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

昭和 63 年 3 月

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６２年度に実施した「情報処理に関する普及促進」の一環としてとりまとめたものであります。

序

情報システムの高度化，ネットワークの拡大化は，今日の高度情報化社会をもたらし，日本経済を強力にするとともに，われわれの生活を豊かなものにしてきた。しかし，一方では，情報システムをめぐる事故・災害の影響が必然的に大きくなっている。

当協会では，このような情報システム環境の変化を厳粛に受けとめ，従前よりコンピュータ・セキュリティに関するリスク分析の方法論のあり方を研究してきた。最近では，その一環として銀行をモデルとし，コンピュータ犯罪のリスク分析を試みたところである。このように，各種モデル・システムを取りあげて，いずれは標準的なリスク分析手法を確立いたしたいと考えている。

本報告書は，昭和６２年度に実施した調査研究の成果であり，内容はつぎのとおりである。

① 流通業におけるＰＯＳシステムのモデルをつくり，それを対象に実際にリスク分析を実施した。

② ヒューマンエラーの発生原因を把握し，その防止策に役立てるため，ヒューマンエラー分析を実施した。

③ 先進諸外国のリスク分析手法の確立状況を知るため，外国文献調査を実施した。

④ 当協会が毎年実施しているコンピュータ利用状況調査の結果にもとづき，業種別にセキュリティ対策の水準を出し，付属資料として収録した。

最後に，本調査を推進するにあたって，ご協力を賜った委員をはじめ関係各位に対して，心から感謝する次第である。

昭和６３年 ３ 月

財団法人　日本情報処理開発協会

昭和６２年度

リスク分析委員会　委員名簿

委員長	森宮　康	明治大学　商学部　教授
委　員	安保二見男	セコム㈱　常務取締役
	太田政弘	㈳情報サービス産業協会　事務局長
	大橋　旦	㈶金融情報システムセンター　安全対策部長
	黒田　巌	日本銀行金融研究所　研究第２課長
	小早川久佳	青山監査法人　代表社員，公認会計士
	小林孝夫	日本アイ・ビー・エム㈱　金融営業推進本部　金融インフォメーション・セキュリティ推進
	佐藤孝雄	日本電気㈱　情報処理第一公共システム事業部担当部長
	田口孝弘	日本電子計算機㈱　大阪営業所長
	竹井正昭	東京海上火災保険㈱情報システム部課長
	中川吉朗	インフォメーション・システムサービス㈱　取締役社長
	中西英夫	情報処理振興事業協会　技術センター所長
	花香俊明	㈱デーシージャパン　第２部長
	三谷保夫	システムコンサルタント
	安田健博	日本電信電話㈱　データ通信事業本部　ＣＥ事業部　ハード技術担当部長

目　　次

第1章 POSシステム・モデルにおける
リスク分析実施例

ここでは，小規模スーパーマーケットでのＰＯＳシステム・モデルを作成してリスク分析を実施した。このリスク分析では，システムが内蔵しているリスクとリスク発生が企業に与える問題点との関連づけを行い，リスクが企業に与える影響の定量化などは，今後の研究に委ねることとした。

1. モデル分析を行う理由

企業における情報システムの利用は，年々幅広く，多岐にわたってきているが，その利用方法・利用度合の進展とともに，リスクの状況・リスクの環境もそれぞれ変化している。

リスク分析の考察を行うにおいては，このような状況を踏まえつつ進める必要があるが，リスク分析の理論の展開だけでは日々変化している現実のリスクと遊離してしまう不安が常に存在する。

そのため，今回小規模なスーパーマーケットにおけるＰＯＳシステムをモデルとして設定し，システムの具体的な「事故事象」，「原因」の洗い出し，さらに「経営に悪影響を及ぼす事象」との関連づけ等の作業を行い，リスク分析の実践を試みた。

―― ＰＯＳシステムを採りあげた理由 ――

ＰＯＳシステムとは，小売業やサービス業などにおいて，店頭にレジスター機能を併せ持つ端末を設置し，チェックアウトの効率化を図るとともに，店頭販売情報を中心として，発注・仕入れ・検品・顧客情報など，小売業やサービス業などの経営活動に関する必要情報を，主としてその販売時点でとらえ，情報システムを活用して管理する小売・サービス業の総合経営情報システムであるといえる。

今回，ＰＯＳシステムをリスク分析のモデルとして採りあげたのは，ＰＯＳ

システムが以下に述べる３つの理由から，わが国における各産業のさまざまな情報システムの１つの代表形態と考えられるからである。このＰＯＳシステムをモデルとしたリスク分析は，リスク分析理論の検証のためにも，あるいはリスク分析を今後実用に供するためにも，有意義なことであると考える。

① ＰＯＳシステム導入店がここ数年急激に増加しており，今後も引き続き増加が見込まれる。

ＰＯＳ機器の性能の向上，価格の低下およびソースマーキング（商品のメーカーまたは発売元の段階でのコード印刷）率の向上，さらには消費者の嗜好の多様化に対応する適切な品ぞろえの必要性の高まり等により，小売・サービス業界を中心として，ＰＯＳシステム導入店が昨今急激に増加しており，今後も増加の傾向は強まることはあっても弱まることはないものと考えられる。

また，すでに導入した店についても，ネットワーク規模の拡大などにより，ＰＯＳ端末の導入台数が今後かなりの勢いで増加する見込みである。

「情報化白書 1987（日本情報処理開発協会編）」の「端末機の利用現状と５年後予定」のアンケート集計結果では，１社当りの端末平均台数の「現状台数」と「５年後予定台数」が，各種端末の合計では２６７.３台から３５８.０台と1.３倍であるのに対し，ＰＯＳ端末では１４３.９台から３８８.０台と2.７倍であり，極めて高くなっている。

② ＰＯＳシステムの内容（機能）が幅広く多岐にわたってきている。

基本のチェックアウトの効率化（商品自動読み取り，プライス・ルック・アップ等によるチェックアウトの生産性向上，レジ登録ミスの削減等）および営業支援のための収集データの活用（売れ筋商品分析，死に筋商品分析，販売員分析，販売店分析等）はもちろんのこと，一歩踏み込んだデータ活用（時間帯別売り上げ分析，生鮮パック品ロス分析等），あるいは在庫管理・発注システムとの連動に代表されるような他のシステムとの組み合せ等，ＰＯＳシステムの内容は，ますます幅広く多岐にわたってきている。

さらに，商品企画や生産計画に結びつけて，経営情報システムとしての役

割を狙ったり，ＶＡＮとの接続，あるいは昭和５９年に大蔵省が認可したキャッシュカードを使った即時決済システム（銀行ＰＯＳ）の機能を付加する等の新しい試みも取り組まれつつある。

③　ＰＯＳシステムは一般市民（消費者）に最も直結した身近な情報システムの１つである。

前述のように，ＰＯＳシステムは，レジスター機能を併せ持つＰＯＳ端末から，店員が顧客の目の前でデータの入力を行うという，一般市民（消費者）が日常最も身近に接する情報システムである。また，システムを利用する企業側のメリットに加えて，チェックアウトの際，より正確で，より迅速な処理が可能になるという顧客の直接のメリットもある。さらには，データの活用により，適切な品ぞろえが期待できるという顧客のメリットも考えられる。

ただし，これらの顧客のメリットがある一方で，もしシステムにトラブルが発生した場合には，直ちに顧客にも影響が及ぶ可能性が高いということにもつながり，その点からも今後一般市民（消費者）のＰＯＳシステムへの関心は高まっていくものと思われる。

2. モ　デ　ル

(1) 前提条件の設定

ここで分析の対象とするのは，以下のモデルにおける店舗のシステムを中心とした。なお，本社のシステムは，通産省の策定した電子計算機システム安全対策基準に基づく安全対策が十分できているものと想定した。

(2) モ　デ　ル

モデルとする店舗は，小規模なスーパーマーケットであり，その概要は次の通りとする。

(a) 業務内容：食料品・雑貨品を中心としたセルフサービス方式の小売店

(b) 業　　容：

(ア) 店舗数・平均売場面積

4店舗・約330平方米

(イ) 営業日・営業時間

360日・10:00～19:00

(ウ) 取扱商品

食料品・雑貨品を中心に

10,000品目～15,000品目

なお，全商品のうち約９０％はあらかじめ，バーコード（ＶＡＮコード）の商品識別コードが付加されている。

(エ) 顧　　客

一日平均来店数約５６０人

客当り売上単価約1,８００円

一店舗当り会員数約3,０００名

なお，会員には会員カード（磁気カード）を発行。

(オ) 従 業 員

店長１名，売場主任４名（内１名は店長代行）の他はパートタイマ。

なお，一時点でのパート就業人員は７～１０名（絶対雇用人数は約３０名）。

(カ) レジ端末

保有数　５台

ＭＡＸ使用　４台

通常　２台

(キ) 売上げ，現金管理

一日平均売上げは約１００万円，内現金売上げは約８０万円。

なお，現金は営業終了後，銀行の夜間金庫に預け入れ，翌日本社口座に集中。

また，会員の売掛けは月に一度会員ごとに集計して本社から請求する。

(ク) 商品価格

商品ごとの販売価格は毎日営業開始前に本社から連絡される。

また，営業終了後商品別の売上げ数量を本社に報告することで，本社が在庫管理，発注を行っている。

(c) ＰＯＳシステムの要件

(ア) レジ端末における顧客請求金額（売上げ金額合計）の自動算出とレシートのプリント。

－商品上のバーコード読取りによる金額算出と集計

－顧客ＩＤカード読取りによる顧客識別

(イ) レジ端末内現金照合のための金額計算と出力

－点検精算時の現金有高照合用金額計算と時間帯別・商品部門別出力

(ウ) 本社からの必要な情報の授受

－商品別価格情報と顧客サービス情報の授受と保管

(エ) 本社において次の処理を行うためのデータの蓄積と本社への送付

－売上金，商品販売実績管理

－商品在庫管理と発注管理

－顧客別売掛金管理，請求処理

(d) ＰＯＳシステムの機能と構成

前述の要件を満たすため，以下のようなＰＯＳシステムを導入するものとする。

(ア) バーコードリーダ，磁気カードリーダ及びレシート・ジャーナルプリント用ミニプリンタを装備したデータ蓄積，集計が可能な端末機を設置。

(イ) 各レジ端末とのデータ授受及び本社とのデータ授受のため一台のターミナルコントローラ（店内制御装置）（以下「ＴＣ」と云う。）を設置し，本社システムと回線接続する。

(ウ) 商品ごとの販売設定価格及び会員サービス用の顧客情報は，営業開始

前に本社から送付されたものをＴＣに記憶し，各レジ端末から常時参照可能にする。

(エ) 会員には顧客ＩＤを記録した磁気カードを交付し，これをレジ端末に提示し顧客ＩＤを読取ることで会員顧客の確定を行う。

(オ) 販売時点において，売上げ商品一品ごとの商品コード，販売価格，顧客ＩＤ（会員の場合），レジ端末操作従業員ＩＤ，販売日時から成るデータを作成し蓄積する。

(カ) 上記蓄積データは，精算時にレジ端末からＴＣに，営業時間終了後にＴＣから本社システムへ一括送付する。

(キ) 機械構成およびシステム構成は次の通り。

表 1. 機器構成（一店舗当り）

機　　器	数　　量
1. レジ＋固定スキャナ（バーコードリーダ）	5　台
2. ＩＤカードリーダ	5　台
3. ＴＣ	1　台
4. 公衆回線	1 回線

(e) 一日の業務処理の流れ

(ア) ＴＣの電源ＯＮ。

(イ) 本社からの商品情報及び顧客情報を受取る。

(ウ) 店長又は店長代行は，各レジ端末を立ち上げ作動確認ののち，釣り銭を準備する。（釣り銭はレジ端末１台当り７万円）

(エ) レジ端末の操作員を配置する。

(オ) 売上登録の処理を行う。

一商品コード読取り

－売上金額計算及び金額表示

－磁気カード読取り（会員顧客の場合）

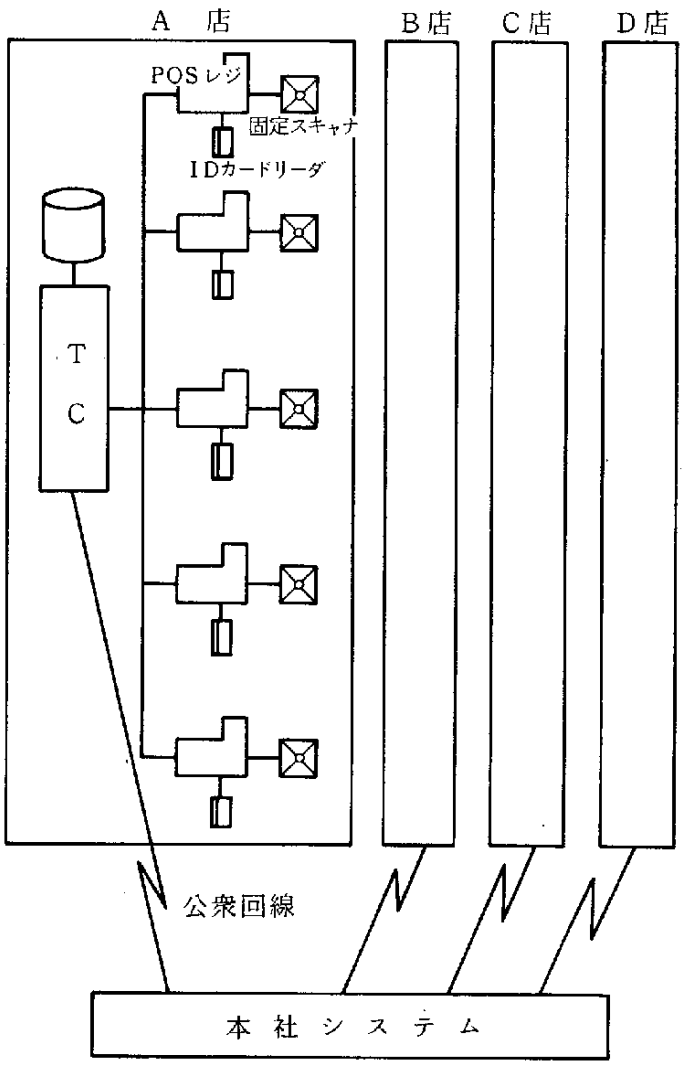
－現金受取り

－釣り銭わたし

－・

－・

図1. システム構成



(カ) 店長又は店長代行は，１２時・１５時・１８時に各レジ端末の点検処理を行って売上状況および現金の確認を行う。

(キ) 閉店後，店長又は店長代行は各レジ端末の精算処理を行って，レジ端末に蓄えられているデータをＴＣに送付したのち，売上げ金額，現金高を確認して現金は銀行の夜間金庫に預け入れる。

(ク) ＴＣに蓄えられた各レジ端末のデータを本社に送付する。

(ケ) ＴＣの電源をＯＦＦにする。

(f) 現在実施しているセキュリティ対策

(ア) 店舗のＴＣの操作は店長又は店長代行のみが行っている。

(イ) 各レジ端末のマスターキーは店長又は店長代行が常時保管している。

(ウ) レジ端末の立ち上げ，点検・精算処理及び釣り銭の準備は，店長又は店長代行が行っている。

(エ) レジ端末の操作員がレジ端末操作の際は，各自の識別コードを入力することにより操作員の識別を行っている。

(オ) 点検・精算時において，現金とレジ端末登録上の金額に不一致があることが判明した時は，次の処置を基本としている。

－不一致金額が1,０００円～ 5,０００円の時，レジ端末操作担当者による報告書の提出

－不一致金額が5,０００円以上の時

レジ端末操作担当者からの始末書の提出

(カ) １万円札の入出金は，特別の管理方式によって厳重な管理を行っている。

(キ) 店舗内の従業員は，全員警笛を所持して万一の時の緊急連絡に備え，また暗号放送による店舗内の非常連絡等の対策も整えている。

3. リスク分析の手順および手法

ここで行ったリスク分析は「リスク発生により企業が受ける損失を最小にするため，有効な対策を立てるための一つの手順である。」との立場に立って，次の手順，手法に従って，事故事象，原因集合の摘出を行った。

なお，今回の作業では，リスク分析のうち「リスクの測定」「リスク処理の評価」は行わず，今後の研究課題とした。

(1) リスク分析の手順

(a) リスク分析の目的となるシステムの事故事象と原因集合（ここではＰＯＳシステム障害など）の明確化

システムに発生する事故などで，システムが期待どうりに稼動しない状態を事故事象というが，これを類型化したシステムの障害状況は非常に限られている。しかし，事故の原因は多種多様で，直接に強い関係を持っている原因，さらにそれを惹起した原因などが見られるが，これらの因果関係は必ずしも整然とはしていない。そこで，これらの諸原因を総称して原因集合と名づけた。

システムの事故事象と原因集合の関連については，業務およびシステムの関係者によるブレーンストーミングを行って，まず事故事象を摘出した。続いて，事故事象に直接関係がある事故の原因を，その原因を引き起こした原因，さらにその原因と，つぎつぎに原因分析を重ね，どのような原因が事故事象を引き起こすのかを究明した。

(b) 経営に悪影響を及ぼす事象（ここではモデルにおける収益減）の明確化

企業のそれぞれの部署には，その業務の目的と業務を遂行するための機能が明確に定められている。しかし，業務を遂行するに際して各種の阻害要因が発生するが，この中にはシステムの障害によるもののほか，システムと直接に関係がない要因も多く見受けられる。リスク分析の結果としてリスク処理を実施する場合，当該部署におけるシステムの障害が全体のリ

スクの中でどのレベルにあるか，また企業全体にどの程度の悪影響を及ぼしているかを把握することにした。

(c) 経営に悪影響を及ぼす事象とシステムの事故事象との関連づけ

リスク分析を行う対象の部署に発生する各種の阻害要因による悪影響のうち，システムの障害によるリスクがどのようにかかわっているのか，また，そのシステムリスクは全体のマイナス要因のうちでどの程度を占めているのか，などを明確にするために関連表を作成した。

(2) リスク分析の手法

(a) 類型化した状況から原因の追及

ＰＯＳシステムの障害状況を全面停止，一部停止，誤作動に類型化し，事故事象を把握する演繹手法を採用した。モデルの経営に悪影響を及ぼす事象についても，同様に「どういう悪い事柄があるか」「その原因はなにか」という方式で体系化した。

(b) ブレーンストーミングによる項目摘出

事故事象とその原因集合は，本リスク分析の関係者およびＰＯＳシステムを熟知している者など，できるだけ各種の機能をもったメンバーに跨がって自由な意見を集めることを前提とした。

(c) 要因系統図の構築

ＰＯＳシステムの事故事象とその直接に原因となる事項，さらにはその原因となる出来事という形でツリー構造を作成した。モデルの経営に悪影響を与える事象についても同様の手法でツリー構造を作った。

なお，このツリー構造の作成に当たっては，原因となる同一事柄が異るレベルに出てこないよう配慮した。（例えば，停電という原因は，各項目に出てきたとしても，同一レベルに記入される）

(d) 要因関連図の作成

「ＰＯＳシステムの事故事象が，モデルの経営に悪影響を与える事象のどの部分に関連しているか。」を明確にするため，事故事象および経営に

悪影響を与える事象の両要因系統図を結合し，要因関連図を作成した。

4. モデルにおけるＰＯＳシステムの事故事象と原因集合分析

ここでは，ＰＯＳシステムの事故事象を整理するとともに，その原因として考えられる事項（原因集合）を洗いだす作業を実施した。

なお，期待した通りにシステムが稼働したにもかかわらず，経営に結果として悪影響を及ぼすということも考えられ，これらについても経営のリスクという点からは分析が必要であるが，「システムの事故」とは異なる質の問題であるため，ここでは分析対象から除外した。

除外事項の例示

・システム構築に対する投資が経営を圧迫する問題

・そもそもシステムへの期待事項が誤っていたことによる問題　など

(1) システム事故事象の類型化

システム事故事象を整理する際に重要となるポイントは，経営に悪影響を及ぼす可能性のある事象をできるだけ漏れなくリストアップすることである。

この段階で事故事象を看過してしまうと，結果としてシステムが内包する重大な問題を分析対象から除外してしまうことになり，最終的にはシステムのリスク評価が正しく行われないことになる。

このため，当作業においては，まず事故事象の種類を何種類かに類型化し，その分類ごとに具体的な事故事象をリストしていく手法をとった。

システムの事故事象の類型化は，現象面からみた分類方式で行う。

（原因面からの分類はこの段階では行わない。）

一般的には，

① システム停止（システムダウン）　……　機能の全面停止

② システム縮退　……　一部機能の停止

③　システム誤作動　……　機能の誤り

の３つに類型化されるが，リスク分析においては，特に③の機能の誤りの中に，期待している機能が正当に行われないという現象に加えて，期待していない余分の機能が行われるという現象をも含まれる。（例えば重要情報が外部に流出するというシステム事故など）

(2)　類型化に沿った具体的なシステム事故事象の把握

つぎに，分類（類型化）に沿ってモデルシステムにおける事故事象を具体的に洗いだす作業に進むが，この際，事故事象の表現レベルの基準を明確にしておくことが必要である。

すなわち，当該事故事象についての共通確認が可能で，その原因となる可能性のある事象が明確に考えられるレベルで記述されなければならない。

さらに，後続の作業で当該事故事象が経営に対してどの程度影響するものかを容易に把握できるレベルで記述されることが望ましい。

特にシステムの縮退やシステム誤作動では，どのような機能が停止するのか，どのような機能がどう誤るという事象であるかを明確にしておかなければ，原因集合の整理や事故事象の影響分析につながっていかないことになる。

(a)　ＰＯＳ機能の全面停止

この事故事象は，「ＰＯＳ機能の全面停止」という表現で現象が共通認識できるため，細分化は必ずしも必要でない。

同じ全面停止であっても，復旧までの経過時間の大小によって影響度の度合は異なるが，原因については同等であるため，ここでは１事象として捉える。この事故事象では，後述(b)の①～⑧が同時に発生する状態になる。

(b)　ＰＯＳ機能の一部停止

これは，停止する機能が明確にされなければ事故事象が認識できないため，モデルシステムが保有する機能ごとに以下の事象に整理する。

①　商品コードテーブルの更新ができないという事故事象

本社から毎朝伝送される商品コードとか金額が，ＴＣのファイルに登録できない。売上処理に時間がかかる。

② 商品の金額が読めないという事故事象

ＴＣのファイルに登録してある商品金額が，障害とかＴＣファイルに未登録のため読めない。売上処理に予定外の時間を必要とする。

③ 商品の合計金額が算出できないという事故事象

売上商品の合計金額が，プログラム誤りとか機器故障により，レジ端末で算出できない。売上処理に時間がかかる。

④ レシート，点検精算表が印字できないという事故事象

売上商品の金額などが，機器故障とかプログラム誤りで印字できない。処理に時間がかかる。

⑤ 顧客カードが読み取れないという事故事象

顧客カードが読み取り器故障，カードの不良などで読めない。売上処理に時間がかかる。

⑥ 商品コードが読み取れないという事故事象

商品ごとに貼付してある商品コードが，ラベル不良とか機器故障などで読めない。売上処理に時間がかかる。

⑦ 点検精算ができないという事故事象

担当者交代時とか，一定時間ごとに実施する中間集計，最終に実施する精算ができない。顧客に直接の悪影響はない。

⑧ センターへのデータ伝送ができないという事故事象

ＴＣに記入してある一日分の取引内容が，機器故障，データ破壊などでセンターに伝送できない。顧客への売掛金の集計請求を行ったり，的確な在庫管理が不可能となり，売掛金の回収不能，欠品（売るものがない），在庫過剰の事態が発生する。

(c) ＰＯＳ機能の誤作動

前述(b)と同じく機能が誤ることを明確にするとともに，機能誤りの内容を表現する必要がある。さらに，要件にない機能が行われる現象を当分類の事故事象に追加する。モデルシステムにおける事故事象は以下のとおり。

① 誤った商品合計金額を算出，表示してしまう事故事象

センターからの伝送誤り，商品に貼付してある商品コードの読み誤り。売上処理の誤りとなる。

② 売掛データを別顧客のものとしてしまう事故事象

顧客カードの読み誤り，機器故障などで無関係の顧客に誤って請求する。売上処理の間違いとなったり，売掛金の回収ができなくなったりする。

③ レシートに誤った商品コード，金額を印字するという事故事象

レシートに金額などを誤印字する。預かり金やつり銭を間違う。

④ 点検精算シート上に誤った結果（数字）を印字するという事故事象

中間集計とか最終の締め集計が誤る。顧客には直接の影響はない。

⑤ ＴＣのファイルに保存しているジャーナルの誤り（重複，欠落，内容誤り）という事故事象

ＴＣファイルに記録する売上，売掛などの記録に重複，欠落とか内容の誤りがある。顧客の売掛金が回収できなかったり，管理情報誤りにより欠品（売るものがない）とか在庫過剰となったりする。

⑥ センターへのデータ伝送誤り(重複，欠落，誤りデータ)という事故事象

一日の最終に，ＴＣファイルの売上，売掛などのデータを本部センターに伝送するが，機器故障，プログラム誤りなどで誤ったデータが伝送される。顧客の売掛金回収不能とか欠品，在庫過剰の状態が発生する。

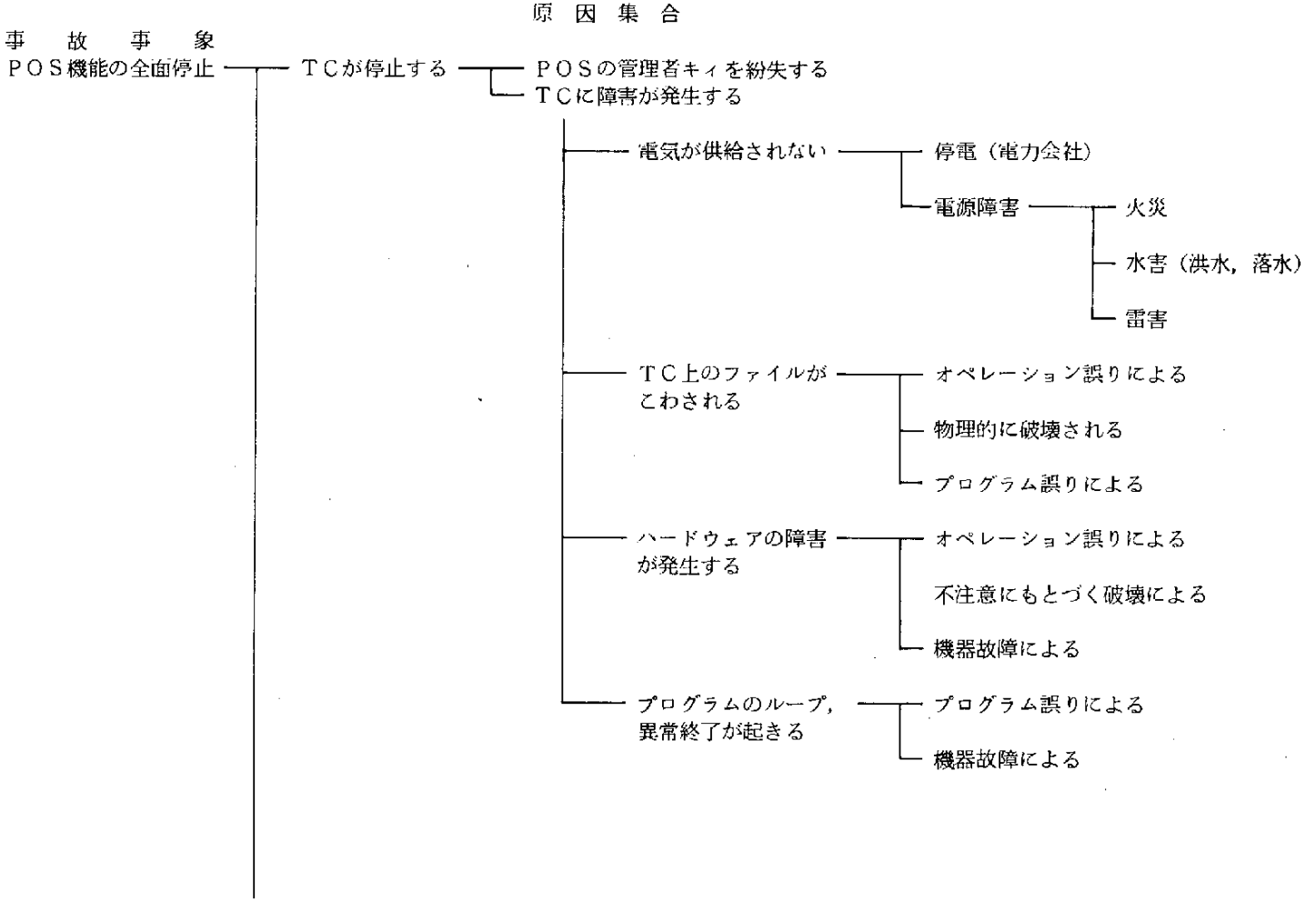
(3) システム事故事象ごとの原因集合の洗い出し

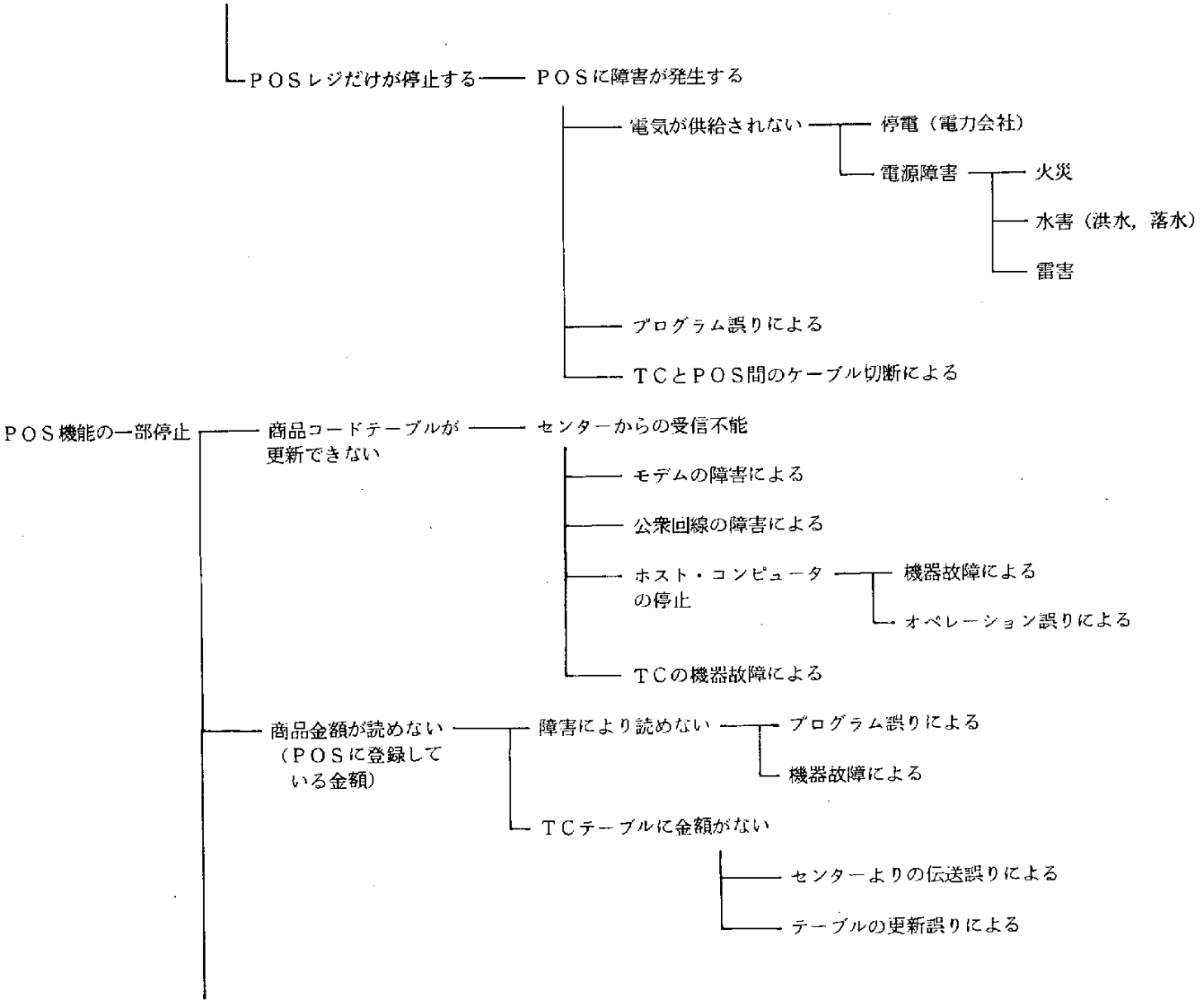
前ステップで整理された事故事象ごとに，その原因となり得る事項をランダムにリストアップする。

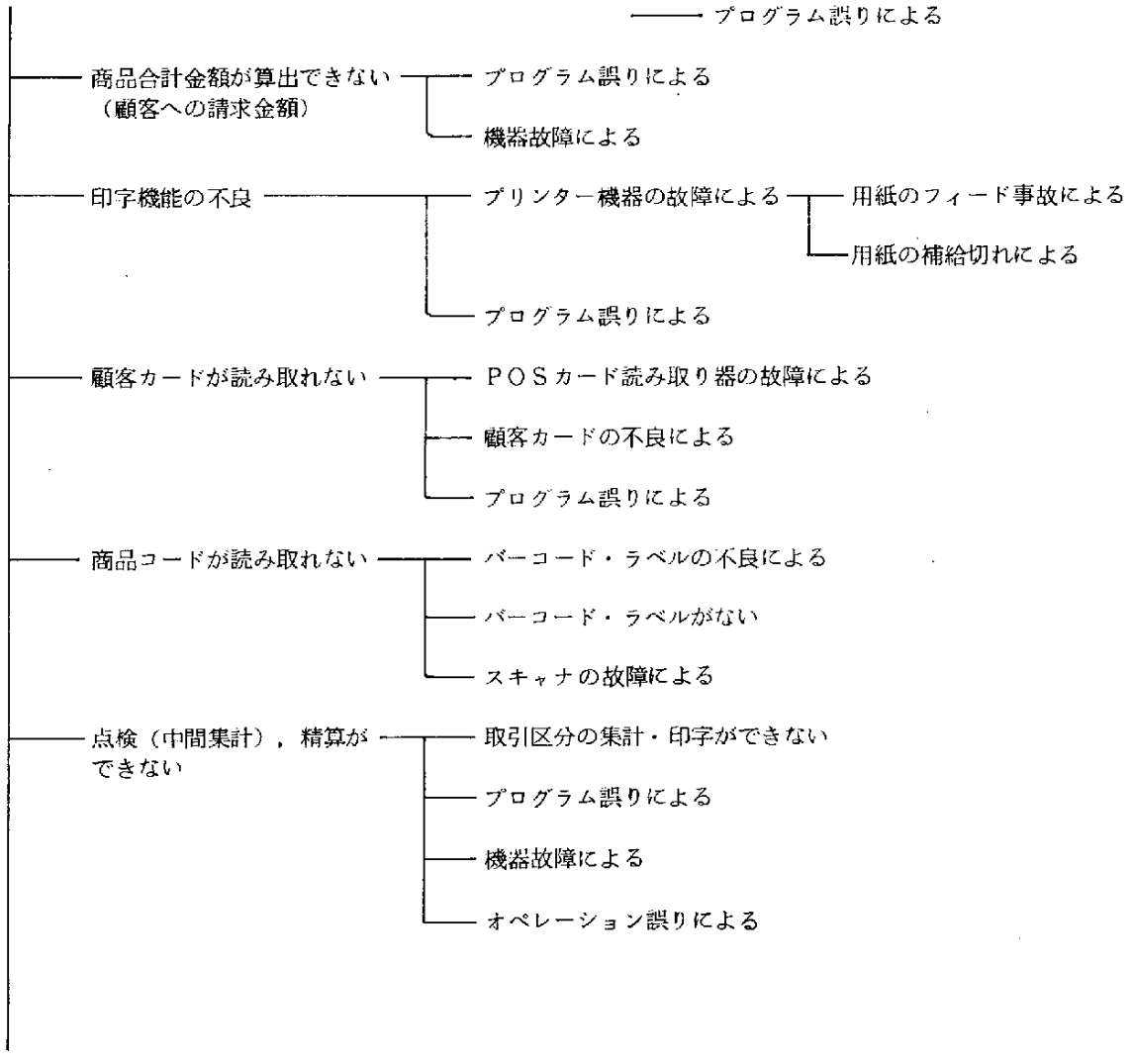
原因は，直接的な原因，その原因の発生原因というように複雑な因果関係を持つことが常であるが，ここでは全ての原因についてのその因果相関を整理しきれなくとも良い。後続の作業で重要な原因を絞り込んだ後に，詳細整理を行うことが現実的である。

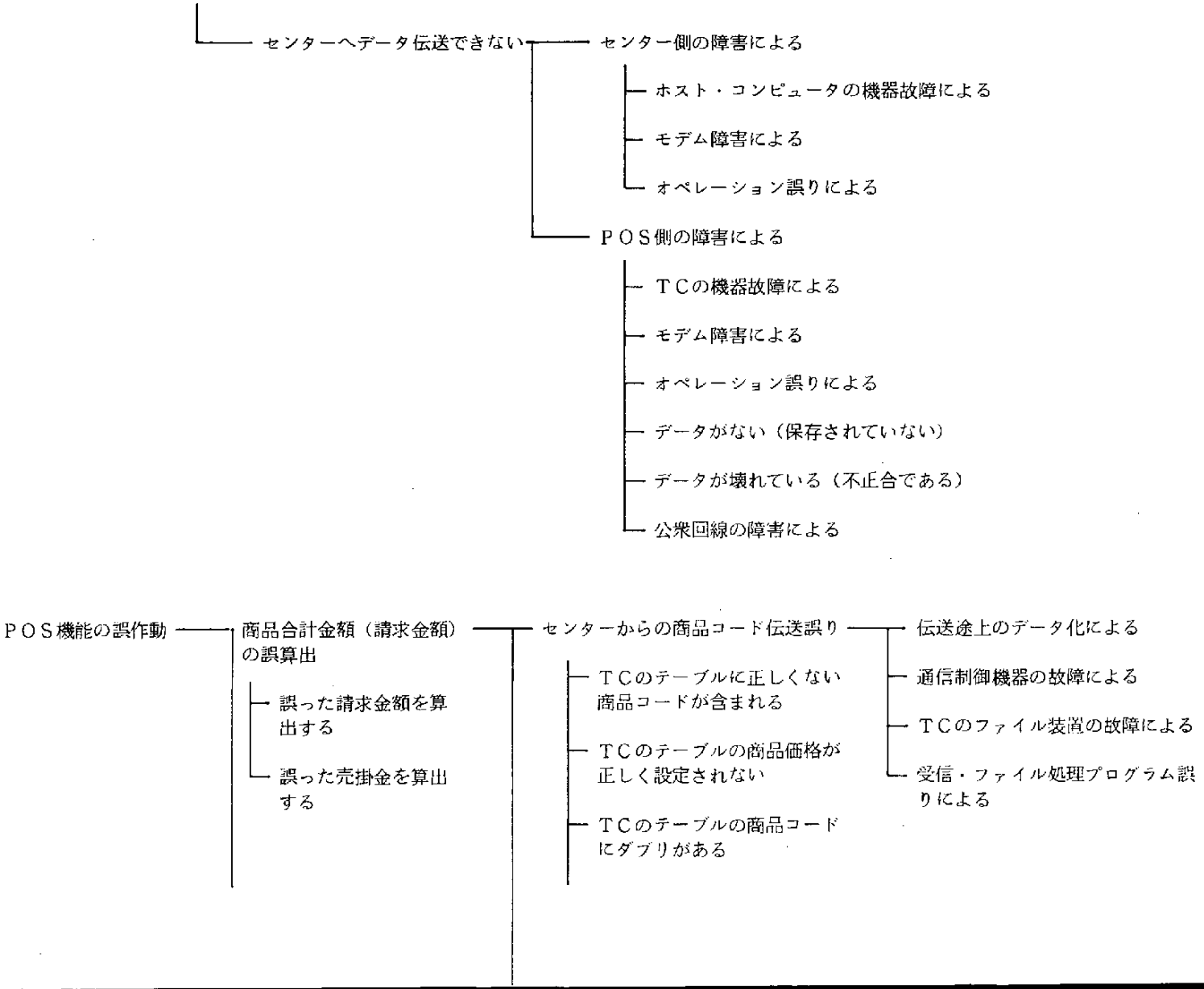
従って，このステップでは，原因を網羅的に掲げることを主目的とし，その掲げられた各原因自体の発生頻度が想定できるレベルまでブレークダウンされていれば十分である。

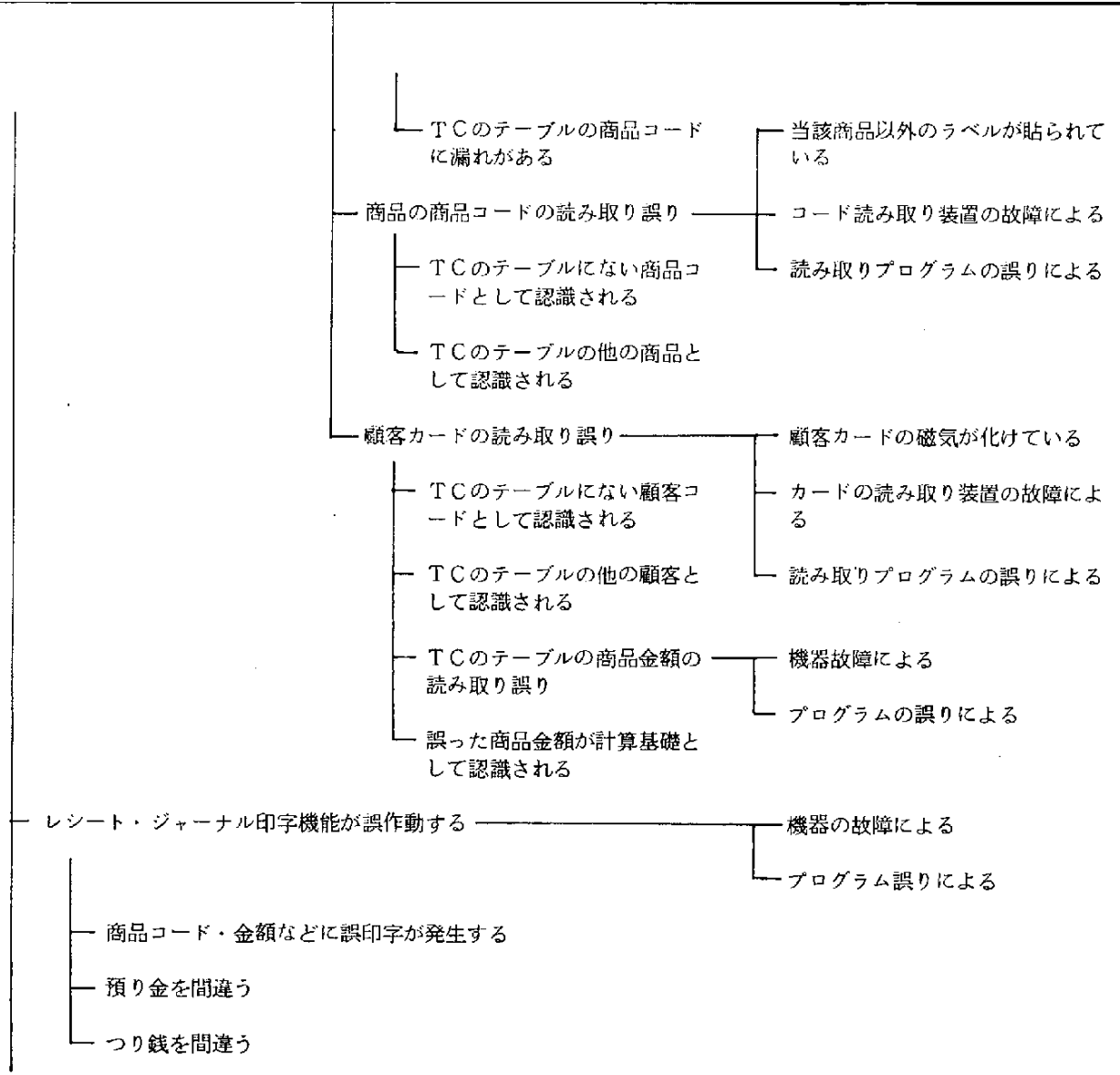
図2.　ＰＯＳシステムの事故事象と原因

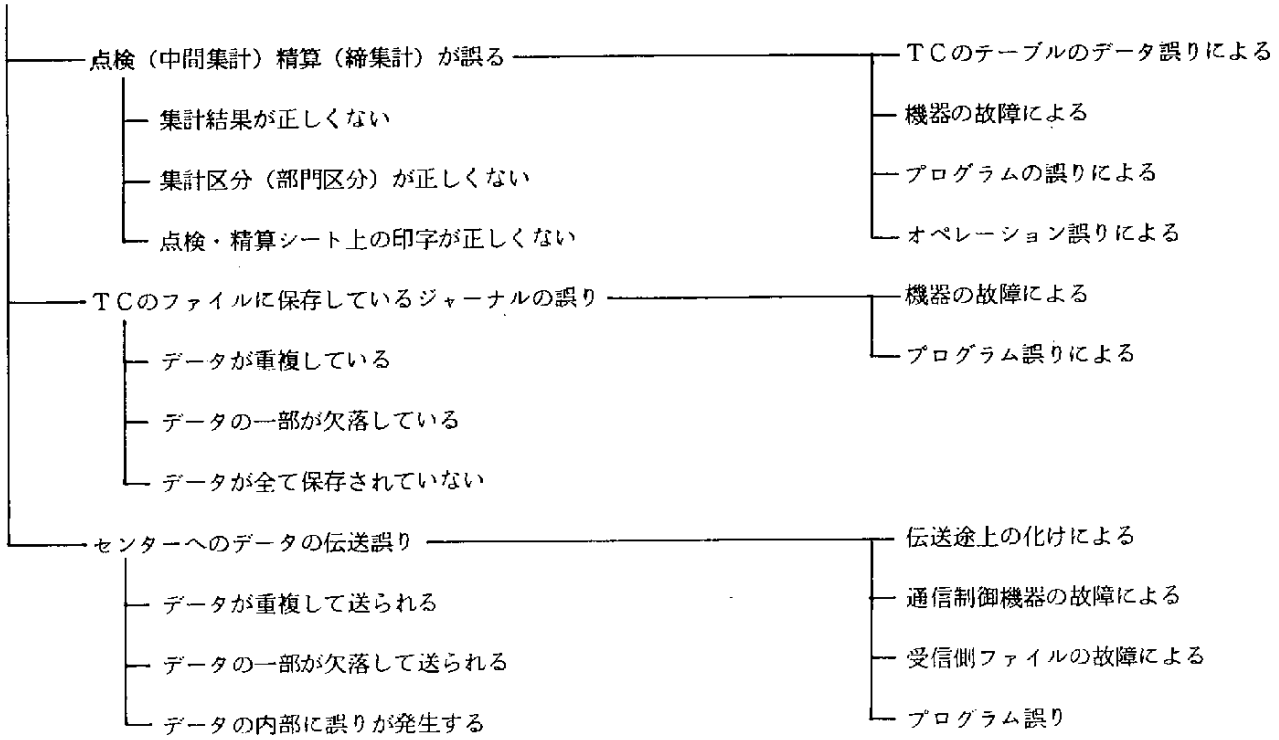



ＰＯＳレジだけが停止する
ＰＯＳに障害が発生する
電気が供給されない
停電（電力会社）
電源障害
火災
水害（洪水，落水）
雷害
プログラム誤りによる
ＴＣとＰＯＳ間のケーブル切断による
ＰＯＳ機能の一部停止
商品コードテーブルが更新できない
センターからの受信不能
モデムの障害による
公衆回線の障害による
ホスト・コンピュータの停止
機器故障による
オペレーション誤りによる
ＴＣの機器故障による
商品金額が読めない（ＰＯＳに登録している金額）
障害により読めない
プログラム誤りによる
機器故障による
ＴＣテーブルに金額がない
センターよりの伝送誤りによる
テーブルの更新誤りによる


プログラム誤りによる
商品合計金額が算出できない
（顧客への請求金額）
プログラム誤りによる
機器故障による
印字機能の不良
プリンター機器の故障による
用紙のフィード事故による
用紙の補給切れによる
プログラム誤りによる
顧客カードが読み取れない
ＰＯＳカード読み取り器の故障による
顧客カードの不良による
プログラム誤りによる
商品コードが読み取れない
バーコード・ラベルの不良による
バーコード・ラベルがない
スキャナの故障による
点検（中間集計），精算が
できない
取引区分の集計・印字ができない
プログラム誤りによる
機器故障による
オペレーション誤りによる


センターへデータ伝送できない
センター側の障害による
ホスト・コンピュータの機器故障による
モデム障害による
オペレーション誤りによる
ＰＯＳ側の障害による
ＴＣの機器故障による
モデム障害による
オペレーション誤りによる
データがない（保存されていない）
データが壊れている（不正合である）
公衆回線の障害による
ＰＯＳ機能の誤作動
商品合計金額（請求金額）の誤算出
誤った請求金額を算出する
誤った売掛金を算出する
センターからの商品コード伝送誤り
ＴＣのテーブルに正しくない商品コードが含まれる
ＴＣのテーブルの商品価格が正しく設定されない
ＴＣのテーブルの商品コードにダブリがある
伝送途上のデータ化による
通信制御機器の故障による
ＴＣのファイル装置の故障による
受信・ファイル処理プログラム誤りによる


ＴＣのテーブルの商品コードに漏れがある
商品の商品コードの読み取り誤り
当該商品以外のラベルが貼られている
コード読み取り装置の故障による
読み取りプログラムの誤りによる
ＴＣのテーブルにない商品コードとして認識される
ＴＣのテーブルの他の商品として認識される
顧客カードの読み取り誤り
顧客カードの磁気が化けている
カードの読み取り装置の故障による
読み取りプログラムの誤りによる
ＴＣのテーブルにない顧客コードとして認識される
ＴＣのテーブルの他の顧客として認識される
ＴＣのテーブルの商品金額の読み取り誤り
機器故障による
プログラムの誤りによる
誤った商品金額が計算基礎として認識される
レシート・ジャーナル印字機能が誤作動する
機器の故障による
プログラム誤りによる
商品コード・金額などに誤印字が発生する
預り金を間違う
つり銭を間違う


点検（中間集計）精算（締集計）が誤る
集計結果が正しくない
集計区分（部門区分）が正しくない
点検・精算シート上の印字が正しくない
ＴＣのテーブルのデータ誤りによる
機器の故障による
プログラムの誤りによる
オペレーション誤りによる
ＴＣのファイルに保存しているジャーナルの誤り
データが重複している
データの一部が欠落している
データが全て保存されていない
機器の故障による
プログラム誤りによる
センターへのデータの伝送誤り
データが重複して送られる
データの一部が欠落して送られる
データの内部に誤りが発生する
伝送途上の化けによる
通信制御機器の故障による
受信側ファイルの故障による
プログラム誤り

5. 経営に悪影響を及ぼす事項

(1) 悪影響を及ぼす事項の洗い出し

経営は，常に各種のリスクに取り囲まれている。本モデルシステムのスーパー・マーケットにおける経営上の重点項目である「店に収益を上げる」に対し，ＰＯＳシステムに関係なく悪影響を与えるものは何かについて，参加者全員によるブレーン・ストーミング方式で洗いだした。「従業員」，「電源設備」，「商品」，「棚」のように断片的な表現は，参加者全員が同じ意味でとらえているとは限らないので，これらの文言を，「何がどうなる（どうする）」の完結型にし，参加者全員が同じ理解になるようにした。

(2) 悪影響を与える項目の類型化

店の収益が上がらない原因は，大きく分けると，「売上が上がらない」，「経費が多い」，「損失が多い」の３分類になる。各々の原因を類型化したのが図３（経営に悪影響を及ぼす事項）である。以下，それぞれの項目について若干の補足説明を加える。

(a) 「売上が上がらない」

店の収益を上げるためには，当然商品の売上が上がることが必要である。売上が上がらない原因を堀り下げると，顧客の来店が少ない，つまり「客足が悪い」と，顧客が来店しても商品を買うことが出来ない，つまり「店がオープン出来ない」の２つに大別することができる。

① 「客足が悪い」

売上が上がらない原因を堀り下げると，できるだけ多くの顧客が来店することにより，多くの売上が期待できるのである。つぎに，その原因について，以下に述べる。

・ 「間違いが多い」

レジにおける請求金額を多く請求したり，釣り銭を少なく渡したりという間違いが多く発生すると，扱っている商品そのものも含めて店

の信用を失うことにつながる。金額を少なく請求したり，釣り銭を多く渡したりすることが多く発生する場合でも，顧客の不満は少ないであろうが，不安が大きくなり，やはり信用がなくなることになる。従って，客足が悪い原因の一つになる。

・「待ち時間が長い」

買い上げた商品をレジで清算するときに，「待ち時間が長い」と感じる原因が２つ考えられる。１つは，ＰＯＳレジの行列そのものが長く順番が遅いと思うとき，２つ目は行列が短くても，レジ担当者の動作が緩慢な場合である。前者はレジを増やせ，後者はレジ係の熟練者を配置しろ，の不満につながる。

・「売るものがない（欠品）」

欠品とは，売るべき商品，あるいは顧客の買いたい商品がない状態であり，毎日一定量の売上が見込まれる商品に欠品が多くなると，顧客の来店は少なくなる。必ずあると期待してきた顧客が，欠品のためにやむなく他の店に出かけることになり，２度手間になるからである。

・「価格が高過ぎる」

ある商品が，他のスーパー・マーケットの商品と比較して，商品の鮮度や大きさに差があれば値段が違うことに納得するが，差が感じられなければ，１円でも高い方の店は全体の商品が全て高いと顧客は感じてしまう。

・「顧客からの返品が多い」

一度買い上げられた商品を返品するには，商品の鮮度が期待した鮮度より低い，商品に欠陥がある，すぐに壊れてしまった，腐っていた等が原因になる。返品が多いことは，店のイメージの失墜になり客足は悪くなる。

・「商品の種類が少ない」

欠品とは違う意味で，店で取り扱う商品の種類が少ないことも問題である。その店で買い物を全部済ませようと期待してくる顧客が，取

り扱い商品が少ないために他の店に行くことになる。そのために客足が段々と遠のく。

・　「良い商品がない」

メーカーや卸問屋から，品質の良い商品を仕入れる事が出来ないと客足に影響する。

・　「棚割りが悪い」

顧客の買いたい商品が，すぐに見つけることができないと，余分な時間がかかってしまう。また，目的の商品（メーカー）をさがしきれずに，違うもので間に合わせる結果となると，商品が無かったとの印象になり客足が悪くなる。一方，店側に立った場合は，顧客の目に止まるような棚割りを行わないと，特に売りたいと思っている商品が売れないことになる。

・　「立地条件が悪い」

自転車や徒歩で来店する顧客については，直線距離が短くても，途中に鉄道の線路や川等があり，遠回りするような場合には，その店に余程の魅力が無いと顧客は来店しない。また，自動車で来店する顧客は，ある程度の広さの駐車場の確保と駐車場に入るまでの道路の道幅や混雑状況にて便利さを測るため，これらが客足を左右することになる。

・　「レイアウトが悪い」

棚割りが悪い項目と若干関係するが，これは買い物通路の広さ，商品棚の位置，レジカウンターの配置，店の入口の配置等で，買いやすい店とか気持ちの良い店等の印象につながり，客足に関係する。

・　「営業時間が短い」

店が営業している時間の長さや閉店する時間に関しては，市街地や住宅地等，立地場所に大きく左右される。共働きや単身者の多い地区では，会社の終業時間に合わせ，帰宅時間を考慮して閉店時間を設定することも一つである。買いたいときに買えることを顧客は願ってい

るのである。

・　「宣伝が足りない」

常に顧客は目新しい物，安いものを追求しているものであり，チラシ，ポスター等で注目させることが必要になる。変化していること（活気）を顧客に感じさせなければ，顧客の来店する回数は段々と減っていく。

・　「サービスが悪い」

このサービスとは，上得意な顧客や買い物の回数が多い等の顧客に対して，特別割引やスタンプ・サービスのような付加価値サービスをいう。同業他店でこのようなサービスを実施している場合に，当店でこのサービスが無ければ，顧客はサービスが無いといい，このサービスがあっても，条件が他の店より悪ければ，サービスの良い店へと顧客は流れて行く。

・　「作業者の態度が悪い」

これは，レジカウンターの人を含めて，顧客に接する全ての人を含んでいる。応対の言葉遣い，態度，物腰等の一つでも悪いと，俗にいう，感じが悪い店となり，イメージが失墜して顧客は来店しなくなる。

②　「店がオープンできない」

売上が上がらない原因のもう一つは，顧客が来店しても店をオープンすることができない状況が発生することである。

・　「従業員が確保できない」

多数の従業員が突然退職する，労組がストライキを行う，あるいは鉄道の事故等で通勤手段が断たれる場合等で，店を営業する最小限の人数が確保できない状態が発生することが考えられる。

・　「店が災害を被る」

店が火災，地震，水害等の自然災害で直接的な被害を被ったり，破壊や爆破のような人間の悪意による行動から被害を被る場合がある。

・　「営業停止処分を受ける」

販売された食料品による食中毒の発生，不良図書や不良玩具の販売，消防法違反等の改善勧告の不履行等により監督官庁からの行政処分を受けることが考えられる。

・「電力が供給されない」

店で使用する照明，冷凍／冷蔵用，ＰＯＳシステムのための電力が，事故や工事により供給されないために店がオープンできない。

・「脅迫を受ける」

恨み，妬み，営利等の目的で商品に毒を混入した，あるいは爆弾を仕掛けた等の脅迫を受け，問題が解決するまで営業することができない事態になる可能性もある。

(b) 損失が多い

収益を低下させる原因の一つは，損失が多くなることである。その損失の原因については，つぎの３項目をあげることができる。

① 売り掛け金が回収できない

商品の売上が上がっても，現金の支払でなく売り掛けの場合は，後日に清算されることになる。この売り掛け金が回収できないと損失になる。その原因としては，支払い能力がない，連絡が跡絶える等の顧客の問題と，売り掛け請求の間違い，記載情報の間違い，電磁記録の消失等の店側の問題がある。

② 現金が合わない

釣り銭の間違いや請求金額の間違い等により，ＰＯＳレジの売上金額の合計と実際の現金が合わない。この項目には不正行為を含めないことにした。

③ 不正行為

顧客とレジ係との共謀により，ＰＯＳレジに入力しないで素通りする。レジの素通りはしないが，商品の価格を不当にディスカウントして実際の請求金額を少なくする。商品が万引きされる。現金が着服されてしまう。

(c) 経費が多い

店の利益は，総収益から損失や経費を差し引いた残りになる。経費が多いことは，収益を左右することになる。経費にかかわる項目をあげると以下の通りである。

① 人件費が多い

1人当たりの人件費が高い場合と，余剰人員が多い場合とがある。

② 設備が過剰

必要以上の設備を設置し，設備費や運用費が多くかかる。

③ 在庫が多い

余剰在庫を保持するために経費が増加する。

(3) 経営に悪影響を及ぼす事項とＰＯＳシステムの事故事象との関連

ＰＯＳシステムの事故事象が，経営上どの程度の影響を及ぼしているかを明確にする必要がある。本モデルにおける経営に悪影響を及ぼす事項とＰＯＳシステムの事故事象を関連づけたのが図4，5，6である。

- ＰＯＳシステム機能の全面停止および一部停止は，顧客に対して「待ち時間が長い」という悪影響に結びつく（図4）。度重なれば，当然客足が遠退き，売上と収益が減少することになる。しかし，ＰＯＳシステムの機能のうち，レジ係の交替時等における中間集計，一日の最後に実行する清算業務，日中の売り上げ等のセンターへのデータ伝送等が何らかの理由で実行不能になっても，ＰＯＳシステムの運用上では大きな問題となる恐れがあるものの，顧客への影響はほとんど考えられない。
- ＰＯＳシステム機能の誤作動により，商品合計金額を誤算出したり，レシート・ジャーナル印字機能の誤作動が発生すると致命的ともいえる「間違いが多い」処理を行うことになる（図5）。その結果として店の信用が失墜し，顧客が減少することになり，売り上げが上がらなくなる。
- スーパー・マーケットの売り上げデータ等のセンターへの伝送誤り，ＴＣ上のファイルの売り上げ情報や売り掛け情報の誤り等が発生した場合に，

センター側では誤った情報を基に各種の処理を実行することになる（図6）。その結果，顧客への「売り掛け金が回収できない」，あるいは，売り上げ情報の不正確から「売るものがない（欠品）」，「在庫が多い」という事態が発生する。そして，客足が悪くなることや予想外の経費が発生したりすることにもつながる。

図 3.　経営に悪影響を及ぼす事項

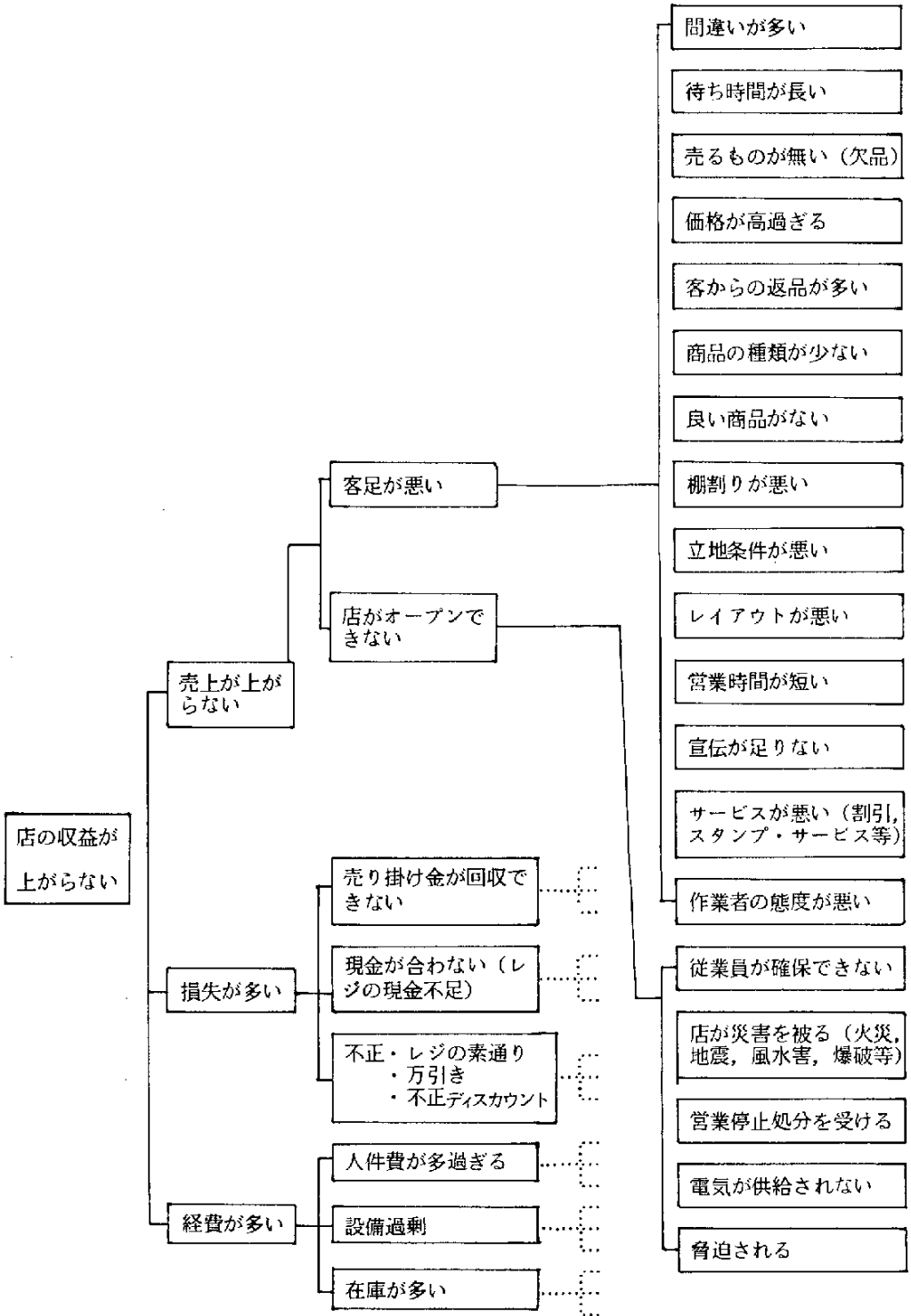


図4.　ＰＯＳシステム機能の全面停止および一部停止と経営に悪影響を与える事象

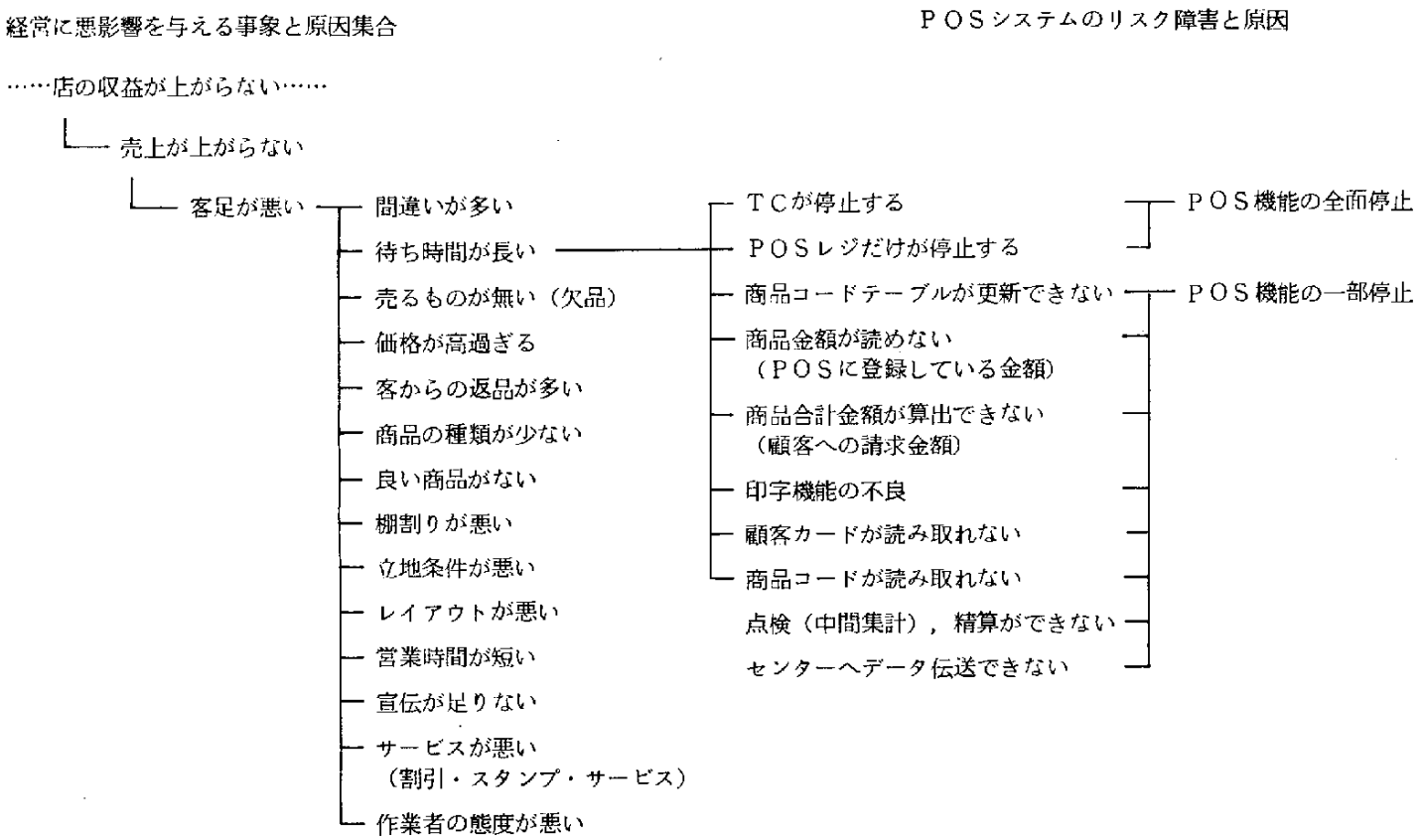


図5.　ＰＯＳシステム機能の誤作動と経営に悪影響を与える事象との関連

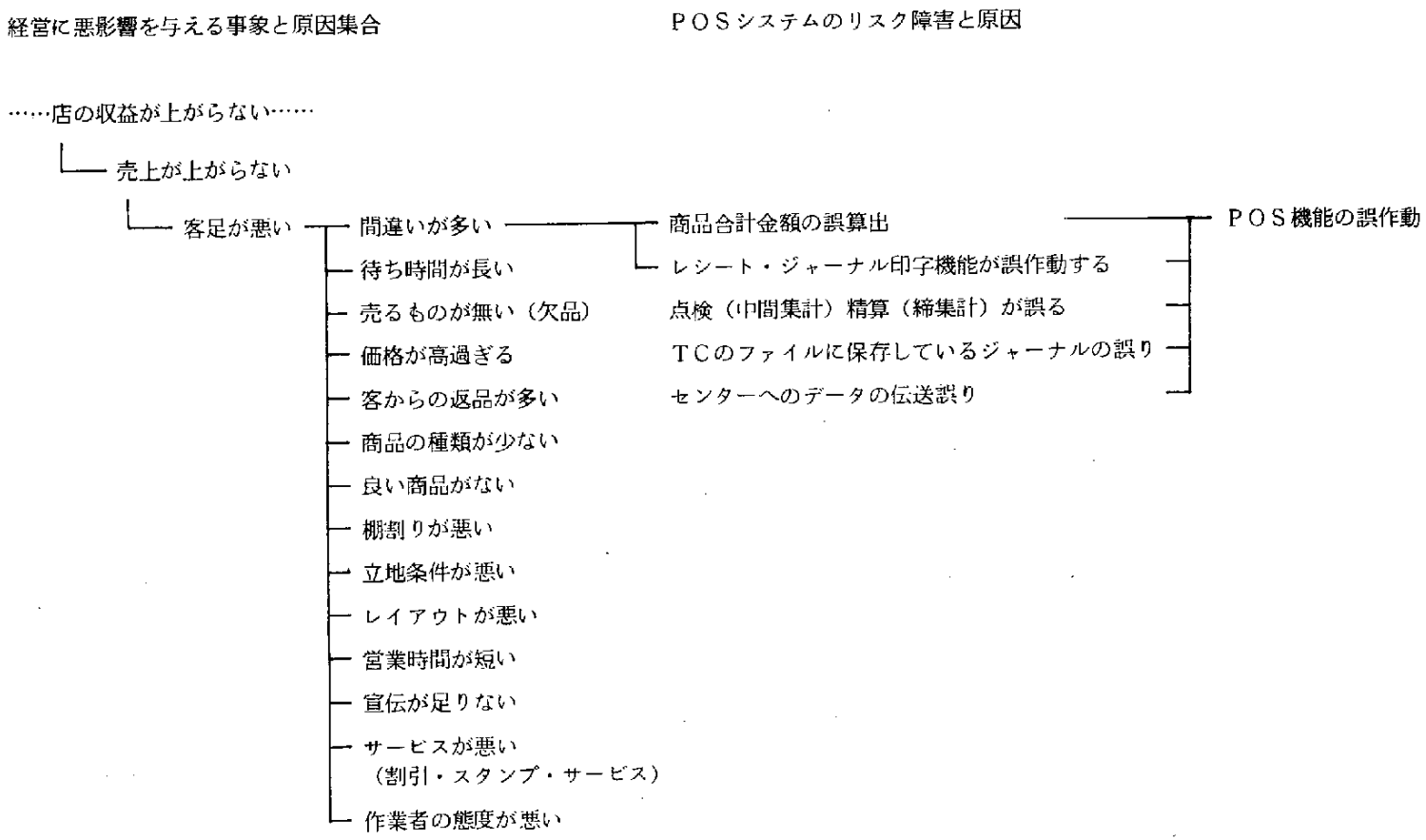
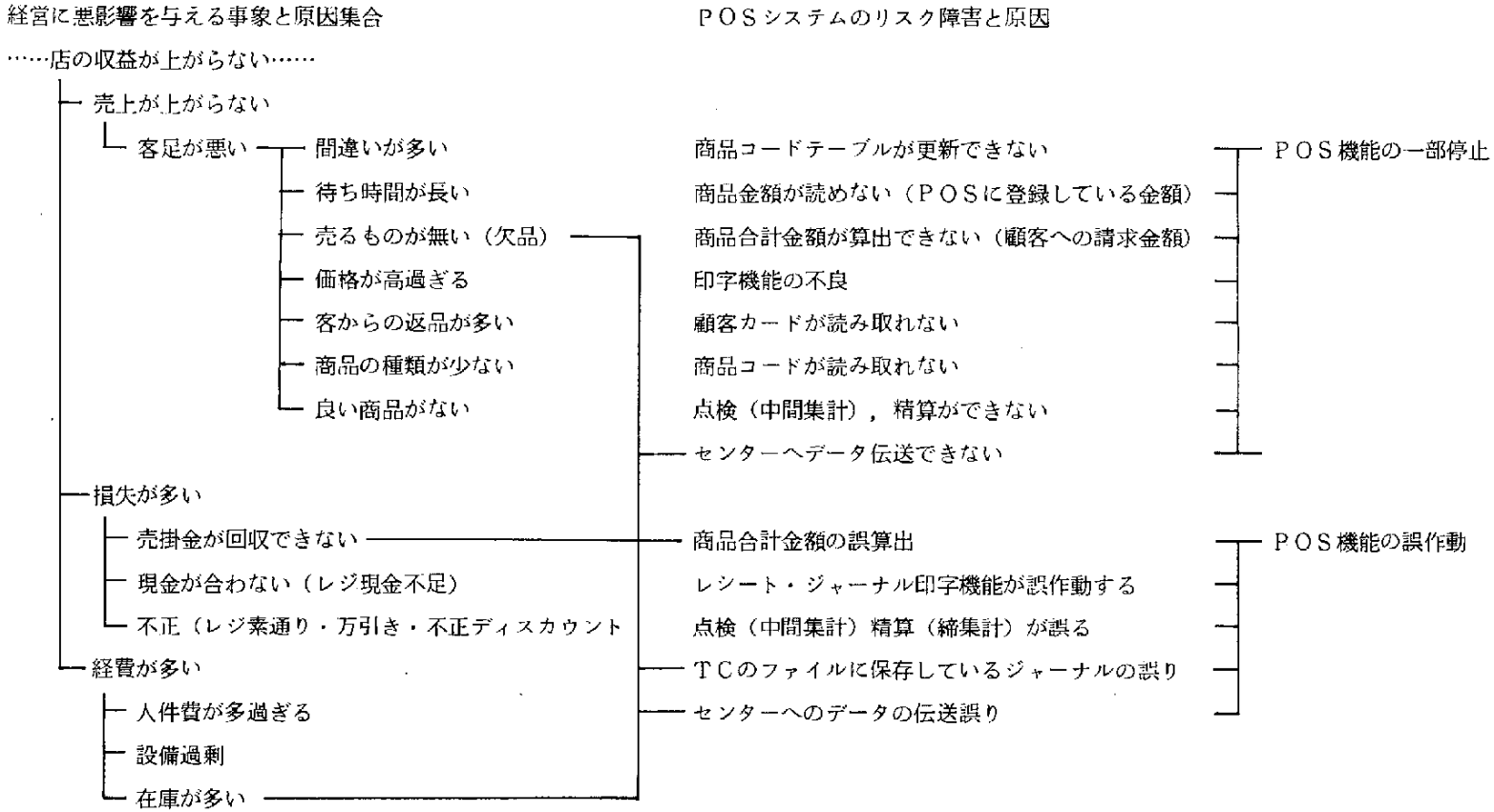


図6.　ＰＯＳシステム機能の一部停止，誤作動と経営に悪影響を与える事象との関連



6. 今後の課題

このリスク分析では，モデルとしたスーパー・マーケットにおけるＰＯＳシステムの事故事象と原因の明確化，経営に悪影響を及ぼす事象の明確化，および経営に悪影響を及ぼす事象とＰＯＳシステムの事故事象との関係づけを行った。

(1) リスク・マネジメントの１ステップとしてのリスク分析

もちろん，これらの悪影響，ＰＯＳシステムの障害のすべてが営業に致命的な打撃を与えるものではなく，収益の大幅減少をもたらすものもあれば，ほとんど無関係なくらい影響を及ぼさないものもある。例えば，数台あるＰＯＳレジ端末の１台が，閑散時に数分ストップしたような障害は，全体からみて影響なしといって差しつかえない。しかし，ＰＯＳシステムが，プログラムの誤りなどで多額の売上代金を顧客に請求した場合，店の信用は凋落し，顧客数の減少によって，売上，収益の激減をきたす恐れが十分にある。

要約すれば，リスク分析を行う対象に発生する阻害要因が引き起こす悪影響のうち，①システム障害によるリスクがどのようにかかわっているか，②そのシステムリスクは全体のマイナス要因のうちでどの程度を占めているか，などを明確にする必要があるといえる。

このためには，リスクの明確化に続いてリスクの測定を行うことが大切で，これらに基づいて，リスク処理といわれる「損失予防」「損失軽減」「リスク分散」「リスク保有」「保険」などの手法の幾つかの組み合わせ，いわゆるツールミックスを実行することになる。

(2) リスク測定へのアプローチ

情報システムは激動する経済環境，ハードウェアの技術革新等のなかで，拡大と変化をつづけていることは衆知のとおりである。このように流動的な立場にあるシステムでは，リスク測定に不可欠な各種の有効なデータが皆無

に近く，加えて，今まで予想もしなかった新しいリスクが発生することも想定される。

しかし，リスクの発生により企業が受ける打撃を回避するためには，リスクを何らかの方法で測定のうえ，重要性が高いと思われるリスクから順次対策をたてることが企業経営の安全性を確保するうえから急務であるといえる。

このリスクの測定とリスク対策および評価には，つぎのことが考えられるが，今後の研究課題として取り組むこととした。

(a) システムの事故事象の測定

システムに発生する事故事象は，「何を原因として，その事故が発生しているか。」でリスクの大きさが異なる。そこで，事故事象とその原因の関係を明確にしたうえで，事故の頻度，事故の影響範囲を踏まえてリスクの影響度の大きさを測定し，企業にどのような形で，どの程度の悪影響を及ぼすのかを分析できるようにしておく必要がある。

(b) 経営に悪影響を与える事象の測定

企業に悪影響を与える各種の事象を分析のうえ，それらの事象が発生する頻度，影響範囲を明確にし，財務上に与えるインパクトを測定したうえで，システムに発生するリスクによる悪影響の度合いを何らかの方法で認識できるようにしておく必要がある。

(c) システムの事故事象が企業に与える悪影響の測定

(a)，(b)で行ったそれぞれの分析と測定に基づき，システムにリスクが発生したときに企業がどの程度の悪影響を受けるか，その損害はどれ位になるかを明確にし，どの事故事象からリスク処理を行うのが最も効果的か，どのようなツールミックスを適用するかを立案する。

(d) リスク処理およびその対費用効果

(c)で立案したリスク処理を権限者の承認を得たのち実行し，一定期間経過後，そのリスク処理の有効性を評価する。このリスク処理の評価に当たっては，リスク対策に投下したリスク対策費とリスク発生防止効果を十分に検証することとなる。

(3) モデルとするシステムの範囲の拡充

本リスク分析では，分析を簡明に進めるため，対象範囲を限定したＰＯＳシステムをモデルとして設定した。しかし，現状におけるＰＯＳシステムは伝送回線を利用して，ＶＡＮとの接続，銀行ＰＯＳへの展開などと巾の広いシステムとなっている。

ＰＯＳシステムに限らず，現在の情報システムでは，ネットワーク・システムが不可欠であることはいうまでもない。このネットワーク・システムのリスク分析は，今後の研究に委ねることとした。

第2章 ヒューマンエラー分析

1. ヒューマンエラー

(1) ヒューマンエラー分析の必要性

ヒューマンエラー分析は，従来の調査研究段階において，その必要性は認識されてはいたが，具体的な形でとりあげられなかった。

しかしながら，最近の動向として，情報システムはますます複雑になる一方，システムの安全性，信頼性がより強く要求される社会環境になってきている。

ハードウェアの面におけるリスク対応としては，構成装置内回路の多重化がはかられている。また，システム構成機器についてもリスク対応として機器の多重化をはかるなど，かなりの進展がうかがえる。

一方，複雑化するシステムに関与する人間が原因で生じるヒューマンエラーは，システム全体のリスクを考える場合，無視できない要素となってきているが，実際にはその実態が明確に把握されていない。

ヒューマンエラーの発生場面は，稼働中のシステムで，その原因を大別すると，ソフトウェアに関するもの，システム運用に関するもの，システム管理に関するもの等があげられる。これらのヒューマンエラーは，リスク分析を行う上で避けて通る事のできないものである。このため，今回は，ヒューマンエラーをとりあげ，ヒューマンエラーをどのように分析すれば把握できるのかに重点を置いて検討した。

ここにおける分析手法は，一つの試みとして行ったものであり，確立した手法ではない。

ヒューマンエラーについては，諸々のアプローチがあるが，FTA（Fault Tree Analysis）や要因系統図を使用して分析することが，視覚的に表現でき，かつ，内容の把握も容易になるとの判断から，ここでは，これらを活用することとした。

(2) ヒューマンエラーの定義

ヒューマンエラーとは，人間がシステムの安全性・信頼性を確保し，かつ効率的にシステムを運転するという観点から見ることとし，つぎのように，「システムで定められた仕様及び運用様式に従わずに行動し，システムに何らかの異常を発生させる行為」と定義した。したがって，故意に行う行為は犯罪であるため，ヒューマンエラーからは除外することとした。

2. 事故事象と原因集合

(1) 事 故 事 象

事故事象とは，ヒューマンエラーが発生した事によって，コンピュータシステムが本来持っている目的を果たせなくなることをいう。

今回のヒューマンエラー分析においては，ヒューマンエラーによって発生する事故事象の主なものとして，次のようなものが把握された。

① 稼働中のシステムが停止する。

システムが運転中にヒューマンエラーによって，各種の障害が発生し，停止してしまう事象。

② 稼働中のシステムが，機能縮退して運転を行う。

ヒューマンエラーによって，運転中のシステムに障害が発生し，一部機能を停止または除外して運転を行う事象。

③ 稼働中のシステムが誤動作する。

ヒューマンエラーによって，運転中のシステムに障害が発生しているにもかかわらず，誤作動したまま運転を続けている事象。

④ 稼働中のシステムが輻湊する。

ヒューマンエラーによって，稼働中のシステムに障害が発生し，障害個所は除外したが所定の性能が出ず，輻湊状態にある事象。

⑤ 処理結果の不正合

ヒューマンエラーによって，処理結果が正しくなされなかった事象。

⑥　稼働中のシステムの破壊

ヒューマンエラーによって，稼働中のシステムの装置および記録媒体等が破壊され，システムの本来機能を満たせなくなった事象。（破壊後上記①～⑤の事象につながる。）

(2)　原　因　集　合

事故事象に結びつくエラー原因の集りを原因集合という。

原因の分析をする場合，どこまで分析するかが問題になる。たとえば，つぎのような考え方もできる。

①　具体的な対策が立てられると思われる明確な原因を把握した時点で，事故終了する。

②　これ以上分析しても意味がないと思われる場合は，その時点で終了する。

3.　原因分析の手順

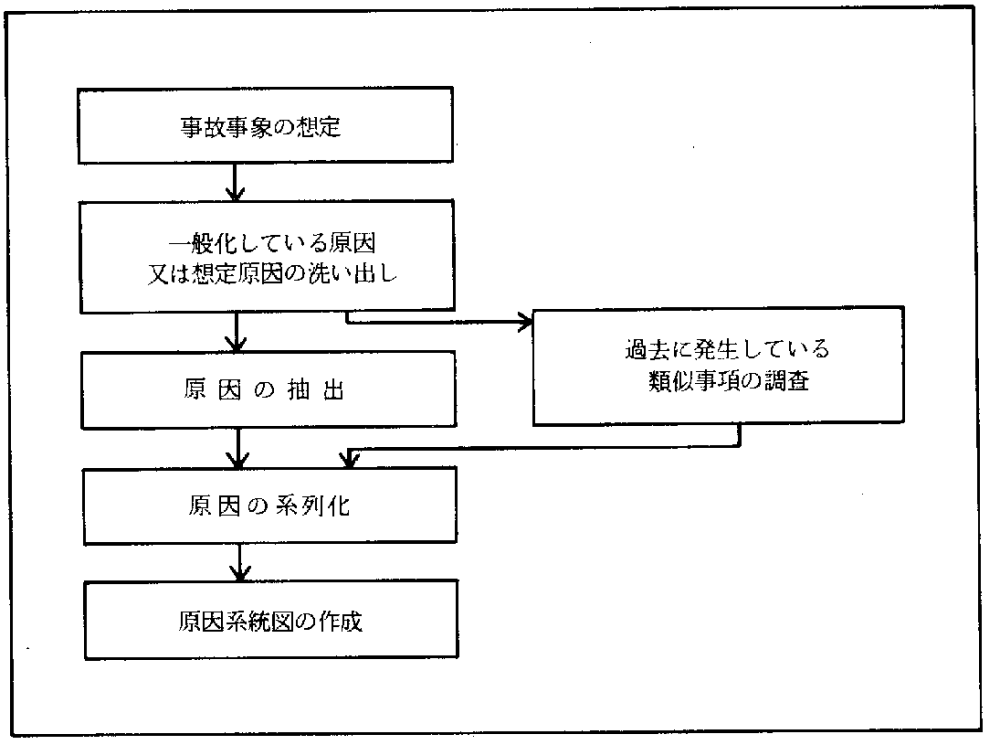
情報システムは，規模およびシステムの運用形態によって，データのインプット方式を始め，運用管理方法も異なってくる。しかしながら，ヒューマンエラーの原因を分析する手順は同じであろうと考えられる。ここでは，次図のように手順を決めた（図7）。

(1)　原因の洗い出し

事故事象に対する原因を洗い出すため，ブレーンストーミングを行った。

まず，事故事象を想定する必要があるため，「稼働中のシステムが停止した」と云う事故事象を想定した。その理由は，一般的にシステムダウンが発生すると損害も大きいからである。

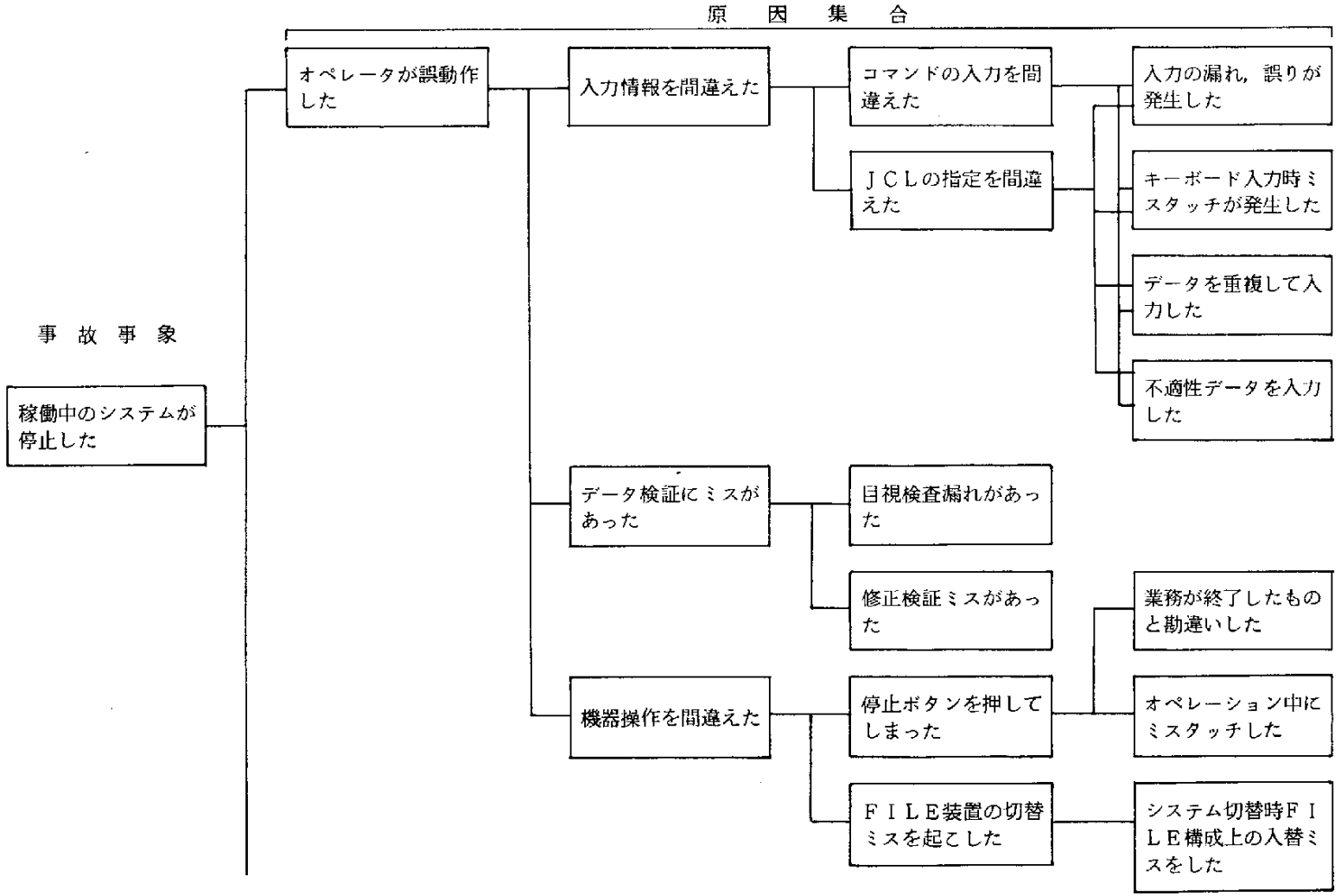
図7. 分析の手順

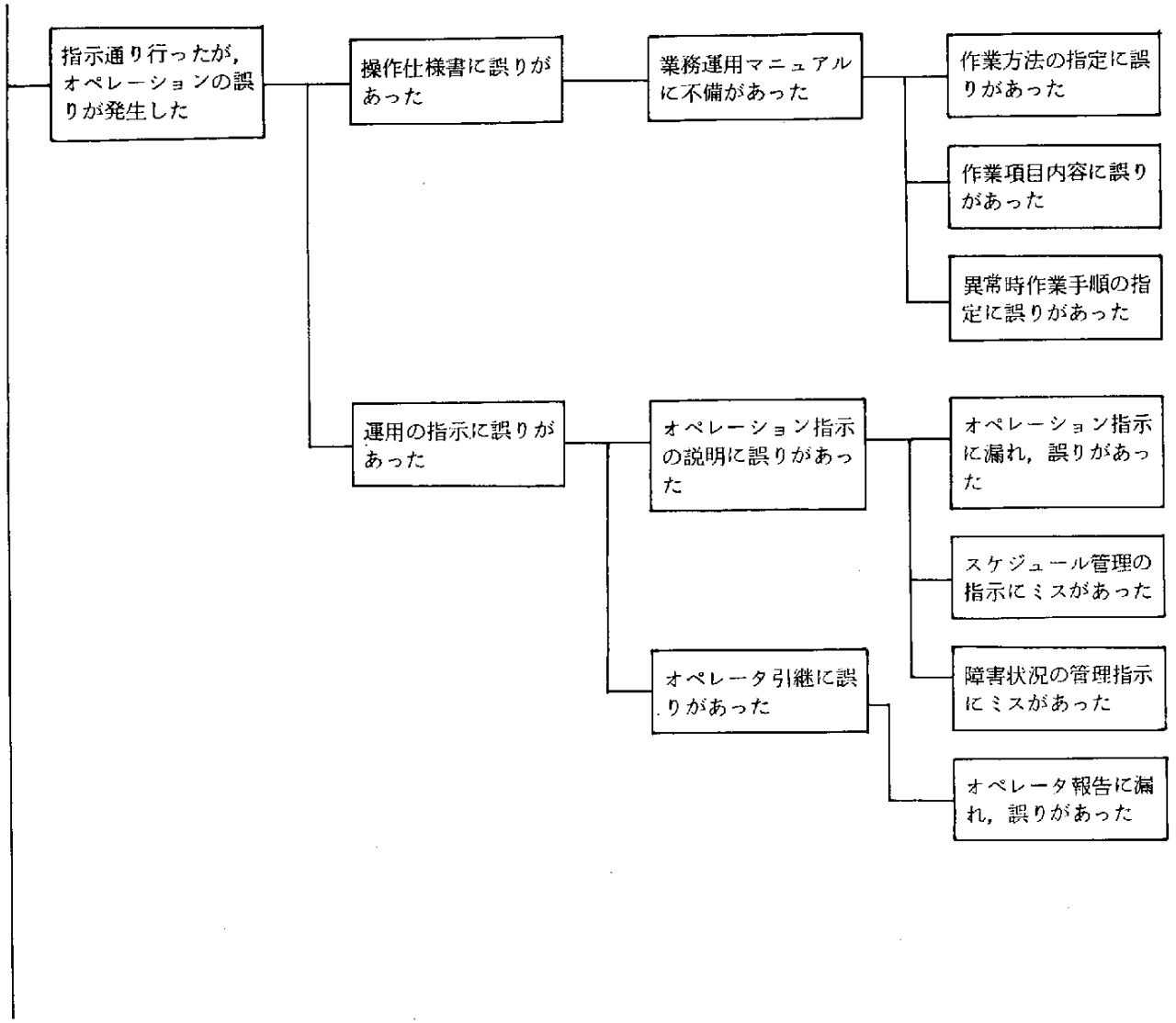


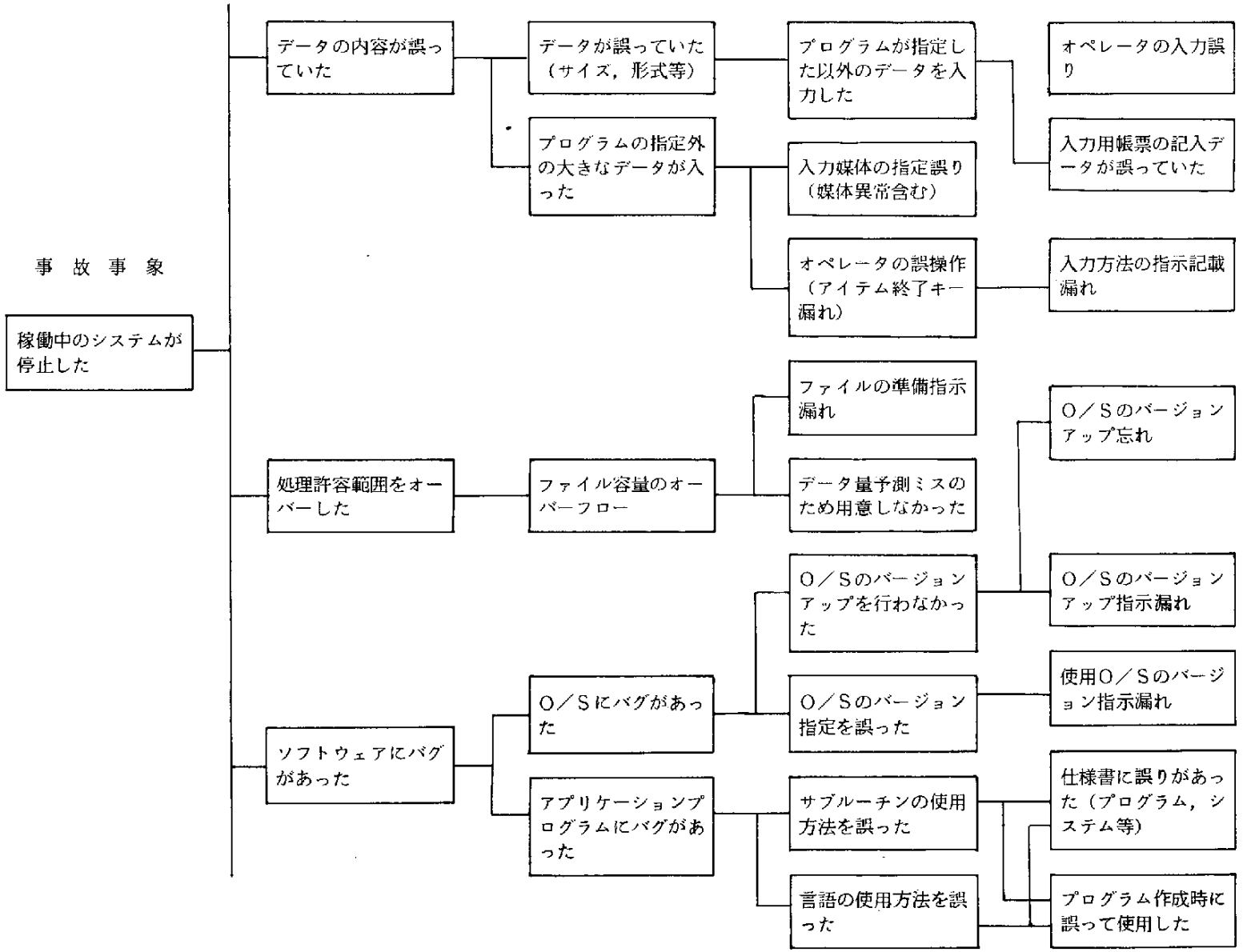
(2) 事故事象と原因集合の整理

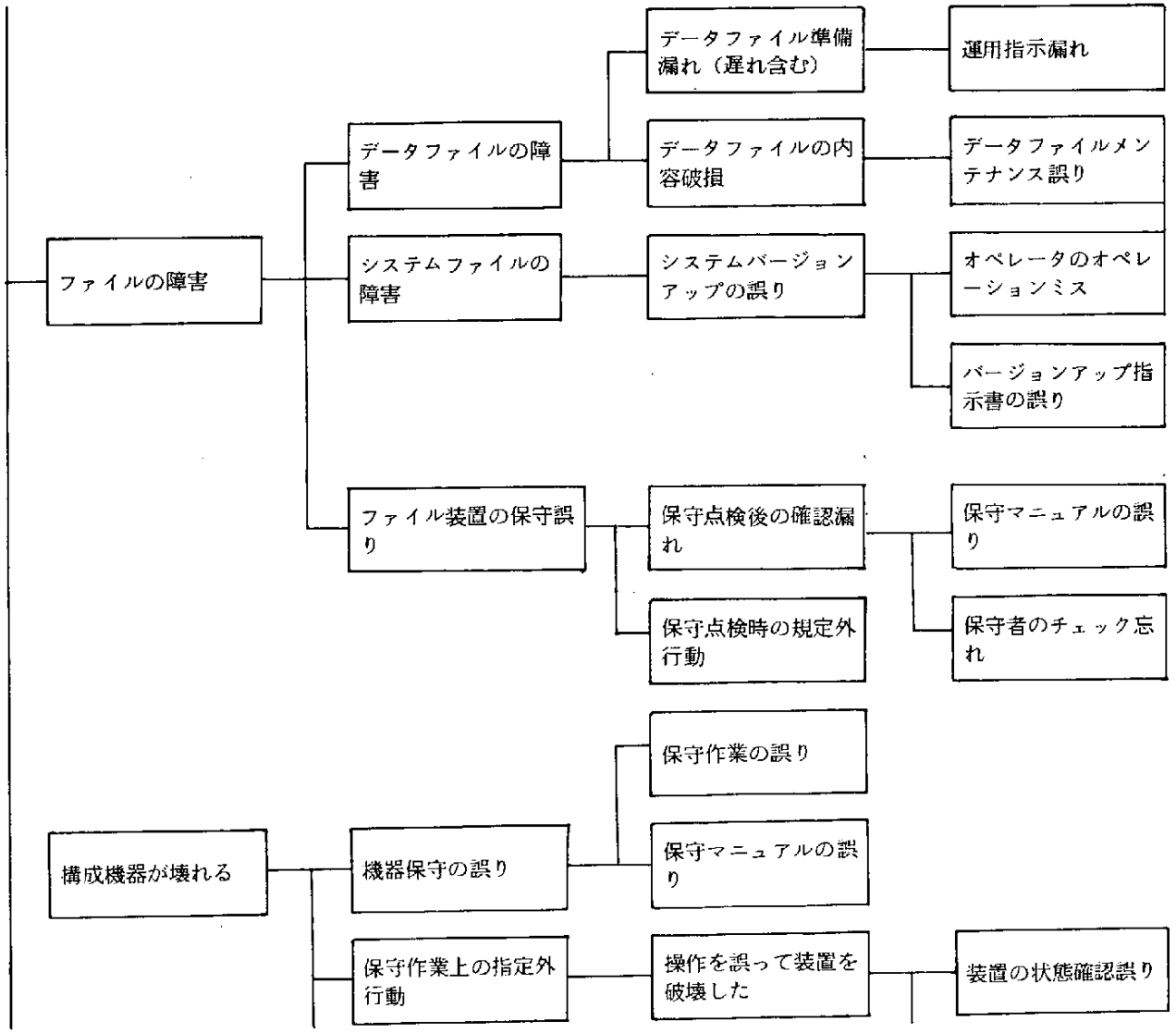
「稼働中のシステムが停止した」という事故事象に対する原因集合を，事故事象に関係の深い順に並べ，系統図を作成した（図8）。

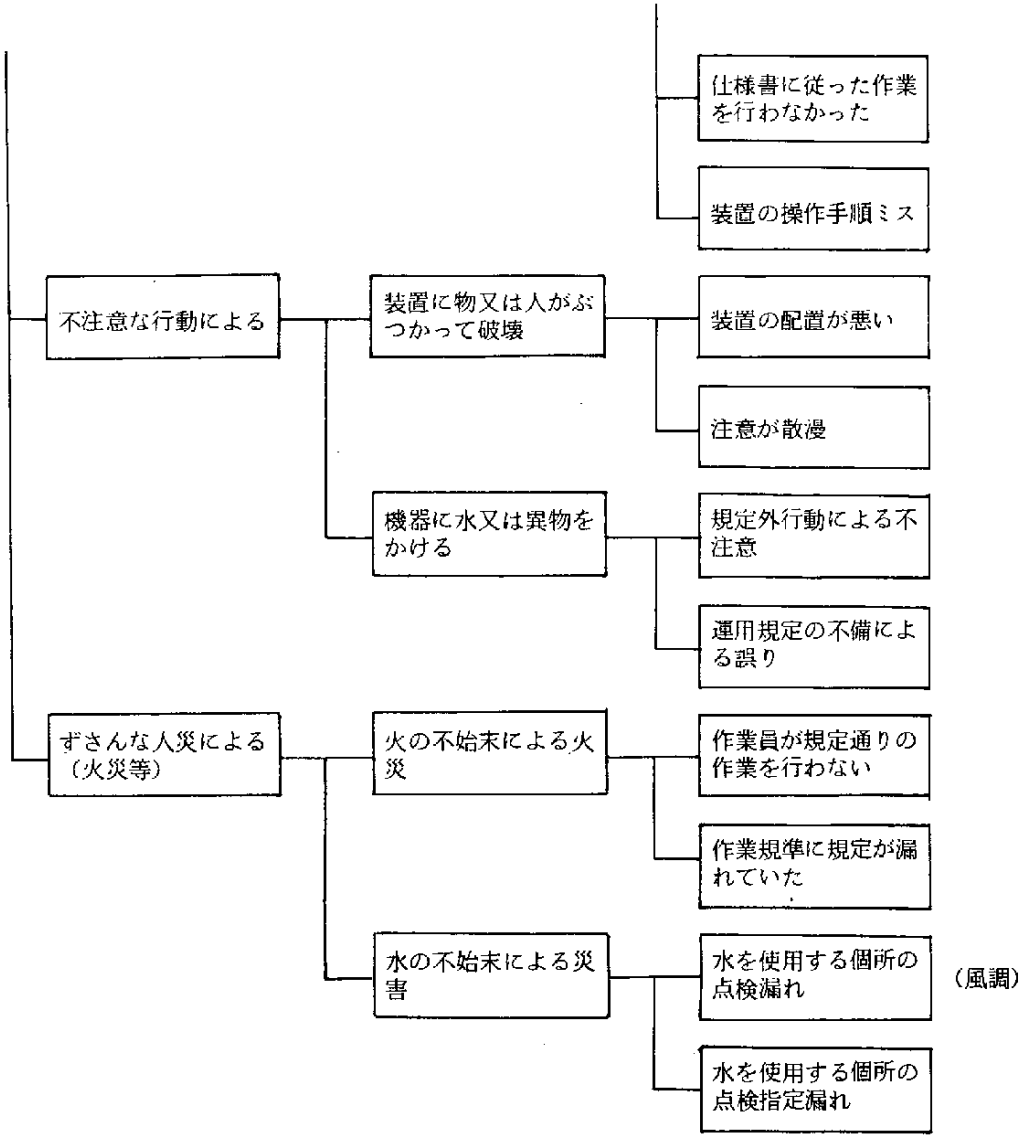
図8.　事故事象と原因集合



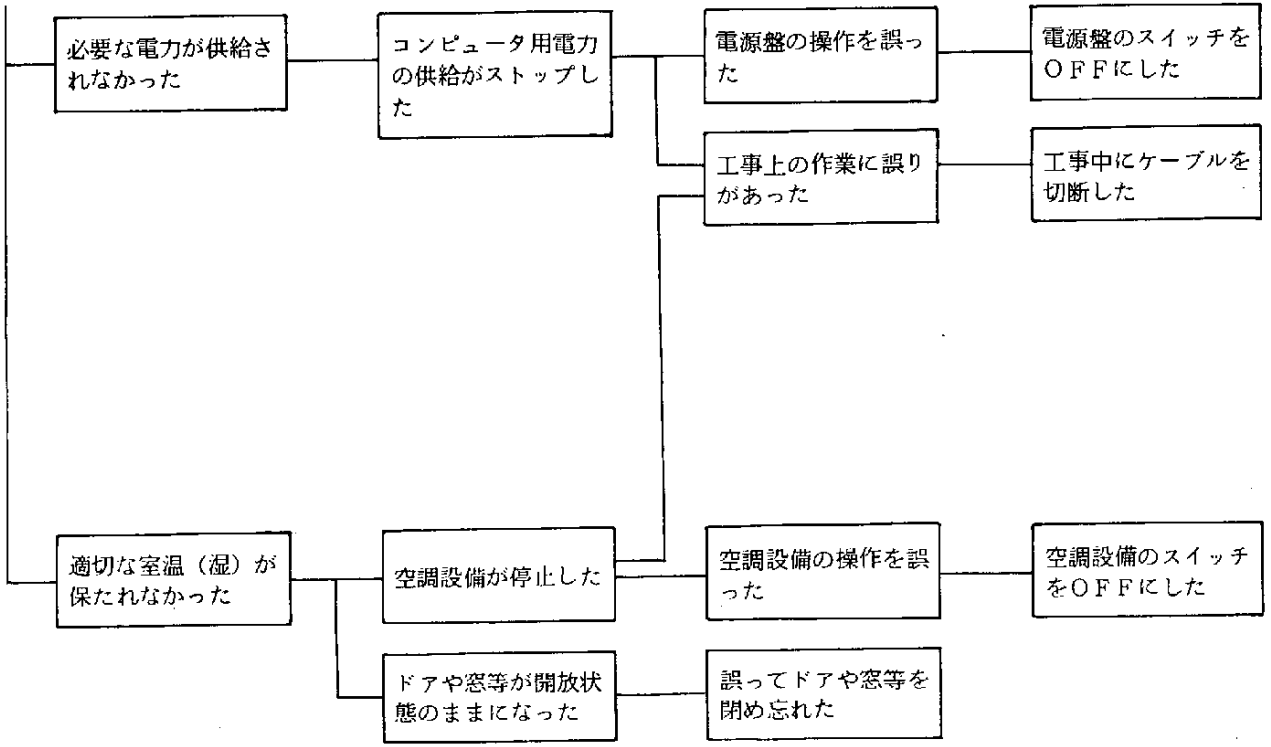

指示通り行ったが，オペレーションの誤りが発生した
操作仕様書に誤りがあった
業務運用マニュアルに不備があった
作業方法の指定に誤りがあった
作業項目内容に誤りがあった
異常時作業手順の指定に誤りがあった
運用の指示に誤りがあった
オペレーション指示の説明に誤りがあった
オペレーション指示に漏れ，誤りがあった
スケジュール管理の指示にミスがあった
障害状況の管理指示にミスがあった
オペレータ引継に誤りがあった
オペレータ報告に漏れ，誤りがあった


事故事象
稼働中のシステムが停止した
データの内容が誤っていた
データが誤っていた（サイズ，形式等）
プログラムの指定外の大きなデータが入った
プログラムが指定した以外のデータを入力した
入力媒体の指定誤り（媒体異常含む）
オペレータの誤操作（アイテム終了キー漏れ）
オペレータの入力誤り
入力用帳票の記入データが誤っていた
入力方法の指示記載漏れ
処理許容範囲をオーバーした
ファイル容量のオーバーフロー
ファイルの準備指示漏れ
データ量予測ミスのため用意しなかった
ソフトウェアにバグがあった
O／Sにバグがあった
アプリケーションプログラムにバグがあった
O／Sのバージョンアップを行わなかった
O／Sのバージョン指定を誤った
サブルーチンの使用方法を誤った
言語の使用方法を誤った
O／Sのバージョンアップ忘れ
O／Sのバージョンアップ指示漏れ
使用O／Sのバージョン指示漏れ
仕様書に誤りがあった（プログラム，システム等）
プログラム作成時に誤って使用した


ファイルの障害
データファイルの障害
データファイル準備漏れ（遅れ含む）
運用指示漏れ
データファイルの内容破損
データファイルメンテナンス誤り
システムファイルの障害
システムバージョンアップの誤り
オペレータのオペレーションミス
バージョンアップ指示書の誤り
ファイル装置の保守誤り
保守点検後の確認漏れ
保守マニュアルの誤り
保守者のチェック忘れ
保守点検時の規定外行動
構成機器が壊れる
機器保守の誤り
保守作業の誤り
保守マニュアルの誤り
保守作業上の指定外行動
操作を誤って装置を破壊した
装置の状態確認誤り


仕様書に従った作業を行わなかった
装置の操作手順ミス
不注意な行動による
装置に物又は人がぶつかって破壊
装置の配置が悪い
注意が散漫
機器に水又は異物をかける
規定外行動による不注意
運用規定の不備による誤り
ずさんな人災による（火災等）
火の不始末による火災
作業員が規定通りの作業を行わない
作業規準に規定が漏れていた
水の不始末による災害
水を使用する個所の点検漏れ
水を使用する個所の点検指定漏れ

（風調）


必要な電力が供給されなかった
コンピュータ用電力の供給がストップした
電源盤の操作を誤った
電源盤のスイッチをＯＦＦにした
工事上の作業に誤りがあった
工事中にケーブルを切断した
適切な室温（湿）が保たれなかった
空調設備が停止した
空調設備の操作を誤った
空調設備のスイッチをＯＦＦにした
ドアや窓等が開放状態のままになった
誤ってドアや窓等を閉め忘れた

(3) 今後の課題

ここでは，ヒューマンエラー分析を机上で実施してみたが，実際に運用されているシステムはもっと複雑であり，すでにある程度のセーフガードも施されていると思われる。しかしながら，ヒューマンエラーの発生しやすい個所はどこか，それを発見するためにはどうしたらよいのかについては，システムの大小にかかわらず共通点も多いと思われる。

従って，今後は，具体的なシステムに対して，事故や犯罪等とともに，エラーも1つのリスクの発生原因として加えて，リスク分析を実験してみる必要性がある。それというのも，既述のとおり，ヒューマンエラーは，システムの諸々の場面で発生し，システムを利用する組織体の損失発生にかかわるため，全体のリスク分析における損失頻度，強度の把握に関係づけ，セーフガード等の対応策の対費用効果分析に寄与すると考えられるからである。

第3章 リスク分析関連海外資料調査

リスク分析関連海外文献

はじめに

現代の情報化社会においては，組織はコンピュータ利用を前提として活動を行っている。しかもコンピュータはこれまでにない新しいリスクを生み出してきている。したがって，情報システムに由来するリスク処理のための出発点となるリスク分析に関する海外の動向を把握するため，米国商務省のNational Technical Information Service（NTIS）が作成しているＮＴＩＳデータベースおよびInstitute of Electrical Engineers（IEE）の情報部作成になるINSPEC（Information Services for Physics, Electronics, Computing）のデータベースから17編のリスク分析関係の論文および論説を入手した。特にそのうち５編を抄訳した。他の１２編の文献に関しては，巻末にそれらの概要を紹介しておいたが，ここで全体的な特徴を総括しておいた。

情報システム・リスクとリスク・マネジメント

企業は，経営上直面する情報システム関連のリスクに対応する必要があり，リスク予防・軽減の方法を勘案することがきわめて重要な課題となってきたのである。しかし，リスクを評価しないがため，多くの組織は十分なセキュリティを有しているとはいいがたい。この点に関しては，護るべき対象である資産にリスクをもたらす状況認識の不適切さに原因があるかもしれない。

例えば，タイプライターのリボンもかつては布製で何回も繰り返し使用したが，今日では一回使用したら使い捨てのカートリッジ・リボンを用いている。それに印字の跡が残されており，読み取ることが可能であり，競争相手より優位に立とうとした会社が掃除人にリボン収集を依頼し，そこから貴重な情報を入手したことも指摘されている。現在のテクノロジーは，リスクにかかわる事態を変化させてきたが，システムが複雑になったがため，多くの場合，専門的な知識のあるアタッカーにとり，犯行を行いやすく，また発見されにくくなっ

てきた。こうした従来と異なったリスク環境は，いわば「見えにくい脅威」を生み出してきているのである(6)。特にコンピュータ犯罪に関する統計からは，国によっても差異があるが，概して女性より男性が，また内部スタッフや部外者より，内部のマネジャークラスが高額な犯罪を犯す傾向もある（17)といわれている。

しかも，情報システムについては，それを利用する組織自体のみならず，社会的にも脆弱性が増してきており(5)，この点の認識も不可欠である。

それだけに情報システムにかかわるリスク処理のため，コンピュータ・セキュリティが重視されることになる。そこでは，コンピュータ・システム固有の脆弱性，脅威，リスク測定，保護手段が考察される(2)（10）。とりわけ脅威に関しては，組織にとり共通と思われる「物理的な脅威」に加えて，最も危険な脅威として「人」（インサイダーおよびアウトサイダー）への注視が肝要とされている(2)。

また，そうした脅威に基づくリスクへの対応に関し，コンピュータ・セキュリティを包含したリスク・マネジメントの導入が組織として求められることになろう。そのプロセスにおいて出発点となるのが，リスクの発見・確認，リスク測定であるが，リスクからの損失推定にあたり，リスク分析が重要である。最近では，コンピュータ支援のリスク分析の技法が展開されてきており（13）（14），組織のコンピュータ・リスク処理担当者には朗報といえるかもしれない。この点，定性的なリスク分析，定量的リスク分析がソフトとして入手可能である（16）。

リスク分析の結果により，リスクの処理方法が勘案されるが，コンピュータ・セキュリティは損失発生頻度・損失強度に対応する方法を中心に展開されている。たとえコンピュータ・セキュリティを適切に実施していたとしても，それにもかかわらず，損失は発生しうるものである。そのために存在するリスク処理方法が組織内でリスクを保有する方法（リスク保有）であり，第三者にリスクを移転する方法（リスク移転）である。後者の代表的方法は保険である。保険は，損失発生頻度が低いが，損失規模が大であるというリスクに対処する重要

な方法である。ちなみに，ＦＢＩの指摘では，コンピュータ関連犯罪の平均損失は＄５００,０００であり，コンピュータ支援の平均横領額は，＄４３０,０００であり，コンピュータがらみでない犯罪による損失を圧倒している(3)。それだけにコンピュータ保険については，先進諸国では価値ある方法とされている(7)。しかし，組織にとり，コンピュータ関連リスクに対する保険の購入は，専門的な知識を必要とする困難な課題の一つとされている(1)。また過去の損失経験に基づく現在の保険技術では，顧客の望む条件で保険を市場化することは困難である。したがって，保険の利用も，何でも保険しうるものではないという認識から出発すべきである(3)。それだけに，リスク保有の認識も今後重視する必要があろう。

こうした視点に加えて，コンピュータをめぐりさまざまな契約上の問題も発生してきており，リスク・マネジメントの観点から，コンピュータ関連の法律にも注視すべきである。それというのも，従来，目に見える商品なり，サービスをめぐって展開されてきている，いわば，１９世紀の経済環境に起源を有している契約原理に基づく財産権からリスクを考察するだけでは十分ではないからである（12）。

〔注記：上述の(　)内の数字は，巻末の参考文献の番号を表している。〕

「リヴァモア・リスク分析方法論」

Sergio B. Guarro, " LIVERMORE RISK ANALYSIS METHODOLOGY : A STRUCTURED DECISION ANALYTIC TOOL FOR INFORMATION SYSTEMS RISK MANAGEMENT ", submitted to society for Risk Analysis, Boston, Massachusetts, November 9-12, 1987 (UCRL-96032).

序

経済的・社会的活動のあらゆるセクターにおいて，過去２０年間に前例のない割合で情報システムの利用が拡大されていった。そうしたシステムを構成するコンピュータ，ネットワーク，さらに補助装置にたいして，我々が依存し，信頼を寄せることが増えるにつれて，脆弱性も増大しているのである。従って，システムについてのセキュリティを評価するツールとして，情報システム・リスク・アセスメントおよびリスク・アナリシス（分析）の方法が受け入れられ，適用されるようになっているのも判るであろう。これらツールを使用する主たる目標は，情報システムの保有者ならびにユーザーが影響を受けるリスクの性質および強度についての理解を広げるためである。

政府のセクターにおいて，最初にリスク分析の技法をコンピュータ・システムに適用しようと働き掛けたのは，連邦政府諸機関に関し，オフィス・オブ・マネジメント・アンド・バジェットにより１９７８年に設定された要請によるものであった。この要請は，最近，再認され，アップデートされたが，私的セクターでも，様々なレベルで，リスク・アセスメント関連のセキュリティ・アセスメント技法が実施されてきている。

リスク・アセスメントの方法は，性質なり深度の点で相違している。情報セキュリティの問題の評価にそうした方法を適用するには，特定の情報システムにおけるセキュリティ・コントロールのデザインおよび実施に関する実際上の質問に，正当化しうる文書で回答を提供する能力に基づいて決定されるべきで

ある。また，意志決定のツールおよびリスク・アセスメントのツールとして，リスク分析は特定のシステムにとり，受け入れがたい潜在的損失を確認できるばかりでなく，どのセキュリティ・コントロールおよび対応策が効果的で，コストの点で正当化しうるかを決定するのに用いられるのである。LRAM（Livermore Risk Analysis Methodology）は，バランスのとれた，包括的な方法で，これらの目的をカバーするために開発されたのであった。

リスク・マネジメント，リスク・アセスメントおよびリスク分析

リスクは，対象物（オブジェクト）本来の価値に，それに何等かの脅威が具体化したことによる効果が結合することから生じるものである。このことは，リスクにさらされている対象物の所有者にとり，通常は望ましくない，時には，極端なほど危険な価値の喪失の潜在性（value loss potential）に転換されることになる。リスクを考慮する際に適用されるシステムの複雑な性質ゆえに，リスクの全面的除去により，リスクの存在および発見に対応するなど，非現実的な事はない。通常，複雑なシステムは，発生するリスクの全面的除去には，無限大の資源配分を必要とする，潜在的脅威の広範・多様なスペクトラムにさらされているのである。よって，意志決定者およびシステム・マネジャーはリスクの除去というより，むしろリスク・マネジメントの面から考慮しなければならないのである。実際上，これは，以下のことをしなければならないことを意味しているのである：

a）システムがさらされている様々なタイプのリスクの性質と強度を理解する；

b）（リスク誘発損失（risk-induced losses）か，セキュリティ・コントロールおよびセーフガードへの配分のいずれかの形式で，費消される資源の大きさに照らして，システムが運用される環境において）どのレベルのリスクであれば容認しうると考えられるかを決定する；

c）対費用効果の点で適切なコントロールの選択，適用，実施により，容認しうるか，少なくとも正当化し得ると確認できるレベル以下に，現存するリスクを減少させる。

リスク・マネジメントは，管理上の責任に割り当てられているシステム内の貴重な情報資産を保護する必要のある意志決定者にとり最も広範な目的であると考えられよう。そこでリスクを管理するために，意志決定者は少なくとも一般的な意味で，彼のシステムのセキュリティの特徴を理解し，適用し得る専門的な調査方法を採用するアナリストから，この目的のため，適切なインプットを受け取らねばならない。これに属するのが「リスク・アセスメント」である。この用語は，今日ではシステムに潜在的に影響を与えている脅威の性質ならびに脅威から生ずる結果（consequence）の強度が調査され，評価されるところの分析活動を示すべく用いられている。これに密接に関係する用語である「リスク・アナリシス（分析）」は，より専門的なコンテクストにおいて用いられており，通常，リスクを，特定の構成要素，即ち，脅威，資産，損害ないし損失結果および対応策との間の関係に入念にメスをいれるため，スペシャリストにより採用されるより詳細な手続きを示している。

定性的・定量的分析のアプローチ

情報システム・リスク分析のフレームワークにおいて，一般に，リスクは（潜在的に有害な作用因および事象（イベント）という）脅威の（情報システムそれ自体の価値ある構成要素たる）資産へのインパクトにより生起されるものと認識されている。さらに，システムに脅威から資産を護る目的に適うようデザインされたセキュリティ手段集合を導入することが必要であると認識されているのである。そのような手段（measures and devices）は，コントロール，時にはセーフガードとして言及されている。

前述の概念なり定義についてコンセンサスがあるとしても，現実にどのよう

にして情報システムのリスク・アセスメントおよびリスク分析を行うかについては意見の相違がある。そうした議論の大部分は，リスク・アセスメントが定性的な技法に基づくべきか，定量的な技法に基づくべきか，また分析上どのレベルの精緻化（sophistication）で十分と考えられるか，に集中している。

この問題の決定には，リスク分析の主たる目的が，次の点にあることを思い出すべきである。すなわち，意志決定者が特定のシステムに影響を与えるリスクを効果的に管理できるようにインプットを提供することである。従って，システムの損害／サービスの中断をもたらす現存する潜在的ロス・イクスポジュアを確認・評価することは，情報システム・リスク分析の典型的な範囲内のことである。しかしながら，リスク・マネジメントの概念に従ってみると，主目的はこのステップの数歩先にある。事実，重大な潜在的危険（danger）を発見した後に，情報システムの管理者（administrator）は，通常，システムがおそらく被る損害の範囲を軽減する手段を追求する。予算という現実，それに管理上の制約に直面して，管理者はどのようにしてそうした損害の軽減が正当化でき，対費用効果の点で有効な（cost-effective）方法で達成し得るかに関心を持つことであろう。

今日，多数の情報システムはかなりの規模で，複雑なものとなっている。システムの複雑性の故に，こうしたシステムにとり有意味なセキュリティ分析は，構造化されていないアプローチによっては遂行され得ないのである。潜在的に被る損失の危険（stakes）が高い時はいつでも，より厳密でフォーマルな分析上のアプローチが推奨されるのである。この理論的根拠の認識は，合衆国のオフィス・オブ・マネジメント・アンド・バジェット（ＯＭＢ）のサーキュラー・レター（Ａ-１３０）において見いだすことができよう。そこでは，政府セクターのための「情報システム・リスク分析・ガイドライン」を設定している：

"……諸機関は，対費用効果の点で適切なセーフガードが現存しているものや新しい装置に組み込まれるのを確証するため，各装置について定期的にリスク分析を行うプログラムを樹立し，維持すべきである。リスク分析の目的は，

セキュリティ資源が，潜在的損失を最小にするため効果的に配分されうるよう，装置にたいしての相対的な脆弱性・脅威の尺度を提供することである。……”

情報システム・リスク分析は，定量的手段により遂行されるべきか，定性的手段により遂行されるべきか否かという議論が長きにわたり続いてきたが，それは関連ある，より重要な問題をしばしば不明確にさせている。例えば，もしも「脆弱性」の操作的な定義が何等与えられず，限定詞である「高い」の指摘も客観的に解釈されていないとすれば，システムの「脆弱性」は「高い」ということを，マネジャーに伝達しようとしてもほとんど役に立たない。

上の例に関して，リスク・アナリストが，特定のタイプの脅威により引き起こされ得る潜在的損失に関する情報を引き出そうと努力している状況を考慮してみよう。アドミニストレータＡは，年間＄１５０,０００の予算を取り仕切っており，その起こり得る損失を「高い」と評価している。ところが年間予算＄1,000,000 を管理しているアドミニストレータＢは，彼のシステムにおける潜在的損失を「中くらい（medium）」と評価している。これらの「高い」，「中くらい」という定性的な評価は，一貫していると期待し得るのであろうか？各々のアドミニストレータが，恐らく，日常業務環境下で処理し慣れていることからくるバイアスをもってアセスメントをするがため，一貫していることは期待しがたい。しかしながら，もしも，二人の評価者があらかじめ近似的に＄１００,０００以上に入る損失を「高い」，＄１０,０００から＄１００,０００の損失に「中くらい」，＄１０,０００以下の損失に「低い」という評価を用いるよう勧告されていたとすれば，何等かの一貫性が得られることになろう。

一段とフォーマルな分析のために，次に勘案されるのは，責任ある情報システム・マネジャーの目からみて重要な，対費用の点で効果的なセキュリティ手段の選択・実施に直接関係する便益（induced benefit）のタイプである。この便益は，徹底的に構造化された分析手続きのパフォーマンスが，アナリストにもたらす情報システムの機能および内部的な作用についての実質的な理解から生じてくる。私的セクターにある企業は，伝統的に財務的・金銭的な部面へ

の考慮には敏感であるが，この「システム・ナリッジ・ベネフィット（system knowledge benefit）」および組織の知覚の増加度を過小評価すべきではないのである。

定量的リスク分析の一般概念

定量的リスク分析は，情報システム・セキュリティの管理および評価のための体系的かつ実証可能な（documentable）アプローチを提供しうる。

情報システムの評価および評価リザルトのマネジャーへの効果的なコミュニケーション双方にとってのツールであるべく，定量的なリスク分析は，定義が客観的でコンテクストに左右されないモデルおよびパラメータに基づくべきである。

一般的なタームでは，定量的なリスク分析は，アナリストがシステム・セキュリティ・リスクの大きさを決定しうる，コントロール・オプションの有効性を評価しうる，システム・セキュリティへの支出を正当化・予算化しうるフレームワークを提供することが可能である。このことは，定量化しうる尺度でのリスクの推定を必要としている。通常採択されているのは，単位時間（unit time）あたりの望ましくない結果（consequence）（損失）の発生率であるが，その他の尺度も用いられる。望ましくない結果は，分析の範囲により定義されるが，情報システムでは概して，次のことを含んでいる： 直接的な金銭損失，システムないしファシリティのミッション遂行能力の喪失，重要情報のディスクロージャやディリーション（抹消）ないし変更，サービス拒否，そしてファシリティを動かしている組織へのその他の望ましくない影響，である。ハードウェア，ソフトウェア，情報および人員を含めたシステム資産に関して，諸結果が検討され，定量化されるのである。

結果の発生を確定するため，システム資産に直接不利益な影響をもたらすイニシエータが確認され，これらの結果を予防／軽減するコントロール手段の有効性が分析されねばならない。イニシエータおよび各々の資産へのそれらのパ

ス（経路）は，様々なシステムの脅威の性質を明らかにし，通常，それらの発生頻度に関する過去のデータ／主観的判断を用いて定量化されている。コントロール手段の分析は，コントロールの失敗確率の決定および付加的なコントロール手段ないし修正が対費用の点で効果的か否かの決定を伴うことになる。

情報システム・セキュリティ領域における定量的なリスク分析の利用にたいして言われている議論の一つは，特定のシナリオについての（例えば，一定の時間における発生確率といった）頻度および被害損失の大きさに関する信頼に足る「保険数理的な」データが，開発されたリスク・モデルに挿入するのに利用可能でないということである。そこでリスク・アナリスト達は，しばしばかれらの主観的な推定なり判断，もしくはその領域のエキスパートの意見を適用させることによって得られた数・値を用いねばならない。

可能であれば実際の観察データを用いるのが望ましいが，確率モデルの定量化にあたり主観的な推定を用いるのも，そうしたデータの払底ないし入手不能性に起因する関係事象なり現象についての知識の不確定な状態からの自然の成り行きである。また客観的な基礎に立ったモデルに入れるパラメータ値の主観的な推定は，定量的であれ，定性的であれ，決定を独断的な要因および主観的な決定スキームに基礎をおくことよりも選好されるのである。客観的な基礎に立ったモデルの使用は，獲得された最初のリザルトの確認のため，より正確で反復可能なデータの収集へと導くことになる。しかしながら，もしも，妥当なモデルが開発されないとすれば，リスク・シナリオに関する最初の不確実性は決して減少されないであろう。一般的な信念とは裏腹に，不確実な知識を反映している確率およびその他のパラメータの推定は，ハードな統計的データに基づいているわけではない。確率のアセスメントは，特定の事象が起こるという「確信度（degree of belief）」を反映するものである。この確信度は，当初から，実際の統計的な証拠により支持されるかもしれないし，されないかもしれないのである。

リヴァモア・リスク分析方法論

リヴァモア・リスク分析方法論（ＬＲＡＭ）は，1985年の始め，ローレンス・リヴァモア国立研究所（Lowrence Livermore National Laboratory＝ＬＬＮＬ）が，合衆国空軍ロジスティックス・コマンド（ＡＦＬＣ）により開発を委託され，同年末までに，基本的な方針を完成させたものである。

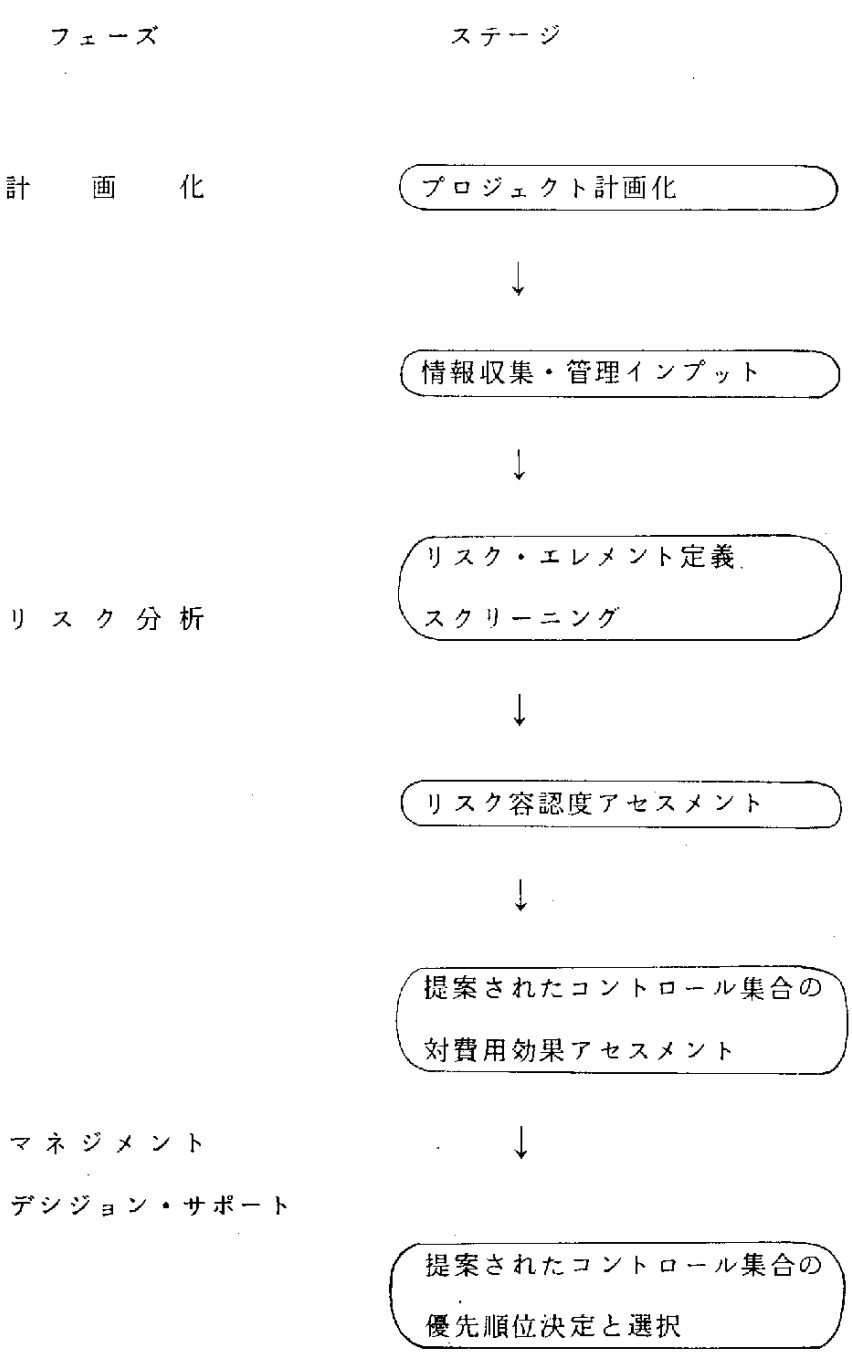
大規模な統合情報システムのセキュリティ・デザインおよび管理のための包括的な意思決定とリスク・マネジメントのツールとして役立つように意図されていたが，ＬＲＡＭは本質的に弾力的にデザインされた。それゆえ，ＬＲＡＭの適用も，分析されるシステムの規模および複雑性に，またアウトプット・リザルトが望まれる詳細さや解答の水準に合わせることが可能である。

フローチャートにおける図１は，ＬＲＡＭアプローチの手続き上のシーケンス（順序）を示している。ＬＲＡＭの主たるフェーズは，図１における「計画化」，「リスク分析」，「マネジメント・デシジョン・サポート」として示されている。これら３つのフェーズは，６つのステージからなっている：
1）プロジェクト計画化（ＰＰ），2）情報収集（ＩＧ），3）リスク・エレメントの定義およびスクリーニング（ＲＥＤＳ），4）リスク容認度アセスメント（ＲＡＡ），5）提案されたコントロール集合の対費用効果アセスメント（ＣＢＡ），6）提案されたコントロール集合の優先順位決定と選択（ＰＳ）である。

ＬＲＡＭのプロジェクト計画化のステージは，その他の計画化活動とさほど相違しない。それゆえ，このステージについての論議は省略する。

現実のＬＲＡＭの分析活動は「情報収集」のステージから始まる。このステージでのアナリストの主たる目的は，情報システムを構成する（ハードウェア，ソフトウェア，データという）資産のインベントリーを作り，それらの貨幣値（例えば，再調達コスト）およびクリティカリティ，分類，センシティヴィティ等のレベルといった非貨幣的な値の属性双方に関する予備的な決定をす

図1　ＬＲＡＭプロセス・ダイアグラム



ることである。その他の重要な情報収集活動は，資産損失結果および資産への潜在的脅威のリスト作成・範疇化を含む。

「リスク・エレメントの定義およびスクリーニング」（REDS）のステージにおいて，ＬＲＡＭリスク・エレメントと呼ばれる個々のリスク・シナリオが十分に確認され，それらの潜在的強度について評価される。まずは，どのジェネリックなタイプの結果が資産の損失から生じ，どのジェネリックな脅威のタイプおよび脅威ー資産のパスが個々の資産に適用しうるかを決定することによって，「ジェネリック（generic）なリスク・エレメント」（GREs）が，ＲＥＤＳにおいて確認されねばならない。ジェネリックなリスク・エレメントは，構造上の構成要素と属性を定義することにより確認され，特徴づけられる。リスク・エレメントの構成要素とは，資産（同じ脅威エージェントにより，ひとつ以上の資産が影響を受ける場合には，複数の資産），脅威，脅威ー資産のパス，脅威事象の（直接的・間接的）結果である。ＧＲＥの例は次のとおりである：

○　直接的な貨幣的損失およびサービス中断〔ジェネリックな結果〕を引き起こす，メインフレーム・コンピュータ〔資産〕への直接的な物理的アタック〔ジェネリックな脅威ー資産パス〕による人間の意図的脅威〔ジェネリックな脅威〕。

GREsは，同一のジェネリックな描写に合致する多くの「特定のリスク・エレメント」（SREs）を含む範疇を構成している。上述のＧＲＥの範疇に対応するＳＲＥの例は，次のとおりである。

○　メインフレーム〔資産〕の電流回路に，サボタージュする人〔特定の脅威〕が水をかけ〔特定の脅威ー資産パス〕，ショート〔特定の直接的結果〕を引き起こす：　ユニットが２週間前に修理されず，重要なアプリケーションが他の処理ユニットに移転されねばならず，かなりのサービスの遅延〔特定の間接的結果〕を引き起こす。

明らかに，このＳＲＥの例は，特定のＧＲＥのタイプ内において確認されるものではない。アナリストは満足のいくまで，同じジェネリックなリスク・エレメントにふさわしい他のシナリオを開発しなければならない。

リスク分析についてのアセスメントおよび評価部分は，ＧＲＥとＳＲＥの定義づけ活動が終了した後，各々のＳＲＥに対して，最大可能損失（maximum possible loss＝ＭＰＬ）を割りあてることにより開始される。分析の様々なポイントにおいて，有体物でない資産を含むか，または損失結果が甚大でないようなリスク・エレメントは，以後の分析から除かれる。このことは，分析上の努力を管理可能な水準に保ち，アナリストの注意を最大の損失をもたらしうる寄与因に向けさせるのである。

「リスク容認度アセスメント」（ＲＡＡ）のステージにおいて，セキュリティ・コントロール手段が確認され，適用可能なリスク・エレメントに関連づけられる。セキュリティ・コントロールは，脅威によりチャレンジされている際の支障（failing）確率が非常に小さい場合，最も効果的である：したがって，「ロス・ポテンシャル・インディケータ」（ＬＰＩ）値を推定するため，コントロール支障確率が考慮される。すでにシステム内に存在しているコントロール手段の有効性は，あらかじめ決められた「リスク容認度閾（threshold）」と，一定のＳＲＥに関し得られるロス・ポテンシャル・インディケータ」（ＬＰＩ）値とを比較して評価されるのである。選ばれる閾値は，ひとつの特定種類の脅威について容認しうると考えられる損失水準に関しての（リスク分析を遂行する組織における）マネジメントの見解を反映するようにする。もしも，リスク・エレメントがこのリスク容認度テストを満たさない場合，容認可能とさせる付加的なセキュリティ・コントロールを確認することが分析内で保持される。そして提案された付加的なコントロール手段は，ＲＡＡステージにおいて，現存するコントロール手段の評価のために用いられるのと同一の基準を適用することにより評価されるのである。

要するに，ＲＡＡステージは，当初，容認不能であったＳＲＥｓの確認と，適用される場合に容認可能となる「提案されたコントロール」との確認で，ＬＲＡＭの「リスク分析」のフェーズが終わることになる。容認可能なＳＲＥｓとは，特定の脅威の実現化にあたり，ロス・ポテンシャルがマネジメントの定義した容認度の閾を越えないというリスク・シナリオなのである。

次にくる「マネジメント・デシジョン・サポート」のフェーズでは，分析の焦点は，「リスク容認度」から「対費用効果アセスメント」および「提案されたコントロール手段の優先順位決定と選択」に移ることになる。

「対費用効果アセスメント」（ＣＢＡ）のステージは，年間の便益と費用の比較を通して，各々の提案されたコントロールに関する「対費用効果比率」の評価を巡って行われる。「優先順位決定と選択」（ＰＳ）のステージは，年間予算配分のサイクルおよび制約要因に鑑みて，提案されたコントロール手段の選択・実施に順位をつける問題にあてられる。全体の優先順位決定のスキームが最終的に開発され，個々の指標にウェートを割り当て，すべての提案されたコントロール手段についての最後の相対的な選好順位を決定するひとつの指標にそれらを結合させ，使用されるのである。

ＬＲＡＭモデルと基礎的な手続きについての論議

前のセクションにおいて示されたように，脅威のイニシエータ，プロパゲーション・パス（伝搬経路），被害資産，起りうる結果，適用可能なコントロール手段といったものの結合が，ＬＲＡＭにおいて「リスク・エレメント」（ＲＥ）として定義されている。すべての信頼に足りうるリスク・エレメントの完全なリストは，分析されるファシリティ，システム，ないしサブシステムに対するリスクの全体の「スペクトラム」を描くことになる。全体のリスクを完全に描写したり，特徴づけるなど必要でないし，実際的でもないがため，ＬＲＡＭのアプローチでは，全体のリスク尺度を得ようとするのではなく，むしろ

単独の事象の損失発生を含む個々のリスク・エレメントにより生み出されるリスクに焦点を当てている。

ＬＲＡＭにおいて採用されているような包括的かつ構造化されたリスク・モデルの構成・利用は，モデル定義およびモデル評価という２つの補足的な活動の遂行を必要としている。

図２が示しているのは，記述的・定量的な表現でのＬＲＡＭリスク・モデルの本質的な構成要素である。記述的部分は，脅威イニシエータ（例えば，サボタージュする人といったアタッカーや，地震といった自然作用因），潜在的なターゲットとなる資産（例えば，コンピュータやコミュニケーション・ハードウェア，ソフトウェア，データ），脅威作用因が資産に達した場合に生じ得る

図２　基本的ＬＲＡＭリスク・モデル

コントロール手段

脅威　→　予防措置　→　資産　→　軽減措置　→　結果

$$R = EF \times PCF \times MPL$$

結果（例えば，ハードウェアの破壊，情報の漏洩，機能喪失等）の間の論理的連関である。これら論理的連関は，ＬＲＡＭにおいて，脅威から，資産へ，そして結果への「プロパゲーション・パス（伝搬経路）」として言及されている。現存するセキュリティ・コントロール（時にはセキュリティ・アナリストにより「セーフガード」として言及されている）は，このパスにおける脅威イニシエータの進行を抑止・対比するものと仮定されている：　「予防的コントロール手段」は脅威から資産へのパス上に置かれており，脅威作用因が資産に著しい影響を与えるのを予防する機能を有している：　他方，「軽減的コントロール手段」は，資産から結果へのパスにそって位置づけられており，予防的コン

トロール手段が脅威の資産への作用を抑止しそこなう場合に，損失を制限・最小化する目的を有している。

定量化モデルは，図２の下の部分に示された公式を用いて測定されるが，繰り返せば，次のとおりである：

$$R(RE_i) = MPL(C_i) \times PCF(PMCO_i) \times EF(T_i)$$

この式が指摘しているのは，ｉ番目のリスク・エレメント（ＲＥｉ）から生じるリスク（Ｒ）の年尺度（annualized measure）が，以下の積として得られる，ということである。すなわち，資産への脅威が軽減されない場合の結果（Ｃｉ）から生じると推定される「最大の潜在的損失」（ＭＰＬ）と，予防的・軽減的コントロール手段（ＰＭＣＯｉ）の結合集合のコントロール支障確率と，脅威（Ｔｉ）の「予想頻度」（ＥＦ）（最後の量はしばしば「年あたり確率」として示される）との積である。

リスク・エレメントの定義は，ＬＲＡＭにおいて，機能的に認知可能なエンティティとして定義しうるシステム資産の確認，これらの資産が破壊された場合に起こりうる最悪の結果の定義で始まる。そこで資産は，貨幣値（monetary value）のみ有する資産と，クリティカルな，センシティヴな，または機密とされる資産とに分類される。直接的に貨幣的値のみ有する資産は，仮に有形性のレベルでスクリーンにかけられる。価値が有形性のレベルを越える貨幣的資産は，分析に保留される。そうした予備的な資産のスクリーニングのプロセスと平行して，結果のタイプがそれらの重要性に関してふるいに掛けられる。当該ファシリティないしシステムを動かしている組織にとり重要と考えられない結果は，その後の考慮から除去される。

分析に残る資産および結果については，起こりうる脅威とそれらのパスが，リスク・エレメントを設定するために確認される。リスク・エレメント評価の最初のフォームがこのステージで行われ，次のことが仮定される。すなわち，脅威が発生したこと，そして，１から６までの範囲の強度クラス値でリスク・

エレメントに関する「最大潜在的損失」（ＭＰＬ）を推定するため，何等コントロール手段が現存していない，ということである。したがって，リスク・エレメントは，それらのＭＰＬ値が評価される情報システムを動かしている組織のマネジメントにより設定された閾以下であるか否か，審査されるのである。

そして残っているリスク・エレメントの各々について，適用可能な現行のコントロール手段が確認され，それらの支障確率が推定されるのである。そこで，ＭＰＬは，各リスク・エレメントについてロス・ポテンシャル・インディケータ（ＬＰＩ）を設定するため，コントロール支障確率（ＰＣＦ）と結合される。このパラメータは，次式で示されるが，強度クラスのフォームで得られる：

ＬＰＩ（ＲＥｉ）＝ＭＰＬ（Ｃｉ）×ＰＣＦ（ＰＭＣＯｉ）

（閾に等しいか，それ以上のＬＰＩをもつ）容認しがたいリスク・エレメントは，新しいコントロール手段かコントロール手段の向上が提案され，新ＬＰＩ値が決定されるのを必要とする。グレードの上がったＲＥ各々について，新ＬＰＩは，初めのＬＰＩと同様のスクリーンに掛けられる。もしも，それが容認しうると判れば，新しく提案されたコントロール手段を有するリスク・エレメントが，対費用効果分析（ＣＢＡ）のステージに回される。さもなくば，そのリスク・エレメントに関して容認可能なＬＰＩ値をもたらす新しいコントロール手段ないしコントロール手段のグレードアップが確認されるまで，反復的な手続きが必要となるか，当該目的の点で，何等コントロール手段が現状として確認されえないことが決定される。

「リスク容認度テスト」に合格した新しいコントロール手段は，次に対費用効果の点で，ＣＢＡステージにおいて評価されることになる。この分析が必要としているのは，現状のコントロール手段のコスト以上になる新しいコントロール手段ないしグレードアップしたコントロール手段実施の増加コストの推定，および，新しいコントロール手段ないしグレードアップしたコントロール手段の適用により，当初容認しがたかったリスク・エレメントすべてについてのリスクの減少の推定である。対費用効果比率（ＣＢＲ）は，リスクの減少を，新

規かグレードアップしたコントロール手段の増加コストで割ることによって把握される。そして，この比率は，新規かグレードアップしたコントロール手段が容認されうるか否かを決定するために，閾値に対して比較されるのである。1に等しいかそれより大である値が，このＣＢＲ閾に関し通常選ばれ，1は「ブレークイーブン」ポイントで，特定のコントロールの向上が装置ないしオペレーションに支出される1ドルにつき，リスクについて等価ドルの価値を節約すると期待されていることを示している。考慮されているコントロール手段が選択される対費用効果閾基準に合致しない場合，異なった新しいコントロール手段が提案され，ＬＰＩ容認度と対費用効果分析のプロセスがグレードのあがったコントロール手段のより良い集合ないし配列を確認するため繰り返されるのである。

グレードのあがったコントロール手段の特定集合に関するＣＢＡ値の計算は，リスク減少値の計算を必要とすることに留意すべきである。提案されたコントロール集合各々についてのリスクの減少（ＤＲ）は，ベースラインＲ値とグレードの上がった配列（configurations）について適用可能なＲ値との差である。数式で示せば，次のとおりである：

$$DR(REi;PCj) = R(REi;PCj) - R(REi;CC)$$

ここで，表記された"ＲＥｉ；ＰＣｊ"は，ｊ番目の提案されたコントロール手段を伴うｉ番目のリスク・エレメントを表し，"ＲＥｉ；ＣＣ"は，現状のコントロール手段のセットを伴うｉ番目のリスク・エレメントを意味している。したがって，ｊ番目の提案されたコントロール・セットに関するＣＢＲ値は，上述の定義にしたがって，次のように計算される：

$$CBR(PCj) = \frac{\text{全てのiの合計}〔DR(REi;PCj)〕}{\dfrac{\text{当初のコスト}(PCj)}{\text{予想寿命}(PCj)} + \text{年間コスト}(PCj)}$$

容認可能なＣＢＲを持つ新規かグレードの上がったコントロール手段は，設置にあたり優先順位を決定し，選択され，予算化されることになる。優先順位の決定プロセスは，最も良くセキュリティを遂行する新規かグレードの上がったコントロール手段を選択・予算化するために，ファシリティを動かしている組織により選ばれたいくつかの指標を考慮することになる。そうした指標は，終極的に，提案されたコントロール手段の選好実施順序を設定するために用いられる「全体的優先順位決定指標（global prioritization index）」（ＧＰＩ）をもたらすように，ウエートづけられた積により結合される。現在利用可能な予算の積み立て水準の範囲内で，実際設置されうる優先順位リストにおける最初のＮ案コントロール手段が，すぐに実行されるべく選択される。低い適用順にあるコントロール手段は，資金積み立てが利用可能となるか，リスク分析の結果に基づき交渉されうるまで，遅らされることになる。

リスク・エレメント審査基準

ＬＲＡＭモデルの定義および評価プロセスと混成されたスクリーニング手続きは，本質的に３つの独特な種類の基準に基づいている。これらは，実際に審査に用いられる評価尺度の３つのタイプに対応している：　(1)損失の値と結果の重要性，(2)ロス・ポテンシャル・インディケータ値，そして(3)対費用効果比率，である。

最初のタイプの審査は，ＲＥＤｓステージでなされ，まず予備的に，貨幣値と結果の「重要性」に関して行われ，その後再度ステージの終わりに，リスク・エレメントの資産と結果の構成要素がより公式的に定義され，ＭＰＬ（最大潜在的損失）値がそれに応じて評価される。こうした審査の目的は，単独で著しい強度の損失発生を引き起こすことのないリスク・エレメントを分析から除去し，リスク・アナリストの注意を分析当初から，著しい強度の損失を引き起こしうるリスク・エレメントに集中させることである。

ロス・ポテンシャル・インディケータ（ＬＰＩ）は，リスク・エレメントに

ついての「リスク容認度」の評価のためのパラメータとして用いられる，換言すれば，特定のリスク・エレメントに対して適用される現行のコントロール手段のセットが十分か否か，グレードアップされねばならないか否か，を決定するために用いられる。

リスク容認度審査をＬＰＩに基づかせる第２の理由は，この選択がアナリストに，ほとんど起こらないが，潜在的に非常に激しい損失結果を伴うリスク・シナリオを保守的に（例えば，リスク回避的に）処理させるようにすることである。

準定量的・非貨幣的推定

ＬＲＡＭのリスク分析のフェーズ終了までに，規模順（order of magnitude）タイプの推定を行うことが必要である。リスク評価手続きは，定量的，より正確な定義を用いれば，「準定量的」に遂行されることになる。「正確な」値よりむしろ，不連続なレンジの値に相応する結果の「強度クラス」が用いられる。損失の値を貨幣値で直接表しがたいシステム資産に関しては，特別の言葉で表した非貨幣的結果の強度クラスが用いられる。これらの「非貨幣的強度クラス」は，ドル推定に服しやすい結果について用いられる不連続なドル・レンジに平行するレンジを有し，したがって，アナリストがあらゆるタイプの結果を同じ測定スケール（例えば，クラス１からクラス６までといった「強度クラス」の不連続なランク付け）に転換するのを許すことになる。これは，ＬＲＡＭの分析過程への他の重要なインプットのように，意志決定プロセスの一貫性およびドキュメンタビリティを確保するため，組織において責任あるマネジャーにより定義されねばならない貨幣的と非貨幣的結果との間の等価基準を満たすことによりなされるのである。

次の「マネジメント・デシジョン・サポート」フェーズにおいて，高度の問題解決が必要とされるので，リスク推定のための準定量的な「強度クラス」アプローチが，脅威頻度およびより正確なコントロール支障確率値の明示的な推

定と並んで，「等価のドル」での結果の評価をもたらす定量的なポイント・推定・ベースの手続きに置き換えられる。これまでに出されてきた多くのデータが再利用され，容認不能とされるリスク・エレメント数が初めの包括的なリスク・エレメント・リスクの部分にすぎないため，分析のこの段階では，完全な定量化はさほど負担にはならない。

最終的なコメントと結論

本論文の始めに，定量的なリスク分析が，中規模から大規模な情報システムのセキュリティに関連する意志決定過程におけるマネジメント・ツールとして非常に満足のいくかたちで用いられていることを論じておいた。この目的の達成のための分析手段および手続きは，今日，知識のある情報セキュリティ・アナリスト達にとり，多大なリスク・ポテンシャルが存在する問題領域の確認のみならず，予算化および優先順位決定に鑑みて，回復策やそれら回復策のための実行戦略の確認にとっても利用可能である。

ＬＲＡＭは，そうした完全なマネジメント・ツールを提供する意図を持って開発されたのであった。その完全な手続きは，リスク・アセスメントになじみのない人には複雑に思われるが，ＬＲＡＭは，個々のリスク・シナリオのリスクの関与の仕方に直接的・客観的に関係し，例証するパラメータに基づいた直感的で単純なリスク・モデルを用いている。リスク・モデルの定義および評価において，セキュリティ・コントロールの有効性に関係するモデル部分が，明らかに確認される。このことは，情報システムのデザイナーないしアナリストが，リスクの最終的な大きさを決定する要因間で影響を与えるひとつの要因に，直接，分析的にアクセスするのが可能となるのである。

ベイジアン確率リスク分析

Ali Mosleh, E. Richard Hilton, and Peter S. Browne " Bayesian probabilistic risk analysis "

ACM SIGMETRICS--Performance Evaluation Review, v.13, no.1, June 1985.

1. はじめに

現代ビジネスや金融業では，管理手段としてますます大規模なコンピュータが使われるようになってきている。しかし，リスクの量やその招きうる危険も比例して増大している。加えて，多重処理，資源の共有，分散処理を有する大規模システムでは，規模の大きさゆえのシステムの脆弱性（Vulnerability），資源の悪用の可能性といった，新しい世代のリスクが増大してきている。こうした大規模システムの故意のあるいは偶発的な損傷は，ビジネスに深刻な結果をもたらす。したがって，リスクはなんとかして管理しなければならない。そのためには，脅威（Threat）を見定め，脅威の発生およびそれぞれの脅威に対するシステムの脆弱性の要素について見込みを立てなければならない。リスク・マネジメント・プログラムは，システムの弱点を見定めランクづけするために脆弱性を比較し，システムが損傷を受ける可能性を安価にかつシステマティックに減らすための，リスク分析に始まる。

本論文では，大規模コンピュータ・システムに関連したリスク評価のためのベイジアン確率法の一つを与え，実際に施行したこの方法より得られた結果を例として示す。次章では，リスク分析について一般的な議論をし，現行のリスク評価法について簡単にレビューを行う。次に，本論文のベイジアン法を数式を用いて説明する。最後に，本方法の実施例を簡単に示す。

2. リスク分析

自動環境におけるリスクについて理解するために，システムの基本要素間の相互関係が，これら各要素の脆弱性および各要素に対する脅威とともに，最初に示される。資源共有についての脆弱性は，一般に5つに分けられる。すなわち，物理的な周囲環境，ハードウェア，システム・ソフトウェア，通信回線，システムを使用する組織の人員や運営形態である。システムへの脅威はこれらの脆弱性の領域（いわゆるイクスポジュア）の1つ以上に働く。リスクの大きさは，実際の経験と予想された経験との起こりうる変動（いい換えれば，どれだけしばしば種々の脅威が種々の脆弱性へのインパクトを有するか）によって測られる。確率論的な定量的なリスクの基準を用いれば，異なったアクションのもたらす異なった結果の予測を表明するリスクモデルが得られる。しかし，リスクの評価それ自体ではデシジョン・メーキングのツールとしては不十分である。必要なのは，リスクを定量的に分析し，かつシステムに悪影響を与えるさまざまな脅威を減らすのに要するコストと予測される損失を比較するための手段である。

リスク評価は基本的に以下の2つの理由のために行われる。まず，有害な事象が起こる確率を小さくするために，あるいは続いて起こる事態を軽減するために（あるいは，所定のリスク許容値に照らしあわせてみて事象の発生の確率は無視できる，ということをいうためにも），コンピュータとそのシステム・・アーキテクチャについての十分な情報が必要だということ。2つ目は，選択的なリスク・マネジメント戦略の比較評価のために，統計的な情報が必要だということである。

2.1 リスク評価法

リスク分析を行う最終的な理由は，決定しなくてはならないデシジョン（あるいは一連のデシジョン）があるということである。理想的には，それぞれの

アクションの選択は，コストと便益の比較の上に行われるべきである。

現行のリスク評価法は，大きく２つのカテゴリーに分けられる。定性的なものと確率論的なものとである。定性的な方法（BRAF81）では，まずシステムに対するあらゆる脅威を見定め，次にどのシステム資源を使うかを決定する。脅威と脆弱性は定性的な方法で比較され，脅威はその深刻さの度合いを数学的に評価されることはない。そのうえ，種々の脆弱性を直すのに要するコストについては何の評価法も示されていない。定性的なアプローチは，典型的な脅威／脆弱性の関係についての指針を提供する。しかし，それは臨界値についての主観的な情報にすぎず，安全性についての定量的な値を何も与えない。したがって，リスク・マネジメントの目的によりかなうためには，さらに効果的なリスク分析がなされなければならない。

確率論的な方法は，脅威の深刻さの度合いの尺度や，各デシジョン・モデルに対して必要な定量的な入力を与える。しかし，不確かさを測る方法が，定量的なリスク分析の正しさ，適切さ，正確さを決定する。残念ながら，多くの確率論的な方法は点評価（いい換えると，好ましくない事象の度数を与えるのに，概算した度数の中で変化する確からしさを求めるために確率的な範囲を計算するのではなく，ある固定の定数を使っている。COUR77，LABE80）。定量的なデータの点評価のみによる方法は，リスク・モデルへの基本入力におけるバリエーションを実現するには敏感すぎる。リスクのレベルを計算する段階でエラーが起きる。というのは，固定度数あるいは強度選択度数（高，中，低）は，システムへの種々の脅威の生起率をカバーするように設定してあるからだ。また，損失見積りの式は，修復費用が特定の金額になることを要求するからだ。不幸にも，脅威の度数は非常に大きく変化する。しばしば，復旧の費用を前もって正確に予測することは困難だ。

対照的に，本論文の確率論的リスク評価法はベイジアン統計論によっており，

ある範囲内の安全性と復旧費用を取り扱うことができる。その数式はシステム内での特定の期間の特定の脆弱性に対する複数の脅威を考慮することができる（点評価法による方法では，一度に1個の脅威／脆弱性のペアしか扱えない）。選択された安全性のレベルに応じて，本方法は管理者にデシジョン・メーキングのツールを提供する。よく知られた「リスク・カーブ」としてあるいは表としてコスト便益オプションの範囲を表示する。そのため，その真価はリスクの管理と制御のためのデシジョン・メーキング・エリアにそれを持ち込むことにある。コスト，便益，リスクのバリエーションの定量化およびそのオプションはデシジョン・メーキングをより確固たるものにする。

3. ベイジアン確率リスク評価

ベイジアン・リスク評価法は，当初原子力産業のために開発された（KAPL et al.）。そこでは，脅威のもたらす結果は破壊的なものであり，そのためリスク評価法は数学的に疑いの余地のない正しさが要求される。この評価法は，金融リスクへのシステマティックな定量的アプローチとしても有効である。リスクの定量的な理解のために，次の4つの基本質問に答えればいい。

1) 何が問題なのか。
2) どれぐらいの頻度で，それは起こると予想されるのか。
3) その結果はどうなるのか。
4) 最初の3つの質問の答えはどれぐらい確かなのか。

大規模なビジネスや金融企業のコンピュータ・システムは多くの脅威にさらされている。最初の質問に答えるために，多くの潜在的な脅威が列挙された。例えば，不正，悪質な破壊行為，火事，地震，コンポーネントの故障によるシステムの停止などである。これらの脅威がある特定の機構に実際に襲いかかるかどうかはわからないが，歴史的な実例や産業界の経験によればどの脅威も現

実のものであり，どのようなコンピュータ・システムにも起こりうるものなのだ。この実例は，これらの脅威の度数とそれによる損失の程度を見積るのに使用できる（PICK82）。

十分に広範囲にわたる歴史的なデータがないとか，時とともに多くの問題のパラメータが失われているなど多くの理由があって，脅威の度数と損失の程度をトータルに正確に見積ることは必ずしも可能でない（実際，これらの量の実際の大きさを取り扱う時には，いつもある程度の不確実さがつきまとう）。先に指摘したように，現行のリスク評価法の多くはリスク分析の各段階における不確実さを無視しているにもかかわらず，不確実さはリスクの一要素であり正しい定量化においては無視してはならない要素であることは明白だ。それゆえ，確実さに関する質問，質問4が用意されている。不確実さを考慮に入れるために，ベイジアン評価法は特定の望ましくない事象の度数と結果を見積るのに，「広がり」という統計的な手法を用いている。数学的モデルについては，次章にゆずる。

3.1 数学的モデル

考察中のシステムがN個の潜在的な脅威にさらされているとしよう。タイプiの脅威の（年間）生起率をλ_iとする。さらに，脅威の生起はポアソン・プロセス(注1)によるものとする。期間tのうちにタイプiの脅威がKi回起こる確率は（CINL75），

$$P(Ki \mid \lambda i) = \frac{1}{ki!}(\lambda_i t)^{ki} e^{-\lambda_i t} \quad ki = 0, 1, \cdots\cdots^{\infty} \quad (1)$$

（注1） ポアソン・プロセスにおいては，考察中の事象の生起率は終始一定であるとみなされる。ポアソン分布とは，ある与えられた期間内に事象の生起する数の確率を表す数学的モデルである。

もしもλの値が正確にわかっていれば，式(1)はkの確率を与える。しかし，前もって指摘しておいたように，実際には私たちはそれぞれの脅威の生起率を高い精度で知っているわけではない。λの値の不確実性を確率分布を用いて表すことにする。数学的な簡便さと，それが0と∞の間にあるという理由から，次式に示すガンマ分布の一種を使うことにする（CINL75）。

$$f(\lambda) = \frac{\beta^{a}}{\Gamma(a)} \lambda^{a-1} e^{-\beta\lambda}, \quad \lambda \geqq 0 \qquad (2)$$

ここで，$\alpha \geqq 0$，$\beta \geqq 0$は分布の2つのパラメータである。典型的なガンマ分布を図1に示す。

タイプiの脅威がki回起こる（絶対）確率は，

$$P(ki) = \int_{0}^{\infty} P(ki \mid \lambda i)\, f(\lambda i)\, d\lambda i \qquad (3)$$

式(3)に式(1)(2)を用いて，

$$Pt(ki) = \frac{(ki + \alpha i - 1)!}{ki!\,(\alpha i - 1)!} \left(\frac{t}{t + \beta i}\right)^{ki} \left(\frac{\beta i}{t + \beta i}\right)^{ai} \qquad (4)$$

それぞれの脅威の生起について，C_j^i（タイプiの脅威のj番目の生起）の潜在的な損失があるものとしよう。損失費用のトータルは，

$$Ci = \sum_{j=1}^{ki} C_j^i \qquad (5)$$

C_j^iの値の不確実さのモデルとして，正規分布を選ぶことにする。すなわち，損失の確率は次の式によって与えられる（WINK75）。

$$f\left(C_j^i\right) = \frac{1}{\sqrt{2\pi}\ \sigma i} \exp\left\{-\frac{1}{2}\left(\frac{C_j^i - C_o^i}{\sigma i}\right)\right\} \quad (6)$$

典型的な正規分布曲線を図2に示す。また，C_o^i は損害の平均値，σi は標準偏差である。

C^i は正規分布をなしたランダム変数 $k i$ の合計であるから，C^i の分布も正規分布となる（WINK75）。

$$f\left(C^i\right) = \frac{1}{\sqrt{2\pi}\ \hat{\sigma} i} \exp\left\{-\frac{1}{2}\left(\frac{C^i - \hat{C}^i}{\hat{\sigma} i}\right)^2\right\} \quad (7)$$

ここで，

$$\hat{C}^i = k i \cdot C_o^i \quad (8)$$

$$\hat{\sigma}_i^2 = k_i \cdot \sigma_i^2 \quad (9)$$

C^i （タイプ i の脅威による損害額の合計）の分布は生起の回数（$k i$）に依存するので，無条件確率を求めるためには，

$$P_t\left(C^i\right) = \sum_{k i = 0}^{\infty} f\left(C^i\right) P_t\left(k_i\right) \quad (10)$$

を求める必要がある。この分布は解析的には求まらない。計算は数値解析によらねばならない。

C^i の累積分布は次式で与えられる。

$$P_t\left(C^i\right) = \sum_{k_i = 0}^{\infty} \phi\left(C^i\right) P_t\left(k_i\right) \quad (11)$$

ここで,

$$\phi(C^i) = \int_0^{C^i} f(C^{i'})\, dC^{i'} \qquad (12)$$

$\phi(C^i)$ の値については表がある（WINK75）。

したがって，タイプiの脅威のリスク曲線は，以下のようになる。

$$R_t(C^i) = \text{Prob.}(\text{Loss} \geqq C^i) = 1 - P_t(C^i) \qquad (13)$$

図1　脅威タイプiの年間度数のガンマ分布

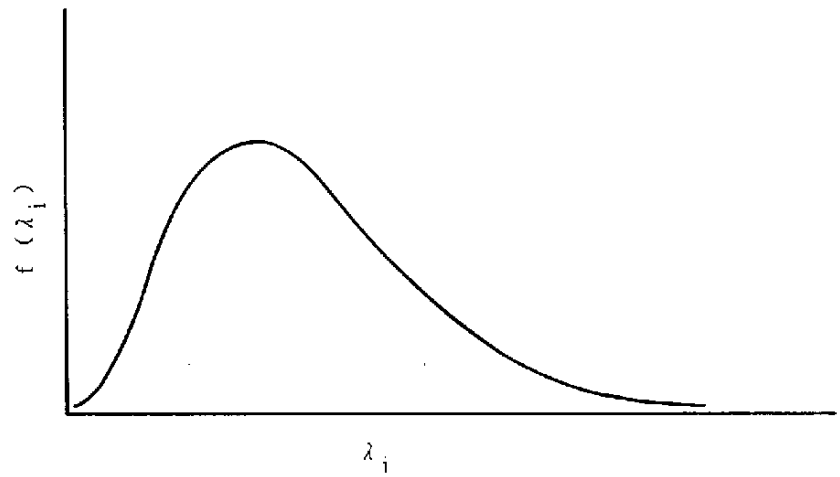


図2　タイプiの単一のイクスポジュアについての損失の分布

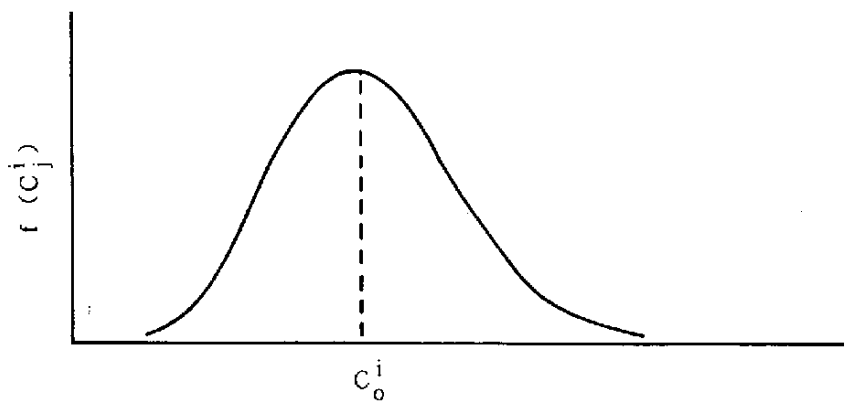
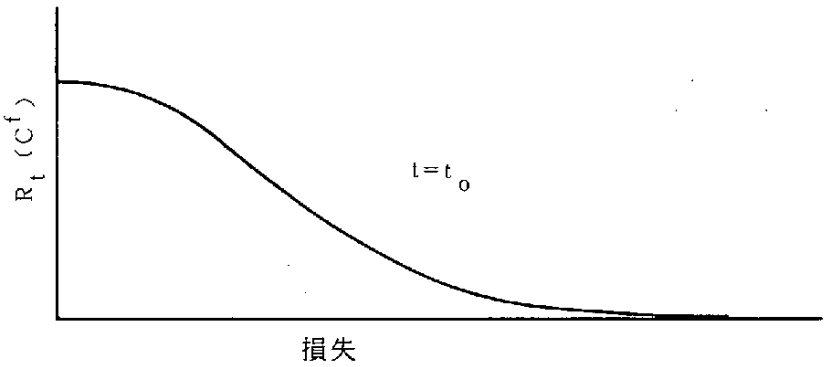


図3　典型的なリスク曲線



すべてのタイプの脅威によるリスクを求めるために，次のランダム変数の分布を求めなければならない。

$$C = \sum_{i=1}^{N} C^i \qquad (14)$$

計算上の困難はあるものの，式(11)で与えられる C^i の分布からCの分布を求めることは理論的に可能である。コンピュータを使えば，この計算は簡単にやってのけられる。最終的な結果は，図4のようになる。

異なった脅威からのリスクを比較するために，それらを同一のグラフ上に描き，リスク容認基準と照合しながらそれらを検証することができる。

図5を見ると，タイプⅢの脅威は最も深刻なもので，全く引き受けられない。タイプⅠは大きな損失を引き起こす確率が低く，リスク引き受け曲線によればほぼ引き受けてもかまわない。

図4　異なった期間における最終的なリスク曲線

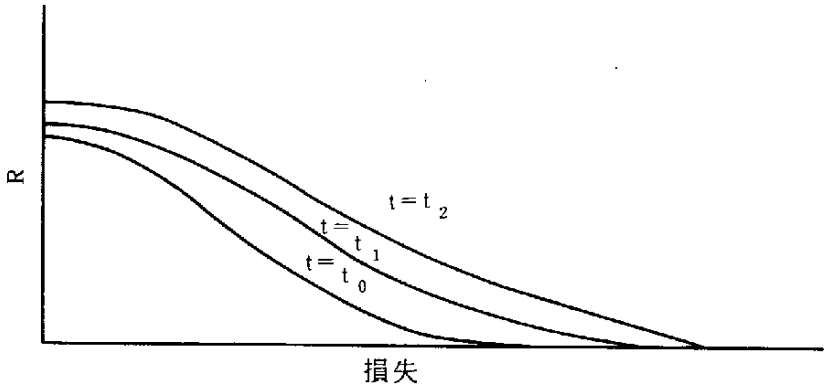
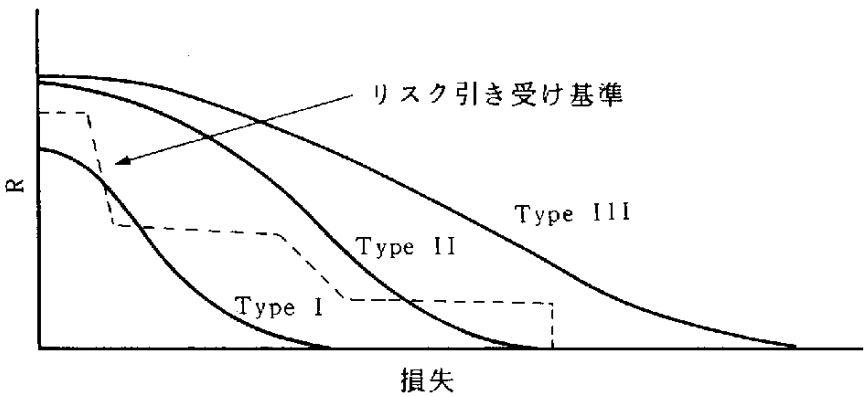
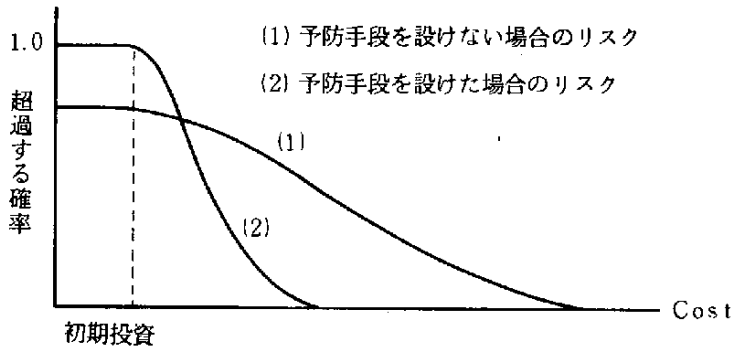


図5　リスクの比較



それぞれの脅威に予防的な処置をとったときの効果を知るために，それぞれの脅威に対する第2の曲線が必要である。この曲線は，予防措置に対する初期投資と，それによるトータルな投資の両方を含む。曲型的な例を図6に示す。数学的手法は先に述べたものと基本的に同じなので，重複することは避ける。

図6　予防措置を行った場合の，向こうｔ年間のリスクの変化



3.2　実　　施　　例

本論文の方法は，大規模コンピュータ・ネットワークの通信セキュリティ環境の分析において実施された（MOSL82）。分析の焦点は，通信に使用される暗号キーだった。考察の結果，いくつかの脅威と脆弱性が明らかにされ，起こりうる結果の程度が定量化された。それぞれの脅威について，統計的な方法で度数分布が求められた（PICK82）。図7にそのなかの1つの脅威の度数について，不確実さが確率分布として描かれている（MOSL82）。

図7　銀行の従業員の不正の年間度数

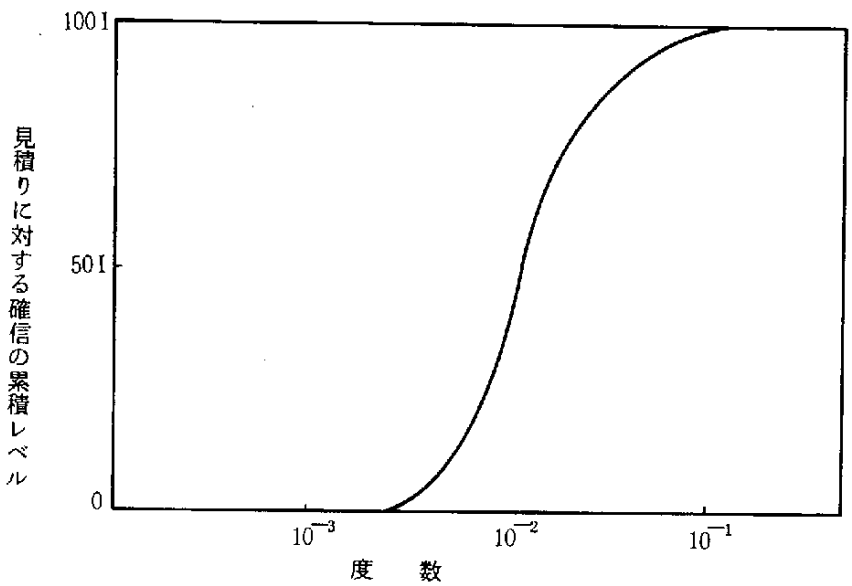
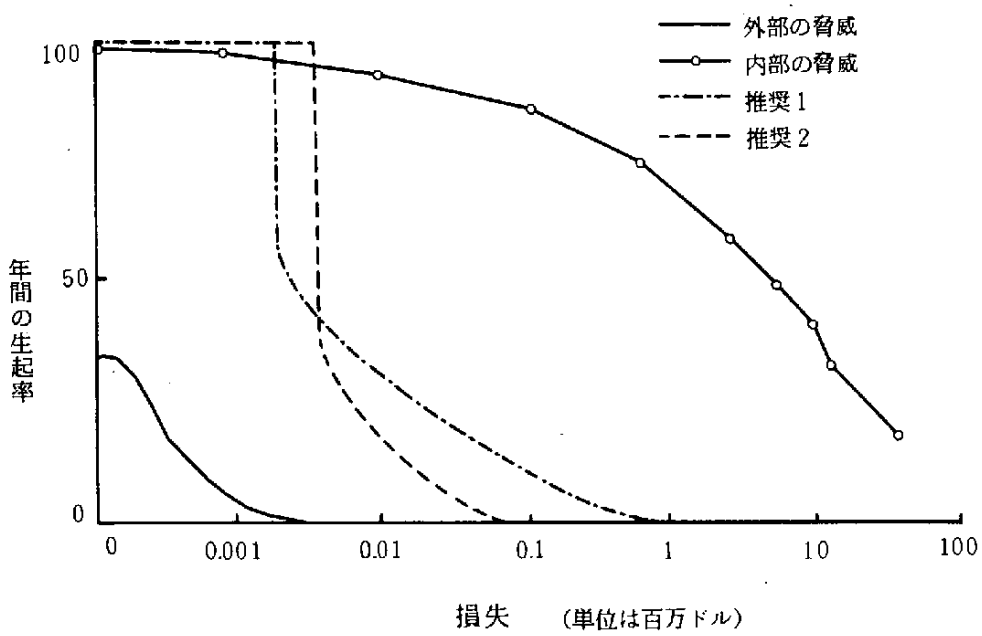


図8には2つの異なる脅威リスクが求められ，1年間の種々のレベルの損失の確率を与えるリスク・カーブとして描かれている。例えば，タイプⅠの脅威による1年間の損失が$ 1,000,000を越える確率は75％あることがわかる。また，脅威Ⅱによる損失が$ 1,000,000を越える見込みは0であることがわかる。

図8　2つの異なった脅威のリスク曲線



参 考 文 献

(BRAF81) Brafman, M.J., 1981, Evaluating computer controls using the matrix approach ; The EDP Audit, Control and Security Newsletter.

(COUR77) Courtney, R. H., 1977, Security risk assesment in electric data processing system ; Proceedings of National Computer Conference.

(LOBE80) Lobel, J., 1980, Risk analysis in the 1980's ; Proceedings of the National Computer Conference.

(KAPL et al.) Kaplan, S., et al., Methodology for probabilistic risk assesment of nuclear power plants ; Pickard, Lowe and Garrick, Inc., PLG-0209.

(PICK82) Pickard, Lowe and Garrick, Inc., 1982, Proprietary data.

(CINL75) Cinlar, E., 1975, Introduction to stochastic process; Prentice-Hall, Englewood, Cliffs, New York.

(WINK75) Winkler, R. L. and Hays, W. L., 1975, Statistics ; Holt, Rinehard and Winston, New York.

(MOSL82) Mosleh, A., Hilton, E. R., and Gersman, A.F., 1982, ATM key management risk analysis ; Pickard, Lowe and Garrick, Inc., PLG-0233, prepared for Target Bank.

ノランのステージ・モデルとコンピュータ・セキュリティ

Eugenio Orlandi, " Nolan's Stage Model and Computer Security" 1986, International Carnahan Conference on Security Technology, Gothenburg, Sweden, August 12-14, 1986

概　　要

リスクマネジメントにおいて，リスク分析が必要なことは明らかである。その一般的方法論の様相は，異なった，しばしば相矛盾するセキュリティ要求の中で個別に確立されていかねばならない。本論文では，リスク分析に構造的な（層状の）手法を用いる。そしてリスク分析の結果を，最もよく知られた組織におけるコンピュータの進化モデルである「ノランのステージ・モデル」に結びつける。

はじめに

コンピュータ・セキュリティはいくつかの副次的な目的（属性）を結び付けるグローバルな目的である因子化（Factoring）と呼ばれるコンピュータ分析の深部において，その主要なコンセプトが指摘されている。すなわち，信頼性（Reliability），完全性（Integrity），脆弱性（Vulnerability），機密性（Confidentiality），プライバシー（Privacy）である。これらのセキュリティ属性は，コンピュータ・セキュリティの帰納的で抽象的な定義のなかで，すなわち，$R \subseteq I \subseteq V \subseteq C \subseteq P$ という包含チェーンのフォーミュラにおいて配列されうるのである。包含チェーンによる手法は，コンピュータ・セキュリティ技術の進歩により見出された。そしてコンピュータ・セキュリティそれ自体はＥＤＰ技術の進歩の副産物だ。包含チェーンの選択により，内的セキュリティ矛盾，ＩＳＣ（Internal Security Conflicts），という各属性間の矛盾を最小にすることができる。すなわちアクセス・コントロール手段（電子ドア，区画）と人のセキュリティ（非常口）とのコンフリクトとか，デ

ータの完全性（バックアップ・コピー）と機密性（保護データの複数のコピーが存在する）とのコンフリクトである。

セキュリティ属性を適切に定義することにより，各属性がノランのモデルのどの段階に対応するのかあてはめてみることができる。ノランのモデルの円熟期に達したものだけが，セキュリティ・コンセプトの再定義が必要である。このコンピュータ・セキュリティ技術は，より正式にはセキュリティ・エンジニアリングと呼ばれる。セキュリティ・エンジニアリングは，上記のすべての属性について触れている。

セキュリティ・エンジニアリングの定義の前に，セキュリティ・フィジックスを紹介しておこう。セキュリティ・フィジックスは，セキュリティの基本構成要素について述べている。守られるべき客体（Object）と，その客体にアクセスしようとする主体（Subject）である。その他に，受権ルール，強制，権利の伝播ルール，主体間のコンフリクトの集合，外的セキュリティ・コンフリクト，ＥＳＣ（External Security Conflict），すなわち同時アクセスの発生，デッド・ロックについても述べられている。

どの組織においてもコンフリクトは起こる。なぜなら現行の保護システムは，増加する一方の潜在的ユーザに対して弱いからである。ノランのステージのどの移行においても，またいかなるＥＤＰ技術の進歩においても，ＥＤＰに登録される人員の数が，結果的には潜在的なコンフリクトの数が増加する。このように，技術的な改善は現在の保護システムの突破口を開く。

そのようなコンフリクトの解決法は，設計に，使用器具に，あるいは適切に客体，主体，アクセス・ルール，権利伝播ルール，コンフリクト解消ルールを定めた保護システムを更新していくに，すなわちセキュリティ・エンジニアリングにある。

もしセキュリティ・エンジニアリングがＥＳＣを解決することに失敗したら，たちどころに未解決のコンフリクトがエラー，悪用，犯罪を生むことだろう。

危険を減らすために，セキュリティ分析は，自動制御であるサプライヤー・セキュリティ・エンジニアリングが現れるまでは，手続き的な制御であるユーザ・

セキュリティ・エンジニアリングを採用する。

コンピュータ・セキュリティの属性

従来の手法では，コンピュータ・セキュリティを，信頼性，識別，アクセス・コントロール，完全性，受権，独立性，計量可能性，検出のようなn個の変数（属性）を持つ関数として扱う。すなわち，

$$S = [\, f\ y_1(x_h),\ y_2(x_h),\ \cdots\cdots,\ y_n(x_h)\,]$$

（$h = 1;\ 2,\ \cdots\cdots,\ m$）。$y_k$（$k = 1,\ 2,\ \cdots\cdots,\ n$）はセキュリティ属性，$\{\, x_h \,\}$は守られるべき客体である。

従来のセキュリティ分析では，セキュリティ計画はチェック・リスト（資産リスト，資産評価，リスク概要）の形で与えられ，関数f_k（セキュリティ属性）の完全加法性を仮定している。

$$S = \sum_{k=1}^{n} S_k = \sum_{k=1}^{n} f_k(y_1, y_2, \cdots\cdots, y_n) \Big|_{y_j = 0}$$

（$j \neq k$）（$j = 1, 2, \cdots\cdots, n$）またそれぞれの属性について，

$$S_k = f_k\,(g\,(x_h)) \qquad (h = 1, 2, \cdots\cdots, m)$$

それぞれのセキュリティ属性f_xについて，$x_h \neq 0$はチェックリストの項目である。y_kのほうは，同一の客体集合において定義されている。つまり，x_hは異なったy_kに繰り返し使われる。そして，同一のx_hについての異なった独立のアクションがコンフリクト（内的セキュリティ・コンフリクト）を引き起こし得るのだ。

チェックリストの項目とは，以下のようなものである。

・　＜t，o＞という対の要素

tは脅威，oは脅威によって影響を受ける客体である。tは頻度評価（レイティング）と強度評価（低，高，全）において詳細に示される。

・　四類＜s，o，r，p＞の要素

セキュリティ取り扱い時の情報を論理的に表現する。仮定された状態p下で客体oに対して権利rを持っているのが主体sである。

本論文では，コンピュータ・セキュリティの歴史的な進化を追いながら，包含チェーン（層状の）手法をセキュリティ分析について展開する。

$$y_1 \subseteq y_2 \subseteq \cdots\cdots \subseteq y_i \quad (i \leqq n)$$

この包含チェーンは，以下のステップにみられるような循環過程の結果として与えられる。

・　属性の導入と定義

・　$＜y_i，y_{i+1}＞$に属するx_h（$h = 1, 2, \cdots\cdots, m$）の定められている区間を狭めていくことにより，新属性と旧属性間のＥＳＣを構成する。この帰納過程は現実の要求（$1 \leqq i \leqq n-1$）と関係する。

定義：内的セキュリティ・コンフリクト

ＩＳＣあるいは属性コンフリクトは，客体の不整合コンフリクトである。あるセキュリティ属性を満たすと，そのセキュリティ・プランに属する他のセキュリティ属性が弱められることをいう。

定義：セキュリティ・フィジックス

すなわち，客体，主体，権利，客体に対する主体の制約，セキュリティにおける基本の概念間の一群の法則。

客体とは，ある一定の論理レベルではこれ以上分割できない価値の論理的あ

るいは物理的実体。主体とは，特定の客体に対してあらゆる権利を持った論理的あるいは物理的実体。権利とは，特定の主体がある客体に対して行使するアクション。述語とは，客体sが主体oに行使する権利rを制限する一つ以上の条件をいう。

ＩＳＣを解決する最も素早い方法は，問題となっている客体をさらに分割することだ。さもなければ，ＩＳＣを一つずつ除いていく方法論を見つけ出さねばならない。これが，包含チェーンによる方法である。

包含チェーンによる手法

コンピュータ・セキュリティの目的は，事故によってあるいは意図的に認定されていない人たちへデータが暴露されることを，あるいは認知されていないデータの変更や破壊を防ぐことにある。セキュリティを確保する第一歩は，ハードウェアとソフトウェアの信頼性の確立にある。

定義：信頼性

信頼性とは，定められた期間内に，あるいは確率で，システムがその機能を果たす能力のことである。$F(t)=P(\tau \leqq t)$ を期間 $0 \leqq \tau \leqq t$ に故障の起きる確率とすると，信頼性は次式で定義される。（$t>0$）

$$R(t)=1-F(t)$$

コンピュータ・システムの非常に一般的な定義ーインタラクションにおける要素の集合ーから，信頼性関数の下限と上限は以下のようになる。

・ 直列構成

システムの成功は，その全ての構成要素の成功による。

$$R(t)=\prod_{i=1}^{n} R_i(t)$$

・　並列構成

構成要素のどれか一つが成功なら，システムも成功となる。

$$R(t) = 1 - \prod_{i=1}^{n} (1 - Ri)$$

両者とも要素の確率に対して独立であると仮定している。今日のハードウェアの高い信頼性は，低いソフトウェアの信頼性と複合している。

もう一つのシステム評価の方法は使用可能性である。

定義：使用可能性

使用可能性とは，時間 t においてシステムが稼働している確率である。

使用可能性は，故障間平均時間 MTBF（Mean Time Between Failures）と平均修復時間 MTTR（Mean Time To Repair）によって表させる。

$$A(t) = \frac{MTBF}{MTBF + MTTR}$$

システムの信頼性のレベルには，経済的な理由での制限がある。しかし，合理的な信頼性のレベルを決めておくことが以下の考察において必要な前提条件である。

コンピュータ・システムが稼働中であり，主体が客体に操作可能な状態であれば，より以上の要件が満たされなければならない。

定義：完全性

完全性とは，完全で不変のシステムの状態である。組織に登録されている個人的データが，不必要に登録，変更，消去されないという保証である。

完全性は客体の一貫性の権利を表し，ハードウェア，ソフトウェア，運用に

おける信頼性を要求する。

これまでに二つのセキュリティ属性が紹介された。信頼性と完全性である。ＩＣＳを分析して解決するために，ＩＳＣテストが行われなければならない。

完全性の定義を見ると，信頼性は完全性必要条件であることがわかる。主体は客体にアクセスするが，このことは客体の使用可能性を意味している。信頼性は，そのシステム機能が重要であろうとなかろうと必要である。

ＲとＩに共通な要素が空集合φでなければ，すなわちＲ∩Ｉ≠φ，かつ（Ｒ－（Ｒ∩Ｉ））≠φ。もしも，（Ｒ－（Ｒ∩Ｉ））がシステムの状態において無視できる集合である場合，たとえば，「システムは使用可能であり作業総量はゼロである」場合にのみ，Ｉ⊇Ｒと書くことも可能である。

定義：脆弱性

脆弱性とは，不完全なデータ処理の結果としての大きな障害のもたらされる確率である。

脆弱性とは，分析についての予想損失または予想インパクトの主観的アセスメントである。これは完全性の概念をさらに押し進めたものだ。まず完全性の概念が定義されたら，脆弱性は完全性の要件を階層化し，定量的な様相を強調する。セキュリティ手段の採択については，増分費用を増加させ，逆に利益を減少させるといった法則に従う。

広い意味では，イニシャル・ロードに始まる，システムによって処理される一つ一つのオペレーションが，可逆的であることが保証される場合にのみ，完全性は満たされる。普通には，そのような要件を満たそうとすると，容認しがたいオーバーヘッドが生じてしまう。もしも完全性が信頼性と復旧プロセスの混合物により保証されるとするなら，脆弱性は信頼性や完全性を特定の組織の諸要求とに対応させ，定量的な様相を強調することになる。

再び，Ｉ∩Ｖ≠φ，かつ（Ｉ－（Ｉ∩Ｖ））≠φとする。特定の組織の実際

の要件との関係において完全性を考慮することにより，脆弱性は集合Ｉを集合Ｉ'に減ずる。したがって，（Ｉ－（Ｖ∩Ｉ））≒φ，かつＶ⊇Ｉ'（Ｉ⊇Ｉ'）となる。

定義：機密性

機密性とは資源情報と情報の収集者，散布者ないし利用者間の関係かつ／あるいは協定を含む。

機密性は，脆弱性アセスメント・プロセスの定性的な補集合として働く。すなわち，より深い主観的なデータ分析である「分類」によれば，実際上保護を必要とするデータに保護を限定することにより，処理時間と記憶を節約することができる。

再び，Ｃ∩Ｖ≠φ，かつ（Ｖ－（Ｃ∩Ｖ））≠φ。しかし，ある種のコンピュータ・システムについては，分類の後，（Ｖ－（Ｃ∩Ｖ）≒φ，かつＣ⊇Ｖ（Ｖ⊇Ｖ'）となる。

非常に一般的な定義と適当なサイト・ナリッジ（センシティヴ情報についてのアウトライン）間のトレードオフから，資源の経済が生ずることになる。

定義：プライバシー

プライバシーとは，個人あるいは組織についての情報やデータがいつ，どのように，どの程度まで他者に伝達されるのかを決定するため個人あるいは組織に対し保証されている権利として定義されている。

組織にとっては，プライバシーとは次のような法則によって課される外部的費用である。すなわち，プライバシーとは，時とともに変化する社会の中に打ち立てられた価値の集合である。プライバシー志向の分類は，プライバシーを守るために不可欠の要件である。Ｐ⊇Ｃという意味で，プライバシー分析を行えば機密性分析も達成される。客体の保護は，組織の機能階層（機密性）のみ

に関係するのではなく，組織と外部環境間の関係に関りがある。

上記の考察を整理すると，次のような包含チェーンが成立する。

$$R \subseteq I' \subseteq V' \subseteq C \subseteq P$$

そして，セキュリティ分析は，上記チェーンの左から右に，以下のステップを繰り返すことにより得られる。

(i) セキュリティ属性の定義
(ii) 内的セキュリティ矛盾の分析および構成。
(iii) 分析が完了するまで(i)(ii)を繰り返す。
(iv) 上記ステップによって保証されるＩＣＳ自動最小化に際しての対抗策の選択。

より深い洞察 — セキュリティ・エンジニアリング

包含チェーンはセキュリティ分析の記述的なフェーズである。その目標はセキュリティの確保にある。セキュリティを確保するための技法は，先にセキュリティ・エンジニアリングとして言及されたものを形成するのである。従来の手法がばらばらにセーフガードを示唆するのに対し，より構造的な計画は，異なったセキュリティ技術を筋のとおった形で組織化するのである。

この包含チェーン（層状の）アプローチは，現実の組織にとっての特定の要件までセーフガード・スペースを一致させる。この方法は主要点が示された必要条件との関係の内に冗長な情報を単純化し，また，各属性の定義間の距離をより小さいサブ集合へと変化させる。すなわち，$R \rightarrow R'$，$I \rightarrow I'$，$V \rightarrow V'$，$C \rightarrow C'$，$P \rightarrow P'$。

定義：外的セキュリティ・コンフリクト

外的セキュリティ・コンフリクト，ＥＳＣは，権限のある利用者間の公正な

競合，あるいは権限の与えられている利用者と与えられていない利用者間の不公正な競合において，主体が同一の客体と競合するとき生ずる。

前者の側面は同時生起に関係しており，基本的に，逐次にアクセスされる資源に適用される連続性（serializability）の手法によって解かれる。後者の側面は包含チェーンの右側（V，C，P）を扱い，コンピュータ・セキュリティの現在のフロンティアである。

定義：セキュリティ・エンジニアリング

セキュリティ・エンジニアリングとは，アクセス規則や権利伝播規則に基づき主体間のコンフリクトを予防・解決するための一群の技法である。

利用者の側からみると，実在のＯＳやデータベース管理システムに組み込まれた効果的なセキュリティ機構の効果的な管理が重要である。この機能は利用者のセキュリティ・エンジニアリングをあらわしている。その目的は，識別，権限とアクセス制御（予防属性），アカウンタビリティと検出（制御属性）といった包含チェーンアプローチを直接に扱うことのない，セキュリティ属性を完全に満足させることにある。

検証のツールとして権限と権利伝播規則の知識が，システム・セキュリティを効果的に分析するために不可欠な前提条件である。設計のツール，ＯＳのアクセス制御システムとセキュア・データベース設計（業者のセキュリティ・エンジニアリングである）に関しては，さらに，概念的，論理的，物理的設計の３つのフェーズに分けられる。

包含チェーンアプローチによってその概要を挙げられたセキュリティの要件は，アクセス制御の方針の明細を含んでいる。その一つ一つは個別のセキュリティ問題への答えを意図しているが，いくつかのアプローチ，技法，システム，方法論といったものがアクセス制御管理のために提案されている。

主要な問題点は，アクセス権，権利伝播規則，動的権限管理の効果的な制御

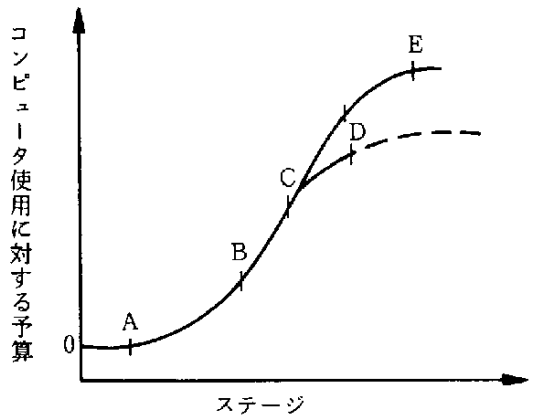
である。データの統合化，マルチ・ユーザ間のデータの共有への傾向が進めば，このような問題の複雑さはさらに拡大される。

ノランのステージ・モデルとコンピュータ・セキュリティ

コンピュータ・セキュリティの属性がその相互の接続について紹介・描写されれば，それぞれの属性がノランのモデルのどのステージにあるのかあてはめてみることが可能である。

ノランのステージ・モデルは，最もよく知られた組織におけるコンピュータの進化モデルである。これは，コンピュータ予算の変化によって示された変化の状態を因子化することをその基礎としている。予算曲線は，環境的・技術的な変数のさまざまな変化のインディケータとして用いられる。

図1　予算曲線とノランのステージ・モデル



ノランの6つのステージとは，簡単に述べると，

(i) 開始期　基本的なニーズを満たすために，組織にコンピュータを導入する。

(ii) 拡張期　コンピュータ使用の急激で無節操な増加。

(iii) 統制期　コンピュータ使用に関する知識の増加とコンピュータへの出費の制限。

(iv) 統合期　無駄遣いせずにコンピュータを使えるまでに制御が洗練される。

(v) データ管理期　コンピュータ管理の焦点がデータの管理に移る。

(vi) 成熟期　アプリケーション・ポートフォリオが完成する。その構造が組織や会社内の情報データの流れに反映する。

この情報システムの発展についての一般的な記述は，情報システムのセキュリティの特定の様相とも合一する。それぞれのステージにおいて，セキュリティの概念が再定義されなければならない。すべてのセキュリティ属性は各ステージに関係するのである。すなわち，従来のアプローチでは十分ではない。しかし，各ステージでそのステージに臨界的な属性を見つけ出すことができる。それがステージの主要属性である。

遅延時間，$\triangle\tau$は，ノランのステージの一般的な学習経験と，特定のセキュリティ属性の学習経験の間の距離である。

ノランのステージとセキュリティ属性は次のように結びつけられる。すなわち，各ステージは入力として主要セキュリティ属性を持っており，出力においては，新しい主要なセキュリティ属性を生み出している。出力属性の定義は，そのステージの間に蓄積された知識（学習経験）を表すことになる。

ノランのモデルは特定の機構の軌跡を表す。それはある者にとっては未来のことなのかもしれない。そういう意味で，これは単に叙述というだけでなく処方ともなる。

ノランの成熟期だけが，セキュリティ概念の再定義を要求する。ここに，過

去の軌跡のシステマティックな整理が未来の推定となるのである。

この，より問題意識を持ったコンピュータ・セキュリティに対する見地がセキュリティ・エンジニアリングとして触れられてきた。セキュリティ・エンジニアリングは先に述べたすべてのセキュリティ関連属性を包含している。不確定な未来について思索するためには，良い戦略がアクセス制御システムデザインの正当性を正式に証明することになる。これには高度な形式化を要する。

図2　ノランのステージと主要セキュリティ属性

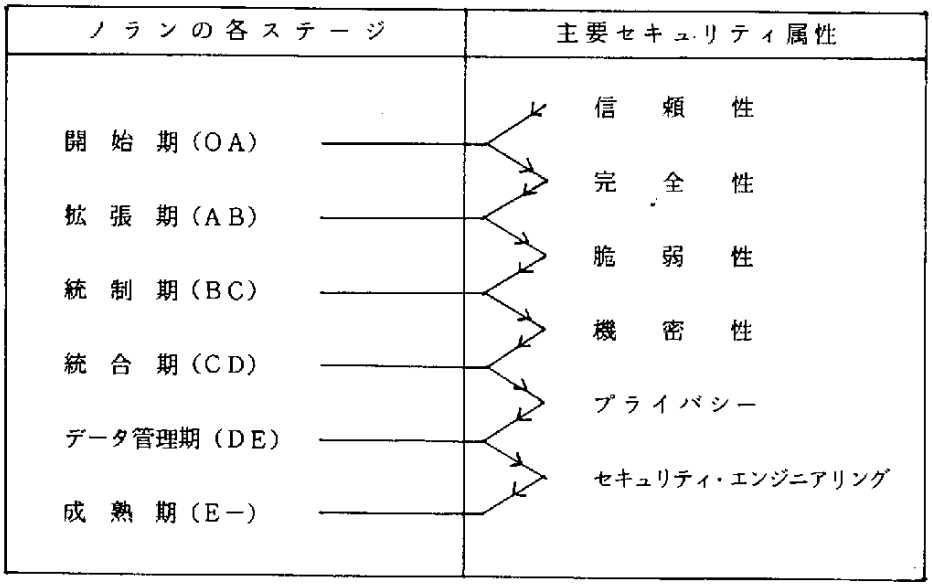


図2を見てみると，信頼性は開始期(i)への前提条件になっている。信頼性は，もとをただせばその起源はハードウェア・システムの信頼性にある。開始期にあるセキュリティ属性は完全性である。コンピュータ使用における不完全なデータ制御はデータ・リカバリーの技術を発展させた。開始期の終わりには，復旧／リスタート手続きの知識は洗練されてきている。それは，拡張期(ii)へのインプットとなる。

急激で無節操にコンピュータの使用は，人間の処理に比べて脆弱である点がわかってくる。資源に制限が起きる制御期(iii)には，「知る必要」あるいは機密

性に照らして需要がモデル化される。

さらに，制御は洗練され，経済性の分析が行われる。すなわち，コンピュータの使用は組織の資源であると見なされるようになる。統合期(iv)のアウトプットは，プライバシーの必要性である。機密性とプライバシーは，データ管理期(v)を可能にした洗練された「データ管理システム」によって確保されるのである。

現在，ローカル・ネットワーク，データ伝送回線，ＯＡ，パソコンの使用には，集中化と分散化の新しいバランスの必要性が持ち上がってきている。したがって，過去の主要なセキュリティ属性についての経験的な知識は，より構造化された知識，すなわち，セキュリティ・エンジニアリングへと転換されなければならない。

結　　論

リスク・マネジメントは，特定のリスク分析技術とは弱い関係しか持たず，概念や意味に深い関心を持った，管理芸術の始まりである。

今日のような技術の時代にコンピュータ・セキュリティを企てるということは，非常に選択的になるということである。類推するに，概念同志の結合や，現象や動向を読み取るための鍵が管理の手順においてそれなりの役割を演じる。

本論文において，リスク管理の問題点に焦点を合わせるべく，コンピュータ・セキュリティの基本概念である「属性」とその相互の関係が個別に分析された。続いて，セキュリティの諸要求がコンピュータ・システムの進化のより一般的で説明的なモデルである，ノランのステージ・モデルと結びつけられた。セキュリティについての層状の手法は，従来のリスク分析を迂回するわけではない。しかし，それらの相互の関係と制限を強調する。

提唱された手法を，コンピュータ・セキュリティの戦術的な企画のための手助けとして，あるいはリスク分析の技術面での骨格を構成するツールとして考えられたい。

参 考 文 献

1. R.L.Nolan, "L'informatica a grosse dosi fa male ai dirigenti", Harward-Espansione, No.10, 1981, pp.1-12

2. D.S.Appleton, "Business Rules : The Missing Link"（ビジネスの諸法則，足りないリンク），Datamation, Oct 15, 1985, pp. 145-150

3. U.Bussolati and G.Martella, "Towards a New Approach to Secure Database Design"（セキュア・データベース設計の新しい手法をめざして），Computers & Security, Vol.2, No.1, Jan 1983, pp.49-62

4. J.M.Carrol and W.R.Mac Iver, "Towards an Expert System for Computer-Facility Certification"（コンピュータ設備保障のためのエキスパート・システムをめざして），Computer Security : A Global Challenge, IFIP／Sec'84, J.H.Finch and E.G.Dougall (eds), 1984, pp.109-122

5. J.L.King and K.L.Kramer, "Evolution and Organizational Information Systems : An Assessment of Nolan's Stage Model"（進化のそして組織化のシステム，ノランのステージ・モデルの評価），Communications ACM, Vol.27, No.5, May 1984, pp.466-475

テクノロジー支援によるリスク・マネジメント

Reed, Alan, "Risk Management by Technology - A Way out of the Impasse - Latest Developments in Software Devoted to Risk and Disaster Management", March 1986.

1. はじめに

1978年7月にアメリカの大統領行政府のオフィス・オブ・マネジメント・アンド・バジェットが，定期的なリスク分析を遂行するよう連邦政府の諸部局に指示した際に，データ処理業界では，最もコストの点で効果的なセーフガード（保護手段）を入手するために，資産との関連の中で，脅威（threats）の発生確率とインパクトについて判断をする努力をなした。この場合の基本線は，コンティンジェンシー・プランの創案ないしセーフガードの購入の手助けとなることであった。データ処理の辞書は，定量的／定性的なリスク分析，FIPS-PUB 65なり，年間損失想定額（annual loss expectancy = ALE）といった指摘により増加されていった。当論文の目的は，現在最もポピュラーである基本的なマニュアル・メソッドをめぐって，最近のソフトウェア技術の開発が，実際前進をとげたのかどうかを評価することである。そうした技術の成果が真に袋小路からの出口を創出しているのか，またデータ処理業界では，常に完成間際か決して検証されないコンティンジェンシー・プランに組み合わされた高，中，低といった脅威頻度の見込みに相変わらず基づいているのかが問われている。

2. リスク・マネジメント〔バックグランド情報〕

リスク・マネジメント・コントロールは，情報処理の環境のなかでより良いセキュリティを得るための出発点である。リスク・ディザスター・コントロールは，現在および未来において通常の業務やシステム機能の範囲内に組み込

まれるべきである。しかしながら，そうしたコントロールは組織内において，経営実践なり企業目標のなかで，本来当然備わっていなければならないのである。

いかなる方法論が用いられようとも，次のようなフェーズがある：

資産のフェーズ　再取得価格との関連で数値を出すための資産の定量化。その価値は事実（売り主）に基づくか，チームの評価（デルファイ法）によることになろう。

データのフェーズ　問題の現実的な性質に関しての，脅威・脆弱性の定量化。言いかえれば，いかなる脅威が，組織なり，類似の組織体や近隣の人達に損失をもたらしてきたのか。デルファイ法が，脅威・脆弱性の評価に用いることができよう。

コスト・ベネフィットのフェーズ（対費用効果）　金額値でのＡＬＥ値（定量的）ないし頻度（定性的）を造りだすため，脅威のインパクトおよび頻度に対して測定された，セーフガードの評価・分析。基本線（bottom line）は，最小のコストで最大の脅威の軽減ないし投資収益をもたらす反応を生みだすことである。

これらの三つのフェーズは，コスト・ベネフィットのフェーズを遂行するにさいして求められる資源を軽減するためにも，リスク・マネジメント・チームのスキルの度合い，データ（脅威）の価値，業務の遂行ないし自動装置の購入にあたり利用可能となる資金に依存している。ところがその業務は厖大であり，定量的なリスク分析はほとんど実行されていない。最近のフロスト・サリバンのＵＳ大企業についての調査（1984年8月　343社回答）では，体系的なリスク評価を実施したのは回答企業の3分の1以下であったとされている。104社の有効回答のうち，そうした評価が定量的であったか，定性的であったかどうかについて報告があったのは，わずか６８回答であった。銀行は最も高い経験度を有していたが，小規模の商業組織では低コストの定性的なアプローチを用

いる傾向があった。

明らかな事実は，多量のデータが処理される必要があるが，低コストの自動化されたツールがないということである。

3. テクノロジー支援によるリスク・マネジメント

利用可能となる基本的な定量的成果は，ＡＬＥの概念に基づいている。それらは，連邦情報処理基準（ＦＩＰＳ）のパブリケーション №31 および 65 から得られたものである。定性的なアプローチについては，スタンフォード・リサーチ・インスティチュート(ＲＩＭ) およびインフォメーション・ポリシー・インコーポレイティド（Fuzzy Metrics）により採用されていた。最初の方法では，自然発生の「地震シンドローム」に基づいており，通常人間に関係するところの内部的な脅威・脆弱性に基づくものではなかった。さまざまなアプローチは，データの計算もなく，限定的であり，それらの多くは経験に拠っている。この最終的な成果は，マネジメントがほとんど確信のないデータに基づいて意志決定するということである。

過去 200 年にわたって進展してきた統計的なベイジアン・メソッドは新しいミクロ・プロダクトのためのフレームワークとして利用されてきている。それは，ベイジアン意志決定支援システム（ＢＤＳＳ）で，データの諸要素すべてを用いて，リスクを評価すべくデザインされている。

それではＢＤＳＳとはなんであろうか。

BDSSとは，Pickard，Lowe，and Garrick Incorporated のスタッフであったDr.Ali Mosleh により開発された新しいプロダクトである。……ＢＤＳＳは，インフォメーション・セキュリティと核技術それぞれの領域において展開されてきた定量的なリスク評価の方法論・テクニックの最初の結合を意味している。ＢＤＳＳにより得られるリポートは適切な脅威のイクスポジュアならびに勧告されるセーフガードの相対的なベネフィットを図示してく

れるのである。

ＢＤＳＳの能力が含んでいるのは以下のとおりである。

- プロジェクトの規模分類
- 資産のインベントリー／損失イクスポジュア
- 脅威・脆弱性のマッピング
- 信頼性ファクター　これは，損失推定値にかかわる不確実性をあらわす。
- グラフィックス　脅威について軽減されない状態の損失のリスク・カーブとリスク軽減手段適用による場合の脅威を表す，軽減後の損失のリスク・カーブを二重写しで描く。
- エグゼグティブ意志決定支援モジュール　熟知のもとで，防御的な意志決定するのに必要な情報を上級経営者に提供する。
- テクニカル・アナリシス・モジュール　ＢＤＳＳの実行により生み出されるか，それを支援する十分詳細な情報を提供する。

4.　ディザスター・マネジメント〔バックグランド情報〕

リスク・マネジメントはいかなるコンティンジェンシー／ディザスター・プランが必要か，どういったタイプのスタンバイ・サイトが必要かを明らかにするのに用いられている。Datapro 1984 British User Surveyでは，ディザスター・リカバリー・プランとの関連で特有の質問をなした。その調査が示したのは，メインフレーム・サイトの４９.２％が，ミニコンピュータ・サイトの４６％がそうしたプランを有していたことであった。

リスク・マネジメントおよびディザスター・マネジメントの実践双方共マネジメントのコミットメントを必要とするし，２０マン・デイと１５０マン・デイとの間で変化するに加え，ハードウェアおよびデータ・コミュニケーション・ネットワークに依存して変わるもろもろの資源を必要としている。このマン・デイ期間は，上級チーム・メンバーが仕事に打ち込んでいるのか，パートタイムなのか

どうかに拠るが，概してプロジェクト・タイムをたやすく２倍にしうる期間に広がっていくのである。通常，パートタイムの方が，一般に標準とされているのである。

リスク・マネジメントの場合のように，ディザスター・プロジェクトは，次のような段階を踏んでいる：

1. プロジェクト・プランニング
2. データの収集および分析
3. プランのテストおよび監査

フェーズ２が主たる要素であり，それは以下の課業を含んでいる：

- 資産の棚卸しを行う。
- 重要な脅威を確認するためイクスポジュア分析を行い，プランの取り扱いを最少限度にするための手続きを勧告する。
- ディザスター・チームを設立するため，マンパワー・スキルおよびマネジメント構成を評価する。
- 決定的に重要なリコード・プログラムを行うために，コミュニケーション・ネットワーク，クリティカル・アプリケーション，ドキュメンテーション，ハードウェアおよびシステム・ソフトウェアに関連するデータを収集する。
- 必要とされるサービスの反応および収入／損失のインパクトを評価するため，プロダクション・ジョブおよびスケジュールを分析する。
- バックアップおよびオフサイト・メディアストレージ・ファシリティをリビューする。
- これまで伝授されたことを展開し，サルベージし，コントロール（プランの修正）手続きを変更する。

マン・デイおよび資源についての要請は，実質的に，ミクロ・プロダクト（micro product）により軽減することができる。そしてプロジェクトのサイクルは７０％まで減少されうると予測されている。

5. テクノロジーによるディザスター・マネジメント

ディザスター・プランの自動化は，多くの有利性を有している。それに含まれるのは次のとおりである：

- 自動更新・編集
- テスト中および現実の災害中，時間に効率的なプランの修正
- フロッピー・ディスクが利用されうるため，より容易なディストリビューションならびにストレージ

EDPセキュリティは，1979年にという最初のミクロ・プロダクト（1979年のDisaster Plan 80）から始まった。このプロダクトは，実際のリカバリー活動中，クリティカル・プロジェクト・パスを修正するためにハーバード・プロジェクト・マネジャー（Harvard Project Manager）と統合されている。Disaster Plan 80 が提供するのは次の特徴である：

- プランニング・モジュール，それは，プロジェクト・プランニング，データ・コレクション，フィジカル・プランニング，トレーニング，そして保険を合体させたものである。
- アクション・モジュール，それは，マニュアル・メンテナンスおよびディストリビューション，データ・バックアップ，プラン・イニシエーション，エスカレーション・プロセデュア，ディザスター・チーム，クリティカル・アプリケーション，それにテスティング・プロセデュアを合体させている。

このプロダクトは，現在，1000以上のサイトで設置されており，ワードスター，マルチメイト，ディスプレイライターといったワード・プロセッサの基でテキスト・ファイルを利用している。

Recovery／1は，新しいミクロ・プロダクトで，コネチカット州のトーランドにあるコンピュータ・パフォーマンス社により開発されたものである。Disaster Plan 80と異なり，Ricovery／1は，データを収集し，組織化し，管理するた

め，データベース・マネジメント・システムを利用するのである。その特徴は以下のものを含んでいる。

- メニュー・ドライブン・オペレーション
- フォーム・オリエンティド・データ・エントリー・スクリーン
- オン・ゴーイング・ベーシスでの，コンティンジェンシー・プランの事前準備，テスト，メンテナンスを認める自動化されたプロセス
- User Defined Data Base Selection Criteria に基づくリポート・ジェネレーション
- プラン構成，トラッキング，報告のためのプロジェクト・マネジメント・アプローチ
- 支持されるミクロ・プロダクツは，IBM PC，Wang Professional，DEC Rainbow を含んでいる。

6. 要約および勧告

リスクがたとえ何であれ，「他人事」症候群（Can't Happen to Me' Syndorome）が依然として根強く存在している。法律により，リスクないしディザスター・マネジメントが命令されていないような環境下では，ほとんど定量的なリスク分析の実践はなされていない。典型的な情報処理装置を保護するために最低のセーフガードが目立つくらいである。代表的なマネジャーはコンティンジェンシー・プランニングが必要であることを実感している。しかしながら，スキルのある十分な資源および資金が無いことは，プロジェクトが財務管理に売り渡されうることを述べている。

最初の質問に立ち返ってみて，リスク・ディザスター・マネジメントにおける最近のソフトウェアの開発は情報処理業界を袋小路から脱出させているのであろうか？回答はイエスである。それは，BDSSおよびRecovery／1 がその他の一般的なソフトウェア・アプリケーション・パッケージとの関係から競争的な価格づけがなされており，業務遂行のために必要な経営資源を実質的に軽減させるべく，反復的なインプット・データを最小化する補助策を提供しているからである。

LAVA－リスク分析のフレームワーク

S. T. Smith, J. J. Lim, J. R. Phillips, R. M. Tisinger, D. C. Brown, and P. D. FitzGerald LAVA：A Conceptual Framework for Automated Risk Analysis LA-UR-86-4113

アブストラクトの要約

当該論文は，ロスアラモス国立研究所（Los Alamos National Laboratory）において開発されたリスク分析のためのメソドロジーについての論文である。リスク分析は，資産（asset）範疇の全体の集合（セット），脅威の全体のスペクトラム，脅威から資産を護るセーフガードのシステム特有のセット，それにセーフガード・システムの弱点につけこむ脅威から生じるアウトカム全体のセットにより特徴づけられるシステムについてなされる。

LAVAとは，Los Alamos Vulnerability and Risk Assessment Methodologyからとったモデルを指している。LAVAは，階層的なシステム理論，イベント・ツリー，あいまい集合（fuzzy sets），自然言語処理，意志決定理論，それに効用理論に基づいている。LAVAのフレームワークは，若干の副次的（きめ細かに嵌め込まれた）分析結果に関わるあいまい・イベント・ツリーの階層集合である。すなわち，システム・セーフガードの存在および有効性について情報を提供する脆弱性の評価，動態的（可変的）な脅威に対する資産のアトラクティブネス分析と連合した静態的（背景にある）脅威・動態的（可変的）脅威の構成要素について情報を提供する脅威分析，アウトカム（outcome）スペクトラムの強度の尺度とインパクトの価値についての情報を提供する結果（concequence）分析である。

LAVAが生み出すのは，定量的・定性的インサイトである：すなわち（貨幣的・言語的）対の価値が，それぞれの脅威／資産／セーフガード機能／アウトカムという4重の組（quadruple）について損失イクスポジュアを表すのである。現在のところ，LAVAは，さまざまに組み込まれたシステムにおけるリスク・マ

ネジメント，サバイバビリティ・システム，兵器システム・セキュリティ等のモデル化のために適用されている。ＬＡＶＡは，特に，大がかりな人的構成要素を含むサブジェクト・システムのモデル化に有効である。

1. 序

ＬＡＶＡは，ロスアラモス国立研究所（Los Alamos National Laboratory）において開発された，リスク・マネジメントへの独自のアプローチである。複雑なセーフガードおよびセキュリティ・システム内の脆弱性ならびにリスクを評価する体系的な方法論である。なお，大規模で複雑なシステム内の脆弱性ならびにリスクを確認するためのツールを提供する研究努力の一部となっているのが，関連するＬＡＶＡソフトである。そして，ＬＡＶＡは，一連のコンピュータ・プログラムとして実行されてきている。

ＬＡＶＡのユーザは，ＬＡＶＡ／ＸＸを利用するにあたり，熟達したリスク・アナリストである必要はない。ユーザにとって求められるただ一つの知識は，彼らが最も良く知っているところの，施設，組織，資産，設備，経営方針，手続き，そしてセキュリティ実践についての情報である。また，ＬＡＶＡソフトウェア・システムでは，これらの情報を，自動化された質問表により引き出すことができ，質問表において得られた情報から経営者には一般的な報告書を，現場のスタッフには詳細な報告書を作成している。

ＬＡＶＡの方法論が適用されるサブジェクト・システムは，大がかりで複雑なシステムで，大規模な人的構成要素，多数の不正確なデータ，明確に決定しがたい出来事などによって特徴づけられている。システムの脆弱性につけこむ脅威から生ずる結果は，しばしば通常の用語での定量化を不可能にする壊滅的な特性を有している。

この方法論が用いているのは，多層のシステム理論，イベント・ツリー型分析，あいまい集合論，意志決定論，効用理論，知識ベースのエキスパート・システム理論，それに自然言語処理である。そして，当該方法論は，セーフガー

ド・システムの脆弱性に定量的・定性的インサイトを与え，対象たるシステムのセーフガード・システムの状態についての正確な構図を生み出し，システムの損失イクスポジュア（リスク）に関し定量的・定性的な表示をもたらしてくれる。

ＬＡＶＡの方法論は，様々なコンピュータ関連のシステムにおける脆弱性とリスクのモデル化に適用されている。例えば，コンピュータ・セキュリティ・システム，プラント・ルーム・コントロール・オペレーション，核セーフガード・コンピュータ・セキュリティ等に適用されている。

2. 用語の定義

ＬＡＶＡのコンテクストにおいては，いくつかの用語が，特別の意味で使用されている。それらには次の用語がある：

資　　産　　対象組織にとり何等かの固有の価値を有する品目ないし品目の範疇。資産は脅威により影響を受け，アウトカムに至る。

ハード・データ　　バルブの欠陥率もしくは既知の出来事が発生する年間平均回数のような，定量的に容易に表示しうるデータないし情報

インパクト　　特定の資産にかかわるセーフガード機能の脆弱性にうまくつけいった脅威から発生した強度＂Ｘ＂のアウトカムの，対象となる組織への結果（consequence）ないしコスト，または影響。インパクトは，貨幣的（経済的）および非貨幣的（言語的）な，対の価値として与えられる。

損失イクスポジュア　　セーフガード機能の脆弱性にうまくつけいった脅威が，ある計算された度合いの強度のアウトカムを生み出す，対象となる組織にとっての，リスク。貨幣的（経済的）および非貨幣的（言語的）という，対の価値として与えられる。

アウトカム（outcome）　特定の資産に関するセーフガード機能の脆弱性に脅威がうまくつけいる際に生じる（通常望ましくない）イベント。（しばしば，誤って，脅威と混同される。例えば，"全壊の脅威"といったように。全壊とは実際上，『アウトカム』のこと（outcome）である。脅威の定義を参照のこと）

アウトカムの強度　この特定のアウトカムに脅威がいかにうまく作用したか，損害（damage）はどのくらいか，の尺度。アウトカムの強度は，セーフガード機能の相対的弱さと脅威の相対的強さの関数である。

セーフガード　方針，手続き，物理的ないし論理的デバイス等で，資産を脅威から護ることにより望ましくない結果を予防するよう企画されたもの。

セーフガード機能　セーフガードないしセーフガード集合が達成すべく意図された防衛機構の機能的表現。

ソフト・データ　人間の生命の価値ないし非常に重要なドキュメント，ないし微妙なイベントが起こったか，発見されたかどうかといった定量化するのが困難か，不可能なデータなり情報。

対象システム　アセスメント（評価）がなされるシステムないし領域（ユニバース）。（対象となる組織は対象となるシステムについて有責である。）

脅威（threat）　資産にたいし，何等かの危険（danger）ないし危害（menace）をもたらすところの人，自然力，事物ないしアイデア（もしくはその範疇）。脅威は，作用因であって，アウトカムと混同されるべきではない。

脆弱性　セキュリティ・システムないしプロセデュアル・システムといったセーフガード機能において，資産もしくは資産集合に害（harm)を引き起こす脅威によりもたらされる弱点ないし欠陥（flaw）。

3. ＬＡＶＡの技術的な基礎

ＬＡＶＡの方法論は，リスク・マネジメントへの，構造化されたモジュール式のシステムズ・アプローチである。特定のアプリケーションのため，当該アプローチは次の４つの段階（phase）からなっている。すなわち，システムのモデル化，ＬＡＶＡの分析のために必要な情報の収集，３つの別々の分析からの対象組織のロス・イクスポジュアの決定，リスク・マネジメント問題の解決，である。

A　モデル化のフェーズ（段階）

対象システムについて，ＬＡＶＡは，システムの脆弱性を評価し，脆弱性につけいった結果を分析し，結果集合から生ずる対象組織の損失イクスポジュア集合を計算する。ＬＡＶＡへのアプリケーションのモデル化に際しては，採択されねばならぬステップがある。（原文と書式を変えて示すと次のとおり：）

1. 対象システムを確認し，当該システムの特徴を明確化し，分析の範囲（scope）を特定化する。
2. システム資産，好ましくないアウトカムの集合，資産に対する脅威を定義する。
3. アウトカムのいずれが脅威と資産との相互作用から生ずるのか，どのようなセーフガード機能が脅威から資産を護るために適所にあらねばならぬのかを理解しうるように，脅威が資産に影響を与える点を考慮する。
4. いずれの要因がアウトカムの強度に影響を与えるのか，どの副次的機能がセーフガード機能のパフォーマンス・レベルを決定するのかを決める。

5. 対象システムの明細をモデル化するため，相互連関的な質問表をデザインする。

資産とは，危害に対しセーフガードされねばならぬ，組織にとっての価値（items of value）である。資産に含まれるのは（以下に限定されるわけではないが），不動産，あらゆる種類の設備，文書類，人員，情報，評判，事業遂行能力，その他，組織自体を含めて，価値のある物である。資産は，次のような価値に影響を与える属性を有している。すなわち，センシティビティ，クリティカリティ，コンプロマイザビリティ（Compromisability），セフトワージィネス（Theftworthiness），タイムリーネス等である。

さてＬＡＶＡのアプリケーションのための資産のモデル化に際しては，次のような資産カテゴリーが作り出されている。すなわち，ヒューマン・リーダブル情報ないしマシーン・リーダブル情報といったような資産を扱うカテゴリーである。脅威は，資産に危険をもたらす作用因であり，（部内者，部外者といった）人，自然力，事物もしくはアイデアである。モデル化に際し用いる脅威のカテゴリーは，自然ハザード，オンサイト・ヒューマン，オフサイト・ヒューマンといった広義のものである。脅威はまた，（変化のない）静態的構成要素と（時間により変化する）動態的構成要素という２つの部分を有するものとして取り扱うことができる。

組織の資産とそれらへの脅威を表すため，資産のスペースをA，脅威のスペースをTと定義する。資産・脅威のスペースは，特定のアプリケーション・システムをモデル化する特有の範疇からなっている。すなわち，

$$A = \{ a_1, a_2, \cdots\cdots a_i \}$$
$$T = \{ t_1, t_2, \cdots\cdots t_j \}$$

そして，アプリケーション・システムに起こりそうな，脅威—資産の相互連関の種類をシステマティックにブレークダウンしうるように，脅威と資産とをペアで考慮するのである。すなわち，

$$T \times A = \{ t_1 a_1, \ t_2 a_2, \cdots\cdots, \ t_j a_i \}$$

そして，好ましくないアウトカムの集合と結び付いた起こりうる相互連関は，

$$O = \{ O_1, O_2, \cdots\cdots, O_q \}$$

として表示され，セーフガード機能集合がどうあるべきかを決定することになる。

脅威，資産，セーフガード機能の関係は，図1，図2における構造（hierachical multilevel disaggregation structures）にて例示されている。ＬＡＶＡモデルでは，それぞれの脅威について別々の階層が有り，トップレベルには脅威があり，次は資産が含まれ，ボトムレベルには，それぞれの脅威－資産のペアについてのセーフガード機能が表示されている。コンピュータ・セキュリティ・アプリケーションにおいては，３つの脅威の範疇がある。すなわち，自然／ランダム・ハザード，オンサイト・ヒューマン，オフサイト・ヒューマンである。そして，資産範疇は４つあり，施設ないしフィジカル・プラント，コンピュータ関連ハードウェア，マシーン・リーダブル情報，ヒューマン・リーダブル情報である。ここでの例（アプリケーション）においては，全体のセーフガード機能集合が予防するようにデザインされている好ましくないアウトカムを組成している６つのアウトカムがある。すなわち，権限のないアクセスないし使用，修正もしくは不正変更（tampering），損傷（damage）ないし破壊，漏洩，盗難，使用拒否である。

図１は，自然ハザード脅威についての階層である。資産は，単独のターゲットとして扱われている。図２は，オンサイト・ヒューマンに関する階層である。

セーフガード・システムは，脅威から資産を護るメカニズムの集合から成っている。そうしたシステムは，ガード，フェンス，犬といった物理的手段；鍵，セキュリティ・クレードルといった機械的な手段；規則，ガイドライン，標準作業手順（ＳＯＰｓ）といった手続き上のコントロール手段；モニター，センサー，アラーム，クローズドサーキット・テレビジョン（ＣＣＴＶ）といった電子

図1　自然ハザード脅威に関するリスク・アセスメント構造

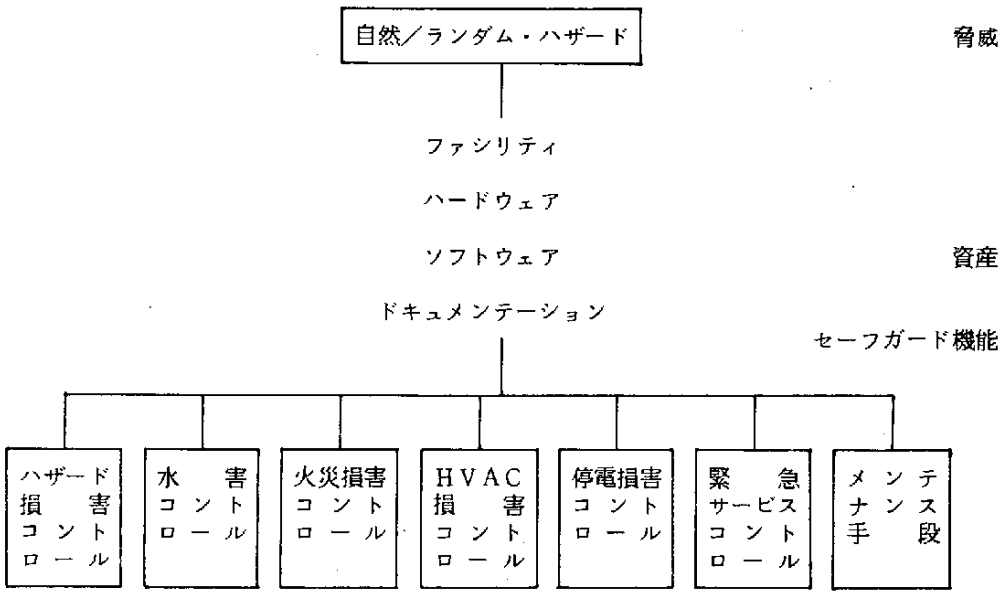
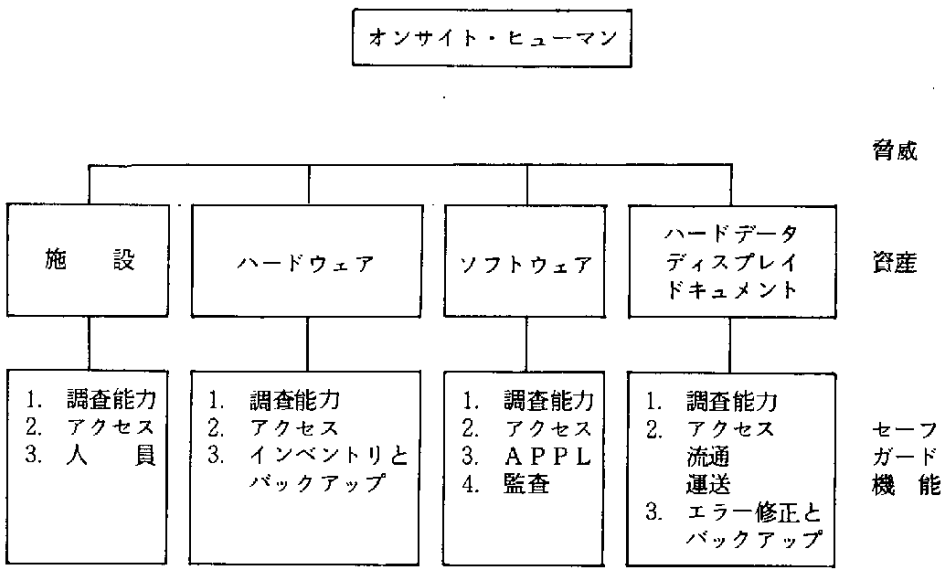


図2　オンサイト・ヒューマンに関するリスク・アセスメント構造



装置；パスワード，インテリジェント・カード，シールディング等のテクニカル手段を含んでいる。セーフガードは，〔脅威，資産，セーフガード機能，アウトカム〕という4重の組（quadruple）に関係する特定のコントロール手段および対抗手段と考えることができる。

セーフガード機能は，資産を脅威から保護するという目的を遂行する。脅威ー資産の相互作用を妨げ，好ましくないアウトカムの発生を予防するのを目的とするセーフガード集合を〔脅威，資産〕のペアが有している〔脅威，資産，アウトカム〕の3重の組に関してセーフガード機能スペースを定義しておく。その関係は次のように表示しうる。すなわち，

$$F\ (T \times A)\ =\ \{\ F_{ij1},\ F_{ij2},\ \cdots\cdots,\ F_{ijk}\ \}$$

ここで，iの資産，jの脅威についてのkのセーフガード機能のそれぞれは，次に示されるセーフガード・サブ機能集合によって遂行される。すなわち，

$$F_{ijk} <=> U_m\ (f_{ijkm})$$

ここで，＜＝＞の記号は，" is defined to be " を意味し，Umは，mの範囲の結合（union）を指している。

それぞれのセーフガード・サブファンクションは，パフォーマンスの適切さを決定づけるエレメントからなっており，次のように表示できる。

$$f_{ijkm}\ =\ \Sigma n\ (e_{ijkmn})$$

各エレメントは，さらにエレメントの完全さを決定づける属性（attributes）たる α_{ijkmnp} および エレメントとその属性についての付加的情報たる λ_{ijkmnp} からなっており，次のように表示される。

$$e_{ijkmn}\ =\ \Sigma_p\ (\alpha_{ijkmnp},\ \lambda_{ijkmnp})$$

エレメントと属性は，特定のセーフガードないしは対応手段のことである。

図3　アウトカム可能性マトリックス

	権限のないアクセス／使　用	修　正　／不正変更	損　害　／破　壊	ディスクロージャ	盗　　難	使用拒否
自然ハザード施設	0	1	1	0	0	1
自然ハザードハードウェア	0	1	1	0	0	1
自然ハザードソフトウェア	0	1	1	0	0	1
自然ハザードドキュメント／ディスプレイ	0	1	1	0	0	1
オンサイト・ヒューマン施設	1	1	1	1	1	1
オンサイト・ヒューマンハードウェア	1	1	1	1	1	1
オンサイト・ヒューマンソフトウェア	1	1	1	1	1	1
オンサイト・ヒューマンドキュメント／ディスプレイ	1	1	1	1	1	1

さて，アウトカム可能性マトリックス（outcome possibility matrics）は，〔脅威，資産〕ペアとアウトカム集合とに関係している。そしてアウトカム可能性マトリックスをファジー・マトリックス（fuzzy matrics）として考えることができる。当該マトリックスにおける値は，特定の〔脅威，資産〕ペアの相互作用の結果として，問題のアウトカムが生じうる可能性の度合いを表している。そのような値については，かなり複雑な分析から得られるし，また，単純に当該アウトカムが，潜在的な〔脅威，資産〕の相互作用について，可能か（可能性の度合い1），可能でない（可能性の度合い0）のいずれかとして仮定することができる。多くのアプリケーションについていえば，より単純なケースのほうが，適切な場合がある。図3は，この論文において用いるコンピュータ・セキュリティのアプリケーション事例でのアウトカム可能性マトリックスを示している。

各々の〔脅威，資産，セーフガード機能〕の3重の組についてのアウトカムは，さまざまな強度で発生しうる。アウトカムの強度は，セーフガード機能の相対的な弱さ（セーフガード機能のパフォーマンス尺度）と脅威の相対的強さとの関数である。動態的な脅威が別々に分析されない場合には，脅威の強さ（strength）は，等しく1であると仮定される。アウトカムの強度は，アウトカム強度のあいまい集合におけるメンバーシップの度合いとして表示されるが，インパクトおよびロス・イクスポジュアについて非貨幣的な尺度で用いられる言語的ディスクリプタに転換しうる。

さらに，アウトカムがなんらかの脅威－資産－脆弱性の相互作用から生じた場合，特定の強度のアウトカムが対象組織にもたらす影響を測定するために，インパクト集合を定義するのである。インパクトは対の値で表示されるが，財務的なタームで測定されるインパクトの構成要素にはマネタリ・タームで，また別の仕方で測定されるのがよいインパクトの構成要素についてはノンマネタリないし言語的なタームで表示される。インパクト集合は次のように示される。

$$I_{ijkq} = \{ I(M)_{ijkq},\ I(L)_{ijkq} \}$$

上の式は，〔脅威，資産，セーフガード機能，アウトカム〕の4重の組の結果（consequences）を示している。

リスク，すなわち潜在的なロス・イクスポジュアは，次の3つの構成要素（components）の相互作用から生じる：脅威構成要素（セーフガード機能の脆弱性につけいることにより特定のアウトカムを生み出す脅威エージェントの相対的，潜在的強さを測る）；脆弱性構成要素（セーフガード機能の相対的，潜在的弱さを測る）；結果（consequence）構成要素（特定のアウトカムの相対的，潜在的コストを測る）。対のロス・イクスポジュアは，各々の〔脅威，資産，セーフガード機能，アウトカム〕という4重の組について与えられ，次のように表示される。

$$R_{ijkq} = \{ R(M)_{ijkq},\ R(L)_{ijkq} \}$$

上式について

$$R(M)_{ijkq} = f(V_{ijk}, S_{ijk}, O_{ijkq}, I(M)_{ijkq})$$
$$R(L)_{ijkq} = f(V_{ijk}, S_{ijk}, O_{ijkq}, I(L)_{ijkq})$$

ここで，V_{ijk}とは，i番目の資産とj番目の脅威との相互作用についてのk番目のセーフガード機能の相対的弱さの尺度をさす；S_{ijk}は，i番目の資産についてのk番目のセーフガード機能に対するj番目の脅威の相対的強さの尺度である；O_{ijkq}は，（通常）1か0で，i番目の資産，j番目の脅威，k番目のセーフガード機能の相互作用に関し，q番目のアウトカムが生じうることをしめしている；そして，$I(M)_{ijkq}$と$I(L)_{ijkq}$は，〔脅威，資産，セーフガード機能，アウトカム〕という4重の組についての貨幣的，非貨幣的なインパクトの尺度であるとされている。

リスクのペアは，望むレベルのところまで集合されうる。集合すればするほど，おおざっぱな指摘となり，上級経営者にボトムラインを与えるが，集合の程度が低くければ，セキュリティおよび全体のリスクにたいする姿勢を改善するのが仕事である人に詳細な，特有の情報を提供することになる。一般に，

より多く集合（aggregation）すれば，情報を失い，重要な結果（results）を不明瞭にする傾向がある。そこで，さほど集合しないほうが，たいていの目的に合致しそうである。

B　情報収集のフェーズ

情報収集のフェーズは，相互作用を知るための質問表（automated，interactive questionaires）を手段として，ＬＡＶＡが操作されるためのデータを必要としている。集められる情報は，組織の使命（mission），資産および資産に対する潜在的脅威，組織環境，セーフガード（ないしコントロール）・システム，そして，組織の価値・選好構造である。

次の質問表との相互作用は，チーム環境によりなされるのである。すなわち，「セーフガード脆弱性質問表」は，マネジメント，業務担当者，セキュリティ担当者によって実行される；「動態的脅威質問表」は，適格な情報へのアクセスをする人々の集合により行われる；「インパクト質問表」は，ハイレベルのマネジメントおよび業務担当者からなるチームにより遂行される。

さて，対象組織の使命は，セーフガード・システムが資産の十分な保護を達成するのに必要なセキュリティ・レベルを決定することである。これは，本質的に，組織の使命のセンシティビティ，クリティカリティ，インテグリティ要請についての評価なのである。

組織環境には，多くの要因が寄与している。分析に関して最も影響を有する要因は，地理的なロケーション，コミュニティ環境，物理的環境，そして手続き環境である。地理的なロケーションは，地震，火山噴火，暴風，旋風，増水した河川や決壊したダムからの洪水などのような潰滅的な自然事象の潜在性を決定する；また，人口密集地，主たる交通センター，スペアパーツの準備場所等への近接度合いを示している。コミュニティ環境は，組織がおかれている社会的，政治的，知的風土を表しており，そして組織犯罪，政治的対立（dissent），大学，社会的・道義的調停者の存在といった要因を含んでいる。物理的環境は，土地，フェンス，建物といった組織の構内を表している。手続き環

境は，組織のマネジメントにより説明される，考え方，方針，手順を列挙している。

組織の価値構造は，サクセスフル・アタックが組織に対してどのような影響をもたらすかを決定づけるのである。もしも，組織の唯一の計算力が単一のコンピュータであるとし，組織が日常の事業の遂行に当該コンピュータに著しく依存しているとすれば，マシンの破壊は，組織に潰滅的な影響をもたらすことになろう。他方，組織がいくつかの強力なスーパーコンピュータとならんで多くのこの程度のコンピュータを有しており，末端部分でx型コンピュータの一つに依存しているとすれば，そうしたコンピュータの一つの破壊は，愉快なことではないが，潰滅的でないばかりか，取るに足りない迷惑なことにすぎないであろう。

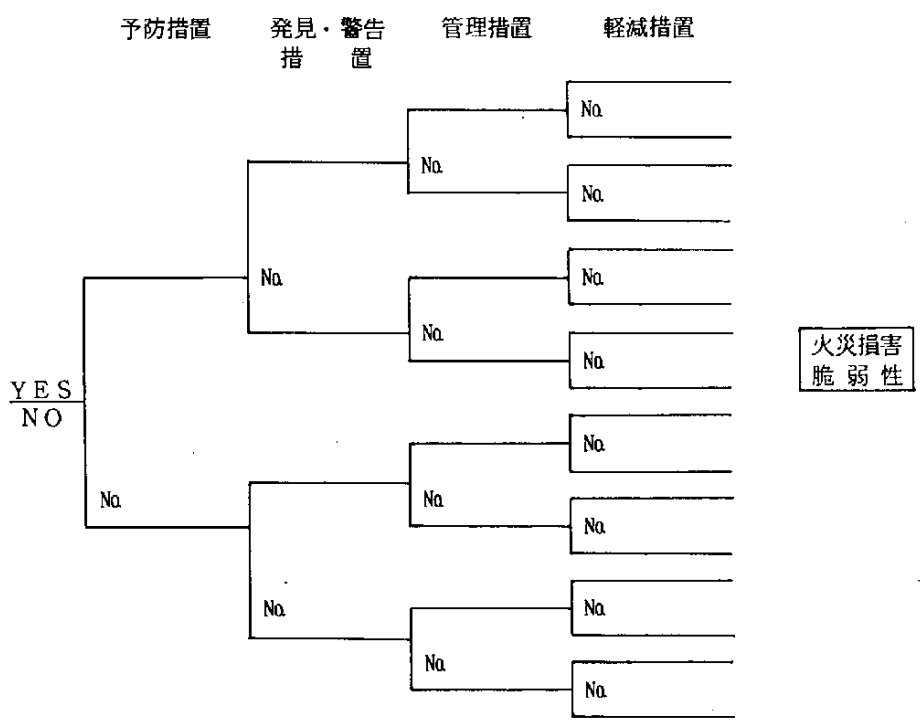
C　分析のフェーズ

分析のフェーズは，潜在的に次の3つの別々の分析からなっている：2つの必要とされる分析と一つのオプショナルな分析である。最初の分析は，システムの脆弱性を評価するため，対象組織のセーフガード・システムについて集められた情報を用いる。オプショナルな第2の分析は，必要とされる場合に，現在の脅威の強さを評価するために，脅威の動態的な構成要素について集められた情報を使用する。第3の分析は，サクセスフル・アタックの潜在的結果を評価するために，対象組織の価値，選好，考え方について収集された情報を用いる。これらの分析から，［脅威，資産，セーフガード機能，アウトカム］という4重の組のそれぞれについて，ロス・イクスポジュアの（貨幣的，非貨幣的）ペアがえられるのである。

1. 脆弱性の分析からは，セーフガード機能の有効性のあいまい集合におけるサブファンクションのメンバーシップの度合いを表す各セーフガード・サブファンクションについて価値が計算される；そのファジィ・コンプリメントはサブファンクションの脆弱性（ないし，相対的な弱さ）を表わしている。

各セーフガード機能は，あいまいの木（ファジィ・ツリー）として表わされ，その小枝（ブランチ）はこの特定の機能のサブファンクションを意味している。たとえば，セーフガード機能が"火災損害コントロール"であれば，的確なサブファンクションは"火災予防コントロール"，"火災発見コントロール"，"火災緊急時対応管理措置"，"火災損害軽減コントロール"ということになる。この例は，図4に描かれている。注意すべきは，このツリーが確率的な木ではないということである。結果的に小枝に表れる価値は，確率ではなく，サブファンクション・コントロールのパフォーマンスのあいまい集合におけるメンバーシップの度合いなのである。セーフガード機能の目的を達成するセーフガードの望ましい集合は，対象となる場にあるセーフガードの存在および質についての特定の情報を引き出してくれる，質問表（automated, interactive questionaires）としてモデル化される。

図4　火災損害コントロール・セーフガード機能についての「あいまいの木」



セーフガード・システムの質問表に点数をつけるにあたり，各々のセーフガード・エレメントは，１に等しい最大の潜在的脆弱性の度合いを有している。もしも存在しているだけで十分なパフォーマンスを意味するようなエレメントであれば，そのエレメントが存在する場合，脆弱性の度合いは０であり，存在しない場合には，１となる。そして，そのようなエレメントは属性を有していない。もしもエレメントが属性を有していれば，エレメント質問により意図されているセーフガードが存在するばかりでなく，セーフガードがエレメントの質およびパフォーマンスの妥当性を決定づける基準に関係していることを意味することになる。パフォーマンス基準の各々（属性）は，等しく重要であり，１／ｐという最大の脆弱性の値を有しており，その場合，ｐは考慮下にある特定のエレメントについての属性数である。この場合，エレメントの脆弱性値は，次式であたえられる。すなわち，

$$v(e_{ijkmn}) = \Sigma_p v(\alpha_{ijkmnp})$$

$v(\alpha_{ijkmnp})$は，質問で表された基準が満たされた場合には０，満たされない場合には１／Ｐのいずれかである。

セーフガード・エレメント（および関連属性）は，ひとつ以上のセーフガード・サブファンクションに寄与しうるのである。そして，どのセーフガード・サブファンクションがいずれのエレメントにより影響されるのか，常に情報を集めるべく，関係のあるデータベースをもちいるし，セーフガード質問表が完全に応えられた後に，サブファンクションの表の作成にあたり，データベースが補助的に用いられる。各サブファンクションについての脆弱性度は，サブファンクションに寄与するエレメントすべてに関する脆弱性値の合計であり，１ないし次式に標準化されるのである。

$$v_{ijkm} = 1/n\left[\Sigma_n v(e_{ijkmn})\right]$$

この場合，ｎはｍ番目のサブファンクションに寄与するセーフガード・エレメント数である。

脆弱性分析において仮定しているのは，脅威が静態的（動態的構成要素は０）であり，すべてのアタックが等しく同様に発生し，結果（consequences）が極端であるということである。その結果発生する脆弱性の尺度は，後で一層現実的なものにすることができる……リスク尺度が計算される際，動態的脅威および"実際の"結果（consequence）の尺度を含めることにより，減少ないし増加されうるのである。ＬＡＶＡは，脆弱性尺度 V_i を"完全なセーフガード機能の有効性" S_i（ないし，$V_i = 1 - S_i$，ここで V_i も S_i も０と１の間にある）のあいまい集合のメンバーシップ関数のコンプリメントとして定義している。

2. 動態的脅威分析は，対象システムが可変的脅威に極端なほど敏感である場合に，また対象組織が分析上必要とされる情報の種類にアクセスする場合に，遂行される。

動態的脅威が考慮にいれるのは，起こりうる脅威エージェントとその潜在的アタックの目標である。脅威のマグニチュードは，アタックのターゲットに関する様々な脅威エージェントの動機，能力，機会から決定される。

様々な目標を有している脅威エージェントの広範な範疇がある。たとえば，脅威エージェントの可能な範疇について，次のとおりである：

a) 情報収集者（たとえば，スパイ，敵の情報機関）

b) テロリスト

c) 反"Ｘ"ラディカルスないし過激論者（この場合Ｘは何でもよい）

d) 組織犯罪の代表

e) その他の犯罪者（悪意のない犯罪者やたちの悪いいたずら者）

f) 部内者（従業員，コントラクターなど）

g) アクセスする部外者

h) Mother Nature

これらの範疇にいる脅威エージェントたちは，異なった理由で行動するし，したがって，動機，能力，機会の点で大幅に違っている。同様に，アタックの目標も異なっている。すべての目標範疇は脅威エージェントのすべての範疇に

より利用される。可能な目標範疇は次のとおりである：

1) 情報／資料収集（たとえば，スパイ網）

2) サボタージュ

3) 窃盗，横領，詐欺行為

4) 損害ないし破壊

5) 恐喝

6) 事業なり任務の崩壊

7) 知的挑戦の打破

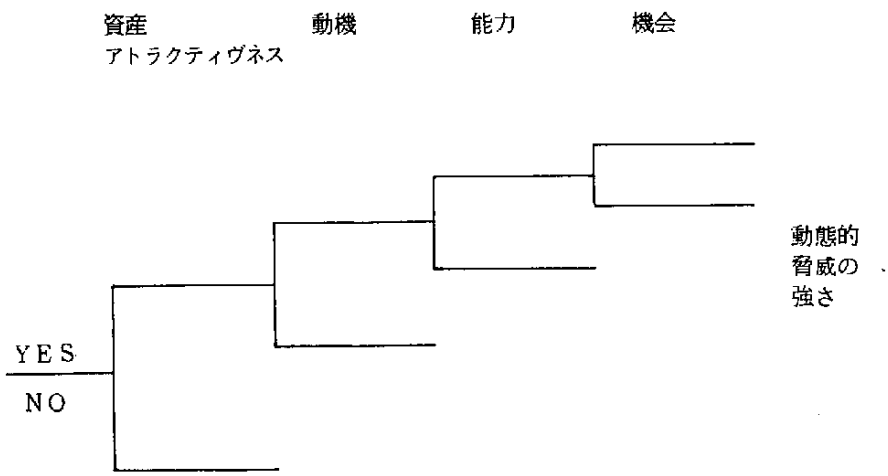
明らかに範疇の一つ以上が単独のアタック目標とされようし，単独のアタックは，脅威エージェントの一つ以上の範疇によって行われよう。

脅威の構成要素は，資産，相応するセーフガード機能，可能なアウトカム集合のスペクトルに関して，動機，機会，能力の点で確認しうる脅威エージェントの相対的な強さを測定するのである。ここで「動機」とは，脅威エージェントがアタックのためにどの程度の努力を費やすか，彼の資源のどの部分をついやす意欲があるか，また，アタックをかけるのにどれだけ献身的か，についての尺度である。「能力」とは，脅威エージェントが処分しうる知識（訓練），情報（情報機関），資金，スキル，設備，武装，人員，といった資源の尺度である。「機会」は，脅威エージェントがアタックのためにどの程度容易に接近しうるかの尺度である。機会は，潜在的なサイトの脆弱性とは別であり，異なっている。脅威エージェントの範疇とアタック目標の可能な範疇とを考慮することにより，脅威構成要素の動態的部分を評価するアプローチは，脆弱性分析と結果分析双方に用いられるアプローチと平行している。潜在的なシナリオは，暗黙のうちに，脆弱性分析における脅威－資産のペアとセーフガード機能との関係として，脅威の評価における資産と脅威エレメント（動機，能力，機会）との間の関係としてモデル化されている。同様に，アタック目標も，暗黙のうちに，動態的脅威尺度の能力構成要素においてモデル化されており，結果（consequence）分析に用いられるアウトカムと近似的に等価である。

相互作用を見る質問表は，特定の脅威グループの，動態的脅威への寄与因を

モデル化している。その強さの度合いは，特定の〔脅威，資産，セーフガード機能，アウトカム〕という4重の組と関係して，動機，能力，機会に基づき各グループについて計算されるのである。

図5　動態的脅威についてのアセスメント構造



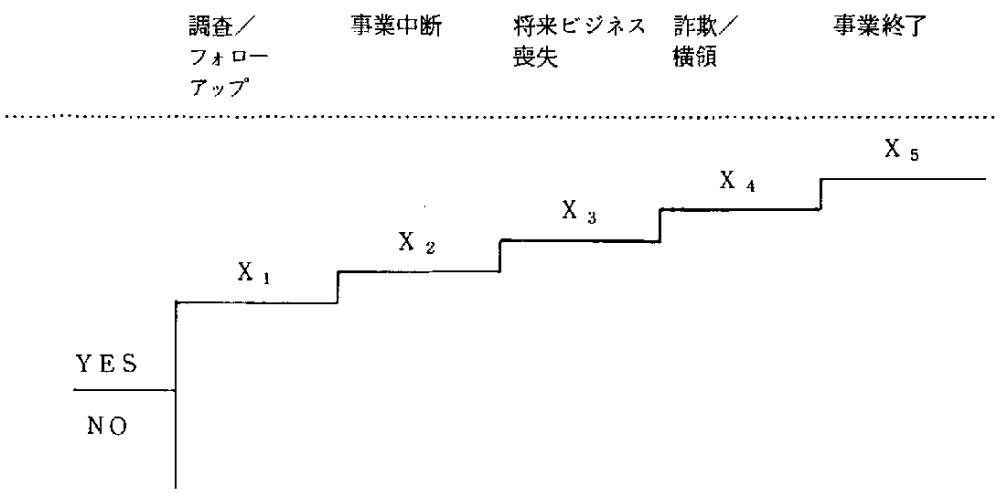
3. 結果（consequence）ないしインパクトの評価は，ＬＡＶＡにおける第3の分析である。この分析目的はサクセスフル・アタックのアウトカムが対象組織に及ぼす影響を決定することである。

結果（consequence）（もしくはインパクト）の構成要素は，セーフガード機能の脆弱性にうまく付け入った（貨幣的，非貨幣的）脅威の潜在的コストを測定する。アウトカム強度のメトリックは，セーフガード機能の相対的弱さと動態的脅威の相対的強さについての先程の2つの分析結果を結合することから得られる。

ＬＡＶＡの結果（consequence）の尺度は，貨幣的・非貨幣的デスクリプタのペアとして与えられる：貨幣的デスクリプタである$I(M)_{ijkq}$は，結果（consequence）が貨幣コストで与えられうる場合に用いられ，非貨幣的デスクリプ

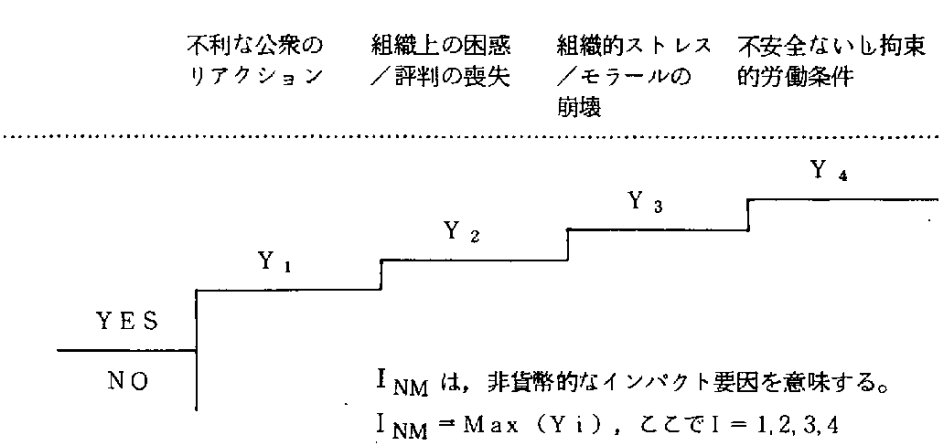
タである$I(L)_{ijkq}$は，結果が（取り返しのつかない評判の喪失といった言語的な尺度である"潰滅的"のような）無形のコストでのみ与えられうる場合に用いられる。そして結果（consequence）の値は，別のクエスチョネアから得られるのである。図6と7は，貨幣的・非貨幣的結果ツリー構造を示している。

図6　貨幣的結果の木



ここでI_Mを貨幣的インパクト要因とすれば，$I_M = X_1 + X_2 + X_3 + X_4 + X_5$と表示される。

図7　非貨幣的結果の木



貨幣的な結果の値は，調査・フォローアップ，事業中断，将来の事業損失，詐欺もしくは横領，事業終了のコストの合計として生じる。これらの寄与因は，各々，次のような特定のコストについての質問から計算される；懲戒ないし法廷訴訟のコスト；喪失時間，臨時業務（interim operation），全額取り替え（full replacement），修復・修繕にかかわるコスト；従業員の配置転換・訓練のためのコスト；損害・破壊，廃棄，詐欺ないし横領からの直接損失，等である。

非貨幣的な結果の値は，公衆の批判的反応のコスト，組織的なモラルの崩壊／喪失のコスト，評判の喪失のコスト，安全でないか拘束的な労働条件に関係する無形のコストから得られる価値の集合の極大値として表現される。

D　リスク・マネジメント問題の解決

組織のリスク態勢を改善するために適切な行動が取られていない場合には，最善の分析といえども何の役にも立たないのである。徹底したコスト／便益分析は，改善されるか，現存のセーフガード・システムに付け加えられるかするセーフガード集合の最適な選択のベースを提供する。分析は，提案されたアクションパスにどのくらいの費用がかかるか，それがどの程度損失イクスポジュアを減少させるかということを含むだけでなく，十分考え抜かれた実施計画およびその実施がモラル，訓練（再訓練），生産額（throughput）の減少等の点で組織に与える影響をも含むべきである。

4. 結　　語

各々の〔脅威，資産，セーフガード機能，アウトカム〕という4重の組に関するロス・イクスポジュアについてのＬＡＶＡの尺度は，セーフガード機能の相対的弱さ（脆弱性），脅威の相対的強さ，サクセスフル・アタックのアウトカムの結果（consequence）の関数である。

基本線となる脆弱性尺度は，次の仮定により求められる。即ち，背景にあ

る（静態的）脅威がただ一つのオペラブルな脅威なのである（相対的強さが1である）。脆弱性がセーフガード機能に存在している場合，サクセスフル・アタックのアウトカムの強度を評価するに際して，脆弱性の影響は，脅威分析に必要な情報がアクセシブルで，入手可能であれば，"実際の"脅威の尺度により増加されうるのである。

対象となるシステムは，システムのアプリケーション特有の重点の望ましさないしは回避指向についての，また対象システムの脅威環境についての，さらには対象組織の価値構造についての，固有のアプリオリ決定を含む質問表（interactive questionaires）としてモデル化されている。そしてイベント・ツリー型の構造は，上記分析の組織化のために用いられている。パフォーマンス尺度および関連の意志決定は定量的・定性的なタームで評価され，厳密な定量的分析がなしうる以上のインサイトをシステム・パフォーマンスに与えることになる。

ＬＡＶＡのアプローチは，技術的に健全，正確，相互作用的，確実であって，ポータブルである。その正確さは，特定のアプリケーションの開発者により与えられる徹底的かつ包括的な質問から得られる。自然言語での質問表（interactive conversational questionaire）は，率直であり，使用しやすい。モデルに組み込まれた専門的知識および厳密さは，モデルの論理構造とならんで，意志決定を単純化している。モデルの機能的構造は，はっきりと，どのセーフガードが欠けているかを指摘し，付け加えられるべきセーフガードの選択に理論的根拠を与えてくれる。ＬＡＶＡのソフトウェア・システムは，標準的なＩＢＭ－ＰＣソフトウェアに適用しうるがため，システムをポータブルとさせている。ＬＡＶＡのシステムは，相互作用的で，それ自体完備しているがため，この方法論および関連のソフトウェアを使用する組織は，外部コンサルタントのサービスを必要としないし，全体のセーフガード・システムにもう一つのセキュリティ層を加えることになるのである。

リスク分析関連海外参考文献

(1) Ardis , P.M. and R.M. Johnson, "Insurance and Fidelity Bonds", Computer Fraud & Security Bulletin, Vol.6 No.6, (April 1984), pp.1-12.

「保険とフィデリティ・ボンド」に関する論稿である。ＦＢＩの指摘にみる損失特徴から論じているが，(3)に示されているように，コンピュータ関連の金額が大である。それゆえ，コンピュータに起因する損失に備え保険が考慮されることになる。まず身元信用保険の何たるかを示し，一般にアメリカの銀行では，バンカーズ・ブランケット・ボンドといわれているスタンダード・フォーム２４が使われていることから，この点に論及し，さらに，ロイズ・オブ・ロンドンのエレクトロニック・コンピュータ犯罪保険に言及している。

コンピュータ関連のリスク保険の購入は，情報時代において，企業にとって専門的な困難な問題の一つであり，この点に固有の問題をスケッチした論文である。

(2) Berting, F.M., " Fundamentals of Computer Security ", submitted to Seventh International Conference of Women Engineers and Scientists, Washington, D.C., June 17-24, 1984.

「コンピュータ・セキュリティの基礎」と題する論文である。この中で，コンピュータ・システムに固有の脅威，リスク推定，コンピュータ保護手段が論じられている。脅威については，共通の脅威に加えて，最も危険な脅威として人（インサイダーとアウトサイダー）に強調点がおかれている。リスク推定の部分では，ＦＩＰＳ PUB 65，W．A．J．Bound and D．R．Ruth（リスク分析調査報告書　昭和５９年１２月において紹介），さらに(13)についても指摘して

いる。リスク分析の次には，重要なコンピュータ・プロテクション手段を論じている。

(3) Davies, D., " Insuring The Risks Of The Changing Technology : The State of The Insurance Art ", SECURICOM 1986, 4TH Worldwide Congress On Computer and Communications Security and Protection, pp.113-131, 1986, March 4-6, 1986, Paris, France.

「テクノロジーの変化のもたらすリスクの付保」についての論文である。コンピュータ・テクノロジーの発展の観点から保険の限界を論及。コンピュータ・リスクとしてコンピュータへの依存状態にかかわる問題状況（コンピュータ詐欺，第三者による詐欺，コンピュータ関連スパイ事件等を新しいリスクの範囲として示す），そしてケース・スタディ（その内に，1984年12月発生の世田谷ケーブル火災にも言及）として事例を紹介，次にコンピュータ犯罪に論及（USAでは，コンピュータ関連犯罪の平均損失が$500,000で，平均の銀行強盗は$3,500；平均コンピュータ・アシスティド横領額は$430,000で，コンピュータ支援なしの場合は$25,000である（FBI））。また，ATM利用の詐欺では，$450百万の損失があったそうである。そして，コンピュータ保険の限界を解説。保険者は完全な保険商品を市場化することはない。それというのも，顧客が望む免責なしの保険の保険料は禁止的な高さとなってしまうことであろうし，現在の保険技術の状態では完全商品からほど遠い。よって，何でも保険しうるものではないということから，われわれは出発すべきである。

たいていの企業では，コンピュータ関係の責任（DPM）と保険責任（財務担当役員）とは別個となっている。互いの活動なり使用言語すら理解されていないきらいがある。保険戦略も，伝統的なリスク・マネジメントの原理に基づかねばならないとして，リスク・マネジメントのプロセスに言及している。

(4) Guarro, Sergio B, " Livermore Risk Analysis Methodology : A Structured Decision Analytic Tool for Information Systems Risk Management ", Lawrence Livermore National Laboratory, prepared for submittal to Annual Meeting of the Society for Risk Analysis, Boston, Massachusetts, November 9-12, 1986.

(抄訳前掲)

(5) Hoffman, L. J. and Lucy M.Moran, " Societal Vulnerability to Computer System Failures ", Computers & Security, vol.5, no.3, Sept.1986, pp.211-217.

「コンピュータ・システム故障に対する社会的脆弱性」についての論文である。特に脆弱性について，2つの範疇を指摘している：〔1〕コンピュータ・システムの乱用，誤用ないしは，そのハードウェアなりソフトウェアの欠陥によるシステムそれ自体の脆弱性；〔2〕乱用，誤用，欠陥の結果による社会の脆弱性，である。そして，脆弱性の問題に対して3つのアプローチを検討している：(a)システム，システムへの脅威，重大な不利益な影響，損害軽減のための回復力要因を確認する社会的リスク分析；(b)システムへの専門的な団体からのフォーカス（Council of the Association for Computing Machinery（ACM）により是認されたアプローチ；(c)この問題へのインタディシプリナリな努力，である。

(6) Jenner, P., " Invisible Threats ", Systems International, October 1986, pp.107-108.

「目に見えぬ脅威」と題する論稿のとおり，新しい技術により，セキュリティ・リスクが増加していることを論じている。たとえば，大部分の組織なり個々人は高度の倫理基準を維持しているが，なかには競争相手より優位に立とうとして何とか機密を入手しようとする者もいる。プリント・アウトプットの悪用のほかに，コンピュータ・システム・ソフトウェアの改変に関する例を示し，現行の法律の修正の必要にも言及している。現在のテクノロジーは，多くの場合，専門的な泥棒の活動にとり，実行しやすく，発見されにくくさせてきた。重要なのは，お粗末なセキュリティは何等セキュリティがないより事態を悪化させうることを認識することである。

(7) Jordan, Helmuth, " Data Processing Insurance : A New Way To Fight Computer Crime ? ", International Computer Law Adviser, April 1987, pp.20-24.

「コンピュータ犯罪への対応のための新しい方法：データ処理保険」について論じられている。ある意味では，保険を付ければ付けるほど，われわれの支払う保険料も多くなる。そうした一般的な評価は，保険の領域では真実かもしれないが，コンピュータ犯罪と保険との関係ということになると，そのことも再検討する価値があるとして，クリミナル・コードとのかかわりから，コンピュータ犯罪に論及している。新しいコンピュータ領域では，概して，立法者側は高度のテクノロジーの発展に追い越されているからである。

ヨーロッパ，アメリカのコンピュータ犯罪による損害推定について，調査研究から数字をあげ，保険されるリスク，保険保護の範囲（特にドイツで開発された標準保険約款のうち保険の目的を定義しているパラグラフ１）について論じている。そして保険については，アングロ・サクソンおよび日本のアプローチが，契約者にとり価値ある救済策としている。

(8) Mosleh, A., Hilton, E.R. and Peter S.Browne, " Bayesian probabilistic risk analysis ", Performance Evaluation Review, Vol.13, no.1, (June 1985), pp.5-12.

(抄訳前掲)

(9) Orlandi, E., " Nolan's Stage Model and Computer Security ", submitted to 1986 International Carnahan Conference on Security Technology, Gothenburg, Sweden, August 12-14, 1986.

(抄訳前掲)

(10) Palmer, I., " Security audit & risk management ", System Security : Online Publication, Pinner, UK, 1985, pp.197-207.

「セキュリティ監査とリスク・マネジメント」に関する論稿である。とりわけ，コンピュータ設置に対する脅威のインパクト評価，年間損失推定額の評価技法に言及しているが，リスクの計算についての展開は，ドルとポンドの違いはあるが，FIPS PUB 65に同じである。

結論として，リスク分析は，情報資産，脅威，脆弱性の分析を通して，組織の情報資源に対するリスクを確認することであり，対抗策の評価・選択・取得・実行に際して優先順位を設定する事であるとしている。

(11) Reed, A., " Risk Management by Technology--a wayout of the impasse--latest developments in software devoted to risk

and disaster management ", submitted to 4th Worldwide Congress on Computer and Communications Security, Paris, France, March 4-6, 1986.

（抄訳前掲）

⑫ Saxby, Stephen, "COMPUTERS AND THE LAW : OLD STATUTES FOR NEW PROBLEMS?" SECURICOM 1986, 4th Worldwide Congress on Computer and Communications Security and Protection, pp.133-53, 1986, March 4-6, 1986, Paris, France.

「コンピュータと法律」と題する論文である。情報社会は，その根源まで法律を震撼させてきた。現存の法律が，産業革命のプリンシプルに基づいたものであり（法律上の規則は目に見える商品・サービスを規制すべく展開された）（１９世紀の経済環境に起源を持つ契約原理における財産権の概念がある），脱工業化世界の到来に備え用意されたものではなかったことが，今日では明瞭である。コンピュータ産業のドラマチックな成長および新しいテクノロジーの発展は，今や次のような実務上の問題を提起している：売り手はどのような責任を有しているのか？；ユーザはどの種の保護について交渉できるのか？；従業員は，事業機密の窃盗から予防されうるのか？；彼らが開発するプログラムに対して，従業員はどのような権利を有するのか？；いつソフトウェアをコピーすることが許されるのか？等に論及している。

そして，契約によりどのリスクが移転されうるか？　適用法における不確実性に直面するなかでビジネス・ユーザがその活動を確保するため何をなしうるか？，に言及している。

(13) Smith, S.T., Lim, J.J., Philips, J.R., Tisinger, R.M., Brown, D.C. and P.D. Fitzgerald, " LAVA:A Conceptual Framework for Automated Risk Analysis ", submitted to 1986 Annual Meeting of the Society for Risk Analysis, Boston, Massachusetts, November 9-12, 1986.

(抄訳前掲)

(14) Smith, S.T. and J.J. Lim, " Framework for Generating Expert Systems to Perform Computer Security Risk Analysis," submitted to First Annual Armed Forces Communications and Electronics Association Symposium and Exposition on Physical and Electronics Security, Philadelphia, August 19-21, 1985.

「コンピュータ・セキュリティ・リスク分析を遂行するためのエキスパート・システム生成のフレームワーク」と題する論文である。ロス・アラモスで，リスク分析を行うため，開発したエキスパート・システムのフレームワークを示している。エキスパートの知識をモデル化するコンピュータ・プログラムがエキスパート・システムであるが，ここでのリスク分析は，全体的な対象システムのセーフガードの有効性を決定し，セーフガード集合における脆弱性を確認し，セーフガードにとり対費用効果の改善を決定することによって，ターゲットに対する脆弱性，サクセスフルな脅威のインパクトを評価する。そして，自然ハザード，直接的な人間の行動，間接的な人間の行動という3つの脅威に対し，コンピュータ装置，ハードウェア，ソフトウェア，ドキュメント・ディスプレイという4つのターゲットを保護するセーフガードを考慮するのである。

(15) Smith, S.T. and J.J. Lim, " An Automated Procedure for Performing Computer Security Risk Analysis ", submitted to Sixth Annual ESARDA Symposium on Safeguards and Nuclear Material Management, Venice, Italy, May 14-18, 1984.

「コンピュータ・セキュリティ・リスク分析遂行のためのオートメイテッド・プロセデュア」と題する論文である。コンピュータ・セキュリティの有効性を評価するためのこのプロセデュアは，脆弱性やリスク分析への伝統的アプローチと異なっている。セキュリティ手段の適確性についてどの決定がなされうるのか，この点が得られる。相互連関的質問表としてモデル化され，イベント・ツリー集合が，質問表をリスク・アセスメントに結合させている。そして，定性的なスコアが，ターゲットとなる脆弱性について得られ，定性的なインパクトの尺度が，脅威ターゲット・ペアのスペクトラムに関して評価されることになる。次に，正確で有意義なリスク尺度を提供すべく，言語的記号マトリックスにより結合されるのである。こうして得られた定性的な尺度は，伝統的なリスク分析により生み出される定量的尺度より一段と有意味であるとしている。

(16) Stix, G., " Gauging Security Risks ", Computer Decisions, June 17, 1986, pp.78-82.

「セキュリティ・リスクの測定」というタイトルの論稿であるが，定性的・定量的なリスク分析のソフトウェアにどんな物があるのか，紹介している。たとえば，ソフトウェアの表には，定性的リスク分析について，ＧＲＡ／ＳＹＳ，Profile Analysis／Riskpac 等が，また定量的リスク分析に関しては，Basic Data Syst.／Risk Analysis Machine, Chesapeake Computer Grp. ／Risk--A, The Spence Grp.／Riskcalc等が示されている。

(17) Wong, K., " Computer Crime -- Risk Management and Computer Security ", Computers & Security, vol.4, no.4, (Dec., 1985), pp.287-295.

「コンピュータ犯罪—リスク・マネジメントとコンピュータ・セキュリティ」と題する論文である。コンピュータ犯罪に対する適切なリスク・マネジメントおよびコンピュータ・セキュリティにとっての出発点は，犯罪統計を分析することであるとして，イギリスにおいて実施したコンピュータ・フロードの９５ケース，その他のコンピュータ犯罪の約６０ケースに基づいて分析した論文である。

コンピュータ・フロードについては，ＵＫよりＵＳＡが，女性より男性が，スタッフ・部外者よりマネジャークラスが高額な犯罪の傾向がある。同論文では，コンピュータ犯罪の傾向を示した後，リスク分析に関し，特に事業中断損失の原因に言及。そして，コントロール・ディテクション，フロード・コントロール（その中には，コンピュータ犯罪保険も指摘されている）にも言及している。

付属資料

業種別セキュリティ対策水準の実態

業種別セキュリティ対策水準の実態

本資料では，当協会が実施した８８年版コンピュータ利用状況調査をもとに，「システムの安全対策，信頼性対策，合目的性」に関する項目を抽出し，現在，わが国で利用されているコンピュータ・システムのセキュリティ対策の実態を把握するために分析したものである。

分析結果は，わが国の現段階におけるセキュリティ対策レベルを明らかにするとともに業種別分析を試み，全産業とのレベルを比較することによって，各業種の現状を的確にした。

これにより，個別ユーザがセキュリティ対策を実施する上で，自社の位置付けを把握することが可能であり，より的確な対応をするための指標となる。

調査の概要

- 発　送　数　　3,４８１
- 回　収　数　　９５９（うち，オンラインユーザ　７９７）
- 回　収　率　　２７.５％

（注）ここでの集計対象は，オンラインユーザ７９７社である。）

質問項目ごとの業種別回答数

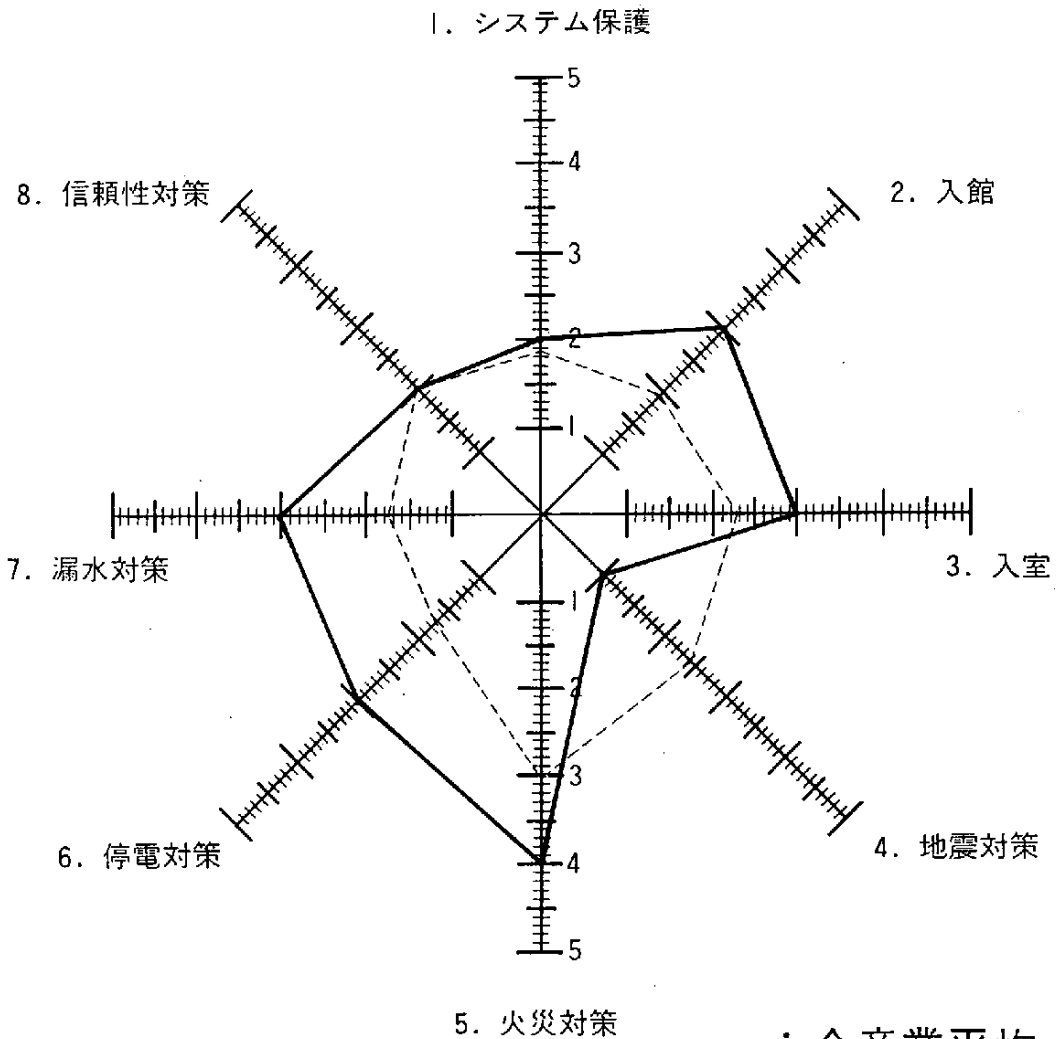
業種＼項目	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
農・林・漁・狩猟・水産養殖業	1	1	1	1	1	1	1	1
鉱業	—	—	—	—	—	—	—	—
建設業	24	26	25	25	25	26	25	25
食品製造業	22	23	23	23	23	23	23	23
繊維工業	17	17	17	17	17	17	17	16
紙・パルプ・紙加工品製造業	10	10	10	10	10	10	9	10
新聞業・出版業	4	5	4	5	5	5	5	5
印刷業．同関連産業	5	5	5	5	5	5	5	5
化学工業	43	42	42	42	43	42	41	39
石油製品製造業	4	4	4	4	4	4	4	4
窯業・土木製品製造業	9	9	9	9	9	9	8	9
鉄鋼業	12	10	11	11	12	12	12	11
非鉄金属製造業・金属製品製造業	29	28	29	28	30	30	30	29
一般機械器具製造業	29	29	28	29	29	29	29	28
電気機械器具製造業	61	60	61	62	62	62	62	61
輸送用機械器具製造業	31	32	30	31	32	32	32	32
精密機械器具製造業	15	15	15	15	15	15	14	15
その他の製造業	27	27	25	27	27	27	27	26
卸業・商社	71	68	68	69	70	69	69	63
小売業	37	36	36	38	38	38	37	34
金融業	79	82	81	81	81	81	78	79
証券業・商品取引業	3	4	5	4	5	5	5	4
生命保険業（含代理業・サービス業）	3	3	3	3	3	3	3	3
損害保険業（含代理業・サービス業）	3	3	3	3	3	3	3	3
不動産業	2	2	3	3	3	3	3	1
運輸・通信業	34	34	34	36	36	36	35	32
電力・ガス事業	9	8	8	9	9	9	8	9
放送業	11	11	11	11	11	11	11	10
広告・調査・情報提供サービス業	7	7	7	8	8	8	8	8
情報処理サービス業・ソフトウェア業	55	55	54	55	55	55	54	54
医療業	8	8	8	8	8	8	8	8
宗教法人	—	—	—	—	—	—	—	—
高校	2	2	2	2	2	2	2	2
大学	23	23	21	20	22	21	21	21
その他の教育機関	8	8	6	8	8	8	8	8
学術研究機関	2	2	2	2	2	2	2	2
法人団体・農協	22	23	23	21	22	22	20	22
その他のサービス業	8	8	8	8	8	8	8	8
政府	5	4	5	5	5	5	4	5
地方公共団体	40	40	42	41	42	43	39	41

質問項目ごとの実施レベル

項目＼レベル	1	2	3	4	5
1. システム保護	特に対策なし	パスワード制，権限規定明確・徹底化	パスワード制，権限規定明確・徹底化，コピー分散	重層パスワード制，権限規定明確・徹底化，コピー分散	重層パスワード制，権限規定明確・徹底化，コピー分散，暗号制
2. 入館	特に対策なし	受付者，来訪者名簿	受付者，来訪者名簿，バッヂ	受付者，来訪者名簿，バッヂand／or ＩＤカード	受付者，来訪者名簿，バッヂand／or ＩＤカード，監視装置
3. 入室	特に対策なし	受付者，来訪者名簿	受付者，来訪者名簿，バッヂ	受付者，来訪者名簿，バッヂand／or ＩＤカード	受付者，来訪者名簿，バッヂand／or ＩＤカード，監視装置
4. 地震対策	特になし	転倒防止装置	転倒防止装置，すべり止め	転倒防止装置，すべり止め，フリーアクセスフロア	転倒防止装置，すべり止め，フリーアクセスフロア，予報機関との連絡ネットワーク
5. 火災対策	特になし	消火器具	消火器具，消火装置	消火器具，消火装置，避難システム	消火器具，消火装置，避難システム，外部防災機関との連絡ネットワーク
6. 停電対策	特になし	バッテリ用意	バッテリ用意，自家発電装置	バッテリ用意，自家発電装置，定周波装置	バッテリ用意，自家発電装置，定周波装置，業者供給電源の２系統化
7. 漏水対策	特になし	防水カバー	防水カバー，マシン上ダクト	防水カバー，マシン上ダクト，感知装置	防水カバー，マシン上ダクト，感知装置，室の水密装置
8. 信頼性対策	自己診断システム保有	定期診断システム制	バックアップ体制	回線の二重化	ＣＰＵデュアルシステム等

各質問項目ごとの実施レベルは，ほとんど対策を実施していないもの（レベル１）から，現時点において最も厳重と思われるもの（レベル５）までを５段階に分類した。

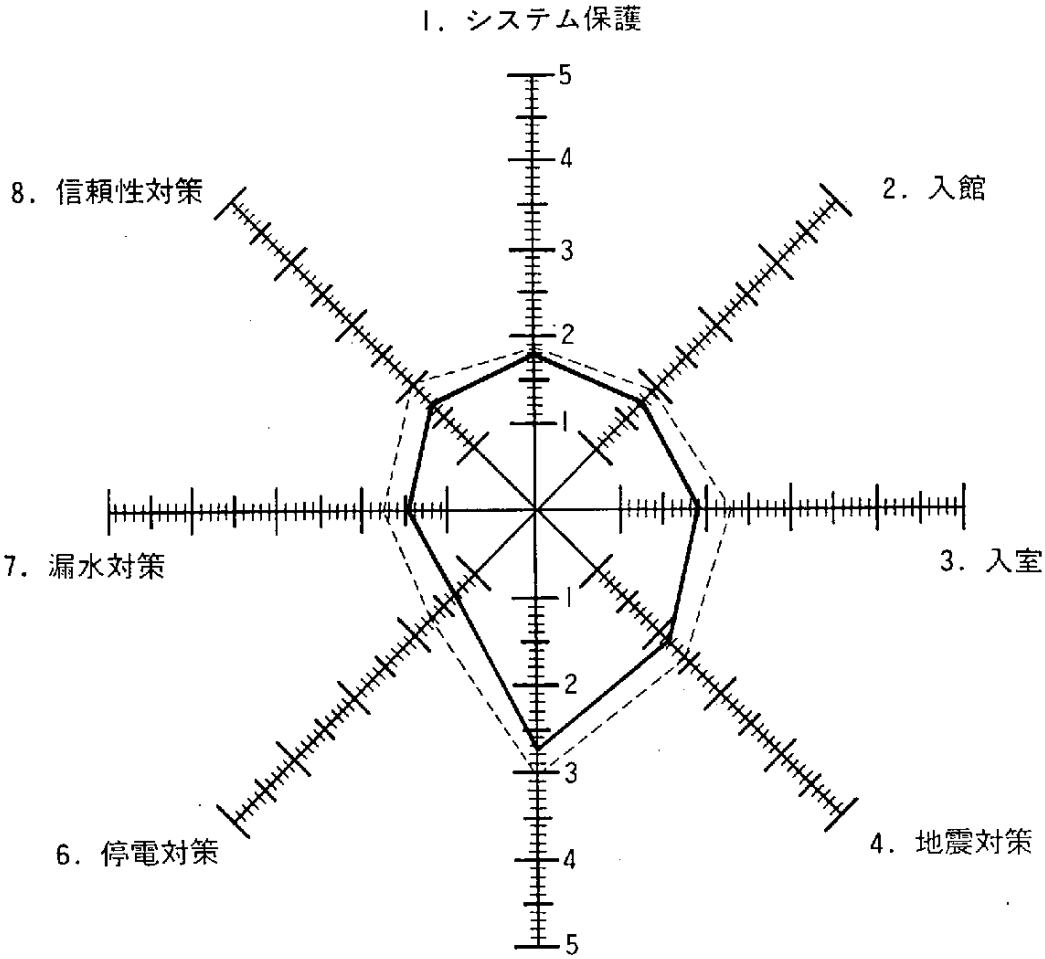
第一次産業計



---：全産業平均

	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
第一次産業計	2.00	3.00	3.00	1.00	4.00	3.00	3.00	2.00

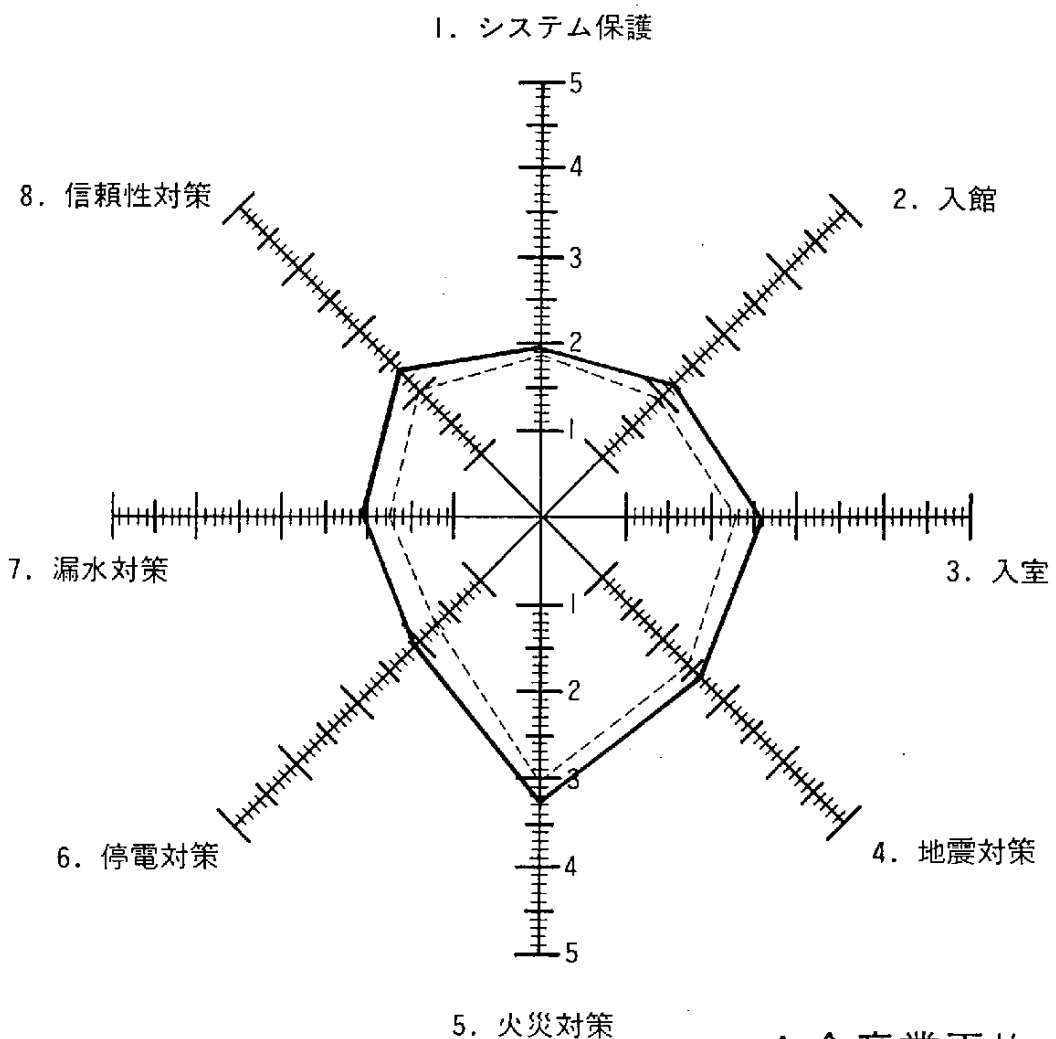
第二次産業計



---：全産業平均

	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
第二次産業計	1.79	1.73	1.90	2.18	2.73	1.32	1.48	1.70

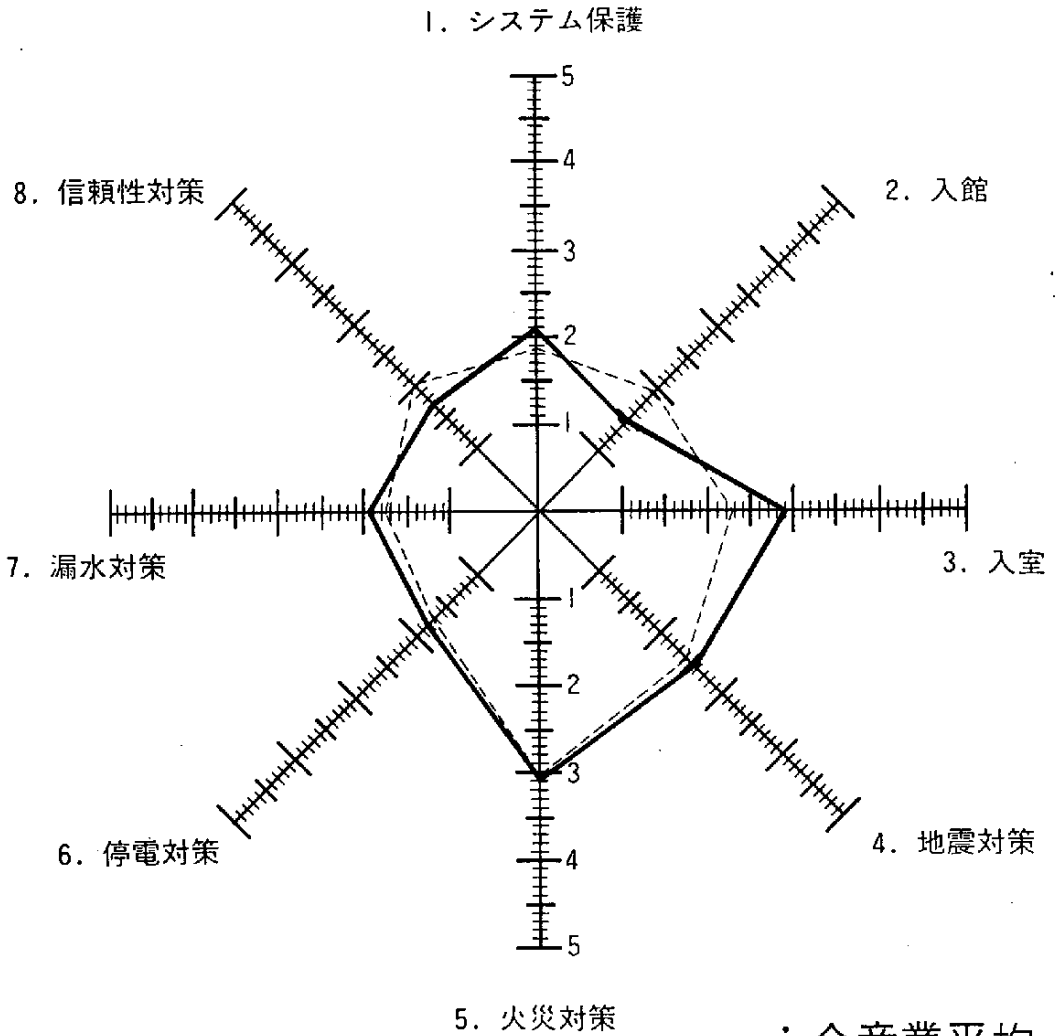
第三次産業計



---：全産業平均

	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
第三次産業計	1.94	2.17	2.55	2.61	3.25	2.08	2.03	2.33

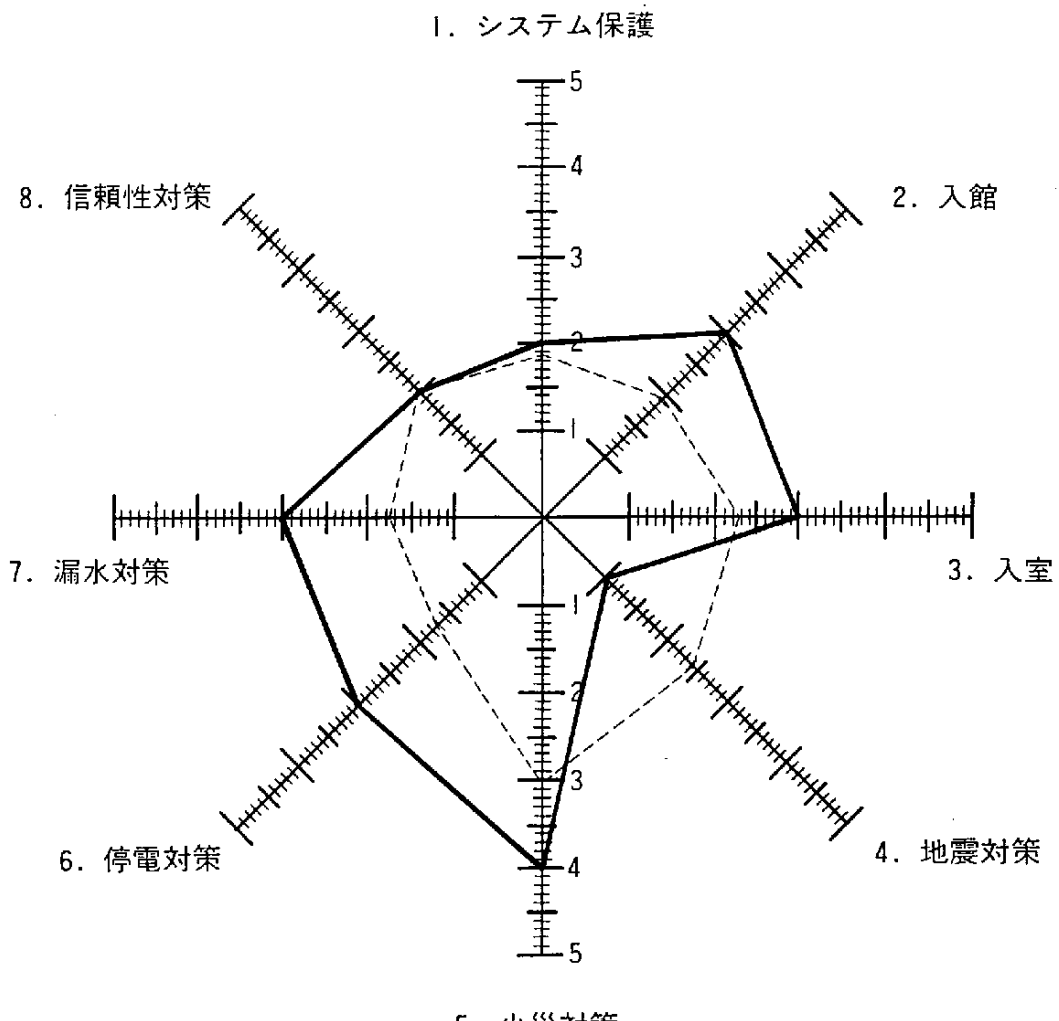
公　務　計



---：全産業平均

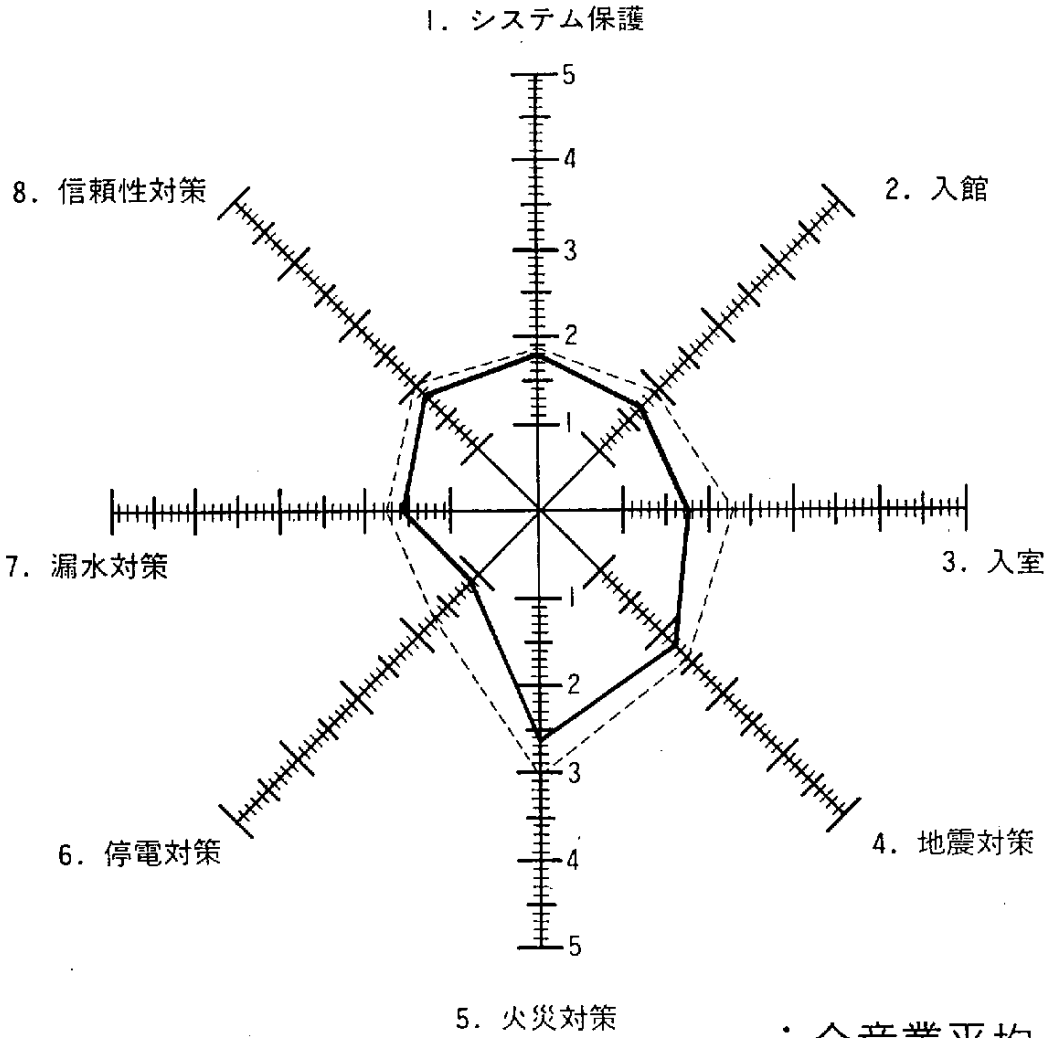
	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
公務計	2.07	1.48	2.87	2.54	3.09	1.81	1.91	1.70

農・林・漁・狩猟・水産養殖業



	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
農・林・漁・狩猟・水産養殖業	2.00	3.00	3.00	1.00	4.00	3.00	3.00	2.00

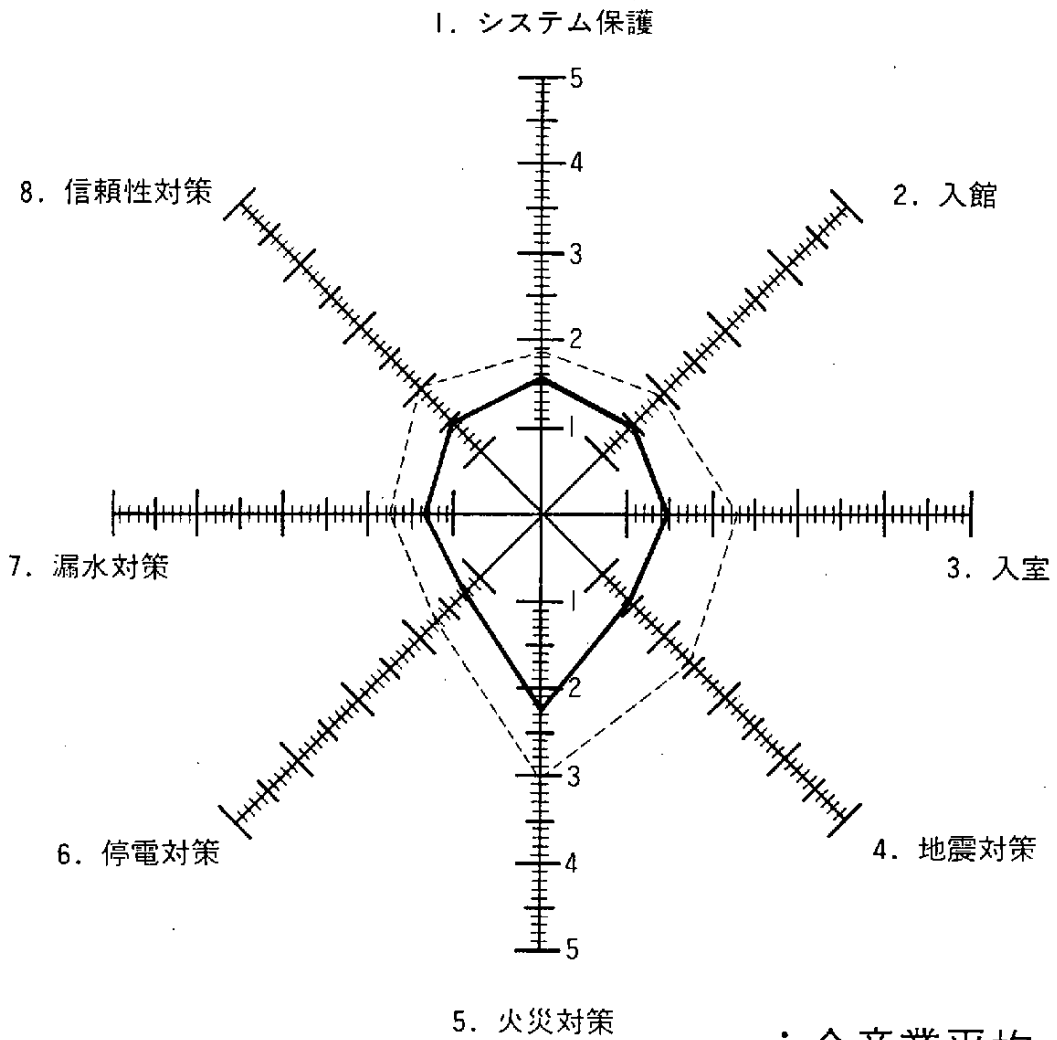
建　設　業



---：全産業平均

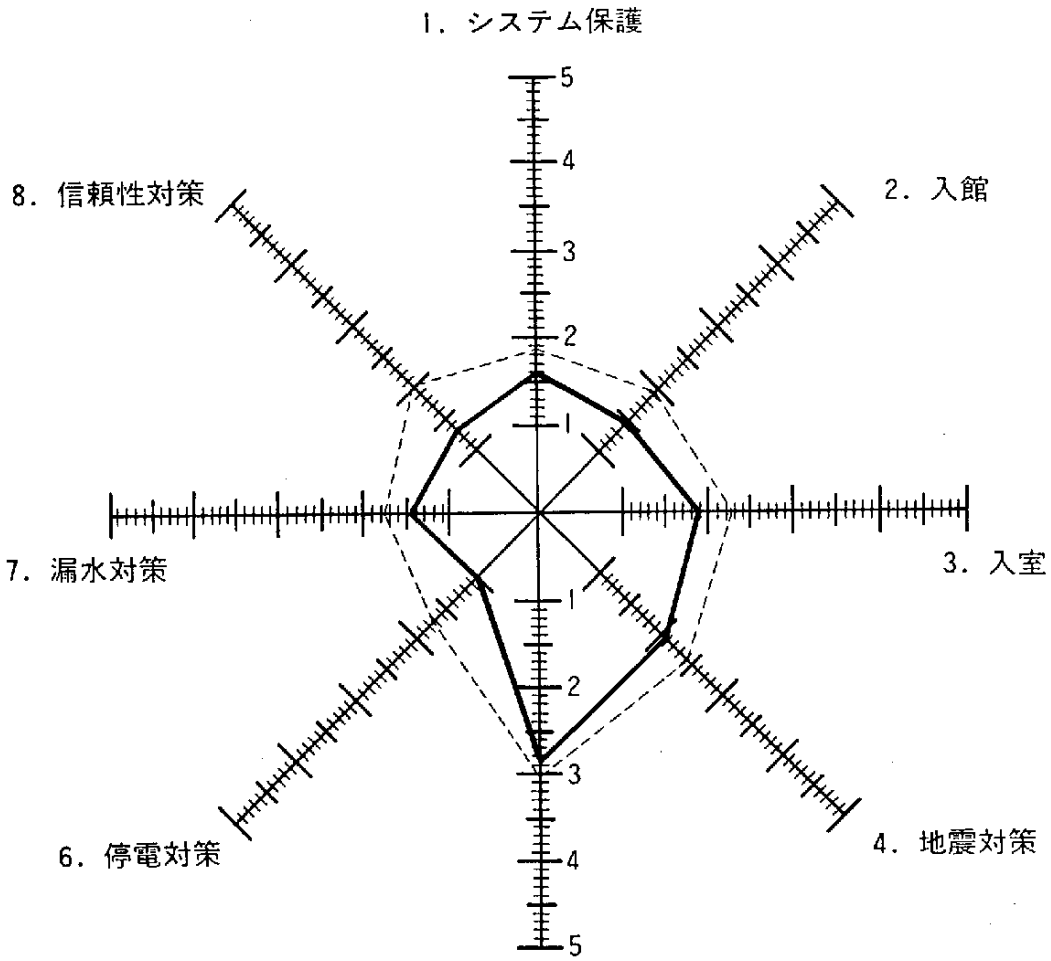
	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
建設業	1.79	1.69	1.72	2.20	2.64	1.12	1.56	1.84

食品製造業



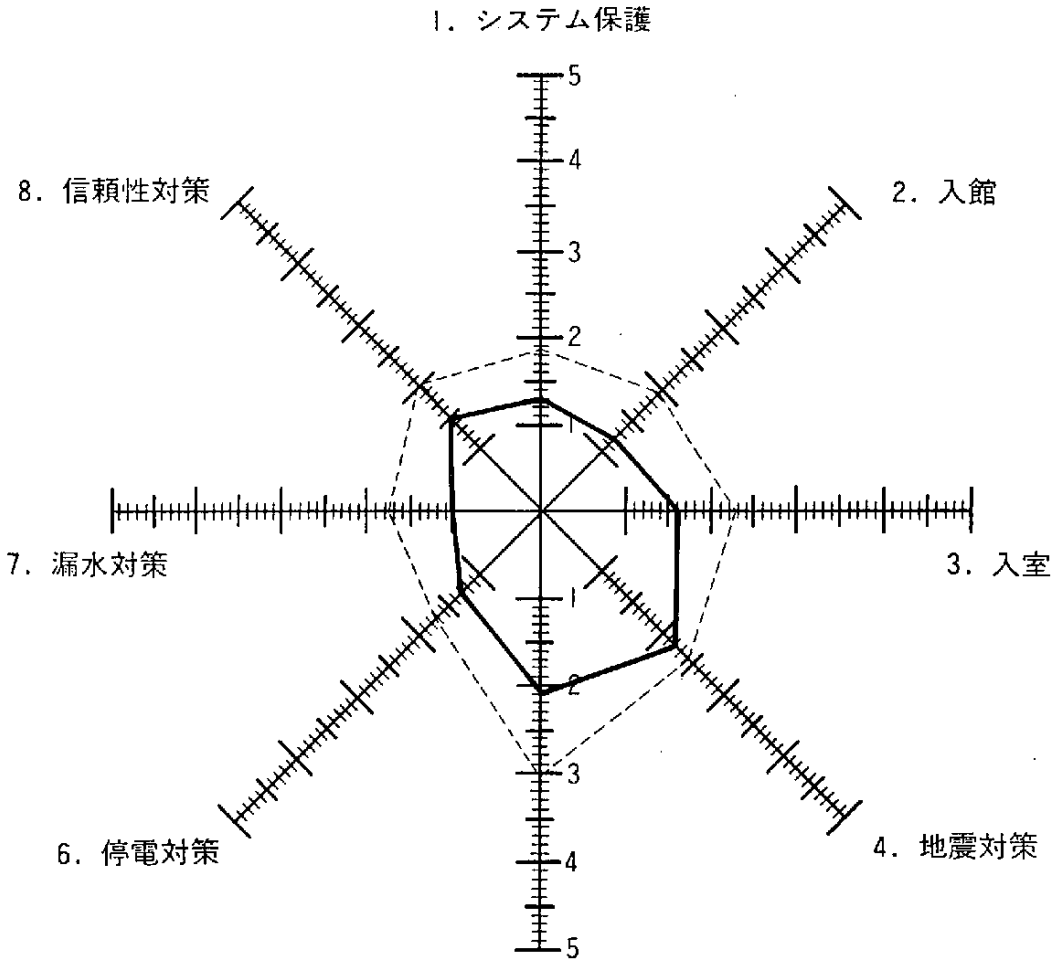
	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
食品製造業	1.55	1.43	1.48	1.43	2.26	1.26	1.35	1.48

繊維工業



	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
繊維工業	1.59	1.47	1.88	2.06	2.88	1.00	1.47	1.31

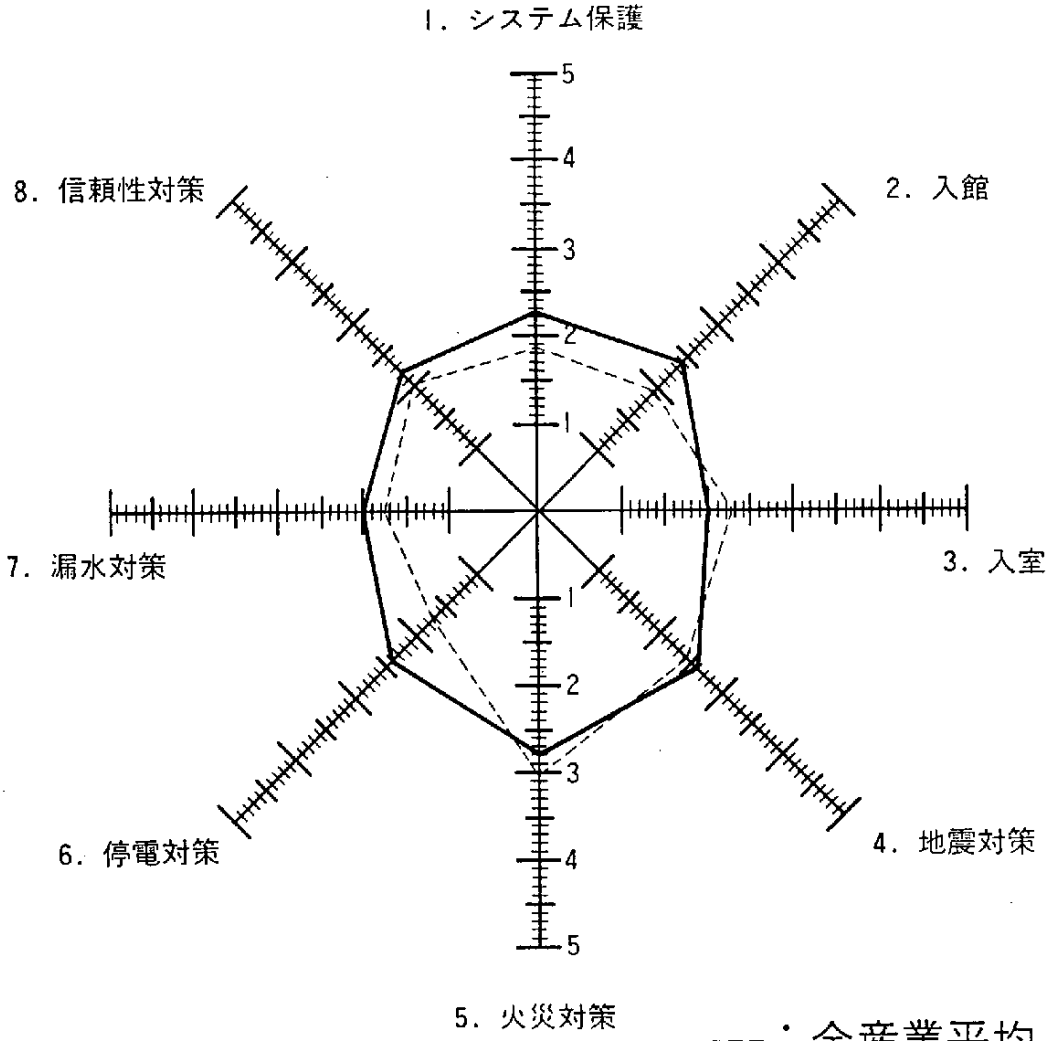
紙・パルプ・紙加工品製造業



---：全産業平均

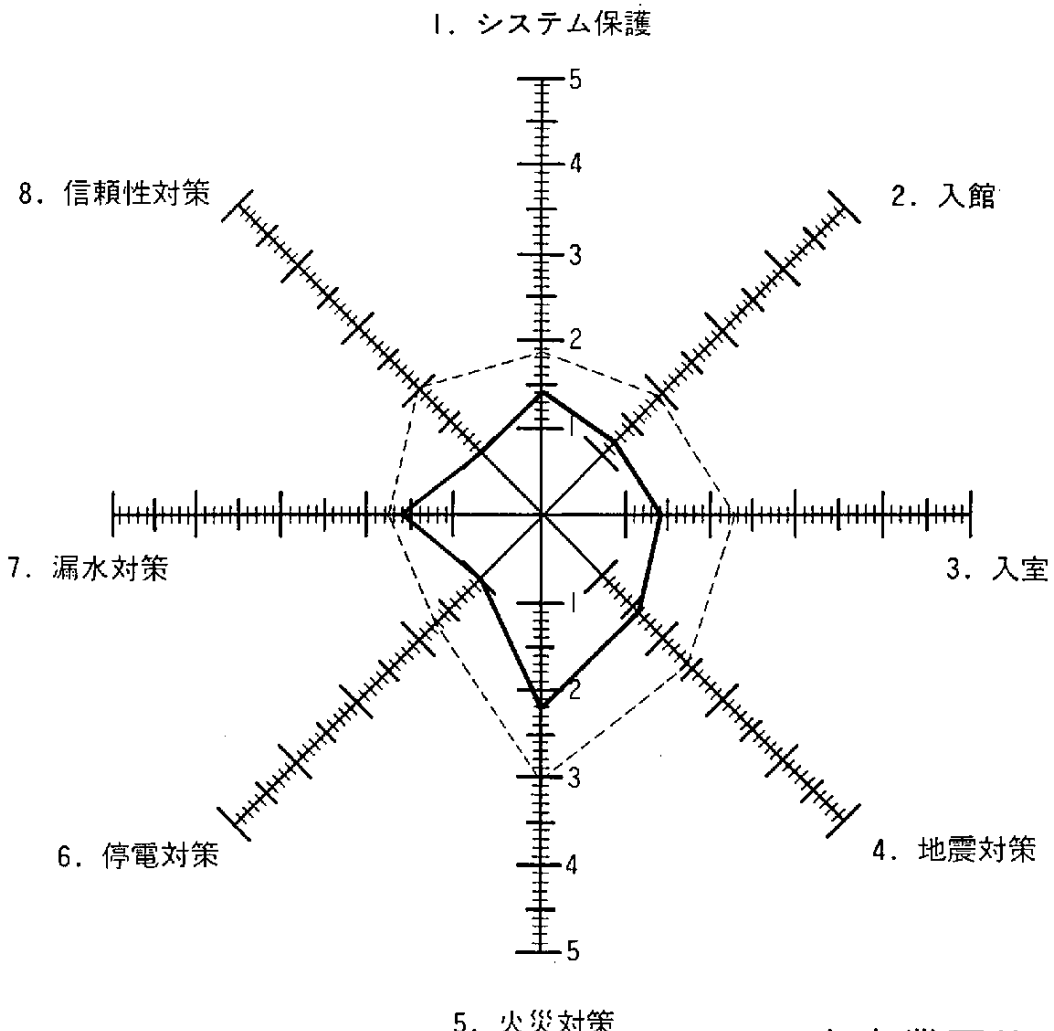
	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
紙・パルプ・紙加工品製造業	1.30	1.20	1.60	2.20	2.10	1.30	1.00	1.50

新聞業・出版業



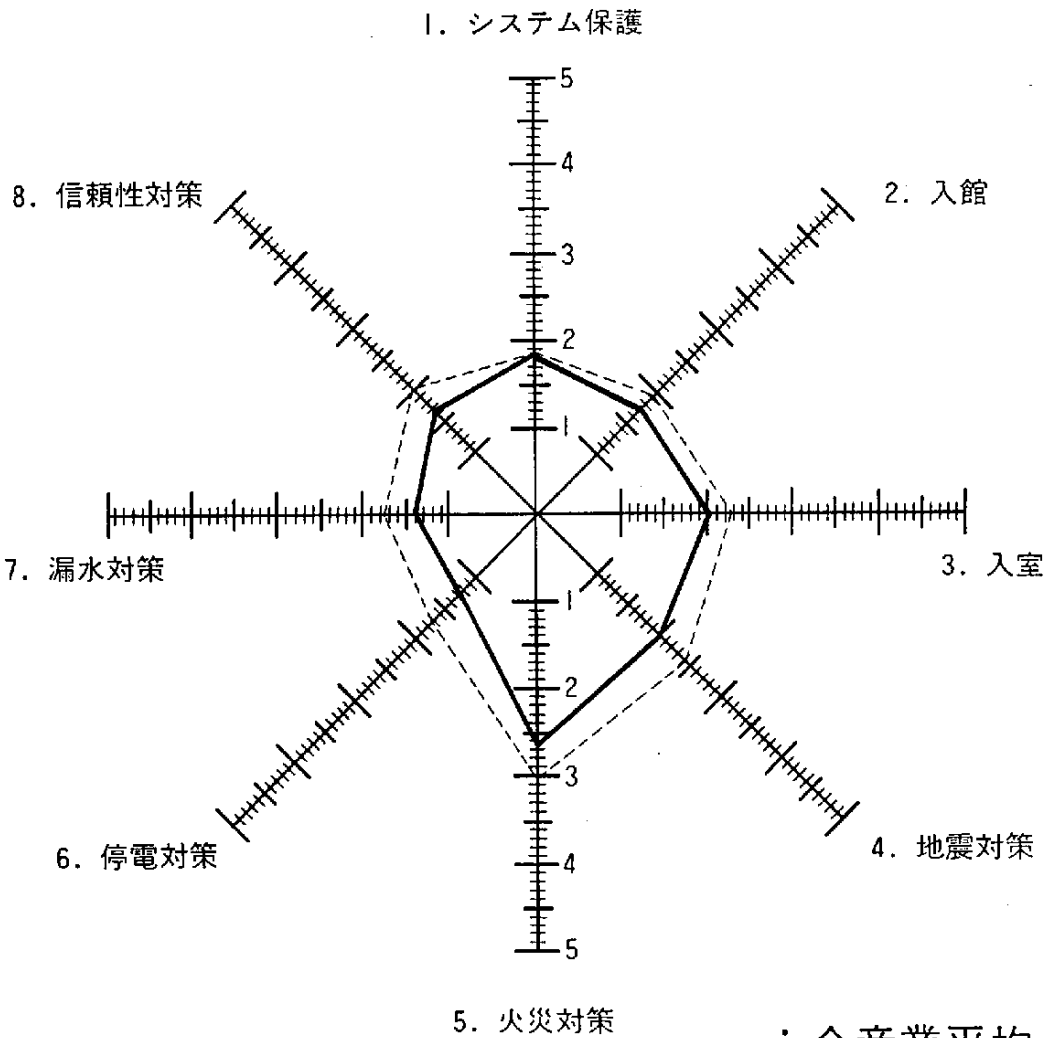
	1．システム保護	2．入館	3．入室	4．地盤対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
新聞業・出版業	2.25	2.40	2.00	2.60	2.80	2.40	2.00	2.20

印刷業・同関連産業



	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
印刷業・同関連産業	1.40	1.20	1.40	1.60	2.20	1.00	1.60	1.00

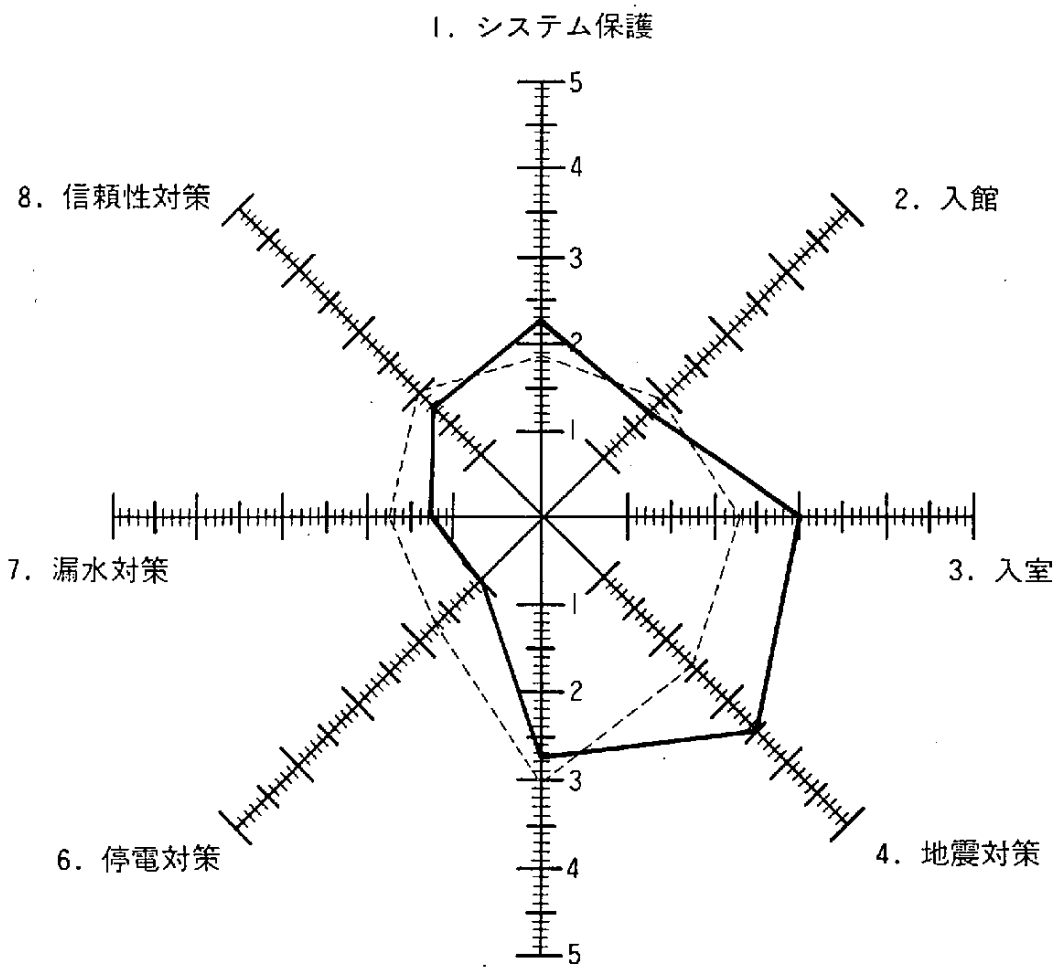
化学工業



---：全産業平均

	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
化学工業	1.88	1.71	2.02	2.02	2.67	1.26	1.41	1.64

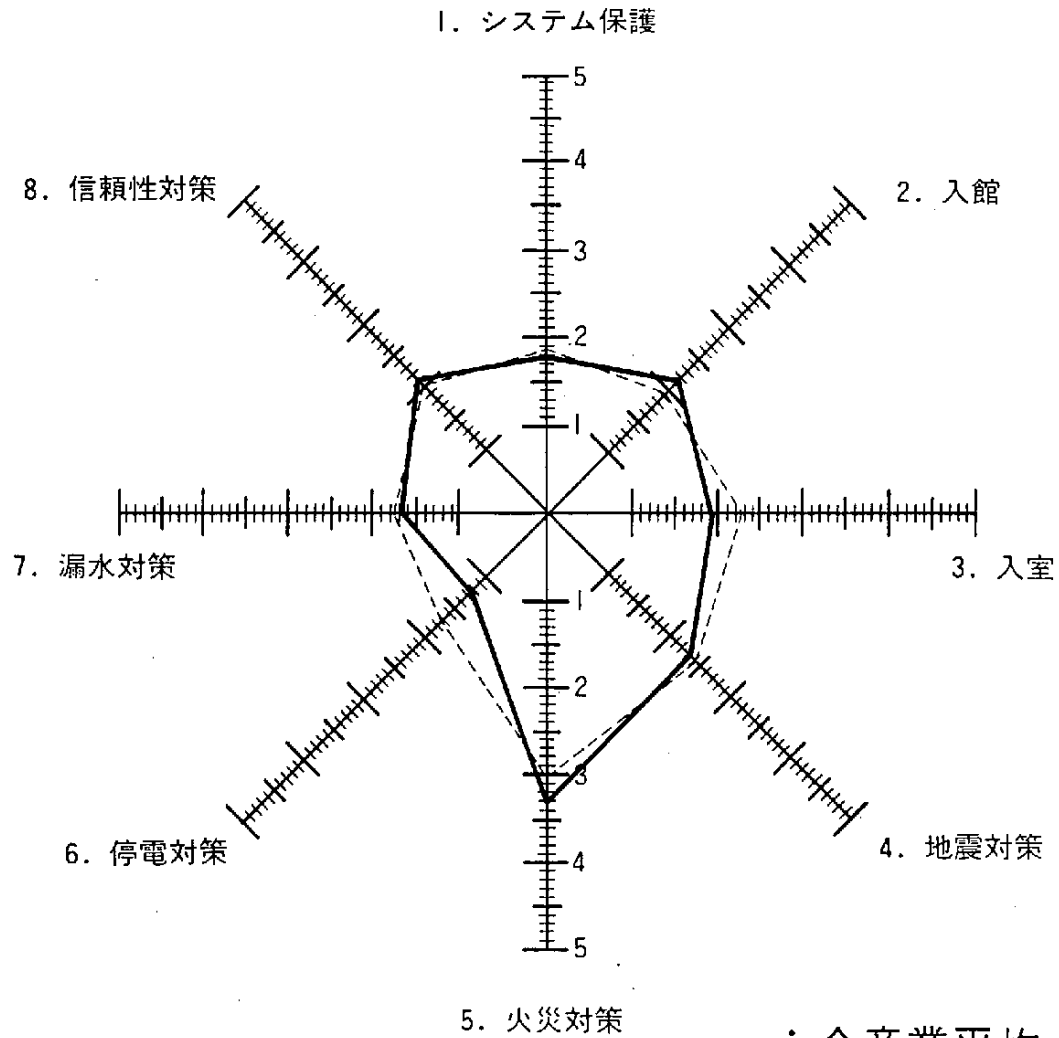
石油製品製造業



---：全産業平均

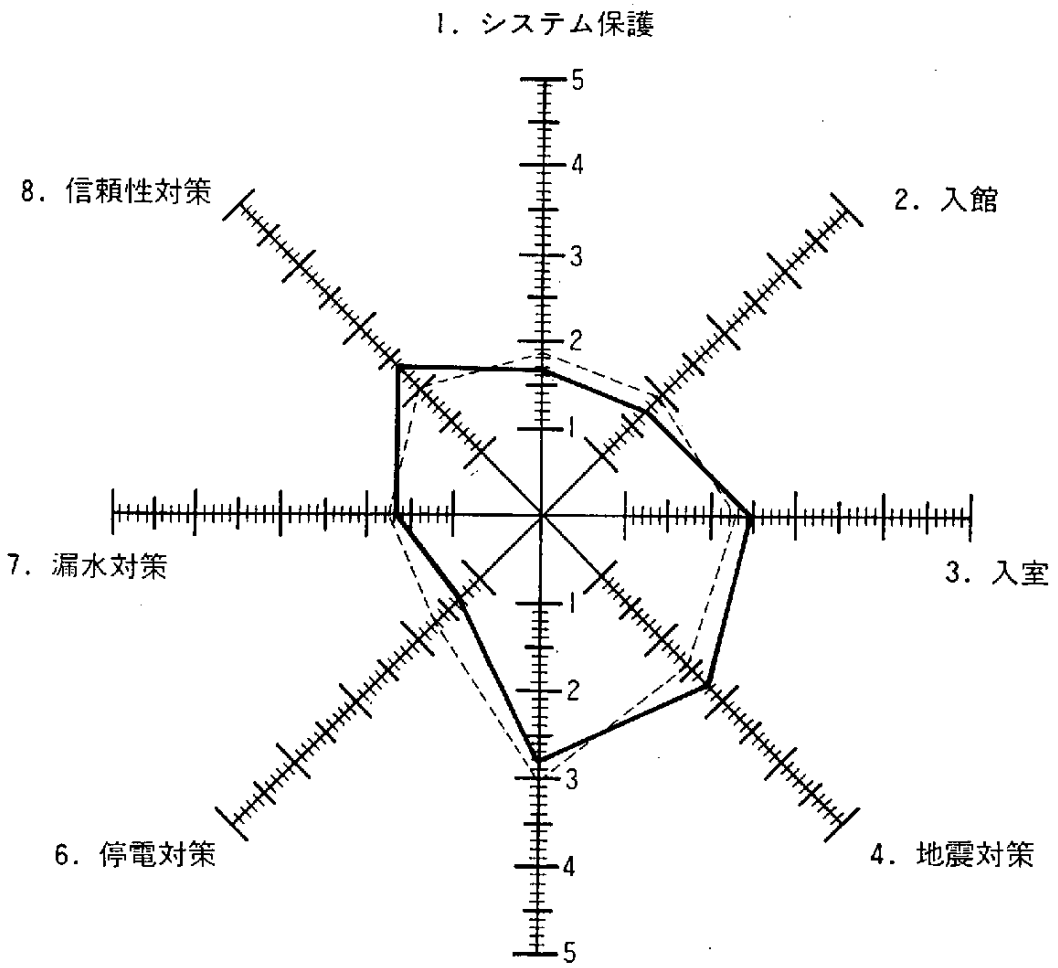
	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
石油製品製造業	2.25	1.75	3.00	3.50	2.75	1.00	1.25	1.75

窯業・土木製品製造業



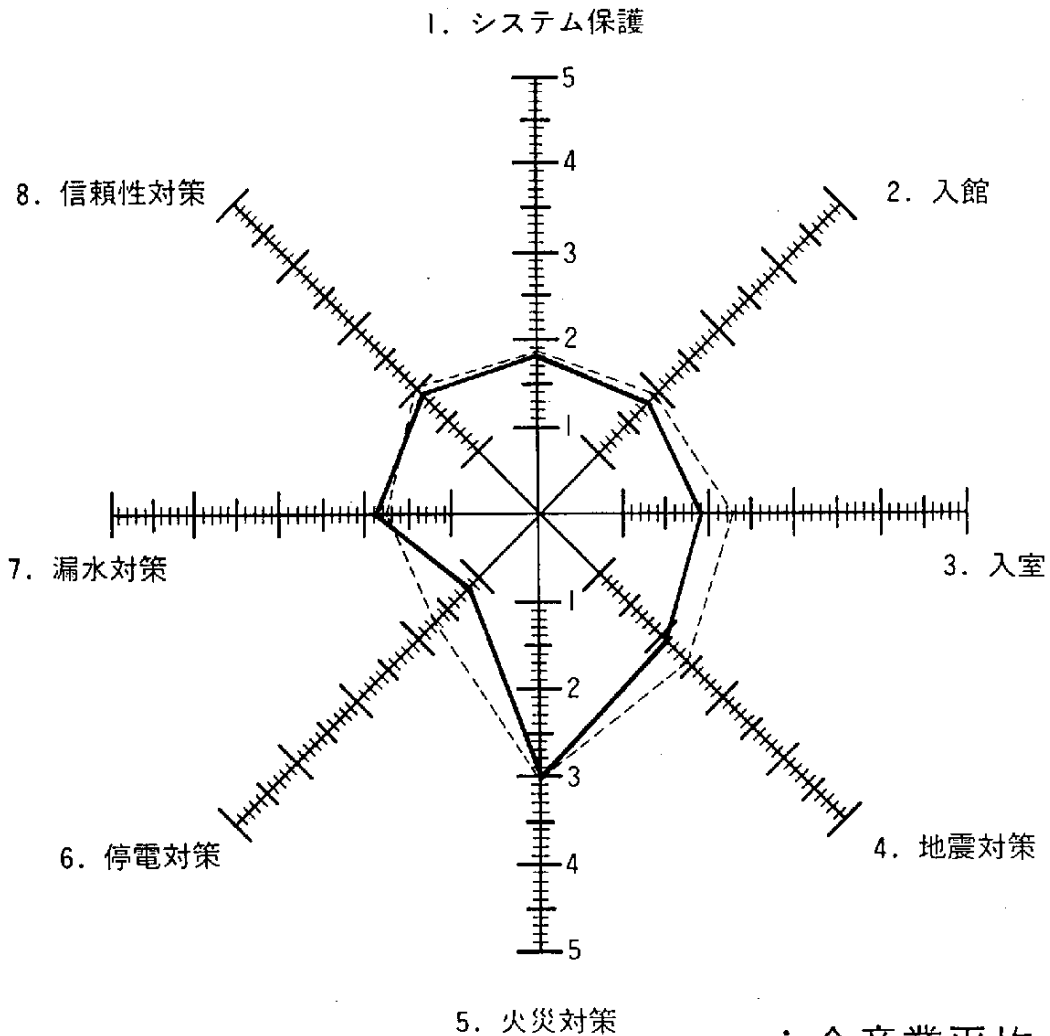
	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
窯業・土木製品製造業	1.78	2.11	1.89	2.33	3.33	1.22	1.63	2.11

鉄　鋼　業



	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
鉄鋼業	1.67	1.70	2.45	2.73	2.83	1.33	1.67	2.36

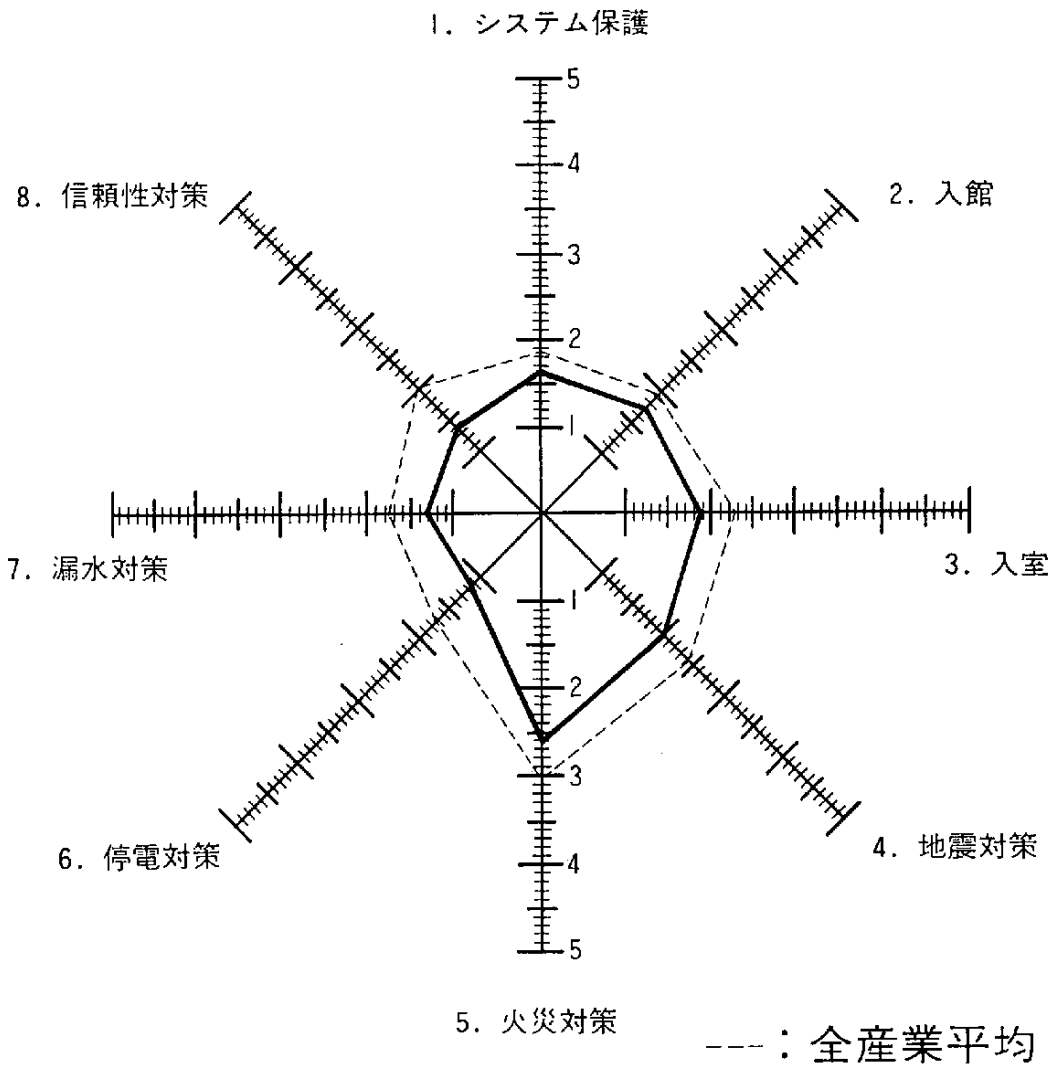
非鉄金属製造業・金属製品製造業



---：全産業平均

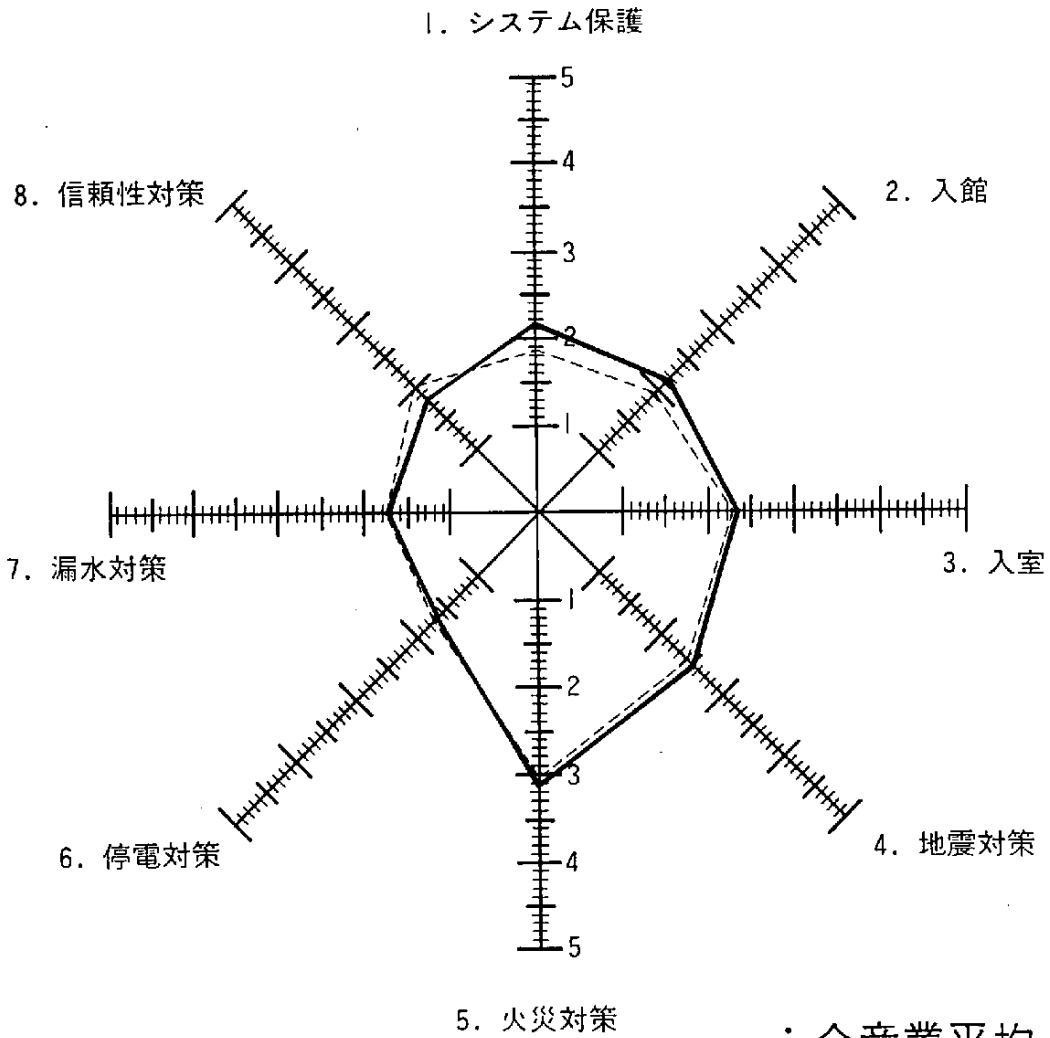
	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
非鉄金属製造業・金属製品製造業	1.79	1.79	1.90	2.07	3.00	1.17	1.87	1.93

一般機械器具製造業



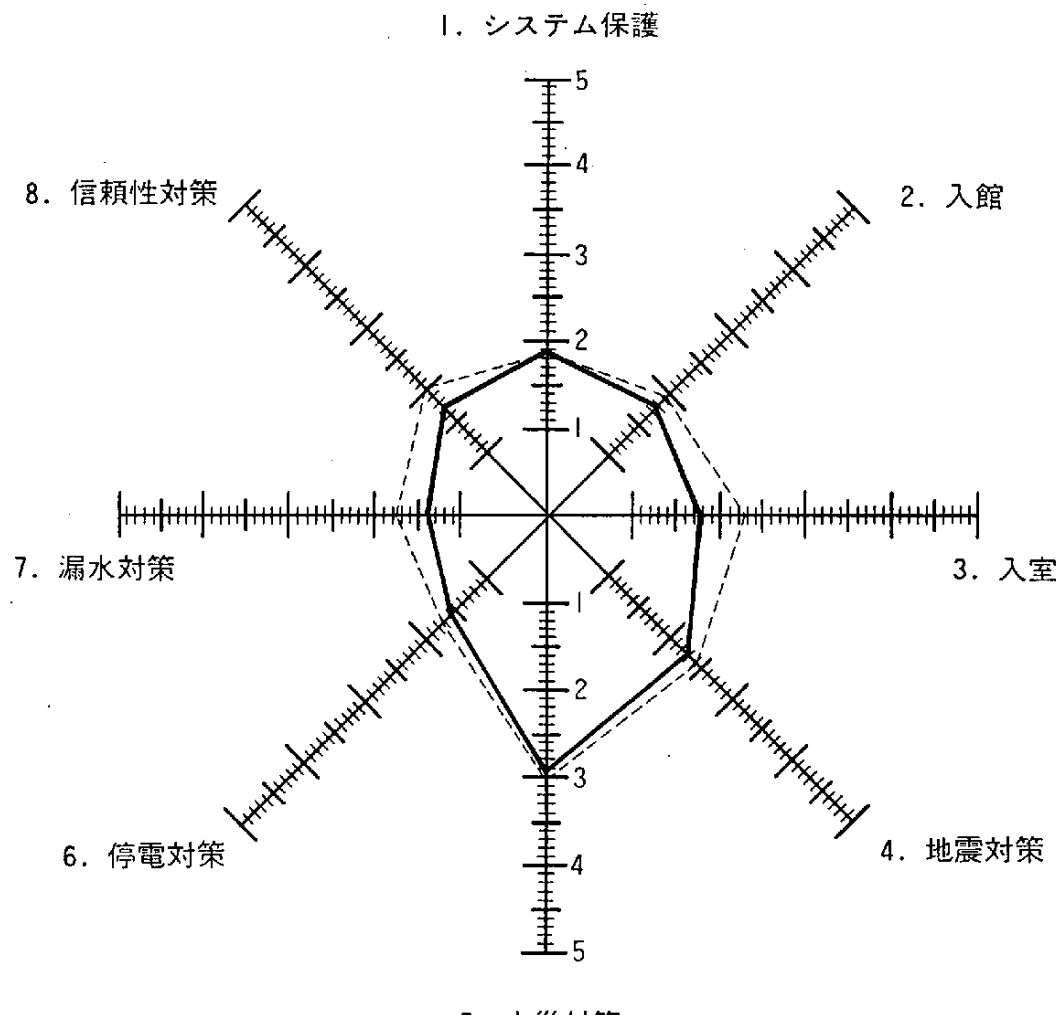
	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
一般機械器具製造業	1.66	1.72	1.86	2.00	2.62	1.17	1.31	1.36

電気機械器具製造業



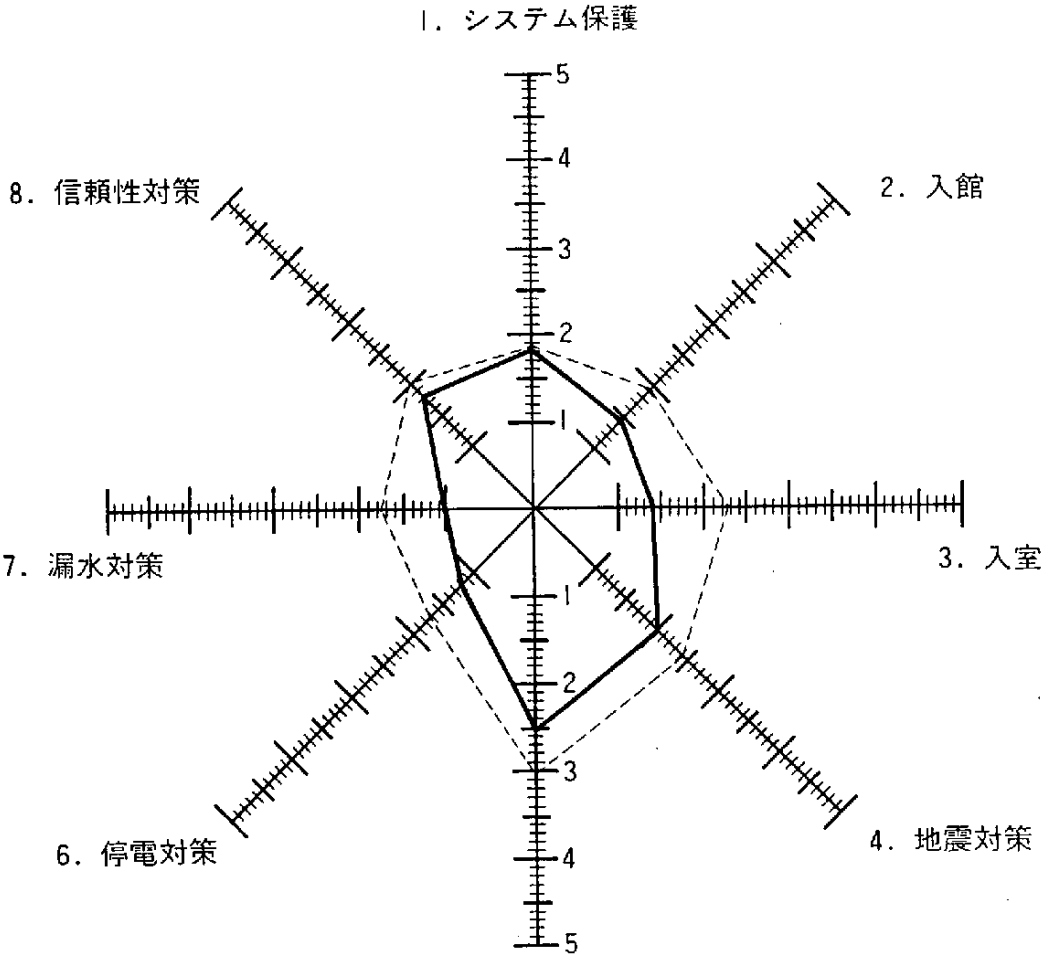
	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
電気機械器具製造業	2.15	2.15	2.33	2.53	3.11	1.68	1.73	1.82

輸送用機械器具製造業



	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
輸送用機械器具製造業	1.87	1.72	1.77	2.29	2.94	1.59	1.38	1.69

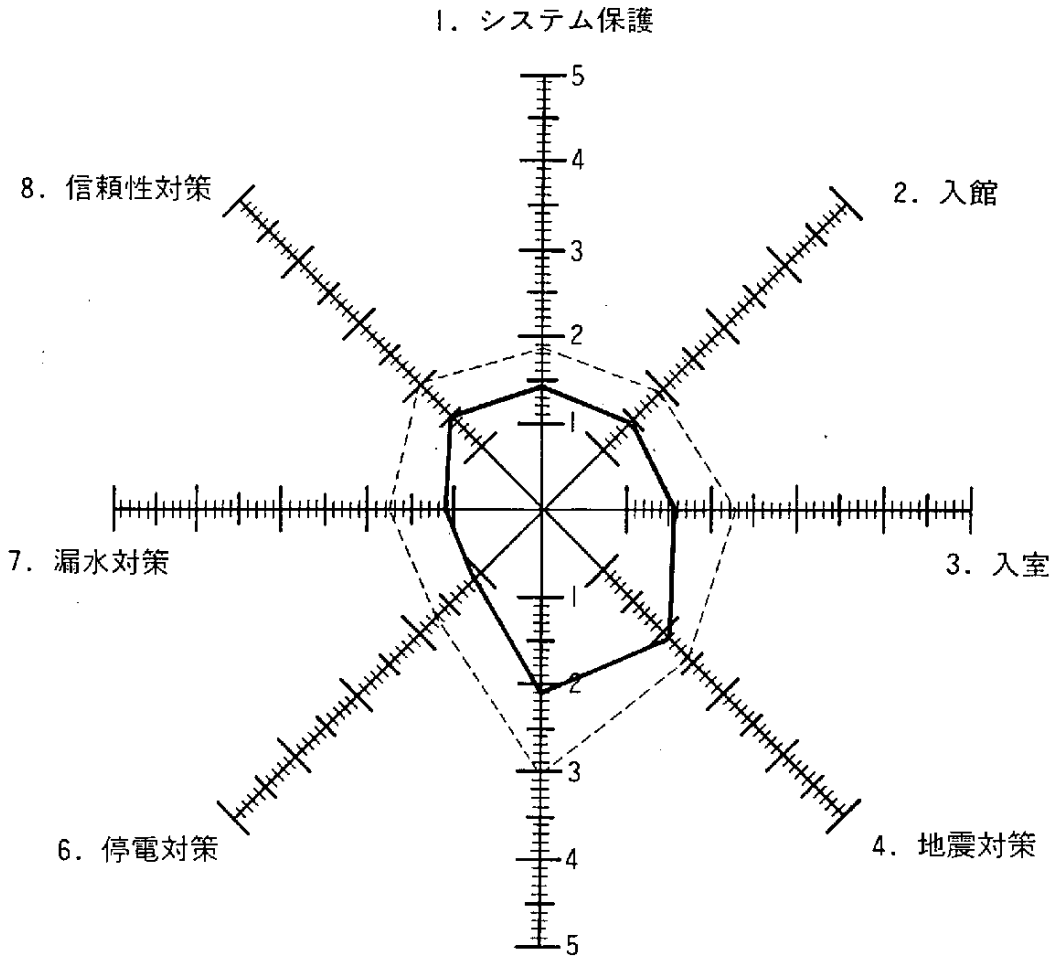
精密機械器具製造業



---：全産業平均

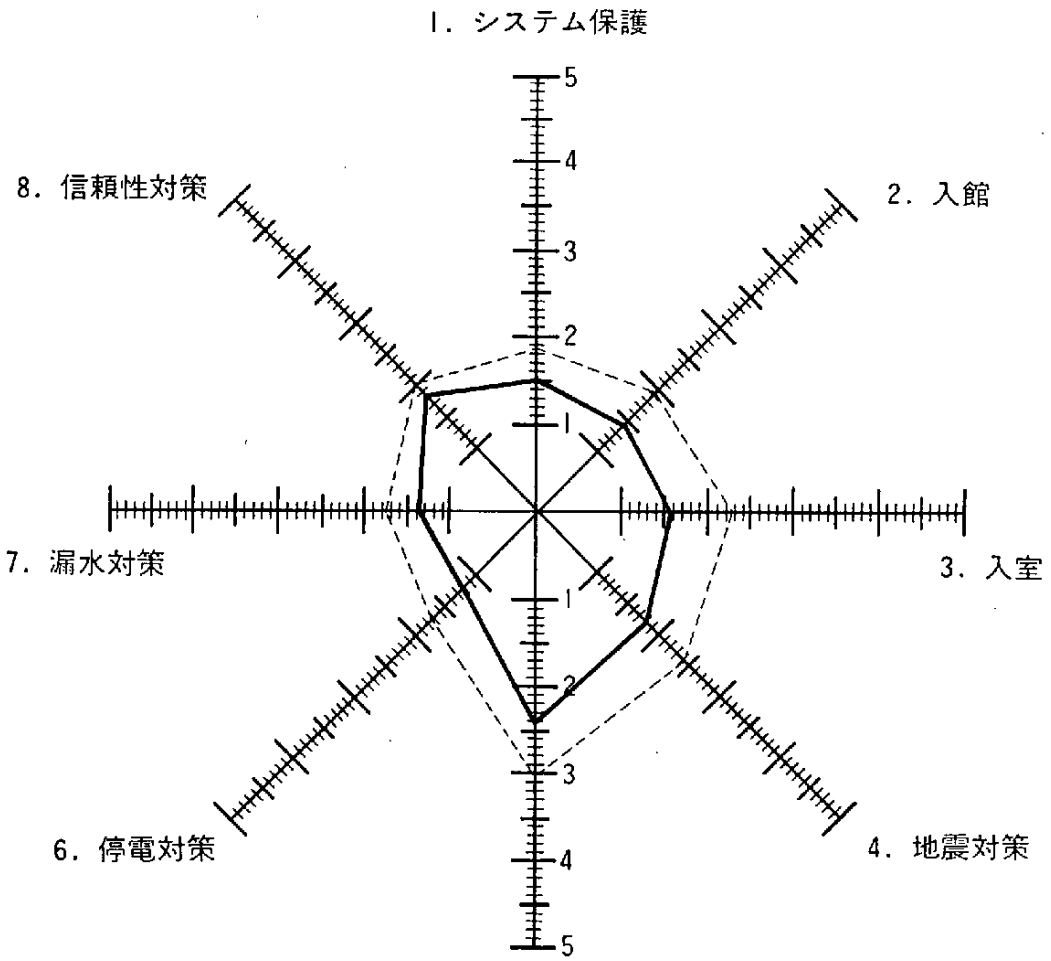
	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
精密機械器具製造業	1.80	1.47	1.40	2.00	2.53	1.20	1.00	1.80

その他の製造業



	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
その他の製造業	1.41	1.44	1.56	2.11	2.11	1.11	1.11	1.50

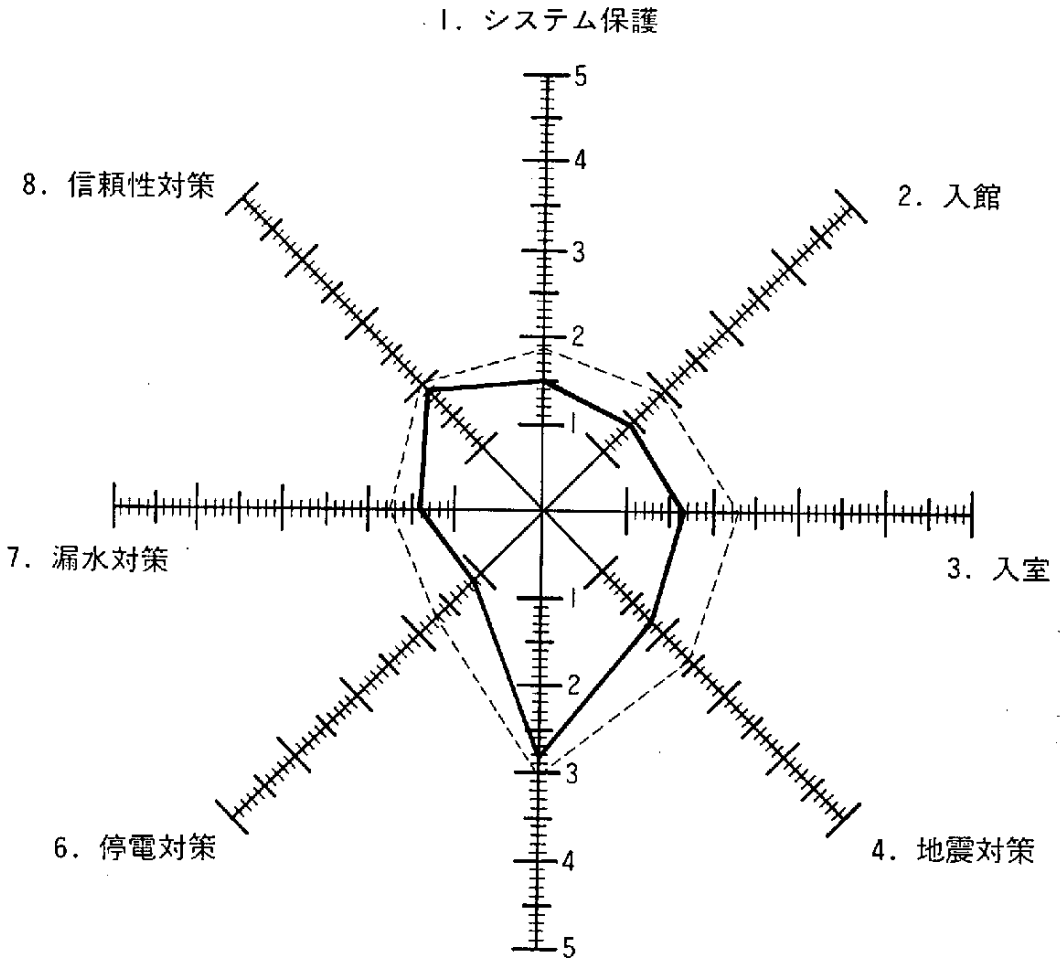
卸業・商社



---：全産業平均

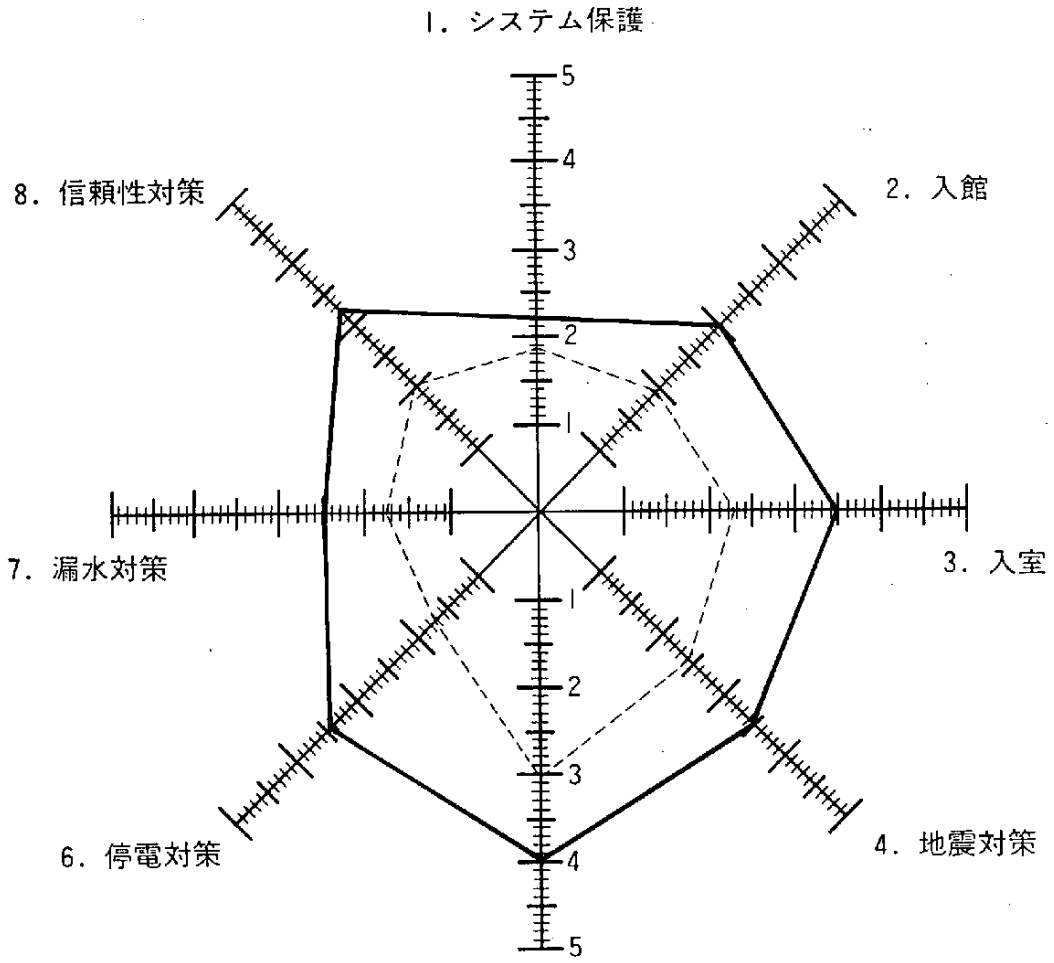
	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
卸業・商社	1.52	1.41	1.57	1.81	2.41	1.20	1.36	1.84

小　売　業



	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
小売業	1.51	1.39	1.64	1.82	2.79	1.13	1.41	1.91

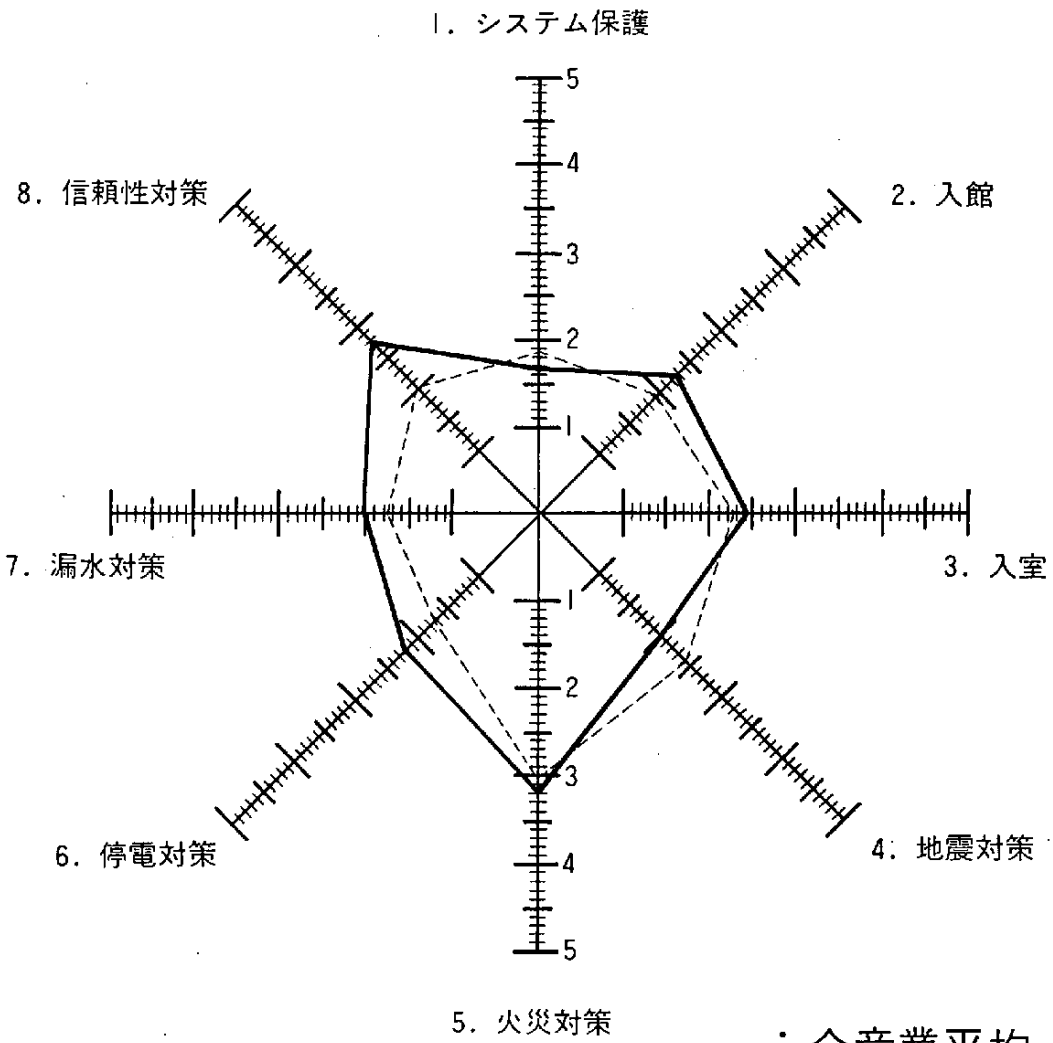
金　融　業



---：全産業平均

	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
金融業	2.19	3.00	3.48	3.46	3.99	3.44	2.49	3.23

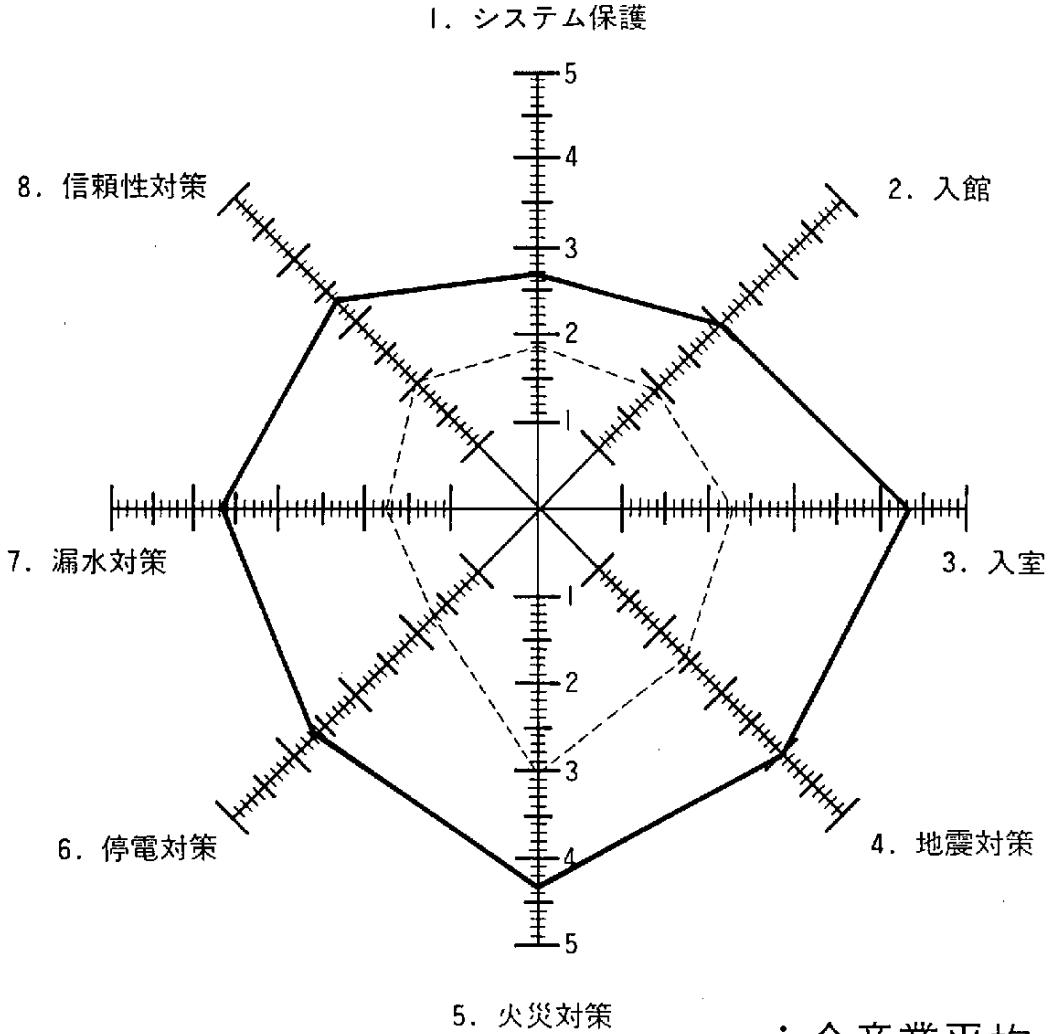
証券業・商品取引業



---：全産業平均

	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
証券業・商品取引業	1.67	2.25	2.40	2.00	3.20	2.20	2.00	2.75

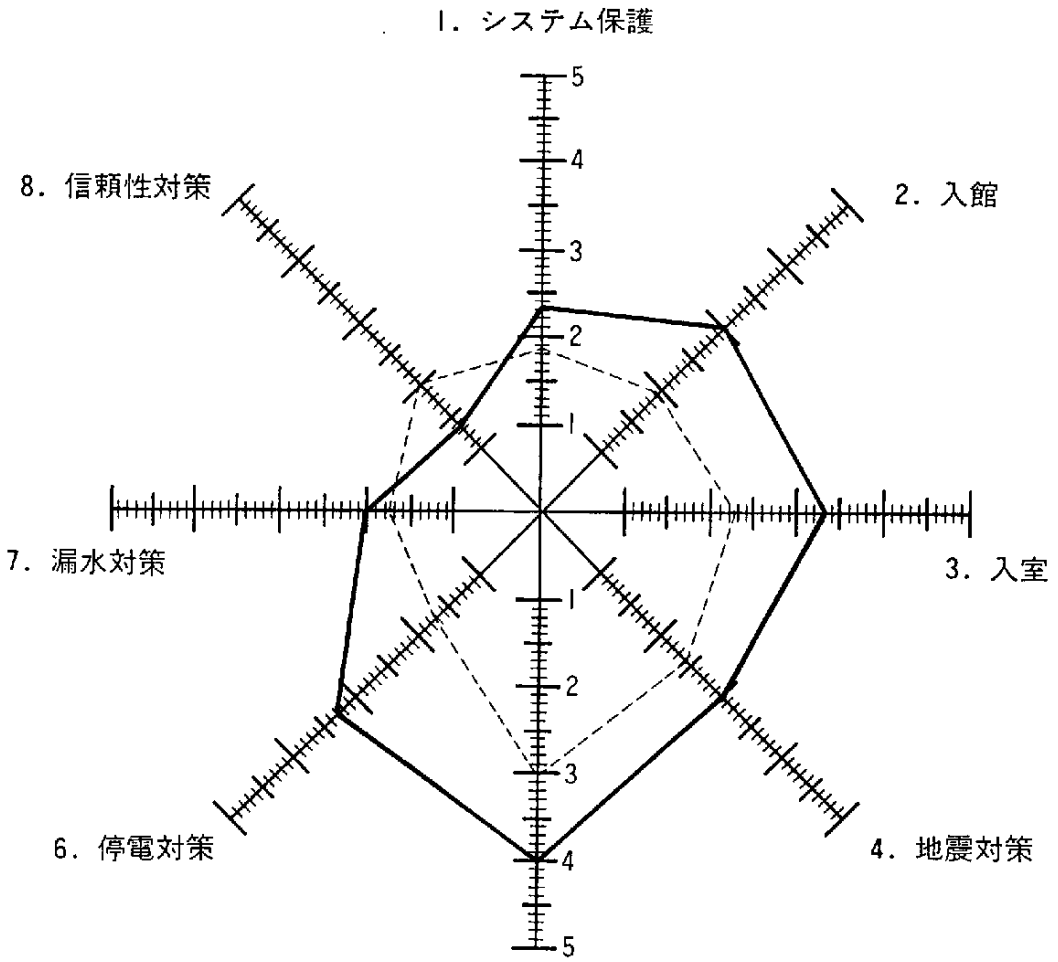
生命保険業(含代理業・サービス業)



---：全産業平均

	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
生命保険業(含代理業・サービス業)	2.67	3.00	4.33	4.00	4.33	3.67	3.67	3.33

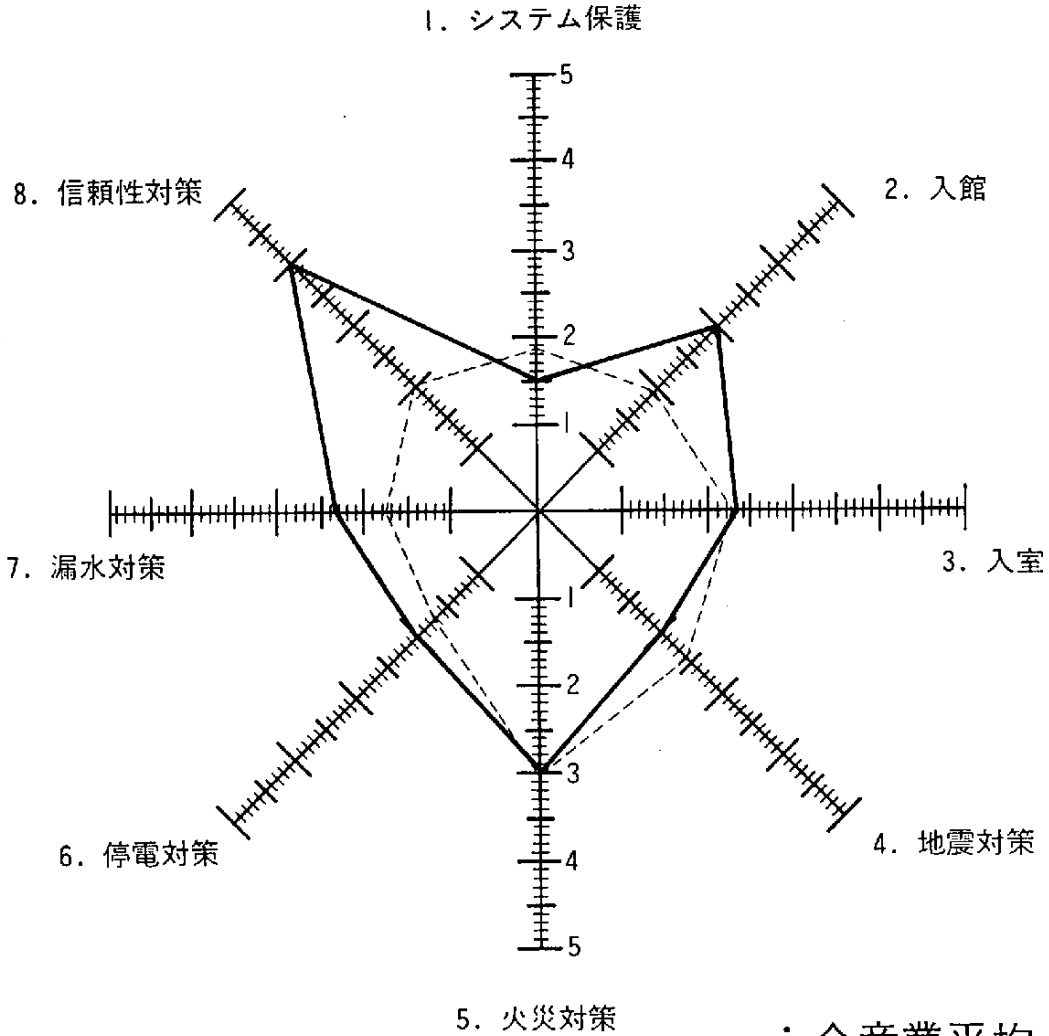
損害保険業(含代理業・サービス業)



---：全産業平均

	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
損害保険業(含代理業・サービス業)	2.33	3.00	3.33	3.00	4.00	3.33	2.00	1.33

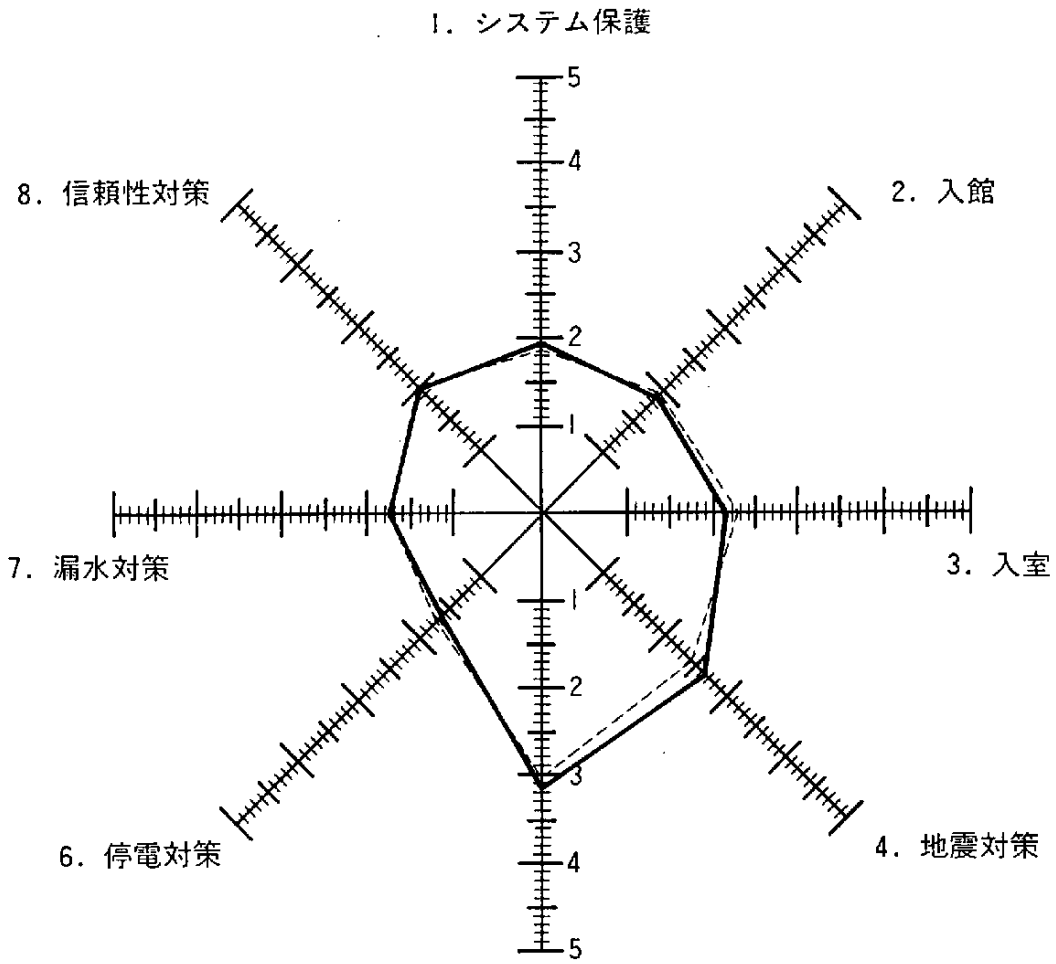
不動産業



---：全産業平均

	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
不動産業	1.50	3.00	2.33	2.00	3.00	2.00	2.33	4.00

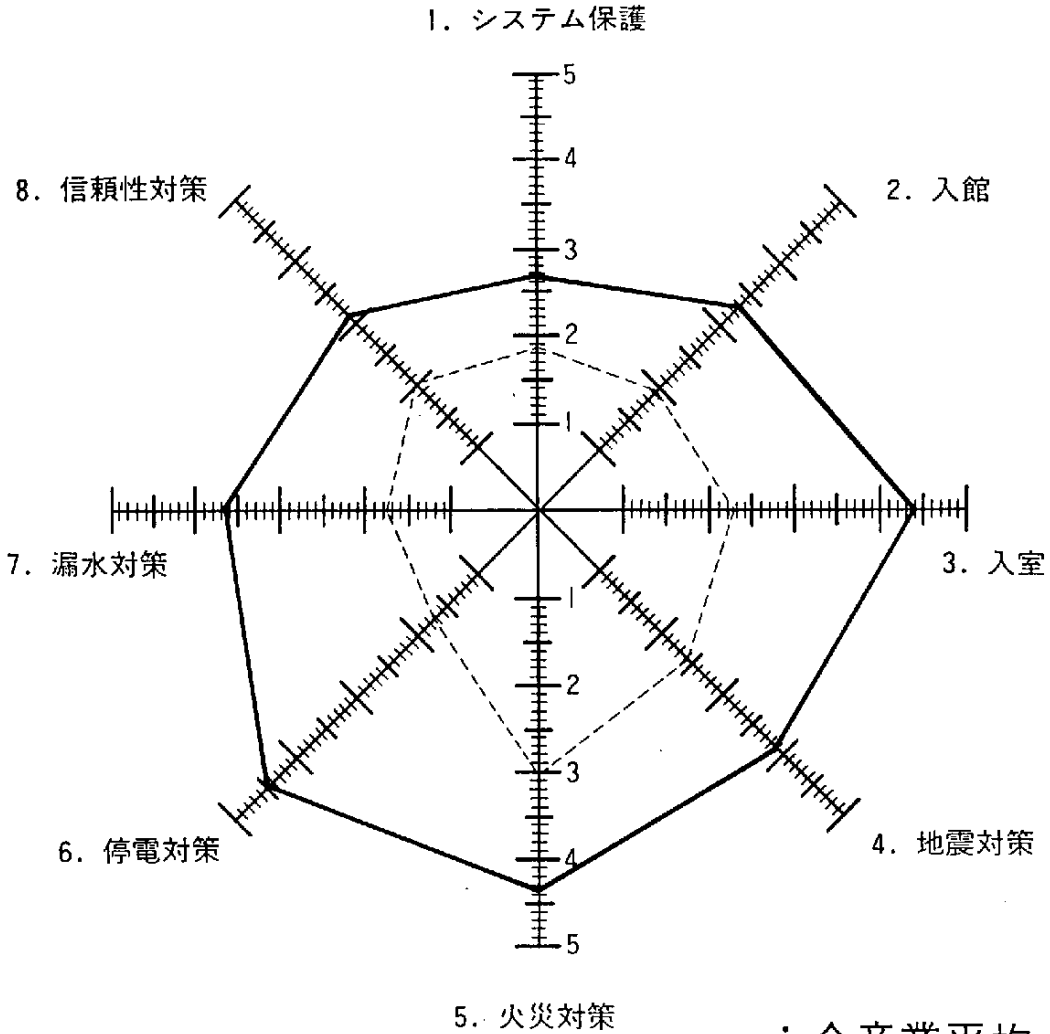
運輸・通信業



---：全産業平均

	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
運輸・通信業	1.94	1.88	2.12	2.64	3.14	1.67	1.74	1.97

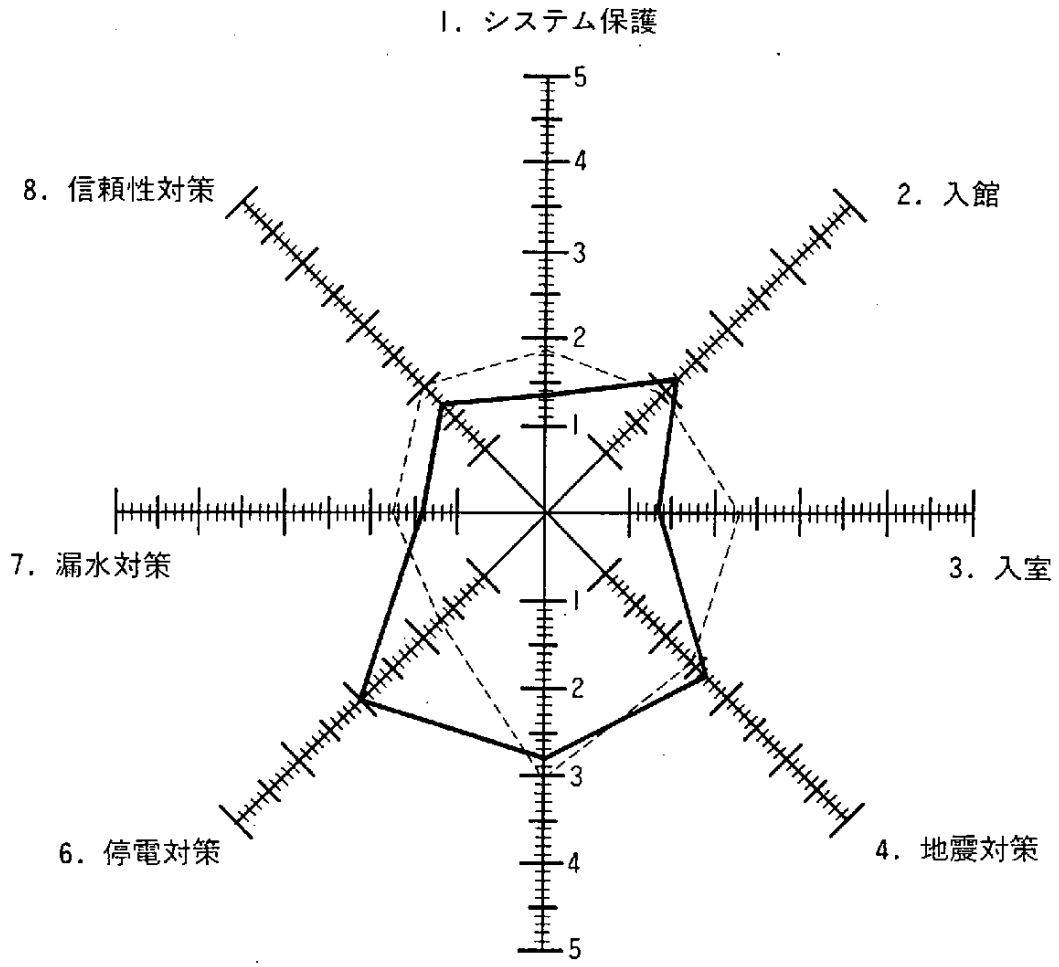
電力･ガス事業



---：全産業平均

	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
電力･ガス事業	2.67	3.25	4.38	3.89	4.33	4.44	3.63	3.11

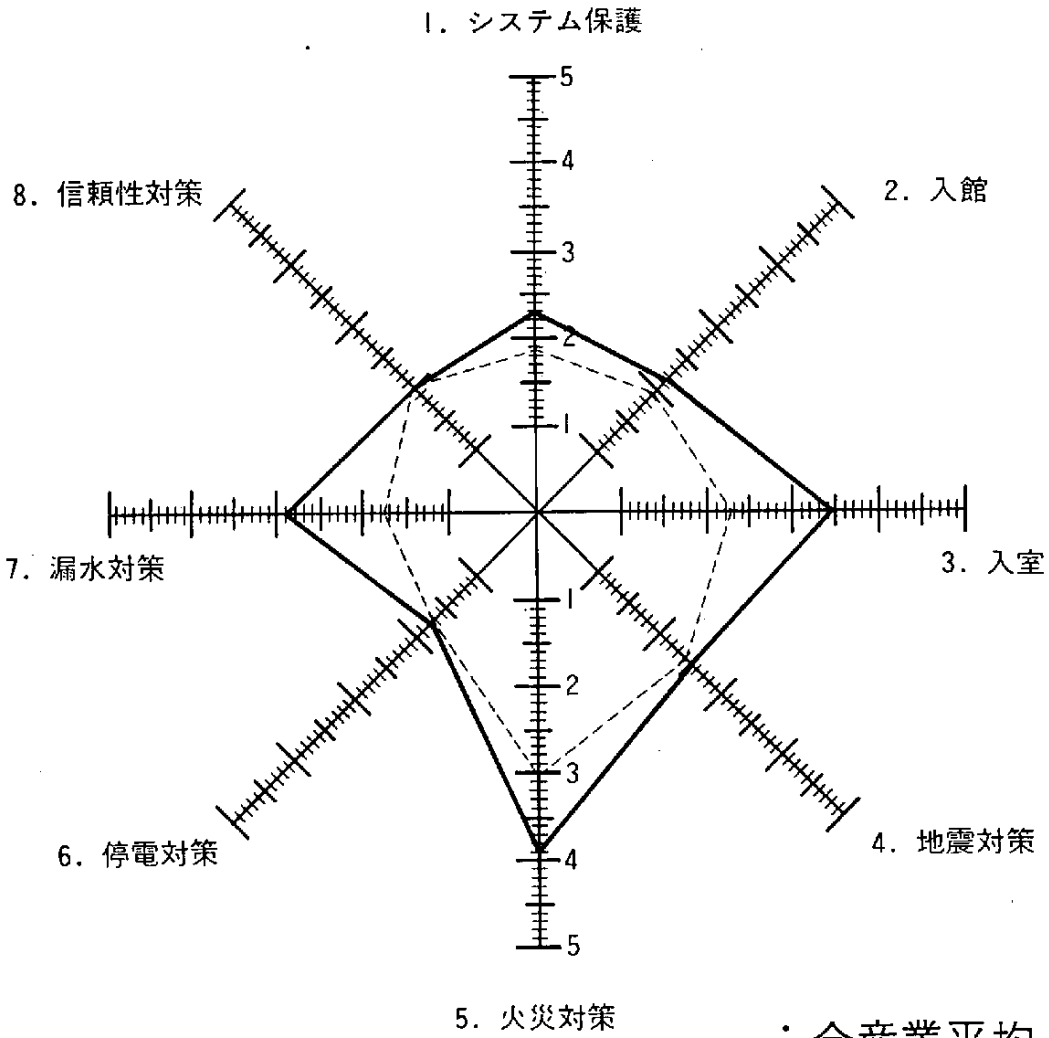
放　送　業



---：全産業平均

	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
放送業	1.36	2.18	1.36	2.64	2.82	3.00	1.45	1.70

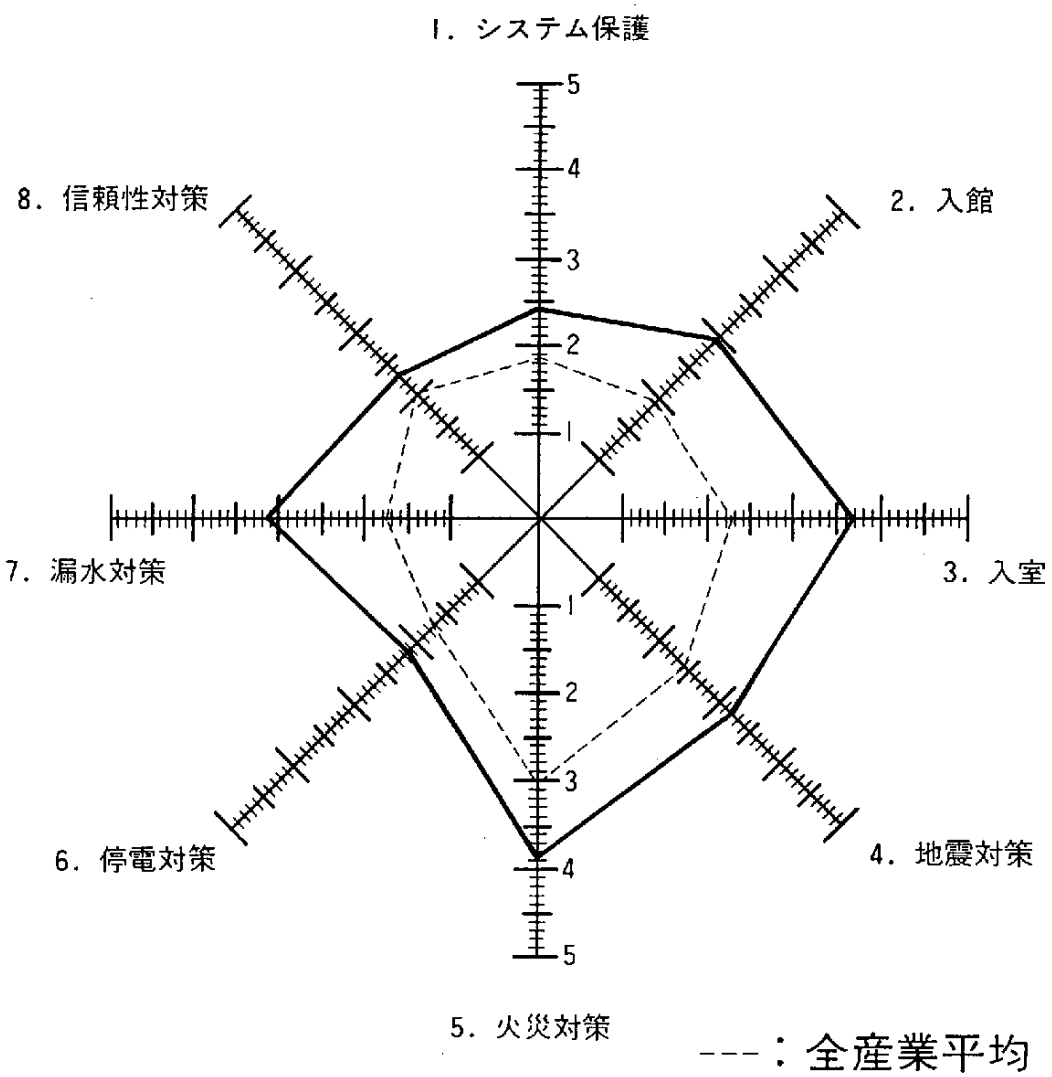
広告・調査・情報提供サービス業



---：全産業平均

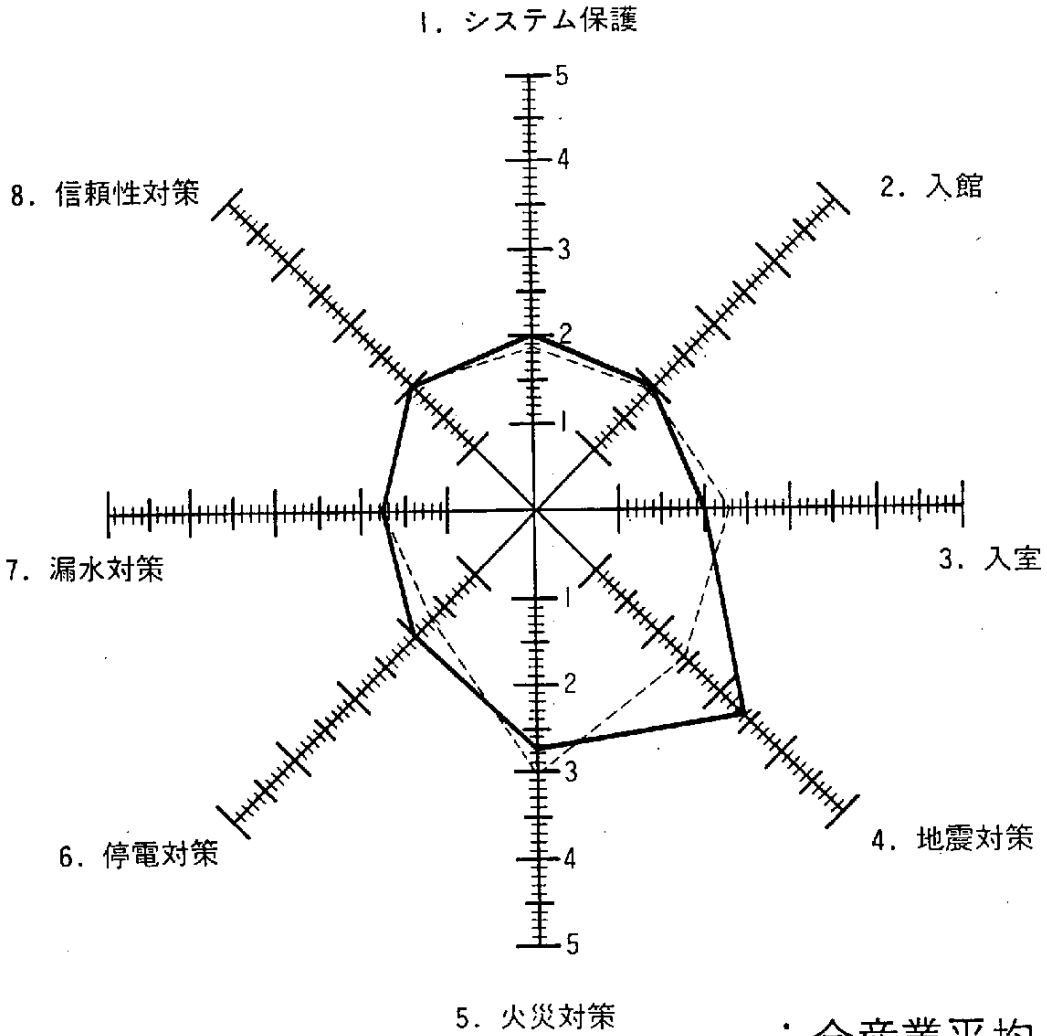
	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
広告・調査・情報提供サービス業	2.29	2.14	3.43	2.50	3.88	1.75	2.88	2.00

情報処理サービス業・ソフトウェア業



	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
情報処理サービス業・ソフトウエア業	2.40	2.96	3.65	3.18	3.87	2.15	3.09	2.33

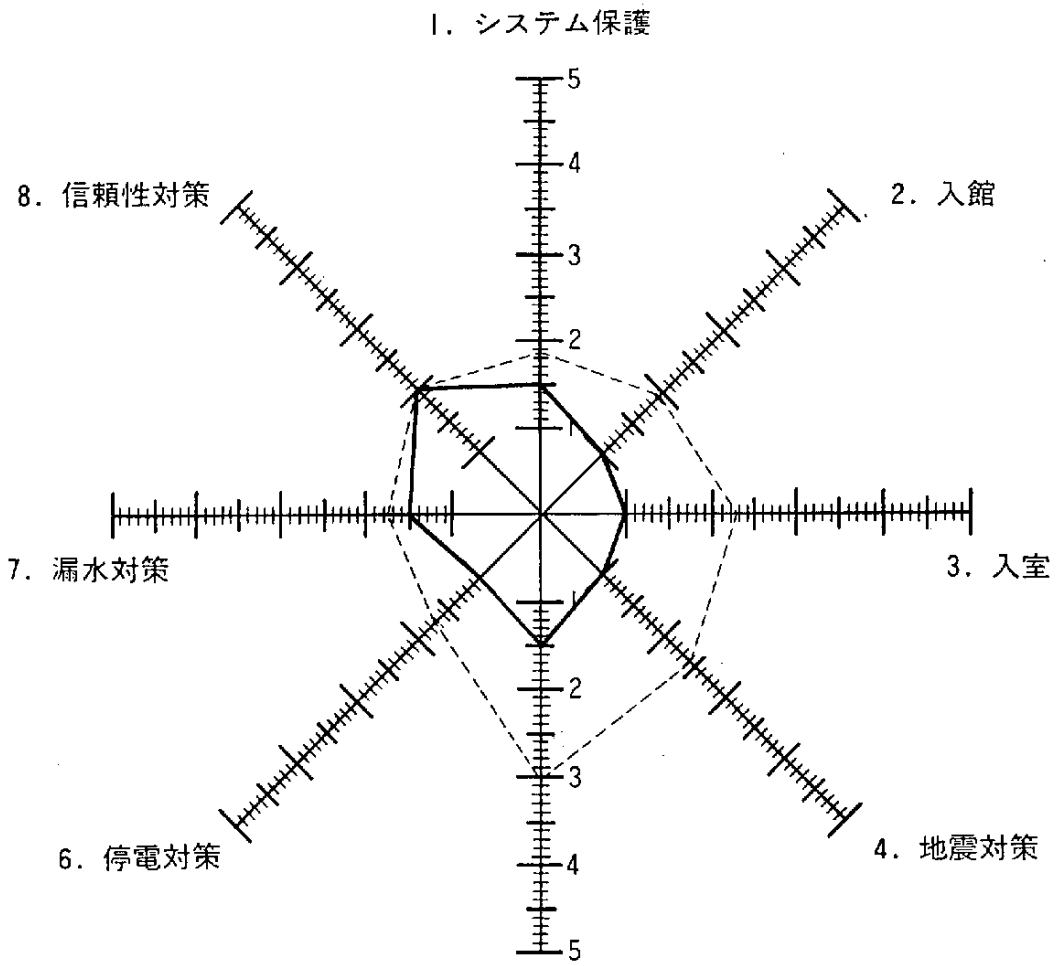
医　療　業



---：全産業平均

	1．システム保護	2．入館	3．入室	4．地盤対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
医療業	2.00	2.00	2.00	3.38	2.75	2.00	1.75	2.00

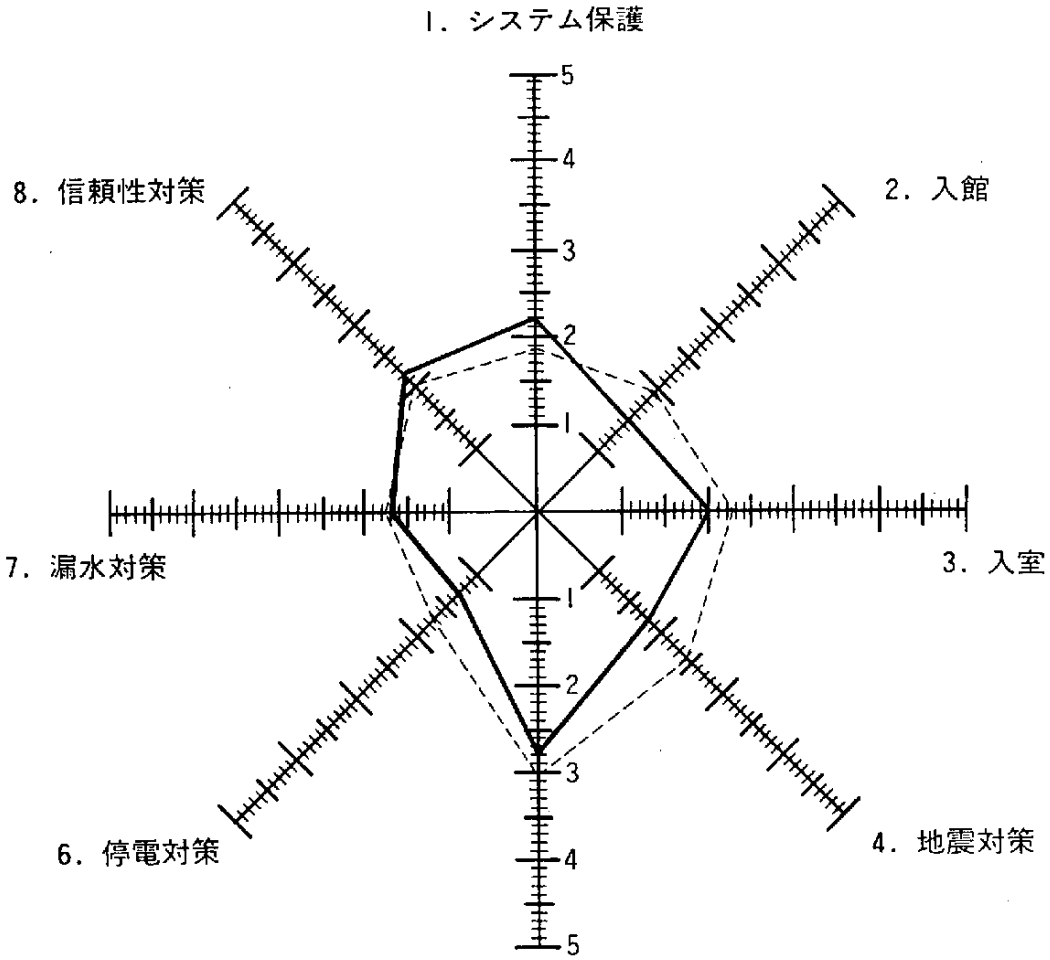
高　校



---：全産業平均

	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
高校	1.50	1.00	1.00	1.00	1.50	1.00	1.50	2.00

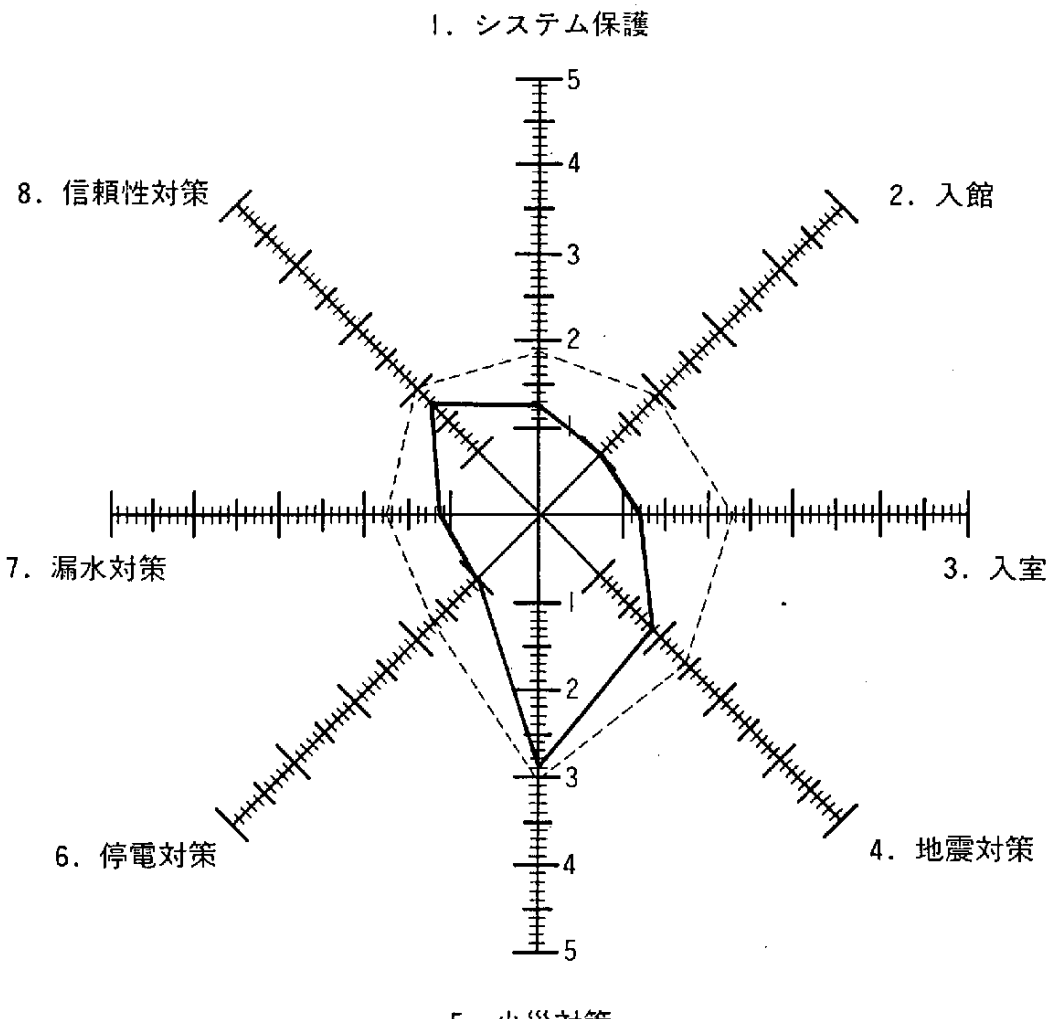
大　学



---：全産業平均

	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
大学	2.22	1.52	2.05	1.80	2.82	1.29	1.67	2.14

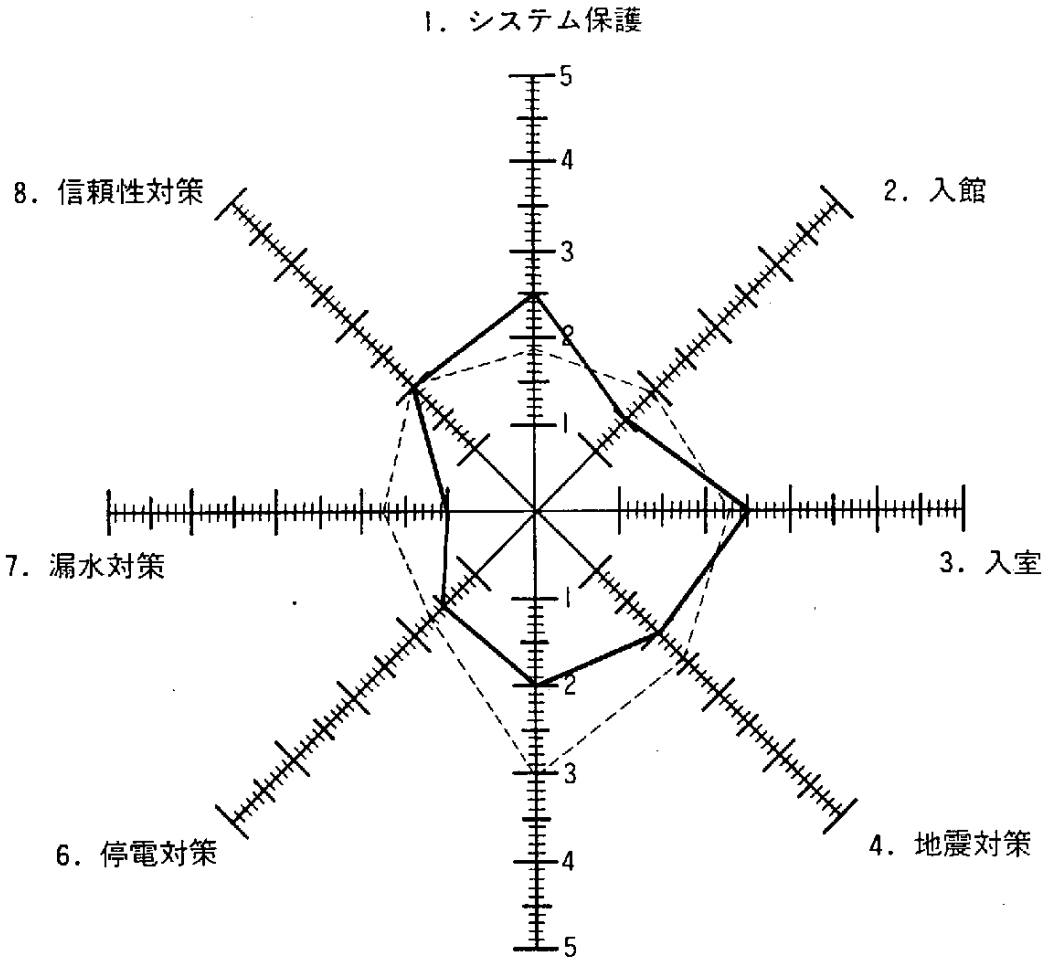
その他の教育機関



---：全産業平均

	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
その他の教育機関	1.25	1.00	1.17	1.88	2.88	1.00	1.13	1.75

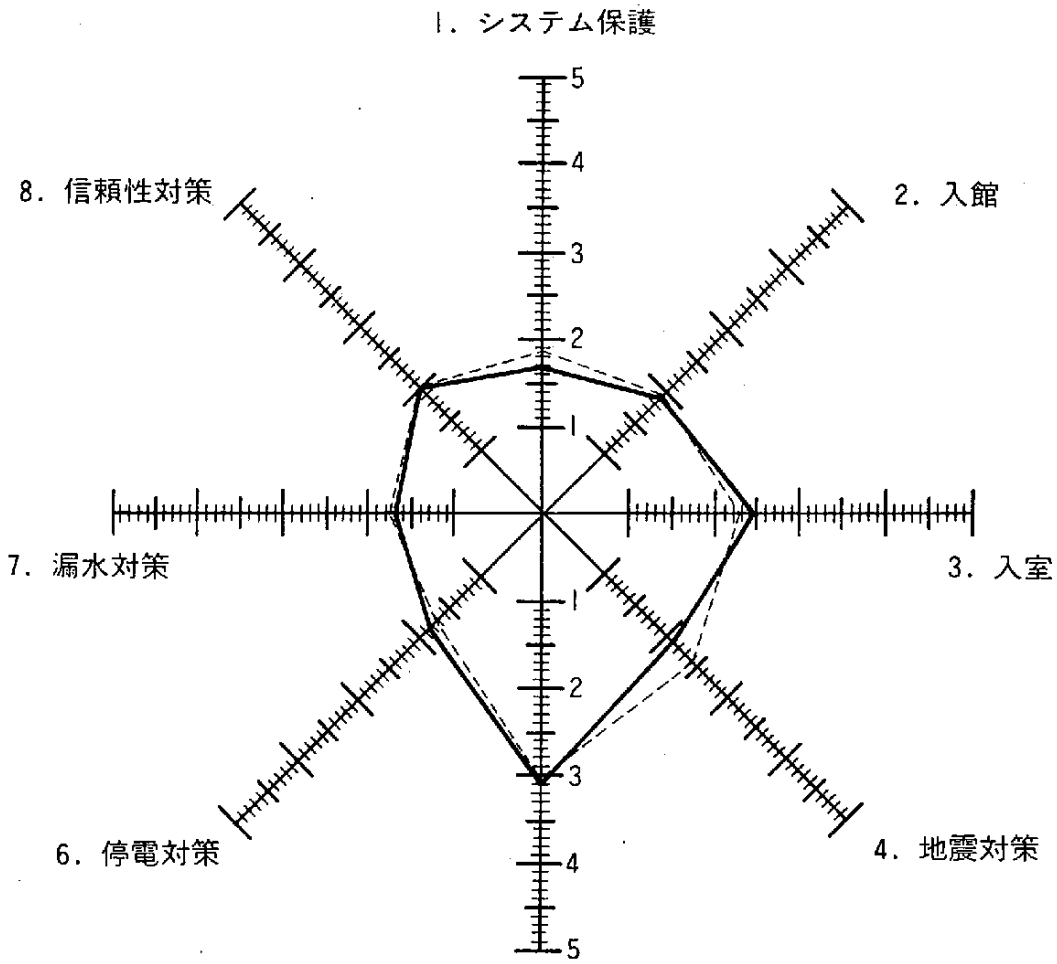
学術研究機関



---：全産業平均

	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
学術研究機関	2.50	1.50	2.50	2.00	2.00	1.50	1.00	2.00

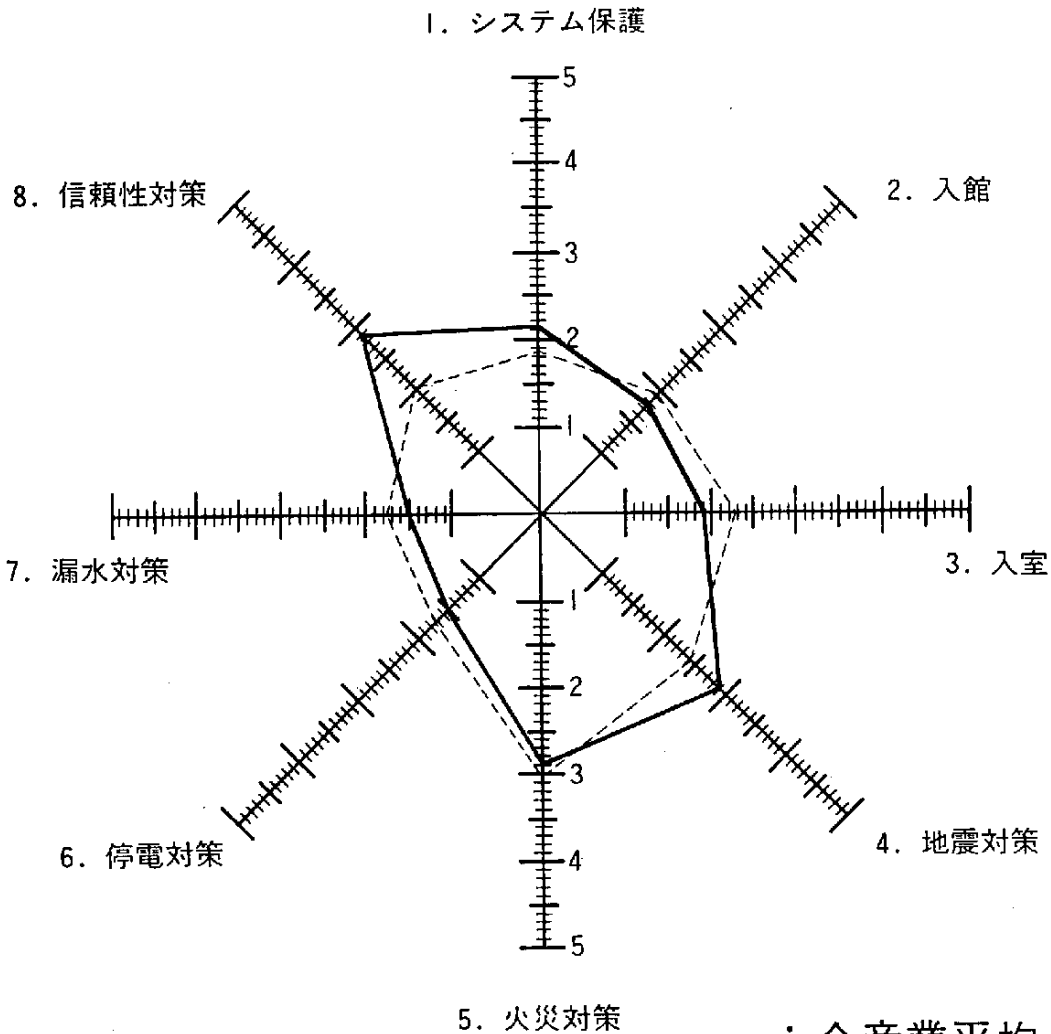
法人団体・農協



---：全産業平均

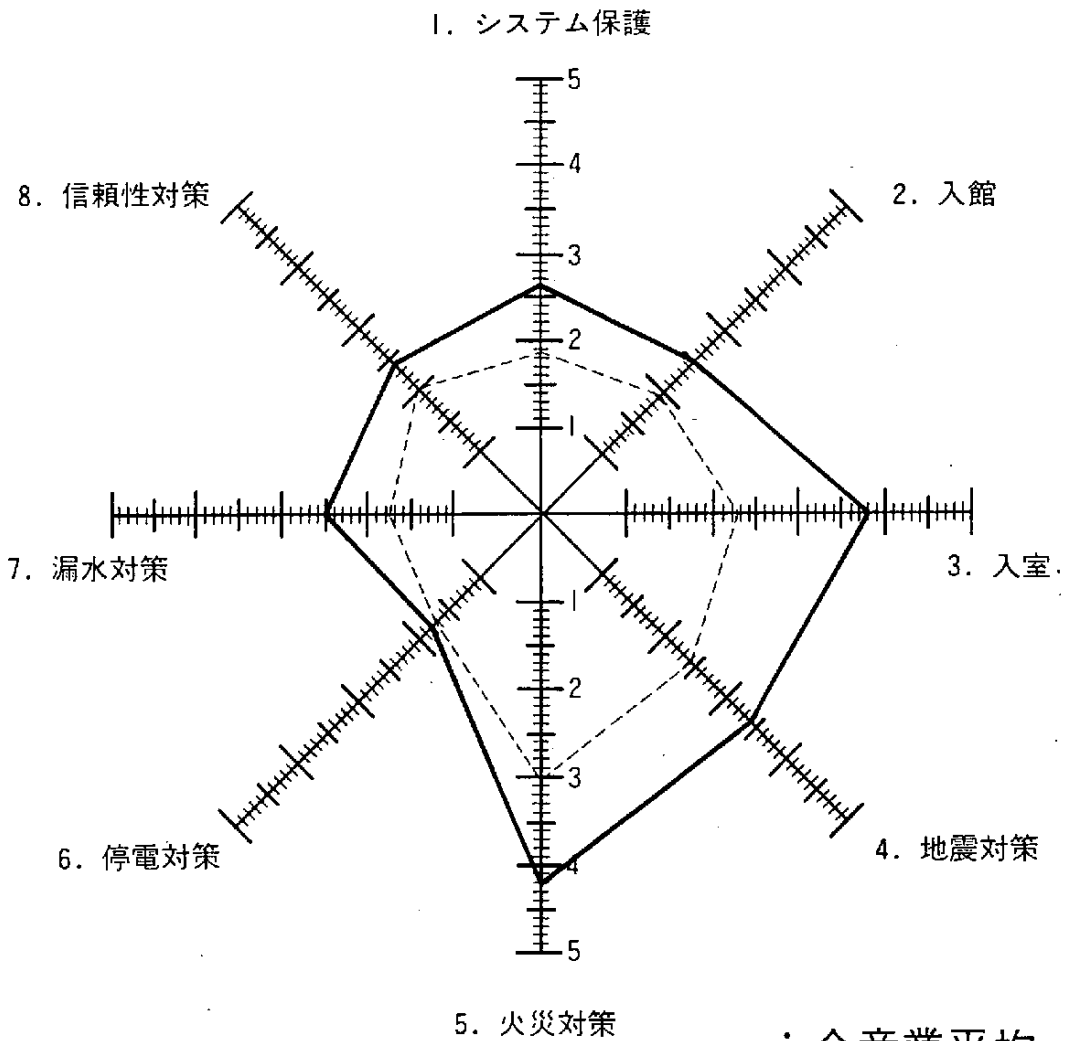
	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
法人団体・農協	1.68	1.87	2.43	2.10	3.09	1.86	1.70	2.00

その他のサービス業



	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
その他のサービス業	2.13	1.75	1.88	2.88	2.88	1.50	1.50	2.88

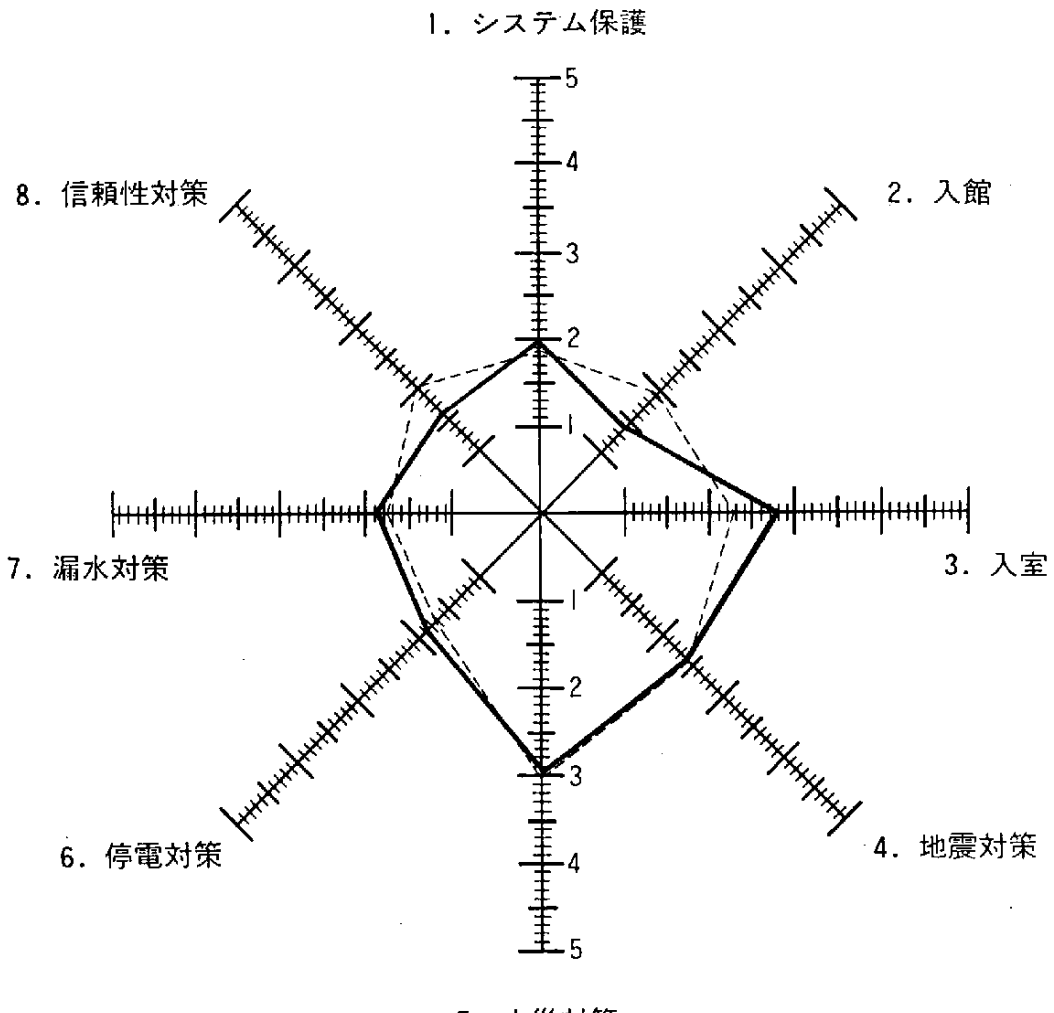
政　府



---：全産業平均

	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
政府	2.60	2.50	3.80	3.40	4.20	1.80	2.50	2.40

地方公共団体



---：全産業平均

	1．システム保護	2．入館	3．入室	4．地震対策	5．火災対策	6．停電対策	7．漏水対策	8．信頼性対策
全産業平均	1.88	1.94	2.29	2.41	3.01	1.73	1.78	2.01
地方公共団体	2.00	1.38	2.76	2.44	2.95	1.81	1.85	1.61

昭和６３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丁目５番８号
機械振興会館内
ＴＥＬ ０３（４３２）９３８７

印刷所　株式会社　東京矢野企画
東京都港区芝大門２丁目１番18号
ＧＳハイム　２０９
ＴＥＬ（４５９）０８３１（代表）