〔非公開〕

TR－C－0022

セキュリティ研究の現状

森住　哲也　　永瀬　宏
TETUYA MORIZUMI　　HIROSHI NAGASE

1988. 12. 6.

ＡＴＲ通信システム研究所

セキュリティ研究の現状

目次

1．はじめに

セキュリティの問題は，必ずしも世の中に十分に理解されていないが，問題意識は広く浸透しつつあるように思われる。これには概ね3つの理由があると考えられる。

第一に巨大システムの出現により，事故による損失が大きくなってきたことである。このため，事故に対する安全性（信頼性と言ってもよい）への要求は高い。この問題がクローズアップされたのは，1950年代後半から1960年代前半にかけて，米国でミサイル地下格納基地が4回に渡り，大事故を起こしたときだと言われている。[1] そして1961年，米空軍がベル研にミニットマンミサイルの制御システムの開発を依頼した際，はじめてフォールトツリー解析という手法があみ出された。1974年には米国原子力委員会がフォールトツリー解析を用いて，原子力システムの安全性をまとめたラスムッセン報告[2] を提出している。ただしこの報告書は数値の不確定性や統計学上の問題を指摘され，1979年にたな上げ状態にされた（その後の経緯は不明）。また最近ではスペースシャトルの爆発で，改めて安全性が意識されている。

第二は情報化社会の進展と共に，システムへのソフトウェアの比重が高まり，金銭に関わる犯罪が単なるデータの書替えで成立するようになったことである。このような犯罪により，企業が被る経済的，社会的損失が大きくなり，セキュリティ対策がコスト増を招くものの，一種の保険のような意義をもつようになっている。

第三はセキュリティ対策がビジネスとして，十分に成り立つようになってきたことである。証券会社のように情報処理システムのユーザであれば，安全なシステムを構築しているということはセールスポイントになる。また計算機のベンダであれば，ユーザのシステム，あるいは運用方法が安全かどうかを診断することが，有償のサービスとして現実に提供されている。

本資料は，コンピュータ犯罪等の主に人為災害に着目して，コンピュータシステムのセキュリティ対策はどうとられているか，またシステムの安全性評価はいかに行われているか，と言う点に関して，現在までの世の中の研究動向を調査したものである。セキュリティグループでは，既に暗号に関して研究動向の調査報告書をまとめており，今回の報告と併せて参照することにより，セキュリティ研究の全般が概観できるようになっている。

2．セキュリティの概要

2．1　セキュリティの概念

銀行オンラインシステムのように，端末とホストコンピュータがネットワーク化された一般的な通信形態において，セキュリティの問題を整理する。まずセキュリティが必要になるのは，システムに対する脅威が存在するからである。脅威には災害，故障，破壊，過失，不正使用がある。このうち，一般には馴染みの薄い不正使用については，トロイの木馬等がコンピュータ犯罪の手口として既に分類されている（3．4に詳述）。これらの脅威から保護すべきシステムの属性には，以下の4つが知られている[3]。

（1）可用性　　システムの利用が妨害されないこと。信頼性を維持できることと言ってもよい。

（2）完全性　　システムのデータが改ざんや破壊を受けずに，本来の処理した値を維持すること。

（3）機密性　　システムのデータが承認されていない開示から保護されること。

（4）システム資源　　システムの資源が無断で使用されないこと。

このようにシステムを保護するため，セキュリティ策が考えられている。セキュリティ策としては暗号（ＤＥＳ等），アクセス制御（パスワード等），業務形態上の対処（複式簿記等）が代表的である。セキュリティ問題とは，例えば商用システムにおいては完全性，軍事システムにおいては機密性等，それぞれの目的に沿うように暗号等のセキュリティ策を，脅威に照らし合わせながら選択していくことである。

2．2　米国の取組み

米国では暗号とコンピュータセキュリティについて，早くから標準化作業が行われているが，セキュリティへの関心が高いだけに，その成り行きは紆余曲折を経ている。まず暗号についてはＮＢＳ（米商務省標準局）が 1972年から標準化作業を開始し，1976年にはＤＥＳを連邦政府標準の暗号として採用している。これを受けてＡＮＳＩ（米国規格協会）は1981年，ＤＥＳを規格案として採用する。しかしレーガン政権の誕生と共に暗号標準化の主管が，米国防総省（ＤＯＤ）の情報収集機関であるＮＳＡ（米国家安全保障局）に移管され，ＤＥＳを非標準としてアルゴリズム非公開の暗号を開発する方針を打ち出した。これに対して全米銀行者協会が反発して，商用暗号の標準化権限がＮＢＳに復帰し，ＮＢＳは1988年以降もＤＥＳを連邦政府標準の暗号として採用する計画を発表して，今日に至っている。

一方，コンピュータセキュリティについては，ＮＢＳが1977年に検討を開始し，これを受けてＤＯＤ* が1981年，セキュリティレベルの評価基準を示した（＊現在はＮＣＳＣ—National Computer Security Center －に移管）。これはＴＣＳＣ（Trusted Conputer System Criteria）[4] と呼ばれる，詳細を極めたものであり，例えばＩＢＭのＲＡＣＦ

（資源アクセス制御管理機能）の評価には2年間の歳月を要したという[5]。それだけにＴＣＳＣで安全と評価されることは，社会的信用につながる。ただし従来はMultics のように安全性の高いシステムが，必ずしも商業的に成功せず，むしろＵＮＩＸのように手軽なシステムが普及しているようである。

商業ベースでは，ＥＤＰ部門に対するシステム監査が早くから普及しているようである。これは経済的被害を食い止める必要性に迫られたからであろう。現在，米国にはＥＤＰ監査人協会があり，この組織が世界レベルの最も権威ある監査法人となっている。

２．３　日本の取組み

我が国でもセキュリティへの関心は高まっている。通産省はシステムの運用上の安全対策を主眼とした，電子計算機システム安全対策基準，並びにシステム開発上の安全対策を重視したシステム監査基準をそれぞれ制定している。また郵政省も主に通信ネットワークの面から同様の安全対策基準を制定している。世の中の普及度という点では，システム監査人の資格試験を設けた，通産省の基準の方が知られているようである。

政府レベルとは別に財団法人金融情報システムセンター（ＦＩＣＳ）という組織があり，金融機関を対象としてシステム監査指針を作成している[6]。ＥＤＰの普及により，従来の会計監査が，よりシテム的な立場から実施されねばならない，という必要性に迫られてのことであるが，内容的には米国のシステム監査の中で我が国に必要なものを抜き出して出来上がったもののようである。

一方，暗号関連では国内標準を制定するというような，具体的な規定にまでは至っていない。米国標準の暗号に追従する限りでは，国防上の理由から使用を制限される恐れもある。一方，米国としてはＩＢＭの製品を売り込みたい，という事情もあり，ＩＢＭが開発したＤＥＳは，おそらく今後も我が国で使われ続けるであろう。いずれにせよ，国産メーカが不利益を被らないためには，継続的に暗号技術を向上しておくことが重要である。

２．４　国際機関の取組み

国際的にはＩＳＯ／ＣＣＩＴＴで，ＯＳＩ（開放型システム間相互接続）へのセキュリティ機能の組み込みが検討されている。７階層の各レイヤにいかなるサービス（アクセス制御や認証等）を，どのようなメカニズム（暗号等）で実現するかが標準化の主目的である。この場合，どの程度まで標準化が行われるかが注目される。欧州では暗号を標準化すると，その主導権を握る政府機関に情報が筒抜けになるという認識が根底にある[7]。このため米国標準のＤＥＳも信用しないという風潮があり，結局，具体的に方式名まで指定した標準化は行われていない。

3．コンピュータシステムのセキュリティ

3．1　米国防総省のセキュリティ評価基準

これは正式にはDepartment of Defense Trusted Computer System Evaluation Criteria と呼ばれ，1983年８月，公開された。通称，オレンジブックとも言い，コンピュータシステムのセキュリティ基準をはじめて体系的に整理したものである。この基準でＢ２クラスと高い評価を与えられた，Ｍｕｌｔｉｃｓの評価結果を表3.1 に示す。また先に述べたＩＢＭ社のＲＡＣＦ（資源アクセス管理機能）は表3.2 に示すように，並みではあるがＣ１クラスの評価が与えられている（セキュリティ機能が十分でないシステムはＤクラスに分類されている）。このような評価の相違は，表3.3 に示す評価基準のうち，機密保護方針への取り組みの違いから生じている。すなわちＭｕｌｔｉｃｓでは，リング保護と呼ばれる多階層のアクセス制御を実現している（強制的なアクセス制御）のに対して，ＩＢＭ社の製品はスーパユーザの区別こそあるが，ごく一般的なユーザ名やディレクトリ管理によるアクセス制御（任意のアクセス制御）を実現しているに過ぎないからである。

アクセス権限を階層的に整理すると，権限に明確な順序関係がある（ＡがＢより上位，ＢがＣより上位ならば，ＡはＣより上位）ため，機密の保護がしやすい。このため，軍のように厳格な組織階層のあるところへ応用するには，おそらく都合のよい方式である。しかし一方では，上位層への権限の集中がシステムの使い勝手を悪くすることもある。例えば下位層が上位層へのデータへアクセスすることは，しばしばあり得ることである。実際，Ｍｕｌｔｉｃｓもこの点に苦心しており，上位層と下位層の間に中間層を設けて，中間層の専用のエントリポイントから上位層へのアクセスを許容したりしている[8] が，システムの複雑化は避けられない。商用システムで多階層の保護が採られないのは，このような理由による。

表3.1　Multicsの評価結果

Honeywell Infomation Systems(HIS)社　Multicsの評価結果(1985年９月１日)。総合評価はB2

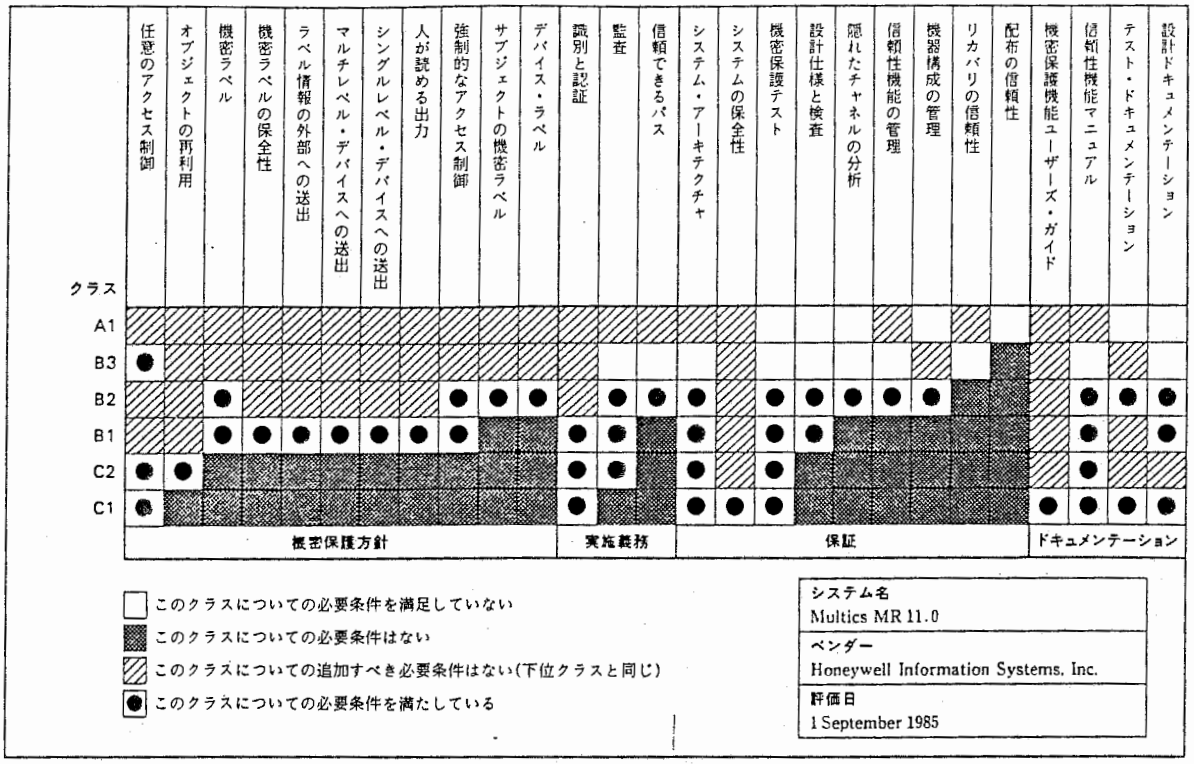

表3.2　RACFの評価結果

IBM社のRACFの評価結果(1984年７月23日)。総合評価はC1

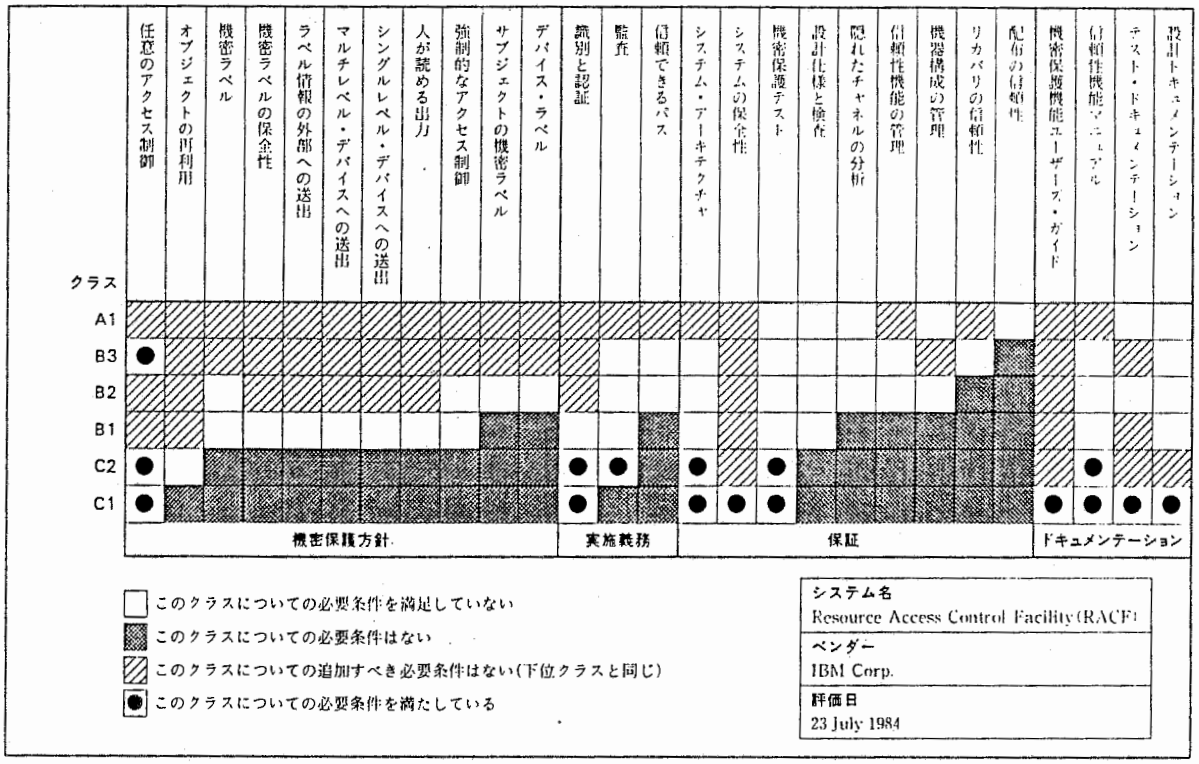

表3.3　米国防総省のセキュリティ評価項目

機密保護方針　(SECURITY POLICY)
任意のアクセス制御　(DISCRETIONARY ACCESS CONTROL)
— Ｃ１クラスでは，ファイルやプログラムへのアクセスを個人ＩＤやグループＩＤで管理すべきことを規定している。これはＵＮＩＸなど，通常のＯＳで実現されている機能である。さらにＢ３クラスになると，オブジェクト指向計算の考え方を採り入れ，アクセス制御リストによる機密保護を規定している。（システムアーキテクチャの項参照）
オブジェクトの再利用　(OBJECT REUSE)
— ＴＣＢ(TRUSTED COMPUTING BASE ：セキュリティ核）は許可されたサブジェクトにのみ，共通データにアクセスできるようにすることを規定している。
機密ラベル　(LABELS)
— ＴＣＢはプロセスやファイル等に，後述する強制的なアクセス制御ができるようラベルづけしなくてはならない。
機密ラベルの完全性　(LABEL INTEGRITY)
— サブジェクト（アクセスする側）やオブジェクト（アクセスされる側）に付与されたラベルと，ＴＣＢが管理するラベルは一致していなくてはならない。
ラベル付情報の外部への送出　(EXPORTATION OF LABELED INFORMATION)
— ＴＣＢはチャネルやＩ／Ｏデバイスをレベル指定でき，かつ状態監視できなくてはならない。
マルチレベル・デバイスへの送出　(EXPORTATION TO MULTILEVEL DEVICES)
— いかなるレベルのオブジェクトも扱えるチャネル，Ｉ／Ｏデバイスは，通信時に機密ラベルの整合性をチェックできなければならない。
シングルレベル・デバイスへの送出　(EXPORTATION TO SINGLE-LEVEL DEVICES)
— レベルの指定されたチャネル，Ｉ／ＯデバイスをＴＣＢが設けることもある。
人が読める出力へのラベル付け　(LABELING HUMAN-READABLE OUTPUT)
強制的なアクセス制御　(MANDATORY ACCESS CONTROL)
— サブジェクトとオブジェクトをクラス階層とカテゴリイの組合せで分類する。クラス階層については，サブジェクトは下位オブジェクトの情報しか読めず，またサブジェクトは上位オブジェクトにしか書き込めない。またカテゴリイについては同一カテゴリイ内のアクセスのみ許容する。Ｂ１クラスに規定されている。
サブジェクトの機密ラベル　(SUBJECT SENSITIVITY LABELS)
デバイス・ラベル　(DEVICE LABELS)
実施義務　(ACCOUNTABILITY)
識別と認証　(IDENTIFICATION AND AUTHENTICATION)
— ＴＣＢは個人の識別情報（パスワード等）を管理する。
監視　(AUDIT)

表3.3　米国防総省のセキュリティ評価項目（つづき）

信頼できるパス　(TRUSTED PATH)
保証　(ASSURANCE)
システム・アーキテクチャ　(SYSTEM ARCHITECTURE)
— Ｂ２クラスにおいて，セグメンテーション等により，最小権限の法則を実現すべきことを規定している。ただし任意のアクセス制御の規定と若干，整合しない。
システムの保全性　(SYSTEM INTEGRITY)
機密保護テスト　(SECURITY TESTING)
設計仕様と検査　(DESIGN SPECIFICATION AND VERIFICATION)
隠れチャネルの分析　(COVERT CHANNEL ANALYSIS)
— システム開発者はメモリやタイミング信号を使った違法通信を探索でき，かつこのような通信路（隠れチャネル）の容量を特定できなければならない。
信頼性機能の管理　(TRUSYED FACILITY MANAGEMENT)
機器構成の管理　(CONFIGURATION MANAGEMENT)
リカバリの信頼性　(TRUSTED RECOVERY)
配布の信頼性　(TRUSTED DISTRIBUTION)
ドキュメンテーション　(DOCUMENTATATION)
略

３．２　形式言語による記述と検証

米国防省のセキュリティ評価基準（通称，マルチレベルセキュリティとも言う）の策定と並行して，それを形式的に厳密に記述しようとする動きがある。Ｂｅｌｌ－Ｌａｐａｄｕｌａモデル[9]は，この基準の機密保護に関する部分，厳密には強制的なアクセス制御を形式化した，この分野で最も著名なモデルである。これは１９７６年，米国防省とも関係の深いＭｉｔｒｅ社から発表され，歴史的には当時，すでに一般の利用が可能になっていた，Ｍｕｌｔｉｃｓの機密保護方式（の一部）をモデル化したものである。ともかく米国防省の基準，Ｍｕｌｔｉｃｓ，並びにＢｅｌｌ－ＬａＰａｄｕｌａモデルは密接に関連しあっている。

Ｂｅｌｌ－ＬａＰａｄｕｌａモデルでは，アクセス主体であるサブジェクトと，アクセスされる側のオブジェクトと呼ぶ処理の実行単位がある。サブジェクトはオブジェクトを

ｒｅａｄ — 読み取りのみ
ｅｘｅｃｕｔｅ — 読み取りも書替えもなし
ｗｒｉｔｅ — 読み取って書替え
ａｐｐｅｎｄ — 書替えのみ

の４種類のモードでアクセスすると考える。サブジェクトS_iとオブジェクトO_jには，予め固有の順序づけられたレベルが付加されている。ｅｘｅｃｕｔｅアクセスについてはレベルの制限はないが，たとえばS_iがO_jをｒｅａｄアクセスするときは，S_iがO_jより上位レベルになければならない。S_iはｒｅａｄアクセスを繰り返すうちに徐々に機密データも保有するようになり，S_iのレベルは上昇していく（S_i自身のレベルを越えることはない）。ここでS_iが他のオブジェクトO_Kにｗｒｉｔｅアクセスするときは，S_iの現レベルがO_Kのレベルより，下位になければならない。

このようにＢｅｌｌ－ＬａＰａｄｕｌａモデルは，マルチレベルセキュリティを満たすということを形式的に記述したものであるが，さらにコンピュータシステムのアクセス制御則が，この基準を満たすかどうかを検証しようとする研究が１９７０年代に盛んに行われた。米ＭＩＴＲＥ社のＣｈｅｈｅｙｌ等は，１９８１年に代表的な形式言語のサーベイを行っている[10]。そのなかの一つである，スタンフォード研究所（ＳＲＩ）のＨＤＭ（Ｈｉｅｒａｒ－ｃｈｉｃａｌ　Ｄｅｖｅｌｏｐｍｅｎｔ　Ｍｅｔｈｏｄｏｌｏｇｙ）の例を以下に示そう。

ＨＤＭは図3.1 に示す構成をしており，図3.2 に示すように，ＳＰＥＣＩＡＬと呼ぶ言語で記述された，トップレベルの仕様を中間言語に落とし，マルチレベルセキュリティの基準に合致するかどうかを検証する。いまシステムのアクセス制御則を表3.4 のように仮定する。書込み，読出しの規則はマルチレベルセキュリティの基準そのものである。しかしこの規則だけでは書込みの度にプロセスレベルが低下する。もしプロセスＡの内容で書き換えられずに残っている情報があると，Ａより下位であった他のプロセスＢは，ある時点からＡより上位になり，Ａの残置情報を読み出せるようになってしまう。ここでもし表中の第３の機能であるリセットがＡに対して行われると，Ａのレベルは最上位となり，

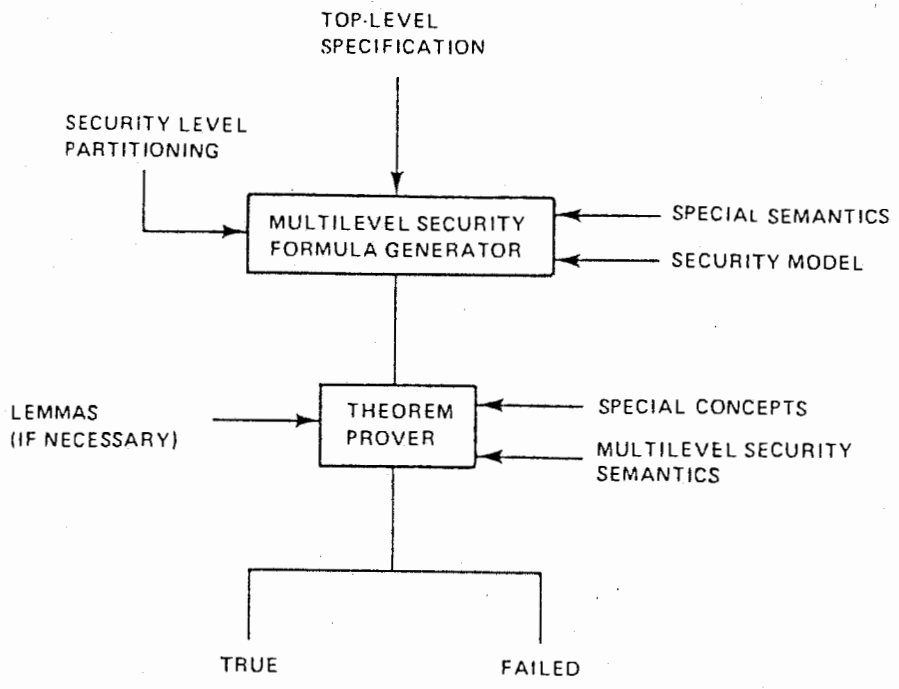

図3.1　Multilevel Security design verification in HDM

```
MODULE Top_Level_Module

    PARAMETERS

        BOOLEAN dominates (INTEGER a, b);

    FUNCTIONS

        VFUN Contents(INTEGER level) -> INTEGER val;
               HIDDEN;
               INITIALLY
                 val = ?;

        OFUN Write(INTEGER val) [INTEGER cur_level];
               EXCEPTIONS
                 EXISTS integer i:
                      ~dominates(i,cur_level) AND Contents(i) ~= ?;
               EFFECTS
                 FORALL INTEGER i | dominates(i,cur_level):
                      'Contents(i) = val;

        VFUN Read() [INTEGER cur_level] -> INTEGER val;
               EXCEPTIONS
                 Contents(cur_level) = ?;
               DERIVATION
                 Contents(cur_level);

        OFUN Reset() [INTEGER cur_level];
               EXCEPTIONS
                 EXISTS integer i:
                      ~dominates(i,cur_level) AND Contents(i) ~= ?;
               EFFECTS
                 FORALL INTEGER i | dominates(i,cur_level):
                      'Contents(i) = ?;

END_MODULE
```

Object レベルがProcess レベルより高くなかったとき，Objectのレベル は出力しない

ReadはObjectの値を返す関数．Process レベル ＞ Object レベルのとき読出す

Process レベル が低かったときは，そのレベルが何かは出力しない

図3.2 SPECIAL top-level specification

表3.4 Example System Summary

Operation	Access restriction	Effect
READ	Process level ≥ object level	Calling process receives contents of object
WRITE(data)	Process level ≤ object level	Object level set to calling process level; contents of object set to data
RESET	Process level ≤ object level	Object level set ≥ all process levels

このような不当な読出しを防ぐことができる。ただしこの場合，本来Aより上位であったプロセスCはAの内容を読み出せなくなる，という別の不都合が生じる。このように様々なケースを想定して，マルチレベルセキュリティ基準が満たされるかどうか，また，システムの運用条件が損なわれていないかどうか，といった検証が行われる。

ＨＤＭに用いられているＳＰＥＣＩＡＬは，ＳＲＩが仕様記述言語として設計したものであり，特にセキュリティを意識して考案されたものではない。ソフトウェア開発を目

的とした仕様記述言語が他の分野に用いられた例は多く，例えばＵＣＬＡのＳＡＲＡは通信システムのプロトコル検証に用いられているし[11]，クイーンズ大のデータフロー言語Ｌｕｃｉｄはセキュリティ評価に用いられている[12]。

実際，ソフトウェアの正当性検証，プロトコル検証，そしてセキュリティ評価は似たような側面を持っていると思われる。例えばべき乗のプログラムが意図通りに作られているかどうかを，Ｈｏａｒｅの記法を用いて公理的に正当性証明する，というような報告がある[13]。この証明ではいろいろな推論規則が使われるが，その中でプログラマーが無意識的に使っている数学の等式が証明の要になっている。同じような手法がプロトコル検証でも用いられている。シーケンス番号を用いる手順で，データの順序乱れや重複がないかどうかをｔｅｍｐｏｒａｌ　ｌｏｇｉｃを用いて証明する，という報告がある[14]。この中でも正しい伝送が行われるためには，送信側と受信側でシーケンス番号に関して，ある条件式が成り立たねばならない，ということが証明に用いられているのである。もう一つの例は，状態遷移モデルを用いたプロトコル検証とセキュリティ評価の関係である。この場合，状態の列挙が一つの技術的ポイントである点が共通している。

このように技術的な共通点があるということは，ある意味では自然な結果といえる。すなわち，マルチレベルセキュリティのように，要求条件が単純で，かつ対象システムの動作も読み書きによるレベルの変化しか考えなくてよい場合は，検証内容も明確であり，プロトコル検証に近い性格を帯びてくる。一方，プログラムの意味的な正当性検証が一般に難しいように，セキュリティ評価においても，正規の担当者による不正のように，実行主体の権限上に問題はなくても，処理の内容に問題がある場合は，異常状態の列挙自体が難しくなる可能性がある。現時点ではここまで踏み込んだ研究はあまり，見当たらない。

ここで今日のコンピュータ資源保護のもう一つの話題である，ケーパビィリティ・アーキテクチャについて触れておく。これは大雑把にはオブジェクトを単位にアクセス制御をするというものであり，米国防総省の基準で言えば任意アクセス制御，Ｂ３クラスに相当する。このアーキテクチャではオブジェクト毎にアクセス可能なオブジェクトの集合が規定でき，かつアクセス権限の変更やオブジェクトの生成が自由に行われる。このため各オブジェクトが相手オブジェクトに正当にアクセスしていても，オブジェクト間のアクセス関係を辿っていくと，意図しないアクセスが可能になっていることがあり得る。

ケーパビィリティ・アーキテクチャにおいて，各オブジェクトが自分の意図するオブジェクトにしか参照されていない，ということは如何に保証されるであろうか。この問題は単純には，束論（順序関係）の上に成り立つＢｅｌｌ－ＬａＰａｄｕｌａモデルを，集合論の上で言い直せばよい。問題はケーパビィリティ・アーキテクチャ上で動くプログラムを作成したとき，安全性の検証が静的に（コンパイル時に）行えるかどうかである。この点については，ｔａｋｅ－ｇｒａｎｔモデルと呼ばれる，特殊なモデルを除いて，一般のケーパビィリティ・アーキテクチャでは安全性が静的には決定不能であることが証明されている[15]。このためプログラマに負担を負わせることなく，安全にシステムを動作させるには，処理実行時のアーキテクチャ・サポートが必要となる。しかし今日のケーパビリティ・アーキテクチャでさえ，性能低下が取り沙汰されており，ここまで徹底したアーキテクチャはまだ出現していない。

3．3　情報フロー解析

これまでに述べたアクセス制御はオブジェクト単位の制御であったが，これに対して個々の変数毎に情報の受け渡しを制御しようとする研究がある。これはｉｎｆｏｒｍａｔｉｏｎ　ｆｌｏｗ　解析と呼ばれており，階層的アクセス制御についてはある程度，成功している[16]。基本的な考え方はＢｅｌｌ－ＬａＰａｄｕｌａモデルと同一であるが，プログラム中の個々の変数を階層づけていること，変数の値まで考慮していること，並びに間接的な情報の伝播も制御対象としている点が異なる。これらの意味を具体的な事例により説明する。

いまプログラムの文（ステートメント）の一般形を

$$\nu := f(u_1, \ldots u_n) \qquad (3.1)$$

とするとき，$u_1, \ldots u_n$ には各々，現実行時点での機密レベル$\underline{U}_1, \ldots \underline{U}_n$ が付与されている。ｆの実行結果は，これらの機密レベルの最高のもの，すなわち

$\underline{U}_1 + \ldots + \underline{U}_n$　　；　＋は束のｌｅａｓｔ　ｕｐｐｅｒ　ｂｏｕｎｄ

なる機密レベルを有する。一方，各変数には予めどのレベルの変数値までは受け取っていいかが決められている。例えば変数νの許容レベルがＮとすると，

$$\underline{U}_1 + \ldots + \underline{U}_n \leq N \qquad (3.2)$$

ならば，νに実行結果を代入してもよい。

以上の手続きはプログラム証明で用いられる，Ｈｏａｒｅの記法で記述することが提案されている。例えば代入文，ｙ：＝ｘ＋１でｘの初期値が$0 \leq x \leq 4$のとき，

$\{0 \leq x \leq 4, \underline{X}\}$　　$y := x + 1$　　$\{1 \leq y \leq 5, \underline{Y} \leq \underline{X}\}$　　(3.3)

となり，$\underline{Y} \leq Y$　が成り立っていれば，安全ということになる。ここでわざわざ変数値を示したのは，プログラムには条件分岐があるからである。例えば

ｉｆ　ｘ＝１　ｔｈｅｎ　ｙ：＝１　　(3.4)

が実行されるかどうかはｘの値に依存する。変数の初期値が与えられていれば，上記のように変数の値域が定まるので，実際に起こりうる状況に照らした検証ができる。もう一つ(3.3.4)で注意すべき点は，これが間接的な情報の伝播を実現していることである。すなわち，ｙ＝１か否かでｘ＝１か否かが推定できる。このようなケースも含めてｉｎｆｏｒｍａｔｉｏｎ　ｆｌｏｗが解析される。

ｉｎｆｏｒｍａｔｉｏｎ　ｆｌｏｗ解析は変数毎に機密レベルを検査している点で，徹底した解析法と言える。従ってオブジェクトの中に，不正なプログラムが紛れ込んでいるトロイの木馬のようなケースでも，一つ一つ機密レベルを検査すれば不正アクセスを防止できる可能性がある。一方，変数値まで考慮するには，実際の計算にほぼ等しいことをコンパイル時に行う必要があり，計算量が膨大になる。さらに外部入力がある場合は，コンパイル時には（全ての予想される入力を列挙しない限り）実際の計算をシミュレートできないという問題がある。また機密レベルを階層づけせずに，ケーパビリティシステムのように，個々にアクセス可能な集合として定義することも考えられるが，この場合，検証に要する計算は極めて煩雑になると予想される。

3．4　コンピュータ犯罪

コンピュータ犯罪の実態は幾つかの報告書から，間接的ながら伺い知れる。その一つは，１９８２年，米国ＳＲＩが米国法務省の依頼を受けて調査したものであり，コンピュータ犯罪の分類とその対策が表3.5 のように述べられている[17]。これによると，現実の犯罪は金銭にからむものが多く，そのような犯罪が成立するのは正当な権限を持つ人が担当業務を遂行する上で不正をする，というケースが殆どである。このことはｓｅｃｕｒｉｔｙ　ａｎｄ　ｐｒｉｖａｃｙ国際会議において，米国の銀行関係者も指摘しており[18]，セキュリティ対策の難しさの一端を示している。

表3.5　コンピュータ犯罪の手口

（1）破壊：　物理的に破壊する。オペレータによりファイルが持ち出される。これに対する有効な技術的手立てはなく，人事管理などで対処せざるを得ない。

（2）便乗と仮装：　電子ロックドアで正規の人に便乗して入室する。銀行員を装ってパスワードを入手する。これも決め手となる対策はなく，個人の意識に負うところが大きい。

（3）データ改変：　正当な権限を持つ事務員が勤務時間計算詐欺を行う。これは応用サイドで業務権限を分離したり，相互監視して対処する。

（4）スーパーザッピングと屑拾い：　緊急時プログラムの特権を利用して預金操作する。石油会社がテープに残した地震データを転売する。対策としては特権の範囲や運用方法で規制する。相互監視も有効である。ファイルは暗号化し，残存データが一括消去できるようにする。

（5）盗聴：　マイクロウェーブを傍受する。これは暗号化や多ルート化等により，技術的に対処できる。

（6）トラップドア，トロイの木馬，資源の無断借用，サラミ：　正規のプログラム（試験用プログラムなど）に不正なプログラムを忍び込ませて，データ用記憶領域に制御権を移行させる。不正なプログラムをパブリックドメインに配布する。使用頻度の少ないＩＤからアクセスする。端数切り捨て犯罪をする。これらはアクセス制御で対処する。

（7）非同期攻撃，論理爆弾，シミュレーション：　予め予備コピーを改ざんしておいて，故意にミスを発生させる。時限付で預金口座に振り込ませる。システム動作をシミュレートしながら，小切手詐欺をする。これらは個々のケースについて，システム設計段階から，漏れを防止する。

このように応用プログラムにまで立ち入らないと防止できないような不正は，ユーザの責任において対処する必要がある。コンピュータシステムのベンダが提供するのは，一般的なセキュリティ機能のみである。従って高価なセキュリティパッケージを購入したか

らといって，必ずしも安全という訳ではない。これが原則的なユーザとベンダの責任分界であるが，それでもベンダは可能な限りにおいてセキュリティ機能を強化しようと努力している。例えばＩＢＭ社では自社製品を導入したユーザに対して，システム管理者（ＳＰＥＣＩＡＬユーザ）とは別に監査担当者を置くことを勧めている。そして監査担当者にはＩＢＭ社が提供するＲＡＣＦ（資源アクセス管理機能）がユーザシステムで十分に機能しているかを検査できるように，数々の監査コマンドが準備されている[17]。その主要な機能はコンピュータ資源への不正なアクセスについて，ログをとることである。ロギング自体は通常の機能であるが，以下のように疑わしき対象を重点的に監視できるようなコマンド構成となっている。

（1）コマンド違反のような徴候に基づいて，特定のユーザの行動を詳しく追跡する。これにより，重大なシステム資源（ＯＳの一部の機能）や，高度に機密性のあるユーザ資源（給与データなど）を許可なしに修正を試みるようなことが発見できる。

（2）ハッカーなどがまず興味を示しそうな，ある種のコマンドについて許可されていない者が使用することがあるかどうかを監視できる。ＲＡＣＦコマンドはまさにこのようなコマンドの一つである。

（3）システムの運用や管理にあたる特権ユーザには，当然のことながらほとんど全ての資源へのアクセス権限が付与されるが，ＲＡＣＦではこれらのユーザをむしろ注意深く監視することが重要と考える。監査担当者はこれらのユーザの活動のログを入手することができ，これをもとに資源アクセスが正しい理由に基づいているかどうかを検討することができる。

さて今日，業務用の大型計算機がハッカー等の攻撃を受けた，という報告は殆ど聞かない。しかし運用形態が開放的な研究施設や，個人のワークステーションでは，被害の事例が多い。図3.3 にＵＮＩＸシステムへの不法侵入の手口を分類して示す。これは日経のセキュリティ特集雑誌に紹介されていた記事[5] をもとに，フォールトツリーを作成したものである。この記事は米国のセキュリティコンサルタントが執筆しており，世の中への悪影響を考慮して，詳細な手順は故意に省かれているが，パスワードを盗み出すトロイの木馬を仕組んだり，プログラムをあたかも物理的なメモリデバイスのように扱う，といった手口が含まれている。

最近ではコンピュータウィルスが，話題性に富むことから，マスコミにしばしば取り上げられている。一説によると，ＵＮＩＸで名高い，Ｋｅｎ　Ｔｈｏｍｐｓｏｎが１９８４年のＡＣＭのチューリング賞受賞講演で，ベル研で過去に行われていたゲームの公開を行ったことが引金になったということである。興味深い話であるので，調べてみると，自己増殖プログラムとトロイの木馬の例が載っていた[20]。

図3.4 はＣ言語で書かれたプログラムであり，コンパイル，実行されるとソースプログラムのコピーを出力する。また図　は同じくＣ言語で書かれたコンパイラであり，トロイの木馬が仕組まれている。このうちｂｕｇ１で例えばパスワードを盗み出すソースプログラムをコンパイルする。次にｂｕｇ２は図3.5 に述べた手法により，ｂｕｇ１の仕組まれたソースをもとの正常なソースプログラムに置き換えるプログラムをコンパイルする。ｌｏｇｉｎコマンドのプログラムが，この不正なコンパイラにより，コンパイルされると

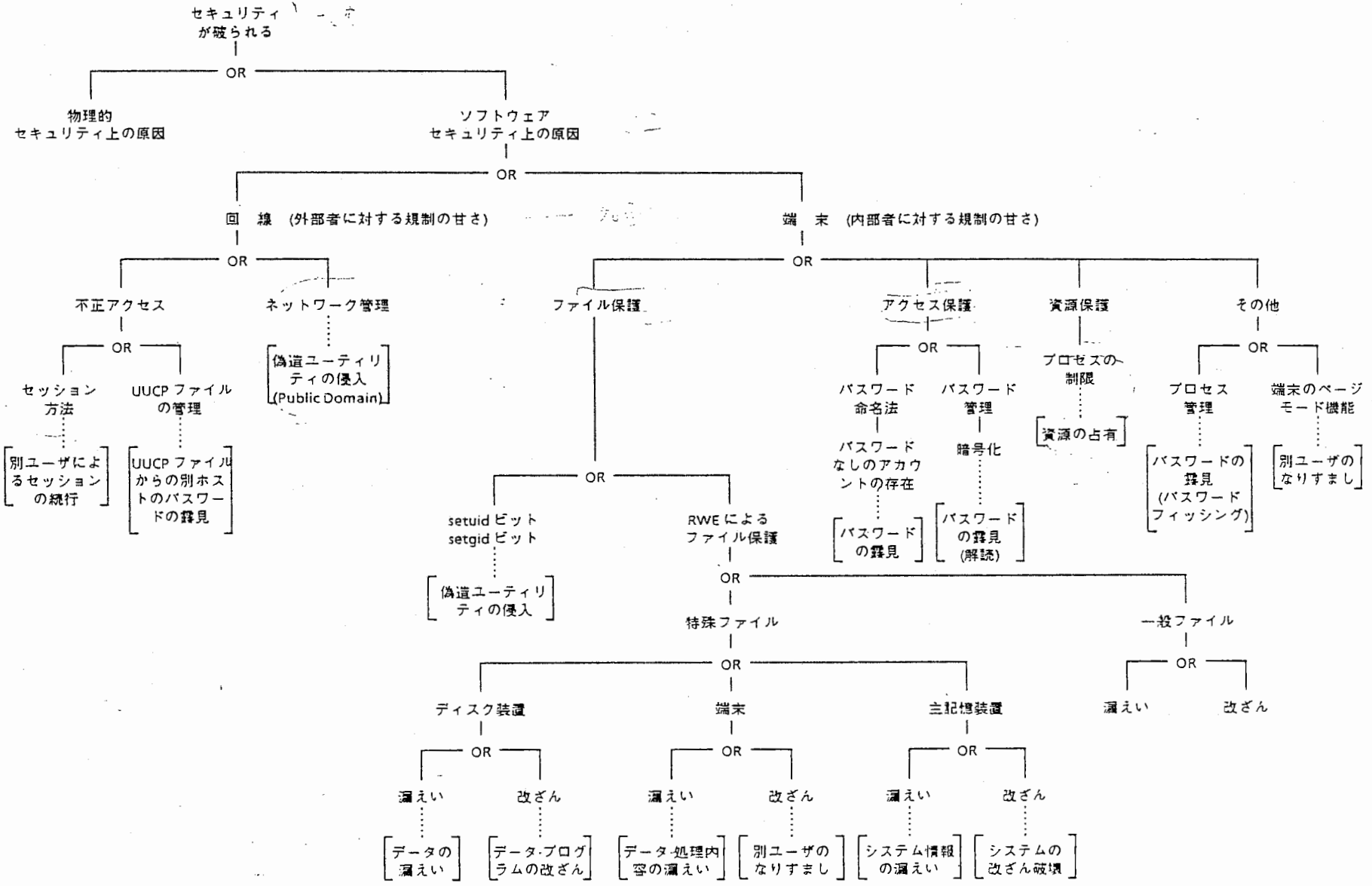

図3.3　ＵＮＩＸシステムへの不法侵入の手口

パスワードを盗み出す実行形式でありながら，ソースプログラムでは何ら異常が認められないという事態が発生する。このような不正を防止するため，暗号技術を応用する動きもあるようである。詳細はさらに調査する必要があるが，筆者は一種の内容認証技術が適用できるのではないかと考えている。

```
char s[ ] = {
        '\',
        '0',
        '\n',
        '}',
        ';',
        '\n',
        '\n',
        '/',
        '*',
        '\n',
        (213 lines deleted)
        0
};

/*
 * The string s is a
 * representation of the body
 * of this program from '0'
 * to the end.
 */

main( )
{
        int i;

        printf("char\ts[ ] = {\n");
        for(i=0; s[i]; i++)
                printf("\t%d, \n", s[i]);
        printf("%s", s);
}
Here are some simple transliterations to allow
    a non-C programmer to read this code.
=       assignment
==      equal to .EQ.
!=      not equal to .NE.
++      increment
'x'     single character constant
"xxx"   multiple character string
%d      format to convert to decimal
%s      format to convert to string
\t      tab character
\n      newline character
```

図3.4 自己増殖するプログラム

```
compile(s)
char *s;
{
        if(match(s, "pattern1")) {
                compile ("bug1");
                return;
        }
        if(match(s, "pattern 2")) {
                compile ("bug 2");
                return;
        }
        ...
}
```

図3.5 トロイの木馬の仕込まれたプログラム

4．　セキュリティ評価技法

4．1　リスク・アセスメント

システムがどの程度の損害を被り得るかを予測することは，セキュリティ評価の基本的な考え方であり，これをリスク・アセスメントという。広義には定性的，定量的な評価が共に含まれるが，狭義には損害額の期待値を計算することとして，一般に理解されている。

昭和６０年に発表された，日本情報処理開発協会の『コンピュータ・セキュリティに関する―リスク分析調査報告書』[21]によれば，わが国企業のリスク分析への取組み方には以下のような特徴がある。

(1) リスク分析の実施率は低い。
(2) 問題点は，「確立された手法がない」ことである。
(3) 実施者は情報システム部門要員であり，リスク分析が組織的に行われていない。
(4) 損害額の予測はあまり行われていない。
(5) 損害額予測の算定基準の設定はごく稀である。
(6) 予測損害額は，コンピュータ犯罪を１とした場合，エラーは0.048,地震は14.5，火災は12.7である。
(7) 情報システムの価値を評価しているのは，全体の約1/5 である。
(8) 情報システム，情報およびプログラムの価値評価の方法は，次の通りである。

表4.1　情報システムの価値評価

システム規模＼項目	直接コストから算定	効果で算定	感覚的に捉えている	その他
５０億円未満	４０．９%	３０．７%	２０．５%	８．０%
５０億円以上	２９．４%	６７．６%	０　%	２．９%

表4.2　情報およびプログラムの価値評価

システム規模＼項目	直接コストから算定	効果で算定	感覚的に捉えている	その他
５０億円未満	５９．７%	１３．３%	２１．４%	５．６%
５０億円以上	８０．０%	１２．０%	０　%	８．０%

このうち，(8)の価値評価に関する調査結果は興味深い。これによれば，規模が５０億円未満のシステムあるいは情報，プログラムの価値は，感覚的に把握できるらしい。一方，大規模になると効果やコストから算定する必要が生じてくる。詳細な調査によると，システム規模が１００億円以上の場合，そのコスト程には実体的な価値観が伴わない，という傾向があるらしい。このため，大規模システムではその効果（システムが世の中に与える効用）を定性的に評価することが，しばしば行われている。その具体的手法までは把握しきれていないが，この方面の研究にとって注目すべき事実である。

４．１．１　リスク・アセスメントの手順

リスク・アセスメントの標準的な手順というものは存在しない。そこで世の中で行われている手法を組み合わせて，手順化した例を示す。

(1) 脆弱性の列挙　：　予想しうる損害（脆弱性）のリストアップ
(2) シナリオ作成　：　損害にいたる経緯のストーリ付け
(3) 順位の決定　　：　どのシナリオが重要かの経験に基づく順位付け
(4) 安全対策の列挙：　導入可能なものの主観的な列挙
(5) 損害額の分析　：　実際的な安全対策が見出し難い脆弱性を対象とする，損害額の査定
(6) 最終順位決定　：　どの安全対策が重要か，また安全対策を施した状況でいかなる脆弱性がクローズアップされるかの判定

以下ではこのうちの幾つかの手法について説明する。

４．１．２　シナリオ分析

シナリオ作成で用いられる主観的な手法であり，安全性評価のための補助手段となる。そのプロセスは，まず主要な脅威源を対象に数種類のシナリオを書く。これにはどの様な損害がいかに起こりうるかが書かれている。次にこれを組織の管理者に対し，提示する。管理者はシナリオを検討し，シナリオが実際的で信頼のおけるものであるかについて意見をまとめる。最後に信頼すべき実用的シナリオが集められる。これには組織にとって重要な資産がどの様な脆弱性を持っているかが示されている。

４．１．３　危険度分析

順位の決定で用いられる簡易な定量化手法である。危険度を算定する実際的な数理統計データはたいていの場合なく，推定に頼り過ぎると，結果は信頼の置けないものとなる。そこで，確率が充分な信頼度で求められない時，損害発生の確率を割り出す手段として，損害を引き起こす可能性のある人数をベースとした危険度分析を行う。即ち，資産に対して特定の職種に属する人員が及ぼす脅威をその行為別に査定する。この方法は組織内の人事関係が明らかな場合に効果的回答を導くことができる。更に脅威に結びつく行為の動機，或いは偶発的か意図的かを考える必要が無い利点がある。但し，このような様々な可能性を持つ人々

を分類出来ない様な場合にはこの方式は無効である。

4．1．4　コートニーのリスク分析[22]

損害額の分析で用いられる手法である。1977年にIBM 社のロバート・コートニーが提唱したリスク分析の定量的方法で，生起した脅威を基にしてそれによる損害を予測評価するものである。1 年間に発生する脅威の予測頻度Ｐは，

$$P = 10^{(q-4)} \quad 〔\ \text{損害件数/ 年}\ 〕 \qquad (4.1)$$

から概算される。但し，qは表4.3 に示すとおりである。

表4.3　脅威発生頻度

q = 0	実質的にゼロの場合
1	1,000 年に1 度の場合
2	100 年に1 度の場合
3	10 年に1 度の場合
4	1 年に1 度の場合
5	1 ケ月に1 度の場合 (10 回/ 年)
6	1 週間に2 回の場合 (100 回/ 年)
7	1 日に 3 回の場合 (1,000 回/ 年)

脅威発生１件当たりの損害額は，10^{V} 〔ドル〕（但しＶは査定値）と表され，1年当たりの予想損害額Ｅは，

$$E = 10^{(V+q-4)} \quad 〔\ \text{ドル／年}\ 〕 \qquad (4.2)$$

で計算される。この方法は数年にわたる損害額データを必要とする為作業量が大きくコストがかかる。従って，潜在的損害が高く重要度の大きい評価対象に適用すべきである。適用に際しての注意点は，リスク分析を多角的なセキュリティ評価の一つの要素として位置付ける事，経験豊富なセキュリティの専門家による査定を行うべきである事が挙げられる。こうした基本的要求が満たされていないと，大量且つ詳細に過ぎるデータが作られ時間と労力の浪費となり，また主観と客観が入り混じった信頼度の低い結果が導かれる可能性がある。

4．1．5　FMEA (Failure Mode and Effects Analysis)[23]

損害額の分析で用いられる手法である。この方法は，定性的評価方法であり故障モード等の質的評価をシステム故障の原因側からシステム故障すなわち結果側へと帰納的に解析するものである。

数学モデルを定式化するのではなく，システムの要素間の機能的関連に着目して，故障やエラーが全体の信頼性や安全性にどう影響するかを技術的に評価する。着目点は，故障の

影響（E），故障の頻度（P），対策の難易，対策時間のゆとり（τ）であり，それぞれ大まかな評価を行う。その手順は，あらかじめ用意した表に評価点を書き込んでいくもので，あらましは，

(1) ブロック・ダイヤグラムでシステムと部分の関係を明らかにする。
(2) 部分に発生する故障モードをデータから整理する。
(3) 考えられる故障原因を挙げる。
(4) 故障発生頻度（ 相対頻度ランク付け ）P のおおよその値を調べる。
(5) システムに対する影響度のランク E によって格付けする。
(6) 対策余裕時間，τ あるいは対策難易性のランク付けを行う。
(7) 致命度評点ランク付け C（ E,P, τの総合評点)を行う。
(8) 故障検出方法の改善を考える。
(9) その他の情報（ 信頼度，保全度，保全方法など ）

である。致命度C は相対的な量であり，絶対評価ではない。このように解析を行い，最もCの大きな故障モードを見出し，対策をたてる。表4.4 に E, P, τの評価点の一例を示す。

表4.4　E, P, τの評価

ランク		影響度　E
1	9 ～10 点	Catastrophic
2	6 ～8	Major
3	3 ～5	Minor
4	1 ～2	Insignificant
ランク		頻度　P
1		きわめて起こりやすい
2		起こりやすい
3		時々起こる
4		ほとんど起こらない
ランク		対策の余裕時間　τ
1		余裕なし
2		対策時間短い
3		対策時間長い
4		対策時間制限なし

4．1．6　フォールト・ツリー解析[24]

損害額の分析で用いられる手法である。複雑なシステムの解析をするために，始めにシステムの故障に関する要素間の関係を大局的に理解する。信頼性ブロック・ダイアグラム，FMEAはその一例である。また，要素間の論理的結合に着目したダイアグラムもしばしば必要になる。この様に，システムの故障に関する動作を把握した後，フォールト・ツリーによる詳細な解析が行われる。

まずフォールト・ツリーの定性的評価は，特定の故障を表す事象をトップ・イベントとし，演繹的分析手法を用いてこの発生原因となる事象を分析し，次々とブール代数によって結合して，分析不可能な基本事象（ベーシック・イベント）までを論理ダイアグラム（AND，OR）を用いて（図4.1 ）簡単な論理によって解析する。

定量的評価はトップ・イベントの事象の確率を計算する事によって成される。但し．入力する事象は，独立であるとする。この仮定がフォールト・ツリー解析の適用性をどの程度まで制約しているのかは明らかでない。

フォールト・ツリー解析に於けるトップ・イベントの事象の確率は，トップ・イベントをベーシック・イベントのブール代数による演算によって表現し，これを縮約して多項式にまとめて求める。図4.1 の例では，top event A1は，basic event A2 ～ A6 を用いて，

$$F_{SYS}(A1) = P(A2 \cdot A3 + A4 \cdot A5 + A4 \cdot A6) = 0.3 \qquad (4.3)$$

となる。

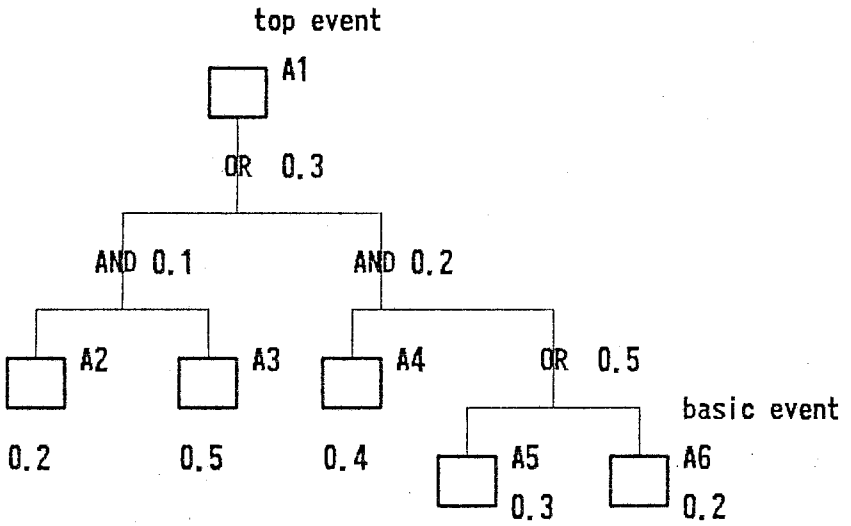

図4.1　フォールト・ツリー解析

フォールト・ツリー解析は，ツリー作成に最も手間がかかると言われている。このため化学プラントでは，流量，圧力等のシステムの内部状態に着目して，状態が異常に変化するのはいかなる理由か，また状態が変化するとどのような事故が起こりうるか，という手順で解析することが行われている。これをオペラビリティ・スタディと言う[25]。

フォールト・ツリー解析のもう一つの問題点は，ツリーが大規模になることである。例えば１８本のリンクからなるグラフで，ある２点間にいかなるパスも存在しなくなる確率を

計算しようとすると，$2^{18}=262144$個の場合が生じる。このときは，概念的にツリーをイメージすることができても，実際にそれを書き下すことはできない。一般に基本事象が数百から数千に及ぶツリーでは，トップ・イベントの生起確率の下限値と上限値を求めるという考え方がある。例えば最小カットセット（トップイベントが生起するのに必要最小な基本事象の組）を幾つか求めて，生起確率の和を計算すれば，それが下限値を与える。先のグラフの例では，フォールトツリーの全体こそ書けないが，カットセットを幾つか数え上げることは可能である。もう一つの手法はモンテカルロ法である[26]。これは，基本事象に対応して，〔0，1〕区間の乱数を発生させ，その乱数が基本事象の生起確率より小さければ，事象が生起したと考えて，トップ・イベントの生起確率を計算するものである。基本事象の生起確率が小さいときは，計算値の分散が大きくなって，精度が悪くなるため，分散を減少させる研究が行われている。

4．1．7　イベント・ツリー解析[27]

損害額の分析で用いられる手法である。イベント・ツリー解析は帰納的手法を用いて故障の引金となる事象，初期事象から出発し，いろいろなシーケンスを経て，さまざまな可能なアクシデントに至るまでのシナリオ（事故波及）を明らかにするものである。図4.2 に示すように，システムの過渡的な内部状態が安全か事故を起こすかという，二値の状態によって分岐していく。ツリーのルートから各リーフへ至る事象のシーケンスはアクシデント・シーケンスと呼ばれ，このシーケンスの集合が初期事象から派生する可能なアクシデントを表す。また各アクシデント・シーケンスには，その発生確率が，条件付確率として付随する。図4.2 に於いては，シーケンスの確率は，それぞれ $P(S_2/S_1I)\cdot P(S_1/I)\cdot P(I)$，$P(F_2/S_1I)\cdot P(S_1/I)\cdot P(I)$，$P(S_2/F_1I)\cdot P(F_1/I)\cdot P(I)$，$P(F_2/F_1I)\cdot P(F_1/I)\cdot P(I)$ となる。

，イベント・ツリー解析の問題点は，情報システムなどの事故波及を記述する上では，事故と通常動作が多数混在し，記述が困難になる程大きなツリーになり，且つ修正，追加が難しい事である。

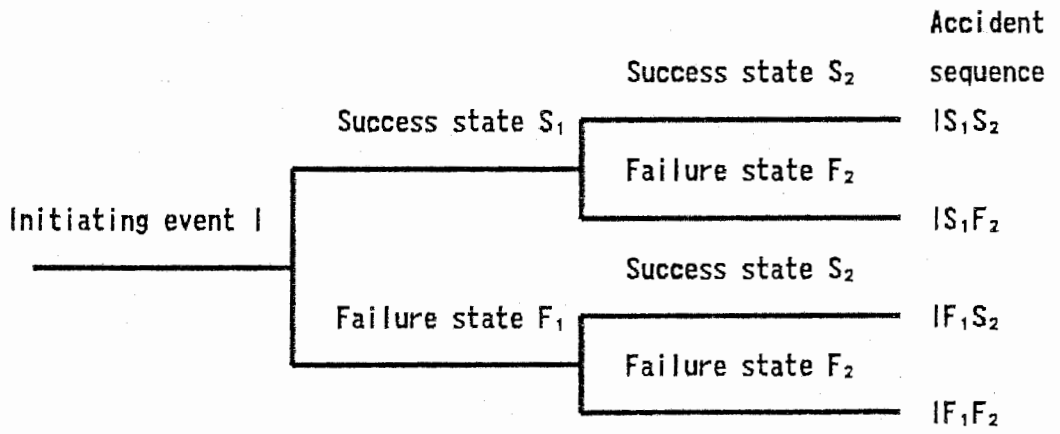

図4.2 イベント・ツリー解析

4．1．8　シーケンス・ツリー解析

損害額の分析で用いられる手法であり，日立が開発中のセキュリティ評価技法 [28] で提案された。実際に事故が起きてしまったとき，その影響がどう波及していくかを解析するものであり，一例を図4.3 に示す。機能的にはイベント・ツリーに近いが，製品として事故シナリオの各事象を紙面を有効に使える様なツリー・ウォークを採用しているので，イベント・ツリーに比較してシナリオの追加，削除を行いやすい，という特徴を有している。

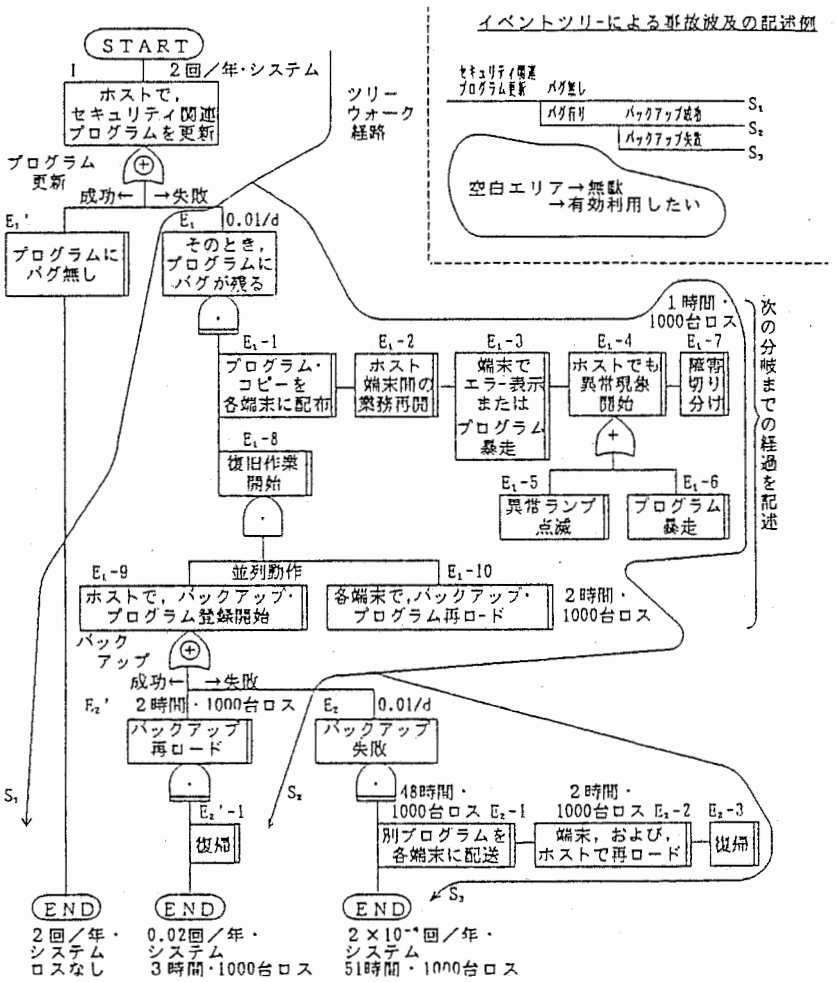

図4.3 シーケンス・ツリーによる事故波及の分析例

4．2　システム監査 [28] [29] [30]

コンピュータ利用をめぐる問題点の主なものは次のような点がある。

(1) コンピュータ利用の効果把握の必要性
(2) コンピュータ犯罪の発生
(3) エラーの影響を与える範囲が拡大
(4) コンピュータに対する破壊行為の発生
(5) プライバシー保護の必要性

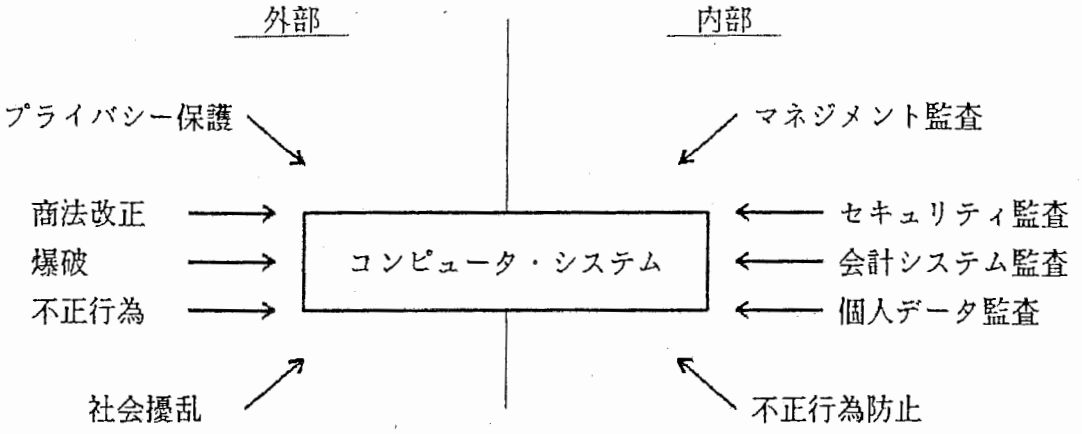

図4.4　システム監査の考え方

(6) 会計処理をめぐる会計監査の問題
(7) ネットワークをめぐる問題
(8) データ・ベースをめぐる問題

この様な問題に対して，システム監査を実施する基本は，企業単位でコンピュータの知識が豊富なシステム監査人によるシステム監査を行い，合理的な問題解決をはかることである（図4.4 ）。この基本に従って，システム監査の目的は，『コンピュータ部門とは独立した客観的な立場でコンピュータ・システムの企画，開発，運用に於ける管理を総括させることによって，全体的な整合性や有効性の高い，総合的な管理・保護対策を実施出来る体制を整え，トップ・マネジメントをサポートする事』　と設定されている。

システム監査を実施するに当たっての着眼点及びチェック・ポイントの一例としては，日本情報処理開発協会が，昭和51年 3月に発表した，「わが国におけるシステム監査のあり方」でとりまとめられているものがある。まず，着眼点の基準は，一般基準，品質基準の2点であり，それぞれ，準拠性，採算性，適時性，生産性及び，安全性，信頼性，機密性の観点からとらえる。具体的なチェックポイントは，システム機能上のチェックポイントとマネジメント上のチェックポイントがあり，前者の重要な機能としては，コントロール機能，セキュリティ機能，プライバシー保護機能があり，後者は承認，標準化，ドュメンテーション，スケジューリングに着目する。適用基準とチェックポイントの関係を表4.5 に示す。

また，昭和60年 8月には通産省の『システム監査基準』が公表され，この中で実施に当たっては，『電子計算器システム安全対策基準』を活用することが，留意事項として挙がっている。これは，項目と対策項目，対策内容ごとのランク付けからなっている。

対策内容は，自然災害，システム構成要素の障害，不法行為等によって生じるシステムダウン，誤動作，不正使用，及びデータの漏洩，破壊，改竄を未然に防止し，発生した場合は，影響の最小化及び回復の迅速化を図るための措置を網羅したものとなっている。

対策内容のランク付けは，基本基準（C基準），標準基準（B基準），強化基準（A基準）の3段階となっている。ランクの分類は，安全性，信頼性等の向上度，対策に必要な資金の額等を勘案の上決定され，基準は，A，B，Cの順に対策が強から弱へと設定される。基準の適用に当たっては，すべてを用いる必要はなく，情報処理システムの適用業務によっ

表4.5　適用基準とチェックポイント

チェックポイント ＼ システム監査実施の際の適用基準		品質基準			一般基準			
		安全性	信頼性	機密性	準拠性	採算性	適時性	生産性
機能	コントロール		◎	○	○			
	セキュリティ	◎	○		○			
	プライバシー		○	◎	○			
マネジメント	承認	○	◎	○	○	○	○	
	標準化		○		○			◎
	ドキュメンテーション		○		○			◎
	スケジューリング						◎	○

◎最も重要な関連を示す
○二重マルに次ぐ重要性を示す

て重要視すべき項目を選択し，監査を行う。表4.6 に電子計算機システム対策基準に於けるチェック項目を整理しておく。

この様に，システム監査は基準が公表され，各方面で注目されて現在に到っているが，実際に導入し，実施している企業はまだ少ない。普及の妨げになっている理由は，①システム監査不要論などの誤解，②監査をする人材がいない，③実施方法が分からない，等と言われている。この問題をもう少し，技術的に言うと，

(1) 内部統制方策が不十分　監査は内部統制と切り離すことが出来ないものであるが，個々の企業が内部統制の在り方を如何に把握しどの様に設定すべきかが明らかになっていない。

(2) 監査基準の実務への応用方法が不明　基準を基にして，必要な項目の選択，検証の手法，検証の重点が実務上の観点から明確になっていない。

(3) チェックリストが検証出来ない　項目の漏れ，ムダの検証の手段がない。

(4) チェックリストの活用法が不明　何をどう調査し，結果を如何に分析すれば良いかが明らかでない。

(5) 監査の技法・ツールがない　現状では監査人を支援するシステムが確立していない。

表4.6　電子計算機システム対策基準

設備基準	技術基準	運用基準
Ⅰ．建物 1．立地及び環境 2．建物の位置周囲，利用形態 3．構造 4．開口部 5．内装等 Ⅱ．電子計算器室及びデータ等保管室 1．位置及び配置等 2．開口部 3．構造，内装等 4．設備 5．什器，備品等 Ⅲ．電源室及び空気調和機械室 1．位置及び配置 2．開口部 3．構造 4．設備 5．電源設備 6．空気調和設備 Ⅳ．監視制御	Ⅰ．信頼性向上機能 Ⅱ．データ保護・不正使用防止機能	Ⅰ．管理体制 Ⅱ．入退管理 1．入館，入室資格の付与 2．入退館管理 3．入退室管理 Ⅲ．電子計算器システムの運用管理 1．標準化 2．運転及び確認 3．管理 Ⅳ．データ及びプログラム（ドキュメントを含む）の保管管理 Ⅴ．電源設備，空気調和設備，防災設備及び防犯設備の管理 Ⅵ．監視 Ⅶ．外部委託 Ⅷ．教育訓練 Ⅸ．システム監査

ということになる。

これらの問題点が現実にどこまで解決されているかは，さらに慎重な検討を要する。一部の企業，例えばＩＢＭ社はシステム監査をビジネスとして実施しており，独自にユーザの

ためのセキュリティチェックリストを作成している。また本報告の2．に述べたように，金融機関の立場からのチェックリストも公開されている。事務処理の分野において，これらのチェック項目がいかなる意味を持つのかを，もう少し形式的な立場から記述する，ということは興味ある研究課題である。

監査ツールに関しては，表4.7 に示すような手法も報告されている[31]。この中で，例

表4.7 システム監査ツール

システム監査の目的 ＼ システム監査のツールまたは手法	監査領域の選定	職務の分割・手続の評価	手順の遵守性の評価	監査データの選択監視	監査データの分類	プログラム機能テスト	プログラム・ロジックの分析	備考
1 監査領域選択法	◉			○	○			複数場所の組織に適用する手法
2 シミュレーション・モデリング法	◉							（実例は少ない）
3 得点法	◉							（実例は少ない）
④ 内部統制質問書	◉	◉	◉					
5 トランザクション選択法				◉				
6 組込み監査データ収集法	○		○	◉				オンライン・システムのデータ抽出に有効な手法
⑦ 汎用監査ソフトウエア			○	◉	◉			パッケージ能力は拡大中，オンライン，データベースにも適用できるものあり。
8 複数現場用監査ソフトウエア			○	◉	◉			分散処理システムに適した手法
9 監査ソフトウエア実行センター	○		○	◉	◉			分散処理システムに適した手法
⑩ テストデータ法			○			◉		
11 基本事例システム評価法		○	○			◉		大企業に適した手法
⑫ 併行オペレーション			○	○	○	◉		
13 統合テスト法（ＩＴＦ）	○		◉			◉		
⑭ 併行シミュレーション			◉	○	○	◉		
⑮ 手作業およびコンピュータによるトレーシング			◉				◉	（現状では手作業分に力点をおく場合が多い）
16 スナップショット			○				◉	
17 コード比較法			◉				○	
18 コントロール・フローチャート法		◉					◉	
19 ジョブ・アカウンティング・データ分析法	○		◉					
20 災害テスト		◉	◉					
21 システム開発に使用するコントロール・ガイドライン		◉	◉			◉	○	大企業に適した手法
22 システム開発ライフサイクル法		◉	◉			◉	○	大企業に適した手法
23 システム検収と統制のグループ		◉	◉			◉	○	大企業に適した手法
24 導入後監査法		◉	◉	○	○	◉	○	

1. 監査ツール・手法のNoに附した○は使用頻度の高いものを示す。
2. システム監査の目的中◉は主要な目的，○は副次的な目的を示す。

（「システム監査概論」富山茂，情報処理研修センター，（財）日本情報処理開発協会）

えばテストデータ法は架空のユーザを作って検証するもの，併行オペレーションは一つの機能を別に作って，２重処理してチェックするもの，コード比較法は先月末決算と当月決算を比較するものである。上述した形式言語による検証は，システムを観察して，モデリングする立場であるが，監査ツールに挙げられている手法は，どちらかといえば実システムについてデータ収集する，という立場が多い。これを見る限りでは，ただ一つの万能な検証法というものはなさそうである。

４．３　曖昧，不確実性理論を用いたセキュリティ評価支援システム

４．３．１　セキュリティ評価支援システムの基本概念

（１）　セキュリティ問題に対するアプローチ

セキュリティ問題は，２．１節で規定した様に，セキュリティ策を脅威に照らし合わせながら重みを付け，選択して行く事である。この問題に対して，従来より上記で説明した手法が用いられて来たが，補うべき点が多い。そこで，まずセキュリティ問題の解法と非常に関連が深い保全についての体系と問題点を文献[32]より引用して概説し，我々が試みようとするアプローチの参考とする。保全とは「運用可能状態を維持し，または，故障などを回復するためのすべての処置および活動」とされ，管理面からその体系は，図4.5 の様に分類されている。

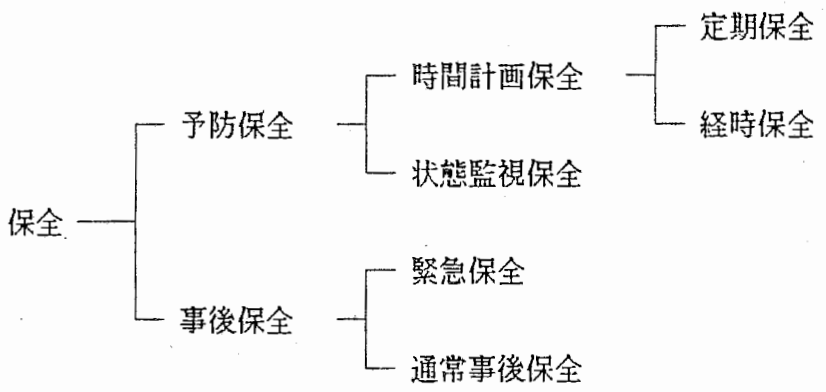

図4.5　保全の分類

これらの実施の基礎にはORなどによる研究成果がある。時間計画保全は，確率論に基づいた数理的な解析により，状態監視保全は，マルコフ決定過程を利用した解析成果が使われる。また，高信頼度設計に限界がある複雑システムでは，事後保全の重要度が増し，障害耐性の要請に伴う障害の早期発見，隔離，早期回復を意図したプログラムが開発されている。これらにより，管理の自動化が行われつつあるが，これらのアプローチは「固定された」モデル内での状態の「回復」を目的としており，数理的な解析結果ではモデルの妥当性が，自動

化では事前の保全方策の確立がそれぞれ前提となっている。

しかし，現実の複雑システムでは，人間の予測限界と認識限界によるモデルとの差異により不確実性が生じこれらの前提が曖昧になってくる。

文献[32]では，そういった不確実性に伴う問題点を，『適応保全』によって解決しようと試みている。これは，保全モデルやそれに基づく保全システムを自己改善するメタ的機能であり，「大規模，複雑だから故に，失敗は不可避であり，むしろ致命的でない小さな失敗から学ぶことが大切である」という経験的な認識に基づいている。そして，故障でなく「失敗」の概念を用い，失敗から得られる効果的な学習による，問題の解決を狙っている。更に，意思決定モデルを利用して，その機能の集合論的表現が試みられている。意思決定のゴールは，サイバネティクスによる動的解析が行われる。

この様なシステムの複雑化に伴って生ずる問題に着目した保全の解析は殆ど無く，　文献[32]が初めてと言って良い。

さて，不確実性により生じる問題点を学習により解決する事は，セキュリティの評価法として今後，我々が対象とする研究課題に於いても重要な事項であると思われる。しかし，その前に解決すべき問題，即ち，セキュリティの表現の問題，及び総合評価の問題がある。そこで，以下にこれらの問題解決のアプローチに対する森住の主張を述べ，次にそれに基づいた解決方法と関連した理論を解説する。

（2）　セキュリティの表現と評価法の在り方

セキュリティ評価は，社会や人間に関連した問題であり，多くの場合，不確実性が存在する。第一は，観察されるデータまたは，証拠に付随する不確実さであり，第二は，表明された知識に付随する不確実さである。従って，評価する対象の明快な記述が困難であるという問題がある。

不確実性を陽に認めてセキュリティを考えると，必然的に絶対的評価は不可能であり，相対的評価（時間的，空間的に）と言う概念が必要になる。

また，この問題は組織の管理，運用に深く関わるものであり，これを解決するには，よりマクロな総合的扱いが可能である必要がある。そのためには，専門家による高度，且つ定性的判断が有効に活かされなくてはならない。更に，評価システムを使用する人間との親和性を持たせるには，評価結果が容易な形で記述されなくてはならない。この様な要求を満たす一つの手段として，曖昧さを伴った自然言語による記述等，定性的な特性に対処できる方法論が考えられる。

以上より，不確実性，相対的評価，曖昧性，総合的扱いなる四つの概念は，セキュリティ問題の解決法にとって不可欠ではないかと考えられる。

しかし，危険と表裏一体の関係にある安全性に関する問題を，不確実性，曖昧性を含めた形で記述し，評価して良いものかどうかと言う問題及びその効果，或いは永瀬による，「柔らかな評価を実践するファジィ理論等の手法が，計算を複雑にしたり，曖昧さを増幅する可能性が有る事の指摘」については今後更に研究して行く必要がある。

次に，上記の概念の，セキュリティ問題に於ける意義を，もう少し明確，且つ定性的に論じておく。

（3）不確実性，曖昧性の意義

物理学では不確定性原理によって，原子核の周りの電子は確率的にしか表現できない。そのアナロジーとして，自然言語の持つ曖昧さに関しても，言語の意味の核があり，曖昧な意味が取り払われることなく，必然的に核の周囲に存在するものであるとする立場がある。安全性に関わる問題もそのように扱うべきであろうか。

この問題を扱うモデルを構成するには，二つの立場がある。一つは，データさえ集めれば問題は全て数学モデルに従って，数理的処理で解決できるというもの，あるいは，非計量的で感覚的なデータを集め，統計処理し評価モデルを作ろうというものである。これは，逆に言い換えればデータがある程度集まらないと解決できないとも言える。もう一つは，対象の客観的且つ正確な評価をするよりも，不確実，或いは曖昧なものを含んだままで，意思決定の支援を重視するシステムを構成するものである。

ところで，安全性を評価する場合，特に人間が関わる問題になるとデータが集まらない事象が多い。しかし，システムは組織の管理者がめざす目標に向かって効率良く，かつ危険を回避して動かなくてはならない。また，この様な場合は現実には専門家の主観判断が重要である。例えば証券会社のファンド・マネージャーは，株に関する統計データのみで売買しているわけではなく，自己の経験に基づく主観判断を行っている。

また，現実の社会を見ると数学的に完全無欠で人間が依存できる安全評価システムなどと言うものはこの先あり得ないし，またあるべきでない様に思える。なぜなら，危険はいくらでも新たに生まれるものであるし，また，人間は独自の価値感を以て，時には，あえて危険に対し，意識的に立ち向かう事もあり，その時の決断は人間が自分自身で行うべきだからである。つまり，システムの安全性に関しては，その評価を評価システムに一任するのではなく，最終的には組織を動かす人間の判断によって成されなくてはならない。

しかし，大規模で複雑なシステムの評価は人間の能力を越えるものであるから，人間が行う評価を，支援するシステムが必要である。すなわち，支援システムは，安全性に関する問題点を整理し，場合によっては判断結果の代替案を優先順位を付けて，提示するようであれば良い。

そこで，システムの安全性評価のためのコンセプトをこの考えに基づいて設定し，不確実，或いは曖昧な事象を含んだままの形で安全性を評価できる意思決定支援システムのモデルを作り，それをインプリメントして人間の主観的判断を支援できる様にする。こうすることによって，その支援システムは，企業の運営や国家の防衛等を行う現場にとって役に立つもの，つまりはその存在の意義の大きなものになると考える。

（4）総合的扱いについて

コンピュータ・セキュリティに要求される事項は，可用性，完全性，機密性，システムの資源の損失となっており管理，運用に関わる問題である。従って，その解決のためには，多くの技術的要素（暗号，認証，アクセス制御etc.）の下地がある上で，結局は人の管理が決め手になるとする意見がある。

また，文献[3]によれば，コンピュータ・セキュリティの計画のための前提条件は，

1) セキュリティは，人間の問題である。
2) 人を通じて解決される。
3) 経営の問題である。

と指摘している。

この前提からセキュリティ問題を扱うと，問題の対象に曖昧性が含まれること，単一の技術のみによる解決が困難であること（学際性）という理由から，従来は技術的な内容を含まない経営戦略的な方法論による解決法を取る以外にはなかった。では，この観点からのアプローチでは技術の入り込む余地がないのであろうか。

この点に関しては，上記の前提条件を基礎に，人の問題，個々の技術の問題を総合的に判断する事を支援する技術が注目される。即ち，コンピュータ・システムのセキュリティの問題に対して，既に述べた意思決定支援システム（知識処理による）を研究し，セキュリティの総合的な判断の支援を目的に，これを実用化して行く必要があるのではないかと考えている。

この問題を研究していく上では，システム工学に於けるシステム的思考法が重要である。システム的思考とは，問題を大局的に把握して，合目的性ということを旗印にして，すべての要素を合理的に組み合わせるというものである。この思考法の中で特に重要で，問題解決モデルとして参考になるものを文献[32]より抜粋する。

・トータル思考 —— 目標をレベルによって階層的に分割し，直面している問題を常に一段上の目標レベルから眺める。そうすることによって全体像が理解でき，独善に陥るのを防止できる。

・階層構造 —— サブシステムを１つのシステムと見做せば，それをまた分割し，合成を考えることによって，より詳細な分析や合成を行うことができる。これは，サブシステムを階層的に積み重ねることで，いわば縦方向の分割である。縦方向には思考が逐次的に行われるので，横方向の分割とは違い，分割数に制限はない。人間の理解を助けるためには構造グラフを用いて視覚を通した直感に頼るのが良い。

・代替案とその選択 —— システムの創造は，代替案とその案出とその選択という形で行われる。これは，評価と密接に関わっている。以上の思考法を基にして，セキュリティ問題の意思決定支援機能を，新たに次のように規定する（図4.6）。

(1) 問題を階層的に構造化することを支援する。これは，始めにセキュリティ問題を一般化した形で階層化した知識を持つ必要がある。

(2)　問題に対する代替案を評価することを支援する。この機能は，評価体系モデルに於いてなされる。

(3)　人間の持つ価値感を，知識として蓄積する。この機能は，価値体系モデルに於いてなされる。

(4)　価値体系と評価体系を効果的に結合するインタフェース系の機能。

以上の機能を実現し，総合的な問題解決支援を行うシステムの構築を目指す。

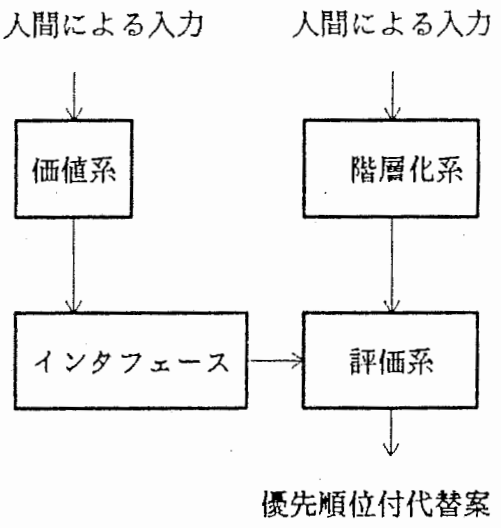

図4.6　意思決定支援機能

4．3．2　セキュリティ表現に関連する理論

（1）概要

図4.7 に，関連する理論と今後の研究課題を織り混ぜて示す。セキュリティ評価支援システムのモデルは，不確実性，曖昧性，相対的評価，総合的評価といった基本的概念を基にして，それらの正当性の検証を試みつつ，作られて行くべきである。

セキュリティの表現については，セキュリティを如何に計量化するかという問題と，如何

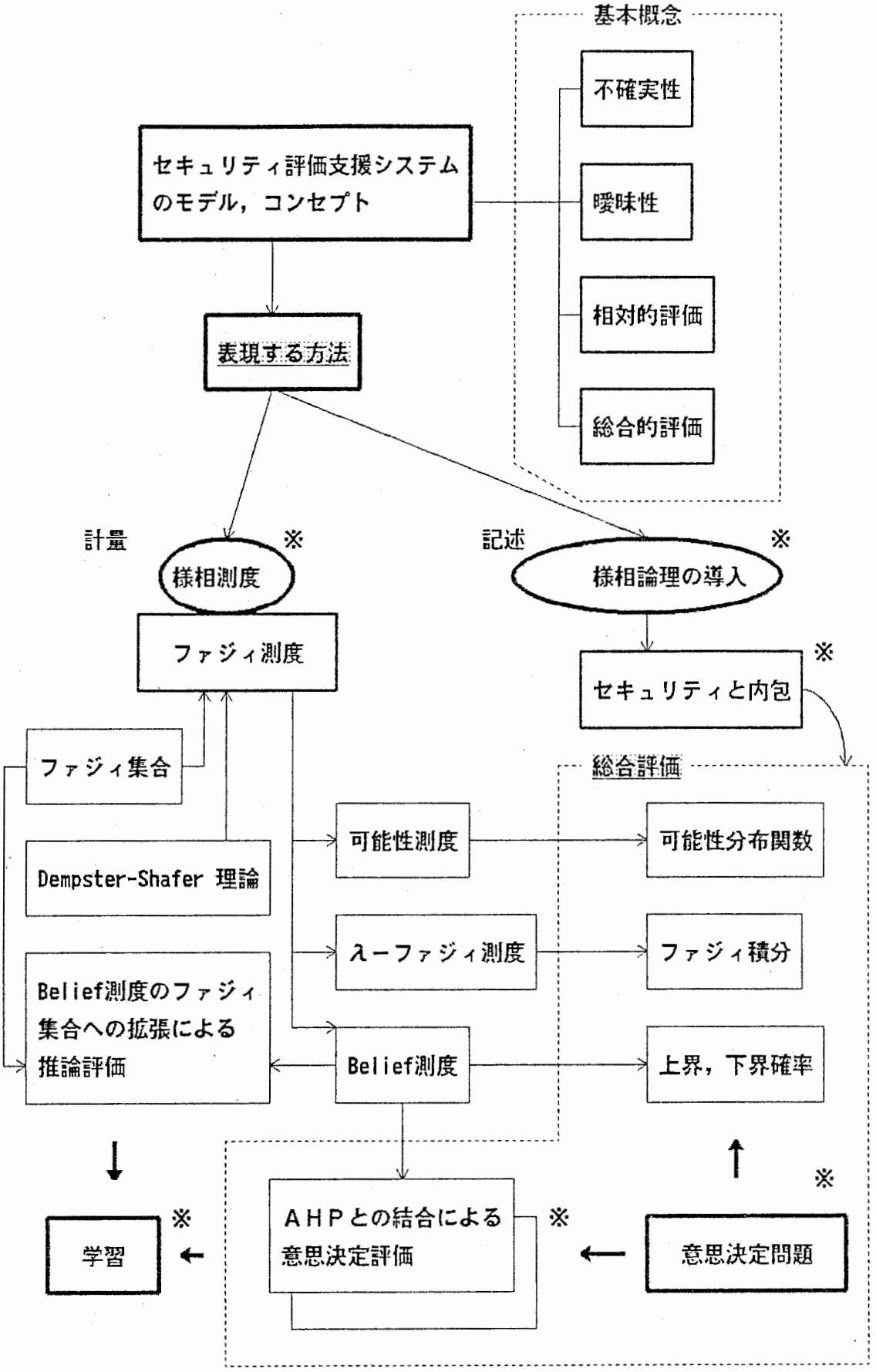

図4.7 関連理論，研究課題(※)

に論理的に記述するかと言う問題に分割される。計量化は，主として測度の問題として，ファジィ測度と，セキュリティの様相との関わりがテーマとなるであろう。ファジィ測度には，可能性測度，λ－ファジィ測度，Belief測度等ある。これらの基礎理論は，測度論，ファジィ集合論，Dempster-Shafer 確率理論がある。

記述の問題は，様相論理の適用の可能性が興味あるテーマであると考える。様相論理は，古典論理に必然，偶然，時間，可能等の様相を導入し，記述能力の向上を計ったものである[34)-39)]。その理由を説明する。様相概念の可能な命題の世界を真偽，及び必然と偶然に着目して　表すと，図4.8 の様になる。つまり真なる命題は，たまたま真と，必ず真の二通りの

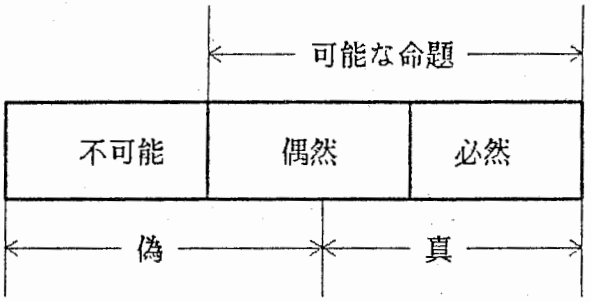

図4.8 様相概念の命題の真偽

解釈が成り立つ。これは，情況に応じて真偽の間を変化する命題の表現法であると言える。例えば，必然演算子□を用いて，□Aが真なる命題は，あらゆる情況，あらゆる世界において真である事を意味する。つまり様相論理では，いくつもの可能世界なる概念を導入し，その中で成立する論理を展開する。

そこで安全を表す言語表現の持つ概念と，物の世界の対応を，内包と外延の関係と見なし，安全という要素の概念と，物理的条件，時間的推移によって作られる可能世界を様相論理によって結び付けられるのではないかと考えている（図4.9)。例えばこれは，安全を時相的

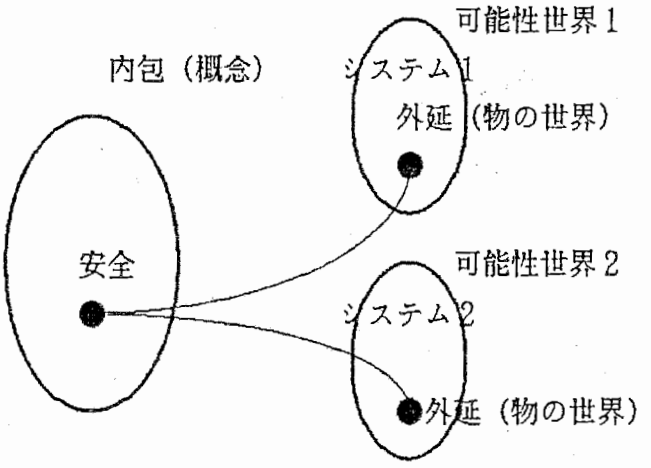

図4.9.　安全性の可能世界

に見れば，安全性という概念の指す物が，物の世界で，時間と共に技術の進歩等で，安全性の条件が変わり（可能世界が変わる），異なる物を指す様になるという事例に対応する。

もう一つの中心的課題である総合評価の問題は，ファジィ測度の表現法である可能性分布関数，ファジィ積分，上界，下界確率等を用いた意思決定問題と見なすことができる。意思決定方式としては，確率測度，又は,Belief 測度を測度として用いた Analytic Hierarchy Process（以後ＡＨＰと記す）がある。これは，曖昧性を含んだ問題を総合的に扱う上で効果的と思われる。これとセキュリティの間の関係の研究テーマは，まずセキュリティを階層化した問題と見なせるかどうかに関する点，更に，どういった測度を用いるのが良いかに関する点等が挙げられる。

最後にFig.4.6.2 で，この研究の最終的課題として，学習による意思決定支援の方向を示唆する。これは，曖昧性，不確実性を含んだ事象を扱うためには，試行錯誤とその結果のフィード・バックの過程が重要と思われるためである。

（2）ファジィ集合

ファジィ集合では曖昧性（ ambiguity ）を扱っている。ある集合Ｘのファジィ集合Ａとは，Ａの要素ｘについて，メンバシップ関数η（ｘ）が，

$$\eta\ (x)\ :\quad X \rightarrow [0,\ 1] \tag{4.1}$$

と定義されている集合をいう。ファジィ集合に於ける基本的な演算，包含関係，和集合，積集合は，メンバシップ関数によって次の様に定義される。
ファジィ集合Ａ，Ｂに関して，

・包含関係　$A \subset B$　：　$\eta_A(x) < \eta_B(x)$　(4.2)

・和集合　$A \cup B$　：　$\eta(x) = \max[\ \eta_A(x),\ \eta_B(x)\ ]$　(4.3)

・積集合　$A \cap B$　：　$\eta(x) = \min[\ \eta_A(x),\ \eta_B(x)\ ]$　(4.4)

ファジィ集合は，自然言語の持つ意味的な曖昧さを表現したり述語論理の非人間的な論理性を和らげるのに適している。つまり，セキュリティ専門化の主観的知識を自然言語的に表現する場合等に効果がある。表4.8 にファジィ理論の適用例の傾向を示すために国際ファジィシステム学会が1985年に会員に対して行ったアンケート調査結果を示す[40]。

マシンシステム	マンシステム	マンマシンシステム
画像，音声の認識	人間信頼性モデル	医療診断
漢字の認識	認知心理学	検査データ処理
自然言語理解	思考・行動モデル	輸液コンサルテーション
知能ロボット	官能検査	エキスパートシステム
農産物認識	民衆の意識分析	ＣＡＩ
プロセス制御	リスクアセスメント	ＣＡＤ
生産管理	環境アセスメント	最適計画
自動車，列車運転	人間関係構造	人事管理
安全・保安システム	需要動向モデル	開発計画
故障診断 [41]	エネルギー分析	設備診断
電力系統運用	市場選択モデル	品質評価
ファジィコントローラ	カテゴリ分析	保健システム
家電機器制御	社会心理学	ヒューマンインタフェイス
自動操縦		経営意志決定支援
		多目的意志決定支援
		知識ベース
		データベース

表4.8　研究中，或いは研究が予測されるテーマ

曖昧理論を用いた評価システムとしては，ホフマン，マイケルマン，クレメンツ [42] によるセキュリティ評価分析システムの発表例がある。これは，システムの安全性を評価する場合に，結果を自然言語表現するという目的でファジィ集合を導入したものである。

その構成は，objects，threats，features から成っており，セキュリティ・システムの設計に於いて，セキュリティの強弱を決定したり，或いは強弱の比較を支援する事を目的としている。ここで，

OBJECT : 脅威に曝されている資産。
　　損害額によって査定される。　　(loss value)
THREAT : 脅威。生起する程度で査定される。(likelihood)
FEATURE: 脅威に対する保護対策　　(resistance)

である。システムの構成を図4.10に示す。各集合は，ファジィ集合であり，変数は自然言語 (very high，high，somewhat low，low ，etc.) で与えられる。評価値はファジィ集合の上の演算によって計算される。

ユーザは，まず始めにセキュリティの観点からobjects-threats-featuresを評価システムに入力しておく。次にセキュリティに対する自分自身の見解についての質問事項に答える。最後に，システムは評価関数を計算してセキュリティの程度を自然言語による表現法で評価し，結果を出力する。

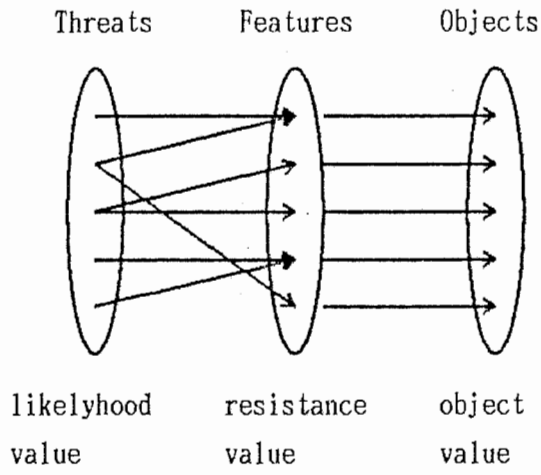

図4.10　basic security system

(3) Dempster-Shafer の理論

Dempster-Shafer の確率[43]は不確実性(uncertainty)，即ち Bayes確率で効果的に扱えない無知量(ignorance) を表現できる。従って，事象自体が正確に分からない場合，事象を取り巻く環境が変動する場合，主観に関わる不確実性を扱う場合に適用できる。

Bayes 確率では，無知量を効果的に扱えないという点を説明する。Aを何らかの状況の信用を表す命題であるとする。P(A) を命題Aが真であるという程度を表すとれば， P(A) ＜ 1 であれば．これは，信用の欠如(lack of belief)の程度を表し，P($\bar{A}$) は不信用 (disbelief)の程度を表す。Bayes 確率では，P(A) ＋ P($\bar{A}$) = 1 であるから，P(A) あるいはP($\bar{A}$) のどちらかが決まればもう一方はその値によって定まり，主観的な不確実さを表す上で適当でない。例えばAを暗号方式が安全であるという命題であるとすると，暗号が安全であるという程度P(A) がその根拠の少なさから0.3 であるからといって，暗号が破られる程度が0.7 であるとは限らず，やはり証拠の少なさから0.4 であるかもしれない。例えば，計算量による強度評価では評価したアルゴリズムより良いものがあるかもしれないという事を否定できない不確実な要素がある。

Dempster-Shaferの確率論では，不確実性を扱うために上界，下界確率を用いる。これらは次に定義する基本確率によって表される。

基本確率mは，A_0 を有限集合，A_i をその部分集合とすると，

$$m : 2^C \rightarrow [0, 1], \quad \text{但し，} C = A_0 \tag{4.5}$$

で定義され，

$$m(\Phi) = 0 \qquad (\phi \text{は空集合}) \tag{4.6}$$

$$\Sigma m(A_i) = 1 \qquad (i = 0, 1, 2, \cdots, N) \quad (4.7)$$
$$A_i \subseteq A_0$$

なる性質を持つ。A_i は焦点要素と呼ばれる。図4.11に基本確率のイメージを示す。
ここで，｛a1, a2, a3｝等は，それぞれの事象の同時確率を表す。もし，a1 ～a6 まで

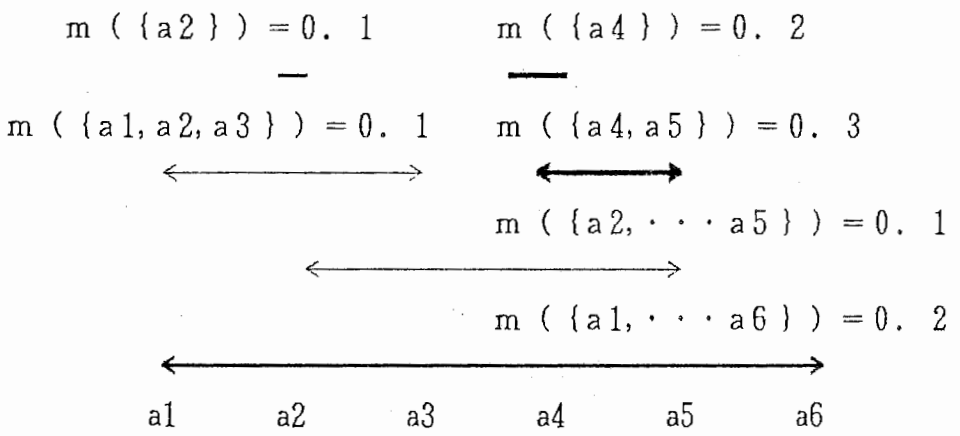

図4.11　Dempster-Shaferの基本確率のイメージ

の組合せ事象の，ベイズ確率の意味での生起確率が与えられるとすれば，それらの総和は1でなくてはならない。従って，Fig.4.3.8 のように全ての組合せが尽くされていない場合は，ベイズ確率では，

$$\sum_{i=1}^{6} m(A_i) \neq 1$$

但し，
$A_1 = \{a2\}$
$A_2 = \{a4\}$
$A_3 = \{a4, a5\}$
$A_4 = \{a1, a2, a3\}$
$A_5 = \{a2, \cdots a5\}$
$A_6 = \{a1, \cdots a6\}$

となってしまう。ところが，式(4.7) では一部の事象で，全ての生起事象が言い尽くされるとしている点が，ベイズ確率と異なる。これは，基本確率を形作る事象は，ベイズ確率に於ける事象の様に確信の持てる数値ではなく，異なる証拠の基では違った値になる事を想定している。Dempster-Shafer確率では，この様に事象間に跨がる基本確率を基に次に示す上界，下界確率を定義する。

焦点要素A_i に閉じ込められた基本確率の和を，下界確率$P_*(A_i)$ とし，

$$P_*(A_i) = \sum_{A_j \subseteq A_i} m(A_j) \quad (4.8)$$

と定義する。上界確率$P^*(A_i)$ は，少しでもA_i 内に入る可能性のある基本確率の総和であり，

$$P^*(A_i) = 1 - \sum_{A_j \subseteq A_i} m(A_j) \tag{4.9}$$

と定義する。

また，独立で異なる証拠に対して基本確率を別々に与え，結果としてまとめるためには，基本確率の結合を定義する必要がある。 Dempster-Shafer確率では，m_1 ，m_2 をそれぞれ独立な証拠より推論された仮説に関する基本確率とし，A_{1i}，A_{2j} $(i,j = 0,1,2,\cdots\cdots)$ をそれぞれの焦点要素とすると，新たな基本確率は結合規則

$$m(A_k) = \frac{\sum_{A_{1i} \cap A_{2j} = A_k} m_1(A_{1i}) \cdot m_2(A_{2j})}{1 - \sum_{A_{1i} \cap A_{2j} = \phi} m_1(A_{1i}) \cdot m_2(A_{2j})} \tag{4.10}$$

によって求まる。

安全性を考える上での要因の中には，上記の例の様に，曖昧な事象というよりもむしろ不確実な事象とした方が良いものがある。従って，安全性評価に於いては，不確実性を扱うDempster-Shafer の確率を取り入れることも必要であると思われる。

その一例に， Dempster-Shafer理論に於ける焦点要素をファジィ集合に拡張したものが，石塚[44]によって提案されている。これによると下界確率，基本確率はそれぞれ次の様になる。

$$P_*(A_i) = \sum_{A_j} I(A_j \subseteq A_i) \cdot m(A_j) \tag{4.11}$$

$$m(A_k) = \frac{\sum_{A_{1i} \cap A_{2j} = A_k} J(A_{1i}, A_{2j}) \cdot m_1(A_{1i}) \cdot m_2(A_{2j})}{\sum_{A_{1i},\ A_{2j}} \{1 - J(A_{1i}, A_{2j})\} \cdot m_1(A_{1i}) \cdot m_2(A_{2j})} \tag{4.12}$$

但し，ファジィ部分集合A_1 がファジィ部分集合A_2 に含まれる程度を次の様に定義し，（$\eta_{A1}(a)$ ，$\eta_{A2}(a)$ はA_1 ，A_2 のメンバシップ関数である。）

$$I(A_1 \subseteq A_2) = \frac{\min_a \{1, 1 - \eta_{A1}(a) + \eta_{A2}(a)\}}{\max_a \{\eta_{A1}(a)\}} \tag{4.13}$$

ファジィ部分集合A_1，A_2が共通部分を持つ程度は，

$$J(A_1, A_2) = \frac{\max_a \{\eta_{A1 \cap A2}(a)\}}{\min\{\max_a \{\eta_{A1}(a)\}, \max_a \{\eta_{A2}(a)\}\}}$$

と定義される。

（4）測度論

測度とは大まかに言って，空間の部分集合の非負関数で完全加法的なものである。但し，完全加法性とは，互いに素な集合k_i，k_j，非負関数f とすれば，

$$f(k_i \cup k_j) = f(k_i) + f(k_j) \qquad (4.14)$$

が成立することを言う[45]。

ところで，3節で簡単に説明した様に，事象の生起に関する曖昧さを表現するために確率論に於ける測度では，完全加法性を仮定している。しかし，これは人間の主観的尺度を取り扱う様相としては厳しい条件であり，必ずしも必要ではない。そこで，評価や計画，決定問題に於ける曖昧さを表現するために，この条件を緩め，単調性を仮定した，ファジィ測度が菅野によって定義された[46]。

ファジィ測度とは，有限集合X，部分集合$\mathcal{A}$（ $\mathcal{A} \subset X$ ）として，

i） $g(\phi) = 0$

ii） $g(X) = 1$

iii） $\forall A \in \mathcal{A}$，$\forall B \in \mathcal{A}$ とし，$A \subset B$ であれば，
$g(A) \leq g(B)$

である。

を満たす関数gを言う。集合$\mathcal{A}$が，集合演算の拡張であるtriangular conorm ＊ なる演算子を用いて，

$\forall A \in \mathcal{A}$，$\forall B \in \mathcal{A}$，$A \cap B = \phi$ であるならば，

$$g(A \cup B) = g(A) * g(B) \qquad (4.15)$$

という代数的構造を持つとき，演算子＊の種類によって様々なファジィ測度が得られる。

(4.15) 式は，集合Aと集合Bが互いに共通部分を持たない時，その和集合の曖昧さは，各々の曖昧さだけに依存することを示す。

（ triangular conorm ＊ は，$I = [0, 1]$，$a \in I$，$b \in I$であるとき，

i) $1 * 1 = 1$

$0 * a = a * 0 = a$ (boundary condition)

ii) $a \leqq c \ \wedge \ b \leqq d$ なら $a * b \leqq c * d$ (monotonicity)

iii) $a * b = b * a$ (symmetry)

iv) $a * (b * c) = (a * b) * c$ (associativity)

を満たす[47]。)

以下に，triangular conorm ＊ をベースとした三種類のファジィ測度を示す[48]。なを，以下では各測度を区別するために，gを別の文字で置き換える。

① ＊ ＝ maximum operator $max(a, b)$ であるとき，＊は，Zadehの可能性測度になる[49],[50]。即ち，

$\forall A \in \mathcal{A}$, $\forall B \in \mathcal{A}$ のとき，

$$\Pi(A \cup B) = max(\Pi(A), \Pi(B)) \tag{4.16}$$

但し，$A \cap B = \phi$ は必要ない。

また，可能性測度と双対の関係にある必然性測度Nは，

$$N(A) = 1 - N(A) \tag{4.17}$$

で与えられえる。

② ＊ ＝ probabilistic sum $a + b - a \cdot b$ であるとき，＊は，菅野のλ－ファジィ測度[46],[51]になる。即ち，

$\forall A \in \mathcal{A}$, $\forall B \in \mathcal{A}$, $A \cap B = \phi$ のとき，

$$g_\lambda(A \cup B) = g_\lambda(A) + g_\lambda(B) + \lambda \cdot g_\lambda(A) \cdot g_\lambda(B) \tag{4.18}$$

③ ＊ ＝ bounded sum $min(1, a + b)$ であるとき，

$\forall A \in \mathcal{A}$, $\forall B \in \mathcal{A}$, $A \cap B = \phi$ のとき，

$$P(A \cup B) = min(1, P(A) + P(B)) \tag{4.19}$$

これは，

$$P(A) = min\left(1, \sum_{x \in A} P_i(\{x\})\right) \tag{4.20}$$

但し，$\sum_{i=1}^{n} P_i \geqq 1$

と書くことができ，等号が成立するとき，probabilistic 測度となる。

ファジィ測度に更に，制限を付加した測度としては，Dempster-Shafer 確率論に基づく，Belief測度，Plausibility測度がある[52]。

Belief測度は,

$$Bel(A \cup B) \geq Bel(A) + Bel(B) - Bel(A \cap B) \quad (4.21)$$

を付加したもので,

$$Bel(A) + Bel(\bar{A}) \leq 1 \quad (4.22)$$

が成立する。 Bel(A) は，基本確率 m を用いて,

$$Bel(A) = \sum_{B \subseteq A} m(B) \quad (4.23)$$

と定義される。この式は，集合Aに含まれる,
集合Bの基本確率の和を表している（図4.12）。

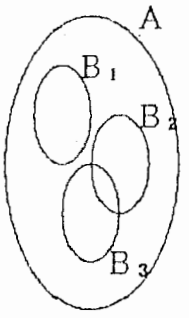

図4.12 Bel(A)

Plausibility測度は，ファジィ測度に

$$Pl(A \cup B) \geq Pl(A) + Pl(B) - Pl(A \cap B) \quad (4.24)$$

但し, $Pl(A) = 1 - Bel(\bar{A})$ (4.25)

を付加したもので,

$$Pl(A) + Pl(\bar{A}) \geq 1 \quad (4.26)$$

が成立する。 Pl(A)は，基本確率 m を用いて,

$$Pl(A) = \sum_{B \cap A \neq \phi} m(B) \quad (4.27)$$

と定義される。この式は，集合Aに入る可能性のある
集合Bの基本確率の和として表される。(図4.13)

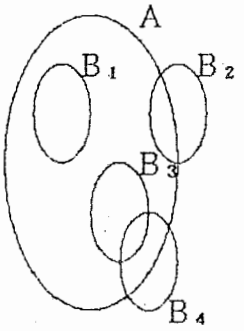

図4.13 Pl(A)

4．3．3 ファジィ評価モデル

（1）可能性モデル

可能性測度Πは，メンバシップ関数μから,

$$\Pi(\cdot) \equiv \mu(\cdot) \quad (4.28)$$

として求められる。評価法としては，可能性線型システムを表現する多項式

$$Y = A_1 x_1 + A_2 x_2 + \cdots + A_N x_N \quad (4.29)$$

に於いて，係数Aを，可能性測度．及び必然性測度を用いたファジィ数とする。この様な応用例には，可能性線型計画法，可能性線型回帰分析がある[52]。

（2）証拠モデル

Dempster-Shafer 確率に於いて，証拠は基本確率で表される。いま実数値の写像 u : X→Yとすると，X上のBel 測度とPl測度から，Y上の上界，下界分布関数は，それぞれ，

$$F_*(v) = Bel(\{x \mid u(x) \leq v\}) \tag{4.30}$$

$$F^*(v) = Pl(\{x \mid u(x) \leq v\}) \tag{4.31}$$

と定義される[53]。F_*，F^* による，u (x)の期待値は，Lebesgue-Stieltijes 積分によってそれぞれ，

$$E_*(u) = \int_{-\infty}^{\infty} v \, dF^*(v) \tag{4.32}$$

$$E^*(u) = \int_{-\infty}^{\infty} v \, dF_*(v) \tag{4.33}$$

従って，与えられた証拠から，期待値は，［ $E_*(u)$, $E^*(u)$ ］となる。つまり，証拠の不知量が，区間として求まる[54]。

証拠モデルと推論を組み合わせた例として，地震振動を受けた建築物を対象とする，被害査定のエキスパートシステム，SPERIL[55],[56] がある。SPERILでは，知識は，複雑な判定問題を効率的に解決するために， Problem Reduction法が用いられ，関連する知識が多数の小知識の集まりとして表される。問題は部分問題に分割され，全体は階層的に記述される。

不確実性を伴う判定問題では，部分問題間は関係 AND/OR/COMB によって表される（図4.14）。

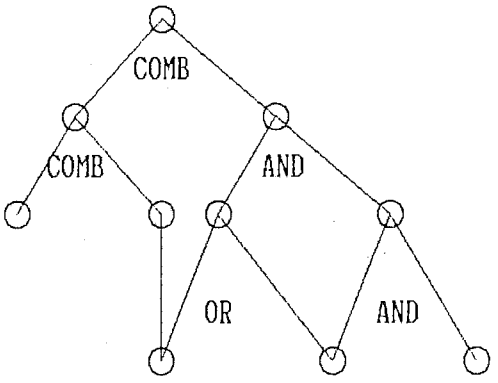

図4.14 不確実性を伴う問題のグラフ

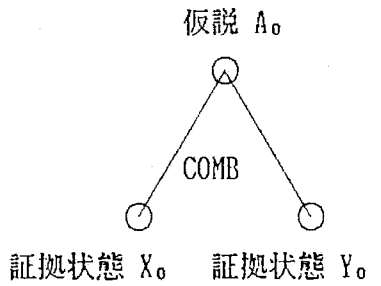

図4.15 異なる証拠の結合による推論

AND/OR関係の推論は，確実性測度上でmin,max 演算を行う。COMB は，結合関係であり，ゴールが二つ以上の証拠によって独立に指示される様な部分問題への分割を表し，不確実性の表現にとって重要である。Dempster-Shafer 理論は,COMB 演算に対して適用される（図4.15）。

小知識のプロダクション・ルールは

Rule1　IF　X_1　(前提)

　　THEN　A_{11}　WITH　C_1　(動作)

Rule2　IF　Y_1　(前提)

　　THEN　A_{21}　WITH　C_2　(動作)

によって書き表わせる。但し，X_1，Y_1は証拠状態，A_{11}，A_{21}は仮説状態であり，有限な全集合X_0,Y_0,A_0の部分集合を示す。C_1，C_2は確実性測度である。証拠状態X_1，Y_1とRule1，Rule2から仮説状態A_{11}，A_{21}の結合を推論する仮定は次の通りである。

前提X_1，Y_1の下界確率$P_*(X_1)$，$P_*(Y_1)$を計算し確実性測度を用いて，A_{11}，A_{21}の基本確率を，

$$m(A_{11}) = P_*(X_1) \cdot C_1 \qquad (4.34)$$

$$m(A_{21}) = P_*(Y_1) \cdot C_2 \qquad (4.35)$$

から求める。次に,Dempster-Shaferの結合規則によって仮説状態A_0の確実性測度が決まる。

この被害査定に必要な情報は,

(1)建築物各所の目視による検査。

(2)地震期間中に得られた建築物に設置された地震計記録の解析。

である。小知識は，所定のルール形式で知識ベースに書かれ，ファジィ等級を持つ知識を表現できる様になっている。

最終判定は，被害状態に対応する最終ゴールに於けるファジィ部分集合の，Dempster-Shafer の下界確率に基づいて成される。即ち，システムからの回答は，次のどれかである。

1) no damage
2) slight damage
3) moderate damage
4) severe damage
5) destructive damage
6) no appropriate answer

SPERIL の推論ネットワークを図4.16に示す。

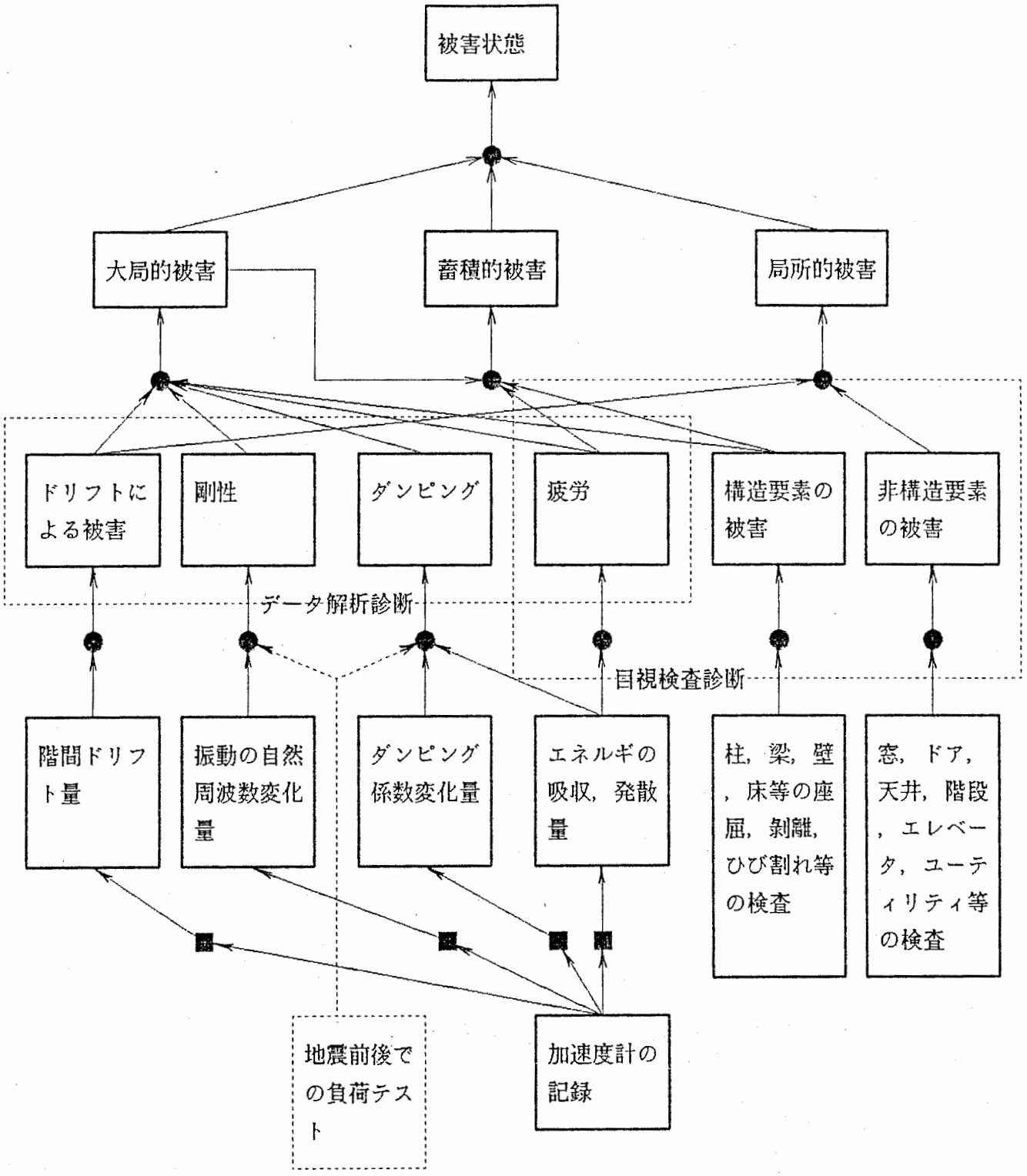

図4.16　SPERILの推論ネットワーク

■：データ解析部，●：ルールの集合

（4）λ－ファジィ評価モデル

総合評価のための期待効用は，Lebesgue-Stieltijes 積分に対応したものとして，菅野によるファジィ積分が提案されている[46),(57)]。いま，関数　h：X→［0，1］　が与えられているとき，λ－ファジィ測度g_λによるファジィ積分は，

$$\int h(x)\cdot g_\lambda = \sup_{\alpha\in[0,1]} [\alpha \wedge g_\lambda(H_a)] \tag{4.36}$$

但し，H_a はレベル集合で，$H_a = \{x \mid h(x) \geqq \alpha\}$

と定義される。有限集合$X=\{x_1, x_2, x_3, \cdots\cdots, x_n\}$ 上のファジィ積分は，X上の関数$h(x_i)$が，

$$h(x_1) \geqq h(x_2) \geqq \cdots\cdots \geqq h(x_n) \tag{4.37}$$

と仮定して，

$$\int h(x_i)\cdot g_\lambda = \bigvee_{i=1}^{n} [\, h(x_i) \wedge g_\lambda(H_i) \,] \tag{4.38}$$

となる。但し，∨：最大，∧：最小　である。

例えば，住宅の好ましさを評価するモデルを作る。住宅の属性として，x_1：価格，x_2：広さ，x_3：設備，x_4：場所　x_5：生活環境，を取り上げる。また，住宅がk個あるして，h_i：X→［0，1］を，j番目の住宅の評価値，$g_\lambda(h_i)$を，属性の重要度とす。これより，j番目の住宅の評価値は，

$$\bigvee_{i=1}^{n} [\, h_j(x_i) \wedge g_\lambda(H_i) \,] \tag{4.39}$$

となる。従来の線型評価モデルは，重みをw_iとして，

$$e = \sum_{i=1}^{n} w_i\, h_j(x_i) \tag{4.40}$$

で表される。これは，属性の独立性が仮定されているが，λ－ファジィ測度では，属性の独立性は不必要であるという長所がある。

（5）AHP(Analytic Hierarchy Process)[58),(59)]

前節で，人間の主観的判断を支援する評価システムの必要性を述べた。セキュリティ評価，設計システムをこの様に捉えたとき，問題を構造的，且つ総合的に扱う手法として，AHPの適用の可能性は興味深い。

AHPの適用から見た問題解決モデルは，図4.17の様になる。ファジィ測度は，確率測度，可能性測度等を含んでいる。従って，これらの測度をセキュリティの様相ごとに適宜，使い分け，セキュリティ対象から抽出した，主観的，客観的データをうまくAHPが扱える手法を研究することが，これからの課題である。特に，λ－ファジィ測度はパラメータによっ

て様々な様相測度となるため，注目に値する。

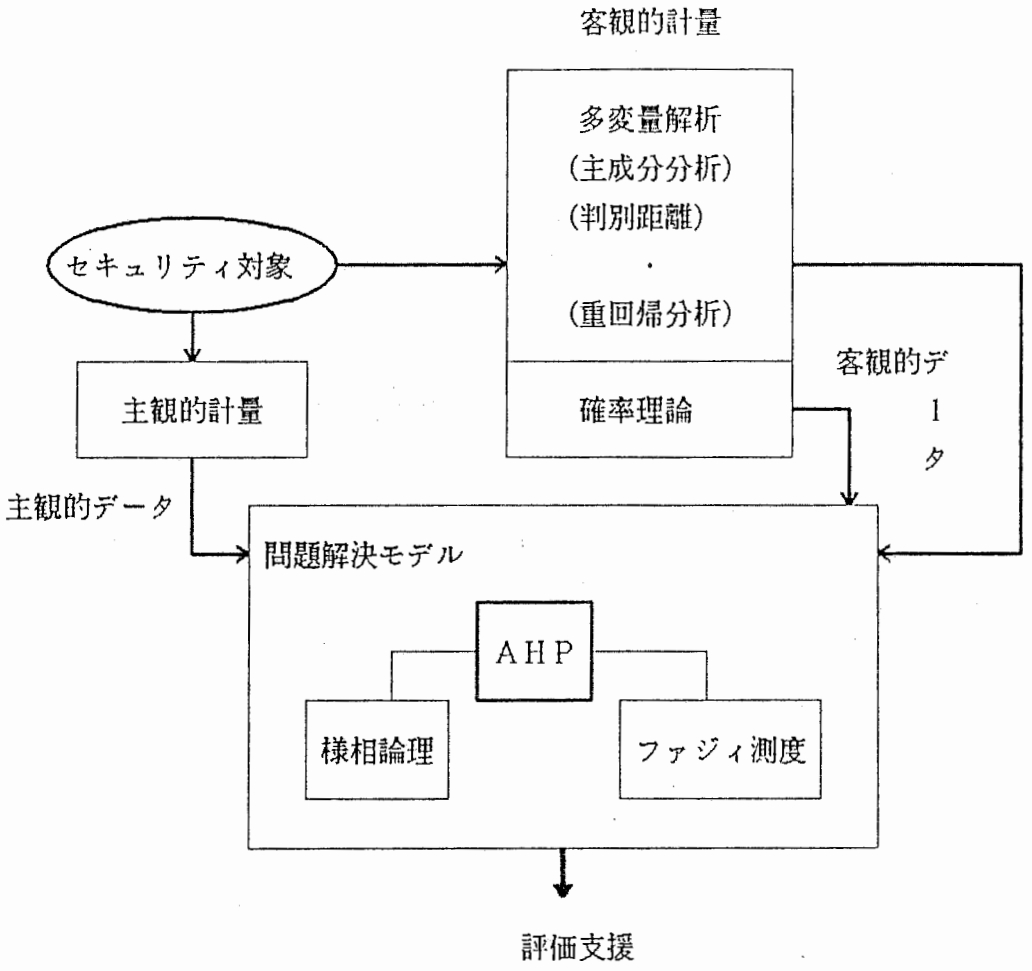

図4.17　ＡＨＰによるセキュリティ問題解決

ＡＨＰは本来，階層的に分析できる問題解決の手法であるため，セキュリティ問題に使っても，大きな誤りは無いと考える[60]。従って，まず上記のような具体的問題から初め，セキュリティ問題の様相を表現する手段の目処を立て，次にその表現法を以て，セキュリティ問題とＡＨＰの適合性を詳細に検討して行くことが，現実的であると考える。

以下では，ＡＨＰの解説を行う。

先ず，ＡＨＰの特徴を列挙すると，次の様に示される。

① 複数の解がある問題に適用される。
② 選好基準に基づいた最適な解を選択する方法である。
③ 階層的に分析できる問題に対して意思決定を行う方法である。
④ 隣接する上位の階層の要素を評価の視点として，一対比較により数段階の評点を付ける。
⑤ 一対比較を用いることによって比較が行いやすくなるのが長所であるが，その反面，全体を眺めた比較とならないために，整合が悪くなることがある。[61]

次に，ＡＨＰの基本プロセスを示す。

① 階層図　　意志決定の対象となる問題を階層化する。
② 一対比較　　人間の曖昧な知識を整理するために評価項目間の重要性を評価し，一対比較マトリクスを作る。
③ 重要度決定　一対比較マトリクスの最大固有値，及び固有ベクトルを求める。
固有ベクトルは，評価項目を，重要度の観点から比較した優先順位であると見做せる。
④ 総合重要度計算
各階層に於ける固有ベクトル（基準値，特に最下層は評価値と呼ぶ）から，階層毎の基準値のマトリクスを作り，各層の積を取る。

重要度決定プロセスに於いて，それが，一対比較マトリクスの固有ベクトルを求める問題に帰着することは，以下の様に説明できる。

重要度ベクトル　$W = \{w_1, w_2, \cdots\cdots, w_N\}$
一対比較マトリクス　A，
但し，マトリクスの要素を，$a_{ij} \equiv w_i / w_j$　とし，w_i が　w_j に比べて何倍優れているかを，１～９　の整数とその逆数で表す。
と置く。
いま，重要度ベクトルW，一対比較マトリクスＡから求めることを考える。一対比較は，主観的判断によって行われるので，マトリクスを作る上で，ある程度の制限はあるが，その要素 a_{ij}　が，w_i / w_j を満たさず，ある程度の誤差を伴う。ところで，重要度 w_i は，a_{ij}　を既知として，

$$w_i = \frac{1}{N} \sum_{j=1}^{N} a_{ij} w_j \qquad (4.41)$$

と書ける。これは，w_i，w_j を真の値として見た場合，平均をとることを意味する。更に，分母のＮを変数として λ_{MAX} と置けば，

$$w_i = \frac{1}{\lambda_{MAX}} \sum_{j=1}^{N} a_{ij} w_j \qquad (4.42)$$

となる。これは，マトリクスＡが既知のとき

$$AW = \lambda_{MAX} W \qquad (4.43)$$

と書くことができ，ここに於いてＷと λ_{MAX} を求める問題はマトリクスＡの固有値及び固有ベクトルを求める問題に帰着される。
一対比較マトリクスＡから，重要度ベクトルを求める仮定を固有値問題とするために，Ａに対して次の様な制限がある。

マトリクスAは，reciprocalである。即ち，$a_{ji} = 1 / a_{ij}$　が成立する。
マトリクスAは，consistentである。即ち，$a_{ik} = a_{ij} \cdot a_{jk}$ が成立する。
マトリクスAの対角成分が全て1 である。

マトリクスAの要素の揺らぎによる，マトリクスの consistencyの変動は，整合度（λ_{MAX} －N）／（N－1）として表される。通常，整合度は0．1以下である事が望ましいとされている。

固有ベクトルの近似解を求める問題は，Satty により，次の様に与えられている。

固有ベクトルの近似解法

(1) crudest

・各行(row) の要素の和　$\sum_{j=1}^{N} S_{ij}$ を取る。

・$w_{i1} = S_{ij} / \sum_{j=1}^{N} S_{ij}$　，i = 1,2, ・・・,N

(2) Better

・各列(column)の要素の和　$\sum_{i=1}^{N} S_{ij}$ を取る。

・$w_{1j} = \left(1 / \sum_{i=1}^{N} S_{ij} \right) / \sum_{j=1}^{N} \sum_{i=1}^{N} S_{ij}$　,i = 1,2, ・・・,N

(3) Good

・各列(column)の要素の和の逆数から，行列〔 x_{ij} 〕を求める。但し，

$$x_{ij} = S_{ij} / \sum_{i=1}^{N} S_{ij}$$

・行列〔 x_{ij} 〕の各列の和　$\sum_{j=1}^{N} x_{ij}$ を求める。

・$w_{i1} = \sum_{j=1}^{N} x_{ij} / N$　，i = 1,2, ・・・,N

(4) Good

・各行(row) の要素の積より，

$$W_{i1} = \left(\prod_{j=1}^{N} S_{ij} \right)^{1/n} \Big/ \sum_{i=1}^{N} \left(\prod_{j=1}^{N} S_{ij} \right)^{1/N} \quad , i = 1,2, \cdots ,N$$

この他に，加重最小二乗法[62]，エントロピー法等がある。

また，最大固有値の近似解は，一例をあげると

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} = \lambda_{max} \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} \tag{4.44}$$

$$\lambda_{max} \equiv \left[\left(a_{11} \cdot w_1 + a_{12} \cdot w_2 \right) / w_1 + \left(a_{21} \cdot w_1 + a_{22} \cdot w_2 \right) / w_2 \right] / N \tag{4.45}$$

一般には，

$$\lambda_{max} \equiv \left[\sum_{i=1}^{N} \left(\sum_{j=1}^{N} a_{ij} \cdot w_j \right) / w_i \right] / N \tag{4.46}$$

となる。

5．おわりに

本稿は，コンピュータシステム，並びに情報ネットワークのセキュリティ問題の中で，主に情報犯罪と言われるような，人為災害への対策と安全性評価法に関して，外部機関の研究動向を調査し，セキュリティ評価に関する若干の主張を織り混ぜて報告したものである。セキュリティの問題にはこの他に，緊急時（パニック）のヒューマン・インタラクションやトラヒック輻輳制御，情報公開とプライバシの問題，個人識別法など，さまざまな研究テーマがある。これらについては，随時，研究動向を把握していきたいと考えている。

今回の調査により，ＡＴＲがどの分野で研究を展開すべきかが，ある程度，明らかになった。この点も踏まえて，本資料の内容を大雑把に要約したものを，一覧表にして示す（表4.8　但し，太字はＡＴＲにふさわしいテーマを表す　）。

表4.8　本稿の要約

	研究動向	課題
アクセス制御	＊メカニズムは存在する。（階層的，ケーパビリティ） ＊形式言語による検証 ＊ケーパビリティは，限定されたモデルでのみコンパイル時の検証が可能。（一般化は原理的に困難）	＊ケーパビリティ制御に於ける性能向上
情報フロー解析	＊理論的な検証（プログラムの意味証明の手法） ＊形式言語による検証	＊検証精度が細かい時，計算実行可能か？
コンピュータ犯罪	＊ウィルスの報告が数件あるが，研究事例は少ない	**＊防御法（暗号等の応用）** ＊事例収集

セキュリテティ評価	＊チェックリストが整備されつつある ＊リスク分析の簡単な評価法 ＊フォルト・ツリーの規模増大時の確率計算法	＊統計的データの準備 ＊形式記述言語による記述 事務処理分野の仕様記述との関連 ＊エキスパート・システムの可能性
曖昧理論	＊ファジィ理論による異常診断 ＊ファジィ測度による主観評価尺度の研究 ＊Dempster-Shafer 確率に基づく被害査定のエキスパート・システム	＊セキュリティとのマッチング ＊理論の枠組みで，不足する部分（曖昧な事象）の強化 ＊曖昧な事象を含む問題の解決法
意思決定理論	＊ＡＨＰによる問題解決法	＊セキュリティとのマッチング ＊システム監査の支援機能
様相論理	＊時相論理によるプログラム検証	＊様相性を採り入れた，セキュリティの記述の可能性

参考文献

(1) "フォールト・ツリー解析 ", 佐山, 井上, 計測と制御,Vol.20,No.2,1981

(2) " Reactor Safety Study ,WASH-1400 ", US AEC,1974

(3) "コンピュータ・セキュリティ戦略 ", William E.Perry,日経マグロウヒル, 1987

(4) " Department of Defense Trusted Computer System Evaluation Criteria ", Department of Defense computer Security Center, 1983

(5) "インフォーメーション・セキュリティ ", 日経マグロウヒル, 1987

(6) "金融機関等のシステム監査指針 ", 財団法人金融情報センター, 1987

(7) " European needs and atitudes towards information security ",R.I.Polis, cryptologia,Vol.12,No.4,1988

(8) " MULTICSシステム 上, 下 ", E.I.オーガニック, 共立出版, 1974

(9) " Secure Computer System:Unified Exposition and Multics Interpretation ", D.E.Bell and L.J.La Padula,The Mitre Corporation,1976

(10) "Verifying Security ",M.H.Cheheyl et al,Computing Surveys,Vol.13,No.3,1981

(11) " Validation of the X.21 Interface Specification Using SARA ",CH1529-7/80 000 0-0155 1980 IEEE

(12) " The Development and Proof of a Formal Specification for a MUltilevel Secure System ",J.I.Glasgow et al, ACM Trans.Computer Systems, Vol.5,No.2,1987

(13) "算法表現論 ", 木村, 米沢, 岩波講座 情報科学１２

(14) "時間論理に基づいたプロトコル記述と検証 ", 越田, 斉藤, 猪瀬, 信学論vol.69D,3 1986

(15) "Foundations of Secure Computation ",R.A.Demillo et al(ed.),Academic Press, 1978

(16) "Cryptography and Data Security ", D.E.R.Denning,Addison-Wesley,1983

(17) "コンピュータ犯罪研究総論 ", ドン. B. パーカー, 秀潤社, 1984

(18) " An analysis of the differences between the computer security practices in the military and private sectors ",L.S.Chalmers,Proc.IEEE Symp.on Security and Privacy,1986

(19) "資源アクセス管理機能（ＲＡＣＦ）使用者の手引 ", 日本ＩＢＭ, 1987

(20) " Reflections on Trusting Trust ", Ken Thompson, Comm.ACM,Vol.27,No.8,1984

(21) "コンピュータ・セキュリティに関するリスク分析調査報告書 ",(財) 日本情報処理開発協会, 1985

(22) "コンピュータ・セキュリティ ", ドン・パーカー ,Ⅱ法情報処理開発協会

(23) "エレクトロニクスに於ける信頼性 ", 電子通信学会

(24) "Reliability and Risk Analysis ", McCormick,Academicpress

(25) "化学プラントの危険度評価 ", 佐山, 安全工学,Vol.19,No.2,1980

(26) "システム信頼性評価問題に対する一般被覆モンテカルロ法 ", 田中, 熊本, 井上, 計測自動制御学会論文集,Vol.23,No.7,1987

(27) "Information Security Evaluation Method : Hisecurity-E ", 宝木, 白石, 佐々木

，永井，1987年暗号と情報セキュリティ・ワークショップ,CIS研究会
(28) "システム監査の基礎知識 "，鳥居，日本生産性本部
(29) "システム監査の一実現方法 "，高橋，坂内，「利用者指向の情報システム」シンポジウム,S.63.6
(30) "システム監査手法による情報システムの評価に関する一考察 "，岡田　定，情報通信網の安全性・信頼性時限研究専門委員会
(31) "システム監査概論 "，富山，（財）日本情報処理開発協会
(32) "システム工学入門",寺野寿郎，共立出版
(33) "複雑なシステムの適応保全と失敗からの学習 "，田中，電子情報通信学会論文誌，A，Vol.J71-A，No.5，1988
(34) "　様相論理",G.E.ヒューズ，M.J.クレスウェル，三浦，大浜，春藤，恒星社厚生閣
(35) "　特集・様相論理 "，数理科学5，1986,サイエンス社
(36) "　様相論理とその情報処理への応用:（Ⅰ）様相論理 "，堂下，西田，三浦，情報処理，Vol.29，No.1，Jan.，1988
(37) "　様相論理とその情報処理への応用:（Ⅱ）ハードウェア・ソフトウェアへの応用 堂下，西田，島田，情報処理，Vol.29，No.2，Feb.，1988
(38) "　様相論理とその情報処理への応用:（Ⅲ）知識情報処理と自然言語処理への応用 堂下，西田，島田，情報処理，Vol.29，No.3，Mar.，1988
(39) "　時空間様相論理ＥＴＳＬとその決定手続き "，岩沼，原尾，野口，電子情報通信学会誌，'86/3Vol.J69-D,No.3
(40) "ファジィシステム入門 "，寺野，浅居，菅野，オーム社
(41) "　あいまい論理を用いた異常診断 "，村山，寺野，システムと制御,Vol.24,NO.11
(42) "SCURATE-security evaluation and analysis using fuzzy metrics "，L.J.Hoffman，E.H.Michelman，D.Clements，Proceedings of the national computer conf.,1978
(43) " a mathematical theory of evidence "，Glenn Shafer，Princeton，1976
(44) " An Extension of Dempster & Shefer's Theory to Fuzzy Set for Constructing Expert Systems —— エキスパートシステム構築のための Dempster & Shefer 理論のファジィ集合の拡張 "，石塚　満，生産研究，34巻,7号,1982,7
(45) "　測度論 "，数学辞典，岩波
(46) " Fuzzy測度とFuzzys積分 "，菅野，計測自動制御学会論文集,8,2,1972
(47) " A THEORY OF FUZZY MEASURES "，E.P.Klement，FUZZY INFORMATION and DECISION PROCESS ,North-Holand，1982
(48) " On Several Representations of an Uncertain Body of Evidence "，D.Dubois，H.Prade，FUZZY INFORMATION and DECISION PROCESS，North-Holland，1982
(49) " Fuzzy Sets as a Basis for a Theory of Possibility ",Zadeh,L.A.,(Int.J.) Fuzzy Sets and Systems,1,1,1978
(50) " POSSIBILITY THEORY: AS A TOOL FOR PRELIMINARY ANALYSIS OF COMPUTER SECURITY SYSTEMS "，David C.Rine，FUZZY INFORMATION and DECISION PROCESS，North-Holland，1982

(51) " 確率とFuzzy 測度の同形性 ", 塚本, 計測自動制御学会,19,3,1983
(52) " ファジィ測度に基づくファジィモデルとその応用 ", 田中, 特集・ファジィ理論と応用, 数理科学2, 1987,サイエンス社
(53) "a mathematical theory of evidence",G.Shafer,Princeton,1976
(54) " ファジィ・システム専門講演会テキスト ", 国際ファジィシステム学会日本支部, 計測自動制御学会
(55) " 建築物被害査定のエクスパート・システム ", 情報処理学会論文誌,Vol.24,No.3, May, 1983
(56) " Inference Methods Based on Entended Dempster & Shafer's Theory for Problems with Uncertainty/Fuzziness ", Ishizuka, New Generation Computing, 1,1, 1983
(57) " Fuzzy測度の構成とFuzzy 積分によるパターンの類似度評価 ", 菅野, 計測自動制御学会論文集,9,3,1973
(58) " The Analytic Hierarchy Process ", Thomas L. Satty, McGraw-Hill, 1980
(59) " A Scaling Method for Priorities in Hierarchical Structures ", T.L.Satty Jounal of Mathmatical Psychology 15, 1977
(60) " 非単調推論に基づく選択問題に評価支援 ", 新谷, 情報処理学会第36回(昭和63年後期)全国大会
(61) "ＡＨＰを応用したExpert System (診断圏予測システム)",大橋, 早川, 橋本, 春木 昭和62年人工知能学会全国大会
(62) " A Comparison of Two Methods for Determining the Weights of Belonging of Fuzzy Sets ", A.T.W.Chu, R.E.Klaba, K.Spingarn, Jounal of Optimization Theory and Applications, Vol.27, No.4, Apr., 1979