

01-R006

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 2 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、平成元年度に実施した「セキュリティに関する調査研究」の一環としてとりまとめたものであります。

序

当協会では、昭和59年に、コンピュータセキュリティに関するリスク分析手法の確立を図ることを目的として、「リスク分析委員会」を設置し、その後6年間にわたり、リスク分析について理論的研究、実務的研究、アンケート調査、あるいは海外文献調査など、多面的に調査研究を続けてきた。

本調査研究では、とくに実務に役立つリスク分析手法の確立をめざすこととし、そのため、その有効性を生かしつつ簡便性を重視した。

このような状況の中で、本プロジェクトでは、モデルを作成してそれを対象にリスク分析を試みるアプローチを行った。たとえば、銀行とか製造業のモデルを作成し、特定の業務について問題点を想定してリスク分析作業を試みた。

その結果、たとえば損失の評価方法については、金額評価法、カテゴリー評価法などの具体的な手順を掲示することができた。また、既存の情報を利用して、コンピュータの基礎知識を持つ者なら誰でも簡単に行えるリスク分析の手法として、通商産業省から公表されている電子計算機システム安全対策基準を活用するチェックリスト法を提案した。

本報告書は、6年間にわたるリスク分析調査研究の成果であるが、企業の中でリスク分析に取り組まれる方々にとって、何らかの参考になり、お役に立てば幸いである。

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2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	郡 山 信	(財)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(株) サービス技術・品質保証-CSP 副部長
	佐 藤 孝 雄	日本ケーブルメディアエンジニアリング(株) 副技師長
	佐 藤 雅 春	日本コンピュータセキュリティ(株) コンサルティング部長
	田 口 孝 弘	国際ファジィ工学研究所 常務理事
	竹 井 正 昭	東京海上火災保険(株) 情報システム部運用課長
	中 川 吉 朗	インフォメーション・システムサービス(株) 代表取締役
	南 波 駿太郎	日本銀行金融研究所 研究第2課長
	花 香 俊 明	コンサルタント
	三 谷 保 夫	(株)ポム 代表取締役
	森 永 正 廣	N T T データ通信(株) フィールドサービス事業部サービス企画担当部長

目 次

第1章 リスク分析に関する視点	1
1. 1 リスク分析委員会における作業の経緯	1
1. 2 作業での確認点	3
1. 3 リスク分析の範囲	4
1. 4 リスク分析を行う際の留意点	6
第2章 製造業における入金システムモデルのリスク分析	9
2. 1 モデルにおけるリスク分析	9
2. 2 代金請求・入金処理システムモデル	9
2. 3 損失タイプの確認と評価	13
第3章 リスク分析の方法	23
3. 1 リスク分析の手順	23
3. 2 リスク発生原因の確認	26
3. 3 チェックリスト法	35
付属資料1 FIPS PUB 65	49
付属資料2 外国文献抄録	87
付属資料3 セキュリティ対策水準の時系列分析	107
付属資料4 業種別セキュリティ対策水準の実態（1989年度）	131

第1章 リスク分析に関する視点

1. 1 リスク分析委員会での作業の経緯

現代社会は、「情報化社会」といわれるように、まさにコンピュータシステムなしに機能し得ないくらいコンピュータに依存する状況にある。日本での汎用コンピュータの実働台数は27万2,275台(1986年9月末現在)で、前年度末比で11.5%増となっている¹⁾。しかし、コンピュータシステムは「もろ刃の剣」である。システムそれ自体は完全でないがため、時としてシステムに異常が発生したり、また通信回線に異常が生じたりすれば、システムに依存する度合いが高いほど、システム利用の事業体は混乱に陥ることになる。このように、コンピュータシステムに依存する状況が増すに連れて、システム関連の脆弱性もまた増大する。

こうした背景から、リスク分析委員会では、リスク分析の必要性に鑑みて、昭和59年より、リスク分析のための方法論を模索する作業に取り組んだのである。これまでの経緯を簡潔にたどってみると、次のとおりである。

昭和59年度には、リスク分析の何たるかを理解するため、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た。とくに米国商務省標準局におけるデータ処理の物理的セキュリティおよびリスクマネジメントに関するガイドライン、さらにIBM社のEDPシステムセキュリティリスクアセスメント、行政管理庁行政管理局におけるデータ保護マニュアルを概説し、わが国におけるリスク分析の適用例を紹介した²⁾。

また、昭和60年度には、「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。そこで明らかにされたことは、リスク分析を実施している企業が、調査対象企業の21.8%にすぎず、コンピュータリスクの影響分析について見ると、システム規模が大である事業体ほどリスク分析を実施し、システム規模が小である事業体ほど実施していないことであった。また問題点として明確化されたのは、リスク分析に「確立された手法がない」(73.9%)ことであった。いうなれば、リスク分析の実施には、まずは分析手法の確立が不可欠であることが認識されたのであった。さらに、同年には、付属資料に形ではあったが、米国商務省標準局が1979年8月に公表した“Guideline for Automatic Data Processing Risk Analysis”(FIPS PUB 65)を紹介した(本報告書の付属資料1に収録)。そこでは、リスク分析のガイドラインと銘を打っているように、経営者の役割から、リスク分析チーム、セキュリティの検討を踏まえ、リスク分析では、被害と頻度について数理的に明示し、分析の具体的事例が紹介されていた。³⁾

ところで、米国商務省標準局が出したガイドラインならびに同種の方法論に基づくリスク分析をそのままの形でわが国の事業体に適用できるかについて委員の間で議論が展開された。結局のところ、商務省標準局のガイドラインでは、たとえば被害と頻度との連環関係が整然とされ

ていても、その根拠が明確にされない限り、システム利用者側の理解なり合意は得られないであろうとの判断から、むしろリスク分析委員の手によるリスク分析手法の提示が必要とされた。

そして昭和61年度において、委員による地道な作業が開始されたのであった。コンピュータシステムの規模が大となれば、それだけセーフティガードが十分装備されるとの認識が一般的であるが、作業にあたって、リスクの影響を把握するリスク分析においては、まずセーフティガードのない状態を前提に出発するのが妥当であるとの合意がなされた。それは、すでにセーフティガードを装備したシステムを前提にしては、「始めにセキュリティないしセーフガードありき」ということにもなりかねず、論理的なリスクマネジメントのプロセスに鑑みても、論理の逆転になりかねないからであった。したがって、まず「始めにリスク分析ありき」という認識から、リスク発生のメカニズムをまず理解し、リスクの影響に対して、いかなる対応策をもってくるのか、というプロセスに基づくことにしたのである。そこで、リスク発生の場の複雑さから、まずは小規模の銀行を分析のモデルとして構成し、分析の対象をコンピュータ犯罪に限定し、リスク分析の机上実験を行った⁴⁾。これはコンピュータシステム利用組織にとりコンピュータ犯罪の「リスク分析」のための手掛かりとなったと思われる。

さて、昭和62年度であるが、とくに、コンピュータシステムに係するリスクの分析のため、目的・範囲をこれまでの研究の成果を踏まえて次の点に設定した。それは、人にかかわる部面である。人にかかわる部面については、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部面とヒューマンエラーの部面があるが、前年度にコンピュータ犯罪に言及したことから、とくにヒューマンエラーを分析対象として取り上げ、リスク分析の手順等の検討を行う計画を立てた。これは、コンピュータシステムを利用するにあたり、ハードの側面についてリスク対応が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得るヒューマンエラー関連のリスクの問題が発生してきており、リスク分析上、避けて通ることのできない領域であるとの認識によっている。しかし、委員構成の変化等の状況から、報告書に記載する段階にまで至らなかった。そうした作業と並んで、海外での動向を理解する必要から、リスク分析関連の海外資料の調査を米国商務省の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)の情報部の作成になるINSPEC (Information Services for Physics, Electronics, Computing)のデータベースから17編のリスク分析関連の文献を入手し、それらの概要を抄録した⁵⁾ (本報告書の付属資料2に編集しなおしたものを抄録しておいた)。

昭和63年度には、前年度の検討方針を踏まえながら、再度、銀行に視点をあて、バンキングシステムモデルにおけるリスク分析実施例を考察した。それは、大規模なネットワークシステ

ムの構築がなされてきた分野がバンキングシステムであり、しかもシステムの内容が市民生活に密着しているという側面から、考察対象としてふさわしいとの判断によっている。とくに金融機関のシステム化により変化が生じた領域に、決済機能がある。そこで、決済にかかわる主要な業務の1つとして内国為替業務を選び、リスク分析の作業を行った。とりわけモデルを設定し、リスク分析の対象となる問題事象の範囲を明確にし、損失のタイプから損失の評価まで考察した。その際、シナリオに基づき、業務事象を洗い出し、それにシステム事象を対応させ、業務事象の損失評価へのプロセスを示した⁶⁾。

1. 2 作業での確認点

これまでの作業から、いくつかのポイントが確認された。まず第1点は、昭和60年度の「コンピュータ・セキュリティ対策実施状況調査」から理解できるように、リスク分析に「確立された手法がない」ことであった。これは、むしろ当然であり、理論的に見ても正しいことである。リスクに対して種々の視点からアプローチできるわけであり、これこそが唯一つの確立された手法であると断定することじたい、おかしいことかもしれない。

しかも、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おり、人、もの、金、情報の関わりから、コンピュータシステムの利用の仕方は非常に複雑であり、汎用的な観点から、コンピュータシステムをめぐるリスクの分析の枠組みを造ることは極めて困難である。

たしかにどのシステムにも当てはまるリスク分析の手法を提示することは困難である。しかし、困難であるからといって、それで済むものでもない。しかもコンピュータリスクの影響分析に関して、システム規模が小である事業体ほど分析を行っていない事実があった。この点に鑑みても、なんらかのリスク分析の手法を踏まえたガイドラインを提示する必要がある。これが確認された2点目である。

さらに第3点としては、リスク分析では、コンピュータシステムを利用する事業体（誰＝リスク分析の行動主体）の、何に対して（対象）、どこまで（範囲）、何のために（目的）リスクを分析するのか、したがって、洗い出す事象のレベルをどこに設定するのか、どのような洗い出しの手法によるのか、といった点の明確化が重要であるとされた。明らかに、分析対象の性質によっては、システムにとっての「脅威」の内容も変化することになる。また事業体のシステムへの依存関係によっては、リスクの影響も異なるであろうし、したがって、分析の範囲も変わってこよう。さらに、リスク分析の目的によっては、損失結果の提示の仕方、リスク

対応策への関わりにも差異が生じよう。そこで、リスク分析を行うにあたっては、分析の対象、範囲、目的を限定せざるをえないということであった。

作業をとおしてえられた経験から、リスク分析委員会では、リスク分析のガイドラインへの手掛かりを提示するため、まずは上記の点を確認し、一定の方向を示すことを重要課題としたのであった。

1. 3 リスク分析の範囲

リスク分析は、リスクの発見・確認・評価からなっている。その場合、1.2 の第3に示したように、リスク分析では、コンピュータシステムを利用する事業体が、何に対して、どこまで、何のためにリスクを分析するのか、この点を明確にしたうえで、リスクにさらされている対象たる種々の資産を脆弱性と脅威との影響下において確認し、リスクの作用を被害（損失）大きさとその発生頻度を把握し、リスクへの対応策へと関係付けるのである。

ところでロスアラモス国立研究所（Los Alamos National Laboratory）はリスク分析のための方法論⁷¹を開発した。LAVAと呼ばれるリスク分析のフレームワークは、システムのモデル化のフェーズ、必要情報の収集のフェーズ、分析のフェーズ、リスクマネジメント問題の解決のフェーズという4つのフェーズ（段階）からなっている。とくにモデル化のフェーズでは、対象システムの脆弱性を評価し、脆弱性からの結果を分析し、ロスイクスポジューア集合の計算を行うのであるが、そのステップを紹介すれば次のとおりである：

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、好ましくない結果の集合、資産に対する脅威を定義する。
3. 結果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. いずれの要因が結果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、相互連関的なクエスチョネア（質問票）をデザインする。

これらのステップは、重要なヒントをわれわれに与えてくれる。すなわち、対象システムの確認と分析の範囲の特定化はリスク分析の出発点であろうし、資産⁸⁾に対する脅威の定義、脅威が与える資産への影響等々は、分析にとり不可欠の部面であるからである。

さらに、リスク分析について指摘すべきは、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、どのリスク対応策が費用対効果の点で正当化し得るかを決定するのに用いられるべきか、という点である。これについて、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）⁹⁾では、リスクマネジメントの面からなすべきこととして、次の点を挙げている：

- (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。

LRAMでの上記の指摘なり、またLAVAのリスク分析の方法論でのリスクマネジメントのフェーズでは、リスク処理方法の選択等の費用効果分析が包含されている。そこでリスク分析の範囲として、リスク処理方法の採用の対費用効果の問題まで含めて論ずるべきかについて、異論があるかもしれない。LRAMおよびLAVAでは、「リスクマネジメントの面から」、「リスクマネジメントのフェーズ」とされているがため、当然のこととして理解できようが、「リスク分析の範囲」としては、リスク処理方法の採択のための情報として、損失発生頻度、損失強度の明示までを任務領域とする見方が一般的である。しかし、資産にとっての脅威を予防し、資産の被った損失を軽減する措置を経て、実際に損失の結果が生じるという

[脅威→（予防措置）→資産→（軽減措置）→損失結果]

流れに目を向けるとき、予防・軽減措置がリスクコントロール手段であることに鑑みて、リスク分析がリスクマネジメントの部分としてリスク処理方法の選択等の費用効果分析を包含することも妥当であると考ええる。しかし、それもリスクマネジメントの視点からという限定の上でのことである。

1. 4 リスク分析を行う際の留意点

リスク分析を実行する際、これまでの作業における議論の中から、つぎのポイントが抽出できた。それは、リスク分析には、事業体の経営者の認識が不可欠であり、リスク対応を組織的に準備することが前提であるということである。たしかに、リスク分析を行う範囲は非常に広く、分析対象を決定することさえ時間のかかる課題である。また、直接的に企業利益をもたらさないがため、組織内において、往々にして、その重要性を軽視するきらいもないではない。しかし、リスク分析をせず、対応をしない場合には、予想外の損失の発生もないとは言いがたい。それだけに、以下簡略に示す一連のチェック項目には、十分な注意を払う必要がある。

リスク分析チェック項目¹⁰⁾

1. 分析対象の確定

(会社の綱領と企業倫理との関わりにも留意すること)

2. リスク確認・測定・評価

3. リスクマネジメントの組織的实践

(セキュリティ対策導入；リスクファイナンス等の組織的対応の観点から、4を含め展開する)

4. 企業行動分析手続き

- ・資産チェック（資産の内容について）
- ・会計システム管理
- ・従業員採用審査（モラルハザード；モラルハザードの点から）
- ・情報保護管理（情報価値の点から）
- ・新規投資審査
- ・データ保護基準
- ・コンティンジェンシープランニング
- ・事故報告態勢
- ・従業員確認（ID）
- ・人事政策
- ・調査行動
- ・身元信用保険
- ・予防セキュリティ

5. コンピュータシステム管理

上記のような項目の内容をリスクの点からチェックするわけであるが、本報告書での作業は、これまでの作業の経緯を踏まえ、分析対象の明確化、リスク確認・測定・評価、セキュリティ対策の有無（「安全対策基準」との関わり）といった部分を中心に展開することにした。

注1) 日本情報処理開発協会編『情報化白書1988』コンピュータ・エージ社、1988年、P33

注2) 『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59年12月、日本情報処理開発協会

注3) 『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60年12月、日本情報処理開発協会

注4) 『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61年12月、日本情報処理開発協会

注5) 『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、日本情報処理開発協会

注6) 『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、日本情報処理開発協会

注7) Smith, S.T., Lim, J.J., Phillips, 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 the 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・セキュリティに関するリスク分析調査報告書』昭和63年3月、日本情報処理開発協会

注8) ここで資産とは、セーフガードされねばならぬ組織にとっての価値項目 (items of value) であり、資産に含まれるのは、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、組織それ自体を含めて価値があるとされるものである。

注9) 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). ; 『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、日本情報処理開発協会

注10) Risk Management -Computers Fraud and Insurance, McGraw-HillのアペンディックスBの Checklists and analysis formsを参考とした。

第2章 製造業における入金システム モデルのリスク分析

2. 1 モデルにおけるリスク分析

2.1.1 製造業を対象

汎用コンピュータの利用に関しては、業種によりかなりの差異がある。1セットあたりの金額の大きいのは証券業、金融業、保険業、政府という傾向であるが、産業別実働状況では、電気機械器具製造業（前年度比11.1%増）、卸し・小売業、飲食店等で、伸びが著しい¹¹⁾とされている。従来、金融機関を中心にリスク分析を進めてきたが、その他の業種においてもコンピュータシステムの利用が不可欠となる状況がある。今回の分析の対象業種として製造業を選んだが、格別の理由はない。ただ、次の2点を主体的理由とした：

①コンピュータ利用

近年、どの企業でもコンピュータシステムを業務に利用してきている。業務への利用の仕方は多様である。ところで、影響の度合はシステムへの依存度によるが、システムのトラブルが事業体の活動そのものに影響するのは事実である。そこで、一般的にみて、システム関連のトラブルが事業体にどのような影響を及ぼすのかに視点を置くことにする。

②入金システムでのトラブル

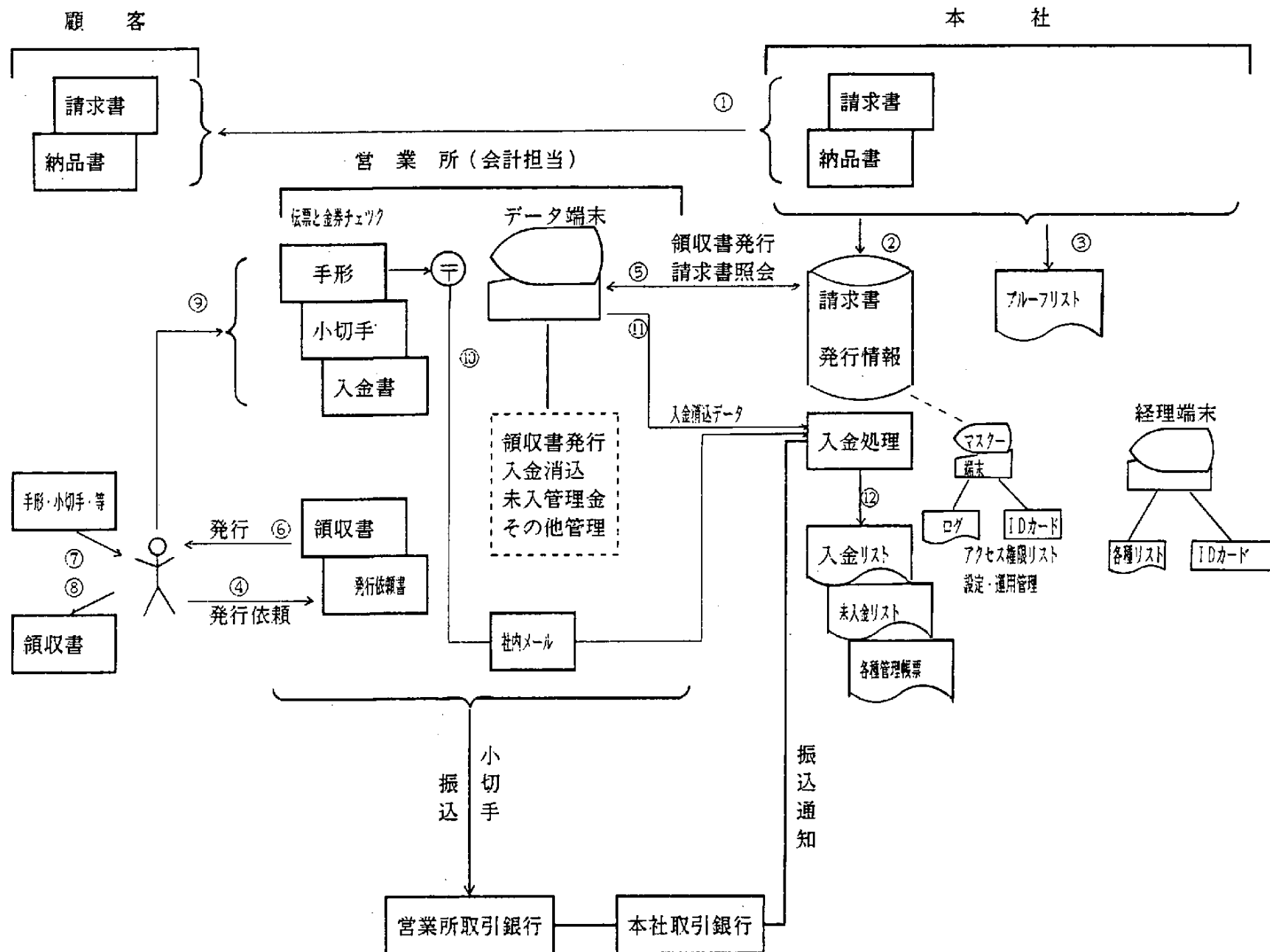
今回は、代金請求・入金処理システムを分析対象として選び、事故事象として「入金漏れ」を選択した。その理由は、「入金漏れ」が、どの企業にも共通に関係する不可欠の業務関連の事故であるとの認識に基づいている。経営体は、人、もの、金、サービス、情報からなっている。そして、システムはこれらすべてに関係するが、とくに事業体にとり血液の役割を演じている「金」の流れとシステムの関係に目を向けることにした。

以上のような理由から、「入金漏れ」を本報告書におけるリスク分析の対象として取り上げるのがふさわしいと考えた。

2. 2 代金請求・入金処理システムモデル

本報告書では、とくにシナリオにおいては製造業における特定の会社（A社）を設定し、A社の代金請求・入金処理システムのモデルを構成し（図1）、リスク分析の方法を示し、リスク評価を実施した。とくに留意した点は、リスク分析を行うにあたり、どのようなステップを取れば良いのかということである。

図1. 代金請求・入金処理フロー



2.2.1 リスク分析のステップ

リスク分析では、事業体にとって阻害要因であるリスクを処理するため、何が組織の業務を妨げるのか、システム関連で何が事故事象となるのか、それがいかなる原因によって引き起こされるのか、事故事象が組織にどのような損失をもたらすのかといった情報が必要となる。重要なのは、事故事象とその原因の因果関係の連鎖の明確化であり、その結果たる損失が組織としての事業体にどの程度のインパクトをもたらすのかである。

まずは、リスク分析におけるステップを『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(P.16)に若干補足して示せば、次のとおりである：

- ①事故原因の洗いだし → 石炭泥のステーション
- ②事故事象の発生確率 → 強度のステーション
- ③損失タイプの確定 → { 評価のステーション(1) }
- ④損失の発生確率(頻度)；潜在的損失の大きさ(強度)の把握
- ⑤損失強度の評価(組織にとっての相対的影響度の評価) { 評価のステーション(2) }
- ⑥リスク処理のための優先順位の決定
- ⑦リスク処理方法の費用対効果の把握、である。

とくに②と④については、統計的なデータを入手しうる場合、リスク処理のための諸変数の確率分布が求められるのが一般的である。また⑤については、現価(net present value)、収益率での換算、効用値などに転換することも一案である。⑥は、どの事故事象からリスク処理を開始したら良いのかについての意思決定がなされる。⑦では、そのため複数の選択的なリスク処理方法の費用対効果の情報提供が求められる。こうしたステップによりリスク処理方法が選択され、実践されるのである。

2.2.2 前提条件の設定

ここで分析の対象となるのは、製造業におけるA社の代金請求・入金処理システムである。分析を行うにあたって、モデルの構成と並んで、リスク発見・確認に関しての分析上、製造業における業務がどのように行われているのかを明らかにする必要がある。そこで業務の何たるかをシナリオを通して明らかにすることにした。その際、シナリオの書き方によっては、リスクに対して楽観的となり、リスク分析の必要がなくなる場合もあるし、また、あまり悲観的となってしまうのは、リスクばかり発見されることになりかねない。この点に留意し、かつ具体性を高めるため数字を用いて、2.2.3 分析モデル(a)～(e)において、定量的に表現すること

とした。

なお、コンピュータセンタのシステムは、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」に基づく安全対策を一応満たす状況にあるものと想定している。

2.2.3 分析モデル

モデルとなるA社は、分析のため仮定した会社で、その概要は次のとおりである。

(a) A社の企業規模

資本金	4.5億円
年商額	450億円
支店数	12支店

(b) A社の代金請求・入金処理システム

- ① A社は、問屋を経由せずに、製品をA社から直接、顧客筋に納入している。A社は製品の納入時に納品書を客に渡し、受領書を受け取っている。受領書の項目を確認の後、「請求書発行情報ファイル」に登録している。
- ② A社では、請求書の発行時に、請求書の発行記録をコンピュータへ登録している。発行記録（ブルースリスト）は、発行時に経理部門の管理者が所定の項目の整合性をチェックしている。

(c) コンピュータシステム関連の環境

- ① プログラムは開発ずみで、テストは十分に行われていた。現在までにプログラムのバグはなく、1年半を経過している。
- ② コンピュータの「請求書発行情報ファイル」のエラーは発生していなかった。しかし、1週間ほど前に、ファイルのデータエラーが発生し、ファイルのリカバリーを行っていた。
- ③ 重要なファイルの情報更新時には、更新ジャーナルを取ることにしていた。「請求書発行情報ファイル」の更新もその対象になっていた。
- ④ ファイルの更新ジャーナルは、保存データ量の関係から、更新後の情報と取引のみをジャーナルにとり保存していた。

(d) 取引の実際

- ① A社は、製品（1,500万円）を顧客Bへ、1月16日に納品した。A社の営業担当者は受領書に顧客の捺印をもらい、営業所に持ち帰った。営業所では、受領書の番号と受領日を営業所の端末から入力した。代金は、納品後1か月後にA社からの請求によって支払

うことになっていた。

(e)事故事象（入金漏れ）の原因の洗い出し

A社では、入金漏れがいかなる事故原因によったのか、その洗いだし作業を第3章に示されているリスク分析（発見・確認）の方法（とくに 3.2.2）に従い実行した。その結果、つぎのような経過があったことが判明した。

①A社では、同年の8月25日に、コンピュータシステムの「請求書発行情報ファイル」が障害を起こし、システムがダウンしていた¹²⁾。そして「請求書発行情報ファイル」を復旧させた後、その内容の確認を行ったところ、B社に關係するファイルが数レコード修復することができていなかった。

②そのため、B社との取引について、1月16日の納品の確認を行ったところ、製品の納品はされていたが、A社からの請求がなかったため、支払いは行われていなかった。

③本件のような事故は、過去にも発生していた（年2回程度発生していた）。ところで、年に2回も発生しながら、何ら対応をしなかったわけではなく、シナリオにおける前提条件に示されているように、コンピュータセンタのシステムについては、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」に基づく安全対策を一応満たすまでに至っていたにもかかわらず、発生したのである。

上記のシナリオに基づき、本章では、リスク分析における事故原因の洗い出しの結果、勘案される損失の評価について以下、検討する。なお、事故原因の洗い出しについては、すでに2.3 分析モデルの(e)において触れておいたが、第3章の 3.2.2リスク分析例に基づいている。

2. 3 損失タイプの確認と評価

A社にとって「入金漏れ」は、どのようなタイプの損失と金額が關係するのであろうか。A社のリスク対応へのインセンティブは、おそらく想定される損失の大きさによるものと思われる。それだけに、損失評価の問題は事業体にとり重要な課題となるのである。

2.3.1 損失のタイプ

損失のタイプは、分類基準によりいくつかに分けることができる。たとえば、3分類のケースでは、「財産損失」（直接損失＝損失を被った財産の取り換えないし修理等に関する／間接損失＝直接損失を被ったことによる財産の喪失価値等／純収益の喪失＝財産損失の結果によ

る利益の喪失《事業中断等》）、

「賠償責任損失」（他人の財産の破損なり第三者への傷害等から生ずる）、「人的損失」（従業員の死亡・傷害・労働不能等による事業体への損失／従業員の死亡・傷害等による家族への損失）とされている¹³⁾。

さらに、上記の財産損失のうち純収益を独立にとりあげ、4分類とすることも可能である。しかし、本報告書では、損失の性質に鑑みて、平成元年の『コンピュータ・セキュリティに関するリスク分析調査報告書』（P.41）に従い、つぎの3分類を用いることにする。すなわち、

「直接的損失」＝事故発生により直接被る損失（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）

「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（事故の影響を分析することにより、明確化されるという性質の損失）

「対応費用」＝上記の損失額ならびに損失発生頻度を最小限に抑えるために、事故後に投下される費用。

これらの損失のうち 間接的損失と 対応費用については、両者の判別がつきにくい場合も考えられなくはない。この点、対応費用は直接的損失か間接的損失のいずれかまたは両者の強度・頻度を減少させるものであり、間接的損失は直接的損失との関係から間接的ないし波及的に生じるかどうか、判別の基準となろう。参考のため、表1に損失のタイプとその具体的内容例を示しておいた。

表1. 損失のタイプ

損失のタイプ	具 体 的 内 容
直 接 的 損 失	代金の不請求分
間 接 的 損 失	事実確認調査費（社内・客先）； システムチェック費用等
対 応 費 用	事後対策経費； システム対応費； 再発防止等

2.3.2 損失強度の算定方法

損失の算定については、リスク分析のステップ③において示したように損失事故の発生確率と潜在的損失の強度が対象となる。ここでは、とくに損失の強度（大きさ）の把握に焦点をあてたい。ところで、昨年度の報告書においては、金額評価法、カテゴリ評価法、確率評価法の3方式を指摘しておいた¹⁴⁾。今回は、損失の強度に限定し、金額評価法とカテゴリ評価法を用いて、A社のケースを考察してみることにする。

①金額評価法

金額評価法とは、業務事故事象により、実際に生じると想定される金額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金額評価のために表2のようなワークシートを用意した。表頭には損失をもたらす業務事故事象をあげ、表側には、表1に示したような事故に関わる損失ないし費用を示している。表側のそれぞれの項目には、直接的損失、間接的損失、対応費用の別を明記しておいた。金額値は、当該事故事象により発生する損失額および関連費用を記入する。その際、可能性として考えられる上限の金額を入れておいた方がリスクの影響をみるうえで参考となろう。

ところで、ワークシートに記載されている金額は、つぎのような作業の結果である。すなわち、直接的な損失は、概して被害にあう金額をそのまま提示すれば良いが、とくに業務事故事象による直接的損失に関係して発生する間接的な損失なり対応費用は、従来、金額的に具体的に評価がなされていない傾向があった。また間接的損失のなかでもモラルの低下なり、信用の低下といった項目も同様に、どちらかといえば实际的に評価が困難で、主観的に見積もられても、表面的に現れることはなかった。本報告書では、この点に目を向け、前者については、当該業務に関連する担当者の「時間的な損失」と見なし、金額評価を試みることにした。また後者のモラル等については、定性的な金額換算基準を設け評価することとした。

表 2. ワークシート

事 故 事 象 = 入 金 漏 れ			
損失タイプ		損失額の 計算の前提	損 失 額
直	不請求分（未入金額）	A	15,000千円
間	事実確認調査費用		
	社内・取引銀行	B	29
	客先	C	20
間	システムチェック	D	1,533
対	事後対策経費		
	事務処理	E	16
対	システム対応経費	F	2,299
対	再発防止経費		
	再発防止通知	G	7
対	防止対応の教育費	H	31
対	手続き手順書改定費用	I	31
間	モラルの低下	J	500
間	信用の低下	K	100
合 計			19,566

(注) 直：直接的損失；間：間接的損失；対：対応費用

◎ 間接的損失額の計算

計算の前提条件

A社のコンピュータ経費	1.1億円／月
作業日数	247日／年
	(1,729時間／年)
作業時間	7時間／日
本件に関わった要員	
担当役員 × 1	年収 1,200万円 (i)
営業所長 × 1	年収 1,000万円 (ii)
セールスマン × 1	年収 730万円 (iii)
経理担当 × 1	年収 650万円 (iv)
S E × 1	年収 520万円 (v)
事務員 × 1	年収 300万円 (vi)

(注：年収は、人事院給与局編『民間給与の実態 平成元年職種別民間給与実態調査の結果』を参考とした。)

◎ 表2 ワークシートにおける損失額の計算の前提

Aの場合 A社の製品の販売代金 不請求分 = 15,000,000

Bの場合 事実の確認調査経費 (社内・取引銀行)

$$(i) \times 1 \text{ 時間} + (ii) \times 1 \text{ 時間} + (iv) \times 3 \text{ 時間} + (vi) \times 3 \text{ 時間} \\ = 6,940 + 5,780 + 11,280 + 5,220 = 29,220$$

Cの場合 事実の確認調査経費 (客先)

$$(ii) \times 2 \text{ 時間} + (iii) \times 2 \text{ 時間} = 11,560 + 8,440 = 20,000$$

Dの場合 システムチェックに要する経費

$$(v) \times 2 \text{ 時間} + \text{コンピュータ経費} = 6,020 + 1,527,000 = 1,533,020$$

Eの場合 事後対策経費（事務処理）

$$(\text{iv}) \times 3 \text{ 時間} + (\text{vi}) \times 3 \text{ 時間} = 11,280 + 5,220 = 16,500$$

Fの場合 システム対応経費

$$(\text{v}) \times 3 \text{ 時間} + \text{コンピュータ経費} = 9,030 + 2,290,500 = 2,299,530$$

Gの場合 再発防止諸経費（再発防止の通知）

$$(\text{ii}) \times 1 \text{ 時間} + (\text{vi}) \times 1 \text{ 時間} = 5,780 + 1,740 = 7,520$$

Hの場合 防止対応の教育費

$$\begin{aligned} &(\text{ii}) \times 2 \text{ 時間} + (\text{iii}) \times 2 \text{ 時間} + (\text{iv}) \times 2 \text{ 時間} + (\text{vi}) \times 2 \text{ 時間} \\ &= 11,560 + 8,440 + 7,520 + 3,480 = 31,000 \end{aligned}$$

Iの場合 手続き手順書の改定

$$\begin{aligned} &(\text{ii}) \times 2 \text{ 時間} + (\text{iii}) \times 2 \text{ 時間} + (\text{iv}) \times 2 \text{ 時間} + (\text{vi}) \times 2 \text{ 時間} \\ &= 11,560 + 8,440 + 7,520 + 3,480 = 31,000 \end{aligned}$$

金額評価を定性的に行った場合

たとえば、ワークシートにおける損害額について、下記のような金額換算基準のもとで、A社の場合、モラルの低下はB基準に従い50万円とおき、信用の低下は事故が事故だけに低いものと判断し、A基準に従い10万円とすることも可能である。

定性的な金額換算基準の例

A	10万円
B	50
C	100
D	500
E	1,000

②カテゴリ評価法

カテゴリ評価法とは、損失頻度および損失規模を事故の発生回数および損失の大きさを特定の金額ごとに何段階かに分けてその影響の範囲を分類する方法である。

今回のモデルにおいては、損失の規模にのみ視点を当て、直接的損失、間接的損失、対応費用のそれぞれについて、昨年度の報告書での5段階評価に基づき示すことにする。重要な点は、組織内部において、損失の評価担当者が変わることであり、評価が変わることのないように、内部的に評価の関して合意を得ておくことであろう。

5段階評価表

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	1億円超の損失

ところで、上記に5段階評価表に基づき、表2のワークシートにおける損失額を表示したのが表3である。

表 3. ワークシート

事 故 事 象 = 入 金 漏 れ		
損失タイプ		損失額
直	不請求分（未入金）	D
間	事実確認調査費用 社内・取引銀行 客先	A A
間	システム・チェック	C
対	事後対策経費 事務処理	A
対	システム対応経費	C
対	再発防止経費 再発防止通知	A
対	防止対応の教育費	A
対	手続き手順書改定費用	A
間	モラルの低下	B
間	信用の低下	A
合 計		D

（注）直：直接的損失；間：間接的損失；対：対応費用

2.3.3 損失の相対的評価

このように算出された損失額に基づき、A社としてどのような損失評価をなせばよいのであろうか。すなわち、組織にとっての相対的影響度の評価（2.2.1 リスク分析のステップ⑤）である。とくに、損失タイプの違いと損失額のもたらす組織への影響の2つが関係する。まず、前者についてであるが、直接的な損失である未入金額15,000千円に対して、間接的損失、対応費用の合計がその約30%と、今回の分析例では直接的損失が大となっている。昨年度の『コンピュータ・セキュリティに関するリスク分析調査報告書』では、金額評価を行わなかったが、分析対象業種を銀行としたがため、損失評価では、社会的信用の低下に特徴づけられた間接的損失が由々しいものとされていた¹⁵⁾。

さらに後者は、損失額の大きさをどのように受け止めるかという重要な課題である。この点は、A社として、業務事事故事象により生じた損失額から、どの程度、それへの対応策を講じる必要を感じるかに結びつく。さて、A社にとり、19,566千円ないしDと評価された損失額が、

A社の資本金さらに年商額 450億円にとり、いかなる財務的なインパクトがあるのか。年商額 450億円に対して、0.043%にすぎない損失は、どのような意味をもっているのだろうか。この場合、効用による評価が必要となろう。それにより、リスク分析のステップで示した、⑥リスク処理のための優先順位が決定され、⑦リスク処理方法についての費用対効果の把握がなされることになる。

本報告書では、このようなリスク処理の優先順位、さらに対応策の費用対効果分析まで提示してはいない。ここでは、製造業での入金システムでのトラブルに関する損失の確認・評価の一端を示すに止め、その他は今後の課題とした。

注11) 日本情報処理開発協会編『情報化白書1988』1988年4月25日、P33.

注12) システム事故事象については、『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、日本情報処理開発協会を参照されたい。本報告書では、システム事故事象の部分を括弧付の形で省略し、業務事故事象と原因集合とを結び付けて展開している。

注13) 『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、日本情報処理開発協会

注14) 同上報告書PP20～24.

注15) 同上報告書P38.

第3章 リスク分析の方法

3. 1 リスク分析の手順（ステップ）

リスク分析の目的は、リスク処理のために必要な情報を入手することである。その目的のため、すでに 2.2.1において示したステップに従い、実践されるのである。

リスク分析における手順（ステップ）は2.2.1 において示しておいたが、本章のコンテキストから再度示せば、次のとおりである：

- ①事故原因の洗い出し
- ②事故事象の発生確率
- ③損失タイプの確定
- ④損失の発生確率（頻度）；潜在的損失の大きさ（強度）の把握
- ⑤損失強度の評価（組織にとっての相対的影響度の評価）
- ⑥リスク処理のための優先順位の決定
- ⑦リスク処理方法の費用対効果の把握、である。

第2章において、③以降について、モデルを通して考察した。この第3章では、とくに事故原因の洗い出しに焦点をあてることにしたい。（なお、事故事象の発生確率の点は省略した。また、リスクの発生にとり、その原因について「脅威」を用いるのがコンピュータセキュリティ等においては一般的であるが、「脅威」には、システムとシステム関連の業務との間のレベルに関して明確さにかけるきらいがある。そこで、本報告書では、事故事象（システム事故事象；業務事故事象）を用い、その原因集合との関連を把握するよう心がけた。）

3.1.1 事故原因の洗い出しにおける事象の明確化

①システム事故事象

事業体の利用するシステムは、常に予定されたとおりに稼働するとは限らない。システムに何らかの障害が発生することにより、システムが期待されたとおりに動かないことがある。こうした事故事象を「システム事故事象」と呼ぶ。これには、システム停止、システム縮退、システム誤作動等が考えられるが、ここでは、システムダウンに要約しておく。

②業務事故事象

システムダウンにより事業体の業務に支障が生ずる場合、それを「業務事故事象」と呼び、リスク処理の対象とする。近年、システムの利用が広範囲、複雑になってきており、それだけにシステム障害が、業務に多大な影響を及ぼすことになる。そこで、「業務事故事象」を勘案する時、何が原因で生じたのが重要な問題とされる。本報告書では、入金システムにおける「入金漏れ」を業務事故事象として考察している。

③原因集合

システム事故事象ならびに業務事故事象の把握に際して、いかなる原因により当該事故事象が発生したのかの原因分析が重要となる。この原因の洗い出し作業にあたっては、事故事象の直接の引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イクダウンして追及することが必要とされる。そこでの原因群を総称して「原因集合」と呼んでいる。

以上の点を簡略に示せば、次のとおりである：

システム事故事象の想定



業務事故事象の想定



想定原因の洗い出し



→ 過去に発生している類似事故の調査

原因集合の抽出



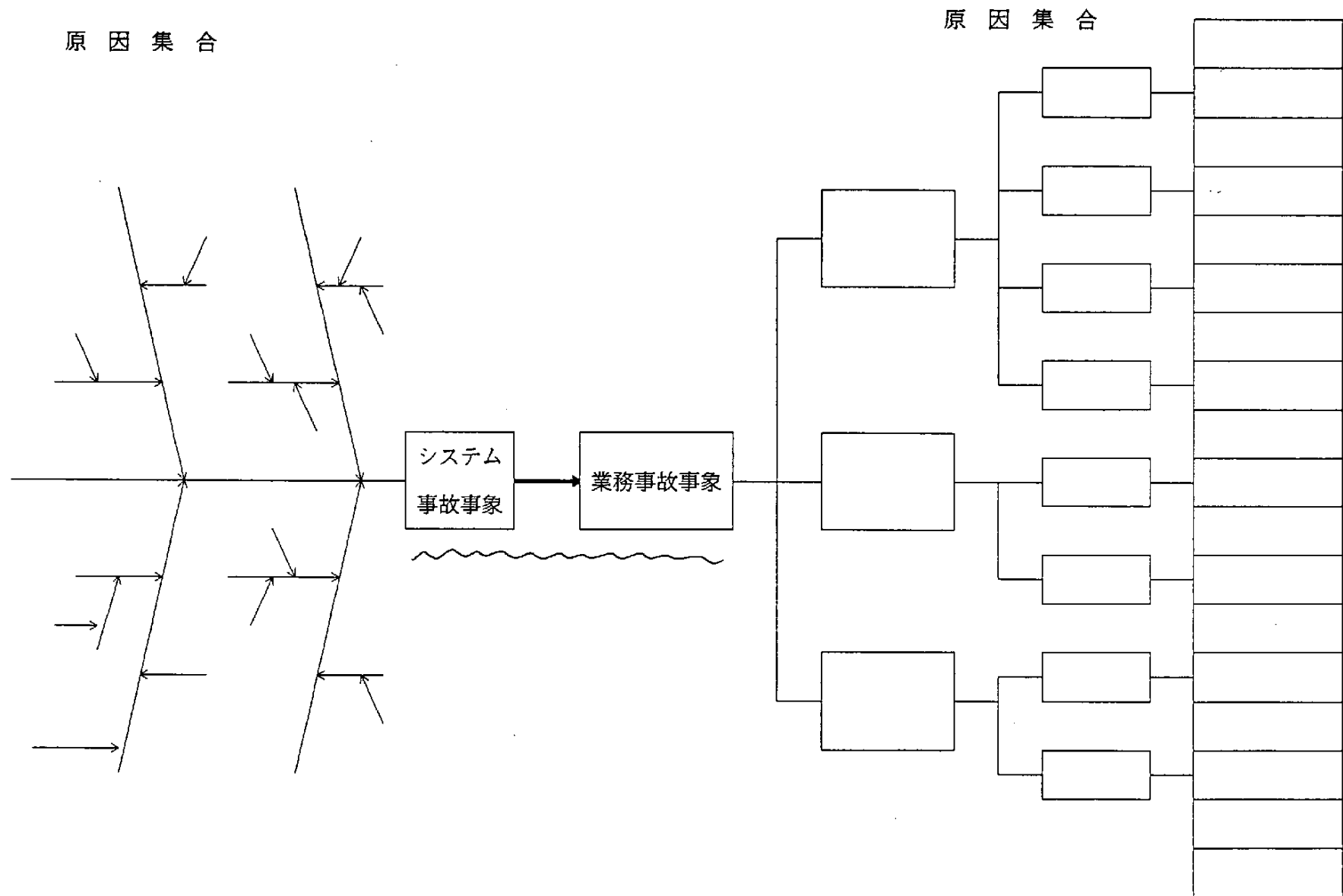
原因集合の系列化



原因系統図の作成

ここで重要なことは、システム事故事象、業務事故事象と原因集合との関係の整理である。整理された結果が、原因系統図に示されることになる。この点の関係を概念的に示したのが、図2のリスク分析系統図である。図2は、システム事故事象を生起させる原因分析の流れと、その結果として生じた業務事故事象の原因集合の分析の流れを結合させたものである。この点は、システム事故事象を生起させる原因の集合と業務事故事象の原因集合では、分析のレベルに違いがあるからである。しかし、原因のなかには業務事故事象の原因とシステム事故事象の原因と同じものも有り得る。（ところで本報告書での分析は、業務事故事象に焦点をあてている。）

図2. リスク分析系統図



3.1.2 事故事象の分析手法

事故事象の分析の手法にはいくつかの手法がある。『コンピュータ・セキュリティに関するリスク分析報告書』平成元年3月では、つぎの3つのアプローチが示されていた。すなわち、ブレインストーミング法、要因系統図法、総合関連図法である。本報告書では、リスク分析を実施する担当者の観点から、関係者のリスク認識の高揚を期するには、どの方法が良いのか検討された。その中で、ブレインストーミング法が妥当と考え、そのベースとして展開されたのであった。ちなみに、ブレインストーミングにより、過去の経験なり他企業の実態等に熟知している者が意見を開陳し、当該事故について先見的な情報を入手し、事故事象とその原因を洗い出したのである。以下に示されるフォールトツリー図は、原因となり得る事象について抽出されたフォールト要因から構成されている。

3.2 リスク発生原因の確認

—— フォールトツリー分析法（F T A法）の応用例 ——

リスク分析委員会では、いくつかのリスク分析の手法の検討から、フォールトツリー分析法（欠陥樹分析法：F T A法）とチェックリスト法を取り上げた。とくに、フォールトツリー法（F T A法）においては、前述した第2章での入金システムモデルの場合を想定して分析を試みている。以下、簡潔にその概略を示しておくことにする。

3.2.1 フォールトツリー分析法（F T A法）

フォールトツリー分析法を用いる場合のリスク分析の手順をまず簡略に示しておくことにする。手順の概要は次のとおりである：

1. リスク分析の対象であるシステムの構成・機能等について、全体像を把握する。
2. 対象となるシステムにおける事故事象を洗いだし、確定する。
3. 事故事象を頂点におき、その原因をさらに洗い出し追及し、その原因集合を明らかにする。
4. 事故事象に直接関与した原因を第一次原因として取り上げ、事故事象との関連を論理式で結ぶ。
5. 一次原因に直接関与した事故原因を二次原因とし、一次原因との関連を論理式で結合する。
6. 事故事象と原因集合間の関連を把握するため、4と5の手順を繰り返す。そして考えられる事故原因と事故事象との関連が薄くなり、意味がないと判断されるところで止める。

7. 同じ原因が一連の因果関係の中で重複していないか、全体を通して原因の相互関係を見直し、整理し、フォールトツリー図を完成させる。
8. 各原因の事故事象への影響を把握する（損失評価）。
9. 損失評価に基づき、事故原因を除去するための方策を検討する。
10. 対応策を講じなかったたときの影響の大きさならびに対応策を講じた時の期待効果を評価する。
11. 期待効果が事故事象による損失に比べ大と評価されれば、導入すべきリスク対策となる。

以上のようなプロセスにより、リスク分析を行うわけである。ところでこうした手順は、概して、あまりに繁雑であると受け取られやすい。しかし、リスク分析は事故が発生し、問題が山積している中で行う場合もないではないが、通常は、事業体にとりリスクがどのような作用をもたらすかという点から、事前に実施しておくのが普通である。それゆえ、コンサルタントに依頼するのも一案であるが、事業体内のリスク分析チームにより、リスクの洗い出し作業として日常の活動の一環として行うことも可能であろう。

3.2.2 リスク分析例

製造業における入金システムモデルにおいて、業務事故事象を対象として取り上げるわけであるが、入金関連の事故についての分析を行えば、つぎのようなプロセスとなろう。

1. 入金関連の事故を洗い出す。その結果、入金漏れ、請求漏れ、金銭の盗用等があげられたとする。本報告書では、「入金漏れ」を業務事象とした。以下は、入金漏れの分析例である。なお、業務事故事象は事務手続きをも含み、事務処理上発生した事故を指す。通常、事業体では、事務処理を実施するにあたり、E D Pシステムを組み込んだ事務手続きを採用している。そのため、E D Pシステムに関する事故事象のみを捕えても意味のないことがある。そこで、事務処理全体のなかで、システムが及ぼす関わりあいがあるのかが把握し分析を行う事が重要である。
2. リスク分析対象のシステムの構成・機能・動作等の全体像を把握する。そのため、入金システムの機能を分析する必要がある。
 - ① A社の入金システム（システムの機能と運用状態を分析・記述する。）
 - ② 代金請求・入金処理・情報のフロー図を作成する（第2章の図1）全体の情報の流れ、手続き等をフロー図により明らかにする。
3. 代金請求・入金処理・情報のフロー図から、事故原因となる事象を洗い出す。

①入金漏れのフォールト要因の洗い出し（表４フォールト要因）

②フォールト要因がどの部面で発生するかを整理する。その部面については以下のとおり：

- i) データの発生部面
- ii) データの入力部面
- iii) データの伝送部面
- iv) データの蓄積部面
- v) 他システムと関連する部面

③入金漏れフォールトツリーへの展開を行う。

- i) 入金漏れを業務事故事象とし、業務事故事象を頂点事象として設定する。
- ii) 入金漏れに直接関連する事故原因をフォールト要因のなかから抽出し、頂点事象である「入金漏れ」に直接関与した事故原因をフォールト要因の中から抽出し、因果関係を分析のうえ、「入金漏れ」との関連を図式化する（一次原因の序列化）
- iii) 一次原因を発生させる要因となる事象をフォールト要因の中から抽出し、因果関係を分析のうえ、その一次原因との関連を図式化する。この時、フォールト要因のなかにはないが、発生原因となる事象が発見されれば、その原因も追加する。
- iv) 上記の iii) の手順を繰り返し行い、これ以上展開しても意味のないところで止める。また、内部的に見て、制御不能である事象は展開しない。
- v) 同じ原因が一連の因果関係の中で重複していないか、全体を通して原因の相互関係を見直し整理し、フォールトツリー図（図３）を完成させる。
- vi) 各原因の事故事象への影響を把握し、事故原因を除去ないし抑制するための方策を検討し、事故原因に対し最も効果的と思える対応策を挿入する。
- vii) 対応策の期待効果を評価する。
- viii) 期待効果が事故事象による損失に比べ大と評価されれば、導入すべきリスク対策となる。

④フォールトツリー分析法による評価

- i) 事故原因となる事象に対して対応策を実施しない場合、当該事故原因が顕在化する頻度を求める。
- ii) 事故が発生した場合の損失について、有形・無形資産の金銭的評価（推定）を行う。
- iii) 各事故原因が、事故事象にどの程度寄与するかを推定し、対応策の効果の序列を作る。
- iv) その序列に従い、対応策のプライオリティを決定する。

表 4. 入金漏れのフォールト要因

データの発生	データ入力	データ伝送	データ蓄積
データ誤り データ漏れ 不正行為 受付番号 受付日付 顧客番号 顧客名 金額	入力誤り 入力漏れ 端末障害 不正入力 伝票間違い 契約条件変更 装置故障による 担当者の不正操作 キータッチミス 入力忘れ (データ脱漏) データ改竄 障害時再入力忘れ (データ重複) 故意のデータ脱漏 受付番号 障害時再操作忘れ (データ化け) 受付日付 入力項目脱漏 (データ入力不能) 顧客番号 入力指示忘れ システム欠陥による 顧客名 誤操作 (データ脱漏) (データ重複) (データ化け) (データ入力不能) 金額	端末障害 伝送路障害 データ送信不能 データ化け データ脱漏 電文抜け データ化け	センタ障害 操作ミス バグに因る 操作誤りに因る (DB破壊) (データの破壊) (データの誤り) (誤データ混入) (O/Sのバグ) (データの紛失) 装置故障 バージョンミス FILE障害(AP) (装置の誤動作) 復旧用データ紛失 (データ破壊) (データ脱漏) (データの紛失)

入金漏れのフォールト要因（続き）

データ蓄積

故意に因る

誤操作

データの破壊

データの改竄

データの破棄

データの漏洩

故意の障害

他システム

銀行システム

振込通知漏れ

振込通知誤り

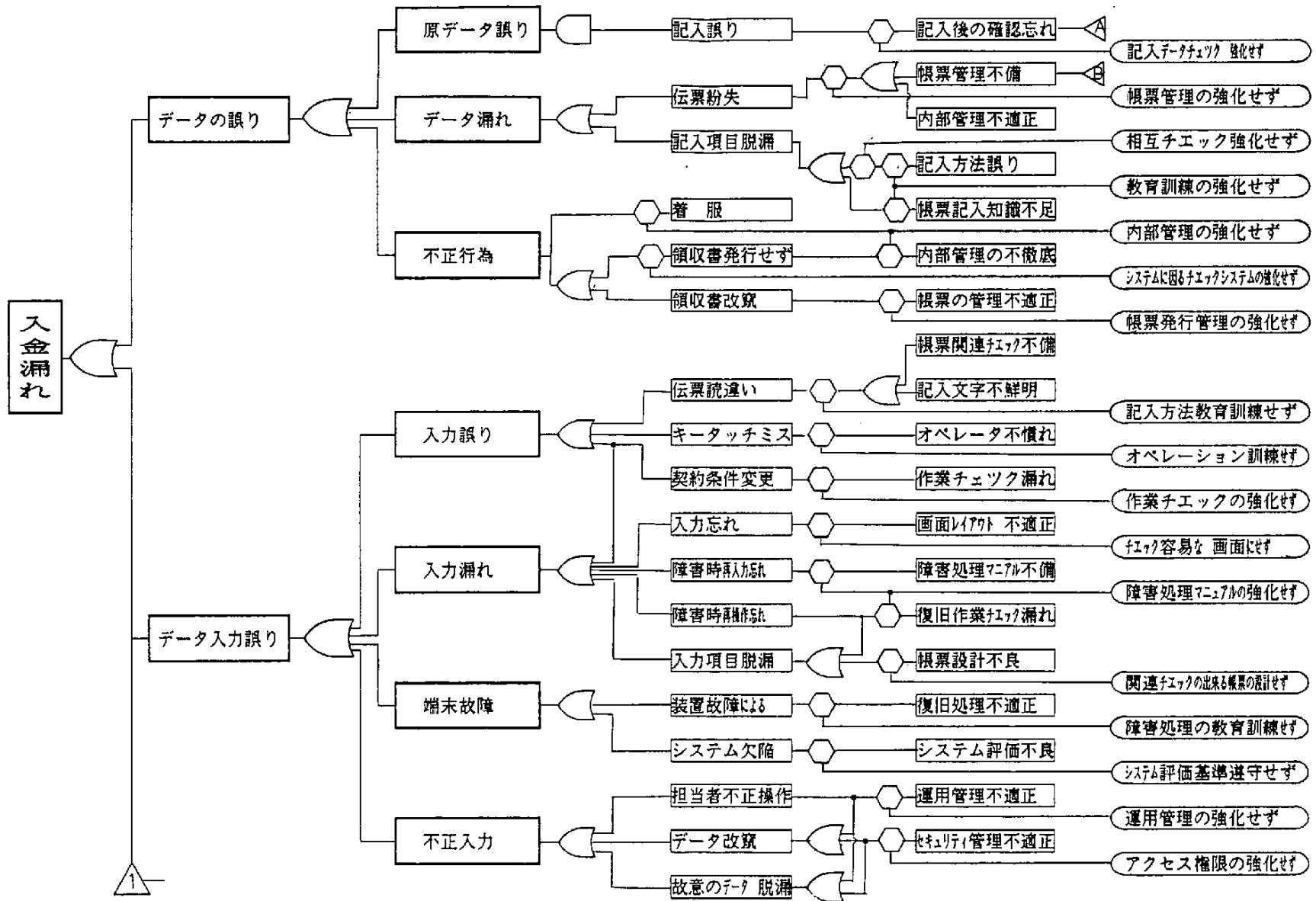
図 3. 入金漏れのフォールトツリー (1 / 2)

業務事故事象
(結果事象)

事故事象

原因集合

条件



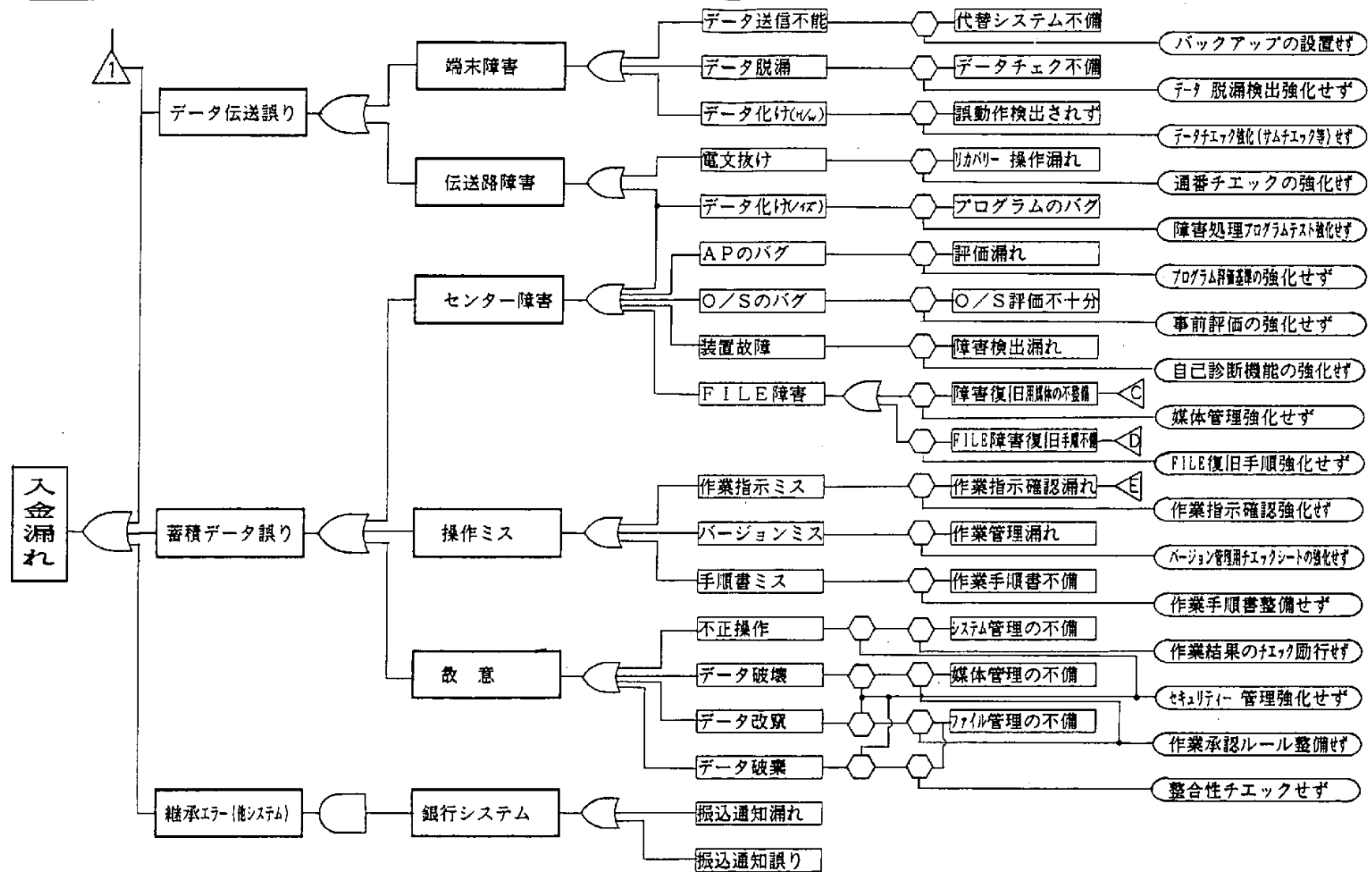
入金漏れのフォールトツリー (2 / 2)

業務事故事象
(結果事象)

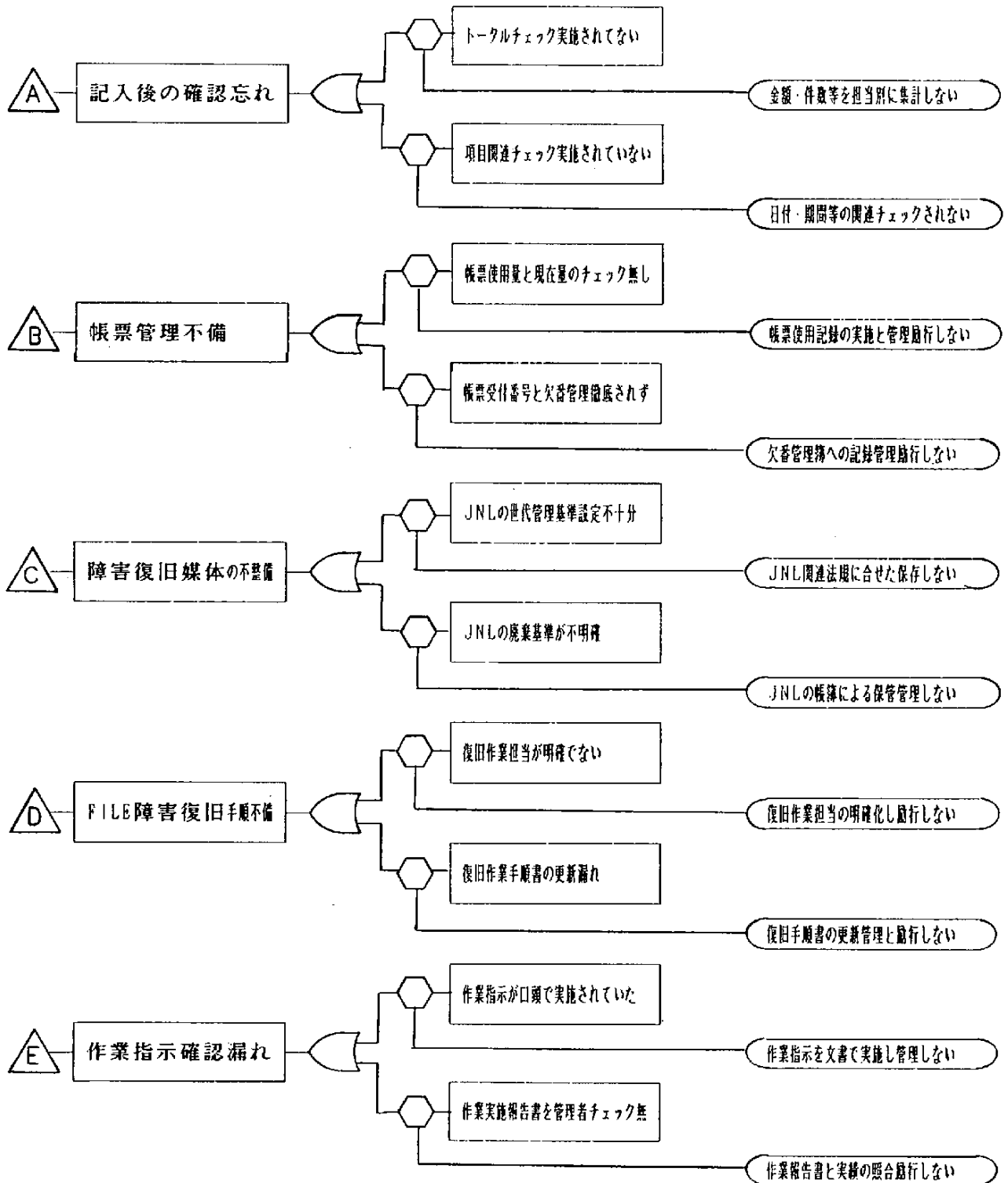
事故事象

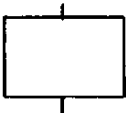
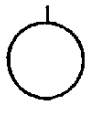
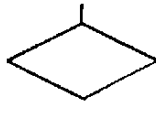
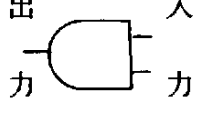
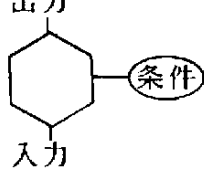
原因集合

条件



入金漏れのフォールトツリー（続き）



NO	記 号	名 称	説 明
01		事 象 Event	トップ事象、及び基本事象などの組合せにより起る個々の事象（中間事象）。
02		基本事象 basic event	此れ以上展開されない基本的な事象又は発生確立が単独に得られる最も低いレベルでの基本的な事象。
03		非展開事象 undeveloped event	情報不足、技術的内容が不明なため、此れ以上展開されない事象を表す。しかし作業の進行により解析が可能となった時には展開を続行する。
04		通常事象 normal event	通常発生すると思われる事象を表す、例えば、オペレーションミスが発生する時は「オペレータが存在する」等である。
05	 I N	移行記号 transfer symbol	FT図上の関連する部分への移行または、連結を示す。三角形の頂上から線の出ているものは、そこへ移行して来る事を示す。
	 O U T		記号のもつ意味は上と同じ 三角の横から線の出ているものは、其処から移行移行して行くことを示す。
06	 出力 入力 力 力	ANDゲート (and) gate	全ての入力事象が共存する時のみ出力事象が発生する。（論理積）
07	 出力 入力 力 力	ORゲート (or) gate	入力事象の内、一つでも事象が存在するならば、出力事象は存在する事を示す。（論理和）
08	 出力 入力 力 力	制約ゲート (INHIBIT) gate	入力事象について、此のゲートで示す条件が満たされる場合のみ出力事象が発生する、条件付き確率を示す。

ところで、本報告書では、上記の分析の手順に従い展開し、フォールトツリー図を作成し、図3に明示しておいた。さらに、事故の原因集合に対し効果的な対応策を必要とする際の条件をも挿入しておいた。なお、対応策については、事業体の内部において、それをみる立場により相違すると考え、あえて記述するのを避けた。

なおA社における場合、「入金漏れ」を発生させた寄与要因は蓄積データの部面におけるセンタ障害の内、ファイル障害にあった。しかし、ファイル障害が直接「入金漏れ」につながったのではなく、障害対応の手続き、管理基準等に問題があったために、最終的に「入金漏れ」という業務事故事象を発生させることになったのである。

「入金漏れ」という業務事故事象の結果たる損失ならびに対応費用については、第2章において示したとおりである。

3. 3 チェックリスト法

リスク分析の最初のステップであるリスクの洗い出し作業を行う手掛かりとして、通商産業省の「電子計算機システム安全対策基準」（昭和59年8月）（以下「安全対策基準」と呼ぶ）を利用することがリスク分析委員会委員により提案され、実行に移された。その場合、「安全対策基準」における項目をベースにチェックリストを作成するというアプローチが展開された。ところで、「安全対策基準」の各項目は、「設備基準」、「技術基準」、「運用基準」から構成されているが、アプローチの仕方を重視したため、特定の項目に限定した。

なお、ここでの基本的な考え方は、「安全対策基準」の対策項目の意図することをくみ取り、設問を細分化することにより、現状を把握し、リスクを発見し、判定を行うことにより、リスクの大きさを評価し、今後の対応に効果的な情報を供することにある。「安全対策基準」の対策項目それ自体は汎用的であるがため、事業体特有の問題状況を想定しながら、チェックリストを作成するのが望ましいことになる。

チェックリストを作成するにあたっての、留意点を若干指摘すれば、次のとおりである。すなわち、

- ①調査対象：リスク分析における調査対象を明確にする。それというのも、ここで示すチェックリストで、当該事業体のコンピュータシステムのリスクすべてを確認することは非常に困難であるからである。たとえば、調査対象を適用業務別、システム別、ワークステーション別、支店別、営業所別、オフィスコンピュータ別

等々、個々についてリスクを把握し、全体としての安全対策実施状況を把握することになる。

②安全対策基準の項目：ここでの項目は、「電子計算機システム安全対策基準」における「対策項目」をそのまま記載してあるが、「安全対策基準」に記載されていない項目を追加することも重要であり、また同基準での項目のレベルは必ずしも同じ水準で示されているとはいいがたい部分もあり、調整する必要があるだろう。

③現状の把握のための設問：「安全対策基準」の対策項目をチェックするためには、何を調べる必要があるかを明確にする手掛かりとなる「現状把握のための設問」を用意するのが望ましい。たとえば、3.3.1 チェックリスト法例 その1において示すことになるが、信頼性向上機能の項目で「～重要な構成機器は、障害時に代替可能な～」とあるけれども、これに対し即座に「はい」もしくは「いいえ」と回答するのは困難である。また、すべての調査対象（適用業務、システム、ワークステーション等々）を満足させる必要もない筈である。そこで、上記の「安全対策基準」の対策項目については、次のような設問が考えられるのである：

「～重要な構成機器は、障害時に代替可能な～」

→◎その調査対象に対して重要な機器／機能は何であるのか？

たとえば、CPU、チャネル、ディスク装置等々があり、それが障害を起こすことにより、適用業務が長期間停止する場合があるからである。

[重要機器の選択] もしも、回答が「いいえ」であれば、できるだけ早い時期に重要機器／機能の選択を行うことが必要となる。

[現状の構成とあっているか] 仮に、「はい」の回答がなされるとすれば、それが現状の構成とあっているのか？（最新版でなければ意味をなさない）、もし構成に変化が起きているのであれば、早い時期に更新する必要がある。

[代替手順は明確か] 代替可能についても、代替手順は文書化されているのかという点も重要である。そうであれば、代替作業の効率化が期待でき、間違いも回避できることになる。[代替テストの実施は] 代替作業についても、障害時を想定して、その手順のテストを実施しておくことも肝要である。

[業務停止最大許容時間は] 障害発生から業務再開までの最大の許容時間を予め検討しておくことも必要である。

〔過去1年最大停止時間〕業務を停止した最長時間の実績を知っておくことも大事である。

〔過去1年業務停止回数〕業務に影響を及ぼした業務停止回数の実績についても認識しておく必要がある。

ここでは上記のような設問を挙げてみたが、必要に応じて設問を増やすことにより、現状の把握が可能となろう。

④これまでプロセスから、事業体にとっての問題状況ないし、リスク原因を明らかにする。

⑤調査対象について、現状の把握に基づき、判定／対策の必要性を勘案することになる。以上の点に基づき、つぎに例示して見ることにする。

3.3.1 チェックリスト法 例その1

これまで指摘した点を考慮に入れ、作成したのが表2のリスク分析チェックリストである。

例 その1では、「安全対策基準」のうち「技術基準」にかかわる信頼性向上機能およびデータ保護・不正防止に視点をあてている。しかし、設問の受取方によっては、「運用基準」に係ると読めなくもない部分もあるが、ここでは技術基準に入れ展開している。

表5. チェックリスト法（例その1）

〔調査対象； 〕〔建物／場所名； 〕〔調査年月日； 〕〔調査責任者； 〕

I. 信頼性向上機能

安全対策基準の項目	現状把握のための設問	現状の把握	リスクの種類	判定／コメント
(1)電子計算機システムの重要な構成機器は、障害時に代替可能な機能を設けること	- 重要機器の選択は - 一 現状の構成と合っているか - 重要構成機器／機能は - 代替手順は明確か - 代替手順のテストの実施 - 業務停止最大許容時間 - 過去1年最大停止時間 - 過去1年業務停止回数	☐ はい ☐ いいえ→重要機器の選択の実施 ☐ はい ☐ いいえ→更新する ☐ 文書化 ☐ いいえ ☐ 重要機器構成変更の都度 ☐ 定期的年__回 分 __分→原因は ☐ H/W ☐ S/W ☐ PRGH ☐ 設備 __回 原因→H/W __回、S/W __回、PRGH __回 設備 __回、その他 __回	☐ 開示 ☐ 変更 ☐ 破壊 ☐ 停止／遅延	☐ 至急対策 ☐ 対策必要 ☐ 検討必要 ☐ 現状で良 ☐ 該当せず
(2)電子計算機システムの負荷状態の監視制御機能を設けること	- 監視制御機能を設けている - 制御機能は - 機能は . . .	☐ はい ☐ いいえ ☐ H/W ☐ S/W ☐ PRGH ☐ 他__ ☐ 十分 ☐ 普通 ☐ 不十分	☐ 開示 ☐ 変更 ☐ 破壊 ☐ 停止／遅延	☐ 至急対策 ☐ 対策必要 ☐ 検討必要 ☐ 現状で良 ☐ 該当せず
(3)電子計算機システムの障害箇所の検出及び切り分け機能を設けること	- 障害箇所の検出 - 切り分けは - 検出機能は - 切り分け機能	☐ S/Wイメージ ☐ H/W ☐ PRGH ☐ 他__ ☐ S/W ☐ 手動 ☐ 十分 ☐ 普通 ☐ 不十分 ☐ 十分 ☐ 普通 ☐ 不十分	☐ 開示 ☐ 変更 ☐ 破壊 ☐ 停止／遅延	☐ 至急対策 ☐ 対策必要 ☐ 検討必要 ☐ 現状で良 ☐ 該当せず
(4)障害時における縮退・再構成機能を設けること	- 適用業務の優先順位 - 縮退に不可欠な機能／機器 - 縮退構成のテスト - 優先業務と縮退構成 - 再構成のタイミング . .	☐ 決定 ☐ 未決→決める ☐ 済み ☐ 未済み→テストする__ ☐ 検討済み ☐ 検討なし→検討する ☐ 検討済み ☐ 検討なし	☐ 開示 ☐ 変更 ☐ 破壊 ☐ 停止／遅延	☐ 至急対策 ☐ 対策必要 ☐ 検討必要 ☐ 現状で良 ☐ 該当せず
(5)チェックポイント機能を設けること	- OSの機能 - PPの機能 - 適用業務プログラム - チェックポイントの間隔	☐ 使用 ☐ 未使用→ ☐ 持っている ☐ 持っていない ☐ 使用 ☐ 未使用→ ☐ 持っている ☐ 持っていない ☐ 組込済み ☐ 未組込 ☐ 適当 ☐ 検討の必要あり	☐ 開示 ☐ 変更 ☐ 破壊 ☐ 停止／遅延	☐ 至急対策 ☐ 対策必要 ☐ 検討必要 ☐ 現状で良 ☐ 該当せず

CFI
component
Failure.

I. 信頼性向上機能（続き）

安全対策基準の項目	現状把握のための設問	現状の把握	リスクの種類	判定／コメント
(6)重要なファイルには次の機能を設けること ①障害時に代替可能な機能を設けること ②バックアップリカバリ機能を設けること ③ダイレクト変更の場合はジャーナル機能を設けること	①重要ファイルの選定 ・ファイルの多重化 ・多重化の方策 ・ ②ファイルの選定 ・バックアップ周期 ・リカバリテスト ・保存期間 ・ ③ジャーナル機能 ・オンラインジャーナル ・ジャーナル機能の提供 ・ジャーナルの保存期間 ・ ・	☐ 済み ☐ 未済み→ファイルを特定する ☐ 二重化 ☐ 単ファイル ☐ OS ☐ プログラム ☐ なし ☐ 済み ☐ 未済み ☐ 一定周期ごと ☐ プログラム、手順変更の際 ☐ 二世世代 ☐ 三世世代 ☐ 未定 ☐ あり→ ☐ 単 ☐ 二重、 ☐ なし ☐ 採取 ☐ 未採取→検討する ☐ メーカー提供 ☐ 適用プログラム ☐ なし 	☐ 開示 ☐ 変更 ☐ 破壊 ☐ 停止／遅延	☐ 至急対策 ☐ 対策必要 ☐ 検討必要 ☐ 現状で良 ☐ 該当せず
(7)複数の電子計算機システムを接続したシステムの場合は、次の機能を設けること ①電子計算機相互の障害の検知機能 ②障害時の電子計算機相互の代替機能	①障害検知機能の提供 ・相互に機能 ・機能の有効性 ・ ②相互のリカバリ計画 ・代替機的能力 ・ ・	☐ メーカー提供 ☐ 適用プログラム ☐ なし ☐ 双方にあり ☐ 片方のみ ☐ 双方になし ☐ 有効 ☐ 不十分 ☐ 低機能 ☐ 検討済み ☐ 未検討 ☐ 十分 ☐ 容量なし	☐ 開示 ☐ 変更 ☐ 破壊 ☐ 停止／遅延	☐ 至急対策 ☐ 対策必要 ☐ 検討必要 ☐ 現状で良 ☐ 該当せず

II. データ保護・不正防止

安全対策基準の項目	現状把握のための設問	現状の把握	リスクの種類	判定／コメント
(1)ユーザ確認のためのパスワード、識別コード等資格確認機能を設けること	・ユーザ登録 ・ユーザ登録台帳確認周期 ・パスワードの桁数 ・パスワード配布 ・パスワード変更周期 ・パスワード取り消し ・取り消し理由の確認 ・ ・	☐ 手続の文書化 ☐ 口答 ☐ 1回6月 ☐ 1回／年 ☐ 周囲ない ☐ 3桁以下 ☐ 4桁～6桁 ☐ 7桁以上 ☐ プログラムで生成／配布 ☐ ユーザ作成 ☐ 書面 ☐ 電話 ☐ 口答 ☐ その他 ☐ 1月 ☐ 2月 ☐ 3～6月 ☐ 7月以上 ☐ 5回連続 ☐ 10回連続 ☐ それ以上 ☐ 日に5回 ☐ 月に10回 ☐ なし ☐ 書面確認 ☐ 口答確認	☐ 開示 ☐ 変更 ☐ 破壊 ☐ 停止／遅延	☐ 至急対策 ☐ 対策必要 ☐ 検討必要 ☐ 現状で良 ☐ 該当せず

念のため確認
完了

Ⅱ. データ保護・不正防止（続き）

安全対策基準の項目	現状把握のための設問	現状の把握	リスクの種類	判定/コメント
(2)各資源のアクセス制御機能を設けること	・資源のアクセス権限階層 ・資源管理 ・アクセス権限取得手続 ・違反確認 ・ ・	☐ 2段階 ☐ 3段階 ☐ 4段階以上 ☐ なし ☐ OS/PP ☐ 自社作成 ☐ 使用せず ☐ 資源アクセス管理プログラム(RACF, ACF2等) ☐ 文書化した手続き ☐ とくになし ☐ 違反調査 ☐ 記録のみ ☐ とくになし	☐ 開示 ☐ 変更 ☐ 破壊 ☐ 停止/遅延	☐ 至急対策 ☐ 対策必要 ☐ 検討必要 ☐ 現状で良 ☐ 該当せず
(3)重要なファイルおよび伝送情報には暗号化機能を設けること	・重要ファイル選別 ・ファイルの暗号化 ・伝送暗号 ・暗号方法 ・ ・	☐ 規定による ☐ オーナーの要求 ☐ その他 ☐ 重要ファイル ☐ 暗号化なし ☐ 暗号化検討 ☐ H/W(制御装置、モデム等) ☐ S/W ☐ 既成 ☐ 自社開発	☐ 開示 ☐ 変更 ☐ 破壊 ☐ 停止/遅延	☐ 至急対策 ☐ 対策必要 ☐ 検討必要 ☐ 現状で良 ☐ 該当せず
(4)次のモニタリング機能を設けること ①アクセスモニタリング ②コンソールログ機能 ③システム使用状況記録機能 ④アプリケーションに組み込むモニタリング機能	①アクセスモニタリング ・機能提供 ②コンソールログ機能 ・機能提供 ③使用状況記録機能 ・機能提供 ④アプリケーション ・ ・	☐ 機能あり ☐ 使用中 ☐ 機能なし ☐ 未使用 ☐ OS/PP ☐ 専用PP ☐ アプリケーション ☐ 機能あり ☐ 使用中 ☐ 機能なし ☐ 未使用 ☐ OS/PP ☐ 専用PP ☐ アプリケーション ☐ 機能あり ☐ 使用中 ☐ 機能なし ☐ 未使用 ☐ OS/PP ☐ 専用PP ☐ アプリケーション ☐ 組込済み ☐ なし	☐ 開示 ☐ 変更 ☐ 破壊 ☐ 停止/遅延	☐ 至急対策 ☐ 対策必要 ☐ 検討必要 ☐ 現状で良 ☐ 該当せず
(5)通信の相手確認機能を設けること	・相手確認機能 ・	☐ コールバック ☐ 回線番号 ☐ 機器ID ☐ デジタル署名 ☐ その他	☐ 開示 ☐ 変更 ☐ 破壊 ☐ 停止/遅延	☐ 至急対策 ☐ 対策必要 ☐ 検討必要 ☐ 現状で良 ☐ 該当せず
(6)複数の電子計算機システムを接続したシステムで、かつ専用の電子計算機室に設置していない電子計算機システムには、プログラム及びデータの不正変更を防止する機能を設けること	・不正防止機能 ・ ・ ・ ・ ・	☐ 資格設定 ☐ パスワード ☐ アクセスモニタリング ☐ データ/プログラム保管施設 ☐ 手続き（使用許可申請→承認→確認）	☐ 開示 ☐ 変更 ☐ 破壊 ☐ 停止/遅延	☐ 至急対策 ☐ 対策必要 ☐ 検討必要 ☐ 現状で良 ☐ 該当せず

注 a：情報資産にかかわるリスクの原因を故意と事故とにかかわらず、許可されていない情報資産の漏洩に関するものを「開示」、データやプログラム等の内容の変更や改ざんを「変更」、データやプログラム等の消去や破壊を「破壊」、として表した。また、以上に含まれないサービス（業務）の停止や遅延を「停止／遅延」とした。変更や破壊の結果、当然、最終的には業務の遅延や停止に結び付く場合もある。この点は、調査の範囲をどこまですべきかの判断によることになる。さらに、どのくらいリスク原因数を挙げるべきかも、調査の性質によることになる。

注 b：判定／コメントの部分は、現状の把握の内容から4つ設定した。すなわち、

「至急対策」は、対策を早急に検討・実施すべきで、実施しないと業務（信用失墜等も含む）に多大な影響を及ぼす可能性が大きいという判定。

「対策必要」は、緊急の度合はそれほど高くないが、対策実施の候補にするべきものを指す。

「検討必要」は、現状の把握を今一步詳細に検討する必要があるもの。「該当せず」以外の判定を下せないこと。

「現状で良い」は、字句どおり、現状でさしつかえない。

「該当せず」は、調査対象に「安全対策基準」の項目が当てはまらない時。

◎判定・コメント例

「安全対策基準」の項目(i)について、調査対象がある事業所のオフコンを勘案してみる：

もしも業務停止最大許容時間が2時間、過去1年最大停止時間が1時間30分、過去1年間の業務に支障を与えた回数が3回、そしてその原因集合についてはH／Wが1回、S／Wが1回、落雷が1回であるとすれば、業務停止／遅延がリスク原因となる。

以上のような現状把握ができた場合、業務停止最大許容時間の2時間を超す可能性が極めて少ないと判定しうれば、「現状で良い」となる。しかし、この点は、調査責任者と現場の責任者が協議し、将来の事態を想定し「検討必要」にチェックするようになるかもしれない。だが、最終的にはマネジメントの判断に委ねられることになる。

3.3.2 チェックリスト法 例その2

チェックリストには、コンピュータセンタと、営業店における場面が想定され、そこでの問題状況が把握できるように構成したのが表3である。現状をまず明確に把握し、その内容を確認すること（回答）により、問題状況を認識するのである。ところで、この問題状況は、

上記の例における設問現状の把握のための設問を通して可能となるともいえる。表6では、安全対策の項目、現状、そして問題状況を基礎に対策が勘案されている。なお、ここでは、「設備基準」、「技術基準」、「運用基準」を取り上げ、構成した。

注c：表6における例は、中央のコンピュータセンタを有し、各営業店とオンラインにより業務処理を行っている中堅企業を想定したものである。

3.3.3 「安全対策基準」に基づくチェックリスト法での考慮点

これまで展開して来たチェックリスト法において明らかなことは、安全対策を十二分に講じるとなれば、莫大な経費が必要となる。限られた予算のなかから対策を実行に移すためには、それなりの情報が必要なのである。ここでは、優先順位を決定するための方法として、「電子計算機システム安全対策基準」を活用する方法を示したものである。判定にあたり、すべからず金銭に換算しうれば、費用対効果が評価でき望ましい訳であるが、それは非常に困難なことである。そこで、事業体にあった判定基準、たとえば、相対的な得点法、減点法等々を勘案し、事業体内でコンセンサスを確立しておくことが不可欠である。

表6. チェックリスト法（例その2）

I. 「コンピュータセンタ」の場合

安全対策の項目・内容	現 状	問 題 状 況	判断・対策
<u>設Ⅱ－1－(9)</u> 電子計算機室及びデータ等保管室 を示す表示は付けないこと	表示がある ・ 室の入口に表示あり …… × ・ 建物内の掲示版に表示あり …… × ・ 建物案内パンフに表示あり …… × ・ 電子計算機室の入口ドア上部が 透明ガラス …… ×	第三者にも電子計算機室およびデータ 保管室の位置が容易に分かることとな り、防犯上好ましくない	各表示をとることとする また、電子計算機室の入口ドア上 部のガラスは不透明なものとする （なお、表示をとることにより緊 急時の非難に支障が生じないよう 訓練等でカバーする）
<u>設Ⅱ－3－(3)</u> 直上階の床には、防水施工を行う こと <u>設Ⅱ－4－(15)</u> 室内及び天井内等には、水配管を 通さないこと	天井内の一部分を排水管が通過してい る ・ 直上階の床は防水施工 …… ○ ・ 天井内を排水管が通過 …… × ・ 天井付近に漏水検知器 …… ×	万一天井内の排水管から漏水した場合 には、電子計算機室内に浸水するおそ れがある	天井内の排水管に防水パンを設置 するとともに、天井付近に漏水検 知器を設置する また、あわせて電子計算機室内に は防水カバーを常備する
<u>設Ⅱ－3－(7)</u> フリーアクセス床は、地震時に損 壊しない構造とすること	フロアカット部の対策が不十分である ・ 支柱の補強と床板の固定 …… ○ ・ ボード部の補強 …… ○ ・ フロアカット部の対策 …… ×	地震時、脆弱なフロアカット部から床 全体に波及してフリーアクセス床が崩 壊してしまう危険がある	フロアカット部について、補強枠 取り付け、ストッパー・補助支柱 取り付け等の措置を構じる なお、免震床の採用はコストが大 きいこと等により見送る

安全対策の項目・内容	現 状	問 題 状 況	判断・対策
設Ⅱ－４－(5) ハロゲン化物消火器または二酸化炭素消火器を設置すること	電子計算機室内にはハロン1301消火器が設置されている ただし、月末のピーク時には大量のプリントアウトがあり、一時的に相当な量の用紙が持ち込まれる	ハロン1301は電気火災には有効であるが、紙類の普通火災にはやや消火力が弱いと考えられる	用紙が持ち込まれる場所には、強化液消火器または粉末消火器も設置する なお、あわせて次の配慮も行う ・一時期に持ち込む用紙の量をできるだけ少なくする ・用紙の山の間は延焼防止のため距離をおく
設Ⅳ－(1) 電源設備には停電等に対する措置を講ずること	電源の瞬断、停電等に対する措置は講じられている ・バッテリー、無停電装置 …… ○ ・C V C F …… ○ ・自家発電機 …… ○ ただし、ここ数年の機器増強で電気使用量が大幅に増えており、自家発電機稼働のための燃料備蓄が足らなくなっている	長時間停電に対応できない (自家発電機稼働のための燃料備蓄量は、当初の機器の電気使用量からすると24時間分確保できていたが、現在の機器の電気使用量では12時間分程度の確保にしかっていない)	オンラインシステムの進展等により、会社の日常業務のコンピュータシステムに負う部分がますます大きくなっている状況からして、少なくとも24時間の停電には耐えられることとしたい そのために必要な燃料備蓄量は確保することとする また、あわせて自家発電機稼働のために必要な水の量も確保する

安全対策の項目・内容	現 状	問 題 状 況	判断・対策
<u>技 I - (1)</u> 重要な構成機器は障害時に代替可能な機能を設けること	CPUの代替手段は確保されていない (通信回線が二重化されていない点は「営業店」のチェックリストで記載) ・CPUの代替手段 …… × ・周辺入出力装置の予備設置 …… ○ ・補助記憶装置の予備設置 …… ○ ・アクセスパスの迂回化 …… ○	CPUに障害が発生した場合代替手段がない (オンラインシステムがダウンすることにより、影響が全営業店に及ぶ)	CPUを複数として、マルチプロセッサシステム構成とすることで、障害発生時の影響を極力抑えることを検討する (当方式の採用はコストが大きいことおよびシステム改訂ロードが大きいことから、メリット・デメリット等を社内で十分ツメることとする)
<u>技 I - (6)</u> 重要なファイルにはバックアップリカバリ機能を設けること	バックアップリカバリ機能は設けられている ただし、バックアップの周期について見直す必要がある	オンラインシステムのファイルにトラブルがあった場合リカバリをタイムリーに行う必要があるが、現行のバックアップの周期ではリカバリのタイミングを失するおそれがある	バックアップの周期を短くすることを検討する (たとえば、現行の1週間ごとの周期から2日ごとに短縮する等) なお、リカバリをより短時間で行うために、必要があればオンラインシステムのファイルを分割してバックアップリカバリをより容易にすることをあわせて検討する

安全対策の項目・内容	現 状	問 題 状 況	判断・対策
<u>技Ⅱ-(1)</u> ユーザ確認のためのパスワード、 識別コード等資格確認機能を設けること	開発のためのT S O端末機には、パスワード、識別コードの資格確認機能が設けられている ・パスワードの使用 …… ○ ・識別コードの使用 …… ○ ただし、パスワードの定期的な変更が強制されていないので、数か月間同一パスワードを使用するケースも生じている	第三者にパスワードを知られる可能性が少ないとは言えず、不正アクセスを排除することが困難となるおそれがある	パスワードの定期的（1か月毎）な変更を強制するシステムとする また、第三者に類推されないパスワードとするよう、各人に徹底する
<u>運Ⅱ-2-(1)、(2)</u> 写真入身分証明書・勤務証により入退館の資格を確認する また、館内にあっては識別章を常時着用させること	識別章の常時着用が実施されていない ・入退館時の写真入身分証明書 または勤務証の確認 …… ○ ・識別章の常時着用 …… ×	第三者が紛れて入館し不正行為を働く場合のチェックが困難である また、無資格者の特定区域立入りのチェックが困難である	識別章の常時着用を実施することとする なお、識別章はチェック効果を上げるため、単なる名札ではなく写真入身分証明書・勤務証（写真入り）を使用することとする

安全対策の項目・内容	現 状	問 題 状 況	判断・対策
<u>運Ⅱ－3－(1)</u> 電子計算機室及びデータ等保管室の入退室者の資格を確認すること	退室者の資格確認は実施していない ・入室者の資格確認 …… ○ (機械＝カード錠により) ・退室者の資格確認 …… ×	退室者の確認をしないと、入室者の在室時間が明確にできず、不正使用等が発生した場合の原因究明が容易にできないおそれがある	退室者の資格確認実施を検討する ただし、退室のための扉をオープンにカード錠を使用して行う場合は、緊急時の避難に支障が生じない手当てを講じる
<u>運Ⅳ－6</u> 重要なデータ及びプログラムを定め、管理の措置を講じること	分散保管が十分でない (同一ビル内で分散保管しているため) ・使用および廃棄の管理 …… ○ ・保管場所の施錠 …… ○ ・世代管理 …… ○ ・分散管理 …… ×	災害等で重要なデータおよびプログラムが全滅してしまうおそれがある	離れた場所で分散保管することとする 遠距離の場所で分散保管する場合は、データ伝送による方法も検討する (地震を考えるとなるべく遠距離の場所が望ましい)

Ⅱ. 「営業店」の場合

安全対策の項目・内容	現 状	問 題 状 況	判断・対策
<u>設Ⅳ－(1)</u> 電源設備には停電等に対する措置を講ずること	電源の瞬断、停電等に対する措置は講じられていない ・バッテリー、無停電装置 …… × ・自家発電機 …… × ・電源車 …… × ・その他予備電源確保措置 …… ×	電源の瞬断、停電には対応できない （過去３年間に於いて、瞬断が２回、１５分間の停電が１回あり、いずれも業務が混乱した）	営業店の規模、業務内容から考えると自家発電機の設置等大がかりな措置はコストの点でも難しい したがって、瞬断および比較的短時間の停電に絞って対応することとし、２０分程度供給可能なバッテリーを用意する
<u>技Ⅰ－(1)</u> 重要な構成機器は障害時に代替可能な機能を設けること	通信回線は二重化されていない ・通信回線の二重化 …… × ・通信制御装置の予備設備 …… ○ ・端末機の予備設備 …… ○ （互いのバックアップにより）	回線トラブル、回線切断に対応できない （過去３年間に於いて、３０分超の回線トラブルが２回あり、いずれも業務が混乱した）	コストを検討し、次のいずれかを実施することとする ①ＤＤＸ網によりバックアップする ②ループ接続を利用してバックアップする
<u>技Ⅱ－(1)</u> ユーザ確認のためのパスワード、識別コード等資格確認機能を設けること	端末機にはパスワード、識別コード等資格確認機能が設けられていない ・パスワードの使用 …… × ・識別コードの使用 …… × ・その他資格確認機能使用 …… ×	不正アクセスを排除することが難しい	つぎの２段階で手当とする ①ＩＤカード方式による資格確認（会計処理の端末機に、ＩＤカード読み取り機構をつける） ③システムにパスワード方式組み込み（全端末機を対象とする）

付属資料 1

FIPS PUB 65

リスク分析ガイドライン

Guideline for Automatic Data Processing Risk Analysis

本資料は、米国商務省標準局が1979年8月に公表した「Guideline for Automatic Data Processing Risk Analysis」(FIPS PUB 65)の翻訳である。

関連資料としては次のようなものがある。

- ・ FIPS PUB 31, Guidelines for Automatic Data Processing Physical Security and Risk Management.
- ・ FIPS PUB 39, Glossary for Computer Systems Security.
- ・ FIPS PUB 41, Computer Security Guidelines for Implementing the Privacy Act of 1974.
- ・ FIPS PUB 46, Data Encryption Standard.
- ・ FIPS PUB 48, Guidelines on Evaluation of Techniques for Automated Personal Identification.

〔ADPリスク分析ガイドライン〕

1. 序 論

コンピュータセキュリティの必要性があるとの意識が高まるにつれて、自動データ処理のサポートを受けている組織が潜在的な脅威からどのような影響を受けるかを定量化する方法の必要性が強く訴えられている。リスク分析はそのような方法の1つである。それは1つの組織が物理的環境、人員、機器、ファイル内容、および処理能力に影響を与えるような条件の下で、その任務と業務を正しく、適切な時期に実行する能力を、そのような条件の発生の確率との関連において見るものである。

このような分析を行う技術はいくつもあるが、2つの主要な要素を常に考慮しなければならない。

1. 好ましくない性質の事象が発生した時に生じる可能性のある損害。
2. そのような事象発生の可能性。

リスク分析の目的はADP（自動データ処理）を使用している経営者がリスクの影響と防護手段との間に経済的なバランスを確立することを助けることにある。それは存在するリスクを指摘し、それに基づいて必要な防護手段を選択するのに役立つ。分析は組織が現在持っているADPに関するセキュリティを検討し、それによって十分で費用効率の高い防護措置を選定するのに必要な基本的な事実を集める。リスク分析の二次的な利益はセキュリティについての意識を高めることで、それは経営者から組織全体を通じて明確にされる。

リスク分析は経営者に、意志決定、たとえばある状況の発生を防止するのか、それが持つ影響を阻止するのか、または単に損失の可能性の存在を認識するだけに止めるのか、という決定の基礎となる情報を提供する。リスク分析はそのような決定の基礎であるため、その損失または損害の推定は、可能な場合には、定量的で比較可能な形で提示されなければならない。

コンピュータシステムのセキュリティを検査、テスト、評価する方法はほかにも多い。たとえば侵入計画の発見、セキュリティ監査、チェックリスト、質問書などである。しかしこれらのいずれもが、リスク分析とは目的が違い、損害と発生の可能性という主要な要素を考慮しないため、リスク分析の代わりにはならない。

リスク分析は1回やればそれで終わるという作業ではない。それは任務、施設、機器などの変化に常に対応するため、定期的に実施しなければならない。そしてシステムの出発時に考案

されたセキュリティ対策は、その後に追加される対策よりも効果的なことが多いので、リスク分析は全てのシステムの設計段階から加えて行くべきである。

リスク分析に必要な重要な資源は人的資源、高度に熟練した要員である。このため、最初の分析が最も費用が高く、後になれば従来の作業に一部を依存することができ、必要な時間も専門知識が増えるところまで減少されよう。

リスク分析に使用する時間はその目的に対応すべきである。複雑な、複数シフト業務と多数のファイルを持つ大規模な施設では、単シフト、小規模の運用施設などよりも多くの時間が必要である。もし価値のある結果を期待するならば、経営者はこの計画を完成するために必要なだけの資源を投入する決意を持つべきである。

2. 経営者の役割

2.1 経営者

リスク分析が成功するかどうかはトップマネジメントがこのプロジェクトに果たす役割にかかっている。その場合、次のことが必要である。

1. 組織の全てのレベルで、プロジェクトに対する経営者の支持が表明されること。
2. 経営者がリスク分析の目的と範囲を説明すること。
3. 経営者が適格なチームを編成し、それに公式に権限と責任を与えること。
4. 経営者がチームの調査結果を検討すること。

経営者はリスク分析チームの調査結果を確実に信頼すべきである。プロジェクトの範囲はA D P施設、機器、要員だけでなく、A D Pユーザ（これは恐らく組織の全部門および組織外のあらゆるユーザを含むだろう）を包含するものと定義されるべきである。

2.2 リスク分析チーム

リスク分析チームの選定はプロジェクトの結果にとって極めて重要である。組織内では次の各部門を代表する要員を参加させることが大切である。

A D P業務管理部門

システムプログラミング（A D P業務と別個の場合）

内部監査部門

物理的セキュリティ部門

適用対象のデータファイル部門（施設が処理するアプリケーションの全てを組織内の一

部門が担当することは少ない。しだがつて各部門は対象となる部門のデータファイルのみを代表すれば良い)

対象ファイルのプログラミングサポート

これらの各部門の代表者は自分の担当の業務だけでなく、組織全体の業務との関連性を良く知っているべきである。この特別チームのリーダーも同様に広い知識を持ち、前記の各部門のうち、最初の3部門のどれかから選ばれるべきだが、その部門の代表とはしない方が良い。つまり、チームリーダーは2つの帽子……1つはリーダー、1つは代表者……を被ってはいけない。これらの条件はただし、前記以外の部門からのチームへの参加を否定するものではない。法務、人事などの部門を少なくとも協議を受けるべきである。

リーダーとチームのメンバーは辞令をもって任命し、その任務、責任、付随する権限を明確にすべきである。また代理が出てくるとこの仕事は満足に進まないことも理解しておくべきである。チームのメンバーは仕事熱心のあまり、必要以上の情報を集めようとする傾向がある。これは業務を長引かせるので、注意しておく必要がある。

契約でリスク分析を行う信頼できる民間会社もある。経営者は内部組織でやるか、こうした会社を選ぶか決定することになる。しかしリスク分析の目的や技術を理解しないために外部に依頼するというのではなく、効率的資源の利用のためにそれを選ぶようでありたい。リスク分析チームに加わる要員は契約社に情報を提供するために必要とされかつ成果が脆弱性のリストを伴う直感で選ばれた解決策のリストではなく、リスク分析である、ことを確実にする人物とすべきである。組織内の要員は、とくに多数のアプリケーションシステムと支持ファイルとを維持している組織では、あまり多くの時間を取れないかも知れないが、リスク分析を通じて契約社のためにすぐに手助けできる体制であることが望ましい。

2.3 時間の配分

リスク分析は時間のかかる、あまり急がせることのできない作業である。参考にできる以前の経験やリスク分析があれば、全ての必要な情報が容易に入手できるので、非常に助けになる。各データセットまたはファイルを、システムを襲うハザードに照らして検討していくのは退屈な仕事だが、それは決定のプロセスで高いレベルの知識と経験を必要とするため、慎重な部下に委任すべき仕事である。しかしこれは見識を豊かにする仕事であり、システムの簡素化にもつながる作業である。

何人かの要員をチームに配属すると、それだけの人数が元の部署から減るために、作業に困難を来すこともある。またチームに配属された者も、以前に与えられていた仕事に早く戻ろ

うと、リスク分析を急ぐ傾向もある。チームが毎日の半分ずつを会合に当てるような合意ができれば、こうした問題を軽減することができよう。

2.4 経営の検討

トップマネジメントは、リスク分析チームの予備的な調査結果および最終的結果の両方を、その妥当性、政策との一致、組織の統一性などの見地から検討し、その後に防護計画を立案すべきである。その計画は必ず財務、管理部門との調整が必要であり、それは組織の長期計画の中に加えられることになる。

3. セキュリティの予備的検討

リスク分析を実施する上での確実な基礎を持つために、チームはプロジェクトの開始に当たって組織の現在のADPセキュリティ、資産交換の費用、組織のADP処理が弱点を持つ実際の脅威などの調査を行うべきである。この調査から得られる知識によってリスク分析に要する時間が多少節約できることになる。このようなグループをスタートさせる時にありがちな不活発さはこの予備調査から得られる3つの特定の成果……資産更新費用リスト、施設が脆弱性を持つ脅威のリスト、現在のセキュリティ対策リストを持つことによって、克服しやすくなる。

3.1 資産費用

検討の産物の1つは資源、施設（コンピュータ、関連機器、データ、建物等）の更新費用、またはその最善の見積のリストである。これらの全ての総額を集めるべきである。この時点で入手できるほかのあらゆる情報よりも、この数字はセキュリティの必要性を良く示すことであろう。もしリスク分析がシステム設計の段階で行われる場合には、完成したシステムにおけるデータ価値の増加とそれを入手する費用の増加とを考慮しておくべきである。

3.2 脅威

予備段階のもう1つの産物はADP施設とその資産がさらされている実際の脅威のリストであろう。たとえば、たつまきの発生は内陸部では実際に可能性のあることだが、海岸地方では可能性は非常に少ない。実際の脅威を認識することによって、リスク分析チームは彼等が分析

している施設およびシステムの脆弱性、すなわち損害の可能性を知ることができる。ここでも、もしリスク分析がシステムの設計段階で行われるならば、現存する脅威を確認するだけでなく、システムの導入または運用から生じる可能性のある将来の脅威をも予測する努力がなされるべきである。この目的のためには、組織内の次の領域を調査すべきである。

◇人事：雇用、解雇手続き、訓練の範囲と期間、全てのレベルの業務監督の質。

◇物理的環境：近隣の状況、ユーティリティ、建物の設計、運用と保守、建物出入りの管理などの質と信頼性。

◇ハードウェア／ソフトウェアシステム：運用上の利用可能性、変更の管理、ソフトウェアの特性、ドキュメンテーション。

◇データ通信：ハードウェアと伝送回路、メッセージの配布を検証し、制御する手順。

◇ADPアプリケーション：技術的設計、ドキュメンテーション、基準（付録A参照）

◇運用：ソースドキュメント保護、情報の配布、I/O制御、テープライブラリ、書式、コンピュータ室処理、ユーザインタフェース、室内管理と保守、運用管理、コンティンジェンシープラン等の基準および手順

システムの脆弱性の原因となる要素を理解することは、リスク分析を行う上で重要である。これらの要素は独立していず、区別することが難しい。以下に脆弱性を見付け出すために使用することができるアプローチの種類の数例を上げてみる。

◇自然災害：どのような自然災害が起こり得る妥当性を持っているだろうか？

どの程度の影響を施設、処理能力、データ、供給品、電力、地域交通などは受けるだろうか？

◇環境：爆発物、可燃性製品、使用されていないか無防備の建物などのような特殊なハザードが近くにあるだろうか？ 近所に火災が発生したらどうなるか？ 消防署は近くにあるだろうか？

◇設備の建屋：ADP施設だけがその建物を使っているのか？ もしそうでなければ、他にどのような使用者がいるのか？ 建物の管理者は誰か？ 保守は誰が責任を持っているのか？ どのような建物の構造となっているか？ どのような警報装置や予防装置が備えられているか？ 暖房器具、調理器具、その他の火災の危険のあるものが近くにはないか？ 床や天井の材料は何を使っているのか？

◇アクセス：処理装置へのアクセスはローカルかリモートか？ 侵入者は処理装置、データ、ソフトウェア、装置、記憶メディア、印刷前書式、供給品、ドキュメンテーション、出力または廃物などに容易に接近できるか？ 職員の場合はどうか？ 偶然に、故意に、また

は利益のために接近する可能性は？

◇作業環境： 職員と管理者との関係はうまく行っているのか？ 監督者はどの程度部下を知っているか？ 管理者はシフト要員の問題を理解しているか？ 監督者は従業員の問題を管理者に良く伝えているか？ 職員は忠実か？

◇データ価値： 侵入者はシステムに侵入し、データを暴露し、事業運営を妨害してどれほどの利益になるのか？ 無許可の暴露または不正確なデータによってその対象者はどの程度の損害を受けるのか？ 組織はデータの暴露、または不正確なデータに基づく決定や処理能力の遅延によってどの程度の損害を受けるのか？

3.3 現有のセキュリティ手段

この段階の最後には、現在使用されている全てのセキュリティ保護手段のリストを、それらのもともとの目的（記憶メディアログ、印刷物配布の管理、データ入力品質管理等）が保護を目的としていなくても、作成すべきである。一般に優れた管理上の慣行はセキュリティを向上させるものである。敷地境界のフェンス、警備員、出入バッジなどの特定のセキュリティ措置も建物内の全てのオフィスや施設の保護のために実施され、ADPが別の場所にある時でも、行われることであろう。これらの現有の手段に対して具体的に考えられる脅威もリストアップすべきである。

3.4 経営者の検討

これらの調査結果は、完成次第に経営者に提出されるべきである。これらの結果は最終的なセキュリティ計画が完全なリスク分析に基づいて実施されるまでの、暫定的な防護措置の必要性を指摘することができる。

4. リスク分析

原因が何であれ、ADPに発生する障害は組織に次のような状態のいくつかを失わせる障害を与えることになる。

データの完全性：自動化データがソースドキュメントにあるものと同じであり、またはソースデータから正確に計算され、偶然の改変または破壊を受けていない時に存在する状態。不完全なデータ、データの無許可の変更または追加、および誤っているソースデータは全てデータ

の完全性に反するものと見なされる。

データの機密性：データが機密として保管され、無許可の開示から保護されている時に存在する状態。限定された目的のみにデータを使用する許可を持つ者がそれを誤用した時も、データの機密性の違反と見なされる。

A D Pの利用可能性：必要なA D Pサービスが不利益な環境下においても許容できる時間内に履行できる時に存在する状態。

リスク分析が細部に捕われ過ぎないように、チームは望ましくない事象が何故発生するかよりも、それらの考えられる結果、すなわちそれらが引き起こす損害の範囲などに集中すべきである。それは組織が脆弱性を持つ有害な事象は予備段階ですでに明らかにされているからである。

4.1 要素

リスク分析の基本的な要素は好ましくない事象が引き起こす可能性のある損害のアセスメントと、そのような事象がある期間内に発生する確率の推定である。

チームにとって多くの事象の被害または頻度を絶対的に知ることは不可能であるため、それらは歴史的データやチームのシステムについての知識、それら自身の経験や判断を用いて推定しなければならない。しかしある大きさの範囲の推定は大部分の場合、リスク分析の目的には十分に正確である。後になって保護措置を選択する時に特定の事項を定義することが重要になった場合には、それを行うことができる。しかし分析の段階では被害と頻度の総体的な表現で必要なものは満たされる。

4.2 被害と頻度の表現

ある事態から考えられる被害とその発生の推定頻度の定量的な表現方法がリスク分析を実施するために必要である。

今日まで、ある不利な事象の被害を定量化する方法としては、損害が具体的なものであれ、抽象的なものであれ、犠牲者が人間であれ機械や装置であれ、金銭的な価値より優れた共通分母はまだ発見されていない。金銭的価値は裁判所が物的損害と精神的苦悩の両方を賠償する時に使用する補償である。一部の方法では被害を抽象的に記号で表わすことを主張している。実際は“\$”がその記号であり、中間的な翻訳をしなくても直接に金銭に移すことができる。

被害は金銭的に表現され、また財政事項は連邦政府諸機関では年度ベースで処理されているので、脅威の予測される発生頻度を表現する場合に特定する時間的期間としては年単位が最も

適当である。脅威の中には数年に1回しか発生しないものも、また一日に何回も発生するものもある。それらを年単位で表現するのは必ずしも容易ではない。たとえば「1日に5回」は「1年に1825回」としなければならず、また「5年に1回」は「1年に1/5回」とすることになる。

もし被害と頻度を図1に示すように、10を単位とする桁の中で端数整理することができれば、分析に要する時間を節約し、その有効性は減少しないだろう。ある事象の損害が11万ドルと推定されても、また14万5千ドルと推定されても、全体的な危険に対するイクスポジユアの程度には変わりはない。機密データの暴露による職歴上の損失、または年金小切手の到着の遅れからくる心配などに金銭的価値を割り振ることは、実際の金額の場合よりも桁数単位の方がずっとやりやすい。またある事象の頻度が1年に12回でも30回でも違いはない。図1の頻度スケールを使えば、面倒な分数の使用が避けられ、1日に何回という高確率の事象やまた何年に1回という低確率の事象を一緒に取扱う場合に弾力性を保つことができる。

図1. 推定被害と頻度の桁数

<u>損害</u>	\$ 10	<u>頻度</u>	300年に1回
	\$ 100		30年に1回
	\$ 1,000		3年に1回 (1000日に1回)
	\$ 10,000		100日に1回
	\$ 100,000		10日に1回
	\$ 1,000,000		1日に1回
	\$ 10,000,000		1日に10回
	\$ 100,000,000		1日に100回

4.3 年間損失イクスポジユア (ALE)

もしある事象の被害、すなわちそれが与える損害の正確な金額、およびその事象の発生頻度、すなわちそれが生じる正確な回数を特定することができれば、その両者の積は損失を表わすことになる。すなわち、損失＝被害×発生頻度

しかし正確な被害も特定することは難しいのが普通であるため、損失の近似値を年間損失イクスポジユア (Annual Loss Exposure) によって表わすことだけが可能である。これはドル計算の推定被害 (I) に年間推定発生頻度 (F) を掛けた積である。

使いやすいように、推定被害と推定発生頻度の係数には図2に示すように指数を付けること

ができる。

図2. i および f の値の選定のための表

事象の推定コスト被害と指数 (i)		推定発生頻度と指数 (f)	
\$ 10	i = 1	300年に1回	f = 1
\$ 100	i = 2	30年に1回	f = 2
\$ 1,000	i = 3	3年に1回	f = 3
\$ 10,000	i = 4	100日に1回	f = 4
\$ 100,000	i = 5	10日に1回	f = 5
\$ 1,000,000	i = 6	1日に1回	f = 6
\$ 10,000,000	i = 7	1日に10回	f = 7
\$ 100,000,000	i = 8	1日に100回	f = 8

i と f とを被害と頻度の可能な桁数とする時、

$$i \text{ と } I \text{ との関係は } I = 10^i$$

$$f \text{ と } F \text{ との関係は } F = \frac{10^{(f-3)}}{3} \quad \text{すなわち}$$

$$F = \frac{10^f}{3,000}$$

このように年間損失予測値は次の公式によって計算することができる。

$$ALE = \frac{10^i}{3} \times 10^{(f-3)} \quad \text{これを通分すると} \quad ALE = \frac{10^{(f+i-3)}}{3}$$

図3に示す表を使えば、公式によって計算するよりも早くALEが得られるが、結果は同じである。図2から必要なiとfの値を選び、図3でそれらに該当する縦列と横列の交差する位置を求めれば、その数値がALEを示している。

図3. ALEの値を決定するための表

		Fの値							
		1	2	3	4	5	6	7	8
Iの値	1					\$300	\$ 3K	\$ 30K	\$300K
	2				\$300	3K	30K	300K	3M
	3			\$300	3K	30K	300K	3M	30M
	4		\$300	3K	30K	300K	3M	30M	300M
	5	\$300	3K	30K	300K	3M	30M	300M	
	6	3K	30K	300K	3M	30M	300M		
	7	30K	300K	3M	30M	300M			
ALEの値									

図2と図3の表を組み合わせると図4の便利な表ができる。

図4. i, f, およびALEの組み合わせ行列表

		(三 十百 万年 日に 一回)	(三 一十 万年 日に 一回)	(三 千 年に 一回)	百 日 に 一回	十 日 に 一回	一 日 に 一回	一 日 に 十 回	一 日 に 百 回
i = f =		1	2	3	4	5	6	7	8
\$ 10	1					\$300	\$3,000	\$ 30K	\$300K
\$ 100	2				\$300	\$3,000	\$30K	\$300K	\$3M
\$ 1,000	3			\$300	\$3,000	\$30K	\$300K	\$3M	\$30M
\$ 10,000	4		\$300	\$3,000	\$30K	\$300K	\$3M	\$30M	\$ 300K
\$ 100,000	5	\$300	\$3,000	\$30K	\$300K	\$3M	\$30M	\$300M	
\$ 1,000,000	6	\$3,000	\$30K	\$300K	\$3M	\$30M	\$300M		
\$ 10,000,000	7	\$30K	\$300K	\$3M	\$30M	\$300M			
\$ 100,000,000	8	\$300K	\$30M	\$30M	\$300M				

4.4 手 順

チームはその作業を進行させる組織的な方法とその調査結果を記録する秩序だった方法を必要とすることになる。チームはデータ処理作業に悪影響を及ぼす全ての事象を列挙することはできないと思われる。したがってリスク分析の作業は、有限な数のデータファイルやアプリケーションシステムの見地からアプローチしていくのが良い方法である。各データファイルまたはアプリケーションシステムについてのワークシートを作り、それに調査結果も記入していけば、作業の基礎的な手順ができ上がる。

ワークシートはその組織が有効と考えるならどんな形式でも良いが、できるだけシンプルで、余分なデータを含まないことが必要である。図5に示したワークシートはコピーして、または作業内容の記入のためにもっとスペースを増やして使うことができる。

組織のアプリケーションシステムとアプリケーションによって作成されたデータファイルの全てをワークシートに記入することになる。システムを通じてデータフローを追跡することにより、チームは予備調査で処理作業に脅威が発生し得るとされた箇所を正確に特定することができるだろう。脆弱性の予備調査がすでに行われ、またチーム全体がシステムのアプリケーションファイルを良く知っているため、チームはこれらの事象の妥当な推定頻度を定めることができるはずである。もしあるファイルが複数のシステムに使用されている場合には、それぞれのシステムのリストにそのファイルを記入すべきである。システムが違えば、受ける脅威も異なるからである。

多数のファイルを持つ組織では、その最初のリスク分析では作業量が非常に多くなるため、ファイル単位ではなく、アプリケーション単位でデータを検討することを希望すると思われる。そして、もし一つのアプリケーション内のファイルごとに保護の要件が著しく異なることが判明した場合には、データごとのもっと詳細な検討を行うべきである。

i と f の値はALEの場合と同様に、各ワークシートの交差位置に記入すべきである。そうでないとある特定のALEのための基礎を再構成することが不可能となるからである。実際の脅威のリストには、各脅威が持つと推定されるALEの現行の総計を記入していく。（もし新たな脅威が表面化したら、それをリストに加えるべきである）「コメント」の欄にALEと特定の脅威との関係を説明しておけば、是正措置を選択する時に役に立つ。

この段階では、好ましくない事象に対して現在備えられている保護手段は考慮に入れるべきではない。それを考慮するためには効能性の判断が必要であり、それは後の防護手段の選定の過程の一部とするのが適当である。

もしデータの完全性、データの機密性、または処理上の利用可能性に複数の状況が影響する

場合、それらの事象の i と f とは個別に記入すべきである。これはセキュリティ措置の決定のために有効である。システムの中で問題が発生する危険のあるステップないし機能を「コメント」の欄に記入する。チームがデータの機密性を検討している場合、内容とする個人、財産、その他の情報が公開されても問題を生じないことが判明しているファイルを最初に除外しておけば作業は非常に簡素化される。

データの完全性については、データの修正と破壊を区別する必要がある。この 2 つは被害が異なり、また同じ頻度で発生することもないからである。

「コメント」の欄は図 6, 7 で示すように、破壊事象が発生する危険のある処理ステップを記入するのに使用できる。またある状況をもっと完全に説明する必要がある時に、この欄に注釈を記入してもよい。

「処理能力の利用可能性」の欄の時間的期間は任務によって左右され、各組織がそれぞれに決定すべきである。これはバックアップ能力の選択のために重要であり、トップマネジメントによる審査を必要とする。機器の破壊は「処理能力の利用可能性」の欄で検討すべきである。機器が破壊されれば、最後にはデータを処理する能力を喪失するからである。被害は機器を交換するコストではなく、処理能力喪失のコストになるだろう。交換も可能な回復措置であり、そのコストはその他の措置と同じように分析すべきである（第 6 章の説明を参照）。

4.5 特殊な助言

A D P リスク分析は、チーム構成員の直観力、経験、専門的知識に対する依存度が著しく高い技術である。この章の説明の目的はいくつかの問題を展開し、チームの決定の根拠となるべき前例や指針がほとんどないような領域においても、チームがその集団としての判断に自信を持てるようにすることにある。

4.5.1 人間の弱さ

チームは、あるシステムのセキュリティに人間的な完全性がどのような役割を果たすのか、考量する際に疑問を持つことであろう。A D P 環境内に働く全ての連邦政府職員は、それが取り扱うシステムの内容や目的に適した資格審査を受けなければならないが、ある個人にどのようなストレスが働き、自宅でどのような圧力を受けており、作業環境にどのような嫉妬が存在し、どのような金銭的な負担を背負っているか、などを常に掌握することは不可能である。このような理由から、個人の人間的な完全性を、リスク分析におけるセキュリティに貢献する要素から除外しておくのが最善である。人間的な完全性を検討するのは各種の防護

手段を討議するセキュリティ計画策定の段階が適切であろう。

コンピュータ犯罪の統計が蓄積されるにつれて、次のようないくつかの一般的な結論が生れている。〔10〕

◇ホワイトカラー犯罪の大部分は従業員がその雇用者をだます形で行われている。

◇一般に、雇用者をだます従業員はその業務の遂行の中で接近できる機器、データなどのリソースを使用して犯罪を犯している。

◇ホワイトカラー犯罪に対する最善の対策は誘因を消滅させること、すなわち与えられた仕事に付随する不正行為が利益をもたらす可能性を極力少なくすることである。もし従業員が不正な行為からほんの僅かな利益しか得られないとすれば、それに引き込まれることは少なくなる。次善の対策は発覚の恐れを高めることである。従業員が作業の監視が十分に行われていることを知れば、危険な行為に手を付ける率は減っていくだろう。

図 5. リスク分析のワークシート

システム／アプリケーション データファイル	データインテグリティ		データの機密性	処理能力の利用可能性			コメント
	修正	破壊					
	(i) (f) (A L E)	(i) (f) (A L E)	(i) (f) (A L E)	(i) (f) (A L E)	(i) (f) (A L E)	(i) (f) (A L E)	

4.5.2 物理的セキュリティ／処理能力の喪失

チームが遭遇するもう1つの困難は、火災、洪水、その他の自然災害を物理的セキュリティの問題としてだけ取り扱うことから生じる混乱である。自然災害がまず与える被害は物的な破壊だが、処理能力に対してもあまり明白ではない影響、たとえば電力の喪失、重要人物のサービスの喪失、データ記憶媒体の損害などを与えることがある。施設に何の損害がなくても、作業ができないこともある。

物的施設の喪失と処理能力利用可能性の喪失とは、それぞれ別個に取り扱うべきである。この両者はお互いの原因には必ずしもならないからである。物的破壊以外の原因によっても処理能力が完全に失われることもある。たとえばハードウェアの故障が全ての処理能力を数日間止めることもあれば、重要なプログラムまたはデータを誤って抹消したために、緊急を要する作業が数時間ストップすることもある。別の建物の火災のためにADPセンタが停電し、アウトプット用紙が詰まって、用紙を取り出すまで、時には何週間もアウトプットを止めたりする。洪水による損害は必ずしも川の氾濫で起きるとは限らない。器具の漏洩、パイプの破裂、近くでの消火活動もその原因となる。

4.5.3 発生の推定頻度

最初のうちはこれまで発生したことがない事象の頻度を推定することは不可能だとチームは考えるかもしれない。しかし常識がそれを助けてくれる。たとえば小切手の数やその金額などを管理している優れた自動支払い制御システムがあるとする。百人から千人の間の人々が検知される危険なしに受取人の住所を変更することが比較的に容易なことを知っている。それらの中の一人が小切手を別の住所に送るようにし、本来の受取人以外の者の手に渡るようにするのは容易である。このような状況での推定頻度は、恐らく30年に1回よりはずっと高く、10日に1回よりはかなり低いだろう。すると3年に1回か、または100日に1回の選択となる。これらの数値の最も妥当なものを選ぶためには、そのシステムが使用されている一般的環境を含むいくつかの要素を考慮する必要がある。もし脆弱性を知っている人間の数が百人か二百人であれば、3年に1回というのが可能性のある数値である。もし知っている人間が千人に近ければ、または従業員の不正がある限界内ならば経営者がそれを認めている状況であれば、推定頻度はもっと高くなるとみてよい。

4.6 ドキュメンテーションの機密性

リスク分析に関連する全ての報告書、ワークシート、その他のあらゆる文書、記録などは高

度の機密性を持つものとして扱い、その組織が使用している適当な方法によってその旨を表示すべきである。

5. 具体的事例

リスク分析において考慮しなければならない局面のいくつかを示すために、仮定の政府機関を使った事例が作成されている。ここではその機関の総ADPアプリケーションのごく一部だけを検討してみる。

5.1 一般的環境

5.1.1 中央コンピュータ施設

◇中央ADP施設はカンサス州中部にある同機関本部の3階建ての別棟にある。

◇装置は大型プロセッサ（CPU 3台、テープドライブ32台、100億文字のディスク記憶装置、総計175の端末機を取り扱う能力＝現在は125がシステムにある＝を持つ）、COMユニット1基、5万リールのテープライブラリから構成される。中央施設と端末機間の通信は専用回線が使用されている。

◇コンピュータ区域に出入りする全ての人物を警備員がチェックしている。バッジが必要である。警備員が警戒していない区域は電子カードシステムによって管理されている。バッジおよびカードパスの紛失、置き忘れ、盗難、損傷、および訪問者に対するバッジの発行については、規定の手順が実施されている。

◇監視下にある火災検知／消火システムがあり、それは燃焼生成物探知装置とドライパイプスプリンクラー装置から成っている。施設の各所に手動の消火器が置かれており、その種類は近くにある装置や備品によって決められている。全てのコンピュータ操作要員には継続的な非常事態訓練が義務づけられている。この訓練には各種の消火器の実際の使用が含まれている。職員が最初に採用された時、およびその後も毎年、火災安全指導が行われている。コンピュータ施設に隣接する建物の区域は火災検知器を持たない。これらの区域はデータ処理以外の操作ユニットの制御下にある。

◇非常用電源または連続電源バックアップはない。最近の7年間、施設は落雷、変電所の火災、建設工事のための給電線切断などによる停電のために、機器の故障を経験している。最近の数か月、とくに夏の間は局地的な電圧低下が電子装置の故障を引き起こした。

これらの電圧低下は3週間に1回程度発生している。

◇電気調節装置は5年前のもので、3回の故障を経験している。1回は据付けから2年後、1回は18か月後、1回は3年目である。ADP施設がある別棟の屋上に100トンの冷却塔2基がある。

◇施設の全てのハードウェアにはプラスチックのカバーが掛けられている。床は24インチ高くなっており、水が入ってきた時のために自動排水ポンプがある。テープライブラリは水からは十分に保護されている。

◇非常パワーダウンスイッチが全てのコンピュータおよび空気調節システムに備えられている。

◇経営者は毎年、適切でない取り扱いによって、または誤ったラベル表示のために400のテープおよび/またはディスクファイルが間違った場所に置かれ、または破壊されていることを知っている。

◇職員の士気は非常に高い。同機関は良好な人事方針を確立しており、職員の苦情処理手続きも公正に、大部分の人間が満足する形で運営されている。すべてのADP要員は、マネジメントが中央および遠隔の施設の双方におけるセキュリティの手順を維持し、実施することに関心を持っていることを知っている。

◇オペレーティングシステムは1週間に数回、再スタートさせなければならない。トラブルはハードウェアの故障のためだと突き止められることもあるが、解決されないのが普通である。システムプログラマは、システムをほとんど直接の監督なしで維持している。変更が行われる前には正式の検討は行われぬ。オペレータはどうすればシステムがうまく動くかを知っているが、夜間の監督者の中にはオペレータのすることをほとんど理解しない者もいる。

5.1.2 端末機

◇遠隔ジョブエントリー端末機は全てGSAのリーススペースに置かれ、各現場事務所に1つずつ配置されている。人がいない時には施錠される。しかし端末機は、機関のいくつかの部門によって多くのシステムのために使用される。磁気テープは端末室の施錠したキャビネットに保管されている。データテープは1か月だけ保存される。マイクロフィルムソースドキュメントは端末室以外の安全な場所に保管されている。データは端末機から中央装置に送られる間は保護されない。

5.1.3 バックアップ施設

◇ADPの非常用バックアップについての計画は何もない。

5.2 特殊システム

5.2.1 アプリケーション100

このアプリケーションは、毎月第3木曜日に報告書を作成、提出することを規定した大統領府命令から生じた業務をサポートするものである。それは10年間にわたって自動化されている。最も新しい報告書を含むマスターファイルは、30の現場事務所から中央施設に送信される新しいデータによって毎月更新されなければならない。新しいデータが加えられると、新しい報告書が作成され、管理下にある公式チャンネルを通じて配布される。

このアプリケーションには、次のような状況のセットがあるものと仮定されている。

◇データが連邦政府諸機関にとって必要である。これらの出力は早期に発表されれば民間部門に経済的影響を与える可能性がある。

◇現場事務所では、データが機械読み取り用フォーマット（磁気テープ）に翻訳された後、ソースドキュメントはマイクロフィルム化される。7事務所がマイクロフィルム化装置を備え、23事務所は契約で外部に依頼している。

◇中央施設へのデータ送信は、各火曜日の第三作業シフト（0001～0800）の間に行われる。

◇通信ネットワークに障害が発生した場合には、データテープは中央施設に空輸される。

通信障害は1年に平均3回の割合で発生する。

◇適当な審査を受けたADP要員のみがこのプロセス全体を通じてデータ取り扱いを許可される。

◇現在まで、データへの無許可の接近または事前発表が判明したことはない。

◇更新された報告のコピーは中央施設の特別の施錠したキャビネットに保管され、バックアップコピーはGSA記録センタに保管される。バックアップコピーは3サイクルで、すなわち当月とその直前の2か月分が保管される。

◇最終報告の一部であるセクションAは予備的データに基づいて作成され、最終データの送信の2日前に送信し、分析を開始できるようにしなければならない。前月の報告の更新のためには、マスターテープの作成が必要である。このプロセスでは別のある種のテープファイルを使用しなければならないが、その中には人事任命データ、地域的プロジェクトデータ、予算状況データなどが含まれる。

◇各要素とも最終製品のためには重要であると見なされている。各段階が終了した時には

持ち込まれた可能性のある誤差を点検しなければならない。これまで重大な誤差が除去されたことはない。発見されてきた誤差は主として、現場事務所で作成された新しいデータテープに限定される。

◇もしこのシステムが侵犯され、または報告が遅延した場合には、若干の悪影響が株式市場に感じられるだろう。政府も国内、国際的に困難な立場に立つであろう。

◇データは「外部」の人間に非常な重要性を持つため、比較的に高い地位の政府職員が情報の早期の入手を求める、または最終レポートを確定している発表期日に間に合わせないようにする誘惑にかられる可能性がある。

◇全ての関係職員は、管理者からあらゆる態度の変化、業績の低下、その他の本プロジェクトのセキュリティ違反につながる恐れがある状況の徴候を観察されている。

◇ソフトウェアシステムについての全ての訂正、更新、または修正は、綿密に監視、テストされ、その後に最終的な承認を受け、マスターシステムに取り入れられる。

システムは次に示す6段階から構成される。

<u>インプット</u>	<u>プロセス</u>	<u>アウトプット</u>
第1段階 データの作成 ソースデータ	テープ化 検証 複製 マイクロフィルム ソースドキュメントの破壊	ソースデータテープ +マイクロフィルムの コピー1部
第2段階 データの送信 ソースデータ テープ	送信 検証	データテープの変更
第3段階 ファイル維持 マスターテープ (当月)	更新 検証 テープ複製	マスターテープ (新規+1サイクル)
第4段階 データテープ作成 セクションAの作成 マスターテープ 人事任命データ 地域プロジェクトデータ 予算状況データ	計算 フォーマット	セクションAの報告
第5段階 最終報告の作成 マスターテープ 人事任命データ 地域プロジェクトデータ 予算状況データ	第4段階に同じ	最終報告
第6段階 疑問点の審査 マスターテープ 人事任命データ 地域プロジェクトデータ	検索 読み取り	ビデオディスプレイ

(このアプリケーションのためのワークシートは図6に示されている。)

5.2.2 アプリケーション870

このシステムは機関の最近5年間、今年、および今後5年間の3種類の機関の計画と総予算情報である、ProgHist CurrProg, および AgPlans を維持、管理するために使用される。このソフトウェアは、同機関が作成したプログラムのPFiles, および商業的専有プログラムであるWWWModからなり、それは将来の計画のための最適のコースを選択するのに必要なモデリングを行うものである。

トップマネジメントのオフィスには、6台のビデオグラフィック端末機がハードコピープリンタとともに備えられ、機関の長官室には大型のビデオスクリーンを持つ小型の制御センタがあり、スタッフ会議でのオンラインモデリングの結果をディスプレイするのに使用される。全てのファイルは通常の作業時間中はオンラインになっている。それは毎日の作業時間後の午前1時に、前日の取引（通常は平均10件）によって更新される。ただし2月と8月は処理時間が1か月1.8時間から同4時間に急増する。

このシステムは次に示す3段階から成っている。

<u>インプット</u>	<u>プロセス</u>	<u>アウトプット</u>
第1段階 日間ファイル維持（午前1時、月間1.8時間、2月と8月は同4時間）		
CurrProg	ファイル更新	CurrProg
PFiles	検証	
	複製	
第2段階 審査とモデリング（毎日午前8時から午後5時）		
AgPlans	ファイル検索	ビデオディスプレイ
CurrProg	ファイル読み取り	プリントアウト
WWWMod	計算	
第3段階 半年報告の作成（作業時間中、2月と8月）		
AgPlans	計算	MBO将来報告
CurrProg	検証	（2CCのみ）
ProgHist	フォーマット	AgPlans
WWWMod	AgPlans更新	ProgHist
PFiles	ProgHist更新	ビデオディスプレイ
	検証	

（このアプリケーションのためのワークシートは図7に示されている）

図6. アプリケーション100のためのリスク分析ワークシート

システム/アプリケーション データファイル	データの完全性		データの機密性	処理能力の利用可能性			コ メ ン ト
	修 正	破 棄		2 時間	24時間	72時間	
アプリケーション 100	(i) (f)	(i) (f)	(i) (f)	(i) (f)	(i) (f)	(i) (f)	
	(A L E)	(A L E)	(A L E)	(A L E)	(A L E)	(A L E)	
ソースドキュメント	4 1	4 1	5 2 ^a	—	—	—	a. テープ変換, 段階 1 ~ 9
			\$ 3 K				
ソースデータテープ	4 4 ^a	3 2	5 3 ^a	—	—	—	a. テープ変換, 段階 1 ~ 9
	\$ 30K		\$ 30K				
マイクロフィルム	—	—	5 3 ^a	—	—	—	a. マイクロフィルム, 段階 1 ~ 9
			\$ 30K				
変更データテープ	3 3 ^a	3 3 ^a	5 4 ^a	—	6 3 ^a	—	a. 送信, 段階 2 ~ 21
	\$ 300	\$ 300	\$ 300K		\$ 300K		
マスターテープ	5 3	5 3 ^{a b}	5 4 ^{a b c}	7 4 ^{a b d}	—	—	a. 全運用, 段階 4 ~ 14 b. 全運用, 段階 5 ~ 14 c. 読み取り, 段階 6 ~ 14 d. 停電, 運転停止
	\$ 30K	\$ 30K	\$ 30M	\$ 30M			
人事任命 データ	5 1	5 1	5 1	5 3 ^a	—	—	a. 計算, 段階 4, 5 ~ 19, 23
	\$ 300	\$ 300	\$ 300	\$ 30K			
地域プロジェクトデータ	3 2 ^a	3 1	4 2 ^a	5 3 ^a	—	—	a. 計算, 段階 4, 5 ~ 19, 23
	\$ 300		\$ 300	\$ 30K			
予算状況データ	3 1	3 1	4 1	5 3 ^a	—	—	a. 計算, 段階 4, 5 ~ 19, 23
				\$ 30K			

図7. アプリケーション870のためのリスク分析ワークシート

システム/アプリケーション データファイル	データの完全性		データの機密性	処理能力の利用可能性			コ メ ン ト
	修 正	破 棄		2 時間	24時間	72時間	
アプリケーション 870	(i) (f) (A L E)	(i) (f) (A L E)	(i) (f) (A L E)	(i) (f) (A L E)	(i) (f) (A L E)	(i) (f) (A L E)	
AgPlans	6 3 \$ 300K	4 2 \$ 300	7 4 \$ 30M	—	—	—	
CurrProg	5 3 \$ 30K	4 2 \$ 300	6 3 \$ 300K	—	—	—	
ProgHist	4 2 \$ 300	—	—	—	—	—	
WWWMod	4 3 \$ 3 K	4 2 \$ 300	4 3 \$ 3 K	—	—	—	
PFiles	4 2 \$ 300	4 2 \$ 300	4 2 \$ 300	—	—	—	

6. 防護措置の選択

6.1 各種の代替的手段

どのような保護手段が最善の全体的セキュリティを確立できるかを決定する過程において、経営者はまず手続き的および物理的防護措置を検討すべきである。手続き上のコントロールは特にそれが物理的障壁と共に用いられた場合は、全ての形式の保護の中で最低のコストによる最高のセキュリティを確立する。それらは1974年プライバシー法の要件、および警備上で必要な、または規則によって規定されているその他の多くの要求を満たすものである。手続き的な手段としては、バックアップデータの所外保管所での全雇用応募者についての審査から、コンティンジェンシープランの作成と試験のためのプログラム開発基準までが含まれる。手続き的手段は手動と自動の処理の間、人間とシステムのハードウェア、ソフトウェアの間のギャップを埋めるために欠かせないものである。それらは人間の過失に起因する誤りや素人の盗難から発生する事故に対して非常に効果的である。それらは管理者がデータと処理のセキュリティについて警備を厳重にしているという雰囲気を生み、それはよほどの覚悟のある者を除いて大部分の者の意志を押さえることができる。

大部分の手段は複数の脅威に対して効果を持つ。施設への立ち入り記録を付けるのも、施設に出入りする者が管理され、ある時刻に施設内にいた者が識別され、施設から無許可で材料を持ち出すのを防止する1つの方法である。記号化はデータを送信中も保管中も保護してくれる。監査証跡はバックアップおよび検索の情報を提供し、また変動検出の基礎を作る。

第5章の例に戻ると、アプリケーション 870において、ファイルは希にしか使用されないが、それらは作業時間中は常にオンラインにあり、そのことはファイルの脆弱性を非常に大きくしていることが判明している。もしファイルが専用のプロセッサで実行されるアプリケーションにとってのみ利用できるようになっていれば、保護の必要性は著しく低減されるだろう。これは定期的な実行、またはある程度の通告で可能になる。この方法を取れば、数百万ドルに値するイクスポジューがシステム要件を検討する費用だけで防止できる。アプリケーション 100の場合、現場事務所で発生し得る損失は僅かなもので、検討してみると、手続き的な手段を取れば回避できる性質のものであるように思われる。このシステムで予測される最大の損失はマスターテープ上のデータ、およびマスターテープ上のデータを必要な報告に変換するための処理能力の利用可能性に直接関連している。これらの2つの領域の防護措置を取れば、同時にその他の重要性が低い多くの問題にも有益な効果があることは明らかである。

システムセキュリティ措置は、物的および手続き的防護措置が組織の保護要件を満たすのに

不十分であることが確認された後に、初めて考慮すべきである。もし組織があるシステムについてソフトウェアまたはハードウェアの保護を使用する必要がある場合、それらの措置は要件の程度が低いシステムの保護計画にも組み込むことができる。ただしそれらのシステムの運用コストがそのことによって異常に高くないことが条件である。

6.2 ALEの低減額対費用

各手段の費用は3つの別々の方法で検討すべきである。第一はそれがもたらすALEの低減額に対比する方法である。次に組み合わされた措置の総費用を純ALE低減額に対比する方法である。第三は各手段によるALE低減額をその総費用の中の比率と対比して検討すべきである。セキュリティ措置の選択については、FIPS PUB31〔6〕、FIPS PUB41〔1〕およびNBS特別出版物500-33〔2〕でも検討されている。

図8に示すようなマトリックスを使えば、脅威とそれらに影響を与え得る保護手段とを表示することができる。脅威はそれが持つALEの順（最大から最小へ）に配列すべきである。マトリックスの各交点には次の3つの情報が含まれる。(a)推定ALE低減額 (b)手段の年間費用 (c)その結果の年間節約金額。これらの3つの数字を得る時には非常な精密さを必ずしも必要としない。手段の年間費用はそれが関係する最も重大な脅威に対応する列に記載されている。影響を受けるその他の脅威の列に記載されている年間費用の数字はそれらの脅威に対応するための費用の増加分を示している。

続いて、現在のセキュリティ手段が施設の全体的なセキュリティにとってどの程度有効かを評価すべきである。これらの手段は全てマトリックスの中に含まれるべきだが、最初の設置費用ではなくて、年間の維持費用のみを検討すべきである。それは設置費用はすでに支出済みのものだからである。コンピュータセキュリティの目的だけではない手段の費用は、可能ならば比例配分すべきである。

図 8. 防護手段と脅威の対比

		<u>手 段</u>			
<u>脅 威</u>		A	B	C	D
	(a)	* \$ 20,000	\$ 20,000	\$ 18,000	
	(b)	9,000	15,000	8,000	
1	(c)	11,000	5,000	10,000	
	(a)	10,000	12,000	—	
	(b)	—	—		
2	(c)	10,000	12,000		
	(a)	4,000	6,000	—	
	(b)	1,000	—		
3	(c)	3,000	6,000		
	(a)	2,000	4,000	—	
	(b)	5,000	2,000		
4	(c)	-3,000	2,000		

*前記の説明を参照。

またこの時期には更新費用をも検討すべきである。装置の更新はその他の救済手段と同様に扱うべきである。装置更新の費用の方がそれを保護する費用よりは安い場合も出てくる。

同じ脅威（またはより低い含まれた脅威）に対処する全ての手段を比較すると、どの手段が所定の状況下で費用効率が最も良いかが判明する。上記のマトリックスでは、保護手段 A は費用 \$ 10,000 で、脅威 1, 2, および 3 に対して合計 24,000 の節約を果たし、一方、手段 B は年間費用 \$ 17,000 で脅威 1, 2, 3, および 4 に対して、合計 \$ 25,000 の節約をもたらす。この 2 つの手段を合わせると、\$ 27,000 の年間費用で A L E が \$ 31,000 節約できる。しかし最終的な比較によると、手段 A のために \$ 10,000 を支出しても、\$ 17,000 の支出で得られるものに、\$ 6,000 だけの追加節約をもたらすだけであることが分る。状況によっては、追加の低減が必要であると決定されることもあるだろう。しかしもっと重要性が低い状況では、代わりに費用の節約が採用されることになろう。さらにある脅威に対処するために選ばれる手段はその他の脅威の予想頻度を確実に増加させないようにするため、注意が必要である。

全ての A L E 低減、費用等の数字を並べてみると、満足できるセキュリティ手段の積み上げが達成されるまでに、さまざまな防護手段の組み合わせを試みとして検討することができる。

このマトリックスは経営者に対して、なぜある防護手段の選択が必要かを説明する上で役に立つものである。

このマトリックスおよびリスク分析に関連するその他の全ての資料は高度に機密性のものとして取り扱うべきである。リスク分析チームが作成した全ての手紙、書類、ワークシート、報告等のコピーはその後においてリスク分析を行う人々のために保管しておくべきである。

付録A アプリケーションシステムの脆弱性

チームがアプリケーションシステムやデータファイルを検討する場合、重大な結果をもたらす多くの有害な事象を知っておくことは、チームにとって役立つことであろう。ここではアプリケーションシステムが脆弱性を持つ多くの状況がリストアップされており、共通のシステム組織構造に従ってグループ化されている。このリストは、全てを含めることを目的としたものではなく、各システムに存在する可能性がある各種の脆弱性を示すために作成されたものである。

1. 誤謬または偽造データ入力：

誤謬または偽造された入力データは、アプリケーションシステムの望ましくないパフォーマンスを引き起こす最も簡単で、最も多い原因である。次のような状況の下でデータが収集され、手作業で処理され、またはコンピュータに入力するために作成された時には、常に脆弱性が発生する。

- ◇ 妥当でない、または一貫性を欠くソースデータ数値が検出できない。

- ◇ 転記の間のキー操作の誤りが検出できない。

- ◇ 不完全なまたは不十分なフォーマットのデータ記録が、完全であるかのように受理され、取り扱われる。

- ◇ 1つのフォーマットの中の記録が別のフォーマットに従って解釈される。

- ◇ 職員が自分の利益（たとえば小切手、流通性のあるクーポン）を得るためにデータ（支払い証書、請求書など）に偽造の追加、削除、修正を加える。

- ◇ ドキュメントの数の計算またはソースデータまたは入力トランザクションについてのその他の管理が欠如し、そのためにデータまたはトランザクションの一部が検出されずに消滅し、または別の記録が追加される結果を生む。

- ◇ データ入力担当者についての記録（たとえば個人の行動記録）がデータ入力の際に修正される。

- ◇ 最後の数分間に（またはその他の特殊なまたは緊急事態下で）到着したデータが処理の前に検証されない。

- ◇ 誤りが検出された記録が、記録全体の検証なしに修正される。

2. 許可されたエンドユーザによる乱用

エンドユーザとはADPシステムを使用する人々である。このシステムは彼等の使用のために設計されているが、彼等が望ましくない目的のためにシステムを乱用することもある。彼等のシステムの使い方がそれらの職務の適正な履行に従っているかどうかを確認することは非常に難しいことが多い。

◇職員が政府の情報を禁止された用途に転用することがある。たとえば個人についての機密データを将来の雇用主、信用調査機関、保険会社、または競争相手に売ることがある。または職員が政府の統計を公表の前に株式市場取引に利用することもある。

◇ファイル中の個人記録を見ることが職務上必要なユーザはファイルの完全なリストを集め、それを禁止された用途に使用することがある。（たとえば職員の住所録を郵送名簿として売る）

◇情報の禁止された改訂を無許可のエンドユーザのために行うことがある。（たとえば個人記録の改変など）

◇許可されたユーザが個人の利益のためにシステムを使用することがある。（たとえばサービスを盗む）

◇監督者が偽りのトランザクションを承認し、入力させることがある。

◇不満を持つかまたは解雇された職員が記録を……恐らくバックアップ記録も破損または使用不能とする方法で……破壊または修正する。

◇許可されたユーザが情報を修正または取得するために賄賂を受け取る。

3. システムへのアクセスの放置

各組織がもしADP区域への立入り、ADPシステムの使用、システムに含まれている情報への接近などをコントロールしそこなえば、不必要なリスクに組織自身がさらされることになるだろう。

◇データまたはプログラムがコンピュータ室またはその他の保管場所から盗まれる。

◇ADP施設が侵入者または職員によって破壊または損傷される。

◇個人がADP区域への立入りを許可される前の十分な識別が行われない。

◇遠隔端末機が無許可の人物による使用から十分に保護されない。

◇無許可のユーザが電話回線および許可を持つユーザのパスワードを使ってシステムに接近する。

◇パスワードが不注意のために無許可の人物に知られる。ユーザが自分のパスワードを便利

の良い場所に書いていたり、パスワードがカードデッキや捨てられた印刷物から判明したり、ユーザがタイプするのを見ていて知られたりする。

◇ユーザがログインした端末機を監視なしで放置し、無許可の人物に使用される。

◇解雇された職員の氏名やパスワードが直ちに許可者名簿や管理リストから削除されないために、それらの者がADP施設に引き続き接近できる。

◇無許可の人物が自分自身の目的のためにシステムに接近する。（たとえばコンピュータサービス、データ、プログラムなどの盗み、データの修正、プログラムの改変、妨害行為、サービスの拒否）

◇システムまたはファイルへの無許可で接近するための、同じユーザまたは端末機からの反復する試みが検出されない。

4. アプリケーションのためのセキュリティの実行が効果的でない

ADPシステムによる正しい処理を確認するための手作業による点検および管理が不十分であるか、または点検を行う担当者が怠慢であれば、多くの脆弱性を生む結果となる。

◇接近許可の基準が明確に規定されていないと、職員等は接近が許可されている情報とそうでない情報とが区別できない。

◇ユーザが与えられた任務の遂行のために必要なプロセスおよびデータのみに接近するように制限するのをセキュリティ担当責任者が怠る。

◇大きな金額の支出、異常な価格の変更、予期されない在庫品の使用などの正しさが点検されない。

◇同じ宛先に対する反復する支払いが、点検が行われなかったために検出されない。

◇機密データがアプリケーションのスタッフ、郵送サービス、または組織内のその他の者によって不注意に取り扱われる。

◇セキュリティ違反を検出するための、処理後の報告分析システム作業が点検されない。

◇訓練生が実際のデータの使用を許可された時に、不注意のためにファイルを破壊または改変してしまう。

◇セキュリティの相違がシステムセキュリティ担当役員または職員の監督者に通告された時に適正な作業が追求されない。そのような事態発生を処理する手続きが存在しない場合もある。

5. A D P 施設内の手続き的誤り

A D P 操作スタッフの誤りおよび意図的な行為の両方とも、不適切な作業手続き、不十分な管理、保管メディアや出力の喪失などの結果をもたらす。

手続きおよびコントロール：

◇ファイルがデータベースの再編成の間、またはディスクスペースのリリースの間に破壊される。

◇オペレータが操作手続きを無視する。たとえばプログラマにコンピュータの操作をさせるなど。

◇ジョブ制御用語のパラメータが誤りやすい。

◇施設の管理者が情報を入手するための操作上の制御を妨害する。

◇停止後の不注意なまたは正しくない再スタートのためトランザクション更新の状態が不明になる。

◇オペレータがC P U コンソールで誤った情報を入力する（制御スイッチが誤った位置にある、端末機ユーザが全面的なアクセスを許可される、オペレータが待ち行列から誤ったジョブをキャンセルするなど）。

◇生産データがオンラインの間にハードウェアの保守作業が行われ、または保守を受けている装置が隔離されていない。

◇オペレータが個人的利益のために禁止された行為をする（競争入札報告の余分のコピーを作る、失業手当小切手のコピーを作る、日計ファイルから記録を削除する）。

◇オペレーションスタッフがコンピュータに妨害行為をする（金属片を端末機に入れるなど）。

◇プログラムの誤っているバージョンが実行される。

◇プログラムが誤ったデータを使用して実行され、または同じトランザクションを使用して2回実行される。

◇オペレータが規定された安全管理をバイパスする（テープリールにリングを書く）。

◇オペレーション要員の監督が作業時間以外のシフトの時に不十分である。

◇手順を誤って学習したため、オペレータがマスターファイルを改変または消去する。

◇コンソールオペレータがセキュリティ記録に行動を記録せずにラベルチェックを無視する。

記憶媒体の取り扱い：

◇重要なテープファイルが書き込み保護をしないで装填される。

◇不注意にまたは故意に誤ったラベルを張った記憶媒体が消去される。それらがバックアップファイルを含む場合は、その消去はファイルが必要とされる時まで気づかれないだろう。

◇記憶媒体の内部ラベルの正確さが検証されない。

◇期限の日付のないまたは誤ったラベル表示のファイルが消去される。

◇カードデッキを落とした時、部分的入力デッキが使用された時、ライトリングがテープの誤った位置に置かれた時、紙テープの装填が不正確な時、または誤ったテープが装填された時などに、データの不正確な処理またはファイルの誤った更新などが発生する。

◇機密データを処理するジョブのために使用されたスクラッチテープが使用後に完全に消去されない。

◇あるジョブステップにおいて次のステップで使用するために書かれた臨時のファイルが、ファイルの保護が不十分であるか、または異常な終り方のために、誤ってリリースまたは改変される。

◇機密情報を含む記憶媒体が、オペレーション要員にその情報内容の性質が伝達されていないために、十分に保護されない。

◇テープ管理手続きが全てのテープの現状について十分に対応していない。

◇非常に機密性の高い情報を含む磁気記憶媒体がリリース前に消磁されない。

◇出力が間違った個人または端末機に送信される。

◇出力または処理後の装置（バースター、デコレータ、またはマルチパートフォームなど）の不適切な操作のために出力が失われる。

◇余分の出力材料（出力データの複製、使用済カーボン紙等）が適切に処分されない。

◇配布のための出力のラベルを持つテープまたはプログラムが誤っているか、または不正な干渉から保護されていない。

6. プログラムエラー

アプリケーションプログラムは完全で正確な、一貫性のあるプログラム設計、正しいプログラミング方法、十分なテスト、点検、そしてドキュメンテーション、および適切な保守手続きを要求し、支持する環境において作成されなければならない。このような環境で作成されたプログラムでも検出できないエラーを含むことがあるが、このような方法で作成されていないプログラムは恐らくエラーが多いことであろう。さらにプログラマは有害な副次的効果を作り出すために、故意にプログラムを修正し、またはそれらが管理しているプログラムを乱用することもある。

◇機密ファイルから記録が削除され、その削除された記録が再構成できるという保証がない。

◇プログラマがそれら自身に関するデータを操作する特殊な方法をプログラムに挿入する

- (たとえば給与支払いプログラマが自分の給与記録を改変する)。
- ◇データがコードと分離されずに記憶され、その結果プログラムの修正が一段と困難になり、修正をより頻繁に行う必要が生じる。
 - ◇プログラムの変更がそのプロダクションランに使用される前に十分にテストされない。
 - ◇プログラムの変更の結果、プログラムモジュール間の予期されない相互反応のために新しいエラーが発生する。
 - ◇プログラム受け入れテストが、ある異常な入力の見合わせの時にのみ発生するエラーを検出できない(特殊な範囲の数値以外は拒否するはずのプログラムが、実際には別の数値も受け入れるなど)。
 - ◇内容の防護を必要とするプログラムがそのように識別されず、保護されない。
 - ◇検証されたプログラムのためのコード、関連出力を含むテストデータ、ドキュメンテーションなどが参照のためにファイル、保管されない。
 - ◇重要なプログラムのためのドキュメンテーションが防護されない。
 - ◇プログラマが変更ログの維持、バックコピーの維持、または記録保管活動の規則化を行っていない。
 - ◇職員が管理しているプログラムを盗み、個人的な利益のためにそれを使用する(商業機関に売却、または別の機関に金銭を要求する)。
 - ◇プログラム設計が貧弱なため、重要なデータが2回初期化される。データ値の変更のためにプログラムを修正する時にエラーが発生し、1か所だけしか変更されない。
 - ◇処理データがテストの際に開示、または破壊される。
 - ◇プログラマがプログラムの変更請求を誤解した時にエラーが発生する。
 - ◇機械コードに直接変更を加えたプログラマが誤りを導入する。
 - ◇プログラムにその所期の目的と両立しない、セキュリティの防護メカニズムを不能化またはバイパスするルーチンが含まれている。たとえば、解雇を予期しているプログラマがプログラムに、もし彼の名前が職員名簿から削除されたら直ちに重要なファイルを削除するようなコードを挿入する。
 - ◇不十分なドキュメンテーションまたはラベリングが、修正されるプログラムの誤ったバージョンを作り出す。

7. オペレーティングシステムの欠陥

設計および実行上のエラー、システム編成および維持上の問題、および故意の侵入などはオペレーティングシステムの修正を招き、アプリケーションシステムに有害な影響を与えることがある。オペレーティングシステムの欠陥は防止や検出が困難であることが多い。

◇ユーザのジョブが割り当てられた記憶領域以外でも読み取り、書き込みができる。

◇2つのジョブが同じファイルについて同時に処理されたため、データが一貫性を欠くことになった。

◇オペレーティングシステムの設計および実行のエラーのために、ユーザが監査コントロールを不能化し、または全てのシステムの情報にアクセスできるようになる。

◇オペレーティングシステムが情報のコピーをオリジナルを保護する場合と同様に完全に保護できない。

◇オペレーティングシステムの無許可の修正のため、データ入力担当者がプログラムに介入できるようになり、その結果システムが停止する。

◇オペレーティングシステムの破損のため、パスワードリストや許可表などの貴重な情報が外部に漏れる。

◇保守要員が保守作業の間にセキュリティコントロール装置をバイパスする。このような時、システムは保守要員またはシステムに接近し、オープニングを発見した者のエラーまたは意図的な行為に対して脆弱性を持つことになる（たとえば、オペレーティングシステムのマイクロコード化されたセクションが干渉され、またはオンラインファイルから機密情報が開示される）。

◇オペレーティングシステムが、出力の複数のコピーがスプールされた記憶装置から作成されたことを記録していない。

◇オペレーティングシステムが破損されていない監査証拠を維持できない。

◇システムの故障の後に再スタートする場合、オペレーティングシステムが以前に使用していた全ての端末機を相変らず同じ個人が保有していることを確認できない。

◇ユーザがモニターまたはスーパーバイザモードに入ることができる。

◇オペレーティングシステムが正常な、または異常なジョブの完了後、ジョブに割り当てられたスクラッチスペースを全部消去しない。

◇ファイルがオープンしないのに読み取りまたは書き込みができる。

8. 通信システムの障害

ある場所から通信回路を経由して別の場所へ送信される情報は、偶発的な事故、または許可されない者による意図的な妨害および改変に対して、脆弱性を持つ。

偶発的障害：

- ◇検出されない通信上のエラーが不正確なまたは改変されたデータを生む。
- ◇情報が誤った端末機に偶発的に送信される。
- ◇通信ノードが処理の予期しない中断の間に、記憶内に保護されないメッセージの断片を残す。
- ◇通信プロトコルがメッセージの送信者または受信者を積極的に識別しない。

意図的な行動

- ◇通信回線が許可のない者によってモニターされる。
- ◇データまたはプログラムが遠隔ジョブ入力端末機から電話回線を通じて盗まれる。
- ◇ネットワーク交換コンピュータ中のプログラムがセキュリティ破壊のために改変される。
- ◇回線のタッピングをする者によってデータが故意に改変される（高度な知識を必要とするが、財政的データについては可能性がある）。
- ◇無許可のユーザがコンピュータ通信施設を、許可されたユーザがそれから切り離された時に「占拠」する。多くのシステムはこの変化を検出できない。現在入手可能である通信機器および多くの通信プロトコルにおいては特にそうである。
- ◇暗号化が実施されている時には、キーが盗まれる。
- ◇端末機ユーザが機密データを提供するようにだまされる。
- ◇偽りのメッセージがシステムに挿入される。
- ◇本当のメッセージがシステムから削除される。
- ◇メッセージがシステムに記録され、リプレイされる（「\$ 100 を預金せよ」のメッセージなど）。

引用および参考文献

1. Computer Security Guidelines for Implementing the Privacy Act of 1974, National Bureau of Standards(U. S.), Federal Information Processing Standards Publication (F I P S P U B) 41, National Technical Information Service, Springfield, V A(1975).
2. Courtney, Robert H., Jr. and Orceyre, Michael J., Considerations in the Selection of Security Measures. National Bureau of Standards(U. S.) Special Publication 500-33, Government Printing Office, Washington, D C(1978).
3. Data Security Controls and Procedures — A Philosophy for DP Installations, G320-5649-00, IBM Corporation, White Plains, N Y(1976).
4. Disaster Preparedness, Office of Emergency Preparedness Report to Congress, Stock Number 4102-0006, Government Printing Office, Washington, D C(1972).
5. Glossary for Computer Systems Security, National Bureau of Standards (U. S.) Federal Information Processing Standards Publication (F I P S P U B) 39, National Technical Information Service, Springfield, V A(1976).
6. Guidelines for A D P Physical Security and Risk Management, National Bureau of Standards (U. S.), Federal Information Processing Standards Publication (F I P S P U B) 31, National Technical Information Service, Springfield, V A(1974).
7. Hoyt, Douglas B., Ed., Computer Security Handbook, McMillan Information, New York(1973).
8. Martin, James, Security, Accuracy and Privacy in Computer Systems, Prentice-Hall, Inc., Englewood Cliffs, N J (1973).
9. Nielson, N. R., Ruder, B., Madden, J.D. and Wong, P.J., Computer System Integrity, S R I International, Menlo Park, C A (1978).
10. Parker, Donn B., Crime by Computer, Charles Scribner's Sons, New York (1976).
11. Wong, k.k., Computer Security Risk Analysis and Control, Hayden Book Company Inc., Rochelle Park, N J (1977).

付属資料 2
外国文献抄録

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ことも非常に重要である。

そこで、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 (IEEE) の情報部作成になる INSPEC (Information Services for Physics, Electronics, and 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選び、入手した。それぞれの論文・論説に関しては、『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月において、全体的な特徴を示すほか、とくに5編の論文が抄訳されていた。ここでは、これら17編の論文・論説の概要を採録することも重要と考え、再編することにした。

「保険とフィデリティボンド」

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

これは、アメリカの2人の弁護士により提出された論文の採録である。彼らの仕事先であるアメリカの銀行では、不正行為がはびこっている。彼らの法律事務所では、身元信用保険・関連クレイムで約\$30,000,000にのぼる金額の回復に関与したことがあるというほどである。

本論文では、FBIの指摘に見る損失特徴から論じている。損失状況については、後述の Davies 著 "Insuring the Risks Of The Changing Technology : The State Of The Insurance Art" (「テクノロジーの変化のもたらすリスクの付保」)においても示されているが、コンピュータ関連の損失金額は非常に大である。それゆえ、コンピュータに起因する損失に備え保険がどうしても考慮されることになる。そこでまず、身元信用保険の何たるかを示している。簡単に定義すれば、身元信用保険とは、従業員の不誠実な行為から被保険者を保護する保険である。

一般にアメリカの銀行向けの身元信用保険では、バンカーズ・ブランケット・ボンドと言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、それによりどんな損失がカバーされ、どんな損失がカバーされないかを論じている。

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も言及している。

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1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。(参考：なお、日本では、経営風土の違いにより、アメリカの企業ほど、身元信用保険は利用されていない。)

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

著者はウェスティングハウス ハンフォード社の上級サイエンティストである。この論文の中で、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。コンピュータセキュリティマネジャーは、重要な情報およびその情報をコンピュータにより処理するプログラムを保護する必要を訴える必要がある。ここで保護されるべきデータとは、それが改変されたり、破壊されたり、漏洩したりすれば、会社に損失をもたらすものである。そこで、たとえば権限のない者のアクセスであるとか、重要なデータの不適切な使用といったコンピュータシステムに特有な脅威について、保護手段もリスクに比べて多く費消することなく、着手しなければならない。その際、そうしたリスクを推定する手続きも利用できる。人々の行動も、火災とか洪水といった災害よりも大なる脅威を提起するようになるとして、共通の脅威に加えて、とりわけ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）に視点がおいている。それゆえ、権限のない人を締め出し、権限のある人を入れ、本質的に重要な業務のため必要なもののバックアップコピーを保持することにより、人に有害なことをさせないようにする予防的な措置が強調されるのである。とくに本論文では、コンピュータシステムにとっての脅威とリスク決定の諸方法、リスクを軽減させるセーフガードが検討されている。

とくに、リスク推定の部分では、FIPS PUB 65、W. A. J. Bound and D.R. Ruth の展開（『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59年12月において紹介されている）、さらにLAVAのフレームワーク13についても指摘している。

「テクノロジーの変化のもたらすリスクの付保」

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

本論文では、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している。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月発生のケーブル火災にも言及）として事例を紹介している。つぎに、たとえば、U S A 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、コンピュータ支援無しの場合は \$ 25,000である（FBI）といったように、コンピュータ犯罪に論及している。また、A T M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する。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、顧客が望む免責無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らうし、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、わわれは出発すべきであるとしている。

ところで、たいていの企業では、コンピュータ関係の責任（D P M）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も言及している。

「リヴァモア・リスク分析方法論」

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

この論文は、1985年の始めローレンス・リヴァモア国立研究所 (Lawrence Livermore National Laboratory = LLNL) が、合衆国空軍ロジスティックスコマンド (AFSC) 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。このリスク分析方法論において、リスクは対象物の価値 (資産) に脅威が具体化することにより生じるものであるとし、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という問題意識のもとに、以下のことをしなければならないとしている :

- (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。

現代の多数の情報システムは、規模が大きく、複雑なものとなっており、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。そこで、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得よう、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ために、LRAMアプローチの手続き上の順序を示している。

LRAMの主たるフェーズは、「計画化」、「リスク分析」、「マネジメントディシジョンサポート」である。そしてこれら3つのフェーズは、さらに

- 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)、

という6つのステージからなっている。

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。IGのステージでは、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 (たとえば、再調達コスト) と非貨幣的な値の属性双方に関する予備的な決定をする。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。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。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。RAAのステージは、当初、容認不能であった特定のリスクエレメント (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。

つぎにくる「マネジメントディシジョンサポート」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。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。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。

「コンピュータ・システム故障に対する社会的脆弱性」

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

本論文の著者であるジョージワシントン大学(GWU)のHoffmanはコンピュータセキュリティとリスク分析に関するパイオニア的研究で知られている教授である。また Moranは GWUの博士過程の院生で、リサーチアシスタントである。

本論文では、コンピュータシステムの脆弱性、コンピュータセキュリティリスク分析過程を考察しているが、とくに脆弱性について、興味深い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 (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。

とくに本論文の構成は、

コンピュータシステムの脆弱性と社会の脆弱性；

社会の脆弱性の歴史的経緯；脆弱性問題への取り組み方；

脆弱性と回復力；

社会的なリスク分析；

コンピュータシステムの脆弱性の軽減；

インタディシプリナリな見通し、

からなっている。

これは「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。どんなセキュリティの水準が必要か、この点の評価にも困難さが付きまとう。これはつぎの3要因によっている：脅威のタイプとその発生確率；リスクにさらされている資産の価値；結果としての損失の影響、である。

ところで、脅威の主たる源泉は「人」である。今日のタフな事業環境のもとでは、役員へのプレッシャーが不正の誘惑に駆られやすいという。多く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。ある組織では、契約先の清掃会社に競争相手のゴミ入れからタイプライターやプリンタリボンを収集してもらうための支払いをした。昔と違い、現在のプリンタは使い捨てのカートリッジを用いており、一度使えば、廃棄されるからである。

別の例では、テークオーバービッドをかわそうとしている会社があった。役員用の会議室でマイクロホン／トランスミッタバグが発見された。誰がそれを置いたか疑惑が残された。自分の給料小切手 200枚を入手したある女性の場合、コンピュータのアウトプットプリンタにアクセスし、彼女の小切手に印字されるまで待ち、プリンターのリピートボタン押え続けた。しかし1つの銀行勘定に全部を入れたために、捕えられたのであった。

こうした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無いより事態を悪化させ得ることを認識することである。

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

コンピュータ犯罪に対応するための新しい方法として保険を論じている。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。クリミナルコードなり裁判所は、犯罪行為について有罪を宣告したり、犯罪行為を思い止どまらせることにより、社会の安定性を維持しようとする伝統的な機能を有しているが、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。多くの国では、コンピュータ犯罪が由々しい問題であるという事実を認識してきている。しかしながらコンピュータテクノロジーとの付き合いはおよそ30年程であるが、大部分の国ではクリミナルコードの中にコンピュータ犯罪を定義することによっても、それに対抗し得ていない。だが、デンマークでは、1985年7月1日に、そのための法律を導入した。そこではコンピュータ犯罪を特有の用語で定義しており、正しい方向への動きとしている。

確かに、公表されているコンピュータ犯罪のケースは、氷山の一角に過ぎない。ジュネーヴ・アソシエーション (the Internationale pur l'Etude de l'Economie de l'Assurance in Geneva) による包括的な研究のほか、ヨーロッパ、アメリカでの調査研究からコンピュータ犯罪による損害推定について数字をあげている。さらに、保険されるリスク、保険会社のサービス、保険保護の範囲（とく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、2等）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。

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

この論文は、大規模なコンピュータシステムに関連したリスク評価のため、ベイジアン統計理論に基づき展開した論文である。まず、リスク評価に関して一般的なリスク分析のための議論を展開した後、ベイジアン確率リスク評価を数学的なモデルを用いて展開し、最後のこの方法を用いた実施例を簡潔に紹介している。

自動環境下でのリスクの理解には、システムの主たる要素間の相互関係が、脆弱性と脅威と共に、まず描写されねばならないとして、資源共有のシステムに影響を与える5つの脆弱性が示されている。物理的環境、ハードウェア、システムソフトウェア、通信回線、組織の人ともろもろの手続きである。これらの理解のもとでリスクが評価されるが、それは2つの目的のために行われる。まず第1に、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を得て、有害な事象の発生確率を低めたり、継起的な環境を軽減するようにする。第2に、選択的なリスクマネジメント戦略の比較評価のため、統計的な情報が必要であるという点である。

ところで、現行のリスク評価法では、定性的なものと、確率論的なものの2つある。ベイジアン統計論による本論文の確率論的リスク評価法は、ある範囲内の安全性と復旧費用とを扱うことができる。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し（点評価では、一度に1個の脅威／脆弱性のペアしか扱えないが）、管理者に意志決定のツールを提供することが可能になるとしている。

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

本論文では、時には相矛盾するセキュリティ要求に応えるため、リスクマネジメントにおけるリスク分析の必要性の認識から、構造的な手法を用いてえられた分析結果を、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合している。

コンピュータセキュリティは、信頼性（R）、完全性（I）、脆弱性（V）、機密性（C）、プライバシー（P）といった属性を有し、それも

R I V C P

という形で配列されている。ところでノランのステージモデルは、コンピュータ予算の変化によってしめされた状態を因子化することを基礎としているが、「開始期」、「拡張期」、「統制期」、「統合期」、「データ管理期」、「成熟期」という6つのステージとこうしたセキュリティ属性との関係が示されている。たとえば、信頼性は「開始期」の前提条件で、開始期にあるセキュリティは完全性である。それはまた「拡張期」へのインプットになる。無節操なコンピュータの利用は脆弱性を高め、そこで、資源に制約が生ずるまえに制御が必要となり「統制期」でのアウトプットは機密性となる。そして、「統合期」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」でのデータ管理システムにより確保されることになる。そこでのアウトプットはセキュリティエンジニアリングで「成熟期」へのインプットとなるのである。

本論文では、リスクマネジメントでの問題点に焦点を当て、コンピュータセキュリティの基本概念である「属性」とその相互関係が分析され、コンピュータシステムの進化についてのステージモデルと結び付けられている。

Palmer, Ian, "Security audit & risk management", System Security: Online Publications, Pinner, UK, 1985, pp.197-207.

この論稿では、リスク分析の目的を、リスクのインパクトと保護手段のコストとの間の経済的なバランスをADPマネジメントが決定するのに資することにある、としている。まず、現存するリスクを指摘し、したがって必要とされる保護手段を選択するのに役立つ。そうした分析は、組織におけるADPについての現状のセキュリティの姿勢を示すことになるし、適格で対費用効果の点ですぐれたセーフガードの選択に必要な基本的な事実が集められることになる。これが第1のリスク分析のベネフィットである。第2のベネフィットとして、管理者層から現場に至るまで、すべての組織のレベルにおいて、セキュリティについての知覚が増加する点を挙げている。

注意すべきは、リスク分析は1回行えばそれで済むという性質の仕事ではないことである。リスク分析は、活動や施設設備の変化に遅れず平行して行くため、定期的に遂行されねばならないのである。したがってリスク分析は、あらゆるシステム導入のデザインの段階で行われるべきである。

本論文では、リスク分析の方法論、それによる資産の確認、リスクの計算、対応策の評価、結論という順序で考察が進められている。コンピュータ設置にたい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は、ドルとポンドの違いはあるが、FIPS PUB 65において展開されたフォーミュラと同じものを用いている。

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。

「テクノロジー支援によるリスクマネジメント」

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.

本論文は、序、リスクマネジメント（バックグラウンド情報）、テクノロジー支援によるリスクマネジメント、ディザスターマネジメント（バックグラウンド情報）、テクノロジー支援によるディザスターマネジメント、要約・勧告という構成になっている。

本論文の目的は、現在、ポピュラー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遂げたのかどうかを評価することである。リスクマネジメントコントロールを情報環境のなかでより良いセキュリティを得る出発点とし、ディザスターコントロールは通常業務やシステム機能の範囲内に組み込まれるべきとしている。その際、資産のフェーズ、データのフェーズ、コストベネフィットのフェーズという3つのフェーズが勘案されることになる。とくにテクノロジー支援によるリスクマネジメントの部分では、定量的・定性的な方法が検討素材とされ、統計的なベイジアン意志決定支援システム（B D S S）について考察している。また、ディザスターマネジメント（バックグラウンド情報）では、フェーズ2が主たる要素となるとしてその中身を示している。さらに、テクノロジーによるディザスターマネジメントの部分では、Disaster Plan 80ならびにRecovery/1の特徴が示されている。

リスクが何であれ、自分には関係ないという「他人事」症候群が根強く存在している現状では、法律でリスクマネジメント等が命令されないようであれば、定量的なリスク分析の実践などなされないし、最低のセーフガードが見られるくらいである。しかし、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かについては、回答はイエスであり、B D S Sおよび Recovery/1 を挙げている。

Saxby, Stephen, "COMPUTERS AND THE LAW: OLD STATUTES FOR NEW PROBLEMS?", SECURICOM 1 986, 4th Worldwide Congress on Computer and Communications, Security and Protection, pp. 133-53, 1986, March 4-6, 1986, Paris, France.

情報化社会は、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。情報技術に関する法律(information technology law)は、もはや理論的概念の段階での主題ではない。

コンピュータ産業のドラマティ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？；

従業員による企業機密の窃盗からどのようにすれば予防され得るのか？；

従業員が自分の時間中に開発するプログラムに対して、彼ら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？

会社があなたの作った作品のコピーを製品として得るのをどうやって止めさせるのか？

本論文は、ビジネスユーザに関するこうした問題等々に論及している。とりわけ、コンピュータ契約によりどのリスクが移転され得るのかということは、リスクマネジメントについての中心的な課題である。また、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得るかについても言及している。

「LAVA：リスク分析のための概念的フレームワーク」

Smith, S. T., Lim, J. J., Phillips, 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.

これは、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。その要約によれば、リスク分析は、資産の全体集合、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明確な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、イヴェントツリー、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・イヴェ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ヴ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、結果 (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 (consequence) 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り、(金銭的・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/結果という4重の組についての損失イクスポジューを表す。現在のところ、LAVAは、様々に組み込まれたシステムにおけるリスクマネジメント、サヴァイヴァビリティシステム、兵器システムセキュリティ等、大掛かりな人的構成要素を含むサブジェクトシステムモデル化のために適用されている。

「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」

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.

この論文の実際の内容は (Smith and Lim, "An Automated Procedure for Performing Computer Security Risk Analysis" 「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ィティドプロシージャ」後掲) をより明確に論じたものと言える。後掲する同論文により、本論文の基盤が理解できるものと思われる。

本論文の内容は、ロス・アラモス国立研究所で、リスク分析を行うため開発され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ならびに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。

「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ィドプロシージャ」

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.

コンピュータは、目に見えないところで原子力関係事業のセーフガードの領域でのバックボーンになっている。コンピュータはプラントを運転する場合にモニターなり制御を行っているほか、マテリアルアカウンティングシステムをもサポートしている。しかしセーフガードに関心が向けられるもののコンピュータセキュリティ問題の重要性に注意がさほど払われていない。コンピュータセキュリティの有効性を評価するための簡単な分析用具がないからである。そこで、脆弱性・リスク分析の通常のアプローチたる伝統的なリスク分析のアプローチとは異なった自動化された方法を開発した。この方法は、環境、直接人間的、間接人間的という3つの脅威の、コンピュータ施設、ハードウェア、ソフトウェア、関連ドキュメントという4つの（保護されるべき）ターゲットへのインパクトを評価するのである。こうした状況下で、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システムは、16ビットの携帯可能なマイクロコンピュータでも容易に使えるものとなっており、セキュリティ手段の適確性についての意思決定がなされるべく、相互連関を把握するクエスチョネアを用いて展開されるようにモデル化されている。そして、イベントツリー集合が、当該クエスチョネアをリスクアセスメントに結びつけている。そして、定性的なスコアが、ターゲットの脆弱性に関して得られ、定性的なインパクトの尺度が脅威と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。そしてつぎに、正確で有意意味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ことになる。

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

本論文では、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、製造業者の製品についての顧客の満足はいくらぐらいなのか？ 会社の注文処理システムが勝手に変更され、3週間の輸送上の遅れがでたら製品の価値にどのような影響があるのか？ コンピュータ施設のリスク分析を行うセキュリティ専門担当者は日常そうした微妙な問題に直面しているわけである。それも、コンピュータなりコミュニケーションネットワークに起こる被害は、システム自体のコスト以上かもしれない。

しかしリスク分析はこれまで起こらなかった事件のインパクトを推定するといったことなどから、多くの企業ではニーズに合致しないという理由で、リスク分析には懐疑的である。組織が必要としているのはコンピュータとネットワークセキュリティへの脅威を予測し得る使い易い方法である。しかしながらリスク評価の技法は時間費消的で、解答より多くの問題を提起し、お金のかかるものである。だが、ファジィメトリックスなりベイジアン分析のような難解な統計的技法がデータセンタ等への脅威の評価に必要でないといった認識は、リスク評価法を開発するコンサルタントや売り手に考え方に急速な変化を促した。何社かはリスク分析に常識的なアプローチを入れたマイクロコンピュータ向けのソフトウェアパッケージを売りに出した。そのパッケージはセキュリティ脅威のインフォーマルな評価を行い、一段と手の込んだチェックリストを提供するようになったのである。そうしたプログラムには、セキュリティの専門家との何百回にも及ぶインタビューに基づき開発されたRiskpac 等々が紹介されている。なお、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, RTS Software 等が、また定量的リスク分析に関しては、Basic DataSyst./RiskAnalysis Machine, Chesapeake Computer Grp./Risk-A, The Spence Grp./Riskcals等が示されている。

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

本論文では、さまざまなコンピュータ犯罪のパターンを確定するため、種々の内外の情報源から、イギリスにおいて実施したコンピュータフラウドの95ケース、その他のコンピュータ犯罪の60ケース以上に基いて分析している。

まず、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り、それによりセキュリティマネジャーは損失規模、過去において犯行に及んだ人、その手口等についてなんらかのアイディアを提示してくれることになる。そして、パターン認識、リスク分析とビジネスインパクトレビュー、コントロールと発見、将来の含意、フラウドコントロールについて展開している。

とくに、コンピュータフラウドについては、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を犯す傾向がある。その他のコンピュータ犯罪については、コンピュータ施設の放火、サボタージュ、情報・メディアの窃盗、設備の窃盗、システム侵入、ロジック爆弾等の状況を示している。またリスク分析に関しては、とくに事業中断損失の原因に言及している。コントロールと発見の部分では、発生頻度の減少に論及し、直接的な対応策に実施には、そのコストと直接的・間接的損失とのバランスが取られるべきとしている。また将来、種々のコンピュータが個々の部門に導入されるがため、その利用上の注意が不可欠となる。とりわけスタッフがセキュリティへの知覚を増すため、セキュリティについての適切な訓練が必要となる。金融機関では電子資金取引（EFT）システムにおけるフラウドの危険に気付いているが、より良いプロテクションが求められよう。なお、フラウドコントロールの部分では、予防／軽減、発見、対応についての戦略が論じられているが、その中でコンピュータ犯罪保険も指摘されている。

付属資料 3

セキュリティ対策水準の時系列分析

セキュリティ対策水準の時系列分析

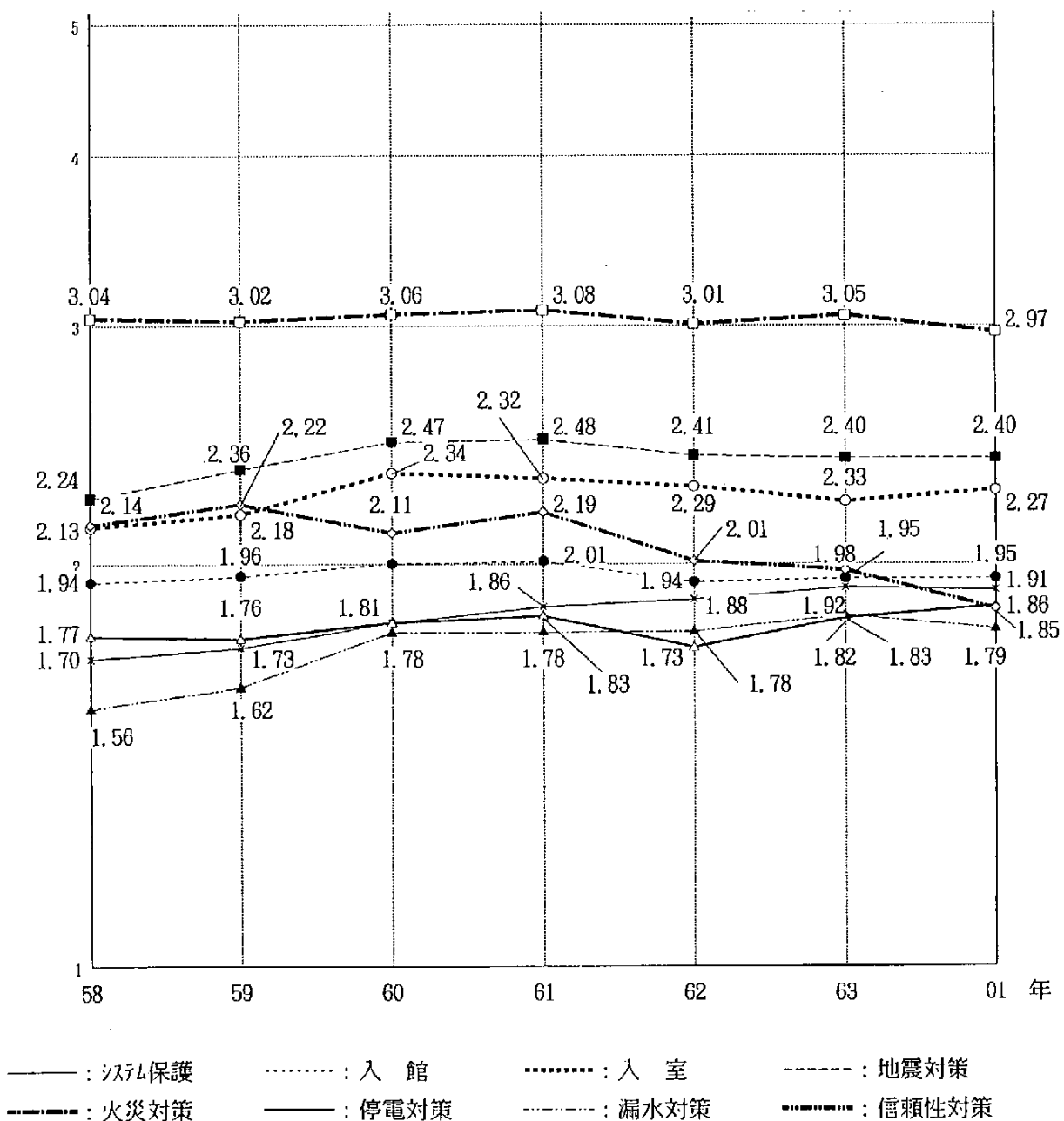
本調査は、システム保護、入館、入室、地震対策、火災対策、停電対策、漏水対策、信頼性対策の8項目について、それぞれ5段階方式により調査した結果を、昭和58年より平成元年までの7年間にわたってとらえ、その傾向を分析したものである。

全産業平均

全体的な傾向としては、わずかながら向上しているといえるが、7年間における変化は非常に小さい。その中でも、「漏水対策」が向上していることと、「信頼性対策」が低下していることが多少目につく程度である。後者については、中・小規模のコンピュータが増加したことによる影響と見ることができよう。

「火災対策」だけが3レベルを維持しているが、従来と比較して向上はしていない。また、火災対策については、消防法や建築基準法などによる規制があるために一定の水準を保っているものと思われる。

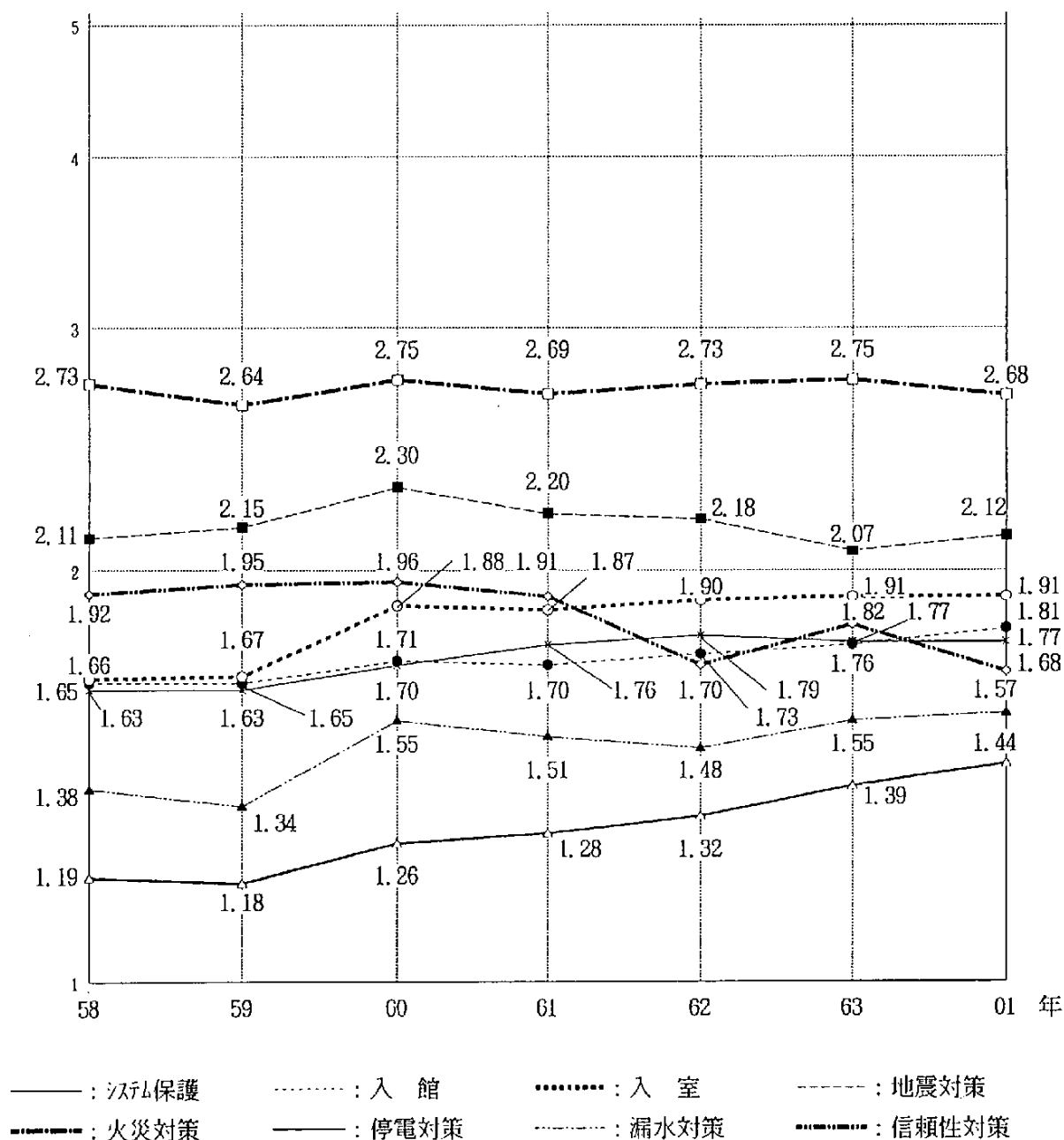
つぎに高いのは「地震対策」であるが、それでも2レベルと3レベルの中間位でしかない。他に2レベルを超えているものには、「入室」がある。



第2次産業計

最も高いのは「火災対策」であるが、それでも3のレベルに到達していない。そして、全産業の傾向と同様に、「信頼性対策」だけが低下傾向にある。

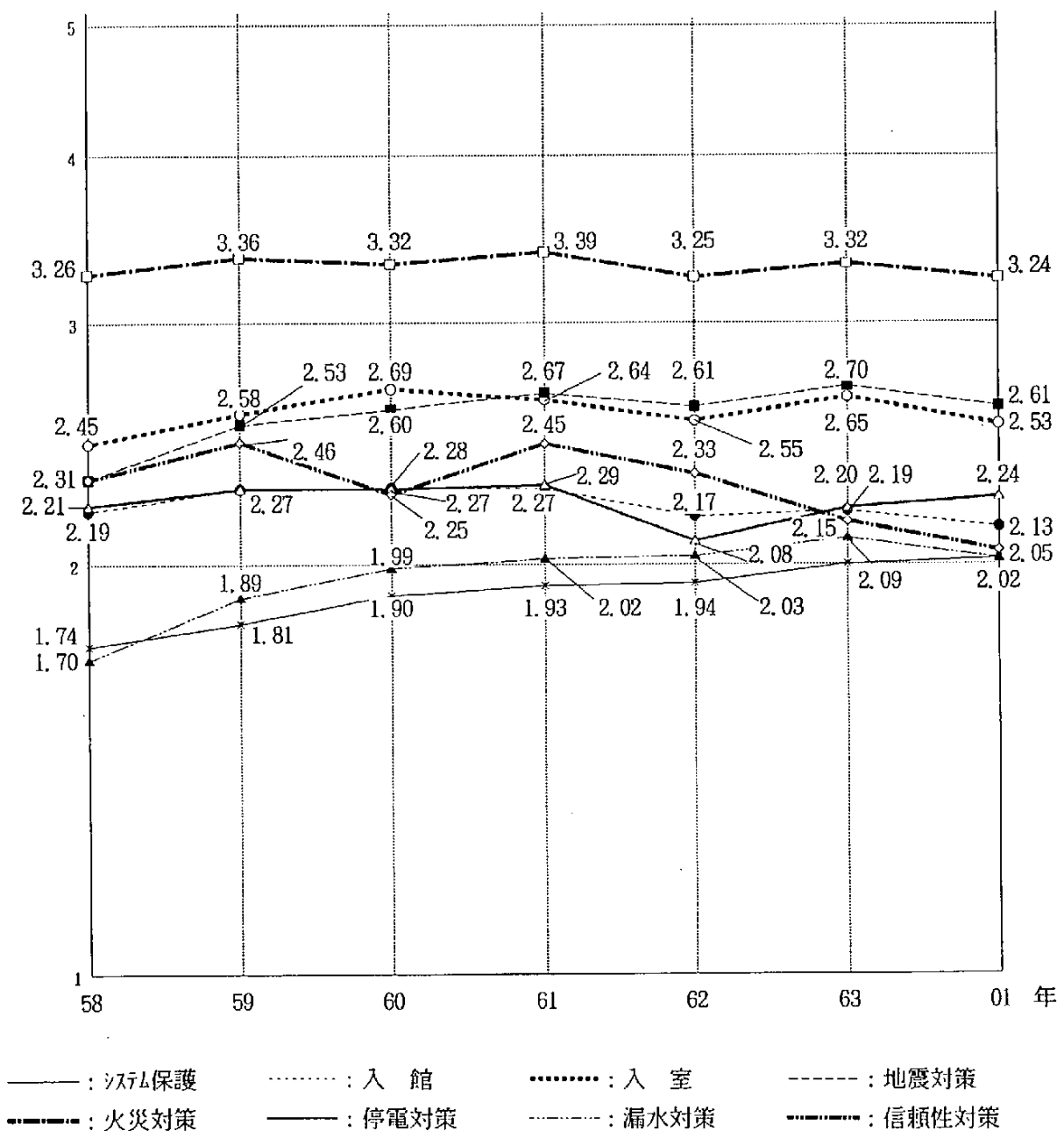
最も低いのは「停電対策」であるが、しかし、これは顕著に向上しているといえる。また、「漏水対策」についても同様のことがいえる。



第3次産業計

8項目ともに2レベル以上であり、全ての項目で全産業平均を上回っている。また、「システム保護」、「地震対策」、「漏水対策」がわずかに向上気味であり、逆に「信頼性対策」が低下気味である。

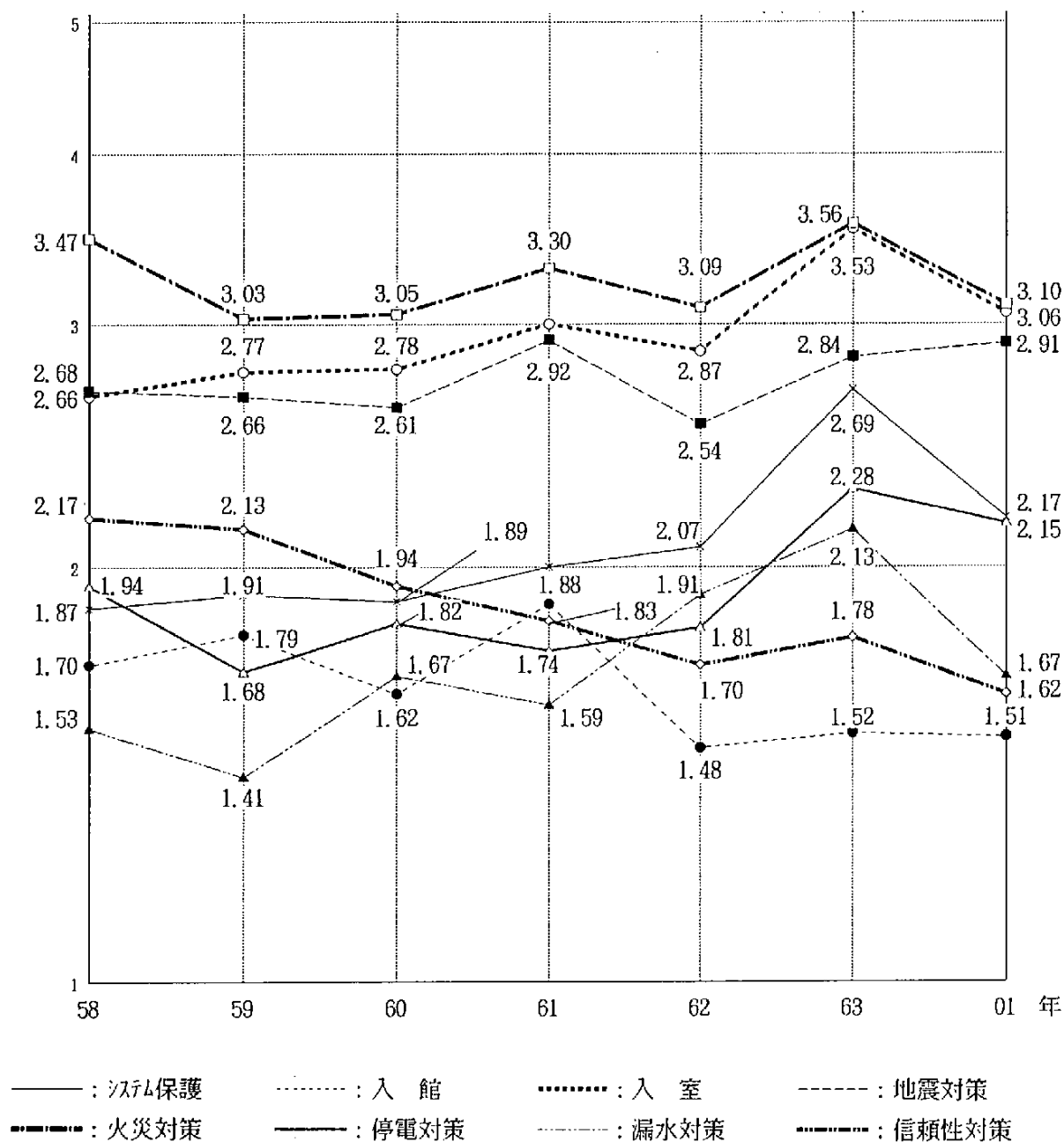
いずれにしても、全ての項目が2レベル以上ということは、情報化が第3次産業で最も進んでいることを物語っているといえる。



公務計

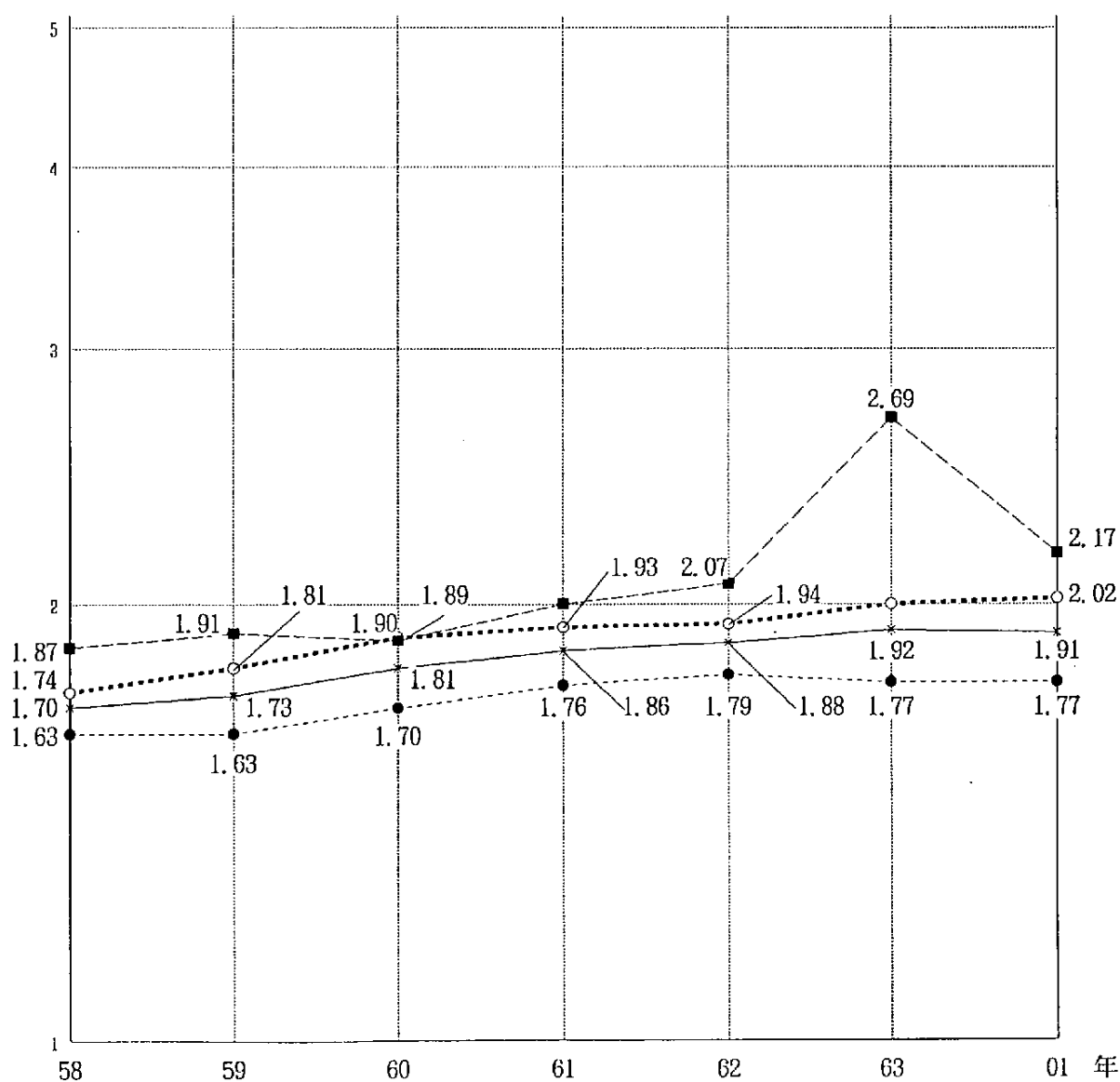
公務は、各年ごとの回答のバラツキが大きいが、これは回答組織体の変動によるものと思われる。

内容的には、3レベルに到達しているのが「火災対策」と「入室」の2項目あるのが目立っている。そして、とくに「入室」が高くて「入館」が低いのも1つの特徴となっている。これは、官庁の場合、入館は制限できないため、それに反比例して入室管理が厳しくなっているといえる。



システム保護

全体的な傾向としては、わずかながら向上しているといえる。そして、第3次産業と公務が全産業平均を上回っている。とくに、63年の公務だけが突出しているが、これは、この年の公務の回答組織体に偏りがあったものと思われる。



——：全産業平均

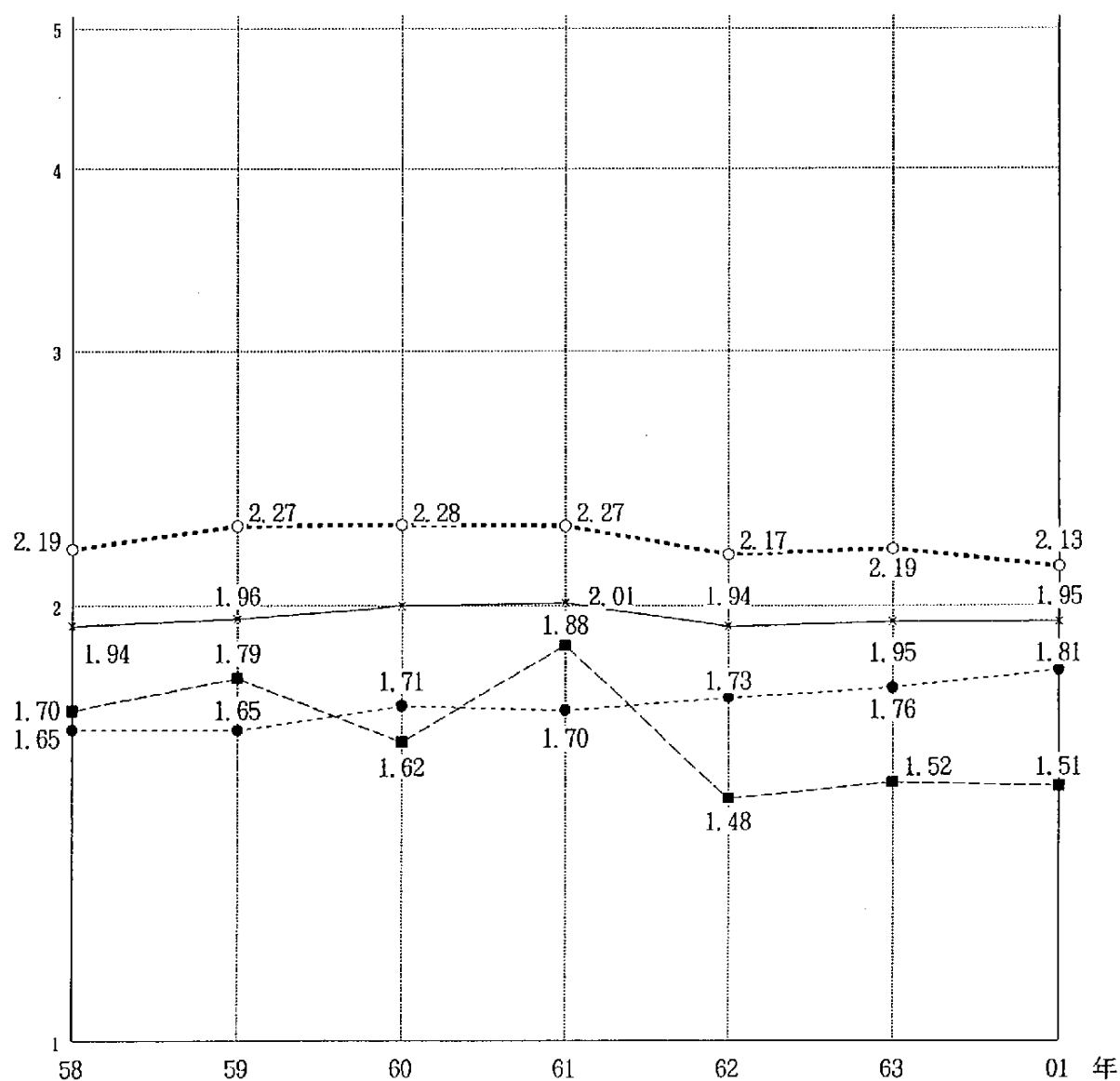
.....：第2次産業計

.....：第3次産業計

----：公務計

入 館

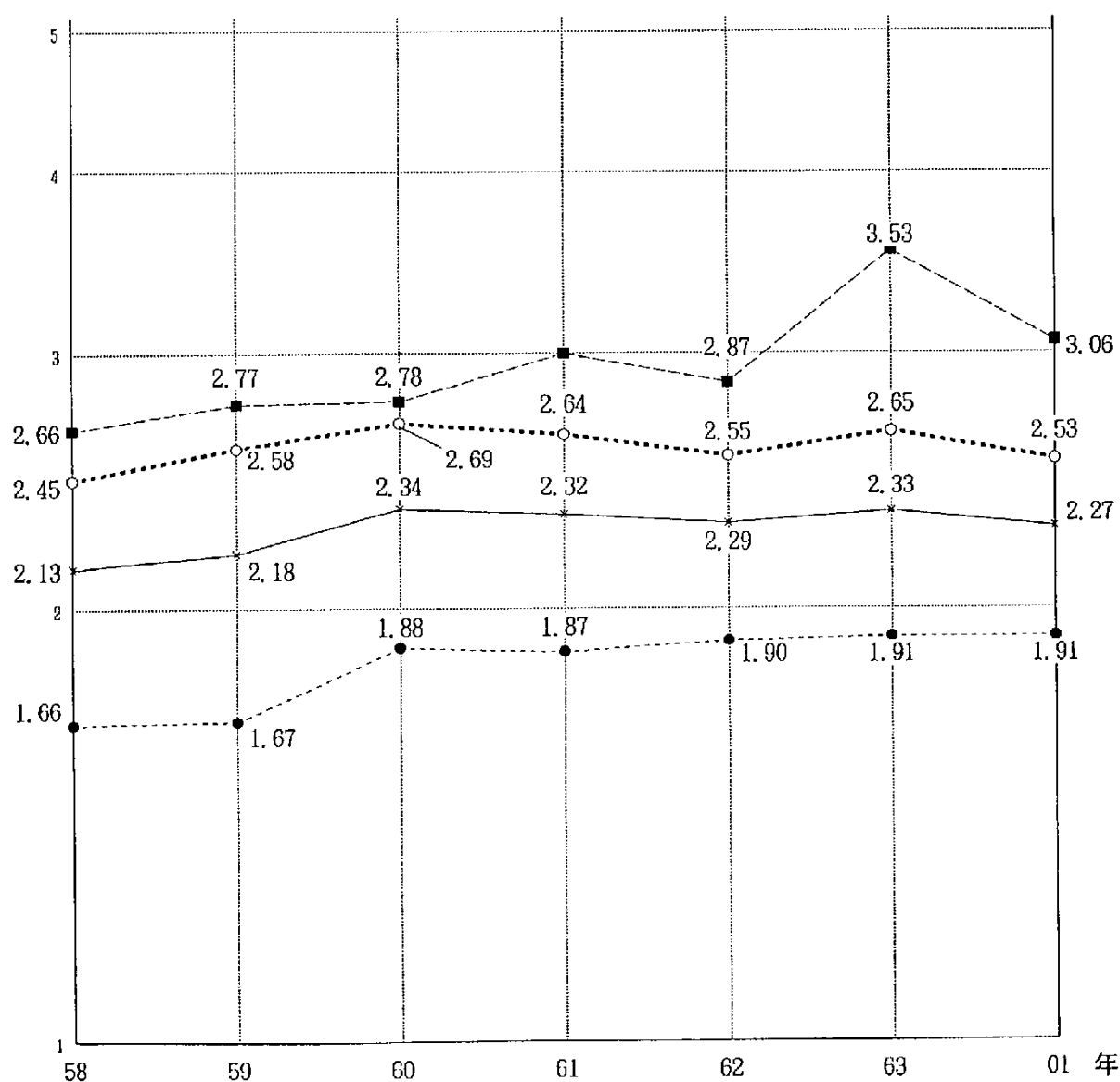
第3次産業のみが全産業平均を上回り、かつ、2レベルに到達している。とくに公務が低い
が、前述のとおり官庁では入館規制が難しいためであろうと思われる。また、全体的な傾向は、
横ばいということができる。



——：全産業平均 ：第2次産業計 ：第3次産業計 ----：公務計

入 室

・全産業平均が2レベルを超えているが、第2次産業だけが1レベルである。全体的な傾向としては、60年に若干の底上げがされ、それ以降は横ばいである。その中で、公務のみが向上傾向にあるといえる（63年の突出をのぞいて）が、これは、先にも述べたとおり、入館との関連が深いものと思われる。また、この入室は、最高と最低とが1ポイント以上差があるという点でも特徴がある。



——：全産業平均

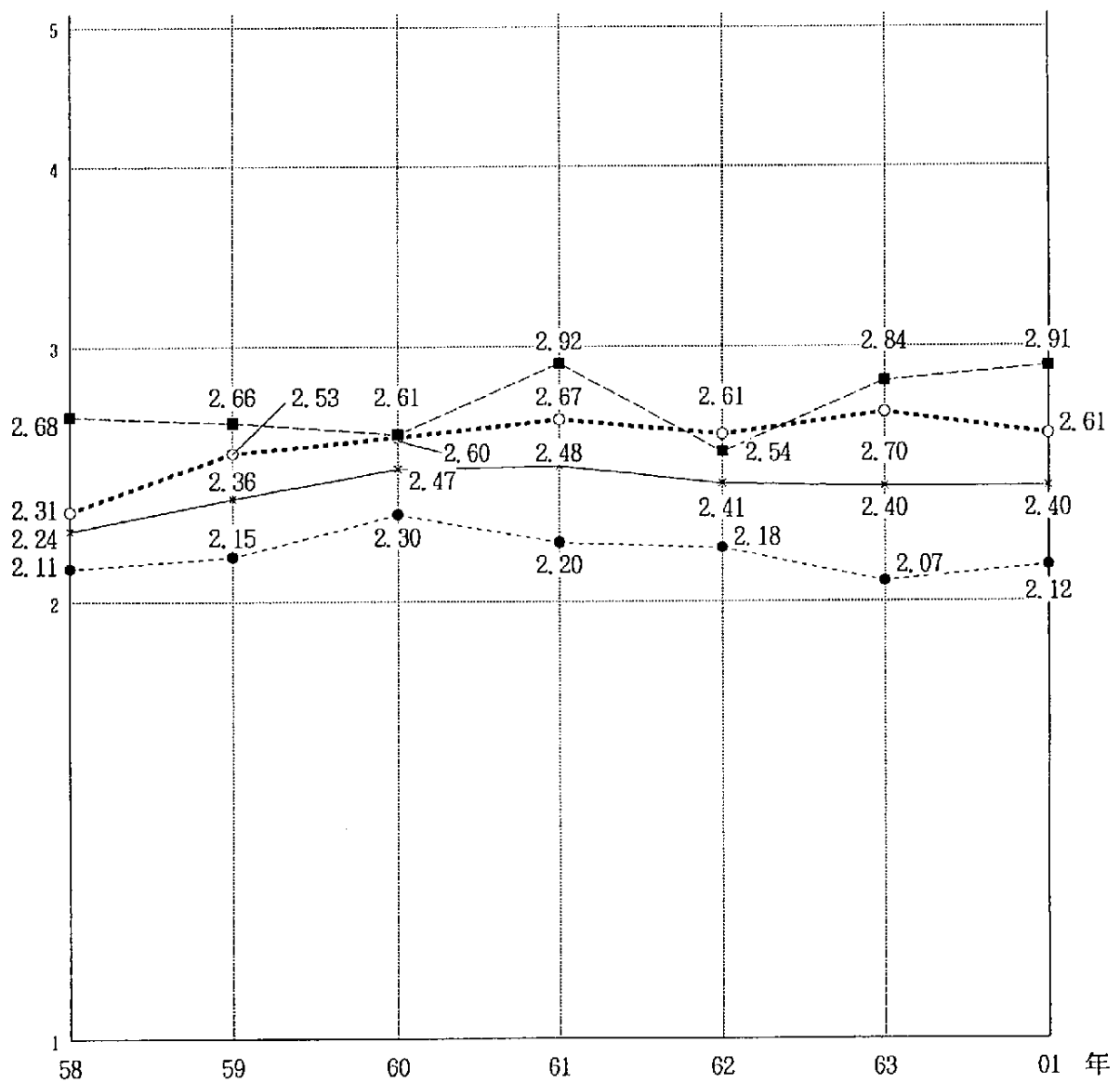
.....：第2次産業計

.....：第3次産業計

----：公務計

地震対策

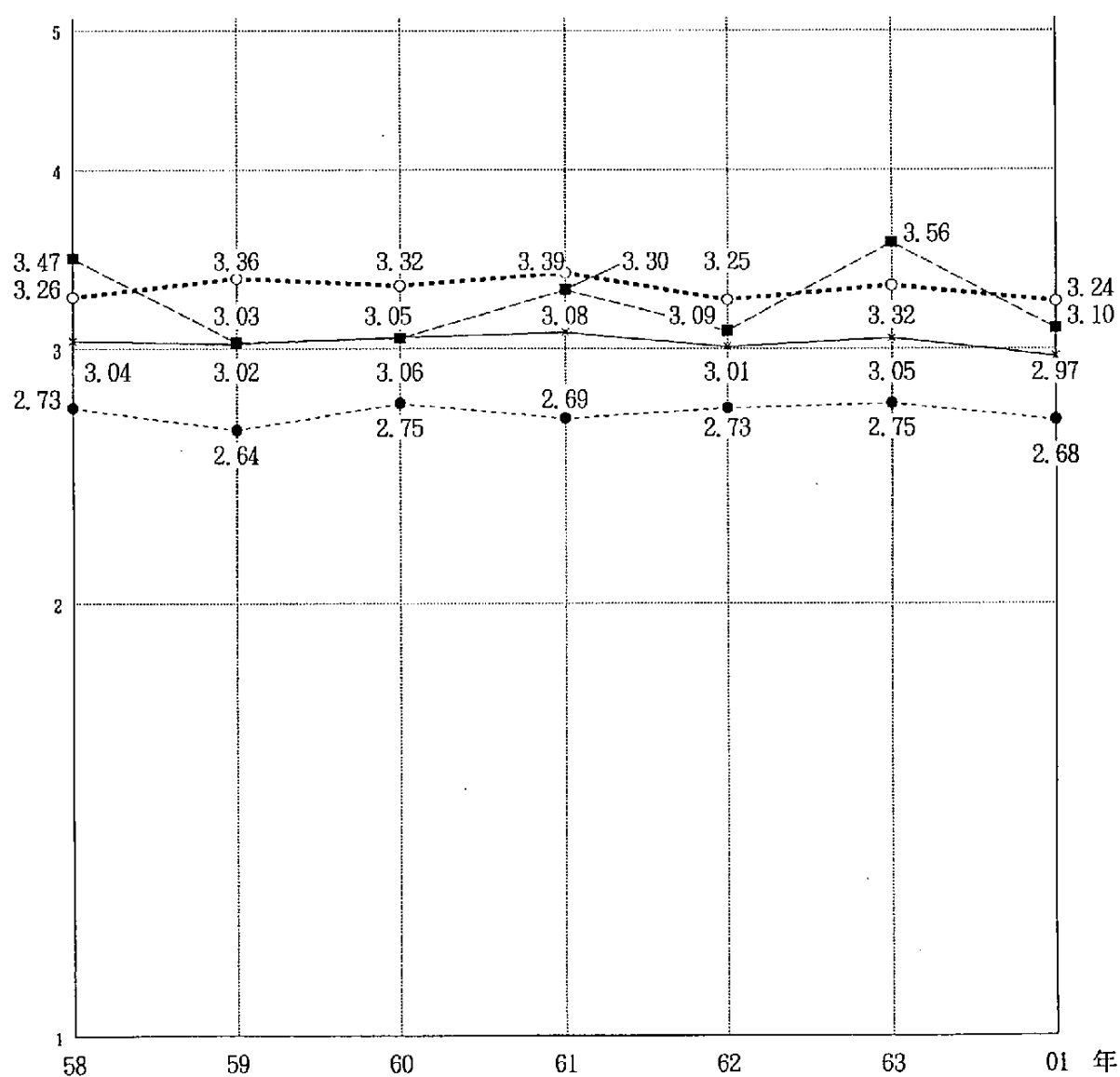
全てが2レベルに納まっている。全産業平均が、2レベルと3レベルの中間程度にあり、全体的には横ばい傾向であるが、第3次産業と公務はわずかに向上傾向にある。



——：全産業平均 ：第2次産業計 ：第3次産業計 ----：公務計

火災対策

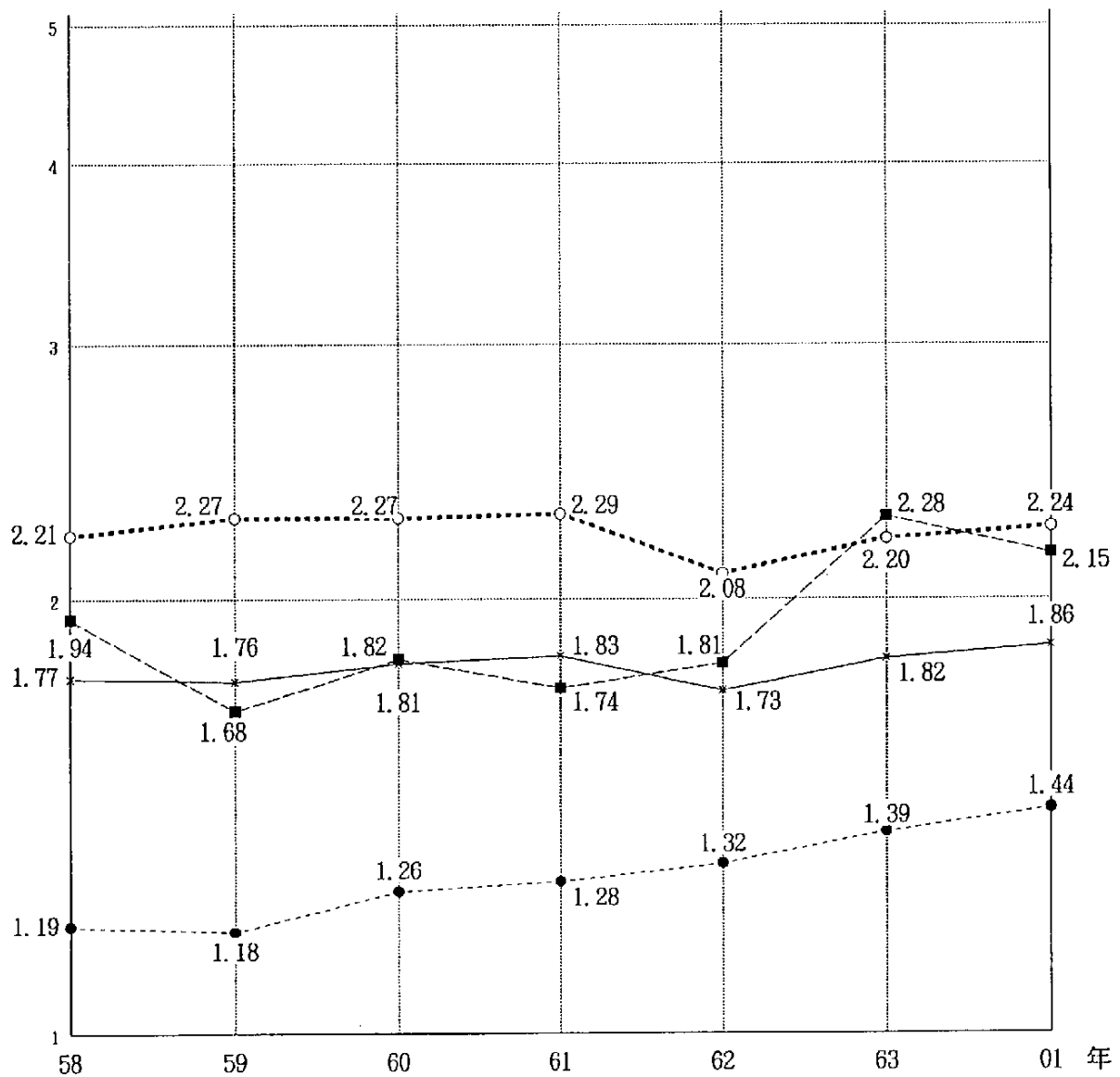
全体的なレベルが最も高い項目であり、全産業平均が3レベルに近い。第3次産業と公務はレベル3である。また、最も低い第2次産業でも2レベルの後半に入っている。この項目は、従来より高いレベルにあり、横ばい傾向が続いていることになる。レベルが高い原因の1つは、消防法などによる消火器などの義務づけによるものと思われる。



——：全産業平均 ：第2次産業計 ：第3次産業計 ----：公務計

停電対策

全体的にレベルの低い項目の1つである。その中でも、第2次産業の1.44という値は、全8項目の中で最も低い。ただし、この低い第2次産業が着実に向上傾向にあるといえよう。また、第2次産業が低い理由の1つには、システムダウンが直接的に顧客へ影響を及ぼすケースが少ないこともあると思われる。



——：全産業平均

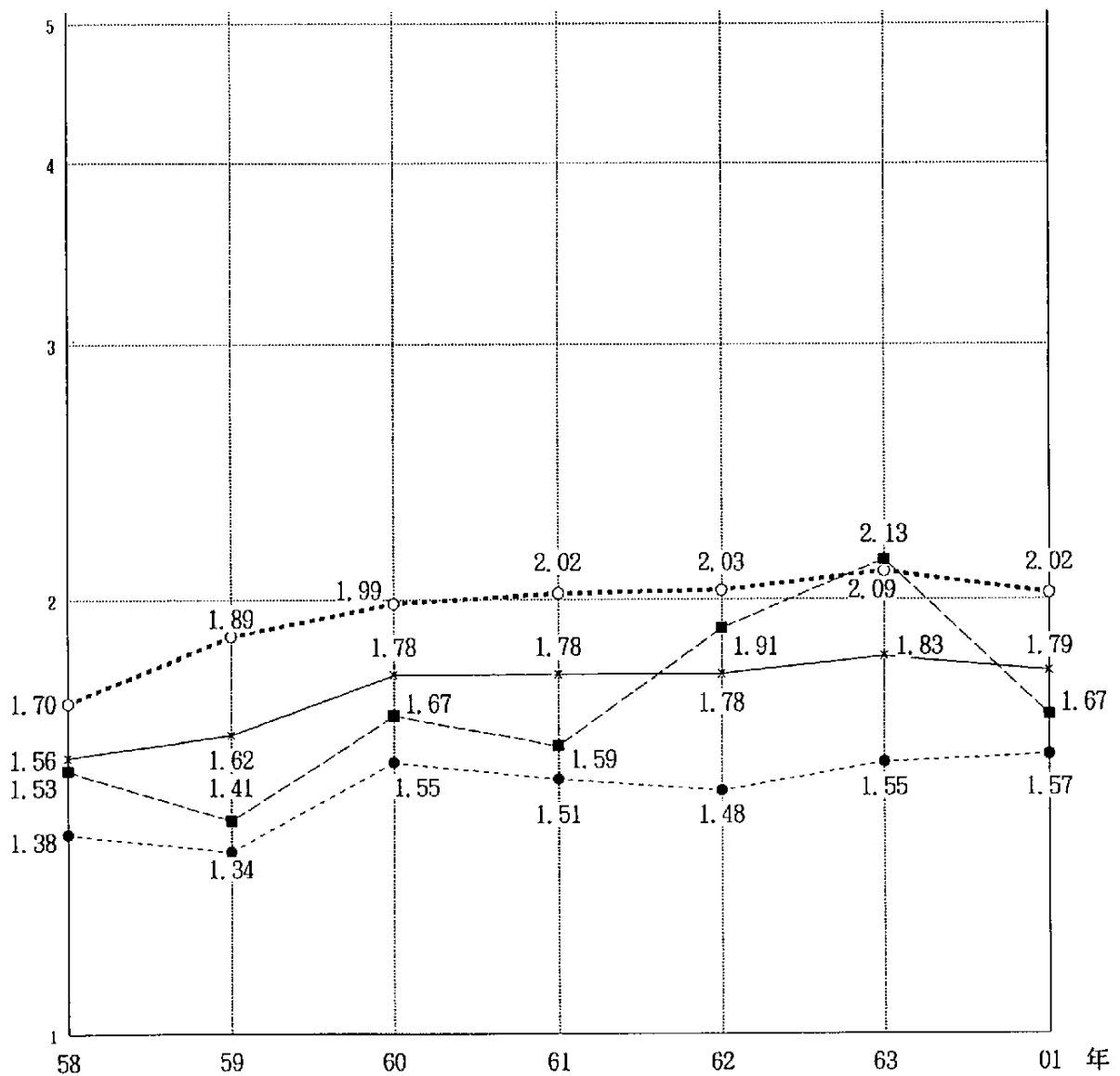
.....：第2次産業計

-----：第3次産業計

-.-.-：公務計

漏水対策

全8項目の中で、最も低い項目である。発生件数も少なく、影響も小さいことを物語っていると思われる。全体的な傾向としては、60年に底上げされて、その後は横ばいである。



——：全産業平均

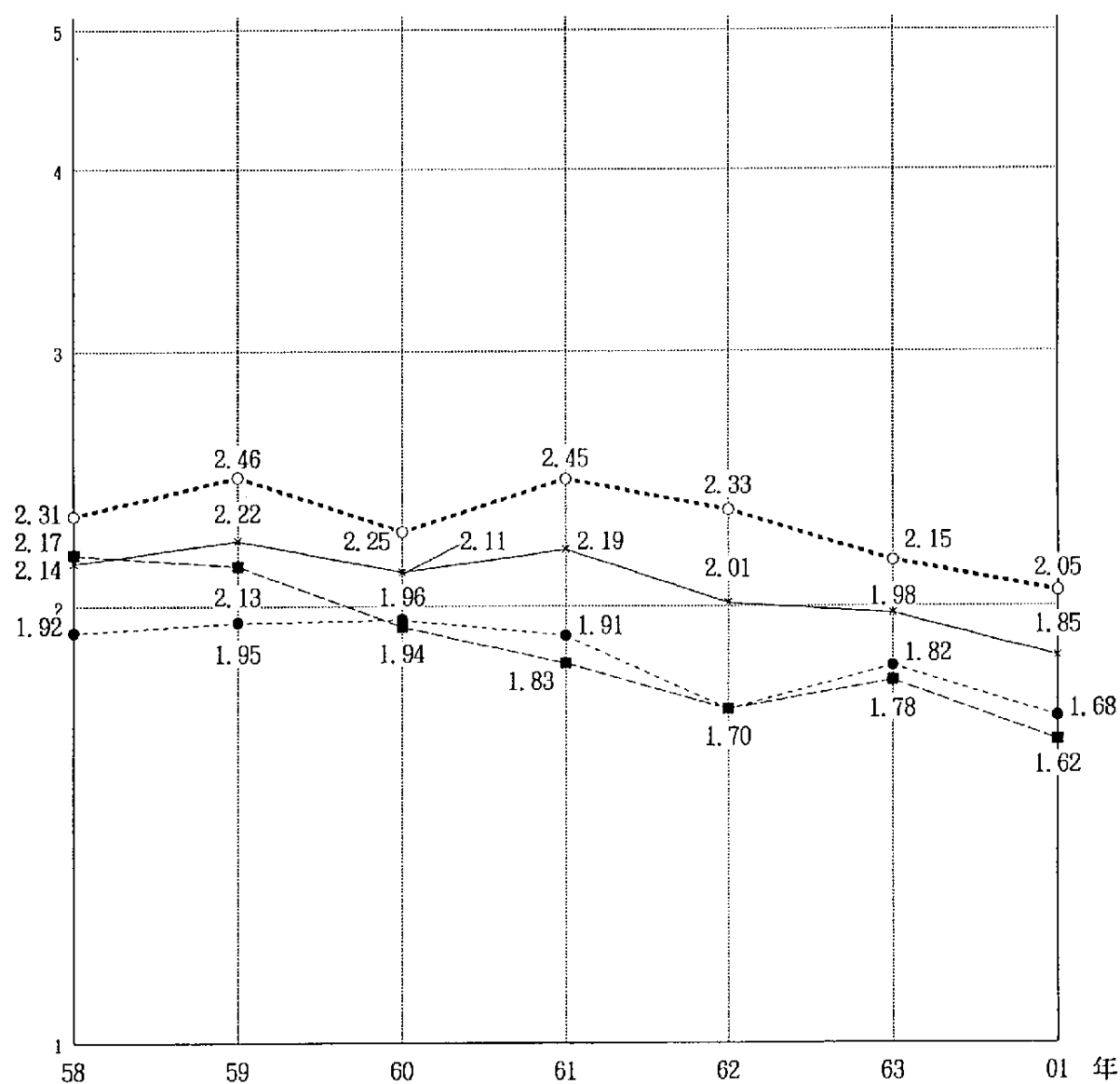
-----：第2次産業計

.....：第3次産業計

----：公務計

信頼性対策

全 8 項目の中で、信頼性対策のみが各産業とも低下傾向を示しているのが特徴である。これは、中・小規模のコンピュータがますます増加していることの現れであると思われる。

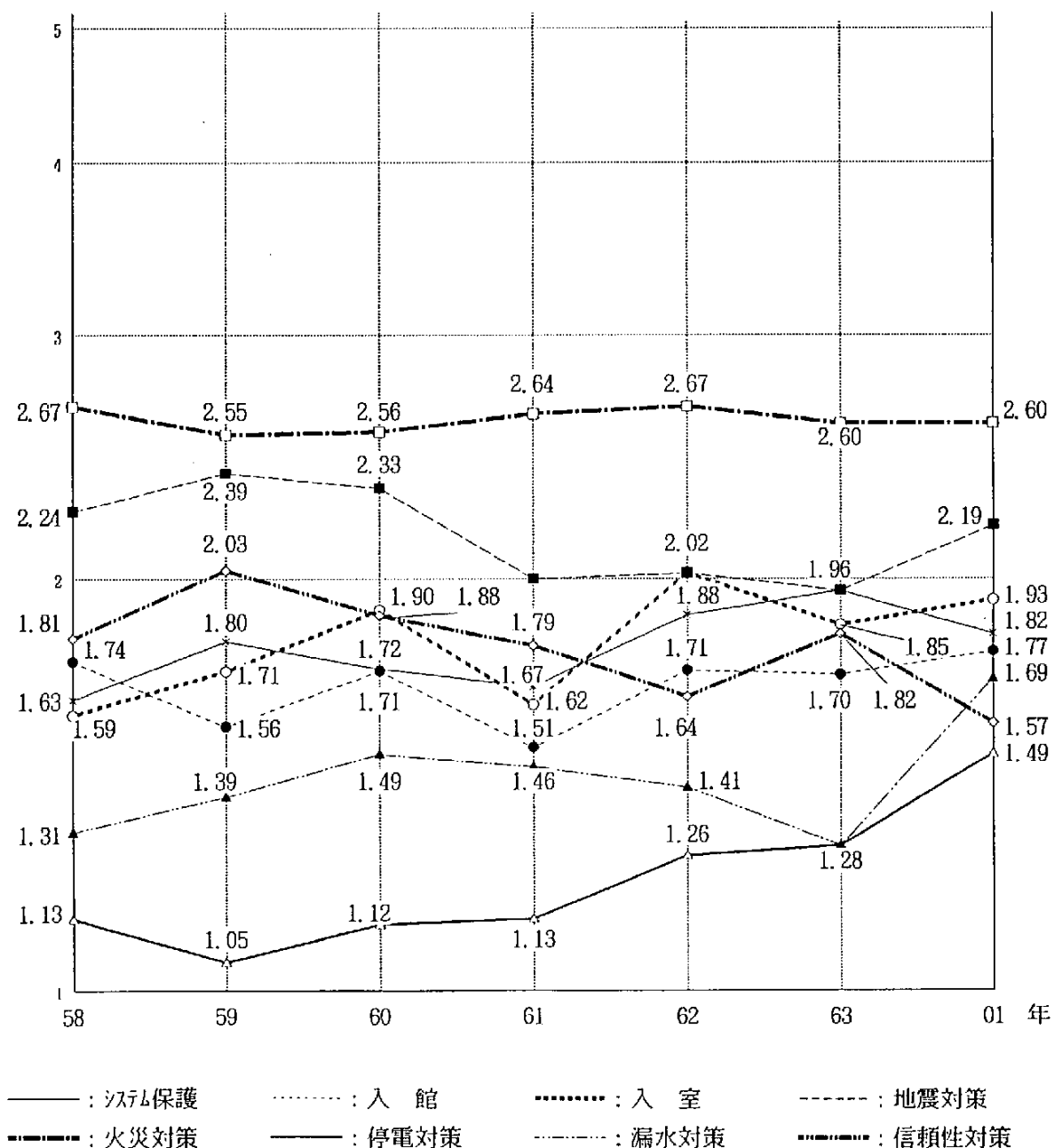


——：全産業平均 ：第2次産業計 ：第3次産業計 ----：公務計

業種別 (回答数のある程度まとまっている10業種について)

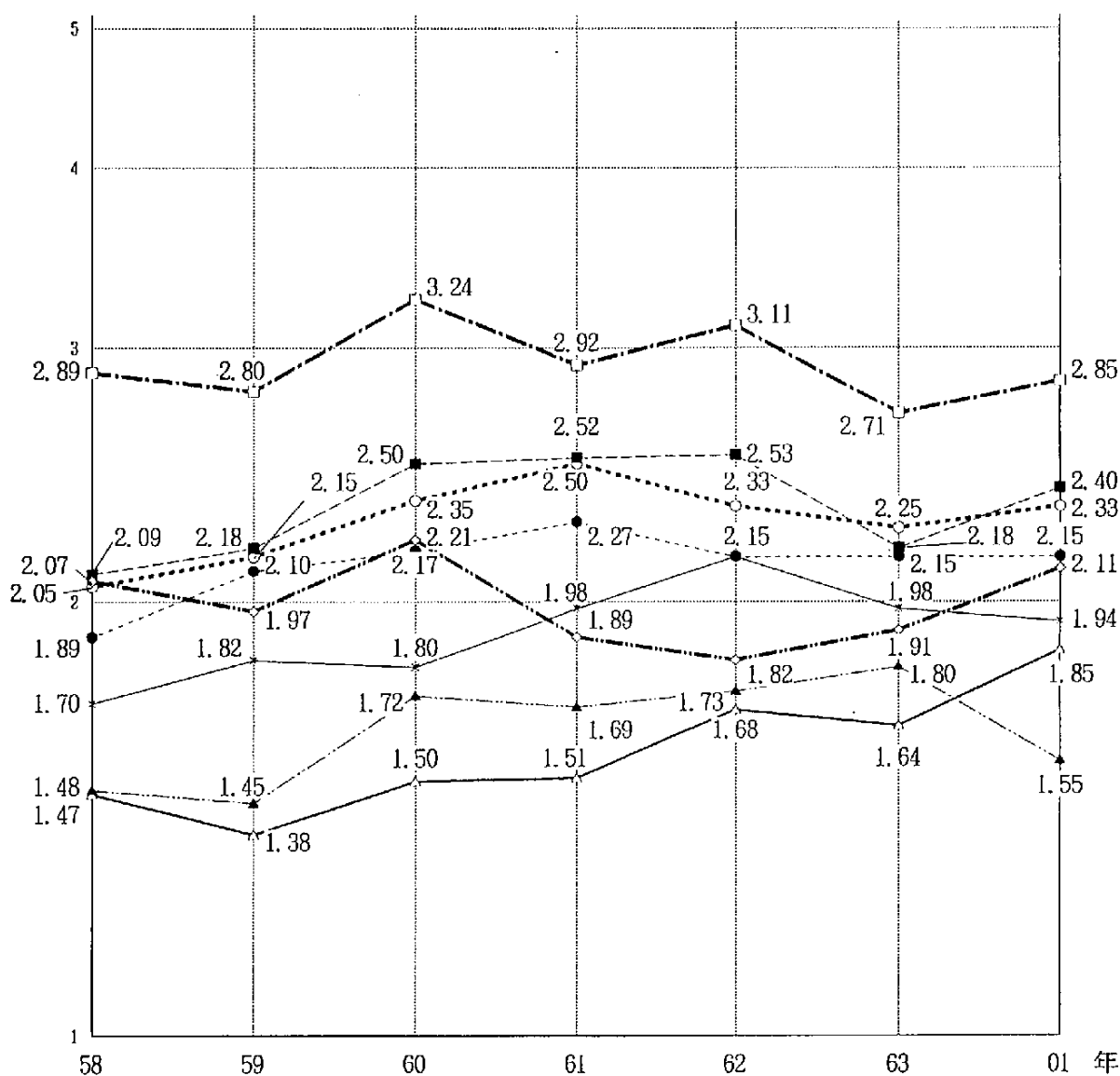
化学工業

化学工業は、8項目ともに全産業平均を下回っている。2レベル以上の項目は、「火災対策」と「地震対策」のみで、他は全て1レベル台の中位から後半にわたっている。全体的な傾向については、各年ごとの回答のバラツキを考慮すれば、ほぼ横ばい傾向であるといえる。その中で、「停電対策」だけが、ここ2～3年向上傾向にあり、1レベルと2レベルの間にまで向上してきている。



電機機器

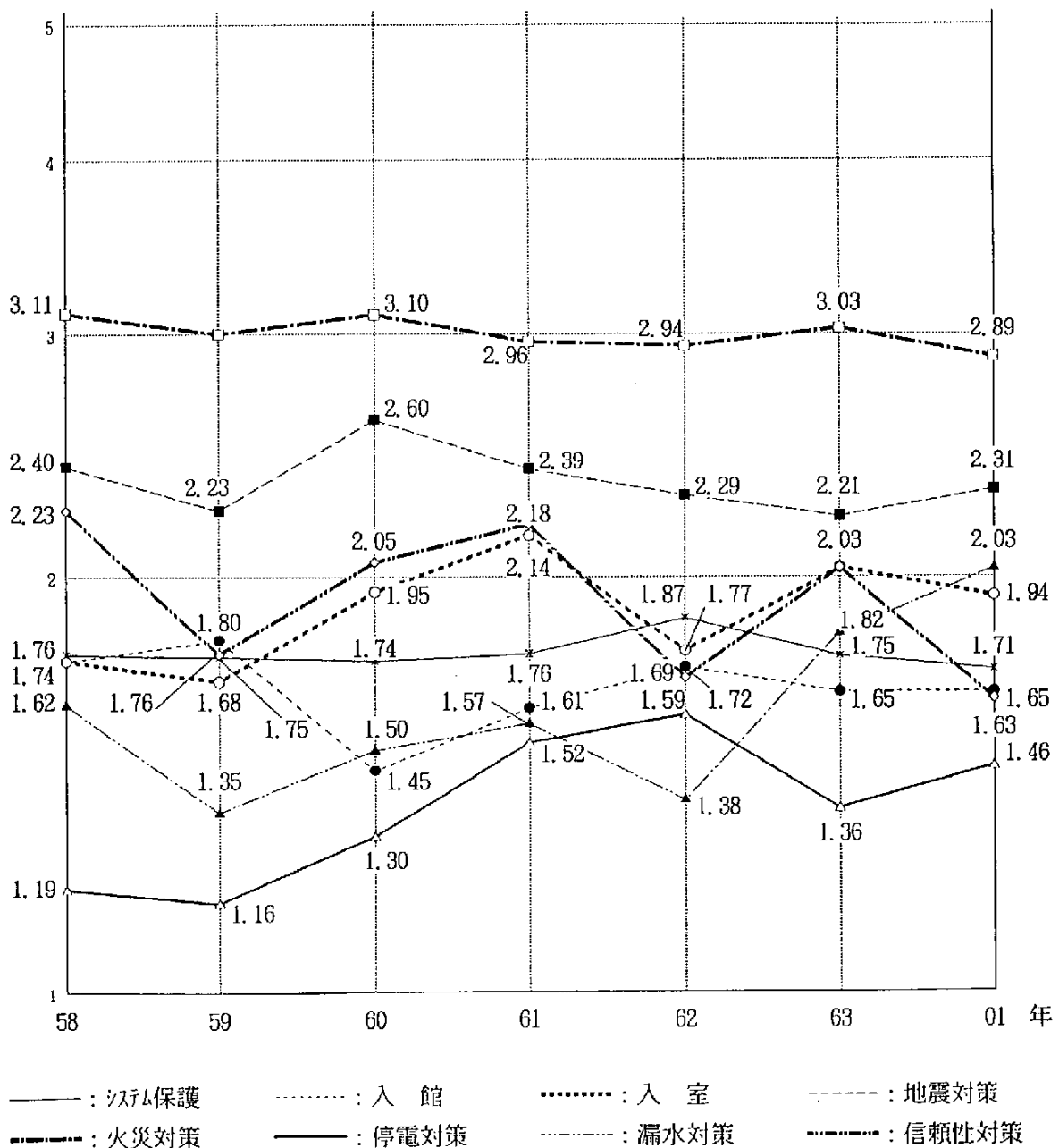
電機機器は、全体的にほぼ横ばいの状況にある。「停電対策」は、58年に1レベルと2レベルの中間程度であったものが、平成元年には2レベルにかなり近づいている。



——— : システム保護 : 入館 : 入室 - - - - : 地震対策
 - - - - : 火災対策 ——— : 停電対策 : 漏水対策 - - - - : 信頼性対策

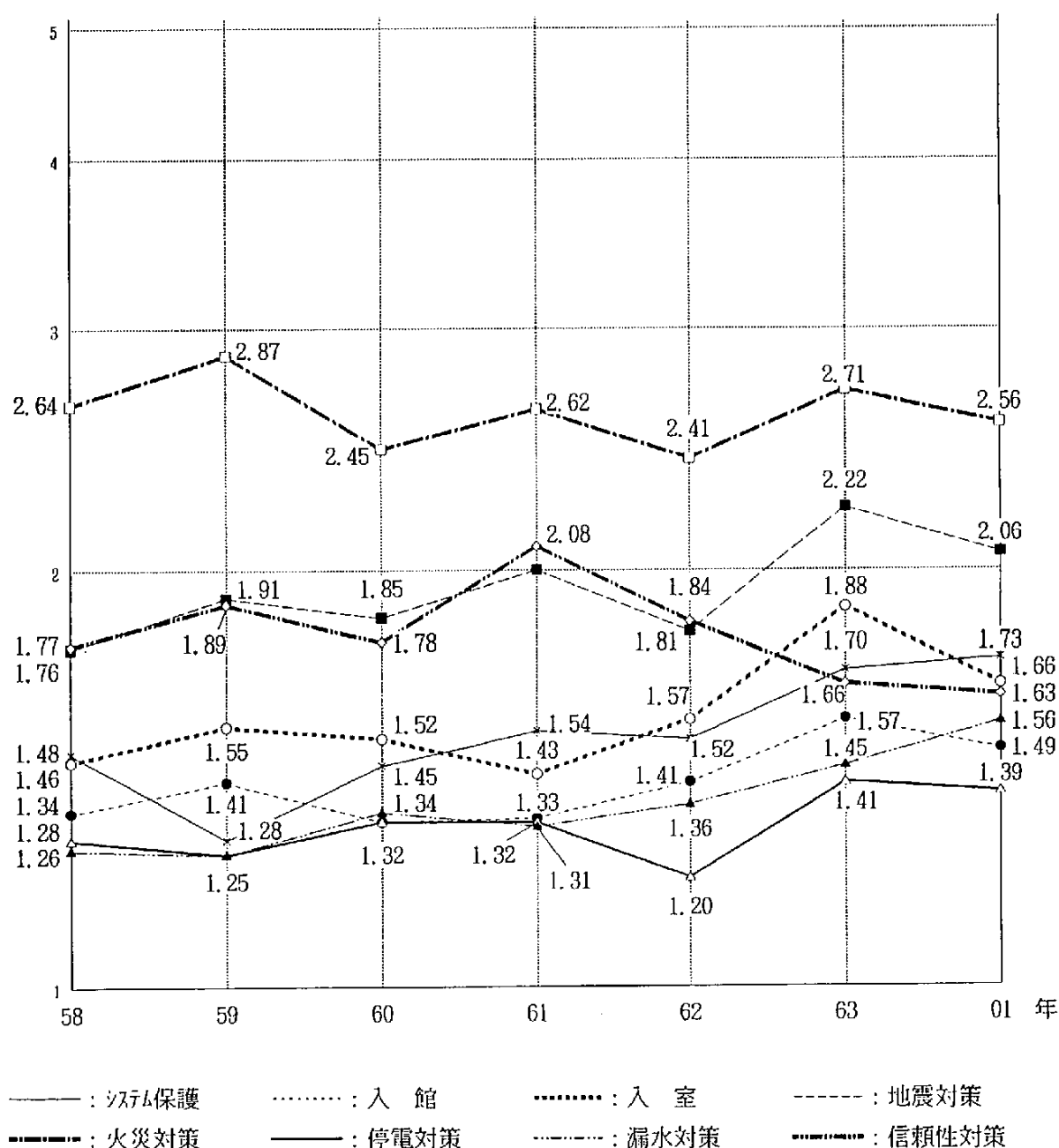
輸送用機器

輸送用機器は、各年ごとの回答のバラツキがかなり大きいですが、全体的にはほぼ横ばいである。



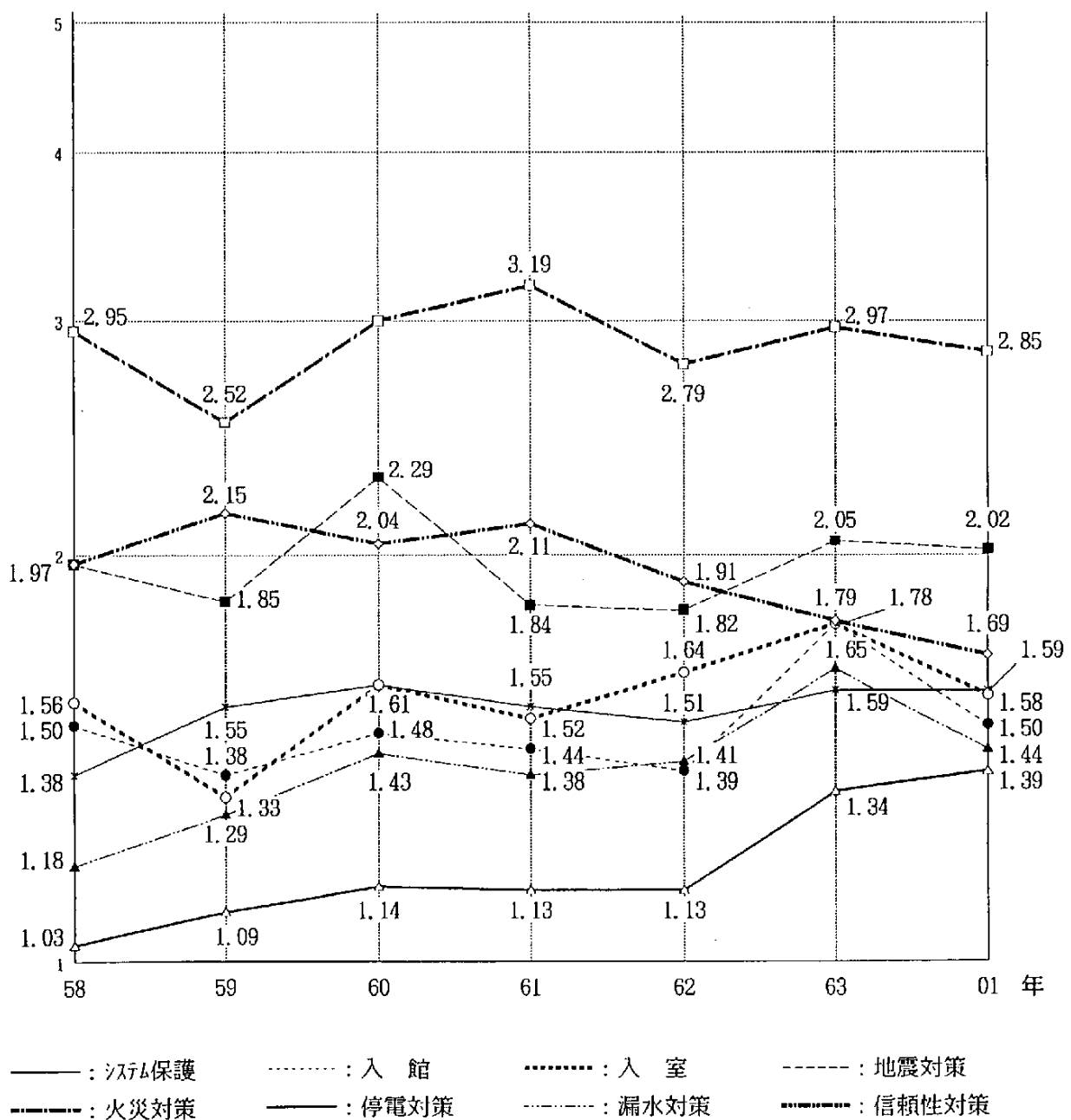
卸業・商社

全体的に横ばい状況である。最もレベルの高い「火災対策」にしても、2レベルと3レベルの中間程度である。



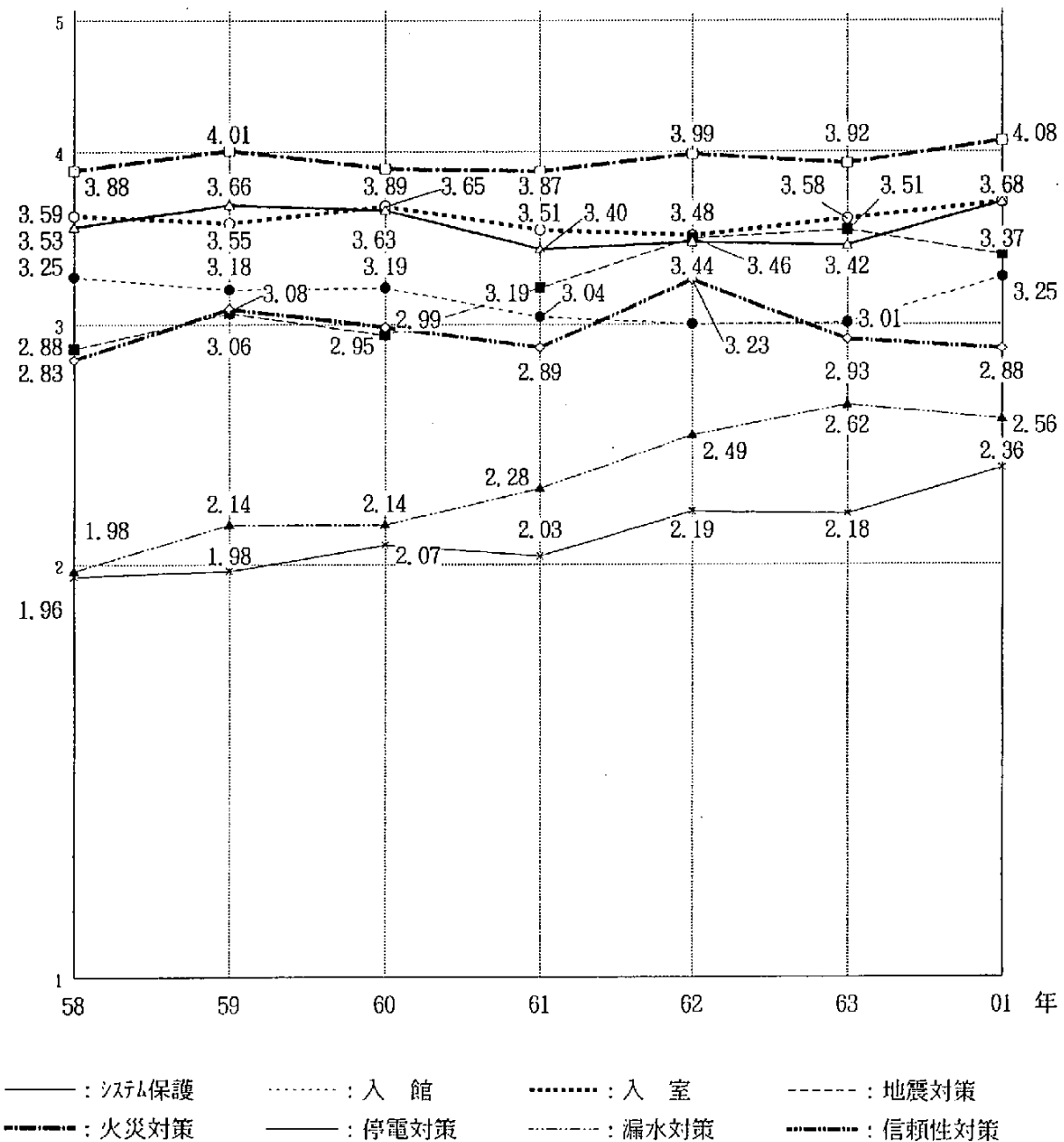
小売業

8項目全てが全産業平均を下回っている。そして、多くの項目が1レベルと2レベルの中間程度に集中している。



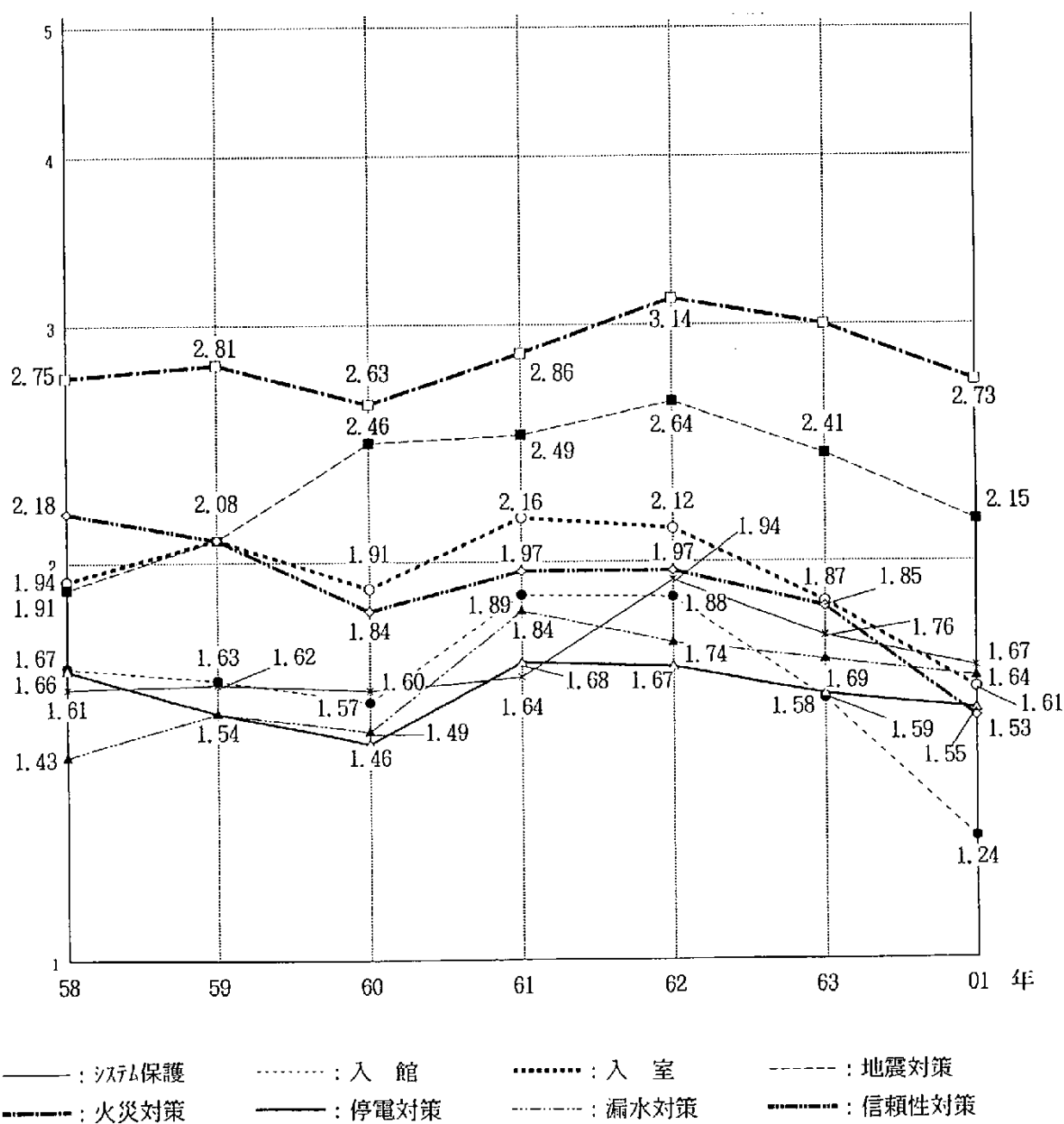
金融業

金融業は、セキュリティレベルの最も高い業種の1つである。「火災対策」は4レベルに到達しているし、最も低い方の「漏水対策」や「停電対策」も着実に向上しており、2レベルと3レベルの中間程度にまで来ている。



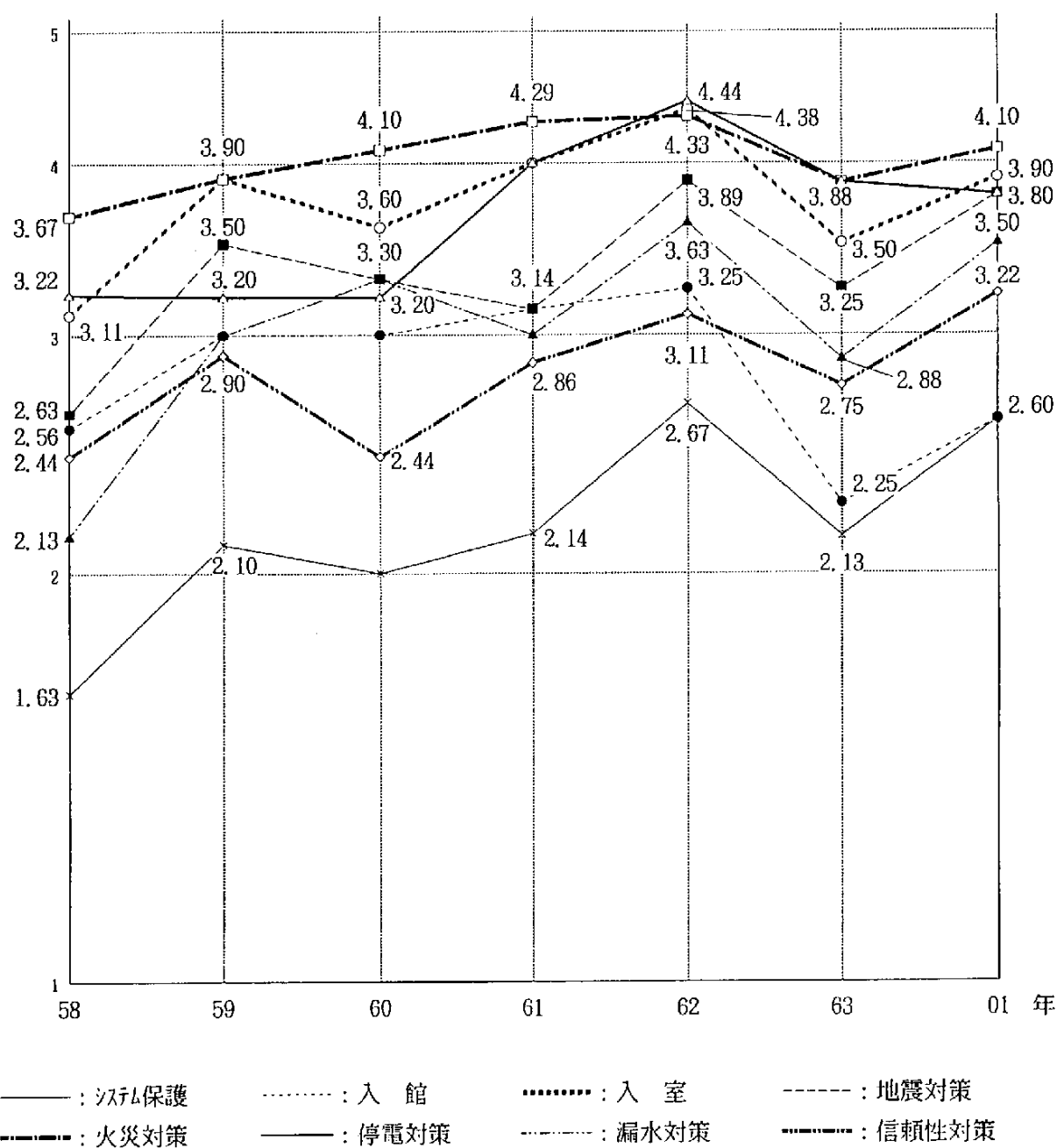
運輸・通信・倉庫業

全体的には横ばい状況であるが、62年以降、急激に下降しているが、これは回答企業のバラツキによるものと思われる。



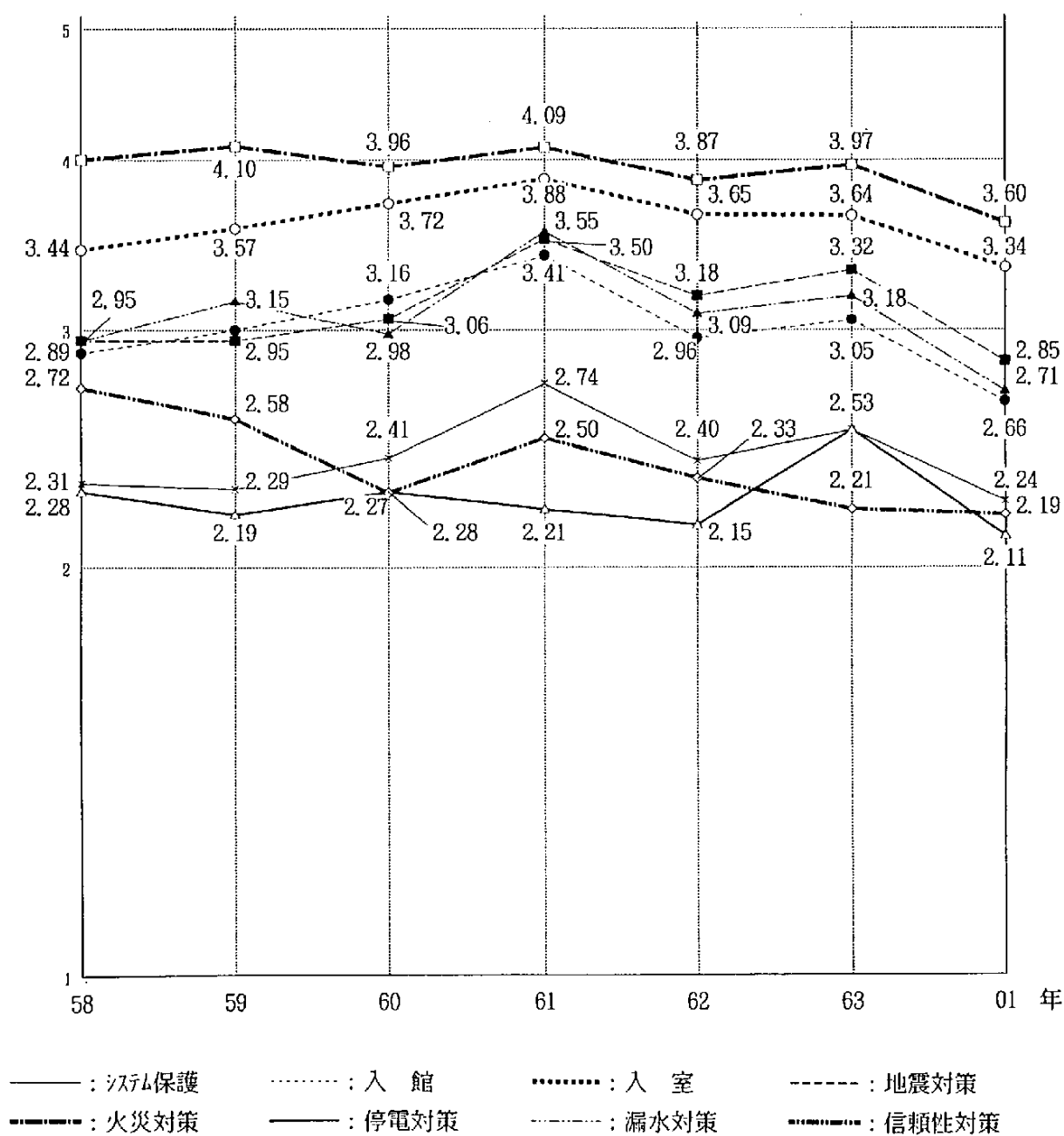
電力・ガス事業

この調査においては、電力・ガス事業が最もセキュリティレベルの高い業種である。しかも、全体的には、バラツキはあるものの、向上傾向を示しているといえる。



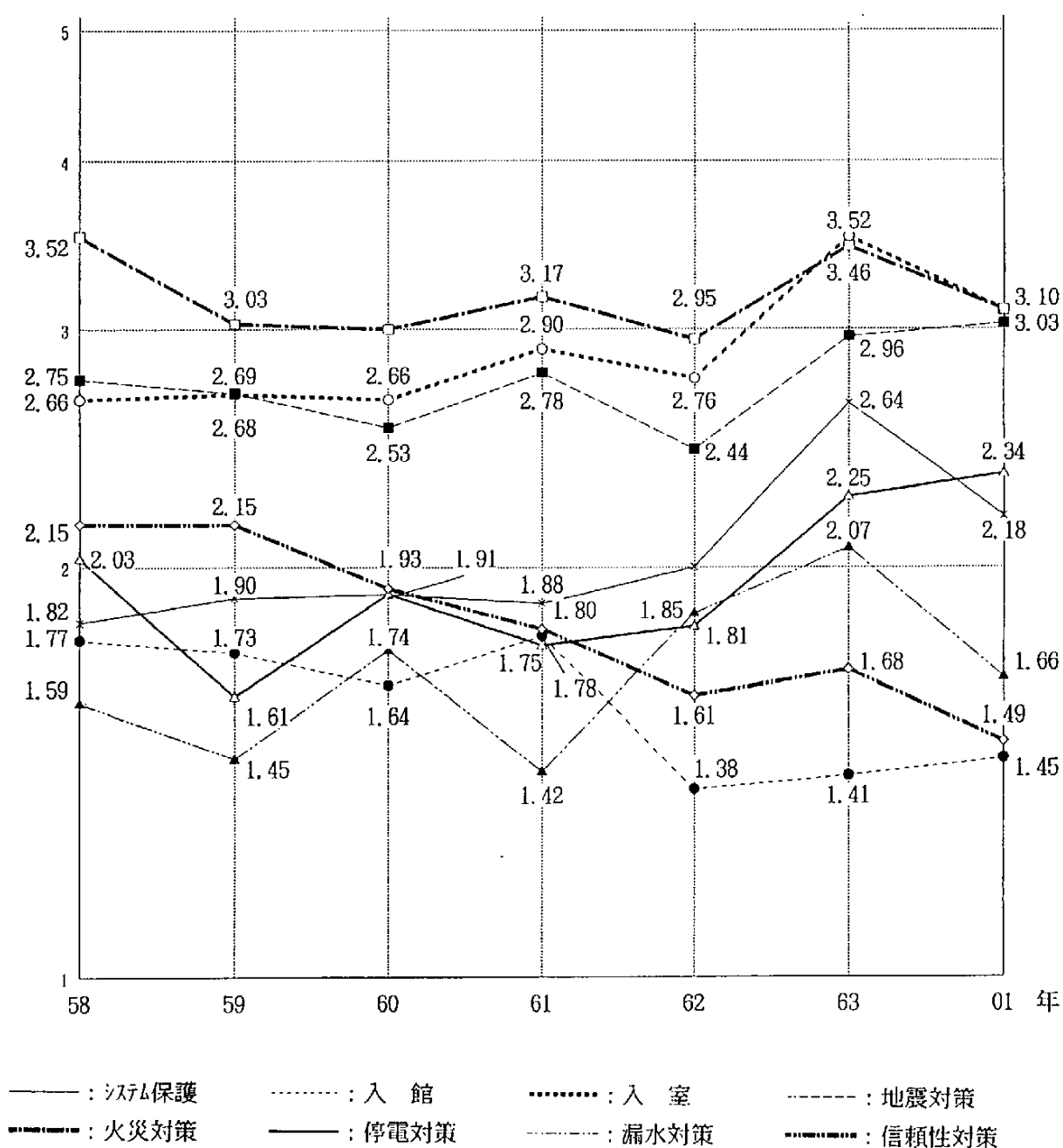
情報処理サービス業・ソフトウェア業

全ての項目が、2レベルと3レベルに入っている。この業種もほとんど横ばいである。全体的には、電力・ガス、金融について、3番目にセキュリティレベルの高い業種である。



地方公共団体

地方公共団体は、「入館」が制限できないため最も低いが、その分、「入室」が「火災対策」なみで最も高くなっている。



付属資料 4

業種別セキュリティ対策水準の実態(1989年度)

表1. 回 答 企 業 数

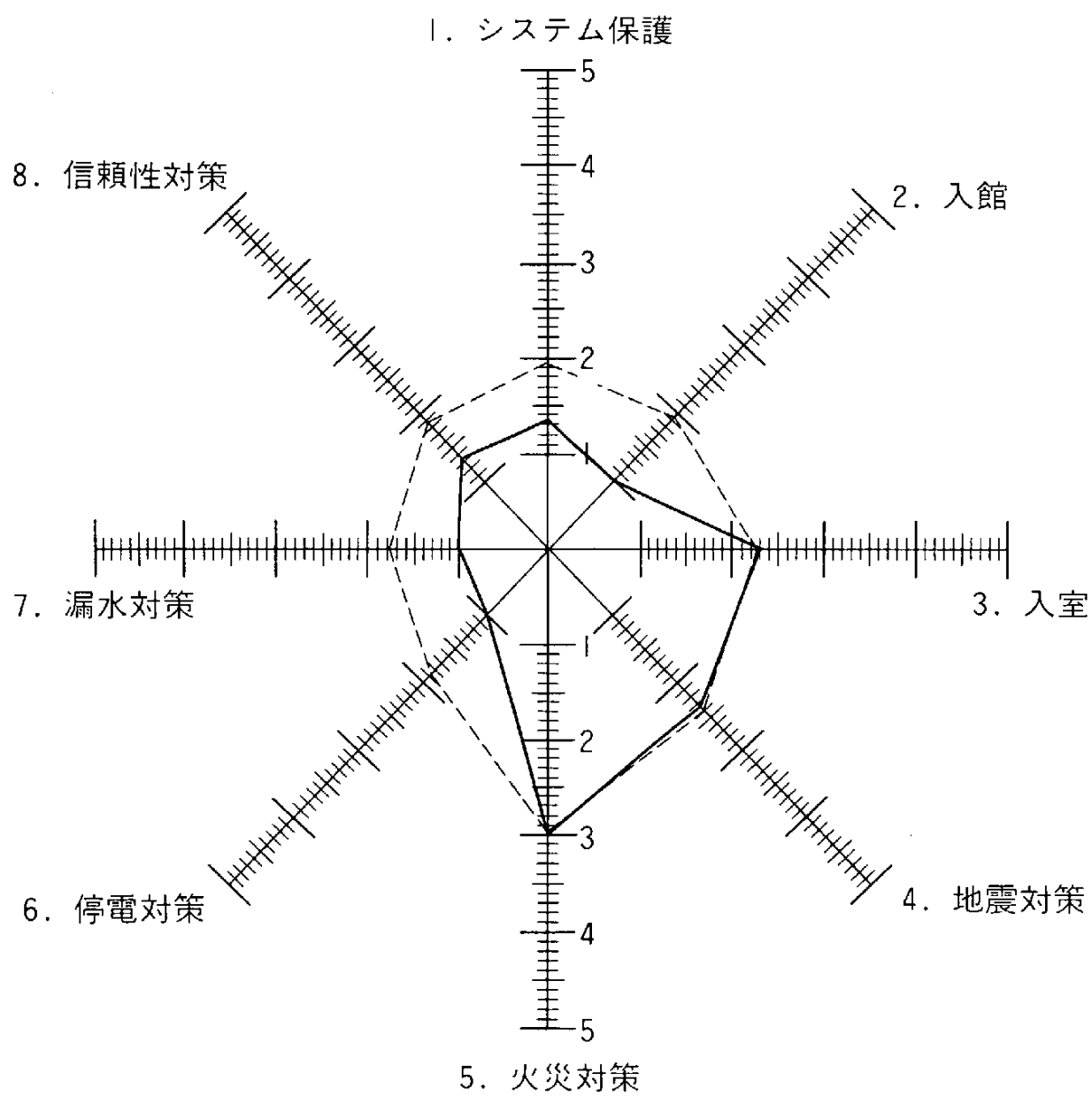
業 種 \ 年 度	58	59	60	61	62	63	1
農・林・漁・狩猟・水産養殖業	4	3	0	1	1	1	2
鉱 業	0	0	0	1	0	2	1
建 設 業	25	21	23	21	26	27	41
食品製造業	27	24	24	16	23	20	24
織 維 工 業	17	13	13	15	17	24	28
紙・パルプ・紙加工品製造業	6	4	5	6	10	11	13
新聞業・出版業	3	6	7	7	5	6	6
印刷業・同関連産業	4	2	0	1	5	4	7
化 学 工 業	48	44	43	40	43	47	62
石油製品製造業	10	5	4	5	4	8	6
窯業・土石製品製造業	11	7	10	5	9	7	7
鉄 鋼 業	10	17	15	17	12	14	11
非鉄金属製造業・金属製品製造業	30	23	21	18	30	23	23
一般機械器具製造業	29	22	21	18	29	35	43
電気機械器具製造業	45	41	46	51	62	56	54
輸送用機械器具製造業	27	28	20	24	32	33	35
精密機械器具製造業	25	18	11	16	15	16	16
その他の製造業	27	22	31	29	27	25	32
卸業・商社	101	55	54	54	71	68	69
小 売 業	41	34	28	34	39	38	46
金 融 業	123	90	90	99	82	86	94
証券業・商品取引業	4	2	3	4	5	3	2
生 命 保 険 業（含代理業・サービス業）	5	4	4	5	3	6	8
損 害 保 険 業（含代理業・サービス業）	2	1	2	1	3	3	3
不 動 産 業	2	2	2	1	3	6	4
運輸・通信業	33	27	35	37	36	40	34
電力・ガス事業	9	10	10	7	9	9	10
放 送 業	8	8	5	7	11	7	15
広告・調査・情報提供サービス業	2	5	4	5	8	5	7
情報処理サービス業・ソフトウェア業	38	43	51	34	55	38	48
医 療 業	6	3	3	6	8	5	7
宗 教 法 人	0	0	0	0	0	0	0
高 校	0	0	0	0	2	0	1
大 学	24	18	19	16	23	12	22
その他の教育機関	0	1	4	2	8	6	7
学術研究機関	3	2	2	2	2	4	3
法人団体・農協	35	23	27	26	23	18	28
その他のサービス業	9	9	5	7	8	5	11
政 府	4	3	4	3	5	4	9
地方公共団体	30	32	35	24	43	29	39

表2. 質問項目ごとの実施レベル

レベル 項目	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、バッジ	受付者、来訪者名簿、バッジ and/or I Dカード	受付者、来訪者名簿、バッジ and/or I D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、バッジ	受付者、来訪者名簿、バッジ and/or I Dカード	受付者、来訪者名簿、バッジ and/or I D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	バッテリー用意	バッテリー用意、自家発電装置	バッテリー用意、自家発電装置、定周波装置	バッテリー用意、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				
	(1項目採用)	(2項目採用)	(3項目採用)	(4項目採用)	(5項目採用)

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嚴重と思われるもの（レベル5）までを5段階に分類した。ただし、信頼性対策については、採用している項目数で5段階とした。

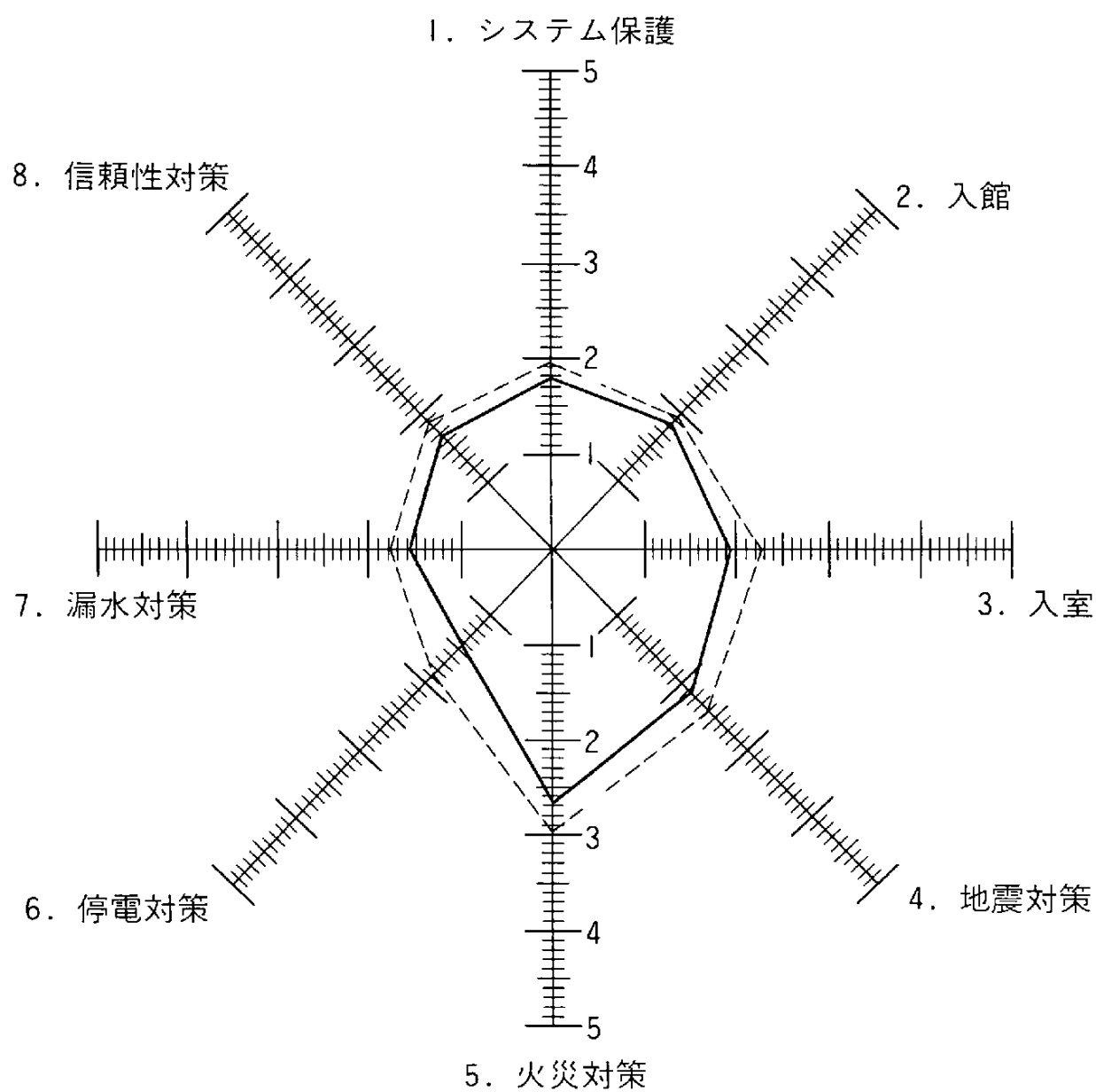
第一次産業計



---: 全産業平均

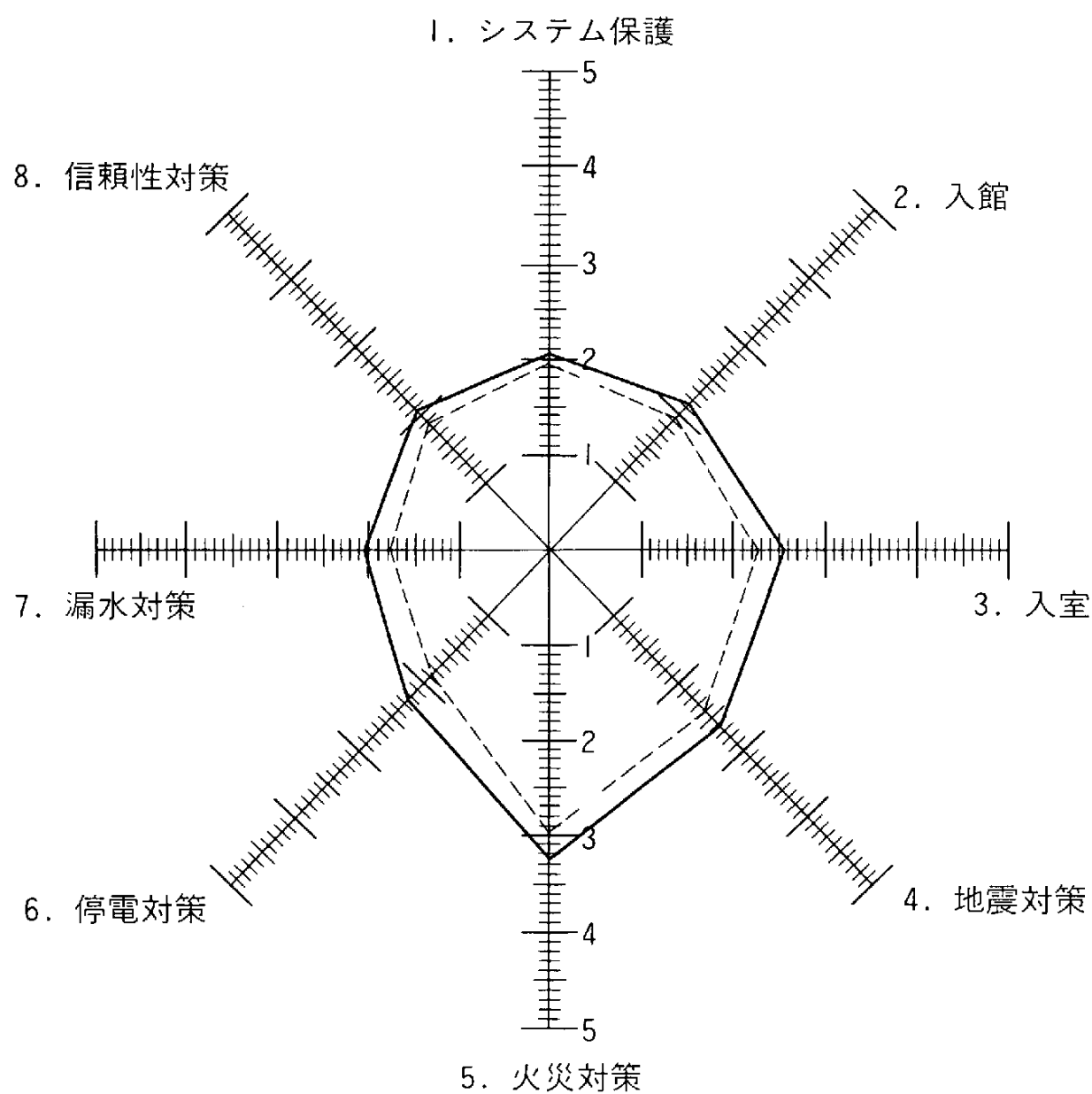
	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1.91	1.95	2.27	2.40	2.97	1.86	1.79	1.85
第一次産業計	1.33	1.00	2.33	2.33	3.00	1.00	1.00	1.33

第二次産業計



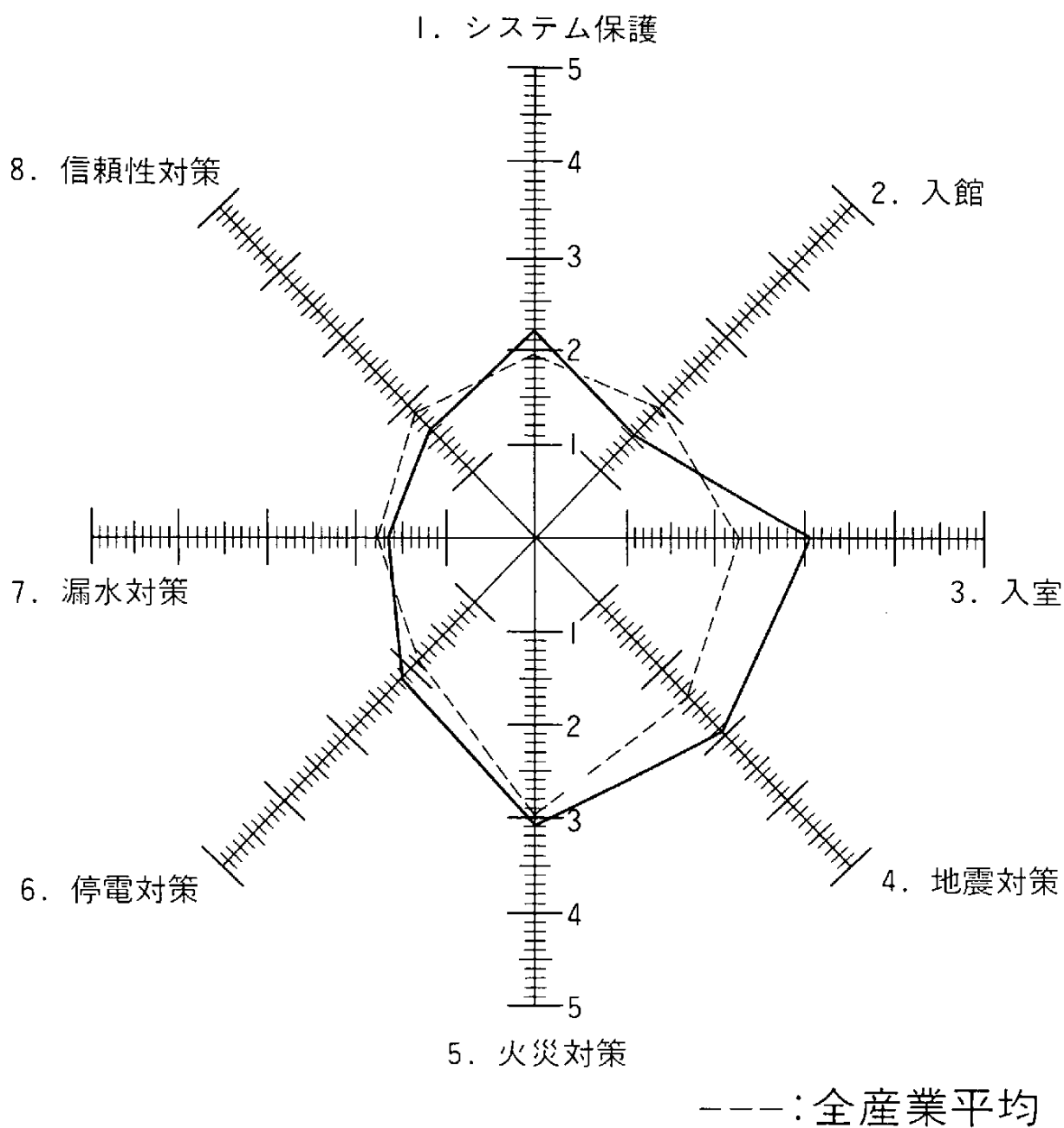
	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1.91	1.95	2.27	2.40	2.97	1.86	1.79	1.85
第二次産業計	1.77	1.81	1.91	2.12	2.68	1.44	1.57	1.68

第三次産業計



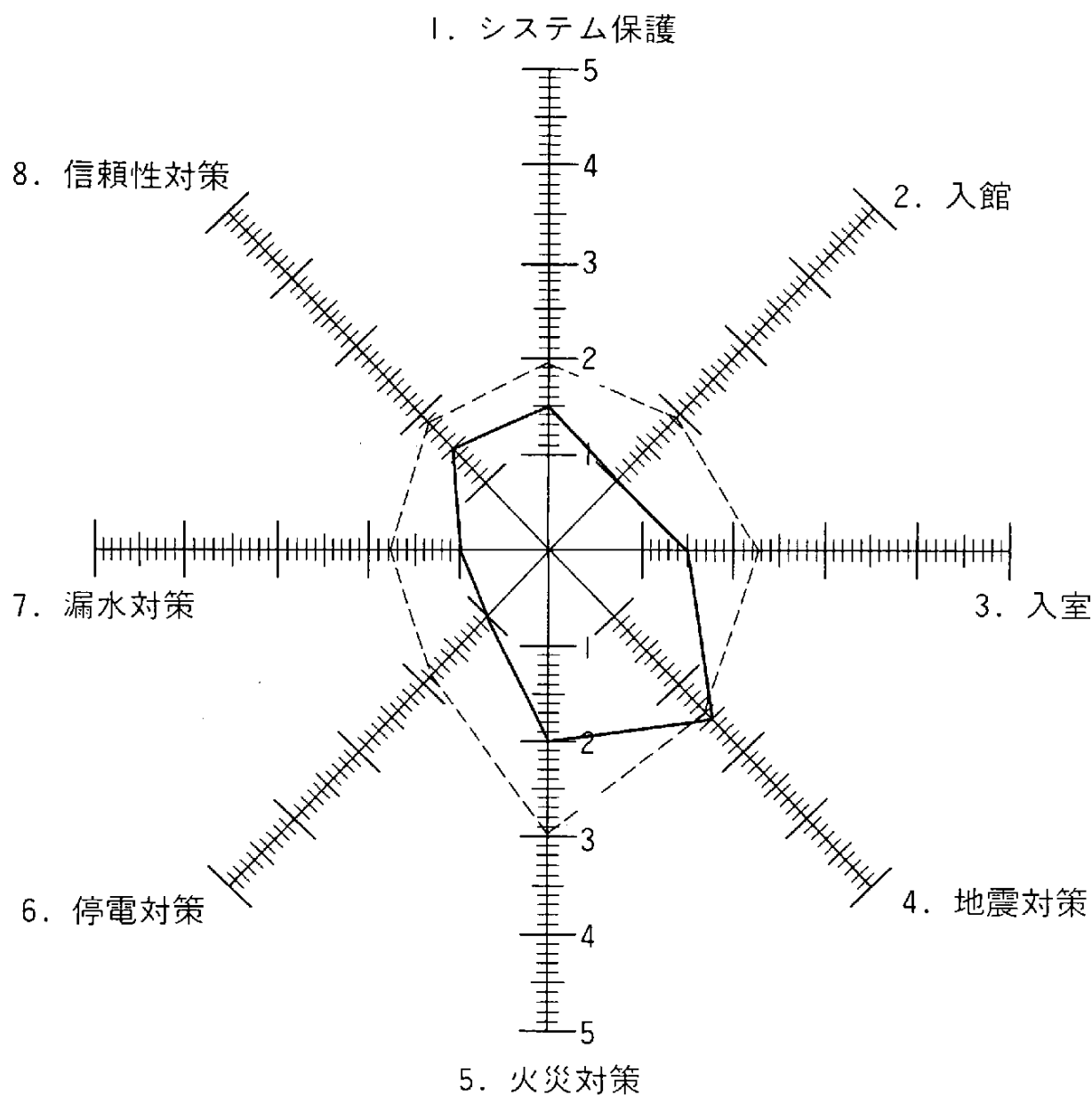
	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1. 91	1. 95	2. 27	2. 40	2. 97	1. 86	1. 79	1. 85
第三次産業計	2. 02	2. 13	2. 53	2. 61	3. 24	2. 24	2. 02	2. 05

公 務 計



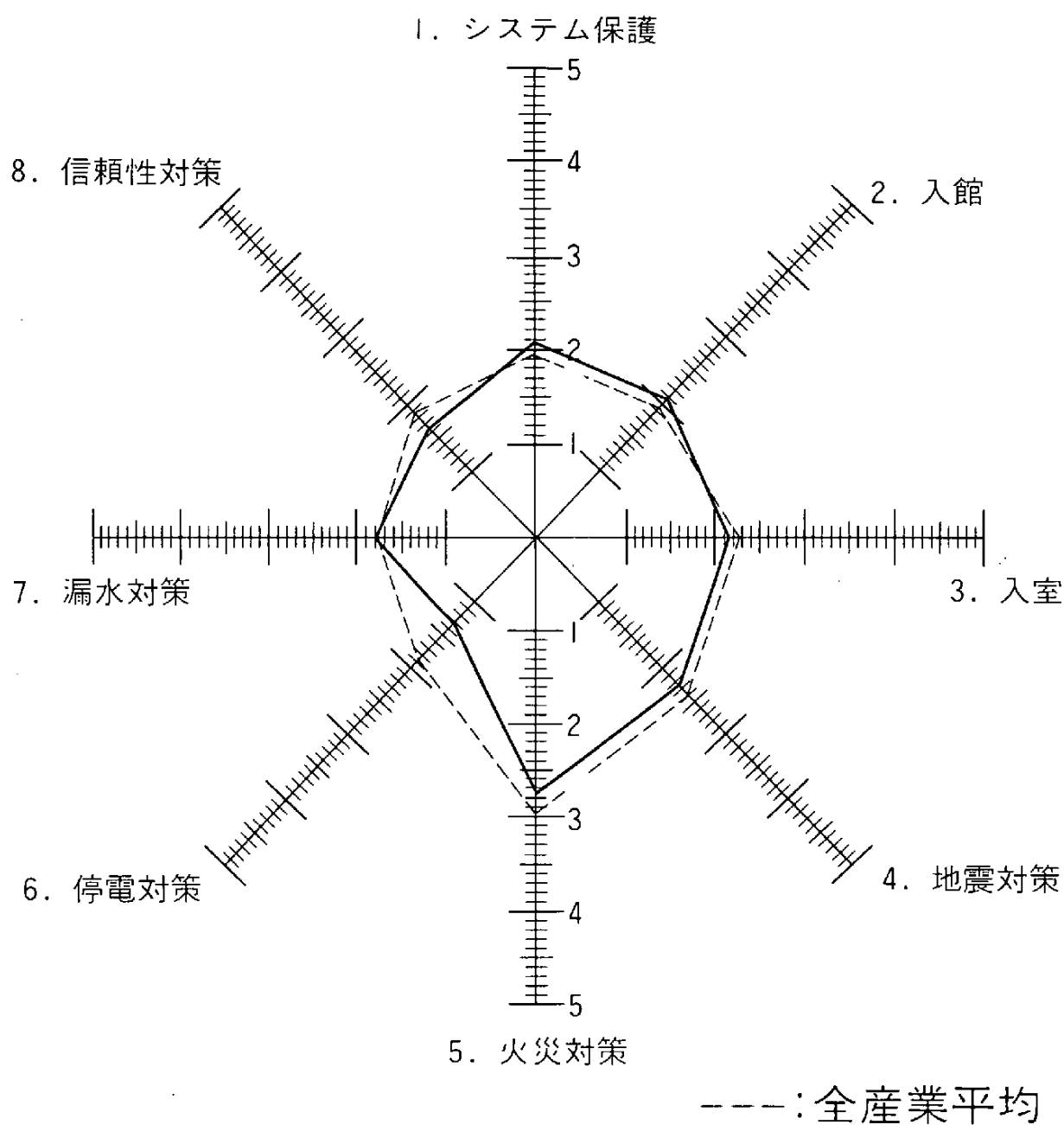
	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1. 91	1. 95	2. 27	2. 40	2. 97	1. 86	1. 79	1. 85
公 務 計	2. 17	1. 51	3. 06	2. 91	3. 10	2. 15	1. 67	1. 62

農・林・漁・狩猟・水産養殖業



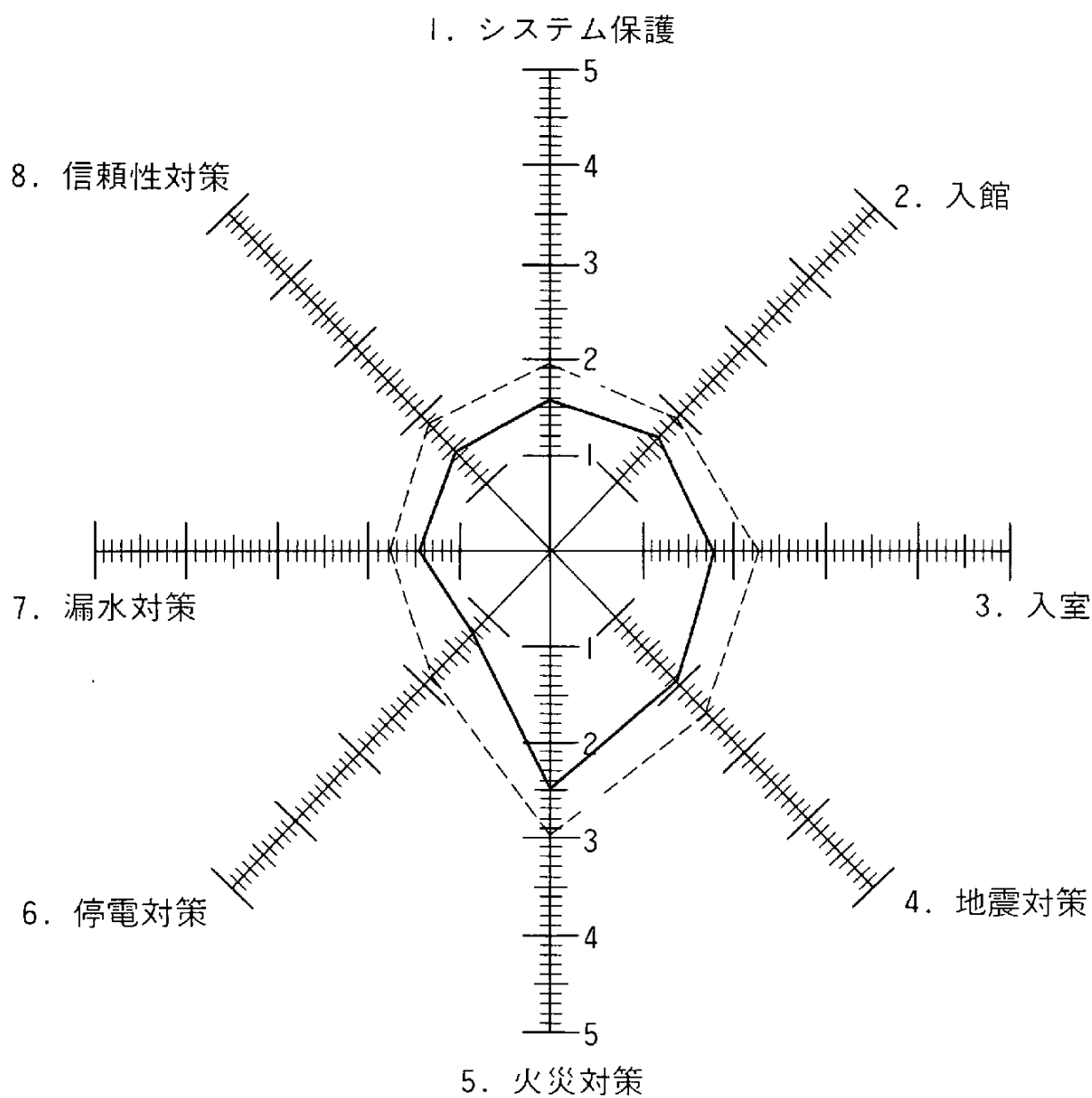
	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1.91	1.95	2.27	2.40	2.97	1.86	1.79	1.85
農・林・漁・ 狩猟・水産 養殖業	1.50	1.00	1.50	2.50	2.00	1.00	1.00	1.50

建設業



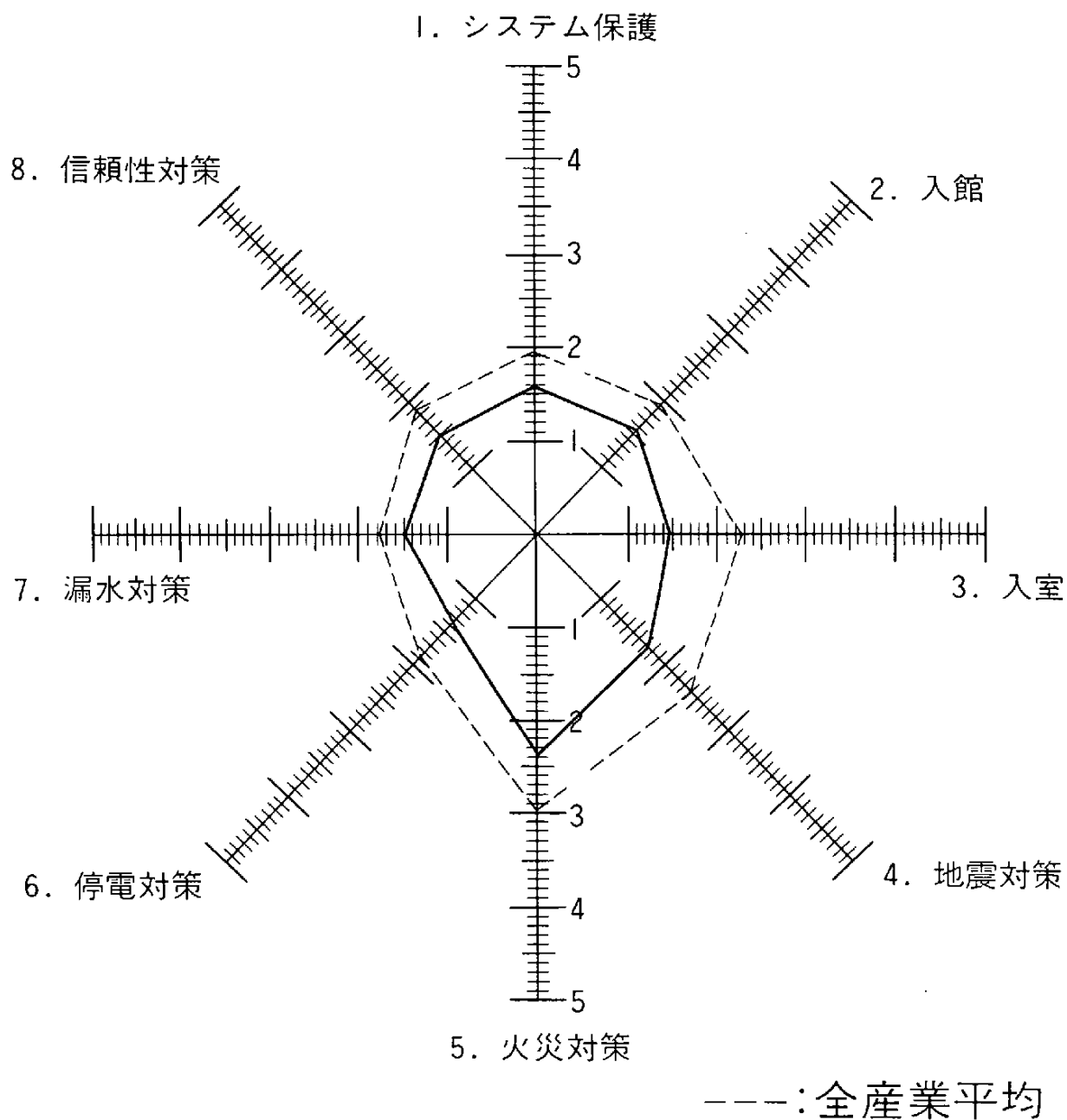
	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1.91	1.95	2.27	2.40	2.97	1.86	1.79	1.85
建設業	2.08	2.05	2.15	2.29	2.73	1.30	1.80	1.61

食品製造業



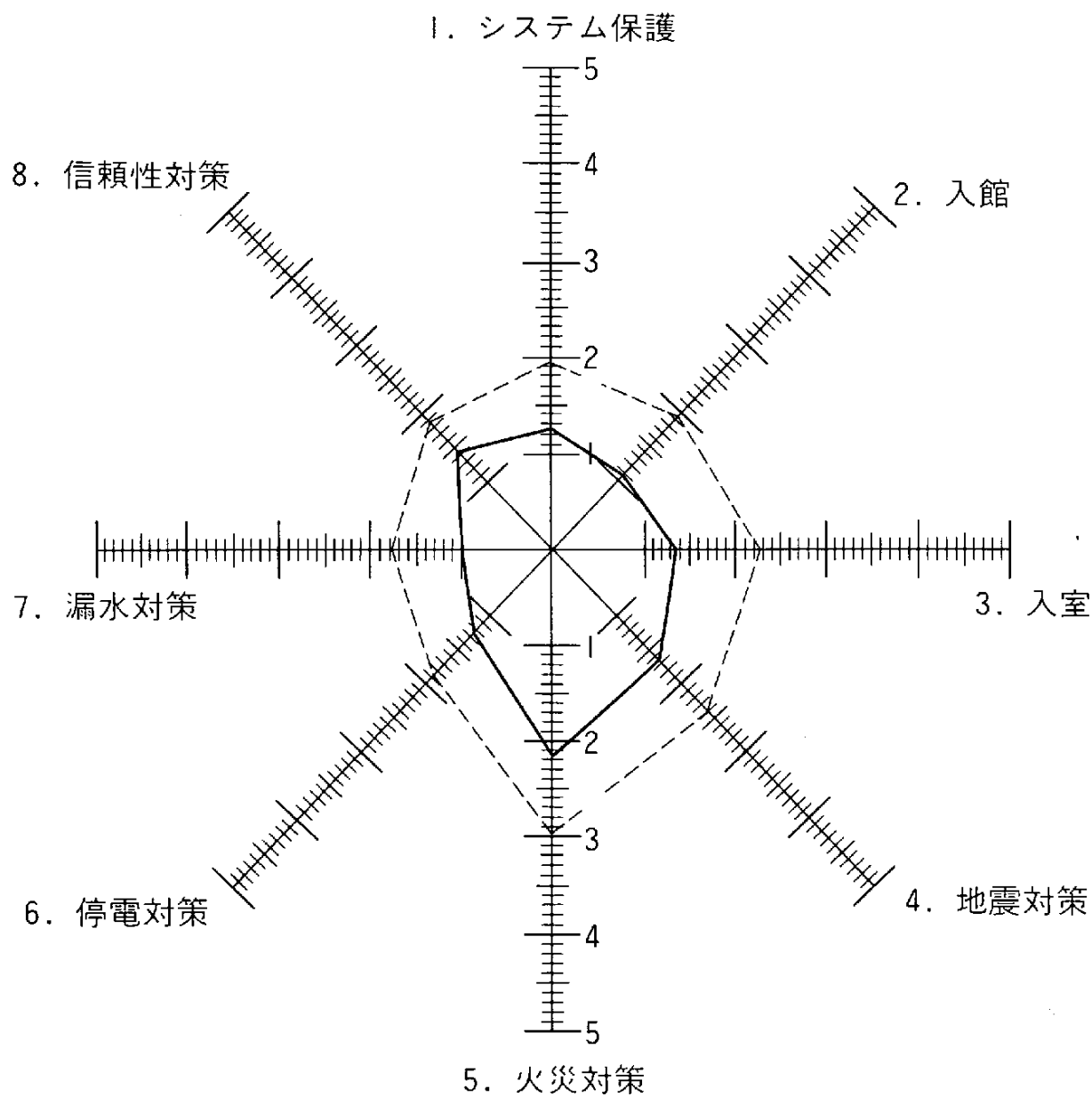
	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1. 91	1. 95	2. 27	2. 40	2. 97	1. 86	1. 79	1. 85
食品製造業	1. 57	1. 63	1. 79	1. 92	2. 50	1. 21	1. 42	1. 43

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. 91	1. 95	2. 27	2. 40	2. 97	1. 86	1. 79	1. 85
繊維工業	1. 56	1. 52	1. 46	1. 71	2. 39	1. 39	1. 50	1. 50

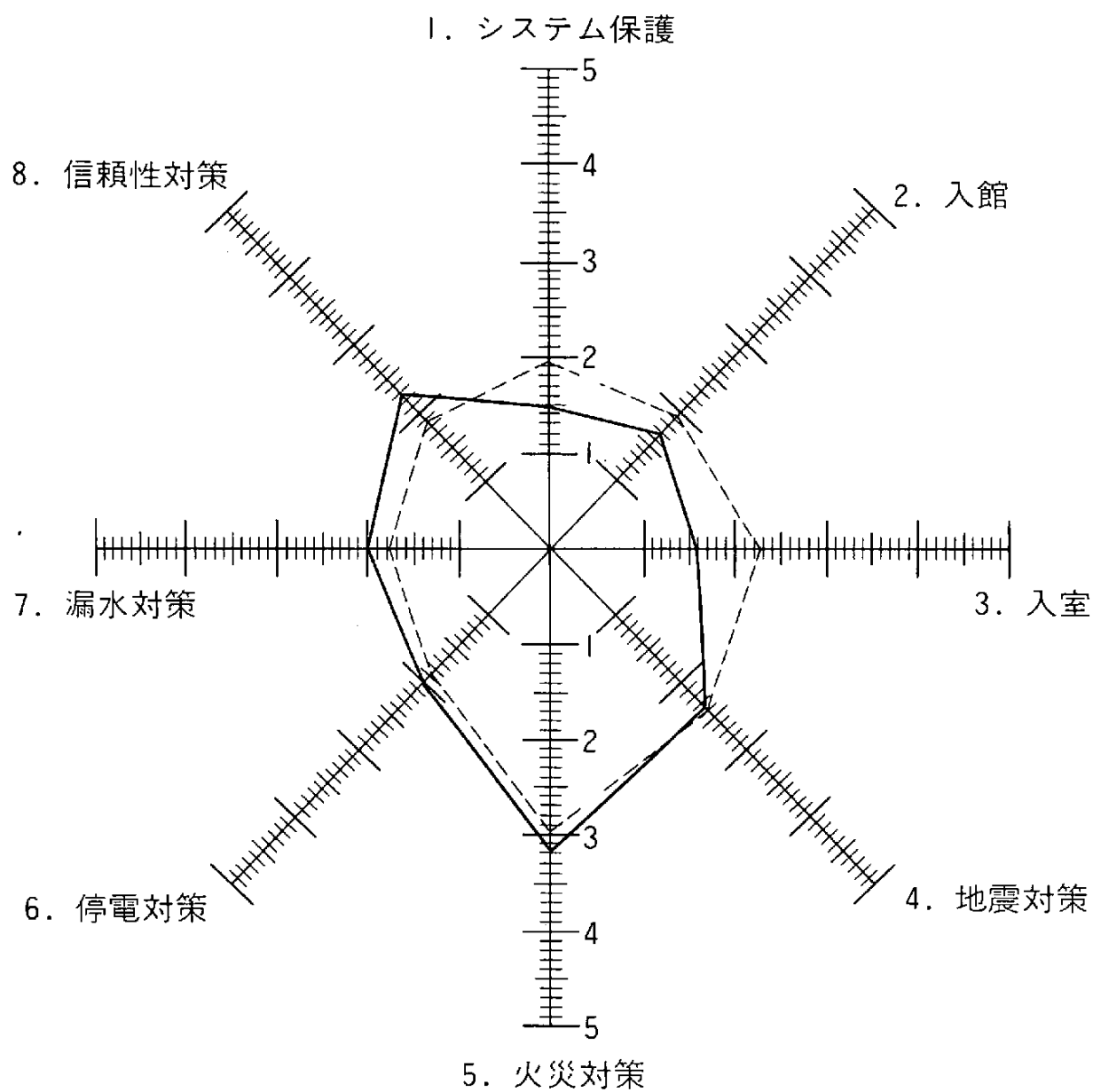
紙・パルプ・紙加工品製造業



---: 全産業平均

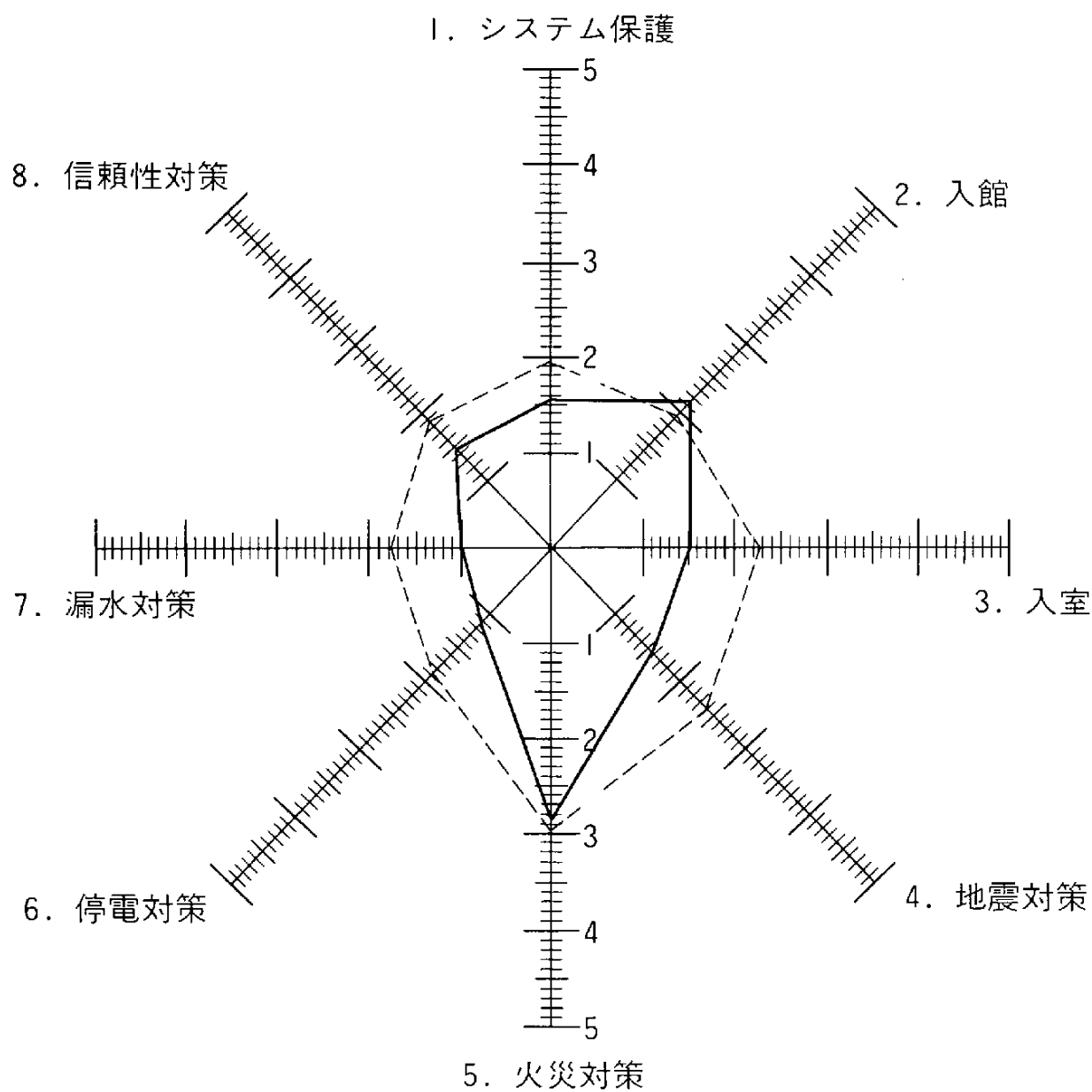
	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1.91	1.95	2.27	2.40	2.97	1.86	1.79	1.85
紙・パルプ・ 紙加工品製 造業	1.23	1.08	1.38	1.62	2.15	1.23	1.00	1.42

新聞業・出版業



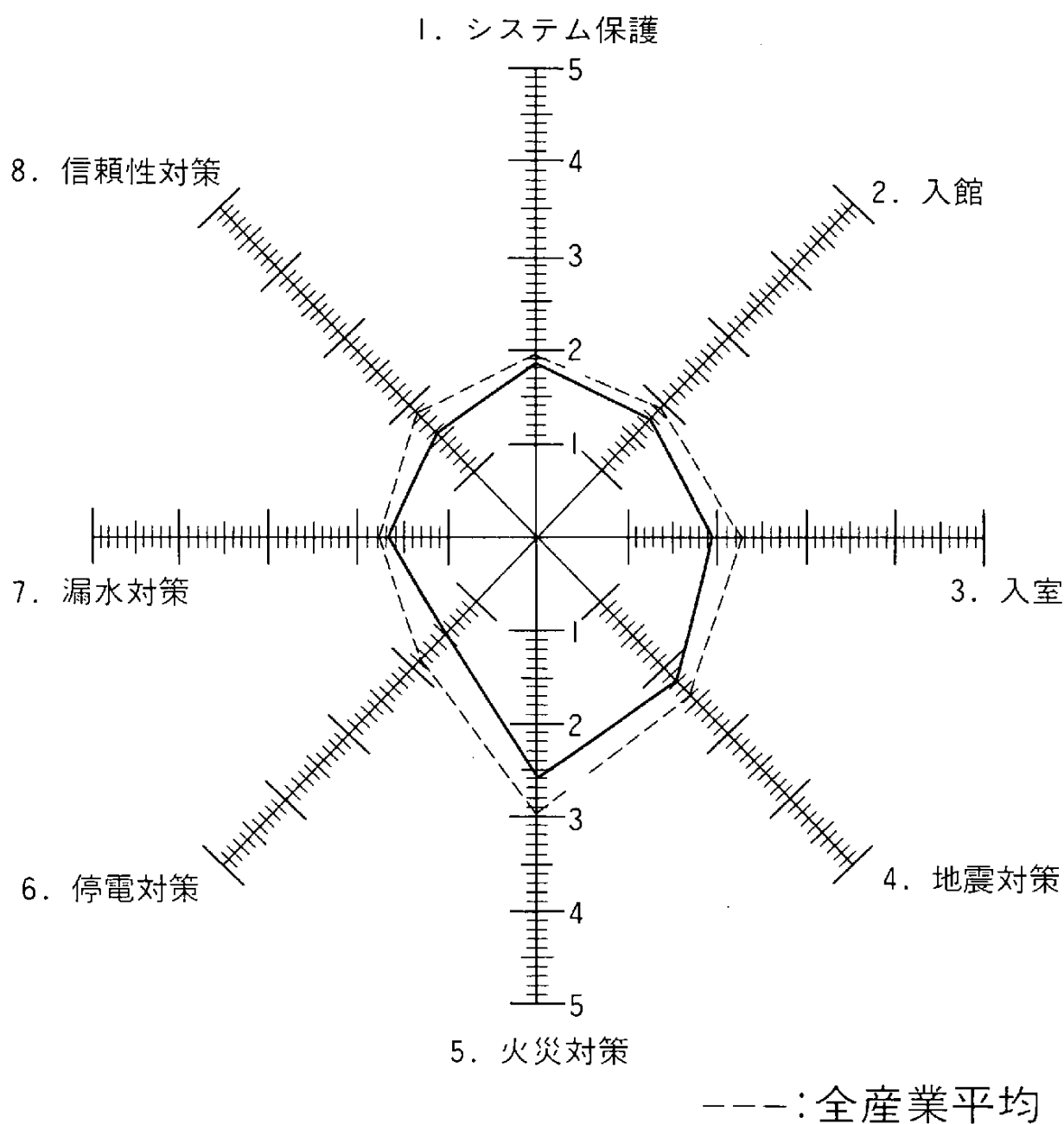
	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1. 91	1. 95	2. 27	2. 40	2. 97	1. 86	1. 79	1. 85
新聞業・出版業	1. 50	1. 67	1. 60	2. 33	3. 17	2. 00	2. 00	2. 25

印刷業・同関連産業



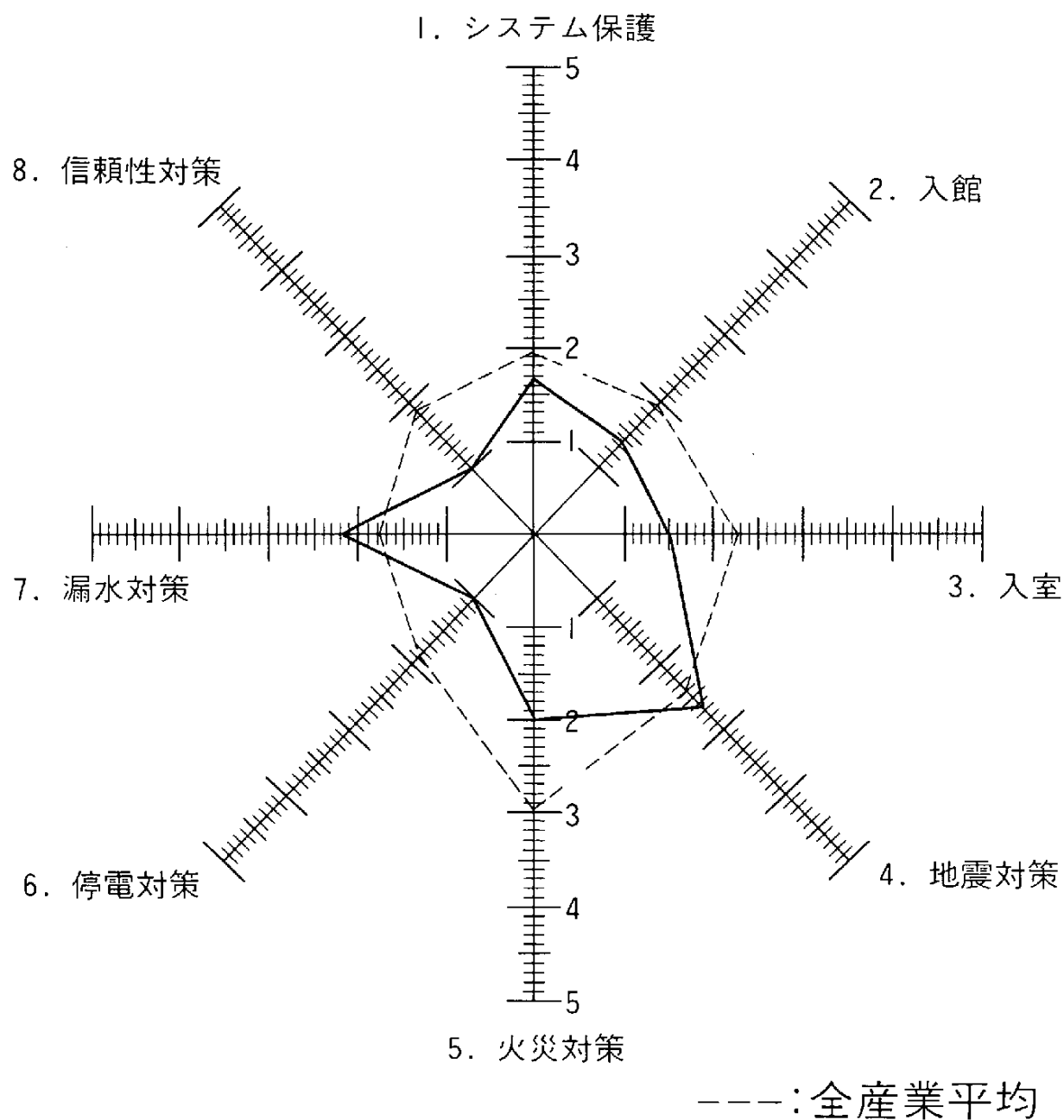
	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1.91	1.95	2.27	2.40	2.97	1.86	1.79	1.85
印刷業・同 関連産業	1.57	2.14	1.50	1.57	2.86	1.14	1.00	1.43

化学工業

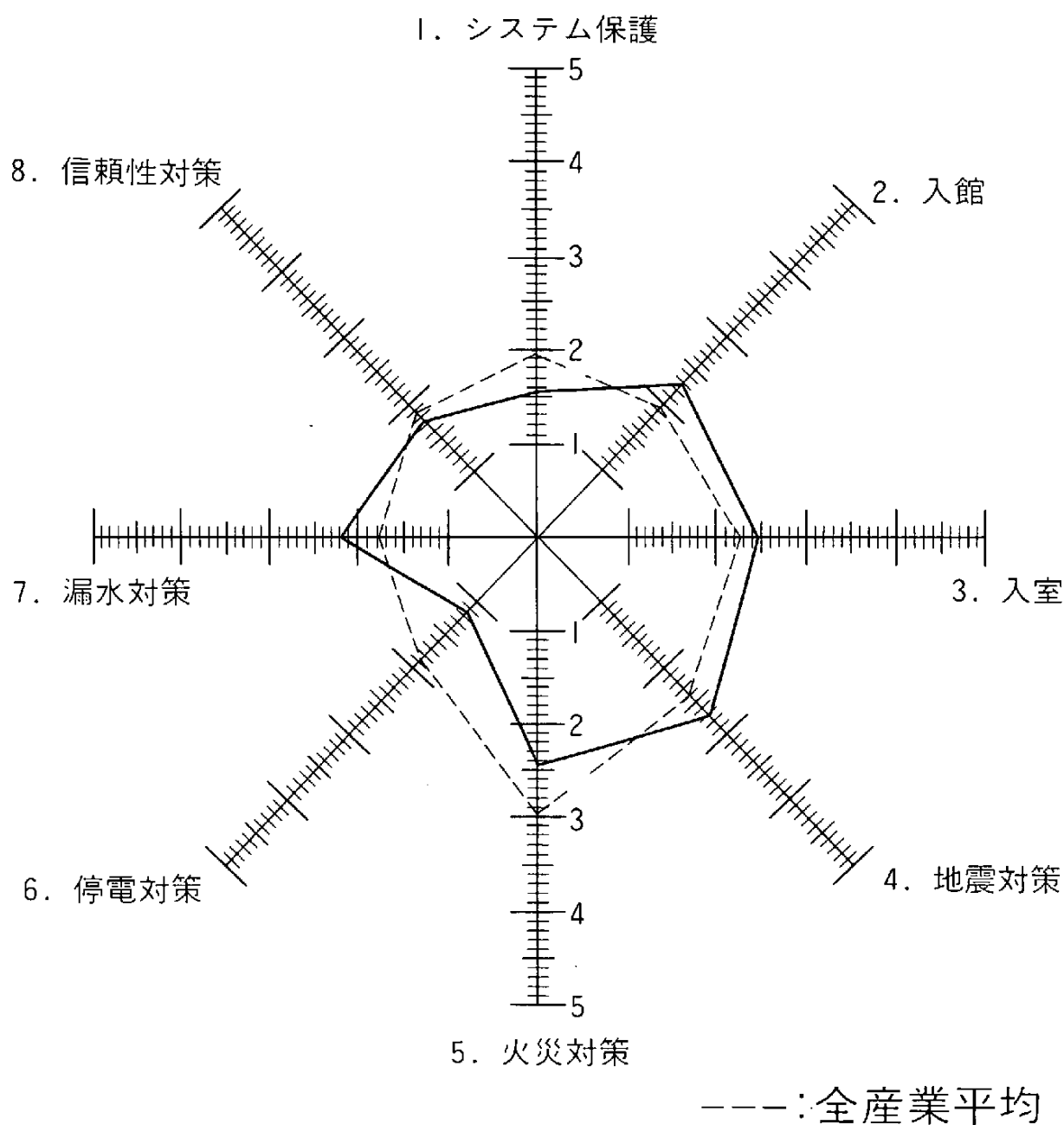


	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1.91	1.95	2.27	2.40	2.97	1.86	1.79	1.85
化学工業	1.82	1.77	1.93	2.19	2.60	1.49	1.69	1.57

石油製品製造業

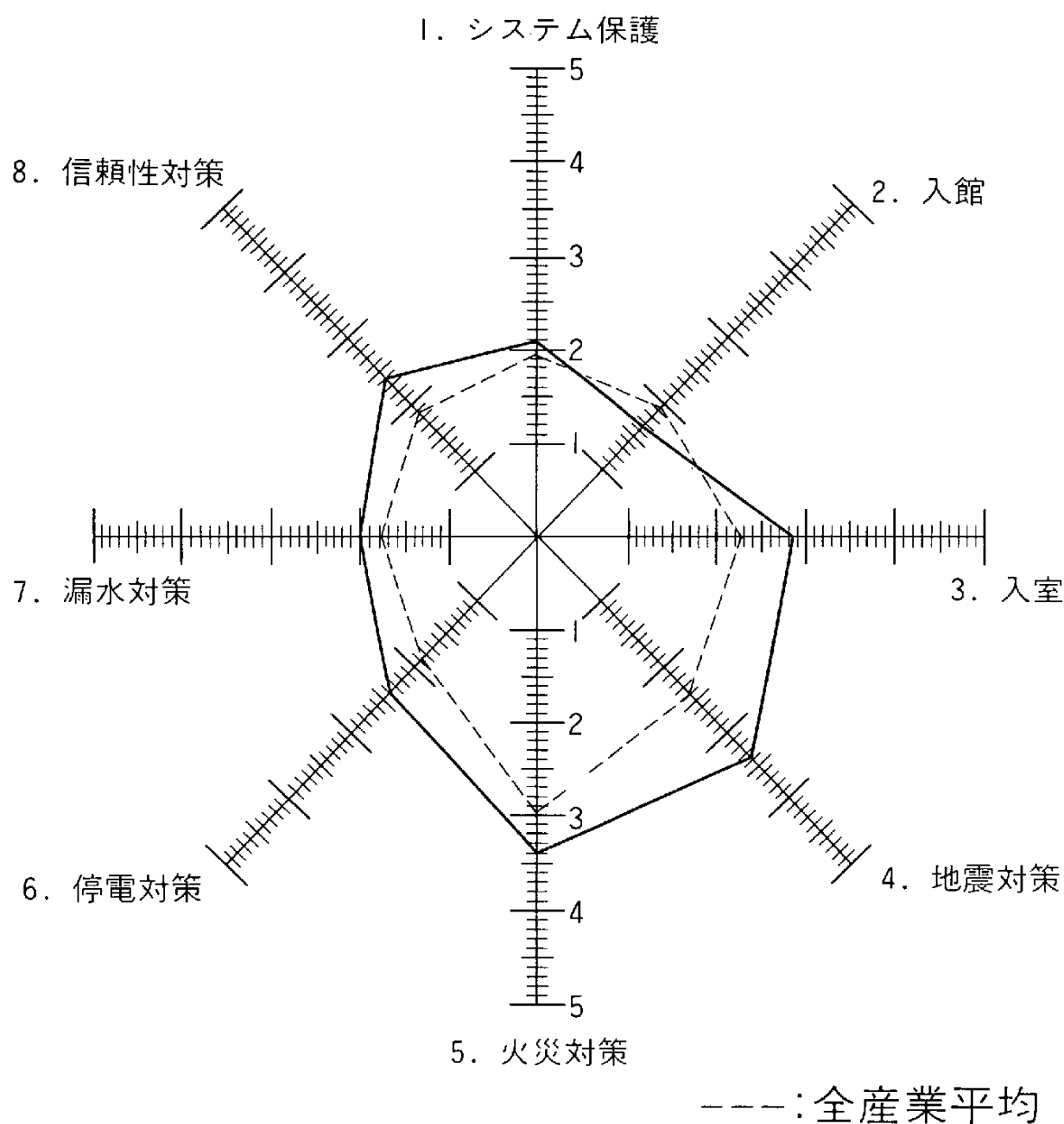


窯業・土石製品製造業



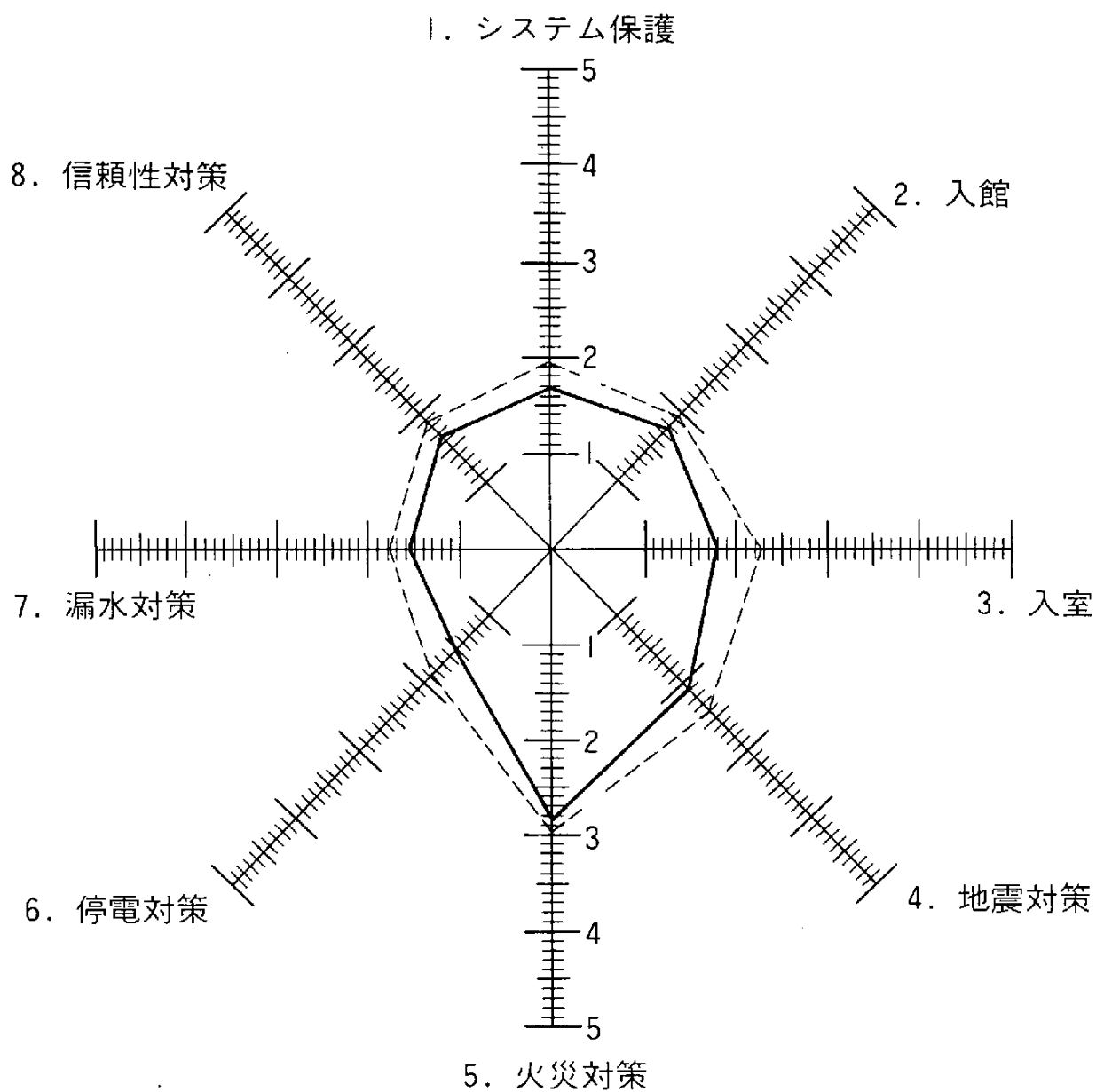
	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1.91	1.95	2.27	2.40	2.97	1.86	1.79	1.85
窯業・土石製品製造業	1.57	2.29	2.43	2.71	2.43	1.14	2.14	1.71

鉄鋼業



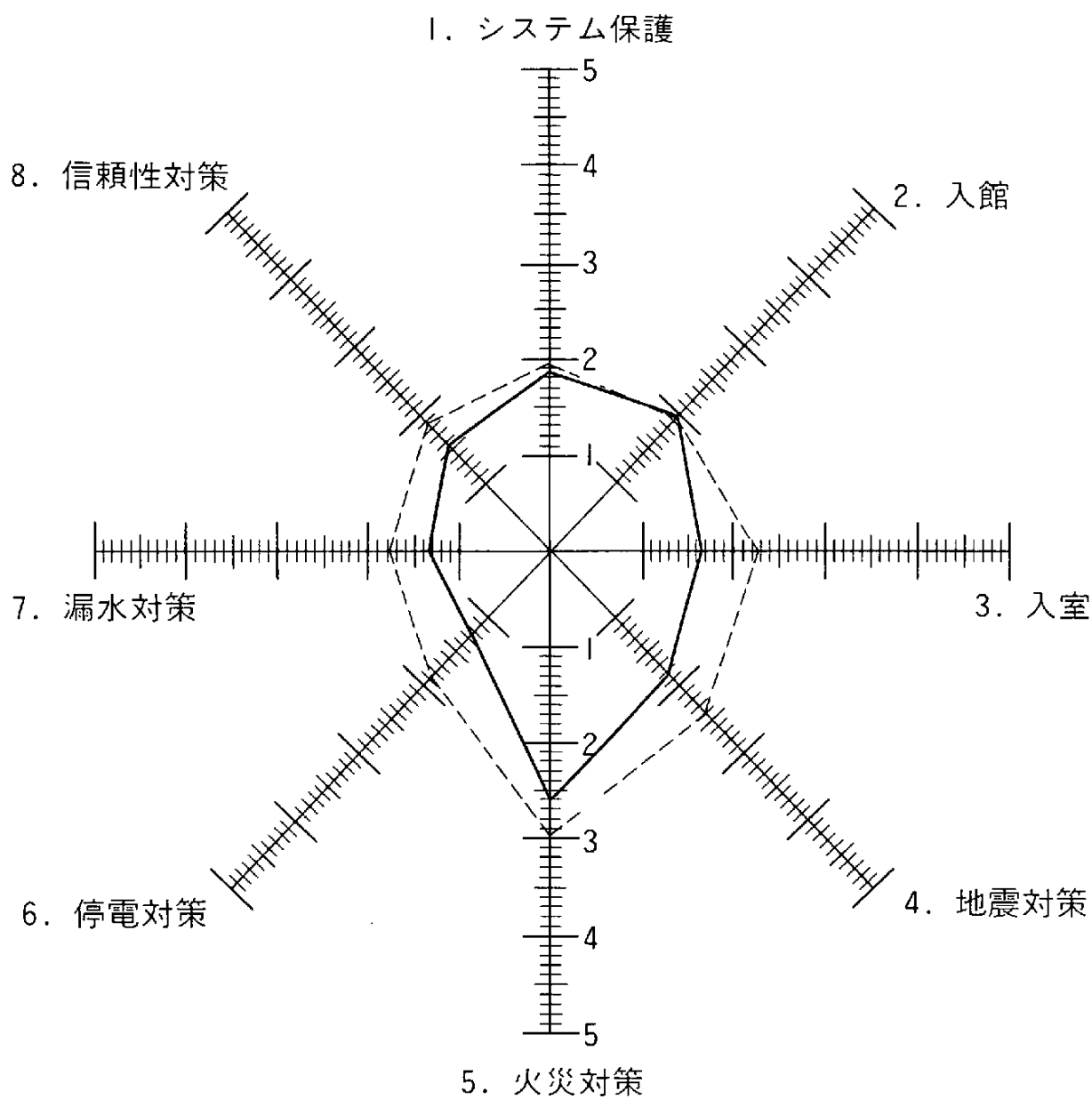
	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1.91	1.95	2.27	2.40	2.97	1.86	1.79	1.85
鉄 鋼 業	2.09	1.64	2.82	3.36	3.40	2.40	2.00	2.40

非鉄金属製造業・金属製品製造業



	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	1.91	1.95	2.27	2.40	2.97	1.86	1.79	1.85
非鉄金属製造業・金属製品製造業	1.70	1.74	1.77	2.04	2.87	1.52	1.57	1.65

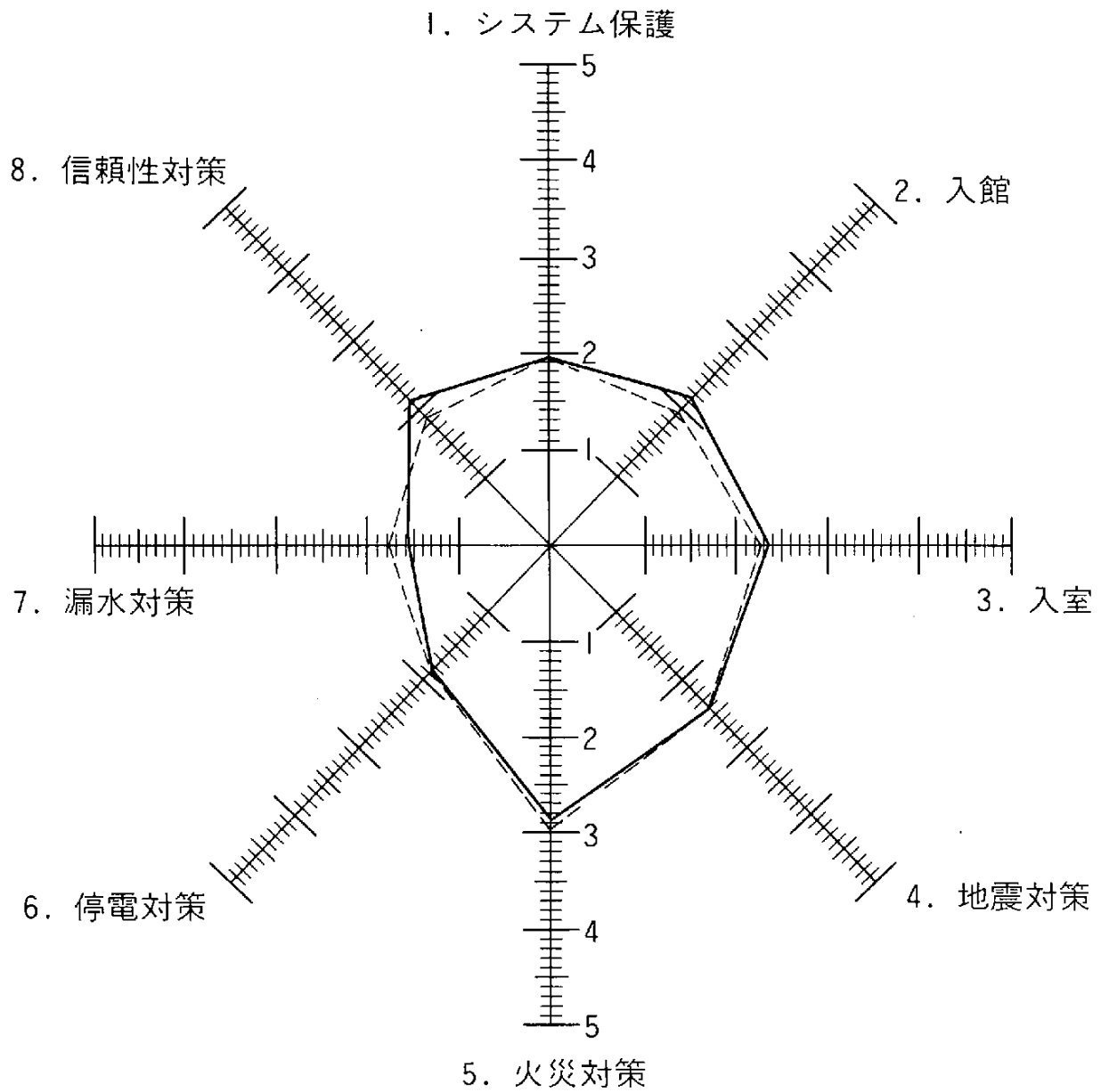
一般機械器具製造業



---: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	1.91	1.95	2.27	2.40	2.97	1.86	1.79	1.85
一般機械器具製造業	1.81	1.98	1.67	1.83	2.60	1.24	1.32	1.53

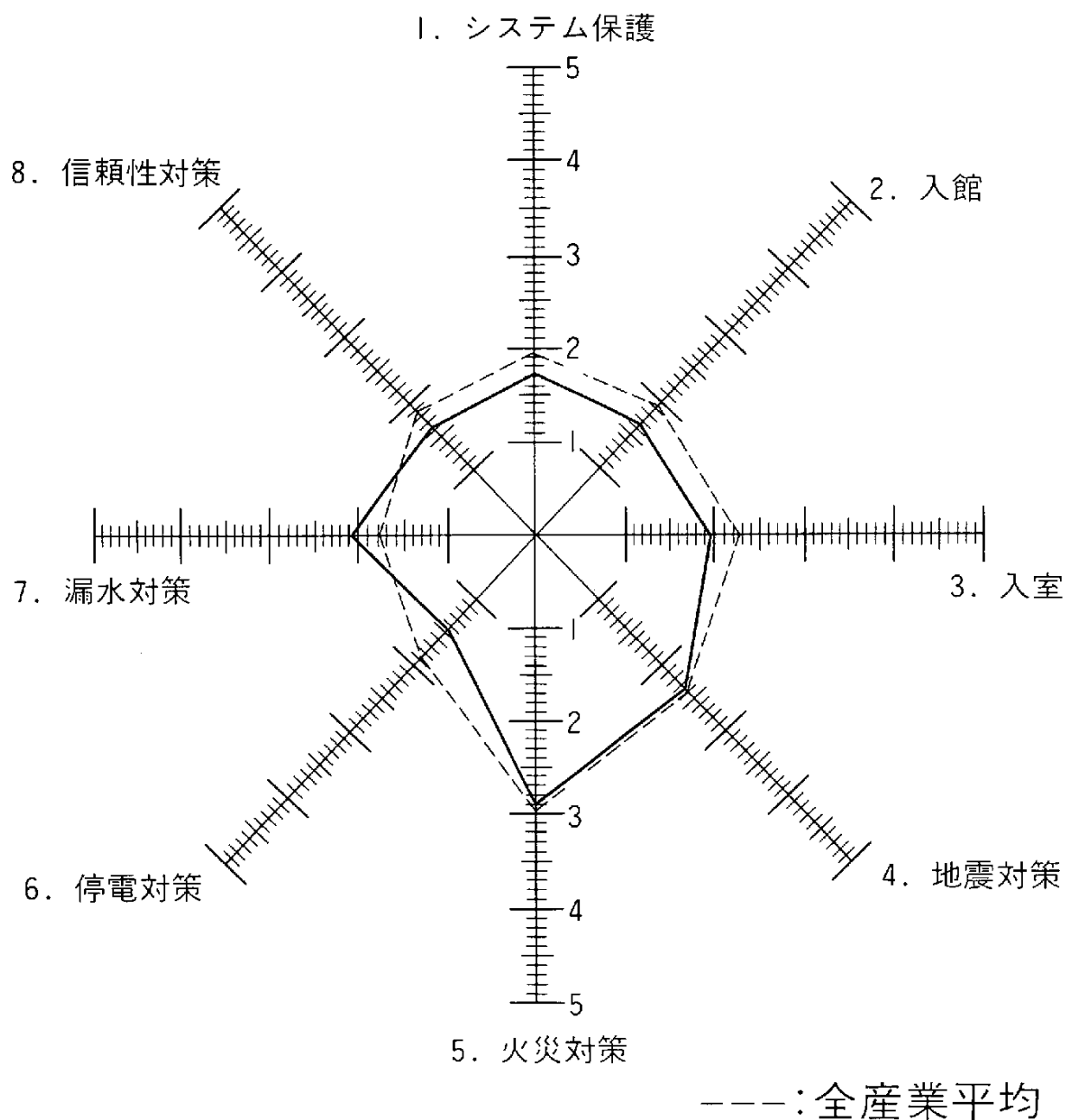
電気機械器具製造業



---: 全産業平均

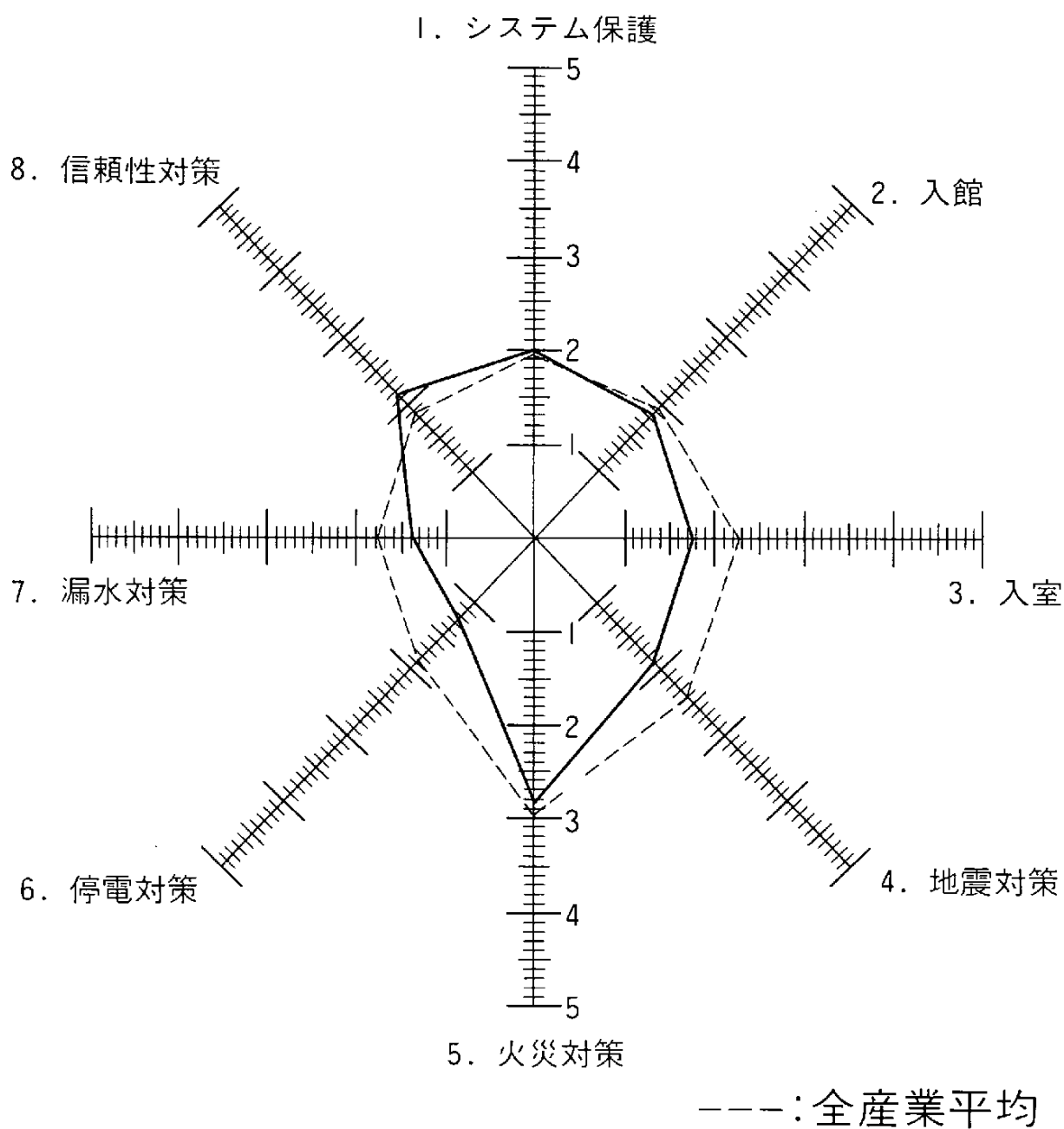
	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1. 91	1. 95	2. 27	2. 40	2. 97	1. 86	1. 79	1. 85
電気機械器具製造業	1. 94	2. 15	2. 33	2. 40	2. 85	1. 85	1. 55	2. 11

輸送用機械器具製造業



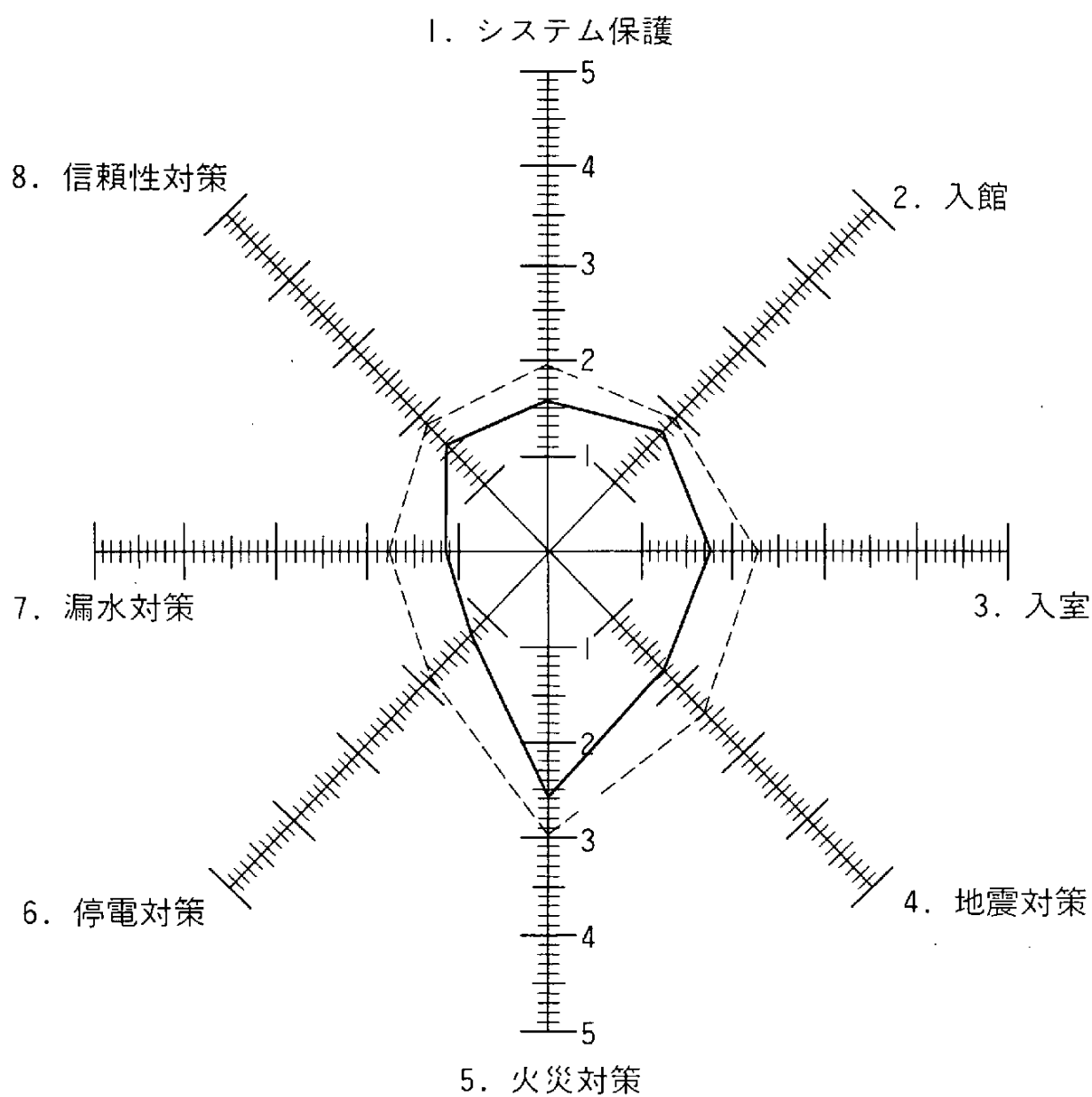
	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1. 91	1. 95	2. 27	2. 40	2. 97	1. 86	1. 79	1. 85
輸送用機械器具製造業	1. 71	1. 65	1. 94	2. 31	2. 89	1. 46	2. 03	1. 63

精密機械器具製造業



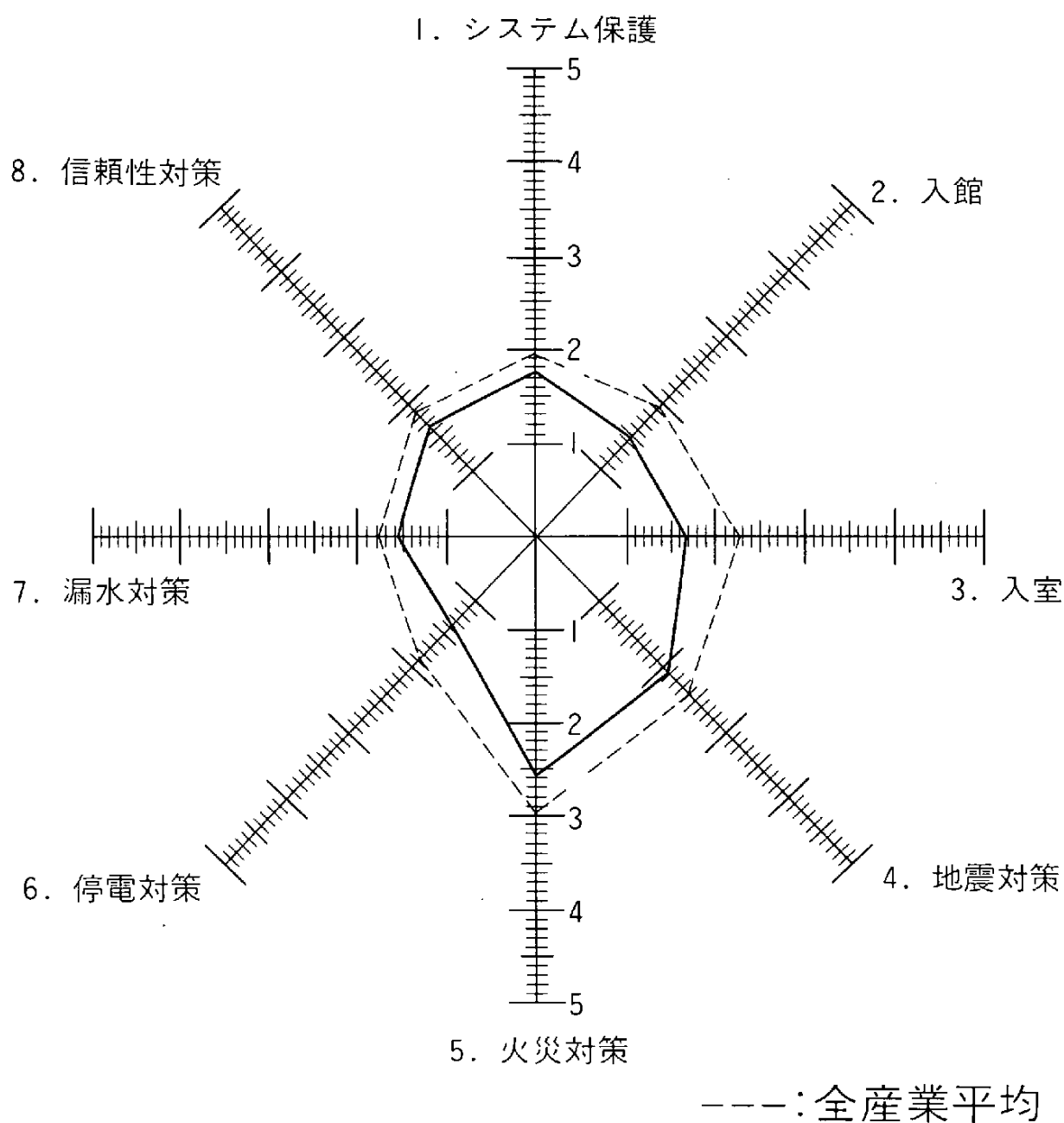
	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1. 91	1. 95	2. 27	2. 40	2. 97	1. 86	1. 79	1. 85
精密機械器具製造業	2. 00	1. 81	1. 75	1. 88	2. 81	1. 25	1. 38	2. 13

その他の製造業



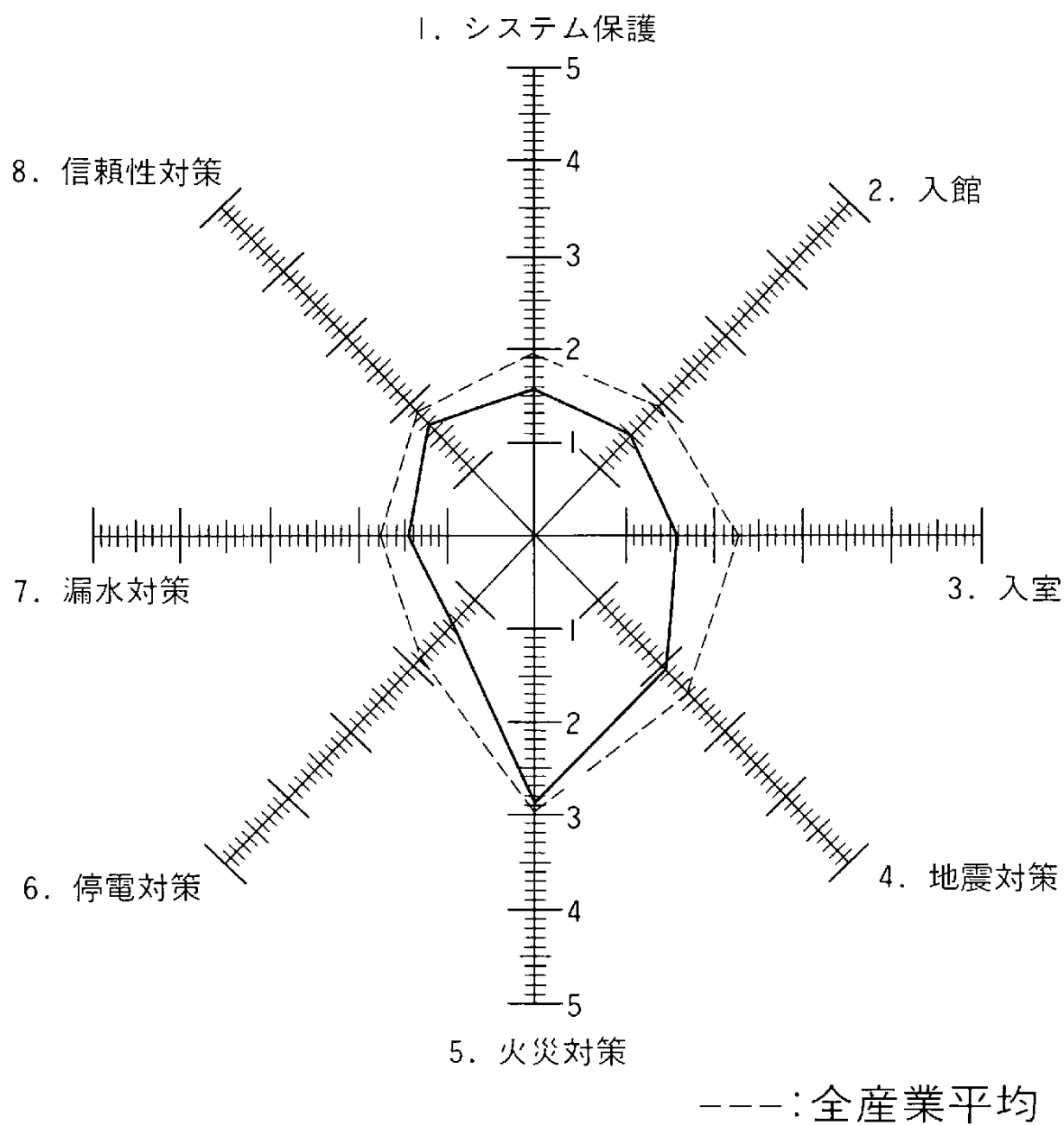
	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1. 91	1. 95	2. 27	2. 40	2. 97	1. 86	1. 79	1. 85
その他の製造業	1. 58	1. 73	1. 78	1. 78	2. 56	1. 22	1. 13	1. 55

卸業・商社



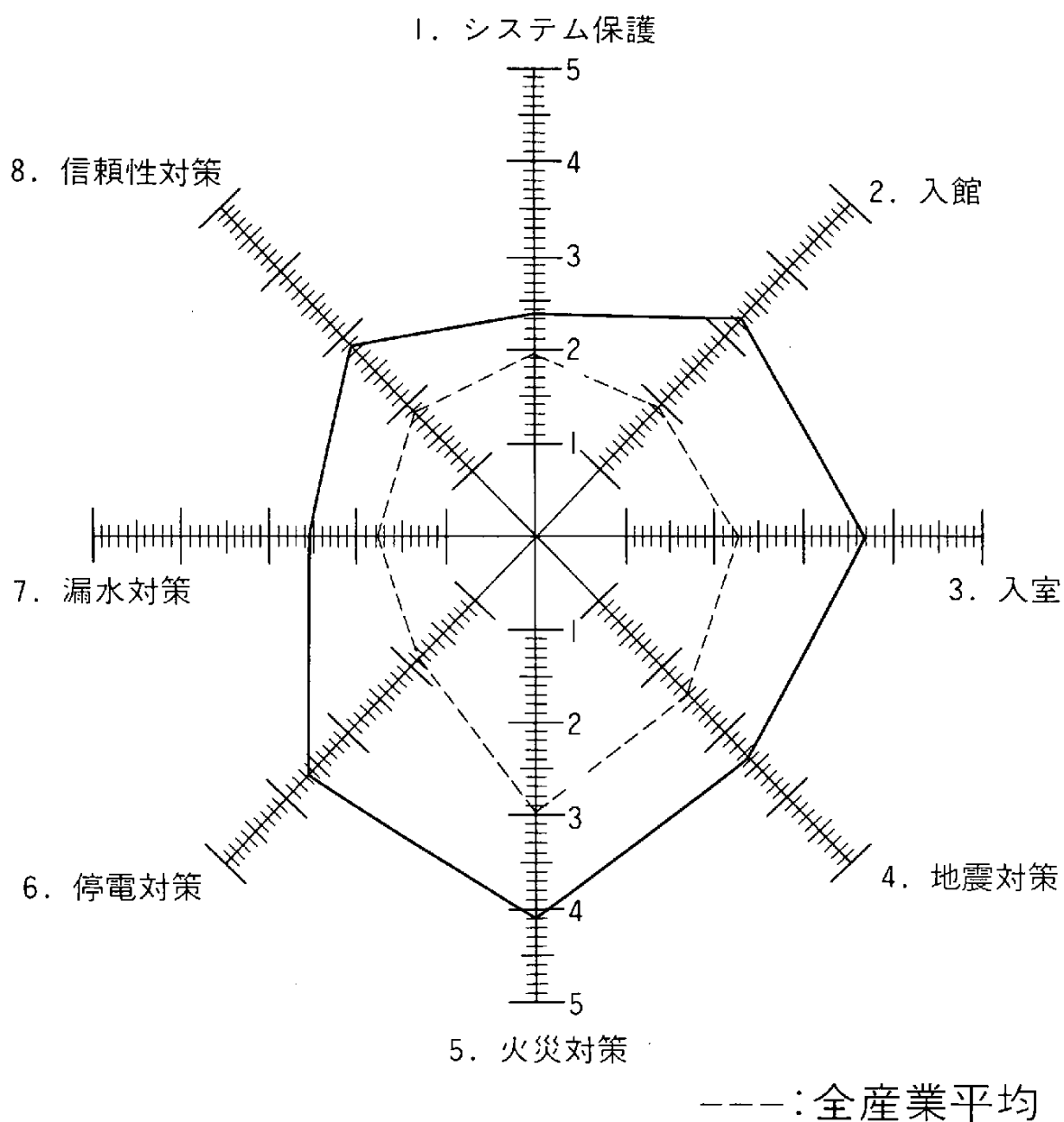
	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1.91	1.95	2.27	2.40	2.97	1.86	1.79	1.85
卸業・商社	1.73	1.49	1.66	2.06	2.56	1.39	1.56	1.63

小 売 業

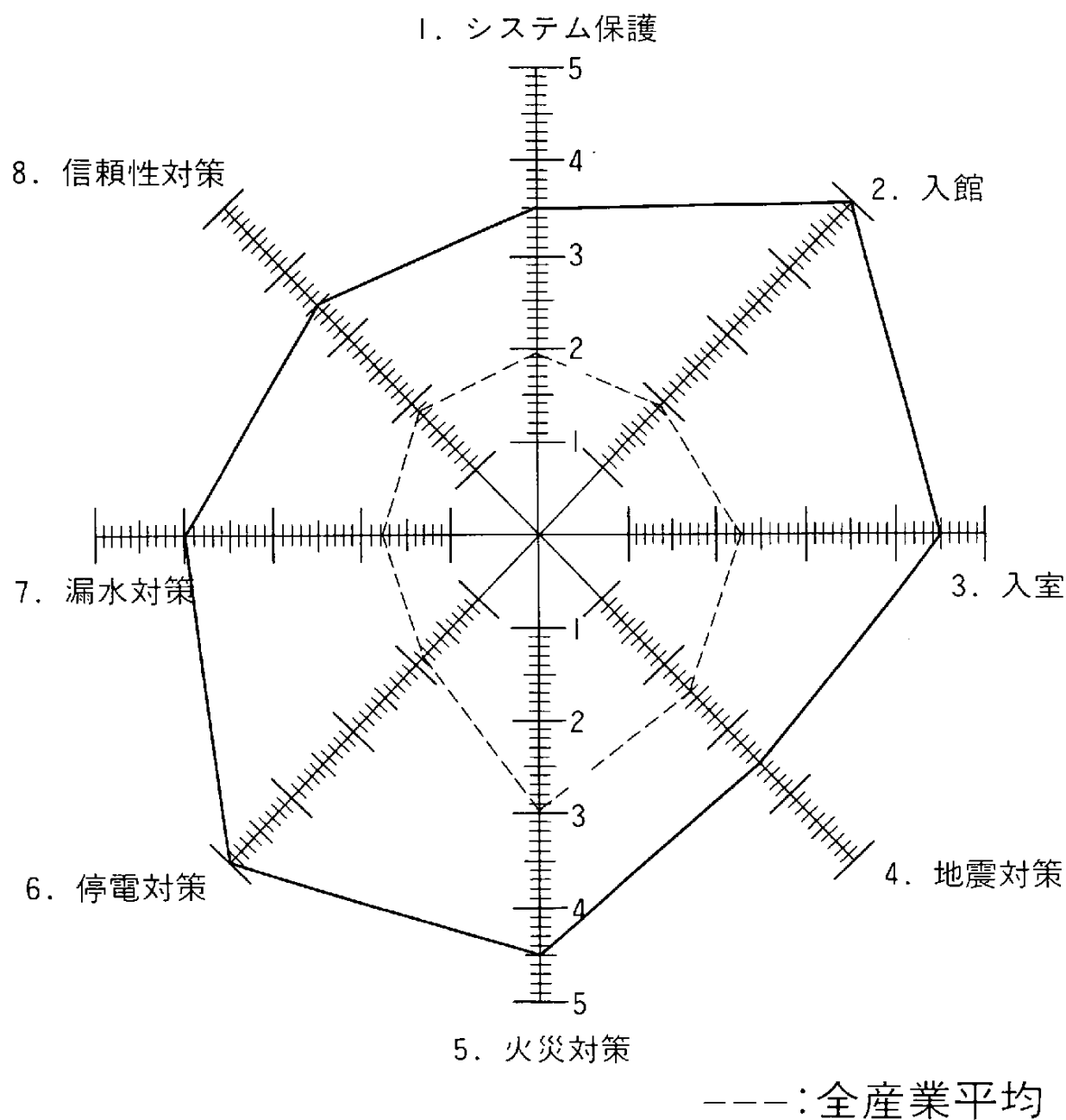


	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1.91	1.95	2.27	2.40	2.97	1.86	1.79	1.85
小 売 業	1.59	1.50	1.58	2.02	2.85	1.39	1.44	1.69

金融業

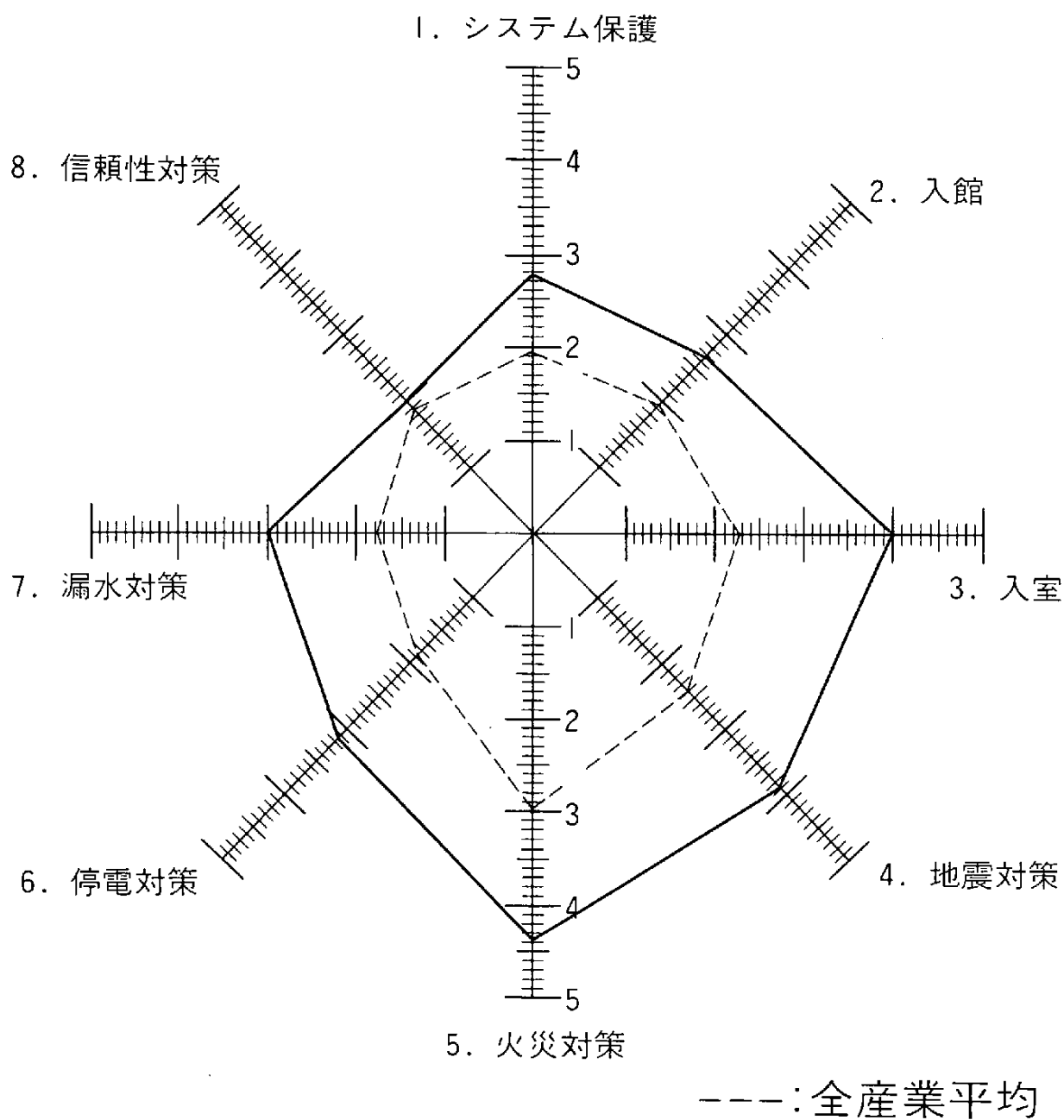


証券業・商品取引業

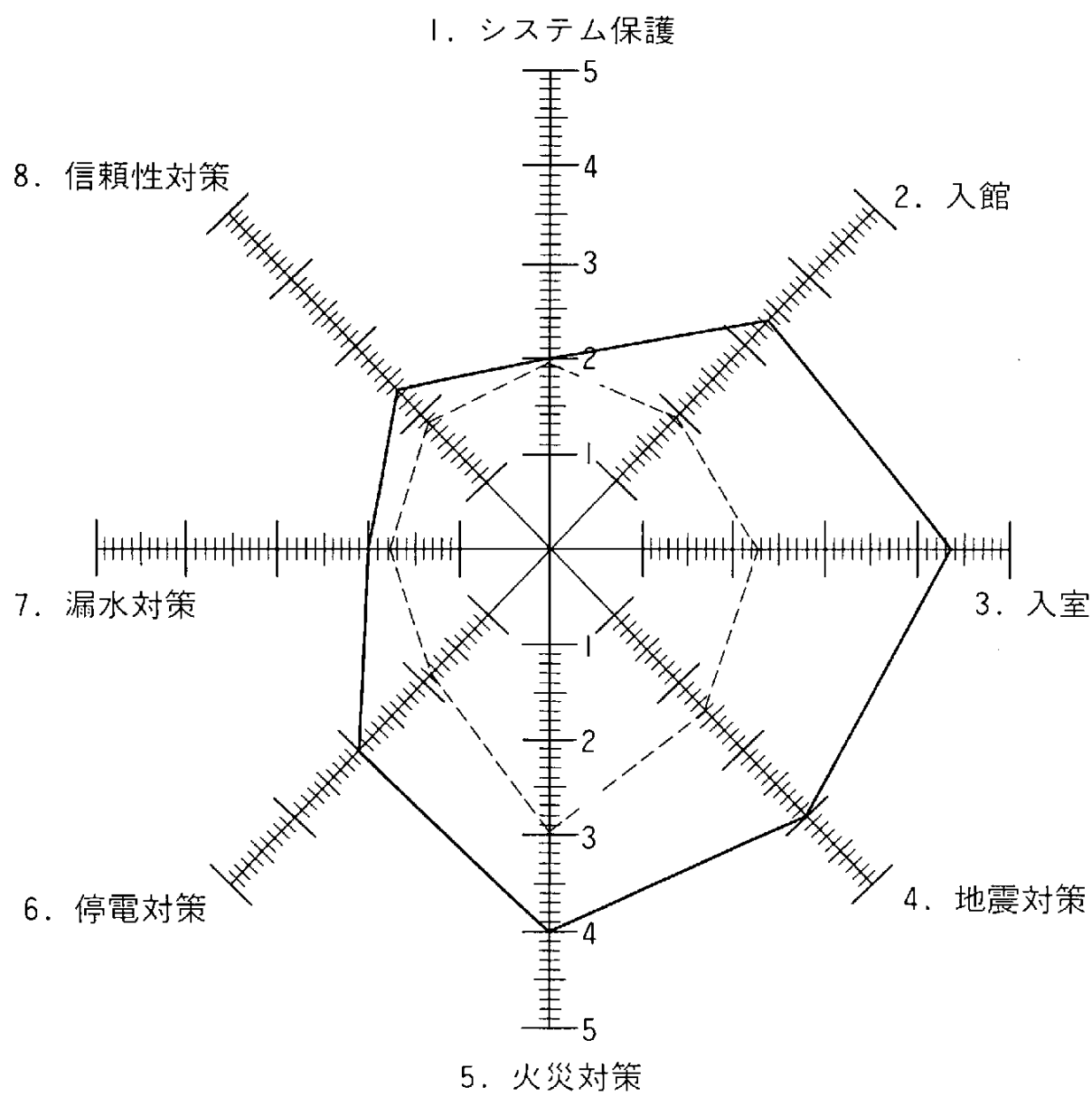


	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1. 91	1. 95	2. 27	2. 40	2. 97	1. 86	1. 79	1. 85
証券業・商品取引業	3. 50	5. 00	4. 50	3. 50	4. 50	5. 00	4. 00	3. 50

生命保険業(含代理業・サービス業)

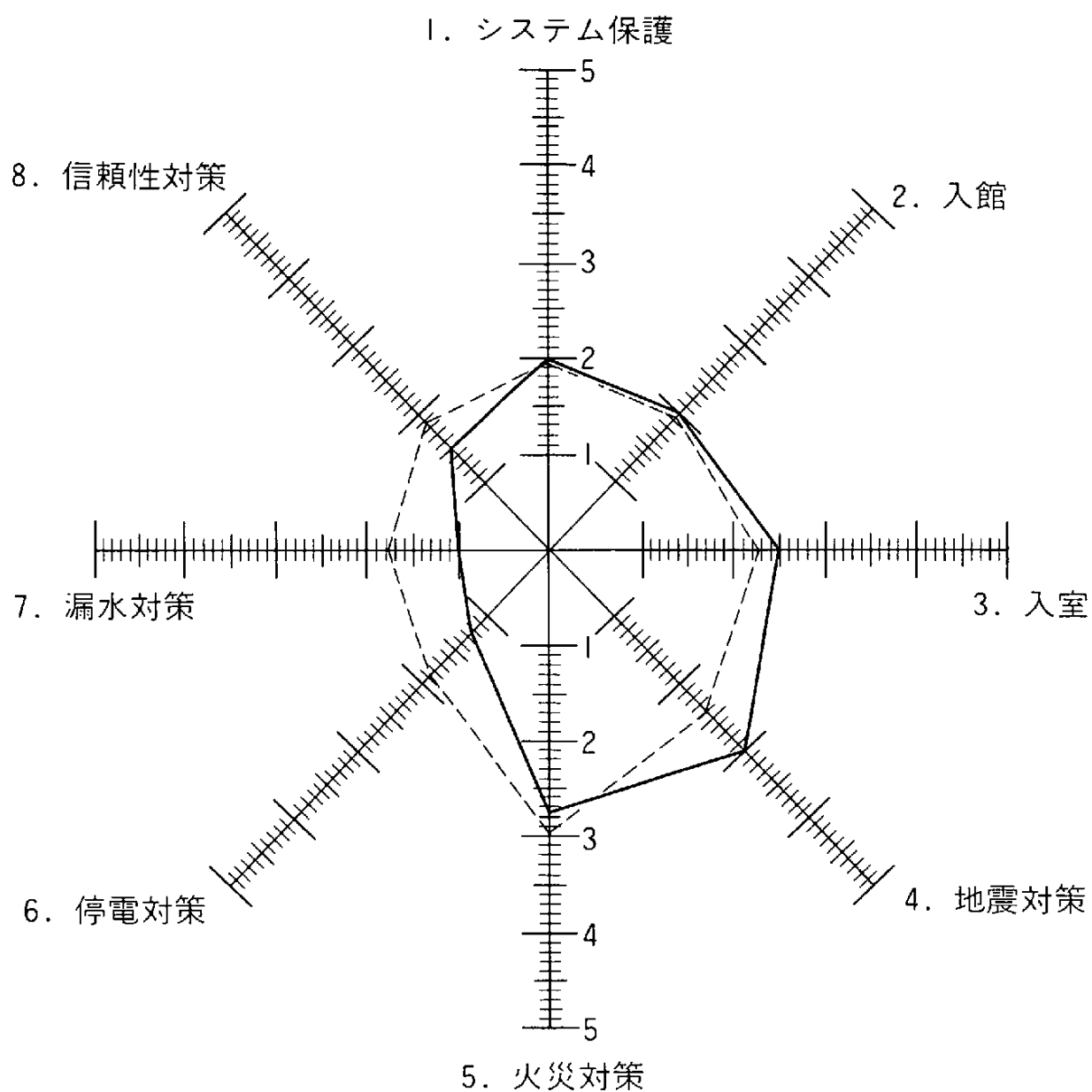


損害保険業(含代理業・サービス業)



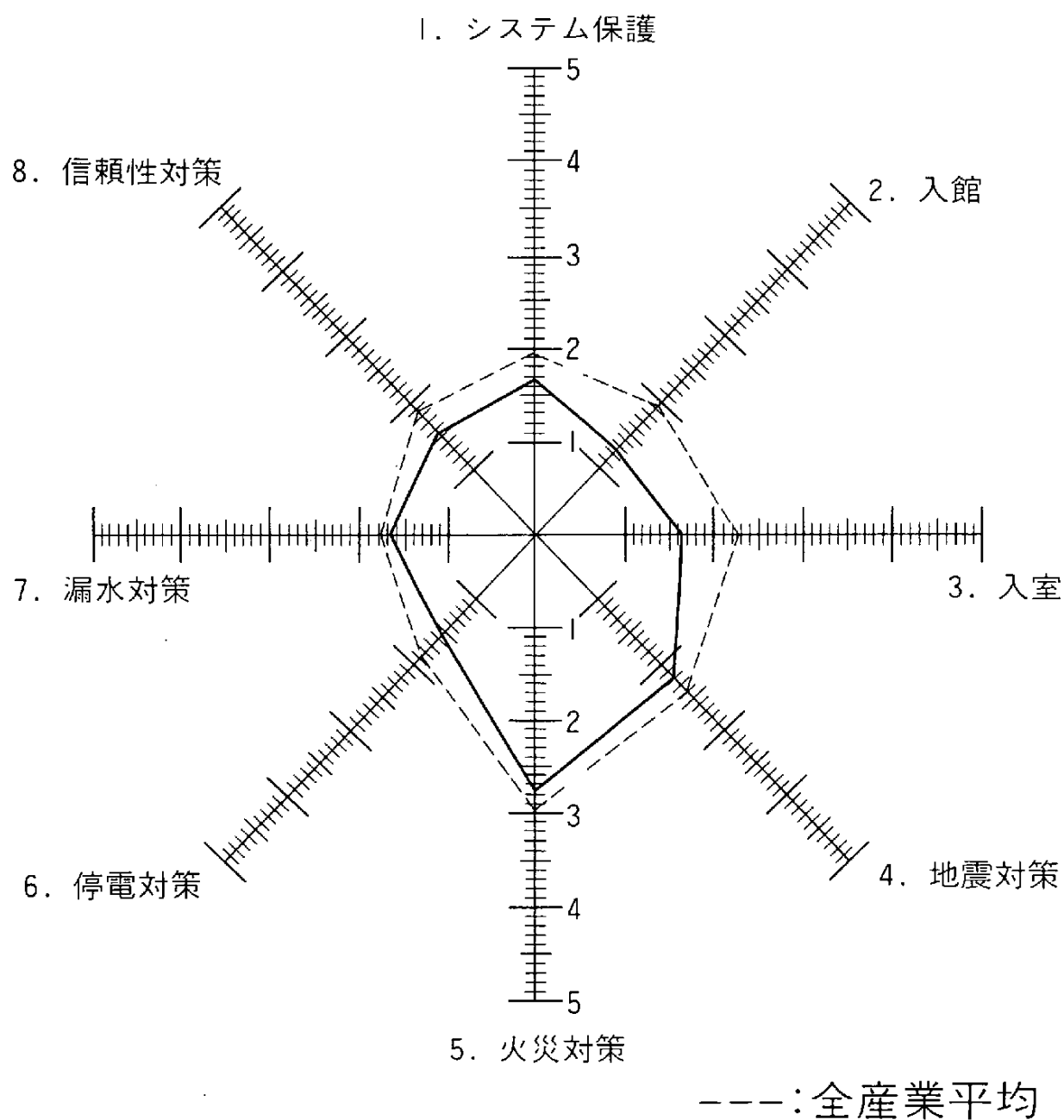
	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1. 91	1. 95	2. 27	2. 40	2. 97	1. 86	1. 79	1. 85
損害保険業 (含代理業・サービス業)	2. 00	3. 33	4. 33	4. 00	4. 00	3. 00	2. 00	2. 33

不動産業



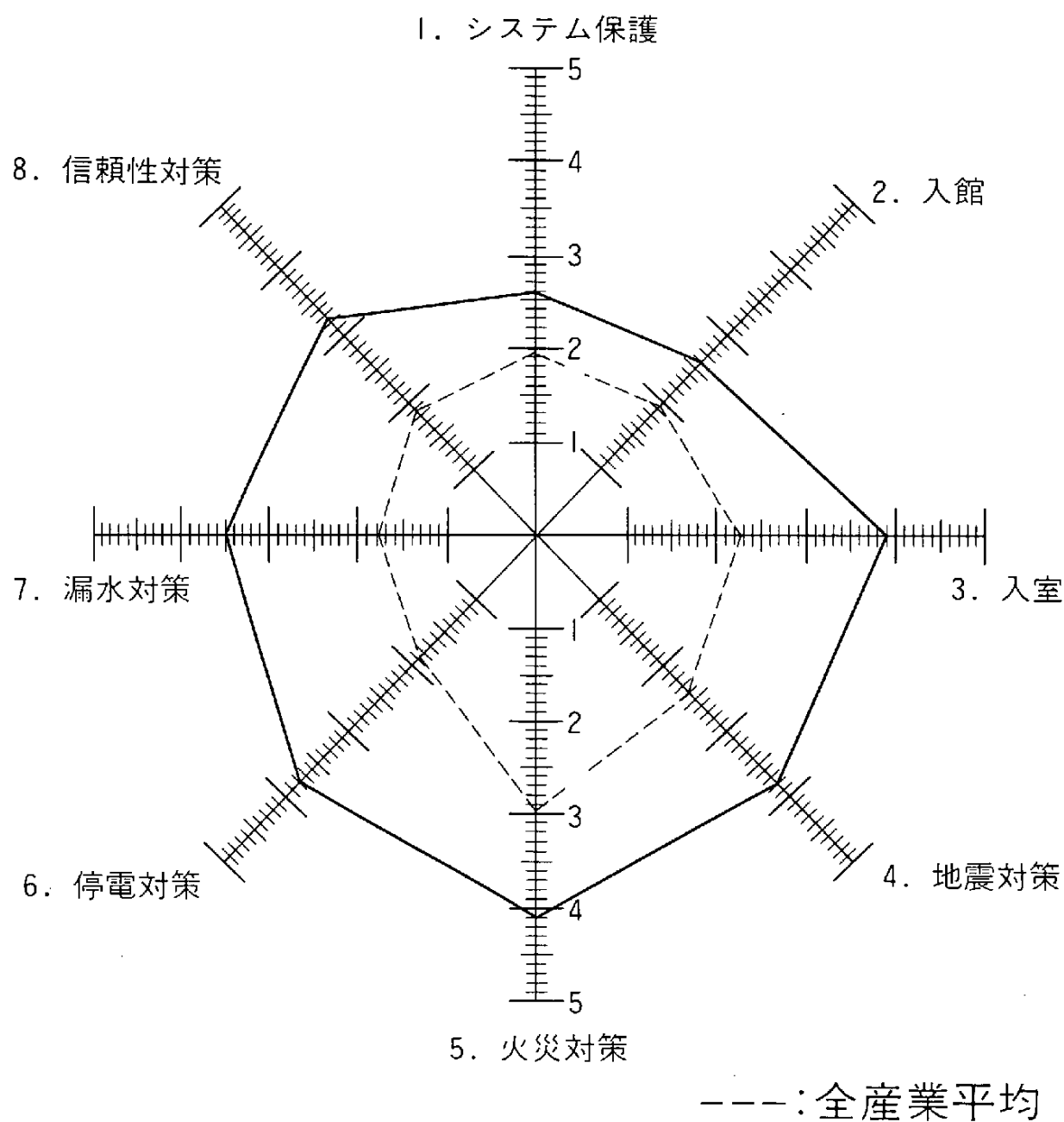
	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1.91	1.95	2.27	2.40	2.97	1.86	1.79	1.85
不動産業	2.00	2.00	2.50	3.00	2.75	1.25	1.00	1.50

運輸・通信・倉庫業



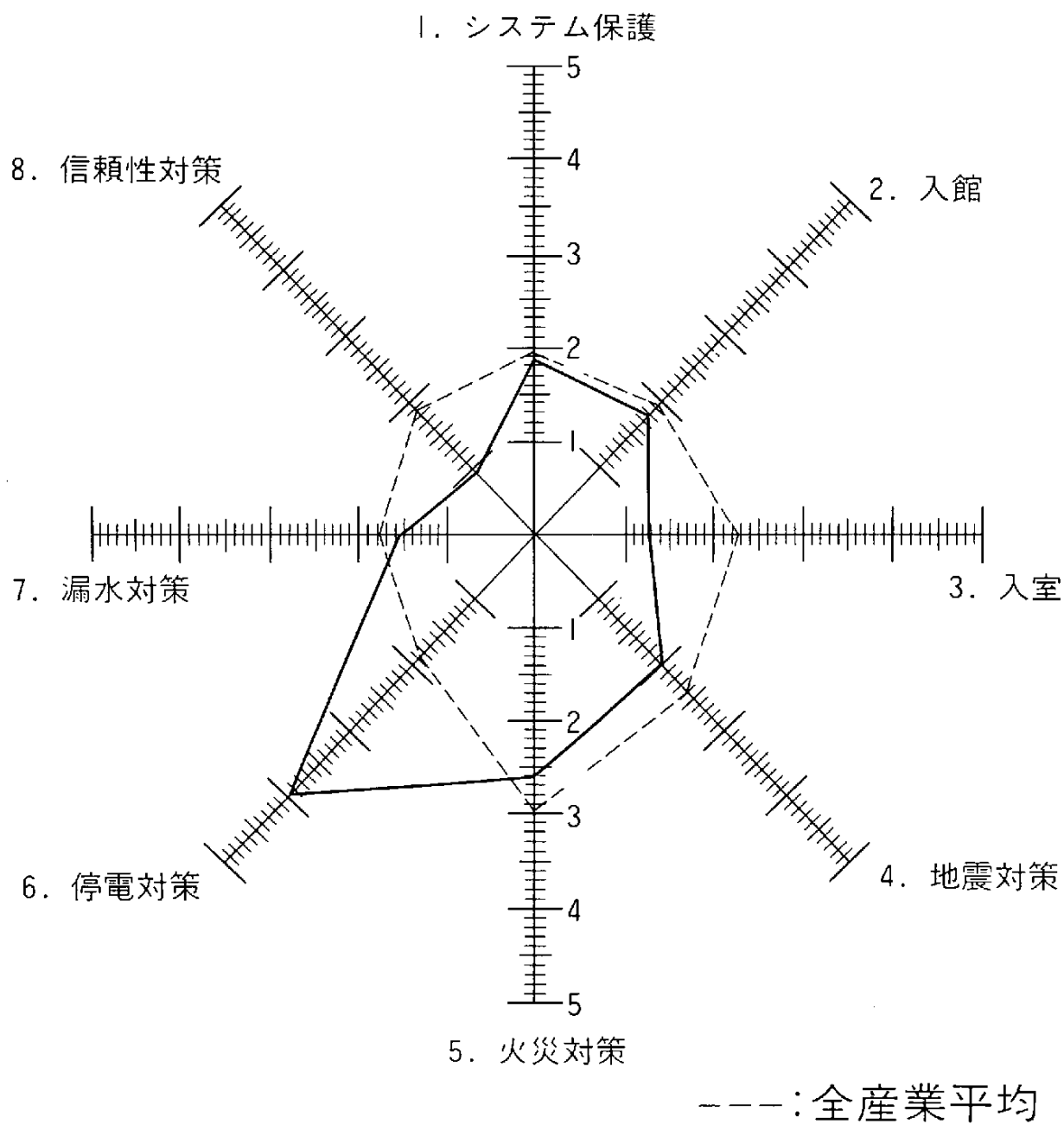
	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1. 91	1. 95	2. 27	2. 40	2. 97	1. 86	1. 79	1. 85
運輸・通信・倉庫業	1. 67	1. 24	1. 61	2. 15	2. 73	1. 55	1. 64	1. 53

電力・ガス事業



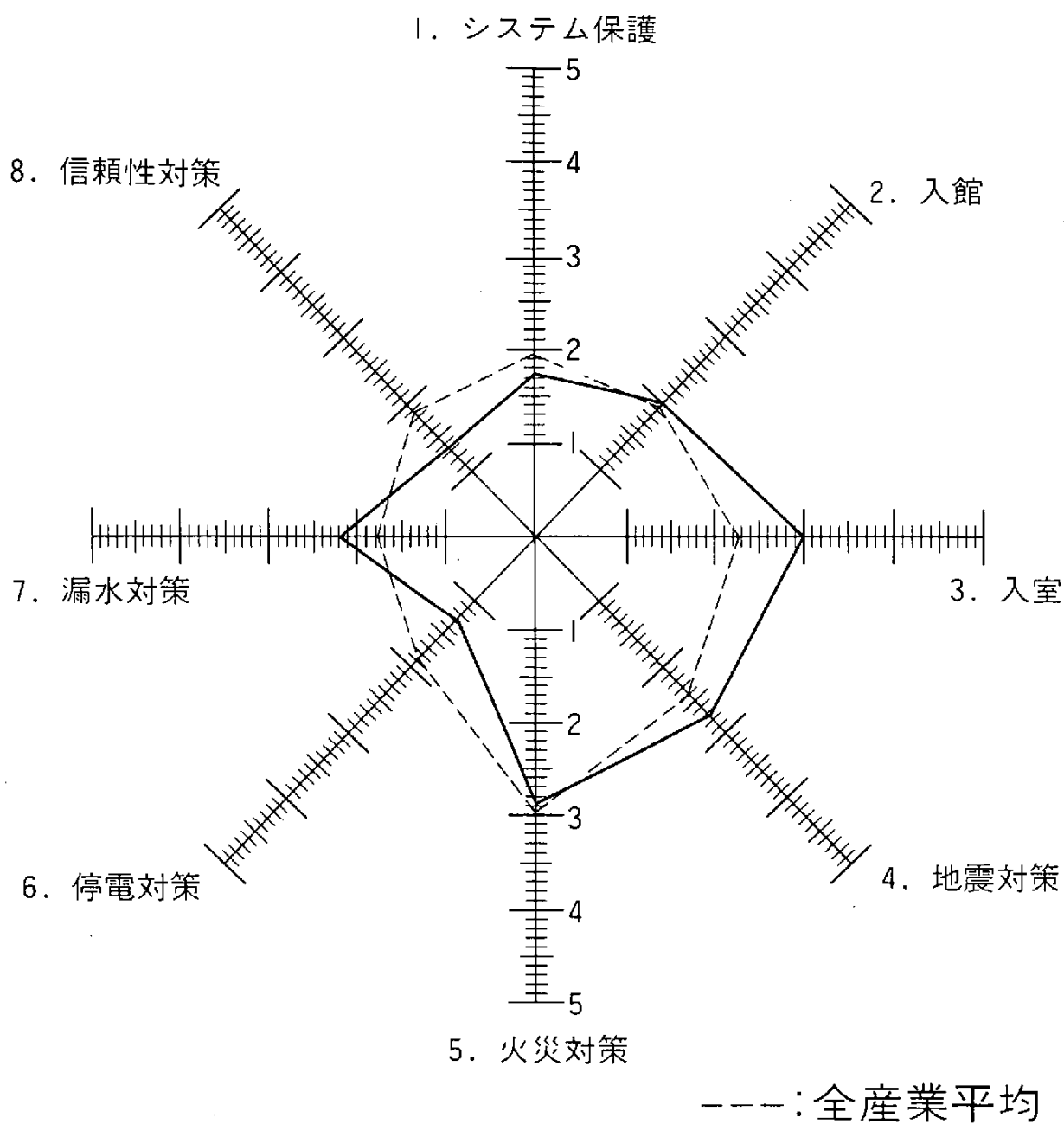
	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1. 91	1. 95	2. 27	2. 40	2. 97	1. 86	1. 79	1. 85
電力・ガス事業	2. 60	2. 60	3. 90	3. 80	4. 10	3. 80	3. 50	3. 22

放 送 業



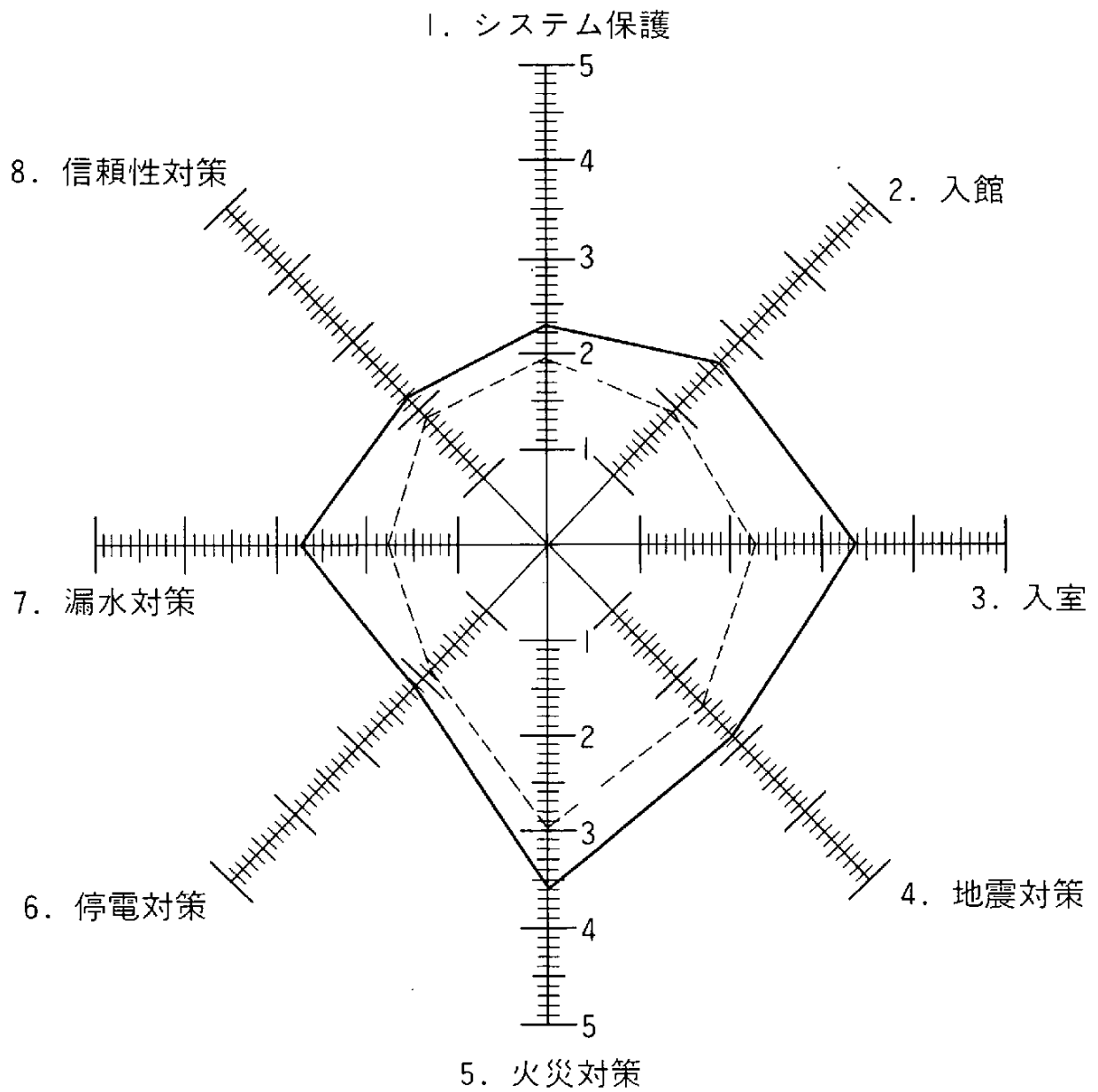
	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1. 91	1. 95	2. 27	2. 40	2. 97	1. 86	1. 79	1. 85
放 送 業	1. 86	1. 79	1. 29	2. 00	2. 60	3. 93	1. 57	0. 93

広告・調査・情報提供サービス業



	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. 91	1. 95	2. 27	2. 40	2. 97	1. 86	1. 79	1. 85
広告・調査・情報提供サービス業	1. 71	2. 00	3. 00	2. 71	2. 86	1. 29	2. 14	1. 33

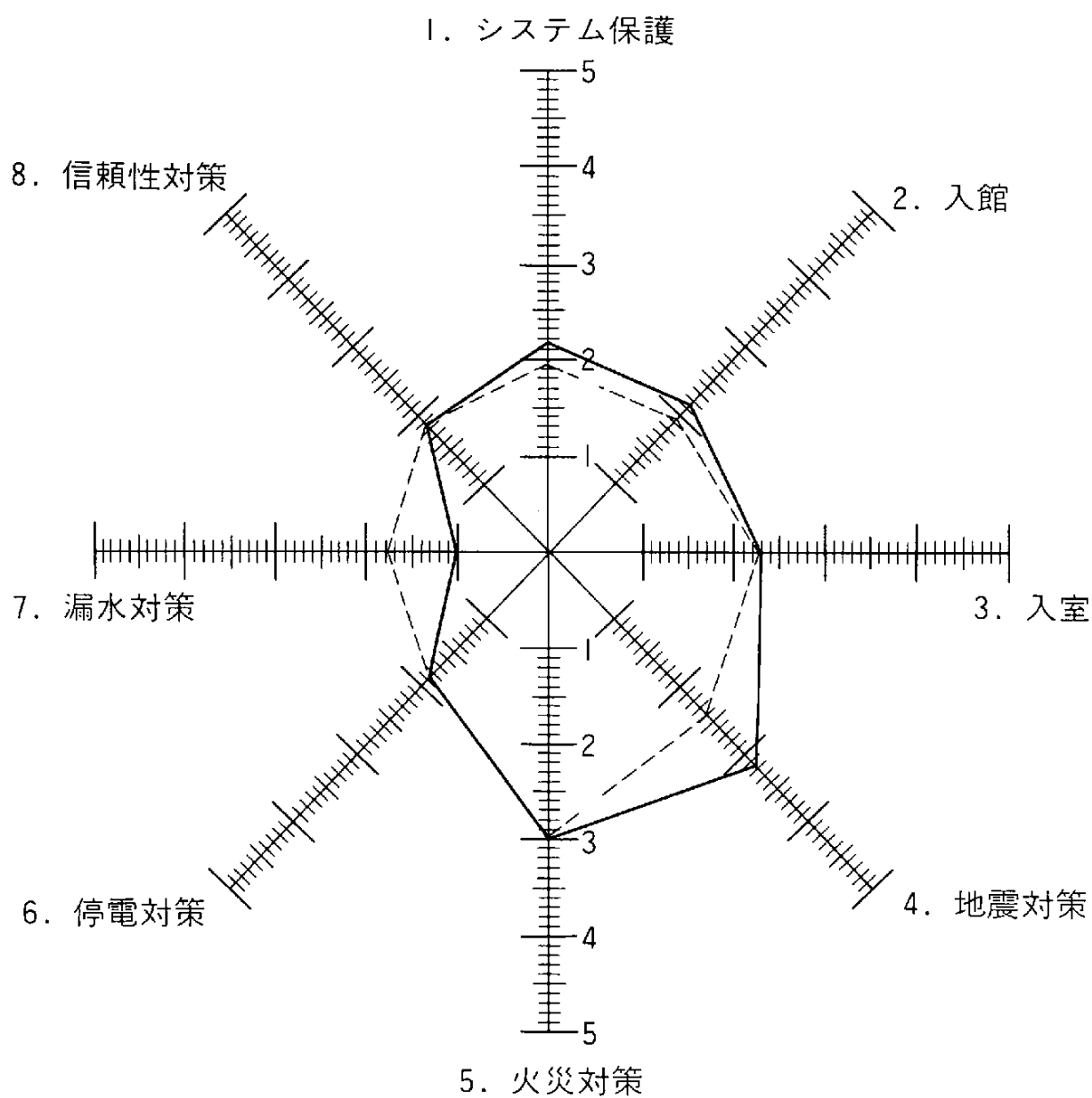
情報処理サービス業・ソフトウェア業



---:全産業平均

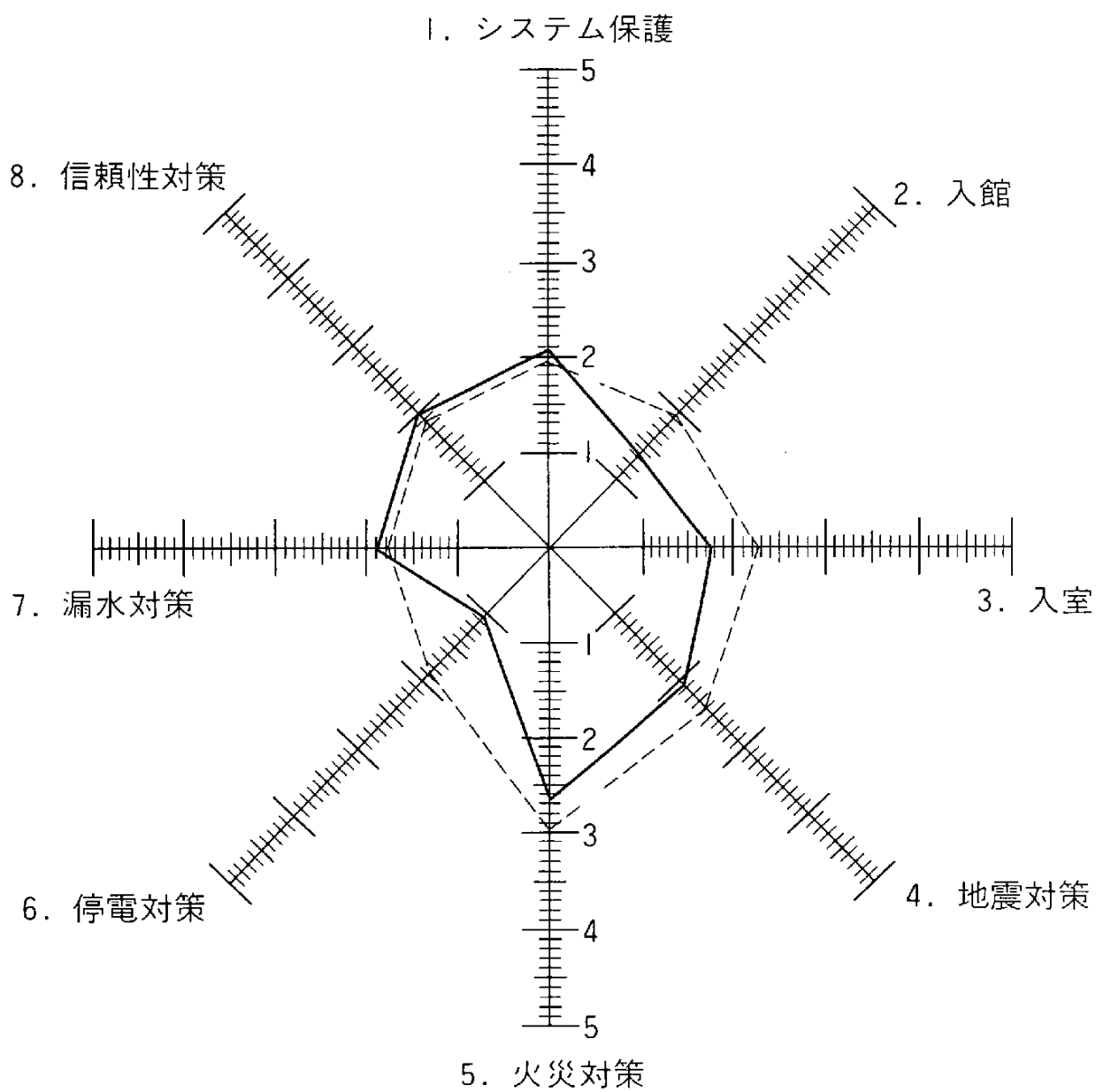
	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1. 91	1. 95	2. 27	2. 40	2. 97	1. 86	1. 79	1. 85
情報処理サービス業・ソフトウェア業	2. 24	2. 66	3. 34	2. 85	3. 60	2. 11	2. 71	2. 19

医 療 業



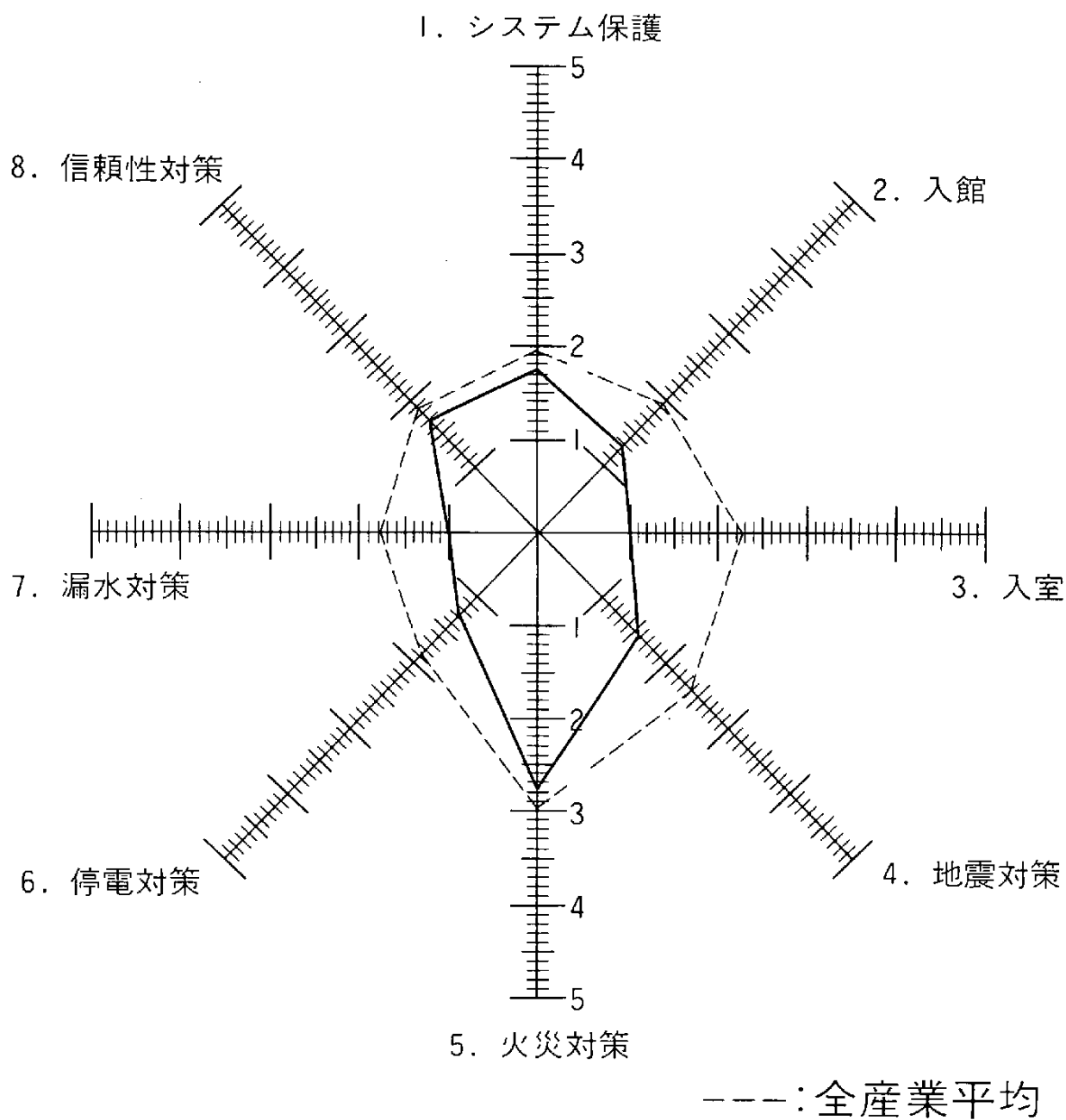
	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1.91	1.95	2.27	2.40	2.97	1.86	1.79	1.85
医 療 業	2.14	2.14	2.29	3.14	3.00	1.86	1.00	1.86

大 学



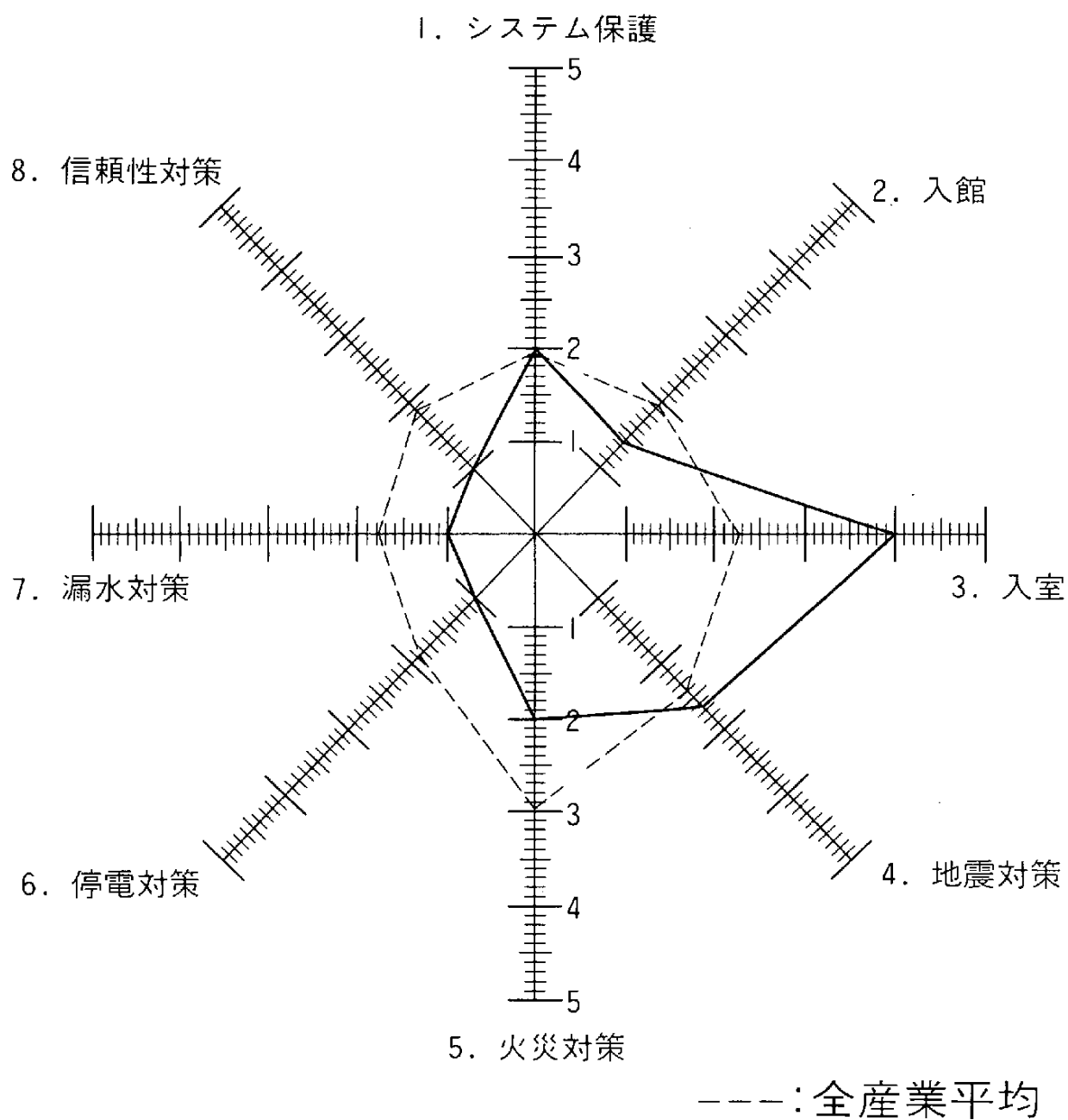
	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1. 91	1. 95	2. 27	2. 40	2. 97	1. 86	1. 79	1. 85
大 学	2. 05	1. 32	1. 77	2. 05	2. 64	1. 05	1. 90	2. 00

その他の教育機関



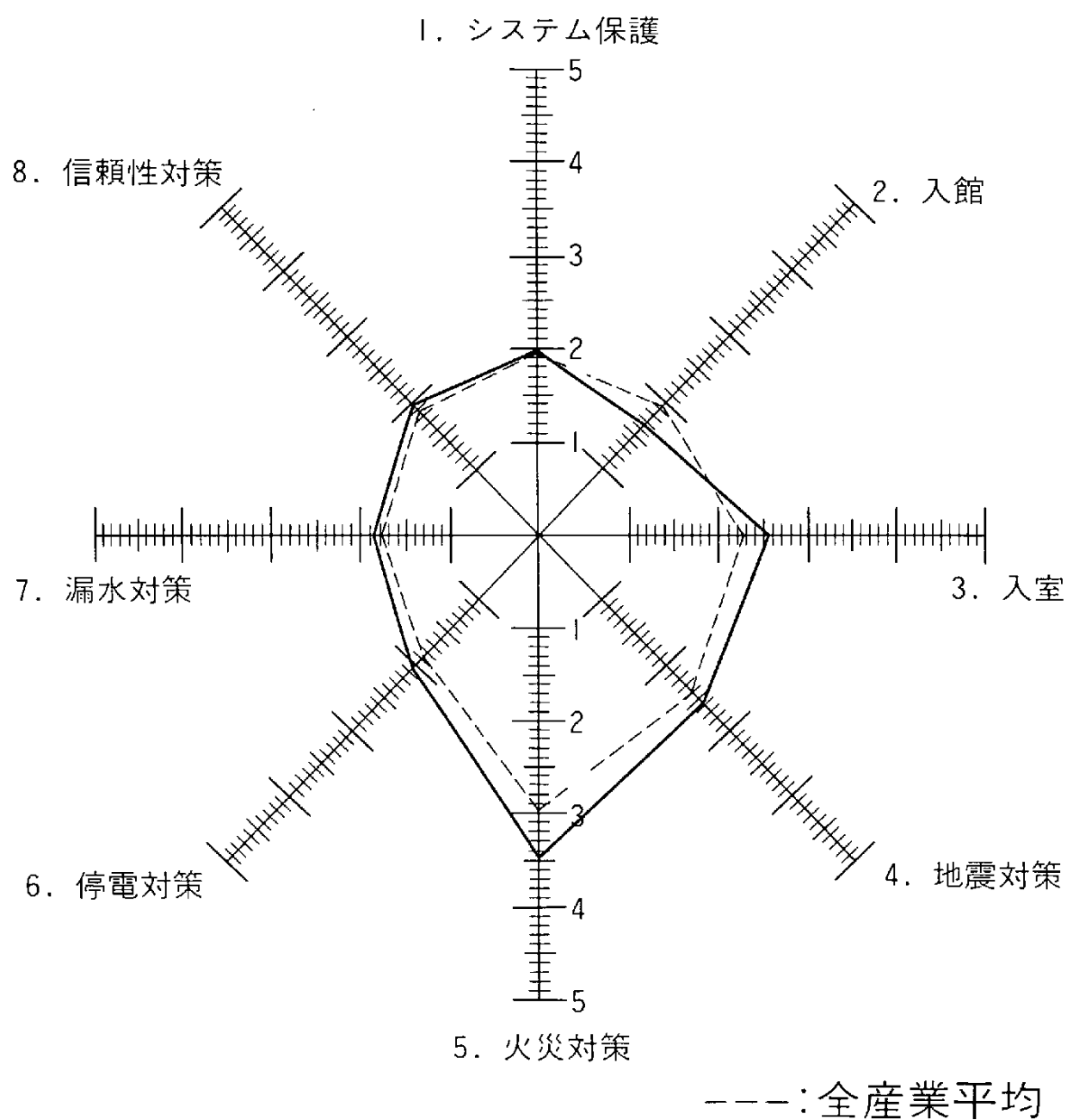
	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1.91	1.95	2.27	2.40	2.97	1.86	1.79	1.85
その他の教育機関	1.71	1.29	1.00	1.57	2.71	1.29	1.00	1.67

学術研究機関



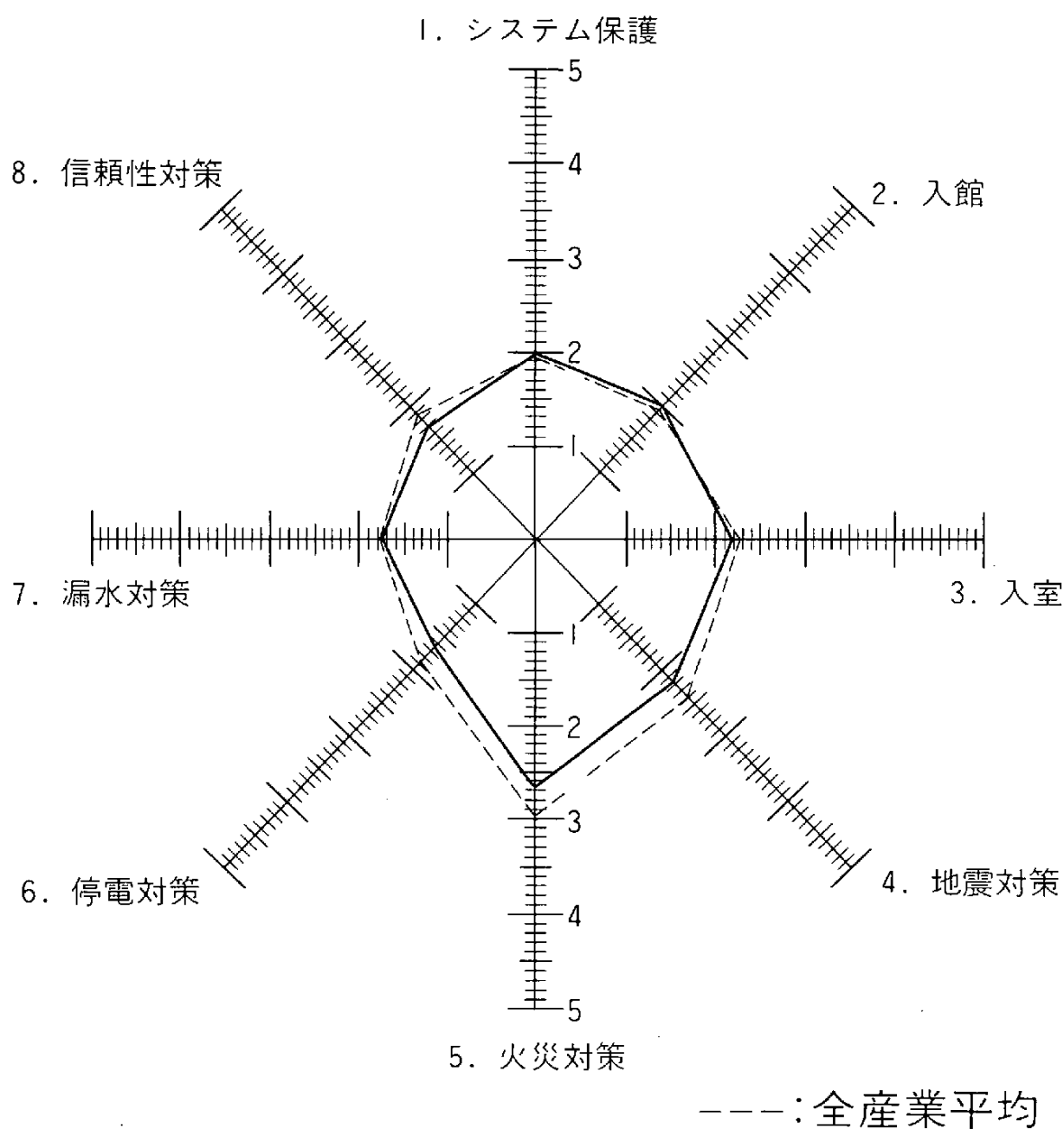
	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1. 91	1. 95	2. 27	2. 40	2. 97	1. 86	1. 79	1. 85
学術研究機関	2. 00	1. 33	4. 00	2. 67	2. 00	1. 00	1. 00	1. 00

法人団体・農協



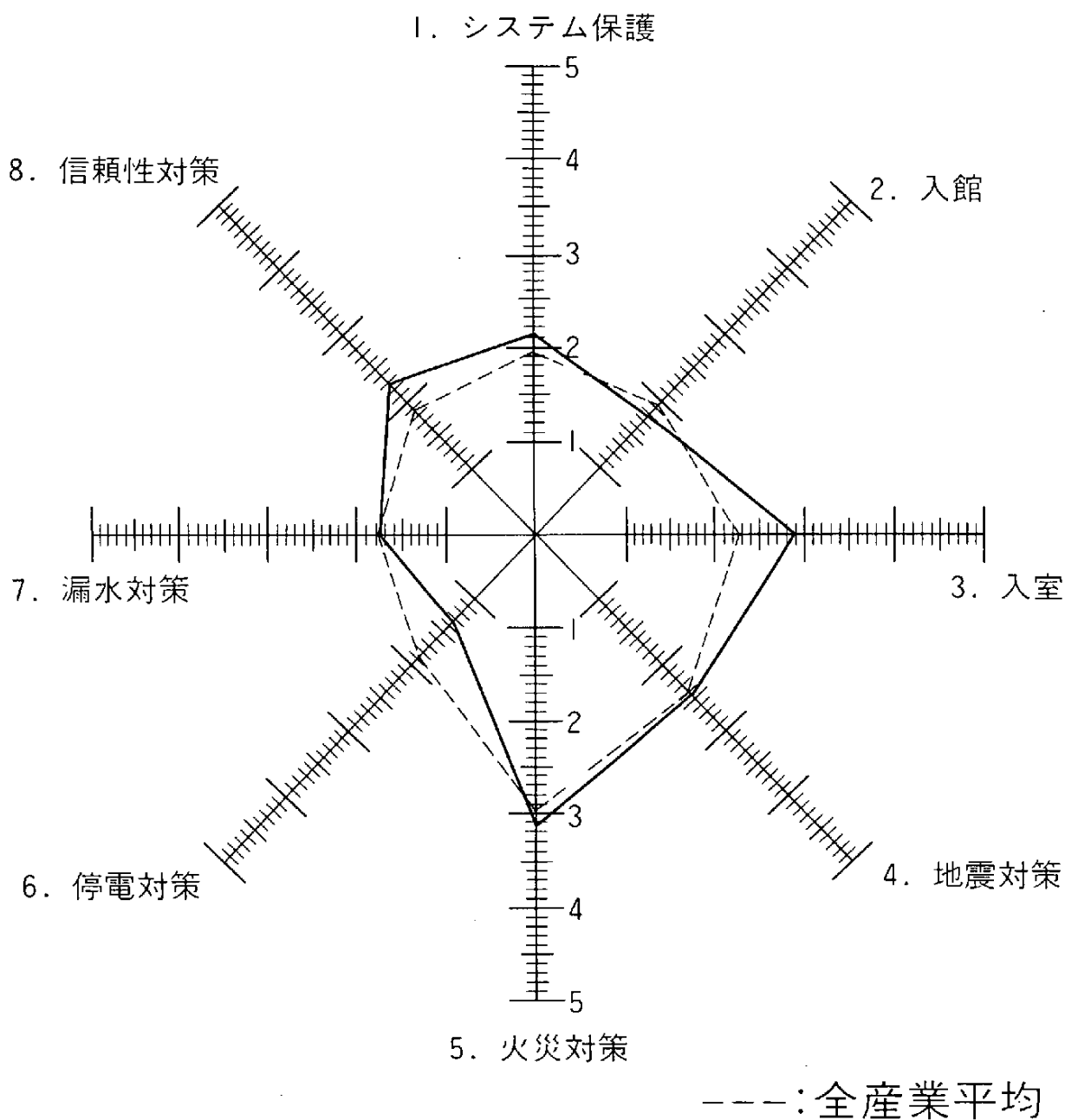
	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1. 91	1. 95	2. 27	2. 40	2. 97	1. 86	1. 79	1. 85
法人団体・農協	2. 00	1. 68	2. 56	2. 57	3. 46	2. 07	1. 88	1. 96

その他のサービス業



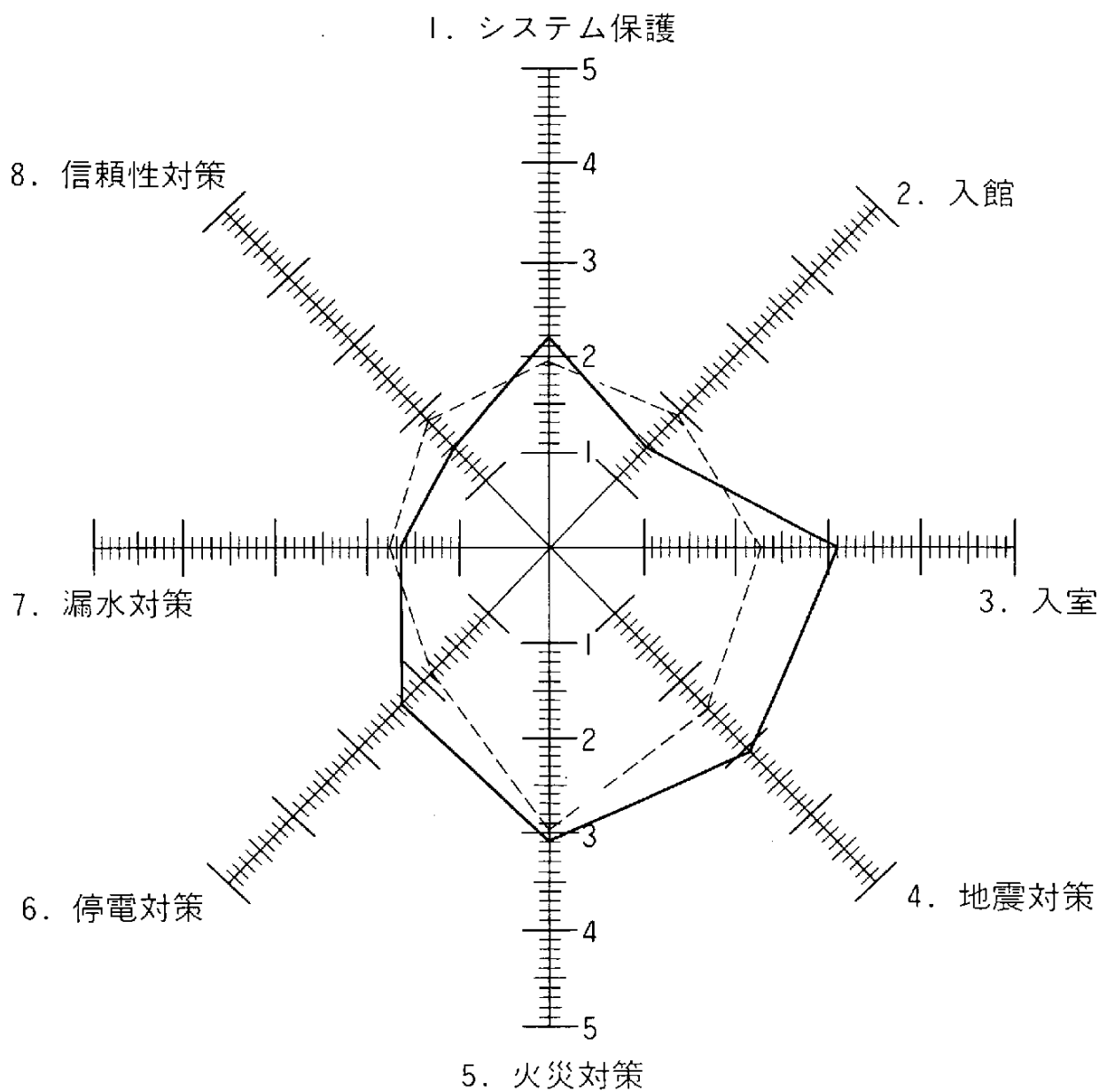
	1. システム保護	2. 入館	3. 入室	4. 地震対策	5. 火災対策	6. 停電対策	7. 漏水対策	8. 信頼性対策
全産業平均	1.91	1.95	2.27	2.40	2.97	1.86	1.79	1.85
その他のサービス業	2.00	2.00	2.18	2.18	2.64	1.64	1.73	1.70

政 府



	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. 91	1. 95	2. 27	2. 40	2. 97	1. 86	1. 79	1. 85
政 府	2. 11	1. 78	2. 89	2. 44	3. 11	1. 33	1. 75	2. 25

地方公共団体



	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. 91	1. 95	2. 27	2. 40	2. 97	1. 86	1. 79	1. 85
地方公共団体	2. 18	1. 45	3. 10	3. 03	3. 10	2. 34	1. 66	1. 49

—— 禁 無 断 転 載 ——

平成 2 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) 9384

印刷所 株式会社 正文社
東京都文京区本郷 3 丁目 25 番 8 号
TEL (815) 7271

