57－S003

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

昭 和 58 年 3 月

JIPDEC

財団法人 日本情報処理開発協会

この報告書は，日本自転車振興会から競輪収益の一部である機械工業振興資金の補助を受けて昭和57年度に実施した「わが国の情報処理に関する動向調査」の成果をとりまとめたものであります。

はじめに

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

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

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

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

最後に，海外調査にあたって，絶大なご協力をいただいた，植松一裕氏，大川繁喜氏を始め内外の関係各位に対し，感謝の意を表します。

昭和58年３月　財団法人　日本情報処理開発協会

本調査研究で作成した報告書

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

訪　問　先　一　覧

訪問日時	訪　問　機　関	場　　所	面　　会　　者
11月8日 (月) ～ 11月10日 (水)	第9回コンピュータ・セキュリティ・コンファレンス (Ninth Annual Computer Security Conference)	ニューヨーク Statlerホテル	(主催) Computer Security Institute.
11月10日 (水)	チェース・マンハッタン銀行 (The Chase Manhattan Bank)	ニューヨーク チェース・マンハッタン・プラザ	G.U.RaO, Vice President. Robert G.Hollinger, Vice President.
11月11日 (木)	テクノロジー・アナリシス・グループ (Technology Analysis Group)	ニューヨーク	Patrick F. Sullivan, Principal.
11月12日 (金)	アメリカン・エクスプレス (American Express Company,Systems Planning Office)	ニューヨーク	John C.Schneider, Manager. Vincent Ditursi, Manager.
11月12日 (金)	ニューヨーク市調査局 (The City of New York Department of Investigation)	ニューヨーク	Rolf Moulton, Divector. E.Gordon Haesloop, Deputy Commissioner.
11月15日 (月)	マサチューセッツAI研究所 (MIT AI Laboratory)	マサチューセッツ・ケンブリッジ	Dr. James S. Miller
11月17日 (水)	プランニング・リサーチ・コーポレーション (Planning Research Corporation)	バージニア マクリーン (Planning Research Drive McLean)	P. Ray Mclnnis, Vice President. John E. Childress, PRC Security. Richard L.Kessinger, Systems Engineer. Ms. Jody E.Heaney, Programmer Analyst.
11月19日 (金)	セキュリティ・パシフィック・ナショナル銀行 (Security Pacific National Bank)	カリフォルニア グランデール (Glendale)	Ms. Sandra M.Mann, Vice President.

11月19日 (金)	カリフォルニア州立大学 (California State University, Northridge)	カルフォルニア ノースリッジ (Northridge)	Dr. Rein Turn, Professor.
11月22日 (月)	スタンフォード研究所 (SRI International)	カリフォルニア メンロ・パーク (Menlo Park)	Charles Cresson Wood, Consultant.
11月23日 (火)	ハネウェル社 (Honeywell Information Systems Inc.)	フェニックス	Jerome Lobel, Manager.

調 査 団 名 簿

山本　欣子	(財)日本情報処理開発協会	開発部長
三木　良治	(財)日本情報処理開発協会	開発部
植松　一裕	ファコム・ハイタック(株)	ファコム本部 システム第一部第三課　主任
大川　繁喜	日本電気(株)	情報処理 第一公共システム事業部 第二システム部　主任

目　　次

1. 調査概要

1982年11月，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を行なった。同時に，ニューヨークで開催された第9回コンピュータ・セキュリティ・コンファレンスに出席した。ここで全体を通しての調査の要点および総合的印象について概要を述べる。詳細は第2章以後を参照されたい。

1.1 背景および目的

1950年代に英国において，初めて出現したコンピュータ・システムは，その後30余年の歳月を経て，今や産業，研究，教育，行政等の社会のあらゆる分野に浸透し，今後，人間生活におけるコンピュータ・システムへの依存度はますます増大し続けるものと思われる。コンピュータ・システムの活用は，社会活動の効率化と利便性の大幅な向上をもたらすのみならず，コンピュータ無くしては不可能と思われる多様な新たな機能の実現を可能とし，それによって人間生活の活動の枠を広げ，併せて人間の能力そのものの拡大に寄与するものとなる。一方，その広範な普及に伴う多様なニーズへの対応として，コンピュータ・システムの高速，大容量化等の基本機能の向上に加え，入出力，処理方式，記憶方式等を始めとする各種機能の向上と多様化が進み，併せて情報処理と通信の融合によるオンライン処理，分散処理，リアルタイム処理等の広域処理の実現により，時間と距離の克服が現実のものとなった。

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

① 先進国，米国においては，既に10数年前から種々のコンピュータ悪用や犯罪の事例が報告されてきたが，我国においてもここ2,3年間に類似のトラブルが急に増加してきた。

② パーソナル・コンピュータの普及により，これらを端末として，種々の社会システムとオンラインで接続しようとする計画もあり，不特定多数のコンピュータ・システムへのアクセスによるトラブル発生の可能性が予見される。

③ コンピュータ・システムは巨大なブラック・ボックスであり，関係者以外は，その処理のメカニズムを知ることができない。特にその処理プロセスの細部にわたっては，それぞれのシステムを作成した極く限られた担当者のみしか理解し得ない。

④ 近年ソフトウェア技術者を中心とするコンピュータ要員の需要は大幅に増大し，これらが一部のエリート集団であった昔とは条件が著しく異なってきた。

このように，コンピュータ・システムに対する危険性は増大してきている。しかしながら，これに対応する有効な対策が少ないという大きな問題があり，当プロジェクトでは，昭和57年度より，2カ年計画で技術的な対策の可能性について，調査研究を開始した。

米国は周知のように，コンピュータ・システムの先進国であるが，同時にコンピュータ犯罪の先進国でもある。米国で起きたコンピュータ犯罪については，我国にも多数のレポートがあるため，詳述を避けるが，エクィティ・ファンディング事件やシュナイダー事件は，有名である。このように事件が多発すれば，当然それに対する防御方法も発達してくる。その結果，コンピュータ・セキュリティに関しても，米国が一番発達することになった。当プロジェクトでは，コンピュータ・セキュリティの最新の動向と，今後の方向を見きわめるため，下記に示す項目を調査テーマとして，米国での調査を実施した。

① 応用システムにおける現状での対策

② 既存のセキュリティ技術の利用状況およびその効果と評価

③ 新たに求められる技術とその研究開発状況

④ 将来のセキュリティ技術の動向

その結果，いくつかの新しい事実を発見することができたが，大勢としては我国と同様米国でも，決め手となる技術的対策はなく，新しい効果的な技術を模策中であり，ほとんどの応用システムでは運用による対策で対処していることが明らかになった。本報告書は，それらについてまとめたものである。

1.2　調査結果（概要）

1.2.1　応用システムにおけるセキュリティ対策

今回調査した応用システムは，いずれも金融機関システムである。金融機関は，もっとも高いレベルのセキュリティを要求されるので，各社とも様々な工夫を凝らして対処している。現状での対策の中心は，運用による対策である。各社ともセキュリティ・ガイドラインを作成していることに大きな特徴がある。このガイドラインには，セキュリティ・レベルを高めるために，どのようなことをすべきか，こと細かに記述してあり，これに従えば，誰でも一定のセキュリティ・レベルを確保できるというものである。もちろんそこには，支援技術として，どのようなセキュリティ技術（装置）を導入すればよいかも記述してある。特に，アメリカン・エクスプレス*1社には，極めて詳細なガイドラインがあり，同社の重要なノウハウとなっている。残念ながら，それを入手することはできない。

また，各社とも新しいセキュリティ技術を独自に研究しており，チェース・マンハッタン銀行*2では，コンピュータ・システムのグレード・アップを（詳細は不明），セキュリティ・パシフィック・ナショナル銀行*3では，通信回線の暗号化を検討している。しかしながら，各社とも現在の技術で充分対応可能であると指摘していたのは注目される。米国と我国では，国情がかなり違うため，米国での対策をそのまま我国に適用しても意味があるかどうか疑わしいが，セキュリティ・ガイドラインの文書化は，我国に採り入れても効果的ではないかと感じられた。

1.2.2　自治体における対応

---

*1：American Express Company

*2：The Chase Manhattan Bank

*3：Securiy Pacific National Bank

ニューヨーク調査局*1は，ニューヨーク市当局の１機関であるが，日本の自治体にはない，大変ユニークな機関である。この機関は，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に設けられ，その日常業務は，不正の調査である。それと同時に，コンピュータ・システムのセキュリティ・レベルの向上について調査研究もしている。ここでは，セキュリティ対策として，運用上の対策とシステム監査を重視している。特にシステム監査は，極めて厳密に行なわれており，既に数件の不正を発見したと言う。そのかわり，その手間も大変なもので，今後の課題の一つはシステム監査の効率化であるとしていた。

ニューヨーク調査局では，セキュリティ技術に対して，現在はあまり期待していないように感じられた。通信回線の暗号化等より先に，他にもっとやるべきことが数多くあると指摘していた。例えば，センタの運用の問題，端末での本人確認の問題等である。これらの問題の解決が急務であると指摘していた。

1.2.3　米国におけるコンピュータ・セキュリティの動向

大学，調査研究機関およびセキュリティ関連製品のベンダーを調査した結果をまとめると，現在の米国内でのコンピュータ・セキュリティの動向として，以下に示す諸点を指摘できる。

(1)　コンピュータの悪用と技術的対策

コンピュータ犯罪や悪用によるトラブルの件数は，統計上はここ数年来，減少してきている。これは公表されないケースが増えたためだという見方もあるが，一方，技術的対策を講じた成果だという意見もある。

(2)　メーカの動向

民間企業に広くセキュリティ機能を普及させるには，コンピュータ・メーカが中心となり，ハードウェア・基本ソフトウェアにわたるベーシックなセキュリティ商品を開発し，標準品に近い形で低価格な商品をユーザに提供することが，最も効果があると言われる。

---

*1：The City of New York Department of Investigation

現在，米国ではＩＢＭ社がもっとも積極的にセキュリティ関連技術の商品化に努めているように見える。またハネウェル社も，現在実用化されているものの中ではもっともきめ細かいアクセス・コントロール機能を持つ汎用ＯＳと言われるMULTICSを持ち，またＩＣカードの開発も行なっている。その他のメーカも軍関連のプロジェクトにおいて得たセキュリティ技術のノウハウをもとに，民間用のセキュリティ関連製品を開発しようとしている。

(3) 多様な商用セキュリティ関連製品

汎用ＯＳにおけるリソース保護やパスワードを中心とするアクセス・コントロール等，既に一般化した基本的セキュリティ機能の他に，通信回線用の暗号装置やファイル保護を中心としたソフトウェア・パッケージ等が民間用に多数市販されている。ソフトウェアのほとんどはＩＢＭ機種対象のものであり，リソース・アクセス制御のパッケージは現在約 1,000 ユーザに普及していると言われる。

(4) 新しい技術の必要性

セキュリティ問題は技術的対応のみで解決するものではないが，なお新たに研究開発すべき技術課題は多いという点では意見が一致していた。

(5) 研究テーマとしてのコンピュータ・セキュリティ

かつてセキュリティ技術の研究開発のメッカとも言われたＭＩＴでは，現在暗号関連のものを除いて，研究が下火となっている。一方，ＳＲＩでは，通信，暗号化，本人確認，ＤＢ，コンピュータ犯罪等テーマ毎のそれぞれの専門家により引き続き研究が行なわれている。その他ＭＩＴＲＥ社，ＢＢＮ社，ＳＤＣ社等いわゆる“シンクタンク”と呼ばれる研究機関がセキュリティＯＳやメッセージ・システム等のセキュリティ技術と取り組んでいるが，いずれも国防省や軍とのタイアップあるいは委託研究の形で研究を行なっている。

(6) 国防省および軍の技術的先導性

米国におけるセキュリティ技術は他のコンピュータ技術と同様に国防省や軍関係の研究開発をベースとして発展してきており，その成果が徐々に民間に技術移転を始めようとしている。

(7) セキュリティ評価基準の設定

1981 年 7 月国防省はその関連機関の中にComputer Security Center (CSC) を設立した。CSCの主たる目的は国防省内のコンピュータ・システムのセキュリティ機能を評価するものであるが，その一環として，セキュリティの評価基準（Trusted Computer System Evaluation Criterion）案を作成し，民間にもこれを公表することによって，その基準の普及と定着とを図っている。この基準はOS機能を中心としたものであり，8 段階のランク付けが具体的機能との対応によって示されている（付属資料Cを参照のこと）。ただし，この基準に運用上の基準は含まれていない。

1.2.4 セミナー・コンファレンス等の開催

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

1.3　米国におけるセキュリティ技術の現状

米国内で，特に大きな話題となっているセキュリティ関連技術

① アクセス・コントロール

② セキュリティＯＳ

③ 暗　号

について，以下に簡単に紹介する。

1.3.1　アクセス・コントロール

最近の汎用コンピュータにおける標準ＯＳの中には，ファイルやプログラム等に対するリソース・アクセス保護の基本的機能はすべて含まれているが，さらにそれらの保護機能を充実し，管理をやり易くするためのソフトウェア・パッケージが，いくつか商品化されている。現在，利用されている主なパッケージとしては以下のようなものがあり，すべてＩＢＭ社のマシン用のものである。対象ＯＳはＭＶＳが多い。

- RACF（IBM）
- ACF2（Cambridge Systems Group）
- SECURE（Boole and Babbage）
- TOP SECRET（CGA Software Products Group Inc.）
- SAC（EDS）

この種のパッケージの米国における利用状況に関して，以下のような意見があった。

① 正確にはわからないが，約1,000社位のユーザがあるのではないかと見られている。但し，すべてのユーザが充分使いこなしているわけではなく，またその機能に満足しているわけでもないとの意見もある。

② 今回訪問した銀行を含む4つのユーザは，いずれも，何等かのシステムを1つないし2つ利用していた。

- Ａ銀行ではＲＡＣＦで不充分な機能の部分にACF2を使っている。

・ B銀行ではRACFとACF２を比較し，ＩＭＳとの整合性がよりよいという理由でRACFを使用している。

③ 上記の５つのシステムの中では，現在はRACFとACF２が最も普及している様であるが，この２つの思想が対象的である。RACFの原則は非保護で，ユーザが指定したファイルのみが保護の対象となる。一方，ACF２の原則はすべてのファイルが保護対象となり，ユーザは保護方式を必ず指定しなければならない。どちらの思想がより適合しているかは，個々のユーザにより異なるのであろう。

④ セキュリティ機能はユーザの要求に応じて，できるだけオプションであるべきだという意見もあり，その観点からみると，この様なパッケージの形でセキュリティを実現する事は妥当性があろう。

1.3.2 セキュリティOS

(1) 代表的なセキュリティOSの概要

コンピュータ・システムにおけるセキュリティ機能は，OSがその主役的役割を果たすという意見が，研究者の間で多い。そのOSのカーネル(核)に，従来以上の強固なセキュリティ機能（具体的にはアクセス・コントロール機能）を持たせるという研究が，1975年頃からＭＩＴRE社やＵＣＬＡで行なわれてきた。これらはＵＮＩＸをセキュアにするという目標でDEC社のＰＤＰ－11/45や11/70等によって実験された。これらの一連の研究は国防省や軍の関心を引くこととなりThe Air Force Electronic Systems Divisionはこの考えに基づき，よりセキュアなMULＴＩＣＳを開発する事を試みた。現在，この強化MULＴＩＣＳは空軍のデータ・サービス・センタで多重レベルの機密情報の処理に使用されていると言われる。その後，引き続き国防省関連のいくつかのプロジェクトが実施されており，代表的なものとしては以下のようなものがある。

① ＫＳＯＳ－11

KSOSとはKernelized Secure Operating Systemの略であり，PDP－11/70の上でのセキュアUNIXをねらったものである。このプロジェクトは1977年から開始されており，当初フォード社(Ford Aerospace and Communication Corp.,FACC)で研究開発され，後にLogicon社によって完成された。KSOS－11では，UNIXエミュレータが，ユーザのUNIXへのコールを，逐一セキュリティ・カーネルへのコールに変換するという機能を持たせたが，処理効率の悪化という大きな問題を抱えることとなった。

② SCOMP

KSOS－11の改良版とも言われ，ハネウェル社Level 6と呼ぶ小型コンピュータ上にインプリントされているところから，KSOS－6と呼ぶこともある。SCOMPはハネウェル社で開発されており，KSOS－11の処理効率を改善するため，メモリ・マネジメント・ユニットを中心にハードウェア・アーキテクチャ上の改善も施し，結果的にはUNIXとの互換性を捨て，独自のセキュリティOSの構想に基づくものになったと言われる。但し，現在なお未完成と言われる。

③ KVM－370

IBM社のVM－370のセキュア版OSであり，現在SDCで開発されている。

(2) セキュリティOSに対する意見

以上のようなセキュリティOSは，もともと軍の要請によるものであるが，最近では国防省自身もセキュリティOSの民間への普及を望んでいると言われる。そしてそのためには，SCOMPやKVM－370などがそのきっかけとなることが期待されている。但し，メーカの一部では現実にはこれらはまだ完成しておらず，コスト面も含め，民間への浸透はまだ先の事となろうという意見もある。今後の動向としては，セキュリティOSの効率を向上させるために，ハードウェア・アーキテクチャを改善することも考えられている。

1.3.3　暗号化

現在米国における暗号化技術の主流は1973年にその標準アルゴリズムを定めたＤＥＳ（Data Encription Standard)暗号と，ＭＩＴ等によって研究され，1976年に発表された公開鍵暗号（ＲＳＡ暗号）の２つである。

ＤＥＳ暗号は慣用暗号とも呼ばれ，事実上米国の標準暗号となっている。元来，暗号化とはアルゴリズムと暗号鍵との双方を秘密にするという考えに基づくものであったが，そのアルゴリズムを強度の高いものにすれば，それを標準化して公開し，鍵のみをそれぞれの利用場面において各自機密裡に保有すればよいという発想が生まれた。そしてアルゴリズムの標準化によって，暗号装置の低価格化に大きく貢献し得ることとなる。この慣用暗号においては，送受信双方が同一の鍵を持つ必要があり，特に通信相手が多い場合には，機密裡にその鍵を配送する方法が大きな問題であった。

一方，公開鍵暗号は，この鍵の配送問題を解決するため，暗号鍵と復号鍵を別のものとし，暗号鍵を公開可能とし（例えば電話番号簿方式で公開),機密配送を不用とした。そして，その暗号鍵から復号鍵を容易に類推できぬ様な特殊な数学変換方式を用いる。１対ｎあるいはｎ対ｎの通信においては，鍵の配送が不用なこの公開鍵暗号が有利とされている。

現在米国では，ＤＥＳ暗号に関しては，それに準拠する幾つもの商用暗号装置が出現し，実用化レベルにあるが，公開鍵暗号は，処理時間の問題が解決していない。ＬＳＩチップ化や，よりスループットの高い実現法は，研究段階にあり，現在まだ実用レベルにはない。

このような背景の中で，今回の暗号化に関する意見を集約すると，以下の通りである。

①　暗号装置の普及状況

商用の暗号装置の普及は今後の課題であり，暗号装置のメーカにとっては期待はずれの状態にある。

②　暗号化技術の研究

大学，研究機関等においては引き続き暗号化に関する研究が行なわれており，例えば，以下のようなテーマが主流になっている。

- 公開鍵暗号系の実現効率の高いアルゴリズムやそのＬＳＩ化の研究
- 暗号の強度に対する研究
- 暗号技術のより広い応用に関する研究

③　暗号の強度

最近専門家の間では，ＤＥＳ暗号に対する強度が問題になっている。これにはＤＥＳの64ビットの暗号鍵の１部に対し，国防省が何らかの規制を加えているのではないかというような懸念が絡んでいるようである。

④　鍵の管理

慣用暗号における鍵の配布の問題は，現在暗号の実用化を阻む１つの要因となっている。特に多数の支店を持つ銀行などでは問題が多い。これには暗号装置自体に鍵の管理の支援を行なう能力を持たせることも考えられる。また鍵の配布のプロトコルを定めるという動きもある。今後の動向としては，オートマティックな鍵の管理が期待されており，例えば，鍵暗号鍵(Key encript key)の考え方もある。

⑤　暗号は万能ではない

ニューヨークのある銀行で通信の暗号化を実現した結果，すっかり安心してしまい，かえって，セキュリティが低下したという例がある。暗号は万能ではなく，１つの手段である。

⑥　その他の意見

その他，下記のような意見があった。我国で暗号化を導入する時，参考となろう。

- ＥＦＴＳは暗号化なしで実施すべきではない。法的に義務付けることが必要である。
- ＤＥＳは米国以外の国でも標準として考えることは問題があるかも知れない。
- 衛星通信システムの暗号化は今後各国で重要視される様になるだろう。

1.4　米国における新技術の動向

今後研究開発すべき新しいセキュリティ技術に関しては，どの調査先でも同じような指摘があった。その主なものを以下に示す。

(1)　新しい本人確認技術

従来のパスワード中心のＩＤ方式に加えて，さらに積極的な本人の確認のために，例えば，指紋，手形，声紋，目の色等の個人の持つ生理的特徴を使用する方法や，個人の特性をよく表現すると考えられるダイナミック・サインによる方法等が考えられている。これらの方法は既に一部で実現しているものもあるが，大幅な低コスト化が可能な新しい技術の確立が求められている。

(2)　セキュリティＯＳ

コンピュータ・システムのセキュリティを強化するには，まずＯＳに充分なセキュリティ機能を持たせることが必要不可欠となる。

(3)　セキュリティ強化のハードウェア・アーキテクチャ

セキュリティＯＳの実現を容易にし，かつ効率上の問題を基本的に解決するには，究極的にはハードウェア自体の改造が要求される。またさらに将来的動向としては，実用性の高いファイルの暗号化や運用監視の自動化等に対処するため，新しいハードウェア・アーキテクチャ構想が求められる可能性が高い。

(4)　暗号化関連技術の進展とオーセンティケーション

暗号化に関しては，

- 暗号キーの管理の自動化
- 高位プロトコルと暗号化の統合による暗号の階層化やEnd-to-End 暗号技術の強化
- 公開鍵暗号系の実用化

などが期待されるとともに，特に公衆網における不正な介入を防止したり，重要なメッセージの通信確認を強化するための通信相手確認方式の実用化が求められる。

(5) 衛星通信のセキュリティ

今後衛星通信の拡大利用に備えて，国際通信を含むセキュリティ機能を強化することが必要となる。

(6) ソフトウェアの検証

前述の米国防省が定めたセキュリティ基準の最高位はソフトウェアの検証の実現である。システム監査の立場から言っても，プログラムの第3者による検証は大きな悲願であり，またソフトウェア工学の立場からも重要課題の1つである。

1.5　その他

米国では一般的にセキュリティ対策が進んでいると考えられている。しかしながら，細かく調べて行くと必ずしもすべての面で，我国より進んでいるわけでない。バンキング・システム（金融機関システム）では，むしろ我国の方が進んでいる場合もある。技術の導入も，民間企業ではそれ程活発ではない。セキュリティは高価なものであるとの認識は，洋の東西を問わないが，ある意味では我国以上にシビアな米国のユーザのコスト感覚の故か，その長い歴史や関心の深さにもかかわらず，セキュリティ対策の具体化に対する躊躇の傾向は今なお強い。

我国では，ことセキュリティ問題に関する限り，技術的問題の優先度は低いという意見が一般的である。すなわち，先ず人間の問題であり，次いで制度や運用の問題，そして最後が技術であると言う。今回の調査でも，特に応用システムでは，同じような意見が多かった。しかし，技術を軽視しているわけではなさそうで，いかに高度な文明でも，それをコントロールするのは人間である，という発想から，人間中心のセキュリティ対策が多いように思われた。従って，効果的な支援技術があれば，すぐに導入されると考えることが可能であり，現実には，米国でも効果的セキュリティ支援技術が少ないのだと結論することもできる。

いずれにしても，セキュリティ問題はもはや一企業の問題ではなく，社会的対応が求められる課題であり，広くコンセンサスの得られるセキュリティ基準あるいは法制度上の措置などの重要性が強く認識された。

2. 第9回コンピュータ・セキュリティ・コンファレンス

(Ninth Annual Computer Security Conference)

開催期日：1982年11月8日～10日

場　　所：ニューヨーク（New York Statler Hotel）

主　　催：Computer Security Institue

2.1 会議のアウトライン

本会議は，米国で行なわれているいくつかのセキュリティ関連の会議の中では最大規模のものであり，その対象は，民・官・軍にわたる管理者から技術者までの広い範囲をカバーしている。内容もセキュリティ全般にわたる管理・運用，技術，法制度等の諸問題を含み，またシステム監査に係わる項目も討議対象となる。

毎年一回開催され，今回は第9回，すなわち9年目に当たる。毎回米国全土から多くの参加者を集め，今回は約750名が参加し，盛況であった。参加者の内訳は，州政府，国防省および軍を含む政府関係者が約1/3，銀行・保険等金融機関を中心とするユーザ企業の関係者が約1／3，情報産業やコンピュータ・セキュリティ関連の各種メーカ，サプライヤ，シンクタンク等の関係者が約1／3と，多彩な顔ぶれである。また職務的にも経営者，管理者，法律担当者，監査担当者，企画担当者，技術者，情報処理システム担当者等セキュリティに関わりのあるすべての職域に広がっている。また米国における他の会議と同様に，この会議も海外にオープンされており，カナダ，メキシコ等の近隣諸国からの参加が若干あったようである。なお参加者リストを見た限りでは日本からの出席は他に見当らなかった。会議の内容としては，以下のような催しがあった。

① 全体会議（General Session）

参加者全員を対象とするもので，今回は，

- 基調講演…… 1件

- 招待講演……2件
- 一般講演……7件
- パネル討論……1件

であった。

② ワークショップ（Workshop）

48のテーマに分かれ，いくつかの会場で並行して行なわれた。登録申込時に各人が参加を希望するテーマを4つ選び，それに基づき，場所やスケジュールが設定されている。

③ 展示会

41社が出展し，セキュリティ関連のハードウェア，ソフトウェア，関連ドキュメント等を展示し，説明していた。

④ その他

会期の前後2日にわたり，6人の講師による任意参加のセミナー（Optional Seminar）が行なわれた。その他特に事前にスケジュールされていないＳＩＧ（Special Interest Group）の会合もあり，また3日間毎日の全員参加の昼食会もスケジュールの一環であり，最終日にはこの席でも講演が1つ行なわれた。

今回が9回目という歴史と経験によるものかも知れないが，全体として，運用上もかなりよく配慮された，実質的かつ内容豊富な会議であった。なお，この会議を主催しているComputer Security Institute（ＣＳＩ）は，1974年に設立され，ボストンに本拠を置くメンバ制の機関である。毎年開催するこのコンファレンスが主要事業の1つであるが，その他適宜セミナーやワークショップを開催すると共に，セキュリティに関する定期刊行物，製品紹介，月刊のニュース・レター等を発行している。また企業や個人のセキュリティ対策のコンサルタント的業務も行なっている。

2.2 会議内容

2.2.1 全体会議（General Session）

3日間にわたり，以下のようなテーマと講師によるセッションが行なわれた。

(1) 基調講演

Managing Our Information：The Key to Increased Productivity

（Robert F. Santos, AT & T）

① 要 旨

情報処理と通信の融合，情報というものの価値の増大，パーソナル・コンピュータの普及，コンピュータ・システムへの社会の依存度の増大，システムの脆弱性やコンピュータの悪用，不正によるトラブルの増大，プライバシ保護，システム信頼性，法制化等に対する社会的要請の増大等により，従来からの物理的セキュリティに重点を置いた対策では不充分になった。システム・アプローチの観点からすれば，セキュリティ機能は言わば，システムの基本的機能の1つであり，「セキュリティは生産性向上のトータルな施策に対しても大きく貢献するものである。」という考え方が望まれる。また併せて，

- セキュリティに対する責任体制の確立
- リスク・マネージメント
- 人事面のコミュニケーションの強化と教育の充実

等にも重点を置くべきである。

② 講 師

R.F. Santos はAT & Tのデータ・システム担当の副社長である。

(2) 招待講演

① National Security Needs and Responses

（Admiral Bobbie R. Inman）

ⓐ 要　旨

国家防衛システムの中枢は，エレクトロニクス技術を駆使した高度の情報処理システムである。最新技術の活用は，それに伴う信頼性，安全性への要求も増大し，物理的セキュリティに比べ，コンピュータ・システムのセキュリティは極めて高価となる。大量のデータベースや通信システムのセキュリティは，現在実現可能な最先端技術でプロテクトされているが，それでもなお，更に新しい高度の防衛技術への需要は無限である。システムの特色としては下記のものがある。

・　各種画像情報のコンピュータ処理の比重が高いため，一層の技術的改善が要求されている。

・　通信のセキュリティ，特に衛星通信のセキュリティの強化は重要課題でありやや長期的テーマとして解決されることとなろう。

・　スペース・シャトルに関するセキュリティも新たな課題である。

ⓑ 講　師

Admiral Inmanは 1981 年 6 月に退役した米国初の情報専門家としての海軍大将と言われる。その経歴は，海軍情報部，国防省情報局の副長官，国家安全保障機構（National Security Agency)の長官，ＣＩＡ 副長官等を歴任している。最近日本の新聞にも報道されたように現在は MCC（Microelectronics and Computer Technology）社の最高経営責任者である。MCC社はCDC社，DEC社，ハネウエル社，UNIVAC社等を始めとするコンピュータ，半導体，エレクトロニクス関連企業等，約30社のメーカが参加するスーパ・コンピュータ共同開発プロジェクトの中核となる新会社で，このコンピュータは日本の第５世代コンピュータに対抗するものと言われている。

② Management for the 80's : Theory Z and Beyond

(Reverend Thomas A. McGrath, S. J. Fairfield University)

ⓐ 要　旨

60年代・70年代を通して,米国は文化革命とも言うべき激動時代を経過してきた。そこでは人間性への自覚，市民の権利，少数民族，女性の権利，労働問題，犯罪等々の諸問題に直面せざるを得なかった。このような変化は，また人間のマネージメントの変化を余儀なくさせる。80年代のマネージメントは，過去の経験の踏襲から脱した新しいものでなければならない。企業における生産性も製品の質の向上も，マネージャの正しい従業員管理の理念とその実行力にかかっている。例えば，個人の文化的，教育的，社会的，人種的背景をふまえた権威，忠誠心，規律等への考え方の変化を理解し，人間間の信頼感に基づくコミュニケーションの促進により，意見や思考を引き出し，社会的，知的，精神的ストレスからの解放をはかること等が要求される。80年代は人間のマネージメントが極めて重大な影響を及ぼす時代と言えよう。

ⓑ 講　師

Reverend （聖域にある人への尊称）McGrathは現在Fairfield大学の心理学の教授である。多くの大企業のマネージメント問題のコンサルタントとして17年の経歴を持っており，心理学者であるとともに，人間のマネージメント問題の権威者である。

(3) 一般講演

① Recovery from a Total Loss : The Parnell Precision Products Case Histoy

（Tim Hill, Parnell Precision Product, Inc.）

採鉱，建設，運輸業等で使用する各種の金属性機械を製造している上記の会社の工場が大火に会い，その復旧の経過を通じての経験から，この種の企業におけるセキュリティ計画につき，意見をまとめたものである。

② Software Management, Hazards &Countermeasures

（Maurice E. Scherer, Jr. Bi-Hex Co.）

従来ソフトウエアは他の工学に比べ，セキュリティというものに対する配慮が不充分であったが，ソフトウエアの障害や安全性への対応等を求める社会的要請が強くなったという背景から，ソフトウエア自身，ソフトウエア作成者，ソフトウエア利用者等，種々の立場でのセキュリティ上のマネージメントにつき，まとめたものである。例えば，企業におけるソフトウエア・セキュリティの専門担当者の必要性などにもふれた。また自動化の度合と特化性（Customization）の度合に対する安全性は図２－１のように考えられ，ソフトウエアに関してもこれはあてはまるとのことである。

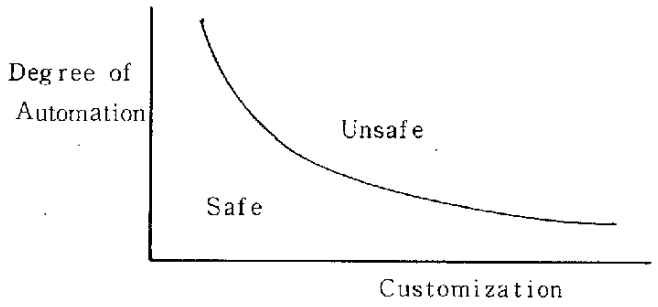


図２－１　自動化率と安全性の関係

③　Security Aspects of Distributed Systems

（William A.J.Bound,DOD Computer Institute）

分散処理システムのセキュリティ上配慮すべき技術的，管理的問題をまとめたものである。分散処理システムでは集中型に比べ，リソースが分散することのセキュリティ上の利点があるが，一方構成要素が多様化，複雑化し，分散型データベースを始めとするシステムの高度化による新たなセキュリティ問題も発生する。例えば，

- ネットワーク化による通信回線上の脅威の増大
- インテリジェント端末のセキュリティ機能の不備とセキュリティ・ポリシィの欠如
- 分散型データベースのセキュリティ機能の検討が不充分

- 本人確認，アクセスに対するＩＤ管理等の一層の充実が要求される。
- システム監査の充実が要求される。
- 公共的システムにおいては法制度上の整備も必要
- コンピュータ・システム，ネットワーク，端末関連システム等，それぞれにセキュリティ・オフィサが存在すべきである。

等の問題がある。また分散処理システムには図２－２に示す“Safeguards Diamond”とも言うべき４次元のポリシィを確立する事が望ましい。

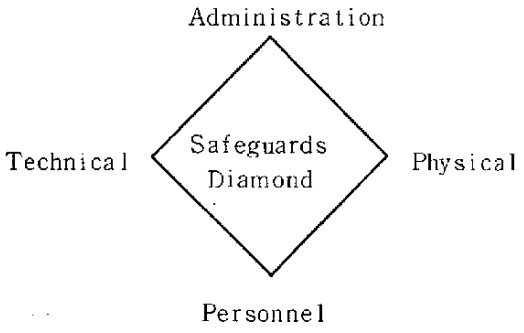


図２－２　Safeguards Diamond

④ The Realities of Netwok Security：Problems & Opportunities

（Peter S. Browne, Burns International Security Services,Inc.）

ネットワーク・システムのセキュリティ上から見た特性，およびその保護のための手段として，

- 端末同士および端末とシステム間の正当性確認
- データおよびソフトウェアの暗号化
- オーセンティケーション（デジタル署名，端末，発信者メッセージ等それぞれに対する確認）
- キーの管理（その発生，配布，記憶，使用および物理的保護,Key-encripting-key 等）
- 監査証跡の確保

等につき，説明と見解を述べたものである。なお図２－３はデジタル署名を使用するシステムのイメージである。

⑤ Computer Crime : Where we're at & Where we're going

（Michael G. Wilson, Federal Bureau of Investigation）

講師はＦＢＩのホワイト・カラーのコンピュータ犯罪捜査チームの責任者

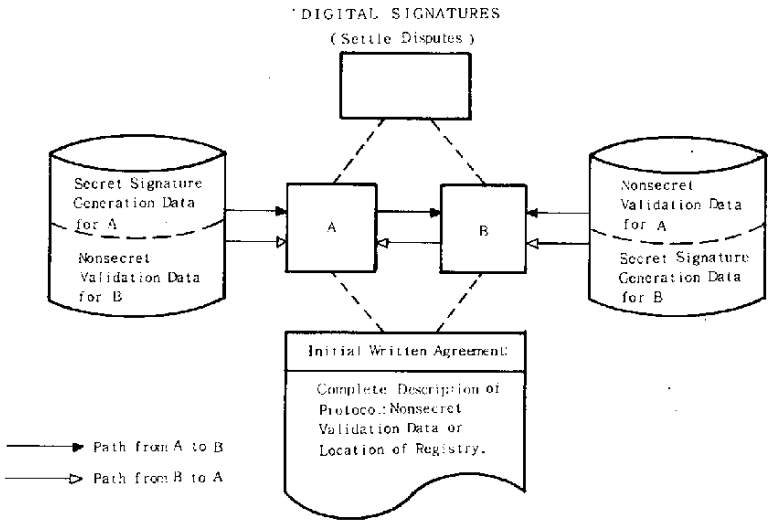


図２－３　デジタル署名を応用したシステムの概念

であり，その専門の立場から，コンピュータ犯罪の現状や将来につき，見解を述べたものである。また 1977 年に米国で設定された Computer Systems Security ACT や 1981 年の Federal Computer Systems Protection ACT 等についての説明もあった。彼の見解によれば，コンピュータ犯罪の防御には，

- すぐれたセキュリティおよびコントロール・システムの存在
- そのシステムの厳格な運用

が必要不可欠である。最近のある１年間のＦＢＩの統計によれば，コンピュータ関連の犯罪は金額的には全ホワイト・カラー犯罪の１％に満たないが，これは発覚したもののみであり，人間がおり，コンピュータが存在し

続ける限り，将来とも多様な犯罪が発生し続けるであろうとのことであった。

⑥ Security in Future Appliations and Environments

（William H. Murray, IBM Corporation）

講師はＩBM社のセキュリティ専門の担当者であり，将来の種々のシステム環境におけるセキュリティ上の危険とその対応策についての分析があり，下記のような対策が示された。

ⓐ 自動化（電子化）オフィスにおける対策

- 自動索引
- 細かいアクセス・コントロール
- 自動ロギング
- 自動バックアップとリカバリ
- 安定したハードウェアとソフトウェア
- 排他的なデータの更新

ⓑ 電子ドキュメント配布（電子メイル）における対策

- クラシフィケーションの明確化
- シークレット・コードの利用
- オーセンティケーション
- 監査トレール
- ディレクトリのコントロール
- 自然語の利用
- 機密文書であることを表記しない

ⓒ 公共システムにおける対策

- レパートリの制限
- 独立したテスト
- 相手関係の明確化と相互確認
- 変更に制約を与える

- 厳格なロギング
- シークレット・コードの利用

ⓓ パーソナル・コンピューティングにおける対策

- ユーザ資源相互の分離
- 責任と義務の明確化

ⓔ ハイブリッド・システムあるいは分散アプリケーション（異業種／異企業間システムやメディア混合システム）における対策

- 利害関係の相反するユーザ同志のシステムであることを確認し設計する
- ハイレベル・プロトコルのみを公開し利用させる
- データ処理手続きを厳格に分離する
- 自然語の利用
- 自動的な障害の分離機能
- コントロールと自由度に伴う責任と義務の明確化

⑦ Baseline Controls : Strengths, Weaknesses, & Practical Use

（Donn B. Parker, SRI International）

ベースライン・コントロールとは，各種のインフォメーション・システムに共通的なセキュリティ・コントロールの基本的セットであり，図2－4のコンポーネントを持つ。

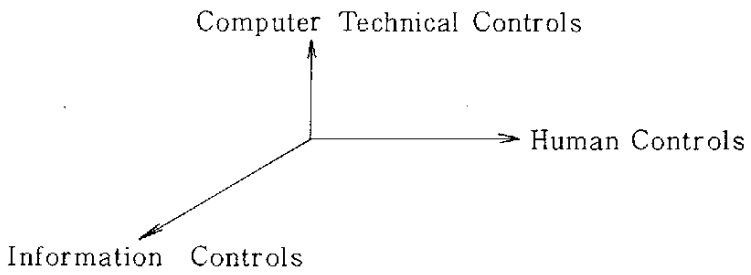


図2－4　ベースライン・コントロールのコンポーネント

ここでのインフォメーション・システムには，従来のEDPシステムに加え，EM，OA，デジタル・テレフォン等のニューメディアもすべて含

む。ベースライン・コントロールの要点は以下のようなもので，人間管理に重点が置かれている。

- インフォメーション・セキュリティ・ポリシィの確立
- 従業員の採用と解雇の手続き
- 従業員のバック・グラウンドの調査
- 従業員のセキュリティ行動の評価
- セキュリティ上のルールや基準書の作成
- 情報提供担当者を定める
- 権限分担，二重制御，ジョブ・ローテーション等，セキュリティ面からの業務担当の決定

2.2.2 ワークショップ（Workshop）

48件のテーマ別のワークショップが3日間にわたり並行的に行なわれた。各々1時間15分ずつのスケジュールで，それぞれ座長がおり，レクチャー方式に近いものもあるが，多くは質疑応答や対話の要素をかなり盛り込み，同一テーマに興味を持つもの同志の，突っ込んだ具体的討議の場を意図したものである。事前の登録時に1人4テーマずつの参加申し込みを行ない，それに基づき，個人毎にスケジュールされている。このワークショップ方式が本コンファレンスの特色の一つでもあるらしく，また毎年好評を得ているアクティビティの由でもある。

今回のテーマの一覧を付属資料Aに示す。なお，各テーマ座長には，国防省，NBS，自治体等公的機関の人々を含め，メーカ，金融，保険関連企業，一般ユーザ，セキュリティ関連機関，シンクタンク，ソフトウェア企業等，多彩な顔ぶれであった。

2.2.3 展示会

会議に並行してセキュリティ製品の展示会が行なわれ，41社からの出展があ

った。主な展示品には以下のようなものがあり多彩であった。

- 暗号化機器
- 物理的セキュリティ機器
- 端末関連セキュリティ機器（アクセス制御用機器，金融機関用端末）
- 本人確認用機器（ダイナミック・サイン，手形識別機器等）
- セキュリティ関連ソフトウェア（アクセス制御用，DBMS用等）
- システム監査ツール（レポート・ジェネレータ，データ収集分析ツール等）
- セキュリティ・サービス

3. The Chase Manhattan Bank

3.1 調査目的

チェース・マンハッタン銀行（The Chase Manhattan Bank）は，米国の代表的な銀行の一つであり，コンピュータ・セキュリティについても，EFTSにおけるメッセージ認証装置の開発，導入等，積極的に取組んでいる銀行の一つである。今回の訪問の目的は，現システムにおけるセキュリティ機能と，今後の検討課題等についての意見を聞くことにあった。

3.2 セキュリティについて

(1) 現在の技術的セキュリティ対策

図3－1に示すようなシステム構成となっており，下記のようなセキュリティ対策が実施されている。

① 通信回線上のデータについては暗号化（DES）している。

② データベース（DB）のアクセス・コントロールについては，RACFとACF2の2つのパッケージを併用している。

③ ファイル上のパスワード原簿は，一部暗号化している。

④ ターミナル・パスワードについては，機能別に設定している。

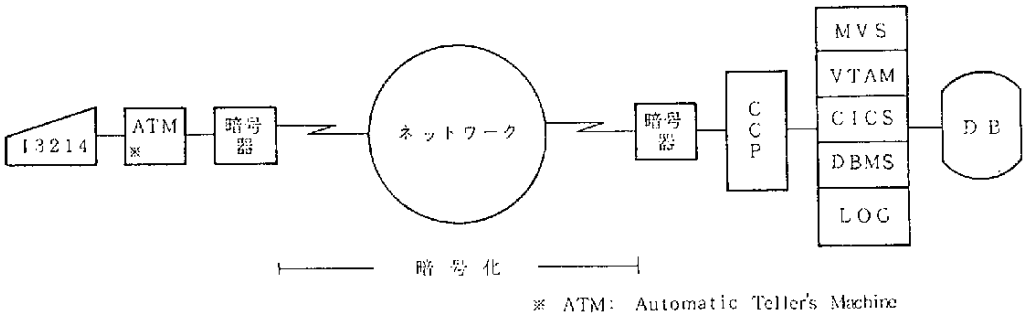


図3－1 システム構成

(2) 現在の運用上の対策

図3－2にプログラムのメンテナンス手順を示す。テスト・ファイル，プ

ロダクション・ファイル共にパスワードによる保護が行なわれている。従って，権限外の者がプログラムを変更することはできない。

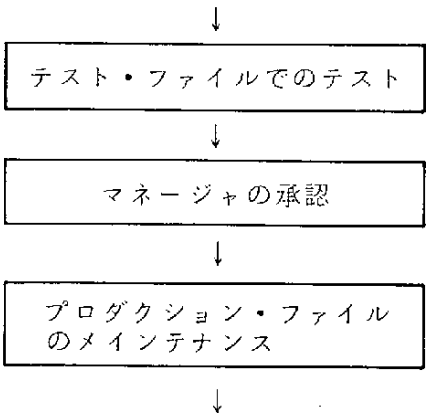


図３－２　プログラムのメインテナンス手順

(3)　今後の対策強化の予定

今後，下記のような対策強化を計画しており，順次実施して行く予定である。

①　パスワードのマスク化

②　アクセス・コントロール（本人確認を含む）の強化

- 指紋による本人確認

  ——現在，内部で試行しているが，認識／登録に時間がかかる問題がある。（登録約20分）

- Signature（サイン）による本人確認

  ——顧客向として検討している。

3.3　システム監査について

(1)　概　要

プログラムの監査については，以前はシステム完成後にチェックしていた。今回，新システム構築を機会に，システム開発段階からカスタマを含めてレビューを行ない，システム監査を行なった。

(2) システム監査支援ツール

システム監査支援ツールとしてオーディタ（Auditor）を使用したが，これは機能的には不充分なものであった。例えば，ファイル等のチェックでは問題ないが，オンラインのチェックには使用できない。当行のオンライン・システムにおけるシステム監査の概念を，図３－３に示す。

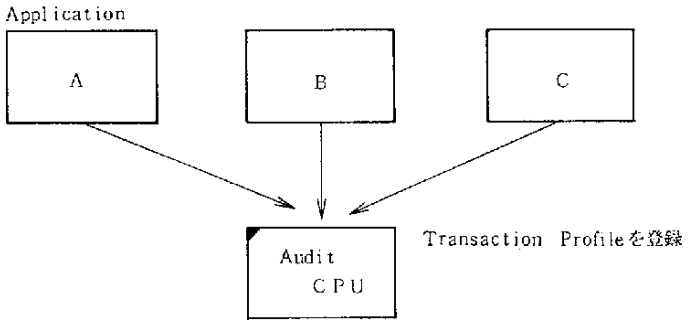


図３－３　オンライン・システムでのシステム監査の概念

3.4　メッセージ認証システムについて

米国規格協会（ＡＮＳＩ）やＩＳＯでは，認証方式の標準化が進んでおり，チェース・マンハッタン銀行では，その標準方式を取り入れたメッセージ認証装置を自社で開発し，導入を行なっている。これは，メッセージの正当性を検証するもので，金融機関における端末からホストへの通信等に向いた方式である。

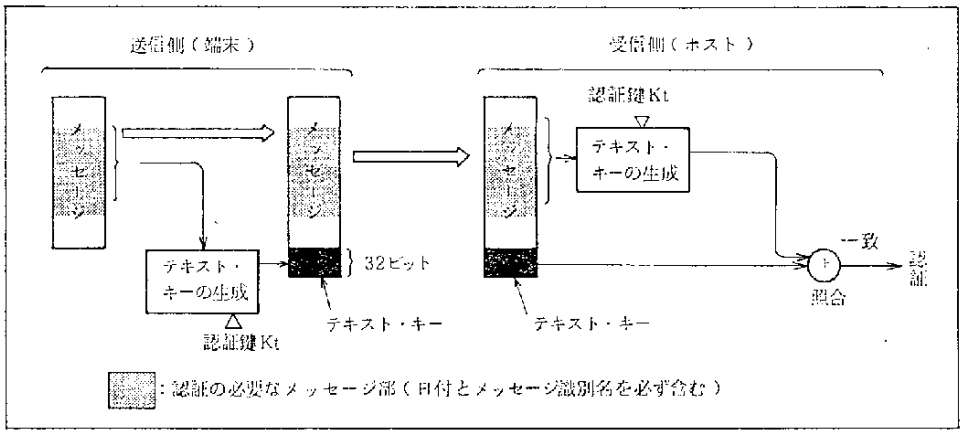
(1) 認証方式の概要（図３－４参照）

① 送信側は，認証の対象となるメッセージを基に，テキスト・キーを作成し，メッセージにそのテキスト・キーを付加して送信する。

② 受信側は，受信メッセージを基に，同じようにテキスト・キーを作成し，それと受信したテキスト・キーを照合する。

③ 照合の結果，一致すれば，受信メッセージは正当と見なす方式である。認証の対象となるメッセージには，日付，メッセージおよび識別名を必ず含むようにしている。

④ テキスト・キーの生成には，ＤＥＳ方式の暗号器を使用している。



標準認証方式，認証の対象となるメッセージからテキスト・キーを作り，メッセージに付けて送る。受信側では同じようにしてテキスト・キーを作り，それと送られてきたテキスト・キーとを比較し，一致していればメッセージに改ざんや誤りがなかったものとみる。

図３－４　標準認証方式（出典：日経エレクトロニクス 1982.10.11 ）

3.5　その他

(1)　集中と分散

今後，コンピュータ・システムは分散化の方向へ向うと考えられる。分散システムの長所は，責任の分担と明確化であり，短所は，セキュリティ・システムに一貫性がなくなることである。そのため，コンピュータ・システムにSecurity Standard（すなわちセキュリティ・ガイドライン）を導入することが重要になる。

(2)　新技術

新しいセキュリティ技術は，Production（製品）ではなくTechnology（応用技術）の形で供給されることを望む。また，すべてのバンキング・システムを同一レベル（内部）にする必要がある。

(3)　投資コスト

図３－５に示すように，セキュリティ機能を強化することにより，生産性は低下する。

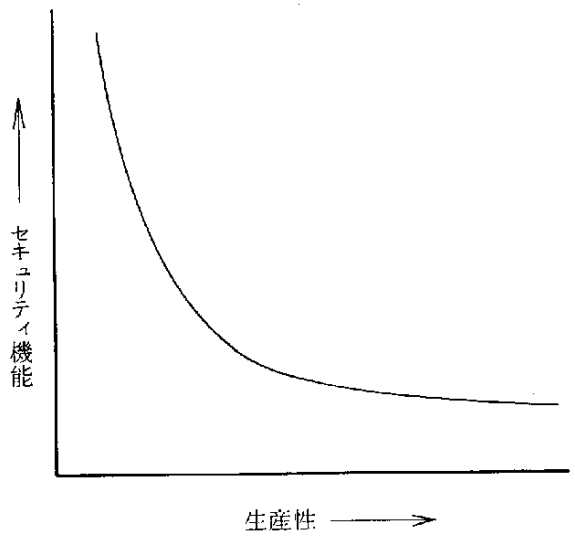


図３－５　セキュリティ機能と生産性の関係

4. Technology Analysis Group (Mr. Patrick F. Sullivan)

4.1 調査目的

テクノロジー・アナリシス・グループ(Technology Analysis Group, 以下テクノロジー社と略す) は, コンピュータ設置状況の調査, ユーザの動向, メーカの動向等の調査から, 各種の予測等も行なう調査会社である。コンピュータ・セキュリティを含む広い分野で調査活動を行なっている。

既に周知のように, IBM社では, 1960年代後半から1970年にかけて, 多額の投資を行なってコンピュータ・セキュリティの研究を行なった。しかしながら, その成果はあまり公表されていない。見るべき成果がなかったからだという説もある。テクノロジー社の代表であるSullivan専務 (Mr.Patrick F. Sullivan) は, かつてIBM社に勤務し, 製品企画部でセキュリティの研究に従事したとのことである。その時以来セキュリティに関して, 興味を持っているという。コンピュータ・セキュリティに関する米国での動向について, 率直な意見を聞くため訪問した。さらに, かってのIBM社の研究に対する評価等についても意見交換を行なうことができた。

4.2 コンピュータ・システムの危険性について

いろいろな意味で, 重要なデータが増大しており (日本では情報化社会という), これが, コンピュータ・システムの危険性を増幅している。ただし, コンピュータが犯罪を行なうのではなく, コンピュータを利用した犯罪が発生していることを認識しなければならない。ある種の統計では, 5億ドル/年の損失があると言われる。これは, 発覚した損失で, 実際には全体の90%が発覚せずに (すなわち, 完全犯罪) 犯罪者の利益になっていると言われている。それでも, エラーあるいはミス等による損失に比べれば, それ程大きい額ではない。このような損失の統計では, しばしば事故による損失が無視されている場合もある。コンピュータ・システムの損失比率は, 次のようになっている。

① エラーあるいはミスによる損失…… 50 %

② 不誠実な従業員による損失…… 15 %

③ 火事による損失…… 10 %

④ 不満をもった従業員による損失…… 7 %

⑤ 水害による損失…… 7 %

⑥ その他…… 11 %

②と④が，いわゆるコンピュータ犯罪と考えることが可能だろう。この統計を見る限り，コンピュータ犯罪の防止と共に，エラーやミスの防止も重要だと言うことになる。

4.3 コンピュータ犯罪に対する認識

コンピュータ犯罪に対して，米国では誤まった概念がいくつかある。この誤まった概念が，コンピュータを導入することにより犯罪が増加するという誤まった認識を生む。実際には，コンピュータ導入により安全性が強化されるか，もしくは安全性の強化が可能なのである。もちろん，しかるべき対策を行なえばの話である。その誤まった概念を紹介しておく。

(1) コンピュータ犯罪としてホワイト・カラー犯罪が増加したと言われているが，コンピュータ導入により犯罪発見率が高くなり，見かけの数字が大きくなったと解釈すべきである。

(2) コンピュータ犯罪では，高度のテクニックが駆使されていると言われるが，実際の犯罪では，高度のテクニックは不要である。従って，ホワイト・カラーの専売特許ではない。

(3) エクィティ・ファンディング事件では，コンピュータを用いてニセの保険証書を大量生産したと言われているが，実際にコンピュータを用いて作成したのは，ニセ書類全体の20%だった。すなわち，不正に対するコンピュータの寄与率は，想像よりずっと少なかったことになる。

(4) コンピュータ犯罪を防止するのは不可能であるという意見が多い。確かに

100％防止するのは無理だが，ある程度防止することは可能であるし，重要なデータを犯罪から保護することは可能だ。

4.4　データの保護

情報は次の３つに分類する。すなわち，①個人情報，②科学技術情報，③企業情報である。これらの情報は，事故あるいは故意の事故（犯罪）から保護しなければならない。

米国では1974年に，データ保護のために政府が為すべき義務を法律で定めた。しかしながら，民間におけるデータ保護を定める法律（いわゆるプライバシ法）の制定には失敗した。従って，例えば病院（患者個人の情報，病歴等）やＩＢＭ社等が持っている情報（企業秘密)を公開させることは可能である。多くの企業では，社内規定で対応しているのが現状である。現在，大きな問題は起きていないようだ。ヨーロッパでは11カ国で，プライバシ法やデータ保護法が制定されている。ただし，規定だけで，規定を守るための方法は明記されていない。

4.5　セキュリティ対策の方針

米国では，最初にコンピュータ・システムに対策が必要だと警告したのは，メーカではハネウエル社である。ＩＢＭ社では，1973年11月15日付のCorporate Policy No. 130で「データ・セキュリティ」への対応方針を発表している。ここで示されたＩＢＭ社の基本方針は,「データ保護はユーザの責任であり，メーカは，ツールの供給とアドバイスを行なう。」というものであった。これは，その後，大きな問題を提起した。ＩＢＭ社の主張は，メーカの責任範囲を明確にしたものだが，ユーザに納入された自社製品が関係した事故あるいは犯罪は，責任範囲外だとしたのである。

車の運転手が事故を起こしても，車のメーカには責任がないのと同様である。ただし，車に構造上の欠陥があれば，メーカの責任が問われることがある。―

方，コンピュータの構造上の欠陥とは何であろうか。コンピュータは構造（電子回路として）も複雑であるし，そのうえソフトウェア（プログラム）という捕えどころのないものを内蔵している。事故が起きても構造上の欠陥が原因かどうか，判断が大変難かしい。

このような条件の中で，ＩＢＭ社は一方的にメーカには責任がないとしたのである。この背景として，ユーザでの事故発生のたびに，いちいち責任問題について検討していては，経営が成り立たないという問題があったと言われる。逆に言えば，事態はそこまで切迫しているとも言える。米国のメーカが，みなこの方針を支持しているわけではない。自社の製品の信頼性については，ユーザ納入後も責任を持つべきだという意見もある。

4.6　セキュリティ関連技術

ＩＢＭ社は，セキュリティ対策のためのツールを提供するとの方針に基き，いくつかの基本的ツールを提供している。それは，

① Identification（本人確認）and Authentication（相手確認）

② Authorization（アクセス権限）and Access Control（アクセス・コントロール）

③ 暗　号

④ システム・ロギング情報

⑤ System Integrity（システムの完全性）

である。④のロギング・データは，特に重要なもので，セキュリティ対策の決め手に近いものである。これらは，図４－１に示すシステム形態を想定して構築された基本的ツールだと考えられる。

これらの基本機能は，常にシステムに備わっている必要があるかと言うと，そうではなく，ニーズに応じて必要なものだけが，システムに取り入れられていれば，商用システムのセキュリティ対策は十分である。そのため，セキュリティ・ツールは，オプションでなければならない。ＩＢＭ社の開発商品は，多

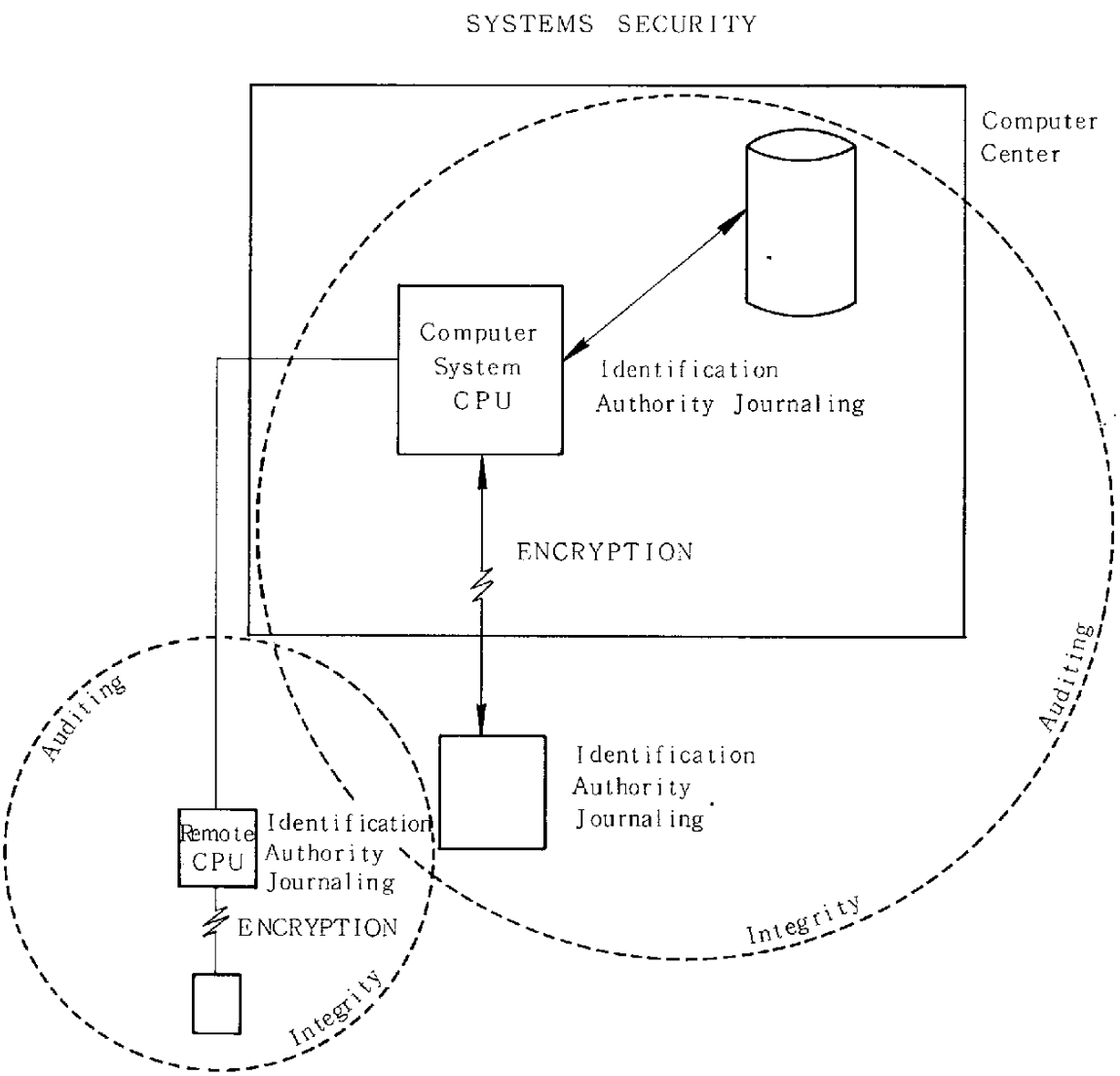


図４－１　システム・セキュリティ

（出典：IBM Corporate Policy Number 130 November 15, 1973.）

少の不満はあるものの，商用システムのニーズを満たしている。従って，現在のツールでも必要な対策は可能だ。もちろん100％安全なシステムは，現在構築できない。そのようなシステムの実現は，かなり先のことであろう。

4.7　今後の課題

技術的課題としては，例えば，指紋による本人確認がある。また暗号方式の統一問題等もある。指紋による本人確認では，技術よりもコストが問題である。近い将来解決すると思う。暗号方式は，DES方式に統一されつつある。キー長の変更等が議論される可能性はある。重要なのは，予想される損失とのバランスを考慮して，セキュリティ対策の投資額を決定することである。軍用システムのような，できる限りの対策を行なうという考え方は，商用システムでは適用できない。従って，当然軍用システムと商用システムでは使用するツールも異なる。MULTICSが商用システムに使用されないのは，この理由による。

4.8　その他

Sullivan専務の考え方は，米国の一方の意見を代表している。この一方の意見とは，現在の技術を用い，運用の見直しを行なえば，セキュリティ対策は十分可能だという意見である。そして，セキュリティ問題を必要以上に誇張せず冷静に対応すべきだという意見でもある。米国の大部分は，この意見を支持している。これに対して，軍の関係者や研究者を中心にして，事態はもっと深刻で今すぐ新技術を開発する必要があるし，セキュリティ対策にもっと投資すべきだという意見がある。ただし，こういう人達の開発目標が，いわゆるセキュリティOSに片寄っているのが興味ぶかい。

商用システムと軍用システムでは，セキュリティ対策に対する考え方が基本的に違っているようだ。

5. American Express Company

5.1 調査目的

アメリカン・エクスプレスは日本でも「GOLD CARD」で知られているが，業務内容は損害保険，生命保険，社会保険，証券，不動産，クレジット，金融，貿易，商社，そして通信をサービスする，いわゆる情報を商品としている企業である。この会社は

① American Express Company

② Fireman's Fund Insurance Companies

③ American Express Travel Related Services Company,Inc.

④ American Express International Banking Corporation

⑤ Shearson / American Express Inc.

の５つの独立した事業体から構成され，American Express Company の総括のもとで

- 保　険
- 旅行運輸
- 金　融
- 投　資

に関する業務を営んでいる。

今回応対していただいた方は，企画担当のJohn C. Schneider氏，およびシステム担当のVincent Di Tursi氏である。

5.2 セキュリティに対する取り組み

この会社にとって情報は命であるだけに，セキュリティ対策については良く体系づけて真剣に取り組んでいる。特に，セキュリティ対策を設定したセキュリティ・ガイドラインは，外部のコンサルタントを使って評価してもらったこと，ニューヨーク市内にある施設を他に移すことも考えているとのことである。

5.3　アメリカン・エクスプレスのセキュリティの説明と質疑

説明は，アメリカン・エクスプレスのセキュリティ・ガイドラインに沿って行なわれた。ガイドラインは，以下の様な項目から成っている。

(1) セキュリティの重要性

(2) 法的な関連

(3) セキュリティと技術の関連

(4) 脅威は何か

(5) 守るべきリソースと，脅威，及び保護の関係は何か

(6) セキュリティの方向性

(7) セキュリティの範囲

(8) セキュリティの階層的方向性

① セキュリティに関するデータの収集

- 守るべきリソースの確認
- 脅　威
- 現在の対策
- 発生しそうな脅威の検討
- 有効なセキュリティ対策の検討

② セキュリティに関するデータの分析と対策の選択

- セキュリティの分析評価
- セキュリティのグルーピング
- 弱点を補う方法の確認
- 危険性の程度
- セキュリティ対策の可能性
- セキュリティ対策の評価
- セキュリティ対策の選択

③ コスト面の評価.

- 対策を講じない時のコスト

- 経営面
- 顧　客
- 訴訟（個人，政府）
- イメージダウン
- 対策に必要なコスト

④　セキュリティ対策の要求のまとめ

- 対策の見きわめ
- 対策のまとめ
- 有効性のレビュー
- 対策実現のためのレポート

⑤　セキュリティの段階的指針

- 現セキュリティ・レベルの承認
- 十分な議論とドキュメント化
- ドキュメントの更新
- 確実なレビューと承認

(9)　作業手順の承認

(10)　責任分担の明確化

このような経過を経て，ガイドラインを設定し，同社のセキュリティ対策を実現しているとのことである。

5.4　その他

訪問の時間的関係もあり，細かな質疑は行なえなかったが，アメリカン・エクスプレスのセキュリティ対策は，新しい技術を使って実現するというよりは，むしろ組織面，および管理面での充実に重きを置いたものであった。ただ具体的な技術問題として，現在 ACF 2を使用しているが，メーカによるオンライン保守は ACF 2を通さないため，すべてのファイルにアクセスできてしまうのが大きな問題であるとのことであった。

6. The City of New York Department of Investigation

6.1 調査目的

New York City Department of Investigation(以下,ニューヨーク調査局と呼ぶ)は，ニューヨーク市当局の一機関であるが，下記のような業務を行なっており日本の自治体には見られない，ユニークな機関である。

① ニューヨーク市職員の犯罪行為のチェック

② ニューヨーク市財務の不正のチェック（横領，使い込み等）

③ 行政執行上の不正行為のチェック

④ 行政執行上の間違い，あるいは汚職の摘発

ニューヨーク調査局は，不正を発見すれば，犯人を告訴する。その意味で，日本の会計検査院と警察の両方の機能を持っていると言えよう。ただし，捜査対象はあくまでもニューヨーク市職員に限られ，不正といってもニューヨーク市が関係する不正だけが捜査対象となる。地方自治が高度に発達している米国ならではの組織である。

ニューヨーク調査局には，およそ15人の捜査主幹および35人の捜査官がいる。そして，捜査対象は，ニューヨーク市当局のすべての部署に及ぶ。米国は，コンピュータの先進国であり，自治体にも多数のコンピュータが導入され，税業務の効率化，福祉業務の効率化等に役立っており，今後もシステム化はさらに進むものと思われる。しかしながら，このコンピュータを利用した犯罪が早くも発生しており，ニューヨーク調査局でもその対策に追われている。今回訪問したMoulton *1局長（Mr. Rolf Moulton)は，コンピュータ犯罪の防止に大変積極的であり，また，かねがねコンピュータ犯罪の危険性について，各方面に警告している人物であった。対応策等について意見交換するため訪問した。

---

* 1 : ROLF MOULTON, DIRECTOR, THE CITY OF NEW YORK DEPARTMENT OF INVESTIGATION,COMPUTER SECURITY SERVICES UNIT

6.2　運用による対策

ニューヨーク市当局のコンピュータ犯罪対策の第一は運用による対策である。ニューヨーク調査局のスタッフは，ニューヨーク市のある部門がコンピュータを導入する時，その運用について助言を行なっている。この助言は，ニューヨーク市に対してだけでなく，民間企業に対しても，依頼があれば行なっている。（ただし公的企業に対して行なうようである。）

Moulton 局長は，セキュリティ対策の第一歩は，運用対策にあると考えているようで，そのガイドラインとも言うべき，標準的なシステム運用方法をまとめている*1。その内容は，通常よく言われている対策と大差はない。例えば，プログラマとオペレータを分離する，コンピュータ室での喫煙を禁止する，入退室管理を行なう等である。ただし，ニューヨーク調査局では，これらを明文化している。米国の他の多くのシステムでも同様に，とるべき対策および注意すべき項目を明文化している。すなわち，文書化は米国でのセキュリティ対策の特徴のように見える。しかしながら，これは米国の特徴というよりは，我国だけが例外的に文書化していないと考えた方が良い。我国では，セキュリティ対策だけでなく，システム設計書，プログラム仕様書等かなりの部分で，米国のドキュメントに比べて見劣りがする。ドキュメントの整備は，我国のコンピュータ・システム共通の課題のようだ。

セキュリティ対策を文書化することによる効果は，いろいろある。すなわち，誰が対策を行なっても同じレベルの安全性が得られる，対策の洩れを少なくできる，効果的な対策を他のシステムへ移植し易くなる等である。また，あるシステムのセキュリティ・レベルを評価する時にも，そのシステムのセキュリティ対策が文書化されていれば，確度の高い判断が可能になる。その結果，対策の洩れを発見するのも容易となり，それをフィードバックすることにより，さ

---

* 1：SYSTEM SECURITY STANDARDS FOR ELECTRONIC DATA PROCESSINGS
The City of New York, DEPARTMENT OF INVESTIGATION. STANLEY N. LUPKIN, PHILIP R. MICAEL, BRIAN BARRETT, ROLF MOULTON

らに安全性を高めることができる。

我国でも文書化の推進は，急務であると考えられる。また，日本の国情に合ったガイドラインの設定も必要であろう。

6.3 システム監査

ニューヨーク調査局では，Moulton局長の指導のもとで，システム監査を徹底的に行なっている。Moulton局長は，セキュリティ対策の第一歩が運用上の対策であり，決め手はシステム監査であると考えているようである。

ニューヨーク調査局のシステム監査は，すべてのコンピュータのログ・データ，処理結果を，人海戦術でしらみつぶしに調べ不正を発見することから始まる。不正が見つかると，今度は過去にさかのぼって追跡調査を行なう。そして，これらの調査は極秘のうちに実行されるのである。このため，1件の不正を摘発するのに，数カ月から1年かかると言う。なぜ，このような徹底した調査が必要かというと，理由は様々であるが，裁判に持ち込んで公判を維持するのに充分な証拠資料を得るというのが一番大きな理由のようである。

ニューヨーク州では，コンピュータ犯罪防止法がなく(1982年11月現在)，せっかく起訴しても，無罪になるケースが多いという。Moulton 局長は弁護士でもあるため，我国におけるコンピュータ犯罪の裁判結果に深い興味を示しており，近畿相互銀行事件の犯人に対して，私文書偽造が適用されたことに，ひどく感心していた。ニューヨーク州では，キャッシュ・カードは文書とは認められず，キャッシュ・カードの偽造に対して，恐らく私文書偽造は適用されないという。そのため，ニューヨーク州でもコンピュータ犯罪防止法かデータ保護法が必要だという。一方で，この種の法律制定には慎重であるべきだとも言っている。法律は，少なければ少ない程良いというのが，その理由だそうである。

現状でのシステム監査の問題点は，その効率の悪さにあるようである。各種のツールを利用してはいるが，決め手は人間によるチェックしかないと言われる。より効率の良いシステム監査ツールが必要という点では，我々と意見が一

致した。

6.4　セキュリティ技術

ニューヨーク市では，高度なアクセス・コントロール（ＡＣＦ２等)の導入は，これからの課題であり，いくつかの新技術について調査検討をしている。しかしながら，Ｍｏｕｌｔｏｎ　局長自身は，やはり人の問題が一番重要であり，技術はそれを支援するものと考えている。また，回線盗聴対策等については次のように言っている。すなわち，センタ，端末でのセキュリティ対策がまだ充分でなく，これらを先に対策する必要がある。その後，通信回線の暗号化等が検討対象になっている。つまり通信回線での暗号化は，まだ時期尚早であり，その前にやるべきことが多くある，ということであった。

6.5　その他

ニューヨーク市では，新しく採用する職員の，素行調査を厳重に行なっている。ニューヨーク市では，内部犯罪の最大の防止策は職員の資質の向上にあると考えていることと，米国では履歴書に虚偽の事実が記入されることが特に珍しくないことが，その主な理由である。米国では，自身に不利になる事実は履歴書に記入しなくても良いことが，慣習として認められている。また，多民族国家であるなど，我国とかなり国情が違っている。従って，この問題（職員採用時の素行調査）は，そのまま我国へ置きかえることはできない。我国では，新職員採用時にそれ程厳しいチェックをしなくても，特に問題は発生しない。このことは，セキュリティ対策全般に波及している。すなわち，性善説によるシステム設計がある程度可能だった。近年，我国でも性悪説による設計が必要だという意見が多くなっている。しかしながら，国情が違っている以上，米国で言われる性悪説と我国における性悪説の違いについて，検討する必要があると考えられる。

ニューヨーク調査局のような機関は，米国でも珍しい存在らしい。新しい問

題の発生に対応して，すぐこのような組織が設立できるのは米国のすぐれた点と言えよう。日本には現在このような組織はない。ニューヨーク調査局は，不正の摘発に関して大きな権限を持っており，極秘資料も含めて各種の資料をチェックできる。それだけに捜査官の採用にあたっての素行調査は厳重であり，捜査官全員が，分野は様々であるが，資格を持った専門家であり，いわば超エリート集団である。米国では，この種の調査官はエリートであり社会的地位も高い。これらの国情も我国とはかなり違っている。しかしながら，我国でも官公庁や地方自治体の機械化が進んでおり，ニューヨーク調査局と同様な機関（あるいは組織）が必要だと考えられる。

7. Massachusetts Institute of Technology
(Dr.James S. Miller)

7.1 調査目的

ＭＩＴ（Massachusetts Institute of Technology）は，世界的に有名な研究機関であり，Dr. Millerは，そこのAI Laboratory（人工知能研究所）の研究員である。しかしながら，今回の訪問の目的は，人工知能について意見を聞くことではない。Dr. Millerは，1年程前（1981年）まで，Bolt Beranek and Newman Inc.というARPAネットワークを始め国防省関連のシステム開発で有名な会社に勤務し，実際にセキュリテイＯＳの開発を行なっていた。この時の経験を基にした，Dr. Millerのコンピュータ・セキュリティに対する意見を聞くため訪問した。以下にDr. Millerの意見を簡単にまとめた。

7.2 セキュア・コンピュータ・システムについて

ＨＥＲＭＥＳ という海軍用のテレコミニュケーション・システムがあり，セキュア・システムのひな型だと言われている。しかし，このシステムにセキュリティ機能はない。その後，ハネウェル社は，米国政府からセキュリティ機構のコンピュータへの組込についての開発業務を受託し，ＭＵＬＴＩＣＳを開発し，セキュリティＯＳの歴史が始まった。コンピュータ・システムにセキュリティ機構を組込む作業を実際に行なった立場で，セキュリティＯＳについての印象を述べれば，開発が困難でありかつパフォーマンスが悪いというのが，現実のセキュリティＯＳだということになる。

セキュリティＯＳがなぜ重要かというと，それがコンピュータ・システムの核だからである。これが破られると，他のどんな構構も役に立たなくなる。しかし，セキュリティ機構の実現は非常に難かしい。セキュリティに係る複雑なスペックを実現するためのロジックは極めて複雑であり，従ってそのプログラムも複雑で作成が非常に難かしい。テキサス大学では，専用言語によるコーデ

ィングも試みられている。

Dr. Miller 自身は，コンピュータ・セキュリティを数学的に体系化しようとする研究を行なっていた。しかしながら，この研究は中断したまま終ったという。

7.3　セキュリティＯＳ“SCOMP”

ハネウェル社では，Secure UNIX といわれるSCOMP を開発中である。このプロジェクトはDEC社の支援も受けている。SCOMPは，ハードウェア・アーキテクチャについても新しい発想で新開発されている。それは“Honeywell Lebel 6 Computer”＋“New memory management unit”で構成され，MULTICS のハードウェアと似ており，リング・プロテクション機構を持っている。SCOMP のソフトウェアは，1978年から開発されており，

- Kernel （オペレーティング・システム核）
- UNIX エミュレータ
- Trusted Job

を含んでいる。図７－１のように，中央のリング（もっともセキュリティ・レベルが高い。）内に，Kernel が有り，次のレベルにTrusted Jobがある。そして一般のレベルとしてUsers Job がある。

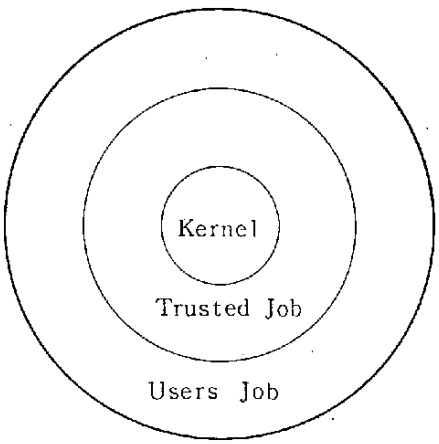


図７－１　　SCOMPのOS

一方，ファイルにはリング番号によるレベル付けが行なわれている。Trusted Job かUsers Job かの認識は，Kernel Job が行ない，ファイル・アクセス時のレベル・チェックはTrusted Job が行なう。すなわち，Kernel Job とは，通常のコンピュータのマスタ・モードに相当する。すなわち，KernelはＯＳそのものであり，通常のスレーブ・モードに相当する部分が，SCOMPでは複数に分れている。すなわち，ＯＳのマルチ・レベル化である。

このSCOMPに対して，ハネウェル社内部でもいろいろ論争があるようだ。例えば，ＵＮＩＸの改良で良いとする意見と，ＵＮＩＸのかわりに，より高度なカーネル・システムが必要だとする意見がある。現在，SCOMP プロジェクトは開発を中断していると言われている。SCOMP については，下記の文献に詳しく記述されている。

" Report on the Verification of SCOMP Kernel
by John Silverman , Honeywell Sand RC Minnepalis , Minn. "

7.4 ハードウェア・アーキテクチャについて

セキュリティＯＳを効率よく実現するためには，アーキテクチャにも専用の機構が必要である。例えば，リング・プロテクション機構（ＭＵＬＴＩＣＳ）やドメイン保護機構（ＰＤＰ－１１）等である。また，各種のチェックをマイクロ・コードで実現するのも有力な方法である。今後，ハードウェアの進歩により，セキュリティＯＳにマッチした効率の良いハードウェアが開発されると思う。

7.5 セキュリティＯＳの問題点

セキュリティＯＳの最大の問題点は，パフォーマンスの悪さである。現存する国防省のプロジェクトで開発されたセキュリティＯＳは，どれもパフォーマンスが悪い。ただし，これらのＯＳを民間のプロジェクトで見直しを行なえば，かなり改善されるのではないかと考えている。

セキュリティ機構をオプションとするのは誤りで，当初から内蔵していなけ

ればならない。しかし，軍用のセキュリティＯＳはパフォーマンスが悪いので，銀行等では使用しない。一方，ＭＵＬＴＩＣＳを軍用に使用したのは誤りである。ＭＵＬＴＩＣＳは，言われる程セキュアではないからである。ＴＥＮＥＸというセキュリティＯＳは，中途で開発に失敗し，ＤＥＣ社が買い取ったが，その後開発は行なわれていないようである。ＫＶＭ３７０は，仮想計算機方式のセキュリティＯＳであるが，詳細はよく分らない。

とにかく，現在のところ成功したセキュリティＯＳと言えるのはなく，開発の困難性を感じる。それだけに，今後が楽しみとも言えるだろう。

7.5　その他

ＭＩＴでは，公開鍵暗号であるＲＳＡ暗号の開発者として知られるProf. Ronald Rivest も訪問する予定であったが，Prof. Rivest の学会出席と重なり，訪問は実現しなかった。この他，ＭＩＴの研究施設の見学も行なったが，ＭＩＴについては，多数の文献がその活動内容や施設の紹介を行なっているので，ここでは割愛する。

8. Planning Research Corporation

8.1 調査目的

プランニング・リサーチ社（Planning Research Corporation 以下，PRCと略す）は，1954年に設立されたコンピュータとエンジニアリングに関連した業務を主としている企業である。現在6,600人の従業員と世界36ケ国に約200のオフィスを持ち，1982年の年商は3億2400万ドルであるという。PRCはPRC Corporate Center の総括のもとに

① PRC Computer Systems

② PRC Government Information Systems

③ PRC Engineering

④ PRC System Services

の4つのセクションより成っている。我々は，特に軍関係のシステム開発を多く手がけ，しかもその関係上，セキュリティについて最も研究の進んでいるPRC Government Information Systemsを訪問し，セキュリティ対策の実際と動向について調査した。当日対応して頂いたのは，以下の4名であった。

- Mr. P. Ray McInnis（Vice President）
- Mr. John E. Childress （セキュリティ担当）
- Mr. Richard L. Kessinger （システム・エンジニア）
- Ms. Jody E. Heaney （システム開発担当）

尚，PRCは民間のリモート情報処理サービス会社としても米国における大手の1つであるが，全業務の48%が前記のような軍や政府のプロジェクトであるため，主な調査項目は，国防省や軍関連のセキュリティ技術に関するものとなった。

8.2 調査内容

(1) 業務概要

PRC Government Information Systems が開発に携わったシステムは,

- 韓国空軍の情報システム
- 国務省の自動パスポート管理システム
- 空軍の戦略データベースの検索システム
- ハイウェイ・パトロールの無線によるデータベース・アクセス・システム
- 海軍の人事レコードの管理システム
- NASAのスペース・シャトルの制御システム

等がある。いずれもセキュリティ上の要求が厳しいシステムである。これらはほとんど国防省のセキュリティ技術を利用したものであり，必ずしも軍用ではないシステムであっても，セキュリティ上必要な機能は，軍事システム等で得たノーハウを活かして利用しているとのことであった。

(2) セキュリティに関する歴史

ⓐ 1970年初期

- Reference Monitor
- UNIX
- Lucifer と称するIBMで開発された暗号装置

ⓑ 1970年中頃

- MULTICS
- 2レベルの利用体系を付け加えたMULTICS改造のGuardian プロジェクト
- Kernelized VM/370

ⓒ 1970年後半

- フォード社[*1]で開発された，国防省のパケット交換通信システムのカーネル，AUTODIN Ⅱ
- UNIX改良版のKSOS（Kernelized Security OS）
- SRIのPSOS（Probably SOS）

＊1：Ford Aerospace & Communication Corporation

・ＤＥＳ暗号

・形式的設計仕様言語（Formal Design Specification Languages）

ⓓ 1980年初期

・SCOMP：ハネウェル社のミニコンを基にしたセキュリティＯＳで，ハードとソフトの双方で国防省のセキュリティ規準のＡ１レベルを目指すものである。

(3) 国防省のコンピュータ・セキュリティ評価センタの設立と評価基準の設定

国防省は1981年にコンピュータ・セキュリティ評価センタ（ＣＳＣ）を設立し，各種のシステムのセキュリティ機能を評価し，その評価データベースを作成しつつある。現在75～100人の担当者がおり，評価の対象となるシステムは軍関連のもののみとは限らず，民間も利用出来ると言われる。

ＣＳＣでは1982年末の設定を目途にTrusted Computer Systems[*1]（ＴＣＳ）のセキュリティ評価基準というものの草案を作成した。この基準はコンピュータ・システムのＯＳあるいはリソース制御に重点を置いたものであり，ＡからＤのマクロなクラス分けの中に，更にそれぞれ2，3のレベルが設定されている。ＰＲＣによれば，この基準案は民間においても，現在1つの大きな目標になっているとのことである。以下にその概略を示す。

① Ｄクラス：最少限の保護

② Ｃクラス：任意選択の保護，すなわちアクセス・カタログに基づくアクセス許可。（2レベル）

＜例＞Ｃ１；ＵＮＩＸ

Ｃ２；ＲＡＣＦ，ＡＣＦ２，ＳＥＣＵＲＥなどのファイル保護の追加

③ Ｂクラス：強制保護，ＴＣＢ（Trusted Computing Base）に基づく保護機構を持つ。（3レベル）

＜例＞Ｂ１；既存ＯＳに保護機構をつけ，改造した第3世代ＯＳ

Ｂ２；アクセス分離機構や保護の階層を持つＭＵＬＴＩＣＳ等

＊１：ハイ・レベルのセキュリティ機能を有するコンピュータ・システム

B３；Guardian プロジェクトにおける再設計されたMULTICS等

④　Aクラス：検証済みの保護，すなわち保護の正確さの理論的保証。（２レベル）

＜例＞A１；KVM，KSOS，SCOMP等

A２；ソースコード・レベルでの検証が行なわれたもので，現存しない

(4)　Multi－Level Security

ADPシステムに対するセキュリティ要求として，低→高の順に次の４つのモードが考えられる。

- Dedicated Security mode
- System high Security mode
- Controlled Security mode
- Multi－level Security mode

Multi-level Security mode においては，

- 多様なクラス分けが行なわれた記憶域（storage）
- 多様な許可レベルでの同時アクセス
- 多様な周知要求カテゴリにおける同時アクセス

が存在する。軍のシステムは，ほとんどこのモードである。そしてMulti－level Security により，

- 分散処理の拡大
- アクセスの容易性
- コンピュータ性能の向上
- 統合化された多機能コンピュータ・システム

等を実現できると言われる。

(5)　軍用システムのセキュリティ機構の例

某国のある軍用システムは，Multi－level Security 機能を持った例であ

る。このシステムにおけるセキュリティ対策は，

- ファシリティ（ハードウェア）
- アクセス・コントロール
- 通信（暗号化を含む）
- ソフトウェアの設計
- 処理手続

のすべてにわたって行なわれている。例えば，ハードウェアの電磁波の漏洩を防止するため，特別の材料の壁や導電塗料を用いることによりシールドする，というような物理的対策も行なっている。またソフトウェアの設計上も，システムの使用者毎に利用し得る機能やコマンドの区別を，きめ細かく制御し，ＩＤコードの入力によってその人が使用できる機能の一覧を出すようにしている。また権限外の機能を使用しようとした場合には、警報が発せられる。

もちろん，ソフトウェアの変更はごく限られた人にしか許されていない。また，ソフトウェアの作成段階においても，構造化設計，構造化プログラミングを始め，充分な開発手法や管理手法を用い，セキュリテイ効果を上げるよう努めた。

例えば，システム構成（Configuration Management，CMと略す。）の担当者が，ハード／ソフトのすべての責任を持ち，作成された全プログラムの仕様をすべてチェックする。システムが完成すると，作成されたプログラムはプログラマの手から完全に引き離され，ＣＭがディスクに移し，以後ＣＭがマスタ・バージョンを保持する。また稼動後のシステムに対しても，ＣＭが検査ソフトによりプログラムの不当な変更が行なわれていないかを，ジャーナル情報を含めてチェックする。

一方，このシステムは非常に機密性の高い部分と，さほどでもない部分とが混在しているのが一つの特徴であり，そのため図８－１のようなコントロールを行なっている。

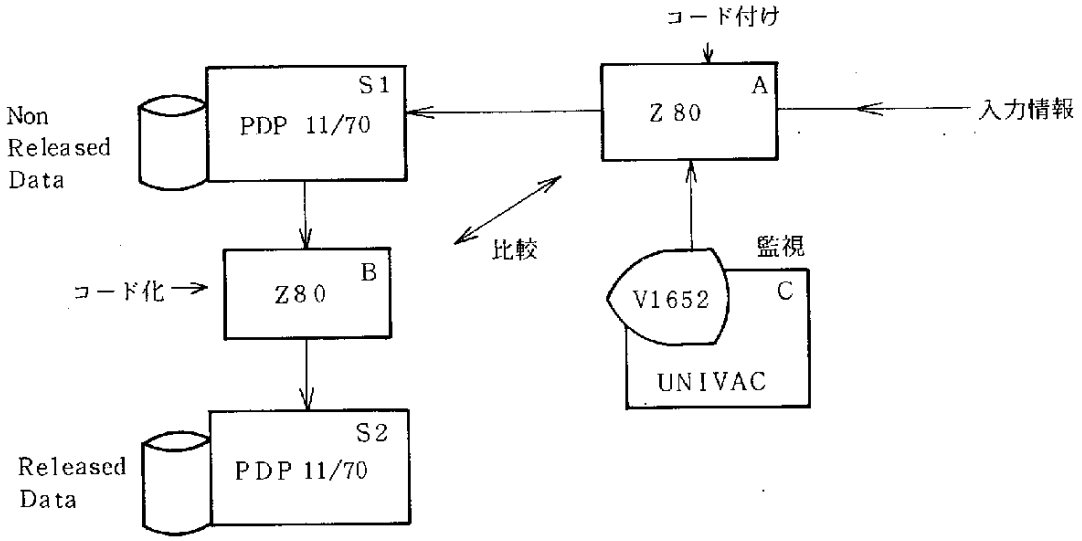


図８－１　コントロールの概略

Ｓ１は機密性の高いシステムでＳ２はさほどではない。Ａを通して入ってくる入力情報は逐一Ｃで監視され，Ｓ１に送れるもの，送れないものなどの区別が付けられ，併せてＡにおいてメッセージ長や内容から割り出したチェック・コードが付け加えられる。Ｂにおいて再び同様のチェック・コードが生成され，Ａでのチェック・コードと比較され，Ｓ１内で不当な変更が加えられなかったか否かをチェックする。また，Ｓ１止まりのデータが誤ってＳ２に流されるのを未然に防ぐ。入力量があまり大量でないシステムでは，このような制御が可能である。

(6)　新しい技術

今後利用されることが期待される技術として次の３つをあげた。

①　新しいハードウェア・アーキテクチャ

例えば，CDC社のCyber 800 シリーズでは，セキュリティ・アクセス・コントロールがハードウェア化されており，Ｂ３レベルをねらっている。

②　光ファイバの利用

通信のセキュリティに効果がある。

③ ソフトウェアのベリフィケーション

現在FDM（Formal Design Methodology）やFSL（Formal Specification Language）等を始め，南カリフォルニア大学やテキサス大学等での研究成果が若干あるが，今後5年から10年位の間にベリフィケーションの実用化が期待できると思うということであった。

8.3 その他

国防省や軍関連のセキュリティ技術を，民間システムに移転するには，様々な問題があるらしい。この点に関しては，PRCから明確な説明はなかったが，国防省のニーズと民間企業でのニーズに違いがあるように思われる。国防省のセキュリティ評価基準には，運用上の基準が含まれておらず，民間企業でのセキュリティ・ガイドライン（例えば，アメリカン・エクスプレス社等の）とは，かなり違っている。このような，コンピュータ・システムだけの基準を民間企業に適用して意味があるのか疑問が残る。

尚，PRCではオフィス内のいたる所に，入退室チェック・ゲートがあり，IDカードを所持していないと通れない仕組みとなっている。従業員の資格によって，オフィス内の通行許可の区域が異なるそうである。セキュリティをセールス・ポイントにしている企業だけに，社内のセキュリティも厳重を極める。このことも，運用上の対策が重要であることを暗示していて，興味深かった。

9. Security Pacific National Bank

9.1 調査目的

セキュリティ・パシフィック・ナショナル・バンク（Security Pacific National Bank,以下SEC BANKと略す）は，米国カリフォルニア州を中心にして多数の支店を有する商業銀行である。おおむね，日本の地銀に相当するが都市銀行的性格が強い。経営規模（資金量，従業員数，支店数等）は，米国内で上位10位以内に入る大きな銀行である。訪問相手であるMiss Mann（Miss Sandra M. Mann）は，ADPセキュリティ部（ADP Security Division）というこの銀行独特の組織の責任者の1人である。

この銀行では，かってリフキン事件（The Rifkin Fraud）が起きたことが知られている。この事件がコンピュータ犯罪かどうかの議論はさておき，今回の調査は犯罪事例の調査ではなく技術調査なので，この事件は特に調査対象になっていない。しかしながら，この事件を教訓として新たな対策が実施されている可能性があり，今回の調査で，その一部が明らかになるのではないかと期待された。

9.2 セキュリティ・グループ

SEC BANKの組織の特徴の一つにセキュリティ・グループの存在がある。図9－1の組織構成図の中のADP Security Divisionがそれである。このグループは，ADPグループ（日本の銀行の事務管理部かシステム部に相当する。）に属している。主な任務は，

① ネットワークのセキュリティ対策案の策定

② 物理的セキュリティ対策案の策定

③ ソフトウェアによるセキュリティ対策案の策定

④ 監査報告で指摘された問題点に対する解決案の策定

⑤ 異常事態（事故等）発生時の対応

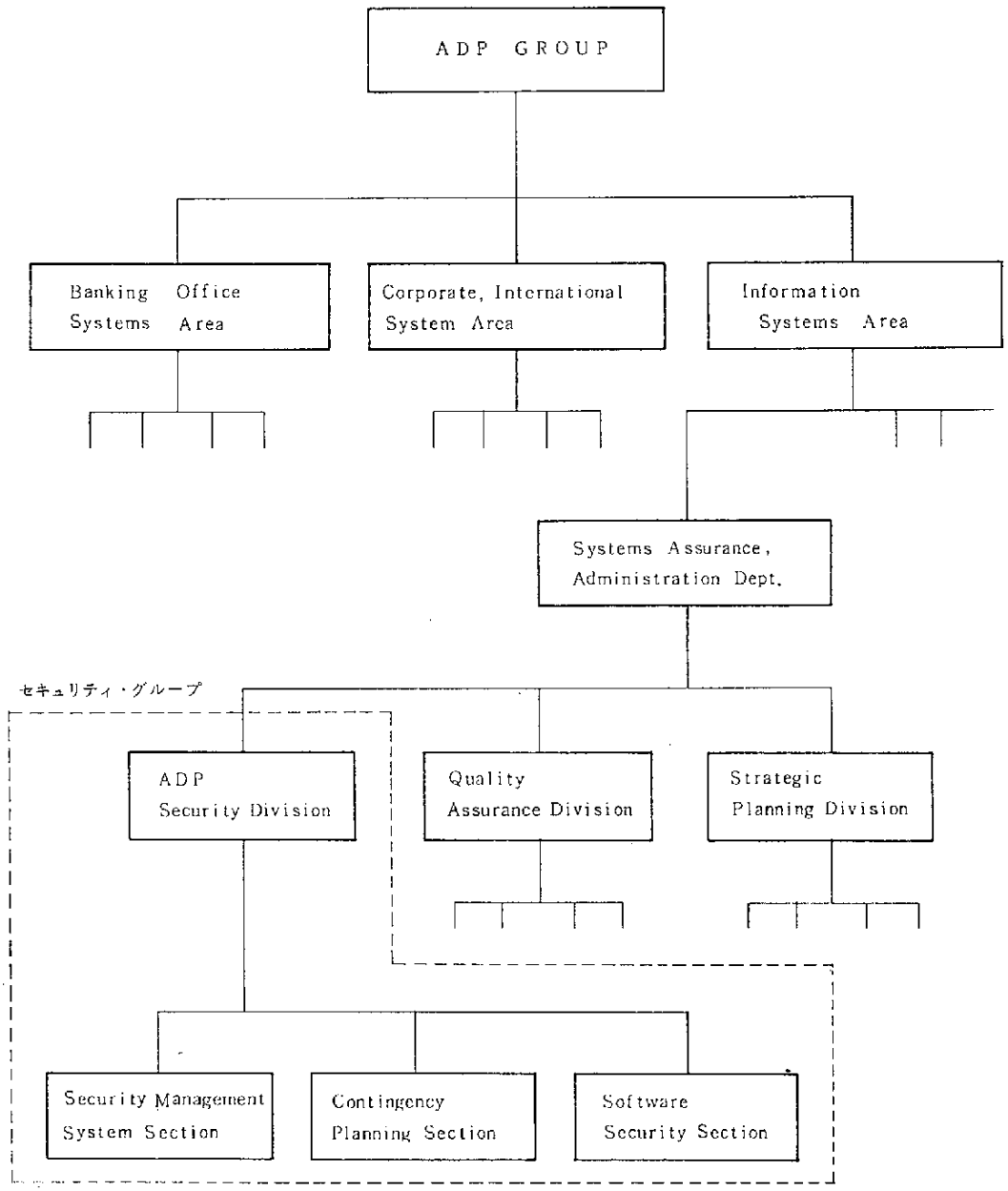


図９－１　Security Pacific National Bank
ADP GROUP組織概略図

である。このグループは，３年前（１９８０年）に設置された。現在，約１６名の専従作業員が居る。セキュリティ・グループの対策案は，ADP GROUPの決定機関へ提案され実行に移されることになる。

セキュリティ・グループは検査（システム監査）は行なわない。検査は，検査グループが行なう。図９－２に検査グループの組織概略を示す。セキュリティ・グループは検査報告で指摘された問題点の対策を検討するセクションである。

9.3 セキュリティ・グループの効用と問題点

セキュリティ・グループは，問題点や対策案を直接社長に報告することが可

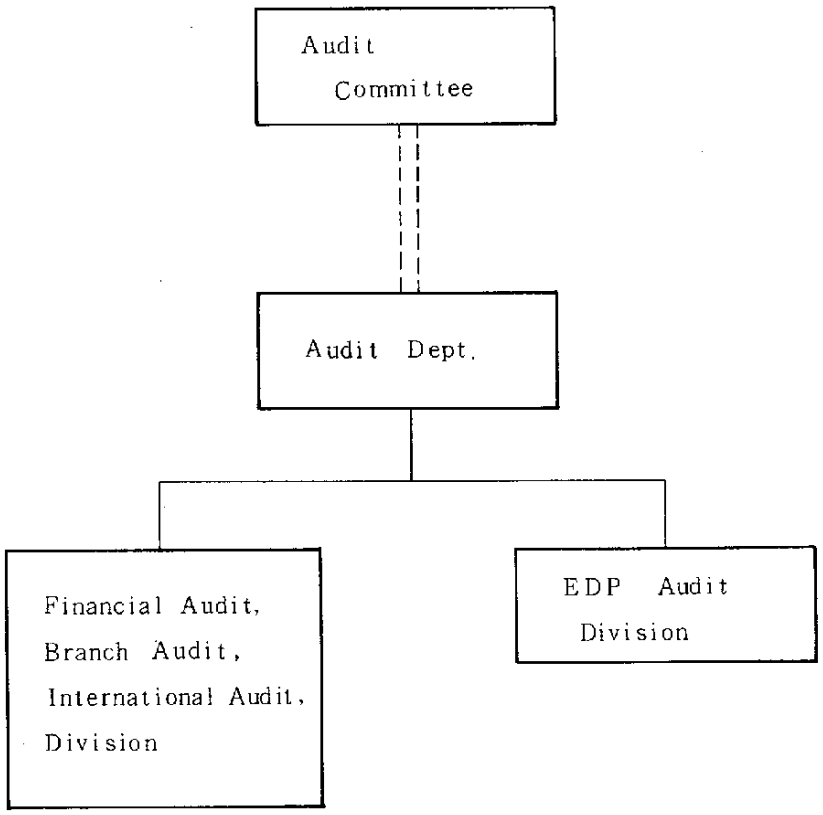


図９－２　Security Pacific National Bank
検査部門組織概略

能である。すなわち，組織上は，ADP GROUP に属しているが，実質的には独立して機能している。このため，問題点を冷静かつ公正中立に検討することができる。検査と同じような立場で検討ができる。これが最大の利点である。この意味では，セキュリティ・グループを組織上も独立した機関とするのが理想的だ。現在のように，ADP GROUP に属していると資金的な問題が発生するかもしれない。ただし，SEC BANKでは現在のところ，何の問題も発生していない。セキュリティ・グループと似た組織を持つ銀行は他にもあるが，その多くはＥＤＰグループに属している。しかしながら組織上の問題は特に起きていないようだ。

このような組織を有効に機能させるためには，経営側の理解が必要だ。資金的問題の解決も重要である。SEC BANKでは，セキュリティ・グループを重要な組織として経営側が認識しているため，この組織の運営はスムーズである。SEC BANKが“National Bank”であることも影響している。米国では，“National Bank”に対しては，政府決定による運営目標（義務ではない）があり，“State Bank”より高いセキュリティ・レベルが要求される。

9.4 セキュリティ・グループの活動内容

ここで，Miss Mann が説明してくれた，セキュリティ・グループの活動内容について，以下に紹介する。

(1) 調査活動

セキュリティ問題に関する情報を雑誌，新聞等から収集した。これらを分類・整理して，現状を知るための手掛りとしている。

(2) 暗号の研究

ネットワークのセキュリティ対策は，結論から先に言うと，大変解決が困難な問題である。現在いろいろな検討をしているが，暗号の使用は有効だと思う。SEC BANKは，暗号利用のパイオニアである。（商用システムではコスト高のため，あまり検討されていない。）暗号は，用いる方針や原則を

決めるのが重要である。機密性の高いデータに応用すべきだと思う。ＳＥＣ BANK では新しい暗号（ＤＥＳ暗号）の評価を行なうため，市販の暗号機を用いて実験を行なった。用いた暗号機は，RACAL−MIL60，MOTOROLA−CODEX，PARADYNE 等である。機能的には，どれも同じようなものであったが，使用上（運用上）の差異が認められた。ＤＥＳ暗号の導入については，現在コストを含めた実現性を検討中である。最大の難点はコストが高いことである。また，運用上の問題点もある。例えば，マスタ・キーのコントロールが，センタでしかできない，というのは不便である。

(3) 監査報告対応（Audit Report Tracking）

検査部門から“Turnaround Document”が送られてくる。この中で，種種の問題点が指摘される。これを分類整理してリストアップしておく。一方，これらの対策方法について検討し，システム開発部門に改善案を示す。これに基づき対策が完了すれば，先の問題点のリストから削除する。このようにして，システムの問題点を解消していく。

(4) セキュリティ対策基本方針の策定

セキュリティ対策を行なう場合，基本方針を定めておくことが重要である。また，これは文書化しておかなければならない。なぜなら，対策案が見つかっても実行できなかったり，不正を発見しても罰することができないことがあるからである。文書化されていれば，費用がかかるので対策しないとは経営者も言えないだろう。SEC BANK では下記の項目につて基本方針を定めている。

① Personal Security
② Data and Software （ADP部門）
③ Physical Security
④ Risk Management
⑤ Insurance
⑥ Outside Data Processing

(5) 技術的検討

SEC BANK では，各種のセキュリティ技術について検討している。暗号技術の研究については先に述べたが，その他以下の項目について検討している。

① アクセス・コントロール

RACFについて検討している。開発段階で，プログラマが，必要最少限のデータセットにのみアクセス可能にするためである。SEC BANK では，ＩＢＭのマシンを使用しているので，RACFを用いる予定である。現在，ＶＭ用のRACFがサポートされていないのが問題点である。

② チェック・ワード

オーセンティケーション（相手確認）のためのチェック・ワード生成に，ＤＥＳ暗号アルゴリズムを応用できないかについて研究している。

③ 新しい本人確認方式

ＰＩＮ番号（Personal Identification Number）にかわる新しい本人確認方式を研究している。指紋，ダイナミック・サイン等の方式は，いづれもコストが高いのが難点である。SEC BANK では，現在，自分自身でＰＩＮ番号を登録する方式を使用している。

9.5 その他

日本の銀行では，SEC BANK のセキュリティ・グループに対応する組織は，まだ一つの組織として独立していないようだ。恐らく事務管理部かシステム開発部等の中の一部として存在するのであろう。SEC BANK でも３年前に初めて組織化されたということである。３年前（1980年）の組織化は，リフキン事件（1978年）と時期的に対応する。やはり，この事件を教訓として，対策を強化するため，このようなセクションが生まれたと考えることが可能であろう。まだ，完全独立組織にはなっていないというが，権限が強化されている（例えば，社長に直接報告可能等）点が注目される。

対策は組織作りからというのは，米国流の方法で，国情も文化も伝統も違う日本へそのまま導入しても意味はないが，一つの運用上の対策方法として，その効果や問題点を研究すべきであろう。

10. California State University, Northridge
(Prof. Rein Turn)

10.1 調査目的

カリフォルニア州立大学（California State University, Northridge）の計算機科学科（Computer Science Department）の教授であるDr. Rein Turnは，コンピュータの信頼性，機密保護，セキュリティ技術などを重点的に研究しており，米国内はもとより，米国以外でのセキュリティ関連シンポジウムやコンファレンスなどでも中心的な役割を果たし，多くの論文も発表している。例えば，最近のものでは，1982年のＮＣＣに発表された"Private Sector Needs for Trusted Secure Computer Systems"という論文がある。我々は米国の研究分野におけるセキュリティの専門家としてのTurn教授に，セキュリティ技術に対する考え方や意見を聞くのが目的であった。以下に，Turn教授の見解をまとめた。

10.2 セキュリティ技術の現状と動向

(1) 本人確認

① 声紋・指紋・ダイナミック・サイン等による本人確認は，現在でも実現可能と言えるが，高価なのが難点である。ダイナミック・サインは，偽造を見極めるのが難かしい。声紋や指紋の方が，技術的問題が少ない。

② キャッシュ・カードやＩＤカードは，現在の磁気テープを貼ったものから，今後はマイクロ・プロセッサを内蔵したＩＣカードに変わるだろう。

③ 米国のコンピュータ・システムの９９％は，パスワードを使っている。しかし，パスワードの重要性の認識が欠けている場合が多く，例えばシカゴに本拠のあるネットワークでは，たった3桁のパスワードを使っていたため，マイコン端末で破られてしまった。尚，ベル研では１４桁のパスワードを使っている。

(2) オペレーティング・システム（ＯＳ）とハードウェア

① ＯＳの強化については，ＯＳの外から手を加えるのではなく，ＯＳの内部そのものを強化する必要があるが，ＯＳの開発に当っては各社とも特徴を出さなくてはならないため，自然と複雑になり容易に強化できない。そのためにはモジュール化などの配慮が必要となる。

② ＯＳのセキュリティは極めて重要であり，ＯＳが強固でなければ暗号化も本人確認も活きない。

③ ＭＵＬＴＩＣＳでは，ファイル分割，ビルトイン機能あるいはセキュリティ・オペレーションの省力化等が達成されており効果的であるが，セキュリティＯＳとしては中間的レベルのものである。

④ 新しいハードウェアとして，ＩＢＭ38やIntel 432，ＳＣＯＭＰ（未完成）のハードウェア等があるが，セキュリティに効果のあるハードウェアとは，セキュリティＯＳを簡素にし得るようなアーキテクチァを持つものであろう。

(3) 暗号化

① 暗号装置はあまり使われていない。また，ＤＥＳの強度について５年間も専門家の間で議論されているが，必ずしもまだ結論は出ていない。

② 暗号鍵の配送問題について，新しい技術は出ていない。

③ 数日前に，事実上解読不可能と言われていた，ナップザック・アルゴリズムを用いた暗号（ＭＨ法）を解読する理論が見つかったと伝えられた。真偽のほどは分らない。

④ 鍵の配送に対する標準的プロトコル設定の気運があり，ＩＳＯ，ＡＮＳＩ，ＮＢＳなどで検討が始まっている。これは重要である。

(4) セキュリティ・パッケージ

① ＲＡＣＦやＡＣＦ２などのパッケージは，後で追加する言わばフロント・エンド・セキュリティ機能ともいうべきもので，セキュリティＯＳの代りにはならない。

② RACFとACF2は，保護ポリシィが異なる。この2つの比較評価がComputer Security Instituteのジャーナルに記載されている。

(5) システム監査

① システム監査の順序としては，何が必要か，何が不必要かをよく確かめることが先決である。

② プログラムの不正は，エラー修正時にまぎれ込ませたり，低レベルのオブジェクト・コードで行なわれたりするので，監査でチェックするのは難しい。

(6) データベース

データベースのセキュリティとしては，その暗号化が今後の1つの鍵である。

(7) ソフトウェアの検証

SCOMPやKVM/370は設計レベルでの検証（国防省のA1レベル）を目指すものであり，コード・レベルの検証（国防省のA2レベル）を行なうものではない。しかし，最近のフォーマル言語を始めとする種々の研究の成果により，解決は目前に迫っていると言える。

10.3 米国におけるセキュリティの現状

① 国防省は，コンピュータ・システムのセキュリティ評価基準を設定した。そして民間企業はその動向を注目している。

② IBM社，ハネウェル社だけでなく，どのメーカもセキュリティに対する研究や対策の工夫を行なっていると思う。

③ 一般企業では，今だにトップ・マネージャにセキュリティに対して投資するよう提言するのは難しい。

④ セキュリティOSの民間への普及については，例えばKVM/370のようなものが効果をあげれば，普及し始めるかもしれない。いづれにしろ大企業が採り入れれば，徐々に中小の企業も採用することになるだろう。

⑤ 技術の開発に当って留意しなければならないのは，エンド・ユーザで使い

方が難しいと普及しないということである。その点，現在のパッケージ等はまだ使いにくく，ＩＤカード等は容易に使える。

⑥ パーソナル・コンピュータの普及に伴うセキュリティ問題という質問に対して，Turn 教授は次のような見解を示した。セキュリティ全般的に対して言えることではあるが，脅威は何であるのか良く分っていないことが多い。従来は，リスク分析をして明確にし，それに対応することでよいと，安易に考えられていたが，リスクがよく分っていないのに，現在の技術で可能か否か答えるのは難しい。

⑦ 情報処理サービス，データベース・サービスあるいはＶＡＮ業者などは，まださほど強力なセキュリティ対策を講じているとは思われない。ただ損害賠償や信用低下との係わりで，おのおの自分の問題として対処している。

⑧ 民間企業ではセキュリティ・コストを，賠償金や保険金とのバランスで考える。そして，こういった金の補償で片付くものなら，その方を選ぶ企業も多い。しかし，国防省や政府関連機関では，そのようにできない。

10.4 その他

米国の研究分野で，コンピュータ・セキュリティが華々しく採り上げられていたのは，1970 年代中期であり，研究テーマとしての最盛期は一段落している。セキュリティ技術全般に対しその造詣が深いと思われる Turn 教授との質疑においても，その傾向はよくうかがわれた。そして教授自身も強調しているように，現在は従来技術の妥当性の見直しおよび商品化／普及化の段階にあるように思われる。

また，パソコンを介してのシステムの大衆化に対しての見解である「どのようなリスクがあるかさえ分っていない」という指摘は，現実味があった。尚，国防省のセキュリティ基準との関連もあり，ソフトウェアの検証がセキュリティ分野でも大きな課題となっているのは注目される。しかし，解決が間近であるというのは，やや誇張があるようだ。

11. SRI International (Mr. Charles C. Wood)

11.1 調査目的

SRIは，各種の調査，研究およびコンサルティングを行なう有名なシンクタンクの1つである。約3200人のスタッフをかかえ，年間2000プロジェクトを超える活動を行なっている。コンピュータ・セキュリティについても,Donn B. Parker氏を始めとするスタッフが，

- コミュニケーション・セキュリティ
- バンキング・セキュリティ
- データベース・セキュリティ

等について，専門的に研究活動を行なっているということである。今回面会したMr. Charles Cresson Woodも，コンピュータ・セキュリティの研究者の1人であり，特に暗号についての専門家である。

今回の訪問の目的は，暗号の現状と今後の応用について，メーカ／ユーザとは異なる立場での見解を聞くことにあった。

11.2 情報通信システムにおける暗号について

最近，アルゴリズム，プロトコルの標準化への努力によって，暗号が容易に，安価に利用できるようになったが，多くのシステムはそれぞれにおいて制御するための特徴がある。例えば，

- 物理アクセス制御……ドアやターミナルの鍵等
- 論理アクセス制御……ログオンやアプリケーションの制御等
- パーソナル・ポリシィ……コンピュータ，リソースの個人使用等

等である。SRIのコンピュータ・セキュリティ・グループにおける研究では，情報通信システムにおける脅威を撃退する手段として，暗号がもっともコスト的に有効であると示唆されている。

しかしながら，暗号が果たす機能と同じ機能を有する手段がある。これらの

手段は，暗号にとってかわるものではなく，暗号と関連して考えられるべきである。具体的には，

- 通信チャネルの物理的プロテクション

  ——例えば，建物の周辺やプロテクトされた地域の中でローカル・ループ通信ラインを設置すること。

- 光ファイバの利用

  ——ワイヤ・タッピングを困難にする。

- コンセントレータの利用

  ——メッセージのリコントラクションを困難にする。

等がある。上記のような手段は暗号の一部の機能の代用として考えることができる。経済性からいって，暗号のような比較的ハイコストであるコントロールは，もっとコスト的に有効なコントロールが最初に適用され検討された後でないと，インストールされ実施されないであろうし，実施しても効果は半減するであろう。一方，脅威の種類から見た場合でも，コンピュータ・オペレータを買収するような低レベルの悪用は，ワイヤ・タッピングのような高レベルの悪用が，暗号のような高価なコントロールで撃退される前に，適切な安価なコントロールで撃退される必要がある。システムが各種の適切なコントロールの展開によって，より保全性の高いものになると，暗号は，より複雑な脅威を撃退するために必要性が増大すると思われる。

ＳＲＩのコンピュータ乱用が記録されているファイルの中に，わずか２件ではあるが，ワイヤ・タッピングによる事件があるということは，入力データの巧みなごまかしと同様に，ワイヤ・タッピングは，今後発生する可能性の高い脅威の一つであることを示している。

既に，米国の銀行においては，暗号の使用は，暗号がコスト面で効果的でかつ有効になるにつれ，当然具備しなければならない事項の一つになりつつある。暗号がバンキング・システムにおける保護のために，一般的に受入れられたものになると，暗号を用いていない銀行や，暗号を用いていれば防げたような損

害を受けた銀行は，暗号の適用を外部から求められるようになる。

11.3 暗号化により生じる脅威

(1) 暗号キーの紛失，破壊

- 暗号キーの紛失または破壊は，バックアップやリカバリ問題における結果と同様に，データ損失を招く可能性がある。
- 暗号化データは固有のキーがなければ，アクセスが不可能で，ほとんど価値がなくなる可能性があるため，盗まれたキーによる恐喝が起り得る。
- 暗号装置の故障は，必ずしもデータ損失，復号不可能の事態を招くわけではないが，運用を妨げ，データを脅威へさらす可能性がある。

(2) 暗号キーの変更

- 暗号キーの誤った生成は，生成されたキーが，安易に見やぶられるような非常に弱いキーでなければ，セキュリティ上または運用上の点で影響を与えない。
- 逆に，むやみに新しいキーを与えることは，システム・セキュリティを劣下させると同時に，もしシステムの他の部門の人が，オン・スケジュールに，むやみにキーを与えてきたならば，運用面に悪い影響を与える可能性がある。

(3) 暗号化による過信

暗号はデータの保全性を高める一つの道具にすぎず，決して万能ではなく，暗号を使ったからといって，気をゆるめることはできない。暗号を過信するあまり，他の面で注意をおこたってはいけない。

11.4 暗号の応用

現在の暗号理論のいくつかを応用したものが，近い将来に利用できるものと思われる。例えば，

① ディジタル署名

——ユニークで個人だけが知っているパーソナル・エンクリプション・キーの利用

② ケーブルと電話に関連したシステムへの応用

——ホーム・ボックス・オフィス（ＨＢＯ），ビュー・データ，テレ・テキスト等

③ タイム・シェアリング・サービス・ビジネスへの適用

④ コンピュータ・プログラムへの適用

⑤ インタ・コムのようなノンブロードキャスト・ラジオ・システムへの適用

⑥ プロセス・コントロール・システムへの適用

等々，種々の分野に暗号が幅広く採用されるものと思われるが，そのために，

- より低コスト
- よりよい使い易さ
- プロトコルの標準化

といったものが重要である。

12. Honeywell Information Systems Inc.
(Mr. Jerome Lobel)

12.1 調査目的

米国のコンピュータ・メーカの中で，コンピュータ・セキュリティに関して，もっとも先進的だったのは，ＩＢＭ社とハネウェル社（Honeywell Information Systems Inc.，以下，ＨＩＳと略す。）であると言われる。セキュリティ技術に関するＨＩＳの貢献は，大きく２つにわけて考える事ができる。その一つは，ＯＳの分野であり，既存のＯＳとしてはセキュリティ上最強クラスといわれるMULTICS（一部ハードウェアで実現）はMITの指導の下にHIS(当時はＧＥ）が開発したものであり，その後の改良も含め，現在もMULTICSはＨＩＳの標準提供ＯＳの一つとしてユーザに提供されている。一方，数年前からの国防省のプロジェクトであるセキュリティOS（Security OS：Security Kernel あるいは Trusted Computing Base，TCB とも呼ばれる。）の研究開発にＨＩＳは早くから参加し，現在も新しいセキュリテイOSとして，SCOMP と呼ばれるシステムを，国防省のプロジェクトとして開発中である。(現在，中断しているとの情報もある。）

もう一つのＨＩＳのセキュリティに対するアクティビティは，頻度高く，セキュリティ，プライバシ，システム監査などに関するシンポジウム，セミナ，あるいはワークショップなどを主催し，HISユーザのみならず広くコンピュータ・セキュリティの啓蒙活動を行なっているということである。また，今回面会したMr. Jerome Lobelは同社の教育部門のセキュリティ担当のマネージャであり，上記の各種セミナのチェアマン，あるいは主たる講師の１人であると同時に，しばしば国際的規模で，セキュリティに関する講演を行ない，またアリゾナ大学でもセキュリティの講座を持っている，コンピュータ・セキュリティの専門家の１人である。

今回の訪問の目的は，コンピュータ・メーカの立場としてのコンピュータ・

セキュリティ技術に対する現在および将来に対する考え方，あるいは米国の民間ユーザのセキュリティに関する対処の全体的状況など，他の訪問先とは異なる立場からの見解を聞くことにあった。

12.2 セキュリティＯＳについて

セキュリティＯＳは1977年に国防省がＵＮＩＸをセキュアにするというプロジェクトKSOS（Kernelized Secure OS）の研究開発を発足させたのをきっかけに，その後いくつかのプロジェクトが引きつづき国防省の援助の下で行われつつある。最初のプロジェクトはKSOS－11と呼ばれ，フォード社[*1]によりＤＥＣ社のPDP－11／70の上に実装された。ここでは，すべての処理がセキュリティ核（Security Kernel）のコントロール下におかれ，またUNIXをセキュアにするという，当初の目的からUNIX OSへのユーザ・コールをセキュリティ核コールに変換するという処理を逐一行なったため，当然のことながら，大きな効率上の問題が発生した。ＨＩＳが開発中の新しいセキュリティＯＳプロジェクトであるSCOMPは，別名KSOS－6とも呼ばれ，KSOS－11の改良版という見方がある。その改良のポイントは先ずパフォーマンス問題であろうと思われるが，前出の元ＢＢＮのMr. Millerの言葉にもある様に，SCOMPでは，UNIXをベースとすることは止め，新たな思想によるセキュリティＯＳとして設計することになったと言われる。今回のいくつかの訪問先でSCOMPの名が聞かれた。大方の評価は，必ずしも悪いものではなかったが，実現性を危ぶむ声もあり，その動向を注目するという見方が多かった。国防省自身も認めているように，セキュリティＯＳというものの実効性は，これが商用に如何に浸透してゆくかが大きな鍵であると言われる。その意味でもＨＩＳが開発中のSCOMPは，現在SDCが開発中のKVM／370（ＩＢＭ社のVM370のセキュリティ版で，これも国防省のプロジェクトの一つである）と共に，セキュリティＯＳの広い普及を占う注目すべきプロジェクトと見られている。

＊１：Ford Aerospace & Communication Corp.

そのため，今回のＨＩＳ訪問の大きな目的の１つはＨＩＳ自身の（あるいはＨＩＳの社員であるLobel氏の）SCOMPあるいはセキュリティＯＳに対する見解を聞きたいということであった。予想に反して，Lobel氏のセキュリティＯＳに対する見方はクールであった。彼の主たる意見は以下の通りである。

① セキュリティＯＳが他の機能，例えば，

- ターミナル・セキュリティ（Terminal security）
- コミュニケーション・セキュリティ（Communication security）

等と比べ，特徴的な点は，決して破られてはならないということである。その意味では大変重要である。

② しかし現在はまだ効率やコストの点で，軍用と言えども本格的に実用になっているわけではない。

③ これが，民間企業で利用されるというようなことは，まだまだ先の事であろう。そしてコスト的観点からも，ユーザ自身がセキュリティＯＳを欲するという状態にもなかなかならないであろう。例えば法律でその使用を義務付けるとか，メーカが無償で提供するとかというようなことがなければ当分民間の実用にはならない。

④ 将来のＯＳの基本機能としてセキュリティ機能が入るとも思わない。むしろＯＳというよりハードウェア・アーキテクチャの思想の問題となるかもしれない。

以上のように彼自身はSCOMPに対し直接言及することを避けたが，上記のような彼の見解から察すると，SCOMPプロジェクト自体がかなり難行しているのではないかとも想像される。

12.3 ＯＳ機能全般に関して

① ＯＳの中のセキュリティ機能部分と他の部分とを区別する方法を見出す

ことが必要である。例えばオーセンティケーション，ＩＤの確認，オーソリゼーション等の機能は，ＯＳのセキュリティ機能に入れる必要がある。

② データベースはＯＳの一つの要素である。ＤＢＭＳがＯＳ以上にセキュアになるとは考えにくい。

③ オーディタビリティ（Auditability：可監査性）の基準やガイドラインがもしできれば，通信データをチェックするための資料収集機能をＯＳに入れるのはよい方法である。現在はメーカがこういう機能をＯＳやシステム・ソフトウェアに入れたがらないため，アプリケーションとして行なっているが，ＯＳやシステム・ソフトウェアを通す方が，これらの機能は安価となるだろう。

④ メーカにとってセキュリティ機能をオプションとして扱う方が売り易い。現在でもＨＩＳのＯＳにはセキュリティ機能がオプションとして入っている。しかし，ＯＳにオプション機能を入れる事は技術的にはむずかしく，結局妥当な価格では作りにくくなる。オプションにせず，すべて含めてしまった方がずっと簡単である。

12.4 セキュリティ対策支援ツールおよびシステム監査支援ツールに関して

① 現在この様なツールはメーカよりもむしろソフトウェア・ベンダが提供しているケースが多い。現在のツールではユーザは不満であるが，より改善された製品が出るとしても，やはりソフトウェア・ベンダ等から出てくることになり，メーカからは出ないであろう。

② 一方，例えばシステム監査の標準がないというようなこともあって改善されたツールの出現はなかなかむずかしい。

③ また，セキュリティＯＳのようなものをソフトウェア・ベンダが提供するということは，コスト的にも不可能であろう。

12.5 分散処理と暗号化等について

① 分散処理のセキュリティ対策には暗号化しか解決法がないように思う。しかしＨＩＳでは暗号関連の製品は出していない（ＩＢＭでは販売しているが）。

② エンド・ツー・エンドの暗号方式が重要である。

③ 暗号装置のコストはかなり下ってゆくだろう。それまでは，特に重要な部分のみを暗号化すればよい。

④ ＤＥＳに関しては専門家の間で，その強度に対し色々と論争がある。また国際的なＤＥＳの利用に対しても問題があり，日本もあまりＤＥＳ中心に考えない方がよいと思う。

⑤ ＤＥＳを強化するには128 bit のサイファ・フィードバックを行えばよいと思う。

⑥ ＥＦＴＳでは暗号化しない電文を用いるべきではない。法律で定めるべきである。

⑦ ＳＷＩＦＴの担当者によると暗号キーの管理が弱みであると言っている。これは，暗号化すべてに言えることで，暗号化が普及しない理由の１つはキー管理の問題である。そしてこれは，むしろ人間や運用の問題である。

⑧ キー管理の自動化の１つとして，例えばプラスティック・カードにエンコードした１回しか使えないキーというようなものが考えられる。

⑨ 米国のユーザの中では，金融関係の企業が唯一のセキュリティ・マーケットであり，セキュリティ・アプリケーションの指導的立場にある，バンキング・システムでは暗号化も必要であろう。他の分野では，高価であることもあって暗号化は，ほとんど考えられていない。

12.6 Smart Card（CP−8）について

Smart Cardは，人々が早合点して，その有効性に期待し過ぎの感がある。経済性の問題も含め，大きな市場になるには時間がかかると思う。現在この種

のカードの最良の用途がはっきりしているわけではない。カードの扱いに関しては，カードの提供とキーの決定とは別のところで行われるようにすべきである。

12.7 OAやパーソナル・コンピュータの普及による脅威について

① ＯＡの実現により，オーソライズされぬコンピュータ・アクセスや，不正の機会は増大するであろう。従ってセキュリティ問題はより重要となる。

② ＯＡ技術の最も重要な要素の１つは使い易さや便利さだと言われる。しかしながら便利さとは，安全性が低下しても良いということではない。

③ ＯＡ環境における対策の１つとしてアクセス権を分散し，例えば２人一緒に協力しなければ，ある業務が果せないという方式が考えられる。

④ 物理的セキュリティや人間の運用管理がより重要であり，むしろ技術の問題ではなく，また技術のみでは解決できない。

⑤ パーソナル・コンピュータをリモート端末として保持する大きなネットワークはセキュリティ上大変弱い。例えば，ネットワークに接続し得るパーソナル・コンピュータの基準というようなものを法律的に定めるなどの配慮が必要になるかもしれない。

12.8 将来のセキュリティ問題全般について

(1) 今後の技術動向として次のようなものがあげられる。

① 指紋，声紋等の本人確認方式

② メーカ自身が基本ソフトウェアやハードウェアとからんだシステム監査支援ツールを提供するようになるかもしれない。

③ ハードウェアのコストが下がるので，セキュリティ機能をソフトウェアよりハードウェアで実現する方が安価になるだろう。

④ 衛星通信の暗号化を含むセキュリティ問題が各国にとって重要な問題となるだろう。

⑤　10年以上先のこととは思うが，セキュリティ機能を強化した場合のオーバヘッドをほとんど気にしなくてよくなるだろう。

12.9　その他

今回面会したLobel 氏は，研究開発や製造の分野ではなく教育担当であったため，メーカとしての戦略的あるいは技術的な細部にわたる問題を話し合うに至らなかったが，メーカに所属するセキュリティ専門家の立場で，むしろ客観的な話をしてくれたと思う。例えば自社のプロジェクトや製品でありながら，セキュリティＯＳやSmart Card に対するクールな意見はその現れの１つと思われる。またＨＩＳが暗号化関連の製品を何も手がけていない事に対しても疑問を持っているようであった。米国では，国防省のセキュリティ技術が徐々に民間に技術移転される段階にあり，ハードウェアやＯＳ等に関するその橋渡しの役目をこのＨＩＳやＩＢＭなどが大きく担っている様に見える。しかしながら，Lobel 氏の話を聞いた限りでは，ほとんどその気負いは感じられず，むしろ冷静に軍用のニーズと民間のニーズの大きなギャップを実務的に評価判断し，技術移転を急いではいないようだ。

付　属　資　料

A．　第９回　コンピュータ・セキュリティ・コンファレンス・ワークショップ一覧

B．　入手資料名一覧

C．　セキュリティ評価基準草案の概要

付 属 資 料　　A

第９回　コンピュータ・セキュリティ・コンファレンス
（Ninth Annual Computer Security Conference）
ワーク　ショップ一覧

WORKSHOP PROGRAM

Monday, November 8, 1982
Conferees can attend two (2) Workshops
One (1) from Section A & One (1) from Section B

Section A

Workshop No.

1. **Introduction to Data Security (For the Newly Appointed DSO)**
   Gerald J. Isaacson, Computer Security Institute
2. **A Strategy for Designing & Evaluating Secure Computer Systems**
   Daniel J. Edwards, DoD Computer Security Center
3. **Long Range Planning for Data Security**
   Robert P. Campbell, Advanced Information Management
4. **Operating System Security: Making it Happen**
   F. W. "Ted" Gerbracht, The Chase Manhattan Bank
5. **Controlling the Applications Programmer: Procedures, Libraries, and Separation of Duties**
   William H. Murray, IBM Corporation
6. **How to Evaluate a Security Software Package**
   Mark S. Hahn, GESCO Corp.
7. **Securing the Automated Office**
   Diane M. Smith, DoD Computer Institute
8. **Electronic Funds Transfer (EFT) Security**
9. **Dealing with Computer Abuse: Prevention, Detection, & Investigation**
   Rolf Moulton, New York City Dept. of Investigation
10. **Long Range Planning for EDP Audit**
    Steve Mar, Seattle First National Bank
11. **Basics of Contingency Planning**
    Toni B. Fish, Shearson-American Express
12. **Phase I of Recovery Planning: Identification of Critical Applications**
    Salvatore C. Catania, Coopers & Lybrand

Section B

13. **Developing & Implementing a Data Security Policy**
    Robert E. Johnston, Phoenix Mutual Life Insurance Co.
14. **A Blueprint for Establishing Security Guidelines and Standards**
    George E. Caldwell, New Jersey Bell Telephone Co.
15. **A Checklist Approach for Evaluating On-Line Security**
    Alan Berman, Bradford Trust Company
16. **How to Conduct a Security Review of the Data Center**
    David A. Griffiths, Coopers & Lybrand
17. **Common Carrier Network Security: Problems & Solutions**
18. **Password Administration Techniques**
    Michael H. Agranoff, The Hartford
19. **The State-of-the-Art in Computer Security**
    Joel Urman, IBM Corporation
20. **Becoming More Effective as a Computer Security Professional**
    Doug DeVries, Hewlett-Packard
21. **Managing the EDP Audit Function**
    William J. Moran, The Chase Manhattan Bank
22. **The Computer Assisted Auditor**
    William C. Mair, Touche Ross & Co.
23. **Disaster Recovery for Large-Scale Users**
    Andrew J. Logan, INA
24. **Disaster Recovery for the Smaller Installation**
    Marvin Golland, Peat, Marwick, Mitchell & Co.

Tuesday, November 9, 1982
Conferees can attend one (1) of these twelve (12) Workshops

25. **Risk Analysis: An Overview**
    Gerald J. Isaacson, Computer Security Institute
26. **User Experiences with ACF2 and TOP SECRET**
    Peter Harding, National Trust Co., Ltd.
27. **A Strategy for On-Line Systems Security**
    Peter P. C. H. Kingston, Kingston, Goulbourn & Associates
28. **Security Standards in a Data Base Environment**
    Steven J. Ross, The Plagman Group
29. **Security and Audit Concerns in a Minicomputer Environment**
30. **Assuring Data Integrity in Computer Systems and Networks**
    Dr. Dennis K. Branstad, National Bureau of Standards
31. **Data Center Relocation: A Before, During, and After Case History**
    Frank C. Collins, The Travelers
32. **Data Security Implementation in Multiple DP Environments**
    Henry J. Mandl, Manufacturers Hanover Trust Co.
33. **Developing a Security and Control Program at JC Penney & Co.**
    Gary M. Dickhart, JC Penney & Co.
34. **Capacity Planning for Disaster Recovery**
    Ilene Halem, The Plagman Group
35. **Meshing EDP into the Overall Organizational Recovery Plan**
    Edward S. Devlin, Devlin Associates
36. **Testing the Disaster Recovery Plan**

Wednesday, November 10, 1982
Conferees can attend one (1) of these twelve (12) Workshops

37. **Give and Take . . . for Advanced Data Security Practitioners**
    Robert E. Johnston, Phoenix Mutual Life Insurance Co.
38. **User Experiences with RACF, SAC, and SECURE**
    Peter Harding, National Trust Co., Ltd.
39. **Implementation of a Security Software Package: How to Manage the Project**
    Leslie S. Chalmers, The Bank of California
40. **Designing Security into EDP Facilities**
    L. B. Compton, Total Assets Protection, Inc.
41. **Information Security: Future Issues**
    Zella G. Ruthberg, National Bureau of Standards
42. **Security & Control Techniques in a Data Base Environment**
    Philip Teplitzky, The Plagman Group
43. **Developing an EDP Security Awareness Program**
    Michael H. Agranoff, The Hartford
44. **"Selling" Security to Data Processing, Users, and Senior Management**
    Martin E. Silverman, Coopers & Lybrand
45. **EDP Audit Tools and Techniques**
46. **Security and Control of Distributed Systems**
47. **Developing a Disaster Recovery Planning Guide**
    Gerald J. Isaacson, Computer Security Institute
48. **Reviewing Your Disaster Recovery Plan: Will it Work?**
    Will Ozier, EDP Audit Controls, Inc.

付属資料　B　　入手資料名一覧

	資料タイトル	頁数	入手先
1	An Assesment of U.S. Competitiveness in High Technology Industries	70	Technology Analysis Group
2	Staying in Charge (IBM)	27	
3	Data Processing Security Guidelines (slide copy)	29	American Express Company
4	American Express 1981 Annual Report	92	
5	MIT Video Short Courses	87	MIT AI Laboratory
6	Laboratory for Computer Science	28	
7	Technical Report TR−83−7 Multi-Level Security	51	Planning Research Corporation
8	PRC Government Information Systems Technical Seminar	50	
9	Office Automation Security Problems	9	
10	Annual Report	4冊	
11	PRC Corporate Overview	11冊	
12	Advances in Computer Systems Security	402	California State University, Northridge
13	Computer Security Journal	113	
14	CBEMA Privacy & Security Bibliography	51	

	資料タイトル	頁数	入手先
15	Application of Cryptography	17	California State University, Northridge
16	Security Issues in Transborder Data Flows	5	
17	EDP Control and Security	14	SRI International
18	Computer Systems Contingency and Recovery Planning Services	4	
19	Computer Security and Privacy Symposium Proceedings 1981	140	Honeywell Information Systems Inc.
20	Systems Security Standards for Electronic Data Processing	109	The City of New York Department of Investigation
21	New York City Department of Investigation	6	
22	A Strategy for Dealing with Computer Fraud and Abuse : A Case Study	10	
23	A Multidisciplinary Approach to the Investigation of Computer Abuse Incidents	8	

付　属　資　料　　C

セキュリティ評価基準草案の概要

評価のためのシステムの区分

区分	タイトル	説明
D	最少限の保護	このシステムは評価されてはいるが，上級クラスの要件に適合しない。
C	任意選択の保護（Discretionary Protection）	このシステムは知覚保護（need-to-know protection）を与える。
B	非選択の保護（Mandatory Protection）	このシステムは主なデータ構造について非選択のラベルを持っている。このシステムの供給者はＴＣＢ[*1]が基礎としている機密保護方針のモデル及びＴＣＢの仕様書並びにそのReference Monitor の概念がインプリメントされている運用保証を提供する。
A	検証済みの保護（Verified Protection）	このシステムは正式に検証され，且つこのシステムにおける情報を有効に保護することが実証されている非選択および任意選択の機密保護コントロールを持っている。

*1 ： Trusted Computing Base

〔任意選択の機密保護システムの要件――クラスＣ１〕

1. このシステムは自己防衛型でなければならない。すなわちそれ自身の実行のための保護領域をハードウェアの中に強制的に組み込むか，あるいはソフトウェアの中で創り出して強制的に組み込まなければならない。従って，システム・データ構造は，勝手に修正されてはならない。
2. このシステムは，指定使用者とシステム内のオブジェクトとの間のアクセスを定義し，コントロールする設計上のベースによって任意選択のアクセス・コントロールを与えなければならない。（埋め込まれたシステムは，ダイナミックに変更可能である必要はない。）
3. このシステムは，ユーザに対してシステム的に強制された確認及びユーザのデータが保護されるような確認を規定しなければならない。
4. このシステムの安全性（セキュリティ）のテストは，その機密保護機構がこのシステムの各ドキュメンテーションごとに働らくことを実証しなければならない。
5. システムのドキュメンテーションはその安全性のテストの結果を含んでいなければならない。システムの管理者用のドキュメンテーションは安全機構をコントロールし得る機能と特権（privileges）とについて注意を示さなければならない。ユーザ用のドキュメンテーションには，保護機構に関する記述，使用上のガイドライン，およびその保護機構がどのような影響を与えるかについての記述がなければならない。
6. 例：　ＵＮＩＸ

   期待される周囲の事情：協同作業しているユーザの処理しているデータが同じ程度の取り扱いの重要度を持っていること。

〔アクセスをコントロールするような保護システムの要件――クラスＣ２〕

このシステムはクラスＣ１のすべての項目を必要とし，さらにファイルの保護を必要とする。

1. このシステムは資源（リソース）を包みこむような保護を与えるものである。すなわち資源が保護され，その結果，付加的なアクセス・コントロールと監督の要件が満たされる。
2. このシステムの任意選択のアクセス・コントロールは，ユーザとシステムについて次のような省略時の解釈を与える。すなわち通常はオブジェクトを保護するようにセットされ，指定ユーザから特別に承認された場合のみ，他のユーザのアクセスを許すのである。
3. このシステムの確認行為は，オペレーティング・システムの確認をさらに強化するであろう。
4. このシステムは保護された資源に対するアクセスを監査しなければならない。そして，ユーザ，資源，アクセスのタイプ，およびアクセス時間を識別するはずの監査記録を保護しなければならない。
5. このシステムの機密保護のテストは，資源を包み込んでしまうことを許すような，あるいは，確認と監査データを侵害することを許すような明らかな欠陥が存在しないことを立証しなければならない。
6. このシステムのドキュメンテーションでは，基本的なオペレーティング・システムの説明をユーザに与えなければならない。もしこれが機密保護をパッケージで追加したものならば，そのパッケージとオペレーティング・システムとの接続方法（インテグレーション）について明記しなければならない。
7. 例：ＩＢＭのＭＶＳ／３７０に対する追加的パッケージ（add－on packages）
   ＲＡＣＦ，ＡＣＦ２，ＳＥＣＵＲＥ．

〔ラベルをつけられた機密保護システムの要件――クラスＢ１〕

1. 定義されたユーザのインタフェースと共に，ＴＣＢはこのシステムの中心であり，このシステムで実施された機密保護方針のモデルの各々は，製作者の保護原理の文書の中に述べられている。
2. ＴＣＢはすべてのシステム・オブジェクトについて８つの階層的なレベルの区分とその各々のレベルについて，それぞれ２９の非階層的カテゴリとで非選択のアクセス・コントロール機構を実施しなければならない。
3. このシステムはＣ２クラスの任意選択のアクセス・コントロールを達成するが，それはＴＣＢによって定義されコントロールされるものであり，知覚保護（need－to－know protection）にふさわしいものである。
4. ＴＣＢは記憶装置内のオブジェクトに結合した保護ラベルを保存しており，このシステムから外に出されるすべての情報にこのラベルを適用する。最小限，印刷された各ページの一番上と一番下とに用いる。
5. ＴＣＢは個々のユーザの識別のための確認作業を実施し，その確認データを保護する。
6. このシステムはＣ２クラスの監査の要件を達成してはいるが，ここで対象としている資源はＴＣＢによって保護されているものである。
7. ＴＣＢの保護機構とそのオペレーティング・システムのその他の部分とについての機密保護のテストは，その機能に関して実行され，二ケ月にわたる侵害テストが経験豊かなチームによって行なわれている。除去することができなかったり，無効にすることができなかったりするような欠陥はどんなものでも容認されない。
8. システム・ドキュメンテーションには製作者の保護原理と，ＴＣＢのリファレンス・モニタの一部でサポートされ識別される機密保護の方針とについて記さなければならない。このドキュメンテーションは，このシステムの保護機構を識別し，それらがどのように機密保護の方針を実施するかを示し，

それらがどのようにして不正にいじれないようにできているか（tamperproof）あるいはどのようにバイパスしないかの理由を説明し，そしてそれらの正確さに対する証明を提供しなければならない。欠陥が除去されない場合には，いかにしてその欠陥を無効にするかについての対策が記載されなければならない。機密保護機構の機能的なテストの結果が記述されなければならない。Trusted Facility マニュアルが用意されなければならない。

9. 例：ユーザのインタフェースに対して機密保護の方針をサポートするような機構をあとから取り付けた十分に完成した第三世代のオペレーティング・システム。

ユーザのインタフェースに対して保護を与え，内在するオペレーティング・システムに対するユーザのアクセスを制限しているような埋め込まれたシステム。

〔構造的保護システムの要件――クラスＢ２〕

このシステムはＢ１クラスのすべての項目を必要とし，さらにＴＣＢの構造化，情報の流れのコントロール，および限定チャネル（confinement channels）の識別を必要とする。

1. ＴＣＢのオブジェクト指向型の構成のある形態を用いながら，また保護の臨界要素（protection－critical elements)を包含したり分離したりするためのハードウェアのサポートを設計しながら，ＴＣＢのモジュールに対する優先権（ privilege） を最少限しか行使させないという原則を適用する。限定チャネルは識別され，重要な開発用（exploitable)の記憶チャネルは閉じられる。
2. ＴＣＢの非選択のアクセス・コントロールは，ＴＣＢの外部の目に見えるすべての資源（すなわちデバイス，相互処理できるコミュニケーション領域，一時的ファイル，端末装置およびプリンタ）に対してコントロールを実施する。
3. ＴＣＢはＴＣＢの外部にあって直接あるいは間接的に見ることのできるすべての情報のオブジェクトについて，コントロールの流れまたは制限を実施する。
4. ＴＣＢの任意選択のアクセス・コントロールは単一のユーザの不統一なアクセスを，包含あるいは排除することができる。ユーザの指定可能な省略時の解釈は，埋めこまれていないシステムにおいてサポートされており，ユーザは自分の所有するファイルに対するアクセスを変えることが可能である。
5. ＴＣＢの保存している保護ラベルは，アクセス・コントロールの決定のために用いられ，そしてそのラベルのつけ方は，指定された端末装置の型と，コンピュータ相互間の連絡に対して強制的に実施されるのである。
6. オブジェクトの再利用はＴＣＢによってコントロールされる。すなわち，ＴＣＢは記憶装置内のデータのオブジェクトを，それらが再利用される以前に除去（purge） する。
7. システムは同一ユーザの識別と，何らかの監査可能な行動の関連事項とに

関して個々の責任体制（accountability）を与える。

8. ＴＣＢはＴＣＢとユーザとの間の機密保護関係の機能についての保証経路（trusted path)をサポートしている。そしてこれはＴＣＢによって情報を損なわれることなく完全に受け取ることのできることを保証するものである。

9. システムの監査機構は，利用可能な帯域幅を持っていることを示すチャネルの使用を，記録しなければならない。

10. ＴＣＢは信頼できる機構管理（facility management）を有している。最少限の特権しか持たずに，オペレータと管理者との機能の分離が維持されている。これらの機能は指示された端末装置からのパフォーマンスを制限するかもしれない。最小および最大の機密保護のレベルが，接続している物理的デバイスに対して，割り付けられうる。

11. 構成（configuration)管理システムはＴＣＢの開発と保守の間中存在している。ソース・コードから，このシステムの新しいバージョンを生成するための手段，およびそれを前のバージョンと比較するための手段が与えられている。

12. 機能的なテストおよび機密保護テストは，ＤＴＬＳ[*1]の要件に従って証明されている。そして侵害テストは経験豊かなチームによって４ケ月にわたって，ＴＣＢについて実行されてきている。すべての欠陥は訂正されていなければならない。

13. ＴＣＢの最上級の仕様書は実施される方針について明確に述べている。現在のＤＴＬＳはこのドキュメントの一部として維持されている。設計解析はＴＣＢがいかにしてReference Mannalのインプリメンテーションの要件を満たすかということおよびＴＣＢがテストを促進するため，また，特権を最少限しか実施しないですむようにするため，どのように構成されているかを記している。限定チャネルの設計解析の結果と，含まれる二律背反性のすべてが示されている。限定チャネルの工学的処理に関する有効性のテストにつ

＊1：Descriptive Top-Level Specification

いても記載されている。

14. 例：MULTICS

Access Isolation Mechanism （ＡＩＭ，アクセス分離機構）の具体化

〔機密保護領域システムの要件――クラスＢ３〕

このシステムはＢ２クラスのすべての項目を必要としているが，さらにこのＴＣＢは保護モデルを基にしており，階層化，抽象化およびデータ秘匿化を具体化している。

1. ＴＣＢは単純で集中的な包含機構を用いるように設計され，構成されている。ここでは特別に保護取り扱いに注意を必要としないモジュールはＴＣＢから取り除かれる。タイミングとストレージ限定チャネルとは識別され，ストレージ・チャネルは，そのモデルの設計と綿密な適用とによって閉じられる。
2. たった一人のユーザのために他の多くのユーザがサービスを全く拒否されてしまうという事態を避けるために，ＴＣＢは臨界的資源の割り当てを，グループやユーザや level basis に対して設定したり維持したりすることによって；保護サービスを拒否することもできる。
3. ＴＣＢとユーザの間には，保証経路が存在しなければならない。ＴＣＢに対してひとつ，ユーザに対してひとつの独自の識別子または機構が，直接的コンタクトを設定するために用意されなければならない。その識別子はＴＣＢかユーザかによってのみ生成できるものでなくてはならない。
4. ＴＣＢは臨界的な出来事の出現や累積を監視するために，そして，しきい値の超過についてオペレータや機密保護の管理者に知らせるための追加的監査機構を与える。
5. 保証機構管理（trusted facility management）はシステムの管理機能のサブセットとしての機密保護管理者の機能の識別を含み，機密保護機能が遂行される以前に，システム管理者が明瞭な行動をとることを要求する。
6. 保証復旧機構（trusted－recovery features）は，保護のレベルを低下させることなく，システムを復旧することの保証を与えられている。
7. システムの保全性の機能はハードウェアおよびファームウェア機構の臨界

点の定期的なチェックを認めることで可能となるであろう。

8. ＴＣＢのインプリメンテーションは十分に文書化されているソース・コードを規定しなければならない。そしてそれは，すべてのモジュールとサブモジュールとの間のインタフェースを十分に定義した，高度に体系化した様式で書かれなければならない。

9. 機密保護に関する侵害テストは，経験豊かなチームによって，6ケ月にわたって，このＴＣＢに対して実行された。設計上の欠陥はなく，ほんの2，3の修正可能なインプリメンテーション上の欠陥がみとめられたのみであった。

10. ＴＣＢの最上級の仕様書はそのＤＴＬＳがいかにして機密モデルをサポートするかを示さなければならない。Trusted Facility マニュアルは安全復旧のための手順を含まなければならない。設計解析は機密保護モデルをサポートするためのＴＣＢにおけるすべての基本的な保護構造の機能について証明しなければならない。

11. 例： Project Guardian におけるMULTICSの再設計

〔検証された設計システムの要件――クラスＡ１〕

このシステムはクラスＢ３のすべての項目を必要とし，さらに保護の正確さの形式的な数学的保証とＴＣＢにおいてインプリメントされたその方針の機構とを必要とする。

1. このクラスの設計の検証のためには，次のような５つの基準に合致しなければならない。
   a. 形式的な機密保護モデルが識別され，記述されなければならない。
   b. 形式的および非形式的なテクニックが，そのモデルと機密保護実施の局面についての最上級の仕様との間に一貫性のあることを示さなければならない。そしてその他のすべての要素について，そのシステムの機密保護の範囲内にあることを示さなければならない。
   c. 形式的な仕様はユーザの見ることのできるＴＣＢの分離や包含をサポートするのに用いられるハードウェア／ファームウェア機構の抽象的定義を含まなければならない。
   d. 形式的で最上級の仕様の要素は，もしそのシステムの抽象的設計でないならば，それらがインプリメントされるであろう設計要素に対応することを示されなければならない。
   e. 形式的な解析方法が限定チャネルに適用されなければならない。
2. ＴＣＢは形式的な最上級の仕様から導き出されなければならず，それをサポートすることを示さなければならない。そしてその高い保全性を得るために，大きな内部的な包含を用いなければならない。アクセス・コントロールの検証と，情報の流れの解析とは，設計とインプリメンテーションの期間中に，相互に影響し合うように適用されなければならない。また，すべてのエラーは改訂され，再検証されなければならない。
3. 保証経路は，ユーザとＴＣＢとの間の経路――すなわち論理的には，通常のデータの経路からは分離されているもの――を保証しなければならない。

4. 保証機構管理はシステムの機密保護の管理者に対して，識別とサポートという分離したシステムの役割を与えなければならない。そしてシステムの管理者は特別な行動をとることなく，その役割を遂行してはならない。

5. ＴＣＢのインプリメンテーションは，その設計の部分的検証が完了するまで始めてはならない。そしてＦＴＬＳ[*1]は，中央の設計の権限として維持されなければならない。

6. 構成（configuration）管理のコントロールは形式的なモデルとFTLSとを包含するものでなければならない。

7. 保証分散機能（trusted distribution facility)とシステム・コントロールとは，コードのマスタ・コピーと，システムの現在のバージョンを記述しているマスタ・データとの間で写像の保全性を維持することを与えられなければならない。そのシステムの更新は，正確にマスタ・コピーによって指定される通りであることを保証する手順が存在しなければならない。

8. 機密保護のテストはＦＴＬＳと Reference Monitor のインプリメンテーションとの要件に従って証明されなければならない。

9. 形式的なモデルについてのドキュメンテーションは，それがその原理と矛盾しないことを証明している。ＦＴＬＳは，ＴＣＢの現在の設計とインプリメンテーションとを反映するように維持されねばならない。ＦＴＬＳの中で取り扱われていないハードウェアとソフトヴェアの機構は設計解析の中に含まなければならない。ＦＴＬＳとコードとの間の手操作による写像の結果についてのドキュメンテーションが与えられなければならない。

10. 任意選択（optional）の機構には次のようなことが必要となるであろう。

    a. 保証経路と結合してユーザ指定の情報のユーザによる再分類を許すのには Trusted Downgrade Facilityを与えること。

    b. ＴＣＢのコントロールの下でシステムに付随する Clearing of Terminals を与えること。

11. 例：ＫＶＭ370，ＫＳＯＳ，ＳＣＯＭＰはこのクラスを目標としている。

---

*1 ： Formal Top-Level Specification

〔検証されたインプリメンテーション・システムの要件――クラスＡ２〕

このシステムはＡ１クラスのシステムのすべての項目を必要とし，さらに，ソース・コードのレベルにまで拡張された形式的な検証，および印刷物のサービスとタイミング・チャネルを瞬時に拒否することのアドレッシングを必要とする。

1. ハードウェアの仕様と障害の許容範囲，および復旧手順の解析が与えられなければならない。
2. ＴＣＢはソース・コードのレベルに至る迄検証されなければならない。そしてＴＣＢのインプリメンテーションは常時呼び出すことのできる不当照合防止（tamperproof reference）の妥当性検査機構を含むことを示されなければならない。
3. その意味（semantics）を十分に，また形式的に記述するために，このインプリメンテーションは高いレベルの言語においてなされなければならない。次の段階では，抽象的形式的な設計と，低いレベルの仕様における形式化されたインプリメンテーションとの間に注意深い写像が施されねばならない。
4. ＴＣＢの設計に当っては信頼できる職員のみのグループと信頼できる環境が与えられなければならない。
5. 機密保護テストを行なうに当っては，そのテスト例のいくつかはＦＴＬＳあるいは形式的な低いレベルの仕様から自動的に生成されたものでなければならない。
6. 任意選択（optional）の機構には次のようなことが必要となるであろう。応用プログラムが基本的ＴＣＢによって実施されるのよりもさらに厳しい制限の機密保護の方針を実施することを許すような抽象的データのタイプあるいはその他の機構が与えられること。
7. 例：現在の技術の段階を越えている。

昭和５８年３月発行

発行所　財団法人　日本情報処理開発協会
東京都港区芝公園３－５－８
機 械 振 興 会 館 内
TEL （434）8211（代表）

印刷所　株式会社　正　文　社
東京都文京区本郷3－25－8
TEL （815）7271（代表）

57－S003