63—R007

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

平成元年3月

JIPDEC

財団法人　日本情報処理開発協会

この報告書は，日本自転車振興会から競輪収益の一部である機械工業振興資金の補助を受けて，昭和63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

わが国の情報システムは，一方では銀行の第３次オンライン・システムに代表されるように高度化・複雑化が著しく，他方ではパーソナル・コンピュータの普及により大衆化が進んでいる。そして，これらの利用をサポートしているのがネットワークであり，最近めざましく進展している。

このような情報化環境においては，情報システムに何らかの障害が発生すると，その影響は広範に及ぶことになり，情報化社会の基盤を揺るがすことになりかねない。

当協会では，このような認識に立ち，昭和59年より，リスク分析委員会を設置して，コンピュータ・セキュリティに関するリスク分析手法を確立すべく，調査研究を続けている。

本年度は，バンキング・システムのモデルを作成し，それを対象に机上にて，業務事故事象の把握，および損失の評価などを中心に分析を試みた。このようなモデルに基づく机上での分析を積み重ね，近い将来，リスク分析ガイドラインをとりまとめ，参考に供することと致したい。

最後に，本調査研究を推進するにあたり，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。

平成元年３月

財団法人　日本情報処理開発協会

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	日本コンピュータセキュリティ㈱ 代表取締役社長
	郡山　信	㈶金融情報システムセンター 安全対策部情報課長
	小早川　久佳	青山監査法人　代表社員
	小林　孝夫	日本アイ・ビー・エム㈱ サービス技術・品質保証-CSP
	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㈱　代表取締役社長
	南波　駿太郎	日本銀行金融研究所 研究第２課長
	花香　俊明	㈱デーシージャパン　第２部長
	三谷　保夫	Ｋシステムプランニング　代表
	安田　健博	ＮＴＴデータ通信㈱ ﾌｨｰﾙﾄﾞｻｰﾋﾞｽ事業部ﾊｰﾄﾞ技術担当部長

目　　次

第１章　リスク分析をめぐって

コンピュータ・システムは，現代社会のあらゆる領域において，過去と比較にならない割合で利用されてきている。われわれが，そうしたコンピュータ・システムに依存する度合いが高まるにつれ，システム関連の脆弱性も増大してきている。それだけに，情報化社会における組織のリスク・マネジメントが重視され，その一環としてコンピュータ・セキュリティが不可欠と認識され，リスク分析が研究対象とされてきているのである（注１）。

一般的に，コンピュータ・セキュリティは，リスク分析を包含した意味で使われているが，コンピュータ・セキュリティそれ自体はリスク処理方法の１つということになる。ここで確認しておくべきことは，先にリスクを処理する方法がくるのではなく，何故にリスクを処理しなければならないかの問題状況の認識・把握が先にくるということである。リスク・マネジメントにおいては，リスク分析に始まる論理的なリスク処理のステップが採択される（注２）。適切なリスク処理方法の選択に関する情報の提供を可能にするのが，リスク分析なのである。

１．リスク分析の視座

リスク分析（リスク・アナリシス）は，リスクの発見・確認・評価という作業から成っている。しかし，場合により，リスク・アセスメントといった用語も見られる。論者により意味づけに差があるが，「リスク・アセスメント」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の強度を調査し，評価する分析活動を示す場合に用いられ，「リスク・アナリシス」については，リスクを特定の構成要素（脅威，資産，損害ないし損失結果および対応策）間の関係に入念にメスを入れるために採用される詳細な手続きを意味する（注３）展開もある。こうした用法上に違いがあるが，ここでのリスク分析は前者を包含した意味で勘案する。その根拠は，単なる脅威から生ずる結果の評価以上に，リスクにさらされている資産，リスクの結果たる損失，それに対する対応策との関係に視点をおくことにある。

例えば，脅威，資産，損失結果との間には，次のような関係がある(注４)。

：脅威→（予防措置）→資産→（軽減措置）→損失結果

ここでの予防措置ならびに軽減措置は，リスク処理方法におけるコンピュータ・セキュリティ（セーフガード）が中心となるが，さらに，損失結果に対し，資金的な対応（リスク・ファイナンス），例えばリスク保有なりリスク移転（情報化保険）といった方法が関係している。リスク分析は，こうした連関関係を視座にすえ展開されるのである。特にリスクの評価については，どの程度までリスクを容認しうるか，さらにリスク処理方法の対費用効果分析まで包含するのがより効果的となろう。

2．リスク分析の意義

さて，組織にとり，どこに，どんなタイプのリスクが，どのような状況のもとで発生するのかという，いわばリスクの洗い出し作業たるリスクの発見が最初に必要となる。

次は，発見されたリスクの組織内での確認である。さらに，そのリスクがどの程度の頻度で発生し，どのくらいの損失規模（強度）となるのか，リスクの測定が重要となる。それらを踏まえた組織内でのリスク評価が，リスク処理方法の選択にあたり，重要な情報となるのである。ちなみに昭和59年11月の世田谷のケーブル火災事故は，そうした事故の可能性は確認されていたようであるが，リスク測定の面からは従来発生した経緯もなく（発生頻度→極小），したがって損失強度の推定はなされなかったのではあるまいか。それ故，組織内でのリスク評価は低く，対応措置までいかなかったと思われる。いわば，組織にとり，たとえ発生頻度が極めて低くとも，損失強度が非常に大となり得る場合の認識がいかに重要かを理解すべきなのかもしれない。

こうした点をふまえ，コンピュータ・システムに関係するリスクの分析のためには，その「目的」・「範囲」を明確にする必要がある。例えば，システム固有の部面，システムと人とのかかわりの部面，システムと資金（移動を含む）とのかかわりの部面，システムと商品（物・情報）にかかわる部面

等である。資金とのかかわりでは，とりわけバンキングシステムが対象となるであろうし，しかも分析の範囲も組織の実態に応じ，明確化しなければならない。また，システムを動かし，利用するのが人である以上，この部面については，特にヒューマン・エラーの分析が不可欠となる。確かに，コンピュータ・システムのセキュリティ関係でハードの側面についてのリスク対応はかなり進展したと思えるが，システムに関与する人間が完全でないがために生じうるヒューマン・エラー関連のリスク，さらには故意ないし悪意によりコンピュータ・システムおよび関連業務に損失をもたらすリスクの問題が発生してきており，これはリスク分析上，避けて通ることのできない領域である。

経営体は，人，もの，金，そして情報をベースにコンピュータ・システムに依存しながら活動を展開している。特に重要なことは，それぞれが，背後に情報を介在させていることである。そのためには，総合的な観点から，コンピュータ・システムをめぐるリスクの分析の枠組みの提示が必要となる。これは，将来の重要な課題であり，コンピュータ・リスク処理にとり不可欠なものである。そこで若干，リスク分析の意義なり，アプローチについて指摘しておくことにする。リスク分析の重要性については，前述のとおりであるが，さらに勘案すべきことがある。リスク処理は，誰が，何の目的のために，どのような条件の基で行うか，ということである。「誰が」の部分は，組織の意志決定者ということで理論上は解決され，「何の目的のために」は組織の目標を阻害するリスクを処理することといえよう。問題は「どのような条件の基で」リスクを処理するかである。無条件のなかでリスク処理を行う組織などありえないし，まして営利企業であれば，利益を度外視してリスク処理のために資金を投入するなどありえないことであろう。この点について，リヴァモア国立研究所で開発されたリヴァモア・リスク分析方法論（ＬＲＡＭ）において（注５），リスク分析を含め，リスク処理についての要約とも言い得る次のような指摘がある。「こうした問題の決定には，リスク分析の主目的が次の点にあることを想起すべきである。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。したがって，システムの損害／サービスの中断をもたらす現存の潜在的ロス・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，システムの管理者は，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方法で達成し得るかに関心をもつことであろう。」。まさに，リスク・マネジメントに従えば，主目的は予算制約下にあって，対費用効果の点ですぐれたリスク処理を行うことであり，このために有効なリスク分析が存在意義をもち得るのである。

3．リスク分析のアプローチ上の留意点

コンピュータ・システムの利用をめぐる問題状況のリスク分析については，リスク・アナリシスとリスク・アセスメントといった用法もあるが，一般に定性的分析と定量的分析の２つがアプローチとして存在している。とりわけ後者については，分析上，どのレベルまで精緻化すべきかといった議論がある。

情報システム・リスク分析のフレームワークにおけるリスクは，「潜在的に有害な作用因および事象（イヴェント）たる脅威の，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(注６)」と認識されている。複雑なシステムにかかわる脆弱性のなかで，多様な脅威との相乗作用により生起するリスクに対し，定性的，定量的アプローチのいずれかにより遂行されるべきかという議論は，重要な問題を不明確にしているきらいがある。システムの脆弱性の把握においても，脆弱性について操作的な概念が与えられなければ，何が「高い」のか，何が「低い」か客観的に

判断できず，したがって，リスク処理担当者への情報とはなりがたい。そのためには，定性的な評価を与える場合にも，いくらからいくらまでを「低い」，いくらからいくらまでを「中くらい」，いくらからいくらまでを「高い」といったアプローチが必要であろう。

また，定量的分析では，定量化の尺度の決定が不可欠である。コンピュータ関連のリスク分析について，一般には，単位時間あたりの望ましくない結果（損失）の発生率が使用されている（注７）が，これも分析の範囲によることになろう。とりわけ，定量的なアプローチの場合，情報システムのリスク処理方法の選択・実施にかかわる費用対効果を提供することが重要である。

次に勘案すべきは，どのレベルまで分析すべきかということである。例えば，ロスアラモス国立研究所で開発されたリスク分析のフレームワーク（ＬＡＶＡ）では，資産範疇の全集合，脅威の全体のスペクトラム，セーフガード・システム集合，セーフガード・システムの弱点に付け入る脅威から生じる結果集合に視点をあてている。しかも，その方法論としては，多層システム論，イヴェントツリー型分析，意志決定論，効用理論，エキスパート・システム論，自然言語処理が用いられている（注８）。例えば，ＬＲＡＭなり，ＬＡＶＡのソフトを用いることは可能であるかもしれないが，情報システム利用の組織は，規模，業種，立地状況等により異なり，必ずしも高度なリスク分析を必要としないと思われる。それだけに，リスク分析の目的・範囲を明確にすることが，前提といえるのである。

４．リスク分析の制約因

リスク分析を第一ステップとするリスク・マネジメントについて，わが国の企業には，そのため率先して費用投下する傾向が少ない。情報化の流れのなかで，多くの企業は積極的にコンピュータの導入を図ってきている。しかし導入に積極的な企業といえども，コンピュータ・セキュリティ関連では，かなり消極的なきらいがある。この点は，リスク処理が企業に利益を直接にもたらさないと判断すれば，一企業だけリスク処理のため費用を投下すれば

それだけ，同業他企業にコストの点で競争上比較優位性を与えてしまうことになるという危惧が関係している。したがって，特定企業が大きな損失を被り，社会的にリスク処理上，費用投下が認知されるまで，消極的であるのが一般的である。横並び的なリスク処理を前提とすれば，リスク分析のためには，対費用効果の点を含め，一般的なフレームワークとして示し得るリスク分析の方法論が必要なのかもしれない。ちなみに，本報告書の試みは，一般的フレームワークへの予備的な考察を意図している。今後の課題については，第２章において言及することにした。

（注１）　これまで，日本情報処理開発協会では，昭和59年以降，『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』を発行してきている。例えば，昭和59年度の調査報告書では，主としてリスク・マネジメントの概念，リスク分析手法に視点を当て，論考している。昭和60年度の報告書は，「コンピュータ・セキュリティ対策実施状況調査」を行い，システム利用の事業体のリスク分析への取り組みの実態を示した。そして昭和61年度の報告書では，小規模の銀行を対象に，コンピュータ犯罪についてのリスク分析の机上実験の成果を示したが，これはコンピュータ・システム利用組織の「リスク分析」のための手掛かりとなった。昭和62年度は，海外文献の紹介に視点をあてた。

（注２）　森宮康『リスク・マネジメント論』（千倉書房）1985年

（注３）　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.

抄訳は，『コンピュータ・セキュリティに関するリスク分析調査資料』昭和63年３月に掲載。しかし，リスク・アナリシスの他に，リスク・アセスメント・アナリシスといった表現から，前者については，

資産の確認，リスクの確認，リスク発生の確率の決定，損失発生時のインパクトないし影響の決定を，後者については，合理的で秩序だったアプローチで，問題確認，確率決定に対し包括的な解決策を示し，推定に強調点を置いた理解が見られる場合もある。例えば，James F. Broder, Risk Analysis and the Security Survey, Butterworth Publishers, 1984.

（注４）～（注７） Guarro, Sergio B, Ibid..；『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

（注８） Smith, S.T., Lim, J.J., Philiips, 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.; 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.

第2章

バンキングシステム・モデルにおけるリスク分析実施例

1．モデルによるリスク分析

(1) バンキングシステムを対象

わが国でコンピュータおよび通信を利用した大規模ネットワークシステムの構築が積極的に進められてきた分野の１つは，バンキングシステムであるといえる。そのバンキングシステムは，規模の大きさ，システムの先進性だけでなく，システムの内容が市民生活に密着した機能を有するといった特徴もそなえている。したがって，コンピュータ・システムの代表例としてとりあげるのにふさわしいと考え，今回リスク分析の対象にとりあげた。

① 金融機関においてはすでに昭和40年代初期に預金業務のオンライン化等第一次オンライン・システムが稼働し，昭和50年代には預金，融資，為替など主要業務をカバーする全科目，全店ベースの総合オンラインである第二次オンライン・システムが稼働した。さらに，昭和60年代に入ると，都銀を中心として，ファームバンキング，ホームバンキング等，対顧客サービス拡大のための対外接続システムを含む第三次オンライン・システムが動き出しつつある。このように，バンキングシステムは，他の分野に先がけてシステム化，ネットワーク化が着実に進展している。

② バンキングシステムは，ＣＤ，ＡＴＭの利用にも見られるように，一般市民（消費者）に最も直結した身近なシステムの１つであり，それと同時に，万一トラブルが発生した場合には市民生活に大きな影響を及ぼすシステムでもある。このようなバンキングシステムの位置づけ，役割，その重要性からいって，今回のリスク分析の対象としてとりあげるのは適していると判断し，モデルとしてふさわしいと考えた。

(2) 内国為替業務

金融機関のシステム化の進展によって，大きな変化があったことの１つが決済のあり方である。その結果，決済機構の安全性・信頼性の確保のためには，コンピュータ・システムの安全性・信頼性の確保が不可欠の条件となっている。したがって，決済にかかる主要な業務の１つである内国為

替業務についてリスク分析を行うことは有意義であると考えた。

① 金融機関の決済の方法は，システム化の進展に伴い，現金，手形，小切手などの紙ベースの決済に加えて，電子送金をはじめとしたエレクトロニック・ベースの電子資金移動（ＥＦＴ）が急増し，昭和62年度には全銀システムによる振込件数が全国手形交換枚数を上回る状況となった。

さらに，今日ではファームバンキングの１つの機能として，企業のパーソナルコンピュータやプッシュフォン，キャプテン端末等を利用して金融機関のコンピュータに直接アクセスし，資金移動を行うことも一般化しつつある。（ノンバンクにおいても，例えばＶＡＮ業務で，企業間の決済に係る相殺および決済データの集計・分類など実質決済機能を果たすサービスも現れている）。

② 決済機能にとって極めて重要なことは，そのしくみの安全性・信頼性の確保であり，電子資金移動においてはそのための条件としてコンピュータ・システムの安全性・信頼性を欠くことはできない。

したがって，電子資金移動の代表的な業務である内国為替業務を選んで今回リスク分析を行うことは，業務の重要性，影響の大きさからいって有意義なことであると思われる。

2．バンキングシステム・モデル

本報告書では，小規模銀行支店における内国為替システムの振込処理モデルを構成し，リスク分析ならびにその評価の一部を実施した。ここでのリスク分析においては，リスクの発生が企業に与える影響の定量化の一手法の紹介を行い，リスク処理の種々の対策およびリスク・マネジメントのための体系化は今後の研究に委ねることとした。

(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銀行店舗のシステムを中心とした。なお，コンピュータセンターのシステムは，通商産業省の策定した「電子計算機システム安全対策基準」に基づく安全対策が一応

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，分析のために仮定した小規模銀行における小型支店であり，概要は次のとおりである。

(a) 業務内容

預金，内国為替，貸付を中心とした普通銀行

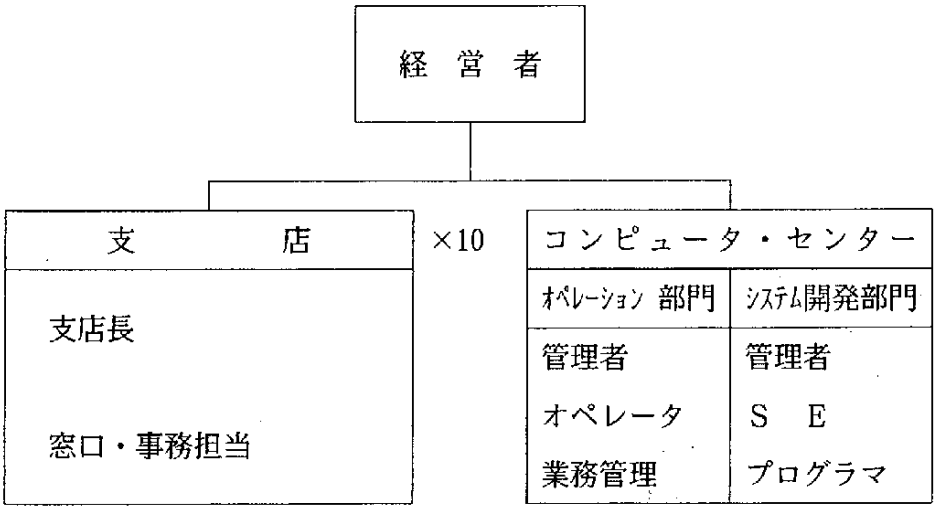
(b) 業　　容

・支店数　10

・各支店の平均保有口座数　1,000

・来店客平均　100人／1日

(c) 関連組織



(d) 内国為替の振込業務受付手続き

受付窓口では，顧客より「振込依頼書」と振込依頼書記載の金額および振込手数料を「現金」（または，預金通帳と預金払出票など現金に相当するもの）で受取る。

窓口担当者は，振込依頼書の記入項目洩れのチェックと現金照合を行ったあと，振込依頼書と同時複写された「振込金受取書」に受領印と担

当者印を押捺して顧客に返却する。

受付けた振込依頼書には，受付機（テラーズマシン）で受入金額，振込金額，振込手数料，つり銭を確認印字し，現金を所定の箇所に保管のうえ責任者のチェックを受けた後で，内国為替の処理部門に回付する。

(e) 内国為替の振込業務処理（図1参照）

受付窓口より回付された振込依頼書（「伝票」として取り扱い）に基づき，次の処理を行う。

① 振込依頼書各項目の記入洩れ，記入誤り，および担当者印，責任者印の押捺洩れチェック。

② 端末機入力操作

振込先銀行，店名（またはコード）

取引種目（振込として入力）

振込金額

振込先の預金項目（普通，当座など）

振込先口座番号

振込先口座名

振込依頼人氏名

入力完了キー

③ 入力確認

端末入力控と振込依頼書の項目チェックを行い，照合担当者印および責任者印を押捺する。

④ 振込伝文送信処理

入力確認が終了した端末機入力操作済の伝文を「全銀センター」を経由のうえ，相手先銀行に発信する。

(f) 内国為替の窓口業務終了後の処理

窓口受付業務終了後，次の処理を行う。

① 窓口保管現金残高，振込依頼書金額および手数料との照合。

② センターより指定端末機に出力される端末入力振込処理件数，金額

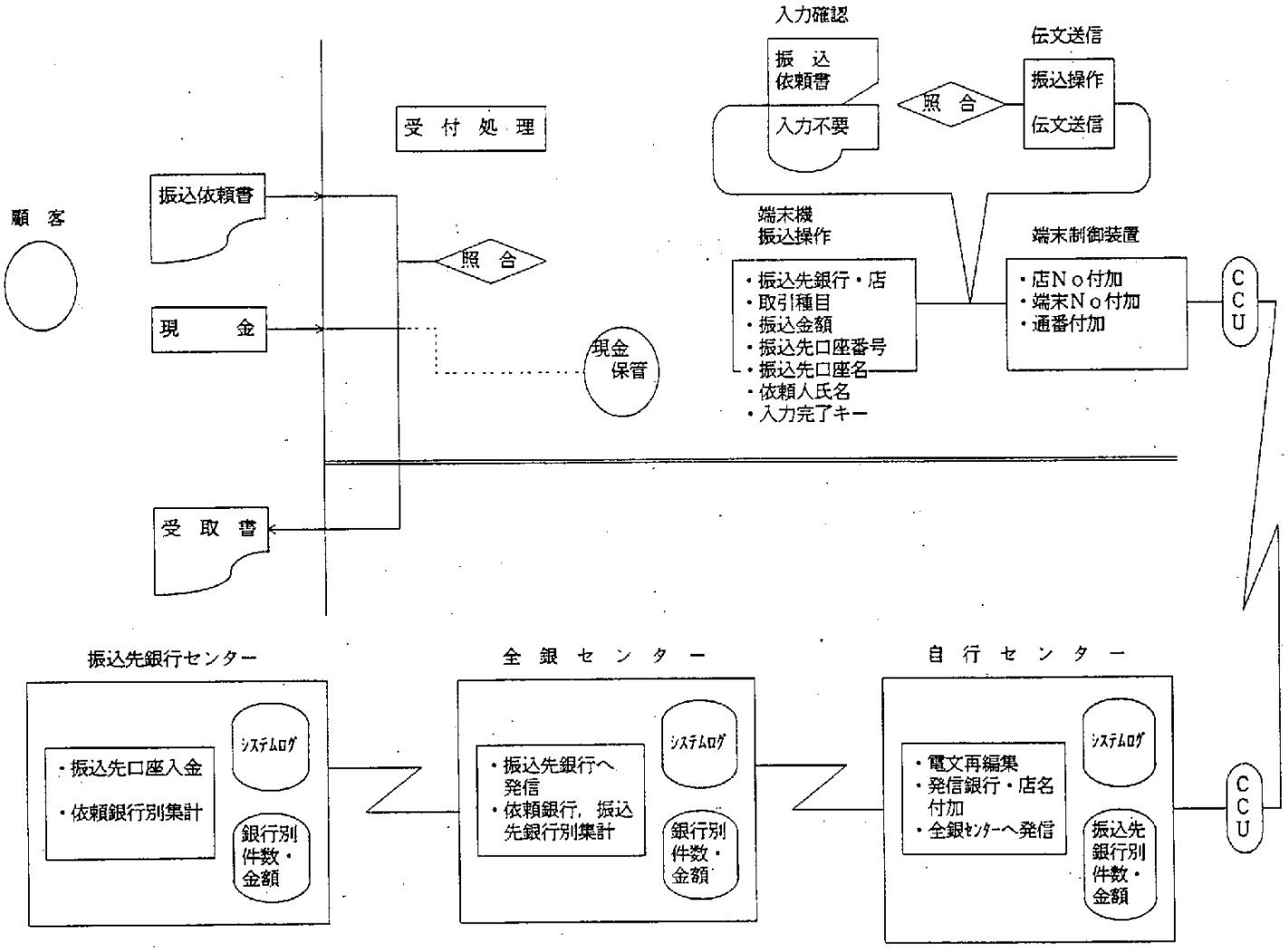


図１．内国為替の振込業務処理

と振込依頼書の枚数，金額の照合。

③　端末機より①②照合済（または照合不一致のときは修正処理）入力。

④　窓口保管の現金残を回金票に明記して現金統括セクションに引き渡す。

(g)　コンピュータセンター，オペレーション部門の処理（図2参照）

①　オンライン・システム開始処理（全銀センターへのオンライン開始処理を含む）。

②　システム稼働状況監視。

③　オンライン・システム停止処理。

④　取引記録ファイルなどのバックアップコピーをとり保管。

⑤　オンライン・システム終了処理（全銀センターとの照合，確認処理を含む）。

⑥　当日分のシステムログに異例な記録がないことを確認。

(h)　現在実施されているセキュリティ対策（主として不正防止対策）

①　支店の端末はオペレータキーをセットしないと動かない仕組みになっており，このキーは業務終了後は管理者が翌日まで保管する。

②　各人が使用するオペレータキーは特定されており，どのキーによって入力された取引かは，事後，セキュリティの取引記録ファイルからトレースする仕組みにしている。

③　1日分の振込依頼書は，10年間保管する。

④　センター障害時は，全銀システムで予め定められている方法で振込処理を行う。

⑤　1日分の振込処理の件数，金額は，全銀センターと照合を行い一致していることを確認する。

⑥　センターコンピュータ室は，オペレーション部門，システム開発部門の者以外は，立入りを禁止している。

⑦　システム開発部門の者がテスト等でコンピュータを使用する際は，必ず定められたアカウント情報を入力することとする。

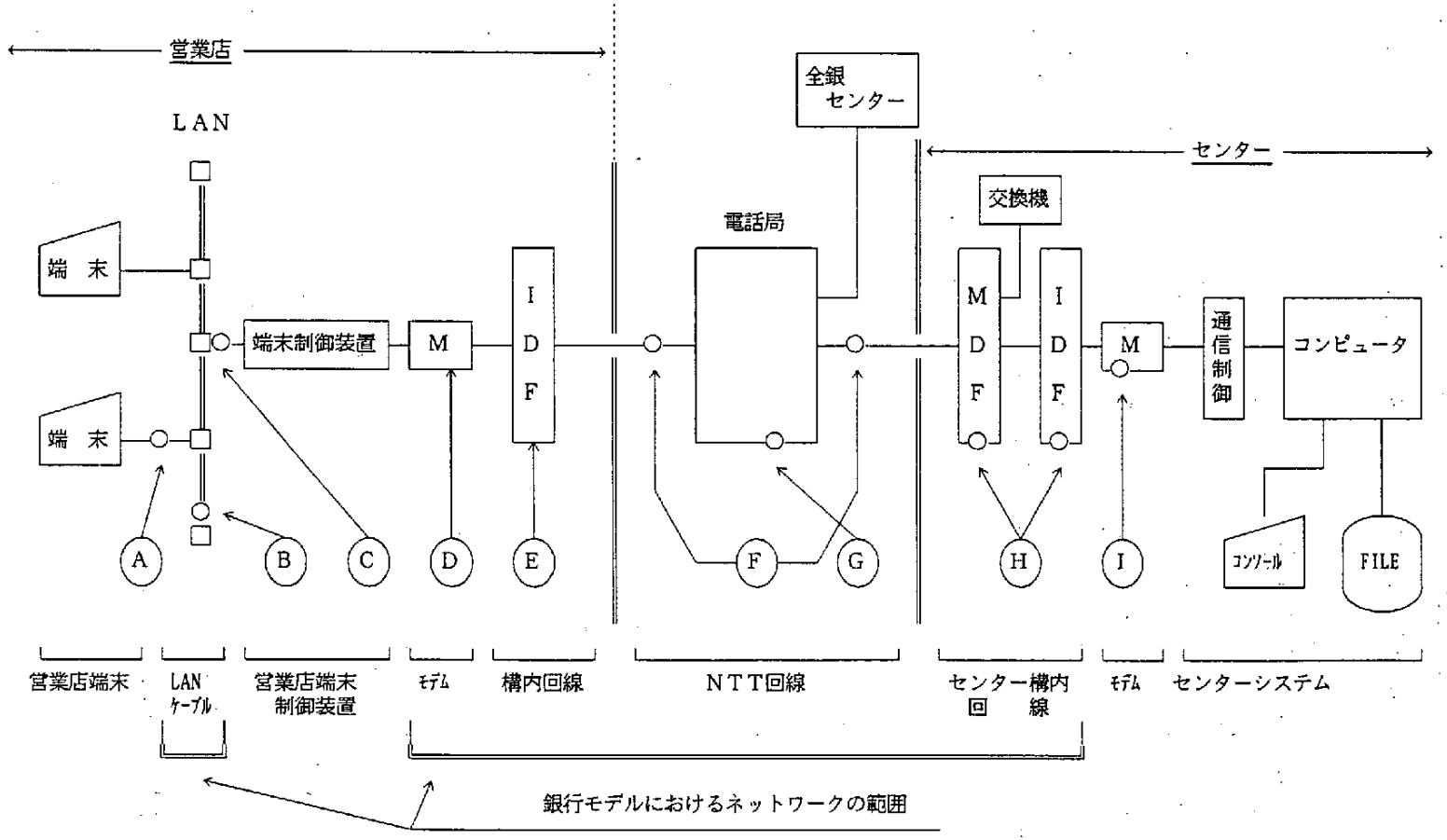


図2．銀行モデルにおけるネットワークシステム

⑧　システム開発部門の管理者は毎日，前日に部員がコンピュータを使用した実績記録（システムログ）をチェックする。

3．リスク分析の手順および方法

(1)　リスク分析の手順

リスク分析では，組織にとっての阻害要因たるリスクを処理するための情報を提供するのが課題となる。そこで，何が組織の業務を妨げるのか，システム利用の組織であれば，対象となるシステムにからむ事故事象が何であるのか，またそれがいかなる原因によるのかの明確化が前提となる。いわば，事故事象とその原因を因果関係の連鎖のなかで把握するのである。とりわけ複雑なシステムを利用する場合には，因果関係が明確に分岐していない場合もあるが，リスク処理のためには，原因への対処が重要となるがため，この点は軽視すべきではない。

さて，リスク分析の手順は，次のとおりである。

①　事故原因の洗い出し

②　損失タイプの確定

③　損失事故の発生頻度，潜在的損失強度（大きさ）の把握

④　損失強度の評価（組織にとっての相対的影響度の評価）

⑤　リスク処理のための優先順位の決定

⑥　リスク処理方法の対費用効果の把握

リスク分析では，上記のことが決められるような情報を求めるのである。ここではバンキングシステムにおける考察対象を取り上げ，事故事象の明確化に重点をおいたがため，リスク分析の手順の全てを扱えなかったことをことわっておきたい。

(a)　事故原因の洗い出し

①　業務事故事象

バンキングシステムを利用する組織（ここでは小規模な銀行）にとり，対処しなければならないのは，業務に関する障害である。これを，

「業務事故事象」と呼び，リスク処理の対象とする。近年，特に，システム利用が複雑・多様になってきているがため，そこに支障が生じると，システムにより処理している業務自体に多大な影響が生ずる。したがって，「業務事故事象」を勘案する時，何が原因で生じたのかが問題となる。その場合，原因のひとつになるのが，システム事故に起因する業務への障害である。

② システム事故事象

システムは，常に予定されたとおりに稼働するとは限らない。例えば，システムに何等かの事故が発生することにより，システムが期待どおり稼働しないことがある。こうした事故を，「システム事故事象」と呼ぶことにする。これには，システム停止，システム縮退，システム誤作動に類型化することができよう。

③ 原因集合

システム事故事象の把握にあたり，重視すべきは，いかなる原因により生じたのかの原因分析である。この原因の洗い出しにあたっては，事故事象の直接の引き金になった，因果関係の明確な事故原因，またそれを引き出した原因，さらにはその原因，といったようにブレークダウンすることが可能である。これらの事故事象にとっての原因群を総称して「原因集合」と呼ぶ。

(b) 損失タイプの確定

損失のタイプには，いくつかの分類がみられる。例えば，ウィリアムス＝ハインズによる分類では，財産損失（直接的損失＝損害を被った財産の取り替えないし修理等に関連する／間接的喪失＝直接的損失を被ったことによる財産の残存物の取り壊し等による／純収益の喪失＝直接的損失の結果，事業中断等による），賠償責任損失（他人の財産の破壊なり第三者への傷害等から生ずる），人的損失（従業員等の死亡，労働不能等による組織自体への損失・従業員等の死亡，労働不能等による家族への損失）（注１）と３タイプに分類されている。また，上記のうち，

純収益の喪失を独立にとりあげ，３タイプに加え，４分類としている論者（G．ヘッド等）もいる。

ここでは，若干，視点を変え，事故事象とのかかわりからアプローチすることにする。まず「損失」は，事故の結果，喪失ないし減少した有形無形の資産への損失が中心となるが，さらにその影響を最小限に抑えるために投入する諸費用も勘案しておく。これらを損失の性格に応じ，次の２つに分類し，費用とあわせ３タイプをここでの対象とする。

① 直接的損失 → 事故発生により直接被る損失（例えば，窃盗犯罪により詐取された金額（直接に金額として表示しがたい場合には，その金銭的評価額）とか，器物破損の場合では，破損により消失した資産価値など）。

② 間接的損失 → 事故発生後，間接的ないし波及的に生じる損失で，事故の影響を分析することにより明確化されるといった性格の損失（例えば，業務事故の結果，損害賠償の請求を受けた場合の損害賠償金とか，業務活動に支障が生じたことによる損失，信用低下による損失など）。

③ 対応費用 → 上記の損失を最小限に抑えるため，事故後に投下する費用（例えば，詐取された金銭を取り戻すために要する費用とか，賠償金支払を回避するための折衝費用，裁判費用，低下した信用を回復するための費用など）。

とりわけ間接的損失か対応費用かの判別がかなり難しい場合もみられようが，性格から①，②を減少させる関係にあるか否かの観点から整理し判別するのが良い。

表1．損失タイプ例

直接的損失	詐取された金額 端末破損額 etc.
間接的損失	損害賠償金 事故調査費 折衝費 etc.
対応費用	信用回復費 裁判費用 etc.

(2) 事故事象の分析の手法（とくに①，②のために）

事故事象分析の手法には種々の指摘があるが，ここでは，次の3つのアプローチを示しておくことにする。

(a) ブレーンストーミング

事故事象とその原因の洗い出しのため，過去の経験なり，他の企業の実態などに熟知している関係者が意見を出し合うことにより，当該事故関連について先見的な情報を得ることが可能となる。互いの意見をベースに刺激しあい，知識を飛躍的に増大させる方法といえよう。

(b) 要因系統図の作成

業務事故事象とその原因集合およびシステム事故事象とその原因集合

について，ツリー構造による系統図を作成する。これにより事故の連関関係を把握することが可能となる。その場合，それぞれの事故関連の因子を要因とし，この系統図を「要因系統図」と呼ぶ。

(c) 総合関連図

上記の2つの要因関連図を作成し，これを1つにまとめる。この図を「総合関連図」と呼ぶ。この図により，全体の連環関係が把握できるのである。

(3) リスク評価へのアプローチ（とくに③，④のために）

これまでの作業に基づき，把握したリスク関連情報から，組織にとってリスクの評価がなされねばならない。ここでは，当該モデルに関するリスク評価のため，業務事故事象により現実に生じると想定される金額を把握する方法（金額評価法と呼ぶ），損失規模を何段階かの範疇に分類し影響を把握する方法（カテゴリイ評価法と呼ぶ），さらに事故事象の発生に関係する要因を抽出し発生確率を求め，影響を評価する方法（確率評価法と呼ぶ）の3方式を勘案してみた。それぞれに簡単な解説を付しておくことにする。

(a) 金額評価法

今回のモデルにおける損失規模の金額評価のため，表2のようなワークシートを構成した。表頭には具体的に損失をもたらす業務事故事象をあげ，表側には事故にかかわる損失ならびに事故処理に関する費用を明記する。表側のそれぞれの項目については，上記の直接的損失，間接的損失，対応費用関連の項目を示すのがよい。そして，当該事故事象により発生すると思われる損失額および関連費用，それも可能性として上限の金額を記入するのである。これにより，事故事象が発生した場合の，最大の損失規模を見積もるのである。リスクを処理する意志決定者としては，リスク対応上の優先順位を損失規模の大きさから判断することが可能となろう。

表2　ワークシート

	事故事象 / リスク対応	業務に結果として現れる事象							
		入金が遅れた		客から振込依頼がないのに他銀行（口座）に振り込まれた		振り込み依頼されたが相手先に届かなかった		依頼された金額と振り込まれた金額が違う	
		犯罪	エラー	犯罪	エラー	犯罪	エラー	犯罪	エラー
直	誤振込金								
間	事実の確認調査経費 ・手続きを確認する経費 －他行の手続き確認依頼								
間	・システム・チェックに要する経費 －自行システムの確認 －他行システム調査依頼								
間	事実確認後 ・振込金回収のための経費 －通信費／手土産 －謝罪のための人件費 －銀行間の謝罪経費								
間	・振込人に対する謝罪経費 －通信費／手土産 －謝罪のための人件費								
対	・振込先に対する謝罪経費 －通信費／手土産 －謝罪のための人件費								
間	・原因が明確になるまで一時的に業務停止のロス								
対	事後回復作業経費 ・振込金回収のコンピュータ運用費								
対	・システムの修正作業に要する								
間	・交渉経費								
間	・示談経費								
間	・対マスコミ対策費								
対	再発防止の諸経費 ・再発防止の通達								
対	・再教育費								
対	・手続き手順書改定								
対	交渉後の経費 ・裁判経費（人件／調査）								
間	・賠償金								
間	信用回復費 ・謝罪広告経費								
間	結果損失（信用低下） －預金者数の減少 －預金高の減少								
間	・監督機関への対策費								
	合　計								

（注）直は直接損失，間は間接損失，対は対応費用

(b) カテゴリイ評価法

損失の発生頻度さらには損失規模について，事故の特定発生回数，損失の大きさを「いくらからいくらまで」をそれぞれ「大」「中」「小」といった範疇に分け（３段階評価の場合），影響の度合いを評価する方法である。

今回のモデルにおける損失規模の評価では，損失関連の項目たる直接的損失，間接的損失，対応費用について，例えば，５段階評価と採択するとすれば，金額の大きさに従い，Ａ～Ｅの段階を設定し，対応のための判断情報を示すのである。その際，重要なのは，組織内において，人が変われば評価が異なるといったことのないように，損失規模に関する判断に差違が生じないよう合意を得ておくことが肝要である。例えば，客観的に判断しうるように，金額値として，いくらからいくらまでを何円といった表示を，５段階評価について例示すれば，次のような表示となろう。

Ａ　10万円以下の軽微な損失

Ｂ　10万円超100万円以下の損失

Ｃ　100万円超1,000万円以下の損失

Ｄ　1,000万円超１億円以下の損失

Ｅ　１億円を超える損失

(c) 確率評価法

事故事象により生ずる損失の発生頻度について，前述の分析方法に基づいて，ある程度の頻度確率が得られるかもしれないことを前提としている。この点については，図３のような流れ図が参考となろう。

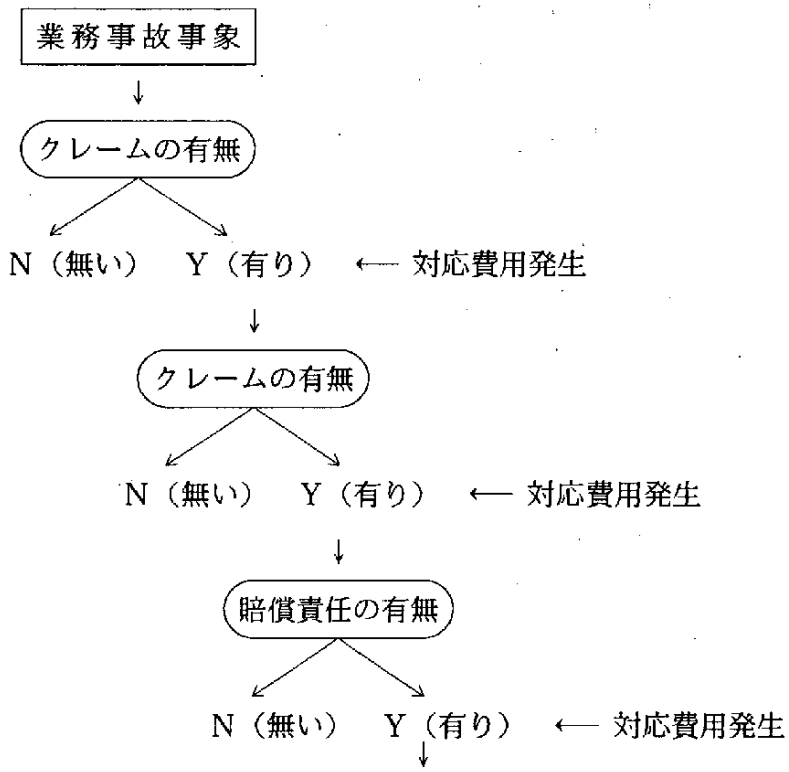


図３．間接的損失の分析例

(4)　リスク処理のための優先順位の決定（⑤に関連して）

これまでの分析を通して，組織にとり何が最大の問題となりうるかを確認することになる。事故による損失額そのものが，リスク対応上の優先順位の決定のための情報となるはずである。その際，直接的損失の評価もさることながら，間接的損失の評価にウエイトを置くべきことを強調しておきたい。特定の事故事象のもたらす損失額に鑑みて，組織として関係者の合意のもとにリスク処理上の優先順位を決定すべきである。

(5)　リスク処理方法の対費用効果の把握（⑥に関連して）

今回のモデルによる損失の評価では，「電子計算機システム安全対策基準」に基づく安全対策が一応できていることを前提としていることから，リスク対応については，それ以上の安全対策，とりわけ物理的対策，技術的対策が対費用効果の点で望まれるかもしれないが，業務事故事象の関係

からは主として管理的対策にウエイトが置かれることになろう。求められる管理的対策は，物理的対策，技術的対策の場合に比べ，費用に対して効果の点で必ずしも明確化しがたい面もある。本報告書では，対応費用の項目の指摘とその期待効果について後述しておくことにする。この場合の対策は，リスク処理上，損失発生後の資金的手当としてのリスク保有（組織内で負担）ということになり，リスク・マネジメントにおけるリスク対応の部分を包含する形となろう。

（注１）C.A.Williams, Jr. and R.M.Heins, Risk Management and Insurance, 6th Edition, McGraw-Hill Book Co., 1989.

4．業務事故事象とシステム事故事象

モデルに従い，バンキングシステムの営業店における事故事象について，それらを整理し，さらに原因とみなしうる事項（原因集合）の洗い出し作業を実施し，その結果のパターン化につとめた。

(1) 業務事故事象の洗い出し

コンピュータ・システムにおける事故（障害）が如何なる形で業務に影響を及ぼすかを考えてみたい。この例では内国為替を扱い，その営業店の立場にたって考えてみることにした。これは，極端ないい方をすれば，銀行へ顧客から苦情がくるのは如何なる場合であるかを想定してみた。これは例題であり，業務を他銀行間との為替業務の一部に限定して，業務に現れる状況について洗い出すことにした。その結果，条件や過程はともあれ次の4つのパターンに業務事故事象を集約することができた。

(a) 「依頼が無いのに他人の口座に振り込まれた」

顧客が自分の口座を確認したところ，入金するはずの無い金銭が入金していたことに気づいた時に銀行の処理方法（オンライン・システム）に不安を感じ，あるいは振り込み主に不気味さを感じて銀行に苦情を申し込むことになる。つまり，その顧客に対して振り込み依頼が無いのに（振込予定が無いのに）顧客（自分）の口座に勝手に振り込まれたことになる。これも顧客に気づかれる前に銀行が察知し，正しく訂正しておけば苦情として表面に現れることがなく事が終わる可能性がある。しかし，顧客がその金額を払い戻した後に銀行が気づくことになると，問題はことによっては面倒な扱いになり，問題解決に時間と経費を要することになる。

(b) 「振り込み依頼されたが相手先に届かなかった」

顧客の口座に振り込まれるはずの金銭が振り込まれていない。振り込み人が相手先に振り込んだ事を連絡し，それをもとに口座を確認したが入金されていなかったので，銀行に苦情を申し立てることになる。振込窓口の銀行が正しく振込依頼を受けていることが確認されれば，振込人

が振込手続きを完了していることになるので，当然それ以降の工程で正しい処理がなされなかったことになる。

以上の２つの業務事故事象は，実際は１つの現象として現れることが多い。となると「振り込み依頼されたが他人の口座に振り込まれてしまった」ということになるが，ここでは２つの現象としてみることにした。

(c)　「振込依頼された金額と振り込まれた金額が一致しなかった」

顧客（受取人）へ入金された金額が，振り込まれた金額と一致しない場合，振り込み金額が少なく振り込まれたときは直ちに苦情となって現れることになる。金額が少なく振り込まれたときの顧客の不満と不信は非常に大きいものになることは想像できる。予定より多く振り込まれた場合は苦情にならないかもしれないが，そのまま引き出されててしまえば，他銀行間との振り込みの場合，いずれかの銀行に損失（保障，弁済等）が発生することになるであろう。

(d)　「入金が遅れた」（予定の期日までに振り込まれていなかった）

顧客（自分）の指定口座に受け取るべき金額（全額）が予定（必要）の期日までに入金されていなかった。そのために，受取人がその金額を使用することができず迷惑（損害）を被ったときに，銀行（支店）に対して苦情（調査依頼）を申し込むことになる。

振り込まれた為替は，翌日まで，遅くても翌々日までに相手先に届くのが一般的な常識になっている。遅れたから必ず苦情に結びつくものではない。支店の手違いで数日遅れても，受取人が直ちにその金銭を必要としなければ，全くその業務の事故事象は表面に現れることなく終わることになるのである。

いわば，大きく分類すると，以上のような４つの現象が業務に現れる業務事故事象になるといえよう。

(2)　業務事故事象と原因集合

ここでの要因分析は，深さをどこまでに留めるかを決めることが必要になる。要因追求の深さは，評価を行うときの考え方によって大きく変化す

る。リスクの評価は，１回の損失額と発生確率から求めることが一般的な常識になっている。しかし，１回の損失額が算出できるものとできないものがあり，また，発生頻度を想定することが困難なものがあることも通例になっている。要因の追求を発生確率と損失額の想定ができる深さまで追いこんでも，極小の数字を操ってみても現実性がなく無味乾燥になってしまうと考え，リスクの大きさを人が感覚で大まかに判断できるところで要因の分析は留めることにした。

このような前提のもとに，前述の４つの業務事故事象の原因集合を，以下考察することにした。

ｹｰｽ ａ．「依頼が無いのに他人の口座に振り込まれた」

知らないうちにある口座に入金していたという現象は，振り込み依頼されたが正しい受取人の口座に入金されず，間違った口座に入金した場合が多いと考えることができる。しかし，ここでは単独に発生したことにする。原因としては，営業店の作業は考えられず，センターシステム障害に起因する適用業務プログラムのエラー，ハードウェア障害，ソフトウェア障害等が考えられる。

ｹｰｽ ｂ．「振り込み依頼されたが相手先に届かなかった」

振り込み依頼が正規の受取人に届かない。間違った処理の結果発生する現象である。原因を考えると，振り込み依頼者が相手先口座を間違えて記入する，伝票の記入が不鮮明で端末機入力する操作員が口座番号を読み違えて作業を行う，あるいは端末入力を間違う，また端末機，端末制御装置の障害により口座番号が間違うこと等が考えられる。以上，営業店内部の作業による事柄と営業店外がある。ネットワーク障害や通信障害によって引き起こされる場合もある。

ｹｰｽ ｃ．「振込依頼された金額と振り込まれた金額が一致しなかった」

振込金額と入金額が一致しない原因は，受付処理で記載金額と現金が一致していない場合の照合を怠りその処理が実行された場合，記載された金額が不明確であり，端末操作員が間違えた金額を入力した場合，端

末機や端末制御装置の障害により金額を間違えた場合，ネットワーク障害により金額が間違えられた場合，センターシステムや適用業務プログラムの障害により金額が間違う等が考えられる。

ｹｰｽ d　「入金が遅れた」

入金が予定される期日までに入金されなかったがその後に入金した場合の原因としては，センターシステムの障害により振込作業が遅れた場合，ネットワーク障害により振込作業が遅れた場合，営業店の手違いで振込作業が遅れた場合等が考えられる。

(3)　システム事故事象の把握と類型化

システム事故事象を整理する上で重要となるポイントは，コンピュータ・システムの正常稼働（銀行業務）に影響を及ぼす可能性のあるシステム事故事象を漏れなくリストアップすることである。システム事故事象としては，次の３点が考えられよう。

①　システム停止（システムダウン）

②　システム縮退（機能を一部停止して，システムを稼働する）

③　システム誤作動（予期せぬ操作を行う）

直接的にシステムそのものの事故事象とは言いがたいが，システム関連の事故原因には次の２項目が考えられる。

④　エラー（過失）（ソフトウェア障害は全てエラーとして捕らえることができる。ここでは「取り扱いに関するエラー」としてプログラムは含まれないことになる。銀行業務関連では，窓口の取り扱いに関する手続きと書類の不備／損失等と各種機器の操作や端末を使用した適用プログラムのオペレーションに関するエラーということになろう。）

⑤　悪意／故意による行為

これらの事故原因を営業店における事故事象として現象面から類型化すれば，次のとおりである。

①　営業店システム障害

営業店内部に起因するシステム障害

② 通信障害

営業店から見る外部接続に関する障害

③ エラー，故意／悪意

営業店，システム運用等に関する全てを含む人的エラーと故意あるいは悪意による行為

なお③はシステムに関わること以外に，手続き，規定，システム機器以外の操作等も含むことになる。

(4) システム事故事象と原因集合

次に，営業店の業務遂行にかかわるシステム事故事象について，現象面から類型化した前述の指摘にもとづき，その原因をランダムにリストアップし，図4のモデルシステムに沿って整理してみることにする。

なお，システム事故事象に対する原因集合の細部に及ぶ掘り下げは，このリスク分析の必要性に応じるものとする。

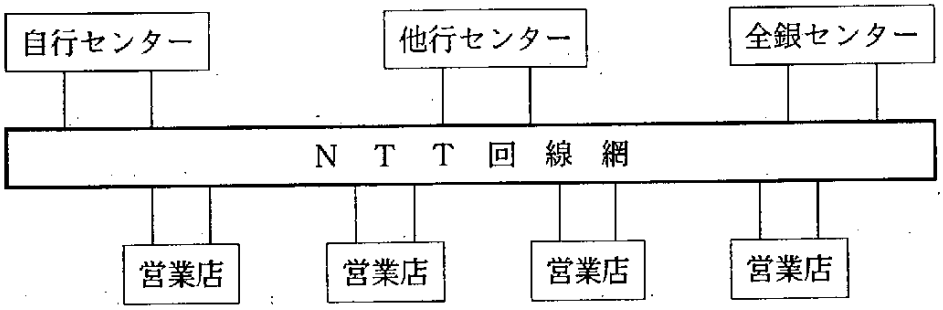


図4．モデルの概念図

(a) 営業店システム障害

営業店内部の要因は「営業店システム障害」として表わす。営業店にかかわるシステム障害は，回線の切断／クロストーク／ＩＤＦの接続に不良等の構内回線障害である。次に端末制御装置／端末機器／モデム／ＬＡＮ関連機器等の構内回線にかかわる構成機器の障害がある。それに加えて，全ての機器／装置にかかわりのある電源に関する障害がある。

(b) 通信障害

営業店システム障害は，営業店の内部で発生する障害のことであり，それ以外を外部として扱った。外部との接続は，一般的に通信回線を介して行うことから「通信障害」として表わした。当然のことであるが，営業店システム障害により通信障害を引き起こすこともあるが，ここでの通信障害は，営業店のシステムは正常稼働可能の状態にあるとの前提で考え，この原因集合には営業店システム障害による通信障害は含まないことにした。すなわち，ここで言う通信障害とは，システム事故事象につながる外部の原因集合の総称とする。そして，通信障害は通信システム障害と回線障害の２つに分けることができよう。

① 通信システム障害

このモデルのバンキングシステムに関するセンターシステムは，自行のセンターシステム，他行のセンターシステム，それに全銀センターシステムであり，いずれかのセンターシステムで障害が発生するとシステム事故事象につながる。

各センターごとに事故事象の原因を洗い出しても，究極的には各センターシステム共通になってしまう。適用業務プログラムのバグ，オペレーティングシステムのバグ，ハードウェアの障害（機器障害）等がシステム通信障害の原因集合となる。このモデルケースはオンライン・バンキングシステムであり，特別に通信制御関連のプログラムのバグを別途扱いにした。

各センターシステムの障害は「システム停止」，「システム縮退」，「システム誤作動」のいずれかの現象になる。

これらについての原因を深く掘り下げることは，このリスク分析において，後述するリスク評価の方法に直接関係しないので，このレベルで留めた。

② 回線障害

回線障害とは，営業店とセンターを接続するネットワークに関連す

るセンター構内回線とＮＴＴが管理している回線網に関する障害を言う。センターの構内回線障害は，前述した営業店システムの障害と同じく回線の切断／クロストーク／ＩＤＦの接続障害が含まれる。またモデム／ＬＡＮ等の機器障害である構成機器の障害があげられる。

(c) エラーと故意／悪意

ここで言うエラーは，操作／判断する人が犯すミス（過失）のことであり，機器のエラー，回線のエラー，ソフトウェアのエラー等は「～の障害」に入れ，これには含まないこととした。また，故意と悪意は，エラーと現象がほとんど同じである。これは，営業店からシステム運用に関して人が介在する工程の全てにかかわることになる。

また，エラー，悪意／故意の行為のほかに，システムの正常稼働を保つために必要な共通項としては供給電源の確保，空気調整設備等も当然考えることになるが，ここでは省略することにした。

(5) 業務事故事象とシステム事故事象との関連

業務事故事象とシステム事故事象の原因集合とを結びつけることは，事故の因果関係等の把握にとり重要である。この点を示したのが図５である。

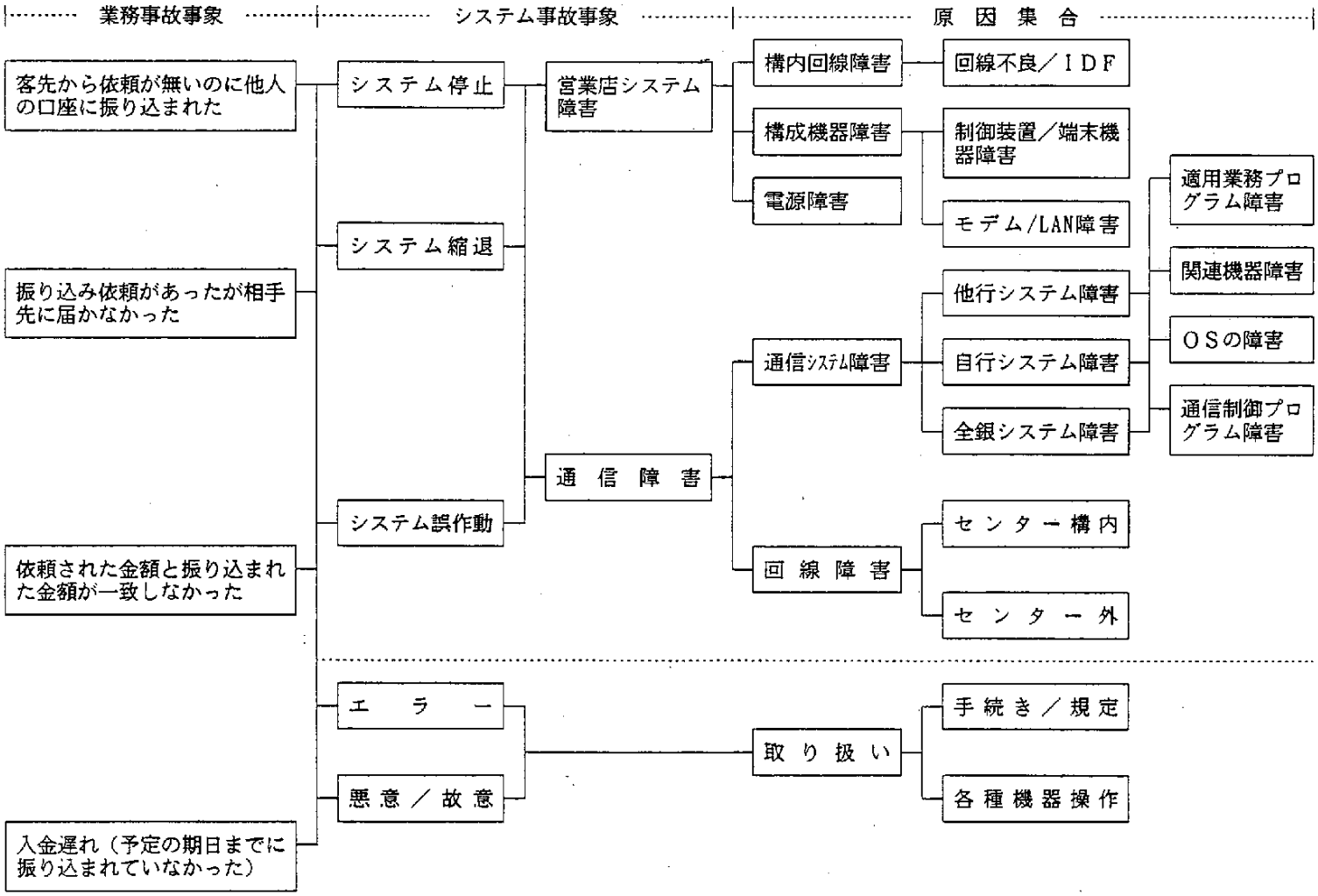


図５．事故事象・原因関連図

5．業務事故事象の損失評価

前述のモデルに従い，バンキングシステムの営業店における業務事故事象から生ずると想定される損失について，事故発生のシナリオをベースに整理し，確定作業を実施してみることにする。

(1) 損失タイプの確定

1つの業務事故が発生した場合においても，それに伴い数種の損失を被るのが一般的である。損失規模の評価に先立ち，当該事故により生じ得る損失のタイプを明確にしておくことにする。ここでは，業務事故発生により通常考え得る最悪な状態（→一番多い種類の損失を被るような状態）を仮定し，事故発生から対応までのシナリオを描くことにより，損失タイプを洗い出してみる。

その際の業務事故としては，「振り込み依頼を受けたにもかかわらず，誤って他人の口座に入金された」ケースを例として採択することにした。（前述の業務事故事象の洗い出しの部分では，「依頼が無いのに他人の口座に振り込まれた」と「振り込み依頼されたが，相手先に届かなかった」という2つの事象として考察しておいたが，一般的に上記の現象形態として現れることが多いために，この事象を用いることにした。とくに，シナリオの右側に損失タイプを併記し，理解しやすいように配慮しておいた。

なお，このシナリオに関連した損失を，直接的損失，間接的損失，対応費用に分類したのが表3である。

事故発生からその対応までのシナリオ	損失種類
A銀行a支店では顧客甲氏より次のようなクレーム申し出を受けた。「5日前ここでB銀行b支店の乙氏の口座に3百万円の振込を依頼したが，乙氏から届いてないと言われている，どうしてなのか説明してもらいたい」	クレーム応対費用
甲氏持参の振込依頼受理票をもとに保管してある帳票を調査したところ，たしかに当日受け付けていたことを確認した。さらに調査を続けた結果，A銀行側のミスでこの3百万円はB銀行b支店の丙氏の口座に入金されてしまっていた事が判明した。	事実関係調査費用 誤振込金
A銀行は，甲氏に対して粗品を手渡し丁重に謝罪するとともに，銀行の資金を充当して乙氏の口座宛3百万円の振込を即刻実施した。またA銀行は，B銀行b支店に対し丙氏に振込した3百万円はミスであったので取り消してもらいたい旨依頼したが，すでに引き出されており取り消しはできないとの回答であった。	依頼人への謝罪費用 再振込事務経費 誤振込金回収費用
A銀行は丙氏に直接交渉し，3百万円の返還を請求したが「すでに商売に利用してしまっておりすぐには返せない」と拒否されたので，専門チームに返還交渉を委ねることとした。	誤振込金回収費用
翌日，今度は乙氏が甲氏を伴ってA銀行a支店に来訪し，「事情は甲氏から聴いたが，この3百万円は重要な取り引きの手付けに使う予定だった。入金が5日も遅れたため絶好の取引機会を逃がすことになっただけでなく，取引先に対する信用も失ってしま	

事故発生からその対応までのシナリオ	損失種類
った。この損失は5千万円を下らないと思うが，何らかの埋め合わせをしてもらえるのか」という申し出を受けた。	クレーム応対費用
A銀行は，乙氏に謝罪するとともに調査を実施し，乙氏が損失を蒙ったのは事実であるがその金額換算は7百万円程度のものと判断し，乙氏との示談交渉に入った。	受取人への謝罪費用 事実関係調査費用 示談交渉経費 （示談金）
示談交渉は決裂し，乙氏側は5千万円の損害賠償請求と謝罪公告請求の提訴をするに至った。	損害賠償金 社会的信用低下
また，このことがマスコミに知れるところとなり，A銀行への取材が殺到した。	取材応対費用
裁判の結果，A銀行は乙氏に4千万円の損害賠償金を支払うことおよび主要新聞紙上に謝罪文を掲載することになった。本件の報道とともにA銀行のミスが周知のこととなり，新しい顧客取引を獲得する営業活動に支障を来たし，業績が低下傾向になった。	裁判費用 損害賠償金 社会的信用低下
このため，A銀行では特別予算7千万円を投じて，イメージ改善のためのキャンペーン実施をするに至った。	信用回復のための費用

表３．業務事故事例における損失の分類

直接的損失	誤振込金

間接的損失	クレーム応対費
	事実関係調査費
	依頼人への謝罪費
	再振込事務経費
	損害賠償金
	示談交渉費
	示談金
	取材応対費
	社会的信用低下

対応費用	誤振込金
	受取人への謝罪費
	裁判費用
	信用回復費用
	（信用低下防止費）

(2) 直接的損失および間接的損失の評価

損失を洗い出した次の課題は，損失のタイプについて個別に損失頻度および損失の平均的な値（損失の大きさ）を評価することである。損失の評価について絶対的な基準は存在しないといえるため，これまでの事故につ

いての報告書（事故統計），さらに関係者（システム関連の担当者・責任者・トップマネジメント）からのヒアリング（業務に精通している関係者からのヒアリング内容はかなり正確性が高いと考えられる），関係者を交えた場での議論を通して，合意を取ったうえで評価をなすのが現実的である。それは，同じタイプの損失でも，組織内の部門が異なれば評価が変わることがあり，また同じ組織でも評価時点での組織の方針により評価のウエイトが相異することがあるからである。

ところで，この段階での損失評価の際に考慮すべき重要なポイントがある。すなわち，次の3点である。

① 損失の大きさを示す指標は，換算金額をおおよそイメージしうること，すなわち，仮に5段階評価方式を取る場合でも，それぞれのランクがどの程度の損失額に相当するのかを明確にしておく。

② 損失評価にあたっては，前に仮定した事故のシナリオに表された金額値に捕らわれるのではなく，できるだけ一般化した状態で評価する。例えば，このシナリオで示された損害賠償金額5千万円が大きいか少ないかを議論するのではなく，通常この種の業務事故で損害賠償金額を請求されるとしたら，平均的にどのくらい請求されると思われるか，という評価が必要である。

③ 損失評価は，当該損失が避けられない状態になった前提の下で行うもので，この損失が発生しやすいかどうか，といった損失発生頻度／確率の問題を混入させない。

上記の考慮により，関係者の合意の下に業務事故事例の損失評価を行った結果は，以下のとおりであると仮定する。

仮説的5段階評価の例（参照→カテゴリイ評価法）

A	10万円以下の軽微な損失
B	10万円超100万円以下の損失
C	100万円超1,000万円以下の損失
D	1,000万円超1億円以下の損失

E　　1億円を超える損失

表4．損失評価表

損失種類	評価	備考
誤振込金	C	振込依頼の金額によって変化する
クレーム応対費用	A	
事実関係調査費用	A	
依頼人への謝罪費用	A	
再振込事務費用	A	
損害賠償金	D	
取材応対費用	B	
社会的信用低下	E	当組織では社会的信用を重要視している
第一次総合評価	E	事故発生に対して何らの方策を講ぜずしかも最悪の経過をたどった場合の損失総額

上表における損失評価から，組織にとり，いかなるタイプの損失が由由しい事態となりうるかが把握されよう。当該モデルにおいては，社会的信用の低下が著しい損失となりうることが示されている。

(3)　業務事故と間接的損失の相関度分析

前項で評価した間接的損失は先に説明のとおり，業務事故が発生したからといって必ず蒙るというものではない（最悪のケースとして考慮しておく必要があるという意味）。

したがってこのステップでは業務事故が各間接的損失に至るまでの経緯と要因を分析し，事故事象と間接的損失の相関度（＝影響損失の発生確率）を把握する必要がある。

手法としては前述の事故ストーリーをより一般化した形で経過の分岐点に着目し，各分岐点のおおよその確率を関係者の合意のもとに１つ１つ決定して求めていくことも考えられよう。

こうして求められた発生確率決定についても，特に基準が存在するものではないので，過去の事例等を参考にしつつ関係者の合意で割り切っていく必要がある。

以下は，間接的損失に関する発生確率を加味した評価の一例である。

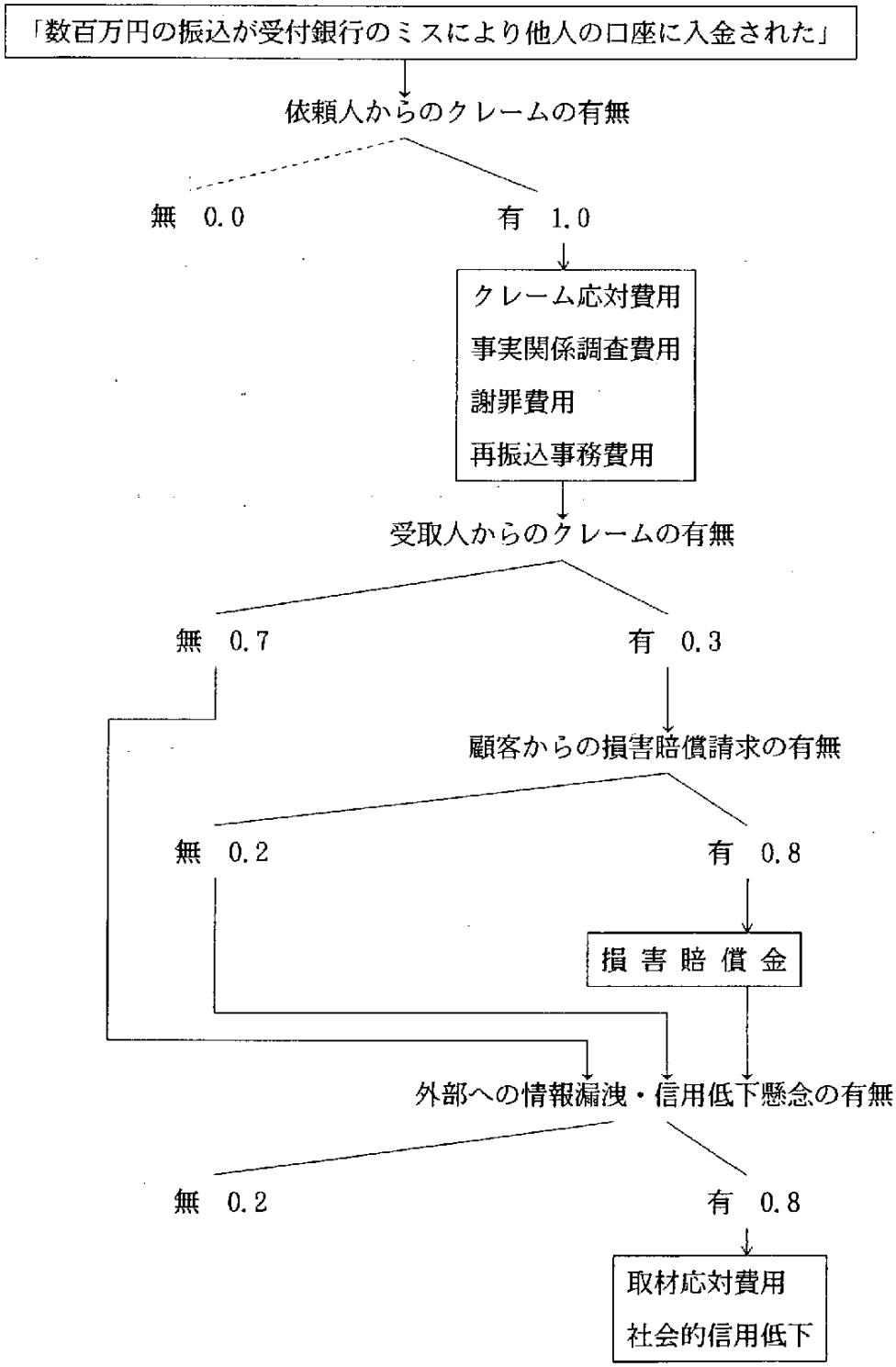


図６．業務事故事象の分析例

表５．業務事故事例における間接的損失の発生確率評価表

	損失額評価（前述）	発生確率
クレーム応対費用	A	1.0
事実関係調査費用	A	1.0
依頼人への謝罪費用	A	1.0
再振込事務費用	A	1.0
損害賠償金	D	0.24
取材応対費用	A	0.8
社会的信用低下	E	0.8

(4) 対応費用の分析

事故事象発生後は，その被害を最小限に抑えるべく対応策を決定・遂行していくのが通常である。このための費用は，本来の「損失」とは性格を異にするものであり，損失総額を算出する際単純に加えるべきものではない。すなわち，この費用は，投入額以上の何らかの効果を期待して支出されるもので，これまで評価・算出してきた損失総額を減少させる方向に働くものである。

対応費用の効果は，大きく次の２種類に分別される。

① 直接損失または間接的損失の損失額自体を減少させる

詐取された金銭を回収工作の費用

損害賠償金支払いを回避するための折衝費用など

② 間接的損失の発生確率を減少させる

クレームから賠償請求に進展しないようにする謝罪費用

信用低下を防止するための広報費用など

個々の対応策に要する費用や期待される効果程度についても絶対的な基準がないので，その決定にあたっては関係者の合意が必要になる。

表６．業務事故事例における対応費用の分析・評価表

対　応　策	必要となるケース	同左確率	費用	期　待　効　果
誤振込金回収	事故が発生すれば必ず	1.0	A	誤振込金損失 C→A 信用低下確率 0.8 → 0.5
受取人への謝罪	受取人からクレームがあった場合	0.3	A	損害賠償請求確率 0.24→ 0.1 信用低下確率 0.5 → 0.2
示談交渉	損害賠償請求を受けた場合	0.1	C	損害賠償金 D→A 信用低下確率 0.2 → 0.1
裁　　判	示談交渉決裂の場合	0.05	C	損害賠償金 D→C
信用回復	信用低下の懸念がある場合	0.1	D	信用低下損失 E→A

(5)　業務事故事象の損失総合評価

総合評価はこれまで考察してきた（下記）３種の指標を組み合わせることで行うことになる。

①　直接的損失と間接的損失との各損失程度を示す指標

②. 間接的損失の発生確率を示す指標

③ 対応費用の必要コストとその期待効果を示す指標

具体的には，③に①，②を補正しておくという作業が中心になるといえる。

例えば，ここで取り上げた業務事故事象について例示すると，以下の表のとおりである。

損失種類	発生確率と対応効果補正後の損失程度
誤振込金	A（回収費用Aと回収不能平均金額Aの合計）
クレーム応対費用	A
事実関係調査費用	A
依頼人への謝罪費用	A
再振込事務経費	A
損害賠償金	B（0.3×A＋ 0.1×C＋ 0.1×A＋0.05×C ＋0.05×C）
取材応対費用	A
社会的信用低下	C（0.1×D＋0.1×A）

上表より振込依頼を受け付けた銀行のミスにより受取人以外の口座に入金されるという業務事故が発生した場合の平均的損失程度はCランクと判定することになる。（100万円から1,000万円程度の損失を蒙るものと評価するという意味であり，これが絶対的標準的な損失額というわけではない）

前にも述べたとおり，１つの業務事故が発生した場合，それが組織に与える損害はケースバイケースで異なるのが現実であるが，リスク分析における損失評価は実際に事故がおきる前に実施しなければならないものである。

このため，ここでは「平均的」という概念を導入し，かつ，多少の曖昧

さをも容認していくことで，「この業務事故が発生した場合は当組織に与える平均的損失はこの程度」の決めを行うことを重視している。

なぜなら，「この事故が発生してもほとんど被害がない場合もあり，また多大な損失を蒙ることもある」という考え方では，当該事故発生防止対策のため，どの程度までならコストをかけるべきかの判断ができないからである。

したがって，ここでモデルを対象に行った評価結果自体は，特に意味があるものではなく，評価に至るまでの考え方とプロセスがリスク分析実施にあたってのポイントになる。

6．今後の課題

本報告書では，バンキングシステムの内国為替業務に視点をあて，モデルを設定し，リスク分析の対象となる問題事象の範囲を明確化し，損失のタイプから損失の評価まで考察した。その際，シナリオを用意し，事故事象・原因とのかかわりから，損失の評価へのプロセスを示している。問題状況の制約から，全てのコンピュータ・システムに妥当とは言い難い面もあるかもしれないが，具体的なモデルを用いることにより，方法論的に，比較的理解しやすく，他にも応用がきく構成を心がけ，具体的にリスク分析を進めるための手順・手法に焦点をあてた。とりわけ，ここでのポイントとしたことは，銀行経営にとりマイナスとなる「業務事故事象」，その原因となりうる「システム事故事象」にメスを入れ，４つの業務事故事象のうち，「振り込み依頼を受けたにもかかわらず，誤って他人の口座に入金された」ケースを対象として損失評価を行った。損失頻度／損失強度についてのマトリックスを構成することも有意味であるが，今回の報告書ではリスク分析の考え方と方法にウエイトをおくことに止めた。

今後，課題とすべきことは，リスクの変化への対応である。コンピュータ・システムの活用が通信回線を利用した単なるオンライン・システムから公衆回線を媒体とした広範囲ネットワーク，ＶＡＮとの接続等，近時になり急

速に複雑多様化してきている状況の中で，「予期せぬ出来事」ですまないリスクの発生が予想されるがため，自分のところは大丈夫という「他人事症候群」に陥らないよう注意する必要がある。それだけに，リスクをもたらす状況（脆弱性，ハザード，ペリル（脅威）間の相互連関）の評価のための操作性，リスク分析のための定性的・定量的アプローチの詳細な構造，セーフガード等のリスク処理方法に対する費用効果分析のあり方が今後問われることになるのである。したがって，リスク対応の重要性から，リスク処理方法としてのコンピュータ・セキュリティ対策（主としてリスク・コントロール）たる物理的対策，技術的対策，管理的対策のみならず，それらのガードの実施にもかかわらず発生する損失への対応としてのリスク・ファイナンス（資金手当）にも目を向けることが不可欠となろう。

さらには，これまでの分析を深化させることが重要とされ，複雑なコンピュータ・システムを利用企業が増大する状況に鑑みて，一般論としてのリスク分析ガイドラインを策定することも課題として求められることになろう。

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89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　　4,087
- 回収数　　891（うち，オンラインユーザ　751）
- 回収率　　21.8%

（注）ここでの集計対象は，オンラインユーザ751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	2	2	2	2	2	2	2	2
建設業	26	26	26	27	27	27	27	25
食品製造業	20	20	19	20	20	20	20	19
繊維工業	23	23	24	23	24	23	23	23
紙・パルプ・紙加工品製造業	11	11	10	11	11	11	11	11
新聞業・出版業	6	6	6	6	6	6	6	6
印刷業・同関連産業	4	4	4	4	4	4	4	4
化学工業	45	47	47	47	47	47	46	45
石油製品製造業	8	8	6	8	8	8	7	8
窯業・土石製品製造業	7	6	6	7	7	7	7	7
鉄鋼業	13	13	14	14	14	14	14	14
非鉄金属製造業・金属製品製造業	22	21	22	23	23	22	23	22
一般機械器具製造業	33	33	33	34	34	34	35	34
電気機械器具製造業	56	53	53	55	56	56	56	55
輸送用機械器具製造業	32	31	29	33	33	33	33	32
精密機械器具製造業	16	16	16	16	16	16	16	16
その他の製造業	25	25	25	25	25	25	25	23
卸業・商社	67	68	66	68	68	68	67	68
小売業	37	37	36	38	38	38	37	38
金融業	82	84	86	85	85	86	82	83
証券業・商品取引業	1	2	2	2	2	2	2	2
生命保険業（含代理業・ｻｰﾋﾞｽ業）	6	6	6	6	6	6	6	6
損害保険業（含代理業・ｻｰﾋﾞｽ業）	3	3	3	3	3	3	3	3
不動産業	6	6	5	6	6	6	6	6
運輸・通信・倉庫業	38	40	38	39	39	39	39	39
電力・ガス事業	8	8	8	8	8	8	8	8
放送業	7	7	7	7	7	7	7	7
広告・調査・情報提供ｻｰﾋﾞｽ業	4	4	4	4	4	4	4	5
情報処理ｻｰﾋﾞｽ業・ｿﾌﾄｳｪｱ業	38	37	36	37	37	38	38	38
医療業	5	5	5	5	5	5	5	5
宗教法人	－	－	－	－	－	－	－	－
高校	－	－	－	－	－	－	－	－
大学	12	12	12	12	12	12	12	11
その他の教育機関	6	6	6	6	6	6	6	6
学術研究機関	4	4	4	3	3	3	3	4
法人団体・農協	18	17	17	18	18	18	18	18
その他のサービス業	5	5	5	5	5	5	5	4
政府	4	4	3	4	4	4	4	4
地方公共団体	28	27	27	28	28	28	28	28

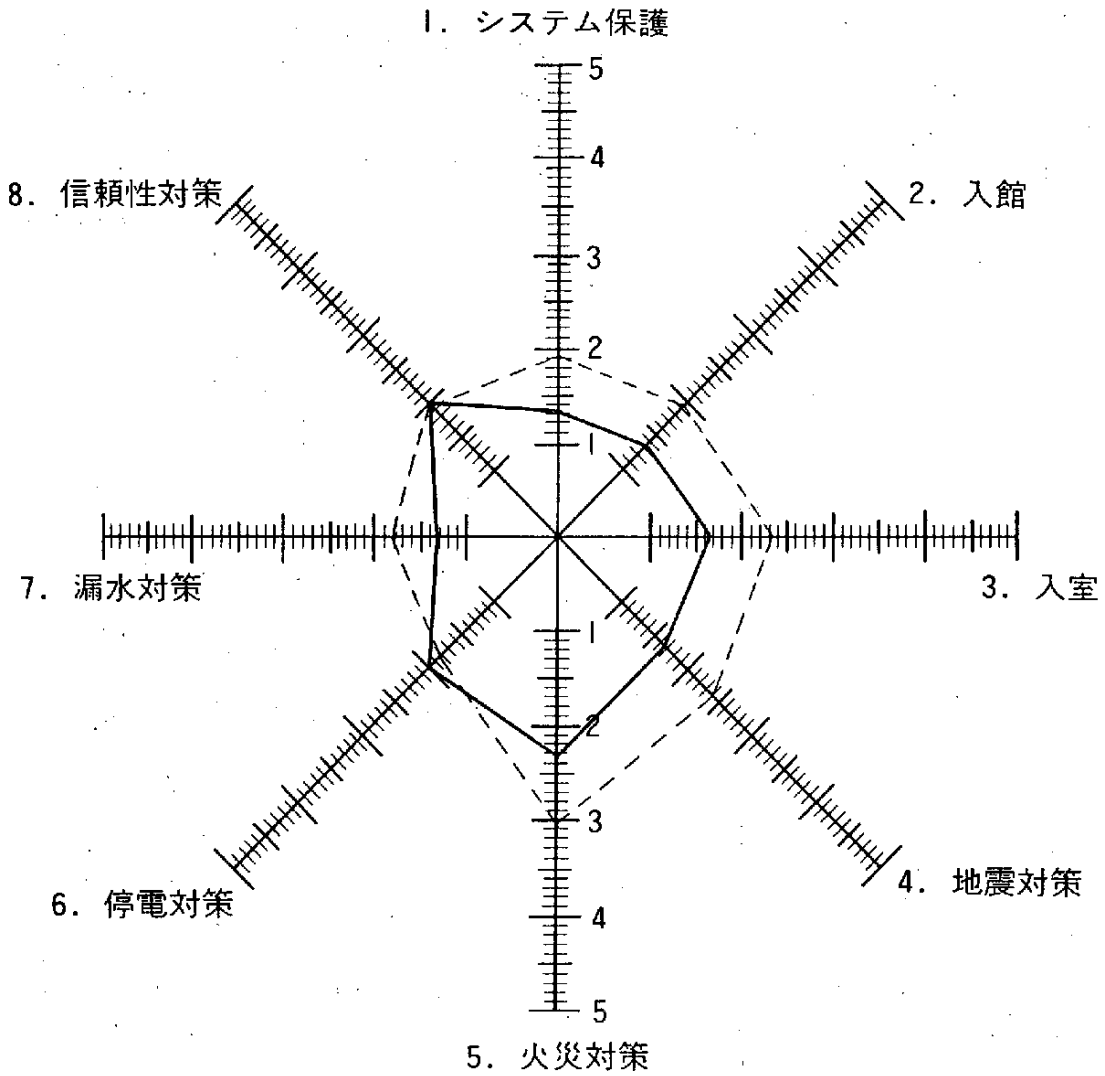
（オンラインユーザのみ）

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，バッチ and/or ＩＤカード	受付者，来訪者名簿，バッチ 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，バッチ and/or ＩＤカード	受付者，来訪者名簿，バッチ 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	消化器具	消化器具，消化装置	消化器具，消化装置，避難システム	消化器具，消化装置，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。

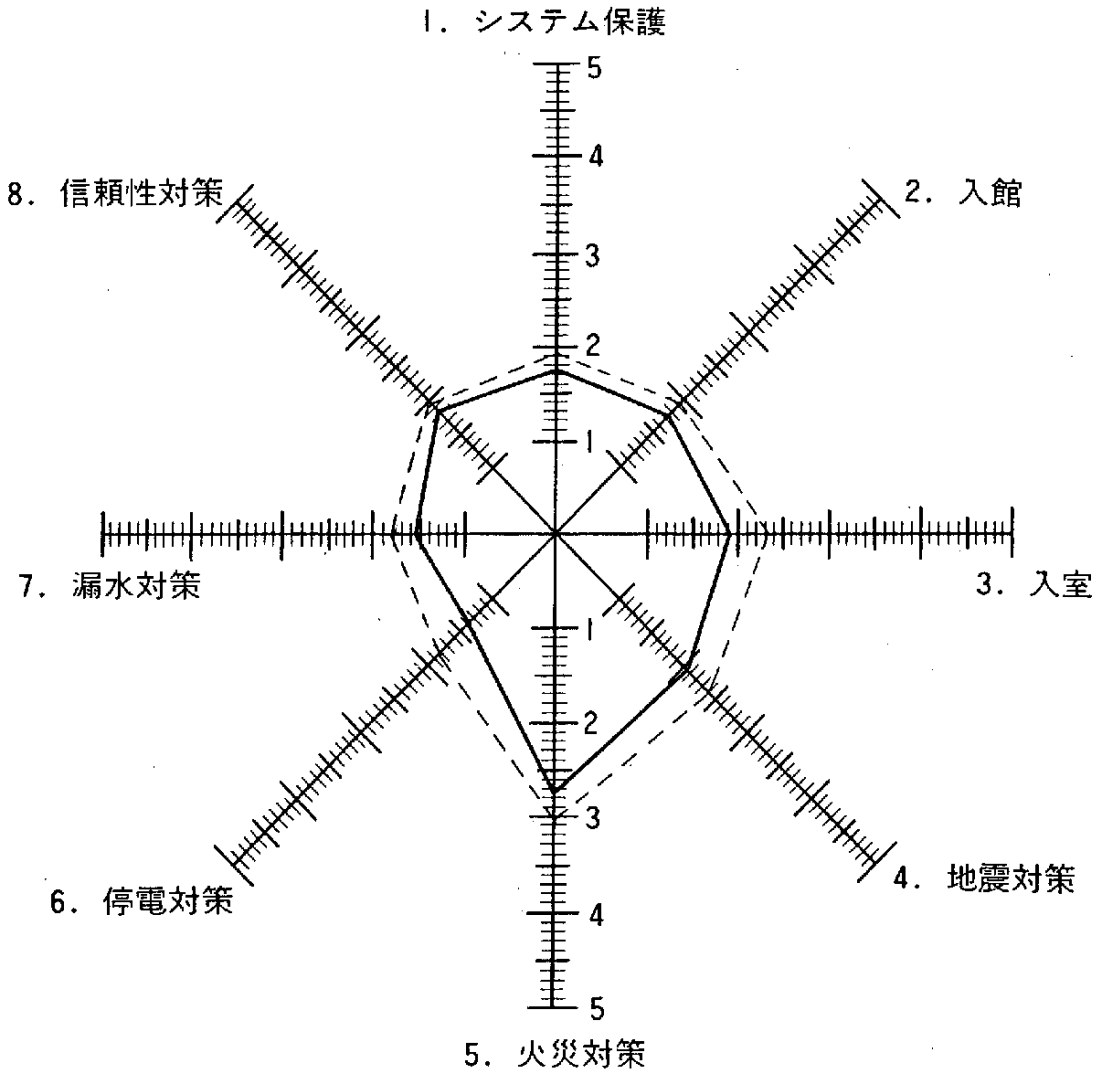
第一次産業計



----：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
第一次産業計	1．33	1．33	1．67	1．67	2．33	2．00	1．33	2．00

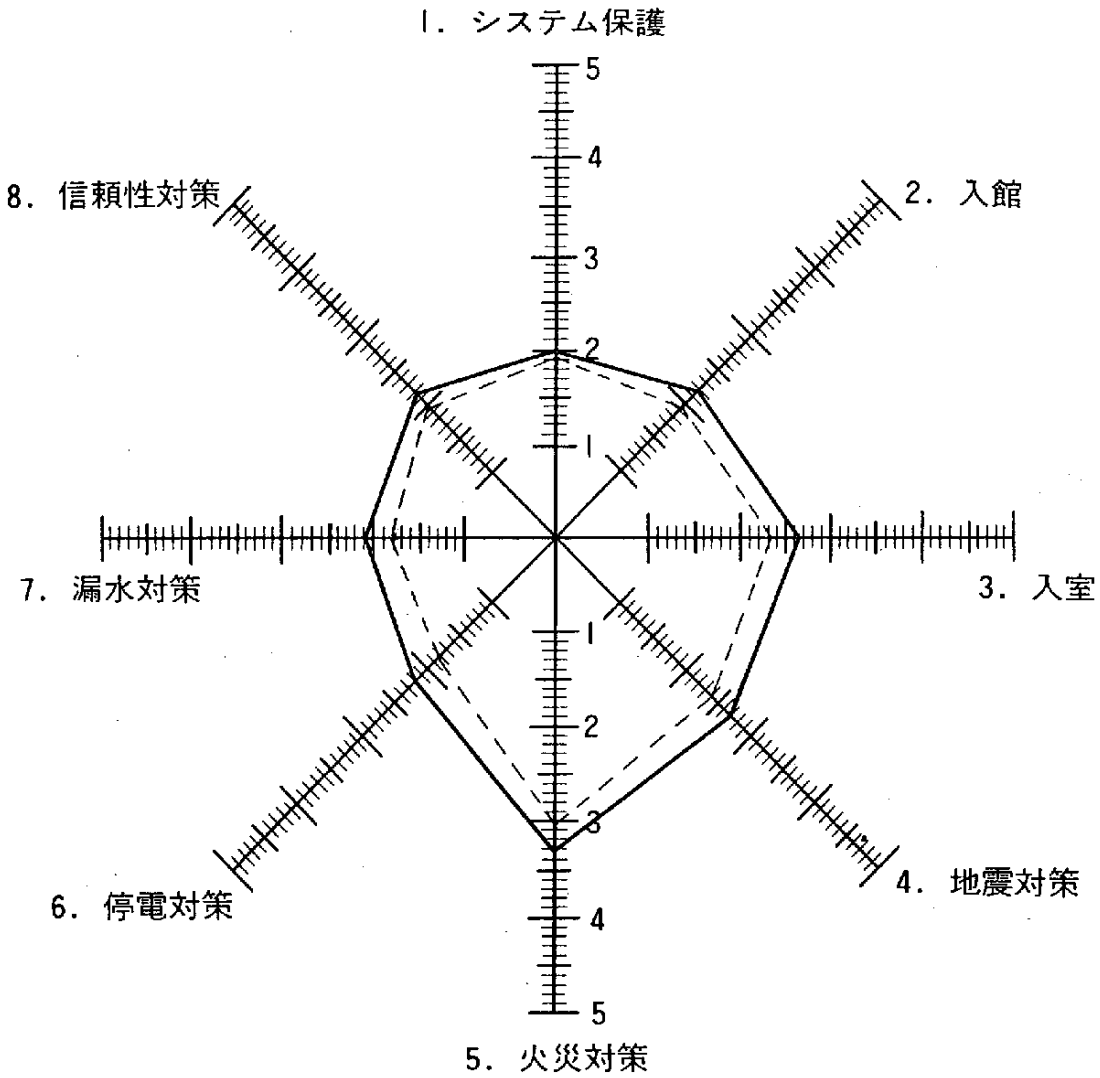
第二次産業計



－－－：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
第二次産業計	1．77	1．76	1．91	2．07	2．75	1．39	1．55	1．82

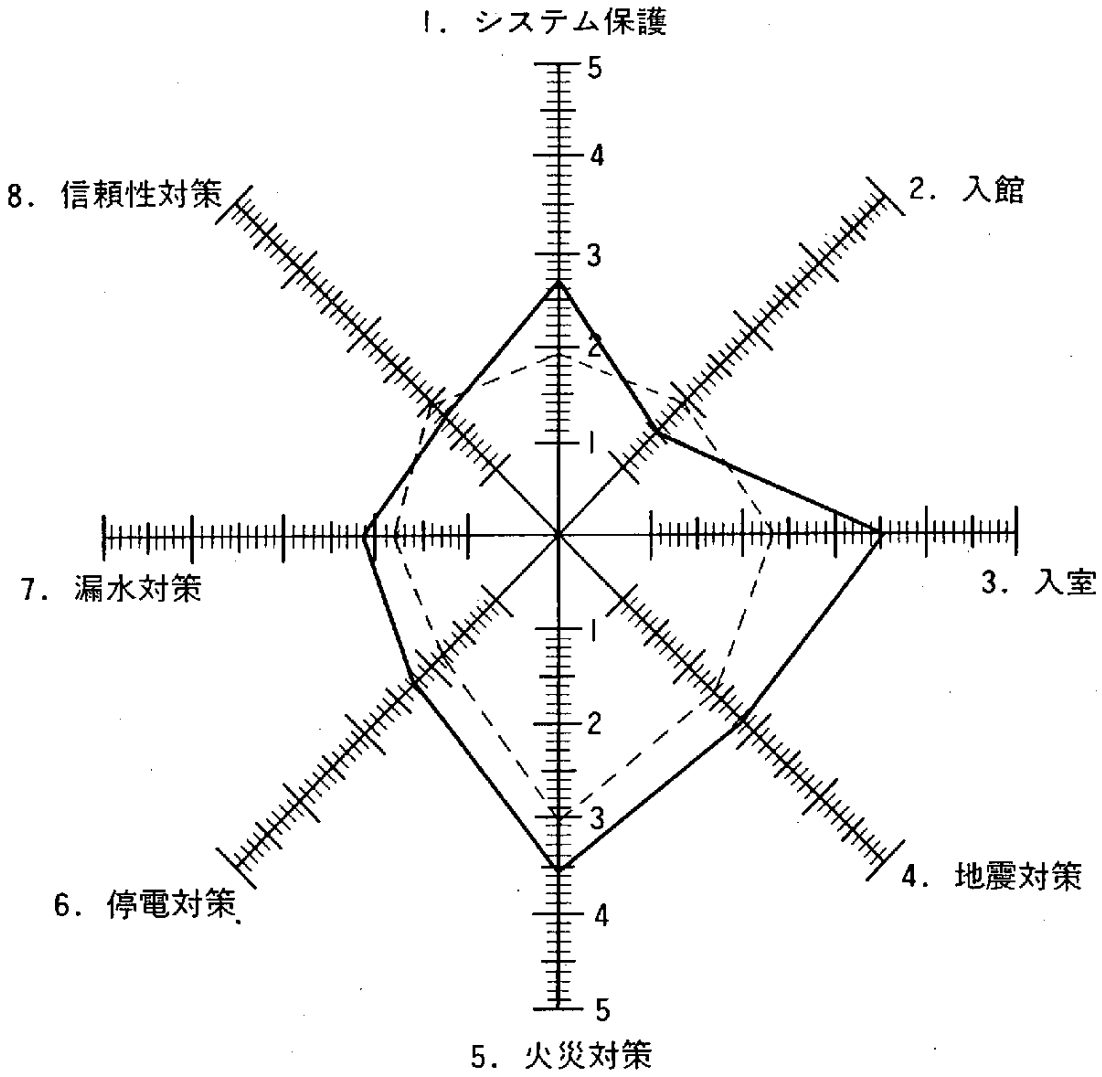
第三次産業計



－－－：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
第三次産業計	2．00	2．19	2．65	2．70	3．32	2．20	2．09	2．15

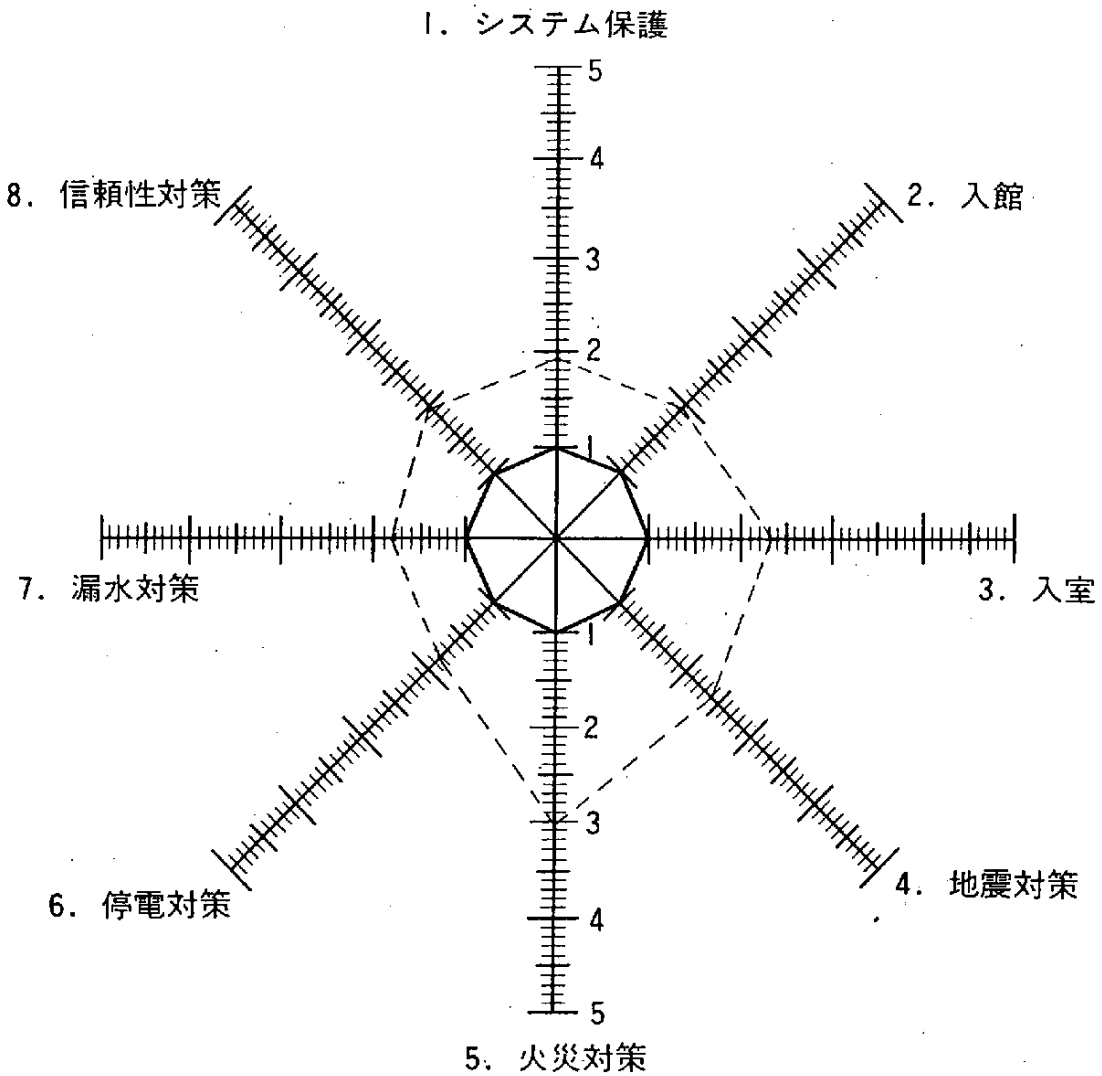
公　務　計



----：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
公　務　計	2．69	1．52	3．53	2．84	3．56	2．28	2．13	1．78

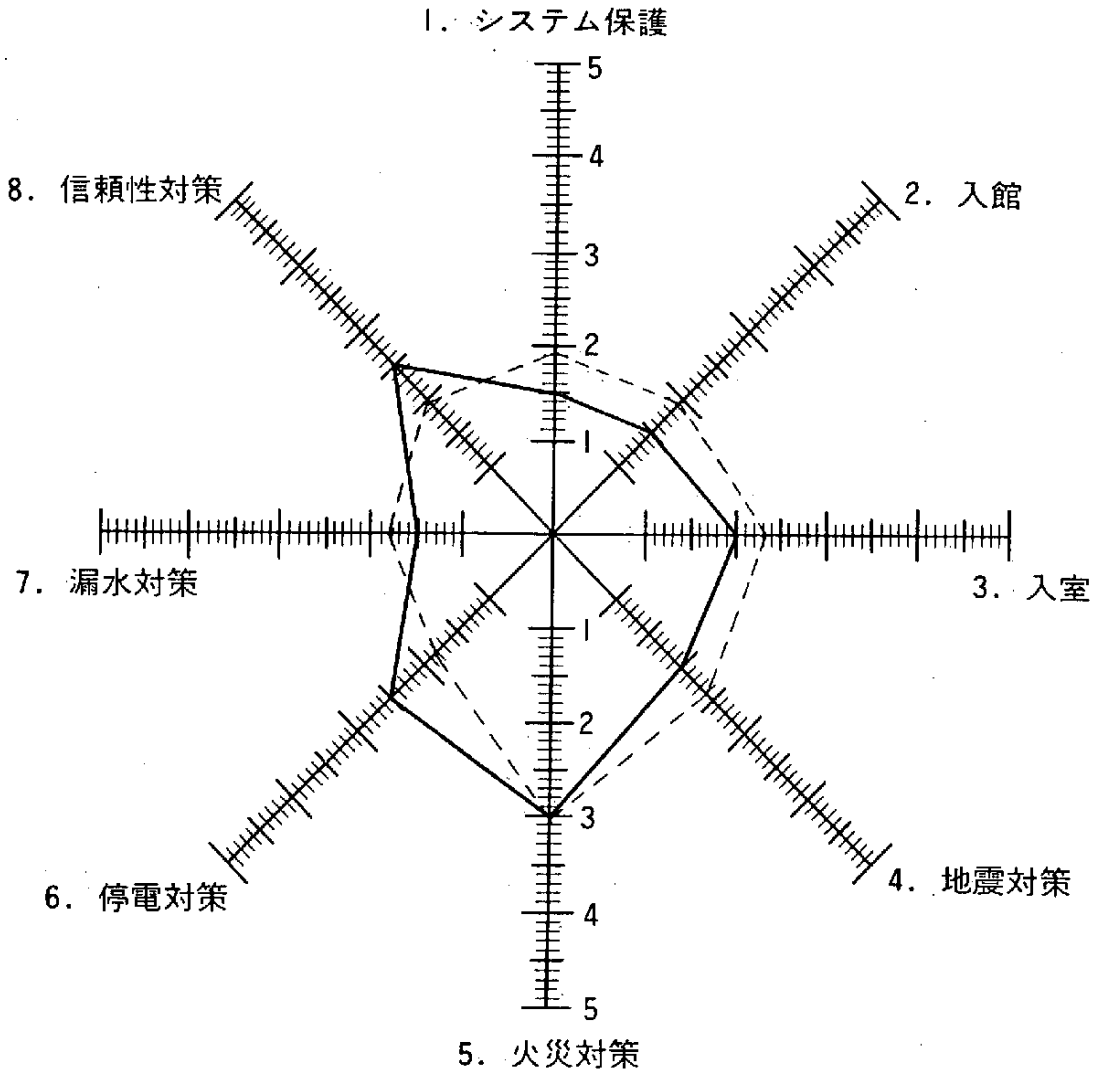
農・林・漁・狩猟・水産養殖業



－－－：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	1.92	1.95	2.33	2.40	3.05	1.82	1.83	1.98
農・林・漁・狩猟・水産養殖業	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00

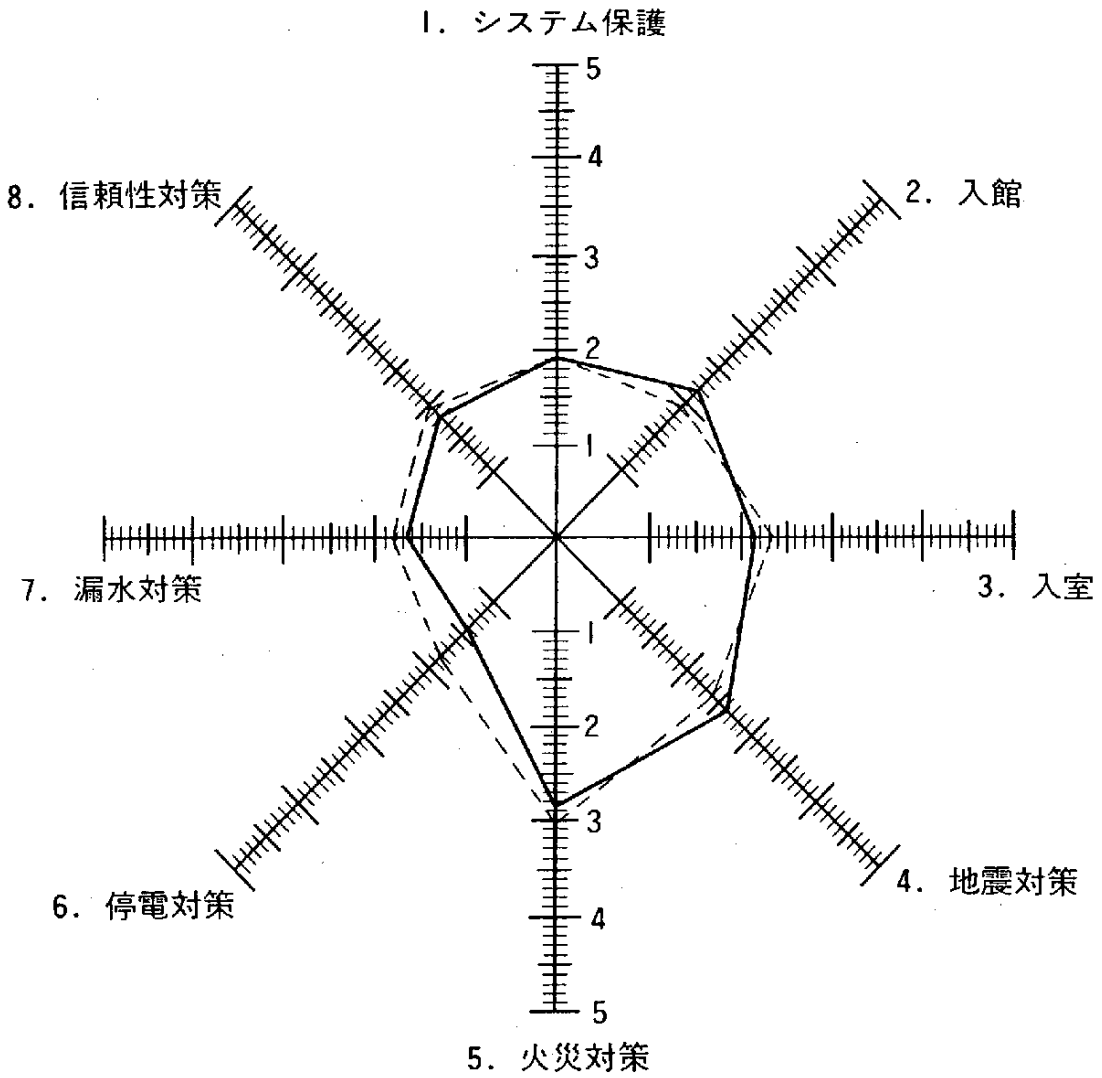
鉱　　業



---：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
鉱　　業	1．50	1．50	2．00	2．00	3．00	2．50	1．50	2．50

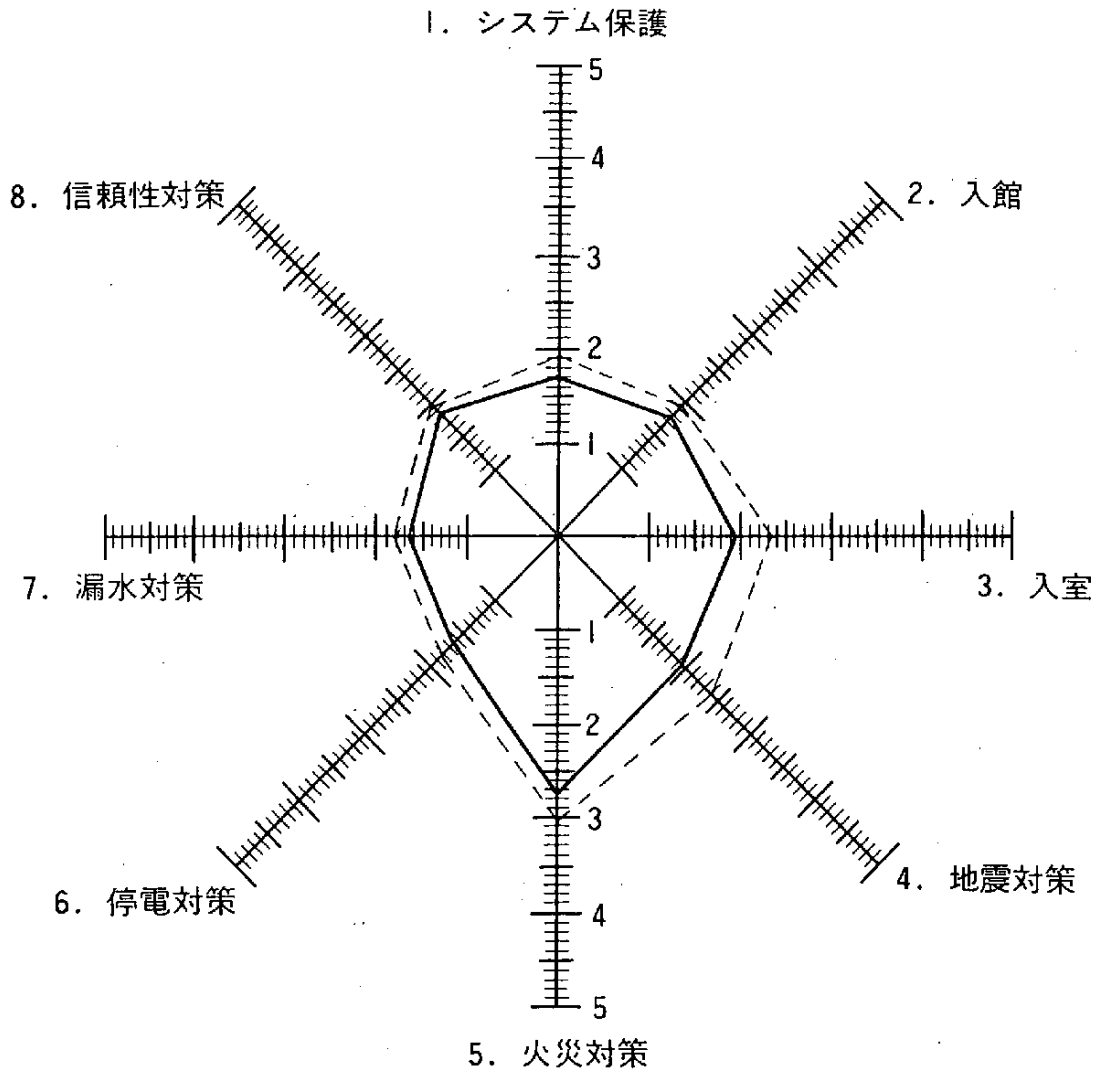
建　設　業



----：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
建　設　業	1．92	2．19	2．15	2．63	2．85	1．41	1．67	1．80

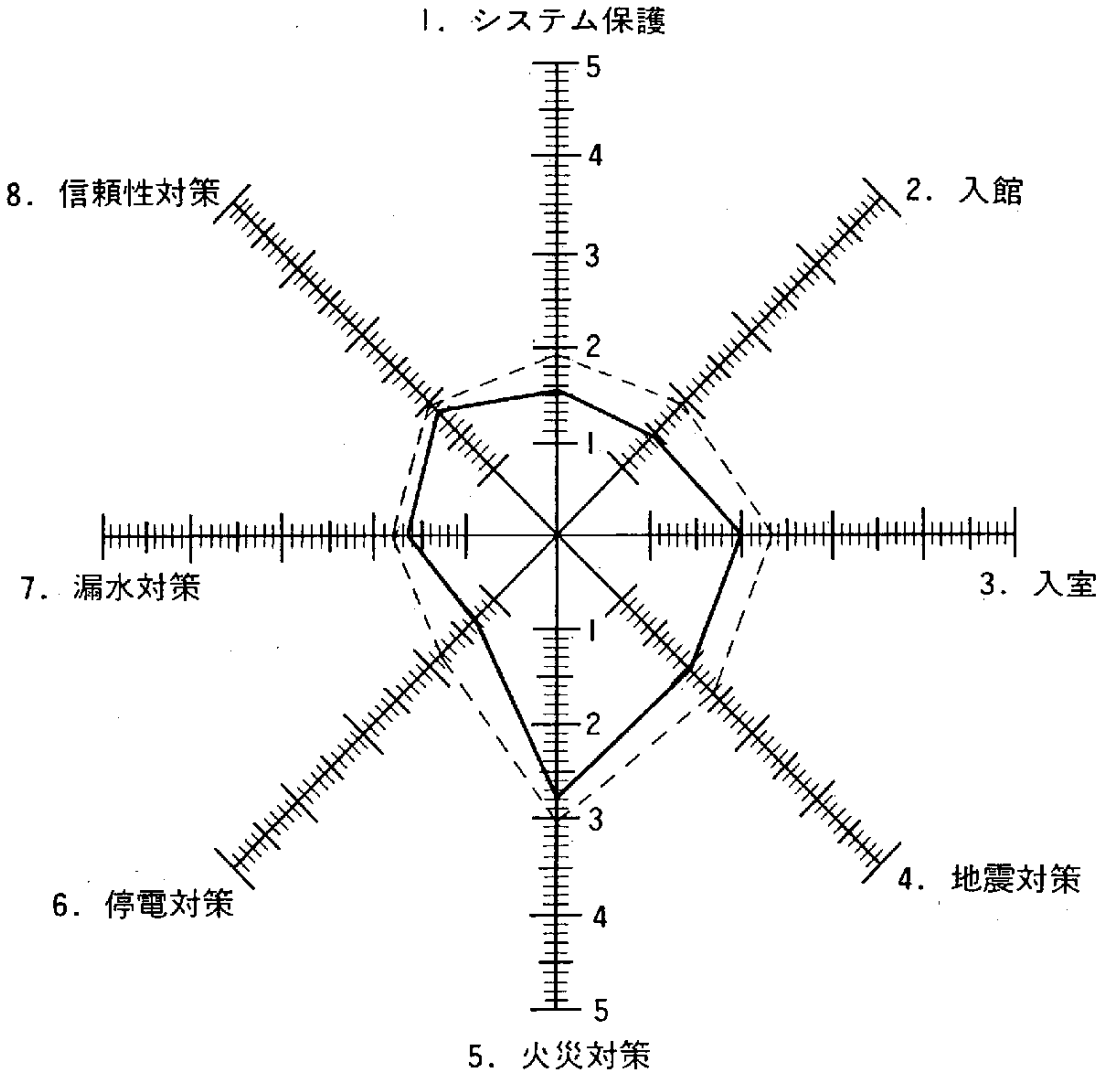
食品製造業



－－－：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
食品製造業	1．70	1．75	1．95	1．95	2．75	1．65	1．65	1．84

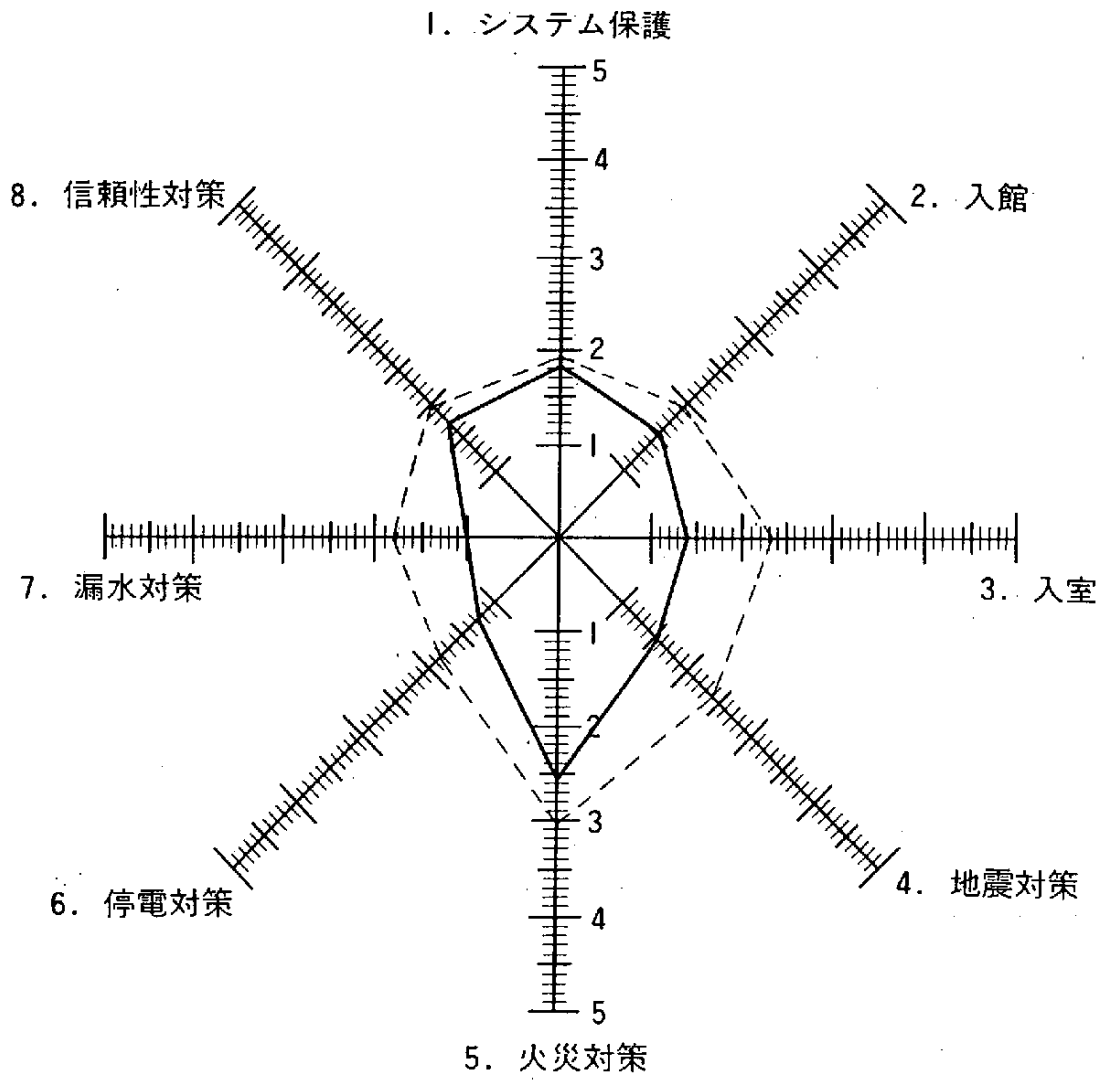
繊 維 工 業



－－－：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
繊 維 工 業	1．57	1．48	2．00	2．04	2．79	1．30	1．65	1．83

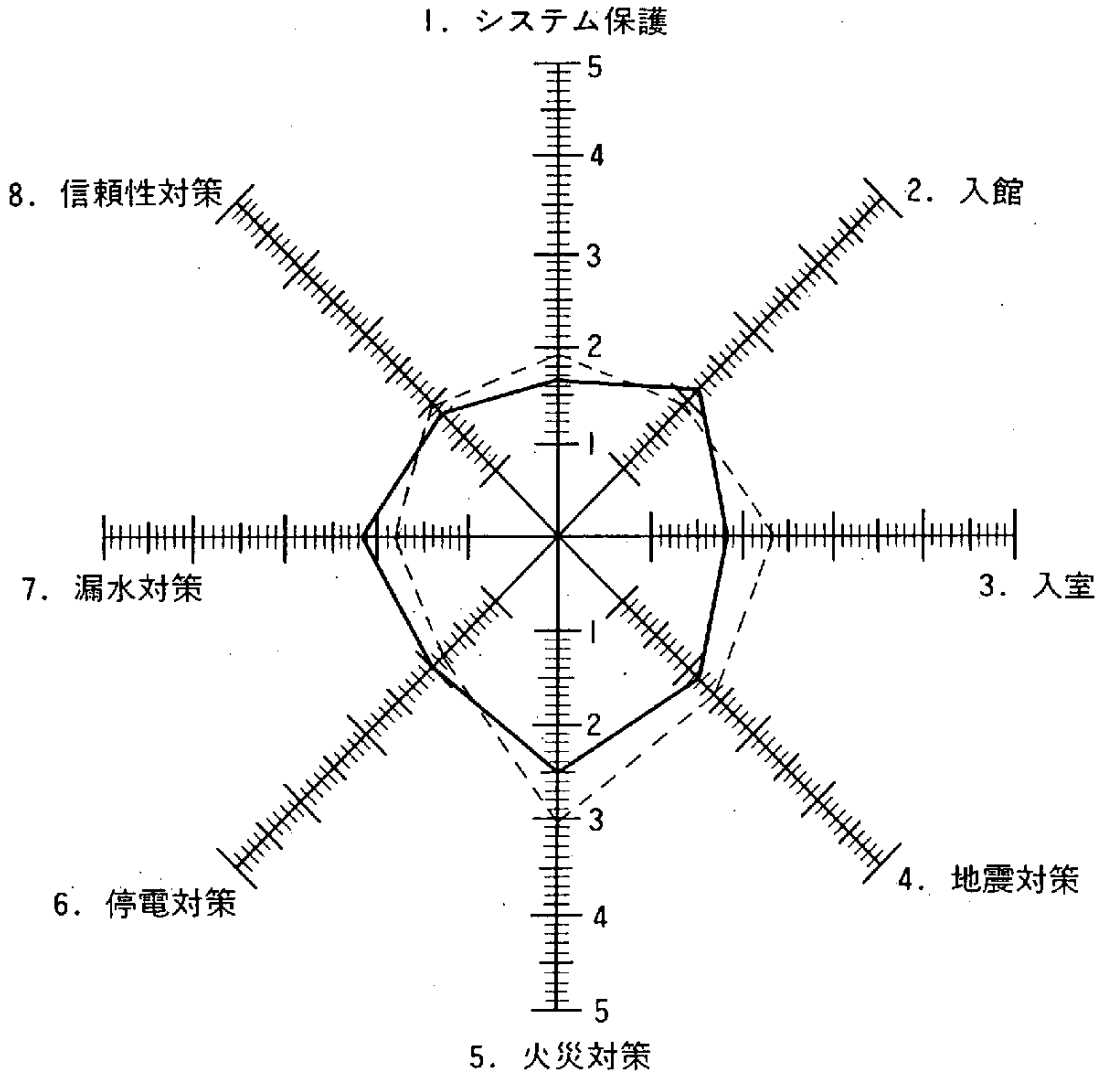
紙・パルプ・紙加工品製造業



－－－：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
紙・パルプ・紙加工品製造業	1．82	1．55	1．40	1．55	2．55	1．27	1．00	1．73

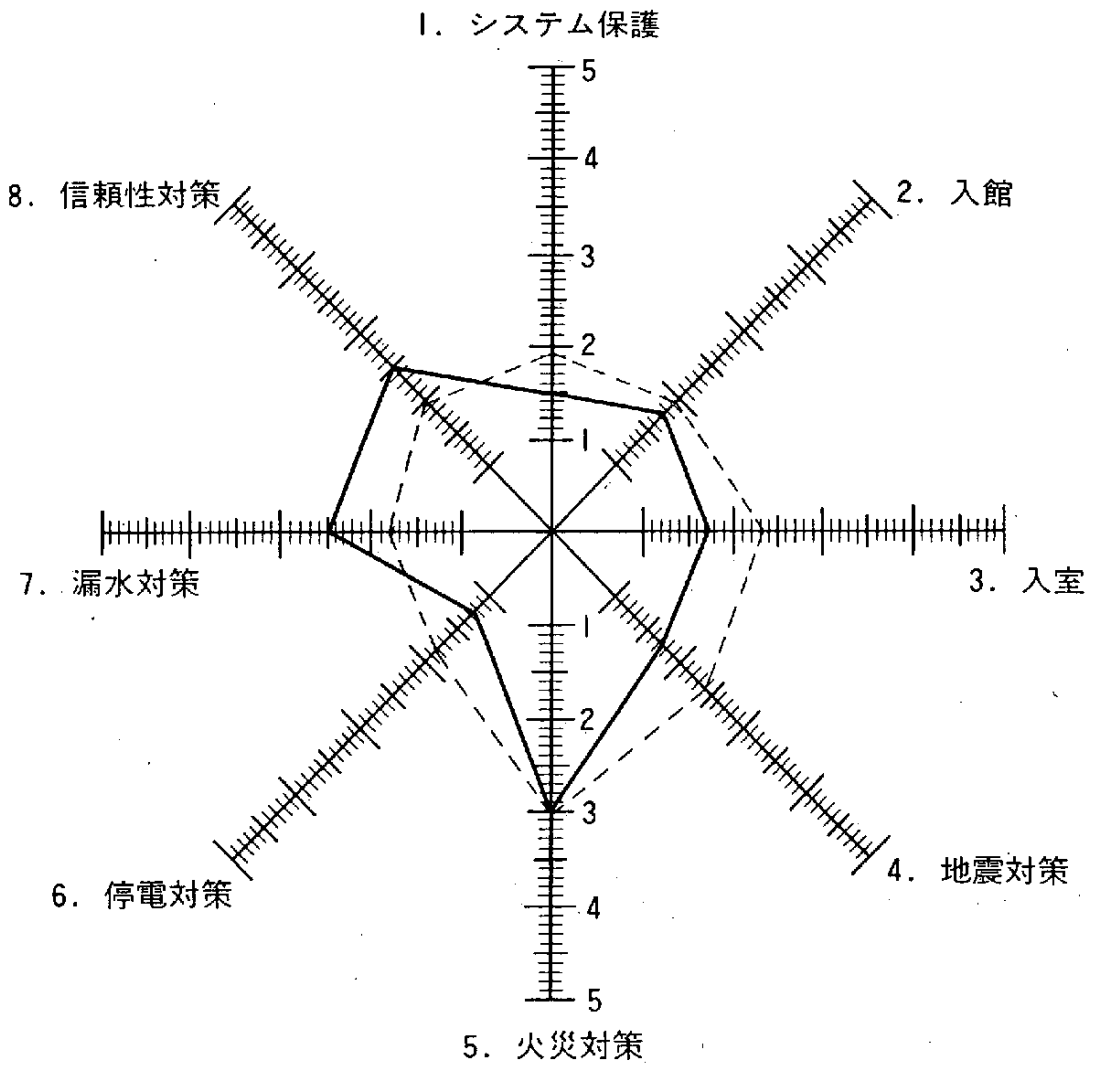
新聞業・出版業



――：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
新聞業・出版業	1．67	2．17	1．83	2．17	2．50	2．00	2．17	1．83

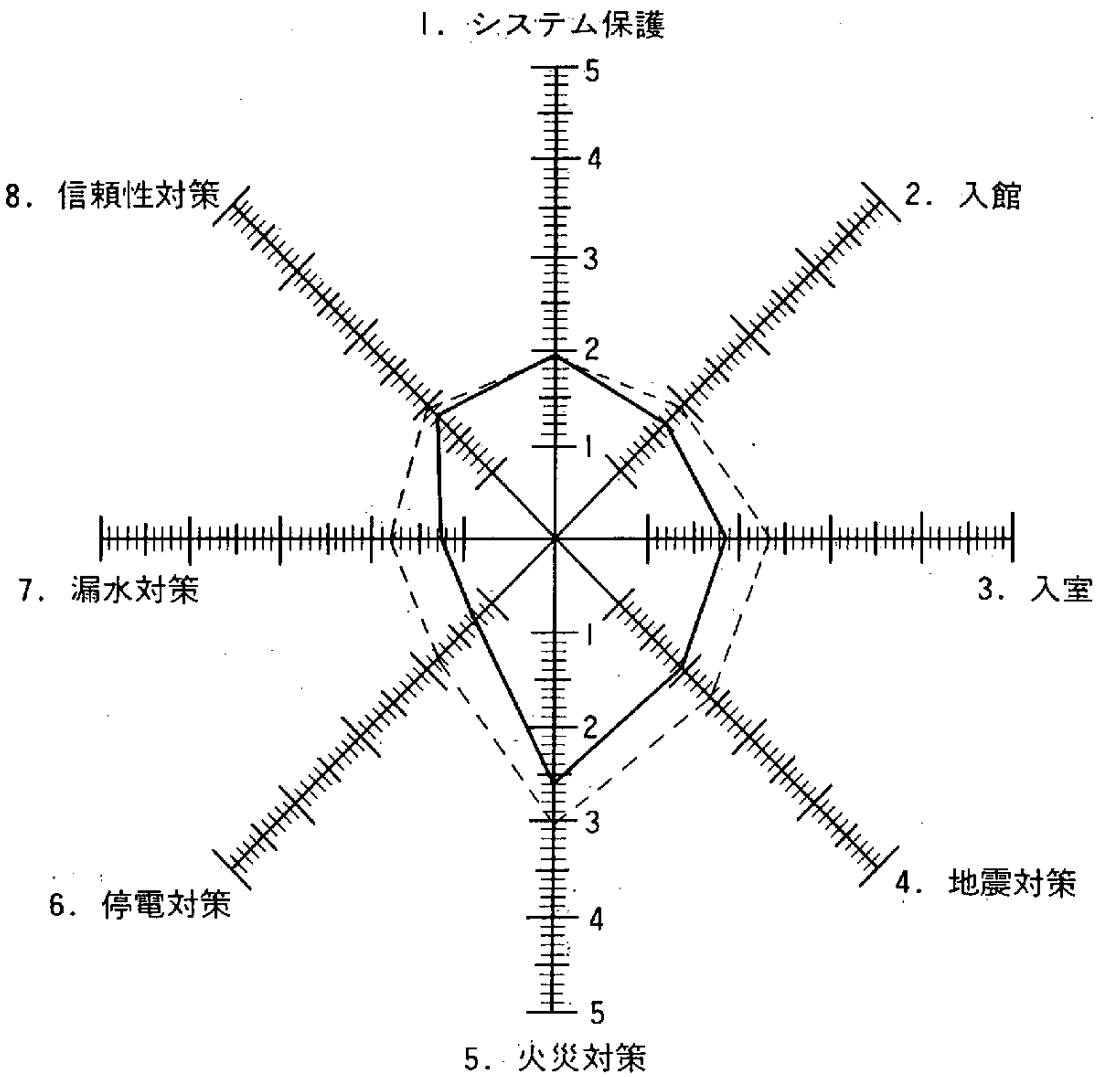
印刷業・同関連産業



－－－：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
印刷業・同関連産業	1．50	1．75	1．75	1．75	3．00	1．25	2．50	2．50

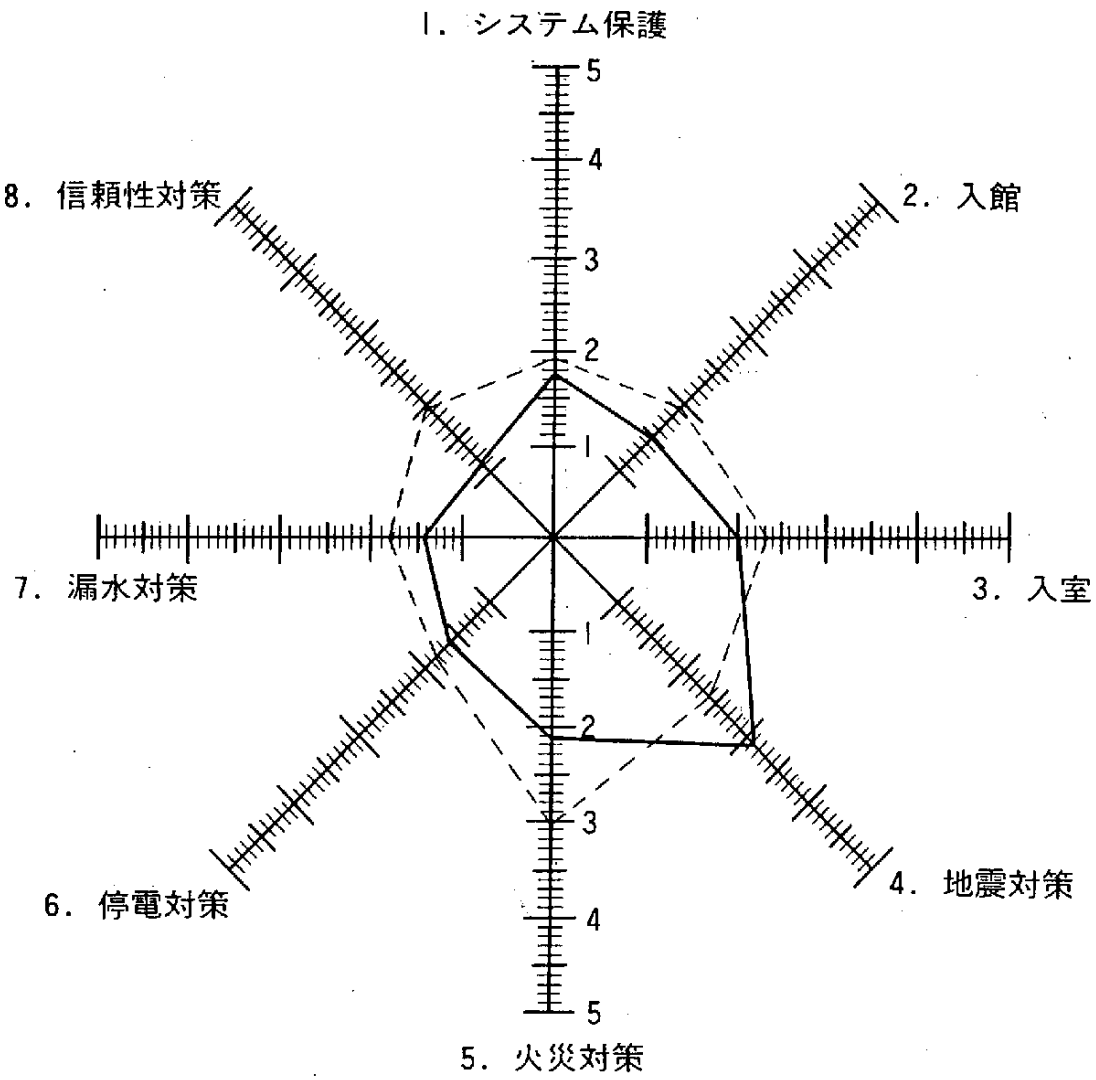
化学工業



－－－：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
化学工業	1．96	1．70	1．85	1．96	2．60	1．28	1．28	1．82

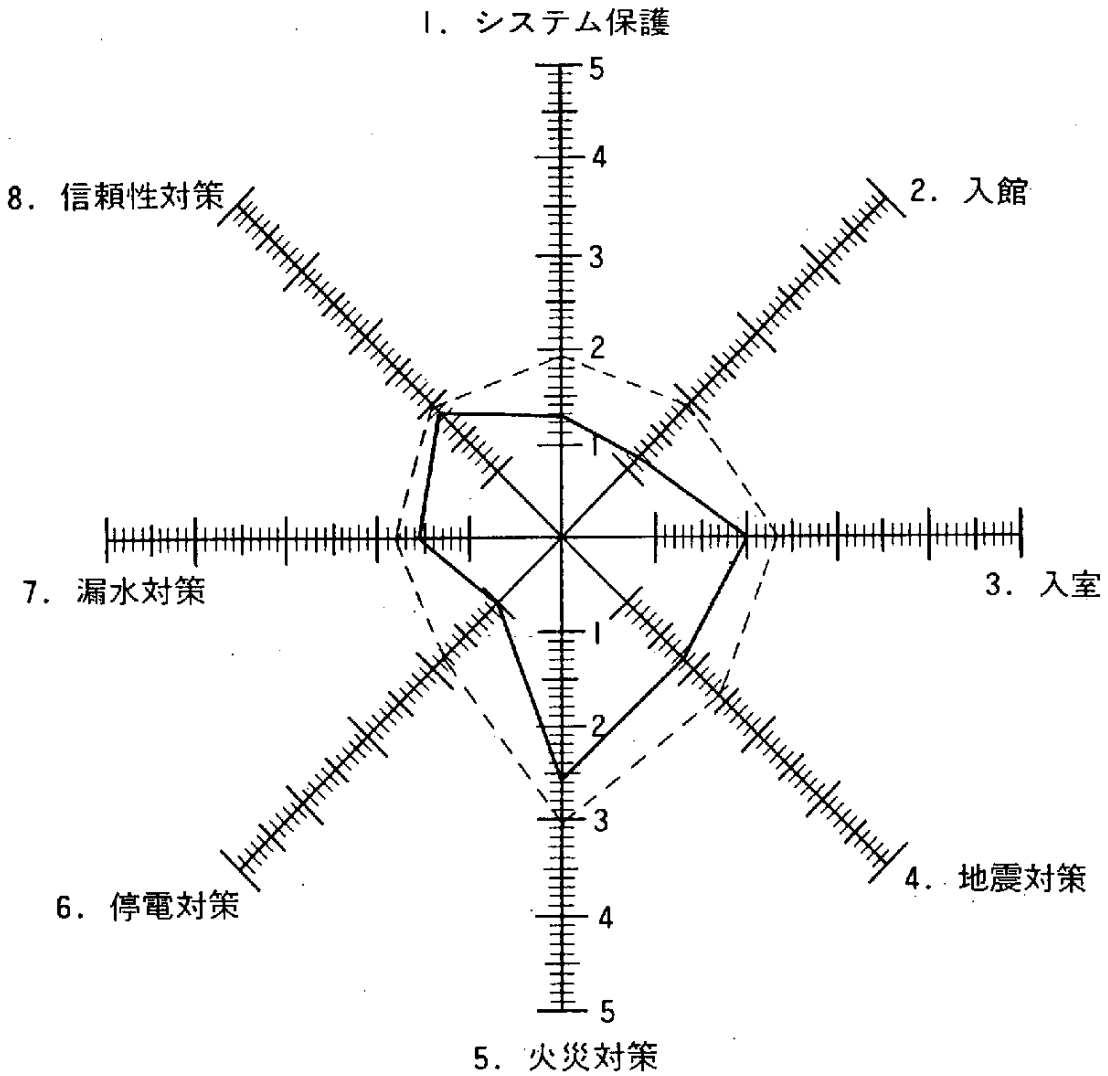
石油製品製造業



－－－：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
石油製品製造業	1．75	1．50	2．00	3．13	2．13	1．63	1．43	1．13

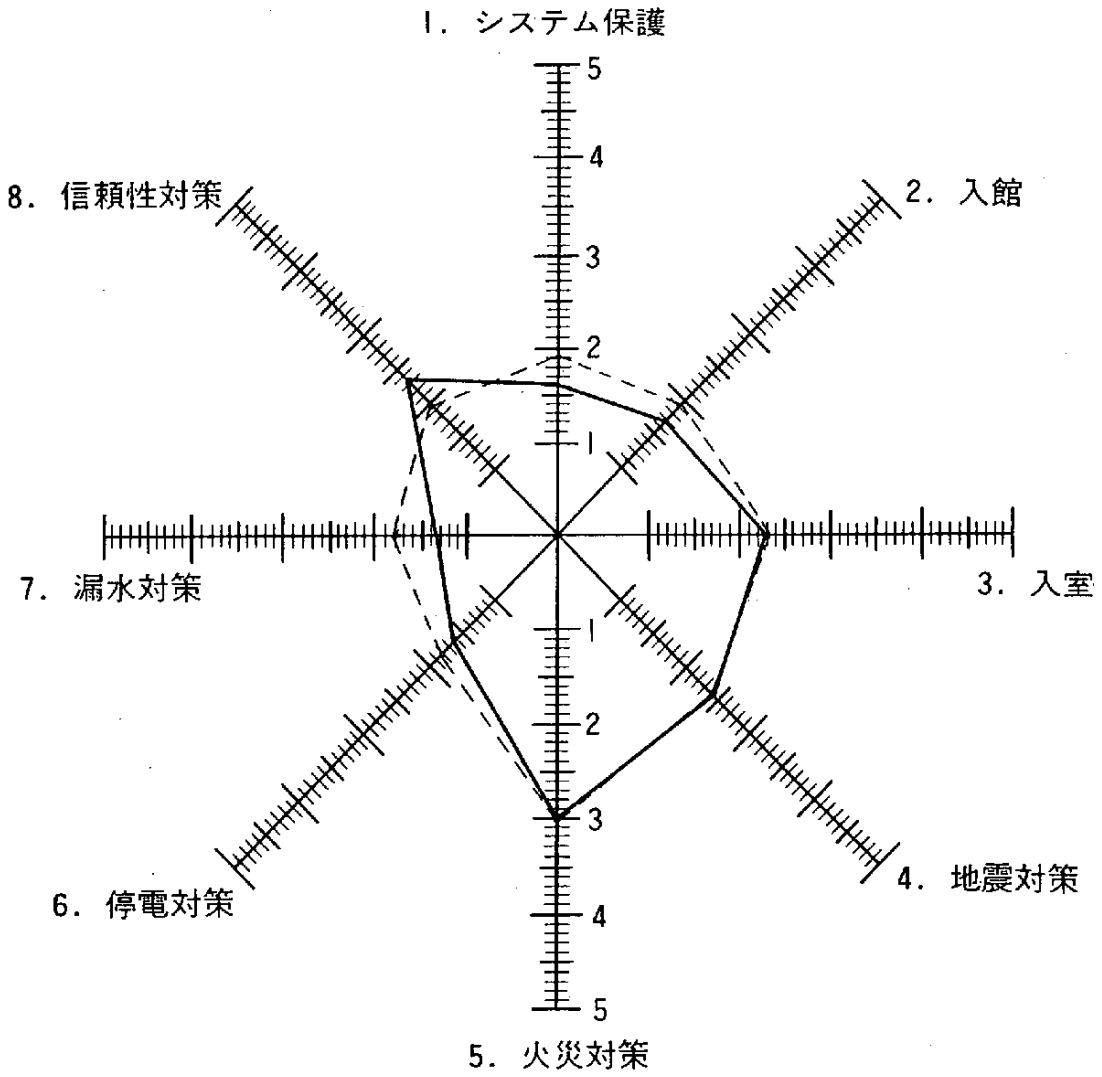
窯業・土石製品製造業



－－－：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	1.92	1.95	2.33	2.40	3.05	1.82	1.83	1.98
窯業・土石製品製造業	1.29	1.17	2.00	1.86	2.57	1.00	1.57	1.86

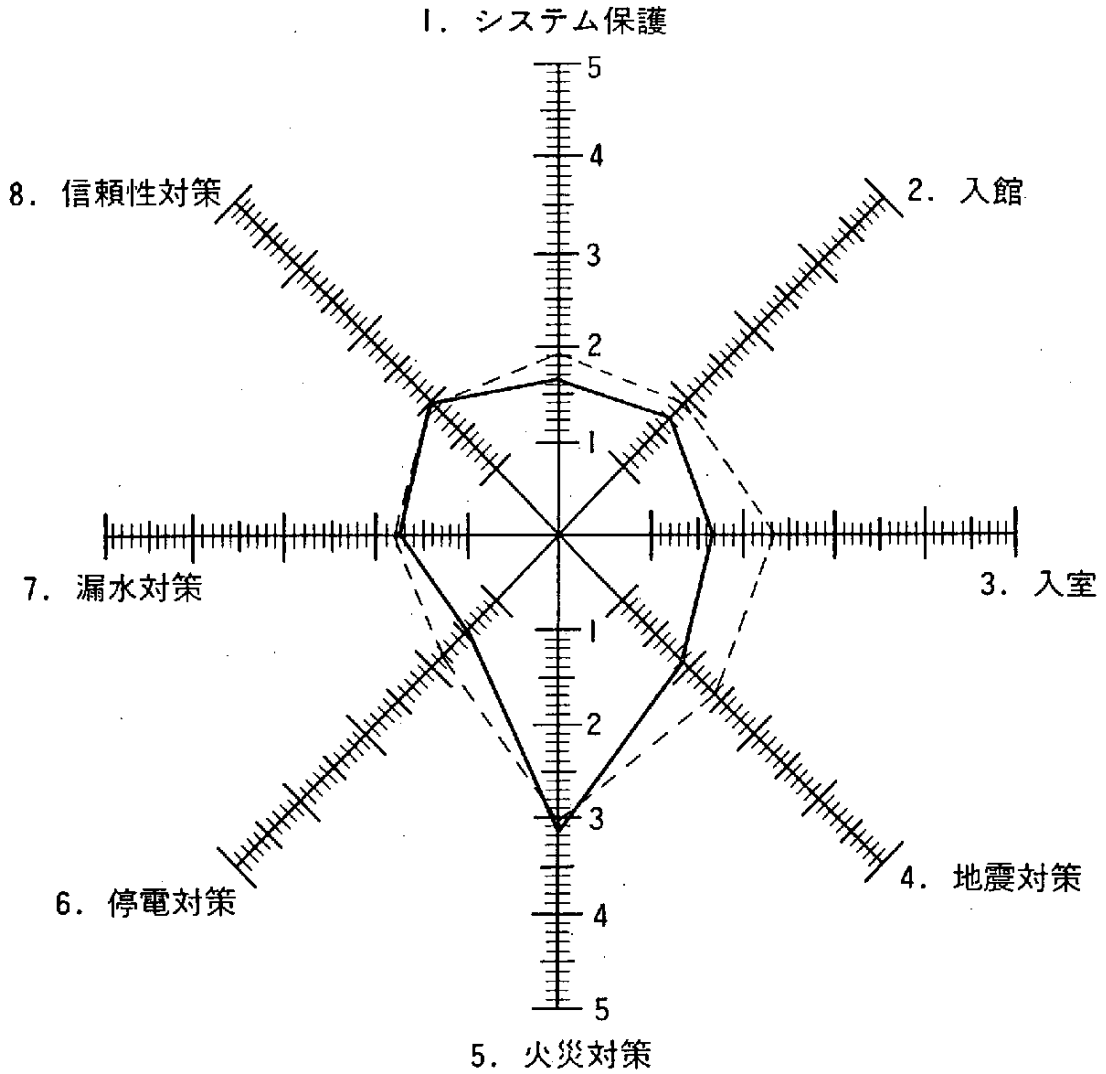
鉄　鋼　業



－－－：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
鉄　鋼　業	1．62	1．69	2．29	2．43	3．00	1．64	1．36	2．36

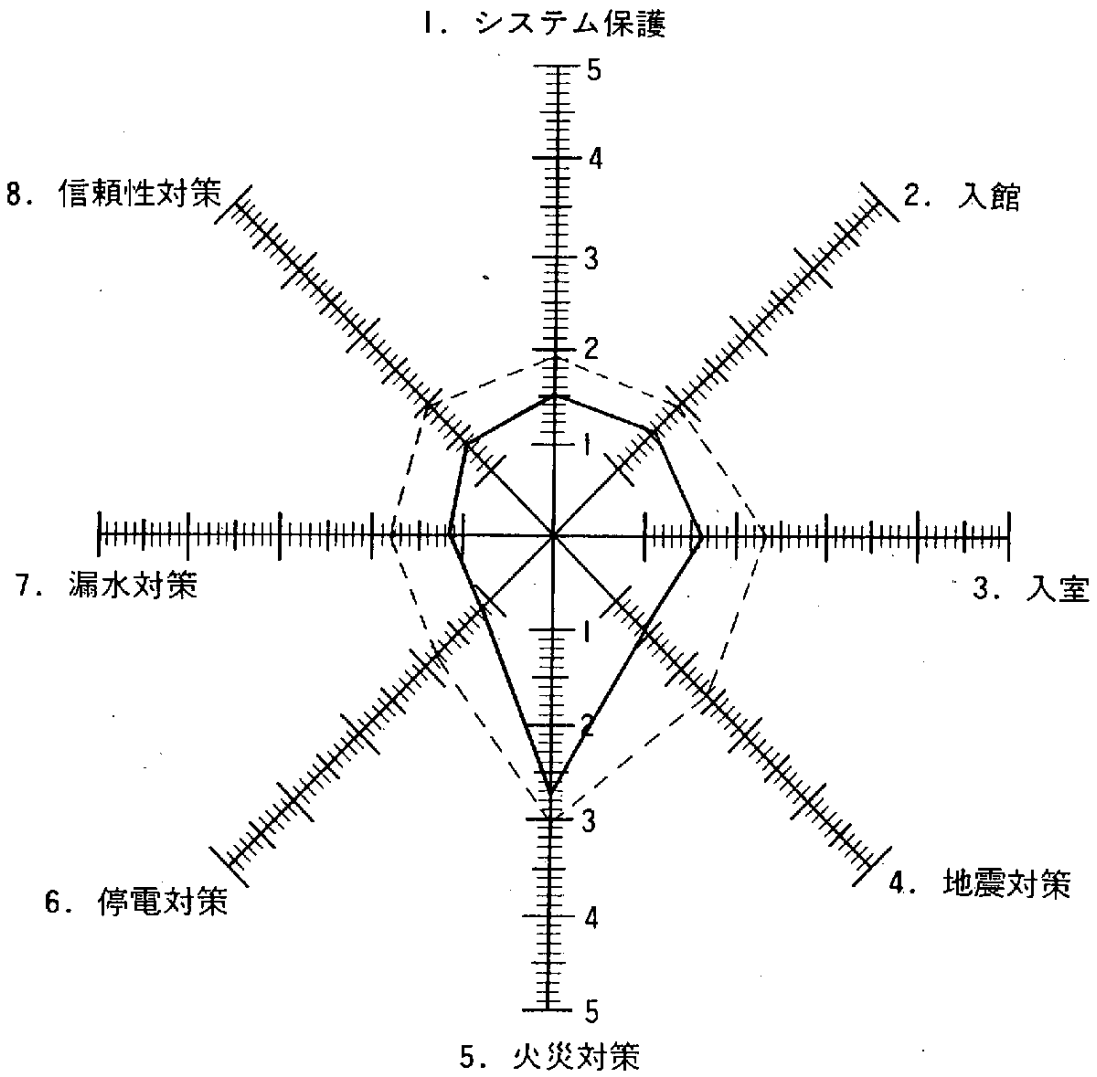
非鉄金属製造業・金属製品製造業



----：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
非鉄金属製造業・金属製品製造業	1．68	1．71	1．68	1．91	3．17	1．45	1．74	2．00

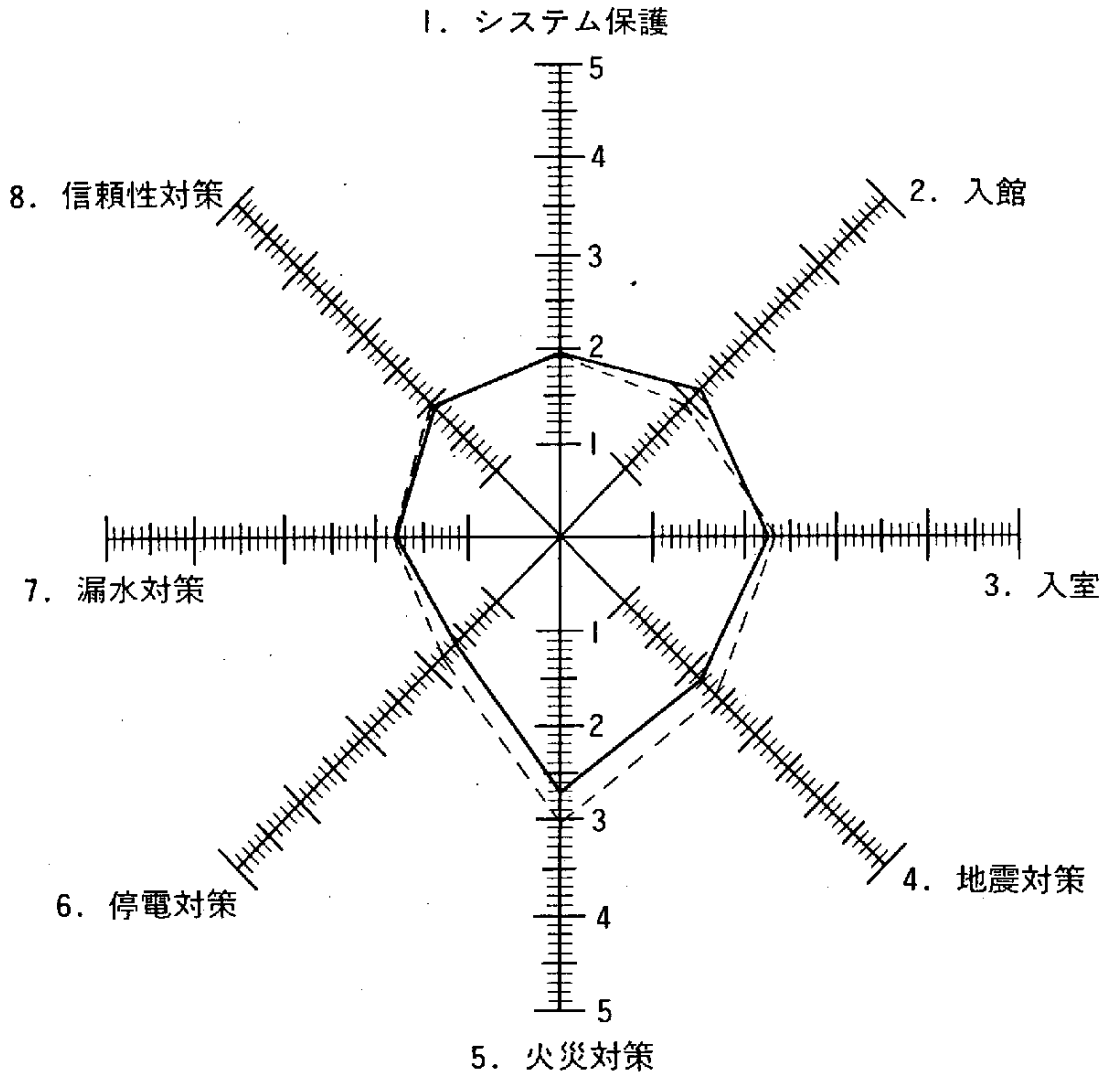
一般機械器具製造業



----：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
一般機械器具製造業	1．52	1．55	1．64	1．44	2．74	1．12	1．17	1．38

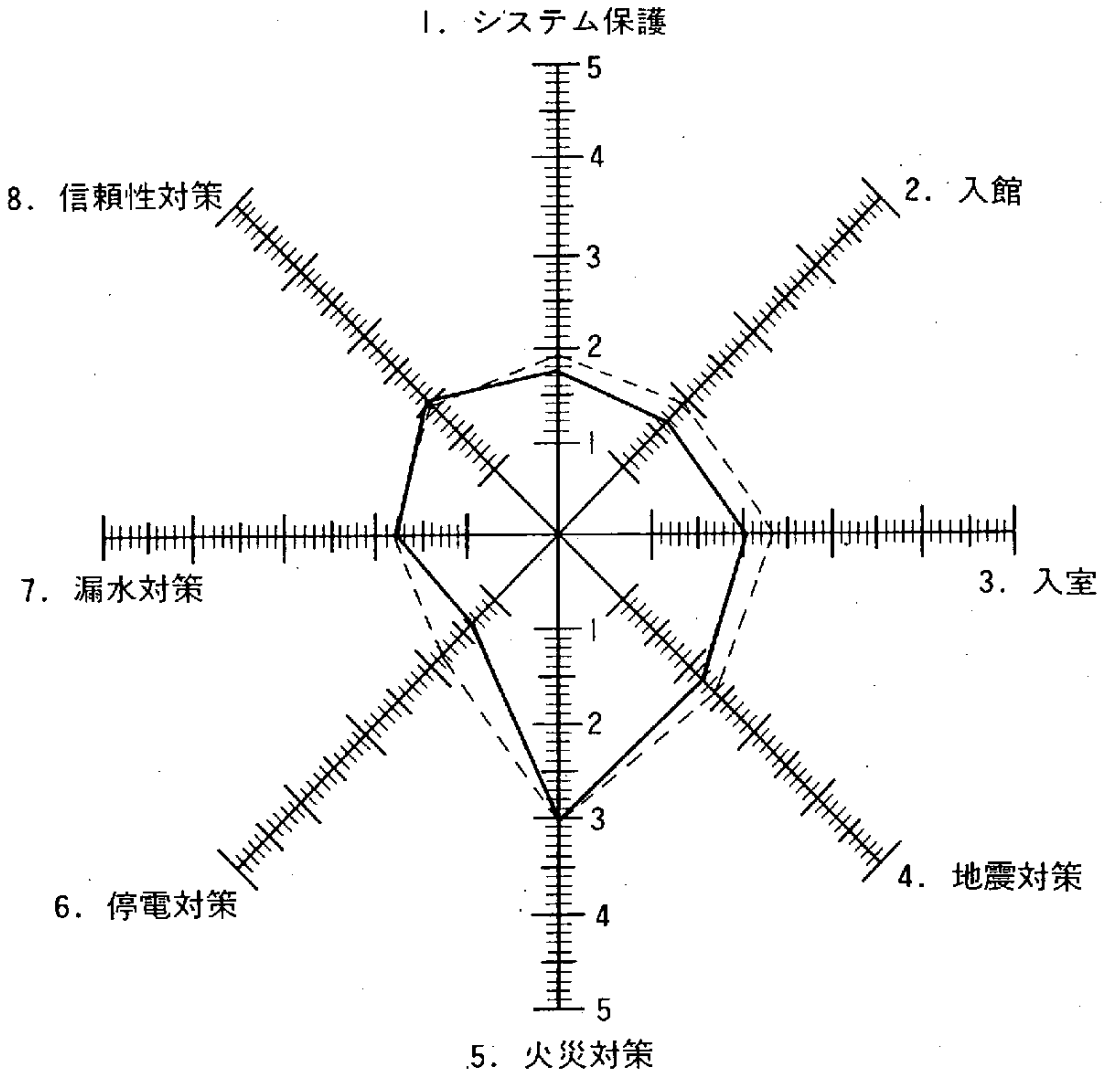
電気機械器具製造業



－－－：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
電気機械器具製造業	1．98	2．15	2．25	2．18	2．71	1．64	1．80	1．91

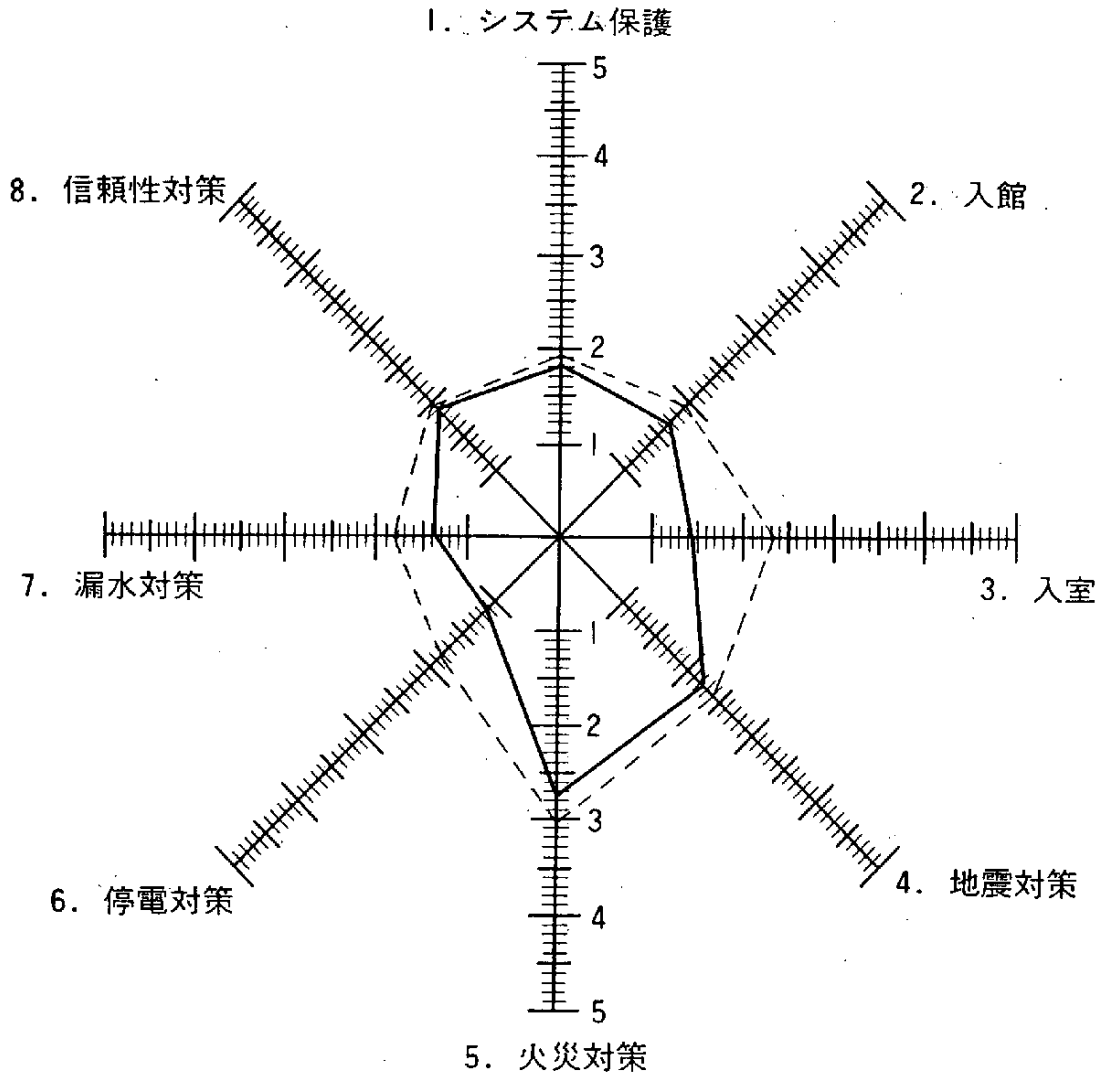
輸送用機械器具製造業



－－－：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
輸送用機械器具製造業	1．75	1．65	2．03	2．21	3．03	1．36	1．82	2．03

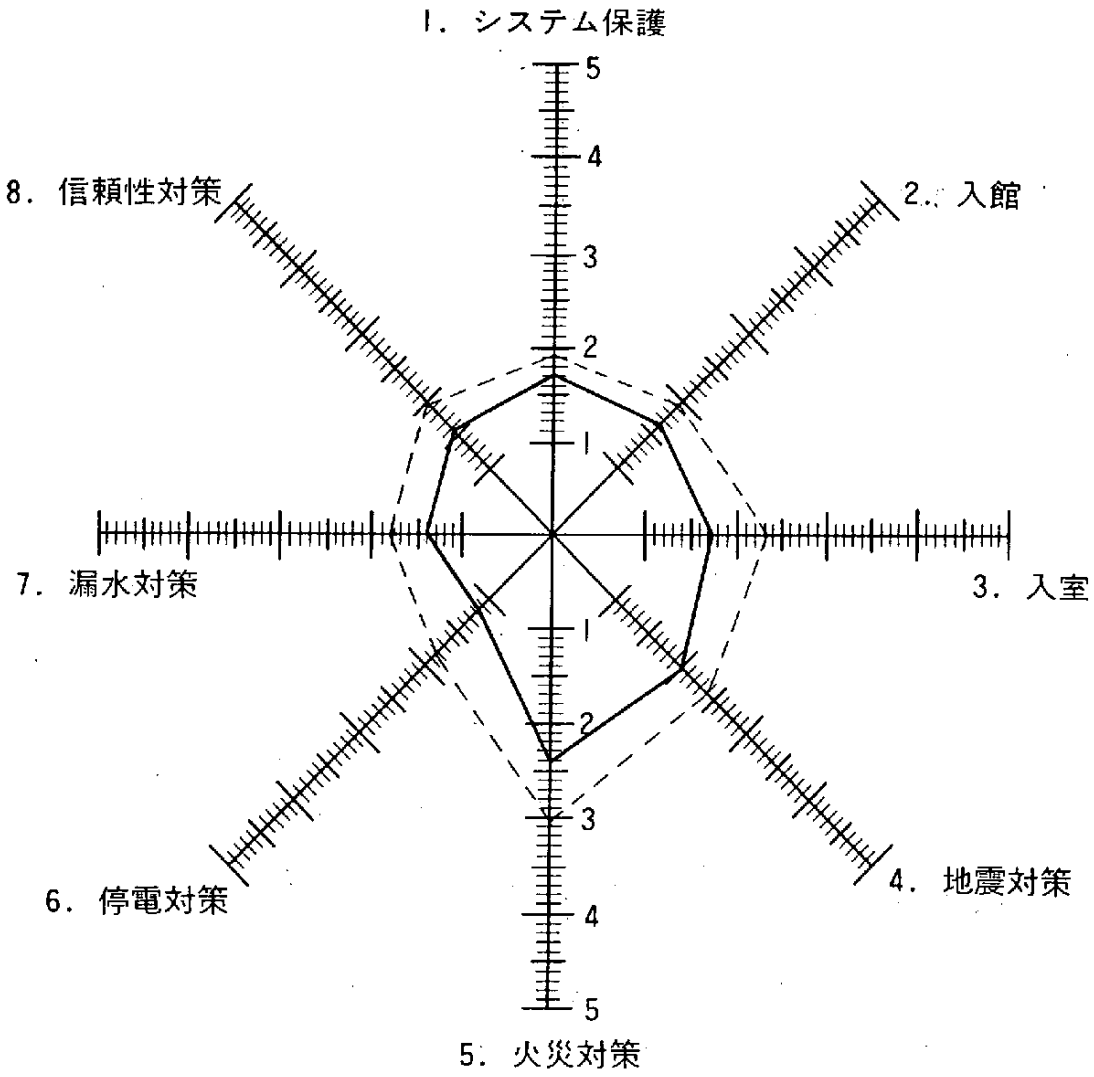
精密機械器具製造業



---：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	1.92	1.95	2.33	2.40	3.05	1.82	1.83	1.98
精密機械器具製造業	1.81	1.69	1.44	2.25	2.75	1.13	1.38	1.88

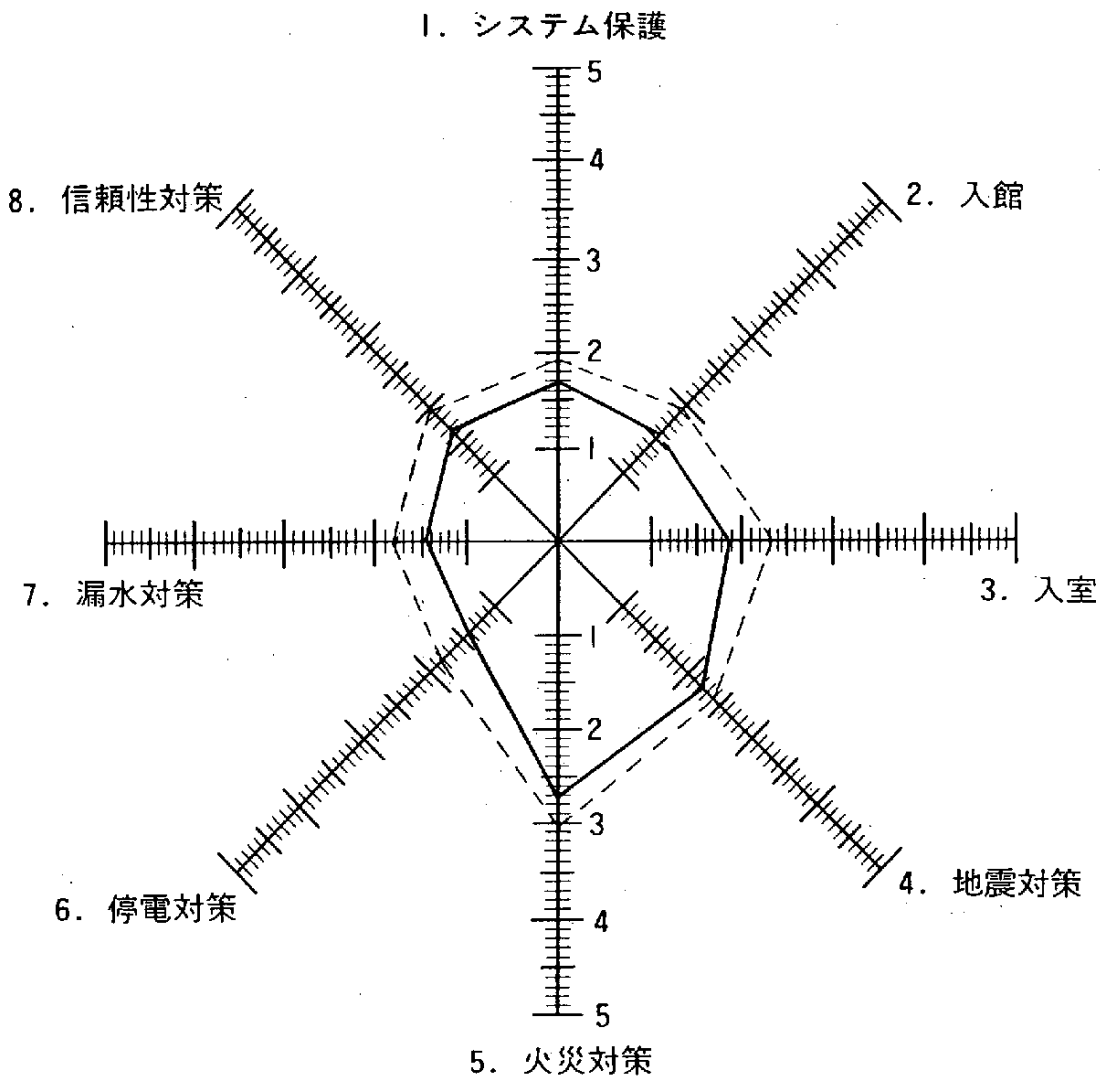
その他の製造業



----：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
その他の製造業	1．72	1．64	1．72	2．00	2．40	1．16	1．40	1．57

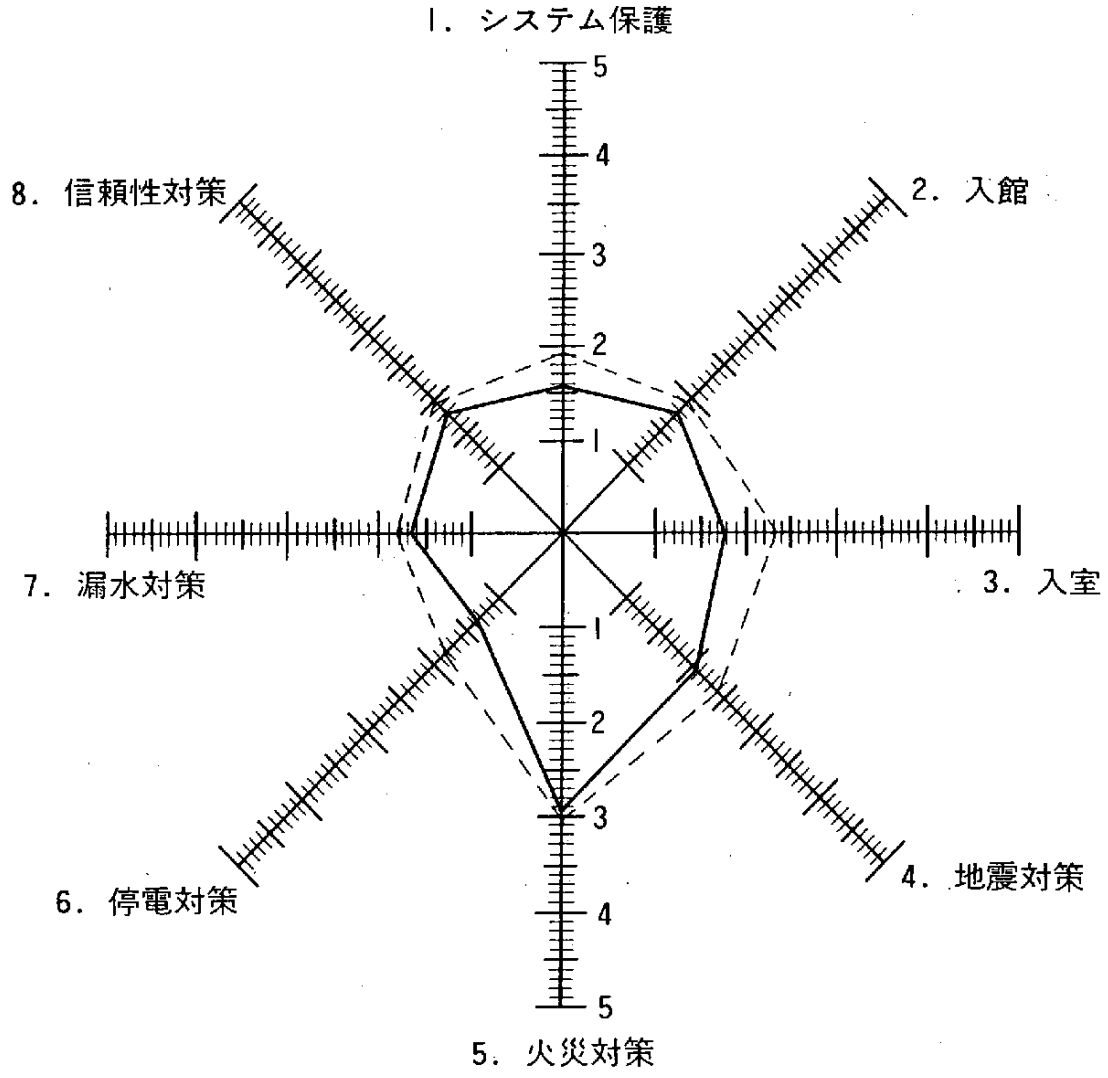
卸業・商社



---：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
卸業・商社	1．70	1．57	1．88	2．22	2．71	1．41	1．45	1．66

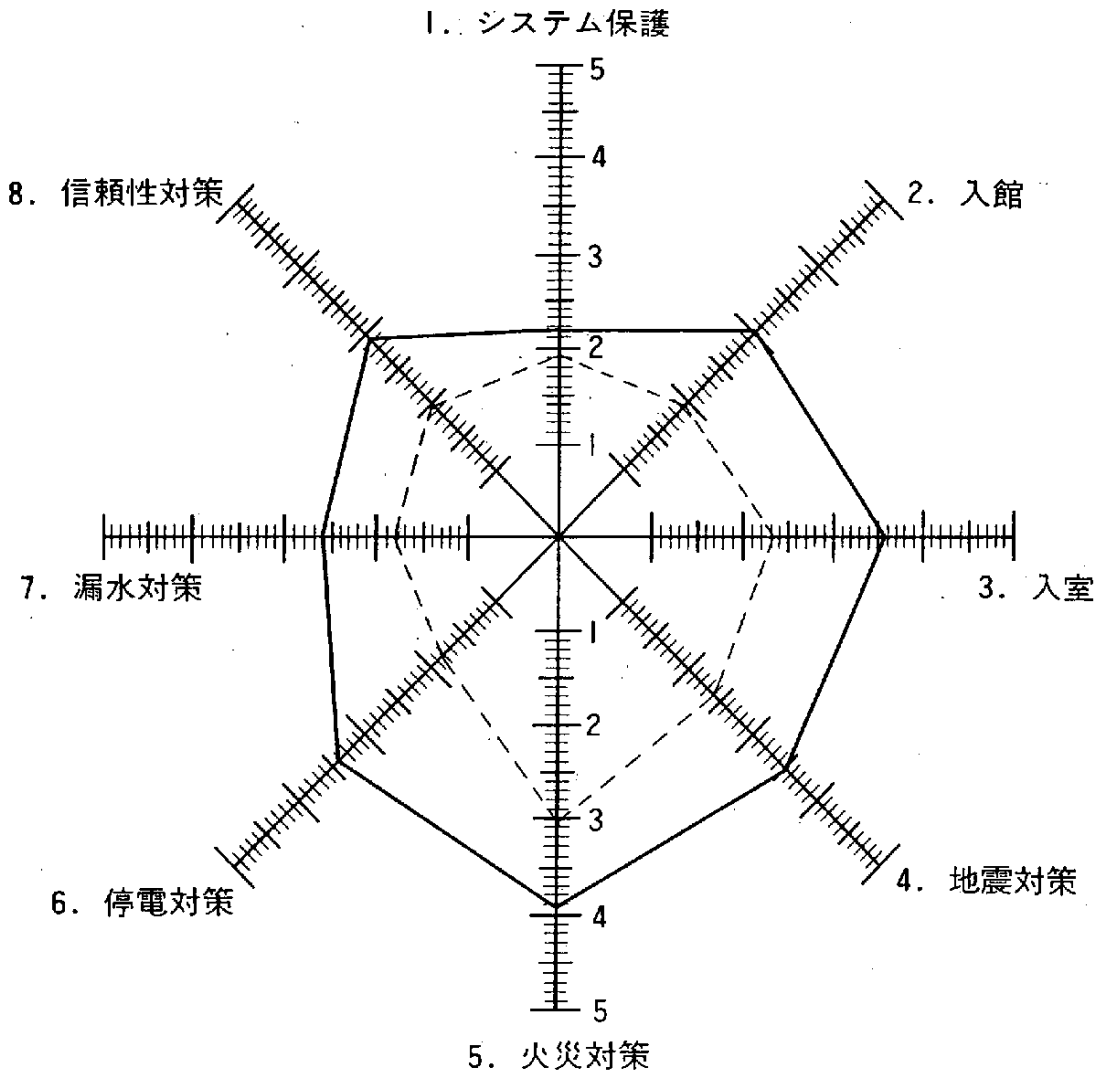
小　売　業



－－－：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	1.92	1.95	2.33	2.40	3.05	1.82	1.83	1.98
小　売　業	1.59	1.78	1.78	2.05	2.97	1.34	1.65	1.79

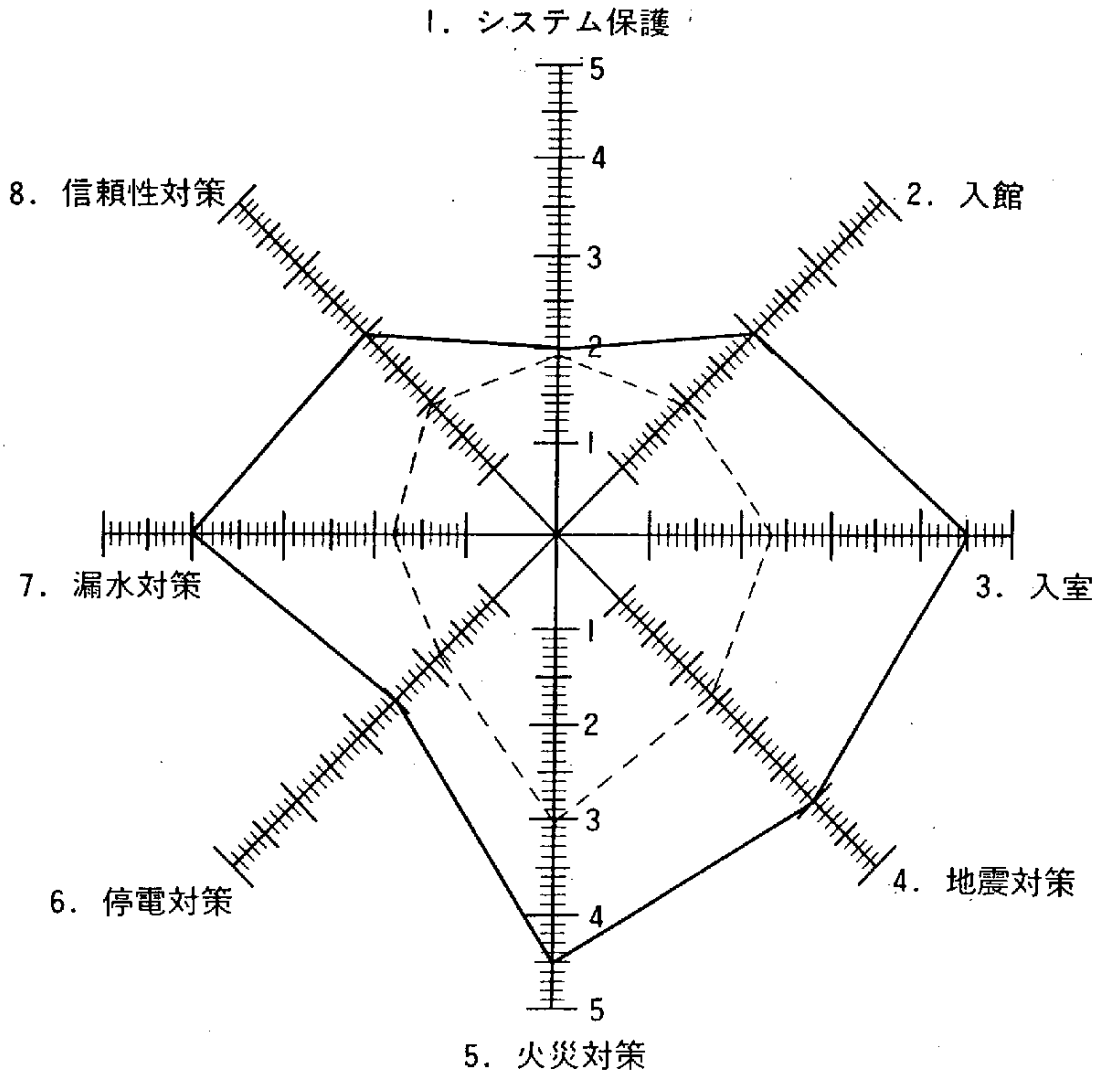
金　融　業



――：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	1.92	1.95	2.33	2.40	3.05	1.82	1.83	1.98
金　融　業	2.18	3.01	3.58	3.51	3.92	3.42	2.62	2.93

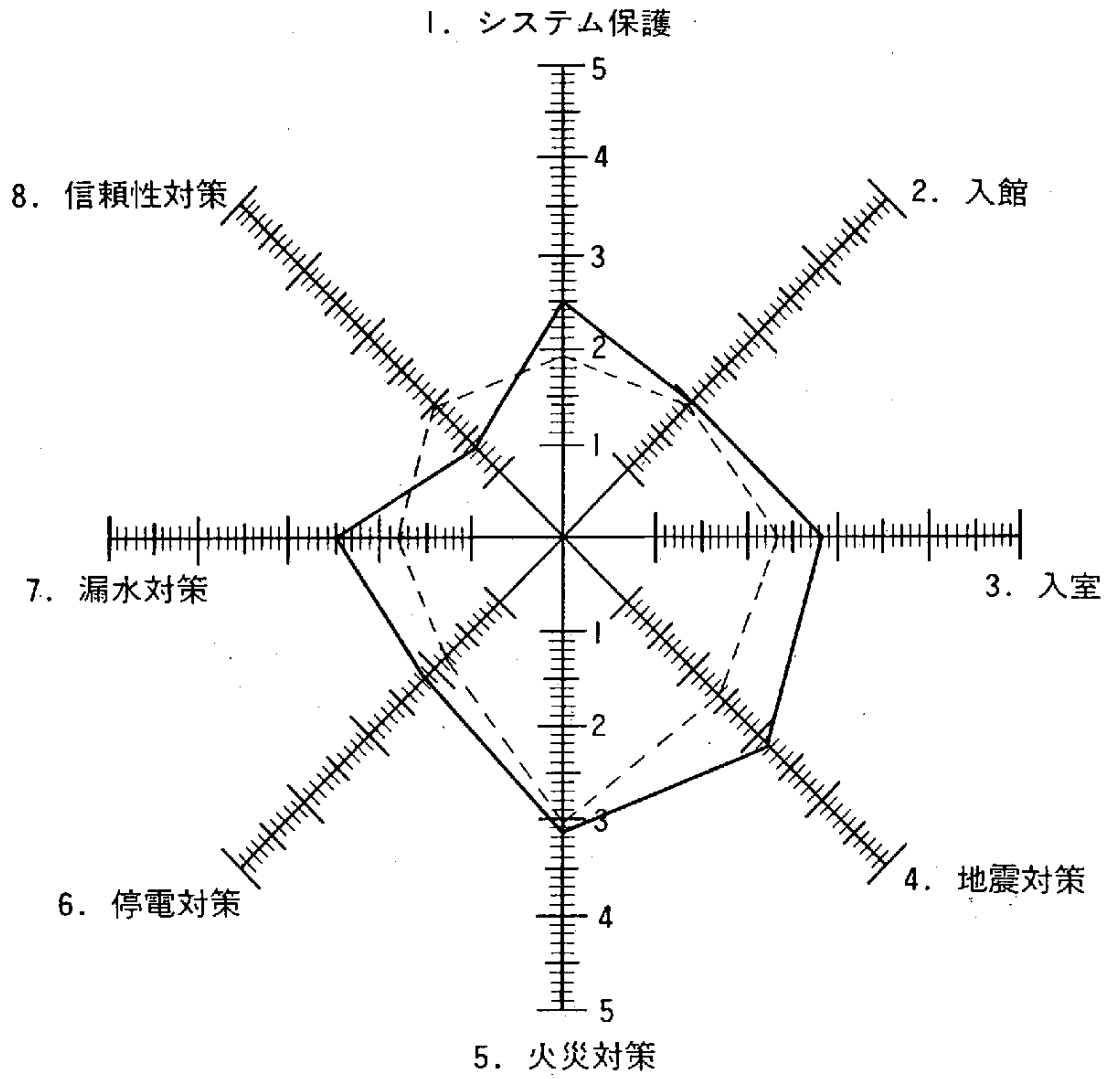
証券業・商品取引業



----：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
証券業・商品取引業	2．00	3．00	4．50	4．00	4．50	2．50	4．00	3．00

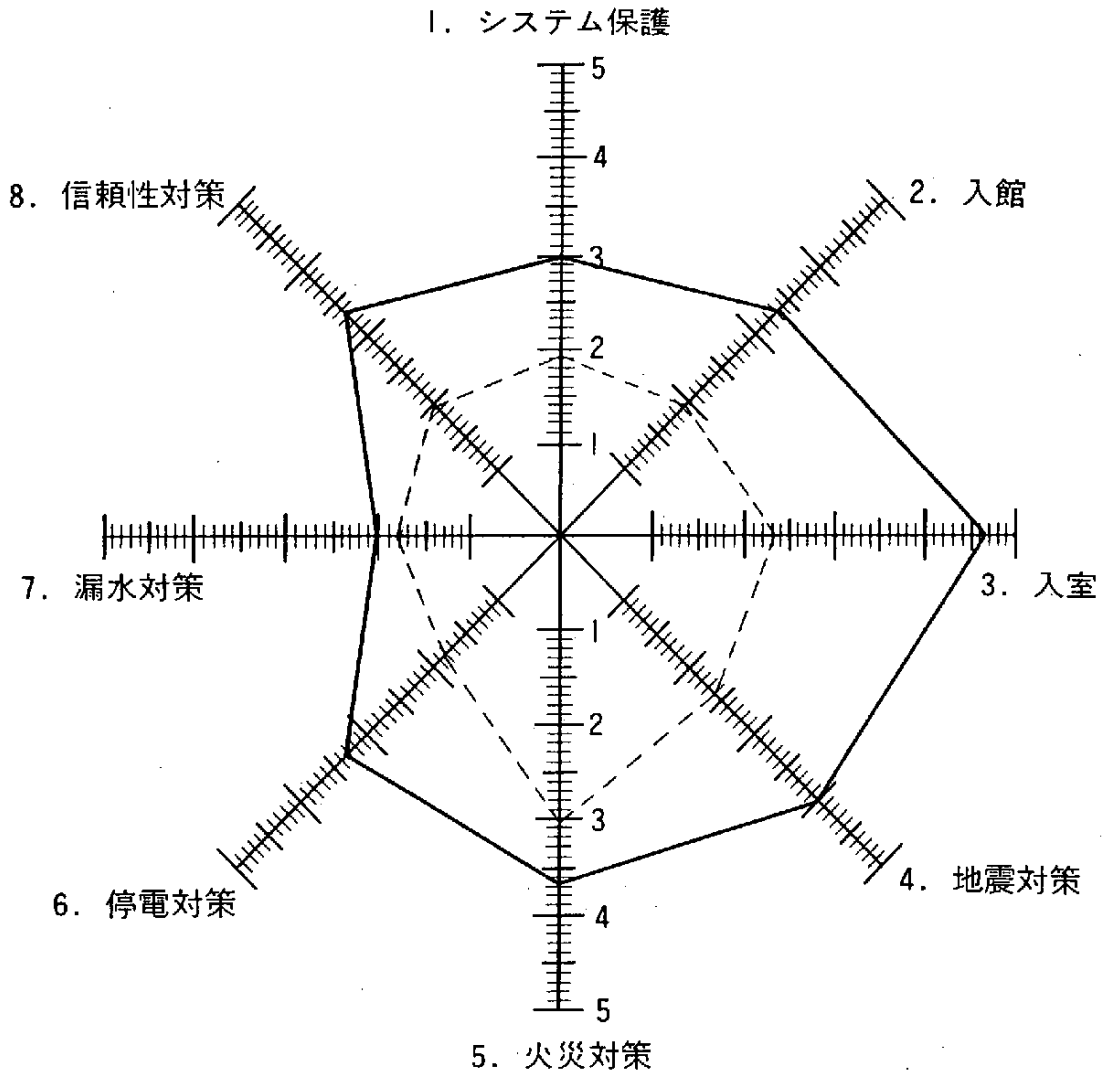
生命保険業(含代理業・サービス業)



---：全産業平均

	1.システム保	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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
生命保険業(含代理業・サービス業)	2．50	2．00	2．83	3．17	3．17	2．17	2．50	1．33

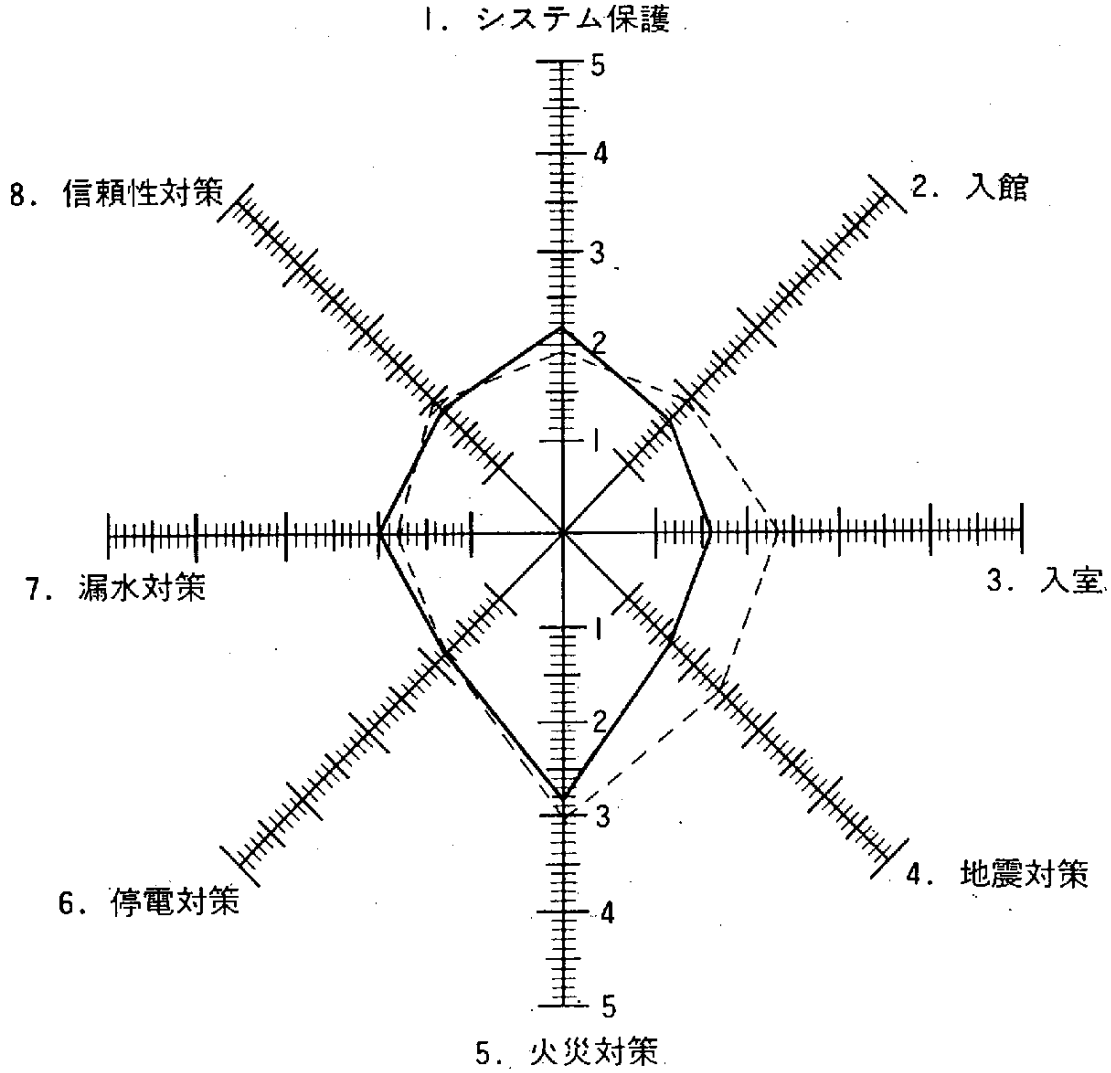
損害保険業(含代理業・サービス業)



－－－：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
損害保険業（含代理業・サービス業）	3．00	3．33	4．67	4．00	3．67	3．33	2．00	3．33

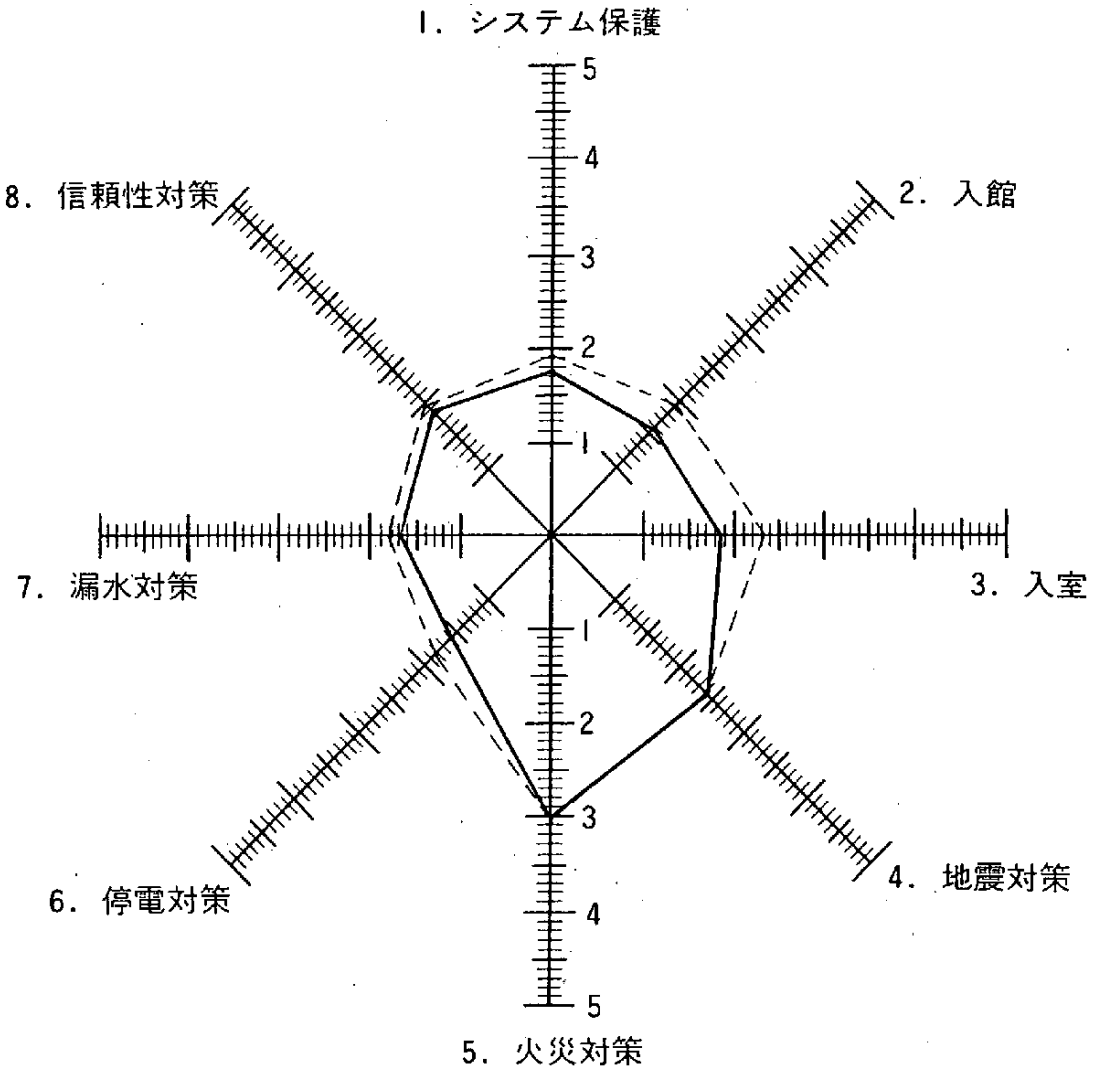
不動産業



----：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	1.92	1.95	2.33	2.40	3.05	1.82	1.83	1.98
不動産業	2.17	1.67	1.60	1.67	2.83	1.83	2.00	1.83

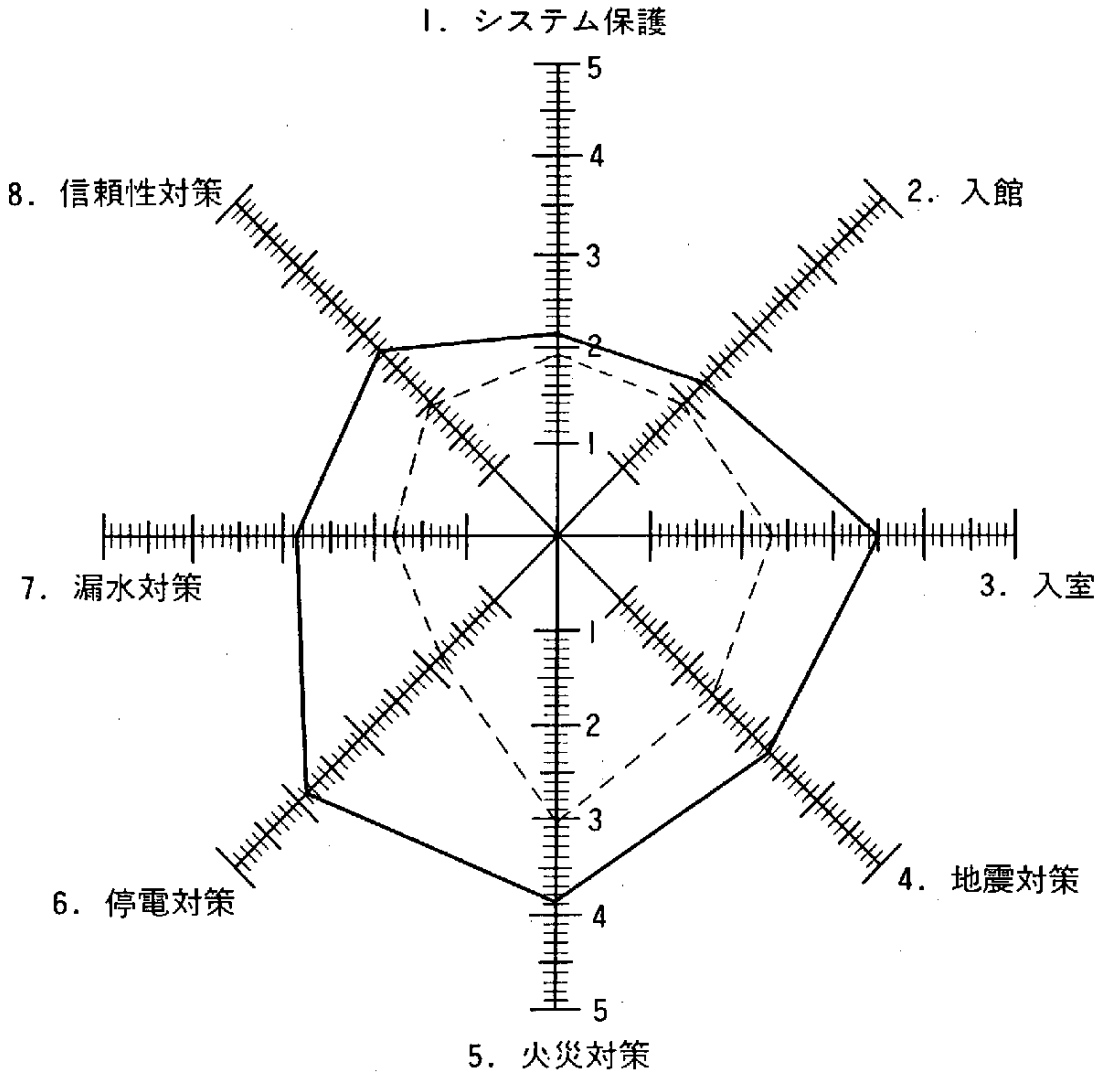
運輸・通信・倉庫業



－－－：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
運輸・通信・倉庫業	1．76	1．58	1．87	2．41	3．00	1．59	1．69	1．85

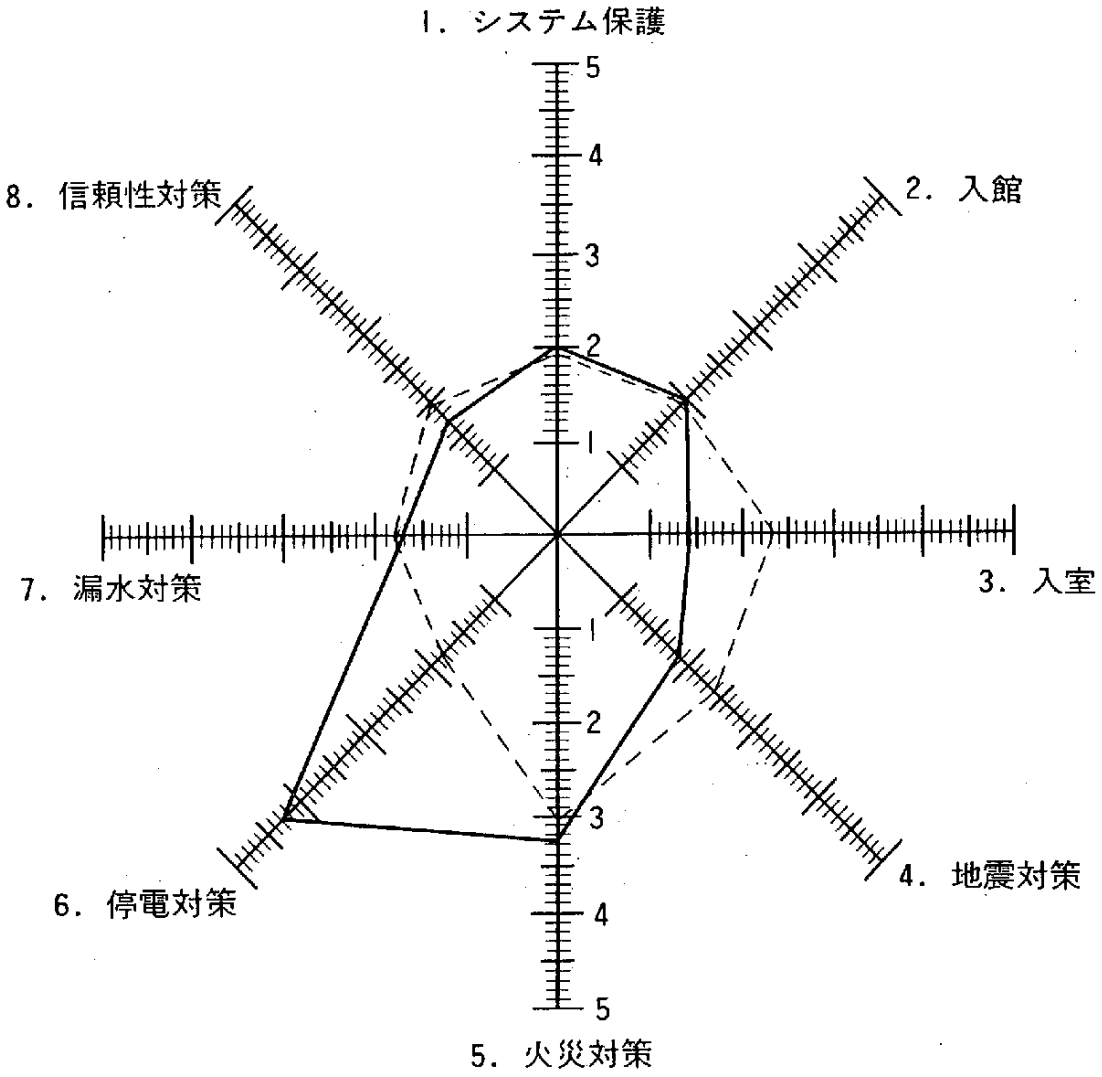
電力・ガス事業



－－－：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
電力・ガス事業	2．13	2．25	3．50	3．25	3．88	3．88	2．88	2．75

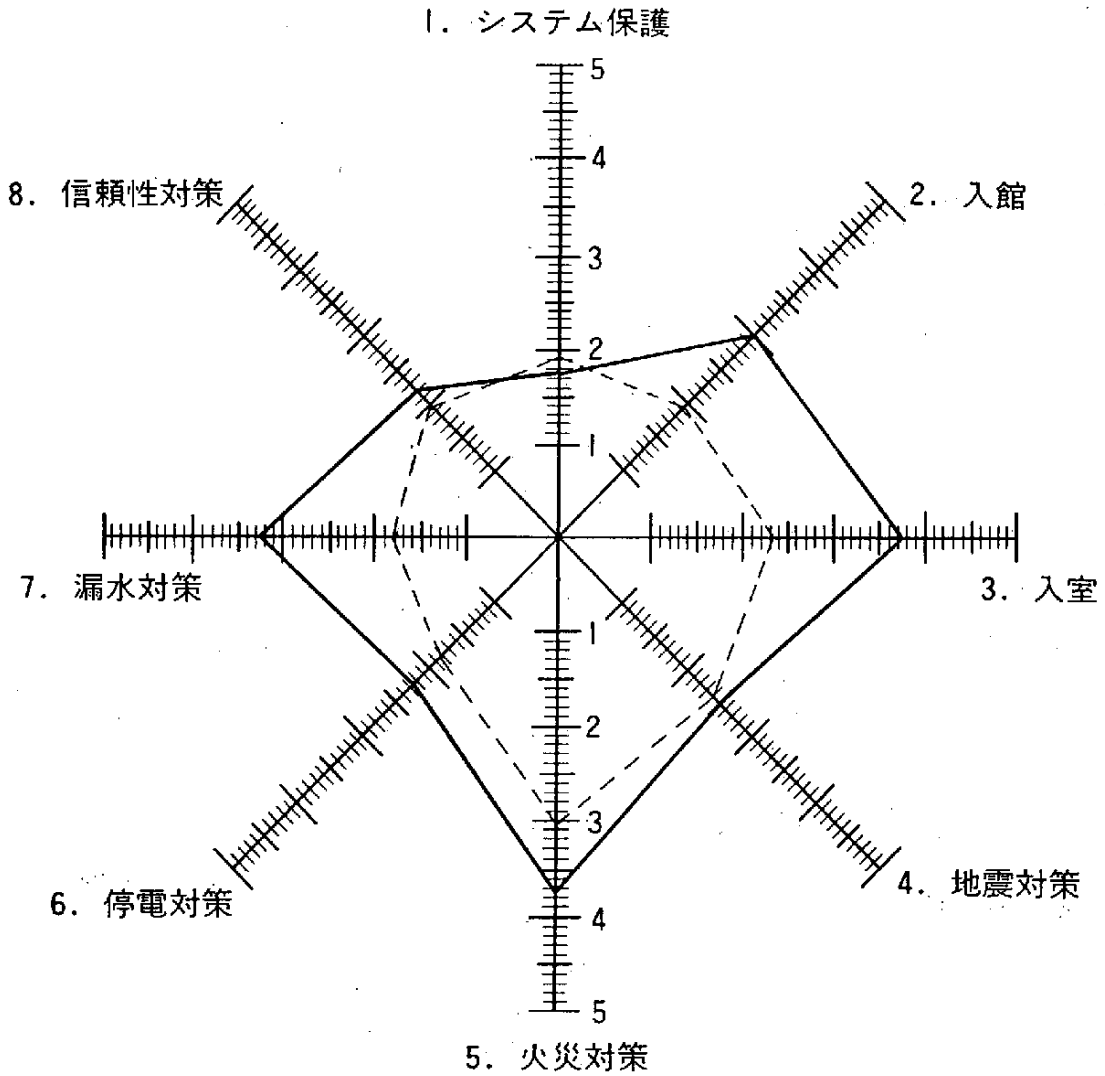
放　送　業



----：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
放　送　業	2．00	2．00	1．43	1．86	3．29	4．29	1．71	1．71

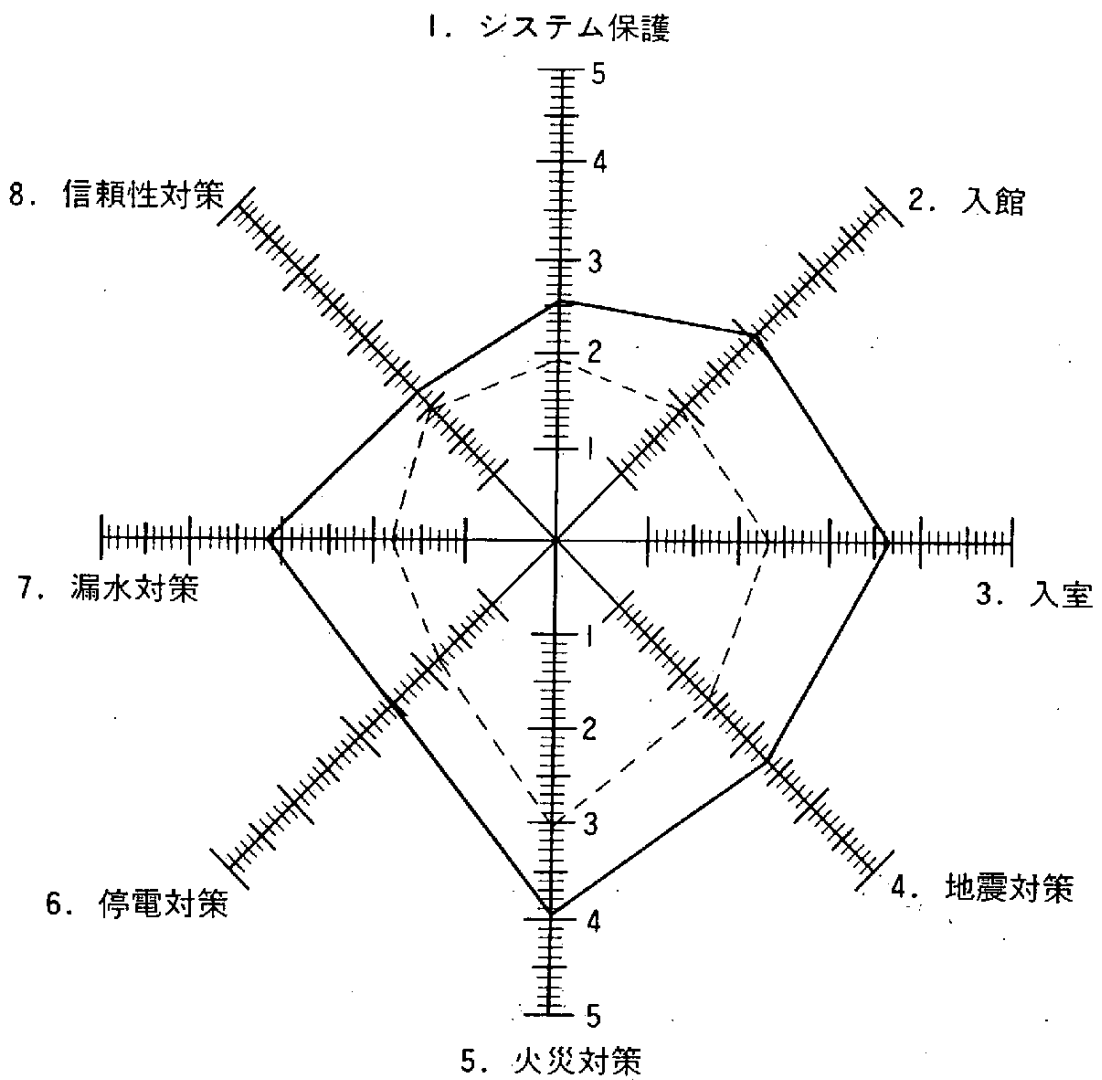
広告・調査・情報提供サービス業



－－－：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
広告・調査・情報提供サービス業	1．75	3．00	3．75	2．50	3．75	2．25	3．25	2．20

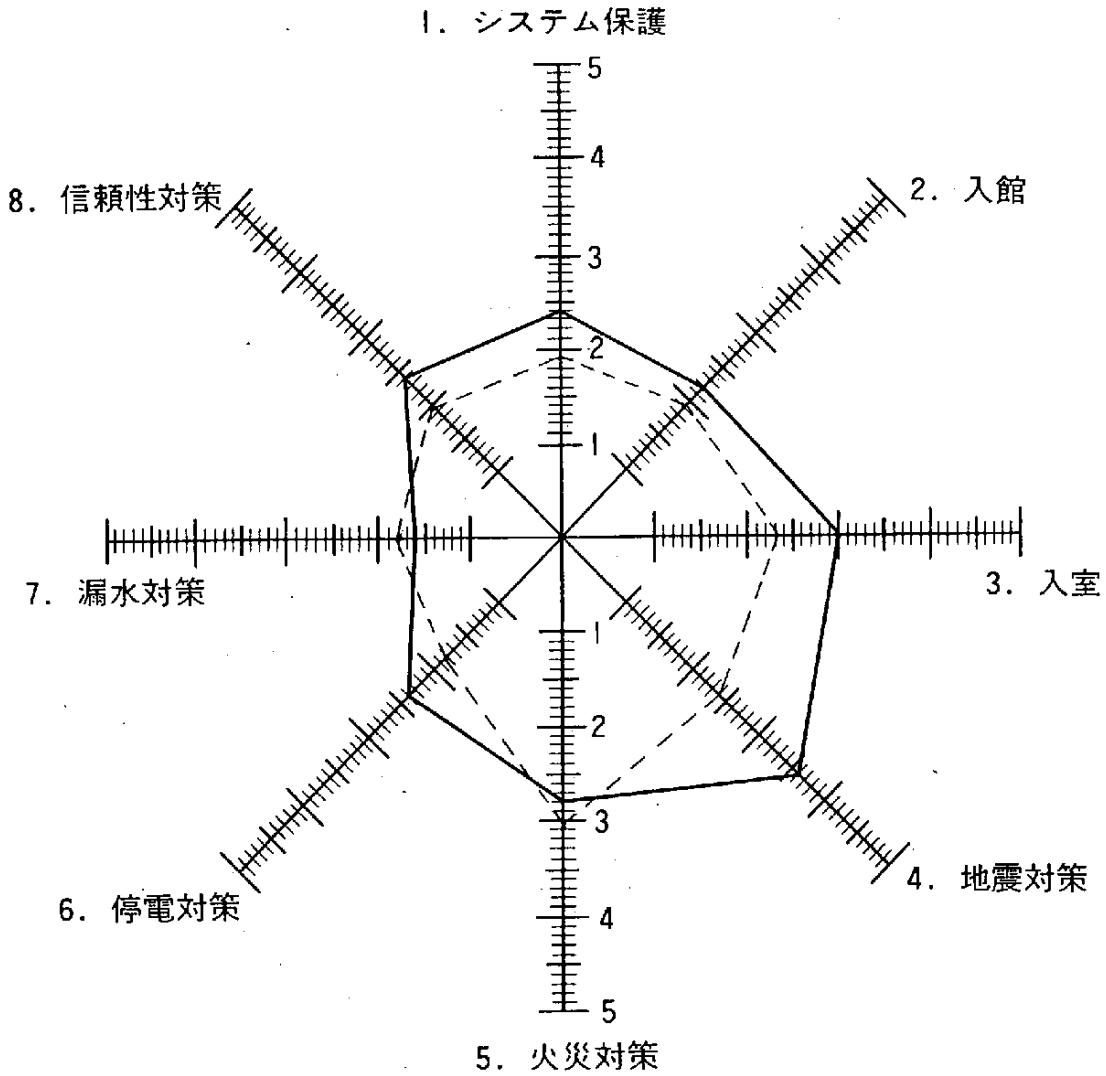
情報処理サービス業・ソフトウェア業



----：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
情報処理サービス業・ソフトウェア業	2．53	3．05	3．64	3．32	3．97	2．53	3．18	2．21

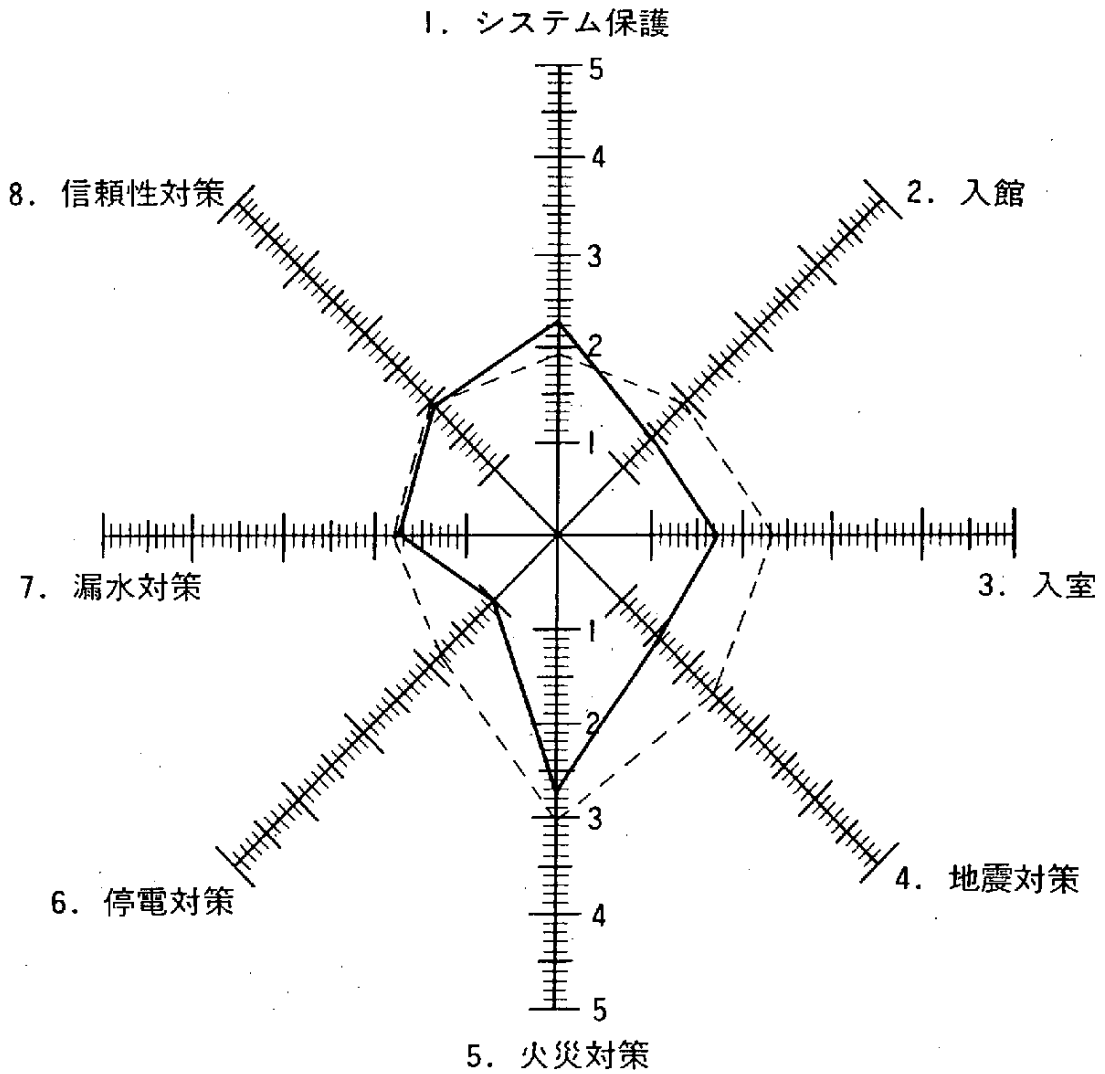
医　療　業



----：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
医　療　業	2．40	2．20	3．00	3．60	2．80	2．40	1．60	2．40

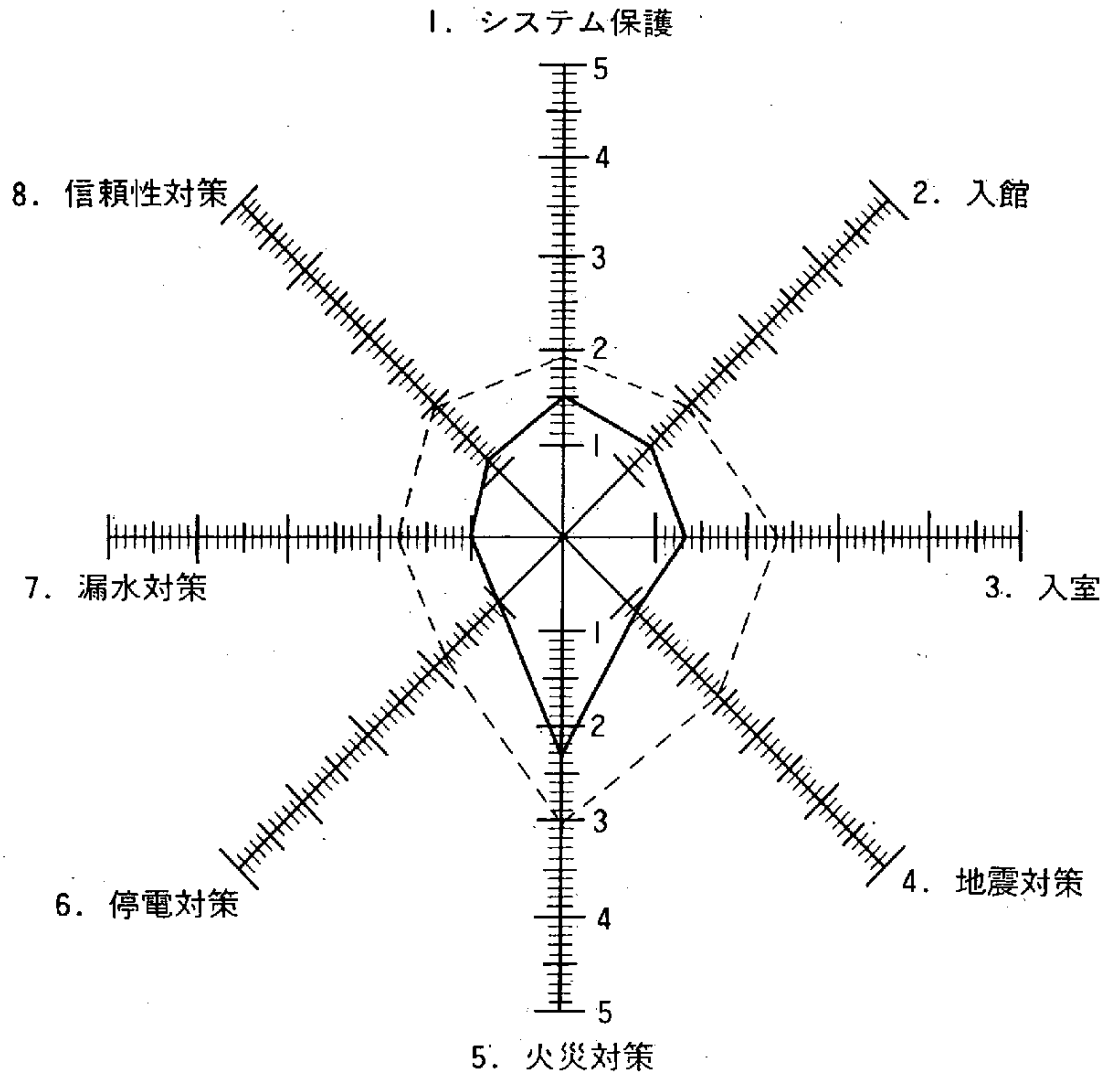
大　　学



――：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
大　　学	2．25	1．42	1．75	1．58	2．75	1．00	1．75	1．91

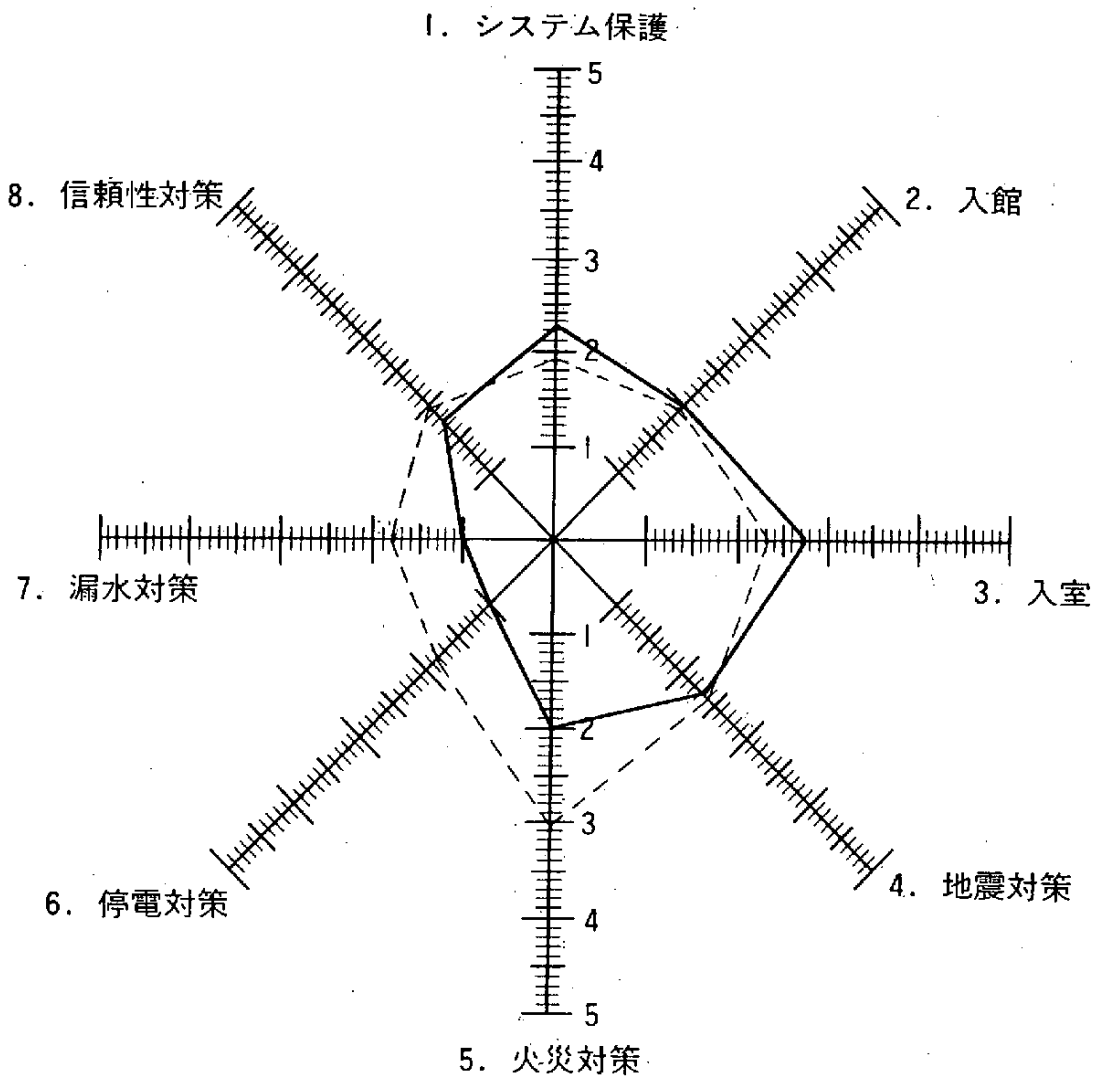
その他の教育機関



----：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	1.92	1.95	2.33	2.40	3.05	1.82	1.83	1.98
その他の教育機関	1.50	1.33	1.33	1.17	2.33	1.00	1.00	1.17

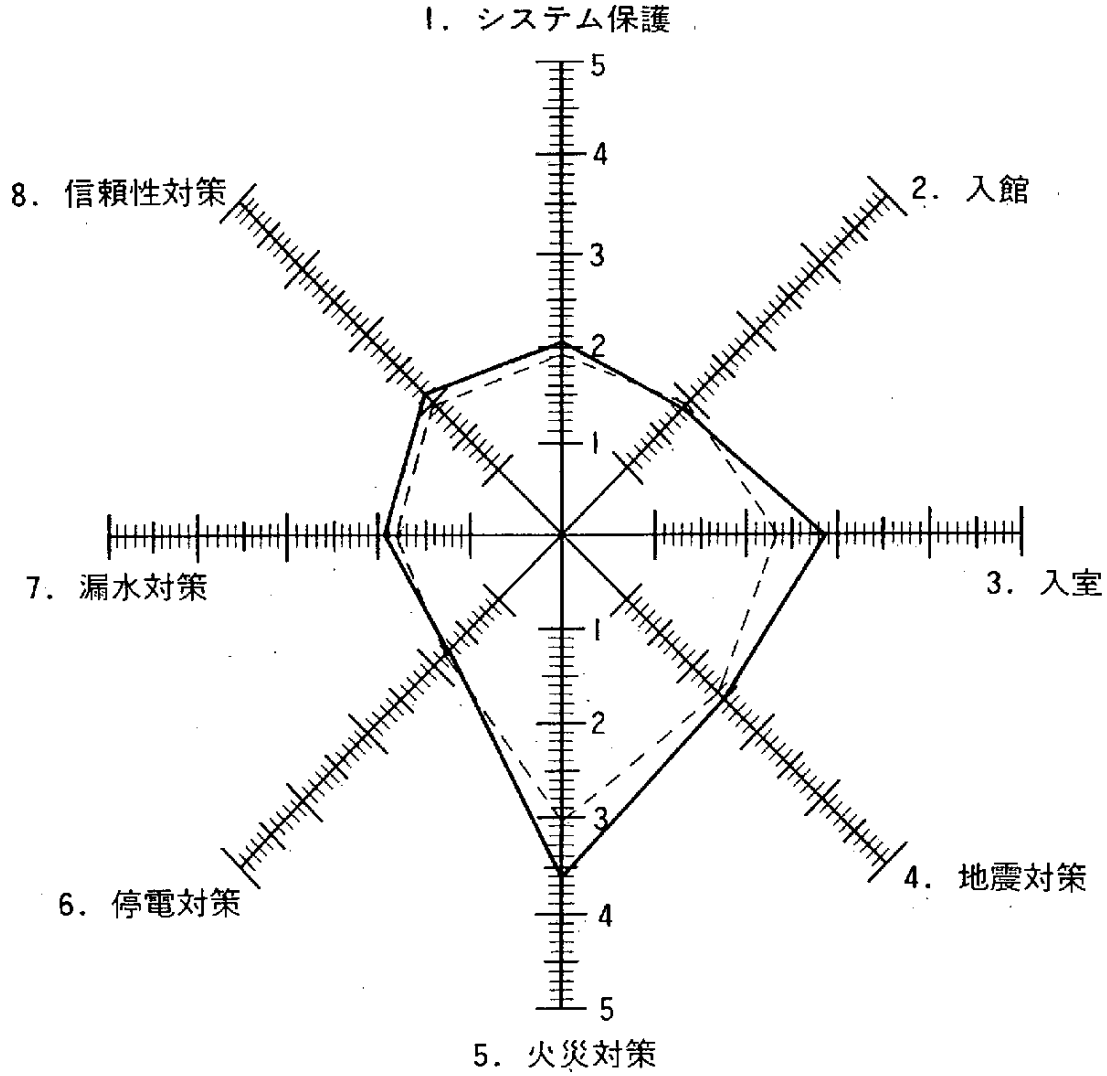
学術研究機関



---：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	1.92	1.95	2.33	2.40	3.05	1.82	1.83	1.98
学術研究機関	2.25	2.00	2.75	2.33	2.00	1.00	1.00	1.75

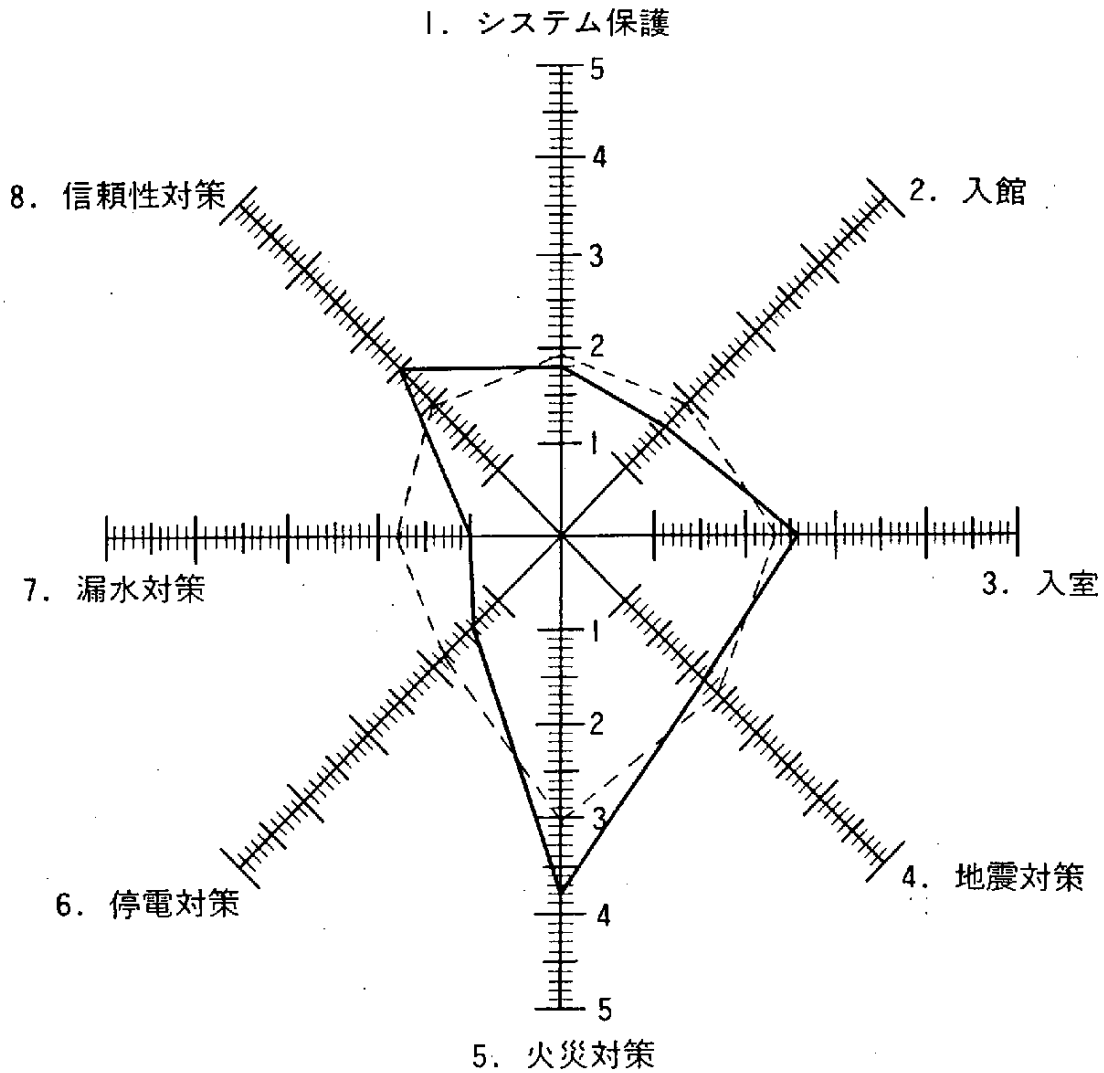
法人団体・農協



---：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
法人団体・農協	2．06	1．88	2．88	2．50	3．61	1．78	1．94	2．11

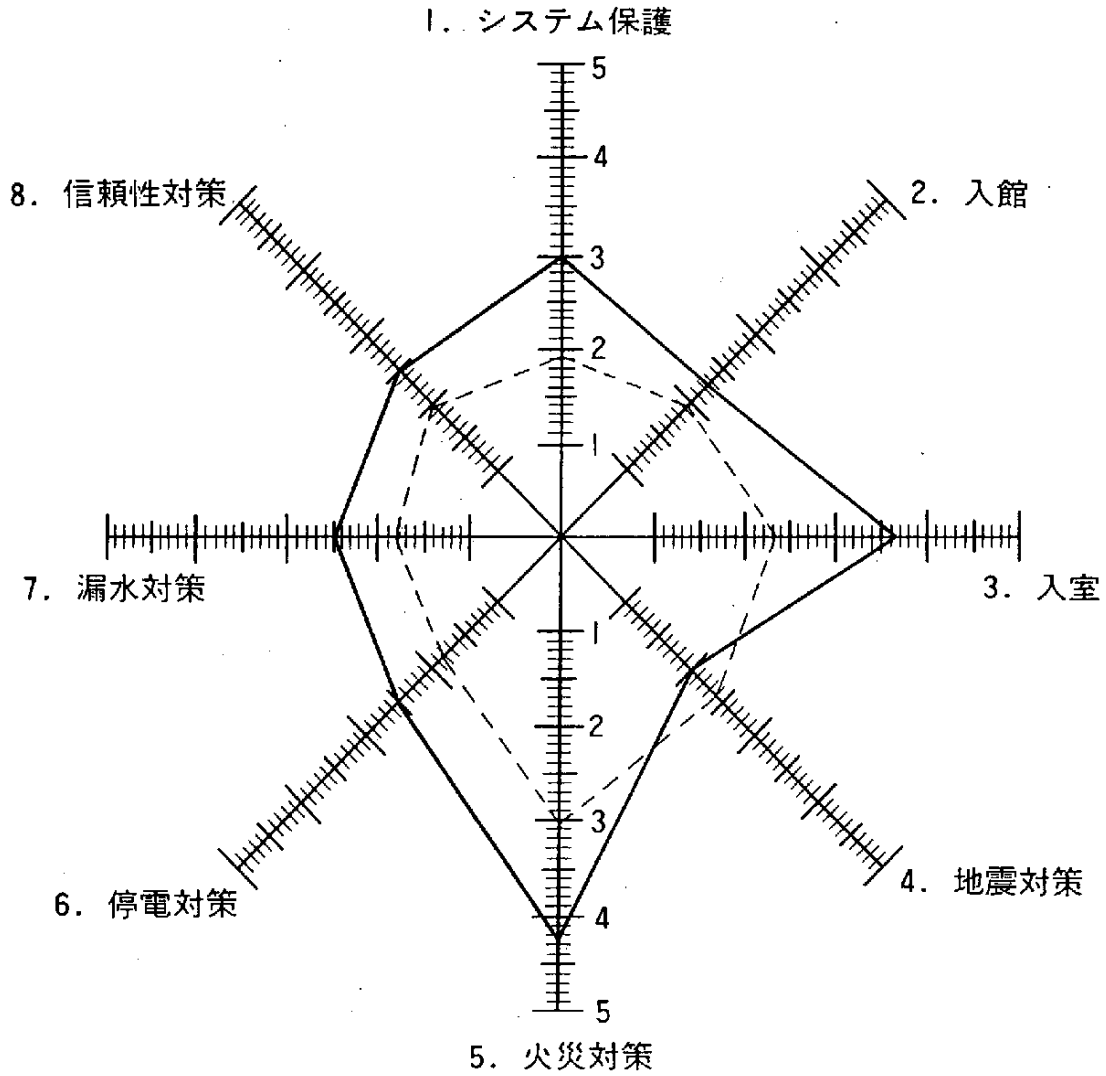
その他のサービス業



---：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
その他のサービス業	1．80	1．60	2．60	2．20	3．80	1．40	1．00	2．50

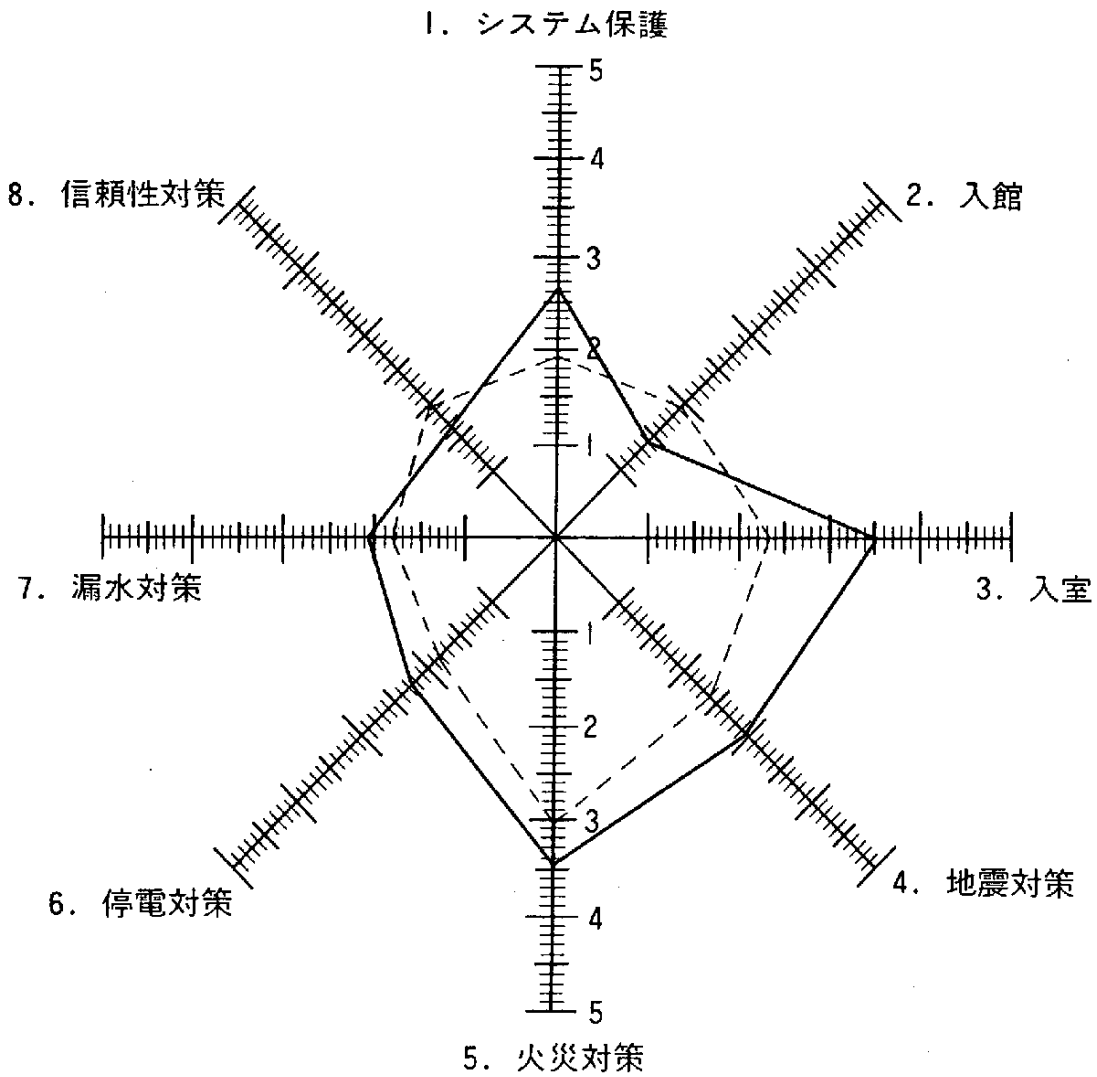
政　　府



－－－：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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
政　　府	3．00	2．25	3．67	2．00	4．25	2．50	2．50	2．50

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	1．92	1．95	2．33	2．40	3．05	1．82	1．83	1．98
地方公共団体	2．64	1．41	3．52	2．96	3．46	2．25	2．07	1．68

平成元年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（432）9387（代表）

印刷所　三協印刷株式会社
東京都渋谷区渋谷3丁目11番11号
TEL（407）7316

63—R007