝segment manager）により遂行されるもので，システム内の各セグメントは各々格納許可に対して，格納制限をもつ資格として表わされる。つまり，あるセグメントがある格納許可に対する格納制限を資格として持てば，その格納許可を持つ資格のみで成ることを意味する。

この制限を全てのsegment - modifying操作上で非常に簡単なチエックで遂行可能である。

先に述べた資格上の創成/限定の操作による資格の増殖は，この格納許可により統制される。つまり，ある種の型（type）をもつ対象上で遂行される操作は，その対象に対するtype managerにより定義され，ある与えられた資格を有する特定の対象上で許される操作は，与えられた資格のアクセス権により完全に統制される。

(4) PSOSの階層構造

PSOSに於けるデータや手続き（procedure）といった抽象対象は表1－5に示す様な抽象階層を成している。下位レベルに位置する抽象（abstraction）はハードウェアやファームウェアで実装され，上位レベルに位置する抽象はソフトウェアにより実装されるのが一般的である。

表1－5　PSOSの抽象化の階層

Level	Abstractions
16	user request interpretation
15	user environments and name spaces
14	user input-output
13	procedure records
12	user processes and visible input-output
11	creation and deletion of user objects
10	directories
9	abstract object manager
8	segments and windows
7	pages
6	system processes and system input-output
5	primitive input-output
4	arithmetic and other basic procedures
3	clocks
2	interrupts
1	registers and other storage
0	capabilities

この表をさらに属性別に類別すると，表1－6の様に階層化できる。これはPSOSの目標としている抽象そのものであり，階層の基礎は正に資格機構であ

る。この階層構造はPSOS の資格が抽象対象（abstract object）を構成する上で非常に役立つ性質を与えてくれる。一つは抽象対象に一意の名前が付けられるということ。もう一つは，資格が偽造不可であるということである。さらにこの資格機構は実現化が簡単であり，データや手続き抽象の創成に於て強力なmodularityを支えてくれる。この種の抽象はPSOSそのものの設計基盤であり，システム・プログラムはもとより，応用プログラムへも適用可能である。

表１－６　PSOSの類別の階層

Level	Abstractions	PSOS Levels
F	user abstractions	14-16
E	community abstractions	10-13
D	abstract object manager	9
C	virtual resources	6-8
B	physical resources	1-5
A	capabilities	0

PSOSの資格機構は一般的であり，任意の方策（policy）を構築するサブシステムに充分耐え得る。しかもシステム・プログラムを保護する特殊な保護機構は全く不要であり，KSOS や UCLA に於けるtrusted process に対しても優位である。

(5)　PSOSの検証

PSOSのプログラム・コードの検証が行なわれたが否かは不明である。

PSOSはUCLAのカーネルと同様，実行機構をセキュリティ方策（policy）から分離しており，これらのシステムは資格を使って対象の参照統制を行っているが，実行機構の検証では実行機構そのものを破壊したり，あるいは迂回することができないということを検証しなければならない。また，機構のある特定の使用がある特定の方策を正しく実行することを示すには別の検証が必要である。

(6)　おわりに

Honeywell社はSPM付のLevel-6 ミニコンピュータと類似の次世代の３２ビット・ミニコンピュータ・ハードウェアを入札した。この契約は１９８１年５月に切れた。Honeywell社は１９８２年に新規に契約して関連するハードウェアの設計作業を継続している。

1.3.8　米国防省のコンピュータ・セキュリティ評価基準

米国防省では，数多くのコンピュータ・システムを建設し運用してきたが，それらの多くはリモート・アクセス／リソース・シェアリングのシステムであり，秘密度の高い軍事情報を取扱う上で種々の問題が発生してきた。そこで1967年，国防省を中心としてコンピュータ・セキュリティに関する調査研究が始められ，1972年に管理的・技術的基準として"DoD Directive：Security Requirements for Automatic Data Processing（ADP）Systems"が定められた。更に，1978年には高信頼コンピュータ・システム（Trusted *1 Computer System）の信頼度を評価するための評価基準を作成する作業が始まり，現在「DoD Computer Security Evaluation Center（1981年設立）」を中心に精力的に作業が進められている。

本項においては，1982年5月*2に公表された高信頼コンピュータ・システム評価基準（Trusted Computer System Evaluation Criteria）の案について概説する。

(1)　高信頼コンピュータ・システムの基本要件

秘もしくはこれに類する情報資料等（以下「秘情報等」という）を取り扱うＡＤＰシステムにとって不可欠であり，かつ高信頼コンピュータ・システム評価基準の基礎となるべき基本要件は以下の5つである。

基本要件第1：秘区分の明示（Marking）

秘情報等を処理・運用するＡＤＰシステムでは，その取り扱う全ての情報資料に秘区分を明示しなければならない。また当該ＡＤＰシステムからアウトプットされるものの中に秘情報等が含まれる場合には，その旨を厳格に明示されることが保証されなければならない。

基本要件第2：強制的セキュリティ（Mandatory Security）

秘情報等を取り扱うコンピュータ・システムにあっては，特別の許可なし

＊1："Trusted"をここでは「高信頼」と訳しているが，文字通り，「信じて頼れる」という意味で，"reliable"とはニアンスが異なっている。

＊2：Final Draftが1983年1月27日に発行されているが，入手できなかった。

に勝手にその情報の秘区分のマーキングを変更したり，情報をより低い秘区分の記憶媒体に移し変えたりすることが不可能であり，かつユーザ個人の取り扱いを認められている秘区分より高い秘区分の情報等に対するアクセスは許可しないということが無条件で保証されなければならない。

基本要件第3：自由裁量的セキュリティ（Discretionary Security）

職務上，当該秘情報等を取り扱う必要があるとあらかじめ認められたユーザと，実際にアクセスしようとしているユーザとが同一であることを先ず確認し，これを基礎として秘情報等に対するアクセスを制限できることがコンピュータ・システムにとって不可欠である。

基本要件第4：責任の明確化（Accountability）

秘情報等を処理，運用するためのADPシステムにあっては，秘情報等がアクセスされたりするごとに，それを実行したユーザ個人の処理を明細に追跡することができるような配慮がなされていなければならない。

基本要件第5：継続的保護（Continuous Protection）

高信頼コンピュータ・システムのセキュリティに関する部分は，運用開始後も秘情報等を制御するシステムの能力を無効にするような不正な改修が，ハードウェア，ソフトウェアを問わずに加えられていないことを保証する必要がある。このため，セキュリティ機能を統制下に継続的に置く必要がある。

(2) 評価段階の概要

本評価基準に定められたシステムの各段階は以下のとおりである。それぞれの段階は，秘情報等を保護するためにシステムに取り入れなければならない改善を示している。

段階D：最少限の保護（Minimal Protection）

一応評価はされているものの，より高次の段階の評価要件を満足するには到らないもの。

段階C：自由裁量的保護（Discretionary Protection）

自由裁量もしくは，職務上知る必要性のない個人に対する保護が行われている。

段階B：強制的保護（Mandatory Protection）

TCB[注1]がそのデータの秘区分に応じた標識をデータに強制的に付け，その標識を不正に変更されないように保護することが，この段階における主要な要件である。本段階に評価される高信頼コンピュータ・システムは，当該システム内のデータ・ファイルに対し，強制的にある種の標識が付加されるものでなければならない。ベンダは，ＴＣＢの拠所となったセキュリティ・モデル及びTCBの仕様書を備えなければならない。また参照モニタ[注2]の概念を満足するものでなければならない。

段階A：検証済みの保護機構（Verified Protection）

システム内で使用されている強制的及び自由裁量的なセキュリティ制御が，当該システムによって格納・処理される秘情報等を効果的に保護していることを保証するのに，形式的なセキュリティ検証方法を用いなければならない。

(3) 評価区分の概要

コンピュータ・セキュリティ評価基準のもとで認められたシステムの区分は以下のとおりである。

区分D：普通（Common Practice＊）

より高次の評価区分の要件を満たさないと評価されたシステムは，この区分にランクされる。

区分C－1：自由裁量的セキュリティ保護（Discretionary Security Protection）

この区分に評価されるには，ユーザ個人を確認する（前述の基本要件第4）ための機構が必要である。ユーザとデータの間の自由裁量的アクセス制御（基本要件第3）は実施しなくとも良く，又，自己防衛型であっても良い。

区分C－2：アクセス制御による保護（Controlled Access Protection）

ユーザに対し，少なくとも強制的に自由裁量的アクセス制御を行うシステ

＊：英語の意味は「一般的な方法」，「技術上の習慣」，「日常茶飯事的に行われること」であり，「コンピュータ・システムに対して特別な技術的対策を行っていない」ことを表わす用語である。

ムは，この区分に評価される。この要件を満足するためにセキュリティ・アド・オン・パッケージやセキュリティ・オーバーレイ・パッケージを使用しても良い。〔C-1〕との主な相違点は，この〔C-2〕が個人の責任の追求（基本要件第4）及びセキュリティ侵害の監査の機構を要することである。

区分B-1：標識によるセキュリティ保護（Labeled Security Protection）

本区分に評価されるシステムは，基本要件第2の強制的アクセス制御及び職務上，知る必要性を有しない個人に対する保護に適した自由裁量的アクセス制御を実施しなければならない。検証済みの形式的セキュリティ・モデルは必要としないが，TCBの概念は明確でなければならない。データには秘区分を明示する必要がある（基本要件第1）。また専門家による侵入テストを行い，その結果発見された重大な欠陥は，全て是正されなければならない。

区分B-2：システム構成全体にわたる保護（Structured Protection）

本区分に評価されるシステムでは，TCB以外の全ての明白な対象にまで強制的セキュリティの適用が拡大され，また情報フローに対する制御と漏洩チャネルに対する封鎖が実施される。TCBが励行しているセキュリティ・ポリシーのモデルが必要である。システム構成全体を保護し，厳格な構成管理[注3]が実施される（基本要件第5）。TCBは，ユーザ確認機構が強化され，高信頼化された設備管理を支援する機能も有する。

区分B-3：セキュリティ機構の専用領域化（Security Domains）

本区分に評価されるシステムのTCBは，セキュリティ・モデルを励行するものであり，特権は最少限度に限定される。全てのセキュリティ関連のプログラム・コードが明確に識別され，セキュリティに関連するコードと，関連しないコードとが，それぞれ異った領域に分けられるように，TCBが構造化される。TCBが参照モニタの要求を満足していることを実証する必要がある。セキュリティに関連しない領域内にあるソフトウェアの突発的な障害が，セキュリティ領域内にあるソフトウェアには全く影響を与えないようにするために，ハードウェアによる保護，もしくは全く影響を与えないことが確認されていなければならない。

区分A－　：検証済の設計（Verified Design）

本区分に評価されるシステムの主な特徴として次の3つの事項が挙げられる。

① 形式的数学モデルが存在すること。

② ＴＣＢの最高水準のユーザ・インタフェース仕様書が形式的に記述されていること。

③ 形式的検証技法を用いてＴＣＢが設計・開発され，完成したＴＣＢが数学モデルを満足することが検証されていること。

更に，ＴＣＢが参照モニタの要件を満足することを確認する（検証はされなくともよい）必要がある。

1982年現在，本区分に評価されるシステムの実用化が可能な技術水準に既に達している。

区分A－2：検証済のプログラム（Verified Implementation）

本区分に評価されるシステムは，形式的に機械で検査することができる方法論を用いてシステムの実際のプログラムを検証し，最高位の仕様書に適合することが保証されている。参照モニタの要求仕様を満たしていることを論証するためには，その他のプログラム開発支援ツール（例えば，コンパイラ群）と同様に，ハードウェア及びファームウェアの設計時にも形式的手法を採用することが重要となる。

1982年現在，本区分に該当するシステムの実用化が可能な技術水準の域にはまだ達していない。

〔注1〕　ＴＣＢ（Trusted Computing Base：高信頼計算機構ベース）

コンピュータ・システムの中のセキュリティ機構の全統合体，即ち，ハードウェア，ソフトウェア，ファームウェアの複合体をいい，この複合体によってセキュリティ・ポリシーの励行に責任を有する。

〔注2〕　参照モニタ（Reference Monitor）

データ（プログラム）のアクセスを要求してきたユーザやプログラムが，当該データ（プログラム）のアクセス権を有するか否かを審査する機構。

〔注３〕　構成管理（Configuration Management）

技術文書の中で示されたもの及び，製品として完成されたものとしてのハードウェアやコンピュータ・プログラムを機能的・物理的に管理すること。

【参考文献】

- Multics Security Enhancements

  Schroeder, M.D., Clark, D.D., and Saltzer, J.H., "The Multics Kernel Design Project," Proc. 6th Symp. Operating Systems Principles, ACM SIGOPS Operating Syst. Rev., Vol. 11, No. 5, pp. 43–56, (Nov. 1977).

- UCLA Data Secure Unix

  Popek, G.J., Kampe, M., Kline, C.S., Stoughton, A., Urban, M., and Walton, E.J., "UCLA Secure Unix," Proc. AFIPS NCC, Vol. 48, pp. 355–364, (June 1979).

- KVM/370

  Gold, B.D., Linde, R.R., Peeler, R.J., Schaefer, M., Scheid, J.F., and Ward, P.D., "A Security Retrofit of VM/370," Proc. AFIPS NCC, Vol. 48, pp. 335–344, (June 1979).

- KSOS

  McCauley, E.J. and Drongowski, P.J., "KSOS -The Design of a Secure Operating System." Proc. AFIPS NCC, Vol. 48, pp. 345–353, (June 1979).

- SCOMP

  Fraim, L.J., "Scomp: A Solution to the Multilevel Security Problem," IEEE Computer, Vol. 16, No. 7, pp. 26–34, (July 1983).

- PSOS

  Feiertag, R.J. and Neuman, P.G., "The Foundations of a Provably Secure Operating System (PSOS)," Proc. AFIPS NCC, Vol. 48, pp. 329–334, (June 1979).

1.4　SOSの背景

1.4.1　SOS出現の背景

アメリカ国防省は，軍事・情報工作用に世界各地にコンピュータを展開し，それをデータ通信回線で結合した地上最大のコンピュータ・ネットワークを構築している。存在自体が秘密にされているものがあることは確実だが，それについては我々は知り得ない。公表されているものだけでも，WWMCCS（世界軍事司令管制システム），COINS（地域情報ネットワーク・システム），陸軍司令作戦ネットワーク，TACFIRE(陸軍戦術火器命令システム），DLDES（師団レベル・データ入力システム）などがある。

これらのネットワークには，故意あるいは偶発的誤操作や破壊活動に対して完全に安全であることを保証する，最高度のセキュリティが要求されている。このセキュリティの範囲は，コンピュータ施設のみならず，ネットワークに接続しているすべての遠隔端末，ユーザ，さらに使用されるすべてのソフトウェア，ハードウェアにまで及ぶものである。むろん，通信回線を流れるデータにはその機密性に応じた強度の暗号化がかけられており，統合参謀本部関係の最高司令には，スーパー暗号と呼ばれる国防省最強の暗号化方式が用いられている。

上記のネットワークのうちWWMCCSは，その構成と操作法のほとんどが公開されているので，これを例にとって国防省のソフトウェア開発にかける姿勢を調べることにする。

1971年統合参謀本部は，国家司令部用に特に有事の情報処理を高速，高精度化する必要性から，WWMCCS の中心をなすコンピュータをネットワーク化することを決定し，1975年にはワシントンD.C.にある3台のコンピュータを結合するプロトタイプのネットワークを設計した。

その後，国内の陸海空軍基地5箇所のコンピュータもネットワークで結び，2度の作戦演習を経た後に，1977年に統合参謀本部への納入試験を終わり，WIN（WWMCCSコンピュータ間ネットワーク）が完成した。現在WWMCCS のコンピュータは全世界に展開された主要な米軍基地40箇所程度に設置されている。使

用されているのはHoneywell社の6000型コンピュータである。このすべてのコンピュータをWINの中に組み込む作業が現在行われている。このうちで，国防省のペンタゴンの中に設置されているコンピュータだけは特殊なもので，全ネットワーク内の情報の監視，記録が可能になっている。WIN が完成すれば，世界各地から集められた軍事情報が即時に，大統領を議長とする統合参謀本部に表示されるようになるのである。

実用化されているネットワークのセキュリティを知るためには，コンピュータ設置個所に常駐しているWASSO と呼ばれるWWMCCS EDPS保安担当将校用マニュアルが参考になる。WASSO はコンピュータのセキュリティの管理者で，セキュリティの規則が忠実に守られているかを監視するのが任務である。

WASSO はセキュリティに関する訓練を受けた将校で，高度なソフトウェア・プログラミングと，コンピュータ設備操作の経験を積み，Honeywell 社の6000シリーズの基本ソフトウェアであるGCOSを受講したものがなる。

WINのセキュリティにはどのようなものがあるか簡単に説明しよう。まず要員セキュリティとして，WINにタッチする人間は，遠隔端末を操作するものに至るまで，最高機密レベルの徹底調査を行う。このレベルの調査を行っていないものに遠隔端末を操作させる必要性が生じたときには，横に調査済みの要員を立ち合わせる。

コンピュータ施設への侵入や，その破壊を防止するための物理的セキュリティとして．設備は外界から完全に遮へいし，入口には衛兵を配置して入所許可リストでチエックを行い，異常発生時には警報を鳴らすようにしている。

コンピュータとコンピュータを結ぶ通信回線はつねに盗聴の危険にさらされているので，WIN では通信セキュリティが重要である。

上述の物理的セキュリティの確立してる設備から外にでる通信は，すべて国防省の暗号化装置を通している。また，設備内でも暗号信号と普通の信号は，混用による暗号強度の低下を防止するため，完全に電気的に分離している。

WINに使用されている基本ソフトウェアはGCOS Ⅲである。基本ソフトウェアが不正なシステム操作を排除できるようにすることを論理的セキュリティとい

う。GCOSⅢについては，考えられるすべての不正操作を加えテストをしてみたところ，危険であるという結論が出たが，前述の他のセキュリティが確保されていれば，最高機密保護は可能と判断されている。予防的手段として暗証パスワードを設定し，頻繁にこれを変更するとともに，すべての操作を記録する監査証跡という，コンピュータ・ファイルを作るようにした。

この監査証跡は定期的に，あるいは異常発生時にコンピュータにかけて分析し，不正操作あるいは誤操作の存在をしらべる。

国防省はWINの他にも，いくつかの世界的広がりのコンピュータ・ネットワークを持っている。次に考えている計画は，これらネットワークを統合して，1つのスーパー・ネットワークともいうべきシステムを作り上げることである。

このシステムが完成すれば，異なる目的のため設計された各種のネットワークで収集・分析された情報をさらに総合し，統合参謀本部における世界戦略の決定を支援する，極めて強力な手段となりうる。

しかしここに1つの大きな障害がある。結合していくネットワークが，それぞれ異なるセキュリティ・レベルで設定されていることである。

国防省の情報は，秘密，機密，最高機密のような，情報の重要性に従った分類の他に，NATO，太平洋，ラテン・アメリカのような区分けがある。これらを1つのネットワークに乗せることは，情報漏えいの危険がある。

さらに，ネットワークの規模が巨大化するにつれ，コンピュータや端末装置を操作運用する要員の数が増加してくるが，この全員について，徹底的に調査・監視を行うことは不可能である。そこで，論理的セキュリティを完全なものにして，権限のないものが自分に許されている以上の，高度の機密性を持つデータを手に入れようと要求を入力しても，それを拒否するネットワークにすることが考えられている。

米国防省のC3I（通信・司令・管制・情報）担当国防次官のWalkerは空軍のシステム・プログラマを中心とするタイガー・チームを組織して，1968年から1974年にわたってすべての商用基本ソフトウェアに対し端末から不正操作を加え，システム内部への侵入に成功し，一般の基本ソフトウェアのガードがいかに甘い

かを実証した。ここで指摘されたのは，コンピュータ内部の重要ファイルに対する不正アクセスを防止するセキュリティ・プログラムが，基本ソフトウェアとデータベース管理ソフトウェアの中に統一的なセキュリティ維持の思想を持たずに分散して置かれていることであった。Walker はこれを基本ソフトウェアの1個所にすべて集中して置き，ファイルに対するアクセスは，必ずそこを経由して行うべきだと提案した。

集中化されたセキュリティ・ソフトウェアは基本ソフトウェアの中核となるので，カーネル（Kernel，核）と呼び，この設計コンセプトで作られる基本ソフトウェアをKSOS（Kernelized Secure Operating System）と呼んだ。

カーネルへの要求事項は次の3つに要約できる。まず，すべてのファイルに対するアクセスは，例外なくカーネルで不正アクセスかどうかを検査できることがある。次に，カーネルを形成しているコンピュータ・プログラムは，いかなるソフトウェアによっても修正，変更，妨害を受けないことである。3番目には，カーネルは指定されたセキュリティに関することのみ行い，指定されない作業は絶対に行わないことである。

国防省は，コンピュータ・システムをそのセキュリティに応じてAからDまでにランク付けしている。さらにこのランク内にも順位があり，C－3とかB－1のように，細かくセキュリティ・レベルが分かれている。最高のAランクは最高機密を扱っても安全というものだが，KSOSはA－1に相当する。A－1とは，基本ソフトウェアに関する仕様が完全に明確であり，かつ最高セキュリティを実現しうることが形式的に検証できるものを指している。この上のA－2では，仕様に従って作成した実物の基本ソフトウェアが，実際に最高セキュリティを具体化していることが形式的に検証できることが要求される。今のところA－2に相当するシステムは，公表されたデータで知り得るかぎりでは存在しない。また，A－1のレベルでも，開発は現在行われているが，完成した基本ソフトウェアはまだない。

KSOSの代表的なものは，1978年Ford Aerospace and Communications 社が受注したKSOS-11である。この基本ソフトウェアはミニコンピュータのIB

MといわれているDEC社のPDP－11／70 ミニコンピュータ用に作られるものである。KSOS－11に要求されているのは，ベル研究所が開発したミニコンピュータ用汎用OS Unixが使えること，各種の機密レベルの情報が扱えること，セキュリティの確立が形式的に検証されていることである。1980年には一応完成しているが，最後の検証の段階が極めて難しいので，いまだにA－1レベルに合致していない。

ここでもわかるように，ミニコンピュータの基本ソフトウェアでも，セキュリティを確立することは極めて難しい。まして，大型コンピュータの基本ソフトウェアに至っては，現在の技術レベルでは不可能な状態にあるといってもよいであろう。コンピュータ・ネットワークはすべてのコンピュータを結合するものであるから，KSOS-11のようなミニコンピュータの基本ソフトウェアでは役に立たないように思えるが，国防省はネットワークを図1－9のような型で計画し，KSOS－11を実際に用いていこうとしている。

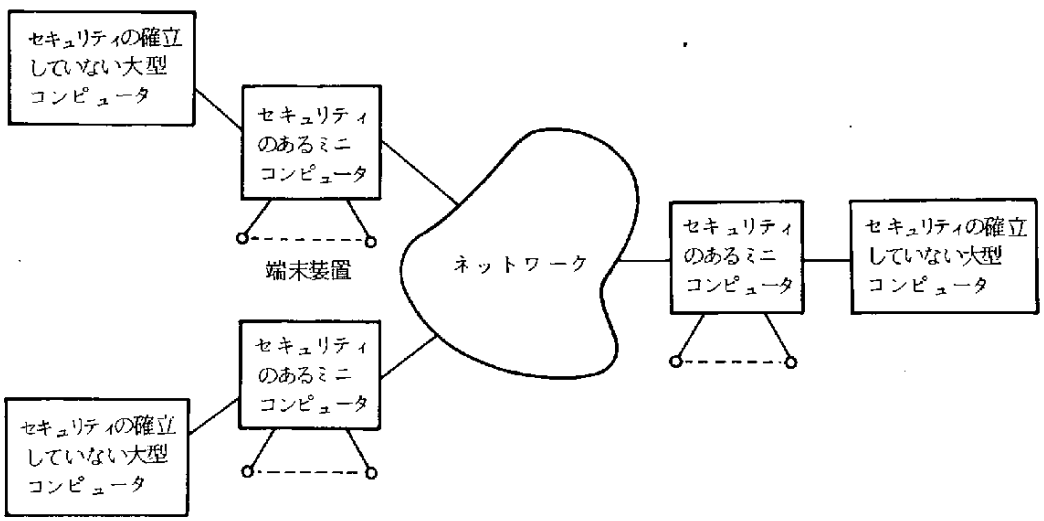


図1－9　KSOSを用いた米国防省のネットワーク構想

大型コンピュータの基本ソフトウェアのセキュリティは検証できない。つまり，信用できないのでそのままネットワークに接続せず，検証済みのKSOSを持つミニコンピュータを必ず介するようにするのである。このような形態でネットワー

クを構成するときに，大型コンピュータをホスト，それとネットワークの間に介在するミニコンピュータをフロントエンドという。ホストの持っているデータに対して，ネットワークの他地点からアクセス要求が出ると，フロントエンドの中に入っているKSOS－11 がその要求が正当か否かを判定する。

このようなカーネルに対する批判もある。IBM社のデータ・セキュリティ支援プログラムの部長Murrayは，カーネルがもしも不完全だと，この方式はすべての基本ソフトウェアに侵入されてしまうし，KSOSは極めて複雑かつ他のコンピュータ機種への応用性が低いので，市場性が少ないと指摘している。

1.4.2 軍用情報システムの現状

(1) 軍用システムの現状

軍事科学技術は近年めざましい発達をみせ，高性能化された多種・多様な兵器を駆使して至短時間内に広範囲な空間を対象とする，錯そう・複雑化した戦闘様相を呈するに至った。このような環境の下で，めまぐるしく変化する状況に迅速・正確に対応し，戦闘力を適時適切に投じて所望の効果を発揮させるためには，戦域内における戦術情報の指揮中枢への伝達と末端兵器に至るまでの指揮統制，並びに指揮中枢と政治中枢との間の戦略情報の伝達を組織的・効果的に実施できるシステムの開発が必要となってきた。今日，通信電子技術の発達により，戦闘指導に必要な全ての要素即ち末端の兵器から戦術・戦略をもシステムとして組み入れ，一元構成することが可能となり，各国ともC^{3}I（Command, Control, Communication and Intelligence）システムとしてこれの構築に力を注いでいる。

現代戦においては，C^{3}Iシステムの良否がそのまま戦闘の勝敗を決するとまで言われ，各国ともその整備・充実に努力を傾注しているが，このシステムを保全上の立場から見た場合，実際に軍事作戦を遂行するための作戦運用システムとしてのC^3 システムと，戦略・戦術を決定するための基盤となる各種軍事情報を取り扱う情報システムとに分けて考えた方が良いと思われる。

(2) 作戦運用システムの保全

作戦運用システムは，兵員・兵器・戦術等の総合力としての戦闘力を有機的に運用し，所望の時に，所望の空間で，所望の戦力を結集して所望の戦果をあげるためのシステムである。

現代の軍隊においては機動力が飛躍的に向上するとともに兵器も高性能化されており，作戦行動が発起されてから戦果を獲得するまでの所要期間が極端に短縮されてきた。特に防空作戦を実施する際には，敵の航空侵攻作戦が発起されたことを自軍が具体的に探知してから，数分ないし最大でも十数分のうちに有効な対策を講じ，防御戦闘を開始できなかったならば，防御側は壊滅的な打撃を被ることにもなりかねない程である。すなわち，自軍を防衛するにあたり，敵の全ての軍事行動に対して即断・即決・即応し効果的な防御作戦を遂行するためには，C^3 システムがその機能を常時・完全に果たすことが絶対条件となる。つまりC^3 システムには，システム障害に対する安全性及び物理的安全性が極限まで要求される。

これに対し最近C^3CM（Command, Control and Communication Countermeasure）という概念が確立されてきた。C^3CMとは，敵のC^3 システムを利用・妨害・混乱及び破壊するとともに，自軍のC^3 システムを敵の攻撃から防護するために軍事的手段を行使することである。すなわち，C^3 システムのセンサ，情報ネットワーク，航空機・ミサイル等の誘導システム，敵味方識別システム及び指揮統制機能そのもの等を対象として自軍のC^3 を敵のC^3CMから防護すること，並びに敵のC^3 を逆用・妨害，敢へん及び破壊して敵の戦力を低下させ，自軍の戦力を強化することを目的としている。つまり，戦場で直面する脅威に対抗して，敵の電子システムの効力を低下させて自軍の生存性を向上させるといった従来の電子戦の概念から一歩踏み出し，電磁スペクトラムを対象とした物理的攻撃及び通信保全を加味したものとしてのC^3CMが確立されてきたのである。

すなわち，C^3 システムの施設，装備，兵員，電磁スペクトラム等を重要防護目標として敵の物理的攻撃からも防護しなければならなくなってきたのである。

(3) 情報システムの保全

日常我々はインテリジェンスとインフォメーションを意識的に使いわけることをあまりしていないが本項の論を進めるにあたり，まずこの用語の相異を明確にしておく。

情報資料：Information

資料源から収集された素資料をいう。

情報：Intelligence

任務達成のために必要とする情報資料，すなわち敵，諸外国及び空域，地域，海域等に関する情報資料を処理して得た知識をいう。

ア．軍事情報の種類

一般に軍事情報と総称されるものの中には，次に挙げる各種の情報が含まれている。

① 戦力組成 ： 外国の軍隊等を兵力，編成，配置及び戦法等の要素に区分整理及び編集した情報

② 電子情報 ： 外国の発射する電磁波（原子爆発又は放射能源から発射されるものは除く。）を傍受又は測定して得た情報及び電子に関する技術的知識

③ 通信情報 ： 外国の通信電波を傍受又は測定して得た情報及び通信に関する技術的知識

④ 技術情報 ： 外国の技術研究開発及び軍隊の使用する装備品等の特性，能力，限界等に関する知識

⑤ 地誌情報 ： 軍事的利用を目的として国あるいは地方又は地域等の構造，特性及び機能等を明らかにすることによって得られた作戦及び用兵に対する地域的価値又は制約に関する知識

⑥ 戦略情報 ： 国家及び国際レベルにおける政策及び軍事計画の策定に必要な，諸外国の能力，特徴及び可能行動等に関する情報

イ．情報の意義

「敵を知り己を知れば百戦して危うからず」とは古来より言われているこ

とであるが，戦場において敵に勝つためには先ず情報において敵に勝つことが必要であり，作戦を成功に導くためには必須の要件である。このため，平時から一貫した組織のもとで，継続的に情報を収集し，敵の動きを未然に察知し，敵に先んじて準備し，事に臨んでは勝機を捕捉できる態勢を整えておかなければならない。今日の作戦においては状況が迅速に推移するため，作戦間における情報については機に即した積極的な情報活動と取得した情報の迅速な活用が必要である。

ウ．情報システムの保全

情報の要は，敵を知り己を知らしめざるにある。自軍の情報活動の背後には必ず敵の情報活動が伴っており，自軍の企図・能力等とともに，自軍が敵について知り得た事からの秘匿を厳にしなければならない。これが保全である。すなわち，保全とは敵の情報活動及び謀略活動を防止又は破砕して，情報活動に対しては情報資料を，謀略活動に対しては人・物・施設・組織及び機能等を防護するためのあらゆる活動をいう。

軍用情報システムの一般的特徴として，自軍の情報システムに対し，常に敵の国家の全技術力を動員した情報活動が行なわれており，敵に有効な情報活動を許すことは，すなわち自国の安全が著しく危険にさらされることになる。したがって情報システムの保全対策を実施するにあたっては，経済性・効率性よりも完全性を重視する必要がある。

以下に個々の保全対策を考える。

<u>コンピュータの保全</u>

- 自然災害，人為的破壊行為及びハードウェアの故障等に起因するシステムの運用停止及びデータ破壊や記録媒体等の破壊を防止するため，コンピュータ・システムあるいはコンピュータ・センタそのものを二重化する等の対象を要する。
- コンピュータ・センタを地下に建設し，電源等のユーティリティ施設の非常用代替設備を十分にする等してコンピュータ・システムそのものの生存性を向上させる。

- コンピュータ・システム内に収納されているデータの秘区分が明確に識別され，事故や不注意による無意識的な秘区分の変更を防止する。
- 異なる秘区分にまたがる複数のデータから新たなデータを作成した場合の秘区分の混乱を防止する。
- データに対する不正なアクセスが絶対不可能なコンピュータ・システムの建設が第一であるが，万一情報が漏洩した場合にすみやかに効果的な対策を講じられるよう，十分な監査機能を有することが必要である。
- 不正なプログラム修正が行なわれないように，また，正規のプログラム修正が行なわれた場合に，システムの保全性が損なわれていないことを確認するために，プログラムに対する監査機能を有することが必要である。

人の保全

- 情報システムに関係する人間の秘密保護の適格性の確認を厳格に実施し，関係職員の質を向上させるとともに，取り扱い得る情報の種類及び立ち入ることのできる施設等の資格の指定を厳密に行う。
- コンピュータ・システム内の情報を取り扱う場合には，個人の資格に加え，その個人が当該情報を取り扱う必要のある職務についているかを確実に点検し，合格した者に対してのみ情報を取り扱わせる。
- 関係職員が情報を取り扱う場合，必ずスーパーバイザを同席させる。又は完全に独立した記録・監査システムにコンピュータ・システムに対する全てのアクションを記録する等の措置を講じ，人的事故を防止するとともに，万一人的事故が発生した場合，効果的な対策を迅速に実施できるようにする。

ネットワークの保全

- 自軍の情報システムのネットワークにおけるメッセージ・データや信号は，敵の電子情報並びに通信情報活動の一環として全て傍受されている。従って，単に電子スペクトラムを解析しただけではそこに含まれている情報を解読できないように，全てのメッセージ・データや信号を高度に

暗号化する必要がある。

- 情報システムのネットワークも当然敵の C^3CM の主要な目標であり，傍受される以外に電子的妨害や物理的攻撃がなされるであろう。これらに対しても有効な対策を講じなければならない。

1.5 ＳＯＳを商用に適用する際の問題点

近年，コンピュータ・システムは広く社会に普及しており，コンピュータ・システムのエラーが社会の広範囲に影響を与える可能性がある。また，金や重要な情報のコンピュータ化が日常のものになったことから，コンピュータ・システムそのものが犯罪や悪用の対象となってきている。このため，民間で使用されているコンピュータ・システム（商用システム）においても，システムを安全なものとするためのセキュリティ機能は極めて重要であり，現行のシステムでも各種のセキュリティ対策が実施されている。

セキュア・オペレーティング・システム（ＳＯＳ）は，システム内のプログラムやデータなどに対する利用者からのアクセス可能範囲を制限するセキュリティ機能（アクセス制御機能）の高度化を目的としたオペレーティング・システム（ＯＳ）であり，米国においていくつか開発されつつある。しかし，既存ＳＯＳは軍用システムのモデルを実現する試行的なシステムであり，一部が実際に使用されていると言われてはいるが，性能的に妥当な段階に至っていないし，モデルが軍用システムをベースとしていることから特殊なものと考えられる。

商用システムでは，経済性が重視される。これはコンピュータ・システムに対しても例外ではない。また，一口に商用システムといっても，その利用形態は多様であり，組織ごとに要求するセキュリティ機能も異なる。商用システム向けコンピュータ・システムでは，この要求に応える必要がある。

以下に，既存ＳＯＳを商用システムに適用する場合の問題点を述べる。

(1) 軍用システムと商用システムとの違い

① コストより安全性を重視

商用システムでは経済性を重視するが，軍用システムでは損失の種類によっては金銭的な解決がつけられないことがあるため，常に最大限の安全策の実施が必要となる。

② 高度な人的管理

軍用システムの場合は，システムの利用者は軍の関係者だけであり，利用者に対する十分な人的管理が達成できる。しかし，商用システムの利用形態は多様であり，利用者の管理についても利用形態に依存する面があると予想される。

(2) ＳＯＳモデルの特徴

ＳＯＳモデルは上記の軍用システムをベースとしている。代表的なモデルとして，Bell－LaPadulaモデルがある。このモデルの特徴を以下に示す。

① マルチ・レベルのセキュリティ

アクセス制御の対象をクラス分けし，複数のセキュリティ・レベルを実現している。

② ＊性

クラス間の情報の流れを，機密情報が下位のクラスへ流れないよう制限する。

(3) ＳＯＳモデルの問題

モデル化により，現実の複雑なシステムの動きの理解が容易になる。モデルを形式的に厳密に記述できれば，セキュリティに関する要求を満足できるかの検証が可能となる。しかし，モデルの形式的検証に関しては，簡単なモデルの場合でも，その系が与えられたセキュリティ条件を満足していることを形式的に検証することは非常に困難だというのが現状であり，商用システムのセキュリティに，このレベルの完全性を期待することは現実的でない。また，単純化されたモデルと現実とのギャップの問題もある。セキュリティの実現に当たっては，これらのことを考慮する必要がある。

商用システムで使われているセキュリティ機構は，個々のリソースごとに，それにアクセス可能なユーザまたはユーザのグループを指定する方式が一般的である。これに対し，ＳＯＳモデルではリソースとユーザに機密レベルを設け，下位レベルへの情報の漏洩を禁止する。ＳＯＳモデルは商用システムのセキュリティ機構に比べて，よりシステムの利用者や管理者の自由裁量範囲を制限し

ており，それだけ組織全体のセキュリティ政策が徹底しやすい。しかし，制御機構が複雑化する分だけ，性能が低下する。商用システムにとっては大きな問題である。また，システムの運用形態によっては，ＳＯＳモデルのような制限が意味を持たない場合があり（例えば，扱う情報の機密レベルが１種類しか存在しない），商用システムとしては，このような複雑な制御機構の必要性に疑問がある。

ＳＯＳモデルの＊性は，紙をベースにした現行の軍の機密文書の管理よりも厳しい管理をコンピュータ内に限って実現しようとするものである。しかし，機密文書の管理がコンピュータ化された場合でも，文書を扱うのは最終的には人間であるから，機密の保持は人間に依存している。したがって，システム全体から見ると，コンピュータ内部での情報の流れだけを厳しく制限してもあまり意味がない。システム全体としてのセキュリティの強さは，人間に依存しており，コンピュータ内部で＊性が保たれることによってあまり改善されない[注]。システムにどのようなセキュリティ機能を持たせても，それでセキュリティが達成されるわけではない。セキュリティの実現状況の確認をしないと意味をなさない。

〔注〕＊性について

現状の紙をベースにした機密文書の管理は，ある機密文書に対するクリアランス（権限）をもつ人間は，その文書の内容をクリアランスを持たない人間に洩らさないことを前提にしている。機密文書の管理がコンピュータ化された場合も，文書を使うのは最終的には人間であるから，この事情は変わらない。人間をコンピュータ内の主体に文書を対象に置きかえると，上に述べたルールはちょうど＊性に対応する。ＳＯＳモデルは，主体が意図的に情報を洩らそうとした場合でも，セキュリティ・カーネルはこれを防ぎ，＊性を保証することを要求している。コンピュータ内では＊性の保証を要求し，コンピュータ外では人間に頼るのでは，機密保持に対する要求が一貫していない。コンピュータ内の主体が信用できないのであれば，それを作った（あるいは

操作している）人間も信用できないはずである。＊性により，コンピュータを使用した高速かつ多量の情報の漏洩は防止できるが，ディスプレイに表示された情報のメモなどは依然として可能である。

(4) 商用システムのセキュリティの特徴

以下に軍用システムと較べた場合の商用システムの特徴を述べる。

① 経済性の重視

軍用システムでは金銭的な補償の得られない損失を防止するため最大限の安全策が必要であり，コストを重視しないが，商用システムの場合にはコストと効果の得失でセキュリティ対策の開発コストがそれによって得られる効果と比べて妥当な値であることが要求される。セキュリティ対策によるシステム性能の低下についても同様である。

② 要求されるセキュリティが多様

軍用システムの場合は要求されるセキュリティはＳＯＳモデルに代表されると思われるが，民間のコンピュータ・システムは組織ごとにシステムの利用形態が様々であり，要求されるセキュリティも多種多様であり，ＳＯＳモデルのような複数レベル管理のみでは対応できないケースも多い。商用システムでは，これらの多様な要求のすべてに応える必要がある。以下に，商用システムのセキュリティを考えるに当り検討すべき項目を示す。

- 取り扱う情報の種類，機密レベルの差異
- システムに関係する人間の種類
- 必要とするセキュリティのレベル
- 保護すべき対象の種類，保護単位

③ その他

商用システムの場合は，単にセキュリティを実現するだけでなく，以下の点についても重視する必要がある。これらの項目は軍用システムの場合には軽視されている。

- 既存のユーザやメーカ資産の保証

・汎用性

・小規模～大規模システムにわたる一貫性

商用システムは，上述したように経済性と多種多様のユーザ・ニーズを考慮する必要がある。したがって，商用システムのセキュリティは，通常，以下の形態になると考えられる。

・特殊用途向けのハードウェアやソフトウェアはコスト面が問題となるので，商用システムでは標準的なハードウェアやソフトウェアがセキュリティ機構構築のベースとなる。

・目的別のシステムだけで必要とするような特別のセキュリティ機能についても実現可能とするため，商用システムにはそのベースとなるセキュリティ機能が要求される。

〔参考文献〕

〔1〕 Landwehr, C.E., " Formal Models for Computer Security," ACM Computing Surveys, Vol. 13, No. 3, pp. 247 - 278, (Sept. 1981).

1.6 ＳＯＳの要求機能とその実現

1.6.1 基本的な視点

コンピュータ・セキュリティ，すなわち，不当な者によるコンピュータ及び重要データへのアクセス保護は，充分な運用管理的な安全対策，技術的な安全対策，そして物理的（設備的）な安全対策が実施されることによって達成される。システム全体のセキュリティ保持を実施する上で，安全対策のある一部にしわ寄せがあると，コスト有効性（cost effectiveness）の面で少なからざる損失を招いたりすることになる。そして，この３者がバランスよく有機的に実行されなければ，すなわち，この３者の内，１つでも低いレベルの安全対策しか実施されないと，全体のセキュリティ・レベルはその最も低いレベル（weakest link）に陥ってしまうことになる。これを回避するためにも，この３者に対して均等な配慮を払うべきである。

ここでは，商用の汎用ＳＯＳ（あるいはコンピュータ・システム）に対するセキュリティ関連の要求機能のみについて，すなわち，主として技術的な安全対策を実施する上での要求機能についてのみ検討するが，技術的な安全対策が真に充分に効力を発揮しつづけるには，残りの２者が（運用管理的安全対策と物理的安全対策）が同等以上に完全に実施されていることが大前提となる。

本節では，まず，1.6.2ではＳＯＳで必須と考えられる要求機能を検討し，1.6.3ではその要求された機能を実現する際に考慮すべき実現手段について検討し，1.6.4ではＳＯＳを実現するソフトウェア及びハードウェアでの本質的な問題，主として品質保証と保守を取り上げ検討し，最後の1.6.5では実際にＳＯＳを運用していく際にぜひあってほしい機能等を検討する。

本節で要求されているセキュリティ機能の内，どの部分をハードウェアで分担実現すべきか，どの部分をソフトウェアで分担・実現すべきか，そして両者のインタフェースをどのようにすべきかは，性能，価格，セキュリティ強度，信頼性，インテグリティ，その時点での実現技術の成熟度等の諸般の点を勘案して決定されなければならない。

コンピュータ・システムのセキュリティ機能は追加／選択機能（add-on or optional）ではなく，組込み／標準機能（build-in or standard）でなければならない。このことは，問題が発生したら対症療法的に関連する部分のプログラムを修正・追加するのではなく，完全にセキュリティ侵害を防止するには，できるだけ早い開発段階，すなわち，要求仕様作成段階あるいはシステム設計段階からセキュリティ侵害防止を検討し，織り込まなければいけないことを意味している。

そして，ＳＯＳで提供されるセキュリティ機能は，善良なエンド・ユーザに対しては，できるだけ透明（transparent）で使用の妨げにならないように，優しく（friendly）なるように実現されていなければならない。

商用の汎用ＳＯＳは，性能面では，従来の軍用ＳＯＳの試作品（プロトタイプ）が，その基となった汎用ＯＳに比べ半分以下の性能低下に陥いってしまったが，セキュリティ強化がなされていない従来の汎用ＯＳに比べて数％程度の性能低下に留め，価格面でも妥当な範囲に実現することが必須の条件である。

商用の汎用ＳＯＳの要求機能を考える上で先ず最初にやるべき事項は，確固たるコンピュータ・セキュリティ・ポリシー．特にデータ保護ポリシーを確立し，それに則した形式的なセキュリティ・モデルを案出する必要がある。しかし，万人に，あるいは大多数の人に受け入れられるような商用向の汎用セキュリティ・ポリシーもないし，ましてそれを反映した形式的モデルもない。コンピュータ・セキュリティの形式的モデルの確立が緊急の課題である。

以上のような視点で本節が検討されており，以下での検討結果を表１－７と表１－８に示しておく。

表１－７を見る際に留意する点は要求度合である。要求度合ＢあるいはＣの機能はＳＯＳの完成後追加されるのではなく，その機能が必要であると決定された場合には，システム設計段階から考慮され，織り込まれていなければならない点である。

表１－７　ＳＯＳの要求機能の一覧表

ＳＯＳの要求機能	要求度合＊
(1) 本人確認機能	A
(2) アクセス制御機能	A
(3) プロセス隔離機能	A
(4) 使用済記録媒体白紙化機能	A
(5) ジャーナル／ログ機能	A
(6) セキュリティ管理者支援機能	A
(7) システム監査支援機能	B
(8) シャットダウン防止機能	B
(9) システム監査用の出口の常設	B
(10) リモート・プログラミング抑止機能	C

＊：要求度合

A：核となる機能で必須である。

B：周辺機能であるが，重要と考えられる。

C：場合によっては必要となる機能である。

表１－８　ＳＯＳの考慮事項の一覧表

	考　　慮　　事　　項
実現手段面	①　主　記　憶 ②　アドレス表現 ③　ＣＰＵの実行モード ④　汎用レジスタ ⑤　チャネル／ＤＭＡ ⑥　アクセス仲介機構 ⑦　ディシジョン・テーブル機構 ⑧　暗号化機構 ⑨　パトロール機構 ⑩　本人確認手段
品質保証・保守面	①　ソフトウェアの品質保証 ②　ＳＯＳの検定（侵入テスト） ③　環境シミュレータ ④　ソフトウェアの遠隔保守 ⑤　ハードウェアの遠隔保守
運用管理面	①　コンピュータ関連要員の資格区分支援機能 ②　開発と本番の隔離支援機能 ③　インストレーション作業の監査支援機能 ④　プログラム移管支援機能 ⑤　システム・ダウン後の復旧支援機能 ⑥　リモート・プログラミング監査支援機能

1.6.2 ＳＯＳの要求機能

コンピュータ・セキュリティの基本はアクセス制御とシステムのインテグリティである。そして提供されるセキュリティ機能が主としてセキュリティ侵害を未然に防止する点に主眼を置いた機能と，セキュリティ侵害が起きたことを事後に監査し，犯人追求を容易にする（責任体制（accountability）と呼ばれる）ことを主眼にした機能に分類することができる。

以下では，これらの観点からＳＯＳに対する要求機能を述べる。

(1) 本人確認機能

本人確認機能（End-user authentication）は，エンド・ユーザがコンピュータ・システムにアクセスした時に最初に作動するもので，アクセス制御の第１関門であり，確かなものが要求される。本人確認機能を強固・高度化する際には，善良なエンド・ユーザには煩わしくなく，安価で，運用も簡単であることが必須条件である。

(2) アクセス制御機能

アクセス制御機能は，本人確認機能によってコンピュータ・システムへのアクセスを許可されたユーザ（あるいはそのユーザによって起動されたプロセス）がコンピュータ資源，特にファイル（含データベース）やプログラム（業務プログラム，ユーティリティ・プログラム等）にアクセスする時に，そのユーザがその資源に対する正当と認められたユーザであるか審査し，審査に合格した場合のみ，アクセスを許可するものである。

ここで重要な問題は，審査手続き，すなわちアクセス制御のポリシーである。商用では，自由裁量のアクセス制御（discretional access control）がよいか，あるいは非自由裁量のアクセス制御（non-discretional access control），すなわち，強制的なアクセス制御（mandatory access control）がよいのか一概に言えぬが，今後は非自由裁量のアクセス制御を標準とすることが望ましいと考えられる。（商用向のアクセス制御のポリシーの研究も必要である。）非自由裁量のアクセス制御では，資源が創成されると同時にアクセス制御下に登録され，明示的にアクセス許可が登録されないかぎり，何人もその資源にアクセ

スできないようにする。

アクセス制御の対象の単位は，ファイルのような大きな単位ではなく，レコード中のデータ項目単位（granuarity level）とか，データ項目の内容に応じた述語ロック*（predicate lock）のようにきめのこまかいアクセス制御機能が要求される。

特定のファイルに対するアクセスは，特定のユーザに限定するのは勿論であるが，特定のプログラムとか特定の端末装置に限定するような機能もぜひ備えてほしい。特にファイル障害を回復する際には，すべてのアクセス制御が解除される危険性があるので，この機能は必須となろう。

(3) プロセス隔離機能

プロセス隔離機能（process isolation）は必須機能であり，完全（secure）なものが要求される。特にユーザ・プロセスから制御プログラム（ＯＳ）を完全に保護（protection）する必要がある。プロセス隔離機能の実現の核はハードウェアで提供されることになろう。

高度な侵害として，アクセス制御を出し抜いて，制御プログラムを経由してユーザ・プロセス間で機密データの通信を行うことが想定されるので，効率のよい仮想マシン（VM, Virtual Machine）を期待する。

(4) 使用済記憶媒体白紙化機能

ＯＳが，主記憶や補助記憶装置（ディスク，ドラム，磁気テープ等）をユーザ（プロセス）に新規に割り当てる際には，その記憶領域を白紙化（ゼロ／スペース・クリア）する機能が必須に要求される。

(5) ジャーナル／ログ機能

ジャーナル／ログ機能は，セキュリティ侵害等に対する事後処理の基礎データを提供するものであり，システム監査や責任追求（accountability）が充分に行えるような必要十分な，例えばレコード・レベルでの監査証跡（audit trail）を収集するものが必須機能として要求される。

＊：アクセス許可の条件を述語式で記述する。

そして，オンライン・アプリケーション・プログラムに対するジャーナル／ログ機能もＯＳで提供されることを期待する。

(6) セキュリティ管理者支援機能

今日までのＯＳでは，セキュリティ管理者（security administrator）の管理作業を容易にする機能が不足しており，充実が要求される。

システム監査は主として事後監査に主眼を置いているのに対し，セキュリティ管理者はセキュリティ侵害を監視するのが任務である。そのため，セキュリティ管理者支援機能では，稼動中のセキュリティ監視に主眼を置いている。セキュリティ管理者支援機能としては，セキュリティ管理者がオンライン・リアルタイムにセキュリティ関連記録（主記憶上と外部記憶上の両方）にアクセスし，セキュリティ侵害に対して迅速なアクションが取れるような支援機能が要求される。

そして，事前でのアクセス制御情報（例えば，ユーザ・プロフィール）などのセキュリティ管理情報の登録，維持，末消などの操作がセキュリティ管理者に限定され，かつ簡易であることを期待する。

(7) システム監査支援機能

システム監査の実施を妨げている要因の１つは，ファイル内容を監査する際に使用する使いやすい高機能のその道の専門家（コンピュータ技術者ではなく，監査（検査）部門の専任者という意味）向の言語の欠如にある。システム監査を容易にするシステム監査言語及び支援システムが要求される。

ＳＯＳの立場でシステム監査をとらえると，システム監査者はオールマイティとなりやすく，システムに蓄積されているすべてのデータにアクセス可能になってしまうので，ある種の歯止めが必要となる。歯止めの一つの手段としてシステム監査言語（あるいはコマンド）で記述されたプログラムでしか有効とならず，他の言語（例えばアセンブラ言語）で記述されたプログラムでは拒否されるようにすることも考えられよう。

(8) シャットダウン防止機能

予定されたシステムの立上げ（start-up）やシャットダウン（shutdown）以

外は，不当な，あるいは不注意によるシステム・シャットダウンや再開（restart）を防止する機能が要求される。

(9) システム監査用の出口の常設

重要なデータを扱うＯＳ，DBMS，ユーティリティ・プログラム，適用業務プログラム（パッケージ）には，システム監査を容易にするために，システム監査用の出口（exit）を備えていることが要求される。その際に，組み込まれる監査用プログラムはシステム監査用言語で記述できることが望ましい。

(10) リモート・プログラミング抑止機能

末端のアプリケーション・ユーザには，業務用（共用）の提供されたプログラム及びデータベースのみの使用に限定させること。共用のデータベースにアクセスするプログラムは特定の担当者だけが作成でき，一般のエンド・ユーザには作成できないようにするプログラミング抑止機能が要求される。

1.6.3 ＳＯＳの実現手段

本項では，高性能なＳＯＳを構築する際に有用と考えられる実現手段，主としてハードウェア機構（アーキテクチャ）について述べる。

ＳＯＳに要求されるセキュリティ機能の一部をハードウェアで分担・実現する際のハードウェア化を決定する場合の判断基準は，コスト・パフォーマンスであることは言うまでもないが，ハードウェア化することによってどの程度インテグリティが向上するか，ソフトウェアできめのこまかいアクセス制御機能を実現した際に過大なオーバヘッドが発生すると考えられる機能か，その機能がハードウェア化に適した規模かどうか，という点になろう。

(1) 主　記　憶

① ＯＳ等の重要なプログラムはＲＯＭ（read-only memory）化またはファームウェア化を考慮すること。

② ＯＳはユーザ空間とは物理的あるいは仮想的に別に（分離）し，専用領域とし，ユーザ空間からはアドレサブルでなくすること。

③ 主記憶領域に記憶されているものが命令なのか，データなのかのタグ等を

保持する手段を導入して，命令を書き換えられないようにすること。特にチャネルに対してもこの保護が適用されること。

(2) アドレス表現

他のプロセスに対して不正な変更や干渉をできなくするために，主記憶の参照の際のアドレス表現として，従来から採用されている数値番地ではなく，記号番地を採用すべきか否かを種々の観点から検討すること。

(3) ＣＰＵの実行モード

従来のＣＰＵの実行モード（execution state of processor ）は，スーパバイザ・モード（あるいはマスタ・モード）とユーザ・モードの２レベルであるが，３レベル以上（例えば，カーネル・モード，スーパバイザ・モード，ユーザ・モード）の実行モードが要求される。

そして実行モードによって実行可能な命令セットを限定するだけではなく，特権プロフィール（priviledge profill：そのプロセスが実行可能な特権命令のリストが入っている）によって実行可能な命令か否かを決定するような，柔軟な機構も期待される。

(4) 汎用レジスタ

実行モードを切り換えたり，タスクを切り換える際には，汎用レジスタの切換え（context switching）が必要であるので，汎用レジスタの数が多い場合には切換えのオーバヘッド時間が増加し，性能低下の要因となる。

半導体集積回路技術，特にメモリに関しては大容量化が進展するので，実行モード毎あるいはプロセス毎に独立した専用のレジスタ・セットを用意すべきである。

(5) チャネル／ＤＭＡ

ＣＰＵについてはセキュリティ面の配慮が充分に行き届いているのに，チャネルやＤＭＡ（Direct Memory Access ）に対する配慮がなされていないのが多々ある。高度な侵入手段としてチャネルの欠陥を活用した事例もあるので，チャネル及びＤＭＡに対してもＣＰＵと同等程度のアクセス制御機構が内蔵されることを期待する。

(6) アクセス仲介機構

きめのこまかいアクセス制御をソフトウェアで実現しようとするとオーバヘッドが増大するので，ハードウェアとして精巧なアクセス仲介機構（access mediation mechanism）が要求される。

ＨＩＳ社のSCOMP（Secure Communications Processor）やＩＢＭ社のＳ/38 は基本的なセキュリティ・ハードウェア機構を実現しているが，更に高度なセキュリティ機構を期待する。

(7) ディシジョン・テーブル機構

不正なアクセスを未然に防止するためには，高度な判断機構が要求される。一般に，正当なアクセスか不正なアクセスかを決定するには，複雑な多数の組合せ条件を検査しなければならず，プログラム・ロジックが複雑となると同時に，実行オーバヘッドが多大になってしまう。プログラムの判断ロジックの作成を不要にし，オーバヘッドを軽減するために，例えばディシジョン・テーブルを直接実行するようなハードウェア機構が要求される。

(8) 暗号化機構

重要なデータに対する保護手段として暗号の重要性が増すことが想定され，ソフトウェアで暗号化処理を行うとオーバヘッドが増大するので，ハードウェアで暗号化機構を用意すべきである。

暗号器のように暗号化機構を外付けするのではなく，ＣＰＵの命令，すなわち暗号化命令を標準命令として用意すべきである。

(9) パトロール機構

ハードウェア及びソフトウェアのインテグリティを保証するため，周期的あるいは常時パトロート（patrol）が行われる必要がある。パトロール機構はハードウェアとソフトウェアの複合体として実現されるが，オーバヘッドを軽減するために，可能な限りハードウェア化されることを期待したい。

(10) 本人確認手段

本人確認手段として従来からよく採用されているパスワードは今後とも簡易な手段としてよく使用されると想定されるか，パスワードをユーザ自身で登録

できるようにしたり，簡単に頻繁に変更できるようにする等の機能が用意されることを期待したい。

本人を確認する手段としてカードを使用することも銀行システム等でよく導入されているが，偽造しにくいものを期待したい。偽造しにくいカードとしてホログラフィ・カードが最近使用され出しており，安価になることを期待したい。そして最近の目覚しい半導体集積回路技術の進展の成果として，超薄型のＩＣ（Integrated Circuit）カードも出現しており，処理・記憶能力を内蔵したこのＩＣカードの適用分野，用途，運用法の実用研究が進展することを期待する。

偽造が不可能な本人の身体的特徴を利用した指紋，声紋，手型，サインによる本人確認技術も今後おおいに期待できるが，安価であることは勿論ではあるが，正真正銘の本人であるのに，例えばカゼのように各種の一時的な身体的条件変化のために，本人であると確認できず，アクセスを拒否される場合が起るので，そのような事態にできるだけ陥らないような技術的完成度を期待したい。

1.6.4　品質保証・保守の問題

ここでは，ソフトウェア及びハードウェアに対する前提条件を述べる。

ソフトウェアの品質保証は，ソフトウェア工学の主要な目的であり，緊急の最重要課題である。保守に関しては，保守そのものの問題も大きいが，ここではセキュリティ面から検討する。

(1)　ソフトウェアの品質保証

ソフトウェアは，他の工業製品（product）と同様に品質及びインテグリティを保証すべきである。静的な品質を保証するだけでなく，動的なインテグリティをも保証すべきである。静的な品質保証とは，他の条件（環境）が正常であると仮定した場合にソフトウェアが正しく動作することを保証することをいう。一方，動的なインテグリティ保証とは，例えばハードウェアのある一部が故障してもソフトウェアのインテグリティが保証されていることをいう。

ソフトウェアに対する静的な品質保証すら，現在満足のいく状態に達してい

ないのが現状であり，緊急の課題である。

一方，ソフトウェアに対する動的なインテグリティ保証では，ソフトウェア自体（自分自身）の誤りに対しても対処できるような機能を備える，特にＯＳの出力ルーチン（exit routine）にセンター独自のルーチンの組込みを許している場合には特にこの機能が重要となる。

(2) ＳＯＳの検定（侵入テスト）

ＳＯＳが正しく作成されていることが必須の前提条件ではあるが，ＳＯＳが正しいからといって，セキュリティの観点から見て，強固であることを保証されているわけではない。

ＳＯＳの実際面でのセキュリティを保証するために，第三者による侵入テスト（penetration test）を義務付けることが要求される。

これと同様なことがアプリケーション・プログラムに対しても要求されるであろう。

(3) 環境シミュレータ

ソフトウェア・システムが大規模・複雑化して，完全なテストが困難となってきている。このような状況に対処するため，使用を想定しているコンピュータ構成（特に端末装置が重要）をできる限り擬似したシステムを実現する環境シミュレータが要求される。

環境シミュレータとしては，想定コンピュータ構成に近い柔軟な構成を実現可能とするだけでなく，機器障害を発生させたり，多数の端末から同時にトランザクションを発生させたりする，現実の環境では作り出すのが困難な過酷なテスト条件や，なまの環境ではテストができない（例えば，核反応制御プログラム，宇宙システム，防空システム）ような機能を提供することが要求される。

(4) ソフトウェアの遠隔保守

ソフトウェアに関して厳格な品質保証をやっても，１００％の完全性を期待できないので，保守作業が不可欠である。

ソフトウェアの場合もハードウェアと同様に，遠隔保守機能（remote maintenance）が要求される。遠隔保守は，システムの障害が発生した際に，遠隔

地にある保守サイトからハードウェア及びソフトウェアを一体にしたシステムの障害を検出し，切分けを行う方式である。システムが高度・複雑化しており，特にソフトウェアの大規模・複雑化に対処して保守を行うためには，高度な知識を備えた人材を，多数必要とするが，その様な人材が不足しているのが現状である。ハードウェアと同様にソフトウェアに対する遠隔保守でも，今までに発生したソフトウェア障害を一元管理し，同種の障害に対しては迅速な対応がとれるようにすることが今後増々重要となってくる。そのためには，トータル・システムに対する遠隔診断機能と，ソフトウェアの障害原因に対する修正情報伝達機能，障害情報検索機能といった諸機能が要求される。

(5) ハードウェアの遠隔保守

ハードウェア保守の複雑化・高度化に対処するため，遠隔保守機能が高度化することが必然であり，要求される。その際にセキュリティ面での配慮がなされていなければならない。

そして，異なるメーカの機器を相互に接続したコンピュータ・システム，コンピュータ・ネットワークが普通となってくるので，メーカ間での保守に関する取り決め，また第3の保守専門会社による保守作業の際のセキュリティ保持が増々重要となってくるので，その対策も要求される。

1.6.5 運用管理面での考慮事項

コンピュータ・セキュリティ保持のために事前に準備された技術的及び物理的安全対策を生すも殺すも運用管理しだいであるといっても過言ではない。そのためには，運用管理を円滑に行う支援機能が充実していることが望ましい。

以下では，運用管理を円滑に行うためにＳＯＳに要求される支援機能について述べる。

(1) コンピュータ関連要員の資格区分支援機能

コンピュータに関連する要員（あるいは部門）を，例えば，

- アプリケーション・プログラムのユーザ
- アプリケーション・プログラムの開発者

・システム・プログラマ

・システム総括者(System Control Population)

・システム管理者(System Management Population)

・システム監査者(System Audit Population)

・システム修復者(System Repair Population)

の7段階の職務分担に分離でき，それぞれの職務分担に応じてコンピュータが使用できるような運用管理支援機能が要求される。

(2) 開発と本番の隔離支援機能

アプリケーション・プログラムの開発者は，テスト用の環境下で開発作業及びテスト作業を行い，プロダクション(本番)用のプログラム(ソース形式とオブジェクト形式)及びデータベースにはアクセスできないようにすること。もしアクセスしたい場合には，開発者は特別な処理過程を得てプロダクション用のプログラム及びデータベースを複写しなければならないようにし，かつ複写作業をできるようにすること。これらの点の運用管理を支援する機能が要求される。

(3) インストレーション作業の監査支援機能

システム・プログラマが行うインストレーション作業を規制し，監査可能にする支援機能が要求される。

(4) プログラム移管支援機能

開発され検査済のプログラムを開発部門から運用部門へ移行する際に厳重な管理を支援する機能が要求される。

(5) システム・ダウン後の復旧支援機能

システム・ダウンが発生すると，通常システムを迅速に復旧させるため，場合によって，すべてのセキュリティ機構を無効にできるようにしている。しかし，システム・ダウンが発生したからといって，無防備で良いということにはならない。必要最少限のセキュリティ機能はいかなる場合でも機能し続けることが要求される。必要最少限のセキュリティ機能としては，事後の最低限のシステム監査が実施可能となるような復旧作業の経過を記録するログ機能である。

(6) リモート・プログラム監査支援機能

分散プロセッサ（あるいはインテリジェント端末）へのダウン・ライン・ローディング機能は勿論であるが，稼動中の分散プロセッサに格納されているプログラムを吸い上げて，ホスト側に蓄積されているオリジナル・プログラムと照合し，不正な変更（あるいは障害）によってプログラムが改変されていないかを検査するシステム監査支援機能が要求される。

1.7　SOSの開発に向けて

コンピュータのハードウェアは過去のすべてのインフレ圧力に逆行して，つねに同一価格を維持しながらより高い性能を実現してきた。

このことは，他の産業製品からみると魔法ともいえる驚異的現象である。魔法には必ずタネがあるもので，それがＬＳＩ（高密度集積回路）技術であることはよく知られている。しかし，じつは隠れたもう１つのタネがある。それはソフトウェア開発の人件費を抑えていることである。旧機種のソフトウェアをそのまま引き継いでいけば，メモリが大きくなったり演算速度が速くなった分だけ，性能が向上することは明白である。ソフトウェアは本質的に手作業を必要とする，純粋に人件費のみを消費する部分であるから，これにできるだけ手をかけないほうが安上がりになり，次々に安く新製品を市場に送り出すことができた。

ところがこの製品開発法にもかげりが出てきた。コンピュータを１台ずつ独立で使用しているうちはそれでもよかったが，コンピュータ同士を結合し，コンピュータ・ネットワークとしてより高度な情報処理をやらせようとすると，飛躍的に複雑なネットワークを開発しなければならなくなる。今の時代に最も高いものは人件費であることは常識であるから，コンピュータ価格の魔法もネットワーク社会となる近い将来に破れてしまうことは確実である。

日米の情報産業の競争を自動車レースにたとえてみれば，ハードウェアはクルマ，ソフトウェアはドライバーである。今まではほとんどが直線でできているサーキットを走るレースだったので，クルマの馬力を上げていくだけでよかった。しかし，コンピュータに複雑な情報処理が要求されるということは，サーキットがカーブやヘアピンの多い難しいものになったことに相当する。このレースに勝つためには，クルマの性能もさることながら，優秀なドライバーを育成しなければならないのは当然である。もし高性能のクルマがあっても，腕の悪いドライバーでは勝ち目はない。

この例からも分かるように，日本のコンピュータは，ソフトウェアでは遅れているがハードウェアではアメリカを抜いている，という説は何の意味もない。ソ

フトウェアの悪いコンピュータはコンピュータとして認められないのである。ハードウェアが悪くても，ソフトウェアの良いコンピュータは我々の期待に応える働きをしてくれる。アメリカのコンピュータ産業は早くからこれに気付き，彼らの戦略はハードウェアからソフトウェアにその重点を移行しつつある。

過去の日本政府の国内産業政策は官民一体の日本株式会社と批判を浴びたが，アメリカ政府はいま，国防省を通してコンピュータ・セキュリティ開発の名目で，自国の情報産業に多額の援助を与え，国防上の理由を盾に外国情報産業をそこから締め出している。また1982年の夏に発生したIBM産業スパイ事件にもアメリカ政府とコンピュータ産業が官民一体となって，日本のコンピュータ産業に対抗していく姿勢が見えるという解釈もある。

８０年代に入って，日本の半導体産業はついにアメリカを製造技術で完全に追い抜いてしまった。この追い上げのパターンは自動車産業と似ており，半導体産業もアメリカの模倣から始まった。この半導体技術の逆転をアメリカは深刻に受け止め，コンピュータ産業全体が自動車産業の“二の舞い”にならぬよう必死の反撃を試みている。

最近になってソフトウェア危機が呼ばれている。このままコンピュータ化が社会の各所で進められていくと，２１世紀に入る前に地球の総人口が全てコンピュータ・プログラマになってもソフトウェア需要を支えきれなくなってくるという予想がそれである。ハードウェアは自動車のような工業生産品と同じように自動化大量生産しやすい。しかし，ソフトウェアは今のところ本質的に手作りに頼る部分が大きい。たとえば日本のソフトウェア会社のほとんどは，２年先の分まで受注しており，新たな受注は断っているのが現状で，そこで働いているプログラマたちは，最低でも毎月５０時間以上の残業を強いられている現状である。

セキュリティＯＳの開発は，コンピュータ・セキュリティの基本レベルの向上という本来の目的と同時に，このようなソフトウェア産業に対して技術的ブレークスルーをもたらすものである。ソフトウェア産業が必要としているものは，ソフトウェアの品質と生産性を画期的に向上させる技術である。それを目標とする学問がソフトウェア工学であり，その根本命題は，ソフトウェアを仕様書通り，

それ以上でも以下でもなく正しく完成することである。セキュリティＯＳはまさしくこの命題を追求し実現しようとしている。この実現には，我々人間の言葉で記述したソフトウェアに対する要求を，自動的に数学的に矛盾のない仕様へと変換し，さらにその仕様をプログラムへと展開していく技術が含まれている。この技術が完成すれば，アメリカの世界の情報産業における主導権は揺るがぬものとなる。最終的に国防省，つまりアメリカ政府の目指しているのは，来るべきソフトウェア危機とネットワーク社会に対する先行技術開発なのである。

日米経済戦争の第１ラウンドは日本の自動車産業の勝利で終わった。第２ラウンドの情報産業にかけるアメリカの意気込みは極めて大きい。このことは，太平洋戦争における日本の緒戦の勝利と，その後のアメリカの反攻を思い出させる。

“勝ってカブトの緒を締めよ”ということわざがあるが，現在進行している経済戦争ではどうだろうか。

今，日本の情報産業の話題は第５世代コンピュータやニューメディアで，ソフトウェアの品質と生産性の貧困から生ずるソフトウェア危機については，政府も本腰を入れて対策を立てようとしていない。今までの先端技術は，ほとんどライセンスやパテントを買うことにより導入できたが，自動車と半導体で痛い目に会ったアメリカは，コンピュータ・セキュリティで開発したソフトウェア技術を日本に提供するようなことは２度としないであろう。

経済戦争の勝敗もさることながら，日本の情報化社会がアメリカのソフトウェアなしには動かないというようなことが起こらないために，ソフトウェアの基礎研究を直ぐに始める必要がある。

2. 応用システムのセキュリティ

当プロジェクトの今年度（昭和58年度）の主たる目的は，昨年度（昭和57年度）に提案した「セキュリティ基本技術」（本章ではセキュリティ要素技術と呼ぶ）を組合せ，新しいセキュリティ機構を構築することである。本章では，個別の応用システムのセキュリティ機構を目標にした，システム化の検討結果を述べる。コンピュータ・ネットワークへの応用を目標にした検討結果は，第3章を参照されたい。

さて，応用システムのセキュリティ対策としては，①不正や犯罪を未然に防止する対策（事前防止対策）と，②たとえ不正や犯罪を起しても，必ず発見し得るという，抑止効果を狙う対策（事後チェック）の2つの流れがある。近年，②の対策は，消極的抑止効果だけでなく，①へフィードバックすることにより，結果的に，積極的な事前防止対策になるという認識が高まり，非常に重要視されるようになってきた。事後チェックは，従来，システム監査の一環として行われてきたため，システム監査の重要性を高める要因にもなっている。

このような状況と様々な理由で，我々は，昨年度提案のセキュリティ要素技術の統合化の目標として，システム監査の道具である，システム監査支援ツールを選択した。以下に，今年度の検討結果を，その背景から順に述べる。

2.1 概　　要

2.1.1 検討経過

昨年度（昭和57年度）の検討経過を説明することから始める。当プロジェクトは，続発するコンピュータ犯罪の防止を目的として，昨年度から，コンピュータ・システムのセキュリティについて，検討を開始した。昨年度は，その時点で把握されていた犯罪を未然に防止する方法（事前防止対策）を，技術的に実現する手段の検討が主な目的であった。

そこで，事前防止対策の幅広い可能性を探るべく，公共性が高くセキュリティ対策が重要だと思われる代表的応用システム

① 金融業のシステム（バンキング・システム）

② 情報処理業のシステム

③ 自治体のシステム

をとりあげ，設備面／技術面／運用面等広範囲に対策手法を検討した。その結果を簡単にまとめると次のようになる。

① 設備面での対策（例えば，通商産業省の「電子計算機システム安全対策基準」で示される対策）は，かなり有効である。

② 技術的対策の手法は多数存在するが，実際に使える技術は少ない。例えば，本人確認方式は各種あるが，実用性を考慮すれば，結局パスワード・システムを用いることに帰着する。しかも，この方式には，欠点が多い。

③ 運用による対策もかなり有効であるが，信頼できる“人”が必要である。また省力化とは相容れない要素がある。

④ 検討対象としたシステムでは，いづれも現時点で可能な設備，技術，運用対策が実施されており，セキュリティ・レベルを更に上げるには，画期的な技術／手法を開発するか，堪え難いコストが必要になる。

上記①～④は，事前防止対策に関する結論である。これらの対策の総合的効果として，現時点で必要にして十分なセキュリティ・レベルが達成されているかどうかについては，意見が分れる。一方は，現実に応用システムは順調に稼動して

いるので十分だとする意見であり，もう一方は，現実に犯罪が発生している以上，不十分であるという意見である。十分かどうかの議論はともかくとして，当プロジェクトは，セキュリティ対策をさらに強化するために技術面で何を開発すべきかを，昨年度提案した。

これらの提案は，早期に実現されることを望むが，これですべてが解決するわけではない。これまでの経験ではっきりしているように，新しい手法／技術ができると同時に，新しい問題が必ず発生するからである。さらに，洩れのない（完全な）事前防止対策を行うことは，非常に難しいとも言われる。従って，補完処置としての事後チェックが必要になる。すなわち，応用システムのセキュリティは，事前防止対策と事後のチェックにより，完全になるということができる。

我々は，昨年度の検討を終えた時点で，事前防止対策に引き続き，事後チェックについて調査研究すべきことを，強く認識した。その結果，今年度（昭和58年度）の調査研究開始にあたり，「事後チェック」を有力な調査研究テーマの一つとしてとりあげることとした。

2.1.2　今年度の作業方針

応用システムの事後チェックは，いわばシステム監査の分野である。

そこで，システム監査とセキュリティ要素技術との関係について考えてみる。システム監査者にとって興味があるのは，要素技術の機能とか応用システム内での有効性であるから，要素技術を監視する立場にあり，要素技術の支援を受ける立場ではない。しかし，これはセキュリティ要素技術が事前防止に使用された場合である。もし，事後のチェック用に使用された場合は，システム監査者は，支援を受ける立場に移行する。この場合，システム監査支援ツールと呼ばれる。この支援ツールは，直接的に（積極的に）不正等の防止を行うものではないので，間接的セキュリティ技術ということができる。

当テーマの目標は，本章の冒頭で述べたように，セキュリティ要素技術を組合わせて，有効なシステム監査支援ツールを組立てることである。我々は，次の手

順で作業を進めることとした。最初に，システム監査そのものの分析と現状調査を行う。次に，既に実用化されているシステム監査ツールを調査し，システム監査の問題点および現状ツールの問題点を研究し，さらに両者の相関について検討する。これらの結果を踏まえて，新しいツールを構築することとした。

システム監査の分析では，標準的なシステム監査実施手順の把握に重点を置いた。その結果を考慮して最大公約数的な実施手順を検討し，そこで有効な支援ツールを検討するためである。以下に，今年度の検討課題を示す。

① システム監査の最大公約数的実施手順の把握

② 既に実用化しているツールを適用する場合の問題点

③ 新しいシステム監査支援ツールの構築

2.1.3 今年度の作業内容

(1) システム監査の分析

作業の第一歩として，現状におけるシステム監査像をとらえるべく，システム監査の定義／目的および具体的な実施方法について調査した。

現状におけるシステム監査は，実に広範囲に解釈されており，標準的システム監査を，模索している状態といえる。個人によりあるいは立場の違いにより，システム監査として，会計監査，システムの信頼性，犯罪の発見あるいは運用状況のチェック等が連想され，品質管理という解釈もある。加えて，これらがすべてシステム監査の領域と呼べることは，例えば，当協会で昭和55年3月に提案した「システム監査基準（試案）」[*1]を見れば明らかである。

しかし，システム監査の解釈の違いがこれだけあれば，当然の結果として実施方法も千差万別になる。すなわち，人手による地道な作業による方法，コンピュータを駆使する方法，システム構築時のチェックを主とする方法，あるいは規定どおりの運用が為されているかをチェックする方法等である。第2.2節～第2.4節で，立場の違いによる解釈の違いを読み取っていただければ幸いで

＊1：「システム監査実施への道標，昭和55年3月 財団法人 日本情報処理開発協会」を参照

ある。

以上のように，システム監査の目標／実施方法等が混乱していることもあって，我国ではシステム監査の検討はしているものの実施が見送られている企業が大半を占める。従って，最優先課題は，手段の充実ではなくて，むしろシステム監査制度の整備である，と言えなくもない。これについては，現在，通商産業省を中心とした政府機関で検討が進められており，その結果を期待することとしたい。しかしながら，手段が整備されていなければ，法制度の有無にかかわらずシステム監査の実施は困難であり，実施の前提条件として，その土台を検討することは重要であると考える。

(2) 短期の課題

当プロジェクトでは，最大公約数的なシステム監査の実施手順を検討し，その結果，業務処理の各種記録は，システム監査用資料の共通の原典の一つであり，システム監査支援ツールの最も重要な入力データであることを確認できた。コンピュータ・システムでは，業務処理の各種記録が，磁気記録であるために生じている問題がかなりある。昨年度の報告書でも検索時の問題について言及している。[*1] 本テーマではその記録段階（ロギング）の問題を緊急に解決すべき問題（短期の課題）として重点的に検討することにした。

ロギングそのものに，特に困難な技術的問題はないというのは，従来の常識であるが，これはデータ量がそれ程多くない場合に成り立つ。データ量が増大すると，ファイルのボリューム，処理効率，データの保全性および運用面で歪が発生する。近年の大規模システムでは，従来の手法の限界に近づいており，今後のシステム拡張の際の大きなネックになると思われる。また，ログ・データは，その性質上，有効な保護対策を講ずることが難しいという大きな問題がある。

本テーマでは，これらの問題に対して，ログ専用の装置（ハードウェア）を付加することによる解決策を検討した。最近のハードウェア技術の進歩を生

＊1：「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 財団法人日本情報処理開発協会」第2部第3.9.5項を参照。

かして，ソフトウェア工数の逓減と，負荷分散による効率向上を狙った。同時に，ログ・データの保護強化，検索手段の強化も期待した。こうして，ロギング・サブシステム等が導き出された。詳細は，第2.5.2項で説明するが，ロギング・サブシステムは，

○　ログ・データを保護する

○　きめの細いデータを記録する

ことによって，極めて有用なデータをシステム監査者に提供することを可能とすると共に，システム効率の改善も可能とする。さらに，ロギング・サブシステムは，後述するより進化したシステム監査支援ツールの入力部分を構成する基本システムでもある。技術的には，2～3年で充分実現可能であり，我々は，短期の開発テーマとして最適であると考えた。

(3)　長期的な課題

システム監査を実施する場合の作業手順を大まかに言えば，資料を収集し，その資料を用いて適切な判断を行い，その結果を報告あるいは勧告するということになる。実際に市販されているツールとしては，資料収集に用いるツールが大部分であり，「判断」の段階で有効なツールが極めて少いことが分る。前述のロギング・サブシステムも，資料収集に用いるツールであり，ひらたく言えば，市販のツールの改良である。「判断」は，人間の作業領域という観念があるという理由もあるが，実は現在のコンピュータの判断機能が幼稚で，「判断」の領域に応用するのが困難であるというのが，最大の理由である。

ある意味では，ノイマン型コンピュータが壁に突き当っているとも言える。これを打開するために，根本的原理が違う新型のコンピュータを用いる方法がある。その一つとして，知識工学の応用がある。詳細は，第2.5.3項で述べるが，特に，コンサルテーション・システムは，「判断」という作業の助言者として期待できる。ただし，知識工学の活用は始まったばかりであり，システム監査用ツールとして実用化するためには，長い年月に渡る研究が必要だと思われるが，その価値は充分あることを敢えて付け加えておく。

2.2　システム監査の分析

2.2.1　システム監査の目的

近年，システム監査の必要性が強く認識されるにいたった背景には，コンピュータとそれを利用したシステムの急速な発展がある（図２－１参照）。

すなわち，①システムのトータル化（部門別システムから全体システムへ），②システムの利用拡大によるデータ量の増加，③システムのオンライン化と異企業間のネットワーク化，④アプリケーション・システムの高度化（取引データ処理から，シミュレーション・システムへ）等により，システムが企業及び社会に深く入り込み重要な役割を負うようになっている。システムの利用の拡大は，非常に大きな便益を利用者にもたらしているが，逆に，システムの大規模化にともない，システムに問題があった場合（システム・ダウン，コンピュータ犯罪，システム設計・導入ミス，通信回線不通，データ破壊等）の，システムの利用者に与える危険と損害の大きさも増している。また現に，これらシステムに関する問題点が発生している。

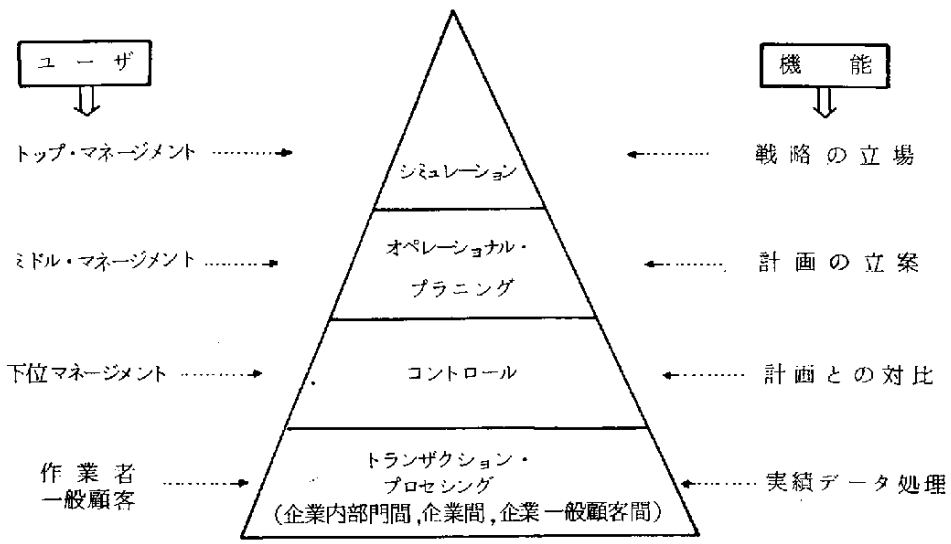


図２－１　システムの発展 － ４つのレベル

このような背景を踏まえて，産構審の答申の中で述べられているように，システムの安全性，信頼性，効率性を高めるというのが，システム監査の目的として一般的に受け入れられているといえるだろう。これら３つの目的の中で，安全性と信頼性については，それらを達成するための手法，及び達成されているか否かをチェックするためのチェック項目を想定してみると，相互にかなり似かよっており，両者は完全にはオーバラップしないけれども，コインの裏表という関係にあるといえよう。

それに対して効率性とは，システム開発の生産性，データのＥＤＰ処理の効率性，及びシステムのトップマネージメントを含めたユーザにとっての有効性の３つを含み，安全性・信頼性とは，かなり範疇の異なる目的といえる。

システム監査を定義づける時（すなわち目的・範囲・対象・実施体制等），基本的には，システム監査とは，上記の３つの目的を達成することに最終的に責任を持ち，それにより利益を受る者が，専門家としての第三者に，システム自体（広く，ハード，ソフト，運用体制も含めて）をレビューさせ，評価させ，報告させることである。従って，システム監査はかなり広く定義されうるため，具体的にシステム監査を実施するに当っては，個々の状況により色々なシステム監査の型がありうるが，ごく大まかに分類すると，次の２つに分けられる。

① システムの安全性・信頼性に重点を置いたシステム監査

公共性の強いシステム，すなわち不特定多数のユーザの情報を扱う，銀行・ガス・電力等のユーティリティ産業・クレジット会社・電算センタ及びデータ通信会社等のシステムが対象となる。

② システムの効率性に重点を置いたシステム監査

限定されたユーザを持つシステム，例えば，生産管理・販売管理・情報検索・人事管理等のシステムは，システム監査を行うとすれば効率的に重点を置かれる場合が現在のところ多い。但し，公共性の強いシステムでも，大量のデータを扱う関係上，効率性に重点を置いた監査も対象として重要である。

以下，本節は，安全性・信頼性に重点を置いたシステム監査を中心に述べる。

2.2.2　システム監査の範囲

システム監査の範囲は，広義にはシステムのマネージメント・サイクルの全過程を含めるべきである。図２－２に示すように，PLAN・DO・SEE・CONTROLの全過程が監査の対象となる。すなわち，

①　組織体制及び運営方針

情報処理に関する方針や，情報処理部門の組織体制が明確に定義され，安全かつ効果的に運用されているかという点について調査，評価する。

②　システム化計画

長期システム化計画がユーザ部門の参加によって立案され，費用・効果分析，開発優先順位等の検討がなされているか，コントロール・セキュリティを維持するための基本的な手段が検討されているか，そしてそれらは，最終的に経営者の承認を得ているかという点について調査する。

③　システム開発

開発中のシステムは，本当にユーザのニーズに合っているのか，開発の標準化は考慮されているか，生産性向上のための配慮がなされているか，コントロール・セキュリティのための仕組みがシステムの中に織り込まれているか，システムのテストは十分に行われているか，開発プロジェクトに対する進捗チェックがきちんとなされているか等の，システム開発に関係する有効性，システムの正確性，及びコントロール・セキュリティに対する配慮について分析評価する。

④　稼動中システムのサポート

稼動中システムのパフォーマンスの測定，システムの正確性及びユーザにとっての有効性のチェック，システム機能変更の際の生産性や信頼性を確保するための考慮がなされているか等，現行システムのサポート体制について監査する。

⑤　オペレーション管理

ハードウェアの効率的利用，オペレーション・スケジュール等の管理体制について監査する。

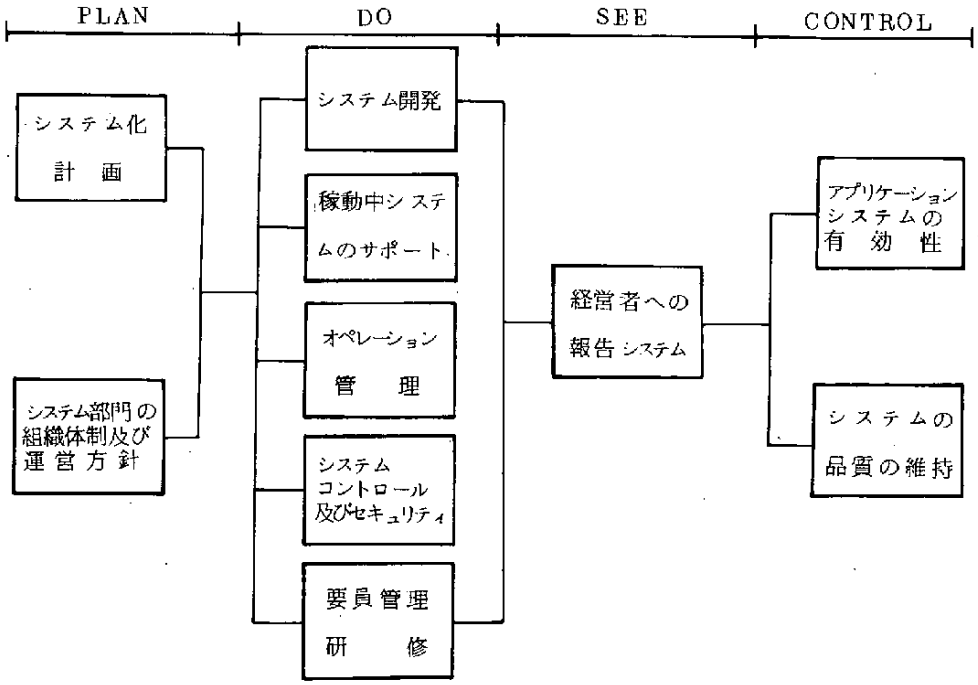


図２－２　システム監査の範囲

⑥　システム・コントロール及びセキュリティ

ハードウェアや設備，データ，ソフトウェアについての保護，保全対策が適切になされているかをレビューする。また，データの正確性を保証することのできるコントロールがなされているかどうかを，システム・コントロールという観点から監査する。

⑦　要員管理・研修

業務の責任範囲や権限の明確化，要員の研修プログラムや特定の職務・責任に対して必要な技能等について，正規の文書が作成されているか，またそれに従って研修されているか等をレビューする。

⑧　経営者への報告システム

情報処理部門の運営・管理に対する経営者の参加，情報処理部門，あるいはシステムに関する種々の活動の経営者への報告手続の有無等，経営者の情報処

理システムに対する管理状況についてレビューする。

⑨ アプリケーション・システムの有効性

システムに対するユーザや経営者の満足度，アウトプットの正確性，ユーザにとっての有効性等，個々のアプリケーションについて有効性をレビューする。

⑩ システムに対する品質の維持

開発中，あるいは開発されたシステムの品質チェックの体制や，経営者による参画，報告体制について適切な管理がなされているかを調査する。

システム監査を，安全性・信頼性の２つの目的に力点を置いて実施する場合でも，マネージメント・サイクルの全過程が直接的または間接的に関連しており，特に次の４段階に分けて監査する必要がある。

① 第１段階

システムの運用体制は，安全性・信頼性を維持できる仕組みになっているか。つまり，人，組織面で責任分担が明確に定められ，内部統制が考えられている運用手続が確立され，正しく運用されているか（人・組織面）。

② 第２段階

システム自体に安全性・信頼性を維持する仕組みが設計され，織り込まれているか（ソフト面）。システムを動かす設備は，安全性・信頼性を維持する仕組みを持っているか（ハード面）。

③ 第３段階

上記ソフト面・ハード面の仕組は，正しく稼動して来たか。

④ 第４段階

もし①～③が著しく弱い場合，テスト・データを作成して，システムの検証を徹底して行う。

2.2.3 システム監査実施上の要考慮点

(1) 改善に役立つ監査

一般的に監査というと，「総ての活動が終った後に監査人が来て，死人の数

を数えていく」という後向きのイメージを与えがちである。しかし，監査の本来の目的は，「監査結果を次の活動に反映させ，改善し，指摘された問題点をなくしていく」という，前向きなプロダクティブなものでなければならない。そのためには，データ処理の結果上の問題点だけでなく，システムの仕組みそのものが，まず第1に監査対象として重要となってくる。

システムの安全性・信頼性は，コンピュータ・システムの中だけではなく，インプット情報を起票する段階から，情報を転送しＥＤＰ処理を行い，その情報をユーザに再転送し，ユーザの手元に引渡すまでの全過程において考慮されなければならない（表２－１参照）。システム監査は，まずその情報の流れの中の，安全性・信頼性を維持する仕組みの妥当性のチェックから始まる。

(2) セキュリティ・チェックのテクニック

表２－１に，情報の流れと予想するリスクの例を上げたが，以下個々のリスクに対するセキュリティ・チェックの技法を示しておく。

① 不正取引の作成について

- ○ 電話による確認チェック
- ○ レビューの二重性
- ○ 取引金額の制限（１件当り累積ベース）
- ○ 定期的固定取引情報のマスタ化
- ○ 固定マスタ情報の設定

② 承認されていない担当者によるシステム・アクセス

- ○ オペレータＩＤカード
- ○ パスワード
- ○ 物理的なアクセス制限
- ○ 勤務時間外のシステム運転停止
- ○ パスワードの定期的変更
- ○ パスワード・リストの保管

③ 回線にアクセスすることによる取引の不正な改ざん及びのぞき

- ○ トランザクション・テスト・ワード（Transaction Test Words）

表２－１　情報の流れと予想されるリスクの例

処理項目	リスク内容
データ作成	○承認されていない担当者による取引の作成 ○承認されていない不正取引の作成
データ・エントリー	○承認されていない担当者によるシステムに対するアクセス
データ転送	○回線にアクセスすることによる取引の不正な改ざん，のぞき
データベース更新	○システム間の同期がとれない事を看破して二重取引の作成
データ保管	○保管されているデータの改ざん ○ファイルそのもののコピー等収集
データ配布	○承認されていない人に対するデータの配布 ○データの改ざん
システム開発	○プログラマによる不正コーディング

- メッセージの暗号化
- 処理一連番号の付与
- 回線の物理的保護
- フロントエンド・セキュリティ・ソフトウェア (Front-end Security Software)
- フロントエンド・セキュリティ・システム (Front-end Security System)
- セキュリティ・オペレーティング・システム

④ システム間の同期のギャップを突いた二重取引の防御

- 単一マスタ・ファイル更新による同期
- 危険な取引を許可する前に，マスタ・ファイルの照会を行う。
- 危険な取引を許可する前に，電話によるマスタ・ファイルの照会を行う。

⑤ 蓄積されているデータの改ざん及びのぞき

- 物理的なアクセス制限
- パスワード
- データの暗号化

⑥ データ（処理結果）の配布

- 物理的アクセス制限
- パスワード
- 配布処理のシステム化と配布手続きの確立

⑦ 不正コーディング

- コード・レビュー (Code Review)
- テスト・データ及びテストの独立性
- プログラマ履歴のレビュー

(3) ミス，誤りによるリスクとコントロール

前述のセキュリティ・チェックでは，データ作成からデータの配布にいたるまでの，情報の流れの中での悪意によるデータの作成，アクセス，改ざん等のチェックについて主として述べたが，それ以外にも，ミス又は誤りによるリス

クも当然存在する。表２－２にそれらのリスク面からみたコントロール技法をリストする。

表２－２　システム・コントロール技法の例

不正内容	対策技法
誤った情報記入，情報の洩れ	○レビューの二重性 ○定期的固定取引情報のマスタ化 ○データ・コントロール（レンジ・チェック等）
情報の二重作成	○レビューの二重性 ○取引ヒストリー・マスタのつき合せ
ミス・パンチ，抜け，二重インプット	○バッチ・コントロール ○バッチ・プルーフ・リスト・レビュー
データ・トランスミッション中の変形抜け	○処理一連番号 ○テスト・ワード
データベースの不正確更新	○コントロール・データ ○オーディット・トレイル ○RUN TO RUN CONTROL
ファイルのかけ違い，使用ミス	○RUN NO.CONTROL
データ配布のミス	○DATA DISTRIBUTION SYSTEM
システム開発上のコーディング・ミス	○UNIT TEST,STRING TEST ○SYSTEM TEST ○USER TEST

(4) 組織管理のコントロール

(2), (3)で各種のリスクとコントロール技法を示したが，システムは，道具としてのＥＤＰシステム（プログラム＋ハードウェア）とそれを運用する人，及び組織でなりたっている。従って，リスクは人及び組織に存在し，又ＥＤＰシステム上考慮すべき点としては，次のものがある。

① 組織構造 － 組織の定義
　　－ 職務分掌

② 内部牽制 － ＥＤＰ部門での内部牽制
　　－ ＥＤＰ部門との内部牽制

③ 標準オペレーション手続
　　－ 文書化

④ 人事方針 － 雇用手続
　　－ 教育プログラム
　　－ 退職手続

⑤ リソース計画 － 設備・機器・ソフトウェア及び人事計画
　　－ 実際と計画との差異のコントロール

(5) システム開発コントロール

道具としてのＥＤＰシステムをリスク・ミニマムにするには，システム開発の段階で，そのためのコントロールが実施される手順が，明確になっていなければならない。そのためには，次の事がしっかりと行なわれていることを，チェックする必要がある。

① システム開発の方法論を，まず最初に明確にする。

② システム化計画を実施し，長期的セキュリティ・コントロール・ニーズを明確にする。さらにトップ・マネージメントによるレビューを実施する。

③ システム基本設計で，セキュリティ・コントロール機能を設計する。

④ システム開発・導入段階で，セキュリティ・コントロール機能をシステムに組み入れる。

⑤ 構造化プログラミングを取り入れ，プログラムのモジュール化，標準化を

図り，システムの正確性を高める。

⑥ 大規模システムを開発する場合には体系的なテスト・アプローチと技法を確立する必要がある。

⑦ 文書化をしっかり行い，併せてプログラム変更の手続を確立する。

(6) オペレーション・コントロール

表２－３にオペレーション・コントロール上チェックすべき項目のリストを示す。

表２－３ オペレーション・コントロール

1. インプット／アウトプット・コントロール
2. ジョブ・ハンドリング手続
3. スケジューリング手続
4. オペレーション・スケジュール
5. データ処理カット・オフ日
6. ジョブの提出・承認
7. ライブラリ・アクセス・コントロール
8. ライブラリ・エリアの分類
9. 物理的セキュリティ
10. 持ち出しの制限
11. 在 庫 記 録
12. 使 用 記 録
13. 保管室のセキュリティ
14. 他の場所での保管及び二重ファイル保管

(7) システムの効率性

システムの効率性のチェックも，非常に大きなシステム監査目的であり，論じ始めると莫大なページ数を必要とするので，その中で主要領域のみ示してお

く。

① システム開発の生産性

② システム・オペレーションの効率性

③ システム・メンテナンスの容易性

④ ユーザにとってのシステムの有効性

(8) システム・ロジックの正確性の監査

今までシステム監査が論じられる時，データ処理結果のチェック又はシステム・ロジックの正確性の検証と，そのための技法の解説に主眼が置かれてきた。例えば，テスト・データ法，平行シミュレーション法，スナップ・ショット法，総合テスト法等がそれにあたる。しかし現実には，システム監査のニーズとコスト／工数／技術面からも，これらの技法は，システム監査の第1段階から第3段階（2.2.2.「システム監査の範囲」を参照）までの監査過程で大幅に問題ありとされた場合に，第4段階として最後にとる手段であろう。定期的に行うシステム監査としては，実務で処理されたデータを必要に応じて検証するのが，システム・ロジックの正確性の監査としては中心である。そのためには，システム設計時から，システム内部でのコントロール・ポイントを定義し，そのポイントで各種データの履歴をきちんと取れるような，システム・コントロール設計をしておく必要がある。さらに，これら履歴データ（又はログ・データ）を必要に応じて簡単に色々な形で取り出せる仕組みがなければならない。

2.2.4 ま と め

システム監査の目的は高く，領域は広い。システム監査は，"第3者によりシステム（EDPシステム＋運用体制）をレビュー及び評価し，監督責任者に報告すること"というのが最も基本的な定義である。

しかし，ひとつのシステム監査で総ての目的と全領域をカバーするには，莫大な工数がかかるため，現実には個々のケースに応じてシステム監査の目的と範囲を決めて実施していくことになる。例えば，内部監査人が実施する場合，外部の公認会計士が会計監査の一部として行う場合，本社のシステム部が事業部，支店，

工場等に対して行う場合，本社の海外統括部門が海外子会社・関連会社に対して行う場合，トップ・マネージメントが外部のコンサルタントにシステムの有効性・効率性等のシステム・レビューを依頼する場合等，色々なケースが存在する。従って，システム監査は，個々のニーズに応じて目的・領域・実務工数・技法等を選択して実施していくべきである。

いずれの場合においても，システム監査はシステムの処理したデータの結果のみにとらわれず，むしろ，システム構築のプロセス，組織も含めたシステム運用のプロセス，システム・オペレーションのプロセス及びシステムに織り込まれたコントロール・セキュリティ・効率性等のための仕組みに重点を置き，システム監査から前向きのプロダクティブなアウトプットを出せるように，調査目的，対象，技法，実施計画等を定めなければならない。

2.3　ユーザの立場からみたシステム監査

2.3.1　システム監査の実施状況

システム監査については，昭和40年代の半ば頃から日本情報処理開発協会を中心に本格的な調査検討が進められ，その普及，充実のために種々のセミナー，講演会等啓蒙活動がなされ，56年の産業構造審議会情報産業部会の答申の中でも，EDPシステムのセキュリティ確保の有力な手段として，位置づけられている。にも拘わらず，種々のアンケート調査の結果をみると，最近実施率はかなり上がっているもののまだ充分とはいえない。

また，システム監査の実施内容についてみると，システムの公共性が高く，システム監査が比較的普及しているといわれる大手銀行においては，その大半で内部検査部門の中にシステム監査専任者を置いているものの，その要員数は多くても数名であり，システムの内容に深く立ち入った監査はできていないのが，現状といえよう。

すなわち，現状のシステム監査は，コンピュータアウトプットを使用しての処理の妥当性チェック，あるいはあらかじめ定められた規程・手続の遵守状況のチェック等を中心とした周辺監査・運用監査が主体であり，コンピュータを使っての監査，設計・開発段階の監査，あるいはシステムの効率性・有効性の監査の実施率となると更にその比率は低下する。

コンピュータを使っての監査では，汎用システム監査ツールが，もともと外部監査用に作られたものであることから，外部監査人による監査から普及してきている。設計・開発段階での監査は，内部監査人の方が数段やりやすい環境にあるものと考えられ，内部監査人によるこの面での監査の実施拡大普及を図っていく必要があろう。

内部監査については，その必要性は総論的には一般に認められてきているものの，現実に実施する場合，費用対効果あるいは内部監査人で可能な範囲・限界等が問題となり，実効を挙げ得る形で一般化していない。たゞ企業体そのものの自発的な内部統制の充実によりシステムの信頼性向上を図り，かつ外部監査実施時

の効率をあげるためにも，各企業における内部監査の体制整備と内容の充実が望まれる。

一方，システム監査に関連する基準・ガイドラインとしては，日本情報処理開発協会から昭和54年に公表された「システム監査基準」が，システム監査実施の具体的方向を示したものとして認められており，また昭和51年に 日本公認会計士協会から発表された「ＥＤＰシステムの内部統制質問書」が，その対象範囲・内容に一部議論はあるものの，主要項目を全般的に網羅したものであり，システム監査に取り組む際のガイドブックとして，有効なものと考えられる。また昭和52年に通商産業省から発表された「電子計算機システム安全対策基準」及び昭和57年に郵政省から出された「データ通信ネットワーク安全・信頼性基準」が，やゝハードウェアに重点を置いたセキュリティ全般についてのガイドラインとなっており，対象範囲が一部異なるものの，システムの監査実施に際してのチェックリストの一部として，活用できるものといえよう。

金融業のシステム監査に関しては，昭和57年に日本公認会計士協会から「銀行業におけるＥＤＰ監査に関する公開草案」が提示され，より具体的なイメージが出てきている。今後他業種についても類似のガイドラインあるいは，チェックリスト的なものが示され，これらを踏まえた事例研究・情報交換を通じて，その内容のレベルアップ・充実がなされることが望まれる。

さらに最近の動きとしては，通商産業省を中心に検討が進められている「システム監査基準」の策定，あるいはシステム監査の情報処理試験科目への組み込み等があり，体制面からのシステム監査の充実・サポートという意味でその結果を大いに期待したい。

2.3.2　システム監査の狙い

システム監査については，日本情報処理開発協会の「システム監査基準」の中で示されている「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・勧告することをいゝ，システムの有効利用の促進と弊害の除去を同時に追求

して，システムの健全化を図るものである。」との定義が一般的に認められている。

また，システム監査の狙いとしては次の様な点が挙げられる。

① システムそのものに潜在する誤謬の発生を未然に防ぐための処理の正確性確保（これは手続・規程の準拠状況と同時に手続・規程そのものの妥当性チェックをも包含するものである。）

② システム内にエラーがあった場合，システムの大規模化・広域化・複雑化等により企業体内外への影響度合は，従来に比べ格段に大きくなっている。これらの影響をできるだけ小さく，短期間に，かつ範囲を狭くする様な安全性・信頼性の確保

③ システムの集中化特にデータの集中とシステムのネットワーク化・オープン化に伴なう集中されたデータの機密性・安全性の確保

④ 企業の存続・発展の為の大前提となる有効性・効率性の確保

システム監査実施に際しては，これらの目的を達成する為にどの様な観点からチェックするのかが問題となる。これらの狙いについての重点の置き方は，業種あるいはシステムそのものの性格により，かなりの差があると思われる。

すなわち金融・流通システムにおいては物と金（財産）の流通を扱っており，社会的影響の大きさからも処理の正確性の確保が最優先課題となる。従って処理に際しての手続・規程の準拠性のチェック，あるいは手続・規程そのものの妥当性のチェックが，監査の最重点項目となろう。また医療・交通関連のシステムにおいては，場合によっては人命にかゝわることもあり，正確性に加え事故発生時のフェイルセーフ機能等も含めた，安全性・信頼性の確保が重要な項目となる。さらに官公庁・自治体等のシステムにおいては，保有しているデータの性格上扱い方によっては，プライバシー侵害を生ぜしめる可能性が高く，機密性・完全性の確保を重視していく必要がある。そして一般の企業にとっては，上記の様な正確性・安全性・機密性等の確保もさることながら，業務目標との一貫性さらにはシステムそのものの効果・費用

分析を踏まえた効率性・有効性の確保が，ポイントとなろう。

2.3.3　システム監査実施上の問題点

システム監査がシステムを点検・評価することから出発するものであるならば，点検・評価するための規程あるいは評価基準が明確になっていることが必要である。また，コンピュータシステムを主たる対象とする場合，磁気データを扱う大量処理が中心であり，人手による作業では限界があり，これをサポートする技術・ツールの普及・活用が必須となる。以下この二点につきやゝ詳細に述べる。

まづ第一のシステム監査の前提となる規程・評価基準については，システム監査そのものの定義・範囲の不明確さにより，未だに具体的・現実的で広く用いられ得る様なものはできていないのが現状である。すなわち一般的には，前述の日本情報処理開発協会の「システム監査基準」及び日本公認会計士協会の「ＥＤＰシステムの内部統制質問書」等に示されている様な事項が，システム監査に関する基準として妥当なものといえよう。たゞこれらの定義・基準についても立場の違い，規模の違い，業種の違い等により，内容がかなり異なるケースが多く，範囲・対象を明確にした上で，各々にふさわしい基準を作る必要がある。

例えば，システム監査に関する立場の違いは，以下の様な問題を生ぜしめる。すなわち公認会計士に代表される外部監査人にとっては，商法等にもとづく経理処理の妥当性と遵法性の点検・評価が主目的であり，この面での立証のために，コンピュータシステムの内容にまで立ち入ってくるものである。この場合，内部統制の状況把握も会社ぐるみの不正・違法行為等のチェックも含まれ，広範囲にわたるものの準拠すべき規程・基準は内部監査に比べれば，比較的明確になっているといえる。一方，内部監査人による監査はその目的・内容が外部監査人によるそれとは自づから異なる。すなわち前述の様に，システムの性格により重点を置くポイントがやゝ異なるものの，当該企業にとってシステム監査そのものが，効果あるものであるということがまづ第一に要求される。公共性の高い企業においては，社会的な要請としてシステムの正確性・信頼性が強く要求され，システム監査実施に際しても，これらへの対応が重視されるが，これとてもこれらが達

成されなければ，その企業が公共性をもった企業として存続できなくなるからに他ならない。また，一般企業システムにおいては，事故等により社会一般に直接的な損害・影響を与えることは少ないものの，システム監査により事故の発生を未然に防ぐこと，あるいは事故をできるだけ早く発見し対応策を講じ得る様にすることは，企業活動の効率を上げる（費用減，生産量増等）ことに結びつくものである。

ただ一方では，監査部門はラインから独立した客観的な立場を堅持する必要があり，内部システム監査人の立場・職務には微妙な部分が多く，定義も明確化しにくいものとなっている。さらに内部監査人にとっては，システム開発部門における品質管理部門との関連・職務分担も大きい問題であり，企業内の組織体制・規模等により，個々に最適なものを選択していく必要があろう。

また監査部門は，監査対象とは独立した組織とすることが望ましいが，分散処理等で対象部門の規模が小さい場合，あるいはシステム監査人の適任者がいない場合等では，組織内での相互牽制機能をうまく働かせながら，当面はシステム開発部門内で対応したり，監査部門と開発部門の共同プロジェクトで実施する等の便宜法も検討していくべきであろう。

また，システムのオンライン化の拡大を踏まえた，システム監査における事後チェック中心から，事前チェック重視への姿勢の変化に伴なうシステム監査部門の開発段階への参画については，次の様なことがいえる。

従来の手作業中心の処理では何段階かの作業過程で人手が入ることにより，ミス・不正が混入するケースが多く，正確性・信頼性の面で問題が多かった。たゞこの場合，一つの処理に何人もの人が係わることとなり，相互牽制効果をもたらし，犯罪・不正防止で有効であった。これが処理の大量化に伴ない，コンピュータ化・自動化・省力化されると，作業過程でのミス・不正の混入は減少するものの，一旦インプットされたデータは，中間段階での他人によるチェックが不可能または不充分となり，犯罪・不正防止という面で逆効果をもたらしているともいえる。また大量の処理を集中的に行なうことにより，一回当りのミス・不正による影響度合は，手作業処理に比べ格段に大きくなった。この様なミス・不正の混

入を少なくするためには，インプット段階でのチェックアウトあるいは処理途中でのチェックを可能とする様な仕組みを，システム中に組み込むことが必要となる。このためにはシステムの設計・開発段階において，これらの仕組みをシステムに組み込むべく，システム監査部門が設計段階で参画することが有効となってくる。

これらの仕組みに，どの様なものがありどれを採用すべきかについては，システムの内容・規模によるちがいが大きいと思われるので，ユーザ相互の情報交換あるいは事例研究等を通じて，具体的な指針が示されていくことを期待したい。またシステム開発段階へのシステム監査部門からの参画については，現状では要員不足・ノウハウの不足が否めず，ガイドラインの充実，専門的な教育機関の設置等体制面の整備が望まれる。さらに，システム参画型レビューについては，システム開発部門内におけるレビュー担当者との職務分担の問題，あるいはシステム監査部門の独立性・客観性をどこまで保てるか等の問題を，解決する必要がある。

第二に大量処理への対応という点から，システム監査実施時に必須とされるツールの活用という面では，次の様なことがいえる。

すなわち，コンピュータによる大量処理結果を監査しようとする場合，人手のみでサンプリング・チェックするのでは限界があり，コンピュータ・ツールを使っての監査実施が必須である。この場合，使用するツールそのものの正確性・信頼性が問題であり，またツールそのものをシステムへ組み込む場合，開発部門との独立性をどの様な形で確保するかが問題となろう。

また，事故の事前発生防止のためのツール・技術として，開発段階におけるテストツール，検証ツールがあり，これらは開発そのものの生産性向上・品質向上技術の一環として，近年急速な進歩をとげている。すなわち開発の生産性は，ミスのないシステムを如何に少ないコスト（負荷）で開発・運用できるかによって判断されるが，システム完成後の修正・変更は開発途中のそれよりも負荷がかゝり，開発途中でもその誤謬発見の時期が早い程修正・変更負荷が小さくて済むと言われており，設計・開発段階での品質管理・検証ツールの重要性が認識される

に伴ない，急速に充実し活用されはじめている。これを監査面で評価するとすれば，システムの信頼性・正確性充実のために有効なものとして，積極的に利用を薦めると共に，システム監査における正確性・信頼性チェックのために，開発部門における品質・管理とは違った視点・アプローチで活用することにより，監査内容の一層の充実が図れることとなろう。

さらにツールに関連して，事後監査のための基本データとなるログの記録・保存の問題がある。すなわち，監査証跡としての処理結果データについては，それが磁気媒体に記録されることから証拠能力に疑問があるにも拘らず，保存すべき年限・範囲等が抽象的にしか論じられず，また処理結果とは別に，その処理過程を立証するデータとなるシステム・ログ，あるいは中間結果データ等の記録すべき範囲・保存期限等については，もっと不明確な状況にある。現状では個々のシステムにおいて，独自の判断で処理しているが，少なくともこれらに関する最少限のガイドラインの提示を望みたい。

一方このログに関する技術的な問題点としては，以下の様なことがいえる。

第一に，特に大規模システムにおいては，本来業務の処理量の増大に伴ない，ログすべきデータの量も比例的に増大するが，これの記録のためのシステム負荷を，本来処理のパフォーマンスに影響を及ぼすことなく，いかに吸収していくか，また大量のデータを如何に低コストで記録・保存できるかが問題となる。

第二にログしたデータの改ざん防止を中心とした機密性・信頼性確保の問題である。ログ・データが監査用のみに限定して使用されるのであれば，物理的に再書込み不能な現状の光ディスク等が最適であろうが，現状ではコスト的にも監査用データのみを大量に保存できる様な状態にはなく，他の目的，例えばリカバリー処理，事後のファイル更新用データ作成等に，兼用しているのが通常である。このため保全性・機密性を重視するとすれば，物理的には再書込みが可能だが論理的に不可能とできる様な媒体あるいは，更新した個所が自動的・強制的に記録される仕組み等が有効であると考えられる。

2.3.4　システム監査用ツール・手法

システム監査用ツール・手法については，ＳＡＣレポート（「システムの可監査性及び統制の研究」）で「コンピュータ適用監査のツールと手法」，「コンピュータ・サービス・センタ監査のツールと手法」，「業務システム開発監査のツールと手法」の三つに大別して詳しく述べられているが，こゝではシステム監査用ツール・手法を，応用システムそのものに組み込まれるものと，応用システムそのものからは独立したいわゆる汎用監査ツールの二つに大別して，ＳＡＣレポートで示されるツール手法と対応づけながら，ユーザの立場からみた問題点，改善要望点等を述べてみたい。

まず第一に組み込み型監査ツールとしては，総合テスト，シミュレーション技法を用いたツール・手法がある。この種のツールの特徴は，システム監査の手法あるいは仕組みを本番システムの中に組み込むものであり，対象システムの大規模化・複雑化に伴ない，開発及び保守負荷が非常に高くなる。この場合既成のシステムにこれらのチェック機能を組み込むのは，負荷が大きくまたリスクも大きいので，システム設計段階でシステム監査部門が参画し，要件を提示してシステムに前以って組み込むことが必須である。このため，自分で設計したシステムを自分で監視することともなり，監査の独立性・客観性確保にやゝ疑問の残るところである。さらにこの様な監査システムの開発作業は，開発部門に任せることとなろうが，この場合監査システムそのものの正確性・信頼性のチェックレベルは，通常のシステムと同様で良いのか等の問題もある。ただ機能的には，システムそのものの処理過程の信頼性までチェック可能なものであり，システムの内容・規模の違いによる組み込み内容の相異点を含めた，設計時の配慮点・ポイント等が明確にされ，広範囲に活用されていく様な環境が整っていくことが期待される。

またこれらを汎用的に提供しようとする場合，いわゆる監査手法・仕組みとしての提供となり，汎用ツールあるいはサブルーチンの形には，なり難いものと考えられる。ただ最近，我国でも徐々に提供され，使用されはじめている汎用アプリケーション・パッケージにおいては，ぜひともシステムの中にこれらの機能を組み込んだ上で提供して欲しいものである。

組み込み型監査ツールの変型としてトレース，スナップショットあるいは事後監査の基本データとなるログ・データの収集機能がある。これについても，どの様なデータをどのタイミングで記録すべきかは，適用業務により異なるものと考えられ，システムの監査部門要員が，システム設計段階で参画することが必要とされよう。ただこれらの機能そのものは定型的であり，汎用化・サブルーチン化も比較的簡単と考えられるので，応用システムのこの領域においても，システム・ログの記録機能と同様の，実用的な技術・ツールの開発・提供を期待したい。

また最近のシステムの大規模化に伴ない，記録・保存するログのデータ量が大きく，これに関する費用増加が問題となる。特に最近の大規模システムでは，システムの効果／費用をかなり厳密に評価しており，監査面からの要求についても，その効果について明確なものを提示しないと，なかなか採用することが難しくなっている。システム監査においてシステムの効率性・有効性の評価をも含めていくとすれば，システム監査に関する効果対費用についても，明確かつ極力定量的な判断材料の提供を心掛けていく必要があろう。さらに小規模システムあるいは分散システム等においては，ログの記録・保存そのものがシステムの効率に大きい影響を及ぼす可能性が高いこと，あるいは記録したログそのものの保管・運用体制の確立が難しいこと等を，充分配慮した上でツールの利用，体制の整備を図っていく必要がある。

なお記録されたログの評価・検証は事後に行なわれるのが通例であるが，これの傾向分析によりエラー・不正防止のための事前対策が検討できることもあり，積極的な活用を図っていきたいものである。例えば間違ったパスワードでのアクセス要求が急増した場合，カードあるいはアクセスのためのＩＤが他人に盗用，あるいは不正使用されていないかのチェックをすべきであり，またオペレーション・ミスの多いケースを分析して，オペレーション要員の教育あるいはシステムの改善要求等に生かす等により，大きい効果が期待できる。

特に応用システムにおけるログの記録分析システムは，汎用アプリケーション・パッケージにおいては標準として組み込まれていることが望ましいが，全部の機能を組み込むことができないとしても，システムの適宜の場所に監査用のエグジ

ット・ルーチン用の出口を設ける等，ユーザ側で簡単に利用可能な形となっていることが必要とされよう。

第二の独立汎用監査ソフトウェアは，既存のデータをベースに抽出・比較・演算・レポート作成等を行なうツールであり，従来からかなりの数の汎用パッケージが市販されている。これらはシステムに関する知識の必要度を最少限に抑え得る様，パラメータ指定等を多用しているが，あくまでも外部監査人用の機能を重視して作られたものであり，内部監査人が使用する場合，監査人のスキルと必要機能の組み合わせを配慮した上で，一般の汎用検索・レポート作成用パッケージの利用も含め検討すべきであろう。いづれにしろ，大量処理を前提としてコンピュータ化されたシステムの監査を行なおうとすれば，従来の様な手作業のみに頼っていたのではその内容充実は期待できない。従って現時点では，機能的に一部不充分なところがある，あるいはスキル面から使いこなせない部分があるにせよ，汎用ソフトウェアを使っていくのが有効であり，使い込むことによって内容のレベルアップを図り，より充実したものにしていくべきであろう。

さらに，汎用監査ソフトウェアの変型として，原始コードの比較，マッピング等の機能をもったソフトウェアがある。これらのツールは本来開発生産性の向上あるいは品質向上のためのツールとして利用されてきたものであるが，特に品質管理・検証ツールについては，テストの妥当性・正確性をチェックするツールとしての有効なものがあり，これらのツールも監査の目的によってはシステム監査用ツールとして，活用していくべきものと考えられる。

ただこれらのツールは，本来システム開発部門向けに提供されたものであり，システムに関する比較的高い知識を必要とするケースが多く，システム開発部門から独立しているシステム監査人にとっては，使いづらいものといわざるを得ない。これらのツールの使い勝手の改善，レベルアップが期待される。

2.3.5 むすび

いづれにせよ内部監査人によるシステム監査は，外部監査人による監査とシステム開発部門内における品質管理担当者によるレビュー等との中間に位置し，そ

の守備範囲の明確化と独立性・客観性を如何に確保するかがポイントであり，これに関するガイドラインの明確化と体制の整備が急務といえる。これについては通商産業省でも本格的な検討が予定されており，体制面からのシステム監査の充実・サポートという意味で，その結果に期待するところ大である。特に現状のシステム監査は業種・規模の違いによる内容・レベルの差が大きいものと考えられるので，実務経験に裏付けられ，かつユーザの立場を充分尊重した形で，これらのガイドラインが設定されることを要望したい。

一方技術的な面では，周辺技術の急速な進歩に対応するため，システム監査に際してもツールの使用は必須であり，機能の充実もさることながら使いやすいツールの提供を望みたい。同時に監査実施のために必要充分なデータを，システム本体のパフォーマンスを確保しつつ記録・保存を可能とする様な技術の確立が期待される。

さらに最近は犯罪防止等を重視する傾向もあり，予防的見地から事前・即時チェックの重要性が増し，使用ツールそのもののオンライン化も必要となってこよう。またシステムが大規模化し効率性・保全性重視の傾向が強まっている現状では，システム全体の効果あるいは効率について定量的・客観的な評価基準の確立が必要であり，これをサポートする様なツールの開発が必要なのではないかと思われる。

2.4 システム監査と支援ツールの現状

2.4.1 はじめに

応用システムの開発，応用システムによる処理およびシステムの運用が，処理結果の正確性と完全性に影響を与える。

それらの三つの範囲のうち，応用システムによる処理の監査に利用されるツールと手法は，以下の六つの処理段階によって分類することができる。

- トランザクションの発生
- トランザクションの入力
- データ通信
- コンピュータによる処理
- データの記憶とアクセス
- 出　力

新しい技術やシステム設計上の考え方が，応用システムの中に採り入れられるにしたがって，監査人はそれらに即応した監査手法やツールを使うことが求められる。

この節では，特にコンピュータによる処理およびデータの記憶とアクセスに焦点をあてて，監査の手法とツールについて，最初に論ずることにする。第二に，メーカが提供するツールについて説明し，次に分散処理とネットワーク化へのシステム監査の対応について，述べることにする。

2.4.2 現在の手法とツール（特に処理の検証とデータの検証について）

(1) 処理の検証

コンピュータによる処理の監査項目には次のものが含まれる。

- 処理の完全性
- 再始動と回復
- 処理の正確性
- 操作員の介入

○　データ保護

○　エラーの取扱い

監査人が，処理の完全性，正確性，データ保護について，統制の適切さやそれの遵守度を検証する方法としてはテスト・データ法がある。また処理統制を検証する方法としては，基本事例評価法とＩＴＦ法がある。監査人は，処理ロジックを客観的にながめ吟味するために，トランザクションのタグ付けを行ない，また各種のプログラム分析法を用いる。トレース・マッピング法は，プログラムを通るトランザクションの流れを文書化して，使われていないロジックを識別するために用いられる。

本番処理中のトランザクションの動きを検証するためには，監査用ソフトウェアやサブルーチンが使われる。入力トランザクションの動きを監視して，監査の規準にもとづいてトランザクションの正確性や完全性の立場から振り分けるためには，入力トランザクションの選択プログラムが使われる。組込ルーチンを使う場合は，内部で生成されたトランザクションの選別にも有効である。

平行シミュレーション法では，選択した特定の処理機能の正確性と完全性を検証するために，汎用監査ソフトウェアが使われる。これにおいては，コピーしたマスタ・ファイルに本番データを入力して，汎用ソフトウェアが処理をシミュレートする。このようにして作られたマスタ・ファイルは，対応する本番マスタ・ファイルと比較され，差異が検出される。この際，検証される処理機能は特定の計算，操作手順に限られる。シミュレーションによって得られたマスタ・ファイルと本番マスタ・ファイルの比較のためにも，汎用ソフトウェアが用いられ，結果は差異を表わすコンピュータ・リストとして与えられる。このリストをもとに，監査人は分析と調整を行なう。

操作員の介入について監査する有力な手がかりとしては，操作卓ログがある。

(2)　データの検証

データの検証には，データ入力にかかわるものと，データ記憶およびアクセスにかかわるものとがあるが，ここでは後者を対象にする。この段階での検証は，マスタ・ファイルの正確性と完全性を確保するための統制が万全かどうか

を確かめるために行われる。ここに関係する領域は次の通りである。

- マスタ・ファイルの更新
- 入力トランザクションの締め
- データ保護
- エラーの取扱い

上記の領域に関する統制を検証するために，監査人は汎用監査ソフトウェアを使用する。それは，マスタ・ファイルの記録を抽出して外部の記録と突き合わせたり，各種の発送確認状を作成するために使われる。またすべてのトランザクションが正しく記録されているかどうかを検証するために，更新前後のマスタ・ファイルの比較が行われる。トランザクションを選択して，データの発生からマスタ・ファイルの更新までトレースが行われる。これらのデータのトレースは，すべてのトランザクションが正しく処理されていること，および締切日に合致していることを確かめるためである。

また監査人は，通常の処理を通して作成された報告書を用いて，ファイル更新後のバランスを更新以前のバランスおよびトランザクション合計に対して，手作業により突合を行ない処理の正確さを検証する。適用業務プログラムがよく設計されている場合には，チェック用の報告書が定期的に得られるので，ユーザはそれらを使って突合ができる。一方，監査人もそれらの報告書を上手に監査のために使うことができる。

テスト・データ法は，ファイル更新の過程で起るエラーや脱落が，正しく見つけ出され，記録され，報告されるように統制が働いているかどうかを検証するために使われる。この監査は，コンピュータによる処理にかかわるものと考えがちであるが，トランザクション・データが該当するマスタ・ファイルに突き合わされるまでエラーが発見できないことがあるので，この段階に含めるべきである。

マスタ・ファイル更新のロジックとエラーの取扱い方法を評価検証するためにも，前述のテスト・データ法やＩＴＦ法が使われる。これらの技法は，オンライン・ファイルのアクセス制御を検証する目的にも使用できる。

データ・ファイルの保護は，適用業務にかかわるものと，媒体のライブラリ管理にかかわるものの両方がある。後者についてはライブラリ・ログを点検する方法がとられる。重要なマスタ・ファイルへのアクセス制御を検証する手がかりとしては，ジョブ会計データ分析法（たとえばＳＭＦの利用）がある。

2.4.3　メーカが提供するツール

表２－４は参考までにメーカが提供する監査およびデータ保護に関する支援プログラムの一覧を示したものである。

それらの中から，いくつかを選んで，その目的と機能を概説することにする。

(1)　監査ファイル比較プログラム

このプログラムは，二つのデータ・ファイル相互間の差異を調べることを目的に作られたものである。

主な機能は次の通りである。すなわち，監査人はファイル相互間を比較して，差異を見出すことができる。調べようとする差異については，限界値を設けることができる。一回の実行で２４通りの報告書を作成することができ，報告書には次の事項が示される。

- 文字フィールドの中の差異
- 数値データ・ファイル中の差異
- 各フィールド内のレコードの重復
- 一つまたは二つのファイルにある特別なレコードの差異

ユーザの要求にしたがい，フィールドの差異を分り易いリストにして示す。また，プログラムは簡単な言語で書かれており，使い易い。

(2)　監査原始コード比較プログラム

このプログラムは，プログラムの原始コードの二つのバージョンを比較して，実際の差異を分析するためのものである。差異は印刷され，メッセージの形式で示される。ユーザは印刷された報告書によって，保護の対象となるプログラムに許可なしの変更が加えられたがどうかを知ることができる。

主な機能は次の通りである。すなわち，原始コードの両方のバージョンはり

表2－4　監査およびデータ保護支援プログラム（IBM社のカタログより）

プログラム名	プログラム番号	情報検索	プログラム文書化統制	承認アクセス統制	検査シミュレーション	訓練	保守マネジメント制	設計開発	分析	変換	事後再シミュレーション始動
ACCAP/CMS Conversion Aid	5798-CNH									X	
Advanced Text Management System–DOS/VS	5746-XX4		X								
Advanced Text Management System–OS/VS	5740-XX3		X								
Advanced Text Management System II–DOS/VS	5746-XXG		X								
Advanced Text Management System II–OS/VS	5740-XXV		X								
Alpha Search Inquiry System	5736-N14	X									
ANS COBOL Conversion Aid for NCR Century COBOL for System/360/370	5798-APG									X	
ANS COBOL from GE 415 COBOL Conversion Aid	5798-ASY									X	
ANS COBOL from UNIVAC 9300 COBOL	5798-AHP									X	
APL Decision Table Processor and Code Generator	5796-PJB							X			
APL Function Editor for APLSV	5796-PGX							X			
APL Function Editor for VS/APL	5796-PGY							X			
APL Programming Development Tracking System	5796-PAD							X			
Audit Source Code Compare–DOS/VS	5796-PDF		X		X						
Audit Source Code Compare - OS/VS	5796-PDH		X		X						
Automated Unit Test for VM/370–CMS	5796-PEB		X		X			X			
Automated Unit Test for TSO & Batch–OS/VS	5796-PEC		X		X			X			
Batch Input Edit for the Interactive Training System	5798-CEF					X		X			
Batch Monitor for VM/370 CMS	5796-PGZ						X		X		
Batch Query Facility	5798-CBY	X						X			
Batch Terminal Simulator–BTS/FORMAT	5796-PBD		X		X						
Batch Terminal Simulator/VS	5796-PCZ				X						
Batch Terminal Simulator II	5796-PGT	X			X						
Burroughs 2500 COBOL to IBM ANS COBOL Conversion Aid	5798-APH									X	
CFO II - DL/I Interface	5798-AXW		X							X	
Chained - DL/I Bridge (DOS/VS and OS/VS)	5748-XX3									X	
Change Management Tracking	5740-DC1		X				X		X		
Change Tracker	5740-DC4		X				X		X		
CICS COBOL Call Interface	5796-AEG				X			X			
CICS Dynamic MAP	5798-AXR	X			X		X		X		
CICS COBOL/PL I One-Step Preprocessor	5798-CHC							X			
CICS/DOS VS	5746-XX3		X	X						X	
CICS/Entry System Statistics	5798-CBZ								X		
CICS/MTCS Online Panel Entry Library System	5798-CET	X	X					X			
CICS/MTCS 3270 Screen Format Utility	5798-CBH							X			
CICS Network Activity Simulator	5798-CCH							X			
CICS Online Test/Debug	5796-AHJ	X	X		X						
CICS/OS VS	5740-XX1		X	X						X	
CICS Performance Analyzer	5798-AZN		X		X				X		
CICS Plot	5798-CCG								X		
CICS Source Program–Maintenance Online	5798-BDT		X		X			X			
CICS Source Program Maintenance–Online II	5798-CFT							X			
CICS Volume Test Facility	5798-CDJ				X						
CICS/VS/COBOL Call Interface	5796-AHK							X			
CICS/VS Dataset Recovery Facility	5798-CJF					X					X
CICS/VS Dump Reading	5798-CJX			X		X					X
CICS/VS Online Test/Debug II	5796-AHJ		X		X						
CICS/VS Performance Analyzer II	5798-CFP		X		X				X		
CICS/3270 Simulator	5798-AXC		X		X				X		

プログラム名	プログラム番号	情報検索	データ定義システム化	水アクセス統制	シミュレーション検査	訓練	マネジメント統制	開発	分析	変換	利用レベル移行シミュレーション
CMS Service	5798-CJZ						X				X
COBIMS	5798-AYK							X			
COBOL Interactive Debug	5734-CB4				X						
COBOL Maintenance Aid/DOS	5796-AHY		X								
COBOL Maintenance and Documentation Aid/OS	5796-AHZ	X	X								
Console Spooling Under Power/VS	5798-CPQ				X						X
Control and Accounting Programs for VM/370	5798-AYP						X		X		
CPU Console/CICS Master Terminal	5798-ANK										X
Credit Management System	5799-ARY	X		X							
Credit Management System II	5799-AHJ	X		X							
Data Base Design Aid (DBDA)	5748-XX4							X			
Data Communications Analyzer	5796-PCA				X			X			
Data Dictionary/Directory	5796-PAG	X	X								
Data Language/I DOS/VS	5746-XX1	X									
Data Language/I Entry DOS/VS	5746-XX7	X									
DB/DC Data Dictionary - OS/VS	5740-XXF	X	X	X			X				
DB/DC Data Dictionary - DOS/VS	5746-XXC	X	X	X			X	X			
DB/DC Data Dictionary Systems for DL/I DOS/VS and IMS/VS (Feature)	5746-XXC	X	X	X			X	X			
DBPROTOTYPE	5796-PBB		X		X			X			
DBPROTOTYPE/VS	5796-PCX		X		X			X			
Direct Access Storage Device Conversion Aid	5798-CLQ									X	
Display Management System - DOS/VS	5746-XC2	X	X	X							
Display Management System - DMS II DOS	5736-XC4	X	X	X							
Display Management System - OS/VS	5740-XC2	X	X	X				X			
Display Management System - DMS II OS	5734-XC4	X	X	X							
Display Management System/3790 (DMS/3790)	5748-XC2							X			
DL/I Batch Monitor - DOS/VS	5796-AKY			X	X						
DL/I DOS/VS Support for the Customer Information File	5798-CDE									X	
DOS ALC from Burroughs 100/200/300/500 Basic Assembler Language	5798-AMC									X	
DOS DASDI JCL Conversion Aid	5798-CHA									X	
DOS Data Entry Control and Audit System	5796-AKC	X	X				X				
DOS/DITTO for System/360/370	5798-ARN				X						
DOS Source Statement Library Maintenance	5798-AWD		X					X			
DOS Time Accounting & Billing	5798-AHB						X		X		
DOS to OS Assembler Macro Conversion	5798-AFL									X	
DOS 3211 -2314/19 - 3330 DASD Device Independence Routines	5798-ALK									X	
DOS 3330 Data Set Conversion Aid	5798-AMN									X	
DOS/VS ANS COBOL from Burroughs B5500 COBOL	5798-CBP									X	
DOS/VS Assembler Testing Aid	5798-AWJ				X						
DOS/VS DASD Device Independence Open	5798-AWH									X	
DOS/VS DASD Space Utilization Analysis	5798-CHW								X		
DOS/VS DB Dump Utility DL/I, VANDL/I	5796-AJE	X			X		X				
DOS/VS DL/I Status Display/Debugging	5798-CGL	X	X		X		X				
DOS/VS File Operations Control Language	5798-CAG		X								X
DOS/VS Incident Reporting and Tracking	5798-CNP	X	X				X		X		
DOS/VS Interactive Debug Facility	5798-CKF				X						
DOS/VS Performance Tool	5796-PGK	X					X		X		
DOS/VS Sort for 1400 Files	5798-BDH										X
DOS/VS Sort/Merge	5746-SM1	X									

ソフトウェア名	プログラム番号	情報検索	プログラム走行制御	東アクセス統制	検査シミュレーション	訓練	システムマネジメント制御	開発	分析	変換	自動再スタート回復
DOS/VS Storage and CPU Utilization Display	5798-CHY								X		
DOS/VS System Display Directory List Optimizer	5796-PFH								X		X
DOS/VS System/360 Model 20 Emulated Disk Backup/Restore	5798-CKE										X
DOS/VS Time Control	5798-CNQ						X			X	
DOS/VS 2560 Sort	5796-AGX									X	
DOS/VS 3330/3340 Data Set Conversion Aid - Extensions	5798-CNA									X	
DP Accounting for IMS/VS	5740-DC2						X		X		
DPS to DOS Conversion Aid for the Model 20	5798-ANJ									X	
DPS to DOS Conversion Aid for the System/370	5798-BDA									X	
ESV Reporter	5798-AKR		X				X		X		
Extending Sequential Disk Files for DOS/VS	5798-CBN										X
Extensions to DOS/DITTO for System/370	5798-CAF				X						
Fixed Asset Accounting and Control	5798-AYD						X				
Format/3800	5798-CPN							X			
FORTRAN Interactive Debug for OS(TSO) and VM/370 (CMS)	5734-FO5				X						
FORTRAN Preprocessor for Structured Programming	5798-CDW		X		X			X			
Fundamentals of Flowcharting	5798-PFY					X					
Generalized Data Area Monitor and Display Program	5798-CKK						X		X		
Generalized Information System - GIS/VS	5740-XX7	X		X							
Generalized Trace Facility	5798-CHT	X					X		X		
Generalized Trace Facility - Direct Access Contention Analyzer	5798-CEZ								X		
Generalized Trace Facility - I/O Concurrency Report	5796-PGD								X		
General Ledger and Financial Accounting	5798-CCZ	X						X			
General Purpose Tape and Disk Scan	5796-AGY	X			X					X	
GIS/DDT Translation from IMS/DBD	5798-BBN										
GIS/GIS-VS Library Maintenance Program	5796-ANG						X	X			
GTF Supervisor Services Analyzer Program (GTFSVC)	5796-PGE								X		
GTF VTAM Buffer Analysis (GTFVTAM)	5796-PGF								X		
HASP-JES2 Spool Transfer Program	5798-CKJ				X					X	
HDAM Reorganization Utility for DL/I DOS/VS	5796-AKF								X		
Hierarchical Monitor System for 3600 (HMS/3600)	5798-CLT							X			
HIPODRAW	5796-PFF		X					X			
Honeywell 200 Series COBOL to IBM ANS COBOL Conversion Aid	5798-AGC									X	
IMS Application Development Facility	5796-PHX			X			X	X			
IMS Availability Reports	5798-CNN						X		X		
IMS Correspondence System	5798-CGA		X								
IMS DC Monitor	5798-BDF		X		X		X		X		

プログラム名	プログラム番号	情報検索	プログラム統制・文書化	業務プロセス検診断	シミュレーション技術	訓練	マネジメント統制	設計開発	分析	変換	オペレーション自動化
IMS Dictionary Enhancements	5798-CEE	X	X	X			X	X			
IMS Dictionary System	5798-BBA	X	X	X			X	X			
IMS History Reporting System	5798-CLB	X					X		X		
IMS Job Development System II	5798-CLP		X	X	X			X			
IMS Log Tape Analysis	5798-CAQ						X		X		
IMS Log Tape Management	5796-AHT		X				X				X
Information Management System - IMS/VS/IOF	5740-XX2		X	X							
IMS Monitor Summary and Systems Analysis	5798-CDT		X				X		X		
IMS Online Program and Job Development	5798-CDR		X	X	X			X			
IMS Space Management Utilities	5796-PFW								X		
IMS Transaction Profiles	5796-PGG		X	X			X		X		
IMS TRAPDL/I System	5798-CEJ		X				X				
IMSMAP	5796-PBC		X								
IMSMAP/VS	5796-PCY		X								
IMS 3270 Local Copy	5796-AHL							X			
IMS/VS HDAM Randomizing Algorithm Analyzer	5796-AJL							X	X		
IMS/VS Virtual Storage Analysis Program	5798-CNC								X		
IMS/VS Local Copy II	5798-CLZ							X			
IMS/VS 2260-3270 Conversion Aid	5798-CBB									X	
IMS/360 2260-3270 Conversion Aid	5798-ASG									X	
Interactive Instructional System	5748-XX6					X					
Interactive Query and Report Processor (IQRP)	5796-PGD	X	X	X							
Interactive Training System	5734-XXC					X					
Introducing the Computer	5796-PDX					X					
ISAM to DL/I COBOL Program Translator for OS, OS/VS and VM/370	5796-PFC									X	
ISAM to DL/I COBOL Program Translator for DOS, DOS/VS	5796-PFB									X	
JES 3 Monitoring Facility	5796-PHR								X		
Job Control Language Device Dependent Parameter Conversion and Replacement (DDPREP)	5798-AJU									X	
Job Control Language Editor	5796-PDC		X								
Life Inquiry/Data Entry	5746-N11	X		X							
Mass Storage Control Table Maintenance Using TSO, TCAM and the System Console	5796-PHY										X
MVS Seek Analysis Program	5796-PJC								X		
MVS/SMF Problem Program Activity Reporting Program	5798-CPP						X		X		
MVS Storage Utility/Display	5798-CGT						X		X		
MVS System Information Routines	5796-PGB								X		
Operations Planning and Control - Entry (OPC - Entry)	5740-XT7								X		X
OS/DITTO Extensions	5798-CDA				X						
OS/DITTO for System/360/370	5798-ARD				X						
OS/TSO COBOL Prompter	5734-CP1							X			
OS/VS Capacity Management Aid	5798-CJB						X		X		
OS/VS Generalized Data Compare	5798-CEQ		X		X						

プログラム名	プログラム番号	情報検索	プログラム統制 文書化	アクセス統制	シミュレーション 検査	訓練	マネジメント統制	開設設計	分析	変換	障害回復
OS/VS Online Problem Tracking	5798-CNJ	X					X		X		
OS/VS Sort/Merge	5740-SM1	X									
Performance Tools - OS/VS 1	5796-PGL	X					X				
Performance Tools - OS/VS 2 (SVS)	5796-PGN	X					X				
PL/I D to PL/I Optimizer Conversion Program	5798-CKL									X	
PL/I F to PL/I Optimizer Conversion Aid	5796-AKG									X	
PMS IV Network Plotting Program	5796-PDE							X			
POWER/VS Cost and Performance Analyzer	5798-CDG						X		X		
POWER/VS RJE Controlled Access Monitor	5798-CPH			X							
Programming Language for IMS (PLIMS)	5796-PBF				X			X			
RCA COBOL to IBM ANS COBOL Conversion Aid	5798-AHT									X	
Register Audit for 3650 Retail	5798-BDK		X								
Resource Access Control Facility	5740-XXH		X	X			X				X
Resource Measurement Facility	5740-XXM	X					X		X		
SCRIPT/370	5796-PHL		X								
Service Level Reporter	5740-DC3						X		X		
SMF Graphical Analysis Program	5796-AFP						X		X		
SMF Job Data Compression Aid	5796-PHN						X	X	X		
SMF Selectable Analyzer	5798-AAR								X		
Statistics Generating Package	5798-AYY	X					X		X		
Storage and Information Retrieval - DOS/VS	5746-XR4	X	X								
Storage and Information Retrieval - STAIRS/VS	5740-XR1	X	X								
Storage Device Migration Aid	5796-PHP						X	X	X		
STREAM - 3270 Information Display System Programming Aid	5798-ANE							X			
Structured Programming Macros	5798-CLF							X			
SVS/MVS System and Job Impact Analysis	5796-AJF								X		
SVS Performance Tool (SVSPT)	5796-PGN								X		
System Activity Measurement Facility - MF/1 Post Analyzer	5798-CHX								X		
System/3 DOS/VS RPG II Conversion Preprocessor	5735-CV1									X	
System/3 RPG II to System/370 RPG II Conversion Aid	5798-CAA									X	
TERMTEXT/Format for System/370	5796-PBR		X								
Test Data Generator	5796-PBP		X		X						
Test IMS Utilities	5796-PBE		X		X						
Test IMS/VS Utilities	5796-PDA		X		X						
TP Network Simulator (TPNS)	5740-XT4				X			X			
TSO Codes Update	5796-PFR			X				X			
TSO Command Package	5740-XT6		X	X							

プログラム名	プログラム番号	情報検索	文書化 プログラム統制	保護 アクセス統制	検査 シミュレーション	訓練	統制 マネジメント	設計開発	分析	変換	[illegible]
TSO Command Processor System/370	5798-AYF							X			
TSO Interactive Data Entry Support for COBOL	5796-CLG							X			
TSO/IQRP Interface	5796-PHZ	X	X	X							
TSO/MSS Archiver	5796-AJK						X				X
TSO Programming Control Facility II	5798-CLW		X	X			X				X
TSO 3270 Display Support and Structured Programming Facility	5740-XT8							X			
TSO 3270 Structured Programming Facility	5740-XT2							X			
TSO/VS2 Program Control Facility	5798-BBJ		X	X							X
Using TSO Effectively	5798-CKW					X					
Utility Data Reducing Subroutines for System/360/370	5798-AZW										
VANDL-1 - DL/I Data Base Utility	5798-CDH										X
VIDEO Support Aids	5796-AKK							X			
VIDEO/370-DOS	5736-RC3	X		X							
VIDEO/370 Online Status Display	5798-CJA										X
VIDEO/370-OS	5734-RC5	X		X							
VM Facility/370 Performance Monitor	5798-CPX						X		X		
VM/SGP - Statistics Generating Package	5796-PDD		X		X		X		X		
VM/370 Control and Accounting Program	5798-AYP		X				X				
VM/370 Graphic Monitor	5796-PDT						X		X		
VM/370 Online Tape and Disk Libraries	5796-AGN		X	X							X
VSAM Access Subroutines (OS)	5796-AJW							X			
VSAM Access Subroutines (DOS)	5796-AJX							X			
VSAM Catalog List (DOS)	5798-ALQ								X		
VSAM Catalog List (OS)	5796-ALR								X		
VS/REPACK	5796-PDZ				X				X		X
VS1 Performance Tool (VS1PT)	5796-PGL								X		
VS/1 Utilization Monitor	5798-CAK		X				X		X		
Wideband Communication Program	5796-PDJ						X				
1419 Fine Sort	5798-BCN										X
3270 Formatting Feature	5796-PBD				X						
3600 Statistics and Message Log Reporting	5798-CLC	X					X		X		
370X Trace Editor Program	5798-CHZ										
3790/3770 PVS Data Set Test Support	5798-CPG				X						
3790 Code Generator Using TSO	5796-AJD							X			
3890 OS/VS Program Testing Aid	5798-CBG				X						

ストされる。リストに記載されたメッセージは差異を示している。両バージョンのリストのページ番号とステートメント番号は対応づけられている。統計情報は次のものを含む。

- ○ 入力ステートメントの数
- ○ 突合せ，削除，追加および変更の数

(3) 変更管理／追跡プログラム（CM／T）および変更追跡プログラム（CT）

変更管理／追跡プログラムは，実働適用業務ライブラリに加えられた変更の記録を保持する。この記録によって問題判別に要する時間を短縮することができる。変更追跡プログラムは，CPUを増設する場合，各増設CPUに対してライセンス・プログラムとして用いられる。

CM／Tの主な機能は次の通りである。すなわち，ユーザ指定のライブラリに加えられた変更を追跡し，変更情報をデータベースに記憶して，問題管理と変更管理に使用する。ユーザ指定のライブラリにある変更されたメンバのバック・アップ・コピーをとる。システム障害が起ったとき，ライブラリを迅速に再構成する。認可されていない変更かどうかを判定し，ソフトウェア上の問題と変更を管理する報告書を作り出す。

CTは次の機能を有する。連係編集プログラムとシステム・ユティリティに関する情報を，CPUごとに作成されるSMFのログに入れる。変更したモジュールのバック・アップを各CPUのライブラリに任意選択で入れる。

(4) データ抽出／処理／再構成システム

このプログラムは，記憶されたデータをある記憶システムの形式から，別の記憶システムの別の形式へ変更するために作られたものである。

データ変換とデータ抽出は，一般的に読取り，変換，および書出しのフェーズに分けて行われる。このプログラムを使用するユーザは，個々のプログラムを書くかわりに制御ステートメントを指定する。制御ステートメントでは，データを定義し，変換処理について記述する。

(5) 財務管理システム

財務管理システムは，報告書を作成して分析するために，企業の財務データにアクセスする必要のある人々を対象に作られたものである。このシステムでは，情報画面表示および印刷報告書として提示される。

主な機能は次の通りである。すなわち，既存のシステムから選択した情報を，それぞれの管理機能の要件に応じた処理レベルで，詳細に，または要約して処理する。報告書は，特殊な要件に合うように作成することができる。グループ別，会社別，部門／構成単位別，製品別，経費または財務状況別に明細書を提示する。また比較報告書を作ることができる。要求に応じて，決められた時期に，特定の報告書および要約報告書を作ることができる。

(6) ＩＭＳテスト・ユティリティ

このユティリティの目的は，ＩＭＳテスト・データベースおよびＯＳ，ＳＡＭテスト・データベースの作成，およびＩＭＳデータベースのリスト作成と比較を行なうため必要なプログラムを提供することにある。

ＩＭＳテスト・ユティリティを使用することにより，テスト・データベースを容易に作成することができる。同一のＩＭＳデータベースの二つのバージョンを比較して，相違点のリストを作成する。プログラム障害のあるデータベースを回復する。更新されたデータベースのリストを作成するとともに，ＩＭＳレコードの内容をセグメントごとの階層順に表示することができる。

2.4.4　分散処理とネットワーク化への対応

分散処理システムの環境で，システム監査を行なう場合，従来の監査に比べて難かしい点がある。それは，技術的に複雑で，遠隔地に散在する現場の状況をリアルタイムに検証する必要があることに起因する。

システム監査の目的のためには，一般に次の六つの分野の作業を行なう手段と情報を得ることが必要である。

- ○　データのアクセスと分析
- ○　トランザクションの追跡
- ○　リアルタイム処理の検証
- ○　プログラムとデータへのアクセスの性能評価
- ○　入力データの正確性
- ○　文書化の検証

次にこれらの項目について，分散処理システムを念頭において考えてみることにする。また，IBM 8100分散処理システムを例にとり，メーカの提供するシステム監査支援ツールについて述べる。

(1)　データへのアクセスと分析

監査人はこの作業を主に例外データを選別するために行なう。これによって例外を発生させている状況を検証することができる。またもう一つの目的は，定常的なデータをサンプリングによって選び出すためである。

複数の分散処理システムが遠隔地にあって，同様の処理プログラムを幾つか走らせているような場合，標準的な質問形式のプログラムはデータ選別に有益な役割をはたす。IBM8100分散処理システムでは，DMS（DPPXの開発管理システム）のpsudo-queryの能力が監査プログラムの作成に役立つ。

適当な監査プログラムが準備されたならば，監査人はDSXを使って，遠隔地の装置内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，リストを収集することができる。またDSXを使って監査人は，遠隔地の分散処理装置に監査用プログラムをロードすることができる。次に監査人は，ロードしたプログラムを，ホスト側に居ながらHCF（ホスト・コマンド機能）を使って

サイン・オンし，端末機の機能を実行することができる。監査プログラムのこのような使い方は，監査人のみができるようにしておく。

(2) トランザクションの追跡

監査人はシステムを通るトランザクションの流れを追跡して，それらが他のトランザクションにどのように影響するか，または他のサブシステムにどのように渡されるかを調べる。この作業は，すでに入力されたトランザクションに，訂正や取消が行われる場合に特に重要である。

オンライン・システムにおいては，一つのトランザクションが，複数のトランザクションに影響を与えることが多い。このため，サブシステムの境界を越えてデータが流れる状況の追跡と，それの統制の存在を確認することが関心事となる。

分散処理システムでは，適用業務サブシステムの境界は通信回線の区分と合致していることが多いので，ネットワークの機能や制御の手順を形成するハードとソフトの働きを検査することによって目的が達せられる。

体系化されたネットワーク・システムにおいては，メッセージの送達とエラー・チェック，バッファリングと再送などはネットワーク制御プログラムによって行われる。そのため適用業務プログラムは，高レベル言語で単純化して記述することができるので，監査人にとってもプログラムは理解し易い。

IBM8100分散処理システムは，DPPXからユーザIDや日付／時刻を受けとることができる。監査人はこれらの情報を，トランザクションの跡付けをするための手がかりとして使用する。またDPPX／DTMS のデータベース・マネージャは復旧のためにデータベースの動きを記録したり，エラー状態を詳細に通知したりすることができるので，問題判別の有力な手がかりが得られる。さらに監査人は，分散処理システムにおける適用プログラムの正しさを検証するためにITF法を使用することができる。

(3) リアルタイム処理の検証

監査人は，リアルタイムの状況で行われる処理が，システムの仕様に合致して反復的に，信頼性をもって行われるかどうかを検査する。

IBM8100分散処理システムのDPPXでは，プログラムの各モジュールが変更または修正されると，アッセンブラ・プログラム・エディタの働きによって，無変更インディケータがリセットされる。LISTMOD コマンドは変更されたモジュールを簡単に識別するためのコマンドであって，監査人は承認なしにプログラムが変更されたかどうかを検査することができる。また起動が自動で行われたか，手動で行われたかを示す印が内部的にセットされるようになっている。

COBOLコンパイラは再入可能なプログラムを作り出すことができる。実行時に変化しそうな値は，プログラム中ではなく，データ作業域に入れられるので，適用業務プログラムのロジックは，実行時に変更されるようなことはない。監査人はこの機能が無効にされていないかどうかを検証する。

DPPXのデータベース・マネージメント・システムのもとでは，すべての入・出力機能がDTMSの管理によって行われるので，適用業務プログラムが特権機能を実行することはできない。IBM8100分散処理システムのメモリ・アドレス方式は，各モジュールの範囲内でのみアドレスが可能なようになっているため，その範囲外への分岐命令は作り出すことができない。

前述したDSXの機能を用いて，監査人は遠隔地の装置に入っているプログラムを，ホストに戻してコピーし，無許可で変更が行われていないかどうかを比較検査することができる。

(4) プログラムとデータへのアクセスの性能評価

監査人は，システムに内蔵されているプログラムやデータが，偶然もしくは故意に失われたり，変更されたりしないことを確めようとする。このためには最初，アクセス制御が適切に機能しているかどうかを調べる必要がある。分散処理システムでは，中央のセンタと比較して，いろいろな面で処理システムの管理が手薄になりがちである。

ネットワーク・システムはユーザにIDとパスワードが割り振られているので，アクセス制御（たとえばRACFによる）が正しく使われているかどうかを調べる。IBM8100分散処理システムでは，アクセス制御用ソフトウェアにお

いては，各ユーザについて，権限を登録したプロフィールが作られており，どのシステム資源にどのユーザのどのようなアクセスが許されるかを示している。このようなユーザ・プロフィールにはそれぞれデータ・セット，データベース，適用業務プログラム，DPPXコマンド，カタログなどについてアクセス権が定義されているので，サイン・オンに続いてアクセス制御が行われる。

またHCFの機能を用いることにより，遠隔地の分散処理装置におけるオペレータ・メッセージをホスト側の端末機に回送することができるので，どのようなオペレータ操作が行われているかを，監査人は知ることができる。

さらに分散処理装置では，各種のアクセス制御機能に加えて，任意機構としてのロック・キーを取付けることができる。キーの設定によって，オペレータは電源のオン・オフを除いて他のスイッチ類の操作ができないようになる。また固定ディスクやコネクタへのアクセス，およびフレキシブル・ディスクの自由な取りはずしを禁止する手段を講ずることができる。

(5) 入力データの正確性

監査人は，システムに入力されたデータが正確であるかどうかをチェックするため，エラー発見の手段とそれの有効性を評価する。すなわちエラー発見のためのデータ編集機能が適切であるかどうかをテストし，原始伝票と照合して未発見エラー率を見さだめる。

IBM8100分散処理システムでは，COBOLとDMS／DPPXの機能の組合せによって，表示端末機の画面上でカーソルの位置決めを行ない，フィールドへの英・数・漢字の入力を指定することができる。このような機能によって，データ入力と編集は簡便化され，入力時のミスを少くすることができる。また入力ミスが発見された場合には，表示のハイライト機能によって，間違いのあるフィールドを目立たせることができる。この際，正しく入力されたフィールドのデータは不用意に変更されないようにしておく。

DPPX／DTMSのデータベース・マネージャは，適用業務システムの設計において，必要ならば入力されたフィールドの属性を固有なものとして，その属性を自動的にチェックしエラーを発見できるようにすることもできる。DPPX／

DTMSは，トランザクションの入力を途中で放棄するような場合のために，更新または挿入以前のデータを念のために保持させておくことができる。

エラー入力をオペレータに知らせるためにブザーをならしたり，キーボードのファンクション・キー配列が使い易くなっているかどうかも検査の対象となる。

(6) 文書化の検証

監査人にとって最後の関心事は，システムに関する文書記録がタイムリに更新され，正確であるかどうかを評価することであり，さらに規定や手続がシステムの目的や運用上の規準に準拠して制定されており，しかも遵守されているかを調べることにある。

IBM8100分散処理システムは,この作業を容易にするためにCOBOL，DMS，DTMSのリスティング形式は，システム／370に良く似たものにしている。

一方，DPPXではすべてのオペレータ・メッセージやコマンドをログし，それらによってとられた動作の記録が跡付けできるようになっている。発生したエラーは別個のエラー・ログに保存され，Display Error Log コマンドを使って，監査人はエラーの状況を時間軸に対して調べることができる。

以上のIBM8100分散処理システムの各種機能は,ユーザとデータ処理部門のために提供されたものであるが，監査の人々にとっても有効であることは云うまでもない。

2.5 監査ツールの新技術

本節では，新たに開発すべきシステム監査支援ツールについて述べる。ここで述べるツールは，従来から言われているシステム監査の，実施面での効率化を目標としている。現状でのシステム監査は多様であるので，ここで提案する新ツールは，すべてのシステム監査に役立つとは言えないかもしれないが最大公約数的なシステム監査を念頭に置いて，新しいツールの検討を行った。

第2.5.2項では，既存技術の若干の改良で実現できる新ツールを提案し，第2.5.3項では，新しいコンピュータ技術（知識工学）の応用可能性について述べる。

2.5.1 新技術開発上の課題

(1) 応用システムのセキュリティとシステム監査

本章の冒頭（第2.1節）で，応用システムのセキュリティ対策として，システム監査をとりあげた理由を述べたが，ここでもう一度，応用システムのセキュリティとシステム監査の関係について総括しておく。

第2.2節で，システム監査の型は大まかに2つに分類されている。それは，

①システムの安全性・信頼性に重点を置いたシステム監査

②システムの効率性に重点を置いたシステム監査

である。応用システムのセキュリティと関連するのは，上記①である。そして，システム監査の範囲は，広義には，システム計画段階，開発段階，運用段階および保守・管理のシステム構築から廃棄までのすべてに渡ると報告されている。さて，このシステム監査を内部監査としたうえで，応用システムの外側から眺めて見よう。やや乱暴ではあるが，図2－3のように見える筈である。この図から日常の運用と，システム監査とは鶏と卵の関係になっていることが分り，「事前」とか「事後」という見方は，実際はあまり意味がないことが分る。

すなわち，応用システムのセキュリティ対策は，日常の運用（事故・犯罪の防止体系）とシステム監査（防止体系のチェックおよびコントロール）の2本柱で成り立つと，考えなければならない。応用システムのセキュリティ対策の半分は，システム監査であり，残りの半分が日常の運用における防止である。

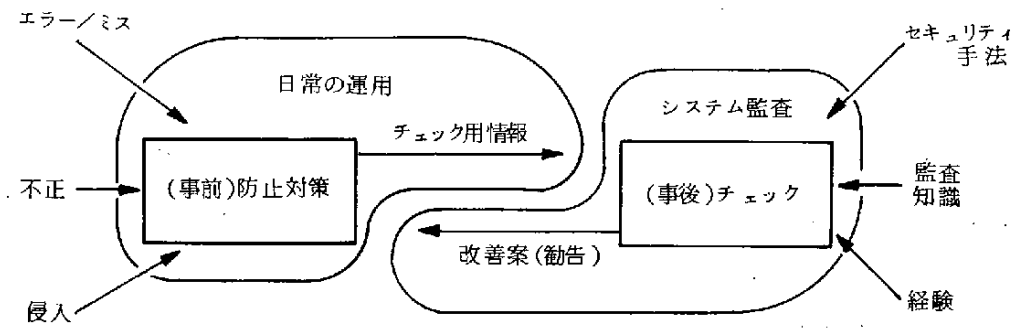


図２－３　応用システムのセキュリティ対策

各種の防止対策は，この日常の運用に組込まれて効果を表す。そして防止対策の中で，技術的な手法あるいは装置（ハードウェア）を，当プロジェクトではセキュリティ技術と呼び，昨年度（昭和５７年度）に検討したのであった。

(2)　システム監査支援ツール

業務処理時における技術的防止対策と同じ発想で，システム監査に組込可能な技術的手法を考案すると，それがすなわちシステム監査支援ツールになる。このツールは，主にシステム監査の作業性を改善するのに役立つのである。システム監査の実効があがれば，応用システムのセキュリティ対策が向上するのは，前述(1)の結論から明らかである。

しかし，通常システム監査支援ツールは，セキュリティの向上に寄与するのにもかかわらず，セキュリティ手法あるいは技術とは言わない。そこでもう一度，図２－３を見てほしい。各種の事前防止技術は，常に各種の侵害と直接接している。それに対して，システム監査支援ツールは，システム監査に奉仕するだけである。システム監査支援ツールは，事故や不正防止の計画に役立つのであり，事故や不正を直接防止するツールではない。いわば，間接的セキュリティ技術である。そのため，システム監査支援ツールは，一見セキュリティ技術には見えないこともある。

例えば，ＩＤカードによる本人確認機構は，見るからにセキュリティ技術である。しかし後述する，システム監査支援ツールとしてのロギング機構は，セキュリティ技術のようには見えないだろう。

しかし，応用システムのセキュリティ対策の２本柱として，業務処理時の防止対策とシステム監査を考えるならば，システム監査支援ツールもセキュリティ技術（やや広い意味で）である。

(3) システム監査支援ツールの役立つ領域

システム監査の領域は，第2.2節に示すように極めて広い。しかし，システム監査支援ツールの有効な領域は，それ程広くない。ここで検討するツールは，コンピュータを用いることが原則であり，主な入力情報は，コンピュータ化されている業務処理の情報に限定される。事前防止手法のような，抽象化された知識をコンピュータに入力する手段は，現状ではないからである。

その結果，「組織体制および運営方針」とか「システム化計画」等のような範囲は，システム監査支援ツールの有効領域から除外され，結局「稼動中システムのサポート」（例えば効率測定）とか「アプリケーション・システムの有効性」（例えば，業務処理結果のチェック）等が，システム監査支援ツールの有効領域になる。

ここで，実際のシステム監査に目を向けてみよう。理想は理想として，実際にシステム監査を実施する場合には，多数の問題点のあることが第2.3節で指摘されている。その対応策として，第一に，標準的な実施基準の必要性が報告されている。また，実施する場合の道具として，いろいろな局面で役立つツールが必要であり，現状のツールでは不充分だと報告されている。

しかし，先に述べたようにシステム監査支援ツールの適用可能領域は限られており，あらゆるシステム監査の領域に対して，ツールを構築することは困難である。従って，標準的なシステム監査に対応させて，汎用ツールを構築しようとするアプローチは，無意味であることが分かる。

(4) 最大公約数的システム監査実施手順と支援ツール

前述したように，システム監査を調査分析した結果

① システム監査支援ツールは，広い意味でのセキュリティ技術であること。

② システム監査の領域は広いが，ツールが適用できる部分は狭いこと。

③ 現状のシステム監査支援ツールの機能は不充分であること。

④ 標準的なシステム監査は，現存しないこと。

等の結論を得た。当プロジェクトは，このような現実を考慮した結果，新しいシステム監査支援ツール構築の第一歩として，最大公約数的システム監査実施手順を検討した。その結果を図２－４に示す。かなり大胆な把握であるが，コンピュータ支援の可能な領域に限定して表すと，図２－４のようになる。図のⓐからⓒに向うに従って，多様性が増加し，またⓒの段階ではツールの必要性は少ない。従ってⓐとⓑの段階に適用するツールが検討対象となる。

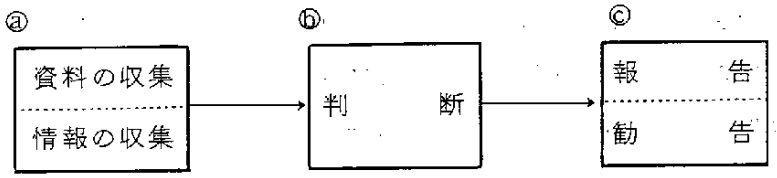


図２－４　最大公約数的システム管理実施手順

次に，我々は市販のツールの調査結果について分解してみた。そのために図２－４のⓐの部分を，図２－５に示すように分解した。

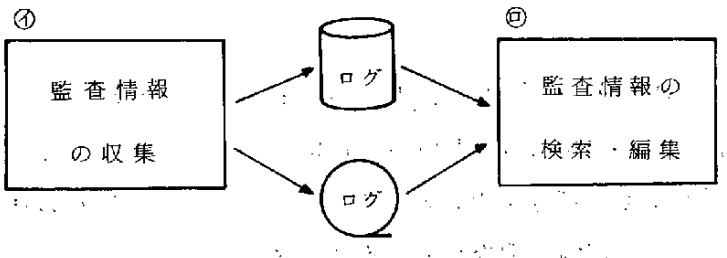


図２－５　資料／情報の収集段階

ここで，第2.4節の報告と突合してみると，市販のツールの大部分は，図2－5の㊁に属していることが分る。図2－4のⓑに対応するツールは極めて少なく，第2.4節では，各種の「ファイル・コンペア」が紹介されているだけである。一方，図2－5の㋑の部分に適用するツールも少ない。この理由を分析してみると，だいたい次のようなことが言えるようである。

① 図2－5の㋑（ロギング）のツール

この部分は，OSあるいはアプリケーションの一部として機能させる必要があり，汎用を第一とする市販のソフトウェア・パッケージは，インタフェースをとるのが困難である。本質的に汎用パッケージを適用しにくい部分である。

② 図2－4のⓑ（判断）のツール

人間の行う判断は，極めて複雑かつ抽象的で，コンピュータのロジックで実現することが非常に難しい。

上記の①と②は，実はシステム監査支援ツールの大きな問題点である。加えて，市販のツールは，図2－5の㊁に使用できるツールは多数あるものの，その操作性にはかなり問題があると言われる。これらの問題点こそ，我々の解決すべき課題である。

(5) 短期的課題

第2.4節で，分散処理システムにおけるシステム監査支援ツールが紹介されている。このようにOSと一体化してメーカが提供する方式は，重要な解決策である。その結果，図2－5の㋑のツールで問題となるインタフェースを吸収し，更に㊁の部分まで一環した機能を提供している（厳密には，図2－4のⓑも一部含む）。

我々は，同様な発想のもとに，専用ハードウェア化を検討した。最近のハードウェア技術の進歩により，専用ハードウェア化が容易になったことと，処理効率をはじめ多くの利点が生じるからである。さらに，既存の技術の応用で実現可能なので，短期的に開発できる利点もある。

具体的には，ロギング・ツールを検討した。ロギング・ツールは，図2－4

からも分るように，すべてのシステム監査支援ツールの入力部分を構成する重要な部分である。第2.3節でも触れられているように，現状でのロギング方式には，2つの大きな問題点がある。記録されたデータの安全性と，ロギング処理の効率の問題である。

ログ・データは，日々の業務処理結果を蓄積するため，容量の関係で一般的に磁気テープに記録保存される。しかし，磁気テープの取扱いには，人手が必ず必要である。磁気テープの保存については物理的対策により，有効な安全対策が可能であるが，磁気テープの取扱時の安全性については，取扱者を全面的に信用する以外にない，というのが大きな問題である。処理量の多いシステムでは，磁気テープの交換は頻繁にあり，常に管理者による監視を行うのは，事実上不可能である。

効率上の問題は，大規模システムで顕著になっている。現在この対策として，収集情報を減らすことが一般的に実施されているが，当然，システム監査にとっては好ましくない対策である。ここで一例を示す。現状でのロギングでは，ファイル（あるいはデータセット）へのアクセス情報は記録されるが，レコードへのアクセスについては，一般的に記録されない。しかし監査上，特定のレコードへのアクセス記録がどうしても必要な場合がある。

金融機関では，レコードへのアクセスについても記録している。多数の顧客の預金データ等が，一つのマスタ・ファイルに収集されているからである。ただし，この記録をとることはかなりの負担になっている。都市銀行等では，1日当りのレコードへのアクセス回数が，数百万回を越えるからである。もちろんレコードへのアクセスを記録するロギング・システムは，通常のＯＳには付属していないので，アプリケーション・システム構築時に，ユーザ作成のサブシステムとして組み込んでいる。そこで，当プロジェクトでは，これをアプリケーション・ログと呼んでいる。しかし，アプリケーション・ログは，ＯＳを構成するサブシステムではないため，保護レベルが低いという問題点が生じている。

記録量が多いことは，さらに多数の問題を引き起こす。最初に保管上の問題

がある。量が多いため，物理的スペースの問題が発生し，保管場所の管理にも人手が多く必要になる。さらに，この多量のデータを検索するのも容易ではない。しかし，記録量を減らすことは本質的に無理なので，これらの諸問題を解決する技術的手段が必要だと思われる。

第2.5.2項で，新しいロギング技術の検討結果を説明する。

(6) 長期的課題

前述のロギング・ツール以外のシステム監査支援ツールとして必要なのは，

① より機能や操作性のすぐれたログ・データの検索／編集ツール

② 図2－4の⑥の判断の段階に適用できるツール

である。しかし現状のコンピュータを用いる限り，今以上の機能を持つツールは不可能ではないかと考えられるのである。ここでは，"検索指令をカードからディスプレイ端末にした"とか"ディスプレイをマルチ・スクリーンにする"等の改善は，大きな進歩とは考えずに，もっと画期的な改良を目標にしたい。そのかわり，長期的な研究開発が必要になるが，新しいコンピュータ技術の応用を前提にできる。それは，知識工学である。

第2.5.3項で，知識工学の応用例を説明することとし，以下に知識工学をとりあげた背景を説明する。

① ノイマン型アーキテクチャの限界

システム監査を実施する場合は，多種類の資料を比較照合して適切な判断を行うというプロセスが，最も工数が多く必要でかつ最も重要である。会計監査のように，比較照合すべき情報の多くが数値の場合には，現在のコンピュータ（ノイマン型コンピュータ）でも，支援システムを構築できる可能性はある。

しかし，システム監査の場合には，数値でない情報も多くあり，算術的手法を用いることができず論理的処理が主体になる。例えば，課金ファイルへのアクセス情報を考えてみよう。この情報には，ⓐ誰が，ⓑ何処から，ⓒ何時，ⓓどのファイルに，ⓔどのようにアクセスしたかという5つの要素がある。何故という6つ目の要素は，これからシステム監査者が調査して求める

結論にしておく。さて，ⓐ～ⓔまでの事実を評価して，次の推論に入るための情報を得るロジックには，最低5回の判断が必要で，現状のコンピュータ・アーキテクチャでは，図2－6に示すように，32通りのケースを想定しなければならない。(実際はもっと複雑になる。)

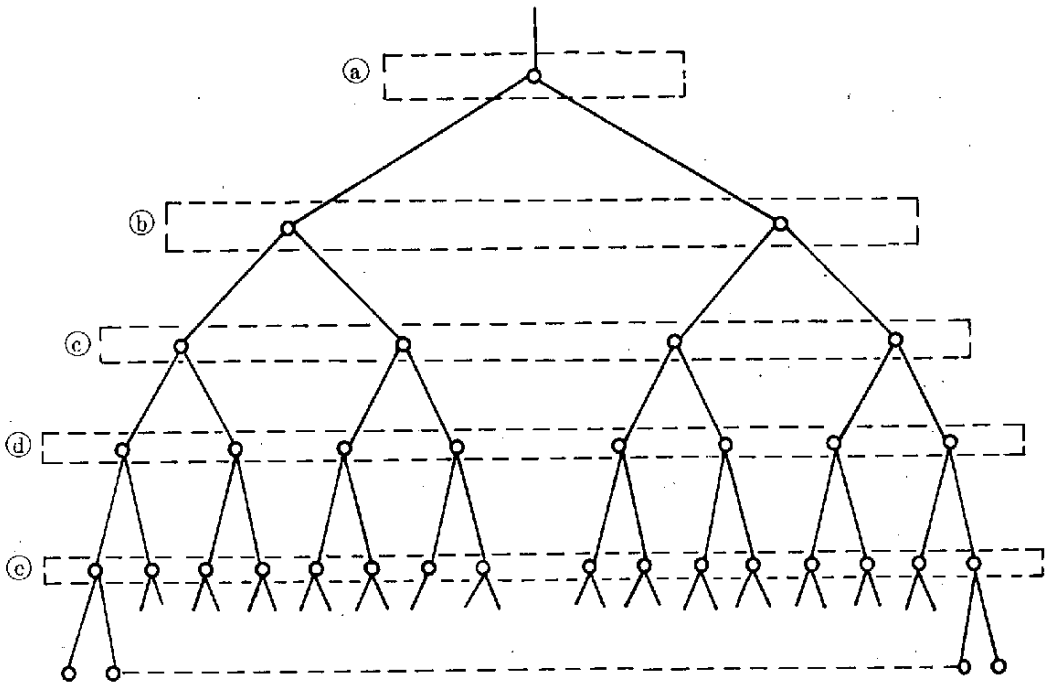


図2－6　5つの要素の判定

このように，たった一つの事実を分析して，次の探索戦略を決定するだけでも，これだけ複雑になってしまう。実際のシステム監査では，いくつもの事実を判断して結論を得るのであるから，膨大なロジックが必要になると予想される。このようなプログラムは，事実上作成不可能と言っていいだろう。

もう一つ問題がある。システム監査のような推論では，ある予定戦略で進めた推論が，途中で情報不足等のため行詰ることがある。この場合，別の戦

略を立ててやり直す（試行錯誤）必要があるが，現状のコンピュータ・アーキテクチャは，このような推論を想定して設計されてはいない。無理矢理実現することは可能であるが，効率が悪化してしまう。

以前から現在のコンピュータは，単純な作業を繰返すプロセスに最適であると言われてはいたが，以上のような理由で，新しい思想に基づくコンピュータが必要だという結論になる。

② 打 開 策

考えられる打開策として，知識工学の応用がある。知識工学の詳細は，専門書に譲るが元々，人間が行う推論をコンピュータで行うために考え出されたもので，人工知能とも呼ばれる。そして，それを実現する具体的なコンピュータを，第５世代コンピュータと呼び，１９９０年代の実用化を目指して，世界各国で研究開発が続けられている。

現在，まだ決定的な構造は確立されていないが，知識ベースと推論機構を内蔵しているのが特徴である。第５世代コンピュータでは，図２－６の判断構造を要素（図２－６のⓐ～ⓒ）に分解して，抽象化した知識として保持しておけばよい，というのが最大の利点である。判断要素の組立ては，実行時（推論をする時）にコンピュータが自動的に行うのである。この結果，これまで複雑すぎて実現できなかった複雑な判断ロジック（推論）が，容易に構築できると言われている。前評判の良さは少々割引きして考えるにしても，システム監査支援ツールに応用する価値が，充分あるのではないかと考えた。

2.5.2 短期課題（ロギング技術）

本項では，第 2.5.1 項の(5)で述べた新しいロギング・ツール －「ロギング・サブシステム」－ の検討結果を説明する。

(1) 構 想

オンライン・システムのジャーナル，システム・ログ（SMF）等，システムの運転状況，ファイル／レコードのアクセス情報，あるいは各種の監査用情報等を記録するログ専用のサブシステムを，新ツールとして提案する。

このサブシステムを組み込んだ応用システムは，図２－７の構成になる。このサブシステムは，それ自身で障害対策／セキュリティ対策が施されており，メイン・システムでは，高信頼高速記録装置として認識することになる。従来のように，ジャーナル／ログの障害対策を考慮する必要がなく，また，超高速の書込みが可能なため，シリアル動作で充分機能する。このため面倒なパラレル動作を必要としない。さらに記録を読み出す時も，書込が完全シリアル動作で実行されるため，完全な時間軸に沿ったデータが得られる。

装置の専用化，新記録媒体および無人運転により，ログ・ファイルのセキュリティ対策を強化できる。このような狙いを持ったサブシステムである。

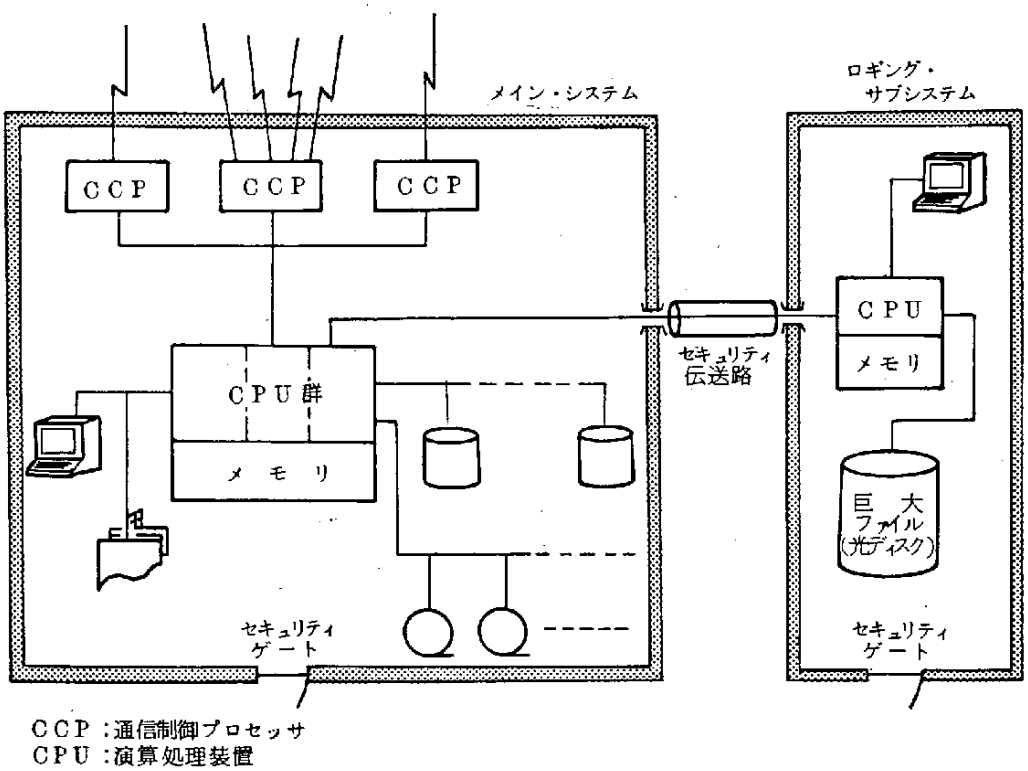


図２－７　ロギング・サブシステムを付加した
オンライン・システムのセンタ

(2) オンライン・システム向ロギング・サブシステムの概要

大規模オンライン・システム向ロギング・サブシステムは，高信頼／超高速／大容量を同時に実現するサブシステムであり，物理的大きさやコスト等は多少犠牲にして設計される。基本的なハードウェア構成例を図２－８に示す。技術的な開発課題は，２次系ファイルの大容量化と高信頼化である。

小規模オンライン・システム向ロギング・サブシステムは，大規模向サブシステムの基本技術を用いて，小規模オンライン・システム向に構成し直したサブシステムである。基本的なハードウェア構成例を，図２－９に示す。記録ファイルは，シリコン・ディスク（バッファ・ファイルとして使用）と光ディスクの２層構造であるが，速度を要求されない場合は，シリコン・ディスクを用いない（単層になる）。

これらのロギング・サブシステムは，オンライン・システムだけでなく，バッチ・システムにも適用できる。

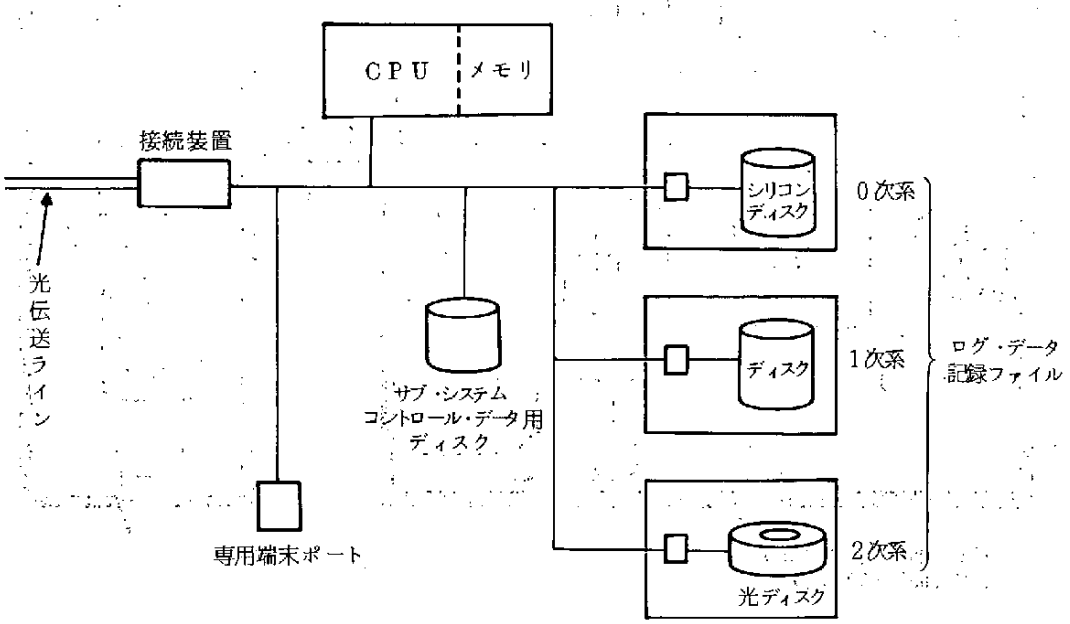
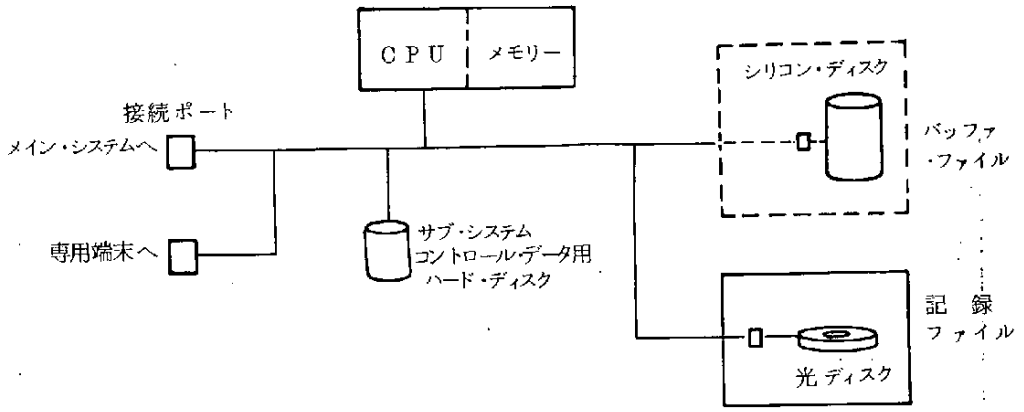


図２－８　大規模オンライン・システム向ロギング・サブシステムのハードウェア構成例



バッファ・ファイル ： シリコン・ディスク　1メガバイト
記録ファイル　　： 光ディスク　　1ギガバイト程度
(媒体交換式，再書込不可)

図２－９　小規模オンライン・システム向ロギング・サブシステムの
ハードウェア構成例

① 大規模オンライン・システム向ロギング・サブシステムの機能目標

１日当りの記録量が，１ギガバイトを越えるような大規模システム向である。また当日中に記録されたデータへの高速アクセスおよび，過去半年程度の間に記録されたデータへの低速アクセスを可能とする。総容量は1,000ギガバイト以上必要である。

このサブシステムは，メイン・システムのファイルのバックアップとして機能できるようにし，メイン・システムで障害が発生した時，リカバリ用データを供給可能とする。加えて，このサブシステムはそれ自身で検索機能を保持し，例えば監査専用端末を接続してシステム監査者が独自に資料を収集できるようにする。さらに，自動運転を原則にし，メイン・システムと同時に運転する。２次系ファイル（図２－８を参照）の媒体交換は自動であるが，例えば毎日１回書込済媒体の搬出と，未記録媒体の搬入およびセットを行う。以上の機能目標を，表２－５にまとめて示す。

表２－５　大規模オンライン・システム向
ロギング・サブシステムの機能

項　　目	目　　標
総　容　量	1,000ギガバイト以上，最終ファイル（２次系ファイル）は媒体自動交換式
記録速度	短　時　間　：　１０メガバイト／秒以上 連　　続　：　１メガバイト／秒前後
検索時のアクセス速度	１００ミリ秒以下：最新データ１ギガバイト以内 １０秒以下　　：全データ
故障によるシステム停止	実用的にゼロ
検索機能	○専用端末から検索可能 ○非専門家向言語による検索 ○標準検索システム内蔵
運転方式	メイン・システムに同期した自動運転

② 小規模オンライン・システム向ロギング・サブシステムの機能目標

スーパー・パソコン／スーパー・ミニコン等によるシステムに適合するよう設計する。低コストを目標にするため，主に信頼性の面で，大規模システム向よりも設計基準を緩くする。例えば，予備装置の内蔵を止めて，障害時は運転を一時停止してリカバリすることを原則にする。

光ディスクの媒体は，手動交換としてコストを削減する。ただし，光ディスク１枚当たりの容量が大きいため，交換頻度は極めて低くできると考えられ，実質的な無人運転が可能であろう。機能目標を表２－６に示す。

表２－６　小規模オンライン・システム向
ロギング・サブシステムの機能

項　　目	目　　標
総　容　量	１ギガバイト以上，記録媒体は手動交換式
記録速度	連続：１００キロバイト／秒前後 （オプション：1メガバイト／秒，バッファ・ファイル付加時）
検索時のアクセス速度	１００ミリ秒以下
故障対策	一時処理停止後，リカバリ処理
検索機能	○専用端末から検索可能 ○非専門家向言語による検索 ○標準検索システム内蔵
運転方式	メイン・システムに同期した自動運転可

(3)　ロギング・サブシステムの意義

このサブシステムが，コンピュータ・システムの効率上のネックの解決に寄与することは明かであるが，ここでは，セキュリティ上の効果について述べる。

①　このサブシステムは，ログ・ファイルの保護対策を強化可能であるが，このことは，システム監査上重要な意味を持っている。ログを用いて，例えば不正の調査を行う場合，ログ・ファイルの記録が正しいことは前提条件であるが，従来のシステムでは，このことが必ずしも成立しないということが既に指摘されていた。ＴＳＳサービス・システムでは，課金データの改ざんが実際に行われたことがあり，さらにその改ざんの証拠を一切残さないことも可能であると言う。これは，ほんの一例でありその他にもログ・ファイルの安全性を脅かす要素は多数存在する。

ロギング・サブシステムは，

○　無人化による，物理的保護（専用ルーム化）が可能になる。

○　光ディスク（再書込不能型）の使用により，本質的に改ざんに対して強くなる。

等のように，ログ・データ保護の強化が可能になり，システム監査者は安心してログ・データを利用できるようになる。

② このサブシステムは，量の問題に対しての解決策に成り得る。ログ・データをシステム監査に用いる場合，きめの細い記録が必要であるが，従来は記録ファイルの容量とシステムの処理速度が壁になって，例えばレコードへのアクセス情報を記録するのは難しい課題であった。先に述べた金融機関のシステムは，例外中の例外であり，通常のシステムでは，レコードへのアクセス情報は記録されない。その結果，プログラム・ファイルへのアクセスは把握できても，どのプログラム（モジュール）を修正したのかは，SMF 等をいくら調べても分らないというのが実情である。

ロギング・サブシステムは，大容量記録が特徴であり，従って，レコードへのアクセス情報も記録可能である。その結果，ログ・データを調べるだけで，どのプログラムを修正したかも判別可能であり，修正されたプログラムだけを例えば，ファイル・コンペアで保存リストと比較し，適切な判断ができるだろう。この結果，従来より作業効率が向上することは明らかである。従来は，ファイル・コンペアですべてのプログラムを保存リストと比較することにより，修正されたプログラムを把握可能ではあったが，修正者や時間を把握することはできなかった。ロギング・サブシステムを用いれば，それも可能になる。

③ きめの細いデータが記録されていれば，将来，検索技術や判断技術が進歩した時，さらに画期的なシステム監査支援ツールを構築できる可能性も生じる。その意味では，ロギング・サブシステムは，システム監査支援ツールの基本的システムと言えよう。

(4) 技術的課題

ロギング・サブシステムは，既存技術の組合せで構築できるような設計が目

標であるが，新たに開発すべき技術も多少ある。以下にそれを示すが，いづれの技術も短期間（３年程度）で，開発可能と思われる。

① 高信頼な光ディスク装置

② 高信頼システムの構築手法

③ ２重化できない部分（例えば，正副ファイル装置切り換え器等）の高信頼化

④ 障害検出技術

⑤ ＶＬＳＩ化などによる装置全体の軽薄短小化

⑥ サブシステムのソフトウェア（特に，アクセス・コントロール，大容量ファイルのデータ管理／コントロール）

⑦ メイン・システムとのインタフェース

2.5.3 長期的な研究開発が期待される技術

本項では，第2.5.1項の(6)で述べた，新しいコンピュータ技術（知識工学）の応用について検討した結果を述べる。

知識処理を実現する新しいコンピュータ（第５世代コンピュータ）は，１９９０年代の実用化が予測されているが，まだかなり先のことである。従って，ここで述べるシステム監査支援ツールの実現も，かなり先になってしまうのは止むを得ない。したがって，今回はまだ具体的構造まで検討したわけではないので，抽象的な説明になることを，あらかじめお断りしておく。

(1) 知的検索・編集

現存するシステム監査支援ツールの検索／編集機能に，問題点が多いことは，第2.5.1項で述べた。その問題点を知識処理によって解決しようというのが，以下に述べる検索／編集ツールの目的である。

最初にツールの概観を説明する。図２－１０に，機能ブロックを示す。知識ベースにはログ・データベースの構造に関する知識および検索／編集に関する知識が蓄積されている。検索指令を入力すると，この知識を活用して，ログ・データベースを検索し（実際は，推論機構の指示に基づき，ロギング・サブシ

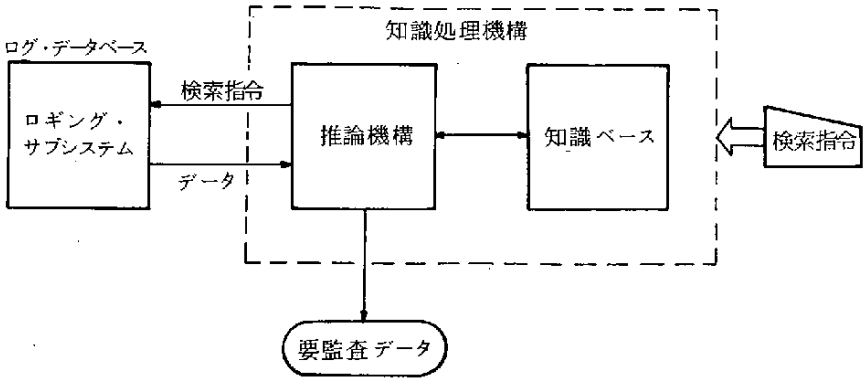


図２－１０　知的検索・編集

ステムがログ・データベースにアクセスする。），結果を出力する。

次に，このツールの特徴について説明する。従来，検索するための条件は厳密に定義しなければならなかった。それでも数値条件であれば，特に難しい問題があるわけではない。例えば，「支払額が千万円以上のもの」等のような条件では検索可能であった。

しかし，論理条件では難しい問題があった。例えば，「機械類の出荷額」という条件を仮定してみる。問題は，「類」である。もし，機械類だけがまとめてファイルしてあれば簡単であるが，そうでない時は「機械類とは何か」を考えて，検索ロジックを作成しなければならない。

このような検索の必要性はいくらでもある。すなわち「月末日の出荷額」，「欠損発生日」，「異例取引の検索」，…… etc。これらは，多大な労力を投入すれば，現状のコンピュータでも可能な検索ではあるが，実用性に欠ける。

知識処理では，これらを容易に実現できる可能性がある。パターン認識とかパターン理解が可能になるからである。その結果，曖昧な条件から検索ロジックを自動生成できる。もちろん，そのための知識はあらかじめ知識ベースに入力しておかなければならない。知識の入力方法は，実は大きな問題になってい

る。しかし，その解決方法は現在活発に研究されており，明るい見通しであるという。知識の自動獲得の研究もされており，非観的になる必要はないだろう。

この検索は，見方を変えればサンプリングである。しかし単純なサンプリングではなく，知的サンプリングである。

(2) システム監査コンサルテーション・システム

検索システムの最も高級な検索条件は「不正取引の検索」である。このような条件を投入できるシステムは，もはや検索システムではなく，コンサルテーション・システムである。このシステムは，まったくの夢物語ではない。原理的には現在研究開発が進められている「故障診断コンサルテーション・システム」と同じだからである。先に述べた知的検索／編集の発展型と考えてもよい。

図２－１１は，システム監査コンサルテーション・システムの機能ブロック図である。ログ・データベースの中から，知的検索／編集によって，調査対象を絞り，次に高度な推論を行って，不正取引を発見する。このシステムでは，知識ベースの更新をある程度自動的に行う。例えば「不正」の結論が出た業務処理が，事実として不正の場合には，操作者の指示（多分「正解」と入力する）で不正の業務処理から，その特徴を抽出する推論を行い，知識ベースを更新する。

知的検索／編集は，知能が低い段階，コンサルテーション・システムは，知能が発達した段階と言うこともできる。従って，重要なのは知識である。ログ・データベースに記録されているデータを用いて，判断できるものであれば，知識を交換することで，何でも処理できる。例えば，不正に関する知識を投入すれば不正の検出を，システム効率に関する知識を投入すれば，システム効率の自動測定を行ってくれる。さらに，システム開発の知識を投入すれば，システム開発時のコンサルテーションも不可能とは言えない。

さらに野心的な使い方もある。システム監査コンサルテーション・システムの出力を，業務処理システムのセキュリティ機構にフィードバックすれば，セキュリティ機構の自動更新が可能になる。例えば，リミット・チェックのチェック値の自動変更，パスワード入力ミスの許容回数の自動変更等が簡単にでき

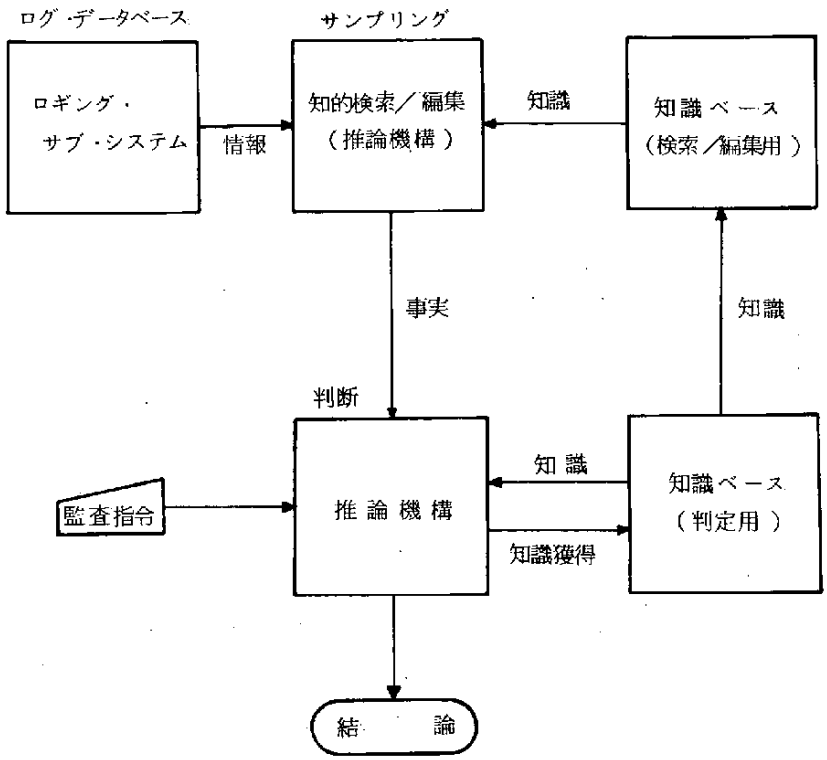


図2－11　システム監査コンサルテーション・システム

る。チェック機構の自動作成／削除等というのも可能になるかもしれない。

第1章で，セキュリティ機構のチェック（検証）には，侵入テストが最も有効であると述べられている。通常，侵入テストを行うためには，かなりの労力が必要であるが，稼動中の応用システムは，特別な作業を実施しなくても，毎日侵入テストを受けている（のと同じである）。ただし，テスト量があまりに多いので，通常評価していないだけである。システム監査コンサルテーション・システムは，この評価を効率よく行ってくれる。これまでの説明で，以上のことは納得できるだろう。しかし弱点もある。このシステムは，コンピュータに入力されたデータだけを用いて判断するため，システム全体が詐欺にかかる可能性がある。そのため，人間による追跡調査が時々必要である（未来のシステム監査？）。

実現を疑問視する向きもあるかもしれない。しかし，夢のようなシステムが，

意外に早く実現してしまうことは，よくある（コンピュータもそうだった）。少なくとも第五世代コンピュータ乃至は知識ベースの活用例の１つとして検討する価値は充分あると考える。

3. コンピュータ・ネットワーク・システムのセキュリティ

通信回線の自由化が進んだ昭和58年には，今までになく大きなコンピュータ・ネットワーク利用の変化が起きた。

それまで，一つのコンピュータ・システムを中心とした，あるいは一企業内に留まっていたオンライン・ネットワーク網を，さらに外部へ広げるのは多年の課題であったが，昭和57年10月の第二次回線開放を起爆剤として，長い間あたためられていたシステム構想が急速に具体化し始め，多数のシステムの拡張が始まった。しかしながら，必ずしもそれらが総て順調に発展しているとは言えない。

通信回線の制度以外にも，オンライン・ネットワーク網の外部への拡張を阻む要因があったからである。コンピータのエラーあるいは悪用による影響が，社会的混乱を引起こすのではないかと心配されていた。わが国より一足早く網の拡張を行った米国では，多数の新手の犯罪が報告され，わが国の関係者を臆病にしたきらいもある。

しかし，省エネ／省資源という厳しい条件下での社会・経済の発展を考えた時，コンピュータ・ネットワークの拡張による高度な情報処理の実現は，必要不可欠であり，エラーの防止や悪用の阻止は，必ず解決しなければならないもっとも重要な課題である。当プロジェクトは，昨年度からこのテーマに取組み，基本的な問題点の検討を行なった。そして，問題点を解決できる可能性のある一つの構想を導き出すに至った。本章では，それを詳細に説明する。

この報告をきっかけとして，各方面で多数のより理想に近づいた対策案が検討され，コンピュータ・ネットワーク・システムのセキュリティ問題が解決されることを期待する。

3.1 概　要

3.1.1 調査研究の経緯

(1) 調査研究の出発点

当プロジェクトは，コンピュータ・システムのセキュリティ対策の確立を目標として調査研究を開始したが，現実のコンピュータ・システムでは，複雑な回線網を用いたオンライン・システムが常識となっており，当然のこととして，回線網もセキュリティ対策研究の対象となった。

日本のオンライン・システムは，専用網（特定通信回線）の使用から始まり，最近になって公衆網（公衆通信回線）の使用が増えてきた。業務処理システムという観点では，初期の自社内のシステムとして閉じたオンライン・システムから，同系列会社（あるいは子会社）等と結合した，やや開いたオンライン・ネットワーク・システムへと変化してきた。今後，他社との結合に向うと予測されている。

このようなシステム構成の変化に伴い，いろいろな面で，例えば同系列企業との結合／他社との結合等で，有利な網である公衆網の利用が増加したとも考えられる。そのようなニーズの変化に応じて，データ通信に適した公衆網であるＤＤＸ交換網[*1]が開発され，さらに次世代の網であるＩＮＳ[*2]の開発計画も進んでいる。以後，交換網（メッセージ交換の機能のある網）を用いた一企業内で閉じていないコンピュータ・ネットワーク形態を，開放型汎用網と呼ぶ。また，一企業内で閉じた専用オンライン網を，閉域型専用網と呼ぶ。

さて，閉域型専用網におけるセキュリティと，開放型汎用網におけるセキュリティとでは，性質が異なるという結論に達したのは，昨年度（昭和57年度）の検討が半ば進んだ頃であった。閉域型専用網が私道であれば，開放型汎用網は，

＊1：ＤＤＸ…デジタル・データ交換網（既にサービスを開始している）

＊2：ＩＮＳ…高度情報通信システム（現在，開発中）

公道である。私道と公道では管理運用が異なるのと同様に，閉域型専用網と開放型汎用網では，かなりの特性の違いが予想された。そのため，開放型汎用網のセキュリティについて，別途検討を開始した。

開放型汎用網によって多数の応用システムが結合した広域システム全体を，コンピュータ・ネットワーク・システムと呼ぶことにする。コンピュータ・ネットワーク・システムでは，巧妙な犯罪が発生する恐れがあり，当プロジェクトは，それに対する対策を中心とした検討を進めている。尚，コンピュータ・ネットワーク・システムでの犯罪については，「昭和57年度コンピュータ・システムのセキュリティに関する調査研究報告書第Ⅱ部4章1節」を参照されたい。

(2) 昨年度（昭和57年度）の検討結果

通常，ネットワークのセキュリティとは，ネットワーク上のメッセージのセキュリティを，意味する場合が多い。このメッセージは，ネットワーク自身の必要性ではなく，そのネットワークに接続しているコンピュータ・システムあるいは端末での必要性に基づいて，送受信されている。従って，あるメッセージをセキュアに伝送すべきかどうかは，送受信者が決定する。このような解決では，ネットワークのセキュリティに，ネットワークだけではなく，ノード，ホスト，端末等も関係していることになり，広域システム全体のセキュリティ問題として検討する必要が出てくる。すなわち，コンピュータ・ネットワーク・システムのセキュリティである。

昨年度は，このような観点で検討を進めた結果

① 閉じたシステムから開いたシステムへ向う。

② その結果，ネットワーク全体の強力かつ統一的な管理が次第に困難になる。

③ その間隙をついた，ネットワーク参加者自身による詐欺の可能性が高まる。

④ それの防止はもちろんのこと，発見さえも困難になってくる。

等を指摘し，予想される詐欺の具体例（図3－1を参照）について言及し，技術的対策として，セキュリティ・ボックスを提案した。

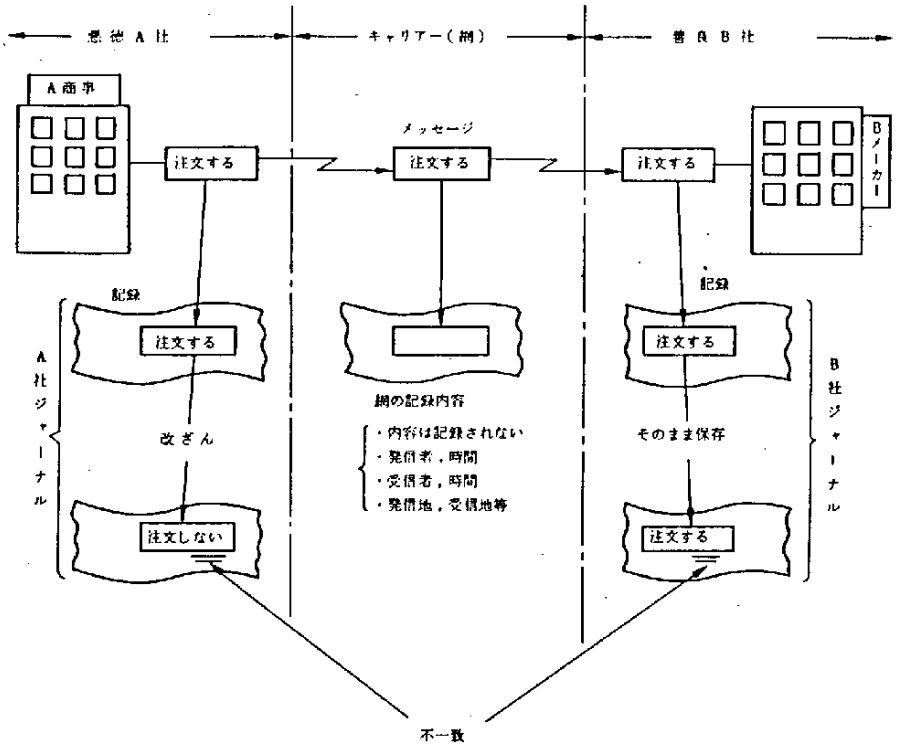


図３－１　メッセージの改ざん

（出典：「昭和５７年（出典：「昭和57年度コンピュータ・システムのセキュリティに関する調査研究報告書」）

もう少し詳しく説明すると次のようになる。昨年度の検討は，いくつかの不確定要素を無視して，多数のコンピュータ・システムが参加するネットワーク・システムの形態を予測することから始めた。各コンピュータ・システムでは，ネットワークに接続するため，純技術的な問題点の解決および利用方式に関する最少限の統一を行う必要があるが，利用者間の話合いで充分解決は可能と思われ，特に検討対象とはしなかった。これでメッセージの送受信は可能になる。

しかし，何かの原因でトラブルが発生した場合，例えば，あるシステムで予定していた他のシステムからのメッセージが到着しない場合，難しい問題が生じる。受信者は，トラブルの発生場所が，ネットワーク上なのか，送信者内部なのかを区別できない。原因を一方的にネットワークに押付けて解決すること

は可能であるが，そのかわり，何らの補償処理も期待できない[*1]。そのメッセージの重要度が高ければ，送信者か受信者に大きな損害が発生する危険性がある。

この弱点を積極的に活用すれば，完全犯罪も不可能とは言えない。そのため，①アプリケーション・レベルで保障を行うネットワーク・システム全体の管理者を定めるか，②それに代わる技術的手段が必要になる。

①の方式の具体例として，全銀システム[*2]等がある。このシステムは，同業企業で構成され，参加数も10^2のオーダなので，可能だったと考えられる。しかし，今後のネットワーク・システムは，異業種を含む広域システムとなり，参加数も10^4に達すると思われる。個人が参加すれば，さらに数が増え，かつ，接続システムも，パソコンから超大型まで予想される。そのため，新しい技術的解決手段が必須になるだろう。

このような想定で問題点を分析した結果，メッセージを文書の代わりに利用した業務処理では，誰もが納得のできる証拠を残すことが重要であるという結論を得た。

その証拠を残す技術的手段として，セキュリティ・ボックス（通信メッセージ・ロギング装置）を提案した。（図３－２参照）

尚，詳細は，「昭和57年度コンピュータ・システムのセキュリティに関する調査研究報告書第Ⅱ部４章１節」を参照されたい。

(3) 今年度（昭和58年度）の検討

昨年度提案のセキュリティ・ボックスは，有効な方式であると確信しているが，実現上の問題，特に技術的問題が多いことも事実である。

予備的検討で，

＊１： 通信回線が原因とされるトラブルの多くの実際の原因は，利用者側のシステム（端末）にあると言われる。現状では，通信回線のトラブルによる被害について，回線供給者が補償するような制度はない。

＊２： 都市銀行を通信回線で結び，他行為替を通信回線のメッセージで処理する集中型ネットワーク・システムである。
最近業務を拡大し，また都市銀行以外の金融機関も参加するようになってきている。

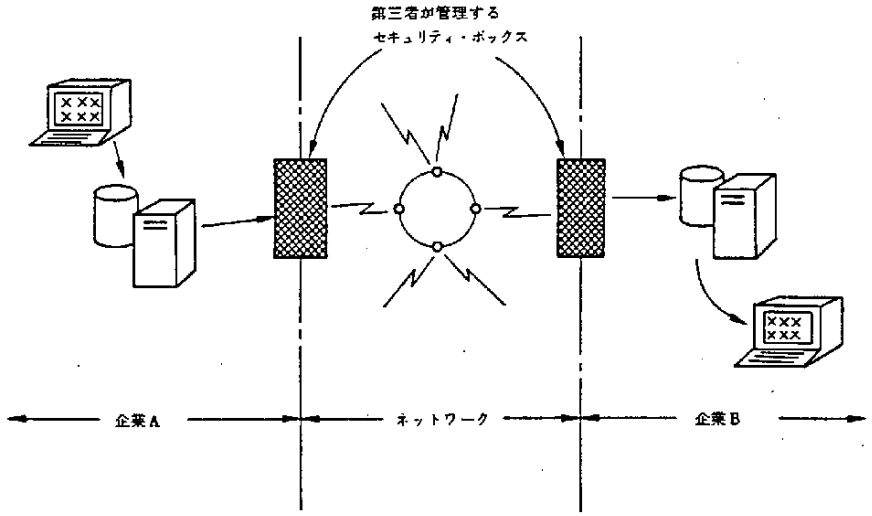


図３－２　セキュリティ・ボックスの概念

（出典：「昭和57年度コンピュータ・システムのセキュリティに関する調査研究報告書」）

① 信頼性

- 証拠としての使用に堪え得る信頼性（十分に低い故障率，記録データの保全性）
- 第３者が運用する予定のセキュリティ・ボックスは設置台数が多くなり，無人運転が前提となる。

② 容　量

- 長期に渡り無保守で運転するために必要な大容量記憶装置
- 必要な時に，必要なデータを迅速に検索可能なファイル管理技術

③ 外観／コスト

小規模ユーザでも使用できるように，物理的大きさが小さく，ローコストでなければならない。

等の問題を分析した結果，現在の技術レベルを考慮すれば，不可能ではないが容易ではない，長期的には実現可能であっても，短期的には悲観的にならざるをえないという結論を得た。セキュリティ・ボックスは，一つの方法であって

唯一の方法ではない。今年度は，他の方式の可能性を調べるため，もう一度，ネットワーク・システムの特性を見直すことにした。

ネットワーク（メッセージ伝送網）のセキュリティ対策の理想は，ネットワークの完璧な信頼性（無故障），そしてメッセージの完全な保全／機密保護である。これらが，極めて容易にかつ日常的に可能になれば，ネットワークのセキュリティ対策の議論は消滅するだろう。ただし，これは遠い夢の話ではある。このような純粋なセキュリティを追求するのは，それなりに価値がある。一方現実的に，ある条件下でのセキュリティを追求するのも有用である。この目的は，実現性を高めることと，コストの引下げである。我々の目標とするセキュリティ対策でもある。

以上のことを踏まえ，次に示す4つの問題を検討することとした。

① 第1の問題は，先に述べた技術上の問題である。より実現性が高い方式を検討する必要がある。

② 第2の問題は，ネットワーク・システムの利用方法である。エラー，ミス等はともかくとして，犯罪が起きるためには，それなりの動機がなければならない。すなわち，犯罪を起こしたくなる程魅力に富んだ業務処理が，本当にネットワーク・システムを利用して行われるかである。

③ 第3の問題は，魅力に富んだ業務処理が存在するならば，その業務処理によってどのようにネットワーク・システムが使用されるかである。言い換えればセキュリティ上重要なメッセージは何かである。

④ 第4の問題は，上記1～3の問題に対する解答を踏まえたネットワーク・システムの形態である。

3.1.2 今年度の検討内容

(1) ネットワークの使用目的

当プロジェクトは，最初に，コンピュータ・ネットワーク・システムを利用して行われる業務処理について，検討した。我々の目標とするコンピュータ・ネットワーク・システムは，図3－3のような全体像を持ち，少なくとも5年

以上先の構築になる高度情報処理体系である。ユーザには，金融機関，メーカー，商社等，多種多様な業種が予測され，個人の参加さえも予想される，汎用ネットワークである。

このような複雑なネットワークのアプリケーションを把握するため，多種多様な多数の機関／企業が結合した場合，どのような業務処理[*1]を行うと効果があるかという検討から出発し，我々が想定しているコンピュータ・ネットワーク・システムの使用目的を定めることとした。

図３－３の体系で，処理される可能性のある具体的業務として分り易いのは，例えば，ＥＦＴＳ[*2]がある。ＥＦＴＳは，金銭移動を表す帳票[*3]を，コンピュータ・メッセージに置き換えたものである。同様な考え方で，昨年度の報告では，商業活動に伴う帳票（例：契約書，発注書，領収書等）のコンピュータ・メッセージへの置き換えを仮定した。今年度も，同一の仮定をしたが，大胆な仮定だけに，そのような業務処理が実際にも実行される可能性があるかが問題になる。

これについては，実態調査を行って確かめることにした。その結果の詳細は，第3.2節に示すが，ここで簡単に結論をまとめると，次のようになる。実際にも，商取引をコンピュータ・メッセージで行うとする試みがあった。加えて，今後の機械化の中心テーマとして期待されていること，解決しなければならない課題の一つとして，セキュリティ問題があること等が判明した。以後これを，「商取引の帳票のコンピュータ・メッセージ化＝電子化伝票による取引」という意味で，電子化取引と呼ぶことにする。

もう一つの別の調査結果を以下に述べる。ＥＦＴＳや電子化取引では，それぞれ，金銭の移動，商品の移動（移動の約束）を表す情報，すなわち事実（証拠にもなる）を表す情報であり，価値の移動を表す情報である。それに対して、

＊１　効果のある業務処理が実際にも行れるという想定である。

＊２　Electric Funds Transfer System

＊３　現状のＥＦＴＳでは，コンピュータ・メッセージと共に，帳票も存在する。

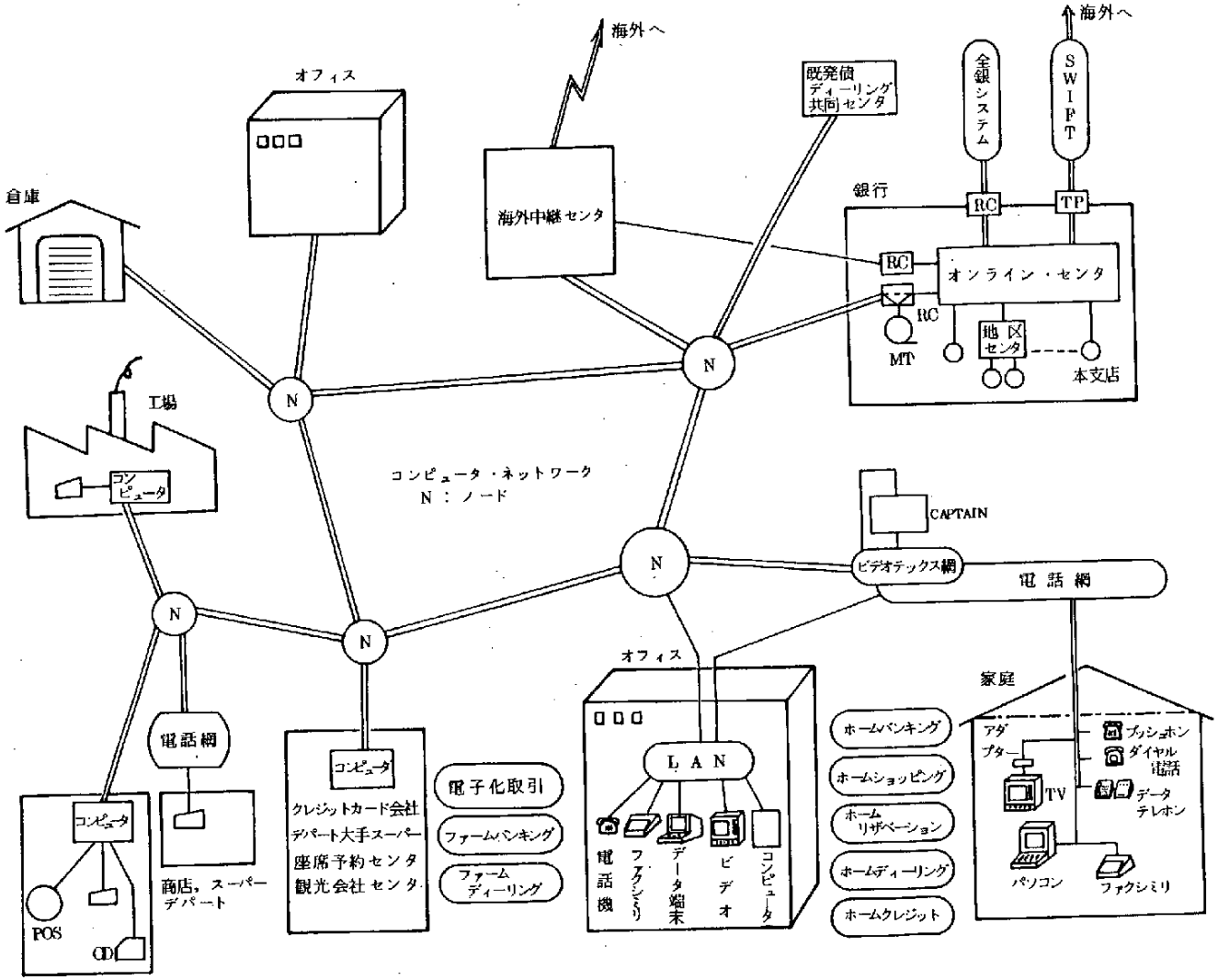


図３－３　高度情報処理体系

情報そのものが価値を保持している（あるいは商品である）場合がある。例えば，データベースに保存されている論文，各種の統計資料，市況情報……等である。ＥＦＴＳや電子化取引の情報は，たとえ当事者以外に洩れても，価値の移動という事実が知られるに過ぎない[*1]。一方，情報そのものが価値を持っている場合には，情報が洩れることは，お金が盗まれることと同じ意味になる[*2]。従って，ネットワークを利用して情報交換を行う場合には，そのセキュリティ対策が非常に重要になり，また今後このようなネットワーク利用のニーズが増加すると考えられる。

以上のことから，コンピュータ・ネットワーク・システムの業務処理（具体的な使用目的）として

- ＥＦＴＳ／ファーム・バンキング
- 電子化取引
- 高付加価値情報の交換／売買

等を，仮定することができた。

(2) セキュリティ対策の基本方針

ここで交通安全の話に言及する。道路交通の安全対策を，すべて道路管理者に任せるというのは，一つの方法である。また道路管理者は，常に安全性の向上に努力するであろう。一方で，安全性を特徴とした運送業も考えられる。荷主が，自身のトラックで荷物を輸送する場合に，もし，事故に遭えば当然荷主がその事故の責任をとらねばならない（すなわち荷主の損害になる）。もし，「高安全運送業」に荷物の輸送を依頼していれば，たとえ事故が発生しても，補償されるというメリットがある。「高安全運送業」は，高付加価輸送という分野で，ビジネスとして成り立つ。

以上の原理を，コンピュータ・ネットワーク・システムに置き換えてみよ

＊１：　例えば，ＥＦＴＳの場合，お金が盗まれるわけではない。ただし，事実が洩れるのが問題になる場合もある。

＊２：　暗証が洩れることは，印鑑が盗まれることと同一になる。

う。「高安全運送業」と同一の発想で，ごく普通の通信回線を利用し，これに特別なからくりを施した高信頼のハードウェアを結合し，信頼のおけるソフトウェアでコントロールし，さらに，整備された運用で，「高安全メッセージ運送業」が成り立ちそうである。これが対策の基本方針である。配達範囲は，もちろん戸口から戸口までである。

この発想にも泣き所がある。荷物の輸送では，荷物という物理的物体の移動をもって，輸送済の証明が可能であるが，メッセージ伝送では，メッセージの伝送をもって，伝送済の証拠とすることはできない。メッセージは，手に取ることはできないし，放っておけば，すぐ消えてしまう。この問題を，どのように解決するかは，今年度検討の中心的テーマである。我々は，この解決策として，公証機関によるメッセージ交換の記録およびメッセージの保存を考えた。詳細は，第3.3節に示す。

(3) 実現技術の問題

昨年度検討したセキュリティ関連基本技術の中から．さらに詳細な検討を必要とする基本技術として，

- 通信回線に関する技術
- 暗号化に関する技術
- メッセージ認証／端末確認に関する技術

等をとりあげ，開発状況および将来動向について分析した。

その結果，いづれの技術も既に実用化しているか，近い将来の実用化が確実化されていた。しかし，実用化の方式は，必ずしも当プロジェクトが期待しているような方式ばかりではない。例えば，暗号装置の多くは，モデム対向型で用いるようになっており，ネットワークと有機的に結びつけるような応用に向いていない。この辺りに，新技術開発の必要性がある。

もう一つ考慮しておくべき重要な項目として，標準化動向がある。最近，全銀協，ＩＳＯ，ＣＣＩＴＴ等で，ネットワークのセキュリティ対策を，標準化しようという動きがある。これらについても調査を行った。これらの標準化の動きと，我々の目標とするコンピュータ・ネットワーク・システムとの関係につ

いて，今後十分に検討する必要があるだろう。

以上の，ネットワーク・セキュリティ関連基本技術の調査結果の詳細は，第3.4節を参照されたい。

(4) セキュア・ネットワーク構想

当プロジェクトは，実際的な応用（あくまでも仮定であるが）におけるセキュリティ上の問題点の検討から出発し，技術的な対策の実現可能性について予測を行った結果，一つのセキュア・ネットワーク構想を構築した。この構想を「ネットワーク・セキュリティ・センタ構想」と呼ぶことにし，以下にその概要を説明する。

① セキュリティ上の問題点

我々は，実応用の仮定として，

- ＥＦＴＳ／ファーム・バンキング
- 電子化取引
- 高付加価値情報の交換／売買

を設定したが，これらの応用におけるセキュリティ上の問題点として，次の4点を指摘することができた。

ⓐ 送信先，受信先の確認
　メッセージの保全（改ざん対策）　} すべての応用に共通の問題

ⓑ メッセージの機密保護（漏洩対策）
　…… 特に，高付加価値情報の交換／売買で重要な問題

ⓒ メッセージ伝送に関する証拠（送受信先，時刻，内容等のセキュアな記録）
　…… 他人（他企業）とメッセージの交換を行う場合は必須項目

② 技術面からみた総合的対策（ネットワーク・セキュリティ・センタ構想）

我々は，前述①の3つの問題点を解決する方法として，一つの総合的対策案を作成した。その概略は次のとおりである。

先のセキュリティ上の3つの問題には，セキュリティ要素技術を組み合わ

せて対応する。その要素技術とは，

- 暗号化技術
- メッセージ認証技術
- 端末確認技術

等である。しかしながら，運用上の問題から，信頼できる公的な第3者の機関（メッセージの交換を専門的に行う機関）の存在が，どうしても必要になった。この機関は，「高安全メッセージ伝送業」とも言えるもので，当プロジェクトはこの対策案を「ネットワーク・セキュリティ・センタ構想」と呼ぶに至った。

この第3者の機関は，ユーザの要望に応じて，戸口から戸口までメッセージを伝送する。そして安全性に関して，いくつかのメニューがあり，メッセージ毎に自由に，ユーザーが安全性のレベルを指定する。例えば，メッセージの改ざん対策だけを指定したり，漏洩対策も含めて指定することもある。これらの改ざん対策・漏洩対策等は，ほとんど技術的に実現される。使用する通信回線は，ごく普通の通信回線であり，必ずしもこの機関所有の通信回線ではない。一般の回線を用いて高付加価値通信を行う機関である。

この提案は，一つの試案である。運用上の問題は言うまでもないが，技術上の問題でも，まだつめの足りない部分が多い。

しかしながら，この章で取り扱った高度情報処理システムの安全対策の効果は大きいことが予想されており，今後の高度情報化社会の円滑な発展のためにも，国家的課題として，今すぐにでも開発研究を開始すべきであると思う。詳細は，第3.5節を参照されたい。

3.2　コンピュータ・ネットワークの利用動向

本節では，セキュリティ対策の検討に先だって行った実態調査の検討結果についてまとめる。応用現場でのコンピュータ・ネットワークの利用動向について調査を行い，コンピュータ・ネットワーク利用の実態を把握し，企業間ネットワークのニーズを検討することが目的である。

尚，今年度の調査は国内で行った。海外の動向については文献その他を参考にして行った。

3.2.1　商取引への応用

(1)　企業内システムから企業グループ間結合へ

我国における本格的なオンライン・システムは，東京オリンピック（1964年：昭和39年）から始まったと言われている。初期のオンライン・システムは，集中型のシステムで，種々の制約から，小規模なものであった。回線構成もネットワークと呼べるような代物ではなかった。

この段階における応用は，自社内業務の機械化であったが，自社内業務の機械化では，この項のテーマである商取引への応用とは，言い難い面がある。商取引の中心的処理は，他の企業との商談や事務処理であり，自社内で閉じたオンライン・システムの利用では，その機械化に限界がある。当時，この事が意識されていたかどうか分らないが，企業グループ間を通信回線で結ぼうとする動きが出てきた。これを可能にしたのが，昭和46年（1971年）の第一次回線開放である。

この結果，親会社と子会社のコンピュータを結ぶことも可能となり，1970年代には，例えば，オンライン受発注システムのような応用システムが構築され始めた。オンライン受発注システムを用いると，以前のように，子会社で入力した発注データを一度出力し，親会社へ運び再度入力するという無駄がなくなり，入力ミスも減少する等のメリットがあった。

また，親会社に集中型のデータベースを構築し，グループ企業で共同利用を

行うという新しいシステムが出現した。それ以前の我国では，情報の持っている価値について特に意識されていなかったが，この頃から，次第に重要視されるようになり，企業グループの持っている情報を有効に使おうという発想に応えたシステムであった。

ハードウェア面から見ると，親会社を中心としたスター状のネットからリング状のネットへ，さらに公衆通信回線網の利用へと変化し，いわゆるコンピュータ・ネットワークと呼べる形態になった。昭和50年（1975年）のコンピュータ白書によれば，コンピュータの設置台数は約26,000台であり，オンライン化しているシステムの内の10％程度は，他システムとの接続があったことが，読み取れる。

金融機関では，この時代に早くも，全銀システム，ＮＣＳ等のような，企業グループを越えた同業他社との相互結合を行うシステムが出現し，以後，コンピュータ・ネットワーク化の牽引車としての役割を果たしている。

1980年代に入り，パソコン及びローカル・エリア・ネットワーク（ＬＡＮ）が導入され，各企業とも，オフィス・オートメーション（ＯＡ）を目標として，さらに徹底した機械化が進められた。パソコンとＬＡＮは，それまで小規模すぎて導入が困難であった企業にも，コンピュータ・ネットワークを普及させ，ネットワークを通じたデータ交換を可能にした。こうして現在では，大企業から中小企業まで，コンピュータ・ネットワークは大きな役割を担っている。

しかし，他企業あるいはグループ外企業との間の業務処理（例えば商取引）では，依然として，書類方式による手作業が行われており，機械化上のネックになり始めている。補助的に，記憶媒体（磁気テープ，フロッピ・ディスク等）の交換が行われているにすぎない。もちろん，グループ企業内でも，すべての帳票をコンピュータ・メッセージに置き換えたペーパーレス処理が行われているわけではないが，最少限の帳票によるコンピュータ・メッセージ中心の業務処理が行われていて，手作業との差は歴然としている。

(2) 他企業との結合

自社のシステムと他企業のシステムを結合[*1]させることは，コンピュータによる機械化の範囲を大きく拡大させる。特に，商取引への応用では効果が大きい。

従来のように，一企業内で閉じたシステムでは，相手企業との情報交換を必要とする段階で，どうしても機械化された処理が跡切れて，迅速性／省力化が十分達成されない。また結合相手は，多ければ多い程，より大きな効果が得られる。今日，一つの相手先としか取引を行わない企業は少ないからである。

そこで，多数の企業間を経済的に結合する方式 ── コンピュータ・ネットワーク・システム（図３－４を参照）── を構築しようという動きが活発になってきた。現在これを実現する技術は十分にあるが，まだ大きな壁がいくつか存在する。それは，

① プロトコルの統一，メッセージ・フォーマットの統一の問題

② 制度上の問題

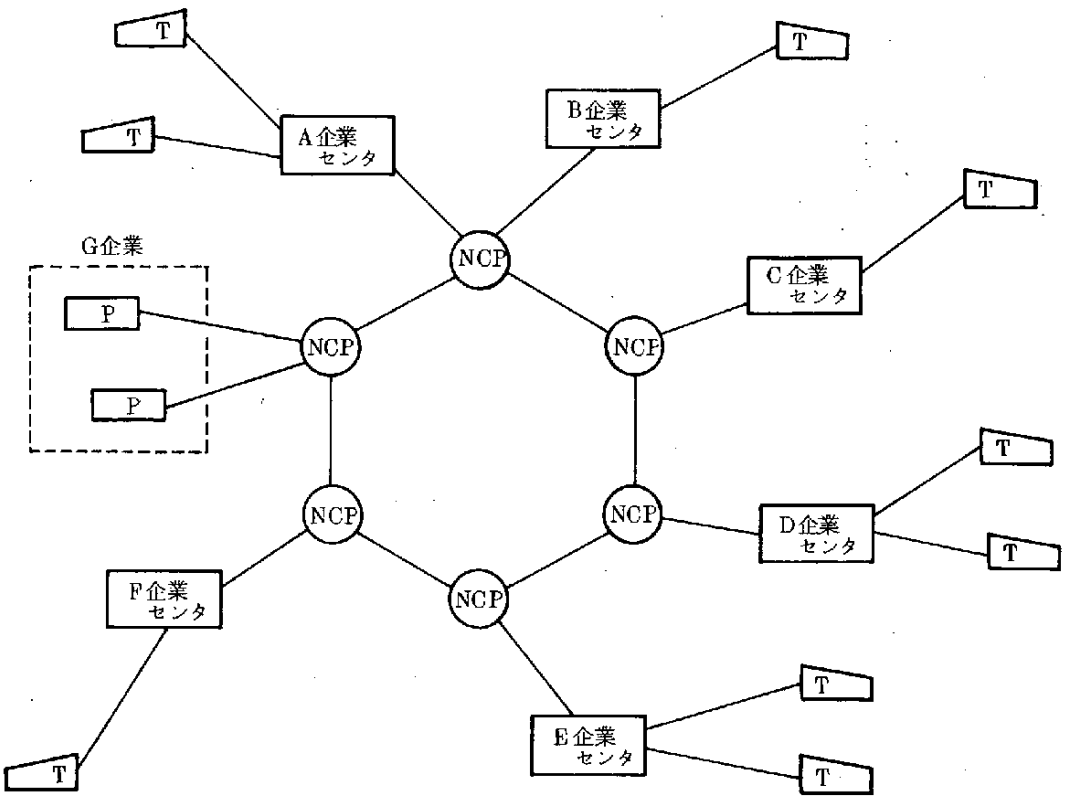
③ セキュリティ上の問題

である。上記の②の問題は，昭和57年10月の第二次回線開放で，半分取り除かれた。①の問題についても解決すべく努力が続けられており，見通しは明るい状況である。難しい問題は，③だと言われている。

実際には，既に他企業と結合したネットワーク・システムがある。それは，ＴＳＳ等を用いる会話型のオンライン・データベース検索サービス等である。これは，図３－５に示すように，メーセージの流れが限定されており，後述する企業間結合例とは，少々異なる。しかし米国では，不正接続の試みが跡を絶たないという。データベース内の情報は公開情報なので，不正接続が発生してデータの漏洩があっても破壊されない限り，被害は小さい。そのため，セキュリティ対策は比較的容易であった。（従って，複数企業間の接続が早期に実行されたとも考えられる。）これに対し，商取引メッセージは，データ量は小さくても大きな価値を動かす可能性があり，セキュリティ対策は非常に重要である。

＊１： オンライン結合を意味する。

一つの解決策は，原則に逆行するが，互いに信頼できる企業同志で，ネットワーク・システムを構築する方式である。最初から接続を限定することによって，災いの源を締め出す方式である。昭和58年には，この方式で，グループ企業を越えた企業間接続が実現された。



NCP：ネットワーク・コントロール・プロセッサ
T　：入出力端末
P　：パーソナル・コンピュータ

－4　リング状ネットワーク

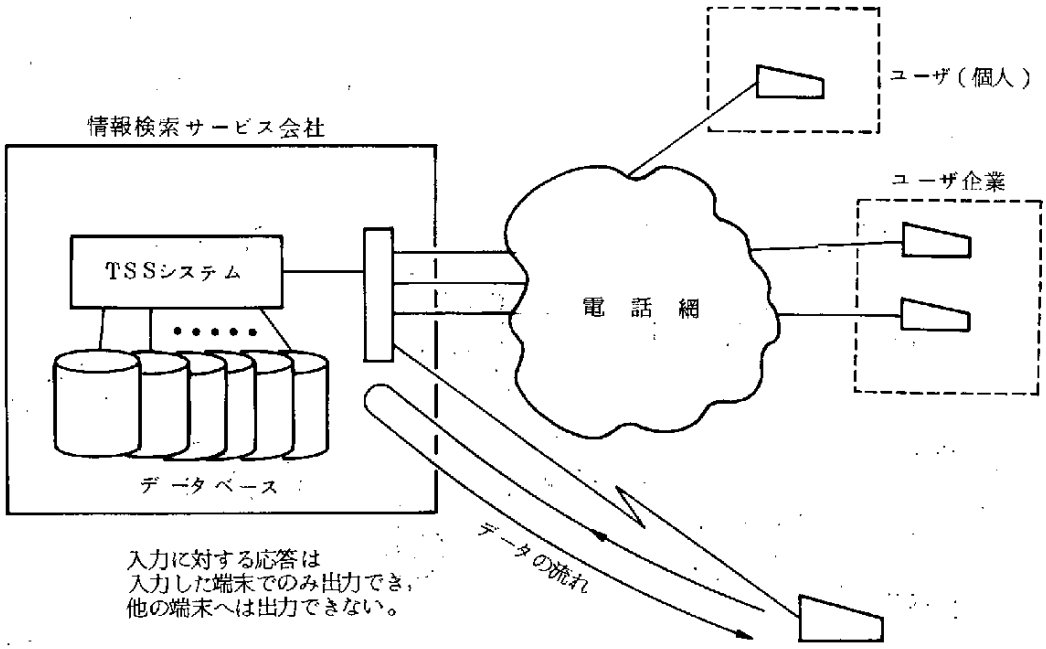


図3－5　データベース検索サービス

(3)　企業間システム

ここで，企業間システムの実例について報告する。この報告は，昭和58年度に行った調査結果に基づいてまとめた。銀行等の金融機関の動向は，「3.2.2 金融業での応用」を参照されたい。

①　総合商社A社

総合商社A社は，昭和58年初から，他企業とのオンライン結合による商取引の機械化を行った。このネットワーク・システムは，第二次回線開放によって構築が可能になった。図3－6に示すように，比較的取引量の多い6社（昭和58年8月現在）と，特定通信回線で結び，A社を中心としたスター型のネットワークを構築した。ネットワークに参加したB～G社は，A社の上得意先ではあるが，系列企業でもなければ親子企業でもないというのが，従来のネットワークになかった特徴である。G－H社間は，従来の系列企業同志の結合で，間接的に，A社と結合したことになる。

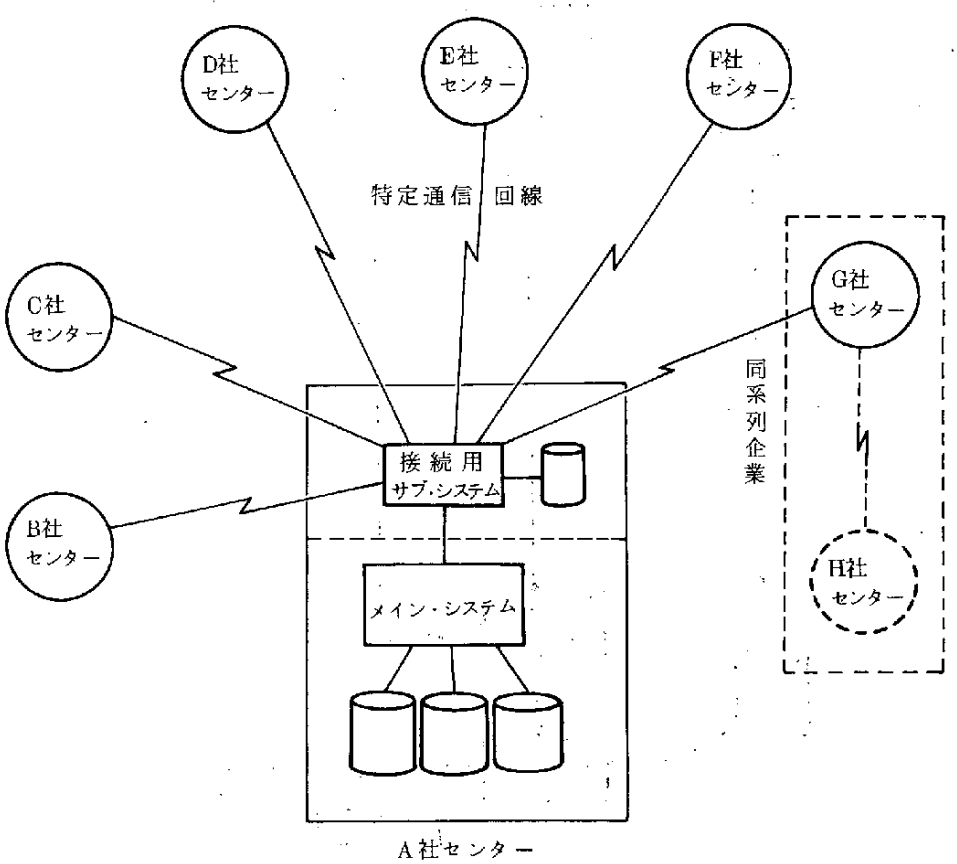


図３－６　A社を中心とする企業間システム

現在の制度では，メッセージ・スイッチングが許されないため，タイムラグを設けてスイッチングを行う（人間が介在する），疑似メッセージ・スイッチングにより，メッセージの転送が行われている（図３－７を参照）。このネットワークを用いて，オンライン受発注及び月末の取引状況確認（取引商品，数量金額等の相互確認）が実施されている。その他，取引に関する各種照会も可能としている。残念ながら，完全ペーパーレス取引ではないが，一括伝票を用いることによって，必要最少限の帳票で商取引が行われている。

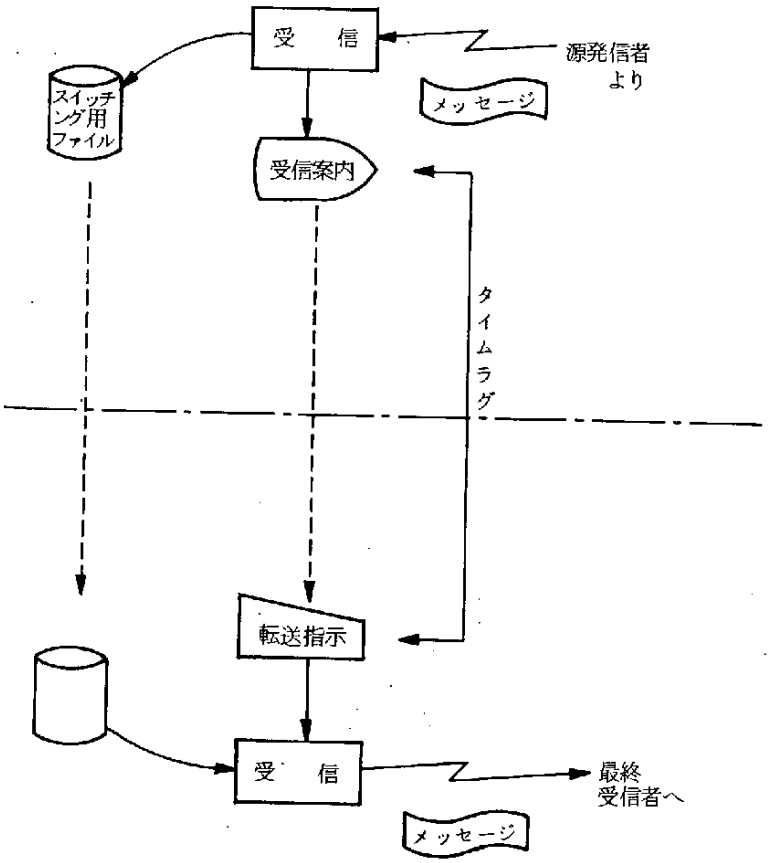


図３－７　疑似メッセージ・スイッチング

その結果は，データ入力の減少，それによるエラー／ミスの減少，省力化，取引状況の即時把握，伝票処理の減少及び取引の迅速化等大きなものがあると言われる。A社全体から見れば，このネットワーク利用による効果は部分的なものであるが，将来の方向を示すものとして，興味深い。

一方問題点はセキュリティ対策である。現在は，７社で構成する限定的ネットワークであり，この７社が悪用（恐らく，その可能性はない）しない限り，このネットワークは安全である。万一トラブル（例えば，端末操作者の不正等）が発生しても，７社であれば事後処理のため話し合いは可能である。

しかし，将来ネットワークが拡大した場合，極端にはA社の全取引先とネッ

トワークで結合した場合，当然のことながら，不特定多数との接続が生じる。この場合の効果的なセキュリティ対策は，まだ見出されていない。

また，発注メッセージを受信した場合，必ず人間によるチェックを行っており，自動受注承認は，セキュリティ上の問題を考慮して実施されていない。より一層の効率化のための自動受注承認の実現は，将来の課題である。

さらに，完全ペーパーレス処理の実現も，大きな課題になっていると思われる。現在のシステムでは，一括伝票を使用することは，ほとんどなく，通常の業務は，電子化伝票（磁気テープ／ディスク内の伝票情報）を用いて行われていると考えられるからである。

② 証券会社Ｉ社

Ｉ社は，昭和55年頃から，それまで自社内で留まっていたオンライン・ネットワーク網を外部へ拡張し，企業間接続の第一歩を踏み出した。

Ｉ社の企業間接続を模式的に表わすと，図３－８になる。Ｉ社のセンタから地方の拠点までを特定通信回線で結び，その先の顧客企業までは，公衆通信回線で結んでいる。顧客企業内には，Ｉ社の専用端末（パソコンも可能）が設置され，Ｉ社のホスト・コンピュータと結合することになる。このネットワーク・システムには，企業だけでなく個人でも参加可能である。

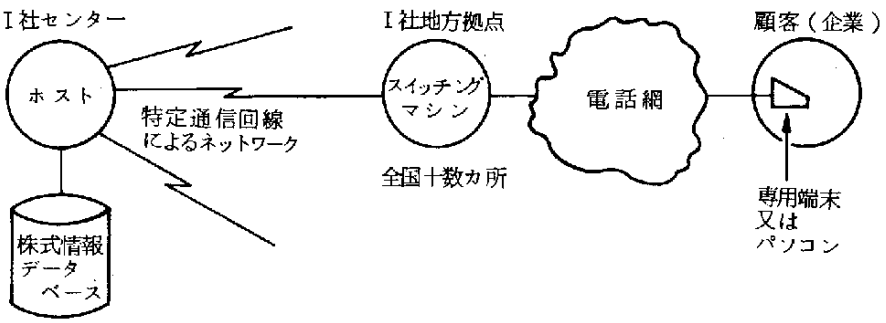


図３－８　Ｉ社のネットワーク

Ｉ社の企業間接続では，前記Ａ社のように，顧客先企業のホスト・コンピュータと直結しているわけではない。従って，厳密な意味では，企業間システムとは言えない。その反面，第二次回線開放を待たずに構築することが可能だったため，現在（昭和58年）既に，約700の顧客先に端末が設置されている。

このネットワーク・システムを用いて，証券投資に関する情報を顧客に提供している。具体的な処理方法は，データベース・サービスにおける情報検索と，ほぼ同一である。Ａ社と違い，公衆通信回線（電話網）を用いているため，パスワード・システムによるセキュリティ対策を行っている。

現在のように株式情報のサービスだけであれば，顧客先のホスト・コンピュータに直結する必要は，あまりないと思われる。しかしＩ社では，今後の開発目標として，ファーム・バンキング／ホーム・ディーリングの早期実現を挙げている。ファーム・バンキングでは，従来Ｉ社から顧客への一方通行だった情報の流れが，双方向に変わる。従って，顧客側では，ホスト・コンピュータ直結の方が，財務処理その他の面で便利であり，また既に保持しているコンピュータ・システムの有効利用にもなり，効率的である。ホーム・ディーリングでは，パソコンの使用が当然であり，パソコンとホスト・コンピュータとは，基本的に同じである。

すなわち，Ｉ社の本格的企業間接続は，ファーム・バンキング／ホーム・ディーリングの実現と同時に始まることになる。セキュリティ上の問題も，その時点で解決すべき大きな課題になることが予想される。

Ｉ社の主業務は，株券売買の代行であるが，そのための株式情報の提供も重要業務である。株式情報は，高付加価値情報とも言えるので，Ｉ社の現行システムは，高付加価値情報の売買を行っているとも言える。ただし，現在はネットワーク参加料（基本料金）のみ課金し，情報そのものは，無料になっている。

③　スーパーＫ社

スーパーＫ社の情報処理システムは発展途上にある。Ｋ社に限らず，日本

の小売業は全体的に，コンピュータによる機械化のテンポが遅い。これは，小売業という個人相手の商売であること，及び，日本独自の商慣習に原因があるのかもしれない。元々，スーパーのような流通業は，物を生産あるいは加工するのではなく，メーカ／問屋等から仕入れて個人に売るのが主業務である。商社と似ているが，個人相手の売買があるのが特徴である。その結果必然的に，少量多品種の在庫管理及び小口の売買が中心となり，どうしても手作業中心となる体質がある。生鮮食料品という扱いにくい商品もある。店舗の大型化だけでは解決できない問題が多い。

しかしながら，改善への努力は続けられている。少量多品種の在庫を改善し，仕入れを大口化してコストダウンを行おうとしたのがチェーン・ストア方式である。チェーン・ストアは，多数の同業小売業が共同で，仕入れ及び在庫管理を行い，規模拡大のメリットを追求している。チェーン・ストアには，統括会社（親会社）が存在するのが普通で，K社もチェーン・ストアの本部になっている。

チェーン・ストアは，外部からは1社に見えても，実際は多数の小売業の集合体（グループ企業）である。オンラインＰＯＳシステムは，末端のストアから，売上げデータ／仕入データを収集し，適切な商品仕入れと在庫管理を行う企業間システムである。

K社のネットワーク網は，公衆通信回線網（電話網）を用いているため，形態は単純である（図３－９を参照）。セキュリティ対策は，特に行われていないので，誰でも端末を操作可能である。ただし悪用するとしても，高々

図３－９　K社のオンラインＰＯＳシステム

いやがらせのための無意味な発注ぐらいしかできないので，あまり問題は発生しないと思われる。

このように，現在は単純明解な情報処理であるが，企業間接続が進むと一変する可能性がある。

スーパーあるいはチェーン・ストア本部では，仕入先企業が極めて多数あり，すべて回線で結ぶのは容易ではない。しかし共同ネットワーク・システムがあり，これを用いて取引できれば，すなわち電子化取引が可能になれば，仕入業務の機械化は一挙に解決してしまう。一方，小売の方は，決済機能の付加されたキャプテン・システム等で，機械化が可能になる。さらに，共同ネットを用いて，電子的に配送を依頼することも可能であり，決済も電子的に行える。こうなると，店舗が不要になるかもしれない。

以上のように，企業間接続は，K社にとって極めて大きな関心事になろう。その段階で問題になるのがセキュリティ対策である。自動化が進むと，人間はコンピュータの内部処理が次第に理解できなくなり，コンピュータが示す結果を信じる以外に方法がなくなる。注文しない商品が届く，商品を注文しないのに，口座から代金を引き落される等のトラブルが発生しないとは言えない。何が起きたのか調べようとしても，コンピュータ内部のことで，分らないということも起きるかもしれない。スーパー／小売業では，1件当りの金額は小さくても，件数は膨大であるだけに，そのセキュリティ対策は難しい課題と言えよう。

④ ビデオテックス（キャプテン・システム）

キャプテン・システムは，ビデオテックスを応用した，新しいサービス・システムである。キャプテン・システムの詳細は，各種の文献で紹介されているので，ここでは，そのセキュリティ面の調査結果を簡単に報告する。

キャプテン・システムの特徴は，主に個人ユーザ（消費者）と企業（商店，スーパー，デパート）を結びつけるシステムになっていることである。本格的に，個人ユーザが参加するネットワーク・システムとしては，我国では初めてと言ってよいだろう。主なサービスは，各種情報の照会，ホーム・ショ

ッピング及びホーム・バンキングであり，昭和59年11月にサービス開始が予定されている。以下に，これら3種のサービスのセキュリティについて，調査結果を報告する。

ⓐ 各種情報の照会

盗聴等があると，商品を万引されたのと同じ結果になるので，理想的には，厳重な対策が必要である。しかし，一部の不心得者のために，多大なコストをかけて対策を施すことは，個人／家庭用のシステムとしては不適当であるため，基本的対策のみ実施されている。それは，登録制（電話回線単位）と，発信回線番号の確認である（センタ側で確認する）。

盗聴（万引）で被害を受けるのは，販売側であり，消費者には被害が及ばないのは救いと言える。

ⓑ ホーム・ショッピング

現在，通信販売で各種のトラブルが報告されているが，これと同種の問題は起り得る。そこで，販売側（業者側）については，優良企業のみを参加可能とするように，厳しい資格審査が行れるようである。

一方，消費者に対しては，商品購入の予約があった時は，必ず販売者が電話で確認することで，対応する。予約の取消を忘れた，あるいは，たまたま訪問してきた他人が，いたづらをした（予約した）等のトラブルを防止するためである。しかし，電話による確認が必要では，新時代のシステムも，色あせて見えるかもしれない。

ⓒ ホーム・バンキング

現在予定されているサービスは，残高照会，振込通知等であり，為替送金等は，セキュリティ上問題があるという理由で，当分の間，サービスされないということである。

以上，簡単にセキュリティ対策を中心に報告したが，キャプテン・システムのサービス内容は，現在（昭和59年3月）もなお流動的であり，一部の報道では，限定的な決済機能の付加及び電話確認の省略も伝えられている。いづれにしても，我国では初めてのシステムであり，その推移を見守りたい。

3.2.2 金融業での応用

近年の金融業におけるネットワーク網の拡がりは，従来にない質的変化がみられる。この現象は，通信回線の自由化と大蔵行政の緩和とが相まって生じたものであるが，各金融業とも，このネットワーク網の拡大により新たな商品開発に，取引先との紐帯強化に，情報産業への脱皮に，合理化・省力化の推進に，新種サービスの提供等，多くの狙いをもって取り組んでいる。確かに今後，金融業が他の競合業界と互して生き伸びていくには，このネットワーク網の拡大への対応は，避けてとおれぬ道である。従来の金融業での機械化の中心が，自行内あるいは金融業間の結合であったものが，異業種・取引先と直結する機械化の新たな展開が急速に進んでおり，機械化の質的変化がもたらされ，さらに今後どのように展開していくのか，予測の難しい面もある。この項では，金融業でのネットワーク網を利用したシステムの状況及び今後の展開，それらシステムにおけるセキュリティ面での考慮点，問題点について述べる。

(1) 金融業オンライン・システムの歴史

金融業の機械化は，昭和30年代のオフライン処理を経て昭和40年代に第一次オンラインとして，預金業務を中心に大量処理業務のオンライン処理が行われ，内部事務の合理化・効率化に大きく寄与した。つづいて第二次オンラインは，昭和50年頃からスタートしたが，金融業のほとんどの業務がオンライン処理され，顧客単位の管理を中心の総合システムとして構築された。この間に，金融業間を結合するシステムとしての全銀システム，預金代払い提携システム（ＮＣＳ，ＴＯＣＳ，ＳＩＣＳ，ＡＣＳ，ＳＣＳ），ＳＷＩＦＴシステムが逐次開始され，また，エレクトロニック・バンキングの萌芽ともいえる取引先と直結したテレックス連絡システム，音声応答連絡システムも実施された。昭和50年代後半に入り，昭和57年10月の公衆電気通信法の改正施行，大蔵行政の緩和を契機として，金融業のオンライン・システムが金融業内の単独システムにとどまらず，顧客のコンピュータ，パソコン，電話等と接続され，外部システムとのオンライン化が急速に展開されていく状況にある。

(2) 金融業の内部システム

大半の金融業のシステムは，一ケ所ないし二ケ所の自社コンピュータ・センタと各自営業店とを，専用回線で接続し，オンライン処理を行っている（図3－10参照）。一部の金融業では共同センタを設立し，オンラインの共同利用をしている例もある。通信回線の効率的活用の観点から，遠隔地の営業店との接続には，集線方式を利用しているケース，あるいは同一回線を複数システムが乗りあって利用するケースがある。

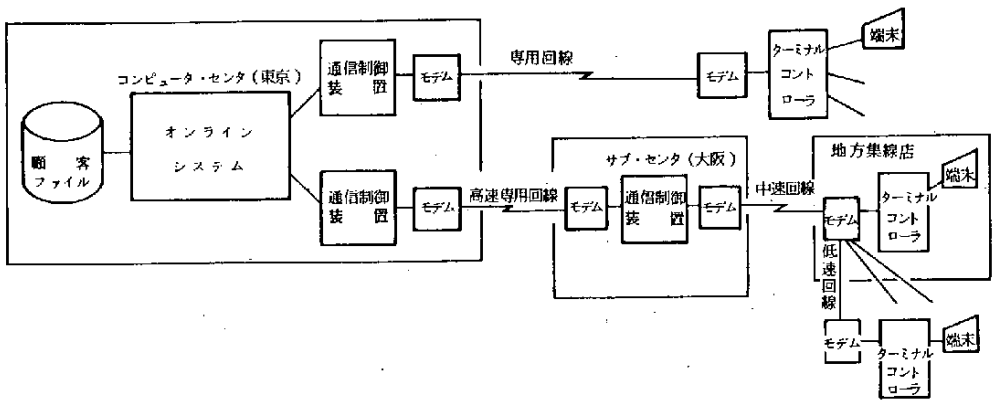


図3－10　金融業の内部システム

近年は，大蔵省の店舗行政の緩和により，店舗形態の多様化が急速に進展し，自動化機器の店舗外設置，無人化・機械化店舗，ポータブル端末等の出現で，従来にない新たなシステム対応が必要となってきている。自動化機器の店舗外設置，無人化・機械化店舗への対応としては，遠隔地からのリモート操作（機械への電源自動オン・オフ，機械の稼動状況監視，シャッタの自動開閉コントロール等）が，また，ポータブル端末対応としては，操作端末の特定，盗聴防止，不正入力防止等の対策が考慮されている（図3－11参照）。

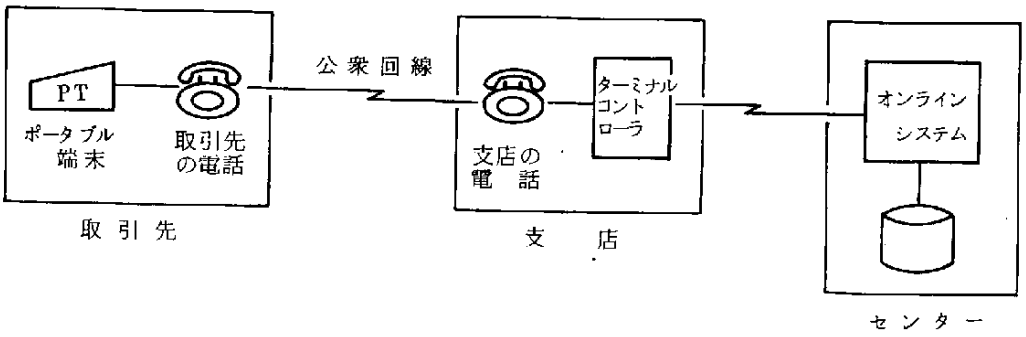


図３－11　ポータブル端末の接続例

(3)　金融業間結合システム

①　全国銀行データ通信システム

金融業間の為替取引をオンライン処理するシステムで，昭和48年第一次システムが，88金融機関，7,200店舗の規模でスタートし，昭和54年には708金融機関，17,000店舗の規模に拡大され，本格的なオンライン・システムが完成した（図３－12参照）。現在，新たな業務の追加，業務量増に対応すべく第三次システムが計画中である。このシステムは参加する金融機関の数，取引量の膨大さにおいて，日本で最大規模のオンライン・システムと言える。

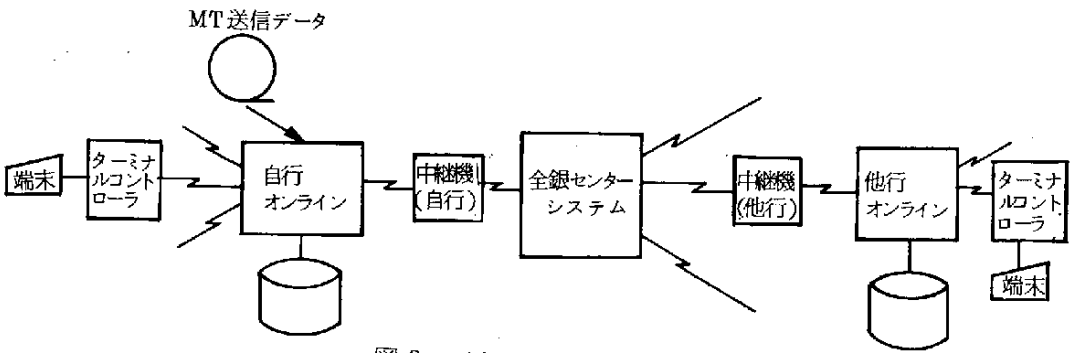


図３－12　全銀システム

全銀システムにおけるセキュリティ面の対策としては，専用線の利用，取引単位の通信番号による管理，仕向・被仕向金額突合等が組みこまれているが，今後の対策として，データの暗号化，入金口座のオンライン確認等，さ

らにセキュリティ面での強化が必要と考えられる。

② 預金代払い提携システム

自動化機器を利用して，金融業間で預金の支払いを相互に行なうシステムが，昭和50年11月のＮＣＳ（日本キャッシュ・サービス）を皮切りに逐次拡大の傾向にある。

代表的なシステムとして

- ＮＣＳ　　昭和50年11月開始
  加盟行　54行
  6大都市周辺のパブリック・スペースに共同のＣＤを設置
- ＢＡＮＣＳ　昭和59年1月にＴＯＣＳ（都銀7行の提携システム，昭和55年4月開始）とＳＩＣＳ（都銀6行の提携システム，昭和55年3月開始）が統合された（図3－13参照）。都銀13行の自動化機器相互共同利用システムである。

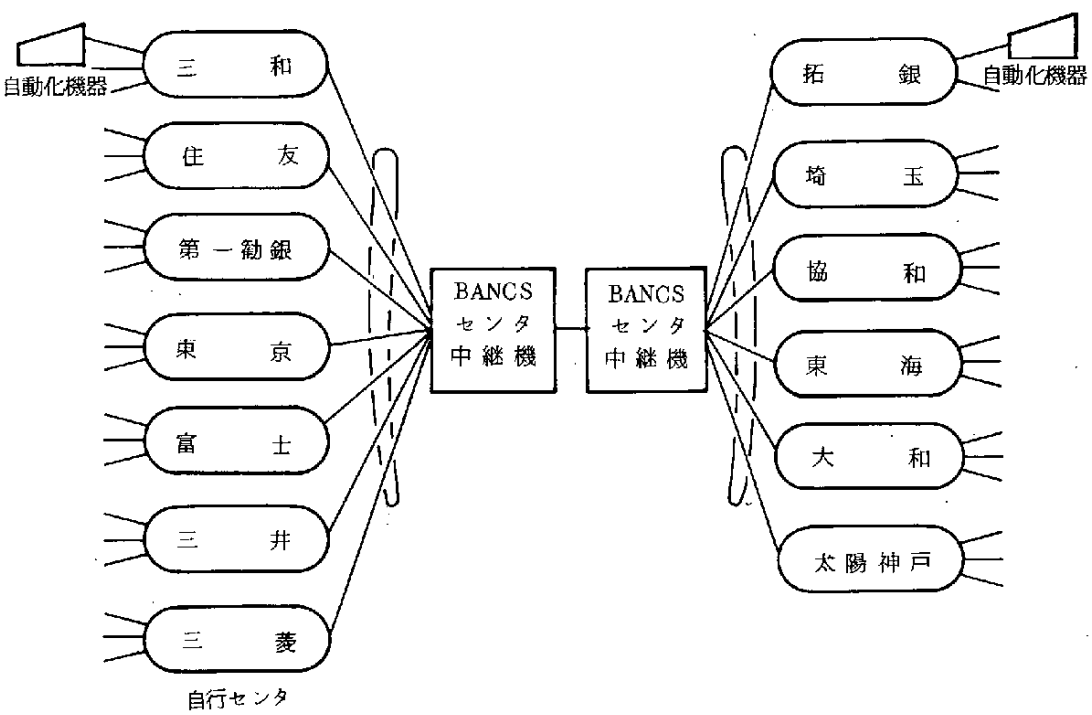


図3－13　ＢＡＮＣＳシステムの構成

以上の他，ＳＣＳ（相互銀行システム），ＡＣＳ（地方銀行システム），信金ＣＤ（信用金庫システム）等がありこれらのシステム間の相互乗り入れの動きもあり，実現すれば全銀システムと匹敵する大規模システムとなる（図３－14参照）。

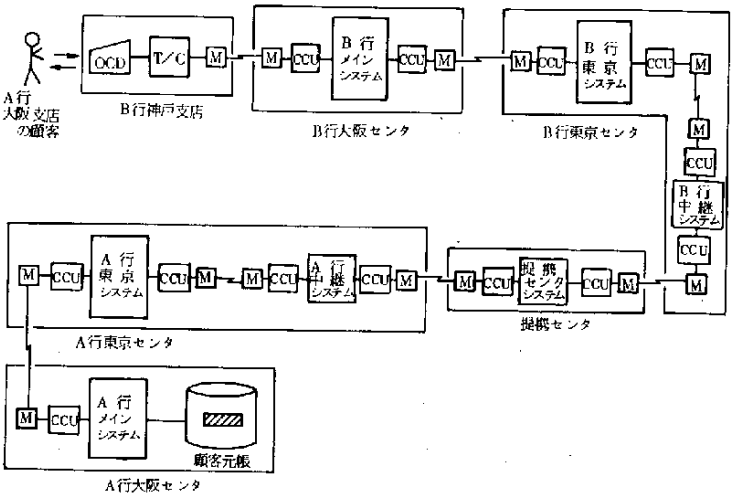


図３－14　都市銀行提携預金支払いシステムの例

③　ＳＷＩＦＴシステム

外国為替業務の抜本的な合理化をはかることを目的とした，国際間を結ぶデータ通信システムがＳＷＩＦＴシステムである（図３－15参照）。昭和48年にシステムの運営主体が，ベルギー法に基づく非営利組織体として発足し，昭和53年にアメリカ，ヨーロッパ諸国を中心にしたシステムがスタートした。日本では昭和56年３月に稼動を開始している。現在，加盟国は35ケ国，加盟銀行数は約800行で，一日の取引量が５０万件に達し，対象業務も逐次拡大され，国際間のデータ通信システムとして，現段階で質量共に有数のシステムといえる。一件当りの取引の金額が数百億円に及ぶ取引もあり，本システムの安全性・信頼性については，ハード面・ソフト面共万全の対策が講じられている。本システムのセキュリティ対策の内容については，第3.4.6項で触れる。

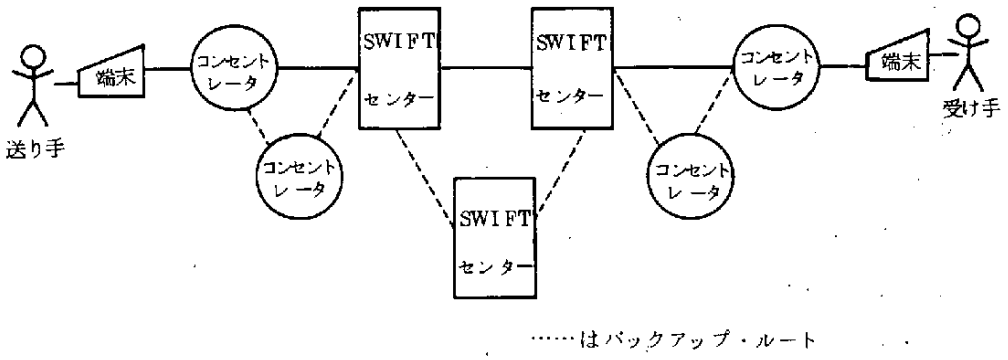


図3－15　SWIFTのネットワーク

(4)　個人・企業との接続システム

金融業のシステムは，自行内のシステム，金融業間のシステムについては前述のとおり，コンピュータ技術の進展と呼応する形で，既に大半の業務をオンライン処理するシステムが構築されており，内部業務の効率化・省力化に大きく貢献している。一方，対外部とのシステム接続については多くの規制，あるいは外部のシステムのおくれ等により，現段階では，かなり限定された接続しか行われていないのが実態である。しかしながら，最近の環境の変化（通信回線の自由化，大蔵行政の緩和，個人を含めた取引先でのＯＡ化，コンピュータ化の進展）により，対外部との接続システムが急展開する状況にある。各金融業とも，新しい試みに意欲的に挑戦しておりここ一，二年の動向はきわめて流動的である。

個人・企業との接続システムのはしりとしては，為替振込の連絡をテレックス回線をとおして連絡する，テレックス連絡システムがあげられる。次に現われたシステムとして，電話による振込連絡，残高照会あるいはファクシミリ連絡システムがあるが，いずれも単なる振込連絡・残高照会に機能が限定されているところに，システムの限界がある。今後の展開としては，個人・企業のコンピュータ／端末から入力されたデータで，直接取引が成立するシステム，個人・企業と金融業との双方向のデータの授受，ＣＭＳ（キャッシュ・マネジメ

ント・サービス）サービス，個人と金融業と企業との複合サービスの提供等が考えられ，まさに開かれたシステムが，急ピッチで展開されていくことになろう（図3－16参照）。これら個人・企業と金融業との有機的結合を，現実的なものとしていくには，データ通信プロトコルの標準化，データ・フォーマットの標準化等システムの標準化が不可欠であり，この観点から現在，全国銀行協会連合会では通信プロトコルの標準化に取り組んでおり，その内容については，第3.4.6項で触れる。

(5) ネットワーク拡大とセキュリティ問題

金融業内にとどまっていた従来のシステムから，開かれたシステムとして，個人・企業とのシステム接続が拡大され，データ通信手順の標準化，電文の共通化，公衆回線の利用等が押し進められ，システムが一般にオープンにされていく事により，セキュリティ対策について，新しい角度から取り組んでいく事が要請される。

現状のシステムにおいては，①特定回線の使用と独自の電文構成・通信手段を使用，②システムに通信可能なターミナルの特定，③通信制御プログラムによる応答電文に加え，業務処理プログラムで入力ターミナルに応答電文を出力する，④通信番号による連続性のチェック，⑤回線・端末単位の件数，金額突合等の対策を講じているが，電文の暗号化は一部に限られ，また電文盗聴のチェック機能がないなどの問題点を抱えており，今後の課題として，電文の暗号化，本人確認手段技術の向上等々，より高度なレベルのセキュリティ対策が必要と考える。

3.2.3 海外のセキュリティの動向

3.2.3.1 海外のセキュリティの動向

海外のセキュリティの動きで，一番注目しなければならないのは，米国である。

(1) 米国国防省

米国のセキュリティの動きを見るには，やはり，米国国防省の動きと，F

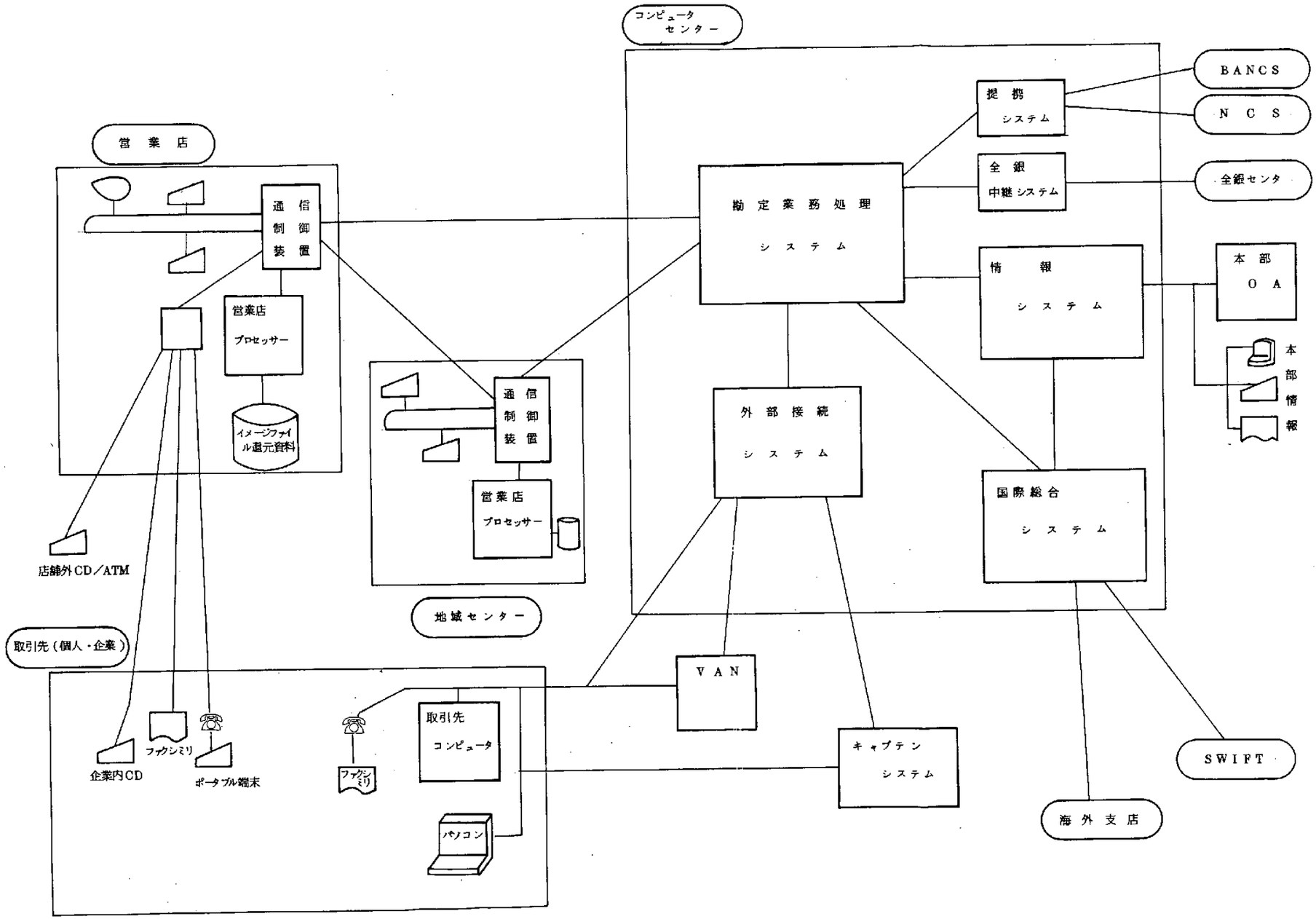


図3－16　ひろがる金融業のネットワーク

ＢＩの動きが重要である。

米国国防省のセキュリティとの戦いは，ネットワークの入ったシステムのセキュリティを見るとき，国防省のＷＩＮ・コミュニケーション・ネットワークの概要を見ると，セキュリティの難しさ，苦労がわかる（図３－18参照）。国防省では，ネットワークのセキュリティは，多くの要素があり，これらの要素がからみ合って，セキュリティのレベルを低下させて行く，と考えている。セキュリティに，必要な要素を，式で表わすと，図３－17の式となる。

$$S = F(O \times A \times Pa \times Ph \times C \times E)$$

S＝システム全体のセキュリティ

F＝関数

O＝組織

A＝管理

Pa＝人的要素

Ph＝物理的

C＝通信

E＝ＥＤＰ

図３－17　セキュリティ・レベルの式

何をさしおいても，セキュリティの基本要素は，組織である。どのようなしくみでどのような組織で，システムを動かすかが重要である。式の右側に行くほど，人によって左右されることが少ない。要素の一つである，ＥＤＰにおいては，あらかじめ，セキュリティのレベルを，ＭＴＢＦ等で計算し，予防策を取ることもかなりのレベルで可能である。

ＥＤＰに次いで，要素Ｃも，セキュリティのレベルを計算し，設計することができる。その手段として，暗号化や，回線の二重化，インタフェースの条件の機密等がある。しかし，国防省のような，国家の重大機能・機密を要するシステムにおいて，通信線として公共の通信網を使用するかぎり，一

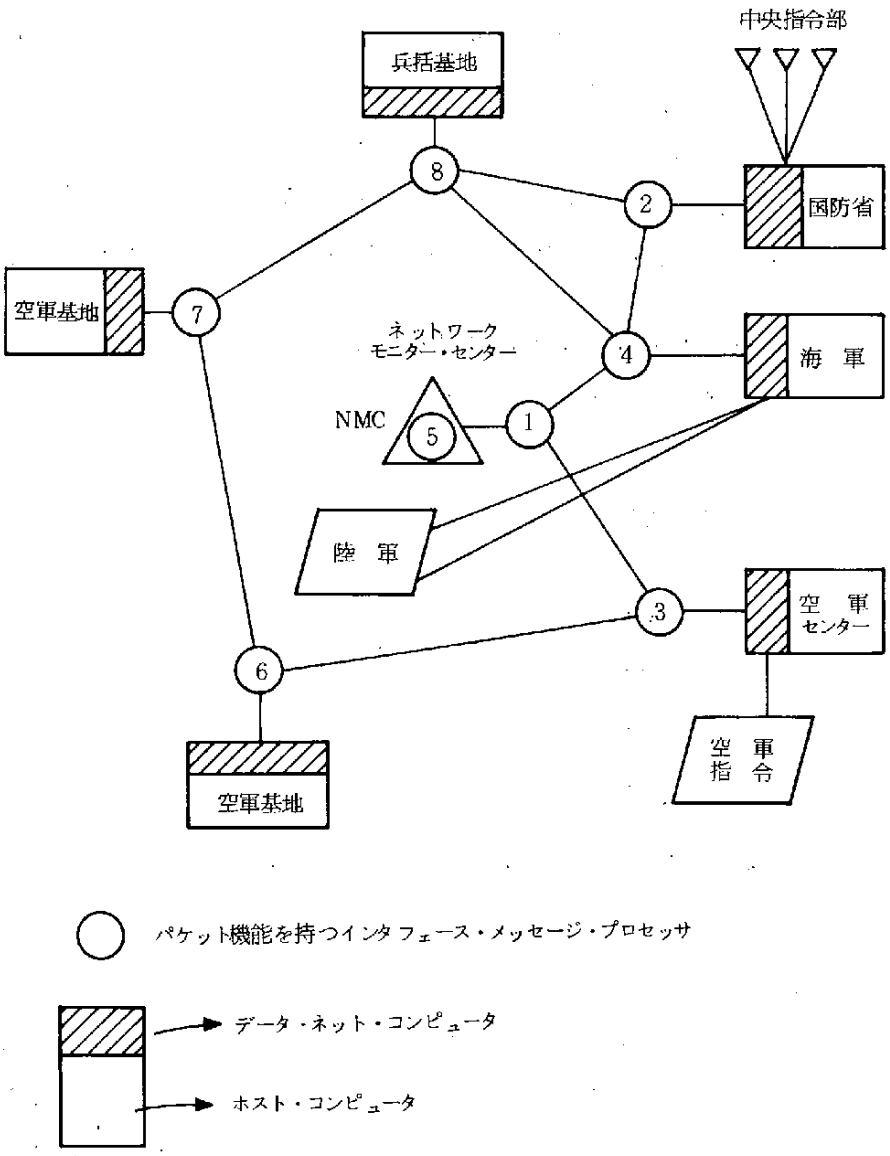


図３－18　米国国防省のネットワーク略図

定レベル以上のセキュリティを保てない。現に，コンピュータ好きの少年によってコンピュータ破りが発生したため，国防省は，軍事用と一般用を独立させると共に，独自の国防データ通信網（ＤＤＮ）を５年後に作ることになった。これは，公共用通信網を使う限り，技術的な面だけでは，セキュリティに限界のあることを示している。

この他，国防省は，ファイル・アクセスとセキュリティ・レベルを上げるための手段として，セキュリティＯＳの開発に意欲を示しており，大学等の研究機関に開発研究を依託している。その成果については，民間にも開放し，セキュリティの重要性を啓蒙している。

(2) ＦＢＩ

外部から電話回線を使って，コンピュータに侵入し，データを盗んだり，システムそのものを破壊する，いわゆるコンピュータ犯罪が増えている。一般的には，自宅にあるコンピュータ（パソコン）を使い，電話回線を利用して通信回線につなげている。大型のコンピュータやデータバンクと接触し，データを盗んだり破壊したり，途中で情報を手に入れるもので，この程度の犯罪は，マニアの少年が腕だめしにトライしているケースとして，今のところ見つかっているが，一つ間違えば大きなコンピュータ犯罪につながる。

特に，通信回線を通じたネットワークの犯罪になって行くと，犯罪を見つけ，つかまえることも困難になることが予想されるので，今般，ＦＢＩは国家の重要課題として，研究・捜査に乗り出した。

参考迄に，ＦＢＩの統計によるコンピュータ犯罪のデータを示すと次の通りである。

① コンピュータ・データの不正移動

＊460,000ドル／件

② 銀行強盗

＊2,000ドル／件

③ コンピュータ・不正使用による横領

＊23,000ドル／件

このデータからも，コンピュータ・データの不正移動による犯罪の損害がいかに大きいかがわかる。

(3) 米国連邦標準局（NBS：National Bureau of Standards）

セキュリティ・ガイドラインの公表

- Guidelines for Automatic Data Processing Physical Security and Risk Management

  （FIPS Pub 31 ：1974／6）

- Computer Security Guideline for Implementing

  （FIPS Pub 41 ：1975 May 30）

- ＤＥＳを民間における標準の暗号化規格として発表（1977）
- コンピュータ・セキュリティの監査評価に関する研究集会を主催

  （1977）

(4) 米国会計検査院（GAO：General Accounting Office）

パンフレット「政府関係の機関，計画，活動，機能等の監査基準」発行

(5) ニューヨーク調査局（The City of New York Department of Investigation）

ニューヨーク市当局の一機関である。コンピュータの悪用や，コンピュータ犯罪を防止するため設置され，次の業務を推進している。

- 不正の調査
- セキュリティ・レベルの向上の調査研究
- 運用上の対策検討
- システム監査

(6) 民間会社のセキュリティ

① アメリカ銀行協会（ABA：American Bankers Association）

- 業務処理と自動化全国大会を開催（1979/5）

  － ＥＦＴＳ法によるプライバシ保護に関する討論会

② チェース・マンハッタン銀行

- セキュリティ対策の強化を検討
- 技術的セキュリティの対策
  - 回線上のデータの暗号化
  - データベース・アクセス・コントロール
  - パスワードの研究

③ シティ・バンク

- ＥＦＴＳ設定時の問題検討
- セキュリティの総合対策
  - 運営時のリスク分析
  - プライバシ保護
  - 通信線のセキュリティ検討

(7) 米国メーカのセキュリティ

① ＩＢＭ社

コンピュータとデータのセキュリティに1965年～1975年にかけ，積極的に取組む。その後一時熱がさめたが1980年に入り，再度研究を促進してきた。メーカの中では，一番熱心である。ベーシックなセキュリティ商品を開発し，標準品に近い形の低価格商品，すなわちセキュリティ関連商品を開発促進中である。また，セキュリティＯＳ：ＫＶＭ／370や汎用監査プログラム（Audit Source Code Compare）を開発している。

② ハネウエル社

ＩＢＭ社に次いで，セキュリティに関心を持つ。既にセキュリティＯＳ：ＳＣＯＭＰを開発している。

(8) その他の国

① 西ドイツ

西ドイツは，内務省内にデータを保護する監督官を設置している。

② カナダ

カナダ会計士協会が２つのガイドライン（ＣＩＣＡ：Canadian Institute of Chartered Accountants）を発表している。

- “ Computer Control Guidelines ” …… 1971
- “ Computer Audit Guidelines ” …… 1975

③ スエーデン

スエーデン国防省が中心となって，ネットワーク・セキュリティ問題を熱心に研究している。

(9) 国際機関

ＣＣＩＴＴの中のＳＧⅦのＷＰ－Ⅳがセキュリティを取上げ論議している。議長は英国で，ヨーロッパのメンバーが中心となっている。この作業部会の中で“テキスト通信の制御手順の拡張の項目Ｑ16”のスペシャル・グループ・オン・エンクリプション（ Special Group on Encryption ）という小グループで検討が進められている。

一方，ＩＳＯの方は暗号の標準化を積極的に進め，暗号の標準化がほぼ固った。セキュリティ関係は，メンバーがＣＣＩＴＴとだぶることもあって，ＣＣＩＴＴの方で取組んでいる。

3.2.3.2 国内の状況

(1) 通産省関連

① 1975年11月

コンピュータ・システム安全対策委員会設置

② 1977年

システム監査に関する調査研究

③ 1977年4月

「電子計算機システム安全対策基準」の策定，公表“運用とコンピュータ設備の安全性”

④ 1978年

システム監査士制度創設のための調査

⑤ 1981年7月

「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”」の発足

⑥　1982年

コンピュータ・セキュリティ・ガイドライン策定計画

⑦　1982年10月

コンピュータ・セキュリティ研究会がシステム安全対策基準，システム監査及びコンピュータ利用の制度的検討

(2)　大蔵省関連

①　1976年

金融機関の内部検査に関する実態調査

②　1981年11月

金融機関の不祥事件の防止策についての銀行局長通達

③　1981年11月

金融機関業務処理の機械化の進展に即応した事故防止策の見直し状況等についての銀行局調査部の報告

(3)　郵政省関連

①　1980年～

「データ通信セキュリティ基準」の作成とＭＩＸ暗号方式の開発

②　1982年3月

データ通信における総合安全対策システム開発調査

③　1982年～

データ通信総合安全対策システムの開発

(4)　民間での動き

①　金融機関

- 1982年1月　……　オンライン事故対策部会

②　ＥＤＰユーザー団体連合会

- 1976年10月　……　システム監査の実施に関する要望書を通産大臣に提出

③　日本公認会計士協会

- 1976年9月　……　ＥＤＰシステムの監査基準及び監査手続試案

発表

- 1976年11月 …… 企業内部におけるＥＤＰシステム監査に関する要望書を通産省に提出

④ 日本情報処理開発協会（ＪＩＰＤＥＣ）

- 1982年 8月 …… システム監査基準試案発表
- 1982 年8月 …… システム監査／セキュリティ訪米実態調査団報告書発表
- 1983年3月 …… 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発表
- 1983年3月 …… 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発表

⑤ 日本情報センター協会

- 1977年6月 …… 電子計算機安全対策基準を発行
- 1981年11月 …… 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解説書発行

⑥ 情報処理学会

- 1977年2月 ……「コンピュータ・システムの高信頼化」を出版

3.2.3.3 海外と国内のセキュリティの相違点

(1) セキュリティ問題の取組み方の相違

① 政府の動向

米国とヨーロッパと日本では，かなり動きが異なっている。米国では，国防省のセキュリティ対策が一番進んでおりまた熱心で，自からの他，研究機関やメーカーに，プロジェクトを依頼している。

合わせて，研究結果等を民間に公開し，セキュリティの普及と啓蒙を行っている。特に，ネットワークのセキュリティに関心が強い。しかし，最近セキュリティ対策の啓蒙はやるが研究結果，情報等は，ほとんど発表しなくなった。ヨーロッパでは，国によってかなり異なり，スエーデンでは国防省を中心に研究が進んでいるが，イギリス，フランス及び，西独等では，

プライバシ問題を中心に，通信事業担当省が熱心である。日本では，通産省，郵政省，大蔵省等が委員会，研究会，研究集会等を組織し，民間と一体となって，セキュリティ問題の重要性を啓蒙し，対策の研究を推進している。

② 民間の動向

米国では，金融機関を中心に，ユーザのセキュリティ対策が，進んでいる。多くの金融機関では，専門的なプロジェクト・チームを設けて推進している。将来ＥＦＴＳが本格化するのに対応して，ＡＢＡ（米国銀行協会）を中心に研究が進んでいる。金融機関のセキュリティ問題に対し，米国政府の主だった動きは今の所見うけられない。

ヨーロッパでは，ホーム・バンキングの普及に合わせ，セキュリティ問題が取上げられつつあるが，プライバシ問題を避けて通れないので，日本や米国と違った動きとなることが予想される。

日本では，金融機関でセキュリティへの関心が高い。今の所，ユーザごとに個別に対策が取られているが，各金融機関共ファーム・バンキング時代には，各金融機関個別の対応では対策し切れないので，行政機関を含めた対応施策が重要課題となりつつある。日本のメーカは，ユーザの関心に沿って製品の開発を進めている。

③ 関係団体の動向

システム監査の面で，公認会計士協会等の金融関連団体が研究や提言を行っている。システム監査に関しては，米国が一歩進んでおり学ぶべき点も多い。

④ 技術動向

米国が一番熱心で，国防省を中心に具体的なものとして，セキュリティＯＳの開発を民間に依託したり，暗号の研究を積極的に進めている。また大学や学会でもセキュリティ技術の学術的研究に取組み始めており，その結果が学術誌や学会で発表され，その件数も年を追って増加している。

(2) 相 違 点

セキュリティに対する考えは，その国のもつ宗教や社会の仕組みや倫理によって影響を受けることが多い。

日本のような単一民族，単一言語，終身雇用と相互監視が歴史の中で育っている国と，複合民族，複合言語，短期雇用(?)と宗教とが入り混じって出来た倫理の米国とでは，セキュリティに対する考えや対策も違ってくる。故に，米国の研究結果や方法は，参考になっても，そのまま取入れることは向かないように思われる。

ここで日本と米国の相違がよくわかる例を２つ掲げる。

〔その１：銀行の窓口員“テラー”について〕

日本では，学校を出た優秀な学生を採用し，社内で十二分に教育をした女子行員が窓口に座っている故，微笑をもって間違いのない親切なサービスを顧客は受けられる。

一方，米国では銀行の窓口“テラー”の仕事は，銀行の中では最低の職業でレベルも低く，間違いも多く，親切なサービスを期待することは難しい。その上，転職率も高いので銀行としての教育も十分ではない。故に銀行窓口業務でも，日本と米国が同じ考えのセキュリティ対策は取れない。

〔その２：犯罪の刑について〕

日本で犯罪を犯し刑を受ける時は，真実に従って裁判を受け，刑を受ける。真実は，裁判により追求される。刑が決まるに当っては，情状・勺量の余地があって，大岡越前守的な裁きにより刑が確定する。

一方，米国では手続きと取引によって刑は決まる。真実は犯人自身が自分を守るため，自分自身の手によって証明して行かなければならない。ある罪で裁れる時，犯人が検事側にどれだけ売るものがあるかによって，刑と売物とのギブ・アンド・テイクで決まる。ここで，犯人の売物について記してみる。

- 黙秘権（黙秘しない事を売る）
- 余罪（余罪の一つ一つが売物）
- 他人の犯罪の情報

それぞれ，売る価値が交渉され，刑が軽くなって行く等々。

故にセキュリティは，その国の風土，宗教，人種，言語，倫理によって対応策は変る。

故に，将来くるであろう高度情報化社会時代の日本の風土，倫理や技術の進歩を予測してセキュリティ対策を立てる必要がある。

3.2.4 ま と め

コンピュータ・ネットワークは，本格的な実用時期に入ったと考えられる。コンピュータ・ネットワークには，２つの利用形態がある。それは，①地理的に離れた同一企業内の複数のコンピュータや端末を結ぶネットワークと，②企業間を結ぶネットワークである。②には，企業と個人（家庭）及び個人と個人を結ぶネットワークも含まれる。当プロジェクトが調査したのは，②である。

我国では，②の形態のネットワークは発展が遅れていると言われていた。しかし，実際に調査してみると，計画中のものまで含めれば，かなりの数の企業間システムの存在が明らかになった。現在，最もセンセーショナルな話題になっているのは，ファーム・バンキングである。我国では，金融業が情報処理革命の先頭を走っているという現状を考えれば，当然のことなのであろう。その他，ペーパーレス処理を目標にした，企業間受発注ネットワークも着実に発展している。キャプテン・システムは，企業と家庭を結ぶ受発注ネットワークとして，とらえることができよう。

さて，そのセキュリティ上の問題は何かと言うことであるが，具体的な対策上の問題を指摘する企業は殆んどなかった。たゞ，ある業務は，セキュリティ上の理由で，コンピュータ化（ネットワークを用いる）できないという話は，しばしば聞くことができた。

このセキュリティ上の問題に対する対応は，国によって，かなりの違いが見ら

れる。第3.2.3項で，これについて報告されているが，この報告から，我国の風土に合ったセキュリティ対策が必要だという感触が得られるだろう。しかし，将来，海外と結ぶネットワークが構築された場合には，国毎にセキュリティ対策が違っていると，問題を引起すかもしれない。尚，当プロジェクトでは我国内部のネットワークについて検討することとした。

さて，本調査の目的は，

① 企業間ネットワークのニーズ

② セキュリティ対策の必要性

③ セキュリティ対策が重要な業務処理

について検討することであった。ここでその結果を説明する。

最初に，企業間ネットワークのニーズは，充分すぎる程あったことを報告する。現実に，多数の企業間ネットワークが，計画あるいは構築されているのは，よい証拠である。次に，大部分の人々が，セキュリティ対策が重要だと指摘していたことも報告する。ただし，具体的問題点になると，先に述べたように，極めて曖昧になってしまうことを指摘しておく。また，セキュリティ対策については，現在の技術，手法及び体制で，十分対応できるという意見と，新しい対策手法や体制が必要だという意見があったことを報告しておく。

このように，前記①，②の項目については，ほぼ予想どおりの結果が得られた。以上の調査結果に基づき，我々は，セキュリティ対策が重要だと思われる，ネットワークを応用した業務処理を検討した。その結果，

① ファーム／ホーム・バンキング

② ペーパーレス取引（電子化取引）

③ 高付加価値情報の売買

が，セキュリティ対策が特に重要な業務処理であるという結論に達した。これらの処理は，現在試行の段階であり，まだ完全な実用化には至っていない。当プロジェクトでは，セキュリティ上の問題がその最大の原因であると考えている。以後の検討は，これらの業務処理が実現できるネットワークのセキュリティ対策とは何か，という観点で進めた。

前述①～③の業務処理では多くの共通点が見られる。例えば，いづれの業務処理でも，コンピュータのメッセージを，従来の伝票のかわりに用いる点である。そこで，我々は，これら3つの取引を，まとめて「電子化取引」と呼ぶことにした。次節（第3.3節）で，電子化取引のセキュリティについて分析した結果を報告する。

3.3 電子化取引の分析

前節で述べたように，企業間を通信回線で結び，これとコンピュータを組合せ，商取引を効率化しようとする試みが多数ある。それらの中には，単なる情報交換から一歩進んで，従来の書類（契約書，注文書，領収書等）をコンピュータのメッセージに置き換えようとしている試みもある。コンピュータ・メッセージへの置き換えを，極限まで進めると，書類が全くなくなり，端末さえあれば，商取引ができるようになる。端末は，通信回線さえあれば，物理的設置場所を問わないので，商取引の様相を一変させてしまう可能性もある。

このように，従来の書類をコンピュータ・メッセージに置き換え，電子的に商取引を行うことを，「電子化取引」と呼ぶことにする。電子化取引は大きな可能性を持っているが，同時に大きな危険性も持っている。千年以上の実績を持つ書類システムに対し，コンピュータ・メッセージは，たかだか十数年の歴史しかない。本節では，当プロジェクトが行った，電子化取引のセキュリティ上の問題点と対策の検討結果を報告する。

3.3.1 問題点の分析

(1) 商取引の分析

分析を容易にするため商取引は，

ⓐ 文書の交換

ⓑ 商品の引き渡し

ⓒ 代価の支払

の３つの行為で構成されると単純化して以下の話を進める。現状では，既にⓒの行為のコンピュータ・メッセージ化（例：ＥＦＴＳ）が進んでいるが，電子化取引では，ⓐもコンピュータ・メッセージ化する。一方，ⓑは，通常コンピュータ・メッセージ化は不可能であるが，商品が，高付加価値情報であれば，これも置き換え可能である。すなわち，データベースの情報の売買では，完全な電子化取引が可能になる。

① 初期の電子化取引

電子化取引を実現するためには，文書の交換をコンピュータ・メッセージに置き換えればよい。この限りにおいて，技術的問題はほとんどない。しかし，法制度上の制約から，文書類を廃止できないという問題がある。そこでそのような法制度は変更すればよいという議論も可能であるが，たとえ法制度の制約がなくても，実際には，書類が存在すると考えられるのである。

現在でも，高付加価値情報の売買では，既に商品の交換を通信回線で行っている。しかしながら，契約書，請求書，領収書等は，文書による交換を行っている。これらのことは，次のようなことを意味している。文書類には，コンピュータ・メッセージに置き換えられない何かがある。

そこで，文書類は必要最少限にして，できるだけ電子化を進める方式が考えられる。事実，このような「準電子化取引」という形態のシステムが構築されている。この形態は，初期の電子化取引と言えるだろう。

② 文書類の機能

文書を送ることと，コンピュータ・メッセージとは，どこが違っているのかが，大きな問題である。表３－１に，簡単な比較を示す。このように，文書を送ることと，コンピュータ・メッセージとは，かなりの本質的な違いがある。この違いがどのような影響を及ぼすかを調べるため，商取引における文書の役割を以下に示す。

ⓐ 売手と買手が行うべき処理を定めた法律……契約行為の事実を表す。

ⓑ 売手と買手が行った事実の記録……納品書，領収書等

ⓒ 第３者に対して，ⓐ，ⓑの事実を伝達する能力……証拠機能

ⓓ 作成者あるいは代理作成されたものを承認したことを表す印（又はサイン）

表３－１のコンピュータ・メッセージの性質は，以上のⓐ～ⓓの機能を実現するために，はなはだ不都合であることが明確になってくる。いずれにしても，インクで書かれた文書，そして印（サイン）は，保存性，改ざん困難性においてすぐれており，千年以上に亘って実績を積み上げてきた。これと

表３－１　文書とコンピュータ・メッセージの違い

比較項目	文書	コンピュータ・メッセージ
送る方法	物的	電子的
修正	困難	容易
コピー	全く同一のものは困難	容易
保存性	数百年の実績	不明
冗長度	非常に高い	非常に低い
印（サイン）	有	特別なからくりが必要

同等の機能をコンピュータ・メッセージに与えるのは，確かに容易なことではないが，電子化取引実現の鍵であり，これを解決しない限り，書類が残ることになる。

(2)　電子化取引の条件

次に，電子化取引を行うための条件 ― すなわち，コンピュータ・ネットワークを通じて交換するメッセージに，どのような機能があれば電子化取引が可能になるか ―について，セキュリティの面から分析する。

①　コンピュータ・ネットワーク

基本的な条件は，指定された行先に，途中で内容が変わることなく，メッセージを正確に送り届けることである。ネットワークが複雑になると，この条件を満たすことが，だんだん難しくなるという問題がある。

セキュリティという観点でこの問題をとらえる時は，次の２つの要素を考えなければならない。

ⓐ　自然発生的な原因による危険性

ⓑ　人為的な原因による危険性

上記ⓐについては，近年技術的対策が進み，所要コストにこだわらなければ，満足すべきレベルのネットワークを構築することは可能であろう。問題は，ⓑである。ⓑについては，その原因が内部（例えば，ネットワーク管理者）にある場合と，外部にある場合がある。通常，内部者による妨害を技術

的に防止するのは非常に難しい。一方，外部者による妨害を防止するのには，次項でも述べるが，メッセージ認証及びメッセージ暗号化が有効である。

② コンピュータ記録

電子化取引では，従来の伝票をコンピュータ記録に置換える。そこで，この伝票を以下では電子化伝票と呼ぶことにする。電子化伝票に要求される条件は，保存性（データが破壊されないこと）と，抗改ざん性（改ざんに対する安全性）である。

第1に，電子化伝票は記録される媒体によって，安全度が異なるという問題がある。例えば，マイクロ・フィッシュ等に記録されると，安全度が高い。しかし一般的に処理中は，―例えば，電子化伝票を他課へ送ったり，取引先へ送付する時等 ― 磁気媒体あるいはメモリ中に記憶されるため，記録される媒体そのものに，保存性や抗改ざん性は，期待できないと考えるべきである。もっとも，各種の手法の進歩は，電子化伝票の保存性を飛躍的に高めたが，抗改ざん性（改ざんは主に人為的原因で発生する）については，何ら改善されていない。

第2に，電子化取引に用いる電子化伝票は，同一データが，運用形態も管理も異なる2つ以上の応用システムで保管されるという問題がある。管理が異なるということは，同一である筈の2つ以上のデータ間に食い違いが発生すると，これがただちに，企業間の責任問題（訴訟問題）に発展する可能性があることを意味する。従って，電子化取引に用いる電子化伝票は，応用システム内に保管されている場合も，保存性と抗改ざん性が保障されていなければならない。

③ 電子化伝票のオーソライズ

前述の電子化伝票の保存性や抗改ざん性は，その電子化伝票の発生から消滅まで維持する必要があるかというと，そうでもない。ここで，電子化伝票の典型的な一生を考えて検討する。図3－19 の伝票送信時点までは，保存性や抗改ざん性は，B企業にとって問題ではない。というより，電子化伝票の中には，B企業へ送信されることなく，A企業内で消滅してしまう伝票も

かなりあるが，これらについては，A企業，ネットワーク及びB企業を含めた保存性や抗改ざん性は，不要である。問題は，図3－19のように，ネットワークを用いて送信した電子化伝票であり，かつ，伝票送信以後の保存性と抗改ざん性である。

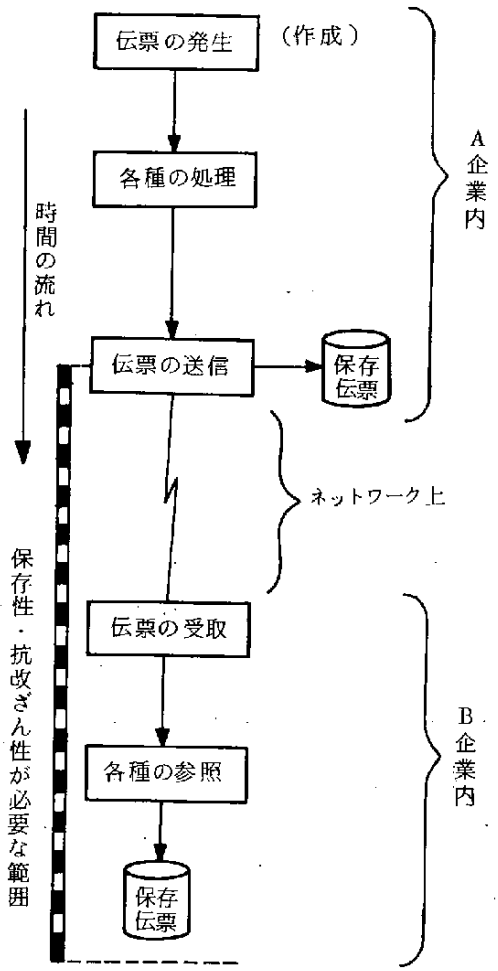


図3－19　典型的な電子化伝票の一生

A企業からB企業へ送るメッセージには，電子化伝票以外に単なる情報もあるので，この2つを区別しなければならない。そこで，正式な電子化伝票であることを，送信する時に宣言しておく必要がある。これは，電子化伝票のオーソライズと考えられる。従って，電子化伝票のオーソライズ以後消滅するまで，保存性や抗改ざん性が必要と言うことになる。

オーソライズは，図3－19の場合，A企業が宣言したことをB企業へ伝達することによって成立する。そのため，宣言したという証拠をどのように残すかという問題に帰着する。A企業内では，承認のない宣言（不当に社長の印を用いることに当る。）を防止しなければならないという問題がある。

3.3.2 基本的対策手法

前項で解決すべき問題として，

① ネットワーク上での人為的妨害の防止（破壊，改ざん，介入等）

② データ（電子化伝票）保管時の保存性及び抗改ざん性の確立

③ データ（電子化伝票）のオーソライズ手法

を述べたが，本項では，その対策方法について述べる。

(1) メッセージ伝送時における妨害対策

最初に技術的対策について検討する。メッセージを指定された送信先へ確実に届けるための基本的技術として，相手先確認技術がある。改ざん対策の基本的技術としては，メッセージ認証技術があり，相手先確認を兼ねることができる。メッセージの漏洩対策としては，メッセージの暗号化が最も有効である。これらの基本的技術の詳細は，第3.4節で述べるが，これらの基本技術は，独立で用いるよりは組合わせた方が，各種の妨害に対して，より一層有効となる。例えば，メッセージ検証子（メッセージ認証に用いる）を付加したメッセージを暗号化すると，改ざんに対しても漏洩に対しても安全になる。従って，どのように組合わせるかが大きな検討課題となる。

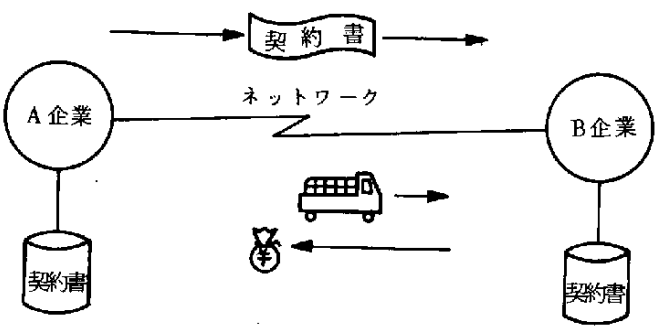
さて，メッセージ認証技術は，改ざんを発見する技術であり，実際は改ざんを防止する技術ではない。しかし，改ざんを発見できれば，再送によって正確

にデータを送ることができるので，結果的に改ざん防止になる。しかし，再送の時，自然発生的エラーが発生するようでは，正確にデータは送れない。従って，これらの技術は，元々信頼性の高いネットワークに適用して初めて有効になる技術であり，ネットワークの信頼性は，すべての対策の基本的要素である。

次に，運用上の対策について触れておく。運用上の対策は，ネットワークの形態に依存する。例えば，ネットワーク管理者を設けると，その管理者を誰にするか，そして管理組織内部での不正に対処する方法が問題になる。慣用暗号を用いると暗号キーの運用が問題になり，メッセージ認証では，そのアルゴリズム（規約：ルール）をどのような手続きで決定するかが問題になる。従って運用上の問題を検討するためには，ネットワークの形態を定める必要がある。

(2) データの保存，改ざん対策

分析を容易にするため，A，B２企業間を通信回線で結び，A企業で作成したメッセージ（電子化伝票）をB企業へ送信し，B企業で保管する場合について検討する。尚，同一のメッセージをA企業でも保管するものとする（図３－20を参照）。この場合，エラーやミスあるいは悪意の改ざん等により，メッセージの安全性が脅かされる機会をまとめると，表３－２のようになる。



・ 電子化伝票を取引を行う企業A，Bの磁気ファイルに保存することとし，伝達をネットワークを通じて行う。

図３－20　電子化取引基本モデル

表３－２　メッセージが脅かされる機会

区分	時点 ＼ 原因	A企業内部	B企業内部	ネットワーク	悪意の第３者
①	メッセージ作成時	○			
	作成後送信までの保管	○			○
②	送信中			○	○
③	受信後の保管（A企業）	○			○
	受信後の保管（B企業）		○		○

①　メッセージ作成時，作成後送信までの保管

この段階では，データはA企業内にあり，A企業の責任でメッセージを保護する必要があり，また可能である。企業内システムのセキュリティ対策の一環である。

②　ネットワーク上（送信中）

この段階の対策は，本項(1)で述べた。

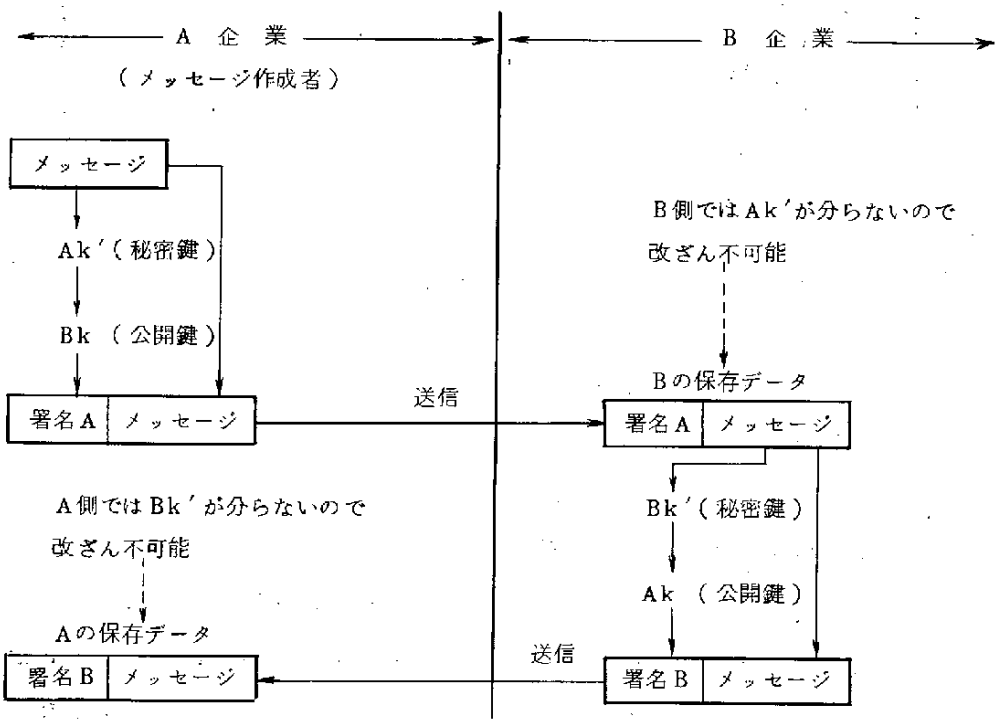
③　メッセージ受信後の保管

B企業受信後の保管では，複雑な問題がある。A企業の作成したメッセージは，AとB共有のメッセージになり，A／B共に承認した場合を除いて，その内容を変更することは許されないからである。従って，A企業，B企業共に，共有メッセージの変更が，特別な場合を除いて，不可能なようなメカニズムが必要である。これに適用できるアクセス・コントロールは，現存しない。

前記①の段階では，メッセージはA企業の所有であったが，②を通して③になった時，メッセージは，A企業とB企業の共有になった。A企業の単独所有の間は，A企業がメッセージをどのように加工しても，B企業にとっては全く無関係だった。しかし，A／B共有になってからは，両企業共，単独では変更できなくなった。A企業の単独所有からA／Bの共有になった時，両者の相互の承認が成されたとも考えられる。すなわちオーソライズであるが，

これについては，(3)で述べる。

いづれにしても，図３－20では，保存性も抗改ざん性も期待できない。そこで，技術的対策を一つ述べる。それは，ＲＳＡ暗号によるデジタル署名の技術（詳細は，第3.4.2項及び第3.4.3項を参照）の応用である（図３－21 を参照）。一方，メッセージのコピーを第３者の機関で保管しておく方法がある。それについては，次の(3)で述べる。



・ 証拠データ作成後にA，Bでかってに秘密鍵（公開鍵）を変更しないような処置が必要

・ 本質的に保存性を強化することにはならない。

図３－21　デジタル署名応用による
保存メッセージの改ざん対策

(3) メッセージのオーソライズ

書類システムにおけるオーソライズとは，押印（サイン）と考えてよいだろう。その意味は，書類を渡す相手に，これ以後内容を変更しないし，内容に責任を持つということである。そして，受取者もその押印（サイン）をオーソライズとして承認する。

しかし，コンピュータ・メッセージでは，印に対応する機能を何か付加しなければ，一般のメッセージとの区別がつかないという問題がある。例えば，デジタル署名を用いる方法もあるが，当プロジェクトでは，仲介者がメッセージのオーソライズを保障する方法を，検討した。

① 調停者の存在

オーソライズとは，(2)で述べたように，承認したことを宣言することであるが，宣言したかどうかが重要になるのは，トラブルが発生した時である。トラブルが発生した時，取引を行った２者間の交渉だけでは解決しない場合があり，この時，第３者が調停することがある。調停者は，トラブルが起きて交渉を行っている２者間で取り交わされた書類の，客観性についてチェックする。その際，書類に印があれば（オーソライズが宣言されていれば），客観的資料と見なす。すなわち，オーソライズにおける宣言とは，将来何かの理由でメッセージ内容が調査された時に，客観性を保障する証拠なので，その時まで保存されなければならない。従って，オーソライズとは，この調停者に向けて宣言するとも考えられる（ただし宣言の時，調停者は実在しない）。

② 仲介者を含めた電子化取引

書類方式では，トラブル発生時に初めて調停者が介入する。ただし書類は，あらかじめ調停者の介入を予測して，作成／承認されている。これは書類方式独特のすぐれた機能と考えられる。

書類とは，物理的形態も機能も異なるコンピュータ・メッセージに対して，同じ処理形態を適用するのには，無理があると思われる。

そこで，メッセージの作成／承認段階から調停者が介入する方法が考えら

れる。もっとも，この段階では調停者ではなく，ただの仲介者である。書類方式とは異なるものの，その本質的な形態は極めて近い。図３－22は，仲介者を含む電子化取引である。仲介者は，企業A及びBの保存メッセージの保障データを保持することにより，オーソライズの機能を実現する。

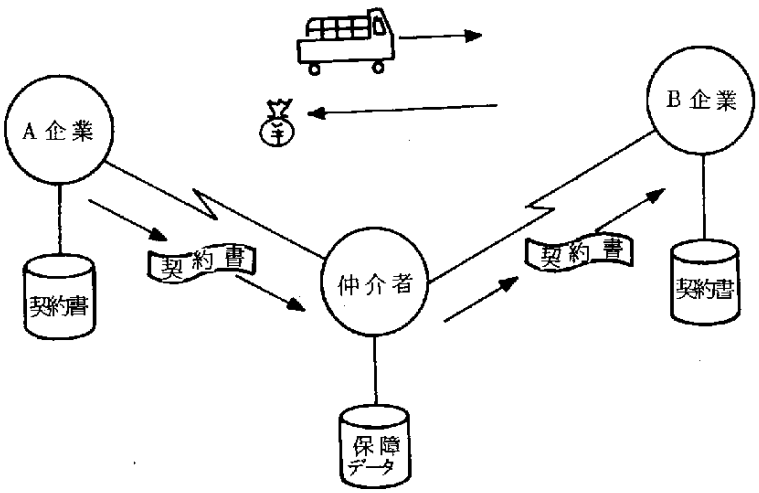


図３－22　仲介者を含む電子化取引

③　仲介者の役割

A企業がB企業へメッセージを送るとする。A企業は，送信する前に，仲介者に対して承認したことを連絡しておく。仲介者は，この承認宣言（すなわちオーソライズ）を記録保存しておく。メッセージを受取ったB企業も承認したことを仲介者へ連絡する。そしてB企業の承認も，仲介者は記録保存する。後日トラブルが発生した時，仲介者はこの承認の記録を提示し，メッセージの客観性を保障する[*1]（以上，図３－23を参照）。

仲介者は，さらにメッセージ内容の記録を行って，内容保障（改ざん対策）

---

*1 ：この場合，A企業及びB企業の保存メッセージは，改ざん対策が成されているものとする。

を行うことも可能である。ただし，ここまでの議論は，すべて仲介者に悪意がない場合に成立する。仲介者に悪意があっては，仲介方式は無意味になる。そのため仲介者は，公正中立な第３者でなければならない。以後この仲介者を，公証機関と呼ぶことにする。

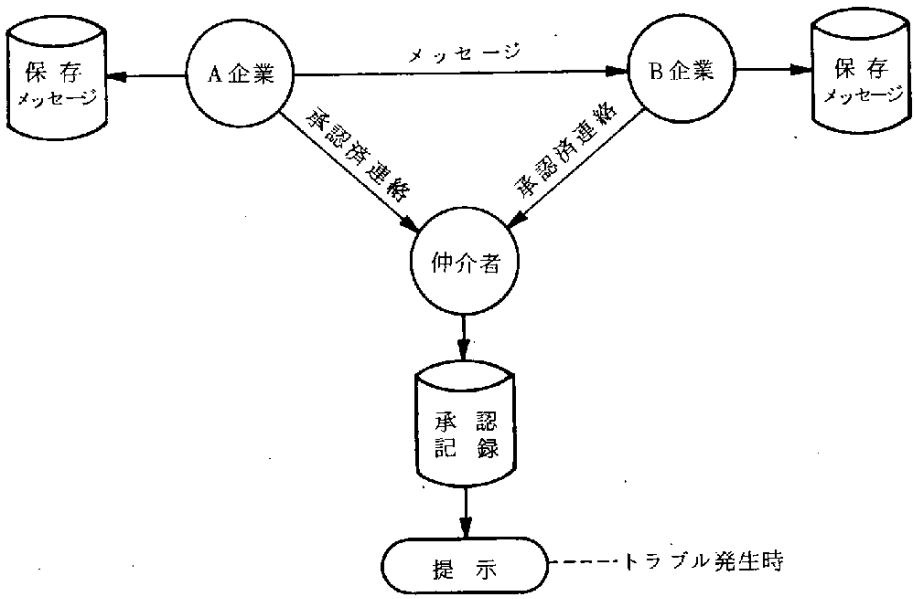


図３－23　仲介者による承認（オーソライズ）の記録，保存

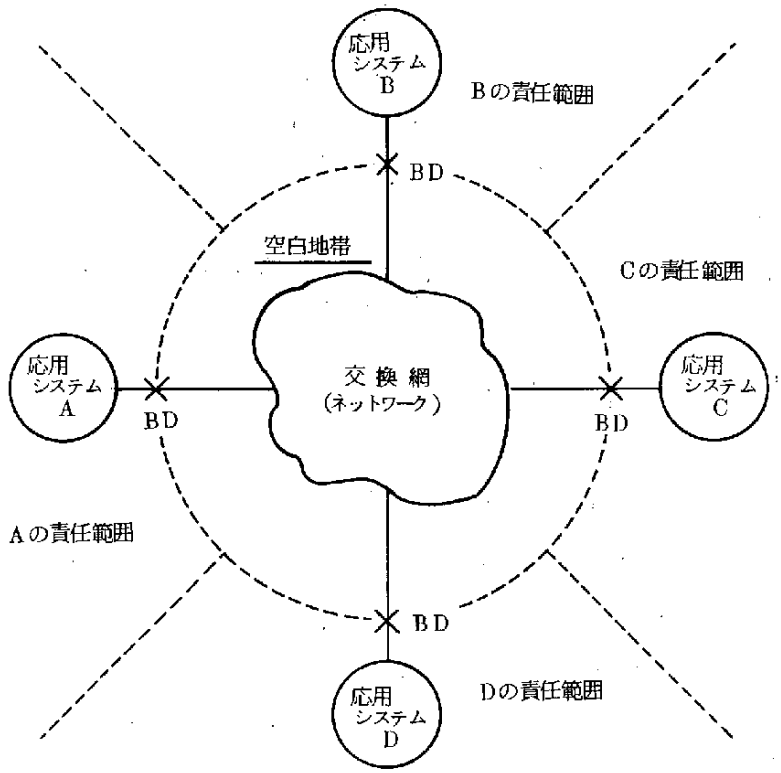
3.3.3　システム化構想への展開

本項では，前項での分析結果を実際のコンピュータ・ネットワーク・システムに投影し，現実的な対策手法あるいは技術について述べる。

(1)　責任分解点と責任者

電子化取引ネットワークは，管理運営主体の異なる複数の応用システムを接続する。接続した結果，個々の管理運営者の責任範囲が不明確になっては困るので，これを明確にする境界が必要になる。もっとも単純で明確な境界は，物理的境界である。そこで，セキュリティ対策の第一歩は，この物理的境界を定めることである。

次に，どこに境界を設けるかが問題である。ごく自然な考え方は，ネットワークと応用システムとの接続点に設ける境界である。この考え方に従って，交換回線網を用いて図3—24のように接続したネットワーク・システムに境界を設けると，個々の応用システムの責任範囲は明確になるが，交換回線網の部分（ネットワークの部分）に，管理運営者の空白地帯が生じてしまう。この部分では，物理回線の管理運営者は間違いなく存在するが，そこを通過するメッセージ（例えば電子化伝票）の内容保障を行う（セキュリティを保障する）管理運営者は存在しない。そこで，新たな管理運営者を設ける必要があるが，それは，第3.3.2項で述べた仲介者，すなわち公証機関である。



BD：物理的責任分解点

図3－24　セキュリティ対策の責任範囲

(2) セキュリティ・レベルと防波提

ネットワークによって結ばれる，すべての応用システムのセキュリティ・レベルは，同一であることが理想であるが，現実的には，すべての応用システムのセキュリティ・レベルは，異なると考えなければならない。その結果，ある応用システムのセキュリティ上の問題が，他の応用システムに波及する可能性があり，大きな問題点になる。

この対策としては，ネットワーク上に統一的なセキュリティ対策を施し，ネットワーク上を通過するメッセージのセキュリティ・レベルを統一する方式が有効である。ネットワークを通じて送られてくるメッセージのセキュリティ・レベルが明確であれば，それを受取る応用システム側での対応も容易である。もし，セキュリティ・レベルが不明確であれば，メッセージを受取る応用システムでの対応は，困難を極める。

公証機関が，ネットワークのセキュリティを統一的に管理すれば，ネットワーク上のメッセージのセキュリティ・レベルを統一化することが可能になり，ここで述べた問題点を解決することができる。

(3) ネットワーク形態と公証機関の役割

多数の応用システムを結合して，自由にメッセージの交換を行うのであれば，交換可能なデータ通信回線を用いるか，米国型のＶＡＮのような共同利用ネットワークを用いるのが，最も経済的である。このように結論するのは，そう難しくないだろう。

ここで，公証機関の位置付けを考えて見る。この共同利用ネットワークには，2種類の管理が必要になる。それは，

① ネットワークの物理的管理（通信回線の管理）

② ネットワークのセキュリティ管理

である。公証機関は，②の管理であり，①に対してはユーザである。もっとも，①と②を兼ねた管理者も可能であるが，責任（逆の見方をすれば権限）は分割した方が，セキュリティ上では一般的に有利である。

(4) メッセージのセキュリティ・レベル

ネットワークを用いて転送するメッセージのすべてが重要情報であるということは，実際にはあり得ないだろう。メッセージの中には，極めて重要な情報もあれば，漏洩してもかまわない情報もあるだろう。従って，ネットワークには，転送するメッセージに見合った保護レベル（セキュリティ・レベル）がある方が合理的である。

このことは，ネットワークの統一的セキュリティ対策と一見矛盾するように思えるが，そのような心配はない。統一的とは，ネットワーク内のセキュリティ・レベルが，どこでも同じであることを意味し，転送メッセージに見合ったレベルが存在するとは，統一的レベルがマルチ・レベルになっていることを，意味するからである。

例えば，ネットワーク内のどこでも，「㊙」というレベルは同一であり，「秘」というレベルもまた同一である。しかし，「㊙」と「秘」というレベルは，異なるのである。郵便に例えれば，「書留」と「封書」との違いと同じである。もちろん，このようなセキュリティ・レベルを設けるのは，コストを削減するためである。

(5) 対策手法

一般的に対策手法は3種ある。物理的対策，技術的対策及び運用による対策である。これらの対策を，バランスよく実施するのが従来の手法であるが，ネットワークの場合には少々違う様相を呈する。ネットワークでは，物理的対策が困難なので，技術的対策が主体となる。現在有効な手法は，メッセージにチェック・データを付加する方法と暗号化である。いづれの方法も，送信する前にメッセージを「ある約束」に基づいて変形し，受信後に「同じ約束」に基づいて元にもどすことを基本とする。どのような「約束」を用いるかを，適切に管理する必要があり，この部分では，運用上の対策が重要になる。「約束」は秘密にする必要があるからである。

公証機関は，この「約束」を統一的に管理することによって運用上の対策を容易にする。もちろん，この「約束」の管理にも，現在ではコンピュータを用

いる。このコンピュータ・センタは，公証機関が管理運用するネットワーク・セキュリティ・コントロール・センタであり，以後略して，ネットワーク・セキュリティ・センタ（ＮＳＣ）と呼ぶことにする。ＮＳＣは，「約束」の管理だけでなく，公証用ログの記録も同時に行う。

ＮＳＣ自身もセキュリティ対策の対象となる。しかし，ＮＳＣのセキュリティ対策は，従来と同様な対策手法が使える。すなわち，物理的対策，技術的対策及び運用上の対策をバランスよく実施すればよい。

(6) システム形態

最後に，これまでに述べた分析結果に対応した，ネットワーク・システムの構築について，概観する。

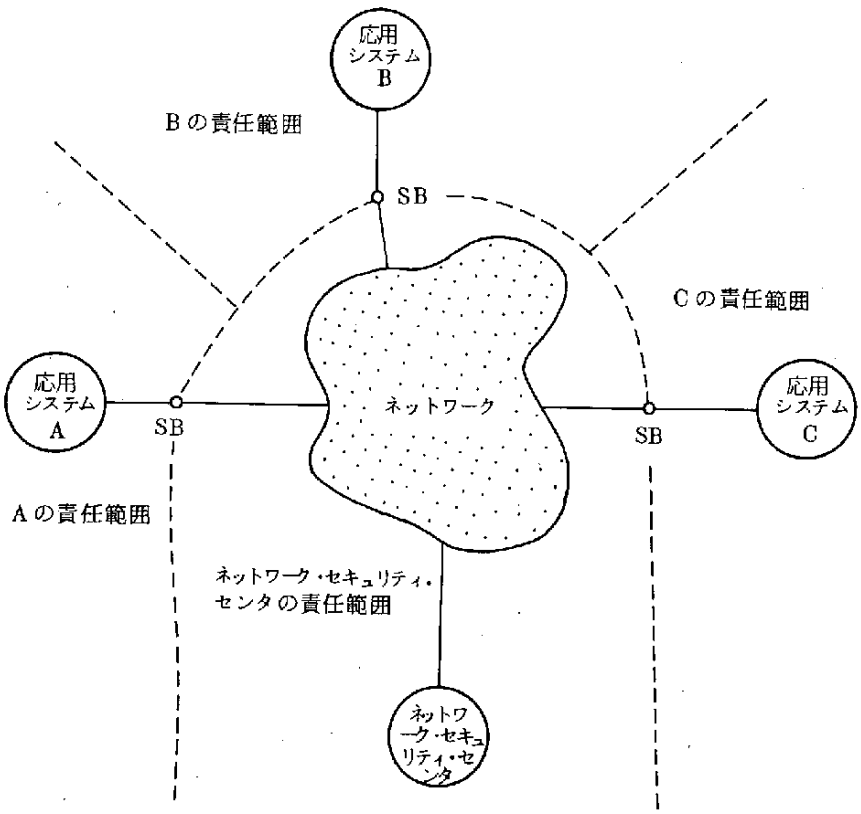
最初にネットワークを設定する。このネットワークは，交換機能を持ち，現在の技術水準に見合った信頼性を保持しているが，セキュリティ対策に関する特別な仕組みは，ないものと仮定する。そこでセキュリティ対策のために，ネットワーク・セキュリティ・センタ（ＮＳＣ）を設け，ネットワークへ接続する。

しかし，ＮＳＣだけでは技術的対策はできない。なぜなら，メッセージは送信前に加工し，受信後に復元することによって，セキュリティ対策を行うからである。そこで，メッセージの加工／復元を行うための特別なハードウェアを，メッセージの送受信点に設置する。この特別なハードウェアを，セキュリティ・ボックス（ＳＢ）[*1]と呼ぶことにする。このＳＢの先に，個々の応用システムが接続される。従って，システム形態は，図３－25のようになる。

ＳＢは，ＮＳＣと個々の応用システムとの責任分解点になる。ＮＳＣは，ＳＢをリモート・コントロールすることによって，メッセージ加工／復元のための「約束」を管理する（ネットワークの統一的セキュリティ管理）。ＮＳＣはメッセージ内容を記録する（公証用ログ）。もちろん，ＮＳＣは，公証機関によって管理運営されることになる。

＊１：　昨年度提案のＳＢは，メッセージ・ロギング装置である。今年度提案のＳＢは，メッセージのセキュリティ対策を行うためのセキュリティ機構であり，ロギング機構はない。

本節での説明は，これで終ることとし，さらに具体的な説明は，第3.5節で行う。その前に第3.4節で，ネットワークに関する基本技術あるいは重要なセキュリティ技術についての，検討結果を述べておく。



ＳＢ：特別なハードウェア（セキュリティ・ボックス）

図３－25　システム形態

3.4 ネットワーク関連基本技術

本節では，ネットワークの基本的ハードウェアである通信回線およびネットワークのセキュリティ対策と特に関連の強い技術

- 暗号化技術
- メッセージ認証技術
- 端末確認技術

等について，最新の動向や将来の見通し等をまとめた。

一方，最近特に活発になってきた内外のネットワーク・セキュリティ対策の標準化動向についても，簡単にまとめた。1984年1月現在では，まだ，内外共に標準化案の提案にとどまっている。全銀協では，基本となるプロトコルの提示は行われているものの，本格的セキュリティ対策は，なお流動的である。

3.4.1 通信回線

3.4.1.1 回線の種類

通信用の回線（伝送路）には，大別して有線系伝送路と無線系伝送路とがある（図3－26参照）。

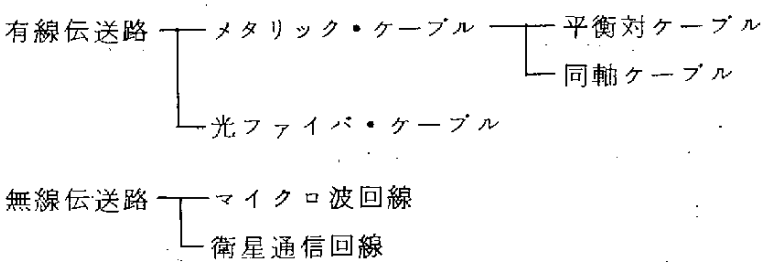


図3－26 通信回線の種類

(1) 有線伝送路

有線伝送路としては，金属導体を使用した平衡対ケーブルと同軸ケーブルのほか，ガラス・ファイバを使用した光ファイバ・ケーブルがある。

① 平衡対ケーブル

平衡対ケーブルは，2本の金属導体（銅又はアルミ）をバランスさせた対により信号を伝送するもので，安価ではあるが高周波伝送には適していない。主として加入者線等に使用されている。

② 同軸ケーブル

同軸ケーブルは，円筒状の外部導体の中心に内部導体を配置した構造の不平衡形ケーブルである。高周波における遮へい性が極めてよく，また，低損失高耐電圧の特質を有しているため，多重化が容易で，大容量の長距離回線用として広く使用されている。

③ 光ファイバ・ケーブル

光ファイバ・ケーブルは，ガラス・ファイバを光の導波路として用いて光信号を伝送するもので，従来の金属導体を用いた通信ケーブルと比べ，低損失，広帯域，無誘導等の優れた諸特性を有しており，伝送路のデジタル化，大容量化，広帯域化を経済的に実現するものとして期待されている。

(2) 無線伝送路

① マイクロ波回線

災害が多く，山地に富むという日本の国情には無線が適していることもあって，日本の無線回線は非常に発達しており，その主流をなすものがマイクロ波回線である。

マイクロ波はその周波数が短波，超短波に比べて高い（300 MHz ～ 30 GHz）ので，小口径のアンテナでも鋭い指向特性が得られる。また，互いに見通しのある2地点間では，伝搬損失も少なく，短波などの他の無線方式に比べ安定しているので，高品質の回線を経済的に実現できる。

② 衛星通信回線

昭和40年のアーリバード（インテルサット1号）衛星の打ち上げ以来，衛星通信は国際通信網の中核として目覚ましい発展を遂げてきた。また，昭和47年にはカナダが国内通信用として初めて衛星を打ち上げた。

現在では，通信衛星はその特徴をいかして，国際通信用のみならず，

国内通信用にも積極的に活用されるようになってきている。日本では，昭和58年2月に国内実用通信衛星が打ち上げられた。

3.4.1.2　多重通信方式

多重通信方式には，周波数分割形と時分割形の2方式がある。

(1)　周波数分割多重化方式（ＦＤＭ）

多数の信号を周波数軸上に一定間隔で配置し，1対の媒体で多数の信号を同時に伝送する方式である。

(2)　時分割多重化方式（ＴＤＭ）

多数の信号を時間軸上に一定の間隔で並べ，1対の媒体で多数の信号を順次に伝送する方式であり，振幅をコード化して送る，ＰＣＭ方式が一般的である。

3.4.1.3　交換方式

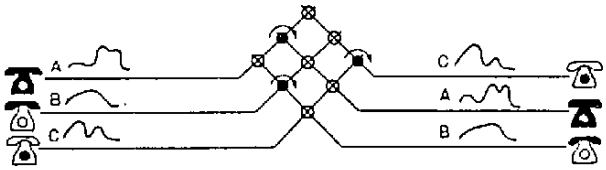
(1)　空間分割方式

交換機の自動化は，ステップ・バイ・ステップ方式から始まり，その後，クロスバ交換機，電子交換機へと発展してきた。これらの交換機の通話路は，いずれも基本的には多数の接点を配置し，一つの通信に対し一つの接続路を専有するもので，空間的に配列された接点により接続路を形成することから空間分割方式と呼ばれている（図3－27ⓐ参照）。

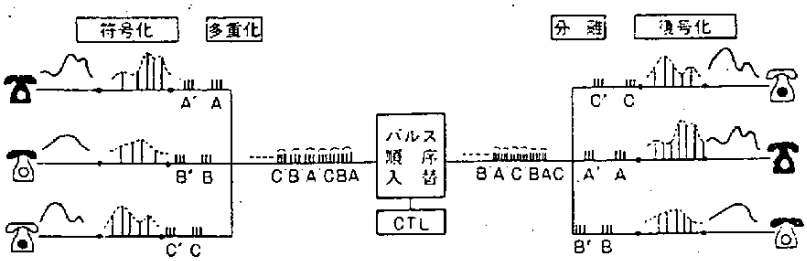
(2)　時分割方式

空間分割形交換機の通話路は，主として電磁形スイッチが用いられていることから，その小形・経済化には限界があること，デジタル多重伝送路との整合性に欠けることなどの問題がある。

これらの問題を解決するものが，デジタル交換機で，その通話路はＬＳＩなどの電子部品で構成され，その高速性を生かし，一つの通話路を多数の通信で時分割して多重利用するもので，時分割方式と呼ばれている（図3－27ⓑ参照）。



ⓐ 空間分割方式



ⓑ 時分割方式

図 3－27　空間分割方式と時分割方式

(3)　パケット交換方式

パケット交換は蓄積交換の一種で，端末相互間で直接情報の送受がなされず，発信端末から送出された情報を，交換機がいったん受信してメモリに蓄積した後，網内を高速で転送して着信端末に送り届ける方式である。

この場合，網内を転送される情報は，ある一定のブロックに分割され，各々のブロックに宛先情報や誤り制御情報など，転送に必要な制御情報を含んだヘッダが付けられる。これをパケット（小包の意味）と呼んでいる（図3－28参照）。

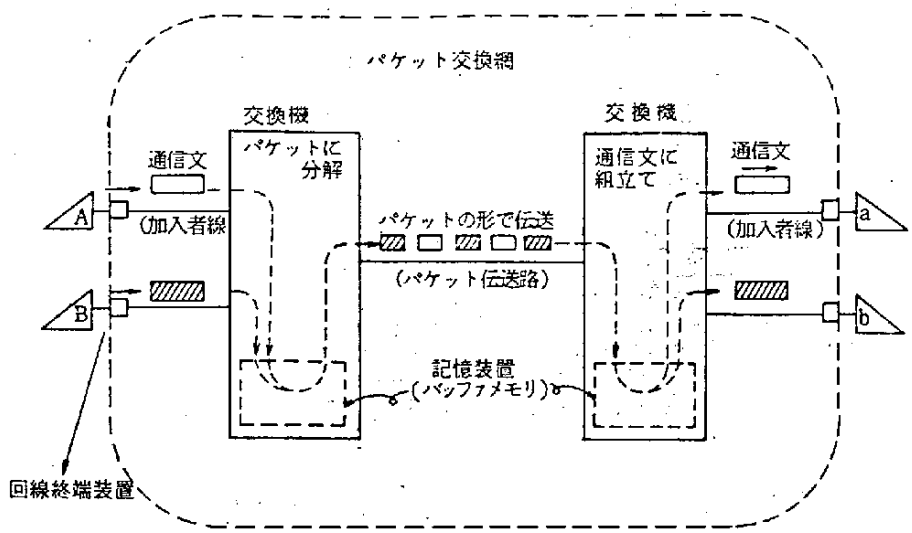


図 3－28　パケット交換方式

3.4.1.4　通　信　網

(1)　既存の公衆ネットワーク

日本の公衆ネットワークは，電話網のほか，電報中継交換網，加入電信網，デジタル・データ交換網（DDX）およびファクシミリ通信網の5つの独立した網から構成されている。

①　電　話　網

電話網は，加入数約4,100万，電話機数約6,000万を有し，今や全国が自動でかつ即時に通話できるようになっている。電話網のような大規模な網を形成するには地域を何段階かに区分し，それぞれの区分内で最も経済的な網形態をとる必要があり，約6,800の電話局を結ぶため，562の集中局，81の中心局，8つの総括局で構成される階位構成がとられている。

②　電報中継網

現在の電報中継網は，電報を一度紙テープにさん孔して交換する方式を採用しており，全国約300の電報局が12の中継交換機に収容されている。この網は50 b/s のパルス伝送による待時式の中継網となっている。

③ 加入電信網

加入電信網（テレックス）は，国際テレックス・サービスが開始されたのに伴い，昭和31年から始まった。加入電信網は伝送速度が 50 b/s に限定されていること，電話網を利用するファクシミリや高速なデータ端末の普及などによって，昭和51年以降減少傾向にある。

④ デジタル・データ交換網

電話網をデータ通信に利用するには，回線品質が不十分であったり，接続時間が長いなどの問題がある。このため，データ通信用の新しいネットワークとして，任意の相手と高速・高品質のデータ伝送が可能なデジタル・データ交換（ＤＤＸ）網がつくられ，昭和54年に回線交換サービス，昭和55年にパケット交換サービスが始まった。

⑤ ファクシミリ通信網

近年，ファクシミリは年率 20～30 %と急速に増加し続けており，電話網を利用するものが現在では25万台にも増大している。漢字を必要とする日本ではファクシミリの効用が高く，将来は商店や小規模事業所あるいは家庭にまで普及していくものと予想されている。このため，端末を出来るだけ単純化，低廉化するとともに通信コストの経済化を図るため，複雑・高度な機能をネットワーク側にもたせたファクシミリ専用網がつくられ，昭和56年からサービスを開始した。

(2) 今後の公衆ネットワーク

① デジタル通信網（デジタル統合網）

現在，電気通信網としては，前述のように電話網をはじめ電報中継網，加入電信網，デジタル・データ交換網，ファクシミリ通信網があり，さらに近くビデオテックス通信網が構築されようとしている。

これらの通信網は，それぞれの目的に応じた個別のネットワークとしてつくられており，それぞれ独立した交換機や回線を有し，また，番号体系や料金方式も異なっている。

このように，従来の通信網が個別網で拡大してきたのは，サービス毎に発

展が異るうえ，個々のサービスについて，主としてアナログ技術でその時最適と思われる設計をし導入せざるを得なかった背景がある。

しかし，通信形態，内容がますます多様化してくると，個々の新しいサービスのために個別のネットワークを構成するのは，不経済であり，新サービスに対する即応性にも問題を生じる。このため，ネットワークの統合ということが考えられるようになってきた。当面は，データ，ファクシミリ等の非電話系サービスに適した個別のデジタル・ネットワークを形成するとともに電話網のデジタル化を進め，将来は，これらの網を統合したデジタル通信網（デジタル統合網）へ発展させることが計画されている。

② デジタル通信網の特徴

デジタル通信網において，豊富な信号がとれることや，各種の加工処理が容易に行えるなどの特徴を活かして，現在のサービスの高度化や新サービスの提供が可能となろう。

デジタル化の特徴を活かしたサービスとして，次のものが考えられる。

ⓘ 加入者線信号の充実

発呼者の電話番号や通話料金等の通知

ⓘⓘ 蓄積・変換処理が容易

メディア変換，異速度端末間通信，同報通信，代行通信

ⓘⓘⓘ 高品質な通信

デジタル伝送により雑音，歪の累加がなく通信品質が向上

ⓘⓥ 通信容量の拡大

64 Kb/s を基本としたデジタル・パルスが経済的に実現

ⓥ 複合通信サービスの提供

1つのネットワークで各種のサービスを統合化して提供

(3) その他の通信網

上述の通信網以外のものとして，農漁村等での通話および放送を目的とした有線放送網や，高速道路で使用されている道路通信網，国鉄，警察，電力会社等の専用網などがある。

さらに，最近では同軸ケーブルを利用し，主としてテレビ画像を中心に情報転送を行うCATVの網なども出てきている。以下に，最近特に注目を浴びているCATVについて紹介する。

〔CATV〕

CATVは，テレビ電波の受信困難な山間辺地における難視聴対策として，1949年に米国で誕生した。

CATVは，同軸ケーブル等の広帯域伝送路を使用するため，難視聴救済以外にもテレビの各種の自主番組の送信，さらには双方向通信機能を付与してコンピュータと接続した多彩なサービスの提供も，行われようとしている。CATVの発展とともに，CATVの言葉の意味も変化しつつある。

① Community Antenna Television 又は Common Antenna Television
山間辺地やビル陰地帯でテレビ番組の再送信を行う施設

② Cable Television System
テレビ放送の再送信だけでなく，自主番組放送，ピックアップ中継放送などのサービス機能を備えた施設

③ Cable and Telecommunication Television System
前述のサービス機能のほか，双方向通信機能を付加して，ファクシミリ端末等による相互通信，コンピュータと接続した各種の情報サービス等が可能である。この段階では，CATV は地域的な広帯域通信網としての性格を持つ。多摩ニュータウンや東生駒ニュータウン地域などで実験システムが実施されている。

3.4.1.5 ネットワークの信頼性と安全性

(1) 回線の品質

回線の品質をビット誤り率でながめてみると，一般には次のようにいわれている。

・電話網（アナログ網） 1,200 b/s で 1×10^{-5} 程度

・特定通信回線（符号品目） 1×10^{-5} 以下

・ＤＤＸ（回線交換）　　1×10^{-6} 程度

・ＤＤＸ（パケット交換）　1×10^{-10} 程度

デジタル・データ交換網は，電話網や符号品目回線の品質に比べてかなり良好な値といえる。

(2) 安　全　性

一昨年の公社職員による銀行カード偽造事件以外に，目立った盗聴事件等は発生しておらず，日本における通信回線の安全性に対する評価は，一般的に高いといえる。回線の提供側（電電公社）は，通信の秘密確保は当然のこととして，事件以降，運用面，設備面において，より一層の対策の強化を図るとともに，情報保護技術についても積極的に研究開発を進めている。

しかしながら，基本的には，通信そのものはトランスペアレントなものであり，情報の中味によって，それをどう保護するか（暗号化等の情報保護を施すかどうか）は利用者側の判断と考えている。

一方，利用者側の方をみると，最近ではセキュリティに対する関心が高くなっているとはいえ，ネットワークは安全なものとする意識が強く（安全であること自体は望ましいことではあるが），情報保護に対する対策や投資にはまだ消極的な状況にあり，欧米に比べて，立ち遅れを示している。これには，“自らの安全は自ら守る”という欧米と，安全が社会的に良く維持されている我国との，国情の違いもあらわれているように思われる。

(3) 今後の問題

通信技術の発達とともに，自動車電話をはじめとする移動通信および衛星通信が実用化され，これらは，いつでもどこでも情報伝達が可能である，という利便性を有しており，今後の利用はますます増大するものと思われる。

だが，セキュリティの面からは，その利便性と裏腹に（かなり困難ではあるが），盗聴の可能性の問題も抱えている。外国の一部には，既に暗号化を行っているところもあるようだが，暗号化等の保護対策を実施するには，それだけの設備投資が必要となり，料金的にも高価になるなどの問題がある。

また，データ通信の高度化，多様化とともにホーム・バンキング，ホーム・

ショッピング，ファーム・バンキングなどの言葉で表わせるように，通信回線を介して，マネー・フロー，物流フローが行われるようになってきており，今後さらに，その傾向は強くなってくるものと思われる。

このように，通信回線を介して送られる情報内容は，単なる日常のあいさつ程度の会話から，個人や企業の重要情報に至るまで，一段と拡がりを示しつつあり，これらの重要情報についてそれをどう保護するか，また，誰がそれを行うのか，真剣に検討する必要があろう。

3.4.2 暗号化技術

暗号は従来から軍事や外交上の秘密通信の手段として用いられてきた。しかしながら，最近のコンピュータ技術の進歩や情報ネットワークの拡大に伴い，暗号はいつのまにか私たちに身近なものへと変貌しつつある。従来の暗号を“守り専門の技術”であったとすれば，最近の暗号は“攻守とりそろえた技術”と言えそうである。すなわち，積極的に暗号を用いることにより，ネットワーク等に付加価値を生むことができる訳である。

3.4.2.1 暗号の目的

暗号の目的は大別して転送データの保護，ファイル等の蓄積データの保護と端末確認等のアクセス制御がある。

(1) 転送データの保護

通信における転送データの保護には以下に示す2通りの意味がある。

① 第3者に電文が盗まれても内容がわからないようにする。

② 第3者による電文の改ざん等の変更を防ぐ。

以上のような目的において，暗号は古くから用いられてきた。

(2) 蓄積データの保護

コンピュータの利用が増えるにつれて，内部に格納されているデータの保護が必要となってくる。たとえば；企業における重要機密文書や病院の医療カルテなどが裸で格納されており，改ざんや内容コピーが容易にできるとしたら大

きな問題となるであろう。

上述の転送データと蓄積データの保護に関する概念図を図３－29に示す。

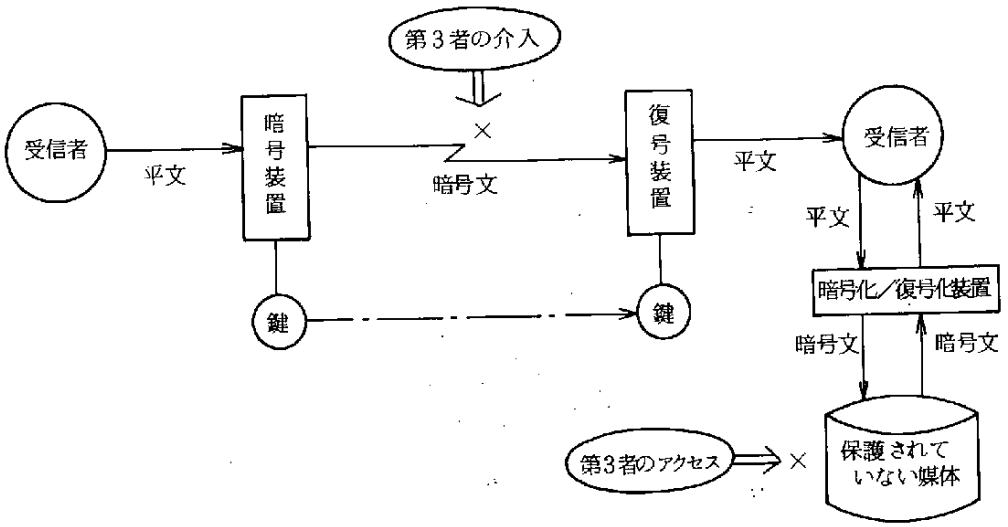


図３－29　転送データと蓄積データの保護

(3)　アクセス制御

暗号は不当なユーザのアクセスを防ぐことができる。たとえば，正当な鍵を持っていないユーザはデータベースやＣＡＴＶなどのサービスが受けられない。また不正なネットワーク・アクセスも防ぐことができる。このように暗号は転送データや蓄積データを保護するだけでなく，自らのサービスをより活性化するためのアクセス制御にも適用できる。

3.4.2.2　古典的暗号

暗号の歴史は極めて古く，約4,000年前の象形文字にさかのぼる。以来幾多の暗号方式が用いられてきたが，大別して２方式に要約される。１つは，文字又は語句を他の文字又は記号に置き換える換字法であり，もう１つは平文をブロック化し，その中の文字の配列をお互いに置き換える転置法である。これら２方式を組み合わせたものを混合形式と呼んでおり，後述するＤＥＳは代表的な混合形成の暗号である。図３－30には代表的な換字式の例としてシーザー暗号を，図３－31には６文字単位に入れかえる転置式暗号の例を示す。

普通文字	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	·····
暗号文字	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	·····

平　文：JIPDEC
暗号文：MLSGHF
鍵　：3

図3－30　換字式暗号の例（シーザー暗号）

平　文	J	I	P	D	E	C
転　字	↓	↓	↓	↓	↓	↓
暗号文	P	E	J	C	I	D
鍵	3	5	1	6	2	4

図3－31　転置式暗号の例

このような暗号を用いた実際の例としては，第2次大戦中のドイツのエニグマ暗号や日本の97式暗号（紫暗号）があり，各々取扱不注意のためイギリスとアメリカに解読された。以上の暗号は短かい鍵を考えたものであるが，バーナム暗号のように，通信文と同じ長さの鍵をもつ暗号方式もあり，事実上，解読は不可能な暗号方式もある。現在，ワシントン・モスクワ間のホット・ラインにおいてこの方式が使われていると言うことである。

以上，古典的な暗号方式を概観したが，1970年後半に公開鍵暗号系が提案され，新しい暗号の幕明けとなる。

3.4.2.3　暗号方式の現状

(1)　暗　号　系

現在，暗号系には大別して慣用暗号系と公開鍵暗号系がある。1976年に，今までの概念とは異った公開鍵暗号系が発表されて以来，従来から広く用いられている暗号系は，慣用暗号系と呼ばれている。

① 慣用暗号系

慣用暗号系は図3－32で示すように，平文を暗号化鍵Kで暗号化を行い，復号化も同じ鍵Kを用いて行われる暗号系である。このため，秘密通信を行う相手と共通の鍵を保有する必要があり，鍵も秘密に安全な経路を通して送られなくてはならない。このように慣用暗号系では，秘密通信を行う相手との共通鍵を，すべて秘密に管理しなくてはいけないため，鍵の管理が問題となる。

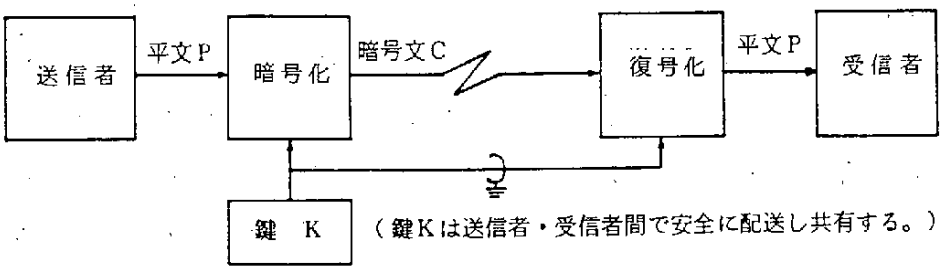


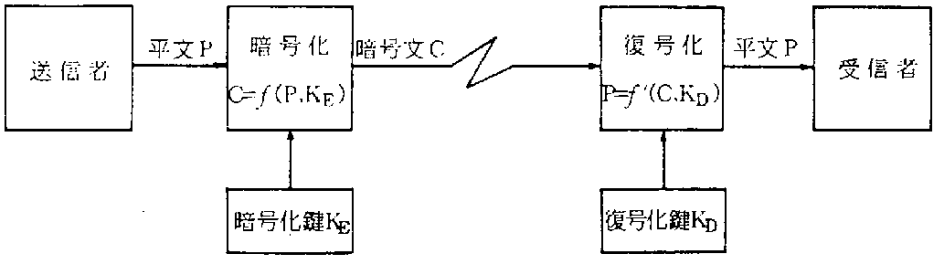
図3－32 慣用暗号系

② 公開鍵暗号系

1976年に発表された新しい暗号文である。図3－33で示すように，暗号化鍵と復号化鍵が異なることを特徴としており，暗号化鍵を公開し，復号化鍵のみ秘密にしておく方式である。このため鍵の配送を秘密にする必要はなくなり，鍵の管理も簡単化される。しかしながら，公開鍵だからと言って，相手を充分に確認することなしに暗号化鍵を送ることは非常に危険であり，公開系はだれの公開された暗号化鍵なのかがはっきりして初めて有効となるものである。

(2) 暗号アルゴリズム

暗号のアルゴリズムは数多く存在し，すべてを紹介することは困難なことから，慣用暗号系の中で米国標準方式となっているDES（Data Encryption Standard）と，最も有力な公開鍵暗号系とされているRSA（作成者Rivest，Shamir，Adlemanの頭文字）を以下にとりあげる。



（鍵K_E, K_Dは受信者が作成し，K_Eは一般に公開するがK_Dは秘密に保管する。）

図3－33　公開鍵暗号系

① DES方式

DES方式は，64ビットのデータ・ブロックを64ビット（このうち8ビットはパリティ）の鍵で暗号化し，同じ鍵で復号化する混合形式慣用暗号系である。図3－34を用いてアルゴリズムの概要を示す。基本的には，換字と転置を組み合せて，16段の反復動作を行っているにすぎない。図中のLn（ブロック左32ビット）とRn（右32ビット）の関係は以下の通りである。

$$L_n = R_{n-1}$$

$$R_n = L_{n-1} \oplus f(R_{n-1}, K_n)$$

ここで示された$f(R_{n-1}, K_n)$は，DESの強さの核となるものであり，逆変換が不可能なS－boxという換字表を用いている。この関数を図3－35に示す。

② RSA方式

公開鍵暗号系の実用例として，1977年にリベスト，シャミール，アドルマンにより発表された一方向性関数として，大きな素数の積の素因数分解を用いている。アルゴリズムは以下に示す通り単純である。

暗号化　$C \equiv M^e \pmod{n}$

復号化　$M \equiv C^d \pmod{n}$

（M：平文，C：暗号文，(e, n)：公開鍵，d：秘密鍵，
$n = p \cdot q$，p：素数，q：素数）

ここで，dは$(p-1)\cdot(q-1)$と互いに素な任意の整数を選び，eは，

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

を満たすように定める。

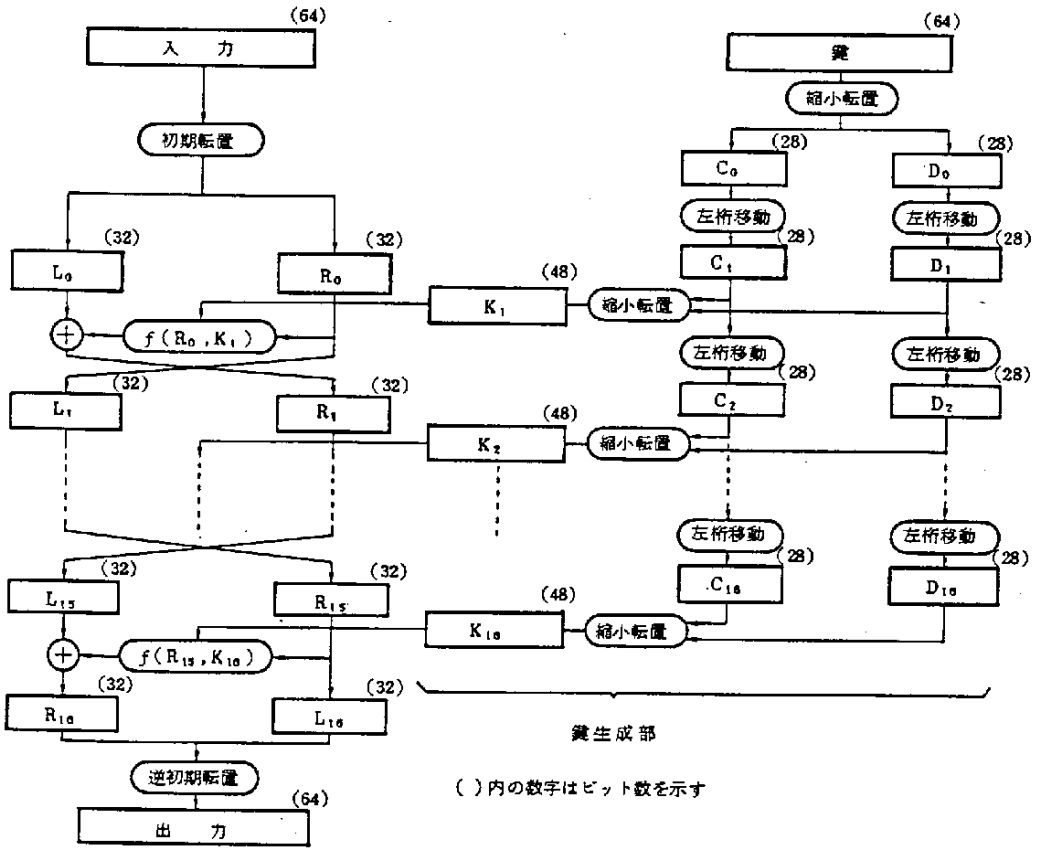


図３－34　ＤＥＳアルゴリズム

（昭和57年度コンピュータ・システムのセキュリティに関する調査研究報告書より）

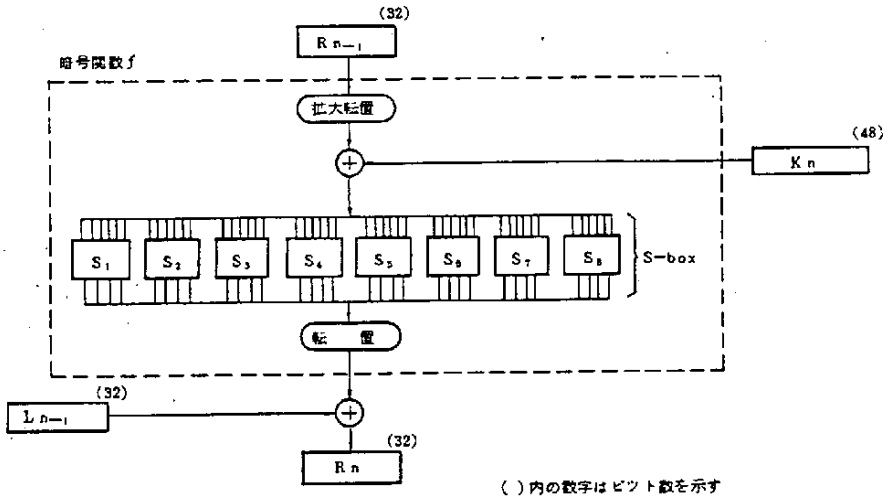


図３－35　DESの関数f（Rn_{-1}, Kn）

（昭和57年度コンピュータ・システムのセキュリティに関する調査研究報告書より）

(3)　暗号方式の適用法

以上の暗号方式も実際にいろいろな適用法が存在し，実用化されている。以下にDES方式とRSA方式の適用法を述べる。

①　DES方式の適用法

DESは，生まれもった安全性と，LSI技術の進歩により高速化という利点をもっているため，いろいろな適用法／利用法が考えられている。単純に転送データの保護として用いる場合も，ECB，CFB，CBCとOFBの４つの適用モードが考えられており，DESをより強くする方式が実用化されている。以上４モードを図３－36に示す。一方，DESはメッセージ認証用のチェック・サムやテキスト・キーの作成やデジタル署名におけるダイジェスティブ・メッセージの作成などにも用いられており，大量メッセージの圧縮をDESを用いて行うことで認証や署名に役立っている。

②　RSA方式の適用法

公開鍵暗号系であるRSA方式は，鍵の配送，管理においてすぐれているため，ただ単に転送データやファイル・データの保護に用いられるだけでなく，いろいろな適用法が考えられている。たとえば，郵政省（日本）の開発した

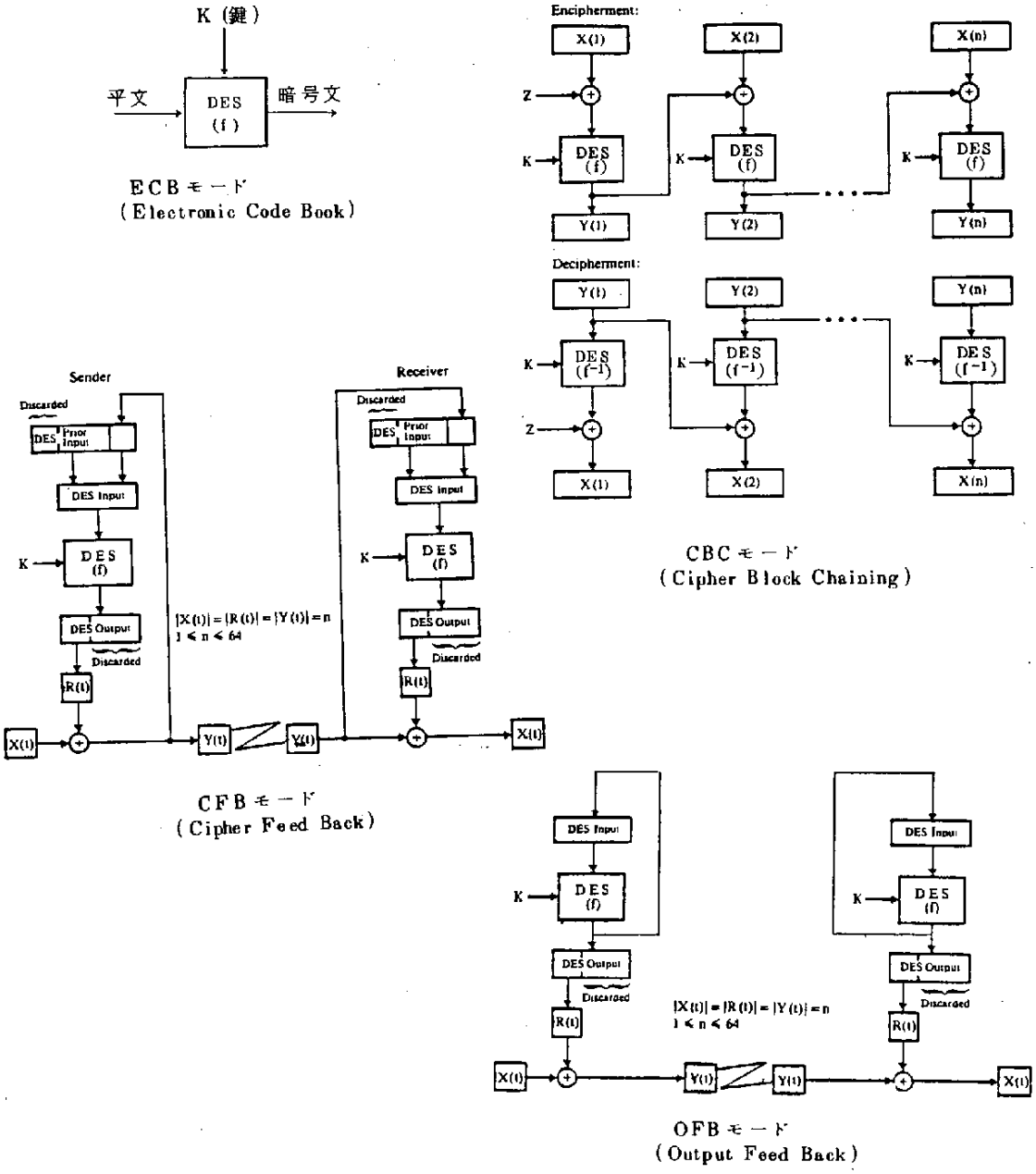


図 3 － 36　DES の利用モード

ミックス方式はRSA方式を用いて通信鍵（Communication Key）を送っており，DES 鍵の配送の問題点を解決している。また，郵便における署名の代りとなるデジタル署名もRSA 方式を用いて実現することができる（第3.4.3項参照）。さらに端末やホストにおける鍵の管理においても威力を発揮している。

(4) 暗号方式の安全性

① DES 方式の安全性

DES 方式の鍵は56ビットで構成されているため，2^{56}回の検査を行えば理論的には鍵を割り出すことができる。これは1つの鍵の検査に1 μs かかると仮定すると，約2,000年かかることになる。しかし，米のリベストは，10^6個のLSI を並列処理すれば，遅くても1日で求められることを指摘しており，鍵の長さを倍にすることを要求している。また，DES 方式には，S−box の設計そのものにも論議があり，DES の安全性を怪しむ向きもある。

しかしながら，DES は現在，国際標準化されようとしており，その安全性においては充分に検討されなくてはならない（ 3.4.5 の(1)参照 ）。

② RSA 方式の安全性

RSA 方式は，計算安全性からいくと，nを10進200桁とすれば，最も速い方法でも解読するのに3×10^9年以上かかるとされている。しかしながら，これは一方向性関数にささえられているものであり，一度素因数分解の有力な方法が見つかれば，RSA 方式の安全性はたちどころになくなる。

(5) 暗号用LSI と暗号装置

① 暗号用LSI

DES の暗号用LSI は各種販売されており，表3－3にそれらを示す。最も高速な処理が可能となるAMD 社のAm 9518は，14 Mbps の処理速度を持ち，先に示した各種の利用モード（ CFB, CBC etc）にも対応できるため，多様な適用が可能となる。

一方，RSA 法におけるLSI 化技術は，現在のところ，開発・研究段階にある。MIT のリベストは，512ビットのALUと40,000トランジスタ

表3－3　ＤＥＳの暗号用ＬＳＩ

ＬＳＩ名	メ　ー　カ　名	処理速度 (Kb/s)	暗号モード	ピ　ン　数
i８２９４	インテル	0.64	ＥＣＢ	４０
ＷＤ２００１	ウエスタンディジタル	1300	ＥＣＢ	２８
ＷＤ２００２	〃	〃	〃	４０
ＭＣ６８５９	モトローラ	400	—	２４
9414－1～4	フェアチャイルド	—	—	４０×４
Ａｍ　9518	ＡＭＤ	14000	ＥＣＢ ＣＦＢ ＣＢＣ	４０
ＡｍＺ 8068	〃	8000	〃	４０
ＴＭＳ99541	ＴＩ	5.12 0.64	ＥＣＢ ＣＦＢ	４０

ＥＣＢ：電子コードブック　（Electronic Codebook）
ＣＦＢ：暗号フィードバック　（Cipher Feedback）
ＣＢＣ：暗号ブロック・チェイニング　（Cipher Block Chaining）
（昭和57年度コンピュータ・システムのセキュリティに関する調査研究報告書より）

とＰＬＵ（プログラマブル論理回路）による1,200 bpsのＬＳＩを試作した。また，電電公社は35キロゲートの４チップ構成による50 kbpsのＬＳＩを検討中である。

② 暗号装置

暗号装置には，ＤＥＳ方式のものと非ＤＥＳ方式のものが市販されており，表３－４に示す通りである。非ＤＥＳ方式としては，バーナム暗号を用いたものが多く，米datotek社，日本電気などで製品化されている。また，通常の電文はＤＥＳを用いて送り，ＤＥＳの鍵のみ他の暗号方式を用いる方法も装置化されつつあり，その例としてＰＫＤＳ（公開鍵配送法，3.4.2.4(3)参照）を用いた富士通のＦ2151Ａがある。

表3－4　暗　号　装　置

	装置名	メーカ（国籍）	仕様		
			基本アルゴリズム	鍵総数（鍵の長さ）	伝送速度
DES方式	IBM3845	IBM（米）	DES	7×10^{16}（56ビット）	0.3~19.2Kbps
	Datacryptor II	Racal-Milgo（米）	DES＋RSA（option）	〃	0.3~9.6Kbps
	LC76DES	LINKABIT（米）	〃	〃	1.2Kbps~6.5Mbps
	F2151A	富士通（日）	DES＋PKDS	〃	0.3~19.2Kbps
非DES方式	HC-550	CRYPTO AG（スイス）	3段フォワードシフトレジスタ	10^{28}（英字20文字）	100bps（max）
	DS-138	datotek（米）	非線形多重レジスタ疑似ランダム発生器使用、bit by bit方式	10^{52}	19.2Kbps（max）
		日本電気（日）	非線形フィードバックレジスタ	7×10^{16}	2Mbps（max）

（ＣＩＳ研究会　PKDアルゴリズムを用いた商用暗号装置　富士通研究所より）

3.4.2.4　暗号方式の導入形態

前に述べた暗号方式をいかに用いて機密通信を行うかは，暗号アルゴリズムと同様に大切な検討事項である。以下に暗号方式を導入するにあたり必要となる項目を示す。

①　ネットワークへの導入法

②　暗号化／復号化鍵の管理

③　暗号化鍵の配送

これらに基づいて，暗号方式の導入形態を論じることとする。

(1)　暗号方式のネットワークへの導入

一般的に，リンクーリンク方式，ノードーノード方式とエンドーエンド方式の３方式が存在する。

① リンクーリンク方式

リンクーリンク方式は，DTEとDCEの間に暗号装置が置かれるものである。交換に用いるヘッダ部もすべて暗号化する方式であって，トラフィック解析に強いと言われる反面，鍵を各ノード毎に持たなくてはならず，鍵管理の面で多少問題のある方式である。図3－37に概念図を示す。

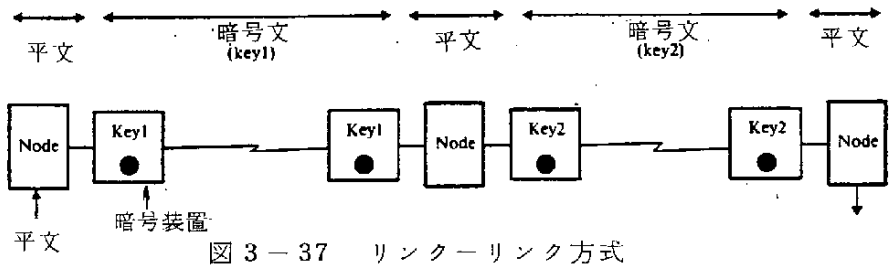


図3－37　リンクーリンク方式

② ノードーノード方式

ノードーノード方式は，交換に用いるヘッダ部には暗号をかけず，ノードにおいて暗号方式の変換を行う方式であり，ノード内の方式変換部の信頼性に強く依存するものである。図3－38に概念図を示す。

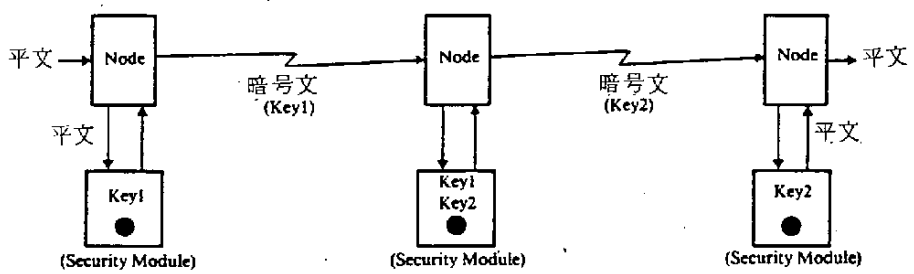


図3－38　ノードーノード方式

③ エンドーエンド方式

エンドーエンド方式は，交換のためのヘッダ部には暗号をかけず，ネットワークより上のレベルにおいて，エンド・ユーザ同志で暗号をかける方式である。この方式は，交換ノードに全く依存しないため，エンド・ユーザ間で自由に暗号化／復号化ができ，適用領域も前述の2方式よりかなり広い。概念図

を図３－39に示す。

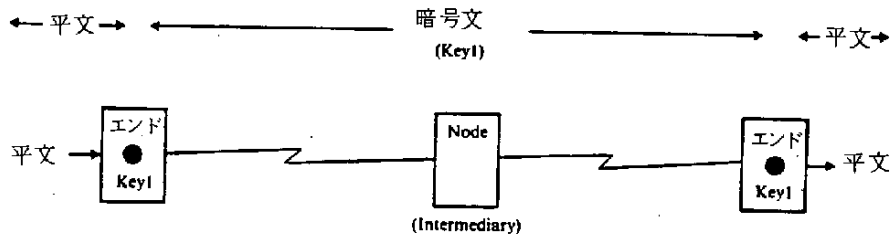


図３－39　エンドーエンド方式

(2)　暗号化／復号化鍵の管理

現代の暗号とは，保護したい大量のデータを，暗号化鍵１つで管理していると言っても過言ではない。このため，秘密とする鍵をいかに管理するかは，暗号方式の導入において重要なファクターとなる。鍵の管理は大別して鍵の生成・保管・更新といった３つのカテゴリーから成る。

①　鍵の生成

鍵の生成において重要なことは，ランダムな値を用い，できるだけ弱い鍵をさけることである。ＤＥＳにおいては，ＩＢＭ社より以下の鍵が弱いと提示されている。

０１０１０１０１０１０１０１
ＦＥＦＥＦＥＦＥＦＥＦＥＦＥ
１Ｆ１Ｆ１Ｆ１Ｆ０Ｅ０Ｅ０Ｅ０Ｅ
Ｅ０Ｅ０Ｅ０Ｅ０Ｆ１Ｆ１Ｆ１Ｆ１　　（16進表示）

一方ＲＳＡにおいては，大きな素数を生成することが必要となる。素数の判定法としてはフェルマー・テストがあるが，ミラーが1975年にその改良を行い，近年アドルマン，ポメランスらによりさらに改良が行われ，最近では，レンストラやコーエンにより，97桁の素数を77秒で判別できるところまできている。

② 鍵の保管

現在，鍵の保管方式として以下の3方式が提案されている。

ⓐ 個別鍵暗号化用マスタ鍵方式

この方式は，複数の個別鍵をマスタ鍵で暗号化して管理する方式であり，個別鍵とマスタ鍵の双方が存在しないと暗号化／復号化ができないものである。この方式は，IBM社やバラダイン社が採用しており，安全性の向上を求めた集中型管理方式である。

ⓑ 個別鍵代替用マスタ鍵方式

この方式は，個別鍵の紛失や破壊に備えて個別鍵の代りに用いるためのマスタ鍵方式である。現在，RSA法とR法のマスタ鍵の存在が明らかになっており，鍵管理の信頼性の向上をねらっている。

ⓒ 暗号化鍵分散共有方式

ある秘密の鍵から複数の分散鍵を生成し，機密通信を行う構成員に分配する。全構成員のうちある一定数の構成員がそろうと，各分配鍵を合成することにより，暗号化秘密鍵が生成できる。しかし，一定数の構成員が集まらないと，機密通信は成立しないという方式である。この方式の実現解として，シャミールは多項式の補間を用いる方式を提案している。

③ 鍵の更新

鍵の保管，生成が正しくとも，長期に渡って同じ鍵を用いることはさけるべきである。そこである周期をもって鍵を更新していく必要があり，その周期も暗号の強度に依存するものとなろう。

(3) 暗号化鍵の配送

従来の慣用暗号系においては，鍵は安全な通路を介して運ばれた。しかしながら，ネットワークの拡大に伴い，通信領域が広がり，1ユーザが複数ユーザと機密通信を行うようになると，安全な通路を用いた鍵の配送も重荷となり，最近ではデータを送る通信回線と同じ回線を用いて，鍵を配送する方法の検討がさかんである。

① 副暗号化鍵（Secondary Key）の導入

暗号を用いた機密通信を行う際，実際のデータを送るときの暗号化鍵を別の副暗号化鍵を用いて送る方法が考えられる。すなわち，図３－40に示すように，転送フェーズで用いる暗号化鍵Ｋを副暗号化鍵ＫＮを用いて，転送フェーズに入る前に送る方法である。この方式は，副暗号化鍵を双方で共通にもつ必要があり，この点では慣用系の鍵配送と同じであるが，実際に保護したいデータの暗号化鍵を，転送のたびに変更することができるため，安全性が高まるという利点がある。

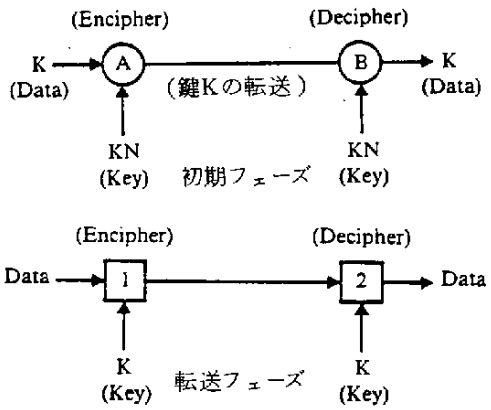


図３－40　副暗号化鍵を用いた通信

② 郵政省ミックス方式

郵政省で開発したミックス方式は，上述の副暗号系にＲＳＡ方式を用いており，ＲＳＡ方式でＤＥＳ方式の暗号化鍵を送っている。このため，副暗号化鍵の配送も容易になった。

③ 公開鍵配送法（ＰＫＤＳ）

ディフィとヘルマンにより考案された鍵配送法であり，離散対数問題の一方向性をうまく利用している。アルゴリズムを以下に示す。

αをある有限体の原始根とすると，

$$Y \equiv \alpha^{X} \ (\mathrm{mod}\ n) \quad (1 \leqq X \leqq n-1,\ n：素数)$$

と表現することができる。各ユーザはXを任意に選び秘密とし，Yを求めて公開する。ここで，Yが与えられても，Xを割り出すことはむずかしい。図3－41に示すようにPKDS方式は鍵を交換し，合成してDESの鍵を得る方式である。

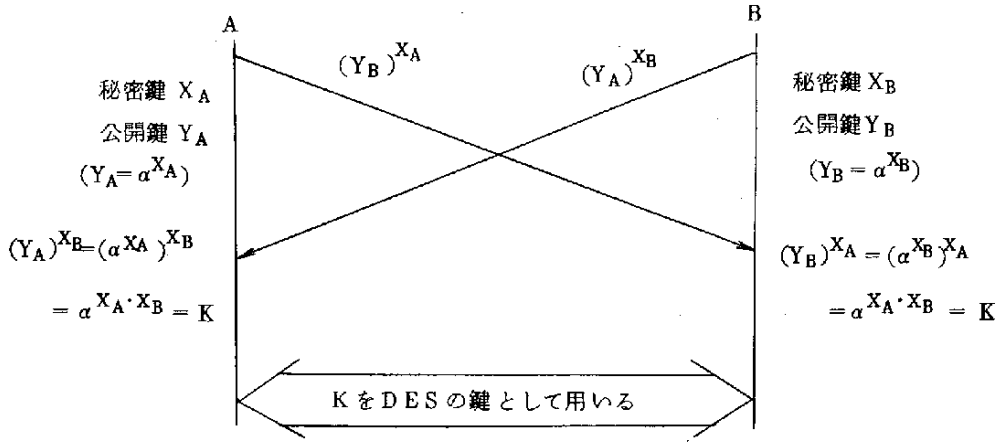


図3－41　PKDS方式

④　KDC（鍵配送センタ）を用いた方式

エンド・ユーザがすべての鍵を管理する負担を軽減するため，鍵の管理と配送を行うための信頼度の高いセンタが考えられている。ニードハムらの提案している方式は，実際の通信を行うための暗号化鍵をセンタ側で生成し，分配するもので，各ユーザは自分の暗号化／復号化鍵のみを管理すればよい。このように，集中的に各ユーザの鍵を管理することは，たとえ公開鍵暗号系においても必要となり，鍵配送センタを構築することは今後の大きな課題の1つとなろう。

【参考文献】

1)　R. L. Rivest, A. Shamir, and L. Adleman :「A Method for Obtaining Digital Signatures and Public-Key Cryptosystems」, Communication of ACM, 1978, Vol.21, №2.

2)　R. M. Needham and M. D. Schroeder :「Using Encryption for Authe-

ntication in Large Networks of Computers」,
Communication of ACM, 1978, Vol.21, №12.

3) G.J. Popek and C. S. Kline : 「Encryption and Secure Computer Networks」, ACM Computing Serveys, Vol.11, №4.

4) D. E. Denning and G.M. Sacco : 「Timestamps in Key Distribution Protocols」, Communication of the ACM 1978, Vol. 21, №12.

5) W.Diffie and M.Hellman : 「New Directions in Cryptography」, IEEE Transactions on Information Theory, IT−22, (November 1976).

6) IBM 3845 Data Encryption Device IBM 3846 Data Encryption Device General Information, GA27−2865−3, International Business Machines Corporation, 1979.

7) R.L.Rivest, "A Description of a Single−Chip Implementation of the RSA Public−Key Crypto−system," Record of National Telecommunications Conference, pp 49.2.1−49.2.5, Dec. 1980.

8) 田中,「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』, 1978年9月4日号, №194, pp.68−103.

9) 嵩, 山村,「暗号化法の最近の話題」,『電子通信学会誌』, Vol.63, №5, pp.460−467, 1980年5月.

10) 秋山,「PKDアルゴリズムを使った商用暗号装置」, 第1回, CIS研究会.

3.4.3 メッセージ認証

メッセージ認証とは, 通信回線から送られて来たメッセージが確かに送信者から送られたものであり, そのメッセージが正当なものであることを検証することである。今後, 回線開放に伴いEFTS(Electronic Funds Transfer System)による電子送金, 電子化取引, 電子郵便等の発達により, 利害関係のあるデータの通信が増して来る。こういった状況のもとでメッセージ認証は重要なものとなってきている。

(1) 標準認証方式

米国ではANSI（米国規格協会），ISO（国際標準化機構）で認証の標準化が行なわれており，一部の銀行では導入が開始されたという。この方式はDESの暗号方式を利用することにより，メッセージの正当性を検証している。標準認証方式の原理を図3－42に示し，以下にそれを説明する。

送信側は認証の対象となるメッセージからテキスト・キーを作成する。ここで認証の対象となるメッセージ部には，日付と識別名を含めなければならない。そこで送信側はメッセージとテキスト・キーを合わせて送り出す。受信側は受信メッセージから同様の方法でテキスト・キーを作成し受信テキスト・キーと照合する。その結果が一致したならば，受信メッセージは送信者が送ったものに相違ないと認証できる。メッセージが途中で改ざんされた場合には，テキスト・キーを照合したときに，それが一致しないので，それを見つけ出すことができる。テキスト・キーの作成方法を図3－43に示す。テキスト・キーの作成は，次に示すようなDESによるデータ圧縮型暗号処理を行うことにより得られる。認証の対象となるメッセージのブロックI_1，I_2，……，I_nを，認証鍵Ktで順次暗号化し暗号ブロックO_1，O_2，……，O_nを得る。最後に得られたブロックO_nの64ビットの上位32ビットを，テキスト・キーとする。

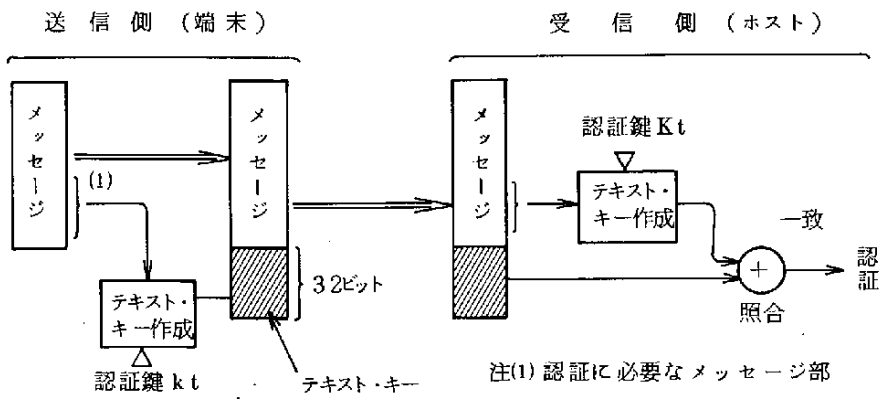


図3－42　標準認証方式

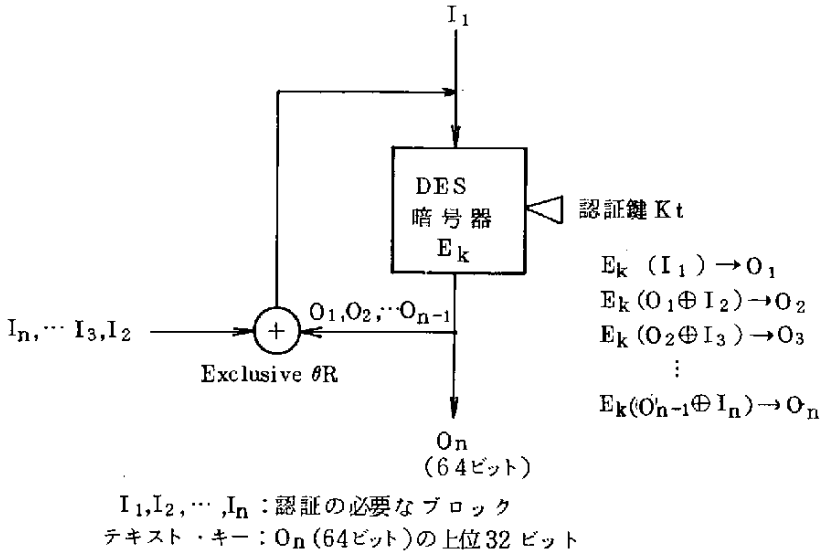


図 3 － 43　テキスト・キーの作成方法

この方式では，メッセージは暗号化せず，生データを送ることになっているため，盗聴される危険がある。また，鍵の配送ができず，鍵が漏れた場合認証の意味がなくなるため，鍵は厳重に管理しなければならない。

(2)　デジタル署名

現在の社会では，契約交渉はサイン，印鑑によりその正統性を認証している。利害関係のあるデータが電子化取引のように通信でやりとりされる場合，サイン，印鑑データをそのままデジタル信号に変換して送っても，簡単にコピーされる恐れがあり認証には使用できない。ここで，通常のサイン，印鑑に相当するデジタル署名が必要になる。ここでメッセージ認証が署名として有効になるためには，次の３つの条件を満足しなければならない。

ⓐ　送信者だけしか署名文を作成できない。第三者によって偽造できない。

ⓑ　受信者が署名文を改ざんすることができない。

ⓒ　送信者が後で送信の事実を否定できない。

デジタル署名を実現する手段として次のような方法が提案されている。

- 慣用暗号を用いたデジタル署名
- 公開鍵暗号を用いたデジタル署名

・　ハイブリッド方式によるデジタル署名

① 慣用暗号を用いたデジタル署名

一般にDES方式の暗号を用いたデジタル署名がいろいろ提案されているが，公証機関が必要であったり，送信側と受信側で共通の認証鍵を持つため受信者が署名文を改ざんすることができるという問題がある。このため実用性のある署名方式はまだない。

② 公開鍵暗号を用いたデジタル署名

RSAの暗号方式を用いることにより比較的容易にデジタル署名が実現できる。

図3－44に公開鍵暗号によるデジタル署名を示す。送信者Aは，メッセージMをAの秘密の復号鍵 D_A で復号し，これを相手の公開鍵 E_B で暗号化し暗号文 $C = E_B\{D_A(M)\}$ を得る。これをBに送信する。Bは受信データCを自分の秘密鍵 D_B で復号化して $D_A(M)$ を得る。これをAの公開鍵 E_A で暗号化すればもとのメッセージMを求めることができる。

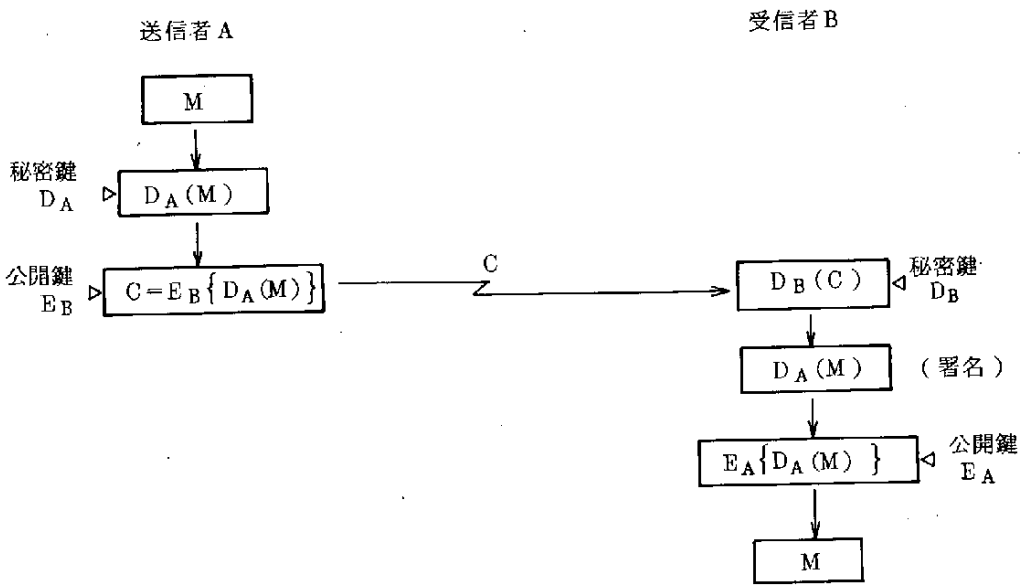


図3－44　公開鍵暗号によるデジタル署名

ここで，暗号文Cは秘密鍵 D_B を知らないと解読できない。即ち，D_B を知っているのはBだけである。また $D_A(M)$ を作れるのは秘密鍵 D_A を知っているAだけである。従って，メッセージMを送信したのは確かにAであり，メッセージMを受け取ったのは確かにBであるということになる。

さらにメッセージMが，通常の文章でなくランダムなデータであったりした時には，Mが正当なものかどうか判定しにくい。この対策としてメッセージに送信者の識別名，受信者の識別名，メッセージの通し番号，日付等の付属情報を付けて送信するとよい。これにより，署名文をコピーして何度も送るような不正行為を防止することもできる。

しかし，RSAによる方式では，演算が複雑になるため暗号化，復号化に時間がかかり，メッセージが長い場合には問題になる。

③ ハイブリッド方式によるデジタル署名

この方式は，DESの暗号方式の利点とRSAの暗号方式の利点をうまく利用しそれぞれの方式をミックスさせたものである。

通常のメッセージはDESによる暗号通信で送信し，鍵の配送と認証はRSAの方式を使っている。認証の対象となるメッセージは，先ず標準認証方式と同じようにDESによるデータ圧縮型暗号処理を行いチェック・サムを求める。図3－45にこの方法を示す。最後に得られた64ビットの暗号ブ

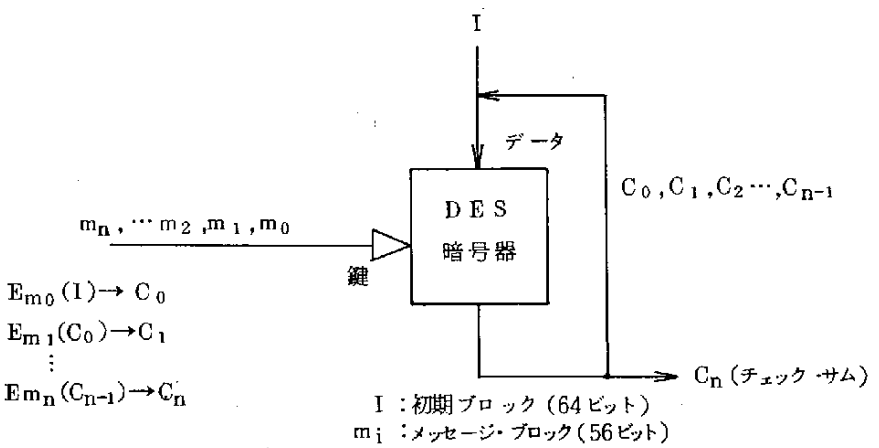


図3－45　チェック・サムの求め方

ロック（チェック・サム）にタイム・スタンプを付加したデータだけに，RSA方式によるデジタル署名を行う。

この方式では長いメッセージに対するデジタル署名でも短時間で処理できる。

以上述べてきた方式は，デジタル署名の条件である©，「送信者が後で送信の事実を否定できない。」を満足していない。慣用暗号，公開鍵暗号のいずれの方式でも同様に，送信者が送信した正当なデータであっても，送信者が偽って秘密鍵が盗まれ，誰かがかってにデータを作成したと主張した場合，事実の究明は難しい。また，実際に秘密鍵が盗まれていたとしたら，それまでに署名したメッセージはすべて信用のおけないものになってしまう。

デジタル署名において秘密鍵は，絶対に保護されていなければならない。さらに秘密鍵が漏れたり，忘れたりした場合に鍵を変更する方法，慣用暗号での鍵の配送の問題等，暗号方式で問題になっていることがデジタル署名においても同様に発生する。

(3) 公証機関を介したデジタル署名

(2)項で述べたように送信者と受信者の二人だけで署名を行う限り，条件©の問題は解決できない。ここで信頼できる公証機関を介して通信を行い，条件©を満足するような方式も提案されている（図3－46参照）。

公証機関は，受信した署名にタイム・スタンプを押して受信者宛に送り出し，これを記録しておく。送信者が，自分のメッセージを否認しようとしても，今度は公証機関に記録が残っているので，そう簡単には否認できない。ところが，またしても送信者は秘密鍵が盗まれていて，誰かが偽造したものだと主張できそうである。これに対しては，送信者にメッセージを返送して確認を取ることによりこれを防ぐことができる。

ここで公証機関は具体的に誰がやるのか，記録を保存するメッセージの量は多くなりすぎないかといった問題がある。

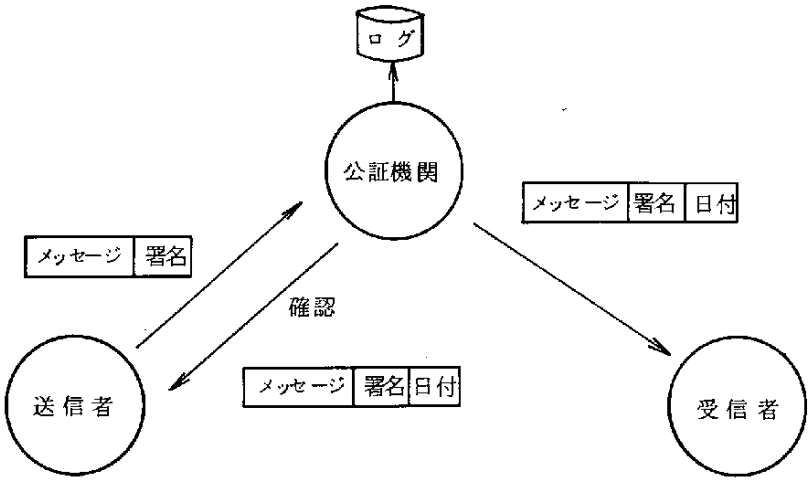


図3－46　公証機関を介したデジタル署名

デジタル署名によってメッセージが認証されたとしても，端末を使用している人が確かに本人であるということが認証された訳ではない。送信者が他人ではないかという疑いを晴らすには，パスワードといった簡単なものでなく強力な本人確認，例えば声紋・指紋の照合を行う必要もある。

国内では電子化取引等は，まだ本格的に行なわれていないが，回線開放に伴って活発に行なわれるようになるであろう。安全で高速処理可能な認証アルゴリズム等を，そのときに備えて，さらに検討していかなければならない。

3.4.4　端末確認

現在バンキング・システム，医療システムといったさまざまなコンピュータ・システムが存在し，それぞれのシステムに端末が接続されている。これらのシステムで，不正な端末からアクセスがないか端末確認をすることは，セキュリティ上大切なことである。そしてこれからは，回線開放の進展に伴ないコンピュータ・システムが広域化，複雑化するであろう。その場合，ある端末からさまざまなコンピュータ・システムへのアクセスの可能性が増大し，不正アクセスの検出が困難になってくる。こうした状況の中で，不正端末からの不正アクセス，改ざん，破壊等さまざまな脅威が生まれてくる。

一方，パソコン，ポータブル端末等各種端末の普及は著しく，各端末はインテリジェント化し，その機能も高くなっている。この機能を有効に利用すれば，容易に不正を行うことができそうである。このような端末が普及し，ホーム・バンキング／ホーム・ショッピング等が実現すれば，不正を行う者も多くなる可能性がある。米国ではこの種の犯罪も現実に発生し，社会的にも問題になっている。また，ポータブル端末のように遠隔地で使用するようなものは，特に端末の確認，管理は重要なものとなる。

以上のことから端末確認は，セキュリティ上重要な項目の一つであることがわかる。次に端末確認技術について説明する。

(1) 端末，センタ側で必要とされる技術

① コールバックの利用

これは端末からセンタを呼び出すと，センタは端末が実際に使用されている回線で，ユーザ権限が与えられているものか確認して，一度回線を切り，あらためて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。これにより異った回線からの不正アクセスだけでなく，端末ユーザの確認まで行うことができる。

② リミット・チェック

通常起こり得ない状況をチェックする。例えばメッセージの発信時間を決めて，定時外のアクセスを禁止する。夜中に不正な操作が行われたとしてもそれを防ぐことができる。またそのログを取っておくことも重要である。あるいは，1日のメッセージ件数に制限を設けておくことも有効となる。1日の通常取引きが数件しかないものが，ある日は1万件も発生したとすれば，何らかの不正が行なわれている可能性がある。また，パスワード，IDコードの誤り回数をチェックすることにより同様の効果が得られる。このようなリミット・チェックは，一般に権限が与えられた正しい端末を不正に操作した場合に有効であるが，不正端末からのアクセスに対しても効果があるであろう。

③ IDの自動発生

ログオン時ハードウェアにより端末自体からIDコードを自動的に発生さ

せ，このコードにより端末確認を行う必要がある。ＩＤコードの作成法としては，過去にアクセスしたデータをパラメータにしたＩＤコードが発生出来れば，端末確認はより確実なものとなるであろう。ここで，ログオン後も定期的にＩＤコードを確認するようにすれば，さらに有効である。

④　暗　号

端末に暗号機能を持たせることにより端末を確認することも可能である。これで一般の暗号機能のない端末からの不正アクセスはできなくなる。また端末ごとに特定の秘密鍵をハード的に割当てておけば，その秘密鍵で送信して来る端末は，その端末しかないということになる。暗号を使用することにより通信回線からの盗聴といったことにも効果がある。

⑤　メッセージ認識番号，その他

不正端末からの侵入を防ぐために，端末からのメッセージに連続認識番号を入れておくことも有効である。また，回線を二重化して回線を交互に利用することにより，不正端末からの侵入をやりにくくすることも可能である。端末接続ログを取ることも重要なことである。センタ側で接続ログを取ることにより，不正端末からのアクセスがあったかどうか確認できる。さらに証拠が残るということで，不正端末からのアクセスの抑止につながるであろう。

(2)　ネットワーク側で必要とされる技術

①　閉域接続，相手通知

ＴＳＳ等，一般公衆回線からアクセス可能なコンピュータ・システムでは，どの回線からもアクセスできるため，不正端末からのアクセスが容易である。ここで，接続回線を指定でき，権限のない回線からのアクセスを排除できれば，不正端末からのアクセスを減少できる。ＤＤＸ等のデータ網では，付加サービスとして閉域接続，相手通知機能がある。今後，回線の開放の進展と共に，この機能の積極的利用が望まれる。

②　ロ　グ

端末の使用状況をネットワーク側でもログしておけばセンタ側のログと合わせ，不正使用の強力な抑止力となる。有料でも，このようなサービスがネ

ットワーク側にあることが望ましい。

以上述べたことは従来行われていることであり，従来技術で可能なものである。個々の技術を見ればそれ程難しい技術ではないが，これらの技術を組み合わせることで，端末確認をかなり強力に行うことができるであろう。次に本人確認技術について述べる。これは直接端末を確認する訳ではなく端末を操作している人が，確かに本人であることを確認する技術であるが，その人を通して間接的に端末を確認していることにもなる。ＩＤカード，ＩＣカード，パスワード等が現在使用されている。これらは盗まれる恐れがあり完全とはいえない。現在サイン，指紋，声紋，手形，印鑑等を照合することにより本人確認を行う技術に期待がよせられている。

今後期待された端末確認技術としては，低コストでどんな端末にも接続可能なセキュリティＬＳＩのようなものがあげられる。そのＬＳＩは，例えば暗号機能，端末確認機能を持ち，端末ごとに個有になるように，一部ＲＯＭあるいはＰＬＡのようなものとし，ネットワークに接続する端末にこのＬＳＩを付加してネットワーク全体のセキュリティを高めることを可能にする。

今後，高度なセキュリティ機能を持ったものから低レベルのものまで，さまざまな端末が普及するであろう。これらセキュリティ・レベルの異る端末がネットワークに接続されて行くとき，セキュリティ対策はより困難なものになってくるであろう。このような状況のもとでは，各レベルの端末に対するアクセスの範囲を，きめ細かに管理してやる必要がある。そのためにも，端末確認技術はセキュリティ上重要な技術の１つとなってくる。

端末をネットワークに接続するとき，端末にはある程度のレベル以上のセキュリティ機能を持たせる必要がある。そのためにはその機能は低コストで実現できなければならず，その標準化についても考えなければならない。また，高レベルのセキュリティを要求するものに対しては有料でサービスするようなものもあってよい。

端末が確認され，いくら正しい端末からアクセスしていることが分っても，正し

く本人が操作しているのでなければ意味がない。端末確認技術だけでなく，本人確認技術，アクセス・コントロール等の技術を複合化することにより，さらにセキュリティ上強いものとすることができる。また，社会的にも，不当な端末がネットワークに接続できないように，端末の登録制度，免許制度を設けることも必要ではないか。

3.4.5 セキュリティ対策の標準化動向（その１）

現在，セキュリティ対策の標準化作業はISOとCCITTにおいて主に行われている。標準化は次のような観点から各々独立に進められている。

① 暗号方式や鍵配送プロトコルを標準化することにより，公衆網における広域的な機密通信を実現できる。

② また標準化に基づき，暗号装置（ＬＳＩ）の量産が行われ，コストの軽減が図れる。

以下にISOとCCITTにおける標準化動向を示す。

(1) ISOにおける標準化動向

ＩＳＯでは，大別して暗号方式の標準化とOSI（Open Systems Interconnection）モデルにおけるセキュリティ・アーキテクチャの検討が進められており，前者はTC 97／SC 20，後者はTC 97／SC 16/WG 1において各々研究されている。

① 暗号方式の標準化

暗号方式の標準化の対象には，暗号アルゴリズムと暗号の利用法がある。暗号アルゴリズムは米国の暗号標準方式であるDESに基づいて作成され，DEA1（Data Encipherment Algorism 1）と名付けられた。ＤＥＡ１は，1982年にDP 8227として郵便投票にかけられ，現在特許権の扱い等が議論されている。ＤＥＡ１とＤＥＳの間には暗号鍵のパリティの規定において，若干の相異（ＤＥＡ１では，鍵にパリティの概念がない）がみられるだけで，暗号のアルゴリズムそのものは全く同じである。このため，ＤＥＡ１の暗号の強度については，米国以外で確認する必要があるとの議論もある。

一方，公開鍵暗号における標準化は時期尚早という見方がされており，技術参考資料をまとめる作業が進められている。そこではＲＳＡ法等を用いた応用技術，ＲＳＡ法における鍵の長さや素数の生成法などの議論がされている。

次に暗号の利用法であるが，ＩＳＯ標準案は以下に示す４つのモードを規定している。

ⓐ　ＥＣＢモード（Electronic Code Book）……ＤＥＡ１をそのまま利用するモードである。

ⓑ　ＣＢＣモード（Cipher Block Chaining）……第3.4.2項参照

ⓒ　ＣＦＢモード（Cipher Feedback）……図３－47に示す。

ⓓ　ＯＦＢモード（Output Feedback）……第3.4.2項参照

暗号の利用モードにおいてもＯＦＢモードが米国標準方式と異っている。

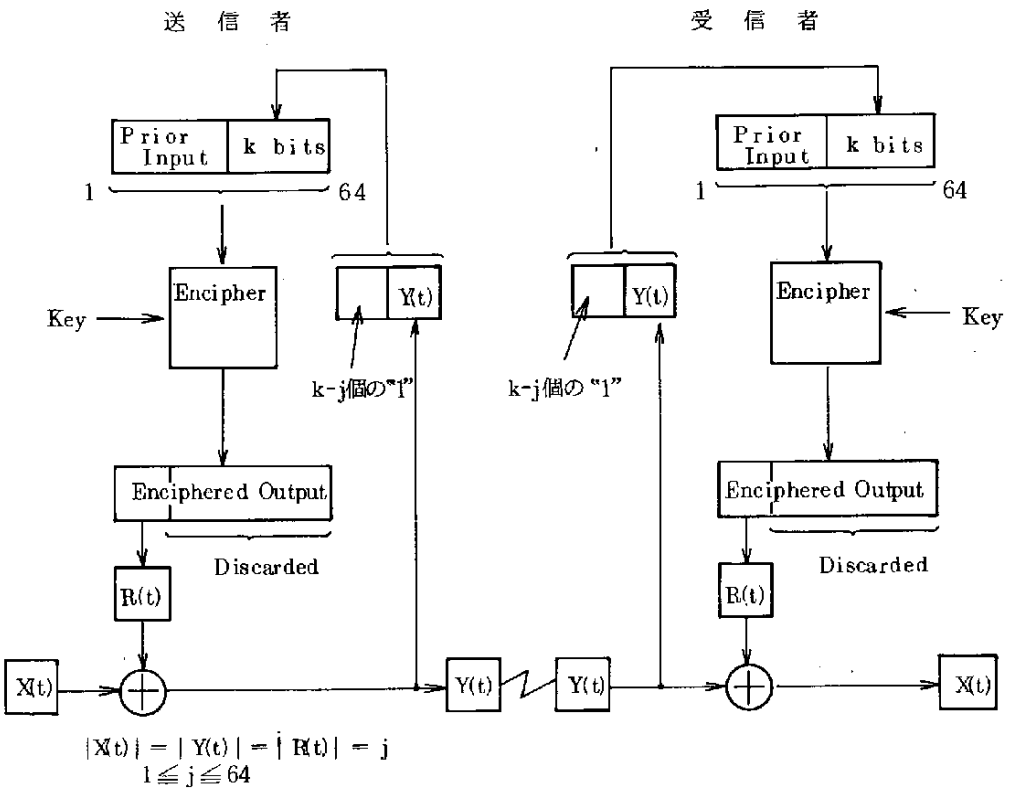


図３－47　ＣＦＢモード（ＩＳＯ案）

以上のように，暗号アルゴリズムや暗号の利用法について，ＩＳＯ案は，米国標準と合致していない点もあり，標準の統一性の観点から問題とされている。

② セキュリティ・アーキテクチャ

ＩＳＯでは，通信インタフェースの標準化において，ＯＳＩ参照モデルを作成し，各レイヤにおける詳細検討を進めている。この参照モデルの中にいかにセキュリティ構造を埋め込むかという研究も同時に行われており，以下に概要を示す。

ⓐ N－Cryptographic Connections

ＯＳＩ参照モデルの中で，対応する各レイヤのエンティティ同志が活性化するための接続を“connection”と呼ぶが，相互に対応するエンティティが正当な暗号化鍵を保有している場合，N－Cryptographic Connectionsを張ることができ，以下のサービスの提供を可能とする。

㋐ Data Privacy (N)－service （第３者の介入から保護）

㋑ Data Integrity (N)－service （データの完全性を保証する）

㋒ Authentication (N)－service

このようなN－Cryptographic Connectionsが，ＯＳＩ参照モデルのどのレイヤに適用できるかが次の問題となる。

ⓑ セキュリティ・サービスに適したレイヤ

現在主に，ＯＳＩ参照モデルの中のレイヤ１，２，４，６について議論されており，以下に各レイヤにおける適用性を述べる。

① 物理レイヤ／データ・リング・レイヤ

物理レイヤにおけるセキュリティ・サービスには２つの特徴がある。１つはすべてのデータが暗号化される点であり，もう１つは暗号装置がＤＴＥとＤＣＥの間に入るため，ＤＴＥにとってトランスペアレントな転送が実現できる点である。

データ・リンク・レイヤにおける暗号化範囲は以下に示す２つが提案されている。

㋐　リンク・レイヤのプロトコル・ヘッダ以外はすべて暗号化する。

㋑　リンク・レベルのヘッダ付加情報（Manipulation Detection Code ＋ Time Stamp）以外を暗号化する。

この付加情報が暗号化されていると，回線盗聴，データの改ざんや，以前の正当なデータの再使用などを検出することができる。図3－48に㋐と㋑の暗号化範囲を示す。

以上のレイヤ1，2におけるセキュリティ・サービスは，トラフィック解析を防ぐためには有力となるが，実質的にレイヤ1，2の暗号はリンクに依存し，エンドーエンドの暗号でないため，暗号のネゴシエイションを実際にどのようにするかという問題点も残されている。

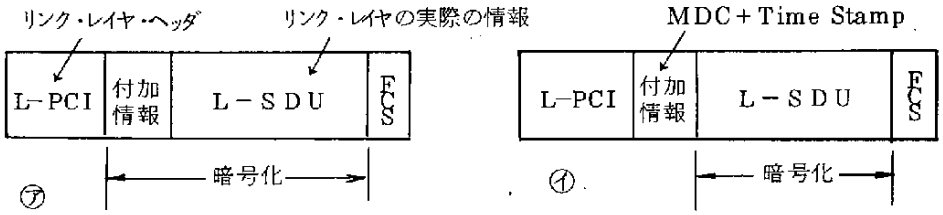


図3－48　データ・リンク・レイヤの暗号化範囲

㋒　トランスポート・レイヤ

このレイヤにおける暗号は，エンドーエンドで完全に実行できるところが利点である。また，セッション設定やプリゼンテーション環境設定時に流れるユーザ識別のためのパスワードをエンドーエンドで保護する場合は，このレイヤで暗号をかけることが有効となろう。

㋓　プレゼンテーション・レイヤ

一番有力なレイヤがプレゼンテーションである。理由としては，

㋑　暗号は本質的にエンドーエンドである。

㋺　平文の処理のあるレイヤを信頼性の観点からできるだけ少なくするため，暗号はできるだけ高位レイヤでかける必要がある。

㋩　プレゼンテーション・サービスを用いるのなら，暗号はアプリケーション・レイヤより下で実行すべきである。

㈢ データの一部分に暗号をかけたいという要求には，プレゼンテーションより上位レイヤでないと対応できない。

などが存在する。

この他にＩＳＯでは，鍵管理の重要性も指摘しており，詳細は継続検討とされている。

(2) ＣＣＩＴＴにおける標準化動向

ＣＣＩＴＴでは，テルマティック・サービス（テレテックス，ファクシミリ，ビデオテックス等）におけるセキュリティの検討が始められたばかりであり，ほとんど，セキュリティにおいて実質的な審議がなされていないのが現状である。そこで，最も審議が進んでいるＳＧⅧ，ＷＰ４における，テレマティック・サービスのセキュリティの審議動向を紹介する。

① テレマティック・サービスにおけるセキュリティ

テレマティック・サービスは，将来のオフィス・ドキュメント通信の中核を担うものと予想されており，各国とも積極的な議論を内外で展開している。テレマティック・サービスは以下の特徴を有する。

- 重要なドキュメントを送受する可能性がある。
- 公衆網を用いてどこにでもアクセスできる。
- 転送するドキュメントの構造をも相手に伝えるため，受信側で受信ドキュメントの編集が可能となる。

以上の特徴を基に，ＳＧⅧ，ＷＰ４では以下の４項目の検討を行っている。

ⓐ 暗号化

ⓑ 暗号化鍵の管理とその配送

ⓒ 暗号のためのネゴシエイション

ⓓ ドキュメント・プロテクション

以下に個々の項目について示す。

ⓐ 暗号化

暗号化アルゴリズムについては，ＤＥＳとＲＳＡが候補にのぼっており，詳細の検討は行われていない。また暗号に適したレイヤとしては，プレゼ

ンテーション・レイヤを考えており，以下の理由が示されている。

- ネットワーク管理とセキュリティの責任は分担した方がよい。
- 暗号化は本質的にユーザにまかせるべきである。
- アプリケーションで暗号化を行うとアプリケーションの個々の実体に暗号が依存するため，標準化がしにくい。
- プリゼンテーション・レイヤの機能として，data syntax transformation 等があり，暗号化を施すにも適している。

結論としては，セッション・プロトコル（S. 62）におけるセッション・サービス・ユーザ・データ，すなわちプレゼンテーション・レイヤのプロトコル・データ・ユニットを暗号化することで合意された。

ⓑ 暗号化鍵の管理とその配送

公衆網を用いていろいろな相手と機密通信を行う形態を考えると，暗号化鍵をいかに管理し，配送するかは重要な問題となってくる。

そこで，Needham らが提案している Key Distibution Centre の考え方を基にして，図３－49に示すKDCを用いたプロトコルを，今後の検討

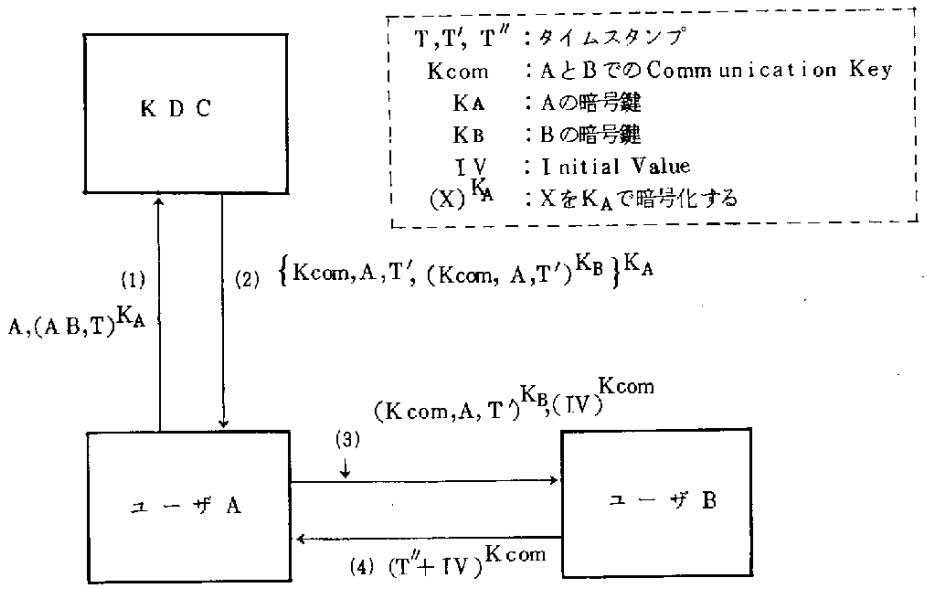


図３－49　Key Distribution Centre を用いた鍵配送プロトコル

のベースとしていくこととなった。また，ユーザAとBがお互いに同じ鍵を保有していた場合は，図3－50に示す手順が考えられている。

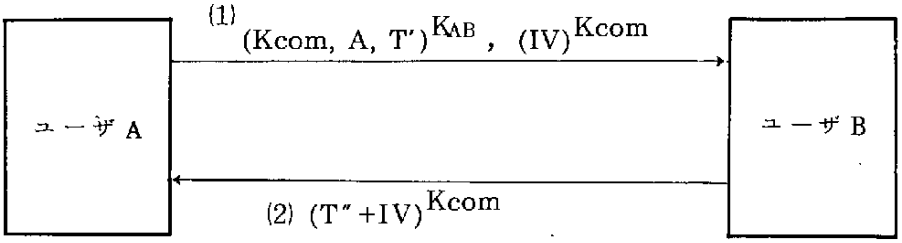


図3－50　Bilateral masterkey "K_{AB}"を用いた鍵配送プロトコル

以上の検討は進められているものの，KDCはどこが運用するのか，複数KDCが存在した場合のプロトコルと鍵更新メカニズムなどの問題点もあり，将来の検討が待たれるところである。

ⓒ 暗号のためのネゴシエイション

プレゼンテーション・レイヤで暗号をかけるため，セッション・レイヤで暗号方式と鍵配送方式のネゴシエイションが必要であり，詳細は継続検討とされている。

ⓓ ドキュメント・プロテクション

前述した通り，テレマティック・サービスでは，ドキュメントの内容と一緒に構造を送るため，受信側に編集の能力さえあれば，容易に受信したドキュメントの再編集が可能となる。このため重要文書に対して，編集のプロテクションが必要となる。現在，このドキュメント・プロテクションの方式として，RSAを用いる方向で議論が進んでいるが，全般的に将来の課題とされている。

以上，CCITT SGⅧ，WP4における標準化動向を概観した。来会期はテレマティック・サービスだけでなく，メッセージ・ハンドリング・システムや会議通信の分野においてもセキュリティ技術が検討されていくことになろう。

3.4.6　セキュリティ対策の標準化動向（その２）

金融業でのネットワーク網が拡大し，多様化する状況については，第3.2.2項で触れた通りである。この拡大・多様化するシステム展開と呼応し，システムのセキュリティ対策を万全に整えていくことが要請される。

この項では，金融業システムにおける，特に複数企業間結合システムの代表的なセキュリティ対策の具体例として，国内システムでは最近制定された「全銀協標準通信プロトコル」について，国際システムでは「SWIFTシステム」について述べる。特にSWIFTシステムは，既に日本がこのシステムに参加して，3年を経過しているが，世界的規模のネットワーク・システムとして軍関係以外のシステムでは，現技術レベルで可能な最高のセキュリティ対策をほどこしたシステムであり，セキュリティ問題を論じる場合の指針を提供する好事例システムと言えよう。

(1)　全銀協標準通信プロトコル

企業と銀行との間を通信回線を介して接続し，新たな金融サービスを提供するシステムが増えつつある中で，全国銀行協会連合会（以下「全銀協」と略す）では，通信プロトコルの標準化を最優先課題として取組み，昭和58年10月に，その第一ステップとして標準通信プロトコル（ベーシック手順）を制定した。さらに昭和59年1月には，第二ステップとしてパーソナル・コンピュータ用標準通信プロトコル（ベーシック手順）を制定し，ひきつづきハイレベル手順の標準化に着手している。従来の通信プロトコルはメーカー別・機種別に，その制御手順，フォーマット，コード体系が違っており，異機種のコンピュータを接続する場合に多大な費用・労力を要したが，この標準化により容易に異機種コンピュータ間の接続が可能となり，エレクトロニック・バンキング発展の下地が出来たことになる。

本項では，標準通信プロトコル（ベーシック手順）の概要を述べ，特に安全性の観点からの考慮点につき触れる。

①　適用回線仕様

企業と銀行を接続する回線の種類および伝送速度は，

・デジタル・データ交換網の伝送速度9600BPS回線を使用する。

・公衆通信回線の伝送速度2400 BPS回線を使用する。

② 制御仕様

本仕様では，伝送制御手順仕様（接続するコンピュータ間のデータリンク制御レベルおよび通信制御レベルの制御手順）と電文制御手順仕様（機能制御レベルおよびアプリケーション・レベルの制御手順）とからなっている。規定にあたっては，従来ベーシック手順では採用されていなかった国際標準化機構（ＩＳＯ）のOSI（Open Systems Interconnection）参照モデルで定義されている機能階層化（レイヤ）の考え方を採用している（図3－51参照）。

レイヤ		レイヤ	機能	制御区分
7. アプリケーション		5. アプリケーション	○再送要求 ○運用管理 ○列信処理 ○データ圧縮処理	電文制御
6. プレゼンテーション		4. 機能制御	○通信制御 ○通信開始・終了制御 ○ファイル伝送／アクセス ○通番管理	
5. セッション				
4. トランスポート		3. 通信制御	○データ順序制御 ○ブロッキング／デブロッキング(ETB)	伝送制御
3. ネットワーク			○誤り制御	
2. リンク		2. データリンク制御	○データリンクの設定・維持・解放 ○データの送受信	
1. フィジカル		1. 回線	○電気的・物理的接続条件	

〔ＩＳＯのＯＳＩ参照モデル〕　〔全銀協標準通信プロトコル（ベーシック手順）〕

図３－51　OSI参照モデルと全銀協標準通信プロトコル（ベーシック手順）のレイヤの比較

ⓐ　伝送制御手順仕様

伝送方式は透過方式とし漢字コードの伝送が可能である。伝送ブロック長は可変長で，9,600 BPS 回線では最大2,048バイト，2,400 BPS 回線では最大256バイトの伝送ブロック長とし，伝送制御コードはEBCDICコードを使用している。

ⓑ　電文制御手順仕様

本仕様では，接続相手の正当性確認のための通信制御電文および伝送するファイルの正当性を確認するためのファイル制御電文を設け，通信の安全を確保している。

①　通信制御電文

通信制御電文は，センタ確認コードおよびパスワードによって接続相手の正当性チェックを行うほか，データ送受信の方向（連絡モード，照会モード）等を制御する電文である（図3－52,表3－5参照）。

センタ確認コードおよびパスワードが一致してデータ伝送が可能となる。

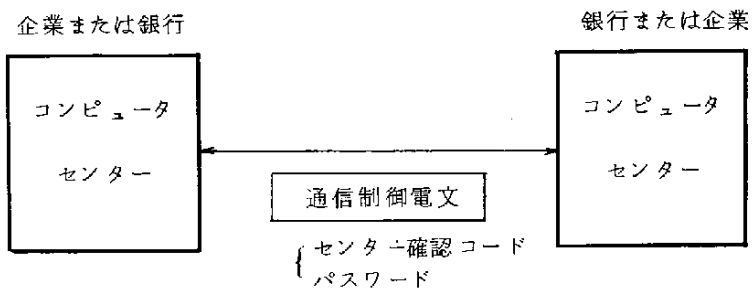


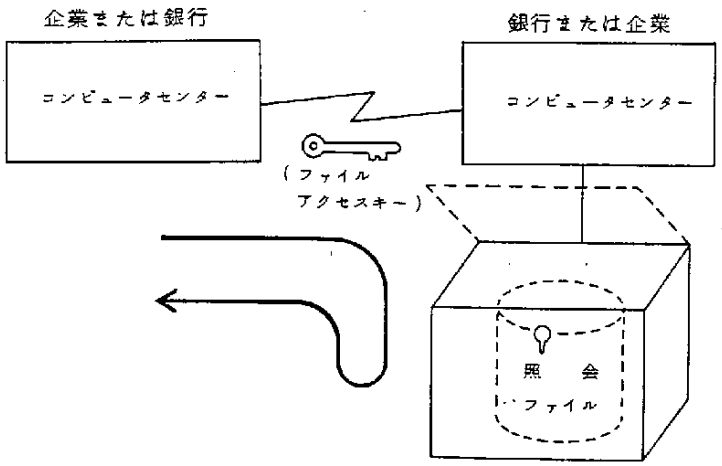
図3－52　通信制御電文の概念

②　ファイル制御電文

ファイル制御電文は，ファイル・アクセス・キーによってファイル・アクセス相手の正当性チェックを行うほか，伝送結果の確認および障害復旧時等におけるデータの再送等に関する制御を行う電文である（図3－53,表3－6参照）。

表３－５　通信制御電文

項　目	説　明
電文区分	通信制御電文の種類を表わすコードで、開閉局の要求、回答等の区分がある。
処理結果	通信制御上の要求（開局または閉局等）に対する回答表示コードである。回答電文においてセットされる。
相手センター確認コード	通信の秘密保護の一環として通信制御上の相手（企業および銀行のセンター、接続相手コンピュータシステム等）の正当性確認を行うためのコードで、通信要求を受信する側のアドレスがセットされる。
当方センター確認コード	相手センター確認コードと同様の目的で使用されるコードで、通信要求を送信する側のアドレスがセットされる。
通信年月日時分秒	通信実行時のタイムスタンプで、事後のデータチェック等データの保護機能の一環として利用する。
パスワード	アクセスコントロール機能の一環として、企業・銀行相互間レベルでのデータ送受信の正当性確認のために使用するコードで、その具体的内容はデータを送受する二者間で任意に決定する（暗号化も可）。なお、電文区分別に異なるパスワードを使用することができる。
アプリケーションＩＤ	通信プロトコルの上位レベルの規定で、通信形態（ファイル伝送、ジョブ伝送、メッセージ伝送等）の区分を表示する。
モード	通信制御権とデータ送受信の方向を示す区分である。
拡張用エリア	暗号化等の将来的拡張用の予備エリアである。特定企業・銀行間で任意に使用はできない。



〔ファイル・アクセス・キーが一致して初めて当該ファイルのファイル伝送が可能となる。〕

図３－53　ファイル・アクセス相手の正当性チェック

表３－６　ファイル制御電文

項　目	説　明
電文区分	ファイル制御電文の種類を表わすコードで、開始・終了要求、開始・終了回答等の区分がある。
処理結果	ファイル制御上の要求（開始・終了等）に対する回答表示コードである。回答電文においてセットされる。
ファイル名	伝送すべきファイル名を表わす。
ファイルアクセスキー	データ保護機能の一環としての「アクセスコントロール機能」のために使用するコードで、その具体的内容は当該ファイルアクセス部署にて任意に決定され、キーの管理は秘密保護の対象とする（暗号化も可）。なお、電文区分別に異なるファイルアクセスキーを使用することができる。
テキスト数	同一ファイル伝送における総テキスト数を表わす。総テキスト数には、再送テキスト数を含めない。
レコード数	同一ファイル中に含まれる総レコード数を表わす。総レコード数には、再送レコード数を含めない。
レコードＩＤ	レコードの固定長または可変長の区分を表わす。
レコード長	同一ファイル中に含まれる固定長レコード１件の長さを表わす。
再送指定区分	ファイル再送時の再送範囲を示す。
データ圧縮ＩＤ	データ電文のデータ圧縮の有無を示す。
拡張用エリア	暗号化等の将来的拡張用の予備エリアである。特定企業・銀行間で任意に使用はできない。

(2)　SWIFT（Society for Worldwide Interbank Financial Telecommunication）システム

SWIFTシステムの概要については，第3.2.2項で触れたが，現在，加盟国35，加盟行800に達し，巨額な資金の移動が本仕組みを利用して行なわれている。１件の取引金額が数百億円を超える取引もあり，正しく取引が処理されることが大前提のシステムで，システムの安全保護機能は極めて水準の高いものといえる。

①　操作の安全保護

メッセージの紛失や棄損，伝送の誤り，機密がもれる，不正な改ざん等を防止するため次の手段を講じている。

ⓐ　メッセージの番号付け

①　入力通番

送信銀行の端末は，送信されるすべてのメッセージに次の入力通番を自動的に割り振る。各端末識別子によって送信されるすべての種類のメッセージに，1つの順番に従って番号がつけられる。SWIFTは，入力通番が次に来るべき番号かどうかチェックし，正しい順番になっていないメッセージは拒否される。

②　出力通番

SWIFTは銀行に送るすべてのメッセージに出力通番を割り振る。受信銀行の端末は，出力通番の順番を検査する。

ⓑ　伝送エラーの検査

端末と地域プロセッサの間，あるいは地域プロセッサとオペレーティング・センタの間で用いられる伝送手順には，伝送エラーを検出するために周期冗長検査（ＣＲＣ）が含まれる。

ⓒ　暗号装置

地域処理センタ（ＲＰＣ）とオペレーティング・センタ（ＯＰＣ）間の回線の両側に暗号装置があり，情報がもれる事，不正な改ざん等の保護を行っている（図３－54参照）。この装置は，送受信局でランダムな発生順序を生成する。さらに安全保護を高めるために，その順序は可変のキーで修正できる。可変のキーは，回線の両側で任意の間隔で同時に変更できる。発生した文字の連続した流れがあるので，回線にアクセスする人は，いつメッセージが伝送されているのか知ることができない。銀行は，ＳＷＩＦＴと相談して，自身の端末と地域処理センタの間に回線を保護する暗号装置を設置できる。

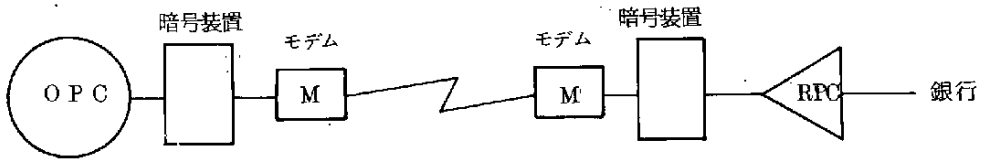


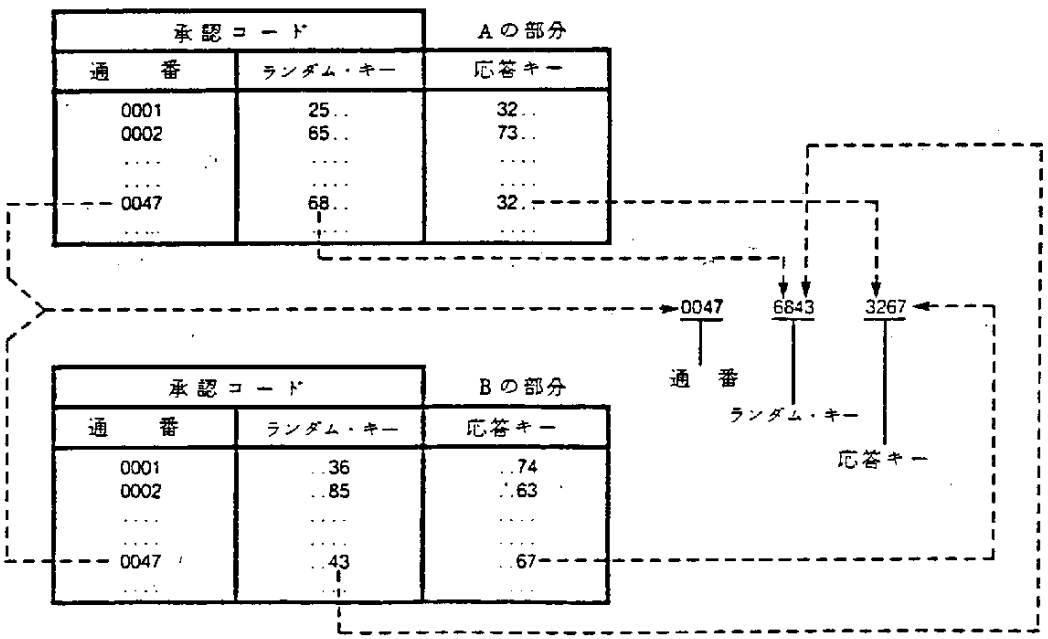
図３－54　ＳＷＩＦＴ伝送系

② ログインとログアウト

銀行とSWIFTとの通信開始は，定められたログイン手順に従って行われる。この手順どおり行われない限りSWIFTとの接続は出来ない。ログイン手順で使用する承認コードは，あらかじめSWIFTから送付されたログイン・テーブルを使用して生成される。

〔ログイン・テーブル〕

SWIFTは，固有の承認順序と応答キーのテーブルを各端末識別子ごとに発行する。各銀行はテーブルの受領者を定めSWIFTに知らせ，SWIFTは，テーブルを2つの部分にわけて指定された人宛に別々に送付する。



ログイン・テーブルは，2つの部分A，Bに分かれている。
通番＋ランダム・キー＝ログイン・メッセージでSWIFTに送られる承認コード
応答キーは，SWIFTからの応答である。

図3－55　テーブルの使い方

銀行は，ログアウト・メッセージを送信して端末の使用を終了する。また銀行から送られるメッセージに，誤りが異常に多くあるときは，一定限界を超えるとシステムが自動的にログアウトを行っている。

③ メッセージの認証

SWIFTのメッセージの認証方法は，銀行間のメッセージで認証の手段や金額の確認に用いられていた電信テスト・キーを改善して自動化したもので，メッセージ・テキスト全部について自動的に計算が行われる（図3－56参照）。

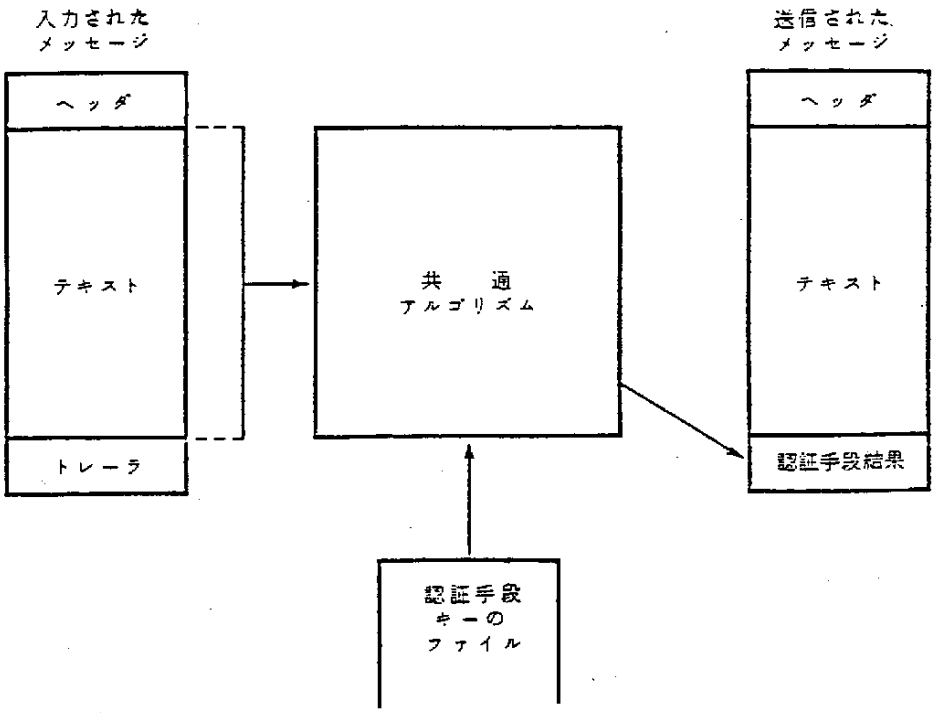


図3－56　SWIFTのメッセージ認証

送信銀行では，送信端末サイドで入力メッセージのテキスト部分を，受信銀行との間でとりきめた認証手段キーを使用し，SWIFT提供の認証手段アルゴリズムにより算出したキーを，送信メッセージに付加してSWIFTに発信する。SWIFTは，キーが指定されたメッセージ・カテゴリの中にあるか検査する。受信銀行では，受信端末サイドで受取メッセージのテキスト部分を，送信銀行との間でとりきめた認証手段キーを使用して，同一のア

ルゴリズムで算出したキーと，受信電文のキーとの一致を確認する。

〔認証手段キーの交換〕

上記機能が果されるためには，事前に送受信が行われる銀行間で認証手段キーの交換がなされている事が前提となる。このキーの交換手順についても安全保護の観点から，望ましい手順がSWIFTにより示されている。

④ メッセージの保存とオフライン・リトリーバル

銀行は，送受信したメッセージのコピーや，それについての情報を以下の方法で入手できる。

ⓐ オンライン・リトリーバル

オンライン・リトリーバルにより入力後0～14暦日内に端末から送られたメッセージにつきリトリーバルが可能である。

ⓑ オフライン・リトリーバル

入力後14日から4カ月後までのメッセージについてコピーや情報をSWIFTチーフ・インスペクタに要求することが出来る。メッセージは暗号形式で保存されており，リトリーバルの処理には時間と費用がかかる。

⑤ 責　任

このシステムに関係する送信銀行，SWIFT，受信銀行のそれぞれの責任・義務の内容・範囲が明定されている。

3.5 総合的対策案

当プロジェクトでは，ネットワーク・セキュリティ調査研究の締括りの作業として，電子化取引を可能にするネットワークの，セキュリティ対策案を作成した。この対策案は，100%完全な対策を実現しているわけではないが，セキュリティ対策研究の起爆剤になることを期待し，新構想として提案するために作成した。本節では，この新構想について説明する。

第3.5.1項では対策方針について述べ，第3.5.2項および第3.5.3項では，新構想の内容を説明する。第3.5.4項ではその効果について言及し，第3.5.5項では開発期間および課題等について簡単に述べる。

この新構想が，具体的開発目標となり，我国のネットワーク・セキュリティ確立の第一歩となることを，我々は期待する。

3.5.1 セキュリティ対策の目的と方針

(1) 目 的

ネットワークにセキュリティ対策を施す目的は様々であるが，ここでの最大の目的は，コンピュータ・ネットワークを利用した電子化取引を，可能にすることである。従来のコンピュータ・ネットワークを用いて送られたメッセージは，参考資料として用いることは可能であったが，証明用資料には成り得なかった。その理由は，これまでの分析結果を総合すると次のようになる。

① コンピュータ・ネットワークの信頼性に実績がない。

② コンピュータ・ネットワークのメッセージは，電子的な記録であり，改ざんが容易である。

③ 改ざんされた場合，痕跡さえも残らない。

上記①の問題は，現在では人間の潜在意識として存在しているだけで，実際は，書類よりも安全な場合もある。すなわち，①の問題は解決済みと言っても良い。しかし，②，③は，現在でも依然として解決の難しい問題として存在している。電子的記録は，本質的に書類のような保存性がないので，特別なから

くり（これをセキュリティ・メカニズムと呼ぶ）を施して，書類と同レベルの保存性を達成することが必要であるが，まだ決定的手法は見い出されていない。もちろん，通信回線を用いる限り，従来からある問題 ― 盗聴／介入 ― にも対処しなければならない。

さて，このように解決の難しい課題を越えて，電子化取引ネットワークを開発する必要があるのか，という疑問も出してくるだろう。これについては，第3.2.4項でも触れたが，開発する必要性は充分あると，当プロジェクトは判断した。ハイレベル・セキュリティ・ネットワークの効果については，第3.5.4項でも触れる。

(2) 対策の方針

当プロジェクトでは，以下に示す方針に従って，セキュリティ対策案を作成した。

① 既存技術の活用

第1に，可能な限り既存の技術を活用することとした。使用する回線もごく普通の通信回線で，特別の回線は用いない。

② 総合的効果を狙う

既存の技術を，システム的視野で組合わせることにより，セキュリティ対策の相乗効果を得られるようにする。

③ ユーザに選択の余地を残す

ネットワークのユーザが，セキュリティ・レベルを選択できることを目標とした。

④ 電子化取引が可能なネットワーク

ここでの目標は，完全な電子化取引（書類を一切使用しない取引）が可能になることである。制度／法律上の問題は，いづれ解決すると判断している。

⑤ 仲介方式の適用

本案のポイントは，公証機関の存在を前提にしたことである。公証機関は，公正かつ中立であることを，全ネットワーク・ユーザが承認している。従って，公証機関はネットワーク・ユーザ間のトラブルを解決する場合に，仲裁

人もしくは証人としての機能を発揮できるとの仮定をしている。現実に，そのような機関が存在可能かどうかは別途検討する必要があるだろう。

⑥ 対策の範囲

対策の範囲は，ネットワーク・ユーザ間（企業間）のネットワークの部分である。ユーザのシステム内の問題には，立入らないことが前提条件である。

⑦ 物理的な責任範囲の明確化

前記⑥を明確にするために，ユーザ・システムとネットワークとの接続点に，特殊なハードウェアを設け，これを境界として，セキュリティ上の責任範囲を物理的に識別する。

⑧ 共同利用ネットワーク

ネットワークの性格は共同利用ネットワークである。すなわち，開いたネットワークであり，誰でも参加可能なネットワークである。

3.5.2 ネットワーク・セキュリティ・センタ構想

共同利用データ通信ネットワークに，公証機関が管理運営するネットワーク・セキュリティ・センタを接続し，電子化取引あるいは高付加価値情報の交換を可能にする，一つの構想を提案する。この構想は，コンピュータ・ネットワークを利用した，高度情報処理を実現するシステム化案でもある。以下に，その概要を説明する。

(1) 全体像

図3－57に全体像を示す。応用システムあるいは端末（これらのネットワーク・ユーザを，以下では単にユーザと呼ぶ）が，多数参加している共同利用データ通信ネットワークに，ネットワーク・セキュリティ・センタ（以下「NSC」と略す）が接続される。

NSCは，公証機関により管理運営され，このNSCに登録されているユーザを，NSCユーザと呼ぶことにする。NSCユーザ間では，電子化取引の条件を満たすメッセージの交換（これを，セキュア・メッセージ交換と呼ぶ）を可能にする。

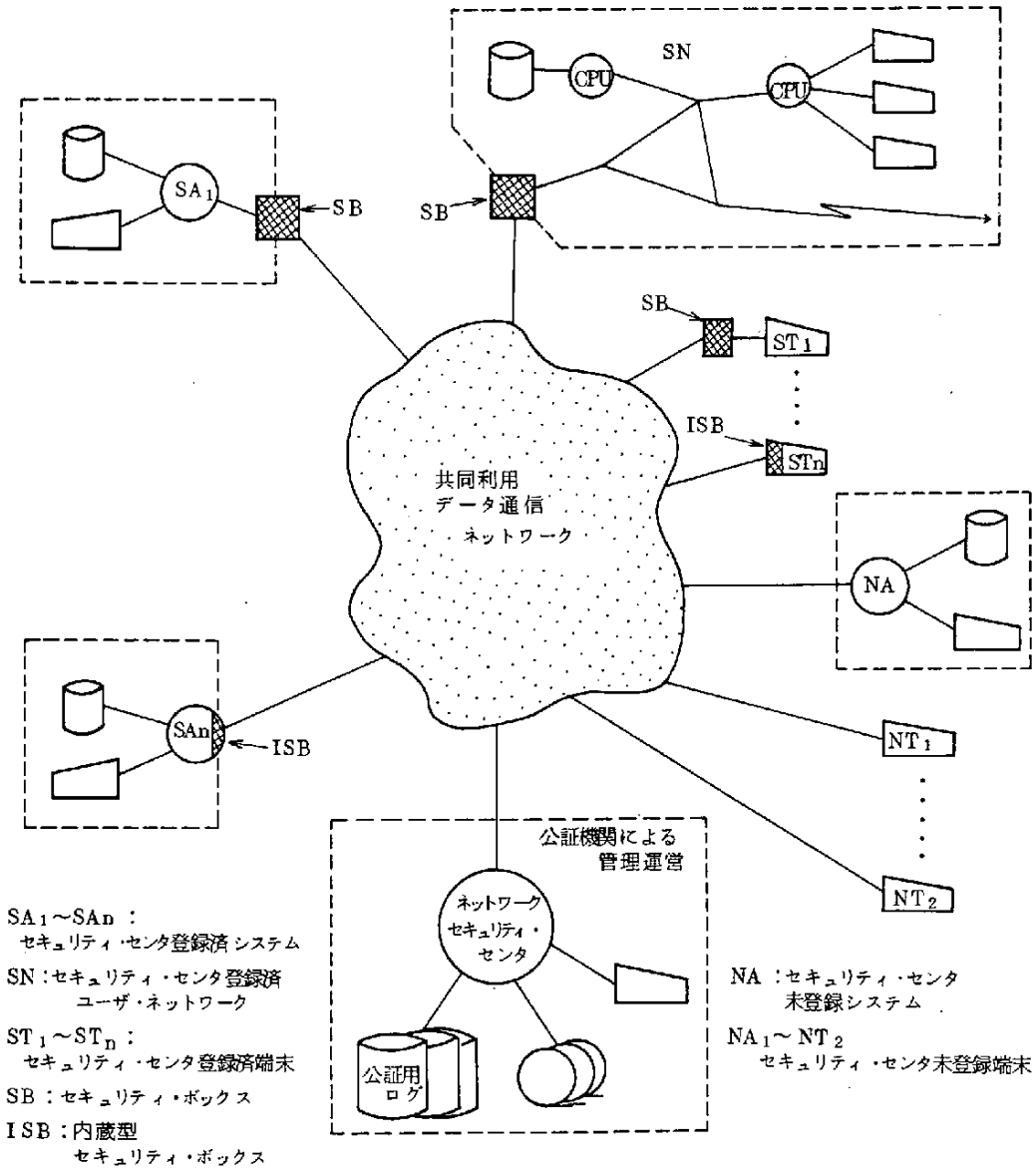


図３－57　ネットワーク・セキュリティ・センタ構想

① NSC ユーザ

NSC ユーザ（図3－57のSA_1～SA_2，ST_1～ST_2等）はNSCに，あらかじめセキュア・メッセージ交換に必要な，ユーザID，パスワード等を登録する。一方，NSCユーザのコンピュータ・センタあるいは端末にはセキュリティ・ボックス（図3－57のSB，ISB）が設置される。

② セキュリティ・ボックスと責任分解点

セキュリティ・ボックスは，NSCユーザと共同利用データ通信ネットワークとの接続点に置かれる，特別なハードウェア（図3－57 SB，ISB）である。昨年度（昭和57年度）提案のセキュリティ・ボックスは，メッセージ・ロギング装置であったが，ここで述べるセキュリティ・ボックス（以下，SBと略す）は，ログ機構の代わりに，NSCのハードウェアと一体となって，セキュリティ・メカニズムを構成する機構を内蔵した，一種のインタフェース装置である。

SBは，責任分解点でもある。すなわち，SBよりもNSCユーザ側のセキュリティ・コントロールは，NSCユーザの責任範囲であり，SBを含むSBよりネットワーク側は，NSC（というより公証機関）の責任範囲となる。

SBは，独立型（図3－57のSB）と，コンピュータ・システムあるいは端末等に内蔵された内蔵型（図3－57のISB）とがある。SBは，ⓐNSCの管理運営者である公証機関が管理運営するか，あるいは，ⓑ公証機関によって認定されたハードウェア（ソフトウェア内蔵）を，NSCのユーザが管理運用する。ⓑの場合は，公証機関が定期的にSBを検査することになる。

③ ネットワーク・セキュリティ・センタ（NSC）

NSCは，公正中立な第3者の機関（公証機関）によって管理運営されるコンピュータ・センタである。NSCは，すべてのSBをリモード・コントロールし，NSCユーザから要求があった時，SBと一体となってセキュリティ・メカニズムを働かし，NSCユーザ間に介在して，セキュア・メッセージ交換を可能にする。

NSCのもう一つの重要な機能は，メッセージ内容の公証用ログへの記録と保管である。このログは，メッセージ内容を法的証拠とする場合に，その正確性が保障可能なものである。

以上のように，NSCはネットワークのセキュリティ対策の要であるため可能な限りの物理的セキュリティ対策，技術的セキュリティ対策および運用上のセキュリティ対策を施す。

④ ノーマル・モード／セキュリティ・モード

NSCユーザはメッセージを送信する場合に，ノーマル・モードかセキュリティ・モードかを選択できる。ノーマル・モードとは通常のメッセージ交換を意味し，NSC／SBは，ノーマル・モードのメッセージ交換に一切介在しない。従って，NSCユーザと通常のユーザとのメッセージ交換も可能である。ノーマル・モードでは，SBは図3－58のようになっている。

セキュリティ・モードとは，セキュア・メッセージ交換が可能な状態を意味する。NSCユーザがこのモードを選択すると，SBは図3－59のようになり，セキュリティ・メカニズムが働くようになる。この状態で，NSCユーザが他のNSCユーザに対してメッセージを送信すると，NSCとSBが介在して，メッセージを保護しつつ目的地へ届ける。セキュリティ・モードでは，NSCユーザ間のみのメッセージ交換が可能で，NSCユーザと通常のユーザとの間で，メッセージを交換することはできない。

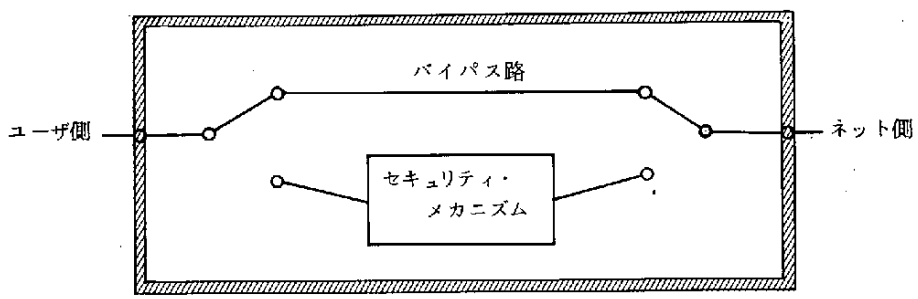


図3－58　ノーマル・モードにおけるセキュリティ・ボックス（SB）の内部状態

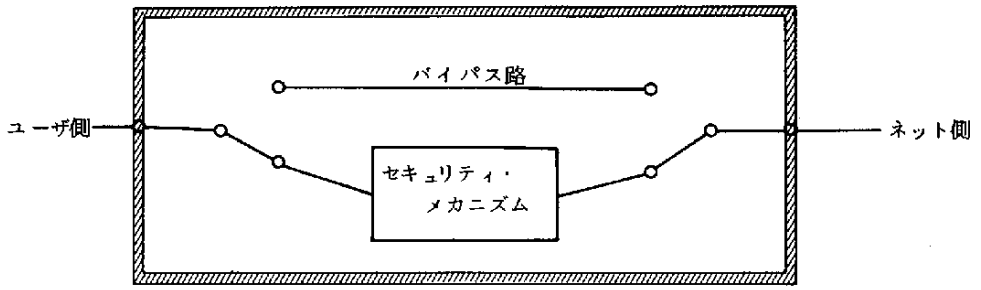


図3－59　セキュリティ・モードにおけるセキュリティ・ボックス（ＳＢ）の内部状態

(2)　安全性の程度による伝送モードの複数化

メッセージ伝送時の安全性を強化すると，伝送コストが高くなるのは止むを得ないことであるが，コストを押さえる何らかの対策も必要である。本構想では，メッセージの伝送コストを低減するため，メッセージ伝送時の安全性のレベルを，ＮＳＣユーザが選択できるようにする。この結果，ＮＳＣユーザは必要に応じた安全度を選択することが可能となり，総体的な伝送コストを引き下げることができる。伝送すべきメッセージがすべて重要であることは希であるから，この方式は合理的である。

先に(1)で述べた，セキュリティ・モードの選択は，ＮＳＣユーザが最初に行う安全度の選択である。本構想では，セキュリティ・モード選択時に，セキュリティ・オプションを指定することにより，メッセージ伝送時の安全度の選択の幅を拡げる。

①　セキュリティ・オプションを指定しない時

ＮＳＣユーザがセキュリティ・モードを選択すれば，セキュリティ・オプションを用いなくても，

- ＳＢ確認（端末確認に相当）
- メッセージ検証子の付加およびチェック
- メッセージ取扱い情報（送受信アドレス，送受信日付／時間，メッセージ長等）の公証用ログ・ファイルへの記録

が，メッセージ伝送時に行われる。この結果，メッセージ伝送の正確性とメ

ッセージ内容の破壊（含む改ざん）に対する安全性が向上する。

② セキュリティ・オプション

セキュリティ・オプションは，3種を予定する。このオプションの内容と効果を表3－7に示し，表3－8には，このオプションの組合せを示す。これらのオプションを用いることにより，NSCユーザは多様な安全度の中から，必要な安全度を選択できる。将来，新しい技術が開発された時も，オプションとして追加できる。このように柔軟性があるのも大きな特徴である。

表3－7 セキュリティ・オプション

オプション名	内容	効果
暗号化	・送信者側SBでメッセージ内容の暗号化を行い，受信者側SBで復合化を行う。 ・暗号キーの管理は，NSCで行う。	・メッセージ内容の漏洩を防止できる。 ・メッセージ改ざんに対する安全性も向上する。
送受信者名義確認	・メッセージ送信直前に，NSCが送信者に対してパスワードを要求する。このパスワードは，あらかじめNSCに登録されたもので，複数個設定できる。（送信者名義確認） ・受信側でも同様なことが可能である。（受信者名義確認） ・将来は，デジタル署名に置き換わる可能性もある。	・送信者名義，受信者名義を確認できる。 ・NSCには，名義（代表権者名，課名，その他）とそれに対応するパスワードが登録されていなければならない。 ・これは，押印（サイン）に相当する。
内容保障	・メッセージ内容をNSCで公証用ログ・ファイルに記録する。 ・暗号化オプションにより，メッセージ内容が暗号化されている時は，暗号のまま記録する。	・メッセージ内容を法的証拠として用いる場合に，公証用ログ・ファイルの記録は，その正確性を証明できる裏付け資料となる。

表3－8　セキュリティ・オプションの組合せ

モード	通信可能相手	セキュリティ・オプション			考えられる用途	参考（郵便制度との対比）
		暗号化	送受信者名義確認	内容保障		
ノーマル・モード	NSCユーザ ⟷ 一般ユーザ NSCユーザ ⟷ NSCユーザ （一般ユーザ ⟷ 一般ユーザ）				各種メッセージの交換	はがき
セキュリティモード	NSCユーザ ⟷ NSCユーザ				重要メッセージの交換	（封書）
				有	〃	内容証明
			有			（親展）
			有	有	承認メッセージ（契約書等）の交換	内容証明（親展）
（SB確認メッセージ認証）		有			高付加価値メッセージ（技術情報等）の交換	書留
‖		有		有	〃	内容証明書留
（郵便制度の配達証明に相当）		有	有			書留（親展）
		有	有	有	極秘契約メッセージ等の交換	内容証明・書留（親展）

(3)　基本的セキュリティ・メカニズム

本構想では，1回の送受信[*1]を5つのフェーズ（区分）に分割し，それぞれのフェーズにおいて，異なるセキュリティ・メカニズムを働かせる。

①　SBの起動（セキュリティ・モードの設定）

SBの起動は，NSCユーザの要求に基づき，NSCから行う。これは，NSCユーザが起動を要求したSBを，技術的手法により確認するためであ

＊1.：1回の送受信は，複数のメッセージで構成される。

る。ＮＳＣは，送信側ＳＢ（以下，㊤ＳＢと略す）と同時に受信側ＳＢ（以下，㊦ＳＢと略す）も起動し，「㊤ＳＢ－ＮＳＣ－㊦ＳＢ」の通信路を確保する。これらは，回線介入によるＳＢの不正な起動を防止する。

② 送受信準備

起動されたＳＢは，そのＳＢの受持ちＮＳＣユーザと一定の手順による接続確認と，セキュリティ・モードの確認を行い，送受信の準備を行う。これは，回線介入対策である。

③ 送受信

送受信は，「送信ＮＳＣユーザ ― ㊤ＳＢ ― ＮＳＣ ― ㊦ＳＢ ― 受信ＮＳＣユーザ」を経由する，複数のメッセージ交換で構成される。１回の送受信で何通のメッセージを交換可能とするかは，要検討項目である。交換可能通数を増加すると，安全性が低下し，減少するとオーバヘッドが増大（効率低下）するからである。

メッセージの伝送時には，「㊤ＳＢ ― ＮＳＣ ― ㊦ＳＢ」間で，メッセージ検証子によるメッセージ認証を行い，介入／改ざん対策を行う他，セキュリティ・オプションにより，以下の対策が実行される。

ⓐ 送受信者名義確認

名義確認とは，ＮＳＣユーザがＮＳＣへ登録した名義（複数設定される）の内のどれを用いて送受信するかを確認することである。送信側は，メッセージ発信直前に，受信側は，メッセージがＮＳＣに到着後で，受信ＮＳＣユーザにメッセージを渡す直前に行う。

ⓑ 暗号化

暗号化は㊤ＳＢで行い，復号化は㊦ＳＢで行う。ＮＳＣで暗号キーを変換することもあり得る（漏洩対策）。

ⓒ 内容保障

ＮＳＣで，メッセージ内容を公証用ログ・ファイルに記録する。これは交換されたメッセージ内容を保障する資料として活用される。

④　メッセージ送受信完了確認

ＳＢは，そのＳＢ受持ちユーザと，メッセージ送受信完了確認を一定の手順に従って行う。この時，なんらかの異常が発見されれば，既に完了した送受信を無効とし，警報を発すると共に，可能であれば回復処理を行う。

⑤　セキュリティ・モードの解除

メッセージ送受信完了確認を終えたＳＢに対して，ＮＳＣがセキュリティ・モードの解除を指令する。この時，ＮＳＣとＳＢとの間で，取扱った送受信の確認を行う。この段階で発見された異常は，関係者すべてに通知されるが，その異常により生じた損害の調査および補償は，ＮＳＣ（実際はＮＳＣを管理運営する公証機関）の負担で行う。もし犯罪であれば，犯罪の告発もＮＳＣが行う。

3.5.3　実現性（技術面）

前項で説明した「ネットワーク・セキュリティ・センタ構想（ＮＳＣ構想）」の技術的実現可能性について検討した結果を，以下に述べる。なお，本項に関連する基本技術の現状と将来の見通しが，第3.4節で述べられている。

(1)　基本通信技術

①　通信回線の利用

データ伝送が可能な通信回線であれば，どのような回線でも使用できる。しかし，回線自身の信頼度が高いことは，ネットワーク・システム全体の信頼性向上に大きく寄与するので，特定通信回線，ＤＤＸ網および21世紀の網であるＩＮＳ網の使用が推奨できる。なお，交換機能のない回線の場合はＮＳＣで交換業務を行う必要がある。

②　高付加価値回線の利用

高付加価値回線とは，ＶＡＮ等と呼ばれる汎用ネットワークであり，データの暗号化が実施されている場合もある。このようなネットワークを使用することも可能である。使用するネットワークが既に暗号化されていれば，本構想による暗号化により，２重に暗号化されることになり，セキュリティ・レ

ベルが向上する。

③ プロトコル

NSCユーザ ― SB間，SB ― NSC間に，標準プロトコル（例えばISOあるいはCCITT等の推奨プロトコル）を用いるのが効果的であろう。ただし，NSCユーザ ― SB間では，もっと単純なプロトコルとする方法も考えられる。SBおよびNSCは，プロトコル変換器の機能を持つことも可能で，この場合は多種類のプロトコルに対応できる。

このように技術的難関は特にないが，NSC構築時の環境に適合したプロトコルを選択する必要がある。

(2) セキュリティ・メカニズム関連技術

① SB確認

SB確認は，端末確認技術の応用であり，その内容は，SBのネットワーク上のアドレスと，SBが保持しているIDの相関を調べることである。問題点は，SBにIDを設定する方法と回線上を流れる確認用IDの改ざん／漏洩防止方法である。各種の対策方法が考えられるが，確認用IDの暗号化は特に有効である。SBをIDに設定する方法は，(3)で述べるが，今一歩の研究開発が必要である。

② メッセージ認証

メッセージ認証手法は，第3.4.3項で記述されている各種の方法が適用可能であるが，本構想では，一定のアルゴリズム（半ば公開）とキー（秘密）を用いて作成した，メッセージ検証子をチェックする方法を推奨する。本構想では，主に介入／改ざん検出用として利用する。（実際は，メッセージの誤配送も検出できる。）

主な問題点は，キーをSBに設定する方法であるが，これについては，(3)で触れる。

③ メッセージの暗号化

暗号化技術の詳細は，第3.4.2項で述べられているが，最も望ましいのはそこでは説明されていない新アルゴリズムの暗号を用いることである。しか

し，開発容易性を考慮すれば，既存の暗号アルゴリズムを利用するのが現実的である。従って，慣用暗号かハイブリッド暗号が適当と思われる。慣用暗号の問題点は，ＳＢへのキーの配布方法であり，(3)で触れる。

なお，本構想では，暗号キーの管理をＮＳＣで一括して行うため，配布以外の運用上の問題は比較的少ない。

④　送受信者名義確認

送受信者名義確認は，ＮＳＣに登録してある名義とパスワードを用いて，送受信者の確認を行うことであり，ＳＢ確認と併わせて，メッセージ送受信先の二重チェックを行う。このように当初案として，パスワード方式を提案するが，将来はより確実な方法が望まれる。例えば，デジタル署名の利用が考えられる。デジタル署名については，第3.4.3項を参照されたい。

さて，実際の運用時に，名義確認用のパスワードが，端末操作者によって必要な時にその都度入力されるか，コンピュータが自動応答するかは，ＮＳＣユーザの選択によって決まる。例えば，非常に慎重な社長は，自ら端末で入力することになろう。従業員が軽率に入力しても，「名義確認」の効力に変りはないからである。

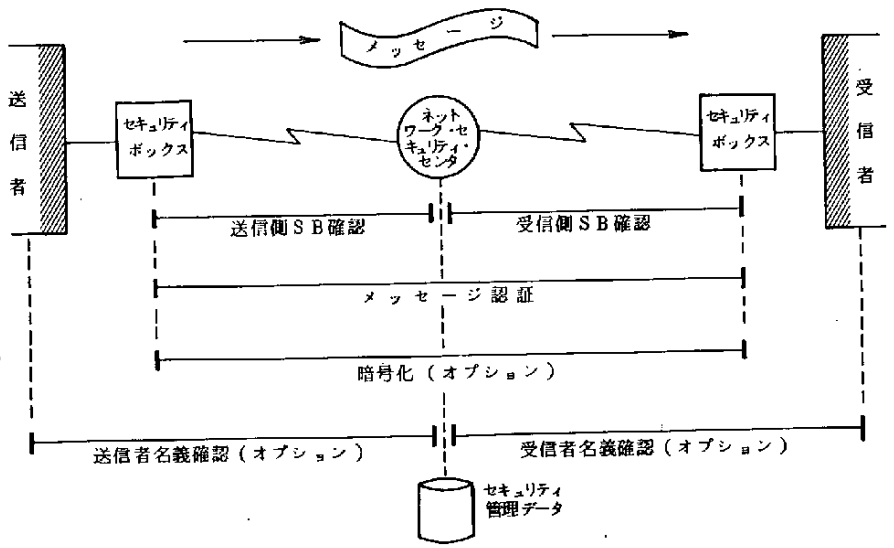


図３－60　ＮＳＣ構想におけるセキュリティ・チェックの範囲

(3) セキュリティ・ボックスの技術（ＳＢ）

ＳＢは，セキュリティ・メカニズムを実現する重要なハードウェアであり，その全体的イメージは，フロント・エンド・プロセッサ（ＦＥＰ）である。ＳＢには，独立型と内蔵型が考えられるが，機能は同一であるので，以下では独立型ＳＢについて記述する。

ＳＢとＦＥＰとで異なる点は，ＳＢにはセキュリティ・メカニズムがあることと，ＳＢが至近距離（物理的距離）にあるＮＳＣユーザのシステムにコントロールされるのではなく，遠方のＮＳＣによってコントロールされることである。

① ＳＢのセキュリティ基本機構

ＳＢには，次に示す２つのセキュリティ基本機構がある。

ⓐ 暗号化／復号化機構

ⓑ メッセージ検証子作成機構

上記ⓐ，ⓑ共にソフトウェアで実現可能であるが，ⓐはハードウェア化すべきことを敢えて述べる。その理由は以下による。

- 従来の暗号器のように，メッセージ全体を暗号化するのではなく，部分的な暗号化，二重暗号化等，かなりきめの細かい暗号化を行う必要があること。
- 変換速度を速くする必要があるが，ＳＢはマイクロ・プロセッサ・ベースで構成するため，ソフトウェアで実現すると変換速度を速くできない。
- 暗号化機構は，メッセージ検証子作成にも利用できる。
- 暗号キーをメモリ内[*1]に保持する必要がない。
- ハードウェア化が容易になった。

従って，マイクロ・プロセッサの機械語命令の一つとして暗号化／復号化命令を設け，外付けのハードウェアとして実現するのが適当である。暗号キーは，特殊なキー・レジスタ等に保持する方法が考えられる（図３－61参照）。

＊１：マイクロ・プロセッサを動かすプログラムが入っているメモリ。

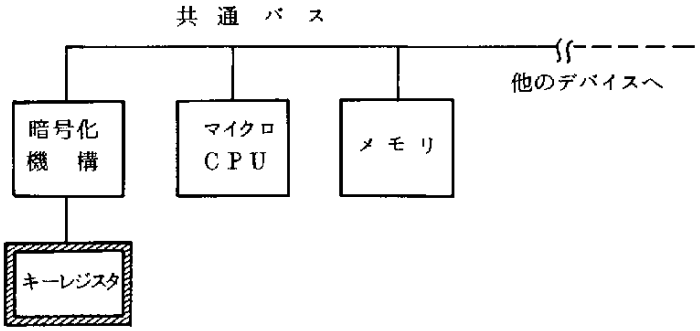


図３－61　外付け方式によるハードウェア化暗号化機構

さて，慣用暗号（例えば，ＤＥＳ暗号）であれば，以上のような実現方法が充分可能であるが，公開鍵暗号であるＲＳＡ暗号の場合には，まだ全面ハード化が難しい段階にある。今後の研究開発が期待されるが，当面はソフトウェアで実現しなければならないだろう。そのため，先に，ハイブリッド暗号（暗号キーだけを公開鍵暗号で暗号化する）を推奨したのである。

②　ＳＢの基本構成

ＳＢのハードウェア構成として図３－62が考えられる。暗号化機構とセキュリティ管理機構を除けば，マイクロ・コンピュータと大差はない。技術的難関は，信頼性の確保にある。これについては，かなりの検討が必要となろう。

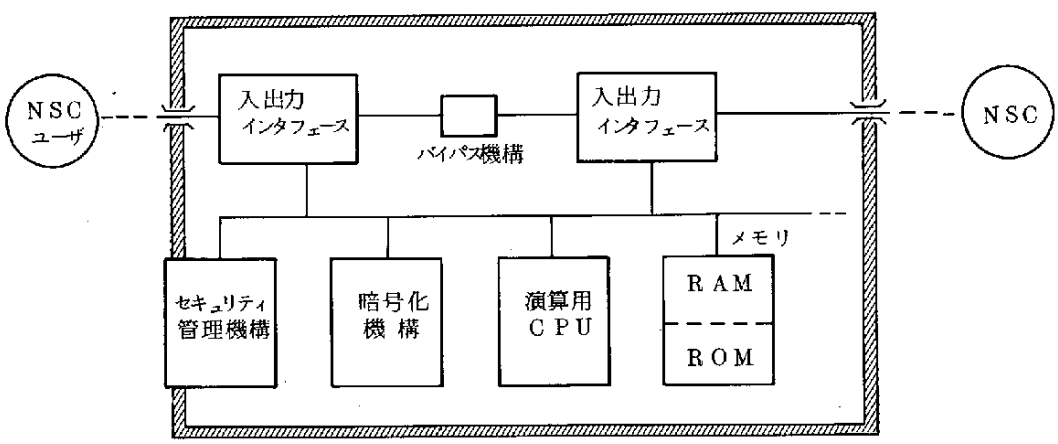


図３－62　ＳＢのハードウェア構成例

ここでは，セキュリティ管理機構について，少し詳細に述べる。前述したように，ＳＢにはＳＢのＩＤ（端末ＩＤ），メッセージ検証子作成用のキー，暗号キーおよび後述するＳＢコントロール・コマンドを暗号化するマスタ・キー等，各種のキー・データを保持する。これらは，セキュリティ上重要なデータで，時々変更することが必要である。

セキュリティ管理機構は，これらのデータを保存する場所である。問題点は，初期化の方法である。当初案として，ＩＣカードを提案する。このＩＣカードは，ＮＳＣで発行し，ＮＳＣユーザ管理者に渡される。ＩＣカードには必要データが入っており，これをＳＢにセットすると初期化が完了する。ＳＢを使用しない時は，ＩＣカードを外しておくことができる。ＩＣカードは一定期間後に無効として，再発行する。ただし，将来的には，回線によるキー・データの配布方法を検討する必要がある。

ＳＢのソフトウェアの構成については，かなり流動的な要素が多いので，今後の研究開発を待って検討すべきである。

③　ＳＢコントロール・コマンドの問題

ＮＳＣは，ＳＢをリモート・コントロールするため，各種のコマンドをＳＢに送信する。その逆もある。このようなことは，テレコミュニケーション・システムの得意とするところであるが，本構想では，大きな問題点となる部分である。このコマンドは，メッセージを安全に転送するための制御メッセージであるが，安全にすべきメッセージと，同一の通信路を通るという矛盾がある。[*1]

この対策のために，コマンドにも，改ざん検証子の付加，暗号化，コマンド送受信一連番号による管理等が必須である。特に暗号化は，対策の切り札として用いられることになり，効率低下を防止するために，暗号化機構のハードウェア化は特に重要である。

＊1.：コマンドを安全に送信できるのであれば，メッセージも安全に送信でき，従ってセキュリティ・メカニズムは必要ないことになる。

(4) ネットワーク・セキュリティ・センタ（ＮＳＣ）の技術

ＮＳＣは，コンピュータ・センタであり，外観的には，通常のコンピュータ・システムと大差はない。しかし，ＮＳＣはセキュリティ対策の要であるので，金融業のコンピュータ・センタに似た形態になることが，予想される。より完全に近い信頼性および安全性を確保するため，可能な限りの物理的，技術的および運用上の対策が必要であるが，各種対策の組合せ手法を別とすれば，基本的対策技術・手法は，現在既に充分なレベルに達していると思われる。ここでは，アクセス・コントロールと公証用ログの技術について，簡単に触れる。

① アクセス・コントロール

ＮＳＣには，ＳＢのＩＤ，メッセージ検証子作成用のキー，暗号キー等，セキュリティ・メカニズムの基本的データがすべて集中しているので，史上最も強力なアクセス・コントロール・メカニズムが必要になる。ソフトウェア上の工夫と運用上の工夫により，必要にして充分な対策を行わなければならない。汎用のアクセス・コントロール・ツールの利用も効果的である。

将来の課題として，第１章で述べられているセキュリティ・オペレーティング・システム（ＳＯＳ）の導入がある。この導入により，ＮＳＣのセキュリティ・レベルを，大きく向上させることが可能となる。ＳＯＳは，まだ商用として実用化されていないので，今後の研究開発が待ち望まれるところである。

② 公証用ログ

公証用ログは，本構想での電子化取引の要である。ここでも，史上最も強力なセキュリティ対策が必要になる。ただし，データ破壊さえなければ，多少の漏洩は致命的欠陥にならないことが，せめてもの救いである。そのため，データの二重保管等の従来の手法が効果的に使用できる。しかし，もっと画期的対策を行いたい。例えば，第２章で述べているロギング・サブシステム（第2.5.2項を参照）の応用である。公証用ログは，セキュリティ・レベルは高いものの，記録と保管という単一機能の処理内容であるので，ロギング・サブシステムを効果的に用いることができる。

一方，暗号化技術を応用し，使用した暗号キーの保管だけで，メッセージ内容の保障を行う方法もある（図３－６３）。この方式を用いれば，メッセージ内容そのものは保存する必要がないので，データ量を減らすことができ，さらに漏洩対策も容易になる。

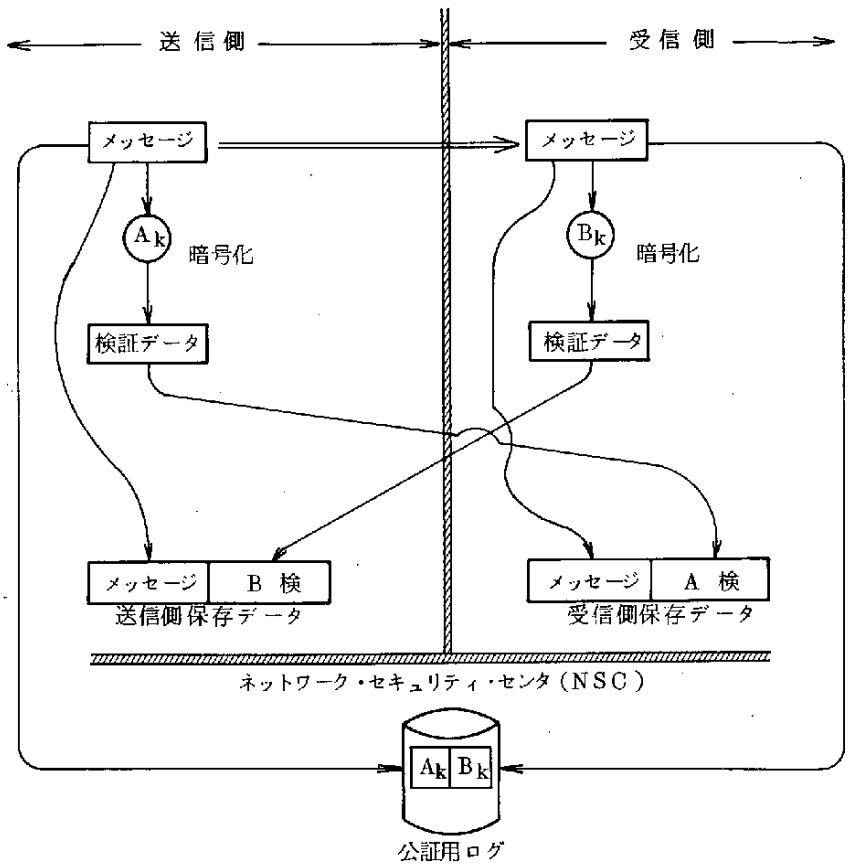


図３－６３　暗号化技術応用による公証用ログ

3.5.4 期待する効果

(1) 直接的効果

コンピュータ・ネットワーク・システムが拡がるにつれ，利用される業務のレベルも当初の，銀行口座残高問合せ，乗物の座席予約あるいはホテルの予約状況問合せ等から，銀行業務における本人了解の公的機関への支払（自動引落し），同一名義人による，口座から口座への資金移動等へ，利用範囲が次第に拡大しつつある。それでも，たとえコンピュータ・ネットワーク・システムが故障したり，あるいはそのシステムで故意の犯罪が起ったとしても，直接金銭的被害が及ぶ範囲は，現在では狭く，本人を中心にすぐ調べることができる範囲で，システムを利用している。

しかし，コンピュータ・ネットワーク・システムが，さらに拡大し，利用範囲が閉ざされた範囲（クローズド・システム）から，開かれてくる高度情報化社会になると（オープンド・システム），先に述べた乗物やホテルの予約における代金の支払いが，また銀行業務では，資金の移動が，本人の範囲ではなく，他人との間で行われるようになり，さらには，契約に基ずく代金決済が，コンピュータ・ネットワーク・システムの中に記憶されている契約条件に従って，自動的に行われるようになる。もちろん，個人のレベルでもキャッシュレス社会になり，代金の決済が自動的にコンピュータ・ネットワーク・システムで行われる。すなわち，電子化取引時代となる。

電子化取引を，従来の取引と比べると今のままでは，次の2つの弱点がある。

① 電子化取引の最大の弱点は，取引行為の結果について，物的証拠が残らないことである。各所で，取引の過程や結果の記録は残るが，物的証拠はない。取引の相手と記録を確認し合って，処理せざるを得ない。しかし，高度情報化社会のコンピュータ・ネットワーク・システムで結ばれた，多人数の間での記録を確認し合うことは難しい。

② 電子化取引は，現在行われている商取引のルールや法制度では，対応しきれなくなって来る。伝票と帳簿によるルールや法制度では，経済活動が廻らなくなってくる。

この２点に対する新しい対応策として，ＳＢ（セキュリティ・ボックス）とＮＳＣ（ネットワーク・セキュリティ・センタ）の考えが出て来た。第３者が管理するブラック・ボックスのＳＢの暗号化機能によって，ネットワークを移動するデータを改ざんしたり，挿入したりすることが困難になる。また，取引の相手が，ＳＢを付けていれば，暗号化されたデータによるデータのやり取りとなるので，安心できる。

しかも，暗号化データの処理プログラムはＮＳＣ（第３者が管理・運営する）より提供される，ブラック・ボックス・パッケージで処理するので，安全性もより高くなる。さらに，ＮＳＣを利用して，電子化取引の内容をＮＳＣに記録させることにより，万一電子化取引において，故障や故意の犯罪が起こりトラブルが発生しても，電子化取引の内容や経緯を，公的第３者たるＮＳＣに証明させることにより，トラブルを解決し易くすることができる。

(2) 波及効果

ＳＢやＮＳＣは，コンピュータ・ネットワーク・システムの高度情報化社会のモラル向上や，社会に対する心理的効果も大きい。

先づ第１に，ＳＢを設置しておけば，ネットワークを通じてアクセスして来ても，ＳＢがセキュリティ・ゲートになって，アクセスできないので，変なアクセスが掛らなくなる。

第２に，ＳＢによってメッセージが暗号化されているので，多くの場合，メッセージの改ざんや挿入等の犯罪を試みても，無駄であることが社会通念となって行く（抑止効果）。これにより新しい情報化社会のルール・倫理の一つができることが期待できる。

ＮＳＣを利用することによって，コンピュータ・ネットワーク・システムを利用した電子化取引を行う企業・団体は，神経質に，電子化取引の内容を，ロギングする必要が少なくなる。電子化取引のキー・ポイント（取引内容のキー・データ）が，すべてＮＳＣにロギングされ，内容についての公的証明が可能となれば，相手側に，この電子化取引はＮＳＣ経由になっているという信号を送るだけで，公的取引と見なされ，取引についての信頼度が高く評価される。

NSCの存在が知られることによって，電子化取引の信頼性が高まり，次第に，電子化取引が活発に行われるようになり，電子化取引の普及について貢献することが，期待できる。次に，NSCの存在が知られることによって，NSCが介在した電子化取引の内容のロギングを取引の参加者の誰かが，改ざんしたり，挿入したりすることもなくなってくる。なぜならば，NSCのロギング内容が公的な絶対的なものであって，自社のロギングは単なる記録としてしか取扱われないことが認識されるようになるからである。その結果，不正や犯罪を社会的倫理面から防ぐことが期待できる。

また一方で，電子化取引中に故障が起きて，取引内容のステイタスがバラバラになったり，不一致になっている時，NSCのロギングのステイタスから，関係者がスタートすれば，電子化取引が再スタートし易い等，故障時における安全性や信頼性を高める効果も期待できる。NSCは，集中的に故障対策が施され高い信頼性を維持しており，一般のシステムに対して故障時のリカバリ用の情報を，ある程度提供できるからである。

さらに，NSCの存在によって，高度情報化社会における電子化取引のあり方についての新しいモラルと，ルールが出来上って来ることも期待できる。

(3) 技術に対するインパクト

SBが公的第3者によって取扱われると，コンピュータ・ネットワーク・システムに接続するインタフェースの条件（プロトコル等を含む）が標準化され，これらが突破口となり，国内におけるネットワーク接続条件を一本化できる可能性もある。

また，暗号化についても，日本独自の暗号化機器として，信頼性が高く安価なものを開発することができる。さらに，各社，各種のパソコン，汎用端末，コンピュータおよび種々のネットワークの相互接続インタフェースの変換機または接続条件の簡易化に，NSCの思想が大きな役割を果たすことが期待される。

NSCで，第3者の公的証明が可能となるように，NSCの役割と機能を含んだ日本独自のSOS（セキュリティOS）が開発され，さらに，これを基本

とした一般応用システム向のSOSが開発され，未来のコンピュータ・ネットワーク・システムとして，全体の安全性と信頼性が極めて高いセキュリティ・システムを構築することが期待できる。また，保存期間が長く信頼性の高い，ロギング用大容量ファイル（例えば，光ディスク装置等）の進展も期待できる。

3.5.5 解決すべき課題

本項では，先に提案したネットワーク・セキュリティ・センタ構想（NSC構想）に基づく電子化取引ネットワークを，実際に開発すると仮定した場合の解決すべき課題と，ネットワークにおけるセキュリティ対策の確立のために，何をすべきか等について，簡単に述べる。

(1) NSC構想実現上の技術課題

第3.5.3項で説明したように，ネットワーク・セキュリティ・センタ（NSC）およびセキュリティ・ボックス（SB）を構成する基本的技術は，既に存在していると考えてよいだろう。むろん理想的技術（例えば，本人確認技術等）は，まだ研究開発中ではあるが，ほとんどの機能を持った技術は，充分応用可能な段階にあると考えられる。従って，技術上の主な課題は，いかに上手に既存の技術を組合わせて，レベルの高いセキュリティ機構を構築するかにある。

① 専用ハードウェア化

第1の課題は，専用ハードウェアの開発である。NSCおよびSBは，既存のハードウェアを用いて実現することは充分可能である。開発初期の実験では，恐らく市販の汎用ハードウェアを用いることとなろう。しかし，最終的なNSCおよびSBのハードウェアは，可能な限り専用ハードウェアにすべきである。その理由を以下に示す。

- 専用ハードウェアは，目的に応じた最適設計が可能である。これは，信頼性を向上させるうえで有利である。
- 専用ハードウェアの開発費は高価であるが，長い目で見れば，余計な機能がないだけコスト的に有利である。
- 汎用ハードウェアには余計な機能が付属しているが，これを取外すこ

とはコスト上の効果を著しく悪化させるので，通常，不必要な機能を抱えたまま使用する。ところが，この不必要な機能が，しばしばセキュリティ破りの入口として使用されてしまう。従って，専用ハードウェア化は，セキュリティ対策上も有利である。

- 技術の進歩により専用ハードウェアの開発が容易になった。

以上のように，専用ハードウェア化は，あらゆる面で有効である。特に，ＳＢは専用ハードウェア化すべきである。ＮＳＣでは，暗号化機構，アクセス・コントロール機構および公証用ログのロギング機構が，専用ハードウェア化したい部分である。

② 理想的基本技術の研究開発

第２の課題は，より完全なセキュリティ基本技術の研究開発である。冒頭で，ほとんどの機能を持った技術は既にあると述べたが，セキュリティ・レベルは高い方が望ましいので，新技術の研究開発も必要である。そして，幸運にも早期に開発できた技術は，ＮＳＣやＳＢに積極的に取込むべきであろう。この範ちゅうに含まれる基本技術は，

- セキュリティ・オペレーティング・システム（ＳＯＳ）
- 公開鍵暗号および新しい慣用暗号
- パスワードやＩＤカードによらない本人確認技術
- 再書込不能型光ディスク（ロギング・サブ・システム）

等である。

③ ソフトウェア

第３の課題はソフトウェアである。器ができれば，これに魂を入れなければならないが，そのソフトウェアが技術課題というのは，なじみにくいかも知れない。しかし，電子化取引ネットワークをコントロールするソフトウェアを構築する際の課題は多い。第 3.5.3 項では流動的要素が多いという理由で，その説明を避けたが，ネットワークの運用と直接リンクしているので，その設計はかなり難しいと予想される。

純技術的見地では，完全性の問題がある。セキュリティ機構が仕様通り構

築されていないと，システム全体のセキュリティ対策が無意味になる恐れがある。ソフトウェアの設計と構築は，最も難しい課題と言っても過言ではない。

(2) ＮＳＣ構想の開発期間／体制

ＮＳＣ構想を実現するためには，技術以外にも解決しなければならない様々な課題がある。その中から，開発期間と開発体制について，ここで触れておく。

① 開発期間

通常の大規模システムの開発期間は，およそ２年間と考えられるが，事前の検討期間を含めると３～４年というのが妥当である。従って，ネットワーク・セキュリティ・センタ構想（ＮＳＣ構想）の実現には，少なくとも３～４年の開発期間が必要である。

次に，ＮＳＣ構想はセキュリティ・レベルの高いことが特徴であることにより，セキュリティ検証という従来の開発にはなかった，特別な作業が必要である。第1.2.4項で述べているように，セキュリティ機構のチェックに最も有効な方法は，侵入テストである。この方法は有効ではあるが，長いテスト期間を要する。さらに，このテストで発見された欠陥は，修正[*1]されなければならない。そのため，６年程度の開発期間（中期的開発テーマ）は，専用ハードウェアの開発も考えれば，是非とも必要である。

しかし，今年度の調査でも明らかなように，既に電子化取引は実現に向って動き出しており，数年先には，本格的な電子化取引が，広範に行われる可能性が大きい。有効なセキュリティ対策が，まだ未確立というのにである。これらのことを考慮すると，６年後の実現では遅過ぎ，もっと早く開発する必要があるかもしれない。犯罪者は，待ってくれないからである。可能であれば，４年後を目標にすべきであろう。

② 開発体制

ＮＳＣ構想が企業間のネットワークであること，開発の難易度およびコスト

＊1：修正後，正しく修正されたかどうかのチェックと，再度の侵入テストが必要である。

等を考慮すれば，官・学・民が協力したプロジェクト（ナショナル・プロジェクト）による開発が，最初に浮び上ってくる。しかしながら，このようなプロジェクトを推進するためには，国民的な合意が必要である。セキュリティ対策については，総論的にはともかく各論となると，必ずしもまだ，その必要性に関して合意が得られる段階ではないようである。そのため，実際に犯罪が発生するまで待つか，あるいは，電子化取引とそのセキュリティの啓蒙活動等，という退屈な作業が必要になり，開発が遅れる可能性がある。

そこで，第3.5.2項の構想をもう少し詳細に検討し，民間ベースの開発プロジェクトとして実施できないかを，検討する必要が出てくる。恐らく，多少の機能低下を許容すれば可能だろう。しかし，大きな問題点もある。民間ベースの事業では，コスト／効果の追求が必須であり，電子化取引とネットワークのセキュリティ対策が分断されてしまう可能性がある。

一方，犯罪者が手を緩めるようなことは考えられず，セキュリティ上問題のあるネットワークには，必ず犯罪が発生するだろう。社会的混乱を発生させないために，有効なセキュリティ対策（ＮＳＣ構想）を真剣に研究開発できる体制，すなわち国家的取組みが望まれる。

(3) ネットワーク・システムのセキュリティ確立のために

当プロジェクトは，コンピュータ・ネットワーク・システムの有効なセキュリティ対策を調査研究するために，「電子化取引」を応用例として，検討を行ってきた。その結果，本節のＮＳＣ構想を提案するに至った。ＮＳＣ構想は，電子化取引という環境では，有効なセキュリティ対策であると確信している。しかし，机上の試案として留まっている限り，何らの効果も表すことはない。必要なのは，具体的な「もの」である。

ＮＳＣ構想の開発とは無関係に，現実に電子化取引は進行する。そして，いづれセキュリティ上の問題が発生すると，敢て断言する。もしその時，有効なセキュリティ対策が確立していないという理由で，電子化取引を中止したら，社会的混乱が起きることは，目に見えている。日本中のＣＤ／ＡＴＭが停止した時の様子を想像すれば，その混乱ぶりが分るだろう。ＮＳＣ構想実現のため

に，一刻も早く具体的開発に着手しなければならないのである。

ＮＳＣ構想は，先に述べたように，電子化取引という環境では有効なセキュリティ対策であるが，ネットワーク・システムには，別の環境もある。そこで，電子化取引以外の環境で有効なセキュリティ対策も，研究する必要がある。そして，いづれ，あらゆるコンピュータ・ネットワーク・システムについて，有効なセキュリティ対策を確立する必要がある。そこへ到達するのに，最も効果的方法は何であろうか。以前によく非難の対象となった，海外で創造されたアイデアの借用は，果たして有効な対策になるであろうか。残念ながら，ネットワーク・システムのセキュリティについて，参考となる実用的システムは，世界中でＳＷＩＦＴぐらいしかない。もし，実証論的立場をとるならば，もはや実際にネットワーク・システムを構築し，セキュリティ対策の研究開発を，我々自身で進める以外に方法はない。ひらたくいえば実験である。しかしこの実験は，現代科学のそれと同じく，大規模かつ多額の費用を必要とし，とても一研究機関の手に負える範囲にはないと思われる。国家的課題として官民が協力して取組む必要があろう。

昭和59年8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丁目5番8号
機械振興会館内
TEL (434) 8211 (代表)

印刷所　日生印刷株式会社
東京都品川区平塚1－8－10
TEL 03 (786) 0404

58－S001