

システム監査学会 第22回研究大会

今求められる経営の変革視点

GRCの意義とその位置づけ

A change viewpoint of management demanded now

Significance of the GRC and the positioning

平成20年6月6日

GRC研究プロジェクト

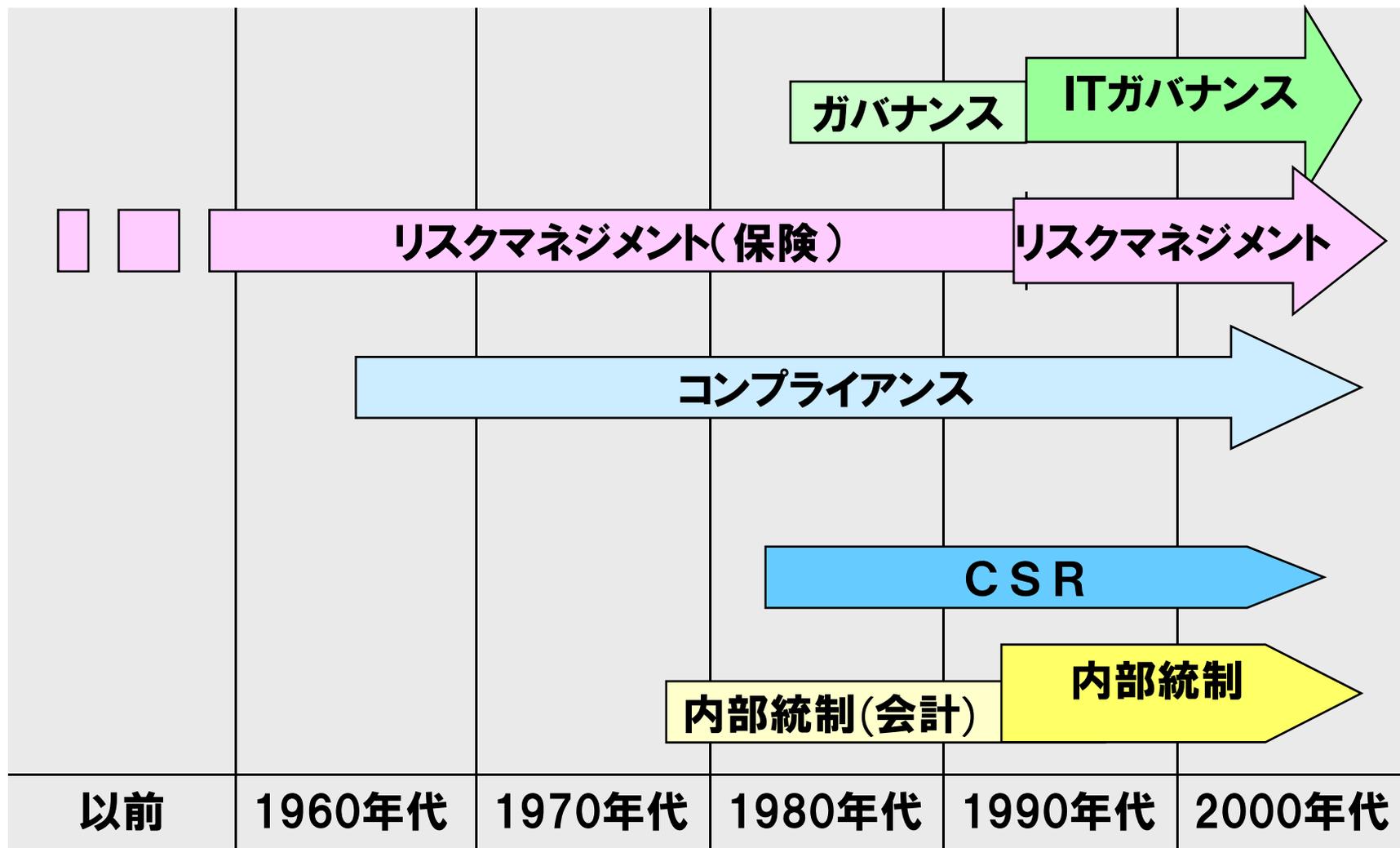
研究の背景

- 2007年ACL Services Ltd. より公開された資料
メンバーの石島氏より「GRC」について報告
- これまで、システム監査に関する研究のなかで発表、討議、
提言されてきたことは：
 - ・ガバナンス, ITガバナンス, CSR
 - ・企業不祥事とコンプライアンス
 - ・SOX法, J-SOX(金融商品取引法及び制度)
 - ・内部統制, IT統制,
 - ・米国資料では、PRCで説明(PはPerformance)
 - ・GRCと企業倫理
 - ・COBIT4.1 FRAMEWORKについて……など

繰り返される企業等の不祥事や事件

- しかし、いつの時代にも企業不祥事がおこり、ハイテク犯罪が発生し、経営者はその対応と責任を取るために奔走し、企業社会は混乱した。そして、新たな経営管理が求められ、二度と不祥事がおこらないように対策を策定し、実施されてきた。
- その一方で、ICT(情報通信技術)は高度化し、経営管理の情報戦略化されたが、新たな脆弱性が内在した。
- その結果、新たな企業不祥事はおこり、より深刻なハイテク犯罪が発生した。

GRC及び関連用語の起源から進化

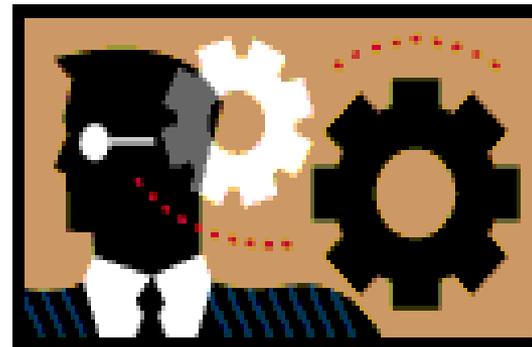


平成19年度研究プロジェクト

- ① 平成19年度研究プロジェクト「GRC研究」を研究テーマ
GRCは企業のガバナンス(Governance)、リスク(Risk)、コンプライアンス(compliance)を一元管理していく概念として体系化を考えていく
- ② GRCは結果的には、何をめざすためのものか
最終ゴールやその目的はなにか
- ③ 従来、ガバナンス、リスク、コンプライアンスは、企業内では個々に、その時代に最適な経営管理として、あるときには企業の取組むべき「理念」や「ミッション(使命)」として、あるいは、マネジメントのキーワードとして取り組まれてきた。しかし、企業の不祥事や犯罪は、繰り返しおこった
- ④ このことへの反省を踏まえ、G, R, Cを個別の対応として捉えるのではなく、統一的な一元管理概念としてのGRCを捉え、理論面及び実践面から研究する

今求められる経営の変革視点

G R C



GRCのめざすべき方向

- 米国のACL Services Ltd.はGRCをソリューションソフトウェアとして、コンサルティング・サービスを提供し始めた。
- SAPジャパンは、同社が提唱する概念「GRC」と、同概念を製品化した「SAP Solutions for GRC version 2.0」として発表した。
- オラクル社では、企業におけるこれらGRC要件への取組みを支援するGRCフレームワークを提案している。

しかし、GRC研究プロジェクトでは、GRCを「ソフトウェアのソリューション・パッケージといった考え方をせずに、企業等の経営管理をすべく、一元的な管理の概念」として位置づけ、その目的はコーポレート・レピュテーションの向上にある」と考えている。

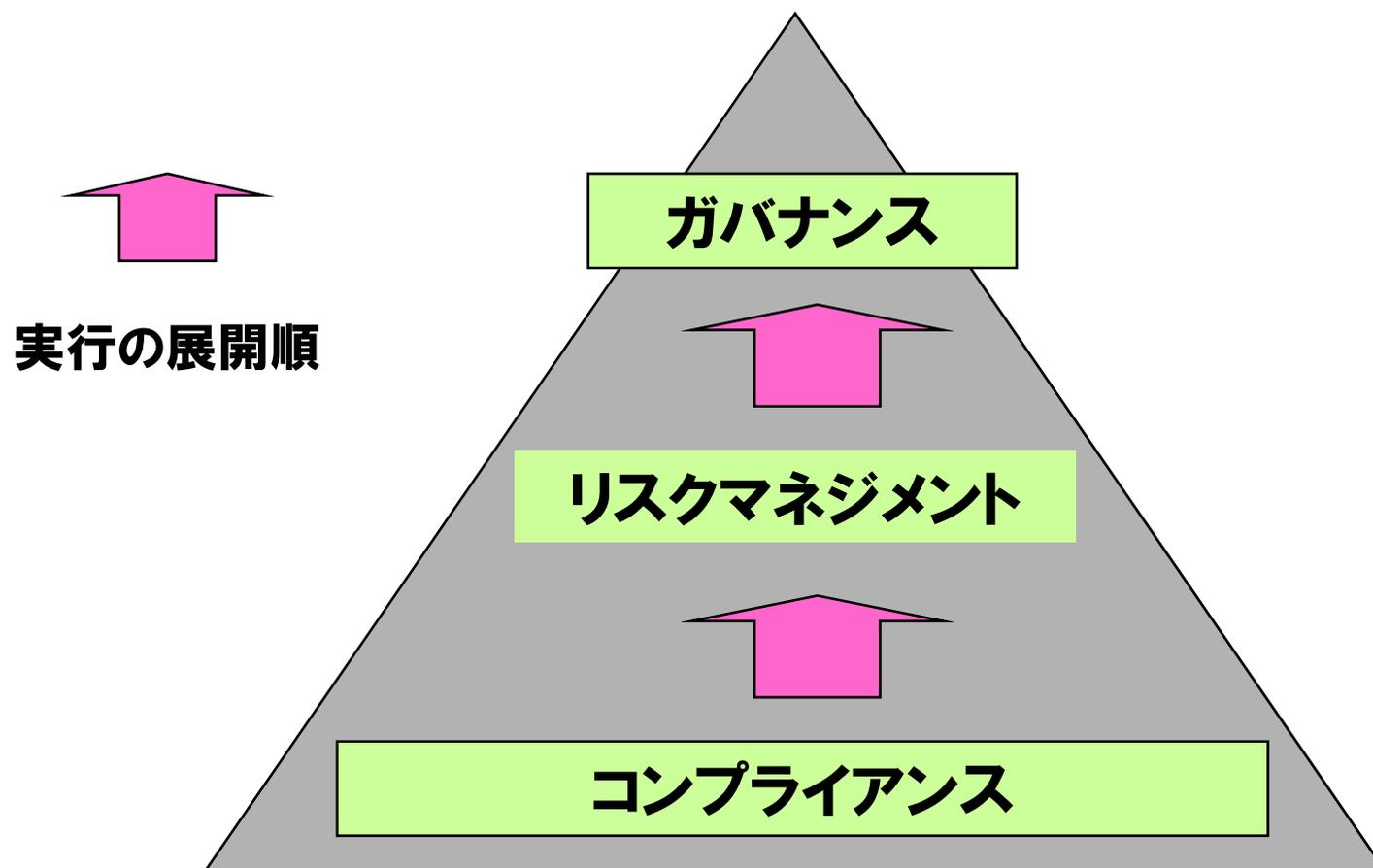
SAP 日本の考え方

SAP日本は、同社が提唱する概念「GRC」と、同概念を製品化した「SAP Solutions for GRC version 2.0」として発表

バイスプレジデント ソリューション & マーケティング統括本部長 安田誠氏。氏はG、R、Cのそれぞれの位置関係を、Gを頂点とした三角形で表した。ガバナンス、リスクマネジメント、コンプライアンスと、下にいくほどに、幅が広がっていく。あえて順序をつけるとするなら、コンプライアンスがあり、リスクマネジメント、ガバナンスという流れで内部統制の具体的な仕組みを充実させていく。

このことは、「SAP Solutions for GRC」の機能拡張に関するロードマップをみるとわかりやすい。「SAP Solutions for GRC version 2.0」の機能拡張の主眼は、統制管理である。統制文書の作成、マニュアル統制テスト、リスクダッシュボードなどの機能を追加した。「SAP GRC Repository」「SAP GRC Process Control」「SAP GRC Risk Management」の3つの製品を製品群に加えることで、これらの機能拡張を実現している。

SAP ジャパンが考えるGRC



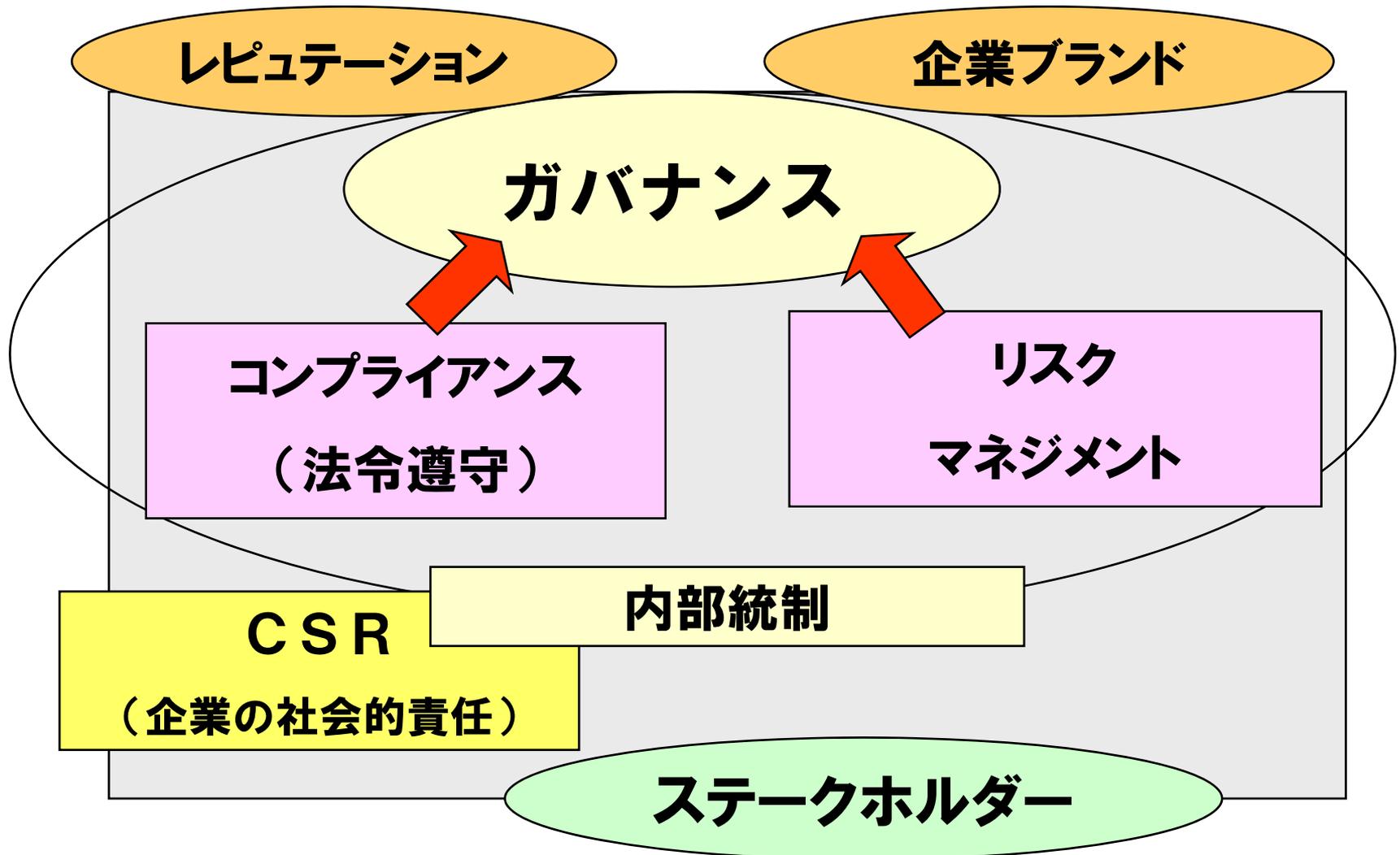
オラクルGRC

オラクル社では企業におけるこれらGRC要件への取組みを支援するGRCフレームワークを提案している。GRCフレームワークはGRC要件への対応を網羅的に体系化したもので以下の4つの要素から構成されている。

- ITガバナンス構築の基盤となる「インフラストラクチャ」
- 内部統制があらかじめ組み込まれた業務プロセスを実現する、ERPに代表される「アプリケーション」
- 内部統制監査や教育といった「プロセス」
- 意思決定に向けた適切な情報を、適時、適切な人に提供して、企業の洞察力を強化する「インサイト」

オラクル社はこの4つの要素に対し、製品、サービス、ソリューションを統合的に提供し、企業における確実な内部統制およびコンプライアンスの実現と情報の適切な可視化によるガバナンスの強化、そしてそれらに基づく企業価値向上をめざしている。¹⁰

GRCの関連性（中間討議）



コーポレート・レピュテーション

一般的にコーポレート・レピュテーション(corporate reputation: 企業の評判)というべき無形資産として取り扱われている。櫻井(2005)はコーポレート・レピュテーションを、「経営者および従業員による過去の行為の結果、および現在と将来の予測情報を基に、企業を取り巻くさまざまなステークホルダーから導かれる持続可能な競争優位」と定義づけている[1]。

すなわち、コーポレート・レピュテーションは、経営者、従業員が過去から現在に至る日々の企業活動の成果の積み重ねであり、この活動において実施する努力が社会から認められ良い成果となれば、ステークホルダー1人1人のインセンティブが向上し、企業への愛着、親しみが増すことになる。これにより、企業の生産性やブランド・エクイティなどが高まり、企業価値の向上が期待できる。

GRCの新たな定義

企業等にとって、環境問題への対応、地域(地元)への貢献度、高齢化問題への対応など様々な取り組みにおいて、ステークホルダー(stakeholder:利害関係者)から社会的評価を受けることも重要な企業価値の一つといえるようになってきた。

これに加え、コーポレート・ガバナンスやコンプライアンス・プログラム、リスク・マネジメント、といった企業内の統制の仕組みが構築でき、社会から安心と信頼を得ることのできる健全な経営も企業が社会から受ける評価であり、企業価値の増減に大きな影響を及ぼす。

これまで、個々に取り組まれてきたコーポレート・ガバナンスやリスクマネジメント、コンプライアンス・プログラムを、企業価値を高める有機的な統合概念として体系化し、コーポレート・レピュテーションを向上させる手法として、確立させる必要がある。それが「GRC」である[2]

図：GRCとコーポレート・レピュテーション

内部統制に依拠したGRCの確立が、企業の社会的責任(CSR)を果たし、コーポレート・レピュテーションの向上につながるのである。

ステーク
ホルダー

コーポレート・レピュテーション

企業内部

コーポレート・ガバナンス

GRC

コンプライアンス・プログラム

リスクマネジメント

内部統制

企業外部

企業の社会的責任(CSR)

今後の課題

- GRCを企業等の経営管理として確立させる
- これまで、個々に確立されたG・R・Cの概念を、相互の関係性を明らかにし、個別のG・R・Cを効果的一元管理の「GRC」として確立させるために、課題を洗い出す。
- GRCを確立させるためには、基底に内部統制があり、その関係性を具体的に明らかにする。
- また、GRCが有効に機能しているか、その評価の方法についても検討する。
- GRCが有効に機能している企業モデルの策定する。

今後の課題への適用の研究を継続

1. 食品偽装問題を対象に「GRC」との関連性を研究

- (財)比較法研究センター「食品偽装の法的問題」
- 日本情報経営学会で発表 「食品偽装のGRCとコーポレート・レピュテーション」 2008. 5. 25

2. 食品偽装事件の時系列データ(内外の動き, トップマネジメントの行動, 組織人事, 事後対策, マスコミ報道)をもとに, GRCとの関連とその評価を分析した。

【事例】

- コンプライアンス:食品衛生法, JAS法, 不正競争防止等
- リスクマネジメント:マスコミへの発言, 謝罪方法, CM等
- ガバナンス:トップ人事(社長の交代人事), 商品の自主回収, 商品販売の停止, 設備・機器改修, 外部委員会の設置, 再建方法など

3. 今後は, さらにGRCとの関連性の研究が必要

- 内部統制アクティビティとの関連
- ハイテク犯罪, コンピュータ事後とGRCとの関連等

ガバナンスとリスクとコンプライアンス

起源と概念の整理

ガバナンスとITガバナンス

コーポレートガバナンスの背景

■ 日本においてコーポレート・ガバナンスが取り沙汰されるようになったのは、1990年代以降に発生した金融機関を中心に起こった一連の不祥事や不良債権処理をめぐってのことである。

それまで国際的にも信頼されていた日本の金融機関が、経済基盤となる機能の不全化を起こし始めたのである。金融機関をはじめとする不祥事や不公正の取引行為を、日本の経営者はなぜ防げなかったのか、日本企業の経営者に対する不信感が積み始め、企業の倫理観が問われるようになってきた。

■ その一方で、株価の暴落、株式投資の利益低迷が続き、日本企業の株主を無視した経営が徐々に非難され出し、それまでのいわゆる「日本的経営」が崩壊し始めたのである。長引く不況の中で、企業や銀行による株式の持ち合いでは資金効率の改善ができなくなり、徐々に持ち合い株の解消を行う。一方で、外人投資家による株式保有率が上昇し、投資収益の改善を求めて、直接、コーポレート・ガバナンスに介入するようになってきた。

コーポレート・ガバナンス

- コーポレート・ガバナンスとは「企業の統治の権利を有する株主の代理として選任された取締役により構成された取締役会が、経営戦略に基づき実施される経営者のマネジメントを監督する行為」である。
- 上記のような背景のもとで、日本でもコーポレート・ガバナンス改革を実現していく企業が増えている。そして、以下のような責任と行動が求められる：
 - ① 「所有と経営に分離」原則に基づき、経営者の独立と責任の明確が求められる。
 - ② 取締役会は、株主、従業員（およびその家族）、顧客、銀行、納入企業、地域社会、国家など、利害関係者となるこれらのステークホルダーに対して、企業利益を最大化するために、誠実に行動することが、第一義的な責務である。
 - ③ 取締役はすべての株主の利益を考慮した、アカウンタビリティ（説明責任）を果たす必要がある。
 - ④ 企業は、人類が存続するための「環境」「社会」「文化」「経済」を持続するためのサステナビリティに寄与すべきである。サステナビリティの達成には、「環境対策やコンプライアンス」への対応とその社会的責任（CSR：Corporate Social Responsibility）の外部評価が求められる。

ITガバナンス(IT governance)

組織体・共同体がITを導入・活用するにあたり、目的と戦略や適切に設定し、その効果やリスクを測定・評価して、IT活用をもって実現する組織メカニズムを確立すること。

1999年ごろ、通商産業省と日本情報処理開発協会は、ITガバナンスを「企業が競争優位性構築を目的に、IT戦略の策定・実行をコントロールし、あるべき方向へ導く組織能力」と説明、

また「主にIT化により新たに生じるリスクの極小化と的確な投資判断に基づく経営効率の最大化、すなわち、リスク・マネジメントとパフォーマンス・マネジメントであり、これらを実施するに当たっての、健全性確保のためのコンプライアンス・マネジメントの確立である」(日本監査役協会 ITガバナンス委員会)とした。

一方、情報システムコントロール協会(IT Governance Institute)は、「ITガバナンスは取締役会および経営陣の責任である。それは企業ガバナンスの不可欠な部分で、リーダーシップおよび組織的な構造、および組織のITがその組織の戦略および目的を保持し拡張することを保証するプロセスから成る」と定義している。

ITガバナンスは個々のIT投資や評価に関するものではない。企業全体として、経営戦略とIT戦略との整合性、ITの投資効果、組織のあり方や人員・体制、リスクに関連する事項も含めて評価のフレームワークを確立し、企業内外におけるITの運用と利用にかかわるルールとマネジメント・システムを構築することで確立されるもの

CSR（企業の社会的責任）

社会的責任(CSR:Corporate Social Responsibility)の考え方は、アメリカでは1980年代半ばの軍需産業の不祥事の表面化などから、社内外で企業倫理に関する取り決めが整備され、企業の自己チェック機能が強化され始めた。わが国では、1990年代はじめに証券会社による損失補填が社会問題となり、この事件後、経済団体連合会(現在の経団連)が、1991年に企業の守るべき「企業行動憲章」を設けた。

1996年に、この憲章をより現実的なものとするべく改定が加えられたが、翌1997年に多くの会員企業から不祥事が起こった。そこで、2002年の再改定時には、企業に対して社内体制整備と運用強化を要請するとともに、経営トップマネジメント自らの自主的な取り組みを促した。そして、法令遵守が社会的責任の基本であることを、再確認するとともに、いっそうの自主的な取り組みを促進するため、2004年5月に再々改定した。

また、1998年には関西経済連合会(関経連)が、「企業と社会委員会」を設置し、企業が「倫理と法令を誠実に遵守」するために、企業内に有効な内部統制システムが急務であるとして、専門家が集まり「倫理法令遵守マネジメントシステム企画(ESC2000)を作成し発刊した。

リスクマネジメント



リスクマネジメントの出現

- リスクマネジメントという発想が登場したのは、1920年代のドイツといわれている。第一次大戦後の悪性インフレ下で、企業防衛のための経営管理ノウハウとして登場したものだ。
- 一説には、1930年代のアメリカが最初ともいう。いわゆる「大恐慌」による不況下で、企業防衛のための費用管理として登場したものだ。もっとも、当時はリスクをどう保険に移転すればいいのかを考える保険管理(純粹リスク管理)が主体であった。
- それが、時代が進むにつれて変化し、リスクマネジメントの管理対象は、単なる純粹リスクから企業活動全般へと移っていくわけである。

出典：浦嶋 繁樹著 「不況だから普及するリスクマネジメント」

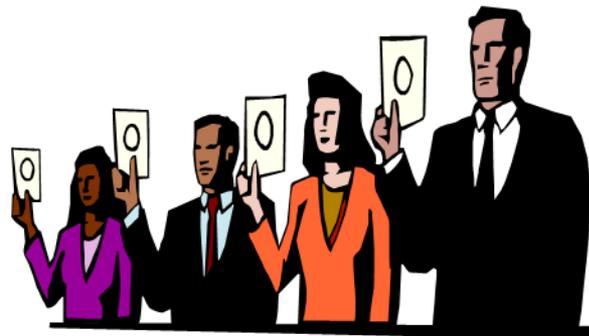
<http://www.nikkeibp.co.jp/sj/2/column/f/06/> (2008.5.18 アクセス)

リスクマネジメントと脆弱性

近年、リスクマネジメントは、主として自然災害に対する保険対策としての財務管理の枠から逸脱して、生産、販売、購買、人事、労務、財務全般に渡る業務活動でのリスク、投資の経済的リスク、さらに企業を取り巻く社会的、国際的リスク等の経営管理の一環として捉えられ、企業の倒産防止として理解されるようになってきた。

しかし、情報システムが高度化し、グローバル化した今日、脆弱性を、異常事態や不測事態といった事故だけでなく、自然災害、ハイテク犯罪、プライバシーの侵害、情報の濫用と社会的混乱、国際的な情報戦争等も含めた脅威を対象に、その脅威の発生原因となった政治、経済、社会、制度、政策、法律、倫理等の起因、事情、環境、状況、状態等を含めた広い「欠陥」として捉える必要が出てきた。つまり、ハザード概念まで含めた欠陥であり、そうになると、ペリル、ハザード、リスクといった厳格な区別は必要なくなり、定量化も目的ではなくなかった。いまや、リスクマネジメントやセキュリティ対策、システム監査等の情報システムの健全化の手法が、より実効ある手法、手続きとして進化させていくうえで、最も基本となるこの脆弱性について分析・整理され、それを理論的に吟味することが必要なのである。

コンプライアンス



コンプライアンスと企業倫理

- コンプライアンスは、一般的に「服従、承諾、追従」などと訳されている。
- 医学界では、薬を守って飲むという「服薬遵守」をいう。
- 実業界では、「法令順守」「法令・規則、社内規定などの遵守」とされている。
- コンプライアンスと企業倫理の関係では、企業における組織倫理、職業倫理、個人倫理の三要素の基盤をなすものである。その基盤の中核がコンプライアンスである。

出典：田中宏司著「コンプライアンス経営」生産性出版 2002

コンプライアンス（法令遵守）

- もともとは1960年代に米国で独禁法違反、株式のインサイダー取引引き事件などが発生した際に用いられた法務関連の用語である。近年では守るべき規範は法律に限らず、社会通念、倫理や道徳を含むと解釈される。
- 企業を取り巻く法律や規則は、民法や商法をはじめ独占禁止法、不正競争防止法、労働法、消費者保護法など多数あり、監督官庁の命令・指導などもある。さらに、営業活動や市場競争の公正さ、消費者などへの情報公開、職場環境（過労死、セクシュアル・ハラスメントなど）、公務員や政治家との関係、証券市場における取引引きなど、多くの面で高い倫理（企業倫理）が求められるようになっている。
- コンプライアンスの重要性が叫ばれるようになった背景には、違法行為や反社会的行為を行って、消費者や取引先の信頼を失い、事業継続が不可能になる企業が頻発するようになったことがある。企業にとってコンプライアンスは、リスクマネジメント活動としてとらえられている場合が多いようだ。しかし、complianceの原義に戻って、社会からの信頼を高めるための戦略的活動として取り組んでいる企業もある。

出典：「IT情報マネジメント」2007. 12.17 アクセス

<http://www.atmarkit.co.jp/aig/04biz/compliance.html>

参考文献

- [1] 櫻井通晴著「コーポレート・レピュテーション」中央経済社 2006
- [2] 松田貴典編著「コーポレート・レピュテーション戦略」工業調査会 2007
- [3] 土田義憲著「財務報告に係る内部統制の実務」中央経済社 2007
- [4] 日本コーポレート・ガバナンス・フォーラム, パフォーマンス協会編『コーポレート・ガバナンスと企業パフォーマンス』白桃書房, 2002
- [5] 松田貴典著「ITガバナンスを支援するシステム監査－ガバナンス関連法の内部統制とシステム監査－」『月刊監査研究』第33巻第8号 (財)日本内部監査協会 2007
- [6] 田中宏司著「コンプライアンス経営」生産性出版 2002
- [7] オラクル社ホームページ, 『「G、R、C」は三位一体で:「戦略的」内部統制を実現し、攻めの経営へ』,
<http://mag.executive.itmedia.co.jp/executive/articles/0711/29/news001.html>
(2008.2.14アクセス)
- [8] SAPジャパン社ホームページ, 『GRCを体系化した「Virsa Compliance Calibrator for SAP」』:
<http://japan.zdnet.com/news/software/story/0,2000056195,20121807,00.htm>
(2008.3.1アクセス)