99-01004

情報化社会における企業の危機管理に関する調査研究(*1)
－情報システムにかかる企業の意思決定問題を中心に－

國　井　昭　男　　財団法人世界平和研究所主任研究員

1.はじめに

従来、「情報化に伴うリスク対策はコンピュータを防災設備の整った堅固な建物に設置し、火災や自然災害などの外来危険から守ることが主流であった」(日本セキュリティ・マネジメント学会[1998])が、社会の情報化の進展・ネットワークの普及に伴って、企業経営における情報システムの重要性がいや増すにつれ、情報化・ネットワーク化に起因する新たな形態の危機が顕在化してきた。『 2000 年問題』に代表されるような企業情報システムのダウンやトラブルといった問題や、企業内ネットワークシステムへの侵入・コンピュータウィルス・顧客情報の漏洩などといった犯罪行為のような企業情報システムに直接起因する危機だけでなく、インターネットのドメイン名の不正取得(サイバースクワッティング)問題や、1999年の『東芝事件』にみられるようなインターネットの潜在力を活用した個人顧客による大企業との対決など、従来にはみられなかった形態での危機が生じるようになっており、情報セキュリティの重要性が問われている。

大塚[2001]によれば、「企業における情報セキュリティ・マネジメントは対象分野として次の3つに分けることができる (中略) ●マネジメント・セキュリティ ●システム・セキュリティ ●ハード・セキュリティ」。冒頭に挙げた「災害などの外来危険から守る」ためのセキュリティマネジメントは「ハード・セキュリティ」に該当するが、近年、重要性を増しているのは「システム・セキュリティ」であり、「マネジメント・セキュリティ」の分野である。

本論では、これら分野にかかる危機発生の現状をサーベイしつつ、わが国の大企業を対象に実施した調査結果に基づき、情報システムにかかる企業の意思決定のあり方に内在する構造的な危機発生要因の分析を試みる。

2.セキュリティの現状

2.1.システム・セキュリティ

本年2月、わが国の 100 社程度の企業のWebPageが中国人と思われるクラッカーグループによって改竄される事件が起きたが、このような不正アクセス事件は既に日常化してしまっている。

安井ら[2000]によれば、わが国の大企業では、約 35%の企業がインターネット経由での不正アクセスを経験しており、コンピュータウィルスによる被害は約 80%の企業が経験している。

WebPage の改竄に限っても、1999 年 6 月に朝日新聞・毎日新聞という、マスコミの WebPage が改竄され話題になったのを実質的な嚆矢に、2000 年 1 月には中央官庁の WebPage が軒並み改竄されるなど、社会的な注目度の高い企業・団体の WebPage を中心として、多くの被害例が報告されている。また、同年 3 月には、九州銀行や神戸信用金庫の WebPage が改竄され、普及が見込まれる電子商取引のインフラたる金融機関の情報システムのセキュリティに対する懸念を生じせしめた事例も発生している。

同年 2 月には DDoS 攻撃(分散型サービス不能攻撃)により、米国の「Yahoo!」「e-bay」「CNN」「amazon.com」「E*TRADE」などの著名商用サイトが同時にシステムダウンを余儀なくされ、経済活動に大きなダメージを与えた事件も発生している。

このように、もはや、経済・社会活動のインフラと言える情報システムに対する不正アクセス等の事案には枚挙に暇がなく、情報システムを利用する企業・団体は常にシステム・セキュリティ対策を迫られている状態にある。

(*1) 本論文は、ワーキングペーパー「情報化社会と企業のリスク」(2001年3月;財団法人世界平和研究所(#269J))の一部について、2001年6月の情報通信学会大会における研究発表の際の議論を参考に再構成し直したものである。なお、本研究は、財団法人電気通信普及財団の研究助成を受けて実施したものであり、貴重な研究の機会を与えていただいた同財団に感謝申し上げたい

2.2.マネジメント・セキュリティ

一方、最近、顕在化している問題はマネジメント・セキュリティに関わる問題である。

電話会社・人材派遣会社・生命保険会社・地方自治体等による個人情報の漏洩に代表されるように、情報システムの整備により、却って顧客情報などの重要情報の漏洩が容易になった側面があり、この種の事件も枚挙に暇がない。企業側でも、パソコンのフロッピーディスクドライブを封鎖したり、社員が送受信する電子メールを検閲したり、といった種々の防衛策を講じているが、システムに依存した対策が目立ち、例えば、わが国では、セキュリティポリシーを策定している企業も約23%程度に過ぎない(安井らibid.)など、社員教育やポリシーの明確化といったマネジメントの側面からの対応策には消極的な姿勢が目立つ。

また、サイバースクワッティングに関しては、gTLD(一般ドメイン)・日本語ドメイン・ jp 汎用ドメインなど、利用可能なドメイン領域が増加していることもあり、多くの大企業がブランド防衛のために多数の人的資源を投入したり、訴訟や仲裁に持ち込むなど、かなりのリソースとエネルギーを充てており、リスク対策が大きな負担を生じる分野となっている。

3.わが国企業の情報セキュリティマネジメントの現状

3.1.調査概要

前章に掲げた情報セキュリティマネジメントの現状に鑑み、リスク発生構造分析の一端を解明すべく、わが国の大企業を対象とした実態調査を実施した。

わが国の上場企業および相互会社たる大手生命保険会社の中から単純無作為に 2,000 社を抽出し、各企業の経営企画・情報システム部門責任者宛に 2001 年 2 月に郵送法による質問紙調査を行った。有効回答数は 186 社であり、有効回答率は9.3%に相当する。(*2)

調査のポイントとしては、「情報システムへの不正アクセス問題」「重要情報の漏洩・管理問題」「インターネットドメイン名問題」「情報システムをめぐる意思決定問題」などである。

以下、特に「情報システムをめぐる意思決定問題」を中心に分析を加える。

(*2) 企業の情報セキュリティの現状や情報漏洩の実態等のセンシティヴな内容を尋ねる記名式質問紙調査のため、十分な有効回答率を確保できなかったものと考えられる。有効回答数が186社に留まっている点と併せ、以下の分析が必ずしもわが国の大企業の実態を正確に反映しているものとは言い難い点に留意する必要がある

3.2.企業特性

3.2.1.IT導入

回答企業の 1995 年以来の IT 導入状況を見ると、「 WebPage 開設」(2001 年時点で 94%)、「電子メール」(同 89%)、「インターネットブラウザによる閲覧」(同 87%)、「グループウェア」(同 84%)、などの IT が広範に普及していることが分かる。(図1)

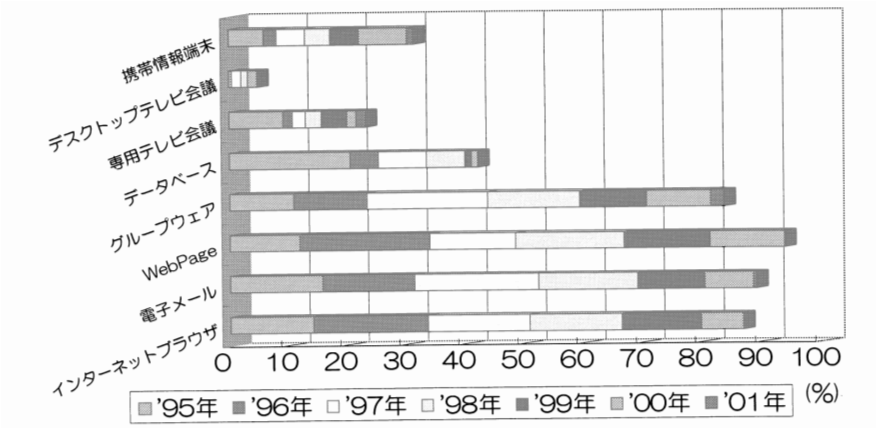

図1　調査対象企業のIT導入状況

また、これらの IT が 96 年から 98 年にかけての 3 年間に急速に導入されたことも図1から明らかになる。これら企業の IT 導入パターンを 0-1 型のダミー変数を用いて数量化Ⅲ類により処理し、サンプルごとの各年度間のスコア差を当該企業の IT 導入量とみなし、95 年～ 01 年のIT導入量の合計値(導入されたITの種類の多さを表す)と変動係数(年度ごとの IT 導入のコンスタントさを表す)によって各企業の IT 導入パターンの分類を試みたところ、概ね 3 群に分類することができた。(*3)

図2に示すように、32%の企業が IT 導入量の合計値が大きく変動係数が小さい企業群(「α群」と呼ぶ)に属する。これらの企業は、積極的かつコンスタントに IT を導入している企業であると言える。同様に、24%の企業をIT導入に消極的な企業群(β群)、45%の企業をIT導入がコンスタントでない(年によりIT導入が区々)企業群(γ群)、にそれぞれ分類することができる。

本調査によれば、α群企業は、β群・γ群企業に比して、情報システムへの不正アクセス被害の経験を多く有している。

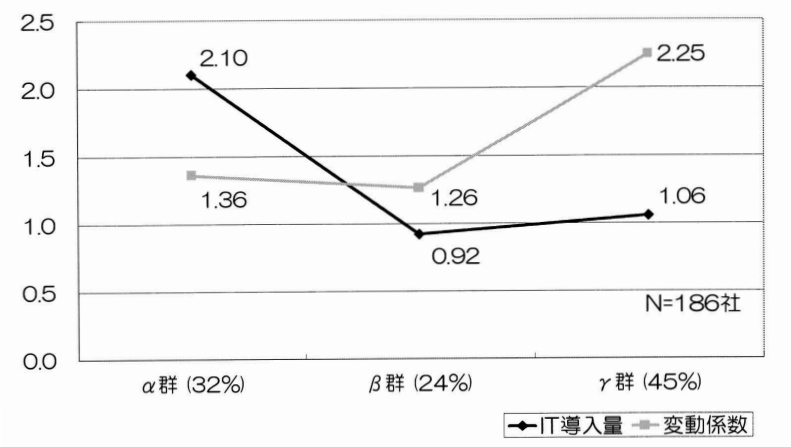

図2　IT導入パターンにによる企業分類

(*3)　k-means法クラスター分析による

3.2.2.CIO

情報システムの整備・運用に関する実質的な責任の所在については、41%の企業では役員に属し、54%の企業では中間管理職社員に属している。これら41%の企業では、Chief Information Officer(CIO)を置く企業は全体の半数に満たないことが分かる。

本調査によれば、CIO を置く企業は、CIO を置かない企業に比べ、情報システム利用の基本的なルールである「e ポリシー」を策定し、遵守されている比率が高い傾向にあり、重要情報の漏洩被害の経験も少ない傾向にある。

3.2.3.組織文化

トップダウン経営であるか、伝統・前例重視であるか、など特徴的な組織文化を示す 38 項目の設問に対する自己評価をリッカートの 5 点評価法により求め、因子分析に基づき、寄与率の大きな 3 つの因子(*4)を用いて企業分類を試みた。

即ち、スピード重視でトップダウンの組織文化を示す第 1 因子、手続き・前例重視の保守的な組織文化を示す第 2 因子、コミュニケーション重視の第 3 因子、であり、これらの因子に対するサンプルスコア(*5)を用いて企業を比較的保守的な組織文化を持つⅠ群企業(44%)と、比較的革新的な組織文化を持つⅡ群(45%)に、ほぼ二分することができる。(*6)

3.3.情報システムにかかる意思決定問題

3.3.1.情報システム構築・運営の制約条件

一般に企業が情報システムを構築・運営するに当たり、種々の制約条件を課せられることが多く、なおかつ、それらの制約条件は背反的な関係にあることが多い。

ここでは、その代表的なものとして「社員の業務効率」「顧客・取引先の利便性」「セキュリティ」「コスト」を例に取り上げて論じることとする。(図3)

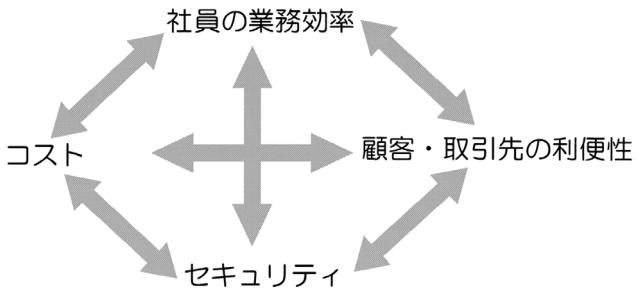

図3　情報システム構築・運営に際しての制約条件の例

例えば、外出がちの社員が多い企業では、社員が外出先からイントラネットにアクセスできる環境を整えれば「社員の業務効率」は向上するものと考えられるが、その場合、「セキュリティ」の水準を低下させる危険性がある。他方、「セキュリティ」を担保するためのシステムを情報システムに付加すると「コスト」が増大し、予算上の制約を受けることが多い。また、得意先企業からインタオペラビリティの高い情報システムの構築を求められ、「顧客・取引先の利便性」と「コスト」の相克に悩む企業も少なくないものと思われる。

(*4)　累積寄与率0.383

(*5)　バリマックス回転後のスコアによる

(*6)　k-means法クラスター分析による

3.3.2.制約条件の評価(ウェイトづけ)

企業はこのような 4 種類の制約条件のバランスを取りながら情報システムの構築・運営を行っていると考えられるが、そのウェイトづけ(意思決定)をAnalytic Hierarchy Process(AHP)を用いて、定量化を試みた。即ち、4 制約条件(評価基準)について、各制約条件間の重要性評価の一対比較を行った(*7)ところ、企業ごとの 4 評価基準に対するウェイトの相関係数を算出すると、「社員の業務効率」と「セキュリティ」の間の相関係数が-0.52、「セキュリティ」と「コスト」の間の相関係数が-0.46、と強い負の相関関係を指摘することができ、このことは、企業が情報システムを構築・運営するに際して、これらの制約条件が、いわば「あちら立てればこちら立たず」の状態にあり、これらのバランスが最大の課題となっている証左でもある。

ここで、全企業平均(*8)での 4 評価基準のウェイト(*9)は、「社員の業務効率」：0.265、「顧客・取引先の利便性」：0.222、「セキュリティ」：0.302、「コスト」：0.212、であり、セキュリティが最も重要視される評価基準であることが分かる。

ただし、各評価基準ごとのウェイトによる企業分布の様子を見てみると、いずれの評価基準についても、極めて強く評価する企業から、ほとんど無視する企業まで幅広く分布しており、また、それぞれ特徴的な分布傾向を示すことが分かる。例えば、評価基準「社員の業務効率」について見てみると、平均値は 0.265 であるが、0.10台・0.25台・0.40台、のウェイトづけで評価する企業がそれぞれ多く、尖度も-0.616 と負の値を示す(図4)のに対し、評価基準「コスト」については、平均値は 0.212 であるが、0.10 台を中心にL型の分布を示し、実際、尖度(0.570)も歪度(1.049)も高い正の値を示している。(図5)

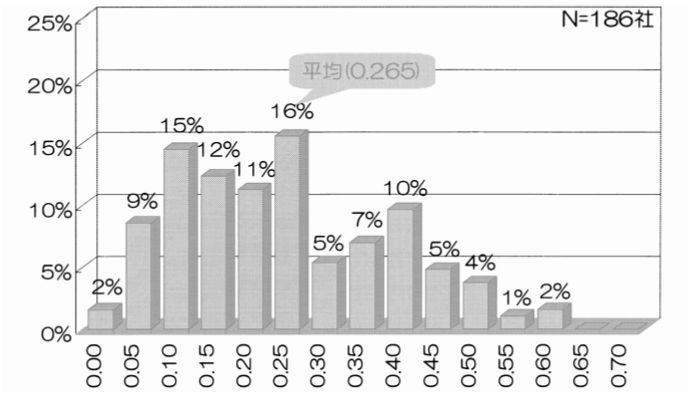

図4　評価基準「社員の業務効率」へのウェイトづけの分布

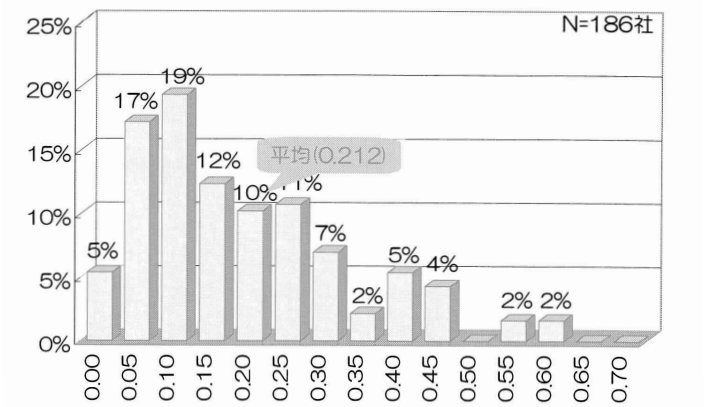

図5　評価基準「コスト」へのへのウェイトづけの分布

(*7)　例えば「セキュリティ」と「コスト」について、どちらをより重要視するか、それぞれ5段階の重要性の度合い(「極めて重要」「非常に重要」「かなり重要」「少し重要」「同じくらい重要」)により評価を求めている。(計9段階の比較評価となる)

(*8)　幾何平均ではなく算術平均である

(*9)　全評価基準のウェイトの合計値が1になるように基準化された値である

最も特徴的なのは、評価基準「セキュリティ」であり、平均値は 0.302 と高いが、企業は 0.20 台を中心に分布している一方で、平均値を大きく超えたウェイトづけで評価する企業も多く、0.50 以上のウェイトづけをする企業が 16%にものぼり(図6)、尖度も-0.361と負の値を示している。このことは、「セキュリティ」については、必ずしもほとんどの企業が重要視している訳ではないが、これを極めて重要視する企業群が一定数存在していることを示していると言えよう。

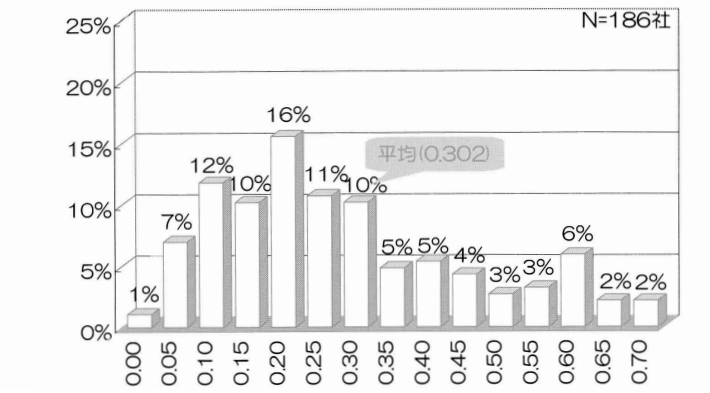

図6　評価基準「セキュリティ」へのウェイトづけの分布

実際、4つの評価基準に対するウェイトスコアによって、企業を分類すると、概ね 4 群に大別されるが(*10)、「社員の業務効率」を重視する企業群(「 U 群」と呼ぶ)が25%、「顧客・取引先の利便性」を重視する企業群(C 群)が 20 %、「コスト」を重視する企業群(T 群)が 28 %、に対して「セキュリティ」を重視する企業群(S 群)は 24 %であり、必ずしも多数派ではない。

これを企業の業種別に見てみると、金融業には S 群企業が多い(40%)のに対し、商業では C 群(28%)、サービス業では T 群(45%)に属する企業が多いなどの特徴を指摘することができる。(図7)

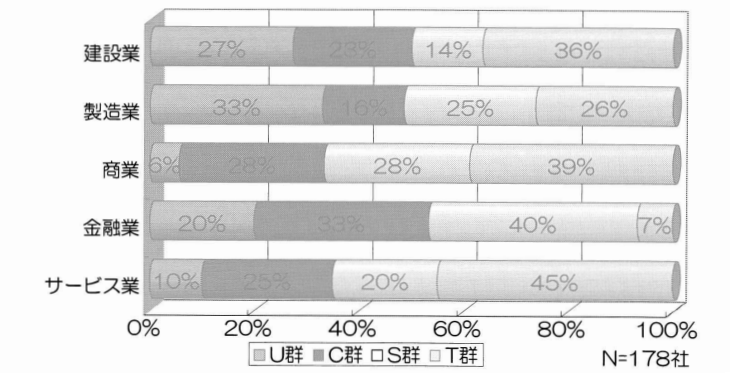

図7　評価基準へのウェイトづけによる企業分類と業種の関係

また、例えば、3.2.3.で示した組織文化に基づく傾向を分析すると、Ⅰ群(比較的保守的な組織文化を示す企業群)では「セキュリティ」よりも「コスト」を重視していることが分かるし(図8・図9)、3.2.2.で示した CIO の有無による差異についても、CIO のいない企業が「コスト」を重視しがちであることもまた言える。(図10)

これらの傾向からは、前例重視・手続き重視などの特徴を示す保守的な企業文化の企業や、部課長級の中間管理職が情報システム関係の責任を負う体制になっている企業においては、予算等の制約条件の下での情報システム構築・運営が行われており、投資効果が顕在化しにくいセキュリティ対策等の観点からの機動的な投資が柔軟には行われにくい状況が現出されてしまっている様子を見て取ることができるだろう。

(*10)　k-means法クラスター分析による

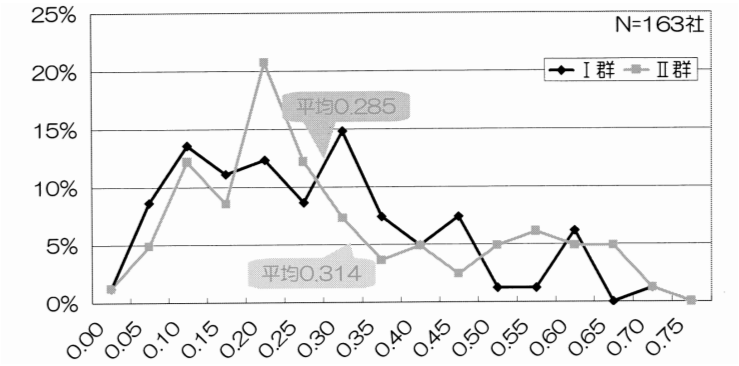

図8　組織文化による企業分類と評価基準「セキュリティ」へのウェイトづけ分布

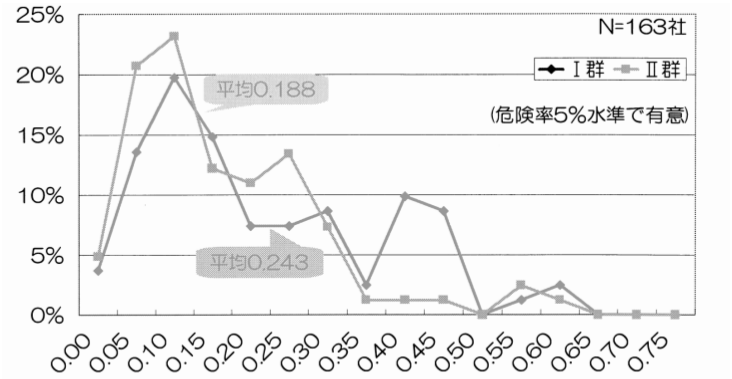

図9　組織文化による企業分類と評価基準「コスト」へのウェイトづけ分布

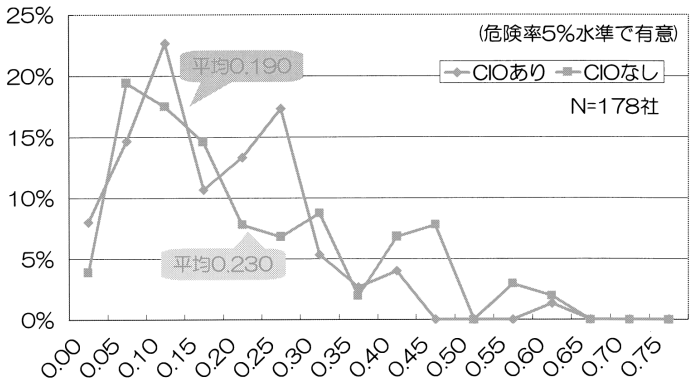

図10　CIOの有無と評価基準「コスト」へのウェイトづけ分布

3.3.3.意思決定プロセスの整合性

ところで、このように企業によって区々の傾向を示す制約条件(評価基準)へのウェイトづけであるが、各企業とも、必ずしも完璧に整合的な論理性を以て意思決定を行っている訳ではなく、場合によっては制約条件間に相矛盾する評価を付与しながら情報システムを構築・運営しているケースも考えられる。そこで、評価の整合性を示すConsistency Index (C.I.)を算出すると図 11に示す分布が得られた。「完全に整合である場合はこの値は 0 であり、この値が大きくなればなるほど、不整合性は高い」「C.I.の値が 0.1(場合によっては0.15)以下であれば合格」(木下[2000])であるから、整合的なバランスを取りながら情報システムの構築・運営に当たっている企業は決して多数派とは言えず、多くの企業の意思決定プロセスに混乱が生じていることが見て取れる。

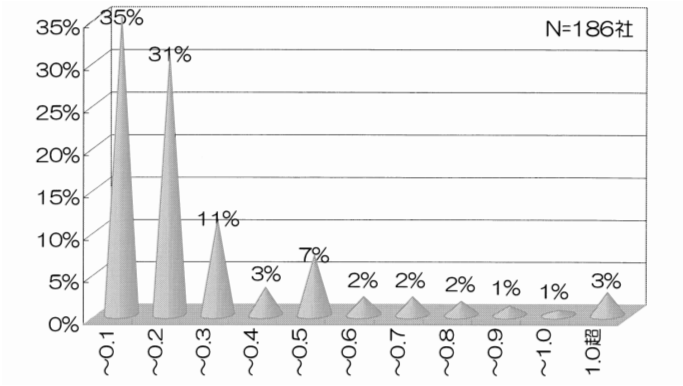

図11　評価基準へのウェイトづけにおける整合性指数（C.I.） の分布

これを3.2.1.で分析した IT 導入パターンによる企業分類に当てはめてみると、IT を積極的に導入しているα群企業の C.I. が際だって高いことが分かる。(図12)

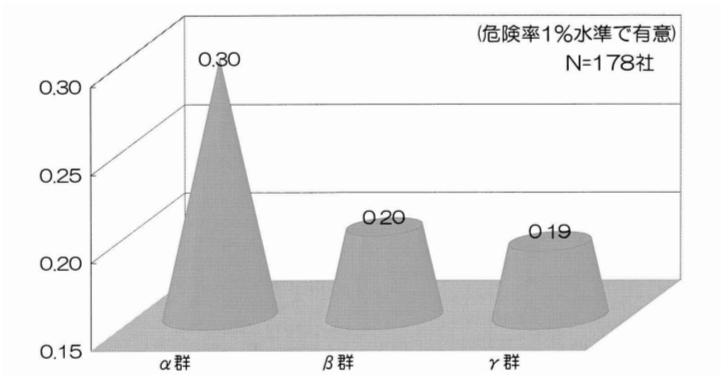

図12　IT導入パターンによる企業分類と評価基準へのウェイトづけにおける整合性指数（C.I.）

とするならば、IT を積極的に導入してきたこれらの企業は、整合的な論理性を以て情報システムの構築・運営に当たってきたというよりは、「IT革命ブーム」の下で、実務的にシステム導入優先の姿勢を採ってきたと推測することができるだろう。

3.2.1.で述べたように、α群企業において、情報システムへの不正アクセスの被害が顕著なのは、単に IT の普及度合いが高いからだけではなく、企業としての情報システム構築・運用への意思決定プロセスが曖昧なまま、大量の IT 導入を図ってきた副作用である面も否定できないのではないだろうか。

4.まとめ

以上、調査票調査によるデータに基づき、企業の情報セキュリティマネジメントに関わる意思決定問題を中心とした分析を加えてみた。

示唆的に言えることは、情報システムにかかる高次元での責任の所在の明確化の重要性であろう。CIO を置く企業が、そうでない企業に比して、全体的に情報システムのセキュリティを重視し、ある程度、奏功していると判断することができる。これらの企業の場合、コストよりもセキュリティを重視する傾向にあるが、責任の所在が不明確であったり、社員レベルに帰せられていたりした場合には、コスト、即ち既定の予算の範囲内での情報システム構築・運営しかできないのは当然である。その意味で、情報化社会の進展の過程でこれまで想定し得なかったような新たな危機が顕在化しつつある企業の体制のあり方へのインプリケーションを求めることができるだろう。

同様に、手続きや予算等の制約が重要視されがちな保守的組織文化もまた、情報セキュリティマネジメントへの障害として機能し得るし、IT 革命ブームの下での明確な意思決定プロセスを欠いたIT導入も、企業に新たなリスクをもたらす可能性を否定できない。

IT の導入に当たっては、ブームに踊らされることなく、明確な責任の所在のもとで、明確な意思決定プロセスを経つつ、企業改革を伴いながら行うことが企業にとっての危機管理の観点からも重要であると言うことができるだろう。

【参考文献】

Anonymous, SE編集部訳, 1999, クラッキング対策ファイナルガイド, 翔泳社
河崎貴一, 2001, インターネット犯罪, 文春新書
木下栄蔵, 2000, 入門AHP, 日科技連
宮脇磊介, 2001, サイバー・クライシス, PHP研究所
日本セキュリティ・マネジメント学会, 1998, セキュリティハンドブックⅠ, 日科技連
大塚寿昭, 2001, コーポレートセキュリティ, ダイヤモンド社
オーバリー, M.R., 藤本叔子訳, 2001, eポリシー, 日経BP社
セコム株式会社, 2000, サイバーセキュリティ入門, 東洋経済新報社
安井晴海・蛯谷敏, 2000, 蝕まれる企業ネットワーク, 日経コミュニケーション8月21日号, 日経BP

＜ 発　表　資　料 ＞

題　　名	掲載誌・学会名等	発表年月
Cybersquatting- latest risk in the IT Revolution	IIPS NEWS 世界平和研究所	2000年８月
情報化社会と企業リスク	IIPS Policy Paper 世界平和研究所	2001年３月
情報化社会における企業のリスク	情報通信学会大会	2001年６月