研究レポート

企業に求められるITガバナンスの新しいモデル

原田　要之助*
Yonosuke Harada

SUMMARY
現在、企業はコーポレートガバナンスの確立が求められている。コーポレートガバナンスの中でも重要となっているのがITや情報セキュリティのガバナンスである。本稿では、企業に要請されるITガバナンスを紹介し、今までのモデルとその限界を示し、新しいモデルを提案する。

1　企業の情報活動とIT

情報活用は、今や、企業にとっての企業価値と等価なものとなっている。そのため、企業にとって、情報の収集、活用、蓄積、転送、廃棄にわたる情報のライフサイクルに対するマネジメント及び情報システムに対する管理が重要となっている。例えば、企業は個人情報の取り扱いについて、企業のITで利用する場合、企業が個人から情報提供を受けて、コンピュータに入力し、データベースとして活用し、その個人の申し出やサービスの終了などで情報を廃棄するまでのプロセスにおいて、情報を正しく管理する義務がある。これを実現するためには、IT機器が必要となる。企業は、資金調達して、ITに対する投資を行い、機器及びソフトウェアを導入して情報処理に利用する。これらの機器についても、技術や性能面で管理を行い、不要となった場合には適正に廃棄することが必要である。廃棄する際には、内部情報の漏えいが無いように管理する必要がある。すなわち、企業は、競争力をつけ情報を活用するためにITを利用する。この利用について、企業の適切なガバナンスが必要となる。

企業の経営者（以下、経営者という）は、このITに対するガバナンスを実施することが求められている。

2　ITガバナンスと情報セキュリティガバナンス

ITガバナンスは、コーポレートガバナンスと同様に、経営者が経営的な観点から投資や活用について判断を下すことを求めている。経営者は、IT活用のプラスとマイナスの両面、すなわちITの様々な機会とリスクに対してバランスを取りながら判断することが要請されている。ITについても、企業の競争優位に役立つよう戦略的な思考と、ITを利用することによって生じるリスクへの危機管理が重要な要素と

なる。マイケル・ポーターが、「競争の戦略」で、ITの戦略的な重要性を指摘して以降、企業や組織にとってITの活用は、経営者にとって欠かすことのできない重要な要素と考えられるようになっている。

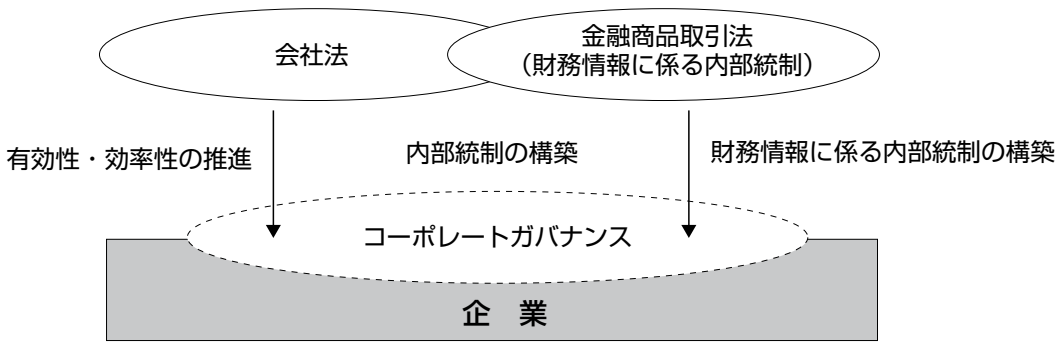
しかし、ITへの負の側面への対応を間違えると企業にとって致命的な問題ともなりうる。みずほ銀行や東京三菱銀行でITシステム統合のミスによって取引ができなかったこと、2006年のみずほ証券の誤発注問題、東京証券取引所の情報システムのトラブルによる証券取引業務の停止、2008年のANAの予約システムのトラブルによる航空便の遅延やキャンセルなど、ITのトラブルが企業の大きなリスクとなることが報告されている。損失については非公表であるが、企業の存続に関わる規模に至ったと言えよう。さらに、金銭的な面のみならず、企業の信用にも大きな汚点となっている。経営者は、ITのプラスの側面ばかりではなく、ITのマイナスの側面についても十分に対応しなければならない。

したがって、ITについてのガバナンスを考えるためには、ITを利用するプラスの戦略面のみならず、ITに伴うリスクをも同時に考えておく必要がある。

2-1　企業の会社法とコーポレートガバナンス

2008年からはじまった金融商品取引法に伴う、内部統制報告書の義務化では、経営者は内部統制を確立し、財務報告が正しいことを報告する義務がある。この内部統制の確立では、企業の売上から経費の支払いに至るまでITがかかわっていることから、ITに係る統制が重要なテーマとなっている。また、会社法では、善管注意義務及びリスク管理が義務付けられており、企業の価値を向上させる義務がある。前者としては、会社法では、「取締役の職務の執行が法令及び定款に適合することを確保するための体制」（法362条4項6号）について、コーポレートガバナンスの必要性を述べている。すなわち、経営者には、企業の重要な資産（ITを含む）を活用させて、収益をあげる義務があることになる。一方、後者については、「損失の危険の管理に関する規程その他の体制」（施行規則100条1項2号）からは、リスク管理体制の整備が要請されている。しかし、会社法では、具体的に「損失の危険の管理に関する規程その他の体制」について規定されているわけではない。例えば、日本監査役協会の「内部統制システムに係る監査の実施基準」では、監査役の責務として、リスク管理体制の整備と運用についての監査やリスク分析・評価等が述べられている。したがって、経営者には、リスク管理体制の整備と実施が結果的に要請されていると考えられる。これを図表1に示す。

図表1　会社法、内部統制とコーポレートガバナンスの関係



2-2　企業の IT ガバナンスと情報セキュリティガバナンス

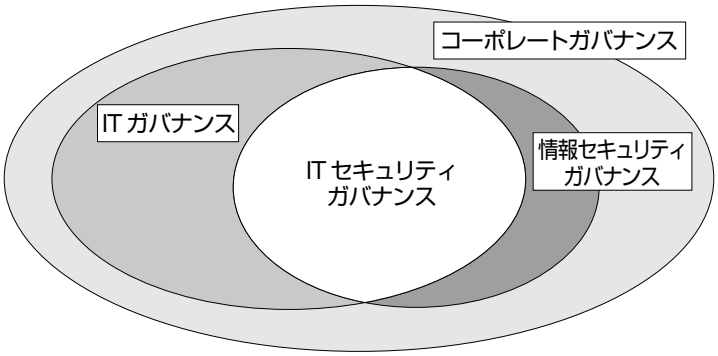
企業の情報活動の観点に絞って見ると、会社法では、効率的な企業の付加価値創造に必要となる情報活用、IT への投資と投資による企業の付加価値の向上が必要となる。企業の効率性向上のための IT 投資はかなりの金額となる。一方、IT は、内部が見えないため、内部でどのような活動がなされているかについて、不明であり、投資金額も多いことから、ステークホルダ（利害関係者）への Accountability（説明責任）が求められている。

金融商品取引法は、すべての上場会社に対して、2008 年度の会計年度から、内部統制について経営者が評価し報告することを義務付けている。この内部統制の確立においても、IT に対する内部統制（IT 統制）が重要な要素として挙げられている。

2-1 では、会社法や金融商品取引法の観点から、これらがコーポレートガバナンスを重視すると述べた。これを IT の側面から見ると、資産に発生する IT による様々なリスクが存在し、これらのリスクを低減するコントロールの実装にはコストが必要である。すなわち、資産を保全するための投資や人的資源が必要となる。これを、一般的には、情報セキュリティガバナンスと呼ぶことになる。この 2 つの関係について、IT ガバナンスと情報セキュリティガバナンスは、包含関係にはない。これを図表 2 に示す。

図表 2 では、IT に係る情報セキュリティについては、IT ガバナンスと共通するが、例えば、入退出管理システムによる物理的セキュリティ（この場合も、IT が利用されていると考えることもできるが、目的が物理的セキュリティなので、IT ガバナンスに含めることは無理がある）や企業で利用する紙情報の管理などが含まれる（なお、このモデルについては、日本が ISO に提案した文書（ISO SC27 WG1 SC27N6946　Japanese National Body contribution to WG 1 Study Period on Information security governance）の中でモデルを提示しており、今後、国際標準の場で議論されて、何らかの方向性が示されると考えられる）。

図表２　IT ガバナンスと情報セキュリティガバナンスの関係



経営者の責任としてのガバナンスの観点からは、情報セキュリティガバナンスに特徴的な物理的セキュリティや紙情報によるセキュリティに、経営者が投資や運用から係わる必要がある。多くの企業では、経営者は、全体の予算の中で、IT や情報セキュリティへの投資を考えており、情報を紙で管理するか IT で

管理するかなどの運用面については、事業の執行にまかされているとも考えられる。すなわち、IT と情報セキュリティは、IT が共通項であり、これらについてのガバナンスは共通するところが多いが、これを分けて議論する場合と共通に議論する場合があることになる。

本稿では、経営者の立場から、IT ガバナンスと情報セキュリティガバナンスは共通する点が多いことから共通する IT ガバナンスについて述べることとする（付録に、経済産業省が検討中の情報セキュリティガバナンスを紹介する）。

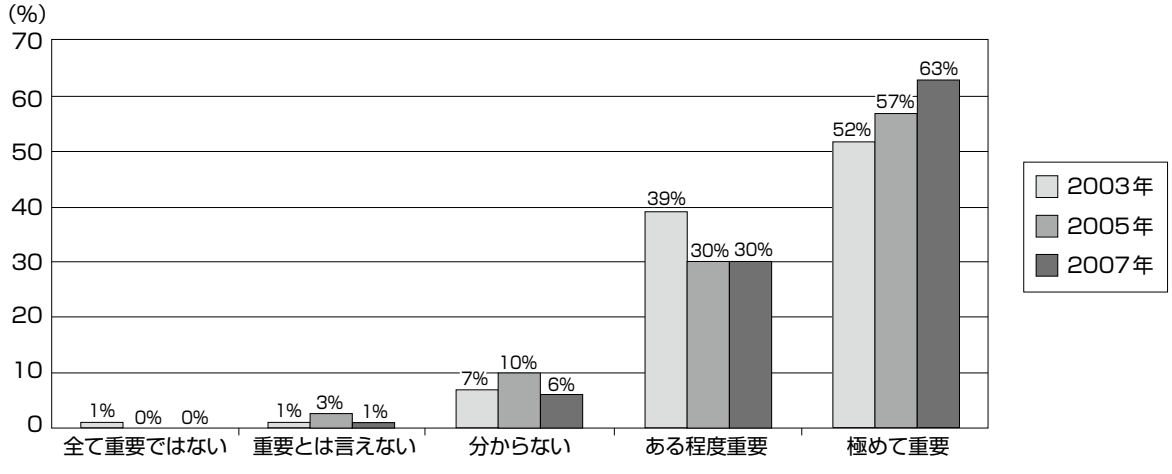
3　IT ガバナンスの現状

現在、多くの企業で IT ガバナンスの実施が行われている。これを検証するために、以下では、2008 年に IT ガバナンス協会（以下、「ITGI」という）と PWC（プライス・ウォータハウス・クーパース：米国の 4 大監査法人の 1 社）が全世界の企業に対し調査して、23 カ国 739 社から回答を得た調査結果を紹介する。

3-1　IT の重要性の認識

図表 3 は、世界の主要企業を対象に企業にとって IT の重要性について認識調査したものである。企業では、「極めて重要」、「ある程度重要」と回答した企業の比率は、2007 年では、63%、30% となっている。合計すると 93% の企業が、IT を重要なものと認識している（このような調査に回答するという観点からも当然の結果である）。また、「極めて重要」は 2003 年、2005 年、2007 年と増加しているが、「ある程度重要」と「極めて重要」の合計については、2003 年の 91% が 2005 年には 87% に減少した。しかし、2007 年には合計が 93% となっていることから、一時的な停滞であり、増加傾向にあると考えられる。すなわち、IT は企業にとって、極めて重要な存在となっていることがわかる。

図表 3　世界の企業における IT の重要性



出所：“IT Governance Global Status Report,” IT Governance Institute, 2008

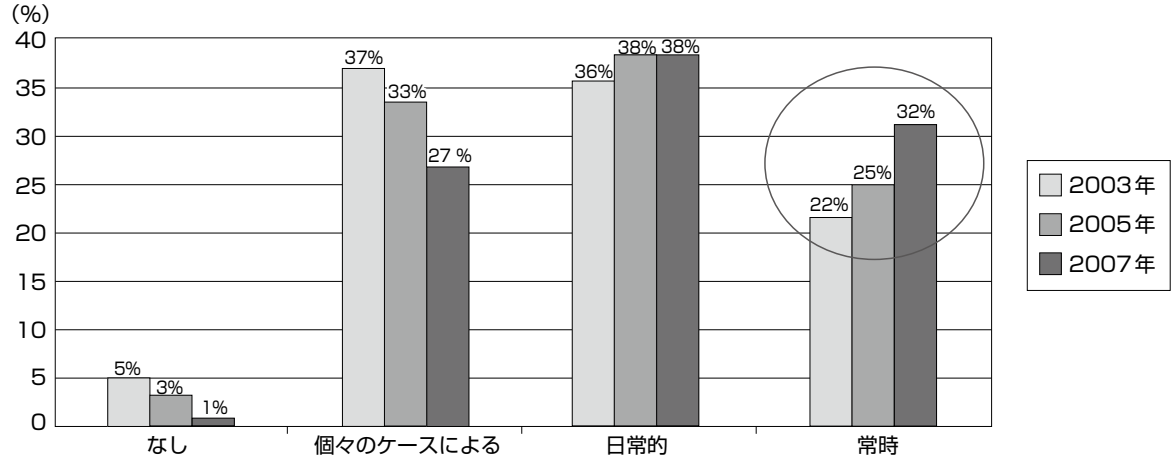
3-2　企業の取締役会（ボード）でのITが議論される頻度

ITガバナンスの重要な議題としては、ITへの投資が挙げられる。

図表4は、企業のボードでITが議題として論じられているかについての頻度を調査した結果である。ここでは、「日常的」、「常時」と回答した企業の比率は、2007年では、38%、32%となっている。合計すると70%の企業が、ボードでITについて議論されていることがわかる。ボードで議論されるのは、ITへの導入や改修などのITへの投資や、IT導入の効果の検討などである。図表4では、2003年の調査で、「日常的」、「常時」の合計が58%、2005年は63%と増加していることが分かる。さらに、2007年の調査では、ボード時でITについて論じたことが「なし」の企業は全体の1%となっている。すなわち、ITは企業にとって、極めて重要となっていることが分かる。

これは、企業の全体の投資の中でITの占める割合が増え、ボードでの重要な議題となっていることが分かる。すなわち、企業にとって、ITガバナンスは、経営者にとって、今後の経営で重要なものとして扱われていることが分かる。

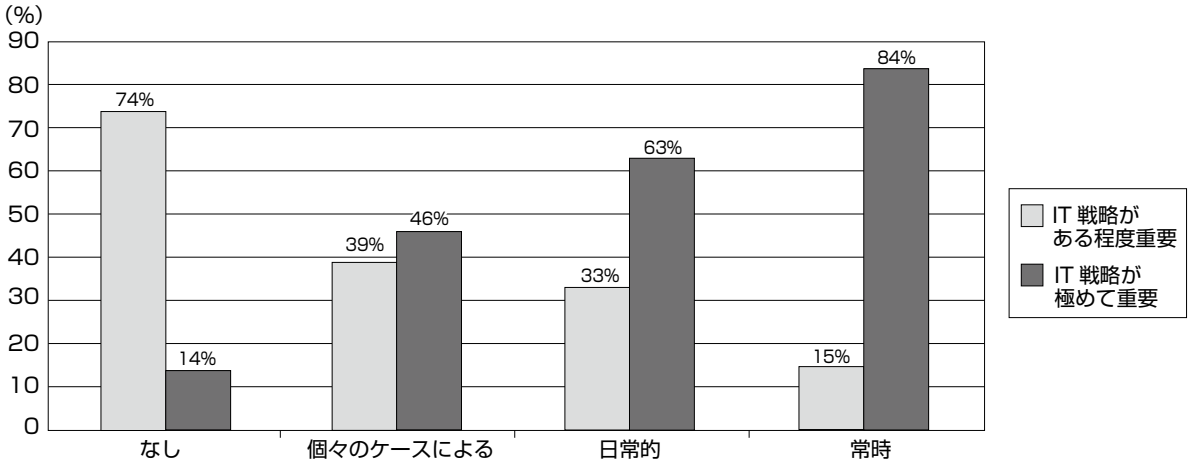
図表４　世界の企業におけるボードでITが議題となる頻度



出所：“IT Governance Global Status Report,” IT Governance Institute, 2008

次に、図表5に企業のボードでのITが議題となる頻度と企業でのIT戦略の重要性についてのクロス分析の結果を示す。ここでは、「IT戦略がある程度重要」、「IT戦略が極めて重要」の2つの回答を、図表4のボードでのITが議論される頻度で示したものである。「IT戦略がある程度重要」とする企業では、ITがボードで、議論されたことが「なし」が最も多く、74%となり、「日常的」に議論されている企業の比率は15%となっている。一方、「IT戦略が極めて重要」としている企業については、ITがボードで、議論されたことが「なし」が最も少なく、14%で、「日常的」に議論されている企業の比率は84%となっている。すなわち、IT戦略を重要視している企業は日常的にボードで、ITが議論され、ITの重要性が認識されていることが分かる。一方、IT戦略がそれほど重要ではない企業はITが十分に活用されていないとも言えよう。

図表５　ボードでの IT の取扱いと IT 戦略の重要性の関係



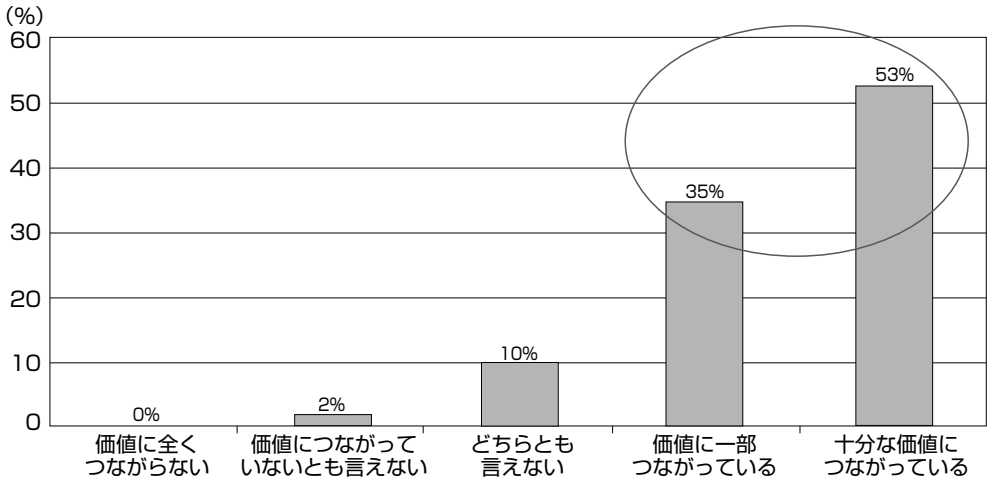
出所：“IT Governance Global Status Report,” IT Governance Institute, 2008

3-3　IT ガバナンスと企業価値の創造

IT は、企業にとって、ビジネスの効率化を高め、収益を保証するものでなければならない。図表 6 は、企業にとって、IT が企業価値の向上にとって役立っているかについて調査した結果である。この結果からは、「十分な価値につながっている」が 53% と「価値に一部つながっている」が 35% で、合計すると 88% の企業が企業価値の向上につながっていると答えている。「価値につながっていないとも言えない」企業は 2% である。すなわち、IT を導入している多くの企業は、IT の及ぼす効果について認知していることが分かる。

換言すれば、企業にとって、もはや、IT をビジネスに利用することの正当化についての議論でなく、価値をより高める効率性に移ったと言いえよう。

図表６　世界の企業のうち、IT ガバナンスが価値の創造につながっているか

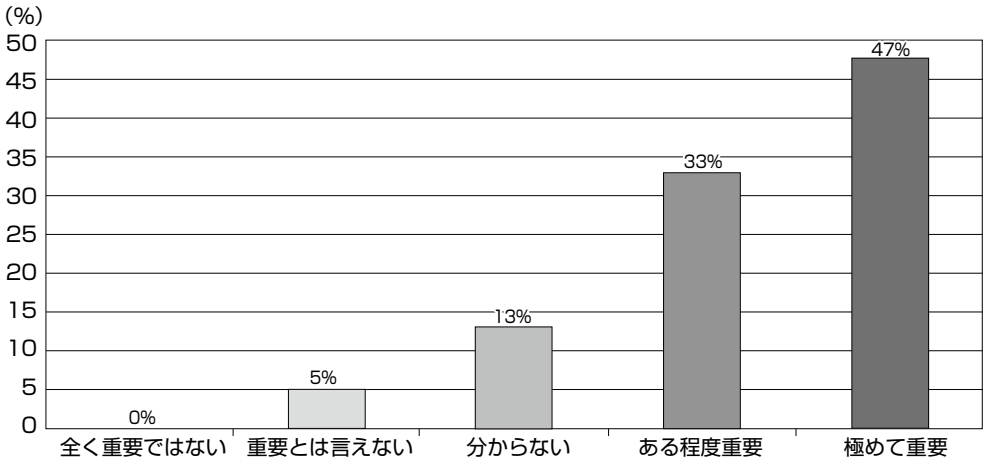


出所：“IT Governance Global Status Report,” IT Governance Institute, 2008

3-4　IT のリスクマネジメント（情報セキュリティガバナンスの重要性）

IT を導入すると、価値の面ばかりではない。IT のマイナスの面についても目を向ける必要がある。図表 7 は、世界の企業が IT リスクマネジメントについて、どのように考えているかについて調査した結果である。この結果からは、「極めて重要」と「ある程度重要」を合わせると 80% の企業が重視していると答えている。「重要とは言えない」企業は 5% である。すなわち、ほとんどの企業が IT のリスクマネジメントについて重視していることが分かる。

図表 7　世界の企業のうち、IT リスクマネジメントの重要性認識

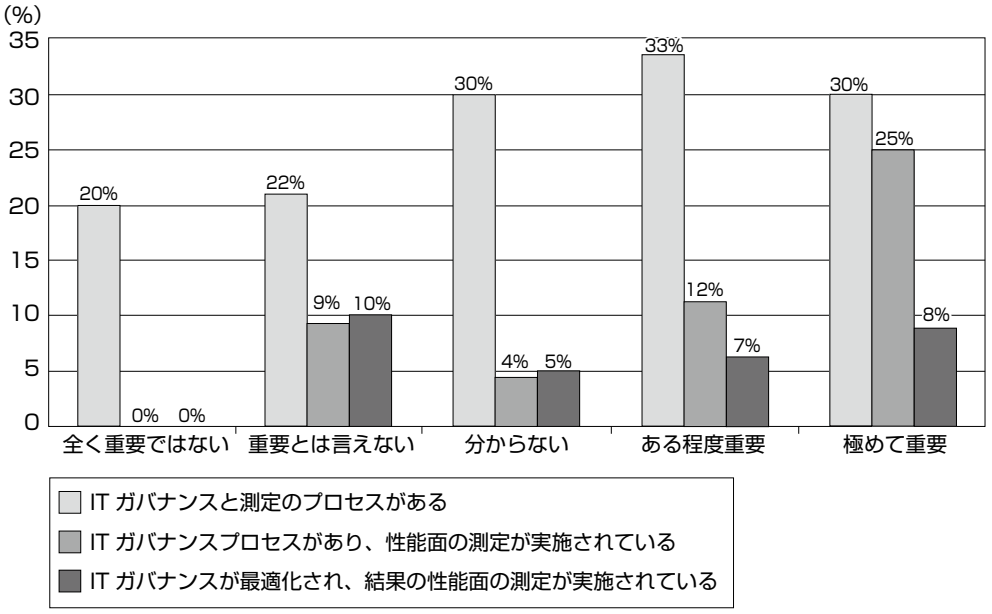


出所：“IT Governance Global Status Report,” IT Governance Institute, 2008

3-5　企業の IT リスクマネジメントと IT ガバナンスの関係

図表 8 は、企業の IT リスクマネジメントの重要性と IT ガバナンスの段階についてのクロス分析をしたものである。「IT ガバナンスと測定のプロセスがある」、「IT ガバナンスプロセスがあり、性能面での測定が実施されている」、「IT ガバナンスが最適化され、結果の性能面の測定が実施されている」の 3 つを、IT リスクマネジメントが「極めて重要」、「ある程度重要」、「分からない」、「重要とは言えない」、「全く重要ではない」のどの段階かを分析した。図表 8 からは、「IT ガバナンスが最適化され、結果の性能面の測定が実施されている」企業は、IT リスクマネジメントが「極めて重要」、「ある程度重要」が、8%、7% となっている。しかし、「重要とは言えない」が 10% ある。「IT ガバナンスプロセスがあり、性能面での測定が実施されている」企業は、IT リスクマネジメントが「極めて重要」、「ある程度重要」が、25%、12% となっていて、重視している企業が若干多いことが分かる。「IT ガバナンスと測定のプロセスがある」企業は、IT リスクマネジメントが「極めて重要」、「ある程度重要」が、30%、33% となっている。すなわち、「IT ガバナンスと測定のプロセスがある」だけの企業では、IT リスクマネジメントの重要視の程度については、ほとんど差が見られない。一方、「IT ガバナンスプロセスがあり、性能面の測定が実施されている」及び、「IT ガバナンスが最適化され、結果の性能面の測定が実施されている」企業では、IT リスクマネジメントを重視する傾向にある。

図表８　世界の企業のうち、IT ガバナンスのレベルと IT リスクマネジメントの重要性認識の一致度



出所：“IT Governance Global Status Report,” IT Governance Institute, 2008

以上、ITGI の調査結果からは、世界の企業では IT ガバナンスが広がりつつあることが分かる。さらに、企業では IT リスクマネジメントの実施についても、IT ガバナンスと相関が高く、IT ガバナンスと合わせて、情報セキュリティガバナンスも重視していることが分かった。

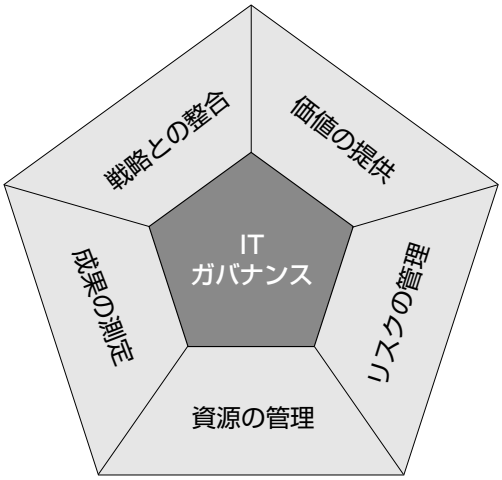
4　企業の IT ガバナンスの構築について

本章では、IT ガバナンスの構築について述べる。

4-1　IT ガバナンスの５つの重要な要素

ITGI のモデルでは、「IT ガバナンスとは、経営者の責務であり、企業のコーポレートガバナンスにとって不可欠な要素であり、透明性が必要な部分であり、IT ガバナンスフレームワークと整合している必要がある。経営者は情報セキュリティにより発生する事故によるサービス中断や情報漏えい機密性に対応する責任がある。また、「取締役会は、情報セキュリティを企業ガバナンスの取り組みの中心的な部分として、IT ガバナンスの目標と整合し、資源を管理するために実施するプロセスと統合する必要がある。」（ISACA/ITGI、取締役のための IT ガバナンス V2 を一部修正）と定義して、IT ガバナンスを支える５つの要素として、戦略との整合、価値の提供、リスクの管理、資源の管理、成果の測定を必要不可欠なものとして列挙している（図表 9）。マイケル・ポーターも競争の戦略では、戦略面を重要視して、他の要素と区別しているように、経営者から見ると、企業の戦略や収益に直結する価値の実現を優先しがちである。ITGI では、これらの５つの要素を等しく重要なものとして扱っている。

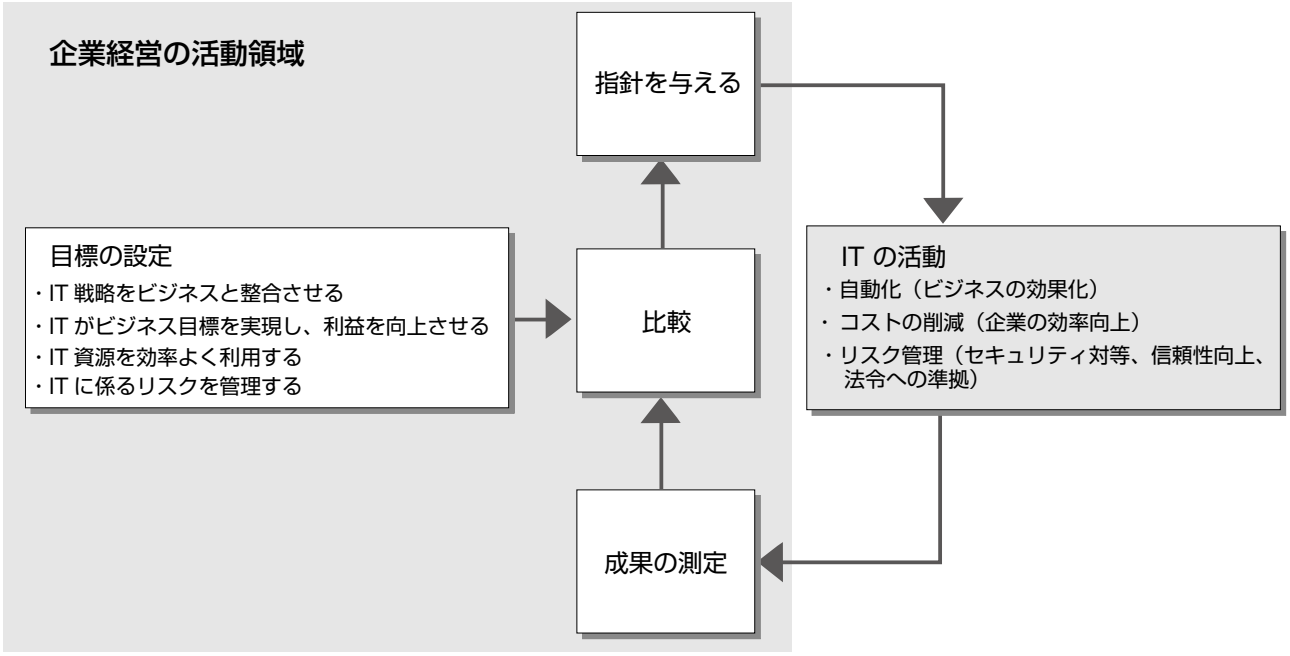
図表９　IT ガバナンスの５つの要素



出所：ISACA/ITGI、『取締役のための IT ガバナンス V2』、2007 年

さらに、ITGI では、経営者が、IT ガバナンスを実施するためのモデルとして図表 10 を示している。このモデルでは、経営者は、組織に対して、目標を与え、IT による具体的な行動（IT アクティビティ）に対して「指針を与え」、結果としての「成果の測定」を行い、目標との乖離を比較する。乖離が大きければ、その原因を分析し、目標に合うように指針を修正する。この際の目標の設定は、具体的に、組織が行動できるためのものでなければならない。このときの目標には、図表 9 の「価値の提供」、「リスクの管理」と、この 2 つをビジネスの目標と整合するように戦略を決める「戦略との整合」が用いられる。

図表 10　IT ガバナンスの実施のための経営者の行動



出所：ISACA/ITGI、『取締役のための IT ガバナンス V2』を一部修正

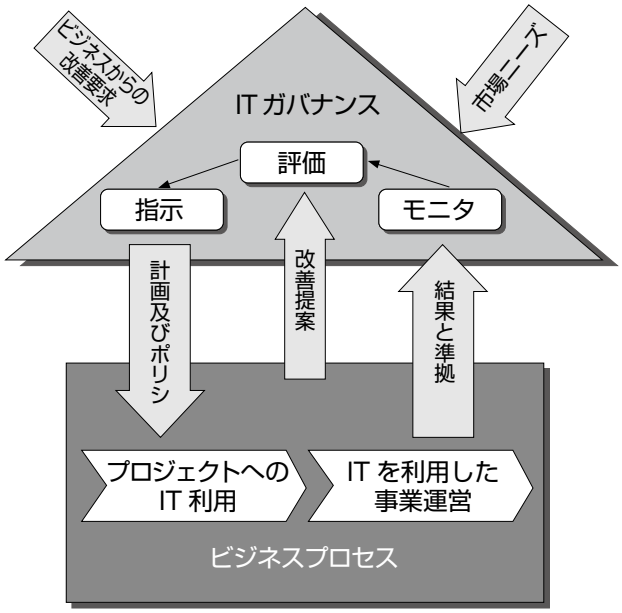
4-2　IT ガバナンスの国際標準化

IT ガバナンスの構造として、ISO/IEC38500 では、ITGI の図表 9 と図表 10 に対応するものとして、図表 11 のモデルを提示している。この標準は、2006 年にオーストラリアの国内基準である AS8500 をベースに、ISOSC7 に早期標準化提案されたものである。ISO/IEC38500 では、企業の経営者が実施するべき行動として、①指示（Direct)、②評価（Evaluate)、③モニタ（Monitor)、がある。経営者は、ビジネス環境からの要求や市場に合わせて、企業としての方針を決定する。企業の執行部門からの活動をモニタして、目標との乖離を調べる。その結果と執行部門からの提案を統合的に評価して、実施部門に対して指示を行う。ここで重要なのは、経営者は、IT の投資や利用について決定し、その結果をモニタして、改善を行うことが求められている。さらに、IT ガバナンスを実現するための 6 つの原則が述べられている。これらは、① IT に対する責任を明確にする原則（Responsibility)、② IT は組織の目的を最大限支援する原則（Strategy)、③ IT の有効性を高める適用原則（Acquisition)、④ IT の可用性を高める性能原則（Performance ）、⑤ IT が法令や企業の内部の取決めに準拠する準拠原則（Conformance)、⑥ IT は人的要素を考慮する人的行動原則（Human behavior）である。これらの原則については、ITGI の「取締役のための IT ガバナンス V2」と同様、ISO の標準というものの、抽象的な表現となっている。今後、ISO では、この標準の具体化とともに、企業に実現するための導入ガイドラインなどの標準を追加予定である。

ISO の国際標準ではあるが、企業がこのガイドラインに従うための認証システムにつながるかは現状では明らかではない。ITGI では、IT ガバナンスについて、企業の努力目標としての概念フレームワークを提示しているのみであり、COBIT などのコントロールを導入する際のフレームワークとしているわけではない。あくまでも、企業の経営者に向けた IT を正しく利用するための考え方を提示しているにすぎない。しかし、IT ガバナンスが ISO で標準とされたことにより、今後、ステークホルダは、企業や組織に対して、IT の適正な利用を確約するためのものとして、要請するようになる可能性がある。企業としても、様々なステークホルダに対して、それぞれの要求事項を満足するよりも、国際的なガイドに従うほうが、実施が簡単ということもある。標準がどこまで具体的に規定するかによって、今後の展開が変わるものと考えられる。

ITGI の図表 10 に示すモデルと ISO/IEC38500 のモデルは、経営者が IT について、戦略的に判断し、その成果をモニタリングして評価する観点では共通している。原則などについても共通するところが多い。今後、この 2 つのモデルは共通化されるか、あるいは、マッピングという形で関連性が示されることになると考えられる（マッピングとは、多数の類似した標準間で、共通する点、異なる点を比較した表を提示することをいう。これによって、一つのガイドラインに準拠していることが、他の基準では、どのように準拠しているか読み替えることができる)。

図表 11　ICT ガバナンスの構造



出所：ISO38500

4-3　IT ガバナンスの進め方

IT ガバナンスや情報セキュリティガバナンスを構築して企業の IT を進めるためには、経営者は、図表 9 と図表 10 を組み合わせて図表 12 のように進めることになる。まず、ビジネスの戦略と整合した IT の戦略を策定（図表 12 「戦略の定義」）して、実施することが必要である。ここで、新しい価値の提供（図表 12 「価値の創出」）と企業のリスクの管理（図表 12 「価値の保全」）をバランスさせる必要がある。この 2 つの領域を進める中で経営資源（図表 12 「資源の管理」）の配分を行い、2 つの活動を統合して改善（図表 12 「継続的な改善」）を行い、その結果を測定（図表 12 「成果の測定」）して、評価する。経営者は、この評価に基づき、戦略の見直しや新しい戦略の策定を行う。

なお、価値の提供とリスク管理を経営者が戦略に基づいてバランスさせながら展開していく観点が重要である。これは、経営者が企業戦略を例えば、リスク管理だけに注力すると、リスクの低減にのみ目が行き、リスクを低減するための投資ばかりするようになり、企業の経営としてバランスを欠くものとなってしまうからである。すなわち、企業戦略では、必ずしも、価値の提供だけやリスク管理の視点のみで進めてはならない。経営者は、企業の戦略の中で、収益を上げ、かつ、リスクを最適化して、結果として、ステークホルダに理解されることが重要である。

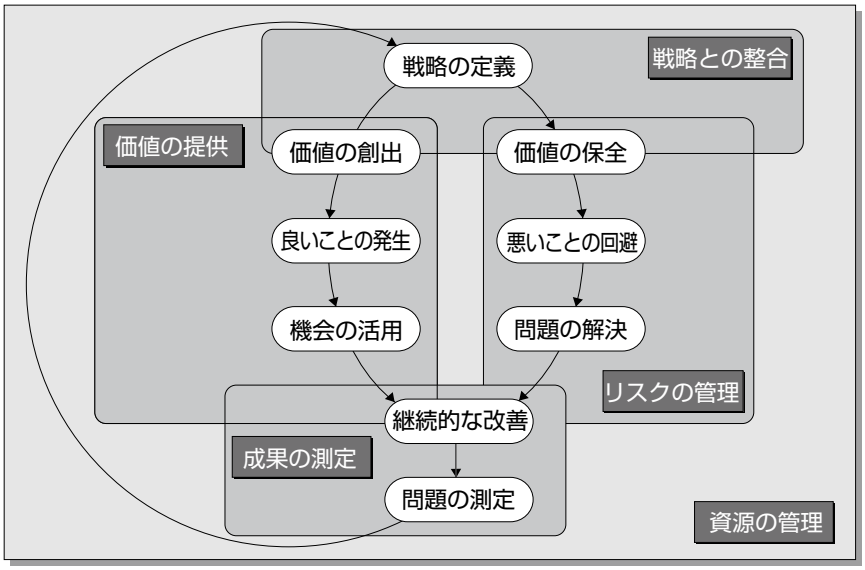
ここで、注意しなければならない点は、図表 12 の流れでは経営者が IT 戦略で「価値の創出」と「価値の保全」を決めれば、あとは、単に、その目的に従って進めていくように読める。価値の創出をするために、自動化されていないビジネスプロセスに IT 投資を行って自動化するケースを考えてみよう。

まず、ビジネスに IT を応用するために BPR などによってビジネスプロセスを見直し、最適な IT を導入するであろう。この際、ビジネスに IT を導入することによって、ビジネスリスクが持ち込まれる。さら

に、導入したITが停止したり、誤動作したりするリスクを考えなければならない。一方、価値の保全として、ITリスク管理を実施する場合には、リスク対応をすることによってビジネス機会が増すこともある(一般に「機会リスク」と呼ばれる)。例えば、情報セキュリティ対策が十分に完備された在庫管理システムを関連会社に利用させて企業グループの情報セキュリティ対策を強化することができる。また、このシステムを外販して収益につなげることもできる。すなわち、機会リスクは企業のさらなる価値の向上につなげることができる。

「価値の創出」と「価値の保全」は、相対する二つのプロセスであるが、それぞれのプロセスの中に、機会とリスクが存在する。すなわち、価値の創出の中のリスク対策と価値の保全のリスク対策のコントロールは、結果的に同じものとなる可能性がある。したがって、リスク対策については、両方のプロセスに、最適なものとする必要がある。これは、機会リスクと価値の創出をうまくマッチさせることにつながる。図表12では、このプロセスが十分に述べられていない。

図表12　ITガバナンスの構築の進め方



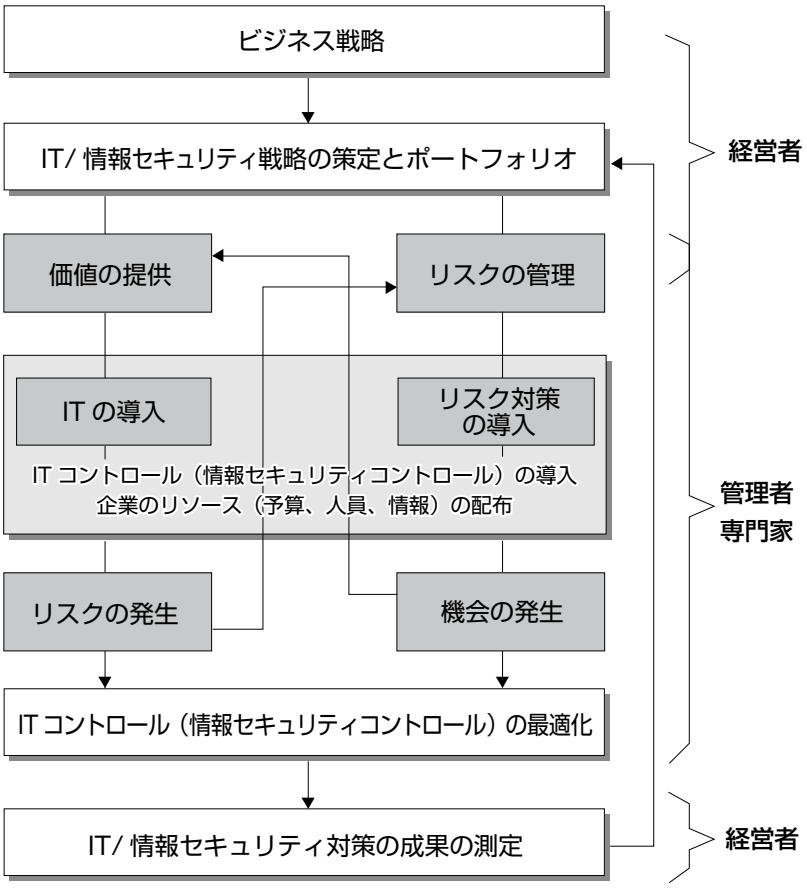
COBIT文書体系の一つである「ITガバナンス導入ガイド」にある図を元に一部改変・追記

出所：日本ITガバナンス協会『COBIT実務者のためのハンドブック』、日経BP、2008年

図表12のモデルに機会リスクと価値の創出を含めると、具体的には、図表13のようなモデルとなると考えられる。図表13では、経営者の役割を価値の提供とリスクの管理までとし、リソースの配分については戦略レベルにとどめ、具体的な展開は管理者層に任せることになる。また、価値の提供とリスクの管理について、上記の複合的な要素を考慮し、価値の提供→ITの導入→リスクの発生については、リスクの管理にフィードバックできるようにしている。同様に、リスクの管理で生じたリスク機会については、価値の提供にフィードバックしている。図表13では、フィードバックの効果を考慮した最適化のプロセスを図表12に追加している。最適化については、与えられた価値の提供、リスクの管理の総合的な実現であり、管理者が実施すべきものである。ここを管理者に任せることにより、現場の総意工夫を促して、企業にとっての価値を最大化できる。経営者は、その結果としての成果を測定評価することになる。

経営者が与えた、「価値の提供」と「リスクの管理」の目標、戦略のバランスについて、得られた成果に問題があるときには、戦略面でのバランスを見直すことになる。

図表 13　リスク機会を考慮した IT ガバナンスのモデル



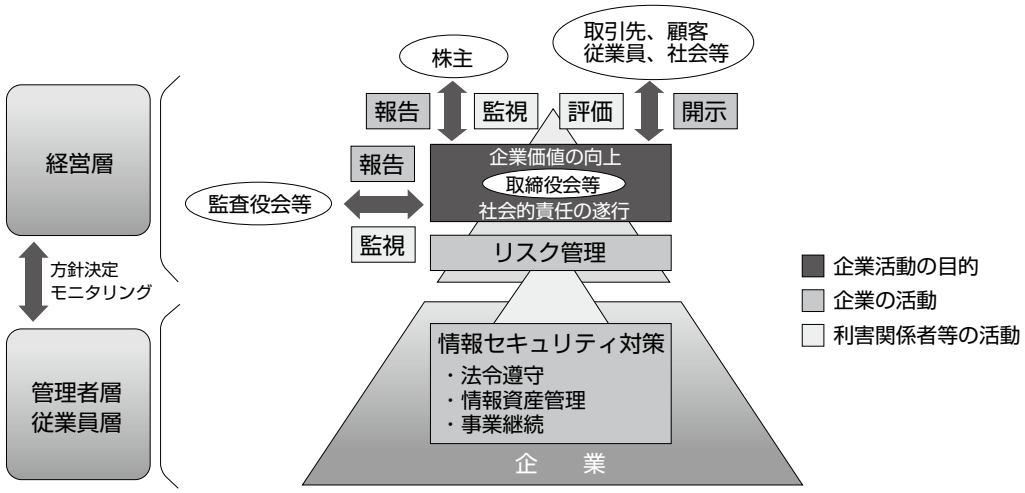
なお、図表 13 のモデルでは、IT や情報セキュリティの側面についての考察だけであり、IT を導入したことによるビジネスの変化や従業員に与える影響についても十分な考察が必要となる。これは、今後の課題である。

5　まとめ

本稿では、企業の IT ガバナンスと情報セキュリティガバナンスについて論じている。とくに、IT ガバナンスは、世界中の企業において、経営者が注目するようになっていることを 2008 年に実施された調査報告から示した。すなわち、日本の企業にとっては、会社法や財務報告による内部統制の導入での IT に対する原則として、IT ガバナンスが目標となると考えられる。既に、導入の済んだ企業にも、次なる目標になる。本稿では、企業に要請される IT ガバナンスと情報セキュリティガバナンスの構造を ITGI 及び ISO のモデルを参考に考察した。従来型のモデルでは、機会リスクを説明できない。そこで、フィードバック効果を考慮に入れた企業の IT ガバナンスを実現するための新しいモデルを示した。

【付録】

経済産業省では、平成 17 年度より、情報セキュリティガバナンスについて検討を行い、下記のモデルを提示している。ここでは、経営者は、リスク管理を実施して、ステークホルダに対して説明責任を持つというものである。



※経営層が取り組む「情報資産に係るリスク管理」を、管理者層・従業員層が取り組む実践的な管理策に詳細化すると、情報資産に係る「法令遵守」、「情報資産管理」、「事業継続」に収斂する構造。
※「監査役会等」、「取締役会等」には、委員会設置会社等の場合を含む。
※「評価」の対象には、顧客からの要望への対応を含む。
※「情報資産管理」には、責任者の設置、情報資産資産の利活用及び漏えい／改ざん防止策等を含む。
※「リスク管理」のリスクには法令違反から生じるリスクを含み、図中の「法令遵守」は管理策を指す。

出所：「企業における情報セキュリティガバナンスのあり方に関する研究会報告書」経済産業省、平成 17 年 3 月

【参考文献】

〔1〕 筆者、「IT ガバナンスと情報セキュリティガバナンスの構築に向けて」、日経 BP セミナー発表原稿、2008 年 8 月

〔2〕 『コーポレートガバナンスの財務的側面に関する委員会報告』（Report of the Committee on the Financial Aspects of Corporate Governance）、キャドバリー・レポート（Cadbury Report）、1992 年）

〔3〕 ISO SC27 WG1 SC27N6946 Japanese National Body contribution to WG 1 Study Period on Information security governance、2008 年 10 月

〔4〕 IT ガバナンス協会、『取締役のための IT ガバナンス V2』、2007 年

〔5〕 日本 IT ガバナンス協会編、『COBIT 実務者のためのハンドブック』、日経 BP、2008 年

〔6〕 ISO/IEC 38500：2008, Corporate governance of information technology、2008 年

〔7〕 AS8015 – 2005, Corporate governance of information and communication technology

〔8〕 IT Governance Global Status Report, IT Governance Institute, 2008

---

* ㈱情報通信総合研究所　主席研究員（ISACA/ITGI 国際本部副会長）